Let’s go

The bridge to possible

Cisco Secure Client

Technical Deep Dive

Aaron T Woland, CCIE #20113
Distinguished Engineer, Threat Detection & Response
loxx@cisco.com | 𝕏 @aaronwoland | in aaronwoland

$ 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 2 years old!

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

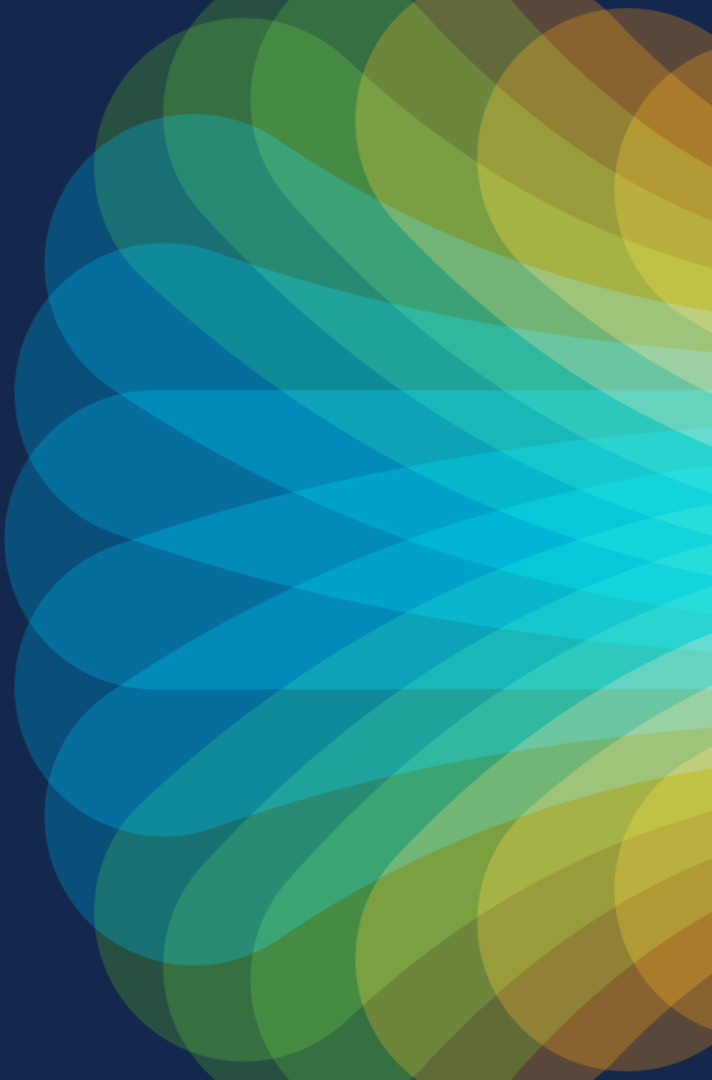
There is a tremendous amount of hidden content, for you to use later!

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

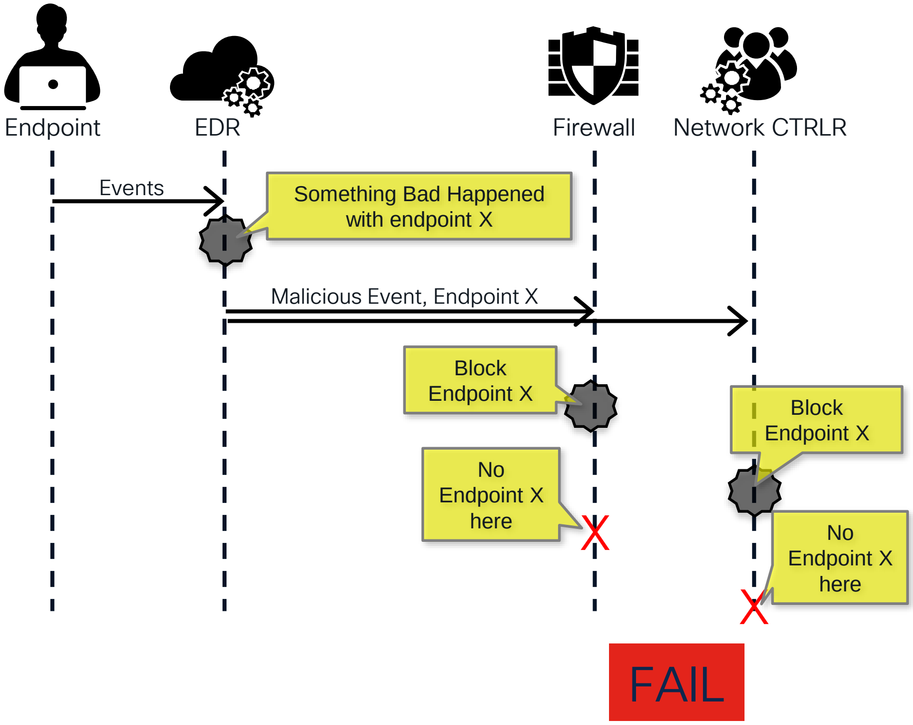
- CSC Overview
- CSC Architecture
- Deploying / Managing from Cloud
- Upgrading to CSC
- FAQs

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

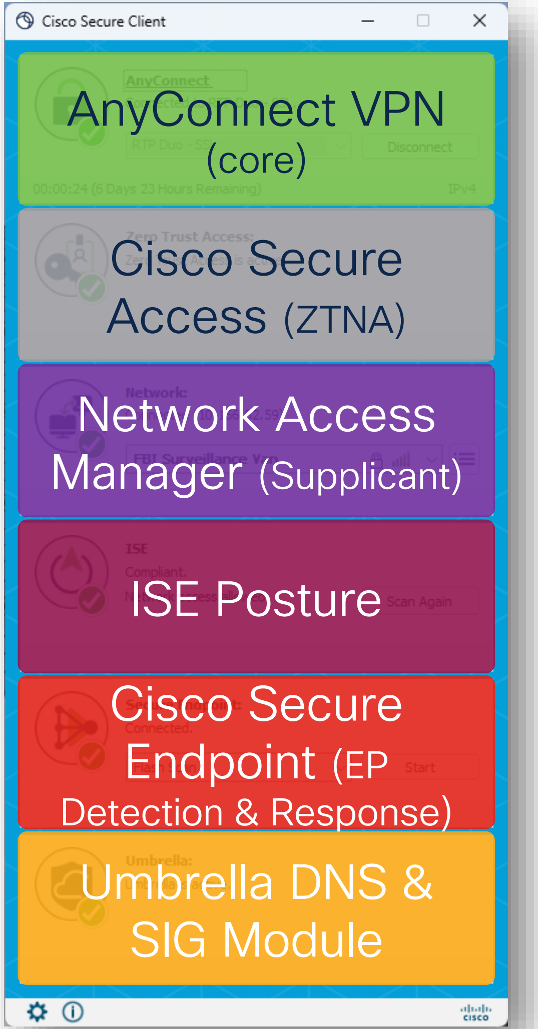
Some basics

- Initial “unified agent” release was 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
- Introduced a new Cloud Management System inside SecureX & 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)



AnyConnect VPN (core)

Cisco Secure Access (ZTNA)

Network Access Manager (Supplicant)

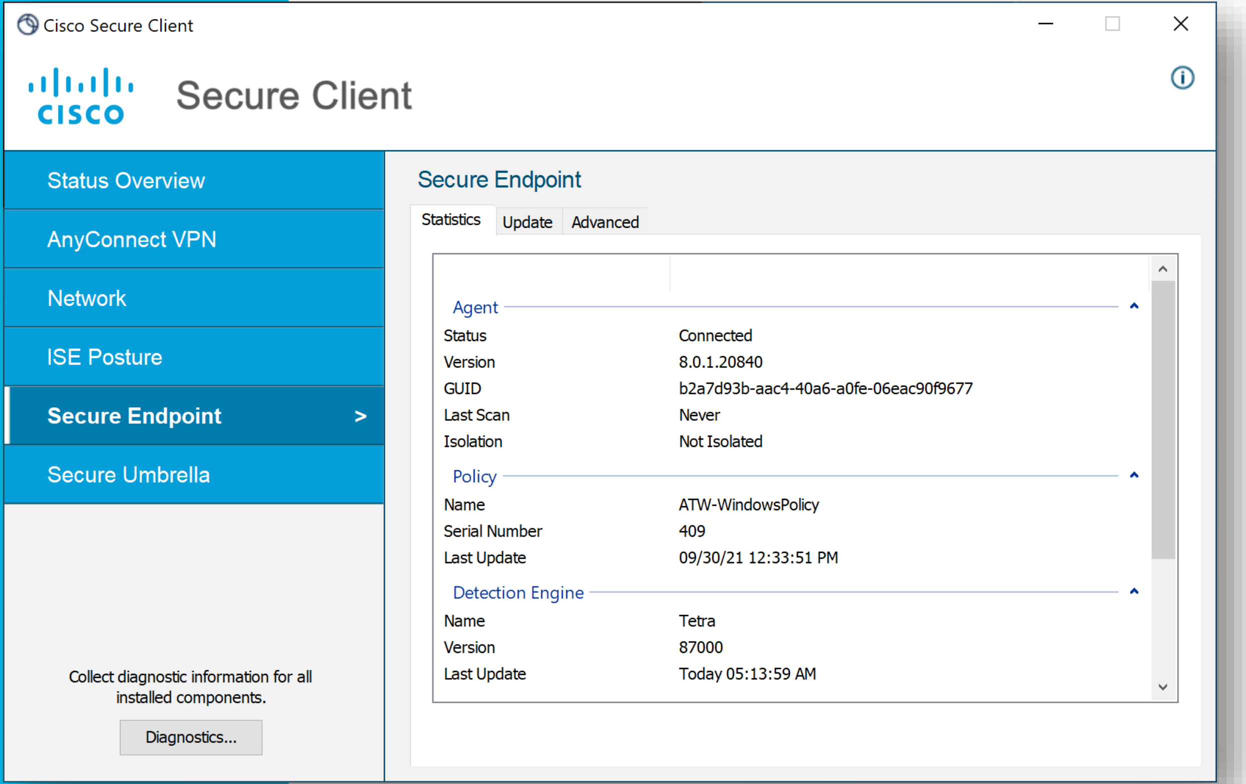
ISE Posture

Cisco Secure Endpoint (EP Detection & Response)

Umbrella DNS & SIG Module

Secure Endpoint Statistics

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



Secure Endpoint

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

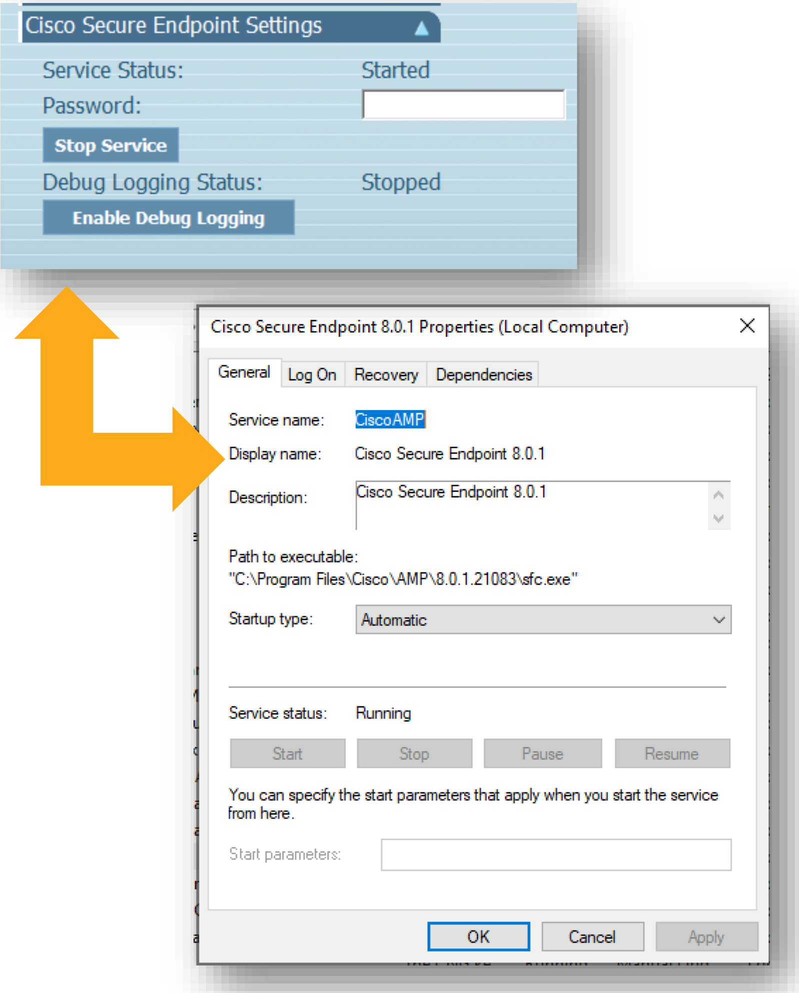
Detection Engine

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

Collect diagnostic information for all installed components.

More Secure Endpoint UI

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



Cisco Secure Endpoint Settings

Service Status: Started

Password:

Stop Service

Debug Logging Status: Stopped

Enable Debug Logging

Cisco Secure Endpoint 8.0.1 Properties (Local Computer)

Service name: CiscoAMP

Display name: Cisco Secure Endpoint 8.0.1

Description: Cisco Secure Endpoint 8.0.1

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

Startup type: Automatic

Service status: Running

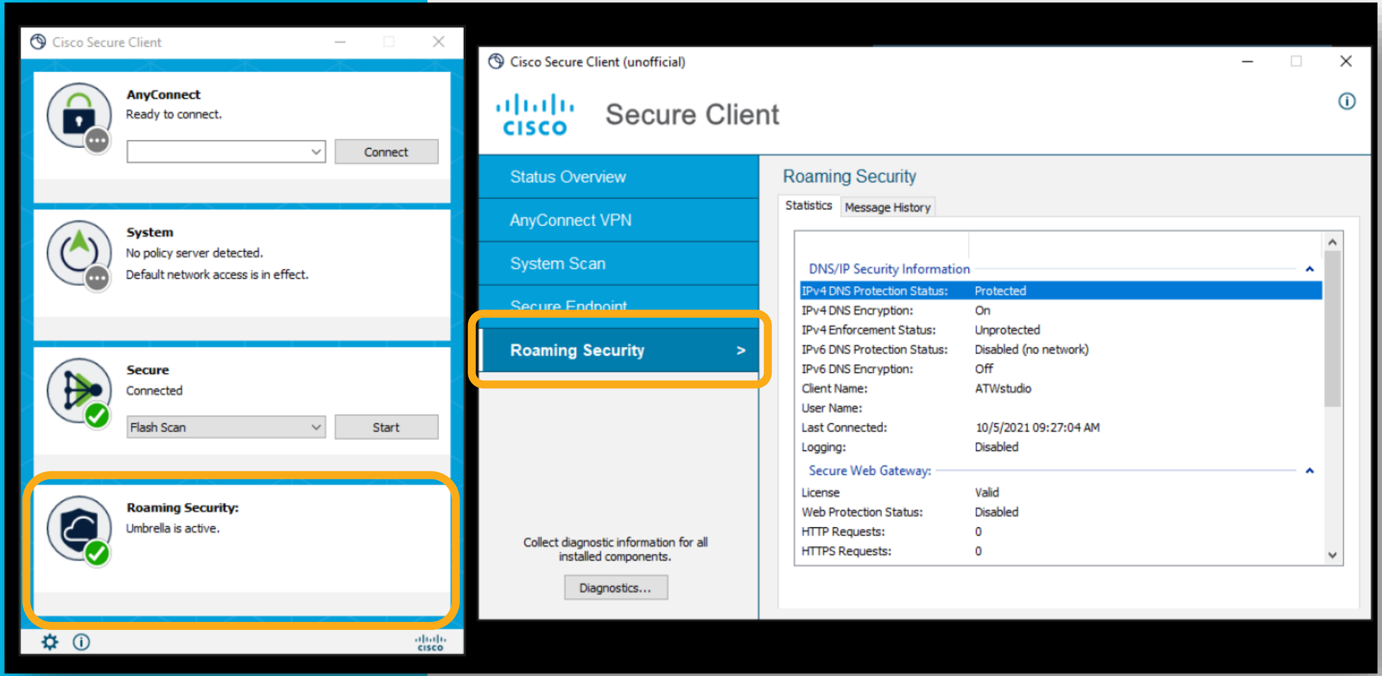
You can specify the start parameters that apply when you start the service from here.

Start parameters:

Umbrella

Same Umbrella Roaming from AnyConnect:

- Umbrella DNS
- Secure Web Gateway



Cisco Secure Client

AnyConnect
Ready to connect.

System
No policy server detected.
Default network access is in effect.

Secure
Connected
Flash Scan

Roaming Security:
Umbrella is active.

Cisco Secure Client (unofficial)

Secure Client

Roaming Security

DNS/IP Security Information

IPv4 DNS Protection Status: Protected
IPv4 DNS Encryption: On
IPv4 Enforcement Status: Unprotected
IPv6 DNS Protection Status: Disabled (no network)
IPv6 DNS Encryption: Off
Client Name: ATWstudio
User Name:
Last Connected: 10/5/2021 09:27:04 AM
Logging: Disabled

Secure Web Gateway:

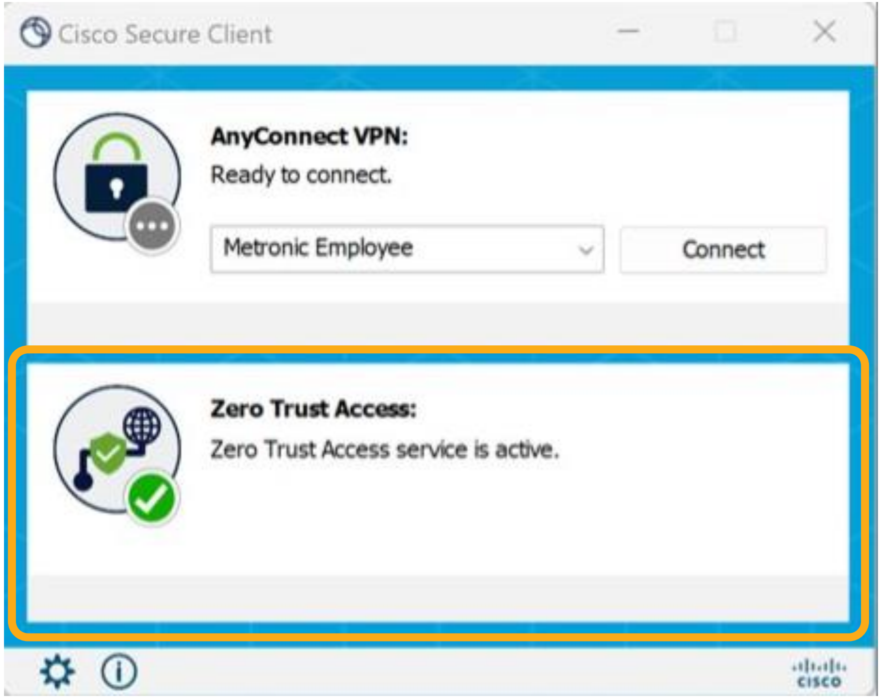
License Valid
Web Protection Status: Disabled
HTTP Requests: 0
HTTPS Requests: 0

Collect diagnostic information for all installed components.

