Microsoft Internet Information Services

Integration Guide

gemalto
security to be free

Document Part Number: 007-011955-001, Rev. F

Release Date: March 2016

Contents

Preface

Scope

This document outlines the steps to integrate Microsoft IIS 7.5 /8.0 /8.5 with SafeNet Luna HSM on Windows Server 2008 R2, Windows Server 2008 R2 SP1, and Windows Server 2012/ Windows Server 2012 R2.

Document Conventions

This section provides information on the conventions used in this template.

Notes

Notes are used to alert you to important or helpful information. These elements use the following format:

NOTE: Take note. Contains important or helpful information.

Cautions

Cautions are used to alert you to important information that may help prevent unexpected results or data loss. These elements use the following format:

CAUTION: Exercise caution. Caution alerts contain important information that may help prevent unexpected results or data loss.

Warnings

Warnings are used to alert you to the potential for catastrophic data loss or personal injury. These elements use the following format:

WARNING: Be extremely careful and obey all safety and security measures. In this situation you might do something that could result in catastrophic data loss or personal injury.

Command Syntax and Typeface Conventions

Convention	Description
bold	The bold attribute is used to indicate the following: Command-line commands and options (Type **dir /p**.)

Convention	Description
	Button names (Click **Save As**.) Check box and radio button names (Select the **Print Duplex** check box.) Window titles (On the **Protect Document** window, click **Yes**.) Field names (**User Name:** Enter the name of the user.) Menu names (On the **File** menu, click **Save**.) (Click **Menu** > **Go To** > **Folders**.) User input (In the **Date** box, type **April 1**.)
italic	The italic attribute is used for emphasis or to indicate a related document. (See the *Installation Guide* for more information.)
`Consolas`	Denotes syntax, prompts and code examples.

Support Contacts

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, contact your supplier or Gemalto Customer Support. Gemalto Customer 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 Gemalto and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Contact Method	Contact Information	
Address	Gemalto, Inc. 4690 Millennium Drive Belcamp, Maryland 21017, USA	
Phone	US	1-800-545-6608
	International	1-410-931-7520
Technical Support Customer Portal	https://serviceportal.safenet-inc.com Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the Gemalto Knowledge Base.	

1
Introduction

Overview

This document is intended to guide security administrators through the steps for Microsoft Internet Information Services (IIS) and SafeNet Luna HSM integration and also provides necessary information to install, configure, and integrate Microsoft IIS with SafeNet Luna HSM. It assumes that you have read the Quick Start Guide and are familiar with the IIS 7.5/8.0/8.5 documentation and setup process.

3rd Party Application Details

- Microsoft Internet Information Services (IIS)

Supported Platforms

For Window Server 2012R2:

SafeNet Luna Appliance Software version / f/w version	SafeNet Luna Client Software version
1. 6.2 f/w 6.24.0/6.10.9 2. 6.1.0 f/w 6.23.0/6.10.9 3. 5.2.0 f/w 6.10.1	6.x(v6.2) 6.x(v6.1) 5.x(v 5.2.1)

For Window Server 2008R2:

SafeNet Luna Appliance Software version / f/w version	SafeNet Luna Client Software version
1. 6.2 f/w 6.24.0/6.10.9 2. 6.1.0 f/w 6.23.0/6.10.9 3. 5.2.0 f/w 6.10.1 4. 5.1 f/w 6.2.1	6.x(v6.2) 6.x(v6.1) 5.x(v 5.2.1) 5.x(v5.1)

For Window Server 2008R2:

SafeNet Luna Appliance Software version / f/w version	SafeNet Luna Client Software version
5.1 f/w 6.2.1	5.x(v5.1.1)

For Window Server 2008R2 SP1 (Standard/Enterprise):

SafeNet Luna Appliance Software version / f/w version	SafeNet Luna Client Software version
5.1 f/w 6.2.1	5.x(v5.0) SafeNet PCI-E HSM

Prerequisites

SafeNet Network HSM Setup

Refer to the SafeNet Network HSM documentation for installation steps and details regarding configuring and setting up the box on Windows/Linux systems. Before you get started, ensure the following:

- SafeNet Network HSM appliance and a secure admin password.
- SafeNet Network HSM, and a hostname, suitable for your network.
- SafeNet Network HSM, network parameters are set to work with your network.
- Initialize the HSM on the SafeNet Network HSM appliance.
- Create and exchange certificates between the SafeNet Network HSM and Client system.
- Create a partition on the HSM, remember the partition password that will be used later. Register the Client with the partition. And run the "vtl verify" command on the client system to display a partition from SafeNet Network HSM.
- Enable Partition "Activation" and "Auto Activation" policies 22 and 23 respectively (applies to SafeNet Network HSM with Trusted Path Authentication).

