



STORMSHIELD

Network Endpoint Data



GUIDE DE DÉMARRAGE RAPIDE SDS Enterprise 9.1.X

Stormshield Data Security Enterprise

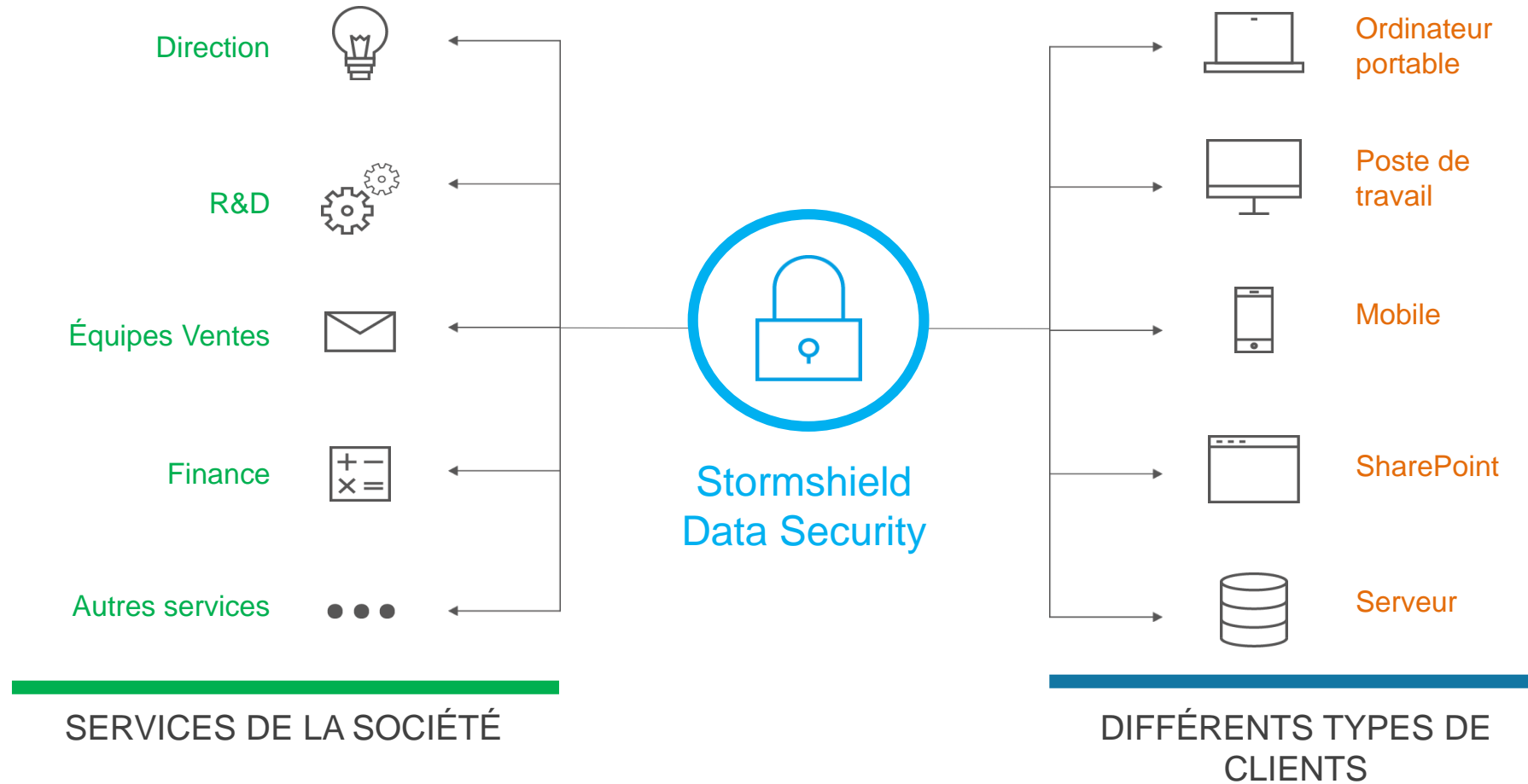


Table des matières

- [Introduction](#)
- [Configuration technique requise](#)
- [Architecture de la validation de principe \(POC\)](#)
- [Installer le serveur IIS](#)
- [Installer le serveur SDAM](#)
- [Installer la Suite SDS sur le poste de travail d'administration](#)
- [Créer la PKI racine](#)
- [Configurer Internet Explorer et initialiser la PKI racine](#)
- [Initialiser une PKI enfant \(option\)](#)
- [Configurer le répertoire virtuel du serveur IIS](#)
- [Configurer le serveur Exchange \(option\)](#)
- [Créer des comptes SDS spéciaux](#)
- [Définir la configuration de compte SDS](#)
- [Créer des modèles de compte SDS](#)
- [Créer des comptes d'utilisateur SDS](#)
- [Déployer des comptes d'utilisateur SDS](#)
- [Installer le poste de travail client](#)
- [Installer le compte SDS](#)
- [Connexion initiale](#)
- [Cas d'usage – Démonstration](#)
- [Support](#)
- [Démarrer la base de données du serveur SDAM](#)



An abstract geometric diagram on the left side of the slide. It consists of several light blue circular nodes connected by thin white lines. The nodes are arranged in a way that suggests a network or a series of interconnected points. One node is at the top left, another is below it, and a third is further down and to the left. Lines connect these nodes to each other and to other nodes that are partially visible on the left edge of the frame.

Introduction

Glossaire

- CRL : Certificate Revocation List (Liste de révocation des certificats)
- EXE : Format de fichier d'installation non personnalisé pour l'agent SDS
- GPO : Group Policy Object (Objet Stratégie de groupe)
- MSI : Format de fichier d'installation personnalisable pour l'agent SDS
- PKI : Public Key Infrastructure (Infrastructure à clés publiques)
- SDAM : Stormshield Data Authority Manager
- SDS : Stormshield Data Security
- SDSe : SDS version Enterprise
- SGBD : Système de gestion de base de données
- SMTP : Simple Mail Transfer Protocol
- USI : Format de fichier d'installation de compte SDSe
- USX : Format de fichier de mise à jour de compte SDSe



Liste des variables

- Recherchez les variables suivantes et remplacez-les par vos propres valeurs pour personnaliser automatiquement la configuration décrite dans ce document :

- *%IP_SDAM*
- *%HOSTNAME_SDAM*
- *%IP_SQL*
- *%HOSTNAME_SQL*
- *%IP_LDAP*
- *%HOSTNAME_LDAP*
- *%IP_MAIL*
- *%HOSTNAME_MAIL*

- *%IP_CLIENT1*
- *%HOSTNAME_CLIENT1*
- *%USERNAME_CLIENT1*
- *%IP_CLIENT2*
- *%HOSTNAME_CLIENT2*
- *%USERNAME_CLIENT2*



Objectif de ce document

- Ce document est conçu pour guider les utilisateurs finaux ou les partenaires afin qu'ils comprennent l'installation, la configuration et l'utilisation de SDSe.
- Il s'agit du guide de démarrage rapide pour établir une validation de principe (POC). Il présente les notions de base pour vous aider à rapidement comprendre le fonctionnement de SDSe.
- Il ne répertorie pas tous les cas d'usage ni toutes les options du produit, mais contient suffisamment d'informations pour vous permettre d'installer SDSe sans avoir reçu de formation certifiante.
- Durée nécessaire pour le POC :
 - 1 jour pour l'installation
 - 1 jour pour tester toutes les fonctionnalités



Détails de la validation de principe (POC)

- Le POC SDSe indique les différentes étapes à suivre pour installer le serveur :
 - Configuration d'un serveur Microsoft IIS
 - Installation d'une PKI (contenue dans le SDAM)
 - Installation d'un poste de travail d'administration qui se connecte au SDAM (PC sous Windows 10)
 - Installation d'un poste de travail utilisateur (PC sous Windows 10)





Configuration technique requisite

Stormshield Data Authority Manager

- **Vous pouvez installer le SDAM sous :**
 - Windows 7 (32 et 64 bits)
 - Windows Server 2008 R2 (64 bits)
 - Windows Server 2012 R2 (64 bits)
- **Éléments nécessaires :**
 - Serveur Web Microsoft IIS version 7.0 ou supérieure
- Ce serveur peut être virtualisé.
- Un compte doté de droits d'administrateur est nécessaire.



Stormshield Data Security Suite

- Un compte doté de droits d'administrateur est nécessaire.
- Vous pouvez installer SDS 9.1.X sous :
 - Windows 7 SP1 (32 ou 64 bits)
 - Windows 8.1 (32 ou 64 bits)
 - Windows 10 (32 ou 64 bits)
- Le module Stormshield Data Mail est compatible avec Outlook (2010 et supérieur).

Outlook

- Pour Outlook 2010 :
 - Office 2010 Service Pack 2
 - KB2597137 (<http://support.microsoft.com/kb/2597137>)
 - KB2881055 (<http://support.microsoft.com/kb/2881055>)
- Pour Outlook 2013 :
 - Office 2013 Service Pack 1
 - KB2878323 (<http://support.microsoft.com/kb/2878323>)
 - KB2881040 (<http://support.microsoft.com/kb/2881040>)



Outlook 2010

Stormshield Data Security	9.1.3		9.1.4	
Service Pack min pour Microsoft Office 2010	SP1	SP2	SP1	SP2
KB Microsoft obligatoires	2597137 2881055	2881055	2597137 2881055	2881055
Version min de SQL Server Compact	Édition 4.0		Édition 4.0	
Version min de Visual Studio 2010 Tools for Office Runtime	VSTO Runtime 4.0		VSTO Runtime 4.0	
Version min de .NET Framework	4.5.2		4.5.2	



Outlook 2013

Stormshield Data Security	9.1.3	9.1.4
Service Pack min pour Microsoft Office 2013	SP1	SP1
KB Microsoft obligatoires	KB2878323 KB2881040	KB2878323 KB2881040
Version min de SQL Server Compact	Édition 4.0	Édition 4.0
Version min de Visual Studio 2010 Tools for Office Runtime	VSTO Runtime 4.0	VSTO Runtime 4.0
Version min de .NET Framework	4.5.2	4.5.2



Outlook 2016

Aucun prérequis



ACTIVE X (obligatoire)

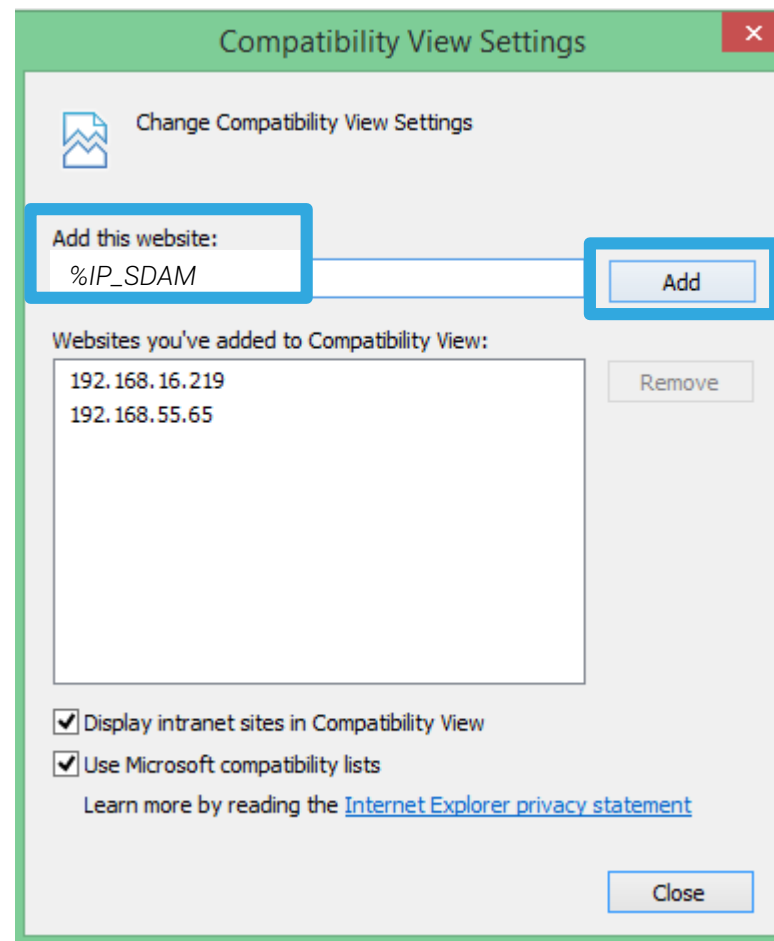
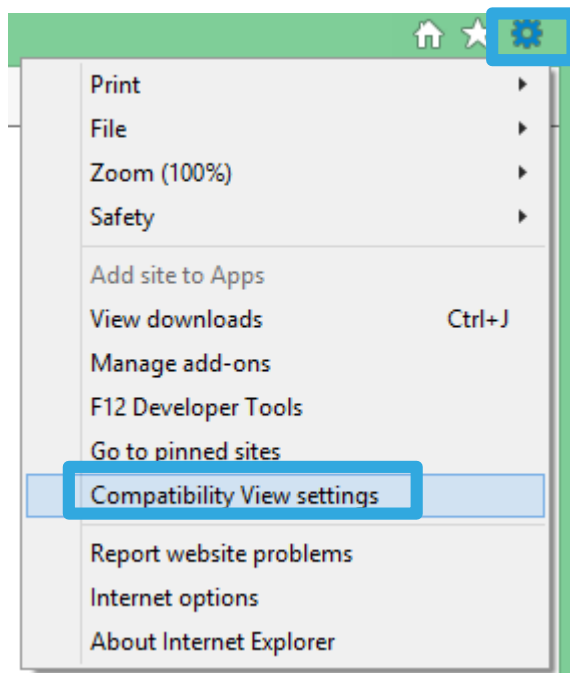
- Réservé à l'administration et aux administrateurs de la solution SDAM.
- Pour accéder à l'interface Web SDAM, le poste de travail doit pouvoir installer un contrôle ActiveX non signé (signé par Stormshield mais pas par Microsoft).
- L'URL du SDAM doit être déclarée comme site de confiance dans IE.
- Des droits d'administrateur sont nécessaires sur l'ordinateur et il ne doit exister aucun GPO restreignant l'utilisation d'Internet Explorer.



INTERNET EXPLORER

Dans Internet Explorer 11, l'URL ou l'adresse IP du serveur SDAM doit être définie dans **Paramètres d'affichage de compatibilité**.

Cliquez sur **Paramètres** → **Paramètres d'affichage de compatibilité**



ACCÈS LDAP (facultatif)

- Le SDAM doit disposer d'un accès en lecture/écriture sur le serveur LDAP pour pouvoir importer des utilisateurs et exporter des certificats utilisateur (dans l'attribut « UserCertificates »).
- Les comptes SDS doivent avoir un accès en lecture seule sur les champs « UserCertificates » pour télécharger les certificats d'autres utilisateurs (l'opération est possible avec des comptes d'utilisateur).



ACCÈS SMTP (facultatif)

- Le SDAM doit pouvoir accéder à un serveur SMTP ou à un relais SMTP pour envoyer des e-mails aux administrateurs et aux utilisateurs (le SDAM peut uniquement envoyer des e-mails, pas en recevoir ; vous n'avez pas besoin de boîte aux lettres pour le SDAM).



PUBLICATION DE CRL

- Si vous avez besoin d'échanger des données sécurisées avec des utilisateurs externes, la CRL doit être publique.
- Sur un serveur Web, la CRL doit être disponible pour téléchargement gratuit (par exemple, à l'adresse <http://www.societe.com/sdsCRL.crl>).
- Il s'agit d'un fichier .crl (SDS le télécharge), alors vous n'avez pas besoin de page Web.
Exemple : <http://crl.stormshield.eu/stormcorpdatasec.crl>



Architecture de la validation de principe (POC)

MATRICE DE CONNEXIONS

- Pour un SDAM situé derrière un firewall et jouant le rôle de PKI :
 - Ouvrez une connexion HTTP (ou HTTPS) permettant à un administrateur d'accéder à l'interface Web d'administration.
Connexion : « Station admin » vers SDAM sur HTTP/HTTPS
 - Ouvrez une connexion SMTP pour que les utilisateurs puissent recevoir des fichiers *.usi* (programme d'installation du compte d'agent SDS) par e-mail.
Connexion : SDAM vers « Serveur d'e-mail » sur SMTP
 - Ouvrez une connexion LDAP (ou LDAPS) pour la distribution du certificat public.
Connexion : SDAM vers « Serveur AD » sur LDAP/LDAPS
 - Définissez le transfert de fichiers afin de retransmettre les fichiers *.usx* (fichier de mise à jour de l'agent SDS) ou l'annuaire Web disponible.
- Vous disposez de trois méthodes pour télécharger la CRL :
 - HTTP/HTTPS
 - LDAP/LDAPS
 - Transfert de fichiers

DIAGRAMME DE POC

SDAM
(Serveur/IIS/LDAP/PKI – 1 CA)
Windows 2012 R2



%IP_SDAM
%HOSTNAME_SDAM

%IP_CLIENT1
%HOSTNAME_CLIENT1
%USERNAME_CLIENT1



Ordinateur portable

SDSe sur PC-Win-1
Poste de travail admin
Windows 10



Ordinateur portable

SDSe sur PC-Win-2
Poste de travail utilisateur
Windows 10

%IP_CLIENT2
%HOSTNAME_CLIENT2
%USERNAME_CLIENT2

Diagramme des meilleures pratiques

SDAM
(Serveur/IIS/PKI –
1 CA et 1 CA enfant)
Windows 2012 R2



%IP_SDAM
%HOSTNAME_SDAM

SQL
Server



%IP_SQL
%HOSTNAME_SQL

Serveur
AD/LDAP



%IP_LDAP
%HOSTNAME_LDAP

Serveur
d'e-mail



%IP_MAIL
%HOSTNAME_MAIL

%IP_CLIENT1
%HOSTNAME_CLIENT1
%USERNAME_CLIENT1

SDSe sur PC-Win-1
Poste de travail admin
Windows 10

Ordinateur
portable

SDSe sur PC-Win-2
Poste de travail utilisateur
Windows 10

Ordinateur
portable

%IP_CLIENT2
%HOSTNAME_CLIENT2
%USERNAME_CLIENT2

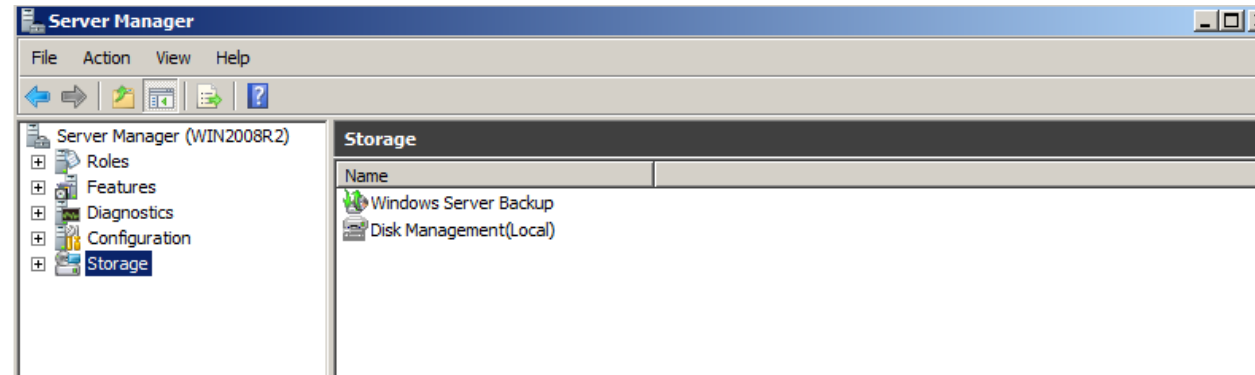


Installer le serveur IIS

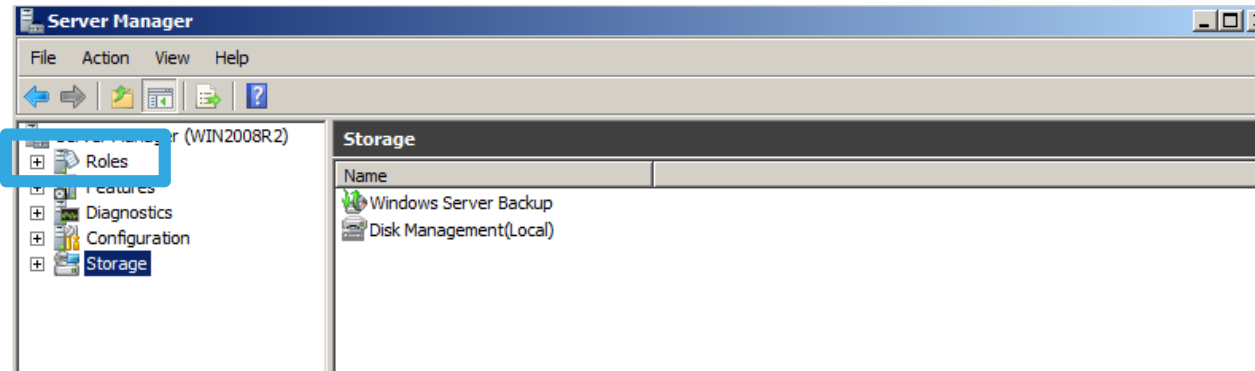
Installer le serveur IIS

Vous devez installer et configurer un serveur IIS pour que la console d'administration SDAM fonctionne correctement (la capture d'écran ci-dessous a été prise sous Windows Server 2008 R2).

Cliquez sur Démarrer → Outils d'administration → Gestionnaire de serveur.

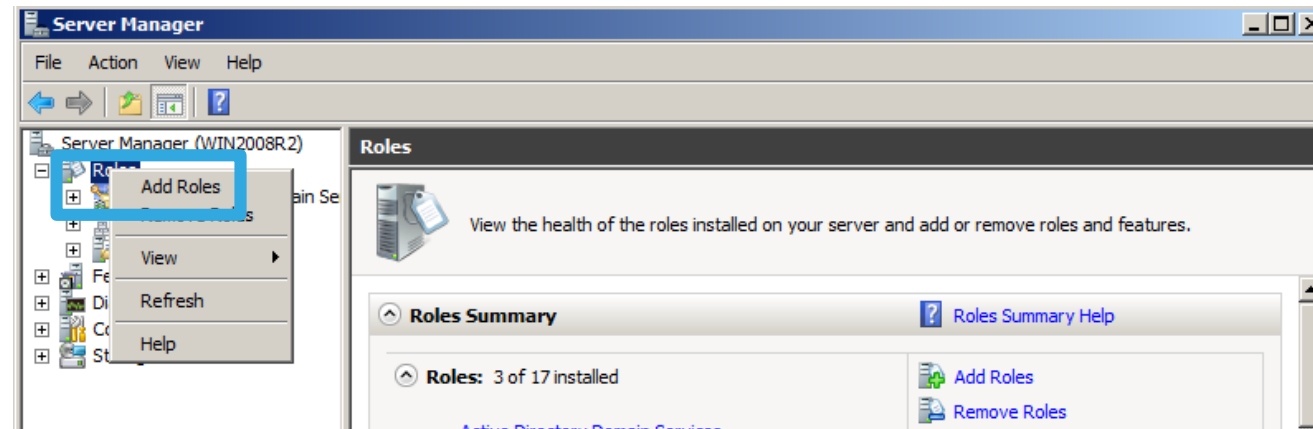


Cliquez sur Rôles.

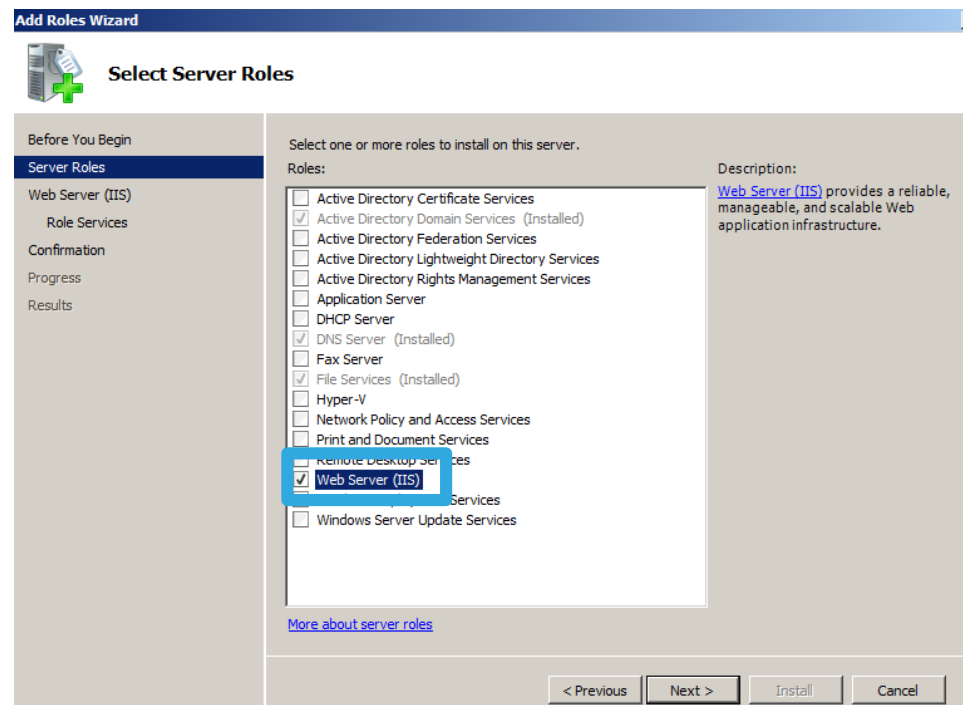


Installer le serveur IIS (suite)

Faites un clic droit sur **Rôles** et sélectionnez **Ajouter des rôles**.

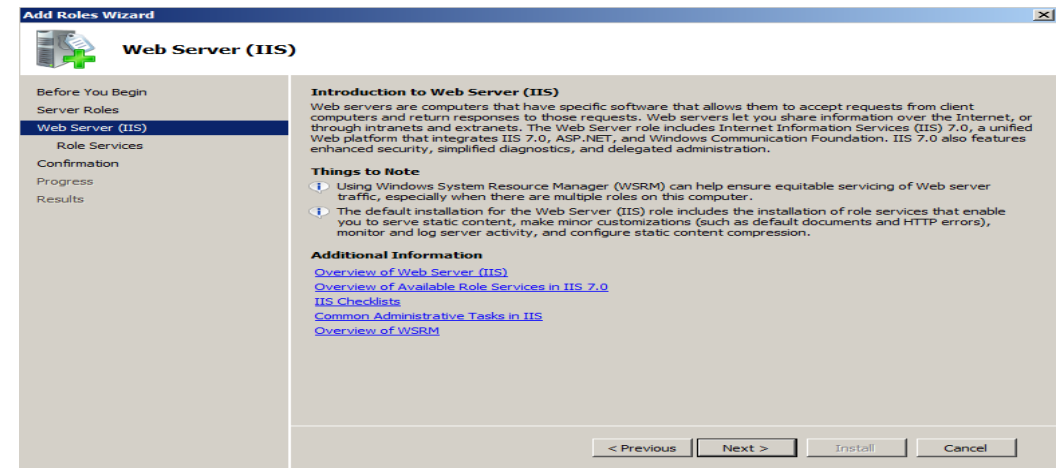


Sélectionnez **Serveur Web (IIS)** et cliquez sur **Suivant**.



Installer le serveur IIS (suite)

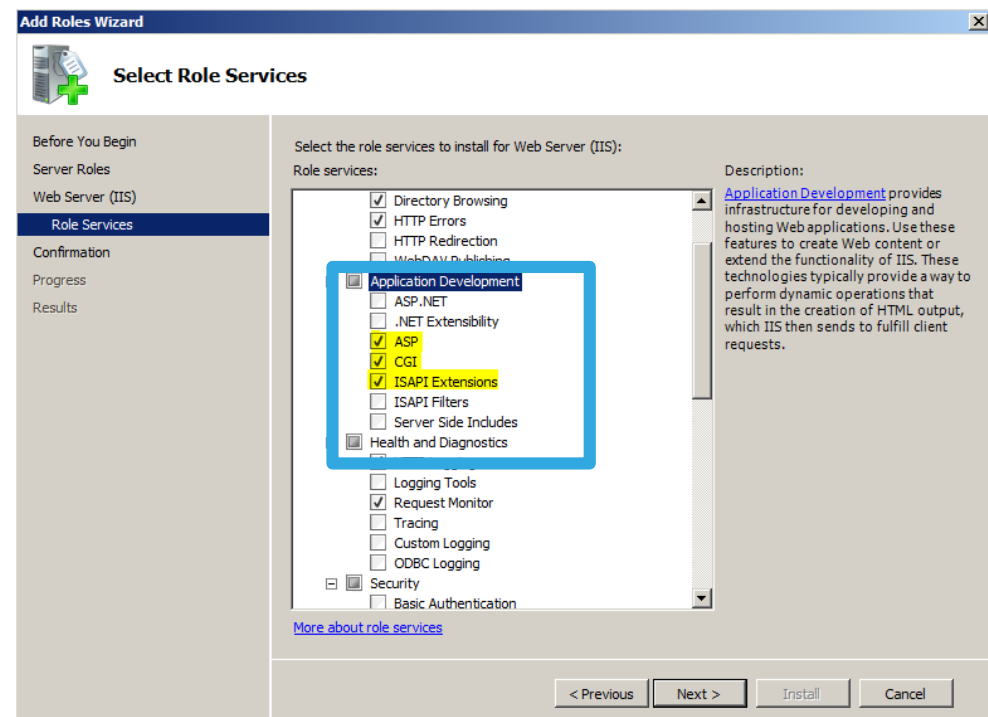
Cliquez de nouveau sur **Suivant**.



À l'étape **Services de rôle**, conservez toutes les options sélectionnées par défaut, en ajoutant ce qui suit :

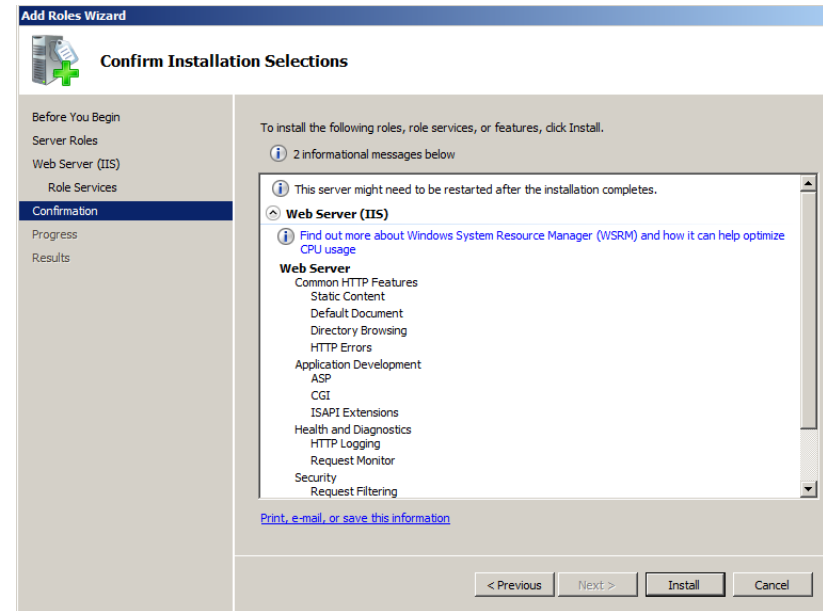
1. **Développement d'applications** : sélectionnez **ASP**, **CGI** et **extension ISAPI**.
2. **Fonctionnalités HTTP communes** : assurez-vous que l'option **Contenu statique** est sélectionnée (sinon, sélectionnez-la).
3. **Sécurité** : assurez-vous que l'option **Filtrage des demandes** est sélectionnée (sinon, sélectionnez-la).

Après avoir vérifié que toutes les options sont correctement sélectionnées, cliquez sur **Suivant**.

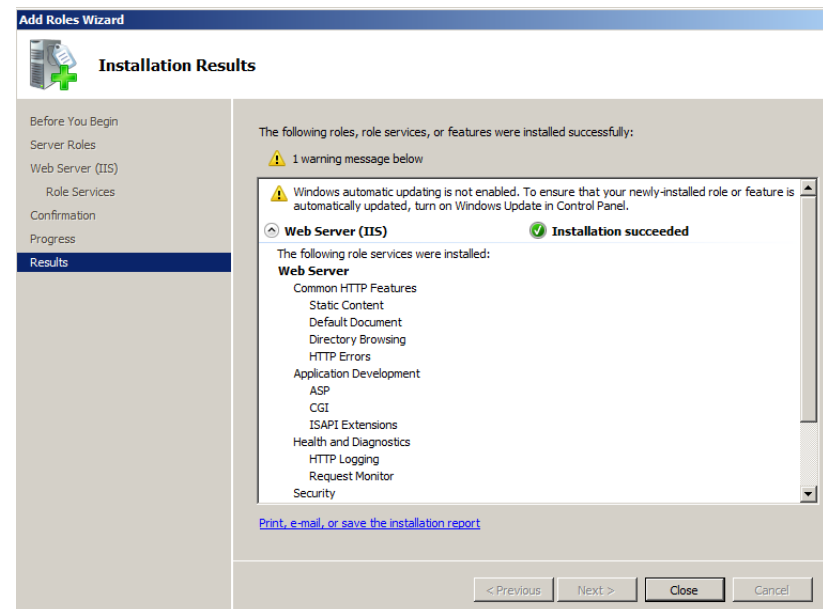


Installer le serveur IIS (suite)

Cliquez sur **Installer** pour démarrer l'installation d'IIS.



Vérifiez que le message **Installation réussie** s'affiche bien, puis cliquez sur **Fermer**.