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



Cisco Secure Client

AnyConnect VPN:

Ready to connect.

Metronic Employee

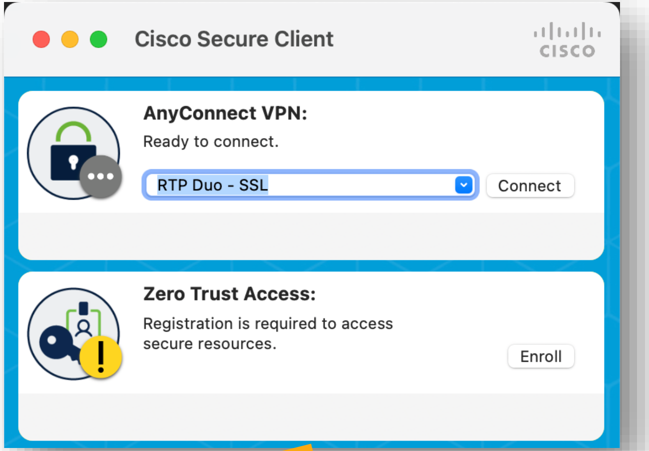
Zero Trust Access:

Zero Trust Access service is active.

ZTNA Module

For Cisco “Secure Access”

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

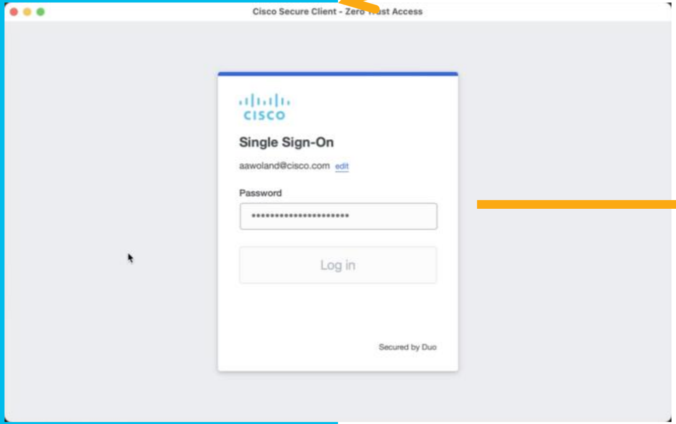


Cisco Secure Client

AnyConnect VPN:
Ready to connect.

RTP Duo - SSL

Zero Trust Access:
Registration is required to access secure resources.

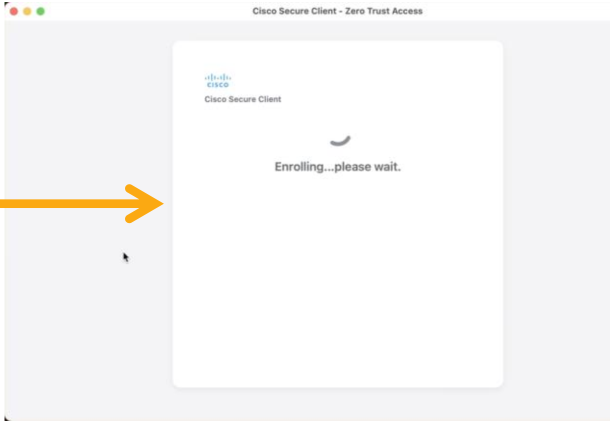


Cisco Secure Client - Zero Trust Access

Single Sign-On

aawoland@cisco.com edit

Password: ••••••••••••••••••••



Cisco Secure Client - Zero Trust Access

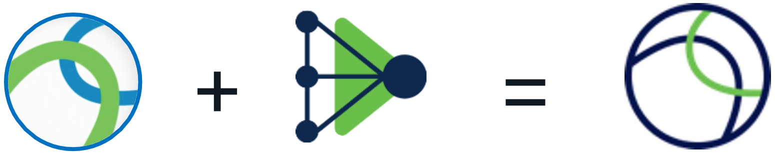
Cisco Secure Client

Enrolling...please wait.

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

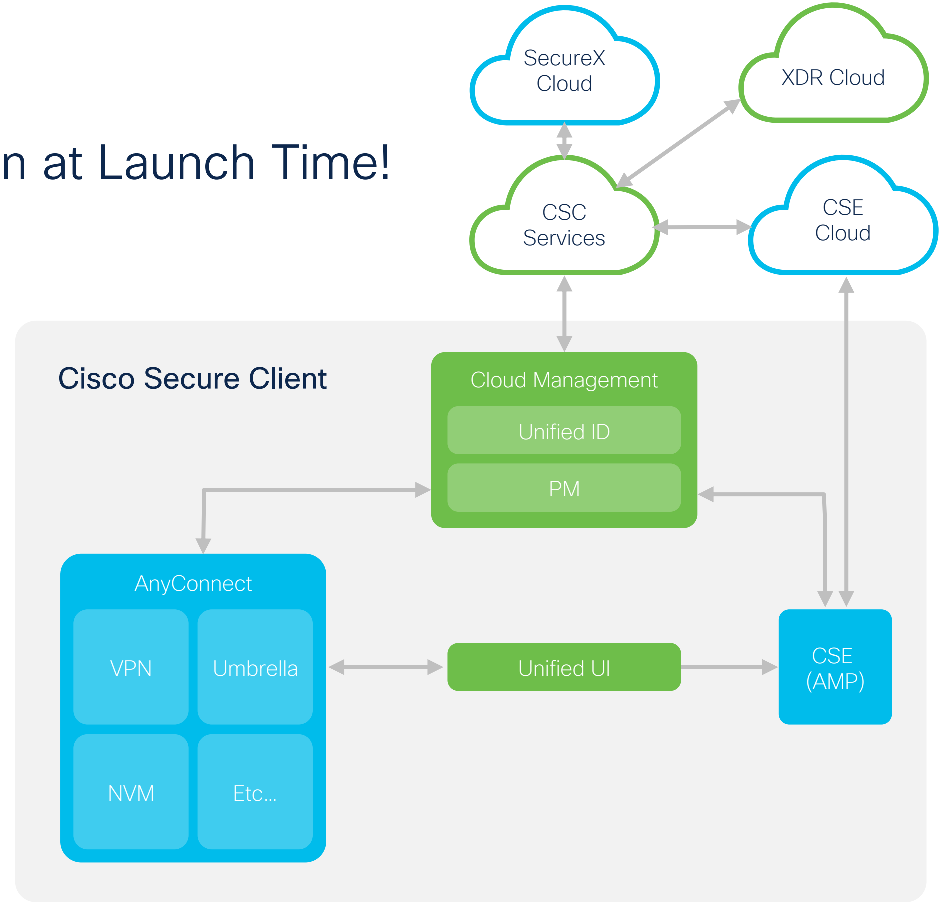
Agenda

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

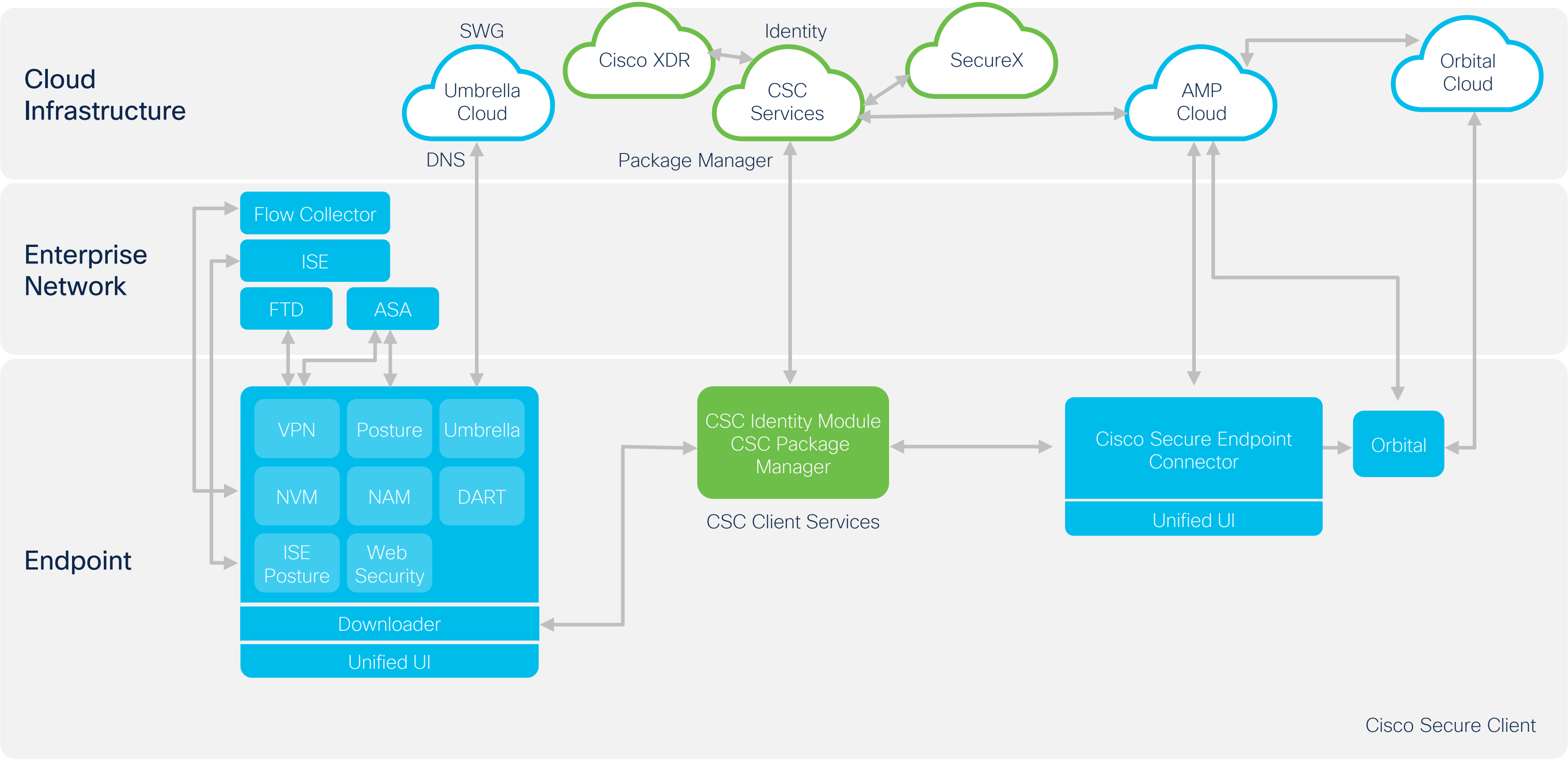
Cisco Secure Client

Architectural Overview – Yes, even at Launch Time!

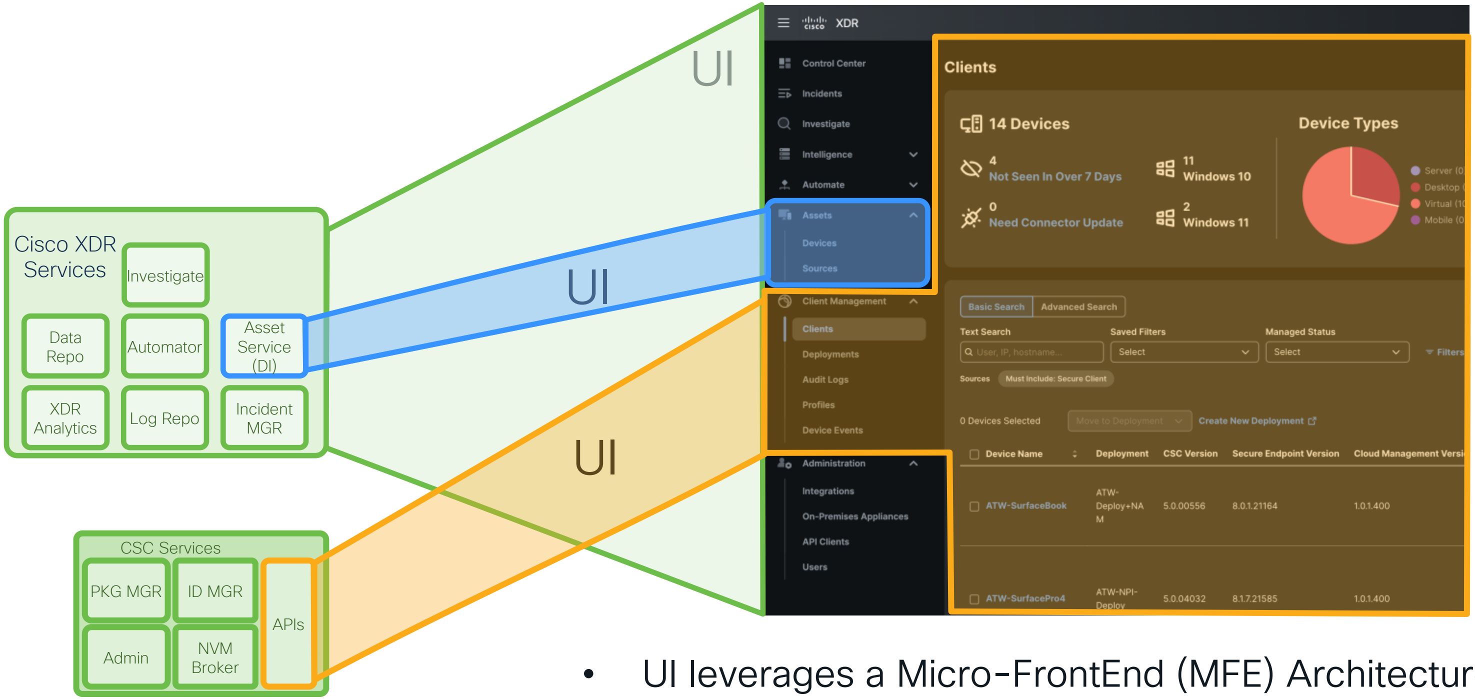
- Existing components that are not fundamentally changing
- New components
- Components that form the Cisco Secure Client



Cisco Secure Client – Architecture



What Happens w/ CSC Management & XDR?



Clients

14 Devices

4 Not Seen In Over 7 Days

0 Need Connector Update

11 Windows 10

2 Windows 11

Text Search: User, IP, hostname...

