ecos

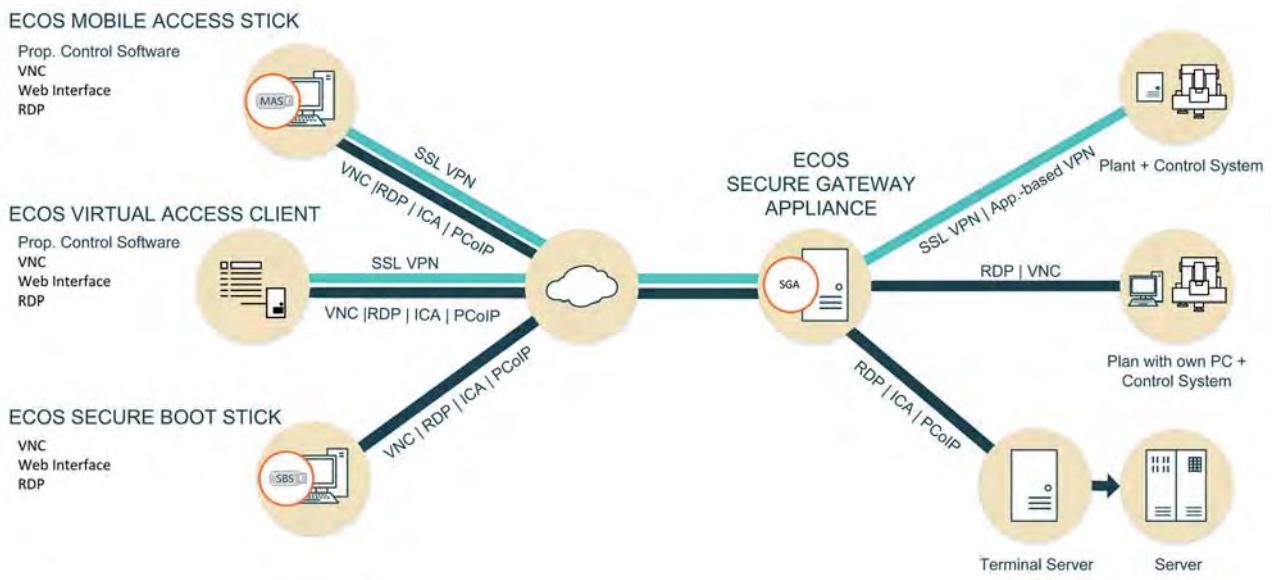
REMOTE MAINTENANCE

Highly secure access to industrial machinery and machine control systems

- Highly secure
- Easy and flexible usage
- Central management

Remote maintenance of industrial machinery and machine control systems

To maintain plants and control systems, organizations and companies often rely on the manufacturer's staff or specialized service companies. But creating the necessary accesses also increases the potential of risks. Both accesses and connection paths must therefore be highly secure to protect the organization from spying and sabotage.



Application scenario remote maintenance

External access to plants

Access to plants can be handled in different ways depending on the construction type and the control systems. Plants with dedicated control systems are often operated by VNC client or web interface. Plants equipped with an own control computer are usually accessed via VNC or remote desktop.

The appropriate solution for any requirement

Depending on your application scenario and requirements ECOS provides appropriate solutions which are randomly combinable and centrally administrable.

ECOS MOBILE ACCESS STICK – simple, flexible, safe

By starting the application from the Mobile Access Stick the authorized service engineer connects securely to the plant control systems he is eligible for. Any PC, Mac or Intel-based tablet is suitable and the usage is absolutely free of installation or configuration.

Mobile Access Stick contains all software required to establish an application-based VPN connection and control the plant systems by RDP, VNC or web interface. The stick can also be provided with the particular browser and pre-installed plugins which the web interface has been customized for. Mobile Access Stick contains all software required to establish an application-based VPN connection and control the plant systems by RDP, VNC or web interface. The stick can also be provided with the particular browser and pre-installed plugins which the web interface has been customized for.