Installer le serveur SDAM

Installer le serveur SDAM

Lancez une invite de commande avec droits d'administrateur, puis exécutez le programme d'installation via la commande suivante : `msiexec /i "Stormshield Data Authority Manager 9.12.688.msi"` (le nom du fichier `.msi` peut varier en fonction de la version du SDAM).

```
Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd ..

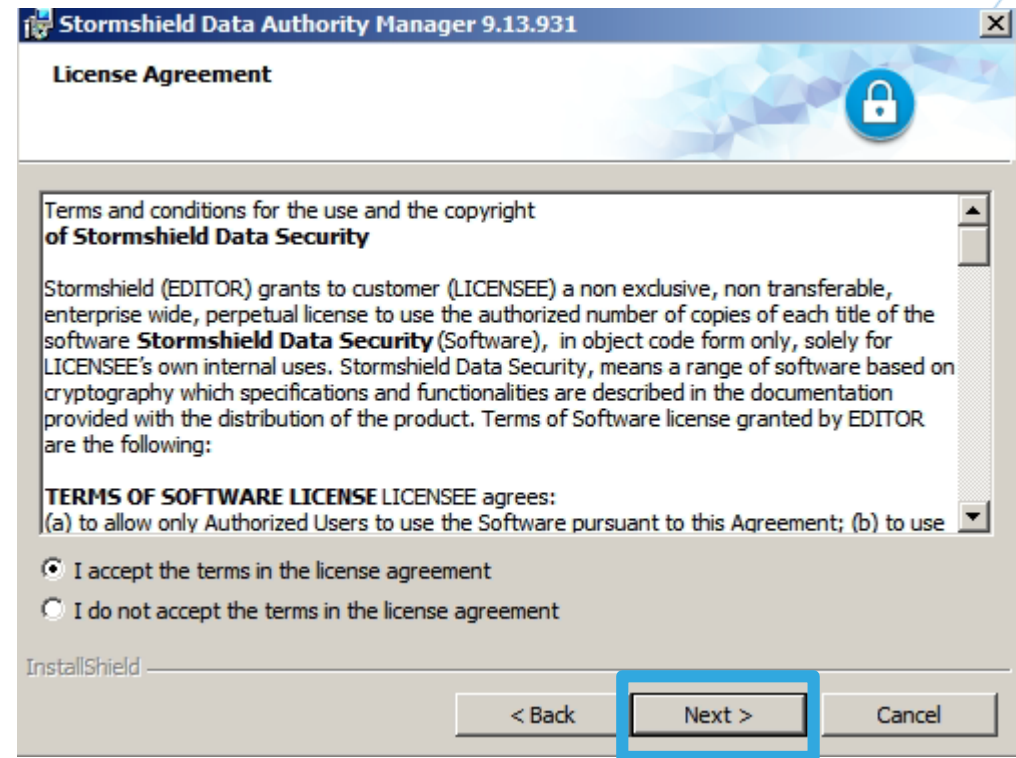
C:\Windows>cd ..

C:\>cd "Stormshield_Data_Authority_Manager_9.13.931_ENU_OFFICIAL_INTERNE(1)"

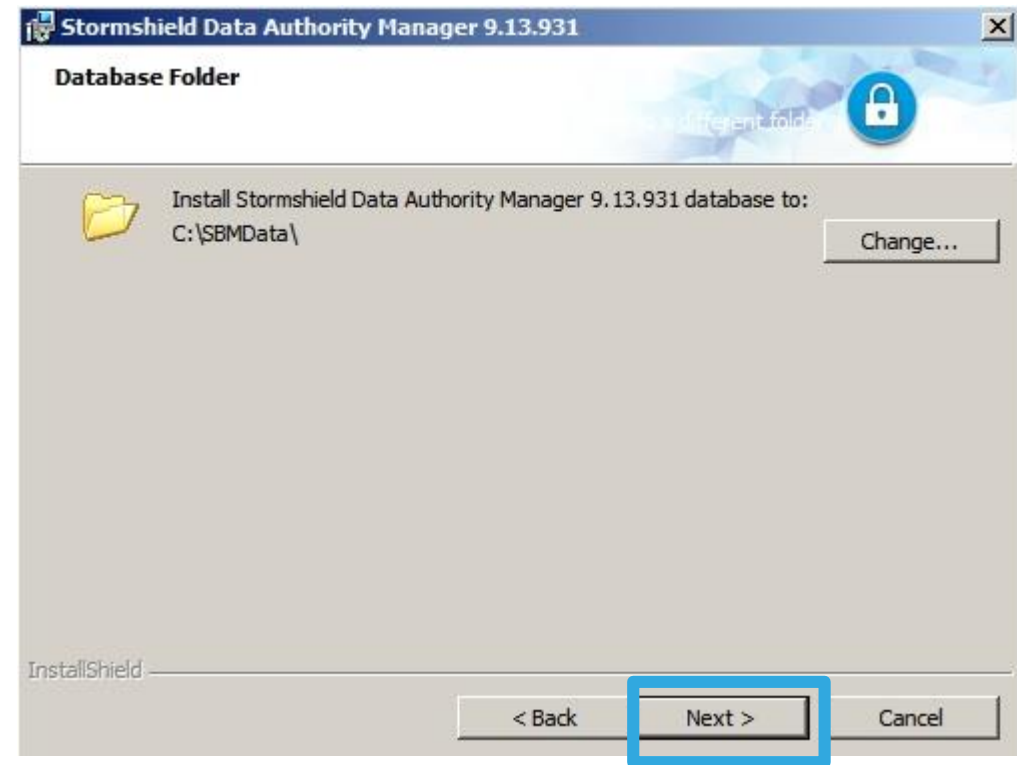
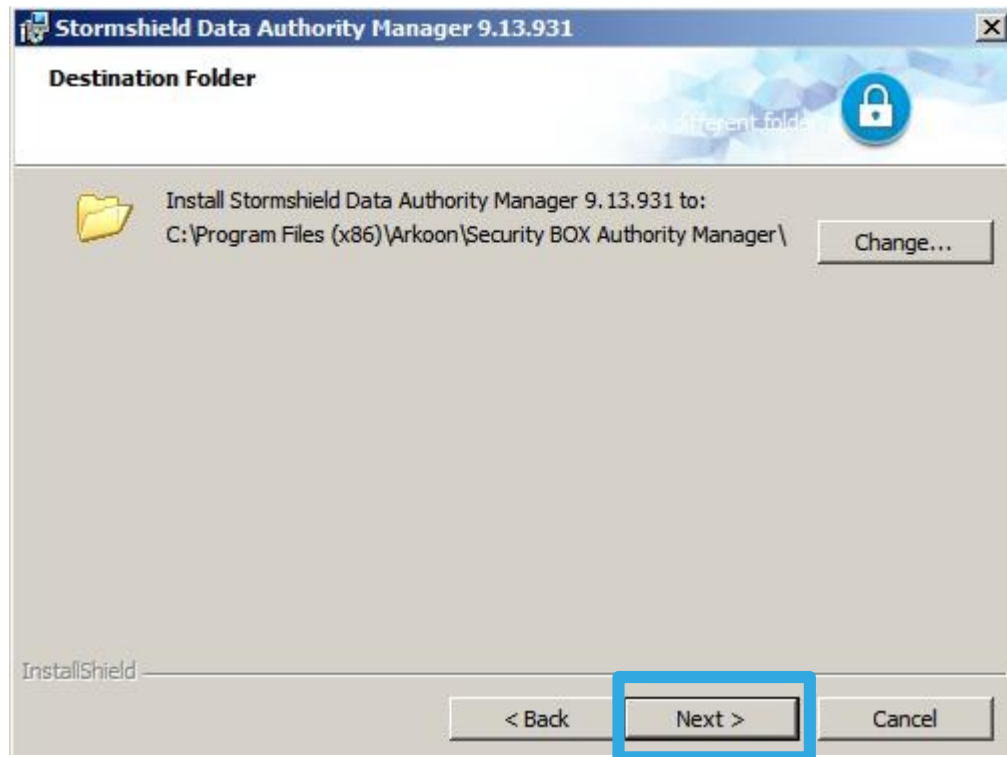
C:\Stormshield_Data_Authority_Manager_9.13.931_ENU_OFFICIAL_INTERNE(1)>msiexec /
i "Stormshield Data Authority Manager 9.13.931.msi"
```



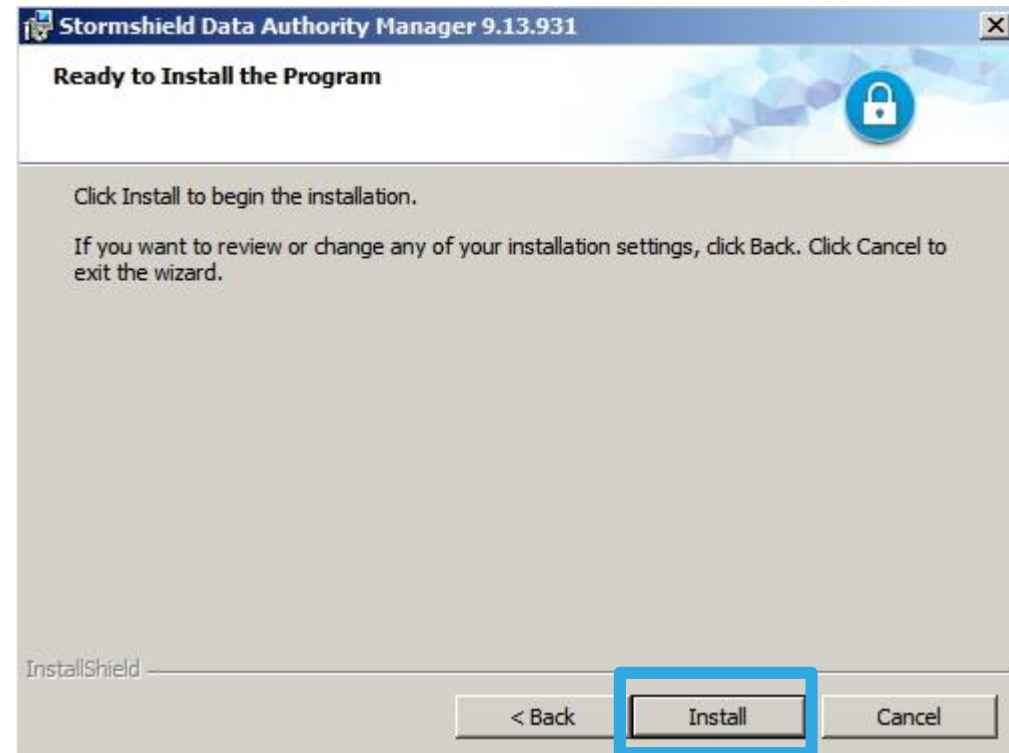
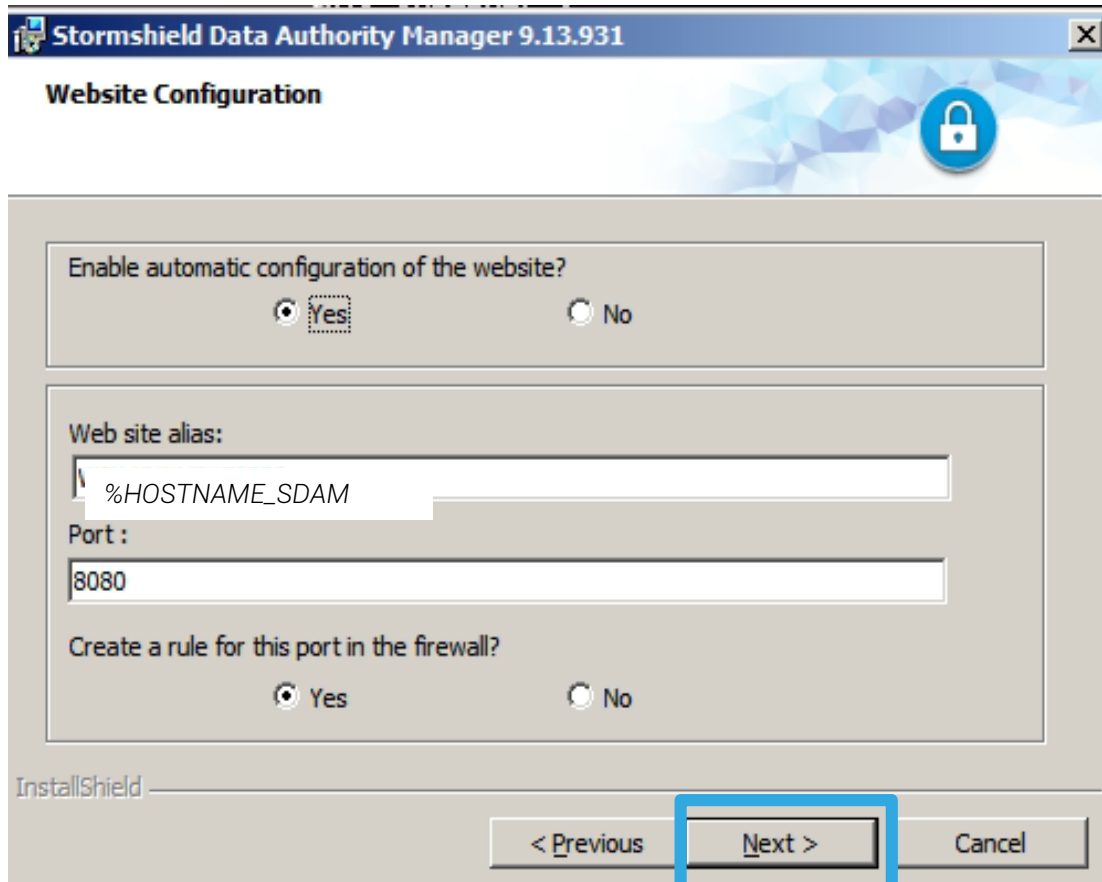
Installer le serveur SDAM (suite)



Installer le serveur SDAM (suite)



Installer le serveur SDAM (suite)



Installer le serveur SDAM (suite)

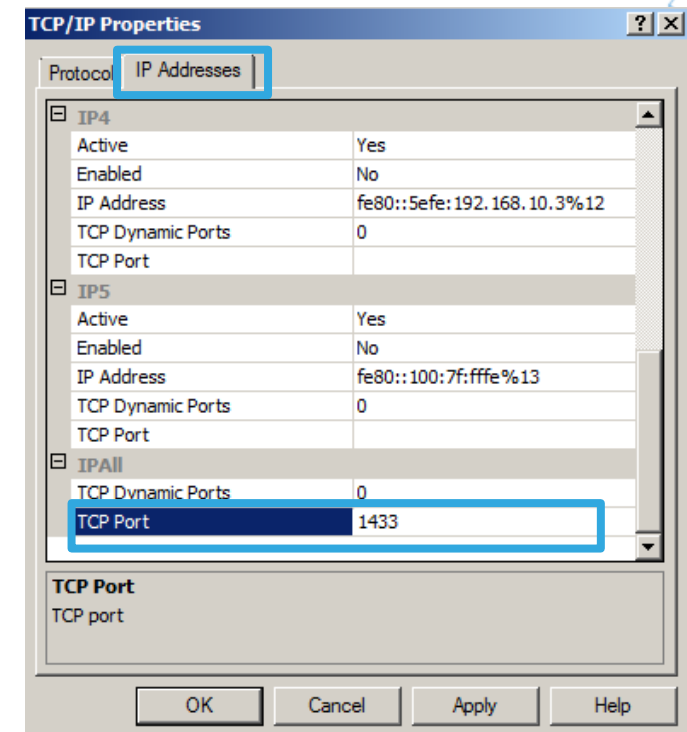
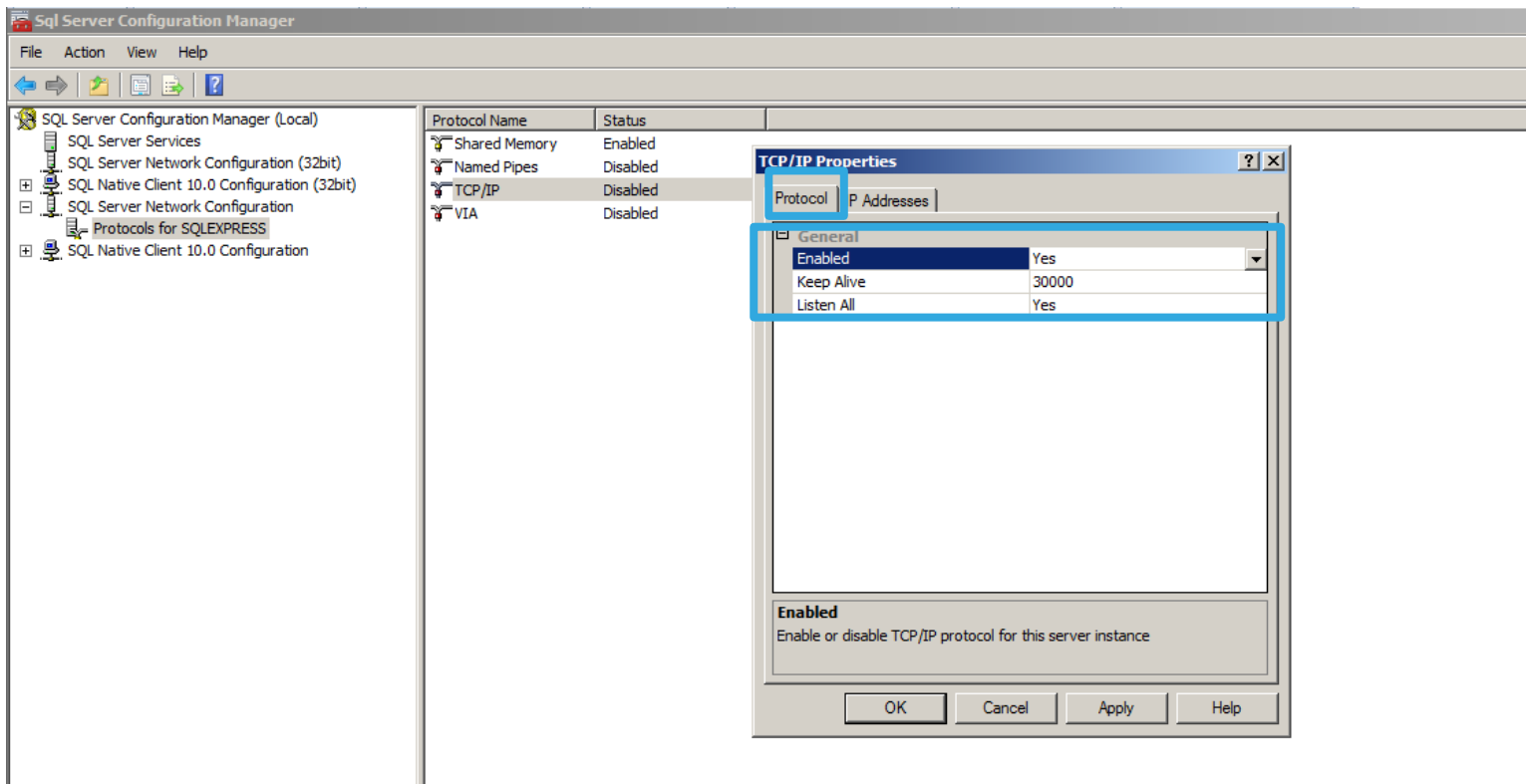


Option : Recommandations pour SQL Server

Dans le cas d'une installation de démo ou de validation de principe (POC), ignorez cette étape. Autorisez les connexions réseau entrantes depuis le serveur **%HOSTNAME_SDAM**.

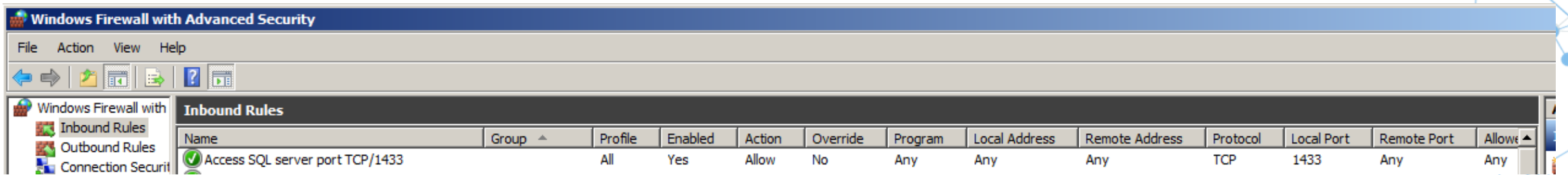
Dans cet exemple, la base de données s'appelle « SQLEXPRESS ».

Dans la même fenêtre **Propriétés TCP/IP**, cliquez sur le deuxième onglet.



Option : Recommandations pour SQL Server

Dans le cas d'une installation de démo ou de validation de principe (POC), ignorez cette étape. Sur le serveur où SQL est installé, créez une règle de firewall pour autoriser le trafic entrant sur le port 1433.



Option : Recommandations pour SQL Server (suite)

- Script pour la création de la base, disponible dans le répertoire suivant :
C:\Program Files (x86)\Arkoon\Security BOX Authority Manager\Database = <path>
- Création de la base en ligne de commande :
sqlcmd -S myServer\instanceName -d Database
-i <path>\create_database_SqlServer.sql



Option : Recommandations pour SQL Server (suite)

- Création de la base avec Microsoft SQL Management Studio

The screenshot displays the Microsoft SQL Server Management Studio (SSMS) interface. The main window shows a SQL script titled "create_database_SqlServer.sql" with the following content:

```
-- SQL script for Microsoft SQL Server database --  
  
-- BEGIN TRAN ARKOON_TABLES;  
  
-- TABLES --  
  
CREATE TABLE ACCOUNTS (  
    szUserID          NVARCHAR(32) NOT NULL,  
    iAccountAlgoCryptID INT NOT NULL,  
    iAccountAlgoHashID INT NOT NULL,  
    PRIMARY KEY (szUserID)  
);  
  
CREATE TABLE ADMINISTRATORS (  
    iAdminID          INT NOT NULL,  
    szAdminName       NVARCHAR(64) NULL,  
    iAdminType        INT NOT NULL,  
    szUserID          NVARCHAR(32) NULL,  
    sztcAdminCertifValue NVARCHAR(max) NULL,  
    sztcAdminKeyId    NVARCHAR(max) NULL,  
    iAdminState       INT NOT NULL,  
    sztcAdminRights   NVARCHAR(64) NULL,  
    PRIMARY KEY (iAdminID)  
);  
  
CREATE TABLE ADMINISTRATORSPARAMSCLEAR (  
    iAdminID          INT NOT NULL,  
    szParamID         NVARCHAR(250) NOT NULL,  
    szParamValue      NVARCHAR(max) NULL,  
    iParamValue       INT NULL,  
    PRIMARY KEY (iAdminID, szParamID)  
);  
  
CREATE TABLE ALGOS (  
    iAlgoID           INT NOT NULL,  
    bAlgoIsForCrypt   INT NOT NULL,  
    bAlgoIsForHash    INT NOT NULL,  
    bAlgoIsForKey     INT NOT NULL,  
    bAlgoIsForBase    INT NOT NULL,  
    bAlgoIsForHash    INT NOT NULL
```

The interface also shows the Object Explorer on the left, displaying the server structure for "SRV-WIN2012\SQLEXPRESS (SQL Server 11.0.2100 - SRV-WIN2012\Administrateur)". The Properties window on the right shows connection parameters for "SRV-WIN2012\SQLEXPRESS (SRV-WIN2012\Administrateur)".



Installer la Suite SDS sur le poste
de travail d'administration

Installer la version d'évaluation

Installez la version DEMO de l'agent SDS sur le poste de travail que vous allez utiliser pour configurer le SDAM à l'aide de l'interface Web d'administration.

To view your download, click on a category below :

STORMSHIELD NETWORK SECURITY
STORMSHIELD DATA SECURITY
STORMSHIELD ENDPOINT SECURITY
STORMSHIELD VISIBILITY CENTER
NETASQ

C&M
ENTERPRISE

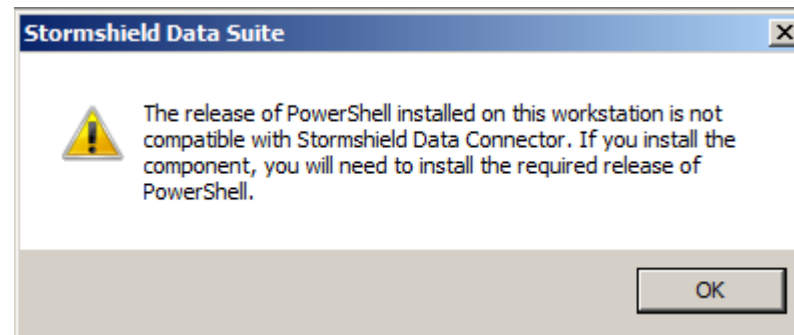
AGENT
DEMO
SERVER
TOOLS

STORMSHIELD DATA SECURITY - ENTERPRISE - V 9.1.30931 Published the 2017-05-11

Release Note : [EN / FR](#) User Guide : [EN / FR](#)

NAME	TYPE	VERSION	FORMAT	ARCHI	OS	LANGUAGE	SIZE	SHA256
SDAM_9.13.931_ENU_EVAL	Enterprise	Demo	zip		windows	en	34M	Display
SDAM_9.13.931_FRA_EVAL	Enterprise	Demo	zip		windows	fr	34M	Display
SDS_Suite_9.1.30931_ENU_Release_eval_x64	Enterprise	Demo	msi	x64	windows	en	83M	Display
SDS_Suite_9.1.30931_ENU_Release_eval_x64_setup	Enterprise	Demo	exe	x64	windows	en	91M	Display
SDS_Suite_9.1.30931_ENU_Release_eval_x86	Enterprise	Demo	msi	x86	windows	en	55M	Display
SDS_Suite_9.1.30931_ENU_Release_eval_x86_setup	Enterprise	Demo	exe	x86	windows	en	61M	Display
SDS_Suite_9.1.30931_FRA_Release_eval_x64	Enterprise	Demo	msi	x64	windows	fr	83M	Display
SDS_Suite_9.1.30931_FRA_Release_eval_x64_setup	Enterprise	Demo	exe	x64	windows	fr	91M	Display
SDS_Suite_9.1.30931_FRA_Release_eval_x86	Enterprise	Demo	msi	x86	windows	fr	54M	Display
SDS_Suite_9.1.30931_FRA_Release_eval_x86_setup	Enterprise	Demo	exe	x86	windows	fr	61M	Display

Pendant l'installation, si vous **N'AVEZ PAS BESOIN** du composant SD Connector, ignorez ce message d'erreur concernant PowerShell.



Installer la version officielle

Installez la version officielle de l'agent SDS sur le poste de travail que vous allez utiliser pour configurer le SDAM à l'aide de l'interface Web d'administration.

To view your download, click on a category below :

STORMSHIELD NETWORK SECURITY
STORMSHIELD DATA SECURITY
STORMSHIELD ENDPOINT SECURITY
STORMSHIELD VISIBILITY CENTER
NETASQ

C&M
ENTERPRISE

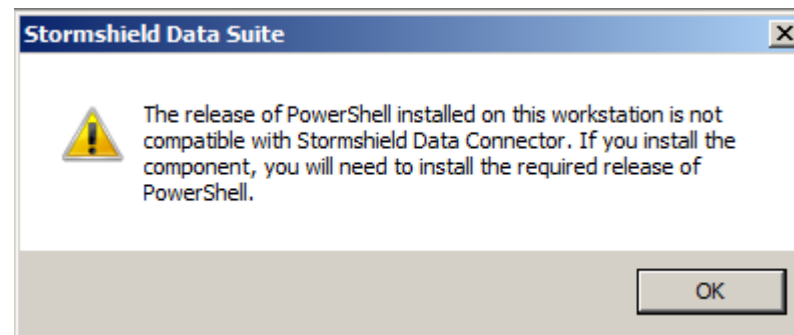
AGENT
DEMO
SERVER
TOOLS

STORMSHIELD DATA SECURITY - ENTERPRISE - V 9.1.30931 Published the 2017-05-11

Release Note : [EN / FR](#) User Guide : [EN / FR](#)

NAME	TYPE	VERSION	FORMAT	ARCHI	OS	LANGUAGE	SIZE	SHA256
SDS_Suite_9.1.30931_ENU_Release_x64	Enterprise	Agent	msi	x64	windows	en	83M	Display
SDS_Suite_9.1.30931_ENU_Release_x64_setup	Enterprise	Agent	exe	x64	windows	en	91M	Display
SDS_Suite_9.1.30931_ENU_Release_x86	Enterprise	Agent	msi	x86	windows	en	55M	Display
SDS_Suite_9.1.30931_ENU_Release_x86_setup	Enterprise	Agent	exe	x86	windows	en	61M	Display
SDS_Suite_9.1.30931_FRA_Release_x64	Enterprise	Agent	msi	x64	windows	fr	83M	Display
SDS_Suite_9.1.30931_FRA_Release_x64_setup	Enterprise	Agent	exe	x64	windows	fr	91M	Display
SDS_Suite_9.1.30931_FRA_Release_x86	Enterprise	Agent	msi	x86	windows	fr	54M	Display
SDS_Suite_9.1.30931_FRA_Release_x86_setup	Enterprise	Agent	exe	x86	windows	fr	61M	Display

Pendant l'installation, si vous **N'AVEZ PAS BESOIN** du composant SD Connector, ignorez ce message d'erreur concernant PowerShell.



Enregistrer votre produit Stormshield Data Security

The screenshot shows a web application interface for registering SDS Software. The top navigation bar includes links for "Legal terms", "Terms of Use and Services", "My profile", and "Log out". The main content area is titled "Register SDS Software" and contains a form with the following fields:

- Associated company: A dropdown menu with "STORMSHIELD (NETASQARKOON)" selected.
- License key: A text input field with a red border, indicating it is required.
- Reseller: A text input field.

A "Register" button is located at the bottom right of the form. On the left side, a sidebar menu is visible with the following categories:

- Order**
 - Create a new order
 - List of drafts
 - Orders in progress
 - Realized orders list
 - Serial number database
- Deal Registration**
 - Register a new Deal
 - Deal List
 - User Guide
- Product**
 - RMA Details
 - Product Details
- Licenses**
 - Register a SNS appliance
 - Register SNS Software
 - End of life
- SES - General**
 - Register an SES instance
- SDS - General**
 - Register an SDS instance

The "Register an SDS instance" option is highlighted with a blue box.

Scénarios

- Les pages suivantes vous présentent deux scénarios :
 1. **Scénario Validation de principe (POC)** : il suffit de créer une seule base de données pour la CA racine (BdD Access). Dans le Guide d'administration téléchargé depuis MyStormshield, vous trouverez la procédure à suivre pour migrer d'une base de données Access à SQL. Reportez-vous aux sections « [Création de la PKI racine](#) » et « [Configuration d'Internet Explorer et initialisation de la PKI racine](#) ».
 2. **Scénario Meilleures pratiques** : vous avez besoin de deux bases de données (BdD SQL) pour la CA racine et la CA enfant. Reportez-vous aux sections ci-dessus et à « [Initialisation d'une PKI enfant \(option\)](#) ».

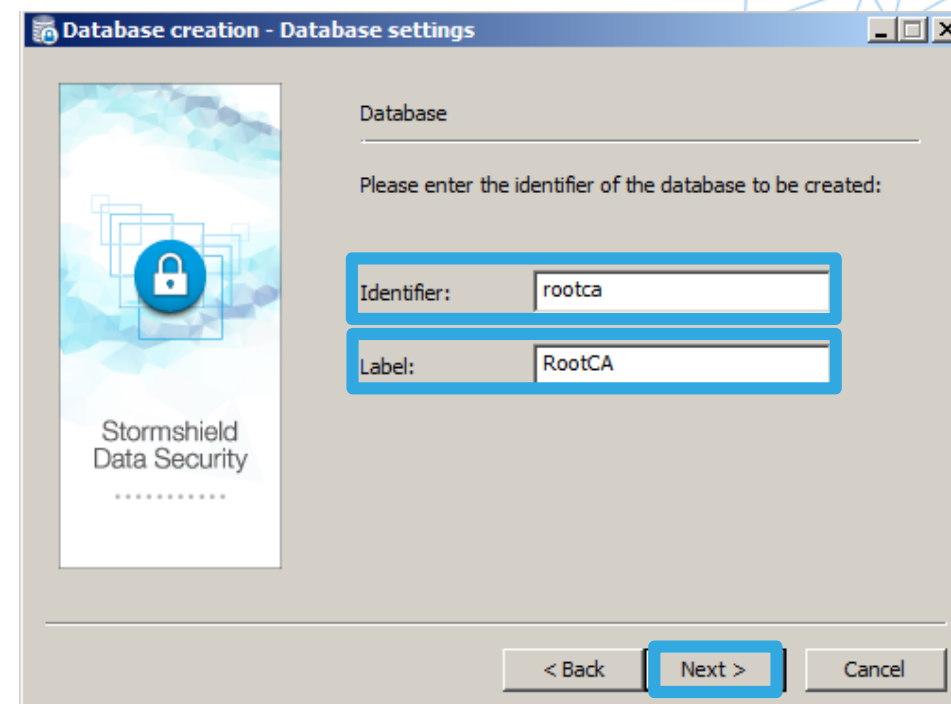
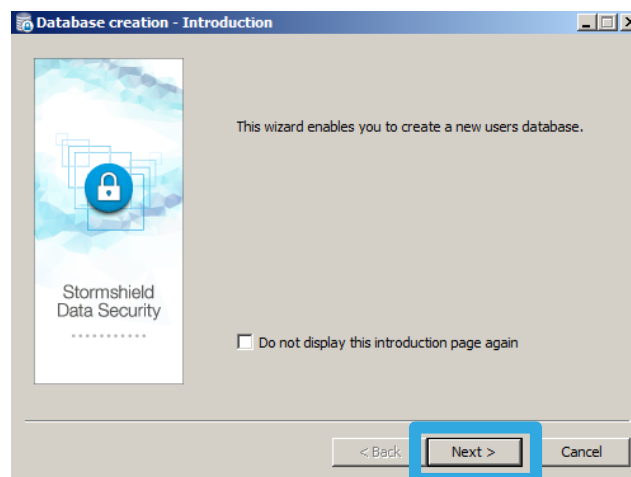
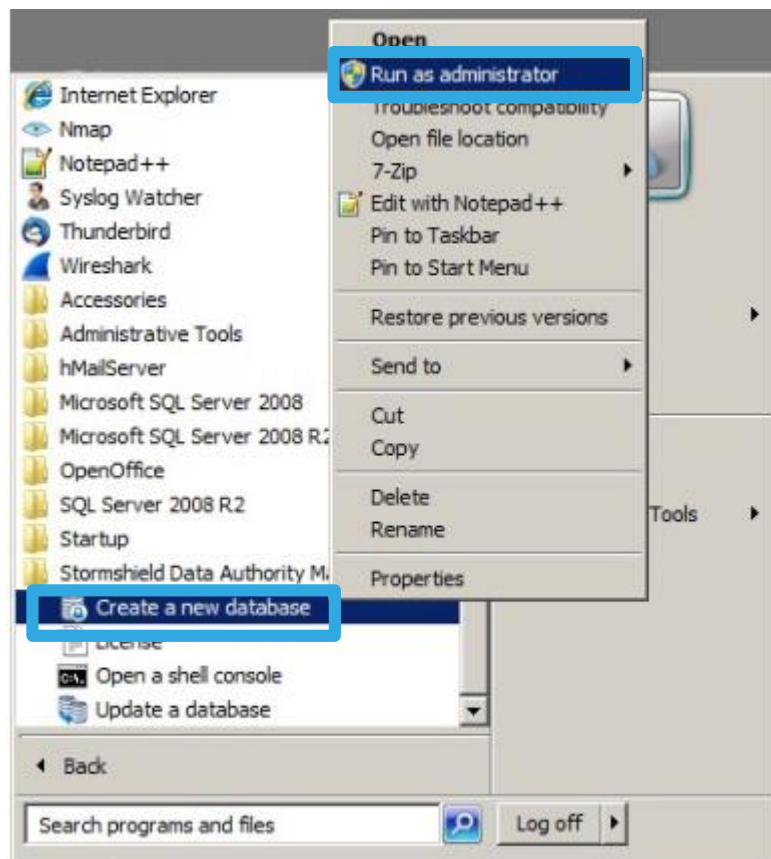


Créer la PKI racine

Installer la base de données Access pour la CA racine

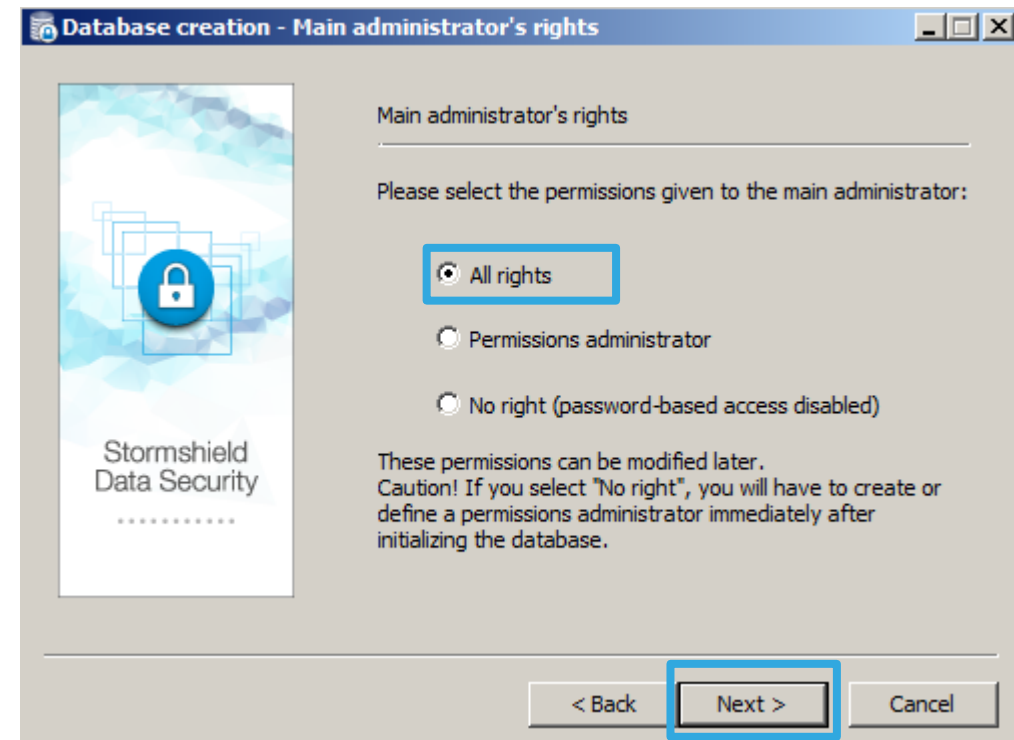
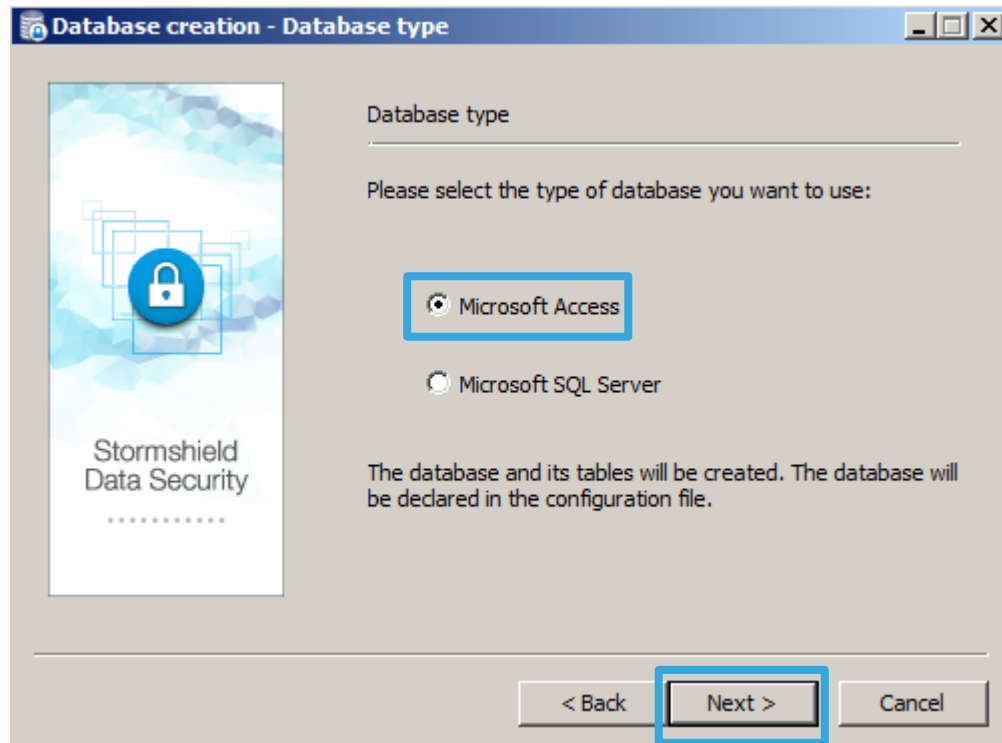
- Identifiant : L'identifiant est principalement utilisé en interne par le SDAM.
- Étiquette : L'étiquette est utilisée dans toutes les pages SDAM pour faire référence à la base de données d'utilisateurs.

