



STORMSHIELD



TECHNICAL NOTE

STORMSHIELD NETWORK SECURITY

CONFIGURING AND USING THE STORMSHIELD TOTP SOLUTION

Product concerned: SNS 4.7.5 and higher versions

Document last updated: April 10, 2024

Reference: [sns-en-configuring_using_totp_technical_note](#)



Table of contents

- Change log 3
- Getting started 4
- Requirements 5
 - A compatible SNS version installed 5
 - Prior connection of the SNS firewall to a directory 5
 - Permissions to access the SNS firewall's captive portal 5
 - Allowing users to generate TOTP's 5
- Operation and limitations 6
 - Authentication modes on the SNS firewall compatible with TOTP 6
 - Built-in and autonomous TOTP solution on each SNS firewall 6
 - How time-based one-time passwords work 6
 - Managing TOTP with the admin account on the SNS firewall 6
- Configuring the TOTP solution on the SNS firewall 7
 - Enabling NTP time synchronization 7
 - Adding and configuring TOTP as an authentication method 8
 - Enabling TOTP in the rules of the authentication policy 9
- TOTP enrollment procedure 10
- Authenticating with a TOTP 12
- Managing TOTP-enrolled users 13
 - Checking whether a user is enrolled for TOTP 13
 - Checking the validity of a user's TOTP 13
 - Resetting a user's TOTP enrollment 14
 - Resetting the TOTP enrollment of all users (resetting the TOTP database) 14
 - Showing and deleting orphan users from the TOTP database 15
- Monitoring use of the TOTP solution 16
 - In SNS firewall monitoring 16
 - In the SNS firewall's audit logs 16
- Troubleshooting 17
- Further reading 18



Change log

Date	Description
April 10, 2024	- SNS 4.7.5 release - Explanations regarding advanced configuration settings added to the section "Adding and configuring TOTP as an authentication method"
May 25, 2023	- Section "Authenticating with a TOTP" modified
February 2, 2023	- Section "Adding and configuring TOTP as an authentication method" modified
January 5, 2023	- New document



Getting started

The Stormshield TOTP solution makes it possible to increase the security of authentications that the SNS firewall manages. This additional security measure functions with 2FA (two-factor authentication), with which time-based one-time passwords (TOTP) can be used.

This solution is built into the SNS firewall and does not require any third-party TOTP solution. Users who authenticate with a TOTP only need to use an application installed on their browsers or mobile devices to generate TOTPs.

This technical note explains how to configure and manage the TOTP solution on the SNS firewall, and presents the enrollment procedure for TOTP solution users.



Requirements

You will need the following to perform the operations described in this technical note:

A compatible SNS version installed

- SNS 4.7.5 and higher versions

Prior connection of the SNS firewall to a directory

The SNS firewall must be connected to a directory so that it can display the lists of users and user groups in its modules. By doing so, the users and user groups required to authenticate with a TOTP can be determined during the configuration of the TOTP solution.

You can check this connection in the SNS firewall's web administration interface in **Configuration > Users > Authentication, Available methods** tab. An **LDAP, Kerberos** or **RADIUS** line should appear, depending on whether your SNS firewall is directly connected to an LDAP directory or whether it uses a specific protocol for authentication. For more information, refer to the section on [Authentication in the SNS v4 user manual](#).

Permissions to access the SNS firewall's captive portal

The SNS firewall's captive portal must be enabled and users who are required to authenticate with a TOTP must be able to access it. This is because users are enrolled through the captive portal.

You can check the configuration of the captive portal in the SNS firewall's web administration interface in **Configuration > Users > Authentication, Captive portal** and **Captive portal profiles** tabs. For more information, refer to the section on [Authentication in the SNS v4 user manual](#).

Allowing users to generate TOTPs

All users who are required to authenticate with a TOTP must have an application on their browsers or mobile devices allowing them to generate TOTPs. You can use, for example, Google Authenticator, Microsoft Authenticator or Authenticator for Firefox.

