



STORMSHIELD



NOTE TECHNIQUE

**STORMSHIELD MULTI-LAYER
COLLABORATIVE SECURITY**

SDS EASY : INTÉGRER UNE PKI SNS DANS UN CLIENT SDS

Produits concernés : SNS 2.4 et supérieures - SDS Suite v9.1.1 et supérieures

Date : Juillet 2016

Référence : mlcs-fr-SDS_Easy_Integration_PKI_SNS_dans_SDS_note_technique



Table des matières

Introduction	4
Prérequis	4
Configurer le Firewall SNS	5
Créer un annuaire LDAP interne	5
Activer le portail captif	5
Créer la CA pour les certificats utilisateurs	6
Modifier les paramètres de la CA	8
Définir la CA comme CA par défaut pour l'annuaire LDAP	9
Créer la CRL	9
Créer le compte de recouvrement	10
Créer le compte de recouvrement dans l'annuaire LDAP interne	10
Créer le certificat du compte de recouvrement	10
Exporter le certificat du compte de recouvrement	11
Créer des comptes et certificats sans enrôlement (méthode recommandée)	13
Configurer le Firewall SNS	13
Créer un utilisateur et son certificat	13
Exporter le certificat et la clé privée d'un utilisateur	15
Mettre à jour et publier la CRL	15
Révoquer un certificat utilisateur et mettre à jour la CRL	16
Configurer le logiciel SDS Suite	17
Créer un nouvel utilisateur dans SDS Suite	17
Ajouter l'annuaire du firewall dans le carnet d'adresses SDS Suite	20
Activer / Désactiver le contrôle de révocation des certificats	23
Importer le certificat du firewall dans les certificats de confiance du poste client	24
Importer la clé de recouvrement dans SDS Suite	26
Utiliser le compte de recouvrement	27
Créer des comptes et certificats par enrôlement (méthode alternative)	29
Configurer le Firewall SNS	29
Activer l'enrôlement et les requêtes de signature de certificats	29
Approuver les requêtes d'enrôlement	30
Mettre à jour et publier la CRL	31
Enrôler d'un utilisateur	32
Demander l'enrôlement	32
Récupérer le certificat	33
Sauvegarder le certificat utilisateur	33
Mettre à jour et publier la CRL	34
Révoquer un certificat utilisateur et mettre à jour la CRL	34
Configurer le logiciel SDS Suite	36
Créer un nouvel utilisateur dans SDS Suite	36
Ajouter l'annuaire du firewall dans le carnet d'adresses SDS Suite	38
Activer / Désactiver le contrôle de révocation des certificats	42
Importer le certificat du firewall dans les certificats de confiance du poste client	43
Importer la clé de recouvrement dans SDS Suite	44
Utiliser le compte de recouvrement	47
Générer un nouveau certificat utilisateur et sa clé privée associée	47
Créer un utilisateur de recouvrement dans SDS Suite	47
Déchiffrer les données de l'utilisateur à l'aide du compte de recouvrement	47



Renouveler la clé de l'utilisateur	47
Chiffrer les données à l'aide du compte utilisateur	48
Cycle de vie des clés	49
Rappels	49
Que faire en cas d'expiration ou de révocation d'un certificat utilisateur?	49
Générer un nouveau certificat et sa clé privée associée	49
Renouveler le certificat et sa clé privée dans SDS Suite	49
Que faire à l'approche de la date d'expiration de la CA ?	50
Configurer les sauvegardes automatiques du firewall	51
Sauvegarder automatiquement la configuration du firewall dans le Cloud Stormshield	51
Activer les sauvegardes automatiques	51
Sélectionner Stormshield Network Cloud Backup	51
Sauvegarder automatiquement la configuration du firewall sur un serveur HTTP/HTTPS personnalisé	52



Introduction

L'objectif de ce document est de décrire la mise en place d'une infrastructure à clés publiques (PKI : Public Key Infrastructure) hébergée sur un Firewall Stormshield Network pour des postes de travail utilisant la solution Stormshield Data Security Suite.

Les firewalls SNS intègrent en effet les fonctions permettant la gestion d'autorités de certification (CA : Certificate Authority), des listes de révocation des certificats (CRL : Certificate Revocation List) associées, du (des) point(s) de distribution de ces CRL (CRLDP : CRL Distribution Point) ainsi que des certificats utilisateurs.

La gestion de la PKI sur le firewall permet ainsi à l'entreprise de s'affranchir de la création d'un ou plusieurs serveurs dédiés à ces fonctions et de l'éventuelle mise en œuvre d'un annuaire LDAP externe ou d'une infrastructure de type Microsoft Active Directory.

Prérequis

- Poste client : SDS Suite v9.1.1 ou supérieure,
- Firewall SNS en version 1.1 ou supérieure (la vérification automatique de CRL depuis SDS Suite ne fonctionne qu'à partir de la v2.4 de SNS).

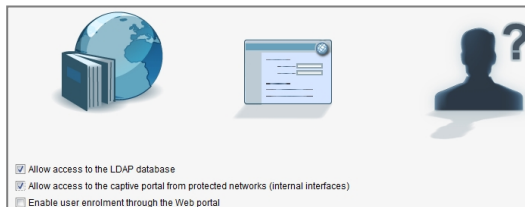


Configurer le Firewall SNS

Créer un annuaire LDAP interne

Si votre firewall dispose déjà d'un annuaire LDAP interne, passez directement au paragraphe [Activation du portail captif](#).

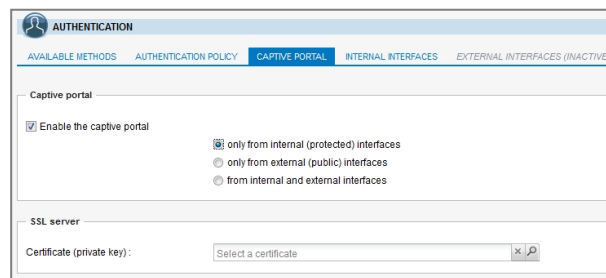
1. Dans le menu **Configuration** > **Configuration de l'annuaire**, cliquez sur l'option **Création d'un annuaire LDAP interne** puis cliquez sur **Suivant**.
2. Renseignez les champs obligatoires :
 - **Organisation**: le nom de votre société (exemple: MyCompany),
 - **Domaine**: le domaine DNS de votre société (exemple: mycompany.org),
 - **Mot de passe**: un mot de passe permettant au firewall de se connecter sur l'annuaire, ou de s'y connecter depuis un navigateur LDAP.
3. Validez en cliquant sur **Suivant**.
4. Cochez ensuite les 2 cases :
 - **Autoriser l'accès à la base LDAP**: cela autorisera, moyennant une règle de filtrage appropriée, les requêtes LDAP depuis les postes utilisateurs équipés de SDS Suite,
 - **Autoriser l'accès au portail captif depuis les réseaux protégés (interfaces internes)**: cette option rend le portail d'authentification accessible depuis le réseau interne. Les requêtes de vérification de CRL à destination du firewall seront ainsi autorisées.



Activer le portail captif

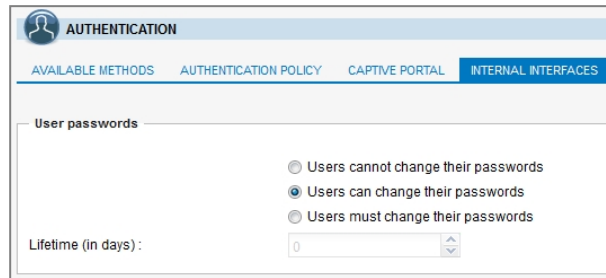
Si vous avez créé votre annuaire interne en suivant la procédure décrite au chapitre [Création de l'annuaire interne](#), le portail captif est déjà activé. Vous pouvez dans ce cas directement passer au paragraphe [Création de la CA pour les certificats utilisateurs](#).

1. Dans l'onglet *Portail captif* du menu **Utilisateurs** > **Authentification**, cochez la case **Activer le portail captif** et sélectionnez **Uniquement depuis les interfaces internes (protégées)**.





2. Dans le volet **Mots de passe des utilisateurs** de l'onglet *Interfaces internes*, sélectionnez l'option **Les utilisateurs peuvent changer leur mot de passe** afin de permettre aux utilisateurs de modifier leur mot de passe depuis le portail captif.



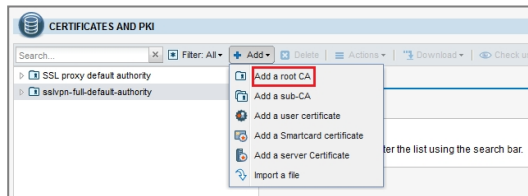
3. Validez en cliquant sur le bouton **Appliquer**. Le portail captif est désormais accessible à l'adresse `https://adresse_ip_firewall/auth/`.

i NOTE

Dans la méthode recommandée par Stormshield, le portail captif n'est utile que pour rendre accessible la CRL aux clients SDS Suite. Dans la méthode alternative, il est nécessaire pour l'enrôlement des utilisateurs.

Créer la CA pour les certificats utilisateurs

1. Dans le menu **Objets > Certificats et PKI**, cliquez sur **Ajouter** et choisissez **Ajouter une autorité racine**.



2. Remplissez les champs de l'assistant de création :

Étape 1 :

- **CN** : saisissez un nom permettant d'identifier votre autorité de certification,
- **Identifiant** : le nom entré dans le champ CN est proposé par défaut,
- **Organisation (O)**. Exemple : le nom de votre entreprise,
- **Unité d'organisation (OU)**. Exemple : le nom du service utilisateur de la CA,
- **Lieu(L)** : ville où est située l'organisation,
- **Etat ou province (ST)** : département ou état où est située l'organisation,
- **Pays (C)** : pays où est située l'organisation.



CN :	<input type="text" value="MyCompanyCA"/>
ID :	<input type="text" value="MyCompanyCA"/>
Select the parent CA (if necessary)	
Parent CA :	<input type="text" value="Select the parent CA"/>
Password for the parent CA :	<input type="password"/>
Certificate authority attributes	
Organization (O) :	<input type="text" value="MyCompany"/>
Organizational Unit (OU) :	<input type="text" value="Users"/>
Locality (L) :	<input type="text" value="Lille"/>
State or province (ST) :	<input type="text" value="North"/>
Country (C) :	<input type="text" value="France"/>

Étape 2 :

- **Mot de passe** : saisissez un mot de passe de 8 caractères minimum afin de protéger l'accès à la clé privée de votre CA. Ce mot de passe vous sera demandé à chaque création ou modification de certificat utilisateur,

! AVERTISSEMENT

Ce mot de passe n'est pas enregistré par le firewall. En cas d'oubli du mot de passe, la CA ne pourra plus être utilisée pour signer les certificats.

- **Taille de clé** : (4096 bits par défaut),
- **Validité** (3650 jours par défaut).

Certificate authority password	
Password (min. 8 char) :	<input type="password" value="....."/>
Confirm password :	<input type="password" value="....."/>
Password strength :	<div style="width: 50%; background-color: #90EE90; display: inline-block;"></div> Good
E-mail address :	<input type="text"/>
Key size (bytes) :	<input type="text" value="4096"/>
The computation of big keys may slow down your appliance.	
Validity (days) :	<input type="text" value="3650"/>

Étape 3 :

Indiquez l'URI du point de distribution des CRL (Listes de Révocation de Certificats). Cette URI sera présente dans chacun des certificats signés par la CA.

La CRL étant destinée à être hébergée sur le firewall, elle prend donc une forme du type :

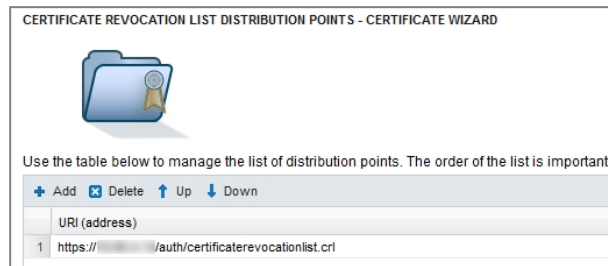
- **https://adresse_ip_firewall/auth/certificaterevocationlist.crl**

ou

- **https://nom_dns_firewall/auth/certificaterevocationlist.crl**

**i REMARQUE**

Le choix d'une URI précisant le nom DNS du firewall implique que ce nom soit renseigné dans un serveur DNS interne accessible depuis les clients SDS Suite.

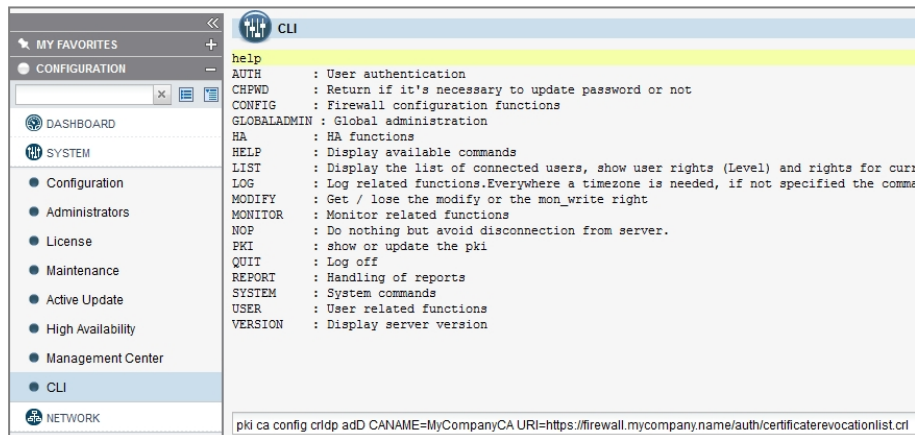


Après création de la CA, il n'est pas possible d'ajouter un CRLDP via l'interface Web d'administration (exemple : ajout d'un CRLDP hébergé dans une autre zone réseau, modification du nom DNS ou de l'alias DNS du firewall). La manipulation des CRLDP n'est alors possible qu'à l'aide des commandes CLI :

```
PKI CA CONFIG CRLDP ADD CANAME=NOM_CA URI=URI
```

```
PKI CA CONFIG CRLDP REMOVE CANAME=NOM_CA ID=NUMBER
```

Exemple :



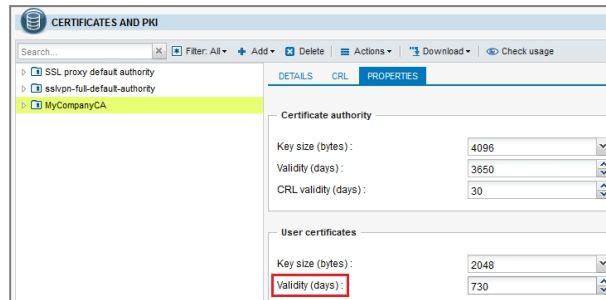
3. Le dernier écran de l'assistant présente un résumé des paramètres de la CA. Validez la création en cliquant sur le bouton **Terminer**.

Modifier les paramètres de la CA

L'assistant de création de CA ne permet pas de modifier la durée de validité des certificats utilisateurs (365 jours par défaut) signés par celle-ci.

Cette opération peut néanmoins être réalisée en éditant les propriétés de la CA après sa création.

