**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 release process starting with the 8.2 release. The changes in the release process are based on customer requirements, and best practices followed by other McAfee teams. For details, read KB78795.

This maintenance release of Network Security Platform is to introduce the integration of Network Security Platform with Intel® Security Controller to deliver IPS service to software-defined data centers (SDDC).

- Network Security Manager software version: 8.2.7.24
- Signature Set: 8.7.45.5
- Virtual Security System software version: 8.1.7.17
- Intel® Security Controller version: 1.0-2031
This version of 8.2 Manager software can be used to configure and manage the following devices also:

- 7.1, 7.5, 8.1 and 8.2 M-series and Mxx30-series Sensors
- 8.1 and 8.2 Virtual IPS Sensors (IPS-VM100 and IPS-VM600)
- 8.1 Virtual Security System Sensors (IPS-VM100-VSS)
- 7.1, 8.1 and 8.2 NS9x00-series (NS9100, NS9200, NS9300) Sensors
- 7.1, 7.5, 8.1 and 8.2 XC Cluster Appliances
- 7.1, 7.5, 8.1 and 8.2 NTBA Appliance software (Physical and Virtual)
- 7.1 I-series Sensors

If you are currently using 8.1.5.x NS7x00 series (such as 8.1.5.39, 8.1.5.57) Sensor software, upgrade to this version of 8.2 NS9x00-series Sensor software is not supported. This version of 8.2 Manager software will not manage the NS7x00 series Sensors.

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 1.7.0_72, it is no longer possible to do so, and the Manager uses port 4166 as the UDP source port to bind for IPv6.

The latest Manager 8.2 uses JRE version 1.7.0_72. 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.

With release 8.1 onwards, Network Security Platform no longer supports the Network Access Control module and N-series Sensors. If you are using Network Access Control with N-series (NAC-only) Sensors, McAfee recommends that you continue to use the 7.1.3.6 version. If you are using the Network Access Control module in M-series Sensors, continue to use the 7.5.3.30 version. That is, you should not upgrade the Manager or the Sensors to 8.1 for such cases.

Manager software version 7.5 and above are 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 includes the following new features:

**Integration with Intel® Security Controller**

Intel® Security Controller is a virtual appliance, which facilitates software-defined security services for software-defined datacenters (SDDC). Intel® Security Controller provides a common set of management services, acting as a broker between the security solutions and the virtual infrastructure.

Consider a VMware-based, large-scale SDDC consisting of hundreds of ESXi hosts aggregated under multiple clusters. Virtualization provides flexibility and agility to its users, wherein they can spin up virtual machines (VMs). Using VMware NSX, users can spin up isolated logical networks as easily as one can spin up VMs. With features such as VMware VMotion, one can move a working VM from one physical ESXi host to another. All these require no changes in the physical networking configuration. When multiple users spin up new networks and move working VMs across physical boxes in such a large-scale datacenter, security is threatened.
To match with the capabilities of virtualization solutions, Intel® Security Controller can seamlessly, non-intrusively, and non-disruptively integrate security services with existing virtualized environments. This enables network security services to keep pace with the speed, agility, and scalability of virtualization features and solutions.

In this release, you can integrate Network Security Platform with Intel® Security Controller to provide next-generation IPS service to virtual networks.

Intel® Security Controller does not take any action directly but orchestrates the required actions by integrating with ESXi, vCenter, NSX, Network Security Manager, and Virtual Security System. When you deploy IPS service, Intel® Security Controller orchestrates the automatic deployment of a Virtual Security System instance in each ESXi host of a protected cluster.

For more details, see Intel® Security Controller 1.0 Product Guide.

With this release, Network Security Platform introduces the Virtual Security System model: IPS-VM100-VSS. A Virtual Security System instance is a virtual IPS Sensor. Functionally, a Virtual Security System instance is to some extent similar to IPS-VM100 Virtual Sensors. However, it varies with respect to deployment method, maintenance, and supported features. When you complete IPS service deployment, Intel® Security Controller orchestrates inline inspection of traffic by the Virtual Security System instances. So, all traffic to and from the protected VMs are inspected for attacks. Even if you migrate a VM to a different ESXi host within the same cluster, the VM is still provided the same IPS service without you having to make any configuration changes.

