



Threat, Detection
& Response

 **SECURE**

Cisco Secure Client

Cisco Secures Unified Security Agent

Jiří Tesař, CCIE #14558, jitesar@cisco.com

Technical Solution Architect - Security

20.9.2022

Agenda



- ▶ CSC Overview
- ▶ CSC Architecture
- ▶ Deploying / Managing CSC
- ▶ Upgrading to CSC
- ▶ FAQs
- ▶ Secure Connect

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*

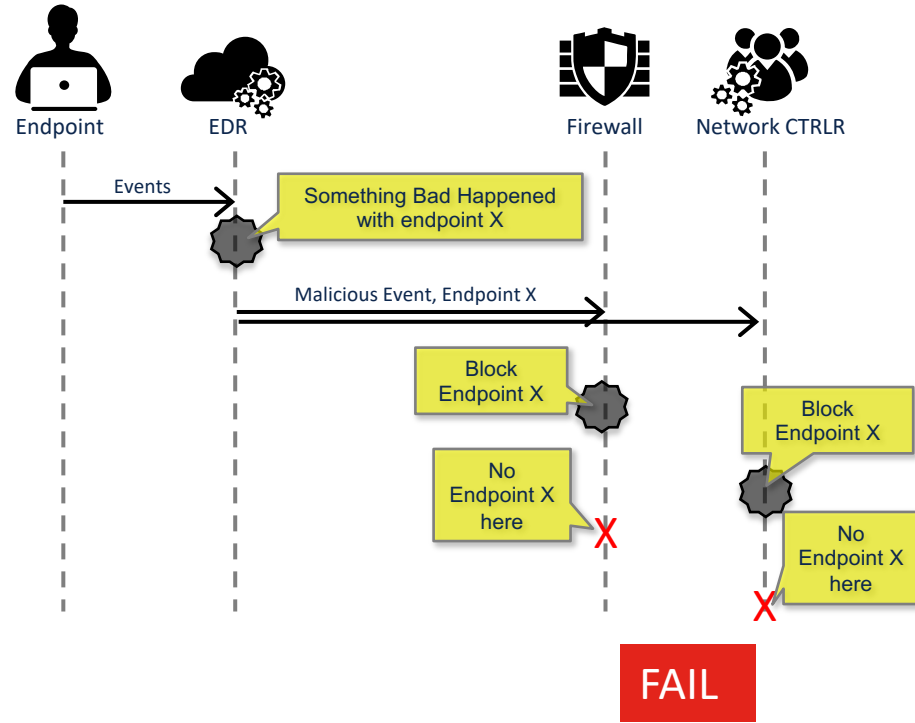
“You cannot put another agent
on our endpoints unless it replaces
two”



-Chris H., CISO Global Bank

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. SecureX 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 release is Windows (64-bit) only
- Seamless upgrade to new unified agent from existing AnyConnect & Secure Endpoint Clients
- Leverages Existing AnyConnect Framework
 - AC already has modules for many services
 - AC UI is starting point for new shared UI
 - Core AC services, such as trusted network detection, become available as common services for all modules
 - UI represents only installed functions
- Introduces a new Cloud Management System inside SecureX

Why AnyConnect Framework



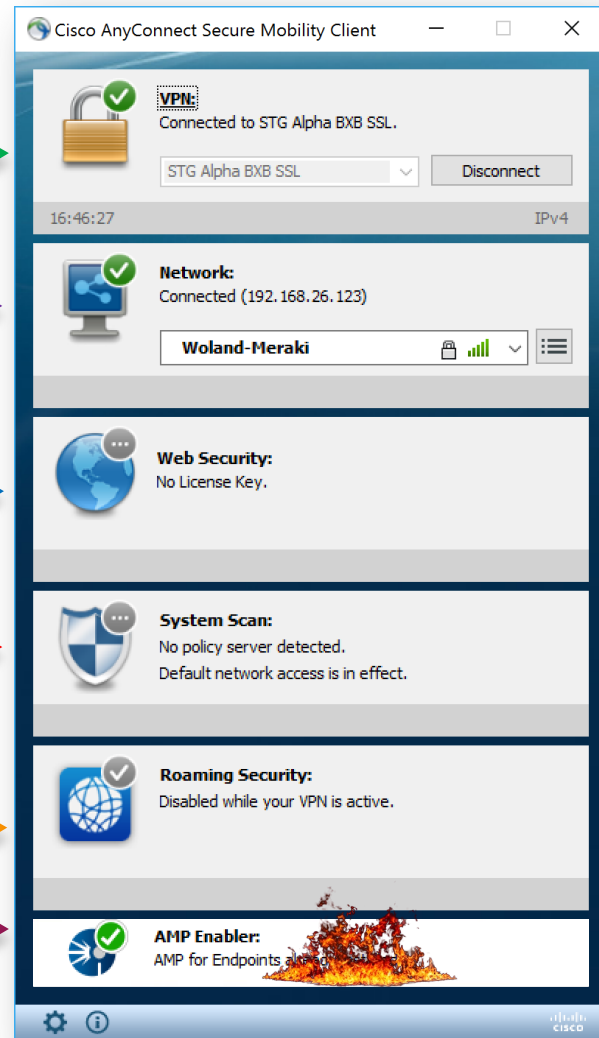
*is
more
than*



Cisco AnyConnect

suite of security service enablement modules

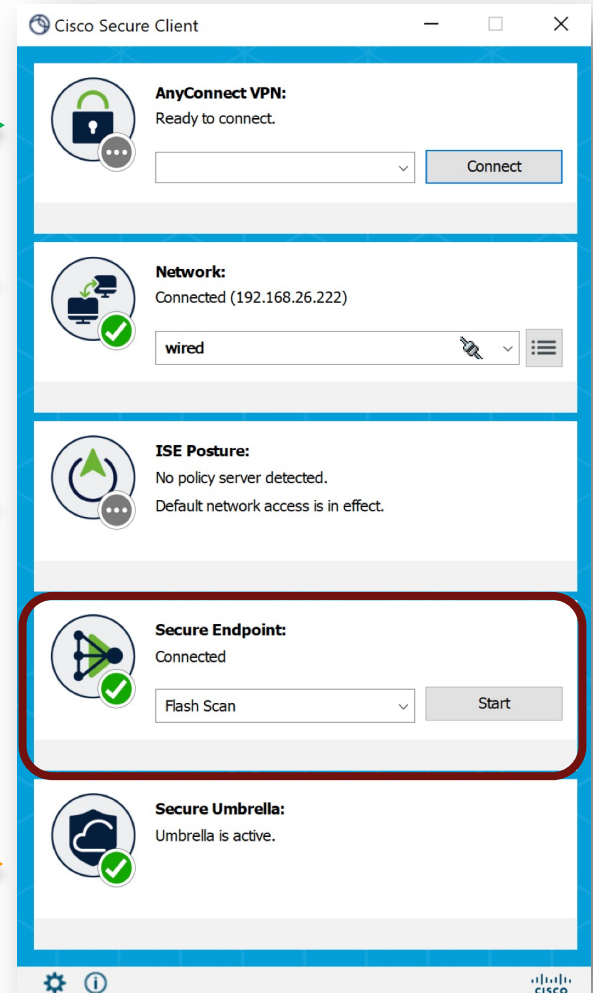
- VPN Module (Core)
- Network Access Manager (NAM)
- ~~Web Security (CWS)~~
- Posture
- Umbrella Module
- HostScan (aka: ASA posture) (No UI)
- Network Visibility Module (NVM) (No UI)
- ~~AMP Enabler Module~~
- Diagnostics and Reporting Tool (DART)



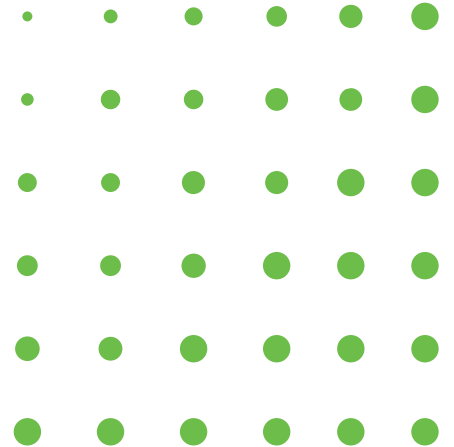
Cisco Secure Client

suite of security service enablement modules

- AnyConnect VPN (Core)
- Network Access Manager (NAM)
- ISE Posture
- HostScan (aka: ASA posture) (No UI)
- Secure Endpoint (AMP)
- Umbrella Module
- Cloud Management Module (No UI)
- Network Visibility Module (NVM) (No UI)
- Diagnostics and Reporting Tool (DART)

