NOTE TECHNIQUE

STORMSHIELD NETWORK SECURITY

CONFIGURER ET UTILISER LA SOLUTION TOTP STORMSHIELD

Produits concernés : SNS 4.7.5 et versions supérieures

Dernière mise à jour du document : 10 avril 2024

Référence : sns-fr-configurer_utiliser_totp_note technique

Table des matières

Historique des modifications 3
Avant de commencer 4
Prérequis 5
Avoir installé une version SNS compatible 5
Avoir connecté le firewall SNS à un annuaire 5
Permettre aux utilisateurs d'accéder au portail captif du firewall SNS 5
Permettre aux utilisateurs de générer des codes TOTP 5
Fonctionnement et limitations 6
Authentifications du firewall SNS compatibles avec la solution TOTP 6
Solution TOTP intégrée et indépendante sur chaque firewall SNS 6
Principe des mots de passe à usage unique basés sur le temps 6
Gestion de la solution TOTP avec le compte admin du firewall SNS 6
Configurer la solution TOTP sur le firewall SNS 7
Activer la synchronisation de temps via NTP 7
Ajouter et configurer la méthode d'authentification TOTP 8
Activer TOTP dans les règles de la politique d'authentification 9
Réaliser la procédure d'enrôlement TOTP 10
Utiliser un code TOTP pour s'authentifier 12
Gérer les utilisateurs enrôlés au TOTP 13
Vérifier si un utilisateur est enrôlé au TOTP 13
Vérifier la validité d'un code TOTP d'un utilisateur 13
Réinitialiser l'enrôlement TOTP d'un utilisateur 14
Réinitialiser l'enrôlement TOTP de tous les utilisateurs (réinitialiser la base TOTP) 14
Afficher et supprimer les utilisateurs orphelins de la base TOTP 15
Superviser l'utilisation de la solution TOTP par les utilisateurs 16
Dans la supervision du firewall SNS 16
Dans les journaux d'audit (logs) du firewall SNS 16
Résoudre les problèmes 17
Pour aller plus loin 18

Historique des modifications

Date	Description
10 avril 2024	- Sortie de SNS 4.7.5 - Ajout de précisions concernant les paramètres de configuration avancée dans la section "Ajouter et configurer la méthode d'authentification TOTP"
25 mai 2023	- Section "Utiliser un code TOTP pour s'authentifier" modifiée
2 février 2023	- Section "Ajouter et configurer la méthode d'authentification TOTP" modifiée
5 janvier 2023	- Nouveau document

Avant de commencer

La solution TOTP Stormshield permet d'accroître la sécurité des authentifications gérées par le firewall SNS. Cette sécurisation supplémentaire fonctionne avec une méthode d'authentification *2FA* (à deux facteurs) permettant d'utiliser des mots de passe à usage unique basés sur le temps (TOTP - *Time-based One-time Password*).

Cette solution est embarquée sur le firewall SNS et ne nécessite pas la mise en place d'une solution TOTP tierce. Les utilisateurs soumis à l'authentification TOTP n'ont besoin que d'une application installée sur leur navigateur Internet ou sur leur appareil mobile pour générer des codes d'authentification TOTP.

Cette note technique présente la configuration et la gestion de la solution TOTP sur le firewall SNS ainsi que la procédure d'enrôlement des utilisateurs à la solution TOTP.

Prérequis

Les prérequis pour réaliser les manipulations de cette note technique sont les suivants.

Avoir installé une version SNS compatible

- SNS 4.7.5 et versions supérieures

Avoir connecté le firewall SNS à un annuaire

Le firewall SNS doit être connecté à un annuaire afin d'afficher dans ses modules les listes d'utilisateurs et groupes d'utilisateurs. Ceci permettra de définir lors de la configuration de la solution TOTP les utilisateurs et groupes d'utilisateurs qui seront soumis à l'authentification TOTP.

Vous pouvez vérifier cette connexion dans l'interface Web d'administration du firewall SNS dans **Configuration > Utilisateurs > Authentification**, onglet **Méthodes disponibles**. Une ligne **LDAP**, **Kerberos** ou **RADIUS** doit apparaître selon si votre firewall SNS est directement connecté à un annuaire LDAP ou s'il utilise un protocole spécifique pour l'authentification. Pour plus d'informations, reportez-vous à la section Authentification du manuel utilisateur SNS v4.

Permettre aux utilisateurs d'accéder au portail captif du firewall SNS

Le portail captif du firewall SNS doit être activé et les utilisateurs qui seront soumis à l'authentification TOTP doivent pouvoir y accéder. En effet, l'enrôlement des utilisateurs s'effectue via le portail captif.

Vous pouvez vérifier la configuration du portail captif dans l'interface Web d'administration du firewall SNS dans **Configuration > Utilisateurs > Authentification**, onglets **Portail captif** et **Profils du portail captif**. Pour plus d'informations, reportez-vous à la section Authentification du manuel utilisateur SNS v4.

Permettre aux utilisateurs de générer des codes TOTP

Tous les utilisateurs qui seront soumis à l'authentification TOTP doivent disposer sur leur navigateur Internet ou sur leur appareil mobile d'une application leur permettant de générer des codes TOTP. Vous pouvez par exemple utiliser *Google Authenticator*, *Microsoft Authenticator*, ou encore *Authenticator pour Firefox*.

Dans cette note technique, les applications permettant de générer des codes TOTP sont désignées sous le terme *Authenticator*.

Fonctionnement et limitations

Authentifications du firewall SNS compatibles avec la solution TOTP

La solution TOTP permet d'accroître la sécurité des authentifications du firewall SNS suivantes :

- Portail captif,
- Tunnels VPN SSL (technologie *OpenVPN* seulement),
- Interface Web d'administration,
- Console ou SSH,
- Tunnels VPN IPsec IKEv1 (méthode *Xauth* uniquement).

Solution TOTP intégrée et indépendante sur chaque firewall SNS

La solution TOTP est intégrée et indépendante sur chaque firewall SNS, sauf dans le cas d'un cluster de firewalls en haute disponibilité. Un utilisateur qui s'authentifie sur plusieurs firewalls SNS bénéficiant de la solution TOTP doit s'enrôler au préalable sur chaque firewall concerné et utiliser un code TOTP correspondant au firewall concerné pour s'authentifier.

