FortiNAC

Detect Persistent Agents Not Communicating

Version: 8.3, 8.5, 8.6, 8.7, 8.8

Date: October 28, 2021

Rev: B

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

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

FORTINET KNOWLEDGE BASE
http://kb.fortinet.com

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

This document provides guidance on configuring alarms to trigger when a Persistent Agent is no longer communicating with FortiNAC.

Configuration Procedure Overview

1. **Administrator Notification**: Configure FortiNAC to…
   - Detect when a Persistent Agent is no longer communicating
   - Email or send SMS message with information regarding the violating host.
   - Not take action against the host.

It is strongly recommended to configure alarms for notification first. This provides an opportunity to validate that the alarms are working as expected without affecting host network access. Once alarms have been validated, proceed with step 2 (if desired).

2. **Isolate Hosts when agent communication is lost**: Configure FortiNAC to…
   - Detect Persistent Agent is no longer communicating.
   - Isolate the violating hosts.
   - Allow for the reinstallation of the persistent agent. Once agent is installed and communication is restored, the host will be allowed back onto the network.

Requirements

- Supported Engine Version: 8.3 and greater
- Supported Agent version: 5.1 and greater
- FortiNAC has up-to-date network connectivity data (in order to determine a host's online status). This requires the following:
  - Wired network devices are successfully polled at a regular interval (typically 1 hour).
  - Wired network devices are sending either Link Up/Link Down or Mac Notification traps.
  - Wireless devices are successfully polled at a regular interval (typically 15 minutes).
- All Persistent Agents can communicate via UDP ports 4567 and/or TCP 4568 across the network.
- For host isolation (#2) Remediation must be already enforced, allowing for the quarantine of any violating hosts.

Configuration

Administrator Notification

Configure

Create the alarm action that will trigger when the "Persistent Agent Not Communicating" event is generated. How long FortiNAC waits before triggering the event is determined by the setting **Agent Contact Window on Host Connect.** To view/modify this setting, navigate to **Policy > Persistent Agent Properties > Security Management.**

Once the alarm is triggered, the Administrator is notified of the event via email or SMS message containing information about the violating host.

1. Navigate to **Logs > Event Management**.
2. Confirm "Persistent Agent Not Communicating" and "Persistent Agent Communication Resumed" events are enabled. The first column (Log) should be set to **Internal** and set to apply to the desired group. For more details on this view see Events in the Administration Guide.

Internal	Persistent Agent Communication Resumed	All Groups	Host	SYSTEM
Internal	Persistent Agent Not Communicating	All Groups	Host	SYSTEM

3. Navigate to **Logs > Event to Alarm Mappings**.
4. Click **Add**.
5. Configure the alarm using the settings in the table below:

Trigger Event	Persistent Agent Not Communicating
Severity	Minor
Clear on Event	Persistent Agent Communication Resumed
Trigger Rule	1 Event to 1 Alarm
Notify Users (check)	Desired Admin User Group to receive notifications.

6. Select the desired notification method (Email or SMS).

For more details on this view see Add or modify alarm mapping in the Administration Guide.

7. Click **OK**.

Validate

Agent not communicating after connecting to the network

On a known working host with the Persistent Agent successfully communicating, do the following:

1. Navigate to **Logs > Events**.
2. Next to **Add Filter**, select **Event** from the drop-down menu.
3. Next to **Event**, select **Persistent Agent Not Communicating** from the drop-down menu.
4. Click **Update.**
5. Disconnect host from network.
6. Disable the Persistent agent service on the host. For instructions see KB article FD42403 or the Persistent Agent Deployment and Configuration reference manual.
7. Reconnect to network.
8. "Persistent Agent Not Communicating" event is generated and displays in Events view.
9. Alarm is triggered when the Trigger Rule setting has been satisfied.
10. Verify alarm notification was received.
11. Re-enable Persistent Agent service.
12. Agent communicates with FortiNAC.
13. "Persistent Agent Communication Resumed" event is generated and alarm cleared.

Agent stops communicating while connected to the network

On a known working host with the Persistent Agent successfully communication, do the following:

1. While connected to the network, disable the Persistent Agent service.
2. "Persistent Agent Not Communicating" event is generated and displays in Events view.
3. Alarm is triggered when the Trigger Rule setting has been satisfied.
4. Re-enable Persistent Agent service.
5. Agent communicates with FortiNAC.
6. "Persistent Agent Communication Resumed" event is generated and alarm cleared.

If Persistent Agent is not detected when it should be, see KB article FD42350 for troubleshooting steps.

If desired, proceed to Isolate when Agent Communication is Lost.

Isolate When Agent Communication is Lost

1. Configure an Admin Scan to mark hosts At Risk or Safe based on the alarm action triggered by the "Persistent Agent Not Communicating" event. Once isolated, hosts will be redirected to the Agent Download page (defined by the Patch URL). This page contains instructions on how to reinstall the Persistent Agent.

    a. Navigate to **Policy > Remediation Configuration**.

