



SE46 Local Whitelist Manager

Protecting business critical systems from the impact of unauthorized software running on production devices is essential. Production stoppages in environments operating 24/7 not only introduce delays in services and additional costs, but can have a knock on affect on product quality, operational safety and profit margins. That's why many leading manufacturers of hospital equipment, automotive plant and industrial robots ship their devices pre-configured with SE46 Application Whitelisting from Cryptzone.

SE46 LWM has been developed in collaboration with system manufacturers to address the business demands within market sectors, such as medical device suppliers and manufacturing/process industries.

SE46 LWM is typically preinstalled by manufacturers and delivered as part of the device to the end customer. In this way the customer can safely make changes to devices during their operational life without jeopardising the manufacturer's warranty.

SE46 Application Whitelisting is a state-of-the-art application whitelisting solution

SE46 Application Whitelisting is a state-of-the-art application whitelisting solution, which provides advanced threat protection to ensure software integrity and security for endpoint devices. By only allowing certified solutions to execute, SE46 Application Whitelisting prevents known and unknown viruses or any unauthorized programs from ever running.

Local certification

SE46 Local Whitelist Manager (LWM) provides organizations with a simple way of locally certifying additional software or hardware for particular devices without accessing the central SE46 Management Server.

Using SE46 LWM an authorized administrator can unlock a system, install and certify new software and hardware before locking it down again for production use. The certification has limited authority, so is non-transferable to other devices.

How SE46 works

1. Unlock SE46 client
2. Reboot if requirement of new software
3. Check new executable to be certified
4. Certify and lock down
5. Run in production mode



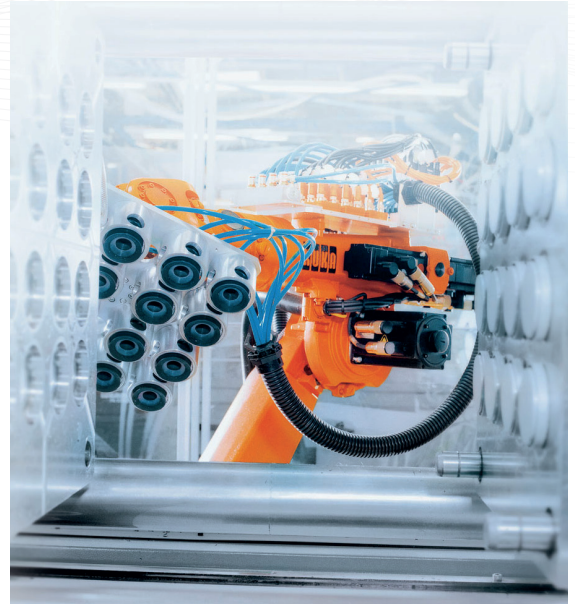
Changes to a system can be done locally on the device

SE46 LWM is particularly suitable for devices that pass through multiple organizations in a supply chain in order to have additional software installed before delivery to the end customer. The manufacturer is able to guarantee only changes by authorized third parties are made to its devices between shipping and installation.

Changes to a system can be done locally on the device by an approved administrator who has the right service key. The service key is generated by the manufacturer, although a local key generator can be handled by a distributor or an end customer if permitted.

Security & Traceability

A device manufacturer can deploy a key structure that is appropriate for each customer. All events and changes to a system are logged and time stamped for full auditability. Locally added software and hardware is only given a local certificate.



Benefits of using SE46 LWM

- Secured system from manufacturer to production environment
- Low CPU usage and disk space
- Prevents any unauthorized system modifications
- Blocks unauthorized hardware devices and ports
- Logs all software changes (what, when & who)
- Stand-alone solution requires no look-ups to external server for updates
- No need for patching
- Strong security with certificates and keys
- Role based access through local, enterprise & service keys
- Fast and simple installation

Visit www.cryptzone.com/case-studies to find out how SE46 Application Whitelisting is helping customers protect their systems:



Elekta AB - a supplier of neuroscience products and solutions uses SE46 Application Whitelisting on its Gamma Knife product to protect patient safety.



KUKA Roboter Gmb - a market leader in the supply of industrial robots for the automotive industry has adopted SE46 Application Whitelisting to improve security and system reliability.



Visma - a leading provider of business software and services for accounting and administration uses SE46 Application Whitelisting to prevent cyber-attacks on critical systems ensuring data protection and business continuity.



Cryptzone solutions mitigate information security risks in the key areas of Policy Compliance, Content Security, Secure Access and Endpoint Security.

International Headquarters

Cryptzone Group AB
Drakegatan 7,
SE-412 50 Gothenburg,
Sweden

www.cryptzone.com
info@cryptzone.com

Regional Offices

Sweden
Tel: +46 (0)31 773 86 00

United States
Tel: +1.949.279.6177

United Kingdom
Tel: +44 (0)370 013 1600

Partner information:

For more information go to
www.cryptzone.com/partners