NetBrain® Integrated Edition 8.03

Release Notes

Version 8.03 | Last Updated 2020-08-03

Contents

1. Summary

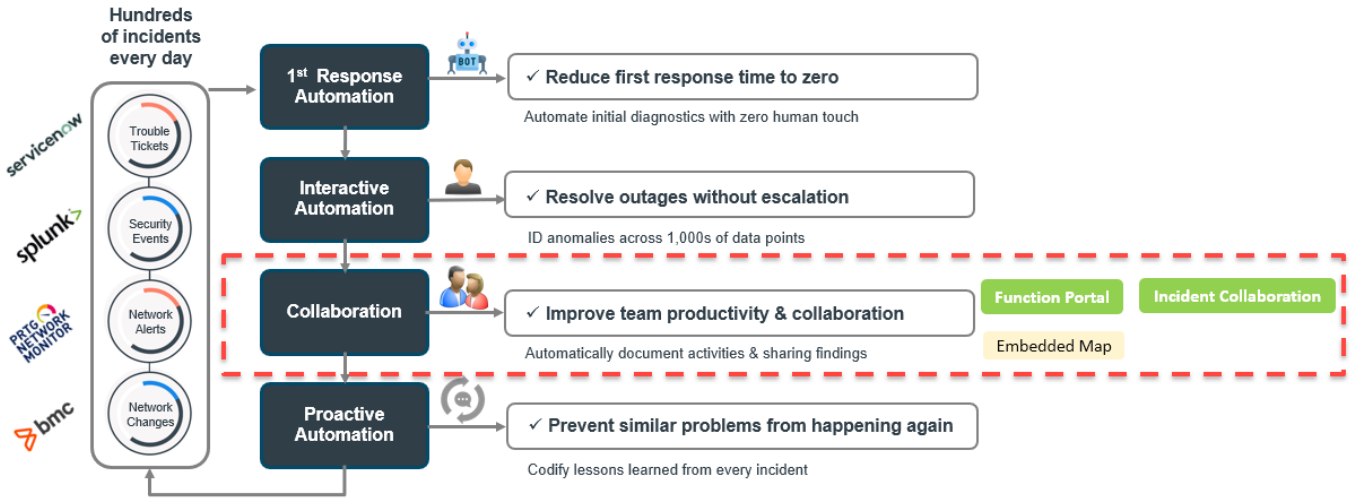
NetBrain Integrated Edition 8.03 (IEv8.03) introduces several new features and feature enhancements, including:

- Function Portal New — to enable network engineers to collaborate with cross-function teams who do not have NetBrain seat licenses.
- Device Health Report New — to assist diagnosis with the visibility about the overall device-level health, such as live access status, topology connection status, key network data existence, etc.
- Enhancements to Domain Health Report, reporting cloud health and path calculation health.
- Enhancements to CLI Automation, including device qualification before CLI automation, etc.
- Enhancements to Granular Data Comparison, including comparing with instantly retrieved live data, comparing selected texts and table columns, and a few usability enhancements.
- Enhancements to SDN, including Service Graph Support and Multi-Site Support.
- Enhancements to Discovery, including Bulk Select API Servers, View History Result, Toggle Additional Operations, Export Access Logs.
- Enhancements to External User Authentication, including mapping user roles and privileges from TACACS+ to NetBrain, and syncing selected user data for LDAP/AD Authentication.
- New SSH fingerprint authentication to improve network security by obtaining and verifying the Fingerprint Key.
- Enhancements to Service Monitor, Email Alerting, etc.
- New Tech Support
- Enhanced Platform Framework, including custom interactive commands and command block in driver definition, etc.
- Enhancements to Path Framework, including replicate active path calculation with auto-saved data, L3 active path calculation with baseline data, etc.
- New REST APIs
- Enhancements to Deployment and Installation

2. New Features and Feature Enhancements

2.1. Collaborative Function Portal to Work with Maps and Paths

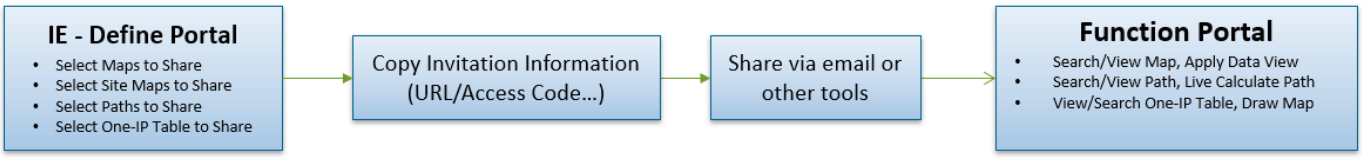
IEv8.03 introduces the Function Portal feature to enable network engineers to collaborate with their colleagues who do not have NetBrain seat licenses. This is one of the key approaches to achieve the goal of MAP EVERYWHERE and improve team productivity and collaboration. With Function Portal, external users from different teams (IT engineers, security engineers, etc.) can gain fast and free access to use selected IE functions and resources through a website, including dynamic mapping, A/B path calculation, and One-IP table query.



Note: Compared to Embedded Map, Function Portal does not require customer's effort to provide a hosting environment or write scripts for initial setup.

Note: Incident Portal Collaboration will be available in the next release to enhance the portfolio.

Use Flow



1. Senior Network Engineers Set Up a Function Portal and Share its URL
2. End Users or External Users Access the Portal
    a. View Dynamic Maps
    b. View A/B Path Result and Calculate Live Path

c. Search One-IP Table and Map Devices

The typical usage for Function Portal includes:

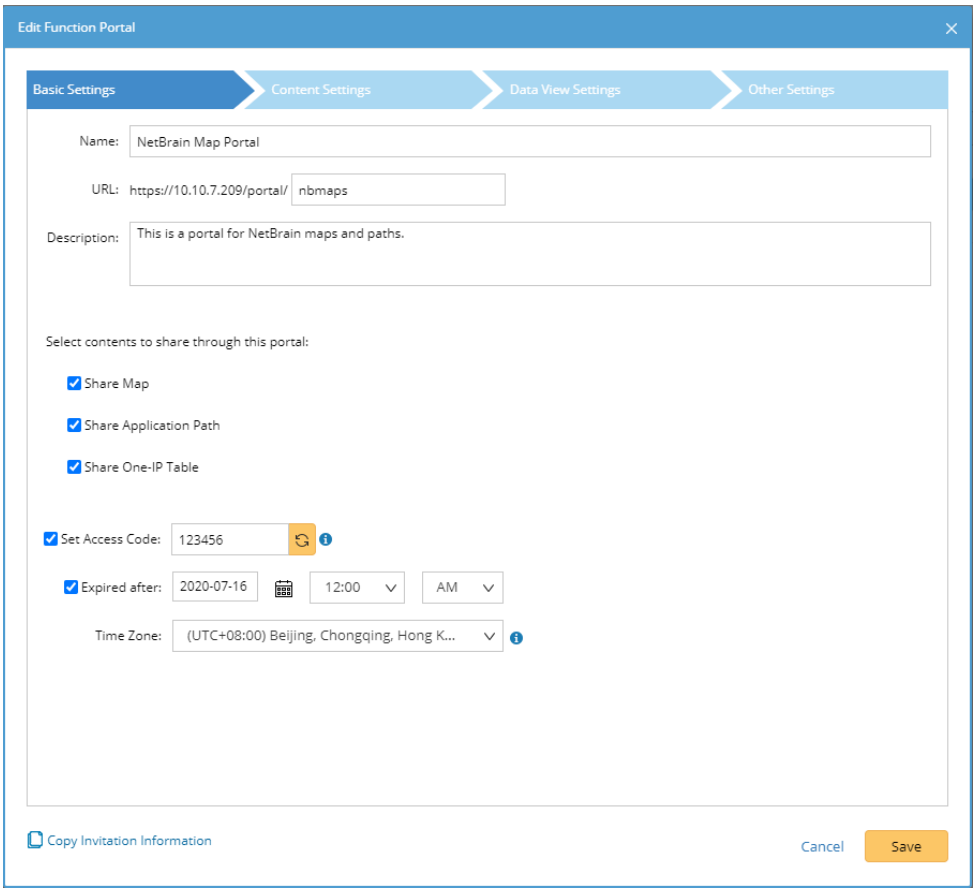
- Publish selected information (Maps/Paths) to different teams without seat licenses required.
- Create a set of portals for key technologies, application flows, sites, or security domains to aggregate network knowledge.
- Build dynamic mapping into existing documentation and collaboration flow to replace static Visio diagrams.

2.1.1.Set Up a Function Portal

Note: Only the users with the Function Portal Management privilege granted can create function portals.

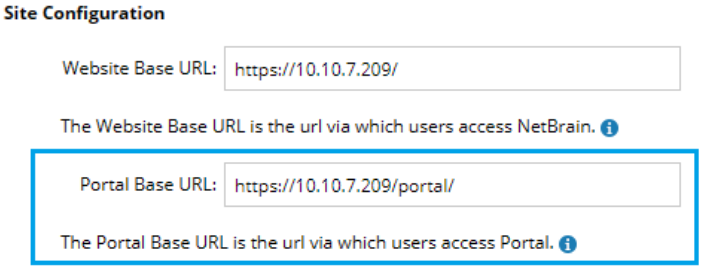
1. Define Basic Information

Senior network engineers can create a function portal by defining a portal name, a query string of URL, NetBrain functions including Map, Path and One-IP Table, and enabling the access code login with an expiry date.



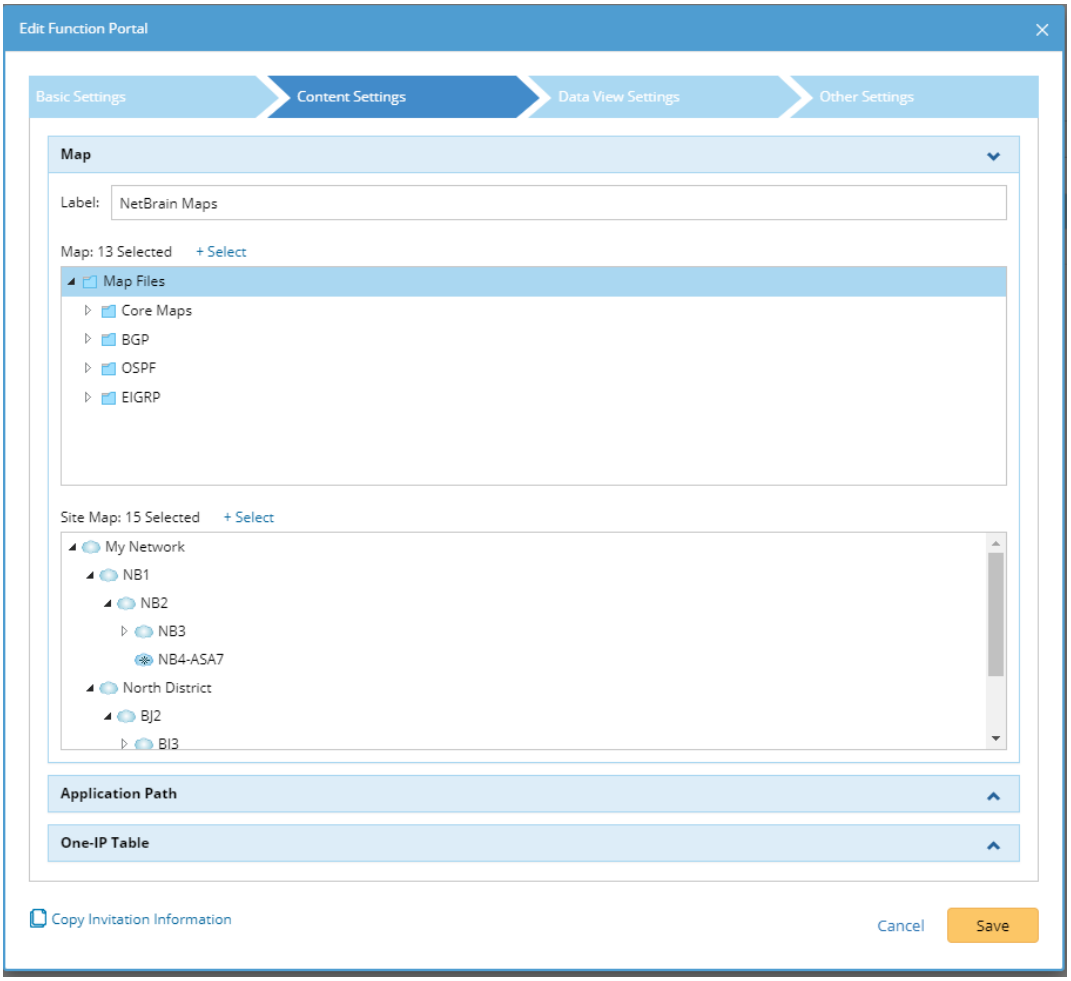
Note: The **Set Access Code** check box must be selected to allow people who do not have NetBrain IE user accounts or portal user accounts to log in to the function portal.

Note: The query string of the URL is the identity of each portal, and must be unique in the system. The base URL is a system-level setting, which can be configured by the system administrator.



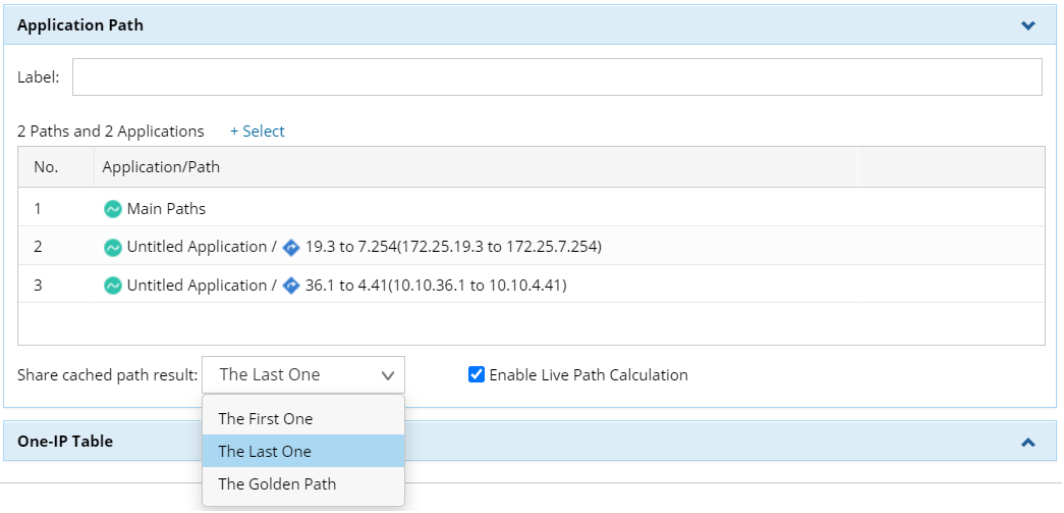
2. Select Maps and Paths

In the context of NetBrain functions (Map and Path) selected in the previous step, senior network engineers can continue to select multiple map files and application paths that they want to share with others through the portal.

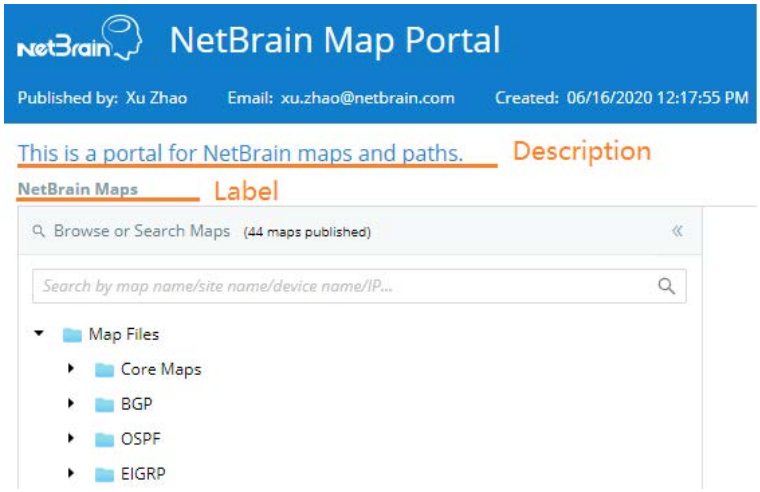


Note: For the selected paths, you can select to publish the first/last calculation result, or the golden one. By default, the last result is selected, and the Live Path Calculation is enabled. The prerequisite of calculating live paths through a portal is that

the Application Assurance Module has been purchased.

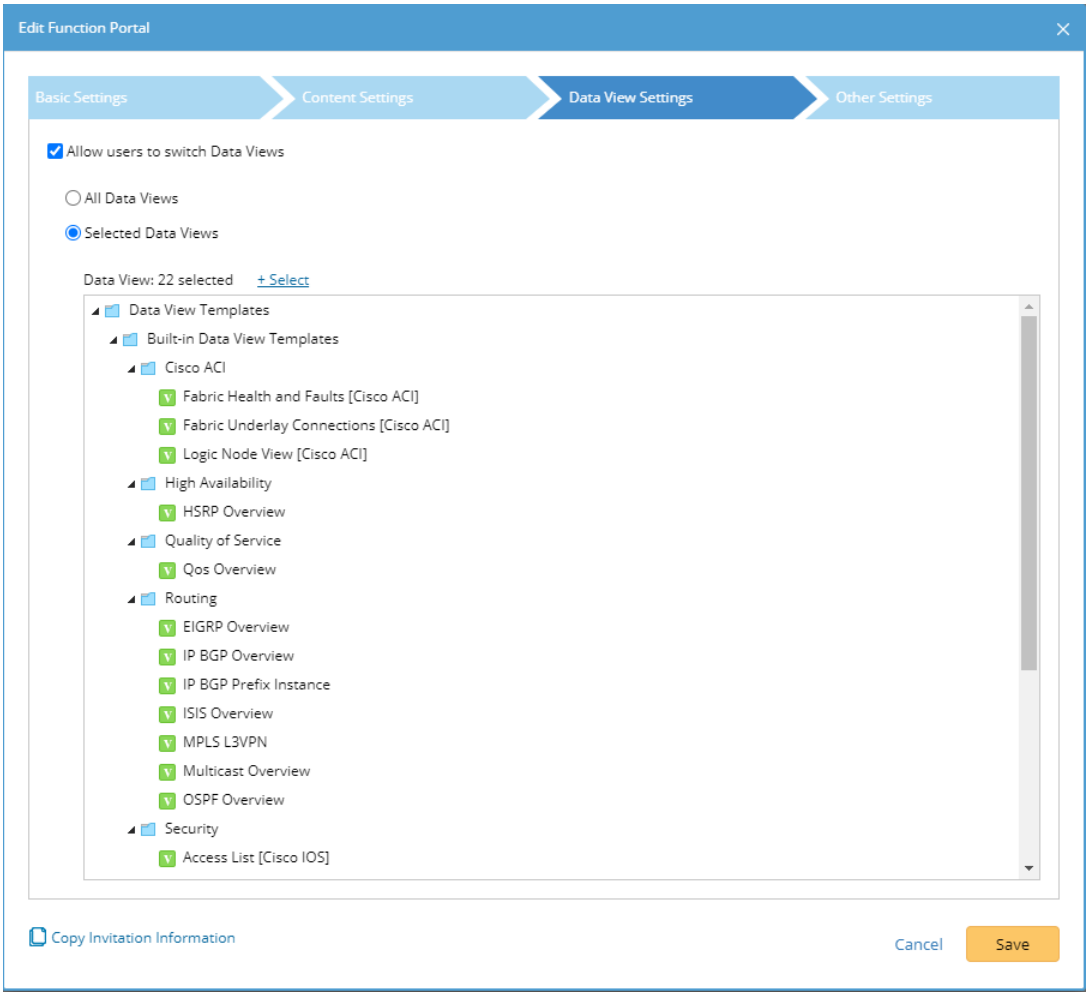


Note: The label setting is optional, which will be used as the area title to introduce the content.



3. Select Data Views

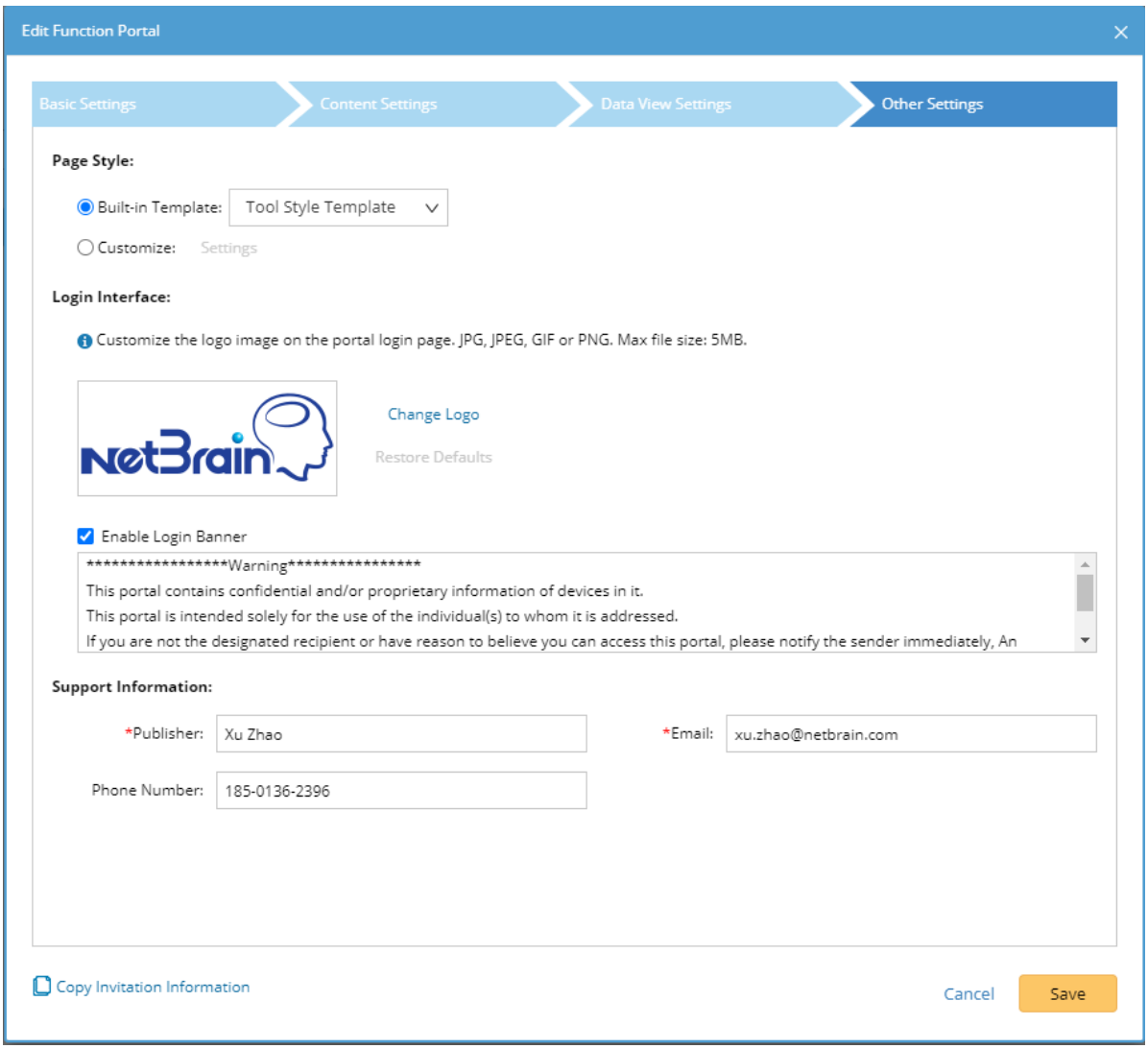
Senior network engineers can determine whether to publish all data views or only selected data views for other users to toggle on the portal.



