Cisco Secure Access Release Notes

First Published: October 27, 2023
Last Revised: March 15, 2025

Notice: Cisco Secure Access – Browser Zero Trust Access URL change

The browser-based Zero Trust Access URL (browser-based only) in Cisco Secure Access is changing from a .com domain to an .io domain as of **Tuesday, December 5, 2023**. The browser-based URL is the custom address that companies configure for end users to connect securely to private resources using browser-based Zero Trust Access.

To help with the transition, the current .com URL will coexist with the new .io URL from December 5-15, at which time the .com URL will be decommissioned. For your part, you do not need to change the URL prefix that uniquely identifies each of your resources. Secure Access will automatically join the prefix *<your organization's tenant ID>-ztna.sse.cisco.io* to form the new public URL address.

What you need to do is to **notify your application owners and end users of the updated URLs**. We recommend that end users bookmark the new URL.

Known Issues – March 15, 2024 Release

Feature	Caveat Description	What is the customer impact?	Which users are impacted?
ISE Integration	ISE Posture requires that the Cisco Secure Client be able to resolve the FQDN of the ISE system.	Configure a private DNS server(s) as part of the VPN profile; or add a host entry on the Secure Client that maps the ISE FQDN to a private IP address.	IT Administrator
ISE Integration	User-Based Access Policies when External Radius/ISE used for RAVPN Authorization do not include the Origin ID.	User-based firewall access rules and user-based SWG rules do not work.	IT Administrator
ISE Integration	When configuring VPN profiles, configure the IP Pool first and save the profile, then add RADIUS groups and servers.	Remote Access VPNs may not work as expected.	IT Administrator
Resource connector deployment	Resource Connector VM should not be cloned and should be deployed independently.	If the Resource Connector is cloned, the original and cloned instance will not function properly.	IT Administrator

Feature	Caveat Description	What is the customer impact?	Which users are impacted?
IPv6 Support for Resource Connectors	Only IPv4 addresses are supported on Resource Connectors. IPv6 is not supported yet.	Resource Connectors can only be configured with IPv4.	IT Administrator
Browser-based/Client-based ZTNA access via Resource Connectors	Your network subnets should not overlap with the CGNAT range 100.64.0.0/10.	Configuring overlapping networks will cause issues routing traffic to the private resource.	IT Administrator
Logging on dashboard	For ZTNA traffic flowing through Resource Connectors, firewall events logged might have inaccurate IP addresses.	Logging events might be inaccurate.	IT Administrator
Resource connector interfaces	Resource connectors can only be launched with a single interface.	A resource connector configured with multiple interfaces is not supported.	IT Administrator
Resource connector group provisioning key	Provisioning keys show up on the API keys page in management dashboard.	If an administrator deletes any of the provisioning keys, it will lead to failure in enrolling new Resource Connectors using the deleted provisioning key.	IT Administrator
Resource connector group region change	An administrator will not be able to edit the region a Resource Connector Group is associated with after it is created.	After a resource connector group is created, the region can't be changed. The group must be deleted from the old region and recreated in the new region.	IT Administrator

Known Issues – October 27, 2023 Release

Feature	Caveat Description	What is the customer impact?	Which users are impacted?
Client-based ZTA	Secure Client ZTA Module only available on Windows 10 and 11 and MacOS versions 11, 12, 13, 14	Other platforms are not supported	End Users

