SSL Certificate Update - Sage X3

Overview	This document covers the Datel process for SSL certificate updates on Sage X3 customer sites. Tickets originate from the Datel Audit App. The process differs depending on customer type.
Customer Type	**Advansys hosted (Advansys / Managed customers):** Completed FOC. Advansys provide and manage the certificate on the customer's behalf. They place the certificate files in C:\dal on the server. Datel then pick up from there to update the relevant apps. **Directly hosted (customer manages own server):** The customer provides the certificate directly to Datel. They typically supply a .pfx file. Datel export this to the required formats and deploy to the relevant certificate stores and app bindings. **Tech Support customers:** Send the document "Sage X3 SEI SSL Certificate Update Nov 2025" from shared documents to the customer to complete themselves.
Advansys / Managed Process	**Customer to do:** The customer provides the new certificate. How it is handled depends on their hosting arrangement: **Advansys hosted:** Customer provides the certificate to Advansys (Datel's hosting partner). Advansys convert the certificate, upload to the server certificate stores and update the IIS site bindings. **Self-hosted:** Customer provides the certificate directly to Datel. Datel handle the upload to the server certificate stores and update the IIS site bindings. **Datel to do:** 1. Arrange downtime to update the following apps: Sage X3 (ensure certs are copied to all Syracuse servers); Fusion Inscribe (URL is still named V1). 2. We will complete the SSL certificate update process for each piece of software listed, ensuring the new certificate is applied across all relevant services, bindings and stores. 3. Confirm IIS site bindings have been updated for all applicable apps. Common apps to check: • SEI • Excel Connect • Any other IIS-hosted Datel apps on the server 4. Run the SSL Certificate Check Script (see step below). 5. Run the Datel Audit App Capture & Send Scheduled Tasks on all servers.

SSL Check Script - Location	TFS: DAT01 - Datel Bespoke / MISCELLANEOUS BESPOKES / SSL_CERT_CHECK_V1 Local server copy: E:\Datel\SSL_CERT_CHECK
SSL Check Script - Instructions	1. Add the customer URLs into the $Urls list in the script. 2. Save and run in PowerShell ISE. 3. The script will output how many days remain on each certificate. Note this down. **Output modes:** • simple = URL + status line only • full = all certificate detail Change $Output in the script params to switch modes. Use -LogPath for optional CSV export. **Origin bypass (advanced):** For sites behind a load balancer, add to $OriginMap to check the cert on the real server. Leave empty if not needed. The script is read-only and safe to run in all environments.
Change Management	Arrange a date and time with the customer for the change window and update as per normal change procedures.
Post-Work Steps	1. Run the SSL check script a second time after the work is complete. 2. Paste the script output into the resolution field of the ticket. 3. Save the customer-specific script in TFS under the customer folder for use next year. 4. Also save the script to E:\Datel\SSL_CERT_CHECK on the server. 5. Update the SSL tab in SLX. See Hawker as a template example (completed by Joe).
Notes	Updated 30/04/26. For SLX SSL tab template reference, see Hawker customer entry.