Saved Filters: Select

Managed Status: Select

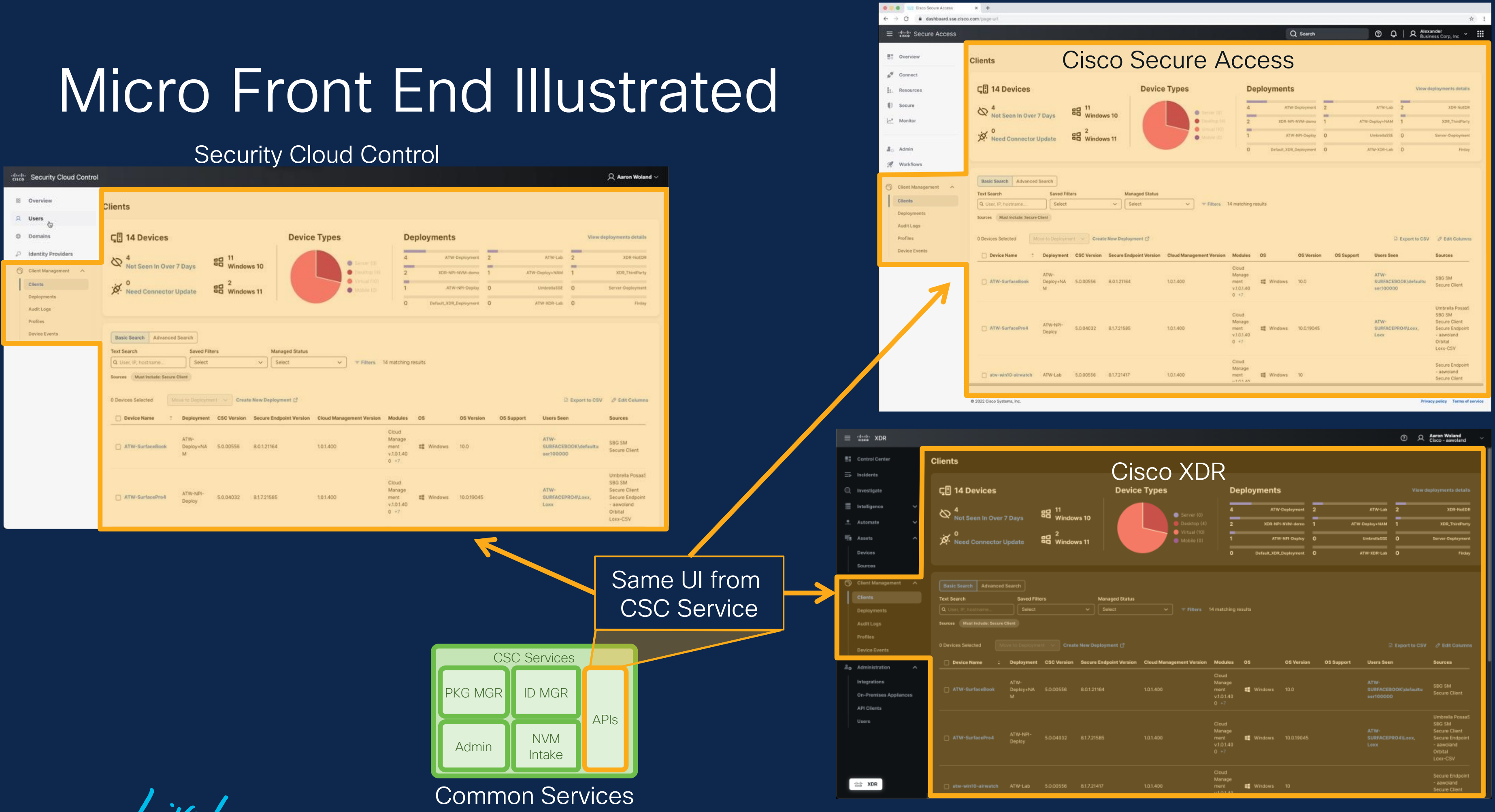
Sources: Must Include: Secure Client

0 Devices Selected

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

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

Micro Front End Illustrated



Security Cloud Control

Cisco Secure Access

Cisco XDR

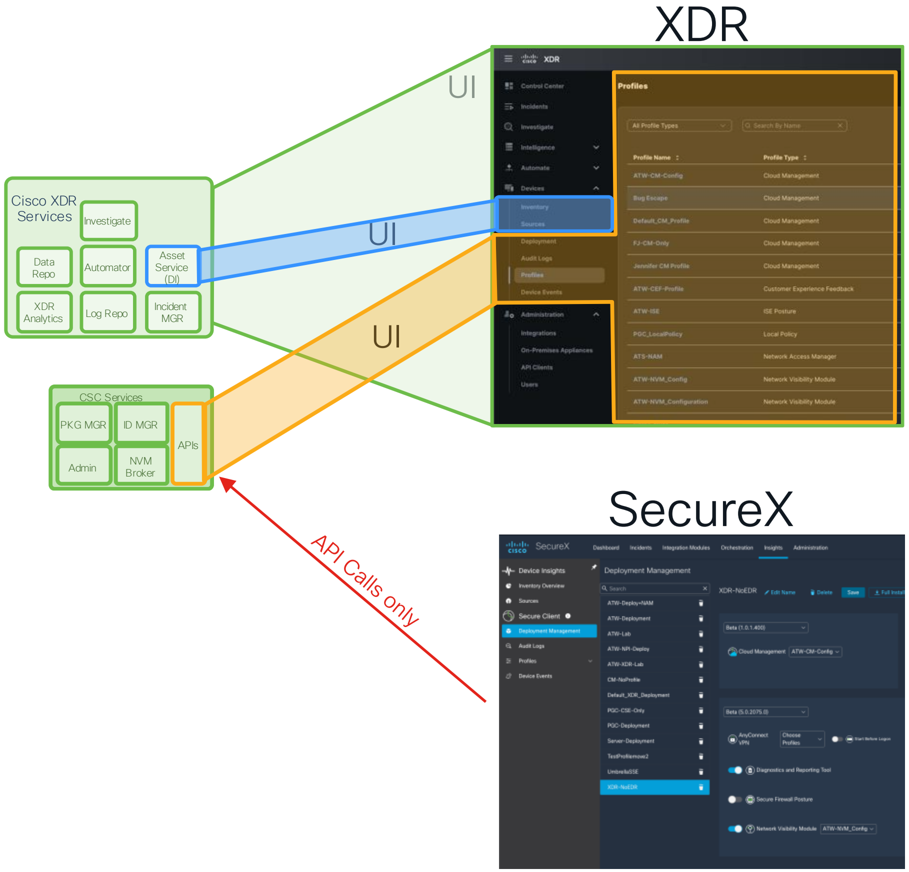
Same UI from CSC Service

CSC Services

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



Profiles

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

Deployment Management

- ATW-Deploy+NAM
- ATW-Deployment
- ATW-Lab
- ATW-NPI-Deploy
- ATW-XDR-Lab
- CM-NoProfile
- Default_XDR_Deployment
- PGC-CSE-Only
- PGC-Deployment
- Server-Deployment
- TestProfilemove2
- UmbrellaSSE
- XDR-NoEDR

XDR-NoEDR

Beta (1.0.1.400)

Cloud Management: ATW-CM-Config

Beta (5.0.2075.0)

AnyConnect VPN: Choose Profiles — Start Before Login

Diagnostics and Reporting Tool

Secure Firewall Posture

Network Visibility Module: ATW-NVM_Config

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

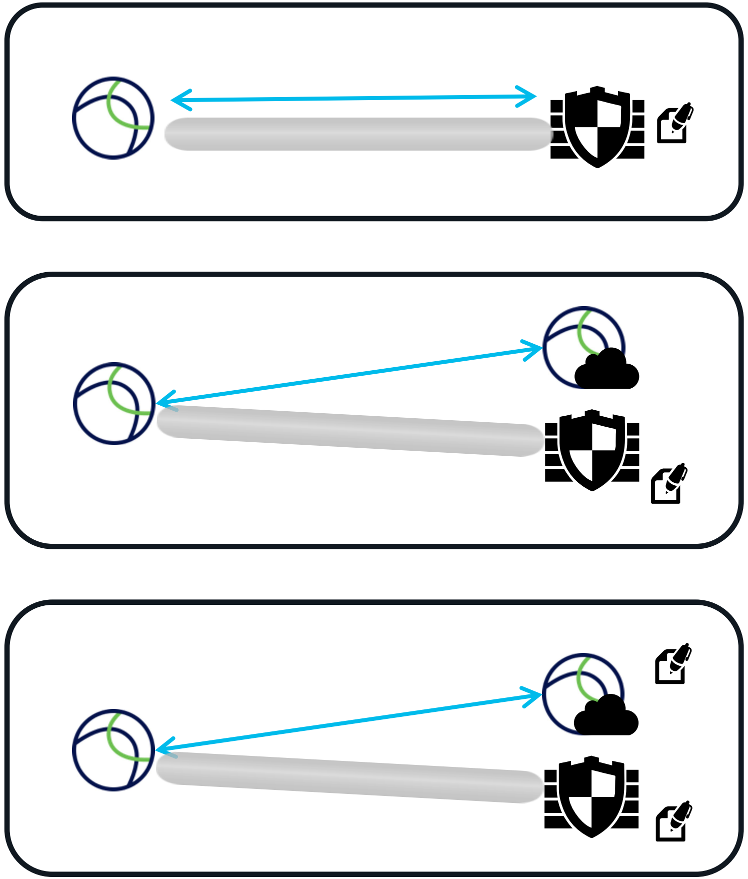
Deploying / Managing from Cloud

Agenda

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

Deployment Models

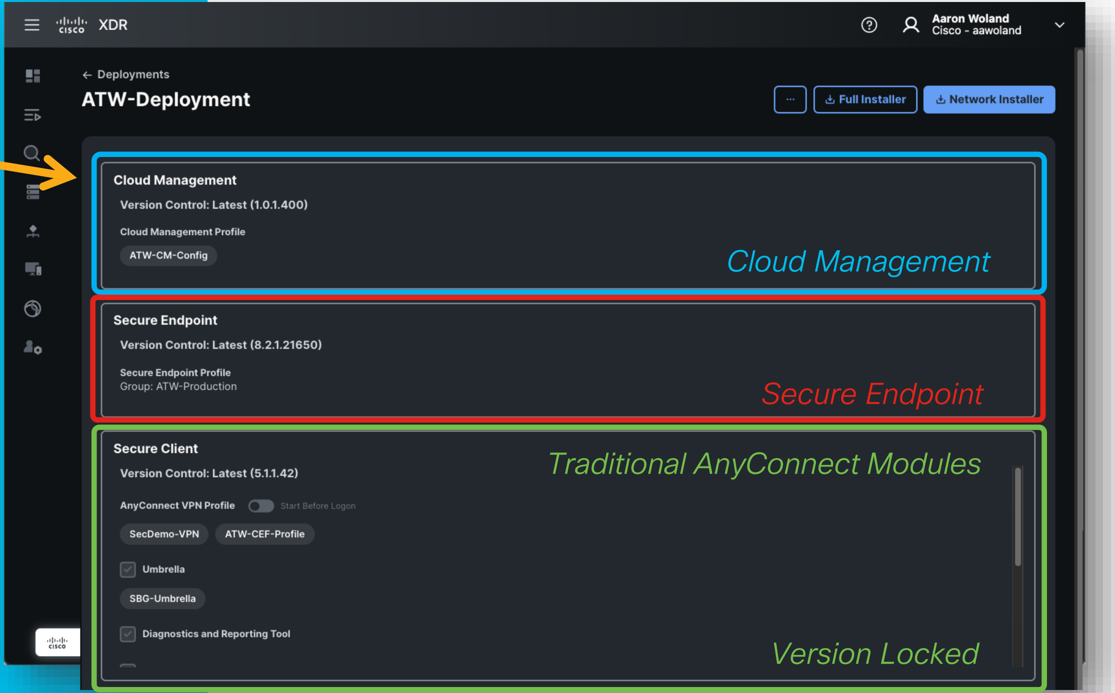
- No Cloud Management
- Cloud Registration – no Package Management
- Cloud Registration – Full Management



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



ATW-Deployment

Cloud Management

Version Control: Latest (1.0.1.400)

Cloud Management Profile

ATW-CM-Config

Secure Endpoint

Version Control: Latest (8.2.1.21650)

Secure Endpoint Profile
Group: ATW-Production

Secure Client

Version Control: Latest (5.1.1.42)

AnyConnect VPN Profile ○ Start Before Logon

SecDemo-VPN ATW-CEF-Profile

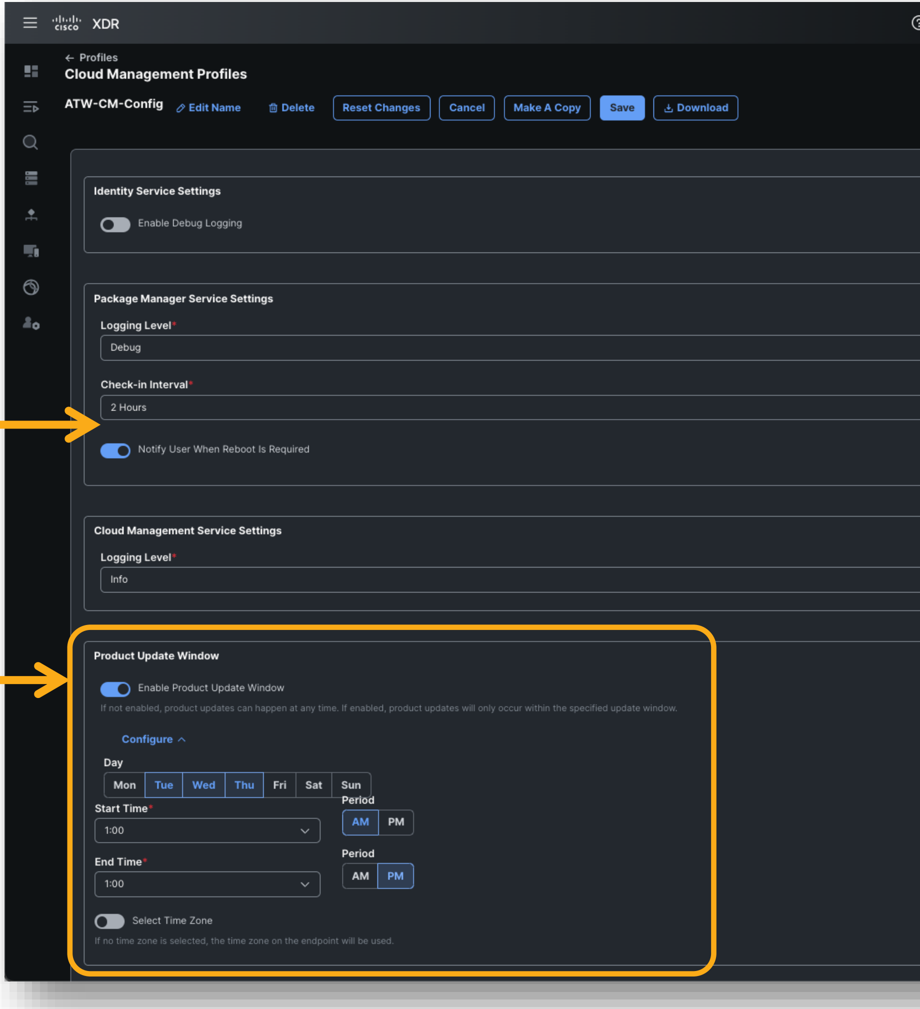
☑ Umbrella

SBG-Umbrella

☑ Diagnostics and Reporting Tool

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



Cloud Management Profiles

ATW-CM-Config

Identity Service Settings

Enable Debug Logging

Package Manager Service Settings

Logging Level*: Debug

Check-in Interval*: 2 Hours

Notify User When Reboot Is Required

Cloud Management Service Settings

Logging Level*: Info

Product Update Window

Enable Product Update Window

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

Day: Mon [✓ Tue] [✓ Wed] [✓ Thu] Fri Sat Sun

Start Time*: 1:00 — Period: [✓ AM] PM

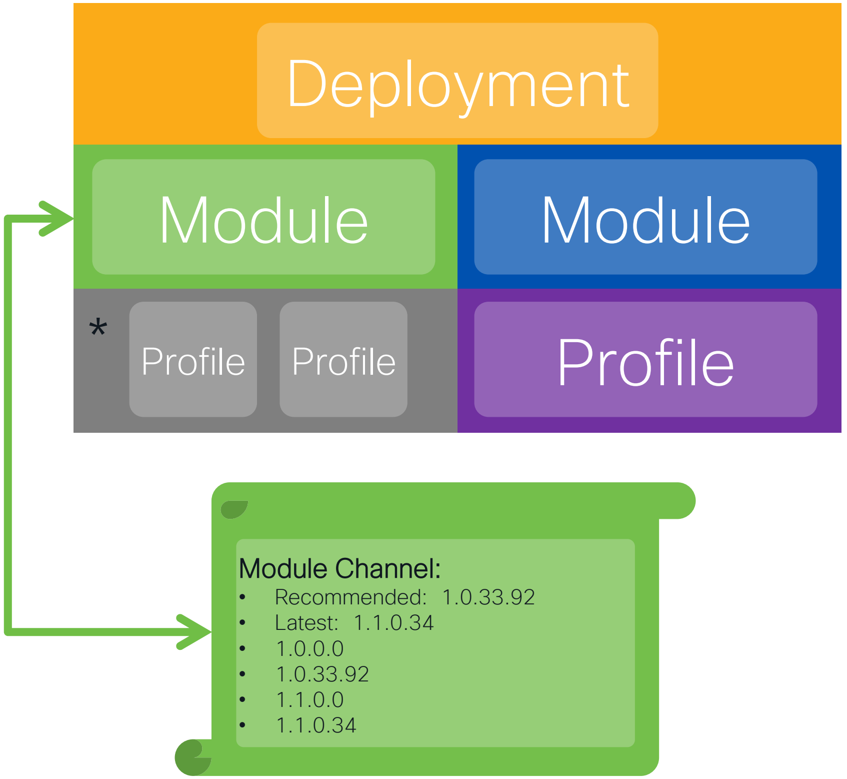
End Time*: 1:00 — Period: AM [✓ PM]

Select Time Zone

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

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

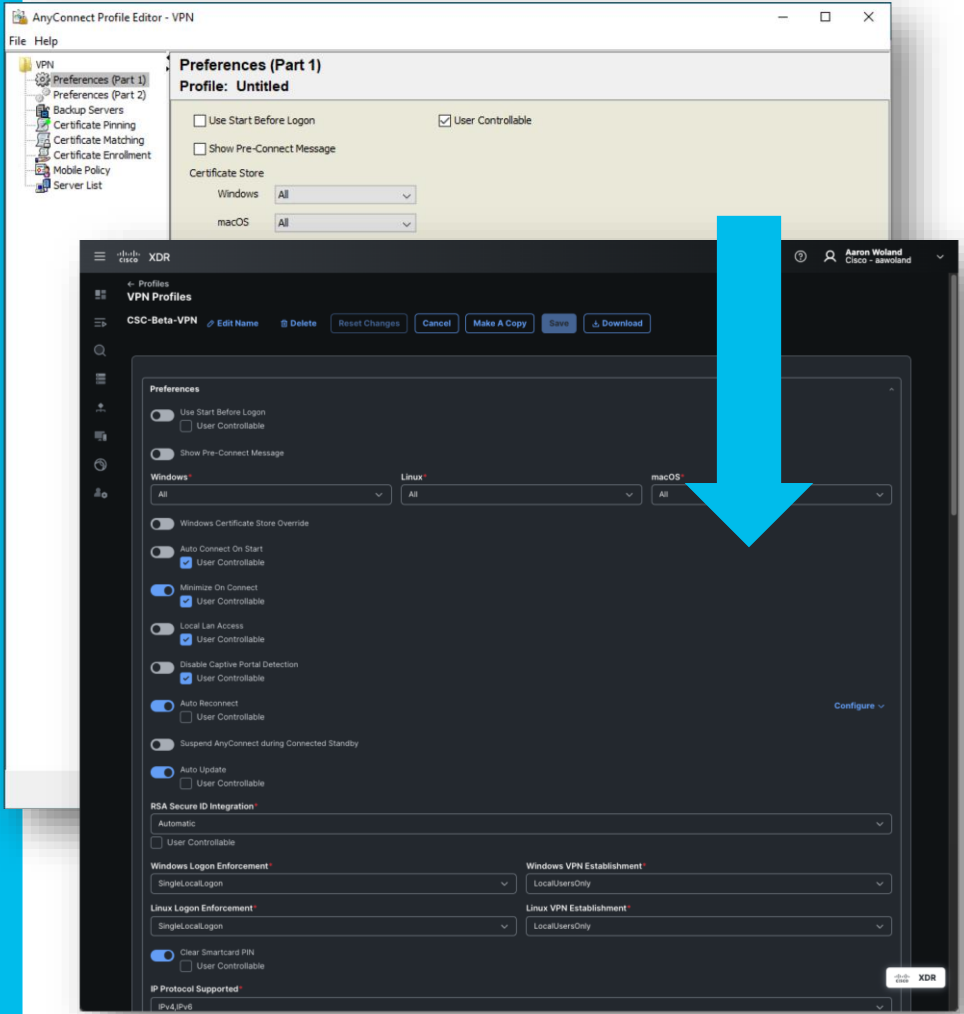


Module Channel:
- Recommended: 1.0.33.92
- Latest: 1.1.0.34
- 1.0.0.0
- 1.0.33.92
- 1.1.0.0
- 1.1.0.34

