NetEyez

NetEyez Version 3.1
Release Notes
June 27, 2024

June 27, 2024: NetEyez V3.1 Initial revision

1. About this release

1.1. Model

This release can be applied to the following models.

● NTEZx-01GC-R2	(NetEyez 1GbE Rackmount)
● NTEZx-10GM-R2	(NetEyez 1/10GbE Rackmount)
● NTEZx-10GM-S-R	(NetEyez Security 1/10GbE Rackmount)

The package for NTEZx-10GM-SP-R and NTEZx-10GM-S-P is under developing.

1.2. Upgrades

- NetEyez V2.5, the setting can be imported but the acquired data will be initialized.
- NetEyez V3.0.1, you can carry over previously acquired data.

2. Main changes in NetEyez Version 3.1

1. Support SYNESIS NEXT (SYNESIS Next), that is linking NetEyez to Synesis to analyze Capture session and traces in Synesis machine.
2. Network management interface enhancement: Implemented netplan configuration file method for improved network management and setup. [#5549]
3. Improvement: Added loading status indicator when retrieving logs by clicking the Get button for a smoother user experience.

3. Major issues fixed in NetEyez V3.1

1. Log data imported and exported from Splunk is not functioning correctly.
2. [Improvement request] About the data displayed in the created report and the data displayed in the monitoring history. [#4970]
3. Security bug: Cannot update IoC records if their timestamp is older than six months. [#5519]
4. Security event detail information for [content] and [PCRE] is not displayed. [#5518]
5. Using the "&&" symbol in a filter on the decode page causes the filtering process to fail. [#4960]
6. When editing, "_Branch Office" is added to the name. [#4460]
7. [VLAN] In the Site-VLAN modal under "Setting>Monitor>Site>VLAN", the VLAN ID example is listed as a colon (:) instead of a semicolon (;).
8. The number of cases is different before and after zooming the map in [TopN Attacks] [#5400]
9. Zooming in on the map with [TopN Attacks] makes the pins disappear. [#5401]
10. Role cannot be changed from administrator to analyst by admin user. [#5576]
11. Proxy setting issue where NetEyez SaaS and IoC download functions did not work through the proxy. [#5553]
12. When downloading IoC failed due to the incorrect configuration, the capacity of OS would continue to increase. [#5623]

4. Restrictions in NetEyez V3.1

1. In the SYNESIS Next, only the 1G link of management ports are confirmed.
2. The Security Event download and decode icon is disabled when data-source select capture session.
3. Importing and exporting settings currently doesn't support SYNESIS probe configurations.
4. ILM applied to file-path analysis for capture session, cause upgrade package can't keep trace file's analysis result.
5. When selecting a time range that includes the latest hour, data may not match due to the ongoing roll-up task. Please select a time range one hour prior to avoid any discrepancies.
6. The maximum capture session size supported in this release is 50GB.
7. Please ensure that the NetEyez and Synesis platforms are set to the same time zone.
8. The logic of IoC license period has an error. Even if it's available, the update of IntSights and Proofpoint would sometimes fail.
   - ➢ This issue will be fixed in the next release.
9. If the proxy settings are enabled, downloading Snort Business would sometimes fail.
   - ➢ This issue will be fixed in the next release.

5. Major Changes in Past Versions

5.1. Major Changes in NetEyez Version 3.0

1 NetEyez Security and NetEyez data are now integrated.

2 Support for Inbyte/Outbyte and InPacket/OutPacket in Connection Flow.

3 Implementation of Expert System Support.

4 DLC & VLAN Support.

5 On the protocol setting page, a list of DPI-supported configurable protocols is provided. However, it's important to note that protocol sniffing takes precedence over port configuration in determining the protocol for analysis.

6 Rename all widgets that have VLAN-based site information to avoid confusion with IP-based Site.

7 Make the "Baseline Updated Time" clearer in the Baseline Alarm configuration modal by adding both Start and End times.

8 Application statistics

8.1 Supports Statistics per application.

9 Charts

9.1 Additional averaged value in baseline trend chart.

9.2 Remember Zoom in/out status on trend chart while changing icon/page.

10 Tables

10.1 To be able to sort by Host pair communication volume.

11 NetEyez Security

11.1 Consolidating Duplicate Events by Status in NetEyez Security's Event Manage.

11.2 Enhances event filtering by incorporating NOT operator, IDS, and IOC security-specific details such as CVE, SNORT-ID, and score.