Principe des mots de passe à usage unique basés sur le temps

La solution TOTP repose sur l'utilisation de mots de passe à usage unique basés sur le temps, appelés codes TOTP. Un code TOTP n'est valide que pour une période de temps prédéfinie et ne peut être utilisé que pour une seule authentification pendant toute cette période. Il n'est donc pas possible de réaliser successivement deux authentifications en utilisant le même code TOTP, par exemple pour se connecter en VPN puis en SSH. Il est nécessaire d'attendre qu'un nouveau code soit généré avant de réaliser la deuxième authentification.

Ce principe ne peut fonctionner que si l'heure et la date du firewall SNS et des *Authenticator* sont parfaitement synchronisées.

Gestion de la solution TOTP avec le compte *admin* du firewall SNS

Le compte *admin* du firewall SNS ne peut pas bénéficier de la solution TOTP. Cependant, être connecté au compte *admin* est indispensable pour réaliser certaines actions, comme réinitialiser l'enrôlement TOTP d'un administrateur ou l'enrôlement TOTP de tous les utilisateurs.

Configurer la solution TOTP sur le firewall SNS

Mettre en œuvre la solution TOTP nécessite de configurer plusieurs modules sur le firewall SNS :

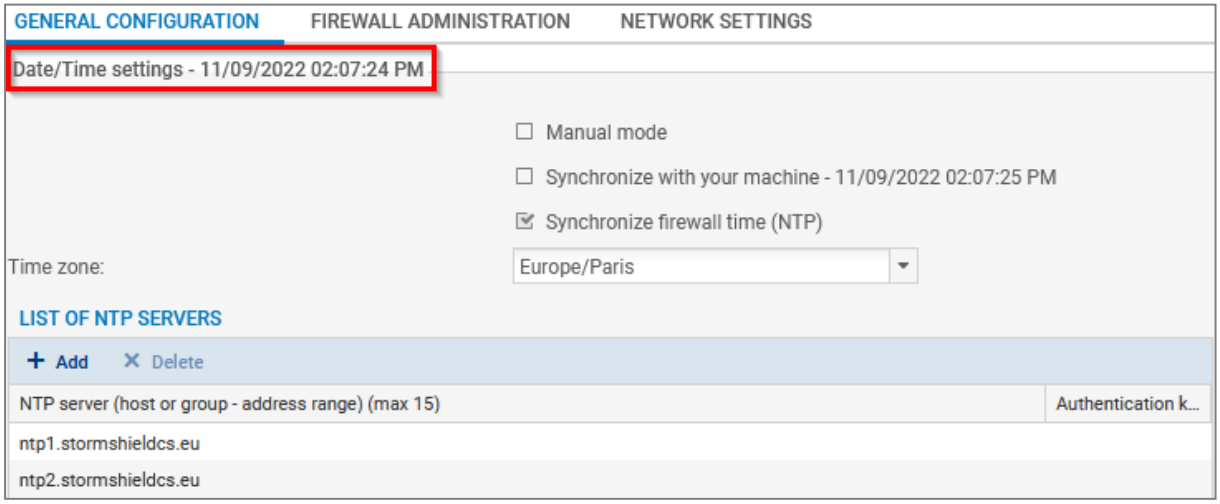
- Activer la synchronisation de temps via NTP,
- Ajouter et configurer la méthode d'authentification TOTP,
- Activer TOTP dans les règles de la politique d'authentification.

NOTE
Les manipulations de ce chapitre sont à réaliser en étant connecté à l'interface Web d'administration du firewall SNS à l'adresse : *https://adresseIP_du_firewall/admin*.

Activer la synchronisation de temps via NTP

Du fait que la solution TOTP repose sur l'utilisation de codes avec une durée de vie limitée dans le temps, l'heure et la date du firewall SNS doivent être à jour. Pour garantir un fonctionnement optimal, il est **fortement** recommandé d'activer la synchronisation de temps via NTP.

1. Rendez-vous dans **Configuration > Système > Configuration**, onglet **Configuration générale**.
2. Dans le cadre **Paramètres de date et d'heure**, cochez **Maintenir le firewall à l'heure (NTP)**.
3. Vérifiez que le fuseau horaire sélectionné est correct. Modifiez-le si besoin.
4. Dans la grille **Liste des serveurs NTP**, vous pouvez conserver les serveurs NTP renseignés par défaut ou les modifier selon vos besoins avec les boutons **Ajouter** et **Supprimer**.
5. Si l'accès aux serveurs NTP nécessite une clé, vous pouvez ajouter des clés dans la grille **Liste des clés NTP**, puis les associer aux serveurs NTP dans la grille **Liste des serveurs NTP**.
6. Cliquez sur **Appliquer**.
7. Un message vous invite à redémarrer le firewall SNS. Cliquez sur l'icône dans le bandeau supérieur, puis sur **Redémarrer maintenant**.
8. Une fois le firewall SNS redémarré, toujours dans **Configuration > Système > Configuration**, onglet **Configuration générale**, cadre **Paramètres de date et d'heure**, repérez si la date et l'heure du firewall SNS sont à jour.

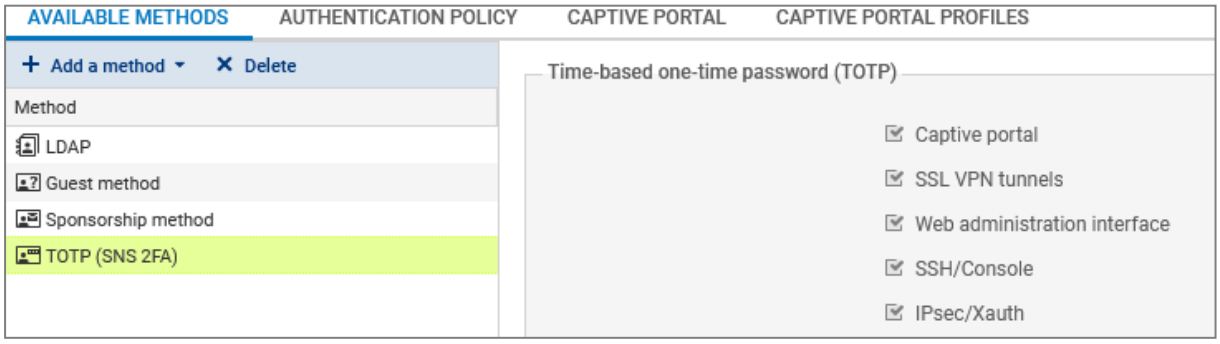


Ajouter et configurer la méthode d'authentification TOTP

Cette section explique comment ajouter et configurer la méthode d'authentification TOTP.

