HX 9.0.2.3 Release Notes

Available firmware
9.0.2.2 (a41dd178b11e80b09f495410a7d45c05a1e450ab)

Supported hardware models
The HX 9.0.2.3 release supports the following models.

HASH
md5: 986a92fee59f40b6118ed23e10c39258
sha1: b2c1fd6683506620299f9c0e0b866c0bacfd82aa
sha256:
4986ac2cbc0eedbb40db0d285d72aa05719ef2a9e85e4211c389a1f524a6f58e

Installation instruction
- After the update is installed, the system will automatically restart twice. Please wait 3-5 minutes.
- Updated log: 2023-09-14 13:38:35 ==> 9.0.2.2 to 9.0.2.3

Upgrade Notes
[Configuration]
[Basic Setting]
- Adds “LAN Acceleration Mode” to [General Setting]
- Adds “Control Bridge Vlan packets” to [General Setting]
- Adds “Security” (TLSv1.1, TLSv1.2, and TLSv1.3 items) to [Administrative Access > Administrative Access]

[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]

[AP Management]

- Supports the following models:

  Zyxel: NWA90-AX, NWA210-AX, and WAX510D.

  Netgear: WAC510.

[Signature Update]

- Adjusts to allow importing update files without license period restriction
- Adjusts buttons and texts size properly on UI

[SSL Certificate]

- Adds “Term” to [Regenerate default certificates]

[Network]

[Zone Setting]

- Adds “IPv6 Settings” to [Default Gateway]

[Route]

- Adjusts that “Line Detection Method” is chosen NONE, invalid settings will be hidden automatically at [Designated Gateway > Add]

[PPPoE]

- Adds “AUTO” option to detect MTU values automatically at [Add]
- Adds the “Remote Address” option to “Detected IP Address” at [PPPoE Alive Detection]

[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 notifications to different subnets at [Source Interface and Source > Add]
- Adjusts that the set VLAN can display interface settings without being activated at [Source Interface > Add]
- Adds IP options to [IPv6] [Source/Destination]

- Adjusts that policies are applied to “Service Group”, detailed info can be scanned via tip at [Outgoing/Advance]
- Adjusts “Mapped IP”, “Mapped Port” and “Server Load Balance to match with IP in the IPSec segments at [Incoming/Advance]
- Adds “Source IP Address” settings to [Search Rule > Define Search]
- Adjusts to display a tip explaining while activating “Application Control” and “URL Access Control” at a time will trigger mutual affection

[IPSec Policy]

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

[Object]

[IP Address]

- Adjusts “Define IP” from judging subnet masks to matching clustering at [IP Address > Assist]
- Adjusts not to display IP address options in the 169.254.0.0/16 address range at [IP Address > Assist]
- Adjusts “Define IP” from judging subnet masks to matching clustering at [IP Address Gorup > Search]

[QoS]

- Optimizes programs to increase packet processing speed

[Application Control]

- Adjusts unlicensed module can be transformed into the new module and 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]

[Firewall Protection]

- Optimizes judgement of “Block Ping of Death Attack” at [Firewall Protection > Other items]

[Authentication]

- Adds “Allow connection” that can limit online authentication pages to [Auth Setting]
- Adds 2-Step Verification to [POP3, IMAP, RADIUS User > Server Lists > Add]
- Adds 2-Step Verification to [AD User]
- Adds “all users/selected users” to [User Group > Add]
- Adjusts to split search results into several pages at [Local User > Search]
- Adjusts to allow using comma(,) and semicolon(:) in password at [Local User > Add]
- Adjusts to unify tips for checking column format of POP3, IMAP, RADIUS User setting at [POP3, IMAP, RADIUS User]
- Adds to display “usage time” after a successful login

[Service]

[DHCP]

- Syncs UI and self-define IP settings in “Default Gateway” at [DHCP Server > DHCP Server Setting]
- Adds “DHCP Flood Attack” to [DHCP Black MAC]
- Optimized page load speed of the DHCP User List
- Adjusts tip suggestion about undistributed IP quantity at [DHCP User List]
- Adjusts IP segments which can be distributed at [DHCP Server > Interface > IP Address]

[SNMP]

- Adds "Visit Control" and "Restrict Source IP Access" settings
- Adjusts SNMPv1/v2
- Replaces “Service Status & Running After Reboot” option with “SNMP Agent: Enable”
- Removes partially unpublished message items