11.3 IoC database updated based on the latest year's data.

11.4 Enrich the metadata section of security events with more threat intelligence information, such as ASN Info, Location, Signature ID, MITRE Attack Info and Malware Family.

12 Capture Actions

12.1 Pause and Resume capture operations to support filter change while capturing to file.

12.2 Developing Capture Actions Based on SNMP Alarm Notification.

13 Capture Upload Files

13.1 Multiple selections for deleting capture and upload files.

13.2 Establishing Trace Banker Support for Data Capture to External Storage Files.

14 Site Enhancements

14.1 Branch/VIP/Site separation and VLAN as Site.

14.2 Enable batch registration of sites using csv files.

15 Email Notifications

15.1 Multiple users support for email notification.

15.2 Can configure nameless e-mail server.

16 Others

16.1 Added packet number to decode details pane.

16.2 Separated alarm and report scheduling.

16.3 IP Global Search box grey out while in real time.

16.4 Create addition manual (KPI) user menu icon.

16.5 Supports Chinese localization.

5.2. Major Changes in NetEyez Version 2.5

1. Baseline trending chart added for supported KPIs. Please see manual for more details
2. Multiple channels traffic aggregation like NPB (Network Packet Broker)
3. Retry count and multicast widget customization support.
4. IP address search from entire database
5. Alarm can be notified now like report notification.
6. Alarm content customization for Mail notification.
7. Enhance mail server setting for Mail notification.
8. Alarm status management.
9. New baseline alarms (Global – CRT, NRT, and ART) support
10. New alarm Channel-based DLC alarm support
11. New “Delete All” function for captured files and uploaded files under Data Collecting->Capture page.
12. Intuitive GUI support for data restore/backup on Setting->Monitor-General page.
13. Trending chart improvement – higher granularity
14. The column width of list table can be adjustable now.
15. Progress bar display to show status for decoding large trace file.
16. Out of resource handling for CPU, Memory, and Disk with Warning at the first threshold and warning and stop operation at 2nd threshold.
17. ELK version upgraded from v7.10 to v8.3
18. T-shark upgrade from v3.2.3 to v3.6.5
19. New filter (Flow, Protocols, and sites) setting for real time monitor and packet capture.
20. Advanced filter instead of site filter support for real time monitoring and pCap decode.
21. HTTPS support for launching Kibana web page.
22. Added total packets/bytes for host-based related statistics table.
23. Second-based support for Multicast IP/LLC - trend chart and table content
24. New Retry trend chart on performance page.
25. Capture File Name adds filter name info automatically if software filter is selected on real time monitoring.
26. Changed “Unknown “Application to “Protocol + Port.”
27. Capture File Name is based on filter plus timestamp.
28. Supported Version up for v2.0B948 settings.

29. Added restore button for restore setting.

Internal notes

30. Packet drops notification support.

6. Issues Resolved in Past Versions

6.1. Issues Resolved in NetEyez Version 3.0.1

1. Resolved the bug related to resource application conflicts to fix connections log to ELK.
2. Resolved the issue where restarting the machine prevented login in NetEyez due to Domain/DNS aggregation.

6.2. Issues Resolved in NetEyez Version 3.0

1. CSV/PDF Export: Units have been removed from exports in CSV/PDF format.
2. Error Icon Display: If an error icon appears in the IP range text box in the "Branch Settings/Site" modal window, it will now disappear upon canceling and reopening the window.
3. Session Timeout: The session timeout time now has consistent lower limits for values set with cursor buttons and direct input.
4. Analyst Privileges Display: In the "Analysis>NetEyez" screen, the "Setting" button in the table on the "Branch Office" tab is now correctly displayed with analyst privileges.
5. Sorting Issues:
   - Sorting issues in various sections have been resolved, including:
   - [Monitoring and Report] > [Created Report] table "Description" column.
   - Sort button in "Branch Office" table.
   - Sorting in [Setting][Alarm] Title, [Setting][Alarm] Alarm description field, and [Setting][Alarm Scheduler] Description and Enable fields.
   - Sorting in [Monitoring and Report] > [Report Scheduler] to correctly sort enabled states.
6. Language-related issues have been fixed, such as English titles appearing in Japanese/Chinese settings.
   - The description field in "Setting>Monitor>Site>IP Range" is now searchable.
   - The "Setting>Monitor>Site>VLAN" description field is now searchable.
7. Alarm description popup does not appear on the Class tab and Host tab of the "Alarm>Alarm" screen.
8. Security Beta Fixes - Fixed feedback bugs:
   - Alarm settings content is now correctly displayed in alarm emails (only in test emails).

