THALES

SafeNet Agent for TokenValidator Proxy 3.0.1

INSTALLATION AND CONFIGURATION GUIDE

Document Information

Product Version	3.0.1
Document Part Number	007-000706-001, Rev. B
Release Date	May 2022

Trademarks, Copyrights, and Third-Party Software

Disclaimer

All information herein is either public information or is the property of and owned solely by Thales DIS France S.A. and/or its subsidiaries or affiliates who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Thales DIS France S.A. and any of its subsidiaries and affiliates (collectively referred to herein after as “Thales”) information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

• The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.

• This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Thales makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Thales reserves the right to make **any change or** improvement in the specifications data, information, and the like described herein, at any time.

Thales hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Thales be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Thales does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Thales be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Thales products. Thales disclaims any liability with respect to security for direct, indirect, incidental or

consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

CONTENTS

PREFACE 6
Audience 6
Support Contacts 6
Customer Support Portal 6
Telephone Support 6
Email Support 7

CHAPTER 1: Overview 8
Applicability 8
System Requirements 8
Introduction 8
Configuring Additional Software Components 9
Architecture 9
Push Authentication 10

CHAPTER 2: Installation and Upgrade 11
Installing TokenValidator Proxy Agent 11
Upgrading TokenValidator Proxy Agent 16
Replacing TokenValidator Proxy Agent 16

CHAPTER 3: Configuration 17
Configuring Transport Layer Security 17
Defining Main and Backup Servers 17
Configuring Logs 18
Activating Certificate Check 19
Configuring Proxy Server 19

PREFACE

Audience

This document is intended for personnel responsible for maintaining your organization's security infrastructure.

The document describes how to install and deploy Token Validator Proxy (TVP) Agent with the SafeNet server.

All products manufactured and distributed by Thales Group are designed to be installed, operated, and maintained by personnel who have the knowledge, training, and qualifications required to safely perform the tasks assigned to them. The information, processes, and procedures contained in this document are intended for use by trained and qualified personnel only.

Support Contacts

If you encounter a problem while installing, registering, or operating this product, please refer to the documentation before contacting support. If you cannot resolve the issue, contact your supplier or Thales Group Customer Support.

Thales Group 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 Thales Group and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Customer Support Portal

The Customer Support Portal, at https://supportportal.thalesgroup.com, is a where you can find solutions for most common problems. The Customer Support Portal is a comprehensive, fully searchable database of support resources, including software and firmware downloads, release notes listing known problems and workarounds, a knowledge base, FAQs, product documentation, technical notes, and more. You can also use the portal to create and manage support cases.

> **NOTE:** You require an account to access the Customer Support Portal. To create a new account, go to the portal and click on the **REGISTER** link.

Telephone Support

If you have an urgent problem, or cannot access the Customer Support Portal, you can contact Thales Group Customer Support by telephone at +1 410-931-7520. Additional local telephone support numbers are listed on the support portal.

Email Support

You can also contact technical support by email at technical.support.DIS@thalesgroup.com.

CHAPTER 1: Overview

Applicability

The information in this document applies to:

- SafeNet Authentication Service PCE/SPE 3.9.1 and later
- SafeNet Authentication Service Cloud Edition

System Requirements

Supported Platforms	> Windows Server 2016 > Windows Server 2012 R2 > Windows Server 2019
Supported Architecture	> 64-bit
Additional Software Components	> IIS 10 > IIS 8.5 > IIS 8.0 > IIS 7.5
	> .NET 4.5 or above

Introduction

The function of SafeNet Agent for TokenValidator Proxy (TVP) is to implement proxy authentication requests from other agents to the SafeNet server.

It has two main uses:

- When working with SafeNet Agent for Windows Logon, without SafeNet Agent for TVP, you will be required to register each workstation's IP address to the SafeNet server and have each workstation communicate directly with it. With SafeNet Agent for TVP, each SafeNet Agent for Windows Logon can be pointed at the TVP Agent, and only the IP address of their SafeNet Agent for TVP needs to be registered with the SafeNet server.
- When using the SafeNet server API with a cloud application (such as MS Azure), you cannot be sure of the IP address of the cloud server, nor you are entitled to claim the IP address as your own. To solve this problem, you can point your cloud application(s) at the SafeNet Agent for TVP and register the agent as their Auth Node.

