

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC



Cisco Secure Client

Technical Deep Dive

Aaron T Woland, CCIE #20113
Distinguished Engineer, Security
loxx@cisco.com | @aaronwoland |  aaronwoland
BRKSEC-2834

\$ whoami



Cisco role: Distinguished Engineer

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 3 years old!

Fun fact 3: Just graduated from SANS: MS in Cyber Security

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!

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

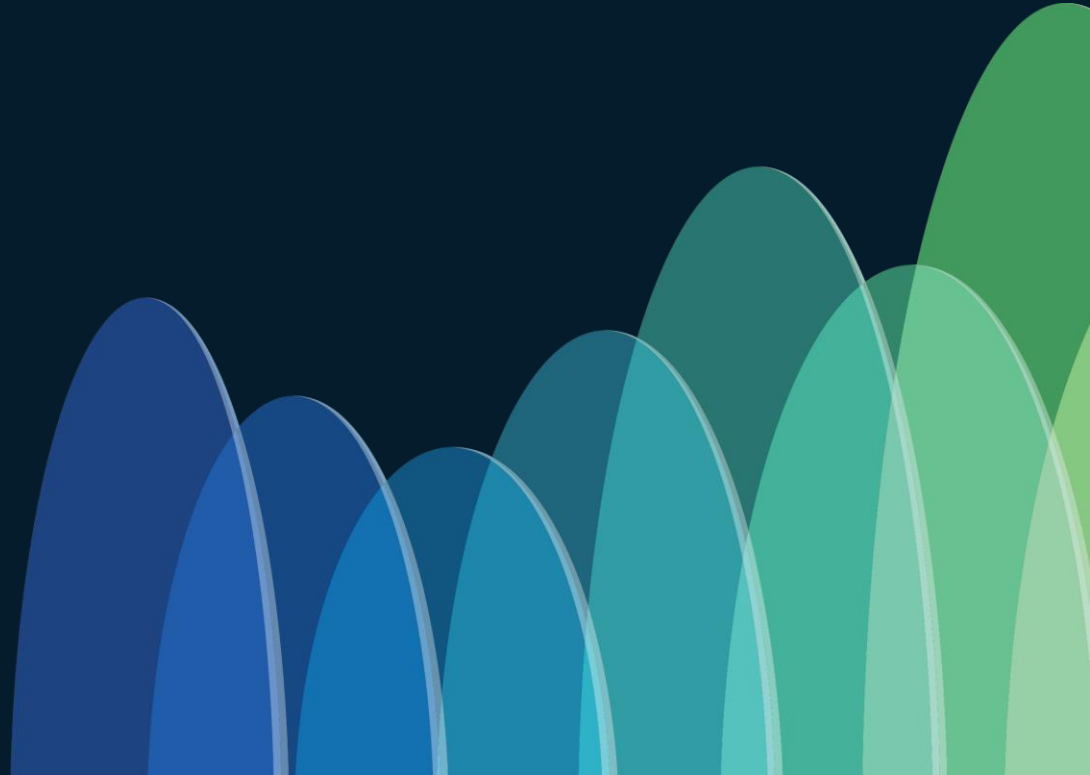
Webex spaces will be moderated by the speaker until November 15, 2024.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2834>



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

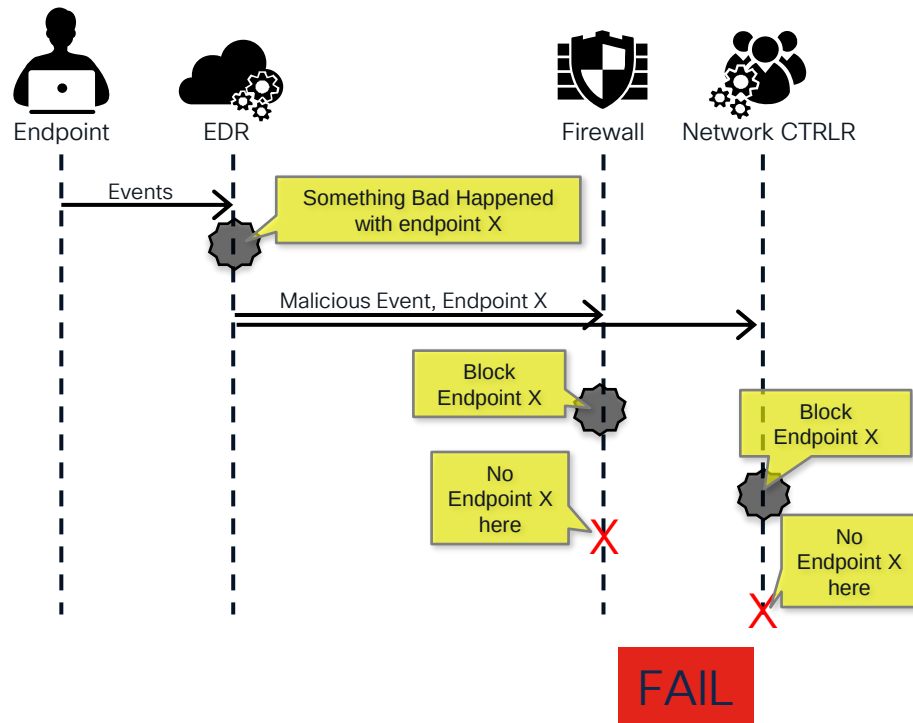
- CSC Overview
- CSC Architecture
- Deploying / Managing from Cloud
- Upgrading to CSC
- FAQs

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”

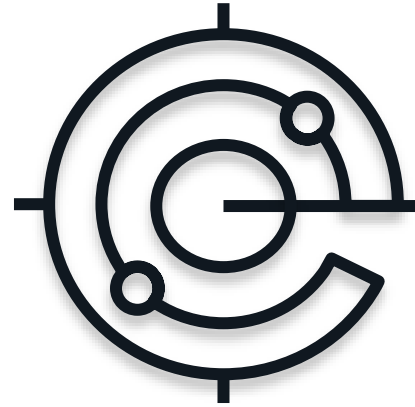
We are doing two things about this

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



Some basics



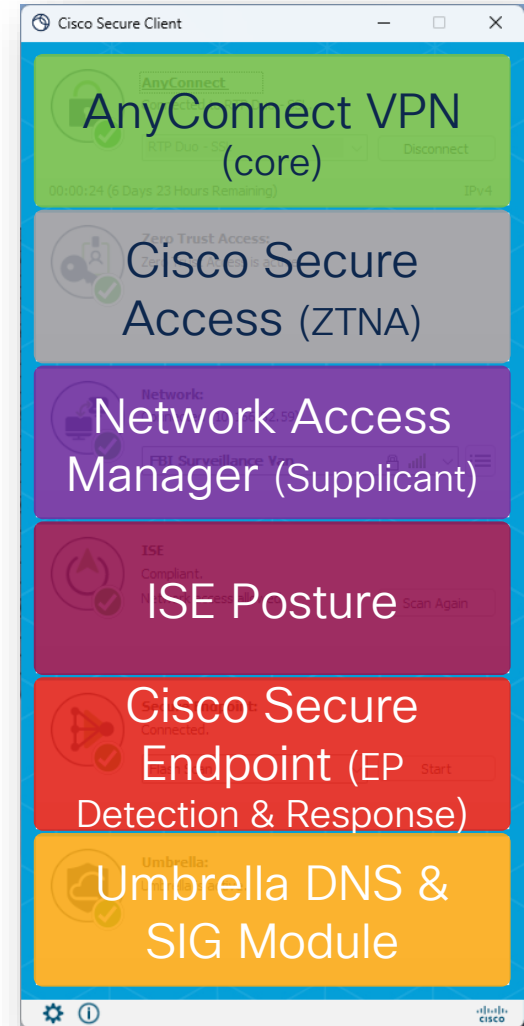
- Windows (AMD64) & macOS** (AMD64 & ARM) Support
- Seamless upgrade to new unified agent from existing AnyConnect & Secure Endpoint Clients
- Leverages Existing AnyConnect Framework
 - AC already has modules for many services
 - AC UI is starting point for new shared UI
 - Core AC services, such as trusted network detection, become available as common services for all modules
 - UI represents only installed functions
- Introduced a new Cloud Management System inside SCCM & XDR

Cisco Secure Client

Suite of security service enablement modules

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

CISCO *Live!*



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 main header area contains the Cisco logo and the text "Secure Client". A left-hand navigation pane lists several options: "Status Overview", "AnyConnect VPN", "Network", "ISE Posture", "Secure Endpoint" (which is highlighted with a right-pointing arrow), and "Secure Umbrella". Below this list is a button labeled "Diagnostics..." with the text "Collect diagnostic information for all installed components." above it. The main content area is titled "Secure Endpoint" and has three tabs: "Statistics" (selected), "Update", and "Advanced". Under the "Statistics" tab, there are three expandable sections: "Agent", "Policy", and "Detection Engine". Each section contains a list of attributes and their values.

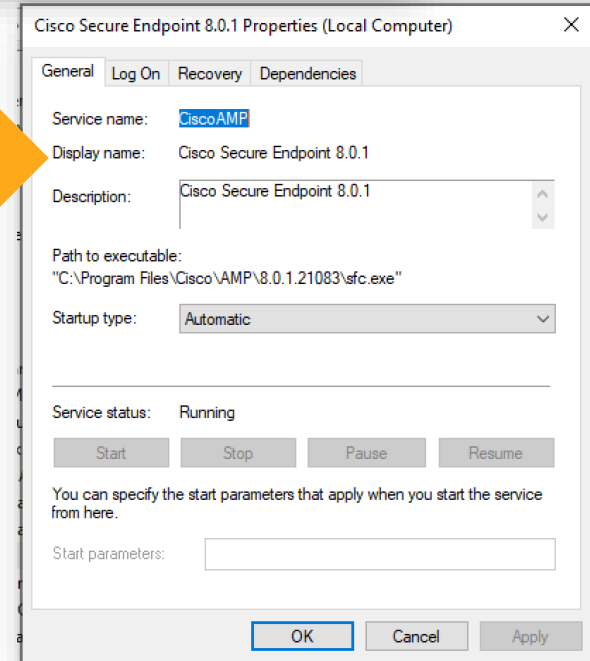
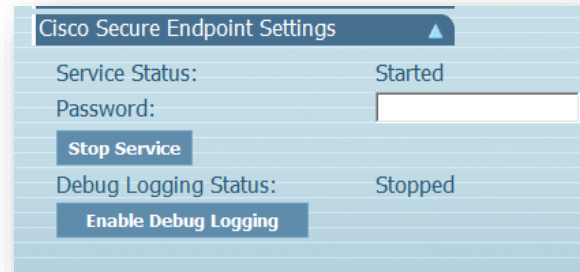
Agent	
Status	Connected
Version	8.0.1.20840
GUID	b2a7d93b-aac4-40a6-a0fe-06eac90f9677
Last Scan	Never
Isolation	Not Isolated

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

More Secure Endpoint UI

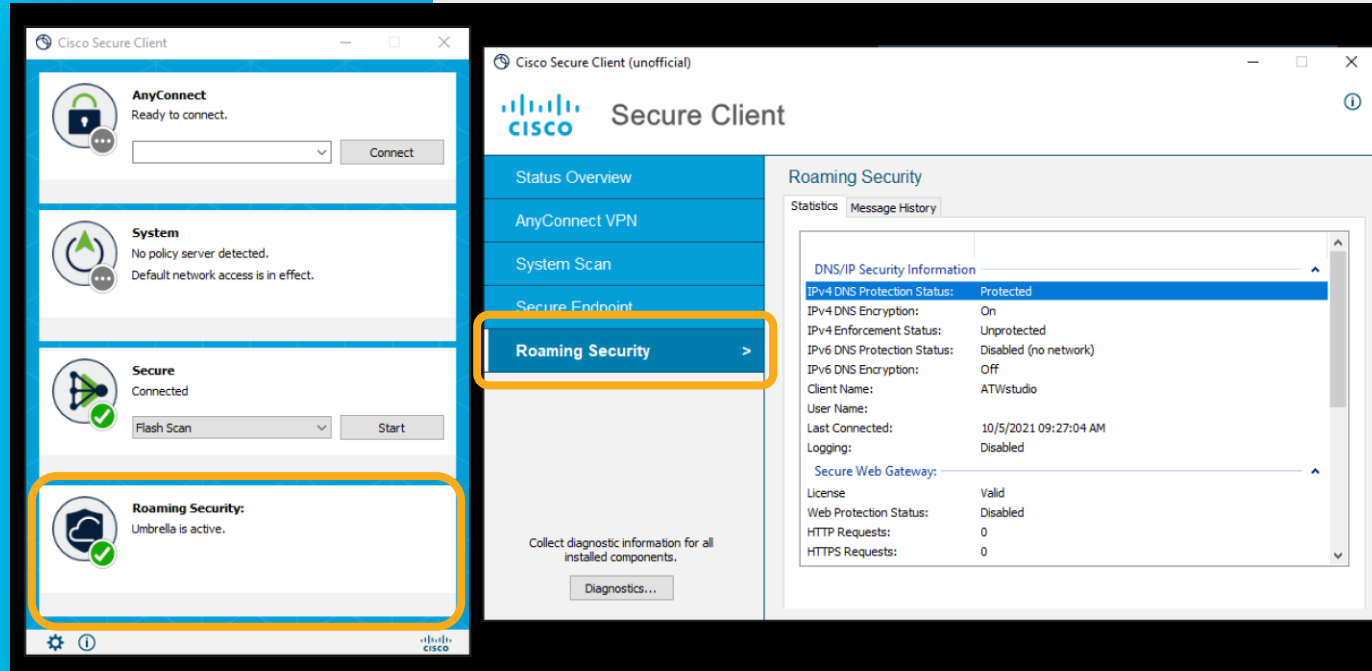
- Removed the ability to control the service from the UI when the connector is protected mode.
 - For security reasons
 - CLI only