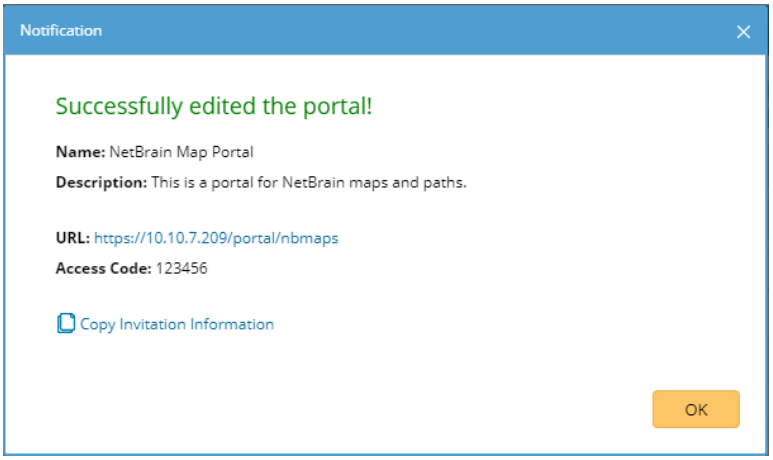
Note: Similar to the qualification in the IE system, only qualified data views against devices on a map can be displayed in the Data View pane.

4. Define Page Style and Others

Before publishing the portal, senior network engineers can select to customize the page style, login interface, and add contact information.



After saving the definition, copy the invitation information from the following prompt and paste the invitation in an email or instant message to share the portal with your colleagues.

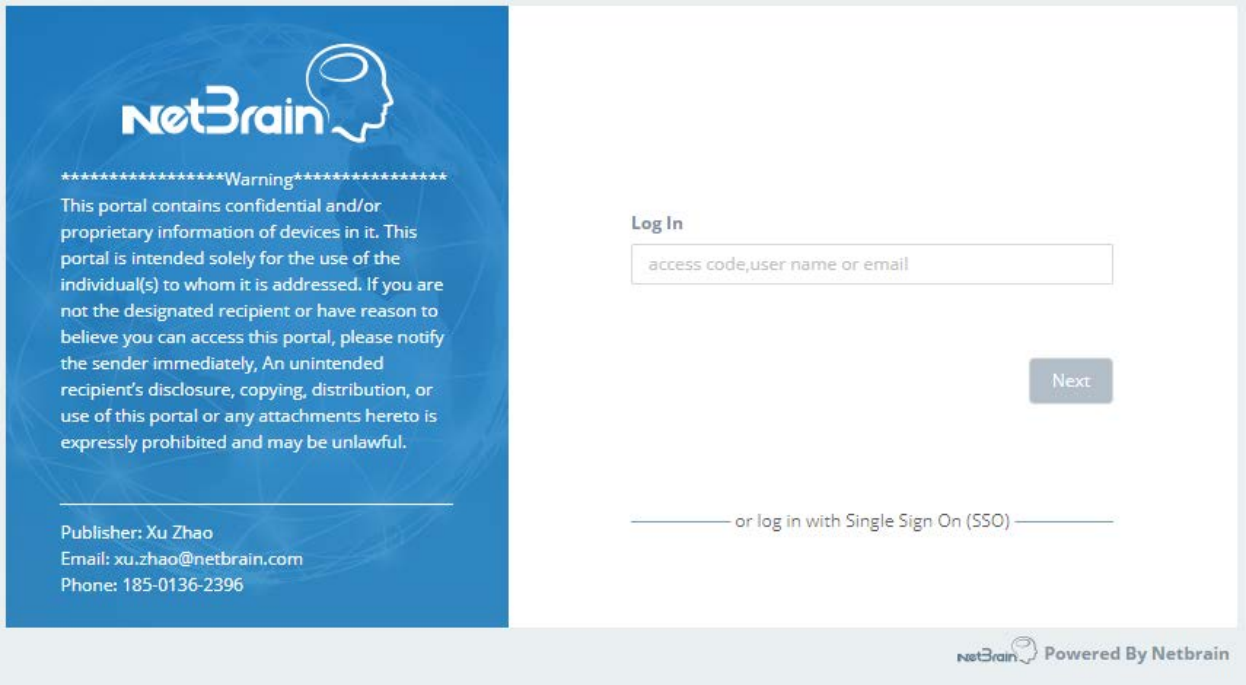


2.1.2.Access a Function Portal

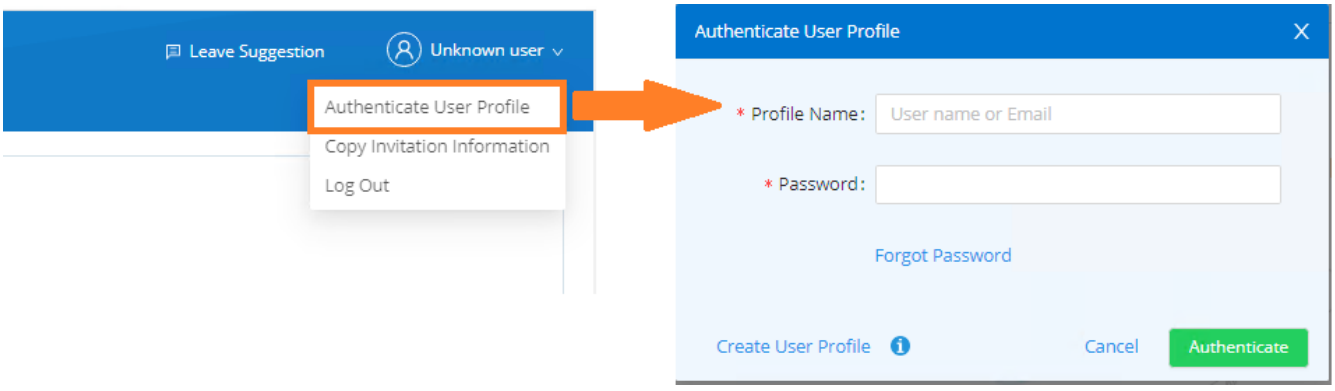
The system offers two access methods for each function portal:

- **Username/Password Login** – users with IE accounts or portal accounts can log in by using their usernames and passwords, or email addresses.
- **Access Code** – both external users who do not have any accounts and IE/portal users can use an access code to access a portal.

  Prerequisites: Access code login must have been enabled when senior network engineers set up the portal.

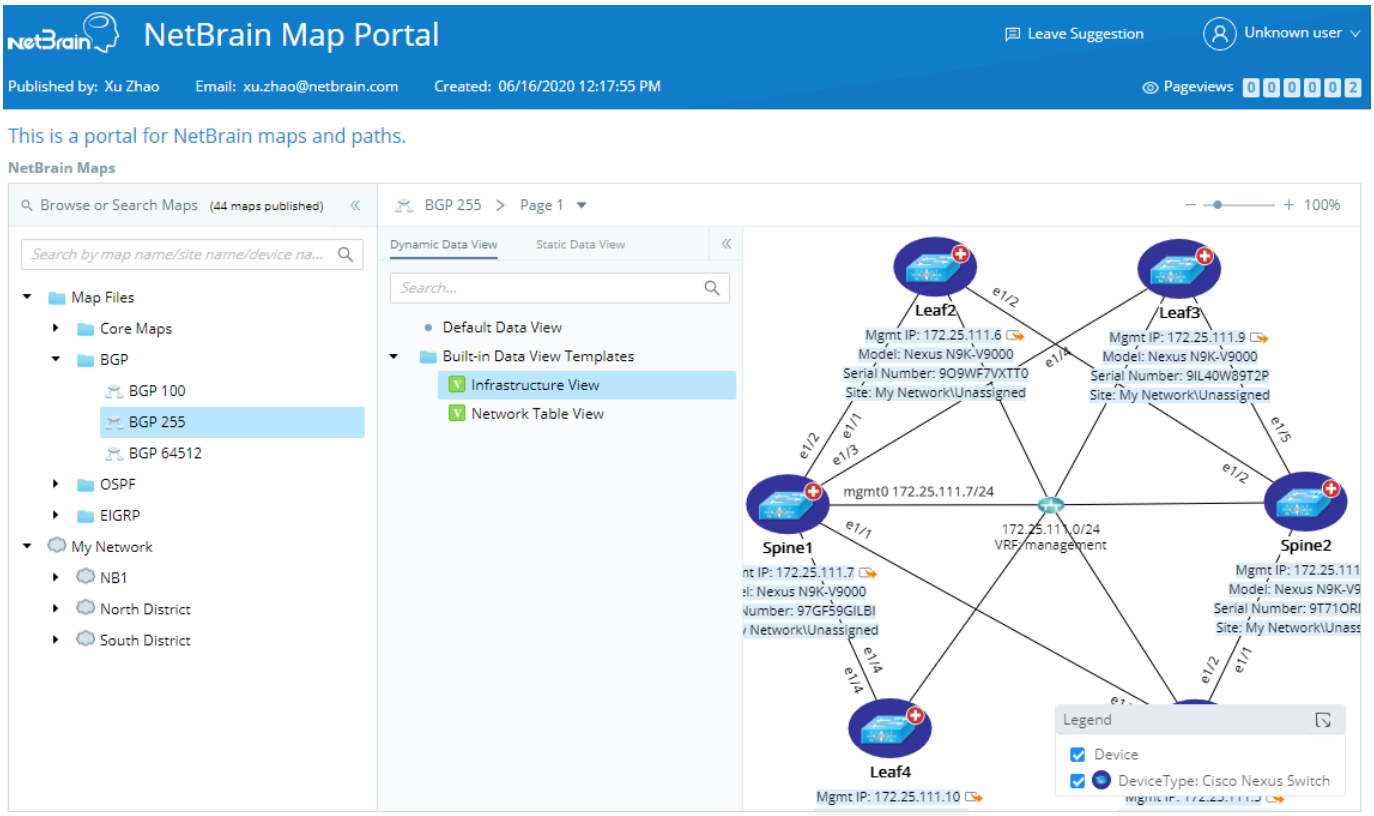


Note: By using an access code to log in, you will be recognized as an unknown user, and you can select to create a user profile for recognition. User profile is only a visual display of personal information associated with a specific user, but cannot be used for portal login.



2.1.3.View Dynamic Maps through Function Portal

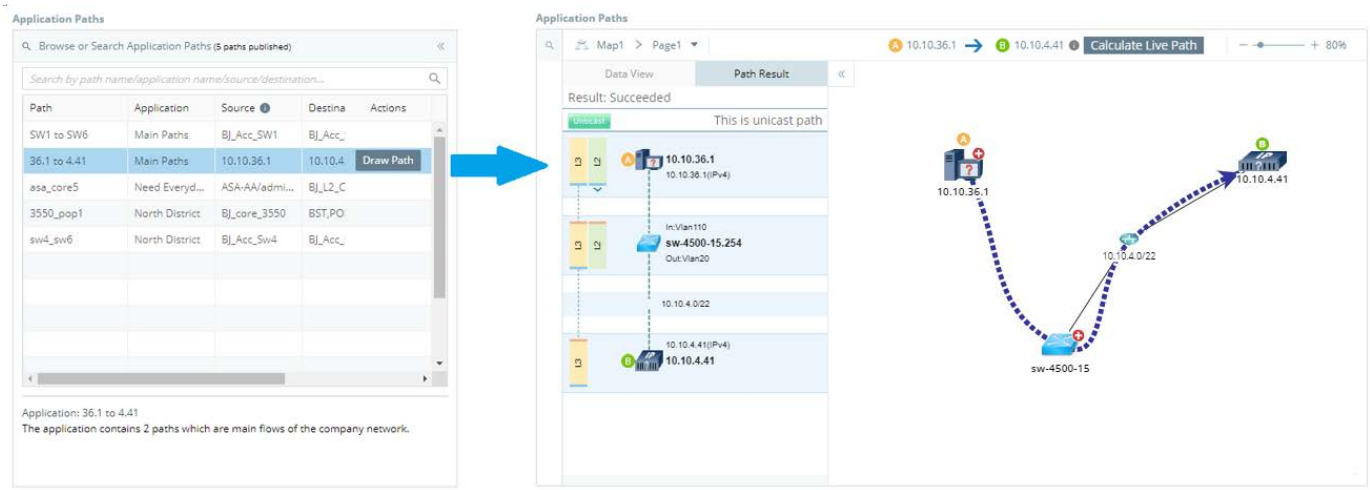
Through the function portal, external users can expand the map tree to view the shared maps, including site maps, and double-click the target map to display it in the working area. Furthermore, they can select to apply a data view to the devices on the map. The data source for data views defaults to the current baseline (the latest data saved in the IE system).



Note: The shared maps and map contents are all view-only on the portal.

2.1.4.View A/B Path Result and Calculate Live Path

Besides mapping devices and sites, external users can mouse over the target A/B path and click the Draw Path button to view the result. Furthermore, they can re-calculate the path by using live data for a refresh.

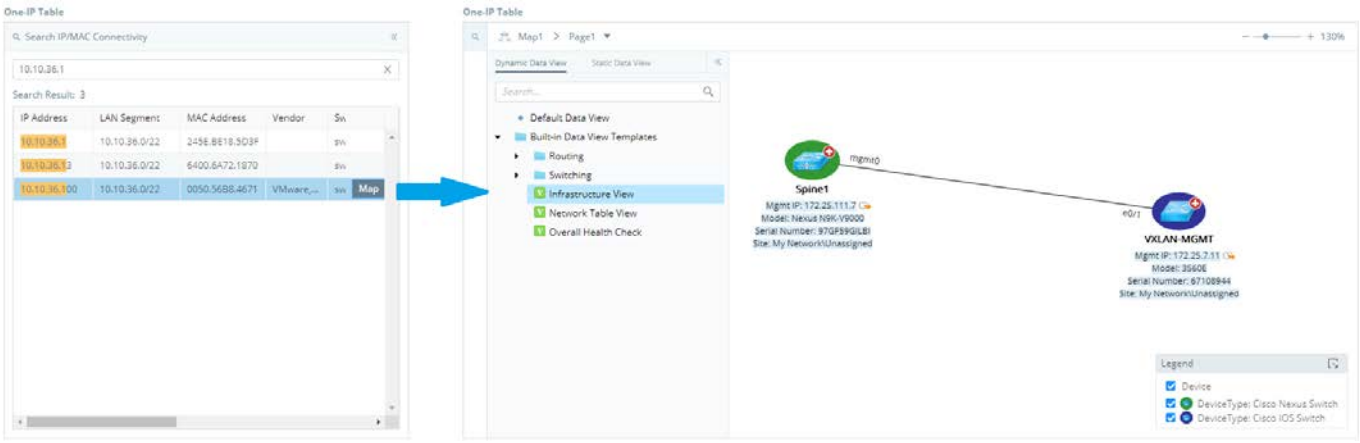


Note: The live path calculation function is only available when the Application Assurance Module has been purchased.

2.1.5.Search One-IP Table and Map Devices

One-IP table, generated based on ARP and MAC tables when the system builds the Layer 2 topology of a network, records the physical connections and can be used to troubleshoot IP/MAC connectivity issues.

With the One-IP table, external users can search for a device in the current domain by using an IP address as the search term, and click the Map button to map out the target device and its connected neighbors. Furthermore, they can select to apply a data view among those applicable ones to the devices on the map.



2.1.6.Feature Comparison Between Portal and IE

The following table lists the comparison of operations that a user can perform between Function Portal and IE.

Feature Category	Functions	Function Portal	IE
Map	▪ Move Devices ▪ Apply/View DVT and Static DV with Baseline Data ▪ Zoom In/Out	√	√
	▪ Edit and Save Map ▪ Export Map to Word/Visio/etc. ▪ Live Run DVT ▪ Manage Map Data View ▪ View Data View with Historical Data ▪ Play Runbook ▪ Device Context Menu ▪ Map Context Menu		√
Path	▪ View Path Result ▪ Calculate Live Path	√	√
	▪ Edit and Save Path ▪ View Path Log ▪ Set Golden Path ▪ View Path Historical Results		√
One-IP Table	▪ Search ▪ Map	√	√
	▪ View ▪ Export ▪ Resolve DNS ▪ Delete		√

2.2. Diagnosis with Device Health Report and Logs

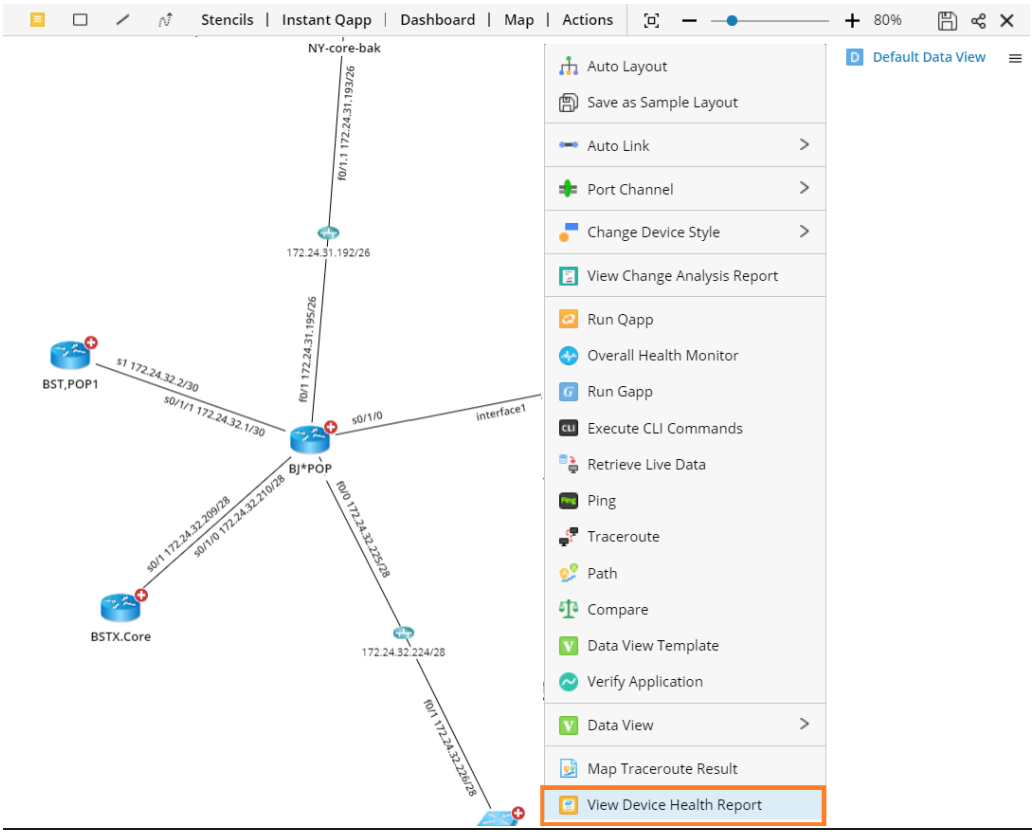
When working on a map, you may run into various anomalies of devices, such as a live access issue, a topology issue, or a path calculation failure across a device. The visibility of the overall health at the device level is critical to achieving map success.

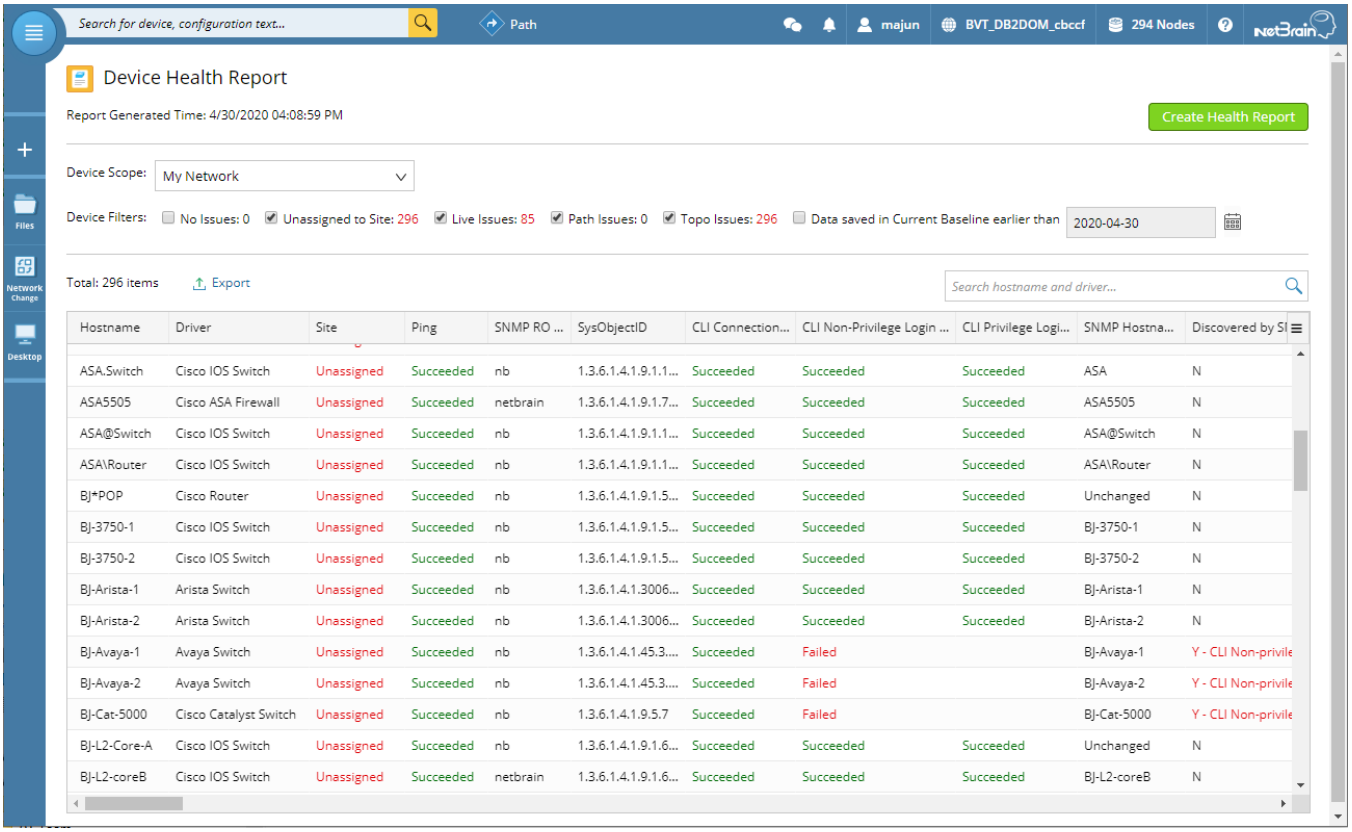
By introducing the new feature Device Health Report, IEv8.03 visualizes a device's health from the following evaluation perspectives:

- **Basic Information** – device driver and site assignment.
- **Live Status** – Ping status, SNMP and CLI connection, hostname change status, etc.
- **Data Existence in Current Baseline** – configuration file and data tables, etc.
- **Topology** – connections for each topology type, such as the number of no neighbor interfaces, whether it is an isolated device, etc.
- **Path Failure** – the failed calculation records for paths across the device, etc.

Generate Device Health Report

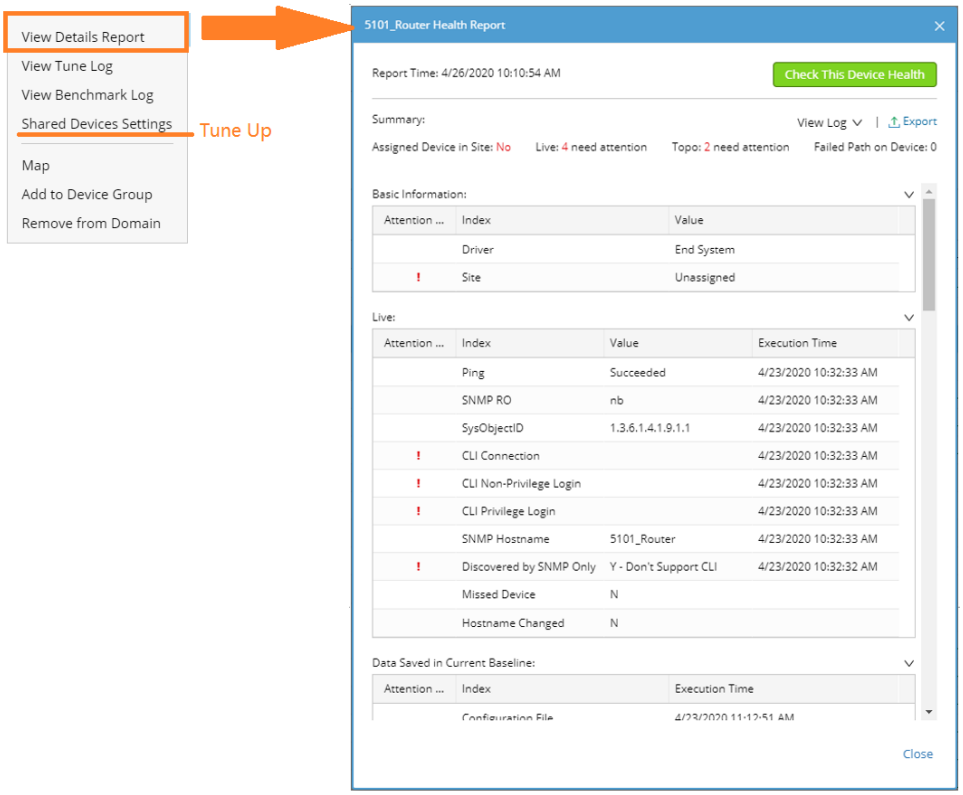
Typically, the health report for devices on a map can be accessed from the map context menu and generated on-demand.





