STORMSHIELD

Network Endpoint Data

QUICK START GUIDE
SDS Enterprise 9.1.X

STORMSHIELD

Stormshield Data Security Enterprise

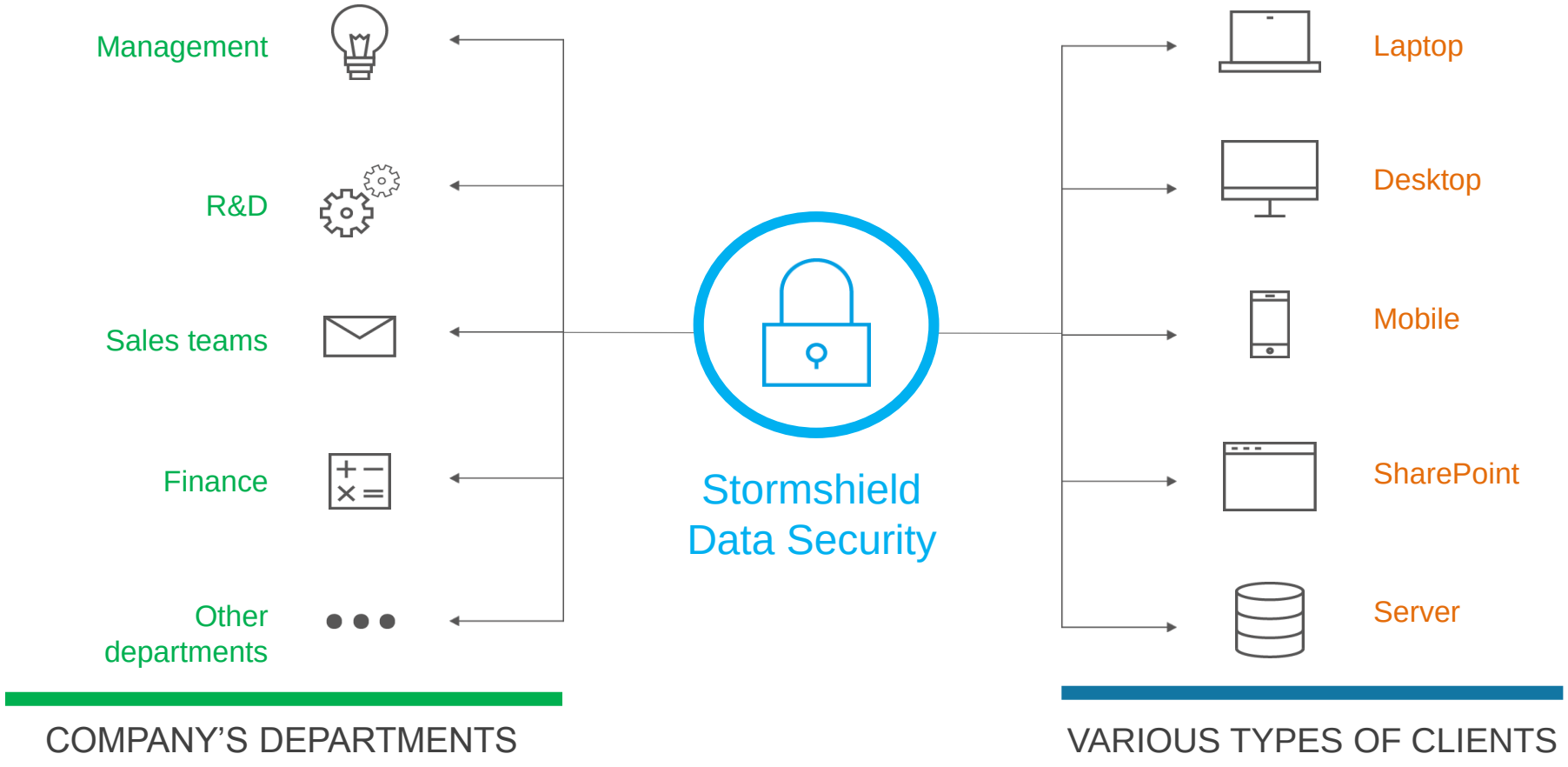


Table of contents

Introduction

Glossary

- CRL: Certificate Revocation List
- EXE: Non-Custom SDS Agent Installation File Format
- GPO: Group Policy Object
- MSI: Customizable SDS Agent Installation File Format
- PKI: Public Key Infrastructure
- SDAM: Stormshield Data Authority Manager
- SDS: Stormshield Data Security
- SDSe: SDS Enterprise version
- SGBD: Database Management System
- SMTP: Simple Mail Transfer Protocol
- USI: SDSe account installation file format
- USX: SDSe account update file format

Variable list

- Find and replace the following variables with your own values to automatically customize the configuration described in this 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*

Objective of this document

- The purpose of this document is to guide end users or partners in understanding the installation, configuration and use of SDSe.

- This is the quick start guide to establish a POC (Proof of Concept), and it gets to the basics to help you quickly understand how SDSe runs.
- It does not deal with all use cases or all of the product's options, but contains sufficient information for you to install SDSe without having received certification training.

- Time to complete the POC:
- 1 day for installation
- 1 day to test all features

POC details

- The SDSe POC consists of several steps in order to set up the server:
  - Configuring a Microsoft IIS server
  - Installing a PKI (contained in the SDAM)
  - Installing an administration workstation connecting to the SDAM (Windows 10 PC)
  - Installing a user workstation (Windows 10 PC)

Technical requirements

Stormshield Data Authority Manager

- The SDAM can be installed on:
  - Windows 7 (32 bits and 64 bits)
  - Windows Server 2008 R2 (64 bits)
  - Windows Server 2012 R2 (64 bits)

- It needs:
  - A Microsoft IIS Web server in version 7.0 or higher

- This server can be virtualized
- An account with administrator privileges is required

Stormshield Data Security Suite

- An account with administrator privileges is required

- SDS 9.1.X can be installed on:
  - Windows 7 SP1 (32 or 64 bits)
  - Windows 8.1 (32 or 64 bits)
  - Windows 10 (32 or 64 bits)

- The Stormshield Data Mail module is compatible with Outlook (2010 and upwards)

Outlook

- For Outlook 2010:
  - Office 2010 Service Pack 2
  - KB2597137 (http://support.microsoft.com/kb/2597137)
  - KB2881055 (http://support.microsoft.com/kb/2881055)

- For Outlook 2013:
  - Office 2013 Service Pack 1
  - KB2878323 (http://support.microsoft.com/kb/2878323)
  - KB2881040 (http://support.microsoft.com/kb/288104)

Outlook 2010

Stormshield Data Security	9.1.3		9.1.4	
Microsoft Office 2010 Service pack **Min**	SP1	SP2	SP1	SP2
Mandatory Microsoft KB	2597137 2881055	2881055	2597137 2881055	2881055
SQL Server Compact **Min**	Edition 4.0		Edition 4.0	
Visual Studio 2010 Tools for Office Runtime **Min**	VSTO Runtime 4.0		VSTO Runtime 4.0	
.NET Framework **Min**	4.5.2		4.5.2	

Outlook 2013

Stormshield Data Security	9.1.3	9.1.4
Microsoft Office 2013 Service pack **Min**	SP1	SP1
Mandatory Microsoft KB	KB2878323 KB2881040	KB2878323 KB2881040
SQL Server Compact **Min**	Edition 4.0	Edition 4.0
Visual Studio 2010 Tools for Office Runtime **Min**	VSTO Runtime 4.0	VSTO Runtime 4.0
.NET Framework **Min**	4.5.2	4.5.2

No prerequisites

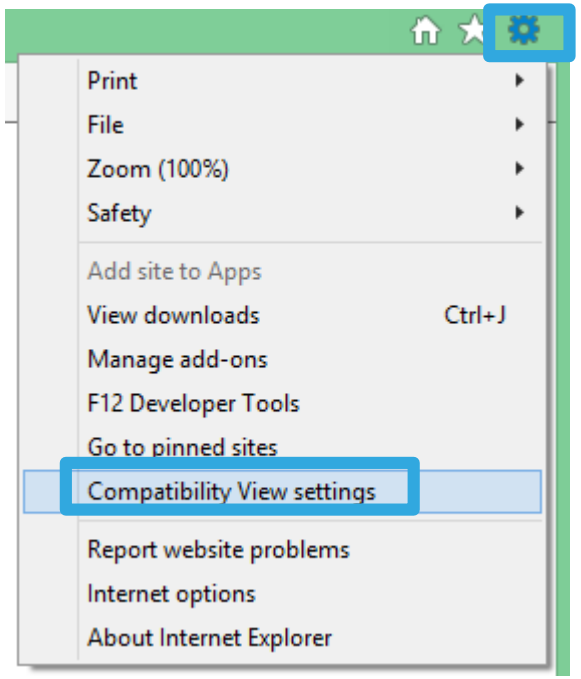
ACTIVE X (mandatory)

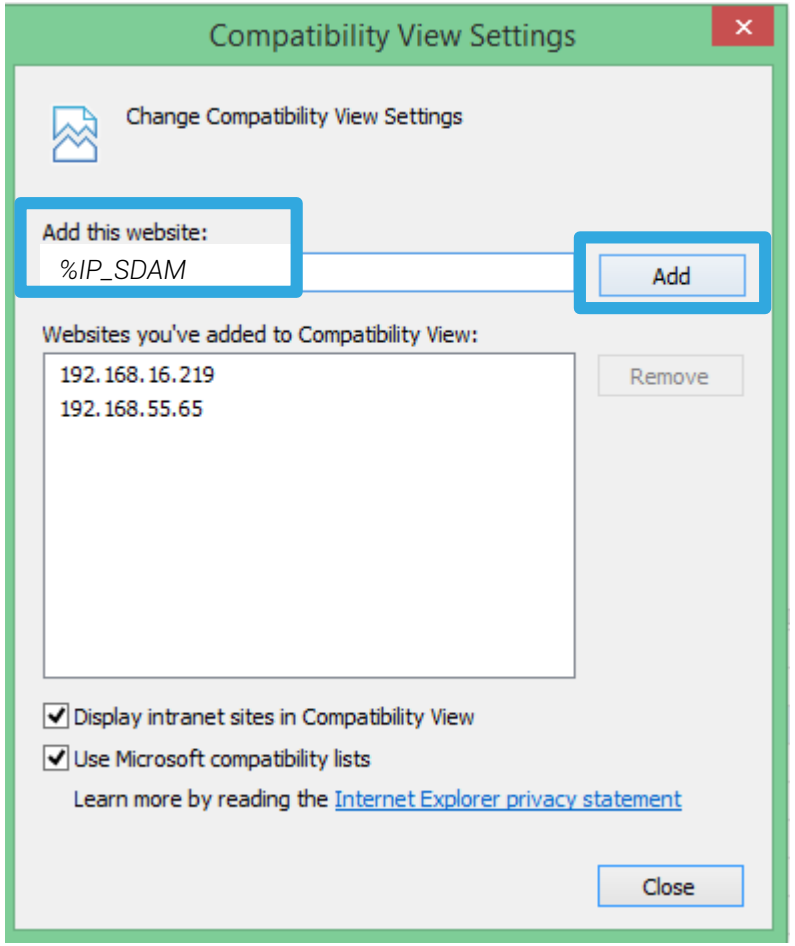
- Only for administration and administrators of the SDAM solution.
- To access the SDAM web interface, the workstation must be able to install an unsigned ActiveX (signed by Stormshield but not Microsoft).
- The SDAM URL must be declared as a trusted site in IE.
- Administrator privileges are required on the computer, and there must be no GPO that restricts the use of Internet Explorer.

INTERNET EXPLORER

On Internet Explorer 11, the URL or IP address of the SDAM server must be defined in the compatibility view settings.

Click on **Settings** → **Compatibility View Settings**





LDAP ACCESS (optional)

- The SDAM must have read / write access to the LDAP server to be able to import users, and export user certificates in the "UserCertificates" attribute.

- SDS accounts must have read-only access to the "UserCertificates" fields to download the certificates of other users (this can be done with user accounts).

SMTP ACCESS (optional)

- The SDAM must be able to access an SMTP server or an SMTP relay to send e-mails to administrators and users (the SDAM only sends e-mails, but does not receive them; you do not need a mailbox for the SDAM).

CRL PUBLICATION

- If you need to exchange secure data with external users, the CRL must be publicly available.

- On a web server, the CRL must be available for free download (for example on http://www.company.com/sdsCRL.crl).

- This is a .crl file (SDS will download it), so no need for a web page.
  Example: http://crl.stormshield.eu/stormcorpdatasec.crl

Architecture of the POC

CONNECTION MATRIX

- For a SDAM located behind a firewall and acting as a PKI:

- Open the HTTP (or HTTPS) connection for an administrator to access the web administration interface

Connection: "Admin Station" to SDAM in HTTP / HTTPS

- Open the SMTP connection so that users can receive *.usi* files (SDS agent account installer) by e-mail

Connection: SDAM to "Mail Server" on SMTP

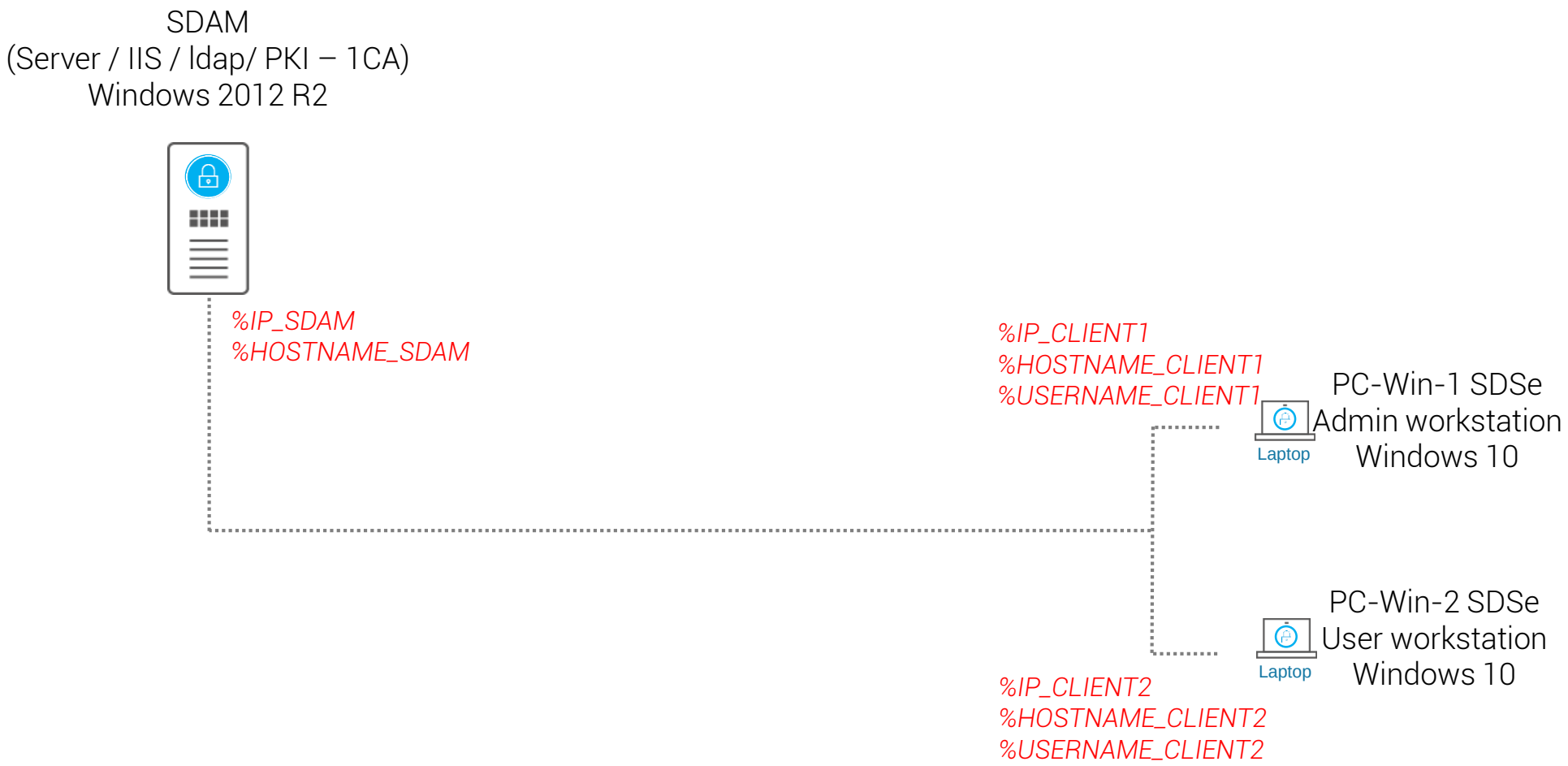
- Open the LDAP connection (or LDAPS) for public certificate delivery

Connection: SDAM to "AD Server" on LDAP/LDAPS

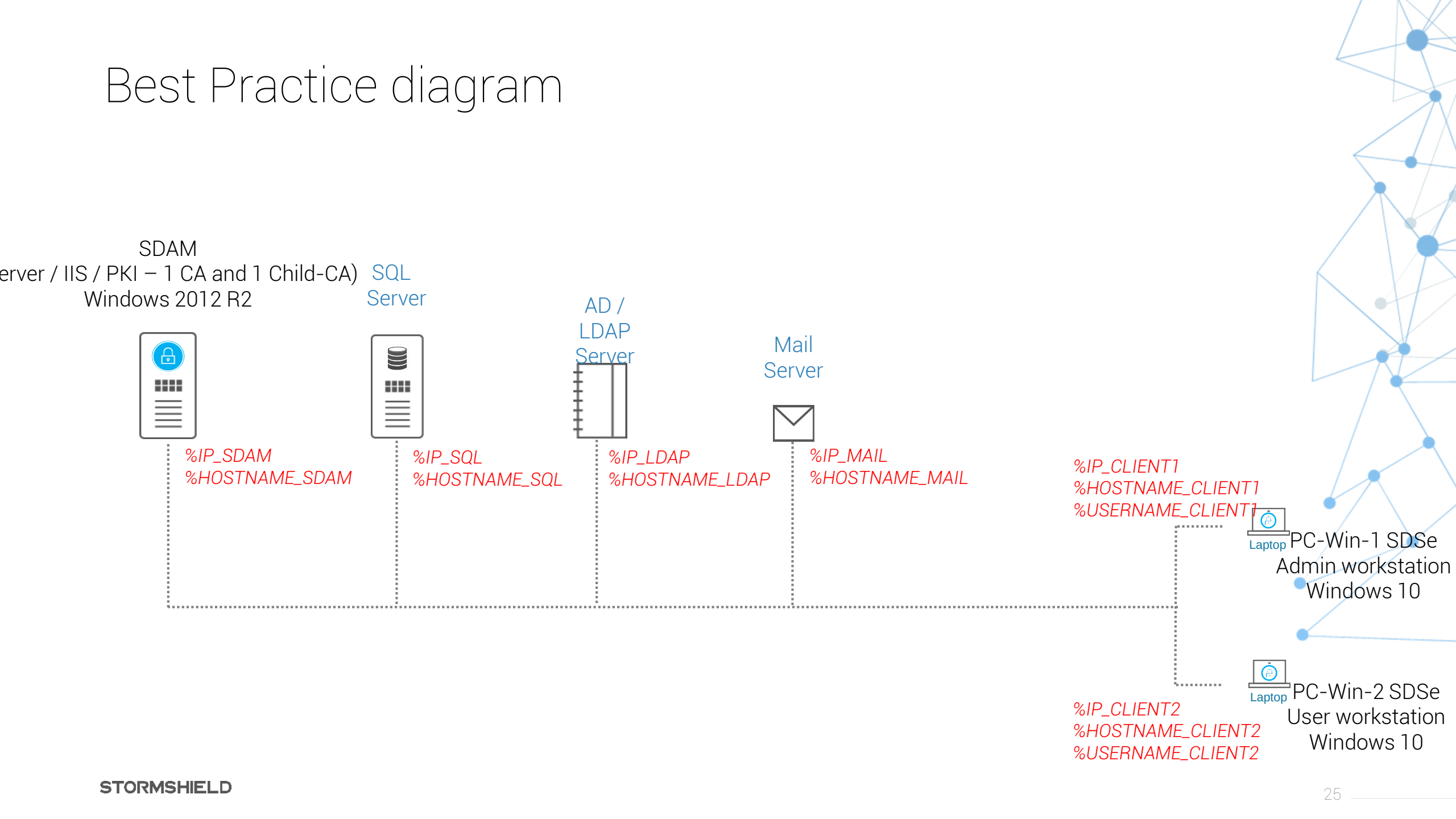
- Set up a file transfer to forward *.usx* (SDS agent update file) or available web directory

- There are three ways to download the CRL:
  - HTTP/HTTPS
  - LDAP/LDAPS
  - File transfer

POC DIAGRAM


SDAM
(Server / IIS / ldap/ PKI – 1CA)
Windows 2012 R2
%IP_SDAM
%HOSTNAME_SDAM
%IP_CLIENT1
%HOSTNAME_CLIENT1
%USERNAME_CLIENT1
Laptop
PC-Win-1 SDSe
Admin workstation
Windows 10
Laptop
PC-Win-2 SDSe
User workstation
Windows 10
%IP_CLIENT2
%HOSTNAME_CLIENT2
%USERNAME_CLIENT2

Best Practice diagram

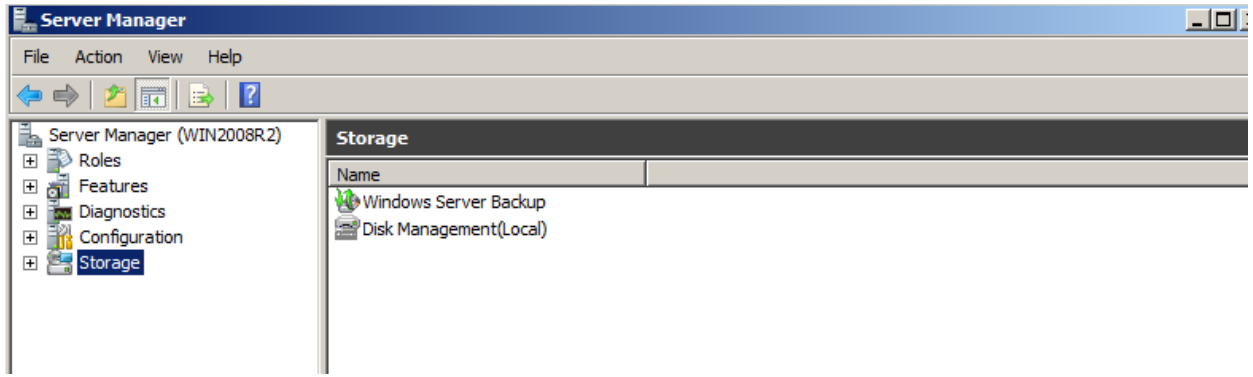


Installing the IIS server

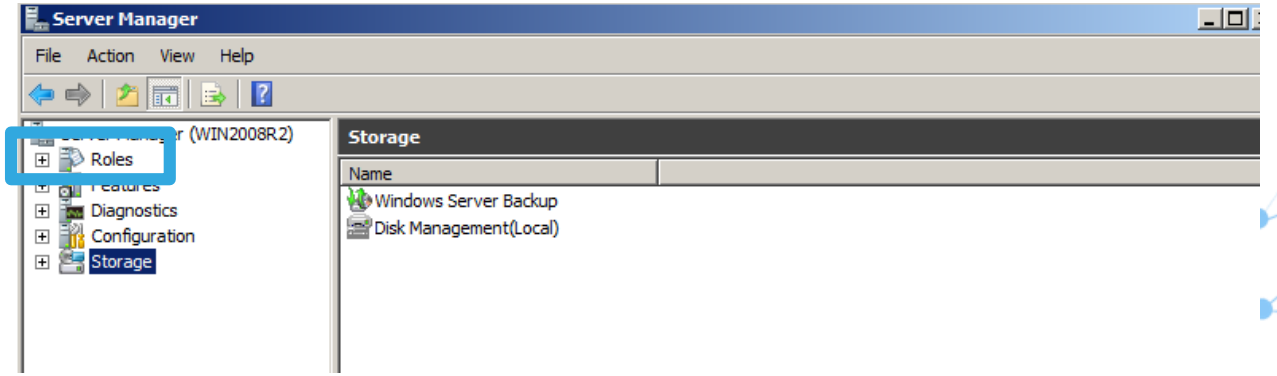
Installing the IIS server

An IIS server must be installed and configured in order for the SDAM management console to run successfully (the screenshot below was taken on Windows server 2008 R2)

Click on **Start → Administrative Tools → Server Manager**

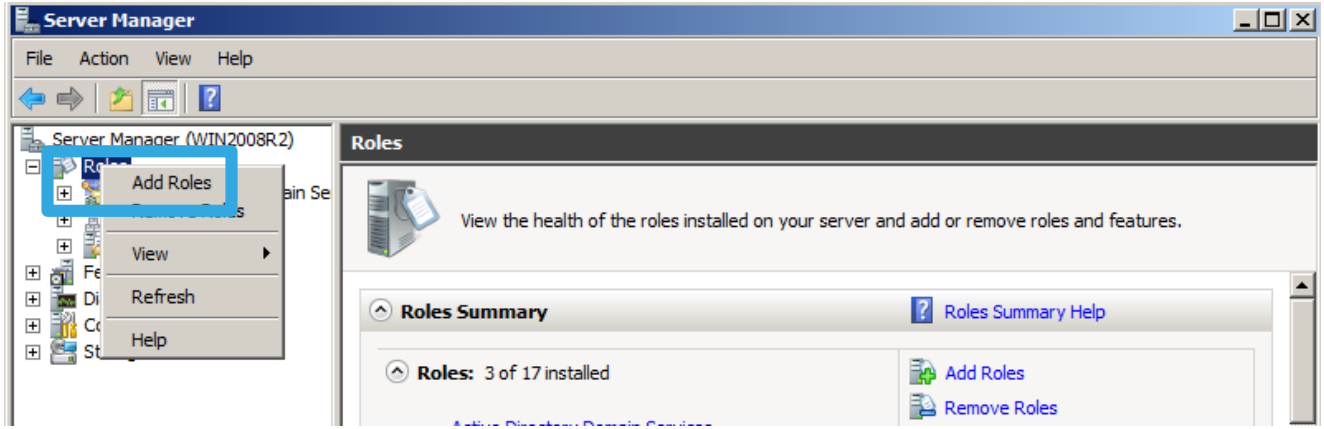


Click on **Roles**

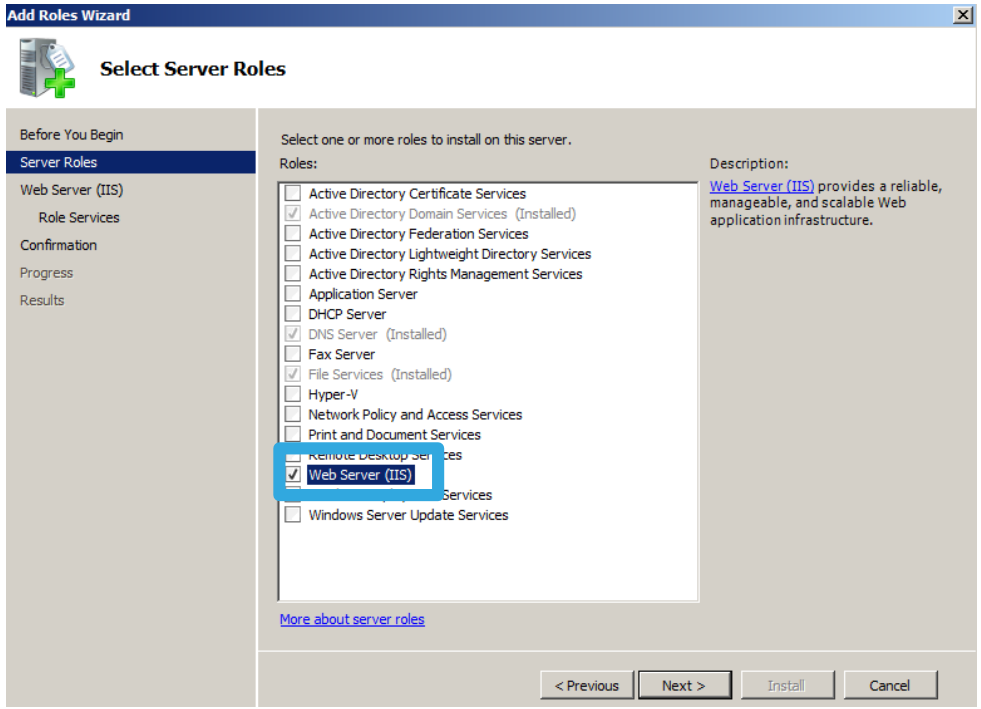


Installing the IIS server (continued)

Right click on **Roles** and select **Add Roles**



Select **Web Server(IIS)** and click on **Next**



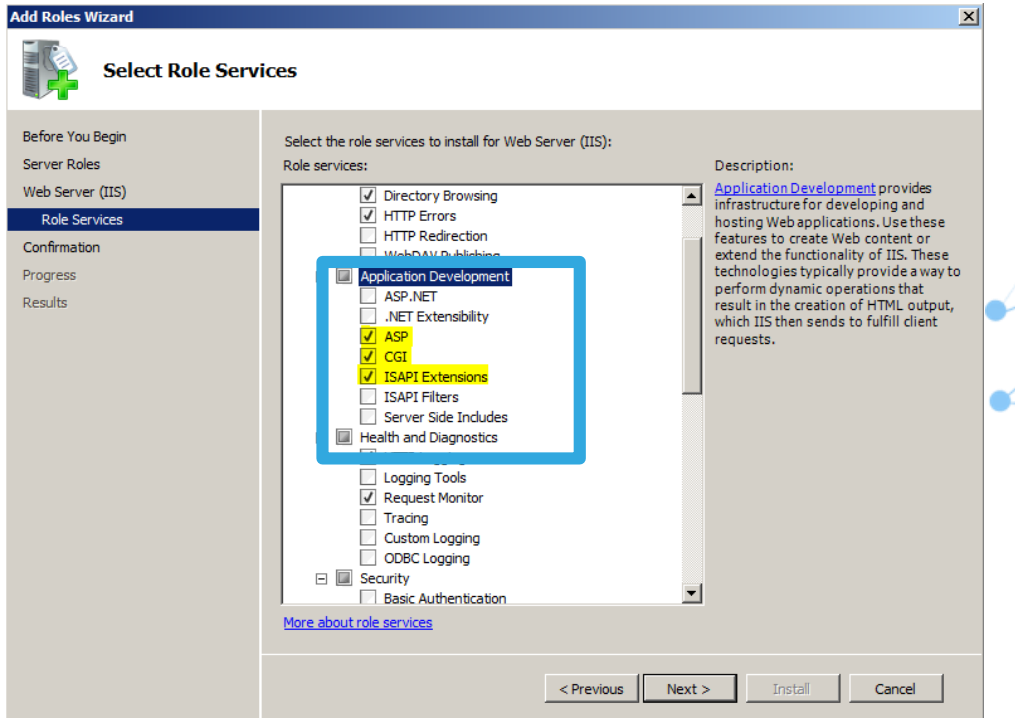
Installing the IIS server (continued)

Click on **Next** again

At the **Role Services** step, leave all the options checked by default and add the following:

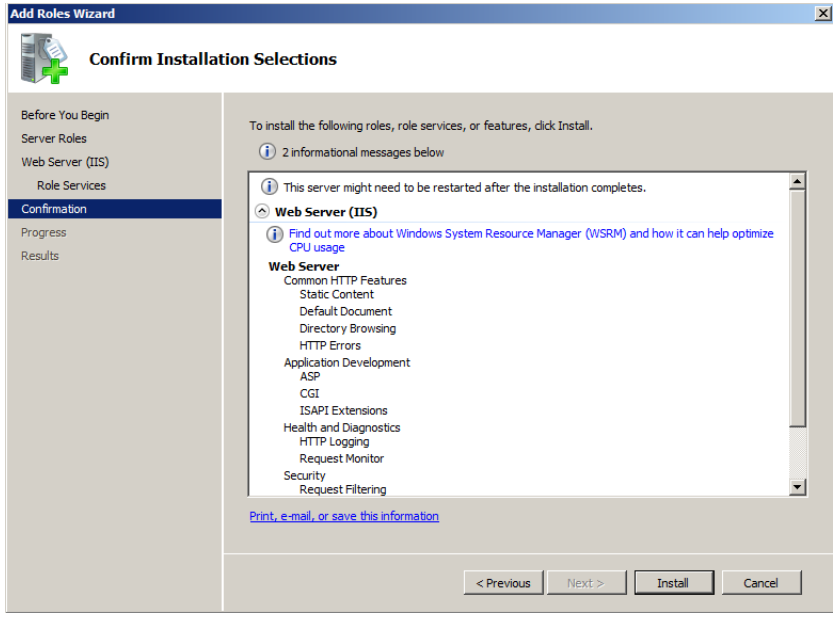
1. **Application Development:** select **ASP, CGI** and **ISAPI Extension**
2. **Common HTTP features:** be sure that **Static Content** is selected (if not, select it)
3. **Security:** be sure that **Request Filtering** is selected (if not, select it)

After you have checked that all options have been correctly selected, click on **Next**.

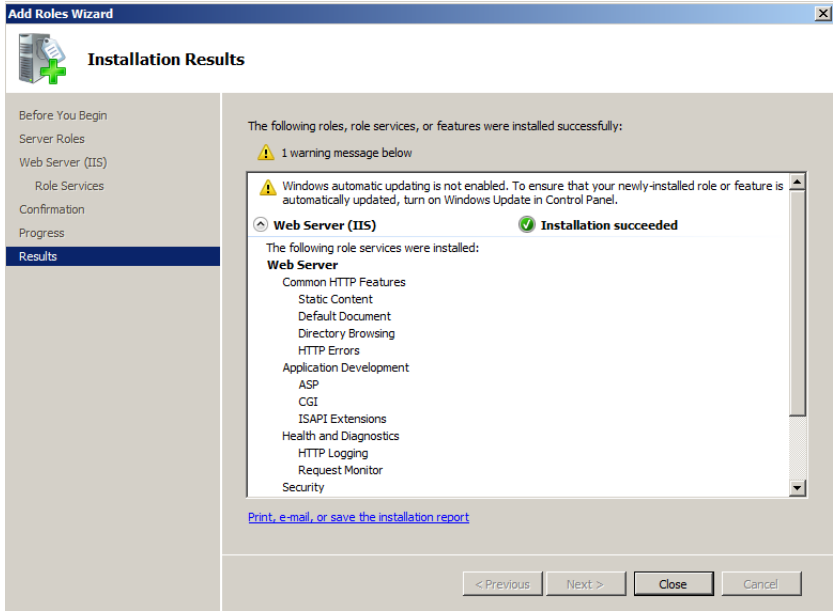


Installing the IIS server (continued)

Click on **Install** to start the installation of IIS



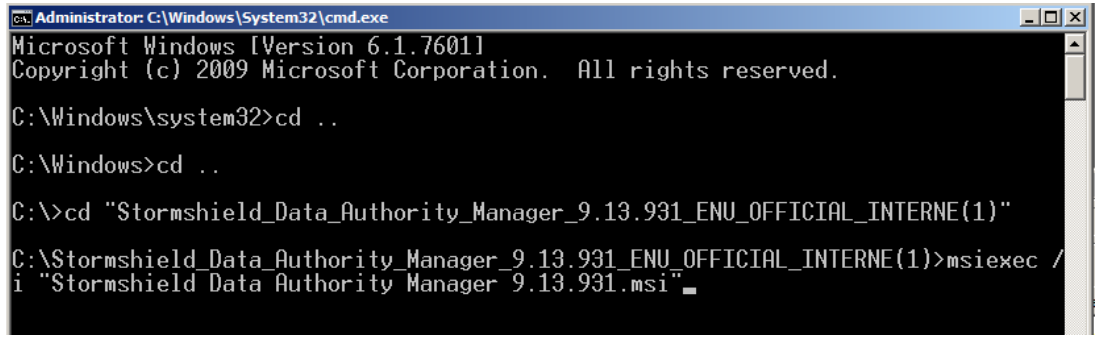
Check that you get an **Installation succeeded** message, then click on **Close**



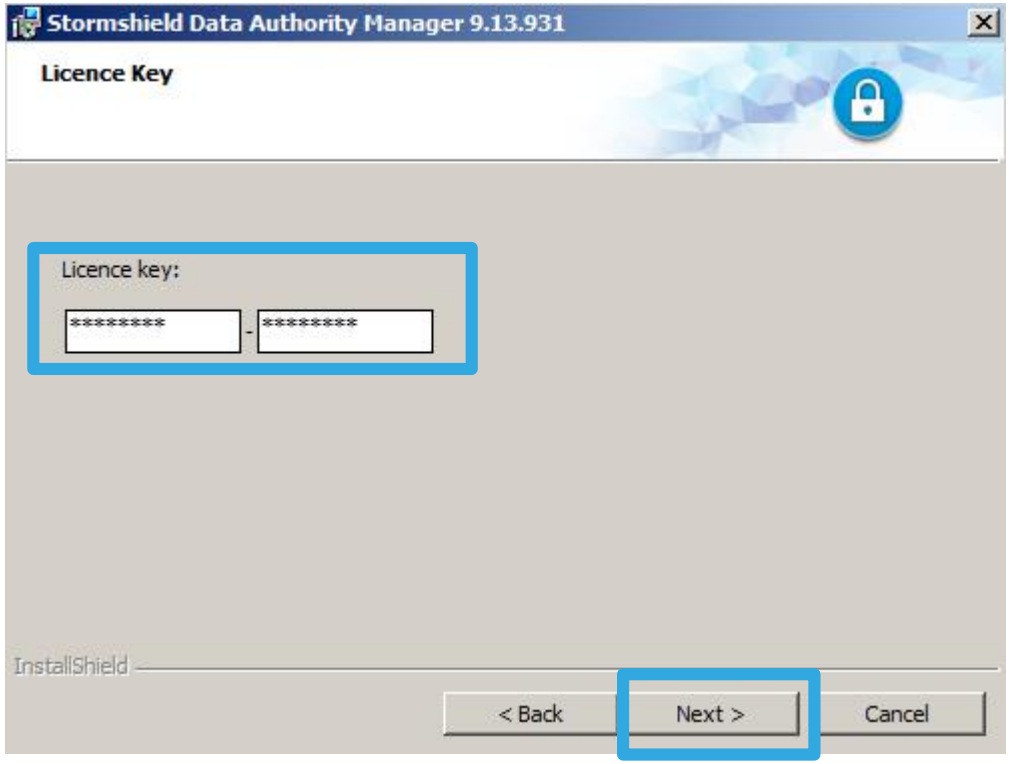
Installing the SDAM server

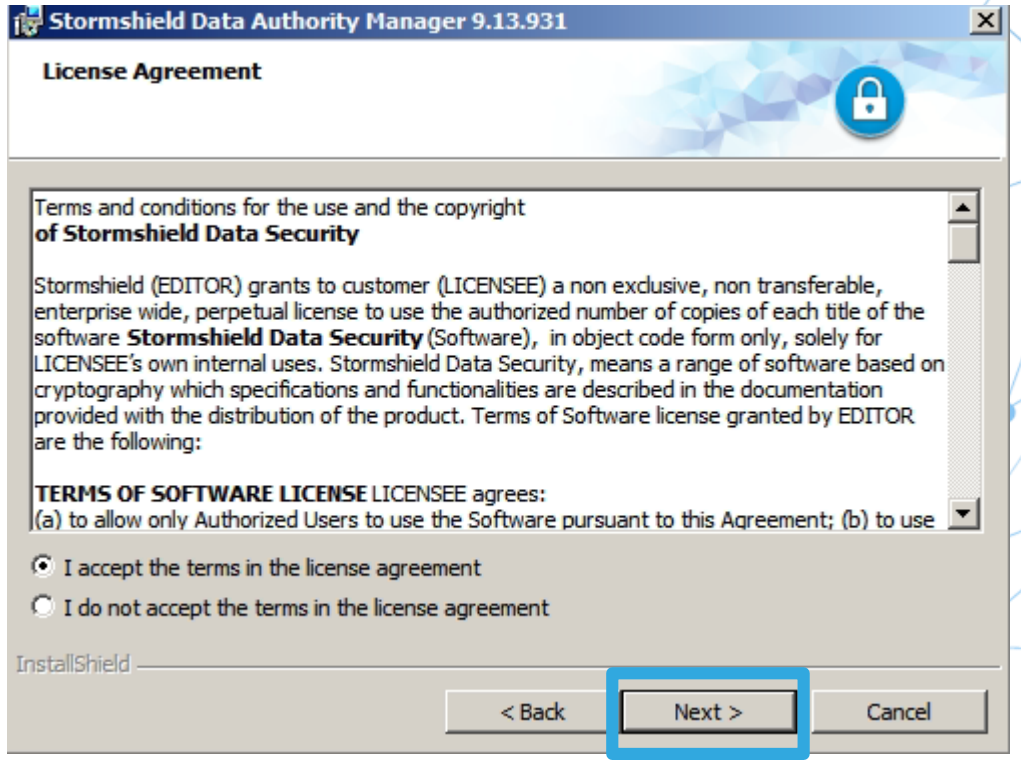
Installing the SDAM server

Launch a command prompt with administrator privileges and then run the installer via the command below msiexec /i “Stormshield Data Authority Manager 9.12.688.msi” (name of the *.msi* could vary based on the SDAM version)

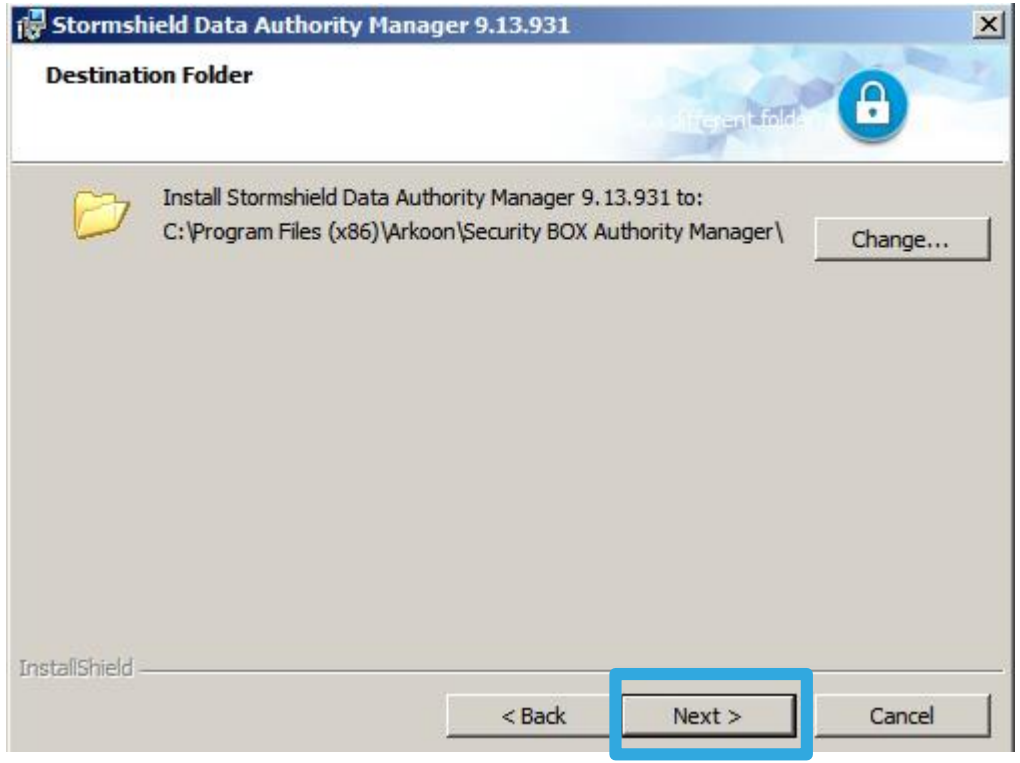


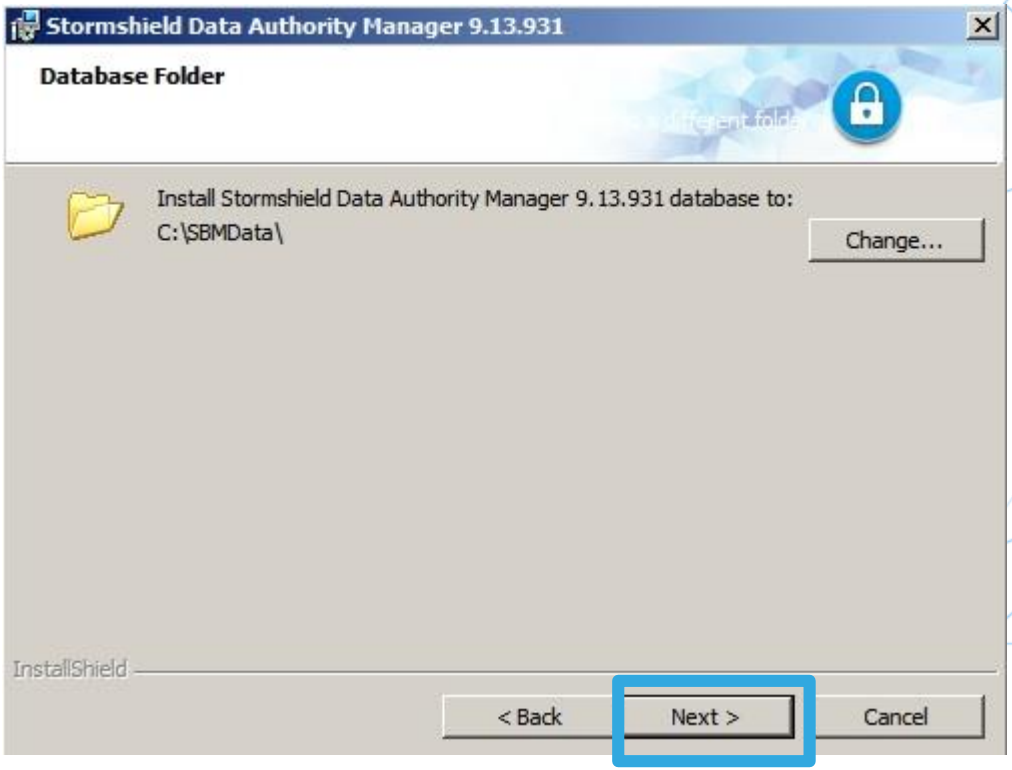
Installing the SDAM server (continued)



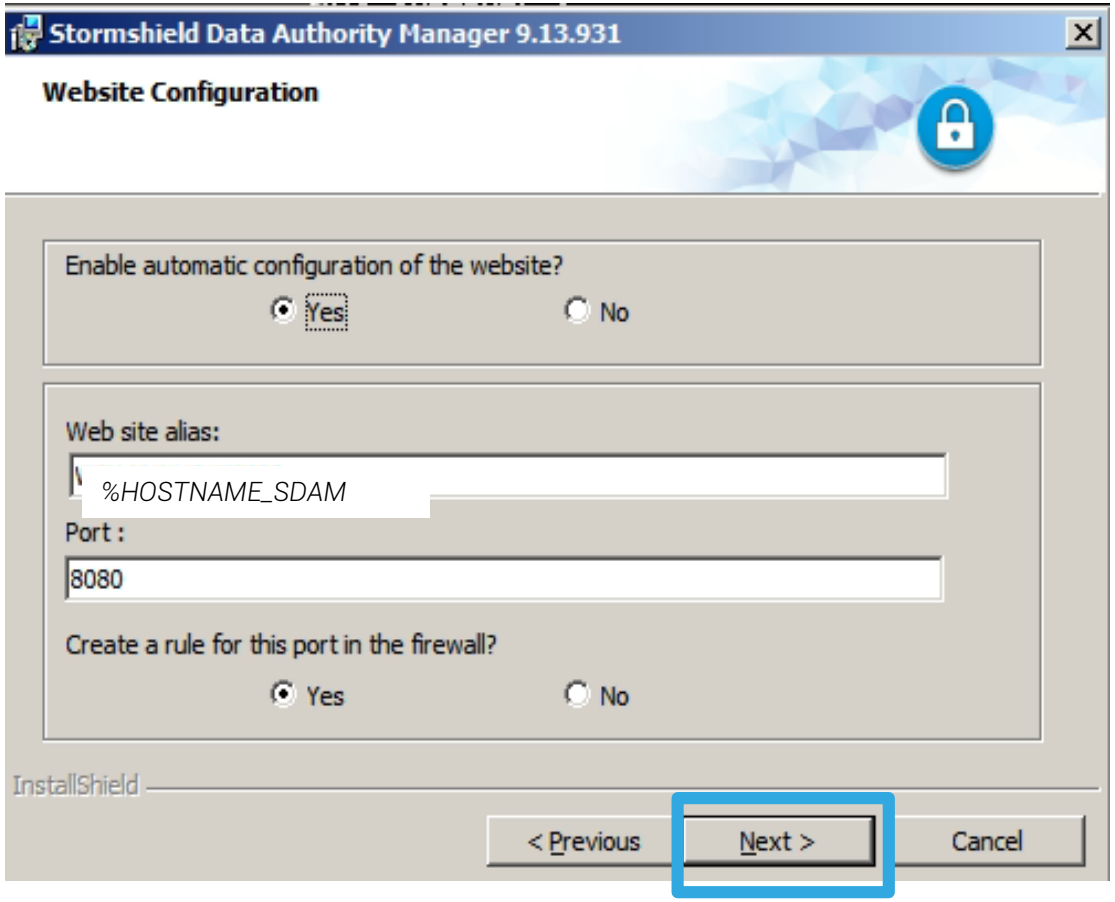


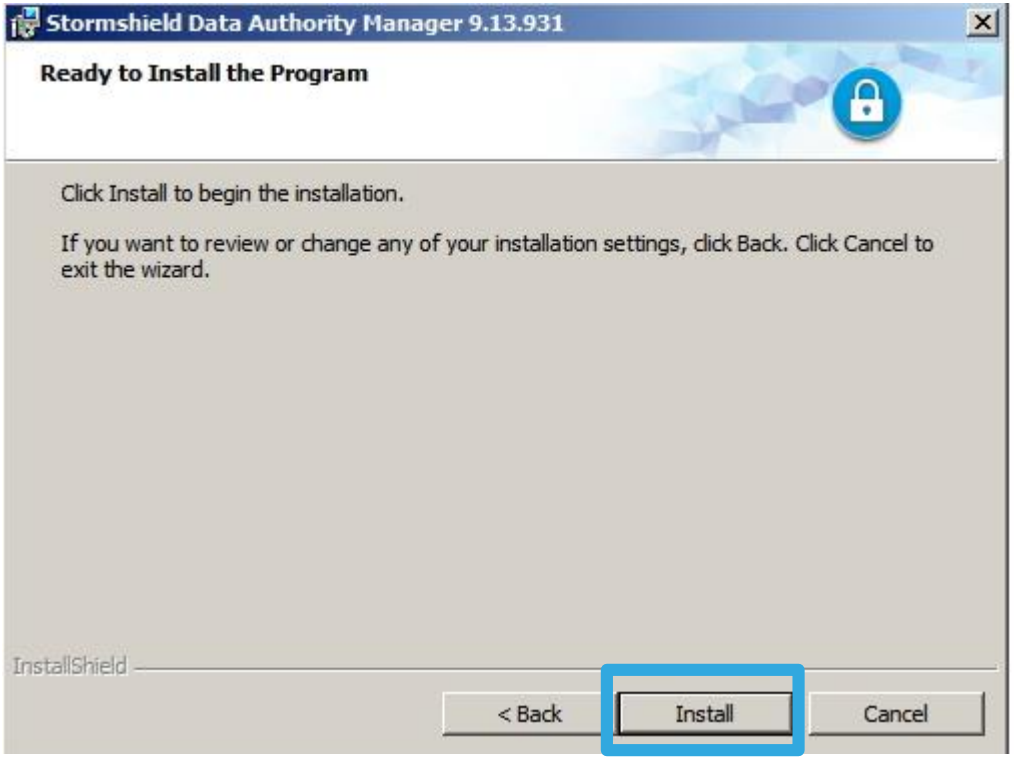
Installing the SDAM server (continued)





Installing the SDAM server (continued)



