

# Release Note

## **SecuExtender**

### **Zero Trust IPSec/SSL VPN Client Subscription (for macOS)**

Version 3.2.4.19

December 12, 2023

## System Requirement

- macOS 11 or above (including macOS 14 Sonoma)
- M1 Mac/MacBook supported (requiring Rosetta)
- The version of the software must be unlocked by the SecuExtender Zero Trust IPsec/SSL VPN Client Subscription for Windows/macOS (1YR/3YR/5YR licenses)
  - SECUEXTENDER-ZZ1Y01F
  - SECUEXTENDER-ZZ3Y01F
  - SECUEXTENDER-ZZ1Y05F
  - SECUEXTENDER-ZZ3Y05F
  - SECUEXTENDER-ZZ1Y10F
  - SECUEXTENDER-ZZ3Y10F
  - SECUEXTENDER-ZZ1Y50F
  - SECUEXTENDER-ZZ3Y50F
  - SECUEXTENDER-ZZ5Y01F
- The version of the software is NOT compatible with the license keys unlocking the legacy SecuExtender IPsec VPN Windows Client (perpetual license):
  - SECUEXTENDER-ZZ0201F
  - SECUEXTENDER-ZZ0202F
  - SECUEXTENDER-ZZ0203F
  - SECUEXTENDER-ZZ0204F
- 30 days trial is supported
- 15 days grace period is supported

## NEW FEATURES, ENHANCEMENTS, FIXES OF RELEASE 3.2.4.19

- (New) SSL VPN is now supported, in that:
  - You can select SSL VPN to get connected to the new USG FLEX H series firewall
  - HOWEVER, THE VPN CLIENT'S SSL VPN IS NOT COMPATIBLE WITH THE USG FLEX/ATP series firewall
  - TLS versions: 1.2 Medium 1.2 High and 1.3
  - AES CBC encryption (128, 192 & 256 bits)
  - SHA-2 hash (224, 256, 384 & 512 bits)
  - Authentication: Preshared Key, EAP, X.509 & Multiple Auth
- Cryptography enhancements

- Support for Diffie-Hellman key group DH 28 (BrainpoolP256r1) [RFC 5639]
  - IKEv1 and vulnerable algorithms are not supported
  - End of support for vulnerable algorithms DES, 3DES, SHA-1, DH 1, DH 2, DH 5 in IPsec/IKEv2
- For certificate authentication and revocation, due to increased security requirements, deprecation of certain algorithms, and stricter rules for using certificates, this latest version comes with certain restrictions on certificates:
  - Method 1: RSA Digital Signature with SHA-2 [RFC 7296]
  - Method 9: ECDSA "secp256r1" with SHA-2 (256 bits) on the P-256 curve [RFC 4754]
  - Method 10: ECDSA "secp384r1" with SHA-2 (384 bits) on the P-384 curve [RFC 4754]
  - Method 11: ECDSA "secp521r1" with SHA-2 (512 bits) on the P-521 curve [RFC 4754]
  - Method 14: Digital Signature RSASSA-PSS and RSASSA-PKCS1-v1\_5 with SHA-2 (256/384/512 bits) [RFC 7427]
  - End of support for Method 1: RSA Digital Signature with SHA-1 [RFC 7296]
  - RSA certificates with less than 2048-bit key length are rejected
  - Key Usage and Extended Key Usage of certificates is verified
- X.509 certificate management
  - DER/PEM
  - PFX/P12
- Create configurations with more than 3 certificate authorities (CAs)
- Choose value automatically assigned to Local ID
  - The Local ID field can now be automatically filled in with a DNS or e-mail value instead of the certificate subject
- Enhancements
  - Password protection for the configuration file now requires a length of at least 16 characters and the use of a 90-character alphabet, including at least one uppercase character, one lowercase character, and one special character
  - Uses certificate authentication method 14 RSASSA-PSS by default with all RSA certificates
  - Forces UDP encapsulation mode for IKEv2

- Child SA rekey now asks for same TS as the one in the original SA that was established
- Greater stability of the IKE module
- Better performance of AES-GCM encryption
- ECDSA certificates with a key size smaller than 256 bits are now rejected
- OpenSSL has been updated to version 1.1.1w
- All CAs of a P12 file are now imported into the VPN configuration
- Uses HMAC 256 instead of SHA256 hash for VPN configuration file signature
- Allow SHA1 IKEV2\_AUTH\_DIGITAL\_SIGNATURE and configure properties
- Default Method 14 PKCS#11
- Allow SHA1 hash with Method 1
- Show Purchase URL
- VPN Client and Network Extension log to Separate Files
- **Fixes**
  - When a redundant gateway is present, the SPI size in the SA\_INIT proposal is set to 8 instead of 0 when the VPN Client switches to the redundant gateway
  - Fixes an issue where a tunnel would not close at the client end when a gateway sends DELETE requests and no longer responds
  - Fixes an issue where tunnel would stop and the error message "unsupported payload 53 for this exchange" was displayed
  - Fixes freezes when selecting Arabic or Greek language
  - Users can now refuse to use a fallback tunnel even when no message is displayed
  - Fixes issue with IKEv2 fragmentation when using AES-GCM
  - Various cosmetic and stability improvements
  - Cannot open a tunnel configuration right after VPN Client activation on a fresh install
- **IPv6 is not supported**
- **Known issue**
  - In stress conditions, the VPN tunnel may get disconnected unexpectedly when your running OS is macOS 14 Sonoma. It is recommended to enable "Split Tunnel" feature, as a workaround to mitigate the tunnel instability symptom

