All information herein is either public information or is the property of and owned solely by Gemalto NV. and/or its subsidiaries 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 Gemalto’s 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, Gemalto 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, Gemalto reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Gemalto 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 Gemalto 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.

Gemalto 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 Gemalto be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Gemalto products. Gemalto 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.

© 2015 Gemalto. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto N.V. and/or its subsidiaries and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

**Product Version:** 2.0  
**Document Part Number:** 007-012423-001, Rev. D  
**Release Date:** 16 August 2016
## Contents

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

2 Overview .............................................................................................................. 6
   Applicability ....................................................................................................... 6
   Environment ....................................................................................................... 6
   Introduction ......................................................................................................... 7
   Architecture ....................................................................................................... 7
   Push Authentication ........................................................................................... 8

3 Installation ........................................................................................................... 9
   Installing the SAS Token Validator Proxy Agent ............................................... 9
   Upgrading to SAS Token Validator Proxy Agent 2.0 ......................................... 14
   Replacing SAS Token Validator Proxy Agent Versions Prior to 1.02 ............... 14

4 Configuring SAS Token Validator Proxy Agent ............................................... 15
   Defining the Main and Backup SAS Servers ..................................................... 15
      Main SAS Server ......................................................................................... 15
      Backup SAS Server ................................................................................... 15
      Setting Time Interval for Checking if Main SAS Server is Operational ......... 15
   Configuring Logs ............................................................................................ 16
   Activating Certificate Check ........................................................................... 17
   Configuring Proxy Server ............................................................................... 17

5 Third Party License ............................................................................................. 18
   Apache Logging Services ................................................................................ 18
Preface

Audience

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

The document describes how to install and deploy SAS Token Validator Proxy Agent with SafeNet Authentication Service.

All products manufactured and distributed by Gemalto, Inc. 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 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>
<tbody>
<tr>
<td><strong>Address</strong></td>
<td>Gemalto</td>
</tr>
<tr>
<td></td>
<td>4690 Millennium Drive</td>
</tr>
<tr>
<td></td>
<td>Belcamp, Maryland 21017, USA</td>
</tr>
<tr>
<td><strong>Phone</strong></td>
<td>US                                     1-800-545-6608</td>
</tr>
<tr>
<td></td>
<td>International 1-410-931-7520</td>
</tr>
<tr>
<td><strong>Technical Support</strong></td>
<td><strong>Customer Portal</strong></td>
</tr>
<tr>
<td></td>
<td><a href="https://serviceportal.safenet-inc.com">https://serviceportal.safenet-inc.com</a></td>
</tr>
<tr>
<td></td>
<td>Existing customers with a Technical Support Customer Portal account can log in to</td>
</tr>
<tr>
<td></td>
<td>manage incidents, get the latest software upgrades, and access the Gemalto Knowledge</td>
</tr>
<tr>
<td></td>
<td>Base.</td>
</tr>
</tbody>
</table>
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 2012 R2</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Windows 2008 R2</td>
</tr>
<tr>
<td>Supported Architecture</td>
<td>64-bit</td>
</tr>
<tr>
<td>Additional Software Components</td>
<td></td>
</tr>
<tr>
<td>IIS 8.5</td>
<td></td>
</tr>
<tr>
<td>IIS 8.0</td>
<td></td>
</tr>
<tr>
<td>IIS 7.5</td>
<td></td>
</tr>
<tr>
<td>.Net 3.5</td>
<td></td>
</tr>
</tbody>
</table>
Introduction

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

It has two main uses:

- **When working with SAS Agent for Windows Logon**, without SAS Token Validator Proxy Agent you would be required to register each workstation's IP address to SAS and have each workstation communicate directly with SAS. With SAS Token Validator Proxy Agent, each SAS Agent for Windows Logon can be pointed at SAS Token Validator Proxy Agent, and only the IP address of the SAS Token Validator Proxy Agent needs to be registered with SAS.

- **When using SafeNet Authentication Service 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 this IP address as your own. To solve this problem, you can point your cloud application at the SAS Token Validator Proxy Agent and register your SAS Token Validator Proxy Agent as their Auth Node.

Architecture

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

SAS Token Validator Proxy Agent 2.0 transfers Push Authentication requests from all SAS agents that support Push Authentication.

No configuration is required for Push Authentication support.
Installation

Installing the SAS Token Validator Proxy Agent

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

1. On the SAS Token Validator Proxy Agent computer, run the following installation file:
   
   **SafeNet TokenValidator Proxy x64.exe** (64-bit)
   
   The Welcome to the InstallShield Wizard for SafeNet Authentication Service Token Validator Proxy window opens.

2. 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, do the following:
   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
   c. Click **Next**.
5. On the Destination Folder window, the installation folder is displayed. To change the location, click Change and then browse to the required location. Select the required location and click Next.

**NOTES:**

- 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**.

![Authentication Service Setup window](image)

**NOTE:** The **Connect using SSL (requires valid certificate)** setting is relevant only for the connection between the SAS Token Validator Proxy Agent and the SAS server. It will not affect the agents that are connected through the SAS Token Validator Proxy 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 process has been completed, the **InstallShield Wizard Completed** window opens. Click **Finish** to exit the installation wizard.

