

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
Préreguis	
Configurer le Firewall SNS	5
Créer un annuaire I DAP interne	5
Activer le portail captif	5
Créer la CA pour les certificats utilisateurs	
Modifier les paramètres de la CA	
Définir la CA comme CA par défaut pour l'annuaire LDAP	
Créer la CRL	
Créer le compte de recouvrement	
Créer le compte de recouvrement dans l'annuaire LDAP interne	
Créer le certificat du compte de recouvrement	
Exporter le certificat du compte de recouvrement	
Créer des comptes et certificats sans enrôlement (méthode recommandée)	
Configurer le Firewall SNS	13
Créer un utilisateur et son certificat	
Exporter le certificat et la cle privee d'un utilisateur	
Péveguer un certificat utilisateur et mettre à jour la CPL	15
Configurer le logiciel SDS Suite	17
Créer un nouvel utilisateur dans SDS Suite	
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	
Utiliser le compte de recouvrement	27
Créer des comptes et certificats par enrôlement (méthode alternative)	
Configurer le Firewall SNS	29
Activer l'enrôlement et les requêtes de signature de certificats	29
Approuver les requêtes d'enrôlement	
Mettre à jour et publier la CRL	
Enröler d'un utilisateur	
Demander l'enrôlement	
Sauvegarder le certificat utilisateur	
Mettre à jour et publier la CRI	34
Révoquer un certificat utilisateur et mettre à jour la CRL	34
Configurer le logiciel SDS Suite	
Créer un nouvel utilisateur dans SDS Suite	
Ajouter l'annuaire du firewall dans le carnet d'adresses SDS Suite	
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	
Utiliser le compte de recouvrement	
Générer un nouveau certificat utilisateur et sa clé privée associée	47
Créer un utilisateur de recouvrement dans SDS Suite	
Dechiffrer 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	
Renouveler le certificat et sa clé privée dans SDS Suite	
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).**

	N			
AVAILABLE METHODS	AUTHENTICATION POLICY	CAPTIVE PORTAL	INTERNAL INTERFACES	EXTERNAL INTERFACES (INACTIVE)
Continuental				
Captive portai				
Enable the captive p	portal			
	i only	from internal (protec	ted) interfaces	
	only	from external (public	c) interfaces	
	from	internal and externa	il interfaces	
SSL server				
Certificate (private key)	Select	a certificate		×



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.

AVAILABLE METHODS	AUTHENTICATION POLICY	CAPTIVE PORTAL	INTERNAL INTERFACE
User passwords			
	Use	rs cannot change th	eir passwords
	O Use	rs can change their j	passwords
	Use	rs must change thei	r passwords

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

🕦 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**.

ERTIFICATES AND PKI				
Search × Fitter: All -	🕂 Add 🔻 🗵 Delete 🗮 Actions 🕶 🐴 Download 🕶 👁 Check us			
SSL proxy default authority	Add a root CA			
Issivpn-full-default-authority	Add a sub-CA			
	Add a user certificate			
	Add a Smartcard certificate			
	Add a server Certificate ter the list using the search bar.			
	Import a file			

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

<u>Étape 1 :</u>

- CN : saisissez un nom permettant d'identifier votre autorité de certification,
- Identifiant : le nom entré dans le champ CN est proposé par défaut,
- Organisation (0). 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.



N :	MyCompanyCA
	MyCompanyCA
Select the parent CA (if necessa	ry) —————————
Parent CA :	Select the parent CA 🛛 🗙 🔎
Password for the parent CA :	ß
Certificate authority attributes -	
Certificate authority attributes -	MyCompany
Certificate authority attributes – Organization (O) : Organizational Unit (OU) :	MyCompany Users
Certificate authority attributes – Organization (O) : Organizational Unit (OU) : Locality (L) :	MyCompany Users Lille
Certificate authority attributes – Organization (O) : Organizational Unit (OU) : Locality (L) : State or province (ST) :	MyCompany Users Lille North

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 	1	
Password (min. 8 char):	•••••	
Confirm password :	•••••	
Password strength:	G	ood
E-mail address :		
E-mail address : Key size (bytes) :	4096	~
E-mail address : Key size (bytes) : The computation of big keys may	4096 slow down your appliance	•