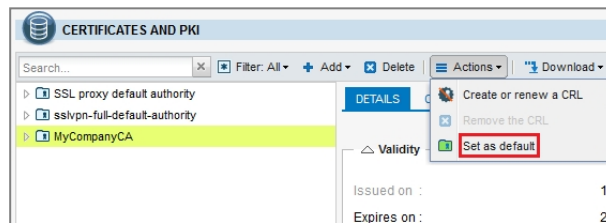
Sélectionnez la CA dans la colonne de gauche, puis cliquez sur l'onglet *Configuration* et modifiez le champ **Validité (jours)** du panneau **Certificats utilisateurs** pour lui affecter la valeur conseillée de 730 jours (2 ans) :




Cette valeur sera ainsi appliquée à chaque lancement de l'assistant de création de certificat utilisateur.

Définir la CA comme CA par défaut pour l'annuaire LDAP

1. Sélectionnez la CA dans le panneau de gauche, puis cliquez sur **Actions** et choisissez **Définir comme défaut**.

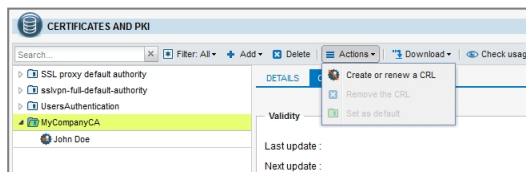


2. Confirmez l'opération en cliquant sur le bouton **Oui**.

La CA est désormais repérée par un symbole de couleur verte  MyCompanyCA indiquant qu'il s'agit de la CA utilisée par défaut pour chiffrer les certificats utilisateurs au sein de l'annuaire LDAP.

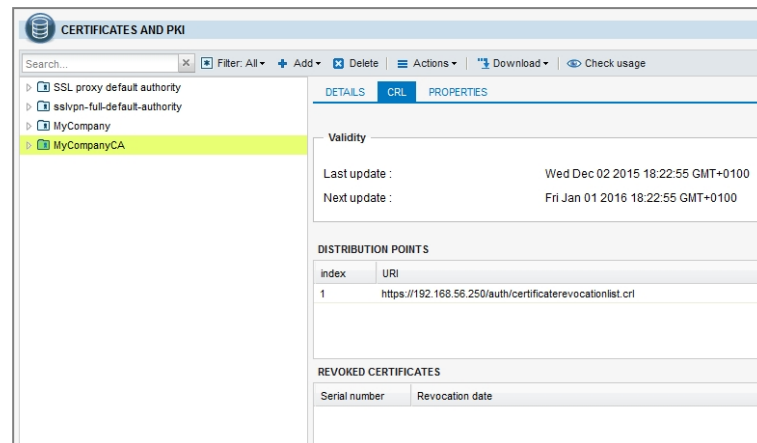
Créer la CRL

1. Dans le menu **Objets > Certificats et PKI**, sélectionnez la CA puis déroulez le menu **Actions** et cliquez sur **Créer ou renouveler une CRL** :



2. Saisissez le mot de passe protégeant la CA, puis terminez l'opération en cliquant sur le bouton **Créer ou renouveler une CRL**.

La CRL est alors initialisée (dates de la dernière et de la prochaine mise à jour). Elle peut être visualisée dans l'onglet **CRL** de la CA :



Créer le compte de recouvrement

Le compte de recouvrement est un compte spécifique destiné à permettre le déchiffrement des données d'un utilisateur dont la clé privée ne serait plus disponible.

La configuration de ce compte est réalisée en quatre étapes (les trois premières sont décrites dans ce chapitre) :

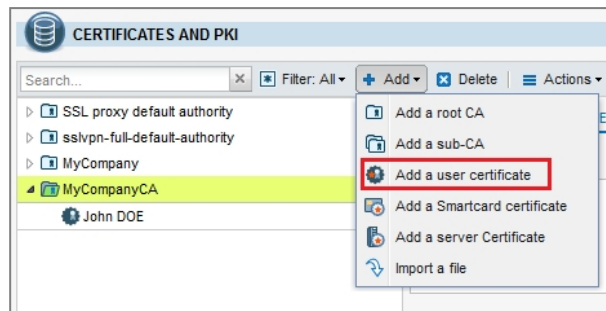
- création du compte de recouvrement dans le firewall,
- création du certificat du compte de recouvrement,
- export de ce certificat (au format *.crt*, sans sa clé privée),
- import de la clé de recouvrement dans SDS Suite. Cette étape est décrite dans le paragraphe [Paramétrage du compte de recouvrement dans SDS Suite](#).

Créer le compte de recouvrement dans l'annuaire LDAP interne

1. Dans le menu **Utilisateurs**, cliquez sur **Ajouter un utilisateur** et saisissez les champs obligatoires de l'onglet *compte* :
 - **Identifiant (login)** : data.recovery dans l'exemple,
 - **Nom** : recovery dans l'exemple,
 - **Prénom** : data dans l'exemple,
 - **E-mail** : data.recovery@mycompany.org dans l'exemple.
2. Cliquez sur le bouton **Appliquer** pour valider cette création.
3. Une fenêtre demandant l'initialisation du mot de passe s'affiche. Renseignez deux fois le mot de passe de l'utilisateur et validez.

Créer le certificat du compte de recouvrement

1. Dans le menu **Objets > Certificats et PKI**, sélectionnez la CA par défaut puis déroulez le menu **Ajouter** et sélectionnez **Ajouter un certificat utilisateur**:



2. Remplissez les champs de l'assistant de création :

Propriétés du certificat utilisateur

- **Nom(CN)** : Data recovery dans l'exemple,
- **Identifiant** : le nom de l'utilisateur est proposé par défaut (Data.recovery dans l'exemple),
- **E-mail** : data.recovery@mycompany.org dans l'exemple.

Options du certificat (écran 1)

Dans le champ **Mot de passe de l'autorité**, indiquez le mot de passe de la CA par défaut.

Options du certificat (écran 2)

- **Validité** : indiquez une durée de validité identique à celle de la CA (3650 jours par défaut),
- Il n'est pas recommandé de cocher la case de publication dans l'annuaire LDAP.

CERTIFICATE OPTIONS - CERTIFICATE WIZARD

Validity (days): 3650

Key size (bytes): 2048

The computation of big keys may slow down your appliance.

Publication in LDAP directory

Publish this certificate in the LDAP directory

Password of the published PKCS#12 container (min. 8 char):

Confirm password:

Password strength:

Résumé

Cliquez sur **Terminer** pour valider la création du certificat.

i NOTE

Le compte de recouvrement ne doit pas être modifié. En cas de modification, il sera en effet nécessaire de modifier le recouvrement sur l'ensemble des clients SDS Suite.

Exporter le certificat du compte de recouvrement

1. Sélectionnez le certificat du compte de recouvrement puis déroulez le menu **Téléchargement** et sélectionnez **Certificat au format DER**.



2. Renseignez puis confirmez un mot de passe pour protéger le certificat et cliquez sur **Télécharger le certificat**. Enregistrez le sur votre station d'administration et/ou sur un média amovible afin de pouvoir l'importer sur le poste client.



Créer des comptes et certificats sans enrôlement (méthode recommandée)

Ce chapitre présente la méthode recommandée par Stormshield et détaille les étapes suivantes :

- création d'un annuaire LDAP interne,
- création et gestion de la CA,
- ajout ou suppression des certificats utilisateurs,
- publication des nouveaux certificats dans l'annuaire LDAP,
- mises à jour de CRL,
- création d'un utilisateur dans le client Stormshield Data Security,
- déclaration de l'annuaire LDAP du firewall dans le carnet d'adresses de l'utilisateur SNS.

Configurer le Firewall SNS

Créer un utilisateur et son certificat

Créer un utilisateur

1. Dans le menu **Utilisateurs**, cliquez sur **Ajouter un utilisateur** et saisissez les champs obligatoires de l'onglet *compte* :
 - **Identifiant (login)**
 - **Nom**
 - **Prénom**
 - **E-mail** (nécessaire pour la création du certificat de l'utilisateur)

ACCOUNT	CERTIFICATE	MEMBER OF THESE GROUPS
ID (login) :	<input type="text" value="john.doe"/>	
Last name :	<input type="text" value="Doe"/>	
First name :	<input type="text" value="John"/>	
E-mail address :	<input type="text" value="john.doe@mycompany.com"/>	
Phone number :	<input type="text"/>	
Description :	<input type="text"/>	

2. Cliquez sur le bouton **Appliquer** pour valider cette création.
3. Une fenêtre demandant l'initialisation du mot de passe s'affiche. Renseignez deux fois le mot de passe de l'utilisateur et validez :

Authentication password

Password :

Confirm password :

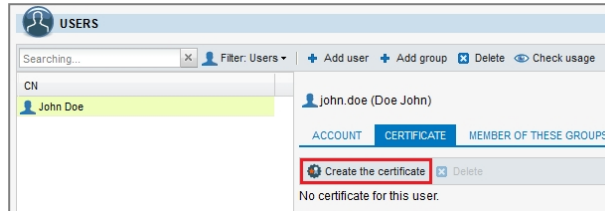
Password strength: Good



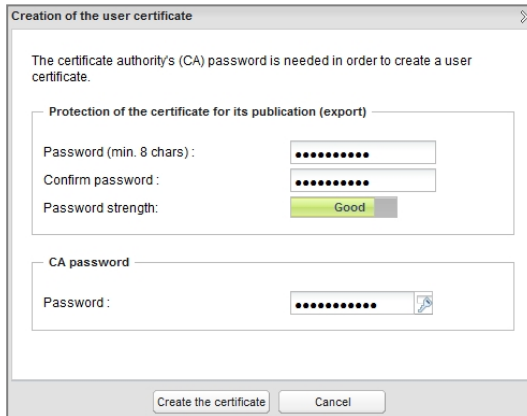
4. Fournissez son identifiant et ce mot de passe à l'utilisateur qui pourra par la suite le modifier depuis le portail d'authentification.

Créer le certificat de l'utilisateur et le publier dans l'annuaire

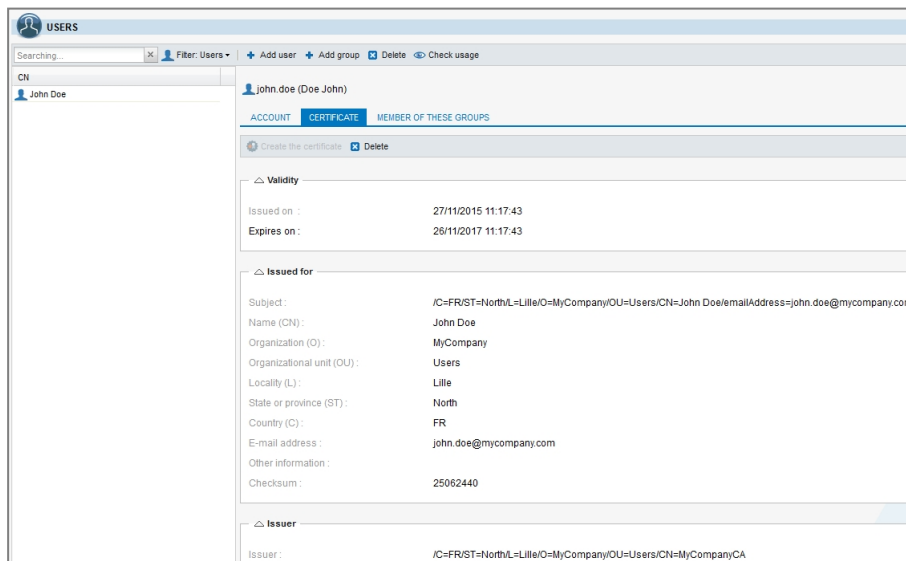
1. Sélectionnez le compte utilisateur précédemment créé et cliquez sur **Créer le certificat** (onglet *Certificat*).



2. Indiquez un mot de passe destiné à protéger le certificat. Ce mot de passe est totalement distinct du mot de passe utilisateur. Il sera demandé lors de l'export du certificat. Saisissez ensuite le mot de passe de la CA puis cliquez sur le bouton **Créer le certificat** :



Le certificat est automatiquement publié dans l'annuaire LDAP ; ses détails peuvent être visualisés dans l'onglet *Certificat* de l'utilisateur :

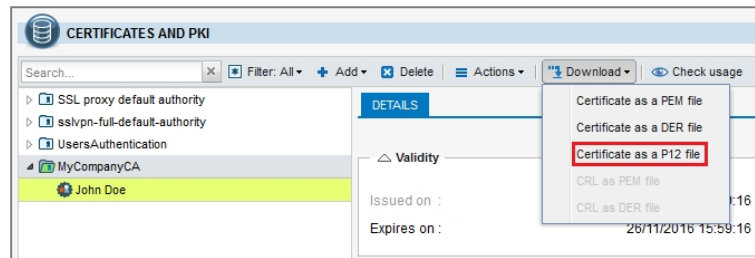


**i** NOTE

La création du certificat au sein de l'annuaire LDAP s'accompagne automatiquement de la création de la clé privée de l'utilisateur.

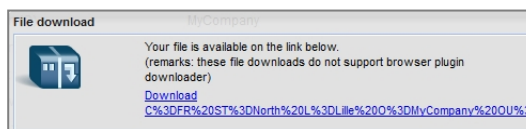
Exporter le certificat et la clé privée d'un utilisateur

1. Dans le menu **Objets > Certificats et PKI**, sélectionnez le certificat à exporter, puis déroulez le menu **Téléchargement** et choisissez **Certificat au format P12** :



2. Saisissez le mot de passe protégeant le certificat (mot de passe initialisé lors de la création du certificat) et validez en cliquant sur le bouton **Télécharger le certificat** :

3. Cliquez sur le lien hypertexte et enregistrez le fichier (extension ".p12") sur votre poste d'administration :

**i** IMPORTANT

Ce fichier au format PKCS#12 est un fichier chiffré contenant le certificat de l'utilisateur et sa clé privée. Il doit donc impérativement lui être transmis de manière sécurisée.

Mettre à jour et publier la CRL

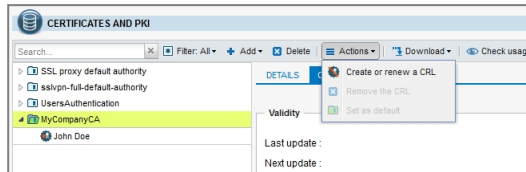
L'interrogation de la CRL est un point critique dans l'utilisation d'un client Stormshield Data Security : en effet, les opérations cryptographiques peuvent être compromises si la CRL n'est pas à jour. Cette mise à jour est réalisée automatiquement lors de la révocation d'un certificat depuis le menu **Certificats et PKI** si la case **Créer la CRL après révocation est cochée** (cette opération est décrite dans le paragraphe **Révocation d'un certificat utilisateur et mise à jour de la CRL**).

En revanche, la mise à jour de la CRL doit être réalisée manuellement dans les cas suivants :

- suppression d'un certificat utilisateur depuis le menu **Utilisateurs**,
- date de validité de la CRL échuë ou proche de son échéance.