ECOS VIRTUAL ACCESS CLIENT – Ad hoc access

Largely identical to the Mobile Access Stick, ECOS VIRTUAL WEB CLIENT is a software-only solution. Accessible through a standard browser all software components required for a secure access are loaded ad hoc into the main memory. As with the Mobile Access Stick, this solution too requires neither installation nor configuration.

ECOS SECURE BOOT STICK – Highly secure on any PC

ECOS SECURE BOOT STICK has been designed to provide access under the highest security requirements. While booting any PC or Mac from the stick, the local hard drive won't be addressed and therefore no malware potentially present on the computer can be activated. This ensures 100% separation of usage of the PC for maintenance purposes from other types of usage. The Secure Boot Stick features several security mechanisms to protect from malware on the computer in usage or from online attacks and manipulation, even if the stick gets into the wrong hands.

Easy and flexible usage

All access solutions provided by ECOS are directly usable on any PC, Mac or Intel-based tablet without the need to deal with an installation or configuration of a software. Service engineers therefore no longer rely on a particular notebook for servicing purposes.

Central dial-in and administration

ECOS SECURE GATEWAY APPLIANCE (SGA) acts as a central access point for the connection to the respective plant. The summary only shows the plants the service engineer in question is personally authorized to access at that moment. The administrator in charge can assign or revoke access permissions to systems or data and set access times in a granular permission assignment.

ECOS MOBILE ACCESS STICK

Through a linkage to Active Directory or other directory services, user and permissions can be synchronized and even controlled entirely remotely by AD. Part of the management and basic prerequisite for a revision-proof operation of a remote maintenance solution is a comprehensive reporting module. It allows at any time to track which service engineer accessed which plant and at what time. Besides a broad selection of pre-defined reports the administrator also has access to all login data with the integrated report editor and can generate own evaluations and graphics.

Distributed locations

ECOS also provides appropriate solutions for site networking. For this purpose, an ECOS SECURE GATEWAY APPLIANCE can be set up at the respective location. Optionally, an ECOS VPN GATEWAY firmware can be made available to both Intel and ARM-based hardware. This solution is particularly suitable when operating VPN routers mounted on top-hat rails.

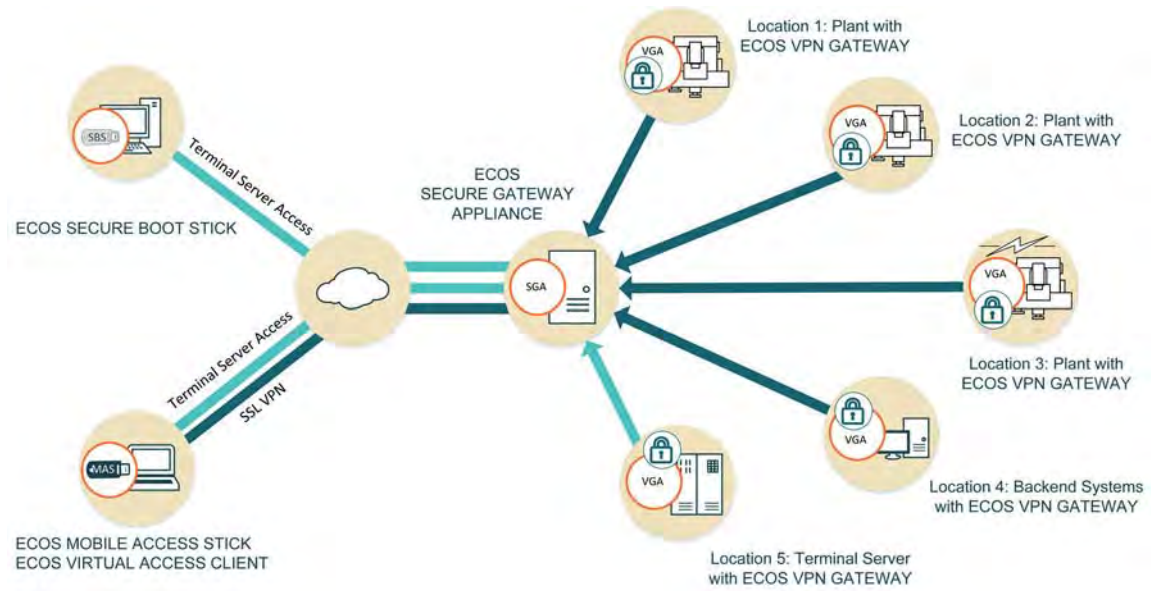
Thanks to ECOS SECURE GATEWAY APPLIANCE, all accesses and gateways can be administrated by one management interface. The maintenance engineer connects to the plant to be serviced through a central dial-in without having to remember different login data. However, it is also possible to set up decentralized access points around the globe. SGA even helps resolving identical IP ranges from the same location, which often constitutes a challenge when implementing new locations.