Configuring Additional Software Components

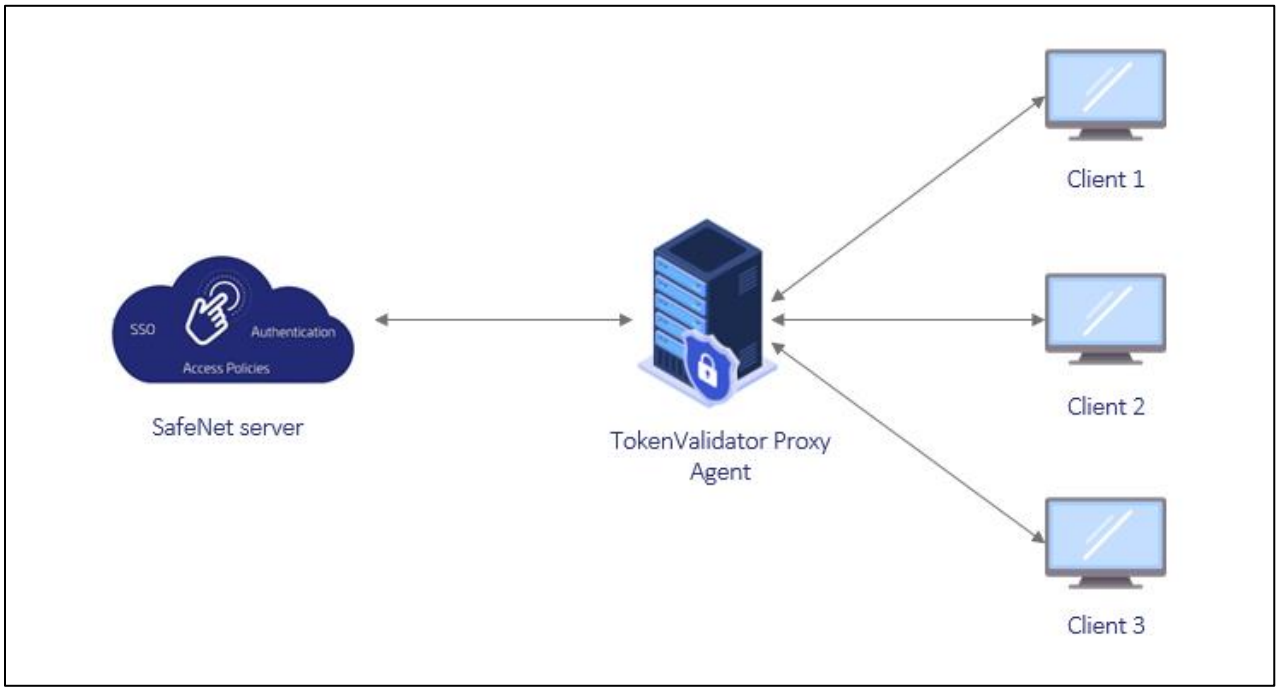
The following IIS components meet the minimum requirements to run the Web Adaptor. If additional IIS components are enabled, they do not need to be removed.

> Web Server
  - Common HTTP Features
    - Default Document
    - Static Content
  - Security
    - Request Filtering
    - Basic Authentication
    - Windows Authentication
  - Application Development
    - .NET Extensibility 4.5
    - .NET Extensibility
    - ASP.NET 4.5
    - ASP.NET
    - ISAPI Extensions
    - ISAPI Filters
    - WebSocket Protocol

> Management Tools
  - IIS Management Console
  - IIS 6 Management Compatibility
    - IIS 6 Metabase Compatibility

Architecture

If each client were to be connected directly to the SafeNet server, each would require its own IP address to be configured. By using SafeNet Agent for TVP, it needs to be configured just once with the IP address of the SafeNet server Auth Node. Multiple clients can then be connected to the SafeNet server through SafeNet Agent for TVP without further IP addresses being configured.