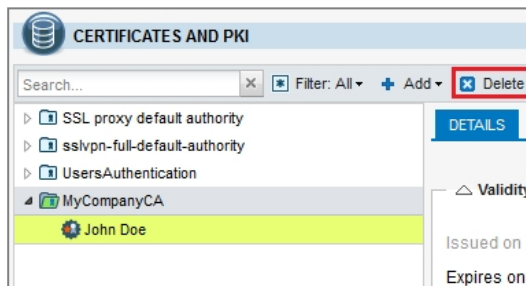
Pour mettre à jour manuellement la CRL, sélectionnez la CA dans le menu **Objets > Certificats et PKI** puis déroulez le menu **Actions** et cliquez sur le menu **Créer ou renouveler une CRL** :



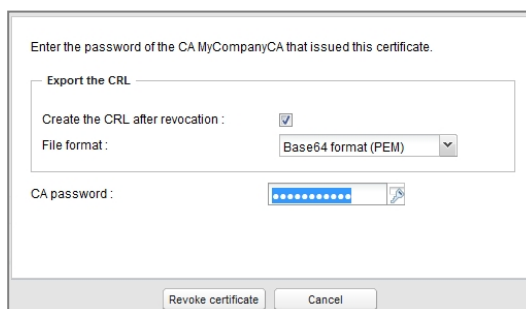
La date de validité de la CRL est alors modifiée en conséquence. La CRL étant stockée directement sur le firewall, la mise à jour de celle-ci est automatiquement prise en compte sans nécessité d'une republication manuelle.

Révoquer un certificat utilisateur et mettre à jour la CRL

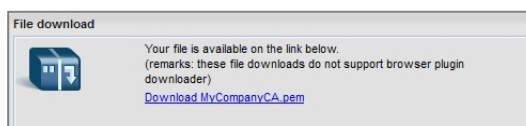
1. Depuis le menu **Objets > Certificats et PKI**, sélectionnez le certificat utilisateur à révoquer, puis cliquez sur le bouton **Supprimer**.



2. Vérifiez que la case **Créer la CRL après révocation** est bien cochée : cela permettra la mise à jour automatique de la CRL en fin de processus de révocation du certificat.
3. Indiquez le mot de passe de la CA et validez la suppression en cliquant sur le bouton **Révoquer le certificat** :

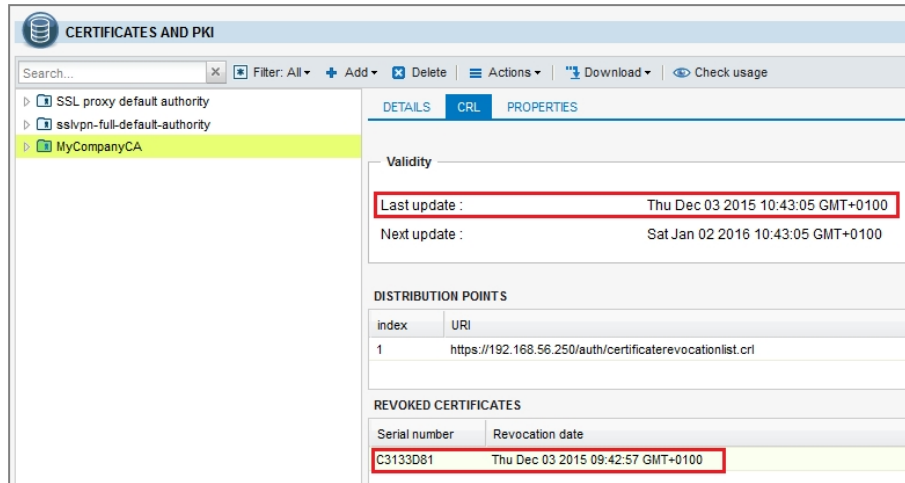


4. Renseignez à nouveau le mot de passe de la CA pour la mise à jour de la CRL et cliquez sur le bouton **Créer ou renouveler une CRL**.
5. Vous pouvez alors télécharger la CRL mise à jour afin de la publier sur les éventuels points de distributions autres que le firewall :



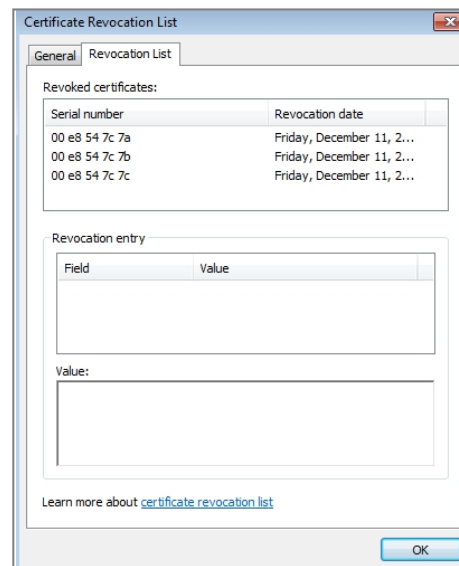
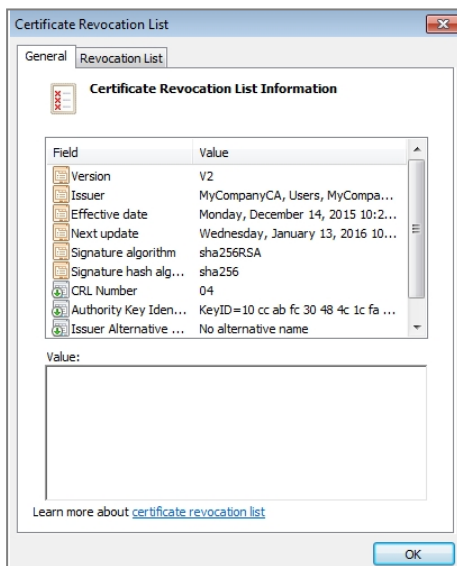


Les informations de la CRL reflètent immédiatement la révocation du certificat :




La CRL étant stockée directement sur le firewall, la mise à jour de celle-ci est automatiquement prise en compte sans nécessité d'une republication manuelle.

La CRL récupérée depuis le CRDLP (https://firewall_dns_name/auth/certificaterevocationlist.crl ou https://adresse_ip_firewall/auth/certificaterevocationlist.crl) permet de vérifier que la révocation du certificat a bien été prise en compte :



Configurer le logiciel SDS Suite

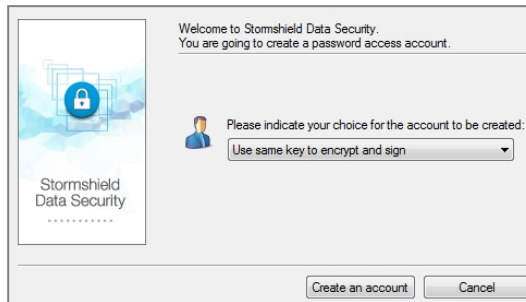
Créer un nouvel utilisateur dans SDS Suite

1. Faites un clic droit sur l'icône  présente dans la barre des tâches du poste utilisateur et sélectionnez le menu **Nouvel utilisateur** :





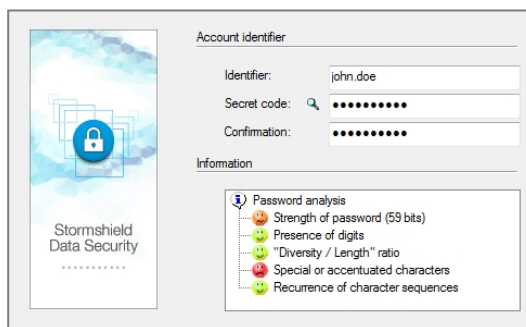
2. Choisissez l'option **Utiliser une seule clé pour chiffrer et signer** puis cliquez sur le bouton **Créer un compte** :



3. Identifiant du compte

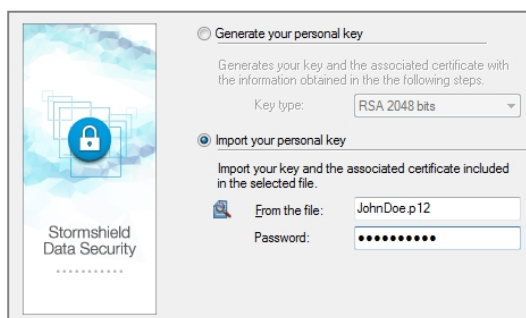
Renseignez les trois champs obligatoires :

- **Identifiant** : cet identifiant de connexion doit être identique à celui renseigné dans l'annuaire LDAP du firewall (john.doe dans l'exemple).
- **Code secret** : l'utilisateur saisit un mot de passe strictement personnel destiné à protéger son compte SDS Suite. Ce mot de passe n'est aucunement lié à celui protégeant sa clé privée. Des critères de complexité de ce mot de passe sont affichés dans la fenêtre **Informations**.
- **Confirmation** : l'utilisateur confirme le mot de passe choisi.



4. Clé personnelle

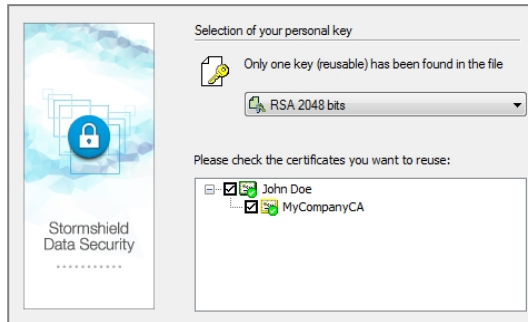
Choisissez l'option **Importer votre clé personnelle** et sélectionnez le fichier PKCS#12 (extension ".p12") contenant le certificat et la clé privée de l'utilisateur. Saisissez le mot de passe protégeant ce certificat et validez en cliquant sur **Suivant** :



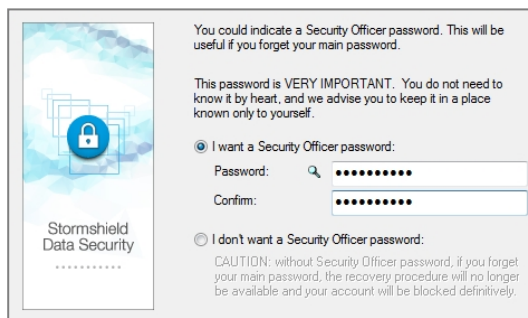


i NOTE

Le certificat de la CA est également proposé à l'import. Veillez à ce que les cases des certificats utilisateur et CA soient cochées.



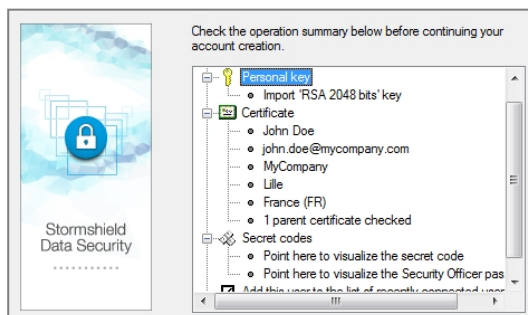
5. Validez en cliquant sur **Suivant**.
6. L'assistant propose alors la création d'un mot de passe de secours permettant de retrouver le mot de passe du compte utilisateur en cas de perte. Il est fortement recommandé de créer ce mot de passe de secours. Renseignez et confirmez ce mot de passe. Validez en cliquant sur **Suivant** :



! IMPORTANT

Sans mot de passe de secours, il est impossible de retrouver le mot de passe de l'utilisateur en cas de perte. Il est donc très fortement recommandé de créer un mot de passe de secours.

7. Validez l'écran proposant un résumé complet du compte utilisateur en cliquant sur **Terminer**.



8. La création de l'annuaire local est lancée automatiquement et le dernier écran propose un résumé des opérations réalisées:



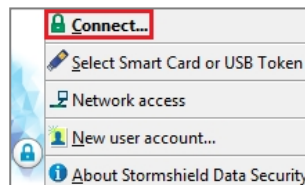
9. Cliquez sur **Quitter** pour fermer l'assistant.

Ajouter l'annuaire du firewall dans le carnet d'adresses SDS Suite

Le référencement d'un annuaire LDAP dans le carnet d'adresses local permet d'indiquer à SDS Suite que cet annuaire doit être systématiquement interrogé lors de l'envoi ou de la réception d'un e-mail.

Connecter l'utilisateur à SDS Suite

1. Faites un clic droit sur l'icône SDS Suite présente dans la barre des tâches et sélectionnez le menu **Connecter...**



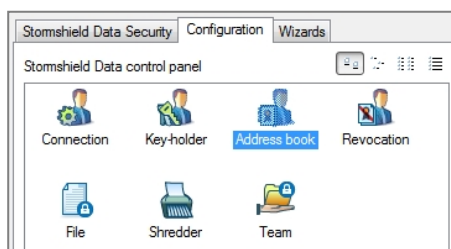
2. Renseignez le mot de passe de l'utilisateur puis cliquez sur le bouton **Valider**.

Ajouter l'annuaire LDAP du firewall

1. Après connexion, effectuez de nouveau un clic droit sur l'icône SDS Suite de la barre des tâches et sélectionnez le menu **Propriétés** :

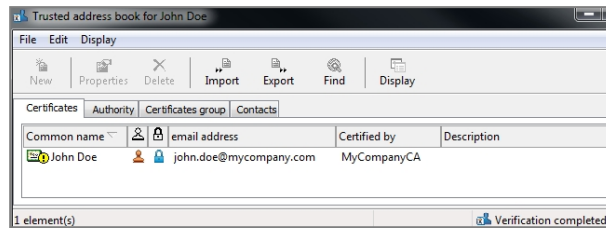


2. Dans l'onglet *Configuration* de la fenêtre des propriétés de l'utilisateur, double-cliquez sur l'icône **Annuaire** :






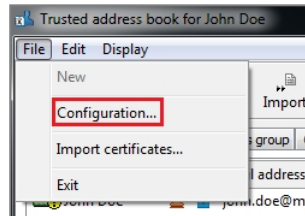
Le contenu de l'annuaire local de l'utilisateur s'affiche :



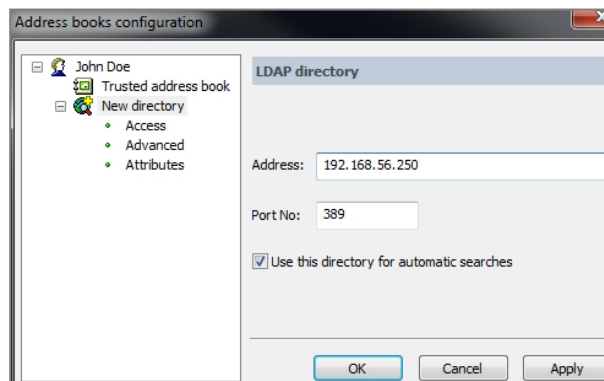
i NOTE

Dans l'exemple, le symbole  indique que le certificat listé est à utiliser avec précaution, car la liste de révocation (CRL) n'a pas pu être consultée.

