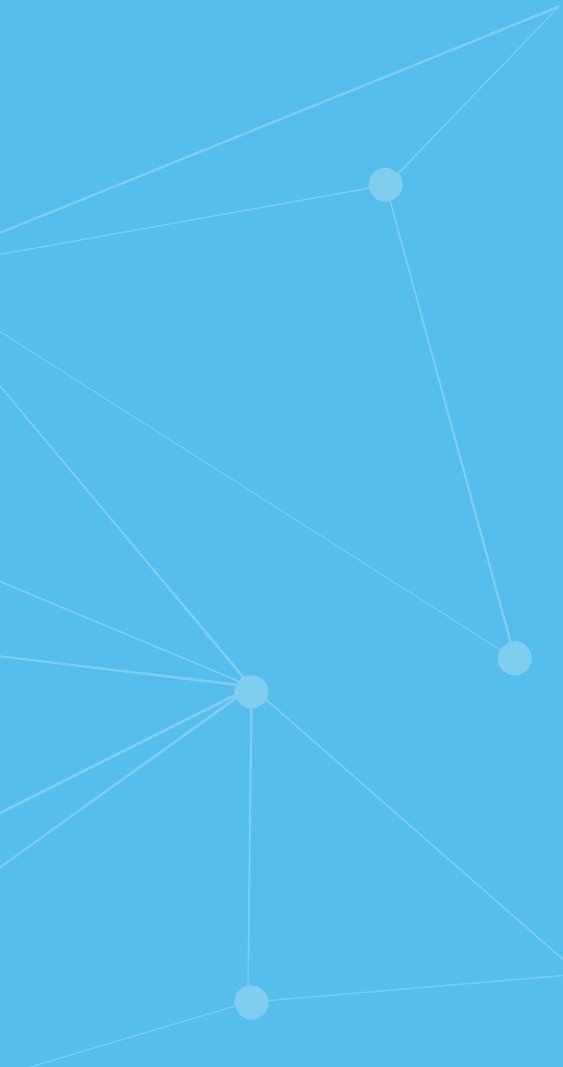




STORMSHIELD

Network Endpoint Data



QUICK START GUIDE SDS Enterprise 9.1.X

Stormshield Data Security Enterprise

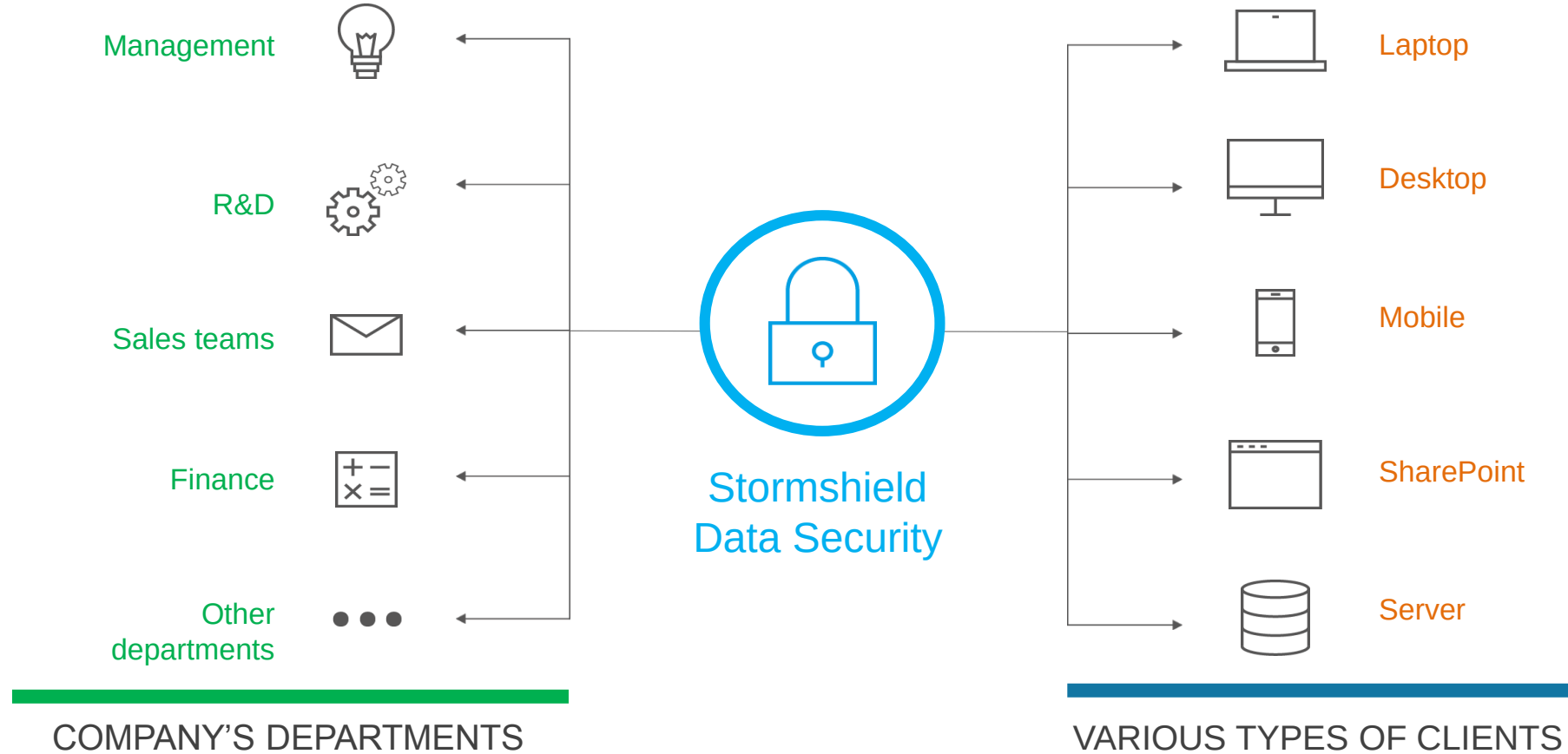
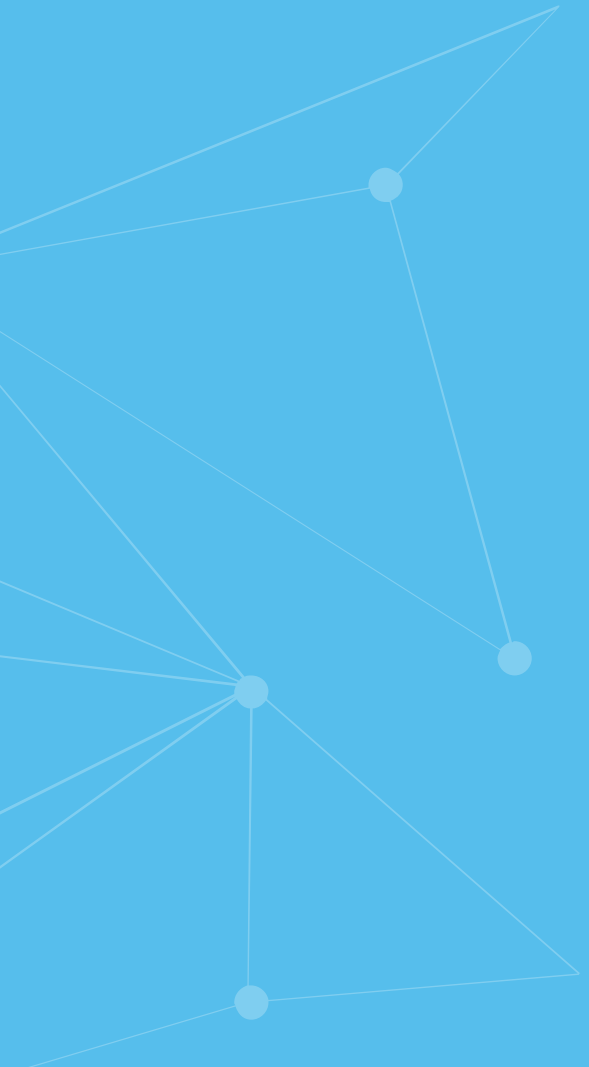


Table of contents

- [Introduction](#)
- [Technical requirements](#)
- [Architecture of the POC](#)
- [Installing the IIS server](#)
- [Installing the SDAM server](#)
- [Installing SDS Suite on the administration workstation](#)
- [Creating the root PKI](#)
- [Configuring Internet Explorer and initializing the root PKI](#)
- [Initializing a child PKI \(option\)](#)
- [Configuring the IIS server virtual directory](#)
- [Configuring the Exchange server \(option\)](#)
- [Creating special SDS accounts](#)
- [Setting up SDS account configuration](#)
- [Creating SDS account templates](#)
- [Creating SDS user accounts](#)
- [Deploying SDS user accounts](#)
- [Installing the client workstation](#)
- [Installing the SDS account](#)
- [Initial connection](#)
- [Use case – Demonstration](#)
- [Support](#)
- [Starting up the SDAM server database](#)





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
- SDS_e: SDS Enterprise version
- SGBD: Database Management System
- SMTP: Simple Mail Transfer Protocol
- USI: SDS_e account installation file format
- USX: SDS_e 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

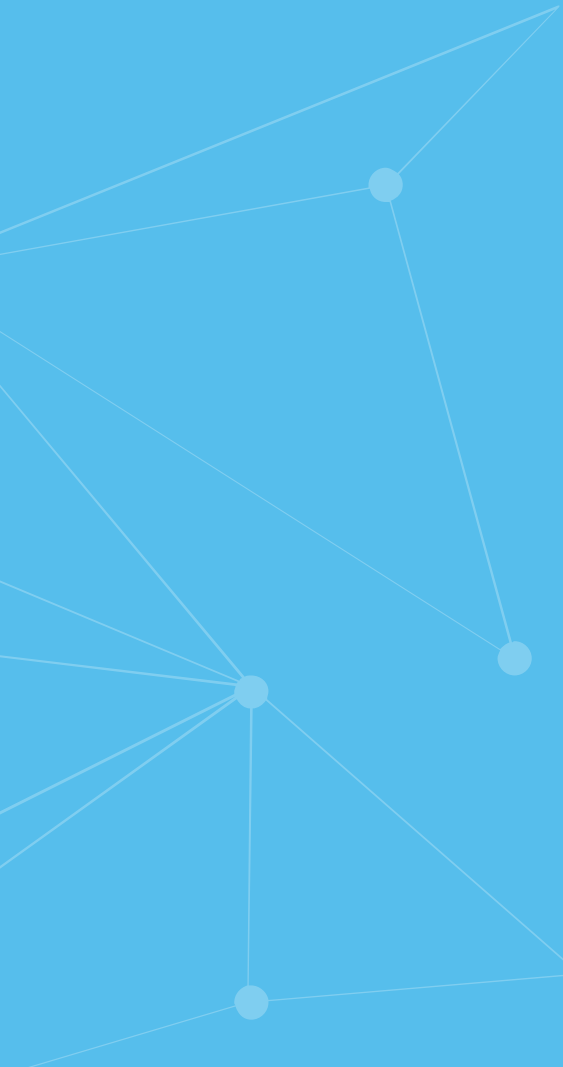
- The purpose of this document is to guide end users or partners in understanding the installation, configuration and use of SDSe.
- This is the quick start guide to establish a POC (Proof of Concept), and it gets to the basics to help you quickly understand how SDSe runs.
- It does not deal with all 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

Outlook 2016

No prerequisites



ACTIVE X (mandatory)

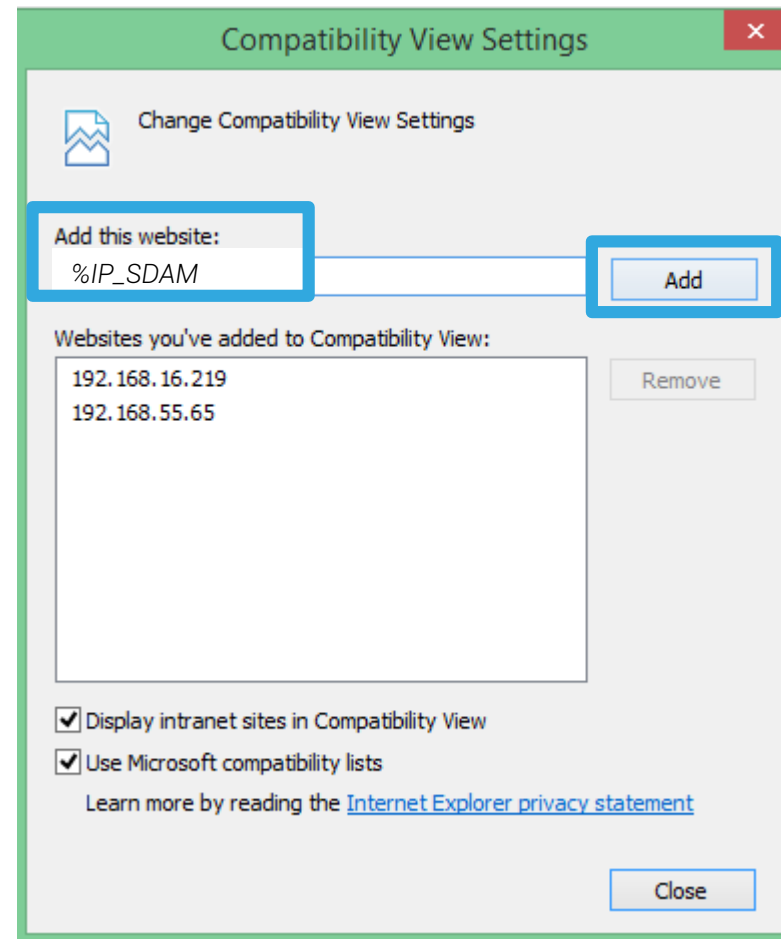
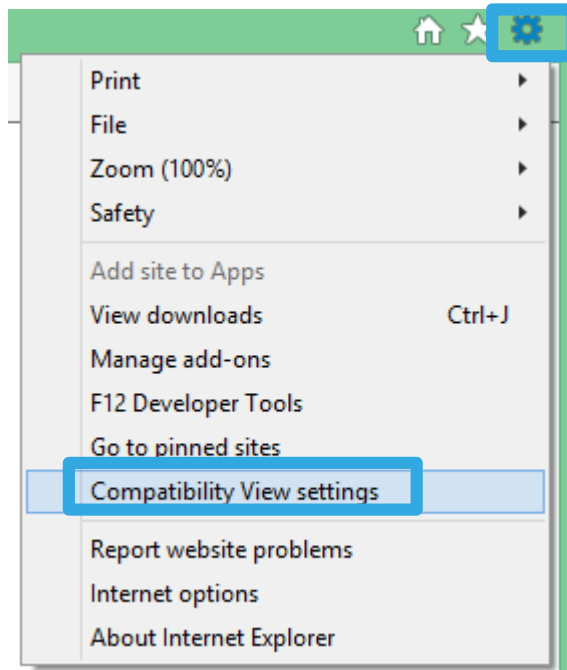
- Only for administration and administrators of the SDAM solution.
- To access the SDAM web interface, the workstation must be able to install an unsigned ActiveX (signed by Stormshield but not Microsoft).
- The SDAM URL must be declared as a trusted site in IE.
- Administrator privileges are required 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).



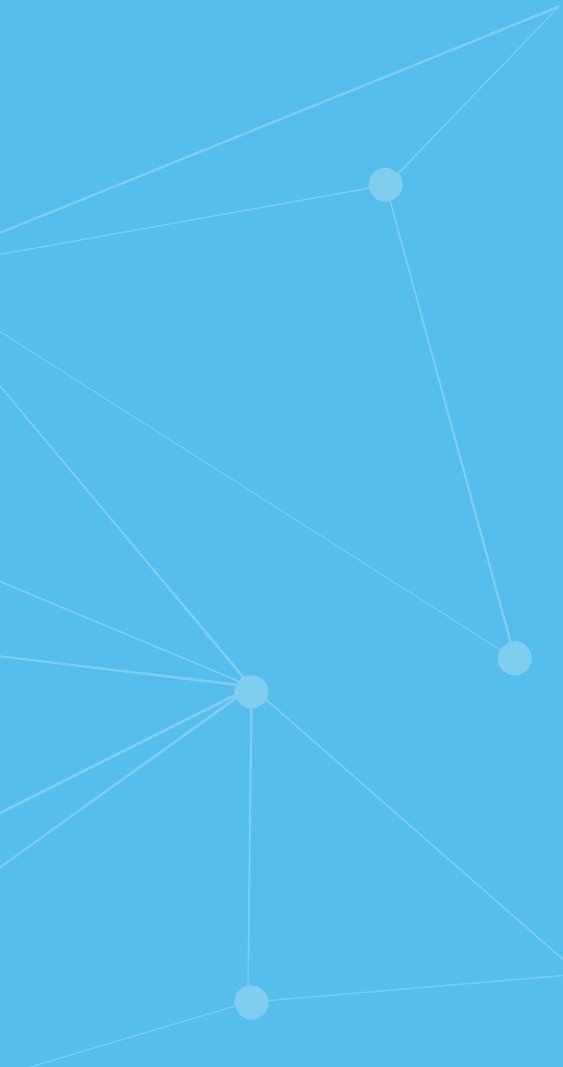
SMTP ACCESS (optional)

- 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 / Idap/ PKI – 1CA)
Windows 2012 R2



%IP_SDAM
%HOSTNAME_SDAM

%IP_CLIENT1
%HOSTNAME_CLIENT1
%USERNAME_CLIENT1



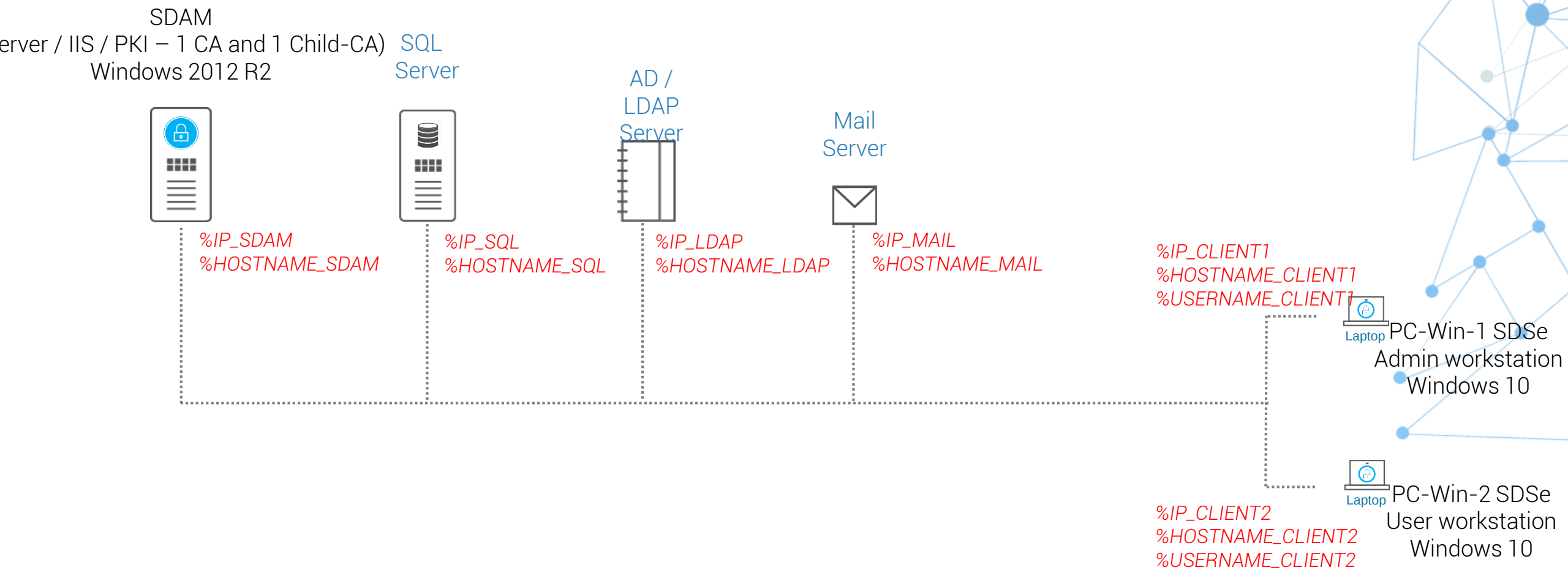
PC-Win-1 SDSe
Admin workstation
Windows 10

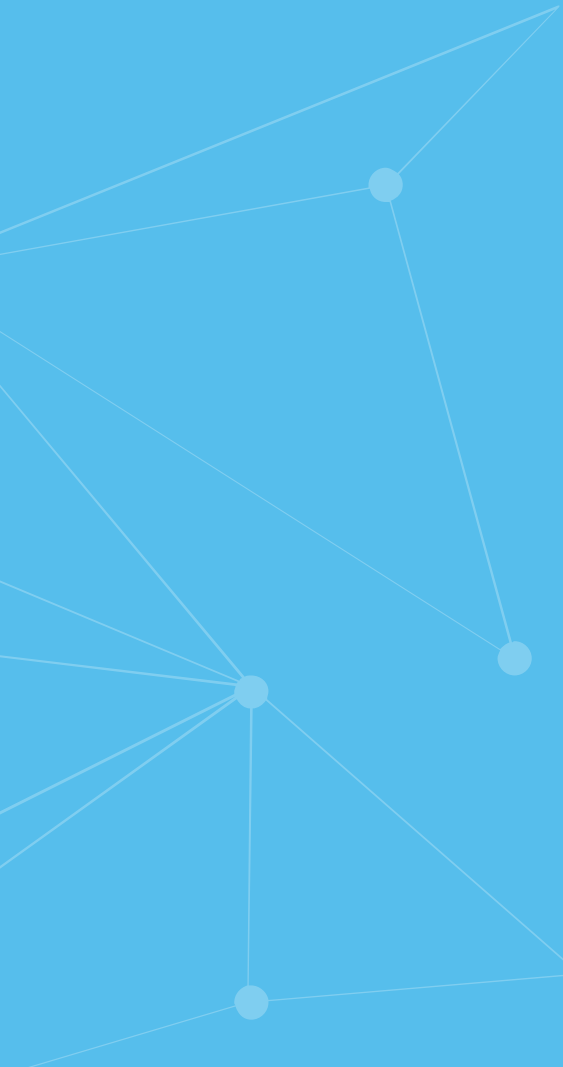
%IP_CLIENT2
%HOSTNAME_CLIENT2
%USERNAME_CLIENT2



PC-Win-2 SDSe
User workstation
Windows 10

Best Practice diagram



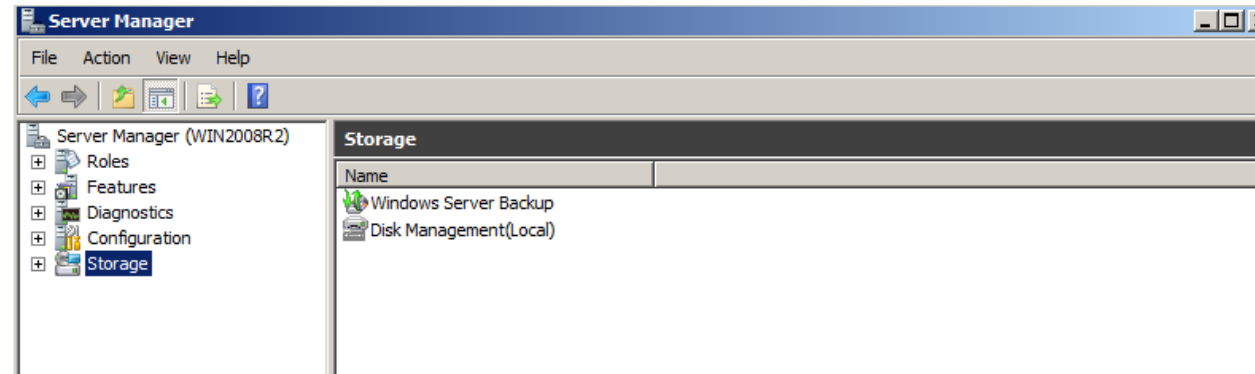


Installing the IIS server

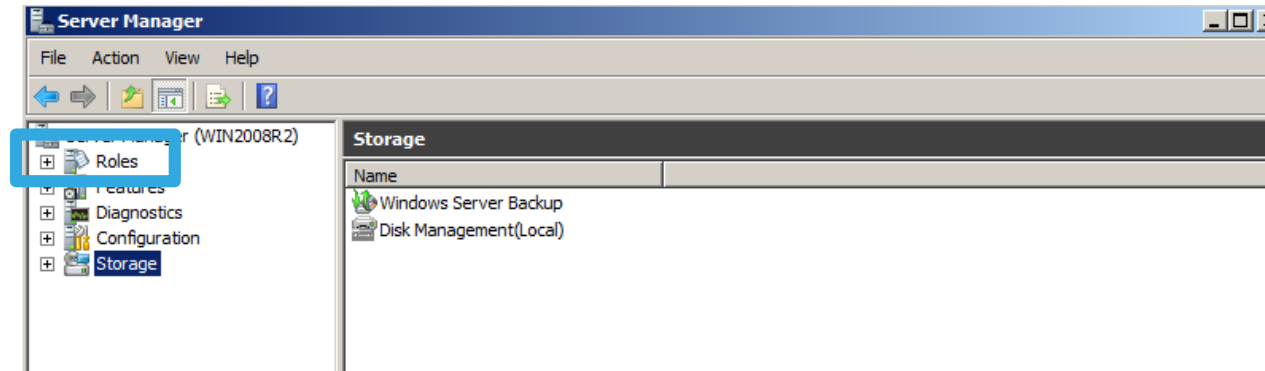
Installing the IIS server

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

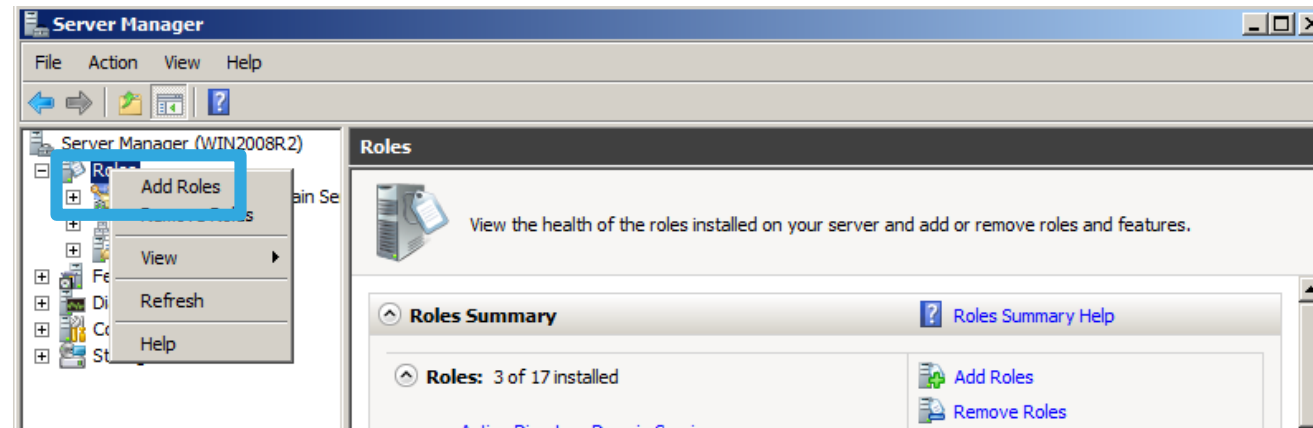


Click on Roles

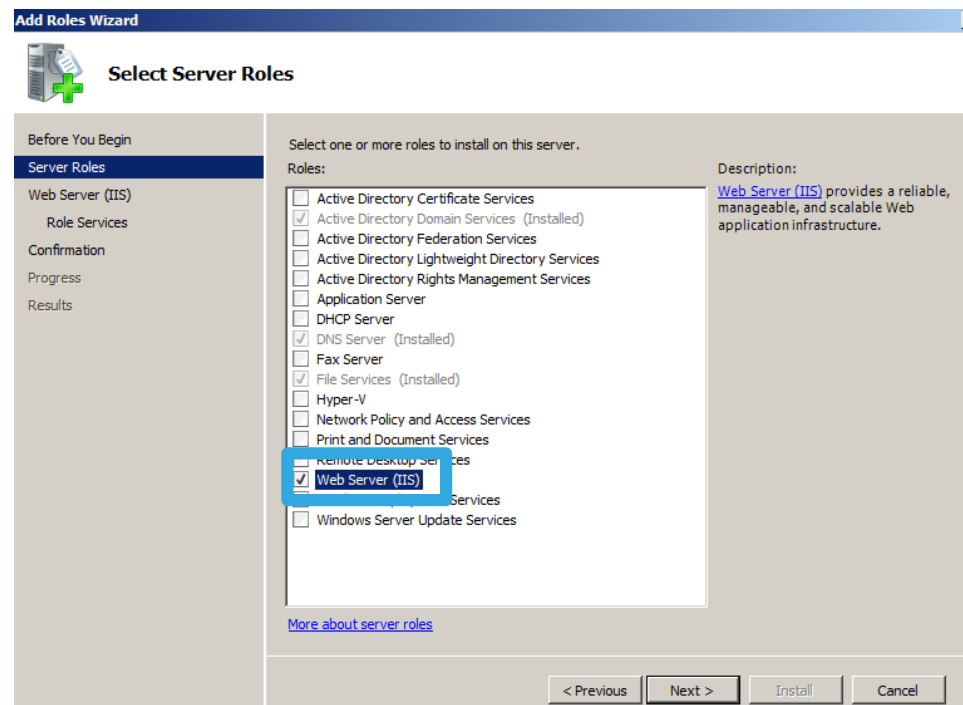


Installing the IIS server (continued)

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

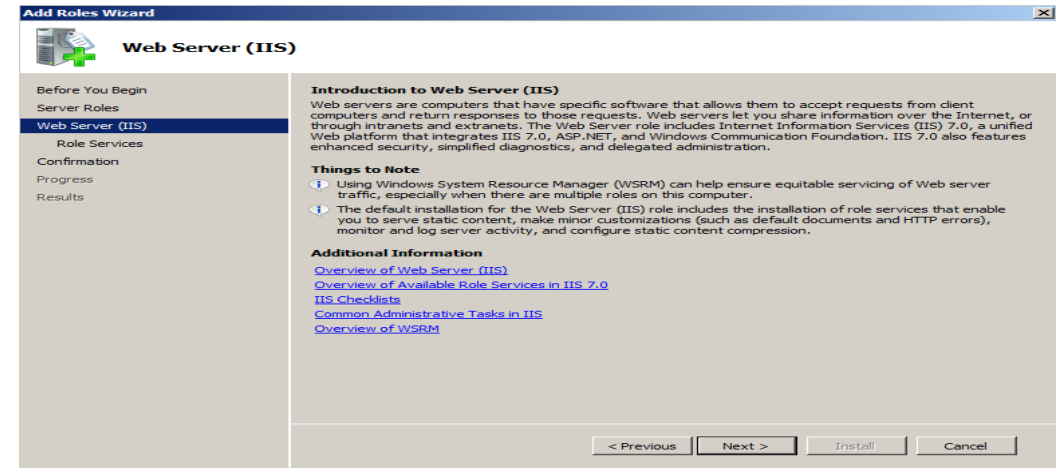


Select **Web Server(IIS)** and click on **Next**



Installing the IIS server (continued)

