SafeNet Authentication Service
Integration Guide
Using RADIUS Protocol for Radiator RADIUS Server
Document Information

<table>
<thead>
<tr>
<th>Document Part Number</th>
<th>007-012995-001, Rev. A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release Date</td>
<td>April 2015</td>
</tr>
</tbody>
</table>

Trademarks

All intellectual property is protected by copyright. All trademarks and product names used or referred to are the copyright of their respective owners. No part of this document may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, chemical, photocopy, recording, or otherwise, without the prior written permission of SafeNet, Inc.

Disclaimer

SafeNet makes no representations or warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, SafeNet reserves the right to revise this publication and to make changes from time to time in the content hereof without the obligation upon SafeNet to notify any person or organization of any such revisions or changes.

We have attempted to make these documents complete, accurate, and useful, but we cannot guarantee them to be perfect. When we discover errors or omissions, or they are brought to our attention, we endeavor to correct them in succeeding releases of the product.

SafeNet invites constructive comments on the contents of this document. These comments, together with your personal and/or company details, should be sent to the address or email below.

<table>
<thead>
<tr>
<th>Contact Method</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mail</td>
<td>SafeNet, Inc.</td>
</tr>
<tr>
<td></td>
<td>4690 Millennium Drive</td>
</tr>
<tr>
<td></td>
<td>Belcamp, Maryland 21017, USA</td>
</tr>
<tr>
<td>Email</td>
<td><a href="mailto:TechPubs@safenet-inc.com">TechPubs@safenet-inc.com</a></td>
</tr>
</tbody>
</table>
Third-Party Software Acknowledgement

Description

Applicability

Environment

Audience

RADIUS-based Authentication using SAS Cloud

RADIUS-based Authentication using SAS-SPE and SAS-PCE

RADIUS Authentication Flow using SAS

Prerequisites

Configuring SafeNet Authentication Service
  Synchronizing Users Stores to SAS
  Authenticator Assignment in SAS
  Adding Radiator RADIUS Server as an Authentication Node in SAS
  Checking the SAS RADIUS Address

Configuring Cisco ASA
  Creating a AAA Server Group
  Editing a Group Policy
  Configuring a Connection Profile for Network (Client) Access

Configuring the Radiator RADIUS Server
  Adding a Client to the Radiator RADIUS Server
  Adding a Realm in Radiator

Running the Solution

Support Contacts
Third-Party Software Acknowledgement

This document is intended to help users of SafeNet products when working with third-party software, such as Radiator RADIUS Server.

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.

Radiator is a highly configurable and extensible RADIUS server. It allows you to easily customize and control how you authenticate users and record accounting information. Radiator can authenticate users from passwords held in:

- Remote RADIUS servers (as a proxy)
- SQL databases, including Oracle, Sybase, Informix, Microsoft SQL Server, PostgreSQL, MySQL, SQLite, ODBC, and others
- LDAP
- Microsoft Active Directory

In this integration, we will use Cisco Adaptive Security Appliance (ASA) as a VPN server, which will act as a RADIUS client for Radiator RADIUS Server. In brief, Cisco ASA is a security device that combines firewall, antivirus, intrusion prevention, and virtual private network (VPN) capabilities. It provides a proactive threat defense that stops attacks before they spread through the network. ASA is valuable and flexible in that it can be used as a security solution for both small and large networks.

This document describes how to:

- Configure Radiator RADIUS Server to work with SafeNet Authentication Service in RADIUS mode.

It is assumed that the Radiator RADIUS Server and Cisco ASA environment is already configured and working with static passwords prior to implementing multi-factor authentication using SafeNet Authentication Service.

Radiator RADIUS Server 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 – Service Provider Edition (SAS-SPE)**
- **Radiator RADIUS Server 4.14**
- **Cisco Adaptive Security Appliance (ASA) 9.2(2)4**
- **Cisco Adaptive Security Device Manager (ASDM) 7.3(1)101**
- **Cisco AnyConnect Secure Mobility Client 3.1.04072**

Audience

This document is targeted to system administrators who are familiar with Radiator RADIUS Server and are interested in adding multi-step and 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.

