SafeNet Authentication Service

Token Guide

GrIDsure

Document Information

Document Part Number	007-012542-001, Rev. B
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

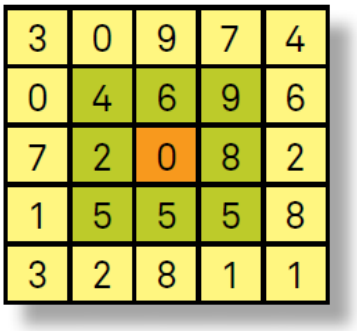
Introduction

About GrIDsure Authentication

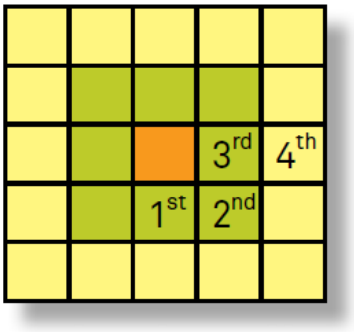
SafeNet's GrIDsure authentication method utilizes a person's ability to remember visual patterns. A GrIDsure token consists of a matrix of cells with random characters from which the user selects a "personal identification pattern" (PIP). Each time a user authenticates to a protected resource, they are presented with a challenge grid containing a new set of random characters from which they enter the characters that correspond to their PIP. Since the user responds to a new challenge in the form of a one-time passcode at each login instance, the end result provides security that is superior to static passwords. To this end, GrIDsure can mitigate such threats as shoulder surfing, keyloggers, password-guessing, and database hacking.

How GrIDsure Works

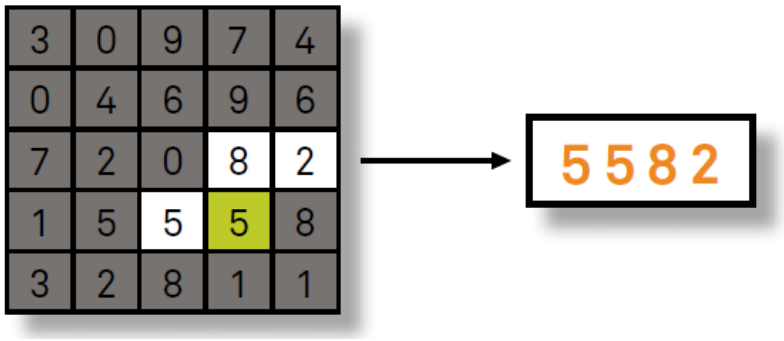
The user is presented a grid with a random set of characters.



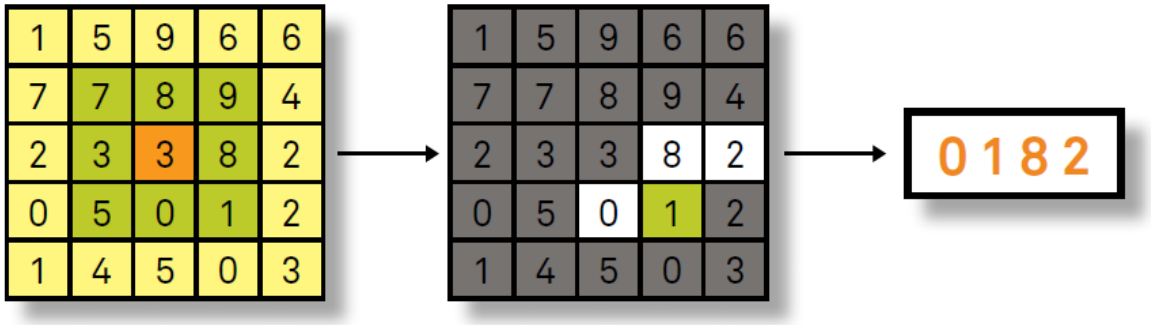
The user selects their personal identification pattern (PIP), consisting of a cell's location in the grid and the sequence in which its value is entered.



In this example, the user enters their PIP, producing an OTP of **5582**. SafeNet Authentication Service stores the PIP to compare it against PIPs entered in the future.



The next time the user logs in the same PIP will produce a new OTP. If the new PIP matches the one on record with SafeNet Authentication Service, access is granted.