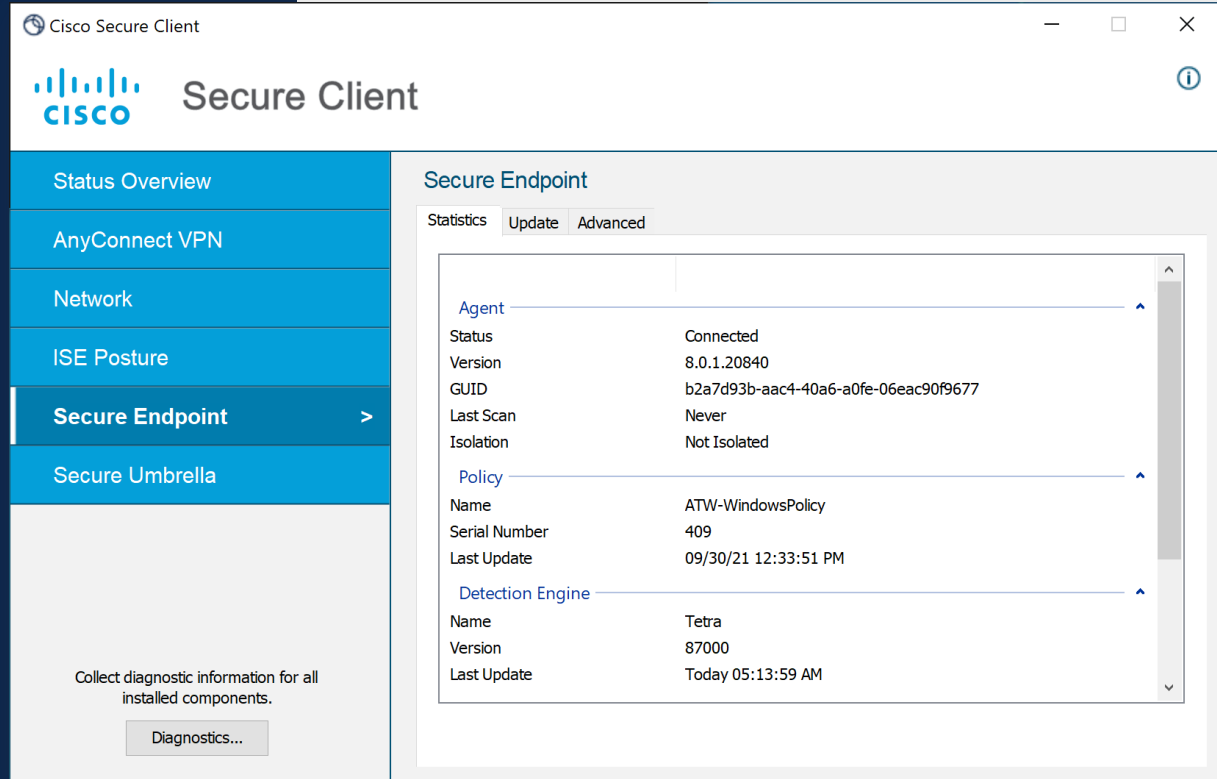


Demo: Secure Client UI on Windows



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 features the Cisco logo and the text "Secure Client". A left-hand navigation pane contains several menu items: "Status Overview", "AnyConnect VPN", "Network", "ISE Posture", "Secure Endpoint" (which is highlighted with a right-pointing arrow), and "Secure Umbrella". Below this pane, a message states "Collect diagnostic information for all installed components." with a "Diagnostics..." button.

The main content area is titled "Secure Endpoint" and has three tabs: "Statistics" (selected), "Update", and "Advanced". The "Statistics" tab displays the following information:

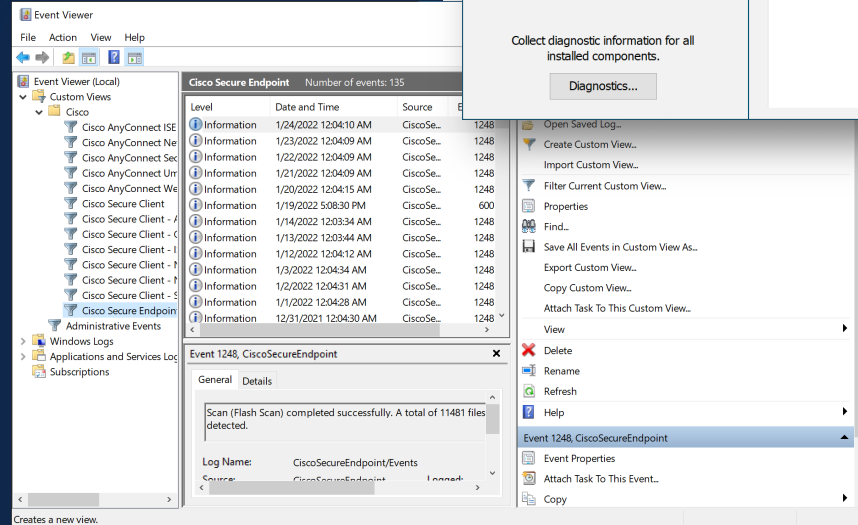
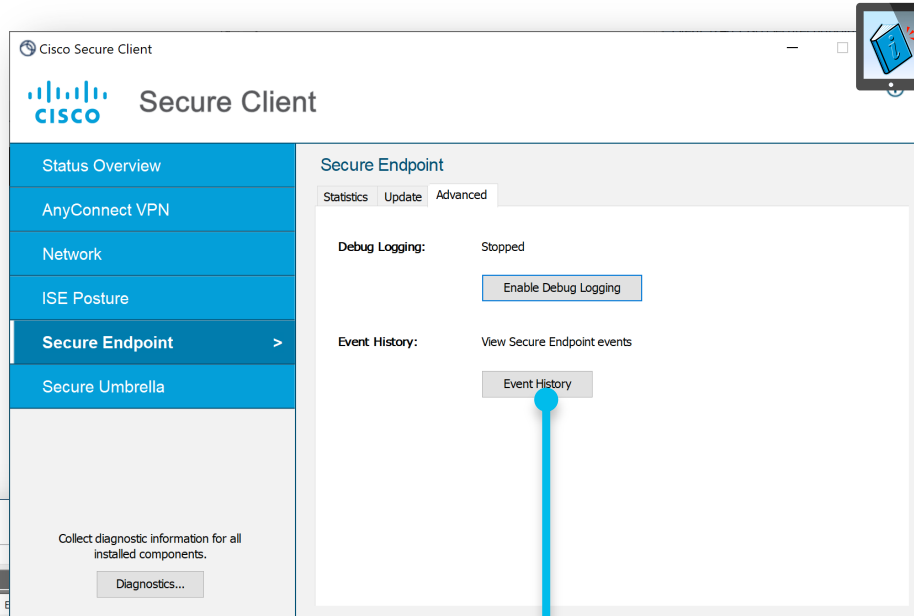
Agent	
Status	Connected
Version	8.0.1.20840
GUID	b2a7d93b-aac4-40a6-a0fe-06eac90f9677
Last Scan	Never
Isolation	Not Isolated

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

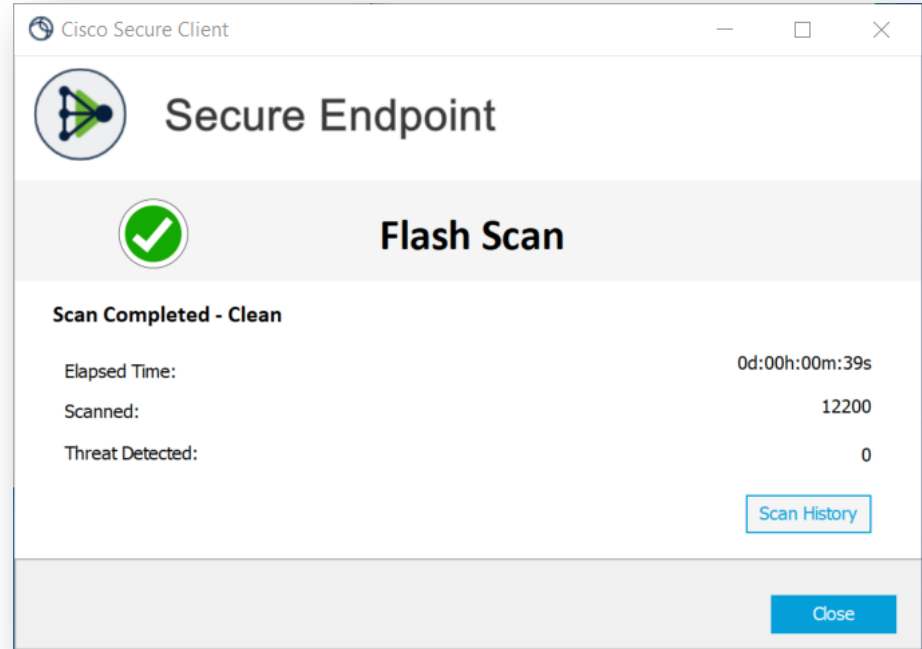
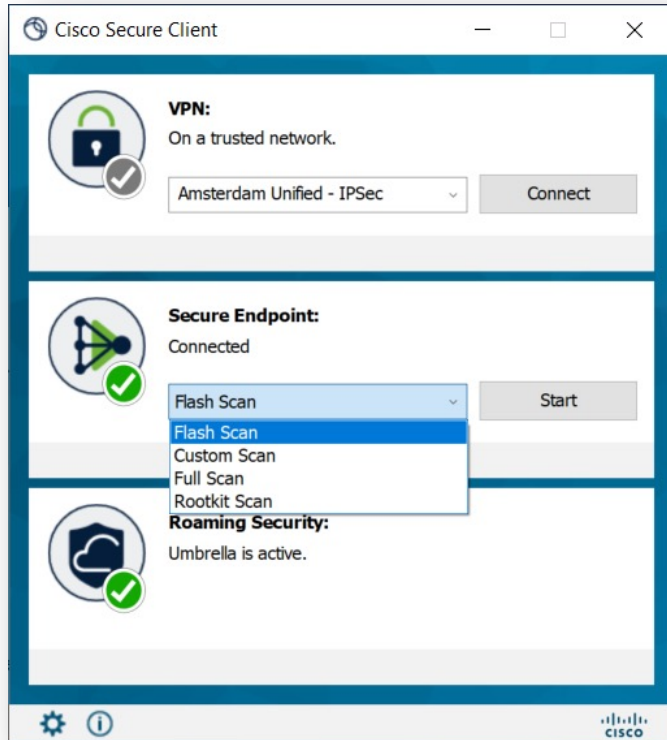
Detection Engine	
Name	Tetra
Version	87000
Last Update	Today 05:13:59 AM