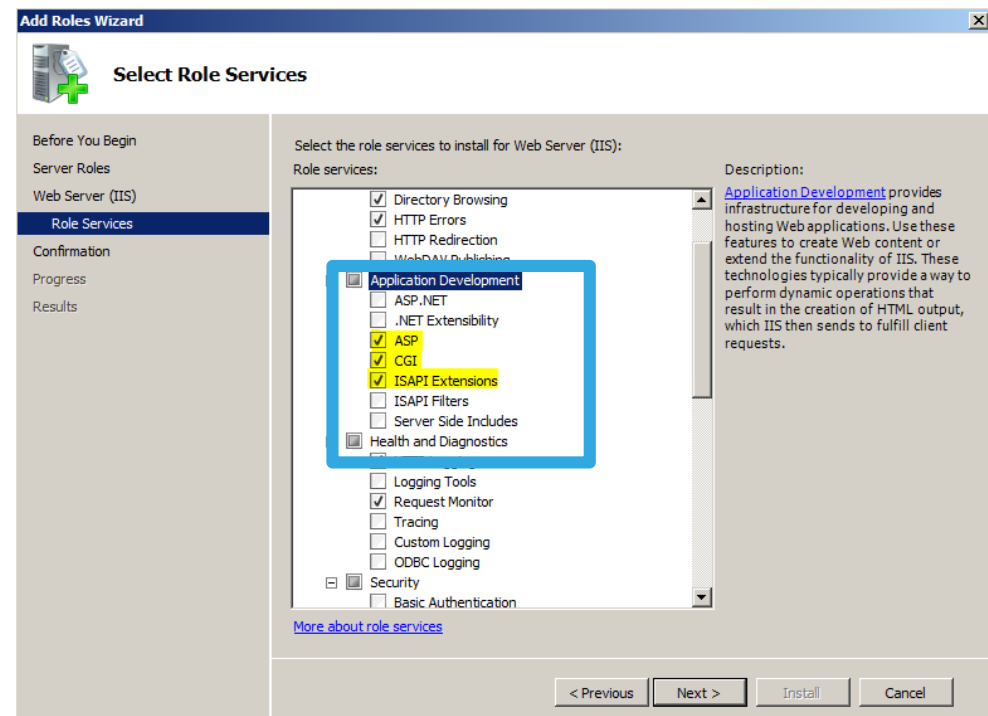
Click on **Next** again



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

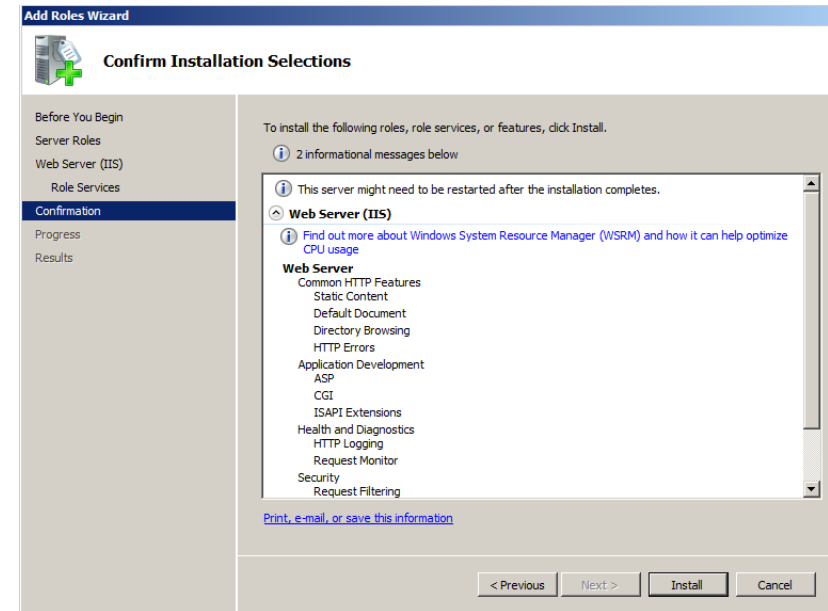
1. **Application Development:** select ASP, CGI and ISAPI Extension
2. **Common HTTP features:** be sure that **Static Content** is selected (if not, select it)
3. **Security:** be sure that **Request Filtering** is selected (if not, select it)

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

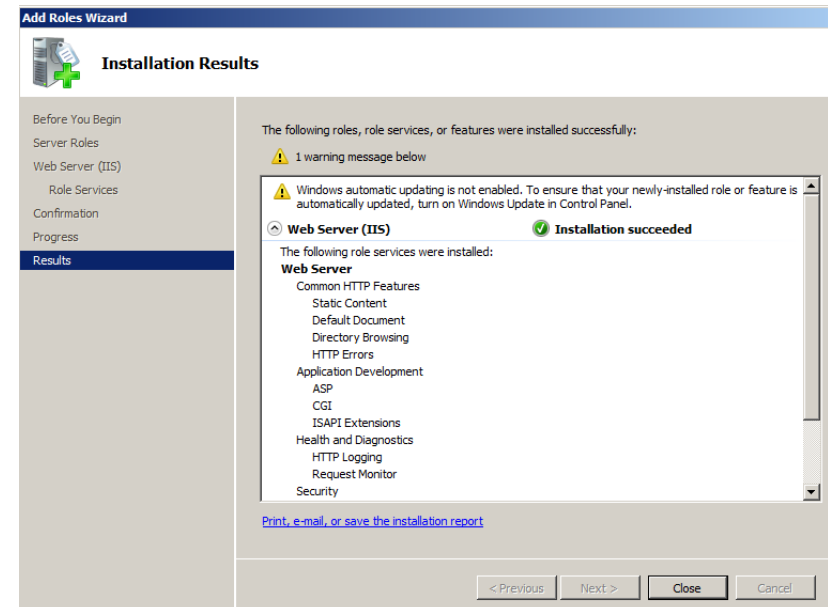


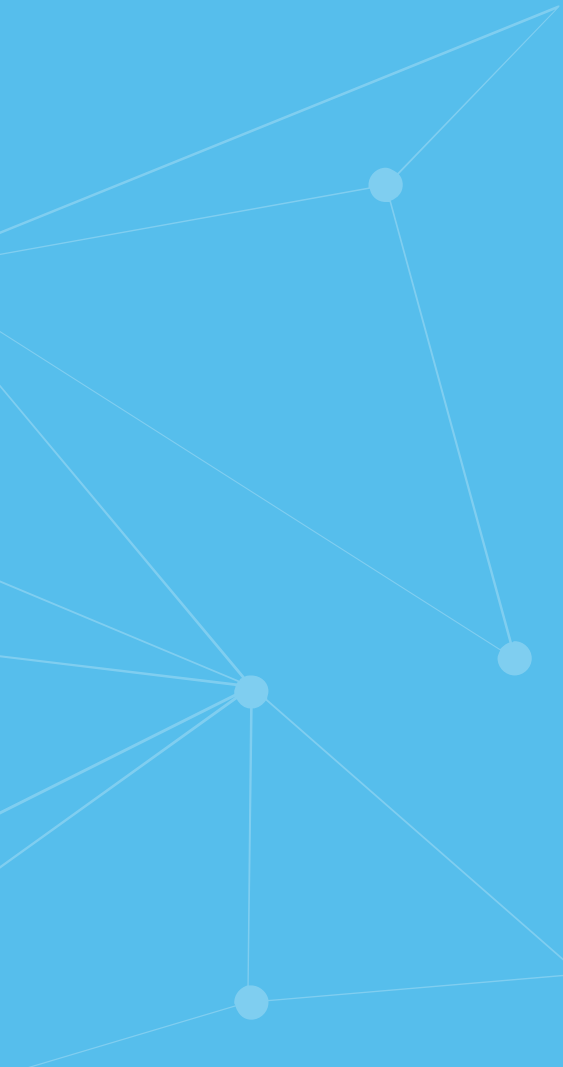
Installing the IIS server (continued)

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

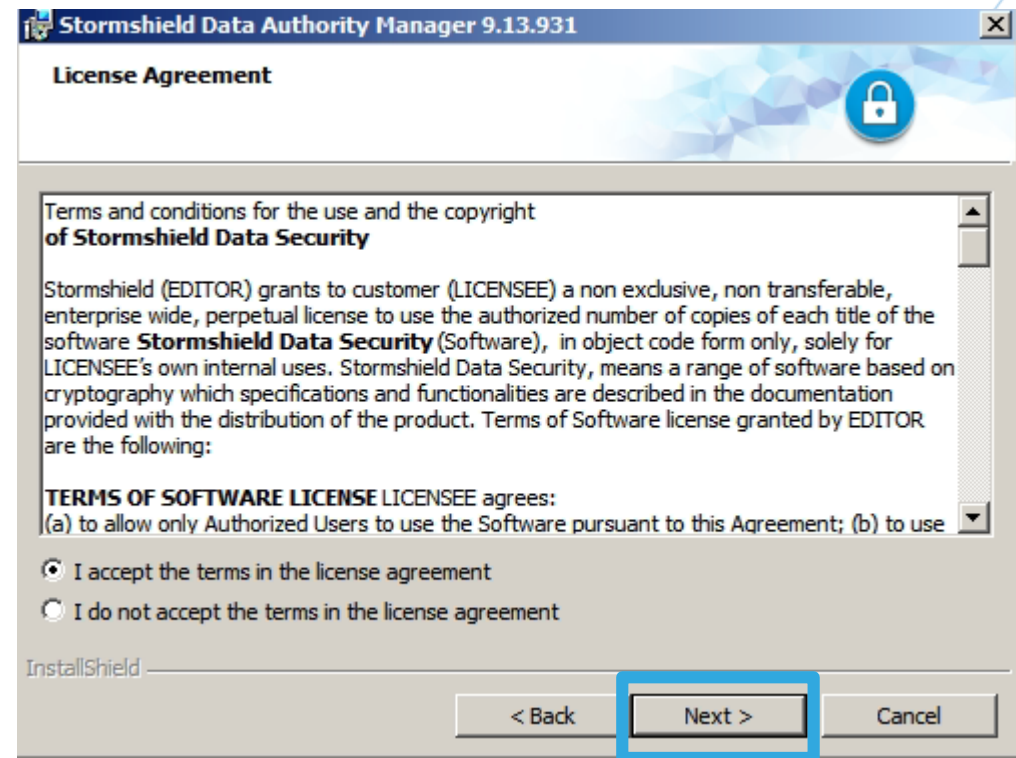
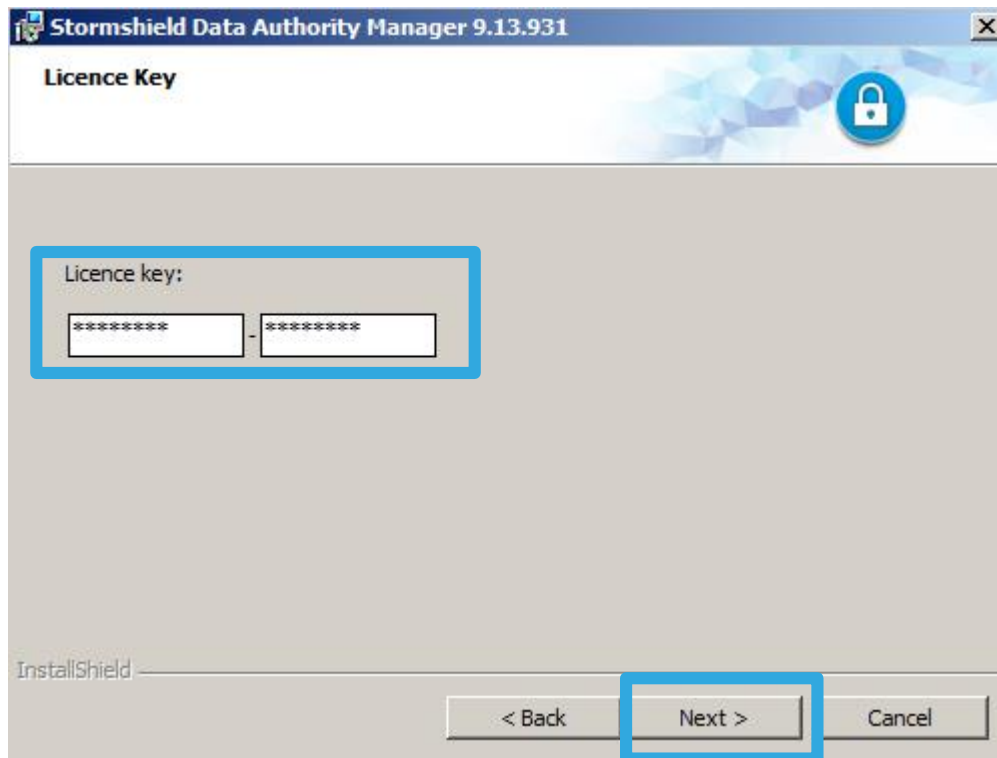
Launch a command prompt with administrator privileges and then run the installer via the command below `msiexec /i "Stormshield Data Authority Manager 9.12.688.msi"` (name of the `.msi` could vary based on the SDAM version)

