conpal®

Information Security Systems.

conpal AccessOn

Enforcement of security policies - by controlling resources and applications

The rapid and straightforward integration and maintenance of different end devices in the IT infrastructure is increasingly playing a key role in the performance of an organization - with many potential weaknesses: sensitive data stored on mobile devices, desktop PCs and network servers requires secure access, a comprehensive configuration protection and a complete access control. Secure authentication and access control are now among the most important requirements of a company's IT security policy. This includes, among other things, controlled access to end devices, files and the corporate network, as well as protection against unauthorized installation of hardware and software. IT organizations are calling for a solution that enables a unified security policy across the IT environment, without reducing user productivity and increasing the administrative burden. conpal AccessOn meets these criteria. Whether the end user works with a PC, a notebook or in a terminal server environment, the conpal AccessOn security modules provide a reliable and cost-effective way to a controlled, secure work environment.

conpal's product, AccessOn, consists of three module modules with the following functionality:

- ➲ The base module provides the functions for administration and logging. The intelligent administration concept implemented here tries to keep the expenses as low as possible for an administrator.

- ➲ The Application Specific Access Rights (ASAR) module allows fine-tuning of user rights regarding the use of data and directories by applications. Applications do not need to be adjusted for this. Even legacy applications can be operated i n a secure environment. Data import and export are easily controlled.

- ➲ The Plug and Play Management Module provides centralized management and control of all Plug and Play devices in a company, including a remote sharing feature, for rapid response to "ad hoc" adaptations in distributed environments.

About *conpal*

conpal specializes in the management of user infrastructure and the development of secure system environments. In this context, the company offers solutions for identity management, enterprise SSO, strong authentication and control of IT infrastructure. Our solutions can easily be integrated into existing system landscapes and are transparent to the user. Our customers appreciate the reliability and simplicity as well as the long-term investment security of our security solutions. We stand for recognized product quality, ease of use of the software, excellent support and a market-driven offer.

Advantages

High Security

- ✚ Simple implementation and enforcing of uniform and consistent security policies when using different endpoints

- ✚ Improved system security and stability by preventing unauthorized installation or execution of programs

- ✚ Protection against unauthorized access and misuse

- ✚ Protection against the use of unauthorized peripherals

- ✚ Protection against unauthorized import and export of data

Easy Integration

- ✚ Seamless integration into existing infrastructures such as Active Directory

- ✚ Quick realization / creation of a policy by supplied rights profiles

- ✚ Reduced help desk costs by maintaining system integrity and security

Easy to use

- ✚ No training required for end users

- ✚ Protection of configurations and directory structures increases the robustness of systems, especially in mobile systems

- ✚ Secure user guidance through automatic allocation of resources

Features

Basic Module

- "Configuration Viewer" provides an overview of the current settings for a revision

Plug & Play

- Controls the use of Plug and Play devices
- Prevents the use of unknown devices and the use of unauthorized devices of known types
- Plug and play management prevents data and applications from being introduced undetected into the IT infrastructure and thus endangering the stability of the IT environment
- Enforced Drive Mapping automatically assigns predefined drive letters to storage devices
- The check is independent of the bus or protocol
- Central administration of the module allows or prohibits access to individual Plug & Play devices or entire device classes
- Simple exception handling: new PnP devices can be allowed in the administration by accessing remote workstations
- integrated access control from the initial detection of the USB device to data access

Application-Specific Access Rights (ASAR)

- Extension of the access rights of the file system. Adds the level of the application to the access rights. Only the execution of defined applications is allowed
- Administrators can implement a three-dimensional security concept with ASAR. The assignment of rights can be defined according to users, data and applications
- Application-specific access rights increase security by identifying processes. No changes to the applications are necessary
- Security for all applications (including legacy applications)
- Configurable rights inheritance for "child processes"

System Administration

Windows Installer (MSI)-based installation

- Configuration via Microsoft Management Console (MMC)
- Does not require special, additional server components
- Policy distribution through
  - Active Directory or compatible solutions
  - Alternative distribution mechanisms based on XML

System requirements

Operating Systems

- Microsoft Windows 7
- Microsoft Windows 8.1 (32/64 Bit)
- Microsoft Windows 10 (32/64 Bit)
- Microsoft Windows 2003 Server Standard Edition
- Microsoft Windows Server 2008
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2

Network

- All networks supported by Windows

Complementary products

- *conpal* AuthomaticOn (SSO):
  Enterprise Single Sign-On for automated registration of authorized users to different platforms and applications.
- *conpal* CerbalOn:
  strong authentication with Smartcards and USB Tokens. conpal CerbalOn replaces traditional Windows passwords with certificate-based values, protecting users from compromising their operating system passwords (no server infrastructure required).

Third-party manufacturers

- Novell ZENWorks
- Citrix MetaFrame, including Terminal Server
- VMware

Interfaces

- XML

Supported Standards/Protocols

- Active Directory
- MMC

Language versions

- English, German

New Functions

- PnP Wildcards
- Windows 10 Support
- File recognition via signatures (hashes)
- Unique application recognition by checking hash signatures

Contact

conpal GmbH
Dornhofstr. 67-69
63263 Neu-Isenburg
Germany
Phone +49 (61 02) 75 198-0
Fax   +49 (61 02) 75 198-99
info@conpal.de

www.conpal.de