CISCO
SECURE

Introducing Cisco Secure Access to Umbrella users

Upasna Gandhi & Michael Neibert

Technical Customer Success Specialists

April 2025

Agenda

1. Introduction
2. Secure Access Packaging
3. Secure Access Architecture
4. Secure Access Use-cases (SIA & SPA)
5. Support
6. Demo and Q&A

Cisco Secure Access Packaging

Category	Features	Essentials	Advantage
Secure Access	Secure Internet Access (SIA) • Roaming module (DNS/Web) • SD-WAN DIA • Roaming firewall • IPSEC tunnels, PAC, Proxy Chain	✓	✓
	Secure Private Access (SPA) • Client-based ZTNA • Clientless ZTNA • VPN access (private app)	✓	✓
Foundational Security	DNS protection	✓	✓
	Cloud Delivered Firewall for layer 3 & layer 4 controls of web and private apps	✓	✓
	Secure web gateway (proxy web traffic, URL filtering, content filtering, advanced app controls)	✓	✓
	CASB - Cloud app discovery, risk scoring, blocking, cloud malware detection; tenant controls	✓	✓
	Remote Browser Isolation (License type- Risky traffic only)	✓+	✓+
	Secure Malware Analytics (sandbox)	Limited	Unlimited
Advanced Security	Layer 7 Cloud Delivered Firewall		✓
	IPS protection		✓
	Data Loss Prevention (DLP) for web applications		✓
	Remote Browser Isolation (License type – Any traffic)		✓+
Support	Cisco 24x7 enhanced support access via email and phone (required Enhanced attach, optional Premium upgrade)	+	+

