HSTS Support

- Parallels Remote Application Server 17.0
- Parallels Remote Application Server 17.1

Parallels RAS v.17 includes support for HTTP Strict Transport Secuirty (HSTS). The HSTS settings button allows you to enforce HSTS, which is a mechanism that makes a web browser communicate with the web server using only secure HTTPS connections. When HSTS is enforced for a RAS Secure Client Gateway, all web requests to it will be forced to use HTTPS. This specifically affects the RAS HTML5 Gateway, which can normally accept both HTTP and HTTPS requests.

? ?

In RAS v.17.1 the button has been moved to **SSL/TLS** tab:

When you click the HSTS settings button, the HSTS Settings dialogue opens where you can specify the following:

- **Enforce HTTP strict transport security (HSTS)** — Enables or disables HSTS for the gateway.
- **Max-age** — Specifies the max-age for HSTS, which is the time (in our case, in months) that the web browser should remember that it can only communicate with the gateway using HTTPS. The default (and recommended) value is 12 months. Acceptable values are 4 to 120 months.
- **Include subdomains** — Specifies whether to include subdomains (if you have them).
- **Preload** — Enables or disables HSTS preloading. This is a mechanism whereby a list of hosts that wish to enforce the use of SSL/TLS on their site is hardcoded into a web browser. The list is compiled by Google and is used by Chrome, Firefox, Safari, Internet Explorer 11 and Edge browsers. When HSTS preload is used, a web browser will not even try to send a request using HTTP but will use HTTPS every time.

Note: To use HSTS preload, you must submit your domain name for inclusion in Chrome's HSTS preload list. Your domain will be hardcoded into all web browser that use the list.

Inclusion in the preload list cannot easily be undone.

You should only request inclusion if you are sure that you can support HTTPS for your entire site and all its subdomains in the long term (usually 1–2 years).

Your website must have a valid SSL certificate. See Assessing SSL Server Configuration.

All subdomains (if any) must be covered in your SSL Certificate. Consider ordering a Wildcard Certificate.
