SafeNet Authentication Service
Integration Guide

Using SAS as an Identity Provider for Blue Coat ProxySG
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.

Document Part Number: 007-013299-001, Rev. A
Release Date: October 2015
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Third-Party Software Acknowledgement</td>
<td>4</td>
</tr>
<tr>
<td>Description</td>
<td>4</td>
</tr>
<tr>
<td>Applicability</td>
<td>4</td>
</tr>
<tr>
<td>Environment</td>
<td>5</td>
</tr>
<tr>
<td>Audience</td>
<td>5</td>
</tr>
<tr>
<td>SAML Authentication using SAS Cloud</td>
<td>5</td>
</tr>
<tr>
<td>SAML Authentication using SAS-SPE and SAS-PCE</td>
<td>5</td>
</tr>
<tr>
<td>SAML Authentication Flow using SAS</td>
<td>5</td>
</tr>
<tr>
<td>SAML Prerequisites</td>
<td>6</td>
</tr>
<tr>
<td>Configuring Blue Coat ProxySG</td>
<td>7</td>
</tr>
<tr>
<td>Downloading the SAS Metadata</td>
<td>7</td>
</tr>
<tr>
<td>Downloading the SafeNet Identity Provider Certificate</td>
<td>7</td>
</tr>
<tr>
<td>Creating a SAML Realm</td>
<td>7</td>
</tr>
<tr>
<td>Configuring the CA Certificate List</td>
<td>11</td>
</tr>
<tr>
<td>Configuring an Authentication Policy</td>
<td>13</td>
</tr>
<tr>
<td>Configuring SafeNet Authentication Service</td>
<td>19</td>
</tr>
<tr>
<td>Synchronizing Users Stores to SAS</td>
<td>19</td>
</tr>
<tr>
<td>Assigning an Authenticator in SAS</td>
<td>19</td>
</tr>
<tr>
<td>Adding Blue Coat ProxySG as a Service Provider (SP) in SAS</td>
<td>20</td>
</tr>
<tr>
<td>Enabling SAML Services in SAS</td>
<td>23</td>
</tr>
<tr>
<td>Running the Solution</td>
<td>27</td>
</tr>
<tr>
<td>Support Contacts</td>
<td>29</td>
</tr>
</tbody>
</table>
Third-Party Software Acknowledgement

This document is intended to help users of SafeNet products when working with third-party software, such as Blue Coat ProxySG.

Material from third-party software is being used solely for the purpose of making instructions clear. Screen images and content obtained from third-party software will be acknowledged as such.

Description

SafeNet Authentication Service delivers a fully automated, versatile, and strong authentication-as-a-service solution.

With no infrastructure required, SafeNet Authentication Service provides smooth management processes and highly flexible security policies, token choice, and integration APIs.

The Blue Coat ProxySG appliances provide complete control over all of your web traffic, delivering world-class threat protection. Robust features include user authentication, web filtering, data loss prevention, inspection, and visibility of SSL-encrypted traffic (including the ability to stream decrypted content to an external server with an Encrypted Tap license), content caching, bandwidth management, stream-splitting, and more.

The Blue Coat Secure Web Gateway Virtual Appliance (SWG VA) combines the market-leading security capabilities of Blue Coat ProxySG with the flexibility of virtualization to provide a cost-effective enterprise branch office solution. With the Blue Coat SWG VA, businesses can support web security and other critical remote office infrastructure on a common platform, reducing costs and IT resource requirements.

This document describes how to:

- Deploy multi-factor authentication (MFA) options in Blue Coat ProxySG using SafeNet one-time password (OTP) authenticators managed by SafeNet Authentication Service.
- Configure SAML authentication in Blue Coat ProxySG using SafeNet Authentication Service as an identity provider.

It is assumed that the Blue Coat ProxySG environment is already configured and working with static passwords prior to implementing multi-factor authentication using SafeNet Authentication Service.

Blue Coat ProxySG can be configured to support multi-factor authentication in several modes. The SAML authentication will be used for the purpose of working with SafeNet Authentication Service.