- Japanese descriptions in the Full Stop status of the Capture section are now accurate.
- In Decode, query rule case inconsistency has been addressed.
- When selecting standard templates, custom footnote content is no longer erroneously displayed.
- Improper error message displayed when non-English characters are entered while typing application class name.
- When network report is enabled for the dashboard, the Dashboard>topology page disappears.

9. When a site is specified in the IP range and analyzed, but all of them become Others.
10. If an error icon is displayed in the IP range text box in the "Branch Settings/VIP/Site" modal window, the error icon remains displayed even after canceling and reopening the window.
11. [Monitoring & Report]: Even in Japanese/Chinese settings, the "Top Threats by Country" in the name field is not translated.
12. [Setting][Monitor]: When creating a new IP address range in Settings> Monitor > IP Range, if you leave the "Description" field blank and save it, "null" is written in the description field.
13. [Dashboard]: "VLANs within each Site" widget is not updated when the date and time are specified in the Monitoring History on the user dashboard with the "VLANs within each Site" widget added.
14. [Setting][User Manager]: Even if you set a User Photo, the file name is not saved in the User Photo item in the User edit modal.
15. [Improvement request][Setting]: File name after downloading PDF/CSV.
16. When the notification rule is set to Syslog in [Setting > Event Notification], the notification can be saved even though the port number is not entered.
17. TopN Node /TopN Application/TopN Host widget support configurate TopN
18. In TopN VLAN, TopN is still displayed in English even if the locale is set to Japanese.
19. Discrepancies between left-side menu labels and page labels
20. Real-time event detection without email notifications
21. Non-functional "Setting>Monitor>Site>VLAN" enable/disable switch.
22. Modified fluentd plugin for security.
23. Report Drilldown links with I18n.
24. Slack event notification issues with URL encoding
25. Zeek failing to start when installing different VM versions at various paths.
26. In host statistics, the bandwidth and response time trend graphs for individual IPs were not displayed correctly when the selected time range exceeded one hour. This has been corrected.

6.3. Issues Resolved in NetEyez Version 2.8

1. Submenu Persistence: Submenus can no longer remain open after entering search mode in the navigation menu.
2. IP Matrix Chart: We've resolved issues related to the IP Matrix Chart to alleviate browser CPU load.
3. Localization: Even when the Japanese locale is selected, the Baseline display options in NetEyez/Analysis/Application/General are now correctly displayed in Japanese.
4. Custom Dashboards: We've addressed the issue where Custom Dashboards were not supporting pcap data sources.
5. Baseline Alarm Settings: Changes have been made to Baseline alarm settings, including Baseline Updated Time and Baseline Reset Time.
6. Baseline Alarm Status Labeling: The Baseline Alarm Status in the Baseline Alarm setup GUI now features clearer labeling as "Enable/Disable," and we've standardized test for all alarm status settings.
7. Mapping Issues: Map-related concerns, such as duplicate entries for the United States and discrepancies between the left-hand menu and page labels, have been resolved.
8. CSV Export Translation: Corrected translation issues in CSV file exports under the "security" section.
9. Data Loss: We've fixed data loss problems that occurred when enlarging data on the Network Device page under the "trending" tab.
10. Fixing internationalization bugs, which include
    - [Setting][Event Notification] When Japanese/Chinese is set, "System Alarms" in the Event Customization modal is not translated.
    - [Setting][Monitor][Filter][Event] When setting Japanese/English, "NOT" is incorrectly displayed in the event filter creation modal.
    - Wording in tables and page buttons do not change when switching languages.
    - [Setting][Alarm] When setting Japanese, threshold validation error wording is incorrect.
    - [Setting][Alarm] Title is written in English even in the Japanese/Chinese setting.
11. [Setting][Security][BeatSensor] "LIST_TABLE_CONTENT.isEmpty" is displayed when switching language with no data.
12. [Setting][Monitor][Protocol] Unable to register on DPI tab.
13. In the "Setting>Monitor>NetEyez" screen, the IP addresses in the table are omitted from the Branch Office tab, even though the column width is wide enough.
14. Error popup in "Setting>Monitor>Site>VLAN" when VLAN ID is out of range is still in English.
15. Long strings in the "Description" field cause the columns after "Range" to be inoperable.
16. [Setting][Alarm] Tooltips in full screen are out of alignment.
17. The table heading "Web Server Agent" in Analysis > Application > HTTP > User Agent is misleading.