Cliquez sur Créer une nouvelle base de données et sur Exécuter en tant qu'administrateur.

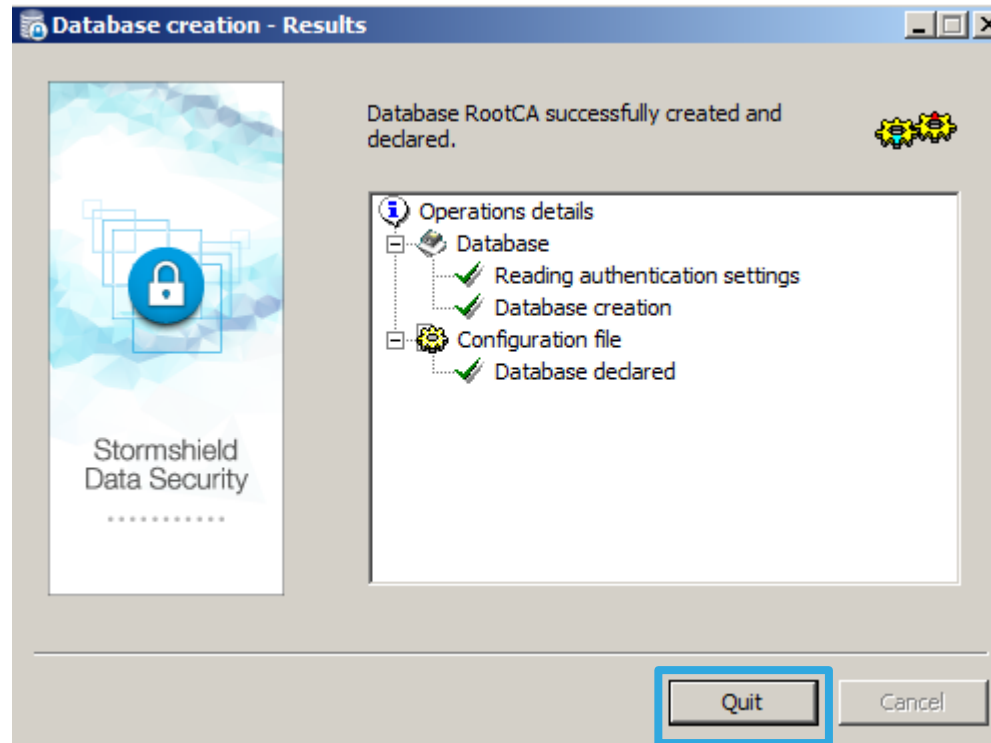
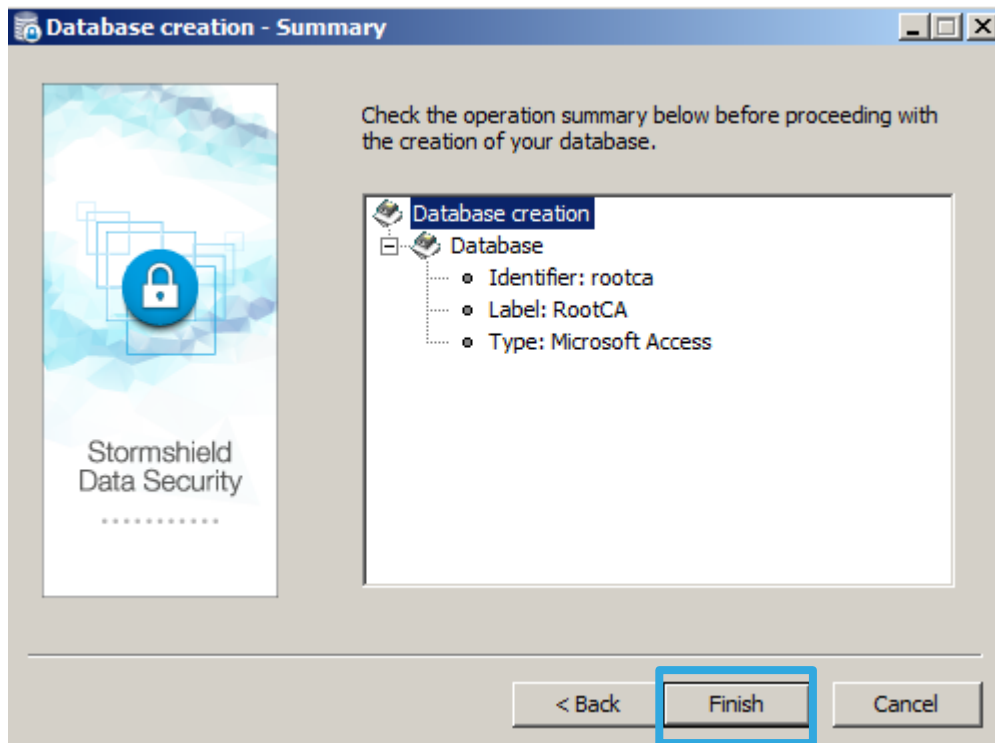


Installer la base de données Access pour la CA racine (suite)

Si vous choisissez de créer une base de données Microsoft SQL Server, reportez-vous à « [Recommandations pour SQL Server](#) ».



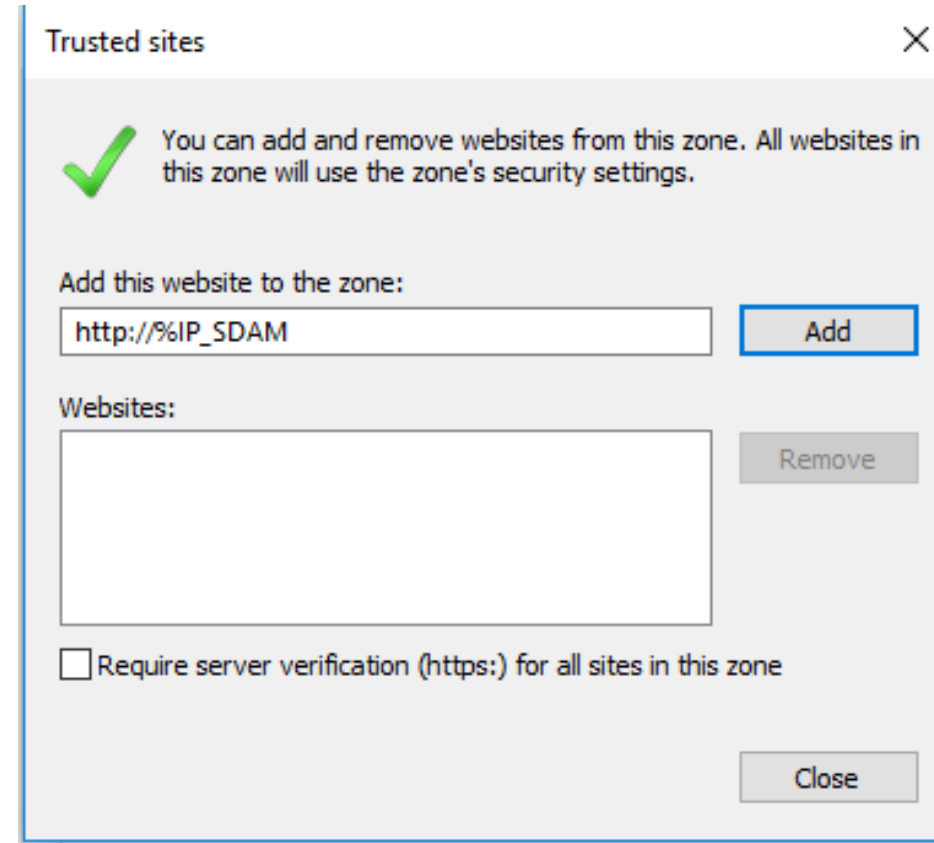
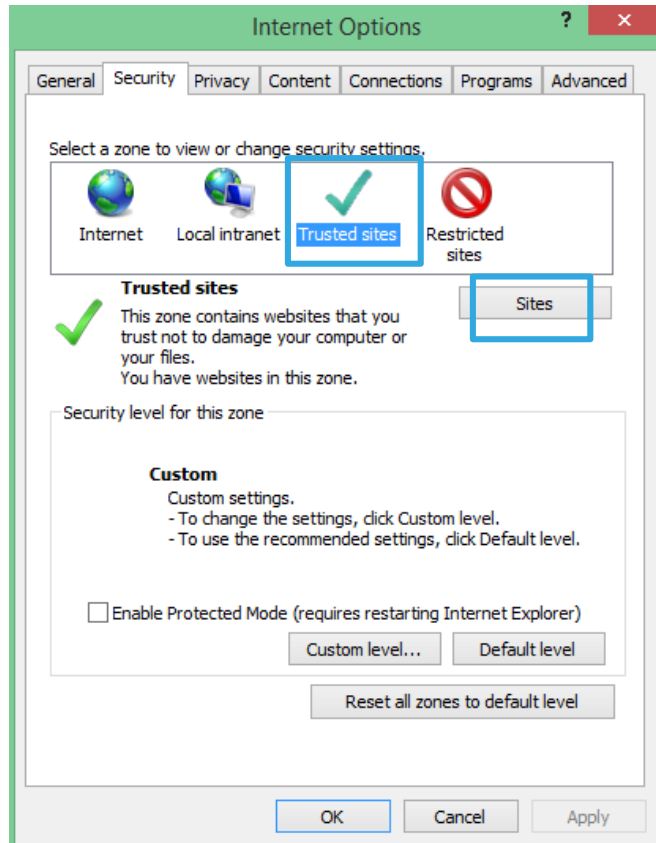
Installer la base de données Access pour la CA racine (suite)



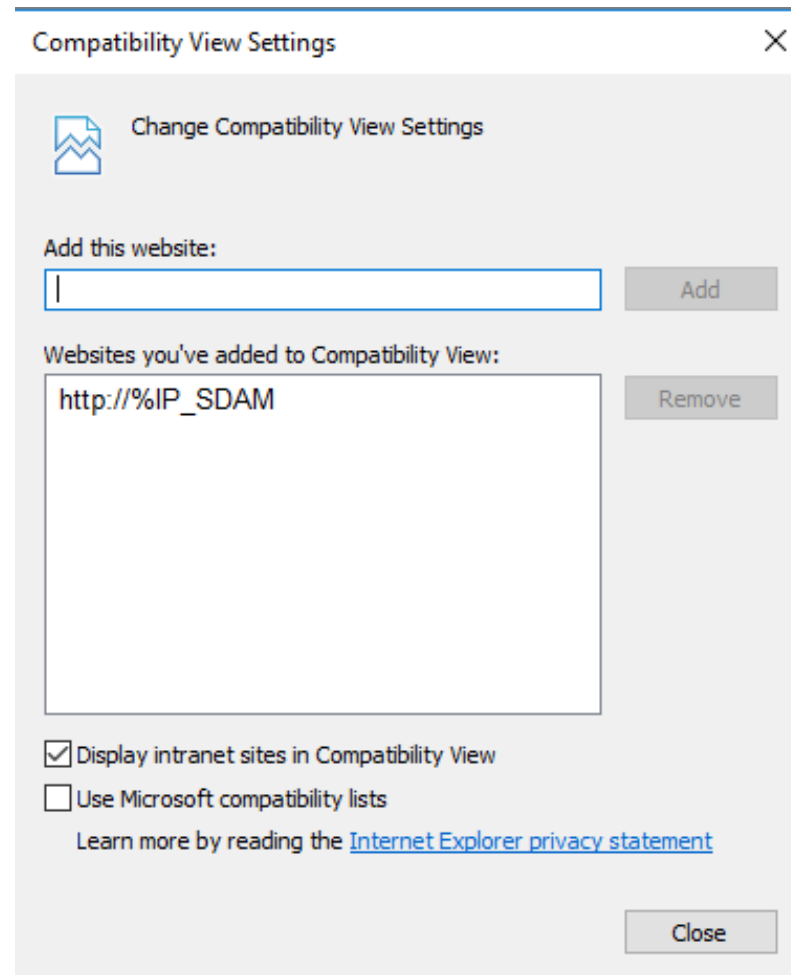
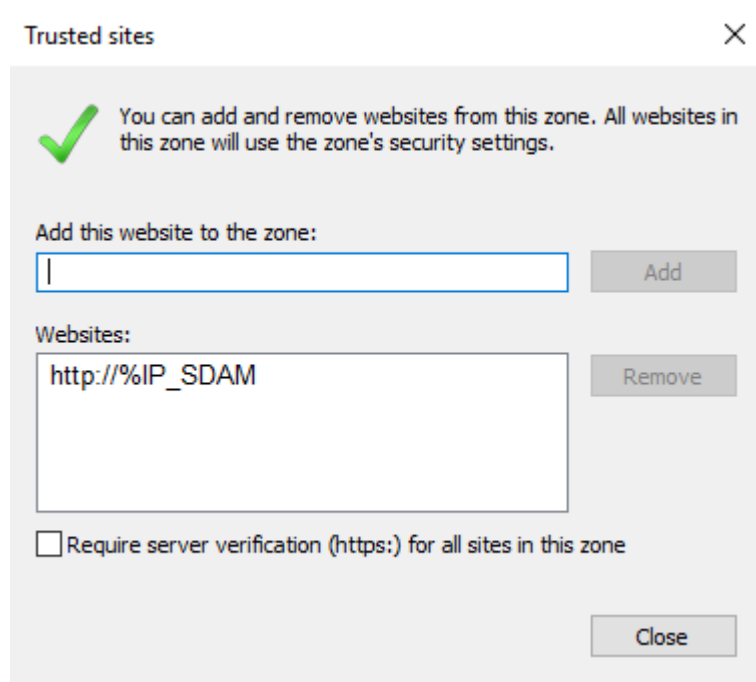


Configurer Internet Explorer et initialiser la PKI racine

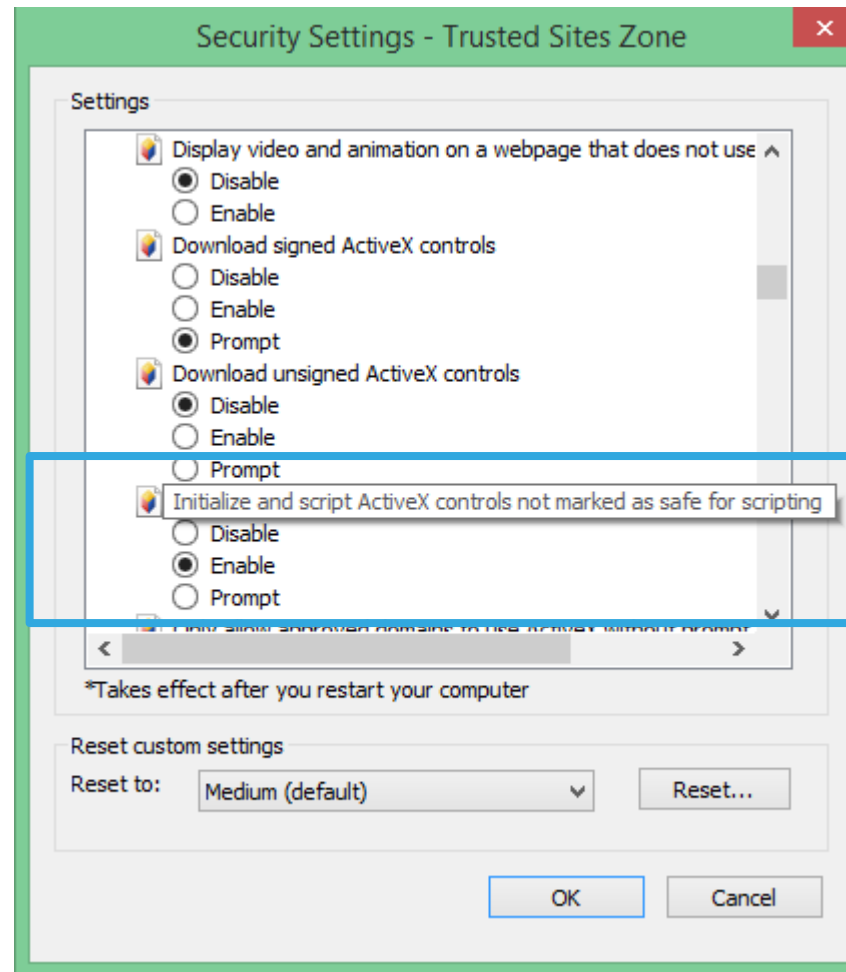
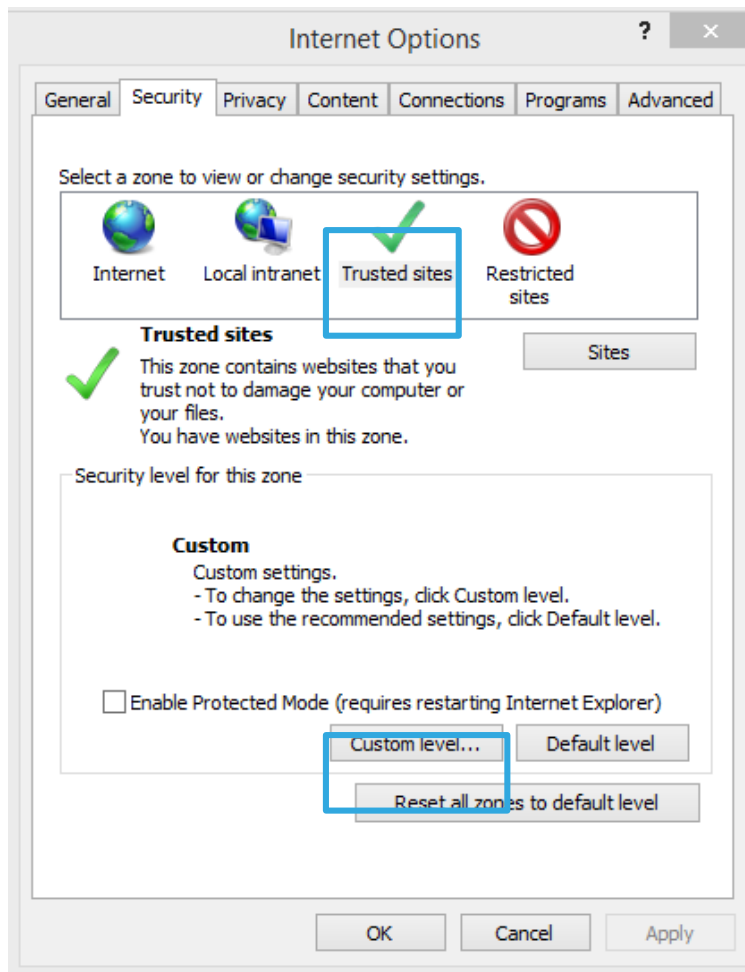
Connexion initiale à l'interface Web d'administration du SDAM



Connexion initiale à l'interface Web d'administration du SDAM (suite)



Connexion initiale à l'interface Web d'administration du SDAM (suite)



Connexion initiale à l'interface Web d'administration du SDAM (suite)

Ouvrez Internet Explorer sur le poste de travail où vous avez installé l'agent SDS et accédez au site Web suivant : http://%IP_SDAM:8080/bin/manager.exe/initBase

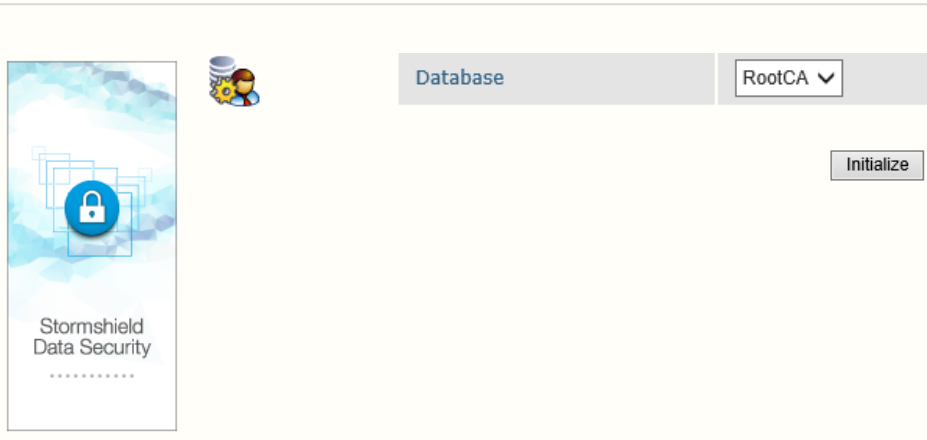
Vous devez installer le contrôle activeX (en cas d'erreur, vérifiez vos paramètres IE dans la diapositive précédente).

The screenshot shows a web browser window with the address bar containing `http://%IP_SDAM:8080/bin/manager.exe/initBase`. The page title is "Stormshield Data Security Authority Manager". The main content area is titled "Initialize database" and features a "Database" dropdown menu set to "RootCA" and an "Initialize" button. A sidebar on the left displays the Stormshield Data Security logo. At the bottom, a copyright notice reads "Stormshield Data Authority Manager 9.13.931 - Copyright © 1996-2017 Stormshield". A yellow security warning bar at the bottom of the browser indicates that the website wants to install the add-on "SboxAuthorityManager.cab" from "Stormshield", with an "Install" button highlighted.

Initialiser la CA racine

Après avoir installé le contrôle activeX, initialisez la base de données **RootCA** (CA racine).

Initialize database



Stormshield
Data Security
.....

Database: RootCA

Initialize

À cet endroit, vous devez insérer le mot de passe qui va servir à démarrer la base de données.

Enter password

Database

Identifier	rootca
Label	RootCA

Startup password

A database must be started up prior to being used. The startup procedure requires a password to be presented. It must contain between 8 and 64 characters.

Password
Password confirmation

Key storage

Key storage	<input checked="" type="radio"/> Store keys in the internal cryptographic module <input type="radio"/> Store keys in a hardware cryptographic module Slot / Token: No slot or token activated
-------------	---

Cliquez sur **Continuer** au bas de la page.

Initialiser la CA racine (suite)

Encryption key creation

Encryption key



Confidential data managed by Stormshield Data Authority Manager are encrypted using a secret key, itself wrapped with an encryption key.

Key creation	<input checked="" type="radio"/> Draw an encryption key	RSA 2048 bits
	<input type="radio"/> Import an encryption key from a PKCS#12 file:	
	File name	<input type="text"/> Browse...
	Password	<input type="password"/>
Exportable key	<input checked="" type="checkbox"/> Mark key as exportable	

Cliquez sur **Continuer**.

Entrez le mot de passe administrateur permettant de se connecter à l'interface Web du SDAM.

Report



The draw of the encryption key by the internal cryptographic module was **successful**.

Main administrator's password



The main administrator is the only administrator authenticated through a password.

Password	<input type="password"/>
Password confirmation	<input type="password"/>

Database certification authority



Certification authority

- Do not create an authority
- Draw an authority key
- Import an authority key from a PKCS#12 file

Validation



The following operations will be performed:

- › backup of the administrator's password;
- › certification authority's key draw by the internal cryptographic module.

Initialiser la CA racine (suite)

Create certification authority's key

Certification authority's key



Key size

RSA 2048 bits

Exportable key

Mark key as exportable

Validation



The following operations will be performed:

- certification authority's key draw by the internal cryptographic module.

Authority certification

Report



The draw of the certification authority's key by the internal cryptographic module was **successful**.

Authority identity

Common name	RootCA
Organization	Stormshield
Organization unit	StormshieldPOC
City	Milan
State or province	Lombardia
Country	Italy (IT)
DN	

Authority certification



Key certified by an external authority

Self-certified (root) key

Validity period

20 years

The certificate will be valid until **Tuesday, February 23, 2038**.

Algorithm

Certificate signed by **SHA-256 and RSA**

Depth

The number of certificates in the certification path starting from this authority, excluding the end certificate

unlimited

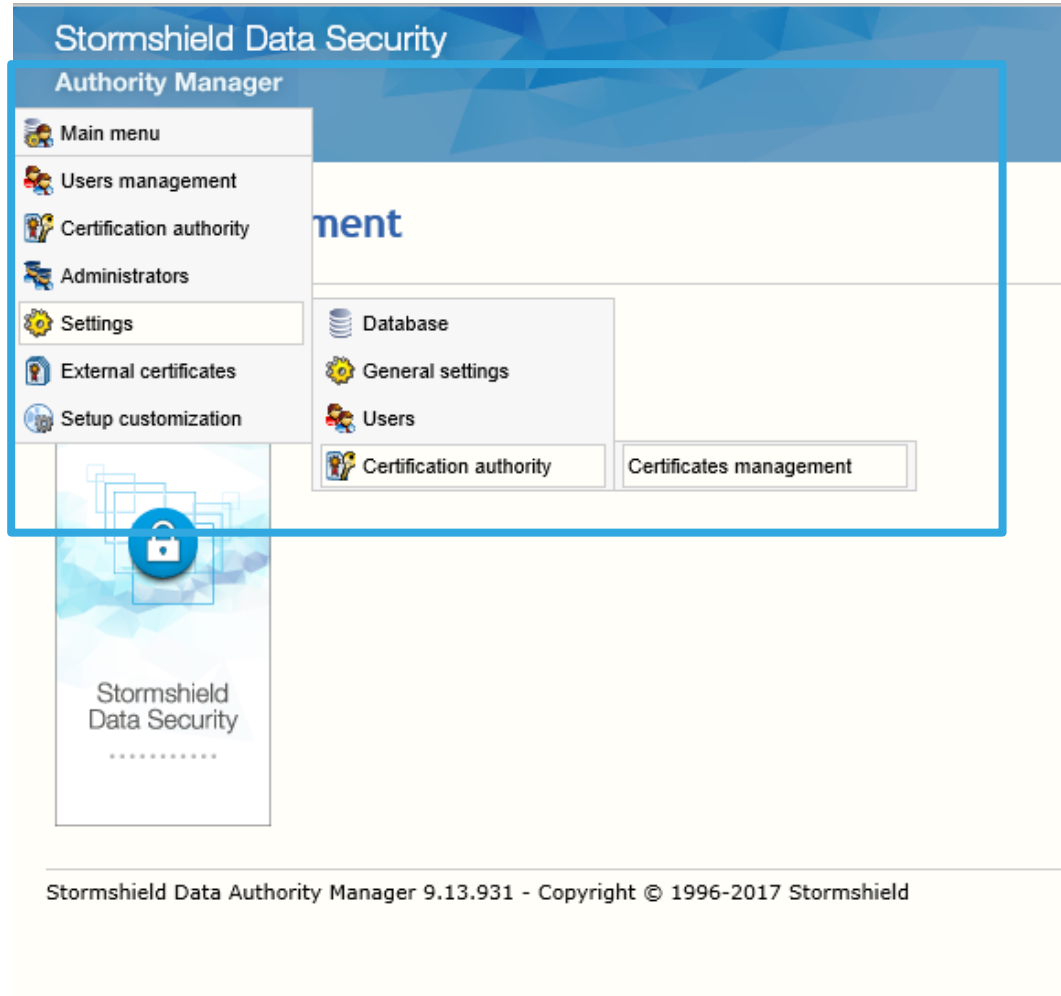
Key identifier

Include key identifier (SubjectKeyId)

Cliquez sur **Terminer**.
La base de données est maintenant initialisée.

Configurer la CRL de RootCA

Vous devez maintenant vous connecter à l'interface Web SDAM et créer la CRL de la CA racine (RootCA). Pour ce faire, utilisez le lien http://%IP_SDAM:8080/bin/manager.exe/OpenSession



Configurer la CRL (suite)

Certification authority

Subject resolution mask:

External certificate requests pre-fill

Organization:

Organization unit:

City:

State or province:

Country:

Generated certificates

Default certificate validity duration	<input type="text" value="2 years"/>
Default key size for CSPs	<input type="text" value="2048 bits"/>
Algorithm	Certificate signed by: <input type="text" value="SHA-256 and RSA"/>
'Email' field	When generating a standard certificate (for which the SubjectAlternativeName extension was not filled at request time) <input type="radio"/> Leave the email address in the identity only <input checked="" type="radio"/> Copy the identity email address into the certificate's SubjectAltName field <input type="radio"/> Move the identity email address to the certificate's SubjectAltName field
Resolution mask of external certificates' LDAP DN	<input type="text"/>
Resolution mask of LDAP entry's search filter	<input type="text" value="(mail=<AltNameEmail>)"/>
Certificates already published on the LDAP server	Default <input type="radio"/> Keep <input type="radio"/> Delete <input checked="" type="radio"/> Replace certificates that have the same usages and the same issuer
File-based publication	<input type="checkbox"/> Activate file-based certificates publication Publication folder: <input type="text" value="C:\SBMD\data\root\ca\CertsPublished"/> File format: <input type="text" value="Binary"/>

Configurer la CRL (suite)

Ajoutez l'URL de téléchargement de la CRL : `http://%IP_SDAM:8080/rootcrl/rootca.crl`
Vous pouvez ajouter plusieurs URL si vous voulez disposer de plusieurs points de distribution.

Revocation lists (CRLs)

Algorithm	Thumbprint algorithm used for signature	SHA-256
CRL validity duration	24	hours
CRLs publication DN LDAP		
Current CRL's generation location	C:\SBMData\rootca\Crl\rootca.crl	
CRLs archiving folder	C:\SBMData\rootca\Crl\History	
CRL generation	<input checked="" type="checkbox"/> By default, request CRL generation at each revocation	
Expired certificates	<input type="checkbox"/> Include expired certificates in CRL	
CRL distribution points	<code>http://%IP_SDAM:8080/rootcrl/rootca.crl</code> Distribution point: <code>http://%IP_SDAM:8080/rootcrl/rootca.crl</code>	

Automatic CRL generation service

Generation service	<input checked="" type="checkbox"/> Activate automatic CRL generation
Frequency	1 hours
Generation time	0 : 00

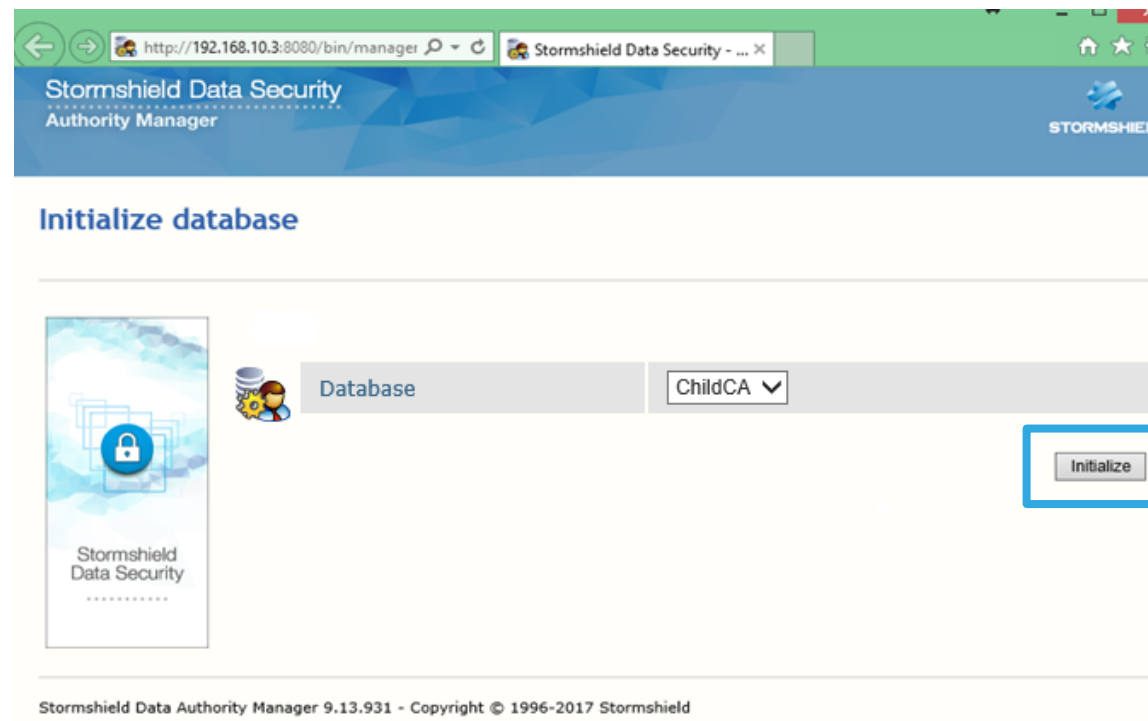
Cliquez sur **Appliquer les modifications**.



Initialiser une PKI enfant (option)

Option : initialiser la CA enfant

Pour initialiser une base, accédez à la page Web suivante, puis sélectionnez la base : *http://%IP_SDAM:8080/bin/manager.exe/initBase*



Cliquez sur Initialiser.

Option : initialiser la CA enfant (suite)

Stormshield Data Security
Authority Manager

childca
Back to selection

Enter password

Database

Identifier	childca
Label	childca

Startup password

A database must be started up prior to being used. The startup procedure requires a password to be presented. It must contain between 8 and 64 characters.

