Vordel XML Gateway and Luna SA

Integration Guide

SafeNet.

Preface

Part Number: 007-011533-001 (Rev A, 06/2011)

SafeNet makes no representations or warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, SafeNet reserves the right to revise this publication and to make changes from time to time in the content hereof without the obligation upon SafeNet to notify any person or organization of any such revisions or changes.

SafeNet invites constructive comments on the contents of this document. These comments, together with your personal and/or company details, should be sent to the address below.
SafeNet, Inc.

4690 Millennium Drive
Belcamp, Maryland 21017
USA

Limitations

This document does not include the steps to set up the third-party software. The steps given in this document must be modified accordingly. Refer to Luna SA documentation for general Luna setup procedures.

Disclaimers

The foregoing integration was performed and tested only with the specific versions of equipment and software and only in the configuration indicated. If your setup matches exactly, you should expect no trouble, and Customer Support can assist with any missteps. If your setup differs, then the foregoing is merely a template and you will need to adjust the instructions to fit your situation. Customer Support will attempt to assist, but cannot guarantee success in setups that we have not tested.

Technical Support

If you encounter a problem while installing, registering or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, please contact your supplier or SafeNet support.

SafeNet support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between SafeNet and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Technical Support Contact Information:
Phone: 800-545-6608, 410-931-7520
Email: support@safenet-inc.com

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

THIS PAGE INTENTIONALLY LEFT BLANK

Chapter 1 Introduction

This document covers the necessary information to install, configure and integrate Vordel XML Gateway v5.2.9 with SafeNet Luna SA v4.4.1 Hardware Security Modules (HSM).

Vordel Gateway is a purpose-built Gateway, often referred to as an XML Gateway or SOA appliance, available in multiple form factors, designed to accelerate, secure and integrate all types of traffic on the SOA network.

The XML Gateway uses OpenSSL to perform cryptographic operations, such as encryption and decryption, signature generation and validation, and SSL tunneling. OpenSSL exposes an Engine API, which makes it possible to plug in alternative implementations of some or all of the cryptographic operations implemented by OpenSSL. When configured appropriately, OpenSSL calls the engine's implementation of these operations instead of its own.

The Luna HSMs integrates with the Vordel XML Gateway to provide significant performance improvements by off-loading cryptographic operations from the Vordel XML Gateway to the Luna HSMs. In addition, the Luna HSMs provides extra security by protecting and managing the server’s high value SSL private key within a FIPS 140-2 certified hardware security module.

Scope

3rd Party Application Details

- Vordel XML Gateway v5.2.9 for Solaris

Supported Platforms

The following platforms are supported for Luna SA 1U v4.4.1:

- Solaris 10 SPARC 32-bit

HSMs and Firmware Version

- K5 HSM f/w 4.6.8

Library and Driver Support

- PKCS#11 v2.01 dynamic library

Distributions

- Luna SA 1U Appliance s/w v4.4.1
- Luna SA Client s/w v4.4.1
- Openssl Toolkit
- LunaSAVordel.zip - Files specific to the Luna SA and Vordel integration

Prerequisites:

Luna SA Setup:

Please refer to the **Luna SA** documentation for installation steps and details regarding to configure and setup the box on Solaris SPARC systems. Before you get started ensure the following:

- Luna SA appliance and a secure admin password
- Luna SA, and a hostname, suitable for your network
- Luna SA network parameters are set to work with your network
- Initialize the HSM on the Luna SA appliance
- Create a partition on the HSM and remember the partition password that will be later used for Vordel XML Gateway. Run the command, vtl verify to display a partition from Luna SA. The general form of command is “/usr/lunasa/bin/vtl verify”.
- Create and exchange certificates between the Luna SA and your "Client" system (registered the Client with the Partition).
- Enable Partition "Activation" and "Auto Activation" (Partition policy settings 22 and 23 (applies to Luna SA with Trusted Path Authentication [which is FIPS 140-2 level 3] only).

Openssl Toolkit:

The Openssl toolkit (630-010135-002.tgz) is provided to make the installation quick and easy. The installation CD along with LunaSAVordel.zip can be obtained from the SafeNet Customer Connection Center.

Note: If you already have Openssl installed, uninstall it before proceeding with the installation.