The IPS-VM100-VSS is similar to the IPS-VM100 Virtual IPS Sensor with respect to Sensor performance and capacity values.

The Virtual Security System software is available only in version 8.1. This release of Network Security Manager 8.2 can manage 8.1 Virtual Security System software.

In the context of IPS service through Intel® Security Controller, you use Network Security Manager to perform the following tasks:

- Define the Manager admin domains, which should manage the Virtual Security System.

- Create a policy group containing the security policies for next-generation IPS. For example, the policy group can contain an IPS policy, Advanced Malware policy, and Firewall policy. When you deploy the IPS service, Intel® Security Controller collaborates with vCenter and NSX to ensure the Virtual Security System instances use the selected policy group for traffic inspection.
  - For a Virtual Security System, the policy assignment is only through a policy group. That is, you cannot assign IPS policy, Firewall policy, and so on separately. To access the Policy Groups page, select Policy | <domain name> | Intrusion Prevention | Objects | Policy Groups. You can assign a policy group to the interfaces and subinterfaces of the regular Sensors as well.
  - For the Virtual Security System, you assign the policy groups that you create in the Manager through the security policies of VMware NSX. That is, you cannot assign the policy group to a Virtual Security System instance or its interface through the Manager.

- Deploy configuration changes, signature sets, and so on for the Virtual Security System instances.

- View details of the deployed Virtual Security System instances. For example, you can view the VMware ESXi servers on which the Virtual Security System instances are installed, the IP addresses of the Virtual Security System instances, and so on.

- View the alert and other details sent by the Virtual Security System instances.

In summary, the following table provides the interoperability versions of the components necessary for the Network Security Platform - Intel® Security Controller integration to work.
IPS features - supported

The following are the list of IPS features supported by Virtual Security Systems in this release:

- Inline fail-open and fail-close are through an NSX mechanism
- To apply the policies, you must use Policy Groups in the Manager
  - IPS policies
  - Advanced Malware policies - except PDF emulation engine
  - Inspection Options policies
  - Connection Limiting policies
  - Firewall policies
- Quarantine (automatic, through IPS policies as well as manual from the Real-time Threat Analyzer). In addition, quarantine through security tags of NSX is also supported.
- Snort custom attack definitions
- McAfee custom attack definitions
- Protection of Web application servers
- Advanced Traffic Inspection
- Layer 2 passthru mode is supported but implemented differently when compared to physical Sensors
- Layer 7 data collection
- MPLS traffic inspection
- IPv6 traffic inspection
- HTTP response scanning
- Inspection of double VLAN tagged traffic
- Monitoring Sensor performance
- Synchronization of Sensor clock using an NTP server
- Display Sensor CLI audit log events in the Manager
- TACACS+ user in audit logs
- Secure Transfer of Files from Sensor CLI
- Application Identification and Visualization
- Advanced Traffic inspection
• SmartBlocking of attacks including use of IP Reputation to augment SmartBlocking
• Integration with McAfee GTI for IP reputation and file reputation. This includes protection from high-risk hosts.
• Inspection of X-Forwarder-For Header Information. Reputation lookup and quarantine of client IP addresses in the XFF header.
• Layer 7 Data Collection
• Stateless Firewall access rules
• Granular access control for CLI commands (for TACACS users)
• Advanced botnet detection including Bot Command and Control server activity detection
• Web server protection against DoS attacks
• Integration with McAfee Endpoint Intelligence Agent (McAfee EIA)
• Sensor autorecovery