[Anti-Virus 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.)
- Adds settings to [Kaspersky Engine]
- Updates ClamAV version
- Optimizes ClamAV memory consumption at [ClamAV Engine]

[WEB Service]

- Adds Term settings to [Encryption Connection Setting > Re-generate Certificate]
- Updates Mac address database of iOS devices

[High Availability]

- Adds "Detection frequency" and "Auxiliary detection interface."
- Adds "Service status", "Pause switching and data synchronization", “Current detection status", and "Recent data synchronization time."
- Fixes system upgrade can still be available when HA is not disabled

[Remote Syslog]

- Adds App ID (CEF: cn1=%u; General: APP=%u)
- Adjusts to keep “Log Item” settings when activation check box is not checked at [Remote Connect Setup]
- Adds "Intranet Protection Log” to [Log item > Advanced Protection] (CEF: SharetechFunction ; General: FUNCTION).

[Advanced Protection]

[Anomaly IP Analysis]

- 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]

- Removes "Model: Juniper-ex2200" because the model does not support “SNMP Write” at [Switch Setup > Add > Switch Model]

[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 packets processing speed

[Mail Security]

[Filter & Log]

- Adds tips to each items explaining about communication ports
- Adds “Enable POP3” to [Retrieve Mail Anti-Virus]
- Adds [SSL Certification Set] setting

[Mail Log]

- Adds colors and description to “Message Responses” in order to help determine the types of source at [Today Mail/Mail Search Result]

[SMTP Log]

- Adds colors and description to “Message Responses” in order to help determine the types of source at [SMTP Log Search Result]
- Removes “communication process” at [SMTP Log Search Result]

[VPN]

- Adds a unified search interface to [PPTP Server Log/PPTP Client Log/L2TP Log]
- Fixes failure to delete accounts in VPN log

[IPSec Tunnel]

- Supports endpoint segments for 0.0.0.0/0 at [Enable Routing]
- Adds a loading icon while importing IPSec policies

[PPTP Server]

- Adds “Accounts Expiration Date” to [PPTP Account List > Add]
- Sorts the accounts list in alphabetical order at [PPTP Account List]
- Adjusts to hide “password” and adds “new password” item that allows editing at [PPTP Account List]
- Adds to display accounts in tip suggestion during execution at [PPTP Account List > Delete]
- Adjusts interface at [PPTP Account List > Import]
- Adds “years” to TIME at [PPTP Server Log]

[PPTP Client]

- Sorts the accounts list in alphabetical order at [PPTP Client List]
- Adds to display accounts in tip suggestion during execution at [PPTP Client List > Delete]

[SSL VPN Server]

- Adds “Software Download Page Setting” that allows to define user download pages to the tab bar
- Adds “2-Step Verification Validity Extension” with a tip suggestion to [SSL VPN Setup]
- Adds “Re-generate Certificate” button to [SSL VPN Setup > Certificate Message]
- 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]
- Sorts the Account List in order
- Adjusts to hide “password” and adds “new password” item that allows editing at [Account List]
- Adds to display accounts in tip suggestion during execution at [Account List > Delete]
- Adjusts interface at [Account List > Import]

[Tools]

[Connection Test]

- Adjusts the display of “IP Tunnel” at [Ping > Source IP]

[Capture Packet]

- Adjusts to select the single port item in bride mode at [Schedule List > Add]
- Adjusts file names in chronological order at [Schedule List > Log]
- Adds file size units like Kbytes & Mbytes to [Schedule List/Completed List]

[Status]

[System Status]

- Adjusts that WiFi bridge mode does not affect the display in [WWAN User List]
- Adds “SSID”, “signals”, "Rx Bytes" and “Tx Bytes” to [WWAN User List]

[Flow Analysis]

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

[Dashboard]

- Adds “report language options”
- Adjust to include logs that are being searched

[Log]

[System Operation]

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

[Others]

[UI]

- Adds an alert message about “database restore failed” at [Homepage]
- Adjusts that no pop up alert message will be displayed after the setup wizard has been run at [Wizard]
- Unifies display interface
- Adjusts to allow copy & paste and adds format judgement at [2-Step Verification]
- Adjusts not to generate operation log and file download when executing an export that has no data
- Adjusts some English interface texts
- Disables autofill password
- 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 > Signature Update > Auto Update]: Default ON

[Configuration > number of items to be displayed]: Default 30 items

[Network > Interface > Visit Control > SNMP]: Default OFF

[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.

[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