1. Rendez-vous dans **Configuration > Utilisateurs > Authentification**, onglet **Méthodes disponibles**.
2. Cliquez sur **Ajouter une méthode** ou **Activer une méthode** (selon la version installée sur le firewall SNS) et cliquez sur **Mot de passe à usage unique (TOTP)**.
3. Dans le cadre **Mot de passe à usage unique basé sur le temps (TOTP)**, sélectionnez les authentifications pour lesquelles vous souhaitez accroître la sécurité avec la solution TOTP.
4. Dans le cadre **Paramètres des codes TOTP**, entrez le nom de l'émetteur des codes TOTP.
5. Dans le cadre **Personnaliser le message d'enrôlement des utilisateurs TOTP**, modifiez le message qui s'affichera sur la page d'enrôlement TOTP. Ajoutez toutes les informations utiles pour vos utilisateurs (*Authenticator* recommandé, comment l'installer, etc.).
6. Dans le cadre **Configuration avancée**, vous pouvez personnaliser les paramètres des codes TOTP. Les paramètres par défaut sont compatibles avec la plupat des *Authenticator*. Les modifier peut être incompatible avec certains Authenticator, comme *Google Authenticator* et *Microsoft Authenticator*, qui ne supportent qu'un nombre limité de paramètres.
   - **Durée de vie (s)** : durée de vie d'un code TOTP. Un nouveau code est généré automatiquement par l'*Authenticator* une fois ce laps temps écoulé,
   - **Taille du code** : longueur (nombre de caractères) des codes TOTP générés,
   - **Nombre de codes valides avant et après le code actuel** : intervalle durant lequel un code généré est considéré comme valide, même si sa durée de vie est écoulée. Cette option permet d'allonger le délai de saisie du code, notamment utile en cas de légère désynchronisation de temps entre le firewall SNS et l'équipement où est installé l'*Authenticator*. Par exemple, la valeur "3" signifie qu'un code généré est considéré comme valide dans un intervalle de 3 codes dans le passé ou dans le futur. Si un code est valide pendant 30 secondes, alors l'intervalle de validité sera de 1m30 avant la génération du code et 1m30 après son expiration,
   - **Algorithme de hachage** : algorithme utilisé lors de la génération des codes TOTP.
7. Cliquez sur **Appliquer**.

IMPORTANT
Si vous modifiez par la suite les paramètres des champs **Durée de vie (s)**, **Taille du code** et **Algorithme de hachage**, vous devrez réinitialiser la base TOTP et les utilisateurs déjà enrôlés devront de nouveau suivre la procédure d'enrôlement.

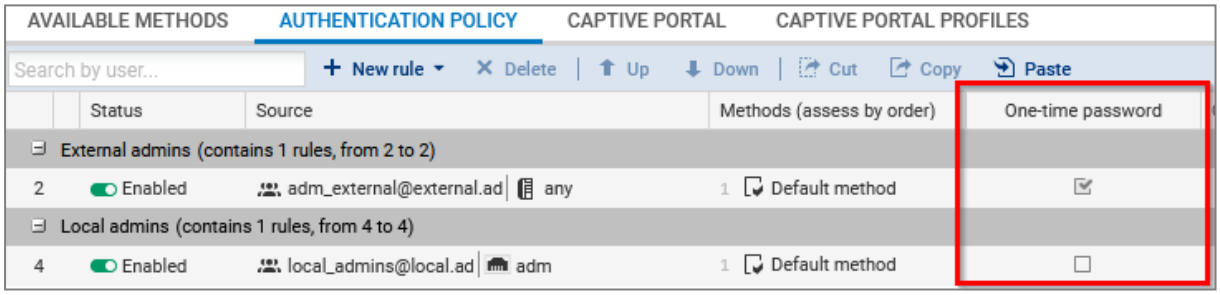


Activer TOTP dans les règles de la politique d'authentification

Vous pouvez activer TOTP pour chaque règle de la politique d'authentification. Les utilisateurs s'authentifiant via ces règles devront alors renseigner un code TOTP lors d'une authentification.

IMPORTANT
Assurez-vous au préalable que les utilisateurs concernés peuvent accéder au portail captif, sinon, ils ne pourront pas s'enrôler au TOTP et ne pourront plus s'authentifier (voir Prérequis).

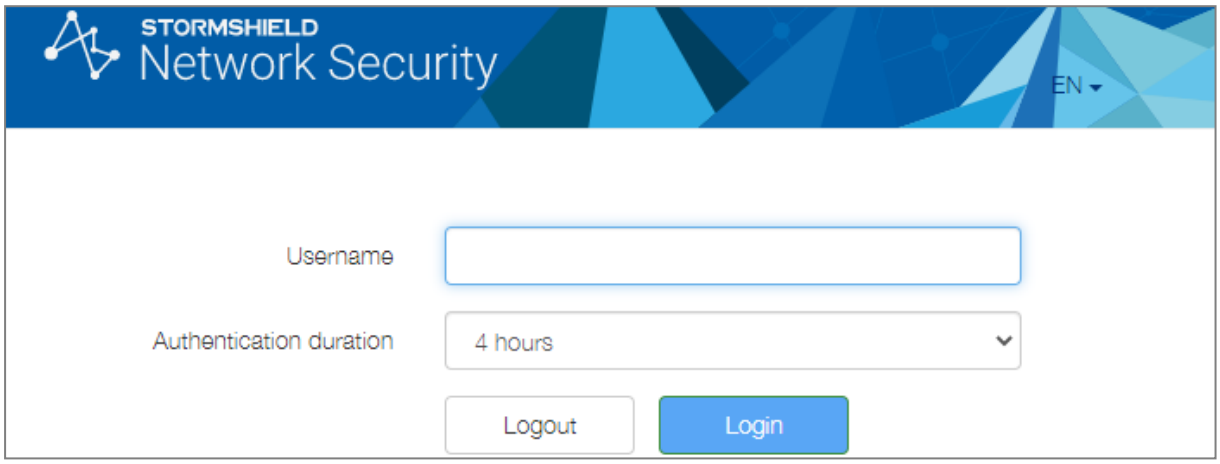
1. Rendez-vous dans **Configuration > Utilisateurs > Authentification**, onglet **Politique d'authentification**.
2. Pour les règles souhaitées, et pour lesquelles la méthode est compatible avec le TOTP (voir Prérequis), cochez la case dans la colonne **Mot de passe à usage unique**. Vous pouvez également adapter la politique d'authentification actuelle en créant des règles qui s'appliquent à des groupes d'utilisateurs spécifiques.
   Les règles sont examinées dans l'ordre de leur numérotation lors d'une authentification, pensez donc à les organiser de manière logique avec les boutons **Monter** et **Descendre**.
3. Cliquez sur **Appliquer**.