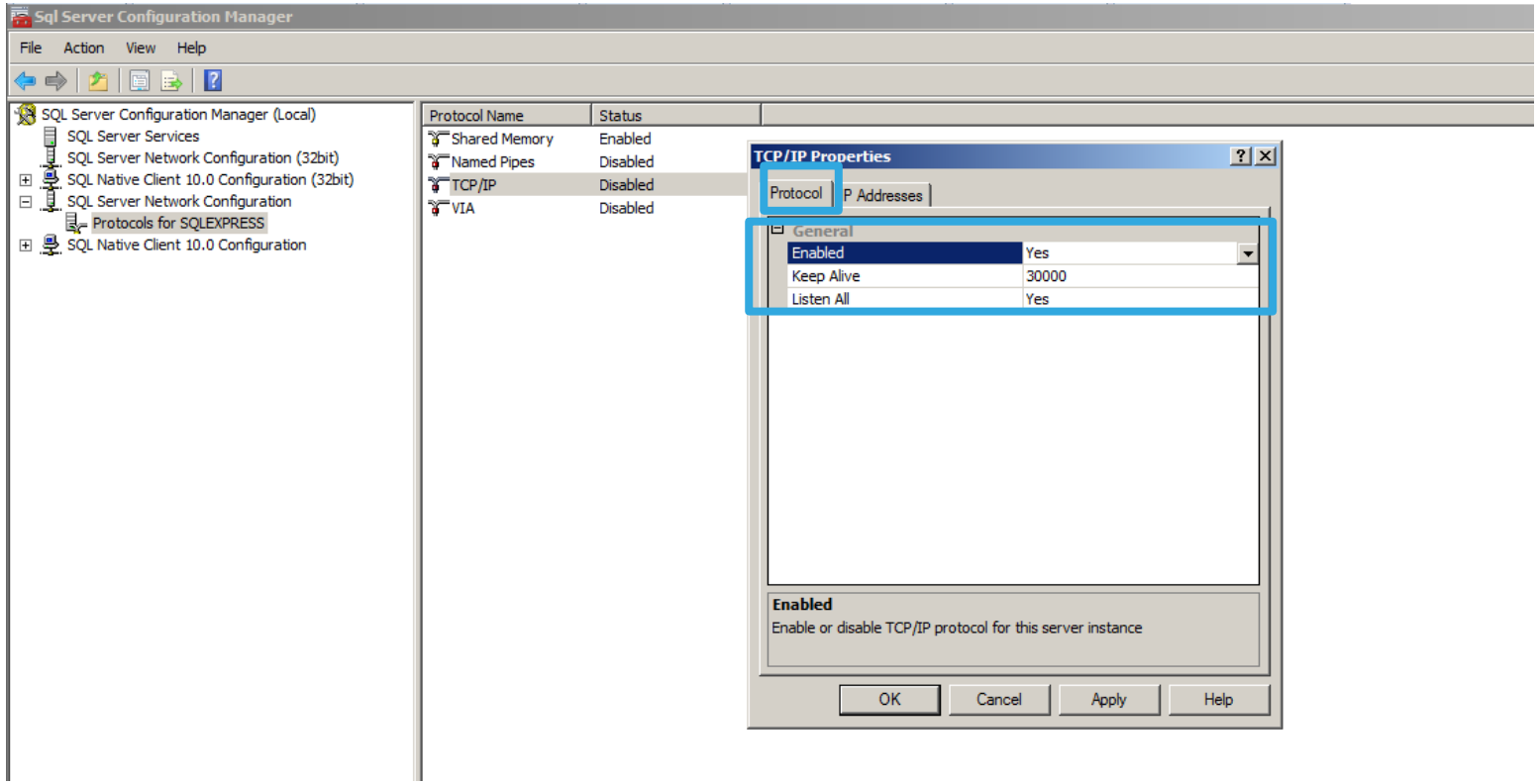


Installing the SDAM server (continued)

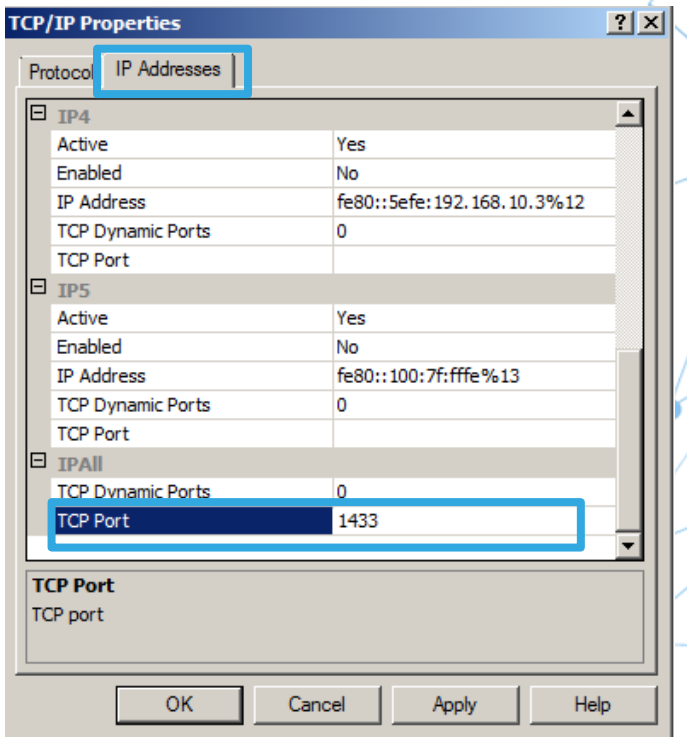
Option: SQL Server recommendations

If this is a demo/POC installation, please do not do this step.
Allow incoming network connections from the server %HOSTNAME_SDAM

In this example, the DB is called "SQLEXPRESS"

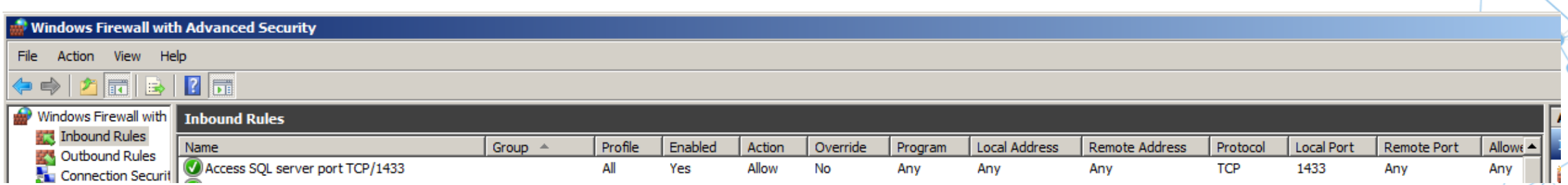


In the same **TCP/IP Properties**window, click on the second tab



Option: SQL Server recommendations

If this is a demo/POC installation please do not do this step.
On the server where SQL is installed, create a firewall rule to allow incoming traffic over port 1433



Option: SQL Server recommendation (continued)

- Script for the creation of the base available in the directory:

C:\Program Files (x86)\Arkoon\Security BOX Authority Manager\Database = <path>

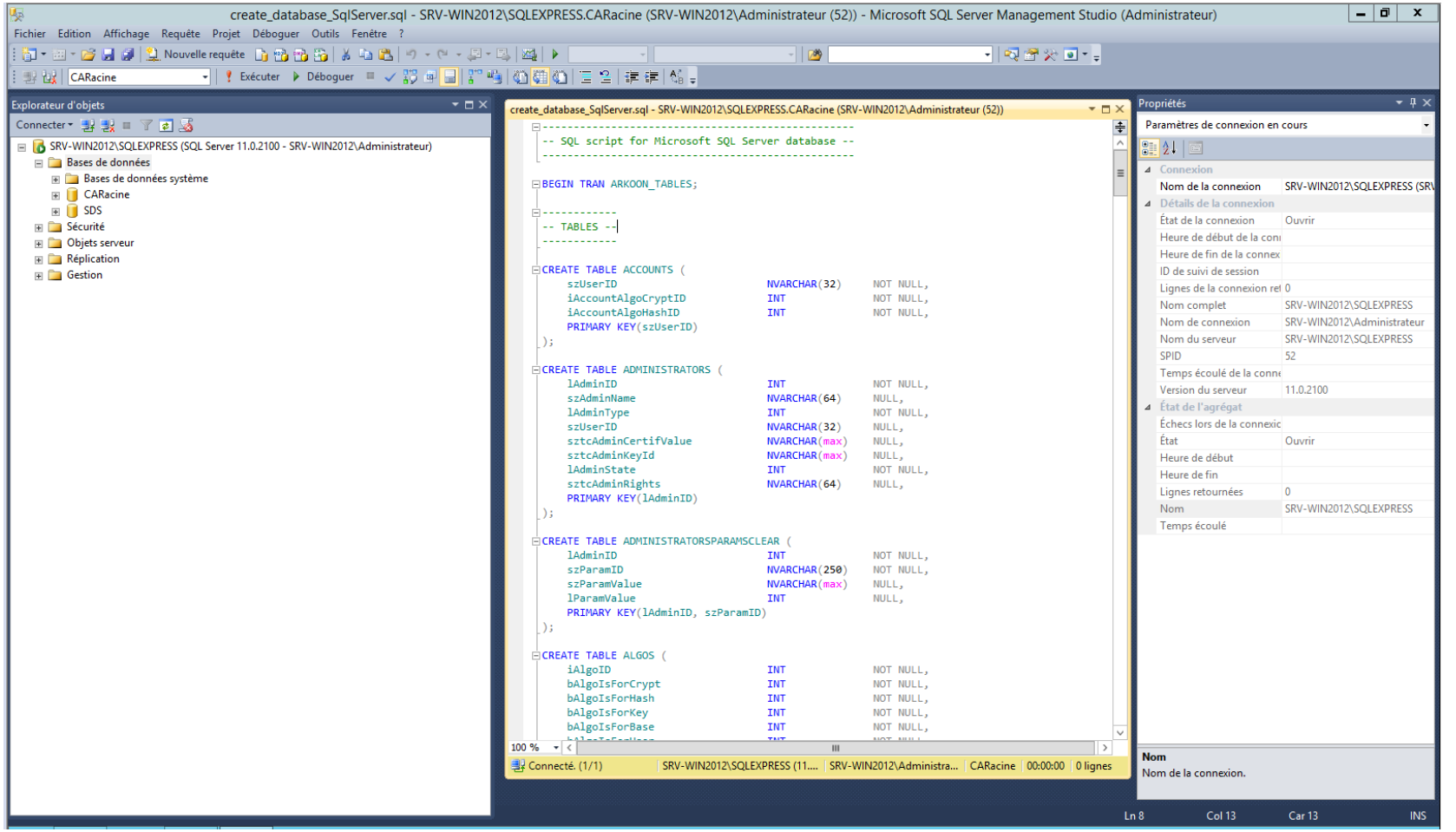
- Creation of the base in command line:

sqlcmd -S myServer\instanceName –d Database

-i <path>\create_database_SqlServer.sql

Option: SQL Server recommendation (continued)

- Creation of the base with Microsoft SQL Management Studio

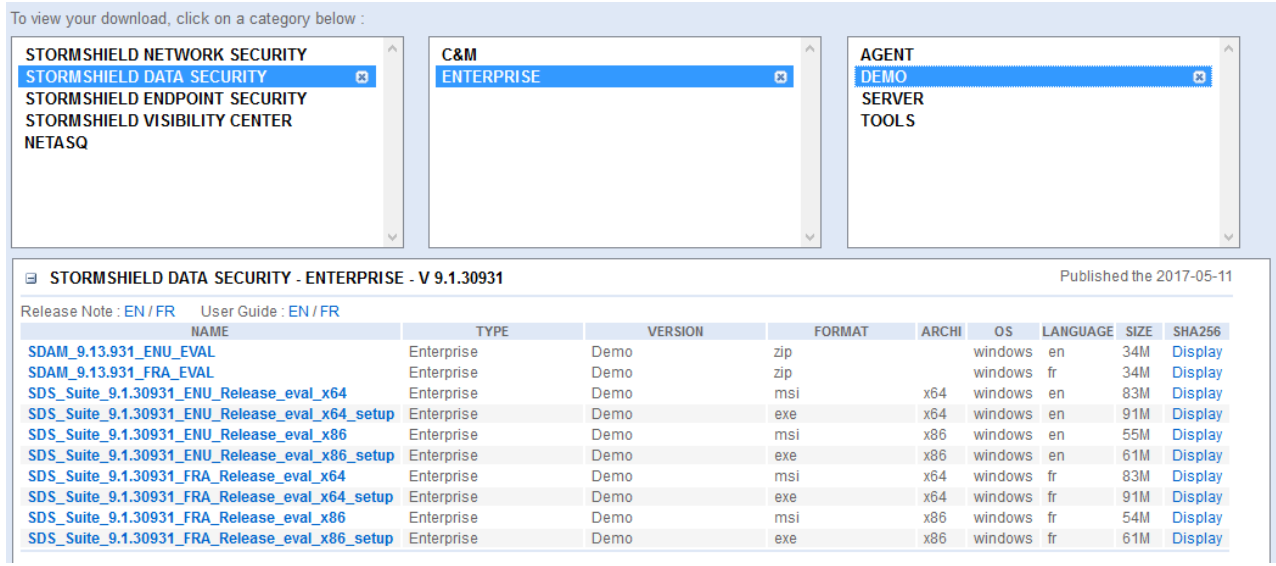


Installing SDS Suite on the administration workstation

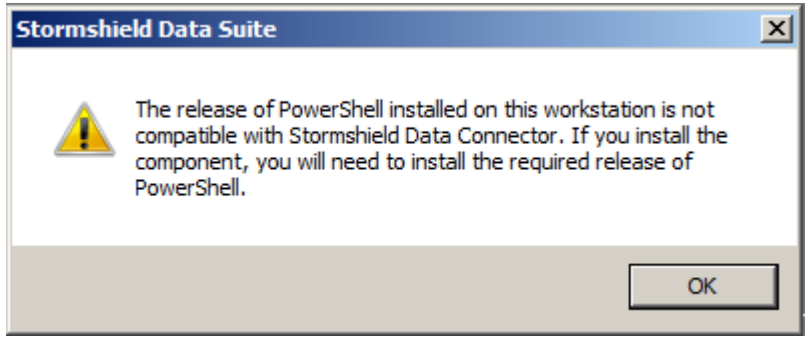
STORMSHIELD

Installing the evaluation version

Install the DEMO version of the SDS agent on the workstation that you will use to configure the SDAM via the web management interface.

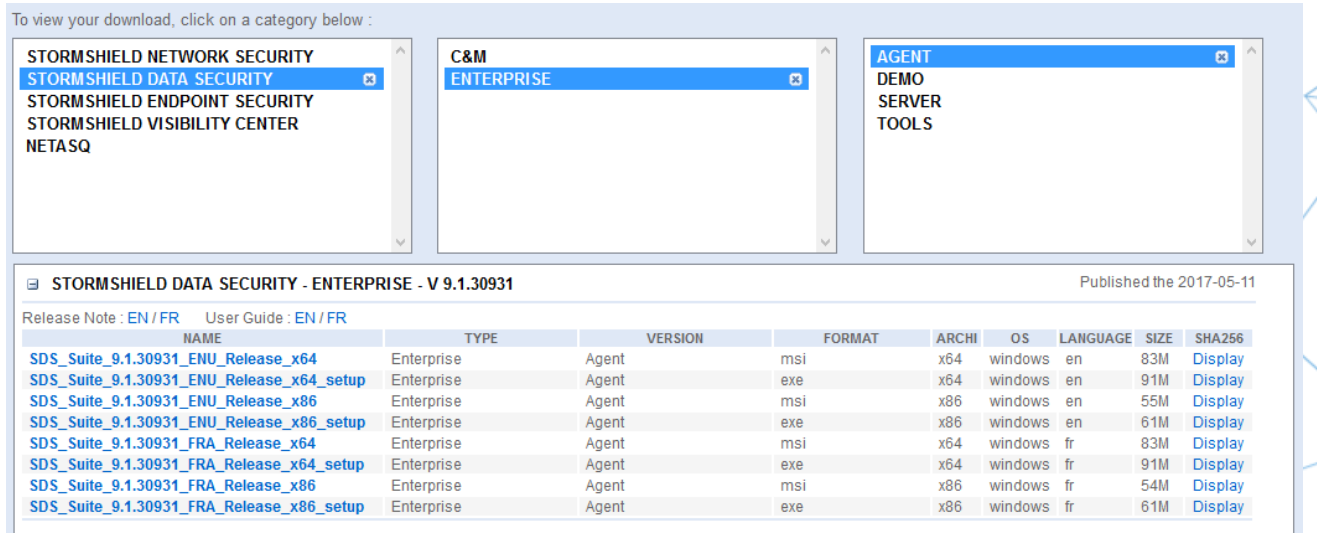


During installation, if you **DO NOT NEED SD Connector** component, please ignore this error message relating to PowerShell



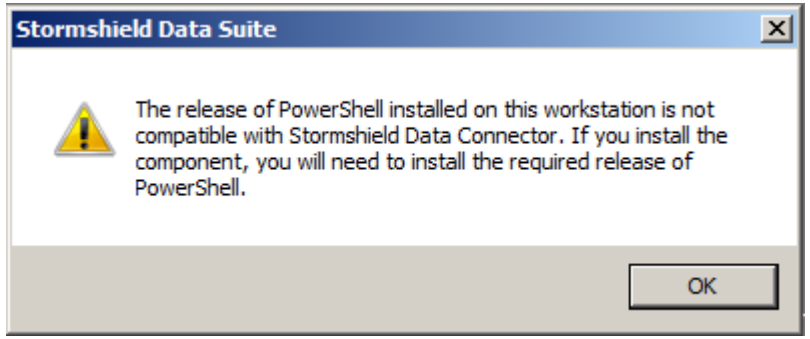
Installing the official version

Install the official version of the SDS agent on the workstation that you will use to configure the SDAM via the web management interface

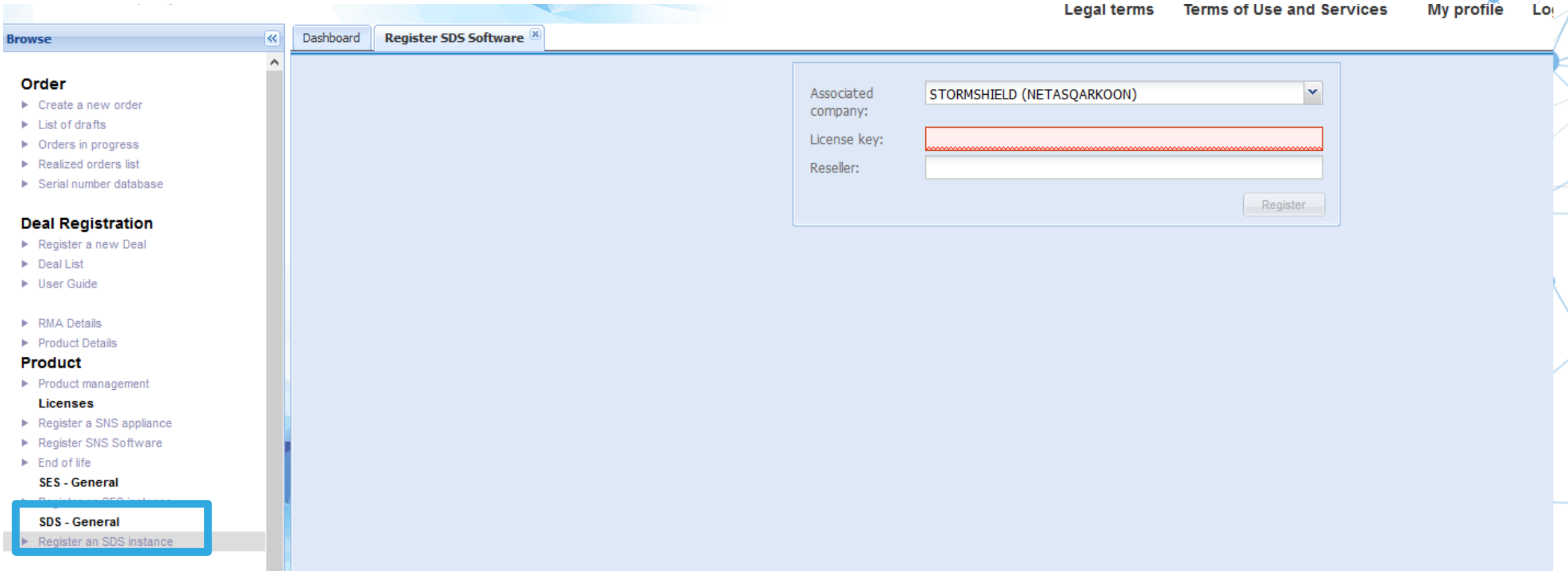


NAME	TYPE	VERSION	FORMAT	ARCHI	OS	LANGUAGE	SIZE	SHA256
SDS_Suite_9.1.30931_ENU_Release_x64	Enterprise	Agent	msi	x64	windows	en	83M	Display
SDS_Suite_9.1.30931_ENU_Release_x64_setup	Enterprise	Agent	exe	x64	windows	en	91M	Display
SDS_Suite_9.1.30931_ENU_Release_x86	Enterprise	Agent	msi	x86	windows	en	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

During installation, if you **DO NOT NEED SD Connector** component, please ignore this error message relating to PowerShell



Registering your Stormshield Data Security product



Scenarios

- In the following pages, two scenarios are presented:

1. POC scenario, only one database needs to be created for the root CA (Access DB). In the Administration Guide uploaded from MyStormshield you will find the procedure on how to migrate from Access DB to SQL. Refer to the sections Creating the root PKI and Configuring Internet Explorer + Initializing the root PKI.

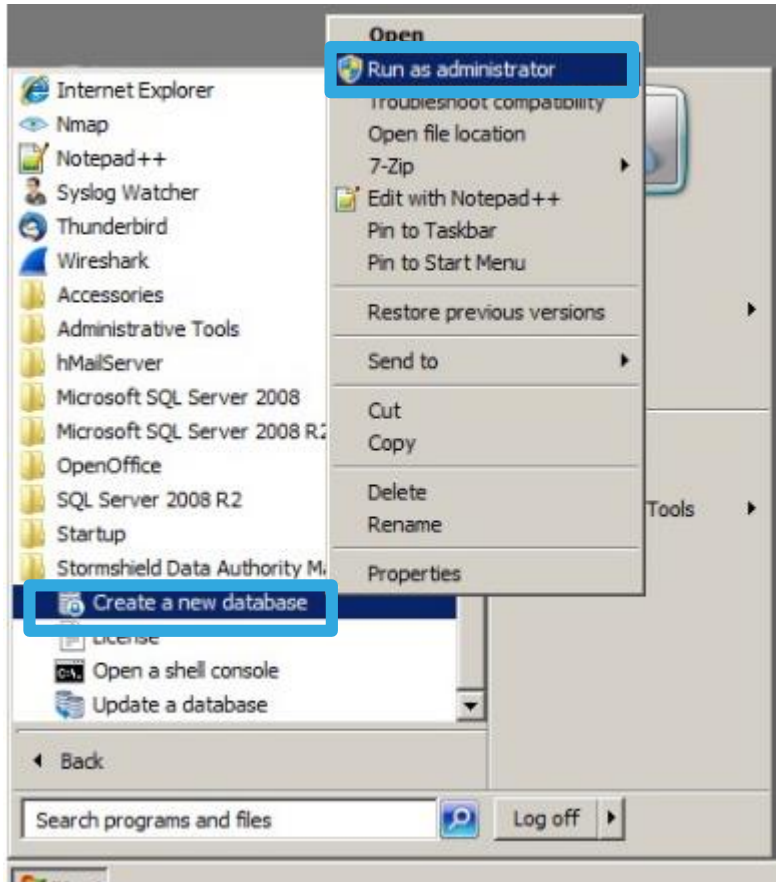
2. Best Practice scenario, two databases are needed (SQL DB) for the root CA and the child CA. Refer to the sections above and to the section Initializing a child PKI (option).

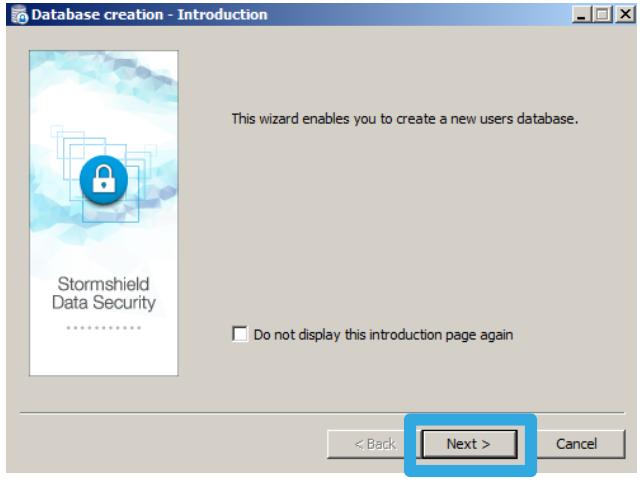
Creating the root PKI

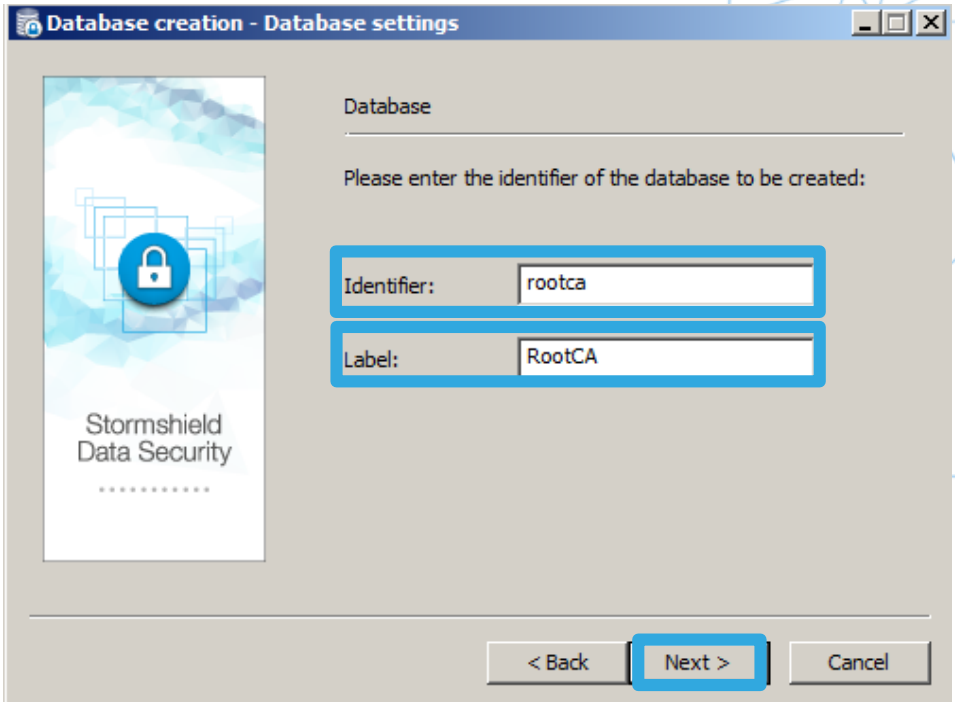
Installing the Access DB for the Root CA

- Identifier: The identifier is essentially used internally by the SDAM
- Label: The label is used in all SDAM pages to refer to the user database

Click on **Create a new database** and
Run as administrator

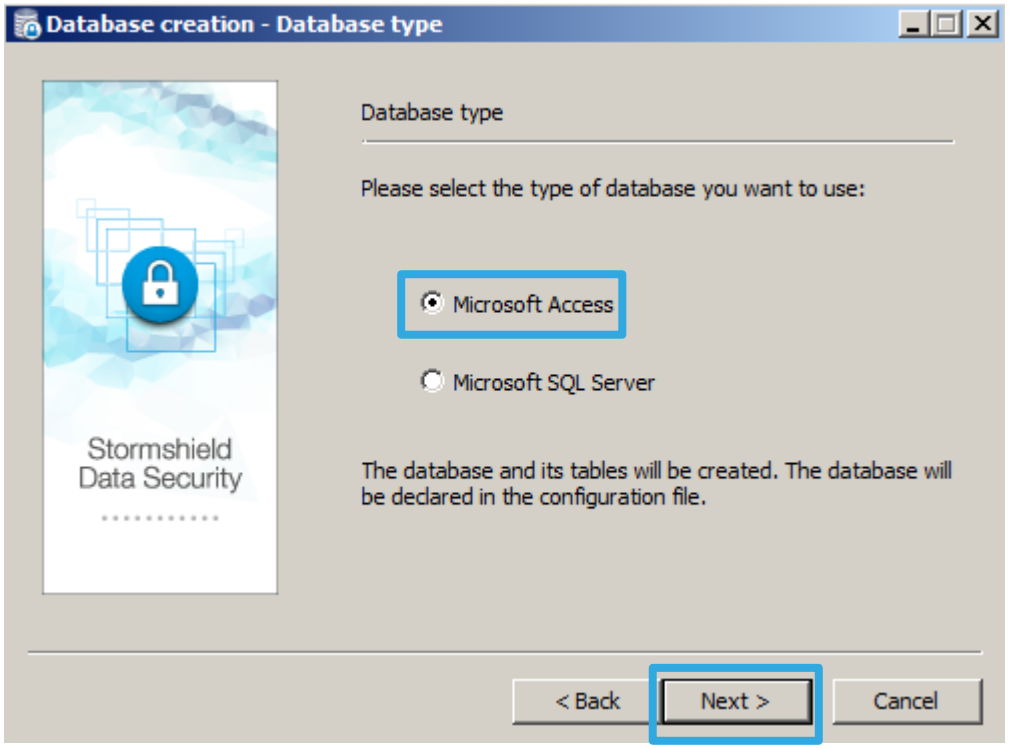


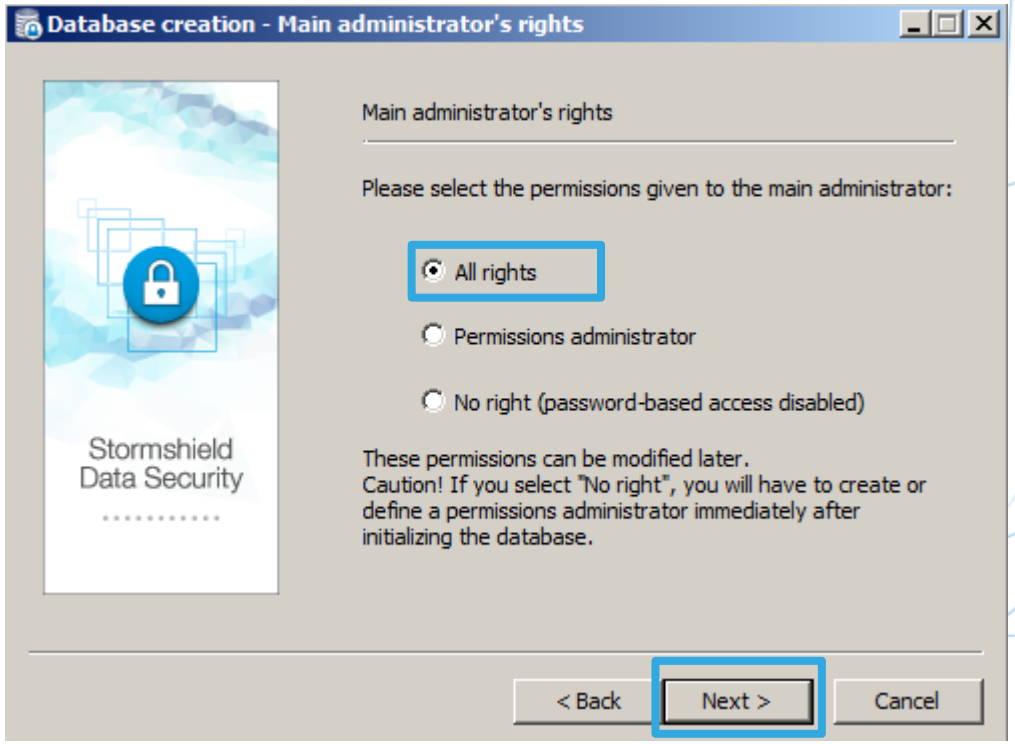




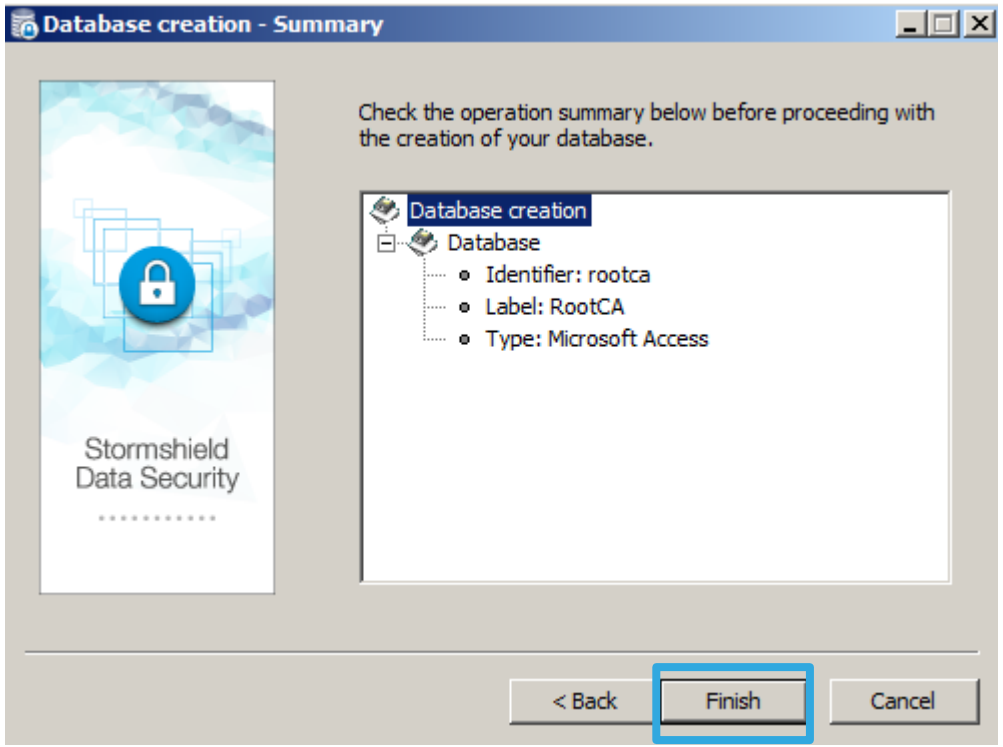
Installing the Access DB for the Root CA (continued)

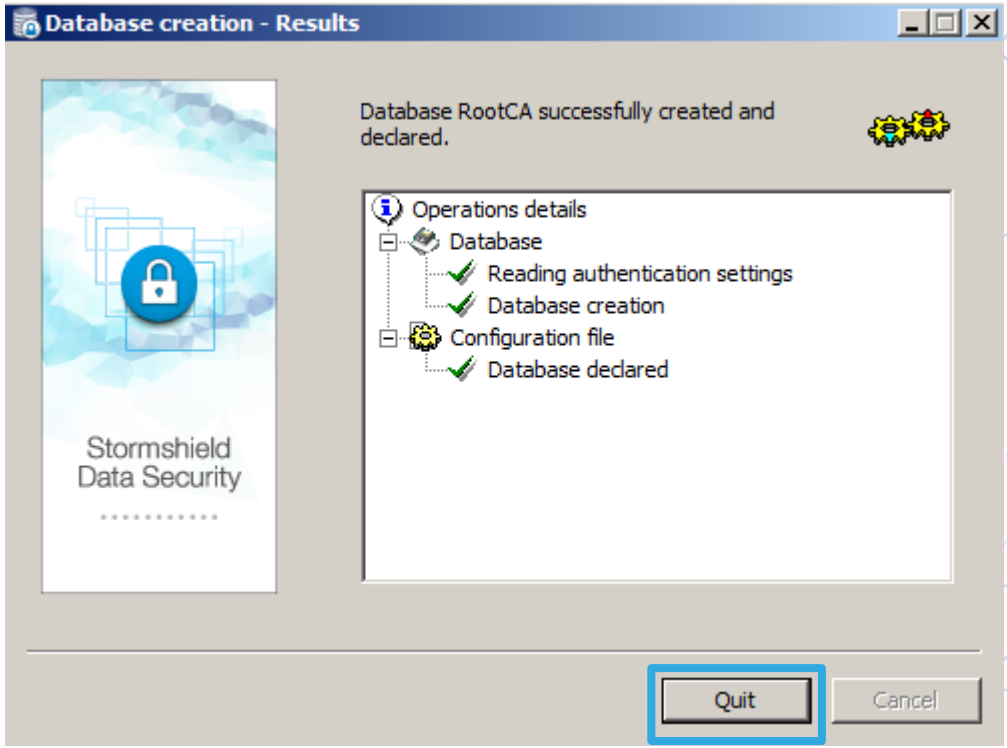
If you choose to create a "Microsoft SQL Server" database, see SQL Server recommendations





Installing the Access DB for the Root CA (continued)

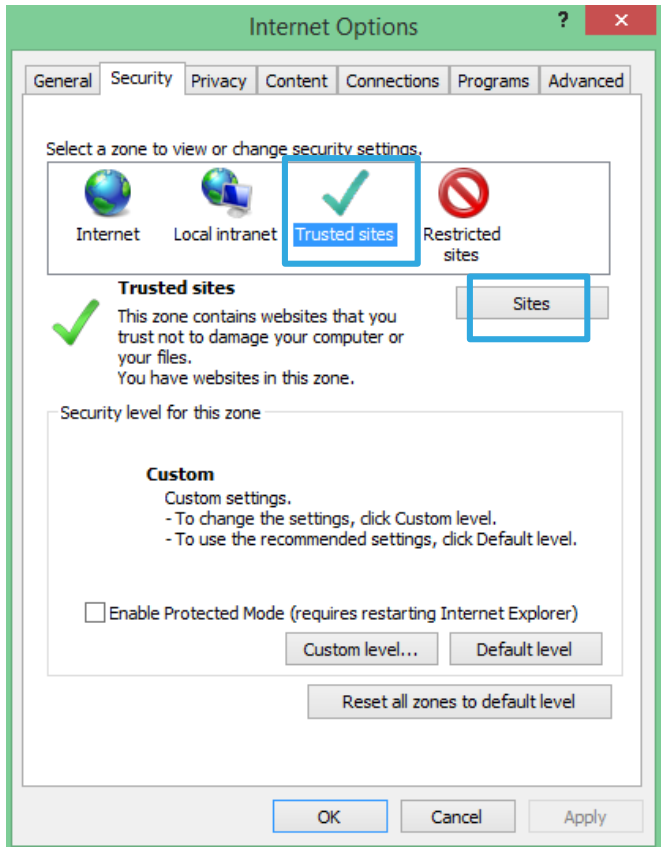


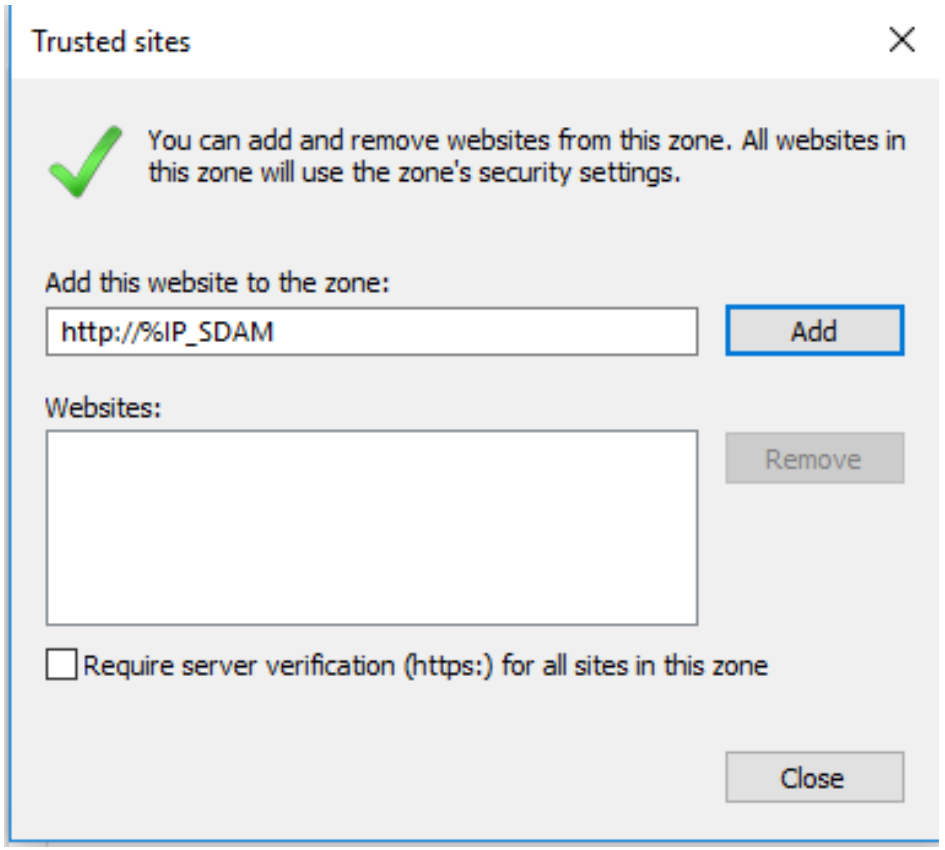


Configuring Internet Explorer
+
Initializing the root PKI

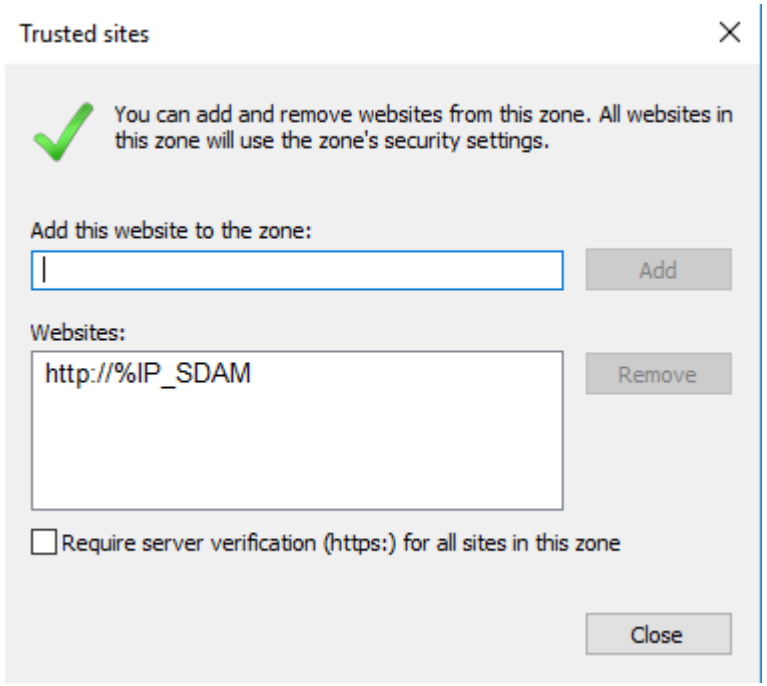
STORMSHIELD

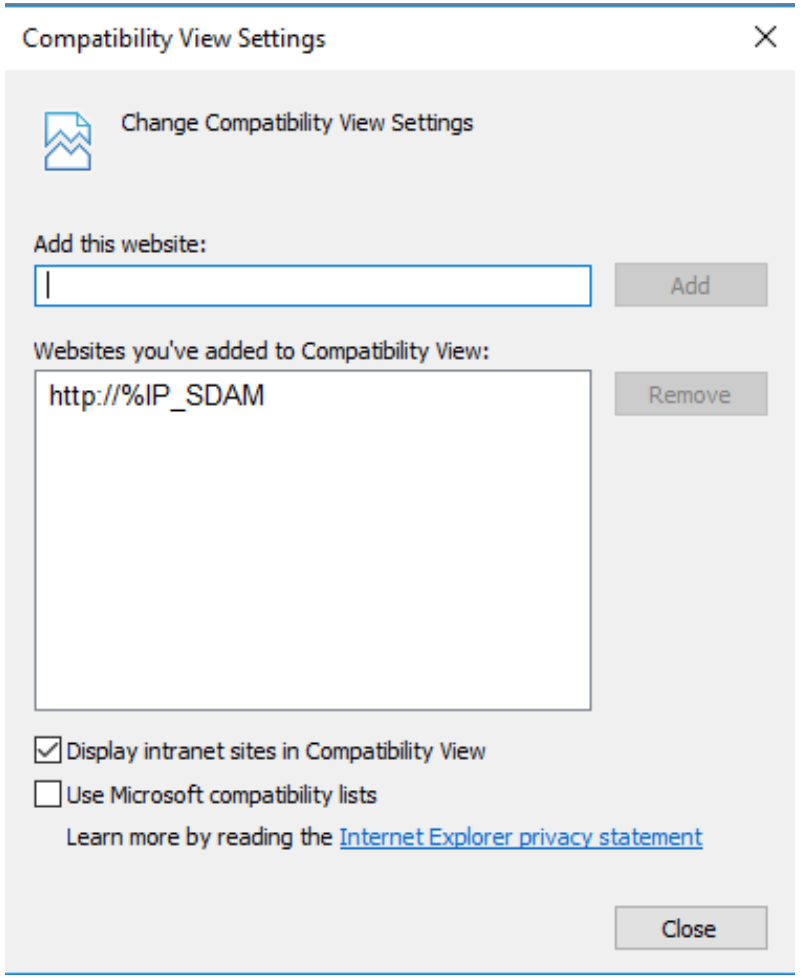
Initial connection to the SDAM web management interface



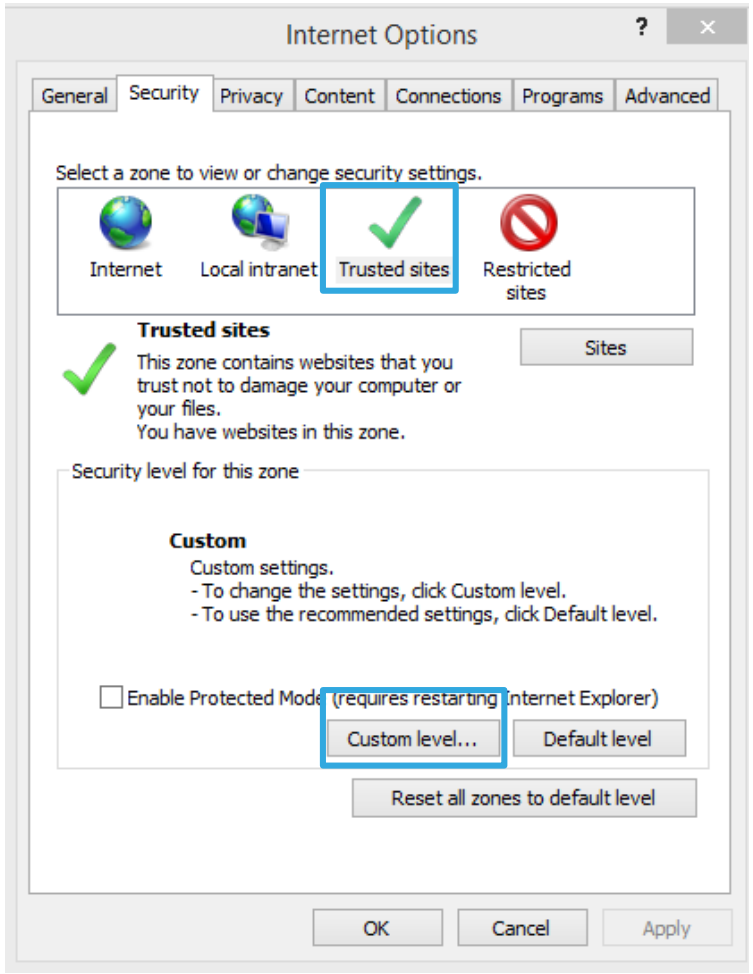


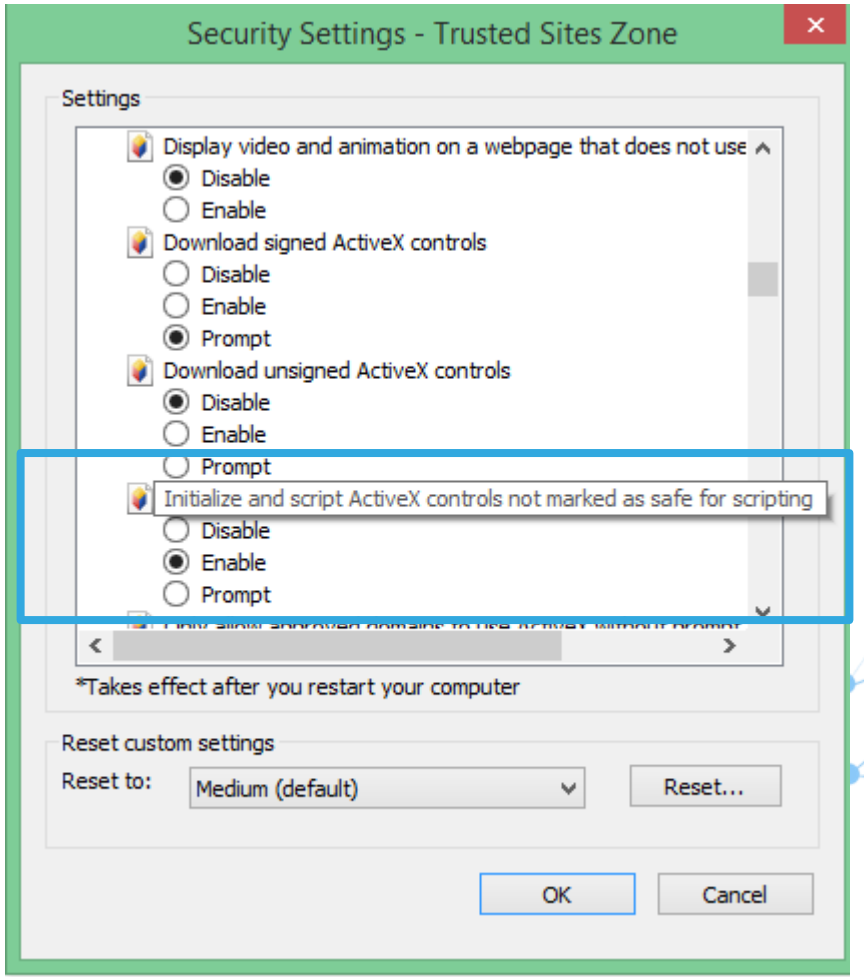
Initial connection to the SDAM web management interface (continued)





Initial connection to the SDAM web management interface (continued)

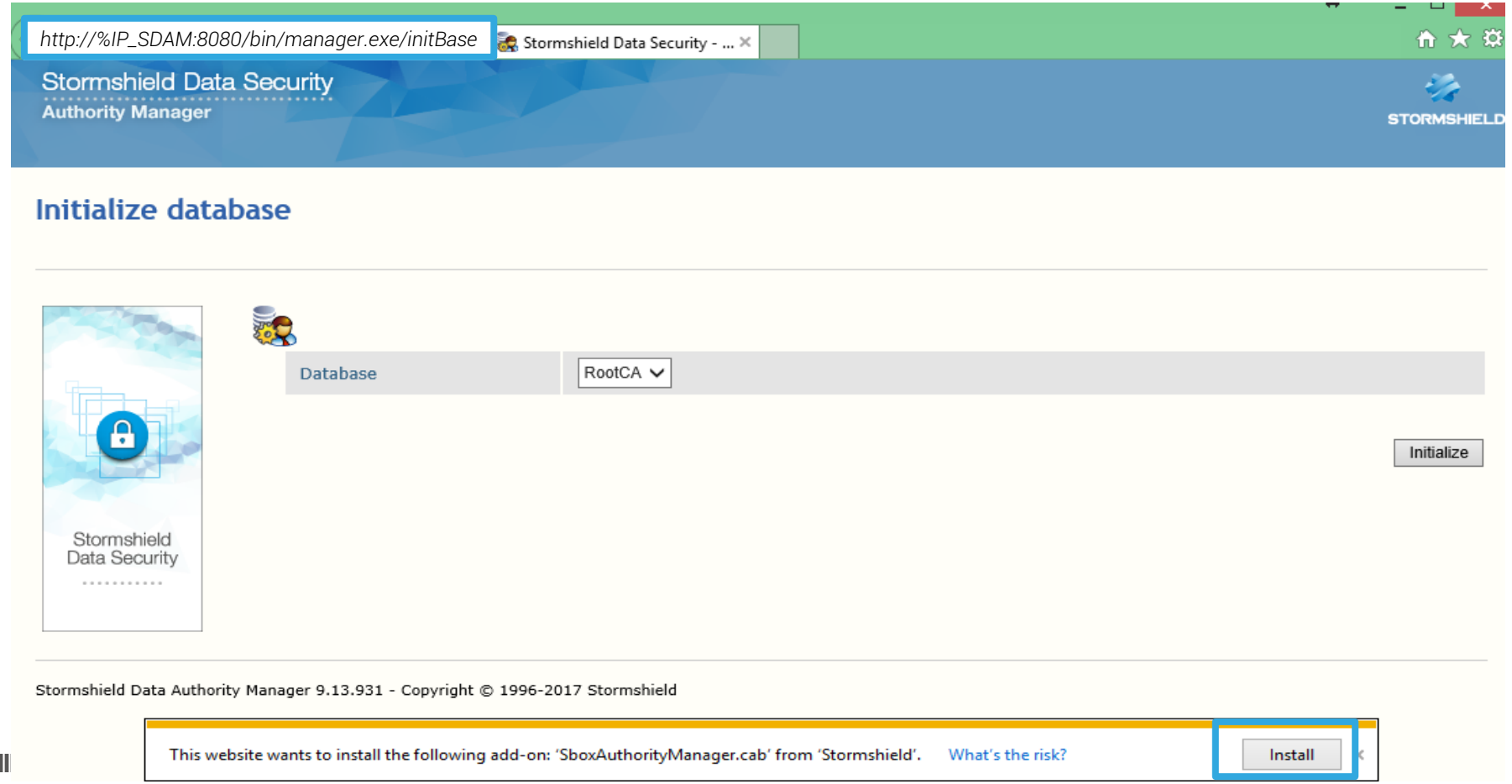




Initial connection to the SDAM web management interface (continued)

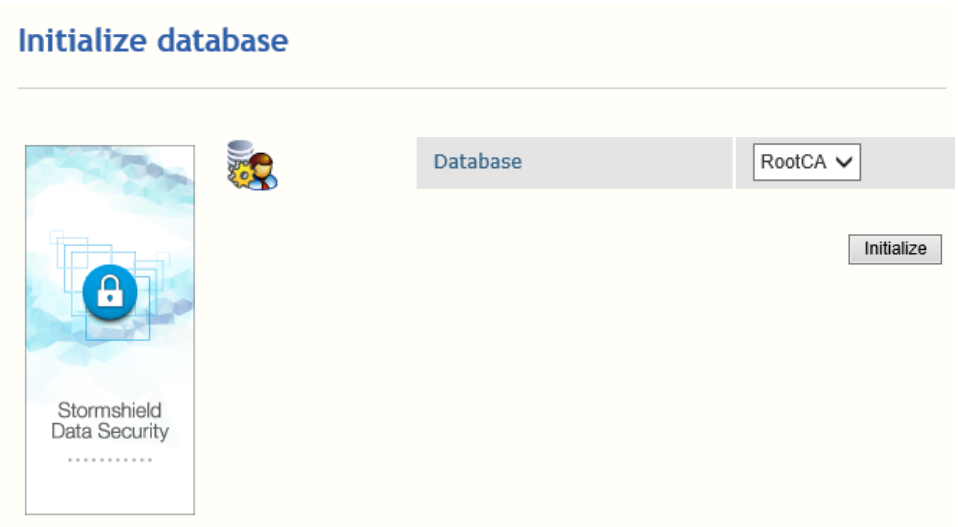
Open Internet Explorer from the workstation where you installed SDS agent and go to the following website: http://%IP_SDAM:8080/bin/manager.exe/initBase