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

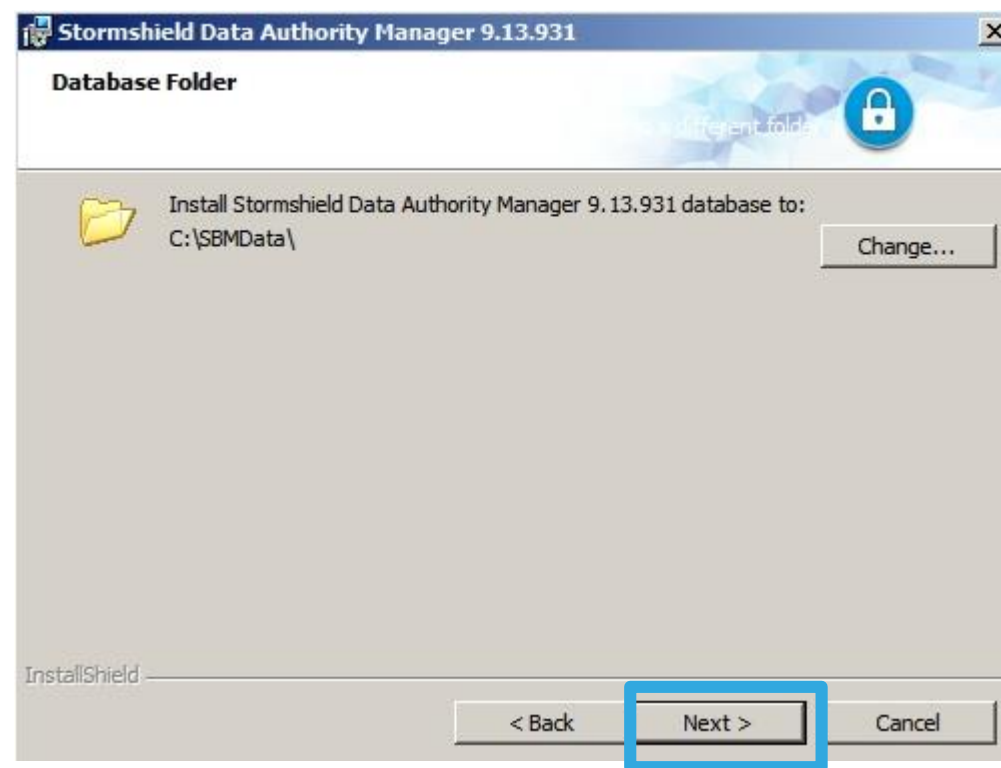
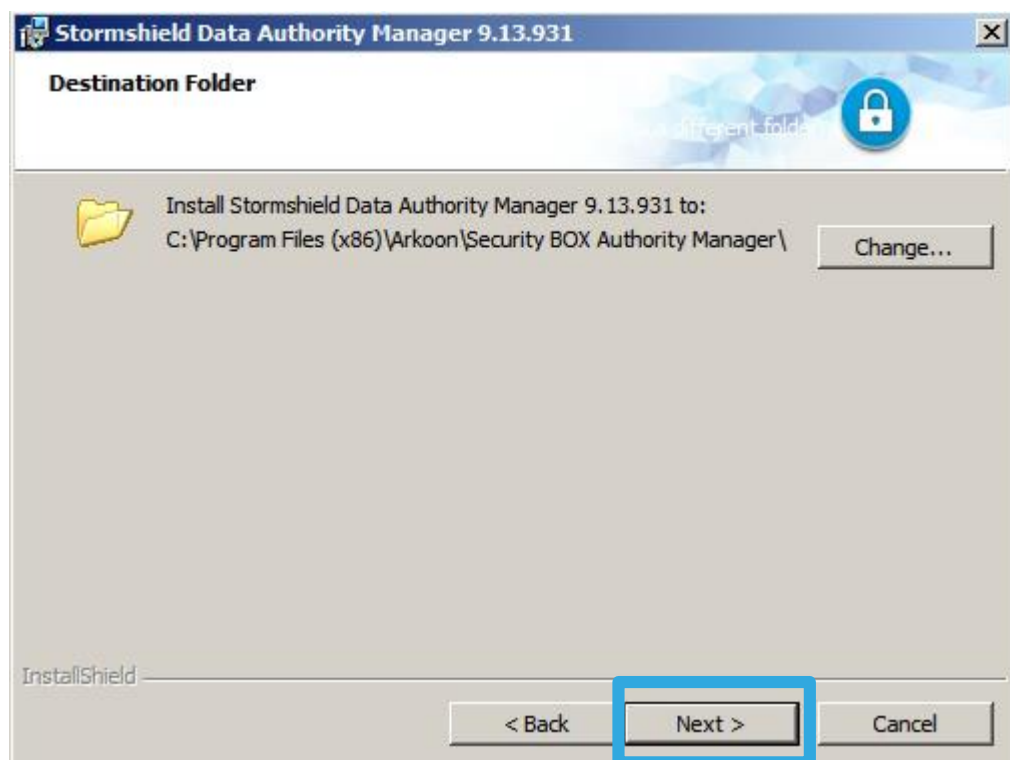
C:\Windows\system32>cd ..
C:\Windows>cd ..
C:\>cd "Stormshield_Data_Authority_Manager_9.13.931_ENU_OFFICIAL_INTERNE(1)"
C:\Stormshield_Data_Authority_Manager_9.13.931_ENU_OFFICIAL_INTERNE(1)>msiexec /
i "Stormshield Data Authority Manager 9.13.931.msi"
```



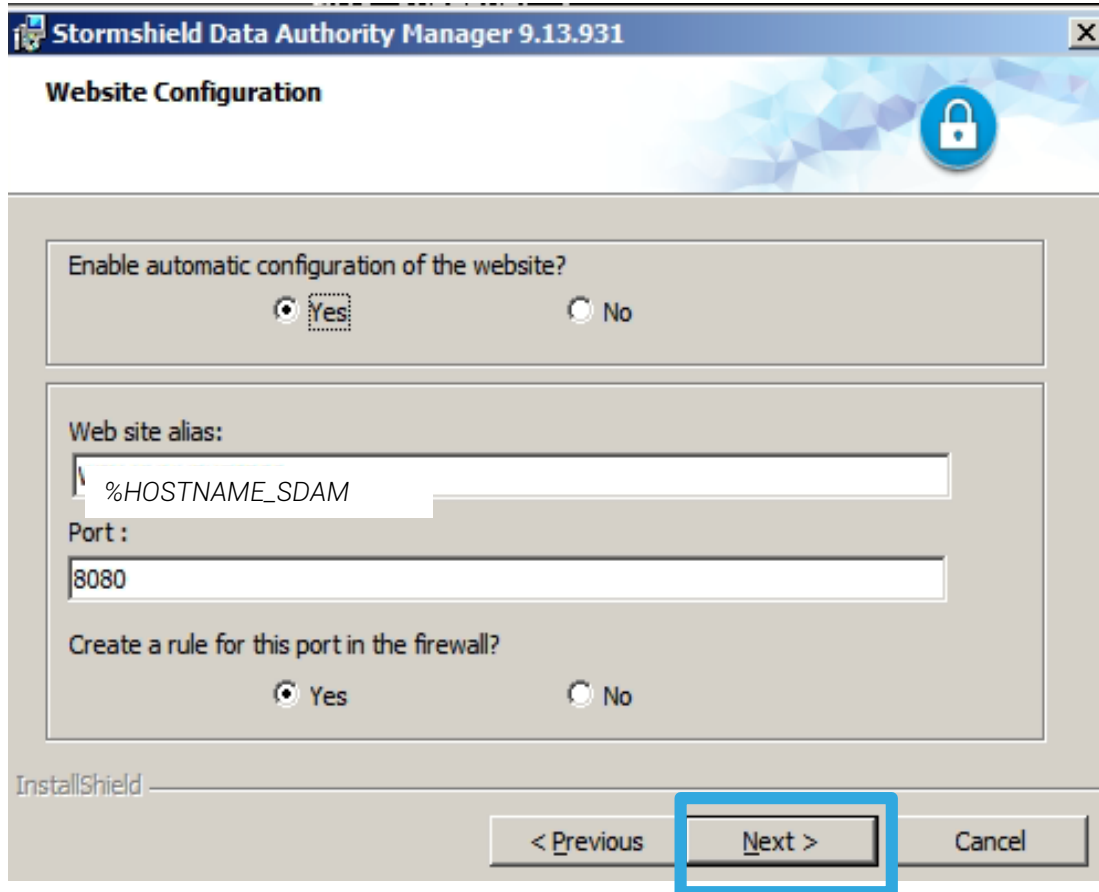
Installing the SDAM server (continued)



Installing the SDAM server (continued)



Installing the SDAM server (continued)



Stormshield Data Authority Manager 9.13.931

Website Configuration

Enable automatic configuration of the website?
☒ Yes ☐ No

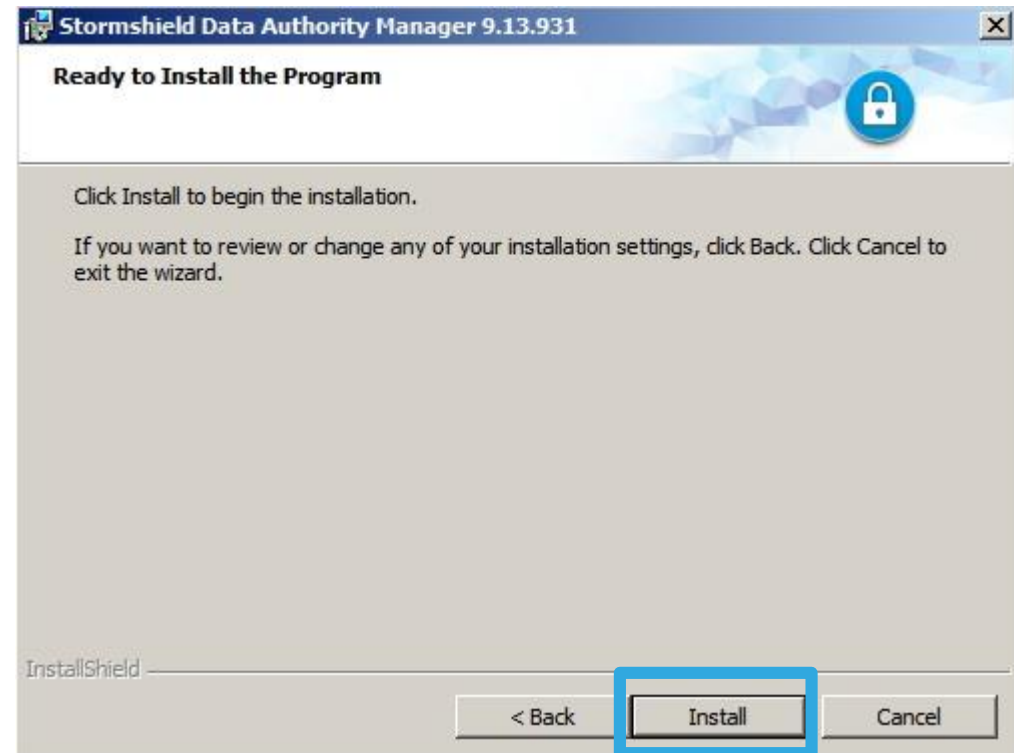
Web site alias:

Port :

Create a rule for this port in the firewall?
☒ Yes ☐ No

InstallShield

< Previous **Next >** Cancel



Stormshield Data Authority Manager 9.13.931

Ready to Install the Program

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

InstallShield

< Back **Install** Cancel

Installing the SDAM server (continued)

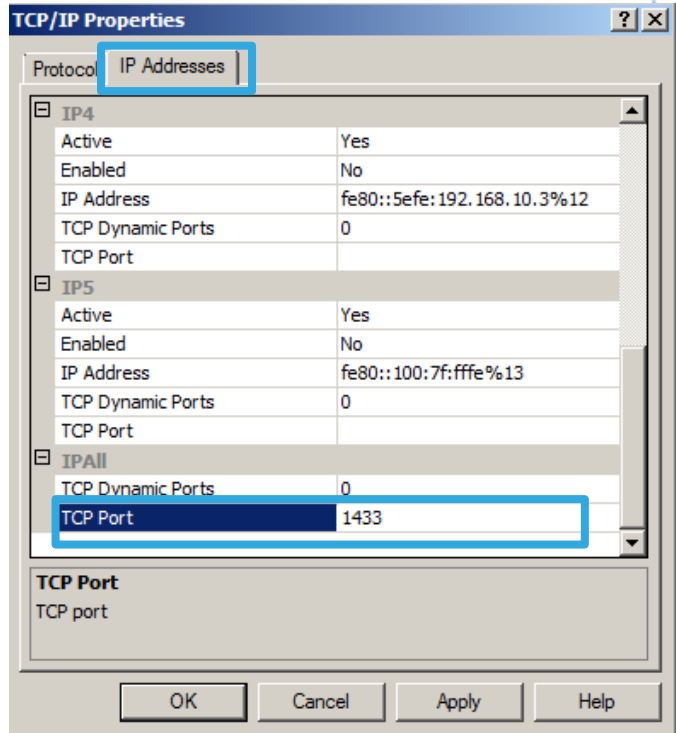
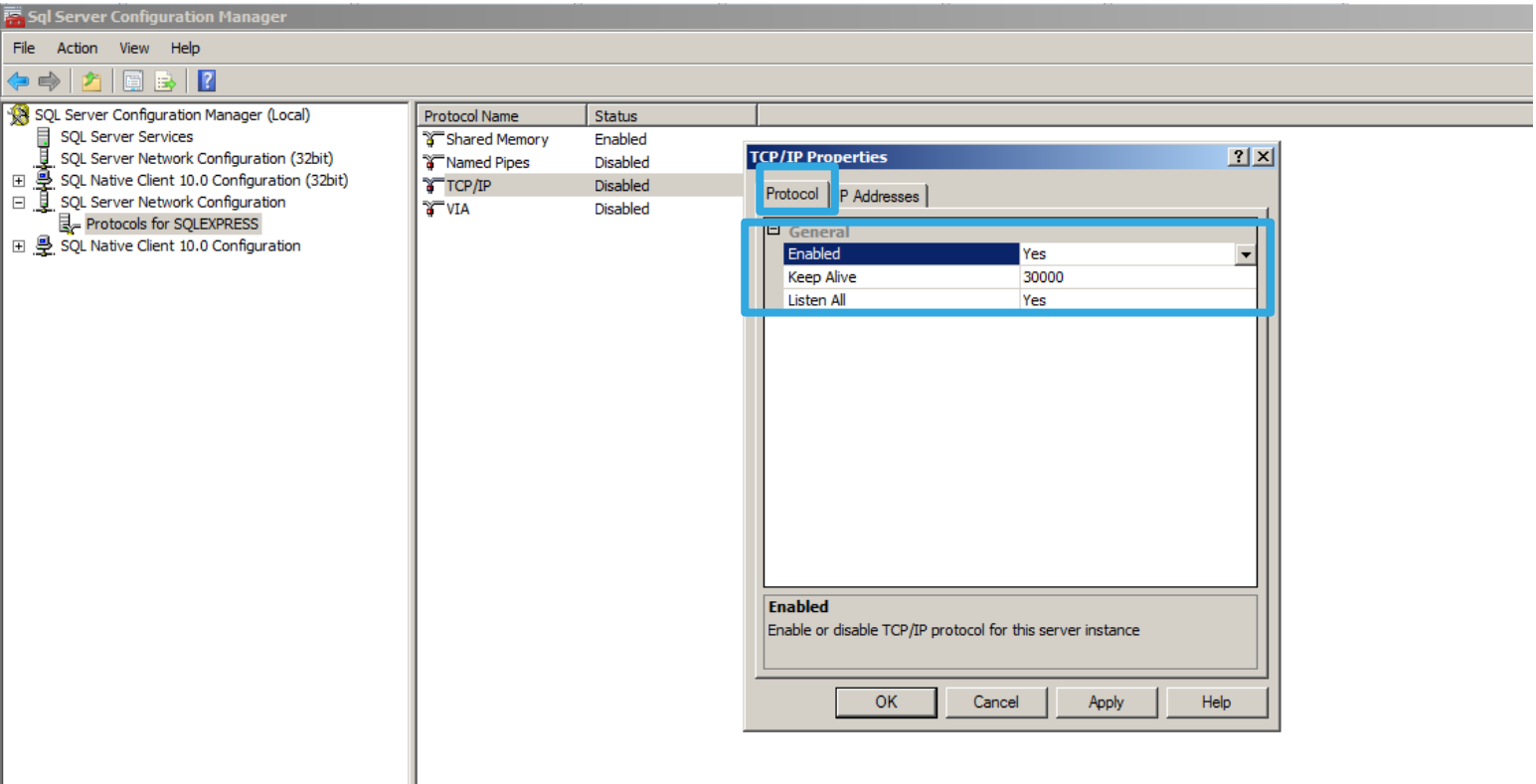


Option: SQL Server recommendations

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"

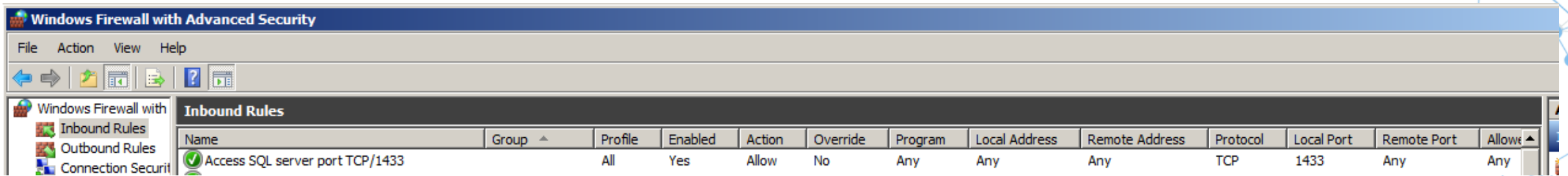
In the same TCP/IP Properties window, click on the second tab



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:

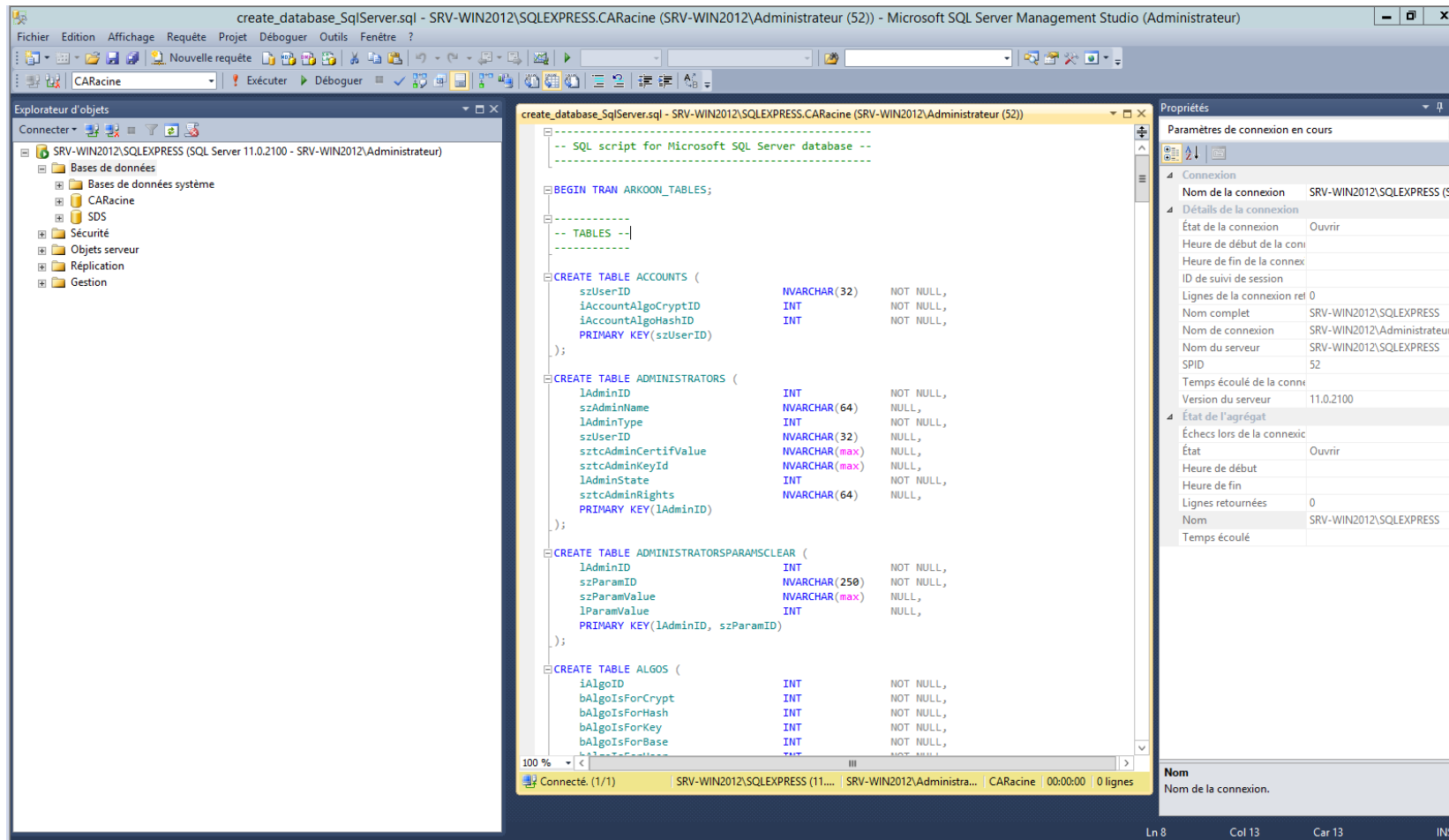
```
sqlcmd -S myServer\instanceName -d Database
```

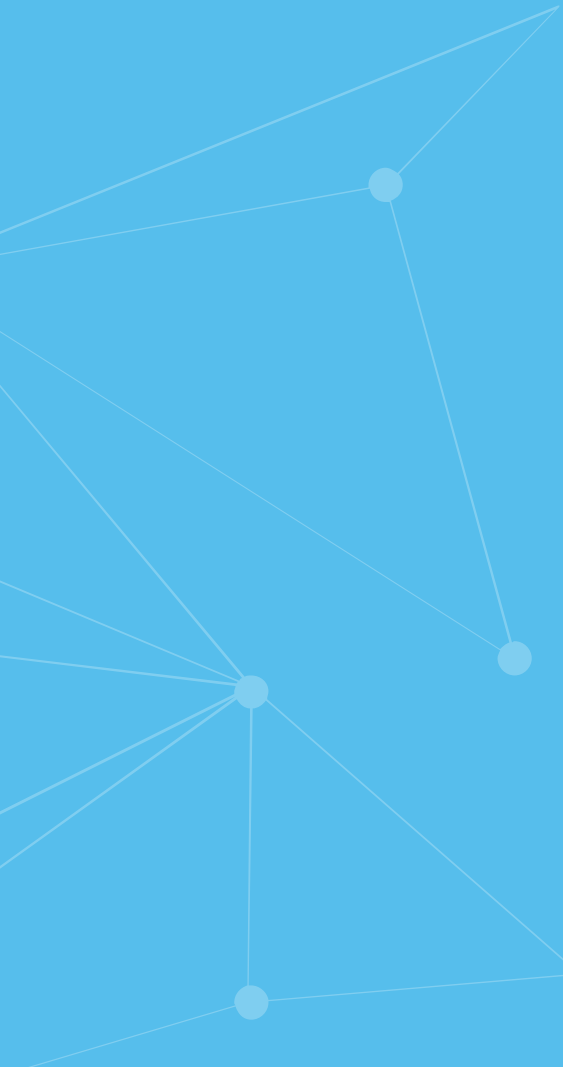
```
-i <path>\create_database_SqlServer.sql
```



An abstract geometric pattern consisting of a network of blue lines and dots. The dots, in various sizes, are connected by thin blue lines to form a complex, interconnected web. The background is a light gray with faint, larger-scale geometric shapes, creating a layered and modern aesthetic.

- Creation of the base with Microsoft SQL Management Studio



An abstract geometric diagram on the left side of the slide. It consists of several light blue dots connected by thin, light blue lines, forming a network-like structure. The dots are positioned at various points, with some lines radiating from a central point and others connecting different points in a non-linear fashion.

Installing SDS Suite on the administration workstation

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.

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

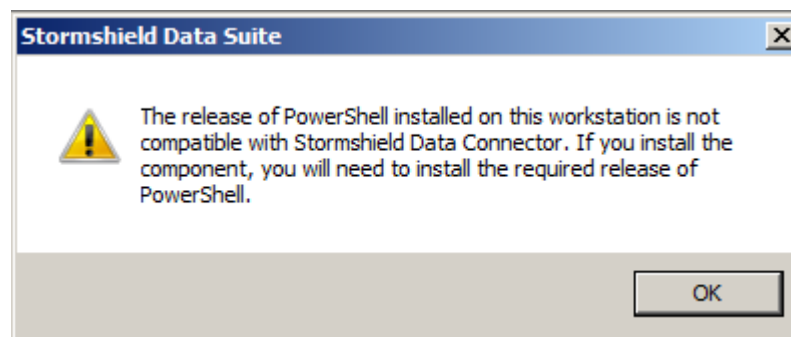
AGENT
DEMO
SERVER
TOOLS

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

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

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

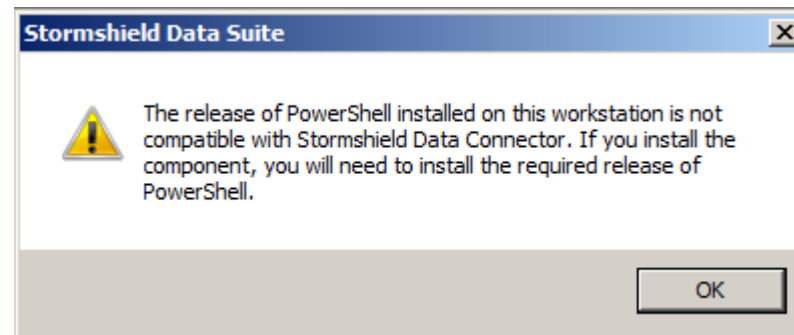
AGENT
DEMO
SERVER
TOOLS

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

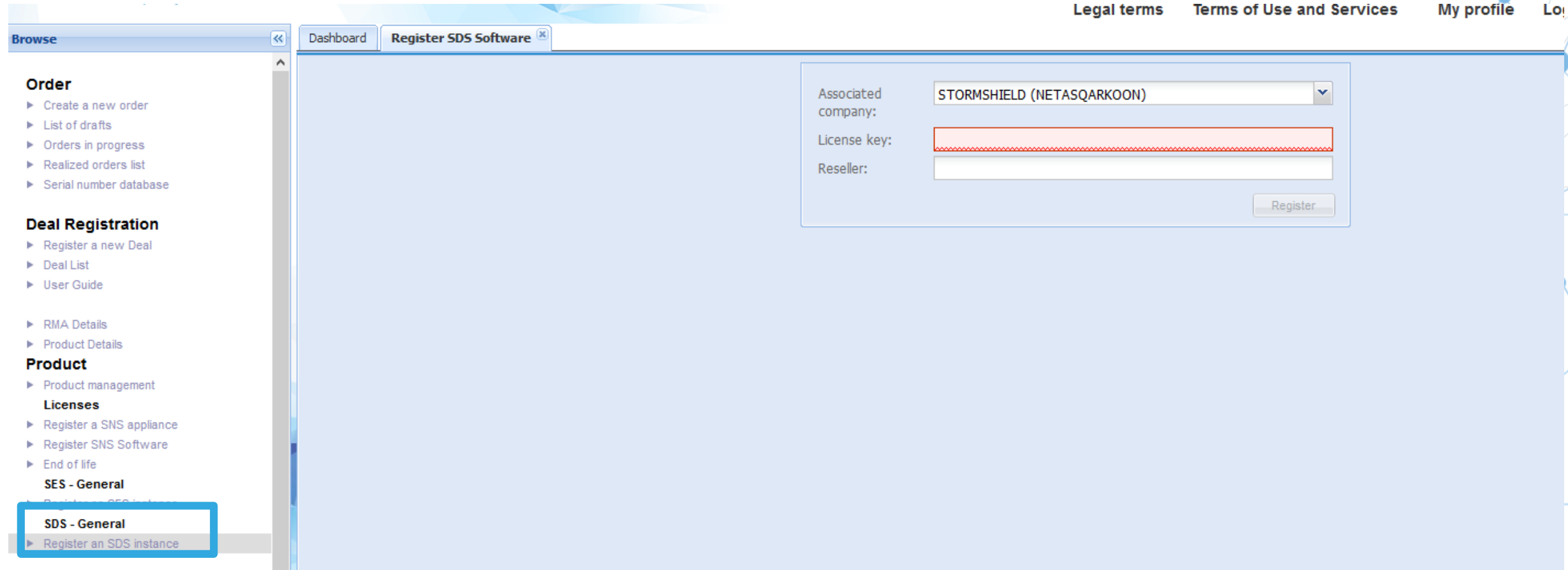
Release Note : [EN / FR](#) User Guide : [EN / FR](#)

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

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



Registering your Stormshield Data Security product



The screenshot shows a web application interface for registering a Stormshield Data Security product. The interface is divided into a left sidebar, a top navigation bar, and a main content area.

Top Navigation Bar: Contains links for "Legal terms", "Terms of Use and Services", "My profile", and "Log out".

Left Sidebar: Contains a "Browse" section with a back arrow and a "Register SDS Software" tab. Below this, there are three main categories: "Order", "Deal Registration", and "Product".

- 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:**
 - Product management
 - Licenses:**
 - Register a SNS appliance
 - Register SNS Software
 - End of life
 - SES - General:**
 - Register an SDS instance

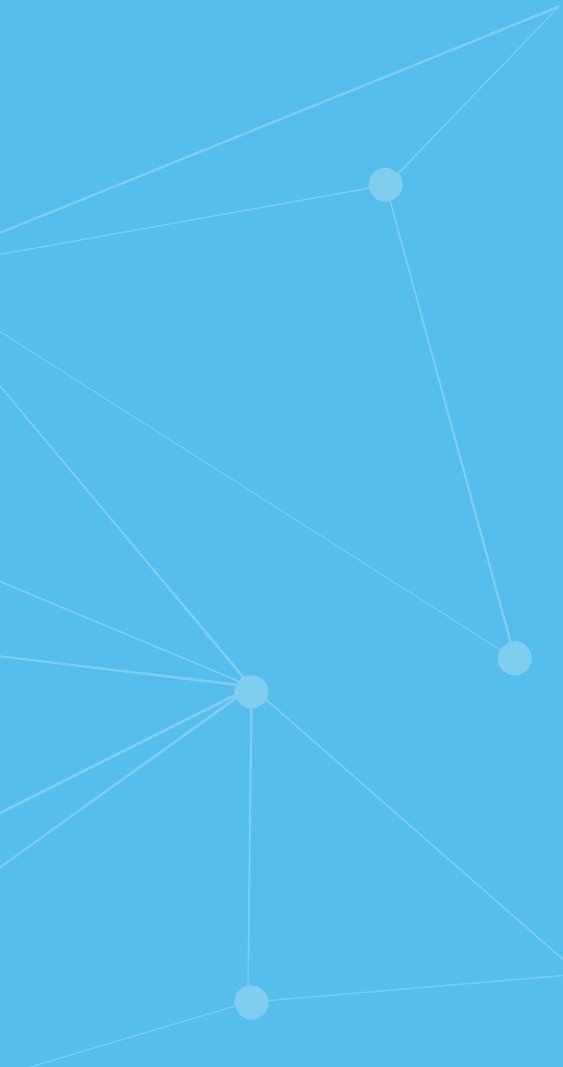
The "Register an SDS instance" link is highlighted with a blue box.

Main Content Area: The "Register SDS Software" tab is active, showing a registration form with the following fields:

- Associated company:** A dropdown menu with "STORMSHIELD (NETASQARKOON)" selected.
- License key:** A text input field with a red border and a dashed pattern.
- Reseller:** A text input field.
- Register:** A button to submit the form.

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 \(option\)](#).

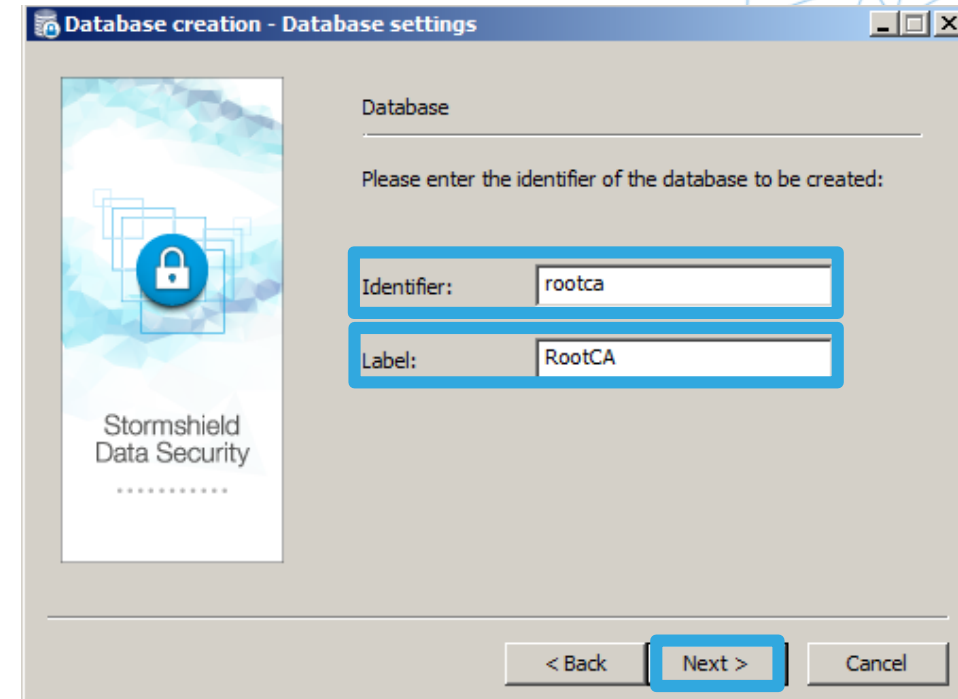
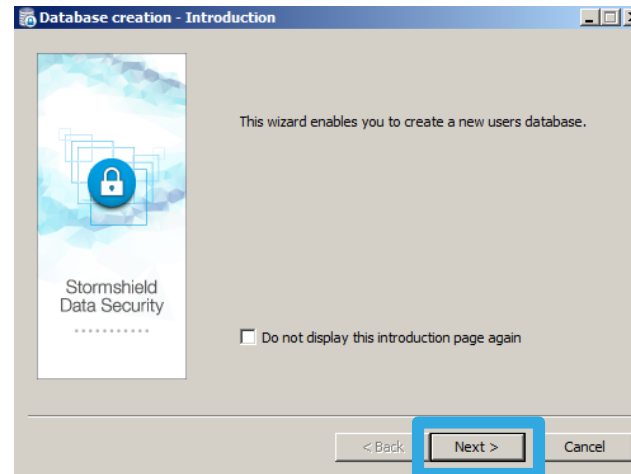
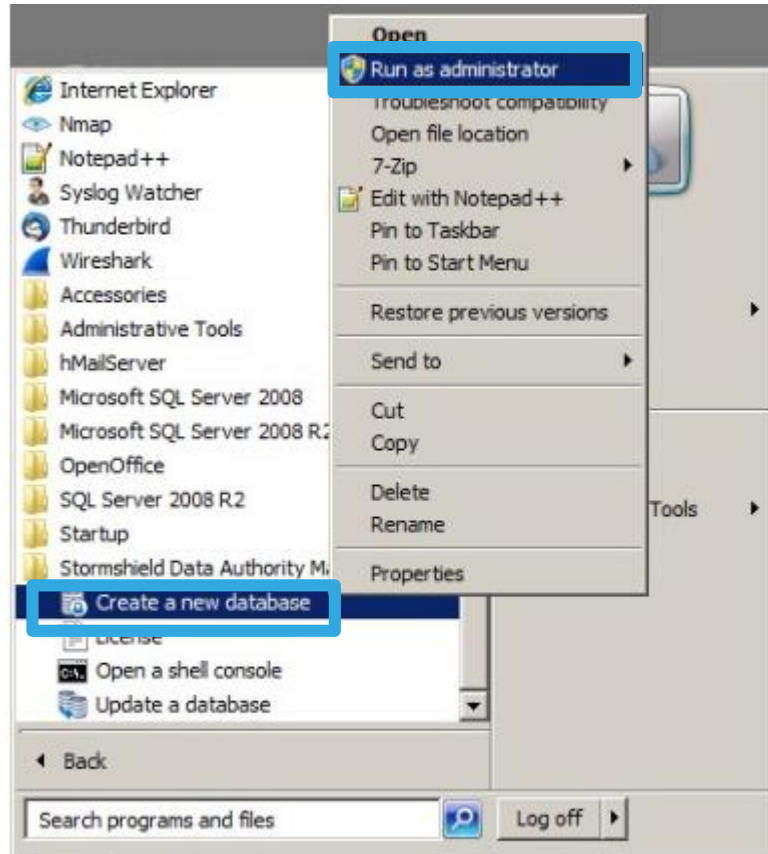
An abstract geometric diagram on the left side of the slide. It features four light blue circular nodes connected by thin white lines. One node is at the top left, another is to its right and slightly lower, a third is further down and to the left, and a fourth is at the bottom left. Lines connect these nodes in a way that suggests a network or a series of interconnected points.

Creating the root PKI

Installing the Access DB for the Root CA

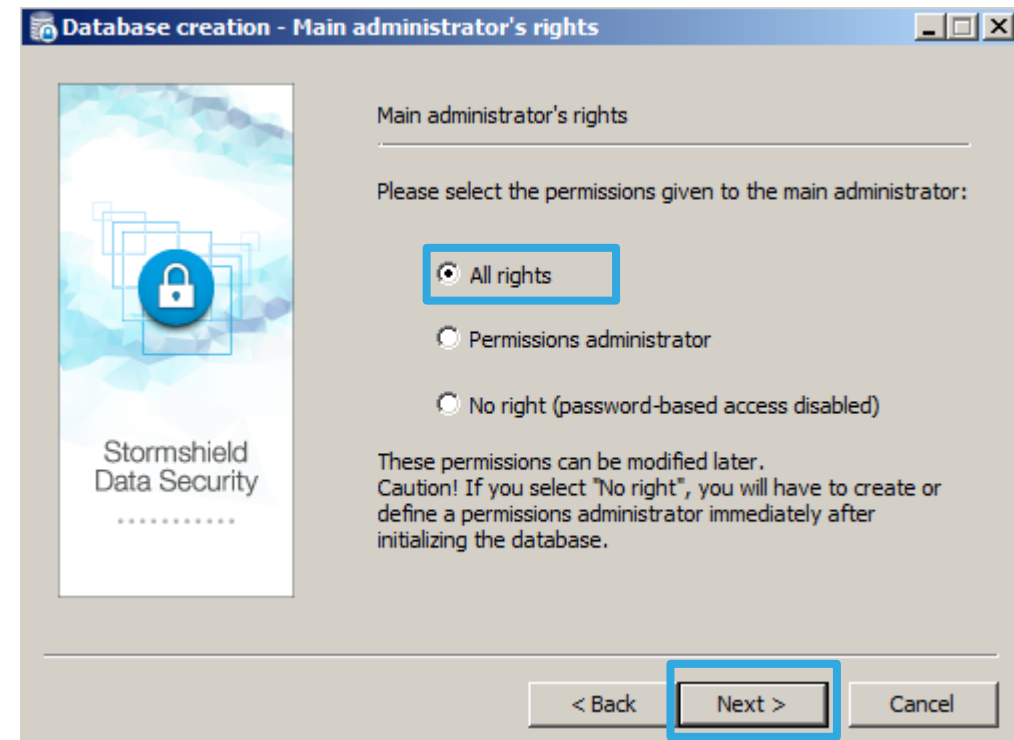
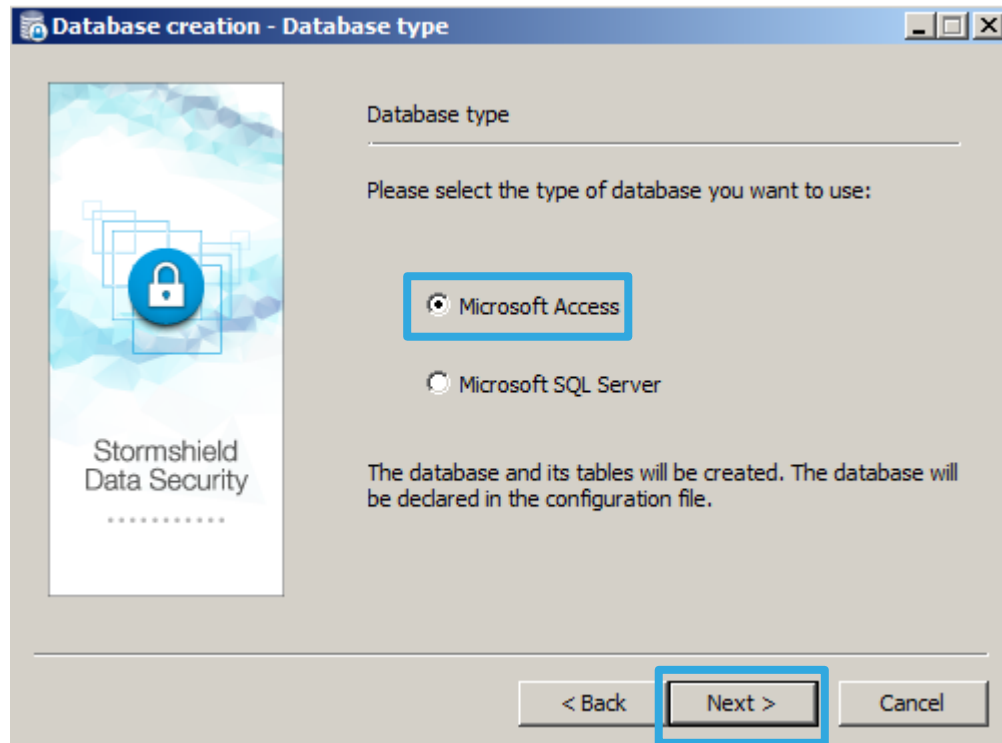
- Identifier: The identifier is essentially used internally by the SDAM
- Label: The label is used in all SDAM pages to refer to the user database

Click on Create a new database and
Run as administrator

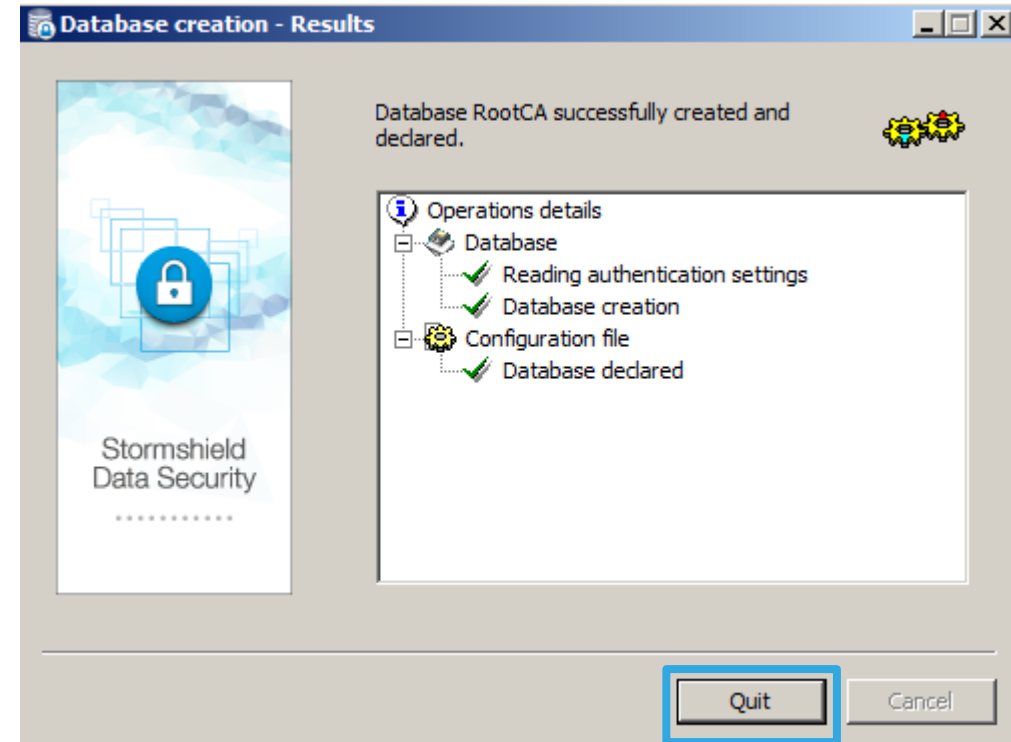
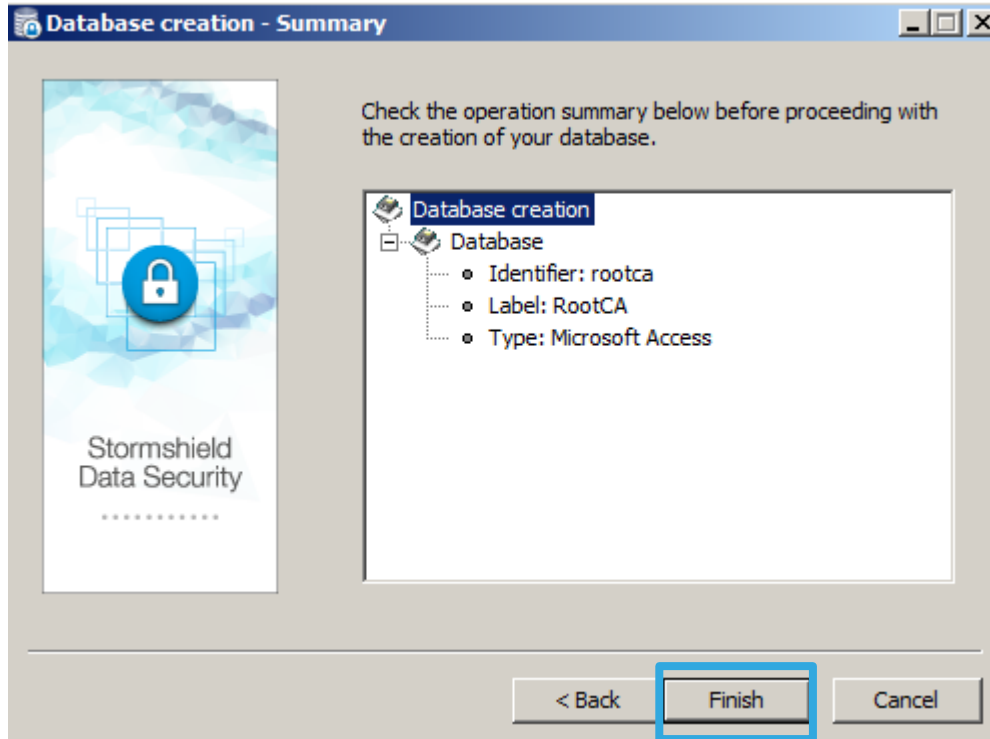


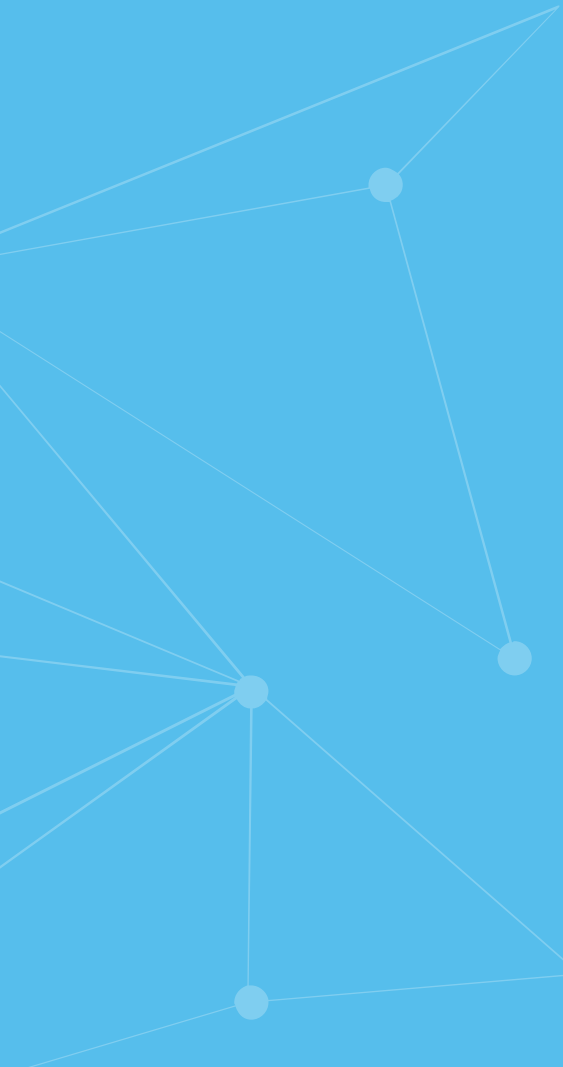
Installing the Access DB for the Root CA (continued)

If you choose to create a "Microsoft SQL Server" database, see [SQL Server recommendations](#)



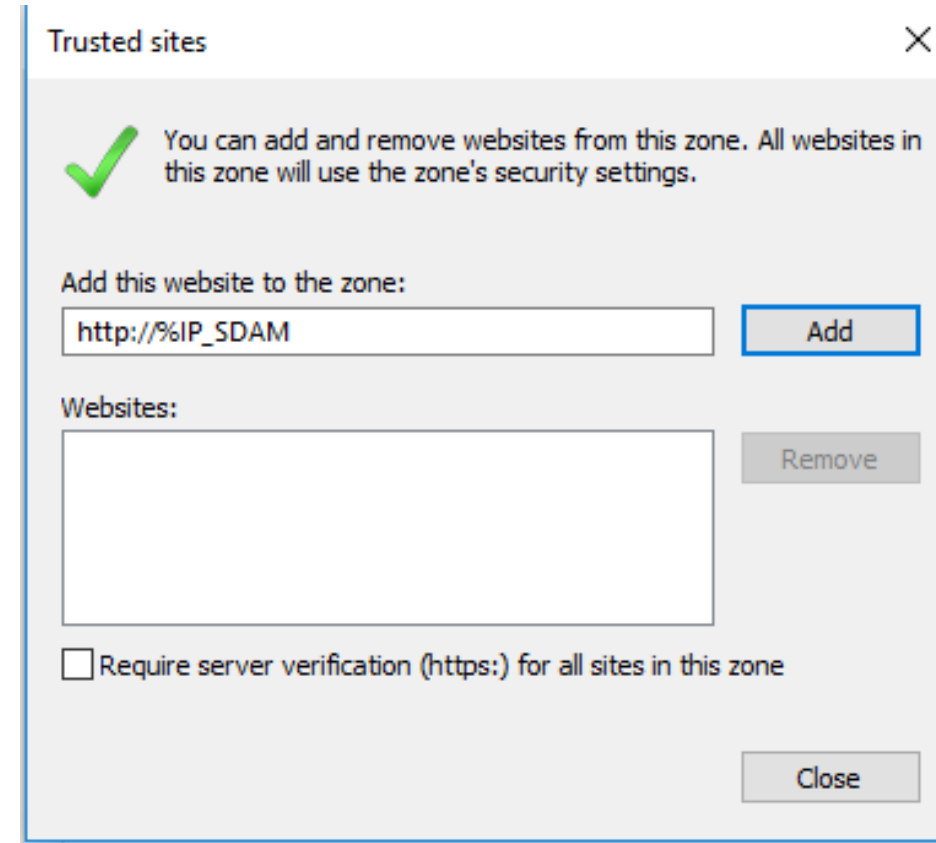
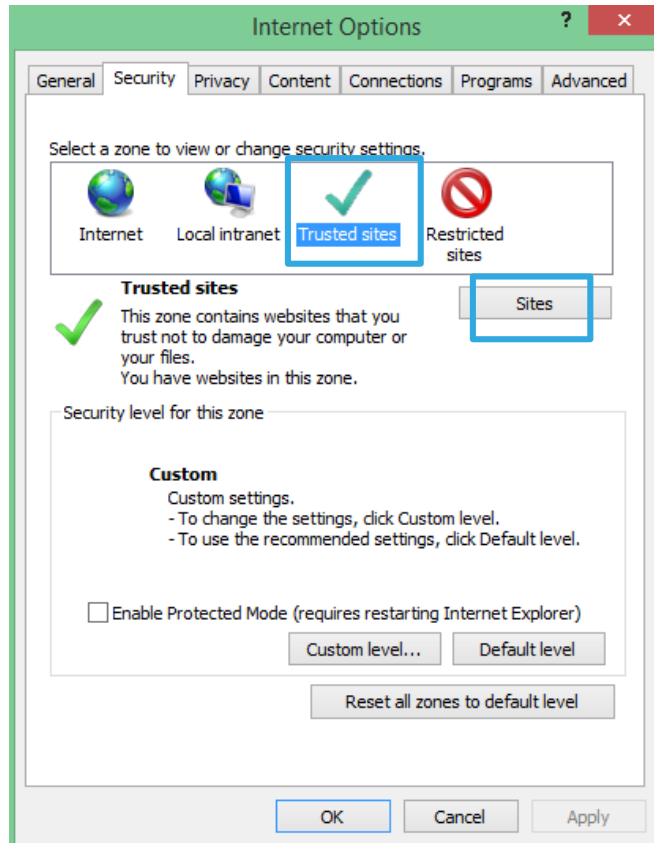
Installing the Access DB for the Root CA (continued)



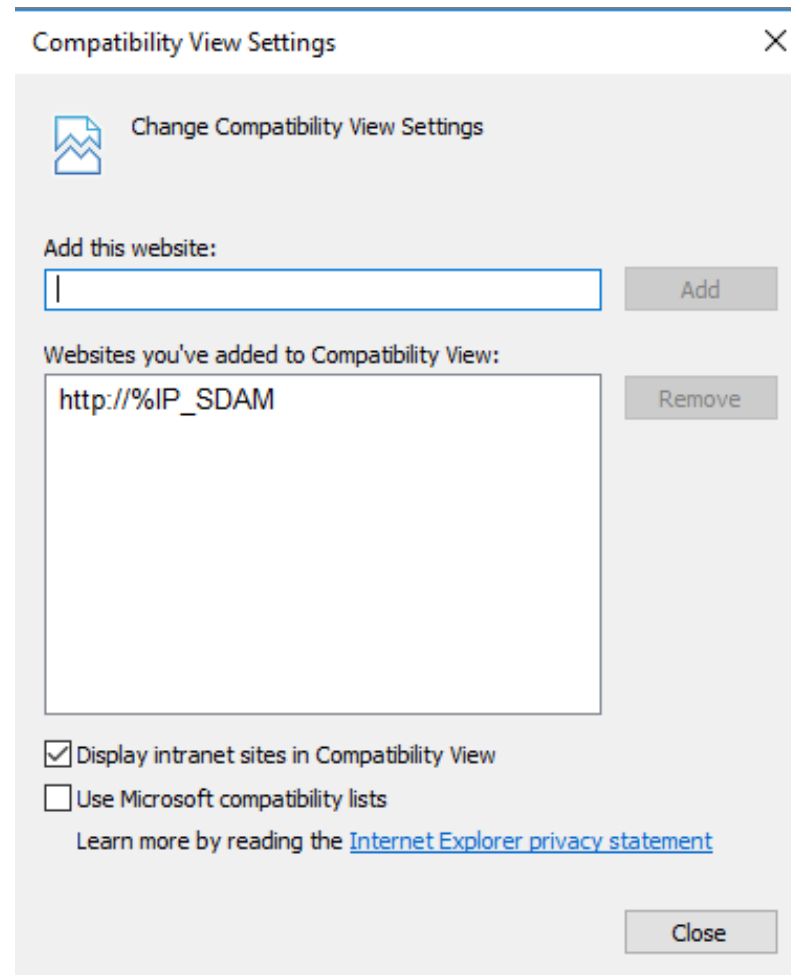
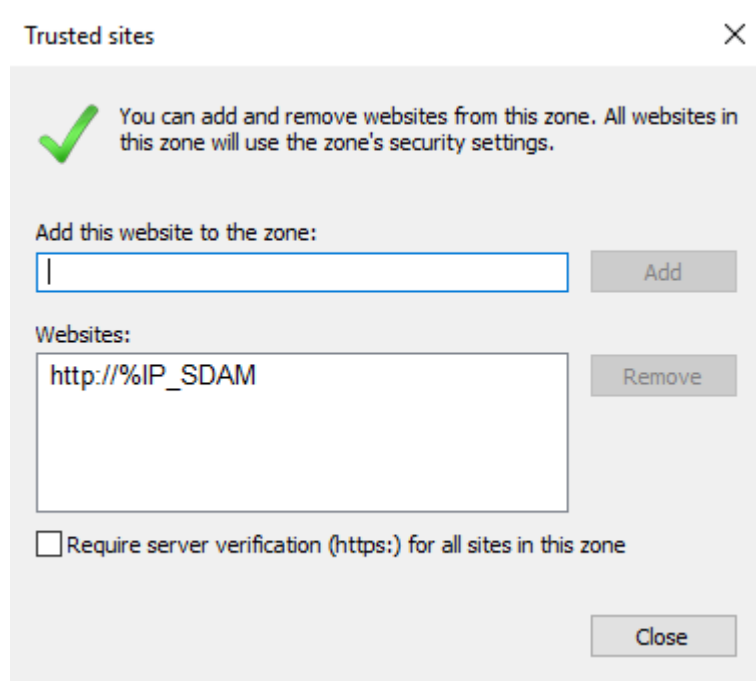
An abstract geometric diagram on the left side of the slide. It consists of several light blue dots connected by thin, light blue lines. The dots are arranged in a way that suggests a network or a series of interconnected points. One dot is at the top left, another is below it to the right, and a third is further down and to the left. There are also dots at the bottom left and bottom right, with lines connecting them to the central dots.

Configuring Internet Explorer + Initializing the root PKI

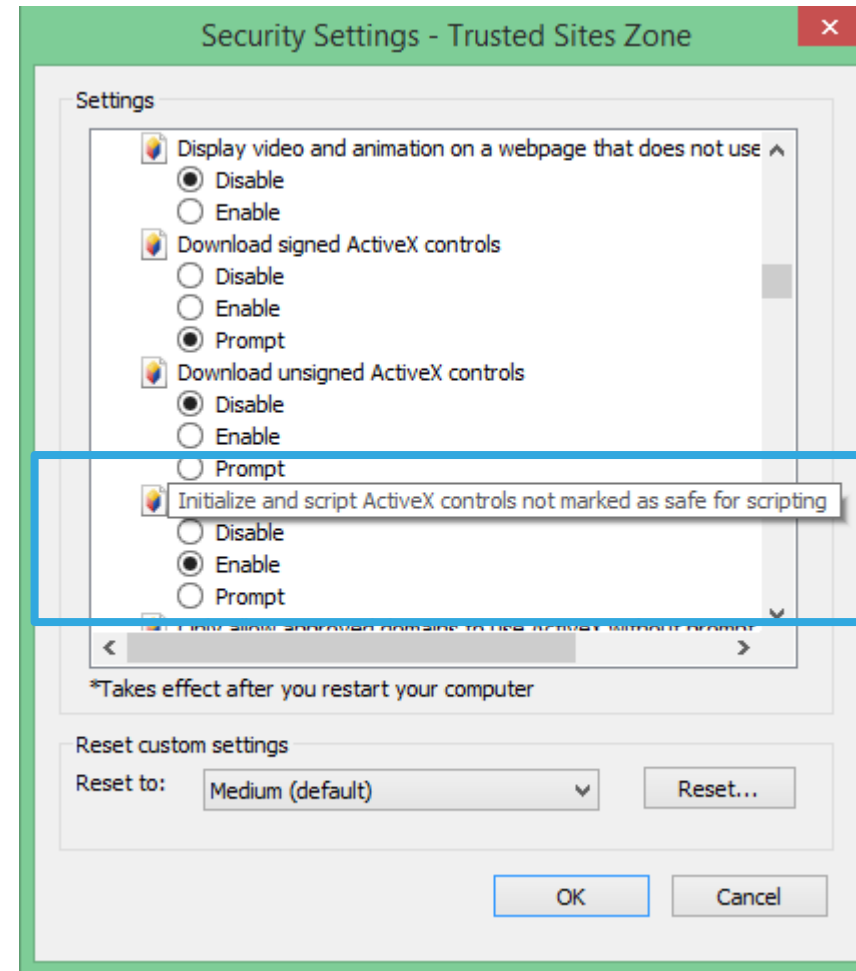
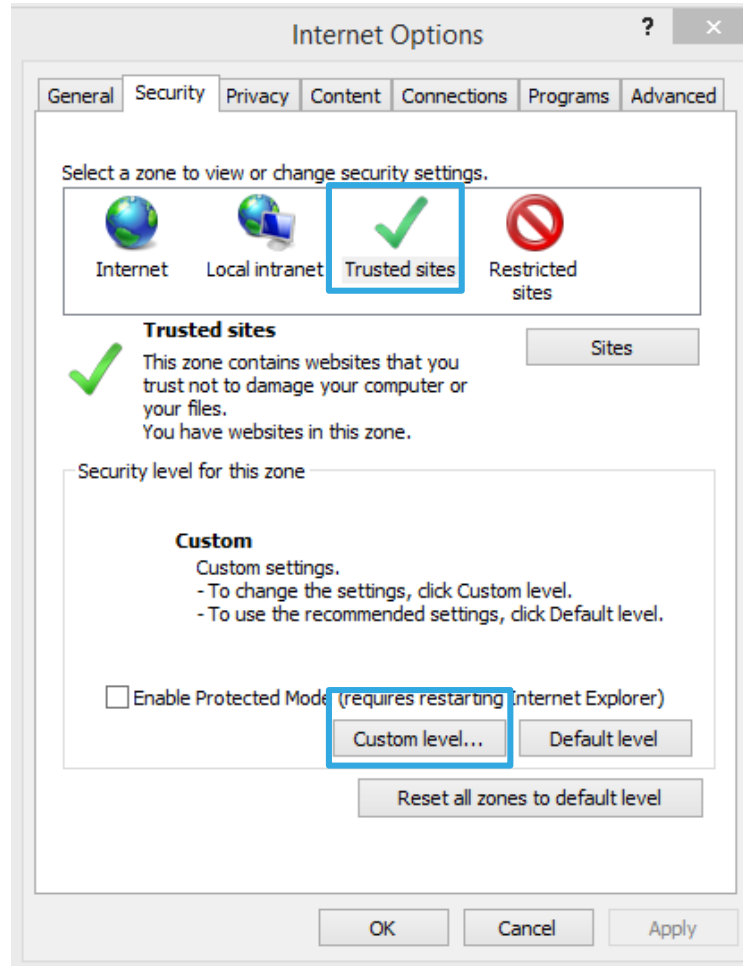
Initial connection to the SDAM web management interface



Initial connection to the SDAM web management interface (continued)



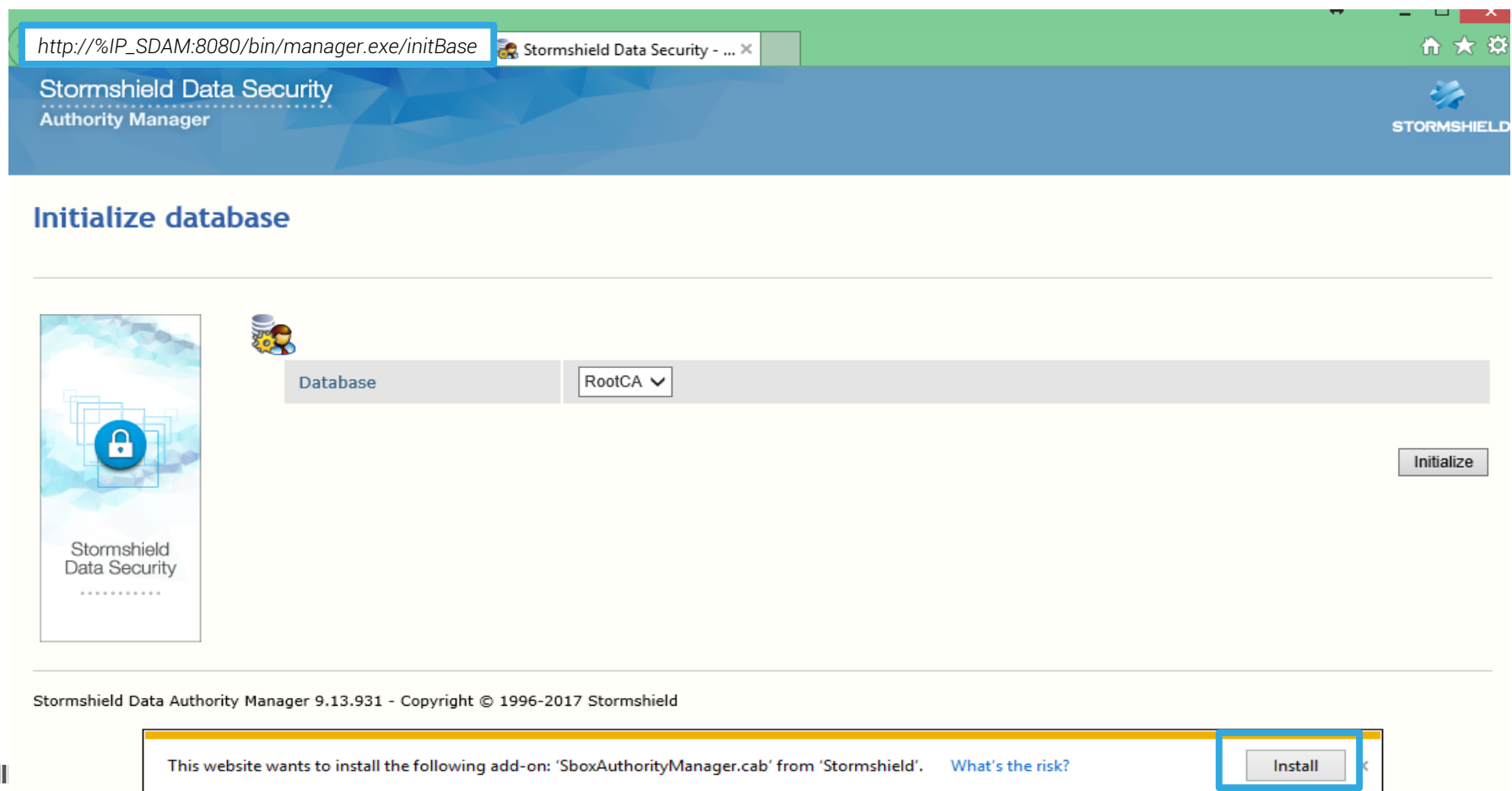
Initial connection to the SDAM web management interface (continued)



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

Initialize database



Database RootCA ▼

Initialize

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

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	☒ Store keys in the internal cryptographic module
	☐ Store keys in a hardware cryptographic module
	Slot / Token: No slot or token activated

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

Initializing the RootCA (continued)

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	☒ Draw an encryption key	RSA 2048 bits
	☐ Import an encryption key from a PKCS#12 file:	
	File name	Browse...