NOTE: Refer to the SafeNet PCI-E HSM documentation for installation steps and details regarding configuring and setting up the SafeNet PCI-E HSM on Windows systems.

2

Integrating Microsoft IIS 7.5/8.0/8.5 with SafeNet Luna HSM

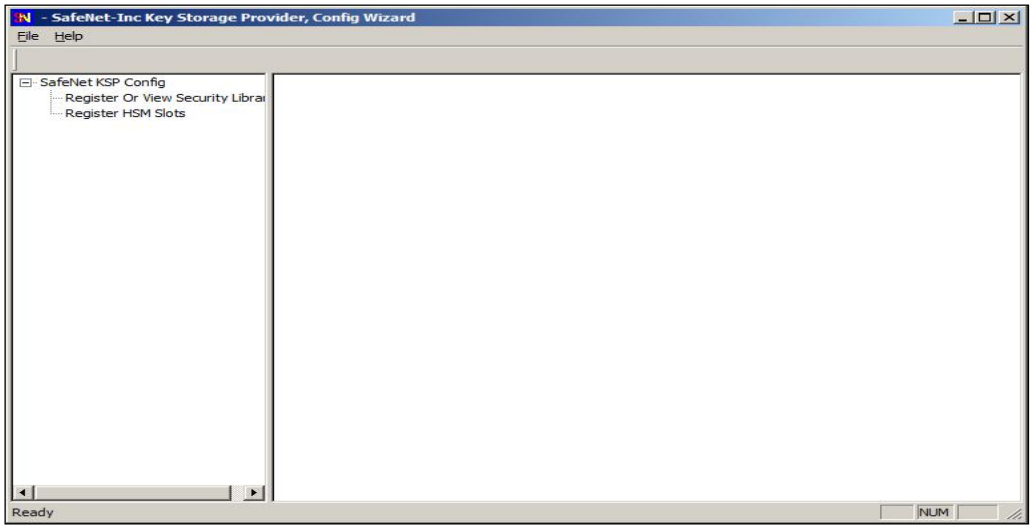
This chapter outlines the steps to install and integrate Microsoft IIS Windows Server 2008 R2/Windows Server 2012. Microsoft IIS uses the SafeNet Luna KSP (Key Storage Provider) for integration.

Before You Begin

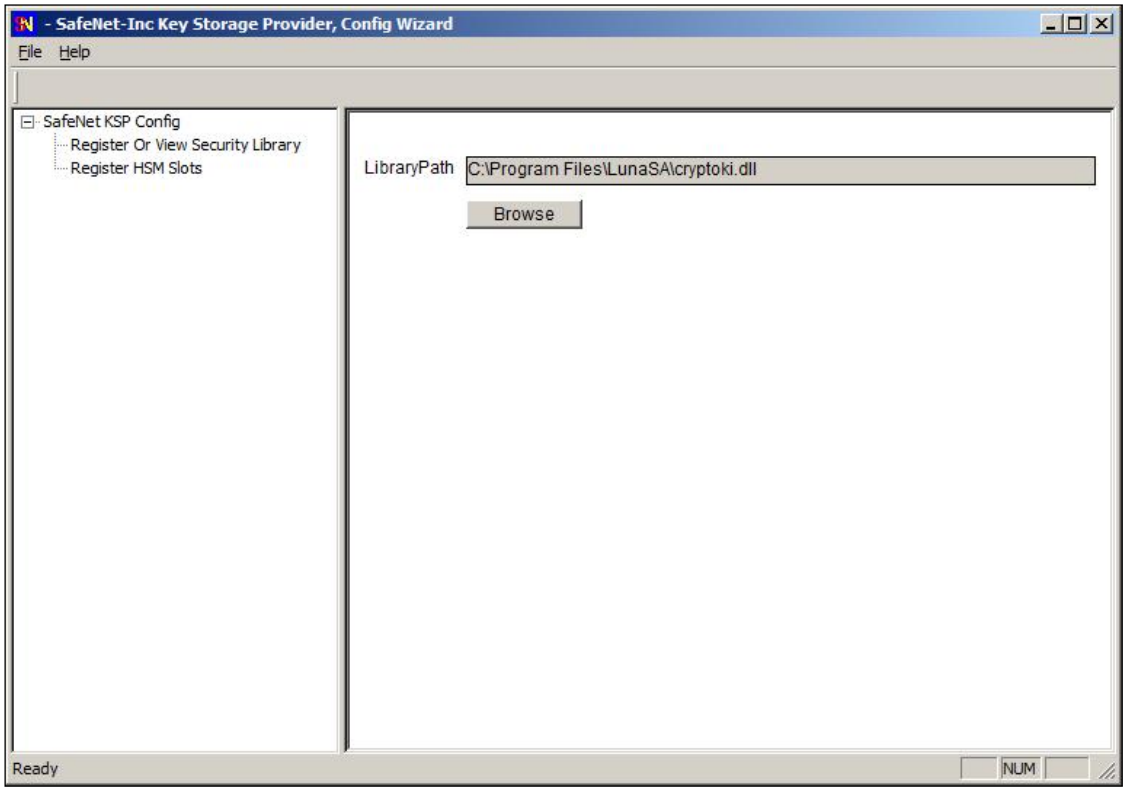
It is recommended that you should familiarize yourself with Microsoft IIS. Refer to the Windows Server 2008 R2/Windows Server 2012 help files for more information.