Feature	Caveat Description	What is the customer impact?	Which users are impacted?
Sync intervals	Certain configuration changes will take up to five minutes to be applied on all system components (this includes steering configuration, posture update from clients, and tunnel settings)		
External API	External APIs are not documented and not supported.	Currently there are only two external APIs supported for SDWAN integration with Secure Access. Some of the existing APIs on Umbrella will be available as undocumented / unsupported APIs.	IT Administrator / Developer community
Data Retention	Data retentions is one year for DNS queries and 30 days for FW, SWG, and DNS.	None	IT Administrator
Access policy support	SWG and DNS does not enforce inline IP in the access policy.	Customer created rule for inline IP in source or destination will be supported by firewall only.	IT Administrator
Policy rule management	Supported rule limit is 5K. If the number of access rules exceed 5K, the performance of the Policy UI and policy enforcement is impacted.	Customer can create up to 5K rules including internet access and private access rules without experiencing significant performance impact.	IT Administrator
ECMP support for branch connections	ECMP-based load balancing is not yet supported.	Branch connections will not be able to leverage ECMP to load balance across multiple tunnels.	IT Administrator
RAVPN	Upgrades to remote access VPN service will disconnect current session.	The users will have to re-establish their session. This is existing ASA design which provides persistent VPN connection.	End Users
RAVPN	Multiple remote access VPN profiles with duplicate SAML configuration does not work properly.	You must use a different SAML configuration per VPN profile.	IT Administrator

Feature	Caveat Description	What is the customer impact?	Which users are impacted?
No Overlapping Subnet support	Each branch within the same organization must use different, non-overlapping subnets. For example, two branches of the same organization cannot both use the subnet 192.168.10.0/24.	Customers must ensure each branch has different subnets, or they must NAT the branch traffic on their side and only configure the NAT addresses to CNHE.	IT Administrator
SAML + IP surrogate	For an org with IP Surrogates enabled, if SAML is enabled and then disabled, user identity may still apply for authenticated users for up to 12 hours after SAML is disabled.	Customers may see user-based policies apply for previously authenticated users. No impact on non-authenticated users.	End Users
Client-based ZTA on Mac	We will not be able to support multiple users on macOS at this time. Only the first user who enrolls will be able to utilize ZTA. We are also unable to enroll different users on the same device. This is due to how security fundamentally works with macOS's Secure Enclave. We are investigating how we can improve the user experience surrounding this issue and will have more information in the coming weeks.	Only one user can do successful ZTA Enrollment on a macOS device.	Customers with multiple users on a single macOS device
Endpoint Posture Management	Posture profile limit per org is 100.	If the number of posture profiles created within an org are more than 100, then customer will be prompted with error message to either delete unused posture profiles or edit existing profiles.	IT Administrator
Auto upgrade configuration for AD	Customer needs to be able to configure the time period for upgrades for AD controllers. However, today the functionality is not available.	Upgrade takes place between 2AM-6AM every day.	IT Administrator
BGP learned routing information is not displayed in user interface	BGP Network Tunnel – Routes/prefixes learned from the remote location are not shown yet.		IT Administrator

Feature	Caveat Description	What is the customer impact?	Which users are impacted?
Client-based and Clientless ZTA	For the private traffic from the ZTNA, the IPS events will have the source IP in the range (100.64.0.0/10) and not the client IP.	Customer will need to instead user ID in the logs for identification of the event.	IT Administrator
Clientless ZTA	Clientless ZTA does not support “TLS 1.3 only” applications.	Customer needs to also enable TLS 1.2 on the application side.	IT Administrator
FWaaS	For access policies with destination as any, application info will not be seen in firewall events.	There is no functional impact.	IT Administrator
FWaaS	SAML authentication may get blocked by Firewall (IPS) if Security over connectivity or Max Detection IPS profile is configured. This is only applicable for Branch to Internet traffic.	SAML authentication login page will not be served for authentication.	End Users
Users and Groups	Azure AD Scope change from 'Sync all Users and Groups' to 'Sync only assigned users and groups' is not sending disable events.	Users and groups outside the defined scope will get listed in the dashboard.	IT Administrator
Secure Internet	Users connecting with the Umbrella roaming module or PAC file in Israel are not reaching the Israel Secure Access PoP. Traffic is going to Frankfurt or London instead. Workaround: Use IPsec tunnel or RAVPN to connect to Israel PoP.	Increased latency, pages rendered in English instead of Hebrew, geolocation, data sovereignty.	End Users