SafeNet Authentication Service

Token Guide

SafeNet OTP Hardware Tokens

Document Information

Document Part Number	007-012477-001, Rev. E
Release Date	February 2015

Trademarks

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.

Contact Method	Contact Information
Mail	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017, USA
Email	TechPubs@safenet-inc.com

Contents

Applicability

The information in this document applies to:

- **SafeNet Authentication Service (SAS)—**The cloud authentication service of SafeNet, Inc.
- **SafeNet Authentication Service – Service Provider Edition (SAS-SPE)—**The software used to build a SafeNet Authentication Service.
- **SafeNet Authentication Service – Private Cloud Edition (SAS-PCE)—**The implementation of SAS-SPE on the customer premises.

OTP Hardware Tokens

In this guide, the terms “token” and “authenticator” are used interchangeably.

The information in this guide applies to the following OTP tokens:

- **eToken PASS**: a One-Time-Password (OTP) authenticator that offers two-factor strong authentication. eToken PASS is available in both time- and event-based versions.
- **GOLD**: an event-based One-Time-Password (OTP) strong authentication device that supports challenge response functionality. It offers an additional layer of security by generating the OTP only after users enter a PIN on the token keypad.
- **SafeNet eToken 3300 (formerly known as Platinum)**: a device having the same features as the GOLD. Its durable case and housing enables it to have the longest warranty available in the industry.
- **SafeNet eToken 3400**: an event-based One-Time-Password (OTP) strong authentication card.
- **SafeNet eToken 3410**: a time-based One-Time-Password (OTP) strong authentication card.

Welcome

Your organization has chosen SafeNet Authentication Service to protect your online identity, networks, applications, and data from unauthorized access.

This guide includes instructions for activating your OTP hardware token. Once it is activated, you will use passcodes generated from this token every time you log in.

What are SafeNet OTP Hardware Tokens?

The following tokens are included in the SafeNet OTP hardware token product line.

eToken PASS

SafeNet eToken 3400 / 3410

GOLD

SafeNet eToken 3300 (Platinum)

The instructions in this guide apply to all tokens in this list. eToken PASS is shown as an example in many of the graphics.

NOTE: The “button” referred to throughout this guide is the OTP-generating button, a common feature of all OTP hardware tokens.

Why Use a SafeNet OTP Token?

Until now, you have probably logged in to your organization’s resources with your user name and a fixed password. The problem is that passwords are easily compromised, putting your identity and the resources you access at risk.

A SafeNet OTP token allows you to generate and use unique one-time passwords (OTPs) each time you log in to your organization’s resources. As the name implies, an OTP can be used only one time. Each time you log in, you use your SafeNet OTP token to generate a unique OTP.

NOTE: Before you can log in using your token, you must activate it through self-enrollmet. The self-enrollment process is described in the section "What is Self-Enrollment?" on page 7 in this guide. Do not use your token until you have completed token self-enrollment.

How Does a SafeNet OTP Token Protect Me?

Password theft is a common method that thieves and hackers use to steal identities and gain unauthorized access to networks and resources. Success depends on the stolen password being valid, in the same way that credit card theft relies on the card being usable until it is reported as stolen. Discovering the compromise is almost impossible until damage has been done.

Using a SafeNet OTP token solves this problem, because once you have logged in using an OTP, that password is no longer valid. Any attempt to log in by reusing the OTP will fail, and it will alert your network security professionals to a possible attack on your identity.

What Additional Security Features Does My Token Offer?

Depending on your organization's policies, your SafeNet OTP token may be protected against unauthorized use by a server-side Security PIN that is known only to you. Like a bank card, a thief not only needs access to your token, but must know your PIN as well. Do not share your PIN with others.

When you log in using a generated token code, you may be required to enter a server-side Security PIN (also known as an OTP PIN) together with the token code. Your organization's policies determine the order in which you must enter the token code and your Security PIN.

You may receive a Security PIN from your administrator. During self-enrollment, you may be required to create a new Security PIN.

What is the Difference Between a Token Code and an OTP?