Push Authentication

The SafeNet Agent for TVP v2.1.0 (and above) transfers Push Authentication requests from all the SafeNet agents that support Push Authentication.

No configuration is required for SafeNet Agent for TVP to transfer the Push Authentication request.

NOTE: Push Authentication is supported only with MobilePASS+ tokens.

CHAPTER 2: Installation and Upgrade

This section describes the steps to install and upgrade the SafeNet Agent for TVP.

> **NOTE:** Always work in **Run as administrator** mode when installing, uninstalling, upgrading, enabling, or disabling the SafeNet Agent for TVP.

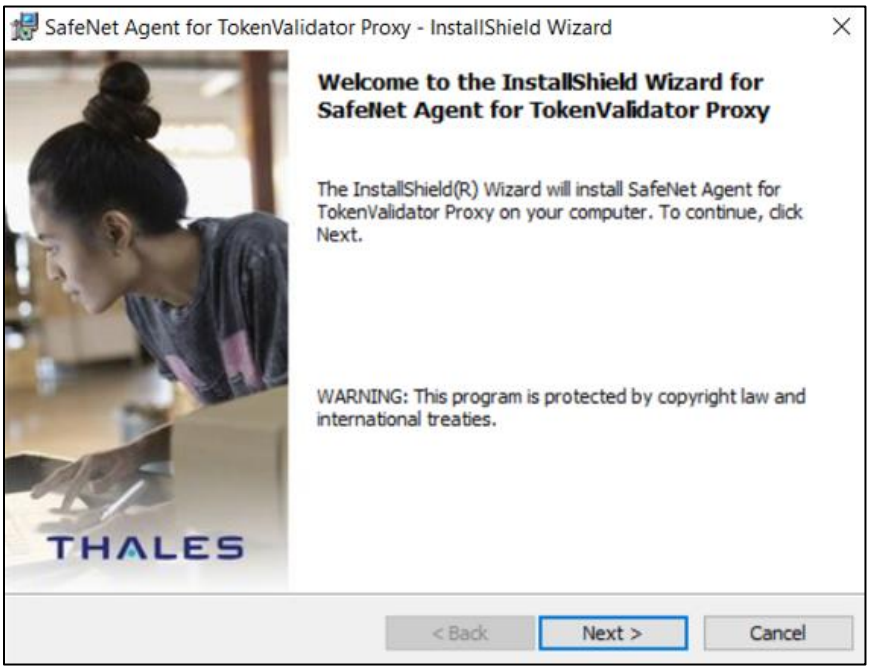
Installing TokenValidator Proxy Agent

Perform the following steps to install the SafeNet Agent for TVP:

1. Locate and run the following installation package:

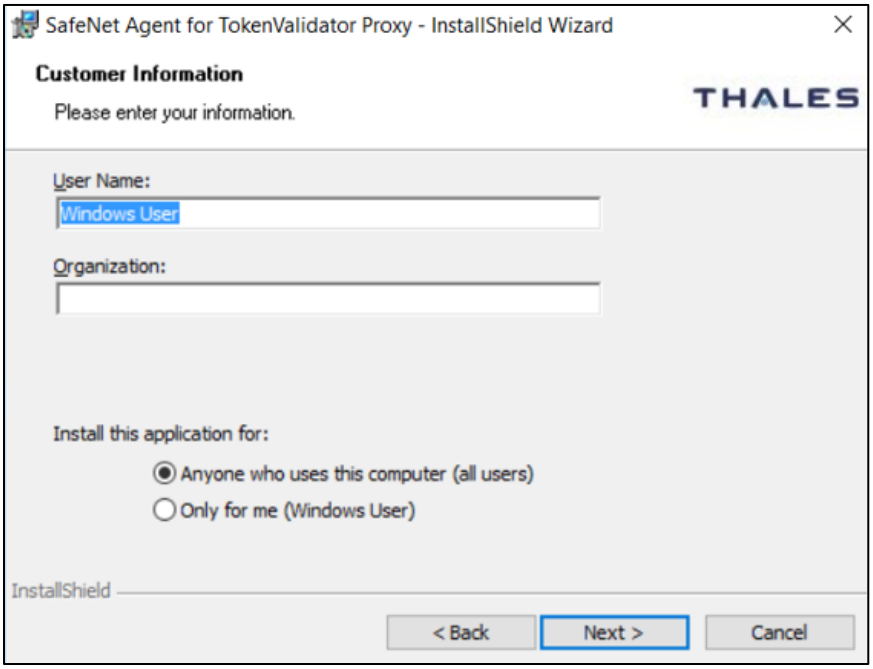
   `SafeNet Agent for TokenValidator Proxy x64.exe` (64-bit)

