SafeNet Authentication Service
Integration Guide

Using RADIUS Protocol for Barracuda SSL VPN
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: 007-012973-001, Rev. B
Release Date: November 2015
Third-Party Software Acknowledgement ................................................................. 4
Description ................................................................................................................ 4
Applicability ................................................................................................................ 4
Environment ............................................................................................................... 4
Audience ..................................................................................................................... 5
RADIUS-based Authentication using SAS Cloud .................................................... 5
RADIUS-based Authentication using SAS-SPE and SAS-PCE ................................ 6
RADIUS Authentication Flow using SAS ............................................................... 6
RADIUS Prerequisites ............................................................................................. 7
Configuring SafeNet Authentication Service ......................................................... 7
    Creating Users Stores in SAS .............................................................................. 7
    Assigning an Authenticator in SAS ................................................................... 8
    Adding Barracuda SSL VPN as an Authentication Node in SAS .................... 9
    Checking the SAS RADIUS Address ................................................................ 11
Configuring Barracuda SSL VPN ........................................................................... 12
    Creating a User .................................................................................................. 12
    Creating an Authentication Scheme .................................................................. 14
    Configuring RADIUS Settings ........................................................................ 15
    Configuring Applications .................................................................................. 17
Running the Solution .............................................................................................. 19
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 Barracuda SSL VPN.

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.

Barracuda SSL VPN only requires a browser to give remote users secure access to network resources from any computer. Built-in and third-party multi-factor authentication and network access control only connects clients that meet chosen security standards.

This document describes how to:

- Deploy multi-factor authentication (MFA) options in Barracuda SSL VPN using SafeNet one-time (OTP) authenticators managed by SafeNet Authentication Service.
- Configure Barracuda SSL VPN to work with SafeNet Authentication Service in RADIUS mode.

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

Barracuda SSL VPN can be configured to support multi-factor authentication in several modes. The RADIUS protocol 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 – Private Cloud Edition (SAS-PCE)**—only when using this version. For Cloud not necessary to fill in version number.
- **Barracuda SSL VPN V480 (Firmware version 2.5.0.4)**
Audience

This document is targeted to system administrators who are familiar with Barracuda SSL VPN, 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.

  ![SAS Cloud Diagram](image1)

- **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.

  ![Local RADIUS Diagram](image2)

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.gemalto.com/cryptocard/implementation-guides/Microsoft/Blackshield Agent Implementation Guide for Microsoft IAS, NPS.pdf

For more details on how to install and configure FreeRADIUS, refer to the SafeNet Authentication Service FreeRADIUS Agent Configuration Guide.
RADIUS-based Authentication using SAS-SPE and SAS-PCE

For both on-premises versions, SAS can be integrated with the following solutions that serve as local RADIUS servers:

- Microsoft Network Policy Server (MS-NPS) or the legacy Microsoft Internet Authentication Service (MS-IAS)—SafeNet Authentication Service is integrated with the local RADIUS servers using a special on-premises agent called SAS Agent for Microsoft IAS and NPS.
  
  For more information on how to install and configure the SAS Agent for Microsoft IAS and NPS, refer to the following document:
  
  http://www2.gemalto.com/cryptocard/implementation-guides/Microsoft/Blackshield Agent Implementation Guide for Microsoft IAS, NPS.pdf

- FreeRADIUS—The SAS FreeRADIUS Agent is a strong authentication agent that is able to communicate with SAS through the RADIUS protocol.

  For more information on how to install and configure the SAS FreeRADIUS Agent, refer to the SafeNet Support Portal.

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 data flow of a multi-factor authentication transaction for Barracuda SSL VPN.

1. A user attempts to log on to Barracuda SSL VPN using an OTP authenticator.
2. Barracuda SSL VPN sends a RADIUS request with the user’s credentials to SafeNet Authentication Service for validation.
3. The SAS authentication reply is sent back to the Barracuda SSL VPN.
4. The user is granted or denied access to the Barracuda SSL VPN based on the OTP value calculation results from SAS.
RADIUS Prerequisites

To enable SafeNet Authentication Service to receive RADIUS requests from Barracuda SSL VPN, ensure the following:

- End users can authenticate from the Barracuda SSL VPN environment with a static password before configuring the Barracuda SSL VPN to use RADIUS authentication.
- Ports 1812/1813 are open to and from Barracuda SSL VPN.
- 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.