Tip: The health report can also be accessed from the Start Menu, which targets all devices in the current domain, or from the device context menu, which targets the selected device only.

The report provides statistics for each issue category, which can also be used as filters to narrow down problematic devices. From the device context menu on a map, you can select to view the detailed report of a single device, view execution logs, or re-tune up.



Tip: The attention (!) is a reminder to ask for your attention. If remedy action is not necessary, you can ignore it.

2.3. Enhancements to Domain Health Report

IEv8.03 adds the health status of Clouds and path calculation to the Domain Health Report.

Report Cloud Health

The added Cloud Health area shows the key properties of the existing clouds in the current domain, for example, the count of the edge device and blank Network Control Table (NCT).

Cloud Health:

Attention	Cloud Name	Cloud Type	Edge Device Count	Created Time	NCT Table (no data)
!	MPLSCloud3356VRF1001	MPLS L3 VPN	13		1
!	MPLSCloud3356VRF1002	MPLS L3 VPN	13		1
!	MPLSCloud3356VRF1003	MPLS L3 VPN	13		1
!	MPLSCloud3356VRF1004	MPLS L3 VPN	13		1

Note: Blank NCT includes those tables with headers only. When the count of blank NCT exceeds 0, the attention mark (!) will display.

Report Path Calculation Health

The health status for path calculation shows the results (the latest ones of paths in Application Manager), categorized by Succeeded and the causes of failure.

Path Calculation Health:

Total 2 paths, 0 succeeded, 0 not executed, 0 running, 2 failed

Attention	Path Result Category	Count	Percentage
	Succeeded	0	0%
!	Lack of related information	1	50%
!	Gateway Issue	1	50%

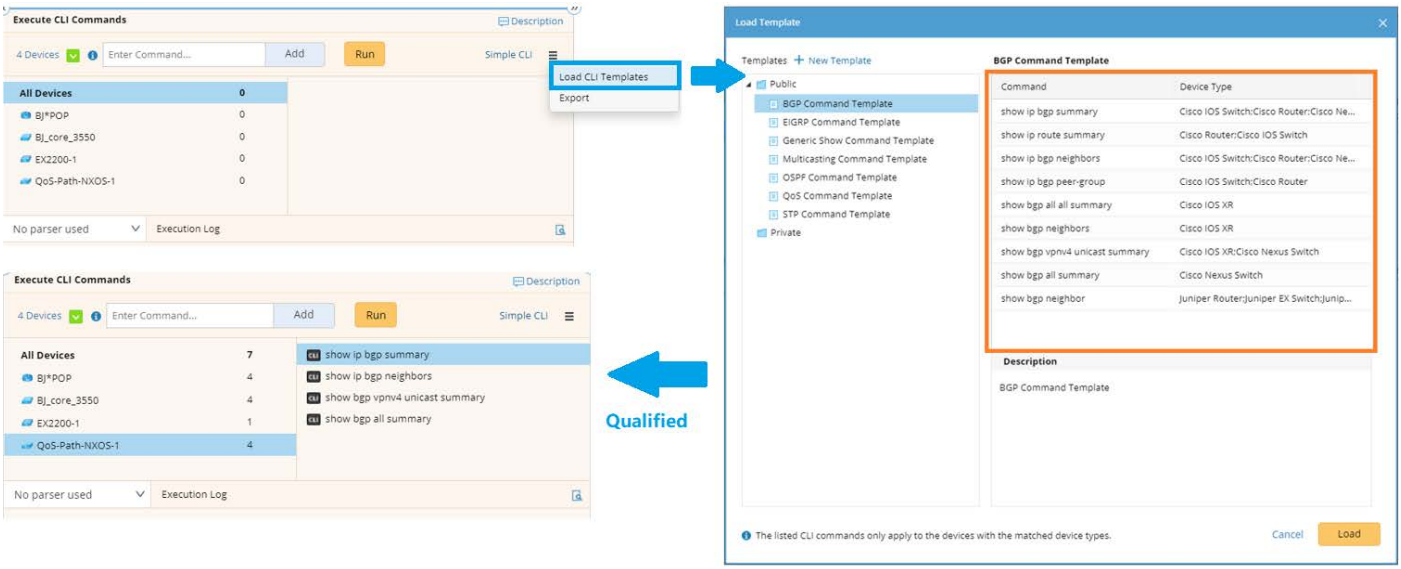
2.4. Enhancements to CLI Automation

In previous versions, the selected CLI commands are executed on all target devices without any qualification. That is, even if a CLI command is not applicable to a device, it will be executed anyway and get an invalid result, which consumes unnecessary resources.

IEv8.03 allows you to define the applicable device types for each CLI command in the features that may task CLI command execution, such as, Runbook, Benchmark, and API-triggered diagnosis.

2.4.1.Qualify Devices for CLI Automation in Runbook

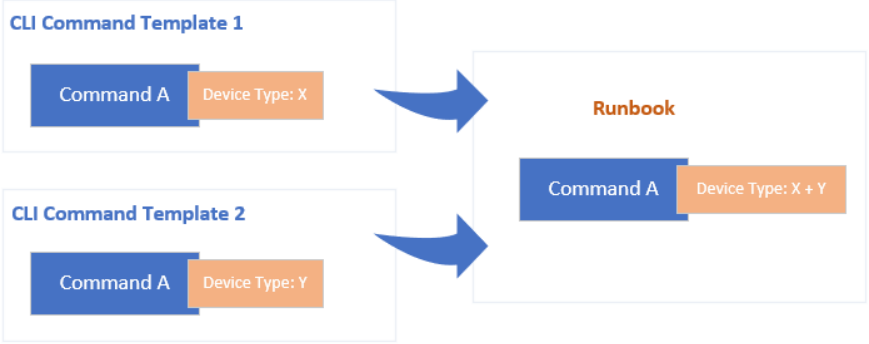
IEv8.03 allows you to define the applicable device types for each CLI command included in a CLI template. By loading a template to add CLI commands to a Runbook, you can leverage the predefined device types as qualifications to exclude the improper commands from the execution scope of target devices.



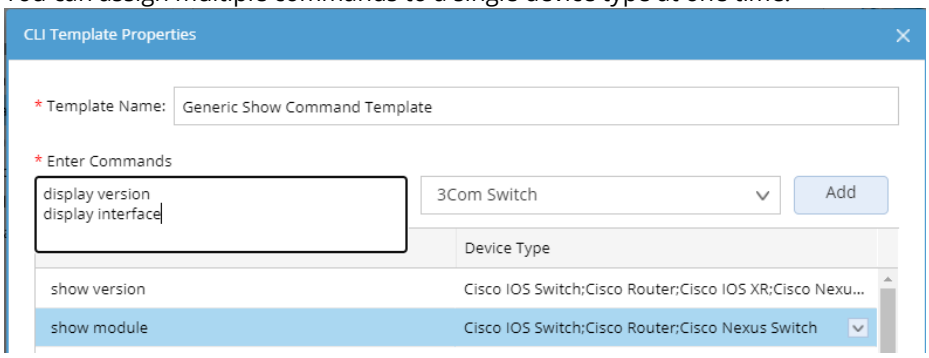
Note: The device qualification is only available to the CLI commands added through a template. Those manually entered or imported commands will still be executed on all target devices.

Tips:

- Besides the Execute CLI Command node, this command qualification is also available to the Retrieve Live Data node in a Runbook and other features that task CLI automation through CLI templates.
- You can assign different device types to a single CLI command in different templates. If duplicate commands from multiple templates are selected, the device types defined in different templates will be combined.



- You can assign multiple commands to a single device type at one time.

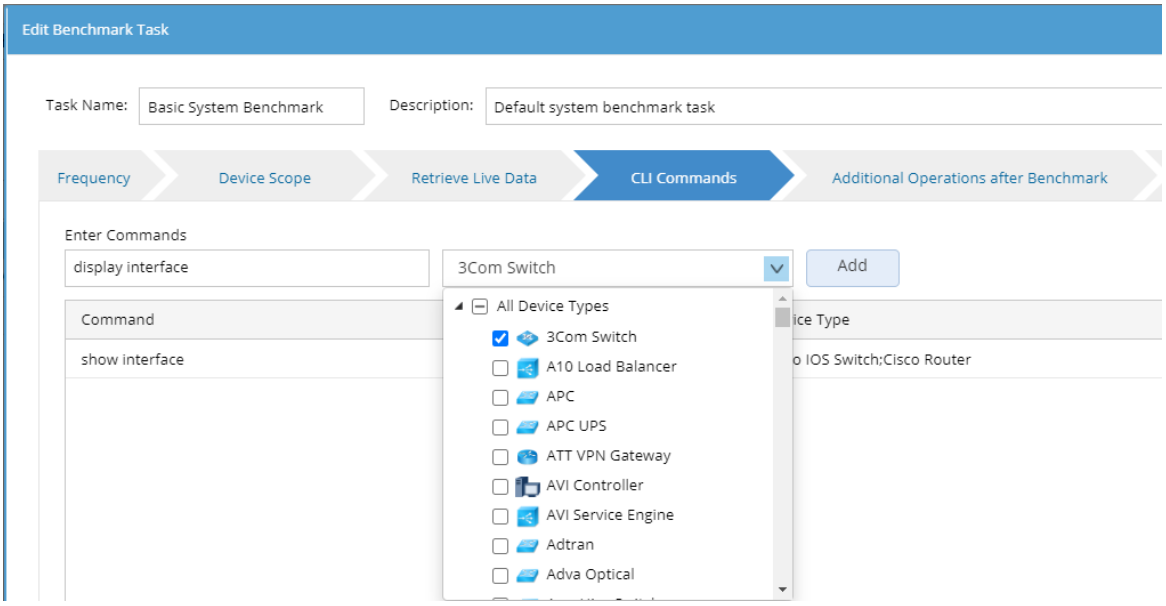


2.4.2.Qualify Devices for CLI Automation in Other Features

Qualify Devices for CLI Automation in Benchmark

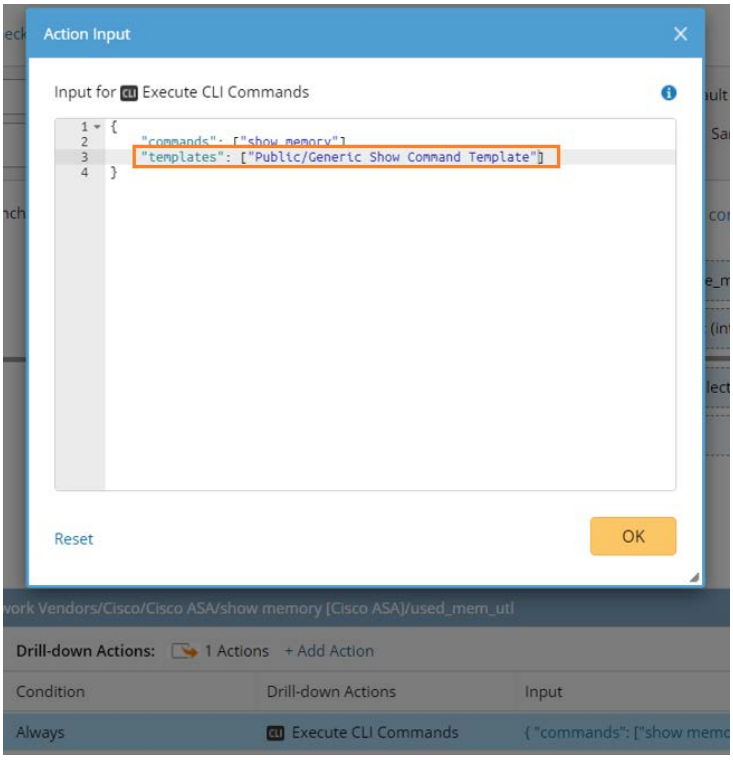
You can select device types for each CLI command as device qualifications when defining a Benchmark task.

By doing this, unnecessary CLI execution will be ignored in the benchmark execution.



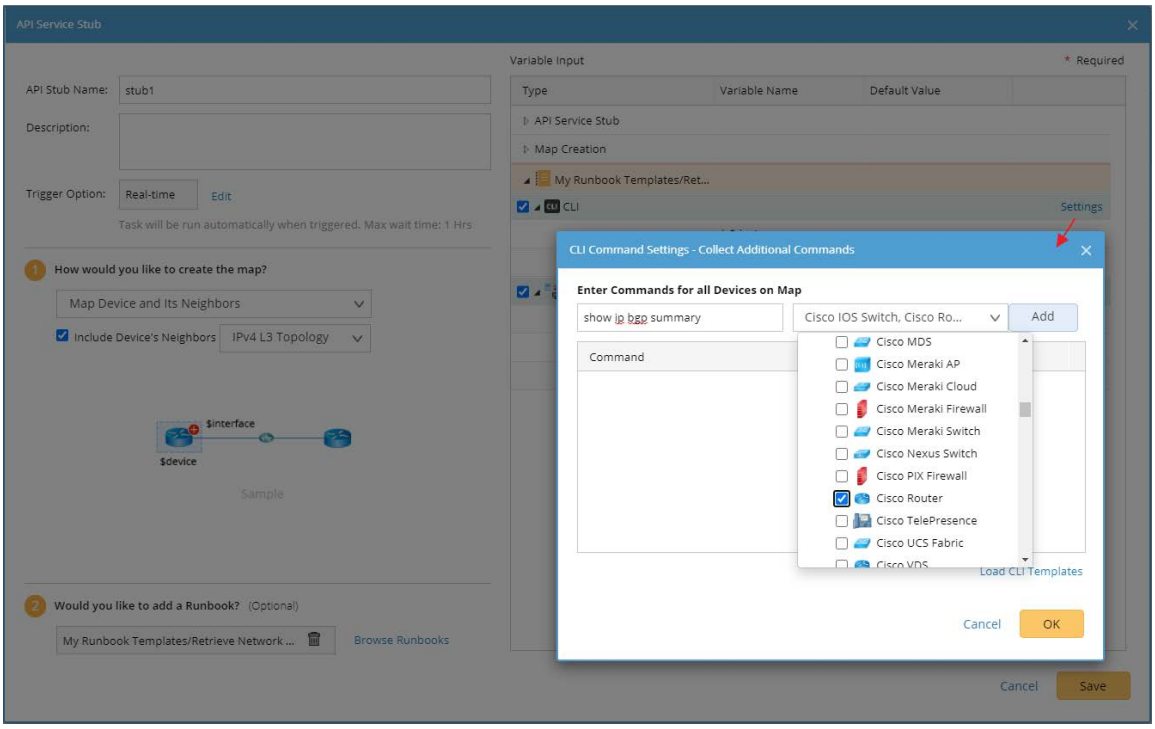
Qualify Devices for CLI Automation in Drill-Down Action of DVT

You can call the execution of CLI templates when defining the input of a DVT's drill-down action. By doing this, the device qualification defined inside the CLI template will be applied to exclude the unnecessary CLI execution.



Qualify Devices for CLI Automation in Triggered Diagnosis

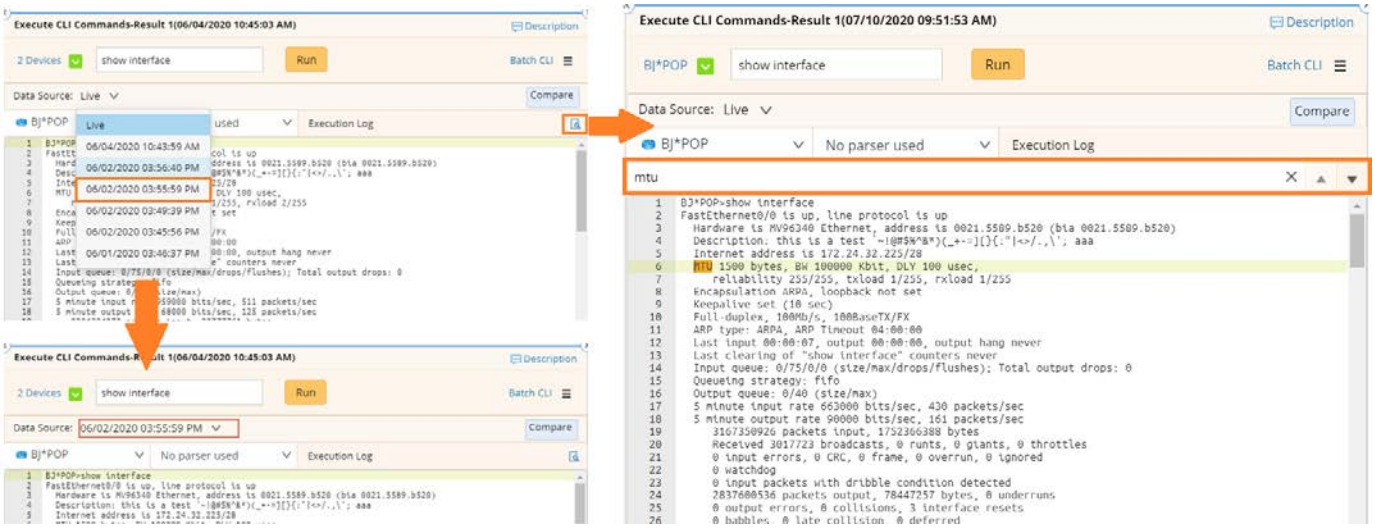
You can select device types for each CLI command as device qualifications when defining an API-triggered task. By doing this, unnecessary CLI execution will be ignored in the diagnosis.



2.4.3.View Historical Execution Results and Search

When working with the CLI automation result, you can:

- toggle the data source to view historical execution results.
- click the search icon to search keywords (case-insensitive).

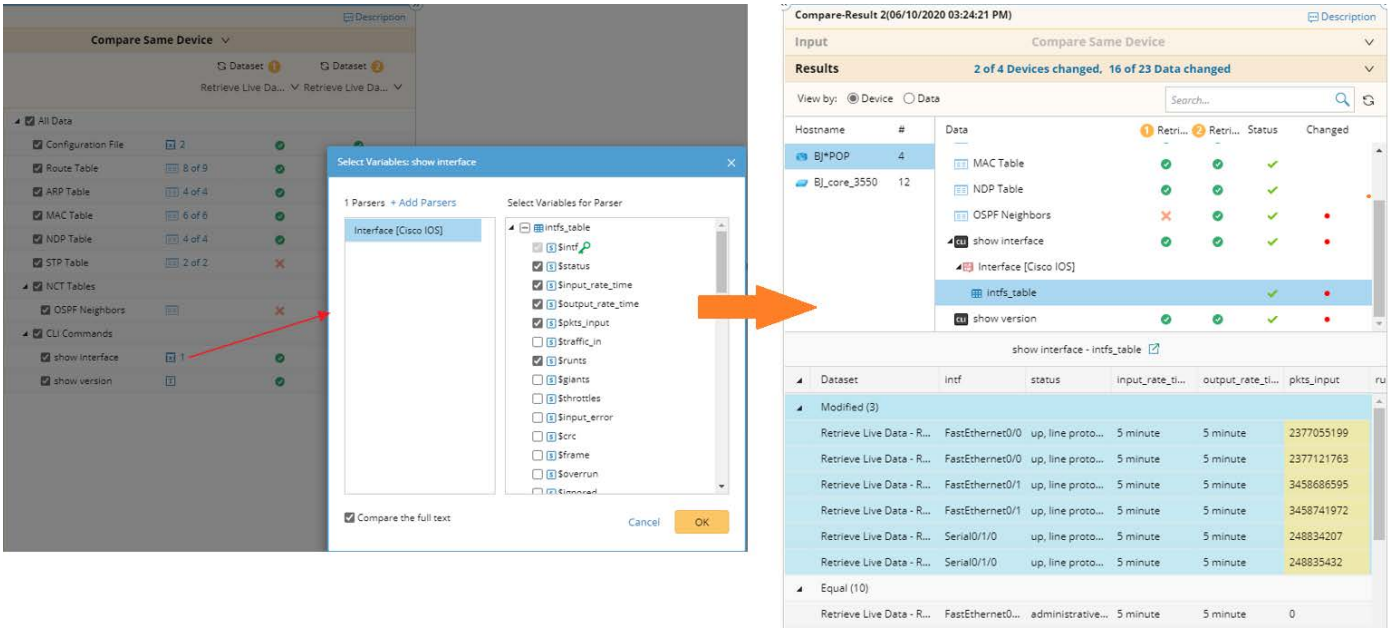


2.5. Enhancements to Granular Data Comparison

To highlight meaningful changes and eliminate noises, IEv8.03 introduces quite a few enchantments to data comparison through Runbook Automation.

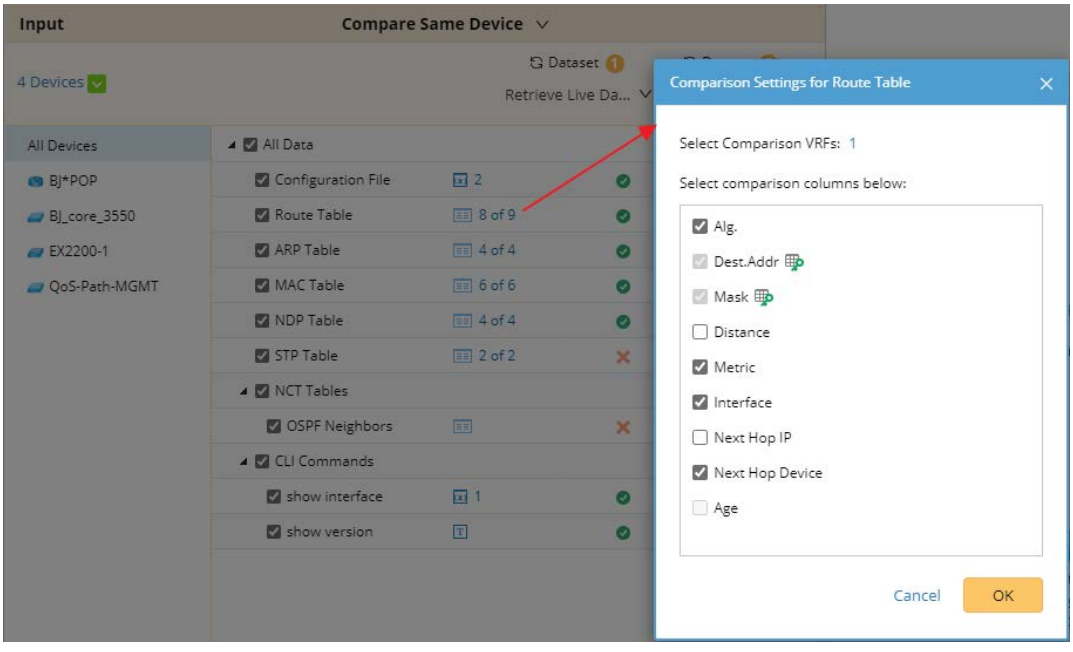
2.5.1.Compare Values of Parser Variables in Configuration/CLI

In addition to comparing the full text of configuration file and CLI commands, IEv8.03 allows you to compare the values of selected parser variables in the configurations or CLI commands.



2.5.2.Compare Selected Columns of System Data Table

Noises sometimes distract you when you check the comparison result; for example, nobody cares about the frequent changes of the **Age** column in the system data table. To eliminate these noises, IEv8.03 allows you to select columns before starting the comparison. The number of selected columns and total columns is displayed for each table, for example, "8 of 9" means there are nine columns in the table, and eight columns have been selected for comparison.

