FORTINET

BrainStorm

Educational Technology Conference

"For Ed Techs, By Ed Techs"

IOT Devices & BYOD changing what is on your network -How to Gain Visibility and Protection

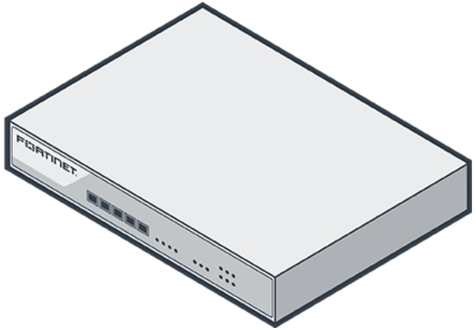
David Ryan – Regional Sales Manager
dryan@fortinet.com

Jeffrey Reed- FortiNAC Sales Engineer
jreed01@Fortinet.com

Architecture, Deployment, & Configuration

FortiNAC

Network Access Control



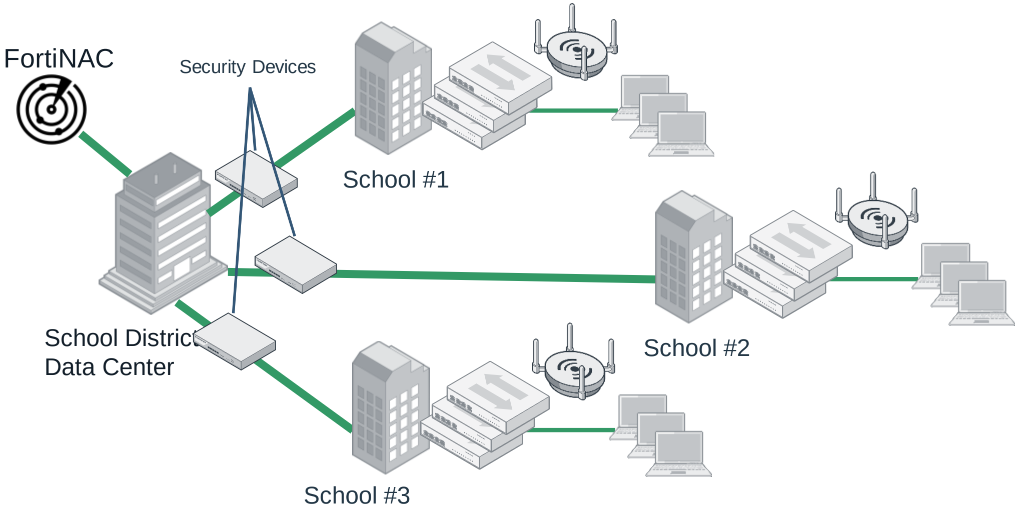
Visibility

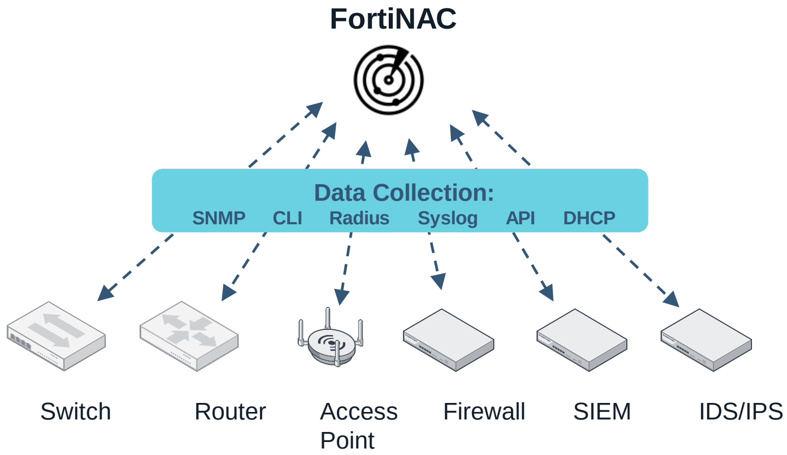
Control

Automated Response

Watching every node on the Network

Architecture and Deployment





FortiNAC Configuration

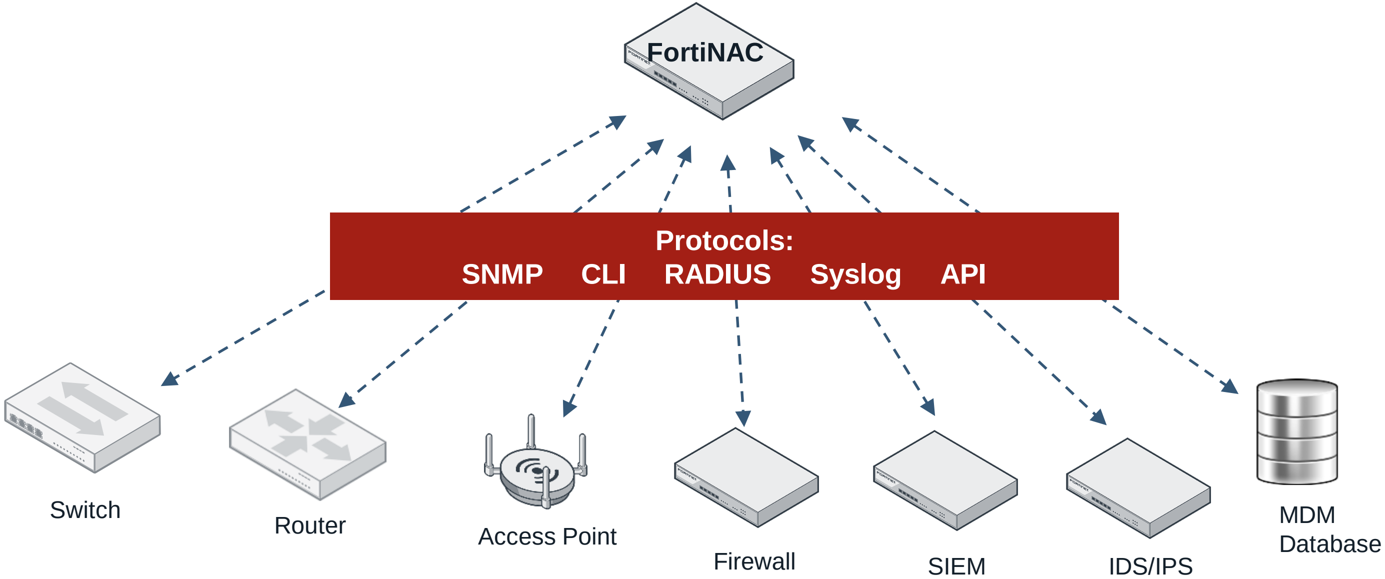
Comprehensive Network Security

Visibility

- Discover all endpoints, IoT devices, users, and applications
  - Inputs from RADIUS, CLI, SNMP, syslog, MDM, DHCP, LDAP
  - Can interact more than 2,300 network devices
- Multi-vendor wired and wireless Connectivity
  - Inputs from virtually all vendors and models
- Identify and profile every endpoint
  - Enables policy rules created by granular device type
  - Extends vulnerability and patch management to non FortiClient users
  - Leverages FortiGate for passive identification via traffic scanning
- Self-registration to simplify guest management

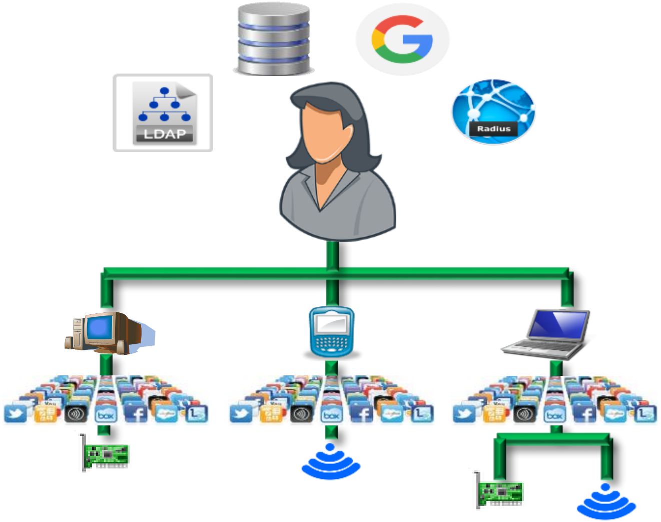
Visibility: Agentless Data Collection

Information Gathered from Multiple Sources



Providing Endpoint Visibility

- Who: User
  - Current logged on user
  - Owner: BYOD, guest, contractor
- What: Host/device
  - Network adapter
    - Physical and IP address
    - Media type
    - Vendor
  - Host name
  - Operating system
  - Applications
- Where: Location
- When: Connection times

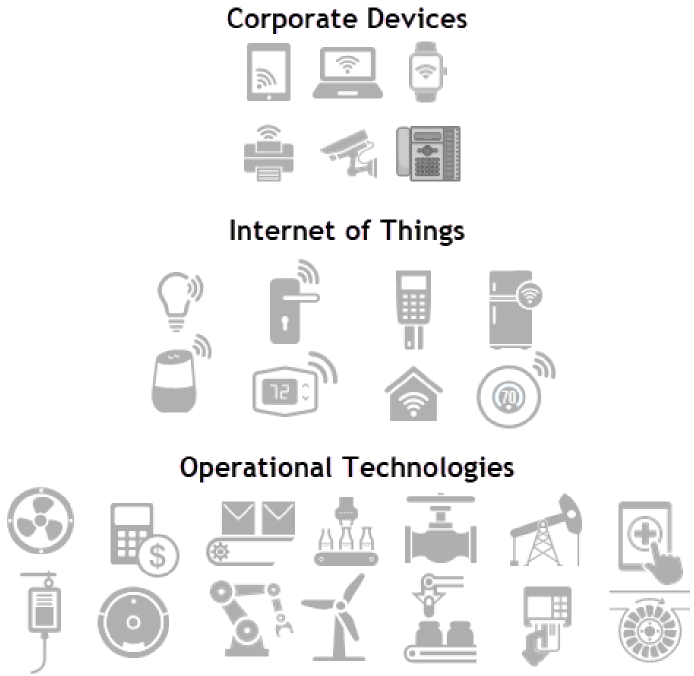


DEVICE ID

IP Address:	192.168.5.95
Physical Address:	00:1D:09:11:21:DA
Vendor Name:	Dell Inc.
Status:	Disconnected
Location:	Concord AP Secure
Connect Time:	10/23/16 07:57 AM EDT
Disconnect Time:	10/23/16 04:55 PM EDT

Enhanced Visibility

Endpoint Identification



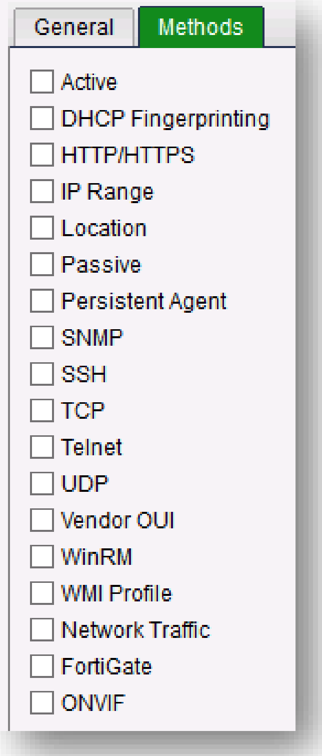
Device Classification

- Automatic or manual

  > Sponsor notification
- Device type
- Confirm on connect
- Disable if confirmation fails

18 Profiling Methods

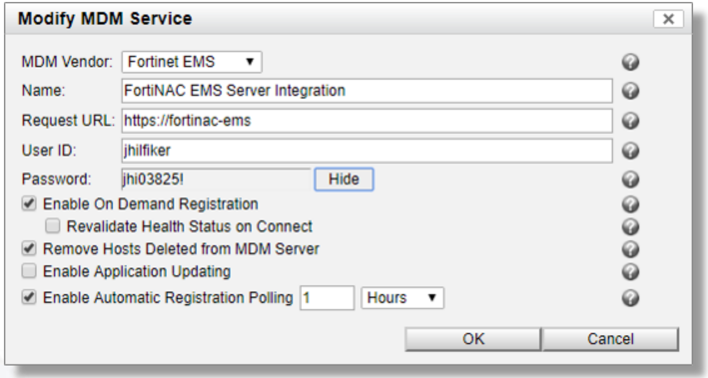
- More methods = Higher Trust



☐ Active
☐ DHCP Fingerprinting
☐ HTTP/HTTPS
☐ IP Range
☐ Location
☐ Passive
☐ Persistent Agent
☐ SNMP
☐ SSH
☐ TCP
☐ Telnet
☐ UDP
☐ Vendor OUI
☐ WinRM
☐ WMI Profile
☐ Network Traffic
☐ FortiGate
☐ ONVIF

MDM Integration

- Synchronize FortiNAC with an MDM
    - Retrieve MDM known hosts
    - Receive MDM host updates
- Mobile device and user association
- Apply security policies
- MDM host view data columns