For more information on how to install and configure SAS Agent for IAS/NPS, refer to: 

For more details on how to install and configure FreeRADIUS, refer to the *SAS FreeRADIUS Agent Configuration Guide.*

This document demonstrates the solution using the SAS cloud hosted RADIUS service.

**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:
  

- **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 dataflow of a multi-factor authentication transaction for Radiator RADIUS Server.

1. A user attempts to log on to Cisco ASA using an OTP authenticator.
2. Cisco ASA sends a RADIUS request with the user’s credentials to Radiator RADIUS Server.
3. Radiator RADIUS Server sends a RADIUS request with the user’s credentials to SafeNet Authentication Service for validation.
4. The SAS authentication reply is sent back to Radiator RADIUS Server.
5. Radiator RADIUS Server, in turn, sends reply back to Cisco ASA.
6. The user is granted or denied access to Cisco ASA based on the OTP value calculation results from SAS.

Prerequisites

To enable SafeNet Authentication Service to receive RADIUS requests from Radiator RADIUS Server, ensure the following:

- End users can authenticate from the Radiator RADIUS Server environment with a static password before configuring the Radiator RADIUS Server to use RADIUS authentication.
- Ports 1812/1813 are open to and from Radiator RADIUS Server.
- 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 signature purposes.
- The Cisco AnyConnect Secure Mobility Client should be installed on the client machine.
- A user with the complete realm name should be present in SAS.
- The SafeNet eToken PASS should be enrolled with the user.
Configuring SafeNet Authentication Service

The deployment of multi-factor authentication using SAS with Radiator RADIUS Server using RADIUS protocol requires:

- Synchronizing Users Stores to SAS, page 8
- Authenticator Assignment in SAS, page 8
- Adding Radiator RADIUS Server as an Authentication Node in SAS, page 9
- Checking the SAS RADIUS Address, page 11

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 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 further details on importing users to SafeNet Authentication Service, refer to the SafeNet Authentication ServiceSubscriber Account Operator Guide (Chapter 2 >Assignment tab>Creating users):


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

Authenticator Assignment in SAS

SAS supports a number of authentication methods that can be used as second authentication factor for users who are authenticating through Radiator RADIUS Server.

The following authenticators are supported:

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

- **Manually provision** – Assign an authenticator to users 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 the *SafeNet Authentication Service - Subscriber Account Operator Guide* to learn how to provision the different authentication methods to the users in the SafeNet Authentication Service user store.

(Chapter 2 > Assignment Tab > Token Module > Provision - Manually provision; Chapter 2 > Policy Tab > Automation Policies Module > Provisioning Rules - Provisioning rules).


**Adding Radiator RADIUS Server as an Authentication Node in SAS**

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

**To add an Authentication Node in SAS:**

1. Log in to the SAS console with an Operator account.
2. Click the **COMMS** tab, and then select the **Auth Nodes** module.

![Image](image1.png)

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

![Image](image2.png)

4. Click **Add**.

![Image](image3.png)

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><strong>Agent Description</strong></td>
<td>Enter a host description.</td>
</tr>
<tr>
<td><strong>Host Name</strong></td>
<td>Enter the name of the host that will authenticate with SAS.</td>
</tr>
<tr>
<td><strong>Low IP Address In Range</strong></td>
<td>Enter the IP address of the host that will authenticate with SAS.</td>
</tr>
<tr>
<td><strong>Configure FreeRADIUS</strong></td>
<td>Select this option.</td>
</tr>
<tr>
<td><strong>Synchronization</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Shared Secret</strong></td>
<td>Enter the shared secret key.</td>
</tr>
<tr>
<td><strong>Confirm Shared Secret</strong></td>
<td>Re-enter the shared secret key to confirm it.</td>
</tr>
</tbody>
</table>
The Auth Node is added to the system.

Checking the SAS RADIUS Address

Before adding SAS as a RADIUS server in Radiator RADIUS Server, check the IP address of the SAS RADIUS server. The IP address will then be added to Radiator RADIUS Server as a RADIUS server at a later stage.