Note that the PIP complexity and minimum PIP character length can be customized in SAS through **Third-Party Authentication Options** under **VIRTUAL SERVERS > POLICY > Token Policy**.

Compatible Network Access Points

SafeNet Authentication Service agents provide out-of-the box support for GrIDsure authentication (for example, IIS Agent, Windows Logon Agent). As a browser-based zero-footprint[1] authentication method, any device with a web browser can support GrIDsure, including desktops, laptops, thin clients[2], tablets, and mobile phones. (Any standard browser can be used.) For custom application integration, a snippet of JavaScript code needs to be included for the protected application to display the grid.

GrIDsure can be used to protect a wide range of applications and use cases, including:

- VPNs
- Network logon
- Cloud applications (SaaS)
- Web portals
- VDI

Grid tokens currently protect popular applications, including the following:

- Cisco ASA
- Citrix NetScaler
- F5 Big-IP APM
- IBM ISAM for Web
- IIS-7-based applications
- Juniper Networks
- Microsoft Office 365
- SonicWall SRA

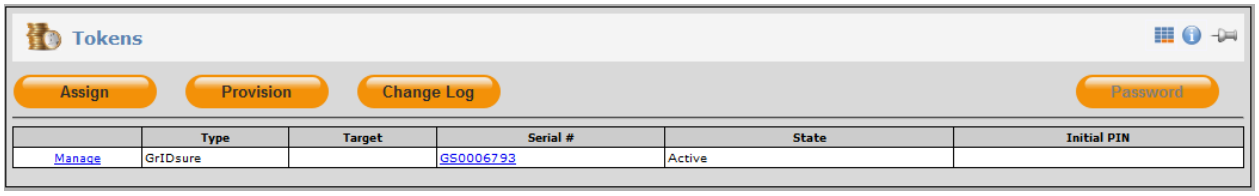
[1] Zero footprint in this context refers to the fact that GrIDsure authentication does not install software or modify the user's system in any way.

[2] Thin clients can authenticate using GrIDsure when the target system supports GrIDsure authentication; for example, the target web portal, remote web application, or network domain server.

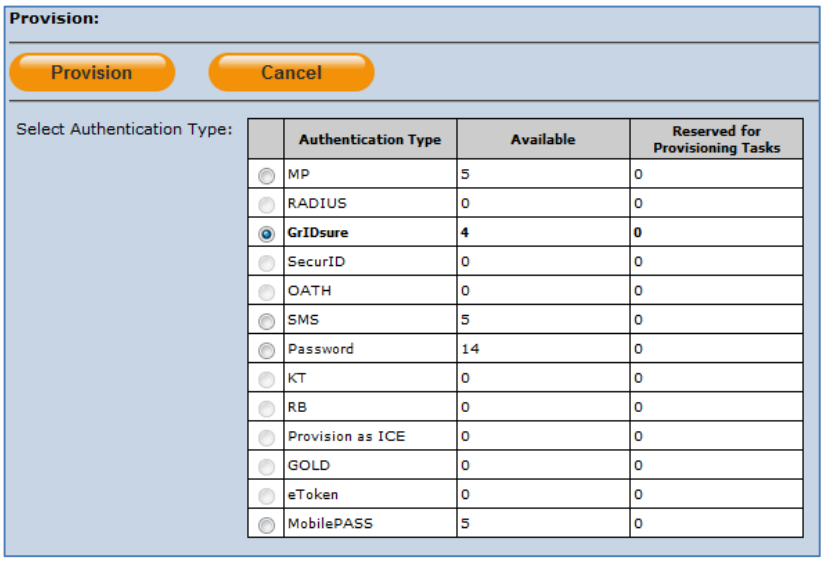
Provisioning a GrIDsure Token to a User

To provision a GrIDsure token to a user:

1. In the SAS Management Console, click the **Virtual Servers** tab.
2. In the **Managed Account** list, select an account.
3. Click the **Assignment** tab.
4. Search for and select a user account.
5. Click the **Tokens** module and then click the **Provision** button.



6. In the **Select Authentication Type** list, select **GrIDsure**.



7. Click the **Provision** button.

Now that the token has been provisioned to the user, the next step is for the user to self-enroll their token. An email will be automatically sent to the user and will contain a link at which they can perform self-enrollment. For information on this process, refer to “Self-Enrolling a GrIDsure Token” on page 8.

