FIREEYE™

macmon
nac smartly simple

MACMON NAC WHITE PAPER

Connection with FireEye Network Security

Contents

Version: 1.2_en

Introduction

FireEye Network Security helps organizations of all sizes minimize the risk of costly breaches by accurately detecting and immediately stopping advanced, targeted and other evasive attacks hiding in Internet traffic. At the core of FireEye Network Security is the Multi-Vector Virtual Execution™ (MVX) and Intelligence-Driven Analysis (IDA) technologies. MVX is a signature-less, dynamic analysis engine that inspects suspicious objects to identify targeted, evasive and unknown threats. The IDA engines detect and block malicious objects based on machine-, attacker- and victim-intelligence. FireEye provides products and services that protect their customers world-wide against advanced persistent threats in the company network. Their headquarters are located in Milpitas, CA.

Use Cases

FireEye Network Security passes threat information to macmon NAC

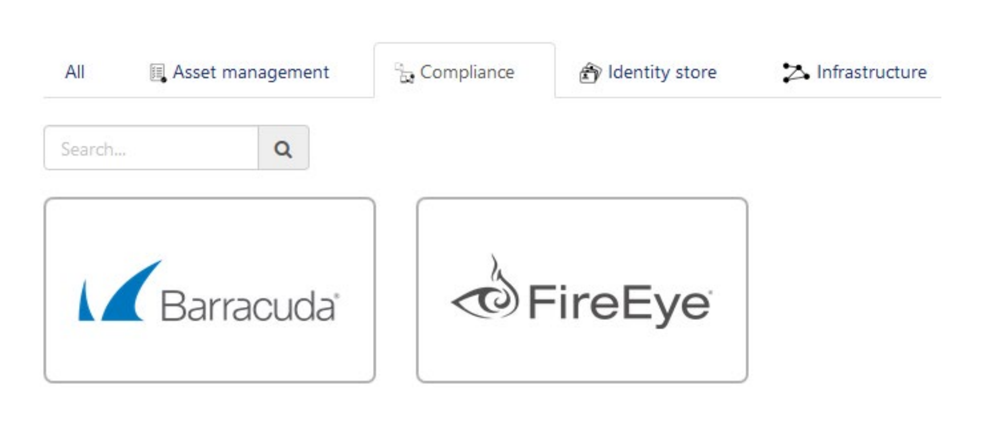
Ransomware can make an administrator's life hard. If a ransomware managed to infect an endpoint despite all security precautions, it's only a matter of seconds to isolate this exact device from the network segment. This prevents the malicious software from spreading over and encrypting other resources available on the network. Using its advanced persistent threat detection engine, FireEye Network Security is capable of detecting a malicious threat in the corporate network within the blink of an eye. The combination of FireEye Network Security and macmon NAC is a powerful combination of threat detection and network enforcement.

macmon NAC enables FireEye Network Security to enforce the compliance status of an endpoint based on its health state determined by FireEye Network Security. This applies to virtually any network you can imagine. In any network you can find devices that potentially are subject to malicious threats. When FireEye Network Security detects such in your network it classifies the malware that was found. It then passes an information message to the compliance interface of macmon NAC that includes information regarding the IP address of the infected system and the name of the malware identified. macmon NAC would extract the information instantly and set the compliance status of said infected device to non-compliant. A pre-set rule then would either isolate the infected device by moving it into remediation VLAN or by physically shutting down the network switch port.

