



Foxboro™ DCS

Trellix Security Products

PSS 41S-4Trellix

Product Specification

December 2024

Legal Information

The information provided in this document contains general descriptions, technical characteristics and/or recommendations related to products/solutions.

This document is not intended as a substitute for a detailed study or operational and site-specific development or schematic plan. It is not to be used for determining suitability or reliability of the products/solutions for specific user applications. It is the duty of any such user to perform or have any professional expert of its choice (integrator, specifier or the like) perform the appropriate and comprehensive risk analysis, evaluation and testing of the products/solutions with respect to the relevant specific application or use thereof.

The Schneider Electric brand and any trademarks of Schneider Electric SE and its subsidiaries referred to in this document are the property of Schneider Electric SE or its subsidiaries. All other brands may be trademarks of their respective owner.

This document and its content are protected under applicable copyright laws and provided for informative use only. No part of this document may be reproduced or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), for any purpose, without the prior written permission of Schneider Electric.

Schneider Electric does not grant any right or license for commercial use of the document or its content, except for a non-exclusive and personal license to consult it on an "as is" basis.

Schneider Electric reserves the right to make changes or updates with respect to or in the content of this document or the format thereof, at any time 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 document, as well as any non-intended use or misuse of the content thereof.

Overview

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 Trellix. Trellix 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 Trellix products on your endpoints from a single, centralized location using the ePolicy Orchestrator® (ePO) console. You can also update antivirus threat detection signature (.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 (Trellix Application and Change Control (TACC)) are supported.

Self-managed Solution

The Self-managed solution only supports Trellix 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 these features:

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

Endpoint Security (ENS)

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

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

Endpoint Security consists of these modules:

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

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 the Foxboro DCS 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

While we recommend that endpoints used in the Foxboro DCS not be connected to the internet, other computers might require this connection. Managed Web control provides for:

- 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

Trellix ePolicy Orchestrator provides the ability to centrally manage these Trellix 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:

- Windows Server 2016 and Foxboro DCS Control Core Services software v9.4 or later
- Windows Server 2022 and Foxboro DCS Control Core Services software v9.8 or later

ePO provides the ability to deploy the Trellix security products automatically, from one location on the Windows-based 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 Trellix provided or customized dashboards. A set of predefined dashboards is provided with the ePO software. However, users can build their own dashboards.

Trellix Agent

The Trellix 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 Trellix products including virus threat prevention 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 Trellix Agent installed and as such are unknown to ePO and are 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 be transferred to the control network and from there, into the Foxboro DCS.

Solidcore (Trellix Application and Change Control (TACC))

Trellix 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 virus threat prevention and Exploit Prevention content cannot be updated frequently. In environments where software updates and patching are frequent, Permission Listing requires more maintenance than antivirus applications.

Hardware and Software Requirements

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

Managed Solution

ePO Server Host Requirements	Client Workstations Requirements
<ul style="list-style-type: none"> HPE DL380 /Gen 10 or Hyper-V Virtual Machine with a minimum 8GB RAM and 200GB free space on HDD HPE DL380 /Gen 11 or Hyper-V Virtual Machine with a minimum 32 GB RAM 	N/A
<ul style="list-style-type: none"> Windows Server 2016 Control Core Services v9.4 or later, if installed 	<ul style="list-style-type: none"> Windows 10 (v1607) or Windows Server 2016 Control Core Services v9.4 or later, if installed Foxboro DCS Control Software v7.1.1 or later, if installed
<ul style="list-style-type: none"> Windows Server 2022 Control Core Services v9.8 or later, if installed 	<ul style="list-style-type: none"> Windows 10 21H2 LTSC or Windows Server 2022 Control Core Services v9.8 or later, if installed Control Software v8.0 or later, if installed

Self-Managed Solution

Self-managed Server Requirements	Self-managed Workstation Requirements		Self-managed Thin Client Requirements
<ul style="list-style-type: none"> HPE DL380 Gen 10, H90 Foxboro DCS Standard Server HPE DL380 Gen 11, H94 Foxboro DCS Standard Server V91 Foxboro DCS Virtualization Server V95 Foxboro DCS Virtualization Server 	<ul style="list-style-type: none"> HP Z4G4 workstation (H92) 	<ul style="list-style-type: none"> Dell P5860 workstation (D96) 	<ul style="list-style-type: none"> HP t740 Thin Client
<ul style="list-style-type: none"> Windows Server 2016 hardware and virtual platforms Control Core Services software v9.4 or later, if installed Control Software v7.1.1 or later, if installed 	<ul style="list-style-type: none"> Windows 10 (v1607) Control Core Services v9.4 or later, if installed Control Software v7.1.1 or later, if installed 	<ul style="list-style-type: none"> Windows 10 21H2 LTSC Control Core Services v9.8 or later, if installed Control Software v8.0 or later, if installed 	<ul style="list-style-type: none"> Windows 10 (v1809)


Self-managed Server Requirements	Self-managed Workstation Requirements		Self-managed Thin Client Requirements
<ul style="list-style-type: none">• Windows Server 2022 hardware and virtual platforms• Control Core Services software v9.8 or later, if installed• Control Software v8.0 or later, if installed	<ul style="list-style-type: none">• Windows 10 21H2 LTSC• Control Core Services v9.8 or later, if installed• Control Software v8.0 or later, if installed		

Ordering Information

Existing customers must first upgrade to DLP v11.9.100 (K0204BM), before upgrading to Trellix DLP v11.10.0 (K0204BX).

New customers can select the media that is applicable to their system.

Part Number	Description
K0204BM	Trellix Security Products (ENS 10.7.0 & ePO 5.10 Update 15) Supported by CCS v9.4 and later.
	The Trellix Security Products kit has the Self-managed set with: <ul style="list-style-type: none"> • Self-managed EP Content and DAT packages • Self-managed Policy • Trellix_Endpoint_Security_10.7.0.5264.1_Standalone_Client_Install_ENS Every endpoint has a J0202AS license.
	The Trellix Security Products kit has the ePO-managed set with: <ul style="list-style-type: none"> • ePolicy Orchestrator 5.10 • Trellix Endpoint Security (ENS) 10.7 • Trellix Agent 5.7.8 • Device Control (DLP) 11.9.100 • Application and Change Control (MACC) 8.3.4 • Rogue System Detection (RSD) 5.0.6 • Root Certificates • McAfee ePO Managed - Exported Policies • Product Compatibility List (PCL) • SQL Express 2014 Adv
K0204BX	Trellix Security Products (ENS 10.7.0 & ePO 5.10 Service Pack 1) Supported by CCS v9.8 and later.
	The Trellix Security Products kit has the Self-managed set with: <ul style="list-style-type: none"> • Trellix Agent 5.7.9 • Root Certificates • SE_Trellix_Endpoint_Security_10.7.0.5264.1_Standalone_Client_Install_ENS Every endpoint has a J0202AS license.
	The Trellix Security Products kit has the ePO-managed set with: <ul style="list-style-type: none"> • ePolicy Orchestrator 5.10 Service Pack 1 • Endpoint Security (ENS) 10.7.0 • Trellix Agent 5.7.9 • Device Control (DLP) 11.10.0 • Application and Change Control (TACC) 8.3.4 • Rogue System Detection (RSD) 5.0.6 • Root Certificates • Trellix ePO Managed - Exported Policies • SQL Express 2022 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.se.com>

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

© 2023–2024 Schneider Electric. All rights reserved.

PSS 41S-4Trellix, Rev D