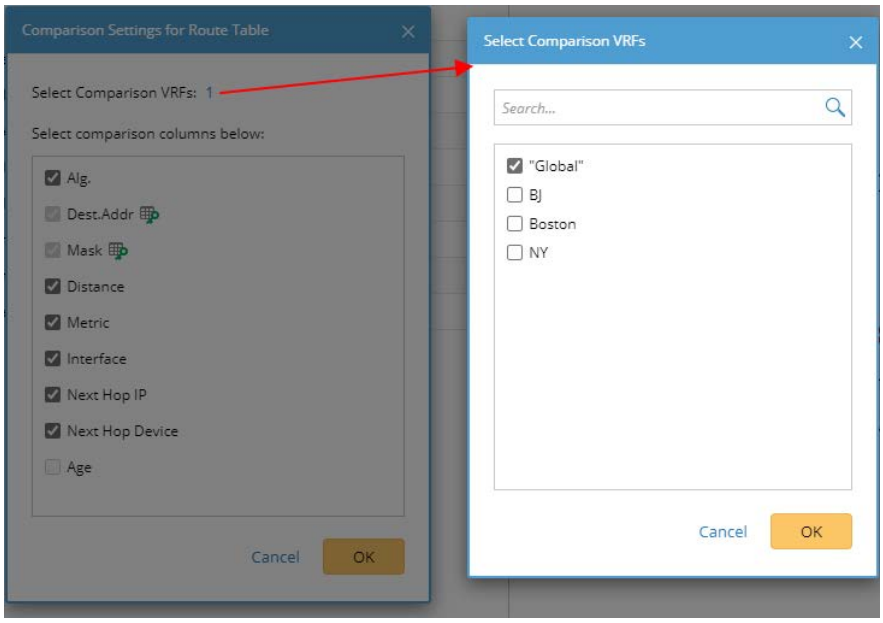


2.5.3.Compare Selected Sub Tables

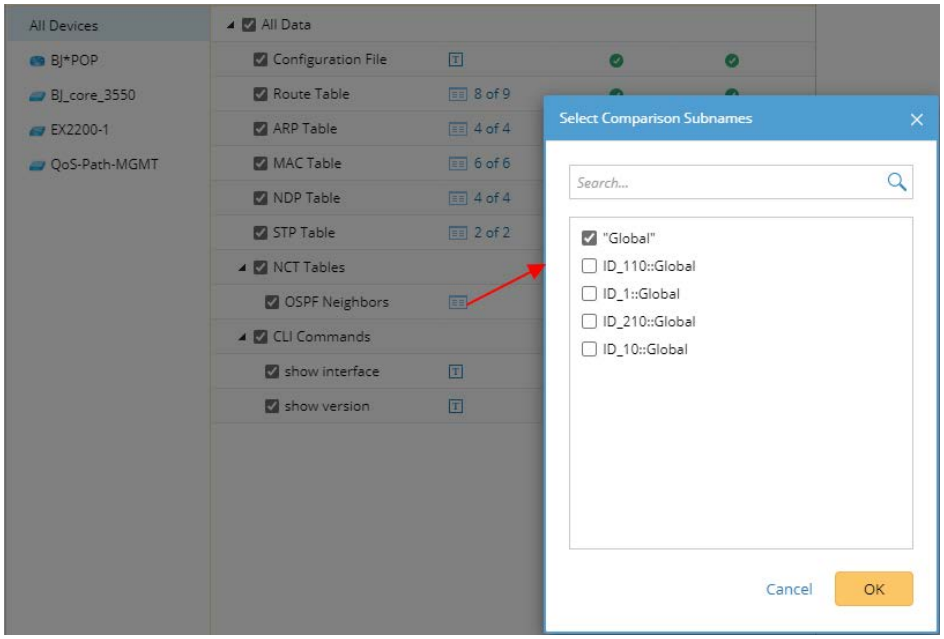
In earlier versions, the system compares all the system data tables or NCTs by default. This may lead to potential performance risks, because some customers may have many VRF tables or subname NCTs.

IEv8.03 separates the sub tables for system data tables and NCTs. By default, only the “global” one is selected for comparison. You can select more sub-tables based on their needs. For example:

- When a route table has multiple VRF tables, you can select one or more to compare.

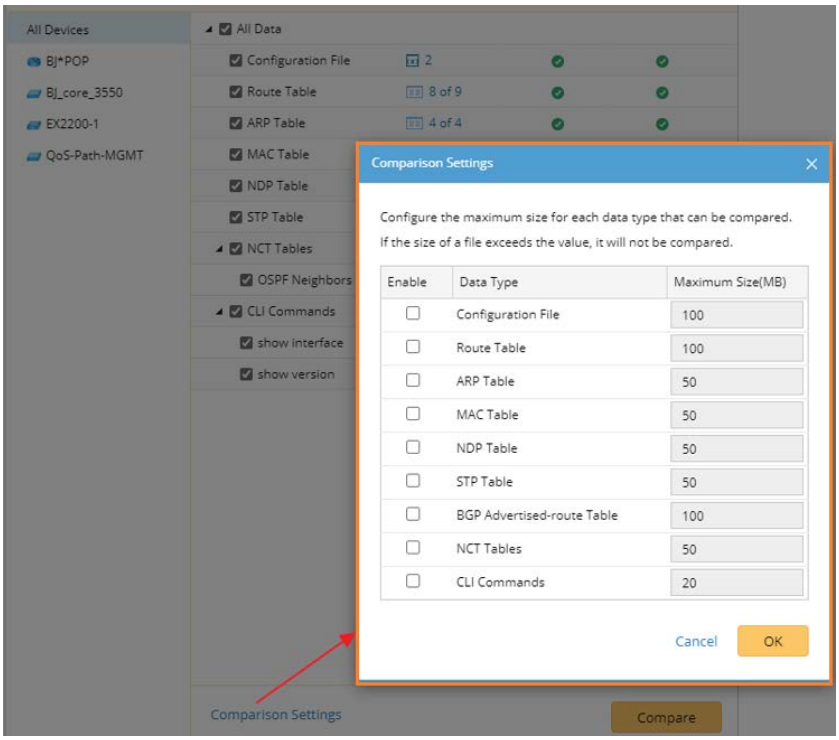


- When an NCT has multiple sub-name tables, you can select one or more to compare.



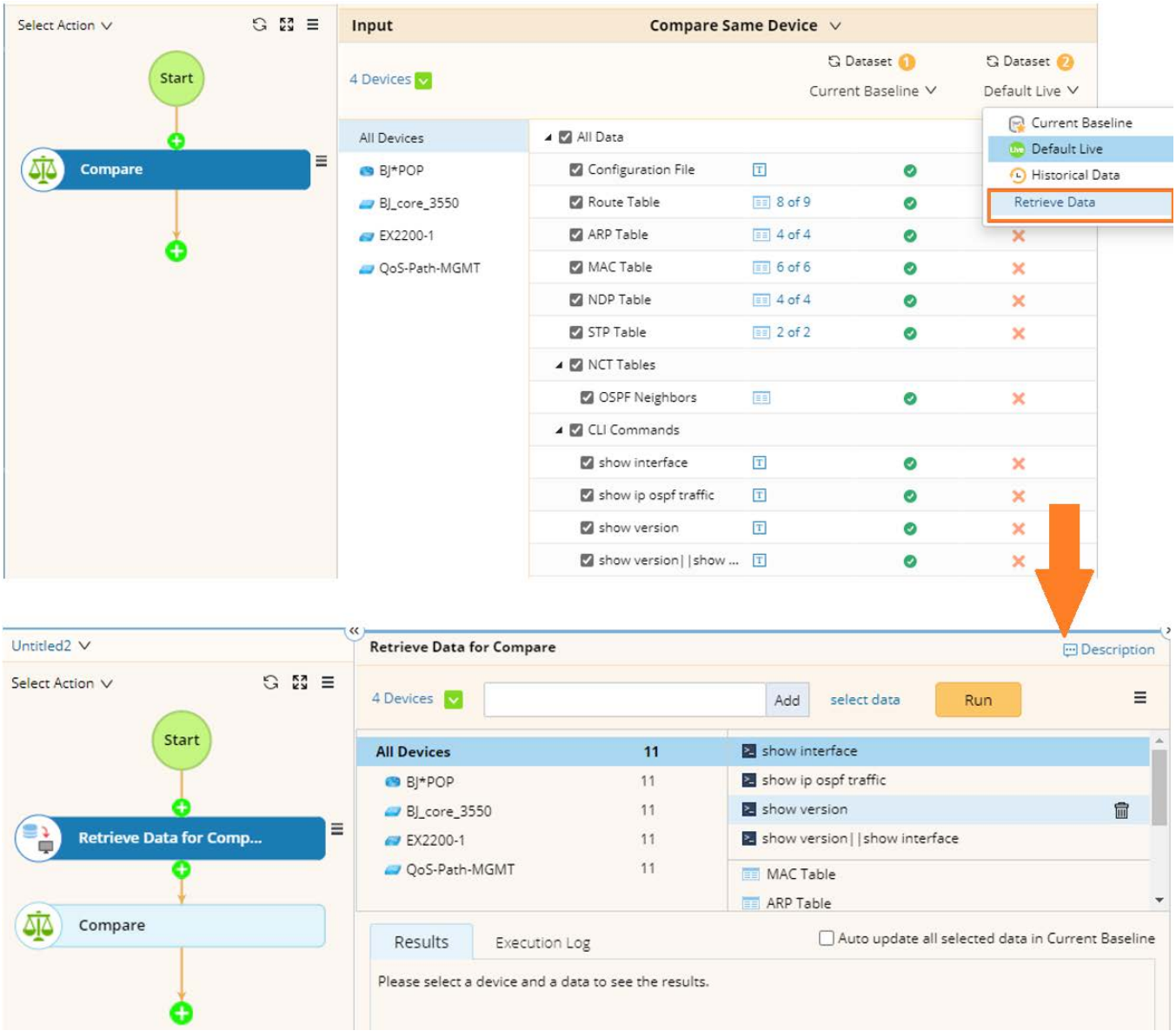
2.5.4.Set Maximum Size for Comparable Data Types

IEv8.03 allows you to limit the size of each data type for comparison to enhance performance. By default, the function is disabled. When enabled, only the data types, of which the size is less than or equal to the threshold, can be compared. These thresholds are configurable before starting the comparison.



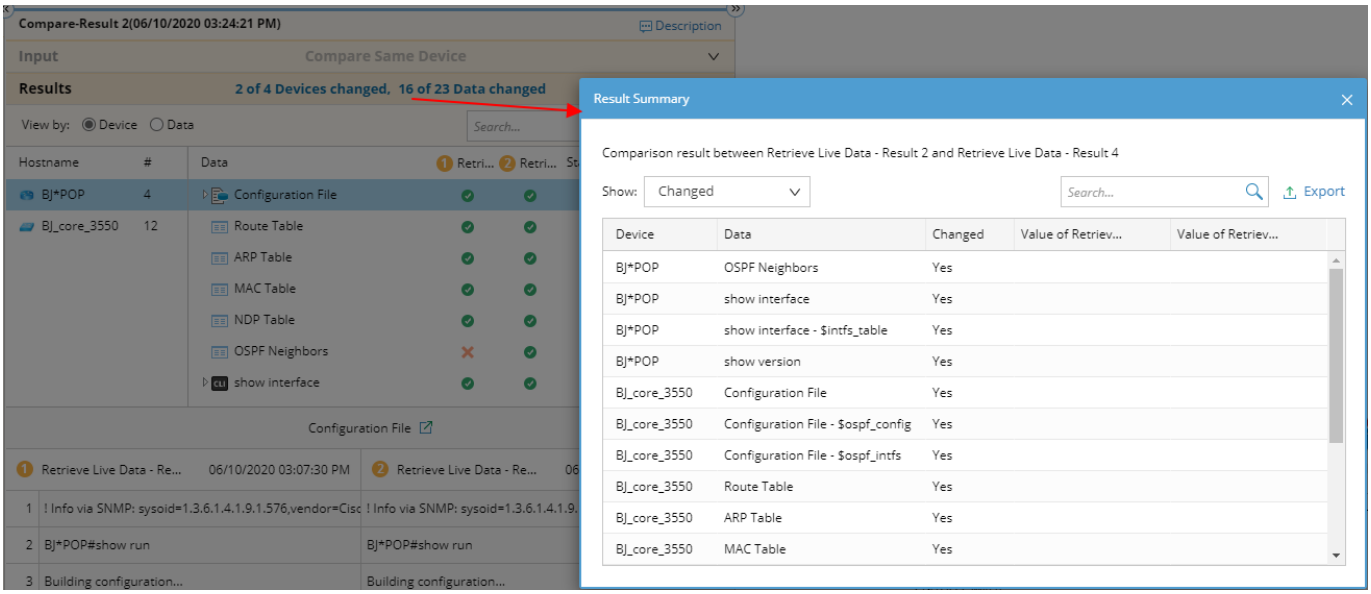
2.5.5.Compare with Instantly Retrieved Live Data

IEv8.03 allows you to use the real-time data for comparison if there is no data existence for any selected source. Once selected, the Retrieve Live Data node will be added to the current Runbook, and all the selected devices will be auto-populated as target devices for the live data retrieval.



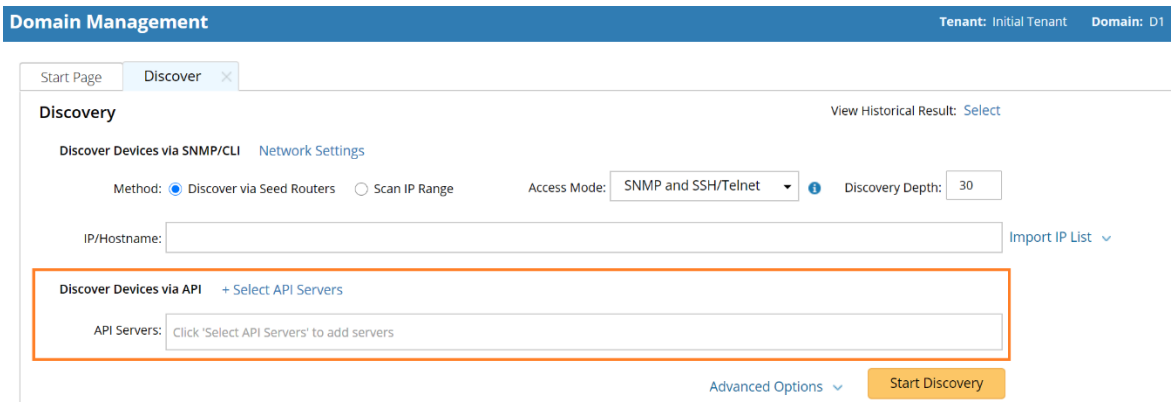
2.5.6.Summarized Comparison Results

IEv8.03 allows you to gain quick access to the summarized comparison results, and provides two filters “changed” and “unchanged” for devices and their different data types.



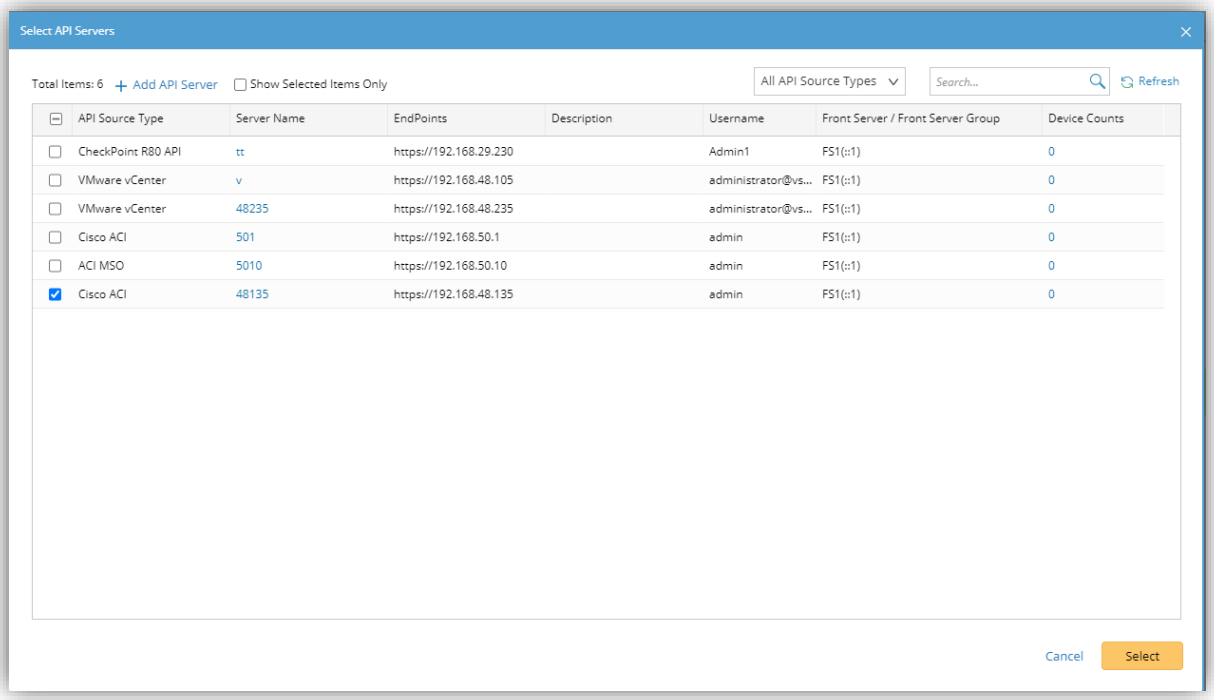
2.6. Enhancements to Discovery

In the previous versions, the API discovery and SNMP/CLI discovery shares the same input bar, which caused lots of confusion. Also, the additional operations after discovery are mandatory, which could lead to a very long discovery time for a large network environment. Besides that, you can only view the last discovery history. In IEv8.03, the system provides a separate input bar for API discovery, which offers you the option to not run the additional operations for every discovery, and allows you to view all the discovery history. The UI for discovery and scheduled discovery has been redesigned accordingly.



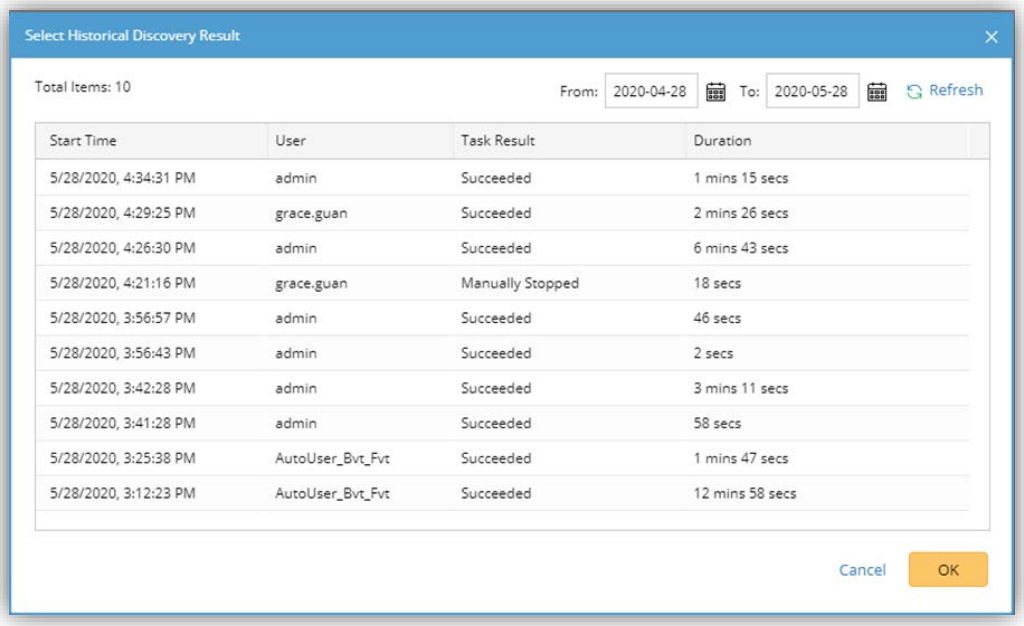
2.6.1.Bulk Select API Servers

In IEv8.03, you can select the API server from the 'Select API Servers' window for the API discovery. To accommodate a large number of API servers, you can choose to select the server by filtering with server type or using the search bar. The selected server in the window will automatically synchronize with the server listed in the input bar. When you delete a server from the input bar, the server will be unchecked in the 'Select API Servers' window as well. You can clearly view all selected servers by checking the option 'Show Selected Items Only' in the 'Select API Servers' window. If a server has been removed from the domain after being selected, a warning message will pop up when you click 'start discovery' asking you to either modify the input or proceed to discovery without the deleted servers. The traditional devices will be discovered through SNMP/CLI first, then the API servers will be discovered via API.



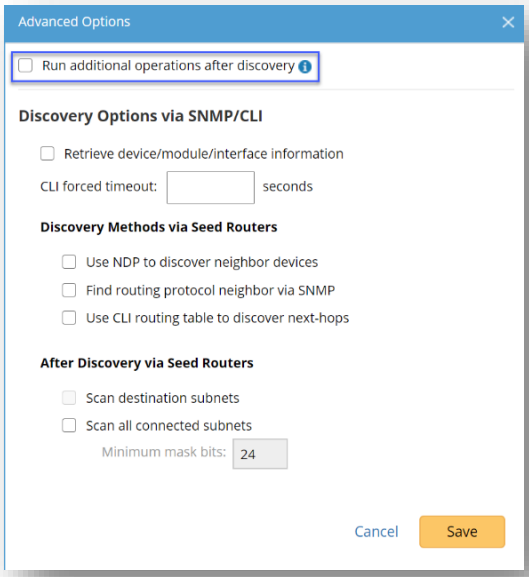
2.6.2.View History Result

In IEv8.03, you can view and select history result in the 'Select Historical Discovery Result' window. By default, it will show the discovery history in the past 30 days, and you can select which history to view. You can adjust the time range for the discovery history on the top of the window. After you make the selection, the discovered devices for the selected discovery will be automatically filled in the input bar so you can easily rediscover those devices. The discover logs will be loaded on the GUI as well.



2.6.3.Toggle Additional Operations

You can choose to not run the additional operations for the discovery by unchecking this option in advanced options. When running the topology incrementally, it will not only run for devices in current discovery but also for devices in previous discovery if the topology has not been built for them. You can also choose to retrieve the device/module/interface information for certain discovery (for example, AWS discovery to merge the multi-source devices and Juniper discovery for complete MIB information).



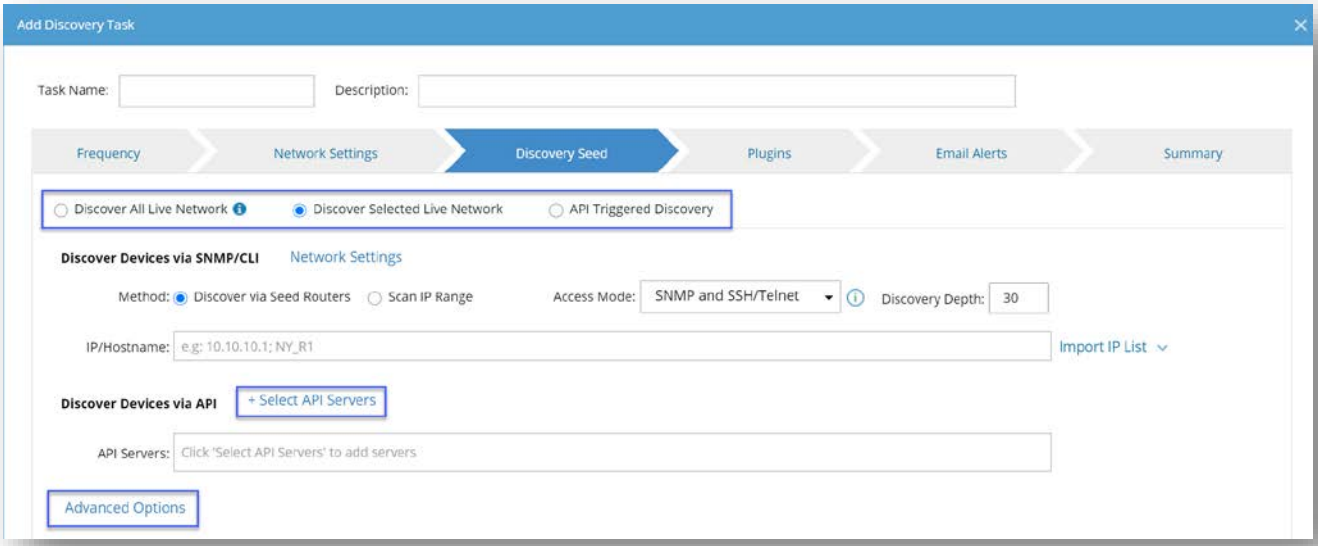
2.6.4.Export Access Logs

Access log is very important for troubleshooting, but there is no option to easily export them in the previous release. In IEv8.03, the export function in device logs will not only export the device logs but also export the access logs for each device.

