FortiNAC

Known Anomalies

Version: 8.x

Date: March 30, 2022

FORTINET DOCUMENT LIBRARY
http://docs.fortinet.com

FORTINET VIDEO GUIDE
http://video.fortinet.com

FORTINET KNOWLEDGE BASE
https://community.fortinet.com/t5/Knowledge-Base/ct-p/knowledgebase

FORTINET BLOG
http://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
http://support.fortinet.com

FORTINET COOKBOOK
http://cookbook.fortinet.com

NSE INSTITUTE
http://training.fortinet.com

FORTIGUARD CENTER
http://fortiguard.com

FORTICAST
http://forticast.fortinet.com

END USER LICENSE AGREEMENT
http://www.fortinet.com/doc/legal/EULA.pdf

CONTENTS

Overview

These are the Known Anomalies in FortiNAC and agent packages. There are four categories:

FortiNAC: Unless otherwise indicated, anomalies apply to the following FortiNAC software versions listed below (and lower)

8.8.11

8.7.6

Agent: Anomalies specific to agent version (and lower):

5.3.0

Endpoint Compliance: AV/AS/OS support

Reporter/Analytics[1]: Anomalies specific to Analytics version (and lower):

6.0.2

[1] This product is no longer available and has been replaced by FortiAnalyzer.

FortiNAC

ID	FortiNAC Anomaly Description
0780312	FortiNAC does not integrate with Azure Active Directory due to SAML connection requirements.
0747921	Portal renaming does not rename the associated CSS files.
0641036	Multi-factor authentication (MFA) for the Administration GUI login is currently not supported.
0710416	There can be a delay in updating IP addresses for isolated hosts in host and adapter view.
0708720	Policy evaluation may not be triggered after a host status update in Microsoft InTune. This can prevent the host from being moved to the proper network. For details and workaround see related KB article 203843.
0694407	Linux hosts running CrowdStrike Falcon sensor 6.11 and later are not being detected by the agent. This causes hosts running CrowdStrike Falcon to incorrectly fail scans. For details and workaround, see related KB article 202694.
0718864	FortiNAC does not send all required attributes in CoA packets sent to Ubiquiti when an online host record is deleted from the database.
0708936	FortiNAC will logoff SSO for sessions that remain connected to a managed FortiGate IPSec VPN tunnel after 12 hours.
0714219 0686910	NCM communication issues when the NAC systems are connected through the WAN. For details see related KB article 192434.
0671121	Wired devices do not automatically register using Microsft InTune. For details and workaround see related KB article 197812.
0726333	Entitlements (such as concurrent licenses) for Subscription Licenses are not accurately reflected in the Administration UI License Management view and only show Base licenses. **Workaround**: Use the License Information panel in the Dashboard instead.

ID	FortiNAC Anomaly Description
0682438	'Page Unresponsive' error when exporting hosts. For details and workaround see related KB article 193878.
0609976	Cisco WLC 9800 Model Configuration tab does not include the drop down VLAN lists under Access Value. For details and workaround see related KB article 198790.
0646580	Restarting FortiNAC services can generate a large number of SSH sessions with ASA. For details, refer to related KB article 195876.
0631115	Only 50000 records display in Adapter and Host Views Example: Adapters - Displayed: 50000 Total: 57500
0609046	A port where the master Aruba Instant AP (IAP) with VIP is connected becomes a "learned uplink". This type of uplink is not dynamically undone / removed when the IAP (with the VIP) is disconnected from that port.
0610581	L3 eth1 sub-interfaces are not removed after re-configuring an appliance configured for L3 Network Type to L2.
0590480	Dell switches configured to use a directory (such as Active Directory) for enable level CLI access will fail CLI credential validation. This will occur whether or not the enable password field is left blank in the Model Configuration. For details and workaround see related KB article 193098.
	Not all models of all network devices can be configured to perform Physical MAC Address Filtering even though the Admin UI indicates that the configuration can be set. **Resolution:** Hosts can be disabled by implementing a Dead-end VLAN.
	For Portal v2 configurations, web pages that are stored in the site directory to be used for Scan Configurations will not be included when you do an Export of the Portal v2 configuration. **Resolution:** The files in the site directory are backed up with the Remote Backup feature, but otherwise keep a copy of these files in a safe place.
	Removing a device from the L2 Wired Devices or L2 Wireless Devices Group does not disable L2 (Hosts) Polling under the Polling tab in Topology.

ID	FortiNAC Anomaly Description
	The "Set all hosts 'Risk State' to 'Safe'" button changes the status of all hosts marked At-Risk to Safe. However, the status of the individual scans for each host remain unchanged.
	In a Layer 3 High Availability (HA) environment, configWizard must have a DHCP scope defined. Running configWizard without a DHCP scope can cause a failover.
	On FortiNAC appliances with CentOS 7, duplicate log messages may appear in dhcpd.log for each sub interface (eth1, eth1:1, eth1:2, etc).
	System > Settings > Updates > Operating System will only record and display dates of OS updates that are completed through the Administrative UI. If Operating System updates are run via command line using the "yum" tool, the update is not recorded. **Resolution:** Execute Operating System Updates through the Administrative UI in order to maintain update history.
0522468	Although there are fields to set the role or access value in the Authentication portal, these functions are currently not supported.