Your SafeNet OTP token generates a new token code each time you press the button on the token. The combination of your Security PIN (if required) and the generated token code form the OTP. For example:

		OTP for Login, PIN Required	
Security PIN	Token Code	Prepended PIN	Appended PIN
6666	12345678	666612345678	123456786666
6666	4Kz6-71R	66664Kz6-71R	4Kz6-71R6666

Successive attempts to log in with an incorrect OTP will automatically "lock" your token's account, preventing access, and allowing your network security professionals to deal with the threat.

What is Self-Enrollment?

Self-enrollment is a simple process during which you activate your token. During the process, you may be required to enter or create a Security PIN. When you complete the self-enrollment process, you will be able to use your token to generate OTPs for login.

What If I Have Not Received a Self-Enrollment Email?

If you have not received a self-enrollment email, contact your help desk to arrange for a new email to be sent to you.

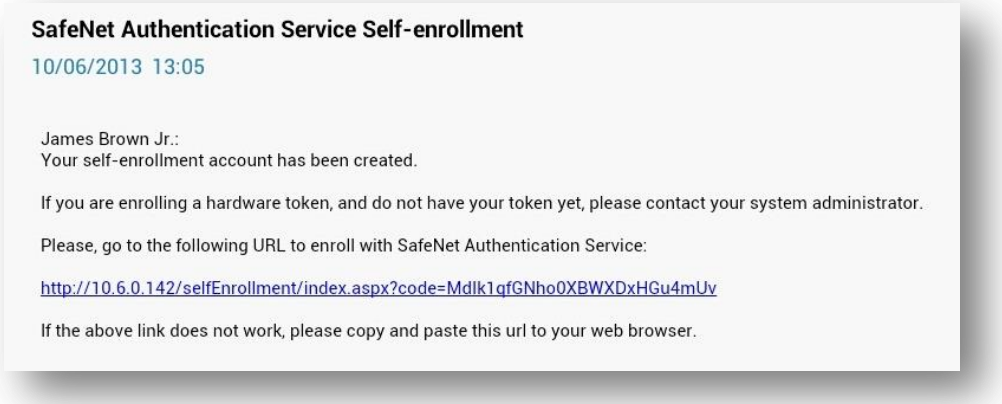
How Do I Self-Enroll My Token?

NOTE: The instructions in this guide apply to all SafeNet OTP hardware tokens described in this guide. An eToken PASS token is shown in the graphics as an example.

The self-enrollment process begins when you receive your self-enrollment email notification. The email contains instructions and your enrollment URL.

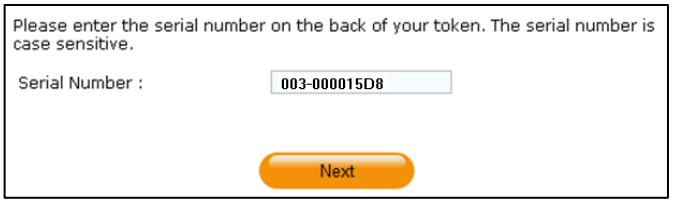
To self-enroll your token:

1. Open the self-enrollment email and read the instructions.



2. Open a web browser, and navigate to the self-enrollment site URL included in the email.

   At the self-enrollment site, you are prompted to enter your token serial number. This is the number found on the back of your token.

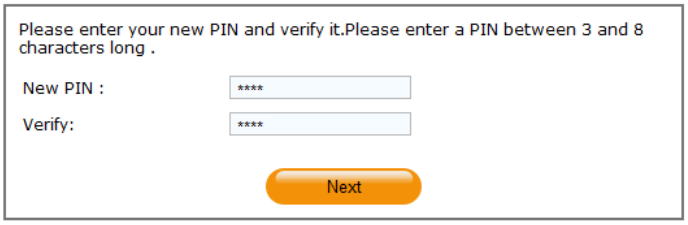


> **NOTE:** The serial number should be entered as displayed on the back of the token label, respecting case sensitivity and special characters.

