SafeNet Authentication Manager
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: 007-013260-001, Rev. A
Release Date: August 2015
## Contents

- Third-Party Software Acknowledgement ......................................................................................... 4
- Description ................................................................................................................................. 4
- Applicability ............................................................................................................................. 4
- Environment ................................................................................................................................. 5
- Audience ....................................................................................................................................... 5
- RADIUS-based Authentication using SAM ...................................................................................... 5
- RADIUS Authentication Flow using SAM ....................................................................................... 6
- RADIUS Prerequisites ................................................................................................................... 6
- Configuring SafeNet Authentication Manager ............................................................................... 7
  - Synchronizing Users Stores to SAM ......................................................................................... 7
  - Configuring SAM’s Connector for OTP Authentication ............................................................. 7
  - Assigning a Token in SAM ........................................................................................................ 8
  - Adding Blue Coat ProxySG as a RADIUS Client in IAS/NPS ..................................................... 8
  - Configuring SAM’s OTP Plug-In for Microsoft RADIUS Client ................................................ 10
- Configuring Blue Coat ProxySG ................................................................................................... 11
  - Creating a RADIUS Authentication Realm ........................................................................... 11
  - Configuring RADIUS Realm Properties ................................................................................. 13
  - Configuring RADIUS Realm General Properties .................................................................. 14
  - Configuring an Authentication Policy ....................................................................................... 15
- Running the Solution .................................................................................................................... 21
- Support Contacts .......................................................................................................................... 22
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 Manager (SAM) is a versatile authentication solution that allows you to match the authentication method and form factor to your functional, security, and compliance requirements. Use this innovative management service to handle all authentication requests and to manage the token lifecycle.

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 (OTP) tokens managed by SafeNet Authentication Manager.
- Configure Blue Coat ProxySG to work with SafeNet Authentication Manager 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 Manager, and that the SafeNet Authentication Manager OTP plug-in for Microsoft RADIUS Client was installed as part of the simplified installation mode of SAM. For more information on SafeNet Authentication Manager installation modes, refer to the SafeNet Authentication Manager 8.2 Administrator’s Guide.

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

Applicability

The information in this document applies to:

- **SafeNet Authentication Manager**—A server version of SAM 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 Manager 8.2 HF 316**—A server version of SAM that is used to deploy the solution on-premises in the organization
- **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 Manager.

**RADIUS-based Authentication using SAM**

SafeNet’s OTP architecture includes the SafeNet RADIUS server for back-end OTP authentication. This enables integration with any RADIUS-enabled gateway or application. The SafeNet RADIUS server accesses user information in the Active Directory infrastructure via SAM.

SAM’s OTP plug-in for Microsoft RADIUS Client works with Microsoft’s IAS or NPS, providing strong authenticated remote access through the IAS or NPS RADIUS server.

When configured, users who access their network remotely using IAS or NPS are prompted for a token-generated OTP passcode for network authentication.

![Image of RADIUS architecture]

For more information on how to install and configure the SafeNet OTP plug-in for Microsoft RADIUS Client, refer to *SafeNet Authentication Manager 8.2 Administrator’s Guide*. 
RADIUS Authentication Flow using SAM

SafeNet Authentication Manager 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 connect to the content server or web application (HTTPS) through Blue Coat ProxySG using an OTP token.
2. Blue Coat ProxySG sends a RADIUS request with the user’s credentials to SafeNet Authentication Manager for validation.
3. The SAM authentication reply is sent back to Blue Coat ProxySG.
   After successful user authentication based on the OTP value calculation results from SAM, ProxySG checks the internal cache for requested content.
4. If requested content is not available in the cache, ProxySG retrieves contents from the web server.
5. ProxySG immediately stores requested contents to the cache and delivers accelerated contents to the user.