cisco SECURE

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Cisco Confidential

Introducing Cisco Secure Access

Proven Network and Cloud security converged into one service

Umbrella DNS >12 years

Umbrella SWG >5 years

DUO Posture >4 years

Umbrella CASB >5 years

RBI >5 years

ZTNA >4 years

Secure Client >3 years

VPN Termination >10 years

Cloud Firewall >5 years

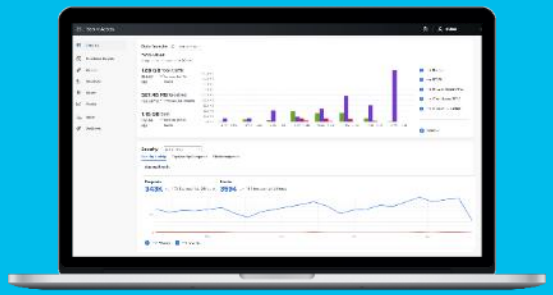
Umbrella DLP >5 years

Umbrella Advanced Malware Protection >7 years

Experience Insights/DEM (ThousandEyes) >3 years

Protecting 70,000+ customers | More than 220M endpoints

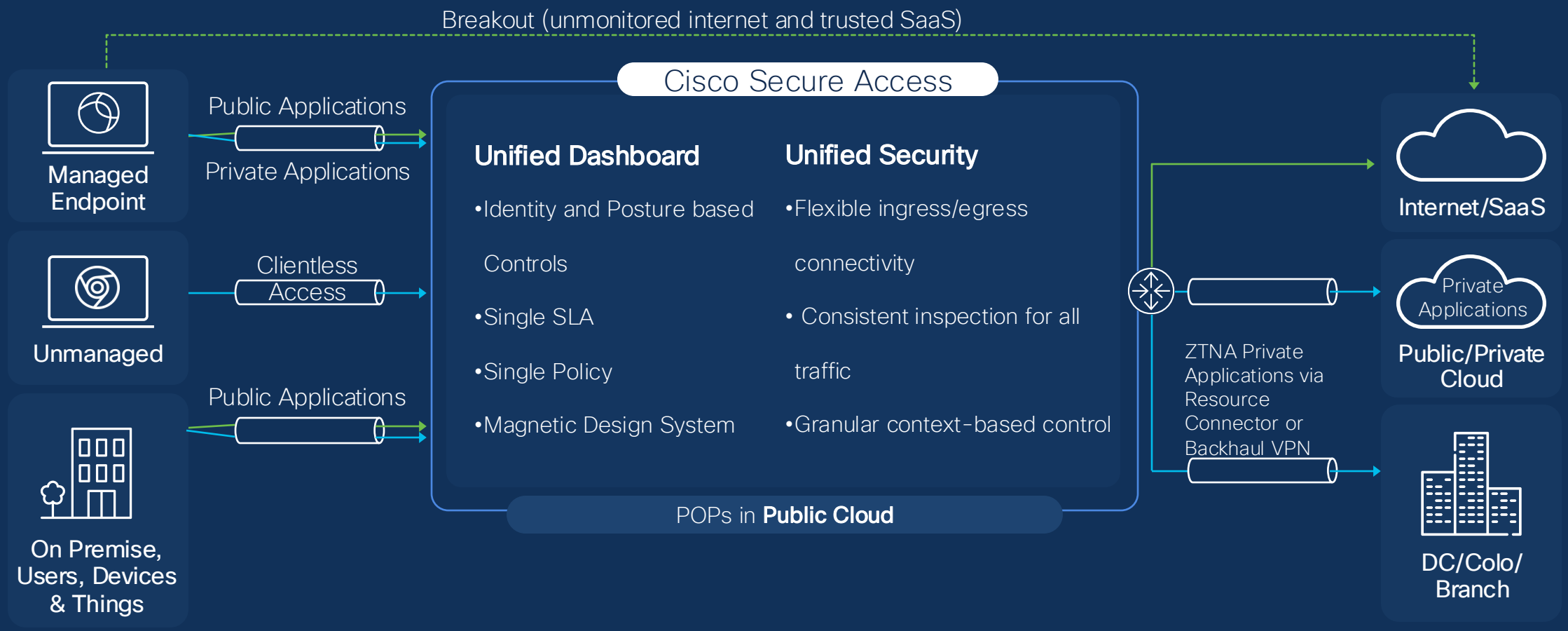
Cisco Secure Access



- **Single Console**
- **Single Client**
- **Unified Policies**

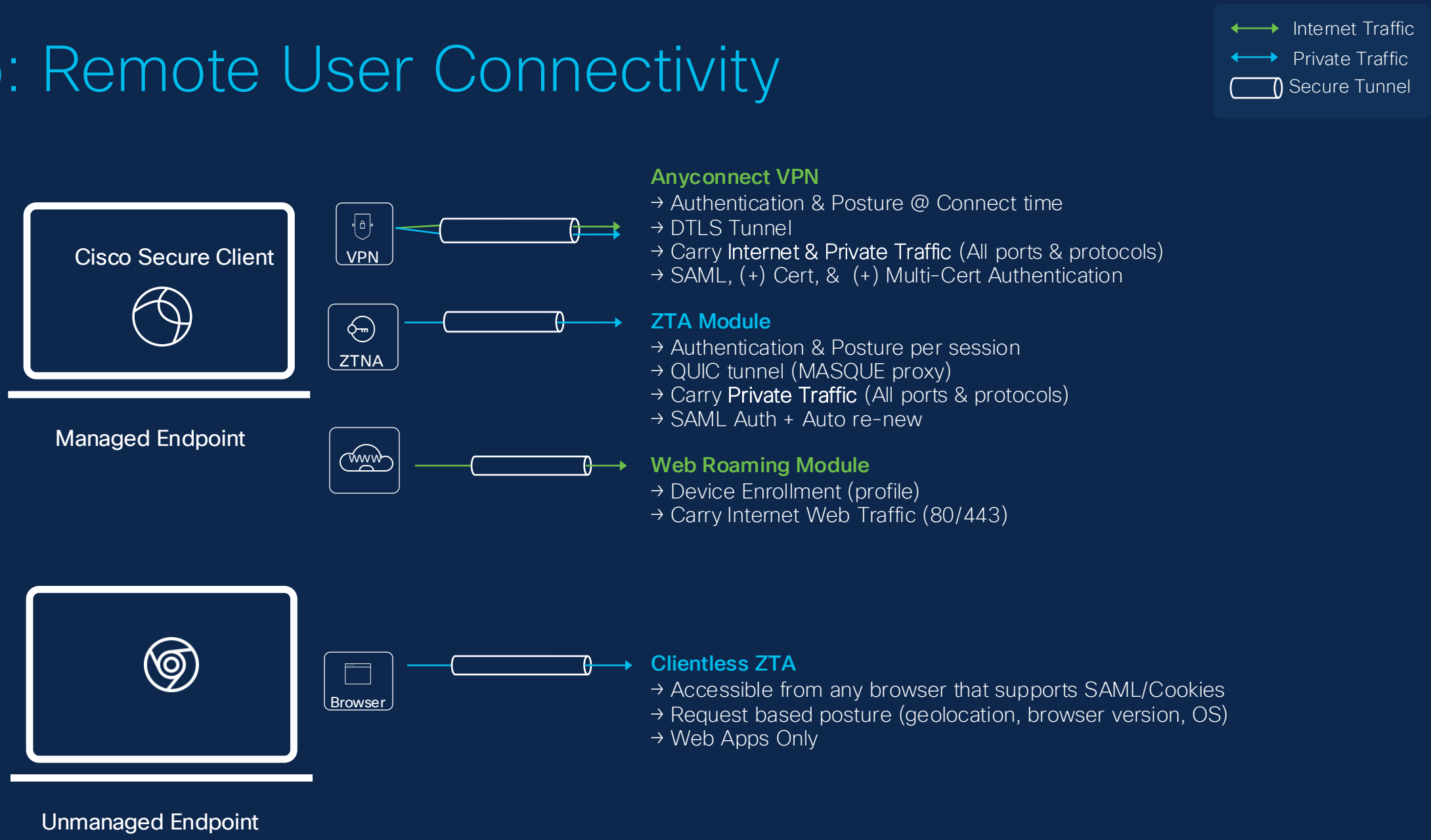
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Architecture Overview