	Password	
Exportable key	☒ Mark key as exportable	

Click on Proceed

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

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	
Password confirmation	

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.

Initializing the RootCA (continued)

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 ▼

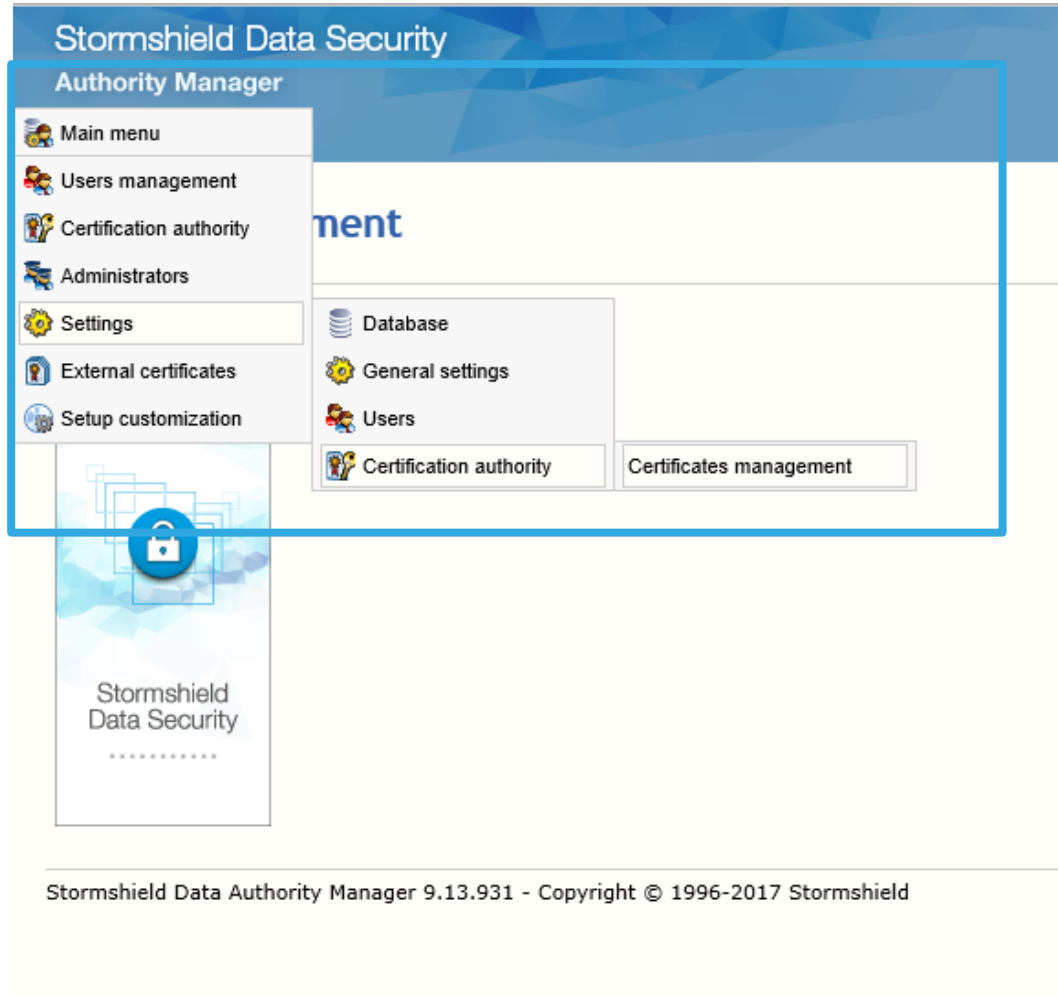
Key identifier

☒ Include key identifier (SubjectKeyId)

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)

Certification authority

Subject resolution mask:

External certificate requests pre-fill

Organization	
Organization unit	
City	
State or province	
Country	(none)

Generated certificates

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

Configuring the CRL (continued)

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

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:\SBMDData\rootcal\Crl\rootca.crl

CRLs archiving folder

C:\SBMDData\rootcal\Crl\History

CRL generation

☒ By default, request CRL generation at each revocation

Expired certificates

☐ Include expired certificates in CRL

CRL distribution points

http://%IP_SDAM:8080/rootcr/rootca.crl

Add

Copy

Delete

Distribution point:

http://%IP_SDAM:8080/rootcr/rootca.crl

Automatic CRL generation service

Generation service

☒ Activate automatic CRL generation

Frequency

1

hours

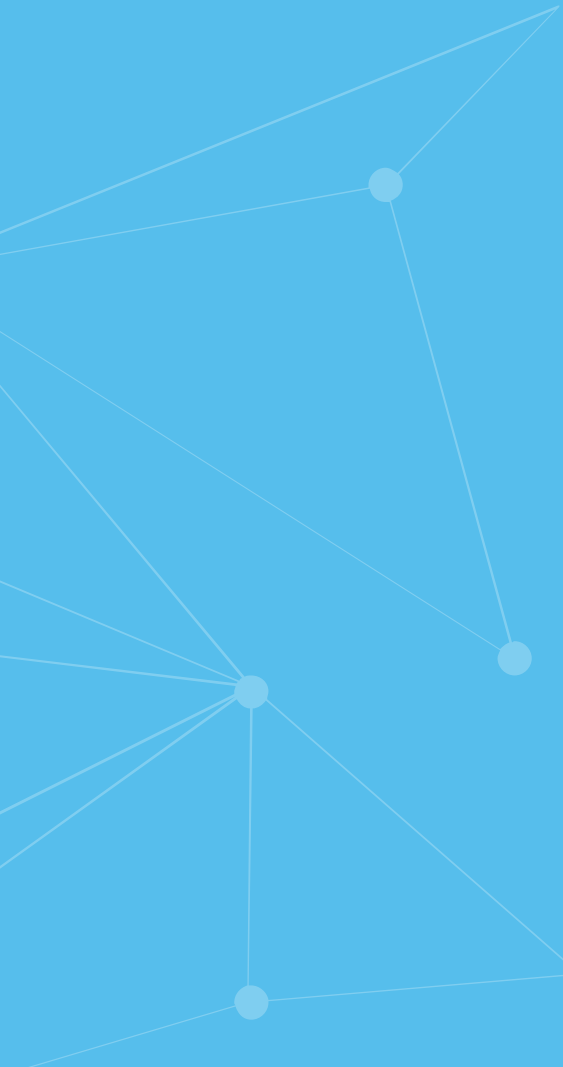
Generation time

0

:

00

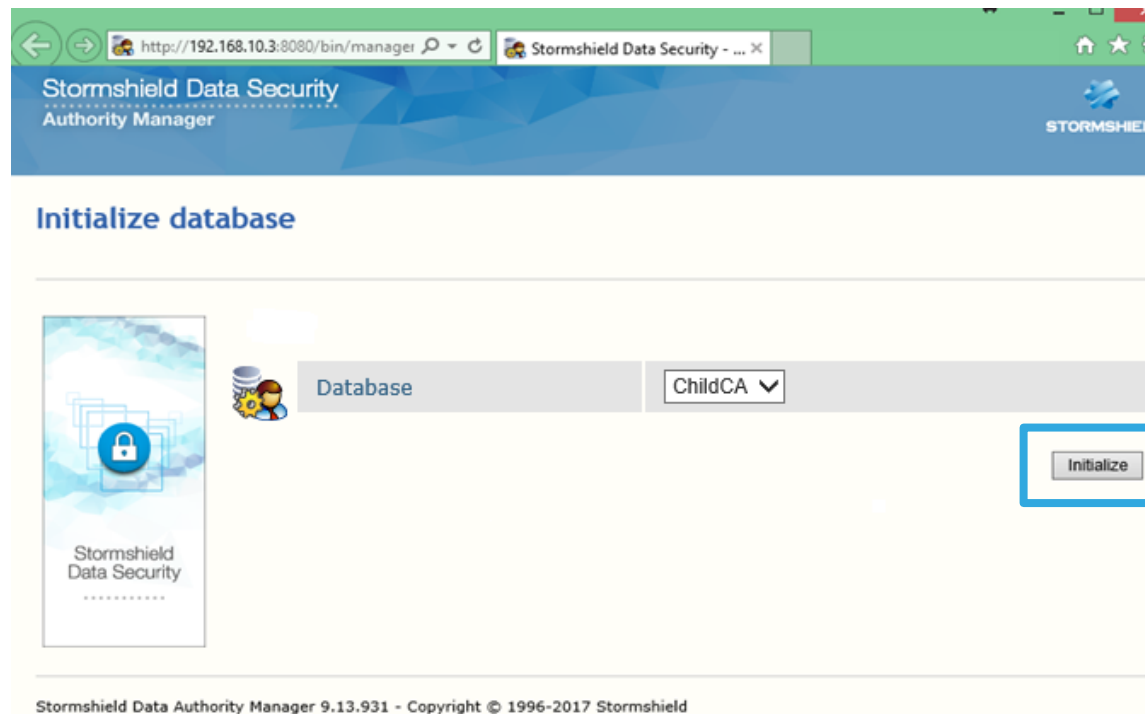
Click on **Apply modifications**



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)

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

☒ Store keys in the **internal** cryptographic module

☐ 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 >>

STORMSHIELD

63

Option: initializing the Child CA (continued)

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	☒ Draw an encryption key ☐ Import an encryption key from a PKCS#12 file:	RSA 2048 bits
	File name	
	Password	
Exportable key	☐ Mark key as exportable	

Validation

The following operations will be performed:

- encryption key drawn by the internal cryptographic module.

Click on Proceed

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	
Password confirmation	

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.

Option: initializing the Child CA (continued)

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.

Click on Proceed

Authority certification

Report



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

Authority identity

Common name	Child CA
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	☒ 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: initializing the Child CA (continued)

 **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: Edit message
Go to the CA's server page	The content of the certificate is automatically copied in the clipboard. Server's URL: Reach URL

Click on **Request processed**

Stormshield Data Security
Authority Manager

Initialize database

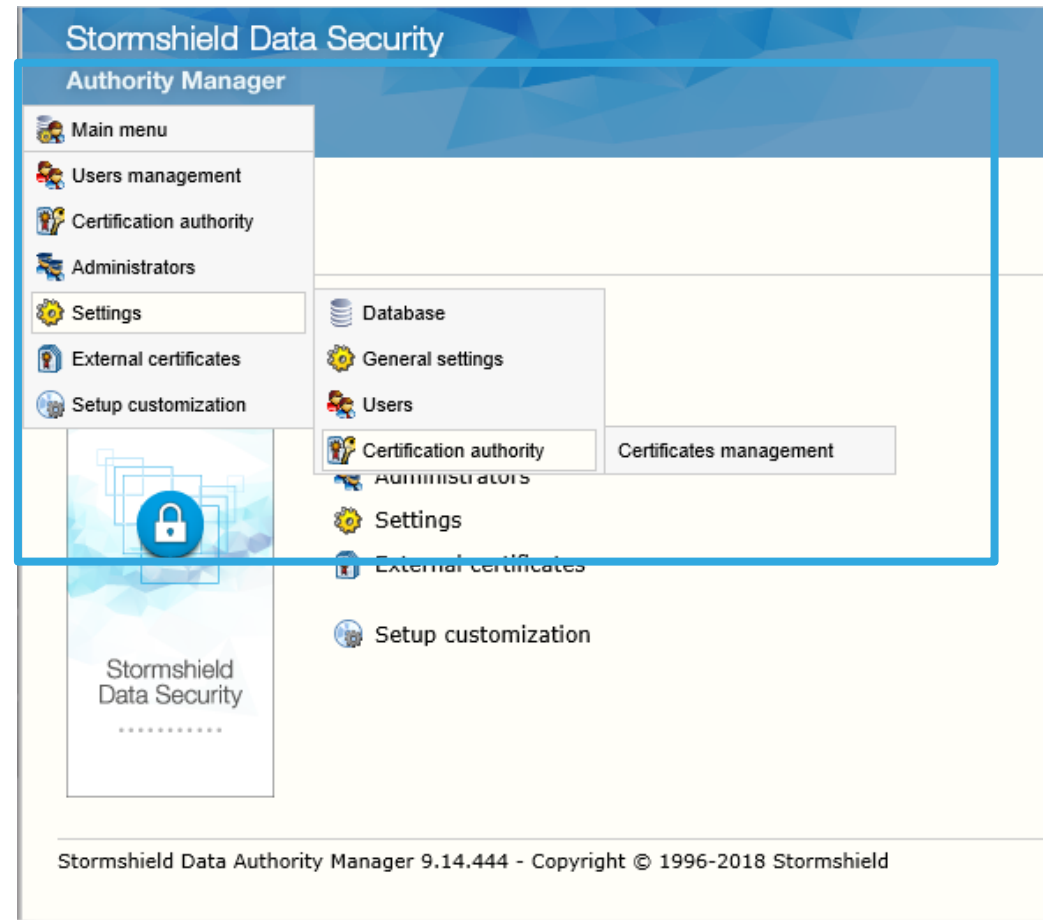
Database initialization complete.

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

 [Home](#)

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

Option: configuring the Child CA CRL



Option: configuring the Child CA CRL (continued)

Certificates management

 **Certification authority**

 Subject resolution mask

 **External certificate requests pre-fill**



Organization	
Organization unit	
City	
State or province	
Country	(none)

Option: configuring the Child CA CRL (continued)

 **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) ☐ Leave the email address in the identity only ☒ Copy the identity email address into the certificate's SubjectAltName field ☐ Move the identity email address to the certificate's SubjectAltName field
Resolution mask of external certificates' LDAP DN	
Resolution mask of LDAP entry's search filter	(mail=<AltNameEmail>)
Certificates already published on the LDAP server	Default ☐ Keep ☐ Delete ☒ Replace certificates that have the same usages and the same issuer
File-based publication	☐ Activate file-based certificates publication Publication folder: C:\SBMDData\jkr\CertsPublished File format: Binary ▼

Option: configuring the Child CA CRL (continued)

 **Revocation lists (CRLs)**

	Algorithm	Thumbprint algorithm used for signature	SHA-1 ▼
	CRL validity duration	24	hours
	CRLs publication DN LDAP		
	Current CRL's generation location	C:\SBMDData\childca\Crl\childca.crl	
	CRLs archiving folder	C:\SBMDData\childca\CrlHistory	
	CRL generation	☒ By default, request CRL generation at each revocation	
	Expired certificates	☐ Include expired certificates in CRL	
	CRL distribution points	http://%IP_SDAM:8080/childcrl/childca.crl Add Copy Delete Distribution point: http://%IP_SDAM:8080/childcrl/childca.crl	

Option: configuring the Child CA CRL (continued)

Automatic CRL generation service



Generation service	☐ Activate automatic CRL generation
Frequency	24 hours
Generation time	0 : 00

Email notifications

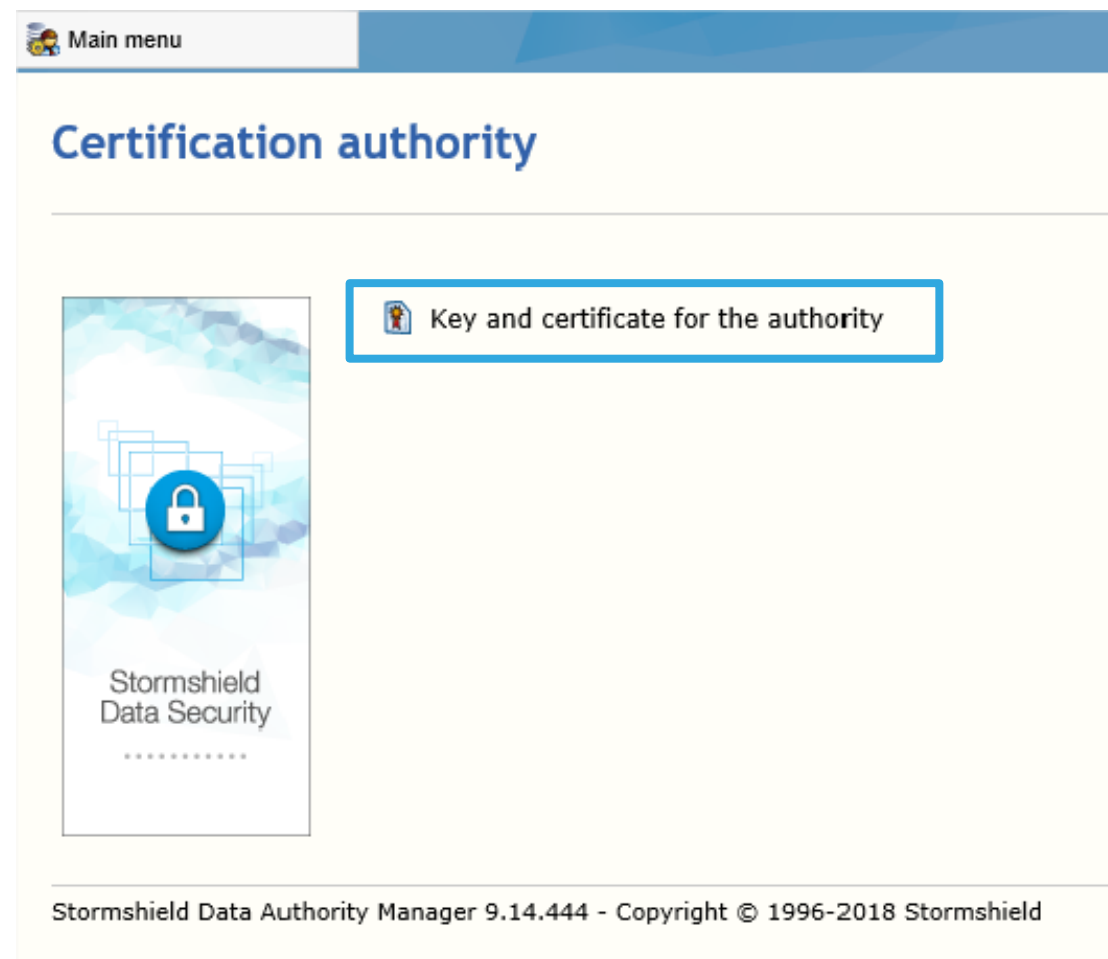
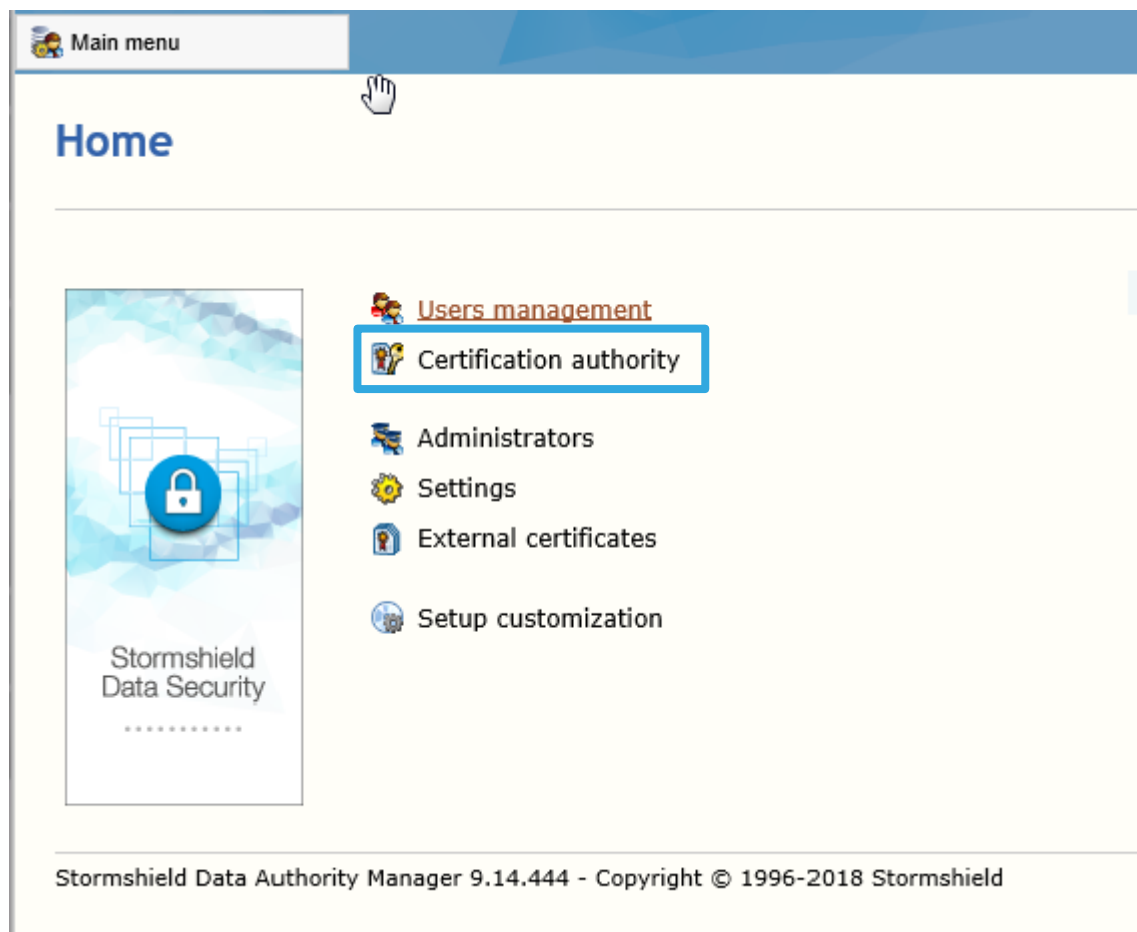


Certificate request deposit	☐ Send email notification on certificate request deposit Email address: Subject: Template: C:\SBMDData\jkr\MailTemplates\template_request.sbp
Internal request validation	☐ Send email notification on validation of internal request Email address: Subject: Template: C:\SBMDData\jkr\MailTemplates\template_validation_internal_admin.sbp
	☐ Send a notification email to the requestor Subject: Template: C:\SBMDData\jkr\MailTemplates\template_validation_internal_user.sbp
	☐ Send email notification on validation of external request Email address: Subject: Template: C:\SBMDData\jkr\MailTemplates\template_validation_external_admin.sbp
	☐ Send a notification email to the requestor Subject: Template: C:\SBMDData\jkr\MailTemplates\template_validation_external_user.sbp

Confirm operation:

Apply modifications

Option: validating the Child CA



Option: validating the Child CA (continued)

Stormshield Data Security
Authority Manager

Main menu Properties Certificate management

Issue a certificate request

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

Certificate request

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

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIICeCCAYACAQAsG9w0BAQAFRAOCQAMIBICgKCAQEAQ17pC4qU6AIIInZHKEhA
xbTm6q25REAMuNWSK2k5zKaGf+knAWlpyglr0P1tiIGOpK6SiEGDhjyeV3XcQwf
WbQqK+IH+8FYOVV1vOQM2Mog188JBvGfyr1xZ/1PCUKtHuI9dKEFa21XEOFPVCNA
R2gIdccFstkrSQq56LbbyaC9eT+w1UTOMP96LIH5a0QUpGKCGOcnjOqJrXq3HB9A
46HgQ14ndCvFPMjpl1LZIRiDng+K+eIv7uMkdKcAdvrymSNWZXIyCCu9A1fzGgU9
v1axFqgh1FkyGvauEvMSyR2oKdhv7Ge0afvcyzhocCFgk8L7nB8ST01COAL
nOIDAQBoA8wOCVJk6Tihv0NAQEFBQADgEBAlvZFDQOQK-rjTV447KKG99MxIVQO
zILAbFfp+R7yKQgtbx1DAQfXSmDxM1Ktdh/dy42UvBjYgLLkppPMS+gvM/8m1PMMC
b08r11ECTatAhpAaFhbZvc/vcFYEYL6R+ORSNvL1Sc1CUIm07mMEW1jx4Op7+7t
DcKntCrdVDmSz+eqV9dIrBkChSGRgzh1y98Cqk6Pa5GgADQeKRIeoJ5MeZTF2b7
8hFqr6pEy5DqWIAf7paw+N5eML3qLC5tJvvNk5drmk0LO3xpxhSOMZDtcG001RiCn
pFKLYkjayin/9RMMGrBG/feY0gzhSgQN7ecUcIvvy0B11YfDYN3ikKfke8k=
-----END NEW CERTIFICATE REQUEST-----
```

