SafeNet Authentication Service
Push OTP Integration Guide

Using RADIUS Protocol 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:** 007-13347-001, Rev. A

**Release Date:** November 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>5</td>
</tr>
<tr>
<td>Environment</td>
<td>5</td>
</tr>
<tr>
<td>Audience</td>
<td>5</td>
</tr>
<tr>
<td>RADIUS-based Authentication using SAS Cloud</td>
<td>5</td>
</tr>
<tr>
<td>RADIUS Authentication Flow using SAS</td>
<td>6</td>
</tr>
<tr>
<td>Push OTP Prerequisites</td>
<td>7</td>
</tr>
<tr>
<td>RADIUS Prerequisites</td>
<td>7</td>
</tr>
<tr>
<td>Configuring SafeNet Authentication Service</td>
<td>7</td>
</tr>
<tr>
<td>Creating Users Stores in SAS</td>
<td>8</td>
</tr>
<tr>
<td>Assigning an Authenticator in SAS</td>
<td>8</td>
</tr>
<tr>
<td>Adding Blue Coat ProxySG as an Authentication Node in SAS</td>
<td>9</td>
</tr>
<tr>
<td>Checking the SAS RADIUS Server’s IP Address</td>
<td>11</td>
</tr>
<tr>
<td>Enabling the Software Token Push OTP Setting</td>
<td>12</td>
</tr>
<tr>
<td>Enabling the Allowed Targets Policy</td>
<td>13</td>
</tr>
<tr>
<td>Configuring Blue Coat ProxySG</td>
<td>15</td>
</tr>
<tr>
<td>Creating a RADIUS Authentication Realm</td>
<td>15</td>
</tr>
<tr>
<td>Configuring RADIUS Realm Properties</td>
<td>16</td>
</tr>
<tr>
<td>Configuring RADIUS Realm General Properties</td>
<td>18</td>
</tr>
<tr>
<td>Configuring an Authentication Policy</td>
<td>19</td>
</tr>
<tr>
<td>Running the Solution</td>
<td>25</td>
</tr>
<tr>
<td>Support Contacts</td>
<td>28</td>
</tr>
</tbody>
</table>
Third-Party Software Acknowledgement

This document is intended to help users of Gemalto 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:

- Configure Blue Coat ProxySG to work with SafeNet Authentication Service in RADIUS mode.

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 RADIUS protocol will be used for the purpose of working with the SafeNet Authentication Service Push OTP solution.

The primary objective of the Push OTP solution is to reduce the friction around two-factor authentication, and provide users with an improved two-factor authentication experience.

Most of the users always carry a device that can be used as a second factor of authentication. Using the mobile phone as an authenticator replaces the need for a user to carry any additional hardware. So, with Push OTP, a user can:

- Receive authentication requests in real-time via push notifications to the smart phone.
- Assess the validity of the request with the information displayed on the screen.
- Respond quickly with a one-tap response to approve or deny the authentication.
Applicability

The information in this document applies to:

- **SafeNet Authentication Service (SAS)**—SafeNet’s cloud-based authentication service
- **MobilePASS+ application**

Environment

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

- **SafeNet Authentication Service (SAS)**—SafeNet’s cloud-based authentication service
- **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.

RADIUS-based Authentication using SAS Cloud

SAS Cloud provides two RADIUS mode topologies:

- **SAS cloud hosted RADIUS service**—A RADIUS service that is already implemented in the SAS cloud environment and can be used without any installation or configuration requirements.

- **Local RADIUS hosted on-premises**—A RADIUS agent that is implemented in the existing customer’s RADIUS environment. The agent forwards the RADIUS authentication requests to the SAS cloud environment. The RADIUS agent can be implemented on a Microsoft NPS/IAS or FreeRADIUS server.
This document demonstrates the solution using the SAS cloud hosted RADIUS service.

For more information on how to install and configure SAS Agent for IAS/NPS, refer to: http://www2.safenet-inc.com/sas/implementation-guides/sfnt-updates/SAS-Agents-IASNPS.pdf

For more details on how to install and configure FreeRADIUS, refer to the SafeNet Authentication Service FreeRADIUS Agent Configuration Guide.

**RADIUS Authentication Flow using SAS**

SafeNet Authentication Service communicates with a large number of VPN and access-gateway solutions using the RADIUS 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 using a Push OTP authenticator.
2. Blue Coat ProxySG sends a RADIUS request with the user’s credentials to SafeNet Authentication Service for validation.
3. SAS identifies the user or mobile device, and detects that the OTP field is empty. Then:
   - SAS will directly trigger a Push OTP authentication request.
   - The user receives a push notification on the configured mobile device to indicate there is a login request pending.
   - The user taps on the notification to view the login request details, and can respond with a tap to approve or deny the request (approving will require providing the token’s PIN code).
4. The SAS authentication reply is sent back to Blue Coat ProxySG.
5. The user is granted or denied access to Blue Coat ProxySG based on the OTP value calculation results from SAS.
Push OTP Prerequisites

