Product Highlights

Centralized Device Management

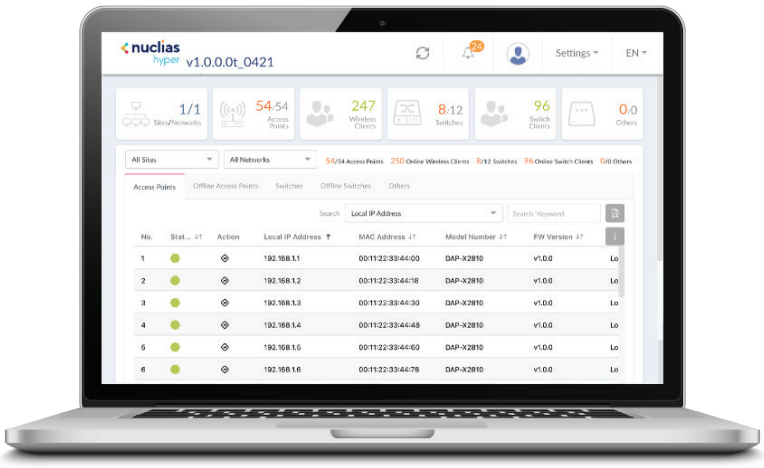
Allows centralized configuration and firmware updates for up to 2000 devices, ensuring optimized and secure devices.

Role-Based Administration

The platform provides role-based access control, ensuring users only have relevant permissions, improving efficiency and security.

Real-Time Monitoring and Alert Notifications

Offers real-time monitoring and alerts, enabling quick responses to network issues and anomalies.



DNC-5000

On-Premises Software Network Controller

Key Features

- Manage up to 2000 APs and core/aggregation/edge switches
- Multi-tenant and role-based administration
- Intuitive user interface
- Remote configuration and batch configuration
- Centralized firmware upgrade (APs/switches)
- sFlow support (core switch only)
- Traffic reporting and analytics
- Searchable and auditable event and audit logs
- Front desk ticket management
- Multilingual support

Welcome to the DNC-5000 On-Premises Software Network Controller, a smart network management platform to analyze, automate, configure, optimize, scale, and secure your network, delivering the convenience of an enterprise wide management solution at a fraction of the cost. The DNC-5000 is a comprehensive network management platform designed to monitor and manage D-Link access points and switches. This integrated solution tailored for on-premises deployment encapsulates a rich spectrum of functionalities aimed at enhancing network oversight and control. What sets DNC-5000 apart is its accessibility; the software is offered at no cost to the user, making advanced network management capabilities available without the financial burden.

Centralized Device Management

The DNC-5000 simplifies network administration by allowing administrators to manage all devices from a single platform. This eliminates the need to access each device individually, saving time and reducing human error. Administrators can automate and schedule configurations, ensuring consistency across devices and reducing manual effort. For example, changes made to network settings or security policies can be deployed across multiple devices simultaneously, streamlining operations and ensuring uniformity. Additionally, firmware updates can be scheduled and applied to all devices at once, ensuring devices remain up-to-date and secure without interrupting network services. This approach not only increases efficiency but also enhances network security and performance, making it ideal for growing networks that require reliable, scalable management.

DNC-5000 On-premises Software Network Controller

Role-Based Administration

Role-based administration is a cornerstone feature of DNC-5000, introducing a structured approach to network management. This functionality allows for the delineation of user roles and permissions, enabling a tailored administrative experience and enhancing network security by ensuring that users only access the features necessary for their role.

Real-Time Monitoring and Alerts

Enable administrators to continuously track network health, performance, and usage from a centralized dashboard. This provides a comprehensive view of network activity, allowing for quick identification of potential issues before they impact operations. Instant alerts notify administrators of anomalies or changes, facilitating prompt responses to mitigate risks and maintain network integrity. Detailed performance reports provide valuable insights into network traffic, device status, and overall efficiency, helping to optimize resource allocation and prevent downtime. By monitoring in real-time, administrators can ensure that the network is functioning at its best, while minimizing the risk of disruptions, enhancing security, and improving overall operational efficiency.

