EcoStruxure™

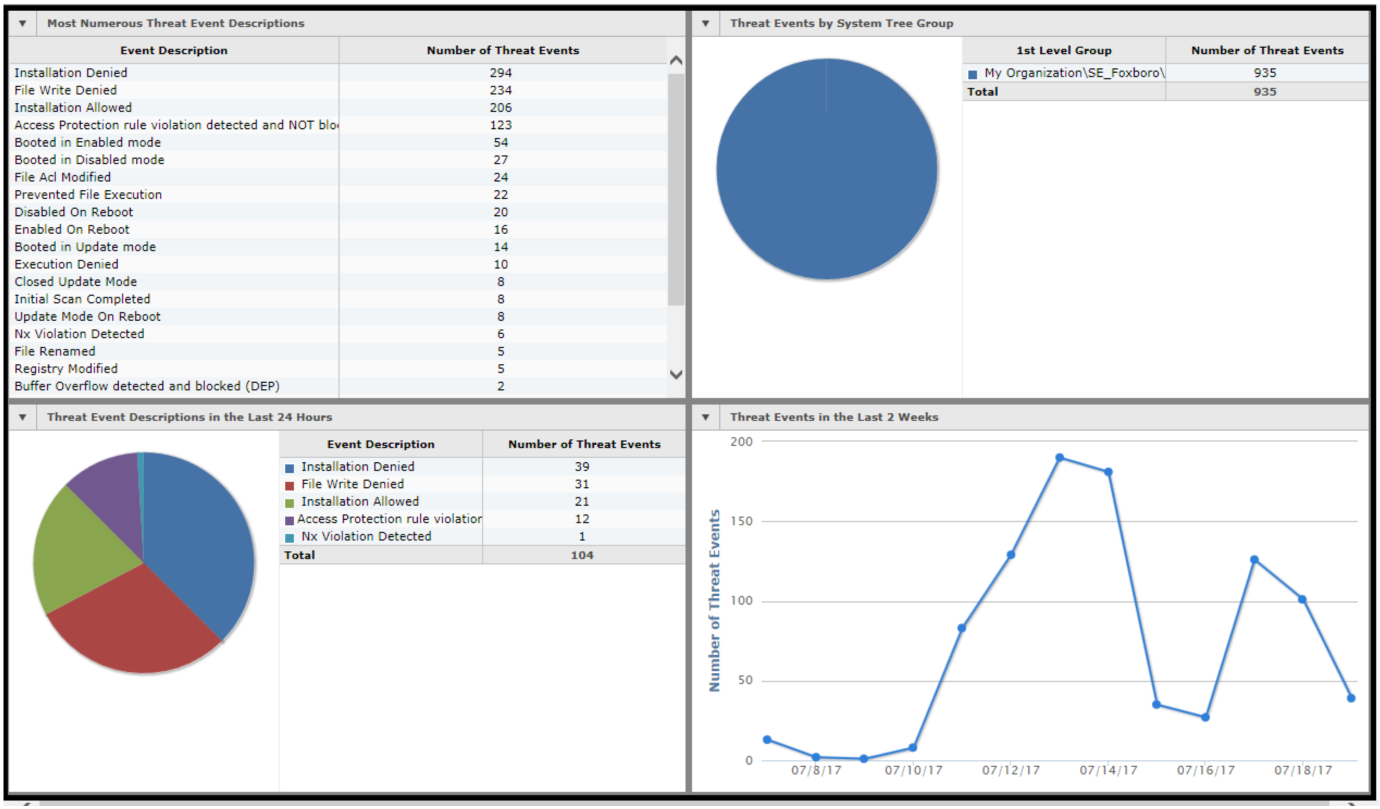
Foxboro™ DCS

McAfee® Security Products

PSS 41S-4McAfee

Product Specification

October 2022



▼ Most Numerous Threat Event Descriptions

Event Description	Number of Threat Events
Installation Denied	294
File Write Denied	234
Installation Allowed	206
Access Protection rule violation detected and NOT blo	123
Booted in Enabled mode	54
Booted in Disabled mode	27
File Acl Modified	24
Prevented File Execution	22
Disabled On Reboot	20
Enabled On Reboot	16
Booted in Update mode	14
Execution Denied	10
Closed Update Mode	8
Initial Scan Completed	8
Update Mode On Reboot	8
Nx Violation Detected	6
File Renamed	5
Registry Modified	5
Buffer Overflow detected and blocked (DEP)	2

▼ Threat Events by System Tree Group

1st Level Group	Number of Threat Events
🟦 My Organization\SE_Foxboro\	935
Total	935

▼ Threat Event Descriptions in the Last 24 Hours

Event Description	Number of Threat Events
🟦 Installation Denied	39
🟥 File Write Denied	31
🟩 Installation Allowed	21
🟪 Access Protection rule violation	12
■ Nx Violation Detected	1
Total	104

▼ Threat Events in the Last 2 Weeks

Schneider Electric

https://www.se.com

Legal Information

Schneider Electric products and equipment should be installed, operated, serviced, and maintained only by qualified personnel.