3. Déroulez le menu **Fichier** et sélectionnez **Configuration...** :



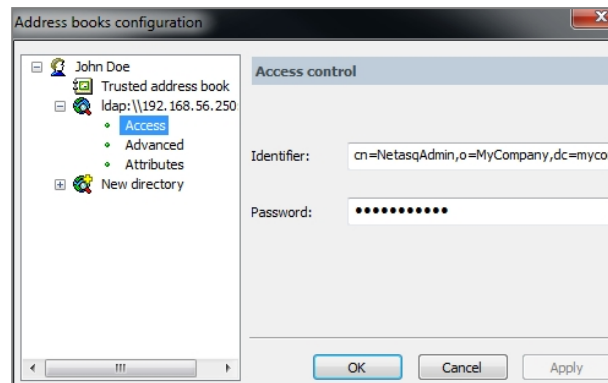
4. Dans la fenêtre de configuration des annuaires, cliquez sur **Ajouter un annuaire** et renseignez l'adresse IP (192.168.56.250 dans l'exemple) ou le nom DNS du firewall (ce nom doit alors être renseigné dans un serveur DNS joignable par les clients SDS Suite). Laissez le port proposé par défaut (LDAP /389) et cochez la case **Utiliser cet annuaire pour les recherches automatiques** :



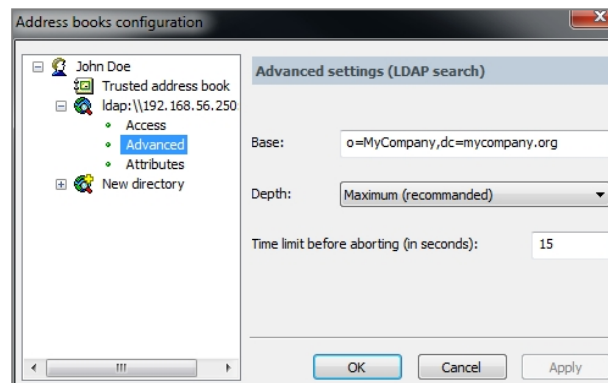
5. Cliquez sur **Appliquer**.

6. Dans les propriétés de l'annuaire LDAP ajouté, sélectionnez **Accès** et remplissez les deux champs :

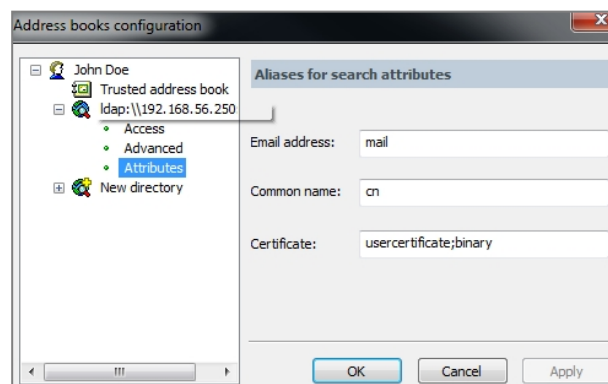
- **Identifiant** : Distinguished Name (DN) de l'utilisateur autorisé à parcourir l'annuaire (NetasqAdmin). Il prend la forme suivante : cn=NetasqAdmin, o=Organisation, dc=Domaine (exemple : cn=NetasqAdmin, o=MyCompany, dc=mycompany.org)
- **Mot de passe** : renseignez le mot de passe utilisé lors de la création de l'annuaire LDAP sur le firewall.



7. Dans les propriétés de l'annuaire LDAP, sélectionnez **Avancé** et remplissez le champ **Base** correspondant à la base DN du stockage des certificats sur le firewall. Il prend la forme suivante : `o=Organisation,dc=Domaine` (exemple : `o=MyCompany,dc=mycompany.org`).



8. Dans les propriétés de l'annuaire LDAP, sélectionnez **Attributs** et vérifiez que les champs ont les valeurs suivantes :
- **Email address** : `mail`,
 - **Common name** : `cn`,
 - **Certificate** : `usercertificate;binary`.



9. Cliquez sur **OK** pour valider la création de l'annuaire LDAP dans le carnet d'adresses de l'utilisateur.



Ajouter automatiquement les certificats des correspondants e-mail

Il est possible de paramétrer l'ajout automatique des certificats de correspondants présents dans l'annuaire LDAP à l'annuaire local SDS Suite lorsqu'un e-mail leur est envoyé.

Il est nécessaire pour cela de modifier le fichier de configuration *sbox.ini* de SDS Suite comme suit :

1. Editez le fichier *sbox.ini* présent dans le répertoire Kernel du chemin d'installation de SDS Suite (C:\Program Files\Arkoon\Security BOX\Kernel\ dans l'exemple).

```
SBox.ini - Bloc-notes
Fichier Edition Format Affichage ?
DefaultPath1=C:\ProgramData\Arkoon\Security BOX\Users
RootPath1=C:\ProgramData\Arkoon\Security BOX\Users
ShowBrowse=1
ShowLastUsers=5
[CRL]
CRLDatabaseModel=C:\ProgramData\Arkoon\Security BOX\Users\default\default.bcr1
TmpCRLPath=C:\ProgramData\Arkoon\Security BOX\CRL
DeleteTmpCRL=1
LDAPTimeOut=60
[TEAM]
ExcludedPath=<%APPDATA%>
[SBox.NewUserWizardExGP2]
AllowNewUser=1
Pkcs12Import=1
```

2. Créez une section [Mail], ajoutez le champ "SilentImportTrustedLdapCert" et affectez-lui la valeur "1" :

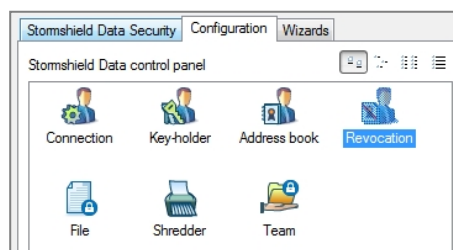
```
[SBox.NewUserWizardExKS1]
AllowNewUser=1
AllowNewUserCipher=1
AllowNewUserSign=1
Pkcs12Import=1
[SBox.NewUserWizardExKS2]
AllowNewUser=1
Pkcs12Import=1
[SBox.NewUserWizardExGP1]
AllowNewUser=1
AllowNewUserCipher=1
AllowNewUserSign=1
Pkcs12Import=1
InternalKeys=0
ExportKeys=1
KeepCardObjects=1
[Mail]
SilentImportTrustedLdapCert=1
```

3. Enregistrez les modifications et fermez le fichier.

Activer / Désactiver le contrôle de révocation des certificats

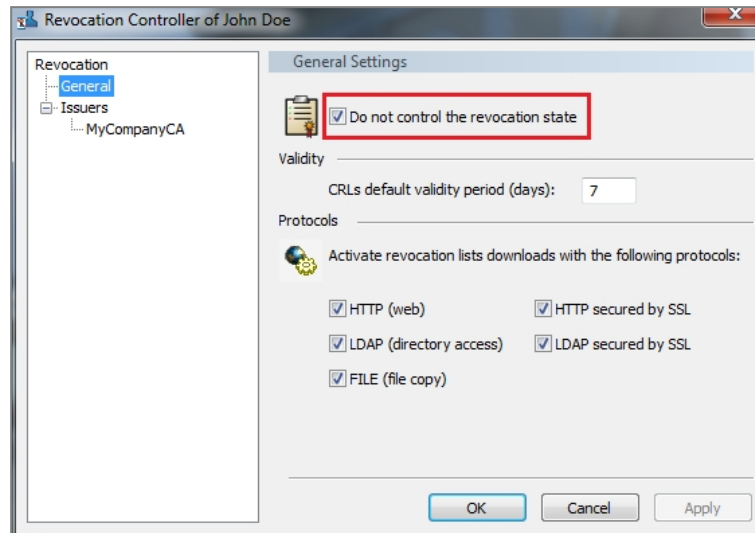
Lorsque la version de firmware du firewall Stormshield Network hébergeant la CRL est inférieure à 2.4, il est nécessaire de désactiver le contrôle de révocation des certificats du client SDS.

1. Faites un clic droit sur l'icône SDS Suite présente dans la barre des tâches et sélectionnez le menu **Propriétés**.
2. Dans l'onglet *Configuration*, double-cliquez sur le menu **Révocation**:





3. Cochez la case "Ne pas contrôler la révocation des certificats" située dans le menu **Révocation** > **Général**. Appliquez et validez:

**i NOTE**

Pensez à décocher cette case lorsque le firewall Stormshield Network hébergeant la CRL dispose d'une version de firmware au moins égale à la version 2.4.

Importer le certificat du firewall dans les certificats de confiance du poste client

Lorsque le client SDS Suite effectue un contrôle automatique de l'état de la CRL, il se connecte en HTTPS au CRLDP hébergé sur le firewall SNS, et c'est alors le certificat du firewall qui est présenté. Pour le bon déroulement de cette opération de contrôle, il est donc nécessaire d'importer le certificat du firewall dans la console de gestion des certificats de confiance de Windows.

Récupérer le certificat du firewall

Depuis Internet Explorer

1. Dans la barre d'adresses du navigateur, saisissez l'adresse de connexion à l'interface d'administration du firewall : **https://adresse_ip_firewall/admin** ou **https://nom_dns_firewall/admin**.

i RAPPEL

Le choix d'une URI précisant le nom DNS du firewall implique que ce nom soit renseigné dans un serveur DNS interne accessible depuis les clients SDS Suite.

2. Lorsque la page d'authentification sur le firewall est affichée, cliquez sur la zone du rapport de sécurité située à droite de la barre d'adresses du navigateur.
3. Dans la fenêtre de rapport de sécurité, cliquez sur **Afficher les certificats**
4. Dans l'onglet *Détails*, cliquez sur le bouton **Copier dans un fichier...**
5. Cliquez sur **Suivant**,
6. Laissez le format proposé par défaut : **X.509 binaire encodé DER (.cer)**, puis cliquez sur **Suivant**.
7. Cliquez sur **Parcourir** pour sélectionner un emplacement de sauvegarde, puis saisissez un nom pour le fichier et cliquez sur **Enregistrer**.




8. Cliquez sur **Suivant** puis sur **Terminer**.
9. Validez le message "**L'exportation s'est effectuée correctement**".
10. Fermez la fenêtre présentant le détail du certificat en cliquant sur **OK**.

Depuis Mozilla Firefox

1. Dans la barre d'adresses du navigateur, saisissez l'adresse de connexion à l'interface d'administration du firewall : **https://adresse_ip_firewall/admin** ou **https://nom_dns_firewall/admin**.

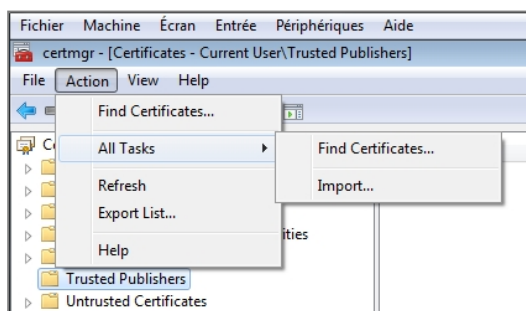
i RAPPEL

Le choix d'une URI précisant le nom DNS du firewall implique que ce nom soit renseigné dans un serveur DNS interne accessible depuis les clients SDS Suite.

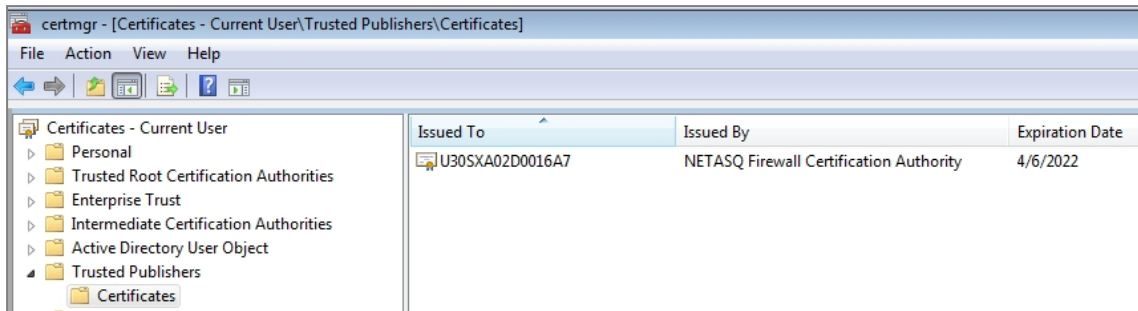
2. Lorsque la page d'authentification sur le firewall est affichée, cliquez sur la zone du rapport de sécurité (cadenas) située à gauche de la barre d'adresses du navigateur.
3. Dans la fenêtre de rapport de sécurité, cliquez sur le signe ">" puis sur le bouton **Plus d'informations**.
4. Cliquez sur le bouton **Afficher le certificat**.
5. Dans l'onglet *Détails*, cliquez sur le bouton **Exporter...**
6. Sélectionnez un emplacement de sauvegarde, puis saisissez un nom pour le fichier (laissez l'extension ".crt" proposée par défaut) et cliquez sur **Enregistrer**.
7. Fermez la fenêtre présentant le détail du certificat en cliquant sur **OK**.
8. Fermez la fenêtre de rapport de sécurité à l'aide du bouton 

Importer ce certificat dans la console de gestion des certificats de confiance du poste client

1. Dans le menu Démarrer > Exécuter de Windows, saisissez certmgr.msc puis validez en cliquant sur **OK** pour lancer la console de gestion des certificats.
2. Dans le menu de gauche de la console, sélectionnez le magasin **Editeurs approuvés > Certificats**.
3. Cliquez sur le menu **Action > Toutes les tâches > Importer...**



4. Sélectionnez le certificat du firewall, précédemment exporté via votre navigateur Internet, puis cliquez sur **Suivant**.
5. Confirmez le choix du magasin de certificat (**Editeurs approuvés**) en cliquant sur **Suivant**.
6. Validez l'import en cliquant sur le bouton **Terminer**.
7. Un message vous confirme que l'import s'est correctement déroulé. Le certificat de votre firewall apparaît désormais dans le magasin. Il est identifiable grâce au numéro de série de votre firewall (ou à son nom DNS s'il en possède un).

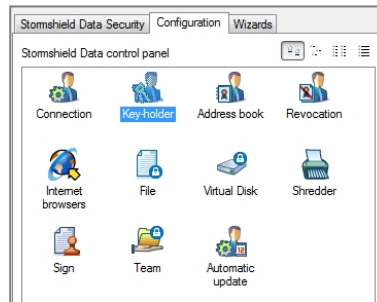


Importer la clé de recouvrement dans SDS Suite

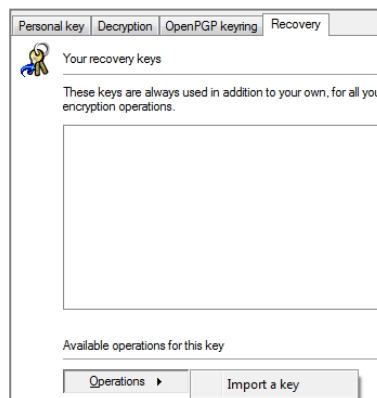
! IMPORTANT

Il est nécessaire d'importer la clé de recouvrement dans le client SDS Suite avant tout chiffrement de données. En effet, les données chiffrées avant l'installation de la clé de recouvrement ne pourront pas être récupérées en cas de perte de sa clé privée par l'utilisateur.

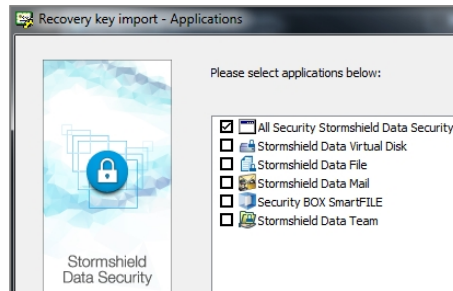
1. Faites un clic droit sur l'icône SDS Suite présente dans la barre des tâches et sélectionnez le menu **Propriétés**.
2. Dans l'onglet *Configuration*, double-cliquez sur le menu **Porte clé**.