Traffic Reporting and Analytics

Provides advanced traffic reporting and analytics features, helping administrators gain deep insights into network usage. Through real-time data visualization, administrators can clearly see traffic trends, device usage, and potential bottlenecks. These detailed insights help identify network efficiency issues and optimize performance, ensuring the best allocation of resources. Customizable reports allow administrators to generate precise data based on different needs, enabling more effective network upgrade planning and strategy adjustments. Additionally, traffic analytics helps forecast future demands, supporting decision-making processes and enhancing overall network performance.

VLAN and Access Control

Offers robust network segmentation and security features, allowing administrators to control access to different parts of the network. VLAN enables the logical division of networks, improving efficiency and reducing congestion by isolating traffic. With advanced access control features, administrators can define which SSID has access to specific network resources based on roles, ensuring only authorized users can access sensitive data or critical systems. In addition, VLANs allow for easier management of network traffic, helping to prioritize important traffic and optimize bandwidth usage. The combination of VLAN and access control provides a scalable, secure, and efficient network architecture that supports both performance and security requirements, while also simplifying network management and troubleshooting.

Auto-RF Management and Bandwidth Optimization

Improve wireless performance by automatically adjusting radio frequency (RF) settings such as channel selection and power levels. This ensures optimal wireless coverage, minimizes interference, and maximizes network stability. The system dynamically monitors the wireless environment and makes real-time adjustments, adapting to changing conditions and traffic demands. Bandwidth optimization ensures that resources are allocated efficiently, prioritizing critical applications and preventing network congestion. This combination of RF management and bandwidth allocation enhances user experience by delivering consistent and reliable connectivity, even in dense environments with multiple devices. Additionally, it reduces manual configuration and troubleshooting efforts, making it easier to maintain high-performing wireless networks.

Multi-SSID and Captive Portal Authentication

Allow administrators to create multiple, isolated networks within the same infrastructure, tailoring each network for specific user groups such as employees, guests, or partners. This feature improves network security by segmenting traffic and ensuring that each group only has access to the resources they need. The Captive Portal Authentication provides secure and customizable login options for both guests and employees, offering flexibility in access methods such as username/password, click through, or passcode. This enhances security by ensuring that unauthorized users cannot easily access sensitive parts of the network. Additionally, the Captive Portal can be branded with a company's logo or messages, providing a seamless user experience while maintaining robust access control. This solution is ideal for businesses looking to offer secure, efficient, and user-friendly wireless access.

Centralized Firmware Upgrade

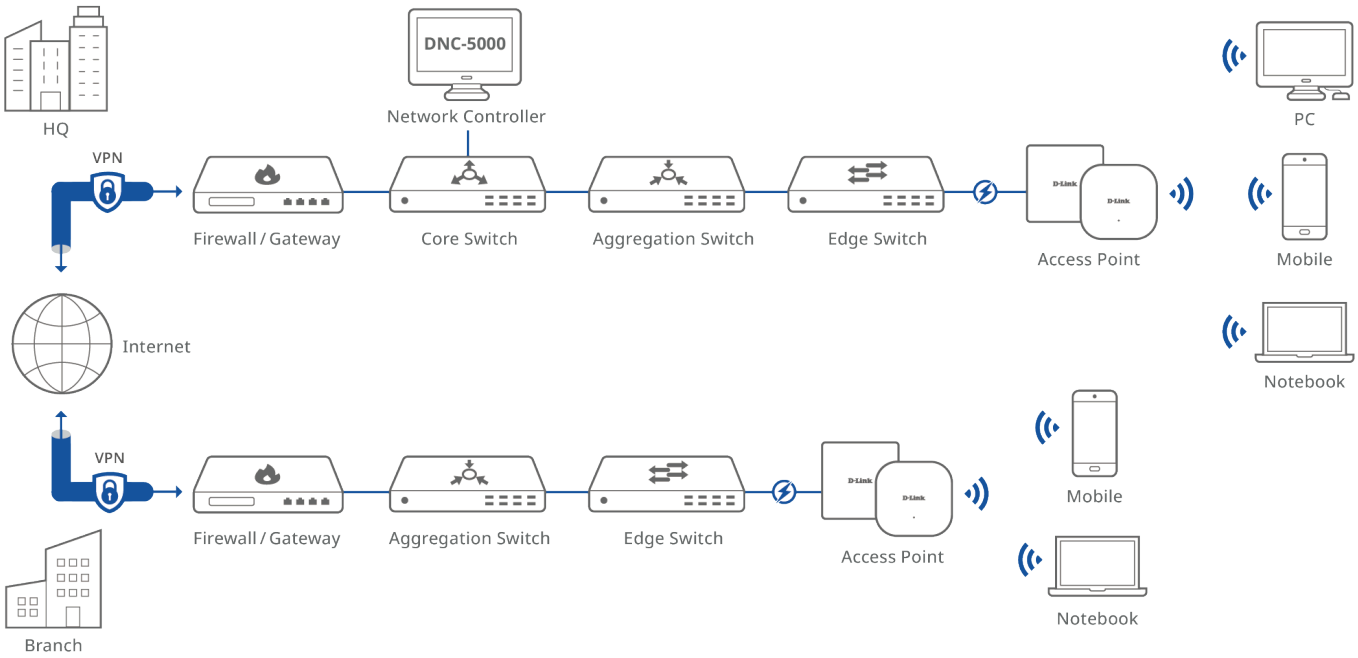
Allows administrators to efficiently manage and deploy firmware updates across multiple devices from a single platform. This feature eliminates the need for manual updates on each device, saving time and reducing the risk of errors. Administrators can schedule updates at convenient times, minimizing network downtime and ensuring that all devices are running the latest security patches and performance improvements. By centralizing the upgrade process, the platform ensures consistency across the network, reducing compatibility issues. Additionally, real-time monitoring of the update status helps identify any failures and enables quick troubleshooting. This approach simplifies device management, enhances network security, and ensures that devices are always optimized and up-to-date, supporting scalable network operations.