You need to install the activeX (if you have an error, please check your IE settings on the previous slide)

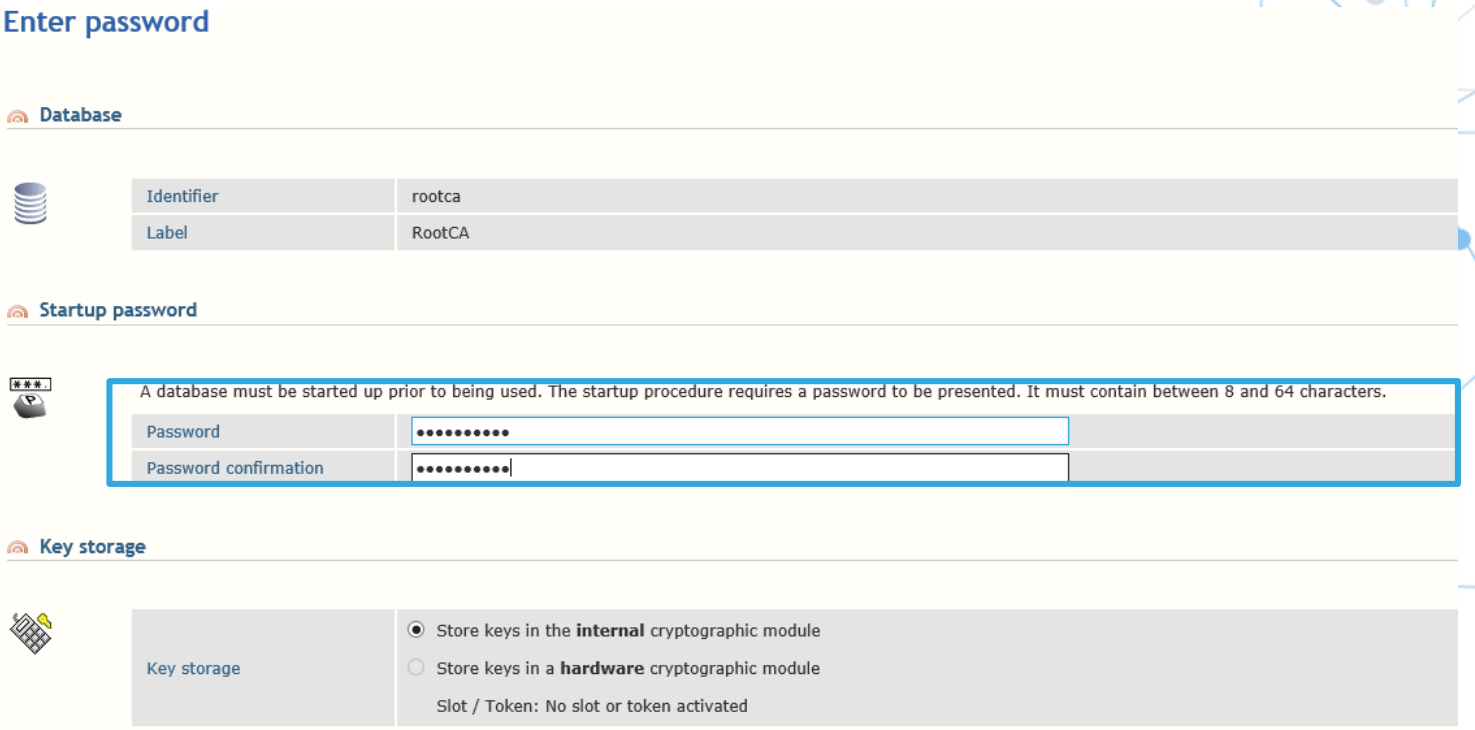


Initializing the RootCA

After you have installed the activeX, initialize the RootCA database

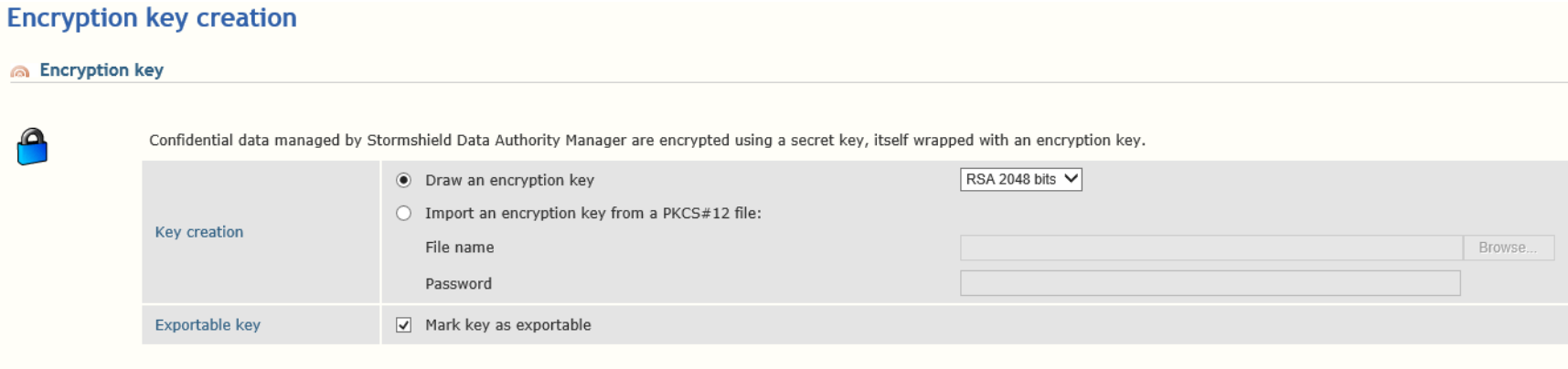


Here, you need to insert the password that will be used to start the database



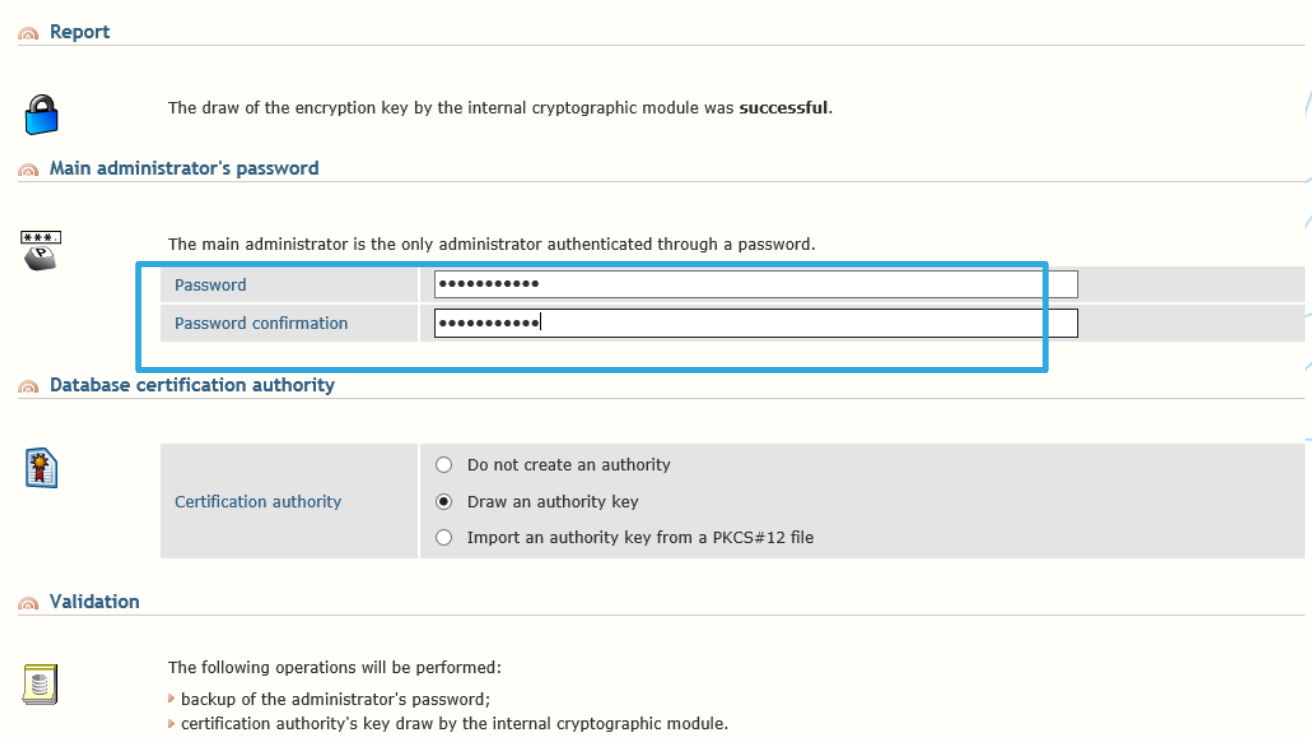
Click on **Proceed** at the bottom of the page

Initializing the RootCA (continued)

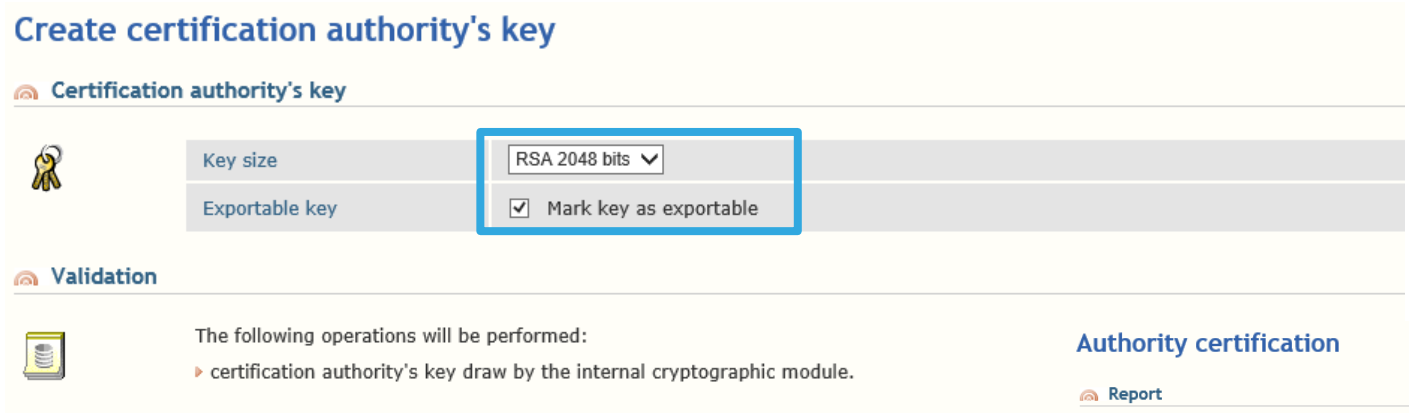


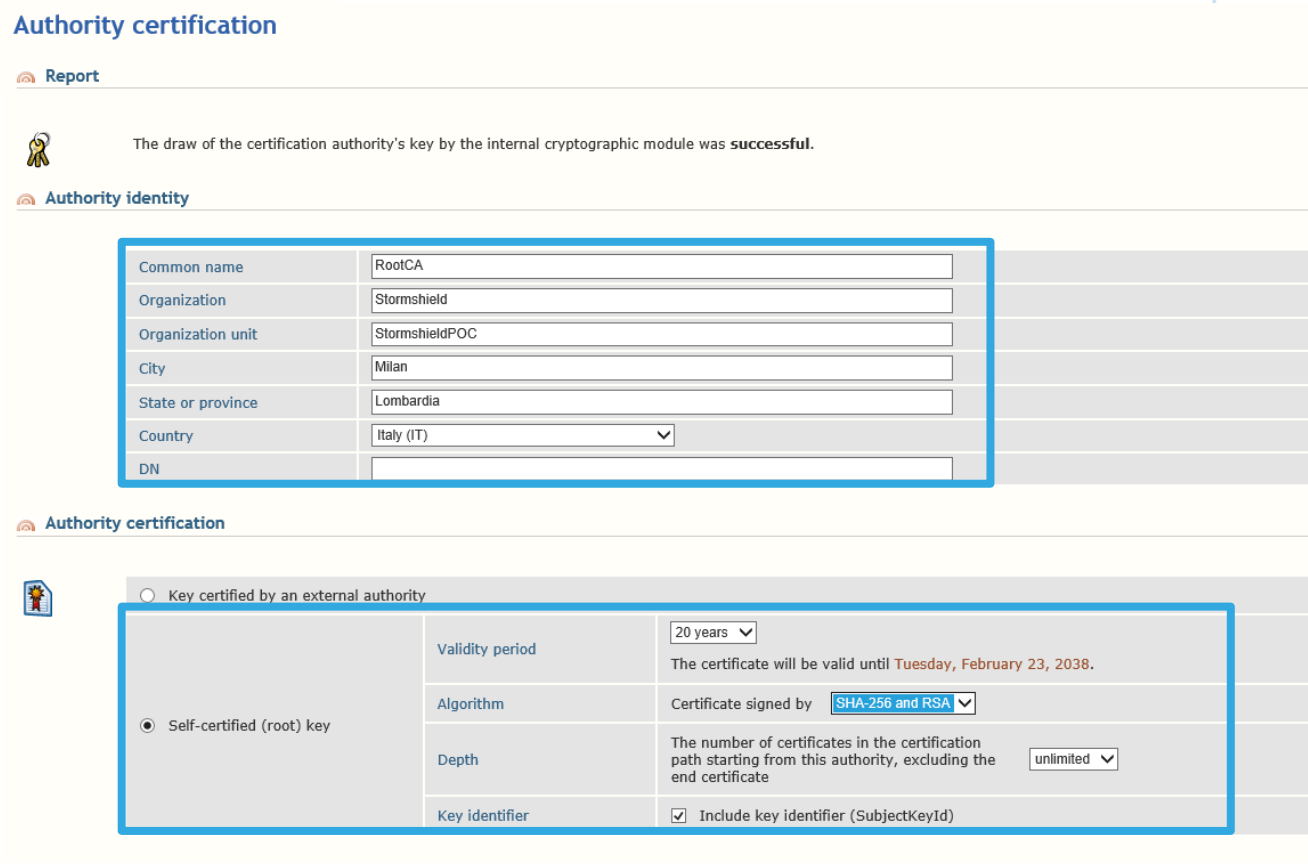
Click on **Proceed**

Insert the Administrator password that you will use to connect to the SDAM web interface



Initializing the RootCA (continued)

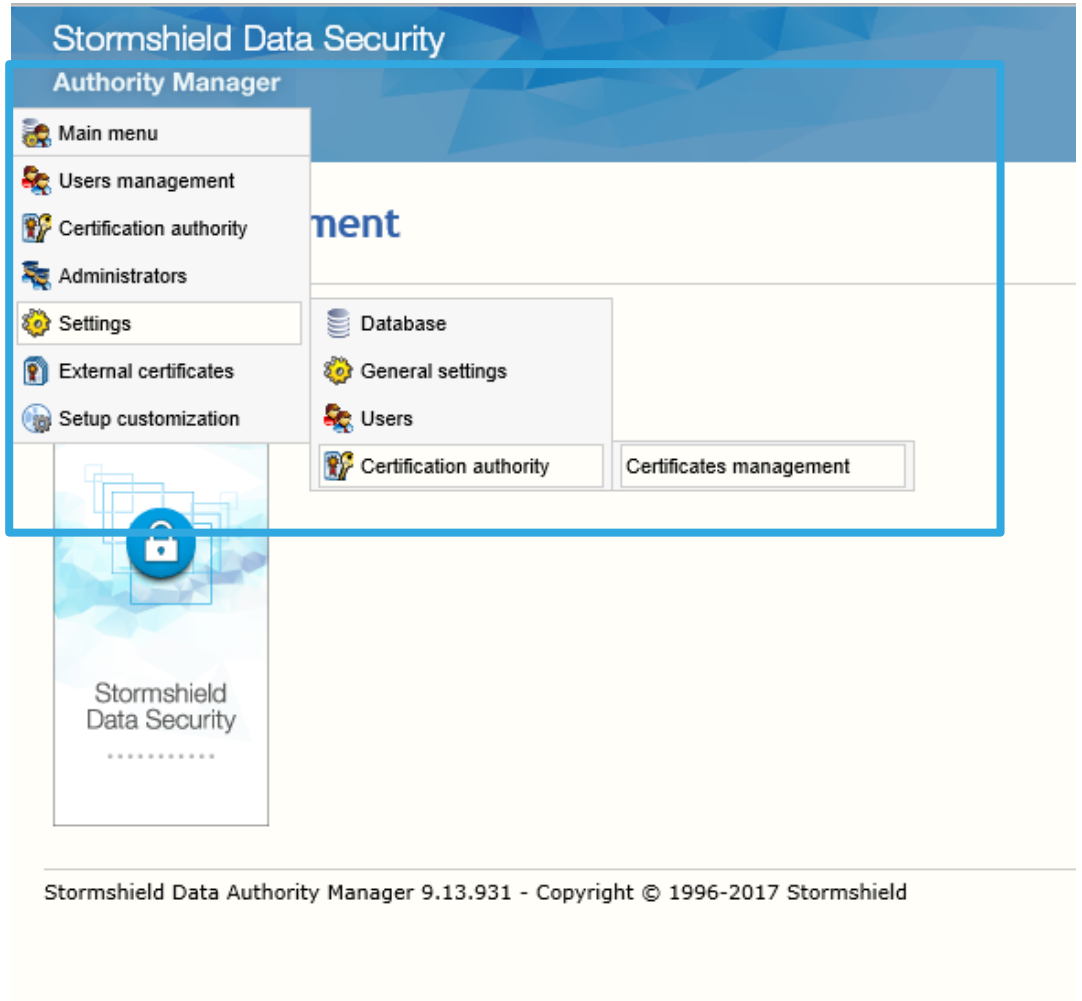




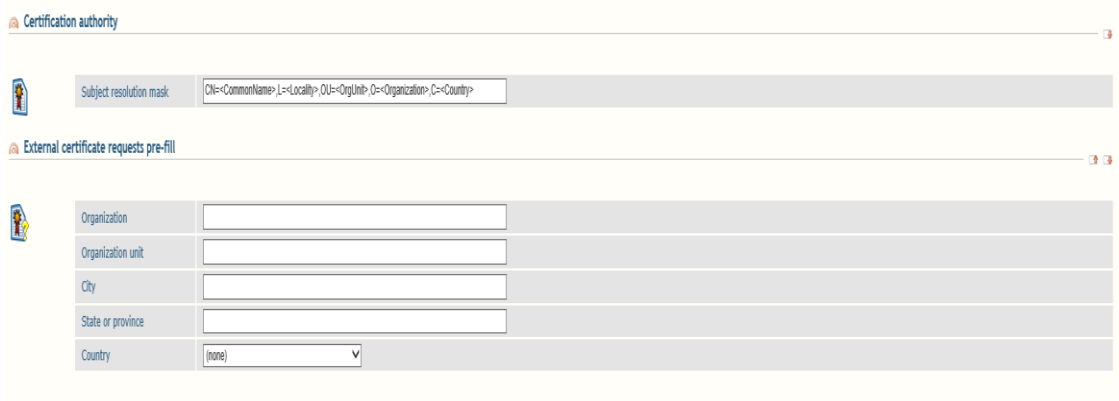
Click on **Finish**.
Now the database has been initialized.

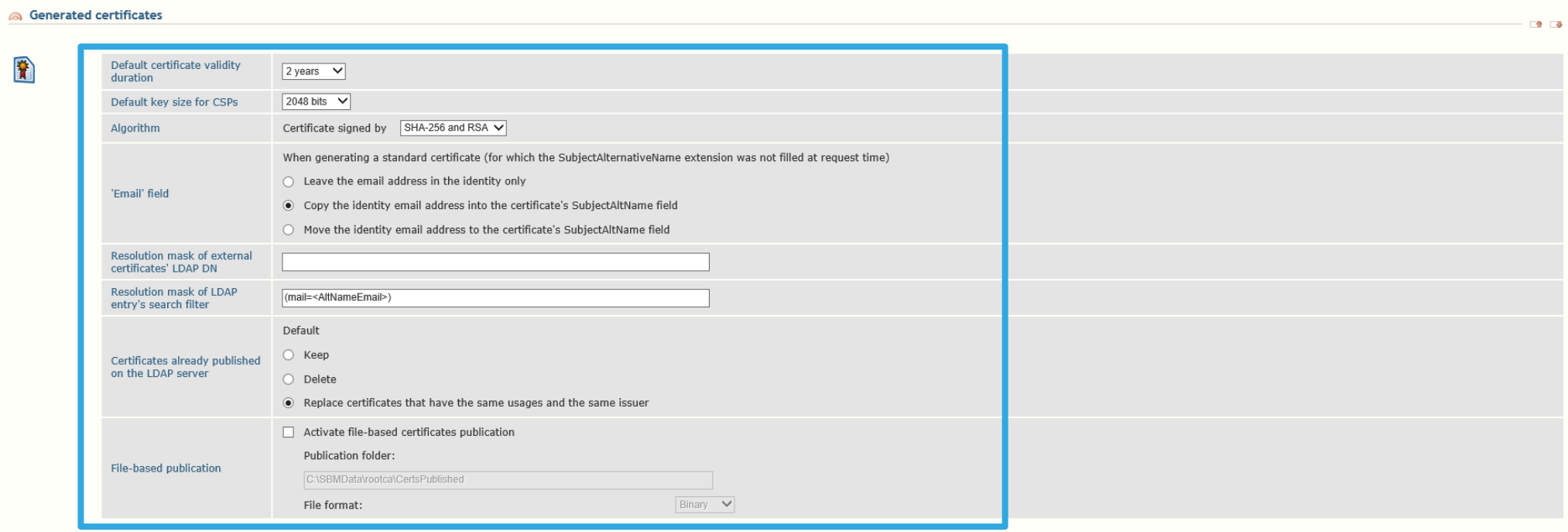
Configuring the CRL of the RootCA

Now you need to connect to the SDAM web interface and create the CRL for RootCA. To do so, use the link http://%IP_SDAM:8080/bin/manager.exe/OpenSession



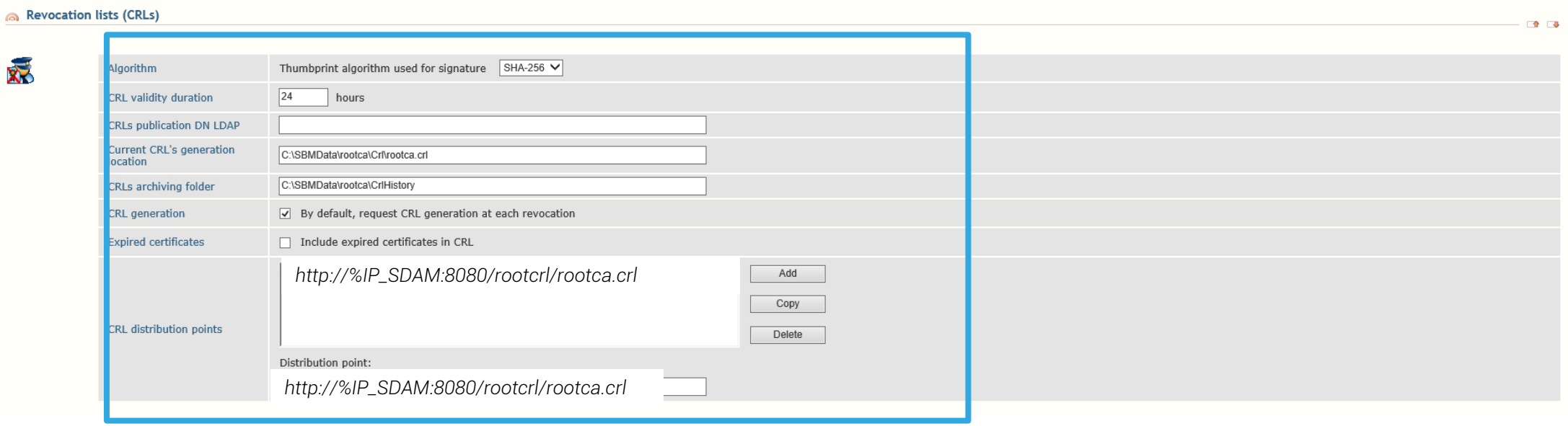
Configuring the CRL (continued)

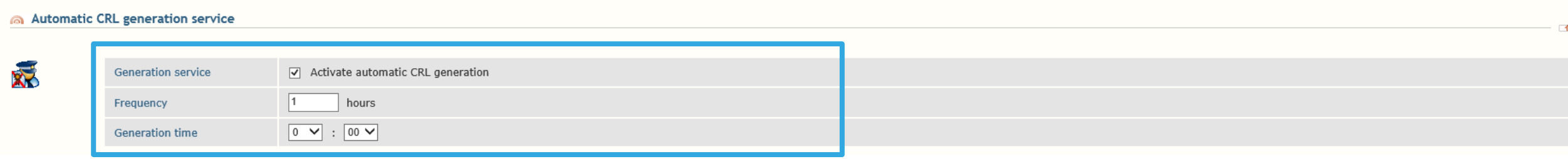




Configuring the CRL (continued)

Add the URL for the CRL download http://%IP_SDAM:8080/rootcrl/rootca.crl
You can add more than one URL if you would like to have more than one distribution point



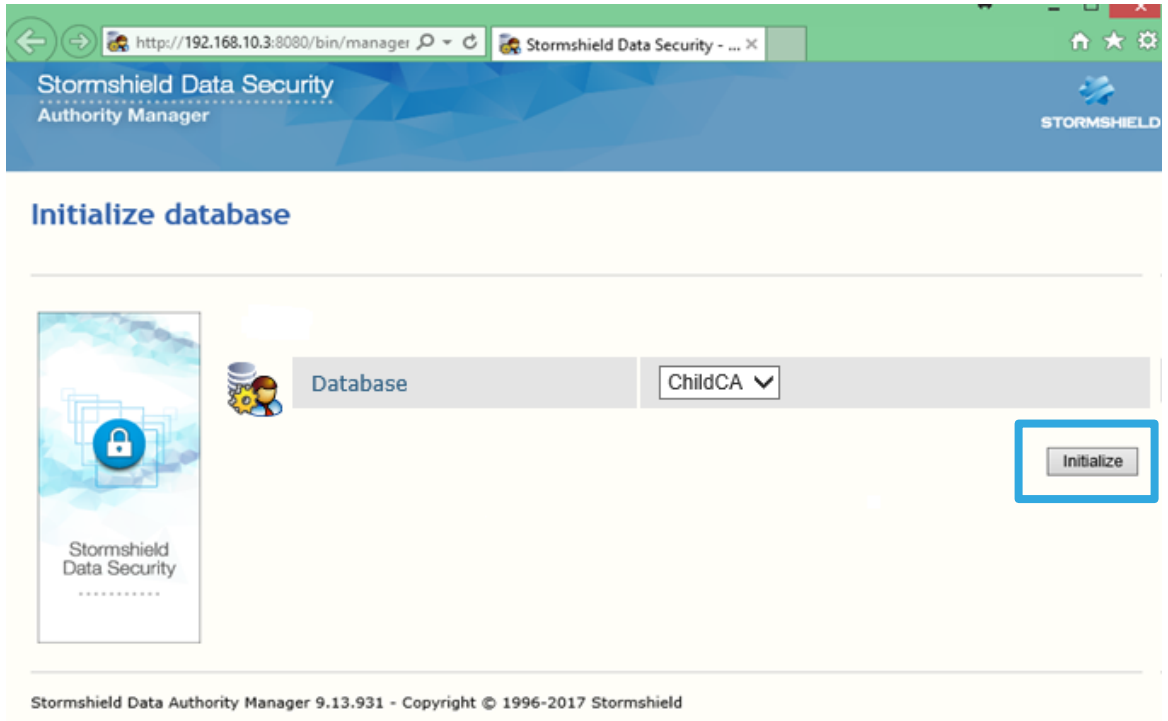


Click on **Apply modifications**

Initializing a child PKI (option)

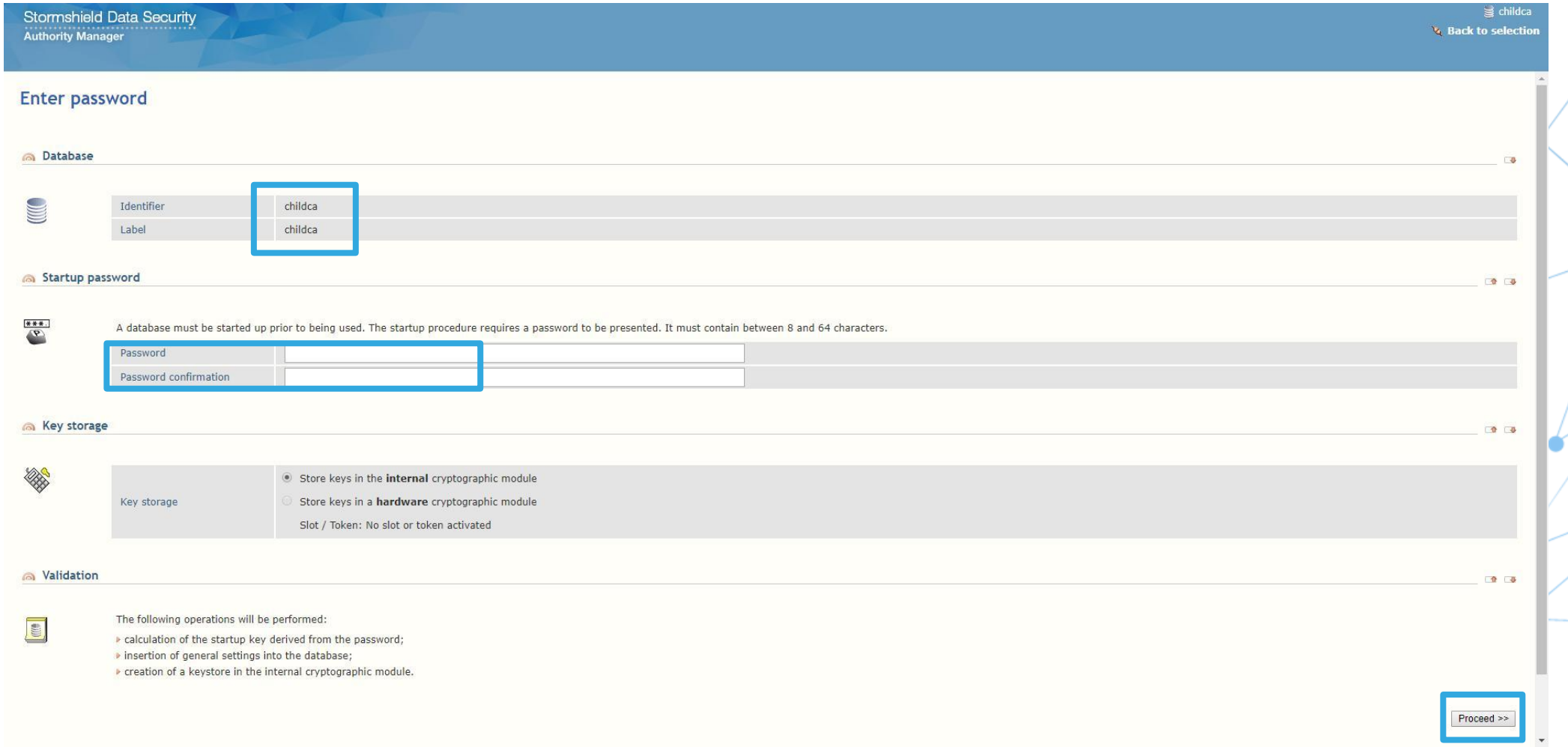
Option: initializing the Child CA

To initialize a base, go to the following web page and then select the base: *http://%IP_SDAM:8080/bin/manager.exe/initBase*

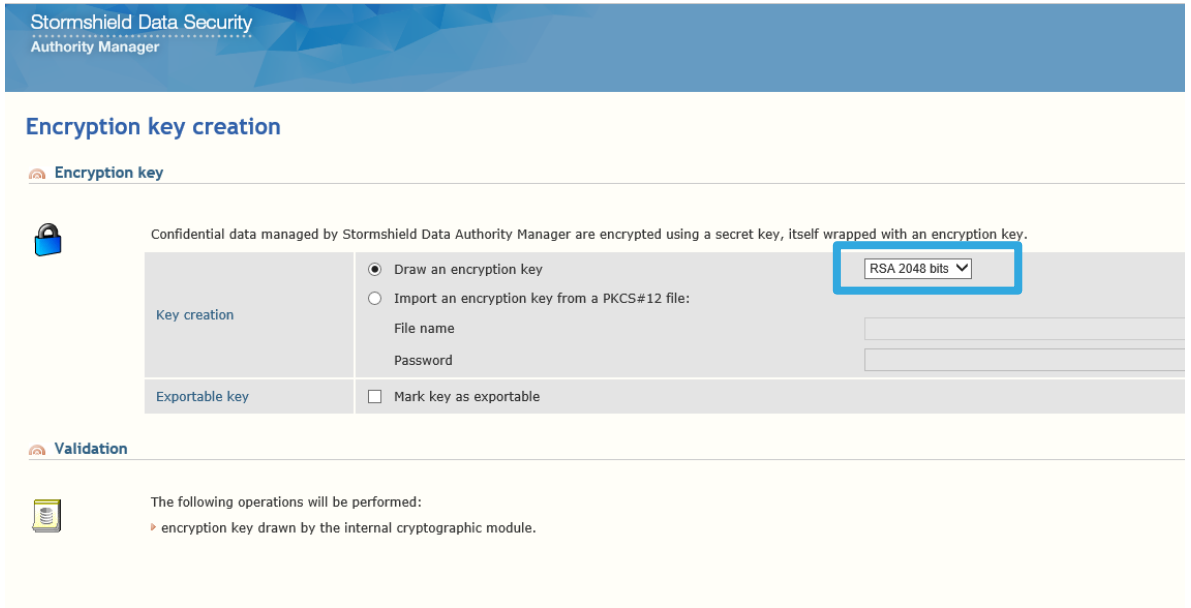


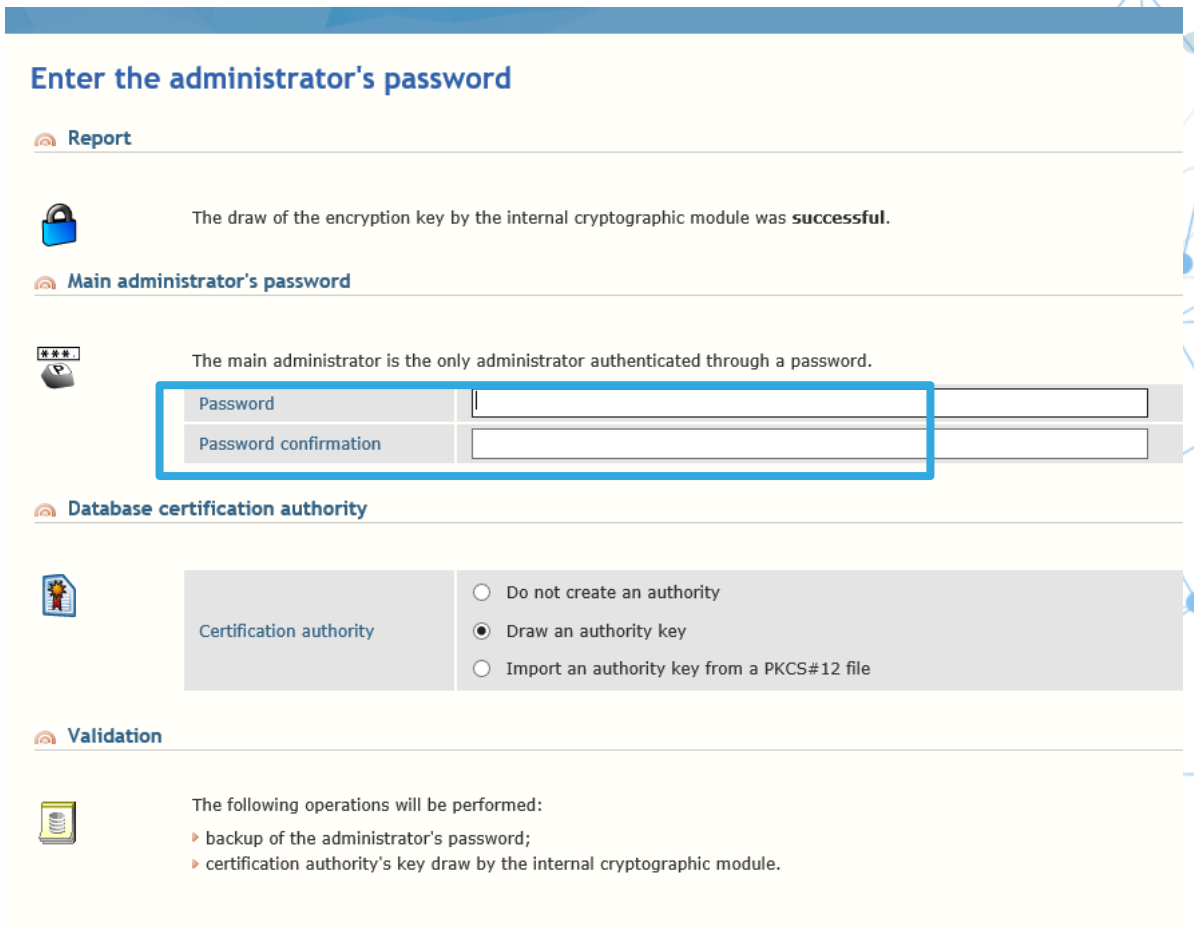
Click on **Initialize**

Option: initializing the Child CA (continued)



Option: initializing the Child CA (continued)

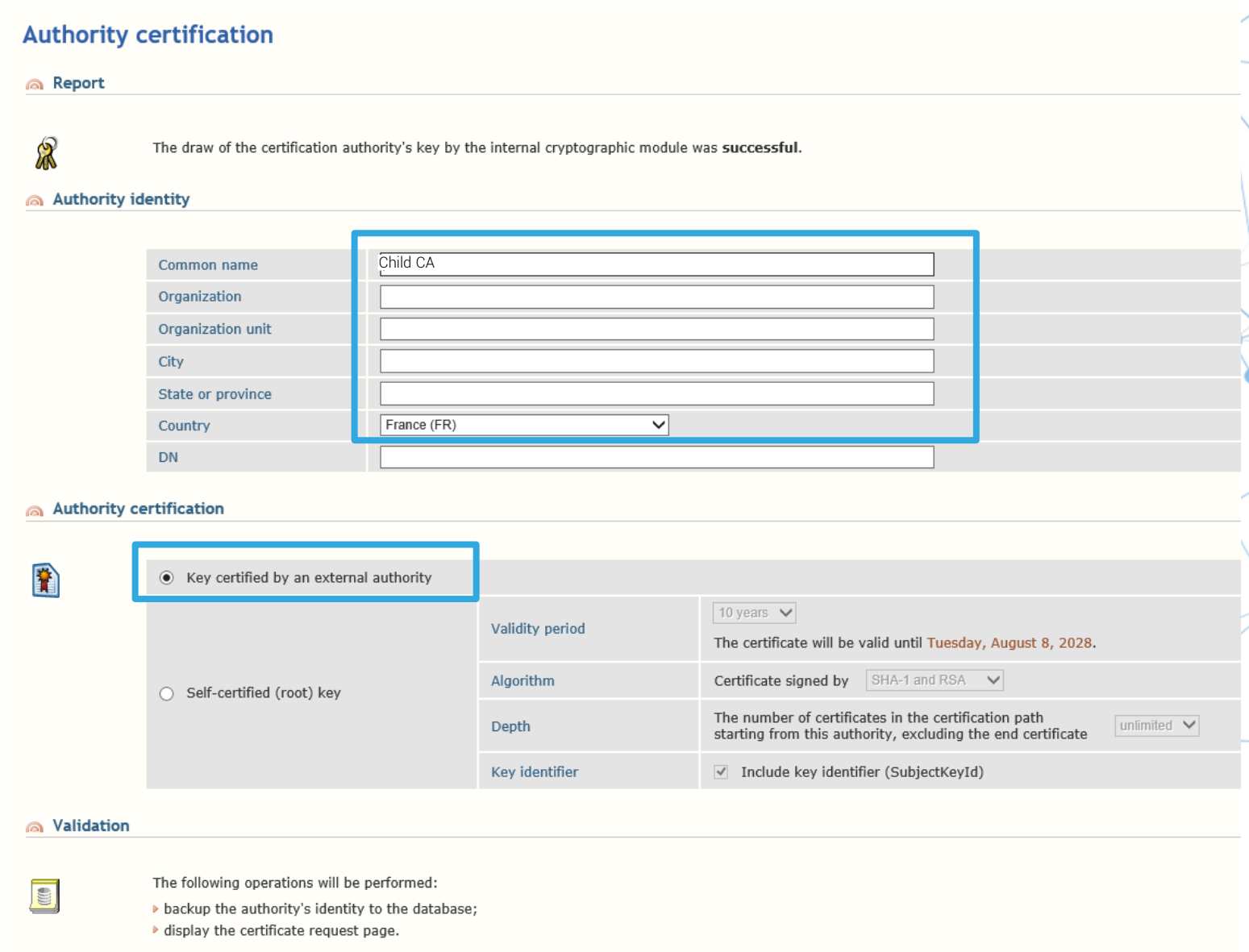




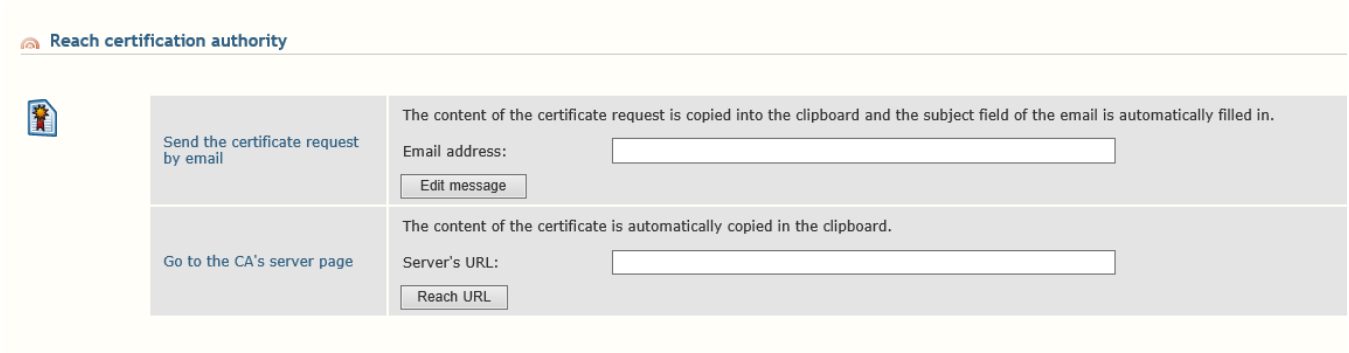
Click on **Proceed**

Option: initializing the Child CA (continued)

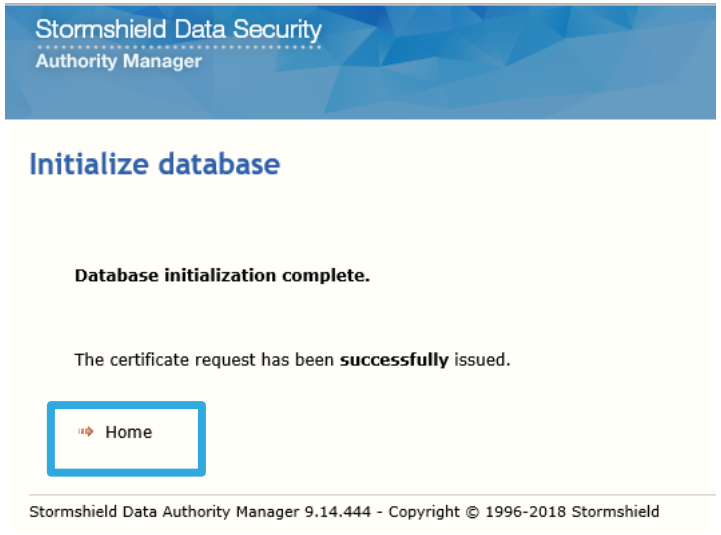
Click on **Proceed**



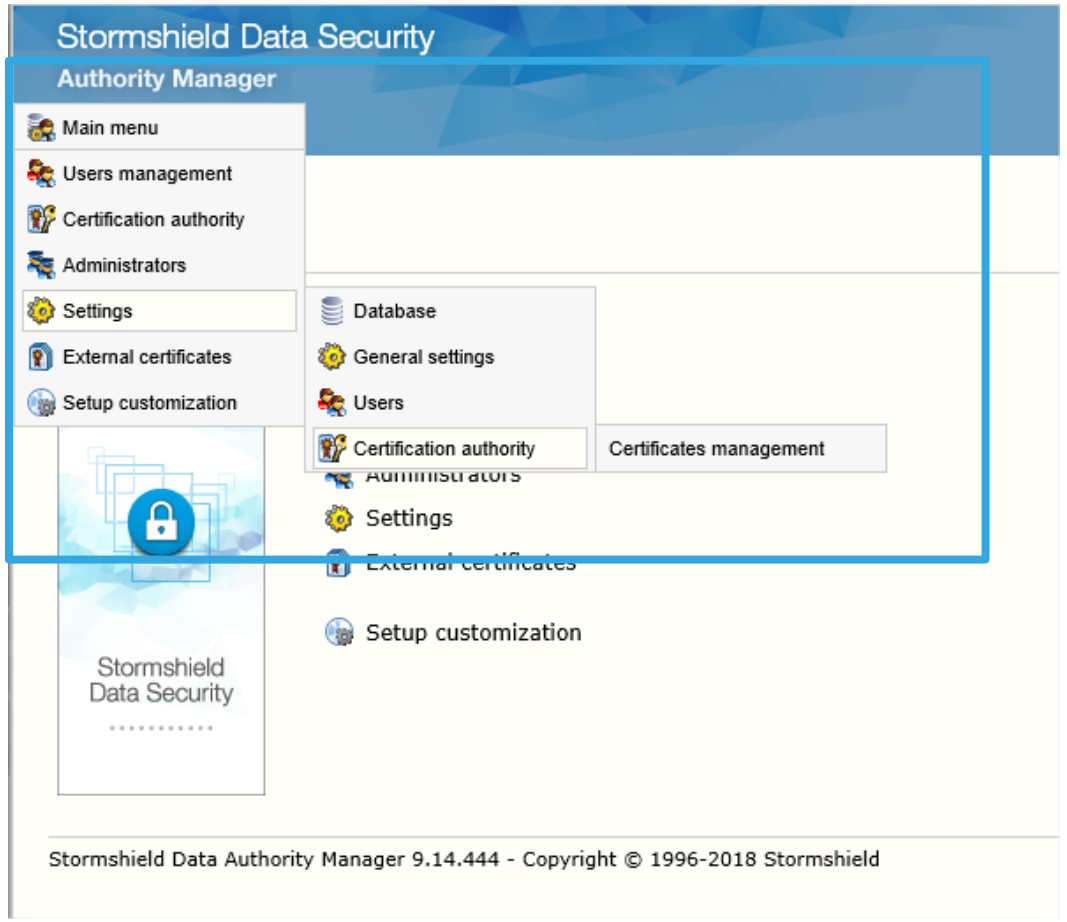
Option: initializing the Child CA (continued)



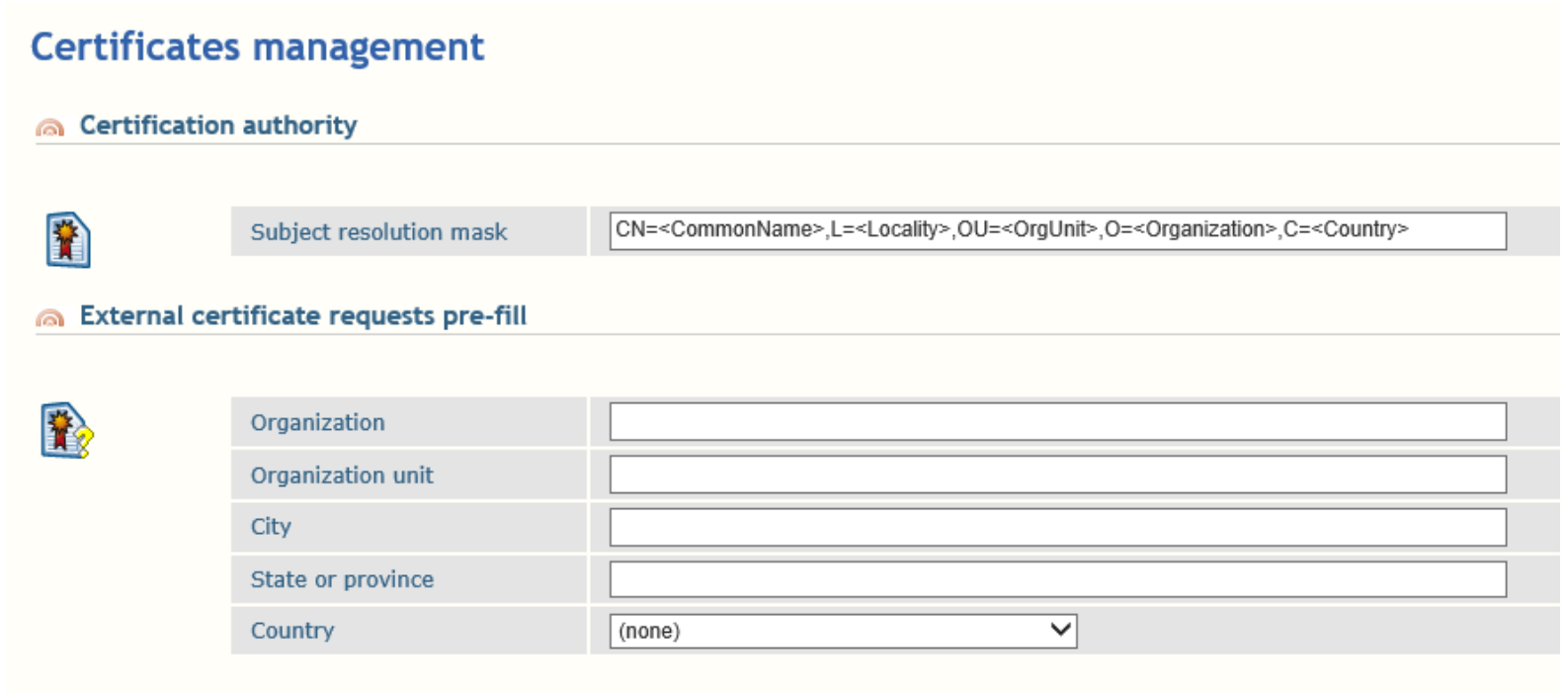
Click on **Request processed**



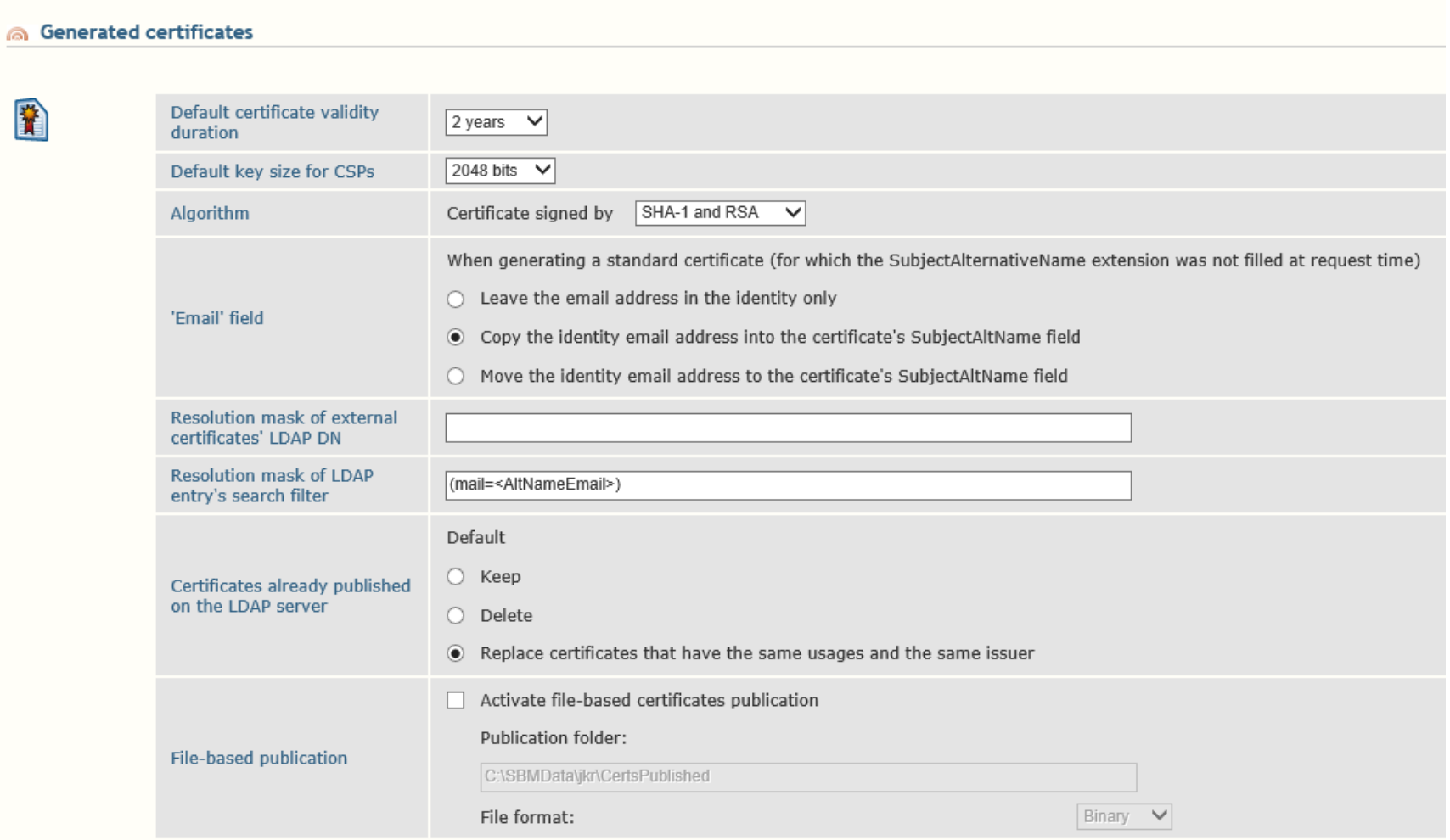
Option: configuring the Child CA CRL



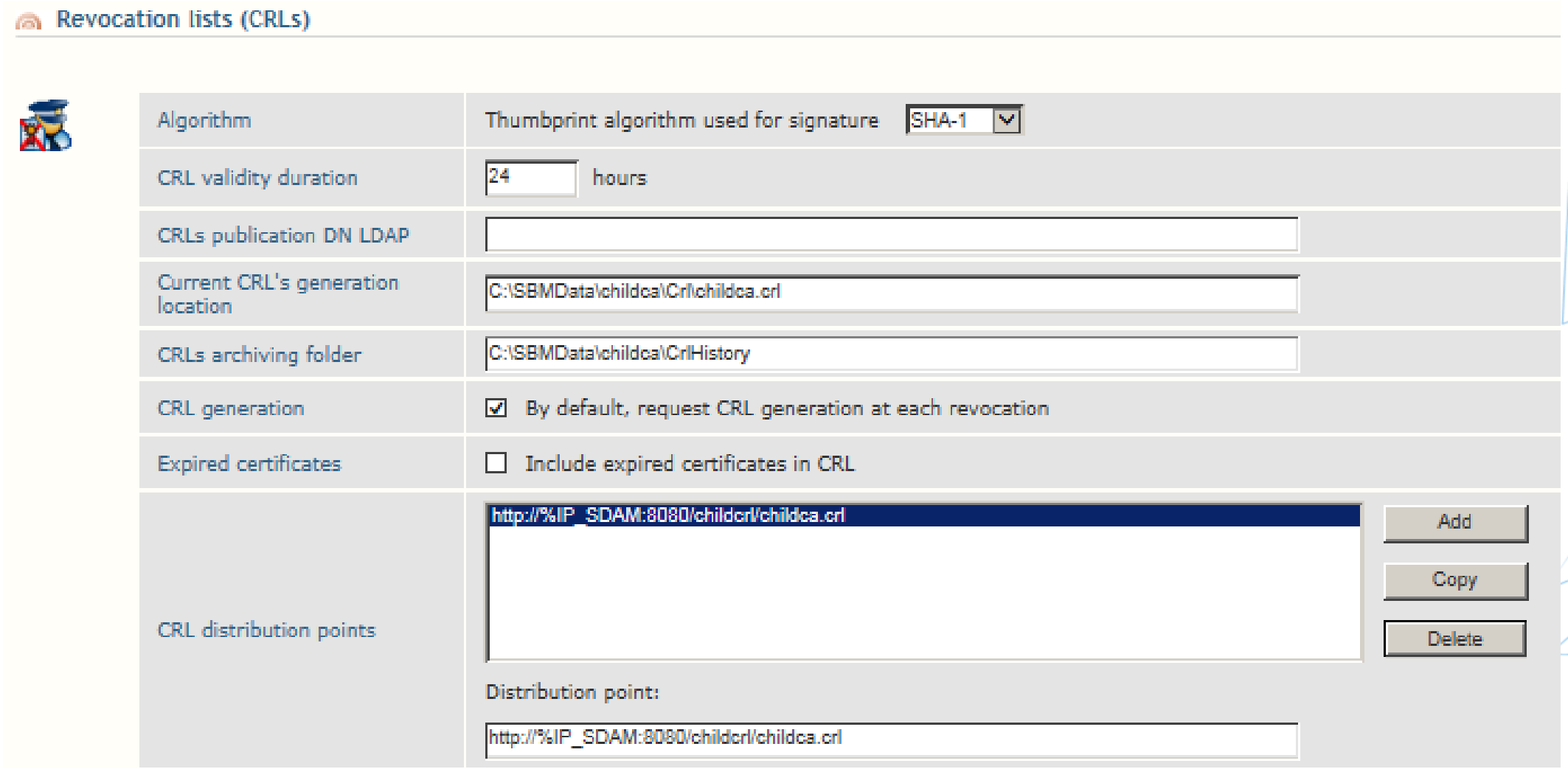
Option: configuring the Child CA CRL (continued)