Protection against hacking attacks and espionage

ECOS solutions display a number of security features to protect plants and organizations against threats and potential harm.

Protection against malware on the end device

The plant control system is, as far as possible, accessed through an application-based VPN tunnel which is usable by the



Application scenario different locations

scheduled applications, but not by potential malware on the guest computer. In case the service engineer should need a transparent SSL VPN access, for example for a proprietary plant software or to install new firmware, it can be coupled to a particular hardened computer.

ECOS SECURE BOOT STICK ensures 100% separation of maintenance usage of the guest computer from other purposes as the local hard drive isn't addressed. Moreover, the specially hardened ECOS Secure Linux will take control of the connected periphery, so even BIOS or UEFI malware will pose no threat.

Protection against sabotage

To protect users from sabotage, it is important to ensure that only authorized personnel have access to the respective plant. That's the role of the strong two-factor authentication. For the Mobile Access Stick and the Secure Boot Stick, this authentication is ensured through a certificate tied to the stick's hardware ID. Thus, besides username and password, all users will need to have their personal ECOS stick at hand for a secure authentication at the gateway. Both products are optionally also available with an integrated smart card or are implementable into an infrastructure with an already existing smart card.

ECOS VIRTUAL ACCESS CLIENT uses one-time passwords (OTP) sent by SMS or e-mail to the user's cell phone, soft token or the traditional OTP token for two-factor authentication. Additionally, all accesses can be secured with a one-time password with limited duration and communicated case-specifically to the maintenance engineer by phone.

The granular permission assignment of the management appliance allows to assign, revoke or limit in time ad hoc permissions for different plants. On the plant-side, the establishment of the internet connection and/or the VPN tunnel can be authorized or restricted by switch if required.

Protection against spying

All ECOS solutions use a VPN connection with a freely configurable encryption method. It is also ensured that no exploitable trace will be left on the guest computer. While, with the Secure Boot Stick, it's the encapsulated environment that provides protection, Mobile Access Stick and Virtual Web Client use their own sandbox to execute all clients and applications.

Protection against manipulation

To protect against any firmware and application manipulation, all processes are digitally signed. For ECOS SECURE BOOT STICK, firmware and applications additionally lie on a write-protected and encrypted partition.

Easy, flexible and secure

All ECOS solutions for highly secure access to industrial plants and machine controls are implementable within a very short time into the existing infrastructure. Thanks to the central administration of a random number of locations and accesses, this solution constitutes a considerable relief for technical departments and IT.

For the individual service engineer, ECOS solutions provide a flexible access to the relevant plants regardless of the location or the devices being used. All plants are reachable through a central access point.

But the most important point: Ensuring safety and protection against attacks and spying. All ECOS solutions therefore provide a cascade of security measures to protect plants and organization from damages.

[1]The usage of a transparent SSL VPN connection instead of an application-based VPN connection requires at first usage on an end device the installation of a software component.