3. Sélectionnez l'onglet *Recouvrement* et cliquez sur le bouton **Importer une clé**.

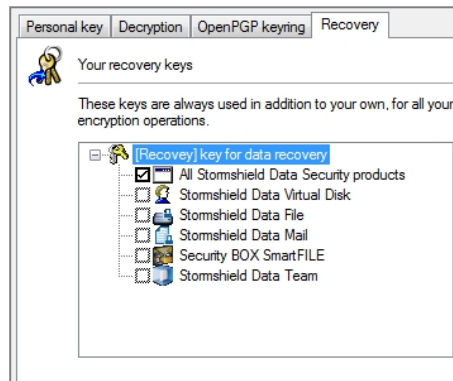


4. Sélectionnez le certificat du compte de recouvrement.
5. Indiquez les applications pour lesquelles vous souhaitez utiliser cette clé de recouvrement en cochant la case **Tous les produits Stormshield Data Security** :



6. Cliquez sur **Terminer** pour valider l'opération.

La clé de recouvrement est désormais déclarée pour le compte utilisateur SDS Suite :



Utiliser le compte de recouvrement

En cas de perte de la clé privée d'un utilisateur, le compte de recouvrement peut permettre à l'utilisateur de déchiffrer ses données.

Générer un nouveau certificat utilisateur et sa clé privée associée

Supprimez l'ancien certificat de l'utilisateur et mettez à jour la CRL (cf. [Révocation d'un certificat utilisateur et mise à jour de la CRL](#)).

Dans une configuration n'utilisant pas l'enrôlement :

1. Générez un nouveau certificat et sa clé.
2. Exportez le certificat et sa clé au format PKCS#12 (cf. [Export du certificat et de la clé privée d'un utilisateur](#)).

Dans une configuration utilisant l'enrôlement :

1. L'utilisateur dépose une nouvelle demande de certificat via le portail d'authentification (menu **Certificats** > **Demandez votre certificat**, accessible après authentification sur le portail).
2. L'administrateur valide cette demande dans le menu **Utilisateur** > **Enrôlement** (cf. [Validation d'une requête de création d'utilisateur et du certificat associé](#)).
3. L'utilisateur récupère son certificat et sa clé depuis le portail d'authentification.
4. Il les sauvegarde au format PKCS#12 et stocke ce fichier dans un emplacement sécurisé.



Créer un utilisateur de recouvrement dans SDS Suite

Sur le poste client, suivez la méthode décrite dans le chapitre [Création d'un nouvel utilisateur SDS](#) pour créer le compte de recouvrement dans SDS Suite.

Déchiffrer les données de l'utilisateur à l'aide du compte de recouvrement

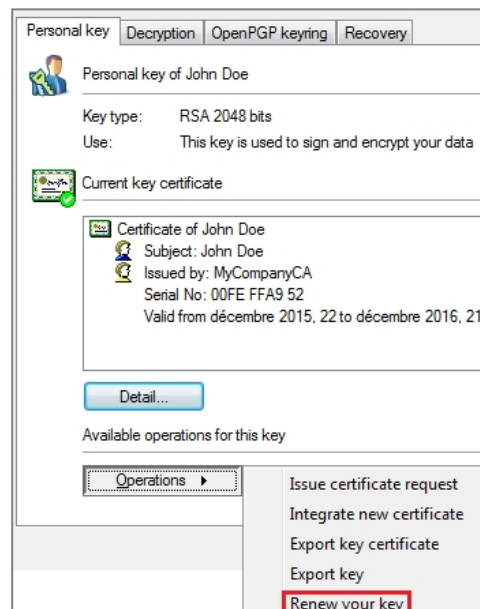
La connexion au logiciel SDS Suite à l'aide du compte de recouvrement permet alors de déchiffrer manuellement les données de l'utilisateur.

i NOTE

Cette opération de déchiffrement doit être réalisée avec l'ensemble des modules SDS Suite ayant été utilisés par l'utilisateur pour chiffrer ses données (File, Mail, ...).

Renouveler la clé de l'utilisateur

1. L'utilisateur se connecte au client SDS Suite à l'aide de son compte personnel.
2. Dans l'onglet *Clé personnelle* du menu **Porte Clé** du client SDS Suite, il déroule le menu **Opérations** et sélectionne **Renouveler votre clé**.



3. Il choisit ensuite l'option **Importer votre clé personnelle**, sélectionne le fichier PKCS#12 contenant sa nouvelle clé de l'utilisateur et saisit le mot de passe protégeant le fichier.

Chiffrer les données à l'aide du compte utilisateur

L'utilisateur peut à nouveau chiffrer ses données.

i NOTE

Cette opération de chiffrement doit être réalisée avec l'ensemble des modules SDS Suite ayant été utilisés par l'utilisateur pour chiffrer ses données (File, Mail, ...).



Créer des comptes et certificats par enrôlement (méthode alternative)

Ce chapitre aborde une méthode alternative autorisant l'enrôlement des utilisateurs via le portail d'authentification. Cette solution présente néanmoins l'inconvénient majeur de ne proposer aucune solution de séquestre des clés privées des utilisateurs sur le firewall.

En cas de perte de sa clé privée par un utilisateur, il est alors impossible de récupérer celle-ci et les données chiffrées de l'utilisateur sont ainsi inaccessibles. Seule l'utilisation d'un compte de recouvrement peut permettre de récupérer des données chiffrées par un utilisateur dont la clé privée serait perdue. Cette méthode impose également aux utilisateurs de gérer le stockage de leur clé privée dans un emplacement sécurisé.

NOTE

L'enrôlement ne fonctionnant pas avec un annuaire de type Microsoft Active Directory, seule l'utilisation d'un annuaire LDAP interne est décrite dans ce document.

Les étapes présentées pour cette méthode sont les suivantes :

- création d'un annuaire LDAP interne,
- activation de l'enrôlement,
- création et gestion de la CA,
- création d'un compte de recouvrement et de son certificat sur le firewall,
- signature des certificats créés après les requêtes des utilisateurs via le portail captif,
- publication des certificats dans l'annuaire LDAP,
- mise à jour de la CRL,
- création d'un utilisateur dans le client Stormshield Data Security,
- déclaration de l'annuaire LDAP du firewall dans le carnet d'adresses de l'utilisateur SDS,
- import de la clé de recouvrement dans SDS Suite.

Configurer le Firewall SNS

Activer l'enrôlement et les requêtes de signature de certificats

1. Dans l'onglet *Interfaces internes* du menu **Utilisateurs** > **Authentification**, déployez le volet **Configuration avancée** et cochez la case **Autoriser l'enrôlement Web des utilisateurs et créer leur certificat**.



AUTHENTICATION

AVAILABLE METHODS | AUTHENTICATION POLICY | CAPTIVE PORTAL | **INTERNAL INTERFACES** | EXTERNAL INTERFACES (INACTIVE)

User passwords

Users cannot change their passwords
 Users can change their passwords
 Users must change their passwords

Lifetime (in days) : 0

Authentication periods allowed

Minimum duration : 15 minute(s)
Maximum duration : 240 minute(s)
For transparent authentication : 240 minute(s)

Advanced properties

Allow access to the .PAC file from internal interfaces

User enrolment

Do not allow user enrolment
 Allow Web enrolment for users
 Allow Web enrolment for users and create their certificates

Notification of a new enrolment : none

2. Validez en cliquant sur le bouton **Appliquer**.

i NOTE

Si vous souhaitez qu'un groupe de destinataires e-mail soit notifié à chaque demande d'enrôlement (champ **Notification d'un nouvel enrôlement**), il est nécessaire de créer ce groupe au préalable dans l'onglet *Destinataires* du menu **Notifications** > **Alertes e-mails**.

Approuver les requêtes d'enrôlement

Chaque requête de création d'utilisateur et de certificat effectuée via le portail d'authentification doit être validée par un administrateur du firewall. L'utilisateur et son certificat sont alors automatiquement publiés dans l'annuaire LDAP interne du firewall.

Valider une requête de création d'utilisateur et de certificat

Le menu **Utilisateurs** > **Enrôlement** affiche les différentes requêtes de création d'utilisateurs et de signature de certificats en attente d'approbation :

	Type	CN User
<input type="checkbox"/>	User	John DOE
<input type="checkbox"/>	Certificate	John DOE

1. Cochez les cases des demandes de création d'utilisateur et de certificat devant être approuvées,
2. Dans le panneau **Configuration avancée**, indiquez le format à utiliser pour créer l'identifiant (login) de l'utilisateur. Pour un format de type *nom.prénom* (minuscules exclusivement), choisissez *%f.%l*. L'exemple sous la fenêtre de saisie affiche dynamiquement le format appliqué :



Type	CN User
User	John DOE
Certificate	John DOE

i NOTE

Il est possible d'alerter l'utilisateur de l'approbation ou du rejet de ses demandes en cochant la ou les case(s) présentes dans le panneau **Configuration avancée**:
Envoyer un e-mail à l'utilisateur : lors de l'approbation de sa requête d'enrôlement
Envoyer un e-mail à l'utilisateur : lors de l'approbation de sa requête de certificat

3. Cliquez sur **Approuver** :

4. Cliquez ensuite sur le bouton **Appliquer** du bas de la fenêtre puis sur le bouton **Sauvegarder** du message de confirmation,
5. Saisissez le mot de passe de la CA pour signer le certificat utilisateur,
6. L'utilisateur et son certificat sont automatiquement publiés dans l'annuaire LDAP du firewall.

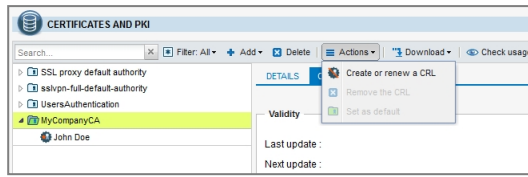
Mettre à jour et publier la CRL

L'interrogation de la CRL est un point critique dans l'utilisation d'un client Stormshield Data Security : en effet, les opérations cryptographiques peuvent être compromises si la CRL n'est pas à jour. Cette mise à jour est réalisée automatiquement lors de la révocation d'un certificat depuis le menu **Certificats et PKI** si la case **Créer la CRL après révocation est cochée** (cette opération est décrite dans le paragraphe [Révocation d'un certificat utilisateur et mise à jour de la CRL](#)).

En revanche, la mise à jour de la CRL doit être réalisée manuellement dans les cas suivants :

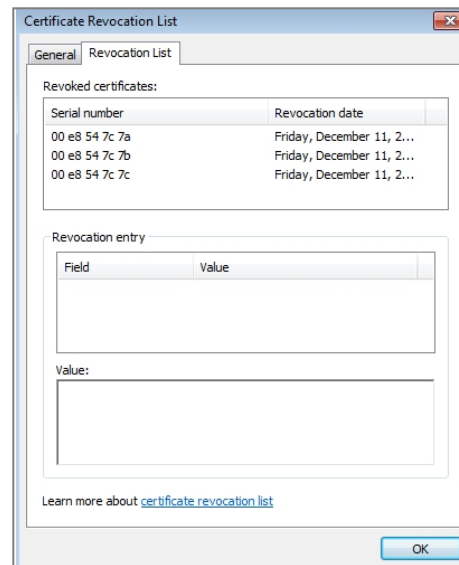
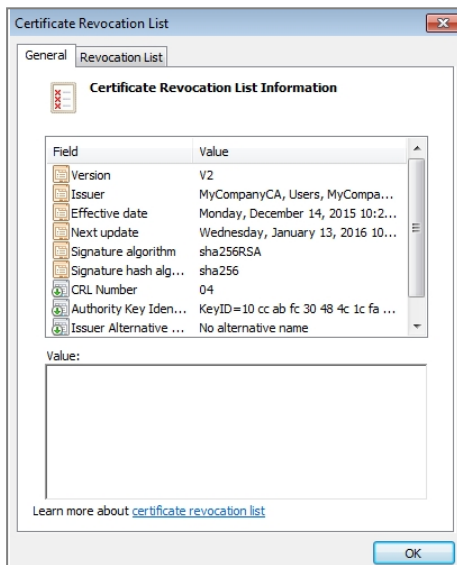
- suppression d'un certificat utilisateur depuis le menu **Utilisateurs**,
- date de validité de la CRL échue ou proche de son échéance.

Pour mettre à jour manuellement la CRL, sélectionnez la CA dans le menu **Objets > Certificats et PKI** puis déroulez le menu **Actions** et cliquez sur le menu **Créer ou renouveler une CRL** :



La date de validité de la CRL est alors modifiée en conséquence. La CRL étant stockée directement sur le firewall, la mise à jour de celle-ci est automatiquement prise en compte sans nécessité d'une republication manuelle.

La CRL récupérée depuis le portail captif (https://firewall_dns_name/auth/ ou https://adresse_ip_firewall/auth puis menu **Certificats** > **Liste de révocation de certificats de votre société**) permet de vérifier que la révocation du certificat a bien été prise en compte :

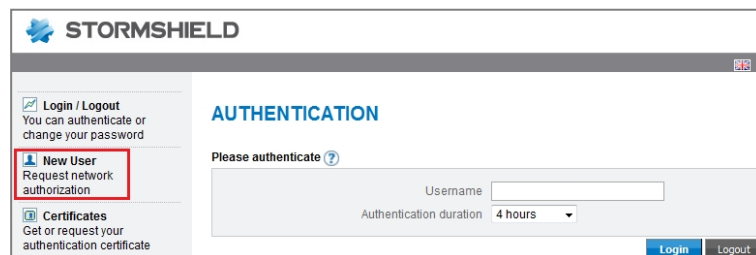


Enrôler d'un utilisateur

Dans ce chapitre, les actions de demande d'enrôlement, de récupération et de sauvegarde du certificat sont réalisées par l'utilisateur du logiciel SDS Suite.

Demander l'enrôlement

L'utilisateur se connecte au portail d'authentification Web du firewall par le biais d'une URL du type : https://adresse_IP_firewall/auth/ afin d'effectuer sa demande de création de compte puis clique sur le menu de gauche **Nouvel utilisateur** :





L'utilisateur remplit alors les champs obligatoires du formulaire de requête (**Nom, Prénom, Adresse e-mail, Mot de passe**) et valide sa demande en cliquant sur le bouton **Soumettre ces informations...**

Sa requête de création de compte et de signature du certificat associé est alors mise à disposition d'un administrateur du firewall pour validation. La validation de cette demande est exposée dans le chapitre [Approbation des requêtes d'enrôlement par un administrateur](#).

Récupérer le certificat

Lorsque la requête de l'utilisateur a été approuvée par un administrateur, il lui est possible de récupérer son certificat sur le portail d'authentification du firewall.

L'utilisateur se connecte au portail d'authentification (https://adresse_IP_firewall/auth/) à l'aide de son nom d'utilisateur et de son mot de passe, clique sur le menu de gauche **Certificats**, saisit son nom d'utilisateur (*john.doe* dans l'exemple) et clique sur **Téléchargez le certificat** :

i NOTE

Avec la méthode d'enrôlement, le certificat et la clé privée de l'utilisateur sont créés et stockés dans le navigateur Internet de l'utilisateur (la clé privée n'est en aucun cas sauvegardée sur le firewall). Cette opération n'étant réalisable qu'une seule fois, il est primordial de sauvegarder immédiatement le certificat et la clé privée dans un emplacement sécurisé, et de les supprimer du navigateur lorsque la connexion au client SDS Suite a été validée pour l'utilisateur.