Following installation, the **SAS Proxy Source Server** service is installed on Windows.
Upgrading to SAS Token Validator Proxy Agent 2.0

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

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

See “Installing the SAS Token Validator Proxy Agent” on page 9.

Replacing SAS Token Validator Proxy Agent Versions Prior to 1.02

SAS Token Validator Proxy Agent 2.0 does not support upgrade from versions earlier than 1.02.

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

**To replace a SAS Token Validator Proxy Agent version previous to 1.02:**

1. Uninstall the previous version of SAS Token Validator Proxy Agent.
2. Ensure that all installed files have been removed. If not, remove them manually.
3. Install SAS Token Validator Proxy Agent 2.0.
4. Configure SAS Token Validator Proxy Agent 2.0.
Configuring SAS Token Validator Proxy Agent

Defining the Main and Backup SAS Servers

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

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

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

Setting Time Interval for Checking if Main SAS Server is Operational

Following failover to the Backup SAS server, SAS Token Validator Proxy Agent will check if the SAS Main server is running.

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

\HKEY_LOCAL_MACHINE\SOFTWARE\CRYPTOCard\BlackShield\ID\TokenValidatorProxy\PrimaryFailureIntervalMinutes
## Configuring Logs

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

```
Program files\CRYPTOCard\BlackShield ID\TokenValidatorProxy\Log4Net.config
```

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Logging level</strong></td>
<td><strong>Default:</strong> 3</td>
</tr>
<tr>
<td></td>
<td>To change the level, set the <code>LogLevel</code> registry key to the required level:</td>
</tr>
<tr>
<td></td>
<td><code>HKEY_LOCAL_MACHINE\SOFTWARE\CRYPTOCard\BlackShield ID\TokenValidatorProxy\LogLevel</code></td>
</tr>
<tr>
<td></td>
<td>The following levels are available:</td>
</tr>
<tr>
<td></td>
<td>1 Fatal – Severe error events that are likely to cause the application to abort.</td>
</tr>
<tr>
<td></td>
<td>2 Error - Error events that might still allow the application to continue running.</td>
</tr>
<tr>
<td></td>
<td>3 Warn - Potentially harmful situations.</td>
</tr>
<tr>
<td></td>
<td>4 Info – Informative messages that provide a high-level view of the progress of the application.</td>
</tr>
<tr>
<td></td>
<td>5 Debug - Detailed informational events that are useful when debugging an application.</td>
</tr>
<tr>
<td><strong>Name and location of Log file</strong></td>
<td><strong>Default:</strong> Logs\TVP.log</td>
</tr>
<tr>
<td></td>
<td>To change the path and/or name of the log file:</td>
</tr>
<tr>
<td></td>
<td>1. Open the configuration file <code>(Log4Net.config)</code> in a text editor.</td>
</tr>
<tr>
<td></td>
<td>2. Change the path and or file name using the following format:</td>
</tr>
<tr>
<td></td>
<td><code>&lt;file value=&quot;\logs\TVP.Log&quot; /&gt;</code></td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> If you change the path, the new location must be accessible to all users. Also, writing to the Log folder requires Network Service permissions.</td>
</tr>
<tr>
<td><strong>Maximum file size</strong></td>
<td><strong>Default:</strong> 15 MB</td>
</tr>
<tr>
<td></td>
<td>To determine the maximum file size:</td>
</tr>
<tr>
<td></td>
<td>1. Open the configuration file <code>(Log4Net.config)</code> in a text editor.</td>
</tr>
<tr>
<td></td>
<td>2. Set <code>MaximumFileSize</code> to the required size, using the following format:</td>
</tr>
<tr>
<td></td>
<td><code>&lt;MaximumFileSize value=&quot;15MB&quot; /&gt;</code></td>
</tr>
<tr>
<td><strong>No. of rollover log files</strong></td>
<td><strong>Default:</strong> 10</td>
</tr>
<tr>
<td></td>
<td>A specified number of log files are saved, with the oldest file being overwritten when a new file is generated.</td>
</tr>
<tr>
<td></td>
<td>To change the number of rollover log file copies:</td>
</tr>
<tr>
<td></td>
<td>1. Open the configuration file <code>(Log4Net.config)</code> in a text editor.</td>
</tr>
<tr>
<td></td>
<td>2. Set <code>MaximumSizeRollBackups</code> to the required number using the following format:</td>
</tr>
<tr>
<td></td>
<td><code>&lt;MaximumSizeRollBackups value = &quot;10&quot; /&gt;</code></td>
</tr>
</tbody>
</table>
Activating Certificate Check

To disable the Certificate Check, set the Registry key DisableCertificateCheck to 1.
To activate the Certificate Check, set the Registry key DisableCertificateCheck to 0.
Default: 0

HKEY_LOCAL_MACHINE\SOFTWARE\CRYPTOCARD\BlackShield ID\TokenValidatorProxy\DisableCertificateCheck

Configuring Proxy Server

To set a proxy server, add the following to the web.config file, located at C:\Program Files\CRYPTOCARD\BlackShield ID\TokenValidatorProxy\TokenValidatorProxy\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 2016 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.