NU Series 9.0.2.4 Firmware Update

Available Firmware

9.0.2.3 (ae77c5d30cf1249146a66fdfab3457b2b72b63b9)

Supported hardware models

The NU 9.0.2.4 release supports the following models.

HASH

md5 : 9302365fac677239a0f22bb010a3921c
sha1 : 7d84701183f127931584a4ec0994686a40914187
sha256 : fe78a71a721fbedc73b632e71171c0693affcc353a342390c63c2c251eef1bee

Installation instructions

After the update is installed, the system will automatically restart twice.
Please wait 3-5 minutes.

Upgrade Notes

[Configuration]

[Basic Setting]

- Adds "Security" (TLSv1.1, TLSv1.2, and TLSv1.3 items) to [Administrative Access > Administrative Access]
- Removes "FTP Active Mode Open Port" and changes into auto module judgment at [General Setting]

[Administration]

- Adds "Log Retention Period" settings to [USB Backup Log] (only support models without hard disks)
- Adjusts max. value of data retention period from 99 days to 180 days for certain models in "Intranet Protection Log" and "Flow Analysis" at [Clear Data]

[Upgrade]

- Sorts logs in chronological order at [Firmware Download Record]

[Backup & Restore]

- Adds "Keep SSL Certification" to [Reset Default]
- Adjusts to keep the license status of [APP Control] and [URL Filter] after executing a system recovery

[Notification]

- Adds "Abnormal System Shutdown", "Virus Engine Abnormal Notification", and "DHCP Flood Attack Notification" to [Notification Items]
- Adjusts some default values for email subject and English interface texts at [Notification]

[Signature Update]

- Adjusts buttons and text size properly on the UI

[Cloud Management]

- Adds site-based delivery tasks for config. files/firmware update (Please refer to the official Eye Cloud website for more information.)

[SSL Certificate]

- Adds "Term" to [Regenerate default certificates]
- Adds "Local DNS server – Automatic update" to SSL Certificate Set and Let's Encrypt Certificate

[UPS]

- Adjusts Network UPS IP/Port to be settable while selecting "Network UPS" as the connection mode at [UPS]
- Adjusts that only set clients IP addresses are allowed to visit the UPS service in "Network UPS" mode at [UPS]

[Network]

[Zone Setting]

- Adjusts that a zone with multiple ports can set up "Switch" or "Bridge" mode individually at [Zone Setting].

[Interface]

- Supports bonding at zone0(MGMT/LAN) interface
- Adds settings to [Network Interface Settings > Default Gateway] at [IPv6]
- Adjusts not to restrict setting IP as the condition to save the settings in the static mode at [IPv6]

[Route]

- Adds settings to [OSPF]
- Adds tips to explain about spare gateway setting collision at [Designated Gateway]

[VLAN (802.1Q)]

- Adds settings to [Visit Control > HTTPS]

[PPPoE]

- Adjusts 100 to be the max. number of PPPoE connection
- Adds “AUTO” option to detect MTU values automatically at [Add]

[WWAN]

- Supports “APAL Dongle”
- Adds SYN, ICMP, UDP, Port Scan, and Sandstorm to [Firewall Protection Items]

[Policy]

[Security Policy]

- Adds “Define Search” to [Advance > Search Rule]
- Adds settings to [Advance > DNS Filter] at [IPv6]
- Adjusts that policies are applied to “Service Group”, detailed info can be scanned via tip at [Outgoing/Advance]
- Adds a tip for different subnets at [Source Interface and Source > Add]
- Adjusts that the set VLAN can display interface settings without being activated at [Source Interface > Add]
- Adjusts “Mapped IP”, “Mapped Port” and “Server Load Balance to match with IP in the IPSec segments at [Incoming/Advance]
- Adjusts to display a tip explaining while activating “Application Control” and “URL Access Control/WEB(S)” at a time will trigger mutual affection

[IPSec Policy]

- Adds “Max. Concurrent Sessions for Each Source IP Address” to [Policy > Add]

[Object]

[IP Address]

- Adds “List of External URL” to [Add Device Name and IP Address]
- Adjusts “Define IP” from judging subnet masks to matching clustering at [IP Address Gorup > Search]
- Adjusts not to display IP address options in the 169.254.0.0/16 address range at [IP Address > Assist]

[QoS]

- Optimizes programs to increase packet processing speed

[Application Control]

- Adjusts unlicensed module can be transformed into the new module and a 14-day trial can be activated at [Objects > Application Control > Transform]

[URL Filter]

- Adds “Upload Extension Blacklist” and “Download Extension Blacklist” that can control over files upload/download via webpages to [BW List Setting > Add > Define Black/White List]

[Authentication]

- Adds 2-Step Verification to [POP3, IMAP, RADIUS User > Server Lists > Add]
- Adds 2-Step Verification to [AD User]
- Adjusts to split search results into several pages at [Local User > Search]
- Optimizes 2-Step Verification setting and adds “select all users” and “account search.”