DNC-5000 On-premises Software Network Controller

Minimum System Requirements

	Large Scale Networks	Small Scale Networks
Recommended Processor	Intel 12th i7 or later	Intel 12th i5 or later
Recommended RAM	32G	16G
Recommended Storage	4TB	1TB
Ethernet NIC	Gigabit Ethernet card	Gigabit Ethernet card
Monitor resolution	1080P	1080P
Platform	Windows Server 2022 (64bit)	Windows 11 Pro(64bit), Linux Ubuntu
Management Browser	Edge, Chrome and Safari	Edge, Chrome and Safari

Connection Diagram



DNC-5000 On-premises Software Network Controller

Specifications

Nuclias Hyper[1] Features

Dashboard

Displays network status summary and device list, click Redirect button in Action item to device management page for more details.

- Network Status
- Alert Notification
- Device List-Access Point
- Device List-Offline Access Point
- Device List-Switch
- Device List-Offline Switch
- Device List-Others

Connection Settings

Provides the link to redirect to Nuclias Connect and NMS

User Management

List users and user privileges; create user for system management

User Level:

- Manager
- User

User Privilege (NMS):

- Org Admin
- Site Admin
- Network Admin
- Network Local User

User Privilege (Nuclias Connect):

- Root Admin
- Root User
- Local Admin
- Local User
- Front Desk User

Log

Displays all audit and alert logs

System Backup & Restore

Backup and restore configuration of Nuclias Hyper, which includes user management settings, SSL certificate management settings, and SMTP settings

SSL Certificate Management

The SSL certificate is self-signed at default settings, it also allows auto signing by third-party Certbot

- Certificate Validity Period
- Upload Certificate
  - Manually
  - Certbot Automatically
- Upload Certificate From File
- Upload Key From File

SMTP Settings

Configure SMTP server settings. Nuclias Hyper will send password reset email if password is forgotten

- SMTP Server address
- Port
- Sender E-Mail Address
- Sender
- Security Type
- Encoding Type
- Authentication
- Test E-Mail

NMS Features

Dashboard

- Analysis
- Overview
- Switch
- Host

Monitor

- Network Discovery
- Device View
- Interface View
- Topology Map
- Connection View
- Rack View
- sFlow Analyzer
- Device Group

Configuration

- Batch Configuration
- Task Management
- Firmware Management
- Configuration Management
- File Management

Alarms and Notifications

- Alarm
- Trap & Syslog
- Trap & Syslog Editor
- Monitor & Alarm Settings
- Notification Center