Password	
Password confirmation	

Key storage

Key storage	<input checked="" type="radio"/> Store keys in the internal cryptographic module <input type="radio"/> Store keys in a hardware cryptographic module Slot / Token: No slot or token activated
-------------	---

Validation

The following operations will be performed:

- calculation of the startup key derived from the password;
- insertion of general settings into the database;
- creation of a keystore in the internal cryptographic module.

Proceed >>

Option : initialiser la CA enfant (suite)

Stormshield Data Security
Authority Manager

Encryption key creation

Encryption key

Confidential data managed by Stormshield Data Authority Manager are encrypted using a secret key, itself wrapped with an encryption key.

Key creation	<input checked="" type="radio"/> Draw an encryption key <input type="radio"/> Import an encryption key from a PKCS#12 file:	<input type="text" value="RSA 2048 bits"/>
	File name	<input type="text"/>
	Password	<input type="password"/>
Exportable key	<input type="checkbox"/> Mark key as exportable	

Validation

The following operations will be performed:

- ▶ encryption key drawn by the internal cryptographic module.

Cliquez sur Continuer.

Enter the administrator's password

Report

The draw of the encryption key by the internal cryptographic module was **successful**.

Main administrator's password

The main administrator is the only administrator authenticated through a password.

Password	<input type="password"/>
Password confirmation	<input type="password"/>

Database certification authority

Certification authority	<input type="radio"/> Do not create an authority <input checked="" type="radio"/> Draw an authority key <input type="radio"/> Import an authority key from a PKCS#12 file
-------------------------	---

Validation

The following operations will be performed:

- ▶ backup of the administrator's password;
- ▶ certification authority's key draw by the internal cryptographic module.

Option : initialiser la CA enfant (suite)

Stormshield Data Security
Authority Manager

Create certification authority's key

Certification authority's key

Key size: RSA 2048 bits

Exportable key: Mark key as exportable

Validation

The following operations will be performed:

- certification authority's key draw by the internal cryptographic module.

Cliquez sur Continuer.

Authority certification

Report

The draw of the certification authority's key by the internal cryptographic module was **successful**.

Authority identity

Common name	CA enfant
Organization	
Organization unit	
City	
State or province	
Country	France (FR)
DN	

Authority certification

Key certified by an external authority

Self-certified (root) key


Validity period	10 years	The certificate will be valid until Tuesday, August 8, 2028 .
Algorithm	Certificate signed by	SHA-1 and RSA
Depth	The number of certificates in the certification path starting from this authority, excluding the end certificate	unlimited
Key identifier	<input checked="" type="checkbox"/> Include key identifier (SubjectKeyId)	


Validation

The following operations will be performed:

- backup the authority's identity to the database;
- display the certificate request page.

Option : initialiser la CA enfant (suite)

 **Reach certification authority**

 Send the certificate request by email

The content of the certificate request is copied into the clipboard and the subject field of the email is automatically filled in.

Email address:

Go to the CA's server page

The content of the certificate is automatically copied in the clipboard.

Server's URL:

Stormshield Data Security
Authority Manager

Initialize database

Database initialization complete.

The certificate request has been **successfully** issued.

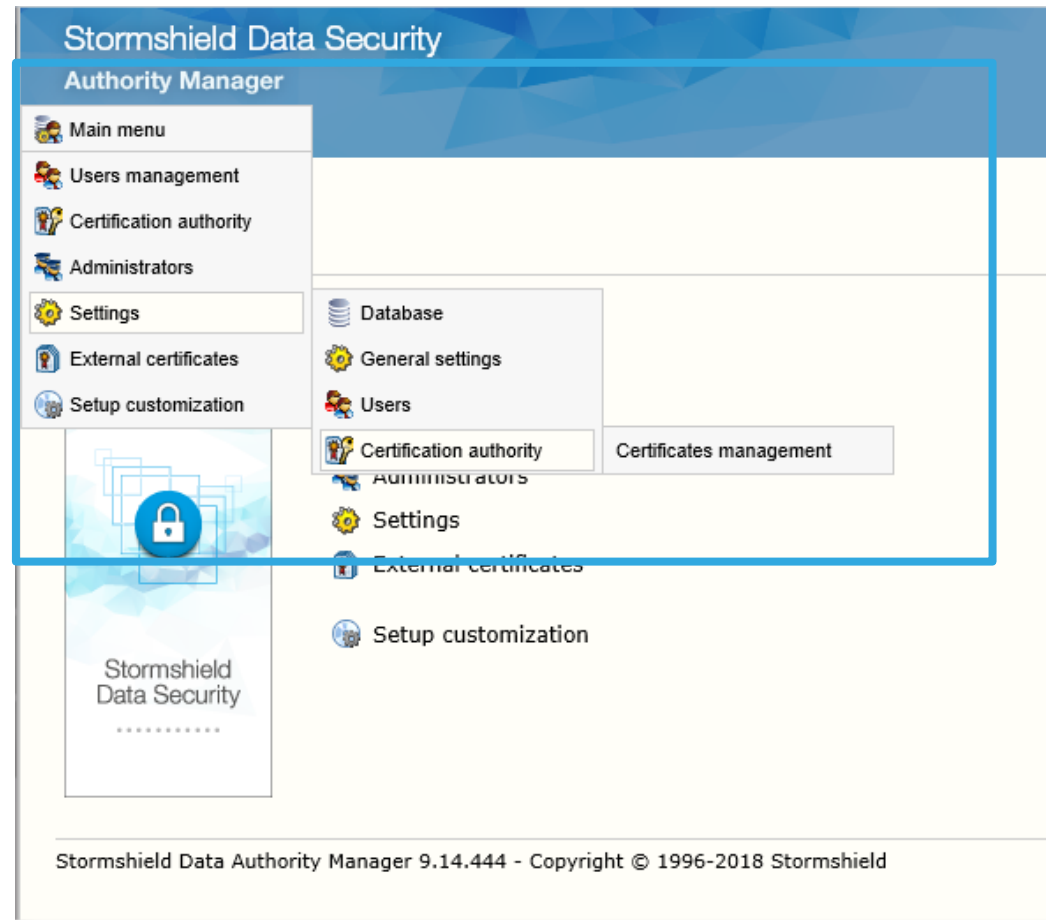
[Home](#)

Stormshield Data Authority Manager 9.14.444 - Copyright © 1996-2018 Stormshield

Cliquez sur **Demande traitée.**




Option : configurer la CRL de la CA enfant




Option : configurer la CRL de la CA enfant (suite)

Certificates management

Certification authority

 Subject resolution mask


External certificate requests pre-fill




Organization	<input type="text"/>
Organization unit	<input type="text"/>
City	<input type="text"/>
State or province	<input type="text"/>
Country	<input type="text" value="(none)"/>



Option : configurer la CRL de la CA enfant (suite)


 **Generated certificates**




Default certificate validity duration	2 years ▼
Default key size for CSPs	2048 bits ▼
Algorithm	Certificate signed by SHA-1 and RSA ▼
'Email' field	When generating a standard certificate (for which the SubjectAlternativeName extension was not filled at request time) <input type="radio"/> Leave the email address in the identity only <input checked="" type="radio"/> Copy the identity email address into the certificate's SubjectAltName field <input type="radio"/> Move the identity email address to the certificate's SubjectAltName field
Resolution mask of external certificates' LDAP DN	<input type="text"/>
Resolution mask of LDAP entry's search filter	(mail=<AltNameEmail>)
Certificates already published on the LDAP server	Default <input type="radio"/> Keep <input type="radio"/> Delete <input checked="" type="radio"/> Replace certificates that have the same usages and the same issuer
File-based publication	<input type="checkbox"/> Activate file-based certificates publication Publication folder: <input type="text" value="C:\SBMData\jkr\CertsPublished"/> File format: Binary ▼



Option : configurer la CRL de la CA enfant (suite)

 **Revocation lists (CRLs)**

	Algorithm	Thumbprint algorithm used for signature	SHA-1 <input type="button" value="v"/>
	CRL validity duration	<input type="text" value="24"/> hours	
	CRLs publication DN LDAP	<input type="text"/>	
	Current CRL's generation location	<input type="text" value="C:\SBMData\childca\Crl\childca.crl"/>	
	CRLs archiving folder	<input type="text" value="C:\SBMData\childca\CrlHistory"/>	
	CRL generation	<input checked="" type="checkbox"/> By default, request CRL generation at each revocation	
	Expired certificates	<input type="checkbox"/> Include expired certificates in CRL	
	CRL distribution points	<input type="text" value="http://%IP_SDAM:8080/childcrl/childca.crl"/> <input type="text"/> Distribution point: <input type="text" value="http://%IP_SDAM:8080/childcrl/childca.crl"/>	<input type="button" value="Add"/> <input type="button" value="Copy"/> <input type="button" value="Delete"/>

Option : configurer la CRL de la CA enfant (suite)

Automatic CRL generation service

Activate automatic CRL generation

Frequency: 24 hours

Generation time: 0 : 00

Email notifications

Certificate request deposit	<input type="checkbox"/> Send email notification on certificate request deposit	Email address: <input type="text"/>
		Subject: <input type="text"/>
		Template: C:\SBMDData\kr\MailTemplates\template_request.sbp
Internal request validation	<input type="checkbox"/> Send email notification on validation of internal request	Email address: <input type="text"/>
		Subject: <input type="text"/>
		Template: C:\SBMDData\kr\MailTemplates\template_validation_internal_admin.sbp
	<input type="checkbox"/> Send a notification email to the requestor	Subject: <input type="text"/>
		Template: C:\SBMDData\kr\MailTemplates\template_validation_internal_user.sbp
External request validation	<input type="checkbox"/> Send email notification on validation of external request	Email address: <input type="text"/>
		Subject: <input type="text"/>
		Template: C:\SBMDData\kr\MailTemplates\template_validation_external_admin.sbp
	<input type="checkbox"/> Send a notification email to the requestor	Subject: <input type="text"/>
		Template: C:\SBMDData\kr\MailTemplates\template_validation_external_user.sbp

Confirm operation:

Option : valider la CA enfant

Main menu

Home

Stormshield Data Security

- Users management
- Certification authority**
- Administrators
- Settings
- External certificates
- Setup customization

Stormshield Data Authority Manager 9.14.444 - Copyright © 1996-2018 Stormshield

Main menu

Certification authority

Stormshield Data Security

- Key and certificate for the authority**

Stormshield Data Authority Manager 9.14.444 - Copyright © 1996-2018 Stormshield

Option : valider la CA enfant (suite)

Stormshield Data Security Authority Manager

Main menu Properties Certificate management

Issue a certificate request

Key and certificate for the authentication

Identity

Common name	Child CA
Organization	Stormshield
Organization unit	R&D
City	Lyon
State or province	
Country	FR

Key

Algorithm	RSA 2048 bits
Created on	Wednesday, August 8, 2018 11:03:26 AM
Security module	Internal

Certificate request

The text below contains the formatted request to be sent to the certification authority.