Secure Endpoint Advanced

- Scan History moved to Advanced Tab

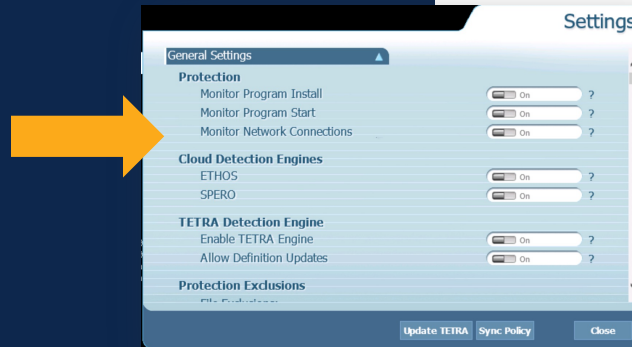
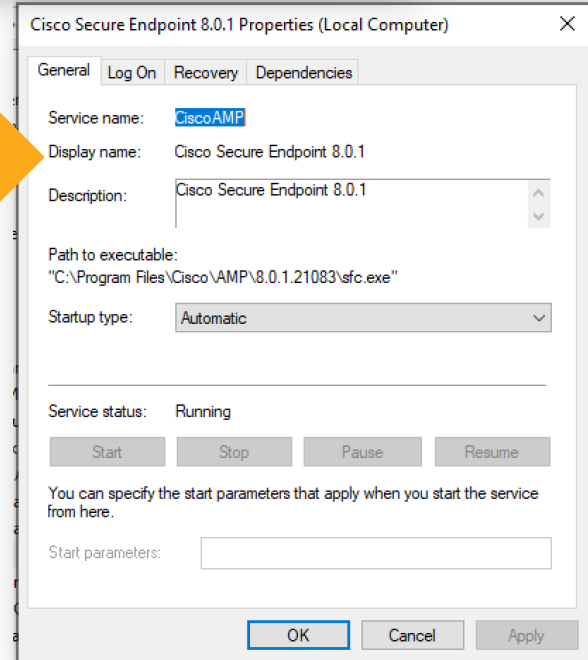
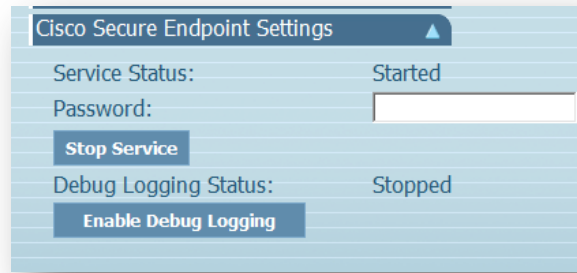


More Secure Endpoint UI



More Secure Endpoint UI

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



Secure Umbrella

Same Umbrella Roaming
from AnyConnect:

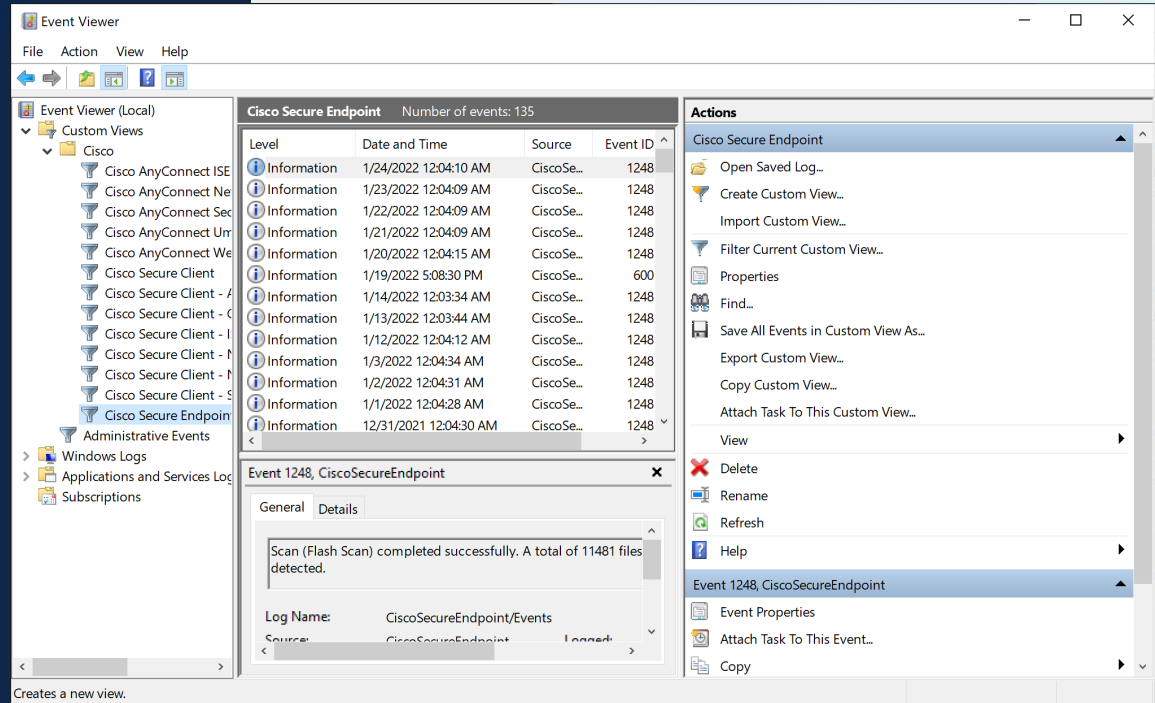
- Umbrella DNS
- Secure Web Gateway

The image displays two screenshots of the Cisco Secure Client interface. The left screenshot shows the main dashboard with four sections: AnyConnect (Ready to connect), System (No policy server detected), Secure (Connected), and Roaming Security (Umbrella is active). The Roaming Security section is highlighted with a yellow box. The right screenshot shows the 'Roaming Security' settings page with a sidebar menu. The 'Roaming Security' menu item is highlighted in a yellow box. The main content area shows 'DNS/IP Security Information' expanded, displaying the following details:

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

Secure Client Events / Logs

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



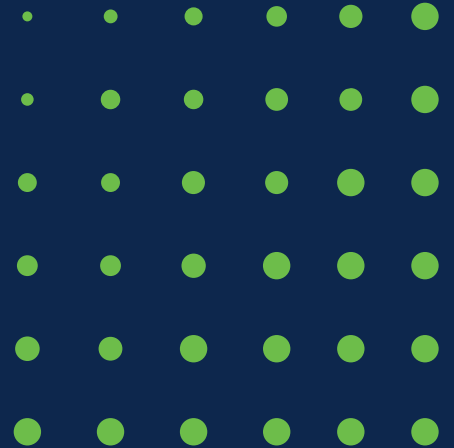
Putting it Simply

- 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 CSC
- ▶ Upgrading to CSC
- ▶ FAQs
- ▶ Secure Connect