* When module supports >1

Managed from XDR / SecureX UI

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



AnyConnect Profile Editor - VPN

Preferences (Part 1)

Profile: Untitled

□ Use Start Before Logon ☑ User Controllable

□ Show Pre-Connect Message

Certificate Store

Windows: All

macOS: All

VPN Profiles

CSC-Beta-VPN

Preferences

○ Use Start Before Logon
□ User Controllable

○ Show Pre-Connect Message

Windows*: All

Linux*: All

macOS*: All

○ Windows Certificate Store Override

○ Auto Connect On Start
☑ User Controllable

● Minimize On Connect
☑ User Controllable

○ Local Lan Access
☑ User Controllable

○ Disable Captive Portal Detection
☑ User Controllable

● Auto Reconnect
□ User Controllable

○ Suspend AnyConnect during Connected Standby

● Auto Update
□ User Controllable

RSA Secure ID Integration*: Automatic
□ User Controllable

Windows Logon Enforcement*: SingleLocalLogon

Windows VPN Establishment*: LocalUsersOnly

Linux Logon Enforcement*: SingleLocalLogon

Linux VPN Establishment*: LocalUsersOnly

● Clear Smartcard PIN
□ User Controllable

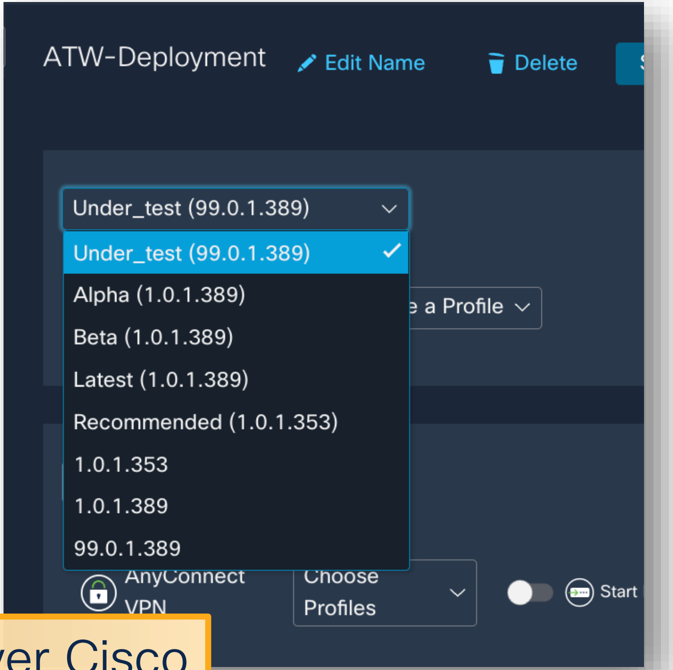
IP Protocol Supported*: IPv4,IPv6

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

  Auto Upgraded whenever Cisco publishes a new version to channel

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

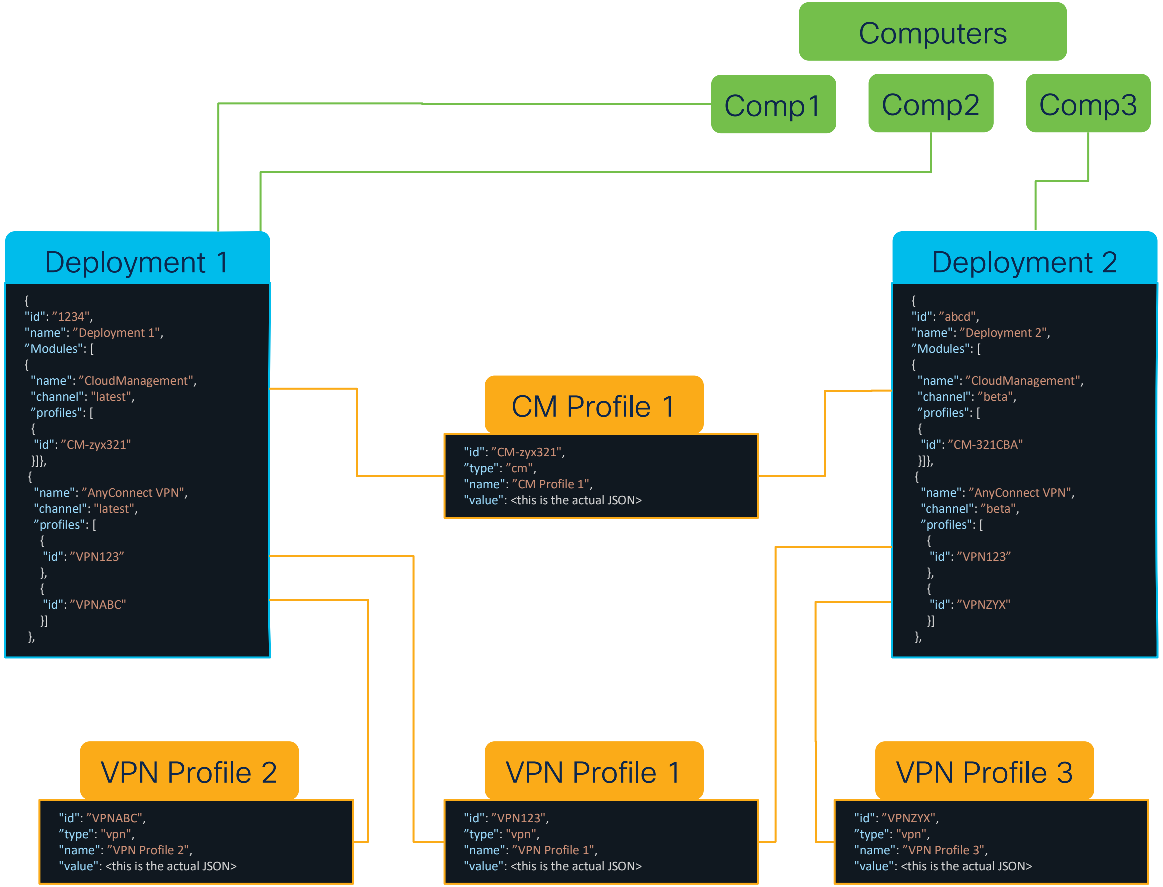


For CM and "AnyConnect" modules
SE module will use latest for bootstrap*

*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



Deployment 1

```
{
"id": ”1234",
"name": ”Deployment 1",
”Modules": [
{
 "name": ”CloudManagement",
 "channel": "latest",
 ”profiles": [
  {
   "id": ”CM-zyx321"
  }]},
 {
  "name": ”AnyConnect VPN",
  "channel": "latest",
  ”profiles": [
    {
     "id": ”VPN123”
    },
    {
     "id": ”VPNABC"
    }]
 },
```

Deployment 2

```
{
"id": ”abcd",
"name": ”Deployment 2",
”Modules": [
{
 "name": ”CloudManagement",
 "channel": ”beta",
 ”profiles": [
  {
   "id": ”CM-321CBA"
  }]},
 {
  "name": ”AnyConnect VPN",
  "channel": ”beta",
  ”profiles": [
    {
     "id": ”VPN123”
    },
    {
     "id": ”VPNZYX"
    }]
 },
```

CM Profile 1

```
"id": ”CM-zyx321",
”type": ”cm",
"name": ”CM Profile 1",
"value": <this is the actual JSON>
```

VPN Profile 2

```
"id": ”VPNABC",
”type": "vpn",
"name": ”VPN Profile 2",
"value": <this is the actual JSON>
```

VPN Profile 1

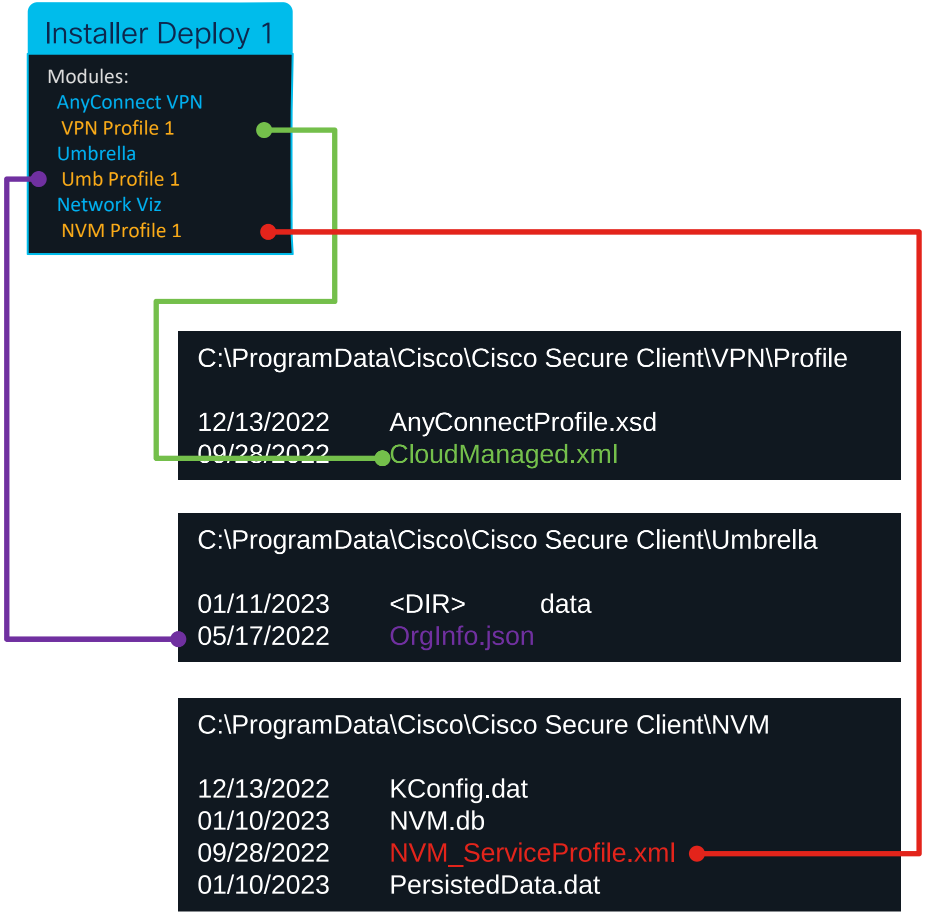
```
"id": ”VPN123",
”type": "vpn",
"name": ”VPN Profile 1",
"value": <this is the actual JSON>
```

VPN Profile 3

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

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)



Installer Deploy 1

Modules:
AnyConnect VPN
VPN Profile 1
Umbrella
Umb Profile 1
Network Viz
NVM Profile 1

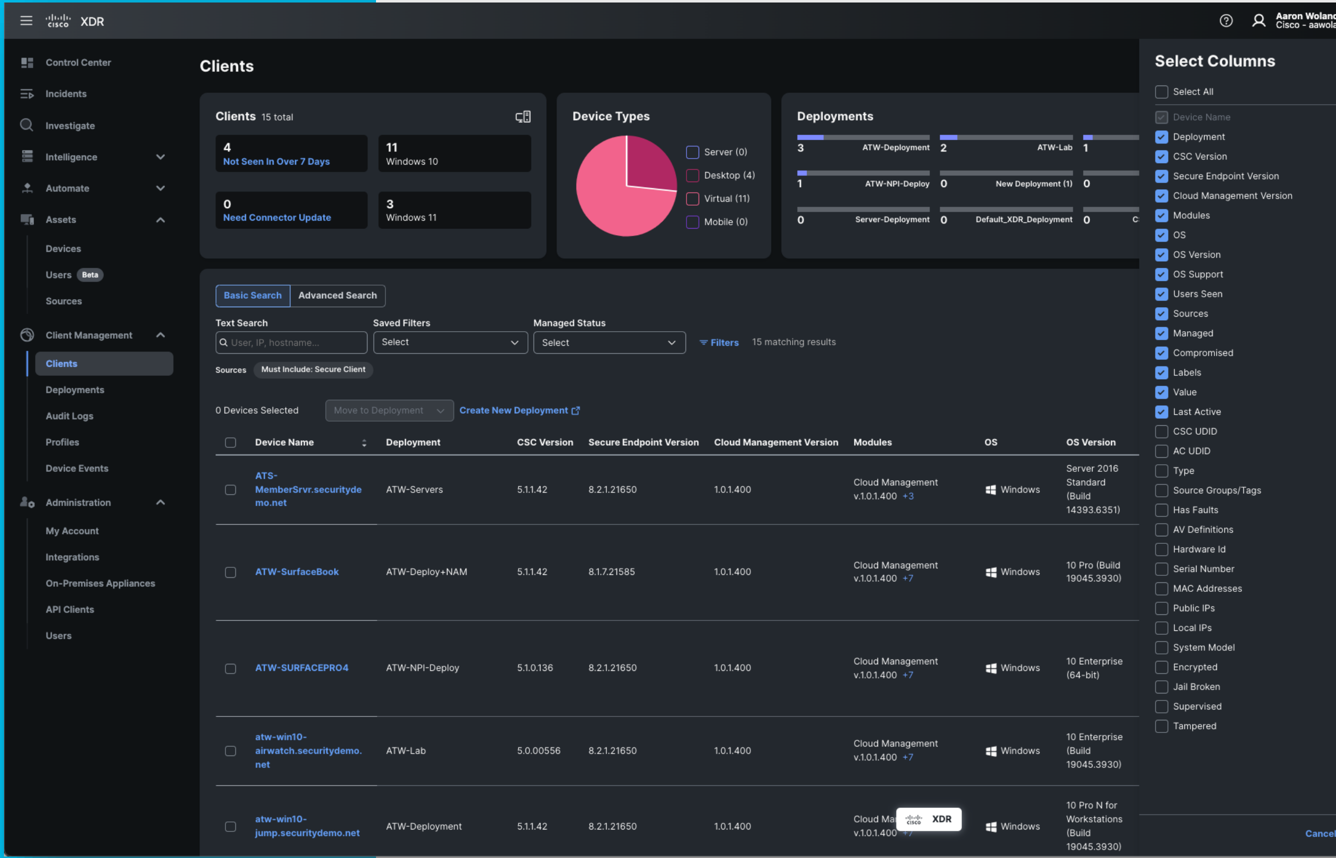
```
C:\ProgramData\Cisco\Cisco Secure Client\VPN\Profile

12/13/2022      AnyConnectProfile.xsd
09/28/2022      CloudManaged.xml
```

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

01/11/2023      <DIR>        data
05/17/2022      OrgInfo.json
```

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

12/13/2022      KConfig.dat
01/10/2023      NVM.db
09/28/2022      NVM_ServiceProfile.xml
01/10/2023      PersistedData.dat
```

Client Management

- Client Management is its own section in XDR
  - Clients
  - Deployments
  - Profiles
  - Audit Logs
  - Device Events



Clients

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	C

Basic Search | Advanced Search

Text Search: 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

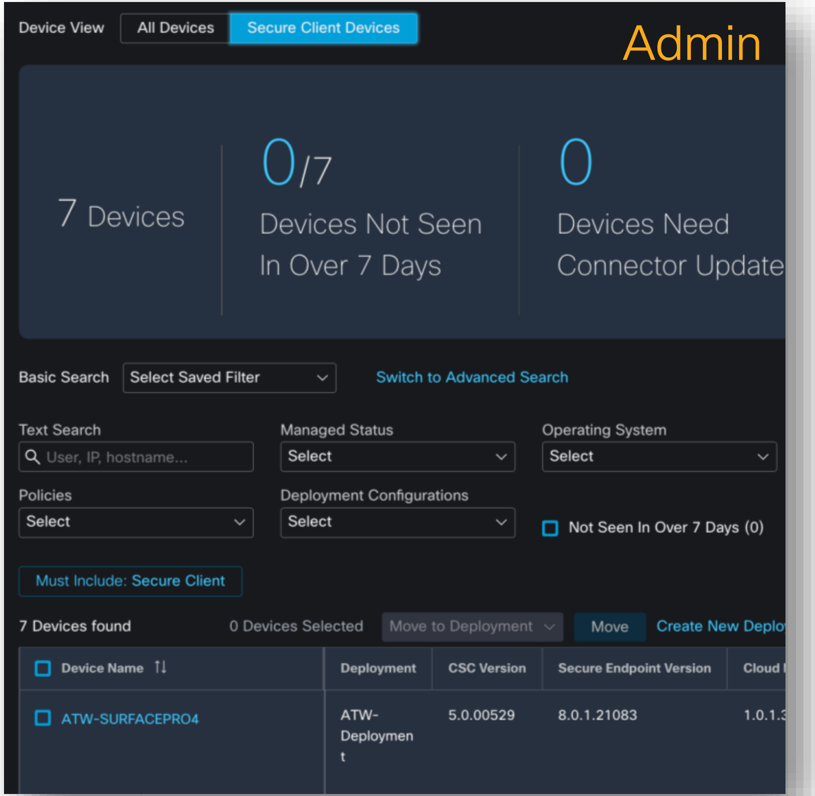
□	Device Name	Deployment	CSC Version	Secure Endpoint Version	Cloud Management Version	Modules	OS	OS Version
□	ATS-MemberSrvr.securitydemo.net	ATW-Servers	5.1.1.42	8.2.1.21650	1.0.1.400	Cloud Management v.1.0.1.400 +3	Windows	Server 2016 Standard (Build 14393.6351)
□	ATW-SurfaceBook	ATW-Deploy+NAM	5.1.1.42	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	5.0.00556	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	5.1.1.42	8.2.1.21650	1.0.1.400	Cloud Ma v.1.0.1.400 +7	Windows	10 Pro N for Workstations (Build 19045.3930)