RADIUS Prerequisites

To enable SafeNet Authentication Manager 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 the RADIUS client for encryption, decryption, and digital signatures.
- Blue Coat ProxySG virtual appliance should be configured as a Reverse Proxy with HTTPS services.
Configuring SafeNet Authentication Manager

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

- Synchronizing Users Stores to SAM, page 7
- Configuring SAM’s Connector for OTP Authentication, page 7
- Assigning a Token in SAM, page 8
- Adding Blue Coat ProxySG as a RADIUS Client in IAS/NPS, page 8
- Configuring SAM’s OTP Plug-In for Microsoft RADIUS Client, page 10

Synchronizing Users Stores to SAM

SAM manages and maintains OTP token information in its data store, including the token status, the OTP algorithm used to generate the OTP, and the token assignment to users. For user information, SAM can be integrated with an external user store. During the design process, it is important to identify which user store the organization is using, such as Microsoft Active Directory.

If the organization is not using an external user store, SAM uses an internal (“stand-alone”) user store created and maintained by the SAM server.

SAM 8.2 supports the following external user stores:

- Novell eDirectory
- Microsoft ADAM/AD LDS
- OpenLDAP
- Microsoft SQL Server 2005 and 2008
- IBM Lotus Domino
- IBM Tivoli Directory Server

Configuring SAM’s Connector for OTP Authentication

SafeNet Authentication Manager is based on open standards architecture with configurable connectors. This supports integration with a wide range of security applications, including network logon, VPN, web access, one-time password authentication, secure email, and data encryption.

If you selected the Simplified OTP-only configuration, SafeNet Authentication Manager is automatically configured with a typical OTP configuration, providing a working SafeNet Authentication Manager OTP solution.

The Simplified OTP-only configuration is as follows:

- Connectors—SAM Connector for OTP Authentication is installed
- SAM Back-end Service—Activated on this server; scheduled to operate every 24 hours
In addition, the SAM default policy is set as follows:

- OTP support (required for OTP) is selected in the **Token Initialization** settings.
- The **SAM Connector for OTP Authentication** is set, by default, to enable enrollment of OTP tokens without requiring changes in the Token Policy Object (TPO) settings. For more information on how to install and configure the SafeNet Authentication Manager for simplified installation, refer to the *SafeNet Authentication Manager 8.2 Administrator’s Guide*.

### Assigning a Token in SAM

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

The following tokens are supported:

- eToken PASS
- eToken NG-OTP
- SafeNet GOLD
- SMS tokens
- MobilePASS
- SafeNet eToken Virtual products
- MobilePASS Messaging
- SafeNet Mobile Authentication (iOS)
- SafeNet eToken 3400
- SafeNet eToken 3500

Tokens can be assigned to users as follows:

- **SAM Management Center**—Management site used by SAM administrators and helpdesk personnel for token enrollment and lifecycle management.
- **SAM Self-Service Center**—Self-service site used by end users for managing their tokens.
- **SAM Remote Service**—Self-service site used by employees not on the organization’s premises as a rescue website to manage cases where tokens are lost or passwords are forgotten.

For more information on SafeNet’s tokens and service portals, refer to the *SafeNet Authentication Manager 8.2 Administrator’s Guide*.

### Adding Blue Coat ProxySG as a RADIUS Client in IAS/NPS

For Windows Server 2003, the Windows RADIUS service is Internet Authentication Service (IAS). The IAS is added as the RADIUS server in Blue Coat ProxySG.

For Windows Server 2008 and above, the Windows RADIUS service is the Microsoft Network Policy Server (NPS). The NPS server is added as the RADIUS server in Blue Coat ProxySG.

Blue Coat ProxySG must be added as a RADIUS client on the IAS/NPS server so that IAS/NPS will authorize Blue Coat ProxySG for authentication.
NOTE: This document assumes that IAS/NPS policies are already configured and working with static passwords prior to implementing multi-factor authentication using SafeNet Authentication Manager. The details below refer to NPS, and are very similar to IAS.