Chapter 2
Integration of Vordel XML Gateway 5.2.9 with Luna SA

To configure Vordel XML Gateway v5.2.9 to recognize the Luna SA v4.4.1 cryptographic device:

1. Uncompress the Openssl toolkit.

   ```
   gunzip 630-010135-002.tgz

   tar xvf 630-010135-002.tar
   ```

2. Copy the openssl package from the openssl toolkit to the Luna SA client installer directory.

   ```
   cp _cdrom_apache/openssl-0.9.8l.tar.gz /610036-042MI/source/apache
   ```

3. Copy the Optimize apache script the Luna SA client installer directory.

   ```
   cp _cdrom_apache/OptimizeApache.sh 610036-042MI/source/apache
   ```

4. Unzip the LunaSAVordel.zip file.

   ```
   unzip LunaSAVordel.zip
   ```

5. Copy the two files extracted from LunaSAVordel.zip to the Luna SA client installer directory:

   ```
   cp install.sh  610036-042MI/source/apache/

   cp abuild-2.0 610036-042MI/source/apache/
   ```

6. Change to the Luna SA client installer apache directory.

   ```
   cd /610036-042MI/source/apache
   ```

7. Run the install.sh script.

   ```
   ./install.sh
   ```

8. Configure the PATH environment variable:

   ```
   PATH=$PATH:/usr/local/bin/
   PATH=$PATH:/opt/SUNWspro/bin/
   PATH=$PATH:/usr/ccs/bin/
   ```

9. Configure the LUNA_CONFIG_BITS environment variable.

   ```
   export LUNA_CONFIG_BITS = 32
   ```

10. Traverse to /usr/lunasa/apache directory:

    ```
    cd /usr/lunasa/apache
    ```

11. Run the abuild-2.0 script.

    ```
    ./abuild-2.0 --openssl
    ```

12. Edit the /etc/Chrystoki.conf file:

    The /etc/Chrystoki.conf file controls the features available for the Luna SA client. The file needs to be edited to ensure that the **Misc** section includes the line Apache=1 (shown below) and the EngineLunaCA3 section needs to be edited to match the following:

    ```
    Misc = {
    Apache = 1;
    }

    EngineLunaCA3 = {
    EnableSessionMutex = 1;
    NO_NORM_FINALIZE = 0;
    NO_FORK_FINALIZE = 0;
    DisableRand = 0;
    DisableDsa = 0;
    DisableRsa = 0;
    DisableEcdsa = 0;
    FORK_CHECK = 0;
    EngineInit = 1:10:11;
    EnableLoadPrivKey=1;
    LibPath = /usr/lib/libCryptoki2.so;
    }
    ```

13. Test the Openssl and LunaCA3 engine.

    ```
    export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/usr/local/ssl/lib/:/usr/local/ssl/lib/engines

    /usr/local/ssl/bin/openssl speed -engine lunaca3
    ```

14. Configure the Vordel application.

    ```
    PATH=$PATH:/usr/local/ssl/bin
    ```

    Ensure there is an openssl.cnf file set for the gateway OpenSSL located at <Vordel Installation Directory>/vordelxmlgateway/conf/openssl.cnf. If the configuration file is missing, use the openssl.cnf file found in the LunaSAVordel.zip file

15. Add a symbolic link from the lunaca3 engine in the the /usrlocal/ssl/lib/engines directory to <Vordel Installation Directory>/vordelxmlgateway/platform/lib/engines directory.

    ```
    ln -s /usr/local/ssl/lib/engines/liblunaca3.so /vordelxmlgateway/platform/lib/engines/libLunaCA3.so
    ```

16. Update the LD_LIBRARY_PATH in the <Vordel Installation Directory>/ vordelxmlgateway/posix/libexec/venv file.

    ```
    OPENSSL_ENGINES=$VINSTDIR/$V_PLATFORM/lib/engines/
    OPENSSL_CONF=$VINSTDIR/conf/openssl.cnf
    +LD_LIBRARY_PATH=$OPENSSL_ENGINES:$LD_LIBRARY_PATH
    export OPENSSL_ENGINES OPENSSL_CONF
    ```

17. Now validate that the installation is working correctly by using the vrun command to execute Openssl.

    ```
    <Vordel Installation Directory>/vordelxmlgateway/posix/bin/vrun openssl speed -engine LunaCA3
    ```