To check the IP address of the SAS RADIUS server:

1. Log in to the SAS console with an Operator account.
2. Click the **COMMS** tab, and then select the **Auth Nodes** module.

![COMMS tab](image1)

3. Click the **Auth Nodes** link.

![Auth Nodes](image2)

The SAS RADIUS server details are displayed.
Configuring Cisco ASA

Configuring Cisco ASA for two-step and multi-factor authentication requires the following:

- Creating a AAA Server Group, page, page 13
- Editing a Group Policy, page 18
- Configuring a Connection Profile for Network (Client) Access, page 20

Creating a AAA Server Group

If you want to use an external AAA server, you must first create at least one AAA server group per AAA protocol, and add one or more servers to each group. AAA server groups are identified by name. Each server group is associated with only one type of server, such as Kerberos, LDAP, NT, RADIUS, SDI, or TACACS+

To configure a RADIUS-enabled AAA server group:

1. To open the Cisco Adaptive Security Device Manager (ASDM) for Cisco ASA, click Start > All Programs > Cisco ASDM-IDM Launcher > Cisco ASDM Launcher.

2. On the Cisco ASDM-IDM Launcher window, enter the Cisco ASA IP Address, Username, and Password, and then click OK.

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)
3. On the main window, perform the following steps:
   a. Click **Configuration**.
   b. In the left pane, click the **Remote Access VPN** tab, and then click **AAA/Local Users > AAA Server Groups**.
   c. In the right pane, under the **AAA Server Groups** section, click **Add**.

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)
4. On the **Add AAA Server Group** window, complete the following fields, and then click **OK**. The newly created AAA server group will be added to the list under the **AAA Server Group** section.

<table>
<thead>
<tr>
<th>AAA Server Group</th>
<th>Enter a name for the AAA Server Group; for example, <strong>Radiator</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>Select <strong>RADIUS</strong>.</td>
</tr>
</tbody>
</table>

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)
5. On the main window, perform the following steps:
   a. In the right pane, under the **AAA Server Groups** section, select the newly created server group (for example, **Radiator**).
   b. Under the **Servers in the Selected Group** section, click **Add**.

   ![Screen image](image.png)

   *(The screen image above is from Cisco. Trademarks are the property of their respective owners.)*
6. On the **Add AAA Server** window, complete the following fields, and then click **OK**. This newly created AAA server will be added to the list under the **Servers in the Selected Group** section.

<table>
<thead>
<tr>
<th><strong>Interface Name</strong></th>
<th>Select an interface that would be used to reach the Radiator RADIUS Server; for example, <strong>outside</strong>. The administrator would have created this interface where the Cisco AnyConnect client will send the authentication request to Cisco ASA. Also, through this interface, Cisco ASA will communicate to the Radiator RADIUS Server.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Server Name or IP Address</strong></td>
<td>Enter the server name or IP address of the Radiator RADIUS Server.</td>
</tr>
<tr>
<td><strong>Server Authentication Port</strong></td>
<td>Enter the RADIUS server authentication port; for example, <strong>1812</strong>.</td>
</tr>
<tr>
<td><strong>Server Secret Key</strong></td>
<td>Enter the secret key shared between Cisco ASA and the Radiator RADIUS Server.</td>
</tr>
</tbody>
</table>

(For the screen image above is from Cisco. Trademarks are the property of their respective owners.)

7. On the main window, click **Apply**.
Editing a Group Policy

Edit a group policy that is present by default in Cisco ASA.

1. Open the **Cisco Adaptive Security Device Manager (ASDM)** for Cisco ASA.
2. On the main window, click **Configuration**. In the left pane, click the **Remote Access VPN** tab, and then click **Network (Client) Access > Group Policies**.

3. In the right pane, select **DfltGrpPolicy (System Default)**. Ensure that **ssl-client** is specified in the **Tunneling Protocol** column. If **ssl-client** is not specified, click **Edit** and perform the following steps:
   a. On the **Edit Internal Group Policy** window, click **More Options**.
b. In the **Tunneling Protocols** field, select the **SSL VPN Client** option, and then click **OK**.

