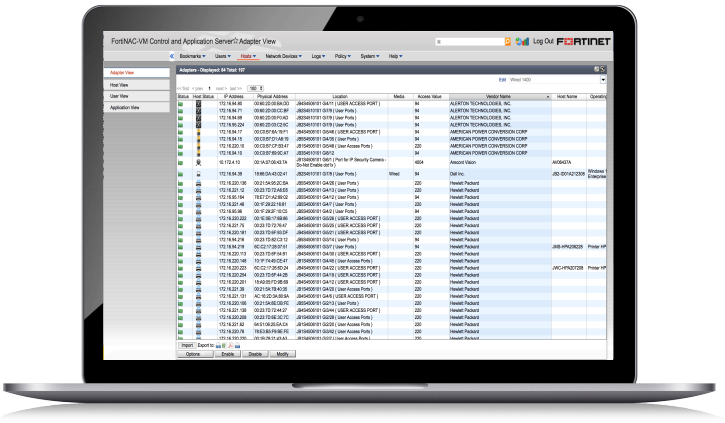
DATA SHEET

FortiNAC™

FortiNAC 500C, 550C, 600C, 700C, VM, and Licenses

FortiNAC™ is Fortinet's network access control solution that enhances the Security Fabric with visibility, control, and automated response for everything that connects to the network. FortiNAC provides protection against IoT threats, extends control to third-party devices, and orchestrates automatic responses to a wide range of networking events.



Visibility Across the Network for Every Device and User

FortiNAC provides detailed profiling of even headless devices on your network using multiple information and behavior sources to accurately identify what is on your network.

Extend Control of the Network to Third-Party Products

Implement micro-segmentation policies and change configurations on switches and wireless products from more than 70 vendors. Extend the reach of the Security Fabric in heterogeneous environments.

Automated Responsiveness

React to events in your network in seconds to contain threats before they spread. FortiNAC offers a broad and customizable set of automation policies that can instantly trigger configuration changes when the targeted behavior is observed.

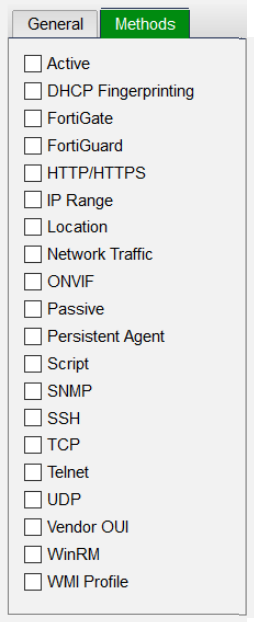
Highlights

- Agent and agentless scanning of the network for detection and classification of devices
- Create an inventory of all devices on the network
- Assess risk of every endpoint on the network
- Centralized Architecture for easier deployment and management
- Extensive support for third-party network devices to ensure effectiveness with existing network infrastructure
- Automate onboarding process for a large number of endpoints, users, and guests
- Enforce dynamic network access control and enable network segmentation
- Reduce containment time from days to seconds
- Event reporting to SIEM with detailed contextual data to reduce investigation time

Highlights

Device Visibility

Fundamental to the security of a constantly changing network is an understanding of its makeup. FortiNAC sees everything on the network providing complete visibility. FortiNAC scans your network to discover every user, application, and device. With up to 20 different techniques, FortiNAC can then profile each element based on observed characteristics and responses, as well as calling on FortiGuard's IoT Services, a cloud-based database for identification look-ups.



FortiNAC Profiling Methods for Device Classification

Scanning can be done actively or passively and can utilize permanent agents, dissolvable agents, or no agents. Additionally, FortiNAC can assess a device to see if it matches approved profiles, noting the need for software updates to patch vulnerabilities. With FortiNAC deployed, the entire network is known.

In addition to knowing the entire network, FortiNAC's enhanced visibility can also use passive traffic analysis, leveraging Fortinet FortiGate appliances as sensors, to identify anomalous traffic patterns, a possible indication of compromise that can be followed up by the SOC team.