Umbrella

Same Umbrella
Roaming from
AnyConnect:

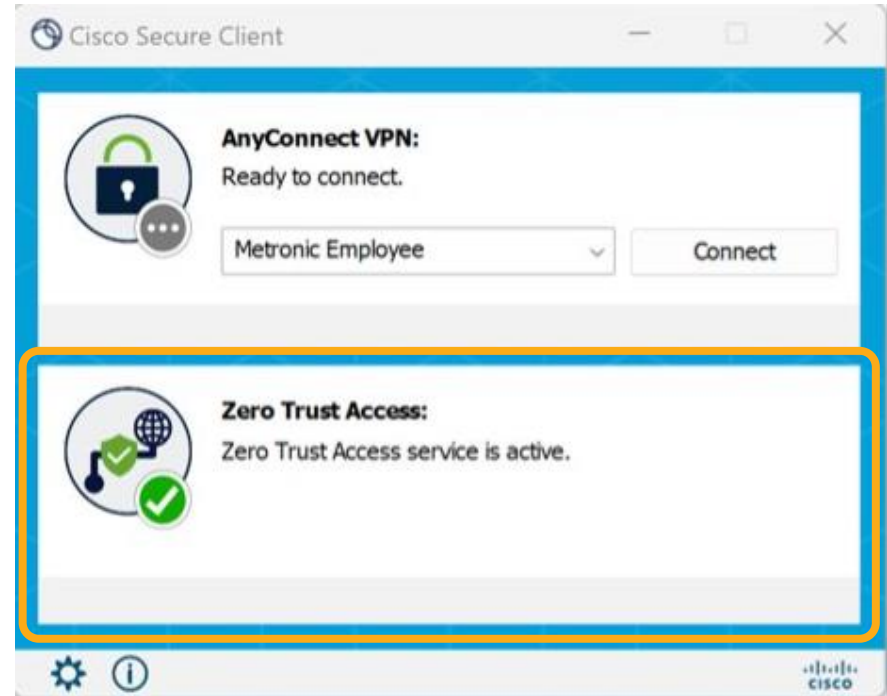
- Umbrella DNS
- Secure Web Gateway



ZTNA Module

For Cisco “Secure Access”

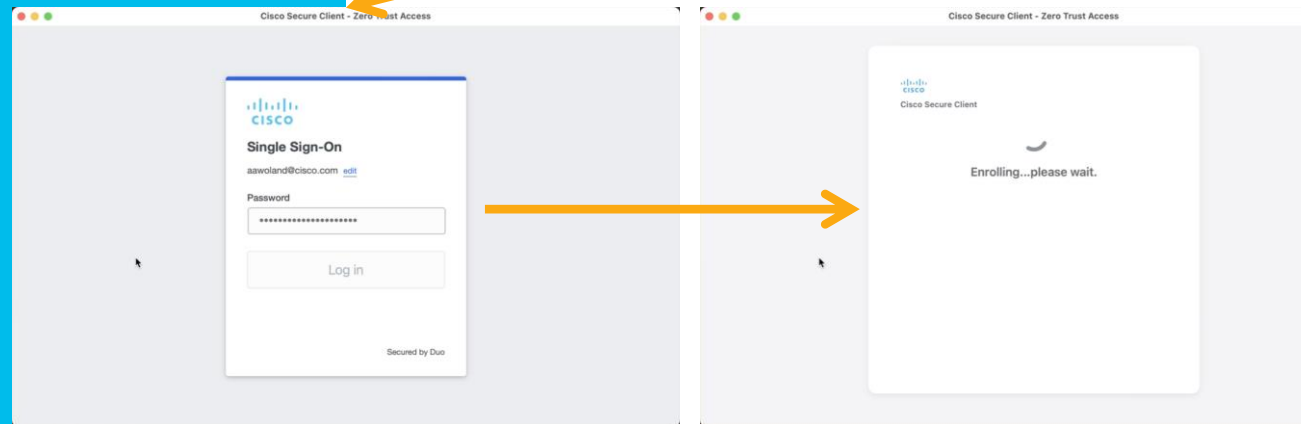
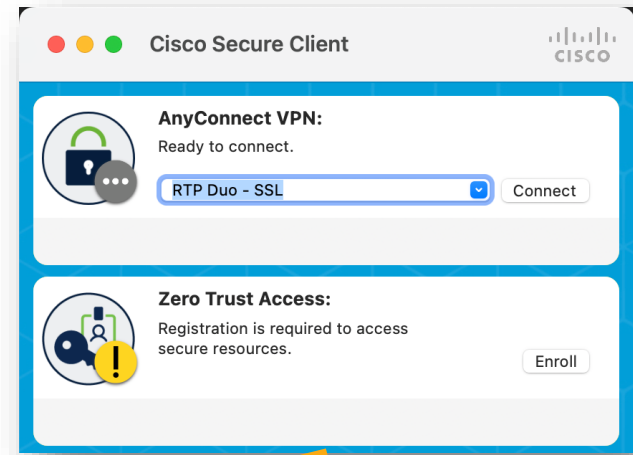
- Brand-New Module
- Dedicated for Cisco Secure Access
- Side-loads the Duo Health Agent (DHA)
- Uses MASQUE & QUIC for seamless transport



ZTNA Module

For Cisco “Secure Access”

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



Putting it Simply

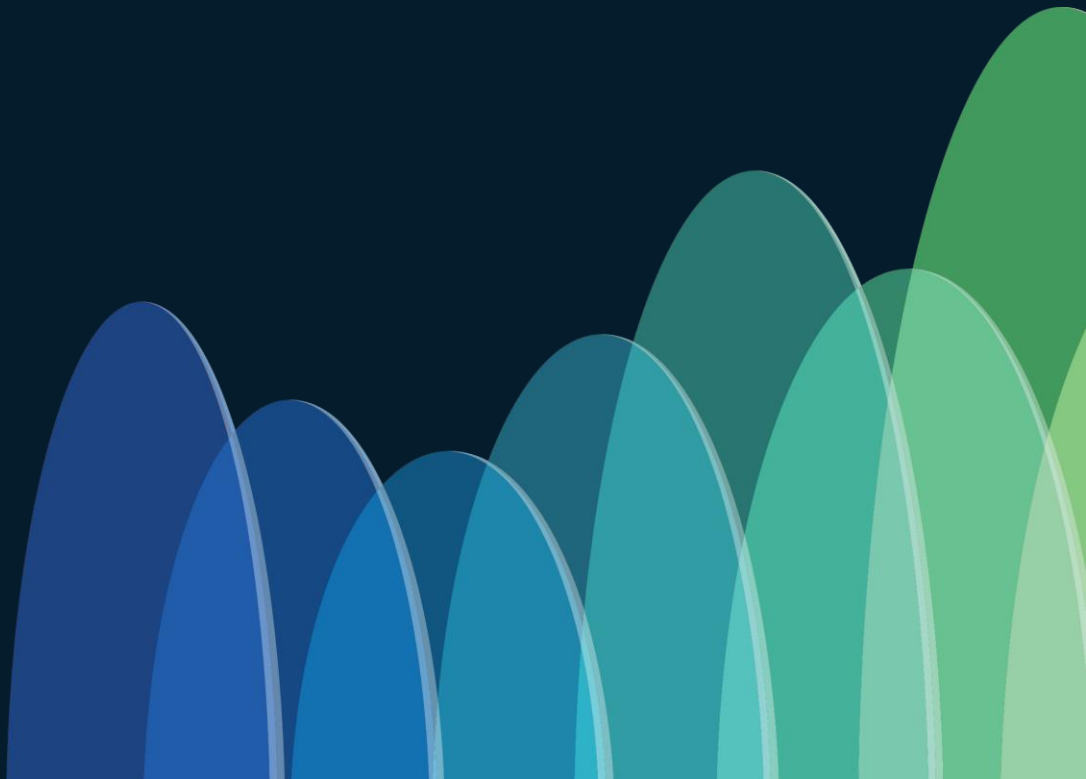
CSC = (rebranded)
AnyConnect 5.x

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

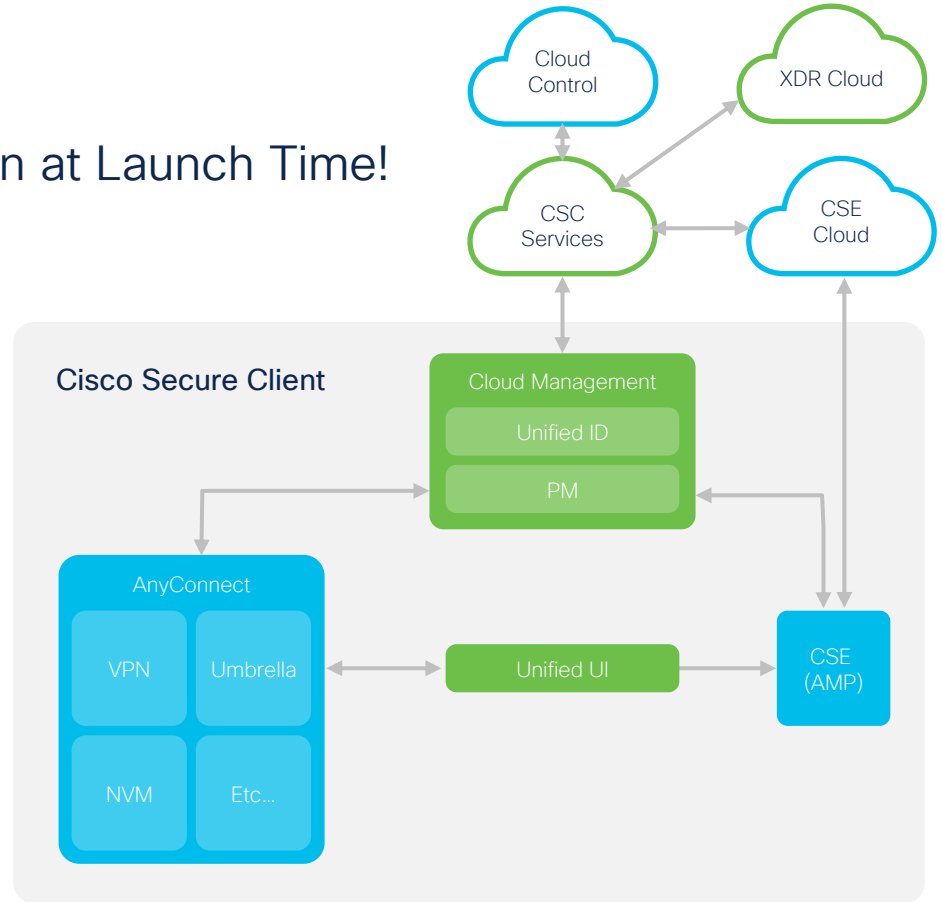
Cisco Secure Client

Architectural Overview – Yes, even at Launch Time!