![Screen image of Tunneling Protocols settings](image)

*The screen image above is from Cisco. Trademarks are the property of their respective owners.*

c. On the main window, click **Apply**.
**Configuring a Connection Profile for Network (Client) Access**

A connection profile consists of a set of records that determine tunnel connection policies. These records identify the servers to which the tunnel user is authenticated, as well as the accounting servers, if any, to which connection information is sent. They also identify a default group policy for the connection, and they contain protocol-specific connection parameters. Connection profiles include a small number of attributes that pertain to creating the tunnel itself. Connection profiles include a pointer to a group policy that defines user-oriented attributes.

**To configure a connection profile:**

1. Open the **Cisco Adaptive Security Device Manager (ASDM)** for Cisco ASA.
2. On the main window, click **Configuration**. In the left pane, click **Network (Client) Access > AnyConnect Connection Profiles**.

![Screen Image from Cisco](Image)

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

3. In the right pane, under **Access Interface**, perform the following steps:
   a. Select **Enable Cisco AnyConnect VPN Client access** on the interfaces selected in the table below.
   b. In the table, for **outside** and **inside** interfaces, under **SSL Access**, select the check boxes in the **Allow Access** and **Enable DTLS** columns.

![Access Interfaces Table](Image)

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)
4. Under Connection Profiles, click Add.

![Connection Profiles](image)

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

5. On the Add AnyConnect Connection Profile window, in the left pane, click Basic. In the right pane, 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 connection profile; for example, <strong>RadiatorProfile</strong>.</td>
</tr>
<tr>
<td>Aliases</td>
<td>Enter the alias for the connection profile; for example, <strong>RadiatorAlias</strong>.</td>
</tr>
<tr>
<td>AAA Server Group</td>
<td>Select an appropriate AAA server group; for example, <strong>Radiator</strong>.</td>
</tr>
<tr>
<td>Client Address Pools</td>
<td>Click Select and assign an address pool.</td>
</tr>
<tr>
<td>Group Policy</td>
<td>Select the group policy configured previously; for example, <strong>DfltGrpPolicy</strong>.</td>
</tr>
<tr>
<td>Enable SSL VPN client protocol</td>
<td>Select this option.</td>
</tr>
</tbody>
</table>

![Add AnyConnect Connection Profile](image)

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)
6. On the main window, under **Login Page Setting**, select **Allow user to select connection profile on login page**.

![Login Page Setting](image)

*(The screen image above is from Cisco. Trademarks are the property of their respective owners.)*

7. Click **Apply**.

### Configuring the Radiator RADIUS Server

Configuring the Radiator RADIUS multi-factor authentication, require:

- Adding a Client to the Radiator RADIUS Server, page 22
- Adding a Realm in Radiator, page 24

### Adding a Client to the Radiator RADIUS Server

A **Client** clause in the Radiator configuration file specifies a RADIUS client that this server will listen to. Requests received from any client not named in a **Client** clause will be silently ignored.

1. In a web browser, open the following URL: **http://<IP address of Radiator Server>:9048**
2. On the login window, enter the valid username and password, and then click **Login**.

![Radiator RADIUS Server](image)

*(The screen image above is from Open System Consultants. Trademarks are the property of their respective owners.)*

3. In the left pane, under **Configuration**, click **Edit**.

![Radiator Configuration](image)

*(The screen image above is from Open System Consultants. Trademarks are the property of their respective owners.)*
4. In the right pane, for the **Client** field, click the **New** link.

   ![ServerConfig](image1.png)

   *(The screen image above is from Open System Consultants. Trademarks are the property of their respective owners.)*

5. Enter the DNS name or IP address of the client (Cisco ASA), and then click **Next**.

   ![Radiator RADIUS Server](image2.png)

   *(The screen image above is from Open System Consultants. Trademarks are the property of their respective owners.)*

6. In the **Secret** field, enter the secret text shared between the Radiator RADIUS Server and the RADIUS client (Cisco ASA), and then click **Apply**. The newly created RADIUS client is added to the Radiator.