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIICeCCACACQIv7eRMA8GAIUEAmdIQ2hpGQqQ0ExDIALBgNVBAcTBEx5b24x
DDAKBjNVBAcMA1IeRDEUMBIzGAIUEChMLU3RvcmlzaGUiYm9ja3EwA1R5
MIIBjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEa17pC4qGAIIn2HXEhA
xbTm6q25REAMuN8K2k5zKaGf+knA1pyglr0P1iIGOpK6SiEGDhjyeV3XcQwF
WbQqX-IH+8FY00V1vOQM2Mog188JBvGfyr1xZ/1PCUKtHuI9dKEPa21XEOFPVCNA
R2gJdcccFstk9Qq56LbbysC9eT+w1UTOMP96I1H5x0qUpGKCGOcnj3OqJrXq3HB9A
46Hg214ndDv7PMjpl1ZTRiDng+K+aIv7uMkdKcAm4vymSNWZK1YdCu9A1fDgQ9
v1x1Fqg11FkyQVauE9MSyR2cKshv7Ge9efavcyzhocFjgk8LJhB5ST01CCAL
nOIDAQBoAAwOCVJkzI1hvcNAQEFAODgEBAIvZFDQOKr1TV44TKGJ99MxIVQO
zILAbFp+r7yKqtbx1DAQEXSmDxM1KtdH/dy42Uv8jYgLkcpPn8+qvM/5mlPMCM
b08r1LECTatAbgAaFhbZvc/vcFYEYL6R+ORSNvL1Sc1LCUIm07mMEW1jx4Op7+7c
DcKntCrDvDm5z+eqV9dIrBkChSGrGzh1y98Cqk6Pa5GgADQeKRIeoj5MeZTF2b7
8hFgz6pEY5DqWIAf7pawN5eML3qLC5tJvVnk5drmkLO3xqxhSOMZDtG001R1Cn
pFKLYkjayin/9RMKtBG/feY0gzhSg2N7ecUcIvry0B11YFDYN3iKkKfeK=
-----END NEW CERTIFICATE REQUEST-----
```

Copy to clipboard Save as...

Reach certification authority

The content of the certificate request is copied into the clipboard and the subject field of the email is automatically filled in.

Email address:

Edit message

The content of the ce

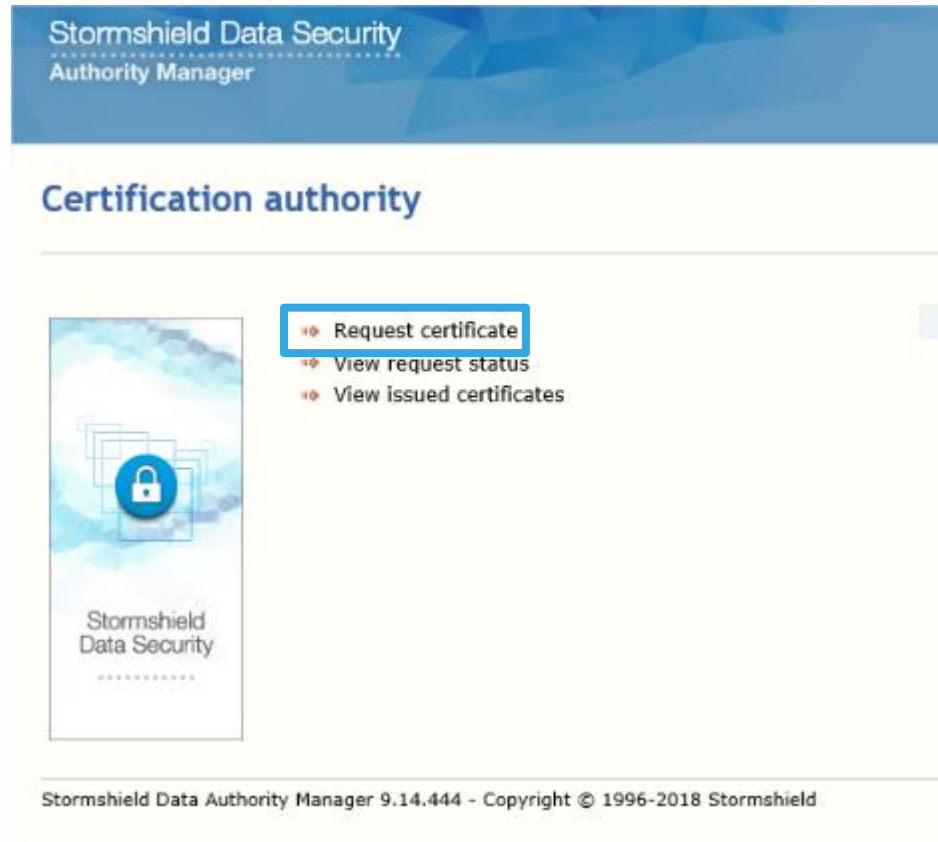
Voulez-vous ouvrir ou enregistrer Child CA.p10 (1000 octet(s)) à partir de 192.168.6.2 ?

Ouvrir Enregistrer Annuler

Cliquez sur Enregistrer.

Option : valider la CA enfant (suite)

- Pour demander un certificat, accédez à la page Web suivante :
http://%IP_SDAM:8080/bin/manager.exe/PkiIndex?baseid=rootca



Stormshield Data Security
Authority Manager

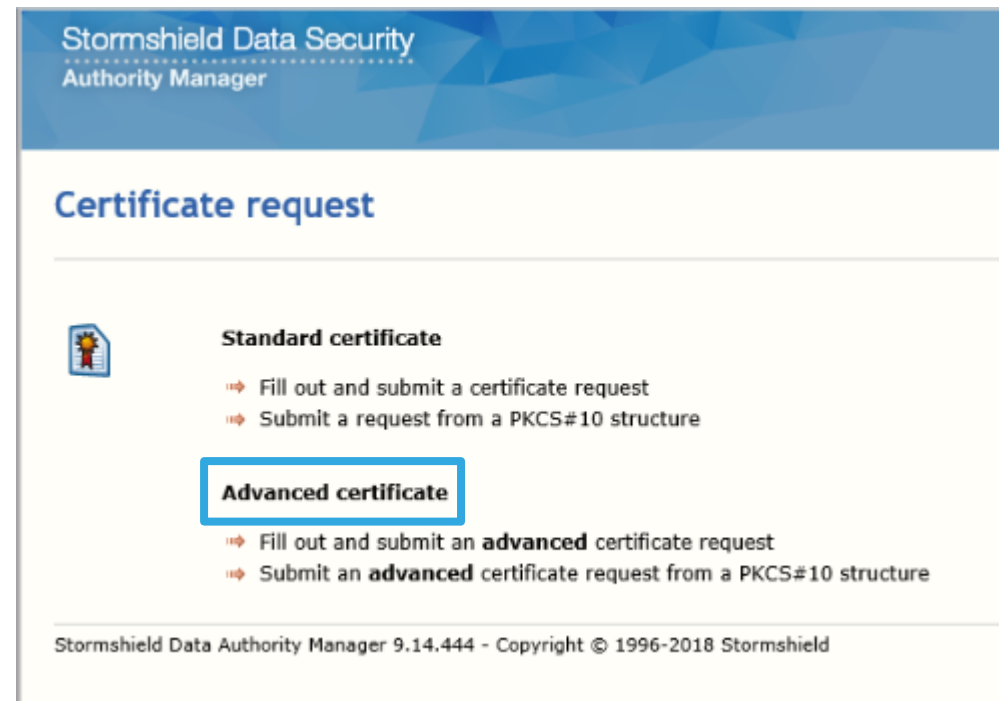
Certification authority

Request certificate

- View request status
- View issued certificates

Stormshield Data Security
.....

Stormshield Data Authority Manager 9.14.444 - Copyright © 1996-2018 Stormshield



Stormshield Data Security
Authority Manager

Certificate request

Standard certificate

- Fill out and submit a certificate request
- Submit a request from a PKCS#10 structure

Advanced certificate

- Fill out and submit an **advanced** certificate request
- Submit an **advanced** certificate request from a PKCS#10 structure

Stormshield Data Authority Manager 9.14.444 - Copyright © 1996-2018 Stormshield

Option : valider la CA enfant (suite)

Stormshield Data Security
Authority Manager

Certificate request

 **Standard certificate**

- ⇒ Fill out and submit a certificate request
- ⇒ Submit a request from a PKCS#10 structure

Advanced certificate

- ⇒ Fill out and submit an **advanced** certificate request
- ⇒ Submit an **advanced** certificate request from a PKCS#10 structure

Stormshield Data Authority Manager 9.14.444 - Copyright © 1996-2018 Stormshield

Paste from the clipboard

Import from a file

File containing the PKCS#10 request to be sent out:

C:\Users\...Downloads\Child CA.p10

Certificate

Template

Alternative identity

Email address	<input type="text"/>
Domain name	<input type="text"/>
IP address	<input type="text"/>
Universal principal name	<input type="text"/>

Contact

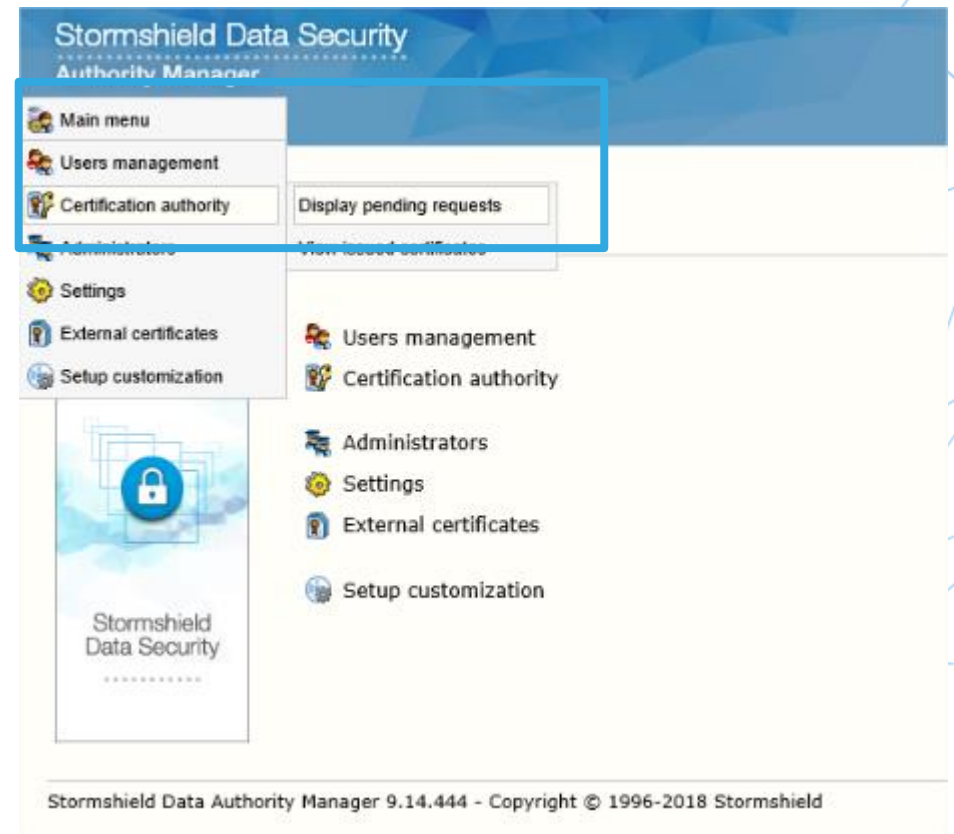
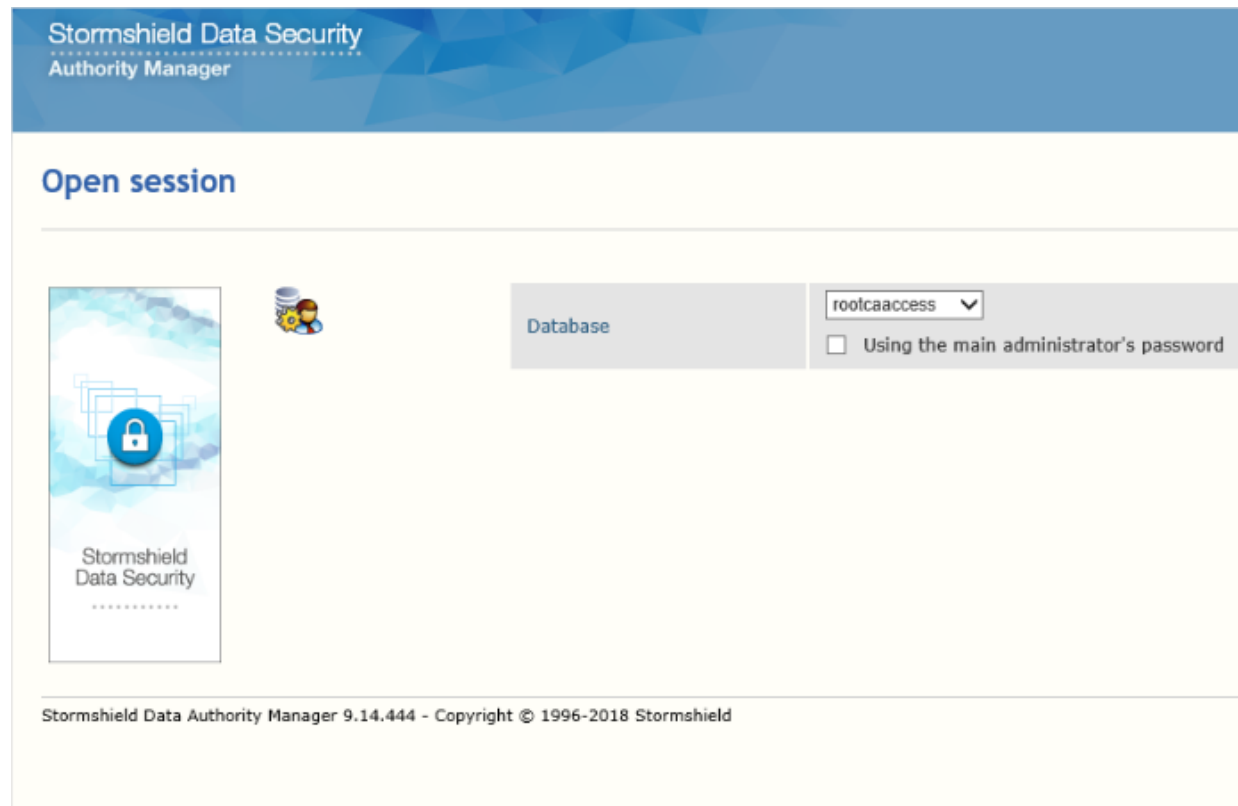
Email address	<input type="text"/>
Phone number	<input type="text"/>
Comment	<input type="text"/>

Cliquez sur Envoyer une demande.

Option : valider la CA enfant (suite)

- Connectez-vous à la CA racine (RootCA) dans la page Web suivante, puis sélectionnez la base :

http://%IP_SDAM:8080/bin/manager.exe/OpenSession



Cliquez sur Ouvrir une session.

Option : valider la CA enfant (suite)

Stormshield Data Security
Authority Manager

Main menu

List of pending requests

Requests: request 1 out of 1

Capture Plain

Request Id	Summary
> 1	Child CA Subject: C=FR,O=Stormshield,OU=R&D,L=Lyon,CN=Child CA Date of request: Wednesday, August 8, 2018 Template: Certification authority

Stormshield Data Authority Manager 9.14.444 - Copyright © 1996-2018 Stormshield

Comments

Requestor's email address

Requestor's phone number

Requestor's comment

Denial comment

In case you deny this request, you may enter a comment that will be displayed when the requestor views the status of his/her request:

Confirm operation: **Confirm request**

Option : valider la CA enfant (suite)

Stormshield Data Security
Authority Manager

Main menu

Certificate request validation

The request has been successfully validated.

Certification authority: **Root CA Access**

Certificate serial number **6**

Certificate of Child CA
This certificate is an intermediate authority certificate

- Subject: Child CA
- Issued by: Root CA Access
- Serial No: 06
- Valid from août 2018, 08 to août 2028, 08
- Public Key
- Certificate footprints
- Signature
- Authority Key Identifier
- Key Identity
- Key Usage
- Issuing Basic Constraints
- Certificate format version: 3

Certificate export

Base 64-encoded certificate's value
Copy to clipboard

Save file
Save as...

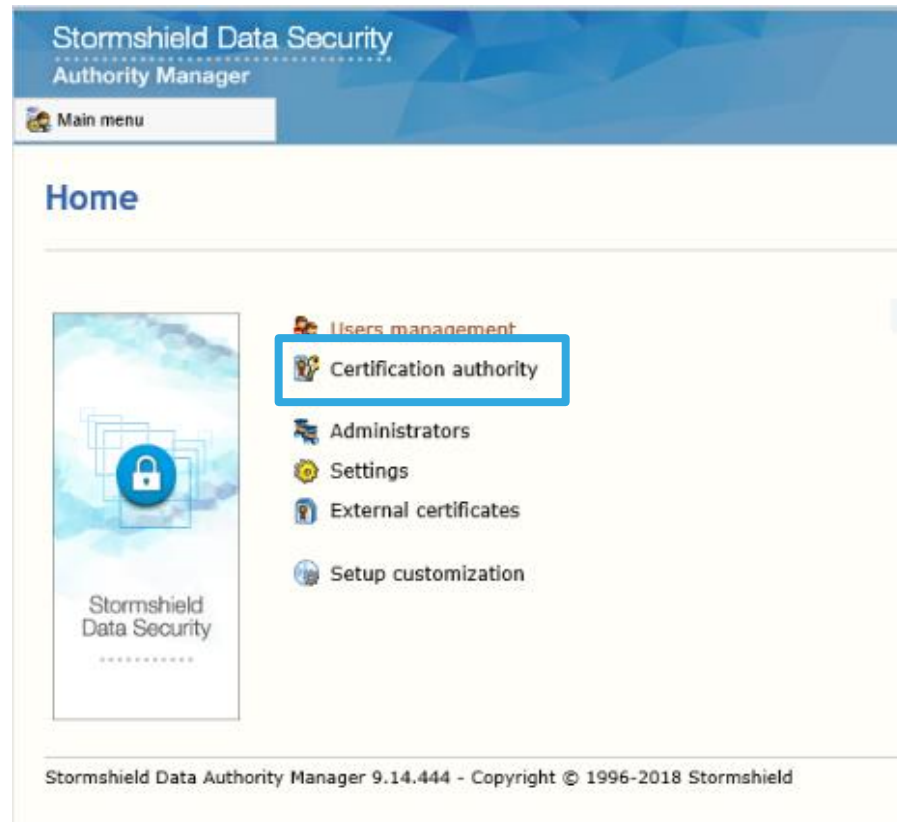
Copy of the certificate into Stormshield Data Security
Copy...

Copy of the certificate into your browser if you possess its private key
Copy...

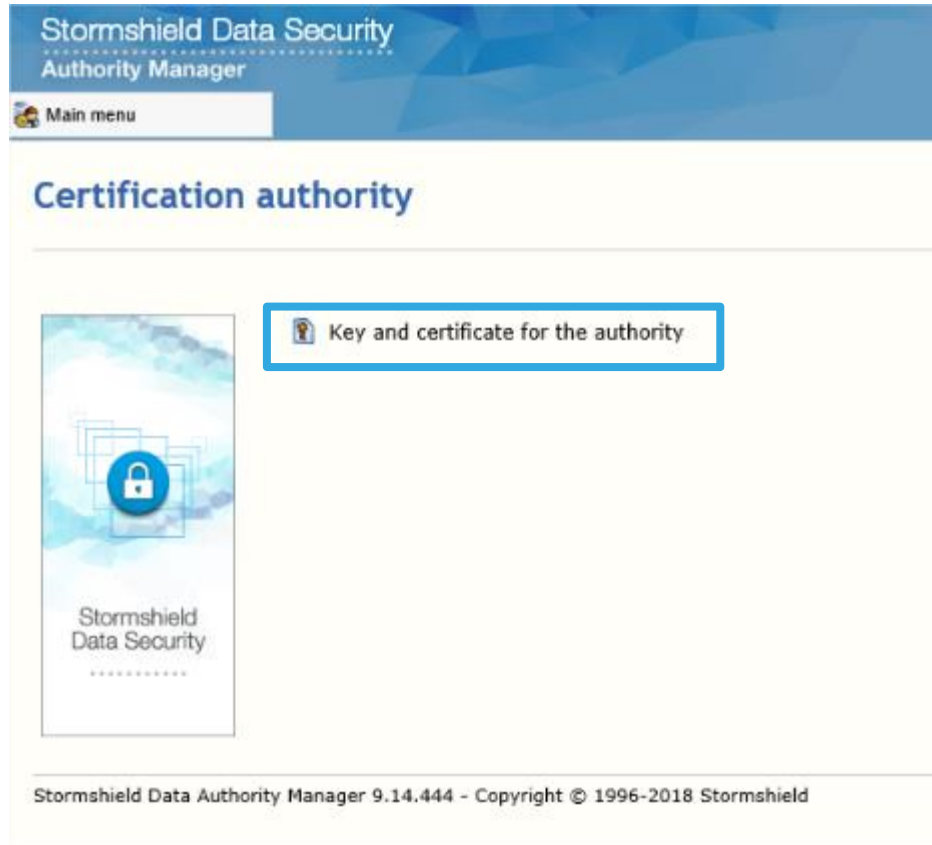
Option : valider la CA enfant (suite)

- Connectez-vous à la CA enfant dans la page Web suivante, puis sélectionnez la base :

http://%IP_SDAM:8080/bin/manager.exe/OpenSession



Option : valider la CA enfant (suite)



Stormshield Data Security
Authority Manager

Main menu

Certification authority

Key and certificate for the authority

Stormshield Data Security

Stormshield Data Authority Manager 9.14.444 - Copyright © 1996-2018 Stormshield



Stormshield Data Security
Authority Manager

Main menu Properties Certificate management

Issue a certificate request
Import a new certificate

Key and certificate for the authority

Identity

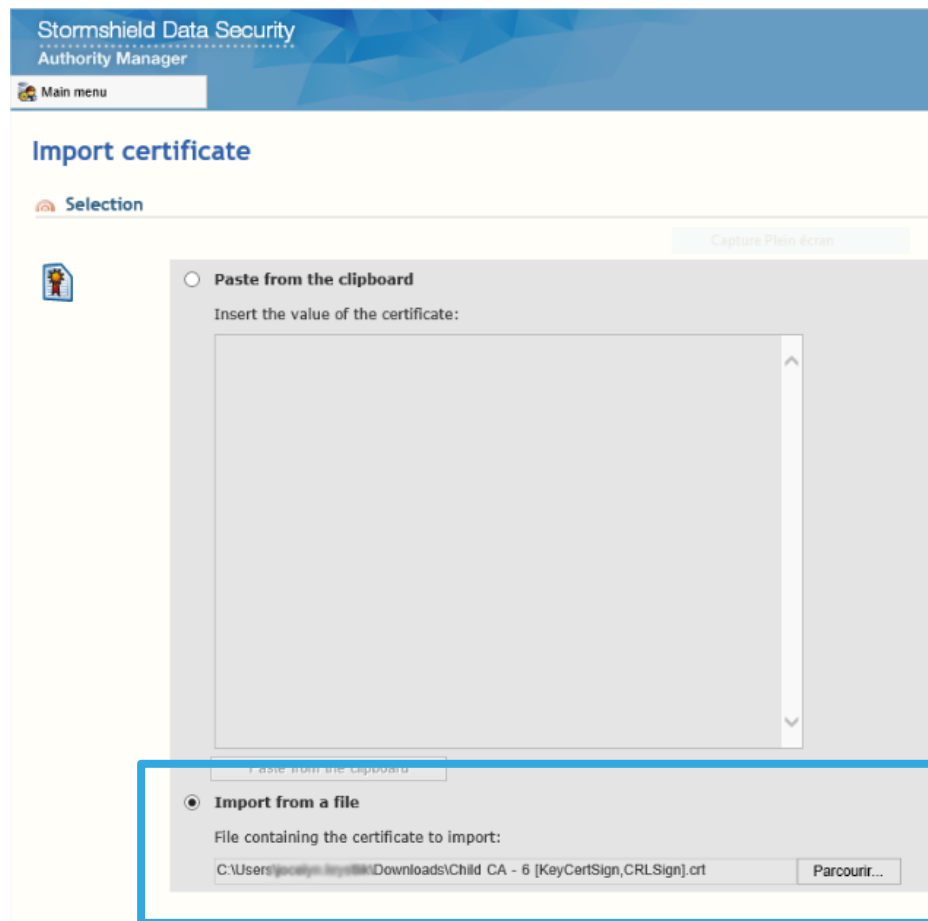
Common name	Child CA
Organization	Stormshield
Organization unit	R&D
City	Lyon
State or province	
Country	FR

Key

Algorithm	RSA 2048 bits
Created on	Wednesday, August 8, 2018 11:03:26 AM
Security module	Internal



Option : valider la CA enfant (suite)



Cliquez sur Importer.

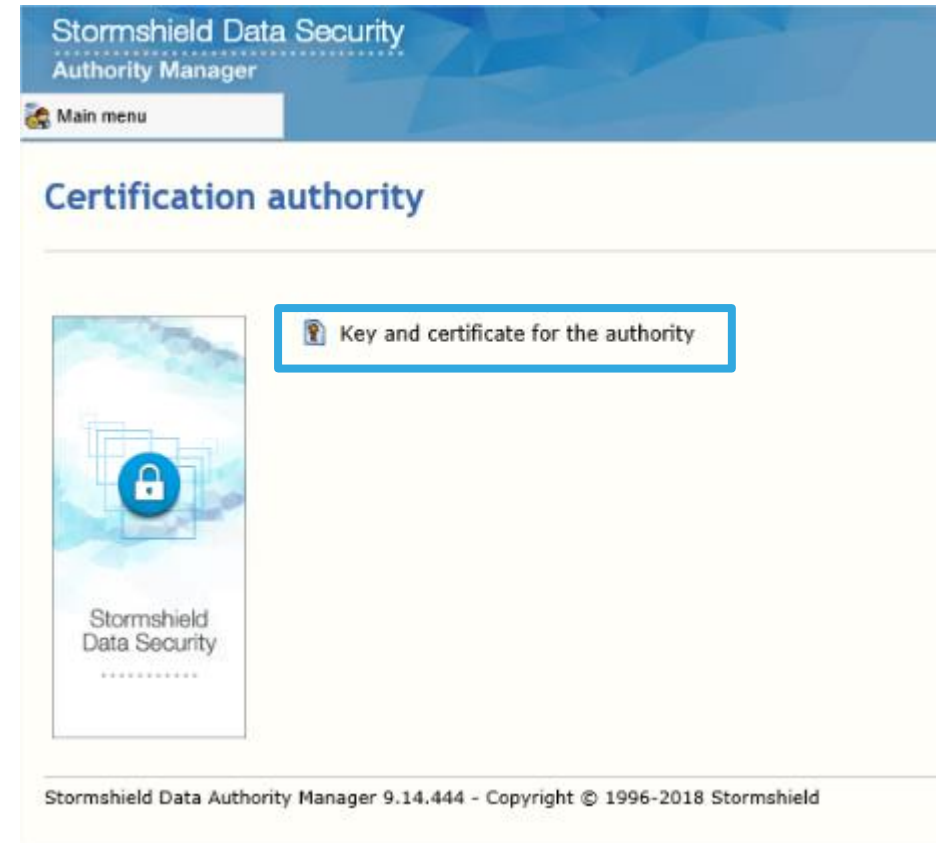
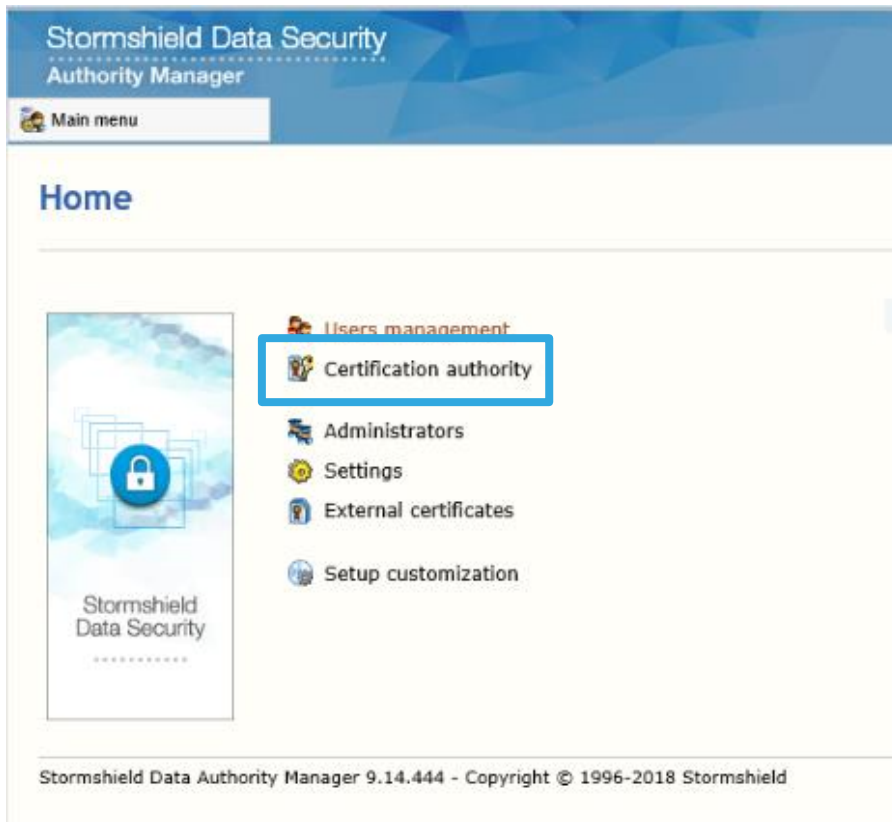


Cliquez sur Importer le certificat.

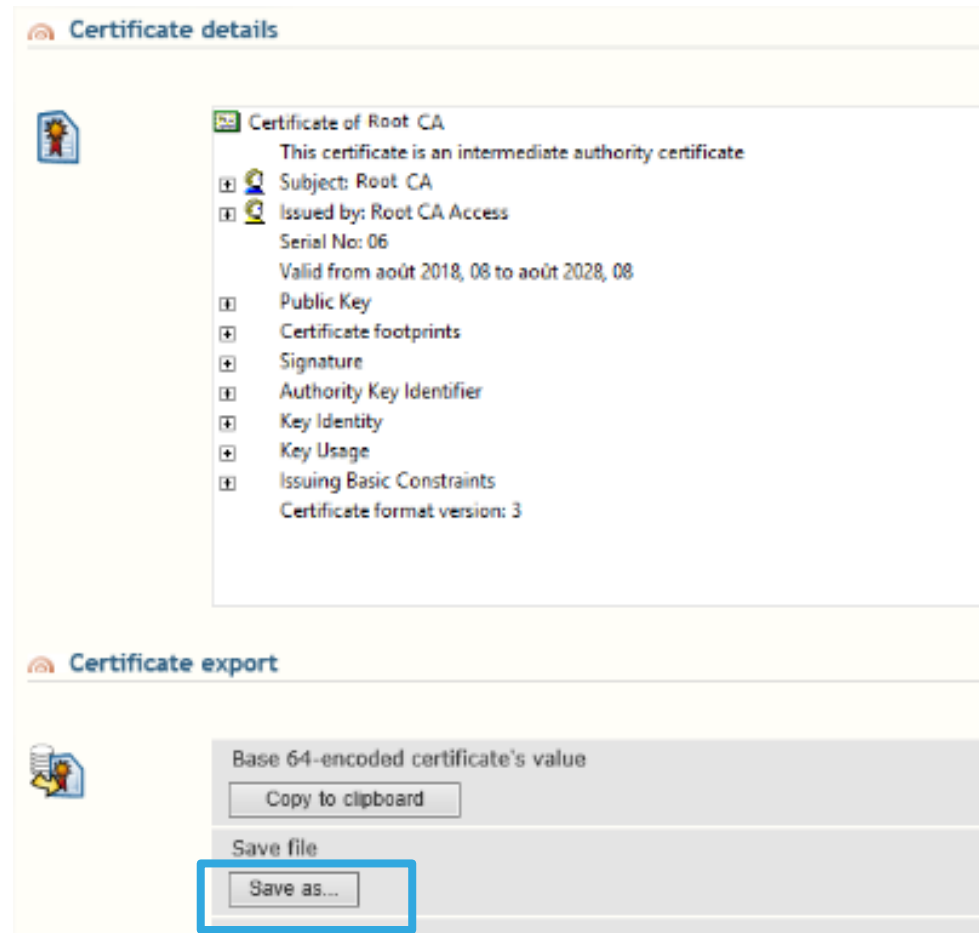
Option : valider la CA enfant (suite)

- Connectez-vous à la CA racine dans la page Web suivante, puis sélectionnez la base :

http://%IP_SDAM:8080/bin/manager.exe/OpenSession



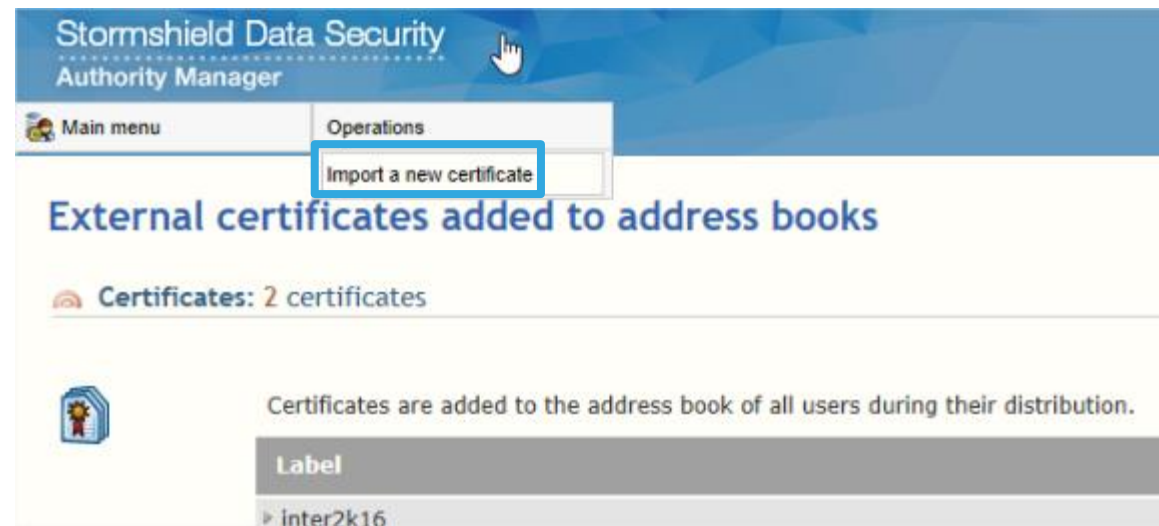
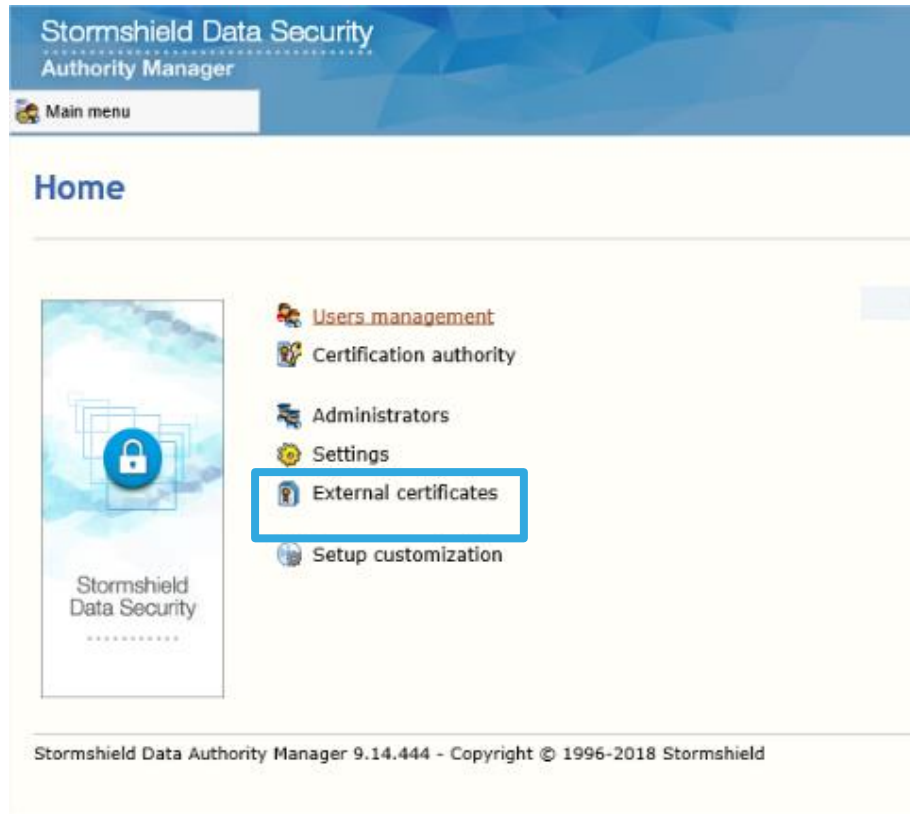
Option : valider la CA enfant (suite)



Option : valider la CA enfant (suite)

- Connectez-vous à la CA enfant dans la page Web suivante, puis sélectionnez la base :

http://%IP_SDAM:8080/bin/manager.exe/OpenSession



Option : valider la CA enfant (suite)

Main menu

Import external certificate

Selection

Paste from the clipboard

Insert the value of the certificate:

Paste from the clipboard

Import from a file

File containing the certificate to import:

Browse...

Confirm operation:

Main menu

External certificate import

Certificate details

Certificate of Root CA

This certificate is a root certificate

- Subject: Root CA
- Issued by: Root CA
- Serial No: 01
- Valid from August 2018, 21 to August 2028, 21
- Public Key
- Certificate footprints
- Signature
- Issuing Basic Constraints
- Key Usage
- Key Identity
- Certificate format version: 3

Properties

Label:

Validation

You are about to add this certificate to users' address books when they are distributed.

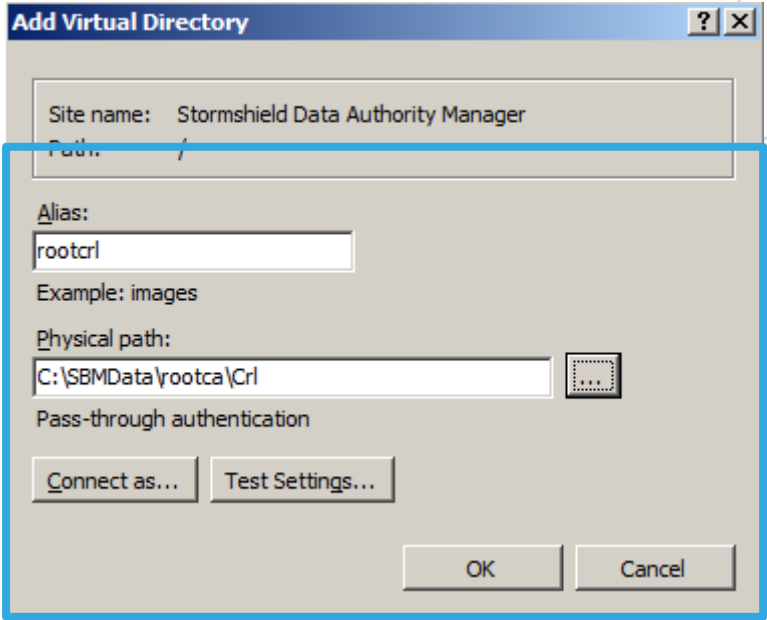
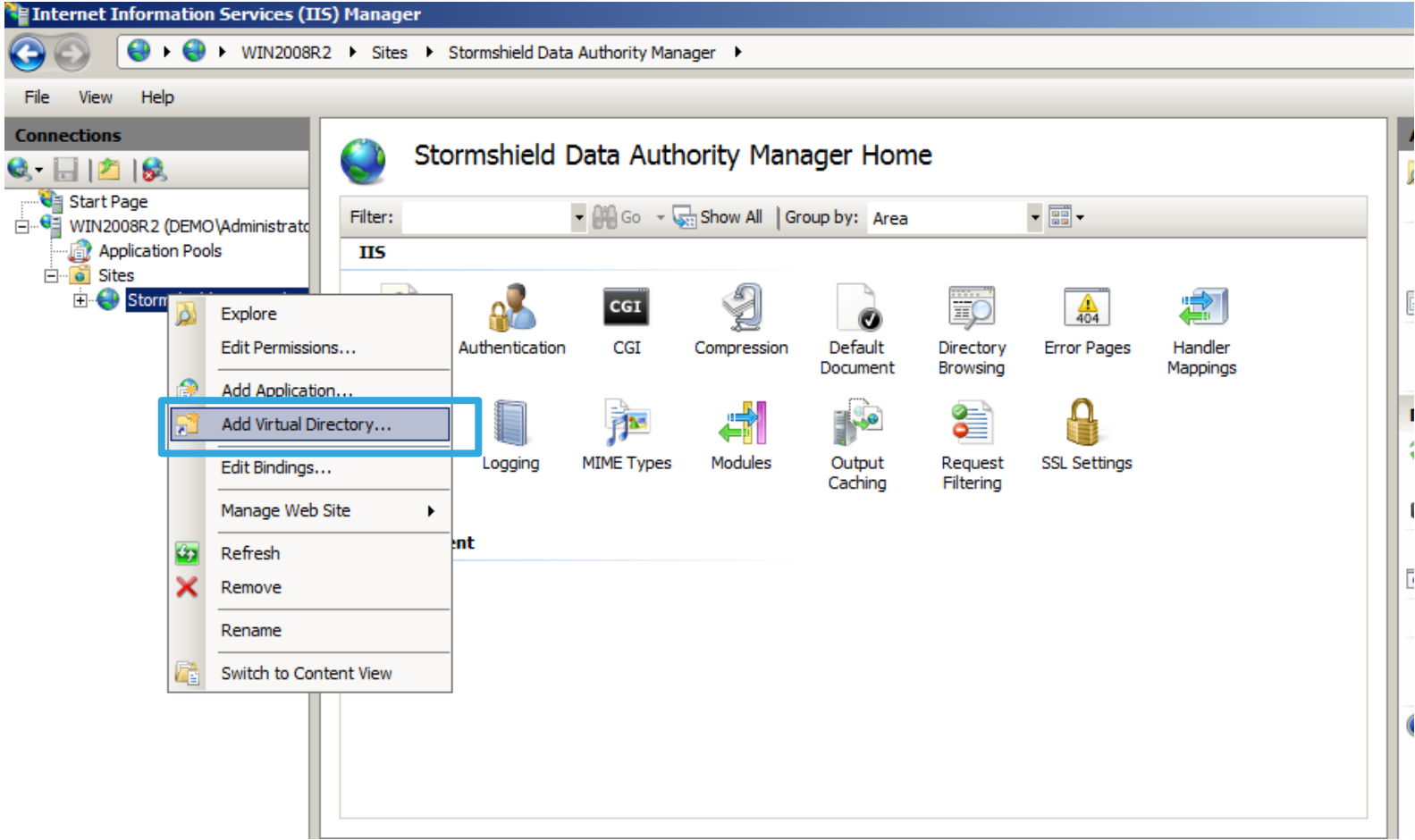
Confirm operation:



Configurer le répertoire virtuel du serveur IIS

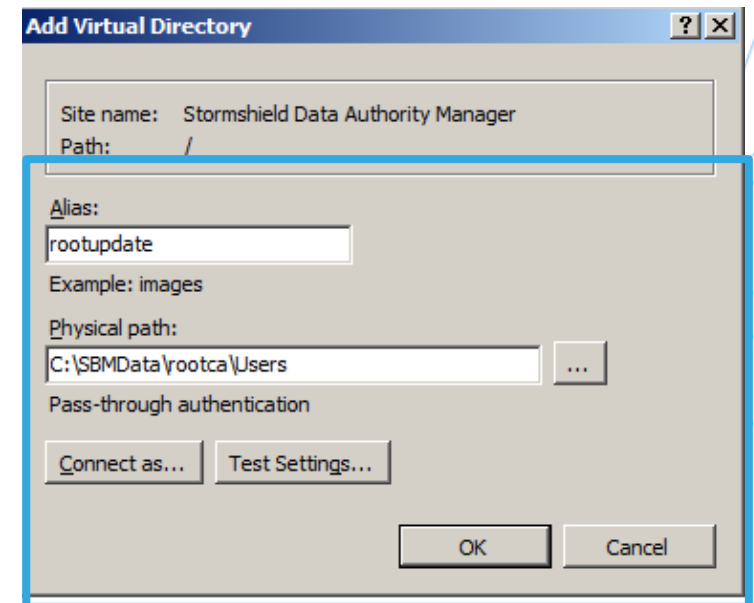
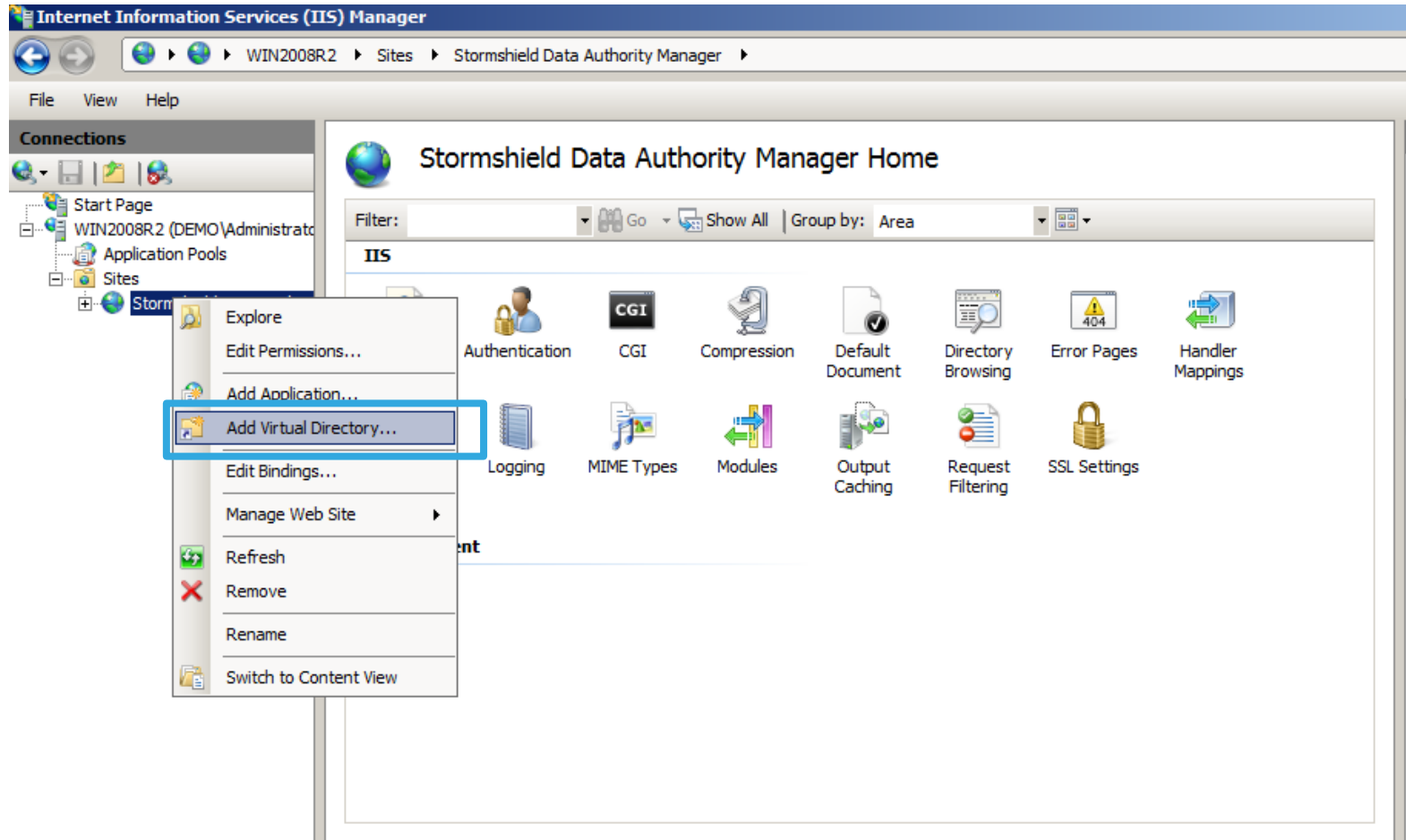
Configurer le serveur IIS

Créez un répertoire virtuel sur le serveur IIS, sous le site Web Stormshield Data Authority Manager correspondant au service de CRL.



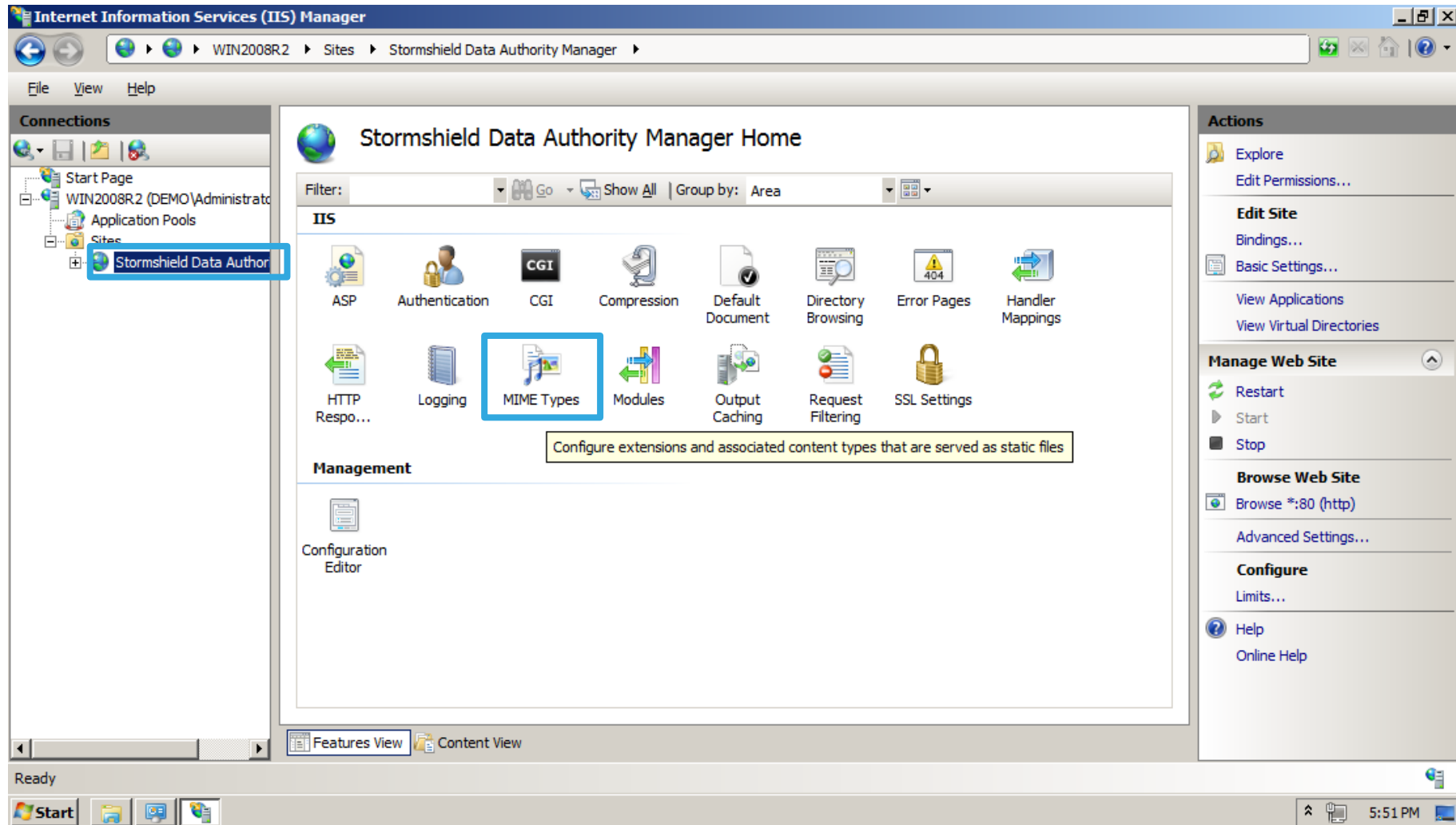
Configurer le serveur IIS (suite)

Créez un répertoire virtuel sur le serveur IIS, sous le site Web Stormshield Data Authority Manager, afin de pouvoir distribuer les fichiers de mise à jour pour SDS.



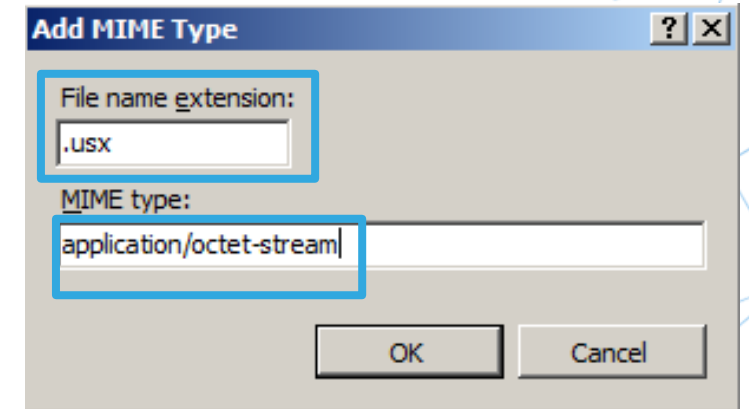
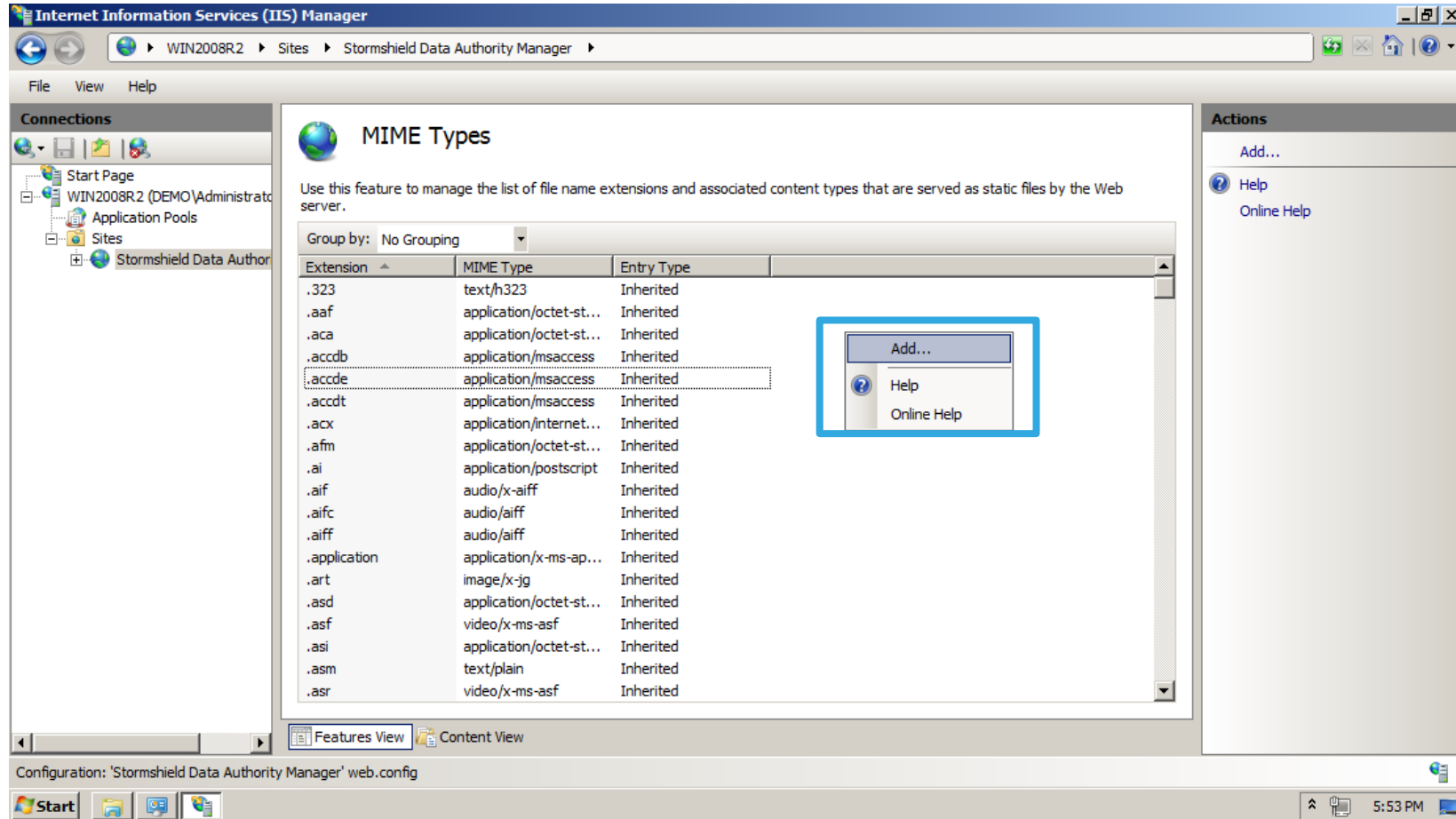
Configurer le serveur IIS (suite)

Double-cliquez sur **Types MIME**.



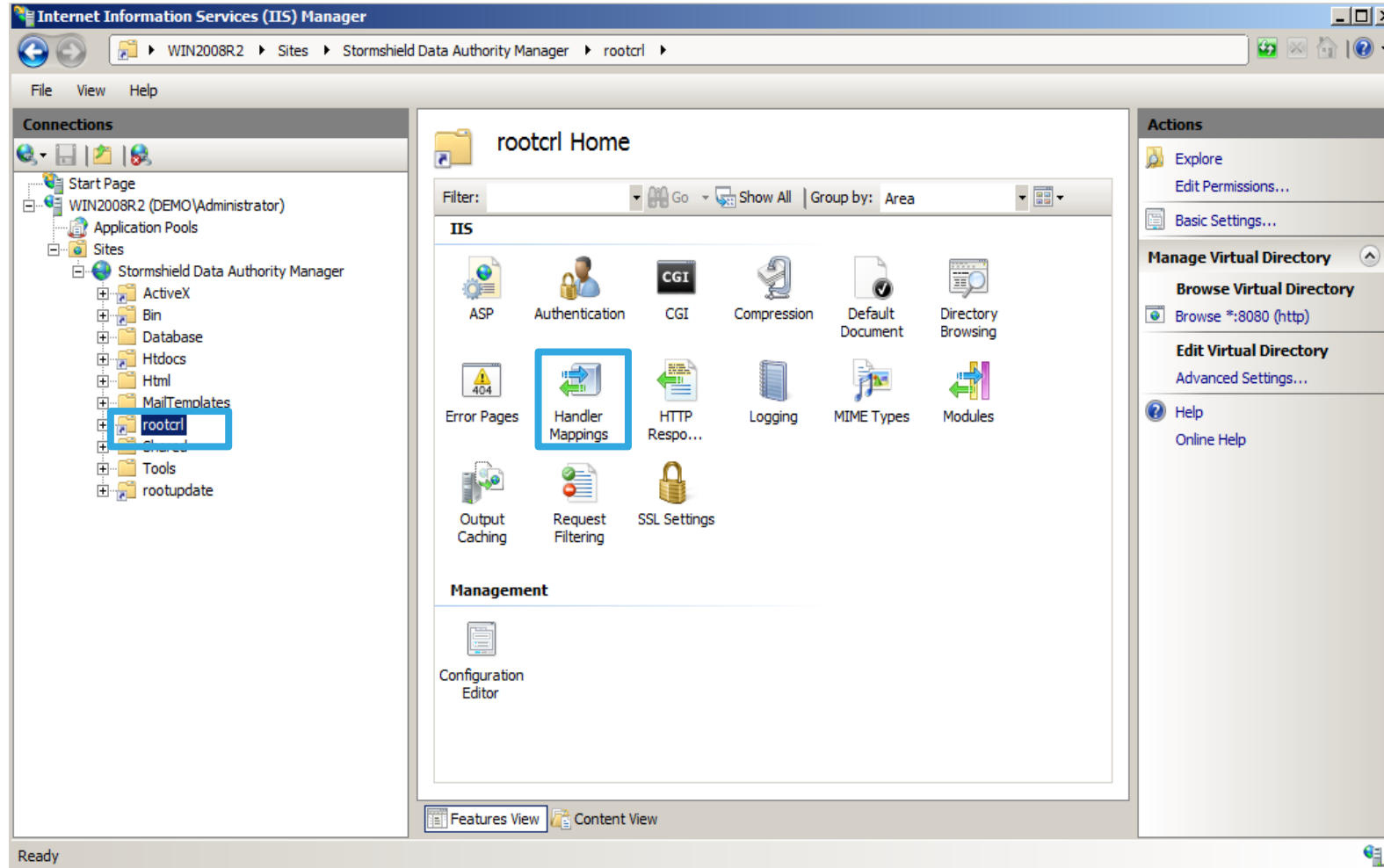
Configurer le serveur IIS (suite)

Faites un clic droit et sélectionnez **Ajouter**, afin d'ajouter les types MIME *.usx*.



Configurer le serveur IIS (suite)

Développez l'entrée **Stormshield Data Authority Manager** et cliquez sur le répertoire virtuel **rootcr1**. Double-cliquez sur **Mappages de gestionnaires**.



Configurer le serveur IIS (suite)

Cliquez sur **Modifier les autorisations de fonction**, cochez l'option **Lire** et cliquez sur **OK**.

Internet Information Services (IIS) Manager

WIN2008R2 > Sites > Stormshield Data Authority Manager > rootcr

File View Help

Connections

- Start Page
- WIN2008R2 (DEMO\Administrator)
- Application Pools
- Sites
 - Stormshield Data Authority Manager
 - ActiveX
 - Bin
 - Database
 - Htdocs
 - Html
 - MultiTemples
 - rootcr**
 - Shared
 - Tools
 - rootupdate

Handler Mappings

Use this feature to specify the resources, such as DLLs and managed code, that handle responses for specific request types.

Group by: State

Name	Path	State	Path Type
Disabled			
CGI-exe	*.exe	Disabled	File
ISAPI-dll	*.dll	Disabled	File
StaticFile	*	Disabled	File or Folder
Enabled			
ASPClassic	*.asp	Enabled	File
aspq-Integrated-4.0	*.aspq	Enabled	Unspecified
aspq-ISAPI-4.0_32bit	*.aspq	Enabled	Unspecified
aspq-ISAPI-4.0_64bit	*.aspq	Enabled	Unspecified
AssemblyResourceLoader-Integr...	WebResource.axd	Enabled	Unspecified
AXD-ISAPI-4.0_32bit	*.axd	Enabled	Unspecified
AXD-ISAPI-4.0_64bit	*.axd	Enabled	Unspecified
cshtm-Integrated-4.0	*.cshtm	Enabled	Unspecified
cshtm-ISAPI-4.0_32bit	*.cshtm	Enabled	Unspecified
cshtm-ISAPI-4.0_64bit	*.cshtm	Enabled	Unspecified
cshtml-Integrated-4.0	*.cshtml	Enabled	Unspecified
cshtml-ISAPI-4.0_32bit	*.cshtml	Enabled	Unspecified

Actions

- Add Managed Handler...
- Add Script Map...
- Add Wildcard Script Map...
- Add Module Mapping...
- Edit Feature Permissions...**
- Revert To Parent
- View Ordered List...

Help

- Online Help

Features View Content View

Configuration: 'Stormshield Data Authority Manager/rootcr' web.config

Edit Feature Permissions

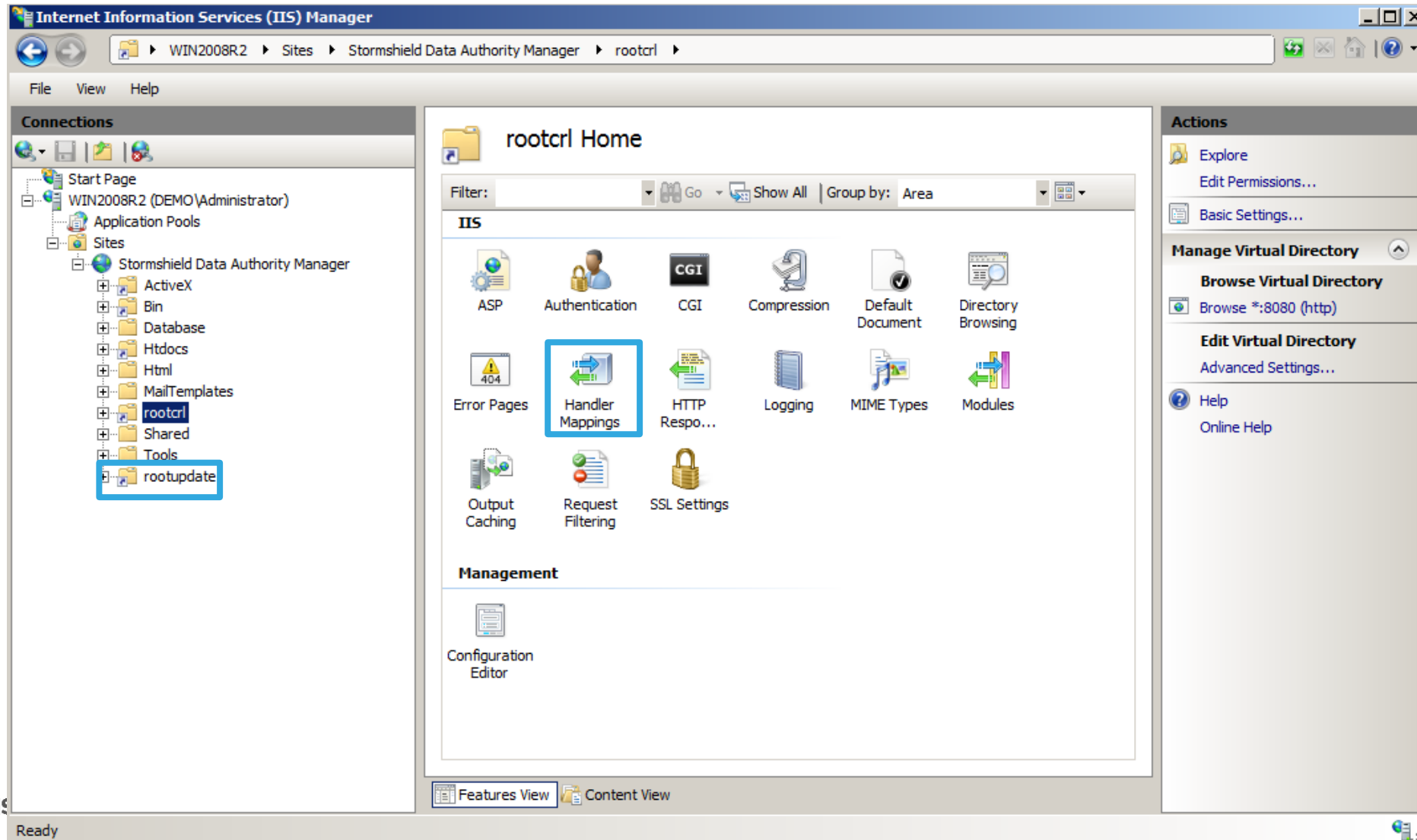
Permissions:

- Read
- Script
- Execute

OK Cancel

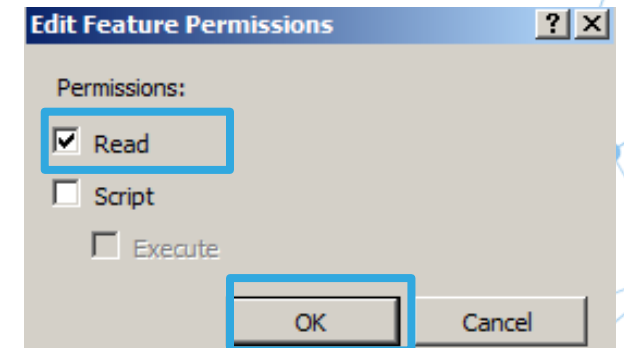
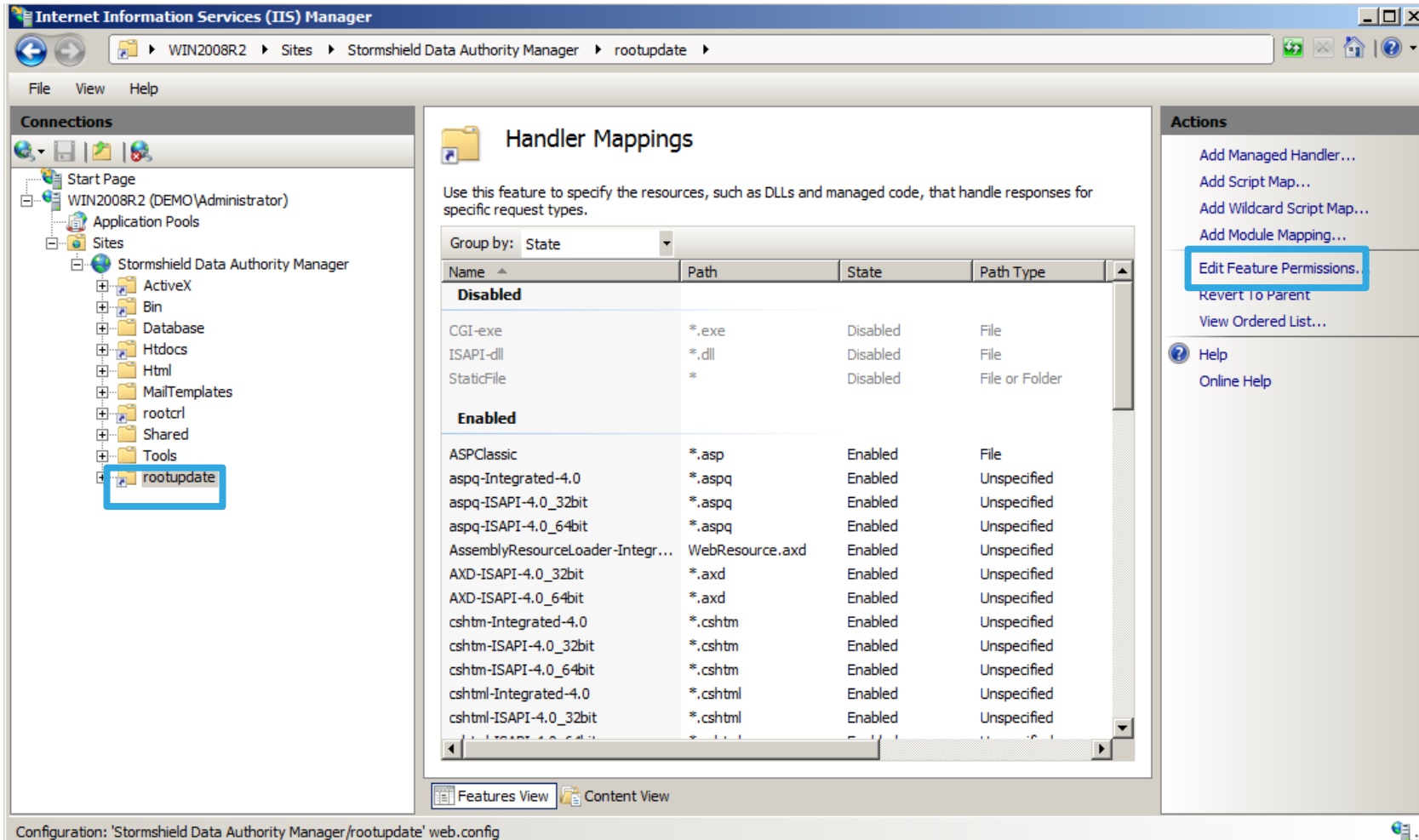
Configurer le serveur IIS (suite)

Sélectionnez le répertoire virtuel **rootupdate** et double-cliquez sur **Mappages de gestionnaires**.



Configurer le serveur IIS (suite)

Cliquez sur **Modifier les autorisations de fonction**, cochez l'option **Lire** et cliquez sur **OK**.





Configurer le serveur Exchange (option)

Configurer le connecteur Exchange entrant

The screenshot shows the Exchange Management Console (EMC) interface. The left-hand navigation pane is expanded to 'Hub Transport'. The main pane displays a table of Hub Transport objects:

Na...	Role	Version	Message Tracking Enabled
2K8R2	Hub Transport, Client Acc...	Version 14.2 (Build 247.5)	True

Below this table, the '2K8R2' object is selected, and the 'Receive Connectors' sub-pane shows a table with one entry:

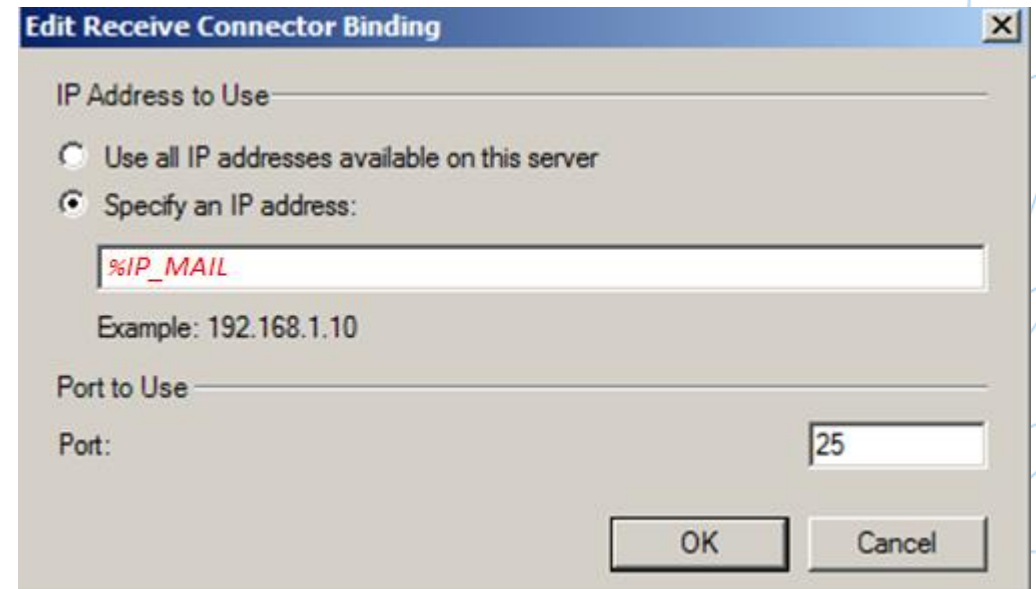
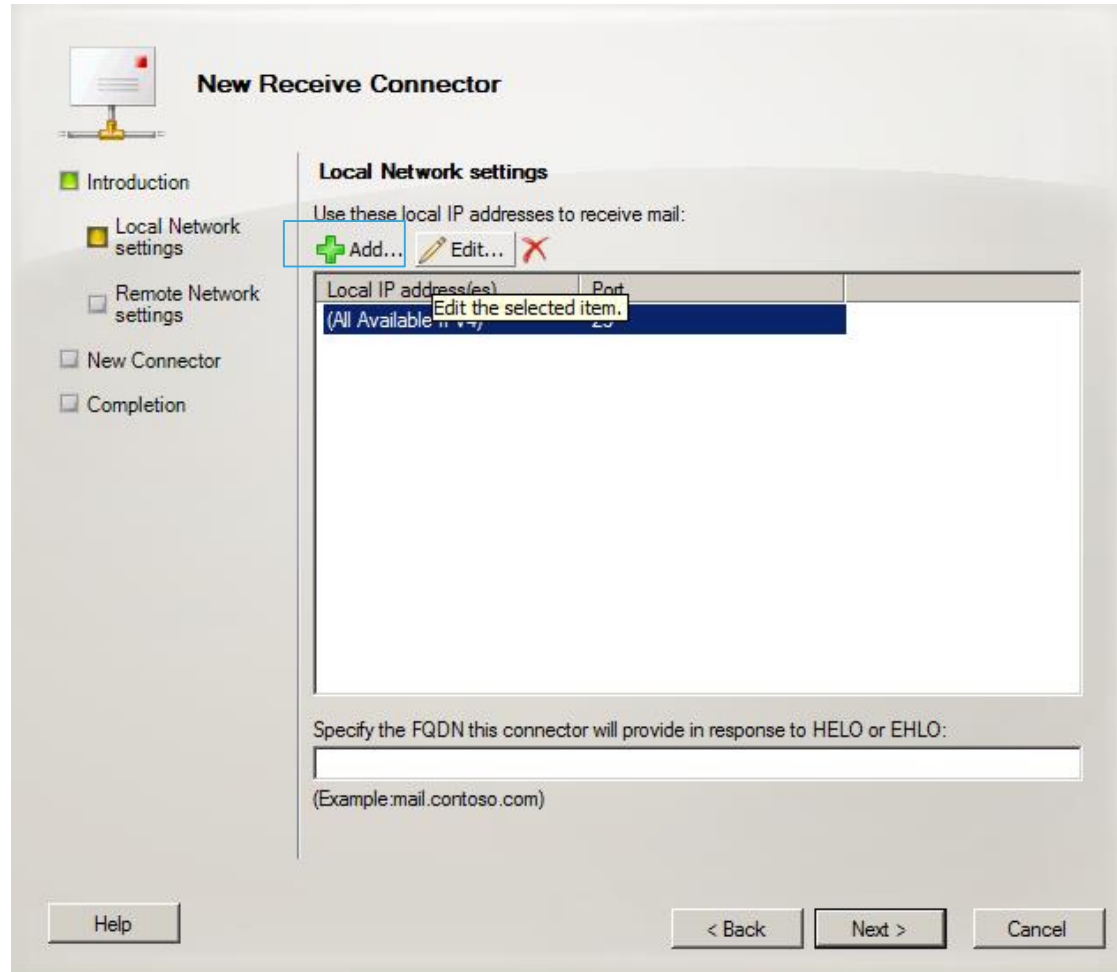
Name	Status
Default	Disabled

A context menu is open over the 'Default' connector, with 'New Receive Connector...' selected. The right-hand pane shows the 'Actions' menu for 'Hub Transport', with 'New Receive Connector...' visible under the '2K8R2' section.

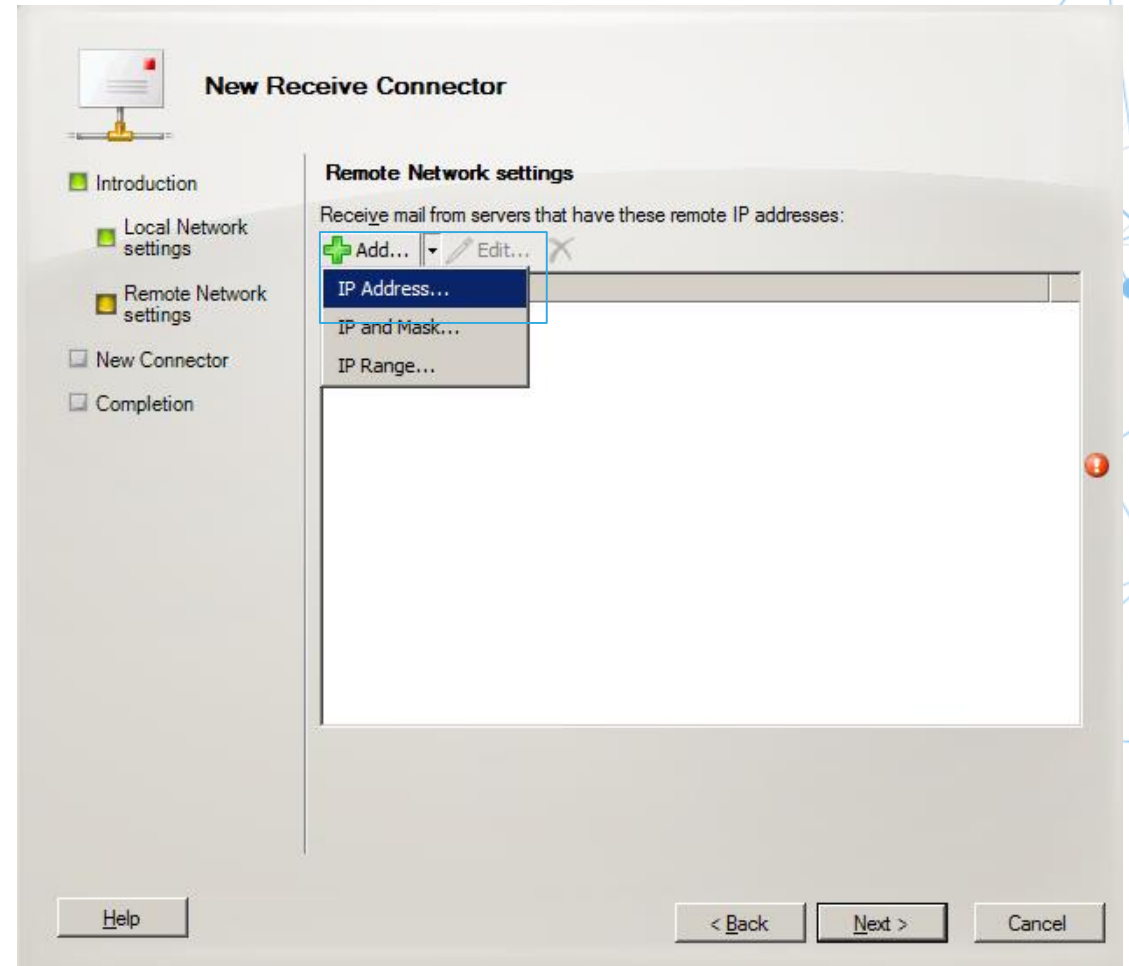
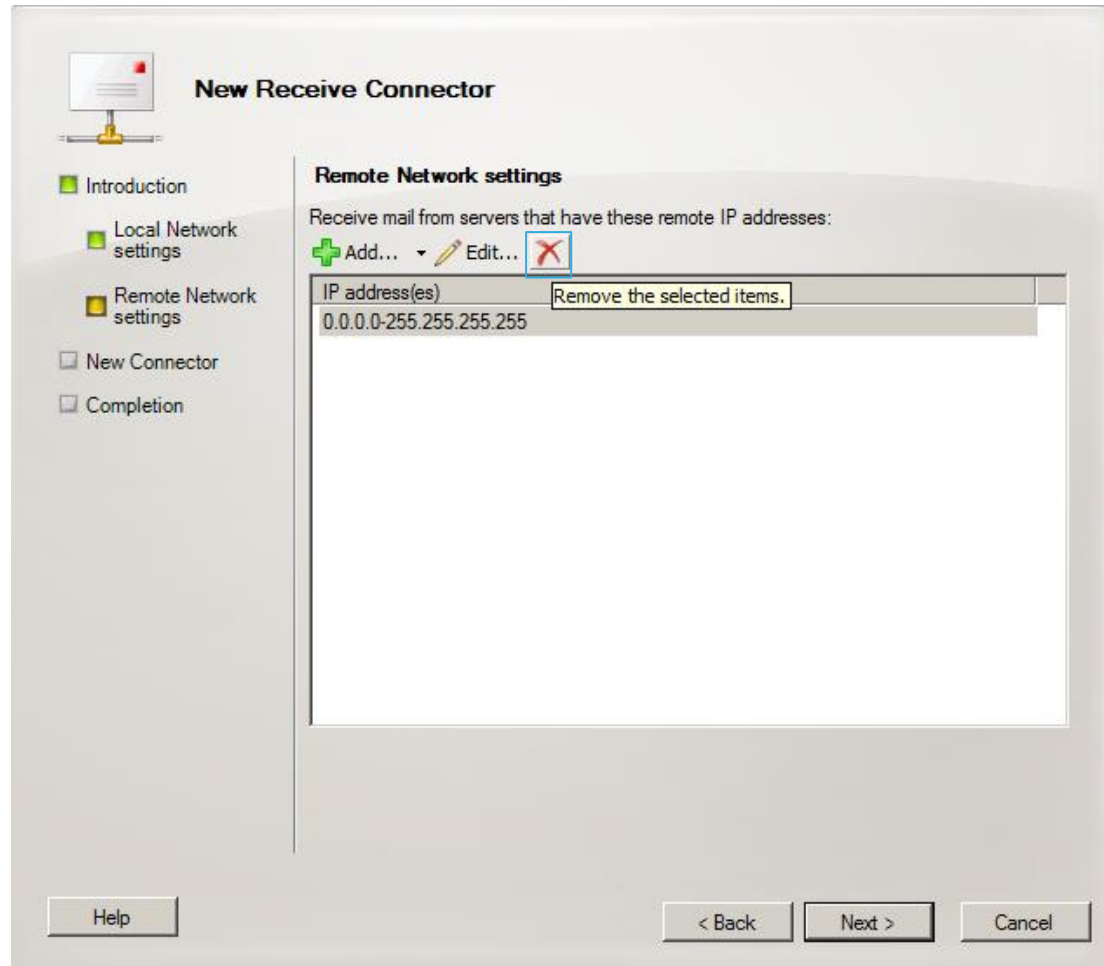
The screenshot shows the 'New Receive Connector' wizard. The 'Introduction' step is selected, and the 'Name' field contains 'SDAM'. The 'Intended use' dropdown is set to 'Custom'. The description reads: 'Description: Select this option to create a customized connector, which will be used to connect with systems that are not Exchange servers.'

Buttons at the bottom include 'Help', '< Back', 'Next >', and 'Cancel'.

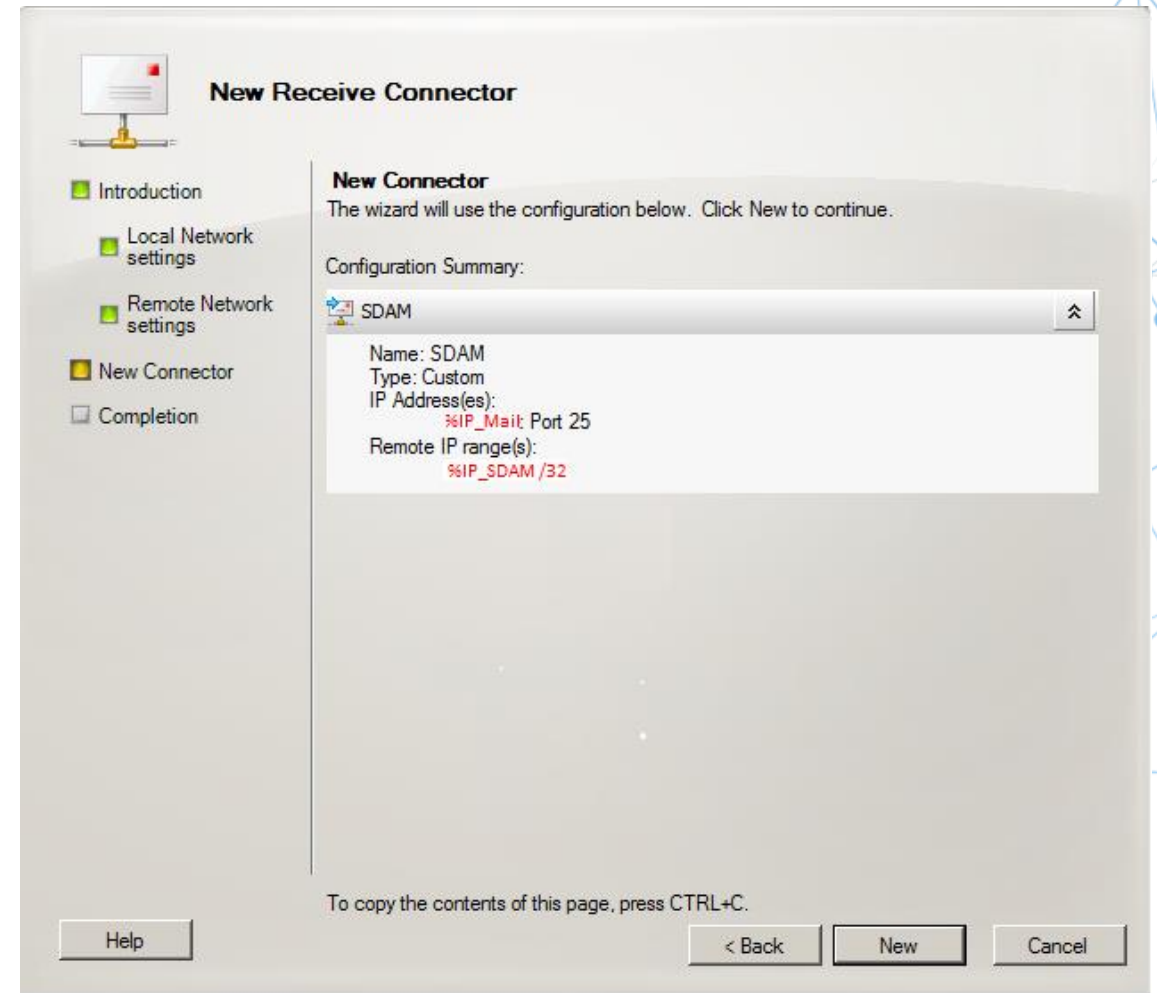
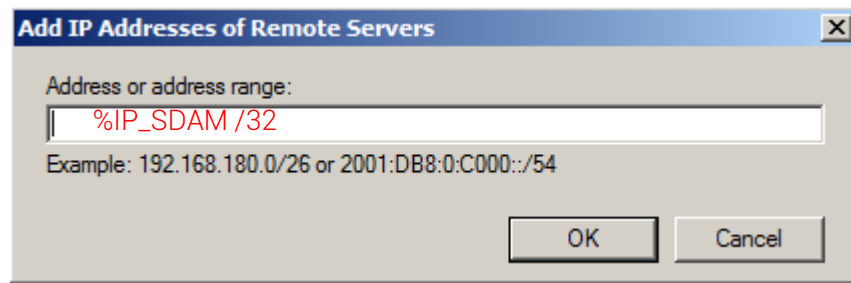
Configurer le connecteur Exchange entrant (suite)



Configurer le connecteur Exchange entrant (suite)



Configurer le connecteur Exchange entrant (suite)



Configurer le connecteur Exchange entrant (suite)

The screenshot shows the Exchange Management Console (EMC) interface. The left pane displays the hierarchy: Microsoft Exchange > Microsoft Exchange On-Premises > Server Configuration > Hub Transport. The main pane shows the 'Hub Transport' node with one object, '2K8R2'. Below it, the '2K8R2' node is expanded to show 'Receive Connectors'. A table lists the connectors:

Name	Status
Default	Disabled
SDAM	Enabled

The 'SDAM' connector is selected, and a context menu is open with 'Properties' highlighted. The 'Authentication' properties dialog box is open, showing the 'Authentication' tab. The 'Authentication' tab contains the following options:

- Enable Domain Security (Mutual Auth TLS)
- Basic Authentication
- Offer Basic authentication only after starting TLS