Configuring SafeNet Authentication Service

The deployment of multi-factor authentication using SAS with Barracuda SSL VPN using RADIUS protocol requires the following:

- Creating Users Stores in SAS, page 7
- Assigning an Authenticator in SAS, page 8
- Adding Barracuda SSL VPN as an Authentication Node in SAS, page 8
- Checking the SAS RADIUS Address, page 11

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 Barracuda SSL VPN.

The following authenticators are supported:

- eToken PASS
- RB-1 Keypad Token
- KT-4 Token
- SafeNet Gold
- SMS Token
- MP-1 Software Token
- MobilePASS
- GrIDsure Authentication

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 Barracuda SSL VPN 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 Barracuda SSL VPN. You will need the IP address of Barracuda SSL VPN and the shared secret to be used by both SAS and Barracuda SSL VPN.

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>Agent Description</td>
<td>Enter a host description.</td>
</tr>
<tr>
<td>Host Name</td>
<td>Enter the name of the host that will authenticate with SAS.</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 Free RADIUS Synchronization</td>
<td>Select this option.</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 entered above to confirm it.</td>
</tr>
<tr>
<td>Agent Description</td>
<td>Enter a host description.</td>
</tr>
</tbody>
</table>
The authentication node is added to the system.

<table>
<thead>
<tr>
<th>Index</th>
<th>Description</th>
<th>Host Name</th>
<th>IP Address</th>
<th>RADIUS Synchronization</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Barracuda</td>
<td>192.168.1.1</td>
<td>192.168.1.1</td>
<td>True</td>
</tr>
</tbody>
</table>

Checking the SAS RADIUS Address

Before adding SAS as a RADIUS server in Barracuda SSL VPN, check its IP address. The IP address will then be added to Barracuda SSL VPN 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.
Configuring Barracuda SSL VPN

Configure Barracuda SSL VPN for RADIUS authentication with SafeNet Authentication Service. To achieve this, perform the following procedures:

- Creating a User, page 12
- Creating an Authentication Scheme, page 14
- Configuring RADIUS Settings, page 15
- Configuring Applications, page 17

Creating a User

1. Open the following URL in a web browser: https://<configured IP address for the Barracuda SSL VPN>
2. On the Login window, enter the default login credentials for the SSL VPN web interface, and then click Login. The default login credentials are:
   - Username: ssladmin
   - Password: ssladmin

(The screen image above is from Barracuda® software. Trademarks are the property of their respective owners.)
3. On the Barracuda SSL VPN web interface main window, perform the following steps:
   a. Click the **Access Control** tab.
   b. Under **Create Account**, enter the details in the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Database</td>
<td>Select a name of the database; for example, <strong>Default</strong>.</td>
</tr>
<tr>
<td>Username</td>
<td>Enter a username of your choice; for example, <strong>Alice</strong>.</td>
</tr>
<tr>
<td>Full Name</td>
<td>Enter the full name of the user.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Enter the password again to confirm.</td>
</tr>
</tbody>
</table>

   c. Click **Add**.

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

   A row containing user details is added under **Accounts**.

   (The screen image above is from Barracuda® software. Trademarks are the property of their respective owners.)
Creating an Authentication Scheme

1. On the Barracuda SSL VPN web interface main window, perform the following steps:
   a. Click Access Control > Authentication Schemes.
   b. Under Create Authentication Scheme, complete the following fields.

<table>
<thead>
<tr>
<th>User Database</th>
<th>Select a name of the database; for example, Default.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a username of your choice; for example, Global_rad.</td>
</tr>
</tbody>
</table>

c. In the Available modules list, select RADIUS, and then click Add. RADIUS is moved to the Selected modules list.

d. In the Available Policies list, select Everyone, and then click Add. Everyone is moved to the Selected Policies list.

e. Click Add.

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

The new authentication scheme is added under Authentication Schemes.

(The screen image above is from Barracuda® software. Trademarks are the property of their respective owners.)
2. Increase the priority of the authentication scheme you created so that it is given first priority over other authentication schemes. Perform the following steps:

f. Under **Authentication Schemes**, in the **Actions** column, click **More** for the authentication scheme you created (for example, **Global_rad**).

g. Keep clicking **Increase Priority** until your authentication scheme is shifted to the top of the list.