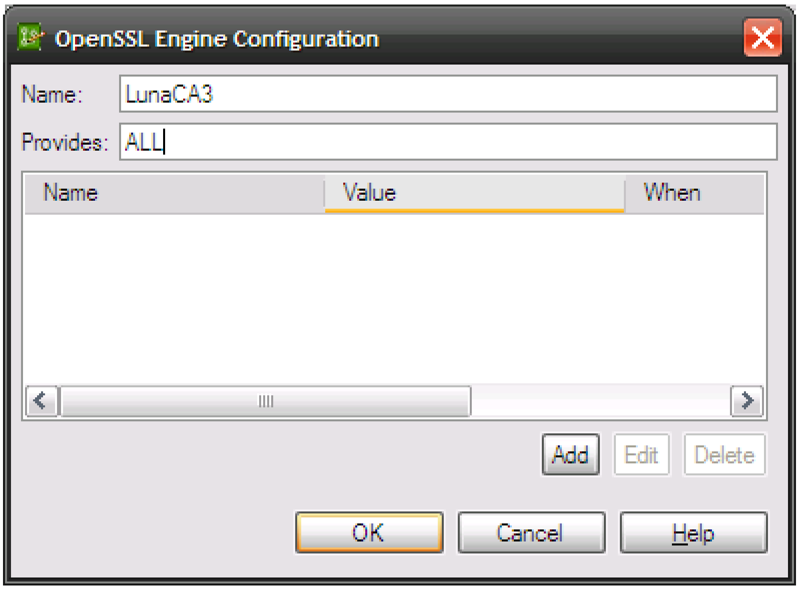
18. Login to the Luna SA partition.

    ```
    /usr/lunasa/apache/solaris/sautil -s 1 -i 10:11 -p <Partition Password> -o
    ```

19. Connect the policy studio to the appliance.

    Go to Processes->Vordel Gateway->Cryptographic Acceleration and choose Add OpenSSL Engine:

    Set the 'Name' to 'LunaCA3' and 'Provides' to 'ALL' in the dialog as shown



OpenSSL Engine Configuration

Name: LunaCA3

Provides: ALL

20. Restart the gateway

    ```
    <Vordel Installation Directory>/vordelxmlgateway/posix/bin/vordelxmlgateway –k
    ```

    ```
    <Vordel Installation Directory>/vordelxmlgateway/posix/bin/vordelxmlgateway –d
    ```

    The trace file should contain the following elements:

    ```
    INFO    14:42:22:141 [0001]    SSL engine LunaCA3 initialized
    INFO    14:42:22:141 [0001]    engine LunaCA3 is default for 'ALL'
    ```

21. Creating a key in Luna SA.

    ```
    /usr/lunasa/apache/solaris/sautil -s 1 -i 10:11 -g 1024 -f server.key
    ```

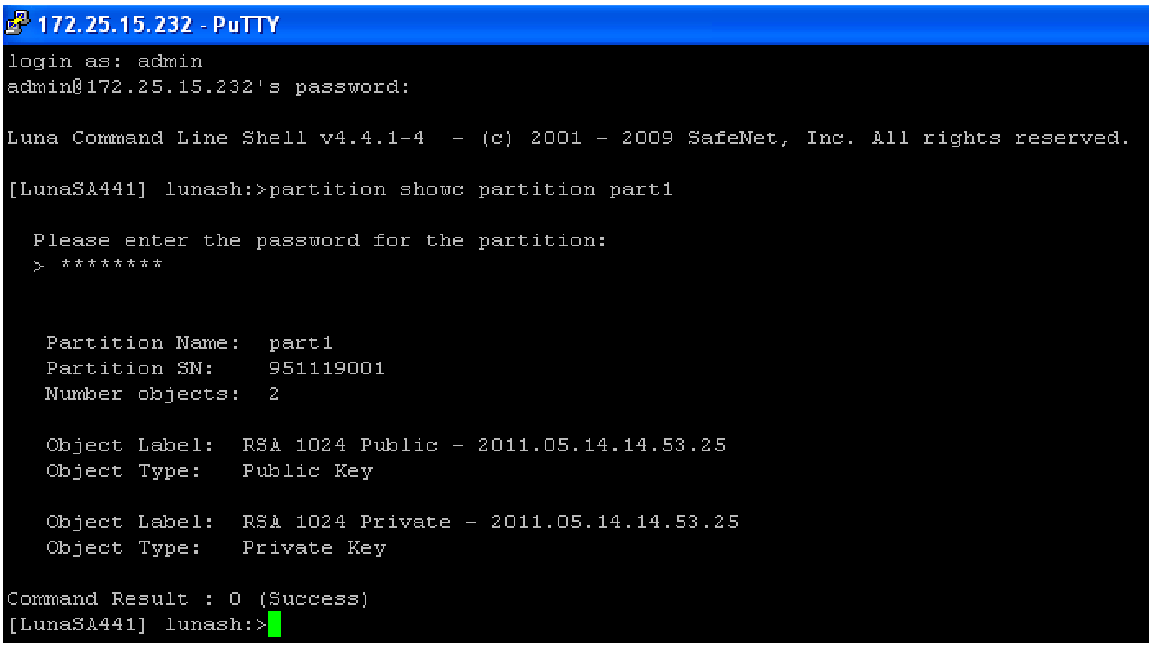
22. Generate a Certificate Signing Request.