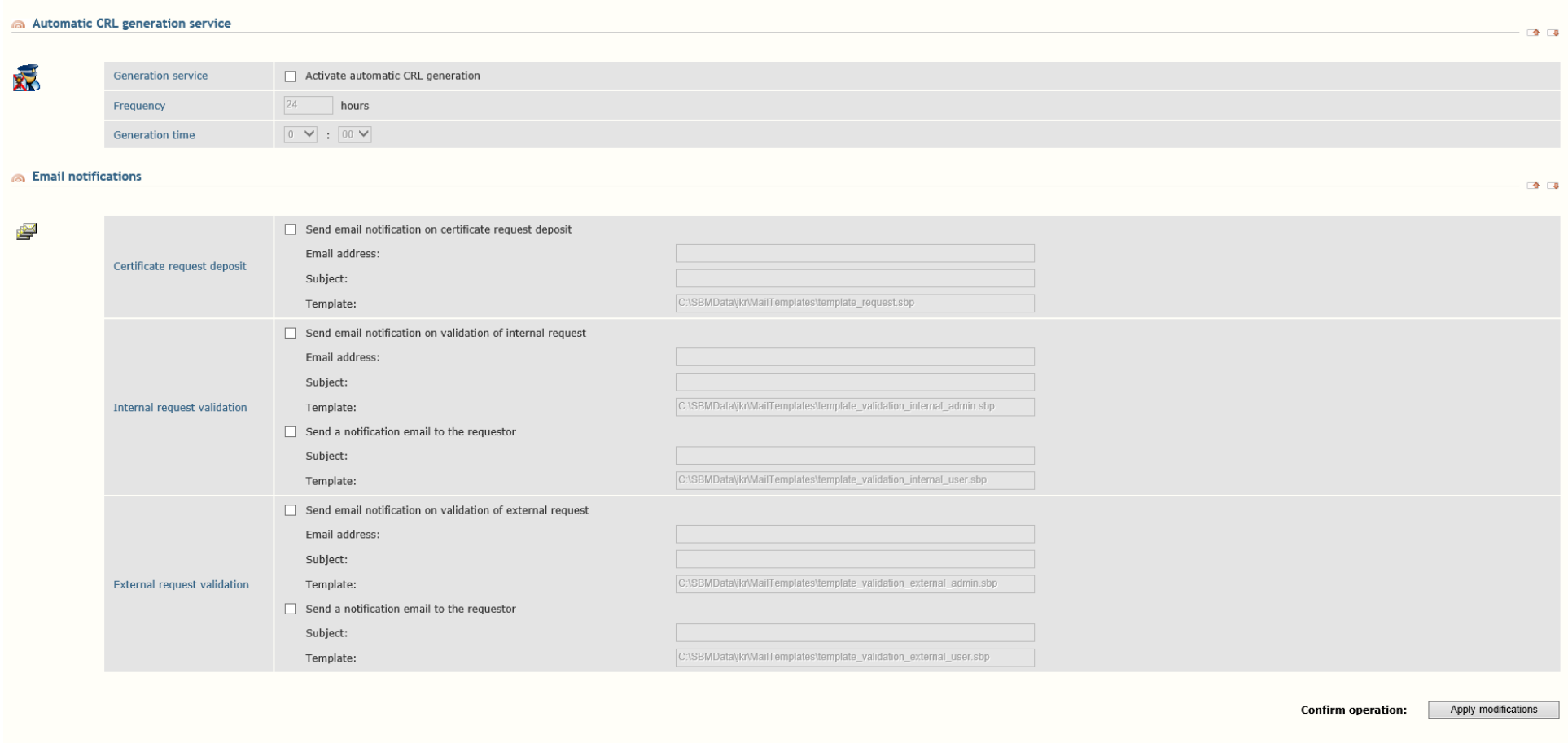
Option: configuring the Child CA CRL (continued)



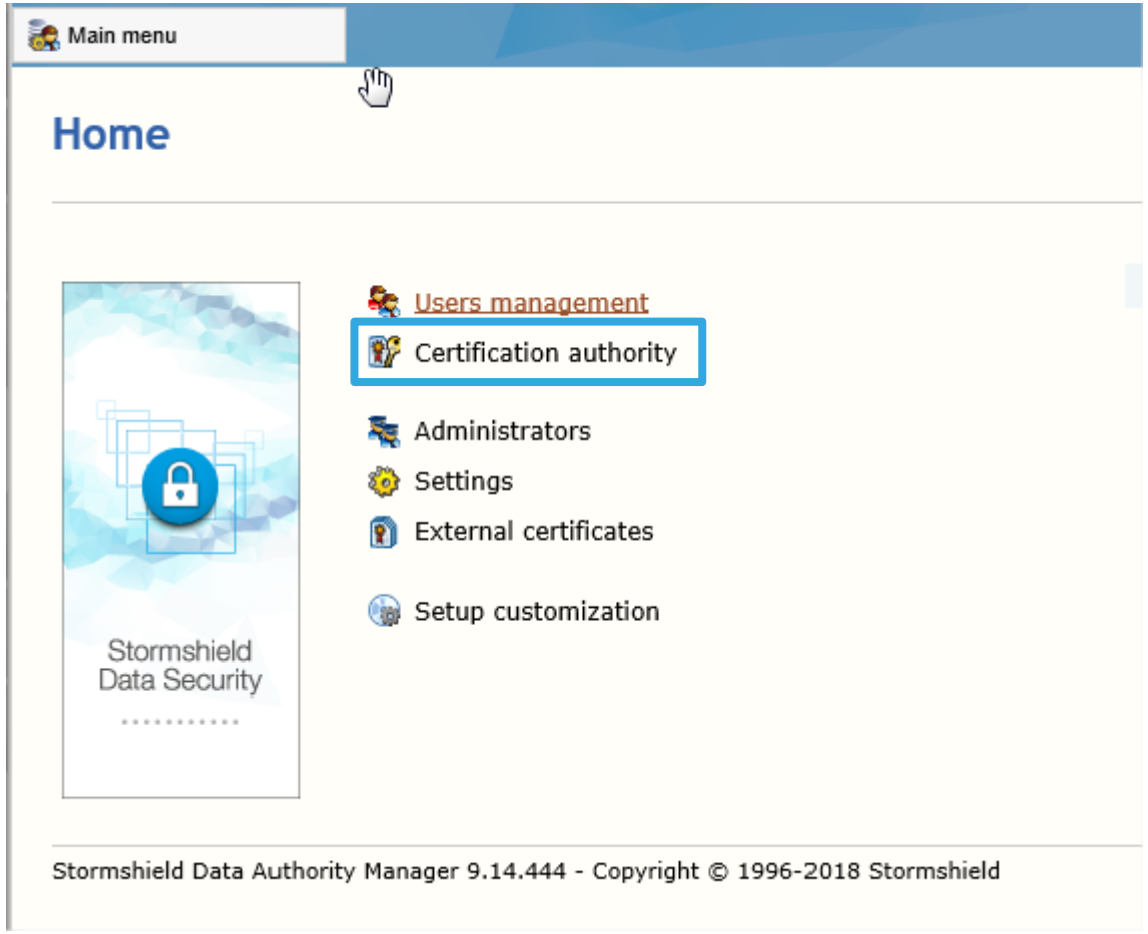
Option: configuring the Child CA CRL (continued)

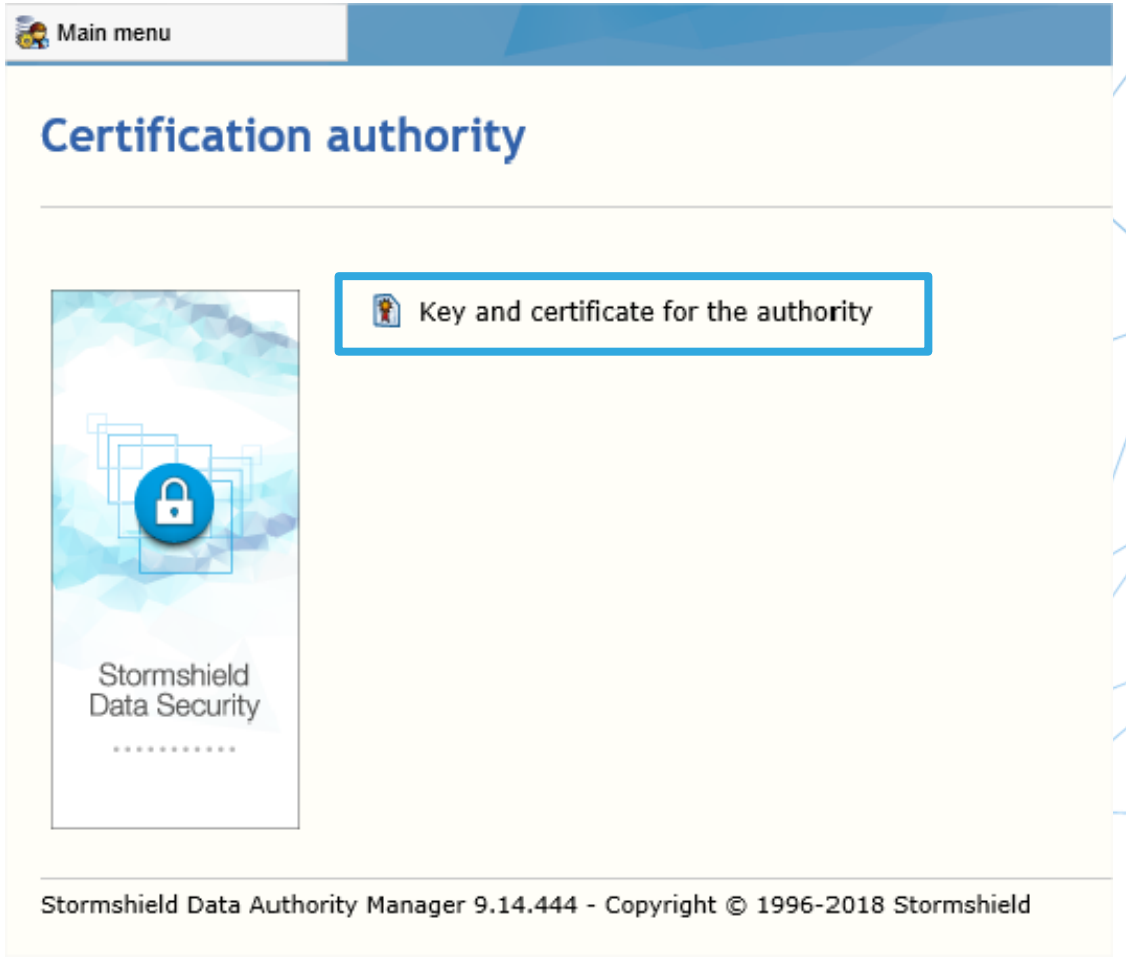


Option: configuring the Child CA CRL (continued)

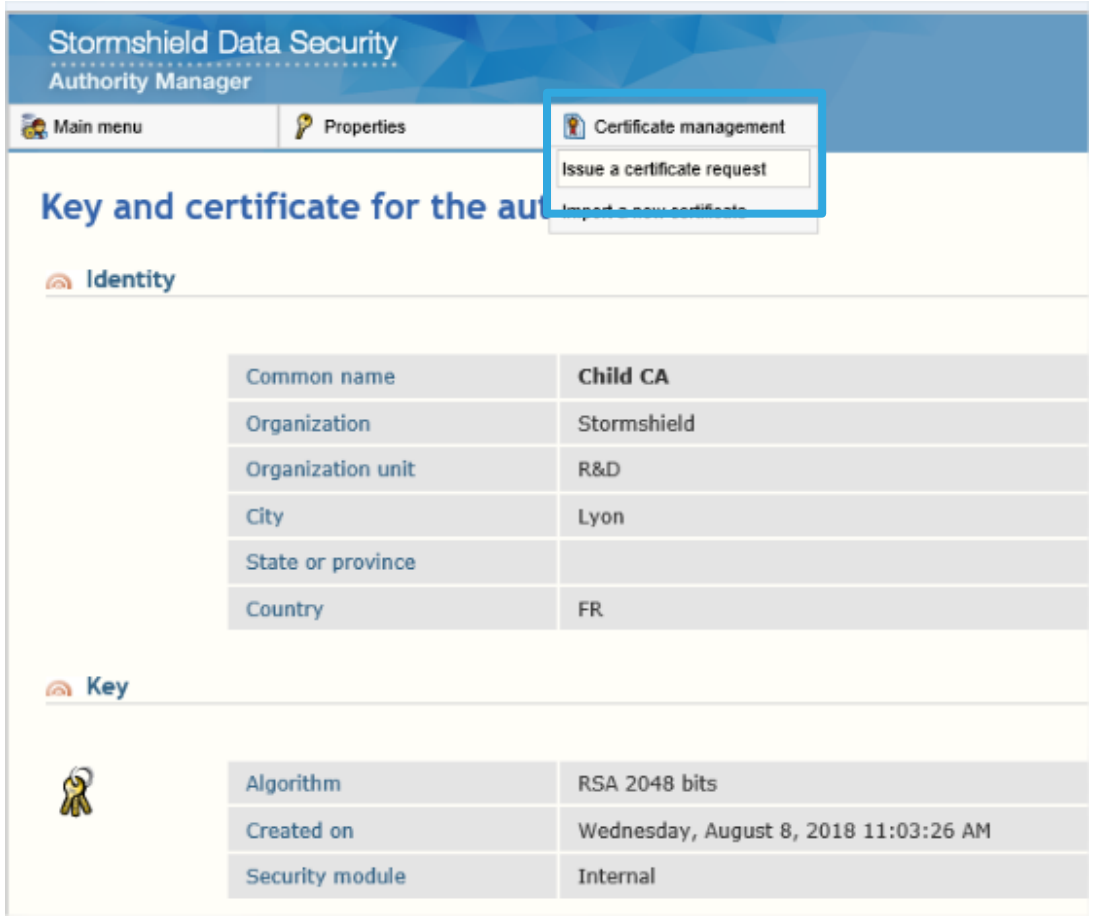


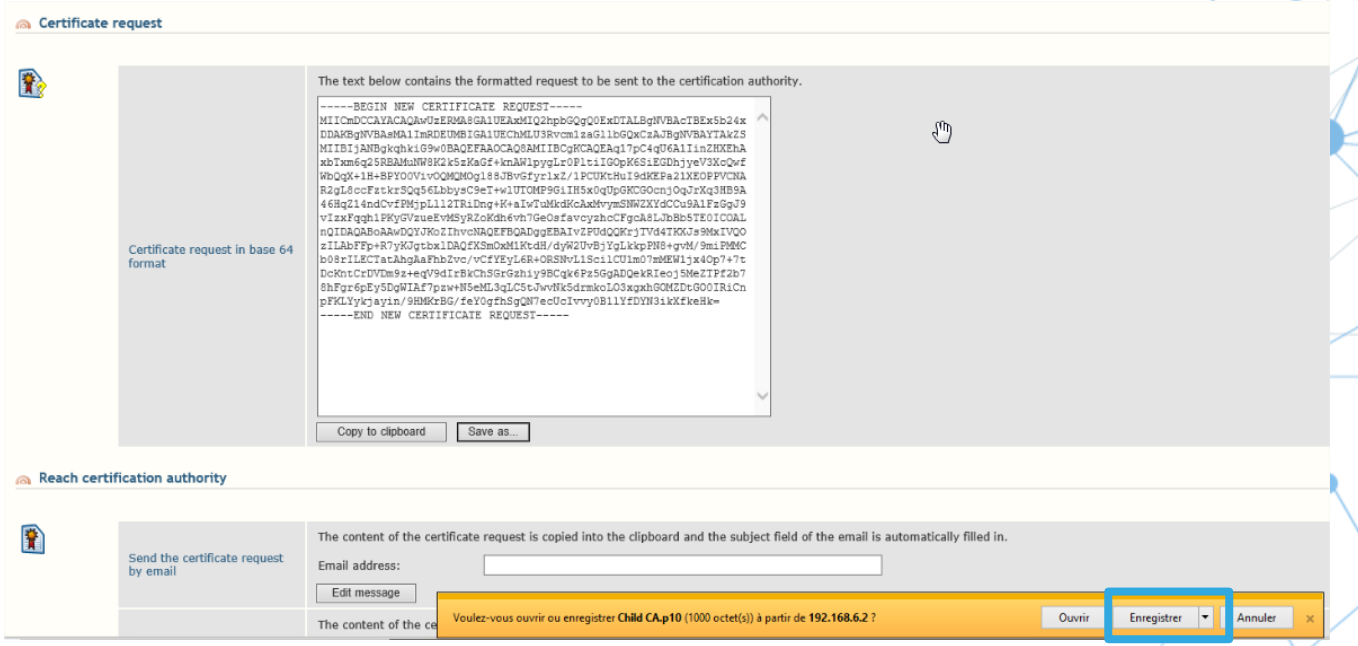
Option: validating the Child CA





Option: validating the Child CA (continued)

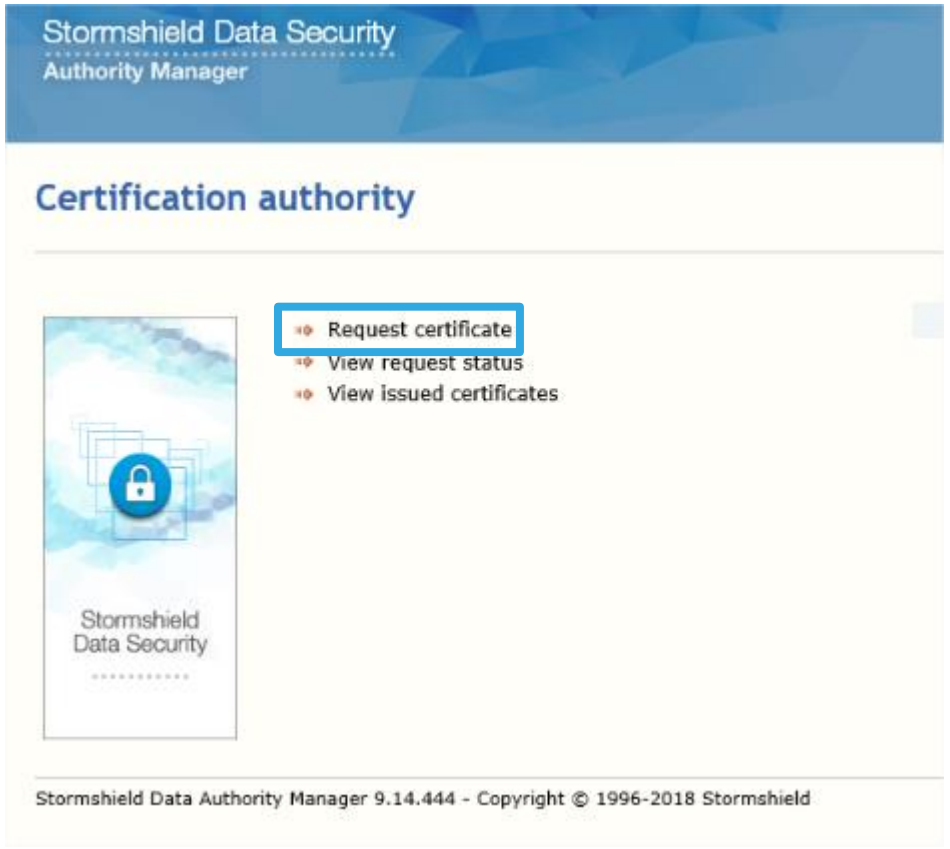




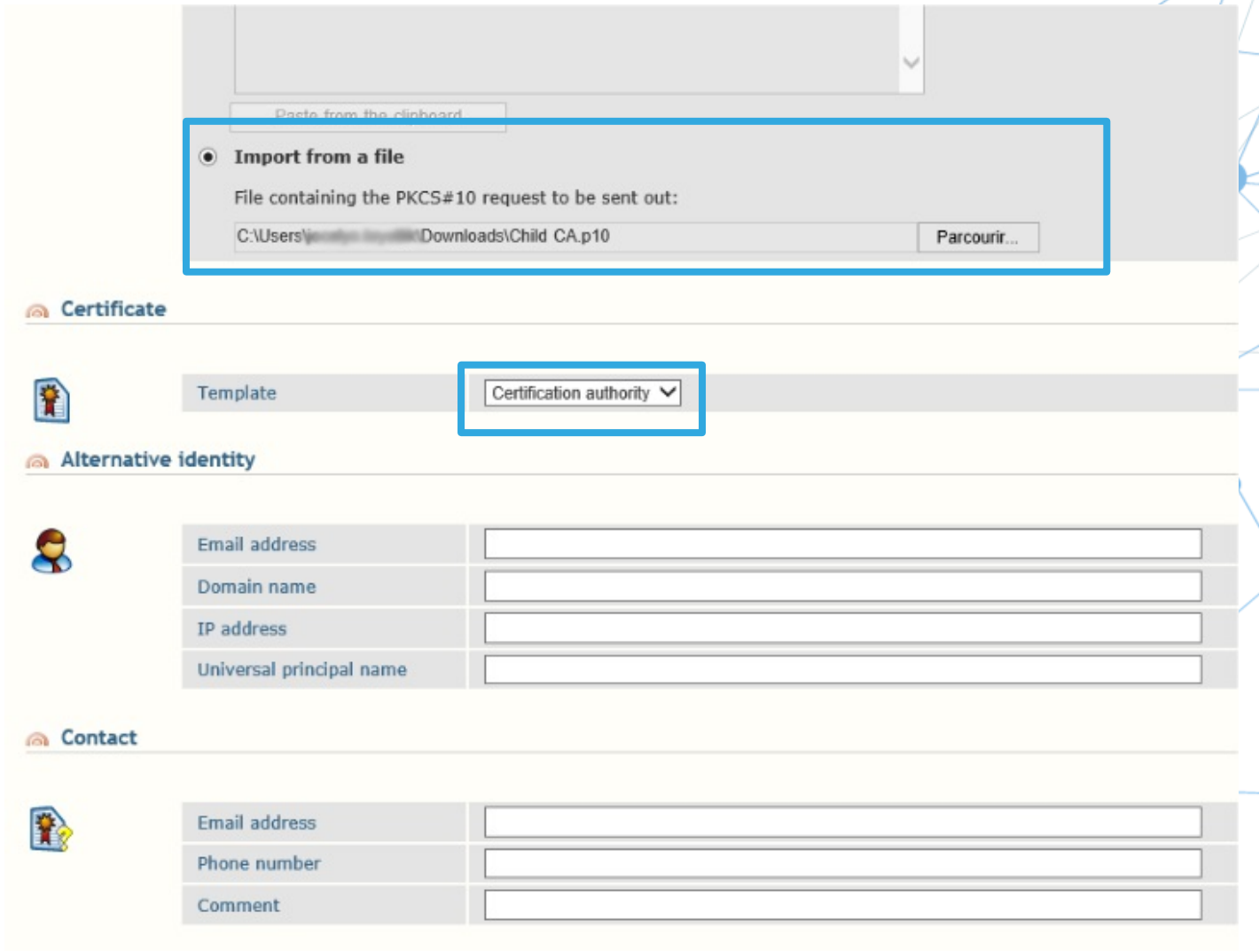
Click on **Save**

Option: validating the Child CA (continued)

- To ask for a certificate, go to the following web page: *http://%IP_SDAM:8080/bin/manager.exe/PkiIndex?baseid=rootca*



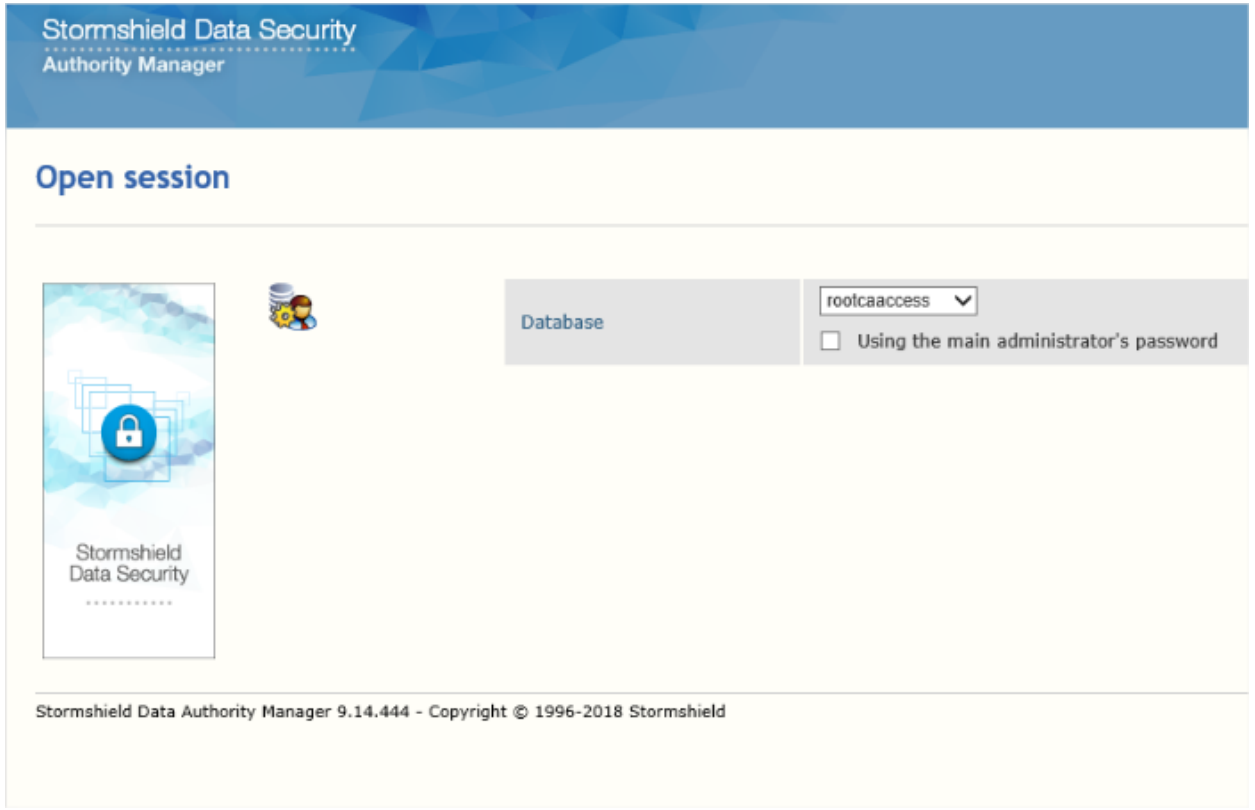
Option: validating the Child CA (continued)

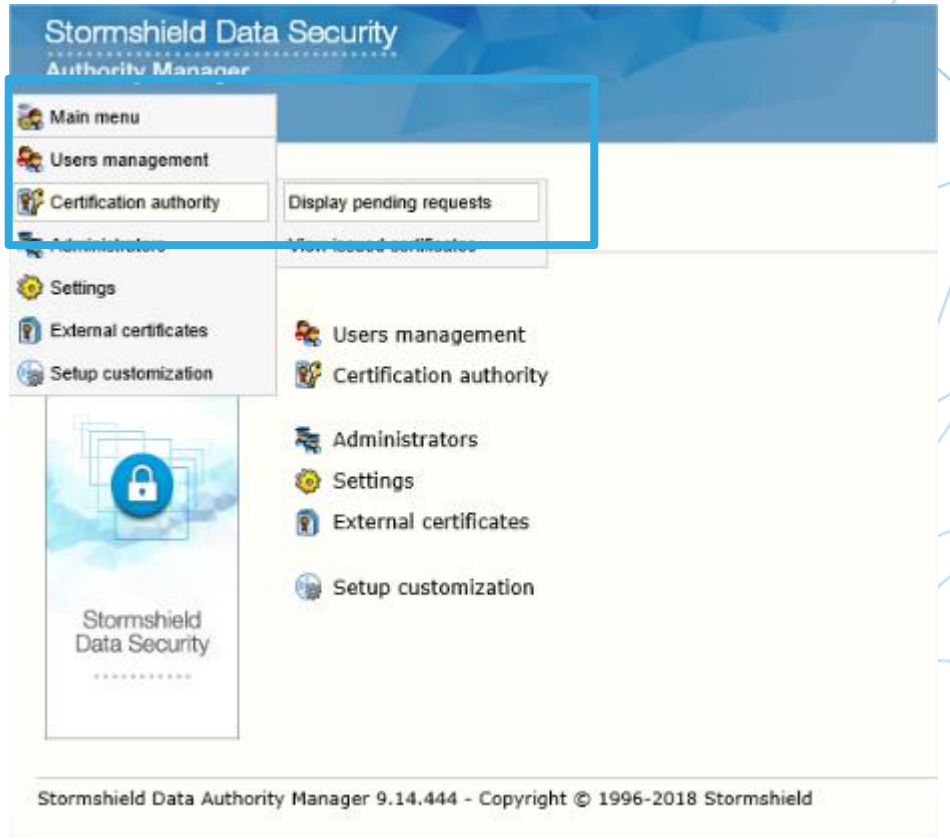


Click on **Send request**

Option: validating the Child CA (continued)

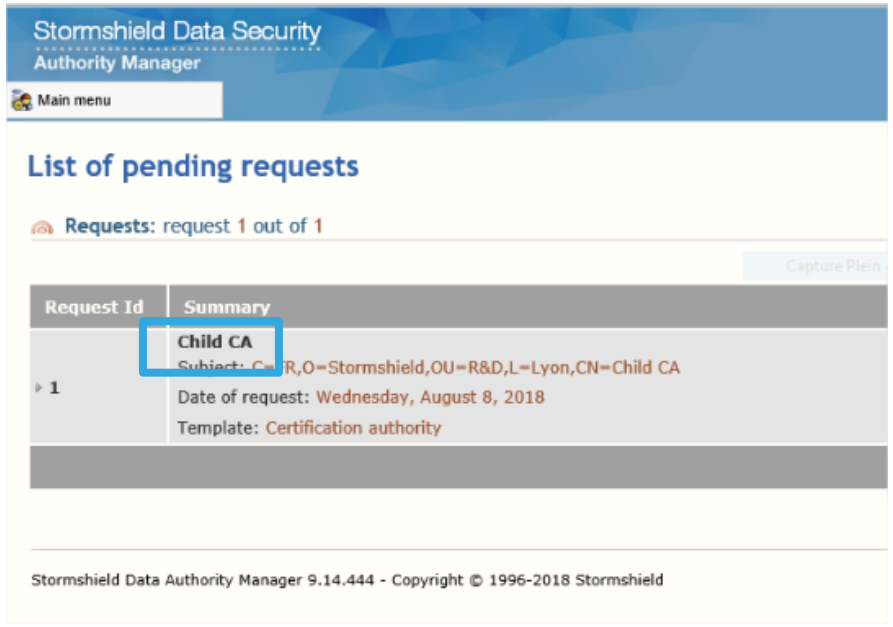
- Connect to the RootCA on the following web page and select the base: *http://%IP_SDAM:8080/bin/manager.exe/OpenSession*

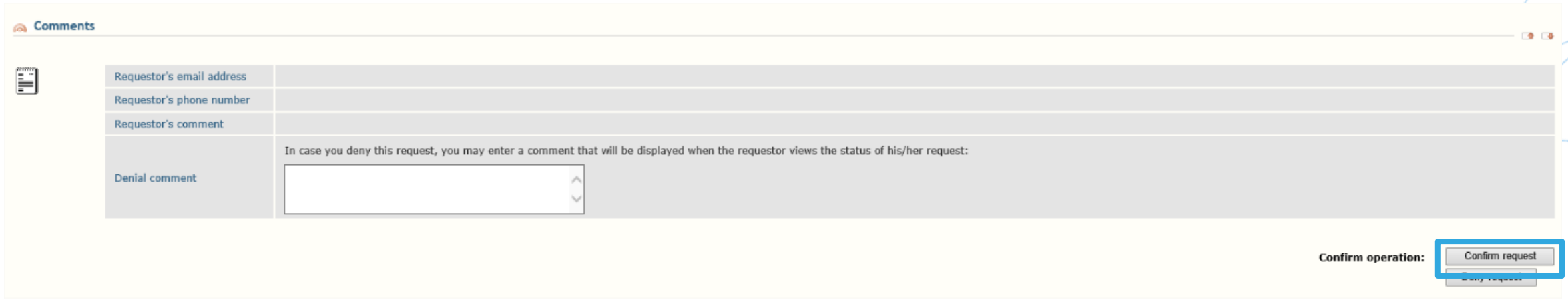




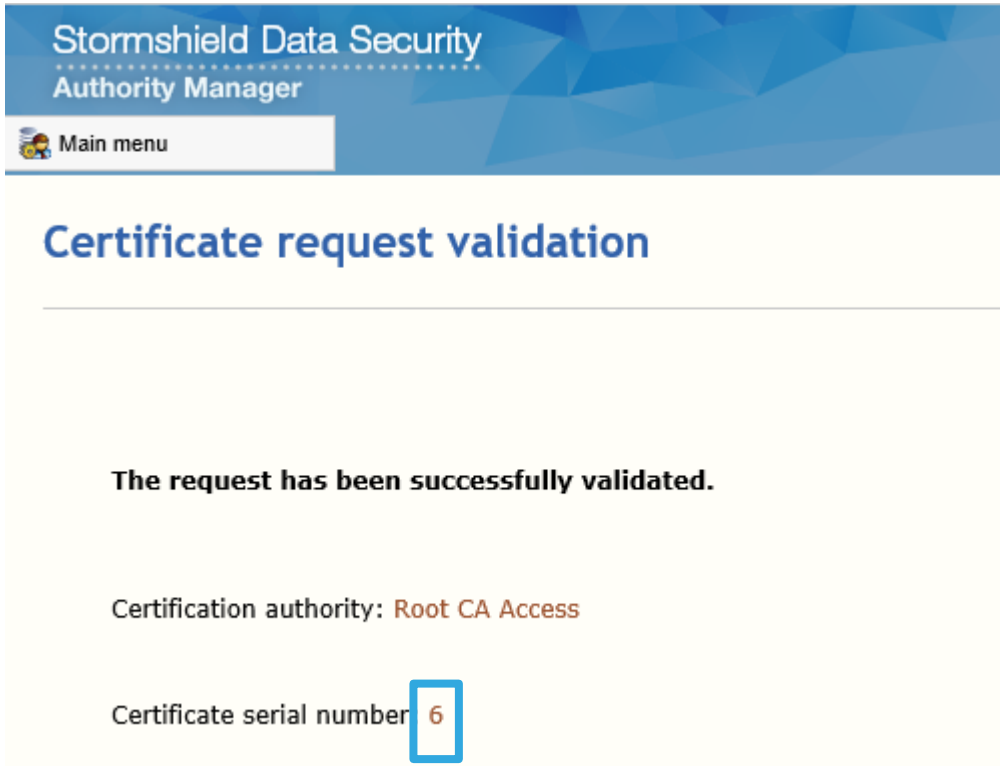
Click **Open session**

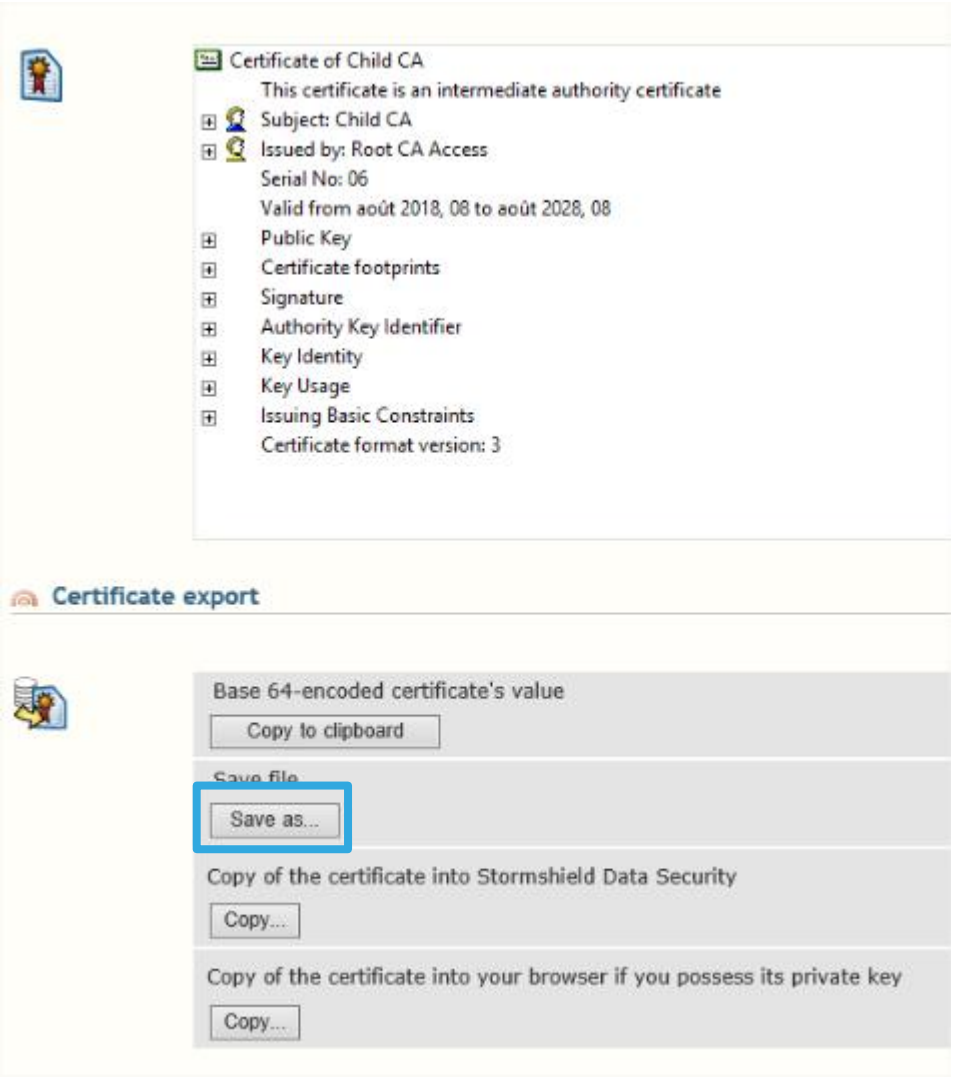
Option: validating the Child CA (continued)





Option: validating the Child CA (continued)

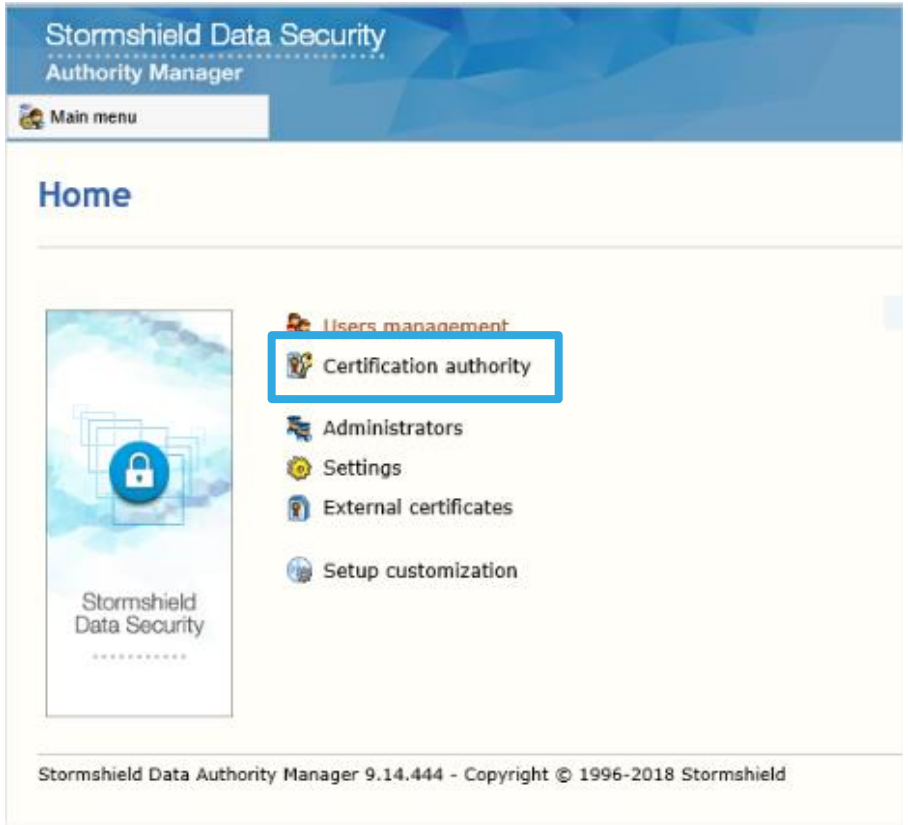




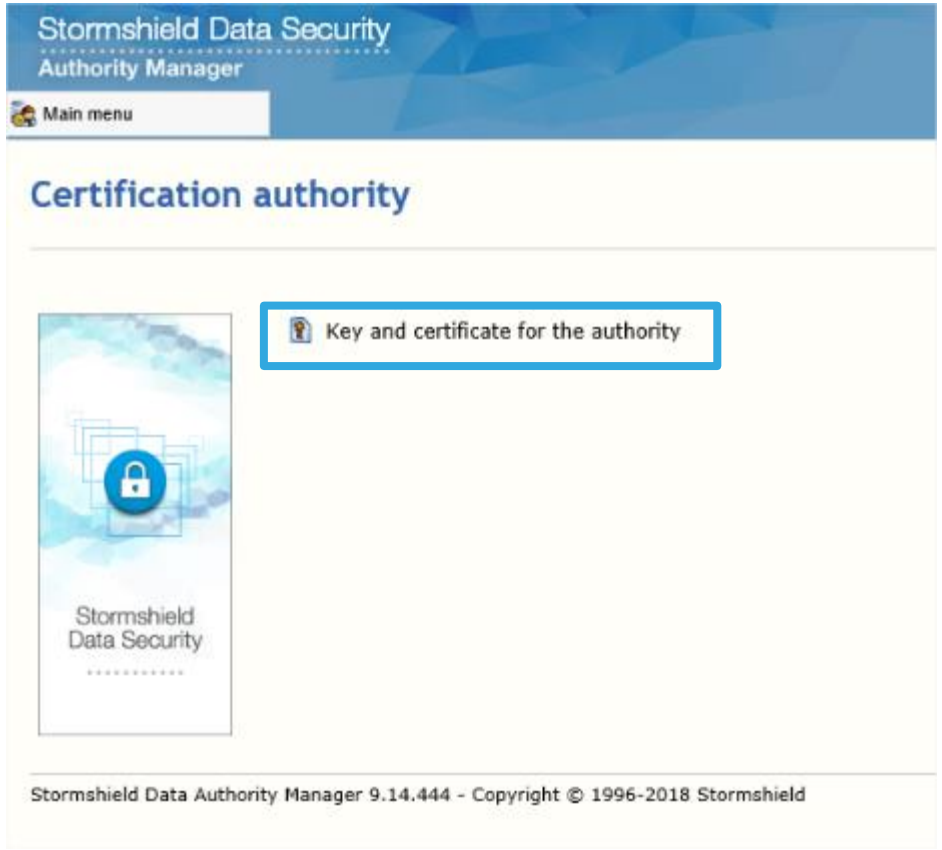
Option: validating the Child CA (continued)

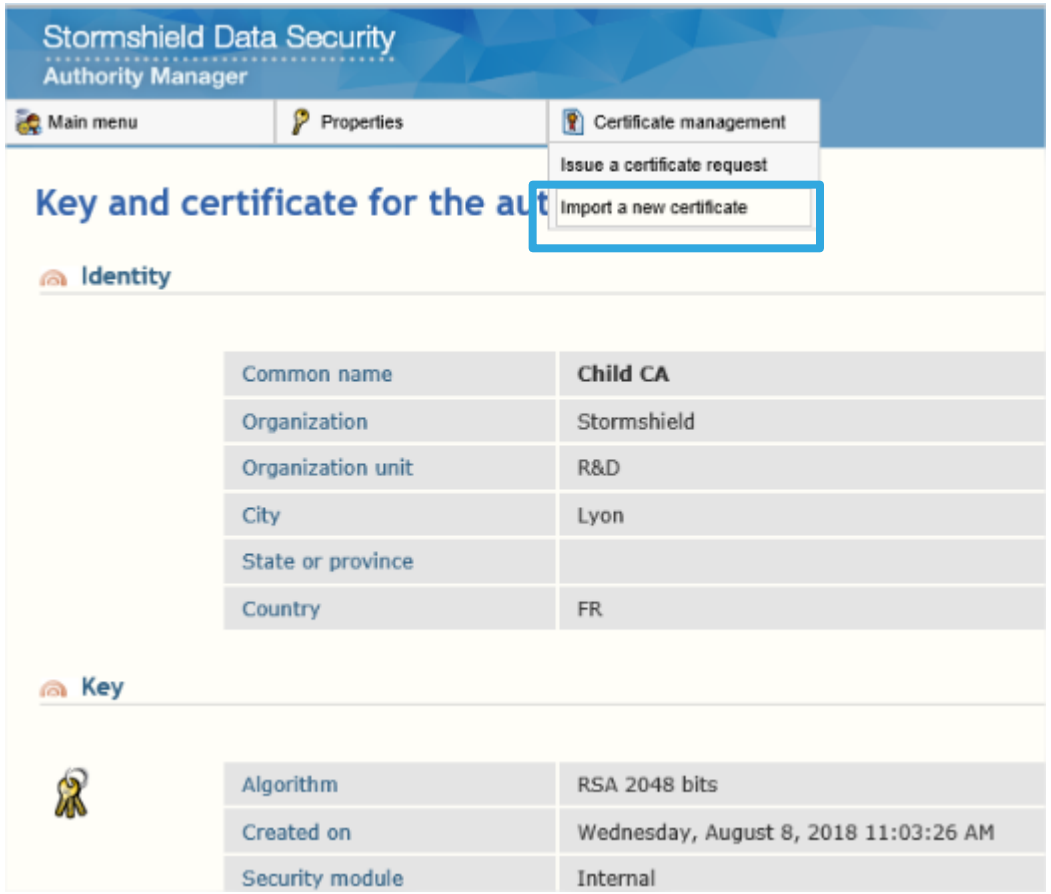
- Connect to the Child CA on the following web page and select the base:

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

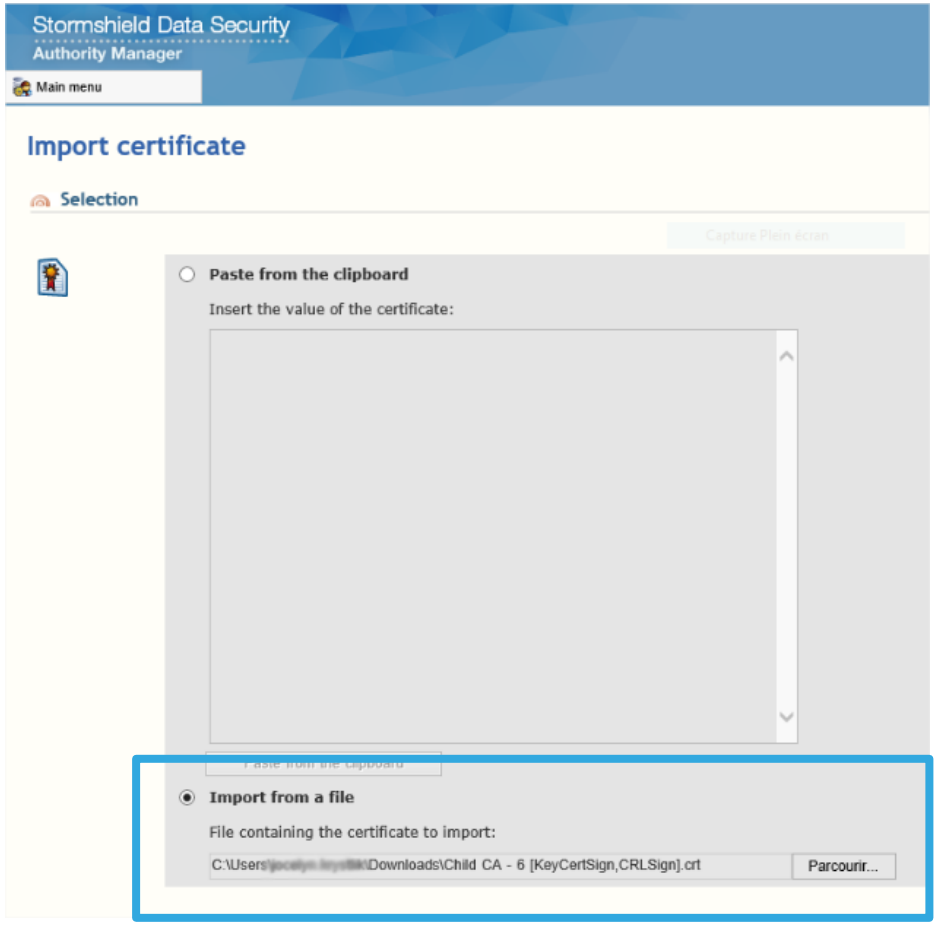


Option: validating the Child CA (continued)





Option: validating the Child CA (continued)