Modify MDM Service

MDM Vendor: Fortinet EMS ▾

Name: FortiNAC EMS Server Integration

Request URL: https://fortinac-ems

User ID: jhilfiker

Password: jhi03825! Hide

☑ Enable On Demand Registration

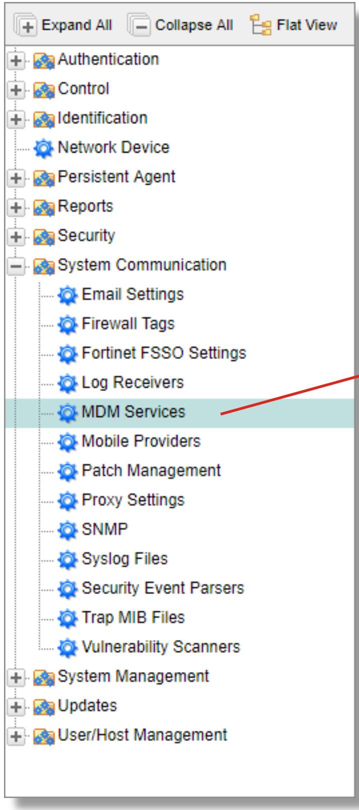
□ Revalidate Health Status on Connect

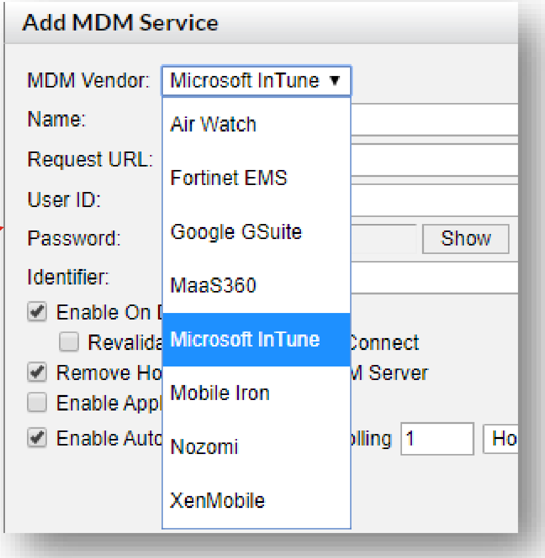
☑ Remove Hosts Deleted from MDM Server

□ Enable Application Updating

☑ Enable Automatic Registration Polling 1 Hours ▾

OK Cancel





Add MDM Service

MDM Vendor: Microsoft InTune ▾

Name:

Request URL:

User ID:

Password: Show

Identifier:

☑ Enable On I

□ Revalida Connect

☑ Remove Ho M Server

□ Enable Appl

☑ Enable Auto lling 1 Ho

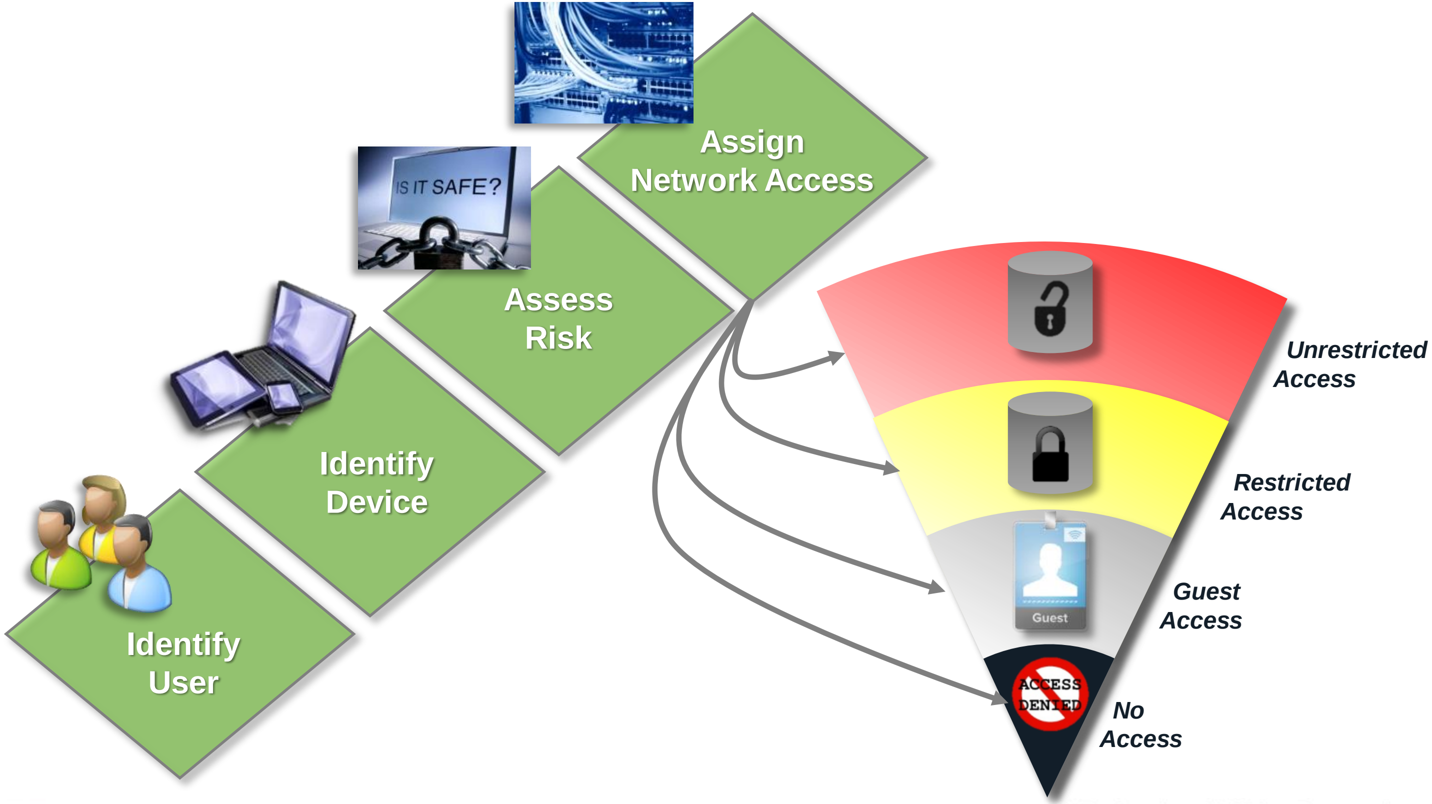
FortiNAC

Comprehensive Network Security

Control

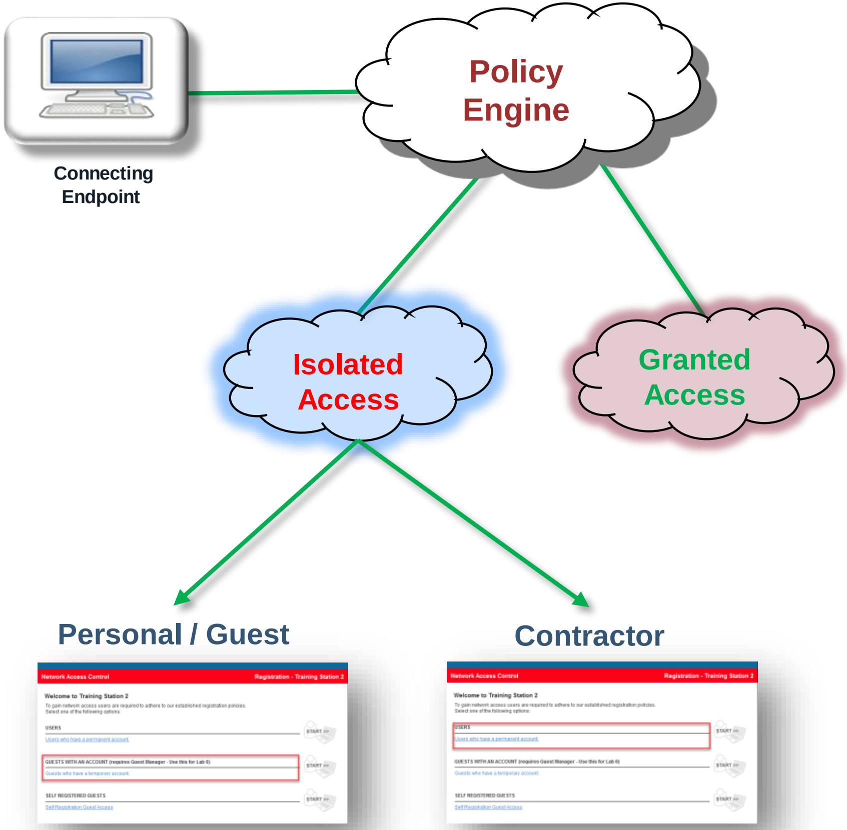
- Automated authentication and authorization
  - Detailed user and device profiles enable automated entry to network
  - Evaluate role, location, time of day, and device metrics for decisions
- Dynamic network access control
  - Adjust device access to assets based on changes in activity or profile
- Enable network micro-segmentation
  - Granular device identification enables thinly sliced networks
  - Devices have limited access to prevent east-west infection

Control: Dynamic Network Access



Pre-Connect Host Evaluation and Onboarding

- Device isolation
  - Unknown devices can be isolated
  - Devices that fail posture evaluation can be isolated
  - Devices that are administratively denied access can be isolated
- Onboarding
  - User authentication
  - Posture evaluation
  - Customized portal



Network Access Control Registration - Training Station 2

Welcome to Training Station 2

To gain network access users are required to adhere to our established registration policies.
Select one of the following options:

USERS

Users who have a permanent account.

START >>

GUESTS WITH AN ACCOUNT (requires Guest Manager - Use this for Lab 6)

Guests who have a temporary account.

START >>

SELF REGISTERED GUESTS

Self Registration Guest Access

START >>

Network Access Control Registration - Training Station 2

Welcome to Training Station 2

To gain network access users are required to adhere to our established registration policies.
Select one of the following options:

USERS

Users who have a permanent account.

START >>

GUESTS WITH AN ACCOUNT (requires Guest Manager - Use this for Lab 6)

Guests who have a temporary account.

START >>

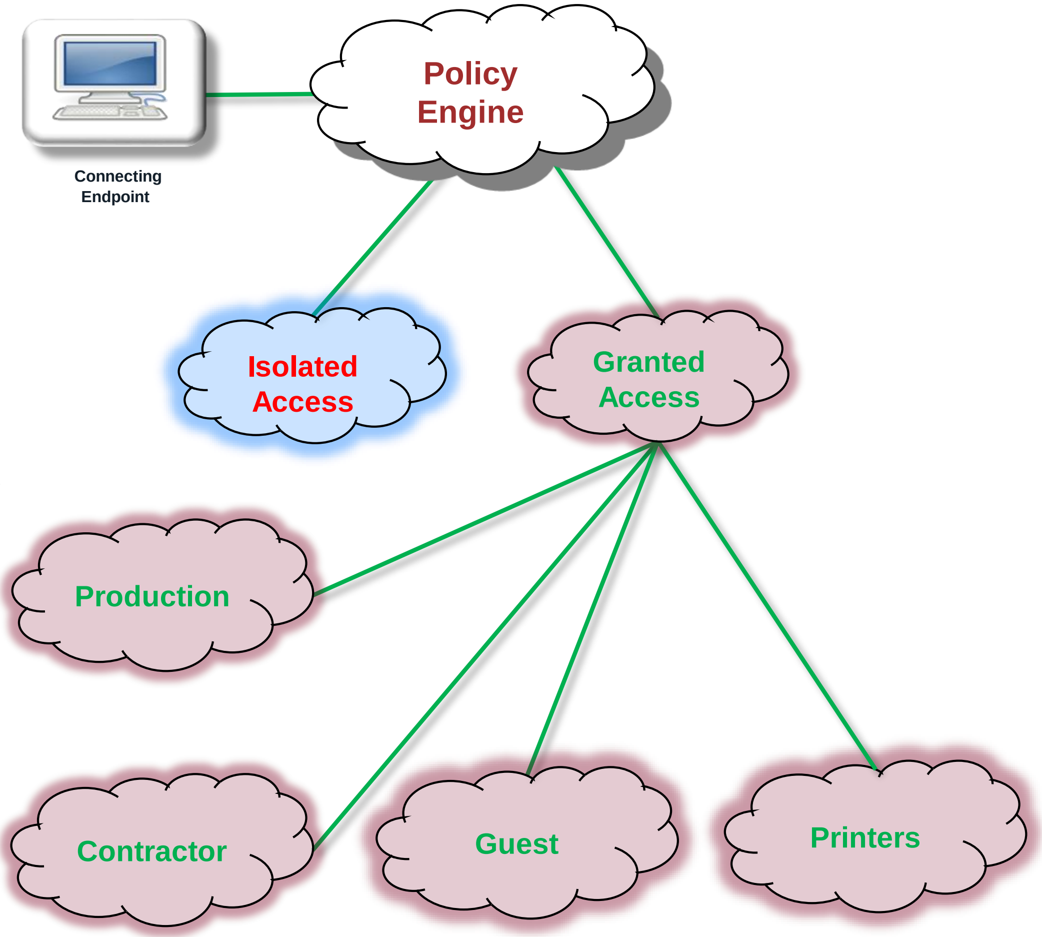
SELF REGISTERED GUESTS

Self Registration Guest Access

START >>

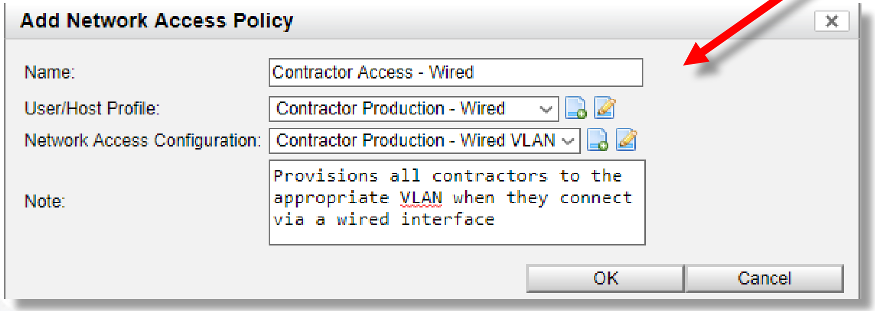
Post Connect Control

- The FortiNAC policy engine continuously evaluates endpoints
- Security policies can:
  - Use who, what, where, and when information to dynamically provision the appropriate access
  - Validate endpoint security posture and isolate if necessary