    ```
    <Vordel Installation Directory>/vordelxmlgateway/posix/bin/vrun openssl req -engine LunaCA3 -new -key server.key -x509 -out CA.crt
    ```

    In a production scenario, this request would be submitted to a Certificate Authority. However, for the purposes of demonstration we have used the CA.crt file as is. Copy this file from the Solaris server to a machine running the Vordel Policy Studio.

23. Confguring the XML Gateway to use the HSM SSL Certificate.

    Make a note of the name of the private key within the HSM which corresponds with the certificate. In order to do this, make an ssh connection to the HSM and issue the partition showContents command.

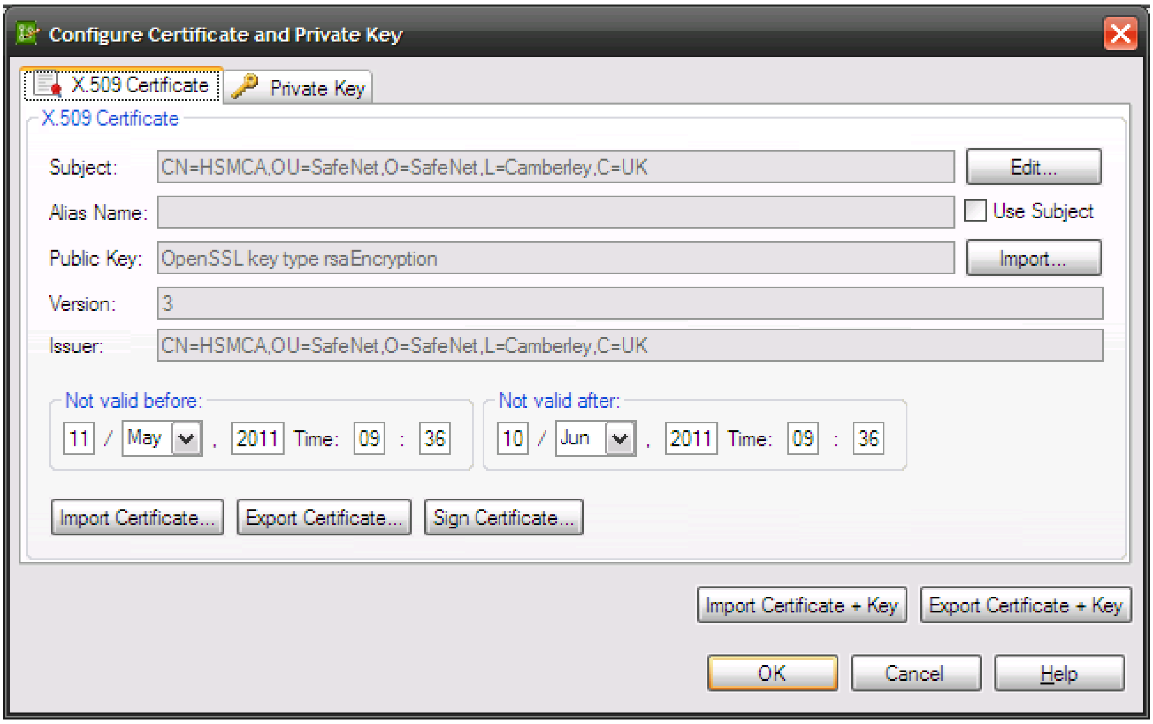


172.25.15.232 - PuTTY

```
login as: admin
admin@172.25.15.232's password:

Luna Command Line Shell v4.4.1-4  - (c) 2001 - 2009 SafeNet, Inc. All rights reserved.

[LunaSA441] lunash:>partition showc partition part1

  Please enter the password for the partition:
  > ********


   Partition Name:  part1
   Partition SN:    951119001
   Number objects:  2

