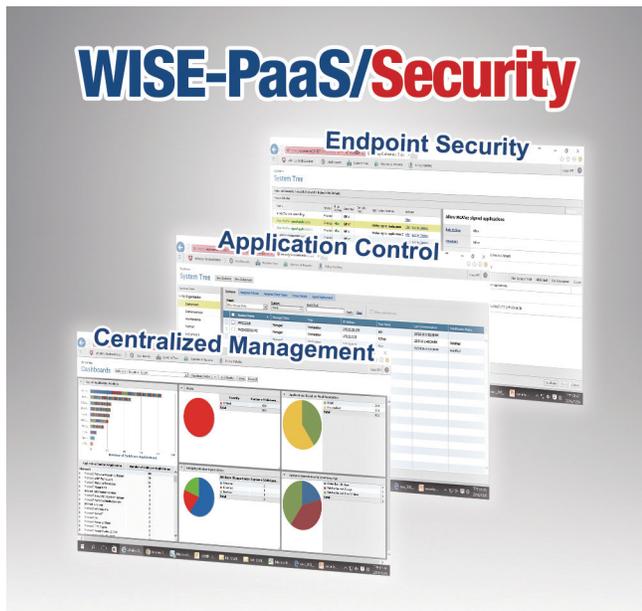


WISE-PaaS/Security

IoT Security Management



Features

WISE-PaaS/Security, empowered by Intel® Security, is a scalable, extensible, and low overhead software solution that enables centralized security management, monitoring, and reporting for IoT devices. The powerful web-based console, ePolicy Orchestrator, can help you to easily deploy security applications, configure policies and tasks, control updates, and monitor events for all managed systems

- Fast and easy to remotely deploy/configure security policies for each device
- Centralized management on Azure/Cloud
- Monitor and report managed client data

Introduction

WISE-PaaS/Security is a central security management console, which is a comprehensive and quickly deployed security solution for the protection of IoT devices. It 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 computing resources, and is equally effective either in non-network standalone mode or in a Cloud.

ePolicy Orchestrator

ePolicy Orchestrator (ePO) is the most advanced, extensible, and scalable centralized security management software in the industry. It provides product deployment and reporting capabilities through a single point of control, which can be standalone server-based or Cloud-based. The centralized policy management and repository can help you build what you need quickly and easily for protection of your IoT system. It can be tailored to fit, with Intel® Security function modules that fulfill each vertical application and scenario.

Three different licensed modules can be equipped on ePO to provide for different security guardian scenarios: Application Control, Integrity Control, and Endpoint Security.

Feature Details

Low Overhead

WISE-PaaS/Security is a low overhead software solution.

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

ePolicy Orchestrator

ePolicy Orchestrator is a complete management software for Intel® Security/McAfee products. It can help you select and deploy software or applications on the network, then do centralized management, using remote configuration and reporting. Using an ePolicy Orchestrator, you can:

- Deploy security products/functions, patches, and service packs to the system in your network.
- Manage the host and network security products deployed to your systems through the enforcement of security policies, client tasks, and server tasks.
- Update the DATs, Engines and other security content required by your security software to ensure your managed systems are secure.

Minimal Requirements

WISE-PaaS/Security

ePolicy Orchestrator can be installed either on a standalone server or in the Cloud.

▪ Server requirements

Component	Requirements and Recommendations
Processor	<ul style="list-style-type: none">▪ 64-bit Intel® Pentium® D or higher▪ 2.66 GHz or higher
Memory	8 GB available RAM recommended minimum
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	20 GB — Recommended minimum
IP address	<ul style="list-style-type: none">▪ Recommends using static IP addresses▪ Also supports both IPv4 and IPv6 networks
Network Interface Card (NIC)	100 Mb or higher
Ports	Port 8443 for HTTPS communication
Supported Operating Systems	<ul style="list-style-type: none">▪ Windows Server 2008 R2 (Standard, Enterprise, and Datacenter)▪ Windows Server 2012 (Standard and Datacenter)▪ Windows Server 2012 R2 (Standard and Datacenter)

Cloud Recommendation

- Microsoft Azure
- Minimum VM Level : A2
- Recommended VM Level : A3

Client Recommended Requirements:

Component	Requirements and Recommendations
Processor	<ul style="list-style-type: none"> ▪ Single / Multiple Intel® Pentium® CPUs ▪ Supporting x86-64/IA64/AMD64 architecture
Memory	Minimum 1 GB RAM
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"> ▪ 100 MB for installation on system volume ▪ 100 MB free disk space on every volume that will be solidified
IP address	TCP/IP protocol should be installed on the system
Supported Operating Systems	<ul style="list-style-type: none"> ▪ Windows 32-bit <ul style="list-style-type: none"> – Windows 2008 SP1 Or later – Windows 7 – Windows 7 Embedded – Windows 7 Embedded POSReady – Windows 8 Pro/Enterprise – Windows 8.1 Pro/Enterprise – Windows Embedded 8 Industry (Pro/Enterprise) – Windows Embedded 8.1 Industry (Pro/Enterprise) – Windows 10 2015 & 2016 (Pro and IoT Enterprise) ▪ Windows 64-bit <ul style="list-style-type: none"> – Windows 2008/R2 SP1 or later – Windows 7 Embedded – Windows 8 Pro/Enterprise – Windows 8.1 Pro/Enterprise – Windows Embedded 8 Industry (Pro/Enterprise) – Windows Embedded 8.1 Industry (Pro/Enterprise) – Windows 10 2015 & 2016 (Pro and IoT Enterprise) – Windows Sever 2012/R2 (Core, Standard, and DataCenter) ▪ Linux <ul style="list-style-type: none"> – Ubuntu 12.04, 14.04, 16.04 – CentOS 5, 6, 7 – OpenSuSE 10, 11 – RHEL 5, 6, 7 – SLES 10, 11/ SLED 11

Order Information

- **31WPSMAP01** WISE-PaaS/Security

At least one of the following Intel® Security products should be chosen to enable security functions.

- **31WPSMAC01** Intel® Security Application Control
- **31WPSMIC01** Intel® Security Integrity Control
- **31WPSMES0A** Intel® Security Endpoint Security 10