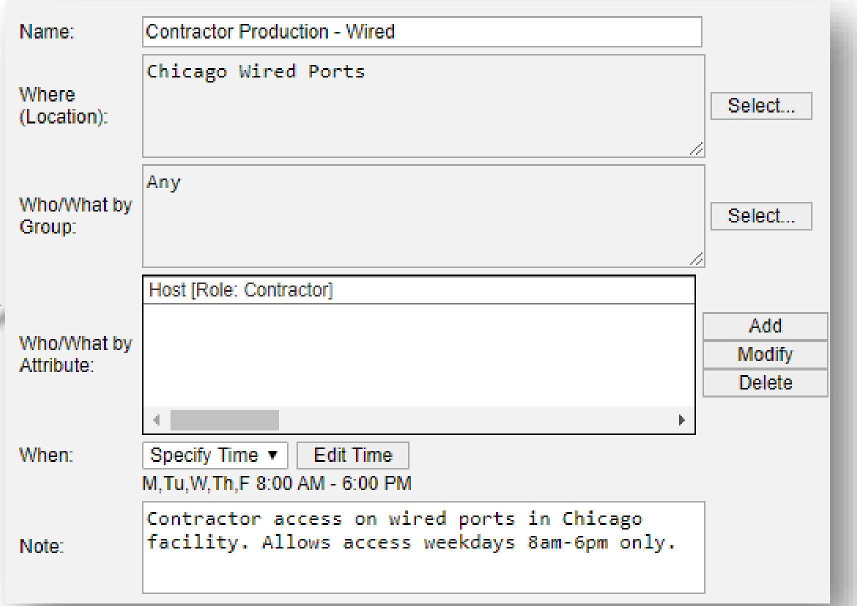
Profiles

- Connected and connecting hosts are continuously evaluated against user/host profiles keying on:
  - Where
  - Who
  - What
  - When
- User/host profiles are components of security policies



Add Network Access Policy

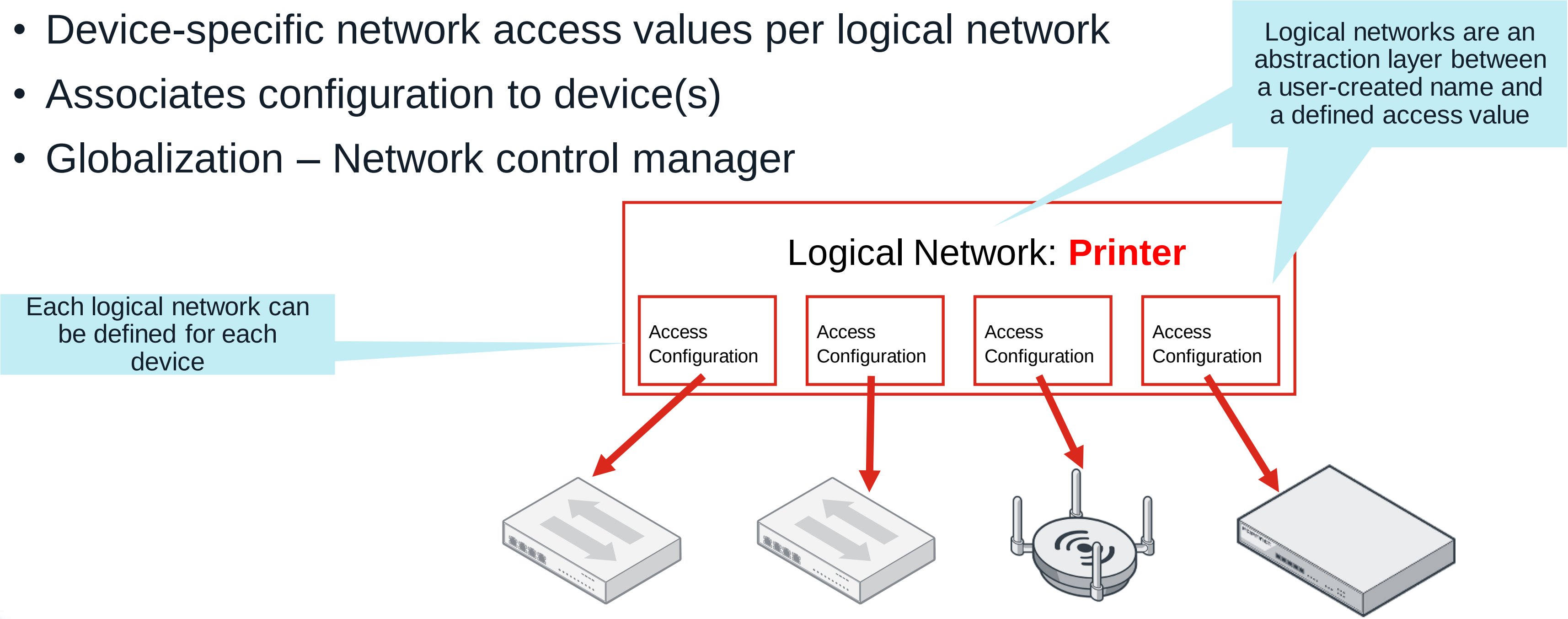
Name:	Contractor Access - Wired
User/Host Profile:	Contractor Production - Wired
Network Access Configuration:	Contractor Production - Wired VLAN
Note:	Provisions all contractors to the appropriate VLAN when they connect via a wired interface



Name:	Contractor Production - Wired
Where (Location):	Chicago Wired Ports
Who/What by Group:	Any
Who/What by Attribute:	Host [Role: Contractor]
When:	Specify Time M,Tu,W,Th,F 8:00 AM - 6:00 PM
Note:	Contractor access on wired ports in Chicago facility. Allows access weekdays 8am-6pm only.

Logical Networks

- Logical network segmentation for access policies
- Centralized device configurations
- Device-specific network access values per logical network
- Associates configuration to device(s)
- Globalization – Network control manager


Logical networks are an abstraction layer between a user-created name and a defined access value
Logical Network: Printer
Access Configuration
Access Configuration
Access Configuration
Access Configuration
Each logical network can be defined for each device

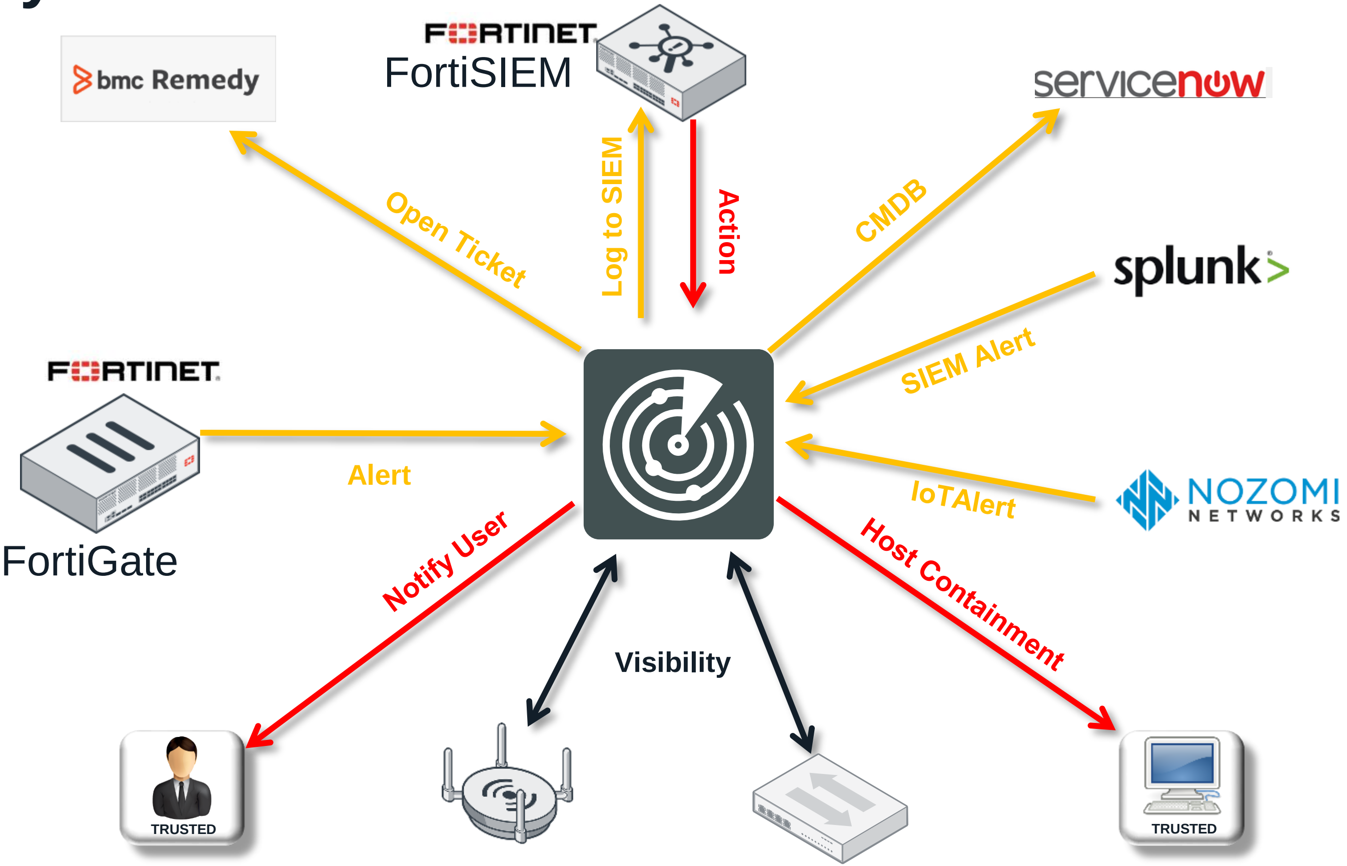
FortiNAC

Comprehensive Network Security

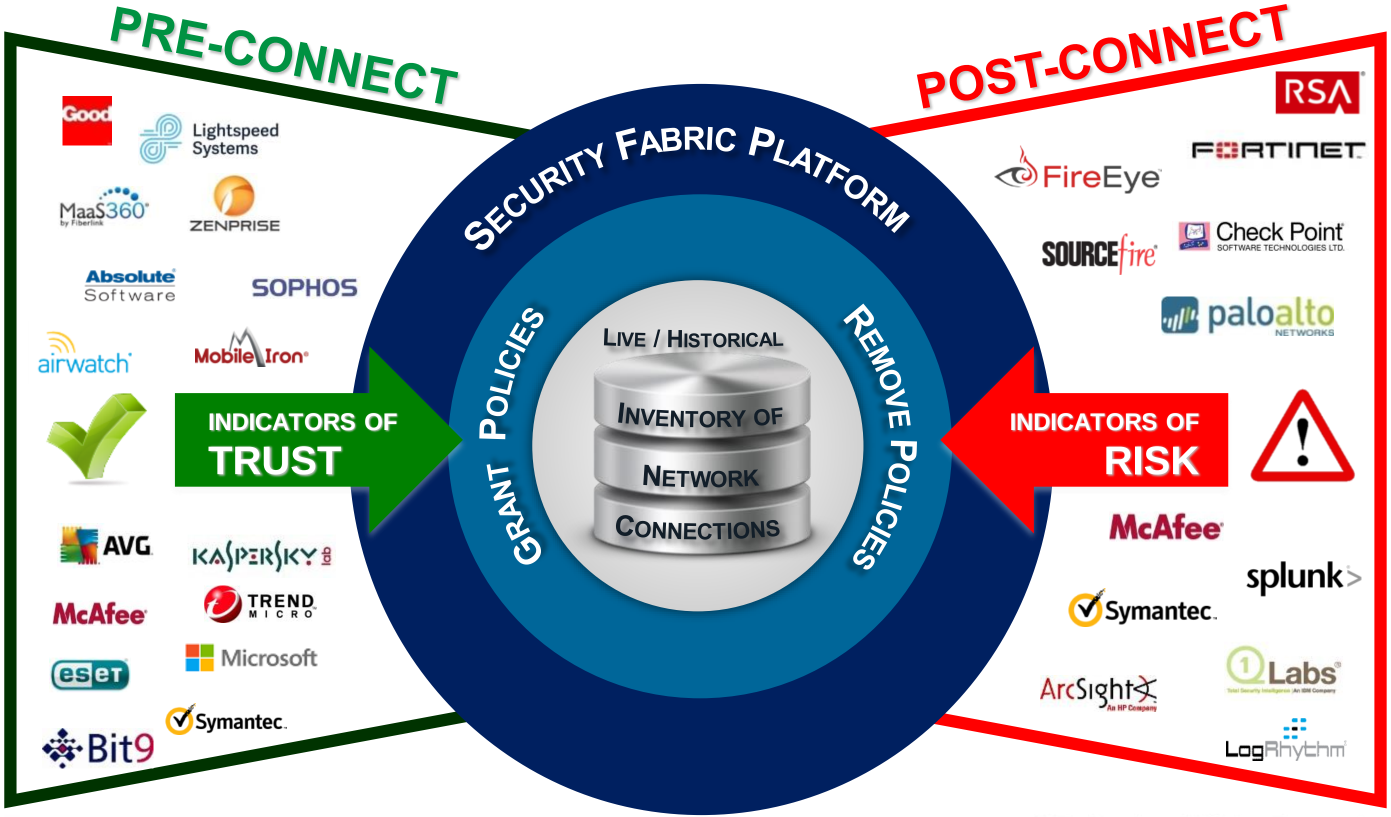
Automated Response

- Bridge the SOC and NOC
  - Security events move from detection to remediation immediately
- Rapid security event triage
  - Automated rules can respond in seconds to bad behavior
  - Anomaly detection of behavioral changes in communication patterns
- Accelerate threat investigations
  - Device history compiled from multiple sources is instantly available
- Granular containment options
  - For example, quarantine or internet-only connectivity