- Exchange Server authentication
- Integrated Windows authentication
- Externally Secured (for example, with IPsec)

The 'SDAM Properties' dialog box is also open, showing the 'Authentication' tab. It contains the following options:

- Specify who is allowed to connect to this Receive connector
- Anonymous users
- Exchange users
- Exchange servers
- Legacy Exchange Servers
- Partners

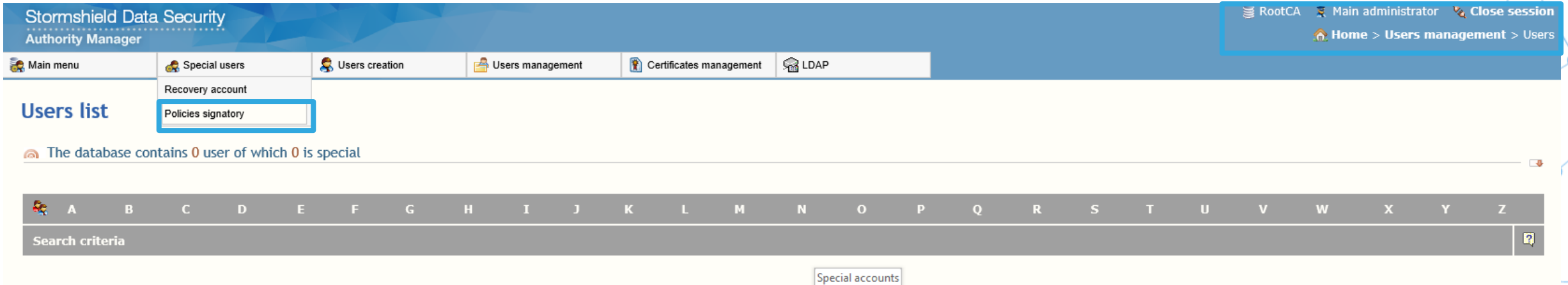


Créer des comptes SDS spéciaux

Comptes spéciaux

Vous devez maintenant créer deux utilisateurs spéciaux (Signataire et Recouvrement).

Cliquez sur **Gestion des utilisateurs** → **Utilisateurs** → **Utilisateurs spéciaux** → **Signataire de politique**.



The screenshot displays the Stormshield Data Security Authority Manager interface. The top navigation bar includes the title 'Stormshield Data Security Authority Manager' and user information: 'RootCA', 'Main administrator', and 'Close session'. Below the navigation bar, a menu is open under 'Special users', with 'Policies signatory' selected. The main content area shows a message: 'The database contains 0 user of which 0 is special'. Below this is a search bar with a 'Search criteria' field and a 'Special accounts' button.

Comptes spéciaux (suite)

Security policies signatory creation

User

Identifier	Signatory account
Description	Signatory account

Account

User account protection algorithms

Encryption: AES 256 bits

Thumbprint: SHA-256

User passwords

Initial password: hCe2G2h1pSf7

Security officer password for user account

Disable the security officer password

Use the following security officer password:

epiAwfPBuSPG+hkA

General password

This password will allow you to unblock the account of a user if he/she loses his/her password.

User's identity

Name	Signatory
Given name	Account
Organization	Stormshield
Organization unit	StormshiedIPOC
City	Milano
State or province	Lombardia
Country	Italy (IT)
Email address	

Key and certificate

Key and certificate

Certification mode: Internal CA - Signature

Validity period: 10 years Until Wednesday, February 23, 2028

Key role: Encryption Signature

Key algorithm: RSA 2048 bits

Subject: CN=Signatory Account,S=Signatory,GN=Account,L=Milano,OU=StormshiedIPOC,O=Stormshie

Publication

DN of LDAP entry: cn=Signatory Account,ou=StormshiedIPOC,o=Stormshield

Comptes spéciaux (suite)

Cliquez sur **Gestion des utilisateurs** → **Utilisateurs** → **Utilisateurs spéciaux** → **Compte de recouvrement**.

The screenshot displays the Stormshield Authority Manager interface. The top navigation bar includes the logo and title 'Stormshield Data Security Authority Manager' on the left, and user information 'RootCA Main administrator Close session' and a breadcrumb trail 'Home > Users management > Users' on the right. Below the navigation bar is a menu with options: 'Main menu', 'Special users', 'Users creation', 'Users management', 'Certificates management', and 'LDAP'. The 'Special users' menu is open, showing 'Recovery account' (highlighted) and 'Policies signatory'. The main content area shows the heading 'Users list' and a status message: 'The database contains 0 user of which 0 is special'. Below this is a search bar with a grid of letters A-Z and a 'Search criteria' input field. A 'Special accounts' button is located at the bottom of the page.

Comptes spéciaux (suite)

Recovery account creation

User

Identifier	Recovery Account
Description	Recovery Account

Account

User account protection algorithms

Encryption	AES 256 bits
Thumbprint	SHA-256

User passwords

Initial password

Security officer password for user account

Disable the security officer password

Use the following security officer password:

General password

This password will allow you to unblock the account of a user if he/she loses his/her password.

User's identity

Name	Recovery
Given name	Account
Organization	Stormshield
Organization unit	StormshieldPOC
City	Milan
State or province	Lombardia
Country	Italy (IT)
Email address	

Publication

Certification mode	Internal CA - Encryption
Validity period	10 years Until Wednesday, February 23, 2028
Key role	<input checked="" type="checkbox"/> Encryption <input type="checkbox"/> Signature
Key algorithm	RSA 2048 bits
Subject	CN=Recovery Account,S=Recovery,GN=Account,L=Milan,OU=StormshieldPOC,O=Stormshield

Usage of recovery certificate

This certificate will be register as a recovery certificate in all users accounts in this database.

Attributes	<input checked="" type="checkbox"/> Visible to every user to whom it is applied <input type="checkbox"/> Modifiable by all the users to whom it is applied
Stormshield Data Security components on which it is applied	<input checked="" type="checkbox"/> All Stormshield Data Security components <input type="checkbox"/> Security BOX SmartFILE <input type="checkbox"/> Stormshield Data Virtual Disk <input type="checkbox"/> Stormshield Data File <input type="checkbox"/> Stormshield Data Mail <input type="checkbox"/> Stormshield Data Team

Cliquez sur Créer un utilisateur.



Définir la configuration de compte SDS

Paramètres utilisateur

Cliquez sur Menu principal → Paramètres → Gestion des utilisateurs.

User creation

Security officer password for the user accounts

By default, use this password for all accounts:

Suggest (and store) a different password for each account

Disable security officer password for all accounts

Subject resolution mask: CN=<CommonName>,S=<SurName>,GN=<GivenName>,L=<Locality>,OU=<OrgUnit>,O=<Or

Common name format

Surname followed by given name

Given name followed by surname

Distribution

User account distribution folder: C:\SBMDData\rootca\Users

Number of password entry attempts before locking

3 for the user password

3 for the security officer password

Card account

Make a copy of the private and public keys into the user account

Address book

Add to each user's address book the certificates of all users present in the database

Thumbprint algorithm for updates (.usx)

Thumbprint algorithm used for signature: SHA-256

LDAP publication of updates (.usx)

Activate LDAP publication of updates

Caution, chose this option only if the users' LDAP entries belong to a class that accepts the update publication attribute, as set in the LDAP configuration.

File-based publication of updates (.usx)

Activate file-based publication of updates

Publication folder:

File-based publication of setup files (.usi)

Activate file-based publication of setup files (.usi)

Publication folder:

Certificate import and export

User certificate import and export folder: C:\SBMDData\rootca\Certs

Certificate import

Authorize import of old certificates

Format for certificate export: C:\SBMDData\rootca\Certs

Binary format

Trust chain export

Add trust chain when exporting certificates

Extension for exporting several certificates

p7b extension

p7c extension

sbc extension

Email notifications

Send an information email before the certificates expiration

Information email

Number of days: 30

Frequency: 7 days

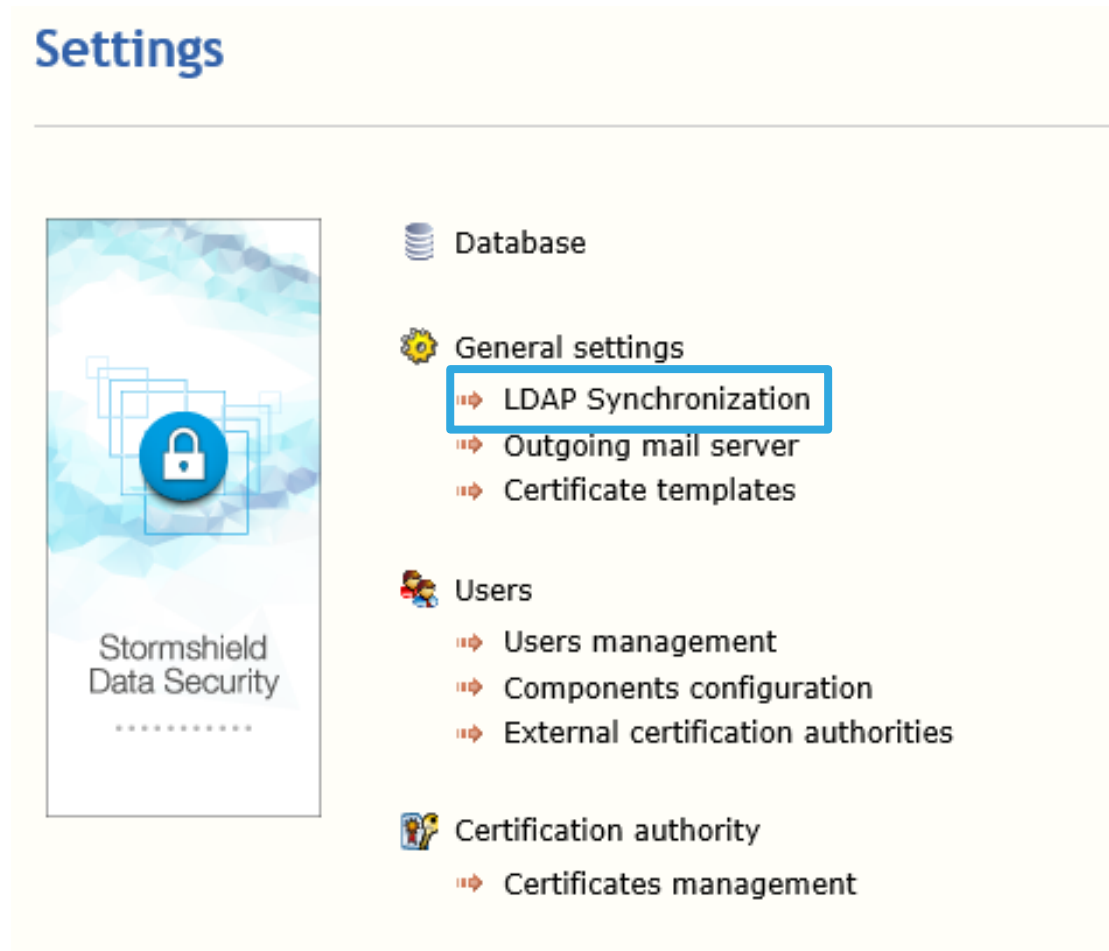
Email address:

Template: C:\SBMDData\rootca\MailTemplates\template_expiration_email.sbp

Cliquez sur Appliquer les modifications.

Option : Paramètres LDAP

Cliquez sur **Menu principal** → **Paramètres** → et sélectionnez **Synchronisation LDAP**.



Settings

Stormshield
Data Security
.....

- Database
- General settings
 - LDAP Synchronization**
 - Outgoing mail server
 - Certificate templates
- Users
 - Users management
 - Components configuration
 - External certification authorities
- Certification authority
 - Certificates management

Option : Paramètres LDAP (suite)

LDAP synchronization settings

Server

Server name	<input type="text" value="%HOSTNAME_LDAP"/>
Port number	<input type="text" value="389"/>
LDAP version	<input type="text" value="2"/>
Protocol	<input type="checkbox"/> SSL
Encoding	<input type="radio"/> UTF-8 <input checked="" type="radio"/> ANSI
Duration of a connection attempt	<input type="text" value="30"/> seconds

Authentication

Authentication selection	<input checked="" type="radio"/> Authentication with a plaintext password
DN:	<input type="text" value="cn=Administrator,CN=users,DC=stotrmshiedl,dc=corp"/>
Password:	<input type="password" value="*****"/>
<input type="radio"/> Negotiated authentication	
Domain or workgroup name:	<input type="text"/>
User name:	<input type="text"/>
Password:	<input type="password"/>

Si vous êtes connecté à AD, désignez *sAMAccountName* comme identifiant.

Search

Base DN	<input type="text" value="CN=users,DC=stotrmshiedl,dc=corp"/>
Class of recognition for "person" type entry	<input type="text" value="person"/>
Search time limit	<input type="text" value="30"/> seconds

Publication

Keys to be published	<input type="radio"/> All keys <input checked="" type="radio"/> The key with the encryption role and the key with the signature role
----------------------	---

Publication of new certificates

DN resolution mask	<input type="text" value="cn=<CommonName>,ou=<OrgUnit>,o=<Organization>"/>
--------------------	--

Name of attributes

Email address	<input type="text" value="mail"/>
Common name	<input type="text" value="cn"/>
Certificate in binary format	<input type="text" value="userCertificate;binary"/>
Identifier	<input type="text" value="uid"/> <i>Ou sAMAccountName si vous êtes connecté à Microsoft Active Directory.</i>
Given name	<input type="text" value="givenName"/>
Name	<input type="text" value="sn"/>
Authority certificate in binary format	<input type="text" value="caCertificate;binary"/>
CRL in binary format	<input type="text" value="certificateRevocationList;binary"/>
Security policies update in binary format	<input type="text" value="sboxPolicyUpgrade;binary"/>

Option : Paramètres SMTP

Cliquez sur **Menu principal** → **Paramètres** → **Serveur d'e-mail sortant** et entrez toutes les informations nécessaires pour autoriser le SDAM à envoyer des e-mails à l'aide de votre serveur d'e-mail.

Stormshield Data Security
Authority Manager

Child-CA Main administrator Close session
Home > Settings > Outgoing mail server

Main menu

Outgoing mail server settings

SMTP Server

Name of local server	<input type="text" value="%HOSTNAME_SDAM"/>
Name of remote server	<input type="text" value="%HOSTNAME_MAIL"/>
Port number	<input type="text" value="25"/>

Connection identifier

Username	<input type="text"/>
Password (non-hidden)	<input type="text"/>
Sender's email address	<input type="text" value="no-reply.sdram@demo.local"/>

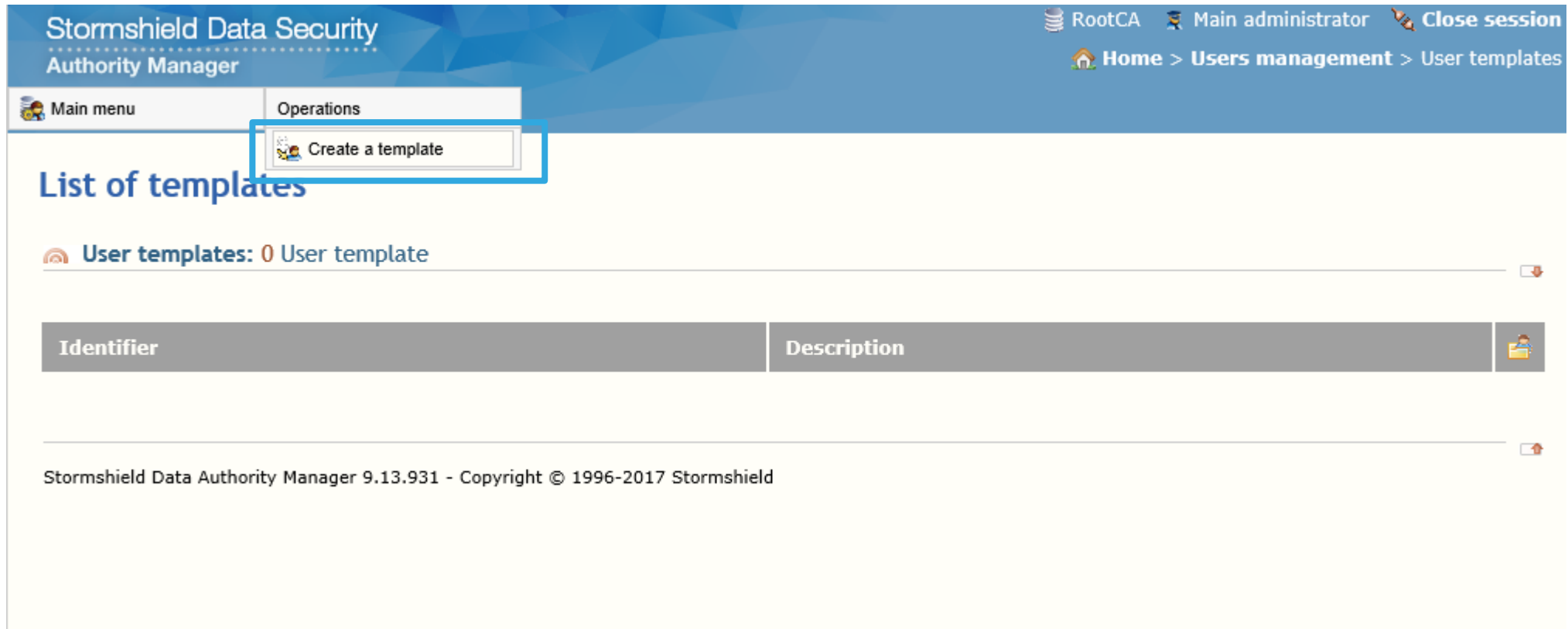
Confirm operation:



Créer des modèles de compte SDS

Créer un modèle

Cliquez sur **Menu principal** → **Gestion des utilisateurs** → **Modèles utilisateur**.
Cliquez ensuite sur **Opérations** → **Créer un modèle**.



The screenshot displays the Stormshield Data Security Authority Manager interface. At the top, the header includes the logo and name 'Stormshield Data Security Authority Manager' on the left, and user information 'RootCA Main administrator' with a 'Close session' link on the right. Below the header, a navigation bar shows 'Main menu' and 'Operations'. The 'Operations' menu is expanded, highlighting the 'Create a template' option. The main content area is titled 'List of templates' and shows 'User templates: 0 User template'. Below this, there is a table with columns 'Identifier' and 'Description'. The footer contains the text 'Stormshield Data Authority Manager 9.13.931 - Copyright © 1996-2017 Stormshield'.

Créer un modèle (suite)

Stormshield Data Security Authority Manager

RootCA Main administrator Close session

Home > Users management > Templates > Template creation

Main menu

Template creation

Template

Identifier	Template1
Description	
Master's password	
DN of LDAP entry used for update file publication	

Users accounts

User accounts protection algorithms	Encryption	AES 256 bits
	Thumbprint	SHA-256

Security officer password for user accounts

Disable the security officer password

Generate a different backup password for every user

Use the following security officer password:

This password will allow you to unblock the account of a user if he/she loses his/her password.

Users' identities

Organization	Stormshield
Organization unit	StormshieldPOC
City	Milan
State or province	Lombardia
Country	Italy (IT)

Users keys and certificates

Key 1

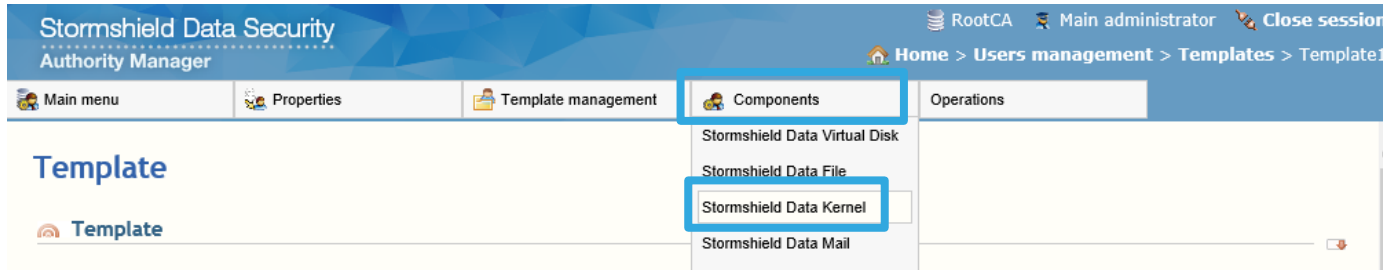
Certification mode	Internal CA - Encryption
Validity period	2 years Until Sunday, February 23, 2020
Key role	<input checked="" type="checkbox"/> Encryption <input type="checkbox"/> Signature
Key algorithm	RSA 2048 bits

Key 2

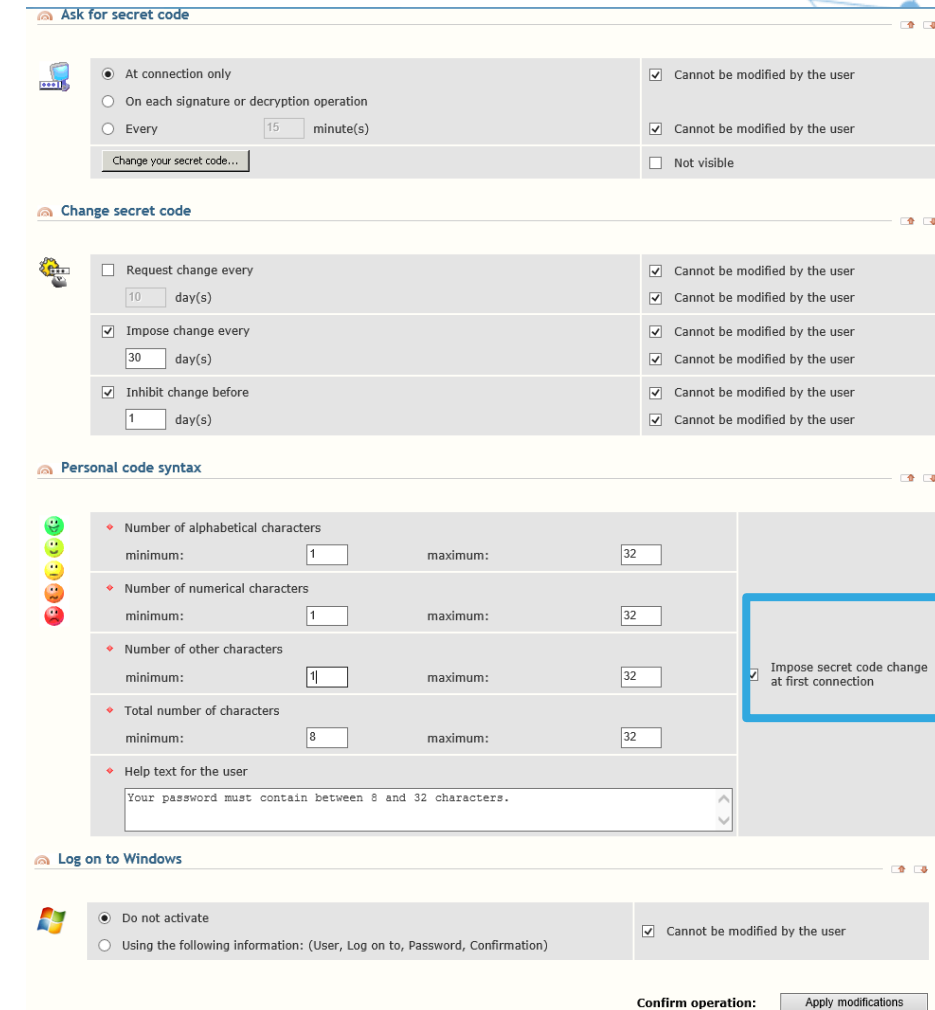
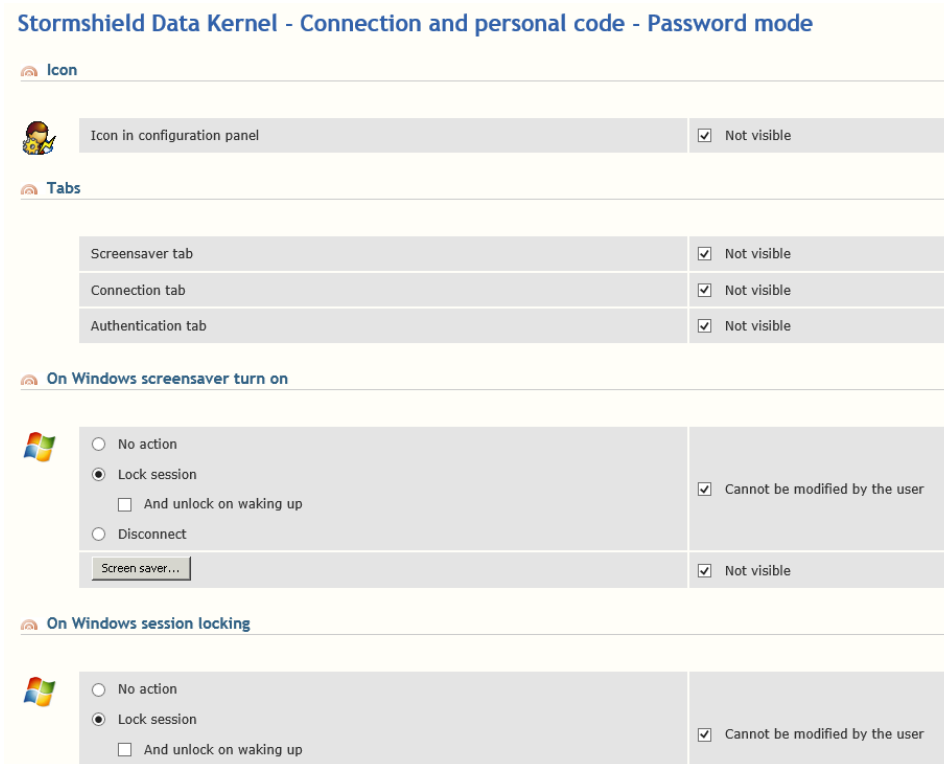
Certification mode	Internal CA - Signature
Validity period	2 years Until Sunday, February 23, 2020
Key role	<input type="checkbox"/> Encryption <input checked="" type="checkbox"/> Signature
Key algorithm	RSA 2048 bits

Créer un modèle (suite) : configurer le POC

Cliquez sur **Menu principal** → **Gestion des utilisateurs** → **Modèle utilisateur** et sélectionnez le modèle que vous avez déjà créé.



Cliquez sur **Connexion et code personnel** – Mode mot de passe



Cliquez sur **Appliquer les modifications**.