Certificate request in base 64 format

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

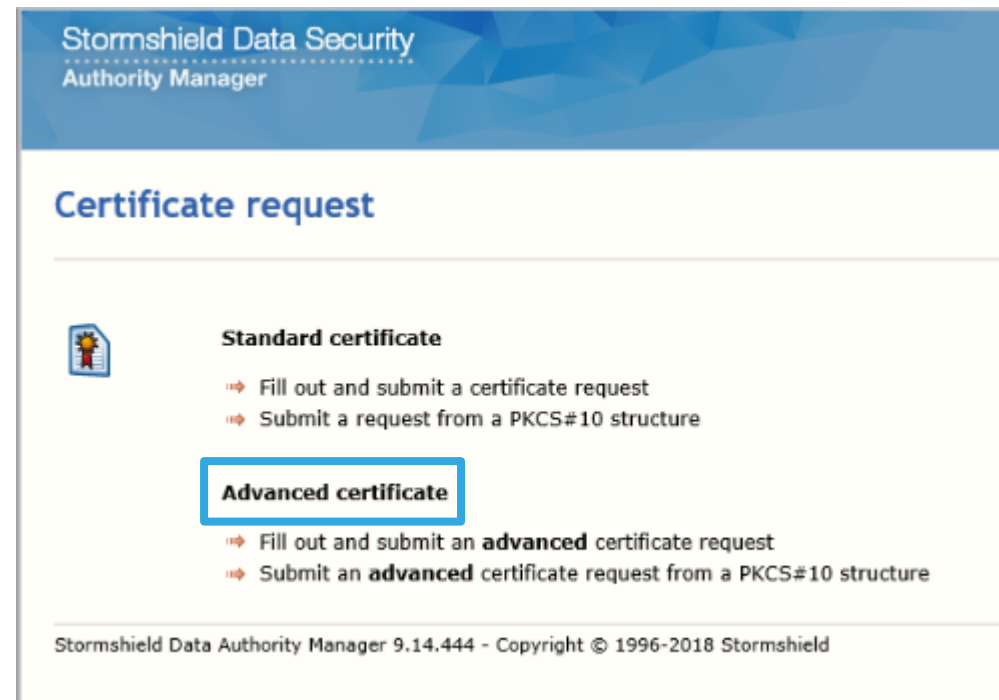
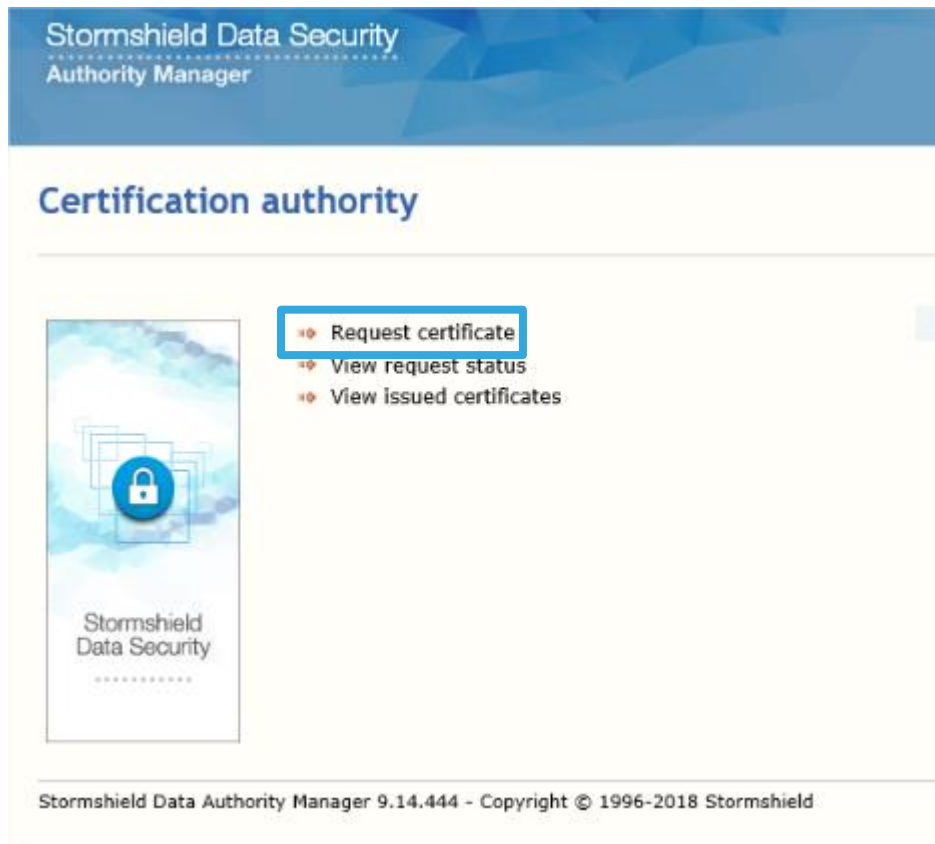
Voulez-vous ouvrir ou enregistrer Child CA.p10 (1000 octet(s)) à partir de 192.168.6.2 ?

Ouvrir Enregistrer Annuler

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)

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 Parcourir...

Certificate

Template Certification authority

Alternative identity

Email address	
Domain name	
IP address	
Universal principal name	

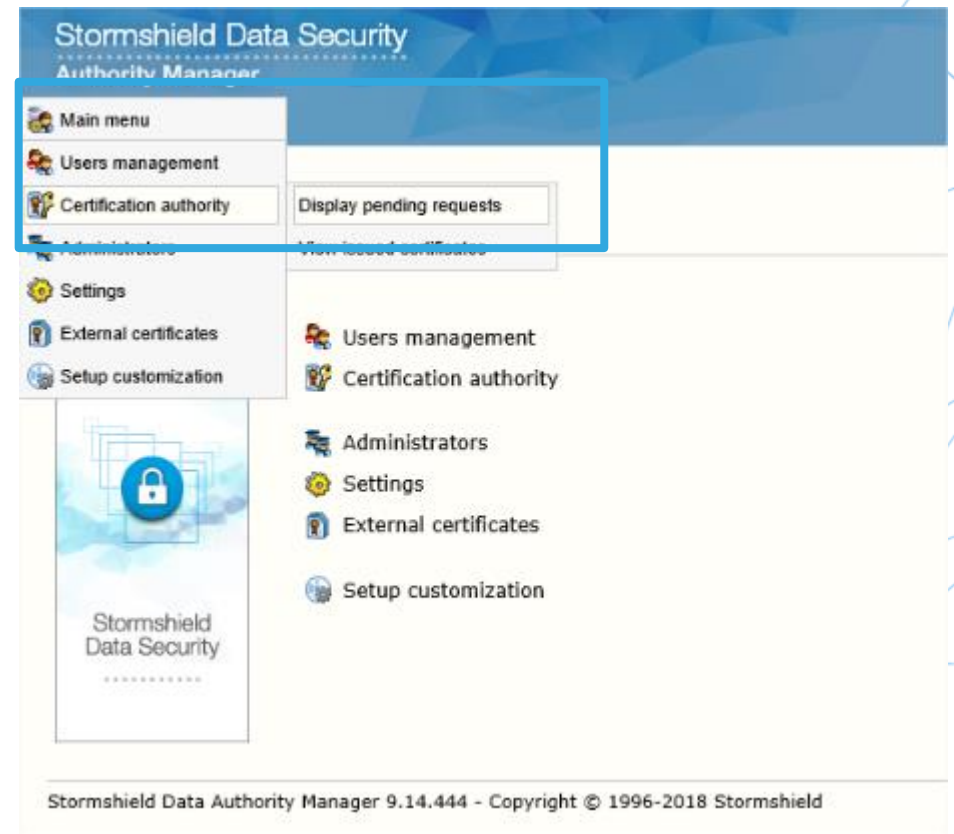
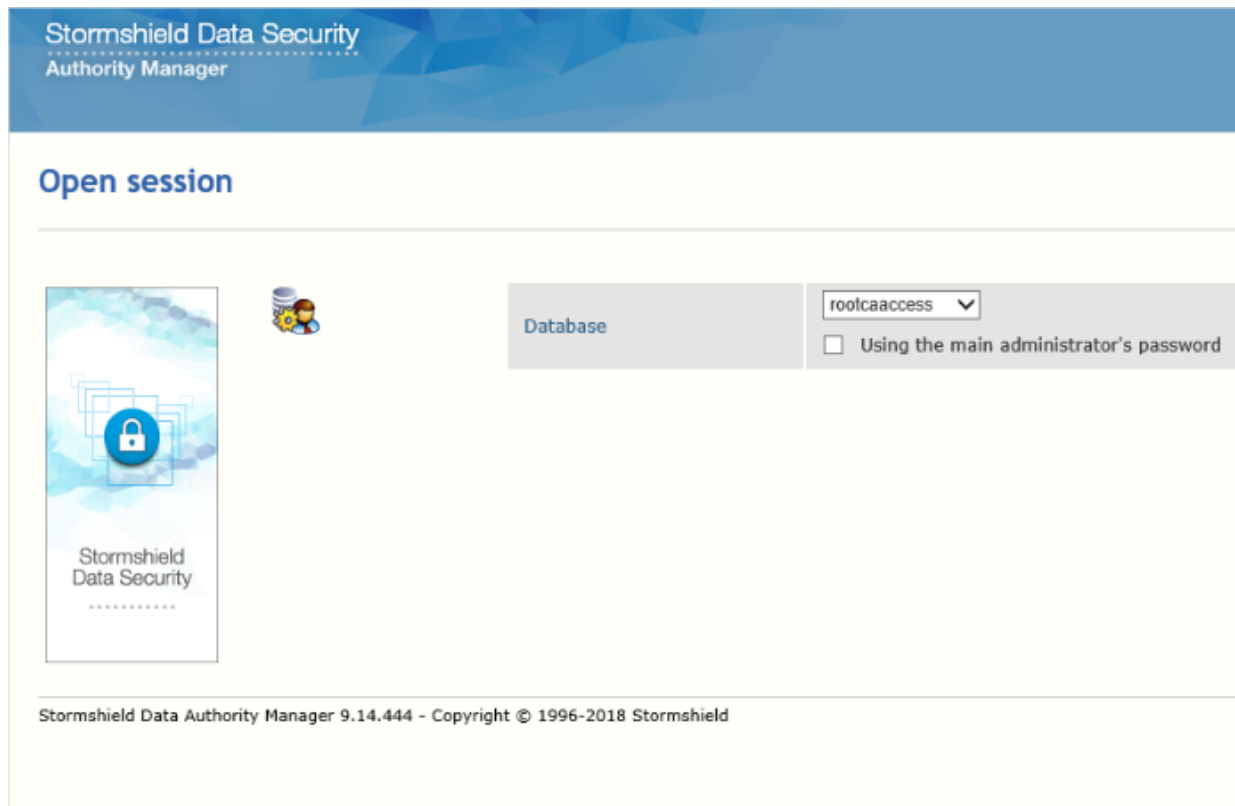
Contact

Email address	
Phone number	
Comment	

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)

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

Deny request

Option: validating the Child CA (continued)

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

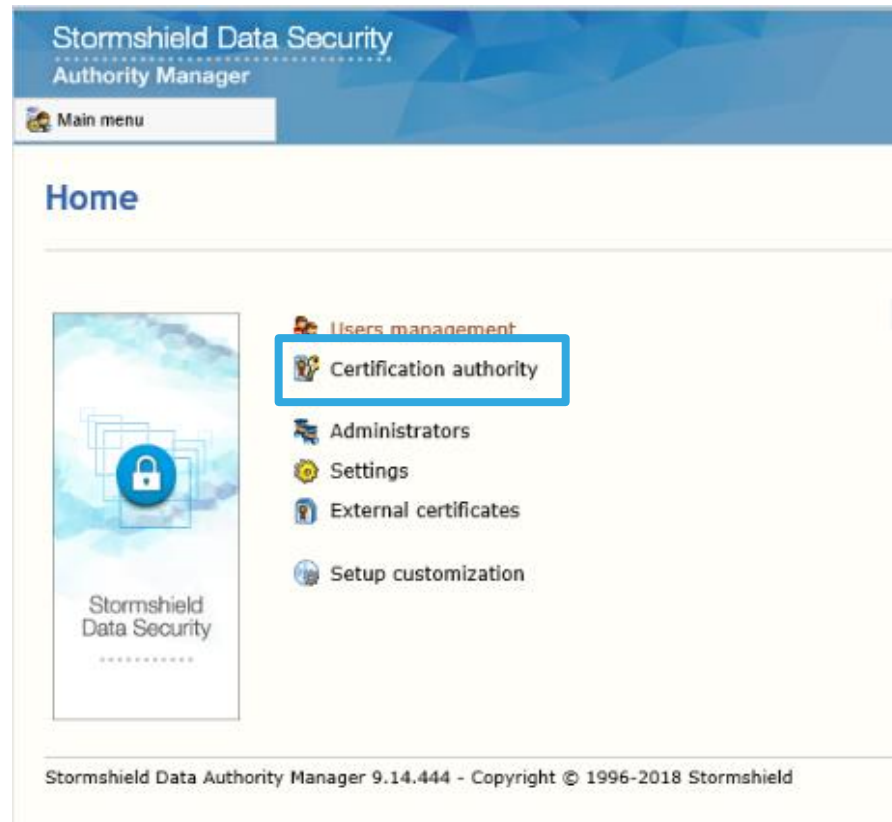
Copy...

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

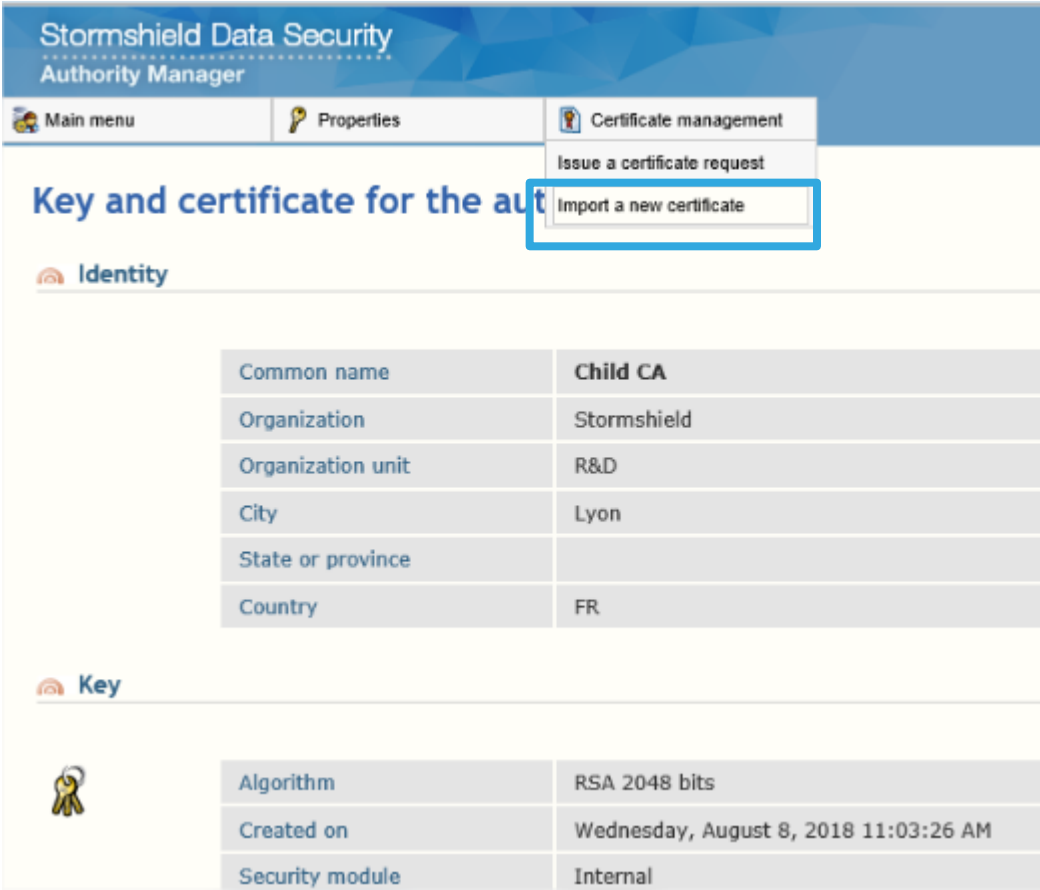
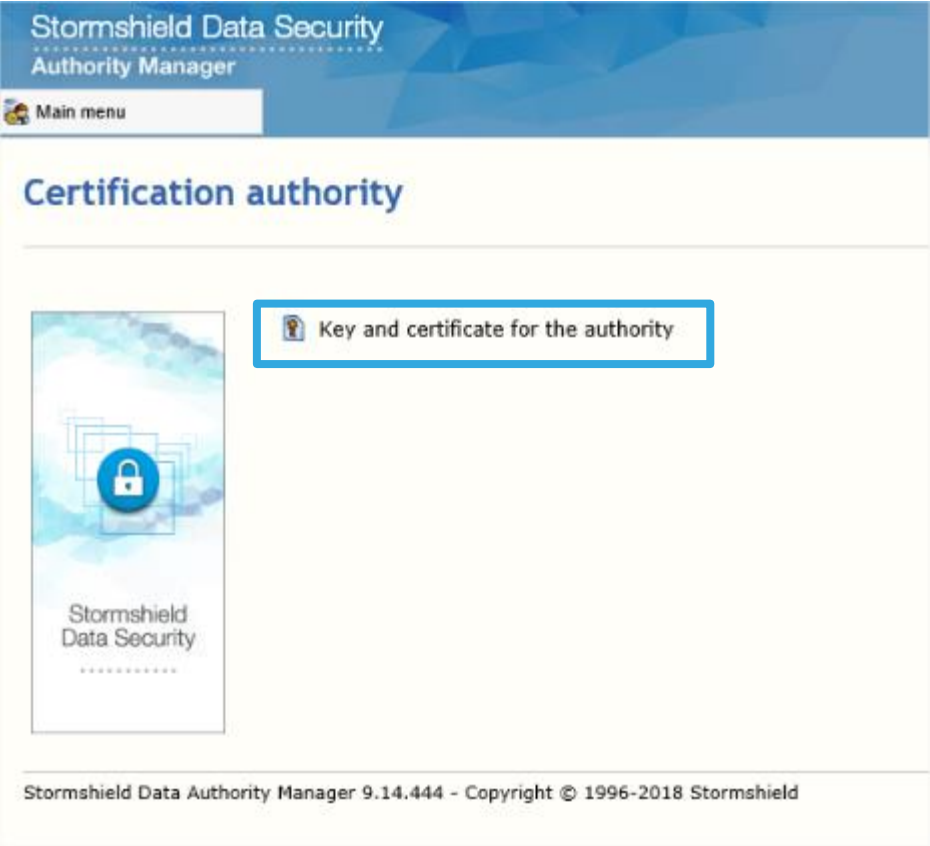
Copy...