Security Automation and Orchestration



Advance Policies with Trust/Risk Indicators



Alert and Contextual Information

Security Alert

Field	Value
Vendor	Fortinet
Type	Threat
Sub Type	Virus
Threat ID	32423
Description	HTTP non RFC-compliant response found
Severity	Critical
IP Address	192.168.102.53

+

Host Information

TRUSTED

Field	Value
Host Name	Johns PC
Operating System	Windows 10
Adapter Physical Address	00:01:02:04:04:05
IP Address	192.168.102.53
Location	Switch-2 Port 8
IP Address	192.168.1.100

+

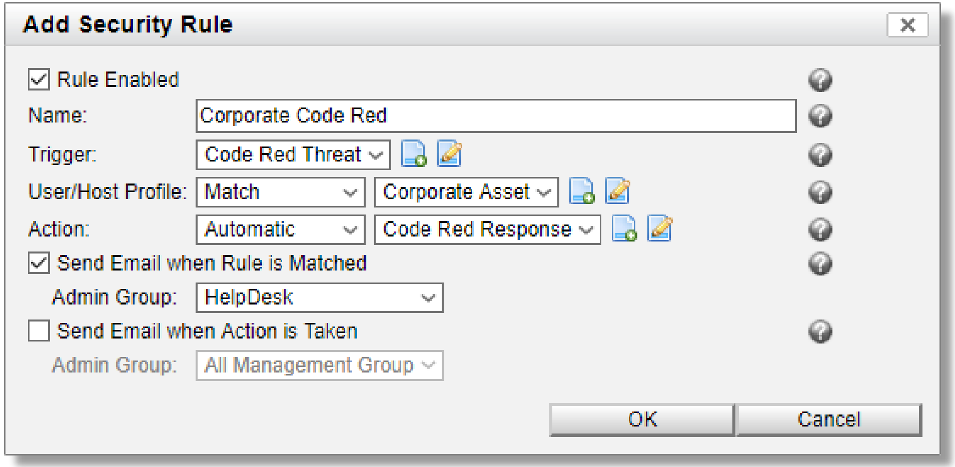
User Information

TRUSTED

Field	Value
First Name	John
Last Name	Doe
Role	Contractor
Email	jdoe@example.com
Phone	603 717-XXXX
Role	Engineering Contractor

Security Rules

- Ranked security rules process incoming security alerts
- User and end station information is correlated with the security event information
- Workflows including notification and containment actions can be automated



Add Security Rule

☑ Rule Enabled

Name: Corporate Code Red

Trigger: Code Red Threat

User/Host Profile: Match | Corporate Asset

Action: Automatic | Code Red Response

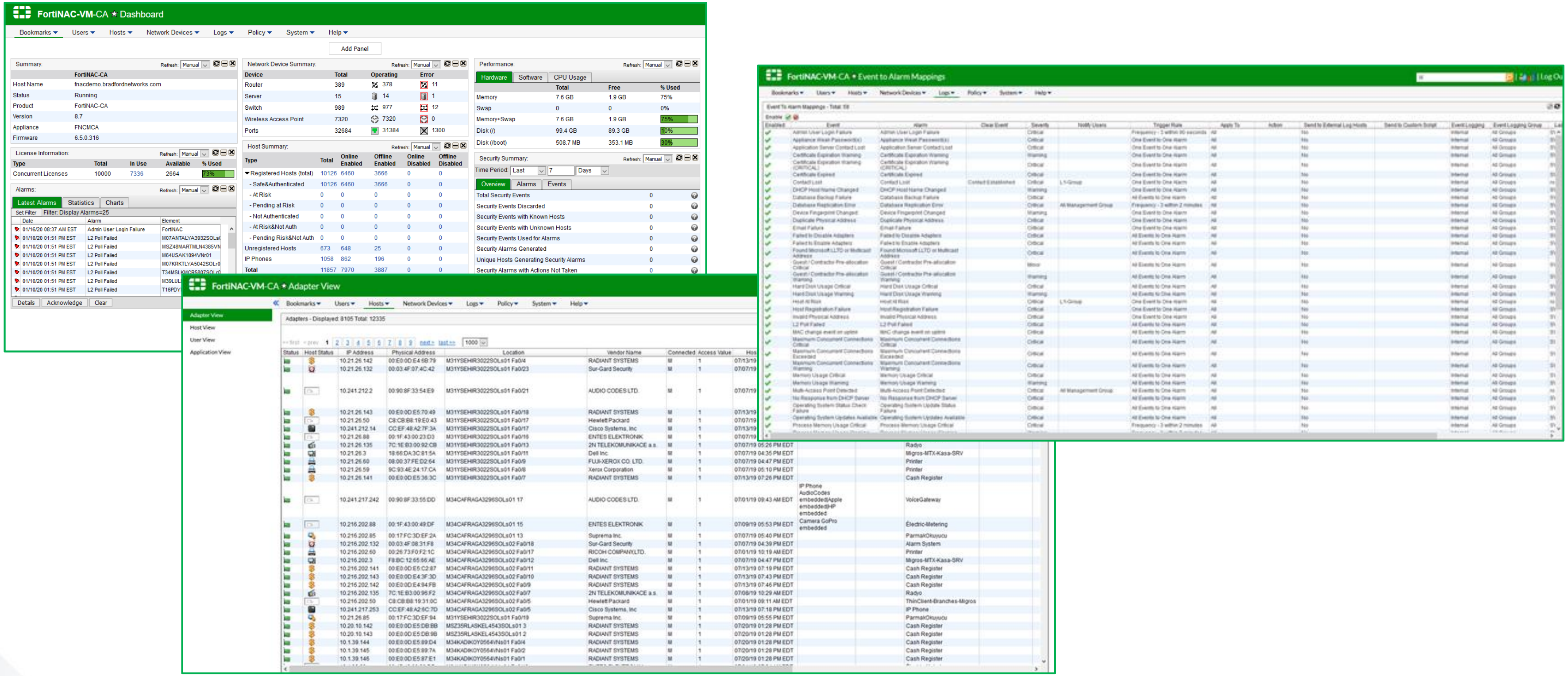
☑ Send Email when Rule is Matched

Admin Group: HelpDesk

□ Send Email when Action is Taken

Admin Group: All Management Group

Management, Reporting, & Incident handling



FortiNAC-VM-CA ★ Dashboard
Bookmarks ▾ Users ▾ Hosts ▾ Network Devices ▾ Logs ▾ Policy ▾ System ▾ Help ▾
Add Panel

Summary: Refresh: Manual

	FortiNAC-CA
Host Name	fnacdemo.bradfordnetworks.com
Status	Running
Product	FortiNAC-CA
Version	8.7
Appliance	FNCMCA
Firmware	6.5.0.316

License Information: Refresh: Manual

Type	Total	In Use	Available	% Used
Concurrent Licenses	10000	7336	2664	73%

Alarms: Refresh: Manual

Latest Alarms Statistics Charts
Set Filter

Filter: Display Alarms=25

Date	Alarm	Element
01/16/20 08:37 AM EST	Admin User Login Failure	FortiNAC
01/10/20 01:51 PM EST	L2 Poll Failed	M07ANTALYA3932SOLs(
01/10/20 01:51 PM EST	L2 Poll Failed	MSZ48MARTMLN4385VN
01/10/20 01:51 PM EST	L2 Poll Failed	M64USAK1094VNr01
01/10/20 01:51 PM EST	L2 Poll Failed	M07KRKTLYA5042SOLr0
01/10/20 01:51 PM EST	L2 Poll Failed	T34MSLKMCR5807SOLr0
01/10/20 01:51 PM EST	L2 Poll Failed	M39LUL
01/10/20 01:51 PM EST	L2 Poll Failed	T16PDY

Network Device Summary: Refresh: Manual

Device	Total	Operating	Error
Router	389	378	11
Server	15	14	1
Switch	989	977	12
Wireless Access Point	7320	7320	0
Ports	32684	31384	1300

Host Summary: Refresh: Manual

Type	Total	Online Enabled	Offline Enabled	Online Disabled	Offline Disabled
▾Registered Hosts (total)	10126	6460	3666	0	0
- Safe&Authenticated	10126	6460	3666	0	0
- At Risk	0	0	0	0	0
- Pending at Risk	0	0	0	0	0
- Not Authenticated	0	0	0	0	0
- At Risk&Not Auth	0	0	0	0	0
- Pending Risk&Not Auth	0	0	0	0	0
Unregistered Hosts	673	648	25	0	0
IP Phones	1058	862	196	0	0
Total	11857	7970	3887	0	0

Performance: Refresh: Manual

	Total	Free	% Used
Memory	7.6 GB	1.9 GB	75%
Swap	0	0	0%
Memory+Swap	7.6 GB	1.9 GB	75%
Disk (/)	99.4 GB	89.3 GB	10%
Disk (/boot)	508.7 MB	353.1 MB	30%

Security Summary: Refresh: Manual

Time Period: Last 7 Days

Total Security Events	0
Security Events Discarded	0
Security Events with Known Hosts	0
Security Events with Unknown Hosts	0
Security Events Used for Alarms	0
Security Alarms Generated	0
Unique Hosts Generating Security Alarms	0
Security Alarms with Actions Not Taken	0

FortiNAC-VM-CA ★ Adapter View
Bookmarks ▾ Users ▾ Hosts ▾ Network Devices ▾ Logs ▾ Policy ▾ System ▾ Help ▾
Adapter View
Host View
User View
Application View
<< first < prev 1 2 3 4 5 6 7 8 9 next > last >>
1000