Mettre à jour automatiquement les profils

Cliquez sur **Menu principal** → **Gestion des utilisateurs** → **Modèle utilisateur** et sélectionnez le modèle que vous avez déjà créé. Cliquez ensuite sur **Composants** → **Stormshield Data Kernel**.

Sélectionnez **Mise à jour automatique** et entrez la valeur suivante dans la section **Téléchargement** :
`http://%IP_SDAM:port/update/<UserId>/<UserId>.usx`

The screenshot shows the Stormshield Data Security web interface. The breadcrumb navigation is: Home > Users management > Templates > Template1 > Stormshield Data Kernel > Automatic update. The page title is "Stormshield Data Kernel - Automatic update".

Automatic update section:

- Icon in configuration panel: Not visible
- Deactivate automatic update
- Cannot be modified by the user
- Protocols:** Activate automatic update with the following protocols
 - HTTP (web)
 - HTTP secured by SSL
 - LDAP (directory access)
 - LDAP secured by SSL
 - FILE (file copy)
 - Cannot be modified by the user
 - Cannot be modified by the user
 - Cannot be modified by the user
 - Cannot be modified by the user
 - Cannot be modified by the user

Download section:

- Input field: `http://%IP_SDAM:port/update/<UserId>/<UserId>.usx`
- The user is not allowed to add distribution points
- Cannot be modified
- Cannot be deleted
- Buttons: Add, Delete

Distribution points:

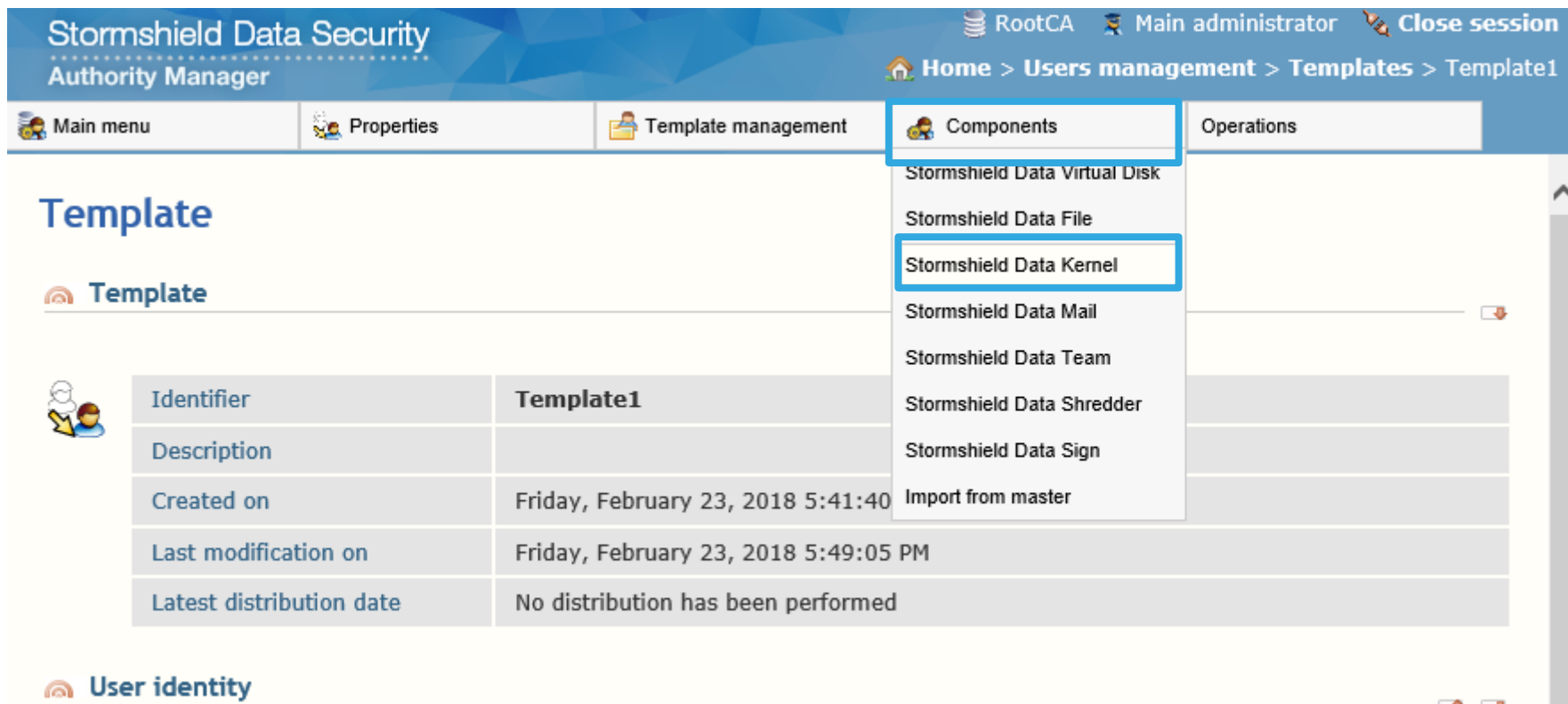
- Input field: `http://%IP_SDAM:port/update/<UserId>/<UserId>.usx`
- Buttons: Add, Delete

Confirm operation:

Cliquez sur **Appliquer les modifications**.

Configurer la CRL

Cliquez sur **Menu principal** → **Gestion des utilisateurs** → **Modèle utilisateur** et sélectionnez le modèle que vous avez déjà créé. Cliquez ensuite sur **Composants** → **Stormshield Data Kernel**.



The screenshot shows the Stormshield Data Security Authority Manager interface. The top navigation bar includes the logo, user information (RootCA, Main administrator), and a 'Close session' button. The breadcrumb trail is 'Home > Users management > Templates > Template1'. The main navigation menu has 'Main menu', 'Properties', 'Template management', 'Components', and 'Operations'. The 'Components' menu is open, showing a list of options: Stormshield Data Virtual Disk, Stormshield Data File, Stormshield Data Kernel (highlighted), Stormshield Data Mail, Stormshield Data Team, Stormshield Data Shredder, Stormshield Data Sign, and Import from master. The main content area displays the 'Template' details for 'Template1' in a table format.

Identifier	Template1
Description	
Created on	Friday, February 23, 2018 5:41:40
Last modification on	Friday, February 23, 2018 5:49:05 PM
Latest distribution date	No distribution has been performed

Configurer la CRL (suite)


Cliquez sur **Contrôleur de révocation** et cliquez sur le bouton mis en évidence ci-dessous.

Stormshield Data Security
Authority Manager Home > Users management > Templates > Template1 > Stormshield Data Kernel > Revocation controller


Main menu

Stormshield Data Kernel - Revocation controller

General settings

 Icon in configuration panel	<input type="checkbox"/> Not visible
<input type="checkbox"/> Do not control the revocation state	<input checked="" type="checkbox"/> Cannot be modified by the user
CRLs default validity period (days) <input type="text" value="7"/>	<input type="checkbox"/> Cannot be modified by the user
Protocols: Activate revocation lists downloads with the following protocols:	
<input checked="" type="checkbox"/> HTTP (web)	<input checked="" type="checkbox"/> Cannot be modified by the user
<input checked="" type="checkbox"/> HTTP secured by SSL	<input checked="" type="checkbox"/> Cannot be modified by the user
<input checked="" type="checkbox"/> LDAP (directory access)	<input checked="" type="checkbox"/> Cannot be modified by the user
<input checked="" type="checkbox"/> LDAP secured by SSL	<input checked="" type="checkbox"/> Cannot be modified by the user
<input checked="" type="checkbox"/> FILE (file copy)	<input checked="" type="checkbox"/> Cannot be modified by the user

Issuers


 RootCA	<input checked="" type="checkbox"/> Prohibit adding issuers
<input type="checkbox"/> Do not control the revocation state	<input type="checkbox"/> Prohibit deleting this issuer from the list
Validity length (days) <input type="text" value="7"/>	<input type="checkbox"/> Cannot be modified by the user

Buttons: Delete, Add database authority: Add, Add an external issuer: Add


Configurer la CRL (suite)


Ajoutez un point de distribution de CRL externe :
http://%IP_SDAM:port/rootcr/rootca.crl


Revocation lists downloading rule:


 Download at the first encryption operation (recommended) ▼


Custom distribution points:

 Enter in order of priority









Cannot be modified by the user

The user is not allowed to add distribution points

Cannot be modified Cannot be deleted

Cannot be modified Cannot be deleted

Cannot be modified Cannot be deleted

Cannot be modified Cannot be deleted

Confirm operation:



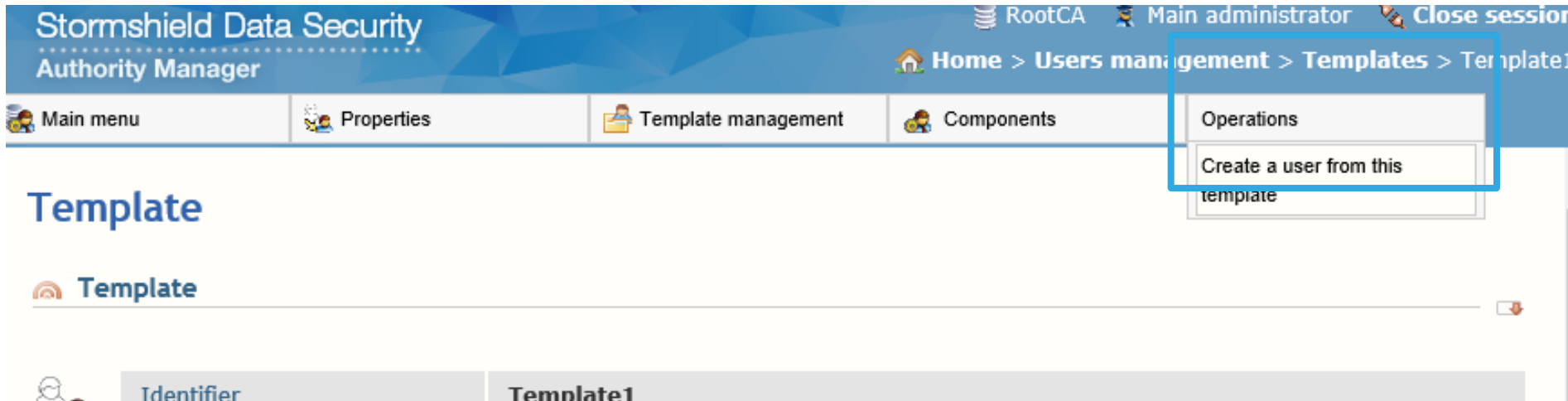


Créer des comptes d'utilisateur SDS

Créer un compte à partir d'un modèle

Cliquez sur **Menu principal** → **Gestion des utilisateurs** → **Modèle utilisateur** et sélectionnez le modèle 1, puis cliquez sur **Opération** → **Créer un utilisateur depuis ce modèle**.

Cette opération vous permet de créer manuellement un utilisateur sur le SDAM mais, si vous souhaitez créer un utilisateur depuis votre annuaire Active Directory, consultez la diapositive suivante.



Créer des utilisateurs via LDAP

Cliquez sur **Menu principal** → **Utilisateurs** → **LDAP** et sélectionnez **Synchronisation LDAP**.

The screenshot displays the Stormshield Data Security Authority Manager interface. At the top, the header includes the product name and user information: "Stormshield Data Security Authority Manager", "RootCA", "Main administrator", and "Close session". Below the header is a navigation menu with options: "Main menu", "Special users", "Users creation", "Users management", "Certificates management", "LDAP", and "LDAP Synchronization". The "LDAP" option is highlighted, and its sub-menu "LDAP Synchronization" is visible. The main content area is titled "Users list" and shows a status message: "The database contains 0 user of which 0 is special". Below this is a search bar with a "Search criteria" input field and a search icon. A navigation bar with letters A through Z is also present.

Créer des utilisateurs via LDAP (suite)

Cliquez sur **À associer ou utiliser pour créer des utilisateurs**.

Stormshield Data Security Authority Manager

RootCA Main administrator %HOSTNAME_LDAP:389 Close session

Home > Users management > Users > LDAP Synchronization

Synchronization with the LDAP directory

Search LDAP entries

- To associate or use to create users
- To associate to users not yet associated

Import certificates from the LDAP directory

- For all users
- For users with at least one non-certified key

Caution, this operation may take several minutes.

Publish users certificates on the LDAP directory

- All certificates
- Certificates which are not yet published

Caution, this operation may take several minutes.

Stormshield Data Authority Manager 9.13.931 - Copyright © 1996-2017 Stormshield

Stormshield Data Security Authority Manager

RootCA Main administrator %HOSTNAME_LDAP:389 Close session

Home > Users management > Users > LDAP Synchronization > Users creation

Users creation from the LDAP directory

Description

This action lists all entries of the LDAP directory. For each entry not yet associated to a user, it searches for a user which has the same email address, same common name, same identifier, or same name and last name. If such a user is found, then the function suggests associating it with the entry. If not, the function suggests creating a new user.

Search criteria

Search base	CN=users,DC=stolrmshiedl,dc=corp
Filter	(Objectclass=person)
Depth	Searching: <input checked="" type="radio"/> entire tree under the base <input type="radio"/> one level under the base <input type="radio"/> base only

Confirm operation: Search

Caution, this operation may take several minutes.

Créer des utilisateurs via LDAP (suite)

L'interface du SDAM vous montre le premier utilisateur trouvé dans l'annuaire AD et vous permet de décider de créer le même utilisateur dans le SDAM.

Stormshield Data Security Authority Manager

RootCA Main administrator 192.168.69.3:389 Close session

Home > Users management > Users > LDAP Synchronization > Users creation > Creation

Confirm user creation

Report of previous operation

User was not created: **User creation canceled.**
No user was created from entry CN=krbtgt,CN=Users,DC=demo,DC=lab.

Do you wish to create a user from the following LDAP entry?

DN	CN=test1,CN=Users,DC=demo,DC=lab
----	----------------------------------

User

Identifier	test1
Description	

User identity

Name	
Given name	test1
Common name	test1
Email address	test1@stormshield.com

Publication

LDAP publication	<input checked="" type="checkbox"/> Publish generated certificate in the LDAP directory
Certificates already published on the LDAP server	<input type="radio"/> Keep
	<input type="radio"/> Delete
	<input checked="" type="radio"/> Replace certificates that have the same usages and the same issuer

User account configuration

Use as template Template1

Validation

The following operations will be performed:

- creation of **test1** in the database;
- key generation for **test1**;
- certificate generation for **test1**;
- account creation for **test1** with copy of the template **Template1**.

Do you confirm user creation? Yes All No Cancel

Stormshield Data Authority Manager 9.13.931 - Copyright © 1996-2017 Stormshield



Déployer des comptes d'utilisateur SDS

Diffuser les fichiers

Après avoir créé l'utilisateur, vous pouvez télécharger/envoyer le fichier concernant cet utilisateur afin qu'il puisse l'installer sur son poste de travail.

Dans le menu **Accueil**, cliquez sur **Gestion des utilisateurs** → **Utilisateurs** → sélectionnez l'utilisateur (dans notre exemple, « test1 ») → puis **Gestion de l'utilisateur** → **Diffuser le compte**.

Stormshield Data Security Authority Manager

RootCA Main administrator Close session

Home > Users management > Users

Main menu Special users Users creation Users management Certificates management

LDAP

Users list

The database contains 3 users of which 2 are special

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Search criteria																									
Users 1 - 3 of 3 found													3 selected users												
Policy Signatory													<input checked="" type="checkbox"/>												
Recovery Account													<input checked="" type="checkbox"/>												
test1													test1@stormshield.com												
Users 1 - 3 of 3 found																									

Stormshield Data Authority Manager 9.13.931 - Copyright © 1996-2017 Stormshield

Stormshield Data Security Authority Manager

RootCA Main administrator Close session

Home > Users management > Users > test1

Main menu Properties User management Keys and certificates

User

User

- Distribute account
- Associate a smart card
- Administrare database
- Delete

Identifier	test1
Template	Template1

Identity

Name	Test1
Given name	test1
Common name	test1
Organization	Stormshield
Organization unit	StormshieldPOC
City	Milan
State or province	Lombardia
Country	IT
Email address	test1@stormshield.com

Diffuser les fichiers (suite)

Cochez la case **Générer un fichier d'installation (*.usi)**, puis cliquez sur **Diffuser le compte** (vous pouvez télécharger le fichier depuis le serveur SDAM vers C:\SBMData\rootca\Users\test1).

Stormshield Data Security
Authority Manager

RootCA Main administrator Close session

Home > Users management > Users > test1 > Selection of the distribution mode

Main menu

Selection of the distribution mode

Distribution mode

Distribution type

- Full (account file, address book file, lists)
 - Generate setup file (*.usi)
 - Update (*.usx)
 - Include user certificates in order to update his key-holder

Transmission by email

- Send the file by email

Template file (*.sbp):

Subject:

Text:

Confirm operation:

Vous pouvez aussi choisir d'envoyer le fichier par e-mail (facultatif) mais vous devez configurer un serveur d'e-mail sous Accueil → Paramètres → Serveur d'e-mail sortant.



Installer le poste de travail client

Installer le poste de travail client

À cette étape, vous allez créer un fichier d'installation personnalisé. Dans le menu **Accueil**, cliquez sur **Personnalisation de l'installation**.

Ici, nous utilisons uniquement des comptes protégés par des mots de passe avec deux clés. Par conséquent, nous allons interdire la création de comptes locaux autres que ceux-là.

Stormshield Data Security Authority Manager

RootCA Main administrator Close session Home

Main menu

Home

- Users management
- Certification authority
- Administrators
- Settings
- External certificates
- Setup customization**

Stormshield Data Authority Manager 9.13.931 - Copyright © 1996-2017 Stormshield

Stormshield Data Security Authority Manager

RootCA Main administrator Close session Home > Setup customization