Dynamic Network Control

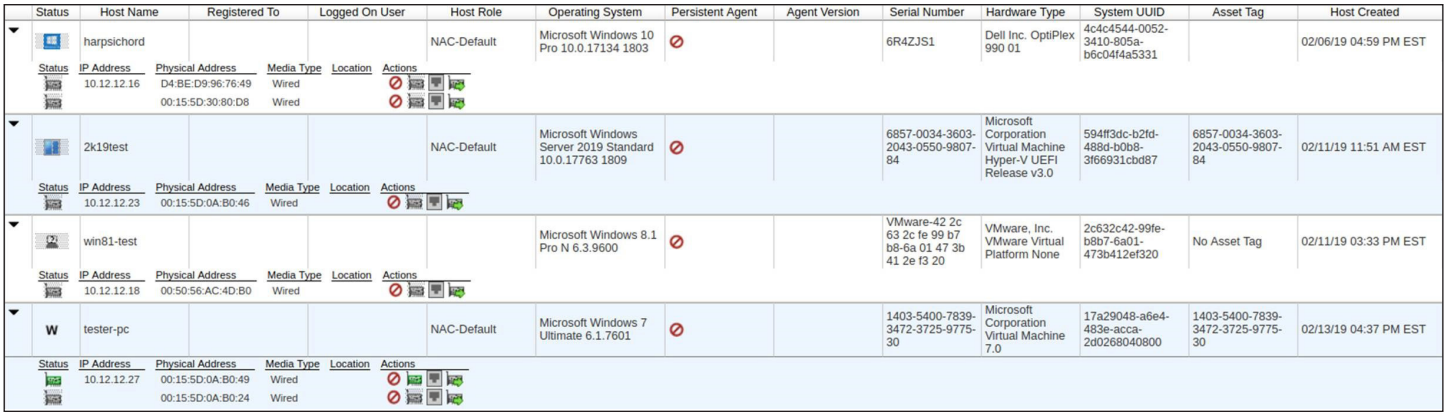
Once the devices are classified and the users are known, FortiNAC enables detailed segmentation of the network to enable devices and users access to necessary resources while blocking non-related access. FortiNAC uses dynamic role-based network access control to logically create network segments by grouping applications and like data together to limit access to a specific group of users or devices. In this manner, if a device is compromised, its ability to travel in the network and attack other assets will be limited. FortiNAC helps to protect critical data and sensitive assets while ensuring compliance with internal, industry, and government regulations and mandates.

Ensuring the integrity of devices before they connect to the network minimizes risk and the possible spread of malware. FortiNAC validates a device's configuration as it attempts to join the network. If the configuration is found to be non-compliant, the device can be handled appropriately such as by an isolated or limited access VLAN.

Automated Response

FortiNAC will monitor the network on an ongoing basis, evaluating endpoints to ensure they conform to their profile. FortiNAC will rescan devices to ensure MAC-address spoofing does not bypass your network access security. Additionally, FortiNAC can watch for anomalies in traffic patterns. This passive anomaly detection works in conjunction with FortiGate appliances. Once a compromised or vulnerable endpoint is detected as a threat, FortiNAC triggers an automated response to contain the endpoint in real-time.

Integration



Status	Host Name	Registered To	Logged On User	Host Role	Operating System	Persistent Agent	Agent Version	Serial Number	Hardware Type	System UUID	Asset Tag	Host Created
	harpsichord			NAC-Default	Microsoft Windows 10 Pro 10.0.17134 1803			6R4ZJS1	Dell Inc. OptiPlex 990 01	4c4c4544-0052-3410-805a-b6c04f4a5331		02/06/19 04:59 PM EST
	2k19test			NAC-Default	Microsoft Windows Server 2019 Standard 10.0.17763 1809			6857-0034-3603-2043-0550-9807-84	Microsoft Corporation Virtual Machine Hyper-V UEFI Release v3.0	594ff3dc-b2fd-488d-b0b8-3f66931cbd87	6857-0034-3603-2043-0550-9807-84	02/11/19 11:51 AM EST
	win81-test				Microsoft Windows 8.1 Pro N 6.3.9600			VMware-42 2c 63 2c fe 99 b7 b8-6a 01 47 3b 41 2e f3 20	VMware, Inc. VMware Virtual Platform None	2c632c42-99fe-b8b7-6a01-473b412ef320	No Asset Tag	02/11/19 03:33 PM EST
	tester-pc			NAC-Default	Microsoft Windows 7 Ultimate 6.1.7601			1403-5400-7839-3472-3725-9775-30	Microsoft Corporation Virtual Machine 7.0	17a29048-a6e4-483e-acca-2d0268040800	1403-5400-7839-3472-3725-9775-30	02/13/19 04:37 PM EST

