

What is the difference between "basic auth" and "form-based auth"?

THE INFORMATION IN THIS ARTICLE APPLIES TO:

- EFT Server, version 6.0 and later

QUESTION

What is the difference between "basic authentication" and "form-based authentication"?

ANSWER

Basic authentication, or "basic auth" is formally defined in the Hypertext Transfer Protocol standard, [RFC 1945](#). When a client (your browser) connects to a web server, it sends a "WWW-Authenticate: Basic" message in the HTTP header. Shortly after that, it sends your login credentials to the server using a mild obfuscation technique called *base64 encoding*. When HTTPS is used, these credentials are protected, so it's not considered insecure, which is why basic auth gained widespread use over the years. The biggest problem with basic auth has to do with the logging off the server, as most browsers tend to cache sessions and have inconsistently dealt with the need to properly close and clear connection states (or sessions) so that another (different) user couldn't log back in by refreshing the browser.

Form-based authentication is not formalized by any RFC. In essence, it is a programmatic method of authentication that developers create to mitigate the downside of basic auth. Most implementations of form-based authentication share the following characteristics:

- 1) They don't use the formal HTTP authentication techniques (basic or digest).
- 2) They use the standard HTML form fields to pass the username and password values to the server.
- 3) The server validates the credentials and then creates a "session" that is tied to a unique key that is passed between the client and server on each http *put* and *get* request.
- 4) When the user clicks "log off" or the server logs the user off (for example after certain idle time), the server will invalidate the session key, which makes any subsequent communication between the client and server require re-validation (resubmission of login credentials via the form) in order to establish a new session key.

What is the difference between "basic auth" and "form-based auth"?

As with basic auth, form-based auth does not protect login credentials when connected over HTTP, therefore it is not more "secure" than basic auth in how it handles user credentials. It is however more secure when it comes to properly logging the user off after a certain period of inactivity or if the user no longer requires use of the system and decides to log out.

For details of basic auth and form-based auth in EFT Server, refer to [End-User Log In to EFT Server](#).

GlobalSCAPE Knowledge Base

<https://kb.globalscape.com/Knowledgebase/10691/What-is-the-difference-betwe...>