As standards, specifications, and designs change from time to time, information contained in this guide may be subject to change without notice.

To the extent permitted by applicable law, no responsibility or liability is assumed by Schneider Electric and its subsidiaries for any errors or omissions in the informational content of this material or consequences arising out of or resulting from the use of the information contained herein.

Introduction

Schneider Electric incorporates globally recognized third-party cybersecurity 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).

Foxboro DCS 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 Solidcore (McAfee Application and Change Control (MACC)) are supported.

Self-managed Solution

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

The Self-managed solution is the only supported option for the t740 Thin Client.

Features

This chapter includes the following features:

- Endpoint Security (ENS)
  - Threat Prevention
  - Firewall
  - Web Control
    - *Managed Web Control*
    - *Self-managed Web Control*
- ePolicy Orchestrator®
- McAfee Agent
- Rogue System Detection
- Device Control
- Solidcore (McAfee Application and Change Control (MACC))
- Application Permissions Listing Advantages

Endpoint Security (ENS)

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

ENS is also the only supported McAfee product that can be installed on the Local Edition of the Foxboro DCS. The rest of the McAfee applications need the Enterprise Edition of the Foxboro DCS.

Endpoint Security consists of these modules:

- Threat Prevention
- Firewall
- Web Control

Threat Prevention

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

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

- 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.

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 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™, Mozilla Firefox™, and Microsoft Edge.

> **NOTE:** We recommend that endpoints used in a control system not be 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, 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 Foxboro DCS 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 Foxboro DCS 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 these tasks:

- Serves as an updater for McAfee products including .DAT files 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 that malware can transfer itself from relatively unsecured home or business networks to the control network and from there, into the Foxboro DCS.

Solidcore (McAfee Application and Change Control (MACC))

McAfee Solidcore 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 permission listing and change control technology.

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

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

Application Permission Listing Advantages

- Malware applications can use self-modifying polymorphic code techniques that avoid signature-based detection by constantly changing. Permission Listing provides a solution because it allows only pre-approved programs to run on the system.
- Permission Listing can be used in environments that do not change frequently. Due to this, it is a good additional security layer in cases where antivirus .DAT and Exploit Prevention content cannot be updated every day or every week. In environments where software updates and patching are frequent, Permission Listing requires more maintenance than antivirus applications.

Hardware and Software Requirements

This chapter lists the hardware and software requirements for Managed and Self-Managed Solution.

Managed Solution

ePO Server Host Requirements	Client Workstations Requirements
• HP DL380 Gen 9/Gen 10 OR Hyper-V Virtual Machine with a minimum 8GB RAM and 200GB free space on HDD • Windows Server 2016 with multi core enabled • Control Core Services v9.4 or later, if installed	• Windows 10 or Windows Server 2016 • Control Core Services 9.4 or later with multi core enabled • Foxboro DCS Control Software 7.x or later, if installed

Self-Managed Solution

Self-managed Server Requirements	Self-managed Workstation Requirements	Self-managed Thin Client Requirements
• HP DL380 Gen 9/Gen 10, H90 Foxboro DCS Standard Server/ V90/V91 Foxboro DCS Virtualization Server/V91 Foxboro DCS Virtualization Server • Windows Server 2016 hardware and virtual platforms • Control Core Services software v9.1 or later, if installed • Control Software 7.0 or later, if installed	• HP Z4G4/Z440/Z420 workstation (H92) • Windows 10 with multi core enabled • Control Core Services v9.1 or later • Control Software 7.x or later, if installed	• HP t740 Thin Client • Windows 10

Ordering Information

Part Number	Description
K0204BJ-B	The McAfee Security Products kit has the Self-managed set with: • Self-managed EP Content and DAT packages • Self-managed Policy • McAfee_Endpoint_Security_10.7.0.1192.5_stand_alone_client_install media Every endpoint has a J0201FL license purchased as of 2016, or a J0202AS license.
	The McAfee Security Products kit has the ePO-managed set with: • ePolicy Orchestrator 5.10 • Endpoint Security (ENS) 10.7 • McAfee Agent 5.7.5 • Device Control 11.6.4 • Application and Change Control (MACC) 8.3.4 • Rogue System Detection 5.0.6 • Engine 6000 • ePO - Exploit Protection Content and V3 DAT file • McAfee ePO Managed - Exported Policies • SQL Express 2014 Adv

⚠ **WARNING**: This product can expose you to chemicals including lead and lead compounds, which are known to the State of California to cause cancer and birth defects or other reproductive harm. For more information, go to www.p65warnings.ca.gov/.

Schneider Electric Systems USA, Inc.
70 Mechanic Street
Foxboro, Massachusetts 02035–2040
United States of America

Global Customer Support: https://pasupport.schneider-electric.com

As standards, specifications, and design change from time to time, please ask for confirmation of the information given in this publication.