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

Cancel

Moving Deployments – Admin Only



Admin

Device View | All Devices | Secure Client Devices

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

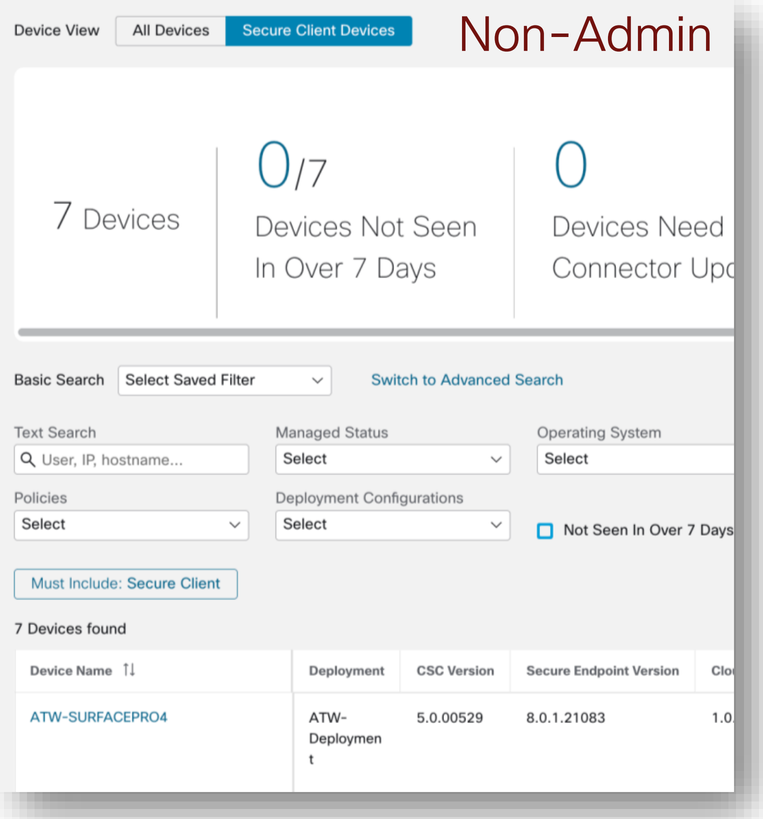
Deployment Configurations: Select

□ Not Seen In Over 7 Days (0)

Must Include: Secure Client

7 Devices found — 0 Devices Selected — Move to Deployment — Move — Create New Deplo

□ Device Name	Deployment	CSC Version	Secure Endpoint Version	Cloud I
□ ATW-SURFACEPRO4	ATW-Deployment	5.0.00529	8.0.1.21083	1.0.1.3



Non-Admin

Device View | All Devices | Secure Client Devices

7 Devices

0/7 Devices Not Seen In Over 7 Days

0 Devices Need Connector Upd

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

Must Include: Secure Client

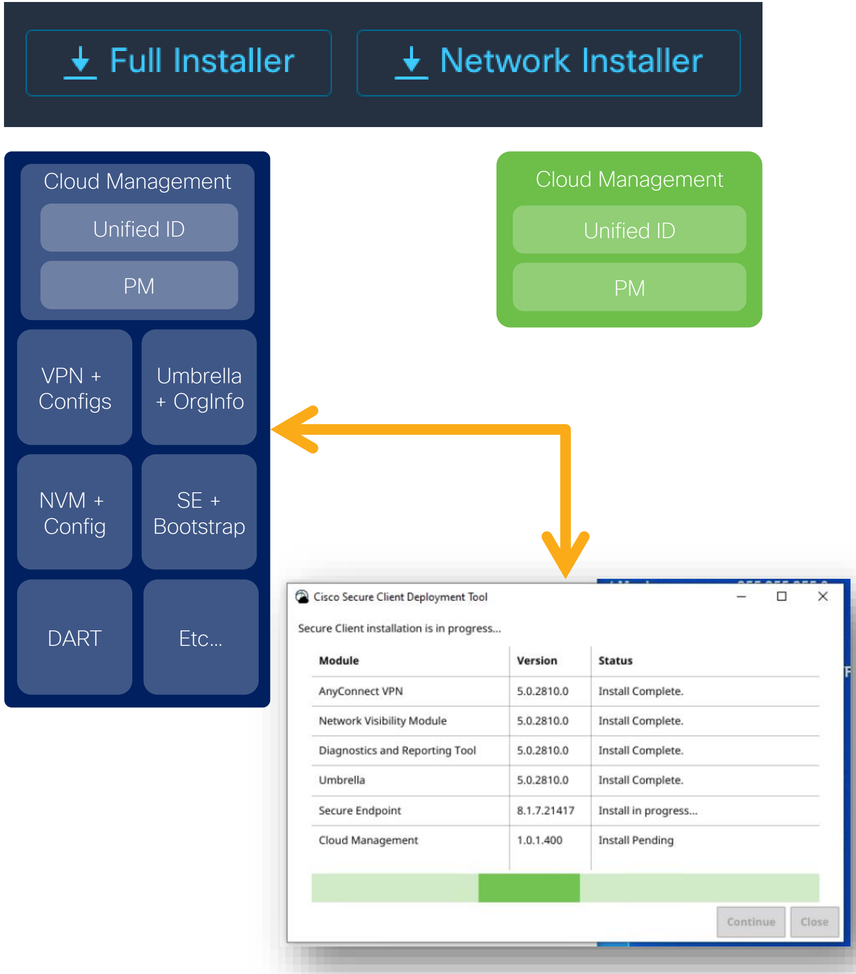
7 Devices found

Device Name	Deployment	CSC Version	Secure Endpoint Version	Clo
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.

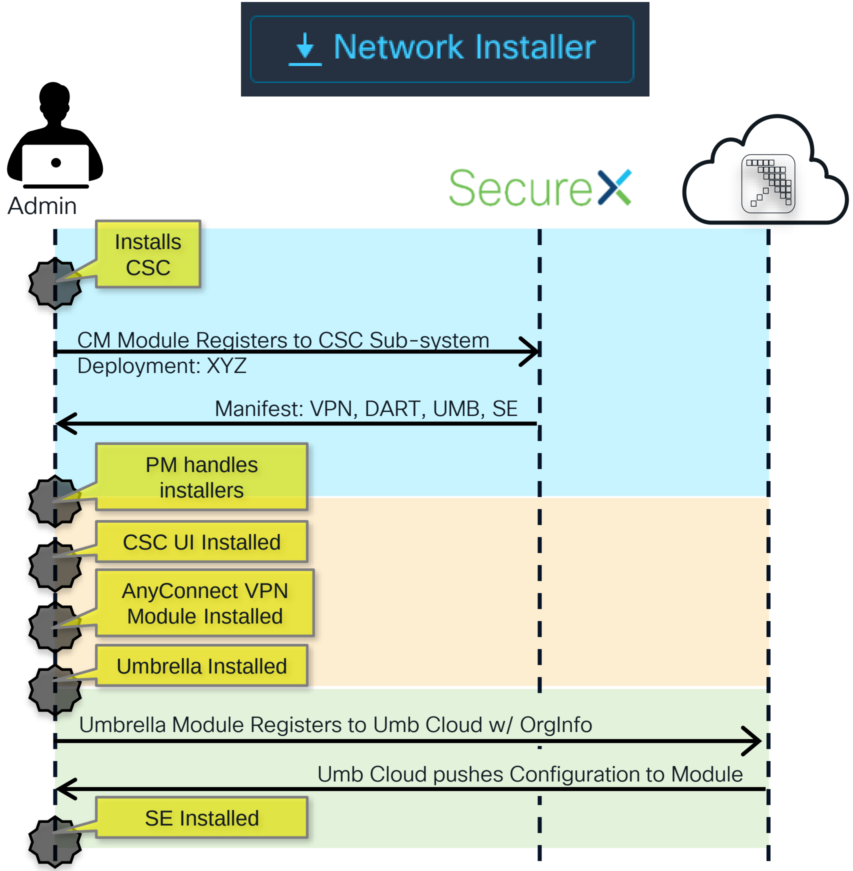


Secure Client installation is in progress...

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

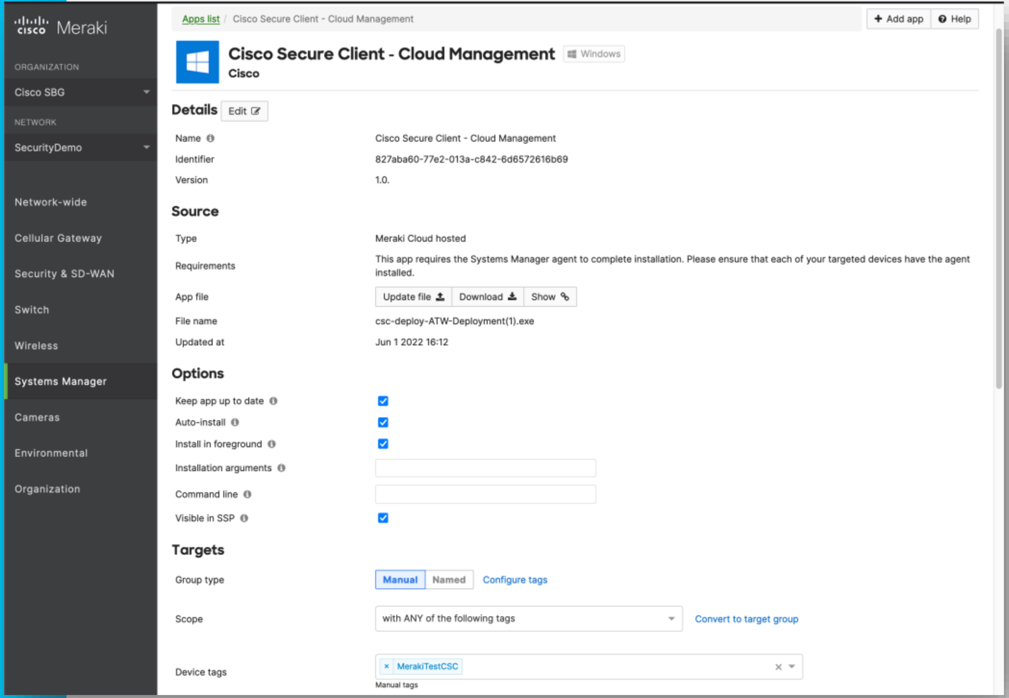
Network Installer

- 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


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

Installing CSC

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



Cisco Secure Client - Cloud Management
Cisco

Details

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

Source

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

Options

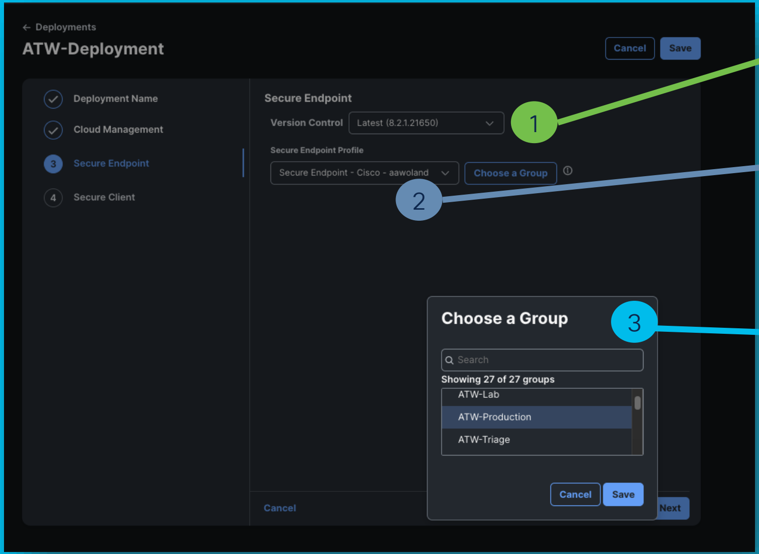
Keep app up to date	☑
Auto-install	☑
Install in foreground	☑
Installation arguments	
Command line	
Visible in SSP	☑

Targets

Group type	Manual · Named
Scope	with ANY of the following tags
Device tags	× MerakiTestCSC Manual tags

Deployments w/ Secure Endpoint and Orbital

Configuring Secure Endpoint



← Deployments

ATW-Deployment

Cancel Save

- ✓ Deployment Name
- ✓ Cloud Management
- 3 Secure Endpoint
- 4 Secure Client

Secure Endpoint

Version Control: Latest (8.2.1.21650)

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

Choose a Group

Search

Showing 27 of 27 groups

- ATW-Lab
- ATW-Production
- ATW-Triage

Cancel Save

Cancel Next

Select Desired SE Version

Select your SE Integration

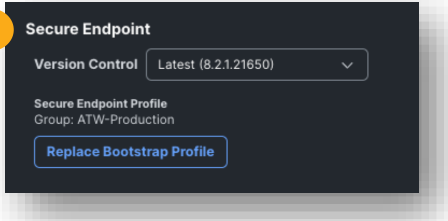
There *can* be more than one

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.

4

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



Secure Endpoint

Version Control: Latest (8.2.1.21650)

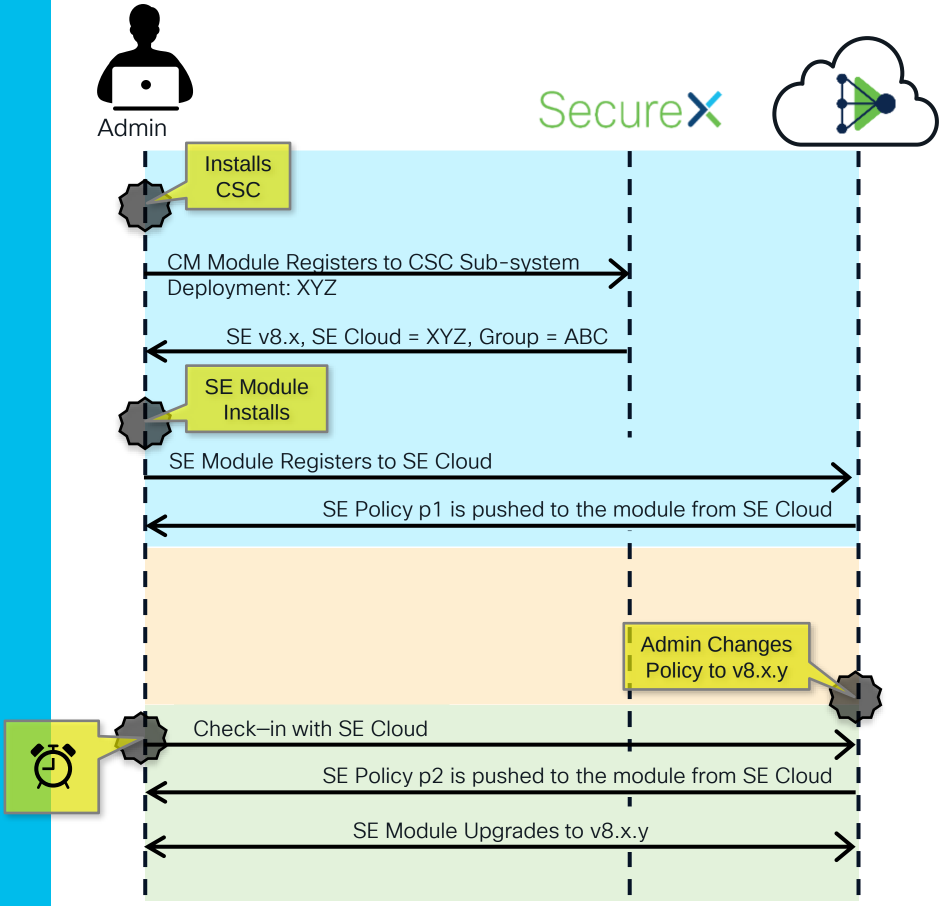
Secure Endpoint Profile
Group: ATW-Production

Replace Bootstrap Profile

cisco Live!

Bootstrap?

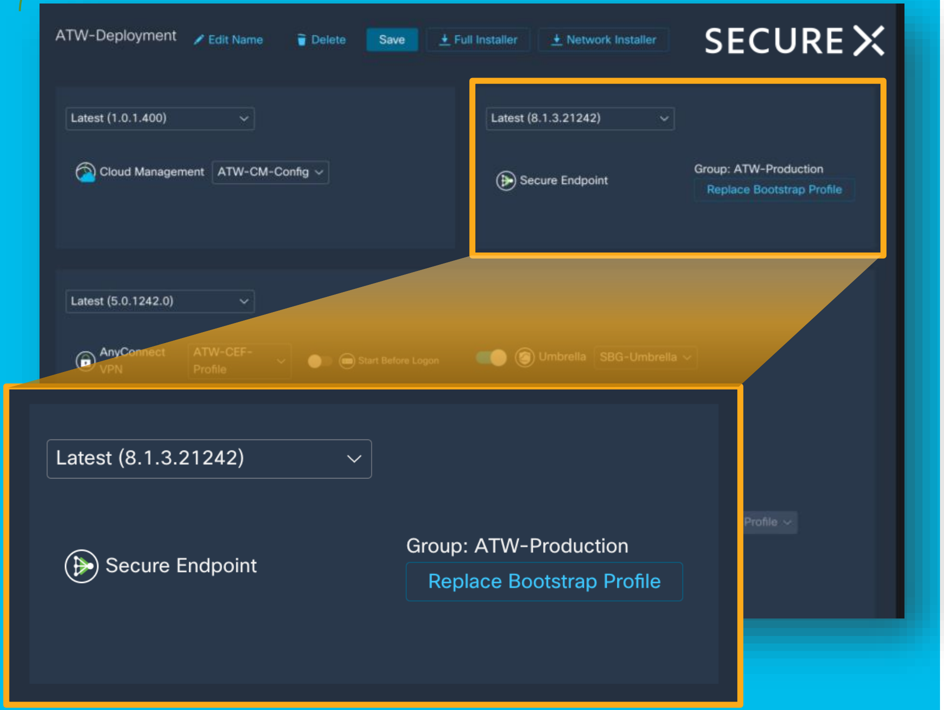
- Secure Client config is just to get the SE module to install & register to SE Cloud.
  - Then: ALL group & policy control of the SE module comes from SE Cloud.
  - SE group changes, software updates, etc...
  - SecureX can still update software versions through deployment.


Admin
SecureX
Installs CSC
CM Module Registers to CSC Sub-system
Deployment: XYZ
SE v8.x, SE Cloud = XYZ, Group = ABC
SE Module Installs
SE Module Registers to SE Cloud
SE Policy p1 is pushed to the module from SE Cloud
Admin Changes Policy to v8.x.y
Check–in with SE Cloud
SE Policy p2 is pushed to the module from SE Cloud
SE Module Upgrades to v8.x.y

cisco Live!