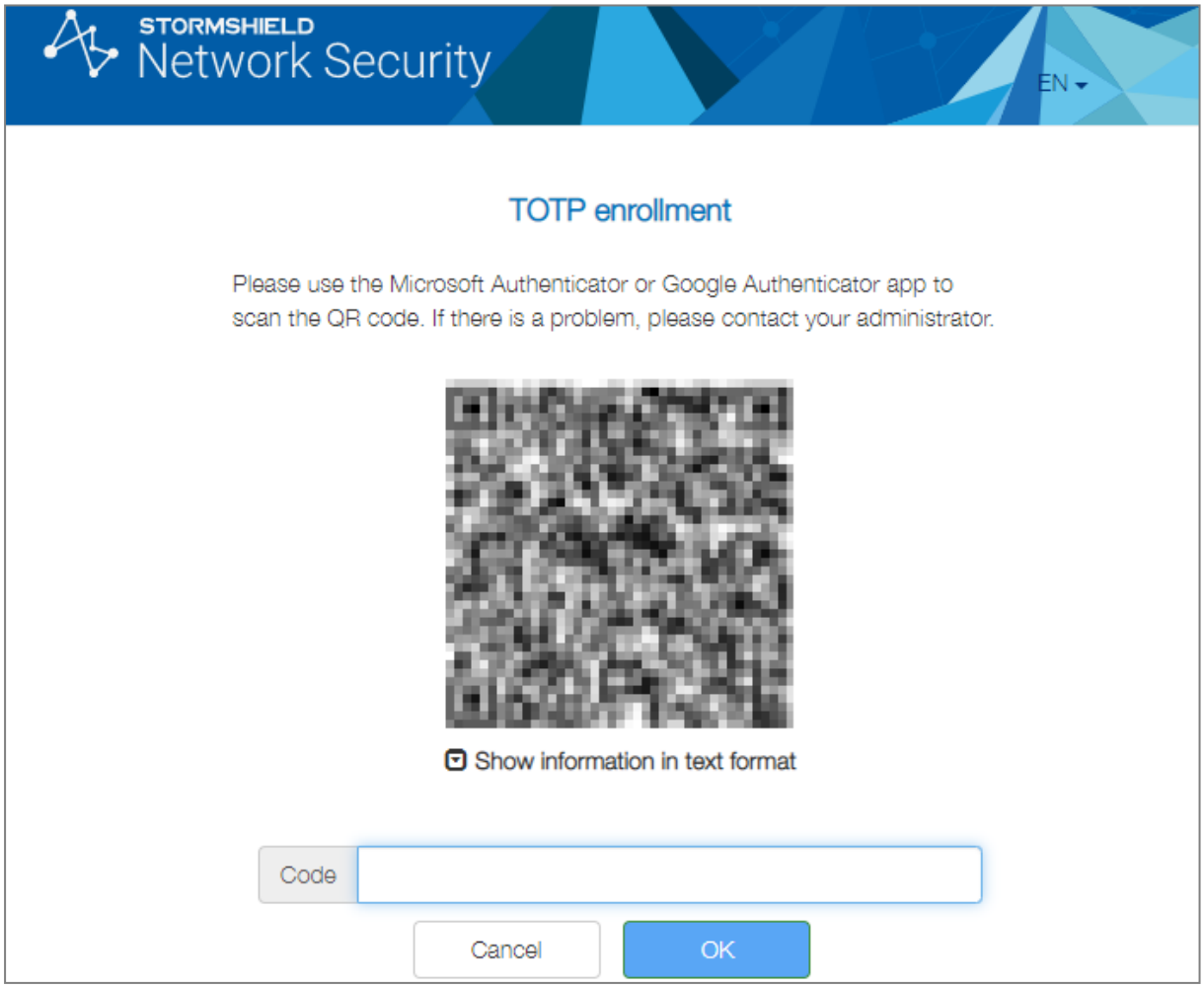
Réaliser la procédure d'enrôlement TOTP

Une fois la solution TOTP configurée, chaque utilisateur concerné par l'authentification TOTP doit réaliser la procédure d'enrôlement suivante.

1. Ouvrez un navigateur Internet récent.
2. Accédez au portail captif du firewall SNS à l'adresse *https://adresseIP_du_firewall/auth*.

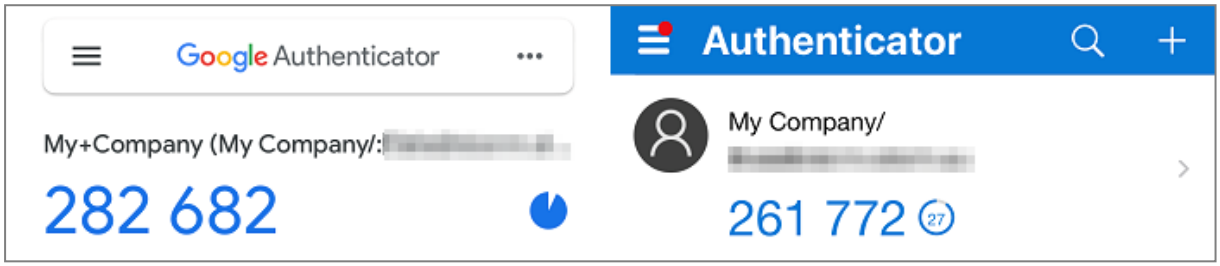


3. Authentifiez-vous avec vos identifiants, comme habituellement.
   La page **Enrôlement TOTP** apparaît (représentée sur l'image ci-dessous). Son adresse ressemble à *https://adresseIP_du_firewall/auth/totp_enroll.html*.



4. Ouvrez l'application *Authenticator* installée sur votre poste de travail ou terminal mobile.
5. Pour ajouter un compte dans votre *Authenticator*, appuyez sur le bouton permettant de scanner un QR code, puis scannez celui de la page **Enrôlement TOTP**. Si votre *Authenticator* ne permet pas de scanner de QR Code et demande une clé (*Key*), cliquez sur **Afficher les informations au format texte** sur la page **Enrôlement TOTP** et récupérez la **Clé secrète**.