3. Copy the serial number, and ensure it is accurate. Click **Next** to continue.

   You are prompted to enter an OTP. Depending on your organization's policies, you may be required to enter a Security PIN together with the code generated on your token. Your organization's policies determine the order in which you must enter the token code and the PIN.

4. Firmly push and then quickly release the button on the face of your token. A unique token code is generated and displayed.
5. Type the token code into the OTP field, together with the PIN, if required.
   Do not leave any spaces. Click **Next** to continue.
6. Depending on your organization's policies, you may be prompted to enter and verify a new Security PIN.

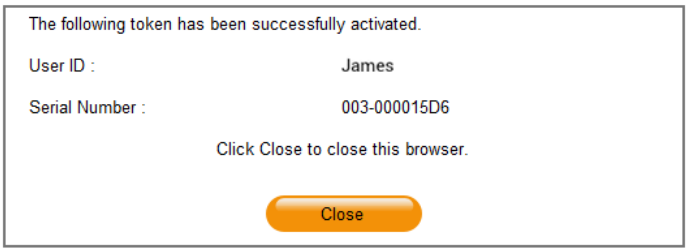


   Enter a Security PIN that only you will know. You will need to enter this PIN every time you log in. Your Security PIN must meet the length and composition requirements set by your organization's policies.

   If the PIN fields do not match or if the PIN does not meet security requirements a red asterisk (*) is displayed next to the input fields.

7. Click **Next** to continue.

   The final window confirms that you have completed enrollment.



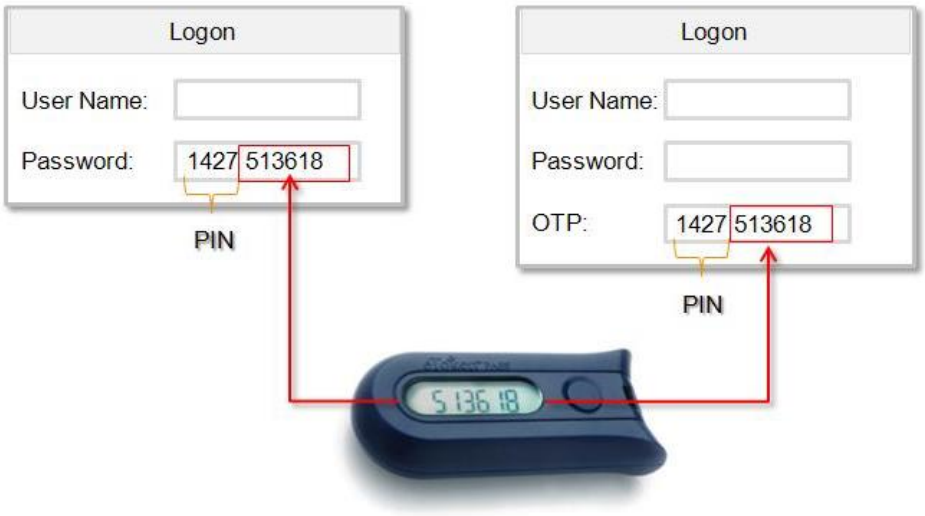
8. Click **Close**.

   You can now use your token to log in to your organization's protected networks and resources.

How Do I Use My SafeNet OTP Token to Log In?

When you need to log in, firmly push and then quickly release the button on the face of your token. A unique token code is generated, and it is displayed 30-90 seconds, depending on your organization's policies. Copy it into the appropriate password or OTP field. Depending on your organization's policies, you may need to enter a personal Security PIN either before or after the token code.

In the example below, the Security PIN 1427 is required before the token code.



What if My Token Shuts Off While I am Copying the Token Code?

If your token shuts off while you are entering the token code, simply generate a new token code by firmly pressing the button and quickly releasing it.

How Do I Use My GOLD and Platinum Tokens in Challenge-Response Mode?

If you are using a challenge-response type token, do the following:

1. Enter the PIN into your GOLD or Platinum tokens.
2. The token displays **Challenge?** on the device.
3. Enter the challenge provided on the SAS server into the **Challenge Code** field on the device.
4. Both tokens generate an OTP to be used for authentication.