Applicability

The information in this document applies to:

- **SafeNet Authentication Service (SAS)**—SafeNet’s cloud-based authentication service.
- **SafeNet Authentication Service – Service Provider Edition (SAS-SPE)**—A server version that is used by service providers to deploy instances of SafeNet Authentication Service.
- **SafeNet Authentication Service – Private Cloud Edition (SAS-PCE)**—A server version that is used to deploy the solution on-premises in the organization.
Environment

The integration environment that was used in this document is based on the following software versions:

- **SafeNet Authentication Service (Cloud)**
- **Blue Coat ProxySG (Virtual Appliance)—Model No. VA-100**
- **Blue Coat ProxySG (Software)—Version SGOS 6.5.6.4 SWG Edition**

Audience

This document is targeted to system administrators who are familiar with Blue Coat ProxySG, and are interested in adding multi-factor authentication capabilities using SafeNet Authentication Service.

SAML Authentication using SAS Cloud

SAS Cloud provides a service for SAML authentication that is already implemented in the SAS Cloud environment and can be used without any installation.

![SAML Protocol](image)

SAML Authentication using SAS-SPE and SAS-PCE

In addition to the pure cloud-based offering, SafeNet Authentication Service comes with two on-premises versions:

- **SafeNet Authentication Service – Service Provider Edition (SPE)**—An on-premises version of SafeNet Authentication Service targeted at service providers interested in hosting SAS in their data center.

- **SafeNet Authentication Service – Private Cloud Edition (PCE)**—An on-premises version of SafeNet Authentication Service targeted at organizations interested in hosting SAS in their private cloud environment.

For both on-premises versions, SAS can be integrated with the Shibboleth infrastructure, which uses a special on-premises agent called SafeNet Authentication Service Agent for Shibboleth.

For more information on how to install and configure the SafeNet Authentication Service Agent for Shibboleth, refer to the SafeNet Support Portal.
SafeNet Authentication Service communicates with a large number of service providers and cloud-based services solutions using the SAML protocol.

The image below describes the dataflow of a multi-factor authentication transaction for Blue Coat ProxySG.

1. A user attempts to log on to Blue Coat ProxySG. The user is redirected to SafeNet Authentication Service (SAS). SAS collects and evaluates the user’s credentials.

2. SAS returns a response to Blue Coat ProxySG, accepting or rejecting the user’s authentication request.

**SAML Prerequisites**

To enable SafeNet Authentication Service to receive SAML authentication requests from Blue Coat ProxySG, ensure the following:

- End users can authenticate from the Blue Coat ProxySG environment with a static password.
- The Blue Coat ProxySG virtual appliance should be configured as a reverse proxy with HTTPS services.
Configuring Blue Coat ProxySG

Adding SafeNet Authentication Service as an identity provider in Blue Coat ProxySG requires the following:

- Downloading the SAS Metadata, page 7
- Downloading the SafeNet Identity Provider Certificate, page 7
- Creating a SAML Realm, page 7
- Configuring the CA Certificate List, page 11
- Configuring an Authentication Policy, page 13

Downloading the SAS Metadata

Browse to the https://idp1.cryptocard.com/idp/shibboleth URL. The SAS metadata will automatically download. Save it locally on your machine.

Downloading the SafeNet Identity Provider Certificate

Browse to the https://cloud.safenet-inc.com/console/cert/idp.crt URL. The SafeNet identity provider certificate will automatically download. Save it locally on your machine.

Creating a SAML Realm

1. In a web browser, open the following URL and log in as an administrator:

   https://<ProxySG_IP_Address>:8082

   where ProxySG_IP_Address is the IP address of the ProxySG virtual appliance, and 8082 is the default management port.

2. On the Blue Coat Management Console window, click the Configuration tab, and then in the left pane, click Authentication > SAML.

3. In the right pane, on the SAML Realms tab, click New.
4. On the **Add SAML Realm** window, complete the following fields, and then click **OK**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Realm name</td>
<td>Enter a valid name for the new SAML realm (e.g., SAS_SAML).</td>
</tr>
<tr>
<td>Federated IDP CCL</td>
<td>Select the browser-trusted CCL.</td>
</tr>
<tr>
<td>Virtual host</td>
<td>Enter the hostname for the SAML endpoint.</td>
</tr>
</tbody>
</table>

(The screen image above is from Blue Coat® software. Trademarks are the property of their respective owners.)