Before You Install

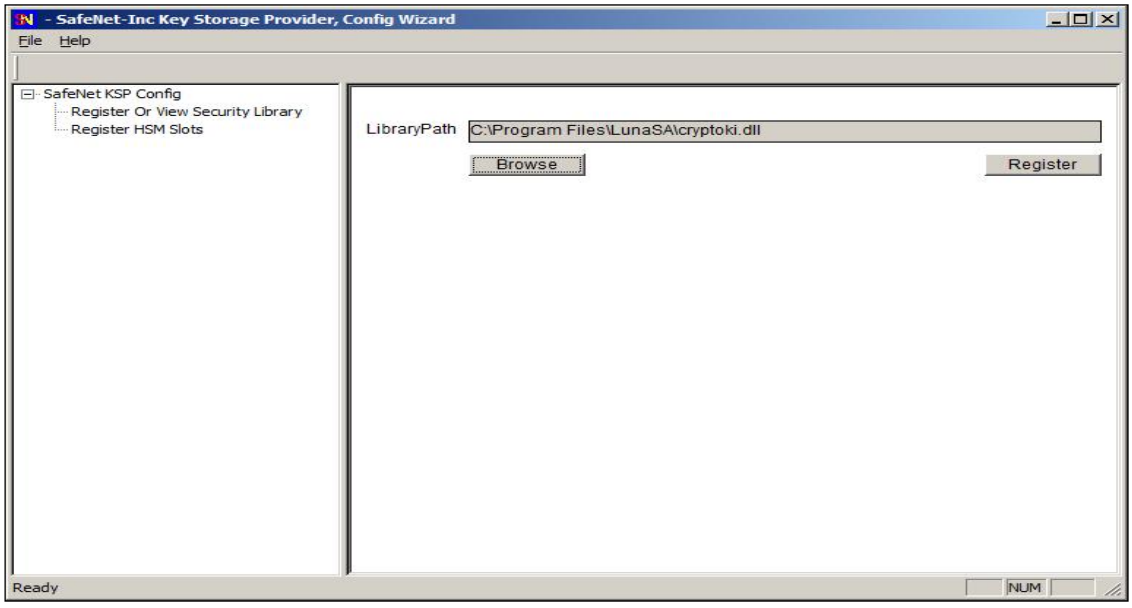
- KSP must be installed in a separate step following completion of the main Luna SA Client software installation. For Luna 5.2, select Luna KSP during installation of Luna 5.2.
- Traverse to the `C:\Program Files\SafeNet` directory. For Luna 5.2, traverse to `C:\ProgramFiles\SafeNet\LunaClient\KSP` directory.
- Run the **KspConfig.exe** (KSP configuration wizard).