Your benefits at a glance:

+ Highly secure remote access for internal/external maintenance engineers
+ No installation[1], no configuration
+ Central user and permission administration
+ Temporally definable service slots
+ Central dial-in and administration for distributed locations
+ Container for software and document distribution
+ Protection against hacking attacks and industrial espionage

Performance Overview

ECOS MOBILE ACCESS STICK

- No installation*, no configuration
- Applications: VPN client, RDP client, Citrix Receiver, VMware Horizon, VNC, Firefox
- Implementation of customer-specific applications possible
- Strong certificate-based two-factor authentication
- All software executed within a sandbox
- VPN connection on application level, alternatively: SSL VPN connection
- Container for software and document distribution
- Software in German and English (pre-configurable)
- For use under Windows 7, Windows 10 and Mac OS X

ECOS VIRTUAL ACCESS CLIENT

- Hardened ECOS SECURE LINUX operating system
- Drivers for all popular PCs with Intel Pentium 3 or AMD Athlon and more, Intel-based tablets and all popular Macs with Intel processor, UEFI Secure Boot support
- Connection through LAN, WLAN, UMTS, LTE incl. browser-based hotspot login
- Applications: RDP client, Citrix Receiver, VMware Horizon, VNC, NoMachine, TeamViewer, Firefox, w/ or w/o Java support
- Connection to any gateway via IPsec, Open VPN or https
- Integrated IPsec and SSL VPN client
- Strong certificate-based two-factor authentication
- Read-only partition for firmware and applications
- 256 BIT AES encryption of firmware, applications and user parameters
- Digitally signed boot loader, firmware and applications
- Signature verification in chain-of-trust process
- Integrated firewall as protection against attacks within the same network
- Prevents from usage in virtual environments
- Software in German and English (pre-configurable)

ECOS SECURE BOOT STICK

- Hardened ECOS SECURE LINUX operating system
- Drivers for all popular PCs with Intel Pentium 3 or AMD Athlon and more, Intel-based tablets and all popular Macs with Intel processor, UEFI Secure Boot support
- Connection through LAN, WLAN, UMTS, LTE incl. browser-based hotspot login
- Applications: RDP client, Citrix Receiver, VMware Horizon, VNC, NoMachine, TeamViewer, Firefox, w/ or w/o Java support
- Connection to any gateway via IPsec, Open VPN or https
- Integrated IPsec and SSL VPN client
- Strong certificate-based two-factor authentication
- Read-only partition for firmware and applications
- 256 BIT AES encryption of firmware, applications and user parameters
- Digitally signed boot loader, firmware and applications
- Signature verification in chain-of-trust process
- Integrated firewall as protection against attacks within the same network
- Prevents from usage in virtual environments
- Software in German and English (pre-configurable)

ECOS SECURE GATEWAY APPLIANCE

- Virtual appliance for operation under VMWare, Citrix XenServer, Hyper-V, Oracle VM VirtualBox or a dedicated hardware
  - Integrated VPN gateway (IPsec, SSL VPN)
  - Unlimited number of VPN users
  - Incl. 10 concurrent VPN tunnels, freely extendable
- Central management of all ECOS products
  - User and permission management on user, group and role level
  - Authorization assignment for target systems, with distributed servers
  - Sharing of local devices such as storage media and printers
  - Synchronization with AD or other directory services
  - Remote permission assignment and revocation
  - Limitable service times
- Certificate management
  - Integrated CA (Certificate Authority)
  - Alternatively connection to an existing PKI
  - Certificate rollout on smart cards
  - Provision of a CRL or an OCSP server
  - Central password policy
  - One-time password system (OTP) incl. Radius server. Supports token, soft token, one-time password per SMS and manual one-time password generation
- Smart reports
  - Pre-defined reports
  - Own report editor
- Token lifecycle management
  - Easy Enrollment
  - Central access creation and suspension
  - License transfer for lost sticks
  - Controllable by AD
- Remote update of access solutions
  - Central update server
  - Distribution to particular users, groups or all users
- Client administration
  - Separate admin logins
  - Separate AD connection
  - Separate PKI connection
  - Separate CAs
- Admin interface
  - Web based
  - User-specific permission assignment (admin, helpdesk, personnel management etc)
  - All system management features optionally controllable via HTTP API
  - Redundant and highly available in combination with HA module

High-availability module (for ECOS SGA, ACA, CAA)

- Redundant operation of two or more appliances
- Automatic load balancing

ECOS TECHNOLOGY GMBH
Sant-Ambrogio-Ring 13a
D-55276 Oppenheim

Phone: +49 (6133) 939-200
E-Mail: info@ecos.de
Internet: www.ecos.de

129.AF.2017/06.EN.01