



8.3.7.28-8.3.3.9 Manager-M-series Release Notes

McAfee Network Security Platform 8.3

Revision A

Contents

- ▶ *About this release*
- ▶ *New features*
- ▶ *Enhancements*
- ▶ *Resolved issues*
- ▶ *Installation instructions*
- ▶ *Known issues*
- ▶ *Product documentation*

About this release





This document contains important information about the current release. We strongly recommend that you read the entire document.

Network Security Platform follows a new process release 8.2 onwards. The changes in the release process are based on customer requirements, and best practices followed by other McAfee teams. For details, read [KB78795](#).

This release of Network Security Platform is to provide few features and enhancements on the Manager and M-series Sensor software.

| Release parameters | Version |
|---|----------|
| Network Security Manager software version | 8.3.7.28 |
| Signature Set | 8.7.78.7 |
| M-series Sensor software version | 8.3.3.9 |

This version of 8.3 Manager software can be used to configure and manage the following hardware:

| Hardware | Version |
|---|--------------------|
| NS9x00-series Sensors (NS9100, NS9200, NS9300) | 7.1, 8.1, 8.2, 8.3 |
| NS7x00-series Sensors (NS7100, NS7200, NS7300) | 8.1, 8.2, 8.3 |
| NS5x00-series Sensors (NS5100, NS5200) | 8.1 |
|  Sensor software versions 8.2 and 8.3 are currently not available for NS5x00-series. | |
| NS3x00-series Sensors (NS3100, NS3200) | 8.1 |
|  Sensor software versions 8.2 and 8.3 are currently not available for NS3x00-series. | |
| Virtual IPS Sensors (IPS-VM100 and IPS-VM600) | 8.1, 8.2, 8.3 |
| Virtual Security System Sensors (IPS-VM100-VSS) | 8.1 |
|  Sensor software versions 8.2 and 8.3 are currently not available for IPS-VM100-VSS. | |
| M-series Sensors (M-1250, M-1450, M-2750, M-2850, M-2950, M-3050, M-4050, M-6050, M-8000) | 7.1, 8.1, 8.2, 8.3 |
| Mxx30-series Sensors (M-3030, M-4030, M-6030, M-8030) | 7.1, 8.1, 8.2, 8.3 |
| XC Cluster Appliances (XC-640) | 8.1, 8.3 |
|  Sensor software version 8.2 is not available for XC-640 Load Balancers. | |
| XC Cluster Appliances (XC-240) | 7.1, 8.1, 8.2, 8.3 |
| NTBA Appliance software (T-200, T-500, T-600, T-1200, T-VM, T-100VM, T-200VM) | 7.1, 8.1, 8.2, 8.3 |

The above mentioned Network Security Platform software versions support integration with the following product versions:

Table 1-1 Network Security Platform compatibility matrix

| Product | Version supported |
|-------------------------------------|------------------------------|
| McAfee ePO™ | 5.1, 5.3.1 |
| McAfee Global Threat Intelligence™ | Compatible with all versions |
| McAfee Advanced Threat Defense | 3.4.8.96, 3.6.0.25 |
| McAfee Endpoint Intelligence Agent | 2.4, 2.5 |
| McAfee Logon Collector | 2.2, 3.0 |
| McAfee Threat Intelligence Exchange | 1.1.1, 1.2 |
| McAfee Vulnerability Manager | 7.5 |
| McAfee Host Intrusion Prevention | 7.0, 8.0 |

Currently port 4167 is used as the UDP source port number for the SNMP command channel communication between Manager and Sensors. This is to prevent opening up all UDP ports for inbound connectivity from SNMP ports on the sensor. Older JRE versions allowed the Manager to bind to the same source port 4167 for both IPv4 and IPv6 communication. But with the latest JRE version 1.8.0_92, it is no longer possible to do so, and the Manager uses port 4166 as the UDP source port to bind for IPv6.

Manager 8.3 uses JRE version 1.8.0_92 and MySQL version 5.6.30. If you have IPv6 Sensors behind a firewall, you need to update your firewall rules accordingly such that port 4166 is open for the SNMP command channel to function between those IPv6 Sensors and the Manager.



Manager software version 8.3 is not supported on McAfee-built Dell-based Manager Appliances. McAfee recommends that you use Intel-based Manager Appliances instead.

New features

This release of Network Security Platform does not include any new features.