NOTE: Use the steps above to enter a Token PIN in the GOLD and Platinum tokens.

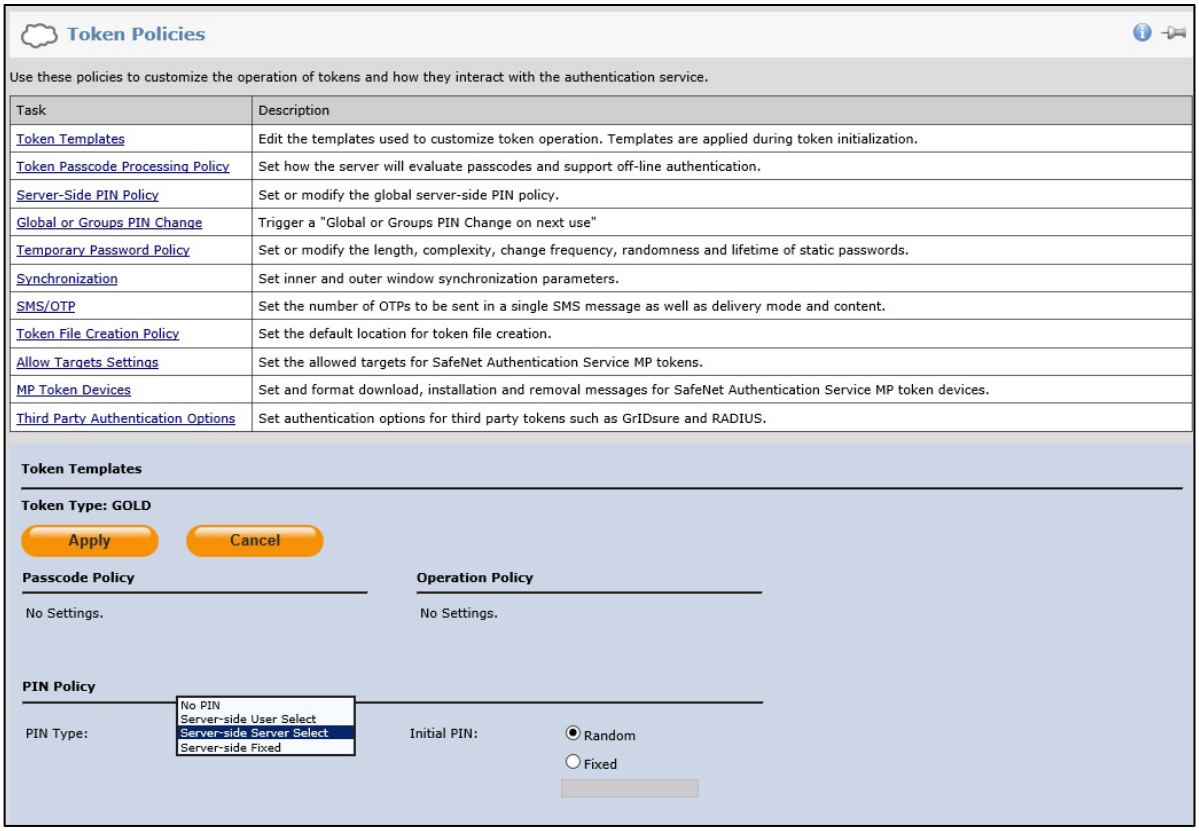
How Does Event-based OTP Authentication Work?

For Event–based OTP authentication, the system calculates the OTP passcode that should follow the OTP passcode saved from the last successful authentication.

How Do I Enter a Server Side PIN with My GOLD and Platinum Token?