<u>Étape 3</u> :

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



🕦 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 :

MY FAVORITES + CONFIGURATION CONFIGURATION X E DASHBOARD SYSTEM Configuration Administrators License Maintenance Active Update High Availability Management Center CLL S NETWORK	Image help half NUTH User authentication CHEWD Return if it's necessary to update password or not CONFIG CONFIG Firewall configuration functions GLOBALARMIN : Global administration HA HA HA HA LIST Display available commands LIST LIST Display the list of connected users, show user rights (Level) and rights for cur: MODIFY Get / Lose the modify or the mon_write right MONITOR MONITOR NOP Do nothing but avoid disconnection from server. FKI Show or update the pki QUIT Co off REPORT System System commands USER User related functions VERSION Display server version
ST NETWORK	pki ca config crldp adD CANAME=MyCompanyCA URI=https://firewall.mycompany.name/auth/certificaterevocationlist.crl

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) :



CERTIFICATES AND PKI		
Search 🗶 🗷 Filter: All 👻 🛧 Ad	d 🗸 🛚 Delete 🚍 Actions 🗸 🐴 Download	I▼ Scheck usage
SSL proxy default authority	DETAILS CRL PROPERTIES	
Issivpn-full-default-authority		
MyCompanyCA	Certificate authority	
	Key size (bytes) :	4096 👻
	Validity (days) :	3650
	CRL validity (days) :	30
	User certificates Key size (bytes) : Validity (days) :	2048 ¥ 730 \$

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**.

	ATES AND PKI		
Search	× Filter: All	🗕 🕂 Add 🗝 🔀 Delete 🛛 🚍	Actions - 🗌 🛂 Download -
SSL proxy d	efault authority	DETAILS 0	Create or renew a CRL
Isslvpn-full-d	efault-authority		
MyCompany	CA	- 🛆 Validity - 🔳	Set as default
		Issued on :	1
		Expires on :	2

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** :

CERTIFICATES AND PKI	
Search × Filter: All - + A	Add 👻 🛛 Delete 🗮 Actions 🗸 🐴 Download 🗸 👁 Check usage
SSL proxy default authority	DETALS Create or renew a CRL
Issivpn-full-default-authority	Remove the CRL
UsersAuthentication	Satur default
4 🛅 MyCompanyCA	Validity and a default
🚯 John Doe	Last update :
	Lasi upuale .
	Next update :

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 :



CERTIFICATES AND PKI			
Search × Fitter: All - + Ada	d 🕶 🔀 Delete	■ Actions •	🔁 Download 🕶 🕼 Check usage
To SSL proxy default authority To SSL proxy default authority To Sslvpn-ful-default-authority To MyCompany To MyCompanyCA	DETAILS	CRL PROPERT	ES
	Last updat Next updat	e: e:	Wed Dec 02 2015 18:22:55 GMT+0100 Fri Jan 01 2016 18:22:55 GMT+0100
	DISTRIBUTIO	N POINTS	
	index	URI	
	1	https://192.168.56.2	50/auth/certificaterevocationlist.crl
	REVOKED CE	RTIFICATES	
	Serial numbe	r Revocation	date

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.



Résumé

Cliquez sur Terminer pour valider la création du certificat.

🕦 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**.



 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

- 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 CE	RTIFICATE MEMBER OF THESE GROUPS
ID (login) :	john.doe
Last name :	Doe
First name :	John
E-mail address :	john.doe@mycompany.com
Phone number :	
Description :	

- 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
V Apply	K Cancel



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*).

USERS				
Searching	× 👤 Filter: Users 🕶	+ Add user + Add group 🛛 Delete 👁 Check usage		
CN John Doe		👤 john.doe (Doe John)		
		ACCOUNT CERTIFICATE MEMBER OF THESE GROUPS		
		Create the certificate S Delete		
		No certificate for this user.		