Enhancements

This release of Network Security Platform includes the following enhancement.

Quarantine enhancement

With this release, while adding an endpoint to quarantine manually, the Manager provides additional option to remediate a host to the remediation portal.

In the **Add to Quarantine** window (in **Threat Explorer**, **Callback Activity**, **High-Risk Endpoint**, **Quarantine** and **Attack Log** pages under **Analysis** tab) a new option (checkbox) is included and when selected while adding the host to be quarantined, the host is remediated to the remediation portal.

Further, a new column **Remediate** is added in the **Quarantine** page which indicates whether the remediation is enabled or disabled for the host.

For more details, see *McAfee Network Security Platform Manager Administration Guide*.

Resolved issues

These issues are resolved in this release of the product. For a list of issues fixed in earlier releases, see the Release Notes for the specific release.

Resolved Manager software issues

The following table lists the **high-severity** Manager software issues:

| ID # | Issue Description |
|---------|--|
| 1124002 | In the Attack Log page, while saving the attack log using the Save Attack Log as option, appropriate file extensions do not get associated with the CSV and PDF files. |
| 1120687 | The IP addresses that are quarantined are not displayed in the Quarantine page located at Analysis <Admin Domain Name>. |

The following table lists the **medium-severity** Manager software issues:

| ID # | Issue Description |
|---------|--|
| 1134439 | In the Capture Now page under Devices Devices Troubleshooting Packet Capturing , the Protocol Number field is disabled when Protocol number is selected in the Protocol field. |
| 1133101 | When child domain is selected in the Dashboard tab, navigating to another tab displays the domain as 'parent domain' instead of the 'child domain'. |

| ID # | Issue Description |
|---------|---|
| 1132014 | Policy changes made to an already synchronized policy does not get reflected in the Manager after the next policy synchronization. |
| 1131532 | When syslog fault notifications for a Sensor high-availability cluster are sent from the Manager, the notification contains the cluster name instead of the node name. |
| 1130813 | In the Attack Log page, filtering the Result column with the filter option Attack SmartBlocked does not display the Smart Blocked attacks. |
| 1129730 | Big Movers report does not display any data. |
| 1126359 | Policies from the parent domain are applied to the interfaces in the child admin domain. |
| 1126263 | All the alerts that were displayed in the Attack Log page prior to the Manager upgrade are not displayed after the upgrade. |
| 1126017 | The Manager attempts to connect to the internet to get information about latest versions of signature sets or callback detectors even when <code>iv.isManagerOffLine=TRUE</code> in <code>ems.properties</code> . |
| 1125279 | When the alerts from the Attack Log page are saved either in a PDF or a CSV file, the report does not display attack details. |
| 1125262 | While adding an Ignore Rule for an alert that is generated in the child admin domain, the rule gets created for the parent domain. |
| 1125259 | In Attack Log , Interface Policy for callback detector alerts are not getting updated. |
| 1125258 | In the Attack Log page, JSON parsing error is displayed while updating a policy created in the child admin domain. |
| 1124267 | HTTP 404 error is displayed when saving the settings for the Report Scheduler under Manager <Admin Domain Name> Reporting Report Automation . |
| 1124266 | After upgrade to 8.3, the existing Snort signatures from 8.2 do not appear in the Snort Format tab when you go to Policy <Root Admin Domain> Intrusion Prevention Policy Types PS Policies and click on Custom Attacks . |
| 1124259 | Version information is not displayed for an IPS policy in the Attack Definitions tab. |
| 1124203 | The health check fails when the Last Database Backup checkbox is selected in the Health Check page located at Manager <Admin Domain Name> Troubleshooting Health Check . |
| 1123807 | Apart from displaying the attacks for the selected domain, the Attack Log page also displays the attacks for the domain that is not selected from the resource tree. |
| 1123804 | The list to select admin domain in the resource tree under Analysis , Policy , Devices , and Manager tabs are not displayed in the alphabetical order. |
| 1123312 | GTI IP Exclusion list under Manager Integration GTI fails to update or save correctly. |
| 1097417 | In the Health Check page, the Last Database Backup check runs for a prolonged period without completing the check. |