2.6.5.Scheduled Discovery Enhancements

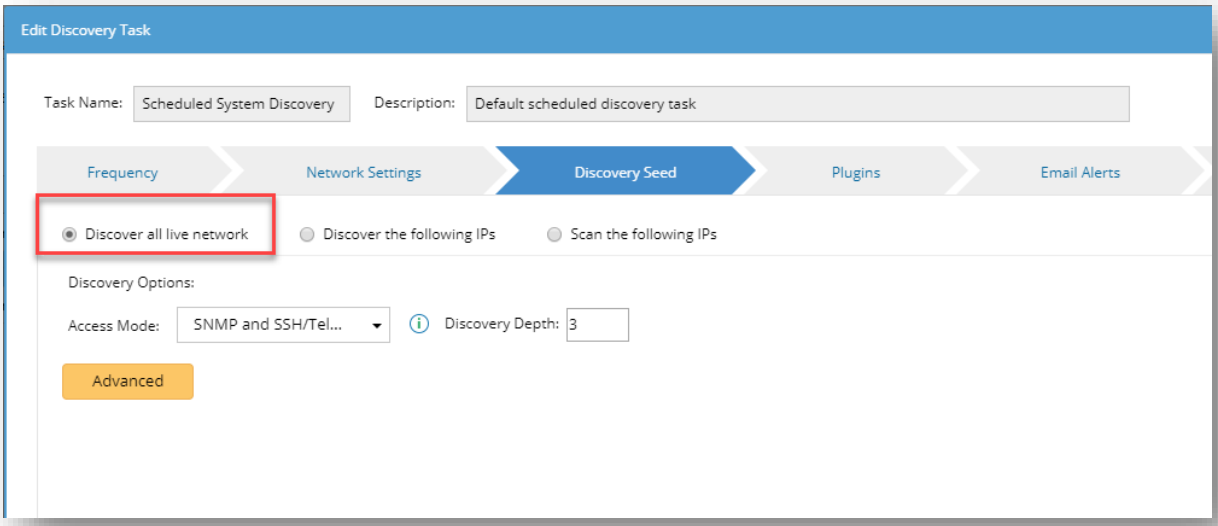
The following improvements have been introduced in IEv8.03 scheduled discovery:

- In 'discover all live network', it will discover all traditional devices in current domain via SNMP/CLI and SDN/cloud devices via API.
- In 'discover selected live network', it now offers the option to scan the IP range and select device for seed discovery.
- The advanced options and API discovery has been added in scheduled discovery according to the changes made in on-demand discovery.



In order to avoid discovering a large number of End Systems (using SNMP and CLI) when performing 'Rediscover All Live Network' via API, the backend logic of 'Schedule Discover' was modified as follows:

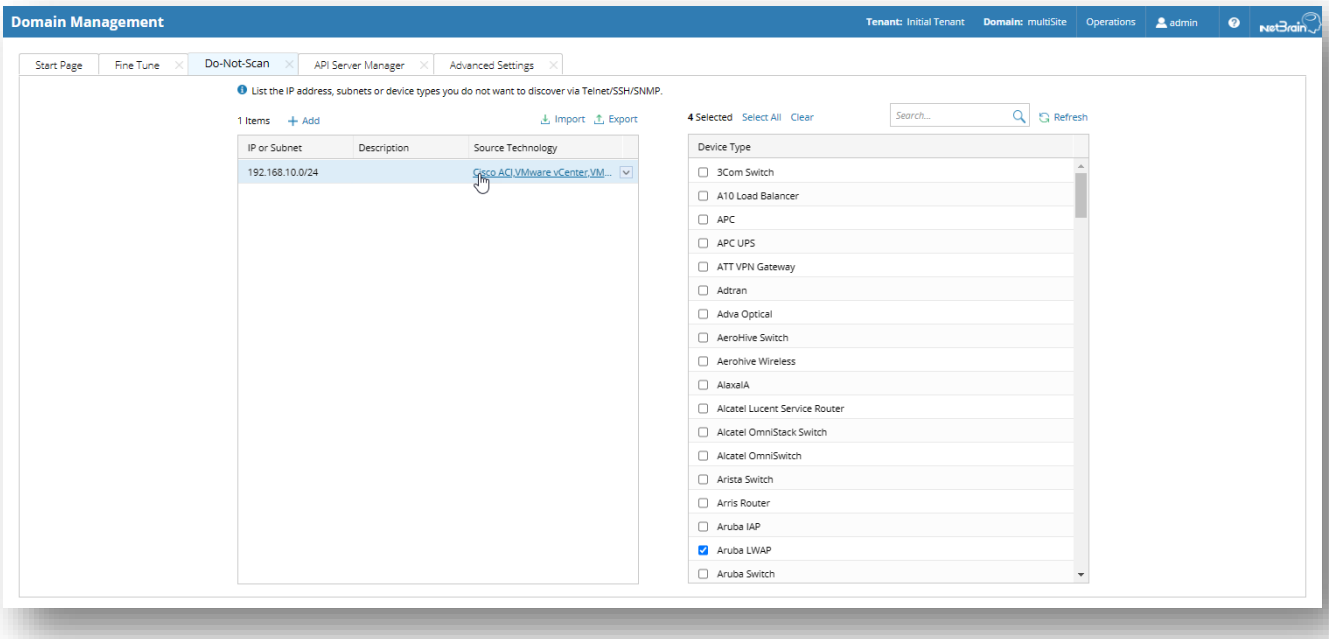
- When the option 'Discover all live network' is selected, API Discover (SDN/Cloud) still uses the API Server to discover and update relevant data,
- Legacy Discover does not perform 'CLI/SNMP Discover' for the devices that are configured to 'Discovered by API Only' nor does it classify these devices as missed devices.



2.6.6.Do not Scan IP Based on Technology

Before IEv8.03, the Do-Not-Scan IP or Subnet function was ineffective for the Discover task via New Tech, due to the discovery of a large number of IP phones and unknown hosts through ACI to join the Domain.

In IEv8.03, you are allowed to add IP or Subnet to Do-Not-Scan and can specify the Technology Source through which you do not want the Discover to be performed.



Note: The Device Type for SDN and Cloud is removed from the Device Type selection box to avoid the scenario where you accidentally select these Device Types, leading to SDN and Cloud function not working properly.

2.7. SDN Enhancements

2.7.1.Service Graph Support

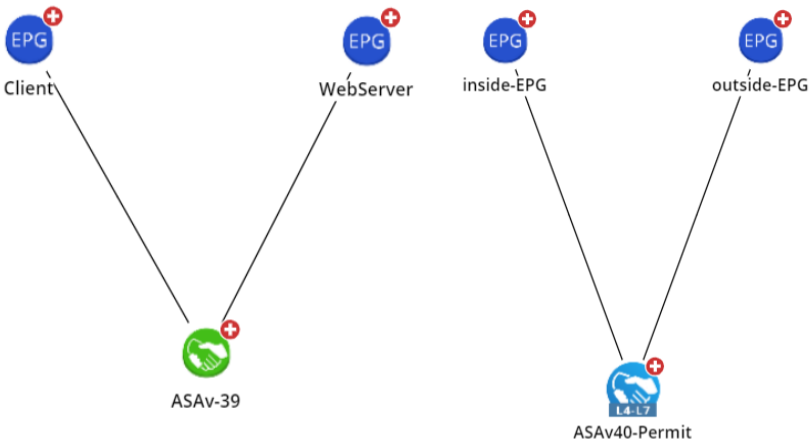
Supported Service Graph Deployment

IEv8.03 supports the following four deployment modes of Service Graph:

- GoThrough
- GoTo
- GoTo with PBR
- OneArm

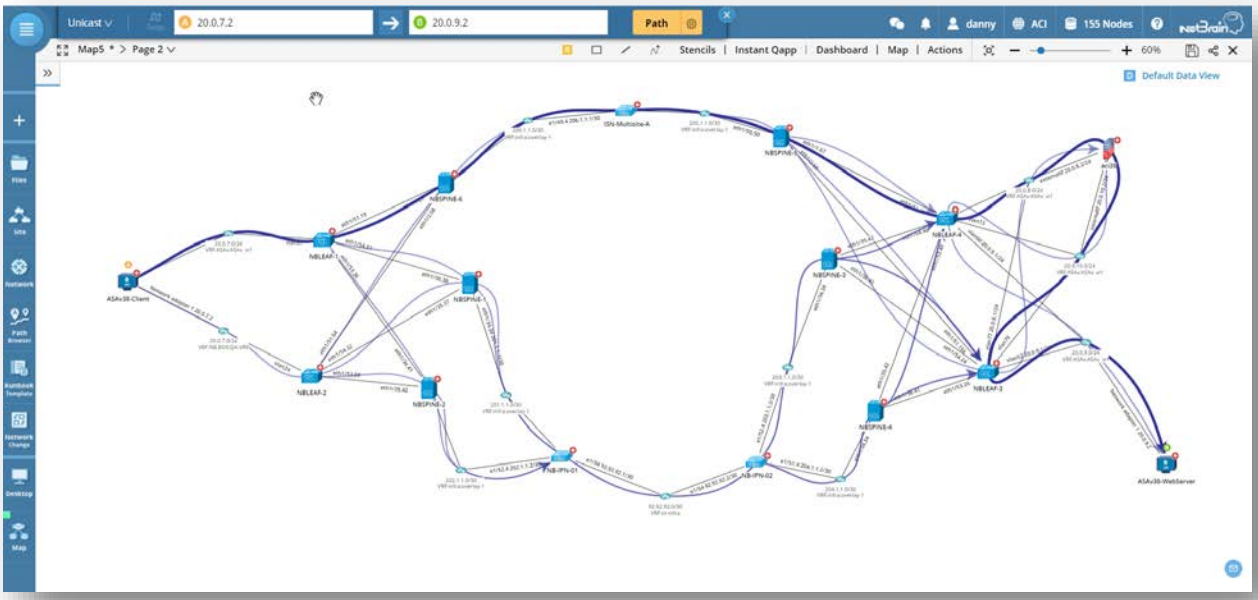
Display Service Graph in Context Map

The Contract configured with Service Graph will be displayed with a special Icon in the Logic Structure Context Map under Application Centric View, allowing you to view the deployed Service Graph in an intuitive manner.



Calculate Path Across Service Graph Device

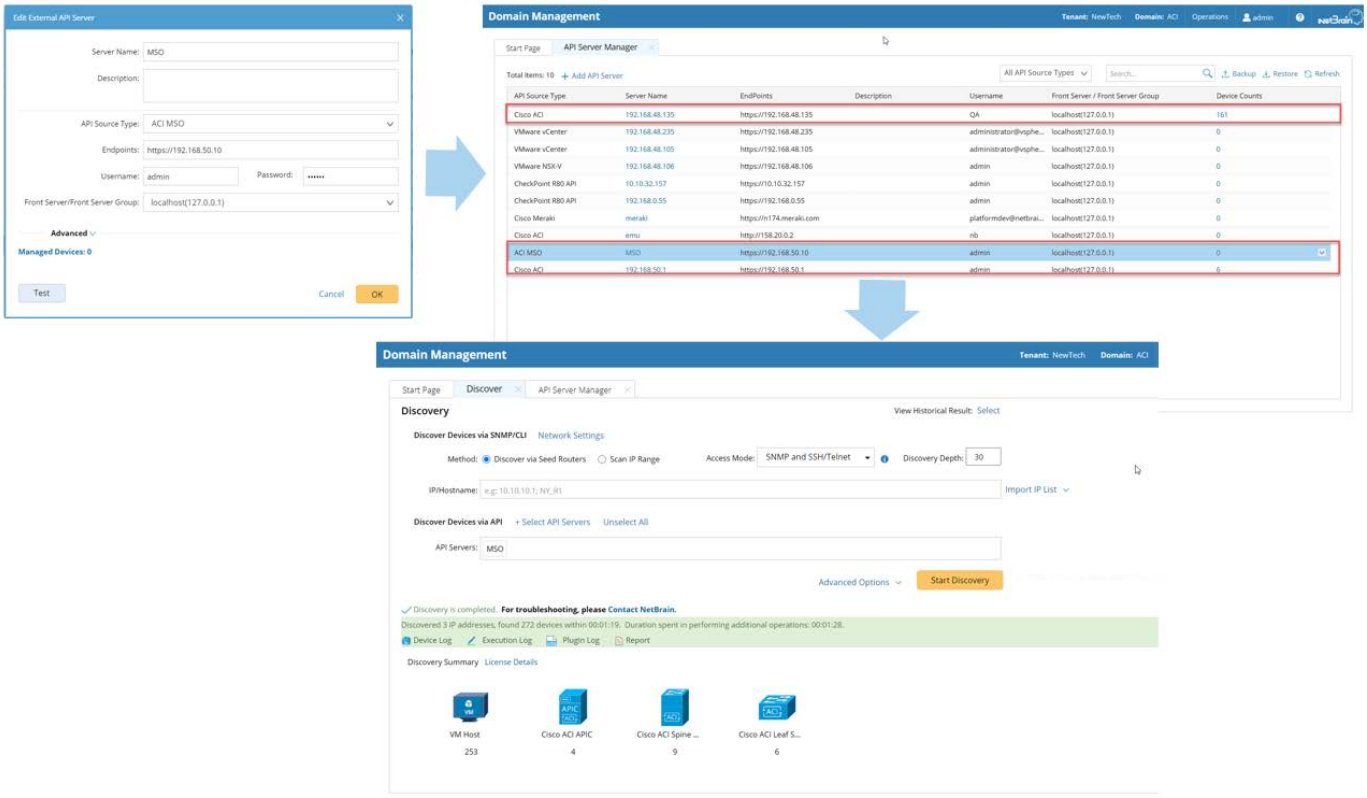
IEv8.03 supports path calculation in the four deployments modes (GoThrough/GoTo/GoTo with PBR/OneArm).



2.7.2.Multi-Site Support

Discover ACI Multi-Site

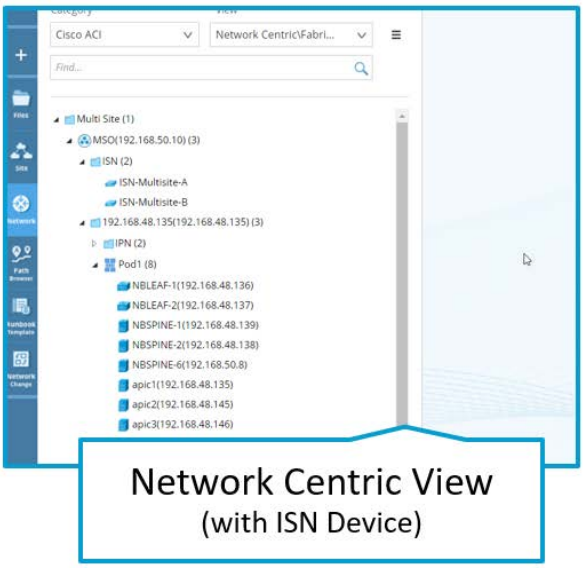
In v8.03 system, new API Source Type "ACI MSO" (Multi-Site Orchestrator) is added to discover ACI Multi Site. After adding MSO and APIC Server of each site to API Server Manager, you can select 'ACI MSO' as the preferred API Source Type when performing discovery. All sites in Multi Site will be discovered to Domain.

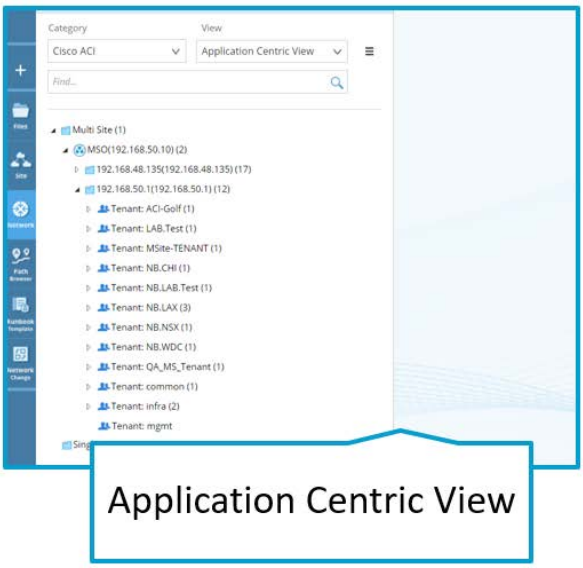


Display Multi-Site on Network Tree

The ACI-related view has been adjusted in the Network Tree. Sites belonging to the same MSO can be placed under this MSO, which is convenient for you to view and use.

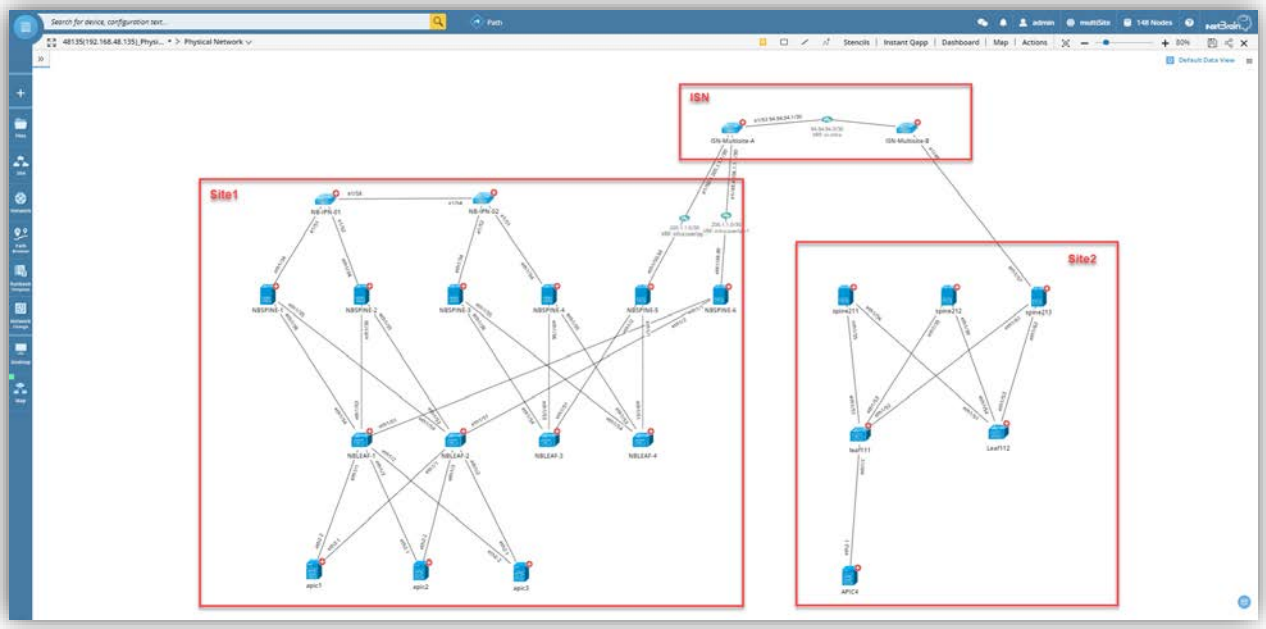
Multi-site structure is also available in the Application Centric View and Network Centric\Tenant View.





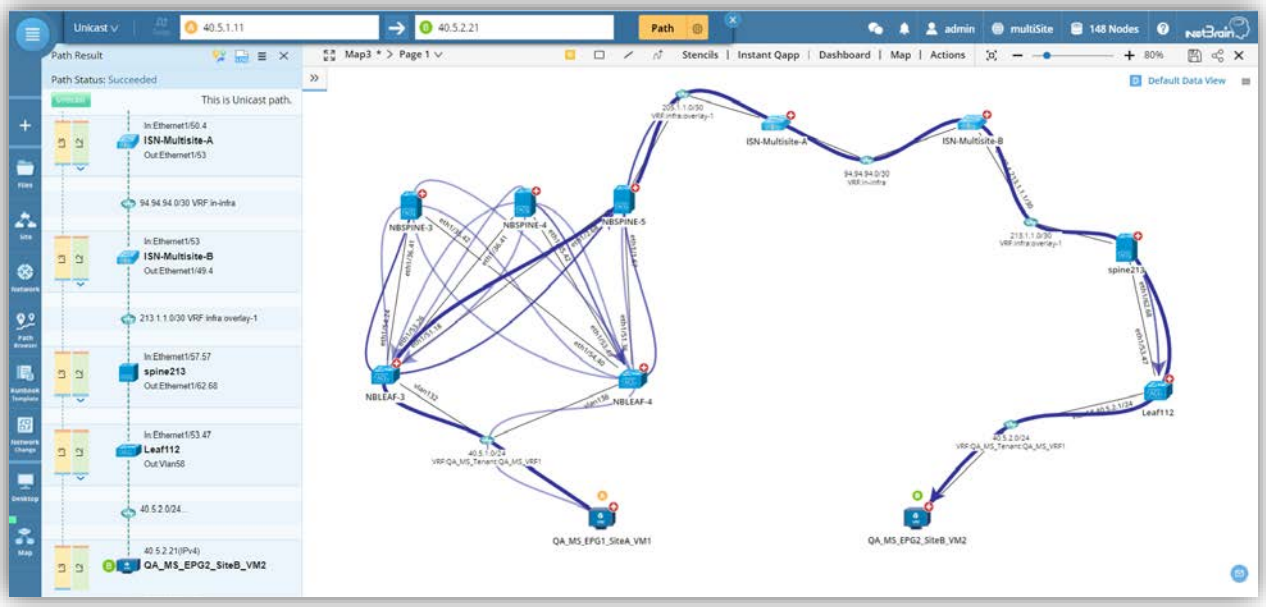
Map Multi-Site

IEv8.03 supports Site to ISN (Inter-Site Network) topology calculation and generating the map depicting Site to ISN to Site relationship.



Calculate Path Across Multi-Site

IEv8.03 not only supports path calculation within the same site, but also supports across-site path calculation.



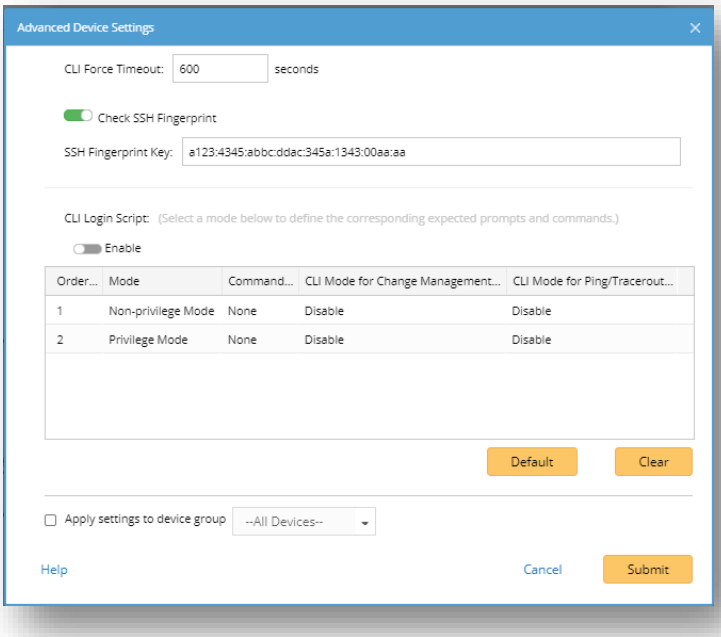
Other Case Driven Features

- ACI Stretched Fabric
    - Transit Leaf is used to connect to other Fabric to make multiple Fabric as a single POD.
    - If there are any DCI devices between Transit Leaf, topology calculation between DCI device and Transit Leaf is not supported. Only the direct connection between Transit Leaf will be displayed in the topology.
- VRF Route Leaking
    - Support route leaking between VRFs that are in the same tenant and different tenants within ACI Fabric.
    - Support route leaking into “Common Tenant” to communicate without network.
- vzAny
    - Use of vzAny to effectively save TCAM resources in policy deployment.
- Preferred Group Under VRF
    - There’s no contract policy check between EPGs within Preferred Group in the VRF.