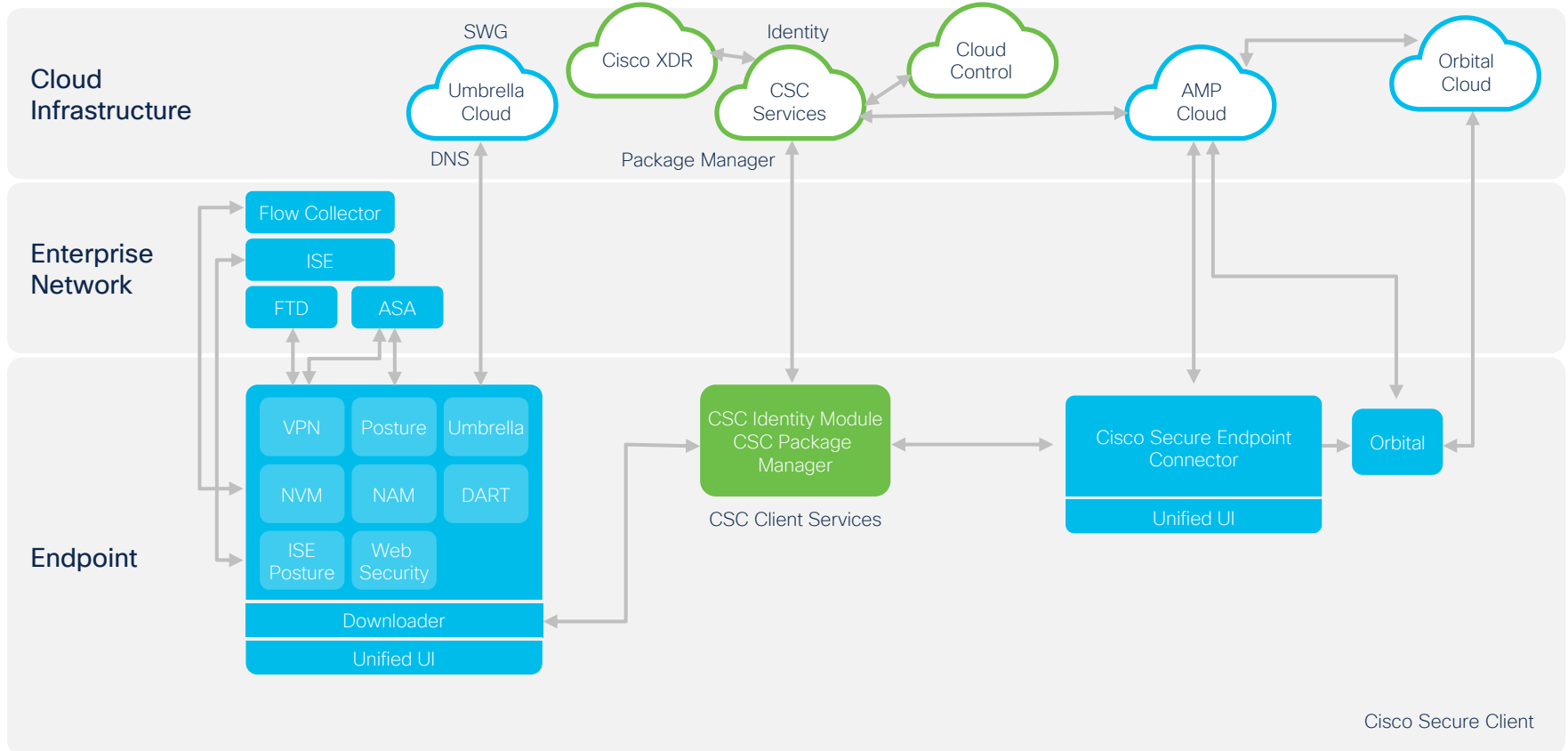
▶ Existing components that are not fundamentally changing

▶ New components

▶ Components that form the Cisco Secure Client



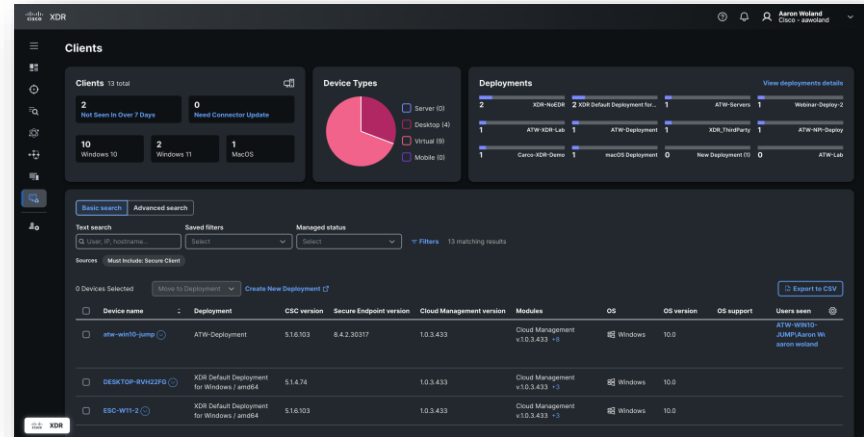
Cisco Secure Client – Architecture



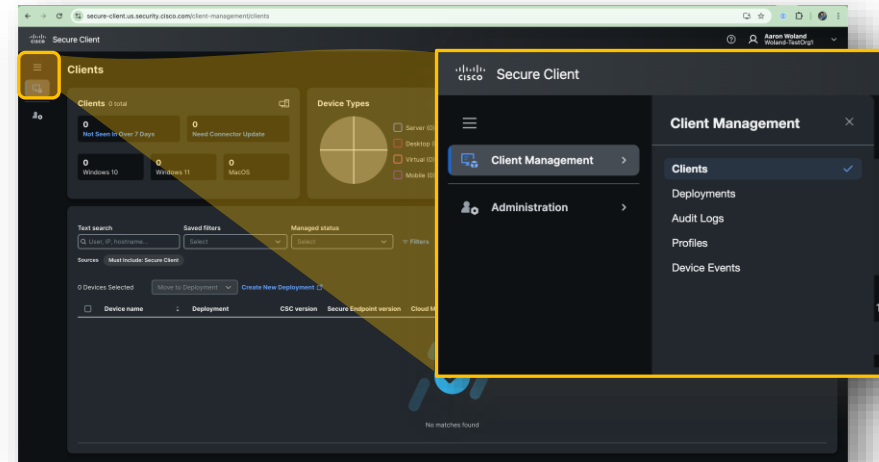
Cisco Secure Client

CSC Management

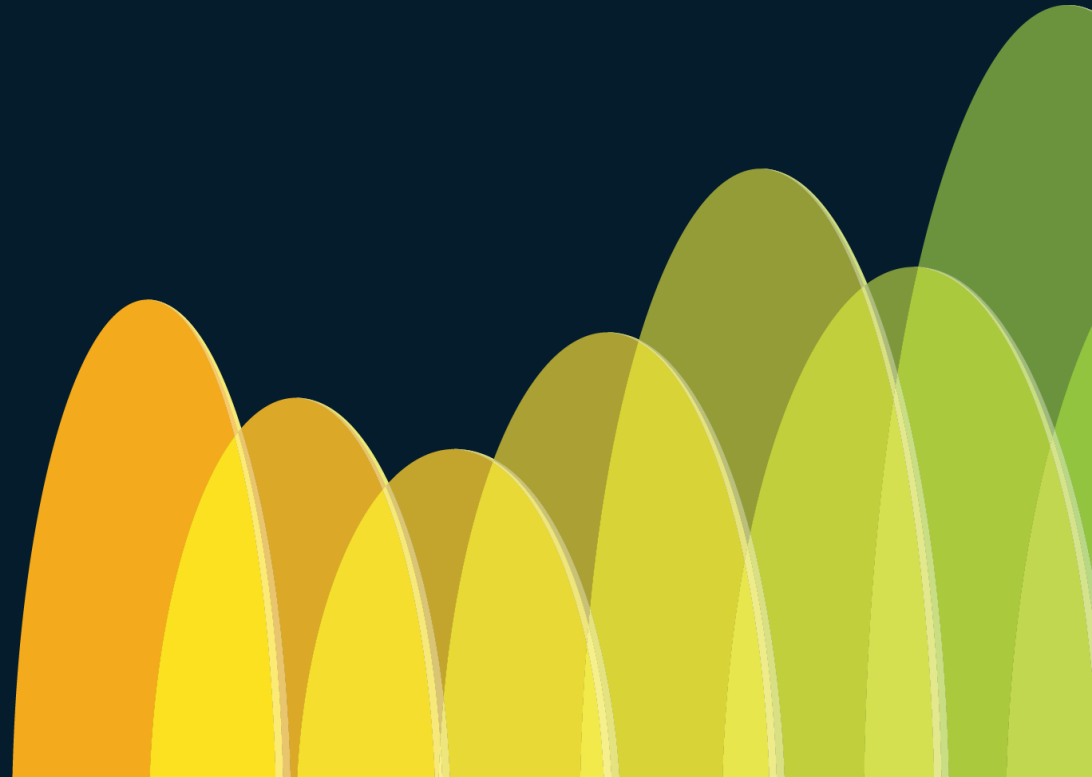
- Still Managed From XDR
 - Provides full Device Insights capabilities
- AND Standalone
 - Secure Client Cloud Management (SCCM)
 - For non-XDR users
 - Only for Secure Client Management, no Device Insights capability
 - Introduced in July 2024 when SecureX was decommissioned



secure-client.us.security.cisco.com



Deploying / Managing from Cloud

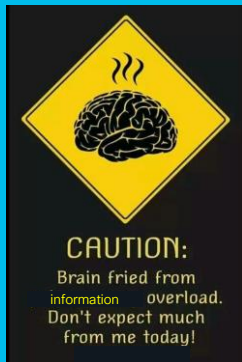


Agenda

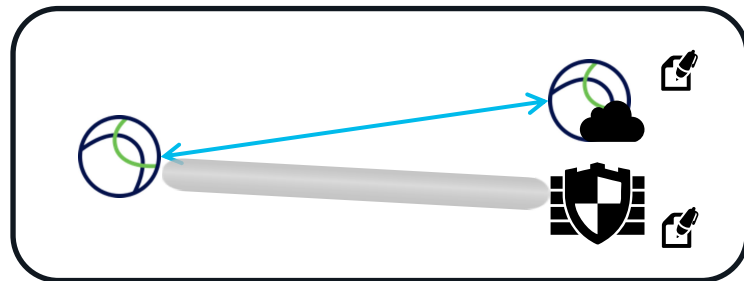
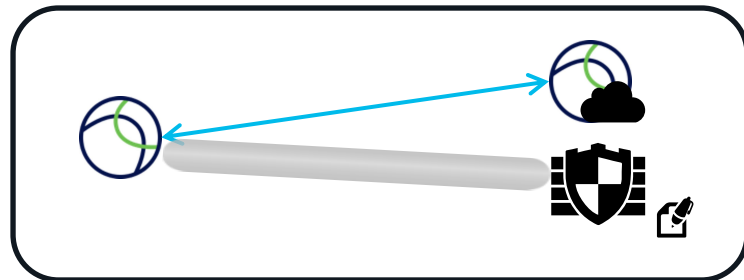
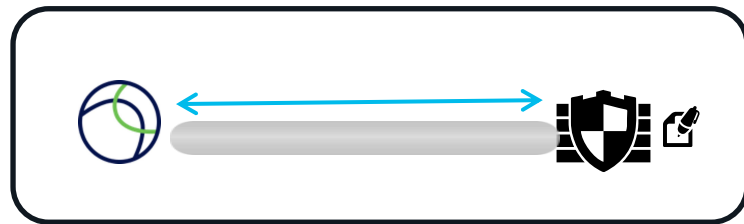
- CSC Overview
- CSC Architecture
- Deploying / Managing from Cloud
- Upgrading to CSC
- FAQs

Deployment Models

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



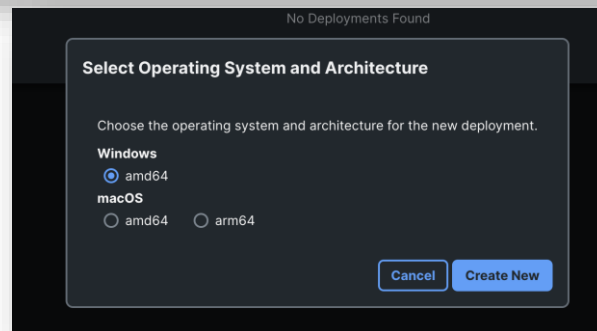
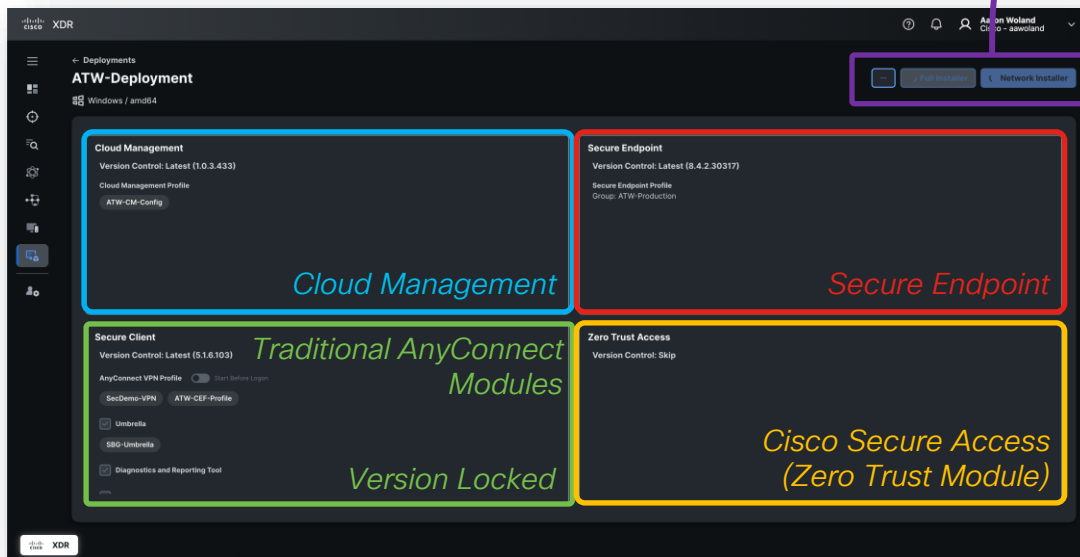
CISCO *Live!*