In this technical note, applications with which TOTPs can be generated are referred to as Authenticators.



Operation and limitations

Authentication modes on the SNS firewall compatible with TOTP

The TOTP solution makes it possible to increase the security of the following authentication modes on the SNS firewall:

- Captive portal,
- SSL VPN tunnels (*OpenVPN* technology only),
- Web administration interface,
- Console or SSH,
- IPsec VPN tunnels in IKEv1 (*Xauth* method only).

Built-in and autonomous TOTP solution on each SNS firewall

The TOTP solution is built into each SNS firewall and operates autonomously, except on firewalls in high availability clusters. Users who authenticate on several SNS firewalls on which TOTP has been enabled must first enroll on each firewall in question and use a TOTP corresponding to the relevant firewall in order to authenticate.

How time-based one-time passwords work

The TOTP solution relies on the use of time-based one-time passwords, also known as TOTP. A TOTP is valid for only a set period and can be used for only one authentication throughout this period. The same TOTP therefore cannot be used for two consecutive authentications, for example to connect via VPN, then via SSH. The user must wait for a new code to be generated before proceeding with the second authentication.

This system can only function if the date and time on the SNS and the various Authenticators are synchronized.

Managing TOTP with the *admin* account on the SNS firewall

The *admin* account on the SNS firewall cannot use TOTP. However, logging in with the admin account is necessary in order to perform certain operations, such as resetting an administrator's TOTP enrollment, or the TOTP enrollment of all users.



Configuring the TOTP solution on the SNS firewall

To set up the TOTP solution, several modules must be configured on the SNS firewall :


- [Enabling NTP time synchronization](#),
- [Adding and configuring TOTP as an authentication method](#),
- [Enabling TOTP in the rules of the authentication policy](#).

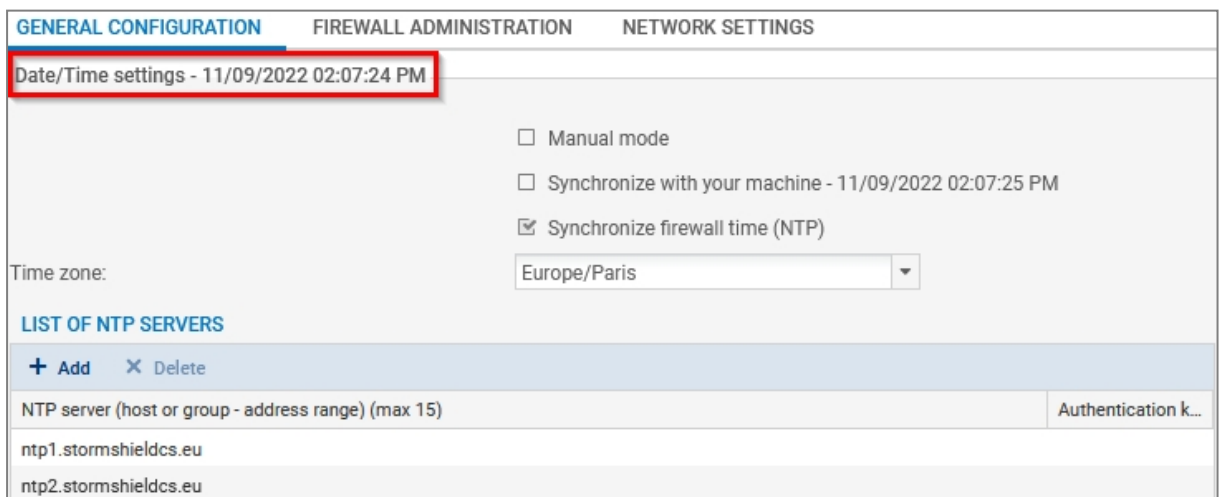
i NOTE

The operations explained in this chapter must be performed when the user is logged in to the SNS firewall's web administration interface at: https://firewall_IP_address/admin.

Enabling NTP time synchronization

Since the TOTP solution is based on limited-duration codes, the date and time on the SNS firewall must be accurate. To guarantee optimal operation, you are **strongly** advised to enable NTP time synchronization.