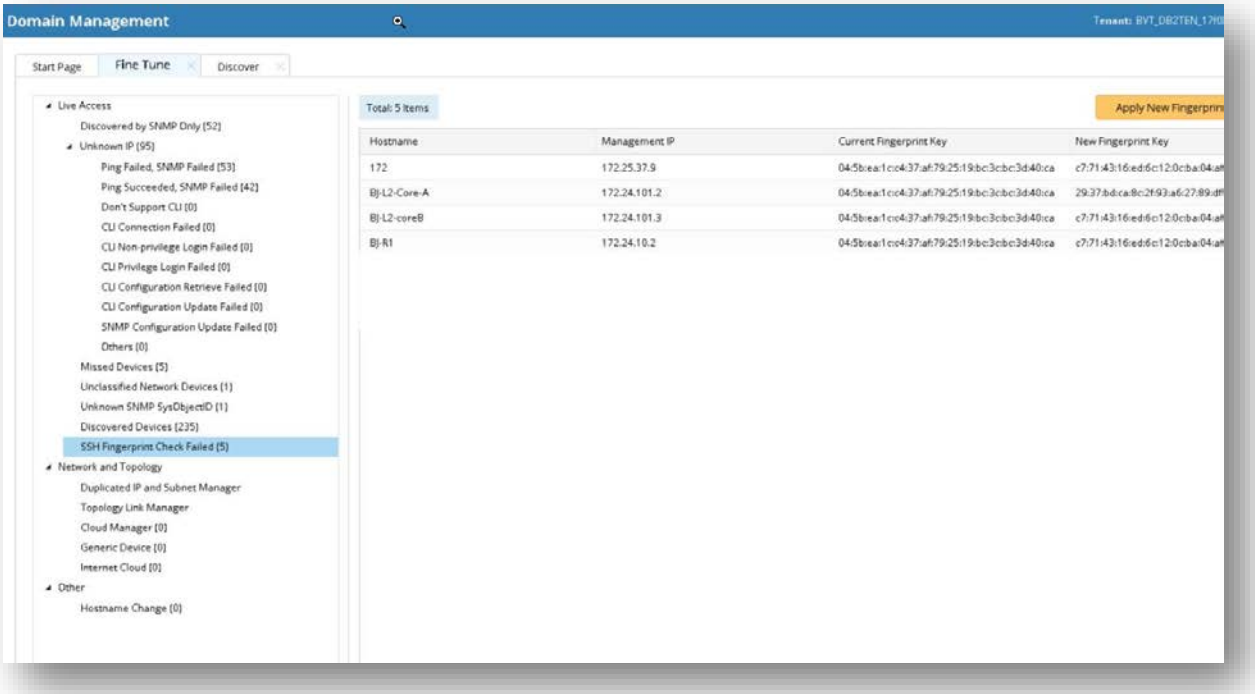
2.8. New SSH Fingerprint Authentication

To improve network security, you may choose Fingerprint for authentication when logging in to the device via SSH. After the SSH Fingerprint authentication function is enabled, NetBrain will obtain the Fingerprint Key from the Device and save it to the Device Setting during the first SSH device login.

In the future, every time you log in to the device through SSH, you will use the Fingerprint Key saved in Device Setting to verify with the Fingerprint Key on the Device. If they are consistent, you can log in to the Device to perform CLI operations; if the verification fails, the failed Device and the Fingerprint Key will be recorded in the SSH Fingerprint Check Failed Table.



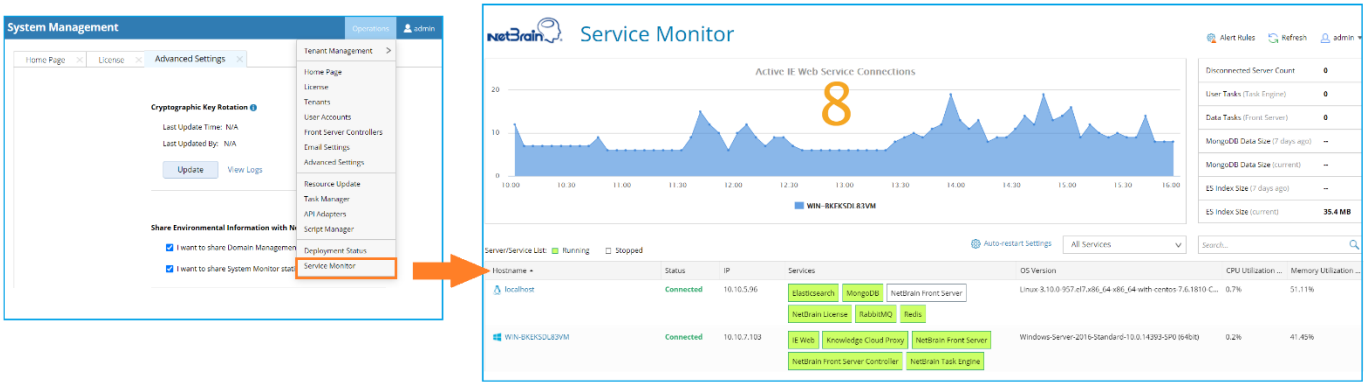
From the table below, you can view the Fingerprint Key saved in the current Device Setting and the new Fingerprint Key obtained from the Device. After verifying the new Fingerprint Key, you can manually update it to the Device Setting for future login.



2.9. Enhancements to Service Monitor

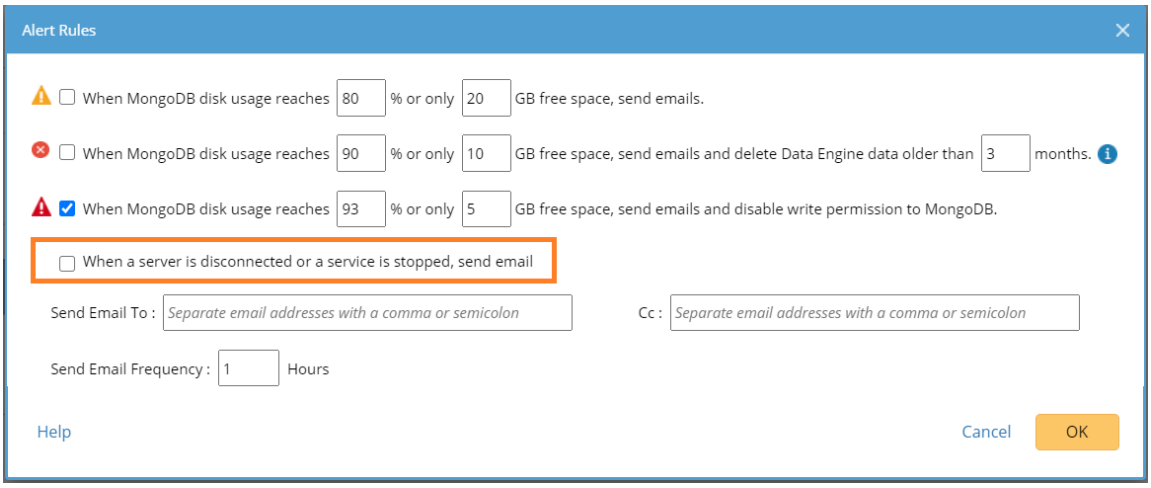
2.9.1.Quick Access and Auto-Login for System Administrators

To enable system administrators to access the service monitor page directly, IEv8.03 adds a drop-down menu of the System Management page. Through this quick access, the system administrators will be automatically logged in to the service monitor page with the current admin account.



2.9.2.Enable Email Alerts for Service Anomaly

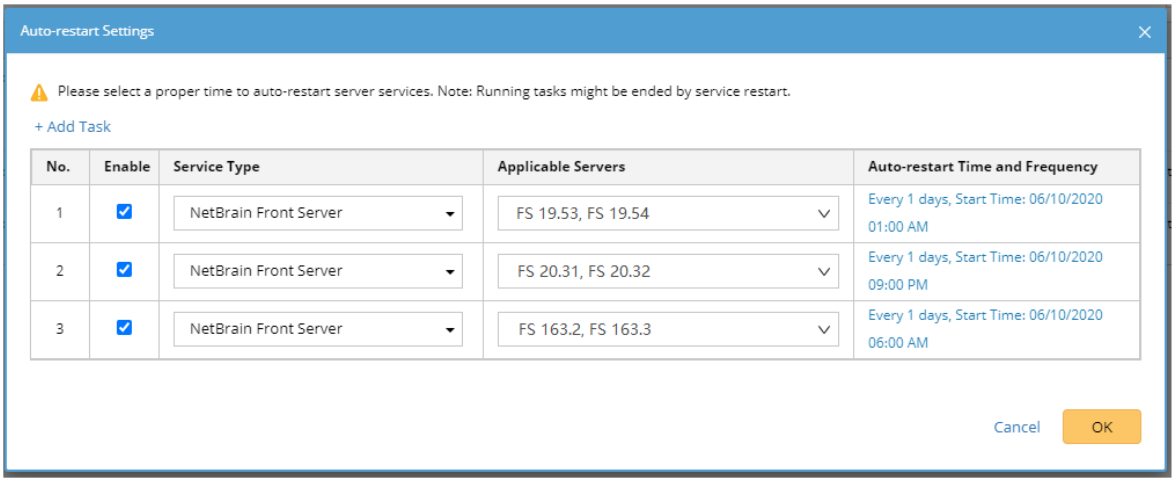
In parallel to in-system alerts, IEv8.03 provides the email alerting function to push alerts when a server is disconnected, or service is stopped. By default, this email alerting function is disabled.



2.9.3.Service Auto-Restart Settings By Server

For customers with a large scale of networks, especially with many Front Servers, IEv8.03 provides a more flexible service auto-restart mechanism for different servers. It allows you to customize multiple auto-restart rules for a single service on a few selected servers.

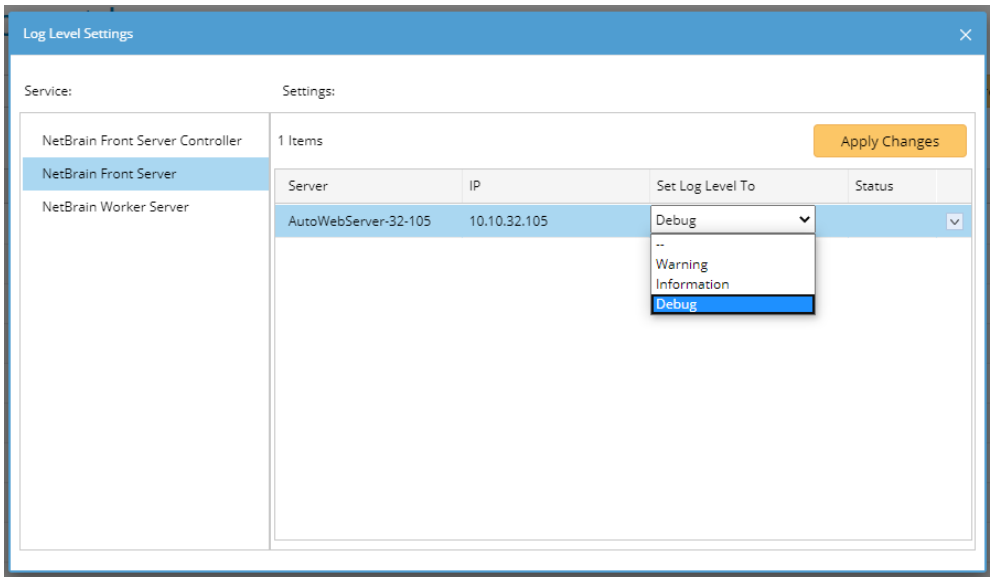
For example, the following figure shows three auto-restart rules have been applied to six Front Servers.



2.9.4.Enhanced Log Collection

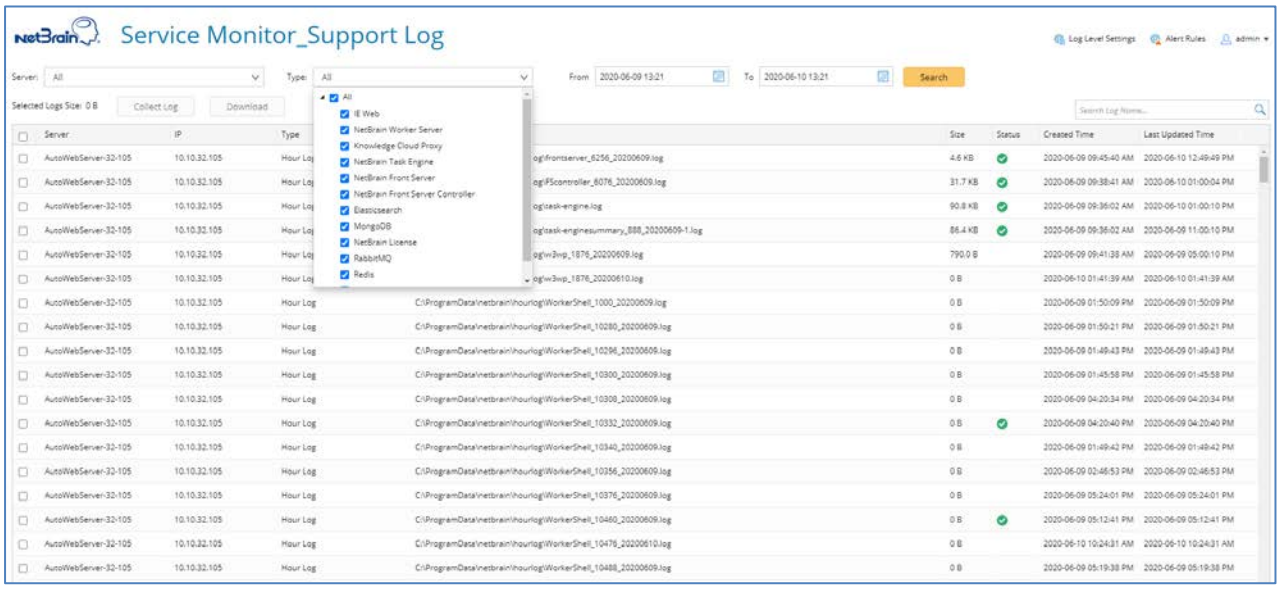
To accelerate the debug process, IEv8.03 separates the log search process and log collection process to improve performance and introduces more enhancements to system log collection, including:

- Allow you to collect different levels of logs for services on different servers.

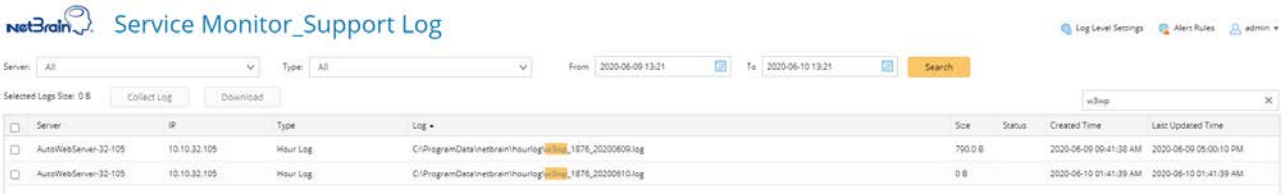


Note: The log level setting is only available to Worker Server, Front Server, and Front Server Controller.

- Allow multi-selection of server/service types as filters.



- Add log file name as one of the search terms.



2.10. More Feature Enhancements

2.10.1. Map User Roles and Privileges from TACACS+ to NetBrain

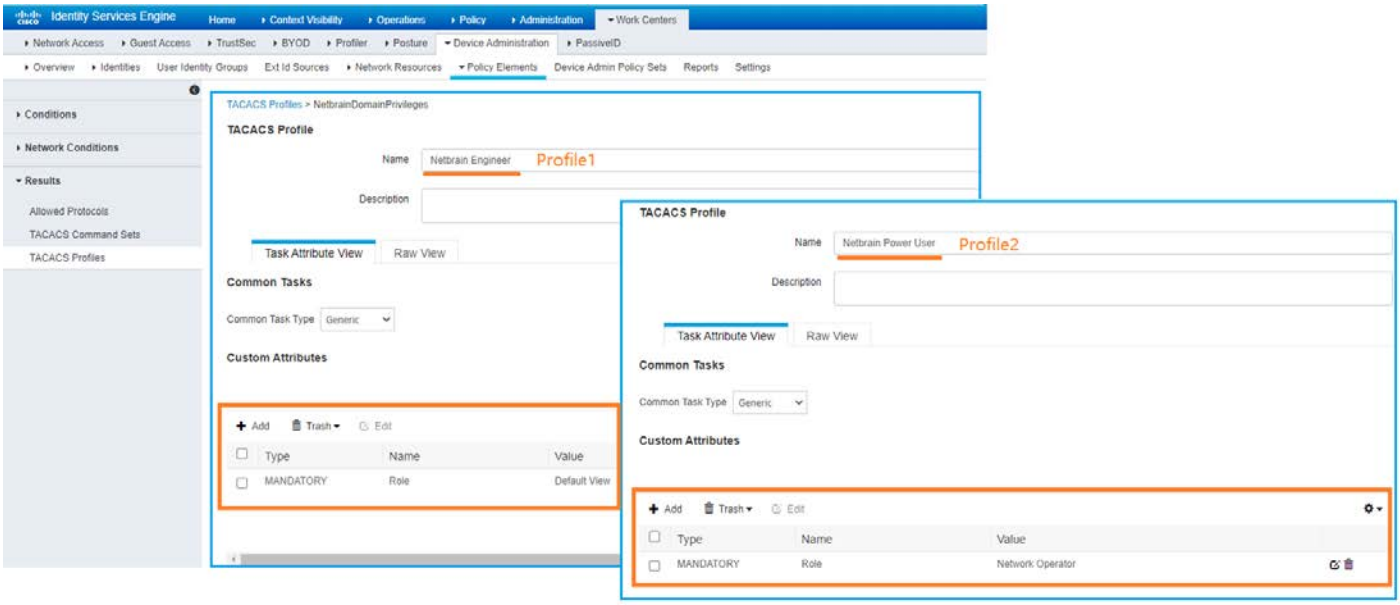
The existing TACACS+ authentication method grants all the external user accounts with the same role (privileges), and the roles can be changed after your first-time login.

The IEv8.03 system provides a new TACACS+ authentication method to assign granular user roles and privileges by mapping roles from the TACACS+ server to NetBrain IE system. Thus, external user accounts can keep finer-grained roles and privileges in good shape before their first-time login to the IE system.

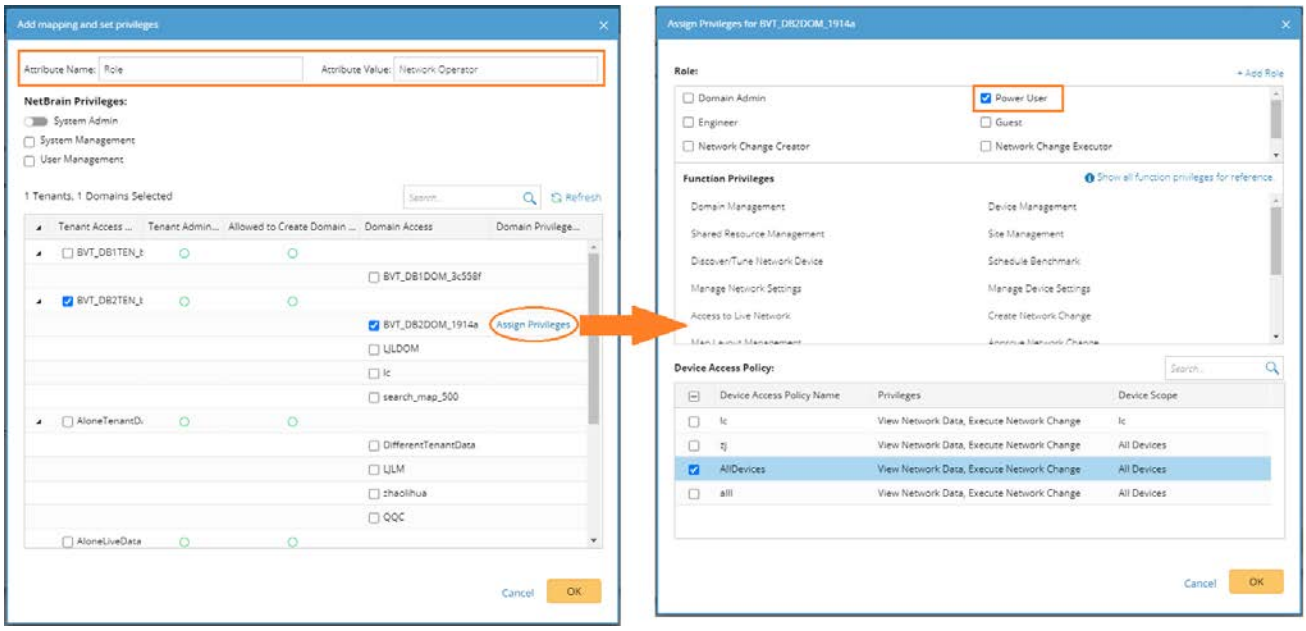
Note: The new TACACS+ authentication only applies to Cisco ISE and Cisco ACS 5.x.

Use Flow

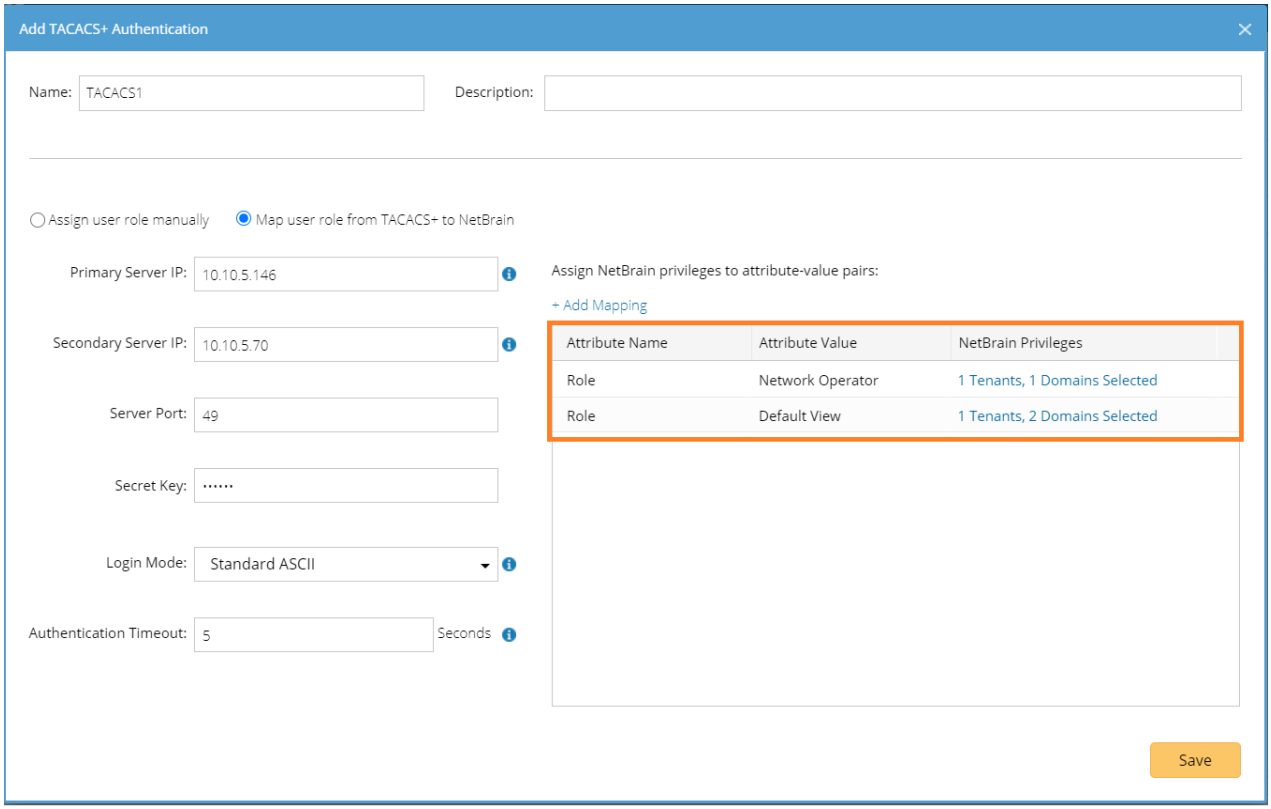
For example, you have two TACACS profiles with two different roles defined in your ISE system, and you want to map them respectively to NetBrain IE roles “Power User” and “Engineer”.



