SafeNet Authentication Service Token Validator Proxy Agent
Installation and Configuration Guide
Table of Contents

Preface ................................................................................................................................................... 4
Audience ................................................................................................................................................... 4
Related Documents ................................................................................................................................. 4
Support Contacts ...................................................................................................................................... 5

1 Overview ........................................................................................................................................... 6
Applicability ........................................................................................................................................... 6
Environment ........................................................................................................................................... 6
Introduction ........................................................................................................................................... 6
Architecture ........................................................................................................................................... 7
Push Authentication ................................................................................................................................. 7

2 Installation and Upgrade .................................................................................................................... 8
Installing Token Validator Proxy Agent .................................................................................................... 8
Upgrading Token Validator Proxy Agent .................................................................................................. 12
Replacing Token Validator Proxy Agent .................................................................................................. 12
Configuring Transport Layer Security .................................................................................................... 13

3 Configuration ...................................................................................................................................... 14
Defining Main and Backup Servers ........................................................................................................ 14
Configuring Logs ..................................................................................................................................... 14
Activating Certificate Check ................................................................................................................... 15
Configuring Proxy Server ....................................................................................................................... 16

4 Third Party License ............................................................................................................................. 17
Apache Logging Services ......................................................................................................................... 17
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 SafeNet Authentication Service (SAS)

All products manufactured and distributed by Gemalto 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.

Related Documents

The following documents contain related information:

- SafeNet Authentication Service Token Validator Proxy Agent v2.1: Customer Release Notes
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.

<table>
<thead>
<tr>
<th>Contact Method</th>
<th>Contact Information</th>
</tr>
</thead>
</table>
| **Address**                    | Gemalto  
|                                | 4690 Millennium Drive  
|                                | Belcamp, Maryland 21017, USA                                                        |
| **Phone**                      | US  
|                                | 1-800-545-6608                                                                       |
|                                | International  
|                                | 1-410-931-7520                                                                       |
| **Technical Support**          | https://serviceportal.safenet-inc.com                                                 |
| **Customer Portal**            | Existing customers with a Technical Support Customer Portal account can login to    |
|                                | manage incidents, get latest software upgrades, and access the Gemalto Knowledge    |
|                                | Base.                                                                                |
| **Documentation**              | All SAS documentation (Cloud, PCE, SPE, Token and Integration) can be found on the  |
|                                | SafeNet Knowledge Base page.                                                        |
|                                | All SAS Agents documentation can be found on the SafeNet Authentication Service      |
|                                | Downloads page.                                                                     |
Overview

Applicability

The information in this document applies to:

- SafeNet Authentication Service PCE/SPE 3.4 and later
- SafeNet Authentication Service Cloud Edition

Environment

<table>
<thead>
<tr>
<th>Supported Platforms</th>
<th>Windows 2016</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Windows 2012 R2</td>
</tr>
<tr>
<td></td>
<td>Windows 2008 R2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Supported Architecture</th>
<th>64-bit</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Additional Software Components</th>
<th>IIS 10</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>IIS 8.5</td>
</tr>
<tr>
<td></td>
<td>IIS 8.0</td>
</tr>
<tr>
<td></td>
<td>IIS 7.5</td>
</tr>
<tr>
<td></td>
<td>.NET 3.5</td>
</tr>
<tr>
<td></td>
<td>.NET 4.5 or above</td>
</tr>
</tbody>
</table>

Introduction

The function of the SafeNet Authentication Service (SAS) Token Validator Proxy (TVP) Agent is to implement proxy authentication requests from other agents to the SAS.

It has two main uses:

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

**Architecture**

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

**Push Authentication**

The SAS TVP Agent v2.1 transfers Push Authentication requests from all SAS agents that support Push Authentication.

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

NOTE: Push Authentication is supported only with MobilePASS+ tokens.
Installing Token Validator Proxy Agent

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

1. On the SAS TVP Agent computer, run the following installation file:
   SafeNet TokenValidator Proxy x64.exe (64-bit)
2. The Welcome ... window will be displayed. Click Next to continue.
3. On the License Agreement window, select I accept the terms in the license agreement, and click Next.

4. On the Customer Information window, complete 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. To change the location, click **Change** and browse to the required location. Select the required location, and 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 SAS 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.

![Authentication Service Setup Window](image)

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

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

![Ready to Install the Program Window](image)
8. When the installation process completes, the **InstallShield Wizard Completed** window is displayed. Click **Finish** to exit the installation wizard.

Following installation, the **SAS Proxy Source Server** service is installed on the Windows.

### Upgrading Token Validator Proxy Agent

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

Run the installation and when prompted, select the upgrade options.

See **Installing TVP Agent** section.

### Replacing Token Validator Proxy Agent

The SAS TVP Agent v2.1 does not support upgrade from versions earlier than v1.02.

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

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

1. Uninstall the previous version of the SAS TVP Agent.
2. Ensure that all installed files have been removed. If not, remove them manually.
3. Install SAS TVP Agent v2.1.
Configuring Transport Layer Security

To configure TLS 1.1/1.2 support on the SAS TVP Agent v2.1, 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 SAS server and the backup SAS server can be changed, if required.

1. **Define Main SAS Server**: Enter the path to the main SAS server in the following Registry key:
   
   ```
   HKEY_LOCAL_MACHINE \SOFTWARE\CRYPTOCard\BlackShield
   ID\TokenValidatorProxy\PrimaryServiceURL
   ```

2. **Define Backup SAS Server**: Enter the path to the backup SAS server in the following Registry key:

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

3. **Setting Time Interval (to check if main SAS Server is operational)**: Following failover to the backup SAS server, the SAS TVP Agent will check if the SAS 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\CRYPTOCard\BlackShield
ID\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:  
\[<MaximumFileSize value="15MB" />\]

No. 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\CRYPTOCARD\BlackShield ID\TokenValidatorProxy\TokenValidator\web.config`

Insert in the section `<system.web>…</system.web>`

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

<system.net>
  <settings>
    <servicePointManager expect100Continue="false"/>
  </settings>
</system.net>
```

where:

`http://myproxyaddress:port` is the address and port of the proxy.
Apache Logging Services

http://logging.apache.org

Copyright 2017 Gemalto.

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License.

You may obtain a copy of the License at http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.

See the License for the specific language governing permissions and limitations under the License.