1. Go to **Configuration > System > Configuration, General configuration** tab.
2. Under **Date/Time settings**, select **Synchronize firewall time (NTP)**.
3. Ensure that you have the correct time zone, and change it if necessary.
4. Under **List of NTP servers**, you can keep the NTP servers entered by default or change them according to your preferences with the **Add** and **Delete** buttons.
5. If keys are needed to access the NTP servers, you can add keys under **List of NTP keys**, then associate them with the NTP servers under **List of NTP servers**.
6. Click on **Apply**.
7. A message will prompt you to restart the SNS firewall. Click on the  icon in the upper banner, then on **Restart now**.
8. Once the SNS firewall has restarted, in **Configuration > System > Configuration, General configuration** tab, under **Date/Time settings**, check whether the date and time on the SNS firewall are accurate.



The screenshot shows the 'GENERAL CONFIGURATION' tab of the SNS firewall web administration interface. The 'Date/Time settings' section is highlighted with a red box, showing the current date and time as '11/09/2022 02:07:24 PM'. Below this, there are three options: 'Manual mode' (unchecked), 'Synchronize with your machine - 11/09/2022 02:07:25 PM' (unchecked), and 'Synchronize firewall time (NTP)' (checked). The 'Time zone' is set to 'Europe/Paris'. Below the 'Date/Time settings' section is the 'LIST OF NTP SERVERS' section, which includes '+ Add' and 'X Delete' buttons. The table below shows two NTP servers: 'ntp1.stormshieldcs.eu' and 'ntp2.stormshieldcs.eu', both with an 'Authentication k...' column.

GENERAL CONFIGURATION		FIREWALL ADMINISTRATION	NETWORK SETTINGS
Date/Time settings - 11/09/2022 02:07:24 PM			
<input type="checkbox"/> Manual mode			
<input type="checkbox"/> Synchronize with your machine - 11/09/2022 02:07:25 PM			
<input checked="" type="checkbox"/> Synchronize firewall time (NTP)			
Time zone:		Europe/Paris	
LIST OF NTP SERVERS			
+ Add X Delete			
NTP server (host or group - address range) (max 15)			Authentication k...
ntp1.stormshieldcs.eu			
ntp2.stormshieldcs.eu			



Adding and configuring TOTP as an authentication method

This section explains how to add and configure TOTP as an authentication method.

1. Go to **Configuration > Users > Authentication, Available methods** tab.
2. Click on **Add a method** or **Enable a method** (according to the version installed on the SNS firewall) and click on **One-time password (TOTP)**.
3. Under **Time-based one-time password (TOTP)**, select the authentications for which you want to increase security with TOTP.
4. In **TOTP code settings**, enter the name of the TOTP issuer.
5. In **Customize the TOTP user enrollment message**, change the message that appears on the TOTP enrollment page. Add all the information that will be useful for your users (recommended Authenticator, installation instructions, etc.).
6. In **Advanced properties**, you can customize TOTP settings. The default settings are compatible with most authenticators. However, changing these settings may make them incompatible with some authenticators such as Google Authenticator and Microsoft Authenticator, which support only a limited number of settings.
 - **Lifetime (s)**: validity period of a TOTP. The Authenticator will automatically generate a new TOTP when this period expires,
 - **Code size**: length (number of characters) of generated TOTPs,
 - **Number of valid codes before and after current code**: period for which a generated code is considered valid, even if its lifetime has expired. This option makes it possible to extend the time allowed to enter the TOTP, which is particularly useful if the time is slightly desynchronized on the SNS firewall and the device on which the Authenticator is installed. For example, a value of "3" means that a generated TOTP is considered valid for the validity period of 3 TOTPs in the past or future. So if a TOTP is valid for 30 seconds, the validity period will therefore be 1m30 before the code is generated and 1m30 after it expires,
 - **Hash algorithm**: algorithm used when generating TOTPs.
7. Click on **Apply**.