FortiNAC Adapter View

Extensive integration with desktop security software, directories, network infrastructure, and third-party security systems provides unparalleled visibility and control across the network environment. The FortiNAC family integrates with*:

Network Infrastructure	Adtran, Aerohive, Alcatel-Lucent, Allied Telesis, Alteon, APC, Apple, Avaya, Brocade/Foundry Networks/ Ruckus, Cisco/Meraki, D-Link, Extreme/Enterasys/Siemens, H3C, HP/Colubris/3Com/Aruba, Intel, Juniper, Riverbed/Xirrus, SonicWall
Security Infrastructure	CheckPoint, Cisco/SourceFire, Cyphort, FireEye, Juniper/Netscreen, Qualys, Sonicwall, Tenable
Authentication & Directory Services	RADIUS — Cisco ACS, Free RADIUS, Microsoft IAS, LDAP — Google SSO, Microsoft Active Directory, OpenLDAP
Operating Systems	Android, Apple MAC OSX and iOS, Linux, Microsoft Windows
Endpoint Security Applications	Authentium, Avast, AVG, Avira, Blink, Bullguard, CA, ClamAV, Dr. Web, Enigma, ESET, F-Prot, F-Secure, G Data, Intego, Javacool, Lavasoft, Lightspeed, McAfee, Microsoft, MicroWorld, Norman, Norton, Panda, PC Tools, Rising, Softwin, Sophos, Spyware Bot, Sunbelt, Symantec, Trend Micro, Vexira, Webroot SpySweeper, Zone Alarm
Mobile Device Management	AirWatch, Google GSuite, MaaS360, Microsoft InTune, Mobile Iron, XenMobile, JAMF, Nozomi Networks

* FortiNAC can be integrated with other vendors and technologies in addition to those listed here. This list represents integrations that have been validated in both test lab and production network environments.

Deployment Options

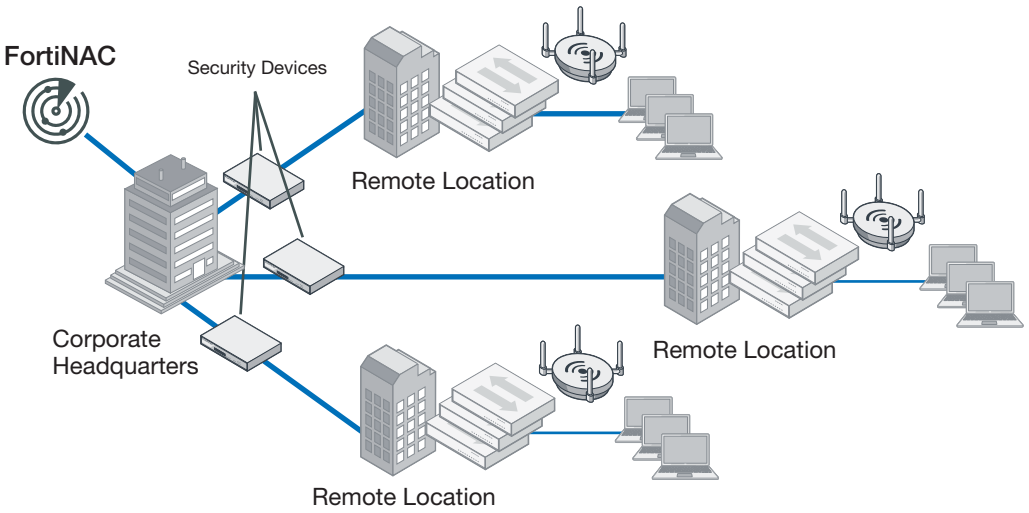
Easy Deployment

FortiNAC is a flexible and scalable solution that spans from mid-enterprise to very large enterprise deployments. There are three elements to the FortiNAC solution:

- **Application and Control** (required)
- **Management** (optional)
- **FortiAnalyzer for Reports** (optional)

The Application provides the visibility and the Control provides the configuration capabilities and automated responsiveness features. The Management portion enables the sharing of concurrent users across a multi-server deployment. FortiAnalyzer provides reports and analytics based on the information gathered from the network through FortiNAC.