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** :

Creation of the user certificate	
The certificate authority's (CA) passw certificate.	ord is needed in order to create a user
Protection of the certificate for its	publication (export)
Password (min. 8 chars) :	•••••
Confirm password :	•••••
Password strength:	Good
CA password	
Password :	•••••
Create the certific	Cancel

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

USERS					
Searching × 👤 Fiter: Users -	🛉 Add user 🔹 Add group 🔀 De	lete 🐵 Check usage			
CN 1 John Doe	👤 john.doe (Doe John)				
_	ACCOUNT CERTIFICATE MEN	ACCOUNT CERTEICATE MEMBER OF THESE GROUPS			
	O course of the second second second				
	Ureate the certificate Delete				
	_ △ Validity				
	Issued on .	27/11/2015 11:17:43			
	Expires on :	26/11/2017 11:17:43			
	△ Issued for				
	Subject :	/C=FR/ST=North/L=Lille/O=MyCompany/OU=Users/CN=John Doe/emailAddress=john.doe@mycompany.com			
	Name (CN) :	John Doe			
	Organization (O) :	MyCompany			
	Organizational unit (OU) :	Users			
	Locality (L) :	Lille			
	State or province (ST) :	North			
	Country (C) :	FR			
	E-mail address : Other information :	John.doe@mycompany.com			
	Checksum :	25062440			
	_ △ Issuer				
	Issuer :	/C=FR/ST=North/L=Lille/O=MyCompany/OU=Users/CN=MyCompanyCA			



🕦 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** :

CERTIFICATES AND PKI		
Search X 💌 Filter: All - 🕂	Add 🕶 🙁 Delete 🗮 Action	ns 🕶 🖳 Download 🕶 👁 Check usage
SSL proxy default authority	DETAILS	Certificate as a PEM file
sslvpn-full-default-authority		Certificate as a DER file
UsersAuthentication		Cortificate en a B12 file
MyCompanyCA	─ △ Validity —	Certificate as a F12 file
🚯 John Doe		CRL as PEM file
	Issued on :	CRL as DER file
	Expires on :	26/11/2016 15:59:1

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** :

Content a password to protect the certain statement of the certain s	rtificate file
Please enter a password :	
Confirm password :	
Password strength:	
	artificata
V Download the co	

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

File download	MyCompany
	Your file is available on the link below. (remarks: these file downloads do not support browser plugin downloader)
	Download C%3DFR%20ST%3DNorth%20L%3DLille%200%3DMvCompany%20OU%3I

🚺 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 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** :

CERTIFICATES AND PKI		
Search × Fitter: All + Add	🔹 🛛 Delete 🗮 Actions • 🐴 Download • 👁 Check us	age
SSL proxy default authority	DETAILS Create or renew a CRL	
Isslvpn-full-default-authority	Remove the CRL	-
UsersAuthentication	Sat an dafault	
a 🛅 MyCompanyCA	Validity Set as default	
🚯 John Doe	Last undate :	
	Last update .	
	Next update :	

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 :**

Enter the password of the CA MyCompanyCA that issued this certificate.					
Create the CRL after revocation : File format :	Base64 format (PEM)				
CA password :					
Revoke certificat	e Cancel				

- 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 :

9			
Search × Filter: All - Ad	d 🕶 🐹 Delete 🛛 🗮 Actions 🕶	💁 Download 🗸 🛛 👁 Check usage	
SSL proxy default authority	DETAILS CRL PROPER	TIES	
Issivpn-full-default-authority			
MyCompanyCA			
	Validity		
	Last update :	Thu Dec 03 2015 10:43:05 GMT+0100	
	Next update :	Sat Jan 02 2016 10:43:05 GMT+0100	
	DISTRIBUTION POINTS		
	index URI		
	1 https://192.168.56	250/auth/certificaterevocationlist.crl	
	REVOKED CERTIFICATES		
	Serial number Revocation	n date	
		2015 00 40 57 ONT-0400	
	https://192.168.56.250/auth/certificaterevocationlist.crl REVOKED CERTIFICATES Serial number Revocation date		

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 :