! IMPORTANT

If you change later the settings of the fields **Lifetime (s)**, **Code size** and **Hash algorithm**, you must **reset the TOTP database** and users who were already enrolled must follow the **enrollment procedure** all over again.

AVAILABLE METHODS	AUTHENTICATION POLICY	CAPTIVE PORTAL	CAPTIVE PORTAL PROFILES
+ Add a method X Delete			
Method			
LDAP			
Guest method			
Sponsorship method			
TOTP (SNS 2FA)			
		Time-based one-time password (TOTP)	
		<input checked="" type="checkbox"/> Captive portal	
		<input checked="" type="checkbox"/> SSL VPN tunnels	
		<input checked="" type="checkbox"/> Web administration interface	
		<input checked="" type="checkbox"/> SSH/Console	
		<input checked="" type="checkbox"/> IPsec/Xauth	



Enabling TOTP in the rules of the authentication policy

You can enable TOTP for individual rules in the authentication policy. Users who authenticate through these rules must then enter a TOTP during authentication.

! IMPORTANT

Ensure beforehand that affected users can access the captive portal. Otherwise, they will neither be able to enroll for TOTP nor authenticate (see [Requirements](#)).

1. Go to **Configuration > Users > Authentication, Authentication policy** tab.
2. Select the checkbox in the **One-time password** column for the desired rules, and for which the method is compatible with TOTP (see [Requirements](#)). You can also adapt the current authentication policy by creating rules that apply to specific user groups. During authentication, rules will be scanned in the order of their appearance in the list, so remember to organize them logically by using the **Up** and **Down** buttons.
3. Click on **Apply**.

AVAILABLE METHODS		AUTHENTICATION POLICY		CAPTIVE PORTAL		CAPTIVE PORTAL PROFILES	
Search by user...		+ New rule		X Delete		↑ Up ↓ Down ✂ Cut 📄 Copy 📄 Paste	
	Status	Source		Methods (assess by order)		One-time password	
[-] External admins (contains 1 rules, from 2 to 2)							
2	Enabled	adm_external@external.ad	any	1	Default method	<input checked="" type="checkbox"/>	
[-] Local admins (contains 1 rules, from 4 to 4)							
4	Enabled	local_admins@local.ad	adm	1	Default method	<input type="checkbox"/>	



TOTP enrollment procedure

Once the TOTP solution is configured, users required to use TOTP authentication must follow the enrollment procedure below.

1. Open a recent web browser.
2. Go to the SNS firewall's captive portal at https://firewall_IP_address/auth.

STORMSHIELD Network Security EN ▾

Username

Authentication duration 4 hours ▾

Logout Login

3. Authenticate with your usual login credentials.
The **TOTP enrollment** page appears (pictured below). Its address should resemble https://firewall_IP_address/auth/totp_enroll.html.

STORMSHIELD Network Security EN ▾

TOTP enrollment

Please use the Microsoft Authenticator or Google Authenticator app to scan the QR code. If there is a problem, please contact your administrator.

Show information in text format

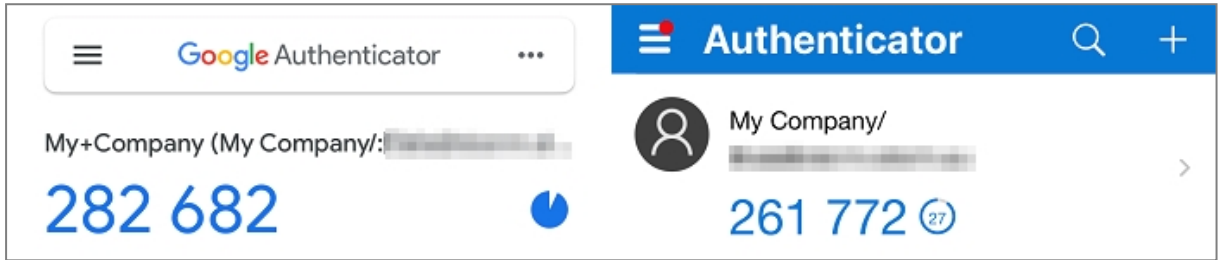
Code

Cancel OK



4. Open the Authenticator app installed on your work or mobile device.
5. To add an account to your Authenticator, click on the button allowing you to scan a QR code, then scan the code of the **TOTP enrollment** page. If your Authenticator does not allow you to scan QR codes and requests a key, click on **Show information in text format** on the **TOTP enrollment** page and retrieve the **Secret key**.