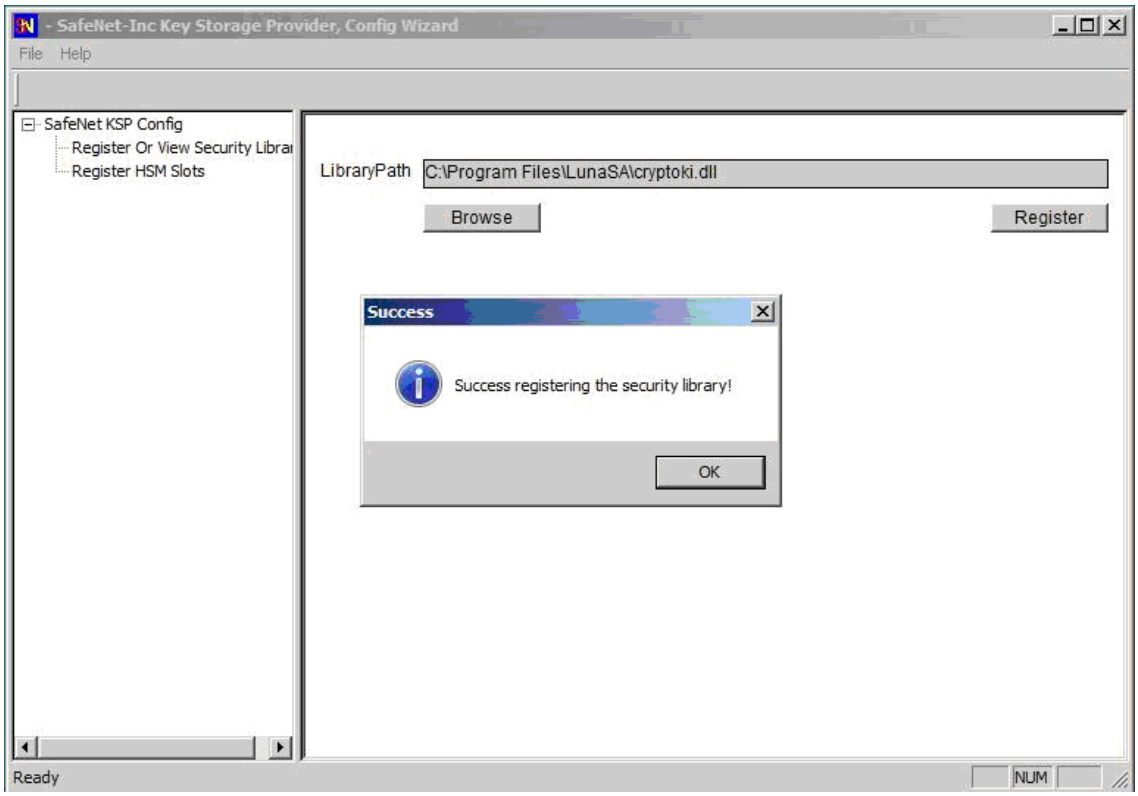
- Double-click **Register or View Security Library** on the left side of the pane.



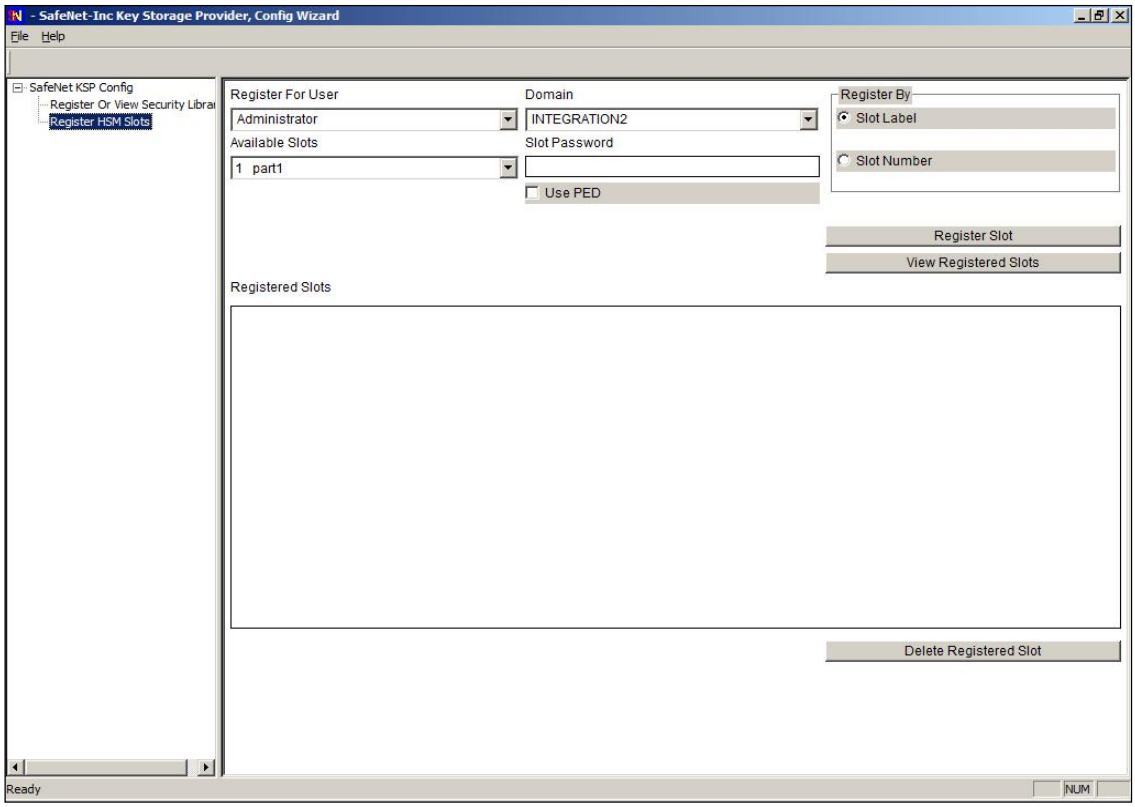
- Browse the library `<Luna Client installation Directory>\cryptoki.dll` and click **Register**.