General Revocation List			General Revocat	tion List	Ľ
	ocation List information		Serial number	ates.	Revocation date
Field Version Susuer Effective date Next update	Value V2 MyCompanyCA, Users, MyCompa Monday, December 14, 2015 10:2 Wednesday, January 13, 2016 10		00 e8 54 7c 7a 00 e8 54 7c 7b 00 e8 54 7c 7c 00 e8 54 7c 7c	τγ	Friday, December 11, 2 Friday, December 11, 2 Friday, December 11, 2
Signature hash alg CRL Number Authority Key Iden Sissuer Alternative	sha256 04 . KeyID=10 cc ab fc 30 48 4c 1c fa . No alternative name	-	Field	Value	
Value:			Value:		
Learn more about <u>certificat</u>	e revocation list		Learn more abou	t <u>certificate revocatio</u>	n list
		ок			ОК

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** :

	Connect	
	Select Smart Card or USB Token	Þ
	PNetwork access	Þ
	 <u>N</u>ew user account 	
Y	1 <u>A</u> bout Stormshield Data Security	



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

	Welcome to Stormshield Data Security. You are going to create a password access account.
0.	•
	Please indicate your choice for the account to be created:
Stormshield Data Security	
	Create an account Cancel

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.

	Identifier:	john.doe
	Secret code: 🔍	•••••
	Confirmation:	•••••
	Information	
	Password ana	lysis
Stormshield		f password (59 bits) of digits
ata Security		/ Length" ratio
	- Special or	accentuated characters
		e of character sequences

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** :

	C Gene	erate your persona	al key	
	Gen the i	erates your key ar nformation obtain	nd the associated certifica ed in the the following ste	ate with ps.
frank l		Key type:	RSA 2048 bits	-
	0	.,	-7	
	Impo in the	nt your key and th e selected file.	ne associated certificate in	ncluded
	Impo in the	nt your key and th e selected file. <u>F</u> rom the file:	JohnDoe.p12	ncluded
Stormshield Data Security	Impo in the	nt your key and the selected file. <u>F</u> rom the file: Password:	JohnDoe.p12	ncluded
Stormshield Data Security	Impo in the	nt your key and the selected file. <u>F</u> rom the file: Password:	JohnDoe.p12	ncluded



🕦 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
	Cl _{jA} RSA 2048 bits ▼
	Please check the certificates you want to reuse:
	⊡… 🗹 👺 John Doe
Stormshield Data Security	

- 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** :

	You could indicat useful if you forge	You could indicate a Security Officer password. This will be useful if you forget your main password.			
	This password is know it by heart, known only to you	VERY II and we urself.	MPORTANT. You do not need to advise you to keep it in a place		
	 I want a Secu 	I want a Security Officer password: Password: Q			
	Password:				
	Confirm:				
Stormshield Data Security	🔘 l don't want a	I don't want a Security Officer password:			
	CAUTION: wi your main pas be available a	CAUTION: without Security Officer password, if you forget your main password, the recovery procedure will no longer be available and your account will be blocked definitively.			

🚺 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.

	Check the operation summary below before continuing your account creation.	
G-	Personal key Normal key Import 'RSA 2048 bits' key	*
	Certificate	
	 John Doe 	
	 john.doe@mycompany.com 	
	···· • MyCompany	
	···· • Lille	Ξ
	···· • France (FR)	
Charmahiald	 1 parent certificate checked 	
Data Security		
Data Security	 Point here to visualize the secret code 	
	 Point here to visualize the Security Officer pas 	
	Add this upperts the list of meanthy connected upper	
	•	

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...**

	Connect					
	Select Smart Card or USB Toker					
N	₽ Network access ▲ New user account					
P	1 About Stormshield Data Security					

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

Ajouter l'annuaire LDAP du firewall

 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 :

al's Trusted address book for John Doe							
File Edit Display							
New Properties Delete Impor	⊫ب ⊗ t Export Find	Display					
Certificates Authority Certificates group	Certificates Authority Certificates group Contacts						
Common name 🔽 🚨 email address	s C	ertified by	Description				
📴 John Doe 🛛 🚨 john.doe@m	nycompany.com	ЛуCompanyCA					
1 element(s)			Werification completed.				

🕦 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... :
 - Tusted address book for John Doe File Edit Display New Configuration... Import certificates... Exit Exit Liddress Joint doe@my
- 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** :

Address books configuration		
Quiress books coningulation Quiress books coningulation Trusted address book Wew directory • Access • Advanced • Attributes	LDAP din Address: Port No:	ectory 192.168.56.250 389 s directory for automatic searches
		OK Cancel Apply

- 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.