Option: validating the Child CA (continued)

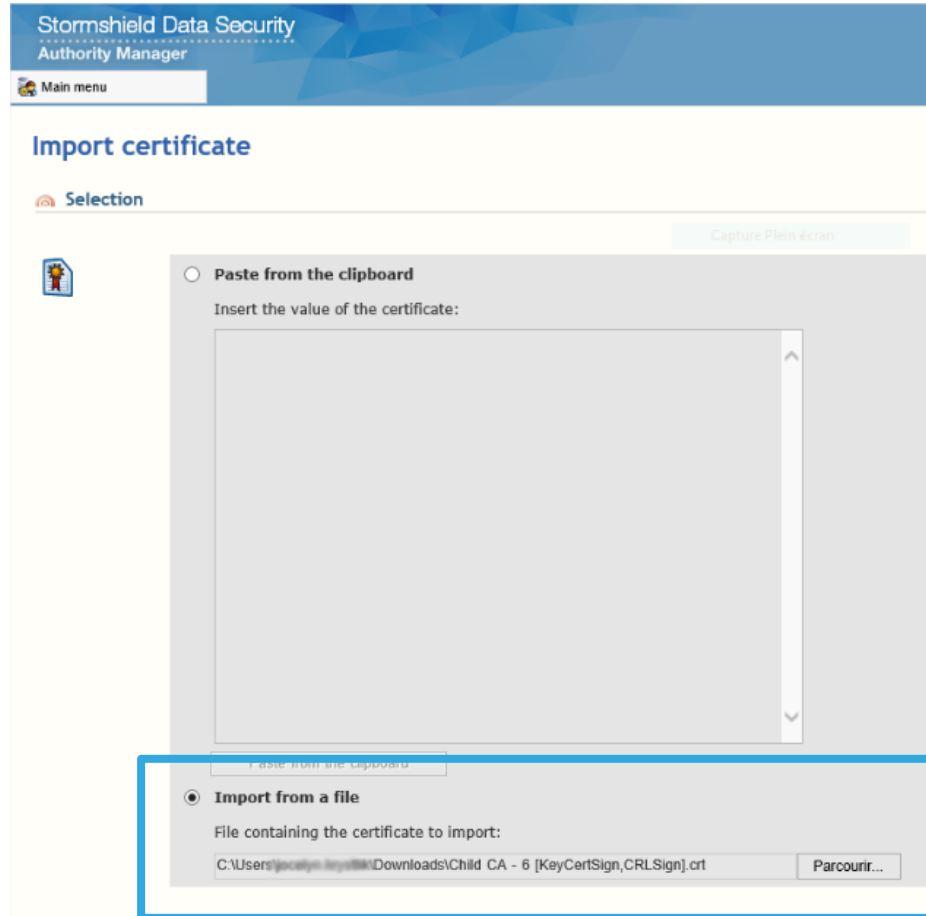
- Connect to the Child CA on the following web page and select the base:
http://%IP_SDAM:8080/bin/manager.exe/OpenSession



Option: validating the Child CA (continued)



Option: validating the Child CA (continued)



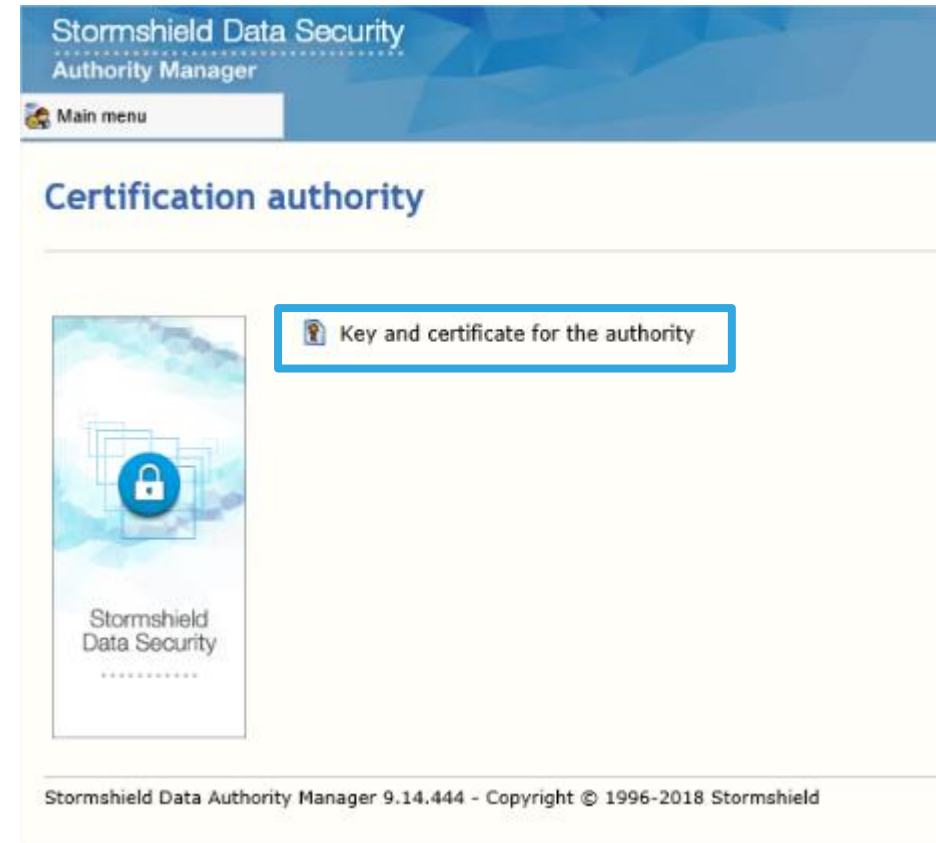
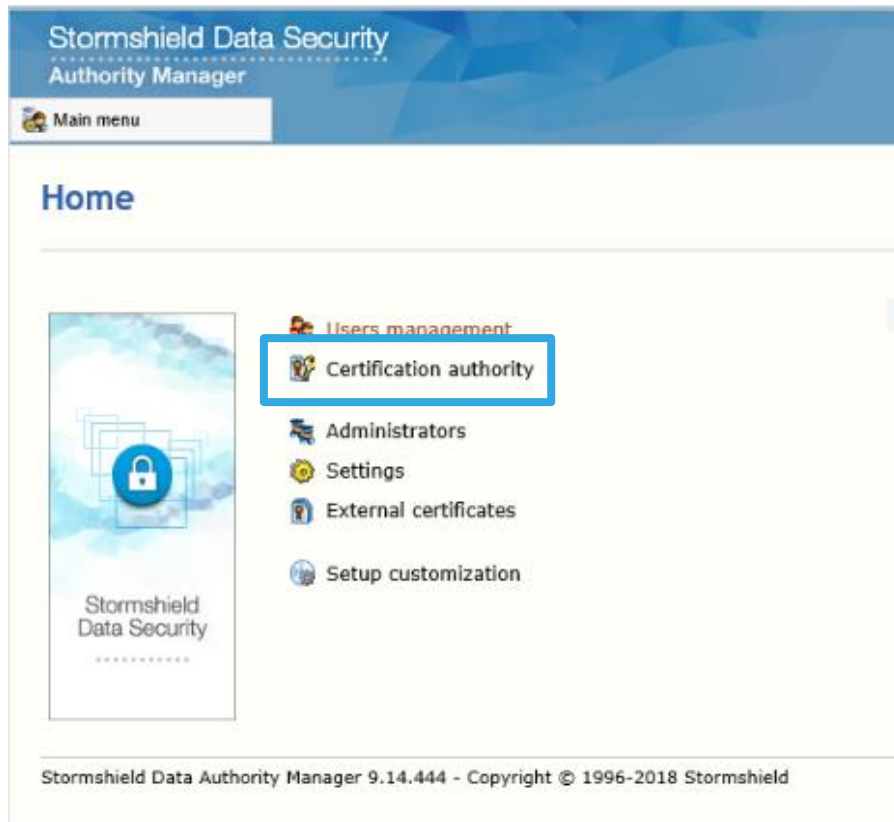
Click on Import



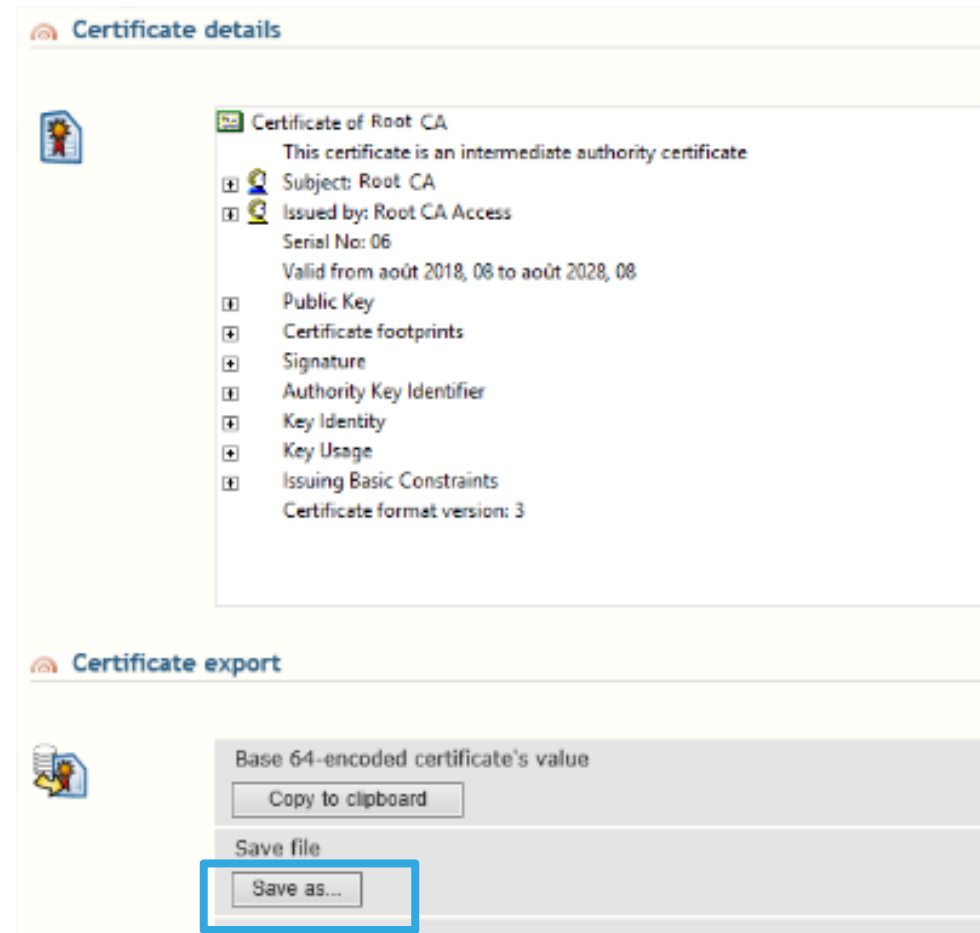
Click on Import the certificate

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

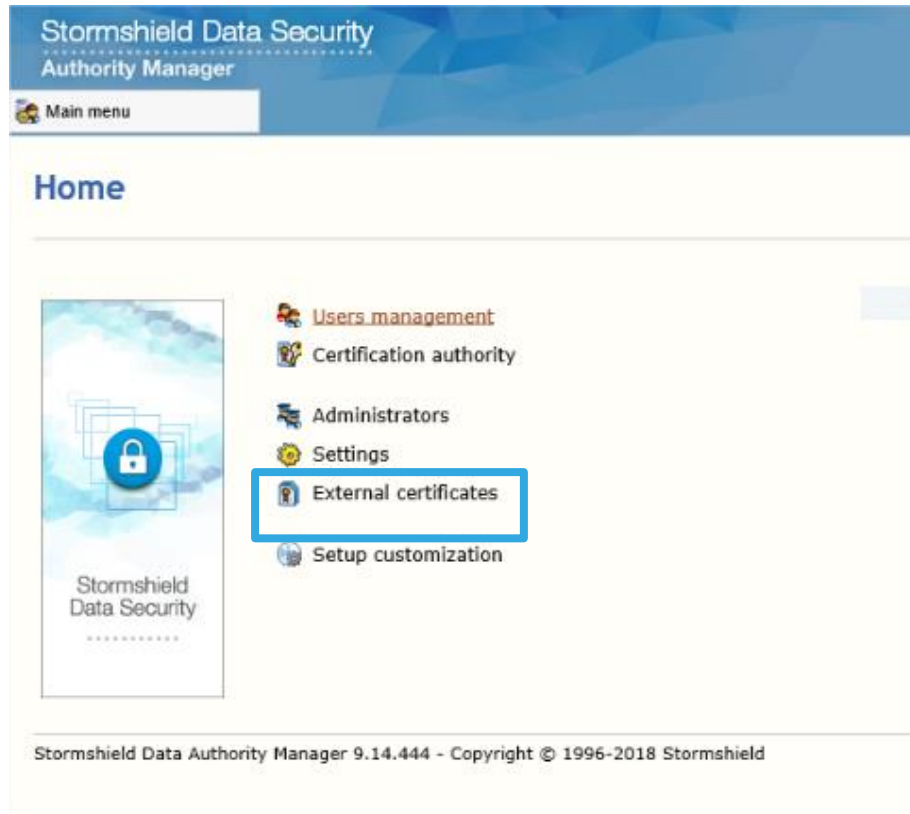


Option: validating the Child CA (continued)



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)

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: [Import...](#)

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

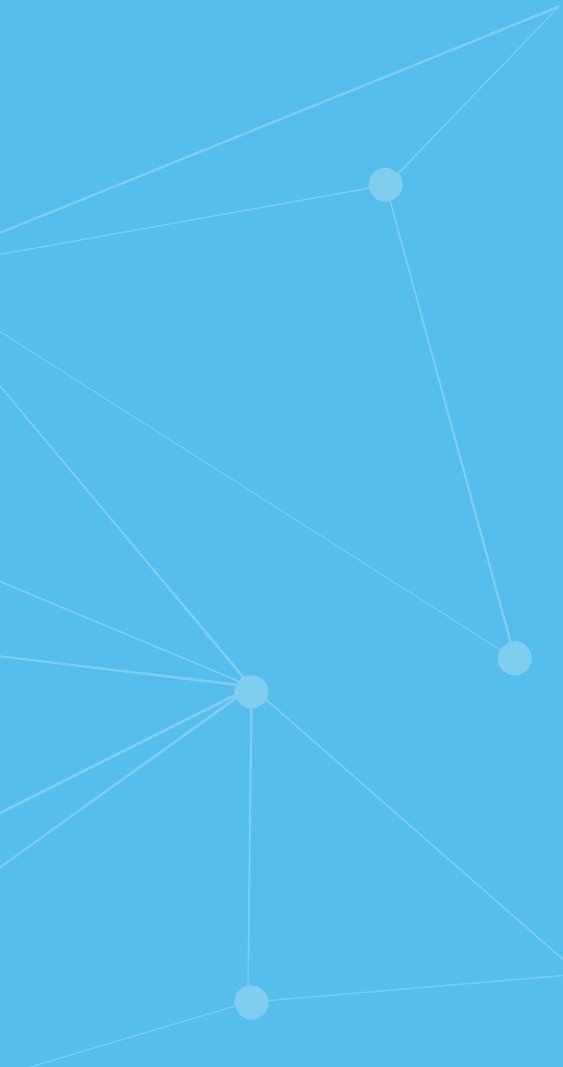
Properties

Label:

Validation

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

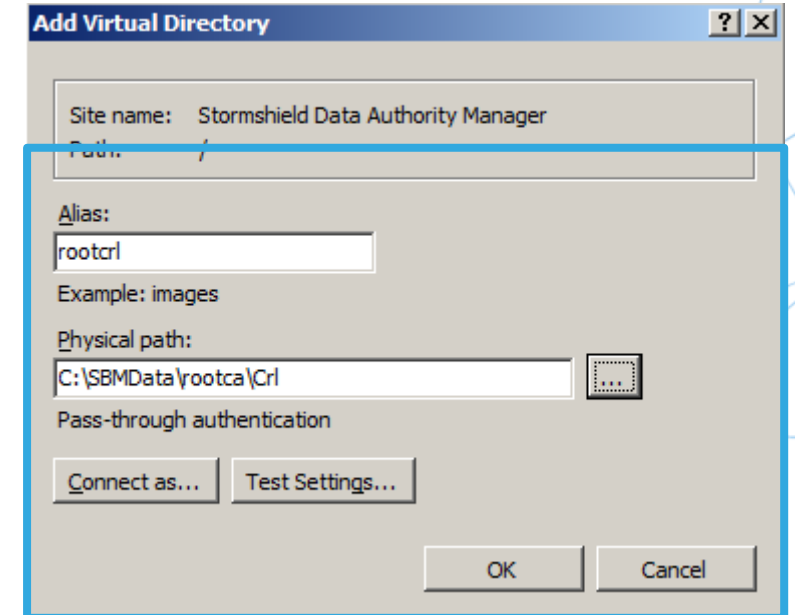
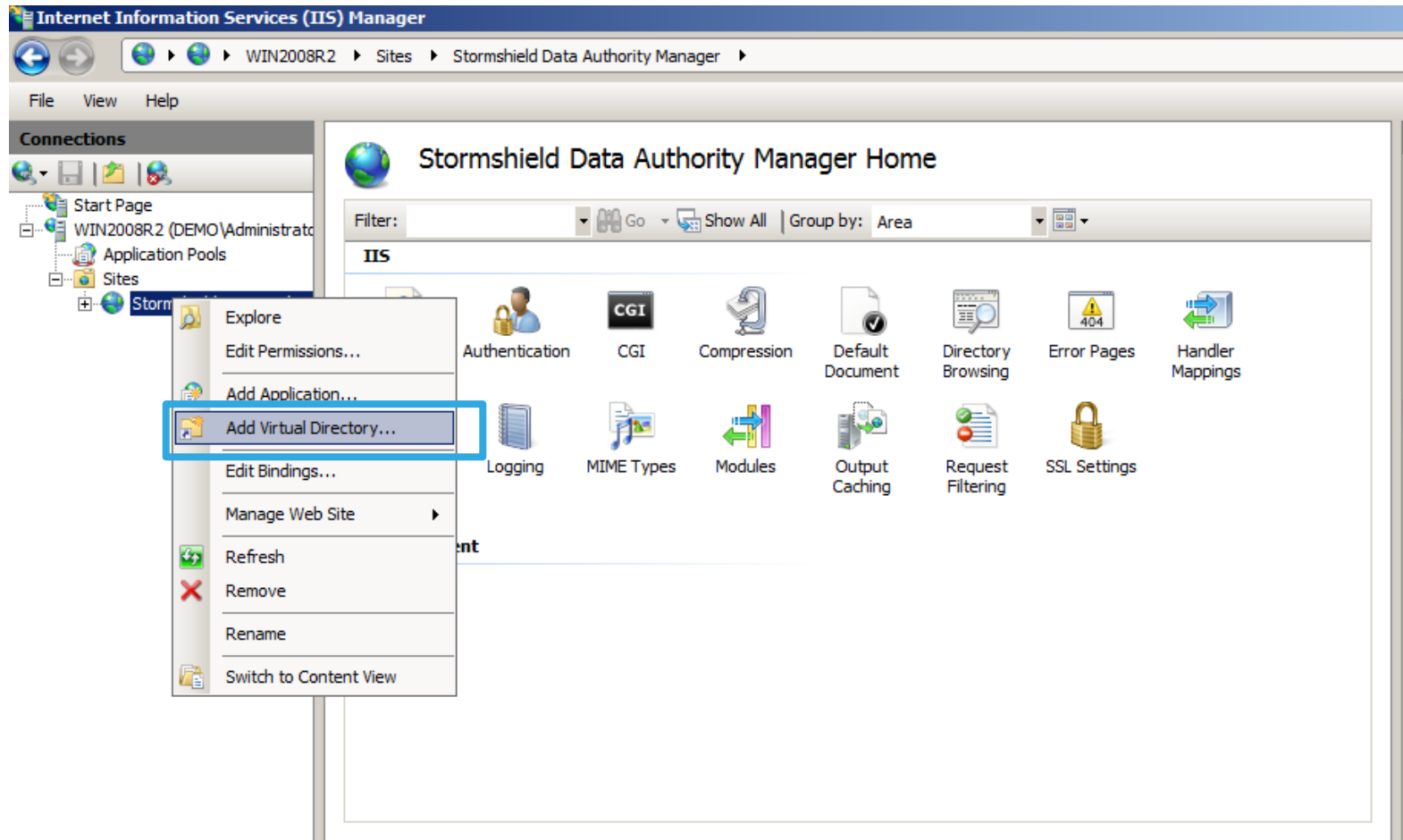
Confirm operation: [Import](#)



Configuring the IIS server virtual directory

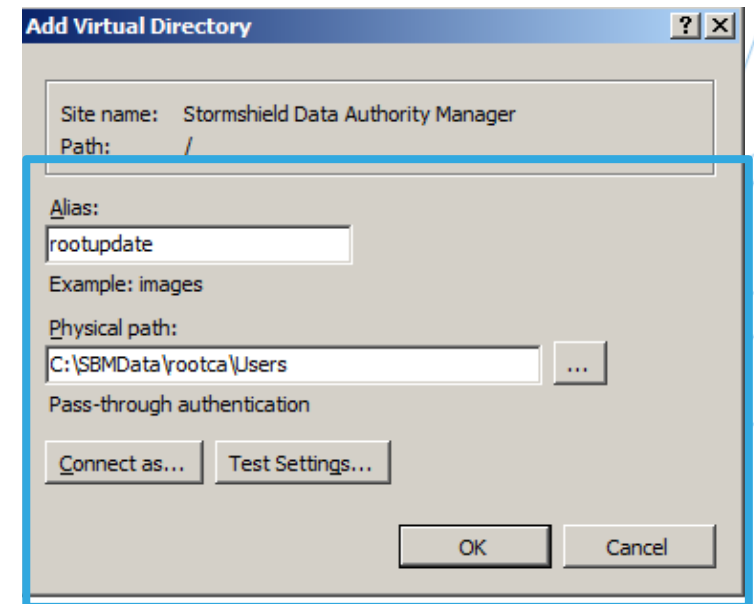
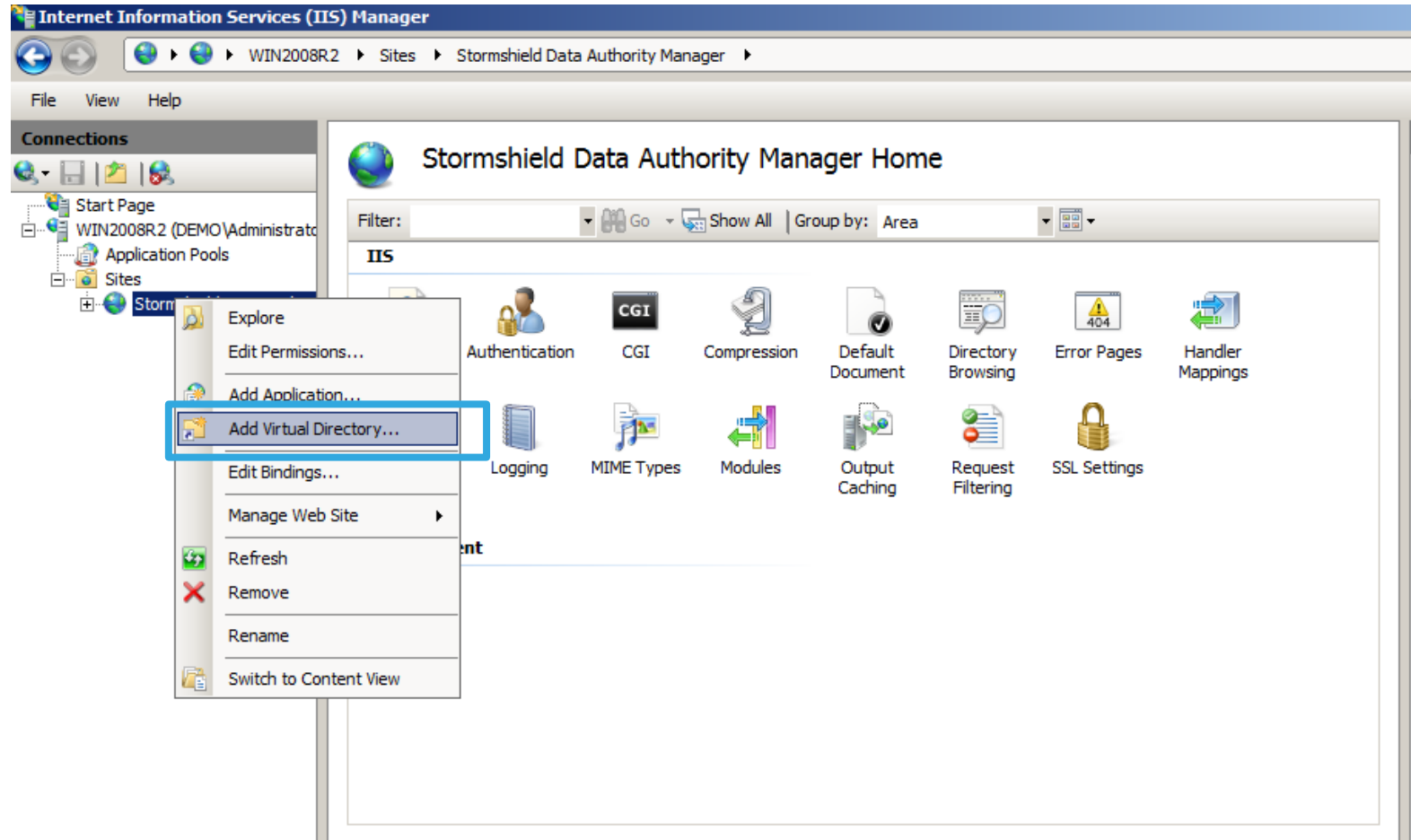
Configuring the IIS server

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



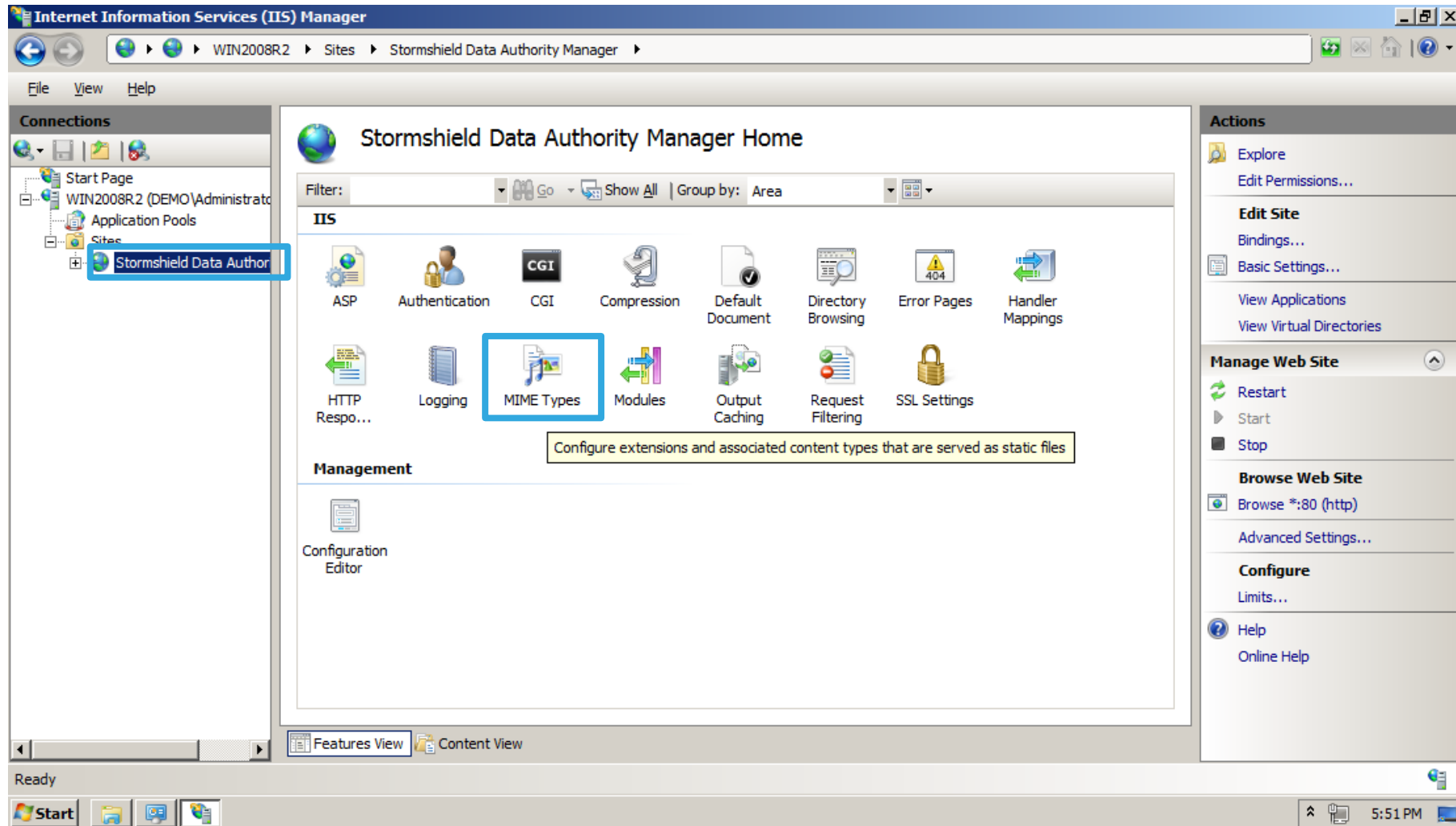
Configuring the IIS server (continued)

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



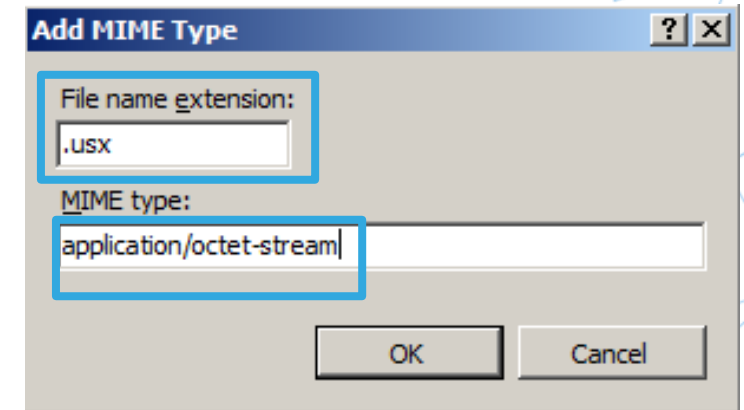
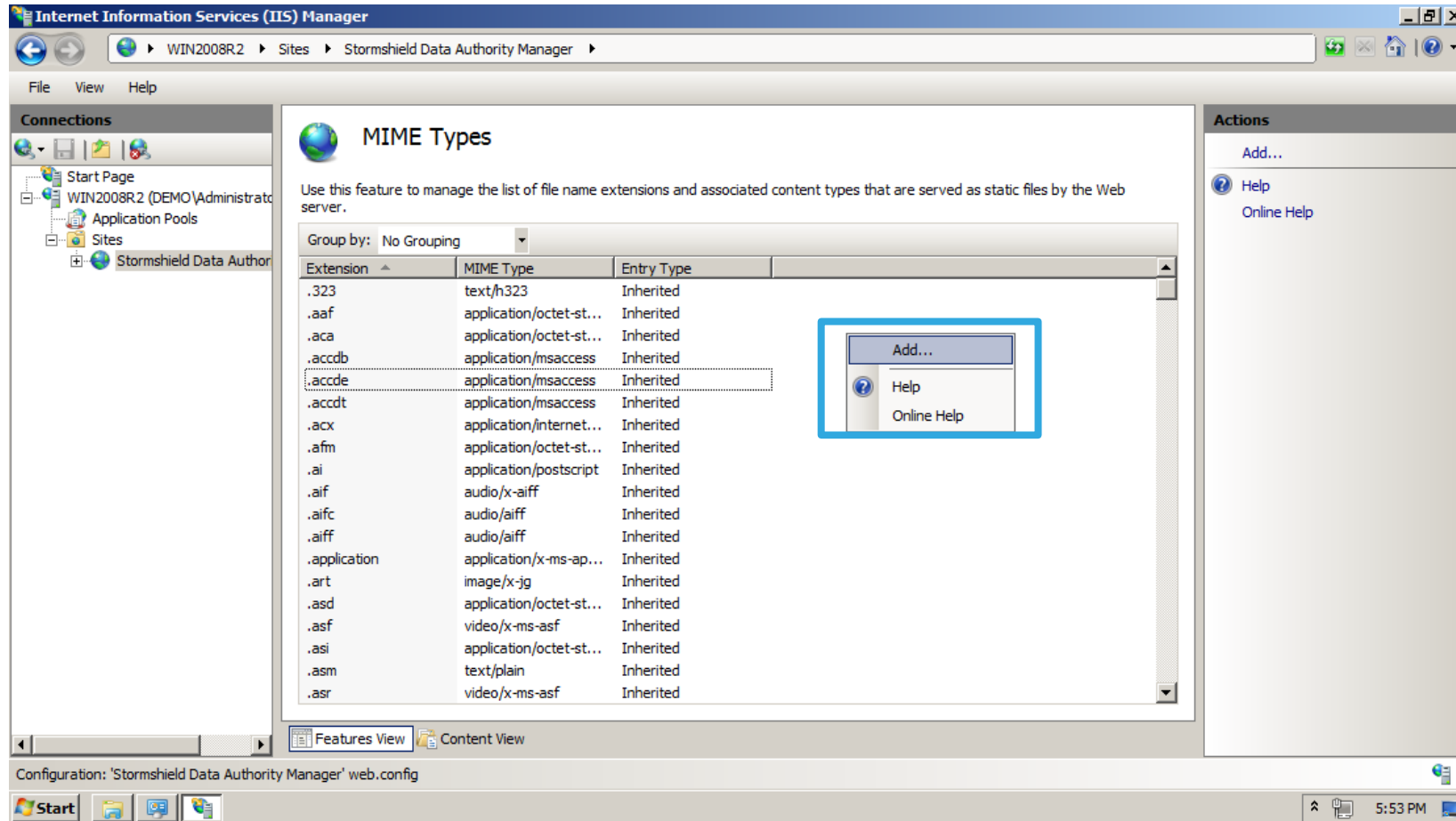
Configuring the IIS server (continued)