5. Click **Apply**.

(The screen image above is from Blue Coat® software. Trademarks are the property of their respective owners.)
6. Click OK.

![Changes Done Successfully](image)

*(The screen image above is from Blue Coat® software. Trademarks are the property of their respective owners.)*

7. Select the newly created SAML realm (for example, SAS_SAML), and then click Edit.

![Blue Coat ProxySG Management Console](image)

*(The screen image above is from Blue Coat® software. Trademarks are the property of their respective owners.)*

8. On the Edit SAML Realm window, complete the following fields, and then click OK.

<table>
<thead>
<tr>
<th>Federated IDP entity ID</th>
<th>Enter <a href="https://idp1.cryptocard.com/idp/shibboleth">https://idp1.cryptocard.com/idp/shibboleth</a>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Federated IDP POST URL</td>
<td>Enter <a href="https://idp1.cryptocard.com/idp/profile/SAML2/POST/SSO">https://idp1.cryptocard.com/idp/profile/SAML2/POST/SSO</a>.</td>
</tr>
<tr>
<td>Federated IDP Redirect URL</td>
<td>Enter <a href="https://idp1.cryptocard.com/idp/profile/SAML2/Redirect/SSO">https://idp1.cryptocard.com/idp/profile/SAML2/Redirect/SSO</a>.</td>
</tr>
</tbody>
</table>
9. Click **Apply**.

10. Click **OK**.
Configuring the CA Certificate List

The ProxySG appliance CA certificate list (CCL) must contain the IDP’s signing certificates.

Importing the IDP Certificate

1. On the Blue Coat Management Console window, click the Configuration tab, and then in the left pane, click SSL > CA Certificates.

   ![Blue Coat Management Console](image)

   *(The screen image above is from Blue Coat® software. Trademarks are the property of their respective owners.)*

2. In the right pane, on the CA Certificates tab, click Import.

3. On the Import CA Certificate window, complete the following fields, and then click OK.

<table>
<thead>
<tr>
<th>CA Cert Name</th>
<th>Enter the name of the certificate.</th>
</tr>
</thead>
</table>

   ![Import CA Certificate](image)

   *(The screen image above is from Blue Coat® software. Trademarks are the property of their respective owners.)*

4. Click Apply, and then click OK.
Creating a CA Certificate List

1. On the Blue Coat Management Console window, click the Configuration tab, and then in the left pane, click SSL > CA Certificates.

2. In the right pane, on the CA Certificate Lists tab, select browser-trusted, and then click Edit.

3. On the Edit CA Certificate List window, perform the following steps:
   a. In the list box on the left, select the imported identity provider certificate (for example, SafeNet).
   b. Click Add >> to move the selected certificate to the list box on the right.
   c. Click OK.
4. Click **Apply**.

![Image of Blue Coat Management Console]

*(The screen image above is from Blue Coat® software. Trademarks are the property of their respective owners.)*

5. Click **OK**.

![Image of Changes Done Successfully]

*(The screen image above is from Blue Coat® software. Trademarks are the property of their respective owners.)*

### Configuring an Authentication Policy

With an authentication realm configured, now configure a policy on the ProxySG appliance to authenticate, log, and control user access to the web server.

The sections below explain about setting up rules to authenticate users, restrict access for specific users and groups, and deny all other access to the web server.

### Creating the Web Authentication Layer

1. On the **Blue Coat Management Console** window, click the **Configuration** tab, and in the left pane, click **Policy > Visual Policy Manager**.

![Image of Blue Coat Management Console]

*(The screen image above is from Blue Coat® software. Trademarks are the property of their respective owners.)*
2. In the right pane, click **Launch**.

3. On the **Visual Policy Manager** window, click **Policy**, and then select **Add Web Authentication Layer**.

4. On the **Add New Layer** window, enter a descriptive name for the Web Authentication Layer, and then click **OK**.

5. Right-click on the **Action** column of the default rule, and then select **Set**.
6. On the Set Action Object window, click **New**, and then select **Authenticate**.

![Set Action Object window](image1)

(The screen image above is from Blue Coat® software. Trademarks are the property of their respective owners.)