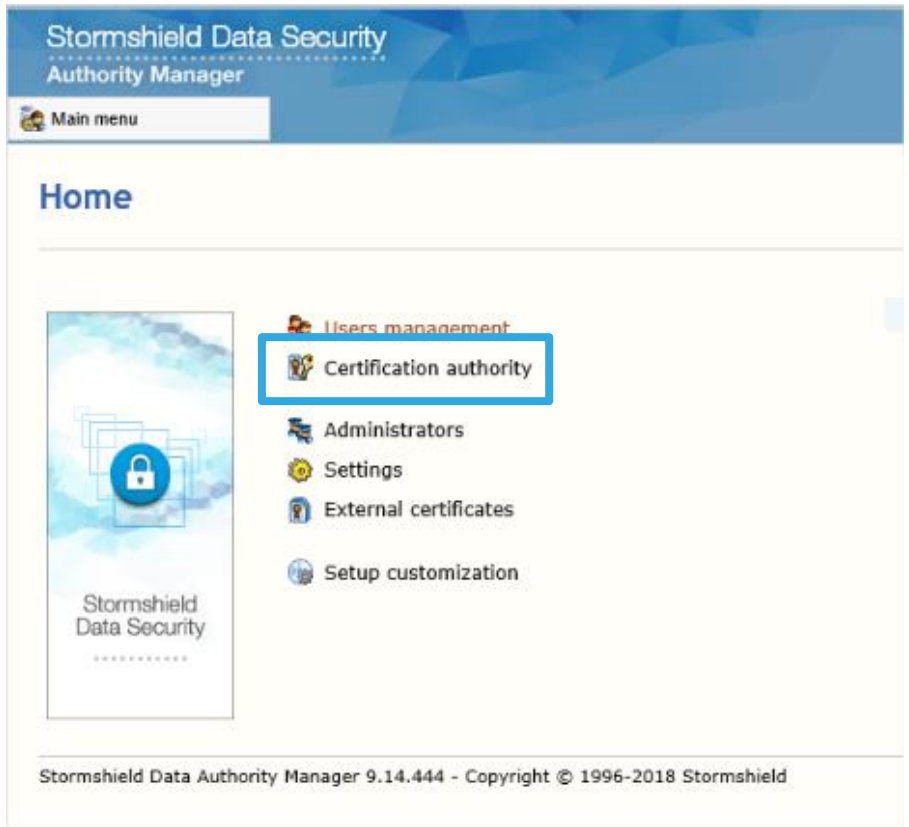
Click on **Import**

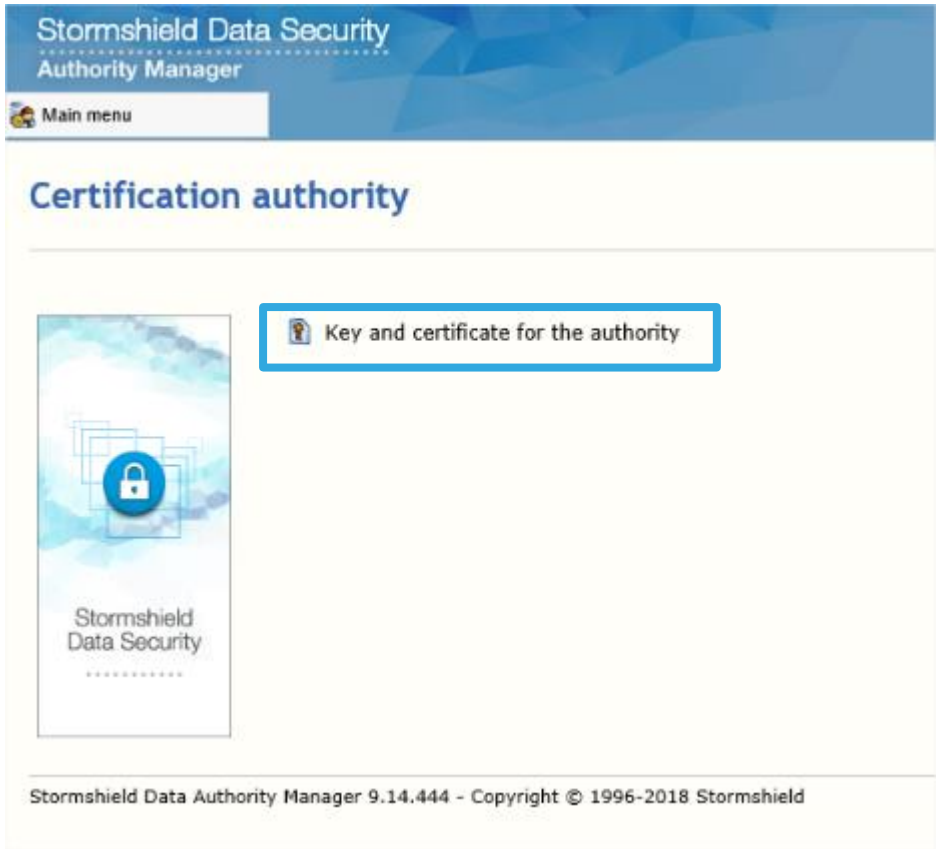
Click on **Import the certificate**

Option: validating the Child CA (continued)

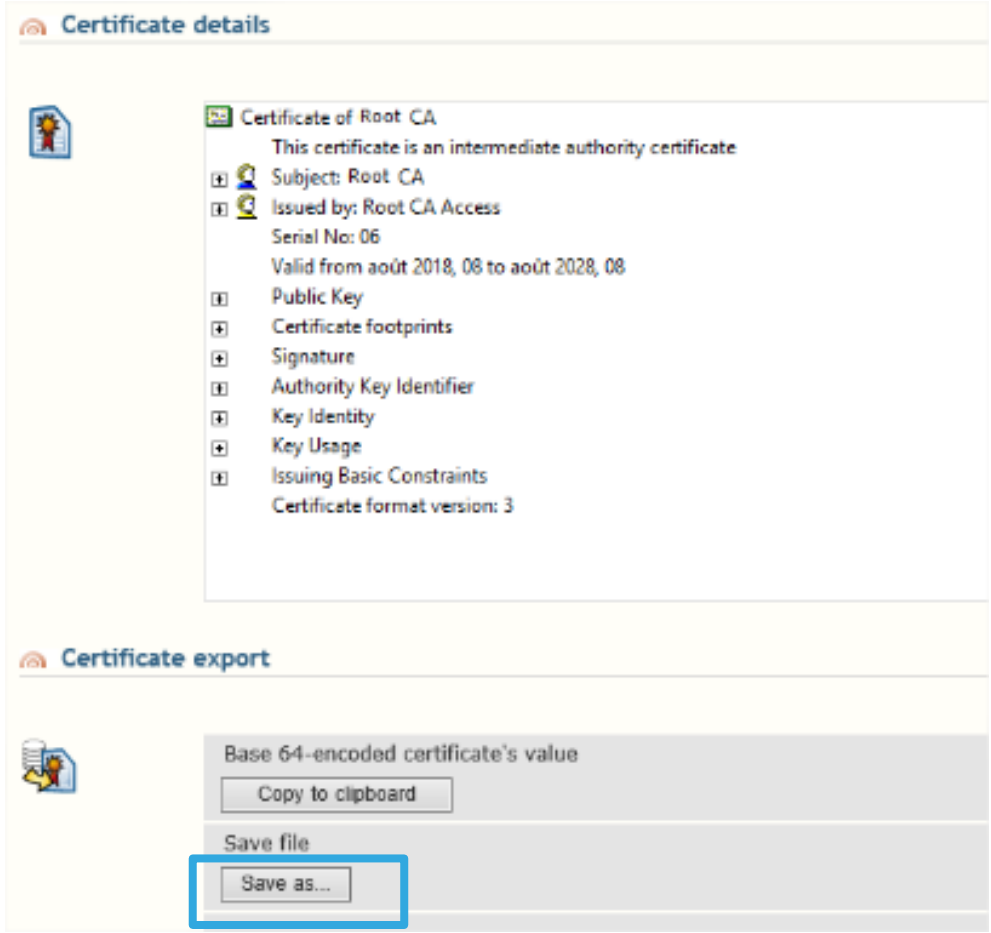
- Connect to the Root CA on the following web page and select the base:

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





Option: validating the Child CA (continued)

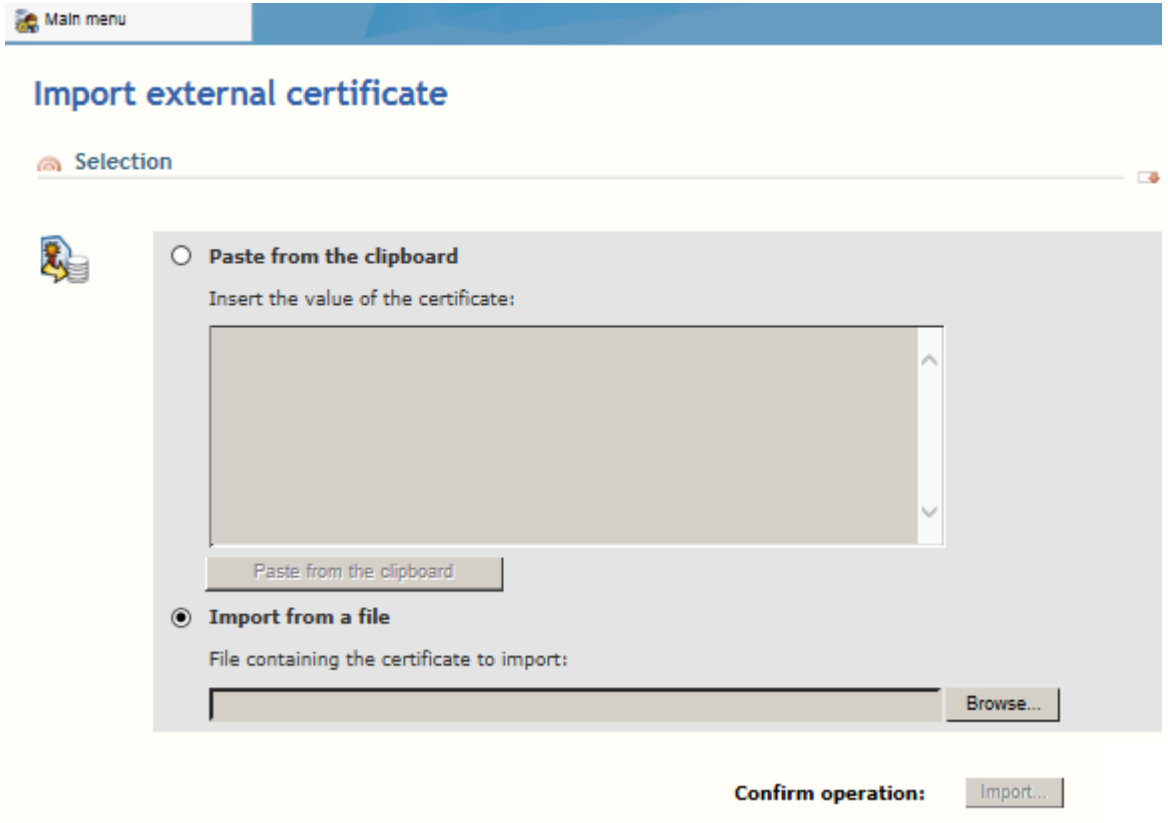


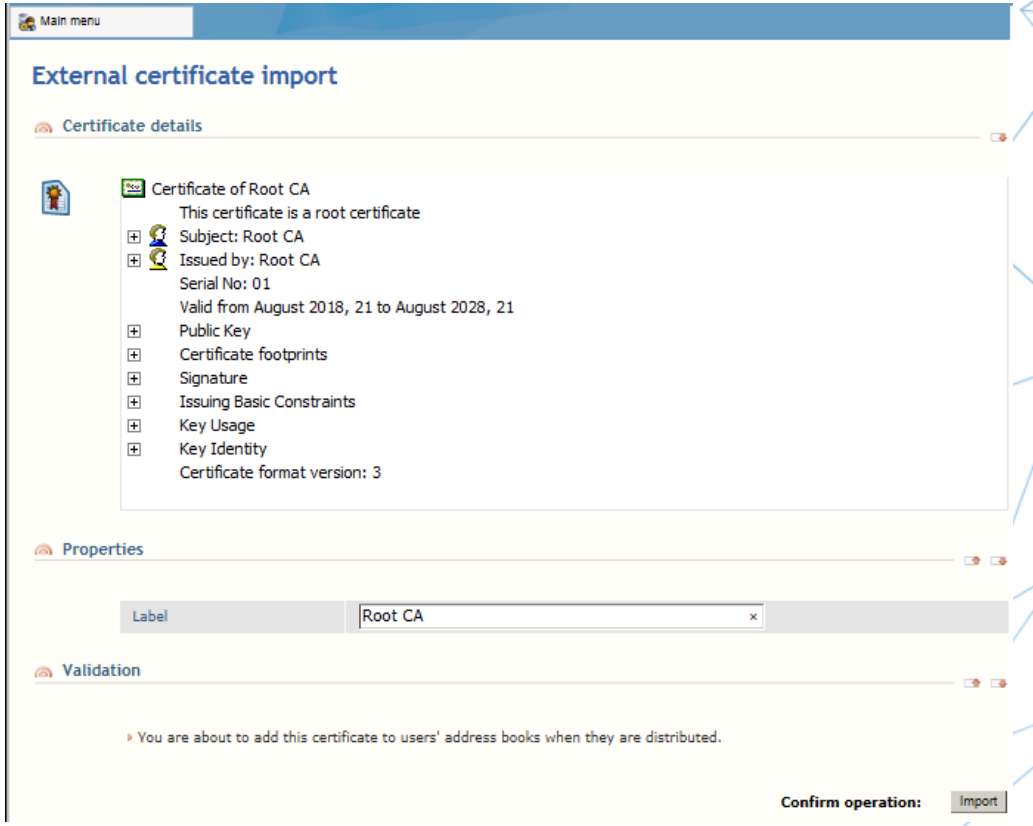
Option: validating the Child CA (continued)

- Connect to the Child CA on the following web page and select the base:

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

Option: validating the Child CA (continued)

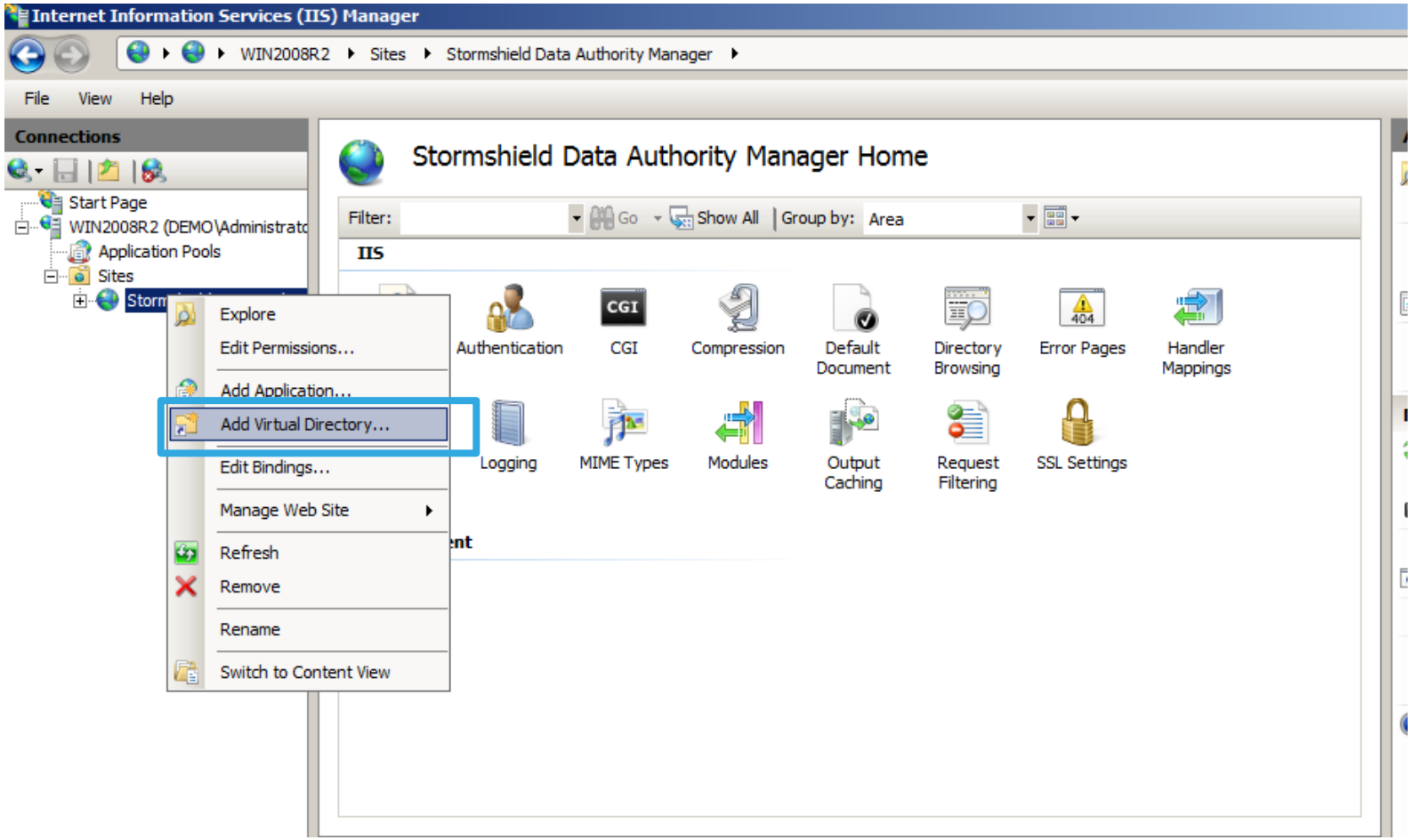


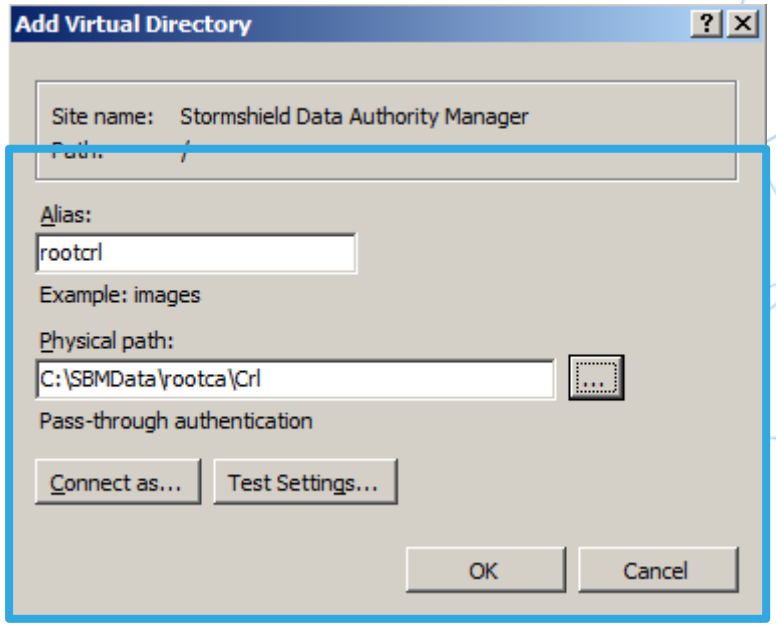


Configuring the IIS server virtual directory

Configuring the IIS server

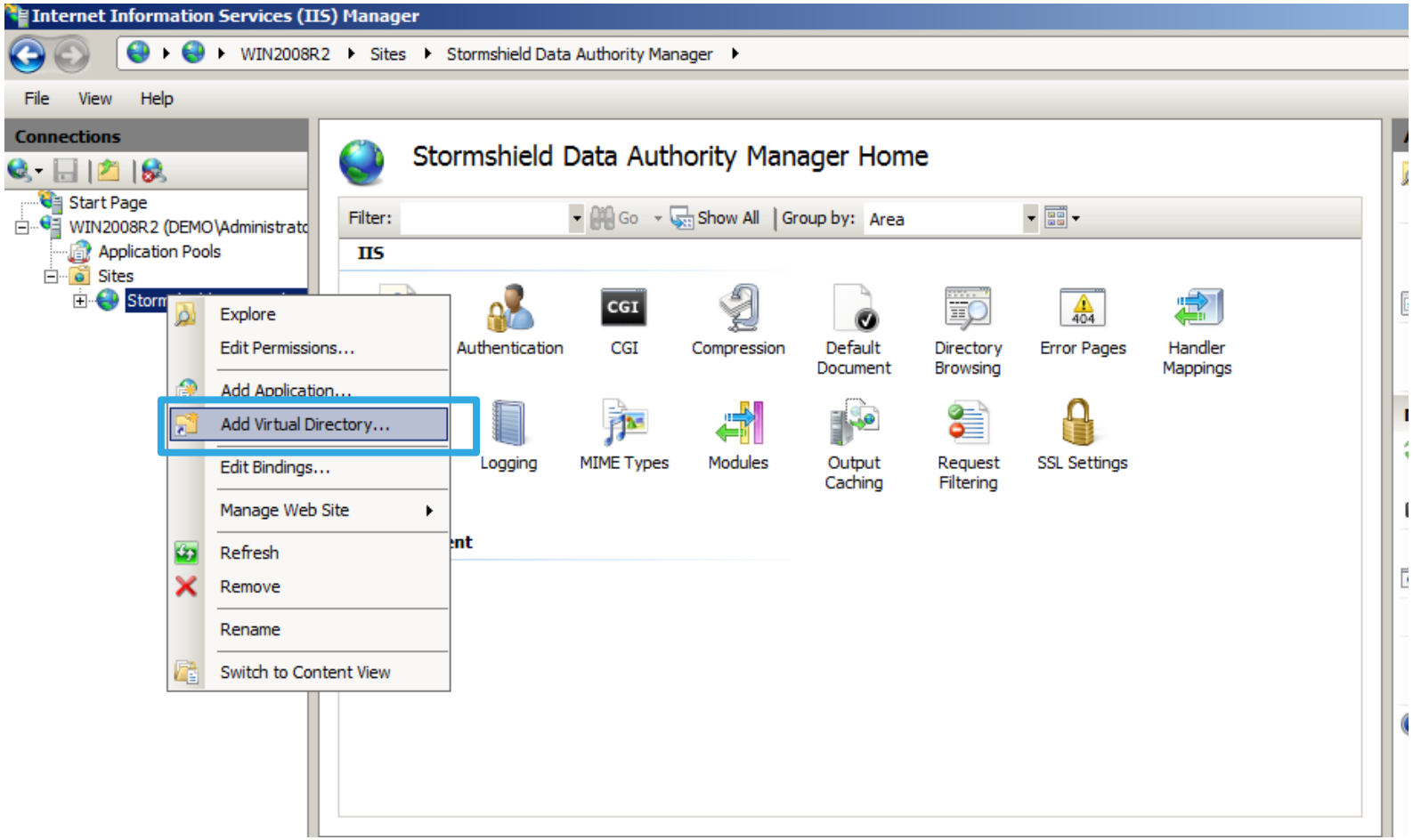
Create a virtual directory on the IIS server under the Stormshield Data Authority Manager website for the CRL service

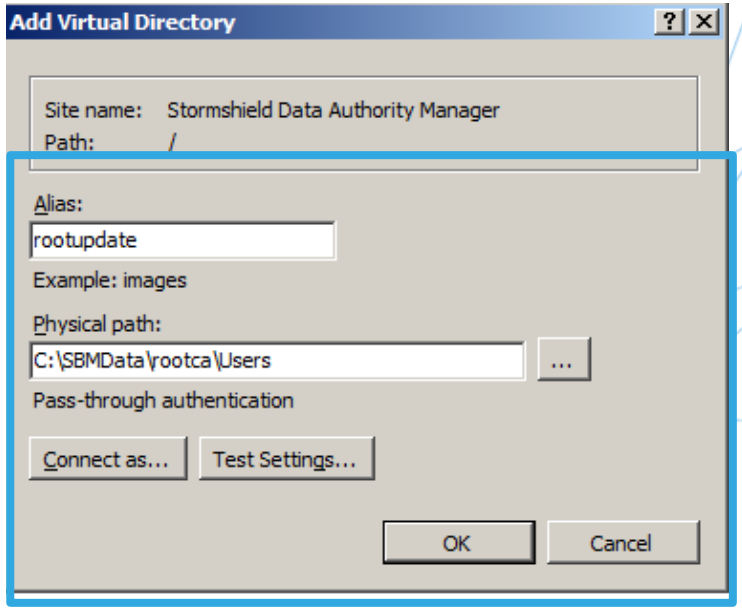




Configuring the IIS server (continued)

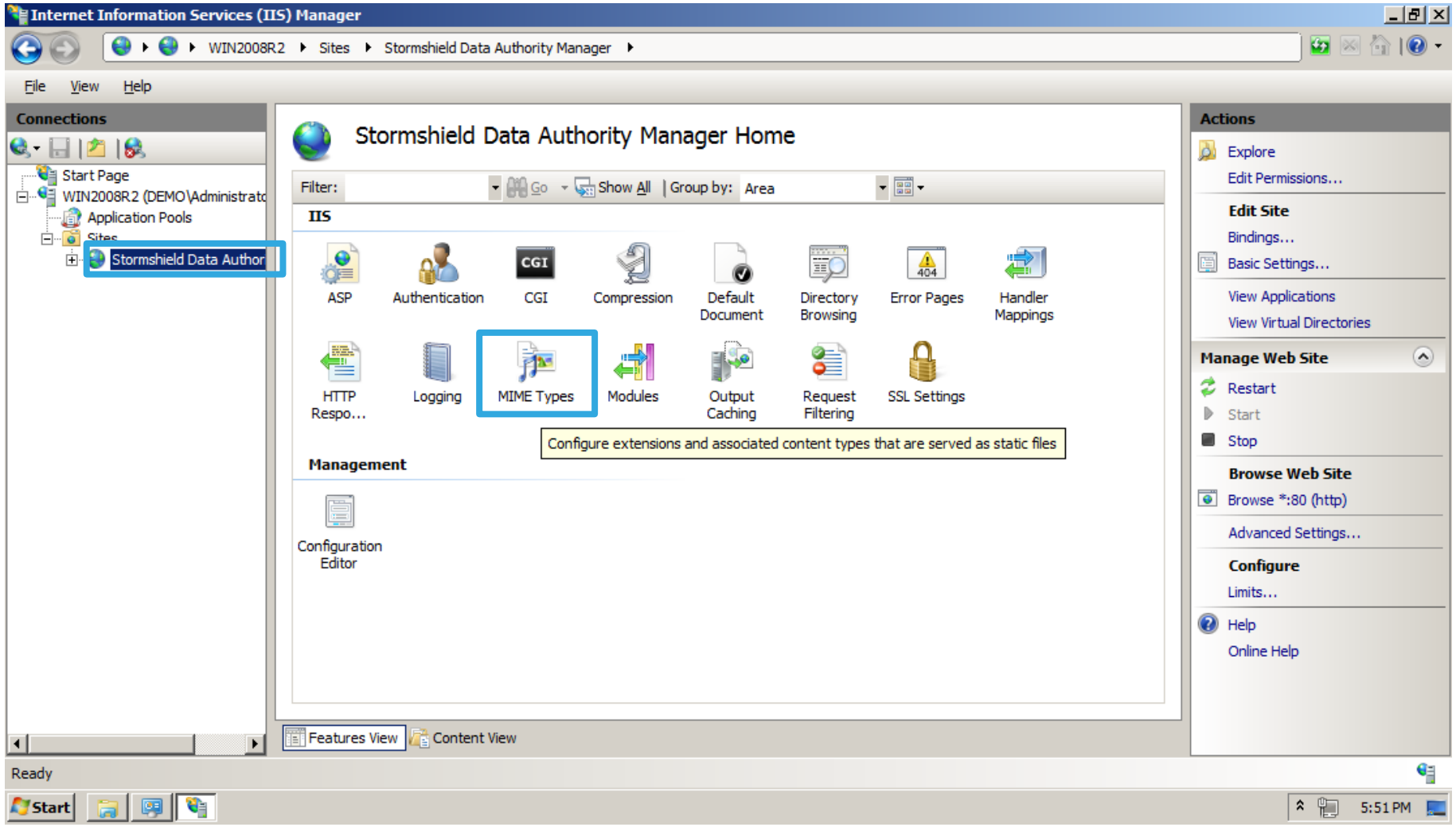
Create a virtual directory on the IIS server under the Stormshield Data Authority Manager website in order to be able to distribute update files for SDS





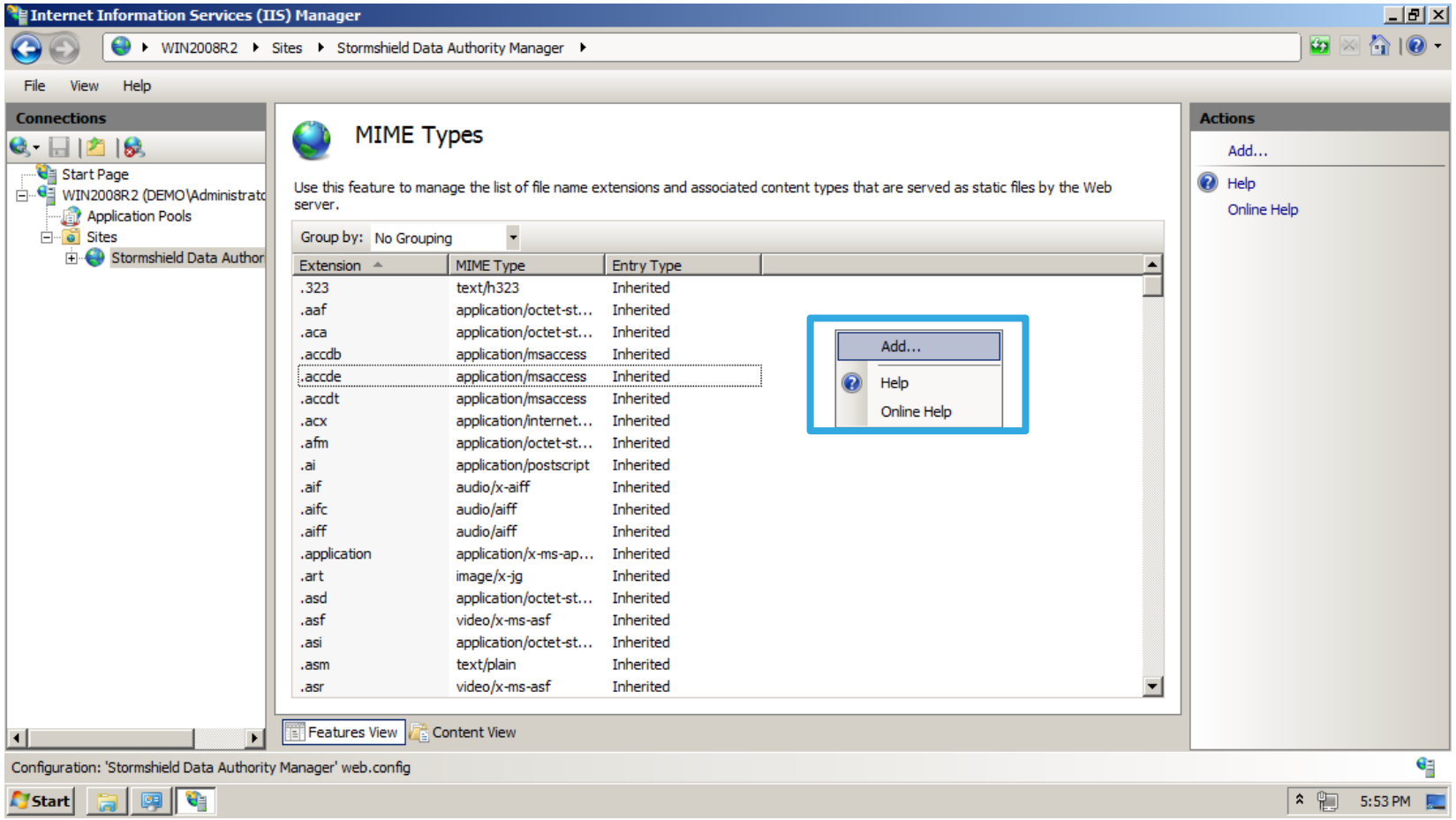
Configuring the IIS server (continued)

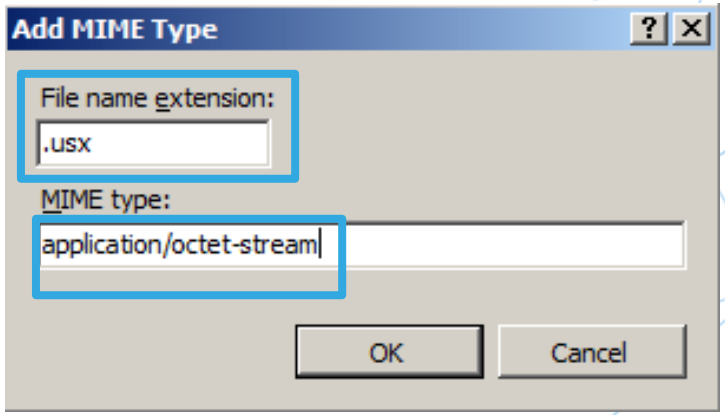
Double click on **MIME Types**



Configuring the IIS server (continued)

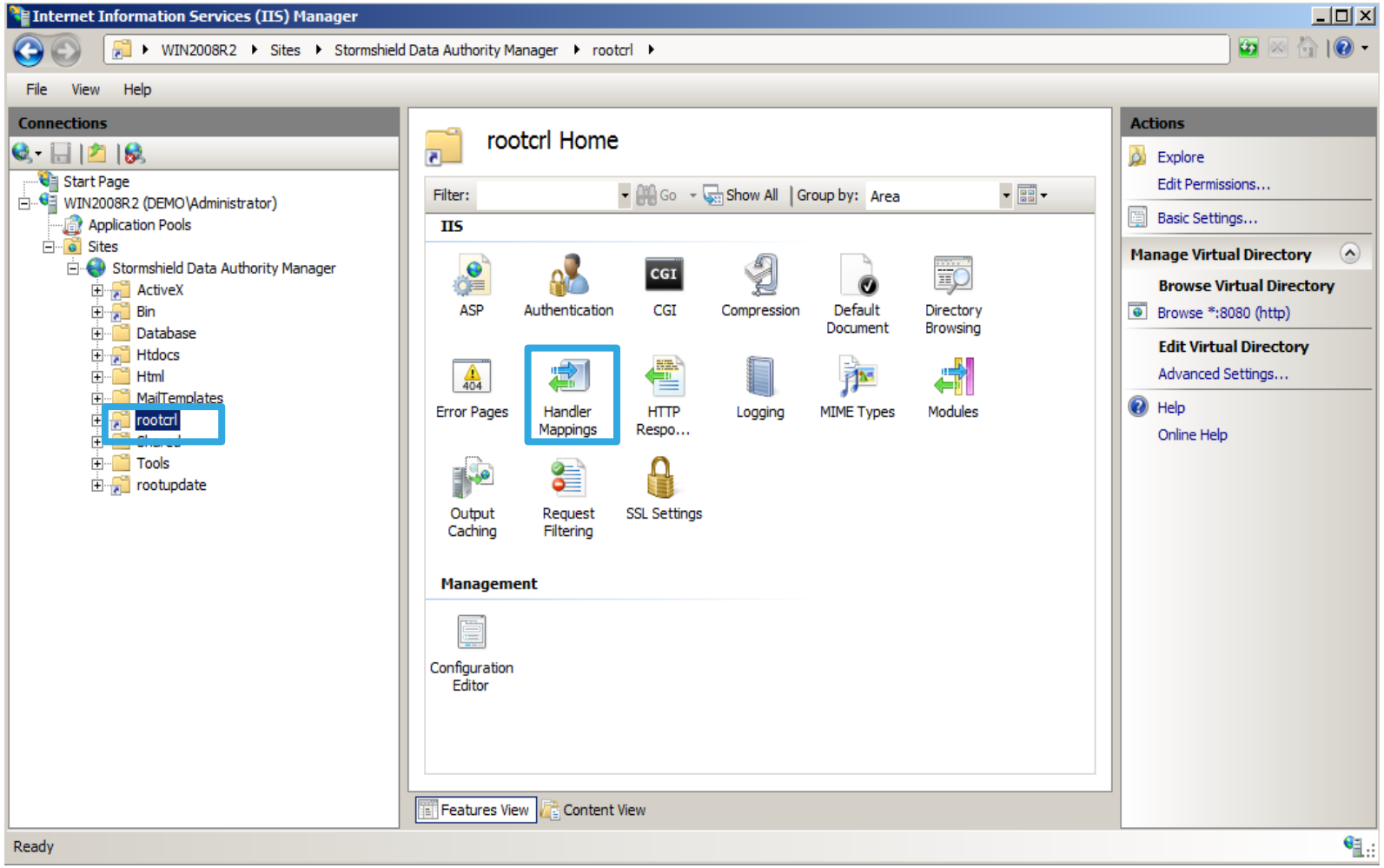
Right click and select **Add** in order to add *.usx* MIME Types





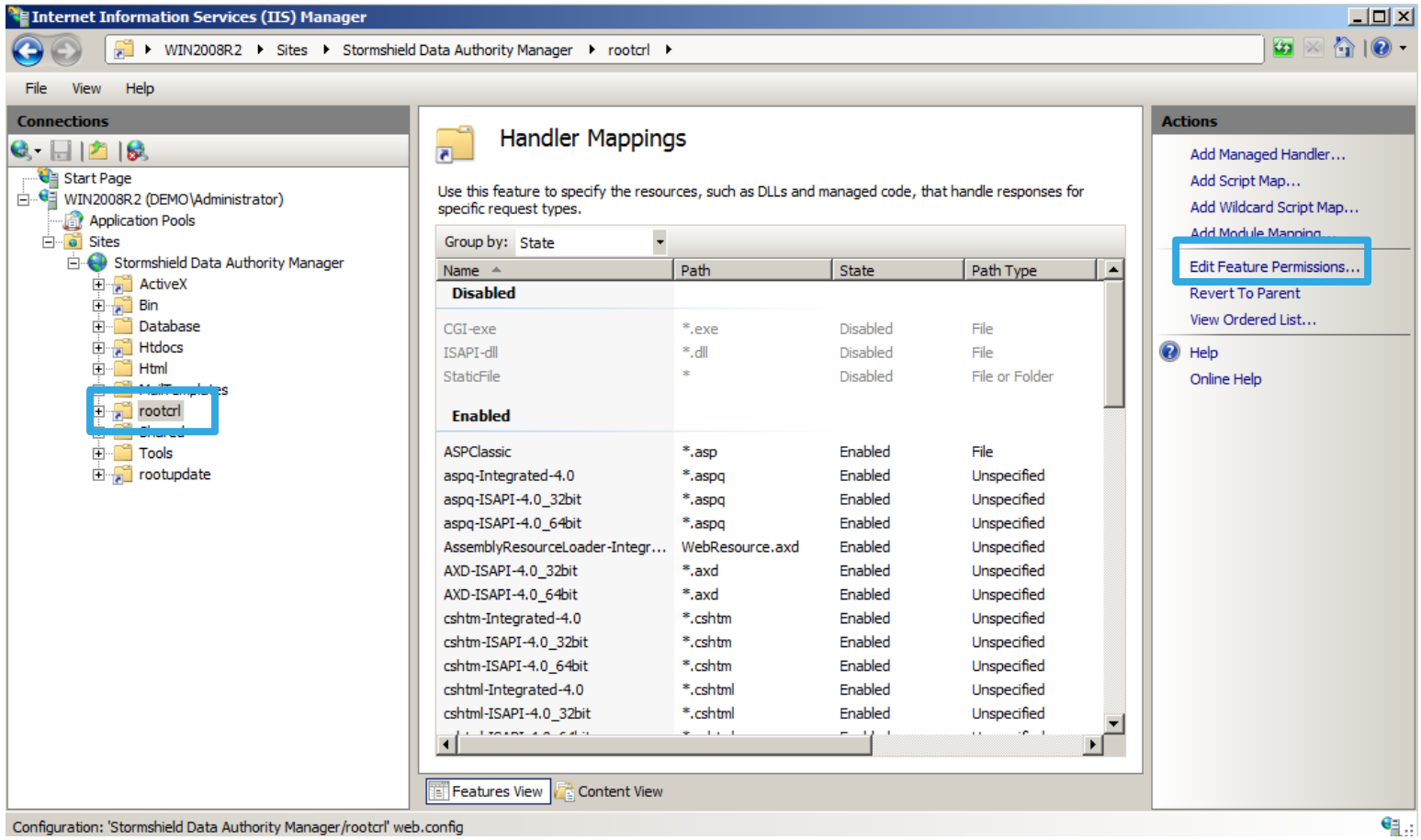
Configuring the IIS server (continued)

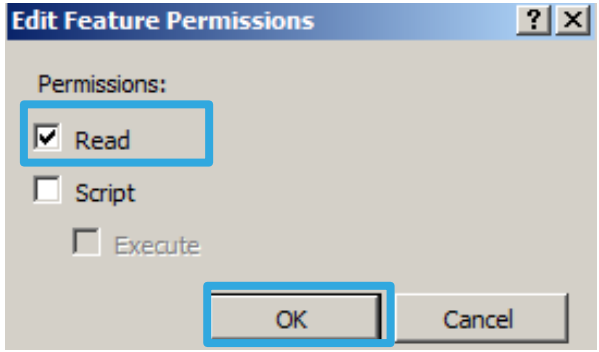
Expand **Stormshield Data Authority Manager** and click on the virtual directory **rootcrl**. Double click on **Handler Mappings**.



Configuring the IIS server (continued)

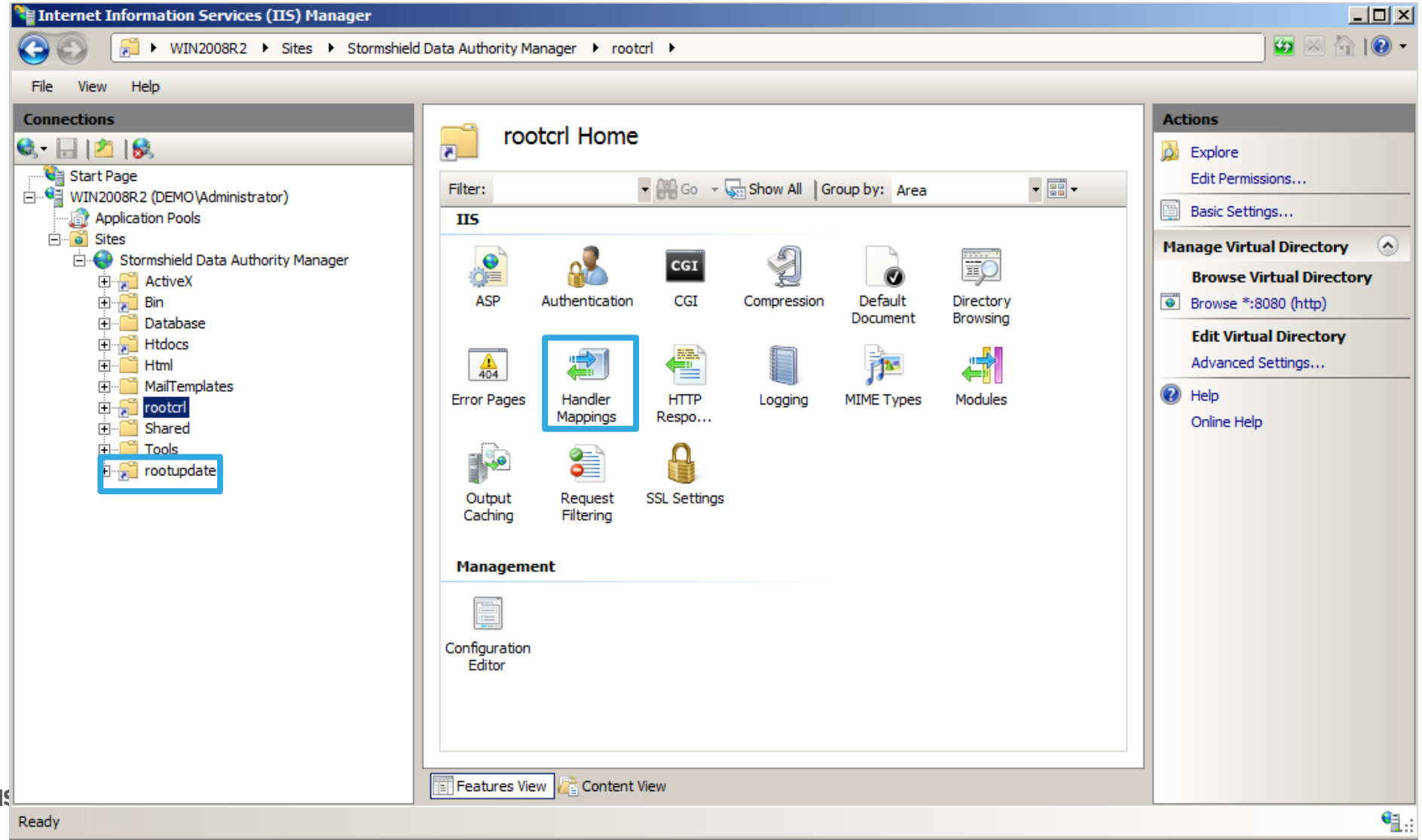
Click on **Edit Feature Permissions**, flag the option **Read** and click on **OK**





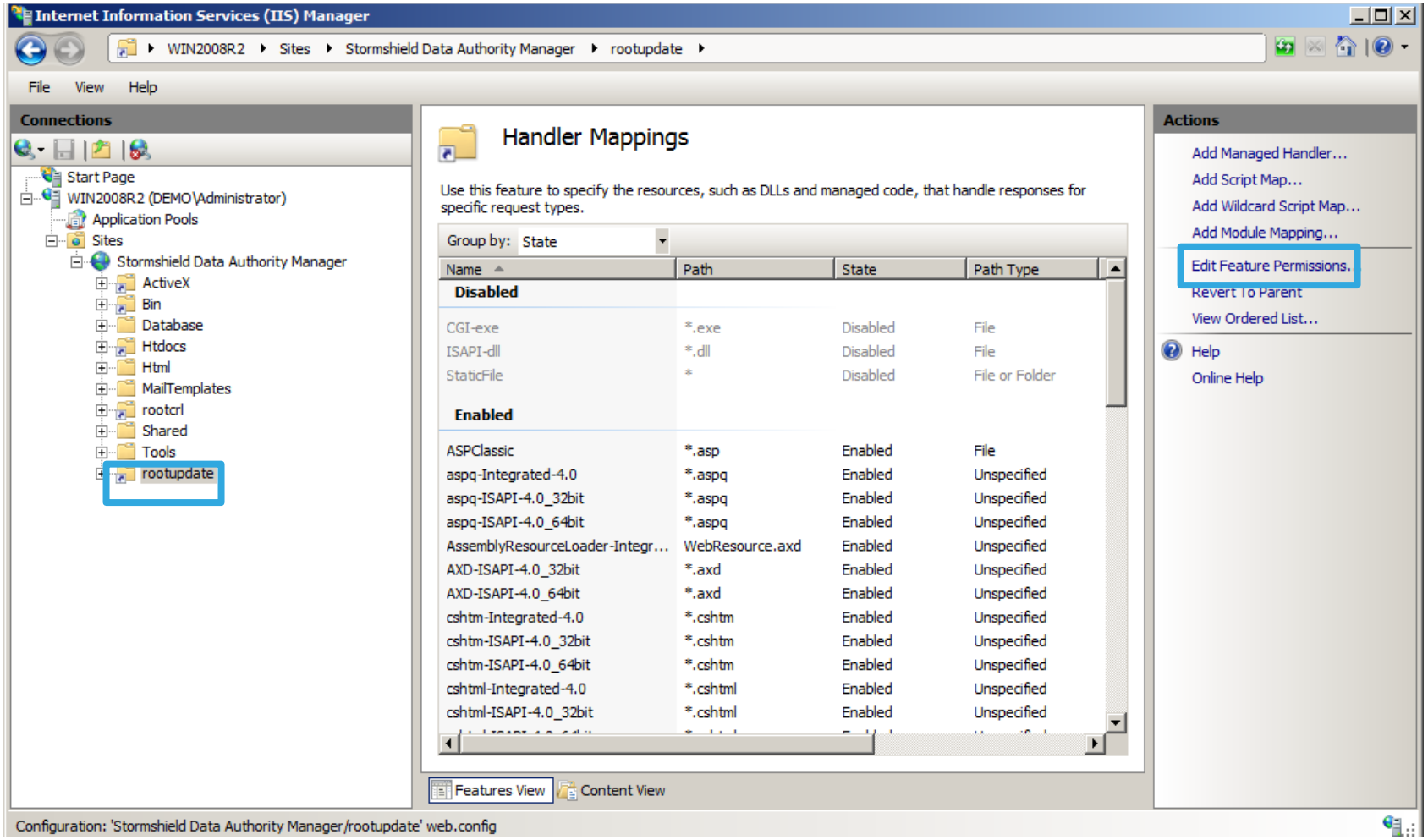
Configuring the IIS server (continued)

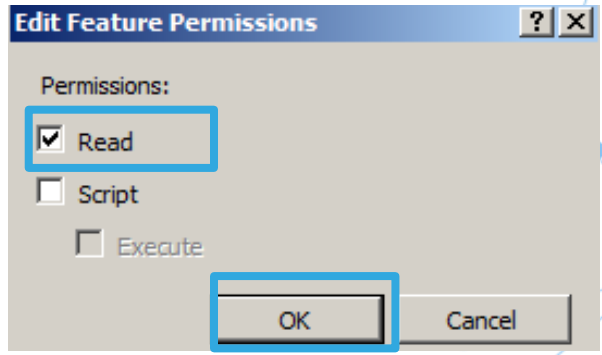
Select virtual directory **rootupdate** and double click on **Handler Mappings**



Configuring the IIS server (continued)

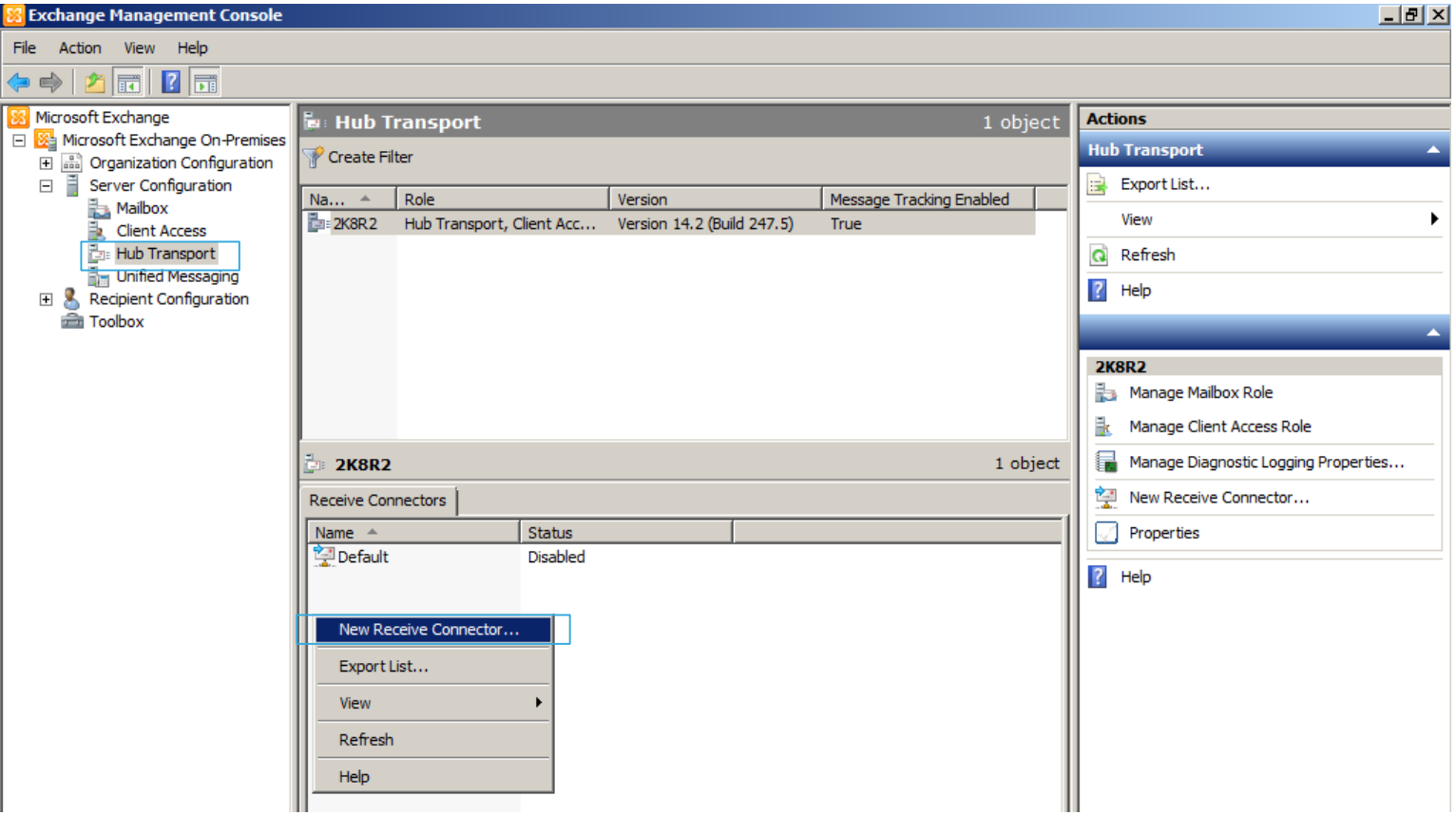
Click on **Edit Feature Permissions**, flag the option **Read** and click on **OK**

