SonicWall Cloud Edge Secure Access 1.1
Release Notes

About Cloud Edge Secure Access

SonicWall Cloud Edge Secure Access is a Zero Trust Network as a Service that helps you to secure your team's network, including valuable local and cloud resources. Incorporating the highest standards of Zero Trust Security, users can create adaptive least-privilege access policies based on device, identity, role, and location. Accordingly, authorized employees are only granted access to the corporate resources they need, and IT administrators can more easily monitor activity across the network and implement a full range of network security features that are easy to scale with organizational growth. The combination of this reduced attack surface and cloud-friendly approach makes it that much more difficult for bad actors to breach your network, but also saves significant IT overheads..

These release notes provide information about the SonicWall Cloud Edge Secure Access (Cloud Edge) 1.1 release.

Versions:

- Version 1.1

Version 1.1

September 2021

Compatibility and Installation Notes

- SonicWall Cloud Edge Secure Access currently provides support for Windows, Linux, MacOS, iOS and Android, and preconfigured installation scripts are provided.

  ⓘ | **NOTE:** Internet Explorer 11 browser does not support Cloud Edge Secure Access web client access.

- A MySonicWall account is required.

What's New

New Features in CE 1.1:

- **Device Posture Check** ensures that only devices that compliant with their predefined security policies can connect using a Cloud Edge agent to a Network.

- **Network Traffic Control** enables stateful FWaaS capability by defining who can access specific network, services and from where.

- Protect and limit access to your resource(s) by defining policies and rules based on user groups, origin and/or destination IPs, ports, and/or network protocols, by enabling Network Traffic Control you can secure and control the entire traffic on one unified Software-Defined Perimeter (SDP).

- Cloud Edge brings the new capabilities to Edge devices (Firewalls, Routers) to connect with Dynamic IP support. Both the tunnels IPSEC and WireGuard can be provisioned using the Dynamic IP tunnel configuration.

- Trusted networks for clients (MAC & Windows) support to specific router's MAC address. These networks will not require VPN connection, even if Always On is enabled.

- Certificate manager is enhanced with the ability to import certificates in PEM/CERT/PFX File format.

- Extended support for SAML2.0 (Pingone for Enterprises, PingFederate, Rippling, etc.).

- Wireguard is supported on any capable docker running systems.

- Cloud Edge new agents brings abilities like seamless connection, improved security, improved performance, improved reporting, and handling of different errors reporting.

- Cloud Edge new Linux agents brings abilities like seamless connection, improved security, improved performance, improved reporting and handling of different errors reporting.

- iOS and Android Cloud Edge agents are available on respective App stores to download.

- Cloud Edge agent support for MAC OS BigSur.

- Cloud Edge agent Support for Windows 11.

Cloud Edge Agents:

- Fixed private DNS and DNS filtering indications on main page.

- Fixed UI issues which lead to app unresponsive when service is killed/crashes.

- Fixed app reconnection after airplane mode with TWN (Trusted Wi-Fi Network).

- Fixed issue with networks staying in quick access after being removed.

- Improved UI enhancement- Always On indication with TWN feature.

- Fixed issue with re-login required when switching between Wi-Fi networks.

- Added support for gateway graceful shutdown - doesn't require re-login now.

- Fixed login issues related to token parse error with Asian language OS.

- Fixed issue with app stuck on connecting to broken gateway.

- Improved UI & performance to periodically measure gateway ping latency.

- Improved UI to provide Always On indication.

- Fixed issue when returning from sleep and immediately hibernate state of endpoints (Re-word).

- Improved UI for macOS when app is launched minimized, it is shown in notification area menu.

- Added Mac OS Agent Always On VPN indication of -Bad "Enforced By Admin".

- Fixed Agent getting stuck on connecting stage after the computer was on the sleep mode.

- Fixed MacOS issue of showing incorrect VPN status on Home screen if Start Minimized=ON and VPN was connected automatically.

- Fixed issue on macOS agent is getting 'Update available!' notification when the new version wasn't rolled out for his tenant.

- Fixed values on Settings - Network tab that were not getting updated on workspace settings change.

Logging:

- Fixed some of the error message handling on the agents.

- Added debug logging for the agents.

- Improved loggings for some of the activities.

Web Console:

- Added Demo admin role in the web console.

- Improvements in certificate import process.

- Disable Create Access Key option is not available.

- Reorganized main menu items for Enhanced UI for CE 1.1 Console.

- Improved downloaded page, we can download the iOS and Android agents now from play store.

- Added Delighted app to provide feedback.

- Added support for Edge Browser for the Application Policies.

Networking:

- Added support for the smaller subnets (/21).

- Added support for Ubuntu 20 for the Wireguard Connector.

- Added Docker support for the Wireguard Connector.

- Added Dynamic IP support for Edge devices firewall and Routers.

Authentication:

- Added support for more IDPs (Rippling, PingFederate etc.).

- Implemented Auth0 login on onboarding for native agents.

Resolved Issues

Issue ID	Issue Description
SASE-526	MSP user experience is improved and simplified for MSP partners. MSP partners can easilty onboard & manage new Cloud Edge tenants in few easy steps.
SASE-492	This is our continuous effort to keep adding regions to deliver optimum network performance to our customers. We are added support for Mumbai region on Cloud Edge.
SASE-472	We can disconnect any connected network on Cloud Edge agent via quick access tab of MAC CE agent.
SASE-465	We support network traffic rules and posture check for the devices for different security compliance. Hence traditional ways of access key usage is disabled for Cloud Edge 1.1 and newer new versions.
SASE-451	While changing any configuration for the IPSEC tunnel on Cloud Edge, routes were updated to default.
SASE-445	MAC Big Sur Cloud Edge agents connects and display the information correctly.
SASE-167	Application Policies can be created for Microsoft Edge browser and it enforces the policy rule accordingly.

Known Issues

Issue ID	Issue Description
SASE-153	Cloud Edge AD/LDAP agent is presently have a valid certificate from our partner. Sometimes Microsoft Defender Smartscreen will throw a warning regarding an unrecognized application, This is because of additional requirements on extended validation certificates that are a Microsoft requirement.
SASE-108	Cloud Edge agents are presently have a valid certificate from our partner. Sometimes Microsoft Defender Smartscreen will throw a warning regarding an unrecognized application, This is because of additional requirements on extended validation certificates that are a Microsoft requirement.

SonicWall Support

Technical support is available to customers who have purchased SonicWall products with a valid maintenance contract.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. To access the Support Portal, go to https://www.sonicwall.com/support.

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- View and participate in the Community forum discussions at https://community.sonicwall.com/technology-and-support.
- View video tutorials
- Access https://mysonicwall.com
- Learn about SonicWall professional services
- Review SonicWall Support services and warranty information
- Register for training and certification
- Request technical support or customer service

To contact SonicWall Support, visit https://www.sonicwall.com/support/contact-support.

About This Document

ⓘ | **NOTE:** A NOTE icon indicates supporting information.

ⓘ | **IMPORTANT:** An IMPORTANT icon indicates supporting information.

ⓘ | **TIP:** A TIP icon indicates helpful information.

△ | **CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.**

⚠ | **WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.**