   Object Label:  RSA 1024 Public - 2011.05.14.14.53.25
   Object Type:   Public Key

   Object Label:  RSA 1024 Private - 2011.05.14.14.53.25
   Object Type:   Private Key

Command Result : 0 (Success)
[LunaSA441] lunash:>
```

24. Import the certificate.

    In the Vordel Policy Studio navigate to the Certificates dialog then select the create/import button. On the following screen select the import certificate button and then choose the certificate file exported from the Solaris box.



Configure Certificate and Private Key

X.509 Certificate

Subject: CN=HSMCA,OU=SafeNet,O=SafeNet,L=Camberley,C=UK

Alias Name:

□ Use Subject

Public Key: OpenSSL key type rsaEncryption

Version: 3

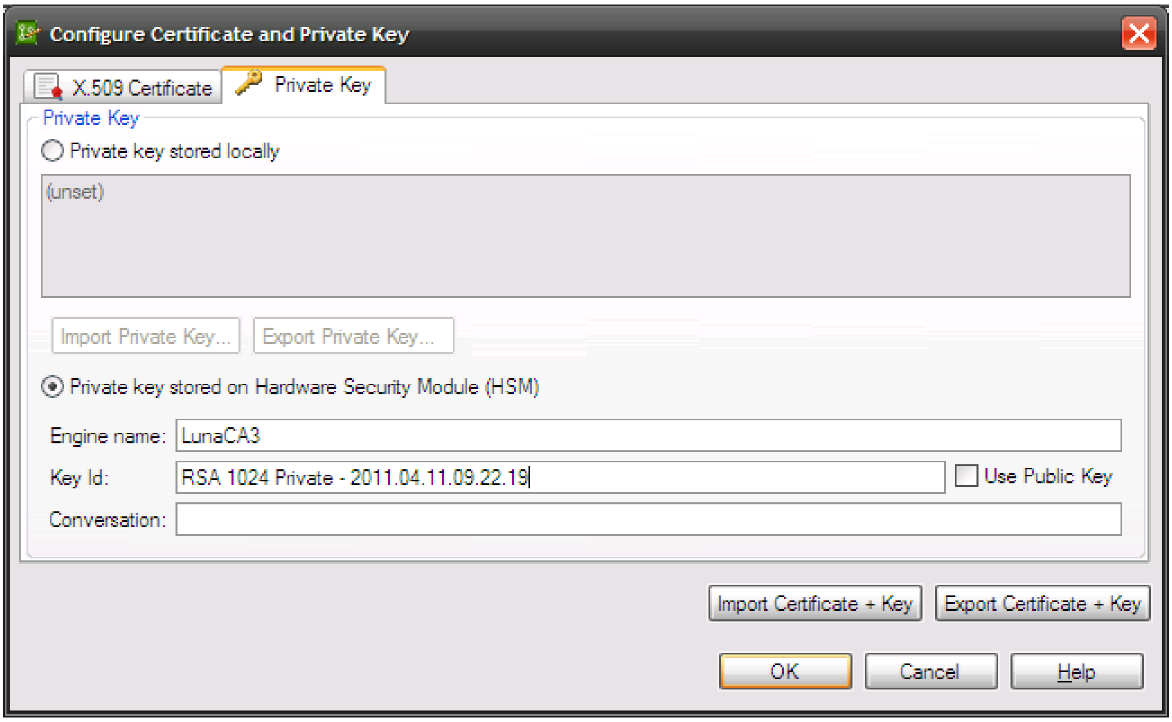
Issuer: CN=HSMCA,OU=SafeNet,O=SafeNet,L=Camberley,C=UK

Not valid before: 11 / May , 2011 Time: 09 : 36

Not valid after: 10 / Jun , 2011 Time: 09 : 36

25. Select the private key.

    Select the private key tab of the dialog. Activate the private key stored in Hardware Security Module radio box and enter the Engine Name as LunaCA3 and the Key Id as the name of the key identified earlier.



