



Klipfolio Dashboard Security

Klipfolio works with your enterprise security infrastructure to protect against unauthorized access to critical data.

Audit and Compliance

Tighter compliance regulations coupled with tougher penalties for data breaches has raised the profile of who can access company data. Klipfolio Dashboard has been designed and built with security as a priority. To ensure the integrity of Klipfolios Dashboard and the data in the Klips that make up those dashboards, Klipfolio Dashboard architecture integrates with existing security infrastructures to ensure only authenticated users can view or update data.

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 only be accessed by properly authenticated users.

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 minimizes the possibility of displayed data being vulnerable to man-in-the-middle-attacks. It is a digitally signed application using Microsoft Authenticode technology to help detect tampering. To provide access to advanced functionality and prevent tampering, Klips can also 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 obfuscates its logic in a signed and encrypted block.

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*

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 prevents the Klip from being executed.

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

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

How Klipfolio Dashboard Addresses Your Security Challenges

Potential Security Issue	Klipfolio Solution
<p>Application tampering. Modification or reverse engineering can allow the distribution of a malicious version of an application, and potential account compromise or malware infection.</p>	<p>Runtime hardening. Klipfolio accommodates strong cryptographic techniques, such as Microsoft's AuthentiCode, 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.</p>
<p>Data interception (man-in-the-middle-attacks). Without transport layer encryption (SSL), data could be intercepted by a third party, leading to possible account compromise and disclosure of sensitive information.</p>	<p>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 and reduces the possibility data being compromised.</p>
<p>Unauthorized Access. If access control mechanisms are inadequate, authorized users may have access to data for which they do not have the correct privileges. Unauthorized individuals may be able to use already active instances of an application to view data.</p>	<p>Role Based Access Controls (RBAC). With Klipfolio, deployment managers can distribute Klips that are easily authenticated against Active Directory or LDAP to ensure the correct level of privilege access. Session timeouts can automatically logout users after a specified amount of time idle.</p>

Education – The Best Security of All

Klipfolio Dashboard has been designed with advanced security features to protect the data contained in your dashboards and limits access to information based upon role and user authentication.

It is good practice to educate users on the responsible use of technology and the importance of security as it applies to their role. They should be accountable for access to their systems and application sessions.

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.