2. From the NPS web console, expand RADIUS Clients and Servers, right-click RADIUS Clients, and then click New.

![Network Policy Server](image)

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

3. On the New RADIUS Client window, complete the following fields on the Settings tab:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable this RADIUS client</td>
<td>Select this option.</td>
</tr>
<tr>
<td>Friendly name</td>
<td>Enter a RADIUS client name (for example, Bluecoat).</td>
</tr>
<tr>
<td>Address (IP or DNS)</td>
<td>Enter the Blue Coat ProxySG IP address or DNS.</td>
</tr>
<tr>
<td>Shared secret</td>
<td>Enter the shared secret for the RADIUS client. This entry must match the shared secret that was used when the RADIUS server was configured in Blue Coat ProxySG.</td>
</tr>
<tr>
<td>Confirm shared secret</td>
<td>Re-enter the shared secret.</td>
</tr>
</tbody>
</table>
4. Click OK.

Blue Coat ProxySG is added as a RADIUS client in NPS.

Configuring SAM’s OTP Plug-In for Microsoft RADIUS Client

RADIUS protocol is used for authentication and authorization. The SafeNet OTP solution supports the Microsoft IAS service (used in Windows 2003) and Microsoft NPS service (used in Windows 2008 and later) as Windows services running a RADIUS server. These services may be extended by adding plug-ins for the authentication process.

SAM’s OTP plug-in for Microsoft RADIUS client works with Microsoft’s IAS or NPS to provide strong, authenticated remote access through the IAS or NPS RADIUS server. When configured, users who access their network remotely using IAS or NPS are prompted for a token-generated OTP passcode for network authentication.

For more information on how to install and configure the SafeNet Authentication Manager OTP plug-in, refer to the SafeNet Authentication Manager 8.2 Administrator’s Guide.
Configuring Blue Coat ProxySG

Configuring Blue Coat ProxySG requires the following:

- Creating a RADIUS Authentication Realm, page 11
- Configuring RADIUS Realm Properties, page 13
- Configuring RADIUS Realm General Properties, page 14
- Configuring an Authentication Policy, page 15

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 details, 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 RADIUS realm (for example, SAM_RADIUS).</td>
</tr>
<tr>
<td>Primary server host</td>
<td>Enter the IP address of the SAM 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**.
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.

![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 RADIUS Servers 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 in the previous section (for example, SAM_RADIUS).</td>
</tr>
<tr>
<td>Primary Server Host / Port</td>
<td>Verify the Host and Port values, and edit them if necessary. The Host field contains the IP address of the SAM RADIUS server. Similarly, the Port field contains the port number of the RADIUS server.</td>
</tr>
<tr>
<td>Alternate Server Host / Port</td>
<td>Specify the IP address and port number of an alternate server, if necessary.</td>
</tr>
<tr>
<td>RADIUS Specific Settings</td>
<td>Do not change these settings.</td>
</tr>
</tbody>
</table>

![RADIUS Servers Tab](image)

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

   ![Image of Blue Coat Management Console](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 11 (for example, SAM_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 (for example, https://&lt;Virtual IP of ProxySG&gt;:4433).</td>
</tr>
</tbody>
</table>

   ![Image of RADIUS General Settings](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 how to set 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 click **Set**.

![Blue Coat Visual Policy Manager](image1.png)

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

6. On the **Set Action Object** window, click **New**, and then select **Authenticate**.

![Set Action Object](image2.png)

*(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 11 (for example, <strong>SAM_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>

![Edit Authenticate Object](image)

*(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.

![Configuration Tab](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.

![Add Web Access Layer](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](image)

(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 click **Set**.

![Image of Blue Coat software showing policy settings]

(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**.

![Image of Blue Coat software showing source object selection]

(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 click **Allow**. The icon in the **Action** column changes from red to green.

8. Click **Install policy**.

(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, the user is enrolled with the MobilePASS token on SAM.

1. Open the following URL in a web browser: https://<Virtual IP of Bluecoat ProxySG>
   where Virtual IP of Bluecoat ProxySG is an IP address that is configured on the ProxySG appliance
2. You are redirected to enter the proxy credentials for the assigned realm.
   a. In the Username field, enter your user name.
   b. Generate an OTP, and enter it in the Password field.
   c. Click Submit.

**Enter Proxy Credentials for Realm SAM_RADIUS**

Reason for challenge: Credentials are missing.

Username: 
Password: 

Submit  Reset

After successful user authentication on SAM, you are 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><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</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>
</tbody>
</table>
|                                | 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.