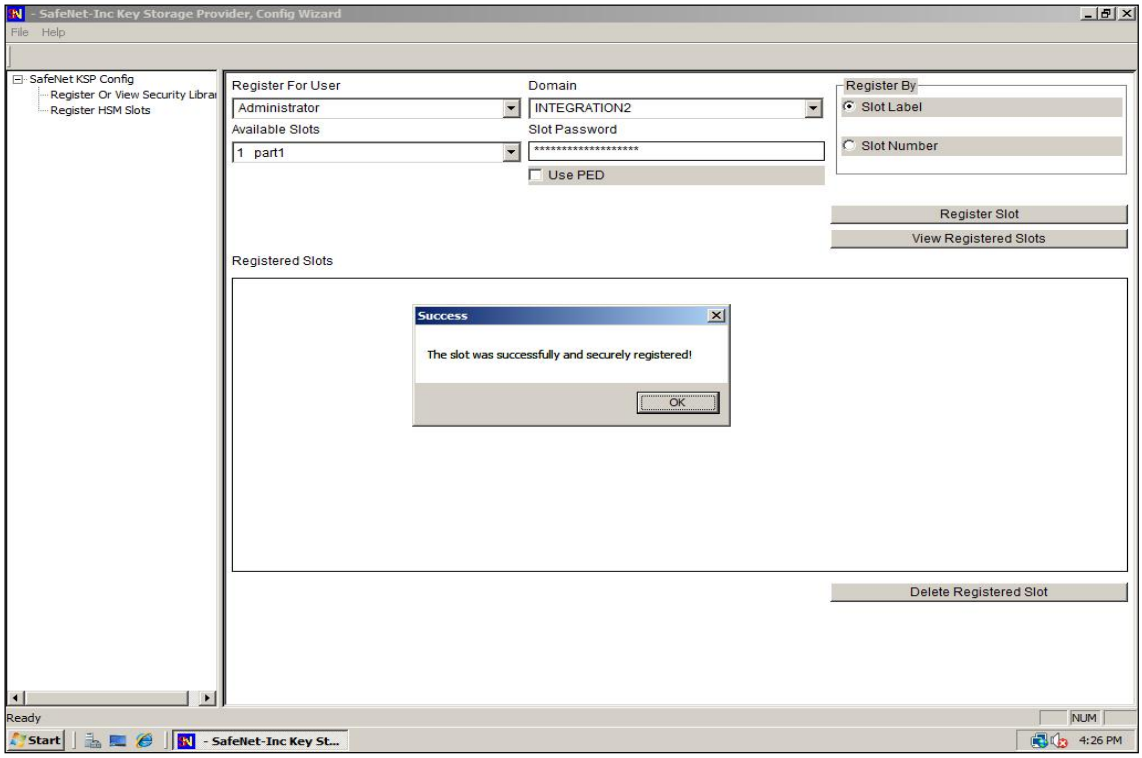
- On successful registration, a message **"Success registering the security library"** displays.