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

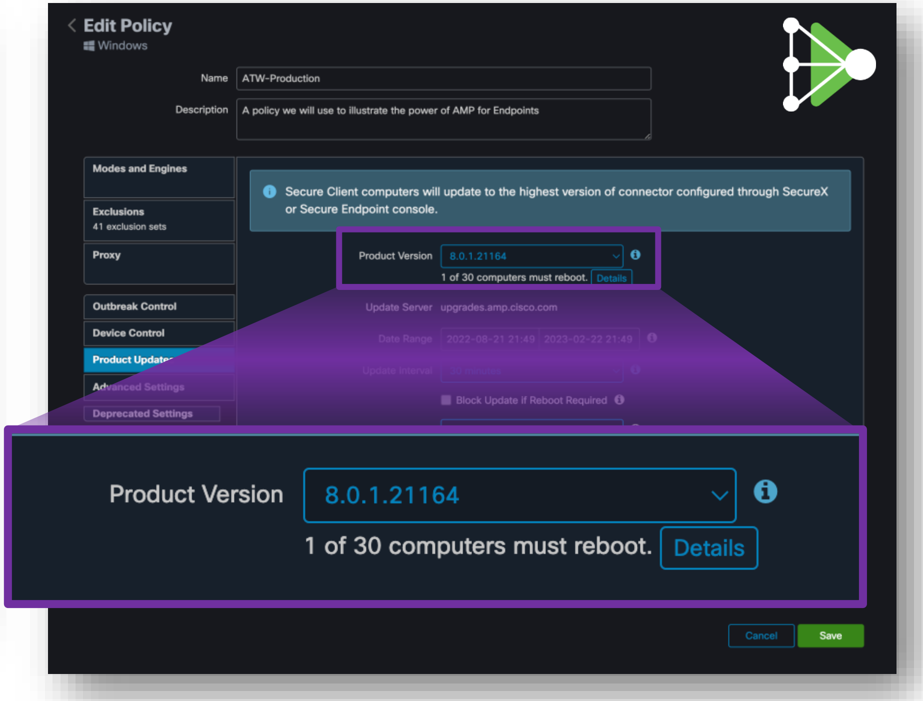
Replace Bootstrap Profile

Latest (5.0.1242.0)

AnyConnect VPN ATW-CEF-Profile

Start Before Logon

Umbrella SBG-Umbrella



Edit Policy

Windows

Name: ATW-Production

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

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

Product Version: 8.0.1.21164

1 of 30 computers must reboot. Details

Update Server: upgrades.amp.cisco.com

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

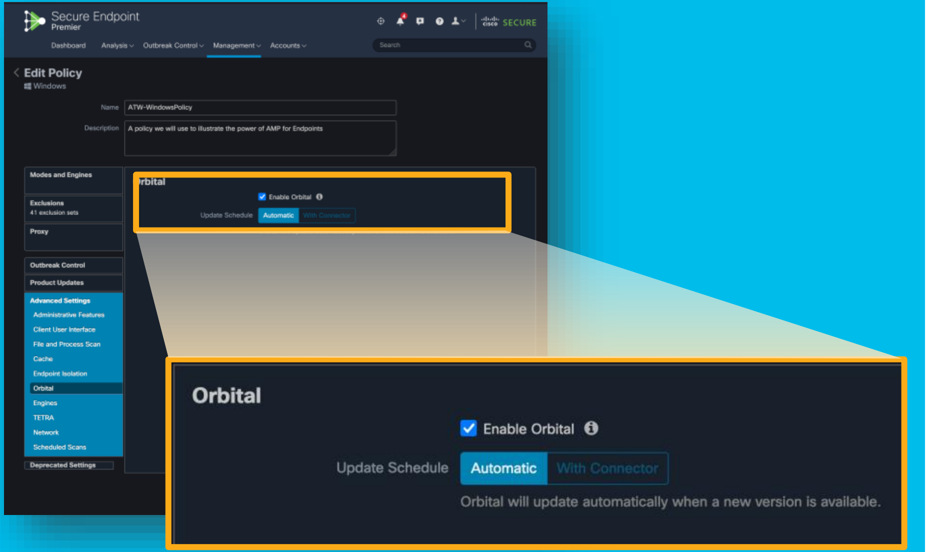
Update Interval

□ Block Update if Reboot Required

Cancel Save

Deploying Orbital

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



Edit Policy

Windows

Name: ATW-WindowsPolicy

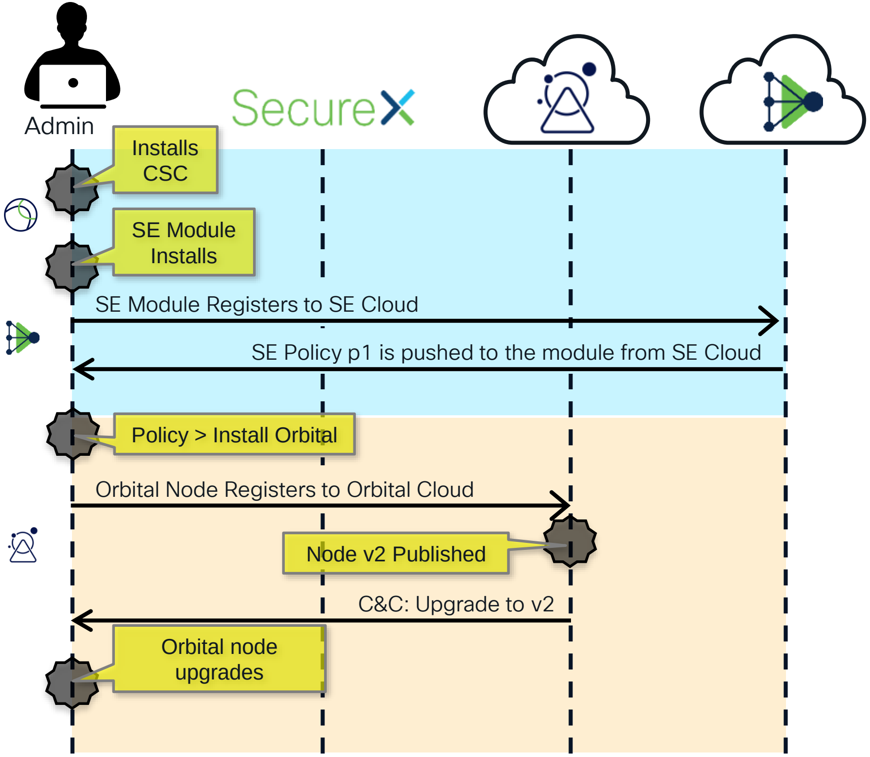
Description: A policy we will use to illustrate the power of AMP for Endpoints

Orbital

☑ Enable Orbital

Update Schedule: [✓ Automatic] With Connector

Orbital will update automatically when a new version is available.



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

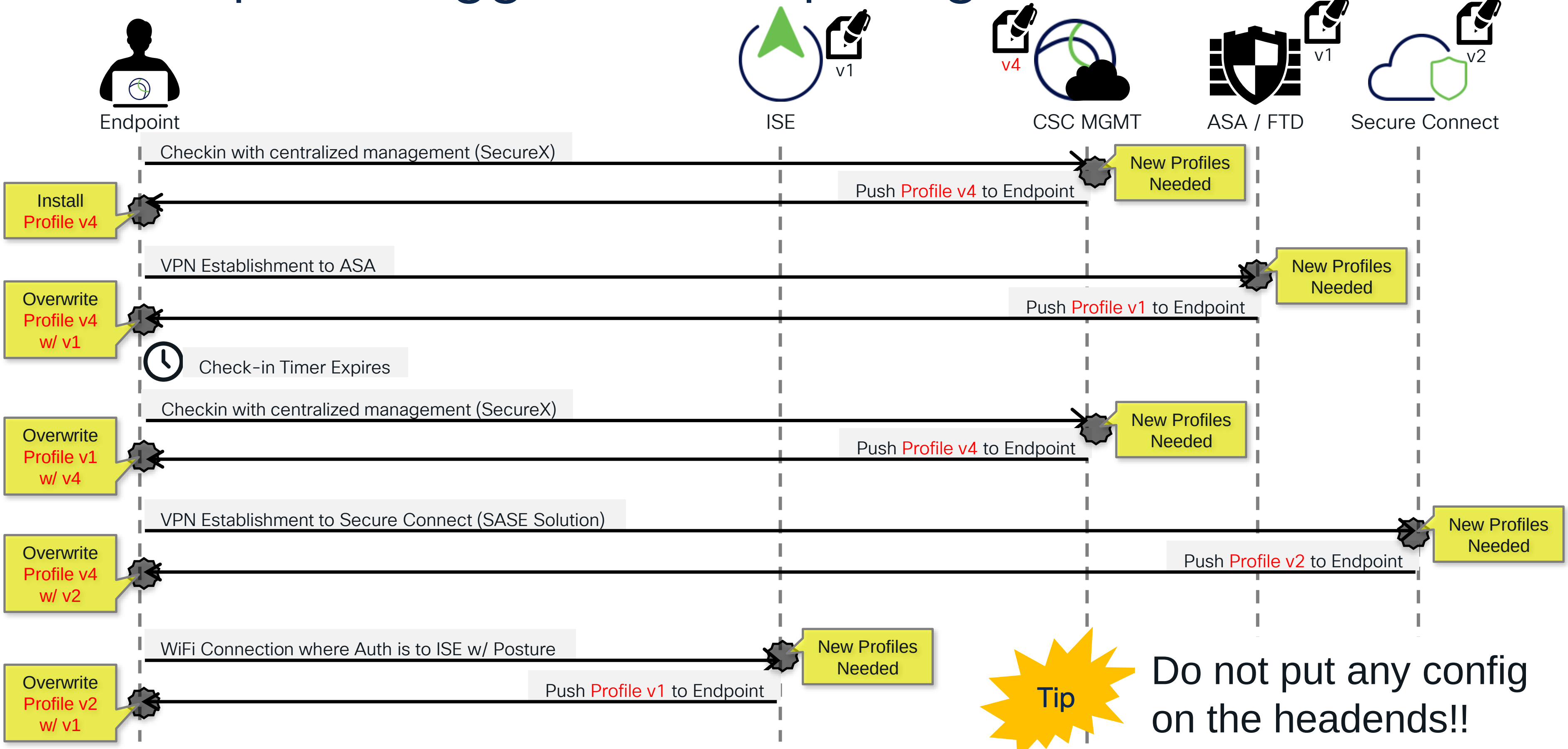
Agenda

- 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



Endpoint

ISE v1

CSC MGMT v4

ASA / FTD v1

Secure Connect v2

Checkin with centralized management (SecureX)

New Profiles Needed

Push Profile v4 to Endpoint

Install Profile v4

VPN Establishment to ASA

New Profiles Needed

Push Profile v1 to Endpoint

Overwrite Profile v4 w/ v1

Check-in Timer Expires

Checkin with centralized management (SecureX)

New Profiles Needed

Push Profile v4 to Endpoint

Overwrite Profile v1 w/ v4

VPN Establishment to Secure Connect (SASE Solution)

New Profiles Needed

Push Profile v2 to Endpoint

Overwrite Profile v4 w/ v2

WiFi Connection where Auth is to ISE w/ Posture

New Profiles Needed

Push Profile v1 to Endpoint

Overwrite Profile v2 w/ v1

Tip

Do not put any config on the headends!!

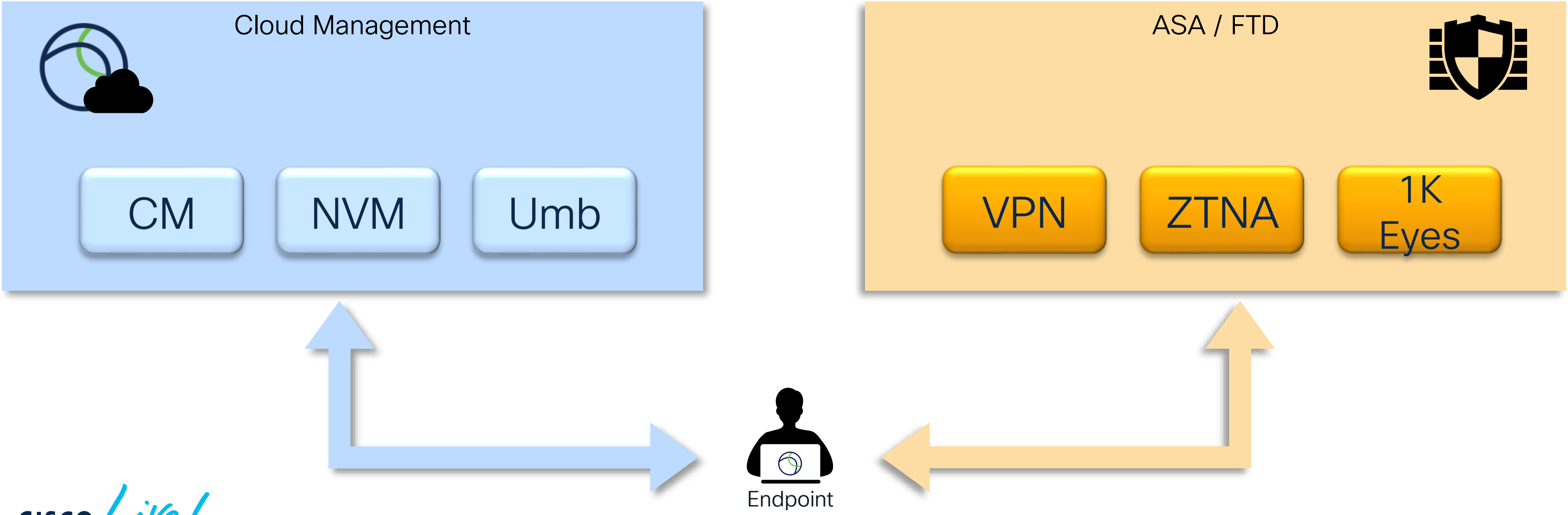
Details on Profile Merges

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

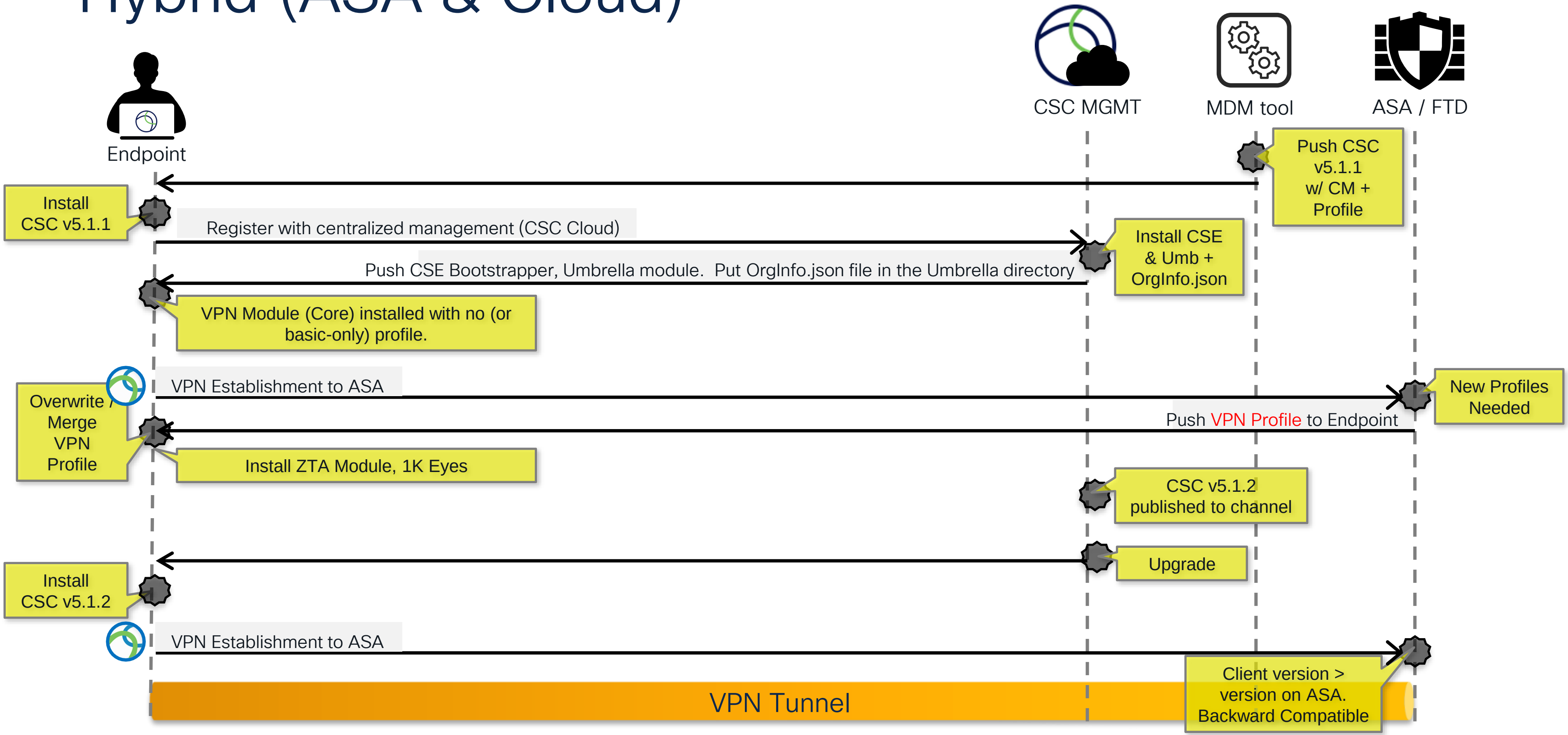
- If filenames match: ASA will overwrite the profile
- If filenames don't match: both profiles will be detected by VPN and behavior might be a little wonky... Some settings get merged from all detected profiles

Hybrid (ASA & Cloud)

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



Hybrid (ASA & Cloud)



Endpoint

CSC MGMT

MDM tool

ASA / FTD

Push CSC v5.1.1 w/ CM + Profile

Install CSC v5.1.1

Register with centralized management (CSC Cloud)