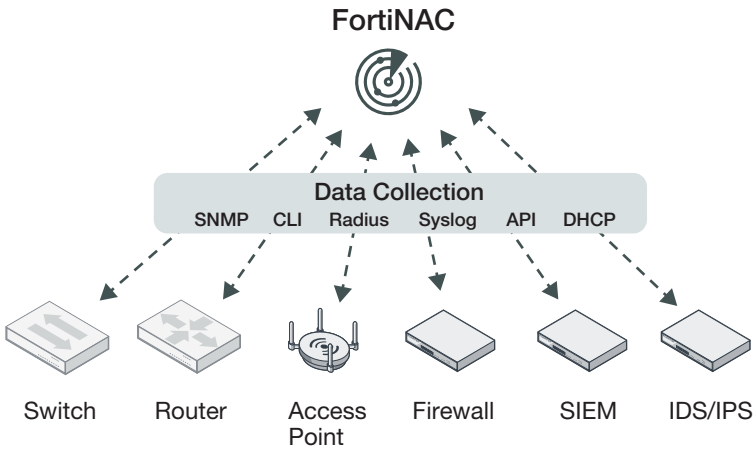
FortiNAC can be deployed in virtual machines (VMWare/Hyper-V/AWS/Azure/KVM) or on hardware appliances. The Application and Control Servers can be deployed in a variety of sizes, depending on the number of ports they need to support. FortiNAC is ideal for support distributed architectures, including SD-Branch locations.



Centralized Architecture

FortiNAC is an 'out of band' solution, meaning it does not sit in-line of user traffic. This architecture allows FortiNAC to be deployed centrally and manage many remote locations. Visibility, control and response are achieved by integrating with, and leveraging the capabilities of, the network infrastructure. Control can be applied at the point of connection, at the very edge of the network while security device integrations allow FortiNAC to process security alerts and treat them as triggers for automated threat mitigation through customizable work flows.

Data collection is gathered from multiple sources using a variety of methods. SNMP, CLI, RADIUS, SYSLOG, API and DHCP fingerprints can all be used to achieve the detailed end-to-end visibility necessary to create a truly secure environment.



Licensing

FortiNAC Licensing

FortiNAC offers flexible deployment options based on the level of coverage and functionality desired.

- The **BASE license level** provides easy, one-step IoT security solution to close pressing endpoint security gaps by seeing all endpoint devices on the network, automating authorization, and enabling micro-segmentation and network lockdown. The BASE license level is appropriate for organizations that need to secure IoT and headless devices, and enable network lockdown with dynamic VLAN steering, but do not require more advanced user/network controls or automated threat response.
- The **PLUS license level** builds on all the functionality of BASE with enhanced visibility and more advanced Network Access Controls and automated provisioning for users, guests, and devices as well as reporting and analytics. The reporting and analytics can greatly assist in providing audit documentation of compliance. The PLUS license level is appropriate for organizations that want complete endpoint visibility and a granular control, but do not require automated threat response.
- The **PRO license level** provides the ultimate in visibility, control and response. PRO license offers real-time endpoint visibility, comprehensive access control, and automated threat response and delivers contextual information with triaged alerts. The PRO license level is appropriate for organizations that want complete endpoint visibility, a flexible NAC solution with granular controls, as well as accurate event triage and real-time automated threat response.

