

```
### SILVERSTRIPE START ###
```

```
# Deny access to templates (but allow from localhost)
```

```
<Files *.ss>  
    Order deny,allow  
    Deny from all  
    Allow from 127.0.0.1  
</Files>
```

```
# Deny access to IIS configuration
```

```
<Files web.config>  
    Order deny,allow  
    Deny from all  
</Files>
```

```
# Deny access to YAML configuration files which might include sensitive information
```

```
<Files ~ "\.ya?ml$" >  
    Order allow,deny  
    Deny from all  
</Files>
```

```
# Route errors to static pages automatically generated by SilverStripe
```

```
ErrorDocument 404 /assets/error-404.html  
ErrorDocument 500 /assets/error-500.html
```

```
<IfModule mod_env.c>
```

```
# Ensure that X-Forwarded-Host is only allowed to determine the request  
# hostname for servers ips defined by SS_TRUSTED_PROXY_IPS in your _ss_environment.php  
# Note that in a future release this setting will be always on.
```

```
SetEnv BlockUntrustedIPs true
```

```
</IfModule>
```

```
<IfModule mod_rewrite.c>
```

```
# Turn off index.php handling requests to the homepage fixes issue in apache >=2.4
```

```
<IfModule mod_dir.c>  
    DirectoryIndex disabled  
</IfModule>
```

```
SetEnv HTTP_MOD_REWRITE On
```

```
RedirectToFinalPage On
```

```

RewriteCond %{REQUEST_URI} cache/. *
RewriteRule cache/(. *)\.html / [R=301,END]

```

```

RewriteCond %{QUERY_STRING} clickTAG=
RewriteRule (. *) /$1? [R=301,END]

```

```

RewriteCond %{REQUEST_METHOD} ^GET|HEAD$
RewriteCond %{QUERY_STRING} ^$
RewriteCond %{REQUEST_URI} /(.*[^/])/?$
RewriteCond %{DOCUMENT_ROOT}/cache/%1.html -f
RewriteCond %{REQUEST_FILENAME} !-f
RewriteRule .* /cache/%1.html [END]

```

```

RewriteCond %{REQUEST_METHOD} ^GET|HEAD$
RewriteCond %{QUERY_STRING} ^$
RewriteCond %{REQUEST_URI} /(.*[^/])/?$
RewriteCond %{DOCUMENT_ROOT}/cache/%1.stale.html -f
RewriteCond %{REQUEST_FILENAME} !-f
RewriteRule .* /cache/%1.stale.html [END]

```

```

RewriteCond %{REQUEST_METHOD} ^GET|HEAD$
RewriteCond %{QUERY_STRING} ^$
RewriteCond %{REQUEST_URI} ^/?$
RewriteCond %{DOCUMENT_ROOT}/cache/index.html -f
RewriteCond %{REQUEST_FILENAME} !-f
RewriteRule ^/?$ /cache/index.html [END]

```

```

RewriteCond %{REQUEST_METHOD} ^GET|HEAD$
RewriteCond %{QUERY_STRING} ^$
RewriteCond %{REQUEST_URI} ^/?$
RewriteCond %{DOCUMENT_ROOT}/cache/index.stale.html -f
RewriteCond %{REQUEST_FILENAME} !-f
RewriteRule ^/?$ /cache/index.stale.html [END]

```

```

RewriteCond %{REQUEST_FILENAME} !-f
RewriteCond %{REQUEST_FILENAME} !-d
RewriteRule ^home/?$ / [R=301,L]

```

```

RewriteCond %{HTTP_HOST} ^www\.(. *)$ [NC]

```

```

RewriteRule ^(.*)$ http://www.$1 [R=301,L]

```

```
RewriteRule ^(.*)$ http://%1/%1 [R=301,L]

# Enable HTTP Basic authentication workaround for PHP running in CGI mode
RewriteRule .* - [E=HTTP_AUTHORIZATION:%{HTTP:Authorization}]

# Deny access to potentially sensitive files and folders
RewriteRule ^vendor(/|$) - [F,L,NC]
RewriteRule silverstripe-cache(/|$) - [F,L,NC]
RewriteRule composer\.(json|lock) - [F,L,NC]

# Process through SilverStripe if no file with the requested name exists.
# Pass through the original path as a query parameter, and retain the existing
parameters.
RewriteCond %{REQUEST_URI} ^(.*)$
RewriteCond %{REQUEST_FILENAME} !-f
RewriteRule .* framework/main.php?url=%1 [QSA]

# If framework isn't in a subdirectory, rewrite to installer
RewriteCond %{REQUEST_URI} ^(.*)/framework/main.php$
RewriteCond %{REQUEST_FILENAME} !-f
RewriteRule . %1/install.php? [R,L]

</IfModule>
### SILVERSTRIPE END ###
```