7. On the **Add Authenticate Object** window, complete the following fields, and then click **OK**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of the Authenticate Object (for example, <strong>Authenticate</strong>).</td>
</tr>
<tr>
<td>Realm</td>
<td>Select the SAML realm that you created in “Creating a SAML Realm” on page 7 (for example, <strong>SAS_SAML</strong>).</td>
</tr>
<tr>
<td>Mode</td>
<td>Select <strong>Auto</strong>. The appliance will automatically determine which mode to use.</td>
</tr>
</tbody>
</table>

![Add Authenticate Object window](image2)

(The screen image above is from Blue Coat® software. Trademarks are the property of their respective owners.)
8. On the **Set Action Object** window, click **OK**.

   ![Set Action Object](image)

   *(The screen image above is from Blue Coat® software. Trademarks are the property of their respective owners.)*

**Creating a Web Access Rule**

Create a policy rule that enables the ProxySG appliance to grant users access to the network.

1. **On the Blue Coat Management Console** window, click the **Configuration** tab, and in the left pane, click **Policy > Visual Policy Manager**.

   ![Blue Coat Management Console](image)

   *(The screen image above is from Blue Coat® software. Trademarks are the property of their respective owners.)*

2. **In the right pane, click **Launch**.**

3. **On the **Visual Policy Manager** window, click **Policy**, and then select **Add Web Access Layer**.**

   ![Visual Policy Manager](image)

   *(The screen image above is from Blue Coat® software. Trademarks are the property of their respective owners.)*
4. On the **Add New Layer** window, enter a descriptive name for the Web Access Layer, and then click **OK**.

   ![Add New Layer Window](image1.png)

   *(The screen image above is from Blue Coat® software. Trademarks are the property of their respective owners.)*

5. Right-click on the **Source** column of the default rule, and then select **Set**.

   ![Set Source Object](image2.png)

   *(The screen image above is from Blue Coat® software. Trademarks are the property of their respective owners.)*

6. On the **Set Source Object** window, select **Authenticated User**, and then click **OK**.

   ![Set Source Object Window](image3.png)

   *(The screen image above is from Blue Coat® software. Trademarks are the property of their respective owners.)*
7. Right-click on the **Action** column of the default rule, and then select **Allow**. The icon in the **Action** column changes from red to green.

8. Click **Install policy**.

9. Click **OK**.
Configuring SafeNet Authentication Service

The deployment of multi-factor authentication using SAS with Blue Coat ProxySG using SAML authentication requires:

- Synchronizing Users Stores to SAS, page 19
- Assigning an Authenticator in SAS, page 19
- Adding Blue Coat ProxySG as a Service Provider (SP) in SAS, page 20
- Enabling SAML Services in SAS, page 23

Synchronizing Users Stores to SAS

Before SAS can authenticate any user in your organization, you need to create a user store in SAS that reflects the users who would need to use multi-factor authentication. User records are created in the SAS user store using one of the following methods:

- Manually, one user at a time, using the Create User shortcut
- Manually, by importing one or more user records via a flat file
- Automatically, by synchronizing with your Active Directory/LDAP server using the SAS Synchronization Agent

For further details on importing users to SafeNet Authentication Service, refer to “Creating Users” in the SafeNet Authentication Service Subscriber Account Operator Guide:


All SafeNet Authentication Service documentation can be found on the SafeNet Knowledge Base site.

Assigning an Authenticator in SAS

SAS supports a number of authentication methods that can be used as a second authentication factor for users authenticating through Blue Coat ProxySG.

The following authenticators are supported:

- eToken PASS
- RB-1 keypad token
- KT-4 token
- SafeNet GOLD
- SMS token
- MP-1 software token
- GrIDsure
- MobilePASS
Authenticators can be assigned to users in two ways:

- **Manual provisioning**—Assign an authenticator to users one at a time.
- **Provisioning rules**—The administrator can set provisioning rules in SAS so that the rules will be triggered when group memberships and other user attributes change. An authenticator will be assigned automatically to the user.

Refer to “provisioning” in the *SafeNet Authentication Service - Subscriber Account Operator Guide* to learn how to provision the different authentication methods to the users in the SAS user store.


**Adding Blue Coat ProxySG as a Service Provider (SP) in SAS**

Add a service provider entry in the SAS **SAML Service Providers** module to prepare it to receive SAML authentication requests from Blue Coat ProxySG. You will need the metadata of Blue Coat ProxySG.