Users & Devices — How — Apps

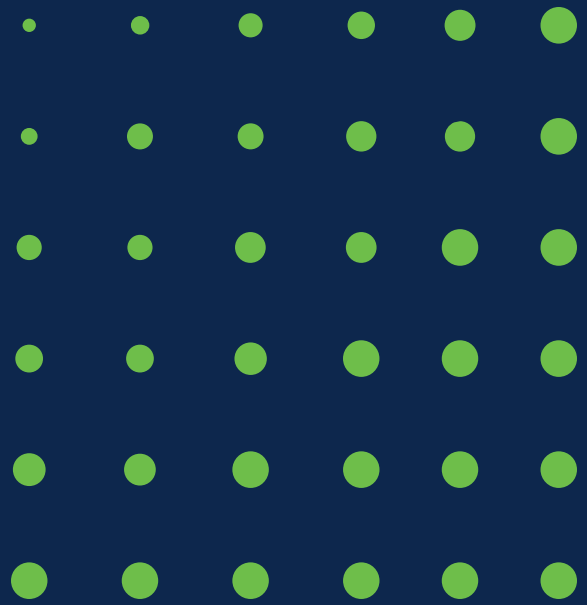
Who: Remote User Connectivity



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Cisco Confidential

Use Cases



Cisco Secure Access

Secure Internet Access

- Secure Web Gateway (SWG)
- Cloud Access Security Broker (CASB) and DLP
- Firewall as a Service (FWaaS) IPS
- DNS Security
- Sandbox
- Multimode DLP
- Advanced Malware protection
- Digital Experience Monitoring*
- Remote Browser Isolation*

Secure Private Access

- Client-based Zero Trust Network Access (ZTNA)
- Clientless Zero Trust Network Access (ZTNA)
- VPN as a Service
- Firewall as a Service (FWaaS) IPS

Both use cases

- Talos Threat Intelligence

* Included in the unified experience / separate license (optional)

cisco SECURE

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Cisco Confidential

Use Cases Connectivity Options

- Secure Internet Access
  - Network Protection
  - Branch (IPsec Tunnel)
  - Roaming Module
  - Pac File
  - RA VPN (Secure Client – VPN Module)

- Secure Private Access
  - RA VPN (Secure Client – VPN Module)
  - Client-Based ZTNA (Secure Client –ZTNA Module)
  - ZTNA Clientless (Browser-Based)
  - Branch (IPsec Tunnel)

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Confidential
Cisco Confidential

SIA Connection options/Deployment Methods

Types of Deployments	Capabilities
Network Protection	1. First line of defense 2. Deployed with in minutes 3. Policy enforcement (Security and Content Access controls
Secure Branch	1. User come online 2. Secure Client detects in office network connection, so VPN not required 3. Private application traffic is routed via optimized SDWAN, Internet bound traffic is routed through SIA tunnel
Roaming Module (Secure Client – Roaming Module	1. DNS/Web Traffic (80/443) Redirection 2. Policy Enforcement 3. Trusted Network Detection 4. Domain/IP proxy bypass and User Identity visibilty

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Confidential
Cisco Confidential

SIA Connection options/Deployment Methods

Types of Deployments	Capabilities
PAC File	1. Browser Web Traffic (80/443) Redirection 2. Policy Enforcement 3. Domain/IP proxy bypass 4. User Identity visibilty(If SAML is configured)
Secure Internet Access (typically coupled with Secure Private Access via VPN)	1. User authenticates, MFA & posture optional, identity determined 2. Authorization based traffic match 3. Traffic determined as Internet vs Private traffic and forwarded to firewall 4. Firewall applies identity-based access control 5. Firewall applies TLS decryption and IPS on the traffic (if enabled) 6. Web traffic sent to SWG; non-web traffic sent to SSE egress 7. SWG applies security policy and advanced scanning (DLP, CASB..) as controlled by the policy. 8. Egress traffic NAT prior to egress