Sauvegarder le certificat utilisateur

Sur le poste client, accédez au magasin de certificats du navigateur Web afin de sauvegarder le certificat :

Firefox :

1. Allez dans l'onglet *Certificats* du menu **Paramètres** > **Avancé** et cliquez sur **Afficher les certificats**,
2. Sélectionnez le certificat de l'utilisateur,
3. Cliquez sur **Sauvegarder**,



4. Sélectionnez un emplacement de sauvegarde sécurisé, choisissez le format PKCS12, indiquez un nom pour le certificat et cliquez sur **Enregistrer**,
5. Entrez un mot de passe de sauvegarde pour le certificat et validez.

Internet Explorer :

1. Allez dans l'onglet *Contenu* du menu **Options Internet** et cliquez sur **Certificats**,
2. Sélectionnez le certificat de l'utilisateur,
3. Cliquez sur **Exporter**, puis sur **Suivant**,
4. Choisissez **Oui, exporter la clé privée** puis le format **Echange d'informations personnelles - PKCS #12**,
5. Indiquez un nom pour le certificat,
6. Entrez un mot de passe de sauvegarde du certificat,
7. Sélectionnez un emplacement de sauvegarde sécurisé, cliquez sur **Enregistrer** et validez.

Supprimez ensuite le certificat et sa clé du navigateur Internet.

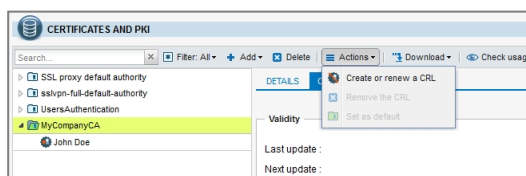
Mettre à jour et publier la CRL

L'interrogation de la CRL est un point critique dans l'utilisation d'un client Stormshield Data Security : en effet, les opérations cryptographiques peuvent être compromises si la CRL n'est pas à jour. Cette mise à jour est réalisée automatiquement lors de la révocation d'un certificat depuis le menu **Certificats et PKI** si la case **Créer la CRL après révocation est cochée** (cette opération est décrite dans le paragraphe [Révocation d'un certificat utilisateur et mise à jour de la CRL](#)).

En revanche, la mise à jour de la CRL doit être réalisée manuellement dans les cas suivants :

- suppression d'un certificat utilisateur depuis le menu **Utilisateurs**,
- date de validité de la CRL échue ou proche de son échéance.

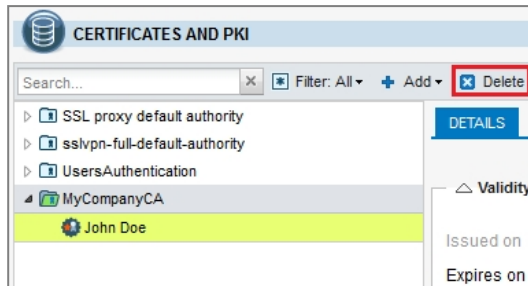
Pour mettre à jour manuellement la CRL, sélectionnez la CA dans le menu **Objets > Certificats et PKI** puis déroulez le menu **Actions** et cliquez sur le menu **Créer ou renouveler une CRL** :



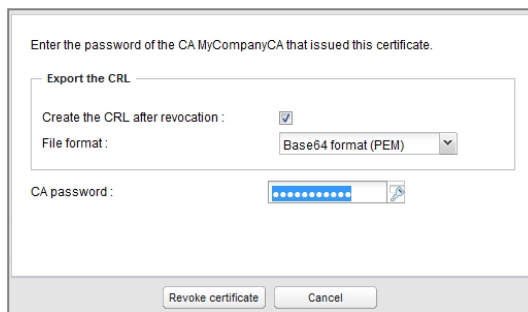
La date de validité de la CRL est alors modifiée en conséquence. La CRL étant stockée directement sur le firewall, la mise à jour de celle-ci est automatiquement prise en compte sans nécessité d'une republication manuelle.

Révoquer un certificat utilisateur et mettre à jour la CRL

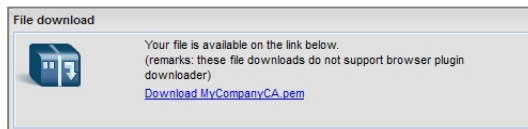
1. Depuis le menu **Objets > Certificats et PKI**, sélectionnez le certificat utilisateur à révoquer, puis cliquez sur le bouton **Supprimer**.



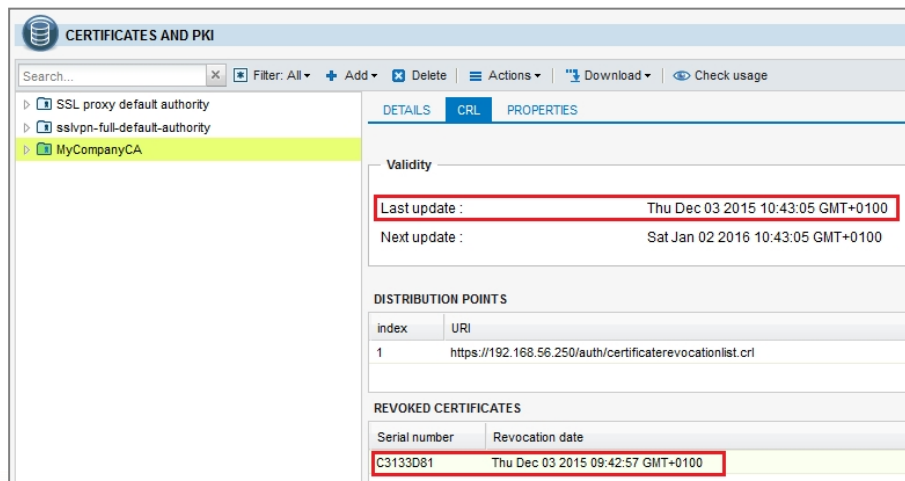
2. Vérifiez que la case **Créer la CRL après révocation** est bien cochée : cela permettra la mise à jour automatique de la CRL en fin de processus de révocation du certificat.
3. Indiquez le mot de passe de la CA et validez la suppression en cliquant sur le bouton **Révoquer le certificat** :



4. Renseignez à nouveau le mot de passe de la CA pour la mise à jour de la CRL et cliquez sur le bouton **Créer ou renouveler une CRL**.
5. Vous pouvez alors télécharger la CRL mise à jour afin de la publier sur les éventuels points de distributions autres que le firewall :



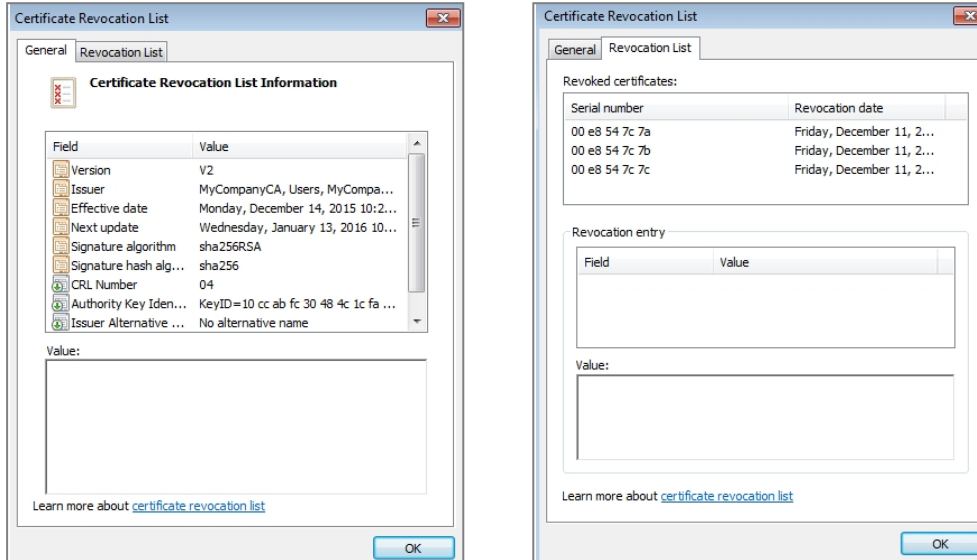
Les informations de la CRL reflètent immédiatement la révocation du certificat :






La CRL étant stockée directement sur le firewall, la mise à jour de celle-ci est automatiquement prise en compte sans nécessité d'une republication manuelle.

La CRL récupérée depuis le portail captif (https://firewall_dns_name/auth/ ou https://adresse_ip_firewall/auth puis menu **Certificats** > **Liste de révocation de certificats de votre société**) permet de vérifier que la révocation du certificat a bien été prise en compte :



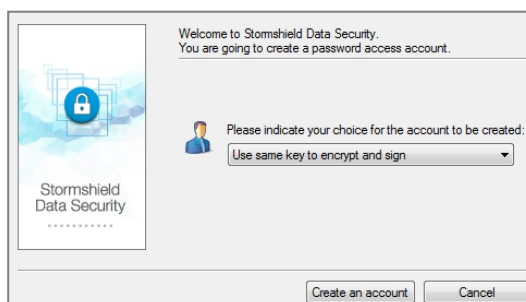
Configurer le logiciel SDS Suite

Créer un nouvel utilisateur dans SDS Suite

1. Faites un clic droit sur l'icône  présente dans la barre des tâches du poste utilisateur et sélectionnez le menu **Nouvel utilisateur** :



2. Choisissez l'option **Utiliser une seule clé pour chiffrer et signer** puis cliquez sur le bouton **Créer un compte** :



3. Identifiant du compte

Renseignez les trois champs obligatoires :



- **Identifiant** : cet identifiant de connexion doit être identique à celui renseigné dans l'annuaire LDAP du firewall (john.doe dans l'exemple).
- **Code secret** : l'utilisateur saisit un mot de passe strictement personnel destiné à protéger son compte SDS Suite. Ce mot de passe n'est aucunement lié à celui protégeant sa clé privée. Des critères de complexité de ce mot de passe sont affichés dans la fenêtre **Informations**.
- **Confirmation** : l'utilisateur confirme le mot de passe choisi.

Password analysis	
Strength of password (59 bits)	Green icon
Presence of digits	Green icon
"Diversity / Length" ratio	Green icon
Special or accented characters	Red icon
Recurrence of character sequences	Green icon

4. Clé personnelle

Choisissez l'option **Importer votre clé personnelle** et sélectionnez le fichier PKCS#12 (extension ".p12") contenant le certificat et la clé privée de l'utilisateur. Saisissez le mot de passe protégeant ce certificat et validez en cliquant sur **Suivant** :

Generate your personal key
Generates your key and the associated certificate with the information obtained in the the following steps.
Key type: RSA 2048 bits

Import your personal key
Import your key and the associated certificate included in the selected file.
From the file: JohnDoe.p12
Password:

i NOTE

Le certificat de la CA est également proposé à l'import. Veillez à ce que les cases des certificats utilisateur et CA soient cochées.

Selection of your personal key

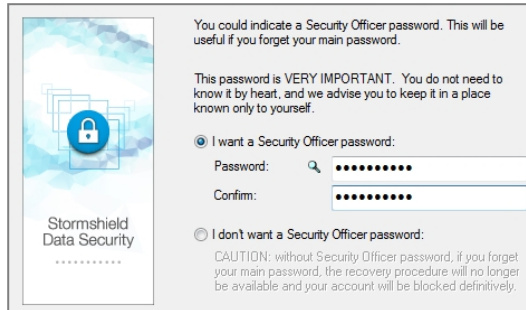
Only one key (reusable) has been found in the file
RSA 2048 bits

Please check the certificates you want to reuse:

- John Doe
- MyCompanyCA



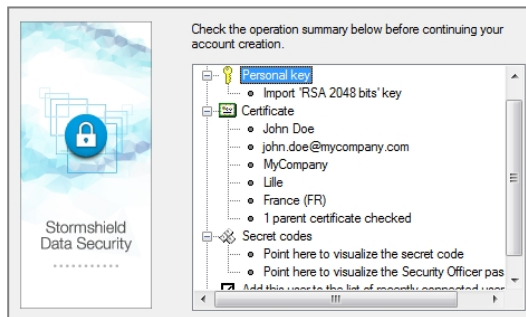
5. Validez en cliquant sur **Suivant**.
6. L'assistant propose alors la création d'un mot de passe de secours permettant de retrouver le mot de passe du compte utilisateur en cas de perte. Il est fortement recommandé de créer ce mot de passe de secours. Renseignez et confirmez ce mot de passe. Validez en cliquant sur **Suivant** :



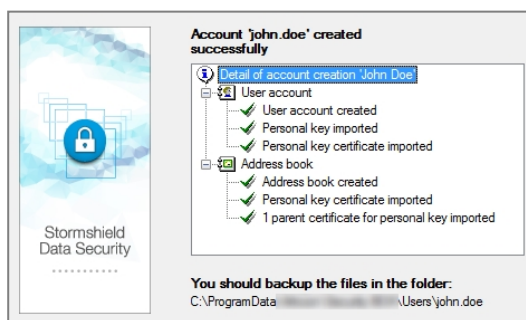
! IMPORTANT

Sans mot de passe de secours, il est impossible de retrouver le mot de passe de l'utilisateur en cas de perte. Il est donc très fortement recommandé de créer un mot de passe de secours.

7. Validez l'écran proposant un résumé complet du compte utilisateur en cliquant sur **Terminer**.



8. La création de l'annuaire local est lancée automatiquement et le dernier écran propose un résumé des opérations réalisées:



9. Cliquez sur **Quitter** pour fermer l'assistant.

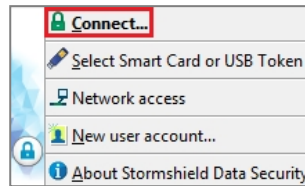
Ajouter l'annuaire du firewall dans le carnet d'adresses SDS Suite

Le référencement d'un annuaire LDAP dans le carnet d'adresses local permet d'indiquer à SDS Suite que cet annuaire doit être systématiquement interrogé lors de l'envoi ou de la réception d'un e-mail.



Connecter l'utilisateur à SDS Suite

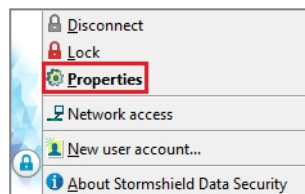
1. Faites un clic droit sur l'icône SDS Suite présente dans la barre des tâches et sélectionnez le menu **Connecter...**



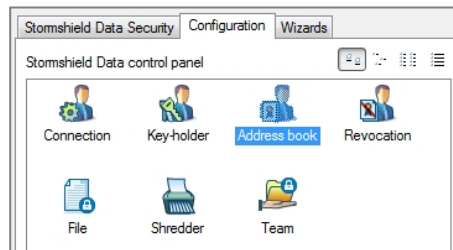
2. Renseignez le mot de passe de l'utilisateur puis cliquez sur le bouton **Valider**.