Once the account is added, a line will appear with the code and a countdown timer next to it. The amount of time shown represents the remaining time before the TOTP expires.



6. On the **TOTP enrollment** page, enter the code that appears in the Authenticator and click on **OK**. The code must still be valid the moment you click on **OK**.

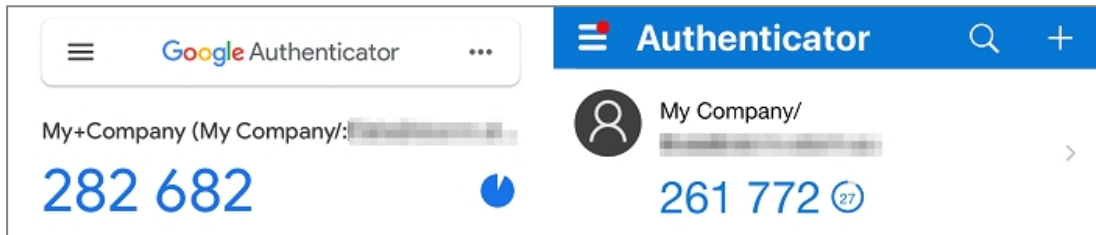
The connection window to the captive portal will appear again, indicating that the enrollment was successful. For future authentications that require a TOTP, it must be obtained in the Authenticator.



Authenticating with a TOTP

Once the TOTP solution is configured, users required to use TOTP authentication and who are enrolled must use a TOTP to authenticate. Users who are not yet enrolled must first follow the [TOTP enrollment procedure](#).

1. Go to the portal or launch the app on which you are authenticating.
2. Enter your user name and password as usual.
3. Open your Authenticator to obtain a TOTP. Check that you are authenticating on the right SNS firewall. As a reminder, the same TOTP cannot be used twice for two consecutive authentications.



4. There are two ways to use the TOTP, depending on the portal or app in question:
 - **When there is a specific field to fill in.** This applies especially to:
 - The SNS firewall's captive portal,
 - The SNS firewall's administration interface,
 - The SN SSL VPN Client app.Enter the OTP code in the specific field and log in. The field may be named "multifactor authentication", "2FA", "Code" or "OTP".
 - **When there is no specific field.** This applies especially to:
 - The console,
 - SSH,
 - The SN VPN Client Standard and SN VPN Client Exclusive apps,
 - The *OpenVPN* apps.

Concatenate the TOTP to your usual password and log in.

The images below provide a few examples of where the TOTP must be used. For more information, refer to the guide relating to the portal or app used.

SNS firewall's captive portal

SN SSL VPN Client connection window



Managing TOTP-enrolled users

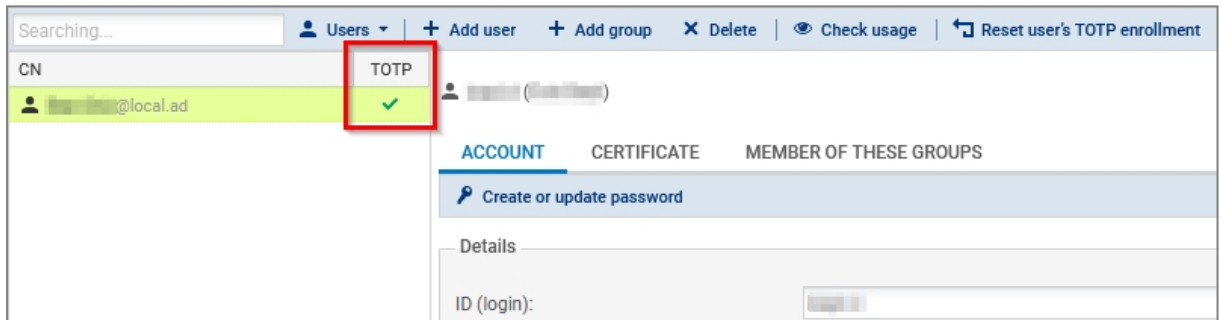
This chapter explains how to manage TOTP-enrolled users (status, resetting TOTP enrollments, validity of TOTP, etc.).