Self-Enrolling a GrIDsure Token

Self-enrollment is a simple process for SAS users to activate a GrIDsure token that has been provisioned to them and to create their personal identification pattern (PIP). When a user completes this process, they will be able to use their PIP to log in to resources protected with GrIDsure.

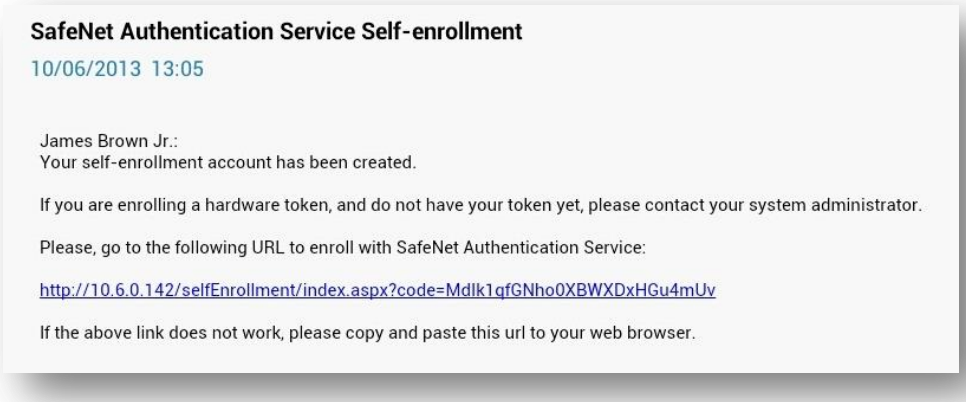
Self-Enrollment Process

A self-enrollment email will be sent from either the default email address or the custom “From” email defined in SAS. Likewise, the subject line will also be different depending on whether the default or a custom value is used. Note that the default values for both the email address and the subject line will be different for SAS Cloud and SAS PCE.

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

To self-enroll your GrIDsure token:

1. Read through the entire email before starting the process of enrolling your GrIDsure token.
2. When you are ready to begin enrollment, click the link in the email.



3. After clicking the email link, you are redirected to the **SafeNet Authentication Service – Self Enrollment** window. In this step, you must select a "personal identification pattern" (PIP) using the displayed grid. Remember, you are selecting a "pattern", not a number or letter sequence. The minimum PIP character length is four (4). Trivial PIPs are not allowed, as illustrated in the examples on the right side of the window.

> **NOTE:** Note that characters are case-sensitive; therefore, capital letter entry must be used for letter characters.

Once you have selected your PIP, click **Next** to continue.

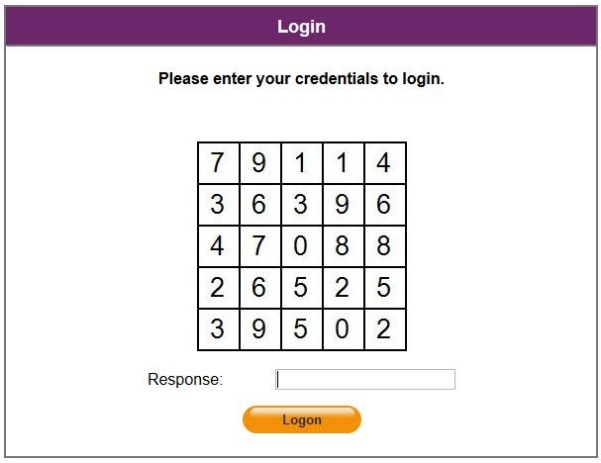
4. The next screen acknowledges that your token has been successfully activated and displays your user ID. You may now close your browser.

Authenticating with GrIDsure

The following steps guide you through accessing a website protected with GrIDsure configured to authenticate against a SAS server.

1. The user launches a web browser and enters a protected website address.
2. On the **Login** window, the user enters their user ID, and then clicks the **Logon** button.

3. The user is challenged with the GrIDsure grid and enters their PIP value in the **Response** field. After clicking the **Logon** button, if the credentials are valid, the user will be authenticated and will gain access to the protected website.



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.	