   Une fois le compte ajouté, une ligne apparaît avec un code et un temps qui s'écoule à côté. Ce temps représente la durée de validité du code TOTP affiché.



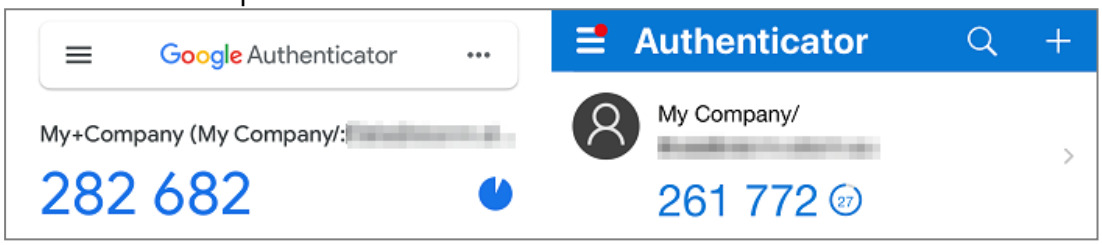
6. Sur la page **Enrôlement TOTP**, renseignez le code qui apparaît dans l'*Authenticator* et cliquez sur **OK**. Le code doit toujours être valide au moment où vous appuyez sur **OK**.

La page de connexion du portail captif s'affiche de nouveau, indiquant que l'enrôlement s'est réalisé avec succès. Pour les prochaines authentifications où un code TOTP est requis, vous devrez le récupérer dans l'*Authenticator*.

Utiliser un code TOTP pour s'authentifier

Une fois la solution TOTP configurée, les utilisateurs soumis à l'authentification TOTP et qui se sont enrôlés doivent utiliser un code TOTP pour s'authentifier. Les utilisateurs qui ne sont pas encore enrôlés doivent au préalable réaliser la procédure d'enrôlement TOTP.

1. Accédez au portail ou lancez le logiciel sur lequel vous vous authentifiez.
2. Renseignez votre nom d'utilisateur et votre mot de passe, comme habituellement.
3. Ouvrez votre *Authenticator* et récupérez un code TOTP. Vérifiez qu'il concerne bien le firewall SNS sur lequel vous vous authentifiez. Pour rappel, il n'est pas possible d'utiliser deux fois le même code TOTP pour réaliser successivement deux authentifications.



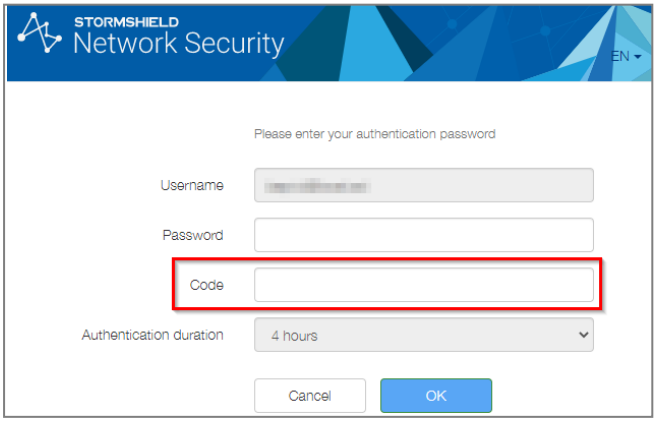
4. Pour utiliser le code TOTP, deux possibilités existent selon le portail ou le logiciel concerné :
   - **Un champ spécifique est à remplir**. Ce cas s'applique notamment :
     - Au portail captif du firewall SNS,
     - À l'interface d'administration du firewall SNS,
     - Au logiciel SN SSL VPN Client.

     Renseignez le code OTP dans le champ spécifique, puis connectez-vous. Le nom du champ peut être "authentification multifacteur", "2FA", "Code" ou "Code OTP".
   - **Aucun champ spécifique n'existe**. Ce cas s'applique notamment :
     - À la Console,
     - Au SSH,
     - Aux logiciels SN VPN Client Standard et SN VPN Client Exclusive,
     - Aux logiciels *OpenVPN*.

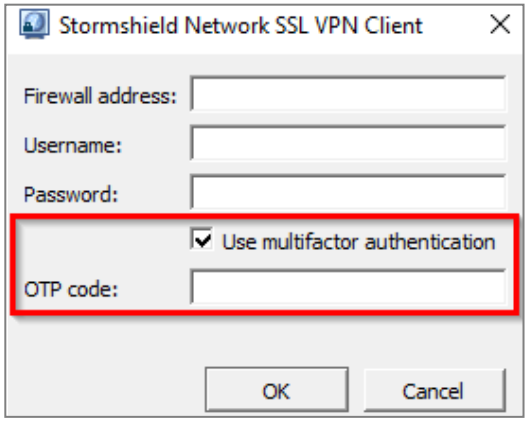
     Concaténez le code TOTP à votre mot de passe habituel, puis connectez-vous.

Les images ci-dessous montrent quelques exemples où le code TOTP doit être utilisé. Pour plus d'informations, reportez-vous au guide du portail ou du logiciel utilisé.

Portail captif du firewall SNS



Fenêtre de connexion du SN SSL VPN Client



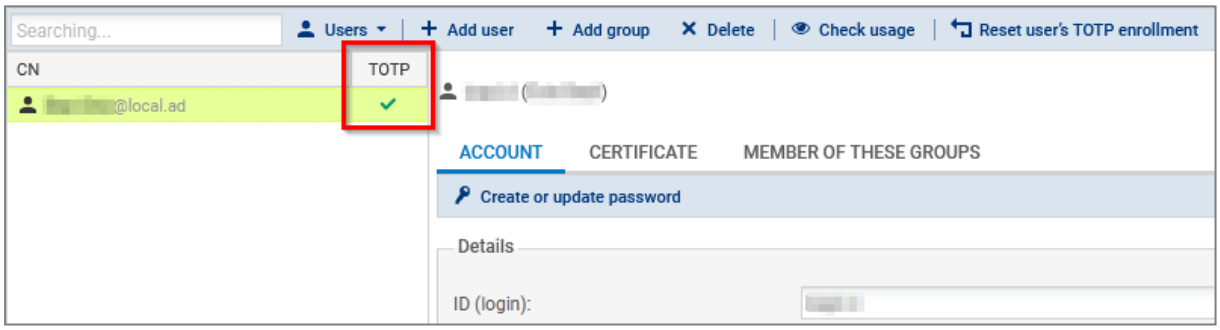
Gérer les utilisateurs enrôlés au TOTP

Ce chapitre explique comment gérer les utilisateurs enrôlés au TOTP (état ou réinitialisation des enrôlements TOTP, validité d'un code TOTP, etc.).