 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).

Address books configuration			— ×
John Doe Trusted address book dap:\\192.168.56.250 Access Advanced Attributes K	Advanced s Base: Depth: Time limit before	ettings (LDAP search) o=MyCompany,dc=mycompan (Maximum (recommanded) re aborting (in seconds):	y.org T
< Þ		OK Cancel	Apply

- 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.

Aliases for sea	rch attributes
Email address:	mail
Common name:	a
Certificate:	usercertificate;binary
	K Cancel Apply
	Aliases for sea Email address: Common name: Certificate:

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).



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

[SBOX.NewUserWizardExK51]
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=11
[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:

5	Stormshield Data \$	Security Config	uration Wizards		
	Stormshield Data	control panel		Pa 1- 11	≣
	<i></i>	~			
	Connection	Key-holder	Address book	Revocation	
			~		
	6	(mm)			
	File	Shredder	Team		



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

Revocation Controller of John	Doe
Revocation 	General Settings Image: Do not control the revocation state Validity CRLs default validity period (days): Protocols Image: Dot control the revocation lists downloads with the following protocols: Image: Dot control the revocation lists downloads with the following protocols: Image: Dot control the revocation lists downloads with the following protocols: Image: Dot control the revocation lists downloads with the following protocols: Image: Dot control the revocation lists downloads with the following protocols: Image: Dot control the revocation lists downloads with the following protocols: Image: Dot control the revocation lists downloads with the following protocols: Image: Dot control the revocation lists downloads with the following protocols: Image: Dot control the revocation lists downloads with the following protocols: Image: Dot control the revocation lists downloads with the following protocols: Image: Dot control the revocation lists downloads with the following protocols: Image: Dot control the revocation lists downloads with the following protocols: Image: Dot control the revocation lists downloads with the following protocols: Image: Dot control the revocation lists downloads with the following protocols: Image: Dot control the revocation lists downloads with the following protocols: Image: Dot contrevo
	OK Cancel Apply

🕦 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

 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.

1 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

 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.

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.
- 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).



certmgr - [Certificates - Current User\Trusted Publishers\Certificates]					
File Action View Help					
🗢 🏟 🖄 🗊 🔒 🛛 🖬					
Certificates - Current User	Issued To	Issued By	Expiration Date		
Personal Trusted Root Certification Authorities	🖏 U30SXA02D0016A7	NETASQ Firewall Certification Authority	4/6/2022		
Enterprise Trust					
Intermediate Certification Authorities					
Active Directory User Object					
Trusted Publishers					
Certificates					

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.

Personal key Decryption OpenPGP keyring Recovery						
R	Your recovery keys		8			
	These encry	e keys are alv ption operatio	vays used in ins.	addition	to your own	, for all your
	Availa	able operation	is for this ke	/		
		Operations		Import	a key	

- 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,.
- 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).
- 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.

🕦 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.

1 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

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



AUTHENTICATION				
AVAILABLE METHODS AU	THENTICATION POLICY	CAPTIVE PORTAL	INTERNAL INTERFACES	EXTERNAL INTERFACES (INAC
lieer neeeworde				
user passwords				
	O Use	rs cannot change the	ir passwords	
	🔘 Use	rs can change their p	asswords	
	🔘 Use	rs must change their	passwords	
Lifetime (in days) :		<u>^</u>		
Authentication periods allo	wed			
Minimum duration :	15	÷	minute(s)	
Maximum duration :	240	÷	minute(s) ¥	
For transparent authenticati	on: 240	<u>^</u>	minute(s)	
△ Advanced properties –				
	Allo:	w access to the .PAC	file from internal interfac	es
liser enrolment				
user enronnent				
	© D	o not allow user enro	ment	
	⊚ AI	low Web enrolment fo	or users	
	(A)	low Web enrolment fo	or users and create their	certificates
Natification of a new enco				
inouncation of a new enrol	none none	9	*	

2. Validez en cliquant sur le bouton Appliquer.

🕦 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 :

🔊 Validate 🔇 Reject 🧿 Ignore 🧬 Refresh Select all			
	Туре	CN User	
	User	John DOE	
7	Certificate	John DOE	