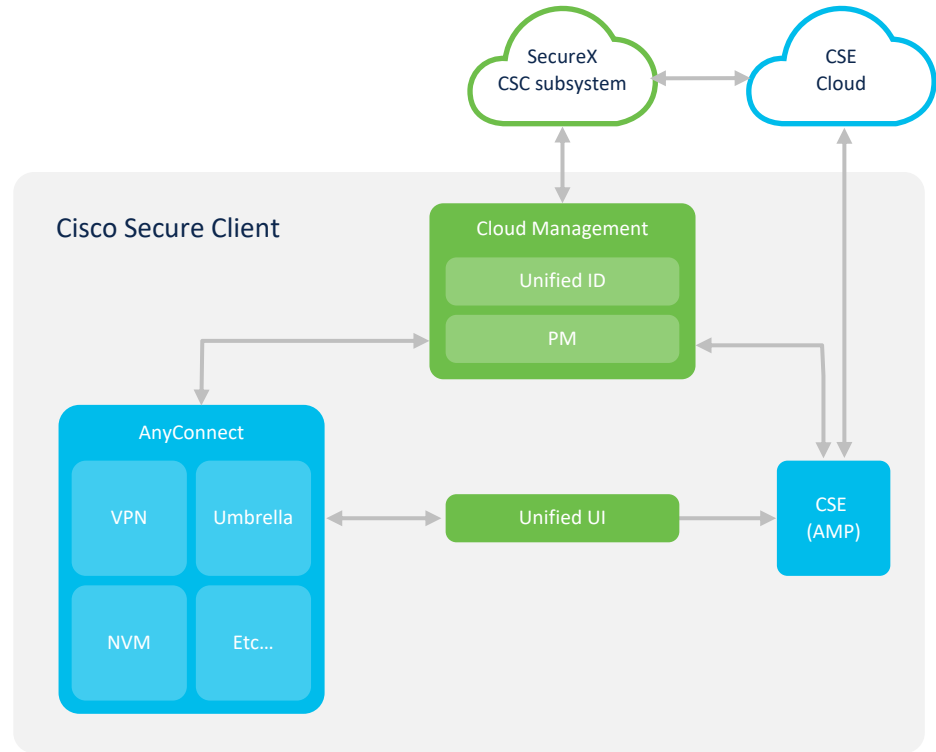
Cisco Secure Client

Architectural Overview

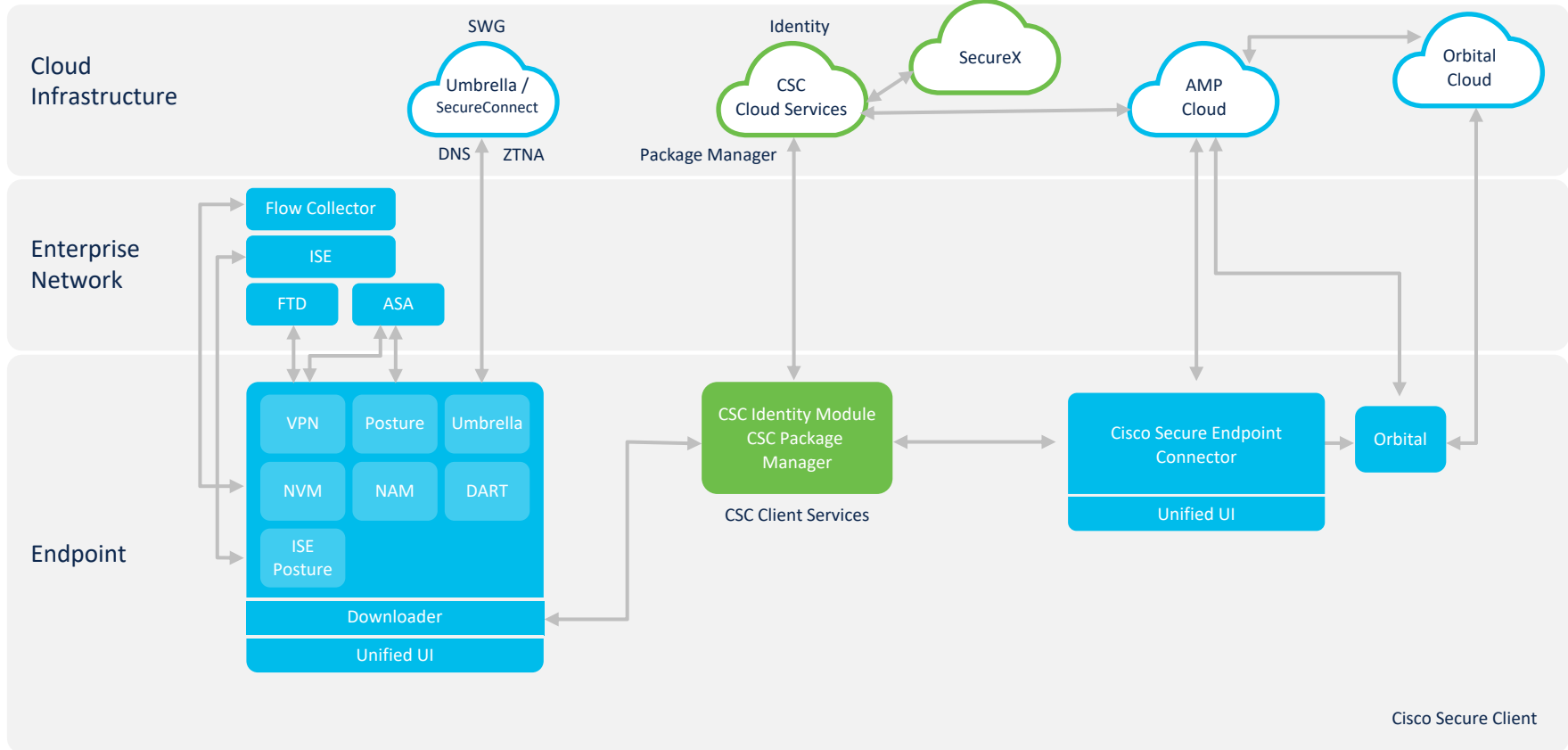
▶ Existing components that are not fundamentally changing

▶ New components

▶ Components that form the Cisco Secure Client

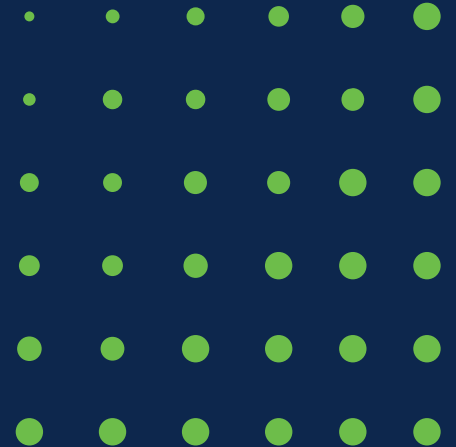


Cisco Secure Client – Architecture



Cisco Secure Client

Deploying / Managing CSC



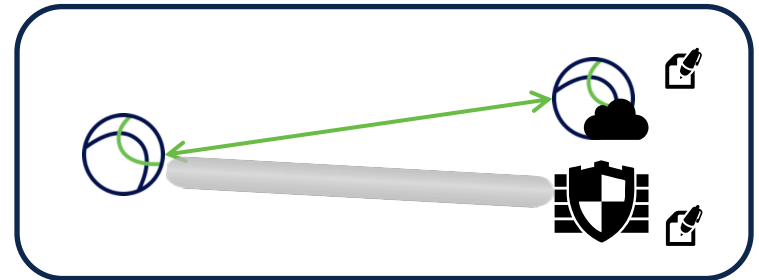
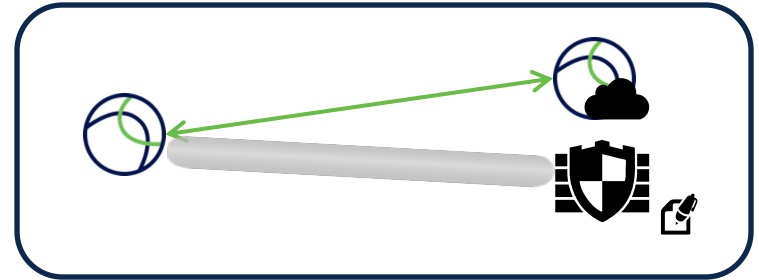
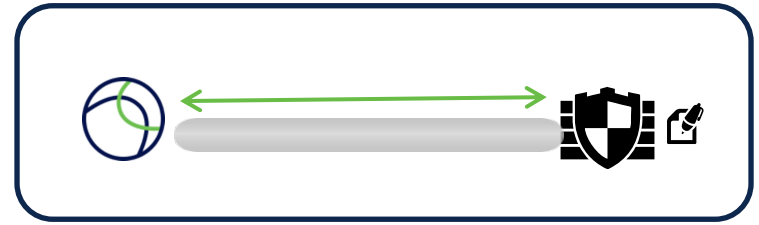
Agenda



- ▶ CSC Overview
- ▶ CSC Architecture
- ▶ Deploying / Managing CSC
- ▶ Upgrading to CSC
- ▶ FAQs
- ▶ Secure Connect