**IPS features - not supported**
The following are the list of IPS features not supported by Virtual Security Systems in this release:
• Monitoring and response ports are not applicable
• SPAN and tap modes are not relevant. Only inline mode is supported. You configure inline fail-open and fail-close modes not on the Sensor but through an NSX mechanism.
• Sensor failover is not supported
• SSL decryption
• Jumbo frames
• Capture data packets (packet capture)
• Hitless reboot
• VLAN bridging
• ARP spoofing protection
• SYN cookie protection
• DNS spoof protection feature
• Advanced Malware policies - PDF emulation engine
• Traffic normalization is not applicable on the NSX platform due to NSX filtering out packets and not sending packets that violate protocols to the Virtual Security System instance
• Simulated blocking
• Latency monitor
• Traffic prioritization
• IP fragmentation flood
• Inspection of tunneled traffic including GRE tunneled traffic
• Passive device profiling
• Attacks using evasion techniques - some of the attacks might not be detected
• MDR
• Virtualization of monitoring ports using VLANs and CIDRs (VIDS) is through Security Group-Service Profile based VIDs
• IP spoofing protection
• IPv6 support for the management port
• Netflow export to NTBA
• Quality of Service (QoS) policies

Enhancements
This release of Network Security Platform does not include any enhancements.

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 medium-severity Manager software issues:

<table>
<thead>
<tr>
<th>ID #</th>
<th>SR#</th>
<th>Issue Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1026537</td>
<td>4-7704677951</td>
<td>After upgrading to version 8.2, the pre-existing configuration for &quot;Layer 7 DoS protection for web servers&quot; stopped working.</td>
</tr>
<tr>
<td>1019704</td>
<td>4-6813974203</td>
<td>The Manager displays incorrect Password Expiration messages.</td>
</tr>
</tbody>
</table>

Resolved Virtual Security System software issues
This is the first release of Virtual Security System. Hence, there are no resolved issues.

Resolved Intel® Security Controller software issues
This is the first release of Intel® Security Controller. Hence, there are no resolved issues.
Installation instructions

Manager server/client system requirements

The following table lists the 8.2 Manager server requirements:

<table>
<thead>
<tr>
<th>Minimum required</th>
<th>Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating system</td>
<td>Any of the following:</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2008 R2 Standard or Enterprise Edition, SP1 (Full Installation), English operating system 32-bit or 64-bit</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2008 R2 Standard or Enterprise Edition, SP1 (Full Installation), Japanese operating system 32-bit or 64-bit</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2012 R2 Standard Edition (Server with a GUI) English operating system</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2012 R2 Standard Edition (Server with a GUI) Japanese operating system</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2012 R2 Datacenter Edition (Server with a GUI) English operating system</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2012 R2 Datacenter Edition (Server with a GUI) Japanese operating system</td>
</tr>
</tbody>
</table>

Only X64 architecture is supported.

<table>
<thead>
<tr>
<th>Memory</th>
<th>8 GB</th>
<th>8 GB or more</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>Server model processor such as Intel Xeon</td>
<td>Same</td>
</tr>
<tr>
<td>Disk space</td>
<td>100 GB</td>
<td>300 GB or more</td>
</tr>
<tr>
<td>Network</td>
<td>100 Mbps card</td>
<td>1000 Mbps card</td>
</tr>
<tr>
<td>Monitor</td>
<td>32-bit color, 1440 x 900 display setting</td>
<td>1440 x 900 (or above)</td>
</tr>
</tbody>
</table>

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

7
### Table 5-1 Virtual machine requirements

<table>
<thead>
<tr>
<th>Component</th>
<th>Minimum</th>
<th>Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating system</td>
<td>Any of the following:</td>
<td>Windows Server 2012 R2 Standard Edition operating system.</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2008 R2 – Standard or Enterprise Edition with SP1 English operating system 32-bit or 64-bit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2008 R2 – Standard or Enterprise Edition with SP1 Japanese operating system 32-bit or 64-bit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2012 R2 Standard Edition (Server with a GUI) English operating system</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2012 R2 Standard Edition (Server with a GUI) Japanese operating system</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2012 R2 Datacenter Edition (Server with a GUI) English operating system</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2012 R2 Datacenter (Server with a GUI) Japanese operating system</td>
<td></td>
</tr>
<tr>
<td></td>
<td>i Only X64 architecture is supported.</td>
<td></td>
</tr>
<tr>
<td>Memory</td>
<td>8 GB</td>
<td>8 GB or more</td>
</tr>
<tr>
<td>Virtual CPUs</td>
<td>2</td>
<td>2 or more</td>
</tr>
<tr>
<td>Disk Space</td>
<td>100 GB</td>
<td>300 GB or more</td>
</tr>
</tbody>
</table>