## **New features, improvements, and fixes of release 2.2.0.019**

- macOS 12.3 now supported
- Enhancement: Connection Panel shows automatically after start
- Enhancement: Activation now works in https
- Enhancement: Support of multiple smartcard/tokens with CNG
- Enhancement: Always-On now automatically reconnects on a WiFi network with different SSID
- Enhancement: Default driver registry keys are now set during update
- Enhancement: Support selection of IP address when a network interface has several IP address
- [ITS#220201062]: VPN configuration (client to site) / fixed issue where Cert CA list was removed when editing EAP settings
- [ITS#220200440]: Fixed issue with RSA/SHA512 certificates
- Enhancement: OpenSSL library update
- Fixed issue that prevented VPN Client from quitting in some rare cases
- Fixed a rare crash in connection panel when quitting
- Fixed DPD issue after a retransmission
- Fixed issue happening after no Delete RECV
- Fixed CA no longer disappear after unchecking EAP Popup
- Fixed a Trusted Network Detection issue
- Fixed a Local Id Issue during authentication
- Fixed Security fix to prevent buffer overflow on response from activation server – this cannot be tested by you as it requires changes on the activation server code to force an error.
- Fixed issue with Yubikey 5 NFC
- Fixed license backup incompatibility during upgrade
- Fixed unexpected « Code 103 Error DNS » error – this cannot be tested by you
- Fixes issue of tunnel disconnects with TrustedConnect whereas the WiFi connection remains UP
- Fixes issue with trusted connect continuously turning with "Connecting" status. impossible to stop
- Fixed license is lost when upgrading from 66x to 6.86 with a new license
- Sets network location for virtual interface should be set to Private

- Fixes Trusted Connect does not handle failed remote endpoint authentication
- Fixes IKEV2 Fragmentation: bad handling in case of resend

### **New features, improvements, and fixes of release 2.2.0.017**

- Feature: reporting a list of client meta to remote VPN gateway via IKE negotiation
  - This feature only works with USG FLEX/ATP/VPN/USG20-VPN series running firmware ZLD5.1 or above
  - The client meta is visible from the "Device Insight" dashboard in ZLD5.1
- **WARNING: compatibility of configuration files**
  - VPN configuration files from previous versions of the software cannot be imported into this version, once it's installed. If a previous version of the software is already present, this installer will automatically convert the previous configuration into the new software.
  - When upgrading from a previous version, it is therefore recommended not to uninstall the previous version before launching this installer.
  - The following items will be preserved when updating from Release 1.2.0.7: software settings, VPN configuration file, license.
- **Enhancements**
  - IKEv2 SA dynamic parameters can be configured from the UI
  - The "Certificate" tabs should always have "CA Management" available
  - Rename ZyWALL to SecuExtender
  - Certificate Checks can be switched off via a dynamic parameter (PkiCheck=0)
  - Fix child SA rekeying when DH mode is set to Auto
  - Use virtual IP address from CP payload
  - Correct FIPS OIDs that lead to wrong certificate verification
  - Ignore policy qualifiers when parsing x509v3 extensions

### **New features, improvements, and fixes of release 1.2.0.7**

- Feature: The macOS version software is now distributed as a DMG installer through Zyxel web site
- Feature: Compatible with Zyxel firewalls USG FLEX/ATP/VPN/USG/ZyWALL series, and virtually all existing IPsec IKEv2 compliant gateways

- Feature: AES CBC 128/192/256 encryption
- Feature: DH Group support (19-21 Elliptic Curves)
  - a. Group 14: MODP 2048
  - b. Group 15: MODP 3072
  - c. Group 16: MODP 4096
  - d. Group 17: MODP 6144
  - e. Group 18: MODP 8192
  - f. Group 19: ECP 256 (IKEv2 only)
  - g. Group 20: ECP 384 (IKEv2 only)
  - h. Group 21: ECP 512 (IKEv2 only)
- Feature: Authentication supports PSK, Certificates, EAP (IKEv2 only)
- Feature: Redundant Gateway, DPD
- Feature: Mode Config (auto, manual)
- Feature: Gateway Certificate Authorities (CA) can now be imported into the VPN Client
- Feature: Ability to force the VPN Client to open a tunnel only if the gateway CAs are valid
- Feature: Added "Get From Server" menu item to retrieve VPN configurations remotely
- Feature: retrieve VPN configuration from gateway
- Feature: EAP pop up for authentication
- Improvement: support of request for "mode-cfg type 3" to receive DNS from gateway

## Design Limitation

1. The macOS version software does not support adding up multiple time-based license keys. Please activate the software with ONE license key, before it is being expired.

2. The macOS version software discontinues the support for IKEv1

3. Discontinuing support for weak ciphers:

- IKEv1: DES, 3DES, MD5, SHA1, DH1, DH2, DH5
- IKEv2: DES, 3DES, MD5, SHA1, DH1, DH2, DH5, and NoDH for Ike Child
- If the configuration on the gateway side uses one of the removed algorithms, then the client will not connect

4. The following ZyWALL/USG VPN Gateway rules configured cannot be provisioned to the SecuExtender IPSec VPN Client for macOS:

- Multiple Authentication not applicable
- Gina mode cannot function in occasions where VPN rules are moved to USB drive
- VPN Client Address will be void in occasions where the Client and the Gateway are not unanimously both IPv4/IPv6, and users will be notified that "VPN Client Address is void so tunnels cannot be built with success"
- IPv4 rules with User-based PSK authentication