Ajouter l'annuaire LDAP du firewall

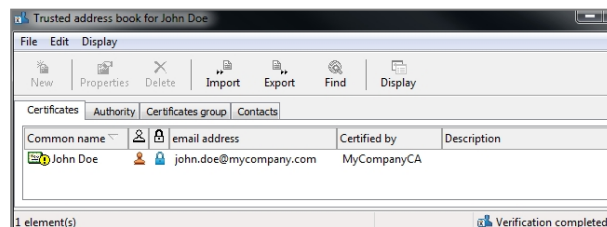
1. Après connexion, effectuez de nouveau un clic droit sur l'icône SDS Suite de la barre des tâches et sélectionnez le menu **Propriétés** :



2. Dans l'onglet *Configuration* de la fenêtre des propriétés de l'utilisateur, double-cliquez sur l'icône **Annuaire** :



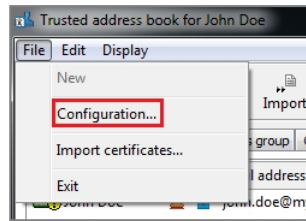
Le contenu de l'annuaire local de l'utilisateur s'affiche :



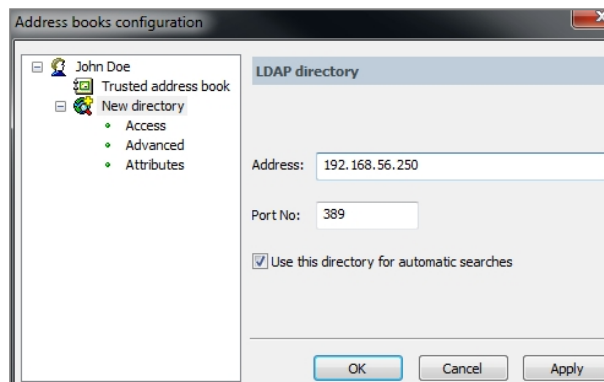
NOTE

Dans l'exemple, le symbole indique que le certificat listé est à utiliser avec précaution, car la liste de révocation (CRL) n'a pas pu être consultée.

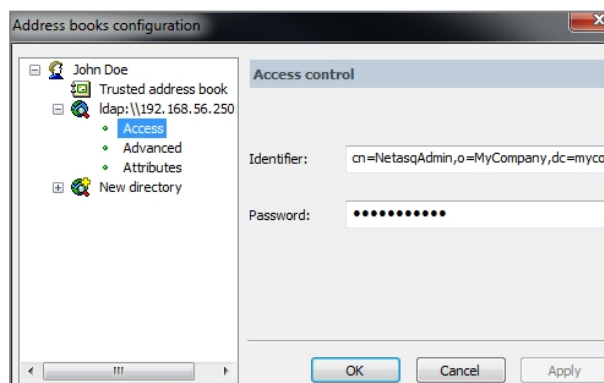
3. Déroulez le menu **Fichier** et sélectionnez **Configuration...** :



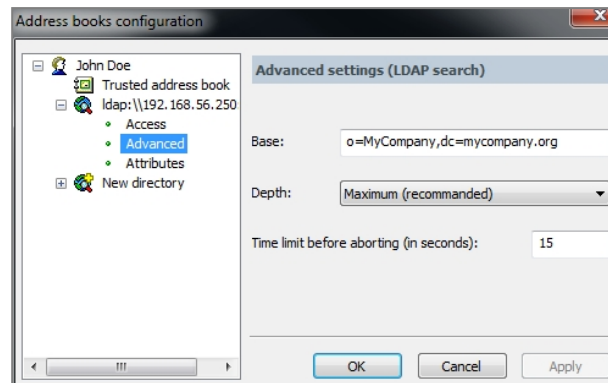
4. Dans la fenêtre de configuration des annuaires, cliquez sur **Ajouter un annuaire** et renseignez l'adresse IP (192.168.56.250 dans l'exemple) ou le nom DNS du firewall (ce nom doit alors être renseigné dans un serveur DNS joignable par les clients SDS Suite). Laissez le port proposé par défaut (LDAP /389) et cochez la case **Utiliser cet annuaire pour les recherches automatiques** :



5. Cliquez sur **Appliquer**.
6. Dans les propriétés de l'annuaire LDAP ajouté, sélectionnez **Accès** et remplissez les deux champs :
 - **Identifiant** : Distinguished Name (DN) de l'utilisateur autorisé à parcourir l'annuaire (NetasqAdmin). Il prend la forme suivante : cn=NetasqAdmin, o=Organisation, dc=Domaine (exemple : cn=NetasqAdmin,o=MyCompany,dc=mycompany.org)
 - **Mot de passe** : renseignez le mot de passe utilisé lors de la création de l'annuaire LDAP sur le firewall.

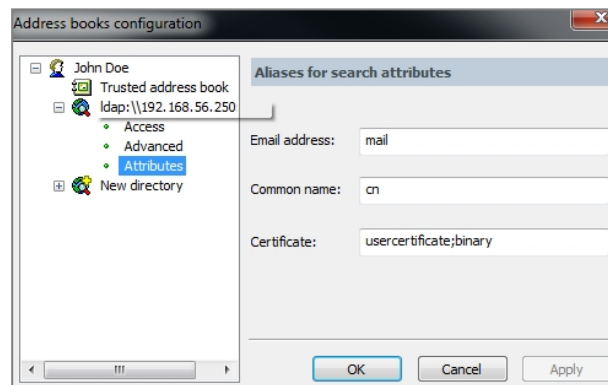


7. Dans les propriétés de l'annuaire LDAP, sélectionnez **Avancé** et remplissez le champ **Base** correspondant à la base DN du stockage des certificats sur le firewall. Il prend la forme suivante : o=Organisation,dc=Domaine (exemple : o=MyCompany,dc=mycompany.org).



8. Dans les propriétés de l'annuaire LDAP, sélectionnez **Attributes** et vérifiez que les champs ont les valeurs suivantes :

- **Email address** : *mail*,
- **Common name** : *cn*,
- **Certificate** : *usercertificate;binary*.



9. Cliquez sur **OK** pour valider la création de l'annuaire LDAP dans le carnet d'adresses de l'utilisateur.

Ajouter automatiquement les certificats des correspondants e-mail

Il est possible de paramétrer l'ajout automatique des certificats de correspondants présents dans l'annuaire LDAP à l'annuaire local SDS Suite lorsqu'un e-mail leur est envoyé.

Il est nécessaire pour cela de modifier le fichier de configuration *sbox.ini* de SDS Suite comme suit :

1. Editez le fichier *sbox.ini* présent dans le répertoire Kernel du chemin d'installation de SDS Suite (C:\Program Files\Arkoon\Security BOX\Kernel\ dans l'exemple).

```
SBox.ini - Bloc-notes
Fichier Edition Format Affichage ?
DefaultPath=C:\ProgramData\Arkoon\Security BOX\Users
RootPath=C:\ProgramData\Arkoon\Security BOX\Users
ShowBrowse=1
ShowLastUsers=5
[CR]
CRLDatabaseMode=C:\ProgramData\Arkoon\Security BOX\Users\default\default.bcr1
TmpCRLPath=C:\ProgramData\Arkoon\Security BOX\CRL
DeleteTmpCRL=1
LDAPTimeOut=60
[TEAM]
ExcludedPath=<%APPDATA%>
[SBox.NewUserWizardEXGP2]
AllowNewUser=1
Pkcs12Import=1
```



2. Créez une section [Mail], ajoutez le champ "SilentImportTrustedLdapCert" et affectez-lui la valeur "1" :

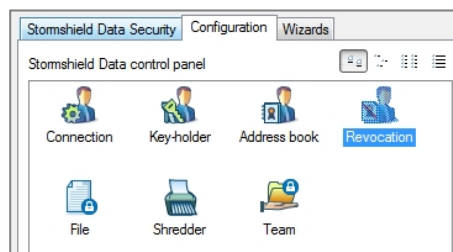
```
[SBox.NewUserWizardExKs1]
AllowNewUser=1
AllowNewUserCipher=1
AllowNewUserSign=1
Pkcs12Import=1
[SBox.NewUserWizardExKs2]
AllowNewUser=1
Pkcs12Import=1
[SBox.NewUserWizardExGp1]
AllowNewUser=1
AllowNewUserCipher=1
AllowNewUserSign=1
Pkcs12Import=1
InternalKeys=0
ExportKeys=1
KeepCardObjects=1
[Mail]
SilentImportTrustedLdapCert=1
```

3. Enregistrez les modifications et fermez le fichier.

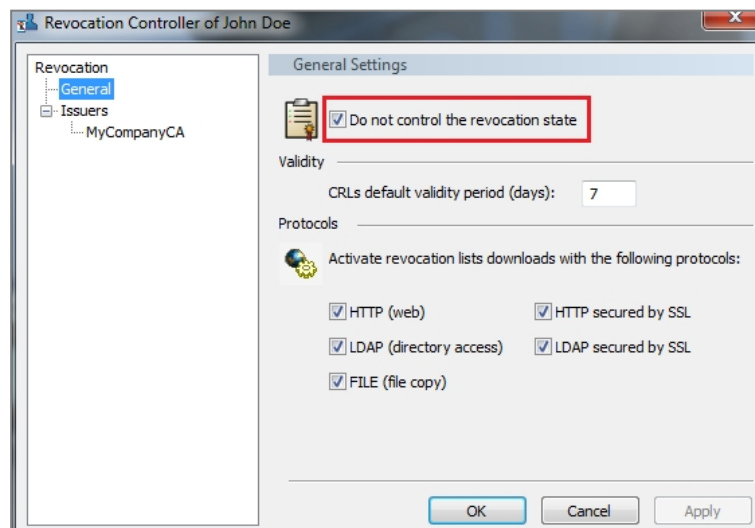
Activer / Désactiver le contrôle de révocation des certificats

Lorsque la version de firmware du firewall Stormshield Network hébergeant la CRL est inférieure à 2.4, il est nécessaire de désactiver le contrôle de révocation des certificats du client SDS.

1. Faites un clic droit sur l'icône SDS Suite présente dans la barre des tâches et sélectionnez le menu **Propriétés**.
2. Dans l'onglet *Configuration*, double-cliquez sur le menu **Révocation**:



3. Cochez la case "Ne pas contrôler la révocation des certificats" située dans le menu **Révocation** > **Général**. Appliquez et validez:



**i NOTE**

Pensez à décocher cette case lorsque le firewall Stormshield Network hébergeant la CRL dispose d'une version de firmware au moins égale à la version 2.4.

Importer le certificat du firewall dans les certificats de confiance du poste client

Lorsque le client SDS Suite effectue un contrôle automatique de l'état de la CRL, il se connecte en HTTPS au CRLDP hébergé sur le firewall SNS, et c'est alors le certificat du firewall qui est présenté. Pour le bon déroulement de cette opération de contrôle, il est donc nécessaire d'importer le certificat du firewall dans la console de gestion des certificats de confiance de Windows.

Récupérer le certificat du firewall

Depuis Internet Explorer

1. Dans la barre d'adresses du navigateur, saisissez l'adresse de connexion à l'interface d'administration du firewall : **https://adresse_ip_firewall/admin** ou **https://nom_dns_firewall/admin**.

i RAPPEL

Le choix d'une URI précisant le nom DNS du firewall implique que ce nom soit renseigné dans un serveur DNS interne accessible depuis les clients SDS Suite.

2. Lorsque la page d'authentification sur le firewall est affichée, cliquez sur la zone du rapport de sécurité située à droite de la barre d'adresses du navigateur.
3. Dans la fenêtre de rapport de sécurité, cliquez sur **Afficher les certificats**
4. Dans l'onglet *Détails*, cliquez sur le bouton **Copier dans un fichier...**
5. Cliquez sur **Suivant**,
6. Laissez le format proposé par défaut : **X.509 binaire encodé DER (.cer)**, puis cliquez sur **Suivant**.
7. Cliquez sur **Parcourir** pour sélectionner un emplacement de sauvegarde, puis saisissez un nom pour le fichier et cliquez sur **Enregistrer**.
8. Cliquez sur **Suivant** puis sur **Terminer**.
9. Validez le message "**L'exportation s'est effectuée correctement**".
10. Fermez la fenêtre présentant le détail du certificat en cliquant sur **OK**.

Depuis Mozilla Firefox

1. Dans la barre d'adresses du navigateur, saisissez l'adresse de connexion à l'interface d'administration du firewall : **https://adresse_ip_firewall/admin** ou **https://nom_dns_firewall/admin**.

i RAPPEL

Le choix d'une URI précisant le nom DNS du firewall implique que ce nom soit renseigné dans un serveur DNS interne accessible depuis les clients SDS Suite.

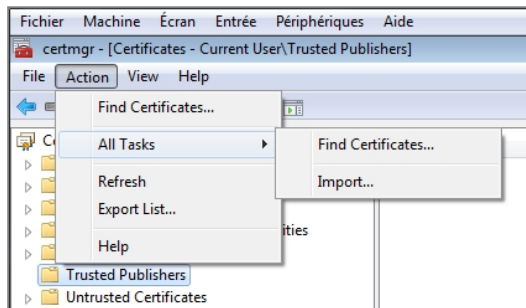
2. Lorsque la page d'authentification sur le firewall est affichée, cliquez sur la zone du rapport de sécurité (cadenas) située à gauche de la barre d'adresses du navigateur.
3. Dans la fenêtre de rapport de sécurité, cliquez sur le signe ">" puis sur le bouton **Plus d'informations**.



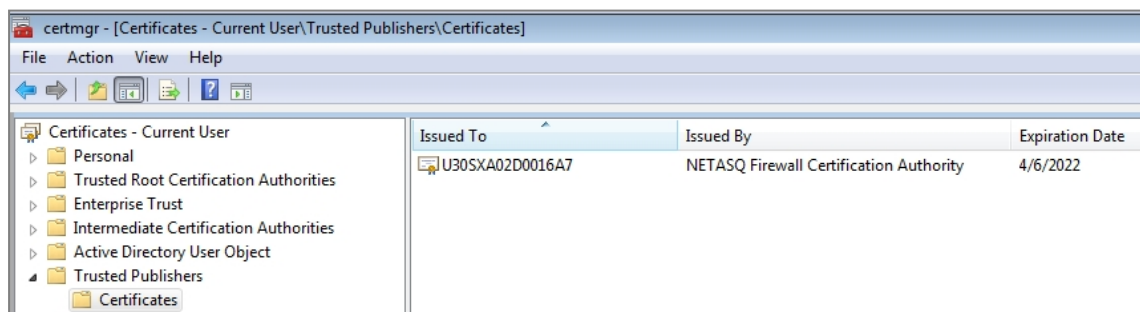
4. Cliquez sur le bouton Afficher le certificat.
5. Dans l'onglet *Détails*, cliquez sur le bouton **Exporter...**
6. Sélectionnez un emplacement de sauvegarde, puis saisissez un nom pour le fichier (laissez l'extension ".crt" proposée par défaut) et cliquez sur **Enregistrer**.
7. Fermez la fenêtre présentant le détail du certificat en cliquant sur **OK**.
8. Fermez la fenêtre de rapport de sécurité à l'aide du bouton

Importer ce certificat dans la console de gestion des certificats de confiance du poste client

1. Dans le menu Démarrer > Exécuter de Windows, saisissez certmgr.msc puis validez en cliquant sur OK pour lancer la console de gestion des certificats.
2. Dans le menu de gauche de la console, sélectionnez le magasin **Editeurs approuvés > Certificats**.
3. Cliquez sur le menu **Action > Toutes les tâches > Importer...**



4. Sélectionnez le certificat du firewall, précédemment exporté via votre navigateur Internet, puis cliquez sur **Suivant**.
5. Confirmez le choix du magasin de certificat (**Editeurs approuvés**) en cliquant sur **Suivant**.
6. Validez l'import en cliquant sur le bouton **Terminer**.
7. Un message vous confirme que l'import s'est correctement déroulé. Le certificat de votre firewall apparaît désormais dans le magasin. Il est identifiable grâce au numéro de série de votre firewall (ou à son nom DNS s'il en possède un).



