Release Notes

McAfee Cloud Workload Security 5.0.0

Contents
- About this release
- What's new
- Installation information
- Known issues
- Additional information
- Getting product information by email
- Where to find product documentation

About this release
This document contains important information about the current release. We recommend that you read the whole document.

We do not support the automatic upgrade of a pre-release software version. To upgrade to a production release of the software, you must first uninstall the existing version.

What's new
The current release of the product includes these enhancements and changes.

Card based user interface for improved usability
The Cloud Workload Security console displays instance details in card based panes. You can manage your instances from a single user interface. You can pivot in to issues, discover, and remediate them in few clicks.
Activate McAfee Adaptive Threat Protection

In addition to McAfee products, you can install McAfee Endpoint Security Adaptive Threat Protection (ATP) on your instances. You can protect your instances from zero day malware using Adaptive Threat Protection.

Activate Network Intrusion Prevention

You can protect your instances from network threats by installing Network Intrusion Prevention. You can view the number of inbound and outbound internal connections, and suspicious and malicious external connections to and from your instances.

Install license extension to enable advanced security features

In addition to installing appropriate extensions for public cloud, private cloud, or hybrid cloud variants to support your cloud vendor accounts, you can install the license extension for Cloud Workload Security. You must install the license extension to enable traffic discovery, traffic assessment, traffic visualization, and Network Security Manager (NSM) account registration.

View traffic details for Microsoft Azure instances

You can view traffic details for your Microsoft Azure instances in the Cloud Workload Security console.

View traffic flow logs

The Cloud Workload Security traffic card has filters to view the flow logs based on time intervals. The traffic card has filters to display inbound traffic, outbound traffic, and blocked connections. In addition to the filters, you can view the direction of traffic for the selected instance and take remediation measures.

Perform DAT assessment

Cloud Workload Security performs DAT assessment for all workloads older than a week. You can view the DAT assessment details for your instances in System Details and pivot table.

System card filters

You can view your accounts and workloads based on Workload Group and Account using the View and By filters in the Systems card.

Improved tagging

Your instances are tagged automatically based on account name and platform name when you register your cloud account. In addition to auto tagging, Cloud Workload Security allows you to create custom tags for your instances. You can create tags for a single instance or bulk tag various instances.

Summary card

You can view the total number of running workloads, compliance events, and threat events in the Cloud Workload Security Summary card. The events are color coded to indicate high and medium risks.

Improved pivot table

In addition to the filters present in the Summary card pivot table like Issues, Workloads, and View, you can view tag details and product details for your instances using the Tag and Product filters. You can also filter your instances based on keywords.

Deploy NSP probe

After registering your NSM account, you can protect your instances by deploying vNSP probe on your cloud infrastructure.
Change Assessment Policy at account level and workload level
You can now create or select assessment policies for accounts and workloads without going to System Tree. You can select any existing assessment policy or create your own policy while registering your cloud accounts. You can also create or select assessment policies from the Workload Details pane for one or multiple instances.

Set AWS and Azure privileges
You can set three levels of user privileges for your AWS and Microsoft Azure cloud accounts. Cloud Workload Security discover workloads, discover traffic, and remediate security groups based on the selected privilege.

Product upgrade
You can upgrade Cloud Workload Security 4.5.1 to Cloud Workload Security 5.0.0 with the required extensions. We recommend upgrading your existing McAfee ePolicy Orchestrator (McAfee ePO) version to 5.3.3, or 5.9 (EPO590HF1208662).

You cannot upgrade Cloud Workload Security 4.0.0 to 5.0.0 directly. You must upgrade the 4.0.0 version to 4.5.1, and then upgrade it to 5.0.0.

Installation information
Common UI Core 1.3 extension must be installed on McAfee ePO to install Cloud Workload Security. For detailed information about installing Cloud Workload Security, see the Cloud Workload Security Installation Guide.

For information about using the product, see the Cloud Workload Security Product Guide.

Known issues
For a list of known issues in this product release, see the McAfee Knowledge Base article: KB90035.

Additional information
Cloud Workload Security is packaged in public, hybrid, and private variants to support different cloud vendor accounts.

<table>
<thead>
<tr>
<th>Packages</th>
<th>Support for vendor accounts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud Workload Security for Private cloud</td>
<td>VMware vSphere</td>
</tr>
<tr>
<td>Cloud Workload Security for Hybrid cloud</td>
<td>VMware vSphere, AWS, and Microsoft Azure</td>
</tr>
<tr>
<td>Cloud Workload Security for Public cloud</td>
<td>AWS and Microsoft Azure</td>
</tr>
</tbody>
</table>

Cloud Workload Security is included in these McAfee suites.

<table>
<thead>
<tr>
<th>Suite</th>
<th>Cloud Workload Security package</th>
</tr>
</thead>
<tbody>
<tr>
<td>McAfee Public Cloud Server Security Suite</td>
<td>Cloud Workload Security for Public cloud</td>
</tr>
<tr>
<td>McAfee Server Security Suite Advanced</td>
<td>Cloud Workload Security for Hybrid cloud</td>
</tr>
<tr>
<td>McAfee Server Security Suite Essentials</td>
<td>Cloud Workload Security for Hybrid cloud</td>
</tr>
<tr>
<td>McAfee Security Suite for Virtual Desktop Infrastructure</td>
<td>Cloud Workload Security for Private cloud</td>
</tr>
</tbody>
</table>

Cloud Workload Security includes these extensions and their versions for this release.
<table>
<thead>
<tr>
<th>Extension</th>
<th>Cloud Workload Security 5.0.0 Release Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>MDCC</td>
<td>5.0.0.193</td>
</tr>
<tr>
<td>Data Center Metering</td>
<td>4.0.0.153</td>
</tr>
<tr>
<td>Data Center Visualization</td>
<td>5.0.0.271</td>
</tr>
<tr>
<td>Data Center Assessment</td>
<td>5.0.0.202</td>
</tr>
<tr>
<td>CWS Azure RM Connector</td>
<td>5.0.0.153</td>
</tr>
<tr>
<td>CWS AWS Connector</td>
<td>5.0.0.159</td>
</tr>
<tr>
<td>CWS vSphere Connector</td>
<td>5.0.0.145</td>
</tr>
<tr>
<td>Data Protection for Cloud (DPC)</td>
<td>4.5.0.118.2</td>
</tr>
<tr>
<td>CWS_LIC</td>
<td>5.0.0.102</td>
</tr>
</tbody>
</table>

**Getting product information by email**

The Support Notification Service (SNS) delivers valuable product news, alerts, and best practices to help you increase the functionality and protection capabilities of your McAfee products.

To receive SNS email notices, go to the SNS Subscription Center at https://sns.secure.mcafee.com/signup_login to register and select your product information options.

**Where to find product documentation**

Go to docs.mcafee.com to find the product documentation for this product.

Go to support.mcafee.com to find supporting content on released products, including technical articles.

Copyright © 2017 McAfee, LLC

McAfee and the McAfee logo are trademarks or registered trademarks of McAfee, LLC or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others.