Install CSE & Umb + OrgInfo.json

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

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

VPN Establishment to ASA

New Profiles Needed

Push VPN Profile to Endpoint

Overwrite / Merge VPN Profile

Install ZTA Module, 1K Eyes

CSC v5.1.2 published to channel

Upgrade

Install CSC v5.1.2

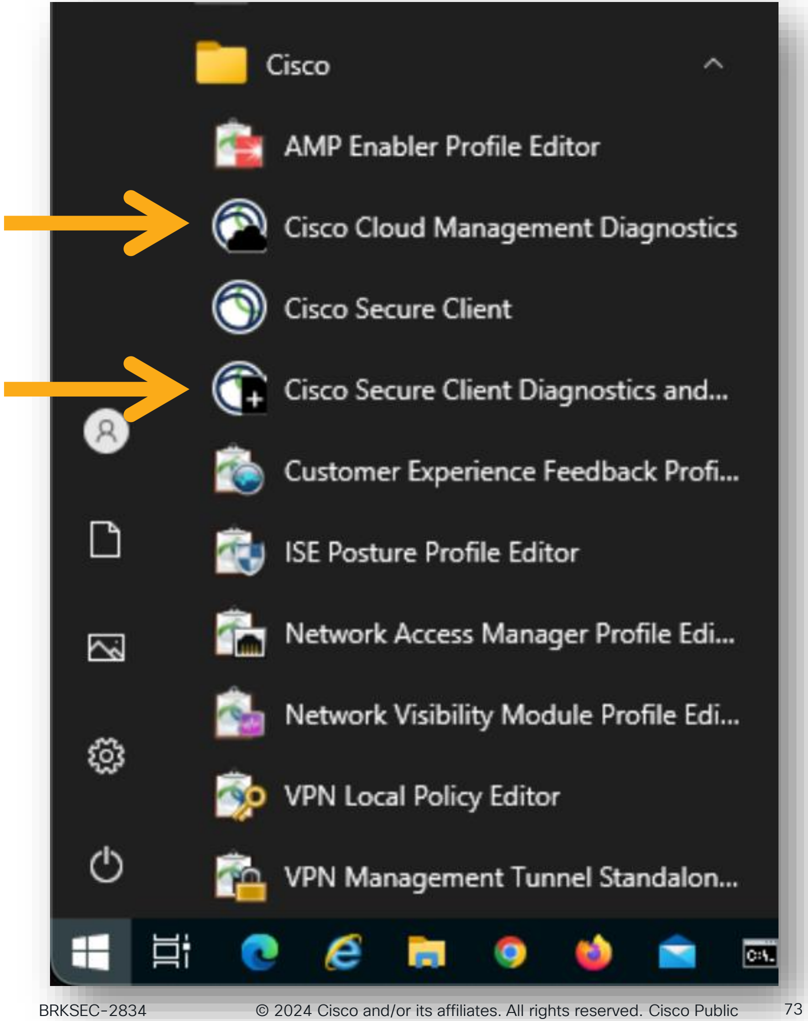
VPN Establishment to ASA

Client version > version on ASA. Backward Compatible

VPN Tunnel

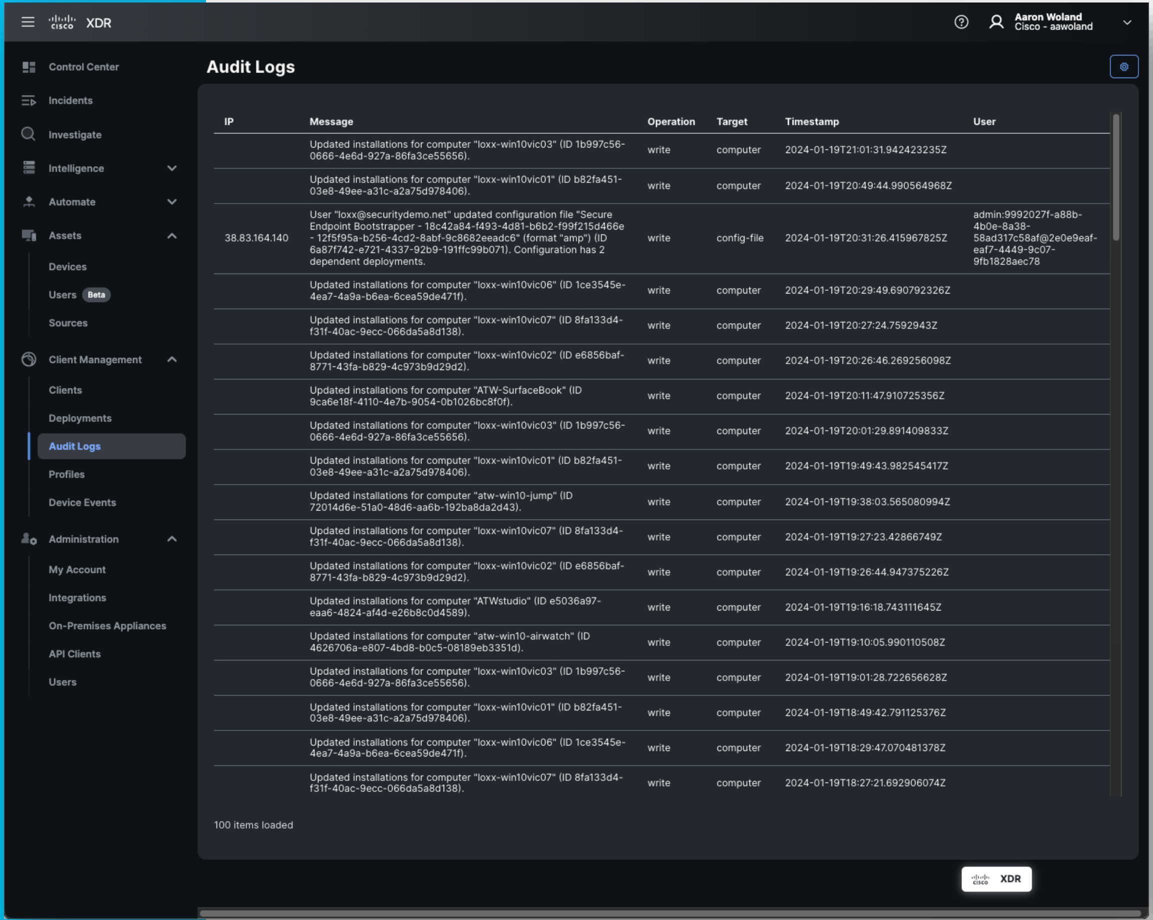
DART & CM Diagnostics

- *"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?


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

Audit Logging

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



Audit Logs

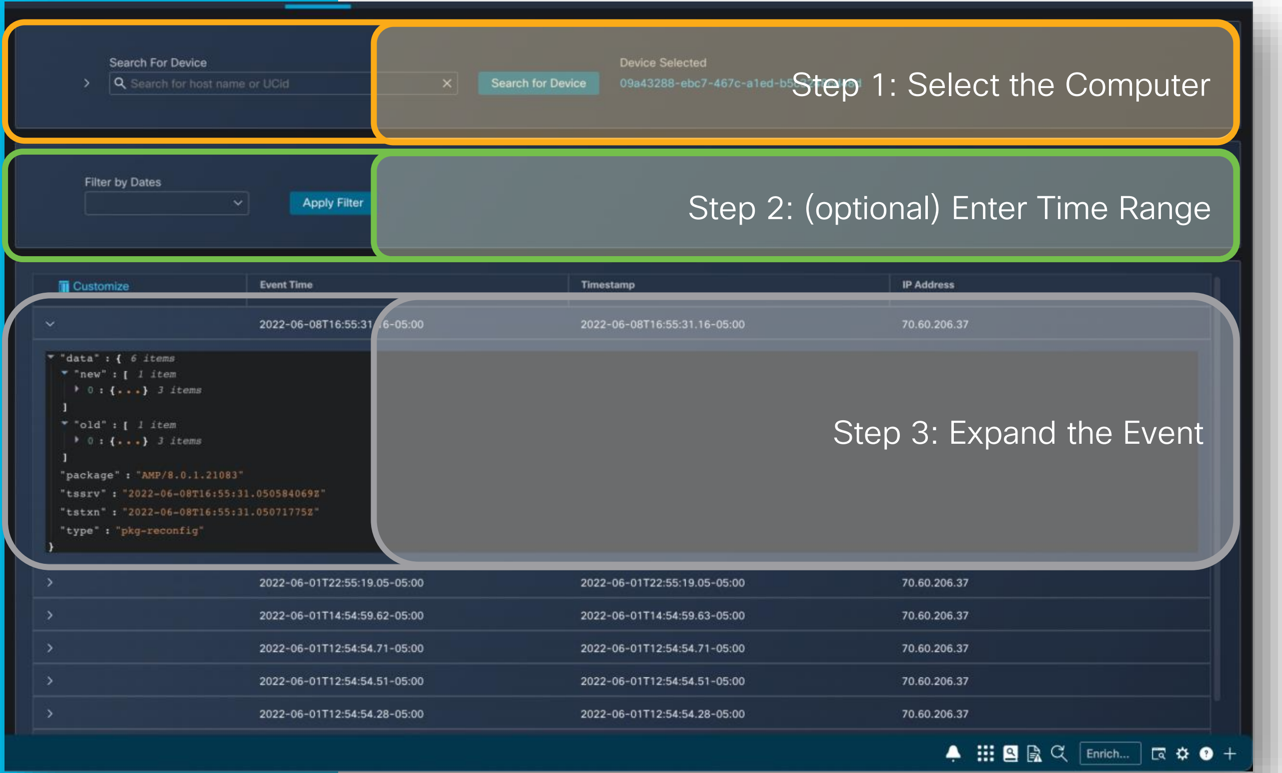
IP	Message	Operation	Target	Timestamp	User
	Updated installations for computer "loxx-win10vic03" (ID 1b997c56-0666-4e6d-927a-86fa3ce55656).	write	computer	2024-01-19T21:01:31.942423235Z	
	Updated installations for computer "loxx-win10vic01" (ID b82fa451-03e8-49ee-a31c-a2a75d978406).	write	computer	2024-01-19T20:49:44.990564968Z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

100 items loaded

cisco Live!

Cloud Event Logging

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



Step 1: Select the Computer

Search For Device

Search for host name or UCid

Search for Device

Device Selected

09a43288-ebc7-467c-a1ed-b5

Step 2: (optional) Enter Time Range

Filter by Dates

Apply Filter

Step 3: Expand the Event

Customize	Event Time	Timestamp	IP Address
⌄	2022-06-08T16:55:31.16-05:00	2022-06-08T16:55:31.16-05:00	70.60.206.37

```
▾ "data" : { 6 items
  ▾ "new" : [ 1 item
    ▸ 0 : {...} 3 items
  ]
  ▾ "old" : [ 1 item
    ▸ 0 : {...} 3 items
  ]
  "package" : "AMP/8.0.1.21083"
  "tssrv" : "2022-06-08T16:55:31.050584069Z"
  "tstxn" : "2022-06-08T16:55:31.050717752"
  "type" : "pkg-reconfig"
}
```

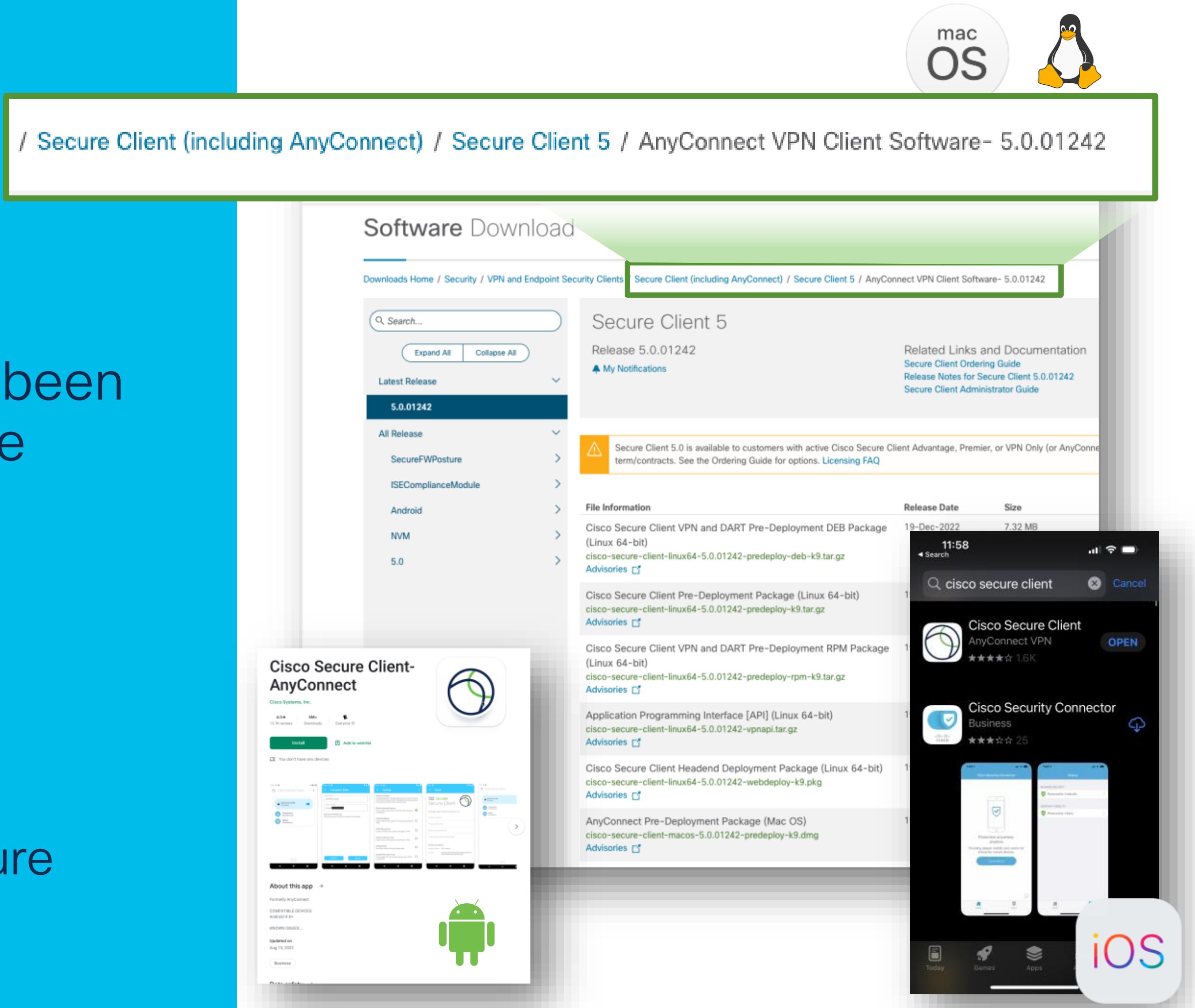
Customize	Event Time	Timestamp	IP Address
›	2022-06-01T22:55:19.05-05:00	2022-06-01T22:55:19.05-05:00	70.60.206.37
›	2022-06-01T14:54:59.62-05:00	2022-06-01T14:54:59.63-05:00	70.60.206.37
›	2022-06-01T12:54:54.71-05:00	2022-06-01T12:54:54.71-05:00	70.60.206.37
›	2022-06-01T12:54:54.51-05:00	2022-06-01T12:54:54.51-05:00	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)



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

Software Download

Downloads Home / Security / VPN and Endpoint Security Clients / Secure Client (including AnyConnect) / Secure Client 5 / AnyConnect VPN Client Software- 5.0.01242

Secure Client 5

Release 5.0.01242

My Notifications

Related Links and Documentation
Secure Client Ordering Guide
Release Notes for Secure Client 5.0.01242
Secure Client Administrator Guide

Secure Client 5.0 is available to customers with active Cisco Secure Client Advantage, Premier, or VPN Only (or AnyConne term/contracts. See the Ordering Guide for options. Licensing FAQ

File Information	Release Date	Size
Cisco Secure Client VPN and DART Pre-Deployment DEB Package (Linux 64-bit) cisco-secure-client-linux64-5.0.01242-predeploy-deb-k9.tar.gz Advisories	19-Dec-2022	7.32 MB
Cisco Secure Client Pre-Deployment Package (Linux 64-bit) cisco-secure-client-linux64-5.0.01242-predeploy-k9.tar.gz Advisories	1	
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	1	
Application Programming Interface [API] (Linux 64-bit) cisco-secure-client-linux64-5.0.01242-vpnapi.tar.gz Advisories	1	
Cisco Secure Client Headend Deployment Package (Linux 64-bit) cisco-secure-client-linux64-5.0.01242-webdeploy-k9.pkg Advisories	1	
AnyConnect Pre-Deployment Package (Mac OS) cisco-secure-client-macos-5.0.01242-predeploy-k9.dmg Advisories	1	

Cisco Secure Client-AnyConnect

Cisco Systems, Inc.

About this app

Formerly AnyConnect

COMPATIBLE DEVICES:
Android 4.X+

KNOWN ISSUES:...

Updated on
Aug 19, 2022

Cisco Secure Client
AnyConnect VPN
★★★★☆ 1.6K
OPEN

Cisco Security Connector
Business
★★★☆☆ 25

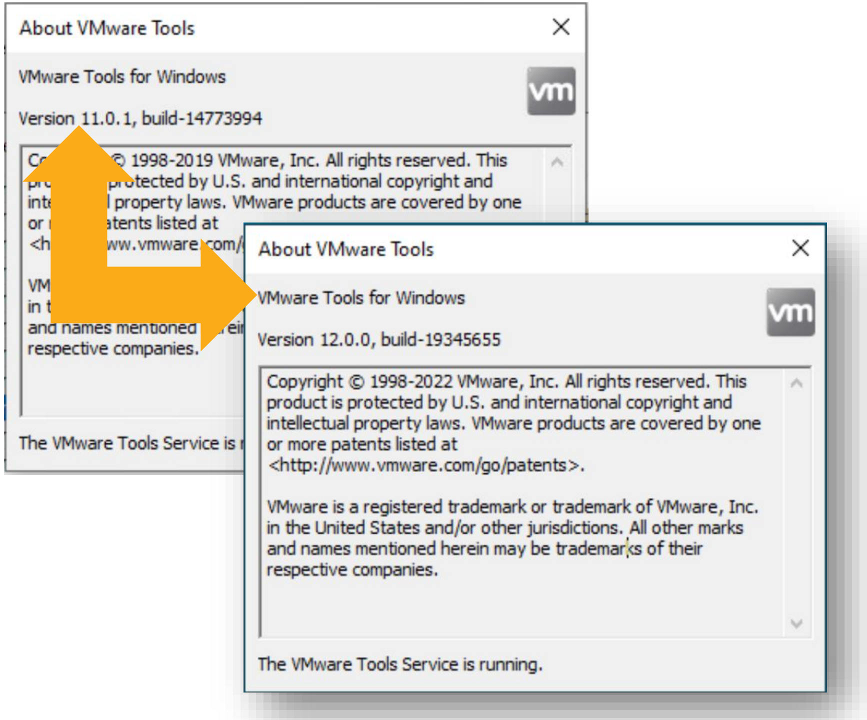
Frequently Asked Questions

- Traditional AnyConnect modules are still version locked together
- Duo is not in CSC yet
- macOS in Beta ~March 2024
- 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



About VMware Tools

VMware Tools for Windows

Version 11.0.1, build-14773994

C… © 1998-2019 VMware, Inc. All rights reserved. This pr… protected by U.S. and international copyright and inte… property laws. VMware products are covered by one or … atents listed at <h… ww.vmware.com/…

VM… in t… and names mentioned …ein… respective companies.

