

Klipfolio Dashboard Security

How Klipfolio protects your information, your users, and your business

The integrity of your information is vital to your reputation and success. So when we designed and built Klipfolio Dashboard we made security a priority. To ensure the integrity of Klipfolio dashboards and the Klips that make up those dashboards, Klipfolio integrates with existing security infrastructures and includes all of the capabilities and features essential in a secure, business-critical application you can depend on.

Easy Integration with Security Infrastructures

Klipfolio ties into your existing gateways, firewalls, Microsoft Active Directory, LDAP services, security policies, and group policies to ensure that data is protected from source to destination, and can be used by only properly identified and authorized personnel.

For communication, Klipfolio supports SSL, TLS, and Kerberos. HTTP and HTTPS authentication are provided using basic, digest, challenge-response, and SSPI technologies. User credentials are input as needed using session-oriented login components in Klips.

Klipfolio Dashboard is a digitally signed application using Microsoft Authenticode technology to help detect tampering. To provide access to advanced functionality and prevent tampering, Klips can be digitally signed and encrypted using RSA PKCS-1 and RC-5. A digitally signed Klip makes its application logic available to view but prevents it from being modified. An encrypted Klip hides that logic in a signed and encrypted block. When Klipfolio Dashboard loads a digitally signed Klip, it validates the signature block against the loaded file. If they don't match, it assumes the script has been tampered with and doesn't run it.

Klipfolio security includes:

- Microsoft Active Directory (SSPI)
- Cryptographic services
- Strong JavaScript sandboxing
- Digital rights management
- A granular permissions model

It supports industry standard protocols:

- SSLv3
- TLS
- Kerberos

And it incorporates important standards:

- PKCS-1
- SHA-1 and SHA-256
- RC-4 and RC-5
- X-400, X-500 and X-509

Klipfolio Sandboxing

To ensure security in your application environment, Klipfolio has at its core a sandboxing solution that is independent from those in web browsers, such as Microsoft Explorer or Firefox, and from Java environments, such as Sun's Java Plug-in.

The sandbox system provides independent runtime environments for the JavaScript code executing in each Klip in a Klipfolio dashboard. It employs a four-tiered approach that:

- creates a discrete runtime and JavaScript context for each Klip
- populates each context with non-shared objects
- provides a set of rights for each runtime based on the digital signature block (or lack of one) to determine permissions and the availability of resources
- ties the JavaScript's underlying native objects to a Klip, to manage the data and rights of the object

How Klipfolio Dashboard Addresses Your Security Challenges

Potential Security Issue	Klipfolio Solution
Application tampering. Modification or reverse engineering can allow the distribution of a malicious version of an application, and potential account compromise or malware infection.	Runtime hardening. Klipfolio accommodates strong cryptographic techniques, such as Microsoft's AuthenticCode, so that you can include digital signatures. Klipfolio's self-validation code technology significantly increases the odds that improper code modification can be detected and prevented, even if the modified application is re-signed.
Data interception. Without transport layer encryption (SSL), data could be intercepted by a third party, leading to possible account compromise and disclosure of sensitive information.	Secure data transmission. Klipfolio's four-tiered validation of the chain of trust involved in signature systems, such as SSL, coupled with resistance to reverse engineering, improves the security of data transmissions.
Application hi-jacking. If access control mechanisms are inadequate, unauthorized individuals might be able to use already active instances of an application.	Session timeouts and logout options. With Klipfolio, deployment managers and users can ensure automatic log out after a specified amount of time idle.

Protecting Sensitive and Private Information

To prevent unauthorized access to intellectual property in the form of executable code, Klipfolio ensures that four things happen:

1. The amount of sensitive data and intellectual property rendered as code is minimized
2. Embedded intellectual property is protected from cursory examination
3. Application hardening techniques increase the difficulty of reverse engineering the algorithms and keys involved in decryption/de-obfuscation
4. Runtime hardening techniques increase the difficulty of discovering the intellectual property through forensic analysis of RAM images and stepwise debugging

Education – The Best Security of All

Klipfolio Dashboard has the security features and capabilities needed to protect the data in your dashboards. But the best insurance against unwanted use of an application is always an educated user.

Make sure your users are aware of the need for security, and know how to ensure the security of their systems and dashboard sessions. Educated users rarely leave their computers and Klipfolio Dashboards vulnerable to misuse.

For more information about Security, or any other aspect of Klipfolio products or services, visit www.klipfolio.com or call us worldwide at +1 613 233 6149.