[Service]

[DHCP]

- Syncs UI and self-define IP settings in “Default Gateway” at [DHCP Server > DHCP Server Setting]
- Supports VLAN(802.1Q) interface at [IPv6 > DHCP Server]
- Adds “DHCP Flood Attack” to [DHCP Black MAC]
- Adjusts tip suggestion about undistributed IP quantity at [DHCP User List]
- Adjusts IP segments which can be distributed at [DHCP Server > Interface > IP Address]
- Adjusts to display the setting on UI after finishing setting VLAN at [DHCP Server]

[DNS Server]

- Adds WWAN settings to “Allow Query” at [Interface]

[Anti-Virus Engine]

- Adds “Stop” to “Virus Engine Setting” at [ClamAV Engine/Kaspersky Engine]
- Supports updating virus signatures database offline using USB flash drives at [ClamAV/Kaspersky Engine] (UI will be displayed only when USB flash drive and update files are properly recognized.)
- Updates ClamAV version
- Removes USB upgrade tip during updating at [Kaspersky engine]

[WEB Service]

- Adds Term settings to [Encryption Connection Setting > Re-generate Certificate]
- Adds an option to import by file (.crt or .csr) at [WEB > Encrypted Connection Setting > Re-generate Certificate]
- Updates Mac address database of iOS devices

[High Availability]

- Fixes system upgrades can still be available when HA is not disabled

[Remote Syslog]

- Adds “WAF Log” to [Log Item]
- Adjusts to keep “Log Item” settings when the activation check box is not checked at [Remote Connect Setup]
- Changes a column name (from "SMTP MAIL SET ID" to "Notification ID") in "Log > System Operation"
- Adds "Intranet Protection Log” to [Log item > Advanced Protection] (CEF: SharetechFunction; General: FUNCTION).

[Advanced Protection]

[Anomaly IP Analysis]

- Optimizes programs to reduce resource consumption
- Adjust the default value into 10 (minutes) at [Block Anomaly > Action > Block]
- Adjust the setting range 1-9999 (Kbps) at [Block Anomaly > Action > Bandwidth Limit]

[Switch]

- Adds “Switch Model: GS1900-48, XGS1930-28HP, and XGS1930-52” to [Switch Type > SNMP]
- Adds “Switch Model: ML-9324E, XGS2210-28, and XS3800-28” to [Switch Type > Co-Defense]

[Intranet Protection]

- Adjusts to take the info of [Object > IP Address] into reference at [IP Collision Log]
- Adds tip suggestion for Mac address to [IP Collision Log > Status > Exceed the threshold/Detected the same IP]
- Adds “Event” to the table at [IP Collision Log]
- Optimizes packet processing speed

[Mail Security]

[Filter & Log]

- Adds Term setting to [SSL Certificate Setting > Re-Generate Certificate]
- Supports to import intermediate certificate at [SSL Certificate Setting]

[Anti-Spam]

- Adds DNS Server settings to [Spam Setting > Anti-Spam Setting]
- Adds Notification Language setting to [Spam Mail Notice > Notification Setting]

[VPN]

[IPSec Tunnel]

- Supports IKEv2 and PFS settings at [IPSec Tunnel] and [Auto VPN Server/Client]
- Adds a loading icon while importing IPSec policies

[PPTP Server]

- Adds “Accounts Expiration Date” to [PPTP Account List > Add]
- Adds a new tab [PPTP Server Log]
- Adjusts interface at [PPTP Account List > Import]

[SSLVPN Server]

- Adds “Re-generate Certificate” button to [SSL VPN Setup > Certificate Message]
- Adds “2-Step Verification Validity Extension” with a tip suggestion to [SSL VPN Setup]
- Adds certificate download URL to [Client SSL VPN] and [Client Download Page Setting]
- Adds sslvpn-gui (PC client) 64bit
- Adds “Certificate Message” with a tip suggestion to [SSL VPN Setup]
- Upgrades SSL VPN Server version and reinforces certificate that helps security
- Supports 2-Step verification to sslvpn-gui (PC client) v1.5.0.6
- Adjusts to disable VPN service after applying a factory reset

[L2TP]

- Adds “Account Expiration Date” to [Account List > Add]
- Adjusts interface at [Account List > Import]
- Adds a new tab [L2TP Log]

[Tools]

[Capture Packet]

- Adjusts to select the single port item in bride mode at [Schedule List > Add]

[Log]

[System Operation]

- Adds the Wizard operation log
- Adjusts to record importing action at [Object > Authentication > Local User]

[Status]

[Flow Analysis]

- Optimizes “export” performance at [Flow Rank Search]

NU Series 9.0.2.4 Firmware Update

[Dashboard]

- Adds “WAF Abnormal Connection” to display relevant WAF events
- Adds “report language options”
- Adjusts to display more query logs at [Report > Query]
- Adds an alert to notify users that queries exceed a certain time threshold at [Report > Query]

[Others]

[UI]

- Adjusts to store the certificate files while running the configuration wizard
- Adjusts some English interface texts
- Disables autofill password to enhance security
- Adjusts to hide “password” and adds “new password” items that allow editing to [each password-related interface]
- Adjusts some factory default values

[Configuration > Basic Setting > Login Failure Block Settings] Temporarily block when login failed more than: 5 (times)
[Configuration > Basic Setting > Login Failure Block Settings] IP blocking period: 5 (minutes)
[Configuration > Basic Setting > DNS > DNS Server 1/2]: 8.8.8.8 / 1.1.1.1.
[Configuration > Backup & Restore> Auto Backup]: Default ON (every day, every 1 hour, and backup reserve copies)
[Configuration > Signature Update > Auto Update]: Default ON
[Configuration > number of items to be displayed]: Default 30 items
[Object > Firewall Protection > UDP Attack Detection Setting]: Allow maximum flow 10000 Packet/Second(s)
[Service > DHCP > Primary/Secondary DNS]: 8.8.8.8 / 1.1.1.1.
[Service > Anti-Virus Engine > ClamAV]: Default OFF
[VPN > SSLVPN Server > DNS Server 1/2]: 8.8.8.8 / 1.1.1.1.
[Status > Flow Analysis > DNS Query Rank Search > DNS Query Rank Log Setting]: Default OFF

[System]

- Optimizes system security and adjusts connection requests and restriction
- Optimizes database performance and recovery procedure
- Updates area IP geolocation database
- Upgrades jQuery UI versions

2024/01