Configuring RADIUS Settings

On the Barracuda SSL VPN web interface main window, perform the following steps:

3. Click **Access Control > Configuration**.

4. Under **RADIUS**, complete the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>RADIUS Server</strong></td>
<td>Enter the IP address of the RADIUS server.</td>
</tr>
<tr>
<td><strong>Shared Secret</strong></td>
<td>Enter the shared secret text as specified in SAS.</td>
</tr>
<tr>
<td><strong>Authentication Method</strong></td>
<td>Select <strong>PAP</strong>.</td>
</tr>
<tr>
<td><strong>Challenge Image URL</strong></td>
<td>If you are using GrIDsure authentication, enter the following URL: <a href="https://grid.safenet-inc.com/blackshieldss/O/O1LL7DKH5L/index.aspx?getChallengeImage=true&amp;userName=$%7Bradius:userName%7D">https://grid.safenet-inc.com/blackshieldss/O/O1LL7DKH5L/index.aspx?getChallengeImage=true&amp;userName=${radius:userName}</a> If you are using any token other than GrIDsure, leave this field blank.</td>
</tr>
</tbody>
</table>
5. Click **Save Changes.**

![RADIUS Configuration Screen](image)

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

The Barracuda SSL VPN allows you to configure a resource you want to access once a VPN connection is established. The resources you can configure include:

- Microsoft RDP Client
- RDP - RDesktop
- Remote Desktop Client v2 for Mac OS X

In this guide, integration is demonstrated using the Microsoft RDP Client. When using the Microsoft RDP Client, Microsoft Windows Server 2008 R2 provides a feature that allows organizations to deploy server-hosted desktop applications without requiring the user to load an entire remote desktop. Only the application window is remotely displayed, integrating seamlessly into the user’s current desktop.

To configure applications:

On the Barracuda SSL VPN web interface main window, perform the following steps:

1. Click Resources > Applications.
2. Under RADIUS, complete the following fields.

<table>
<thead>
<tr>
<th>User Database</th>
<th>Select a name of the database; for example, Default.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a username of your choice; for example, My RDP Application.</td>
</tr>
<tr>
<td>Application</td>
<td>Select only the Remote Access option, and ensure that other options (Published Clients, Remote Control, and System Tools) are clear. Then, in the list of applications, select RDP-Microsoft RDP Client.</td>
</tr>
<tr>
<td>Hostname</td>
<td>Enter the IP address of the machine you want to connect after the VPN connection is established.</td>
</tr>
<tr>
<td>Port</td>
<td>Keep the default port number as 3389.</td>
</tr>
</tbody>
</table>

3. In the Available Policies list, select Everyone, and then click Add. Everyone is moved to the Selected Policies list.
4. Click Add.

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

The application (for example, My RDP Application) is added under Applications.

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

A user can be assigned several types of SAS-supported tokens. For this integration, a SafeNet eToken is configured for authentication with the SAS solution.

In this solution, remote access is demonstrated using the Microsoft RDP client. For remote access, the Barracuda SSL VPN Agent application is installed on the client machine, which establishes a secure tunnel to the Barracuda SSL VPN and then launches the application specified by the application resource.

1. Open the following URL in a web browser: https://<configured IP address for the Barracuda SSL VPN>

2. On the Login window, in the Username field, enter your user name, and then click Login.

3. In the RADIUS Password field, enter your password, and then click Login.

4. When the authentication is successful, the application resources are displayed. Click the application you have configured as a resource; for example, My RDP Application.
5. If a security warning is displayed, click **Continue**.

![Security Warning](image1.png)

6. If a confirmation message is displayed to install the Barracuda SSL VPN Agent, click **Run**.

![Do you want to run this application?](image2.png)

7. The Barracuda SSL VPN Agent is installed and then the Remote Desktop connection is established. Enter your Windows password.

![Remote Desktop](image3.png)

*(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)*
When the login credentials are verified, you are able to access the remote machine.

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
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></td>
</tr>
<tr>
<td>United States</td>
<td>1-800-545-6608</td>
</tr>
<tr>
<td>International</td>
<td>1-410-931-7520</td>
</tr>
<tr>
<td><strong>Technical Support</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Customer Portal</strong></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 manage incidents, get the latest software upgrades, and access the Gemalto Knowledge Base.</td>
</tr>
</tbody>
</table>