- 1. Cochez les cases des demandes de création d'utilisateur et de certificat devant être approuvées,
- 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 :



ENROLMENT			
🔿 Validate 🔇 Reject 💿 Ignore 🍣 I	Refresh Select all		
Туре	CN User		
User User	John DOE		
Certificate	John DOE		
L			
User identifier format for empty ID	fields		
Identifier format :	%f.%l		
Example :	john.doe		
- E-mail potification			
Send an e-mail to the user :	vhen approving/rejecting user's enrolment request		
	when approving/rejecting user's certificate request		

🕦 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 :

🔿 Validate 😯 Reject 💿 Ignore 🍣 Refresh Select all				
	Туре	CN User		
	User	John DOE		
	Certificate	John DOE		

- 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** :



CERTIFICATES AND PKI			
Search X Filter: All + Ad	id 🕶 🔀 Delete	🚍 Actions 🗸 🛛 🏪 Download 🗸	Check usage
SSL proxy default authority	DETAILS	Create or renew a CRL	
Issivpn-full-default-authority		Remove the CRL	
UsersAuthentication	Maliatia	Set as default	
4 🛅 MyCompanyCA	validity -		
🚯 John Doe	Last update :		
	Next update :		

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 :

ertificate Revocation List	×	Certificate Revocation List	— ×	
General Revocation List		General Revocation List		
8- Certificate Revocation List Information		Revoked certificates:		
		Serial number	Revocation date	
Field Value	·	00 e8 54 7c 7a 00 e8 54 7c 7b	Friday, December 11, 2 Friday, December 11, 2	
Version V2 Issuer MyCompanyCA, Users, MyCompa Effective date Monday, December 14, 2015 10:2		00 e8 54 7c 7c	Friday, December 11, 2	
Next update Wednesday, January 13, 2016 10	E	Revocation entry		
Signature hash alg sha256 Signature hash alg 04		Field Va	lue	
Authority Key Iden KeyID=10 cc ab fc 30 48 4c 1c fa Elssuer Alternative No alternative name	-			
Value:		Value:		
Learn more about certificate revocation list				
	ок		ОК	

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** :

🐇 STORMSHIELD				
Login / Logout You can authenticate or change your password	AUTHENTICATION			
💄 New User	Please authenticate 🕐			
Request network authorization	Username			
Certificates	Authentication duration 4 hours -			
Get or request your authentication certificate	Login Logout			



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 mort 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** :

👹 STORMSHI	ELD
Zucgin / Logout You can authenticate or change your password	CERTIFICATE
New User Request network authorization	Download certificate now Email or Username john.doe
Certificates Get or request your authentication certificate	Download certificate now Download your company's certificates
	Your company's certification authority Certificate revocation list of your company
	Request a certificate
	 If you have not already asked for a certificate or if it is going to expire soon, you can request one by dicking here

🕦 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 fiewall). 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** :

CERTIFICATES AND PKI					
Search	🗙 💽 Filter: All 👻 💠 A	dd 🔻 🔀 Delete		Actions - 🔤 Download -	Check usage
SSL proxy default au	thority	DETAILS	-	Create or renew a CRL	
Issivpn-full-default-au	thority		⊠	Remove the CRL	
UsersAuthentication		Validity			
4 🛅 MyCompanyCA		- validity -		oor do donada	
🚯 John Doe		Lastundate			
		Luciupuuto			
		Next update			

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 :**

Base64 format (PEM)
•••••

- 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 :

<u>t</u>	Your file is available on the link below. (remarks: these file downloads do not support browser plugin downloader) <u>Download MyCompanyCA pem</u>
----------	---

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

CERTIFICATES AND PKI		
•		
Search X Filter: All -	🕇 Add 🕶 🔀 Delete 🛛 🚍 Actions 🕶	强 Download 🗸 💿 Check usage
SSL proxy default authority	DETAILS CRL PROPE	RTIES
Issivpn-full-default-authority		
MyCompanyCA	M-R-R-R	
	validity	
	Last update :	Thu Dec 03 2015 10:43:05 GMT+0100
	Next update :	Sat Jan 02 2016 10:43:05 GMT+0100
	DISTRIBUTION POINTS	
	index URI	
	1 https://192.168.5	6.250/auth/certificaterevocationlist.crl
	REVOKED CERTIFICATES	
	Serial number Revocation	on date
	C3133D81 Thu Dec I	03 2015 09:42:57 GMT+0100