NOTE
Les manipulations de ce chapitre sont à réaliser en étant connecté à l'interface Web d'administration du firewall SNS à l'adresse : *https://adresseIP_du_firewall/admin*.

Vérifier si un utilisateur est enrôlé au TOTP

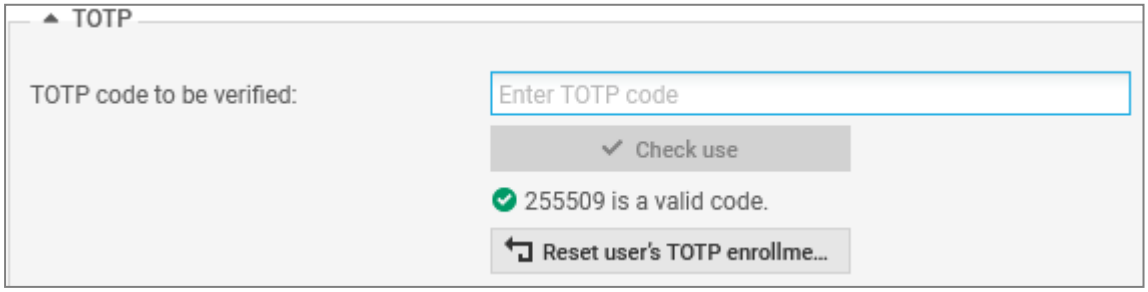
1. Rendez-vous dans **Configuration > Utilisateurs > Utilisateurs**.
2. Cliquez sur **Filtrer > Utilisateurs**.
3. Chaque utilisateur enrôlé voit son nom suivi d'une coche verte dans la colonne TOTP. Vérifiez l'état de l'enrôlement TOTP de l'utilisateur concerné.



Vérifier la validité d'un code TOTP d'un utilisateur

Si un utilisateur rencontre des difficultés pour s'authentifier avec un code TOTP, vous pouvez vérifier la validité des codes TOTP qu'il utilise.

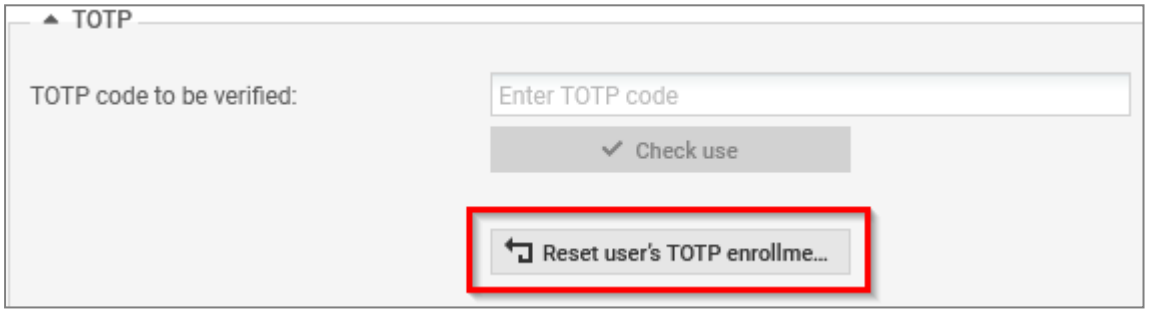
1. Rendez-vous dans **Configuration > Utilisateurs > Utilisateurs**.
2. Cliquez sur **Filtrer > Utilisateurs**.
3. Cliquez sur l'utilisateur concerné.
4. Dans le cadre **TOTP**, champ **Code TOTP à vérifier**, renseignez le code concerné. Si le cadre **TOTP** n'apparaît pas, l'utilisateur n'est pas enrôlé au TOTP sur ce firewall SNS.
5. Cliquez sur **Vérifier**.
   Un message indique si le code est actuellement valide ou non. Même si un code n'apparaît plus dans l'*Authenticator* de l'utilisateur, il peut être toujours valide pendant quelques instants selon les paramètres de configuration avancée de la méthode TOTP (voir Ajouter et configurer la méthode d'authentification TOTP).



Réinitialiser l'enrôlement TOTP d'un utilisateur

> **NOTE**
> Réinitialiser l'enrôlement d'un administrateur nécessite d'être connecté avec le compte *admin*.

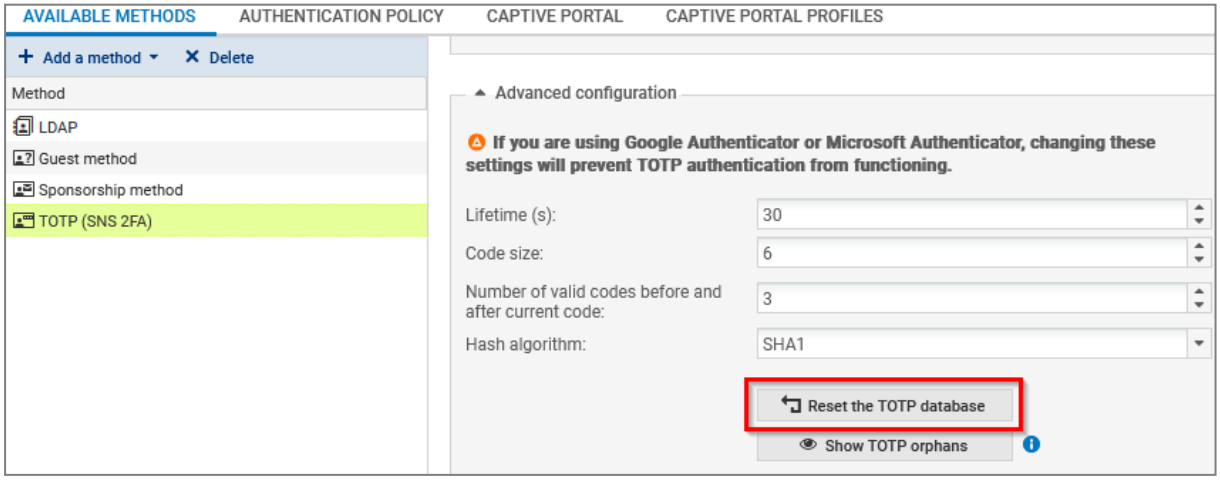
1. Rendez-vous dans **Configuration > Utilisateurs > Utilisateurs**.
2. Cliquez sur **Filtrer > Utilisateurs**.
3. Cliquez sur l'utilisateur concerné.
4. Dans le cadre **TOTP**, cliquez sur **Réinitialiser l'enrôlement**.
5. Cliquez sur **OK**.
6. Invitez l'utilisateur à supprimer de son *Authenticator* le compte correspondant et à suivre de nouveau la procédure d'enrôlement TOTP.