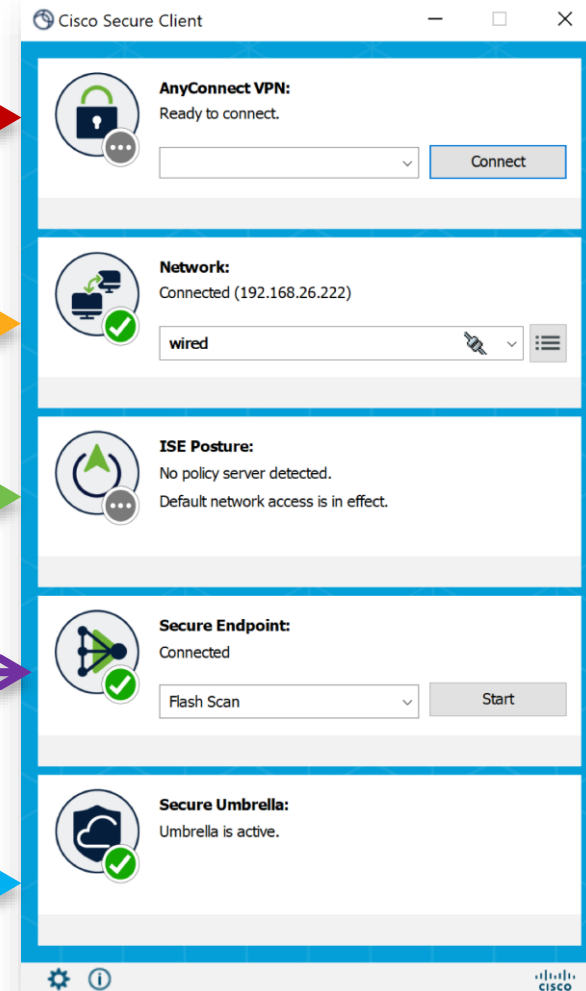
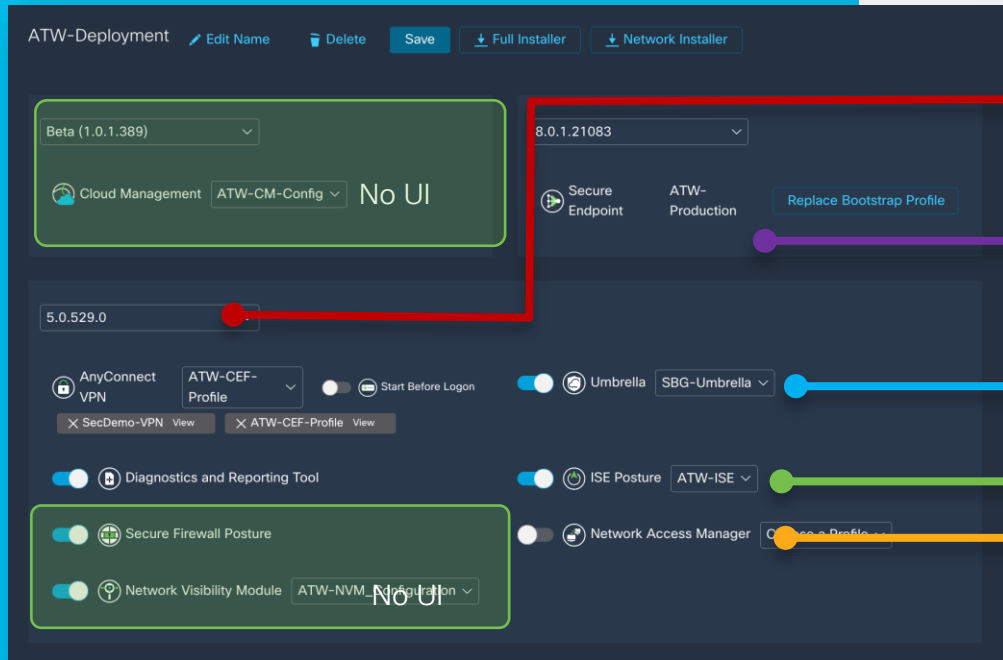
Managed from the Cloud

Deployments

- Links endpoints to get specific modules + configs
- Builds the installer dynamically
- OS Specific
 - Windows AMD64
 - macOS AMD64
 - macOS ARM

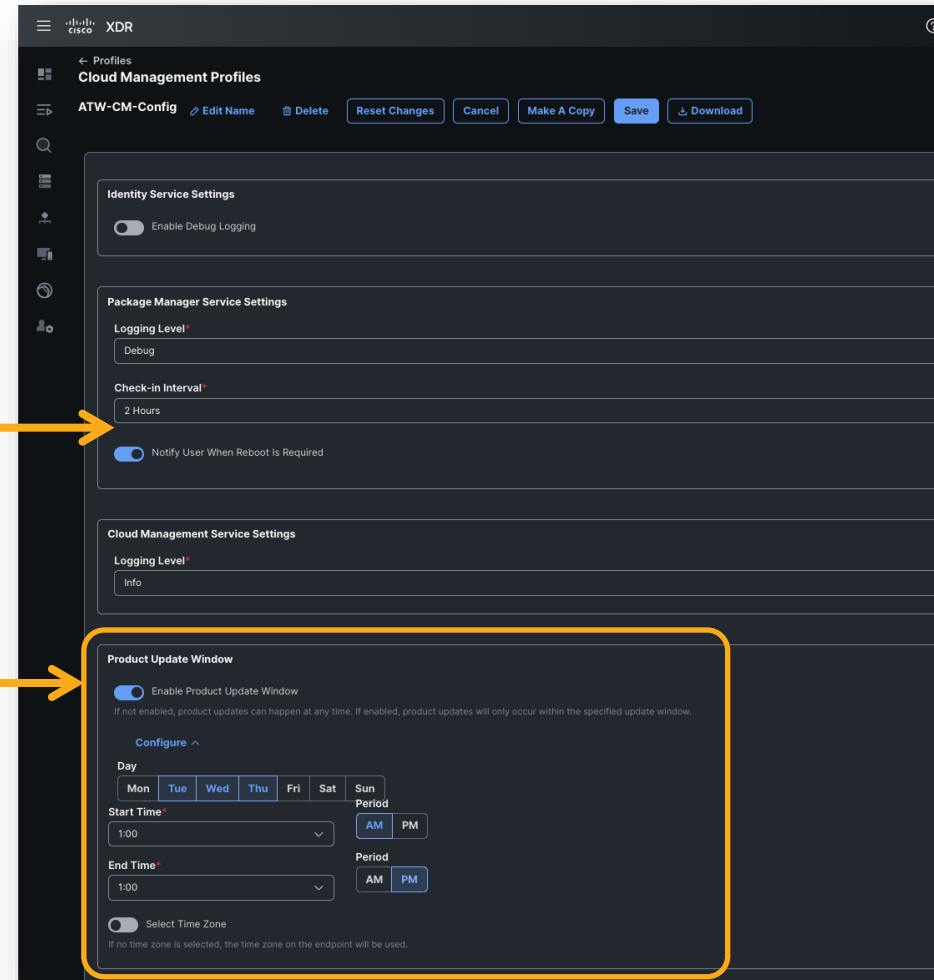


Managed from the Cloud



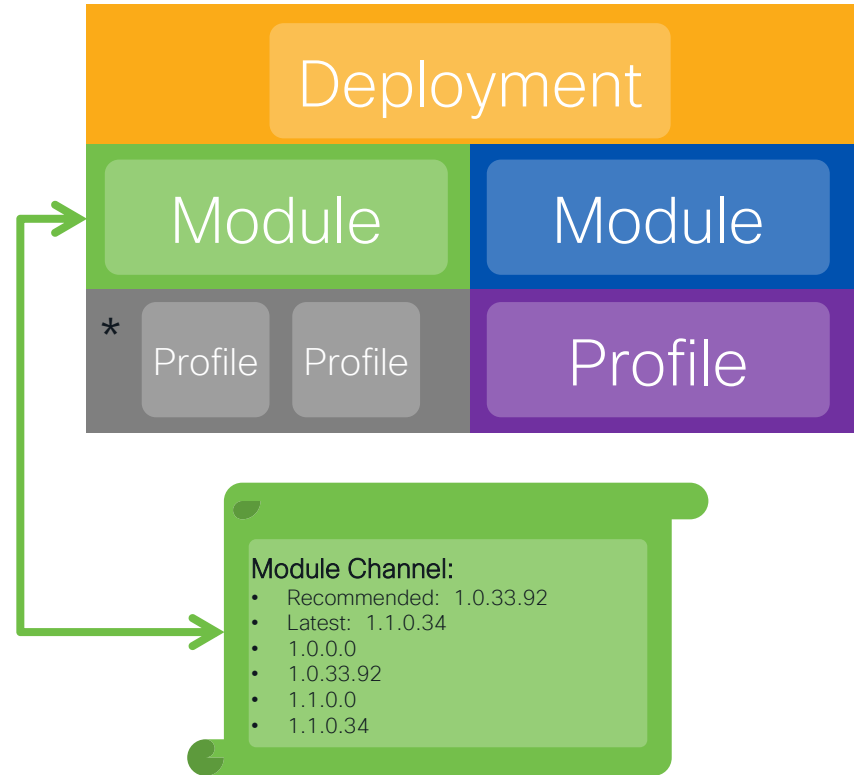
Managed from Cloud

- 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



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

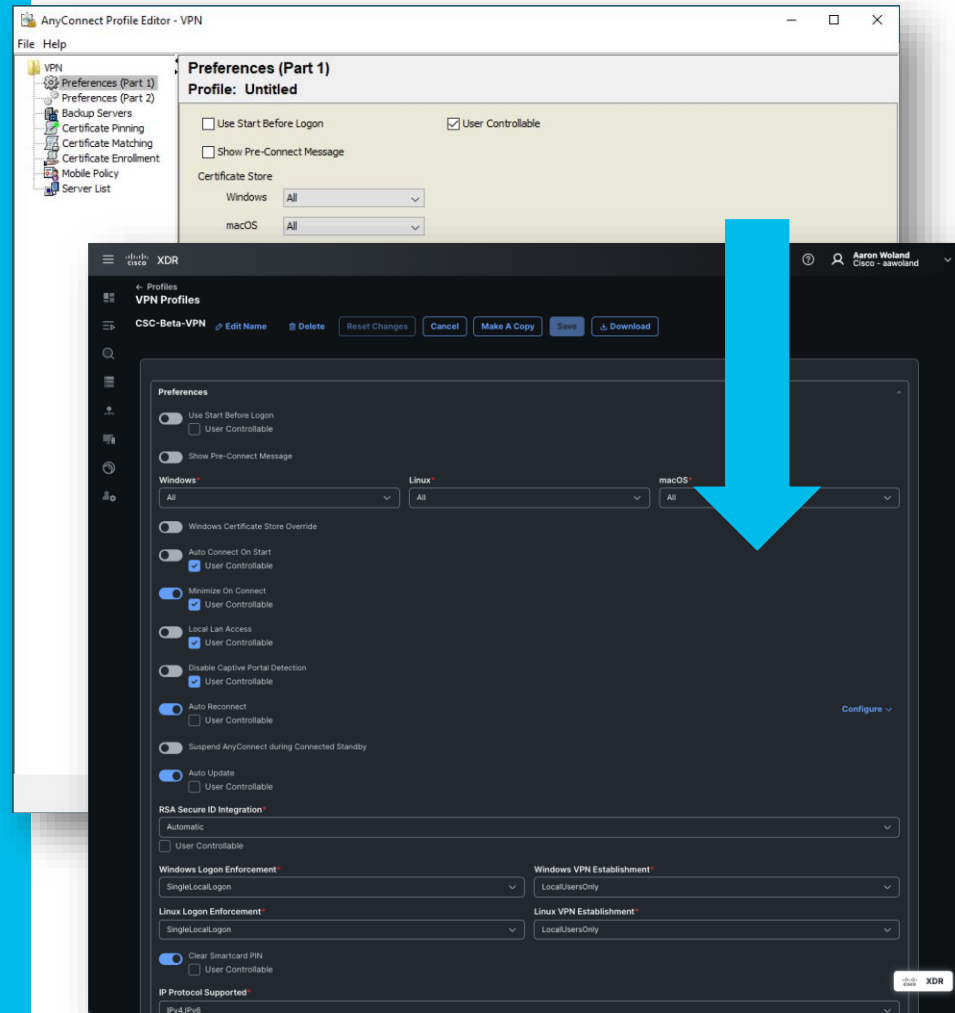


* When module supports >1

Managed from Cloud

- From XDR – everything is there
- Also “Secure Client Cloud Management” (SCCM)
 - No NVM for XDR or Default Deployments
- Profiles
 - Each module has a profile for its “configuration”
 - Used to be standalone Windows-only configuration tool