### Table 5-2 VMware ESX server requirements

<table>
<thead>
<tr>
<th>Component</th>
<th>Minimum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtualization software</td>
<td>• ESXi 5.0</td>
</tr>
<tr>
<td></td>
<td>• ESXi 5.1</td>
</tr>
<tr>
<td></td>
<td>• ESXi 5.5</td>
</tr>
<tr>
<td>CPU</td>
<td>Intel Xeon® CPU ES 5335 @ 2.00 GHz; Physical Processors – 2; Logical Processors – 8; Processor Speed – 2.00 GHz</td>
</tr>
<tr>
<td>Memory</td>
<td>Physical Memory: 16 GB</td>
</tr>
<tr>
<td>Internal Disks</td>
<td>1 TB</td>
</tr>
</tbody>
</table>

The following table lists the 8.2 Manager client requirements when using Windows 7, Windows 8, or Windows 2012:

<table>
<thead>
<tr>
<th>Minimum</th>
<th>Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating system</td>
<td>• Windows 7 English or Japanese</td>
</tr>
<tr>
<td>• Windows 8 English or Japanese</td>
<td>• Windows 8.1 English or Japanese</td>
</tr>
<tr>
<td>The display language of the Manager client must be same as that of the Manager server operating system.</td>
<td></td>
</tr>
<tr>
<td>RAM</td>
<td>2 GB</td>
</tr>
</tbody>
</table>
**Minimum** | **Recommended**
---|---
CPU | 1.5 GHz processor | 1.5 GHz or faster
Browser | • Internet Explorer 9, 10 or 11  
• Mozilla Firefox  
• Google Chrome (App mode in Windows 8 is not supported) | • Internet Explorer 11  
• Mozilla Firefox 20.0 or above  
• Google Chrome 24.0 or above

Add the Manager web certificate to the trusted certificate list to avoid the certificate mismatch error and security warnings.

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 table lists the 8.2 Central Manager / Manager client requirements when using Mac:

<table>
<thead>
<tr>
<th>Mac operating system</th>
<th>Browser</th>
</tr>
</thead>
</table>
| • Lion  
• Mountain Lion | Safari 6 or 7 |

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

**Virtual Security System**

See the *Intel® Security Controller 1.0 Product Guide* for information on how the Virtual Security System instances are deployed.

**Intel® Security Controller**

See the *Intel® Security Controller 1.0 Product Guide* for information on how to install the Intel® Security Controller virtual appliance.

**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:

<table>
<thead>
<tr>
<th>Component</th>
<th>Minimum Software Version</th>
</tr>
</thead>
</table>
| Manager/Central Manager software | • 7.1 — 7.1.3.5, 7.1.5.7, 7.1.5.10, 7.1.5.14, 7.1.5.15  
• 7.5 — 7.5.3.11, 7.5.5.6, 7.5.5.7, 7.5.5.10  
• 8.1 — 8.1.3.4, 8.1.3.6, 8.1.7.5, 8.1.7.12  
• 8.2 — 8.2.7.5 |
| Virtual Security System (IPS-VM100-VSS) | This is the first release of IPS-VM100-VSS, and upgrade is currently not applicable. |
| Intel® Security Controller | This is the first release of Intel® Security Controller, and upgrade is currently not applicable. |
Known issues

For a list of known issues in this product release, see this McAfee KnowledgeBase article:
Network Security Platform software issues: KB83288

Product documentation

Every McAfee product has a comprehensive set of documentation.

Find product documentation

2. Enter a product name, select a version, then click Search to display a list of documents.

8.2 product documentation list

The following software guides are available for Network Security Platform 8.2 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