This document provides information about the new features and enhancements in McAfee® Firewall Enterprise Control Center version 5.3.0.

The 5.3.0 release is based on McAfee Linux Operating System (MLOS) server 2.1.0 64-bit version.

See the McAfee Firewall Enterprise Control Center Installation and Migration Guide, version 5.3.0 for more details.

About this release

McAfee Firewall Enterprise Control Center (Control Center) version 5.3.0 provides support for McAfee Firewall Enterprise version 8.3.0 and earlier (8.x.x and 7.0.1.xx).


Compatible McAfee products

For the latest information about the McAfee firewall products and versions that interoperate with Control Center, see KnowledgeBase article KB67462.

Additional information

Use the listed resources to find additional information.
Table 1  Product resources

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Help</td>
<td>Help is built into the Control Center Client application and the Initialization Tool. Press F1 from a specific window or page or click ? on the title bar.</td>
</tr>
</tbody>
</table>
| McAfee Technical Support ServicePortal | Visit mysupport.mcafee.com to find:  
• Product announcements  
• Product documentation  
• KnowledgeBase  
• Technical support |
| Product updates | Visit go.mcafee.com/goto/updates to download the latest McAfee Firewall Enterprise Control Center patches. |

New features and enhancements

These are the new features and enhancements included in the Control Center 5.3.0 release.

Firewall features supported by Control Center

Control Center 5.3.0 supports these Firewall Enterprise 8.3.0 features:

- **SPAN mode** — You can enable SPAN mode on firewalls to passively analyze network traffic without disrupting the existing network. Firewall Enterprise connects to the switch’s SPAN port, analyzes two-way traffic, and uses output data to generate audits and reports for users like McAfee® Logon Collector, Host Agent, Geo-Location, and Threats (IPS).

- **Host firewall interlock** — When you enable McAfee® Network Integrity Agent on a host endpoint, the agent collects host details like applications and user name. Firewall Enterprise uses this host data for identity control, auditing, reporting, and decision making for updating policies.

- **CloudShield** — Control Center can manage and support firewalls that are deployed on the CloudShield CS-4000 platform to provide maximum security for high-assurance environments.

Firewall Enterprise ePolicy Orchestrator extension

Administrators can configure managed firewalls at version 8.3.0 and later to report firewall and host information to McAfee® ePolicy Orchestrator®. See the McAfee Firewall Enterprise ePolicy Orchestrator Extension Integration Guide, version 5.3.0 for more information.

Real-time audit from firewalls

Administrators can view real-time audit from one or multiple firewalls. A maximum of eight firewalls can be selected to view real-time audit. Use the filters on the Firewall Audit window to filter the real-time data. You can view and export the audits. Two client applications cannot view real-time audit from the same set of firewalls (one or more) simultaneously.

- Real-time audit is supported only on firewall version 8.3.0 and later.
- The selected firewall must be registered with Control Center.
**Demo mode**

Demo mode enables you to evaluate Control Center and experience the management console. In demo mode, Control Center demonstrates key features even if no real firewall exists. These are the benefits of demo mode:

- Ease of evaluation
- Test key features
- Create VMware images for distribution — You can manually generate VMware images of the Control Center Management Server. These files can be played on a VMware Player, in turn creating a local instance of the virtual Control Center Management Server. A Control Center client can connect to the virtual Control Center Management Server and allow you to evaluate the features.
- Capture demo data from a real firewall — Control Center uses prestored firewall configuration and reports in demo mode. When a firewall is added, this default configuration (static data) is used for retrieval and reports. In demo mode, you can capture data from a real firewall (demo data), replace static data, and use demo data for retrieval and reports.

In demo mode, you can view prepopulated objects, policies, dashboards, and reports.

**Summary report**

Administrators can view an improved Summary report of the top applications, threats, users, and source and destination geo-locations and IP addresses. The Dashboard | Summary page displays 20 firewall reports under seven categories. The reports allow you to drill down data, view audit logs, and get specific details.

Benefits of the Summary report include better operation, use in forensics, and ease of use. The category reports have pre-filters that enable you to select a variable and view corresponding audits.

**Client application experience**

This release includes these usability improvements:

Monitor | Alerts — This tab and options are simplified for ease of use.

- The Alert pop-up window allows you to enable or disable the pop-ups. The window also allows you to view, acknowledge, or unacknowledge alerts.
- The Alert browser is re-organized to simplify configuration.
- The Alert browser allows you to search for alerts based on search criteria.
- You can select one or more alerts, and create and audit query for these alerts.

**Stability and performance improvements**

This release includes various stability and performance improvements.