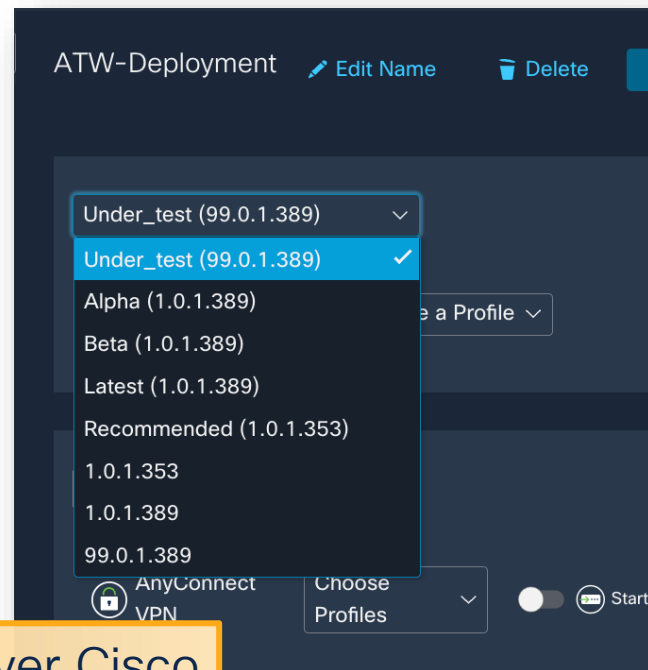
CISCO *Live!*



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

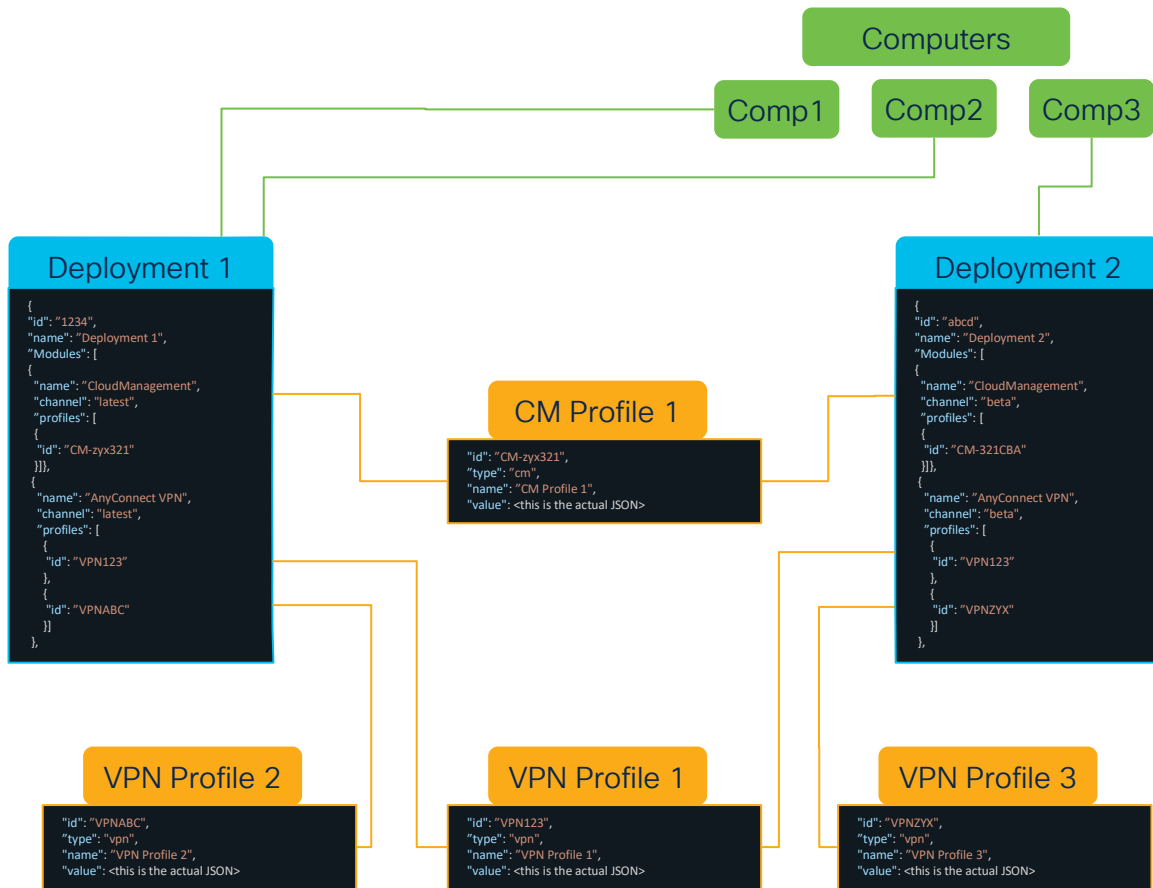


For CM and “AnyConnect” modules
SE module will use latest for bootstrap*

*SE upgrades handled by SE Cloud

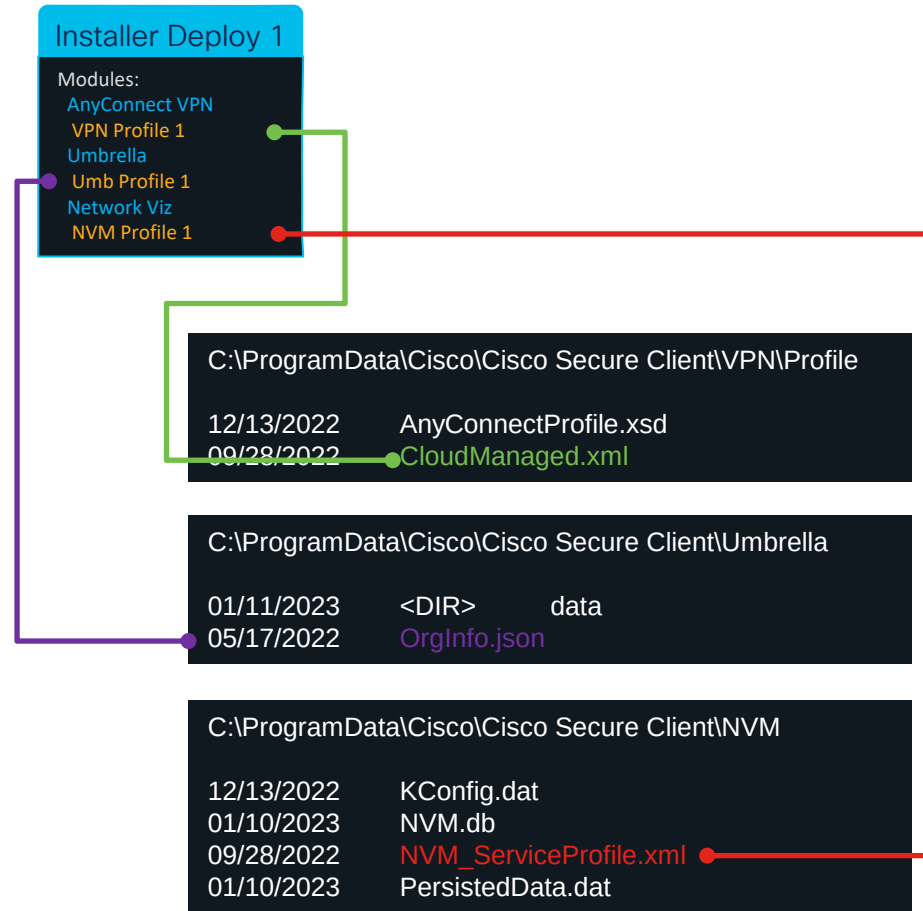
Deployment Hierarchy

- 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)



Client Management

- Client Management is its own section in XDR

- Clients
- Deployments
- Profiles
- Audit Logs
- Device Events

Clients 15 total

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

Device Types

Server (0)
Desktop (4)
Virtual (11)
Mobile (0)

Deployments

3 ATW-Deployment 2 ATW-Lab 1
1 ATW-NPI-Deploy 0 New Deployment (1) 0
0 Server-Deployment 0 Default_XDR_Deployment 0

Select Columns

☐ Select All
☒ Device Name
☒ Deployment
☒ CSC Version
☒ Secure Endpoint Version
☒ Cloud Management Version
☒ Modules
☒ OS
☒ OS Version
☒ OS Support
☒ Users Seen
☒ Sources
☒ Managed
☒ Compromised
☒ Labels
☒ Value
☒ Last Active
☐ CSC UDID
☐ AC UDID
☐ Type
☐ Source Groups/Tags
☐ Has Faults
☐ AV Definitions
☐ Hardware Id
☐ Serial Number
☐ MAC Addresses
☐ Public IPs
☐ Local IPs
☐ System Model
☐ Encrypted
☐ Jail Broken
☐ Supervised
☐ Tampered

Basic Search **Advanced Search**

Text Search: Q User, IP, hostname...
Saved Filters: Select
Managed Status: Select
Filters: 15 matching results

Sources: Must Include: Secure Client

0 Devices Selected Move to Deployment Create New Deployment

Device Name	Deployment	CSC Version	Secure Endpoint Version	Cloud Management Version	Modules	OS	OS Version
ATS-MemberSrvr.securitydemo.net	ATW-Servers	5.11.42	8.2.1.21650	1.0.1.400	Cloud Management v.1.0.1.400 +3	Windows	Server 2016 Standard (Build 14393.6351)
ATW-SurfaceBook	ATW-Deploy+NAM	5.11.42	8.1.7.21585	1.0.1.400	Cloud Management v.1.0.1.400 +7	Windows	10 Pro (Build 19045.3930)
ATW-SURFACEPRO4	ATW-NPI-Deploy	5.1.0.136	8.2.1.21650	1.0.1.400	Cloud Management v.1.0.1.400 +7	Windows	10 Enterprise (64-bit)
atw-win10-airwatch.securitydemo.net	ATW-Lab	5.0.0.0556	8.2.1.21650	1.0.1.400	Cloud Management v.1.0.1.400 +7	Windows	10 Enterprise (Build 19045.3930)
atw-win10-jump.securitydemo.net	ATW-Deployment	5.11.42	8.2.1.21650	1.0.1.400	Cloud Management v.1.0.1.400 +7	Windows	10 Pro N for Workstations (Build 19045.3930)

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

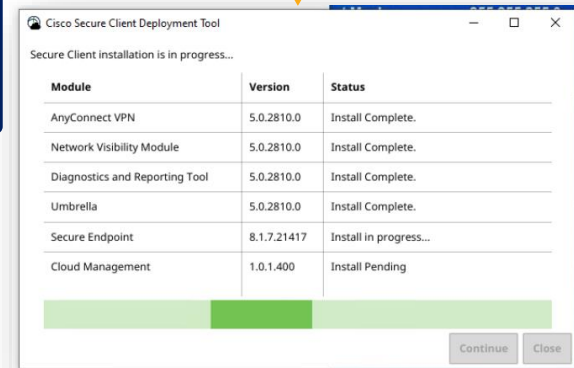
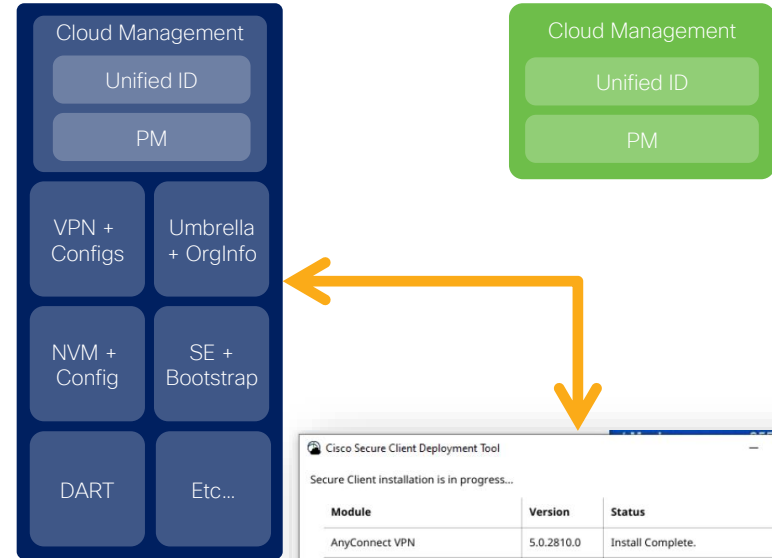
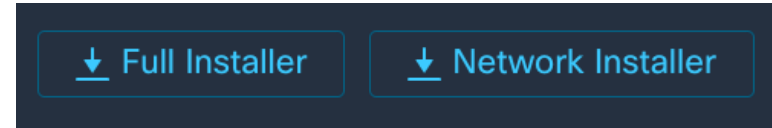
Device Name	Deployment	CSC Version	Secure Endpoint Version	Cloud
ATW-SURFACEPRO4	ATW-Deployment	5.0.00529	8.0.1.21083	1.0

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.