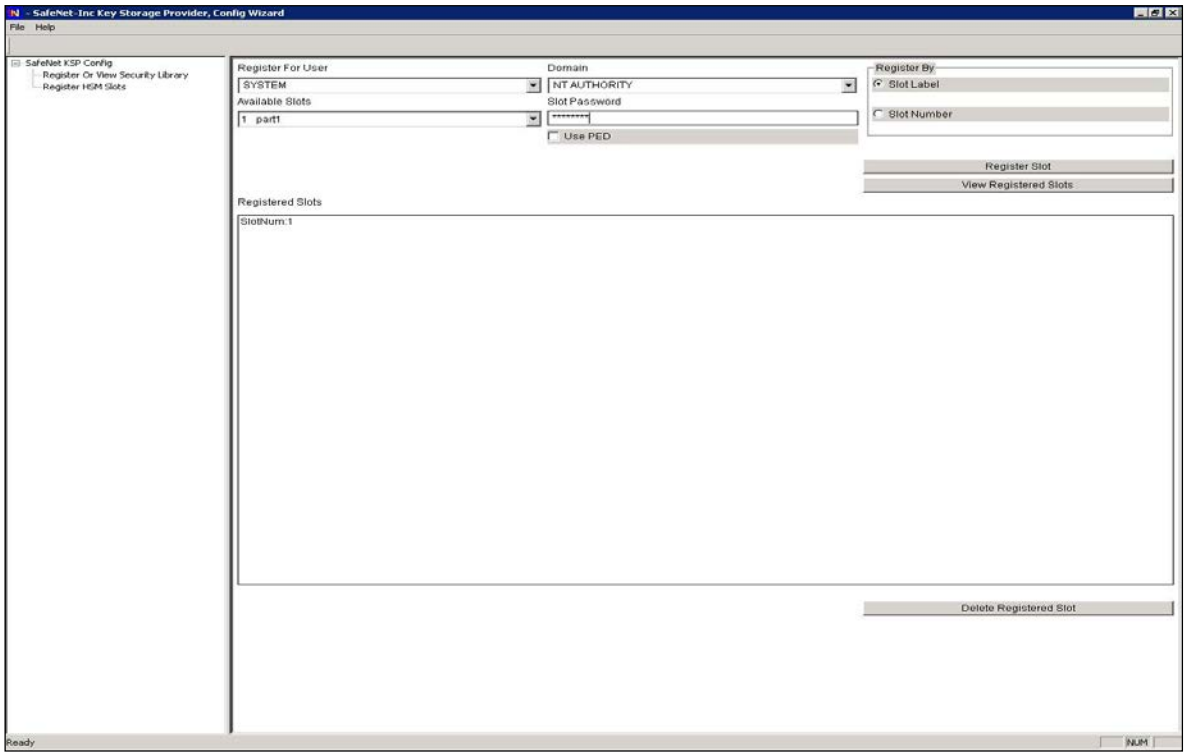
- Double-click **Register HSM Slots** on the left side of the pane.



- Enter the Slot (Partition) password.
- Click **Register Slot** to register the slot for Domain\User. On successful registration, a message **"The slot was successfully and securely registered"** displays.



- You need to register the slot for **NT_AUTHORITY\SYSTEM**.



Install IIS

To install IIS7.5:

- Open Server Manager: Start > Administrative Tools > Server Manager > Add Roles > Web Server.
- Select the Default (or desired) components from within the wizard and proceed with installation.

To install IIS8.0/8.5

- Open Server Manager: Configure this local server > Add roles and feature > Web Server (IIS).
- Select the Default (or desired) components from within the wizard and proceed with installation.

Create a Certificate Request

IIS Manager does not support the creation of certificates protected by CNG Keys and these need to be created using the Microsoft command line utilities.

Generate a certificate request

To generate a request for an SSL certificate linked to a RSA key, create a file called **request.inf** with the following information:

```
[Version]
Signature= "$Windows NT$"
[NewRequest]
Subject = "C=IN,CN=IIS.com,O=Safenet,OU=HSM,L=Noida,S=UP"
HashAlgorithm = SHA256
KeyAlgorithm = RSA
KeyLength = 2048
ProviderName = "Safenet Key Storage Provider"
KeyUsage = 0xf0
MachineKeySet = True
[EnhancedKeyUsageExtension]
OID=1.3.6.1.5.5.7.3.1
```

- Specify the subject details of the Domain Controller which is issuing the certificate.
- Specify the key algorithm and key length as required (e.g. RSA).
- Specify the Provider name as "SafeNet Key Storage Provider"
- Save the above content in the file request.inf.