Réinitialiser l'enrôlement TOTP de tous les utilisateurs (réinitialiser la base TOTP)

> **NOTE**
> Réinitialiser la base TOTP nécessite d'être connecté avec le compte *admin*.

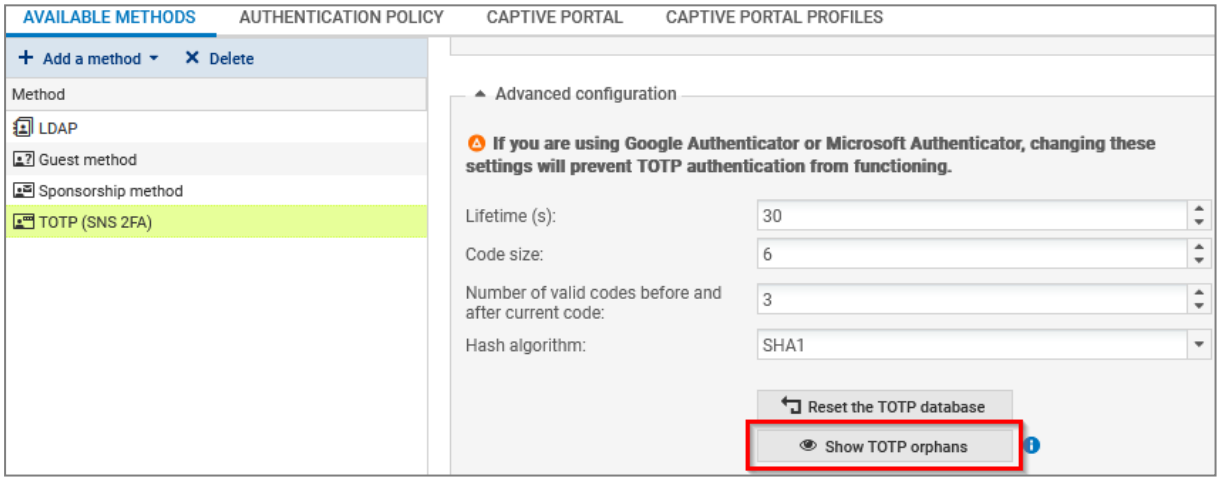
1. Rendez-vous dans **Configuration > Utilisateurs > Authentification**, onglet **Méthodes disponibles**.
2. Cliquez sur **TOTP (2FA SNS)**.
3. Dans le cadre **Configuration avancée**, cliquez sur **Réinitialiser la base TOTP**.
4. Cliquez sur **Suivant**.
5. Invitez tous les utilisateurs à supprimer de leur *Authenticator* le compte correspondant et à suivre de nouveau la procédure d'enrôlement TOTP.



Afficher et supprimer les utilisateurs orphelins de la base TOTP

Un utilisateur orphelin est un utilisateur présent dans la base TOTP mais qui est introuvable dans les annuaires LDAP configurés sur le firewall SNS. Vous pouvez afficher la liste des utilisateurs orphelins et les supprimer de la base TOTP.

1. Rendez-vous dans **Configuration > Utilisateurs > Authentification**, onglet **Méthodes disponibles**.
2. Cliquez sur **TOTP (2FA SNS)**.
3. Dans le cadre **Configuration avancée**, cliquez sur **Afficher les orphelins TOTP**.
   La liste des utilisateurs qui ne se sont pas authentifiés depuis 3 mois (et qui sont introuvables dans les annuaires LDAP) s'affiche dans la fenêtre.
4. Vous pouvez modifier la date de la dernière authentification prise en compte pour afficher la liste des utilisateurs orphelins. Cliquez sur **Date choisie** et sélectionnez la date souhaitée.
5. Cliquez sur **Supprimer**. Cette action supprime de la base TOTP **tous** les utilisateurs orphelins actuellement affichés dans la liste.



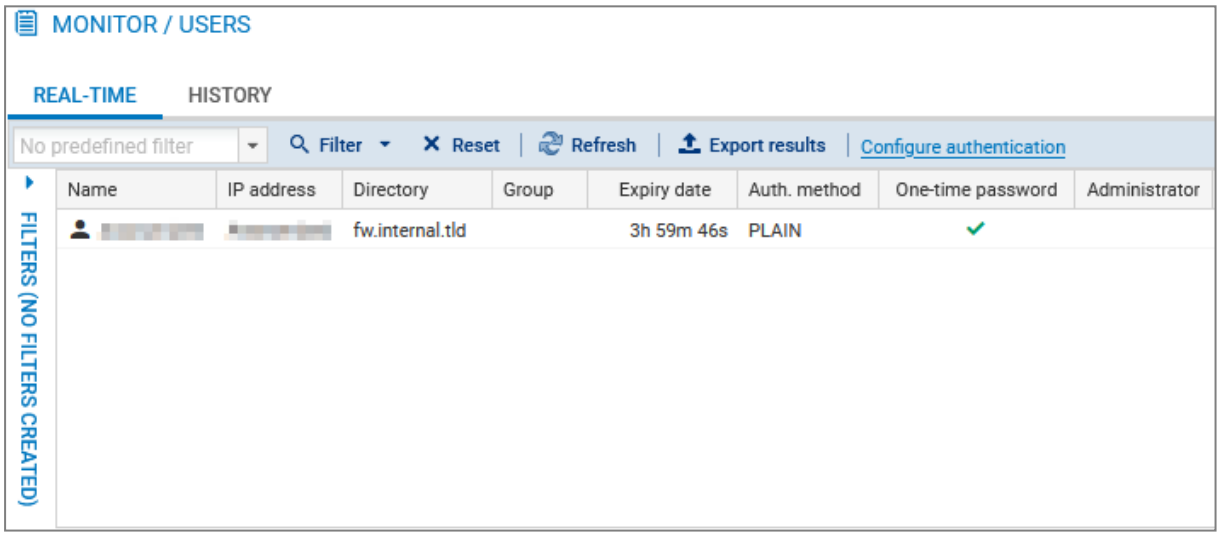
Superviser l'utilisation de la solution TOTP par les utilisateurs

Ce chapitre explique comment superviser dans l'interface Web d'administration du firewall SNS l'utilisation de la solution TOTP par les utilisateurs.

