Browsers reject SSL Certificates signed by VeriSign as expired

THE INFORMATION IN THIS ARTICLE APPLIES TO:

- Secure FTP Server (all versions)
- EFT Server, all versions prior to 5.1

QUESTION

Why do clients connecting to my server via HTTPS report that my VeriSign-signed SSL certificate is invalid even though it's not expired?

ANSWER

When VeriSign signs your SSL certificate, they do so with an intermediate certificate, not their root certificate. The copy of the intermediate certifcate on the vast majority of client systems is expired. The intermediate certificate has since been reissued, but few client systems will contain the more up-to-date, valid certificate. Therefore, because the client system only contains an expired copy of the certificate that signed your certificate, it will in turn treat *your* certificate as invalid.

When a client connects to your server, the client will receive its certificate, which references a chain of certificates. For example, Myhost -> VeriSign Public Class 3 Primary. The client then looks at its certificate store and fails to see your host certificate (unless imported prior), but it does see the VeriSign Public Class 3 Primary certificate--which happens to be expired.

To fix the problem (other than signing your server certificate with a certificate that isn't expired in most browsers' certificate stores), you should ask your client to update their expired intermediate certificates stored on their machine. See http://support.microsoft.com/kb/834438 for more information. Ideally the client should update all their VeriSign certificates, as there are several that have expired, even in IE7 on Vista. Updated root certificates can be obtained from VeriSign at http://www.verisign.com/support/roots.html.

This issue was resolved in EFT Server 5.1.

GlobalSCAPE Knowledge Base
https://kb.globalscape.com/Knowledgebase/10346/Browsers-reject-SSL-Certific...