In order to use SAS Push OTP, you will need:

- SAS configured to enable Push OTP
- MobilePASS which is supported on the following OS platforms:
  - MobilePASS+ (Push OTP support)
    - Android 4.x, 5.x
    - iOS 7+

RADIUS Prerequisites

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

- End users can authenticate from the Blue Coat ProxySG environment with a static password before configuring Blue Coat ProxySG to use RADIUS authentication.
- Ports 1812/1813 are open to and from Blue Coat ProxySG.
- A shared secret key has been selected. A shared secret key provides an added layer of security by supplying an indirect reference to a shared secret key. It is used by a mutual agreement between the RADIUS server and RADIUS client for encryption, decryption, and digital signatures.
- On the client machine, set the RADIUS timeout value at least 60 seconds.

Configuring SafeNet Authentication Service

The deployment of multi-factor authentication using SAS with Blue Coat ProxySG using RADIUS protocol requires the following:

- Creating Users Stores in SAS, page 8
- Assigning an Authenticator in SAS, page 8
- Adding Blue Coat ProxySG as an Authentication Node in SAS, page 9
- Checking the SAS RADIUS Server’s IP Address, page 9
- Enabling the Software Token Push OTP Setting, page 9
- Enabling the Allowed Targets Policy, page 12
Creating Users Stores in SAS

Before SAS can authenticate any user in your organization, you need to create a user store in SAS that reflects the users that 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 additional 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 who are authenticating through Blue Coat ProxySG.

The following authenticators are supported:

- 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 Rules” 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 an Authentication Node in SAS

Add a RADIUS entry in the SAS **Auth Nodes** module to prepare it to receive RADIUS authentication requests from Blue Coat ProxySG. You will need the IP address of Blue Coat ProxySG and the shared secret to be used by both SAS and Blue Coat ProxySG.

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

2. Click the COMMS tab, and then select **Auth Nodes**.

3. In the **Auth Nodes** module, click the **Auth Nodes** link.

4. Under **Auth Nodes**, click **Add**.
5. In the **Add Auth Nodes** section, complete the following fields, and then click **Save**:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auth Node Name</td>
<td>Enter a host description.</td>
</tr>
<tr>
<td>Resource Name</td>
<td>Enter a resource name which will identify in a push notification which authentication node it relates to.</td>
</tr>
<tr>
<td>Low IP Address In Range</td>
<td>Enter the IP address of the host that will authenticate with SAS.</td>
</tr>
<tr>
<td>Configure FreeRADIUS</td>
<td>Select this option.</td>
</tr>
<tr>
<td>Synchronization</td>
<td></td>
</tr>
<tr>
<td>Shared Secret</td>
<td>Enter the shared secret key.</td>
</tr>
<tr>
<td>Confirm Shared Secret</td>
<td>Re-enter the shared secret key.</td>
</tr>
</tbody>
</table>

The authentication node is added to the system.
Checking the SAS RADIUS Server’s IP Address

Before adding SAS as a RADIUS server in Blue Coat ProxySG, check its IP address. The IP address will then be added to Blue Coat ProxySG as a RADIUS server at a later stage.

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

2. Click the COMMS tab, and then select Auth Nodes.

3. In the Auth Nodes module, click the Auth Nodes link. The SAS RADIUS server details are displayed.
Enabling the Software Token Push OTP Setting

To use Push OTP authentication, the setting must be enabled in the SAS token policy.

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

2. Click the POLICY tab, and then select Token Policies.
3. In the **Token Policies** module, click the **Software Token Push OTP Setting** link.

![Token Policies Module](image)

4. Select **Enable Push OTP communication with MobilePass+** , and then click **Apply**.

**Enabling the Allowed Targets Policy**

For Push OTP to be permitted during authentication the user must have a MobilePASS+ token enrolled and this policy must be enabled.

The settings to enable this policy will determine which OS targets are presented to users during the self-enrollment of MobilePASS tokens. You can restrict the targets on which MobilePASS+ or MobilePASS 8 tokens are allowed to be activated or enrolled.

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

![Manager_Yariv](image)
2. Click the **POLICY** tab, and then select **Token Policies**.

3. In the **Token Policies** module, click the **Allow Targets Settings** link.

4. On the **MobilePASS** tab, select the desired targets to allow for each MobilePASS application for this virtual server, and then click **Apply**.
Configuring Blue Coat ProxySG

Configuring Blue Coat ProxySG requires the following:

- Creating a RADIUS Authentication Realm, page 15
- Configuring RADIUS Realm Properties, page 16
- Configuring RADIUS Realm General Properties, page 18
- Configuring an Authentication Policy, page 19

Creating a RADIUS Authentication 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 > RADIUS.