Double click on **MIME Types**



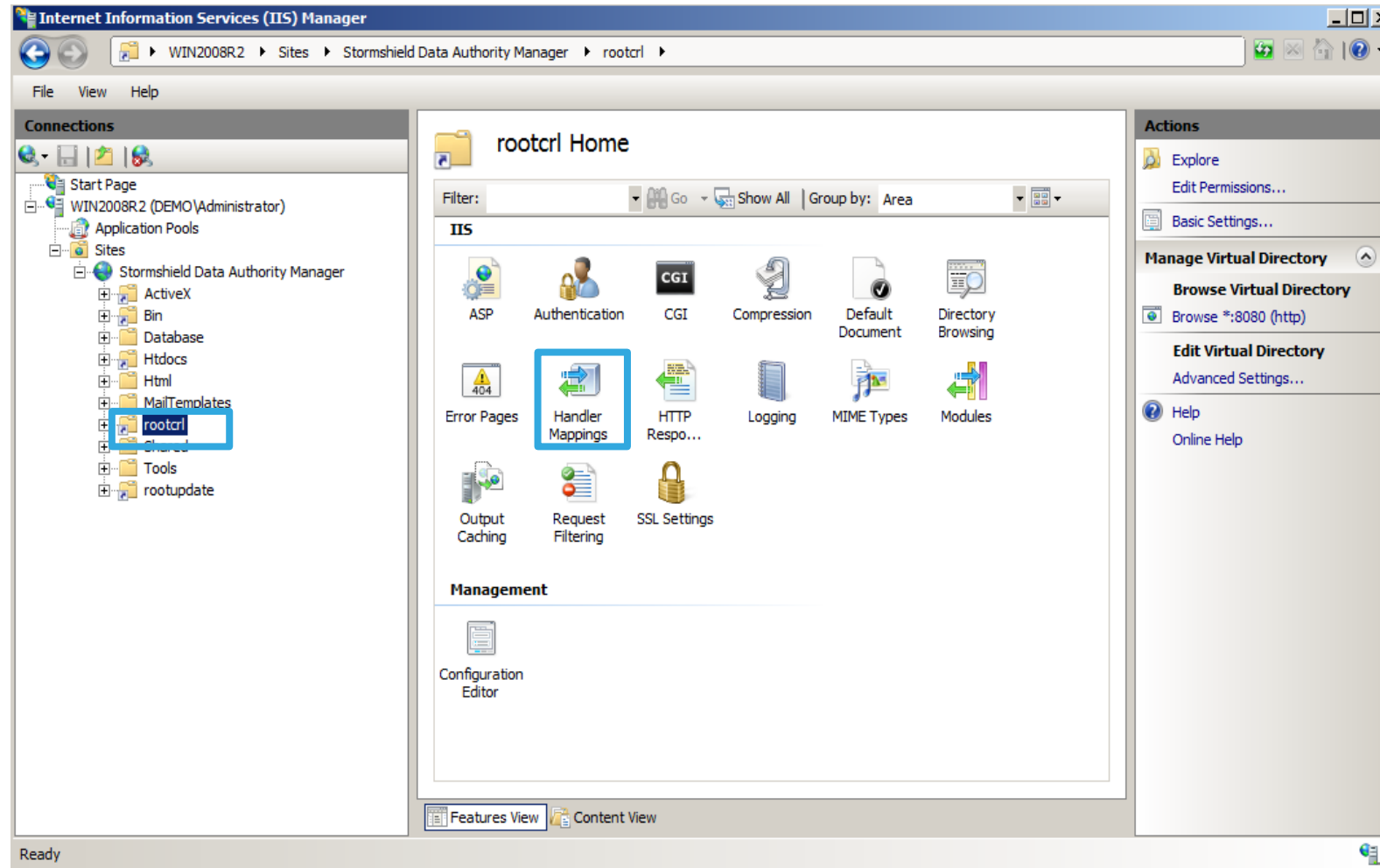
Configuring the IIS server (continued)

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



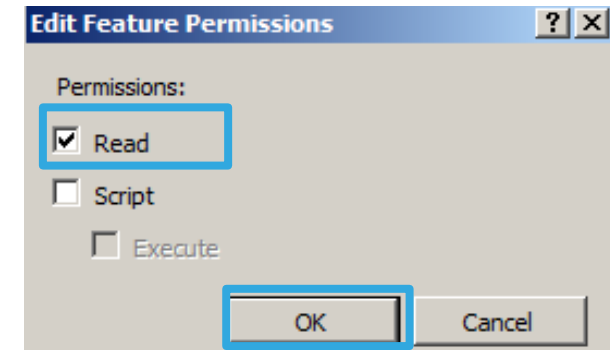
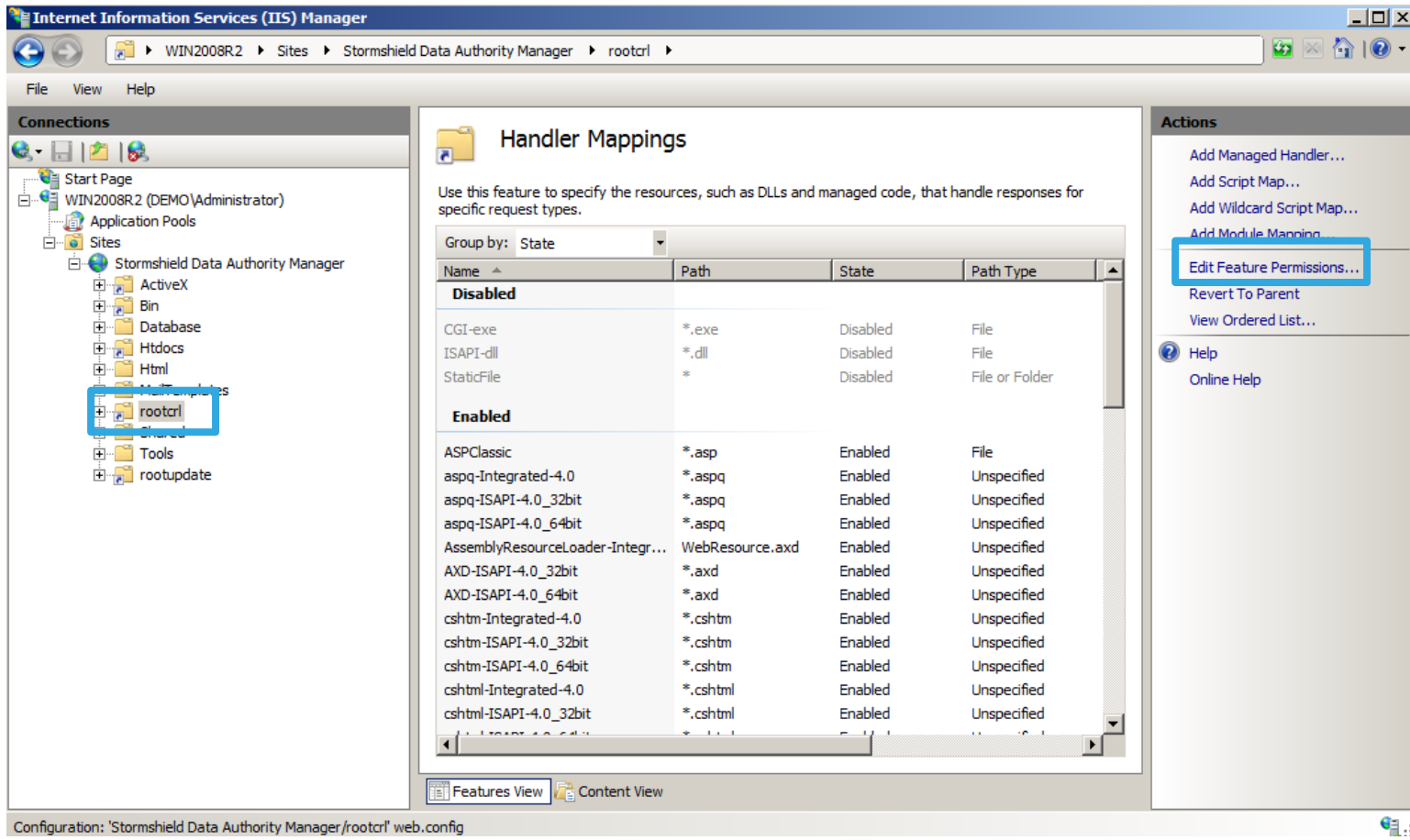
Configuring the IIS server (continued)

Expand **Stormshield Data Authority Manager** and click on the virtual directory **rootcr1**. Double click on **Handler Mappings**.



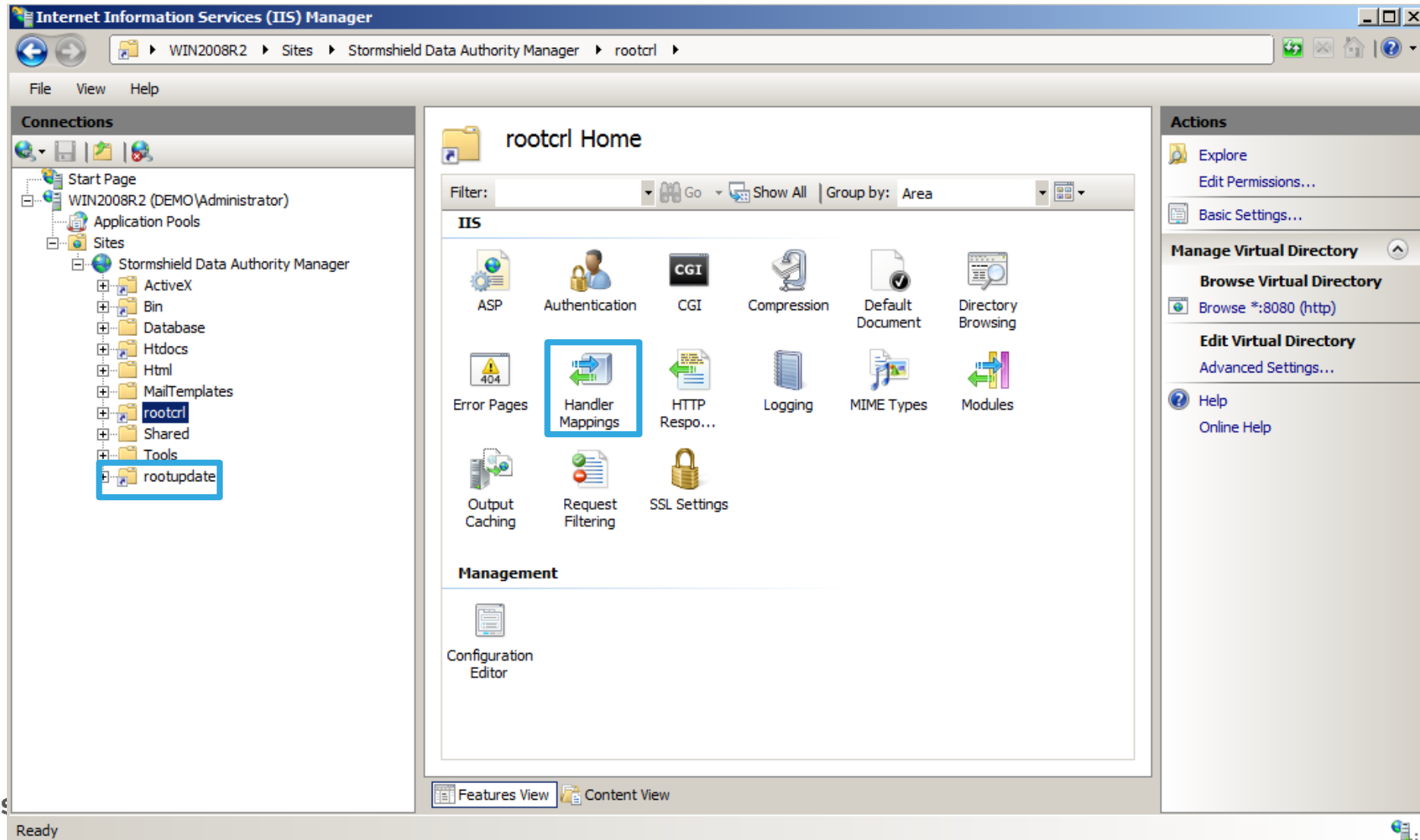
Configuring the IIS server (continued)

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



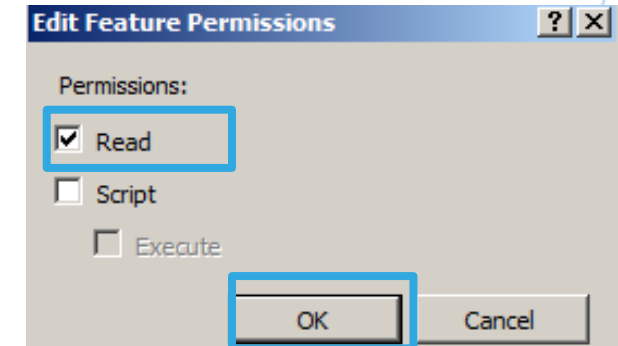
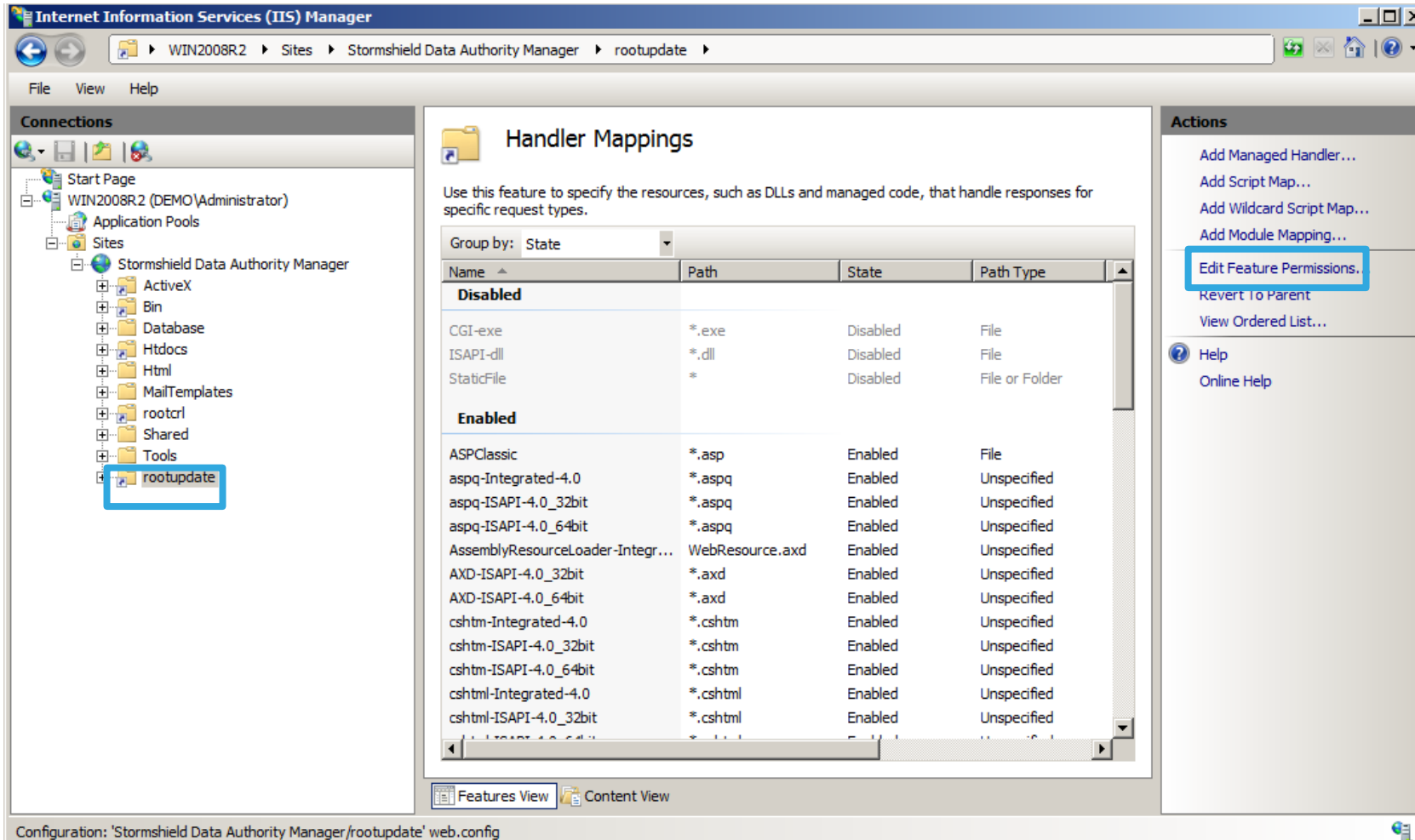
Configuring the IIS server (continued)

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



Configuring the IIS server (continued)

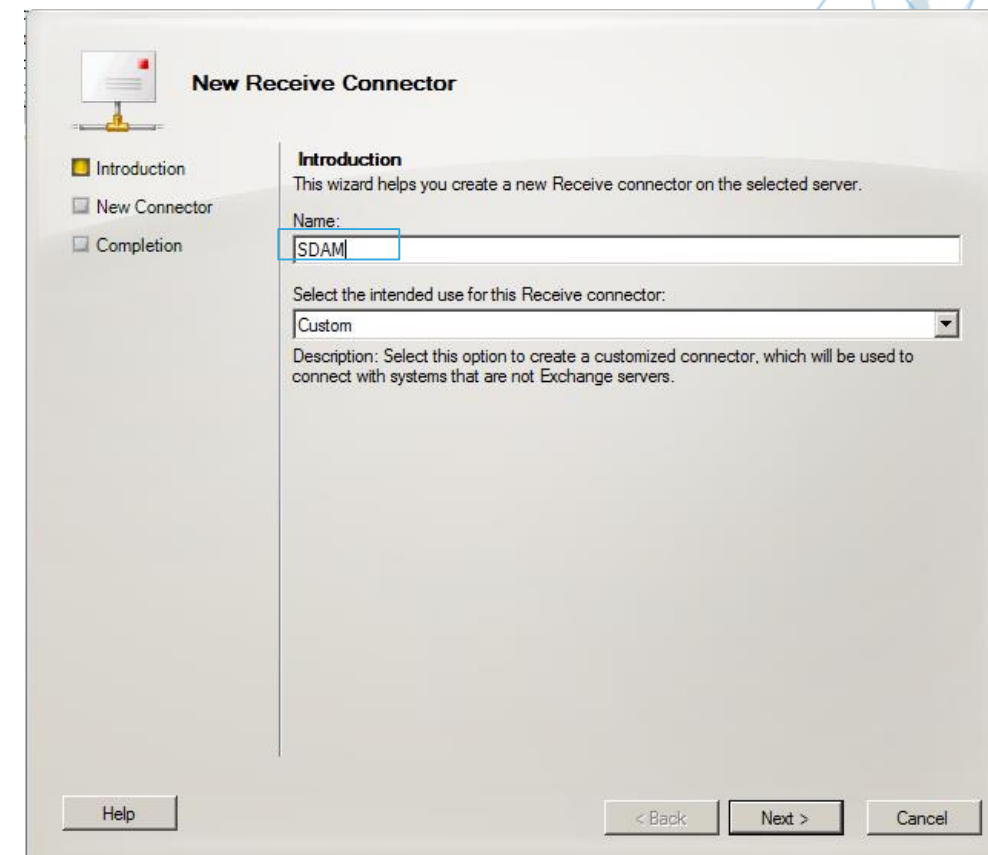
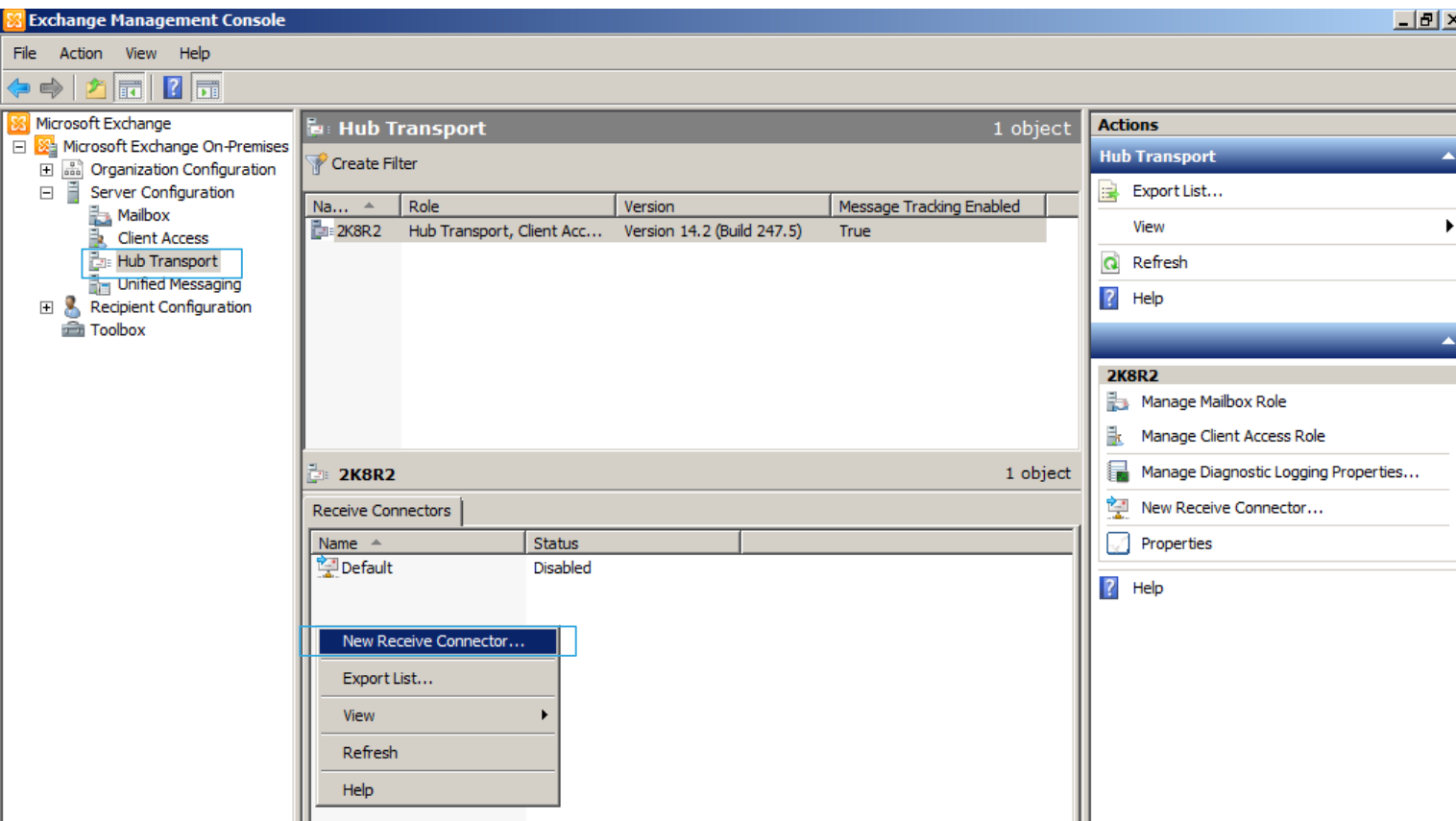
Click on **Edit Feature Permissions**, flag the option **Read** and click on **OK**



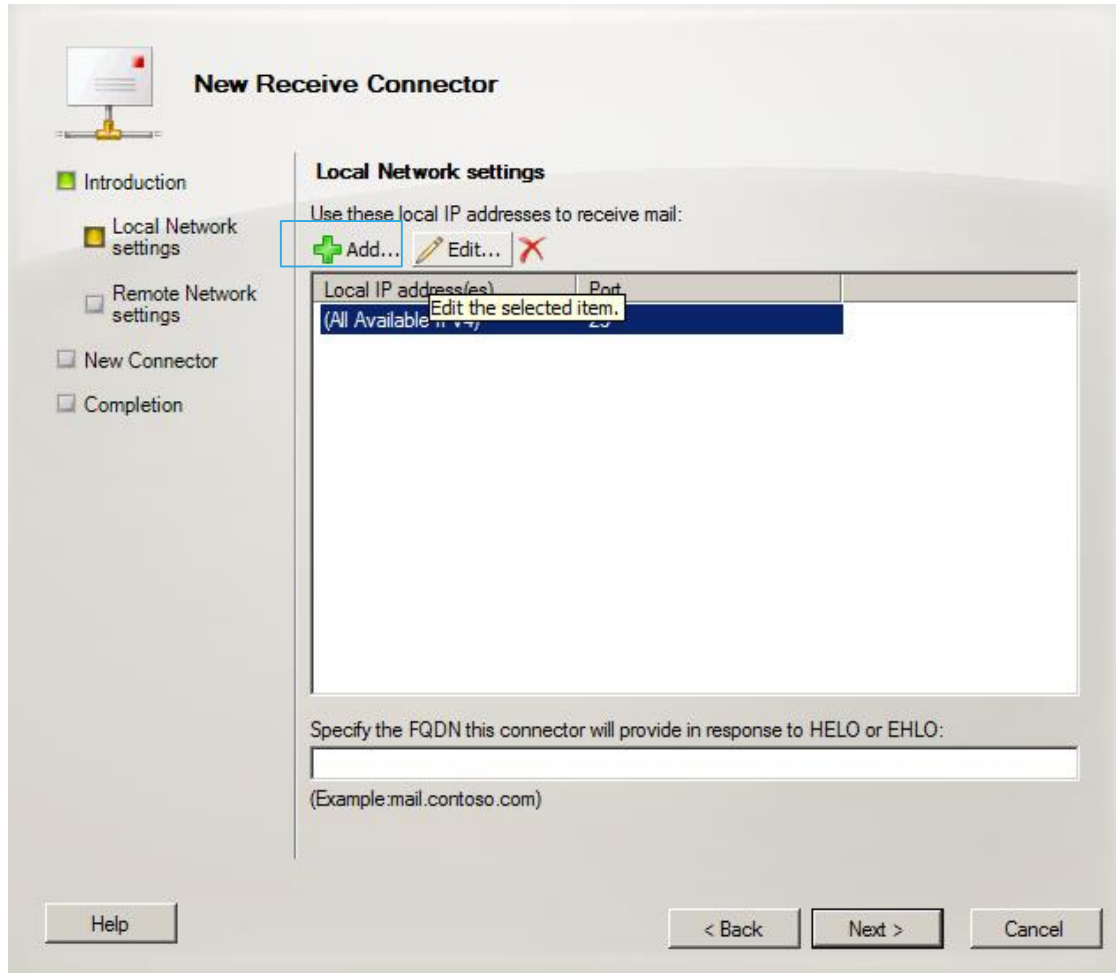


Configuring the Exchange server (option)

Configuring Exchange Inbound Connector



Configuring Exchange Inbound Connector (continued)



The 'New Receive Connector' wizard is shown at the 'Local Network settings' step. The left sidebar contains the following steps: Introduction, Local Network settings (selected), Remote Network settings, New Connector, and Completion. The main area is titled 'Local Network settings' and includes the instruction 'Use these local IP addresses to receive mail:'. Below this are three buttons: 'Add...' (highlighted with a blue box), 'Edit...', and a red 'X' button. A table with two columns, 'Local IP address(es)' and 'Port', is present. The first row contains '(All Available)' and '25'. A tooltip 'Edit the selected item.' is visible over the first row. At the bottom of the main area is a text box for 'Specify the FQDN this connector will provide in response to HELO or EHLO:' with the example '(Example:mail.contoso.com)'. Navigation buttons at the bottom are '< Back', 'Next >', and 'Cancel'. A 'Help' button is in the bottom left corner.

New Receive Connector

Introduction

Local Network settings

Remote Network settings

New Connector

Completion

Local Network settings

Use these local IP addresses to receive mail:

+ Add... Edit... X

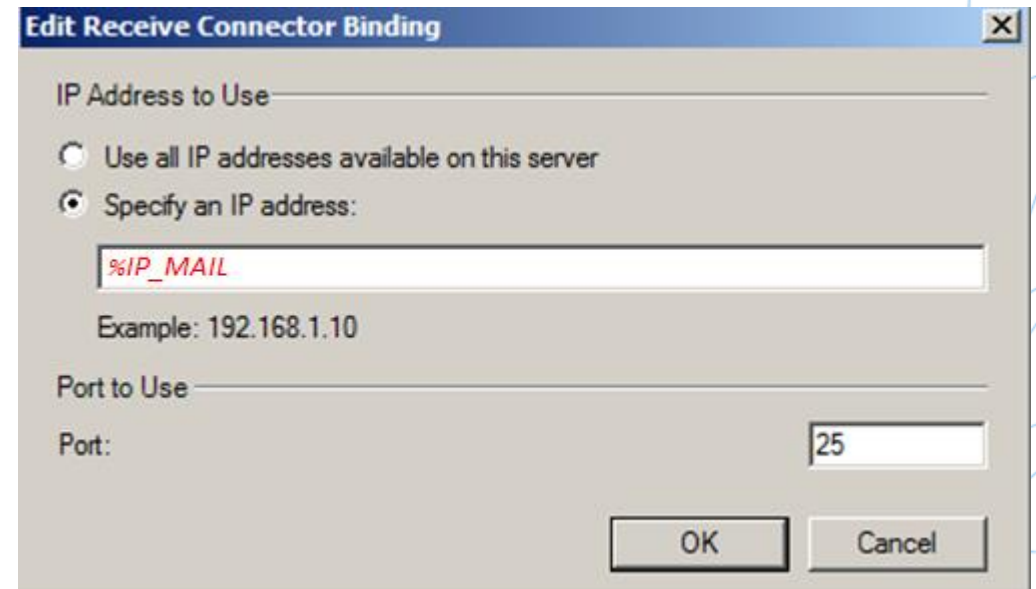
Local IP address(es)	Port
(All Available)	25

Edit the selected item.

Specify the FQDN this connector will provide in response to HELO or EHLO:

(Example:mail.contoso.com)

Help < Back Next > Cancel



The 'Edit Receive Connector Binding' dialog box is shown. It has a title bar with a close button. The main content area has two sections. The first section is 'IP Address to Use' with two radio buttons: 'Use all IP addresses available on this server' (unselected) and 'Specify an IP address:' (selected). Below the radio buttons is a text box containing '%IP_MAIL' and an example '192.168.1.10'. The second section is 'Port to Use' with a text box containing '25'. At the bottom right are 'OK' and 'Cancel' buttons.