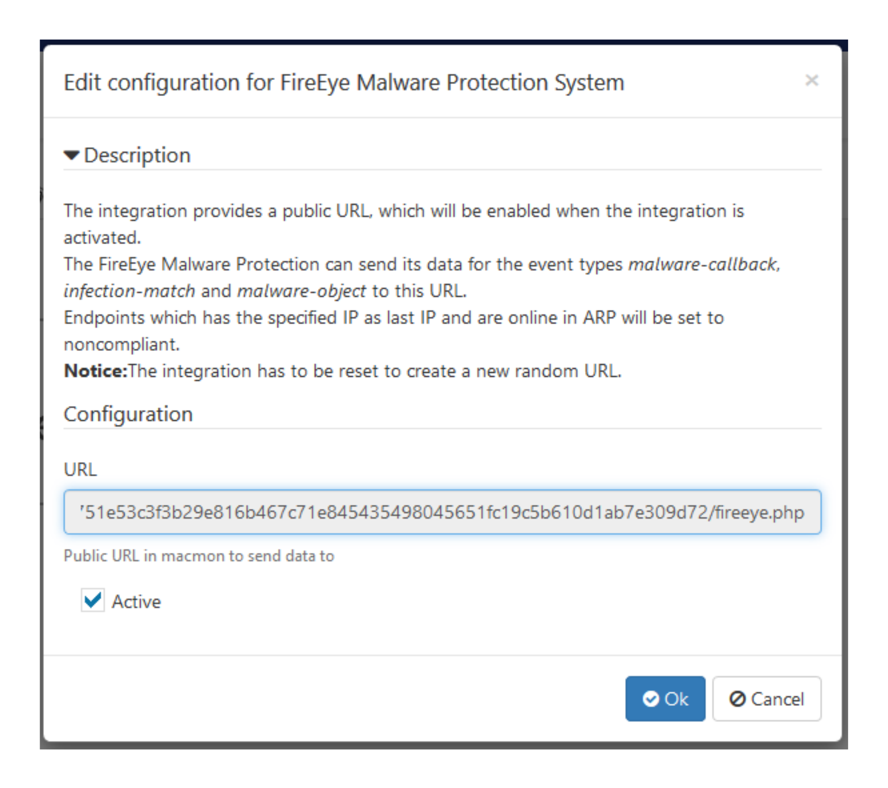
Configuration of macmon NAC

Configuration of the FireEye Network Security integration

The configuration is done via the web GUI. Please tap on *Settings* and *Third party integrations*, then on *Compliance*.



If the border of the FireEye tile appears gray the integration is not yet activated. Please tap on the tile for the configuration dialog to be shown and copy the given URL. You will need this URL when configuring the other part of the integration in the FireEye Network Security web GUI. Please make sure to check the box with the label “Active” and confirm by tapping “Ok”.



Edit configuration for FireEye Malware Protection System ×

▾ Description

The integration provides a public URL, which will be enabled when the integration is activated.
The FireEye Malware Protection can send its data for the event types *malware-callback*, *infection-match* and *malware-object* to this URL.
Endpoints which has the specified IP as last IP and are online in ARP will be set to noncompliant.
Notice: The integration has to be reset to create a new random URL.