Configure Certificate and Private Key

Private Key

○ Private key stored locally

(unset)

● Private key stored on Hardware Security Module (HSM)

Engine name: LunaCA3

Key Id: RSA 1024 Private - 2011.04.11.09.22.19

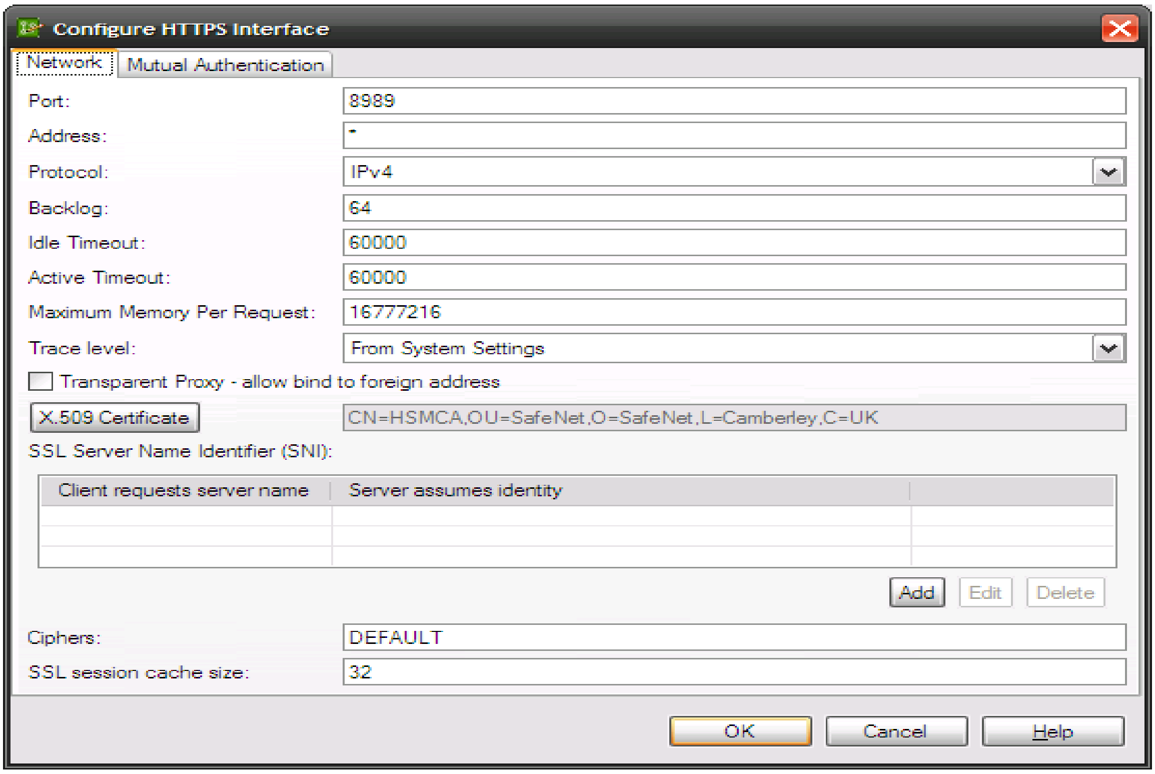
□ Use Public Key

Conversation:

The certificates dialog should now show the newly added certificate in the list of certificates.

26. Associate the certificate with the SSL service.

In order to use the certificate it needs to be associated with an SSL service. Select an SSL service within Policy Studio, choose Edit and then under the X509 certificate option, select the newly imported HSM certificate:



Configure HTTPS Interface

Port: 8989

Address: *

Protocol: IPv4

Backlog: 64

Idle Timeout: 60000

Active Timeout: 60000

Maximum Memory Per Request: 16777216

Trace level: From System Settings

□ Transparent Proxy - allow bind to foreign address

X.509 Certificate: CN=HSMCA,OU=SafeNet,O=SafeNet,L=Camberley,C=UK

SSL Server Name Identifier (SNI):

Client requests server name	Server assumes identity

Ciphers: DEFAULT

SSL session cache size: 32

Once activated, restart the XML Gateway and connect to the SSL service to test the HTTPS connection.