What is a Subject Alternative Name (SAN) and how do I submit multiple SANs?

Tell Me

1. Subject Alternative Name (SAN): SANs allow you to protect multiple host names with a single SSL certificate.
2. If your server has more than one alias, we can add a SAN, or multiple SANs, to your certificate to insure that certificate mismatch errors do not happen.
3. Submitting a CSR with multiple SANs:
   a. When you submit your certificate signing request you will need to select under certificate type InCommon Multi Domain SSL (SHA-2) and add the SANs under the common name.

   ![Certificate Signing Request Form]

<table>
<thead>
<tr>
<th>Certificate Type</th>
<th>InCommon Multi Domain SSL (SHA-2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Term</td>
<td>2 years</td>
</tr>
<tr>
<td>Server Software</td>
<td>OTHER</td>
</tr>
<tr>
<td>CSR</td>
<td></td>
</tr>
</tbody>
</table>

   - GET CSR FROM CSR
   - UPLOAD CSR
   - Max CSR size is 32K

   Common Name: test.uncc.edu
   Subject Alternative Names: test.its.uncc.edu,
   its-test.uncc.edu

Related FAQs

- How do I generate a Certificate Signing Request (CSR)?
- How do I submit the InCommon certificate signing request (CSR)?
- How do I install the certificate on my server once I receive my new InCommon Certificate?
- What are the InCommon Certificate Service and Certificate Signing Request (CSR)?
- What is a Subject Alternative Name (SAN) and how do I submit multiple SANs?