i NOTE

The operations explained in this chapter must be performed when the user is logged in to the SNS firewall's web administration interface at: https://firewall_IP_address/admin.

Checking whether a user is enrolled for TOTP

1. Go to **Configuration > Users > Users**.
2. Click on **Filter > Users**.
3. Enrolled users will see their names followed by a green check in the TOTP column. Check the TOTP enrollment status of the user in question.



Checking the validity of a user's TOTP

If a user encounters issues while authenticating with a TOTP, you can check the validity of the TOTP that they use.

1. Go to **Configuration > Users > Users**.
2. Click on **Filter > Users**.
3. Click on the user in question.
4. Under **TOTP**, in the **TOTP code to be verified** field, enter the code in question. If the **TOTP** section does not appear, this means that the user is not enrolled for TOTP on this SNS firewall.
5. Click on **Check use**.
A message will indicate whether the code is currently valid. Even if a TOTP no longer appears in the user's Authenticator, it may still remain valid for some time, depending on the settings in the TOTP advanced configuration (see [Adding and configuring TOTP as an authentication method](#)).



▲ TOTP

TOTP code to be verified:

✓ Check use

✓ 255509 is a valid code.

↶ Reset user's TOTP enrollme...

Resetting a user's TOTP enrollment

i NOTE

The user must be connected with the *admin* account to reset the enrollment of an administrator.

1. Go to **Configuration > Users > Users**.
2. Click on **Filter > Users**.
3. Click on the user in question.
4. Under **TOTP**, click on **Reset user's enrollment**.
5. Click on **OK**.
6. Ask the user to delete the corresponding account from their Authenticator and to follow the [TOTP enrollment procedure](#) all over again.

▲ TOTP

TOTP code to be verified:

✓ Check use

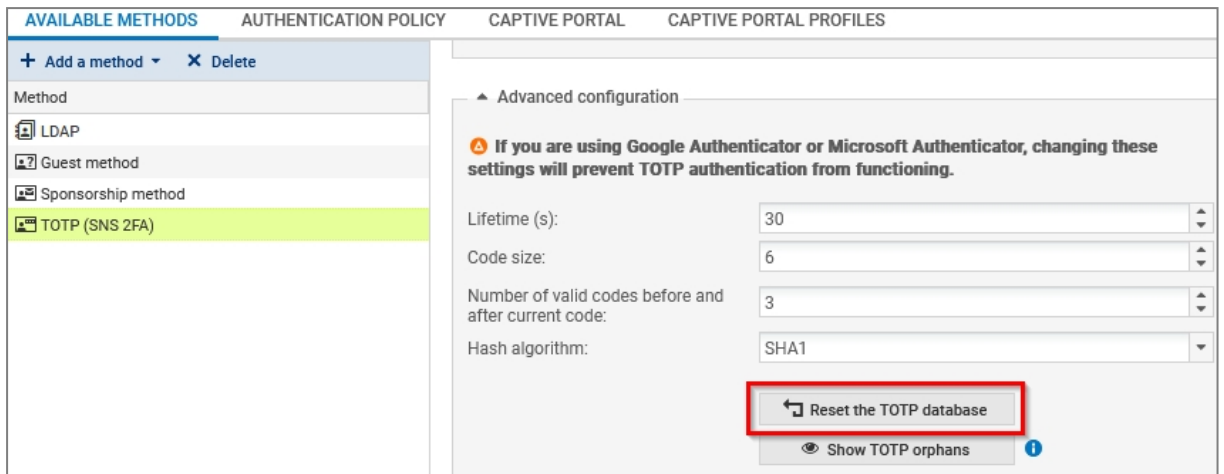
↶ Reset user's TOTP enrollme...