Adapters - Displayed: 8105 Total: 12335

Status	Host Status	IP Address	Physical Address	Location	Vendor Name	Connected	Access Value	Hos			
		10.21.26.142	00:E0:0D:E4:6B:79	M31YSEHIR3022SOLs01 Fa0/4	RADIANT SYSTEMS	M	1	07/13/19			
		10.21.26.132	00:03:4F:07:4C:42	M31YSEHIR3022SOLs01 Fa0/23	Sur-Gard Security	M	1	07/07/19			
		10.241.212.2	00:90:8F:33:54:E9	M31YSEHIR3022SOLs01 Fa0/21	AUDIO CODES LTD.	M	1	07/07/19			
		10.21.26.143	00:E0:0D:E5:70:49	M31YSEHIR3022SOLs01 Fa0/18	RADIANT SYSTEMS	M	1	07/13/19			
		10.21.26.50	C8:CB:B8:19:E0:43	M31YSEHIR3022SOLs01 Fa0/17	Hewlett Packard	M	1	07/07/19			
		10.241.212.14	CC:EF:48:A2:7F:3A	M31YSEHIR3022SOLs01 Fa0/17	Cisco Systems, Inc	M	1	07/13/19			
		10.21.26.88	00:1F:43:00:23:D3	M31YSEHIR3022SOLs01 Fa0/16	ENTES ELEKTRONIK	M	1	07/07/19			
		10.21.26.135	7C:1E:B3:00:92:CB	M31YSEHIR3022SOLs01 Fa0/13	2N TELEKOMUNIKACE a.s.	M	1	07/07/19 05:26 PM EDT			Radyo
		10.21.26.3	18:66:DA:3C:81:5A	M31YSEHIR3022SOLs01 Fa0/11	Dell Inc.	M	1	07/07/19 04:35 PM EDT			Migros-MTX-Kasa-SRV
		10.21.26.60	08:00:37:FE:D2:64	M31YSEHIR3022SOLs01 Fa0/9	FUJI-XEROX CO. LTD.	M	1	07/07/19 04:47 PM EDT			Printer
		10.21.26.59	9C:93:4E:24:17:CA	M31YSEHIR3022SOLs01 Fa0/8	Xerox Corporation	M	1	07/07/19 05:10 PM EDT			Printer
		10.21.26.141	00:E0:0D:E5:36:3C	M31YSEHIR3022SOLs01 Fa0/7	RADIANT SYSTEMS	M	1	07/13/19 07:26 PM EDT			Cash Register
		10.241.217.242	00:90:8F:33:55:DD	M34CAFRAGA3296SOLs01 17	AUDIO CODES LTD.	M	1	07/01/19 09:43 AM EDT	IP Phone AudioCodes embedded|Apple embedded|HP embedded		VoiceGateway
		10.216.202.88	00:1F:43:00:49:DF	M34CAFRAGA3296SOLs01 15	ENTES ELEKTRONIK	M	1	07/09/19 05:53 PM EDT	Camera GoPro embedded		Electric-Metering
		10.216.202.85	00:17:FC:3D:EF:2A	M34CAFRAGA3296SOLs01 13	Suprema Inc.	M	1	07/07/19 05:40 PM EDT			ParmakOkuyucu
		10.216.202.132	00:03:4F:08:31:F8	M34CAFRAGA3296SOLs02 Fa0/18	Sur-Gard Security	M	1	07/07/19 04:39 PM EDT			Alarm System
		10.216.202.60	00:26:73:F0:F2:1C	M34CAFRAGA3296SOLs02 Fa0/17	RICOH COMPANY,LTD.	M	1	07/01/19 10:19 AM EDT			Printer
		10.216.202.3	F8:BC:12:65:66:AE	M34CAFRAGA3296SOLs02 Fa0/12	Dell Inc.	M	1	07/07/19 04:47 PM EDT			Migros-MTX-Kasa-SRV
		10.216.202.141	00:E0:0D:E5:C2:87	M34CAFRAGA3296SOLs02 Fa0/11	RADIANT SYSTEMS	M	1	07/13/19 07:19 PM EDT			Cash Register
		10.216.202.143	00:E0:0D:E4:3F:3D	M34CAFRAGA3296SOLs02 Fa0/10	RADIANT SYSTEMS	M	1	07/13/19 07:43 PM EDT			Cash Register
		10.216.202.142	00:E0:0D:E4:94:FB	M34CAFRAGA3296SOLs02 Fa0/9	RADIANT SYSTEMS	M	1	07/13/19 07:46 PM EDT			Cash Register
		10.216.202.135	7C:1E:B3:00:96:F2	M34CAFRAGA3296SOLs02 Fa0/7	2N TELEKOMUNIKACE a.s.	M	1	07/08/19 10:29 AM EDT			Radyo
		10.216.202.50	C8:CB:B8:19:31:0C	M34CAFRAGA3296SOLs02 Fa0/5	Hewlett Packard	M	1	07/01/19 09:11 AM EDT			ThinClient-Branches-Migros
		10.241.217.253	CC:EF:48:A2:6C:7D	M34CAFRAGA3296SOLs02 Fa0/5	Cisco Systems, Inc	M	1	07/13/19 07:18 PM EDT			IP Phone
		10.21.26.85	00:17:FC:3D:EF:94	M31YSEHIR3022SOLs01 Fa0/19	Suprema Inc.	M	1	07/09/19 05:55 PM EDT			ParmakOkuyucu
		10.20.10.142	00:E0:0D:E5:DB:BB	MSZ35RLASKEL4543SOLs01 3	RADIANT SYSTEMS	M	1	07/20/19 01:28 PM EDT			Cash Register
		10.20.10.143	00:E0:0D:E5:DB:9B	MSZ35RLASKEL4543SOLs01 2	RADIANT SYSTEMS	M	1	07/20/19 01:28 PM EDT			Cash Register
		10.1.39.144	00:E0:0D:E5:89:D4	M34KADIKOY0564VNs01 Fa0/4	RADIANT SYSTEMS	M	1	07/20/19 01:28 PM EDT			Cash Register
		10.1.39.145	00:E0:0D:E5:89:7A	M34KADIKOY0564VNs01 Fa0/2	RADIANT SYSTEMS	M	1	07/20/19 01:28 PM EDT			Cash Register
		10.1.39.146	00:E0:0D:E5:87:E1	M34KADIKOY0564VNs01 Fa0/1	RADIANT SYSTEMS	M	1	07/20/19 01:28 PM EDT			Cash Register

FortiNAC-VM-CA ★ Event to Alarm Mappings
Log Ou
Bookmarks ▾ Users ▾ Hosts ▾ Network Devices ▾ Logs ▾ Policy ▾ System ▾ Help ▾

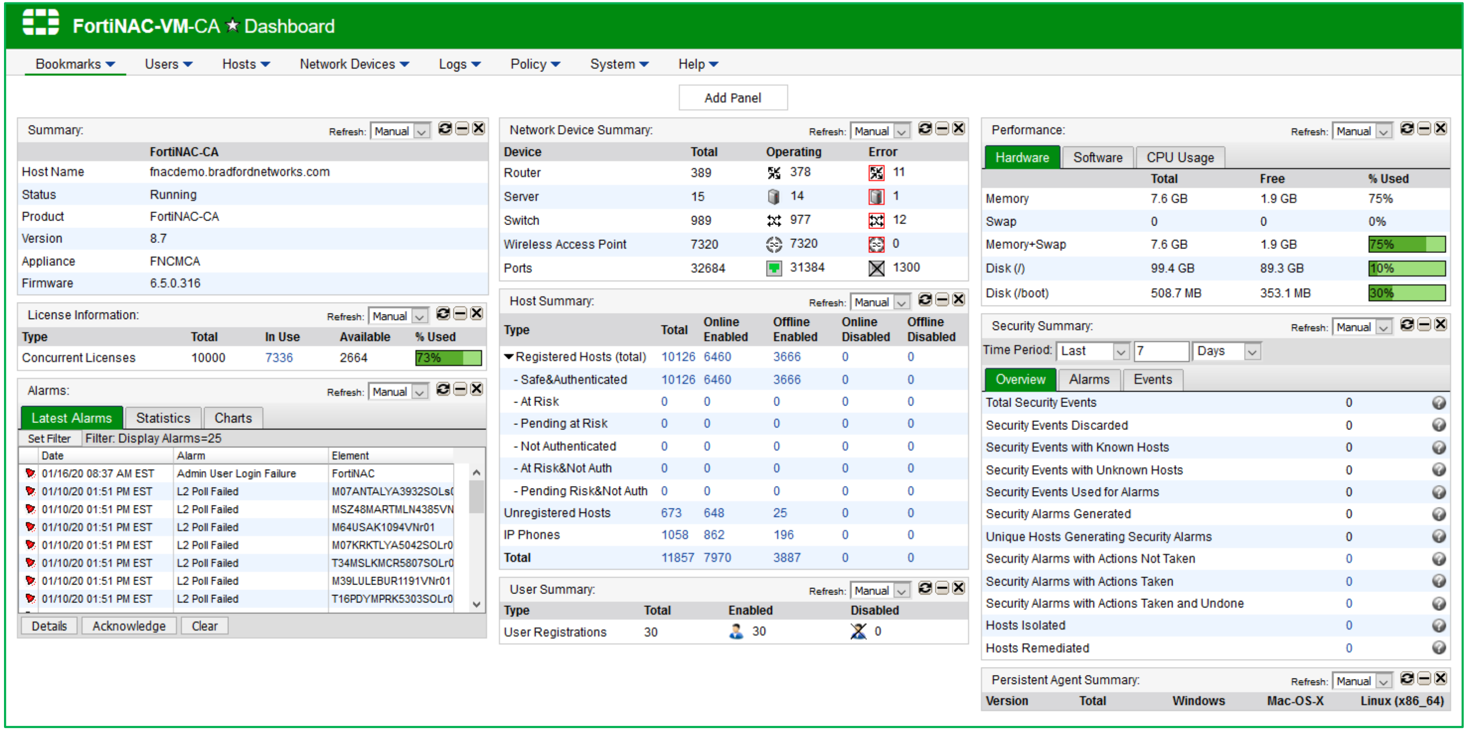
Event To Alarm Mappings - Total: 58

Enable ✓

Enabled	Event	Alarm	Clear Event	Severity	Notify Users	Trigger Rule	Apply To	Action	Send to External Log Hosts	Send to Custom Script	Event Logging	Event Logging Group
✓	Admin User Login Failure	Admin User Login Failure		Critical		Frequency - 3 within 90 seconds	All		No		Internal	All Groups
✓	Appliance Weak Password(s)	Appliance Weak Password(s)		Critical		One Event to One Alarm	All		No		Internal	All Groups
✓	Application Server Contact Lost	Application Server Contact Lost		Critical		One Event to One Alarm	All		No		Internal	All Groups
✓	Certificate Expiration Warning	Certificate Expiration Warning		Warning		One Event to One Alarm	All		No		Internal	All Groups
✓	Certificate Expiration Warning (CRITICAL)	Certificate Expiration Warning (CRITICAL)		Critical		One Event to One Alarm	All		No		Internal	All Groups
✓	Certificate Expired	Certificate Expired		Critical		One Event to One Alarm	All		No		Internal	All Groups
✓	Contact Lost	Contact Lost	Contact Established	Critical	L1-Group	One Event to One Alarm	All		No		Internal	All Groups
✓	DHCP Host Name Changed	DHCP Host Name Changed		Warning		One Event to One Alarm	All		No		Internal	All Groups
✓	Database Backup Failure	Database Backup Failure		Critical		All Events to One Alarm	All		No		Internal	All Groups
✓	Database Replication Error	Database Replication Error		Critical	All Management Group	Frequency - 3 within 2 minutes	All		No		Internal	All Groups
✓	Device Fingerprint Changed	Device Fingerprint Changed		Warning		One Event to One Alarm	All		No		Internal	All Groups
✓	Duplicate Physical Address	Duplicate Physical Address		Critical		One Event to One Alarm	All		No		Internal	All Groups
✓	Email Failure	Email Failure		Critical		One Event to One Alarm	All		No		Internal	All Groups
✓	Failed to Disable Adapters	Failed to Disable Adapters		Critical		All Events to One Alarm	All		No		Internal	All Groups
✓	Failed to Enable Adapters	Failed to Enable Adapters		Critical		All Events to One Alarm	All		No		Internal	All Groups
✓	Found Microsoft LLTD or Multicast Address	Found Microsoft LLTD or Multicast Address		Critical		All Events to One Alarm	All		No		Internal	All Groups
✓	Guest / Contractor Pre-allocation Critical	Guest / Contractor Pre-allocation Critical		Minor		All Events to One Alarm	All		No		Internal	All Groups
✓	Guest / Contractor Pre-allocation Warning	Guest / Contractor Pre-allocation Warning		Warning		All Events to One Alarm	All		No		Internal	All Groups
✓	Hard Disk Usage Critical	Hard Disk Usage Critical		Critical		All Events to One Alarm	All		No		Internal	All Groups
✓	Hard Disk Usage Warning	Hard Disk Usage Warning		Warning		All Events to One Alarm	All		No		Internal	All Groups
✓	Host At Risk	Host At Risk		Critical	L1-Group	One Event to One Alarm	All		No		Internal	All Groups
✓	Host Registration Failure	Host Registration Failure		Critical		One Event to One Alarm	All		No		Internal	All Groups
✓	Invalid Physical Address	Invalid Physical Address		Critical		One Event to One Alarm	All		No		Internal	All Groups
✓	L2 Poll Failed	L2 Poll Failed		Critical		All Events to One Alarm	All		No		Internal	All Groups
✓	MAC change event on uplink	MAC change event on uplink		Critical		All Events to One Alarm	All		No		Internal	All Groups
✓	Maximum Concurrent Connections Critical	Maximum Concurrent Connections Critical		Critical		All Events to One Alarm	All		No		Internal	All Groups
✓	Maximum Concurrent Connections Exceeded	Maximum Concurrent Connections Exceeded		Critical		All Events to One Alarm	All		No		Internal	All Groups
✓	Maximum Concurrent Connections Warning	Maximum Concurrent Connections Warning		Critical		All Events to One Alarm	All		No		Internal	All Groups
✓	Memory Usage Critical	Memory Usage Critical		Critical		All Events to One Alarm	All		No		Internal	All Groups
✓	Memory Usage Warning	Memory Usage Warning		Warning		All Events to One Alarm	All		No		Internal	All Groups
✓	Multi-Access Point Detected	Multi-Access Point Detected		Critical	All Management Group	All Events to One Alarm	All		No		Internal	All Groups
✓	No Response from DHCP Server	No Response from DHCP Server		Critical		All Events to One Alarm	All		No		Internal	All Groups
✓	Operating System Status Check Failure	Operating System Update Status Failure		Critical		All Events to One Alarm	All		No		Internal	All Groups
✓	Operating System Updates Available	Operating System Updates Available		Critical		All Events to One Alarm	All		No		Internal	All Groups
✓	Process Memory Usage Critical	Process Memory Usage Critical		Critical		Frequency - 3 within 2 minutes	All		No		Internal	All Groups

FortiNAC Management

Active Dashboard



Summary:

	FortiNAC-CA
Host Name	fnacdemo.bradfordnetworks.com
Status	Running
Product	FortiNAC-CA
Version	8.7
Appliance	FNCMCA
Firmware	6.5.0.316

License Information:

Type	Total	In Use	Available	% Used
Concurrent Licenses	10000	7336	2664	73%

Alarms:

Filter: Display Alarms=25

Date	Alarm	Element
01/16/20 08:37 AM EST	Admin User Login Failure	FortiNAC
01/10/20 01:51 PM EST	L2 Poll Failed	M07ANTALYA3932SOLs(
01/10/20 01:51 PM EST	L2 Poll Failed	MSZ48MARTMLN4385VN
01/10/20 01:51 PM EST	L2 Poll Failed	M64USAK1094VNr01
01/10/20 01:51 PM EST	L2 Poll Failed	M07KRKTLYA5042SOLr0
01/10/20 01:51 PM EST	L2 Poll Failed	T34MSLKMCR5807SOLr0
01/10/20 01:51 PM EST	L2 Poll Failed	M39LULEBUR1191VNr01
01/10/20 01:51 PM EST	L2 Poll Failed	T16PDYMPRK5303SOLr0

Network Device Summary:

Device	Total	Operating	Error
Router	389	378	11
Server	15	14	1
Switch	989	977	12
Wireless Access Point	7320	7320	0
Ports	32684	31384	1300

Host Summary:

Type	Total	Online Enabled	Offline Enabled	Online Disabled	Offline Disabled
Registered Hosts (total)	10126	6460	3666	0	0
- Safe&Authenticated	10126	6460	3666	0	0
- At Risk	0	0	0	0	0
- Pending at Risk	0	0	0	0	0
- Not Authenticated	0	0	0	0	0
- At Risk&Not Auth	0	0	0	0	0
- Pending Risk&Not Auth	0	0	0	0	0
Unregistered Hosts	673	648	25	0	0
IP Phones	1058	862	196	0	0
Total	11857	7970	3887	0	0

User Summary:

Type	Total	Enabled	Disabled
User Registrations	30	30	0

Performance:

	Total	Free	% Used
Memory	7.6 GB	1.9 GB	75%
Swap	0	0	0%
Memory+Swap	7.6 GB	1.9 GB	75%
Disk (/)	99.4 GB	89.3 GB	10%
Disk (/boot)	508.7 MB	353.1 MB	30%

Security Summary:

Time Period: Last 7 Days

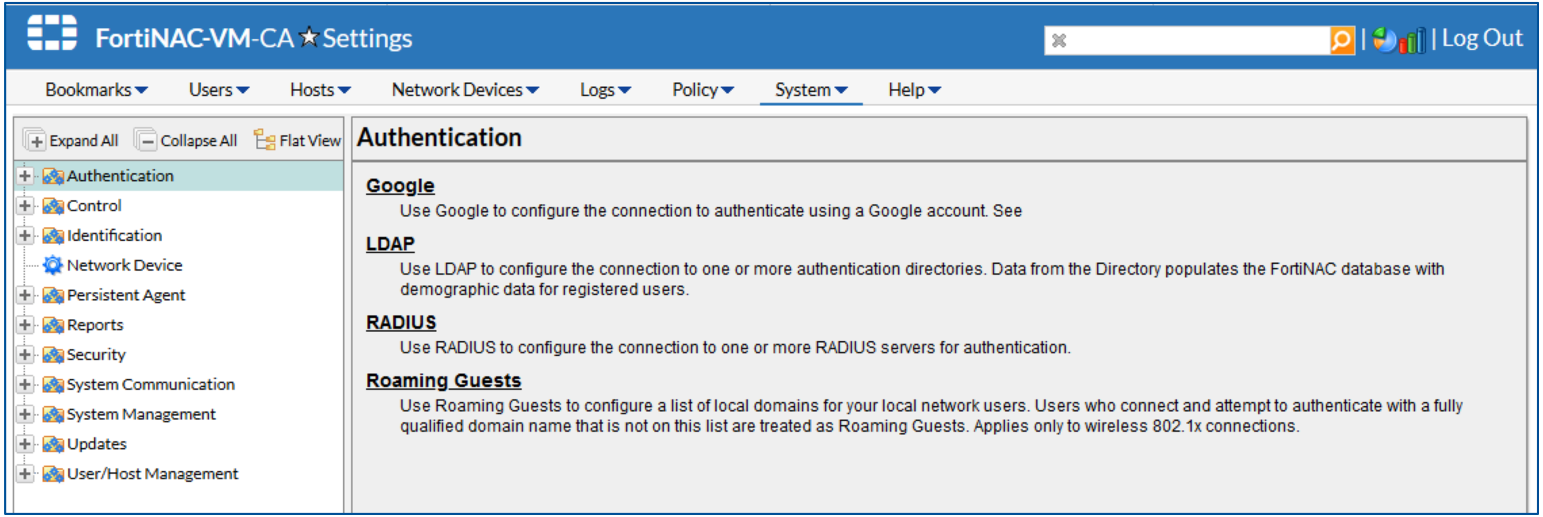
Total Security Events	0
Security Events Discarded	0
Security Events with Known Hosts	0
Security Events with Unknown Hosts	0
Security Events Used for Alarms	0
Security Alarms Generated	0
Unique Hosts Generating Security Alarms	0
Security Alarms with Actions Not Taken	0
Security Alarms with Actions Taken	0
Security Alarms with Actions Taken and Undone	0
Hosts Isolated	0
Hosts Remediated	0

Persistent Agent Summary:

Version	Total	Windows	Mac-OS-X	Linux (x86_64)

FortiNAC Management

Easy to Navigate Settings



Authentication

Google

Use Google to configure the connection to authenticate using a Google account. See

LDAP

Use LDAP to configure the connection to one or more authentication directories. Data from the Directory populates the FortiNAC database with demographic data for registered users.

RADIUS

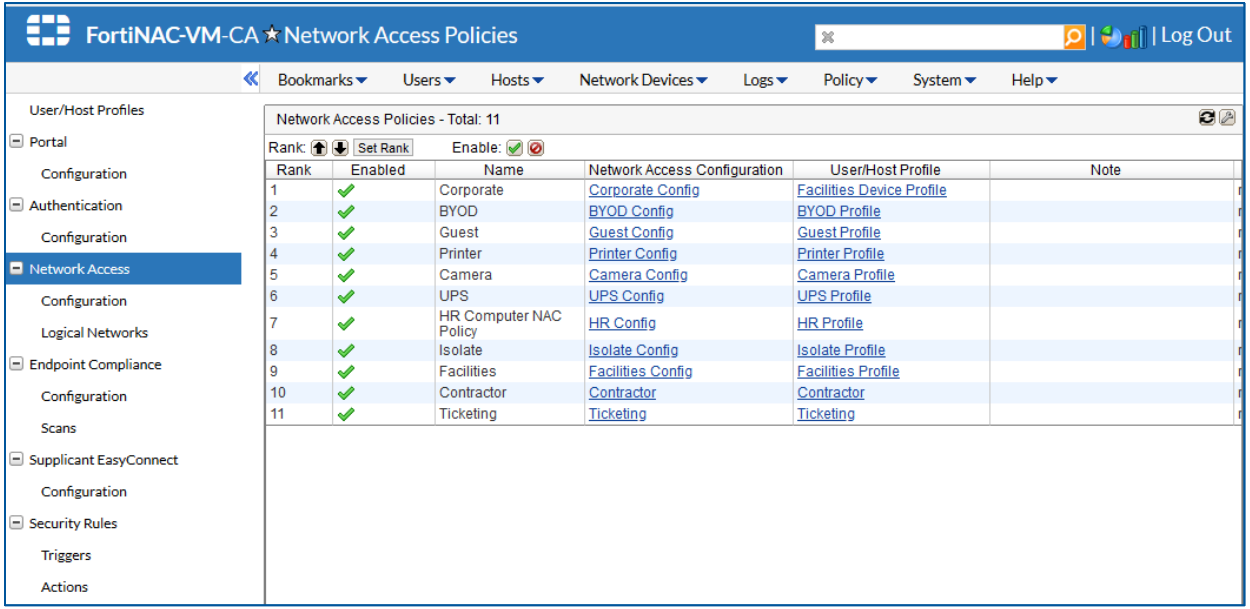
Use RADIUS to configure the connection to one or more RADIUS servers for authentication.

Roaming Guests

Use Roaming Guests to configure a list of local domains for your local network users. Users who connect and attempt to authenticate with a fully qualified domain name that is not on this list are treated as Roaming Guests. Applies only to wireless 802.1x connections.

FortiNAC Management

Easy Network Access Policy Management

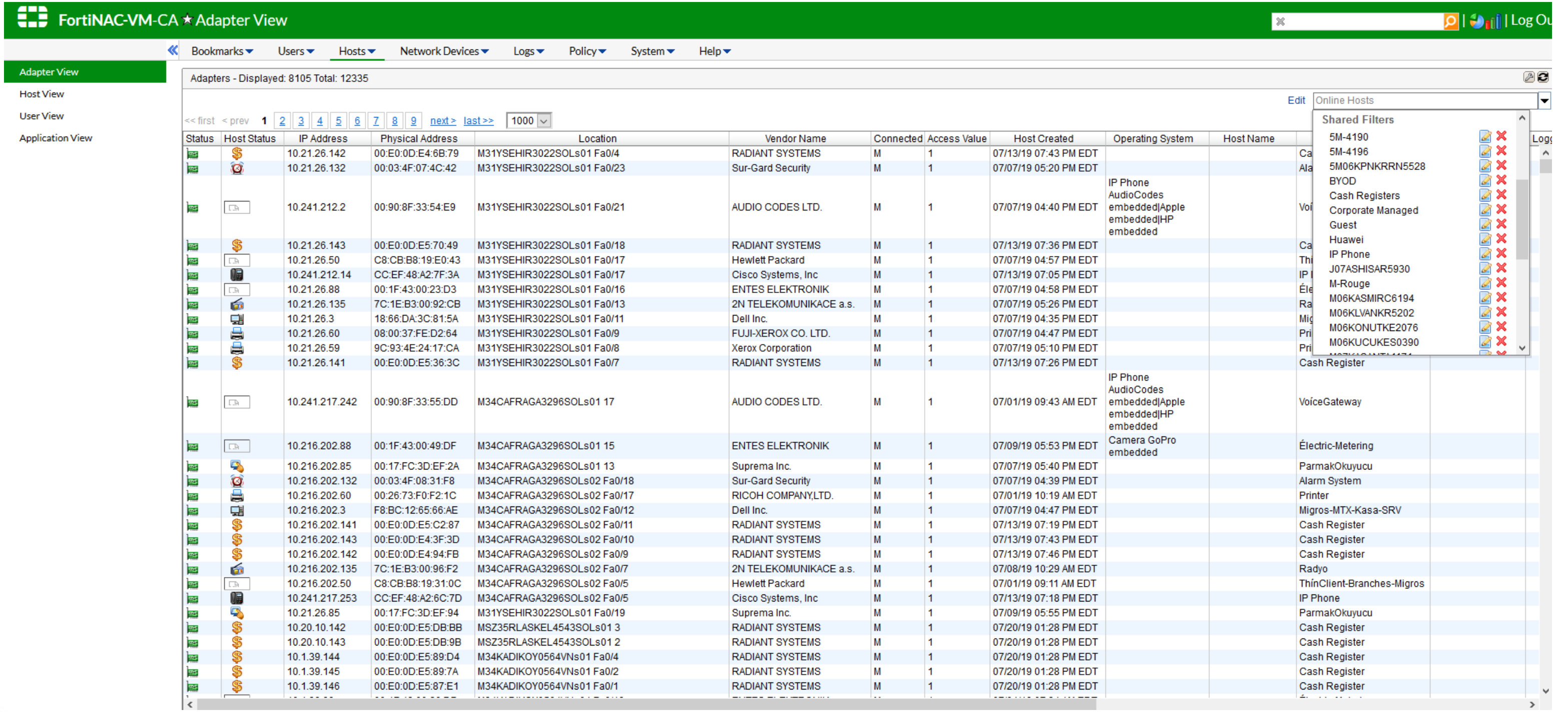


Network Access Policies - Total: 11

Rank	Enabled	Name	Network Access Configuration	User/Host Profile	Note
1	✓	Corporate	Corporate Config	Facilities Device Profile	
2	✓	BYOD	BYOD Config	BYOD Profile	
3	✓	Guest	Guest Config	Guest Profile	
4	✓	Printer	Printer Config	Printer Profile	
5	✓	Camera	Camera Config	Camera Profile	
6	✓	UPS	UPS Config	UPS Profile	
7	✓	HR Computer NAC Policy	HR Config	HR Profile	
8	✓	Isolate	Isolate Config	Isolate Profile	
9	✓	Facilities	Facilities Config	Facilities Profile	
10	✓	Contractor	Contractor	Contractor	
11	✓	Ticketing	Ticketing	Ticketing	