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 :

Certificate Revocation List		×	Certificate Revocation List	
General Revocation List			General Revocation List	
Kertificate Revo	ocation List Information		Revoked certificates:	
S.			Serial number	Revocation date
Field	Value V2 MuCompanyCA Lisers MuCompa	<u>^</u>	00 e8 54 7c 7a 00 e8 54 7c 7b 00 e8 54 7c 7c	Friday, December 11, 2 Friday, December 11, 2 Friday, December 11, 2
Effective date Next update Signature algorithm	Monday, December 14, 2015 10:2 Wednesday, January 13, 2016 10 sha256RSA sha256	E	Revocation entry Field	Value
CRL Number Authority Key Iden Issuer Alternative	04 KeyID=10 cc ab fc 30 48 4c 1c fa No alternative name	-		
Value:			Value:	
Learn more about <u>certificate.</u>	revocation list		Learn more about <u>certificate re</u>	evocation list
		ОК	L	ОК

Configurer le logiciel SDS Suite

Créer un nouvel utilisateur dans SDS Suite

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

	Connect	
	Select Smart Card or USB Token	•
X	PNetwork access	►
	 <u>N</u>ew user account 	
Y	1 About Stormshield Data Security	

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

	Welcome to Stormshield Data Security. You are going to create a password access account.				
	Please indicate your choice for the account to be created: Use same key to encrypt and sign				
Stormshield Data Security					
	Create an account Cancel				

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.

	Identifier:	john.doe
	Secret code: 🔍	•••••
	Confirmation:	•••••
	Information	
	Password ana	alysis
mehiold	- 😕 Strength o	of password (59 bits)
Security	Presence	of digits
	- Special or	r accentuated characters

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** :

	Gene the in	erates your key ar nformation obtaine	nd the associated certificate with ad in the the following steps.
THE A		Key type:	RSA 2048 bits
0	 Impor Impo 	t your personal ke rt your key and th	e associated certificate included
•	Impor Impo in the M	t your personal ke rt your key and th selected file. <u>F</u> rom the file:	e associated certificate included
Stormshield Data Security	Importing Importing Importing Important Imp	t your personal ke rt your key and th e selected file. <u>F</u> rom the file: Password:	e associated certificate included JohnDoe.p12

🕦 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
Stormshield Data Security	





- 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 :

	You could indicate useful if you forget This password is N know it by heart, a known only to you	You could indicate a Security Officer password. This will be useful if you forget your main password. This password is VERY IMPORTANT. You do not need to know it by heart, and we advise you to keep it in a place known only to yourself.			
	 I want a Security 	ity Offic	er password:		
	Password:	٩	•••••		
	Confirm:		•••••		
Stormshield Data Security	I don't want a Security Officer password: CAUTION: without Security Officer password, if you your main password, the recovery procedure will no be available and your account will be blocked defin				

🚺 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.

	Check the operation summary below before continuing your account creation.	
francis	Personal key Import 'RSA 2048 bits' key	^
	□- <u>I</u> Certificate 	
	john.doe@mycompany.com MyCompany	
	Lille France (FR)	=
Stormshield	1 parent certificate checked	
Data Security	Point here to visualize the secret code Print here to visualize the Secret with Officer page	-
	Add this user to the list of meanth, exponented user	Ŧ

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

	Account 'john.doe' created successfully
Stormshield	Detail of account creation 'John Dec' Sure account created Ver account created Personal key imported Personal key certificate imported Address book Personal key certificate imported Personal key certificate for personal key imported
Data Security	You should backup the files in the folder: C/ProgramData /Users \ohn.doe

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...**

	Connect
	Select Smart Card or USB Token
X	Network access
	1 <u>N</u> ew user account
Y	1 About Stormshield Data Security

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** :

Stomshield Data	Security Config	guration Wizards		
Stormshield Data	control panel		9g (2-)))	≣
5	2	al a		
Connection	Key-holder	Address book	Revocation	
		~		
File	Shredder	Team		

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

als Trusted address book for John Doe						
File Edit Display						
New Properties Delete Import Export F	ind Display					
Certificates Authority Certificates group Contacts						
Common name 🤝 🚨 email address	Certified by	Description				
🔄 John Doe 🙎 🔒 john.doe@mycompany.com MyCompanyCA						
1 element(s)		📽 Verification completed.				

