How to assign an SSL Certificate

With the new Real-Time Registration (RTR) process live since May 1st, 2025, SSL certificates can now be assigned, issued and renewed with a streamlined process. This guide walks you through two main flows depending on how you're assigning the SSL certificate — either using a shared hosting package at Heart Internet or using your own CSR (Certificate Signing Request). Flow 1: Assigning an SSL cert to a domain hosted on a shared hosting package at Heart. Flow 2: Assigning an SSL cert using your own CSR. **Flow 1: Assigning and installing an SSL to a Shared Hosting Package at Heart Step 1: Start SSL Assignment** Navigate to the Heart Internet Customer Area Go to Manage SSL certificates > choose the SSL > Assign From the list, choose the domain hosted on the shared hosting package at Heart. **Note**: Once an SSL certificate is issued, it is locked to the domain it was created for and cannot be moved to another domain. If revoked, the certificate is cancelled, and you'll need to order a new one.Â **Step 2: No CSR Needed** You don't need to provide a CSR. The system generates it automatically. **Step 3: Approval Email Sent Automatically** Â An approval email is sent to admin@yourdomain.com automatically. **Note**:Â Make sure this email is active and accessible, or you could use other emails from the list.Â **Step 4:Â Choose Alternative Approval Methods (if needed)** On the next â€œPendingâ€• page, you can choose other approval methods (e.g., DNS or HTTP-based validation) if email approval isn't suitable. The DNS and website method work the same and the steps are displayed within the same page by pressing on 'Show me how'. This can take up to 2 hours to complete. You only need to complete one of them. 1. DNS Method (Recommended if you manage your domain's DNS) Log into your account and access 'Manage domain names' section, select the domain name Go to the DNS Management section. Choose to Add a new record. Type: CNAME Name / Subdomain: Copy only the code before your domain name. Example: If the code looks like randomnumbersandletters.yourdomain.com you only enter randomnumbersandletters in the subdomain/host field. Do not type â€œyourdomainname.comâ€• here — the system already adds that automatically. Value / Points to: Copy the full target value given. Save the record. Wait for the DNS to update (this can take a few minutes up to a few hours). We recommend allowing 2 hours for the verification to complete. **Note**:Â If your name servers point externally, you will need to add the CNAME record with the company where your domain's nameservers are managed. 2. Website Method (If you have access to your website files) Log in to your hosting control panel or use FTP/File Manager to access your website files. Open the folder called public_html (this is your main website folder). Inside it, create the following path if it doesn't exist: .well-known/pki-validation/ (both folders may need to be created if they are not already there). Upload the verification file as per instructions (in this case: fileauth.txt) into this folder. The full path should be: yourdomainname.com/.well-known/pki-validation/fileauth.txt Once uploaded, test it by visiting the link in your browser. If the text file opens and shows the code, the verification is working. That's it! Once you complete either the DNS Method or the Website Method, the SSL provider will automatically detect the verification and issue your certificate.Â **Step 5:Â Certificate Issuance** For Simple SSLs: The certificate is issued within seconds after approval. For Organization (Org) or Extended Validation (EV) SSLs: Additional validation is required (similar to previous SSL process). **Step 6:Â Automatic installation** If the domain is hosted on a shared Heart package, the certificate is automatically installed once issued. Please note that this process may take up to 60 minutes to complete. During this time, your website may not immediately show as secure, but the certificate will reflect on your website as soon as the installation is complete.Â Â **Note:** Â The CSR option is only intended for use with Cpanel, MWP (Managed WordPress), VPS, or external hosting platforms. If you have your websites hosted on the eXtend hosting platform, the domain name will be present in the list and you won't need to use a CSR. cPanel and MWP packages cannot be selected for the dropdown list so the CSR flow is necessary. Â **Flow 2:Â Assigning an SSL using a CSR Step 1: Paste the CSR**Â If you're hosting your website externally, on Cpanel, Managed WordPress, or VPS. Paste your CSR (Certificate Signing Request) into the designated field. The system will decode and display CSR details for confirmation. **Step 2: Submit The Assignment Request** Review the CSR information and submit the request. **Step 3: Validation Process** As per Flow 1: Approval email sent to admin@domain.com. Option to use alternative validation methods. Org SSLs will require more details for organization verification. **Step 4:**

Download and InstallÂ Once issued: If the domain is not hosted at Heart, you can download the SSL certificate from the Manage page. Manually install it on your external server. Â **Additonal Notes for Organizational (Org) and Extend Validation (EV) SSLs:** Please note that for Organisational SSL certificates, the Certificate Authority will reach out to you directly to confirm the organisation's information and request any documentation necessary to complete the validation process. **Â Q: What if none of the emails listed exist ?**

You can choose to switch to DNS or HTTP-based validation on the Pending screen. **Q: Is manual installation needed for all certs?**

No, ifÂ your domain is on a Heart shared hosting package, the system installs the cert automatically.

For external hosts, download and install it manually. **Q: Can I reuse a CSR for multiple domains?**

No. Each CSR is domain-specific. Generate a new CSR for each domain. Q: Can SSL certificates be revoked and used for a different domain name once installed?

No. Please note that once you revoke your certificate, it will no longer be valid and you will need to purchase a new certificate to secure your site.

Posted - Tue, Dec 15, 2020 at 3:44 PM.

Online URL: https://www.heartinternet.uk/support/article/how-to-assign-an-ssl-certificate.html