If you are using a challenge-response type token, do the following:

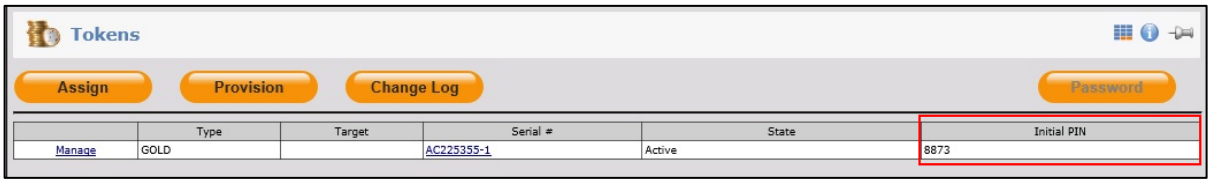
1. Click **Policy >Token Templates**.
2. In **Token Templates** panel, select **Gold** under the **Token Type** field, and click **Edit.**
3. Under **PIN Policy**, select one of the options below in the **PIN Type** field:
   - Server-side User Select
   - Server-side Server Select
   - Server-side Fixed



4. Select **Random** if you want the SAS server to randomly provide the PIN, or **Fixed**, if you want to specify a static PIN.

> **NOTE:** The Initial PIN is provided only after the self-enrollment process has been completed.

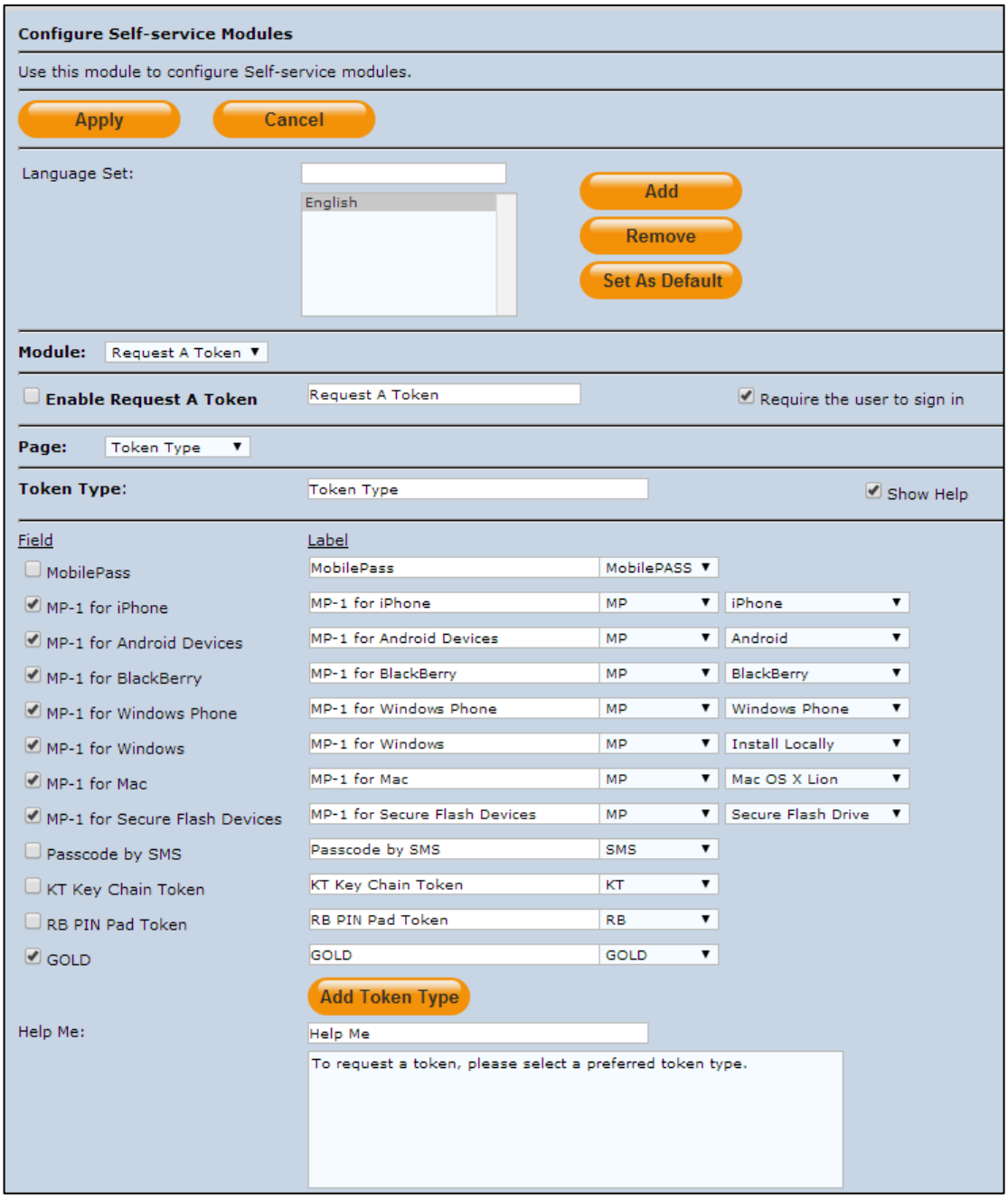
5. Get the Initial PIN by going to **Virtual Servers > Policy > Token Policies > Token Template > Tokens**.