Agent

ID	Agent Anomaly Description
0676680	Custom service scans do not pass as expected on Linux CentOS 8 machines. See KB article 198335.
0739990	Android Mobile Agent prompts for server name. For details and workaround see related KB article 195909.
	Additional login requests may occur when using the Persistent Agent with a lengthy scan.
	Agent versions 3.4.0 through 3.5.5 are not supported on Mac OS X 10.6, Snow Leopard, and 4.x versions of the Agent will only be supported on Mac OS X 10.7 and above. **Resolution:** Apple delivered its final update for the Mac OS X 10.6 Operating System in September 2013, but if hosts with this Operating System are still allowed on your network, use a 3.x version of the Agent - 3.5.6 or greater. **Note**: 10.6 is no longer supported. For a list of currently supported client platforms, refer to the Agent Release Notes in the Fortinet Document Library.
	Linux hosts cannot be prevented from accessing the network via VPN based on FortiNAC group membership that is referenced in a User/Host Profile to assign a Network Access Policy. **Resolution:** There is no workaround.
	Currently the Linux Persistent Agent does not have the ability to be updated via the FortiNAC Administrative UI.
	Currently the Agent is not supported on Windows 10S and will not run.
	When a user attempts to register a host which exceeds the user's maximum number of hosts allowed, if the user is using the Dissolvable Agent a message is displayed, "Over Registered Limit". If the user is using the Persistent Agent, however, "Registration Failed" is displayed.
	Hosts connecting to VPN via a local SSID do not match the VPN Client: Yes

ID	Agent Anomaly Description
	criteria.

Endpoint Compliance

ID	Endpoint Compliance Anomaly Description
	Only English versions of AV/AS and their corresponding definitions are supported.
	Anti-Virus product Iolo technologies System Mechanic Professional is currently not supported.
0675180	False positive Scan Results when there are no sub-settings selected in Operating System check.
0674438	"Processes" Scan Type option is not available when creating custom scans for macOS systems.
0695435	FortiEDR is currently not supported. If required, contact sales or support to submit a New Feature Request (NFR).
	Fortinet does not support the Sophos UTM.

Reporter/Analytics

ID	Analytics Anomaly Description
	There is currently no method to backup the Analytics database using the Administrative UI.
	When trying to retrieve data from a report, the "Please Wait" message does not disappear if there is a server issue.
	In the **Reports > Security Reports > Security Alarms** view, the Action Email Group is listing the database ID number instead of the Group name.
	Device data is lost when upgrading Analytics from version 3.x directly to 5.x. **Workaround:** Prior to upgrade, export the reports pertaining to device data. Navigate to the following locations in the Analytics Administrative UI and click the **Export Reports** button: **Reports > PCI Compliance Report > Network Device Count** **Reports > Network Report > Device Graphs**
	If the ETL Job Scheduler frequency is set to “Daily,” the Dashboard calculation becomes erratic. Sometimes the Dashboard is calculated, but most of the time is does not, resulting in a blank Dashboard screen. **Resolution:** Change the frequency to either hourly or every 12 hours.
	On a large data set, Analytics GUI will time out and the report cannot be run. If this occurs, call support.
	The process name for the Analytics agent appears as "jar" when viewing the results of the jps command in the FortiNAC Server/Control Server CLI.
	Analytics custom date range displays dates outside of the search criteria.
	When attempting to add a client in Analytics using a name that already exists for "Clients FortiNAC DB" name, a generic message "Error - return to dashboard" is returned.
	On-Premise Analytics does not support LDAP authentication. User accounts must be created along with credentials.

ID	Analytics Anomaly Description
	There is no Single Sign-On for On-Premise Analytics. If accessing Analytics via the FortiNAC Administrative UI, user must enter their Analytics UI credentials.
	Attempting to export large amounts of data to Excel from Analytics may fail. **Resolution:** Export to PDF.
	Analytics On-Premise Server occasionally displays 404 error on the landing page of the GUI. **Resolution:** Restart the wildfly service **service bsc-wildfly restart**
	Unable to perform upgrade using the Analytics Administration UI. **Resolution:** Upgrade via Analytics CLI. Contact Support for assistance.

Device Support Considerations

ID	Description
0711696	Cisco SG200 support is limited to visibility only. The switch does not provide the management capabilities required for control/enforcement.
0679230	Aruba 9012-US currently not supported. If required, contact sales or support to submit a New Feature Request (NFR).
0548902	Management of wired ports on Aerohive AP-150W controlled by AerohiveNG is currently unsupported.
0606729	The feature "Palo Alto VPN Integration" is currently not supported. It has been determined not to be ready for customer production use for managing remote user VPN connections through Palo Alto firewall.
	At this time, integration with Juniper MAG6610 VPN Gateway is not supported. This includes Pulse Connect Secure ASA.
	At this time, integration with Cisco 1852i Controller is not supported due to the device's limited CLI and SNMP capability. For details, see related KB article 189545.
	At this time, integration with Ubiquiti AirOS AP is not supported. Ubiquiti AirOS AP does not have the necessary capabilities to allow for full integration with FortiNAC. The limitations are as follows: • No support for external MAC Authentication using RADIUS. • Limited CLI and SNMP capability. No ability to dynamically modify access parameters (ie. VLANs) for active sessions.
	At this time, UniFi AP AC-Pro is not supported. The AP does not have the necessary capabilities to allow for full integration.
	At this time, Fortinet does not support wired port management for the Cisco 702W. The access point does not provide the management capabilities required.
	At this time, Fortinet is not able to support the Linksys LAPN600 Wireless-N600 Dual Band Access Point.

ID	Description
	Ports on Avaya Networks 4850GTS-PWR+ switches sometimes show "Not Connected" even though the port is active. This is due to multiple ports on the switch using the same MAC Address. This prevents NAC from correctly discerning which are "Connected" versus "Not Connected". There is no workaround.
	Device models for Avaya 4800 switches (and potentially other related models) only support SSH. Device models for Avaya Ethernet Routing Switches only support Telnet. Contact Support if the alternate protocol is required.