To create the certificate request for the Certification Authority, execute the command:

```
certreq.exe –new request.inf request.req
```

This creates a certificate request file request.req that can be sent to a Certificate Authority.

Install the Certificate

Submit the CSR file to a CA such as VeriSign, Entrust, and so on. The CA authenticates the request and returns a signed certificate or a certificate chain. Save the reply in the current working directory.

To make the certificate available for use in IIS, execute the below command:

```
certreq.exe –accept somecert.cer
```

Where **somecert.cer** is the binary signed certificate received from the CA.

Binding the Certificate with a Secure IIS Web Server

To bind the certificate with a secure IIS Web Server:

1. Open the IIS Manager from Start > Administrative Tools > Internet Information Services (IIS) Manager.
2. Under Sites on the left hand side of the IIS Manager Window, select the desired Web site.
3. On the right hand side of the IIS Manager, click **Bindings**.
4. In the Site **Bindings** window, click **Add**.
5. Select the protocol as **https**.
6. Select IP address of the machine running IIS from the IP Address drop-down list.
7. Select the certificate from the drop-down list.
8. To complete the certificate binding for SSL connection, click **OK**.
9. Open a browser and type **https://machinename:443**. If necessary, accept the certificate in the browser to continue with SSL connection to the IIS Web Server.

3
Integrating Microsoft IIS 6.0 with SafeNet Luna HSM

This chapter outlines the steps to install and integrate Microsoft IIS Windows Server 2003. Microsoft IIS uses the SafeNet Network CSP for integration.

Before You Begin

You should familiarize yourself with Microsoft IIS. Refer to the appropriate Windows Server 2003 help files for more information.

Before You Install

- Go to `<Luna installation Directory>\CSP`.
- Run **`register.exe`** registering the partition with CSP. Follow the steps below to configure SSL on IIS 6.0

Certificate Creation

1. Login as Local Administrator or as a user with local Administrator privileges.
2. Start IIS from **Start** > **All Programs** > **Administrative Tools** > **Internet Information Services (IIS) Manager**.
3. From the IIS Manager window, select the **Default Web Site**, right-click and select **Properties**.
4. Select the tab **Directory Security** from the available tabs.
5. Select **Server Certificate**. A window **Welcome to the Web Server Certificate Wizard** displays. Click **Next**.
6. Select **Create a New Certificate** and click **Next**.
7. From the **Delayed or Immediate Request** window, select **Prepare the request now**, **but send it later** and click **Next**.
8. From the **Name and Security Settings** window, type the name for the new certificate and select the bit length 2048 and check the option **Select cryptographic service provider (CSP) for this certificate** and click **Next**.
9. Select **Luna Enhanced SChannel Cryptographic Provider** from the Available Providers and click **Next**.
10. Select Organization and Organizational Unit from the **Organization Information** window and click **Next**.
11. Enter the **Common name** and click **Next**.
12. In the **Geographical Information** window give the **Country/Region, State/province, City/locality** information and click **Next**.

13. In the **Certificate Request File Name** window, enter the **File name** for the certificate request and click **Next**.
14. The **Request File Summary** gives the certificate request information. Click **Next**.
15. The **Web Server Certificate** wizard displays. Click **Finish**.

Certificate Installation

1. Once the certificate is created, re-start IIS from **Start** > **All Programs** > **Administrative Tools** > **Internet Information Services (IIS) Manager**.
2. From the **IIS Manager** window, select the **Default Web Site**, right-click and select **Properties**.
3. Select the tab **Directory Security** from the available tabs.
4. Select **Server Certificate**. A window **Welcome to the Web Server Certificate Wizard** displays. Click **Next**.
5. From **Pending Certificate Request** select **Process the pending request and Install the certificate** and click **Next**.
6. Browse to the location (path and file name) where the certificate is saved and click **Next**.
7. In the SSL port window, specify the SSL port (an integer between 1 and 65535) and click **Next**.
8. **Certificate Summary** displays, now click **Next**.
9. The **Web Server Certificate** wizard displays. Click **Finish**.
10. Open a browser and type **https://machinename:443**. If necessary, accept the certificate in the browser to continue with SSL connection to the IIS 6.0 Web Server.