2. On the **Welcome to the InstallShield Wizard for SafeNet Agent for TokenValidator Proxy**, click **Next**.



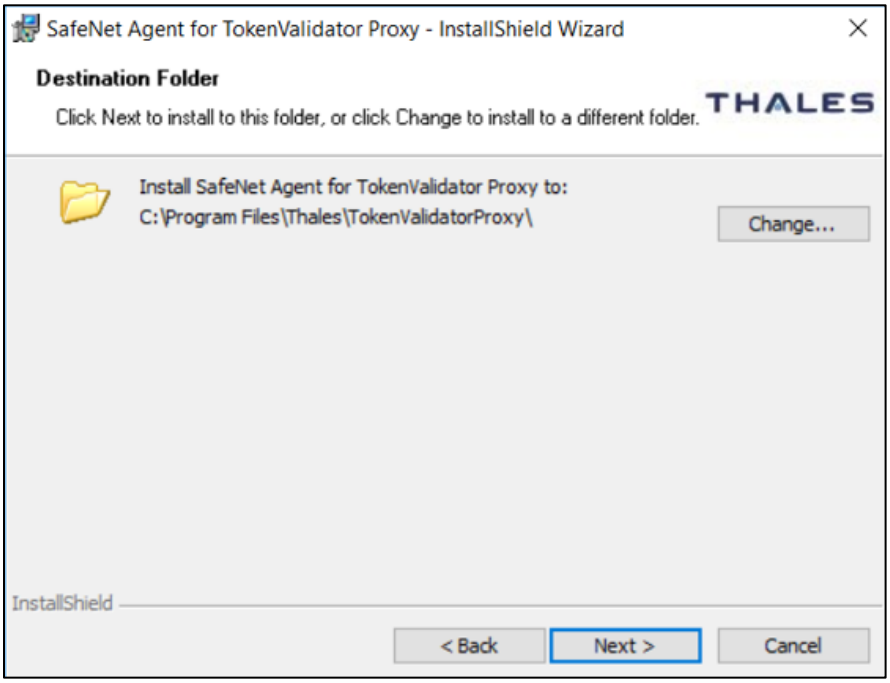
3. On the **License Agreement** window, read the software license agreement and to proceed, select **I accept the terms in the license agreement** option, and click **Next**.

4. On the **Customer Information** window, enter the following fields, and click **Next**:
   a. Enter the **User Name** and **Organization**.
   b. Select one of the following options to determine who can use the application:
      – **Anyone who uses this computer (all users)**
      – **Only for me (Windows User)**