FortiNAC LICENSE TYPES			BASE	PLUS	PRO
Visibility	Network	Network Discovery	✓	✓	✓
		Rogue Identification	✓	✓	✓
		Device Profiling & Classification	✓	✓	✓
	Endpoint	Enhanced Visiblity	✓	✓	✓
		Anomaly Detection	✓	✓	✓
		MDM Integration	✓	✓	✓
		Persistent Agent		✓	✓
	User	Authentication		✓	✓
		Captive Portal		✓	✓
Automation / Control		Network Access Policies	✓	✓	✓
		IoT Onboarding with Sponsor	✓	✓	✓
		Rogue Device Detection & Restriction	✓	✓	✓
		Firewall Segmentation	✓	✓	✓
		MAC Address Bypass (MAB)	✓	✓	✓
		Full RADIUS (EAP)		✓	✓
		BYOD / Onboarding		✓	✓
		Guest Management		✓	✓
		Endpoint Compliance		✓	✓
		Web & Firewall Single Sign-on		✓	✓
Incident Response		Event Correlation			✓
		Extensible Actions & Audit Trail			✓
		Alert Criticality & Routing			✓
		Guided Triage Workflows			✓
Integrations		Inbound Security Events			✓
		Outbound Security Events		✓	✓
		REST API	✓	✓	✓
Reporting		Customizable Reports	✓	✓	✓

Specifications

	FNC-M-550C	FNC-CA-600C	FNC-CA-500C
System			
CPU	Intel Xeon Silver 4110 2.1 G, 8C/16T, 9.6 GT/s, 11M Cache, Turbo, HT (85W) DDR4-2400 (Qty 2)		Intel Xeon E3-1220 v5 3.0 GHz, 8M cache, 4C/4T, Turbo (Qty 1)
Memory	8 GB RDIMM, 2666 MT/s, Single Rank (Qty 4)		8 GB UDIMM, 2400 MT/s, ECC (Qty 2)
Hard Disk	1TB 7.2K RPM SATA 6 Gbps 2.5in Hot-plug Hard Drive (Qty 2)		1TB 7.2K RPM SATA 6 Gbps 3.5in Hot-plug Hard Drive RAID1 (Qty 2)
Optical Drive	None Required		DVD ROM SATA Internal (Qty 1)
BMC	iDRAC9 Express, integrated (Qty 1)		iDRAC8 Express (Qty 1)
Network Interface	Broadcom 5720 QuadPort 4x 1 GB Ethernet, RJ45		4x 10/100/1000 Ethernet, RJ45
RAID Card	PERC H330 Integrated RAID Controller (Qty 1)		PERC H330 Integrated RAID Controller (Qty 1)
RAID Configuration	RAID 1		RAID 1
Console Access	None		Front LCD Panel
Form Factor	1U Rack mountable		1U Rack mountable
Dimensions			
Height x Width x Length (inches)	1.68 x 18.9 x 29.73		1.68 x 17.08 x 24.60
Height x Width x Length (mm)	42.8 x 482.4 x 755.12		42.8 x 434.0 x 625.0
Weight	43.056 lbs (19.76 kg)		43.87 lbs (19.9 kg)
Environment			
Power Supply	Dual 550W Hot Plug Power Supply		Dual 350W Hot Plug Power Supplies
Input Power	100-240V AC Autoranging		100-240V AC Autoranging
Input Current	6.25 A		3.0 A
Cooling	7 fans		4 fans
Panel Display	No LCD		20 Char LCD
Heat Dissipation	2559 BTU/hr		1357.1 BTU/hr
Operation Temperature Range	50–95°F (10–35°C)		50–95°F (10–35°C)
Storage Temperature Range	-40–149°F (-40–65°C)		-40–149°F (-40–65°C)
Humidity (Operating) Humidity (Non-operating)	10–80% non-condensing 5–95% non-condensing		10–80% non-condensing 5–95% non-condensing
Certification			
Safety	Certified as applicable by Product Safety authorities worldwide, including United States (NRTL), Canada (SCC), European Union (CE).		
Electromagnetic (EMC)	Certified as applicable by EMC authorities worldwide, including United States (FCC), Canada (ICES), European Union (CE).		
Materials	Certified as applicable by Materials authorities worldwide, including European Union (ROHS) and China (ROHS).		

