SSL with SNI technology

Server Name Indication (SNI) is an extension to the TLS networking protocol that provides the hostname that the client is connecting to. This allows a server to support and provide multiple different SSL certificates on the same IP address and port and therefore allows multiple secure (HTTPS) websites without the need for individual dedicated IPs for each domain.

Previous version of TLS didn't recognize HTTPS requests that contained the domain name. It only worked correctly only if an IP address was provided. Because of this, it was required that each domain have a dedicated IP address if they needed to use SSL. Now, with **cPanel version 11.38 and higher**, **SNI** is available for use. Unfortunately there are a few issues that might still appear:

If you try to gain HTTPS access using a server IP address, issues may occur.

Using the server's default IP address, the connecting browser will receive the "default" certificate which is set for the server's hostname (e.g. serverX.hostname.com) and reach the first site hosted on this IP, if an HTTPS request does not have the name of the site specified.

Way to resolve the issue: order a dedicated IP address and assign it to this domain.

If SNI works for you, we will install the SSL certificate without the need for a dedicated IP address. You can obtain a dedicated IP address with any account for $24.00/year. In case you would like to request one, please open a ticket here.

The list of browsers that support SNI:

- Internet Explorer 7 or later, on Windows Vista or higher
- Mozilla Firefox 2.0 or later
- Opera 8.0 (2005) or later (the TLS 1.1 protocol must be enabled)
- Opera Mobile at least version 10.1 beta on Android
- Google Chrome (Vista or higher, XP on Chrome 6 or newer, OS X 10.5.7 or higher on Chrome 5.0.342.1 or newer)
- Safari 3.0 or later (Mac OS X 10.5.6 or higher and Windows Vista or higher)
- Konqueror/KDE 4.7 or later
- MobileSafari in Apple iOS 4.0 or later
- Android default browser on Honeycomb (v3.x) or newer
- Windows Phone 7
- MicroB on Maemo
- Odyssey on MorphO

SNI is incompatible with some old versions of the web browsers. SNI does not work on:

- Windows XP + Internet Explorer (any version) or Safari
- Internet Explorer 6 or earlier
- BlackBerry Browser
- Windows Mobile up to version 6.5
- Nokia Browser for Symbian at least on Series60
- Opera Mobile for Symbian at least on Series60

The websites will still be available via HTTPS, but a certificate mismatch error will appear.

Ways to resolve the issue: Use a different browser to access the web site. Also, the user can accept another certificate with an incompatible browser and the requested site will open up normally via HTTPS, but a different certificate will be used to establish the secured connection. Please note that all visitors with incompatible browsers will see the warning message.

Related articles

- What is my IP Address?
- Redirect from HTTP to HTTPS using mod_rewrite
- How to Enable Free Let's Encrypt SSL Certificates for Resellers
- SSL with SNI technology
- How do I upload my site before my Domain resolves?