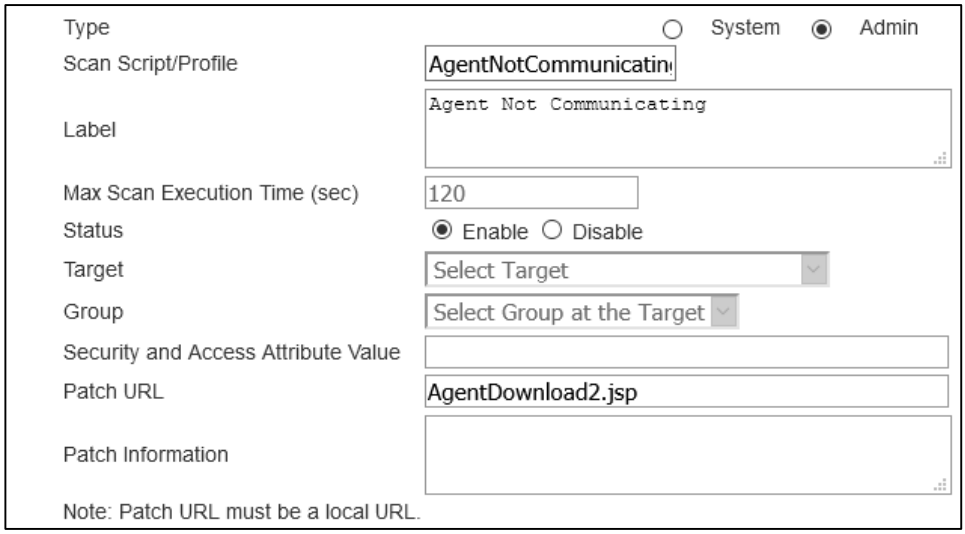
    b. On the Scan Configuration tab, click **Add**.

    c. Configure the Scan using the settings in the table below:

Type	Admin
Scan Script/Profile (Name for the Admin scan)	AgentNotCommunicating
Label (Displayed on the failure page when a network user's PC has failed a scan. If no label is provided, the scan name is used. The label or scan name is a link that takes the user to a page indicating why the PC has failed the scan.)	Agent Not Communicating
Max Scan Execution Time (sec)	120
Status	Enable
Patch URL (Can be found under Remediation/Agent Download in the Portal Configuration Content Editor)	AgentDownload2.jsp

    d. Click **APPLY**.

For more details on this view see Add a scan in the Administration Guide.



2. Review the Agent Download Captive Portal page and modify if necessary.
    a. Navigate to **System > Portal Configuration**.
    b. Under the **Content Editor** tab, expand **Remediation** and click **Agent Download**. The following fields are available:

       Adjust Width
       Window Title: Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
       Left Column Content: Text displayed in the left column of the page.
       Introduction: Introductory text explaining what steps need to be taken.
       Download Link Prefix: Text displayed before the download link.
       Download Link: Text displayed as a link.
       Download Link Suffix: Text displayed after the download link.
       Secondary Text: Text displayed below the Download link Suffix.

    c. Click **Apply**.

For more details on this view see Remediation in the Administration Guide.

3. Modify the alarm to mark the host "At Risk" and place in remediation.
    a. Navigate to **Logs > Event to Alarm Mappings**.
    b. Select the **"**Persistent Agent Not Communicating" alarm and click **Modify**.
    c. Configure the Action alarm using the settings in the table below:

Action	Host Security Action
Primary Task	At Risk

    d. Click **OK**.

4. Create a second alarm action that will trigger when the "Persistent Agent Communication Resumed" event is generated. This event is generated when the Persistent Agent is able to communicate with FortiNAC again. Once the alarm action is triggered, the host will be marked as safe and moved back to the production network.
    a. In **Mappings** screen, click **Add** or select the "Persistent Agent Communication Resumed" alarm and click **Modify**.
    b. Configure the alarm using the settings in the table below:

Trigger Event	Persistent Agent Communication Resumed
Severity	Minor
Trigger Rule	One Event to One Alarm
Action	Host Security Action
Primary Task	Safe

    c. Click **OK**.

For more details on this view see Add or modify alarm mapping in the Administration Guide.

Validate

Agent not communicating after connecting to the network

On a known working host with the Persistent Agent successfully communicating, do the following:

1. Under **Logs > Events & Alarms** click **Alarms**.
2. Next to **Add Filter**, select **Event** from the drop-down menu.
3. Next to **Event**, select **Persistent Agent Not Communicating** from the drop-down menu.
4. Disconnect host from network.
5. Disable the Persistent agent service. For instructions see KB article FD42403 or the Persistent Agent Deployment and Configuration reference manual.
6. Reconnect to network.
7. "Persistent Agent Not Communicating" event is generated.
8. Alarm triggers after the Event Frequency value has been satisfied.
9. Verify alarm notification was received.
10. Under **Users & Hosts > Hosts**, search for the test host.
11. Verify host record is marked At-Risk
12. Under **Adapters**, verify adapter record has been assigned the VLAN used for remediation under the **Access Value** column.
13. Re-enable Persistent Agent service.
14. Agent communicates with FortiNAC.
15. "Persistent Agent Communication Resumed" event is generated and alarm cleared.
16. Host is marked Safe and moved back to production network.

Agent stops communicating while connected to the network

On a known working host with the Persistent Agent successfully communication, do the following:

1. While connected to the network, disable the Persistent agent service.
2. "Persistent Agent Not Communicating" event is generated.
3. Alarm triggers after the Event Frequency value has been satisfied.
4. Host is marked At-Risk and moved to remediation VLAN.
5. Re-enable Persistent Agent service.
6. Agent communicates with FortiNAC.
7. "Persistent Agent Communication Resumed" event is generated and alarm cleared.

Host is marked Safe and moved back to production network.