3. In the right pane, on the RADIUS Realms tab, click New.

4. On the Add RADIUS Realm window, complete the following fields, and then click OK.

<table>
<thead>
<tr>
<th>Realm name</th>
<th>Enter a valid name for the new RADIUS realm (for example, SAS_RADIUS).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary server host</td>
<td>Enter the IP address of the SAS RADIUS server.</td>
</tr>
<tr>
<td>Port</td>
<td>Do not change this field.</td>
</tr>
<tr>
<td>Secret</td>
<td>Enter the shared RADIUS secret.</td>
</tr>
<tr>
<td>Confirm secret</td>
<td>Enter the shared RADIUS secret again.</td>
</tr>
</tbody>
</table>
5. Click **Apply**.

6. Click **OK**.

## Configuring RADIUS Realm Properties

After you have created the RADIUS realm, you can change the primary host, port, and secret of the RADIUS server for that realm.

1. On the **Blue Coat Management Console** window, click the **Configuration** tab, and then in the left pane, click **Authentication > RADIUS**.
In the right pane, on the RADIUS Servers tab, complete the following fields, and then click Apply.

<table>
<thead>
<tr>
<th><strong>Realm name</strong></th>
<th>Select the RADIUS realm that you created on page 15 (for example, SAS_RADIUS).</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Primary Server Host / Port</strong></td>
<td>Verify the Host and Port values, and edit them if necessary. The Host field contains the IP address of the SAS RADIUS server. Similarly, the Port field contains the port number of the RADIUS server.</td>
</tr>
<tr>
<td><strong>Alternate Server Host / Port</strong></td>
<td>Specify the IP address and port number of an alternate server, if necessary.</td>
</tr>
<tr>
<td><strong>RADIUS Specific Settings</strong></td>
<td>Value of Timeout request after field should be at least 60 seconds.</td>
</tr>
</tbody>
</table>

2. Click OK.
Configuring RADIUS Realm General Properties

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

![Configuring RADIUS Realm General Properties](image.png)

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

2. In the right pane, on the RADIUS General tab, complete the following fields, and then click Apply.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Realm name</td>
<td>Select the RADIUS realm that you created on page 15 (for example, SAS_RADIUS).</td>
</tr>
<tr>
<td>Display name</td>
<td>(Optional) Modify the RADIUS realm display name. The default display name is the realm name.</td>
</tr>
<tr>
<td>Virtual URL</td>
<td>Enter the virtual URL configured for reverse proxy setup.</td>
</tr>
</tbody>
</table>

![Configuring RADIUS Realm General Properties](image.png)

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

3. Click OK.

![Configuring RADIUS Realm General Properties](image.png)

(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.

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**.

(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>Name</th>
<th>Enter the name of the Authenticate Object (for example, <strong>Authenticate</strong>).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Realm</td>
<td>Select the RADIUS realm that you created on page 15 (for example, <strong>SAS_RADIUS</strong>).</td>
</tr>
<tr>
<td>Mode</td>
<td>Select <strong>Form Cookie Redirect</strong>.</td>
</tr>
<tr>
<td>Authentication Form</td>
<td>Select <strong>authentication_form</strong>.</td>
</tr>
<tr>
<td>New PIN Form</td>
<td>Select <strong>new_pin_form</strong>.</td>
</tr>
<tr>
<td>Query Form</td>
<td>Select <strong>query_form</strong>.</td>
</tr>
</tbody>
</table>

8. On the **Set Action Object** window, click **OK**.

(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**.

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

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

4. On the **Add New Layer** window, enter a descriptive name for the Web Access Layer, and then click **OK**.
5. Right-click on the **Source** column of the default rule, and then select **Set**.

![Set Source Object](image1.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](image2.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.

![Policy Manager screenshot](image1.png)  
*The screen image above is from Blue Coat® software. Trademarks are the property of their respective owners.*

8. Click **Install policy**.

![Policy Manager screenshot](image2.png)  
*The screen image above is from Blue Coat® software. Trademarks are the property of their respective owners.*
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, you are enrolled with a Push OTP token on SAS Cloud, and is using an Android device.

1. In a web browser, open the following URL to connect to the content server (web server):
   
   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 enter proxy credentials for the assigned realm. In the Username field, enter your user name, and then click Submit.

   **Enter Proxy Credentials for Realm sastest**

   Reason for challenge: Credentials are missing.

   Username: [ ]

   Password: [ ]

   Submit  Reset

3. SAS will trigger an on-the-go authentication request. You will then receive a push notification on the configured mobile device.

4. Tap on the notification to view the login request details.
5. Tap **Approve**.

6. Type the token PIN, and then tap **Continue** to send the approval with OTP to SAS.

A successful message is displayed on the mobile device.
After successful user authentication on SAS, user will be redirected to access the 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>Address</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>Phone</td>
<td>United States</td>
</tr>
<tr>
<td></td>
<td>1-800-545-6608</td>
</tr>
<tr>
<td></td>
<td>International</td>
</tr>
<tr>
<td></td>
<td>1-410-931-7520</td>
</tr>
<tr>
<td>Technical Support</td>
<td><a href="https://serviceportal.safenet-inc.com">https://serviceportal.safenet-inc.com</a></td>
</tr>
<tr>
<td>Customer Portal</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>