MEIDENSHA CORPORATION

ThinkPark Tower, 2-1-1, Osaki, Shinagawa-ku, Tokyo, 141-6029 Japan
Phone: 81-3-6420-7510 Facsimile: 81-3-5745-3053
www.meidensha.co.jp

Overseas Offices & Group Companies

China

DONGGUAN MEIDEN ELECTRICAL ENGINEERING CO., LTD.
Yan Wu Industrial District, Wan Jiang Country, Dongguan,
Guangdong 523049 P.R. China
Phone: 86-769-22285210 Facsimile: 86-769-22285250

MEIDEN ZHENGZHOU ELECTRIC CO., LTD.
No.87 Hehuan Street, Zhengzhou Hi-Tech Industries Development Zone,
Zhengzhou, Henan Province, P.C.450001, P.R.China
Phone: 86-371-67848800 Facsimile: 86-371-67848797

MEIDEN SHANGHAI CO., LTD.
15F, Hengji Plaza, No.99 Huaihai-Donglu, Huangpu-Qu,
Shanghai, P.C. 200021, P.R.China
Phone: 86-21-63860358 Facsimile: 86-21-63860058

MEIDEN HANGZHOU DRIVE SYSTEMS CO., LTD.
No.168, Hongxing Road, Qiaonan District,
Xiaoshan Economic & Technological Development Zone,
Hangzhou, Zhejiang, P.C. 311231, P.R.China
Phone: 86-571-8369-6808 Facsimile: 86-571-8369-6818

Hong Kong

MEIDEN PACIFIC (CHINA) LTD.
Unit 01-02A, 16/F, Tower 1, Ever Gain Plaza,
88 Container Port Road, Kwai Chung, N.T., Hong Kong
Phone: 852-2503-2468 Facsimile: 852-2887-8046

India

MEIDEN INDIA PVT. LTD.
910, International Trade Tower, Nehru Place, New Delhi-110019, India
Phone: 91-11-46539381 Facsimile: 91-11-46539385

Indonesia

P.T. MEIDEN ENGINEERING INDONESIA
20th Floor, Summitmas I, Jl. Jenderal Sudirman Kaveling 61-62
P.O.BOX 6920/KBY/Summitmas I Jakarta Selatan 12190, Indonesia
Phone: 62-21-520-0612 Facsimile: 62-21-520-0240

Korea

MEIDEN KOREA CO., LTD.
Royal Building No. 410, 5 Dangju-Dong, Chongro-ku, Seoul, Korea
Phone: 82-2-736-0232～3 Facsimile: 82-2-736-0234

Malaysia

MEIDEN ASIA PTE. LTD. MALAYSIA BRANCH OFFICE
G.03, Ground Floor, Wisma Academy, 4A, Jalan 19/1,
46300 Petaling Jaya, Selangor Darul Ehsan, Malaysia
Phone: 60-3-79554646 Facsimile: 60-3-79546466

Singapore

MEIDEN ASIA PTE. LTD.
5, Jalan Pesawat, Jurong Industrial Estate, Singapore 619363
Phone: 65-6268-8222 Facsimile: 65-6264-4292

MEIDEN SINGAPORE PTE. LTD.
5, Jalan Pesawat, Jurong Industrial Estate, Singapore 619363
Phone: 65-6268-8222 Facsimile: 65-6264-4292

Thailand

THAI MEIDENSHA CO., LTD.
15th Floor, Rasa Tower II, 555 Phaholyothin Road, Chatuchak,
Chatuchak, Bangkok 10900, Thailand
Phone: 66-2792-4200 Facsimile: 66-2792-4299

MEIDEN ELECTRIC (THAILAND) LTD.
898 Moo 2, Bangpa-in Industrial Estate, Udomsorayuth Rd.,
Klongjig, Bangpa-in, Ayudhaya 13160, Thailand
Phone: 66-35-258258～262 Facsimile: 66-35-221388

United Arab Emirates

MEIDENSHA CORPORATION
Office 302, New Century City Tower Port Saeed Road Deira, Dubai, U.A.E
P.O Box: 117841
Phone: 971-4-298-1127 Facsimile: 971-4-298-1135

The United Kingdom

MEIDEN EUROPE LTD.
NYK Complex, Bradbourne Drive, Tilbrook, Milton Keynes MK7 8BN,
England, U.K.
Phone: 44-1908-276000 Facsimile: 44-1908-276010

The United States

MEIDEN AMERICA, INC.
15800 Centennial Drive, Northville Township, MI 48168, U.S.A.
Phone: 1-734-656-1400 Facsimile: 1-734-459-1863

MEIDEN TECHNICAL CENTER NORTH AMERICA LLC
15800 Centennial Drive, Northville Township, MI 48168, U.S.A.
Phone: 1-734-656-1400 Facsimile: 1-734-459-1863

MB65-3102Ⓐ As of Jan., 2011
2011-1ME(0.5L)0.5L

MEIDEN

Security Reinforcement Software

AhnLab
WhiteShield for MEIDEN

Protecting your controllers against the threat of viruses and worms

Empower for new days

Prevention of Human Errors and Intrusion by Viruses and Worms

WhiteShield offers a high level of authority management by which the Windows system administrators is controlled through compulsory access in order to protect the controllers against the intrusion of viruses and the like. When WhiteShield is loaded on a controller, it functions as a filter driver between the application and the kernel. When a process or a user tries to access a local system, access control is activated for the resources based on the preset permission list (white list) irrespective of the competence of the OS. This product prevents the intrusion of viruses and worms and also human errors.

