www.zyxel.com

SecuExtender

IPSec VPN Client Subscription Service

Software Release Note

For macOS
Version 2.2.0.019

Jun 8, 2022

System Requirement

- macOS 11 or above
- M1 Mac/MacBook supported (requiring Rosetta)
- The version of the software must be unlocked by the SecuExtender Zero Trust IPSec VPN Client Subscription for Windows/macOS (1YR/3YR licenses)
  - SECUEXTENDER-ZZ1Y01F
  - SECUEXTENDER-ZZ3Y01F
  - SECUEXTENDER-ZZ1Y05F
  - SECUEXTENDER-ZZ3Y05F
  - SECUEXTENDER-ZZ1Y10F
  - SECUEXTENDER-ZZ3Y10F
  - SECUEXTENDER-ZZ1Y50F
  - SECUEXTENDER-ZZ3Y50F
- 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, 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 Managment" 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