Resolved Sensor software issues

The following table lists the **medium-severity** Sensor software issues:

| ID # | Issue Description |
|---------|---|
| 1137363 | Establishing MDR between two Managers after resetting to standalone causes the authentication channel to go down in all Sensors. |
| 1122077 | The Sensor is vulnerable to CVE-2015-3197. <code>ssl/s2_srvr.c</code> in OpenSSL 1.0.1 versions prior to 1.0.1r and OpenSSL 1.0.2 versions prior to 1.0.2f do not prevent use of disabled ciphers, making it simpler for man-in-the-middle attackers to overcome cryptographic protection mechanisms by performing computations on SSLv2 traffic. |
| 1121608 | During processing of application based firewalls, the Sensor runs into exception in a rare scenario causing it to switch to layer 2, auto-recover, or reboot based on the auto-recovery settings. |

| ID # | Issue Description |
|---------|---|
| 1117936 | When using Manager version 8.3 and Sensor version 8.2 or lower, the Sensor reboots or auto-recovers when some SNORT rules are matched. |
| 1112442 | When a malware policy is assigned for APK files, the Sensor does not conform to malware confidence score and performs incorrect action. |
| 1112210 | During Snort rule import, Verbose debug messages are displayed in the Sensor log. |
| 1104386 | After multiple successful datapath auto-recoveries, the Sensor M-8000P and M-8000S may get out-of-sync due to internal Sensor resource exhaustion. |
| 1056662 | In a rare scenario, the Sensor detects the attack only for the first packet when it sees multiple duplicated UDP packet in a quick succession and misses the attack detection for the UDP subsequent packets. |




The following table lists the **low-severity** Sensor software issues:

| ID # | Issue Description |
|--------|--|
| 882329 | In a rare scenario, when a non-encrypted flow is received on port 443, the Sensor may fail to raise an alert for that particular flow. |

Installation instructions

Manager server/client system requirements

The following table lists the 8.3 Manager server requirements:

| | Minimum required | Recommended |
|------------------|---|---|
| Operating system | Any of the following: <ul style="list-style-type: none"> Windows Server 2008 R2 Standard or Enterprise Edition, English operating system, SP1 (64-bit) (Full Installation) Windows Server 2008 R2 Standard or Enterprise Edition, Japanese operating system, SP1 (64-bit) (Full Installation) Windows Server 2012 R2 Standard Edition (Server with a GUI) English operating system Windows Server 2012 R2 Standard Edition (Server with a GUI) Japanese operating system Windows Server 2012 R2 Datacenter Edition (Server with a GUI) English operating system Windows Server 2012 R2 Datacenter Edition (Server with a GUI) Japanese operating system  Only X64 architecture is supported. | Windows Server 2012 R2 Standard Edition operating system. |
| Memory | 8 GB  Supports up to 3 million alerts in Solr. | >16 GB  Supports up to 10 million alerts in Solr. |
| CPU | Server model processor such as Intel Xeon | Same |
| Disk space | 100 GB | 300 GB or more |

| | Minimum required | Recommended |
|---------|--|-----------------------|
| Network | 100 Mbps card | 1000 Mbps card |
| Monitor | 32-bit color, 1440 x 900 display setting | 1440 x 900 (or above) |

The following are the system requirements for hosting Central Manager/Manager server on a VMware platform.

Table 5-1 Virtual machine requirements






| Component | Minimum | Recommended |
|------------------|---|---|
| Operating system | Any of the following: <ul style="list-style-type: none"> Windows Server 2008 R2 Standard or Enterprise Edition, English operating system, SP1 (64-bit) (Full Installation) Windows Server 2008 R2 Standard or Enterprise Edition, Japanese operating system, SP1 (64-bit) (Full Installation) Windows Server 2012 R2 Standard Edition (Server with a GUI) English operating system Windows Server 2012 R2 Standard Edition (Server with a GUI) Japanese operating system Windows Server 2012 R2 Datacenter Edition (Server with a GUI) English operating system Windows Server 2012 R2 Datacenter (Server with a GUI) Japanese operating system  Only X64 architecture is supported. | Windows Server 2012 R2 Standard Edition operating system. |
| Memory | 8 GB  Supports up to 3 million alerts in Solr. | >16 GB  Supports up to 10 million alerts in Solr. |
| Virtual CPUs | 2 | 2 or more |
| Disk Space | 100 GB | 300 GB or more |