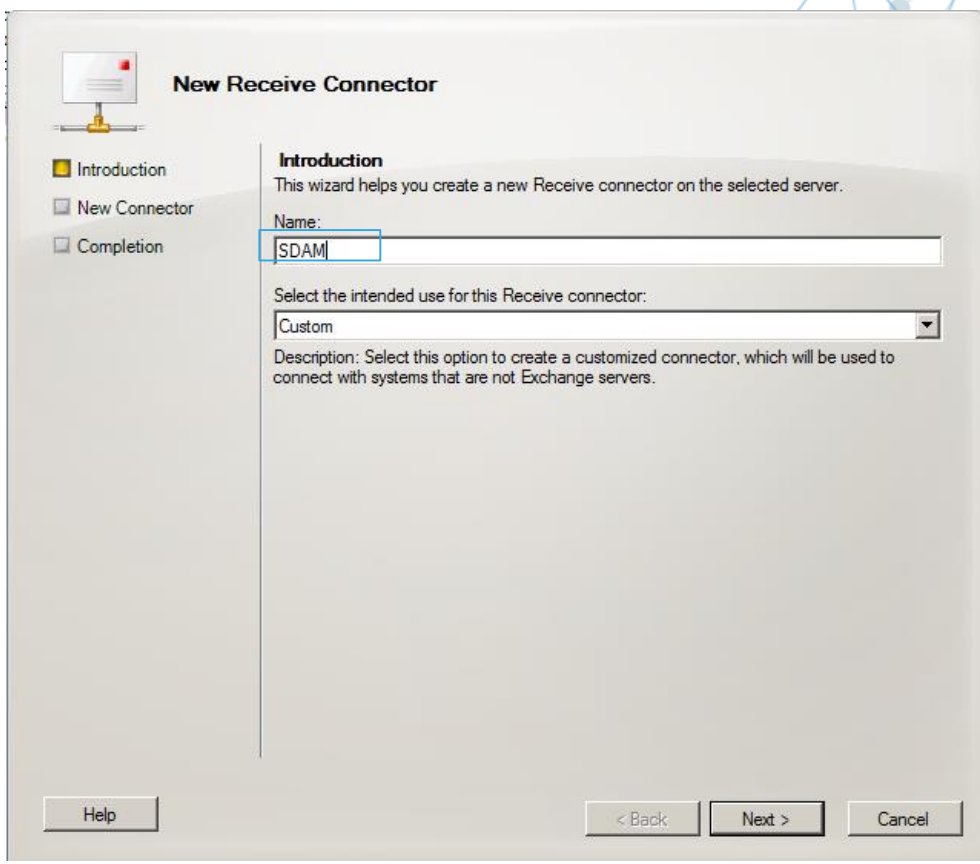




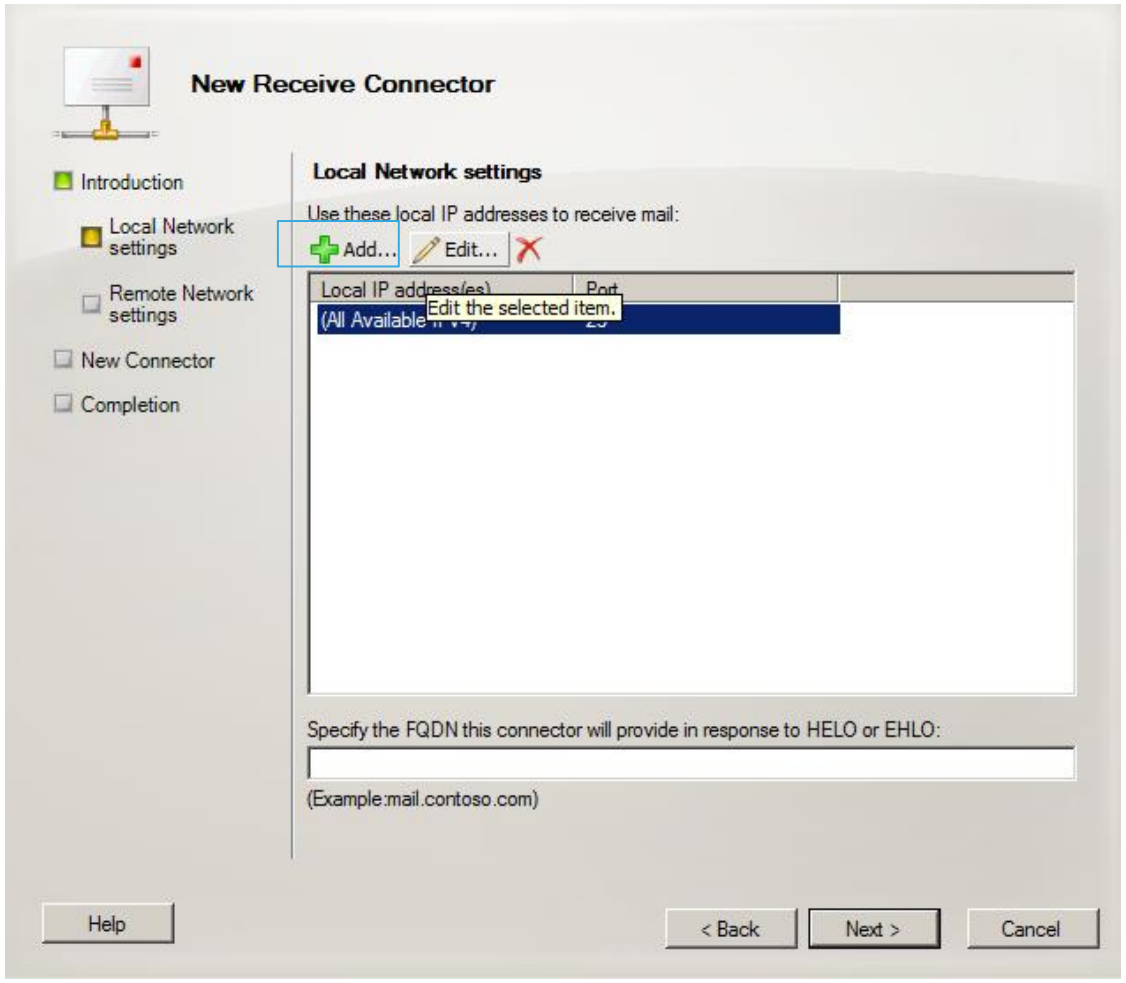
Configuring the Exchange server (option)

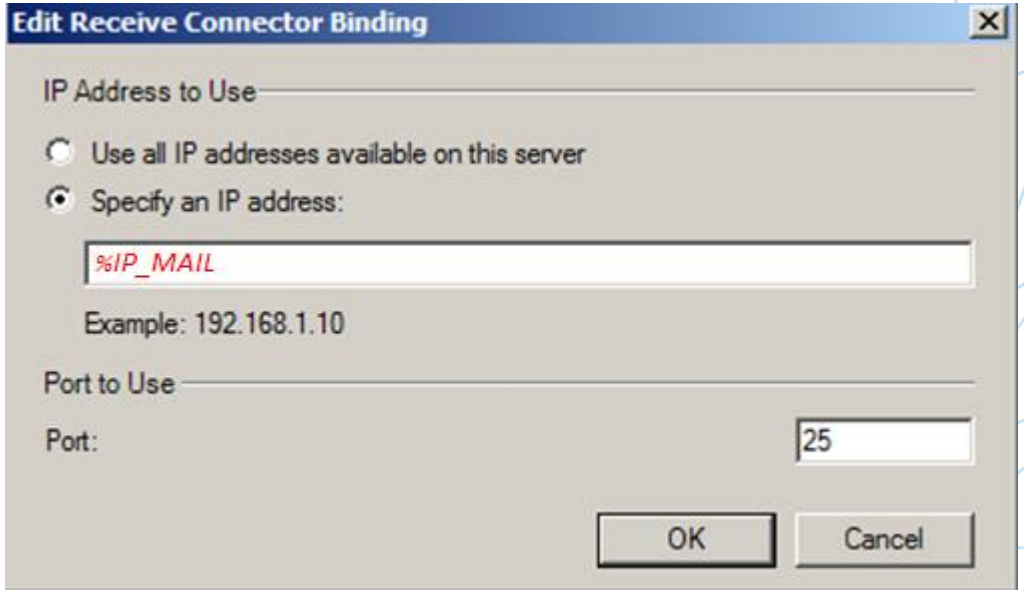
Configuring Exchange Inbound Connector



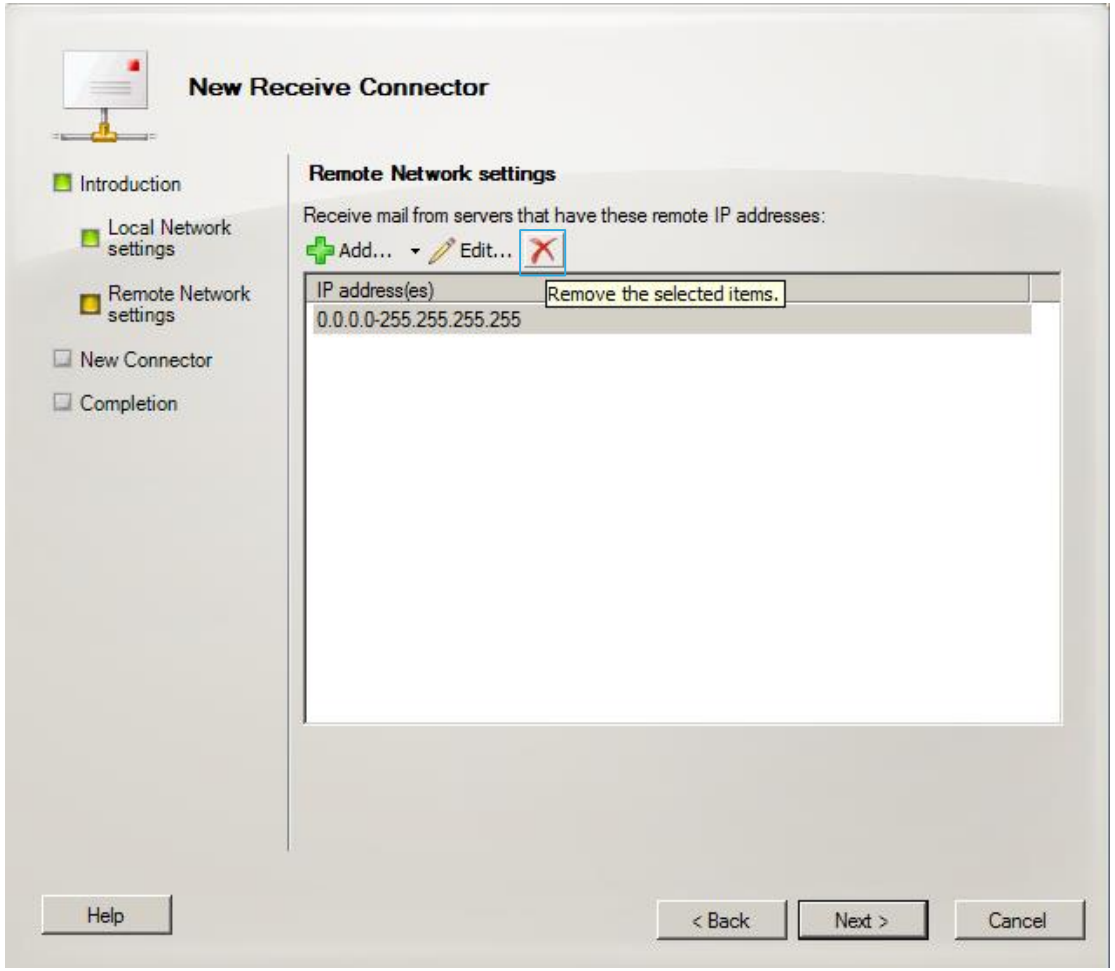


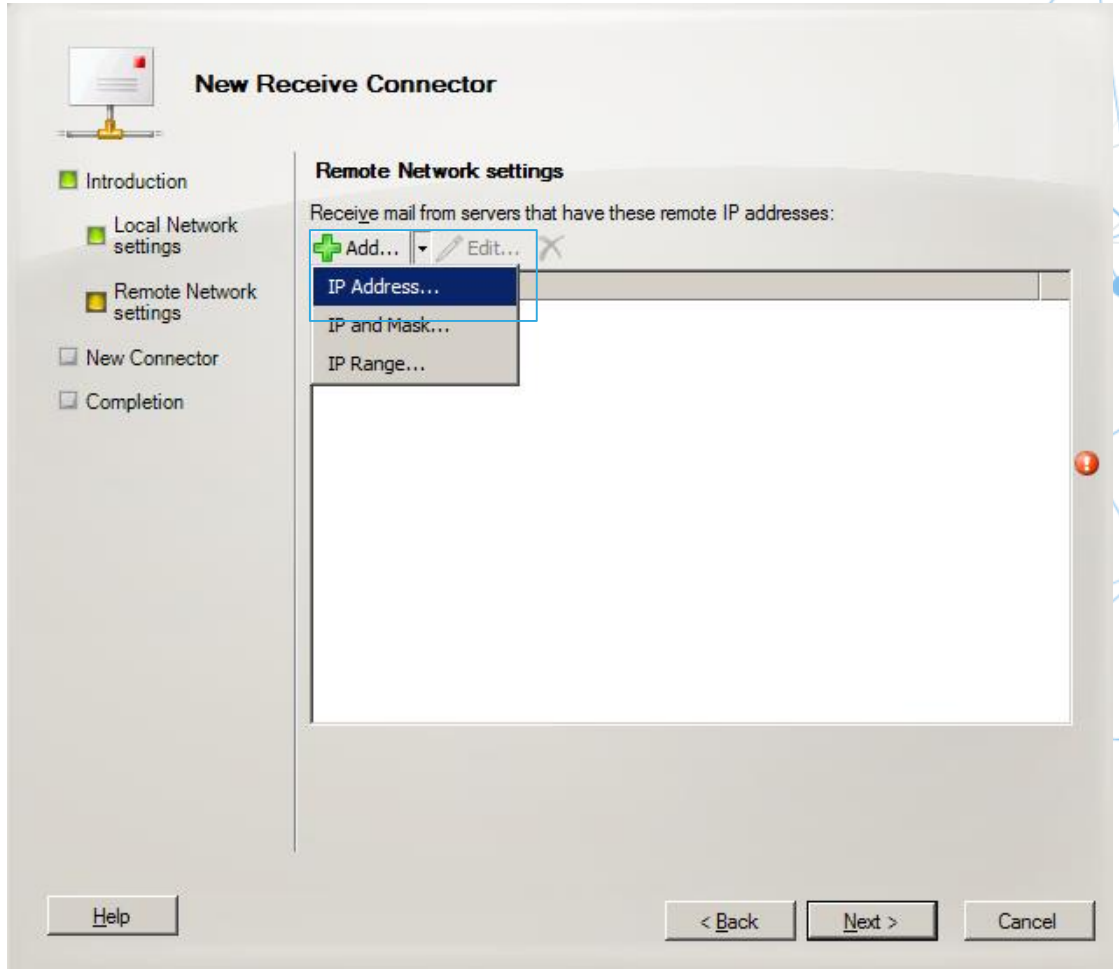
Configuring Exchange Inbound Connector (continued)



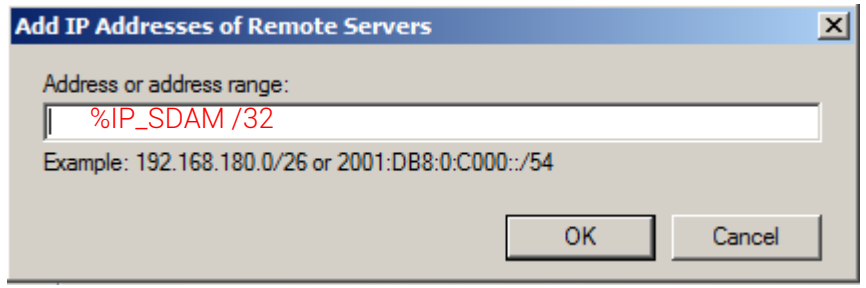


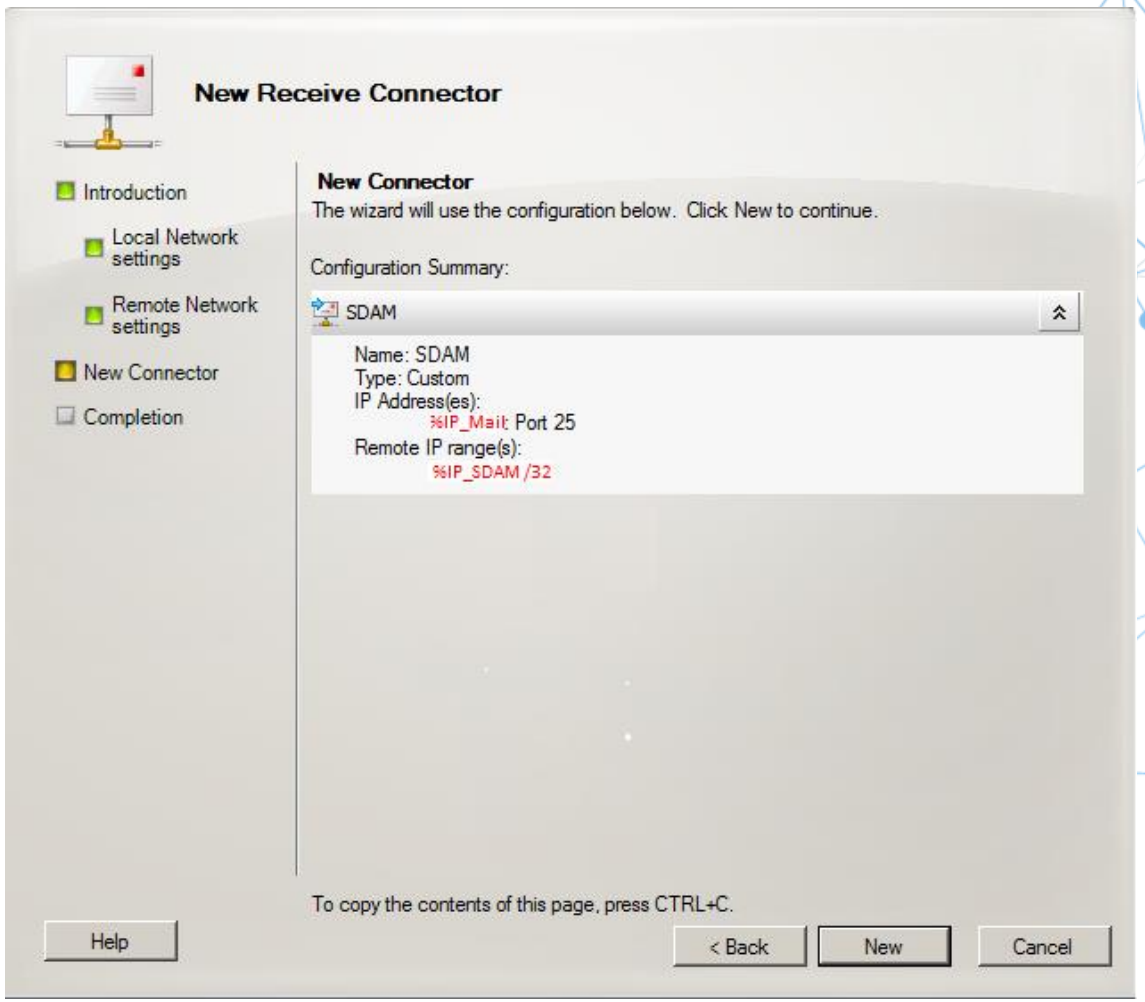
Configuring Exchange Inbound Connector (continued)



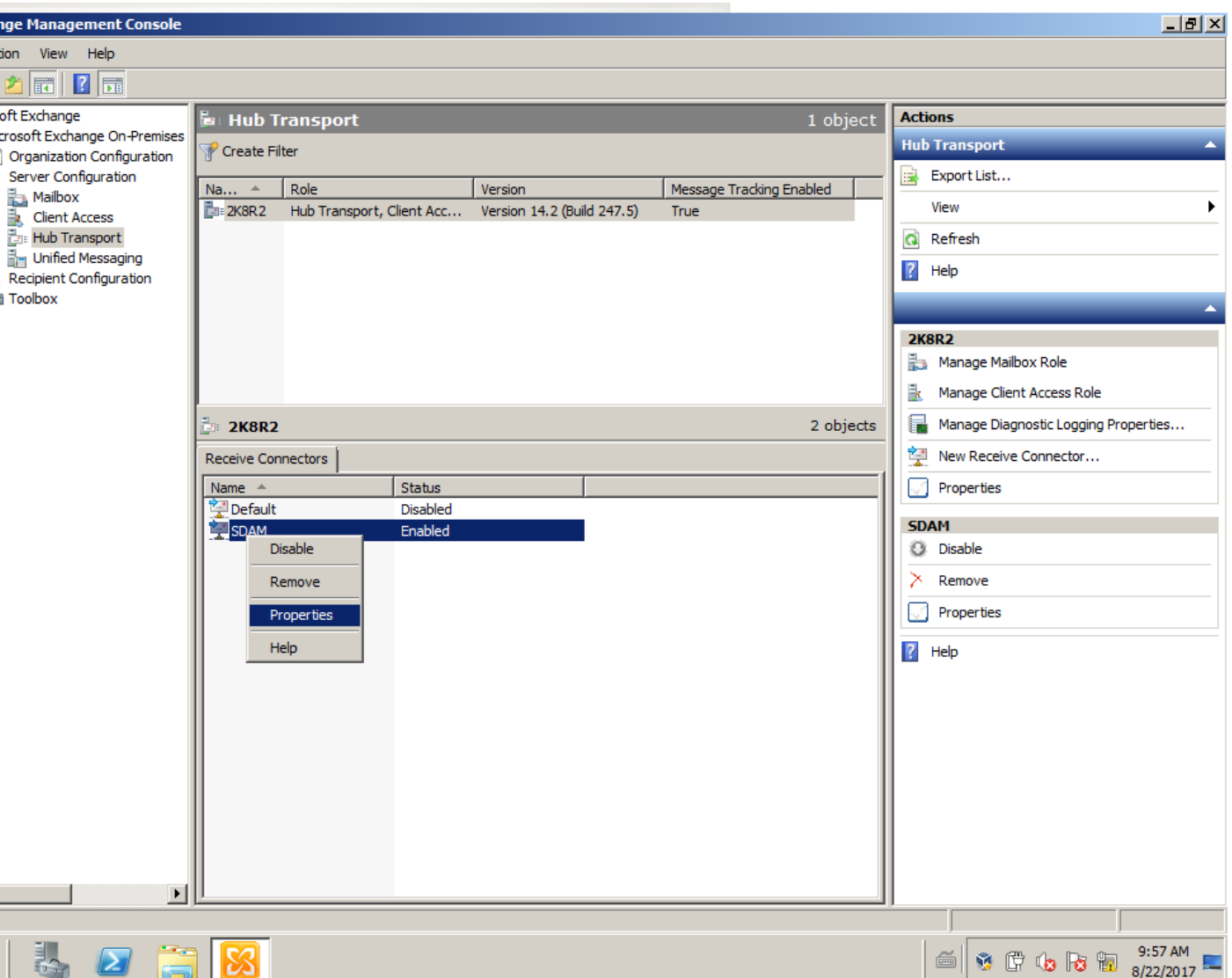


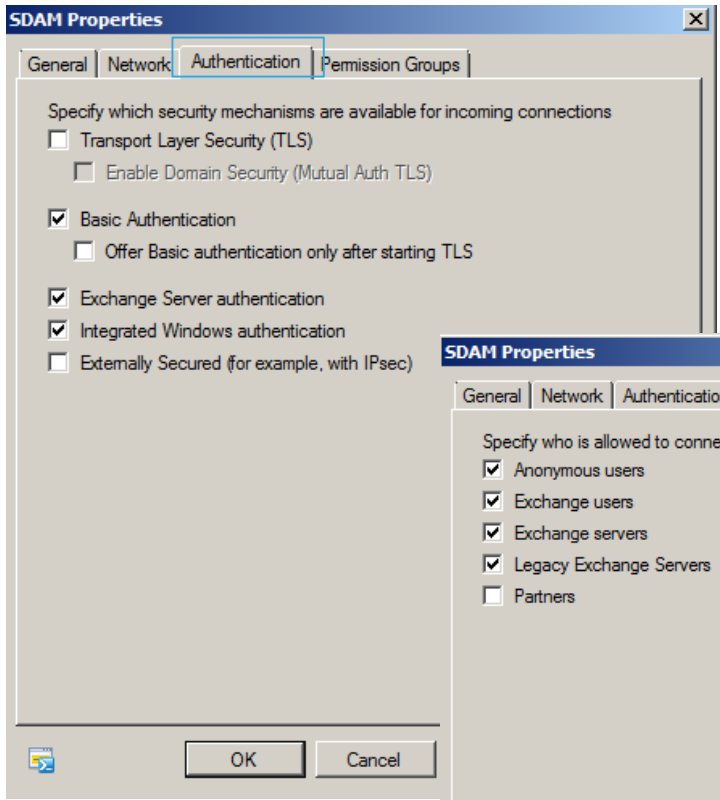
Configuring Exchange Inbound Connector (continued)

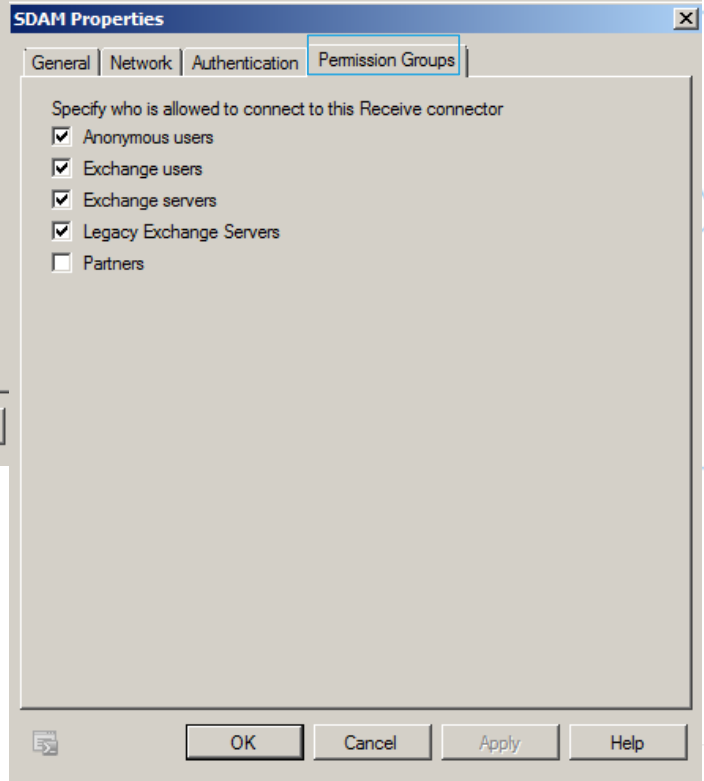




Configuring Exchange Inbound Connector (continued)





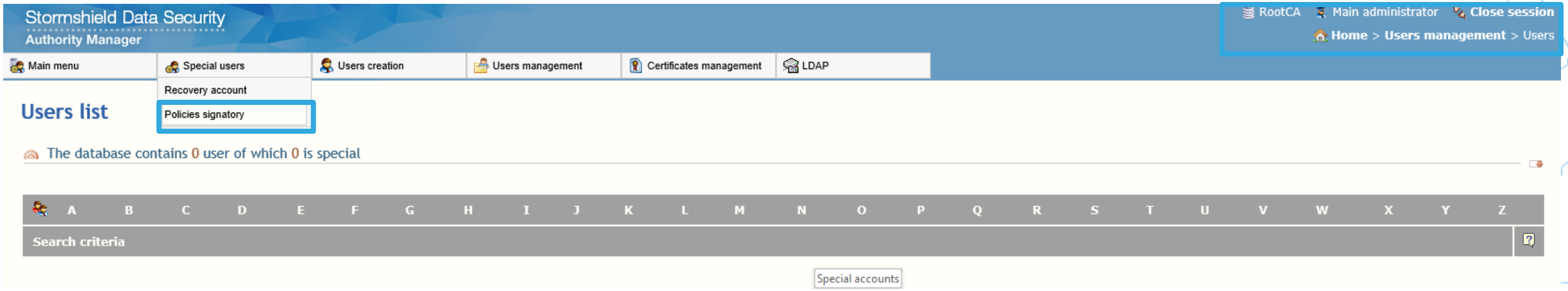


Creating special SDS accounts

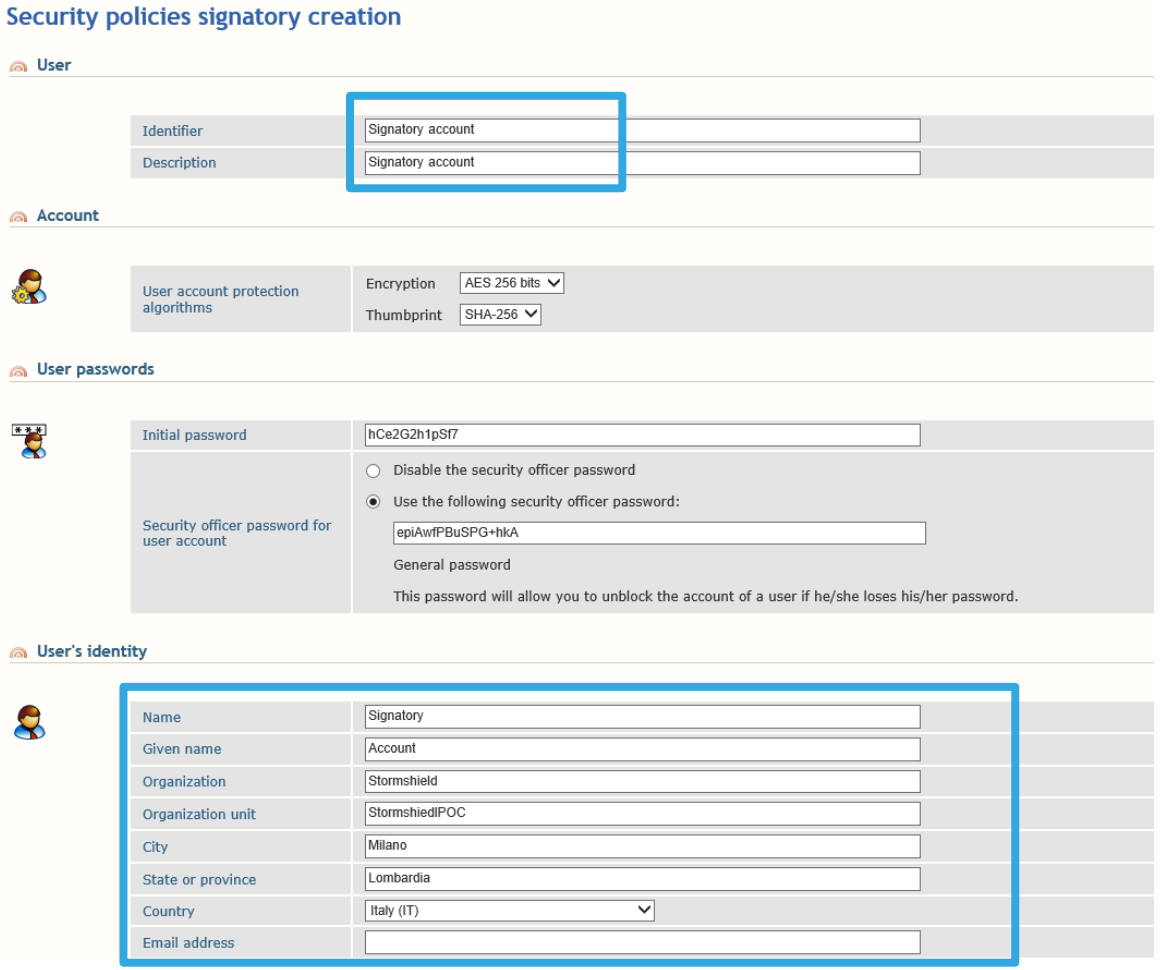
Special accounts

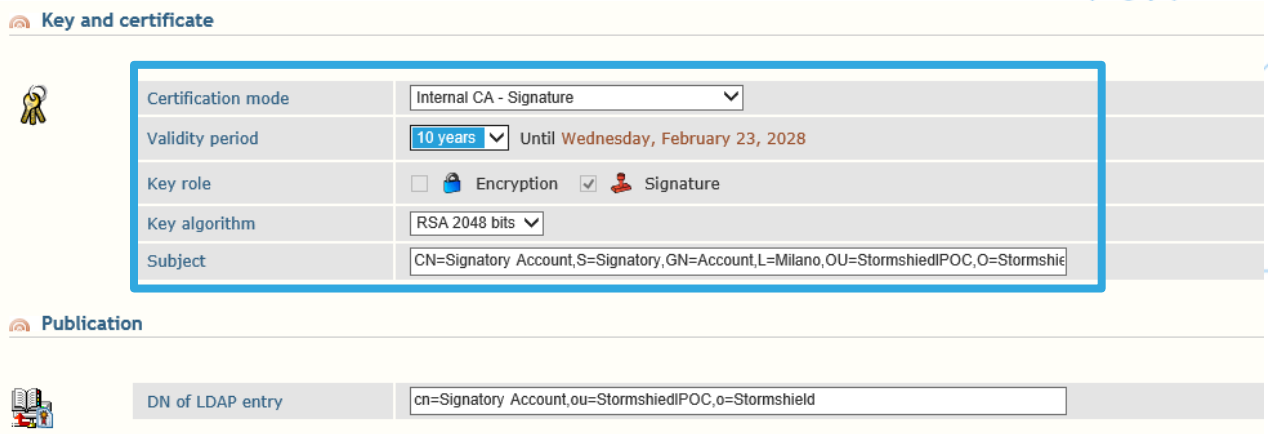
Now you need to create two special users (Signatory and Recovery)

Click on **Users Management → Users → Special users → Policies signatory**



Special accounts (continued)

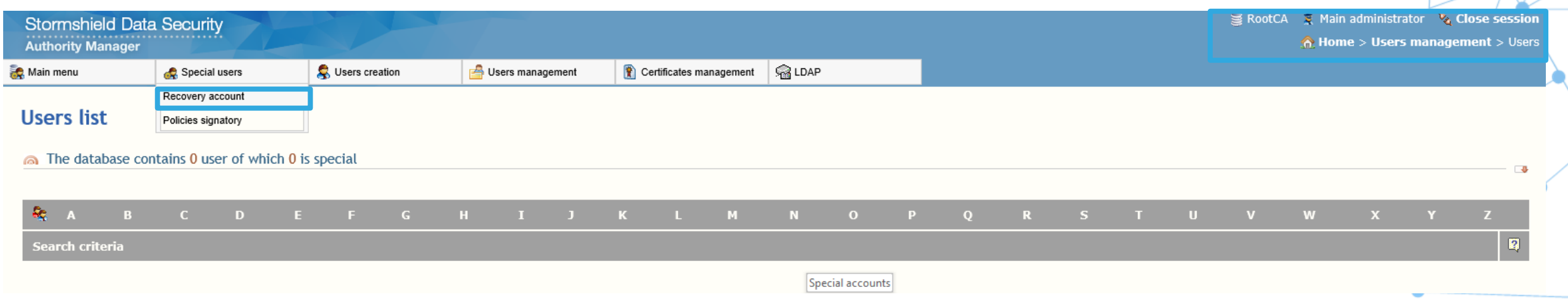




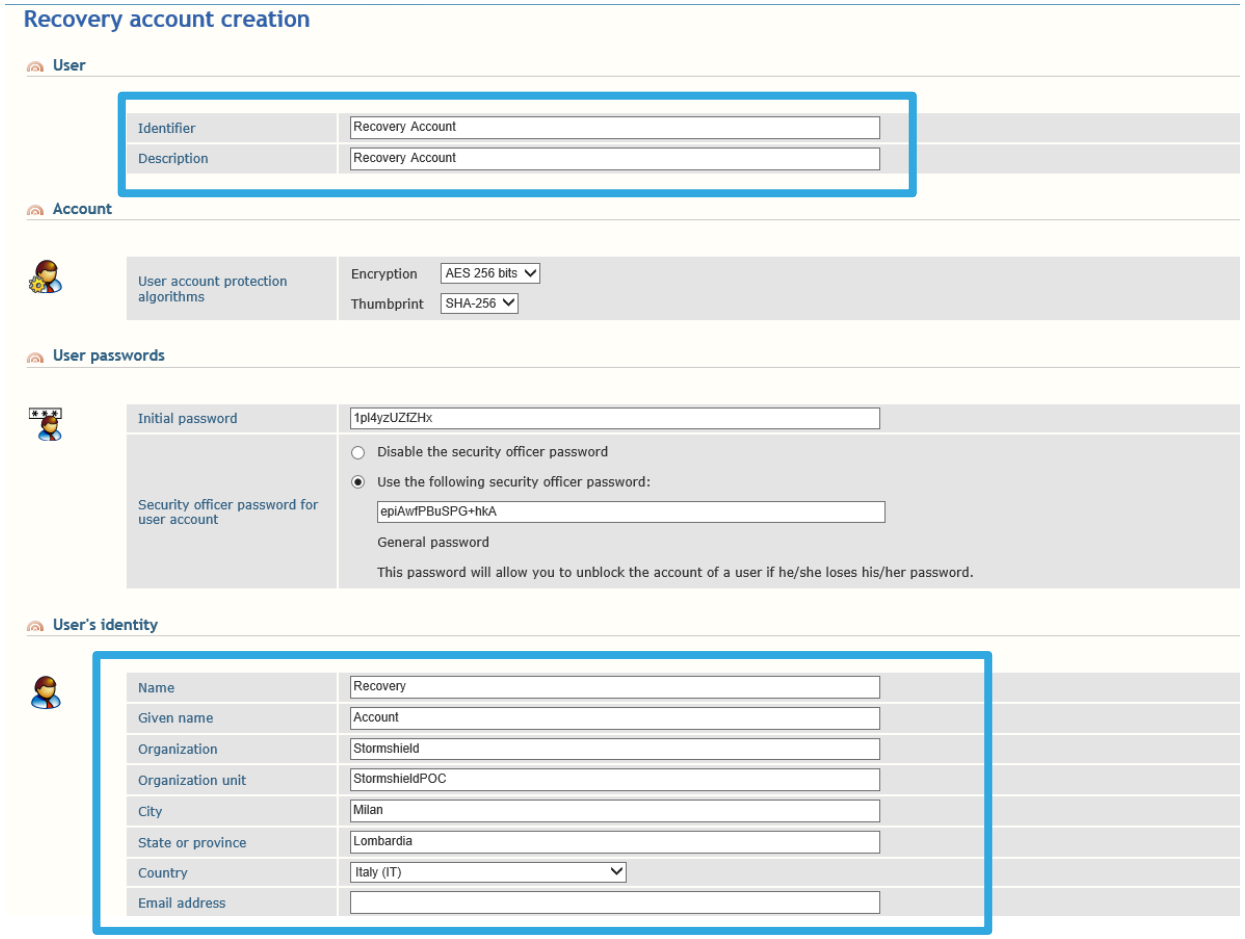
Click on **Create user**

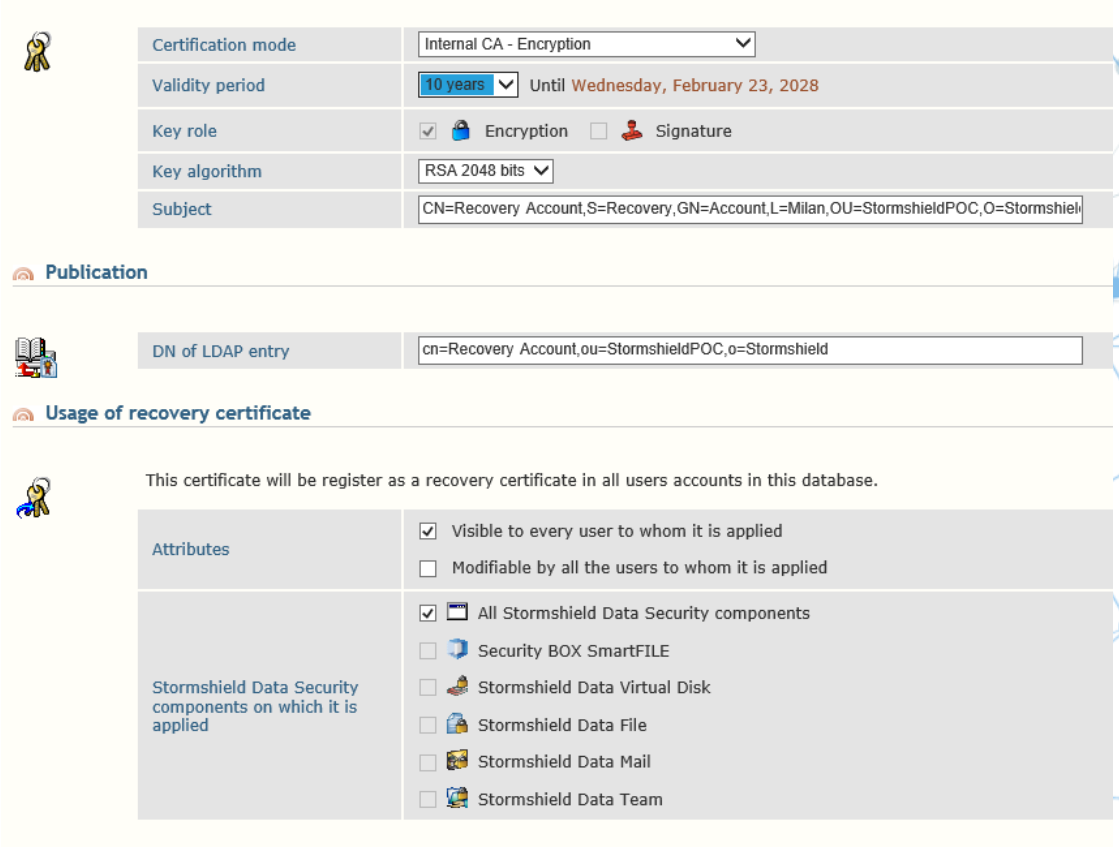
Special accounts (continued)

Click on **Users Management** → **Users** → **Special users** → **Recovery account**



Special accounts (continued)



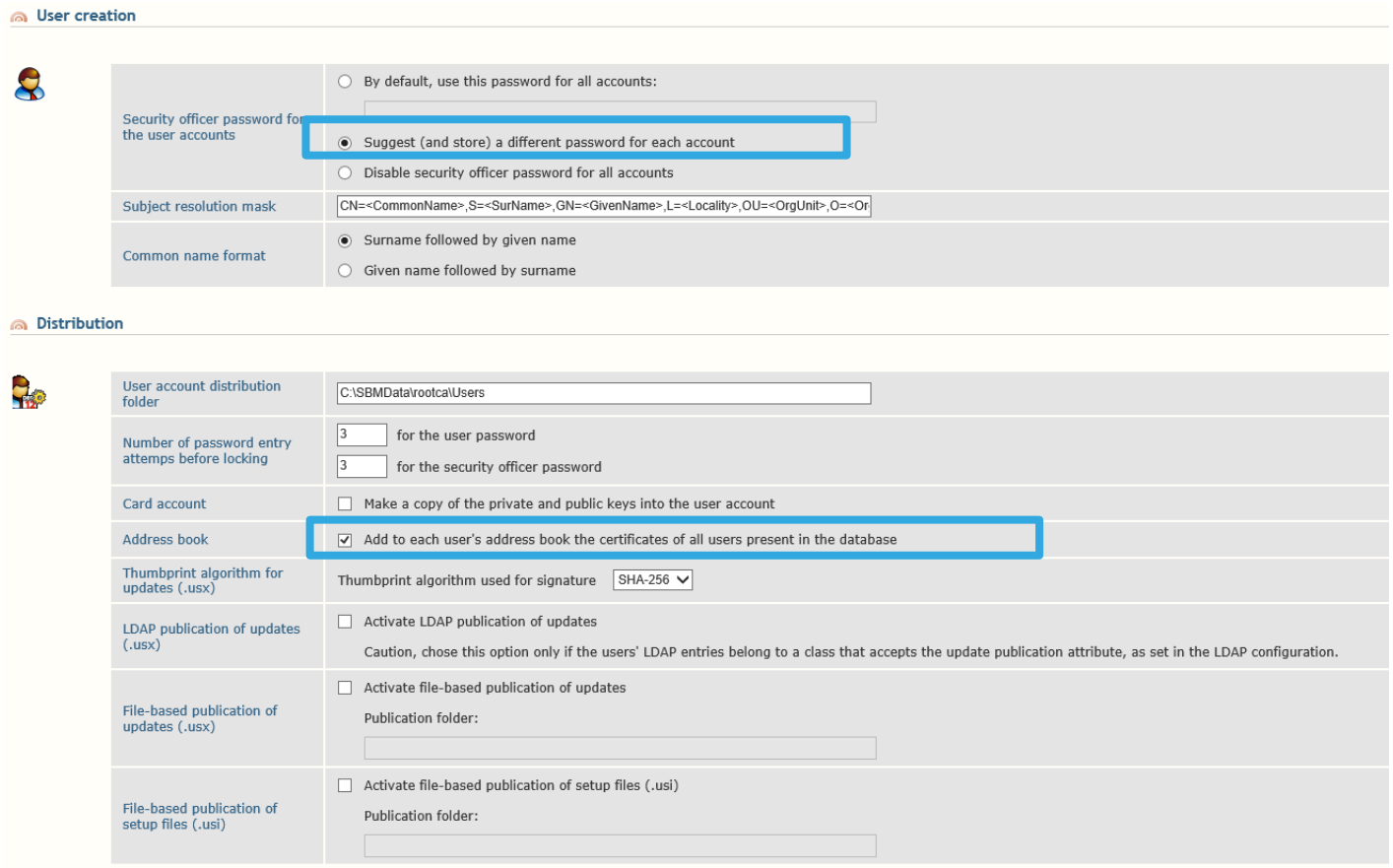


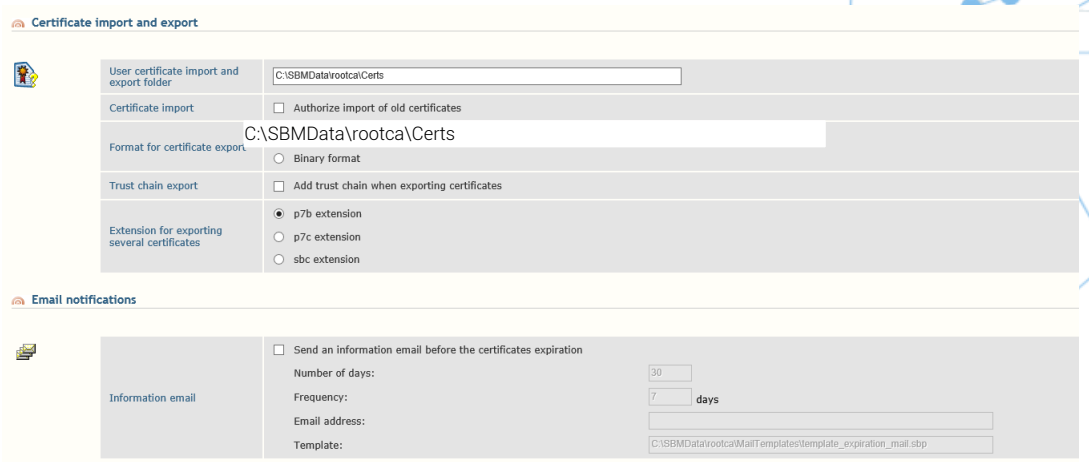
Click on **Create user**

Setting up SDS account configuration

User settings

Click on **Main menu → Settings → Users Management**

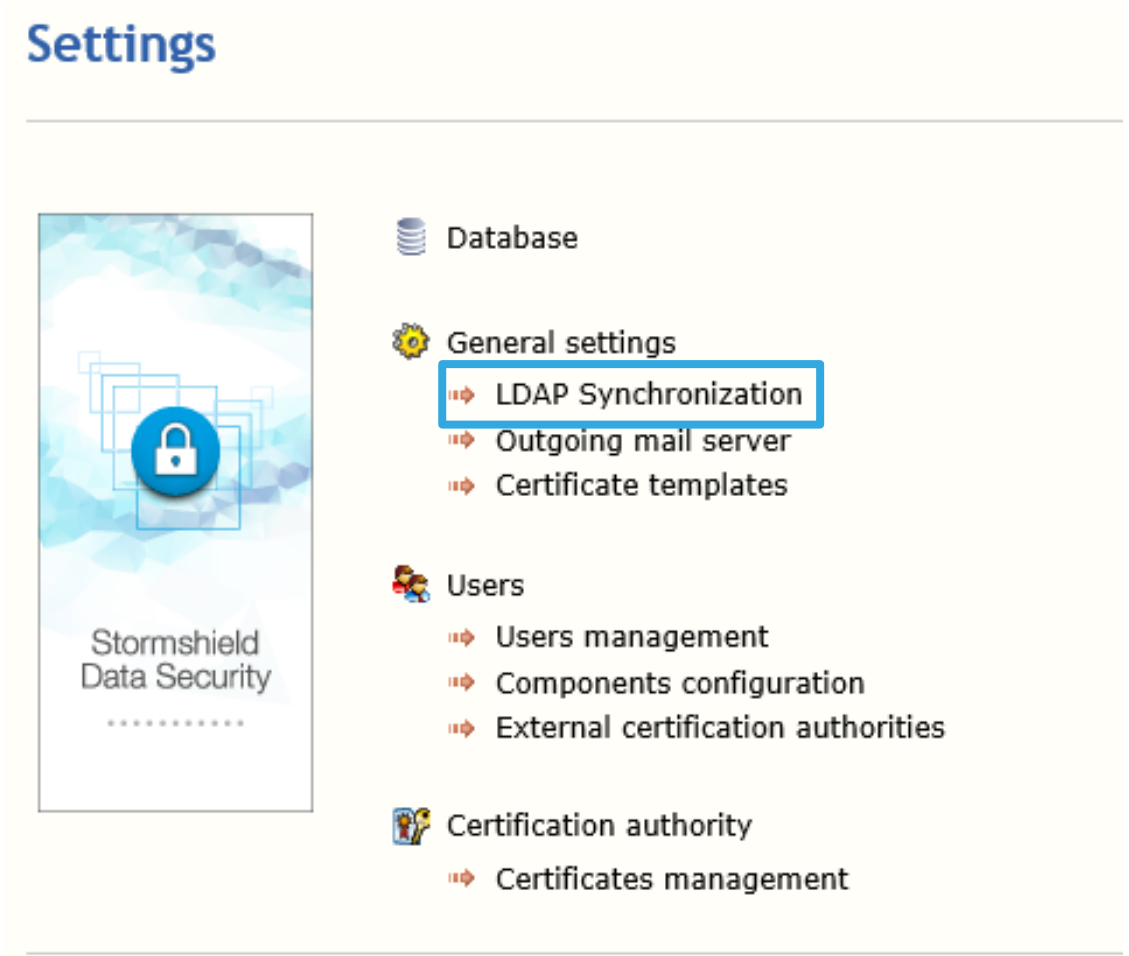




Click on **Apply modifications**

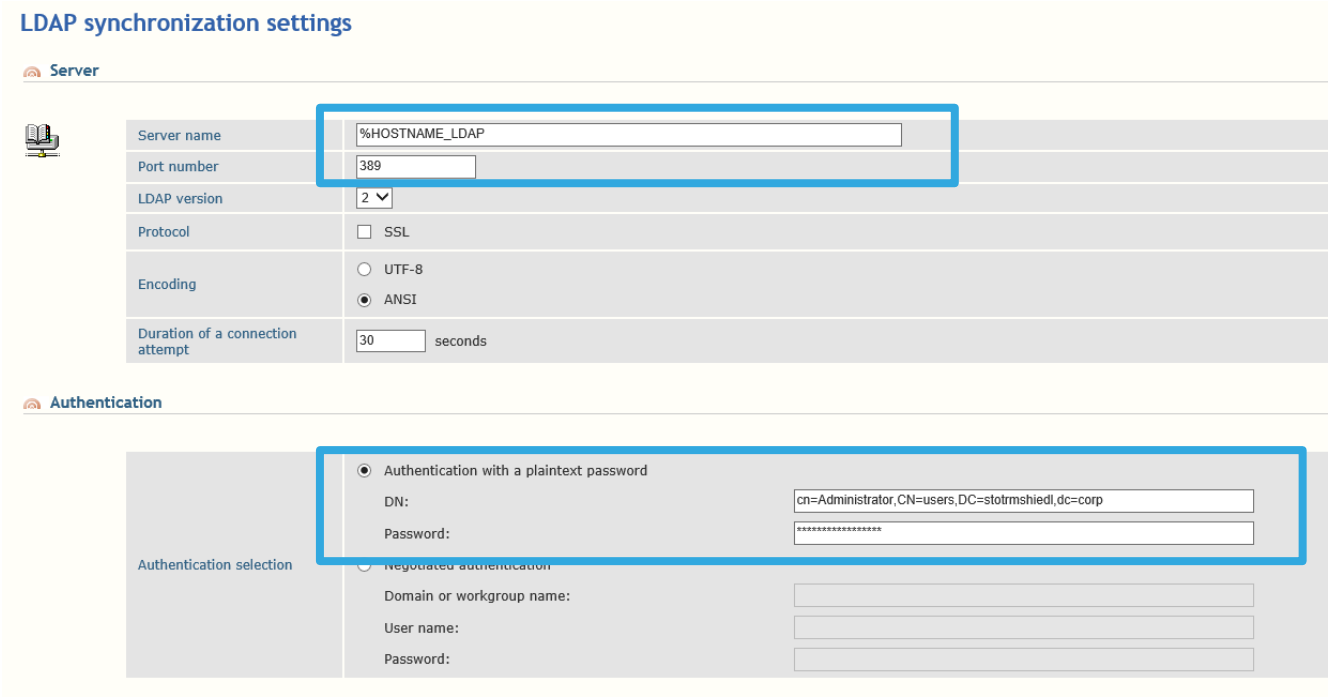
Option: LDAP settings

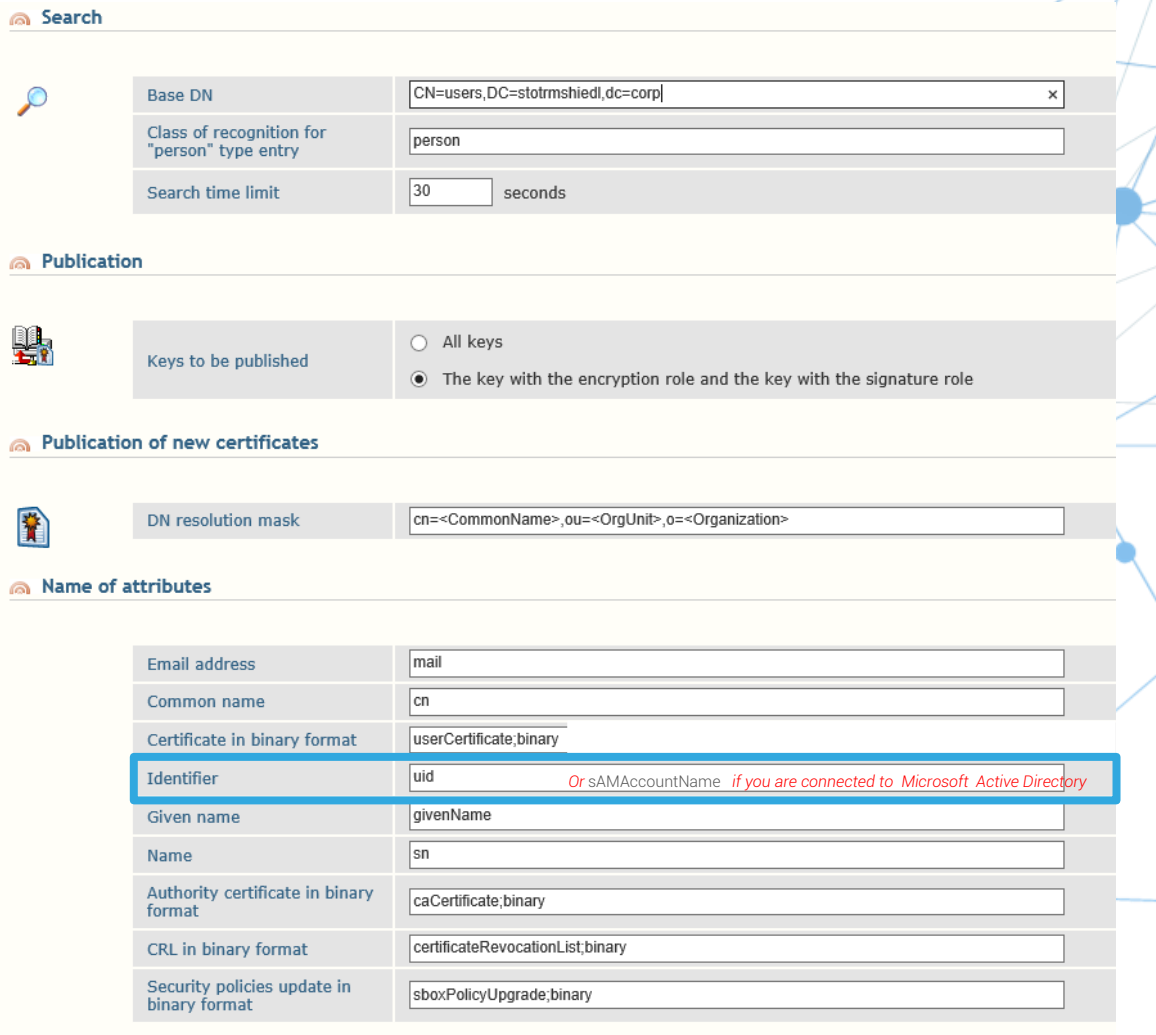
Click on **Main menu** → **Settings** → then select **LDAP Synchronization**