Configuration

URL

'51e53c3f3b29e816b467c71e845435498045651fc19c5b610d1ab7e309d72/fireeye.php

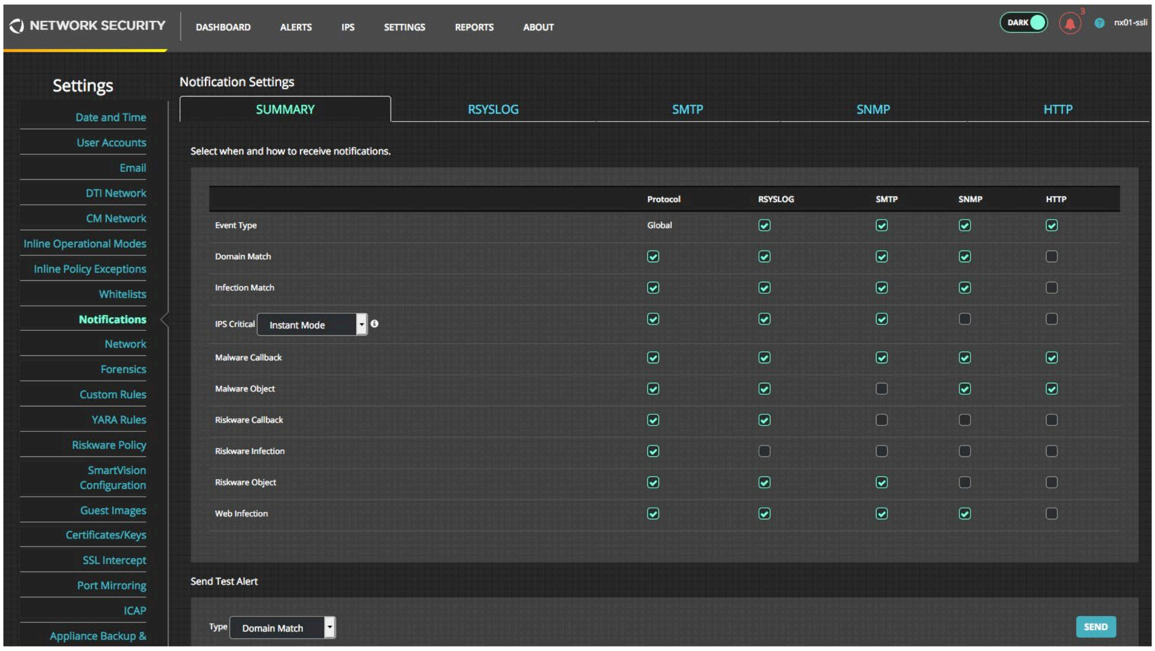
Public URL in macmon to send data to

☑ Active

Configuration of FireEye Network Security

Notification settings

1. Please tap on Settings in the navigation bar above.
2. Then please tap on Notifications in the navigation bar left.
3. For “Malware Callback” and “Malware Object” please check the boxes in the HTTP column.



Notification Settings

Select when and how to receive notifications.

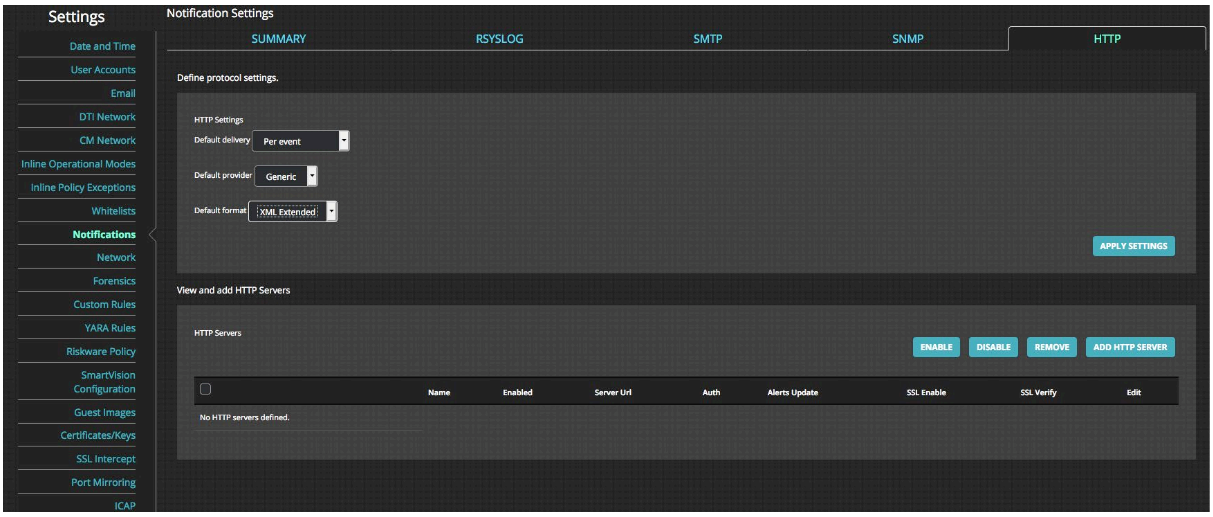
	Protocol	RSYSLOG	SMTP	SNMP	HTTP
Event Type	Global	☑	☑	☑	☑
Domain Match	☑	☑	☑	☑	□
Infection Match	☑	☑	☑	☑	□
IPS Critical Instant Mode	☑	☑	☑	□	□
Malware Callback	☑	☑	☑	☑	☑
Malware Object	☑	☑	□	☑	☑
Riskware Callback	☑	☑	□	□	□
Riskware Infection	☑	□	□	□	□
Riskware Object	☑	☑	☑	□	□
Web Infection	☑	☑	☑	☑	□