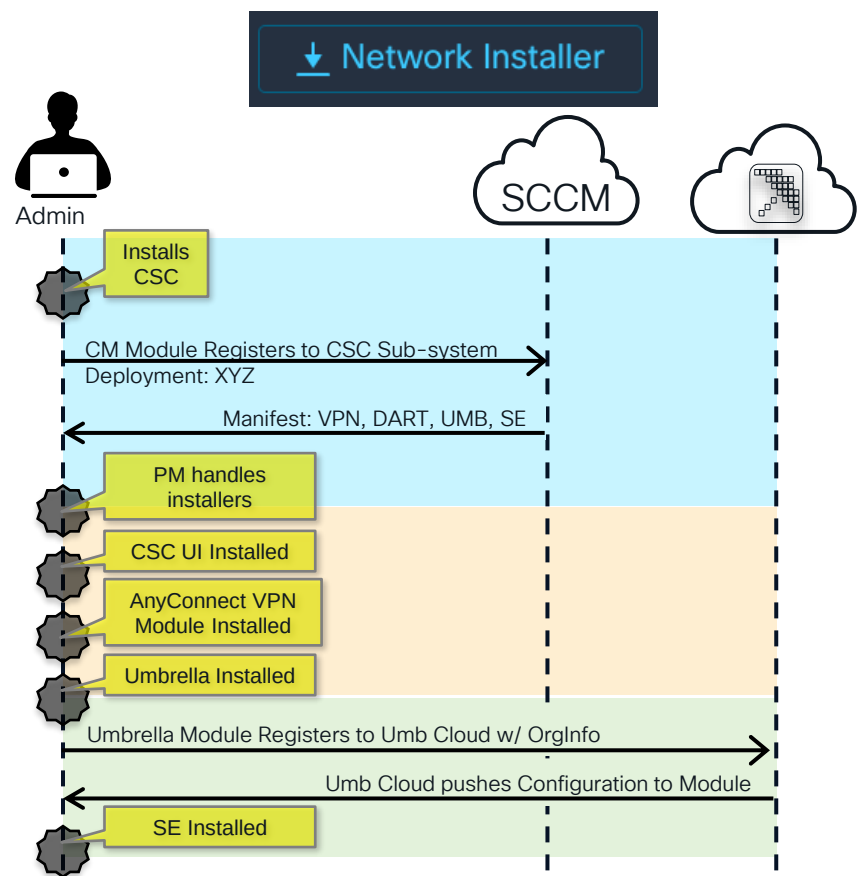


The screenshot shows the 'Cisco Secure Client Deployment Tool' window. The title bar reads 'Cisco Secure Client Deployment Tool'. The main text says 'Secure Client installation is in progress...'. Below this is a table showing the status of various modules. A progress bar at the bottom indicates the installation progress, with a green bar for 'Install Complete' and a dark green bar for 'Install Pending'.

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

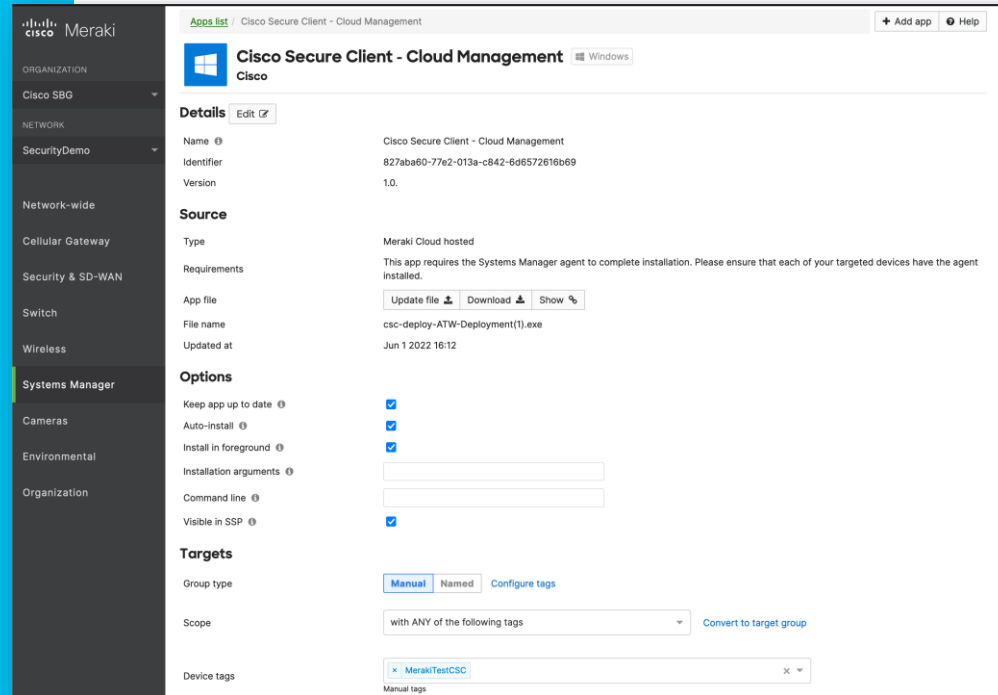
Network Installer

- Lightweight installer
 - Installs the Cloud Management Module with its config only
 - After CM registers to SCCM, 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

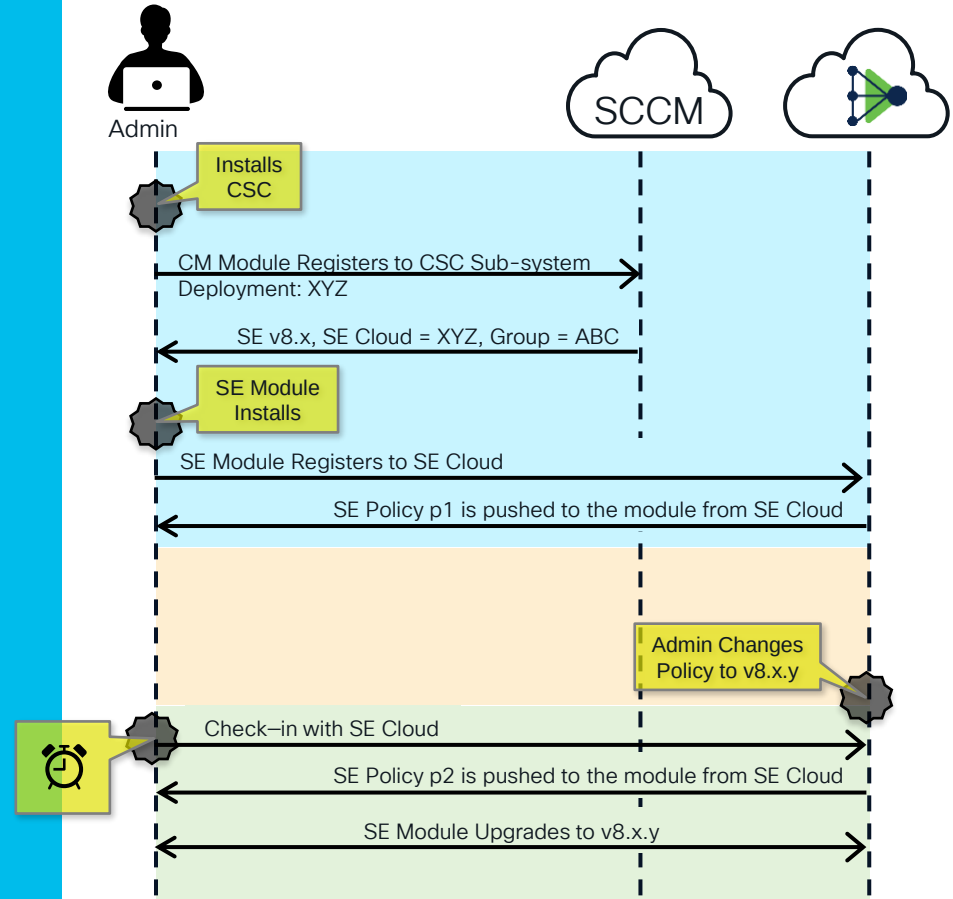
Choose the SE Group

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



SE Version Updates

Highest Version Wins!

ATW-Deployment

Latest (1.0.1.400)

Cloud Management

ATW-CM-Config

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

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

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: 14 days

Block Update if Reboot Required

Product Version: 8.0.1.21164

1 of 30 computers must reboot.

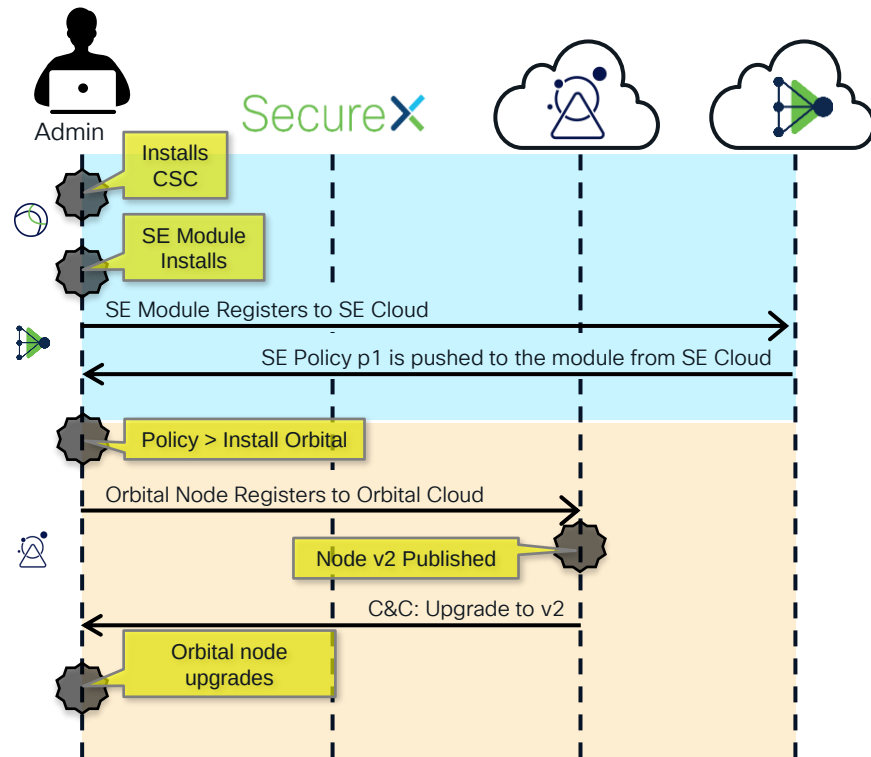
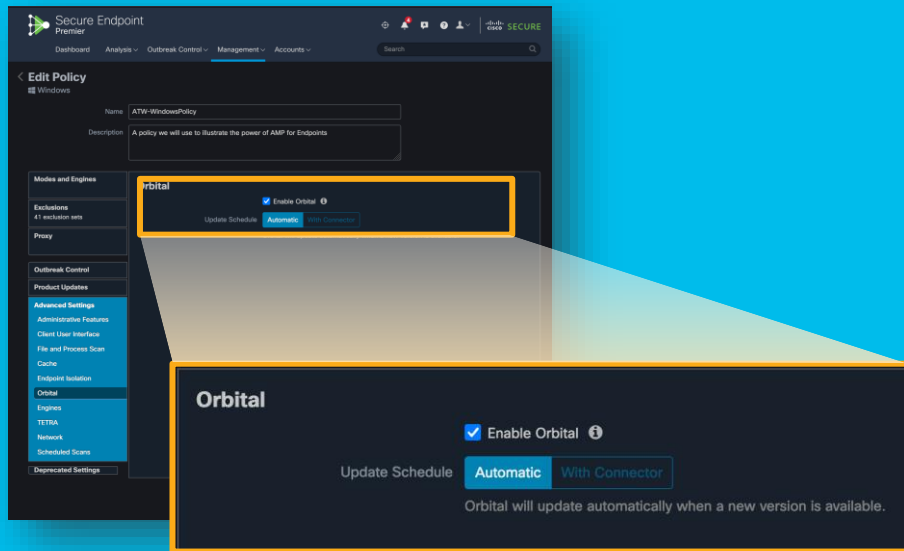
Details