🕦 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** :

Address books configuration		
John Doe John Doe Trusted address book New directory Access Advanced	LDAP dir	ectory
Attributes	Address: Port No:	192.168.56.250 389
	☑ Use this	directory for automatic searches
		OK Cancel Apply

- 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.

Address books configuration		
☐	Access contro	ol
Advanced Attributes Mew directory	Identifier:	cn=NetasqAdmin,o=MyCompany,dc=myco
	Password:	•••••
4		OK Cancel Apply

 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.

Address books configuration		
Dohn Doe Don Tusted address book Doe Doe Trusted address book O	Aliases for sea	nch attributes mail
	Common name:	cn usercertificate:binary
۲	0	K Cancel Apply

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 ?
DefaultPathl=C:\ProgramData\Arkoon\Security BOX\Users RootPathl=C:\ProgramData\Arkoon\Security BOX\Users ShowBrowse=1 ShowLastUsers=5 [CRL]
CRLDatabaseModel=C:\ProgramData\Arkoon\Security BOX\Users\default\default.bcrl TmpCRLPath=C:\ProgramData\Arkoon\Security BOX\CRL DeleteTmpCRL=1 LDAPTimeOut=60 [TEAM] ExcludedPath=<%APPDATA%> [SBOX.NewUserWizardExGP2] AllowNewUser=1 Pkcsl2tmport=1



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



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



🕦 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

 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.

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

 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.

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...

Fichier	Machine 8	Écran	Entrée	Périp	hériques	Aide	
🚡 certm	ngr - [Certifica	ates - C	urrent Use	er\Tru	sted Publi	shers]	
File A	ction View	Help	•				
(= =	Find Certi	ficates.					
	All Tasks		×		Find Cert	tificates	
	Refresh				Import		
	Export List	t					
	Help			ities			
TI	rusted Publish	hers					
🕨 🧮 N	ntrusted Certi	ificates					

- 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).

🧟 certmgr - [Certificates - Current User\Trusted Publishers\Certificates]						
File Action View Help						
🗊 Certificates - Current User	Issued To	Issued By	Expiration Date			
Personal	🔄 U30SXA02D0016A7	NETASQ Firewall Certification Authority	4/6/2022			
Forterprise Trust						
Intermediate Certification Authorities						
Active Directory User Object						
Trusted Publishers						
Certificates						

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.

Persona	l key	Decryption	OpenPGP ke	yring Re	covery		
R	Your recovery keys						
	These keys are always used in addition to your own, for all yo encryption operations.						
	A						
	Available operations for this key						
	9	Operations I	► I	mport a k	ey		

- 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 :



SNS - NOTE TECHNIQUE SDS EASY : INTÉGRER UNE PKI SNS DANS UN CLIENT SDS





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,.
- 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.

1 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.

1 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.

🕦 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.
- 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 chaine 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**.

🗙 MY FAVORITES -		
CONFIGURATION -	CONFIGURATION BACKUP RESTORE	SYSTEM UPDATE
× E		
R DASHBOARD	Configuration backup	
🛞 SYSTEM	Backup filename :	V50XXA3E0000011_2014-09-04.na
Configuration		Download the configuration backup
 Administrators 	— ▽ Advanced properties ————————————————————————————————————	
License		
Maintenance	Configuration sutematic backup	
 Active Update 	Configuration automatic backup	
 High Availability 	Enable automatic backup	
CLI	Backup server selection :	Cloud backup
		Customized server
	Server URL :	Backup Cloud server
OBJECTS	Backup server :	~ 6

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**.

1 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.



Cloud backup		
Customized server		
Backup Cloud server		
autobackup2008	~	₽,
	 Cloud backup Customized server Backup Cloud server autobackup2008 	 Cloud backup Customized server Backup Cloud 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.





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.