Resetting the TOTP enrollment of all users (resetting the TOTP database)

i NOTE

The user must be connected with the *admin* account to reset the TOTP database.

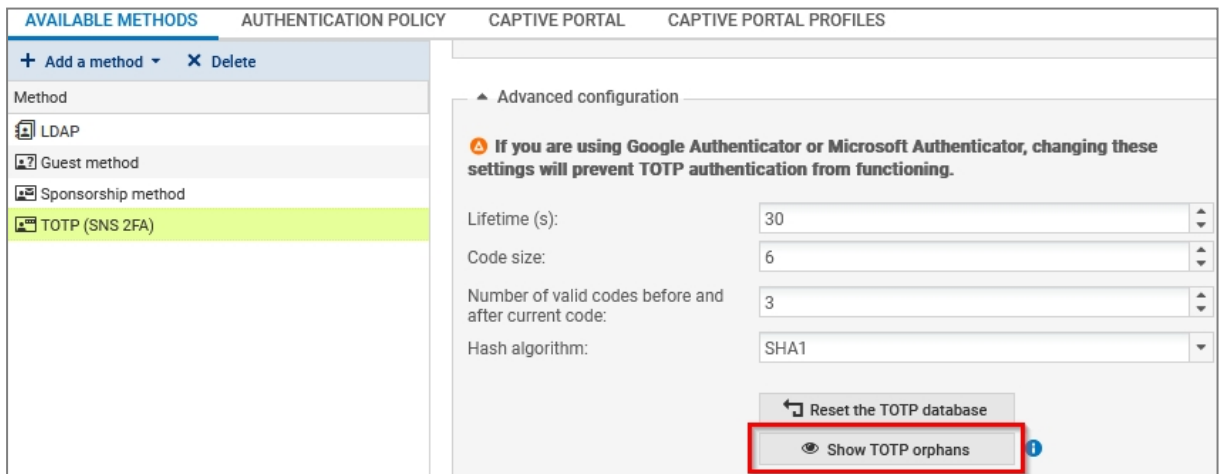
1. Go to **Configuration > Users > Authentication, Available methods** tab.
2. Click on **TOTP (2FA SNS)**.
3. Under **Advanced configuration**, click on **Reset the TOTP database**.
4. Click on **Next**.
5. Ask all users to delete the corresponding account from their Authenticator and to follow the [TOTP enrollment procedure](#) all over again.



Showing and deleting orphan users from the TOTP database

Orphan users are those found in the TOTP database but cannot be found in the LDAP directories configured on the SNS firewall. You can display the list of orphan users and delete them from the TOTP database.

1. Go to **Configuration > Users > Authentication, Available methods** tab.
2. Click on **TOTP (2FA SNS)**.
3. Under **Advanced configuration**, click on **Show TOTP orphans**.
The list of users who have not authenticated in the past 3 months (and who cannot be found in the LDAP directories) will appear in the window.
4. You can change the date of the last authentication taken into account to display the list of orphan users. Click on **Chosen date** and select the desired date.
5. Click on **Remove**. This operation will delete from the TOTP database **all** orphan users currently shown in the list.





Monitoring use of the TOTP solution

This chapter explains how to monitor the way users use the TOTP solution from the SNS firewall's web administration interface.

In SNS firewall monitoring

Monitoring allows you to view in real time the users who are currently authenticated and shows you whether they used a TOTP. A history graph is also available to show the distribution of authentications on the SNS firewall by type (including TOTP).