Option: LDAP settings (continued)

If you are connected to AD, set ***sAMAccountName*** as the Identifier

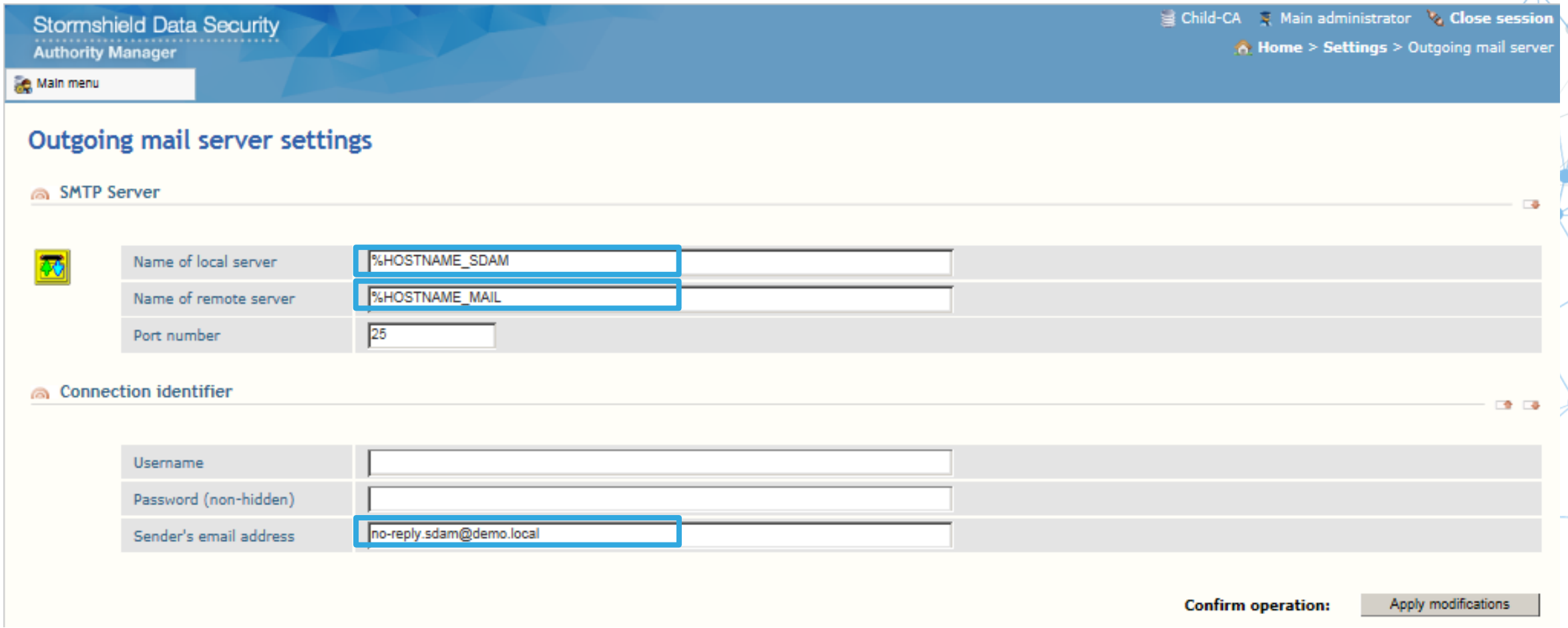




Click on **Apply modifications**

Option: SMTP settings

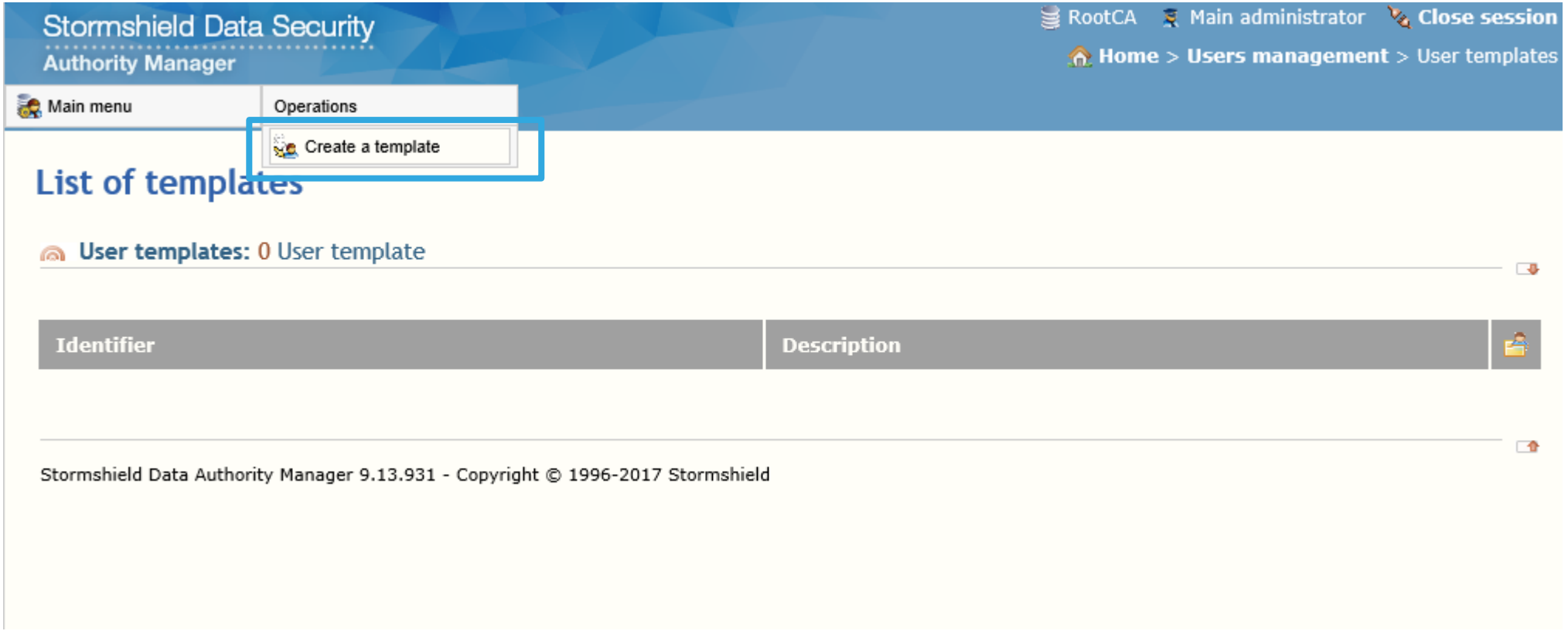
Click on **Main menu → Settings → Outgoing mail server** and add all necessary information to allow the SDAM to send e-mail using your e-mail server



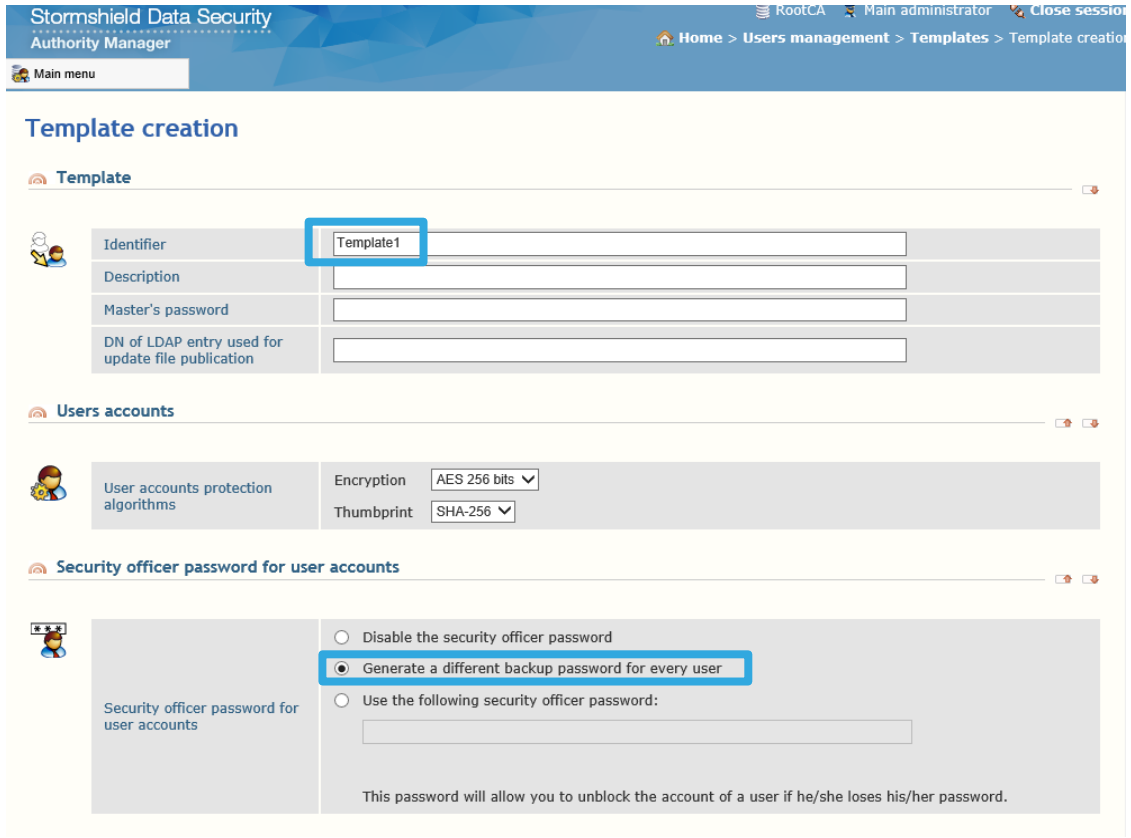
Creating SDS account templates

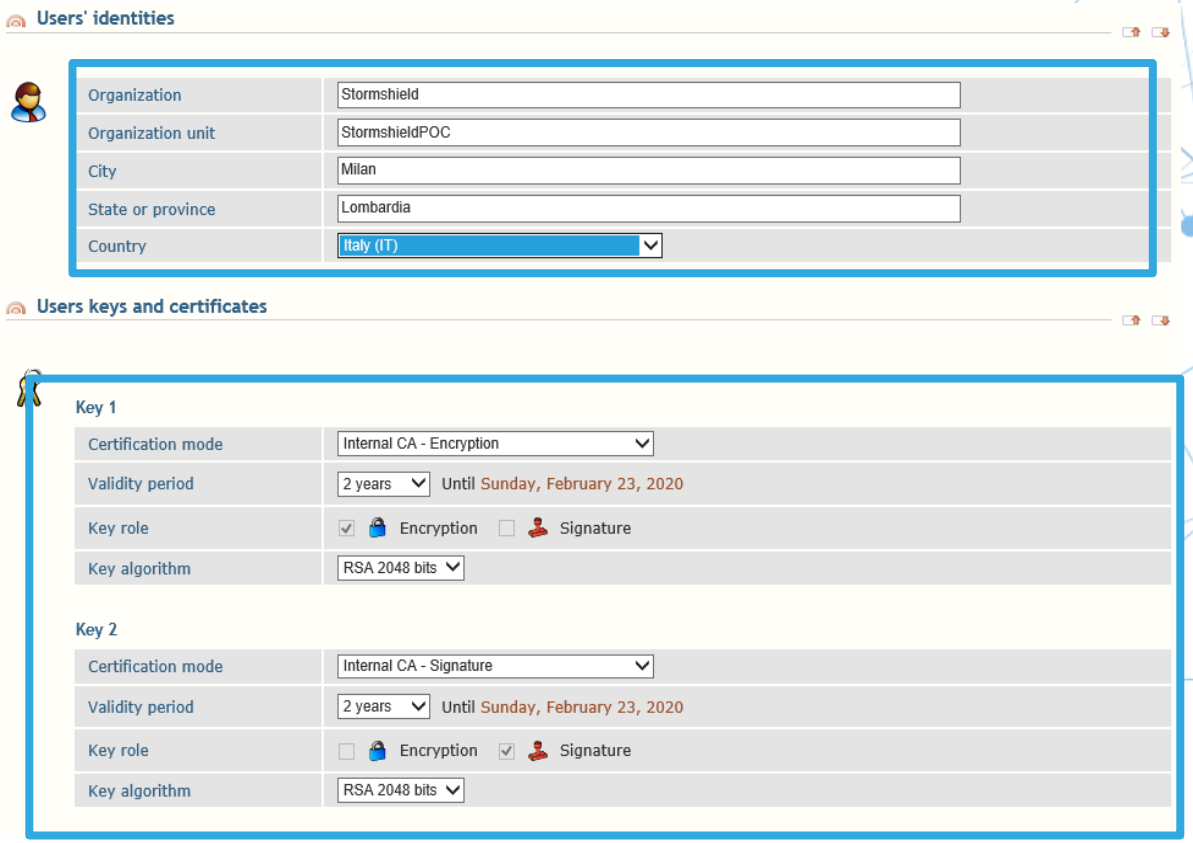
Creating a template

Click on **Main menu** → **User management** → **User templates**
then click on **Operations** →**Create a template**



Creating a template (continued)

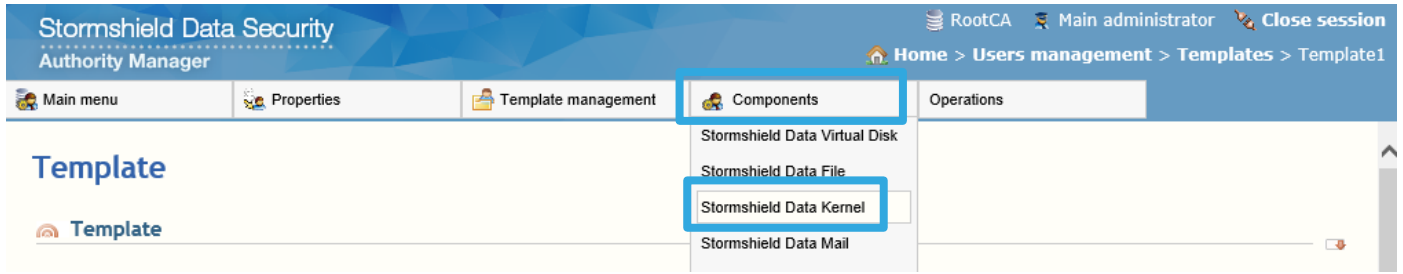




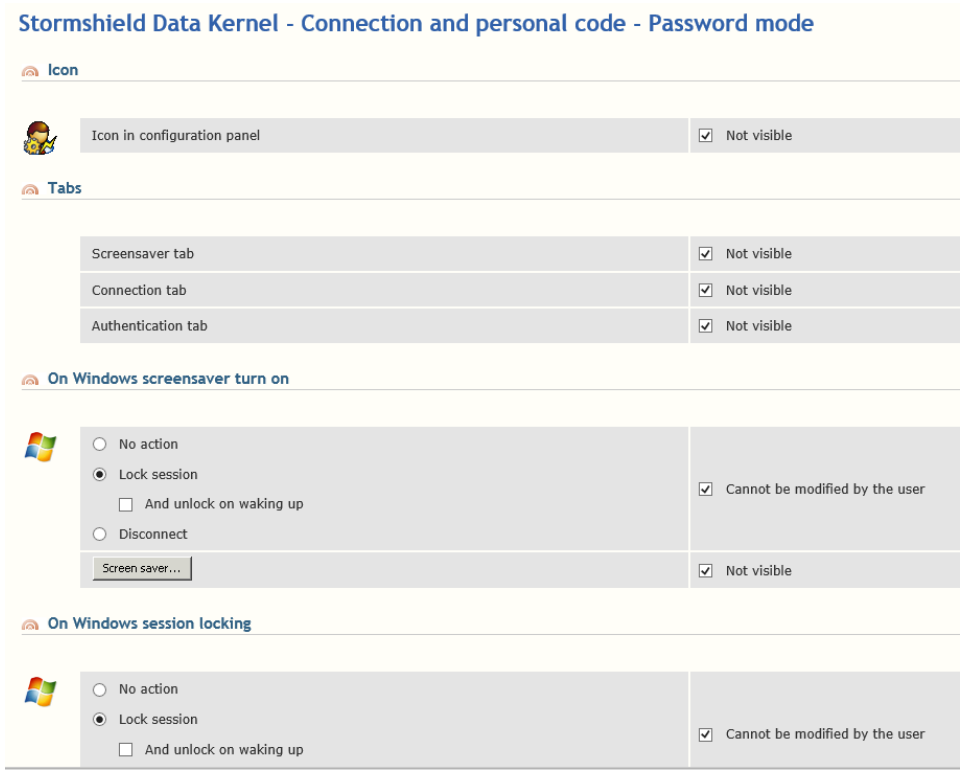
Click on **Create template**

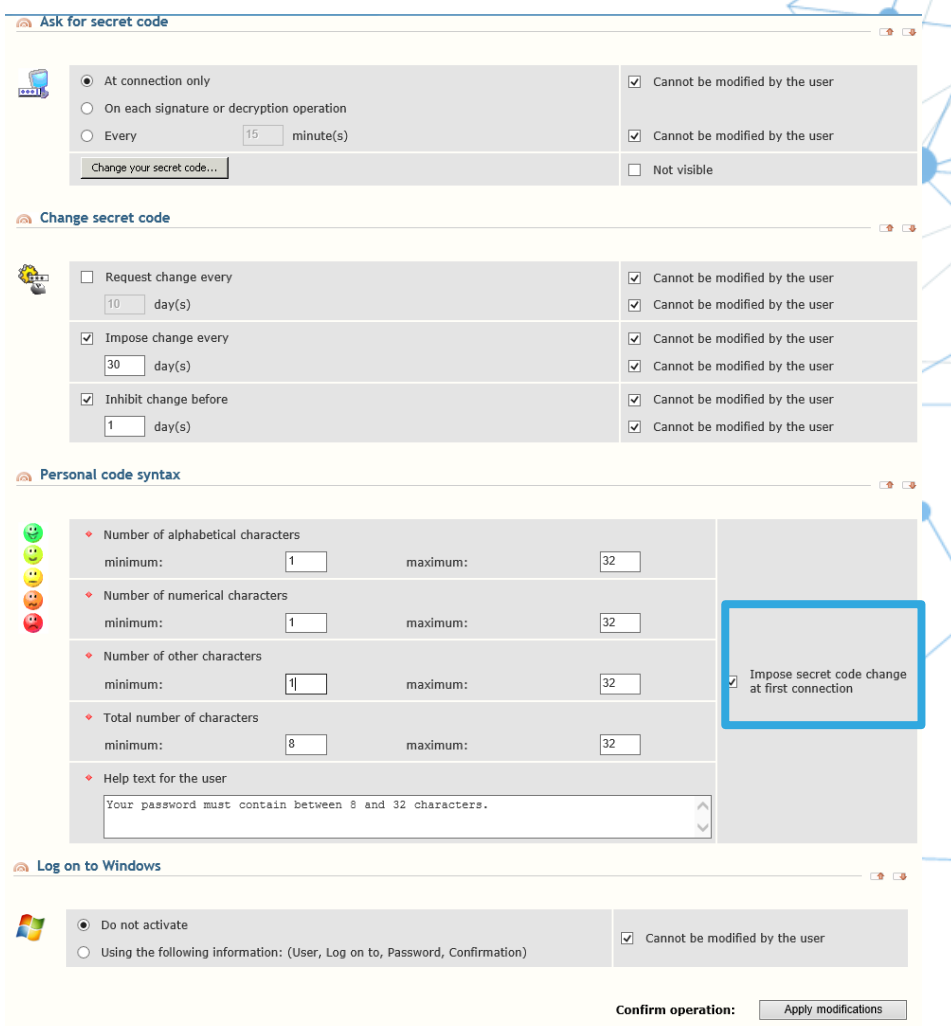
Creating a template (continued): configuring the PoC

Click on **Main menu → Users management → User template** and select the template that you have already created



Click on **Connection and personal code – Password mode**



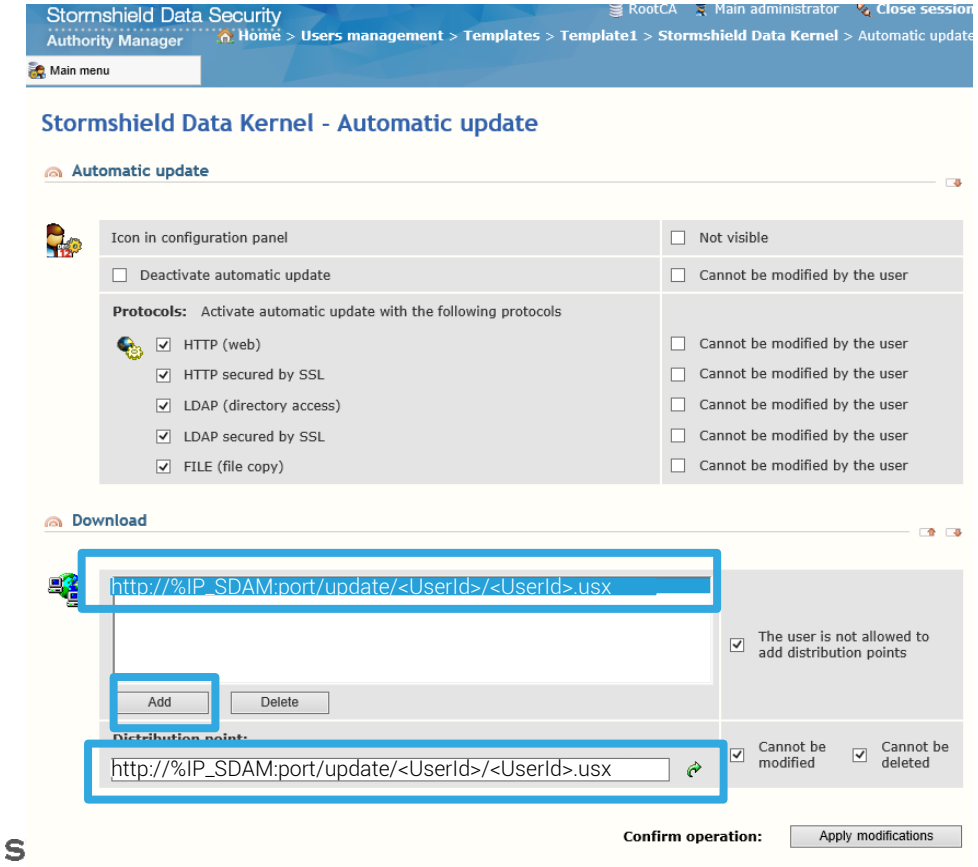


Click on **Apply modifications**

Automatic profile updates

Click on **Main menu → Users management → User template** and select the template that you have already created. Then click on **Components → Stormshield Data Kernel**.

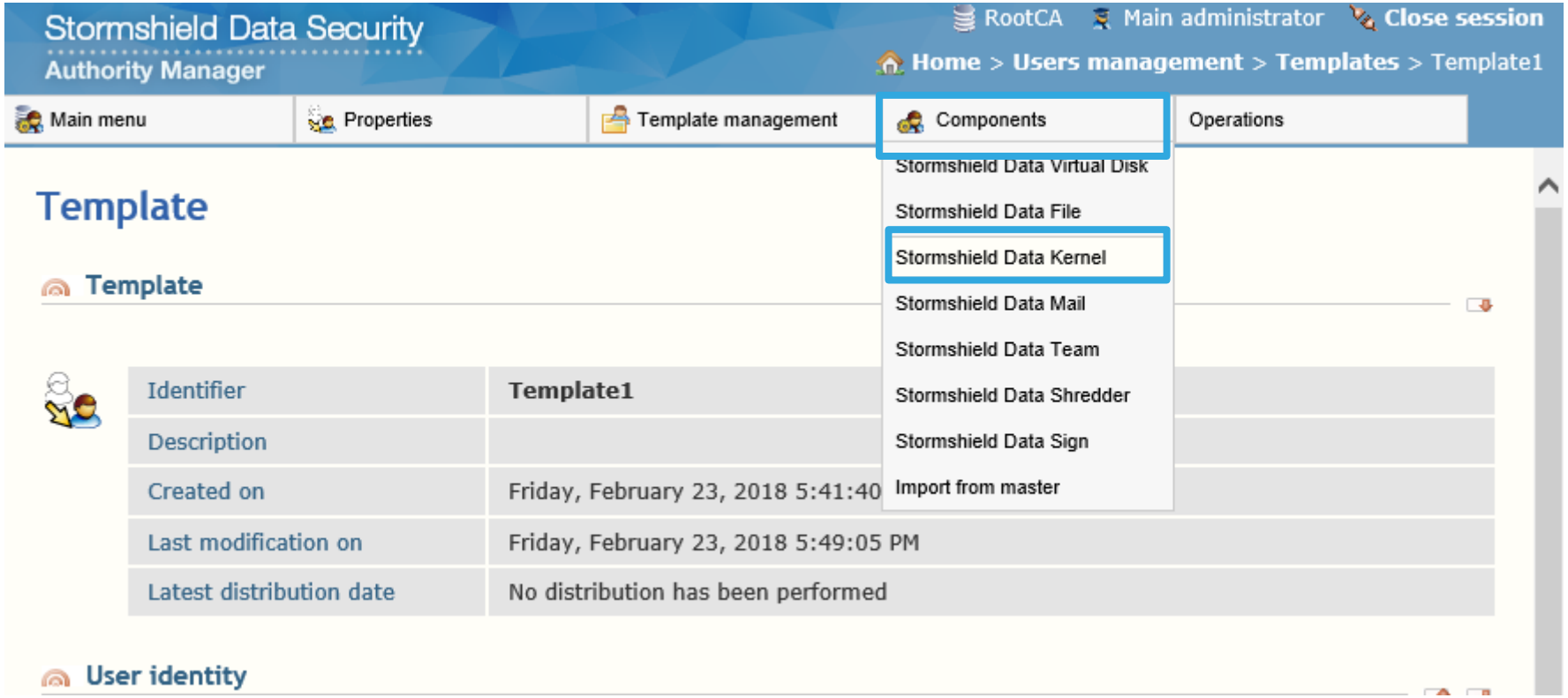
Select **Automatic update** and fill in the following value under the **Download** section:
http://%IP_SDAM:port/update/<UserId>/<UserId>.usx



Click on **Apply modifications**

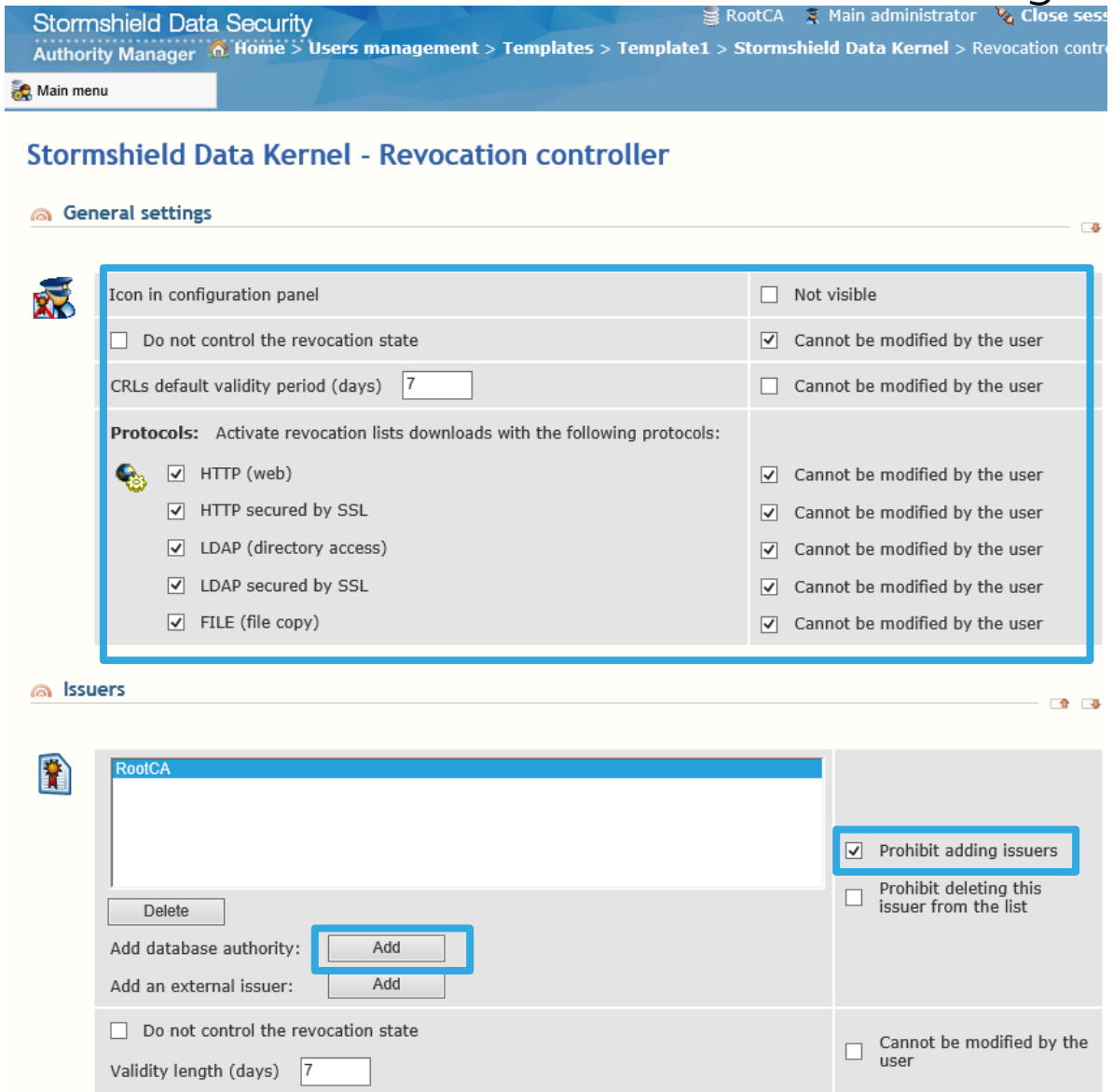
CRL configuration

Click on **Main menu → Users management → User template** and select the template that you have already created. Then click on **Components → Stormshield Data Kernel**.



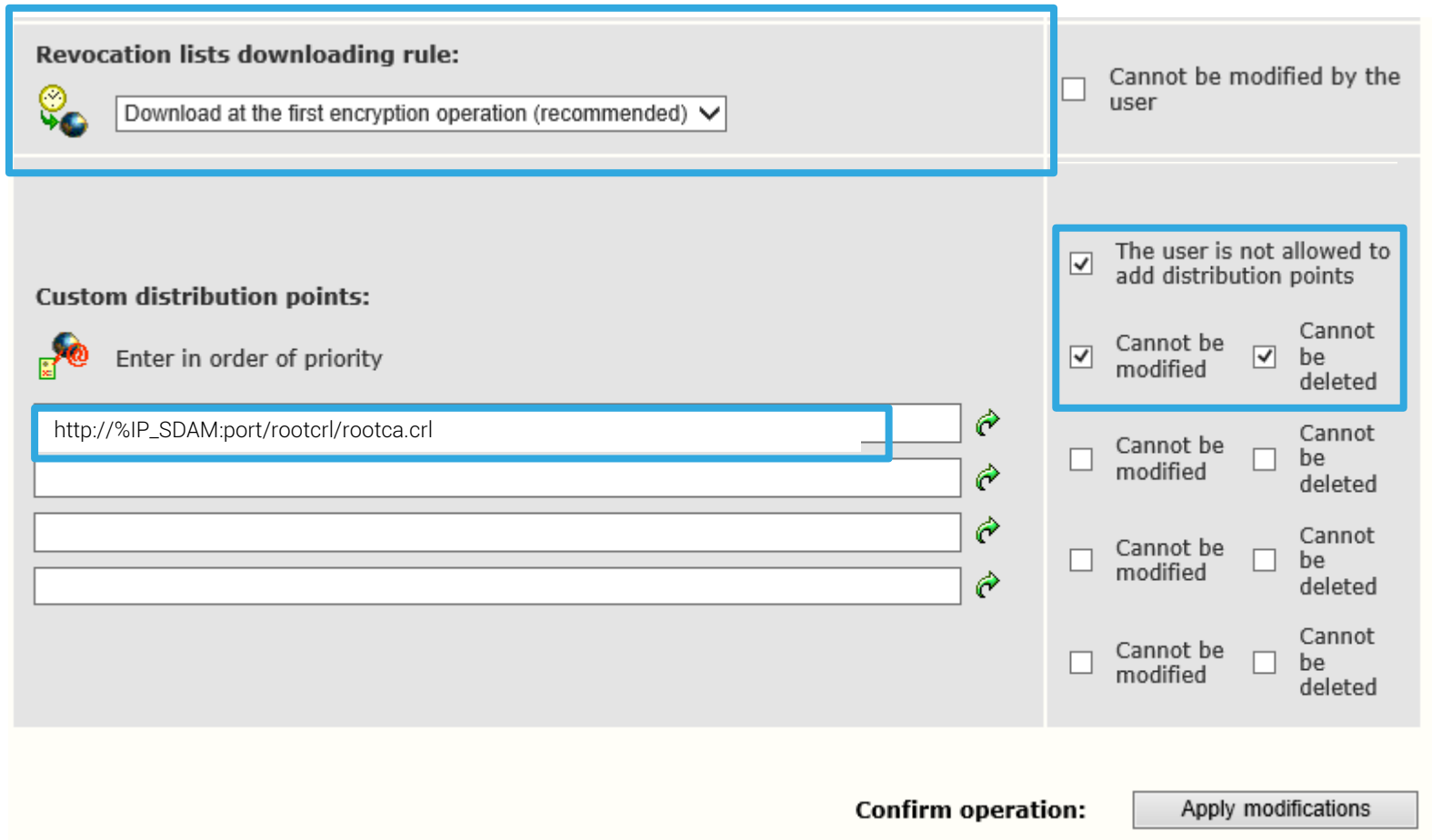
CRL configuration (continued)

Click on **Revocation controller** and click on the button highlighted below



CRL configuration (continued)

Add an external CRL distribution point: http://%IP_SDAM:port/rootcrl/rootca.crl

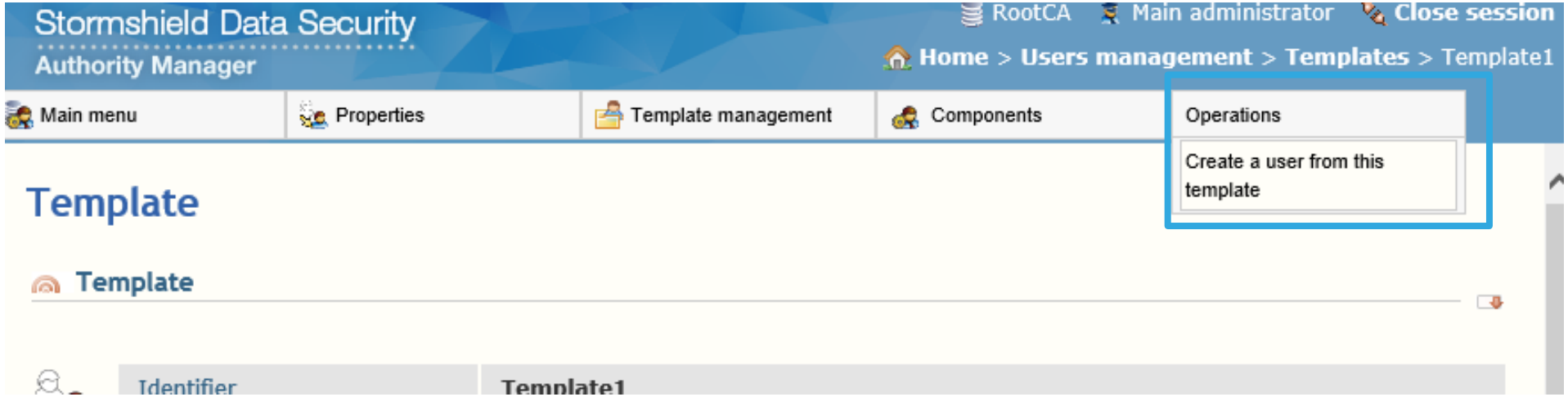


Creating SDS user accounts

Creating an account from a template

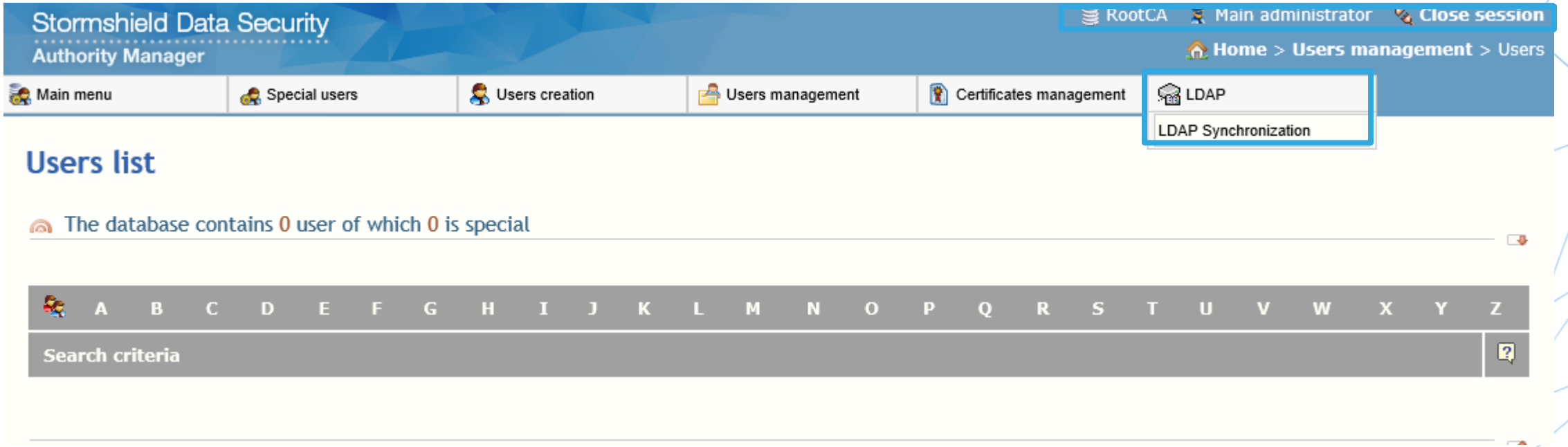
Click on **Main menu → Users management → User template** and select Template1, then click on **Operation → Create a user from this template**

This operation allows you to create a user manually on the SDAM but if you want to create a user from your Active Directory, please see the next slide.



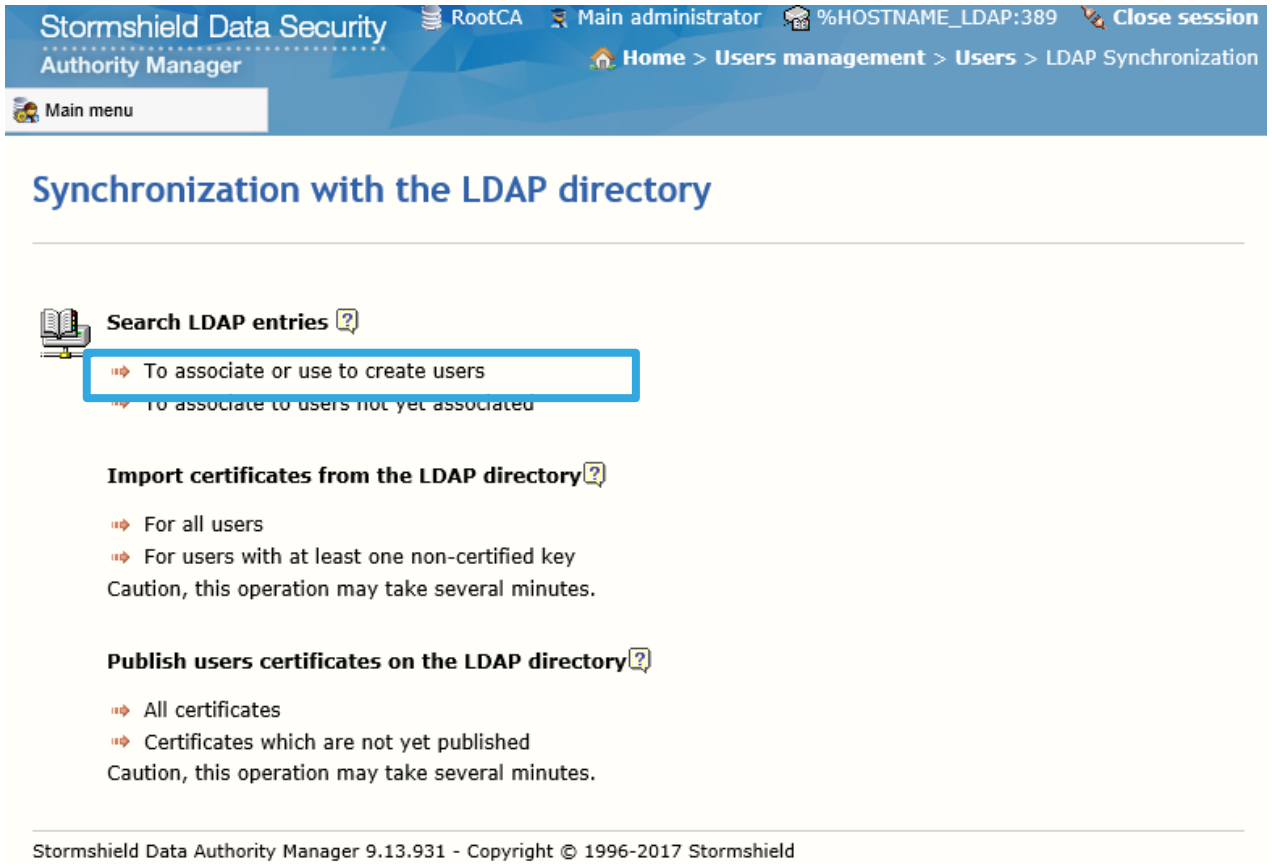
Creating users via LDAP

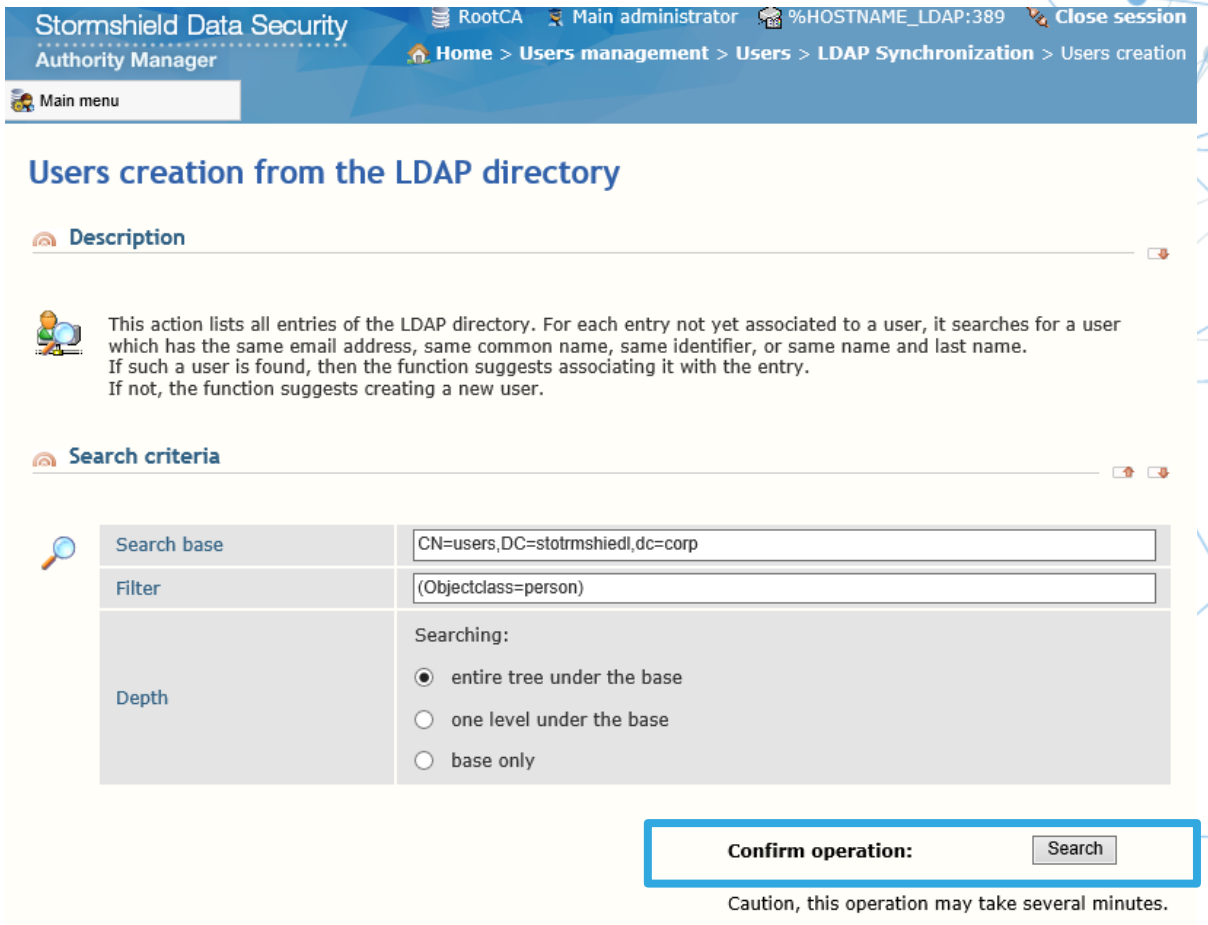
Click on **Main menu → Users → LDAP** and select **LDAP Synchronization**



Creating users via LDAP (continued)

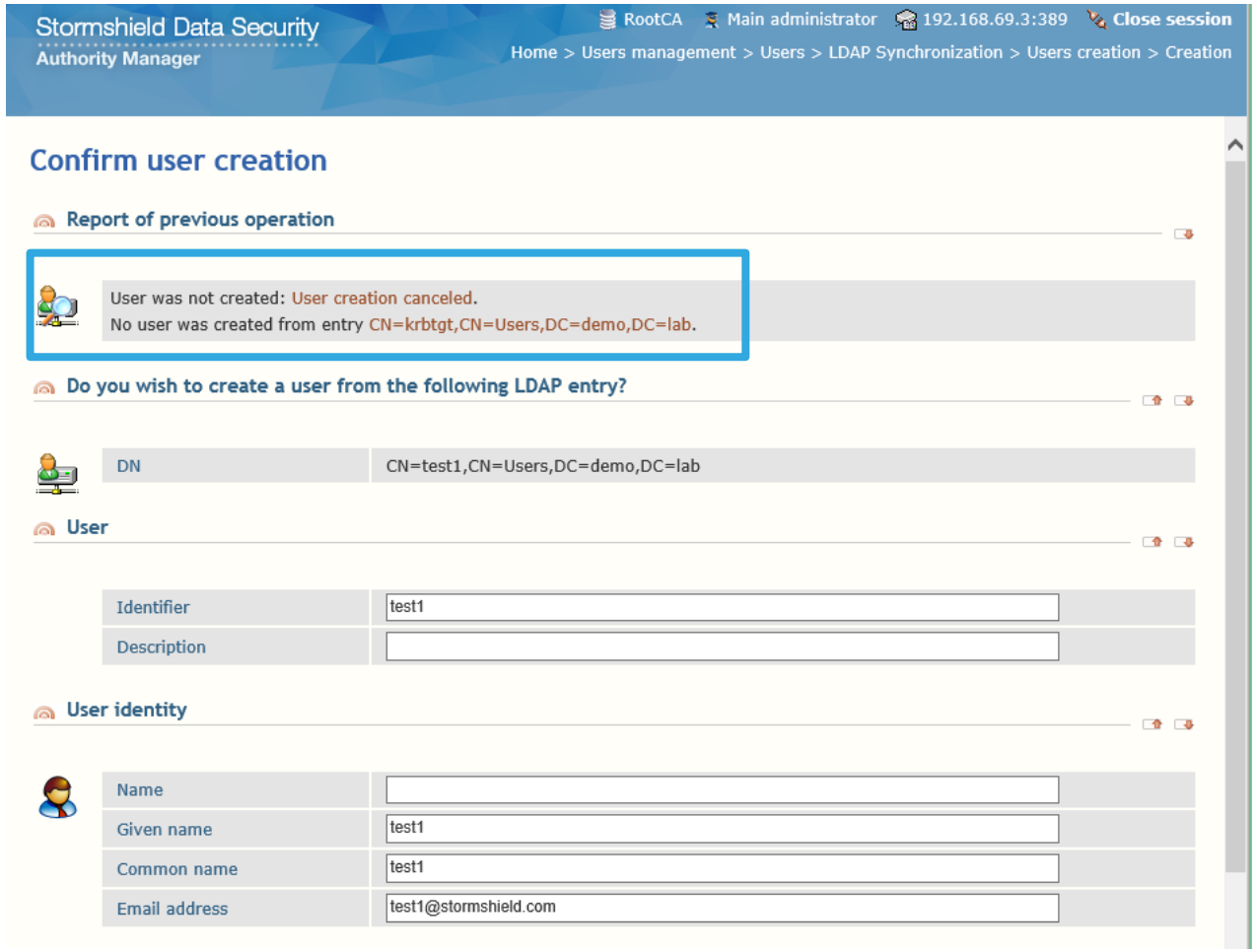
Click on To associate or use to create users

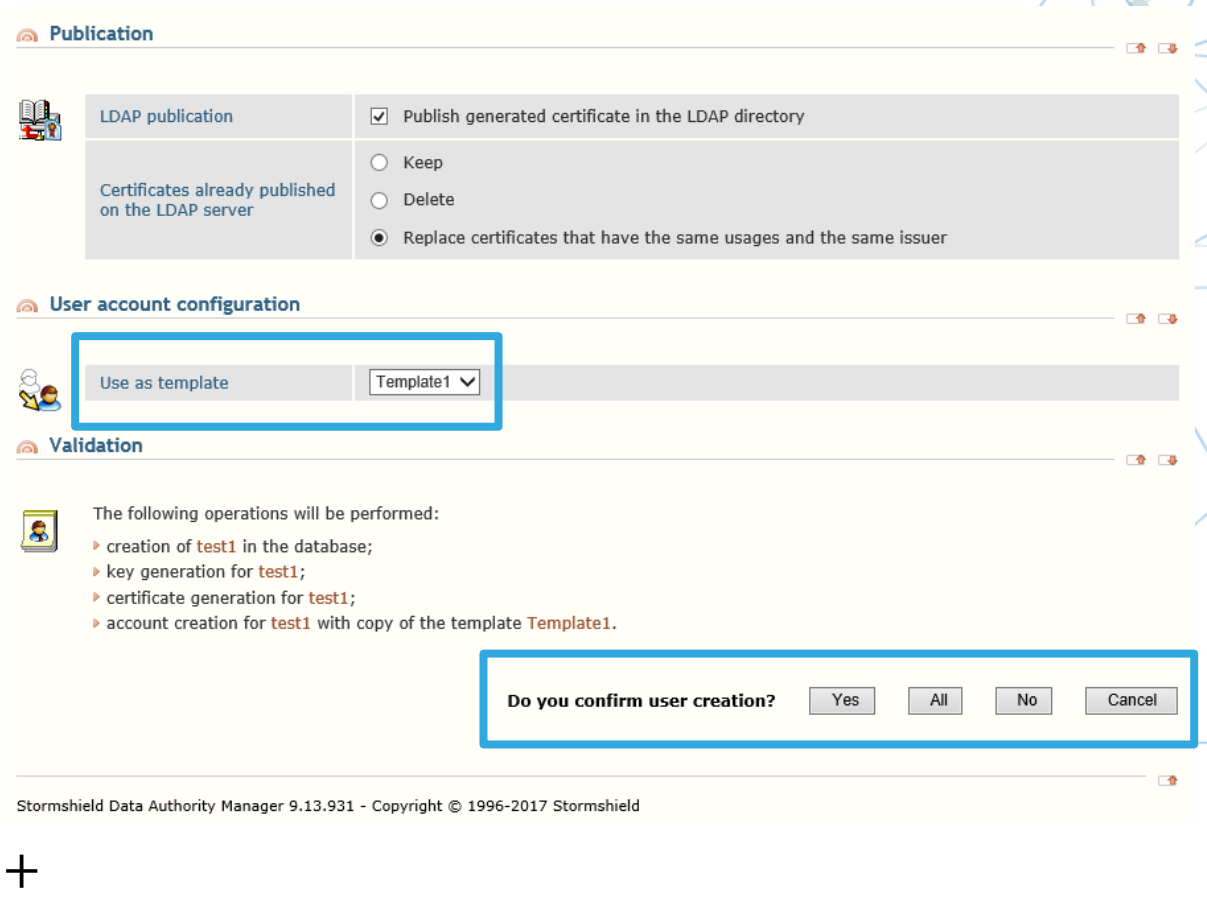




Creating users via LDAP (continued)

The SDAM interface will show you the first user found in the AD and will let you choose whether to create the same user in the SDAM.