WhiteShield for MEIDEN

Features

Easy introduction to manufacturing sites

Virus intrusion and other malicious actions can be avoided by incorporating this software in controllers and industrial PCs used in the manufacturing sites where introduction of anti-virus software is difficult to accomplish.

Prevention of new virus types possible without suspension of fieldwork

In an environment where WhiteShield has been introduced, virus pattern filing and program updating are unnecessary to carry out. It is unnecessary to stop production. It is possible to prevent new virus types for which pattern recognition is impossible with normal anti-virus software.

No influence upon CPU loads

Stable operation of controllers and industrial PCs can be realized while perfect security is maintained since there is no high load on the CPU like virus scanning, etc.

Provision of folder protection functions

Thanks to the folder protection functions that control the accessible applications for specified folders, confidential data and files relating to production are protected with a high degree of security.

Modal changes enabled

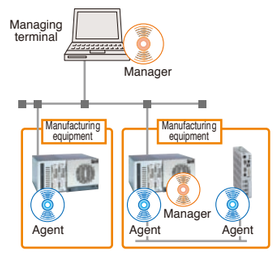
Operation mode	Functions
Enable Mode	The white list is active and data are saved in a log if a violation of access occurs. In this case, such violations are stopped.
Disable Mode	No white list is active and data are not saved in the log even if a violation of access should occur. In this mode, WhiteShield functionality is turned off and the ordinary OS is actuated.
Install Mode	This mode is used when installing an application. If there is any executable file, it is automatically added to the white list.
Test Mode	The white list is active and data are saved in the log if an access violation occurs. However, violations are not interrupted. This mode is used to test if there is any problem in the preset white list.

Scope of WhiteShield applications

- Security-based measures taken for controllers and industrial PCs
- Prevention of diffusion of viruses and worms
- Protection of confidential data

Configuration

WhiteShield is composed of the agents in charge of executing security functions and the manager in charge of security policy setup and management of such agents.



● Agent

An agent is defined as the main WhiteShield program installed in the controller that is being protected. Based on the white list, it performs access control for the processes and users. According to the managerial needs and requests, measures are taken for responses and transactions. Therefore, the manager is never called by an agent.

● Manager

A manager is defined as a managing program intended to control one or multiple agents. In order to control the agents, there are functions to establish, revise, and circulate the white list to be applied to the respective agents. It is possible to put agents in groups by examining each agent log.

◆ Hardware environment Least specifications

CPU: Intel Celeron M/600MHz or above
RAM: 256MB or more
HDD: 50MB or more
Network: 10Base-T/100Base-TX

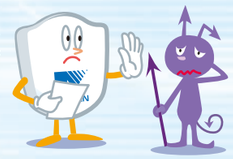
◆ OS environment

Windows XP Embedded SP1/SP2/SP3
Windows XP Professional SP2/SP3
Windows 2000 Professional SP4
Windows Server 2003 SP2
Windows Embedded Standard 2009

Functions

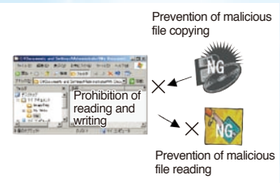
Starting process restrictions with the White List system

When a process or a user tries to access a local system, access control is carried out for the resources based on the preset permission list irrespective of the competence of the OS of the process or the user. This permission list is called the white list. When the white list is adopted, by controlling the accessing actions, WhiteShield is powered to prevent the intrusion of viruses and worms and also misoperations due to human errors.



Folder access control

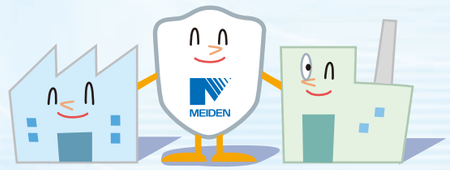
By setting up an accessible process for a folder, access control becomes possible for this folder. With this function, it is possible to protect important files and prevent the leakage of confidential files.



- Since data writing is impossible, no data can be copied into a file. = No intrusion of viruses
- Since data reading is impossible, files cannot be fetched by unscrupulous means. = Prevention of information leakage

Low resources

Industrial controllers have been optimized where conditions are rigorous in terms of hardware resources. Therefore, operation with low resource utilization is possible.



File access control with extensions

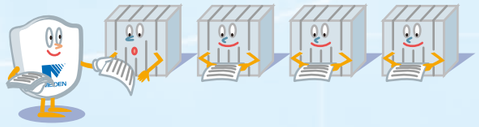
For files with extensions that are considered liable to be attacked by hackers, intrusion of malicious files can be prevented by controlling the usage-enabled files in advance.

Audit log functions

If there is any action that violates the preset white list, information about the violation is recorded.

Simultaneous distribution of policy

For controllers under the same environment, the same white list can be distributed all at once. By taking such an action, it is possible to unify the security level easily.



※AhnLab WhiteShield is the product of AhnLab, Inc. and it is also the registered trademark in the Republic of Korea.
※Other names of companies and merchandise found elsewhere in the text are the trademarks and registered trademarks of the respective organizations. Information contained herein is subject to modification and change without preliminary notice.