Deployment Models

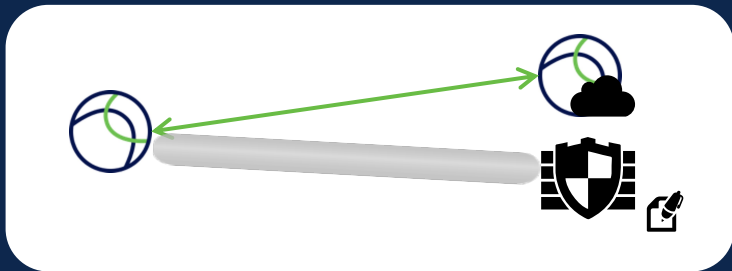
- No Cloud Management
- Cloud Registration – no Package Management
- **Cloud Registration – Full Management**





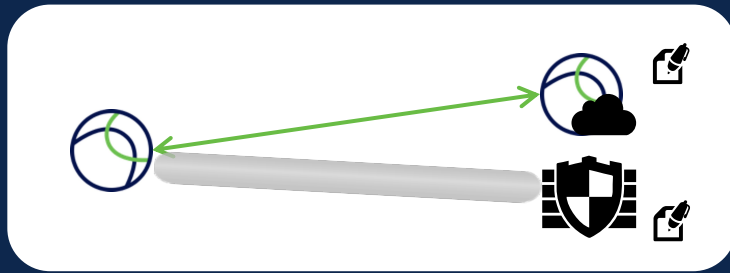
No Cloud Management

- No Cloud Management Module
 - For customers who are used to running AnyConnect & want to keep same practices
 - Must download software from CCO (and/or Secure Endpoint Portal), not from SecureX (all installers from SecureX include the CM module)



Cloud Registration w/o Package Management

- Use CM for inventory, but not for package delivery/management
 - Customer wants/needs the UID; especially important for XDR use-cases
 - Create a Deployment with only CM module defined
 - The rest of the software comes from the CCO downloaded pkg's hosted on the ASA or ISE, SE Cloud, etc.



Full Cloud- Management

- Using either the network or full installer for the endpoints.
- CM Module handles package management and the cloud identity.
- Allows for Cloud Configuration of profiles & module management

Enable Secure Client Management

- Currently within Device Insights
 - Click **Enable**
 - This starts the process of spinning up your CSC Sub-system
- CSC entitles a customer to SecureX
 - Flow will allow CSC to bring SecureX into a full-enabled state
 - Future version will do more to enforce entitlement

The screenshot shows the Cisco SecureX web interface. The top navigation bar includes 'Dashboard', 'Integration Modules', 'Orchestration', 'Insights', and 'Administration'. The left sidebar contains a menu with items: 'Device Insights', 'Inventory Overview', 'Sources', 'Source Settings', 'Secure Client', 'Deployment Management' (highlighted in blue), 'Audit Logs', 'Profiles', and 'Device Events'. The main content area is titled 'Secure Client' and contains the text 'Secure VPN Access for Remote Workers' and a paragraph: 'Cisco Secure Client bundles the Cisco Security suite of products to your Windows 10 devices so that installation on the endpoint is simpler. With a centralized management interface upgrades across all our endpoint products are a breeze.' Below this text is a blue 'Enable' button. A green callout box points to the 'Enable' button with the text: 'Clicking this IS what triggers the creation of the CSC Tenant'.

Managed from SecureX Cloud UI

Deployments

- Groups of endpoints to get specific modules + configs
- “Groups” are coming in future version & can assign entire groups to a Deployment



The screenshot displays the Cisco SecureX Cloud UI for Deployment Management. The interface is organized into several sections:

- Cloud Management:** A blue-bordered section containing a dropdown menu for Beta (1.0.1.389) and a Cloud Management button.
- Secure Endpoint:** A red-bordered section containing a dropdown menu for 8.0.1.21083 and a Replace Bootstrap Profile button.
- Traditional AnyConnect Modules:** A blue-bordered section containing various configuration options such as AnyConnect VPN, Start Before Logon, Umbrella, and Network Access Manager.

The interface also includes a search bar, a list of deployment types (ATW-Deployment, PGC-Deployment, Server-Deployment), and a footer with the Cisco SecureX logo and navigation icons.

Managed from SecureX Cloud UI

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

Beta (1.0.1.389) **No UI**

Cloud Management ATW-CM-Config

5.0.529.0

AnyConnect VPN ATW-CEF-Profile Start Before Logon

SecDemo-VPN View ATW-CEF-Profile View

Diagnostics and Reporting Tool

Secure Firewall Posture **No UI**

Network Visibility Module ATW-NVM_Configuration

8.0.1.21083

Secure Endpoint ATW-Production [Replace Bootstrap Profile](#)

Umbrella SBG-Umbrella

ISE Posture ATW-ISE

Network Access Manager

Cisco Secure Client

AnyConnect VPN:
Ready to connect.
 [Connect](#)

Network:
Connected (192.168.26.222)
wired [Settings](#)

ISE Posture:
No policy server detected.
Default network access is in effect.

Secure Endpoint:
Connected
Flash Scan [Start](#)

Secure Umbrella:
Umbrella is active.

Managed from SecureX Cloud UI

- Profiles
 - Cloud Management (UC) module
 - Includes package manager
 - Check-in timer
 - Update Window:
 - *Also leveraged for **Installation Window for Network Installer***
 - If CM checks in with the cloud within that time window, the updates will be pushed to the endpoint
 - CM has no idea what this window is, it's all controlled at the cloud

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

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
Debug

Product Update Window

Enable Product Update Window [Configure](#)

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

Day
Mon Tue Wed Thu Fri Sat Sun

Start Time
1:00

Period
AM PM

End Time
11:00

Period
AM PM

Select Time Zone [Configure](#)

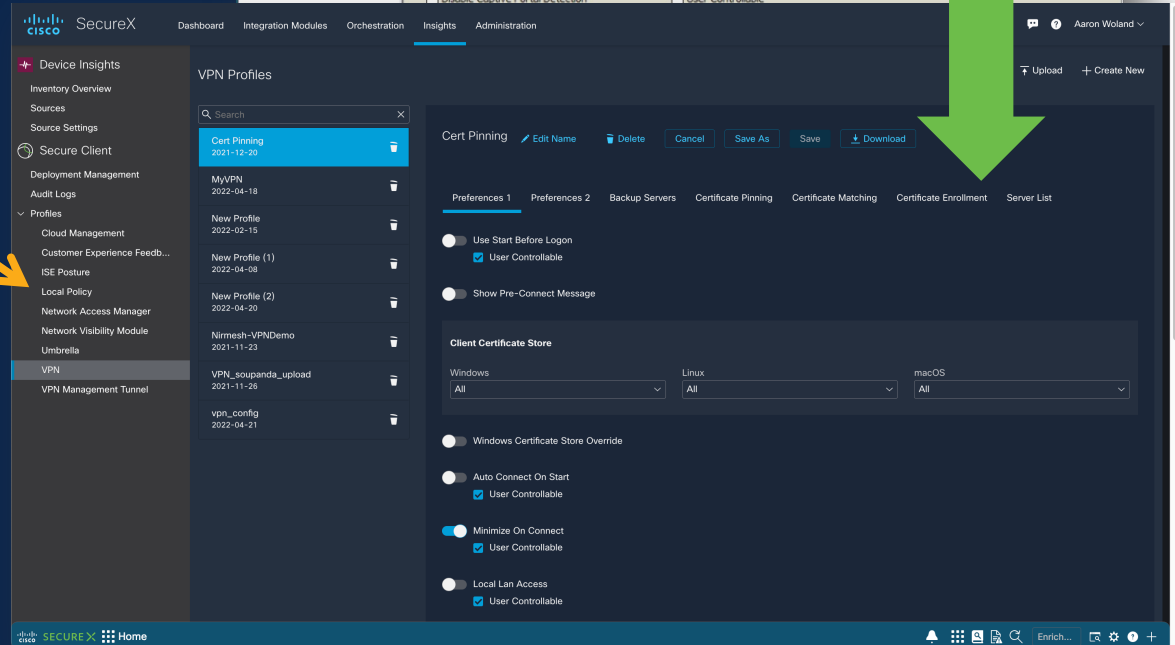
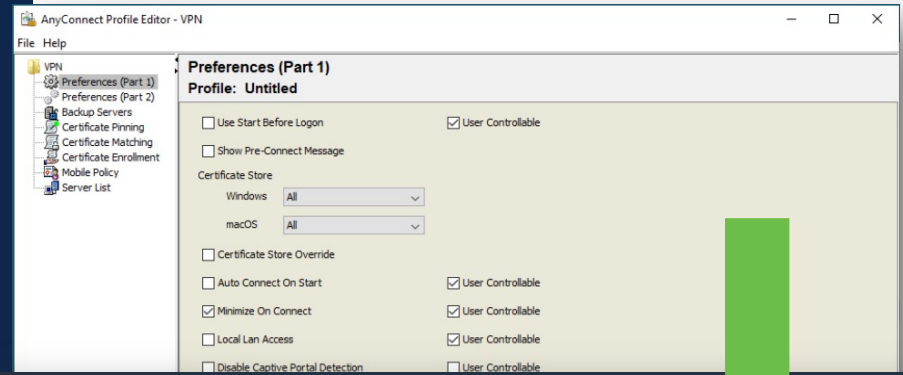
If no time zone is selected, the time zone on the endpoint will be used.