Main menu Operations

Customize Stormshield Data Security Suite setup

Settings for all types of accounts

- General settings**

"Password" accounts settings

- General settings
- Account creation with a single key
- Account creation with two keys
- Key renewal

"Card or USB key" accounts settings

- General settings
- Account creation with a single key
- Account creation with two keys
- Key renewal

Stormshield Data Authority Manager 9.13.931 - Copyright © 1996-2017 Stormshield

Configurer l'installation

Autorisez uniquement l'utilisation du mode mot de passe, pas celui du mode carte.

The screenshot shows the 'Stormshield Data Security Authority Manager' web interface. The top navigation bar includes the product name, user information (RootCA, Main administrator), and a 'Close session' link. Below the navigation bar is a 'Main menu' button. The main content area is titled 'Stormshield Data Security Suite: General settings' and contains a 'User connection' section. This section is a table with various settings:

Setting	Description
Authorize a connection	<input checked="" type="checkbox"/> In password mode <input type="checkbox"/> In card mode
Shutting down Windows	<input type="checkbox"/> Refused if a user is connected
Main folder	If you wish that Stormshield Data Security creates and searches for users accounts in a specific main folder (on a server for example), please indicate the full path to this folder: <input type="text"/> ...
Backup folder	You may define a backup folder on which Stormshield Data Security will look for the user account in case it cannot be found in the main folder: <input type="text"/> ...
Backup folder	In the Stormshield Data Security connection window: <input type="checkbox"/> Do not display the pathname of the second users accounts search folder ?
Contextual menu	<input type="checkbox"/> Do not display the contextual menu ?
"Browse" item	In the connection window, a right click on the "Identifier" field displays a menu in which the "Browse" item allows to directly select the user account: <input type="checkbox"/> Do not display the "Browse" item
Command line utility	In the SBCMD.EXE command line utility: <input type="checkbox"/> Ignore a secret code supplied on the command line. User must enter his/her secret code.

Configurer l'installation (suite)

Sélectionnez l'option
Interdire la création
de comptes



Stormshield Data Security
Authority Manager

RootCA Main administrator Close session
Home > Setup customization > General settings

Main menu

Account creation

 New accounts	<input checked="" type="checkbox"/> Prohibit account creation
Self-certified certificates	Validity length of self-certified certificates generated by Stormshield Data Security: <ul style="list-style-type: none">when creating an account: <input type="text"/> yearswhen renewing a key: <input type="text" value="20"/> years
Certificate request by email	When the user makes a certificate request, he/she may send it by email. Enter the authority's email address , and optionally the body of the message created by Stormshield Data Security, according to the 'mailto:' link syntax: <email>[?subject=<objet>[&body=<text>]] <input type="text"/>

Address book

 LDAP search	In an LDAP search launched from the address book: <ul style="list-style-type: none"><input type="checkbox"/> Do not append '*' to the search criteria<input type="checkbox"/> Do not include the search filter "usercertificate;binary"
---	--

Configurer l'installation (suite)

Accédez à la fin de la page de configuration **Stormshield Data Security Suite : Paramètres généraux**. Cochez la case **Ne pas afficher la clé de licence**, puis cliquez sur **Appliquer les modifications**.

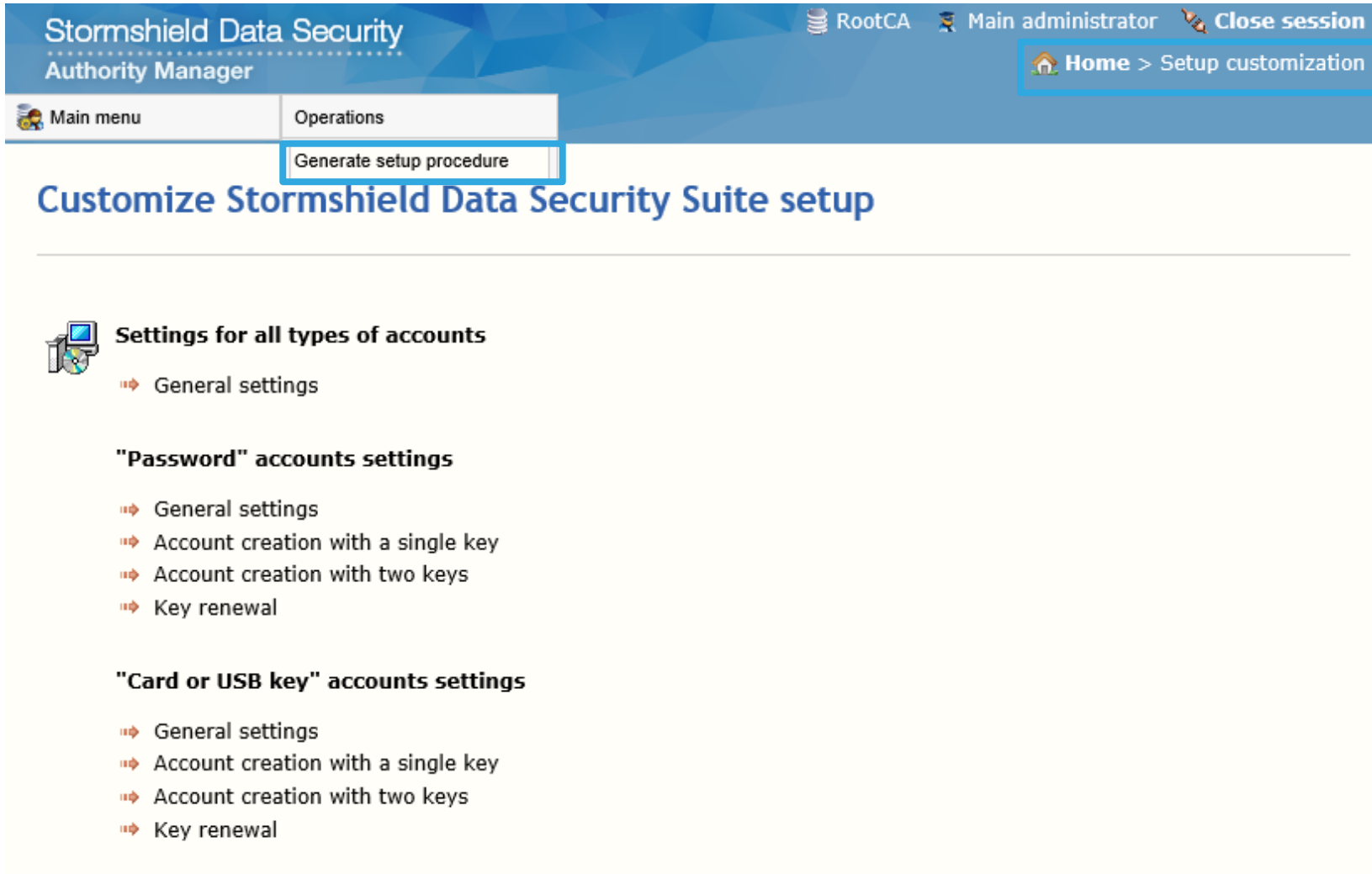
The screenshot displays the configuration interface for the Stormshield Data Security Suite. It is divided into three main sections:

- Revocation controller:** Contains settings for CRL download, with input fields for 'Maximum time limit for a CRL download in LDAP' and 'Maximum time limit for a CRL download via HTTP', both set to 120 seconds.
- Miscellaneous:** Contains the 'License key' section, where the checkbox 'Do not show license key' is checked. This section is highlighted with a blue border.
- Adding settings to the SBox.ini file:** Contains a 'Select a file:' field with a 'Browse...' button and a warning icon with the text: 'Reminder about the merge: the values of the settings present in this file replace those already present in the SBox.ini file, as well as the values configured in the pages of "Setup customization".'

At the bottom right, the 'Confirm operation:' label is followed by the 'Apply modifications' button, which is also highlighted with a blue border.

Générer le fichier d'installation

Vous allez maintenant créer le fichier *.msi* personnalisé en sélectionnant **Opération** → **Générer la procédure d'installation**.



The screenshot shows the Stormshield Data Security Authority Manager interface. The top navigation bar includes the product name, user role (Main administrator), and session management options. The 'Operations' menu is expanded, with 'Generate setup procedure' highlighted. The main content area displays the 'Customize Stormshield Data Security Suite setup' page, which is organized into sections for account settings: 'Settings for all types of accounts', 'Password accounts settings', and 'Card or USB key accounts settings'. Each section lists specific configuration options like 'General settings', 'Account creation with a single key', 'Account creation with two keys', and 'Key renewal'.

Stormshield Data Security
Authority Manager

RootCA Main administrator Close session

Home > Setup customization

Main menu Operations

Generate setup procedure

Customize Stormshield Data Security Suite setup

Settings for all types of accounts

- General settings

"Password" accounts settings

- General settings
- Account creation with a single key
- Account creation with two keys
- Key renewal

"Card or USB key" accounts settings

- General settings
- Account creation with a single key
- Account creation with two keys
- Key renewal

Générer le fichier d'installation (suite)

Depuis MyStormshield, téléchargez le fichier `.msi` (par exemple, `Stormshield_Data_Security_Suite_9.1.30931_ENU_Release_x64.msi`). Copiez-le ensuite sur le serveur Windows où vous avez installé le SDAM (dans notre exemple, sous `C:\SBMData\rootca`).

Generating setup procedure

Source and target

Setup procedure: Original (*.msi) setup procedure:
C:\SBMData\rootca\Stormshield_Data_Security_Suite_9.1.30931_ENU_Release_x64.msi

Target folder: Target folder in which the setup procedure will be generated:
C:\SBMData\rootca\MSITarget

Components installed

License key: Enter the license key which will be pre-filled in the setup procedure:
DSDFSDFD - EEFQDFGF Checking...

Components: Select the Stormshield Data Security Suite components:

- Stormshield Data Mail - Microsoft® **Outlook** edition
- Stormshield Data Mail - Lotus® **Notes** edition
- Stormshield Data **File**
- Stormshield Data - **Connector**
- Stormshield Data **Shredder**
- Stormshield Data **Sign**
- Stormshield Data **Disk**
- Stormshield Data **Team**
- Stormshield Data **Card** extension

Setup folder: Default setup folder on user's computer:
[Empty text box]

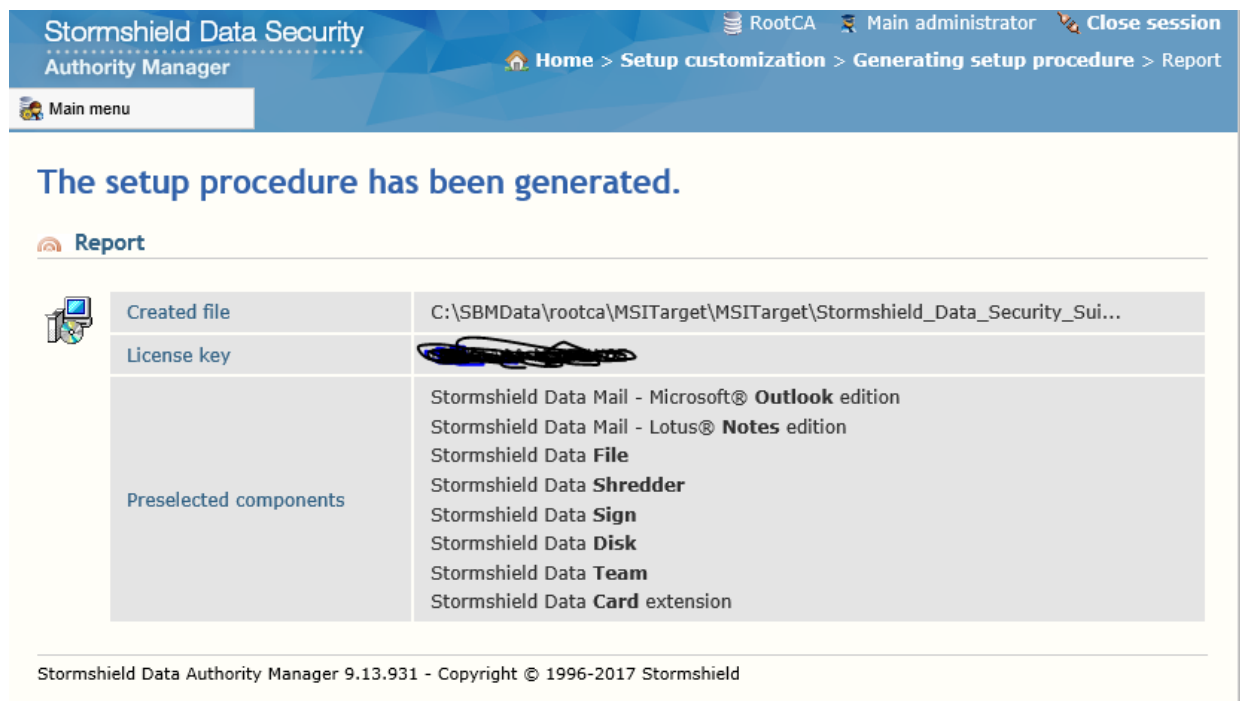
Generating setup procedure

The customized setup procedure of Stormshield Data Security Suite will be generated in the folder `C:\SBMData\rootca\MSITarget`.
Caution, this operation may take several minutes.

Confirm operation:

Télécharger le fichier .msi

Après la génération, vous obtenez cette page à partir du SDAM et vous pouvez alors télécharger le fichier .msi personnalisé, depuis le dossier C:\SBMData\rootca\MSITarget\MSITarget.



Stormshield Data Security Authority Manager


RootCA Main administrator Close session

Home > Setup customization > Generating setup procedure > Report

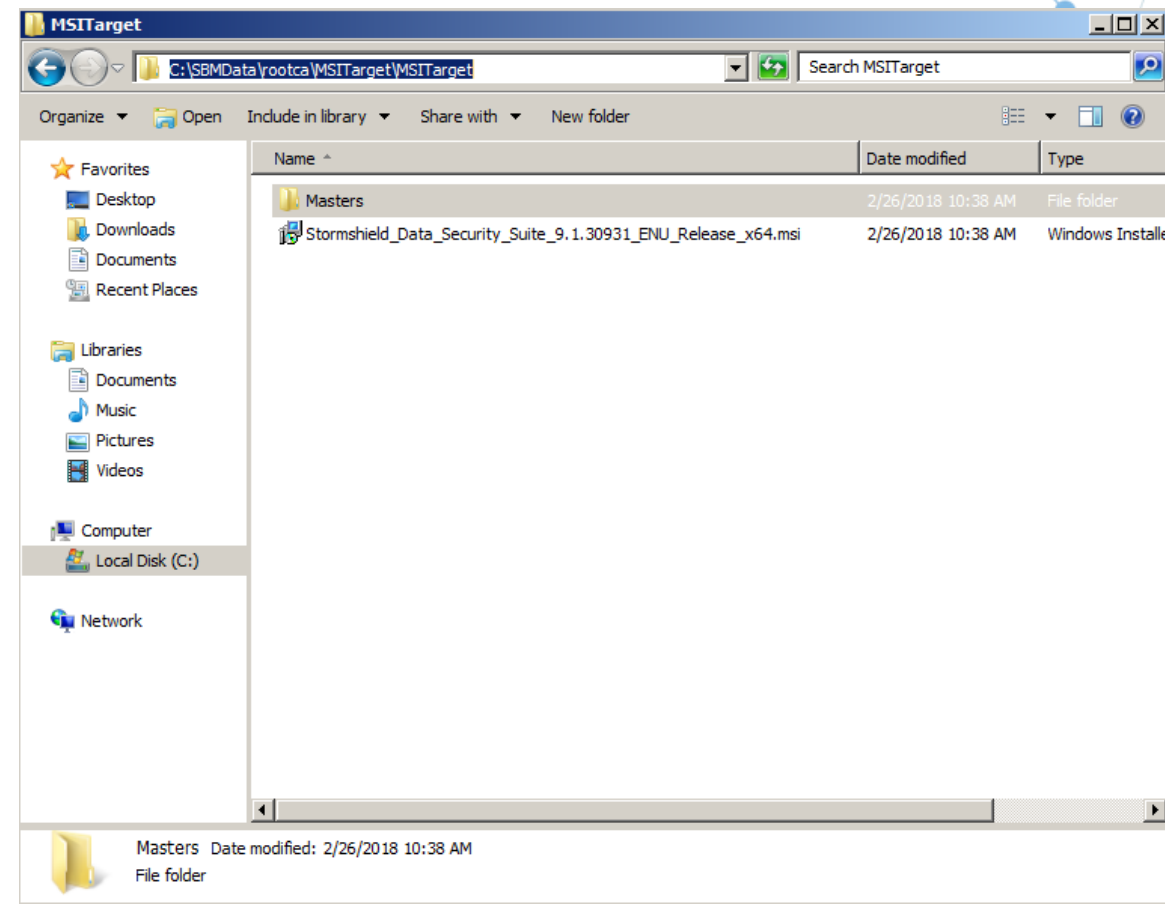
Main menu

The setup procedure has been generated.

Report

Created file	C:\SBMData\rootca\MSITarget\MSITarget\Stormshield_Data_Security_Sui...
License key	
Preselected components	Stormshield Data Mail - Microsoft® Outlook edition Stormshield Data Mail - Lotus® Notes edition Stormshield Data File Stormshield Data Shredder Stormshield Data Sign Stormshield Data Disk Stormshield Data Team Stormshield Data Card extension

Stormshield Data Authority Manager 9.13.931 - Copyright © 1996-2017 Stormshield

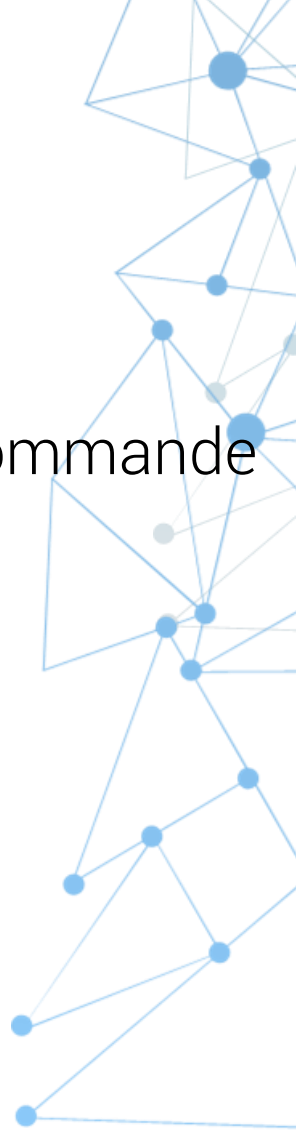


Vous pouvez renommer le fichier d'installation personnalisé, si vous le souhaitez. Par exemple, Custom_SDS_file.msi.

Installer le fichier *.msi*

Pour installer le fichier *.msi* sur un poste de travail, vous pouvez entrer cette commande dans une invite de commande avec droits d'administration.

Msiexec /I "C:\Custom_SDS_file.msi" /qb+

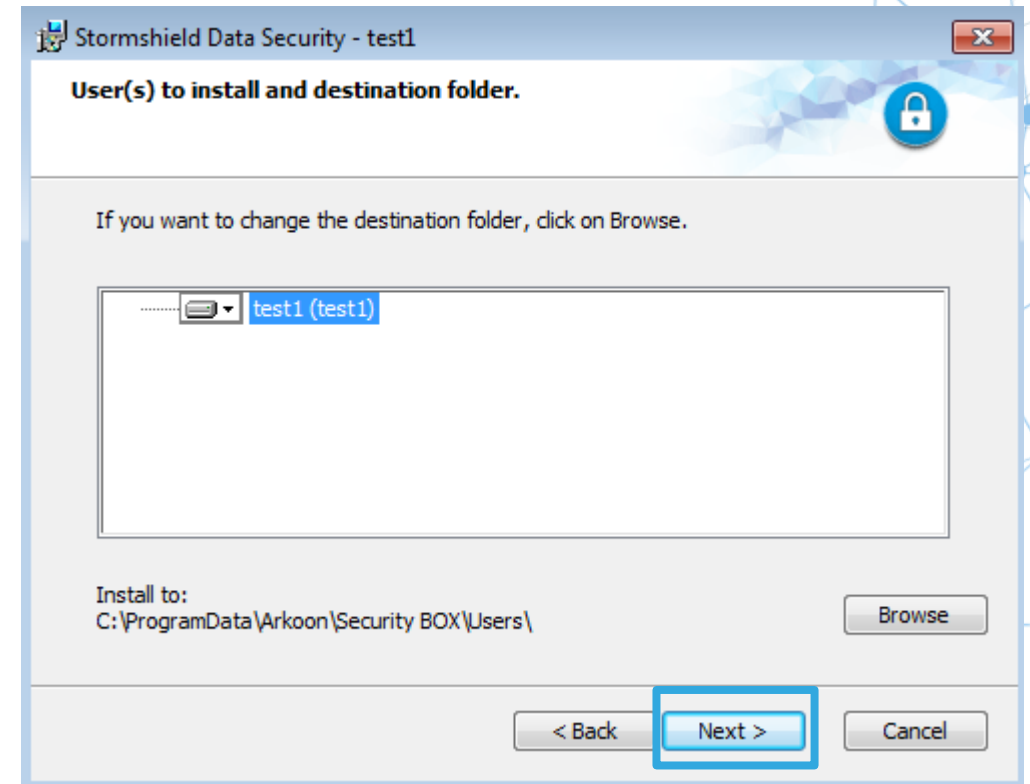
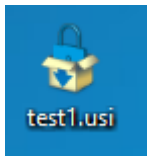




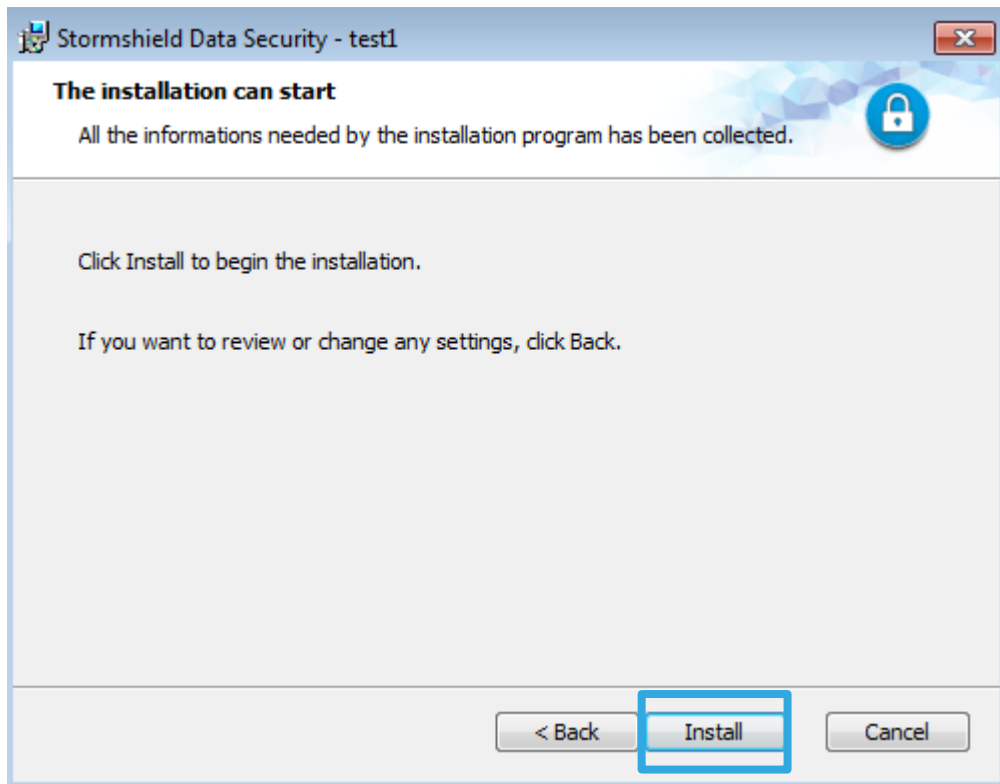
Installer le compte SDS

Installer le compte SDS

Récupérez le fichier utilisateur à partir du serveur, dans le dossier suivant :
C:\SBMData\rootca\Users\test1



Installer le compte SDS (suite)



An abstract geometric diagram on the left side of the slide. It consists of several light blue circular nodes connected by thin white lines. The nodes are arranged in a way that suggests a network or a series of interconnected points. One node is at the top left, another is below it, and a third is further down and to the left. Lines connect these nodes to each other and to other nodes that are partially visible on the left edge of the frame.

Connexion initiale

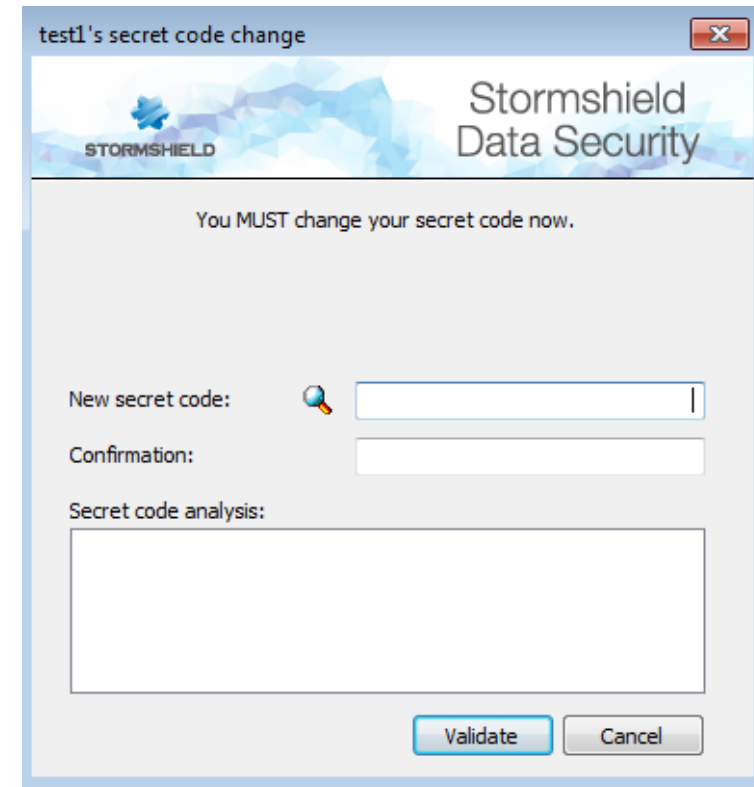
Connexion initiale

L'icône utilisateur affichée sur la gauche indique que le compte existe sur le poste de travail. Entrez le mot de passe initial de l'utilisateur. Après sa première connexion, le système demande à l'utilisateur de modifier ce mot de passe initial.



Pour obtenir le mot de passe initial, vous devez accéder au SDAM, rechercher l'utilisateur « test1 » et cliquer sur

Propriétés → **Mot de passe** et consulter le champ **Mot de passe initial**.



Définissez le nouveau mot de passe.



Cas d'usage – Démonstration

Module Mail

- Envoi d'un e-mail chiffré en interne
- Réception d'un e-mail chiffré en interne
- Comment envoyer un e-mail chiffré hors du réseau
 - `%USERNAME_CLIENT1` envoie un e-mail signé à `%USERNAME_CLIENT2`.
 - `%USERNAME_CLIENT2` reçoit un e-mail signé et importe les certificats dans le répertoire.
 - `%USERNAME_CLIENT2` envoie un e-mail chiffré à `%USERNAME_CLIENT1`.



Module Disk

- Création manuelle d'un volume disque sur l'ordinateur `%HOSTNAME_CLIENT1` avec montage automatique.
- Création manuelle d'un volume disque par `%USERNAME_CLIENT1` sur un lecteur USB, partagé avec `%USERNAME_CLIENT2`, avec option de modification manuelle.



Module Team

- Création d'une règle locale pour vous-même dans un répertoire confidentiel sur le poste de travail de **%HOSTNAME_CLIENT1**.
- **Création par %USERNAME_CLIENT1** d'une règle (dans un répertoire confidentiel sur le serveur de fichiers), partagé avec **%USERNAME_CLIENT2** depuis le poste de travail **%HOSTNAME_CLIENT1**.



Module File

- Chiffrement par **%USERNAME_CLIENT2** d'un document avec un mot de passe pour une utilisation en externe.
- Partage du document protégé par mot de passe avec une personne qui ne possède pas la solution SDS.
- Accès au site Web Mystormshield.eu pour télécharger le logiciel SDS SmartFILE Reader.
- https://www.stormshield.com/wpcontent/uploads/2016/09/SmartFile_Reader.zip



An abstract geometric diagram on the left side of the page. It consists of several light blue circular nodes connected by thin white lines. The nodes are arranged in a way that suggests a network or a series of interconnected points. One node is at the top left, another is below it, and a third is further down and to the left. Lines connect these nodes to each other and to other points that are partially visible on the left edge of the frame.

Support

Contacts

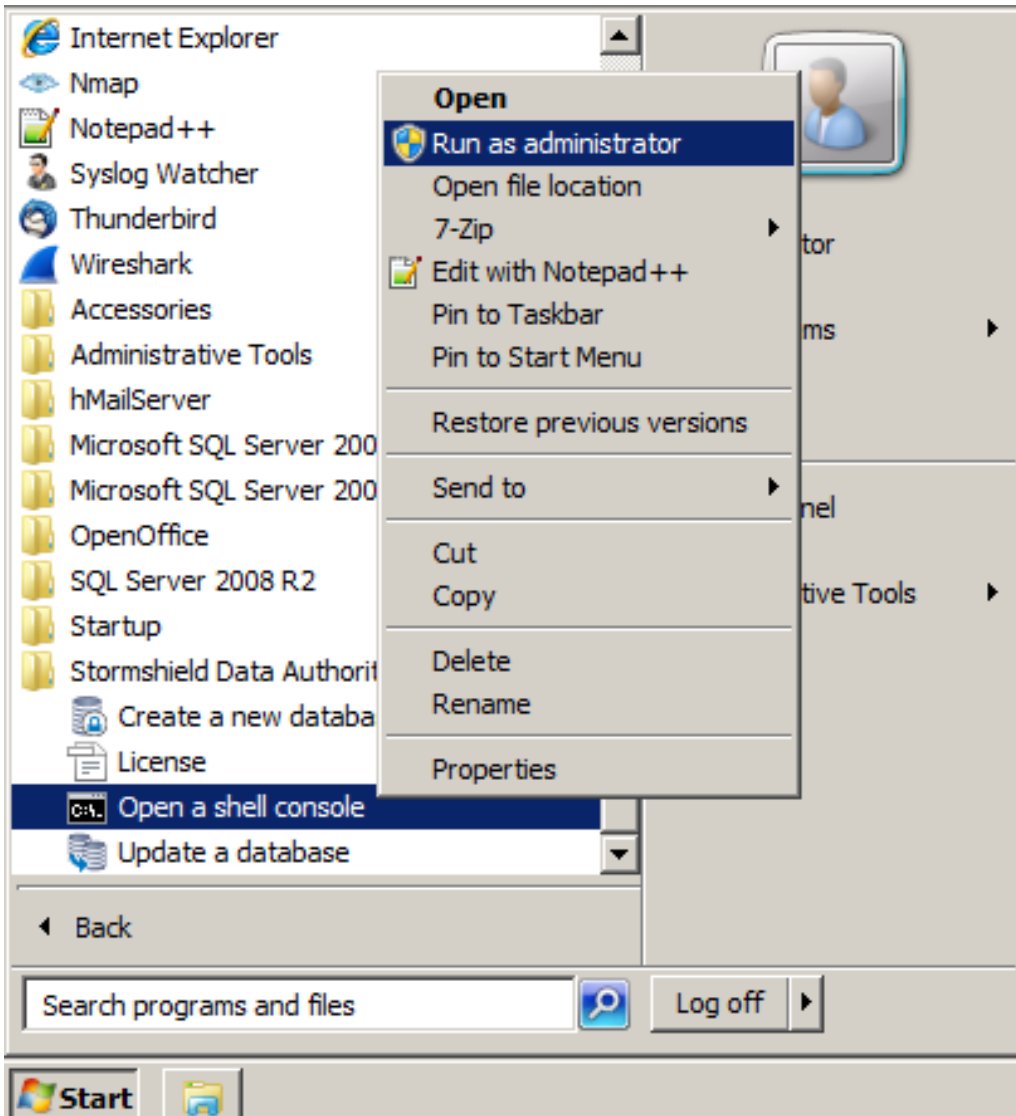
- Pour obtenir de l'aide concernant la validation de principe (POC) en cours :
 - Si vous êtes un partenaire disposant d'une licence d'ÉVALUATION :
 - Vous pouvez contacter directement votre ingénieur avant-vente Stormshield local.
 - Si vous êtes un partenaire disposant d'une licence NFR (Revente interdite) :
 - Vous pouvez contacter directement le support Stormshield.
 - Si vous êtes un client (détenteur d'une solution avec licence permanente et contrat de maintenance valide) :
 - Vous avez déjà accès au service de support de votre intégrateur.
 - Vous avez déjà accès au support Stormshield.





Démarrer la base de données du serveur SDAM

Comment démarrer la base de données si j'arrête le serveur SDAM ?



- Ouvrez une ligne de commande avec droits d'administrateur, exécutez la commande suivante pour démarrer la BdD : *C:\Program Files (x86)\Arkoon\Security BOX Authority Manager\Tools> SBMSTART.exe /o*
- Exécutez *SBMSTART.exe /?* pour connaître toutes les options de cette commande.



STORMSHIELD

COLLABORATIVE SECURITY

Network Security

Endpoint Security

Data Security