Specifications

	FNC-CA-700C
System	
CPU	Intel Xeon Gold 6132 2.6 G, 14C/28T, 10.4 GT/s, 19M Cache, Turbo, HT (140W) DDR4-2666 (Qty 2)
Memory	8 GB RDIMM, 2666 MT/s, Single Rank (Qty 12)
Hard Disk	600 GB 15K RPM SAS 12 Gbps 2.5in Hot-plug Hard Drive (Qty 2)
Optical Drive	None required
BMC	iDRAC9 Express, integrated (Qty 1)
Network Interface	Broadcom 5720 QuadPort 4x 1 GB Ethernet, RJ45 (Qty 1)
RAID Card	PERC H730P+ RAID Controller, 2 GB Cache (Qty 1)
RAID Configuration	RAID 1
Console Access	No LCD Panel
Form Factor	1U Rack mountable
Dimensions	
Height x Width x Length (inches)	1.68 x 18.9 x 29.73
Height x Width x Length (mm)	42.8 x 482.4 x 755.12
Weight	43.056 lbs (19.76 kg)
Environment	
Power Supply	Dual 750W AC power supplies
Input Power	100–240V AC, Autoranging
Input Current	6.25 A
Cooling	7 fans
Panel Display	No LCD
Heat Dissipation	2559 BTU/hr
Operation Temperature Range	50–95°F (10–35°C)
Storage Temperature Range	-40–149°F (-40–65°C)
Humidity (Operating) Humidity (Non-operating)	10–80% non-condensing 5–95% non-condensing
Certification	
Safety	Certified as applicable by Product Safety authorities worldwide, including United States (NRTL), Canada (SCC), European Union (CE).
Electromagnetic (EMC)	Certified as applicable by EMC authorities worldwide, including United States (FCC), Canada (ICES), European Union (CE).
Materials	Certified as applicable by Materials authorities worldwide, including European Union (ROHS) and China (ROHS).

Hardware Server Sizing

HARDWARE			
Hardware Server	**Type**	**Target Environment**	**Capacity**
FortiNAC-CA-500C	Standalone Appliance (Integrated Control Server and Application Server)	Small Environments	Manages up to 2,000 ports in the network*
FortiNAC-CA-600C	High Performance Control and Application Server	Medium Environments	Manages up to 15,000 ports in the network*
FortiNAC-CA-700C	Ultra High Performance Control and Application Server	Large Environments with few Persistent Agents	Manages up to 25,000 ports in the network*
FortiNAC-M-550C	Management Appliance (Provides centralized management when multiple appliances are deployed)	Multi-site environments with multiple appliances	Unlimited

* "Ports" in the network = total number of switch ports + maximum number of concurrent wireless connections. FortiNAC sizes the appliance capacity based on total port counts not total number of devices.

VM Server Resource Sizing

Network Size	Target Environment	SKU	vCPU**	Memory	Disk
Up to 2,000 ports in the network*	Small Environment	FNC-CA-VM	4	16 GB	100 GB
Up to 15,000 ports in the network*	Medium Environment	FNC-CA-VM	6	32 GB	100 GB
Up to 25,000 ports in the network*	Large Environment	FNC-CA-VM	14	96 GB	100 GB
Unlimited	Large Environment	FNC-M-VM	4	12 GB	100 GB

* "Ports" in the network = total number of switch ports + maximum number of concurrent wireless connections. FortiNAC sizes the appliance capacity based on total port counts not total number of devices.
** The values in the vCPU column are only guidelines. Individual environments may vary.