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Confidential
Cisco Confidential

Use Cases Connectivity Options

- Secure Internet Access
  - Network Protection
  - Branch (IPsec Tunnel)
  - Roaming Module
  - Pac File
  - RA VPN (Secure Client – VPN Module)

- Secure Private Access
  - RA VPN (Secure Client – VPN Module)
  - Client-Based ZTNA (Secure Client –ZTNA Module)
  - ZTNA Clientless (Browser-Based)
  - Branch (IPsec Tunnel)

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Confidential
Cisco Confidential

SPA Connection options/Deployment Methods

Types of Deployments	Capabilities
RA VPN (Secure Client – VPN Module)	1. SAML 2.0 + cert-based authentication 2. Posture verification (optional) 3. Trusted Network Detection 4. Start before logon 5. IPS 6. Granular context-based control
ZTNA Client-Based (Secure Client – ZTNA Module)	1. SAML 2.0 authentication 2. Posture verification (optional) 3. Supports most TCP/UDP protocols 4. Masque over QUIC or TLS 5. IPS 6. Granular context-based control

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Confidential
Cisco Confidential

SPA Connection options/Deployment Methods

Types of Deployments	Capabilities
ZTNA Clientless (Browser-Based)	1. Clientless 2. App specific access 3. Undiscoverable IP address 4. Least privileged user access 5. Reduced threat surface
Branch (IPsec Tunnel)	1. Branch connectivity through tunnel 2. Traffic flows through cloud firewall 3. Traffic gets routed to private apps

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Confidential
Cisco Confidential

ZTA Clientless, ZTA Client-Based and RAVPN comparison

	Cisco Secure Access		
Hosting	SaaS		
Type	Clientless	Client-Based	
Client	Web Browser	ZTA Module OS Native Clients	VPN Module
Supported Traffic	Client-to-server	Client-to-server	Client-to-server, Client-to-client, Server-to-client
Supported Apps	HTTP, HTTPS	TCP & UDP	All TCP, UDP & ICMP
Client Protocol(s)	TLS	MASQUE over QUIC or TLS	TLS, DTLS, IPSec
Device Posture	Per-Rule	Per-Rule	On Connect
Per-App Controls	User/Group-Based Access Control, TLS Decrypt, IPS		

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Cisco Confidential

Migration tool Update

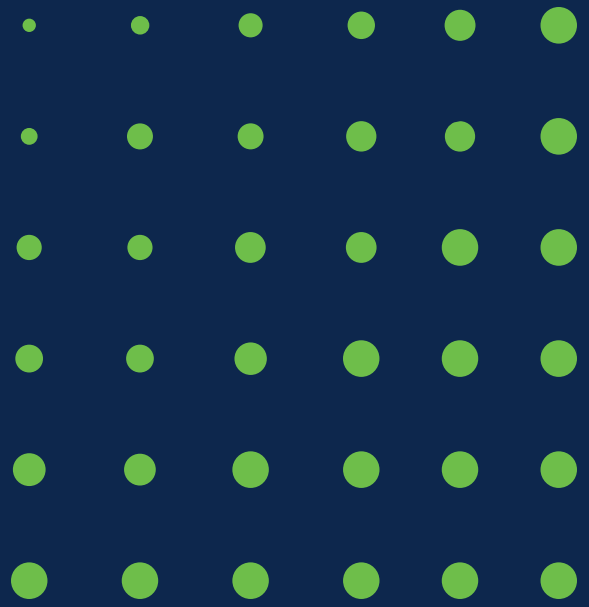
Cisco is working on Migration tool (for DNS ONLY) from umbrella to secure access which will be available soon.

More details to come!!

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Cisco Confidential

Support & Documentation



Support Services for Cisco Secure Access

Deliverables	Software Support Enhanced (Required for all packages)	Software Support Premium (Optional Upgrade)
Technical support (24x7 access to Cisco Cloud Security Support – phone/online)	✓	✓
Initial response target (Severity 1 and 2 cases)	30 minutes for phone	15 minutes for phone
Software updates	✓	✓
Prioritized case handling		Prioritized over Enhanced Support
Primary point of contact with software expertise	✓	✓
Technical onboarding including configuration guidance	✓	✓
Technical adoption including periodic system risk evaluations and guidance for software usage	✓	✓
Support case analytics		✓
Designated service management: assigned expert who provides incident, case, and change management plus consultation and recommendations		✓

To learn more about Cisco Support Services for Security Software, click here.