18. [Setting][Monitor][NetEyez] Even in Japanese/Chinese settings, "Custom" is displayed in the Your Internet Bandwidth pull-down.
19. [Setting][Channel Group] When you mouse over the enable status switch, a tool tip will be displayed.
20. Sort by table "packets" button does not work on the Site-VLAN tab of the "Analysis>DLC" screen.
21. [Setting] Menu item names and breadcrumbs do not match.
22. [Monitoring and Report] Breadcrumb list are not displayed properly.
23. Alarm description popup does not appear on the Class tab and Host tab of the "Alarm>Alarm" screen.

6.4. Issues Resolved in NetEyez Version 2.7

1. The security event country selection will only display valid countries with recorded attacks.
2. The payload graph on the right end of the trend chart may not show any data.
3. Importing settings will delete logs from ELK related to trace analysis results, and the trace status will change to analyzable.
4. Trend graphs for bandwidth and response time of individual IPs may not display correctly if the selected time range exceeds one hour.
5. Graphs will not be displayed on the overview tab of the file monitoring screen if there is no data available.
6. The "Save As" feature in the decode page has been enhanced to show a red alert if the file extension is not in the pcap or pcapng format.
7. It is currently not possible to change the permissions of a newly created account.
8. When entering a value of 19 or more digits as the capture period in minutes, moving the cursor to the right of the text box may result in exponential conversion. The maximum value is currently set to 43200 minutes, which is equivalent to 1 month.
9. Capture duration is now controlled to 1 month with a unit of minutes.
10. Host-based statistics are not displayed when selecting more than one hour.
11. Edit protocol was not taking effect.
12. Decoding Chinese channel names caused garbled characters.
13. Fixed the bug where the configuration of trend charts was not taking effect on the TopN Thread by Country page.
14. Completed some Internationalization bug fixes.

6.5. Issues Resolved in NetEyez Version 2.6

1. Reversion of configured report logo to the default one
2. Overlapping IP addresses, subnets, or address ranges in branch, VIP, and site definitions causing incorrect analysis results
3. Greyed out IP Global Search box in real-time.
4. Widget time selection not working for maximized view.

5. Restoration of 10 as an option in Widget/template
6. Correction of sorting direction toggles by revisiting the tab
7. Byte sorting not displaying data.
8. Change in the number of lists displayed in the Setting-> Monitor- > Protocols -> Classes tab page.
9. Correction of annotation start position in the report template edit screen.
10. Notification of completion of analysis of pCap file not displayed.
11. Difficulty in using Analysis > NetEyez tabs and Settings > Monitoring > NetEyez tabs due to different tab order.
12. Display unit of trend chart in the remote access tab shown as "ns".
13. Failure to draw graphs in Protocol tab > Host-based Statistics tab > Protocols tab in Network.
14. Failure to switch to the Overview tab display when reselecting Analysis > Network while displaying anything other than the Overview tab.
15. Misbehavior for user/application byte sorting
16. Display of an inappropriate error message when registering or updating a duplicate site name in the site settings
17. Automatic deletion of widgets in templates
18. Hiding of one integer digit and labels below the decimal point
19. Inability to sort application-based statistics by bytes.
20. Display of incorrect annotation "Some well-known SaaS service goes here".
21. Inability to close submenu after entering search mode in navigation menu.
22. Addition of frame number in decode details pane.
23. Internationalization bugs fixed, including navigation not being localized, "No Data" not being translated, and no I18N support on trend charts.
24. Translation of #Active User / User JP in Microsoft Page
25. The configurable range of port numbers is incorrect. All port-related modals are fixed and updated accordingly.
26. Host-Statistic - Trend graphs of bandwidth and response time for individual IPs are not displayed correctly if the selected time range is more than one hour.