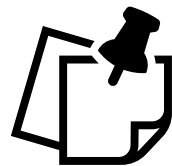
Cancel

Save

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



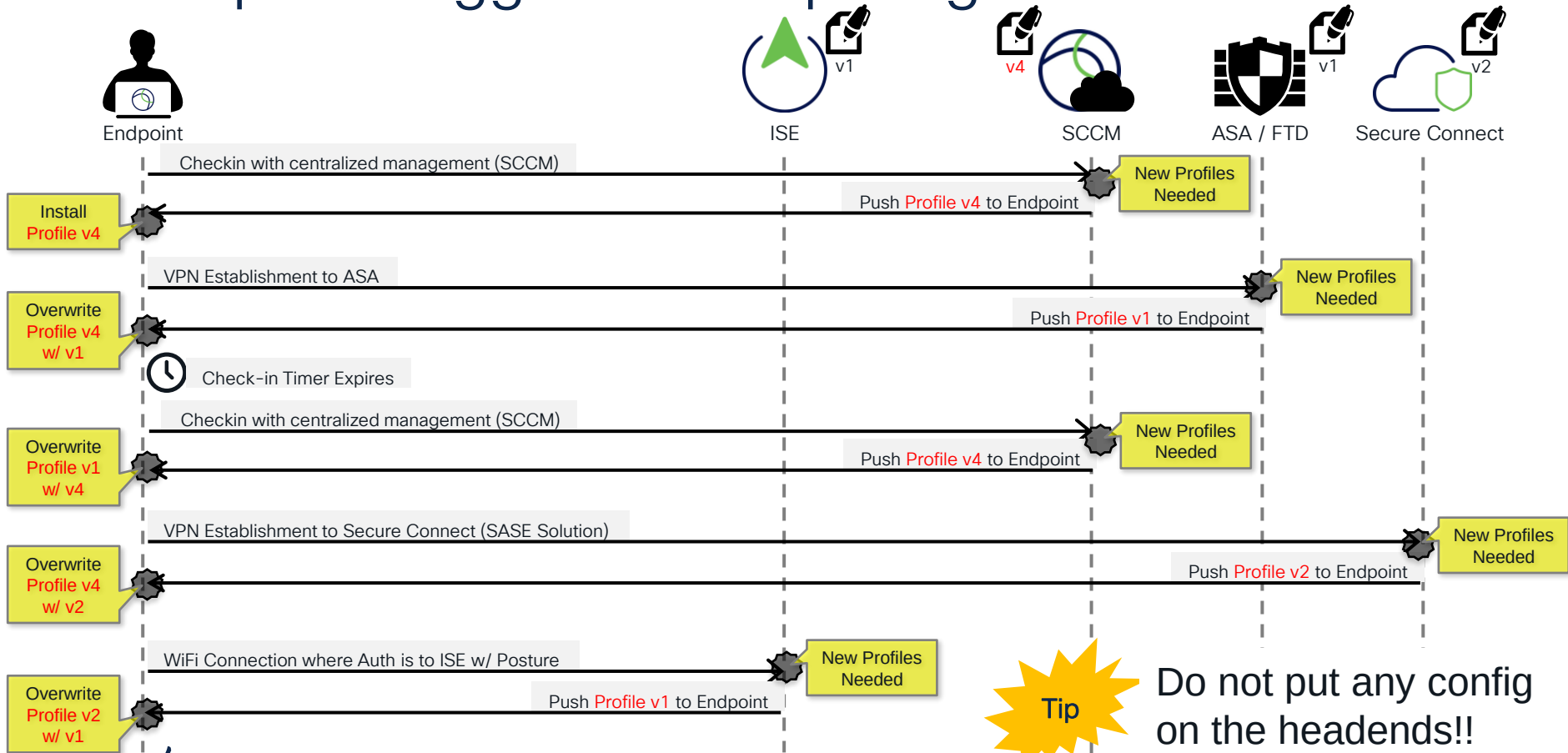
Agenda

- 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

The Epic Struggle of Competing Control Points



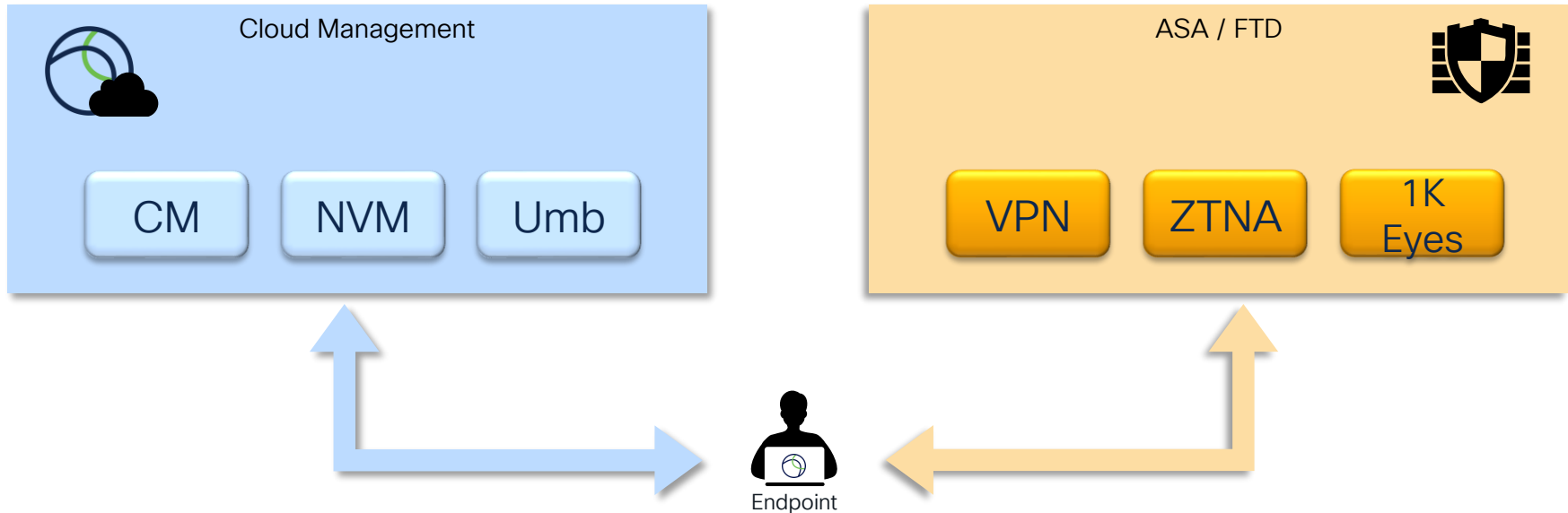
Details on Profile Merges

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

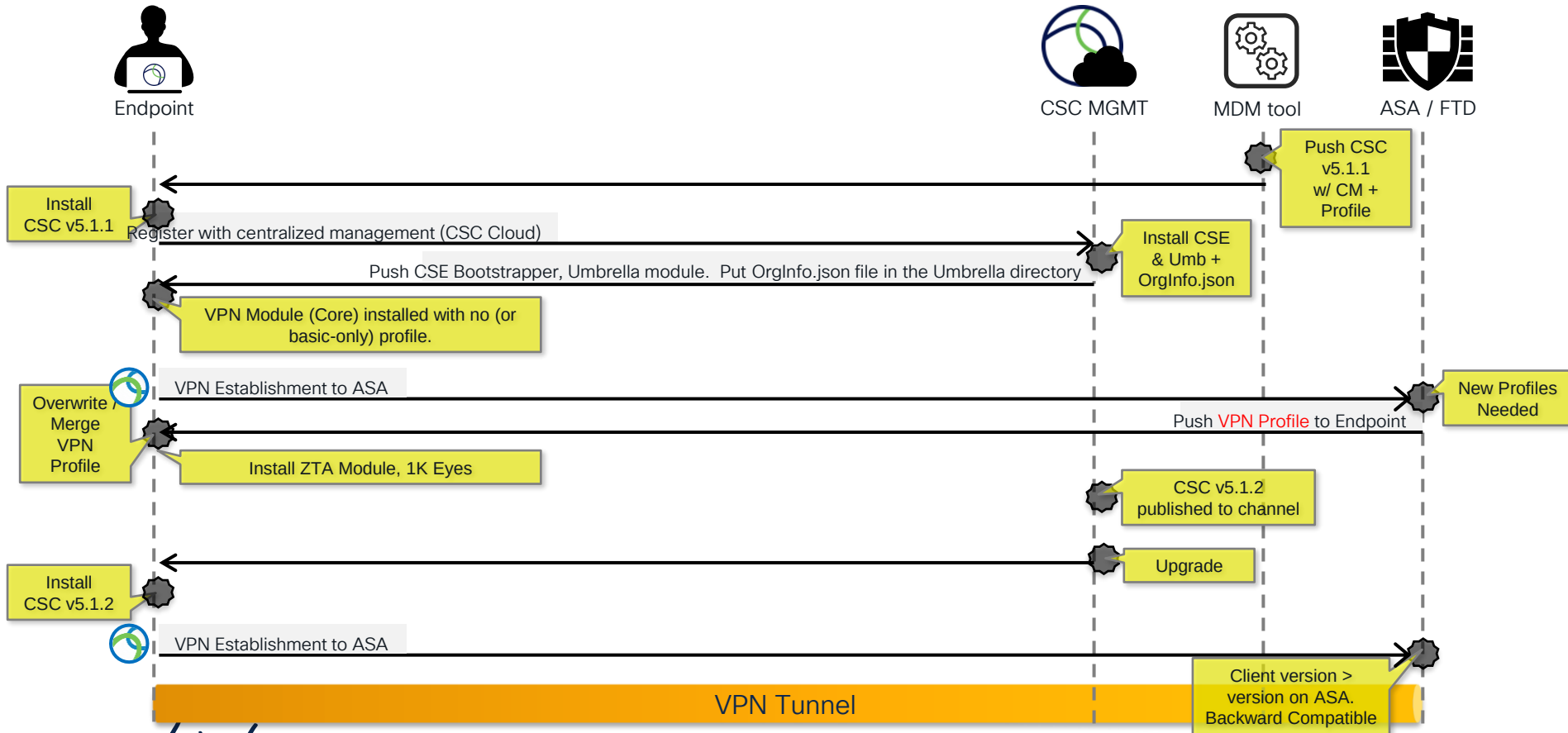
- If filenames match: ASA will overwrite the profile
- If filenames don't match: both profiles will be detected by VPN and behavior might be a little wonky... Some settings get merged from all detected profiles

Hybrid (ASA & Cloud)

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

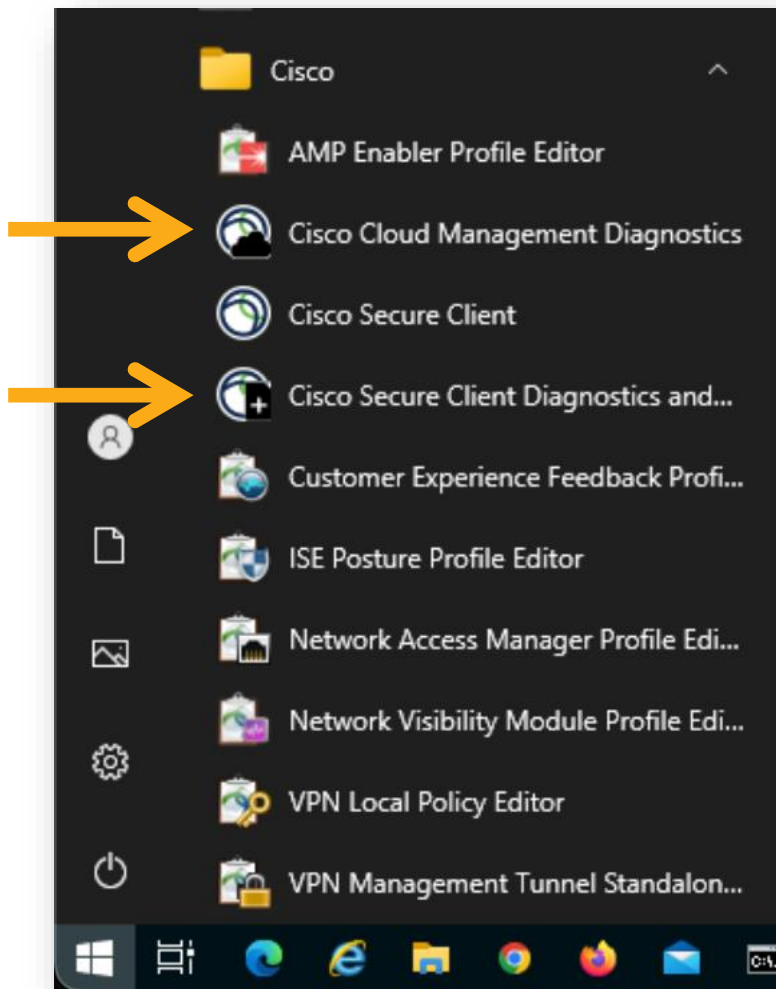


Hybrid (ASA & Cloud)



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?