Templates

- Device Template
- Device Support
- Panel Template
- Monitor Template
- Configuration Template

Report

- General Reports
- Scheduled Reports
- My Reports

Tools

- ICMP Ping
- SNMP Test
- Trace Route
- CLI
- File Comparison

System

- Basic Settings
- Scheduling
- Server Management
- NMS Log
- About

DNC-5000 On-premises Software Network Controller

Specifications

Nuclias Connect Features

Dashboard

Summarized information of site, network, access points and wireless clients will be displayed on this section

- Real time information
- Displays information in the last hour and past 7 days for following items:
  - Number of clients
  - Downlink and uplink traffic usage
  - Total traffic usage
  - Top SSID traffic usage diagram
- Channel Utilization
  - Shows channel usage information
- Event
  - Displays latest 10 event logs

Monitoring

- Access Point
  - Access Point
  - Wireless Client
  - Neighbor AP
- Switch
  - Switch
  - Switch Client
  - Switch Port

Topology

- Displays connections between devices
- Displays the on/off-line status of devices
- Displays the link status of devices
- PNG or JPG format files can be uploaded as the background image
- Supports Star and Tree topologies
- Zoom in/out of the topology map
- Export map file

Floor Plan

Floor plan is a drawing to scale, a bird's-eye view of the relationships between rooms, spaces, traffic patterns, and other physical features at one level of a structure.

Configuration

- Create Profile
- Profile Settings
- Firmware Upgrade
- SSL Certificate
- Payment Gateway
- Backup & Restore

Report

- Access Point
  - Peak Network Activity
  - Hourly Network Activity
  - Daily Network Activity
  - Most Active AP
- Switch
  - Hourly Network Activity
  - Daily Network Activity
  - Top Ranking

Log

- Device Syslog
- System Event Log
- Device Log
- Audio Log
- Alerts

Supported Devices

Access Points

Technology	Model	HW Version
Wi-Fi 7	• DAP-E9560	A1
Wi-Fi 6	• DAP-X2810 • DAP-X2850 • DAP-X3060 • DAP-X3060W • DAP-X3060OU	A1
Wi-Fi 5	• DAP-2662 • DAP-3666	A1

Switch

Technology	Model	HW Version
Core	• DXS-3610-54S/54T	Ax
	• DXS-3410-32XY/32SY	A1
	• DGS-3630-28PC/28SC/28TC/52TC/52PC	Ax
Aggregation	• DXS-3130-28/28P/32S	A1
	• DMS-3130-30TS/30PS	A1
	• DGS-3130-30S/30PS/30TS/54PS/54S/54TS	Bx
Smart Switch	• DGS-1530-10/20/28/28P/52/52P/28S/28SC	A1
	• DGS-1520-28/28MP/52/52MP	Ax
	• DGS-1510-20/28X/28XMP/28/28P/52/52X/52XMP	A1
	• DXS-1250-28YP	A1
	• DXS-1210-10TS/10MP/12SC/12TC/16TC	B1
	• DMS-1250-10S/10SP/10SPL/12TP/12/18/18P/28/28P	A1
	• DGS-1250-28X/28XMP/52X/52XMP	Ax
	• DGS-1210-10/10MP/10P/20/26/28/28MP/28P/52/52MP	Fx
	• DGS-1100-10MPV2/10MPPV2/16V2/18PV2/24PV2/24V2/26MPV2/26MPPV2	Ax

1. Nuclias Hyper is a management portal that controls two subsystems, Nuclias Connect and NMS for device management.

Actual performances may vary due to settings, cabling, temperature, network configuration, interface, device compatibility, environmental and on-site conditions, and other similar factors. References to power capability, signal or processing speed, signal range or distance, data encryption, storage capacity, display properties, or other performance metrics are based on optimal conditions derived from industry standards and provided for informational purposes only. Specifications may be subject to change without prior notice.

HQ | No. 289, Xinhu 3rd Road, Neihu District, Taipei 11494
©2025 D-Link. All Rights Reserved. D-Link and the D-Link logo are trademarks or registered trademarks of D-Link. All other third-party marks mentioned herein may be trademarks of their respective owners.
v1.00 WW