HTTPS and HSTS

For public bodies serving their site only over HTTPS - the steps Exponential's installation guide gives (HTTPS on every name, redirects, Secure cookies, HSTS raised gradually, certificate monitoring), the settings for…

Source file: `doc/eng-us/help/government/security/https-and-hsts.md` Last changed 2026-11-04
https://doc.exponential.earth/learninminutes/exphelp/viewer/help/government/security/https-and-hsts.md

This page is for administrators and hosting teams. Many governments expect their public sites to be served only over HTTPS. HSTS (HTTP Strict Transport Security) makes browsers remember that and refuse plain HTTP to the host. In Exponential HSTS is **empty by default** and must be set by the operator once the whole site is HTTPS-only (Security standards: Known gaps).

Contents

1. The order of steps
2. HSTS settings
3. Raising HSTS safely
4. Checking
5. Related pages

The order of steps

From HTTPS everywhere:

1. Serve every name of the site over HTTPS: Velocity `[HTTPSSettings]` or its ACME support, Apache `mod_ssl`, nginx `ssl`.
2. Redirect plain HTTP to HTTPS (web server), or for individual subtrees `[SSLZoneSettings]`.
3. Set `[Session] CookieSecure=true`.
4. Turn HSTS on, short first, and raise it once everything works.
5. Keep certificates renewed and watched (`./console exp:velocity ssl show --json`, field `daysLeft`, or your ACME client's timer).

HSTS settings

Engine	Setting	Shipped
Velocity	`settings/velocity.ini [HTTPSSettings] HSTSMaxAge`, `HSTSIncludeSubDomains`, `HSTSPreload`	`HSTSMaxAge=300`
Apache or nginx with PHP-FPM	`site.ini [HTTPHeaderSettings] SecurityHeaders[Strict-Transport-Security]`	empty

For Apache or nginx, in `settings/override/site.ini.append.php`:

INI

```
[HTTPHeaderSettings]
SecurityHeaders[Strict-Transport-Security]=max-age=300
```

The kernel sends it only over HTTPS. Clear the INI cache and reload PHP afterwards.

Raising HSTS safely

A browser remembers HSTS for the whole period and refuses plain HTTP to that host, **even after you lower the value**.

Stage	Value	Move on when
1	`max-age=300` (5 minutes)	every page and asset of every name works over HTTPS
2	`max-age=86400` (1 day)	a week without problems
3	`max-age=2592000` (30 days)	a month without problems
4	`max-age=31536000` (1 year)	every name is served over HTTPS for good

Add `includeSubDomains` only when **every** subdomain of the domain is HTTPS-only: on a government domain that may include services run by other teams. Preload lists are hard to leave; decide with whoever owns the domain.

Checking

Shell

```
curl -sI http://www.example.gov/ | head -3                        # a redirect to https
curl -sI https://www.example.gov/ | grep -i strict-transport
curl -sI https://www.example.gov/user/login | grep -i set-cookie   # Secure; HttpOnly; SameSite=L
ax
```

Behind a proxy that terminates TLS, the kernel must know the request was HTTPS: configure `TrustedProxies[]` (see "Proxies and trusted headers"), or `CookieSecure=true` signs users out on every page.

Related pages

- 13.9 Security headers and HTTPS
- Velocity HTTPS and certificates
- Going live: hosts and HTTPS
- Free documentation: this page is free to copy, translate and improve under the GNU FDL 1.3.

> **Become an Exponential Partner**
>
> Partners share their information, provide funding, contribute back and develop the products with us, and that is how Exponential grows. A partner website and dashboard are planned for mid-2027: please become a partner today to speed up our growth rate and land new features faster.
>
> Partners: start here | How to apply

Exponential Copyright © 1998-2026 Exponential Foundation and 7x
Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.3 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled "GNU Free Documentation License".
This documentation is free documentation, licensed under the GNU Free Documentation License 1.3 or later:
https://www.gnu.org/licenses/fdl-1.3.html.