Managed from SecureX Cloud UI

- Profiles

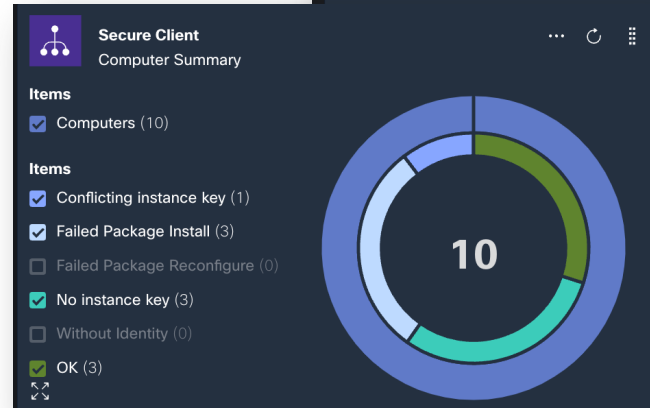
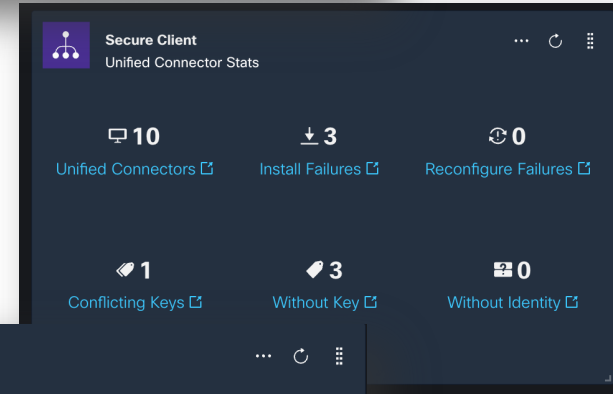
- Each module has a profile for its “configuration”

- Used to be standalone Windows-only configuration tool



SecureX Dashboards

- Two dashlets that exist today
- The links will bring the admin to pre-filtered SxDI inventory page



Inventory is part of Device Insights

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

The screenshot displays the Cisco Secure Client (CSC) inventory management interface. At the top, there are tabs for 'All Devices' and 'Secure Client Devices', with an orange arrow pointing to the latter. The dashboard features several summary cards: '5 Devices', '0/5 Devices Not Seen In Over 7 Days', '4 Devices Need Connector Update', '5 Windows 10 / 0 Windows 11', a 'Types' donut chart showing 0 Server, 4 Desktop, 1 Virtual, and 0 Mobile devices, and '3 Deployments'. Below these are search and filter options, including 'Basic Search', 'Text Search', 'Managed Status', 'Operating System', 'OS Support', 'Type', 'Sources', and 'Policies'. A table at the bottom lists device details:

Device Name	Deployment	CSC Version	Secure Endpoint Version	Cloud Management Version	Modules	OS	OS Version	OS Support	Users Seen	Sources	Managed	Compromised
06385286146	PGC-Deployment	5.0.00117	8.0.1.20940	1.0.1.331	Cloud Management v.1.0.1.331 Cisco Secure Endpoint v.8.0.1.20940 AnyConnect MPN v.5.0.00117 DART v.5.0.00117	Windows	10 Pro			Secure Endpoint - Cisco - aawoland Orbital Secure Client	No	
loxx-surfacepro	ATW-Deployment	5.0.00117	8.0.1.20940	1.0.1.353	Cloud Management v.1.0.1.353 Cisco Secure Endpoint v.8.0.1.20940 AnyConnect VPN v.5.0.00117 Umbrella v.5.0.00117 DART v.5.0.00117 ISE Posture v.5.0.00117 Secure Firewall Posture v.5.0.00117 Network Visibility Module v.5.0.00117 Cloud Management v.1.0.1.389	Windows	10.0	loxx, loxx-surfacepro/Aaron, loxx@securitydemo.net, Aaron, eden, nyah	Umbrella PosaaS SBG SM Duo Secure Endpoint - Cisco - aawoland Orbital Secure Client	Yes		

Quick SxDI review

- Combines all the known attributes from integrated sources into a common endpoint DB
- Not only Secure Client



Duo Access
Duo Beyond



Secure Endpoint



Umbrella (DNS)
Win / macOS only



Meraki SM



Secure Client



Orbital

3rd Party MDMs



Microsoft Intune



Mobile Iron



Airwatch



Custom CSVs



Jamf Pro

All the Normal DI Searches are Usable

- String Searches
- Management:
 - By DM, NOT CSC
- OS Support
- Type:
 - Server, Desktop, etc.
- Other sources
- CSC Specific

The screenshot shows the Cisco Secure Management Center interface. At the top, there are several search and filter controls: Text Search (Surface), Managed Status (Select), Operating System (1 Selected), OS Support (Select), Type (Select), and Sources (1 Selected). Below these are checkboxes for 'Not Seen In Over 7 Days (0)', 'Need Connector Update (0)', 'Has Faults (0)', and 'AV Definitions out of date (0)'. There are also buttons for 'Must Include: Secure Client' and 'Windows'. The main area displays a table with 3 devices found out of 7. The table has columns for Device Name, Deployment, CSC Version, Secure Endpoint Version, Cloud Management Version, Modules, OS, Sources, OS Version, and OS Support. The devices listed are ATW-SurfacePro4, ATWSTUDIO, and loxx-surfacepro.


Device Name	Deployment	CSC Version	Secure Endpoint Version	Cloud Management Version	Modules	OS	Sources	OS Version	OS Support
ATW-SurfacePro4	ATW-Deployment	5.0.00529	8.0.1.21083	1.0.1.389	Cloud Management v.1.0.1.389 Cisco Secure Endpoint v.8.0.1.21083 AnyConnect VPN v.5.0.00529 Umbrella v.5.0.00529 DART v.5.0.00529 ISE Posture v.5.0.00529 Secure Firewall Posture v.5.0.00529 Network Visibility Module v.5.0.00529	Windows	Umbrella PosaaS SBG SM Secure Client Secure Endpoint - Cisco - aawoland Orbital	10 Enterprise	
ATWSTUDIO	ATW-Deployment	5.0.00529	8.0.1.21083	1.0.1.389	Cloud Management v.1.0.1.389 Cisco Secure Endpoint v.8.0.1.21083 AnyConnect VPN v.5.0.00529 Umbrella v.5.0.00529 DART v.5.0.00529 ISE Posture v.5.0.00529 Secure Firewall Posture v.5.0.00529 Network Visibility Module v.5.0.00529	Windows	Duo Umbrella PosaaS SBG SM Secure Endpoint - Cisco - aawoland Orbital Secure Client	10 Pro (64-bit)	
loxx-surfacepro	ATW-Deployment	5.0.00529	8.0.1.21083	1.0.1.389	Cloud Management v.1.0.1.389 Cisco Secure Endpoint v.8.0.1.21083 AnyConnect VPN v.5.0.00529 Umbrella v.5.0.00529 DART v.5.0.00529 ISE Posture v.5.0.00529 Secure Firewall Posture v.5.0.00529 Network Visibility Module v.5.0.00529	Windows	Umbrella PosaaS SBG SM Duo Secure Endpoint - Cisco - aawoland Orbital Secure Client	Microsoft Windows 11 Pro Insider Preview 10.0.25120	

CSC Specific Filters

- Deployment
- Not Seen in Over 7 Days
- Need Connector Update

The screenshot shows a dark-themed interface with several filter sections:

- Text Search:** A search box containing the text "Surface" with a clear button (X).
- Managed Status:** A dropdown menu with "Select" as the current selection.
- Operating System:** A dropdown menu with "1 Selected" as the current selection.
- OS Support:** A dropdown menu with "Select" as the current selection.
- Policies:** A dropdown menu with "Select" as the current selection.
- Deployment Configurations:** A dropdown menu with "Select" as the current selection.
- Not Seen In Over 7 Days (0):** A checkbox filter, highlighted with a red box.
- Need Connector Update (0):** A checkbox filter, highlighted with a red box.



“Cloud management capability is a game-changer for configuration management of Secure Client on the endpoint, particularly for software updates and config file management.”

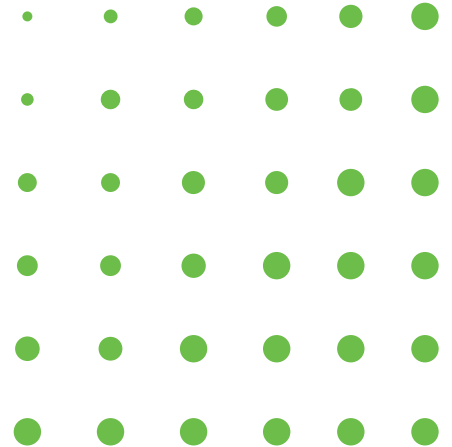
- Early Field Trial Customer

“Once complete, the product will be a huge improvement over the old way of managing SSL VPN clients.”