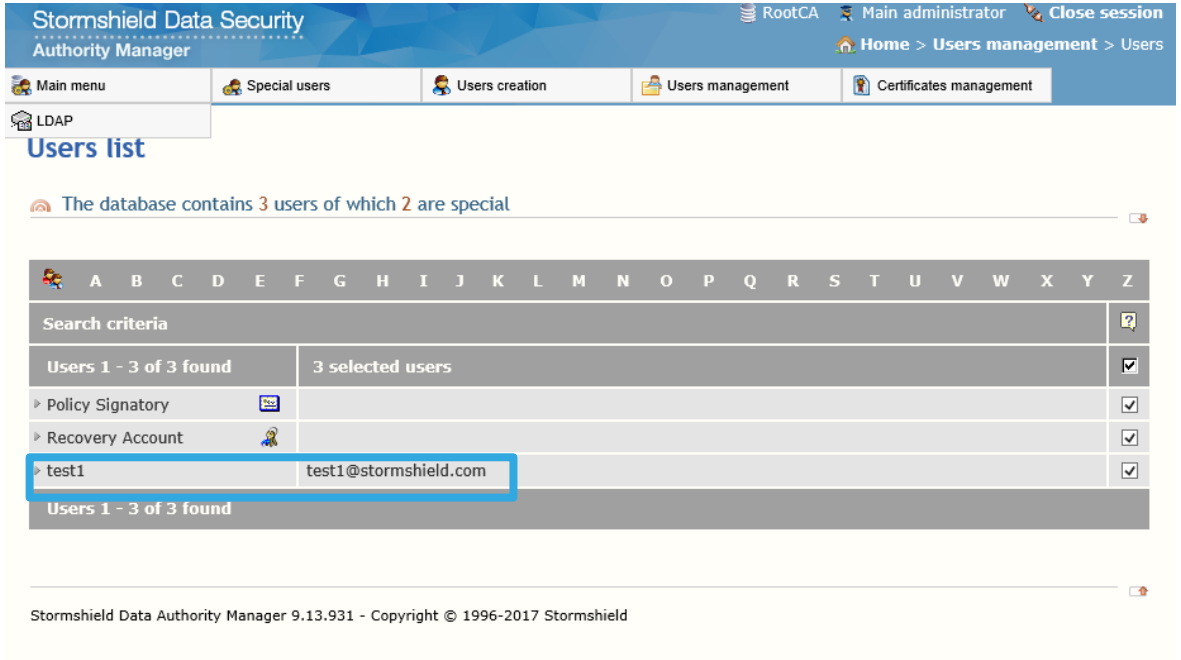
+

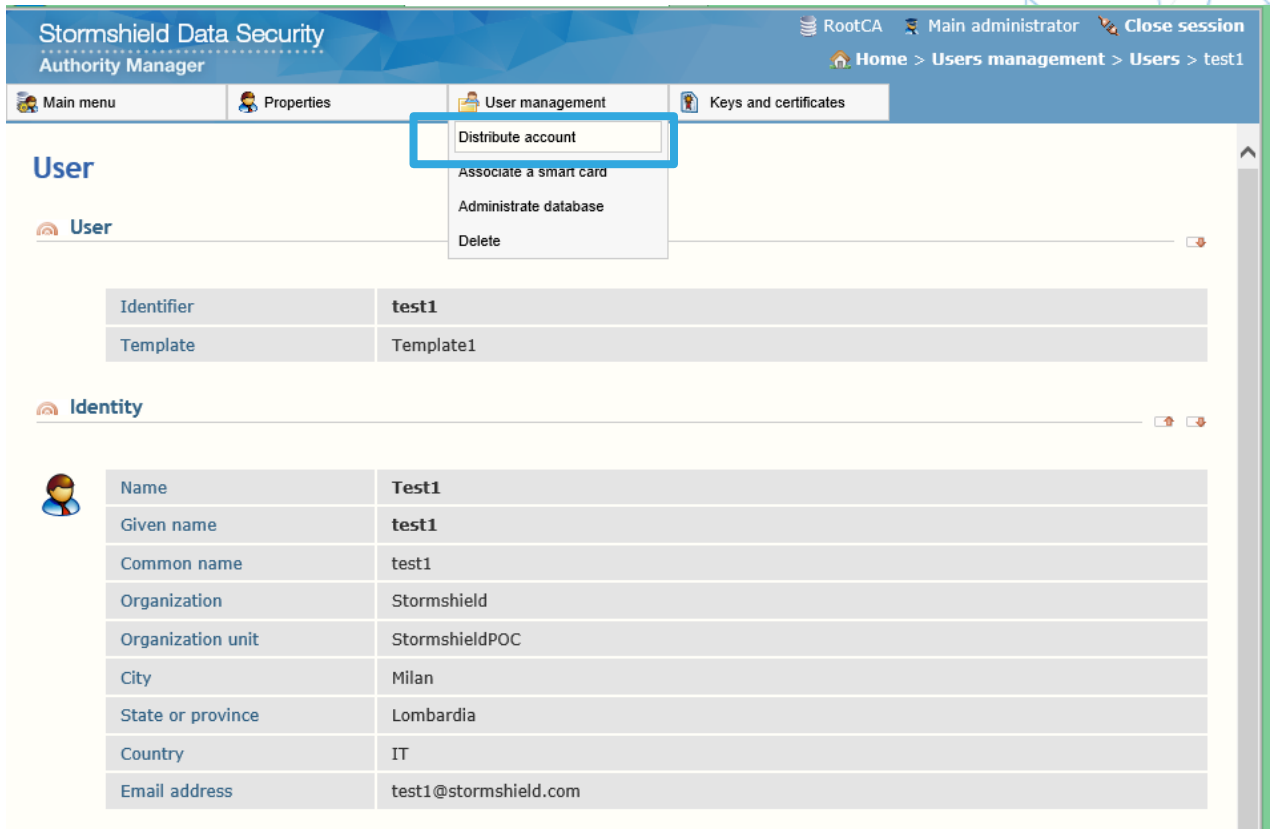
Deploying SDS user accounts

File distribution

After you have created the user, you can download/send the file relating to this user so that he will be able to install it on his workstation

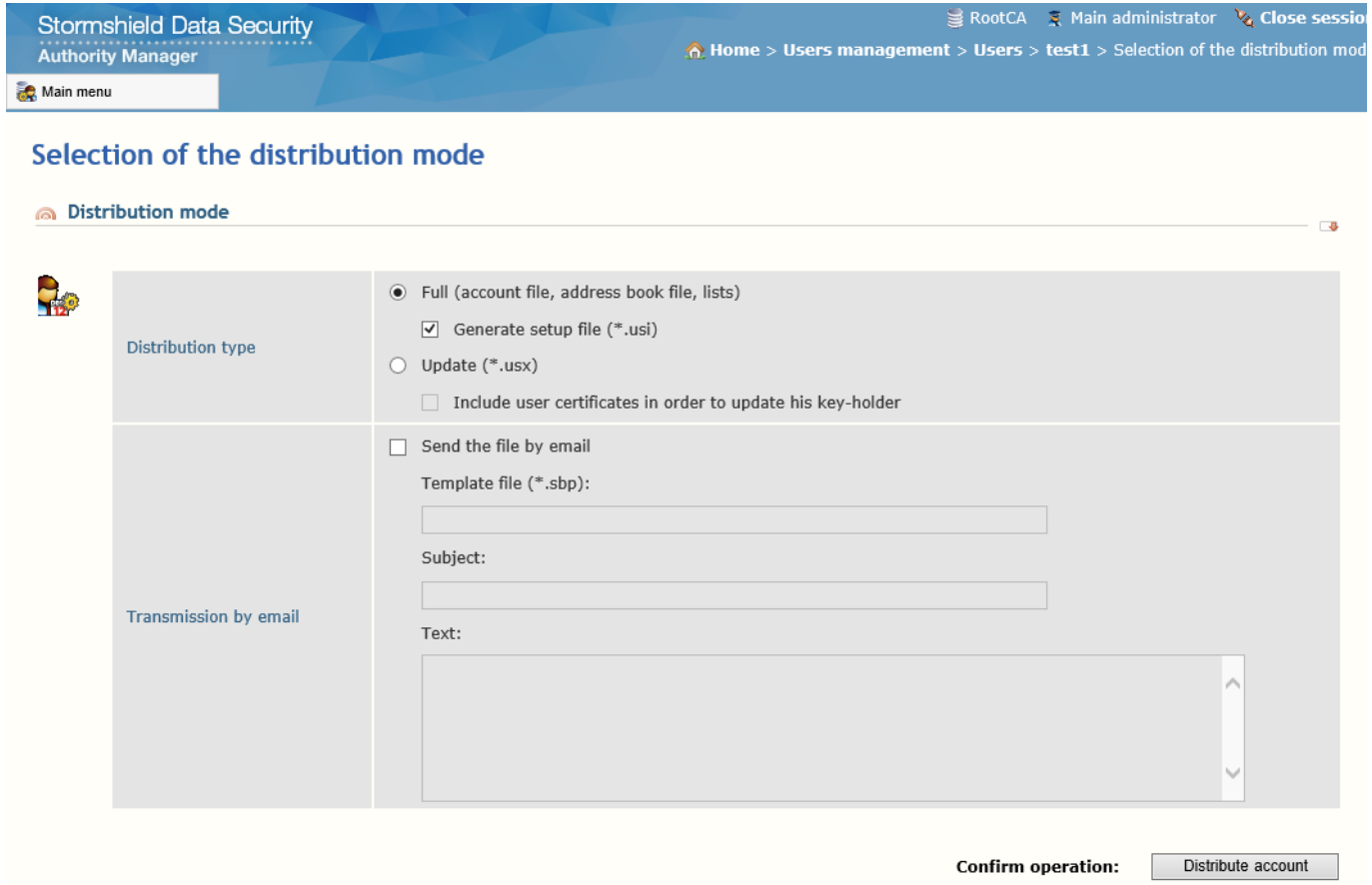
From the **Home** menu, click on **Users management** → **Users** → select the user (in this example "test1") → then **User management** → **Distribute account**





File distribution (continued)

Check the option **Generate setup file(*.usi)** then click on **Distribute account** (you can download the file from the SDAM server to C:\SBMData\rootca\Users\test1)



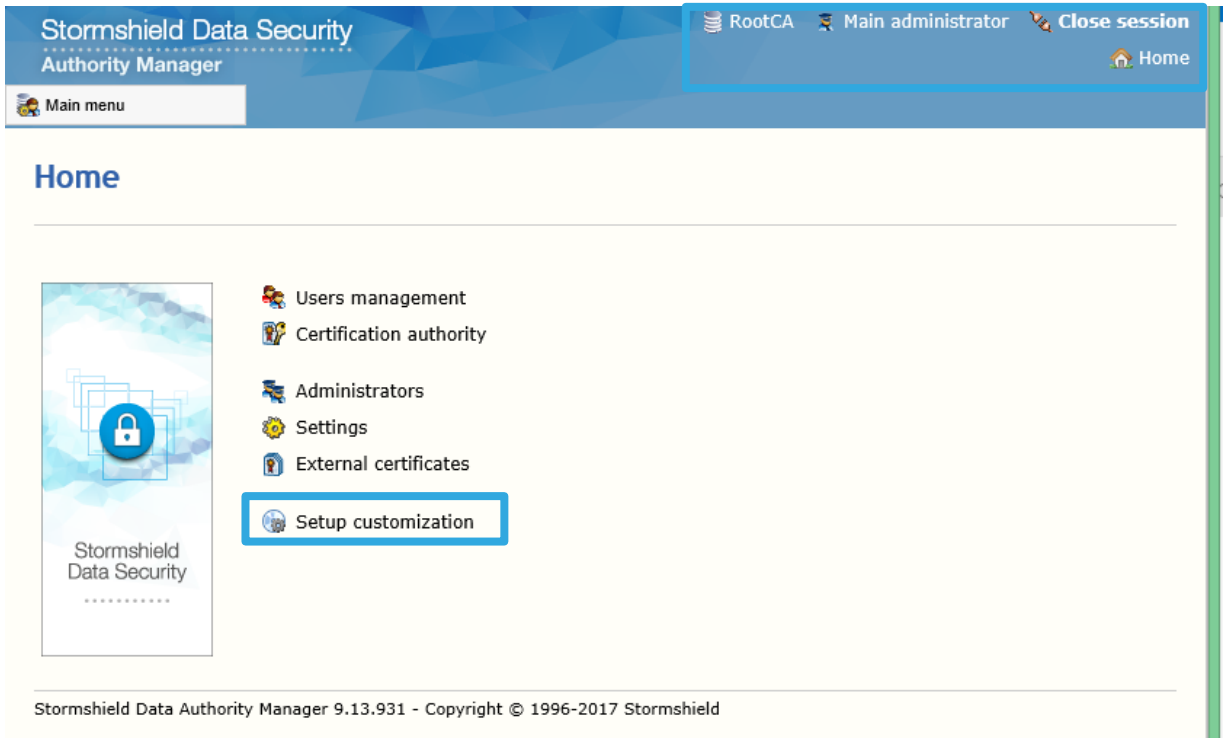
You can also choose to send the file by e-mail (optional) but you need to configure an e-mail server under
Home → Settings → Outgoing mail server

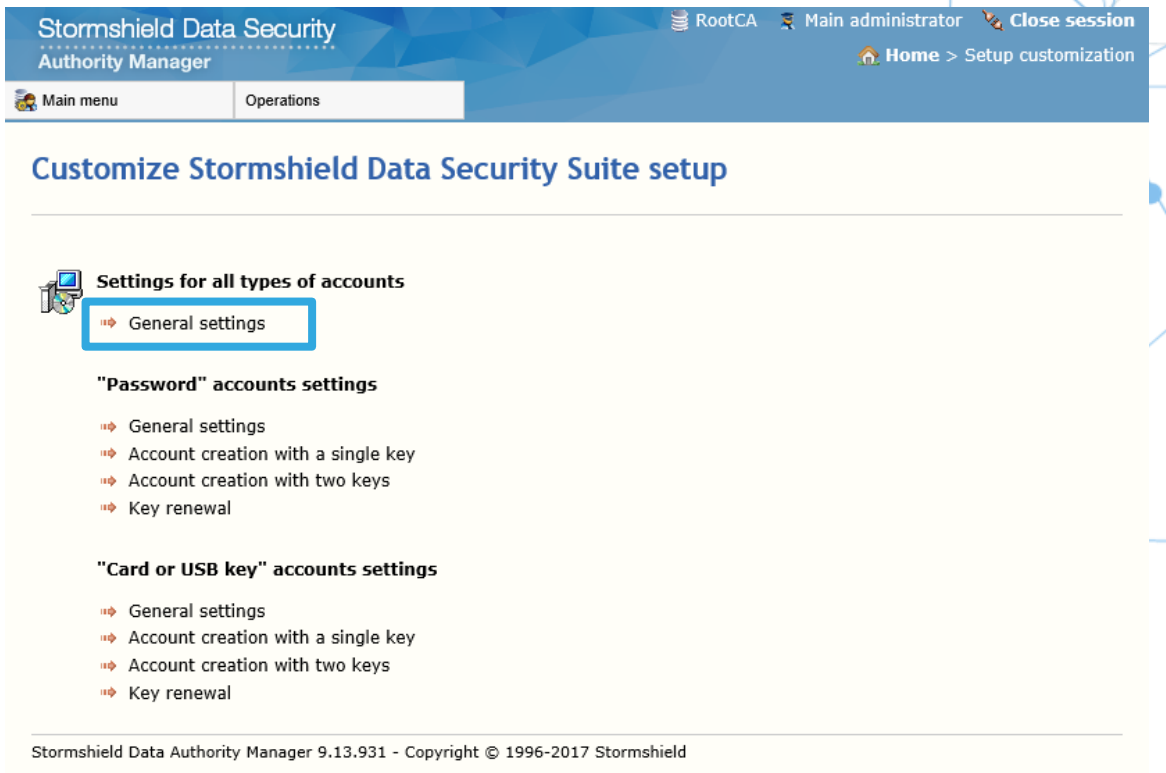
Installing the client workstation

Installing the client workstation

In this step you will create a custom setup file. From the **Home** menu, click on **Setup customization**.

In our case, we use only accounts protected by passwords with two keys.
We will therefore block the ability to create any local accounts other than these.





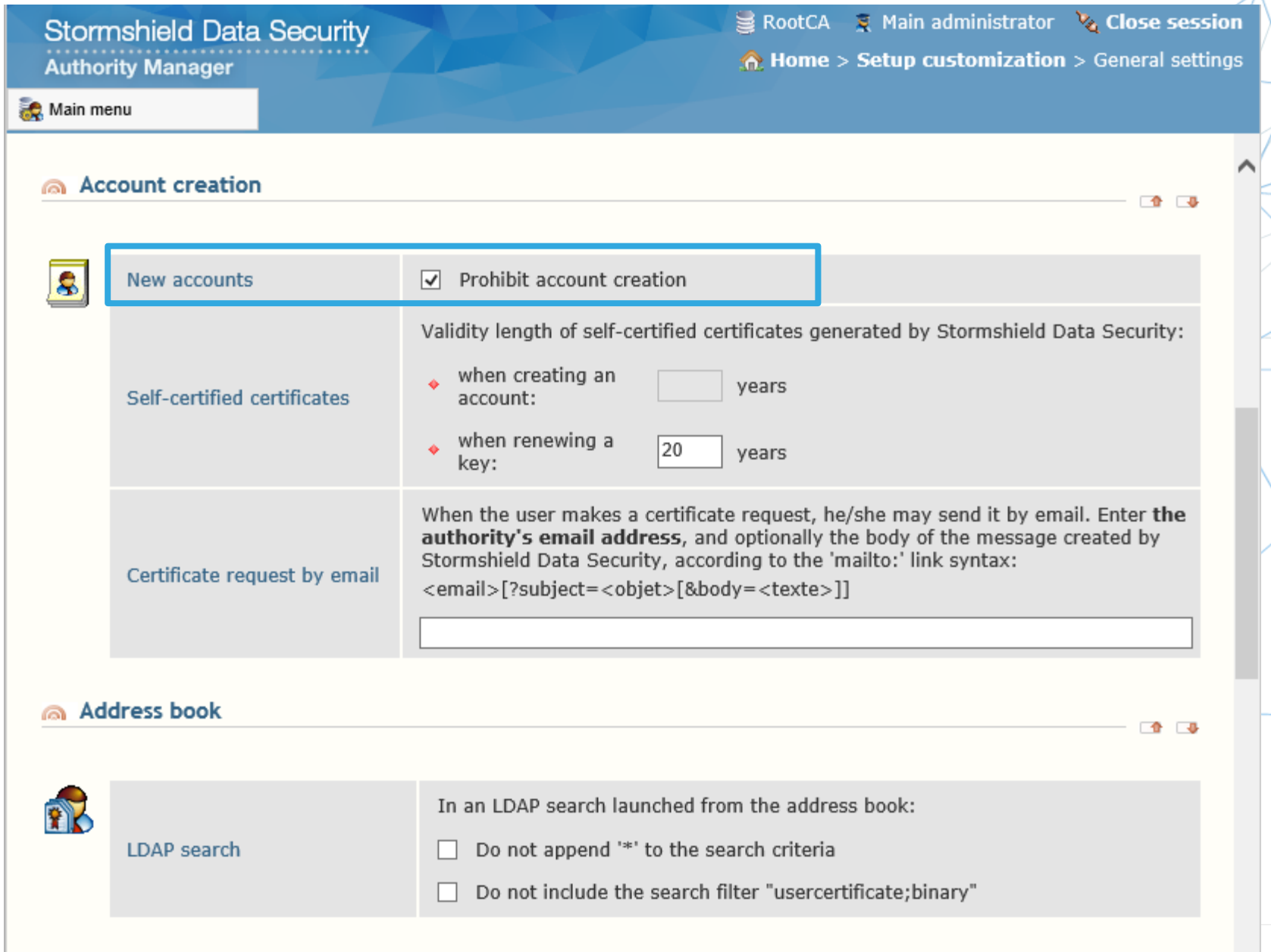
Configuring the setup

Allow only the use of password mode but not card mode

Configuring the setup (continued)

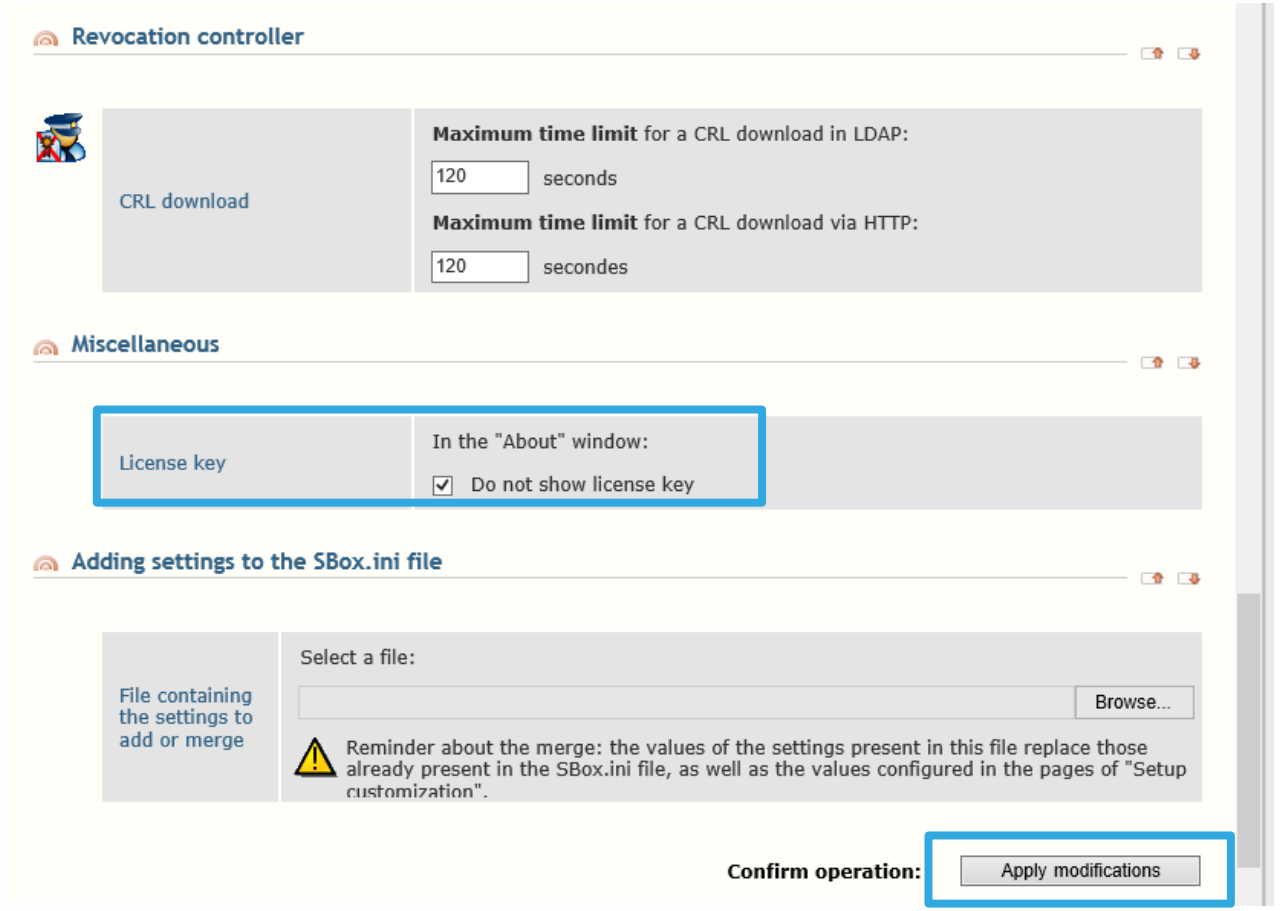
Check the option

Prohibit account creation



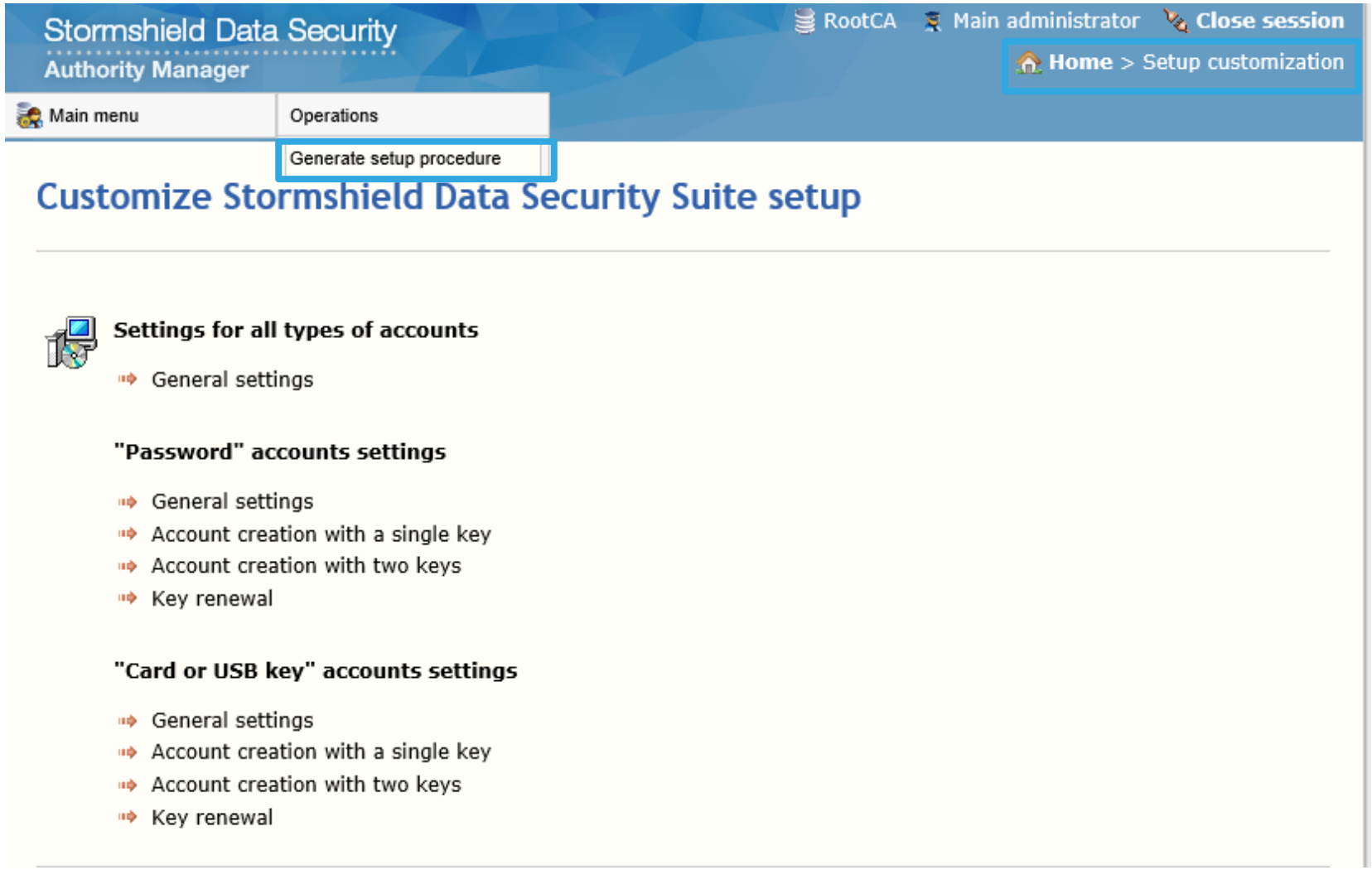
Configuring the setup (continued)

Go to the end of the **Stormshield Data Security Suite: General settings** configuration page. Check **Do not show license key** and then click on **Apply modifications**



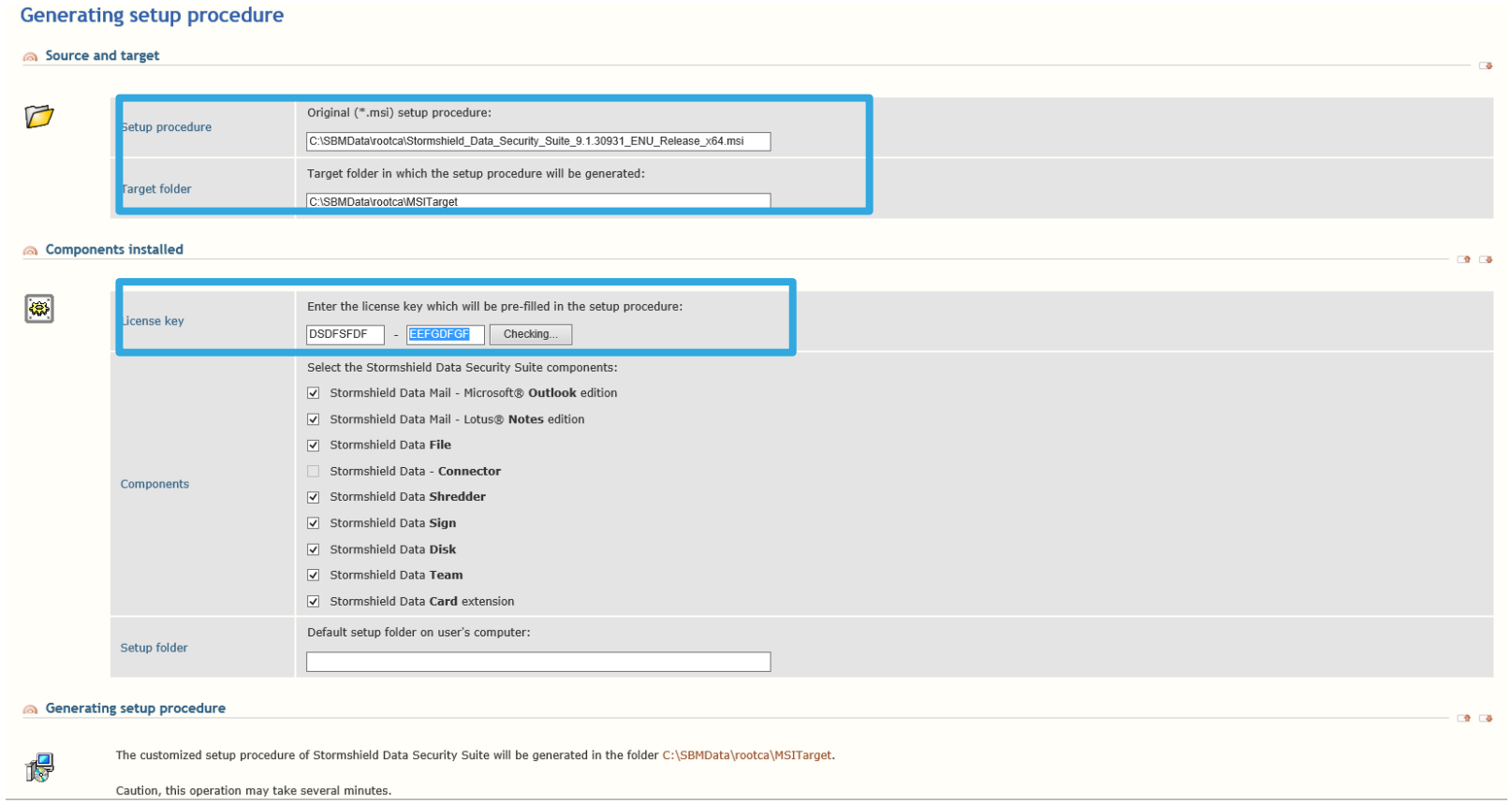
Generating the installation file

You will now create the customized *.msi* file by selecting
Operation → Generate setup procedure



Generating the installation file (continued)

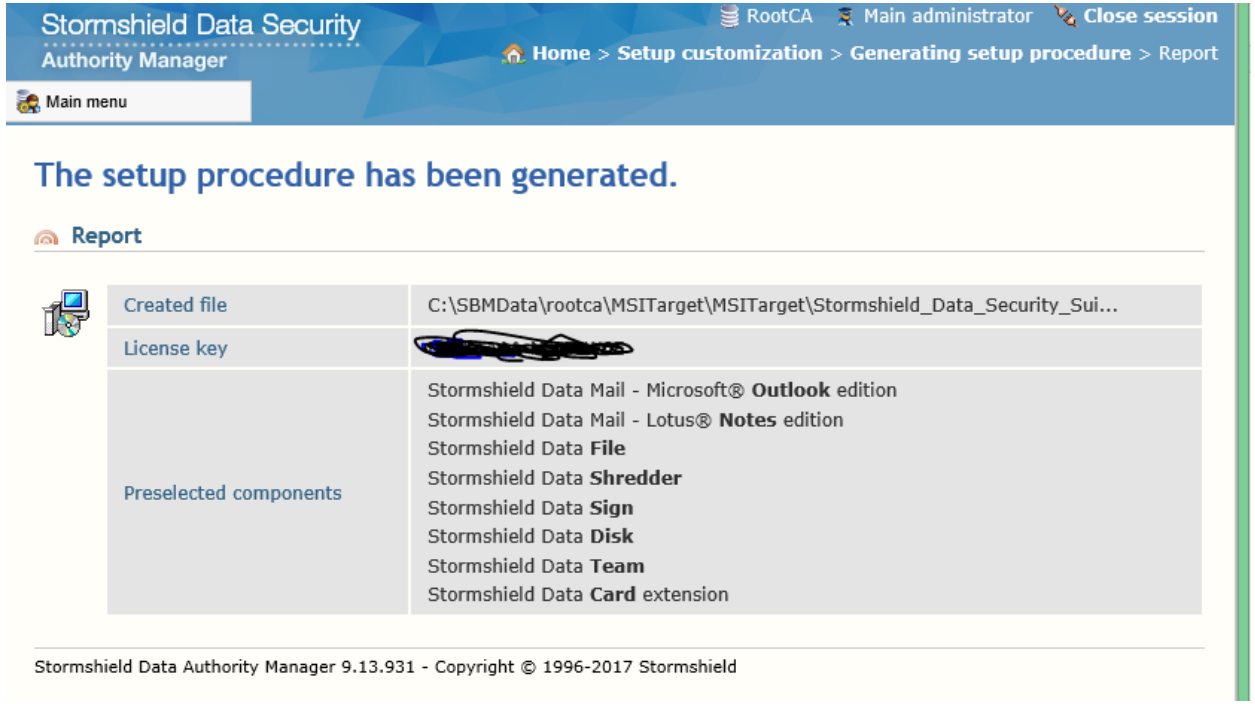
From MyStormshield, download the *.msi* file (for example Stormshield_Data_Security_Suite_9.1.30931_ENU_Release_x64.msi) and copy it to the Windows server on which you have installed the SDAM (in this example, under C:\SBMData\rootca)

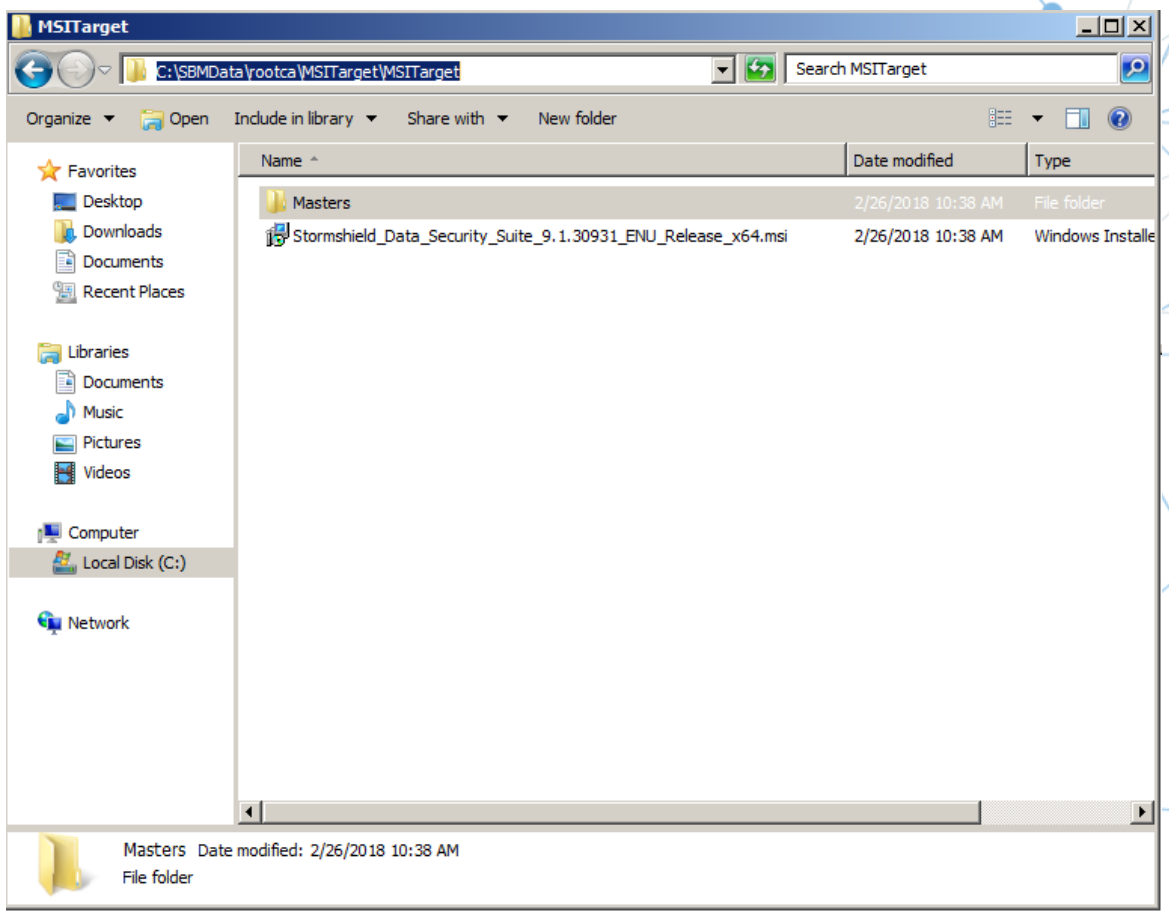


Click on **Generate setup procedure**

Downloading the *.msi* file

Once it has been generated, you will get this page from the SDAM, and you will then be able to download the customized *.msi* file from the folder C:\SBMData\rootca\MSITarget\MSITarget





You can rename the customized setup file if you wish to, for example **Custom_SDS_file.msi**

Installing the *.msi* file

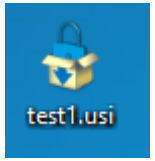
In order to install the *.msi* file on a workstation, you can enter this command in a command prompt with administration privileges

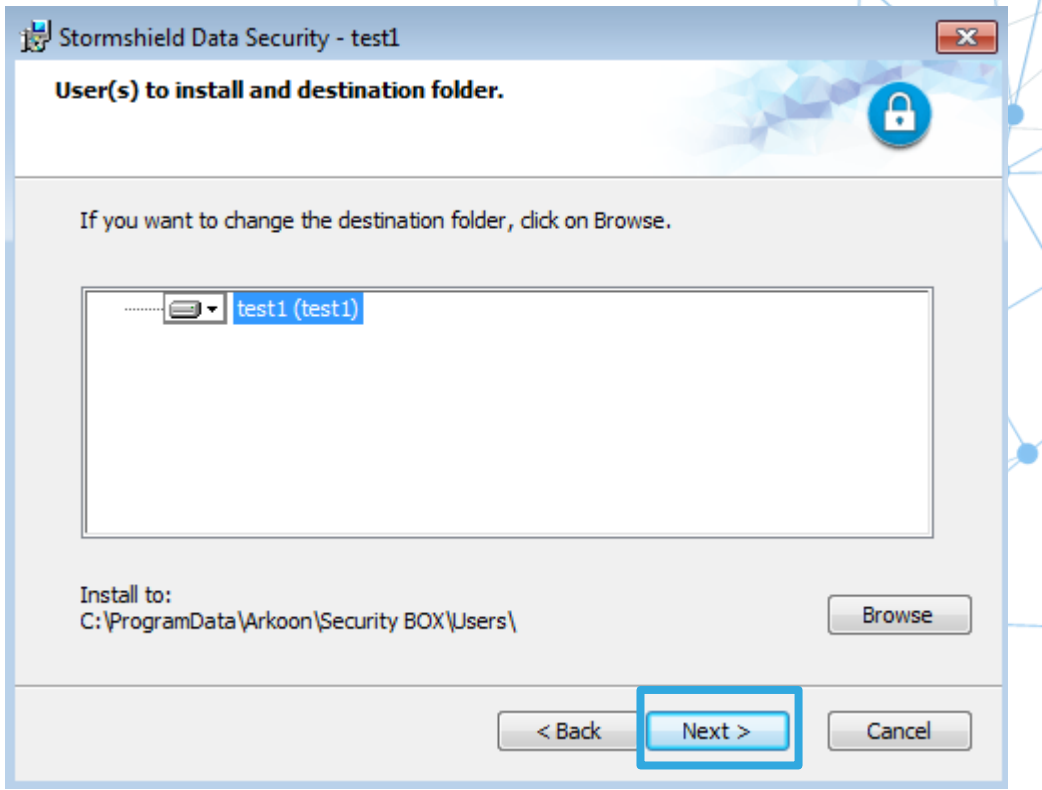
Msiexec /I "C:\Custom_SDS_file.msi" /qb+

Installing the SDS account

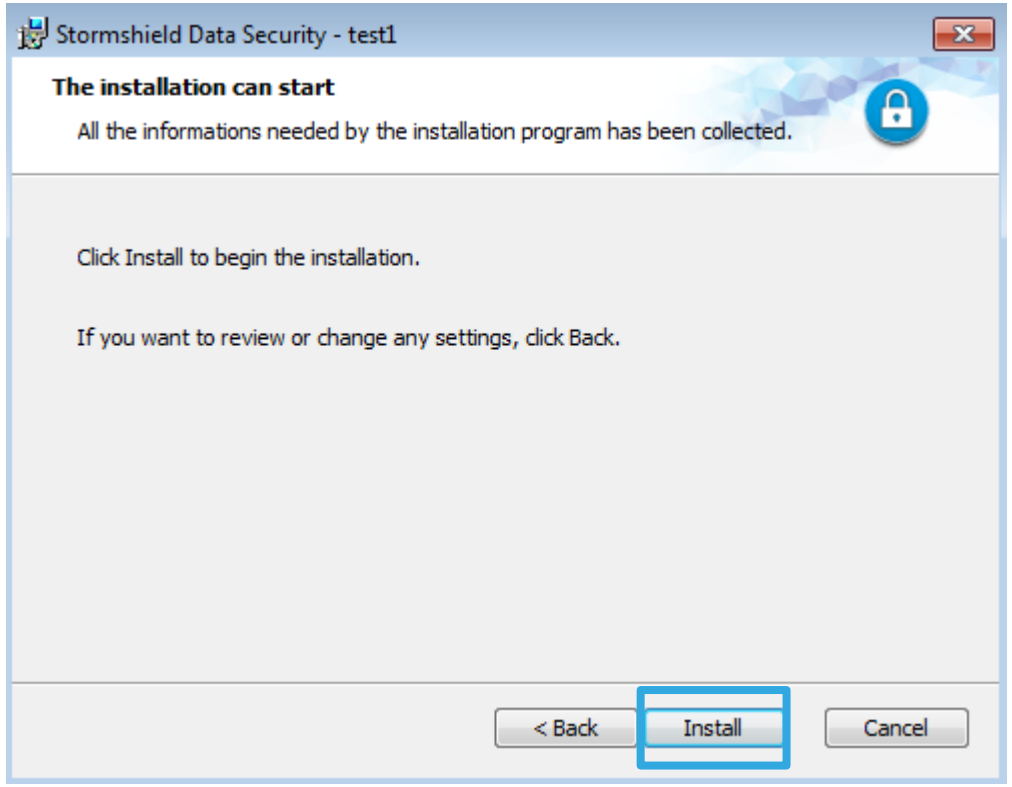
Installing the SDS account

Retrieve the user file from the server in the following folder:
C:\SBMData\rootca\Users\test1





Installing the SDS account (continued)



Initial connection

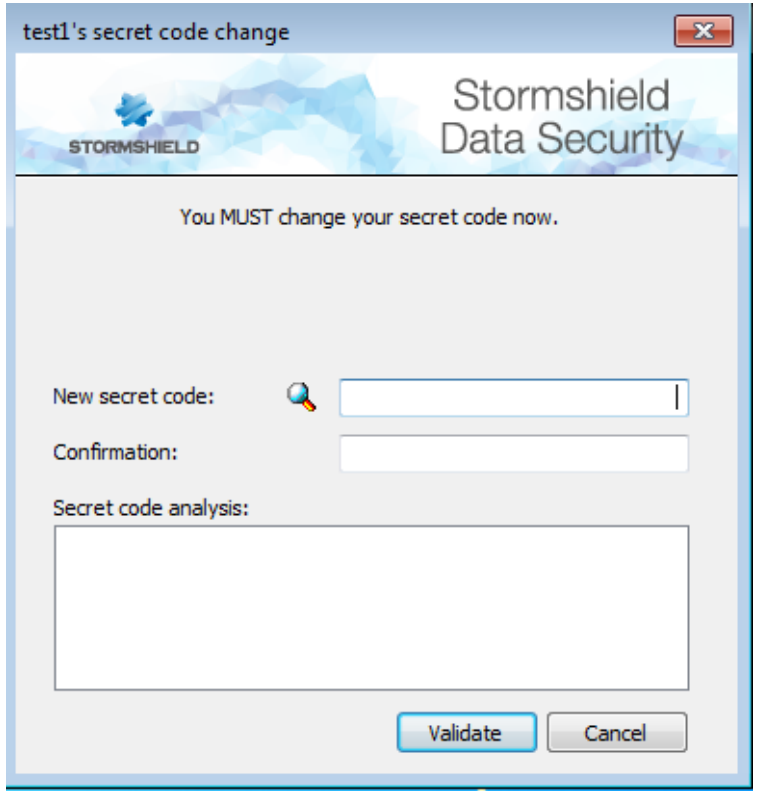
Initial connection

The user icon displayed on the left indicates that the account exists on the workstation.

Enter the user's initial password. After the initial connection, the user will be asked to change his initial password.

In order to get the initial password, you need to go to the SDAM, search for the "test1" user, and click on

Properties → **Password** and see the **Initial password** field.



Set the new password

Use case - Demonstration

Mail module

- Sending an encrypted e-mail internally
- Receiving an encrypted e-mail internally
- How to send an encrypted e-mail outside the network
  - %USERNAME_CLIENT1 sends a signed e-mail to %USERNAME_CLIENT2
  - %USERNAME_CLIENT2 receives a signed e-mail and imports the certificates into the directory
  - %USERNAME_CLIENT2 sends an encrypted e-mail to %USERNAME_CLIENT1

Disk module

- Manually creating a disk volume on the computer %HOSTNAME_CLIENT1 with an automatic mount

- %USERNAME_CLIENT1 manually creating a disk volume on a USB drive shared with %USERNAME_CLIENT2 with manual editing

Team module

- Creating a local rule for yourself in a confidential directory on %HOSTNAME_CLIENT1's workstation

- %USERNAME_CLIENT1 creating a shared rule in a confidential directory on the file server with %USERNAME_CLIENT2 from the workstation %HOSTNAME_CLIENT1

File module

- %USERNAME_CLIENT2 encrypting a document with a password for external use
- Sharing the password-protected document with someone who does not have the SDS solution
- Going to the Mystormshield.eu website to download the SDS SmartFILE Reader software
- https://www.stormshield.com/wpcontent/uploads/2016/09/SmartFile_Reader.zip

Support

Contacts

- For assistance on the ongoing POC:

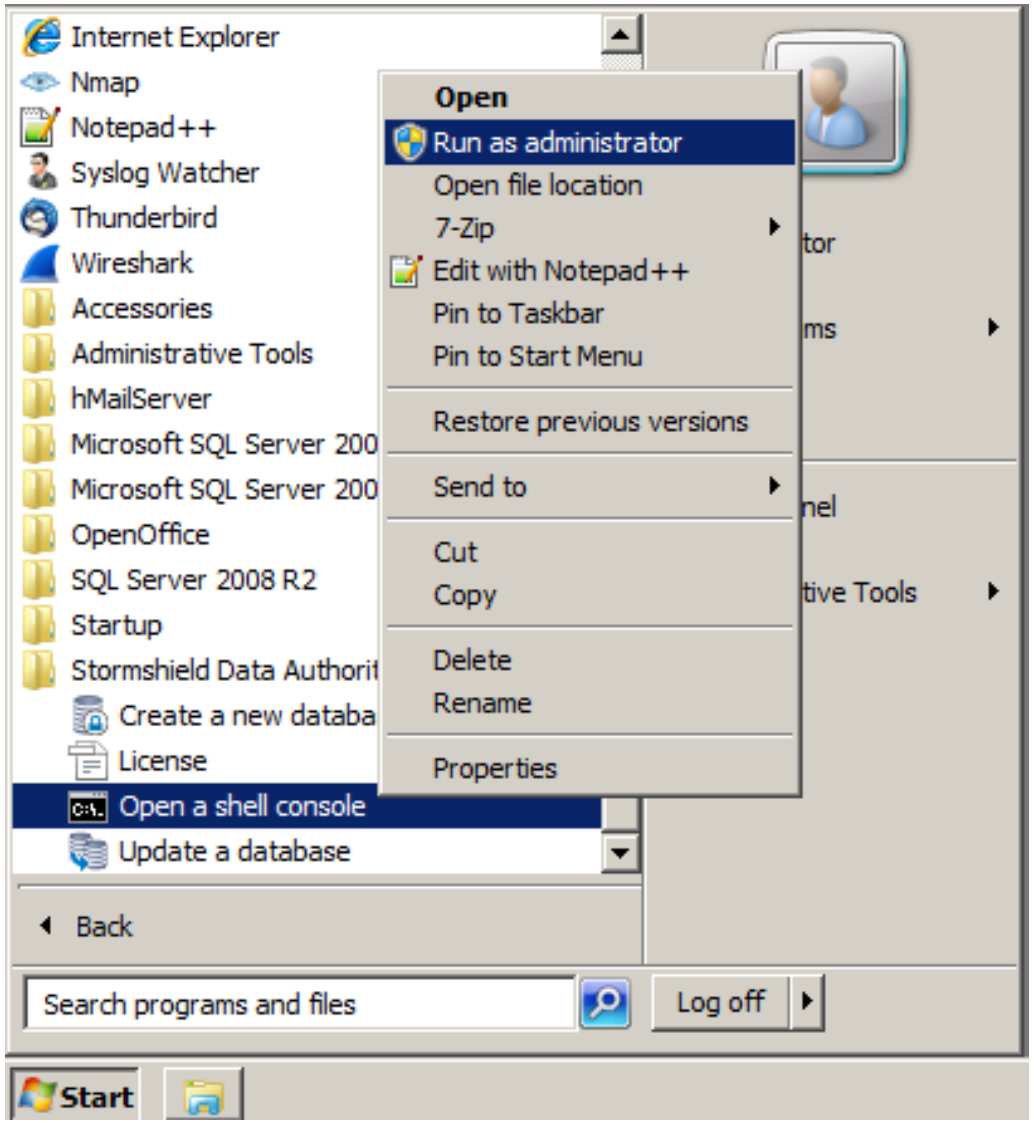
- If you are a partner and have an EVALUATION license:
  - You can contact your local Stormshield pre-sales engineer directly

- If you are a partner and have an NFR license (Not For Resale):
  - You can contact Stormshield Support directly

- If you are a customer (solution with permanent license under a valid maintenance contract):
  - You already have access to your integrator's support department
  - You already have access to Stormshield Support

Starting up the SDAM server database

How to start up the database if I shut down the SDAM server



- In the command line with administrator privileges, run this command in order to start the DB *C:\Program Files (x86)\Arkoon\Security BOX Authority Manager\Tools> SBMSTART.exe /o*

- Run *SBMSTART.exe /?* to get all the options of this command

STORMSHIELD

COLLABORATIVE SECURITY

Network Security

Endpoint Security

Data Security