6. Enter the Initial PIN plus the OTP generated by the GOLD and Platinum tokens when authenticating.

How Do I Add a Hardware Token to the Self-Service Portal?

1. In the SAS Management Console, go to: **Self-Service > Configure Self-Service Modules**.
2. Select **Request A Token** in the **Module** filed.
3. Select **Token Type** in the **Page** field.
4. Click **Add Token Type**. A **Token Type** row is added.
5. Click the drop-down arrow and select the relevant token type from the list.
6. Select the check box on the left, and click **Apply**.



What are My Responsibilities?

Using your SafeNet OTP token provides strong security, and simplifies your work efforts by reducing or eliminating the need to remember or periodically change passwords. As an additional measure, SafeNet recommends that you observe the following tips to ensure the highest level of security.

Where Should I Store My Token?

You should keep your token separate from your computer. Do not leave it on your desk, or with your computer bag. Treat it as you would your wallet, purse, or credit cards, and keep it with you at all times.

What If I Lose My Token?

If you lose your token, report it immediately to your helpdesk. The help desk will take the necessary actions to ensure the lost token does not present a security risk, and they will provide you with a temporary alternative for logging into the network until you receive a replacement token.

What If I Forget My Token?

Your token is a primary security device designed to protect you and the resources you access. Keep it with your car keys or purse or other valuable items that you use on a regular basis to minimize the potential to forget it. If you do forget your token, contact your help desk.

How Should I Protect My Personal Security PIN?

If you have a PIN, protect it just as you would the PIN for your bank or credit card. Never share it with anybody, including people you trust. Never write down your PIN.

How Can I Change My Security PIN?

If you wish to change your Security PIN, or if you are concerned that it has been compromised, go to your organization's self-service web site, and select the **Change PIN** option. Authenticate by entering your username and an OTP (your current Security PIN together with a token code). After authenticating, you will be prompted to enter and verify a new Security PIN.

What if I Forget My Security PIN?

If you forget your Security PIN, contact your help desk. Upon verifying your identity, the help desk will give you a temporary PIN. The next time you log in, you will be required to change the PIN to one known only by you.

What If I Cannot Log In Using My Token?

The most common cause of a failed login is copying the token code incorrectly. Never attempt to reuse a token code, and always ensure that you enter the token code exactly as displayed on the token. Be sure to include upper- and lower-case letters and punctuation characters.

If your organization requires you to enter a Security PIN together with the token code, ensure that it is entered correctly and that no spaces are entered.

Contact your help desk to resolve login issues.

How Long Will My Token Continue to Operate?

There are several factors that affect the battery life of a token. Your token should continue to function for five to 12 years before token replacement is required. Roughly two to three months before the battery is exhausted, a low battery warning will display for three to four seconds before each token code is displayed. You should contact your help desk as soon as possible when this warning appears. Your help desk will provide you with further instructions at that time.

Thinking Green

Never discard your token. It contains a battery and other materials that should be recycled or disposed of in an eco-friendly manner. Contact your help desk for proper disposal instructions.

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.

Contact Method	Contact Information	
Address	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017 USA	
Phone	United States	1-800-545-6608
	International	1-410-931-7520
Technical Support Customer Portal	https://serviceportal.safenet-inc.com 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.	