- Early Field Trial Customer

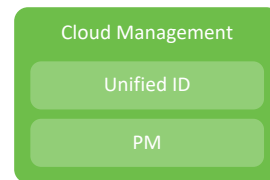
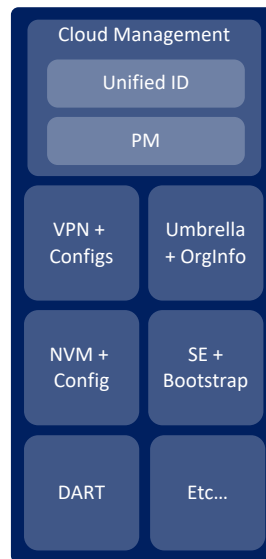
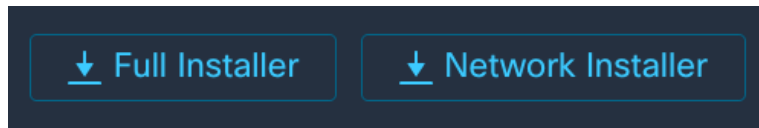


Installing Cisco Secure Client



Installing CSC

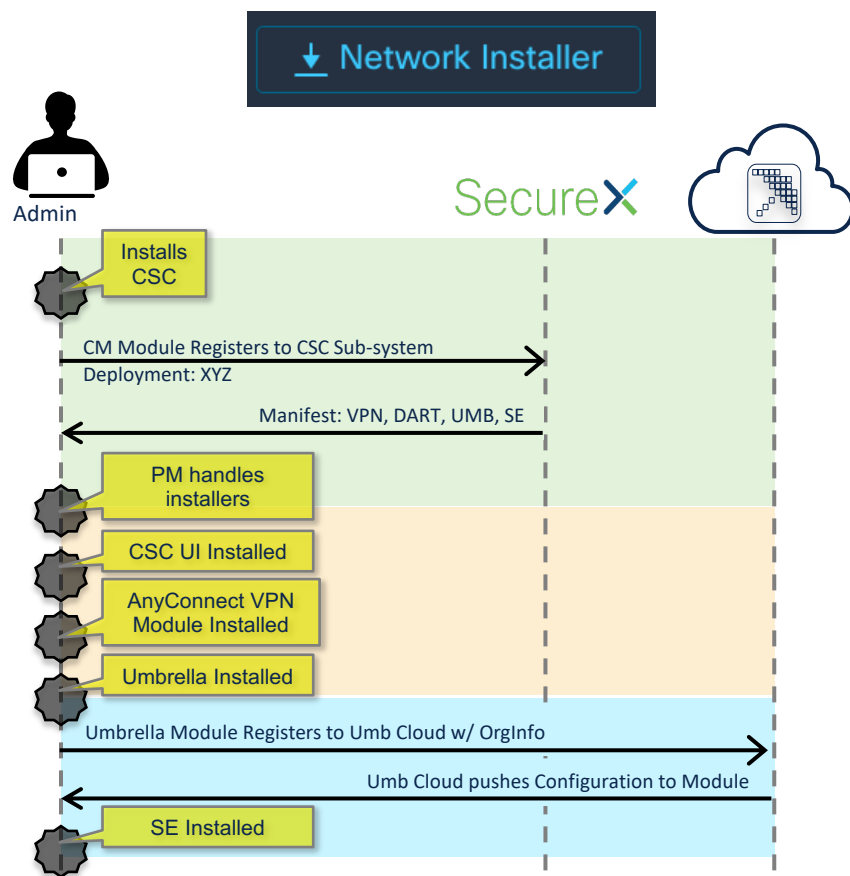
- Full Installer:
 - All selected Modules & their configurations.
- Network Installer:
 - Installs Cloud Management first, then PM pulls the manifest from deployment and installs each module and configuration one at a time.



**These installers will ALWAYS include the CM module*

Network Installer

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



Installing from a Device Manager

- Either Full or Network Installer
 - Using a Device Manager
 - Using your own endpoint software manager
 - Whatever tools your company normally uses to push out / install software

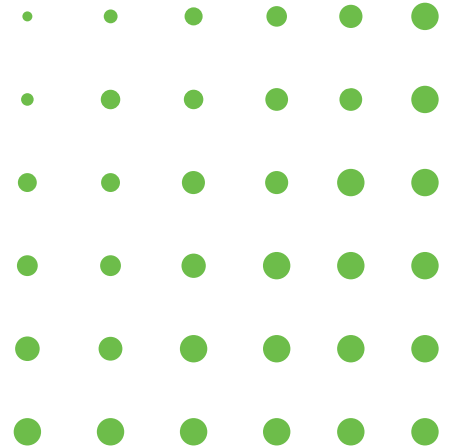
The screenshot displays the Meraki Cloud Management interface for the Cisco Secure Client - Cloud Management application. The left sidebar shows the navigation menu with 'Systems Manager' selected. The main content area is titled 'Cisco Secure Client - Cloud Management' and includes the following sections:

- Details:** Name (Cisco Secure Client - Cloud Management), Identifier (827aba60-77e2-013a-c842-6d6572616b69), and 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), and Updated at (Jun 1 2022 16:12).
- Options:** Keep app up to date (checked), Auto-install (checked), Install in foreground (checked), Installation arguments (empty field), Command line (empty field), and Visible in SSP (checked).
- Targets:** Group type (Manual, Named, Configure tags), Scope (with ANY of the following tags), and Device tags (MerakiTestCSC).

Installing CSC

- Can be installed from headend (web deploy) just like AC 4.x
 - All “AC” modules and configurations can be pushed this way
 - Not: Cloud Management or Secure Endpoint
- Umbrella will continue updating ERC & AC Module
 - CSC Umbrella Module will no longer be controlled by Umbrella

Deployments w/ Secure Endpoint and Orbital



Configuring Secure Endpoint

The screenshot shows the 'Deployment Management' interface for 'ATW-Deployment'. It includes a search bar, a list of deployment types (ATW-Deployment, PGC-Deployment, Server-Deployment), and several configuration sections. A dropdown menu is open, showing a list of SE Groups. Numbered callouts 1, 2, and 3 point to the version selection, the SE integration dropdown, and the SE group selection respectively.

Select Desired SE Version

Select your SE Integration

There *can* be more than one

Choose the SE Group

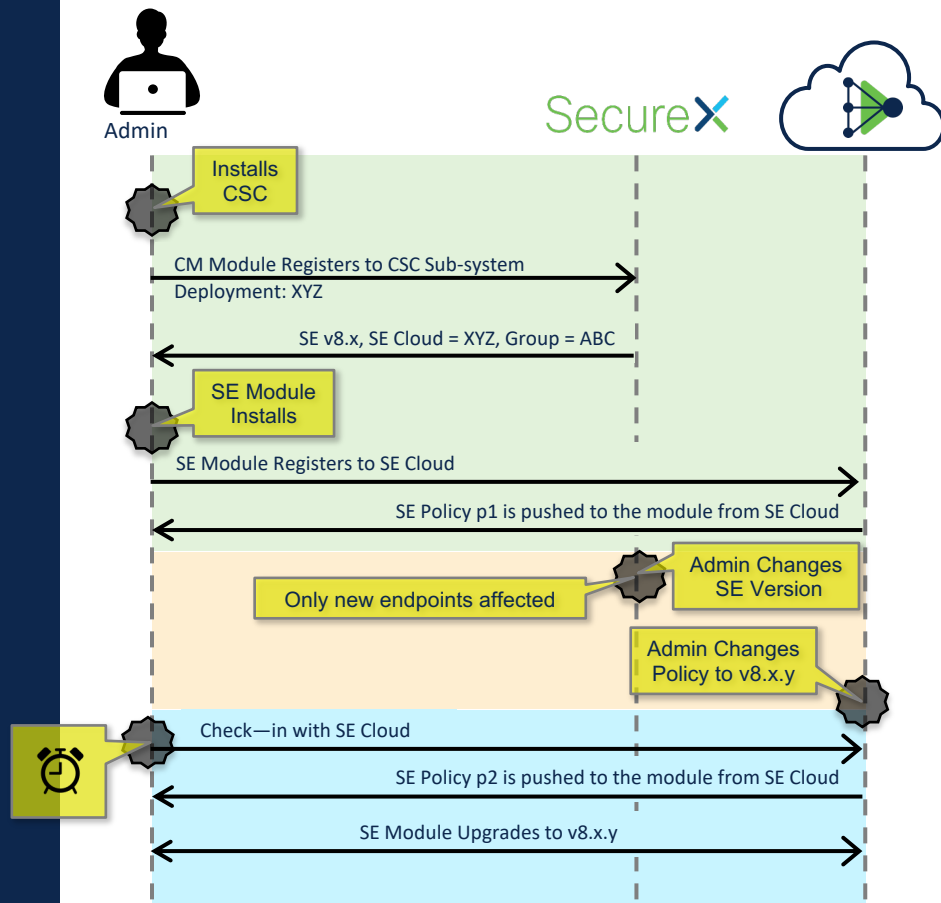
All endpoints who install the module via this deployment, will be assigned to this group, when the CSE module registers with the CSE cloud.