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@2e0e9eaf-eaf7-4449-9c07-9fb1828aec78
	Updated installations for computer "loxx-win10vic06" (ID 1ce3545e-4ea7-4a9a-b6ea-6cea59de471f).	write	computer	2024-01-19T20:29:49.690792326Z	
	Updated installations for computer "loxx-win10vic07" (ID 8fa133d4-f31f-40ac-9ecc-066da5a8d138).	write	computer	2024-01-19T20:27:24.7592943Z	
	Updated installations for computer "loxx-win10vic02" (ID e6856baf-8771-43fa-b829-4c973b9d29d2).	write	computer	2024-01-19T20:26:46.269256098Z	
	Updated installations for computer "ATW-SurfaceBook" (ID 9ca6e18f-4110-4e7b-9054-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-a6b-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-ea6-4824-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

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 steps highlighted:

- Step 1: Select the Computer**: A search bar labeled "Search For Device" with a dropdown arrow and a search icon. A "Search for Device" button is next to it. The "Device Selected" field shows "09a43288-ebc7-467c-a1ed-ba".
- 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 "Customize", "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": {
      "items": 3
    },
    "old": {
      "items": 3
    }
  },
  "package": "AMD/8.0.1.21083",
  "tsrx": "2022-06-08T16:55:31.050840692",
  "tsrxn": "2022-06-08T16:55:31.05071752",
  "type": "pkg-reconfig"
}
```

The table below shows a list of events:

Customize	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)

cisco *Live!*



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

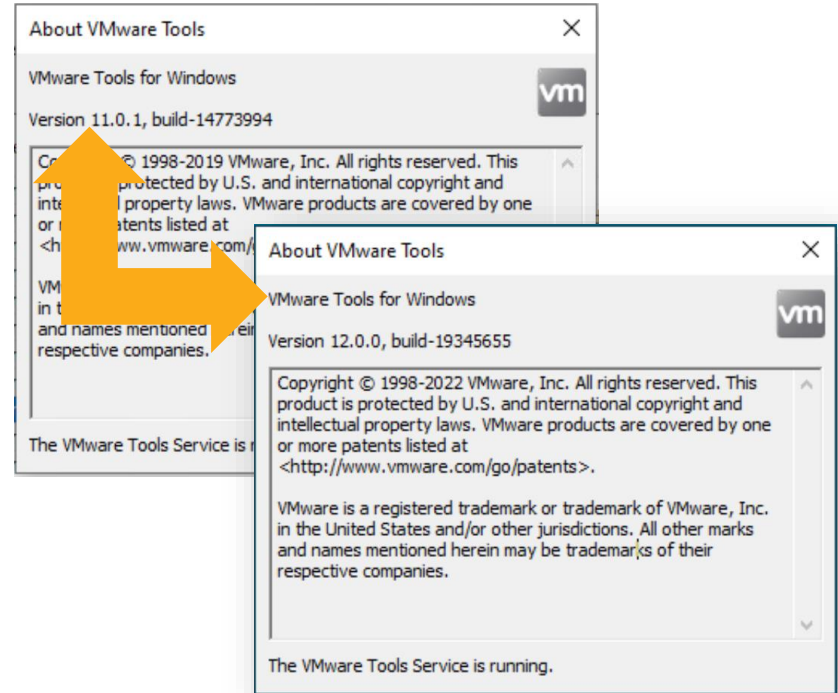
The image is a composite showing the Cisco Software Download page for 'Secure Client 5' (version 5.0.01242). The page lists various download packages for Linux (64-bit), including pre-deployment, VPN, and RPM packages, along with their release dates and sizes. It also includes links to related documentation like the 'Secure Client Ordering Guide' and 'Release Notes for Secure Client 5.0.01242'. In the bottom left, there's a preview of the 'Cisco Secure Client-AnyConnect' app interface. In the bottom right, there's a screenshot of the app as it appears on an iPhone, showing the 'Cisco Secure Client AnyConnect VPN' app with an 'OPEN' button.

Frequently Asked Questions

- Traditional AnyConnect modules are still version locked together
- Duo is not in CSC yet
- macOS in out! AMD64 & ARM
- Linux: no date yet
- Future version of CSC will have module independence
- A profile may only be in up-to 50 deployments
 - TAC case to extend it
- CSC may be used with or without the Cloud Management
- No “web-deploy” package for the Cloud-Management Module

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
```

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

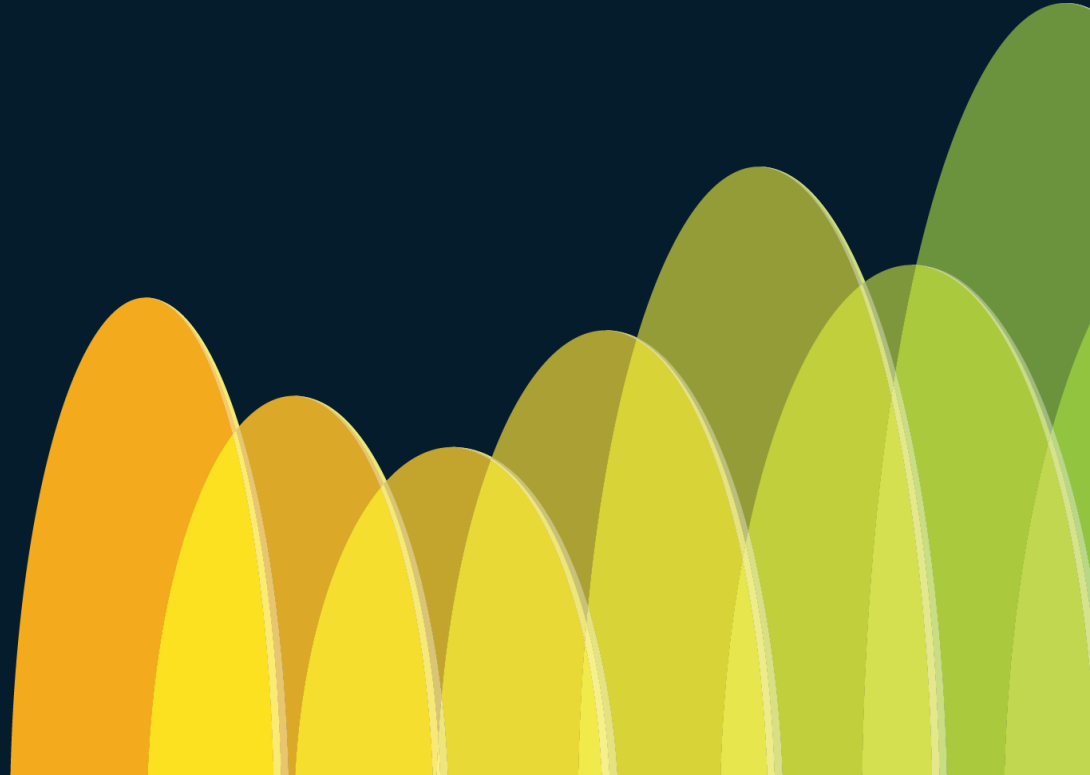
The screenshot shows the 'Product Update Window' configuration page. Three green arrows point to the following elements:

- Enable Product Update Window:** A toggle switch that is currently turned off. Below it, a note states: "If not enabled, product updates can happen at any time. If enabled, product updates will only occur within the specified update window."
- Day:** A row of buttons for days of the week: Mon, Tue, Wed, Thu, Fri, Sat, Sun. 'Mon' is currently selected.
- Start Time:** A dropdown menu showing '1:00' and a 'Period' selector with 'AM' and 'PM' options. 'AM' is selected.
- End Time:** A dropdown menu showing '6:00' and a 'Period' selector with 'AM' and 'PM' options. 'AM' is selected.
- Select Time Zone:** A toggle switch that is currently turned off. Below it, a note states: "If no time zone is selected, the time zone on the endpoint will be used."

There are 'Configure' buttons with up/down arrows in the top right and bottom right corners of the configuration area.

Profiles > Cloud Management > [Profile]

Example Issue: Virtual Machines



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
- NVM Troubleshoot
 - 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:
```

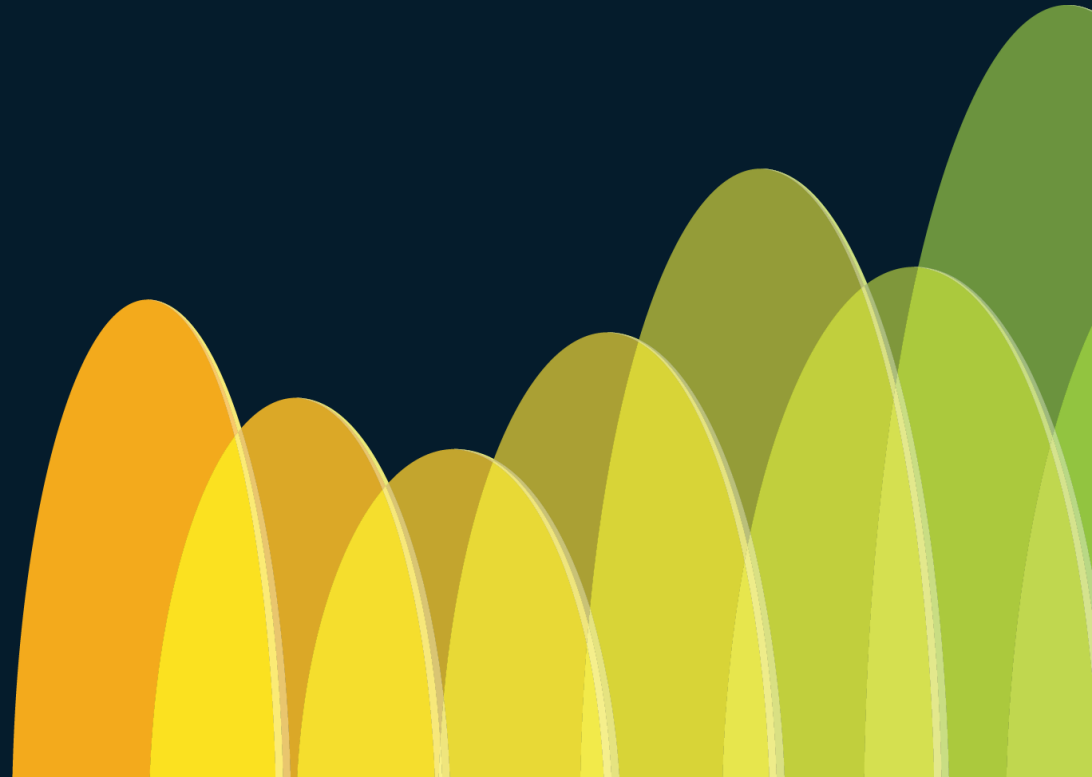
- Result: was using QEMU hypervisor & it didn’t have usable hardware to generate the CMID.

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'/'>
```

Other Troubleshooting Guidance



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 later 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).

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

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 Len=0
631	7.890966	10.1.82.157	44.215.189.243	TCP	60	53958 → 443 [ACK] Seq=1 Ack=1 Win=262 Len=0
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 Len=0
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 Len=0
645	7.965245	10.1.82.157	44.215.189.243	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
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 Len=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
0000000000000000	Cisco Secure Client ID	1d279cb4-20e4-417b-a819-73094c60c272
	Cisco Security Risk Score	56

Investigate in Orbital

Events 17

Q Scan... Diagnose... Move to Group... **Uninstall Connector** Delete

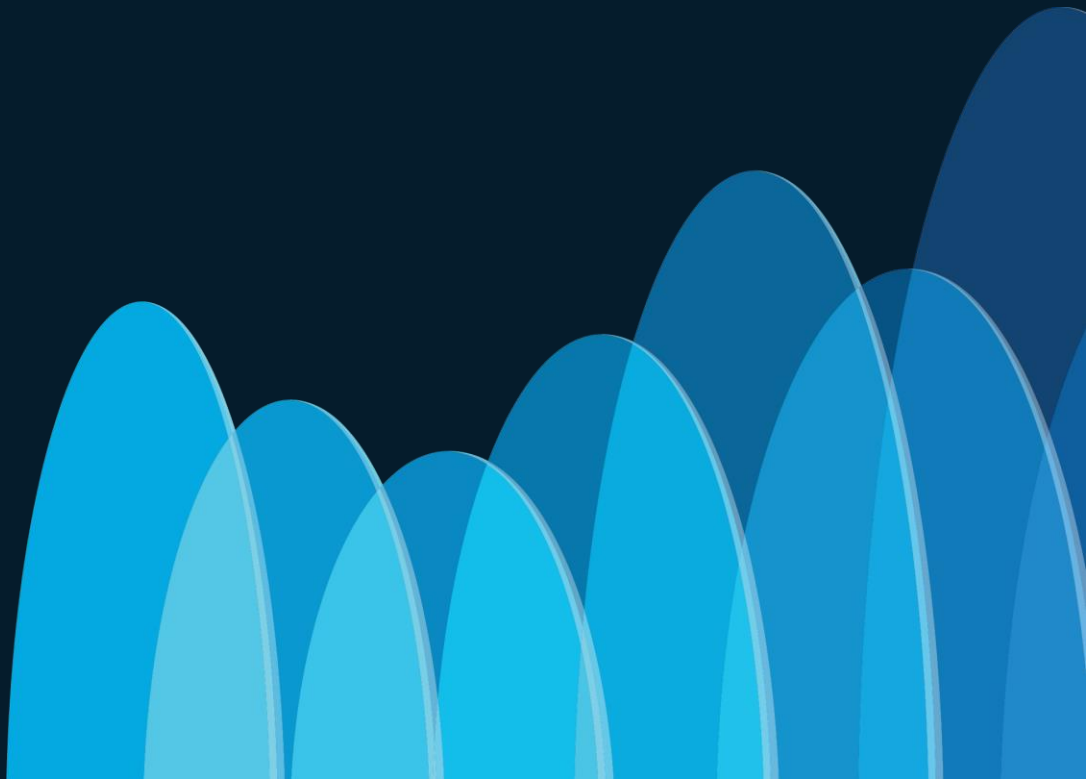
25 / page

1 of 1

Export to CSV

Cisco Secure Client does not support remote uninstall.

Continue your
education



Please fill out the survey



Drop your email in the comments – I WILL respond!

Keynote Deep Dives

Wednesday
10:30am – 11:30am



Experiences Amplified:
How AI Can Fuel Better Employee and Customer Experiences

Level 1
Room 106



Smart, Secure, Seamless:
Transforming Experiences with Next-Generation Networking

Level 2
Room 204



Harness a Bold New Era:
Transform Data Centre and Service Provider Connectivity

Level 2
Room 203



Securing User to Application and Everything in Between

Level 2
Melbourne Room 2



Unlocking Digital Resilience through Unified Observability

The HUB
Centre Stage

Complete Your Session Evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to claim a **Cisco Live T-Shirt**.



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



Continue your education



- Visit the Cisco Stand for related demos
- Book your one-on-one Meet the Expert meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand



Thank you

CISCO *Live!*

#CiscoLiveAPJC

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC