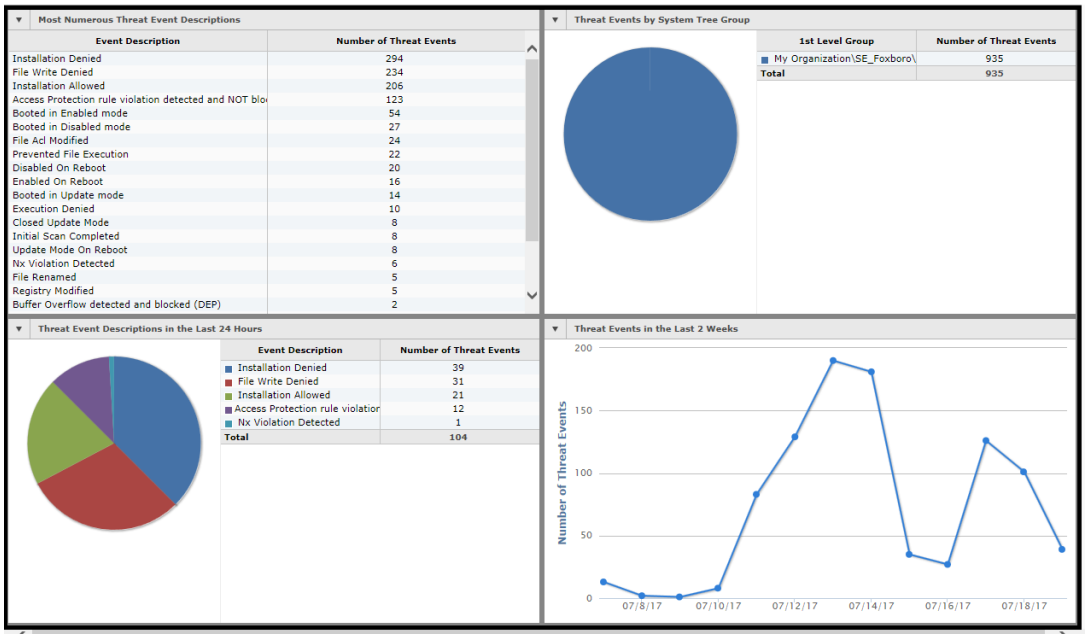
Foxboro Evo™ Process Automation System

Product Specifications

Foxboro® by Schneider Electric

PSS 31S-4McAfee

McAfee® Security Products



INTRODUCTION

Schneider Electric incorporates globally recognized third-party security packages that provide additional security enhancement features to help complement the security features already built into our products.

Contemporary security applications go beyond traditional firewall and antivirus software to provide advanced host intrusion prevention, application and device control, and more. These security suites are referred to as Endpoint Protection (EPP).

A system with I/A Series v8.8 or Control Core Services v9.0 or later supports the addition of these packages from McAfee. McAfee EPP products can be installed in two ways:

- Managed Solution
- Self-Managed Solution

Managed Solution

The Managed solution allows you to install and monitor the McAfee products on your endpoints from a single, centralized location using the ePolicy Orchestrator (ePO) console. You can also update DAT files, Exploit Prevention content, and patches on the endpoints from the ePO console. In Managed mode, Endpoint Security along with additional applications such as Rogue System detection, Device Control, and Integrity Control are supported.

Self-Managed Solution

The Self-Managed solution only supports McAfee Endpoint Security. You need to install and update each endpoint manually.

FEATURES

Endpoint Security (ENS) 10.5

ENS is the only supported McAfee product that can be installed without ePO in a Self-Managed mode. The other applications such as McAfee Agent, RSD, Device Control, and Integrity Control need ePO.

ENS is also the only supported McAfee product that can be installed on the Standard edition of Foxboro Evo™. The rest of the McAfee applications need the Security Enhanced edition of Foxboro Evo.

Endpoint Security consists of these modules:

- Threat Prevention
- Firewall
- Web Control

Threat Prevention

- Threat Prevention replaces traditional antivirus protection and intrusion prevention.
- It improves performance and productivity by optimizing the scanning.
- It prioritizes suspicious processes and applications.
- It also provides adaptive behavioral scanning to monitor and report on suspicious activity.

Keeping this solution patched and up to date with the latest qualified version is crucial to the security of a system.

Threat Prevention consists of ENS AMCore DAT File and Exploit Prevention content products that the user needs to update as per the need.

In addition to these types of changes, they also provide product patches to incorporate fixes for installed security applications.

- ENS AMCore DAT File: Users need to continually update the security products to address new vulnerabilities as they are discovered. For example, users need to continually update the virus scanning software with virus definition files (DAT files) that are part of ENS Threat Prevention. McAfee frequently releases new DAT files to incorporate results of its ongoing research on the characteristics of new viruses.
- Exploit Prevention Content: An exploit is a sequence of commands that allows an attacker to take advantage of a vulnerability or a bug in a process or software application. To control a system, the attacker needs to take advantage of a chain of vulnerabilities in the system. Blocking any attempt to exploit a vulnerability in the chain results in blocking the entire exploitation attempt.

The Threat Prevention module in McAfee ENS provides a content based Exploit Prevention update every month. This content helps provide protection against zero-day exploits.

Firewall

There is also a host based firewall available in the package, which is not turned on by default because its configuration will be specific to each customer endpoint.

The firewall monitors communication between the computer and other resources on the network, helping intercept suspicious communication. The firewall rules determine how to manage network traffic. Each rule provides a set of conditions that the network traffic has to meet.

When ENS finds traffic that matches the conditions of a rule, it either allows or blocks the traffic based on the rule conditions. ENS applies the rule at the top of the firewall rules list first.

Web Control

ENS Web Control works as a browser extension or add-on with Internet Explorer, Google Chrome™, and Mozilla Firefox™.

NOTE

We recommend that endpoints used in a control system are not connected to the

Internet. Web Control can add a layer of protection in case any inadvertent connections are made.

Before using web control, users need to activate the ENS web control extensions manually on each endpoint for these browsers. Below are the features for Managed and Self-Managed Web Control that users can configure in the system and create policies for.

Managed Web Control

- Enable or disable Web Control on the user's system with an option for disabling the software and browser plug-ins.
- Help control access to sites, pages, and downloads, based on their type of content. For example, for file downloads, users can block red sites (vulnerable sites) and send a notification when users try to access yellow sites (that do not have a reputation for being vulnerable). Green-rated (safe sites) sites and downloads are allowed automatically.
- Identify sites as blocked or allowed, based on the URLs and domains.
- Help prevent a user from uninstalling or changing Web Control files, registry keys, registry values, services, and processes.
- Customize the notification that appears when a user attempts to access a blocked website.

Self-Managed Web Control

- Enable or disable Web Control on the user's system with an option for disabling the software and browser plug-ins.
- Help control access to sites, pages, and downloads, based on their safety rating or type of content. For example, users can block red sites and send a notification to users trying to access yellow sites.

ePolicy Orchestrator®

McAfee ePolicy Orchestrator provides the ability to centrally manage the following McAfee components: Agent, RSD, DLP, Solidcore/Integrity Control, and ENS. It allows users to install, configure, update, monitor, and deploy these applications to client workstations and servers. For example, ePO can be used to keep the virus signature (DAT) files up to date from a single location, which helps avoid updating DAT files and performing other tasks manually on each machine in the system.

ePO can be installed on any server running Microsoft Windows Server 2008 SP2 or later and I/A Series software v8.8 or Control Core Services software v9.0 or later. ePO provides the ability to deploy the McAfee security products automatically, from one location on the Windows-based workstations and servers on the control network that are in the I/A Series or the Foxboro Evo Active Directory domain. It also manages and distributes the policy settings and other options of the packages.

Another major benefit of ePO is the ability to monitor these packages from the ePO console. Dashboards help users to quickly view the status of the products and stations that ePO is managing. They also contain monitors that run queries and display the results. When the ePO console is opened, it initially displays the dashboard window, displaying McAfee provided or customized dashboards. A set of predefined dashboards is provided with the ePO software. However, users can build their own dashboards.

McAfee Agent

The McAfee Agent is the client-side component that helps provide secure communication between the ePO and managed products. It performs the following tasks:

- Serves as an updater for McAfee products including DATs and Exploit Prevention content.

- Runs in the background, gathers information and events from managed systems, and sends them to the ePO server.
- Installs products and their updates on managed systems.
- Enforces policies and tasks on managed systems and sends events back to the ePO server.

Rogue System Detection

Rogue devices are devices that do not have the McAfee Agent installed and as such are unknown to ePO and not part of the management framework. This means that they are not part of any standards, security controls, policies, or patch updates.

Rogue systems are unprotected systems that create entry points for potentially harmful programs to access the network. Rogue System Detection (RSD) provides near real-time discovery of rogue systems through the use of a Rogue System Sensor installed on your network. The sensor monitors the network broadcast messages to detect systems connected to the network. If the server cannot recognize the system, RSD provides information to ePO through a notification in the dashboard.

Device Control

Device Control is the subset of Data Loss Prevention (DLP) that is used with Foxboro DCS products. It helps organizations to reduce the risk of an unintentional disclosure of confidential information. It helps prevent unauthorized use of removable media devices (such as CD/DVD, USB, and floppy disk) to guard against data leaks. Such devices are one of the common ways malware can transfer itself from relatively unsecured home or business networks to the control network.

Integrity Control/Solidcore

McAfee Integrity Control consists of two components: Application Control and Change Control. It uses an application called Solidcore that helps block unauthorized applications and changes to the process control networks by combining whitelisting and change control technology.

Integrity Control functions by listing the processes that are allowed to run (whitelisting) on fixed function devices. It helps block vulnerable, unauthorized, or malicious applications that can compromise the integrity of systems. Whitelisting helps secure the system and allows only authorized updates or changes that are defined by administrators or trusted sources.

Integrity Control software also supports change-control technology that can block unwanted, out-of-policy changes before they occur. Solidcore/Integrity Control enabled systems block the changes attempted outside of policy. The change attempt is logged and sent as an alert to administrators.

Application Control

Application Control operates in four modes and can change from one mode to another mode:

- Disabled mode
- Enabled mode
- Observe mode
- Update mode

Application Whitelisting (AWL) Advantages

- Malware applications can use self-modifying polymorphic code techniques that avoid signature-based detection by constantly changing. AWL provides a solution because it allows only pre-approved programs to run on the system.
- Additionally, AWL typically needs less maintenance than antivirus applications. Therefore, it is a good alternative in cases where daily or weekly maintenance is not feasible.

SYSTEM REQUIREMENTS

Software Requirements

- Windows 7 Standard
- Windows Server 2008 R2 Standard
- I/A Series v8.8 or Control Core Services 9.0 or later
- FCS 4.0 or Control Software 6.0 or later

Hardware Requirements

- Server: HP DL380 Gen 7/Gen 9, H90/V90/V91
- Workstation: HP Z440/Z420

ORDERING INFORMATION

Part Number	Description
K0204AF (previously K0204AB)	McAfee Security Products kit with ePolicy Orchestrator 5.3.2, Endpoint Security (ENS) 10.5, McAfee Agent 5.0.4, Device Control 10.0.1, Integrity Control 8.0, and Rogue System Detection 5.0.4. The kit does not contain the J0202AS license, which is needed for each endpoint that runs any McAfee applications. The required number of J0202AS licenses are now included with all new platform purchases but can also be ordered separately as needed for older platforms.

Foxboro®

by Schneider Electric

Schneider Electric Systems USA, Inc.
38 Neponset Avenue
Foxborough, MA 02035-2037
United States of America
www.schneider-electric.com

Global Customer Support
Inside US: 1-866-746-6477
Outside US: 1-508-549-2424
https://pasupport.schneider-electric.com

MB 031 0917