Management, Reporting, & Incident handling

Database Views – Search & Filter & Export



Online Hosts

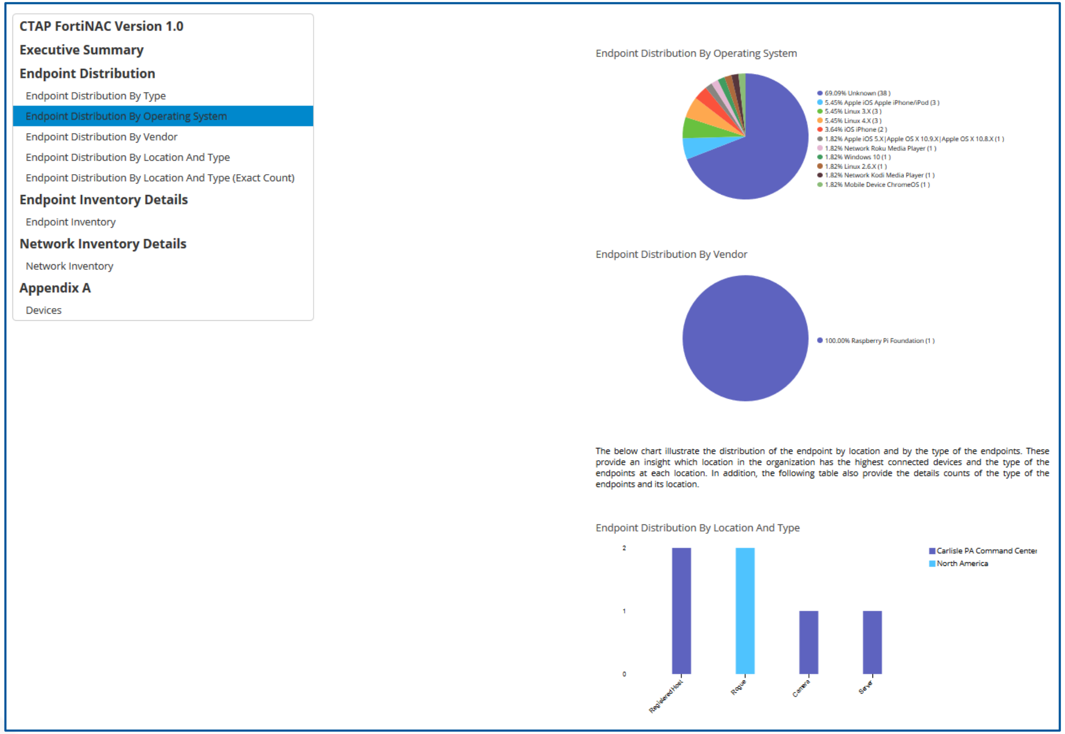
Shared Filters
- 5M-4190
- 5M-4196
- 5M06KPNKRRN5528
- BYOD
- Cash Registers
- Corporate Managed
- Guest
- Huawei
- IP Phone
- J07ASHISAR5930
- M-Rouge
- M06KASMIRC6194
- M06KLVANKR5202
- M06KONUTKE2076
- M06KUCUKES0390

Adapters - Displayed: 8105 Total: 12335

Status	Host Status	IP Address	Physical Address	Location	Vendor Name	Connected	Access Value	Host Created	Operating System	Host Name		Logg
🟩	$	10.21.26.142	00:E0:0D:E4:6B:79	M31YSEHIR3022SOLs01 Fa0/4	RADIANT SYSTEMS	M	1	07/13/19 07:43 PM EDT			Ca	
🟩	⏰	10.21.26.132	00:03:4F:07:4C:42	M31YSEHIR3022SOLs01 Fa0/23	Sur-Gard Security	M	1	07/07/19 05:20 PM EDT			Ala	
🟩	□	10.241.212.2	00:90:8F:33:54:E9	M31YSEHIR3022SOLs01 Fa0/21	AUDIO CODES LTD.	M	1	07/07/19 04:40 PM EDT	IP Phone AudioCodes embedded|Apple embedded|HP embedded		Voí	
🟩	$	10.21.26.143	00:E0:0D:E5:70:49	M31YSEHIR3022SOLs01 Fa0/18	RADIANT SYSTEMS	M	1	07/13/19 07:36 PM EDT			Ca	
🟩	□	10.21.26.50	C8:CB:B8:19:E0:43	M31YSEHIR3022SOLs01 Fa0/17	Hewlett Packard	M	1	07/07/19 04:57 PM EDT			Thi	
🟩	☎	10.241.212.14	CC:EF:48:A2:7F:3A	M31YSEHIR3022SOLs01 Fa0/17	Cisco Systems, Inc	M	1	07/13/19 07:05 PM EDT			IP I	
🟩	□	10.21.26.88	00:1F:43:00:23:D3	M31YSEHIR3022SOLs01 Fa0/16	ENTES ELEKTRONIK	M	1	07/07/19 04:58 PM EDT			Éle	
🟩	📻	10.21.26.135	7C:1E:B3:00:92:CB	M31YSEHIR3022SOLs01 Fa0/13	2N TELEKOMUNIKACE a.s.	M	1	07/07/19 05:26 PM EDT			Ra	
🟩	🖥	10.21.26.3	18:66:DA:3C:81:5A	M31YSEHIR3022SOLs01 Fa0/11	Dell Inc.	M	1	07/07/19 04:35 PM EDT			Mig	
🟩	🖨	10.21.26.60	08:00:37:FE:D2:64	M31YSEHIR3022SOLs01 Fa0/9	FUJI-XEROX CO. LTD.	M	1	07/07/19 04:47 PM EDT			Pri	
🟩	🖨	10.21.26.59	9C:93:4E:24:17:CA	M31YSEHIR3022SOLs01 Fa0/8	Xerox Corporation	M	1	07/07/19 05:10 PM EDT			Pri	
🟩	$	10.21.26.141	00:E0:0D:E5:36:3C	M31YSEHIR3022SOLs01 Fa0/7	RADIANT SYSTEMS	M	1	07/13/19 07:26 PM EDT			Cash Register	
🟩	□	10.241.217.242	00:90:8F:33:55:DD	M34CAFRAGA3296SOLs01 17	AUDIO CODES LTD.	M	1	07/01/19 09:43 AM EDT	IP Phone AudioCodes embedded|Apple embedded|HP embedded		VoíceGateway	
🟩	□	10.216.202.88	00:1F:43:00:49:DF	M34CAFRAGA3296SOLs01 15	ENTES ELEKTRONIK	M	1	07/09/19 05:53 PM EDT	Camera GoPro embedded		Électric-Metering	
🟩	🖥	10.216.202.85	00:17:FC:3D:EF:2A	M34CAFRAGA3296SOLs01 13	Suprema Inc.	M	1	07/07/19 05:40 PM EDT			ParmakOkuyucu	
🟩	⏰	10.216.202.132	00:03:4F:08:31:F8	M34CAFRAGA3296SOLs02 Fa0/18	Sur-Gard Security	M	1	07/07/19 04:39 PM EDT			Alarm System	
🟩	🖨	10.216.202.60	00:26:73:F0:F2:1C	M34CAFRAGA3296SOLs02 Fa0/17	RICOH COMPANY,LTD.	M	1	07/01/19 10:19 AM EDT			Printer	
🟩	🖥	10.216.202.3	F8:BC:12:65:66:AE	M34CAFRAGA3296SOLs02 Fa0/12	Dell Inc.	M	1	07/07/19 04:47 PM EDT			Migros-MTX-Kasa-SRV	
🟩	$	10.216.202.141	00:E0:0D:E5:C2:87	M34CAFRAGA3296SOLs02 Fa0/11	RADIANT SYSTEMS	M	1	07/13/19 07:19 PM EDT			Cash Register	
🟩	$	10.216.202.143	00:E0:0D:E4:3F:3D	M34CAFRAGA3296SOLs02 Fa0/10	RADIANT SYSTEMS	M	1	07/13/19 07:43 PM EDT			Cash Register	
🟩	$	10.216.202.142	00:E0:0D:E4:94:FB	M34CAFRAGA3296SOLs02 Fa0/9	RADIANT SYSTEMS	M	1	07/13/19 07:46 PM EDT			Cash Register	
🟩	📻	10.216.202.135	7C:1E:B3:00:96:F2	M34CAFRAGA3296SOLs02 Fa0/7	2N TELEKOMUNIKACE a.s.	M	1	07/08/19 10:29 AM EDT			Radyo	
🟩	□	10.216.202.50	C8:CB:B8:19:31:0C	M34CAFRAGA3296SOLs02 Fa0/5	Hewlett Packard	M	1	07/01/19 09:11 AM EDT			ThínClient-Branches-Migros	
🟩	☎	10.241.217.253	CC:EF:48:A2:6C:7D	M34CAFRAGA3296SOLs02 Fa0/5	Cisco Systems, Inc	M	1	07/13/19 07:18 PM EDT			IP Phone	
🟩	🖥	10.21.26.85	00:17:FC:3D:EF:94	M31YSEHIR3022SOLs01 Fa0/19	Suprema Inc.	M	1	07/09/19 05:55 PM EDT			ParmakOkuyucu	
🟩	$	10.20.10.142	00:E0:0D:E5:DB:BB	MSZ35RLASKEL4543SOLs01 3	RADIANT SYSTEMS	M	1	07/20/19 01:28 PM EDT			Cash Register	
🟩	$	10.20.10.143	00:E0:0D:E5:DB:9B	MSZ35RLASKEL4543SOLs01 2	RADIANT SYSTEMS	M	1	07/20/19 01:28 PM EDT			Cash Register	
🟩	$	10.1.39.144	00:E0:0D:E5:89:D4	M34KADIKOY0564VNs01 Fa0/4	RADIANT SYSTEMS	M	1	07/20/19 01:28 PM EDT			Cash Register	
🟩	$	10.1.39.145	00:E0:0D:E5:89:7A	M34KADIKOY0564VNs01 Fa0/2	RADIANT SYSTEMS	M	1	07/20/19 01:28 PM EDT			Cash Register	
🟩	$	10.1.39.146	00:E0:0D:E5:87:E1	M34KADIKOY0564VNs01 Fa0/1	RADIANT SYSTEMS	M	1	07/20/19 01:28 PM EDT			Cash Register	

Management, Reporting, & Incident handling

Detailed Customer Reports Using FortiAnalyzer



CTAP FortiNAC Version 1.0

Executive Summary

Endpoint Distribution

Endpoint Distribution By Type

Endpoint Distribution By Operating System

Endpoint Distribution By Vendor

Endpoint Distribution By Location And Type

Endpoint Distribution By Location And Type (Exact Count)

Endpoint Inventory Details

Endpoint Inventory

Network Inventory Details

Network Inventory

Appendix A

Devices

Endpoint Distribution By Operating System

● 69.09% Unknown (38)
● 5.45% Apple iOS Apple iPhone/iPod (3)
● 5.45% Linux 3.X (3)
● 5.45% Linux 4.X (3)
● 3.64% iOS iPhone (2)
● 1.82% Apple iOS 5.X|Apple OS X 10.9.X|Apple OS X 10.8.X (1)
● 1.82% Network Roku Media Player (1)
● 1.82% Windows 10 (1)
● 1.82% Linux 2.6.X (1)
● 1.82% Network Kodi Media Player (1)
● 1.82% Mobile Device ChromeOS (1)

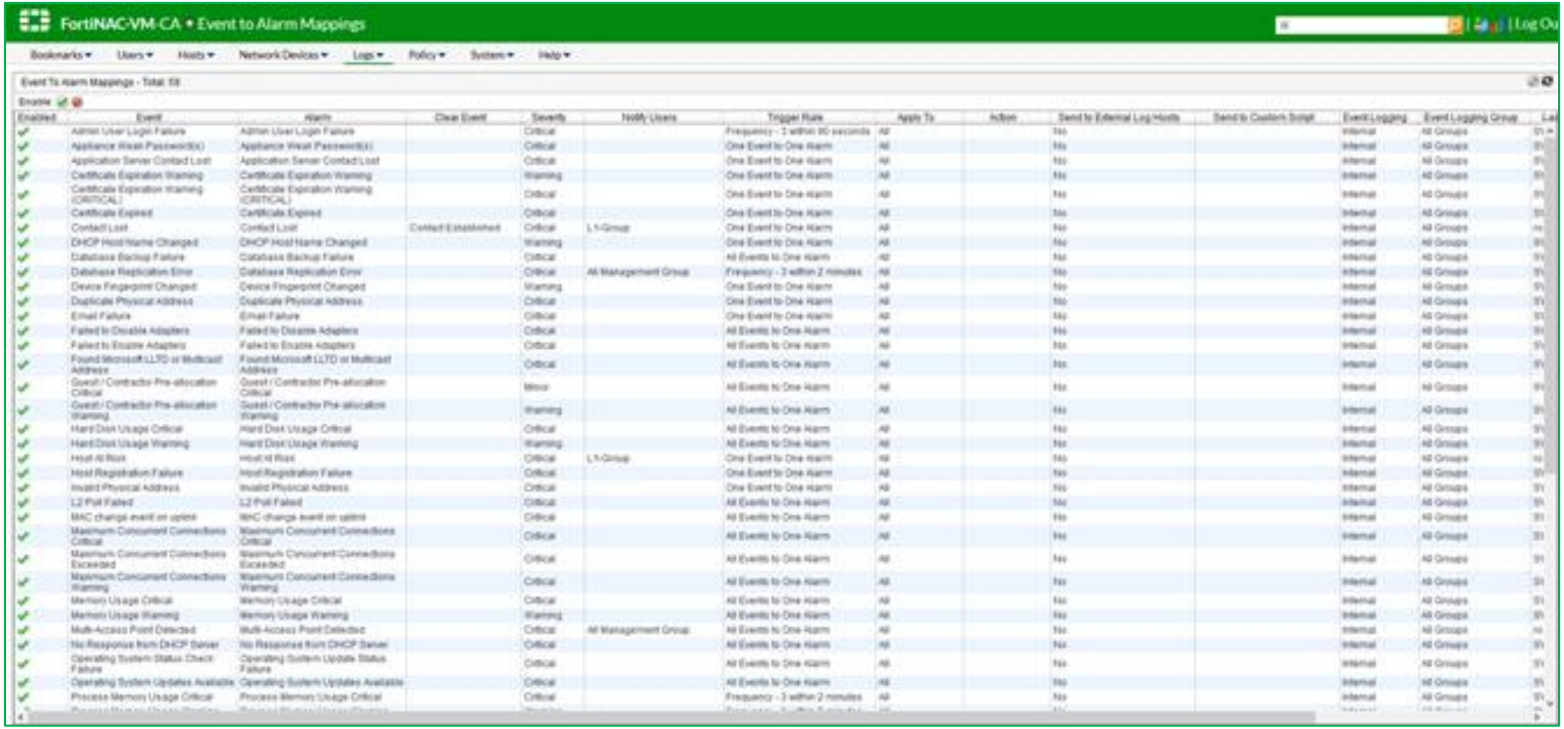
Endpoint Distribution By Vendor

The below chart illustrate the distribution of the endpoint by location and by the type of the endpoints. These provide an insight which location in the organization has the highest connected devices and the type of the endpoints at each location. In addition, the following table also provide the details counts of the type of the endpoints and its location.