Send Test Alert

Type: Domain Match

Adding an HTTP server

1. Afterwards, please tap on the HTTP tab as you can see in the screenshot
2. Then tap on ADD HTTP SERVER in the View and add HTTP Servers section



Notification Settings

Define protocol settings.

HTTP Settings

Default delivery: Per event

Default provider: Generic

Default format: XML Extended

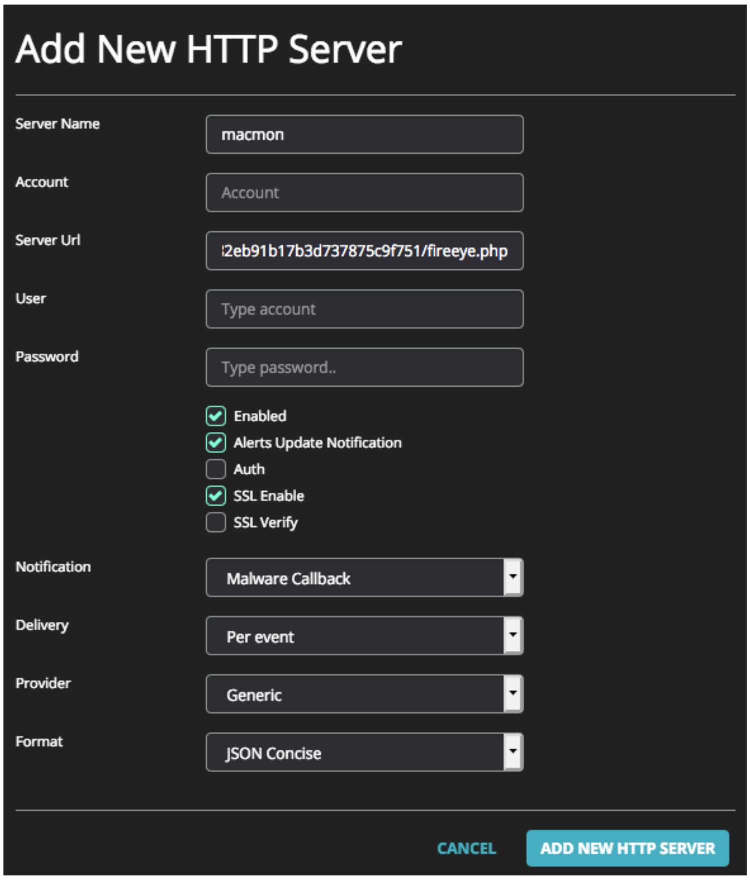
View and add HTTP Servers

HTTP Servers

□	Name	Enabled	Server Url	Auth	Alerts Update	SSL Enable	SSL Verify	Edit
No HTTP servers defined.								

Configuring the connection

1. Please enter a Server Name that suits best to your configuration
2. Please paste the previously copied URL as the Server Url
3. Please check the boxes Enabled, Alerts Update Notification, SSL Enable and in case of using an officially signed certificate on SSL Verify.
4. Please select "Malware Callback" as Notification
5. Please select "Per event" as Delivery
6. Please select "Generic" as Provider
7. Please select "JSON Concise" as Format



Add New HTTP Server

Server Name: macmon

Account: Account

Server Url: 2eb91b17b3d737875c9f751/fireeye.php

User: Type account

Password: Type password..

☑ Enabled
☑ Alerts Update Notification
☐ Auth
☑ SSL Enable
☐ SSL Verify

Notification: Malware Callback

Delivery: Per event

Provider: Generic

Format: JSON Concise

Contact at FireEye

If you've got any questions, please contact FireEye at https://www.fireeye.com/support/contacts.html