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

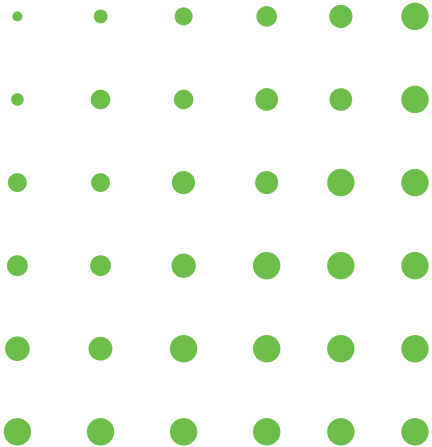
This close-up shows the 'Beta (8.0.1.21083)' version selected in a dropdown. Below it, the 'Secure Endpoint' and 'ATW-Production' integration options are visible, along with a blue 'Replace Bootstrap Profile' button.

Bootstrap?

- Secure Client's SE config is just to get the SE module to install & register to SE Cloud.
- Then: ALL control of the SE module comes from SE Cloud.
- Version updates, group changes, etc...



Secure Endpoint Cloud



SE Cloud

Management > Download Connector

Secure Endpoint Premier

Dashboard Analysis Outbreak Control Management Accounts

Download Connector Legacy Version

Select Group to Download Connector

ATW-Production

Secure Client

Cisco Secure Client bundles the Cisco Security suite of products to your Windows 10 and 11 devices so that installation on the endpoint is simpler. With a centralized management interface upgrades across all our endpoint products are a breeze.

Secure Client deployments can be configured on Deployment Management page in the SecureX console.

Manage deployment on SecureX

Windows 10 & 11

SecureX Deployment

Select a Deployment

Search

- ATW-Deployment
- NPI-Dep-1
- NPI-Dep-2
- PGC-Deployment

Show URL Download

Secure Endpoint

Windows

Connector Version: 7.4.3.20679
Policy: ATW-WindowsPolicy

- Flash Scan on Install
- Redistributable

Linux

Connector Version: 1.18.0.814
Policy: ATW-Linux-Policy

Linux Distribution

Select SE Group

Unchanged Behavior

CSC Deployments

List of CSC Deployments from SecureX Loads & one should be selected.

Download

Downloads the FULL Installer

Manage deployment in SecX

X-Launches a new tab/window – to the SecureX dashboard... It doesn't redirect to the deployment management page (yet)

SE Portal - URL

- Yes, you still have the direct URL to send out to download the installer.
- URL is for the FULL Installer

The screenshot displays the Cisco Secure Endpoint Premier web interface. The main content area is titled "Download Connectors" and includes a "Select Group to Download Connector" dropdown menu with "ATW-Production" selected. A modal window titled "Download URL" is overlaid on the page. This modal contains the text "You can email this URL to users so they can download and install the Connector" followed by a long URL: `https://cisco-ucb-nam-pass-
repo.s3.amazonaws.com/77aaa0c7976cc469a090c8de756fb6b28f864febaf688b445b6651fe4f0
deploy-ATW-Deployment.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-
Credential=ASIAUJEL5KAUXKRFQPKND%2F20220624%2Fus-east-
1%2Fs3%2Faws4_request&X-Amz-Date=20220624T035705Z&X-Amz-Expires=3600&X-
Amz-Security-Token=
Amz-
Signa`. Below the URL, the word "REDACTED" is displayed in a black box. At the bottom of the modal are "Cancel" and "Copy URL" buttons. In the background interface, a "Show URL" button is highlighted with a yellow box, and a "Download" button is visible to its right. The interface also shows sections for "Secure Client" and "Secure Endpoint" with details for Windows and Linux connectors.

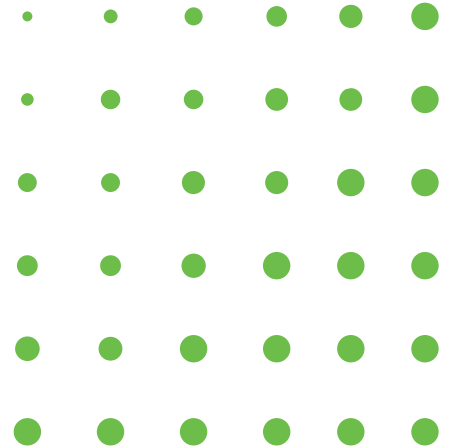
SE without “AC”

- It is possible to deploy Secure Endpoint v8.x by itself
 - No other modules, no Cloud Management with SecureX, etc.
 - Deploy just like Secure Endpoint v7.x – and it will have the Secure Client UI; but no other SC components

The image displays two screenshots related to Cisco Secure Endpoint. The top screenshot is the management console, showing the 'Secure Client' section for Windows 10. It includes a search bar, navigation tabs (Dashboard, Analysis, Outbreak Control, Management, Accounts), and a 'Group' dropdown set to 'Protect'. Below this, there's a 'Secure Client' header and a 'Windows 10' section with a description and buttons for 'Manage Secure Client Modules', 'Show URL', and 'Download'. The bottom screenshot shows the 'Secure Endpoint' management page with sections for 'Windows Server / 7 / 8' and 'Mac', each with 'Protect Policy' settings and 'Flash Scan on Install' options. In the foreground, a 'Cisco Secure Client' application window is open, displaying the 'Secure Endpoint' logo, a 'Disconnected' status with a warning icon, and a 'Flash Scan' dropdown menu with a 'Start' button.



Upgrading



Agenda



- ▶ CSC Overview
- ▶ CSC Architecture
- ▶ Deploying / Managing CSC
- ▶ Upgrading to CSC
- ▶ FAQs
- ▶ Secure Connect



Upgrading Secure Endpoint

- Cisco Secure Client WILL uninstall the old version when it is installed
 - Cloud Install from SE Cloud to v8.x
 - 64-bit Windows Only
 - Win10/Server2016 or newer
 - Older OS's & 32-bit will remain in 7.5.x train



Upgrading Secure Endpoint – Using Policy

Name: ATW-WindowsPolicy

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

Modes and Engines

Exclusions
41 exclusion sets

Proxy

Outbreak Control

Product Updates

Advanced Settings

Deprecated Settings

Product Version: 8.0.1.21160 (1 of 44 computers must reboot. Details)

Update Server: upgrades.amp.cisco.com

Date Range: 2022-07-28 18:56 to 2022-08-03 23:59

Update Interval: 30 minutes

Block Update if Reboot Required

Reboot: Ask for reboot

Reboot Delay: 2 minutes



Upgrading AnyConnect

- Cisco Secure Client WILL uninstall the old versions when it is installed.
 - Inline upgrade from AnyConnect Headends
 - ASA, FTD, ISE
 - No webdeploy for Cloud Management Module (yet)
 - Even removes the Endpoint Roaming Client (ERC) and uses its configuration

Agenda



- ▶ CSC Overview
- ▶ CSC Architecture
- ▶ Deploying / Managing CSC
- ▶ Upgrading to CSC
- ▶ FAQs
- ▶ Secure Connect

Frequently Asked Questions

- No, Duo & 1000 Eyes are not part of this release
 - 1000 Eyes in planning right now
- macOS and Linux on short follow roadmap
- CSC may be used with or without the Cloud Management
- Web-based management is only available within SecureX
- CSC is Windows Only in this release
- Seamless upgrade through existing paths
- AnyConnect 4.x still exists for customers who don't want/need to upgrade
- Cisco Branding has gone ahead and re-branded AnyConnect as Cisco Secure Client everywhere

Agenda



- ▶ CSC Overview
- ▶ CSC Architecture
- ▶ Deploying / Managing CSC
- ▶ Upgrading to CSC
- ▶ FAQs
- ▶ Secure Connect

Cisco+ Secure Connect

Radically simple, unified SASE turnkey solution

Simple

Increase business agility through an easy to consume and use as-a-service subscription that is cost-effective

Secure

Protect across every point of service - user, device, application - enforcing security closest to threats

Intelligent

Deliver actionable insights end-to-end, to predict, understand, and remediate the application experience



Built for Speed and Simplicity

Cisco+ Secure Connect

Secure Remote Worker

Core elements

- Internet Security
 - DNS-Layer Sec
 - SWG Proxy
 - CASB
 - DLP
 - Cloud Firewall
- Private access
 - Device posture
 - SAML Auth
 - Access control