**Resolved issues**

These issues are resolved in this release.

1 **Performance** — If the number of rules is high and there are lot of associated firewalls, the Merge Wizard is slow.

2 **Scalability** — As the number of firewalls and rules increase, the database gets loaded and restarts when you perform an Apply action on the firewalls.
Known issues

For known issues in this product release, refer to KnowledgeBase article KB76039.

Installation and upgrade

You can install Control Center on a standard or virtual appliance. You can upgrade from Control Center version 5.2.x to 5.3.0 for these appliances.

McAfee Firewall Enterprise ePolicy Orchestrator extension version 5.3.0 can work only with Control Center version 5.3.0, as the open SSL upgrade to version 101c does not support older SSL-compatible layered security communication channels.

See the McAfee Firewall Enterprise Control Center Installation and Migration Guide for more details.

Hardware appliance requirements

Before you install 5.3.0, make sure the Control Center Client application and Management Server requirements are met.

Client application requirements

The computer that hosts the Control Center Client application must meet these requirements.
Table 2  Client application minimum requirements

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating system</td>
<td>One of the following Microsoft operating systems:</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2008</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2003</td>
</tr>
<tr>
<td></td>
<td>• Windows 7</td>
</tr>
<tr>
<td></td>
<td>• Windows Vista</td>
</tr>
<tr>
<td></td>
<td>• Windows XP Professional with SP2 or later</td>
</tr>
<tr>
<td>Web browser</td>
<td>One of the following:</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Internet Explorer, version 6 or later</td>
</tr>
<tr>
<td></td>
<td>• Mozilla Firefox, version 1.0 or later</td>
</tr>
<tr>
<td>Hardware</td>
<td>• 3.0 GHz Intel Pentium 4 processor or higher</td>
</tr>
<tr>
<td></td>
<td>• System memory</td>
</tr>
<tr>
<td></td>
<td>• Windows Server or Windows XP — 3 GB (2 GB minimum)</td>
</tr>
<tr>
<td></td>
<td>• Windows Vista or Windows 7 — 4 GB (3 GB minimum)</td>
</tr>
<tr>
<td></td>
<td>• 150 MB of available disk space</td>
</tr>
<tr>
<td></td>
<td>• CD drive</td>
</tr>
<tr>
<td></td>
<td>• Network card (with access to network hosting the Management Server)</td>
</tr>
<tr>
<td></td>
<td>• USB port (for USB drive)</td>
</tr>
<tr>
<td></td>
<td>• USB drive formatted in MS-DOS (hereinafter configuration USB drive)</td>
</tr>
<tr>
<td></td>
<td>You must provide a configuration USB drive; the USB drive provided by McAfee</td>
</tr>
<tr>
<td></td>
<td>cannot be used to store the configuration file.</td>
</tr>
<tr>
<td></td>
<td>• 1280 x 1024 display (1024 x 768 minimum)</td>
</tr>
<tr>
<td></td>
<td>• Keyboard</td>
</tr>
<tr>
<td></td>
<td>• Network cables</td>
</tr>
</tbody>
</table>

Management Server requirements

Control Center 5.3.0 uses the McAfee® Linux Operating System 2.1.0 64-bit version (hereinafter MLOS).

These requirements are applicable to both physical and virtual appliances. See the McAfee Firewall Enterprise Control Center Installation and Migration Guide for more details.
Table 3  Management Server minimum requirements

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirements</th>
</tr>
</thead>
</table>
| Hardware  | • Any server-class type hardware. Examples:  
• Dell R910  
• Dell R610  
• System memory — 2 GB |
| VMware    | • Hard drive — 150 GB (Thick Provisioning)  
   - For a VMDK installation, we recommend you to select thin provisioning.  
   • Guest operating system — RHEL 5 (64 bit)  
   • Enable Virtual Technology (VT) in BIOS  
   • ESXi Server  
   • Version 4.1.0 update 2  
   • Version 5.0.0 update 1 |

Find product documentation

McAfee provides the information you need during each phase of product implementation, from installation to daily use and troubleshooting. After a product is released, information about the product is entered into the McAfee online KnowledgeBase.

Task

2. Under Self Service, access the type of information you need:

<table>
<thead>
<tr>
<th>To access...</th>
<th>Do this...</th>
</tr>
</thead>
</table>
| User documentation | 1 Click Product Documentation.  
2 Select a product, then select a version.  
3 Select a product document. |
| KnowledgeBase | • Click Search the KnowledgeBase for answers to your product questions.  
• Click Browse the KnowledgeBase for articles listed by product and version. |