1. When configuring TACACS authentication, add a role mapping from TACACS (**Role/Network Operator**) to NetBrain (**Power User**).



2. Repeat step 1 to add a role mapping from TACACS (**Role/Default View**) to NetBrain (**Engineer**), and save.



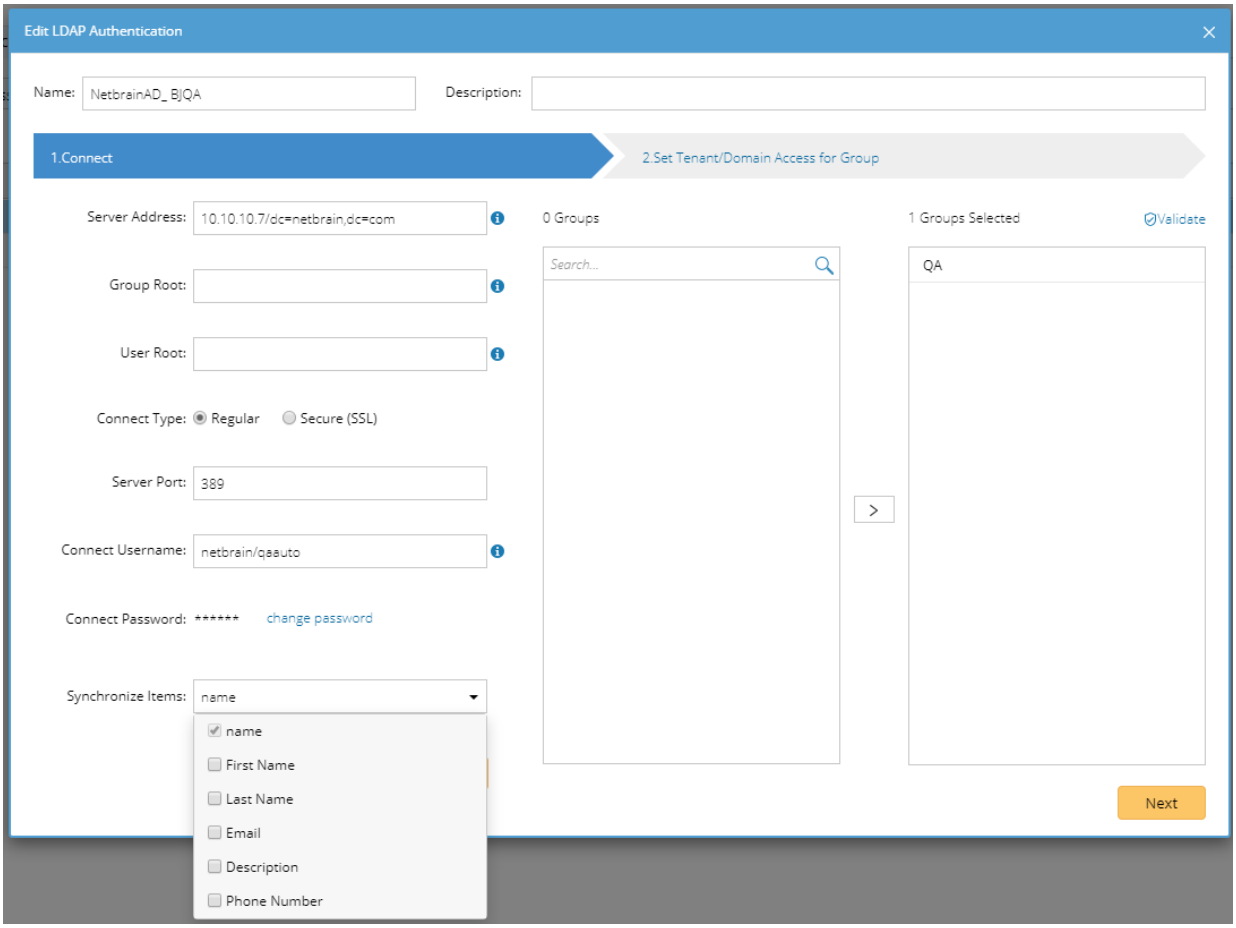
When authenticating TACACS+ users' login, the NetBrain system checks the attribute name and value of their roles in the TACACS+ server. It assigns the corresponding roles and privileges of the IE system to them.

Note: Once external users have logged in to the IE system, their roles and privileges can be manually changed and locked. Locked user roles and privileges will not be synced with any changed authentication settings.

2.10.2. Allow Selection to Sync User Data for LDAP/AD Authentication

In earlier versions, the system synchronizes all the attributes of LDAP/AD user accounts by default when authenticating these external accounts. To meet specific security requirements, the IEv8.03 system allows you

to determine the user data that can be synced in the LDAP/AD authentication process.

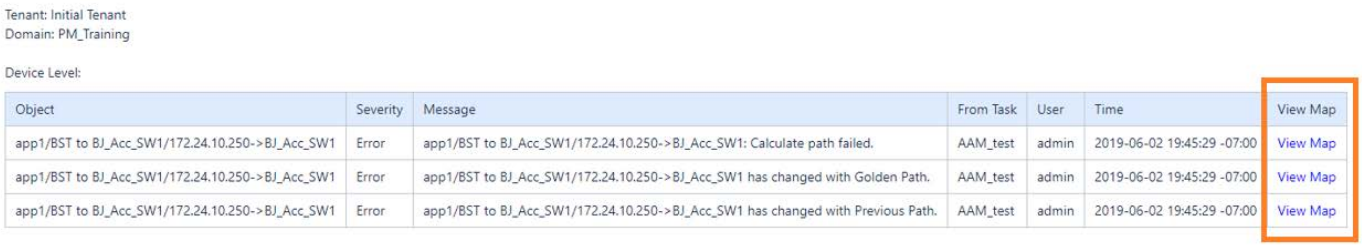


2.10.3. Direct Map Access from Alerting Email

In previous versions, alerting emails generated for Qapp/Data View Template, etc., did not provide a "View Map" link for you to quickly address the problematic map in the IE system. This was because the Worker Server cannot perceive the required information from the Web Server to compose the map URL under the infrastructure at that time.

In the context of the **Server Base URL** setting (**System Management > Advanced Settings > Site Configuration**) introduced in IEv8.02, the "View Map" link has been implemented and introduced in this IEv8.03 release to enhance the user journey.

The following figure shows a sample email with the new "View Map" function added to each alert message:



Tenant: Initial Tenant
Domain: PM_Training

Device Level:

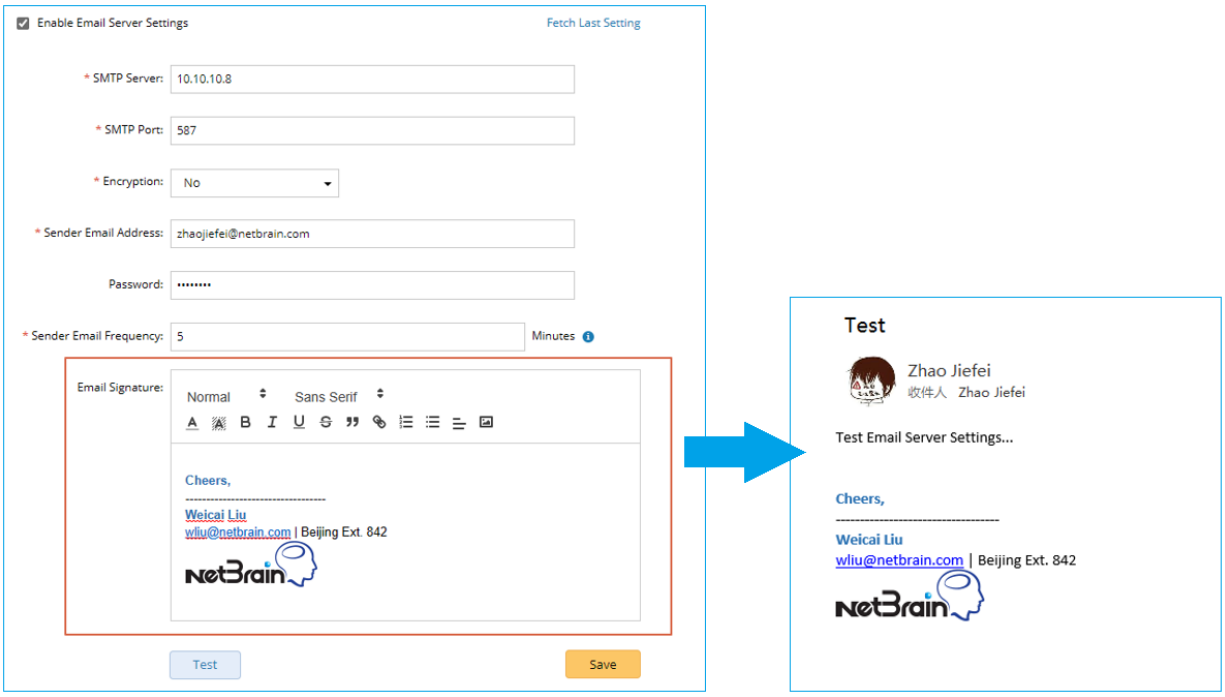
Object	Severity	Message	From Task	User	Time	View Map
app1/BST to BJ_Acc_SW1/172.24.10.250->BJ_Acc_SW1	Error	app1/BST to BJ_Acc_SW1/172.24.10.250->BJ_Acc_SW1: Calculate path failed.	AAM_test	admin	2019-06-02 19:45:29 -07:00	View Map
app1/BST to BJ_Acc_SW1/172.24.10.250->BJ_Acc_SW1	Error	app1/BST to BJ_Acc_SW1/172.24.10.250->BJ_Acc_SW1 has changed with Golden Path.	AAM_test	admin	2019-06-02 19:45:29 -07:00	View Map
app1/BST to BJ_Acc_SW1/172.24.10.250->BJ_Acc_SW1	Error	app1/BST to BJ_Acc_SW1/172.24.10.250->BJ_Acc_SW1 has changed with Previous Path.	AAM_test	admin	2019-06-02 19:45:29 -07:00	View Map

The following table lists the landing page after you click on the "View Map" link, which depends on different tasks.

Task	Landing Page after clicking on "View Map"
Qapp/Gapp	Target map page, with Runbook node (Qapp/Gapp) focused
Instant Qapp	Target map page, with the Instant Qapp panel opened
Schedule Qapp – Qapp Alert	▪ If the target device is a device group, path, unassigned site, or manually selected devices, then an on-demand map page will be created and opened. ▪ If the target device is a leaf site, then the leaf site map will be opened. ▪ If the target device is a container site, then the leaf site map where the problematic device belongs to will be opened.
Schedule Qapp – Path Alert	
Data View Template	Target map page, with Runbook node (DVT) focused
AAM	On-demand map page will be created and opened (alerts are detected by scheduled Benchmark tasks).

2.10.4. Enable Email Signature for System Messaging

To email uniform information in an automated way, IEv8.03 allows system administrators to set up an email signature, which will be included at the bottom of the message sent by the NetBrain IE system.



Email Signature Setting *Email Instance*

By default, the email signature is blank. To set up one, go to **System Management > Email Settings**.

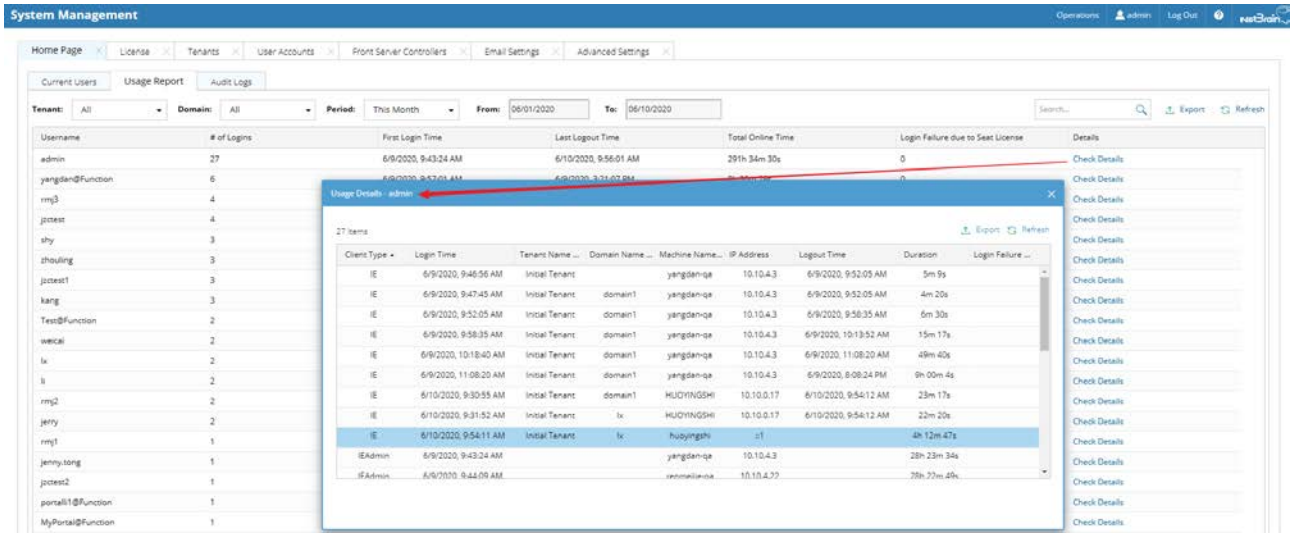
2.10.5. Allow Multiple User Accounts to Share One Email Address

To adapt to diverse customers' needs, the IEv8.03 system allows multiple user accounts to sign up using one email address. In other words, each email address can be registered to multiple user accounts in the system. Hence, the username is an identical attribute for these accounts and required as the login credential.

2.10.6. Report Online Users and Portal Users in System Usage Statistics

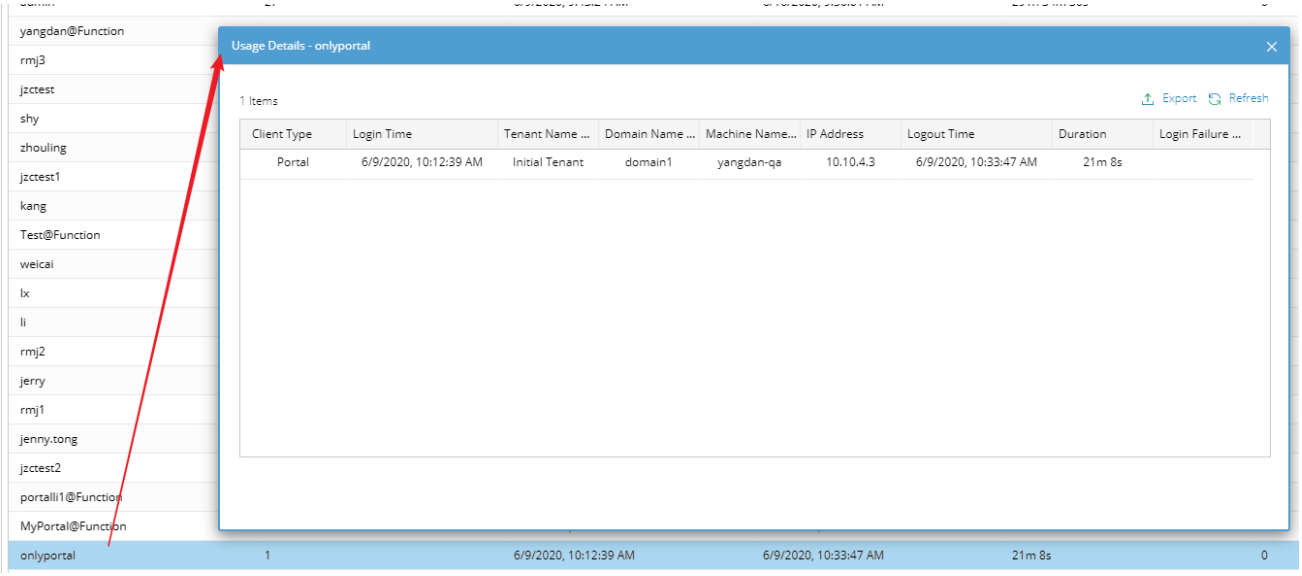
To detail more helpful information for system usage statistics, IEv8.03 introduces the following enhancements:

- Report online user accounts (the value of logout time is blank).



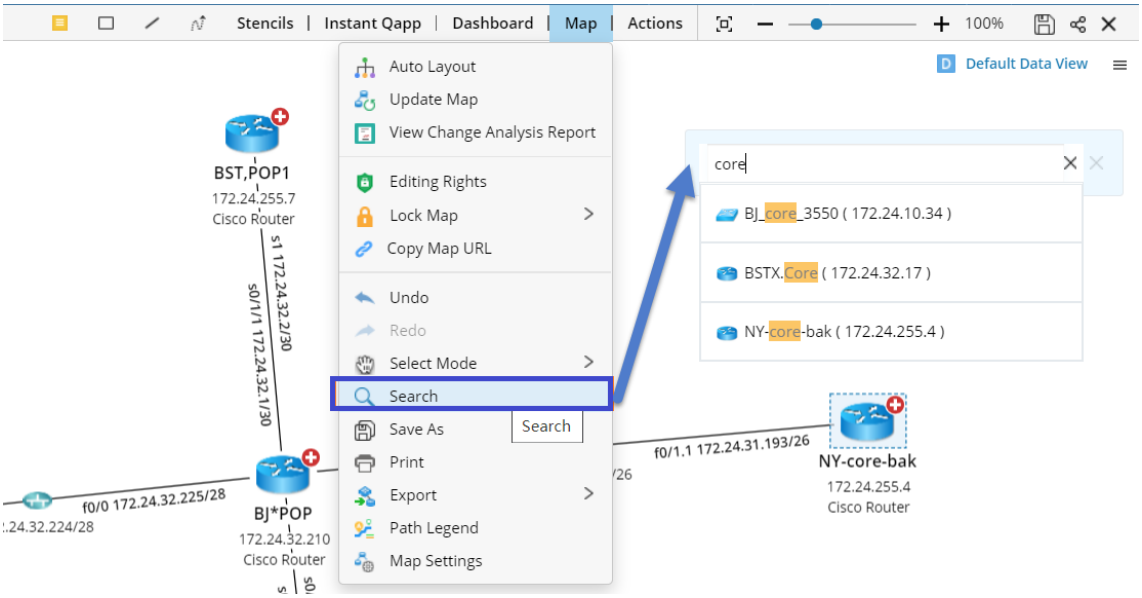
Note: A refresh is required to get the continuously increasing results of the total online time/duration for online users.

- Report portal user accounts



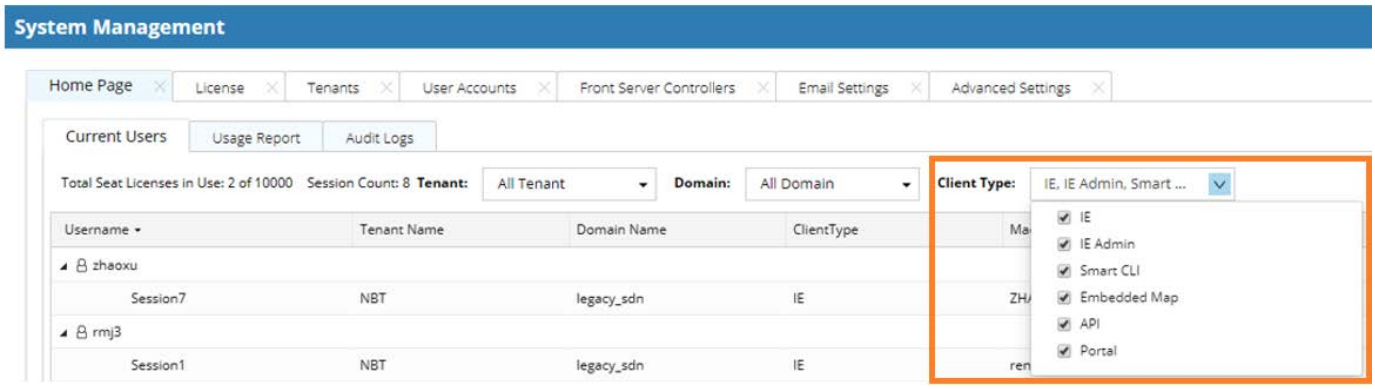
2.10.7. New Map-Based Search

IEv8.03 adds a new option **Search** to the drop-down of the map toolbar, which enables you to search for a specific device on the map by using “hostname” and “management IP” as the search term. When you click on a search result, the device will be focused and highlighted on the map instantly.



2.10.8. Optimized Categories of Logged-in User Accounts

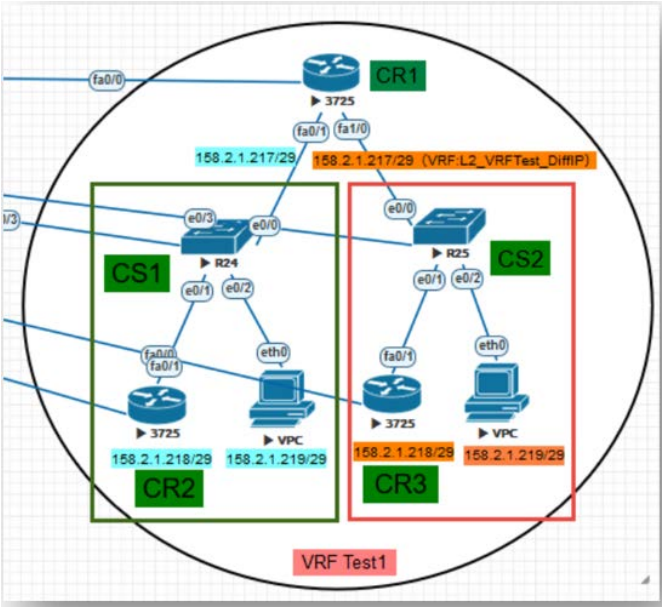
Because of the introduction of the function portal in IEv8.03, the client types of logged-in user accounts have been expanded. The client types can be viewed and used as filters both in the System Management page and Domain Management page.



Note: Only the "IE" user accounts consume seat licenses.

2.10.9. Enhanced L2 Topology Accuracy

In IEv8.03, the existing L2 topology calculation algorithm is optimized to support the scenario where duplicate IP addresses with different VRFs configured on the device (as shown in the figure below).

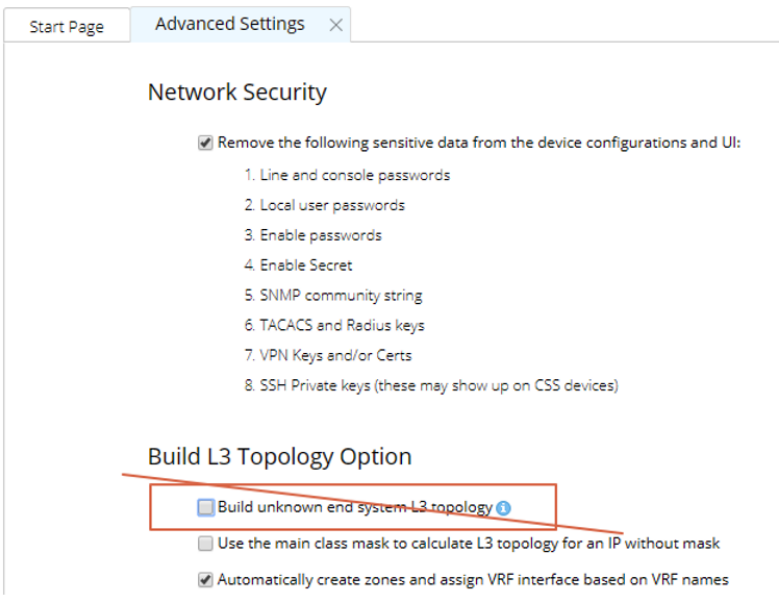


2.10.10. Enhanced Performance to Build L3 Topology for Unknown End Systems

In previous versions, the system added the option as one of the domain's advanced settings to build L3 topology links for unknown end systems, which brought benefits to L3 path calculation. On the contrary, it also brought potential performance risks to process such a huge amount of data.