The VMware Tools Service is r…

About VMware Tools

VMware Tools for Windows

Version 12.0.0, build-19345655

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

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

The VMware Tools Service is running.

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

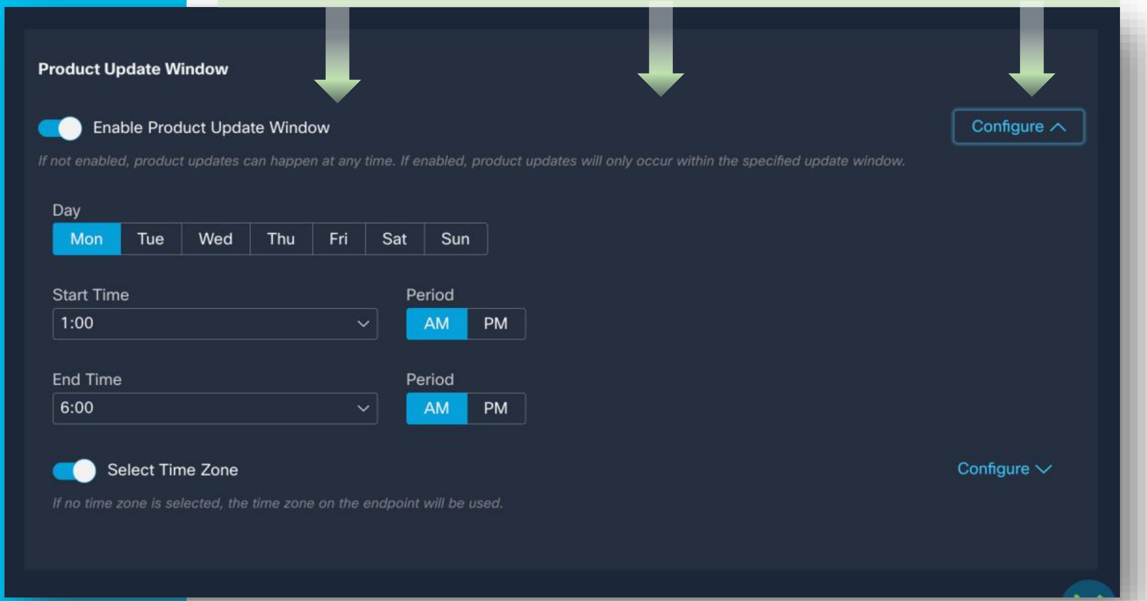
CLI Install w/ a –q option

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



Product Update Window

Enable Product Update Window (enabled)

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

Day: Mon

Start Time: 1:00

Period: AM

End Time: 6:00

Period: AM

Select Time Zone (enabled)

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

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

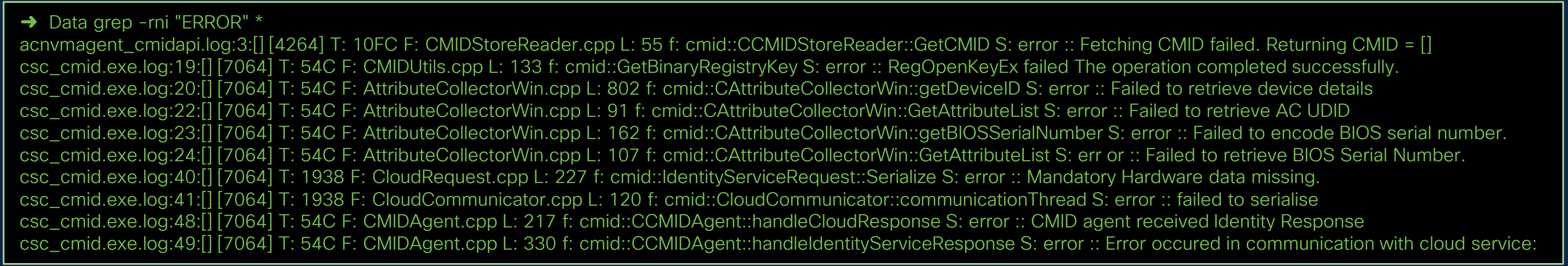
Example Issue: Virtual Machines

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_cmidapi.log:3:[] [4264] T: 10FC F: CMIDStoreReader.cpp L: 55 f: cmid::CCMIDStoreReader::GetCMID S: error :: Fetching CMID failed. Returning CMID = []
csc_cmid.exe.log:19:[] [7064] T: 54C F: CMIDUtils.cpp L: 133 f: cmid::GetBinaryRegistryKey S: error :: RegOpenKeyEx failed The operation completed successfully.
csc_cmid.exe.log:20:[] [7064] T: 54C F: AttributeCollectorWin.cpp L: 802 f: cmid::CAttributeCollectorWin::getDeviceID S: error :: Failed to retrieve device details
csc_cmid.exe.log:22:[] [7064] T: 54C F: AttributeCollectorWin.cpp L: 91 f: cmid::CAttributeCollectorWin::GetAttributeList S: error :: Failed to retrieve AC UDID
csc_cmid.exe.log:23:[] [7064] T: 54C F: AttributeCollectorWin.cpp L: 162 f: cmid::CAttributeCollectorWin::getBIOSSerialNumber S: error :: Failed to encode BIOS serial number.
csc_cmid.exe.log:24:[] [7064] T: 54C F: AttributeCollectorWin.cpp L: 107 f: cmid::CAttributeCollectorWin::GetAttributeList S: err or :: Failed to retrieve BIOS Serial Number.
csc_cmid.exe.log:40:[] [7064] T: 1938 F: CloudRequest.cpp L: 227 f: cmid::IdentityServiceRequest::Serialize S: error :: Mandatory Hardware data missing.
csc_cmid.exe.log:41:[] [7064] T: 1938 F: CloudCommunicator.cpp L: 120 f: cmid::CloudCommunicator::communicationThread S: error :: failed to serialise
csc_cmid.exe.log:48:[] [7064] T: 54C F: CMIDAgent.cpp L: 217 f: cmid::CCMIDAgent::handleCloudResponse S: error :: CMID agent received Identity Response
csc_cmid.exe.log:49:[] [7064] T: 54C F: CMIDAgent.cpp L: 330 f: cmid::CCMIDAgent::handleIdentityServiceResponse S: error :: Error occured in communication with cloud service:
```

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

QEMU & KVM Hypervisors

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

```
<sysinfo type='smbios'>
    <bios>
      <entry name='vendor'>LENOVO</entry>
      <entry name='version'>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:

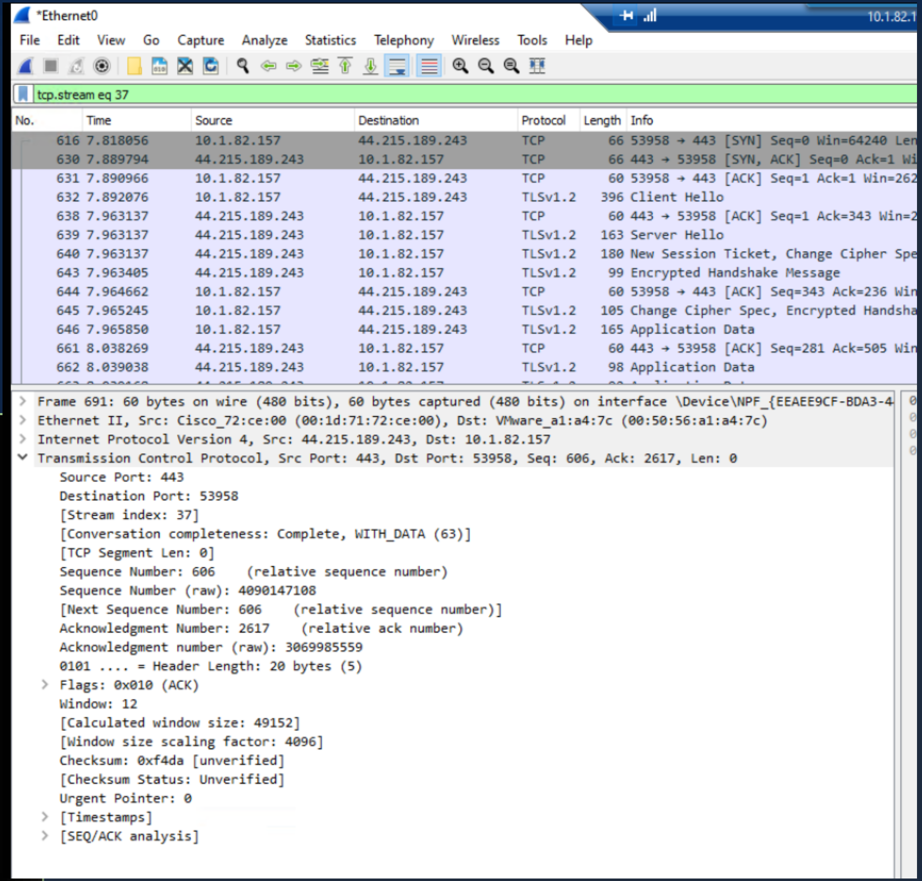
```
06/04/2023  03:00 PM          311 NVM_BootstrapProfile.xml
06/04/2023  03:25 PM        1,019 NVM_ServiceProfile.xml
```

- 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
```



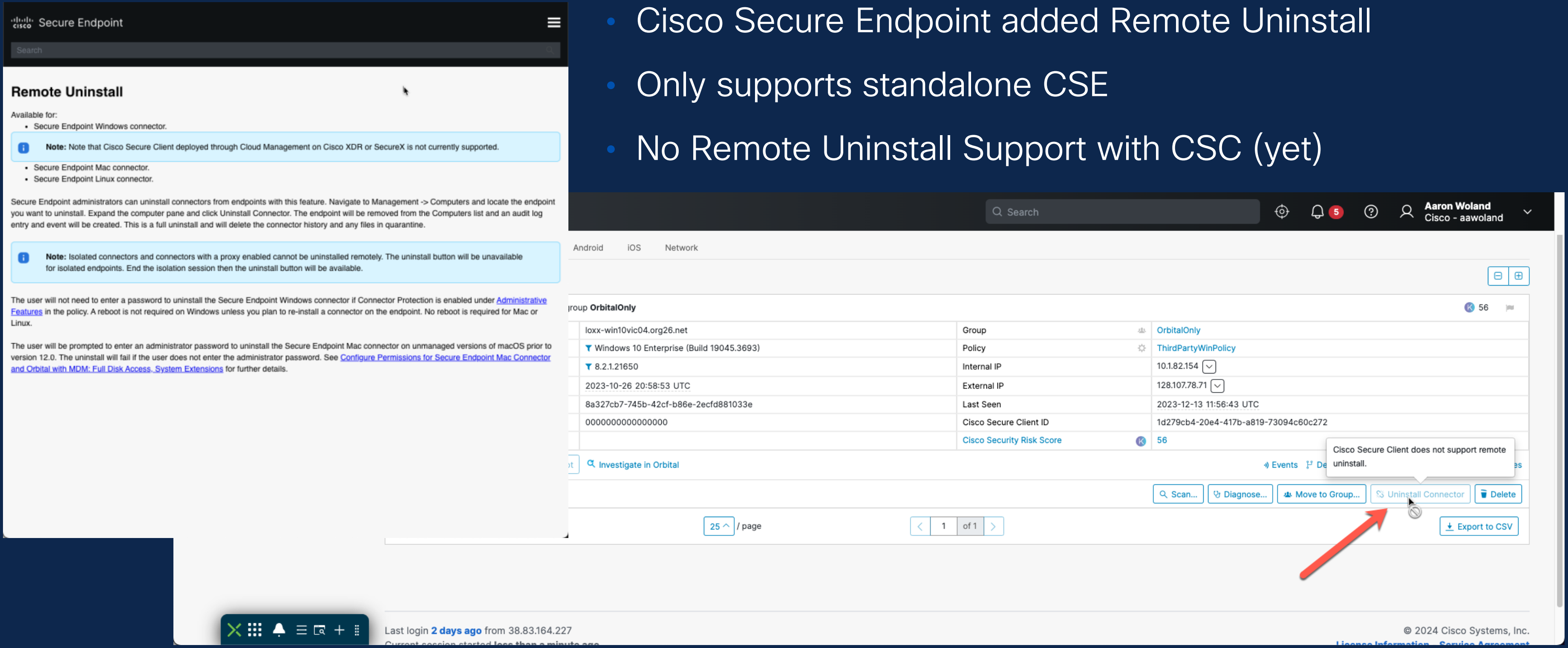
tcp.stream eq 37

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

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

Cisco Secure Endpoint 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.

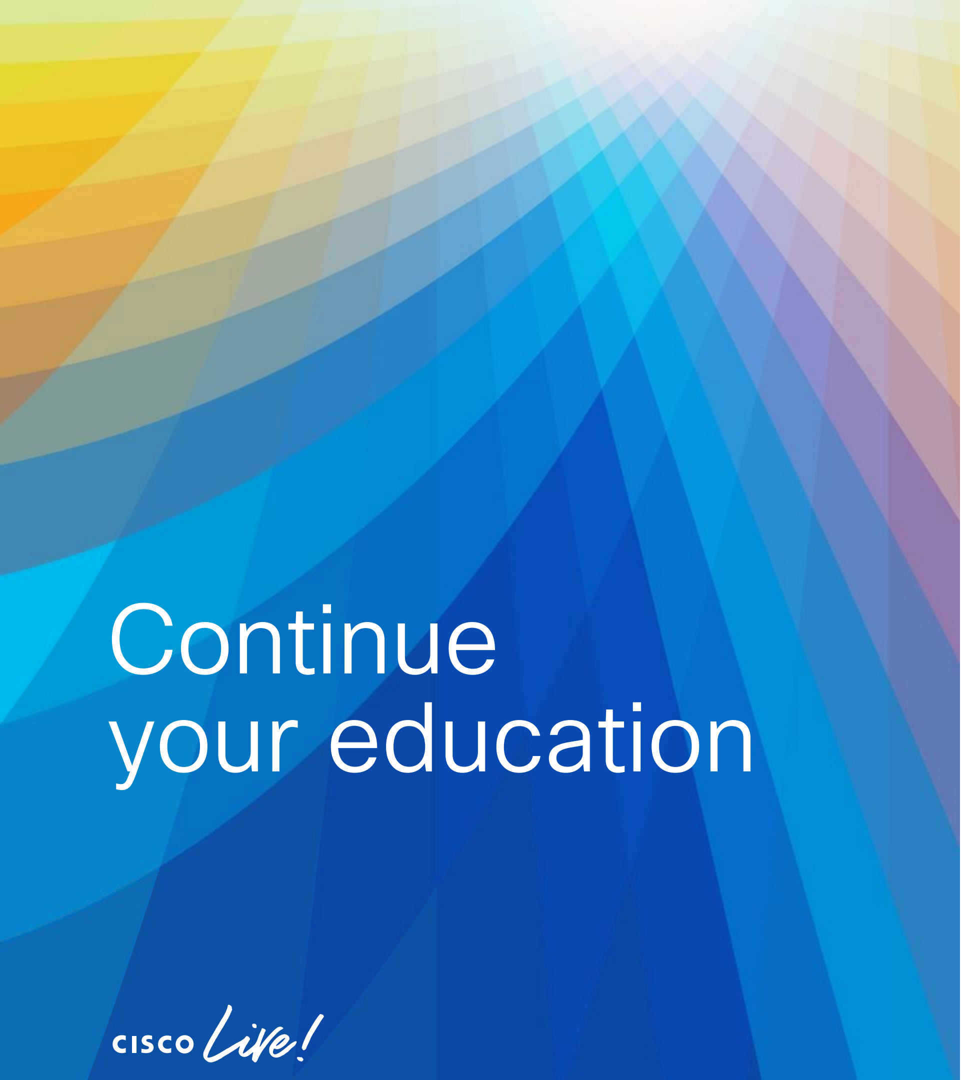
loxx-win10vic04.org26.net	Group	OrbitalOnly
Windows 10 Enterprise (Build 19045.3693)	Policy	ThirdPartyWinPolicy
8.2.1.21650	Internal IP	10.1.82.154
2023-10-26 20:58:53 UTC	External IP	128.107.78.71
8a327cb7-745b-42cf-b86e-2ecfd881033e	Last Seen	2023-12-13 11:56:43 UTC
0000000000000000	Cisco Secure Client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

Cisco Secure Client does not support remote uninstall.

Last login 2 days ago from 38.83.164.227

© 2024 Cisco Systems, Inc.

Continue your education



Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at ciscolive.com/on-demand. Sessions from this event will be available from February 23.

Other XDR sessions

Matthew Robertson

Distinguished TME

Extended Detection with Cisco XDR: Security analytics across the enterprise

BRKSEC-2178

Thursday @ 4:45 PM

Aaron Woland

Distinguished TME

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

BRKSEC-2834

Tuesday @ 5:00 PM

Aaron Woland

Distinguished TME

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

BRKSEC-2113

Wednesday @ 10:30 AM

Other Sessions

Serhii Kucherenko

Customer Escalations Engineer

Cisco Secure Client and Device Insights - better together

LABSEC-2776

Walk-in Lab

Steven Chimes

Platform Security Architect

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

BRKSEC-2079

Friday @ 11:00 AM

Radek Olszowy

Technical Consulting Engineer

Best troubleshooting practices in Secure Endpoint deployment

LABSEC-2313

Walk-in Lab

The bridge to possible

Thank you

cisco Live!

Let’s go