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Cisco Confidential

Support

- Technical Support (24x7 access to Cisco Cloud Security Support - phone/online).

Contact TAC by
Phone US/Canada
1 800 553 2447
1 408 526 7209

Email Support
tac@cisco.com

Open a TAC Case
Online

Cisco Worldwide Support Contacts:

https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

Additional Resources

Manage Support Cases

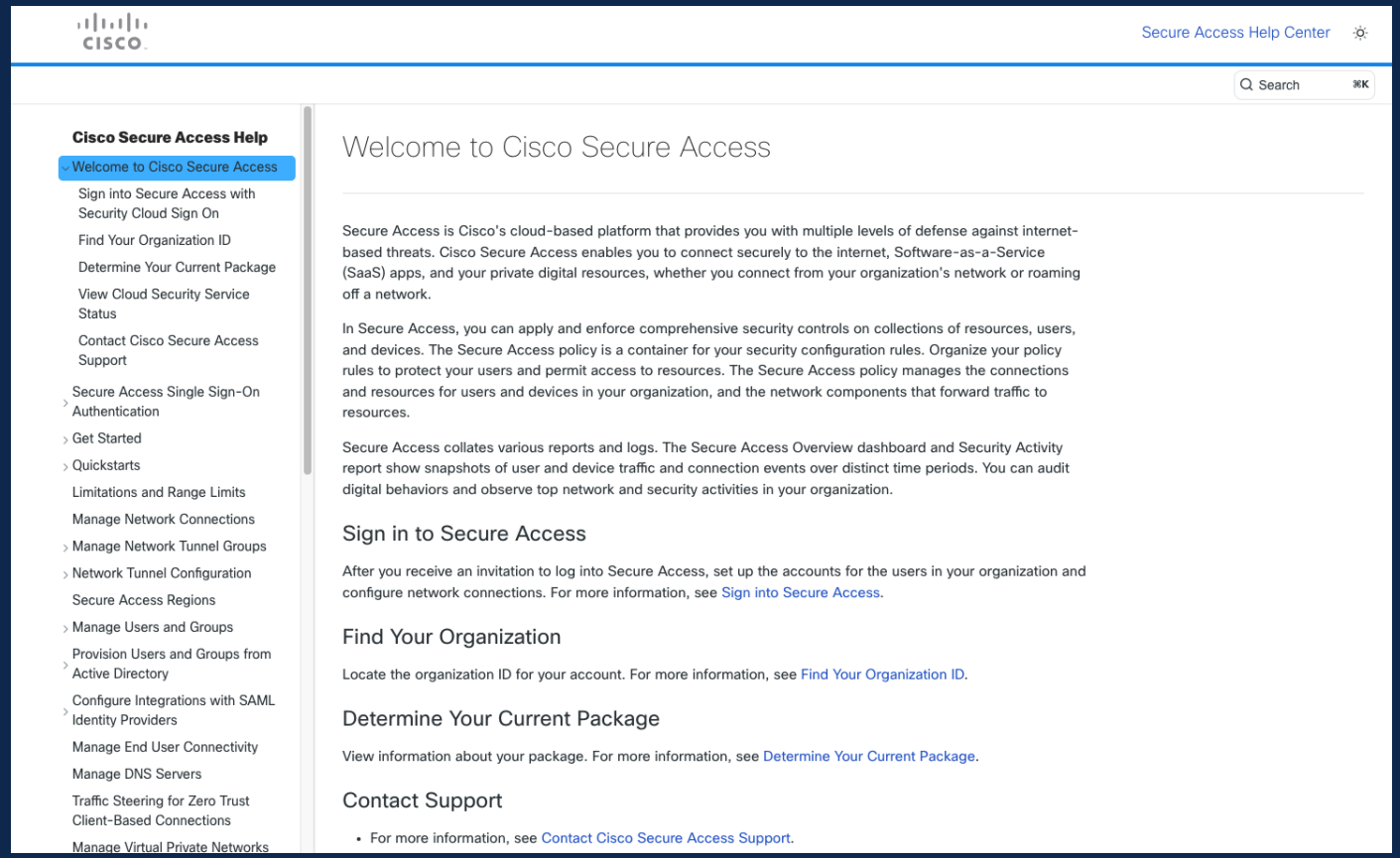
Cisco Support Assistant

Cisco Community

Cisco - Secure Access Service Status

Documentation

Cisco Secure Access Help Center: https://docs.sse.cisco.com/



Demo and Q&A.

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Cisco Confidential

SECURE