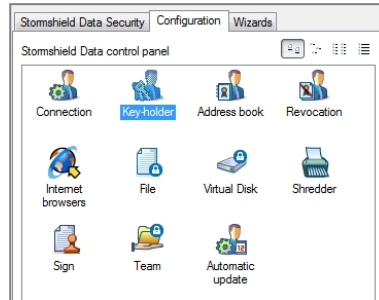
Importer la clé de recouvrement dans SDS Suite

! IMPORTANT

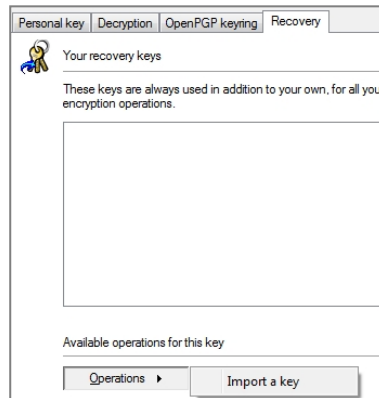
Il est nécessaire d'importer la clé de recouvrement dans le client SDS Suite avant tout chiffrement de données. En effet, les données chiffrées avant l'installation de la clé de recouvrement ne pourront pas être récupérées en cas de perte de sa clé privée par l'utilisateur.



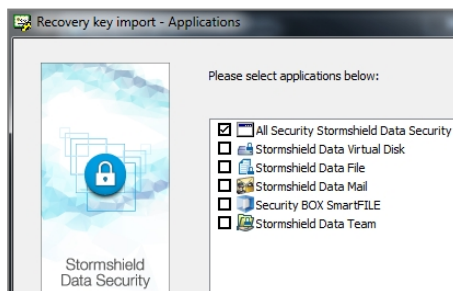
1. Faites un clic droit sur l'icône SDS Suite présente dans la barre des tâches et sélectionnez le menu **Propriétés**.
2. Dans l'onglet *Configuration*, double-cliquez sur le menu **Porte clé**.



3. Sélectionnez l'onglet *Recouvrement* et cliquez sur le bouton **Importer une clé**.

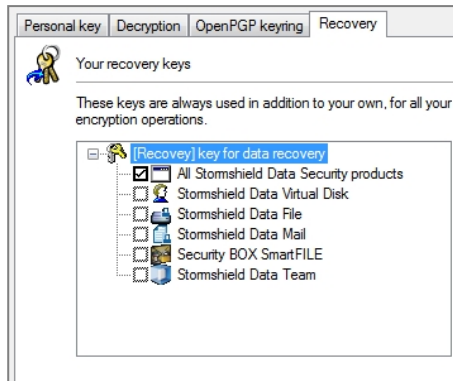


4. Sélectionnez le certificat du compte de recouvrement.
5. Indiquez les applications pour lesquelles vous souhaitez utiliser cette clé de recouvrement en cochant la case **Tous les produits Stormshield Data Security** :



6. Cliquez sur **Terminer** pour valider l'opération.

La clé de recouvrement est désormais déclarée pour le compte utilisateur SDS Suite :





Utiliser le compte de recouvrement

En cas de perte de la clé privée d'un utilisateur, le compte de recouvrement peut permettre à l'utilisateur de déchiffrer ses données.

Générer un nouveau certificat utilisateur et sa clé privée associée

Supprimez l'ancien certificat de l'utilisateur et mettez à jour la CRL (cf. [Révocation d'un certificat utilisateur et mise à jour de la CRL](#)).

Dans une configuration n'utilisant pas l'enrôlement :

1. Générez un nouveau certificat et sa clé,.
2. Exportez le certificat et sa clé au format PKCS#12 (cf. [Export du certificat et de la clé privée d'un utilisateur](#)).

Dans une configuration utilisant l'enrôlement :

1. L'utilisateur dépose une nouvelle demande de certificat via le portail d'authentification (menu **Certificats** > **Demandez votre certificat**, accessible après authentification sur le portail).
2. L'administrateur valide cette demande dans le menu **Utilisateur** > **Enrôlement** (cf. [Validation d'une requête de création d'utilisateur et du certificat associé](#)).
3. L'utilisateur récupère son certificat et sa clé depuis le portail d'authentification.
4. Il les sauvegarde au format PKCS#12 et stocke ce fichier dans un emplacement sécurisé.

Créer un utilisateur de recouvrement dans SDS Suite

Sur le poste client, suivez la méthode décrite dans le chapitre [Création d'un nouvel utilisateur SDS](#) pour créer le compte de recouvrement dans SDS Suite.

Déchiffrer les données de l'utilisateur à l'aide du compte de recouvrement

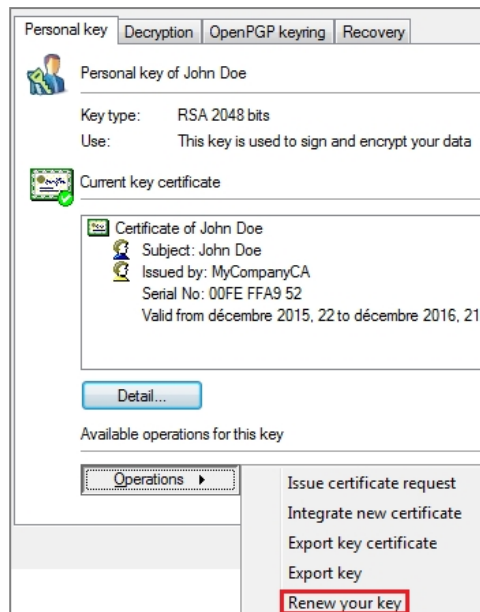
La connexion au logiciel SDS Suite à l'aide du compte de recouvrement permet alors de déchiffrer manuellement les données de l'utilisateur.

NOTE

Cette opération de déchiffrement doit être réalisée avec l'ensemble des modules SDS Suite ayant été utilisés par l'utilisateur pour chiffrer ses données (File, Mail, ...).

Renouveler la clé de l'utilisateur

1. L'utilisateur se connecte au client SDS Suite à l'aide de son compte personnel.
2. Dans l'onglet *Clé personnelle* du menu **Porte Clé** du client SDS Suite, il déroule le menu **Opérations** et sélectionne **Renouveler votre clé**.



3. Il choisit ensuite l'option **Importer votre clé personnelle**, sélectionne le fichier PKCS#12 contenant sa nouvelle clé de l'utilisateur et saisit le mot de passe protégeant le fichier.

Chiffrer les données à l'aide du compte utilisateur

L'utilisateur peut à nouveau chiffrer ses données.

i NOTE

Cette opération de chiffrement doit être réalisée avec l'ensemble des modules SDS Suite ayant été utilisés par l'utilisateur pour chiffrer ses données (File, Mail, ...).



Cycle de vie des clés

Rappels

Dans ce document, les clés et certificats utilisateurs ont une durée de vie de deux ans tandis que l'autorité de certification est définie pour une durée de 10 ans. Pour des raisons de sécurité, il est en effet déconseillé de délivrer des certificats dont la durée de vie serait égale à celle de la CA les ayant signés.

Les firewalls Stormshield Network ne permettent pas de renouveler un certificat expiré (conservation de la clé privée et nouvelle signature de celle-ci par la CA par défaut) : il est donc nécessaire de générer un nouveau certificat associé à une nouvelle clé pour l'utilisateur.

i NOTE

La clé de recouvrement ayant été créée avec une durée de validité égale à celle de la CA par défaut (10 ans dans l'exemple), cette clé reste valide après l'expiration du certificat de l'utilisateur et ne nécessite pas de renouvellement dans le client SDS Suite.

Que faire en cas d'expiration ou de révocation d'un certificat utilisateur?

Générer un nouveau certificat et sa clé privée associée

Dans une configuration n'utilisant pas l'enrôlement :

1. Générez un nouveau certificat et sa clé.
2. Exportez le certificat et sa clé au format PKCS#12.

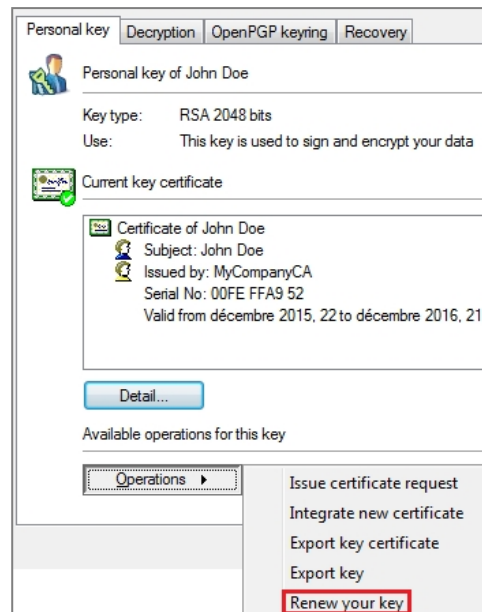
Dans une configuration utilisant l'enrôlement :

1. L'utilisateur dépose une nouvelle demande de certificat via le portail d'authentification (menu **Certificats** > **Demandez votre certificat**, accessible après authentification sur le portail).
2. L'administrateur valide cette demande dans le menu **Utilisateur** > **Enrôlement**.
3. L'utilisateur récupère son certificat et sa clé au format PKCS#12.
4. Il les sauvegarde au format PKCS#12 et stocke ce fichier dans un emplacement sécurisé.

Renouveler le certificat et sa clé privée dans SDS Suite

Installer la nouvelle clé

1. L'utilisateur se connecte au client SDS Suite à l'aide de son compte personnel.
2. Dans l'onglet *Clé personnelle* du menu **Porte Clé** du client SDS Suite, il déroule le menu **Opérations** et sélectionne **Renouveler votre clé**.



3. Il choisit ensuite l'option **Importer votre clé personnelle**, sélectionne le fichier PKCS#12 contenant sa nouvelle clé et saisit le mot de passe protégeant le fichier.

Transchiffrer les données de l'utilisateur.

Après la mise à jour de sa clé dans SDS Suite, l'utilisateur doit :

1. Déchiffrer manuellement ses données à l'aide de chacun des modules utilisés : File, Mail, ... (SDS Suite sélectionne automatiquement l'ancienne clé, toujours présente).
2. Chiffrer à nouveau manuellement ses données à l'aide de chacun des modules concernés (SDS Suite sélectionne alors automatiquement la clé la plus récente de l'utilisateur).

Que faire à l'approche de la date d'expiration de la CA ?

Lorsque la date de validité de la CA approche, il est nécessaire d'anticiper son expiration en redéfinissant une nouvelle chaîne de confiance et en mettant à jour l'ensemble des clients SDS Suite :

1. Création d'une nouvelle CA définie par défaut pour les utilisateurs.
2. Génération des certificats utilisateurs signés par cette nouvelle CA.
3. Import des nouveaux certificats sur les Clients SDS (cf. [Renouvellement du certificat et de sa clé privée dans SDS Suite](#)).
4. Transchiffrement des données par chacun des utilisateurs (cf. [Renouvellement du certificat et de sa clé privée dans SDS Suite](#)).



Configurer les sauvegardes automatiques du firewall

Ce chapitre décrit le paramétrage des sauvegardes automatiques du firewall au sein du Cloud Stormshield. La sauvegarde automatique de configuration permet ainsi de restaurer partiellement ou totalement la configuration du firewall en cas de mauvaise manipulation ou de sinistre.

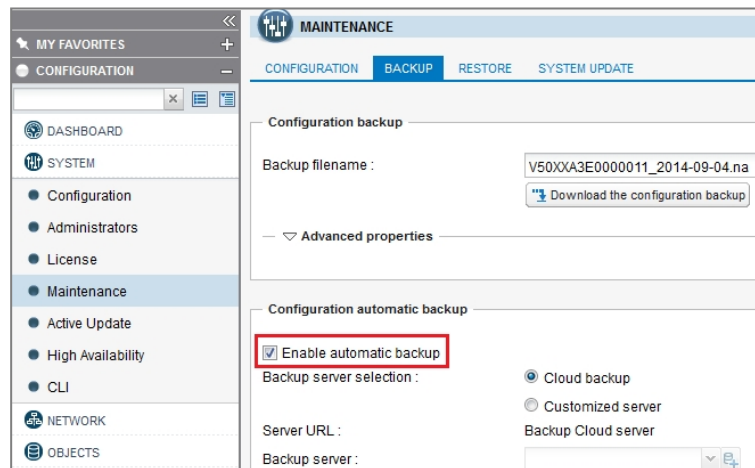
Notez que seule l'utilisation de la méthode recommandée par Stormshield (sans enrôlement) permettra la restauration des clés privées des utilisateurs depuis une sauvegarde automatique du firewall.

Sauvegarder automatiquement la configuration du firewall dans le Cloud Stormshield

L'option **Cloud backup** permet d'envoyer directement les sauvegardes du firewall dans votre espace sécurisé (<https://mystormshield.eu>). Les 5 dernières sauvegardes (quotidiennes, hebdomadaires ou mensuelles) de votre équipement sont ainsi stockées et accessibles.

Activer les sauvegardes automatiques

1. Sélectionnez l'onglet *Sauvegarder* du module **Configuration > Système > Maintenance**.
2. Dans l'écran *Sauvegarde automatique de configuration*, cochez la case **Activer la sauvegarde automatique**.



Sélectionner Stormshield Network Cloud Backup

Pour activer les sauvegardes automatiques vers le service **Stormshield Network Cloud backup**, sélectionnez la valeur « Cloud backup » pour le champ **Choix du serveur de sauvegarde**. Les sauvegardes sont alors enregistrées dans votre espace sécurisé (<https://mystormshield.eu>) grâce à l'identification du numéro de série du Firewall. Il n'est donc pas nécessaire, pour cette fonctionnalité, de renseigner un identifiant et un mot de passe dans le module **Préférences**.

i NOTE

La fonctionnalité SN Cloud Backup est présente sur l'ensemble des Firewalls Stormshield Network. Le service nécessite cependant que le firewall soit sous maintenance.



Configuration automatic backup

Enable automatic backup

Backup server selection :

Cloud backup

Customized server

Server URL :

Backup Cloud server

Backup server : autobackup2008

Seuls deux champs complémentaires sont à renseigner :

- **Fréquence des sauvegardes** : sélectionnez l'une des trois fréquences proposées (chaque jour, chaque semaine ou chaque mois).
- **Mot de passe du fichier de sauvegarde (optionnel)** : indiquez un mot de passe destiné à protéger le fichier de sauvegarde. Ce mot de passe sera demandé lors de l'utilisation du fichier en vue d'une restauration de la configuration.

Sauvegarder automatiquement la configuration du firewall sur un serveur HTTP/HTTPS personnalisé

Pour le paramétrage détaillé des sauvegardes automatiques du firewall vers un serveur HTTP/HTTPS personnalisé, consultez la Note Technique *Sauvegardes Automatiques* disponible dans votre [espace sécurisé](#).



STORMSHIELD

documentation@stormshield.eu

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

Copyright © Stormshield 2018. Tous droits réservés. Tous les autres produits et sociétés cités dans ce document sont des marques ou des marques déposées de leur détenteur respectif.