Order Information

Appliances	SKU	Description
FortiNAC-CA-500C	FNC-CA-500C	FortiNAC 500, Network Control and Application Server with RAID and Redundant Power Supplies
FortiNAC-CA-600C	FNC-CA-600C	FortiNAC 600, High Performance Network Control and Application Server with RAID and Redundant Power Supplies
FortiNAC-CA-700C	FNC-CA-700C	FortiNAC 700, Ultra High Performance Network Control and Application Server with RAID and Redundant Power Supplies
FortiNAC-M-550C	FNC-M-550C	FortiNAC Manager 550, Network Manager with RAID and Redundant Power Supplies
Virtual Machines	**SKU**	**Description**
FortiNAC Control and Application VM	FNC-CA-VM	FortiNAC Control and Application VM Server (VMware or Hyper-V or AWS or Azure or KVM)
FortiNAC Manager VM	FNC-M-VM	FortiNAC Manager VM Server (VMware or Hyper-V or AWS or Azure or KVM)
LICENSES		
Perpetual License	**SKU**	**Description**
FortiNAC BASE License 100	LIC-FNAC-BASE-100	FortiNAC BASE License for 100 concurrent endpoint devices. The BASE license provides Endpoint Visibility and Dynamic VLAN Steering.
FortiNAC BASE License 1K	LIC-FNAC-BASE-1K	FortiNAC BASE License for 1K concurrent endpoint devices. The BASE license provides Endpoint Visibility and Dynamic VLAN Steering.
FortiNAC BASE License 10K	LIC-FNAC-BASE-10K	FortiNAC BASE License for 10K concurrent endpoint devices. The BASE license provides Endpoint Visibility and Dynamic VLAN Steering.
FortiNAC BASE License 50K	LIC-FNAC-BASE-50K	FortiNAC BASE License for 50K concurrent endpoint devices. The BASE license provides Endpoint Visibility and Dynamic VLAN Steering.
FortiNAC PLUS License 100	LIC-FNAC-PLUS-100	FortiNAC PLUS License for 100 concurrent endpoint devices. All the functionality of BASE with more advanced Network Access Controls and automated provisioning for users, guests, and devices.
FortiNAC PLUS License 1K	LIC-FNAC-PLUS-1K	FortiNAC PLUS License for 1K concurrent endpoint devices. All the functionality of BASE with more advanced Network Access Controls and automated provisioning for users, guests, and devices.
FortiNAC PLUS License 10K	LIC-FNAC-PLUS-10K	FortiNAC PLUS License for 10K concurrent endpoint devices. All the functionality of BASE with more advanced Network Access Controls and automated provisioning for users, guests, and devices.
FortiNAC PLUS License 50K	LIC-FNAC-PLUS-50K	FortiNAC PLUS License for 50K concurrent endpoint devices. All the functionality of BASE with more advanced Network Access Controls and automated provisioning for users, guests, and devices.
FortiNAC PRO License 100	LIC-FNAC-PRO-100	FortiNAC PRO License for 100 concurrent endpoint devices. PRO license level provides the ultimate in visibility, control and response.
FortiNAC PRO License 1K	LIC-FNAC-PRO-1K	FortiNAC PRO License for 1K concurrent endpoint devices. PRO license level provides the ultimate in visibility, control and response.
FortiNAC PRO License 10K	LIC-FNAC-PRO-10K	FortiNAC PRO License for 10K concurrent endpoint devices. PRO license level provides the ultimate in visibility, control and response.
FortiNAC PRO License 50K	LIC-FNAC-PRO-50K	FortiNAC PRO License for 50K concurrent endpoint devices. PRO license level provides the ultimate in visibility, control and response.
Upgrade License	**SKU**	**Description**
BASE to PLUS License Upgrade	FNC-LIC-BASE-UPG-100	BASE to PLUS License Upgrade for 100 concurrent endpoint device.
BASE to PRO License Upgrade	FNC-LIC-PRO-UPG-100	BASE to PRO License Upgrade for 100 concurrent endpoint devices.
PLUS to PRO License Upgrade	FNC-LIC-PLUS-UPG-100	PLUS to PRO License Upgrade for 100 concurrent endpoint devices.
Subscription License	**SKU**	**Description**
FortiNAC Subscription PRO 500	FC1-10-FNAC1-209-02-DD	FortiNAC Subscription PRO License for 500 concurrent endpoints. Pro license level provides the ultimate in visibility, control, and response. (MOQ 500).
Training	**SKU**	**Description**
FortiNAC Classroom Training	FT-BNS-TR	One seat in a 3-day Administration and Operations training class. Classes are held in Concord NH and at regional locations.
FortiNAC Online Training	FT-BS-TWB	One seat in a 3-session (total 12 hours) web-based Administration and Operation overview training. Remote sessions are delivered online.

FORTINET®

www.fortinet.com