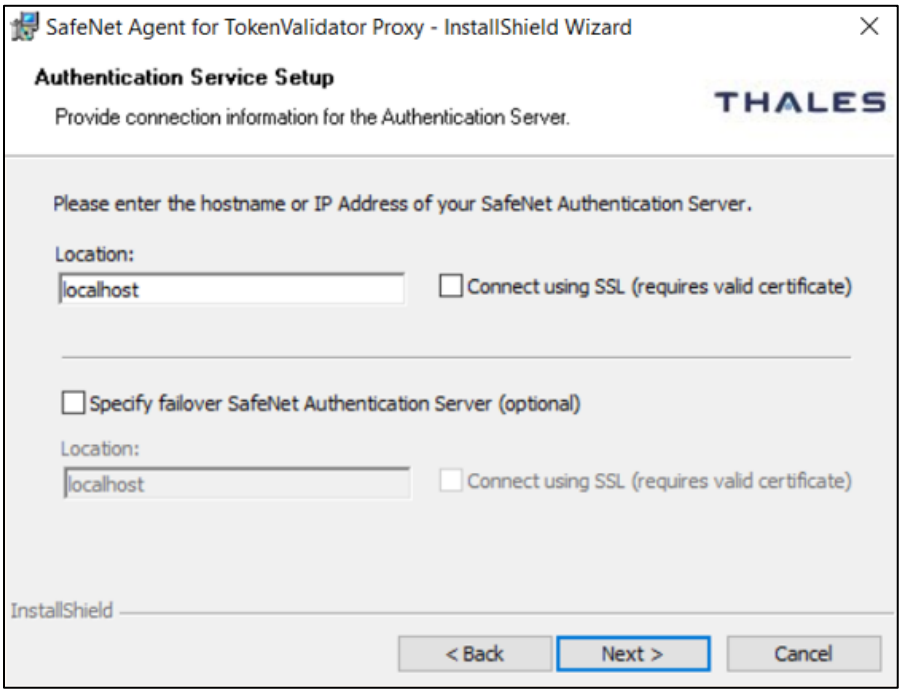
5. On the **Destination Folder** window, the installation folder is displayed.
   a. To change the location, click **Change** and browse to the required location. Select the required location, and then click **Next**.
   b. To accept the default installation folder as displayed, click **Next**.

> **NOTE:** If changing the default destination folder, do not locate on a root drive. This will cause the agent to malfunction.
>
> If a non-default destination folder is selected, the SAS Connectivity Test in connected agents will not work.



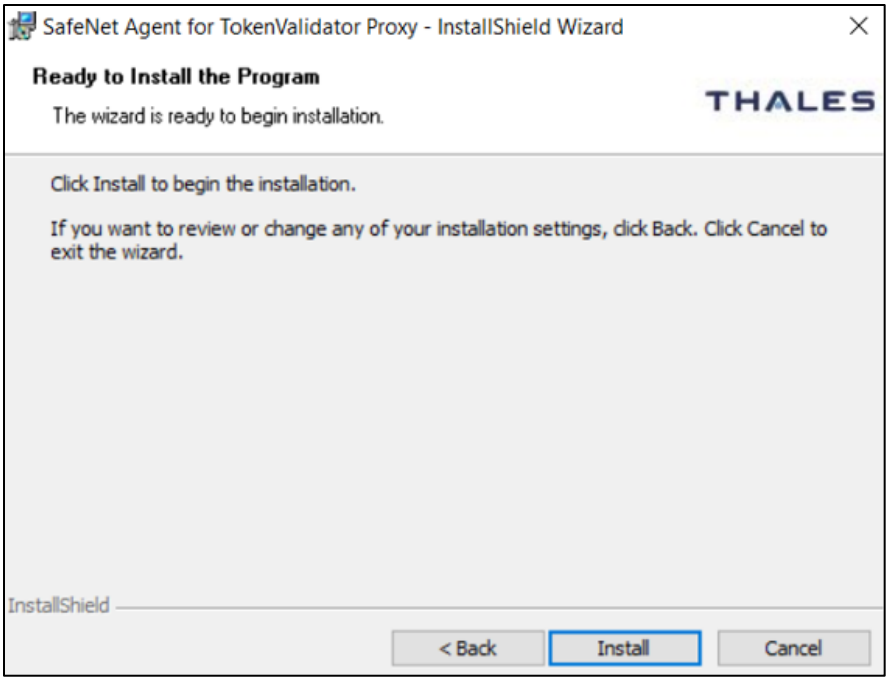
6. On the **Authentication Service Setup** window, enter the IP address of the SafeNet server and click **Next**.

