

SecuExtender

Zero Trust IPSec/SSL VPN Client Subscription

Software Release Note

For Windows
Version 7.7.40.019

September 19, 2023

System Requirement

- Windows 10, Windows 11 (64bit) or above on Intel processors only
- Windows device with ARM processor is NOT supported
- Hardware requirement
 - 1 GHz x86-64 processor
 - RAM: 2 GB
 - 40 MB available disk space
- The software can be directly installed in a system with previous versions (SecuExtender v5.6.80.007 or later)
- THE SOFTWARE IS NOT COMPATIBLE WITH SecuExtender v3.8.204.61.32 OR EARLIER
 - PLEASE UNINSTALL THE PREVIOUS VERSION BEFORE INSTALLING THE NEW VERSION
- MSI installer
- 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 7.7.40.019

- (New) SSL VPN support
 - 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
 - End of support for vulnerable algorithms: MD5, SHA-1, BF-CBC, TLS 1.1, LOW security suite for TLS V1.2
 - Compression is no longer enabled by default
- Support for Diffie-Hellman key group DH 28 (BrainpoolP256r1)
 - [RFC 5639]
- 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
- Certificate authority management
 - Uses certificate authentication method 14 RSASSA-PSS by default with all RSA certificates
 - Create configurations with more than 3 certificate authorities (CAs)
- IKEv1 and vulnerable algorithms are not supported. The security of the software has been enhanced with the following:
 - End of support for the vulnerable IPsec/IKEv1 protocol, which has been deprecated by the IETF in September 2019
 - End of support for vulnerable algorithms DES, 3DES, SHA-1, DH 1, DH 2, DH 5 in IPsec/IKEv2 (even in "auto" mode)
- Forces UDP encapsulation mode for IKEv2
- Support for a greater number of subnetworks
 - The number of subnetworks supported has been increased to 16
- 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
- Enhanced security
 - 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
 - Default behavior in USB mode has been improved for enhanced security. The connection configuration can no longer be modified simply by inserting a USB drive containing a configuration file
- Graphical interface
 - Window height of the Connection Panel window can now be increased or decreased
- Other enhancements

- Warning messages and error codes are now harmonized between the Connection Panel and the panel displayed on the Windows logon screen when GINA mode is enabled
- Local ID can now be filled automatically with DNS or e-mail in addition to certificate subject
- 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
- Systray fade-out pop-up is now disabled by default
- LZ4 library has been updated to version 1.9.3 for OpenVPN
- User interface now only allows adding CAs in the CA Management dialog box
- 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
- **Fixes**
 - Fixes an issue where VPN Client installation would roll back on Windows 11
 - 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
 - DSCP fields are now properly handled in ESP packets that are created
 - VPN Client no longer crashes when waking up from sleep
 - Activation module now reads all tgbcodes files and uses the one with the latest renewal date
 - Fixes an issue where the Console no longer recorded logs when user left workstation or locked session
 - Fixes an issue where the activation server returned an undue error message

- Fixes an issue where tunnel would stop and the error message “unsupported payload 53 for this exchange” was displayed
- Fixes support for press and hold right-click to open the contextual menu for Windows in tablet mode
- 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
- **Limitations**
 - Rebooting your endpoint (laptop/desktop) right after provisioning the VPN client is required, as long as you wanted to have the VPN client reporting client meta to the Zyxel firewalls correctly
 - USB Mode: machine-specific configuration has been disabled in this version
 - IPv4 within an IPv6 connection does not work with all configurations

NEW FEATURES, ENHANCEMENTS, FIXES OF RELEASE 6.6.87.108

- Enhancement: Add “purchase link”. This is available when:
 - The product is in the trial period
 - When the subscription has expired
 - Note. This enhancement does not apply to the macOS version.
- 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
- Enhancement: upgrade to OpenSSL 1.1.1.n
- [ITS#210900282]: IPsec VPN Client / Gina mode
- [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
- 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 6.6x 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, ENHANCEMENTS, FIXES OF RELEASE 6.6.86.016

- End of support for Windows 7 32/64-bit, Windows 8 32/64-bit and Windows 10 32-bit
 - This version of the software is compatible with Windows 10 64-bit or above on Intel processors only.
- **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 5.6.80.007: software settings, VPN configuration file, license.
- **Gateway certificate check**
 - By default, the gateway certificate will be checked each time a tunnel is opened.
 - It may be necessary to import the complete chain of certification authorities (CAs) to authenticate the gateway, either into the Windows store or into the VPN configuration file. You can change this default behavior, though we do not recommend doing so (Options menu -> PKI Options).
- **End of support for vulnerable algorithms**
 - For security reasons, this version no longer supports the following algorithms: DES, 3DES, MD-5, SHA-1, DH 1-2, DH 5. If a previous configuration contains one of these algorithms, the installer will

- convert them to "auto" (automatic negotiation with the gateway).
- If the gateway only supports this type of algorithm, you will not be able to establish a connection with this version of the VPN client.
- Gateway certificate authentication:
 - Method 9: EC-DSA on elliptic curve secp256r1 with SHA-256 (RFC 4754)
 - Method 10: EC-DSA on elliptic curve secp384r1 with SHA-384 (RFC 4754)
 - Method 11: EC-DSA on elliptic curve secp521r1 with SHA-512 (RFC 4754)
 - Method 14: Digital Signature Authentication RSA (RFC 7427)
- Initiation IKE Childless (RFC 6023)
- ESN: Extended Sequence Number (RFC 4304)
- Configuration Panel
 - Option for restricting the VPN configuration to Windows administrators only
 - Password has been removed from Configuration Panel
 - Increased configuration file protection with SHA-2
- Features : 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
- Improvement: Updated OpenSSL to version 1.1.1l
- BugFix:
 - Fixed "Wrong password" error when retrieving config from Gateway
 - Change proprietary Zyxel Notification payloads from IKE_AUTH to INFORMATIONAL
 - Backported "Error when trying to import public key for EV cert during Setup"
 - Fixed error when importing older vpn config files

- Logs for SecuExtender VPN Client now stored in the correct folder
- corrected an issue that sometimes created sockets on port 500/4500 when not required

New features, improvements, and fixes of Release 5.6.80.007

- Feature: The Windows version software is available for download 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)
 - ✓ Group 14: MODP 2048
 - ✓ Group 15: MODP 3072
 - ✓ Group 16: MODP 4096
 - ✓ Group 17: MODP 6144
 - ✓ Group 18: MODP 8192
 - ✓ Group 19: ECP 256 (IKEv2 only)
 - ✓ Group 20: ECP 384 (IKEv2 only)
 - ✓ 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: IPSec/L2TP over IPSec can be co-exist
- Improvement: support of request for "mode-cfg type 3" to receive DNS from gateway
- Improvement: Multi-lingual GUI supports 25 languages

Design Limitation

1. The Windows 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. Discontinuing support for weak ciphers:

- IKEv1: DES, 3DES, MD5, SHA1, DH1, DH2, DH5
- IKEv2: DES, 3DES, MD5, SHA1, DH1, DH2, DH5, and No DH for Ike Child
- If the configuration on the gateway side uses one of the removed algorithms, then the client will not connect

3. The following USG FLEX/ATP/VPN/USG/ZyWALL rules configured cannot be provisioned to the SecuExtender IPsec VPN Client for:

- 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