1. Go to **Monitoring > Monitoring > Users**.
2. Click on the tab of the data that you want to view.

The screenshot shows the 'MONITOR / USERS' interface with tabs for 'REAL-TIME' and 'HISTORY'. The 'REAL-TIME' tab is active. The interface includes a search bar with 'No predefined filter', a 'Filter' button, 'Reset', 'Refresh', 'Export results', and 'Configure authentication' links. A table displays user information:

Name	IP address	Directory	Group	Expiry date	Auth. method	One-time password	Administrator
[Redacted]	[Redacted]	fw.internal.tld		3h 59m 46s	PLAIN	✓	

A vertical label on the left side of the table reads 'FILTERS (NO FILTERS CREATED)'.

In the SNS firewall's audit logs

The *Users* log can show whether a TOTP was used during an authentication. A message indicates the status of the authentication (success, failure, disconnection, etc.). To look up a log, go to **Monitoring > Logs - Audit logs > Users**.

Some information can be accessed if the user has been granted permissions to look up private data. If you hold this permission or a code to access private data, click on **Logs: restricted access** in the upper banner. For further information, refer to the Technical note [Complying with privacy regulations](#).

The screenshot shows the 'LOG / USERS' interface. It features a time range selector set to 'Last hour', a 'Refresh' button, and a search bar. Below the search bar, the search range is specified as 'SEARCH FROM - 11/14/2022 02:32:07 PM - TO - 11/14/2022 03:32:07 PM'. A table displays the audit log entries:

Saved at	User	Source	Method	One-time password	Message
03:30:56 PM	[Redacted]	[Redacted]	PLAIN	TOTP code used	authentication failed, invalid TOTP code
03:30:44 PM	[Redacted]	[Redacted]	PLAIN	TOTP code used	user is logged out
03:30:17 PM	[Redacted]	[Redacted]	PLAIN	TOTP code used	user is logged in for 4 hours
03:29:57 PM	[Redacted]	[Redacted]		TOTP code used	totp enrolment: user TOTP request registered



Troubleshooting

In this chapter, you will see some of the issues that occur most frequently when using the the TOTP solution. If the issue you encounter cannot be found in this chapter, we recommend that you refer to the [Stormshield knowledge base](#).

Using hash algorithm SHA256 or SHA512 may generate the error "Wrong TOTP code"

- *Situation:* During a user's TOTP enrollment, the error "Wrong TOTP code" appears.
- *Cause:* The Authenticator used does not support the SHA256 or SHA512 hash algorithm specified in the configuration of the TOTP authentication method on the SNS firewall.
- *Solution:* In **Configuration > Users > Authentication, Available methods** tab, on the **TOTP (2FA SNS)** line, change the hash algorithm for SHA1 and reset the TOTP database. Next, ask your users to follow the [TOTP enrollment procedure](#) again. For more information, refer to [Wrong TOTP code - Stormshield Knowledge Base](#) [authentication required].

Authenticating with a TOTP or enrolling for TOTP is not or no longer possible

- *Situation:* One or several users cannot or can no longer enroll for TOTP or authenticate with a TOTP.
- *Cause:* The date and time on the device on which the user's Authenticator is installed are different from the date and time configured on the SNS firewall. If a user is already enrolled for TOTP, you can [check the validity of the TOTPs that they use](#). If you notice that the TOTPs in the user's Authenticator appear as valid but the verification on the SNS firewall indicates otherwise, the issue is likely due to the synchronization of the date and time.
- *Solutions:*
 - Check the date and time set on the SNS firewall in **Configuration > System > Configuration, General configuration** tab, under **Date/Time settings**. If any of the properties are incorrect, change them. As a reminder, we strongly recommend that you [enable NTP time synchronization](#).
 - On the device on which the user's Authenticator is installed, check whether the date and time match those configured on the SNS firewall. They must be completely synchronized.



Further reading

Additional information and answers to questions you may have about TOTP authentication are available in the [Stormshield knowledge base](#) (authentication required).



STORMSHIELD

documentation@stormshield.eu

All images in this document are for representational purposes only, actual products may differ.

Copyright © Stormshield 2024. All rights reserved. All other company and product names contained in this document are trademarks or registered trademarks of their respective companies.