To balance system performance and required functionality, IEv8.03 removes the option of building L3 topology links for unknown end systems, but introduces an alternative solution, including:

- When finding the next hop is an unknown end system, the system processes the path script to ensure the unknown end system can be mapped out along the path.
- The system will not delete L3 links for unknown end systems when auto-updating maps.
- The system will not automatically extend unknown end systems as L3 neighbors.



3. Platform Enhancements

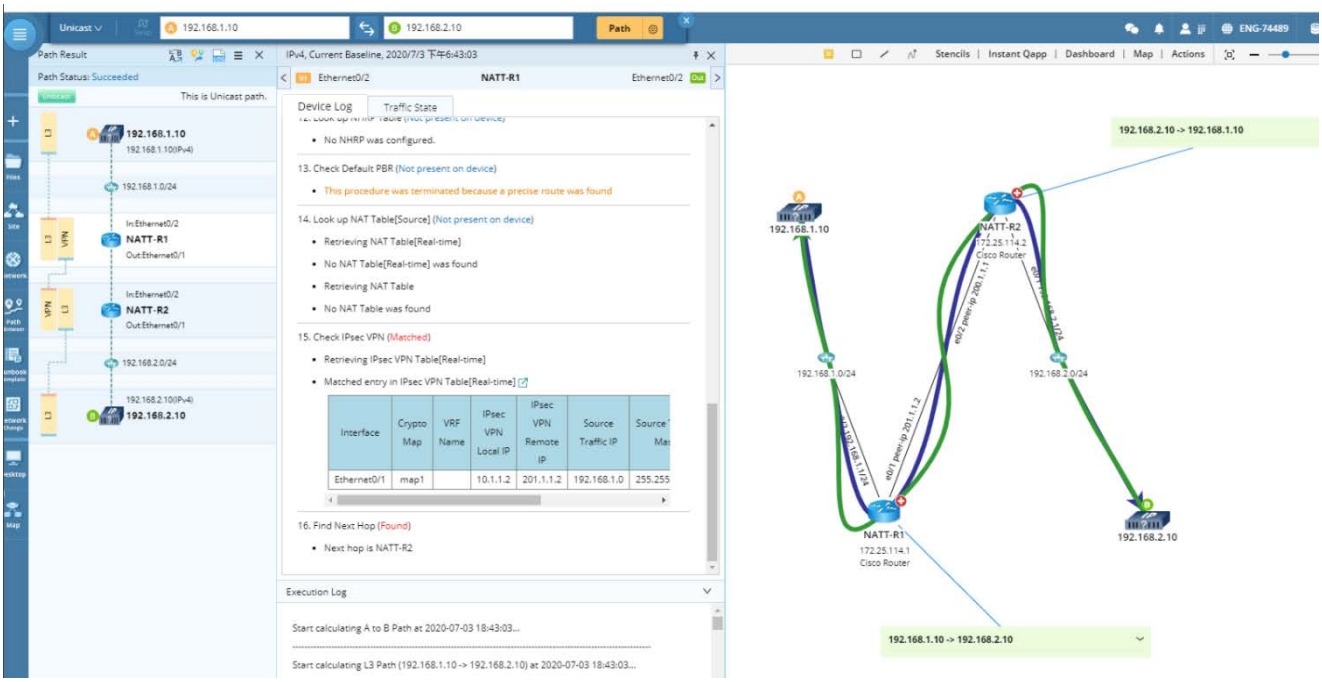
3.1. New Tech Support

IEv8.03 introduces multiple new techs to enable more topology related functionalities.

New Tech Name	Description
VeloCloud SD-WAN New	Support discovery, L3 topology build and path calculation for Velocloud edge and gateway.
AVI SDN New	Support discovering AVI Controller Service Engine by API, logical topology between Service Engines.
CloudGenix ION SD-WAN New	Support discovering CloudGenix ION SD-WAN devices by both API and CLI, logical topology between SD-WAN devices.
Citrix (Netscaler) SD-WAN New	Support discovering Citrix (Netscaler) SD-WAN devices by CLI.
Segment Routing - Cisco IOS XR	Support SRGB NCT table, SR Pfx Parsing, multiple IGP control plane, segment routing only deployment, SR co-existence with LDP (without sr-prefer configured/ with sr-prefer configured), multiple SR segments pushed at ingress PE.
Cisco VXLAN	Support BGP EVPN VXLAN.
Cumulus VXLAN New	Support VXLAN Peer Table, L3VNI VRF configuration, and L2 VNI path calculation.
NAT-Traversal	Support the mapping of topology and aligned devices along two-way paths.

3.1.1.NAT-Traversal Support

IEv8.03 adds the support for NAT-T (traversal), by mapping its topology and aligned devices along the two-way paths. Here is a sample screenshot:



The logic for NAT-T technology support includes:

1. When generating interfaces for IPSec VPN, the system checks all the neighbors for each hop device to determine whether any neighbor has been configured with NAT by using its GDR property `hasNATConfig`.

   (a) If yes, the system will obtain the NAT-related information, and then check whether the local IP address of the current interface has been translated to an outside global address in the NAT table.

   (i) If yes, the system will save the information of the outside global address to the GDR property `NAT outside global` of the interface.

   (b) Repeat (a) until all devices have been checked.

2. During the Qapp automation for IPsec VPN topology calculation, the system will link two interfaces (**A** and **B**) when the following two conditions are met:

   - The VPN local IP address of **A** equals to the remote IP address of an interface **B**.
   - The remote IP address of **A** equals to the NAT outside global address of **B**.

3.2. Enhanced Platform Framework

3.2.1.Customize Interactive Commands in Driver for Live Data Retrieval

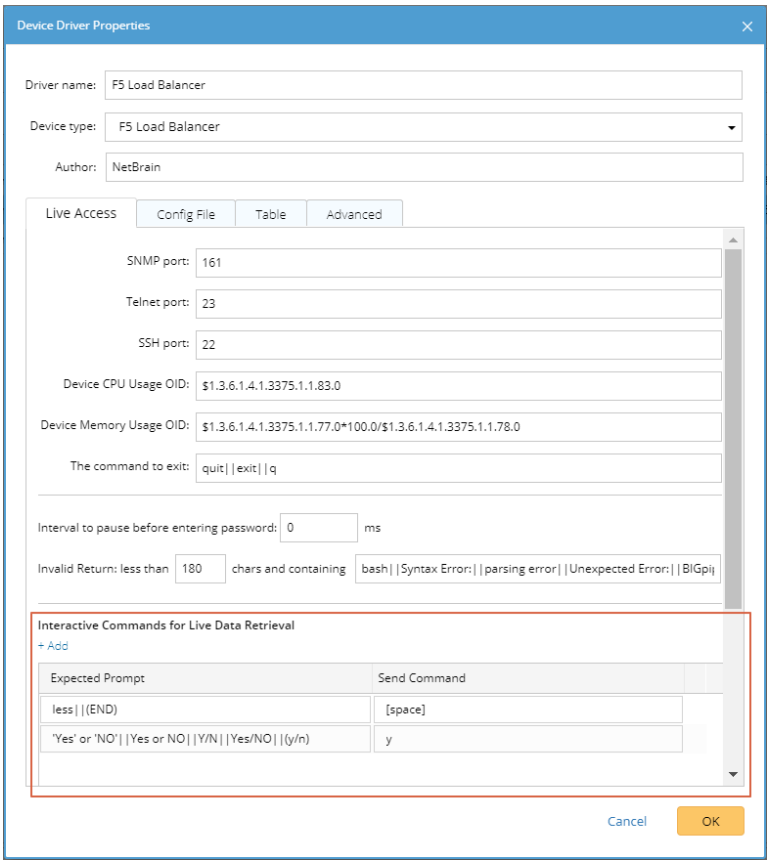
When the system attempts to access devices in a live network, some devices may return particular CLI prompts and pause the process until getting a valid response. In earlier versions, the system has already built the support of custom driver definition for the following two interactive cases:

- Respond "Y" to resume when "Yes/No" is returned in the prompt.
- Respond a whitespace when a page break appears in the returned prompt.

To adapt to more diverse CLI interactive scenarios, IEv8.03 allows you to customize interactive commands depending on the different CLI characteristics of different devices from both global and individual perspectives.

Define Generic Interactive Commands for Devices Applying the Same Driver

IEv8.03 introduces the "Interactive Commands for Live Data Retrieval" settings in driver definition for you to define the generic interactive commands for devices that use the same driver. Besides the exiting two pairs of expected prompt and responsive command, you can add more pairs.



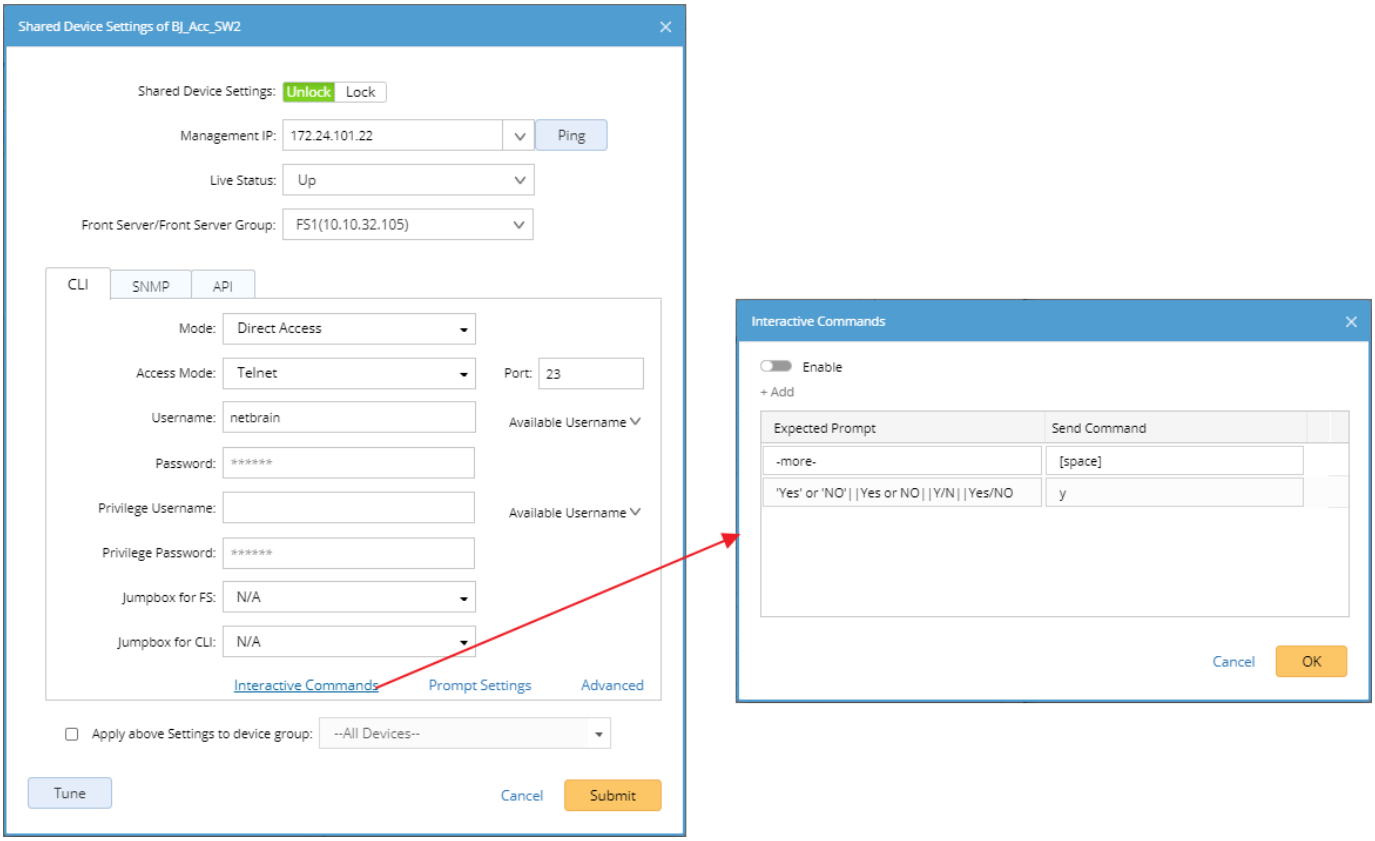
Notes:

- The built-in two pairs cannot be deleted, but can be modified.
- Use "||" to separate multiple expected prompts, and use "regex:" as suffix for regular expressions.
- Use "[ ]" to include a keyboard key or a key combination. For example, [Ctrl + q].

Define Interactive Commands for Individual Device

IEv8.03 introduces the customized interactive commands for each device in the Shared Device Settings, which takes priority over those defined in drivers. That is, once the interactive commands are defined and enabled the Shared Device Settings of a device, the system will not apply those defined in its associated driver to the device.

By default, the customization of interactive commands in the Shared Device Settings is disabled, indicating that those commands predefined in its device drivers will be applied.



3.2.2.Define Command Block in Driver for Live Data Retrieval

As per customer cases, the CLI command method to retrieve route table cannot be applied to the route tables with multiple VRF instances, and different commands are required to enter different modes before issuing the `show ip route` command. For example:

```
BR-K6-Albright-G27(su)->su secure
BR-K6-Albright-G27(su-secure)->show ip route

BR-K6-Albright-G27(su)->su student
BR-K6-Albright-G27(su-student)->show ip route
```

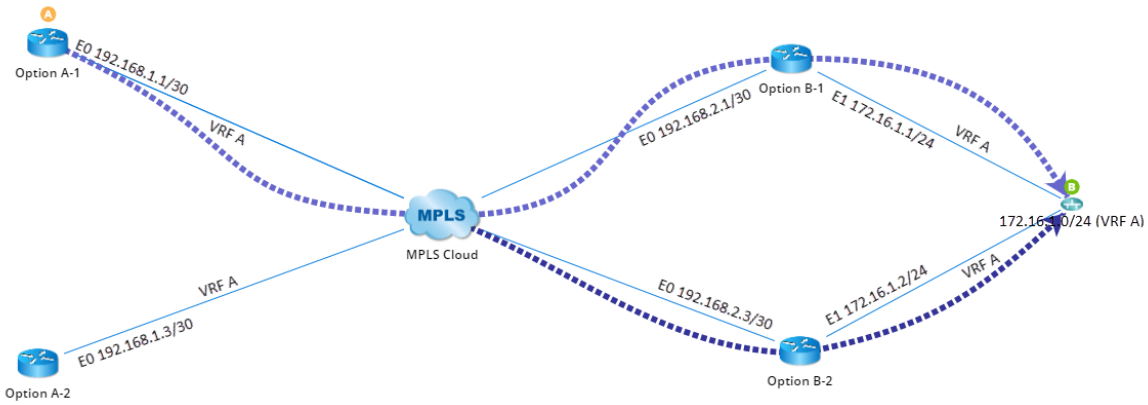
With this context, IEv8.03 introduces a new format rule to enable and standardize the use of command blocks to retrieve live data in the driver definition. For example: `CommandBlock::[["su $vrfName", ["BR-K6-Albright-G27(su-secure)>", "show ip route"], ["regex:\s\S+>", "Y"], ["regex:\s\S+>", ""]]]`

The following table explains the format of a command block in detail:

Command Block Element	Explanation
`CommandBlock::[[ ]]`	Precursor string, indicating the following content is a command block (JSON array).
`"su $vrfName"`	The first command in a command block, which is also the only one that will be issued without any conditions.
▪ `["BR-K6-Albright-G27(su-secure)>", "show ip route"]` ▪ `["regex:\s\S+>", "Y"]` ▪ `["regex:\s\S+>", ""]`	Command pairs, including the expected prompt and responsive command. Multiple string pairs can be attached in a command block. **Tips:** Regular expression can be used to define an expected prompt. The **Ctrl + C** keys and **whitespace** can be used to define a responsive command.

3.2.3.MPLS Inter-AS Support

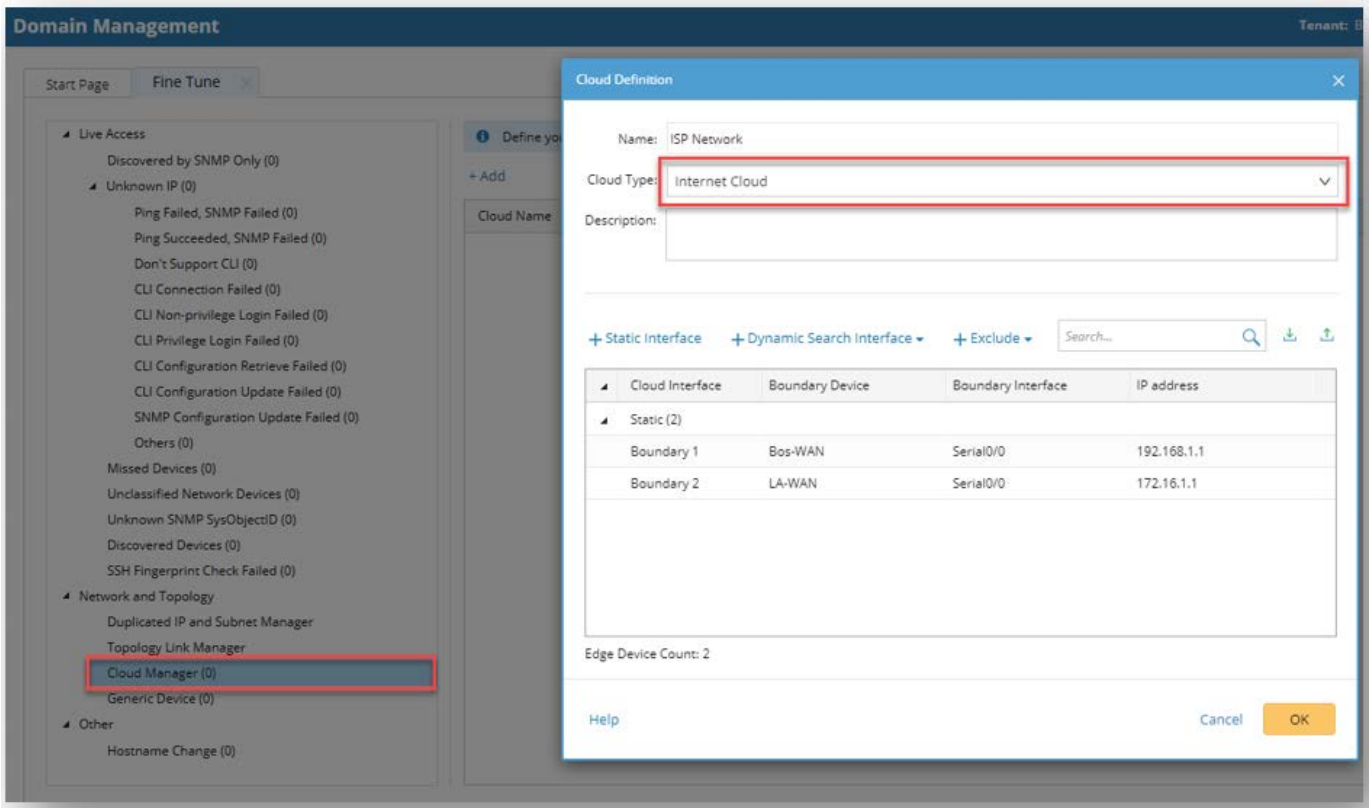
In IEv8.03, the MPLS Cloud has been expanded to support two deployment methods: option A (Back to Back VRF) and option B (Multiprotocol EBGP for VPNv4) in MPLS inter-AS. You can add the CE device and CE interface to the MPLS Cloud through static addition or dynamic search via BGP AS to support topology and path calculation.



Note: If the CE device deployed by option B is included in the MPLS Cloud, you need to select the BGP All VPNv4 Advertised Route Table NCT table in the server benchmark task to complete the calculation of the MPLS Cloud virtual route table.

3.2.4.Internet Cloud Adjustment

In IEv8.03, the internet cloud is integrated into the new cloud framework (offered in v8.02) as a new cloud type. Starting from this version, NetBrain will use this new cloud framework to simulate various types of inaccessible networks in the customer's environment. According to the network deployment methods of different customers, the platform team is responsible for maintaining the existing cloud types and adding new cloud types.



Notes:

1. The definition entrance of Internet cloud is different from the previous version. It is now located in the cloud manager interface.
2. Compared with the previous version, an additional cloud interface is required for static addition. Cloud interface has no format requirements, it can be defined according to your specific needs.
3. In addition to static addition, automatic addition is also provided through advanced search.

3.3. Enhancements to Path Framework

3.3.1.Replicate Active Path Calculation with Auto-Saved Data

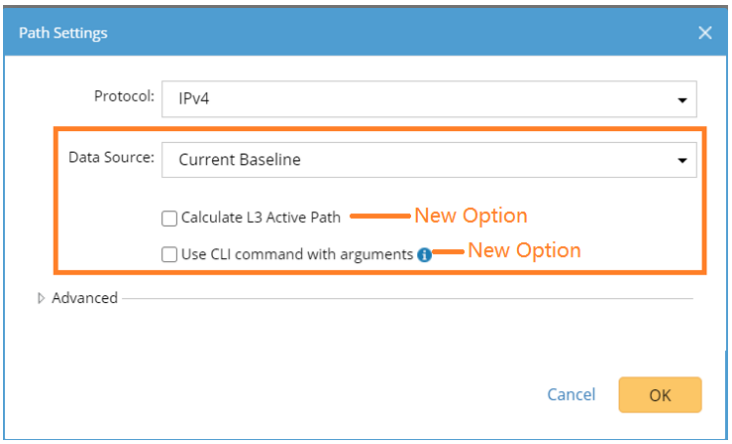
In earlier versions, it was usually difficult for the Platform Team to debug Active Paths for customers. This was because the data retrieved for the Active Path Calculation cannot be saved and reused in another system environment.

To enhance the supportability, IEv8.03 automatically saves the specific commands when calculating an Active Path and also the returned results to the current baseline for future reuse.

3.3.2.Calculate L3 Active Path with Baseline Data

Customers may encounter path calculation failure when Juniper devices are involved. This is because some data tables are too large to be retrieved. For example, the file size of a VPNv4 table is 8GB.

In parallel with the backend optimization of data acquisition, transmission, and storage, IEv8.03 also adds two options when using baseline data to calculate A/B path. That is, the system allows you to calculate L3 Active Path as well, and also use CLI commands with arguments, such as `show ip route 1.1.1.1`, to narrow down the data processing scope.



Limitations:

- This function of using CLI command with arguments only applies to most device types, but not all.
- Whether the data can be retrieved by specific CLI commands depending on both the data existence and data matching. With these conditions, the path scripts can determine whether to use CLI commands with arguments.

3.3.3.Optimized Conditions to Determine Next-hop Device

When it comes to path calculation logic, the system always looks up the source IP address in the ARP table, for example, the ARP table of a VXLAN anycast gateway or HSRP device, to determine the next hop. If there is a matching one in the ARP table, that device will be identified as the next hop; otherwise, the calculation will fail. However, the fact that the first hop of a path is not a VXLAN or HSRP device may happen, and cannot be supported due to the lookup limitation.

To support this case, IEv8.03 adds a supplementary condition when the above condition cannot be met — the system will look up the outgoing interface IP of the device, which can be calculated and confirmed along a path, in the ARP table of VXLAN anycast gateway or HSRP device. If there is a matching one in the ARP table, that device will be identified as the next hop; otherwise, the calculation will fail.

3.4. New REST APIs

IEv8.03 introduces the following new REST APIs:

API	Description
Get Audit Logs	Call this API to get the overall system license node information.
Get Shared Device Settings	Call this API to get shared device settings in current domain.
Update Device CLI Settings	Call this API to update device CLI settings in current domain.

3.5. Enhancements to Deployment and Installation

- Add Support for RHEL/CentOS v7.8
- Allow customized installation path for Linux Front Server
- Unify the installation/upgrade log path to **C:\NBIEInstall** for all Windows components
- Upgrade third-party dependencies to the latest
    - Upgrade Redis from 5.0.4 to 6.0.4
    - Upgrade IPWorks SSH from 2016 to 2020

- Upgrade Jquery from 3.4.1 to 3.5.1