Dans la supervision du firewall SNS

La supervision permet de visionner en temps réel les utilisateurs actuellement authentifiés et de savoir s'ils ont utilisé un code TOTP. Un graphique historique est également disponible représentant la répartition des authentifications sur le firewall SNS selon leur type (dont TOTP).

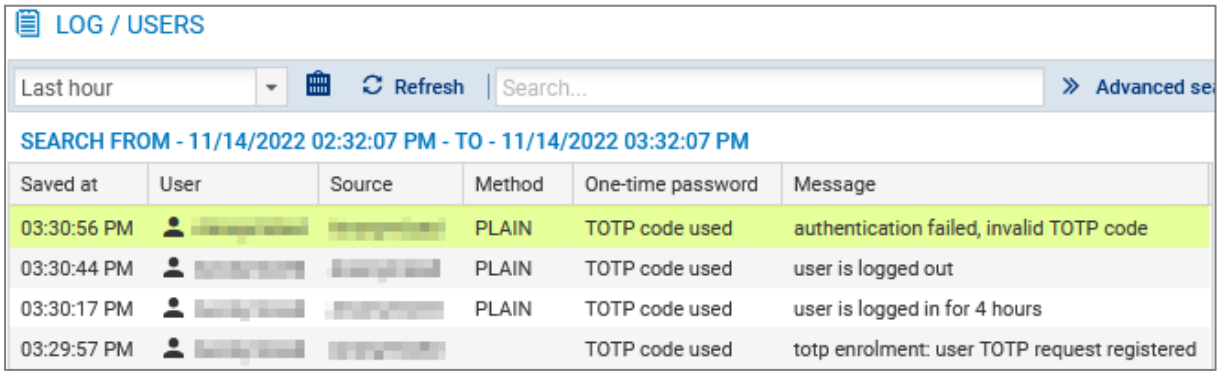
1. Rendez-vous dans **Monitoring > Supervision > Utilisateurs**.
2. Cliquez sur l'onglet des données que vous souhaitez voir.



Dans les journaux d'audit (logs) du firewall SNS

Le journal *Utilisateurs* peut afficher si un code TOTP a été utilisé lors d'une authentification. Un message indique l'état de l'authentification (réussite, échec, déconnexion, etc.). Pour consulter ce journal, rendez-vous dans **Monitoring > Logs - Journaux d'audit > Utilisateurs**.

Certaines informations sont accessibles sous réserve d'activer le droit de consulter les données personnelles. Si vous disposez de ce droit ou d'un code d'accès aux données personnelles, cliquez sur **Logs : accès restreint** dans le bandeau supérieur. Pour plus d'informations, reportez-vous à la note technique Se conformer aux règlements sur les données personnelles.



Résoudre les problèmes

Ce chapitre liste certains problèmes fréquemment rencontrés lors de l'utilisation de la solution TOTP. Si celui que vous rencontrez ne se trouve pas dans ce chapitre, nous vous recommandons de consulter la Base de connaissances Stormshield.

Utiliser l'algorithme de hachage SHA256 ou SHA512 peut générer l'erreur "Mauvais code TOTP"

- *Situation* : Lors de l'enrôlement TOTP d'un utilisateur, l'erreur "Mauvais code TOTP" s'affiche.
- *Cause* : L'*Authenticator* utilisé ne prend pas en compte l'algorithme de hachage SHA256 ou SHA512 spécifié dans la configuration de la méthode d'authentification TOTP sur le firewall SNS.
- *Solution* : Dans **Configuration > Utilisateurs > Authentification**, onglet **Méthodes disponibles**, ligne **TOTP (2FA SNS)**, modifiez l'algorithme de hachage pour SHA1 et réinitialisez la base TOTP. Invitez ensuite vos utilisateurs à réaliser de nouveau la procédure d'enrôlement TOTP. Pour plus d'informations, reportez-vous à l'article Wrong TOTP code - Stormshield Knowledge Base (authentification nécessaire).

S'authentifier avec un code TOTP ou s'enrôler au TOTP n'est pas ou plus possible

- *Situation* : Un ou plusieurs utilisateurs n'arrivent pas ou plus à s'enrôler au TOTP ou à s'authentifier avec un code TOTP.
- *Cause* : L'heure et la date de l'appareil où est installé l'*Authenticator* de l'utilisateur sont dififérentes de celles configurées sur le firewall SNS.
  Si l'utilisateur est déjà enrôlé au TOTP, vous pouvez vérifier la validité des codes TOTP qu'il utilise. Si vous constatez que les codes dans l'*Authenticator* de l'utilisateur apparaissent comme valides mais que la vérification sur le firewall SNS indique le contraire, un problème de synchronisation de la date et de l'heure peut expliquer cette situation.
- *Solutions* :
  - Vérifiez la date et l'heure configurées sur le firewall SNS dans **Configuration > Système > Configuration**, onglet **Configuration générale**, cadre **Paramètres de date et d'heure**. Si un élément n'est pas correct, modifiez-le. Pour rappel, nous recommandons fortement d'activer la synchronisation de temps via NTP,
  - Vérifiez sur l'appareil où est installé l'*Authenticator* de l'utilisateur que la date et l'heure correspondent à celles configurées sur le firewall SNS. Elles doivent être parfaitement synchronisées.

Pour aller plus loin

Des informations complémentaires et réponses à vos éventuelles questions sur l'authentification TOTP sont disponibles dans la Base de connaissances Stormshield (authentification nécessaire).

documentation@stormshield.eu

Les images de ce document ne sont pas contractuelles, l'aspect des produits présentés peut éventuellement varier.

Copyright © Stormshield 2024. Tous droits réservés. Tous les autres produits et sociétés cités dans ce document sont des marques ou des marques déposées de leur détenteur respectif.