You can export the Blue Coat ProxySG metadata from:

https://<IP-address>:8082/saml/metadata/<realm-name>/sp

where **IP-address** is the ProxySG appliance IP address, and **realm-name** is name of the realm created in “Creating a SAML Realm” on page 7.

**To add Blue Coat ProxySG as a Service Provider in SAS:**

1. Log in to the SAS console with an Operator account.
2. Click the COMMS tab and then click **SAML Service Providers**.

![SAML Service Providers](image)

3. In the **SAML Service Providers** module, click the **SAML 2.0 Settings** link.

![SAML 2.0 Settings](image)

4. Click **Add**.

![Add SAML 2.0 Settings](image)
5. In the **Add SAML 2.0 Settings** section, complete the following fields, and then click **Apply**:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Enter the Blue Coat ProxySG name.</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAML 2.0 Metadata</td>
<td>Select <strong>Upload Existing Metadata File</strong>. Click the <strong>Choose File</strong> button, select the service provider’s metadata file, and then click <strong>Open</strong>.</td>
</tr>
</tbody>
</table>

![Add SAML 2.0 Setting](image)

**NOTE:** The remaining options are used to customize the appearance of the logon page presented to the user. For more information on logon page customization, refer “Configure SAML Service” in the **SAML Configuration Guide**: http://www2.safenet-inc.com/sas/implementation-guides/sas-on-prem/SAS-QS-SAML.pdf

Blue Coat ProxySG is added as a service provider in the system.

![SAML Service Providers](image)
Enabling SAML Services in SAS

After Blue Coat ProxySG has been added to SAS as a service provider, the users should be granted permission to use this service provider with SAML authentication.

There are two methods to enable the user to use the service provider:

- Manually, one user at a time, using SAML Services module
- Automatically, by defining groups of users, using SAML Provisioning Rules

Using the SAML Services Module

Manually enable a single user to authenticate against one or more configured SAML service providers.

1. Log in to the SAS console with an Operator account.

2. Click the ASSIGNMENT tab, and then search for the required user.

3. Click the appropriate user in the User ID column.
4. Click **SAML Services**.

5. Click **Add**.

6. Under **Add SAML Service**, do the following:
   a. From the **Service** menu, select the Blue Coat ProxySG service provider.
   b. In **SAML Login ID** field, select the appropriate option (**User ID**, **E-mail**, or **Custom**) to be sent as a UserID to Blue Coat ProxySG in the response.
   c. Click **Add**.
The user can now authenticate to Blue Coat ProxySG using SAML authentication.

### Using SAML Provisioning Rules

Use this module to enable groups of users to authenticate to SAML service providers.

1. Log in to the SAS console with an Operator account.

2. Click the **POLICY** tab, and then click **Automation Policies**.
3. Click the **SAML Provisioning Rules** link.

4. Click **New Rule**.

5. Configure the following fields, and then click **Add**:

   - **Rule Name**: Enter a name for the rule.
   - **User is in container**: Users affected by this rule must be in the selected container.
   - **Groups**: The **Virtual Server groups** box lists all groups. Click the user groups that will be affected by the rule, and then click the right arrow to move it to the **Used by rule** box.
   - **Parties**: The **Relying Parties** box lists all service providers. Click the service providers that the groups of users will authenticate to, and then click the right arrow to move it to **Rule Parties** box.
   - **SAML Login ID**: Select **User ID**. The User ID will be returned to the service provider in the SAML assertion.
Running the Solution

Before running the solution, ensure that the Blue Coat ProxySG virtual appliance is configured as a reverse proxy with HTTPS service.

In this solution, the SafeNet GrIDsure token is used as the enrolled token.

1. Open the following URL in a web browser: https://<Virtual IP of Bluecoat>
   where Virtual IP of Bluecoat is an IP address that is configured on the ProxySG appliance.
2. You are redirected to the SAS Login page. Enter your User Name, and then click Login.
3. In the **Password** field, enter your Personal Identification Pattern (PIP), and then click **Login**.

If authentication is successful, you are allowed to access the requested web page.
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, Inc.</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>United States 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><a href="https://serviceportal.safenet-inc.com">https://serviceportal.safenet-inc.com</a></td>
</tr>
<tr>
<td><strong>Customer Portal</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>