   ![Client Configuration](image3.png)

   *(The screen image above is from Open System Consultants. Trademarks are the property of their respective owners.)*
Adding a Realm in Radiator

For the simplest RADIUS server configuration, you should define at least one client and realm. Inside the realm, you should define at least one AuthBy clause to perform the authentication.

Radiator can manage multiple clients and realms, possibly with multiple different authentication methods in each realm.

1. On the Radiator main window, in the left pane, under Configuration, click Edit.

   ![Radiator Configuration](image)

   *(The screen image above is from Open System Consultants. Trademarks are the property of their respective owners.)*

2. In the right pane, for the Realm field, click the New link.

   ![ServerConfig](image)

   *(The screen image above is from Open System Consultants. Trademarks are the property of their respective owners.)*
3. Enter a unique name for the realm (for example, safenet.com), and then click Next.

4. In the AuthByPolicy field, select ContinueUntilIgnore, and then click Apply.

5. For the AuthBy field, click the New link.

6. Select AuthBy RADIUS, and then click Next.
7. Complete the following fields, and then click **Apply**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AcctPort</td>
<td>[Optional] Enter <strong>1813</strong>. This is the default UDP port on the destination host to which Radiator will send accounting requests.</td>
</tr>
<tr>
<td>AuthPort</td>
<td>Enter <strong>1812</strong>. This is the default UDP port on the destination host to which Radiator will send authentication requests.</td>
</tr>
<tr>
<td>Secret</td>
<td>Enter the default secret text for target RADIUS hosts.</td>
</tr>
</tbody>
</table>

(The screen image above is from Open System Consultants. Trademarks are the property of their respective owners.)

8. For the **Hosts** field, click the **New** link.

9. Enter the DNS name or IP address of the remote RADIUS server (SAS FreeRADIUS server IP address), and then click **Next**.

(The screen image above is from Open System Consultants. Trademarks are the property of their respective owners.)

10. Complete the following fields, and then click **Apply**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AcctPort</td>
<td>[Optional] Enter <strong>1813</strong>. This is the default UDP port on the destination host to which Radiator will send accounting requests.</td>
</tr>
<tr>
<td>AuthPort</td>
<td>Enter <strong>1812</strong>. This is the default UDP port on the destination host to which Radiator will send authentication requests.</td>
</tr>
<tr>
<td>Secret</td>
<td>Enter the default secret text for target RADIUS hosts.</td>
</tr>
</tbody>
</table>

(The screen image above is from Open System Consultants. Trademarks are the property of their respective owners.)
11. On the main window, in left pane, under Configuration, click Save.

12. In the right pane, click Save.

Running the Solution

To securely connect to Cisco ASA, the Cisco AnyConnect Secure Mobility Client can be used. The Cisco AnyConnect Secure Mobility Client provides remote users with secure VPN connections to Cisco ASA using the Secure Socket Layer (SSL) protocol and the Datagram TLS (DTLS) protocol. AnyConnect provides remote end users with the benefits of a Cisco SSL VPN client, and supports applications and functions that are unavailable to a clientless, browser-based SSL VPN connection.

In this solution, the SafeNet eToken PASS is used as the enrolled OTP token.

1. Start the Cisco AnyConnect Secure Mobility Client application from Start > All Programs > Cisco > Cisco AnyConnect Secure Mobility Client.
2. In the VPN field, enter the fully qualified domain name or IP address for Cisco ASA, and then click Connect.

(The screen image above is from Open System Consultants. Trademarks are the property of their respective owners.)

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)
3. Complete the following fields, and then click **OK**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Group</strong></td>
<td>Select an appropriate group alias; for example, <strong>safenet</strong>.</td>
</tr>
<tr>
<td><strong>Username</strong></td>
<td>Enter your domain user name.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>Enter the password associated with your domain user name.</td>
</tr>
</tbody>
</table>

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

If authentication is successful, the VPN session will be established and you will see the following message on your system.

(The screen image above is from Cisco. 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 SafeNet Customer Support. SafeNet 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 SafeNet 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>SafeNet, 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>
<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 SafeNet Knowledge Base.</td>
</tr>
</tbody>
</table>