

# McAfee Embedded Security

## McAfee Whitelisting Technology



### Features

- Low overhead because dynamic whitelisting eliminates manual effort
- Low impact on system performance
- Low CPU and memory requirements
- Low ownership costs result from no-need-to-manage as long as devices are operating well

#### Key feature 1: Application Control

- Protects against zero-day-attack
- Only authorized software is allowed to run
- Prevents all unauthorized applications from being executed
- Makes sure the machine does what it should do
- Automatically accepts new software added through authorized process

#### Key feature 2: Change Control

- Sets access rights for who or which application can access protected data
- Prevents outages resulting from unplanned changes

#### Key feature 3: ePolicy Orchestrator

- Fast time to remote deployment/configuration
- Reporting
- Central management
- Compliance requirements
- Monitors data of managed clients

## Introduction

McAfee Embedded Security Solution is ideal for protecting systems that are fixed-function in terms of CPU or memory resources. Its low overhead does not impact system performance, requires very low initial and ongoing operational overhead, and is equally effective in standalone mode without network access. We provide four different combinations to satisfy different embedded industry needs.

### Package 1: McAfee Application Control (MAC) without ePO

McAfee Application Control, protects your system by only allowing authorized code to run. It automatically creates a dynamic whitelist of the “authorized code” on the embedded system. Once the whitelist is created and enabled, the system is locked down to the known good baseline; no program or code outside the authorized set can run.

### Package 2: McAfee Application Control (MAC) with ePO

With all the functions of Package 1(MAC without ePO), McAfee Application Control with ePolicy Orchestrator centrally manages all McAfee products through remote deployment, remote configuration and report generation. It effectively saves management costs for users who have more than one device with installed McAfee.

### Package 3: McAfee Embedded Control (MEC)

McAfee Embedded Control combines the functions of application control and change control (i.e., it includes all the functions of package 1 (MAC without ePO), plus the function of change control). With a dynamic whitelist of “authorized code”, the system is locked down to the known good baseline; no program or code outside the authorized set can run, and no unauthorized changes can be made. It blocks unauthorized changes to critical system files, directories, and configurations. It allows you to enforce change-control processes by specifying the authorized means of making changes. You may control who can apply changes, which certificates are required to allow changes, what may be changed (for example, you can restrict changes to certain files or directories), and when changes may be applied (for example, update windows might only be opened during a certain time in the week).

### Package 4: McAfee Integrity Control (MIC)

McAfee Integrity Control combines application control, change control plus ePolicy Orchestrator (i.e. with all the functions of Package 3 (MEC), and adds in the function of ePolicy Orchestrator). McAfee Integrity Security unifies the management of endpoints, networks, data, and compliance for all the McAfee products. More than remote deployment, remote configuration, and reports generated, McAfee Integrity Control monitors who read and changed protected data, and when, while streamlining the implementation of compliance measures. It effectively saves management costs for users who have more than one device with McAfee installed.

## Feature details

### 1. Low Overhead

McAfee Embedded Security Solution is a low-overhead software solution.

- Easy setup and low initial and ongoing operational overhead
- Minimal impact on CPU cycles, and uses less than 10 MB of RAM
- No file system scanning that could impact system performance
- Designed to work in connected and in offline modes
- Requires no signature updates

### 2. Application Control

Application Control helps provide protection against any existing and unknown, zero-day polymorphic threats via malware such as worms, viruses, Trojans, buffer-overflow threats, etc., thereby ensuring that the operating device is secure and cannot be compromised. It also helps eliminate emergency patching, reduces number and frequency of patching cycles, and enables more time for testing before patching. It also reduces any security risk on difficult-to-patch devices that are remote and distributed in areas with little or no local support. The Application Control feature helps reduce costs of operations by reducing both planned patching and unplanned recovery downtime, thereby increasing device availability. This turns out to be an ideal solution, especially for lower end devices as it reduces the support costs by reducing number of touch points needed.

### 3. Change Control

Change Control allows you to prevent reading/changes to the file system registry. You can view details of who made changes, which files were changed, and when and how the changes were made. You can write-protect critical files and registry keys from unauthorized tampering. You can read-protect sensitive files. To ease maintenance, you can define trusted programs or users to allow updates to protected files and registry keys.

Real-time visibility for changes made across all systems is the foundation of the Change Control product framework. It provides real-time change tracking with minimal consumption of CPU, memory, disk, and network resources. It comprehensively logs all change attempts made to files and Windows registry keys on the target systems.

### 4. ePolicy Orchestrator

ePolicy Orchestrator is a complete management software for Intel® Security/McAfee products. It helps McAfee Application Control do central management by remote deployment/configuration and reporting.

In McAfee Integrity Control, with ePolicy Orchestrator, file content changes can be viewed and compared side-by-side to see what was added, deleted, or modified. This is handy while troubleshooting configuration-related outages. ePolicy Orchestrator in McAfee Integrity Control may also be utilized to ensure that the control requirements are met for PCI, FDA, HIPAA, and other regulatory mandates. It provides the necessary tamperproof audit logs on the device to prove that regulatory controls are in place.

## Specifications

### Supported OSs

#### ▪ Windows 32-bit

Windows XP, Windows 2003, Windows 2003 R2, Windows 2008, Windows XPE, Windows Embedded Point of Service (WEPOS), POS Ready 2009, WES 2009, Windows Vista, Windows 7, Windows 7 Embedded, Windows 8 (Pro and Enterprise), Windows 8 - based tablets (32-bit only), Windows 8.1 - based tablets (32-bit only)

#### ▪ Windows 64-bit

Windows XP (x86-64/AMD64), Windows 2003 (x86-64/IA64/AMD64), Windows Vista (x86-64/AMD64), Windows 7 (x86-64/AMD64), Windows 2008 Server (x86-64/AMD64), Windows 2003 R2 (x86-64/AMD64), Windows 2008 Server Core (x86-64/AMD64), Windows Server 2008 R2 (x86-64/AMD64), Windows 8 (Pro and Enterprise), Windows 8.1 (Pro and Enterprise), Windows 8.1 update 1 (Pro and Enterprise), Windows Embedded 8 Industry (Pro and Enterprise), Windows Embedded 8.1 Industry (Pro and Enterprise), Windows 2012 (Server Core, Standard, and Datacenter), Windows 2012 R2 (Server Core, Standard, and Datacenter)

#### ▪ Linux

RHEL 5, 6, 7  
Suse 10, 11  
CentOS 5, 6  
OEL 5, 6  
SELD 11  
OpenSUSE 10/11

## Minimum Requirements

### McAfee Application Control without ePO, McAfee Embedded control

Component	Requirements and Recommendations
Processor	<ul style="list-style-type: none"> <li>▪ Single / Multiple Intel® Pentium® CPU</li> <li>▪ supporting x86-64/IA64/AMD64 architecture</li> </ul>
Memory	<ul style="list-style-type: none"> <li>▪ 2 GB RAM</li> </ul>
Free Disk Space	<ul style="list-style-type: none"> <li>▪ 100 MB for installation on system volume</li> <li>▪ 100 MB free disk space on every volume that will be solidified</li> </ul>

### McAfee Application Control with ePO, McAfee Integrity Control - Server:

Component	Requirements and Recommendations
Processor	<ul style="list-style-type: none"> <li>▪ 64-bit Intel® Pentium® D or higher</li> <li>▪ 2.66 GHz or higher</li> </ul>
Memory	<ul style="list-style-type: none"> <li>▪ 8 GB available RAM recommended minimum</li> </ul>
File System	NT file system (NTFS) partition recommended
Domain Controllers	The server must have a trust relationship with the Domain Controller on the network
Free Disk Space	<ul style="list-style-type: none"> <li>▪ 20 GB — Recommended minimum</li> </ul>
IP Address	<ul style="list-style-type: none"> <li>▪ Recommends using static IP addresses</li> <li>▪ Also supports both IPv4 and IPv6 networks</li> </ul>
Network Interface Card (NIC)	<ul style="list-style-type: none"> <li>▪ 100 Mb or higher</li> </ul>
Ports	<ul style="list-style-type: none"> <li>▪ Port 8443 for HTTPS communication</li> </ul>

### McAfee Application Control with ePO, McAfee Integrity Control -Client:

Component	Requirements and Recommendations
Processor	<ul style="list-style-type: none"> <li>▪ Single / Multiple Intel® Pentium® CPU</li> <li>▪ Supporting x86-64/IA64/AMD64 architecture</li> </ul>
Memory	<ul style="list-style-type: none"> <li>▪ 2 GB RAM</li> </ul>
Domain Controllers	The server must have a trust relationship with the Domain Controller on the network
Free Disk Space	<ul style="list-style-type: none"> <li>▪ 100 MB for installation on system volume</li> <li>▪ 100 MB free disk space on every volume that will be solidified</li> </ul>
IP Address	<ul style="list-style-type: none"> <li>▪ TCP/IP protocol should be installed on the system</li> </ul>

### Other

For Package 1: McAfee Application Control without ePO, and Package 2: McAfee Embedded Control, Advantech provides a user interface tool "McAfee Manager", which allows users to do basic operations without using the command line.

## Ordering information

### For Asia Pacific Region:

- **968EMLMAC2** McAfee Application Control without ePO
- **968EMLMAP1** McAfee Application Control with ePO
- **968EMLMEC1** McAfee Embedded Control
- **968EMLMIC1** McAfee Integrity Control

### For Japan, America, Europe and other regions:

- **968EMQMAC1** McAfee Application Control for bundle
- **968EMQMAP1** McAfee Application Control w/ePO for bundle
- **968EMQMEC1** McAfee Embedded Control for bundle
- **968EMQMIC1** McAfee Integrity Control (MEC w/ePO) for bundle