> **NOTE:** The default location “localhost” is not valid. It must be replaced with the SafeNet Authentication Server IP address here, during installation, or changed later in the Windows Registry.

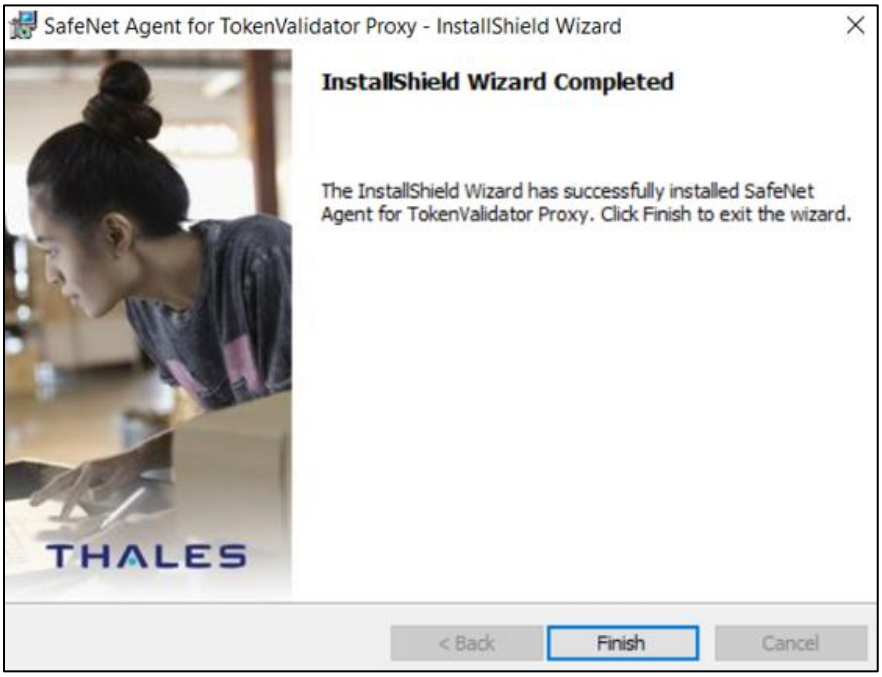


NOTE: The **Connect using SSL (requires valid certificate)** setting is relevant only for the connection between the SafeNet Agent for TVP and the SafeNet server. It will not affect the agents that are connected through the SafeNet Agent for TVP.

7. On the **Ready to Install the Program** window, click **Install** to begin installation.



8. When the installation process completes, the **InstallShield Wizard Completed** window is displayed. Click **Finish** to exit the installation wizard.



NOTE:
> Ensure that the IIS server is configured securely.
> Ensure the TLS private key of SSL certificate on IIS server is protected securely from any unauthorized access.

Upgrading TokenValidator Proxy Agent

The SafeNet Agent for TVP 3.0.1 supports upgrade from v1.02 (or later versions).

To upgrade the agent, run the installation and select the appropriate upgrade options when prompted.

See Installing TVP Agent section.

Replacing TokenValidator Proxy Agent

This version of SafeNet Agent for TVP does not support upgrade from version earlier than v1.02.

NOTE: Always work in **Run as administrator** mode when installing, uninstalling, upgrading, enabling, or disabling the SafeNet Agent for TVP.

To replace a SafeNet Agent for TVP version earlier than v1.02, perform the following steps:

1. Uninstall the previous version of the SafeNet Agent for TVP.
2. Ensure that all the installed files are removed. If not, remove them manually.
3. Install the latest version of SafeNet Agent for TVP.
4. Configure the latest version of SafeNet Agent for TVP.

