Secure Socket Layer

For E-Sales 2.1 with Servicepack 3 & E-Collaboration 2.1 with Patch A

Currently E-Collaboration 2.1 and E-Sales 2.1 are not able to make use of the SSL protocol.
To enable SSL for these applications a patch has been created.
This document describes how this patch should be installed and how to configure the website in order to enable SSL.

This patch has been created for the combination E-Sales 2.1.3 and E-Collaboration 2.1.0.a. Therefore it is necessary to install Servicepack 3 for E-Sales 2.1 and Patch A for E-Collaboration 2.1. Otherwise some compatibility problems will occur.

First install the Patch on, just, the webserver.
In the case the Patch is to be installed on a stand-alone E-Collaboration server, one file has to be copied manually afterwards. This is the file: “Global.asa”. It is located in the folder where the Self-extracting archive has been unpacked. It should be copied to the rootfolder of the website. In a standard environment this is the following folder: “c:\Program Files\Baan\E-Enterprise 2.0\ee11\”

After the installation of the patch, the website has to be configured in order to enable SSL.
On the database server the SSL mode is registered as a Common parameter. This parameter “SSLMODE” can be modified in the Manager\E-Common page and should be set to “All” in the case of SSL or “None” in the case of no SSL.
After enabling SSL in the Manager\Common page the following should be done:

A SSL certificate has to be created on the default website.

- Open the SiteServer MMC;
- Rightclick on Default Web Site (below Internet Information Server) and choose properties;
- Open the tab Directory Security;
- Click on the Edit-button of Secure Communications;
- Click on the button Key Manager;
- RightClick on WWW and choose Create New Key;
- Choose: Put the request file in a file, and choose C:\NewKeyRq.txt as destination file;
- Click Next;
- Now type a name for the Key and a password. For the first test, set the Bit length to 512;
- Click Next;
- Fill in the next 3 lines;
- Click Next;
- Fill in the lines;
- Click Next;
- Fill in the next 3 lines;
- Click Next;
- Click Finish.

Now the certificate file is created. The next step is to process the certificate. Certificate server of NT Option Pack has to be installed, otherwise the file can not be process the file.

To process the Certificate file:

- Go to start->programs->windows NT 4.0 option pack->Microsoft Certificate Server->Process Certificate Request File;
- The window Open Request File appears. Now you have to select the file C:\NewKeyRq.txt and press Ok;
- Enter a file name for the processed Certificate file. For example: “output”;
- Go back to the Key Manager window that should be still open on your webserver. (The window with WWW);
- Below WWW, a key is visible ,followed by the name of your certificate;

- Right click on that key and choose Install Key Certificate;
- Select the, as example, "output" file;
- After selecting it choose Ok;
- Enter the password you gave to the certificate;
- A window called server bindings will appear. Just click here on the Ok-button;
- Close the keymanager-window;
- Click 'Yes' when you get the question: Commit all changes now?
- You will be back in the window Secure Communications, where the Key Manager-button is visible;
- In this window, select the option: Require Secure channel when accessing this resource;
- Click 'OK';
- Now you will be in the Default Web Site Properties window;
- Click 'OK'.

Go to Commerce Host Administration within the Site Server MMC.

- Right click on E-Enterprise 2.0 (just some levels within Commerce Host Administration) and choose properties;
- Select here : Enable HTTPS;
- Choose 'OK';

At this point the website is SSL enabled.
To disable it, first set the Common parameter: "SSLMODE" to "None" then disable HTTPS on the Commerce host under MMC. Secondly the "Require Secure channel when accessing this resource" checkbox for the default website has to be unchecked.