Endpoint Distribution By Location And Type

Management, Reporting, & Incident handling

431 Unique Events – Custom Map Events to Alarm



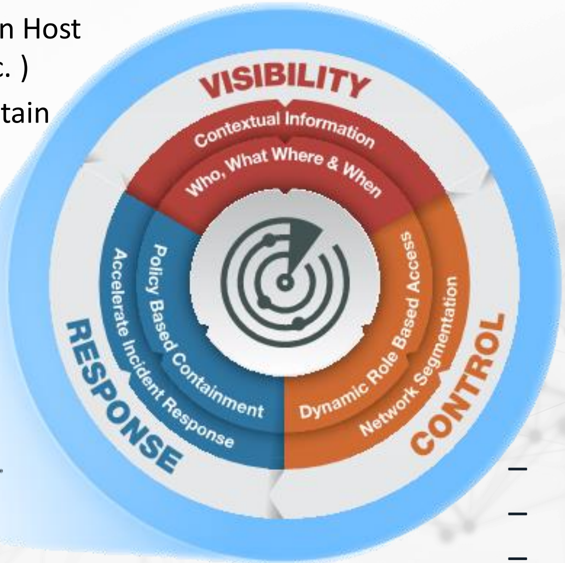
Event To Alarm Mappings - Total: 58

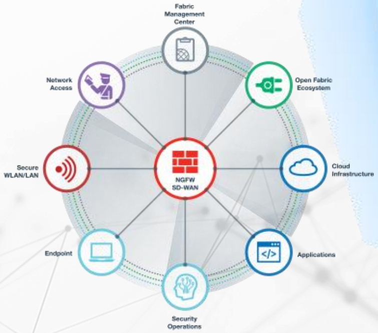
Enabled	Event	Alarm	Clear Event	Severity	Notify Users	Trigger Rule	Apply To	Action	Send to External Log Hosts	Send to Custom Script	Event Logging	Event Logging Group	La
✓	Admin User Login Failure	Admin User Login Failure		Critical		Frequency - 3 within 90 seconds	All		No		Internal	All Groups	[illegible]
✓	Appliance Weak Password(s)	Appliance Weak Password(s)		Critical		One Event to One Alarm	All		No		Internal	All Groups	[illegible]
✓	Application Server Contact Lost	Application Server Contact Lost		Critical		One Event to One Alarm	All		No		Internal	All Groups	[illegible]
✓	Certificate Expiration Warning	Certificate Expiration Warning		Warning		One Event to One Alarm	All		No		Internal	All Groups	[illegible]
✓	Certificate Expiration Warning (CRITICAL)	Certificate Expiration Warning (CRITICAL)		Critical		One Event to One Alarm	All		No		Internal	All Groups	[illegible]
✓	Certificate Expired	Certificate Expired		Critical		One Event to One Alarm	All		No		Internal	All Groups	[illegible]
✓	Contact Lost	Contact Lost	Contact Established	Critical	L1-Group	One Event to One Alarm	All		No		Internal	All Groups	[illegible]
✓	DHCP Host Name Changed	DHCP Host Name Changed		Warning		One Event to One Alarm	All		No		Internal	All Groups	[illegible]
✓	Database Backup Failure	Database Backup Failure		Critical		All Events to One Alarm	All		No		Internal	All Groups	[illegible]
✓	Database Replication Error	Database Replication Error		Critical	All Management Group	Frequency - 3 within 2 minutes	All		No		Internal	All Groups	[illegible]
✓	Device Fingerprint Changed	Device Fingerprint Changed		Warning		One Event to One Alarm	All		No		Internal	All Groups	[illegible]
✓	Duplicate Physical Address	Duplicate Physical Address		Critical		One Event to One Alarm	All		No		Internal	All Groups	[illegible]
✓	Email Failure	Email Failure		Critical		One Event to One Alarm	All		No		Internal	All Groups	[illegible]
✓	Failed to Disable Adapters	Failed to Disable Adapters		Critical		All Events to One Alarm	All		No		Internal	All Groups	[illegible]
✓	Failed to Enable Adapters	Failed to Enable Adapters		Critical		All Events to One Alarm	All		No		Internal	All Groups	[illegible]
✓	Found Microsoft LLTD or Multicast Address	Found Microsoft LLTD or Multicast Address		Critical		All Events to One Alarm	All		No		Internal	All Groups	[illegible]
✓	Guest / Contractor Pre-allocation Critical	Guest / Contractor Pre-allocation Critical		Minor		All Events to One Alarm	All		No		Internal	All Groups	[illegible]
✓	Guest / Contractor Pre-allocation Warning	Guest / Contractor Pre-allocation Warning		Warning		All Events to One Alarm	All		No		Internal	All Groups	[illegible]
✓	Hard Disk Usage Critical	Hard Disk Usage Critical		Critical		All Events to One Alarm	All		No		Internal	All Groups	[illegible]
✓	Hard Disk Usage Warning	Hard Disk Usage Warning		Warning		All Events to One Alarm	All		No		Internal	All Groups	[illegible]
✓	Host At Risk	Host At Risk		Critical	L1-Group	One Event to One Alarm	All		No		Internal	All Groups	[illegible]
✓	Host Registration Failure	Host Registration Failure		Critical		One Event to One Alarm	All		No		Internal	All Groups	[illegible]
✓	Invalid Physical Address	Invalid Physical Address		Critical		One Event to One Alarm	All		No		Internal	All Groups	[illegible]
✓	L2 Poll Failed	L2 Poll Failed		Critical		All Events to One Alarm	All		No		Internal	All Groups	[illegible]
✓	MAC change event on uplink	MAC change event on uplink		Critical		All Events to One Alarm	All		No		Internal	All Groups	[illegible]
✓	Maximum Concurrent Connections Critical	Maximum Concurrent Connections Critical		Critical		All Events to One Alarm	All		No		Internal	All Groups	[illegible]
✓	Maximum Concurrent Connections Exceeded	Maximum Concurrent Connections Exceeded		Critical		All Events to One Alarm	All		No		Internal	All Groups	[illegible]
✓	Maximum Concurrent Connections Warning	Maximum Concurrent Connections Warning		Critical		All Events to One Alarm	All		No		Internal	All Groups	[illegible]
✓	Memory Usage Critical	Memory Usage Critical		Critical		All Events to One Alarm	All		No		Internal	All Groups	[illegible]
✓	Memory Usage Warning	Memory Usage Warning		Warning		All Events to One Alarm	All		No		Internal	All Groups	[illegible]
✓	Multi-Access Point Detected	Multi-Access Point Detected		Critical	All Management Group	All Events to One Alarm	All		No		Internal	All Groups	[illegible]
✓	No Response from DHCP Server	No Response from DHCP Server		Critical		All Events to One Alarm	All		No		Internal	All Groups	[illegible]
✓	Operating System Status Check Failure	Operating System Update Status Failure		Critical		All Events to One Alarm	All		No		Internal	All Groups	[illegible]
✓	Operating System Updates Available	Operating System Updates Available		Critical		All Events to One Alarm	All		No		Internal	All Groups	[illegible]
✓	Process Memory Usage Critical	Process Memory Usage Critical		Critical		Frequency - 3 within 2 minutes	All		No		Internal	All Groups	[illegible]
✓	Process Memory Usage Warning	Process Memory Usage Warning		Warning		Frequency - 3 within 5 minutes	All		No		Internal	All Groups	[illegible]

FortiNAC Feature Overview

Pro Features

- Receive trigger event from IPS/SIEM/Tenable/Qualys
- Intelligent containment and notification options based on Host Profile (device type, user etc.)
- Immediately isolate and contain Indicators of Compromise





BASE Features

- Discovery of Enterprise Network Infrastructure
- Active Directory Integration
- Builds Endpoint Database of MAC/IP/Port/Interface
- Rogue Hunting Tools
  - MDM Integration (AirWatch, InTune, Chromebook etc.)
  - Industrial OT Integration with Nozomi integration
  - FortiClient EMS integration
  - Agentless Device Profiling – Active & Passive
  - Fortigate as a sensor & FSSO Integration

Control
  - Rogue Device Detection and containment
  - Network Access Policies (wired 802.1x not required)

PLUS Features

- Lightweight NAC agents (Dissolvable & Persistent)
- Endpoint Compliance for Windows, OSX & Linux
- Captive Portal for BYOD, Contractor and Guests
- Outbound Security Events to SEIM, Syslog or API

vmware vSphere   Microsoft Hyper-v   KVM   aws   Microsoft Azure

FortiNAC Components

Virtual Machines

vmware vSphere

Microsoft Hyper-v

KVM

aws

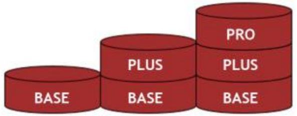
Microsoft Azure

FNC-CA-VM VMs scale up to 25,000 potential access ports*

FortiNAC Hardware Appliances

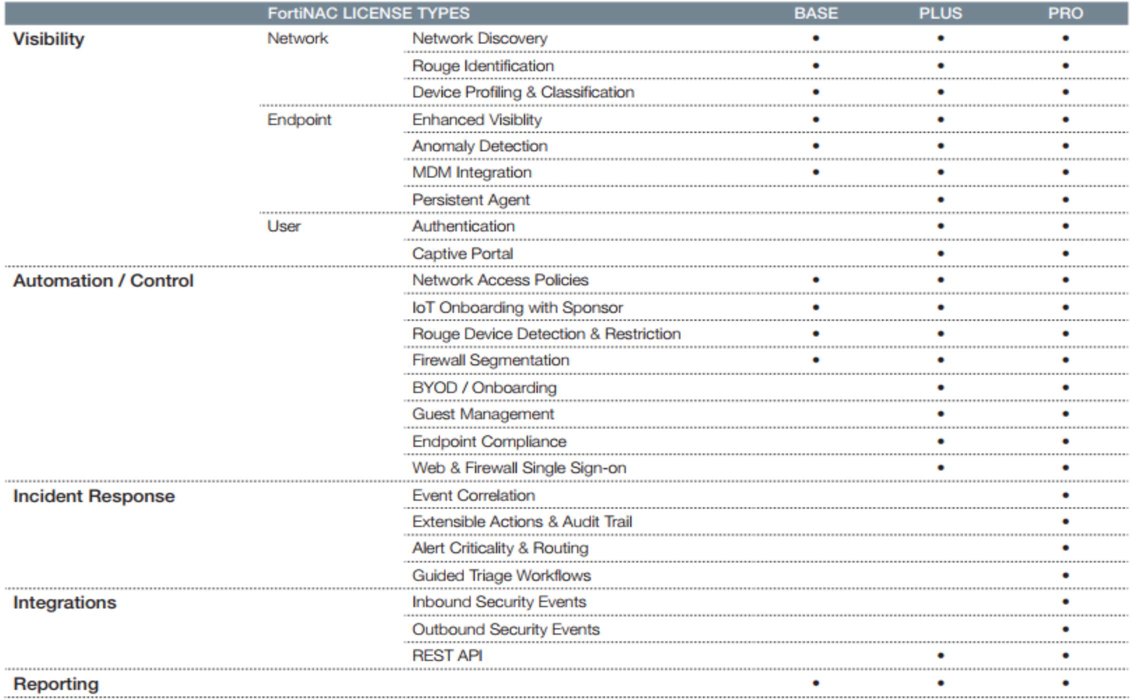
- FortiNAC-CA-500C (up to 2k potential access ports*)
- FortiNAC-CA-600C (up to 15k potential access ports*)
- FortiNAC-CA-700C (up to 25k potential access ports*)
- FortiNAC-M-550C (FortiNAC-CA Manager)

*Total Number of Used or Unused Switch Ports + Total Number of Active Wireless Users = **Potential Access Ports**



Perpetual Licenses:
BASE-PLUS-PRO
Subscription Available For PRO only

FortiNAC Licenses



	FortiNAC LICENSE TYPES		BASE	PLUS	PRO
Visibility	Network	Network Discovery	•	•	•
		Rouge 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	•	•	•
		Rouge Device Detection & Restriction	•	•	•
		Firewall Segmentation	•	•	•
		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			•	•	•

FORTINET®