Cisco Secure Access Pre-Onboarding Checklist

Complete the following tasks before signing into Secure Access for the first time.

Application and team information

☐ **Identify at least 2 internal applications for testing the access controls.** For each application, determine:

- ☐ IP addresses/FQDNs
- ☐ Ports/protocols
- ☐ Decide if VPN, client-based Zero Trust Access or clientless ZTA

☐ **Decide which users and groups you want to include in testing.**

- ☐ Ask Active Directory admin (Identity Management team) to provision relevant users and groups. Choose one provisioning method:
  - ☐ Microsoft Entra ID provisioning Help – Microsoft Entra ID
  - ☐ Okta provisioning Help – Okta
  - ☐ On-premise AD provisioning Help – Active Directory

☐ **Choose your SAML 2.0 compatible identity provider.**

- Out-of-the-box supported IdPs: AD FS, Microsoft Entra ID, Duo Security, Okta, OpenAM, and PingID

☐ **Request 2 SAML SSO applications in SAML IdP.**

- ☐ One SAML SSO application for client-based ZTA and clientless ZTA
- ☐ One SAML SSO application for VPN

Network requirements

☐ **For private access**

- ☐ Select IP address ranges for VPN.
- Each cloud data center to which users will connect must have one user and one management IP range Help.
- ☐ If using IPsec tunnels for backhauling private access traffic (VPNaaS, ZTA):
- For static routing: Route traffic to the Remote Access VPN pools and CGNAT pools (100.64.0.0/10)
- For dynamic routing: Configure BGP peering with Secure Access platform
- ☐ If using resource connectors:
- Static or dynamic routing is only needed for VPNaaS Client IP pools
- CGNAT is no longer needed or visible within customer networks
  - ☐ Internally submit a firewall request to allow access from the backhauling IPSec tunnel and/or resource connectors to internal DNS service and previously selected internal applications.
- ☐ Optional: To facilitate IPSec site-to-site communication, open UDP ports 500 and 4500 Help.

Network requirements, continued

☐ **For internet access**

- ☐ Reference the public IPs used for SSE functions Help: Secure Access Secure Web Gateway Services.
- ☐ Select preferred integration method:
  - ☐ Branch to internet: Backhauling IPSec tunnels used for private access can also be used for internet access. Appropriate routes must be in place to steer the traffic.
  - ☐ Roaming user to internet: Remote access VPN can be used to route all traffic to internet, or roaming module can be used to route DNS and web traffic.
- ☐ Highly recommend: Review your organization's acceptable usage policy to understand which site categories should be blocked.

Computer requirements

☐ **Highly recommend: Use dedicated machine(s) for testing.**
Secure Access supports: PC, Mac, iOS Apple device and Samsung Android.

- ☐ Ensure you have admin-level access to the machine(s).
- ☐ To test client-based ZTA, the machine(s) must have Trusted Platform Module 2.0 (TPM) available.
- ☐ Ensure that the Secure Client software has been downloaded and installed on the test machine(s).