CHAPTER 3: Configuration

Configuring Transport Layer Security

To configure TLS 1.1/1.2 support on the SafeNet Agent for TVP v2.1.0 (and above), set the registry settings as follows:

> **HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Client DisabledByDefault => 0x0**

> **HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client DisabledByDefault => 0x0**

NOTE: The agent will always connect with the highest enabled protocol.

Defining Main and Backup Servers

Once installed, the paths to the main SafeNet server and the backup SafeNet server can be changed, if required.

1. **Define main SafeNet server**: Enter the path to the main SafeNet server in the following Registry key:

   HKEY_LOCAL_MACHINE \SOFTWARE\CRYPTOCard\BlackShield ID\TokenValidatorProxy\PrimaryServiceURL

2. **Define backup SafeNet server**: Enter the path to the backup SafeNet server in the following Registry key:

   HKEY_LOCAL_MACHINE \SOFTWARE\CRYPTOCard\BlackShield ID\TokenValidatorProxy\OptionalSecondaryServiceURL

3. **Setting time interval** (**to check if main SafeNet server is operational**): Following failover to the backup SafeNet server, the SafeNet Agent for TVP will check if the SafeNet main server is running.

   The interval (in minutes) between checks is set in the following registry key (default value: 10 minutes):

   HKEY_LOCAL_MACHINE \SOFTWARE\CRYPTOCard\BlackShield ID\TokenValidatorProxy\PrimaryFailureIntervalMinutes

Configuring Logs

The logging level is set in the Windows Registry. Other related settings are changed in the configuration file located at:

`Program files\Thales\TokenValidatorProxy\TokenValidator\Log4Net.config`

Setting	Description
Logging level	**Default:** 3 To change the level, set the **LogLevel** registry key to the required level: **`HKEY_LOCAL_MACHINE \SOFTWARE\CRYPTOCard\BlackShield ID\TokenValidatorProxy\LogLevel`** **The following levels are available:** **1 Fatal –** Severe error events that are likely to cause the application to abort. **2 Error –** Error events that might still allow the application to continue running. **3 Warn –** Potentially harmful situations. **4 Info –** Informative messages that provide a high-level view of the progress of the application. **5 Debug –** Detailed informational events that are useful when debugging an application.
Name and location of Log file	**Default:** Logs\TVP.log To change the path and (/ or) name of the log file: 1. Open the configuration file **(Log4Net.config**) in a text editor. 2. Change the path and (/ or) file name using the following format: **`<file value="..\logs\TVP.Log" />`** **Note**: If you change the path, the new location must be accessible to all users. Also, writing to the Log folder requires Network Service permissions.
Maximum file size	**Default: 15 MB** **To determine the maximum file size:** 1. Open the configuration file **(Log4Net.config**) in a text editor. 2. Set **MaximumFileSize** to the required size, using the following format: **`<MaximumFileSize value="15MB" />`**
Number of rollover log files	**Default: 10** A specified number of log files are saved, with the oldest file being overwritten when a new file is generated. To change the number of rollover log file copies: 1. Open the configuration file **(Log4Net.config**) in a text editor. 2. Set **MaximumSizeRollBackups** to the required number using the following format: **`<MaximumSizeRollBackups value = "10" />`**

Activating Certificate Check

To activate the Certificate Check, set the Registry key **DisableCertificateCheck** to **0**, at the following location:

HKEY_LOCAL_MACHINE \SOFTWARE\CRYPTOCard\BlackShield ID\TokenValidatorProxy\ DisableCertificateCheck

To disable the Certificate Check, set the Registry key **DisableCertificateCheck** to **1**.

Default: 0

Configuring Proxy Server

To set a proxy server, add the following to the **web.config** file, located at the following location:

C:\Program Files\Thales\TokenValidatorProxy\TokenValidator\web.config

Insert in the section `<configuration>…</configuration>`

```
<system.net>
 <defaultProxy>
  <proxy proxyaddress="http://myproxyaddress:port"/>
 </defaultProxy>
 <settings>
  <servicePointManager expect100Continue="false"/>
 </settings>
</system.net>
```

where:

http://myproxyaddress:port is the address and port of the proxy.