6.6. Issues Resolved in NetEyez Version 2.5

1. Made some of widget titles more meaningful. Ex: “Performance” changed to Microsoft performance
2. Added back marginal to availability status. It has Excellent, Marginal, Critical status now.
3. Added “-“support for name of email address.
4. Table widget can adjust width and show all information in Alarm detail column.
5. It shows site table when click on Site trend chart on Analysis – Application- Performance
6. Reports generation should be based on Language selection.
7. The details of Customized alarm description are incorrect
8. Chinese locale issue for navigation menu

9. Misbehavior for user/application byte sorting
10. Port scan small threshold hang by importing settings of B948.
11. Admin user cannot be deleted now.
12. Make title and description consistent with scheduler list and new schedule modal box.
13. The Host IP address appears in the Host2 column.

7. Restrictions Found in Past Versions

7.1. Restrictions Found in NetEyez Versions 3.0

1. Support for the NOT operation across all filters, including flow, protocol, and site, is not available.
2. Recorded statistics and KPIs in ES will be removed when the aggregation status is toggled on or off.
3. Some standard threshold values for alarms are different from those described in the User's Guide
4. Name resolution results are retained when aging erases previous analysis results, but this is not explicitly stated in the user's guide.
5. The behavior of packets with IP checksum errors differs between real-time monitoring and other types of analysis (e.g., pcap). Real-time monitoring counts the packets and bytes as 0 (the network application requests retransmission of the correct packets for packets with checksum errors), while analysis such as pcap file counts them also as the number of packets and bytes observed. (This is an artificial checksum retransmission. (This is a convenience for analyzing packets that contain checksum errors created without artificial checksum recalculation).
6. The application-specific statistics function is not described in the user's guide.

7.2. Restrictions Found in NetEyez Versions 2.5

1. Data cannot be kept from previous versions due to database format changed.
2. The status of Zoom in/out on trend chart is only supported on the selected page. The status is reset to original after leaving page.
3. No warning if new capture file name is already in capture list table. The existing one will be overwritten.
4. Selection on trend chart such as IP address will be reset in 30 seconds in real time mode.
5. No I18N support on trend charts
6. Submenu can no longer be closed after entering search mode in navigation menu.
7. The scrollbar is not shown on TopN host widget. Also, the line is displayed outside of the frame.
8. Limited setting import from NetEyez v2.0 B948 and v2.0 Patch B961 to NetEyez2.5. The Reports and Template page, Setting-Monitor-General page and Image for user created cannot be imported.

9. If IP addresses, subnets, or address ranges overlap in branch, VIP, and site definitions, correct analysis cannot be performed. Currently, a warning message is displayed to avoid duplication within each category, but cross-category checks are not performed.
    - Any duplication will cause at least the following symptoms:
        - ✧ Analysis results are not displayed in the branch widget of the NetEyez view.
        - ✧ Results are not displayed even if All is selected first in Analysis>NetEyez branch tab. It becomes visible when you select a specific branch.
        - ✧ Subnet definitions for branches and sites are not reflected correctly.
10. IP global search with real-time monitoring (when you select monitor as the data source), the search will stop every 30 seconds.
    - The search is stopped every 30 seconds, even though the contents of the search box and the IP global search checkbox settings remain the same. Toggle the IP Global Search checkbox to recover.
11. Sorting and search on the following pages:
        - ✧ Analysis > Network/Host
        - ✧ Analysis > Network/IP Matrix
        - ✧ Analysis>Application>HTTP/Server,
        - ✧ Analysis>Application>HTTP/Transaction,
        - ✧ Analysis>Application>Microsoft/Transaction,
        - ✧ Analysis>Application>Performance/Transaction,
        - ✧ Analysis>Application>Performance/Proxy Server/Server
        - ✧ Analysis > Application > Performance/Proxy Server/Transaction,
        - ✧ Analysis>Application>Performance/Remote Access
        - ✧ Analysis > Application > Performance/Server
    - The search is for the data in the list table. If IP global search is checked, then user can search IP address from entire database. For all sorting (User, Application, bytes, and packets), it will sort from the whole data base, not just list table.