Table 5-2 VMware ESX server requirements

| Component | Minimum |
|-------------------------|---|
| Virtualization software | <ul style="list-style-type: none"> ESXi 5.1 Update 2 ESXi 5.5 Update 3 ESXi 6.0 Update 1 |
| CPU | Intel Xeon ® CPU ES 5335 @ 2.00 GHz; Physical Processors – 2; Logical Processors – 8; Processor Speed – 2.00 GHz |
| Memory | Physical Memory: 16 GB |
| Internal Disks | 1 TB |

The following table lists the 8.3 Manager client requirements when using Windows 7, Windows 8, or Windows 2012:

| | Minimum | Recommended |
|------------------|---|--|
| Operating system | <ul style="list-style-type: none"> Windows 7, English or Japanese Windows 8, English or Japanese Windows 8.1, English or Japanese Windows 10, English or Japanese <div>  The display language of the Manager client must be the same as that of the Manager server operating system. </div> | |
| RAM | 2 GB | 4 GB |
| CPU | 1.5 GHz processor | 1.5 GHz or faster |
| Browser | <ul style="list-style-type: none"> Internet Explorer 10, 11, or Microsoft Edge Mozilla Firefox Google Chrome (App mode in Windows 8 is not supported.) <div>  To avoid the certificate mismatch error and security warning, add add the Manager web certificate to the trusted certificate list. </div> | <ul style="list-style-type: none"> Internet Explorer 11 Mozilla Firefox 20.0 or later Google Chrome 24.0 or later |

If you are using Google Chrome 42 or later, the NPAPI plug-in is disabled by default, which means that Java applet support is disabled by default. Perform the following steps to enable NPAPI plug-in:

- 1 In the address bar, type `chrome://flags/#enable-npapi`.
- 2 Click the **Enable** link in the **Enable NPAPI** configuration option.
- 3 Click **Relaunch Now** at the bottom of the page to restart Google Chrome for the changes to take effect.

For the Manager client, in addition to Windows 7, Windows 8, and Windows 8.1, you can also use the operating systems mentioned for the Manager server.

The following are Central Manager and Manager client requirements when using Mac:


| Mac operating system | Browser |
|--|---------------|
| <ul style="list-style-type: none"> Yosemite El Capitan | Safari 8 or 9 |

For more information, see *McAfee Network Security Platform Installation Guide*.

Upgrade recommendations

McAfee regularly releases updated versions of the signature set. Note that automatic signature set upgrade does not happen. You need to manually import the latest signature set and apply it to your Sensors.

The following is the upgrade matrix supported for this release:

| Component | Minimum Software Version |
|----------------------------------|---|
| Manager/Central Manager software | <ul style="list-style-type: none">• 7.1 — 7.1.5.14, 7.1.5.15• 8.1 — 8.1.7.73, 8.1.7.82 <div> Manager version 8.1.7.52 is only for 8.1 NS5x00 and NS3x00 Sensors.</div> <ul style="list-style-type: none">• 8.2 — 8.2.7.71, 8.2.7.83• 8.3 — 8.3.7.7 |
| M-series Sensor software | <ul style="list-style-type: none">• 7.1 — 7.1.3.106, 7.1.3.119• 8.1 — 8.1.3.89, 8.1.3.100• 8.2 — 8.2.3.84, 8.2.3.113• 8.3 — 8.3.3.4 |

Known issues

For a list of known issues in this product release, see this McAfee KnowledgeBase article:
Network Security Platform software issues: [KB86387](#)

Product documentation

Every McAfee product has a comprehensive set of documentation.

Find product documentation

- 1 Go to the McAfee ServicePortal at <http://mysupport.mcafee.com> and click **Knowledge Center**.
- 2 Enter a product name, select a version, then click **Search** to display a list of documents.

8.3 product documentation list

The following software guides are available for Network Security Platform 8.3 release:

- Quick Tour
- Installation Guide (includes Upgrade Guide)
- Manager Administration Guide
- Manager API Reference Guide (selective distribution - to be requested via support)
- CLI Guide
- IPS Administration Guide
- Custom Attacks Definition Guide
- XC Cluster Administration Guide
- Integration Guide

- NTBA Administration Guide
- Best Practices Guide
- Troubleshooting Guide

© 2016 Intel Corporation

Intel and the Intel logo are trademarks/registered trademarks of Intel Corporation. McAfee and the McAfee logo are trademarks/registered trademarks of McAfee, Inc. Other names and brands may be claimed as the property of others.