force-ssl

Source code of released version | Source code of development version

Purpose

This package, part of Webapp, causes Meteor to redirect insecure connections (HTTP) to a secure URL (HTTPS). Use this package to ensure that communication to the server is always encrypted to protect users from active spoofing attacks.

Meteor bundles (i.e. `meteor build`) do not include an HTTPS server or certificate. A proxy server that terminates SSL in front of a Meteor bundle must set the `x-forwarded-proto` or `forwarded` (RFC 7239) header for this package to work.

The `x-forwarded-proto` or `forwarded` header is used to determine if the connection arrived over HTTPS and a heuristic is used to guess if it's running in development. To simplify development, unencrypted connections from `localhost` are always accepted over HTTP.

We recommend this package only for deployment platforms that do not have their own ability to force SSL. If you're deploying with Galaxy, you should instead use the "Force HTTPS" setting (on the specific domain in the "Domains & Encryption" section of your application's "Settings" tab). If you're using another deployment platform, you should attempt to provide this redirection on the proxy which terminates your SSL (e.g. HAProxy, nginx, etc.), outside of Meteor and without this package.