ACE Lite

Security and Compliance Assurance

Date: 28 April 2021

Table of Contents

Data Protection

Output file content & its protection

ACE Lite executable extracts operating system level information, that is required for compliance evidence for certifications such as PCI DSS, ISO 27001, SOC2 and HealthCare etc. The output file (.enc) created after running ACE Lite is in a encrypted format.

To view the information that ACE Lite extracted from your machine, you can follow the instructions below.

- Login to SkyCAM portal.. Navigate to "Compliance Scanner" page. Download the extractor and run it on the host machine following commands/instructions given in the ACE Lite page on SkyCAM portal..
- If you want to confirm what is being uploaded by you, you can verify it by running following commands to de-crypt the data ***"acelite.exe -d"*** for Windows and ***"./acelite -d"*** for Linux.
- A decrypted text file (.txt) gets created with information that ACE Lite gathered from host machine.

To ensure that the data created on your system is securely uploaded to the SkyCAM portal by you, we implement security at following two layers:

1. Storage: Files created and uploaded to SkyCAM are saved with 256-bit AES encryption. When a file is uploaded, it is encrypted before being copied to its storage location. The file encryption keys are not stored on the same server with the files themselves, ensuring that someone with physical access to our storage servers has no access to the files contained on their hard drives.
2. Transmission: When transferring evidence files (.enc), it is important to use encryption to ensure that any outside sources cannot read the data contained within the files. All file transfers through the SkyCAM are encrypted using 2048-bit RSA public key. This is the same security used by banks and many e-commerce sites. TLS works by establishing a private connection and each end of the connection is authenticated before transfer begins. Data traveling between these endpoints can only be decrypted by the intended recipient by using unique decryption keys.

Information that we collect.

ACE Lite collects compliance information such as running processes, user security policy, system level settings and values within application configuration files, password complexity, system settings, registry values and most settings that can be described in a Windows policy file. In order to provide our solutions and services to you, we must necessarily collect this information automatically.

How long do you keep data for?

If you are a customer, we will retain your information for as long as your account is active, or as needed to provide you products and/or services as per the signed contract. In all other cases, we will retain and use your information as necessary for legitimate business reasons, including as needed to comply with our legal obligations, to resolve disputes, and to enforce our agreements. When we have no ongoing legitimate business reason to process your information, we will securely delete the data.

Digital signing of executable files

Data Protection for Ace Lite executable file have a digital signature. Code signing employs digital IDs, also known as certificates. Having a valid digital signature ensures the authenticity and integrity of an executable file. It identifies the software publisher as ControlCase to the person who downloads or starts it. However, it does not mean that the user or a system administrator implicitly trusts the publisher. A user or administrator must decide to install or run an application on a case-by-case basis. The factors of their decision are based on their knowledge of the software publisher and application. By default, a publisher is trusted only if its certificate is installed in the Trusted Publishers certificate store.

Digitally signed executables also ensure authenticity and integrity.

- Authenticity: This tells the user (and the computer) where the software came from. This is the "who." Authenticity ties ControlCase's identity to executable. Because no one else has our key, no one else can sign software that claims to be from you.
- Integrity: Demonstrates that the code has not been modified. The digital signature does not just tell devices who signed the software, but what they signed. This allows a computer to know if the code has been changed at all since it was signed. This prevents attacks that rely on modifying legitimate executables. This will also alert users to file corruption which may happen during downloading.

This prevents a large number of attacks that rely on unauthorized/malicious modification of code, fraudulent software, and purpose-built malware.

Execution

ACE Lite executable does not install any component in the host machine. The purpose of executable is to read the system level information, write it into an encrypted file and end its process thread once encrypted file is created.

ACE Lite does not create any stale thread or process in the background once the extraction is complete.

Performance

As ACE Lite executable utilizes standard inbuilt operating system level commands to extracts system level information, the consumption of CPU and memory of the host machine shall be equal to consumption of running standard operating system level commands.

We recommend running the executable in your test machine once to check the performance parameters.

ACE Lite is a one-time run executable and does not create any background process or thread to consume resources.

Commands

ACE Lite executable contain standard inbuilt operating system level commands to fetch the information as required. As sample, some commands are as follows.

- netstat -putan
- sudo cat /etc/passwd
- sudo auditctl -l
- sudo ps cax
- sudo rpm -qa
- sudo uname -a
- sudo lastlog -b

Dependencies

There is no package, version or installed software dependencies to run ACE Lite for Windows and Linux operating system.

For database such as Oracle, Oracle instant client shall be required to run ACE Lite to collect database evidence.

Application Security and Compliance

Encompassing every phase of the product development lifecycle, ControlCase Software Security Assurance is ControlCase's methodology for building security into the design, build, testing, delivery, and maintenance of its products. ControlCase' s goal is to ensure that ControlCase's products, as well as the customer systems that leverage those products, remain as secure as possible.

ControlCase Secure Coding Standards are a guide for developers in their efforts to produce secure code. The standards discuss general security knowledge areas such as design principles and common vulnerabilities and provide specific guidance on topics such as data validation, data privacy, user management, and more.

Security testing at ControlCase includes both functional and non-functional activities for verification of product features and quality. Although these types of tests often target overlapping product features, they have different goals and so are carried out by different teams. Functional and non-functional security tests complement each other to provide comprehensive security coverage of ControlCase.

Security Code Reviews and Application penetration testing is regularly performed on products built by ControlCase.