Edit Receive Connector Binding

IP Address to Use

☐ Use all IP addresses available on this server

☒ Specify an IP address:

%IP_MAIL

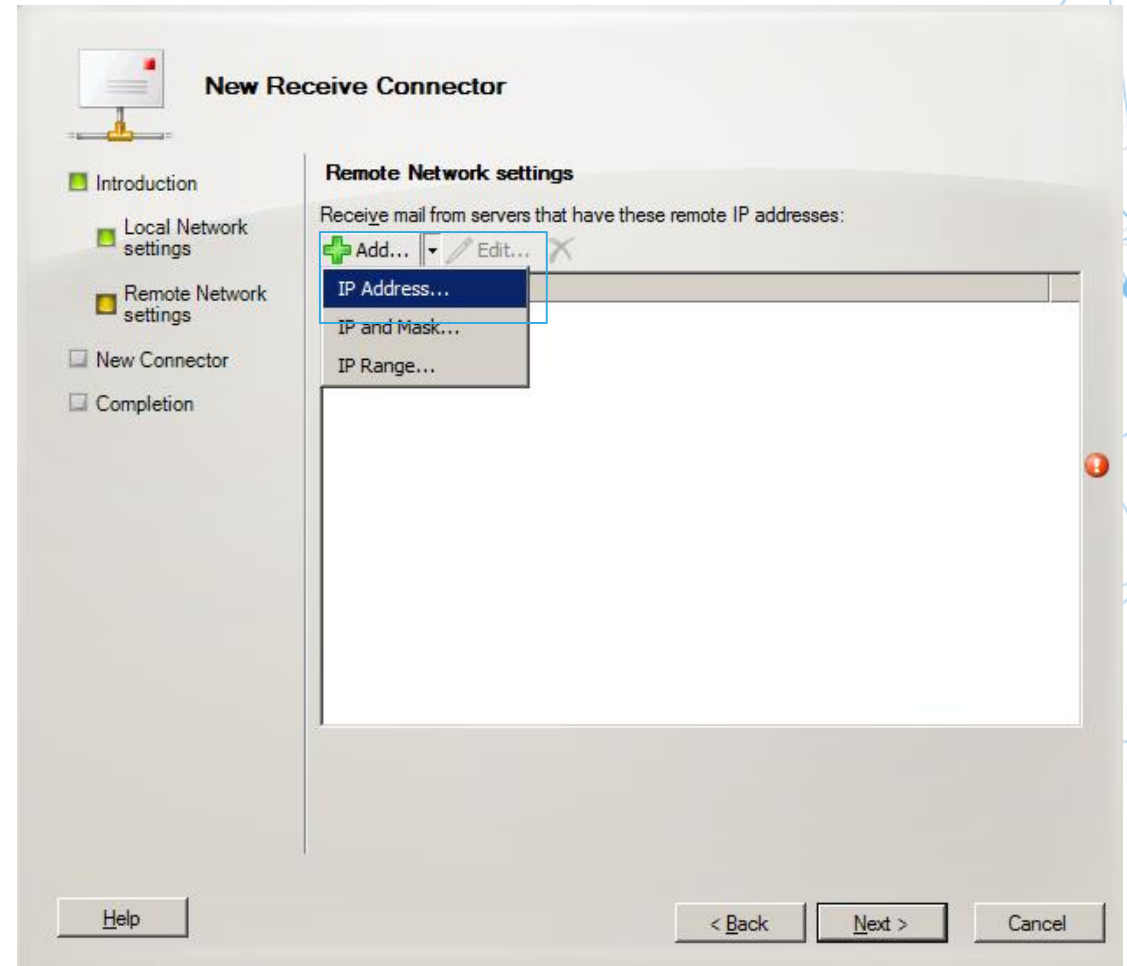
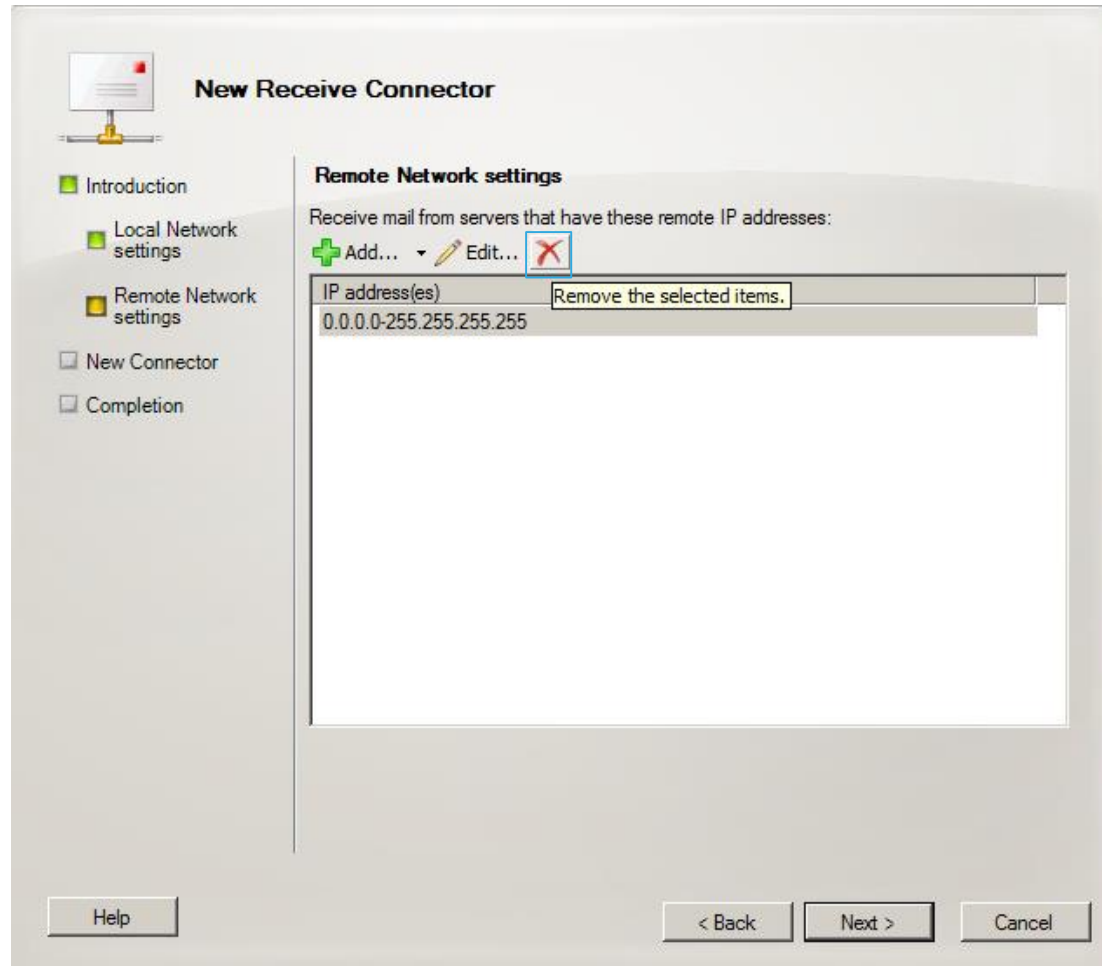
Example: 192.168.1.10

Port to Use

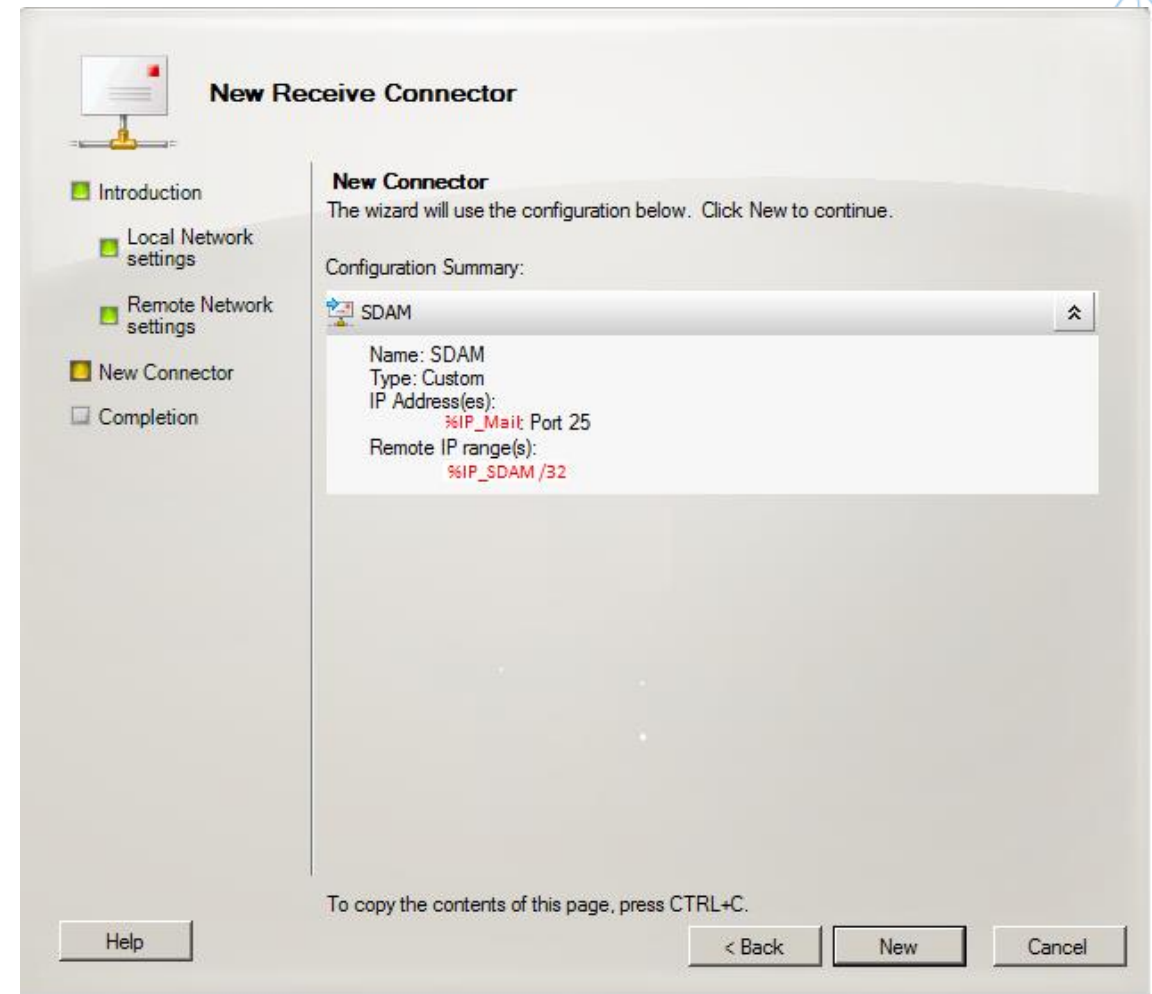
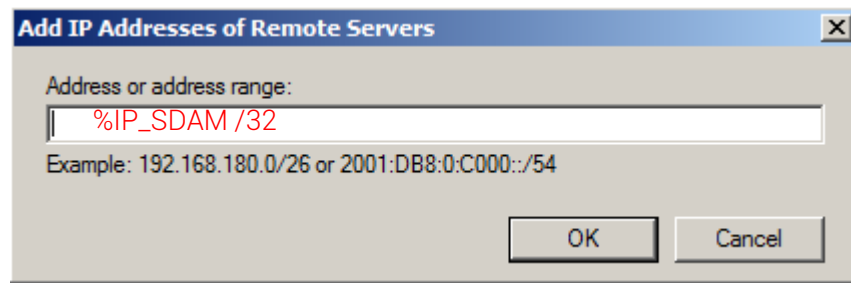
Port: 25

OK Cancel

Configuring Exchange Inbound Connector (continued)



Configuring Exchange Inbound Connector (continued)



Configuring Exchange Inbound Connector (continued)

The screenshot shows the Exchange Management Console (EMC) interface. The left pane displays the navigation tree with 'Hub Transport' selected. The main pane shows the 'Hub Transport' configuration for the '2K8R2' server. The 'Receive Connectors' tab is active, showing a table with two connectors: 'Default' (Disabled) and 'SDAM' (Enabled). The 'SDAM' connector is selected, and a context menu is open with the 'Properties' option highlighted. The right pane shows the 'Actions' for 'Hub Transport' and '2K8R2', including 'Export List...', 'View', 'Refresh', 'Help', 'Manage Mailbox Role', 'Manage Client Access Role', 'Manage Diagnostic Logging Properties...', 'New Receive Connector...', 'Properties', 'Disable', 'Remove', and 'Help'.

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

Name	Status
Default	Disabled
SDAM	Enabled

The screenshot shows the 'SDAM Properties' dialog box, 'Authentication' tab. The 'Specify which security mechanisms are available for incoming connections' section has the following options:

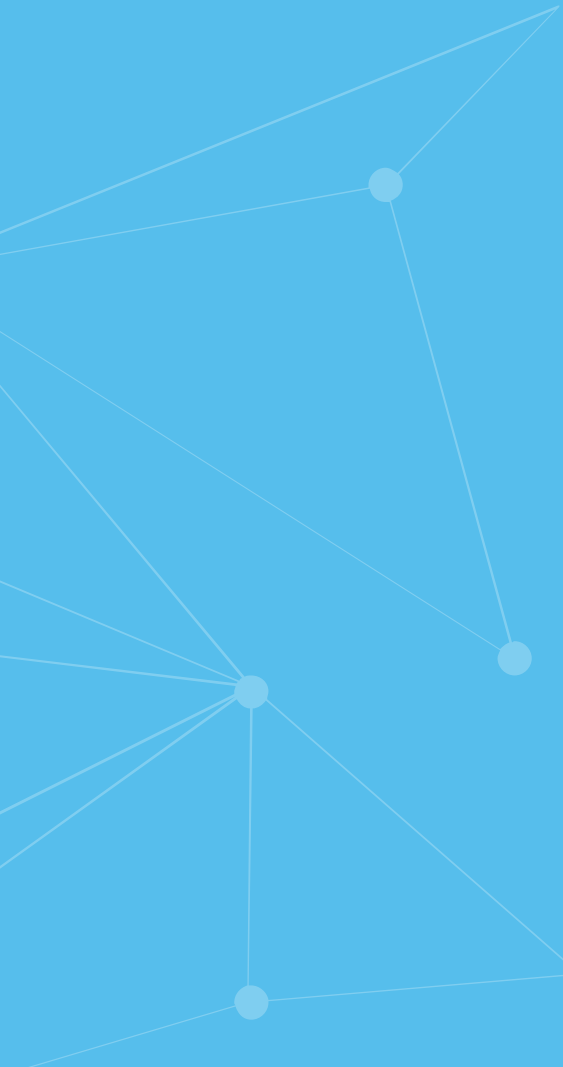
- ☐ Transport Layer Security (TLS)
 - ☐ Enable Domain Security (Mutual Auth TLS)
- ☒ Basic Authentication
 - ☐ Offer Basic authentication only after starting TLS
- ☒ Exchange Server authentication
- ☒ Integrated Windows authentication
- ☐ Externally Secured (for example, with IPsec)

Buttons: OK, Cancel

The screenshot shows the 'SDAM Properties' dialog box, 'Permission Groups' tab. The 'Specify who is allowed to connect to this Receive connector' section has the following options:

- ☒ Anonymous users
- ☒ Exchange users
- ☒ Exchange servers
- ☒ Legacy Exchange Servers
- ☐ Partners

Buttons: OK, Cancel, Apply, Help

An abstract geometric diagram on the left side of the slide. It consists of several light blue dots connected by thin, light blue lines. The dots are arranged in a way that suggests a network or a series of interconnected points. One dot is at the top left, another is below it, and a third is further down and to the right. There are also some lines that don't connect to dots, creating a sense of movement or a larger structure.

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

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

Recovery account

Policies signatory

The database contains 0 user of which 0 is 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

Special accounts

Special accounts (continued)

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
------------------	--

Special accounts (continued)

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

The screenshot displays the Stormshield Data Security Authority Manager interface. The top navigation bar includes the title 'Stormshield Data Security Authority Manager' and a user menu with 'RootCA', 'Main administrator', and 'Close session'. Below the navigation bar, a breadcrumb trail reads 'Home > Users management > Users'. The main content area is titled 'Users list' and shows a status message: 'The database contains 0 user of which 0 is special'. A search bar with a dropdown menu is visible, with 'Recovery account' selected. The dropdown menu also lists 'Policies signatory'. At the bottom, there is a 'Special accounts' button.

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

Recovery account
Policies signatory

The database contains 0 user of which 0 is 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

Special accounts

Special accounts (continued)

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 1p4yzUZtZhx

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



Certification mode	Internal CA - Encryption
Validity period	10 years Until Wednesday, February 23, 2028
Key role	☒ Encryption ☐ Signature
Key algorithm	RSA 2048 bits
Subject	CN=Recovery Account,S=Recovery,GN=Account,L=Milan,OU=StormshieldPOC,O=Stormshield

Publication



DN of LDAP entry	cn=Recovery Account,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	☒ Visible to every user to whom it is applied ☐ Modifiable by all the users to whom it is applied
Stormshield Data Security components on which it is applied	☒ All Stormshield Data Security components ☐ Security BOX SmartFILE ☐ Stormshield Data Virtual Disk ☐ Stormshield Data File ☐ Stormshield Data Mail ☐ Stormshield Data Team



Setting up SDS account configuration

User settings

Click on Main menu → Settings → Users Management

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=<OrgUnit>
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	☐ Binary format
Trust chain export	☐ Add trust chain when exporting certificates
Extension for exporting several certificates	☒ p7b extension ☐ p7c extension ☐ sbc extension

Email notifications



Information email	☐ Send an information email before the certificates expiration Number of days: 30 Frequency: 7 days Email address: Template: C:\SBMDData\rootca\MailTemplates\template_expiration_mail.sbp
-------------------	--

Click on Apply modifications

Option: LDAP settings

Click on Main menu → Settings → then select LDAP Synchronization

Settings



Database

General settings

LDAP Synchronization

Outgoing mail server

Certificate templates

Users

Users management

Components configuration

External certification authorities

Certification authority

Certificates management

Option: LDAP settings (continued)

LDAP synchronization settings

Server

Server name	%HOSTNAME_LDAP
Port number	389
LDAP version	2
Protocol	☐ SSL
Encoding	☐ UTF-8 ☒ ANSI
Duration of a connection attempt	30 seconds

Authentication

Authentication selection	☒ Authentication with a plaintext password	
	DN:	cn=Administrator,CN=users,DC=stotrmshiedl,dc=corp
	Password:	*****
	☐ Negotiated authentication	
	Domain or workgroup name:	
User name:		
Password:		

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

Search

Base DN	CN=users,DC=stotrmshiedl,dc=corp
Class of recognition for "person" type entry	person
Search time limit	30 seconds

Publication

Keys to be published	☐ All keys ☒ The key with the encryption role and the key with the signature role
----------------------	---

Publication of new certificates

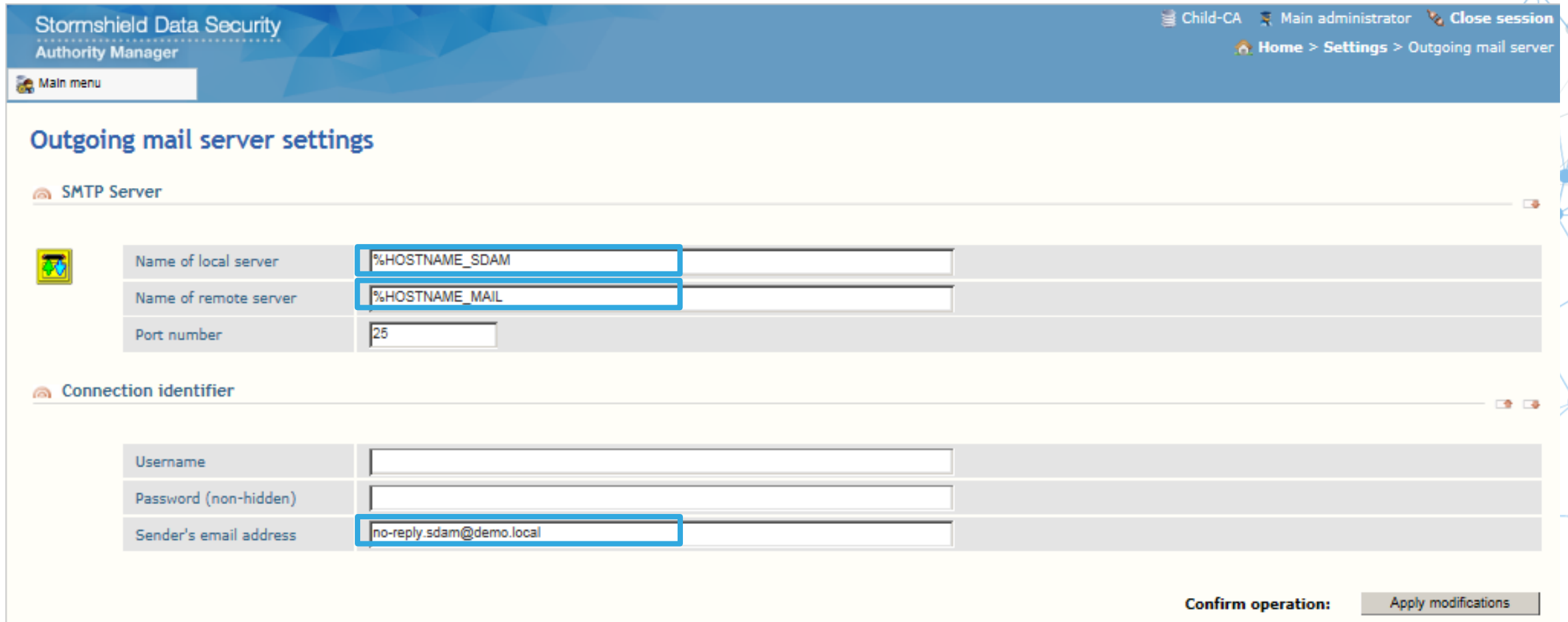
DN resolution mask	cn=<CommonName>,ou=<OrgUnit>,o=<Organization>
--------------------	---

Name of attributes

Email address	mail
Common name	cn
Certificate in binary format	userCertificate;binary
Identifier	uid <i>Or sAMAccountName if you are connected to Microsoft Active Directory</i>
Given name	givenName
Name	sn
Authority certificate in binary format	caCertificate;binary
CRL in binary format	certificateRevocationList;binary
Security policies update in binary format	sboxPolicyUpgrade;binary

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

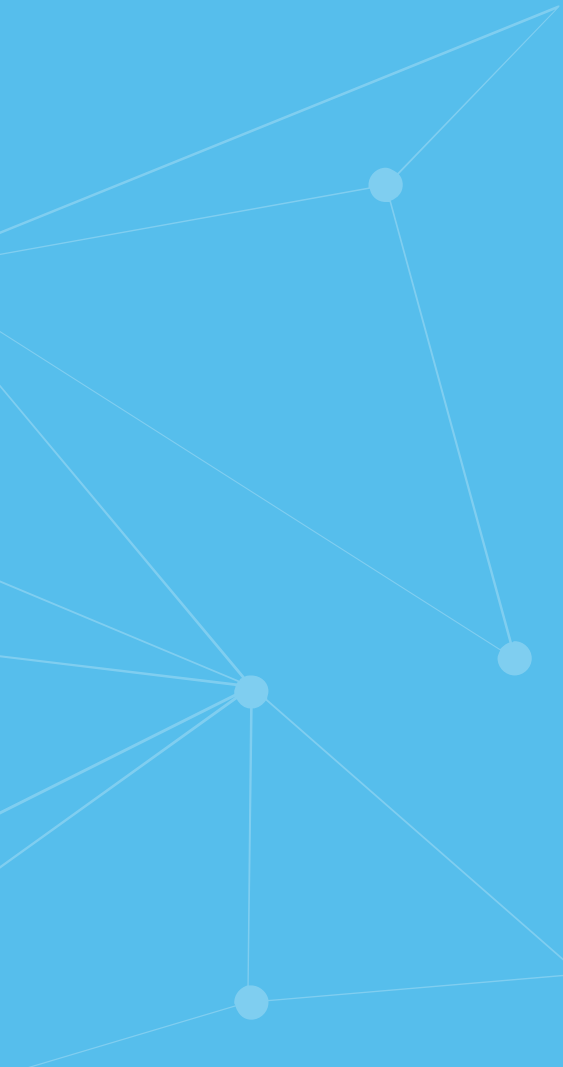


The screenshot shows the Stormshield Data Security Authority Manager interface. The top navigation bar includes the logo, user information (Child-CA, Main administrator), and a Close session button. A breadcrumb trail shows Home > Settings > Outgoing mail server. The main content area is titled 'Outgoing mail server settings' and contains two sections: 'SMTP Server' and 'Connection identifier'. The 'SMTP Server' section has three input fields: 'Name of local server' (containing %HOSTNAME_SDAM), 'Name of remote server' (containing %HOSTNAME_MAIL), and 'Port number' (containing 25). The 'Connection identifier' section has three input fields: 'Username' (empty), 'Password (non-hidden)' (empty), and 'Sender's email address' (containing no-reply.sdam@demo.local). A 'Confirm operation:' button labeled 'Apply modifications' is at the bottom right.

SMTP Server	
Name of local server	%HOSTNAME_SDAM
Name of remote server	%HOSTNAME_MAIL
Port number	25

Connection identifier	
Username	
Password (non-hidden)	
Sender's email address	no-reply.sdam@demo.local

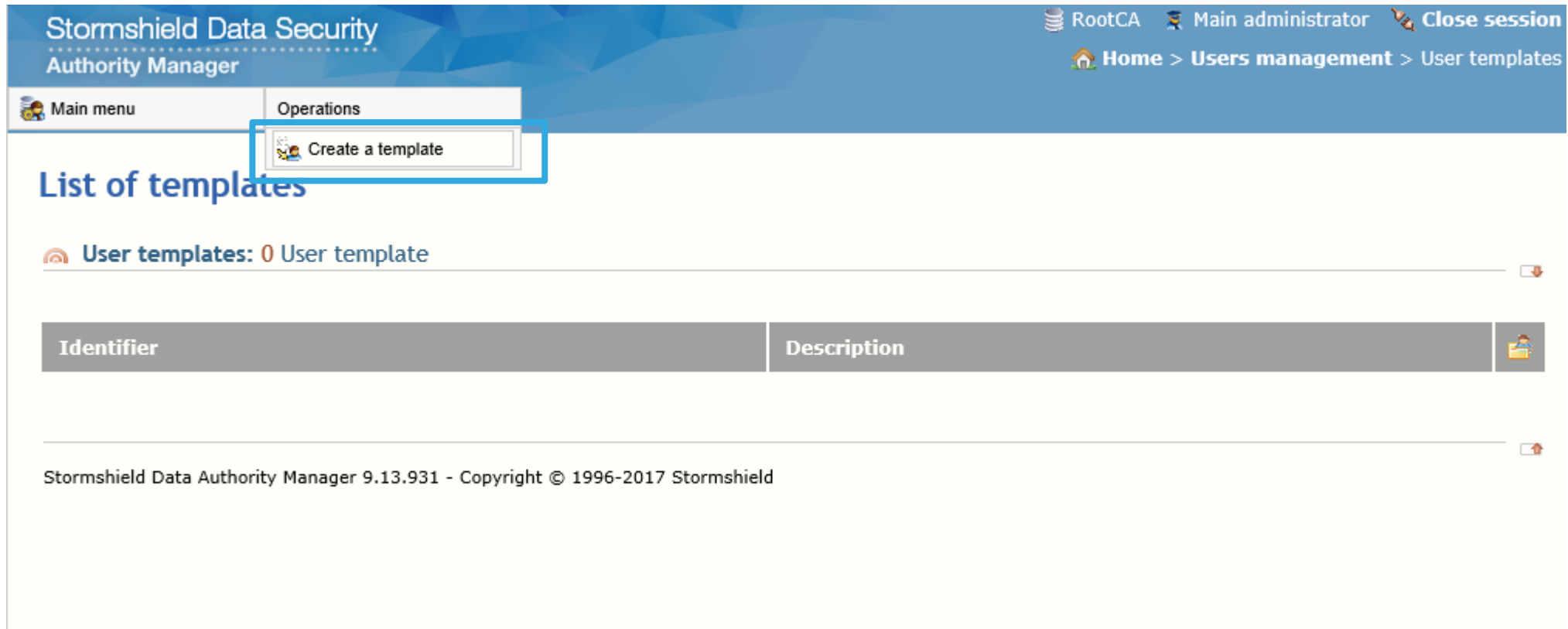
Confirm operation: Apply modifications



Creating SDS account templates

Creating a template

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



Stormshield Data Security
Authority Manager

RootCA Main administrator Close session
Home > Users management > User templates

Main menu Operations

Create a template

List of templates

User templates: 0 User template

Identifier	Description
------------	-------------

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

Creating a template (continued)

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	☒ Encryption ☐ Signature
Key algorithm	RSA 2048 bits

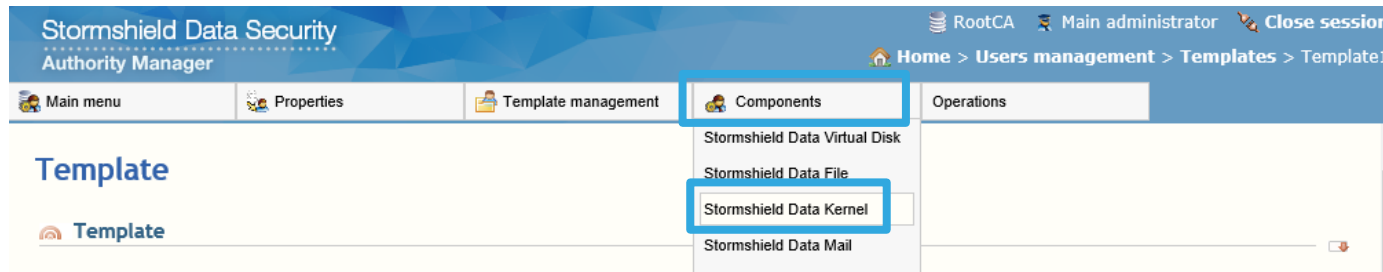
Key 2

Certification mode	Internal CA - Signature
Validity period	2 years Until Sunday, February 23, 2020
Key role	☐ Encryption ☒ Signature
Key algorithm	RSA 2048 bits

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**

Stormshield Data Kernel - Connection and personal code - Password mode

Icon

Icon in configuration panel	☒ Not visible
-----------------------------	---

Tabs

Screensaver tab	☒ Not visible
Connection tab	☒ Not visible
Authentication tab	☒ Not visible

On Windows screensaver turn on

☐ No action	☒ Cannot be modified by the user
☒ Lock session	
☐ And unlock on waking up	
☐ Disconnect	
Screen saver...	☒ Not visible

On Windows session locking

☐ No action	☒ Cannot be modified by the user
☒ Lock session	
☐ And unlock on waking up	

Ask for secret code

☒ At connection only	☒ Cannot be modified by the user
☐ On each signature or decryption operation	☒ Cannot be modified by the user
☐ Every 15 minute(s)	☐ Not visible
Change your secret code...	

Change secret code

☐ Request change every 10 day(s)	☒ Cannot be modified by the user
☒ Impose change every 30 day(s)	☒ Cannot be modified by the user
☒ Inhibit change before 1 day(s)	☒ Cannot be modified by the user

Personal code syntax

Number of alphabetical characters minimum: 1 maximum: 32	☒ Impose secret code change at first connection
Number of numerical characters minimum: 1 maximum: 32	
Number of other characters minimum: 1 maximum: 32	
Total number of characters minimum: 8 maximum: 32	
Help text for the user Your password must contain between 8 and 32 characters.	

Log on to Windows

☒ Do not activate	☒ Cannot be modified by the user
☐ Using the following information: (User, Log on to, Password, Confirmation)	

Confirm operation: Apply modifications

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`

Stormshield Data Security
Authority Manager
Main menu

Home > Users management > Templates > Template1 > Stormshield Data Kernel > Automatic update

Stormshield Data Kernel - Automatic update

Automatic update

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) ☐ Cannot be modified by the user
- ☒ HTTP secured by SSL ☐ Cannot be modified by the user
- ☒ LDAP (directory access) ☐ Cannot be modified by the user
- ☒ LDAP secured by SSL ☐ Cannot be modified by the user
- ☒ FILE (file copy) ☐ Cannot be modified by the user

Download

☒ The user is not allowed to add distribution points

☒ Cannot be modified ☒ Cannot be deleted

Confirm operation:

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**.

Stormshield Data Security
Authority Manager

RootCA Main administrator Close session

Home > Users management > Templates > Template1

Main menu

Properties

Template management

Components

Operations

Template

Template

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

User identity

Stormshield Data Virtual Disk

Stormshield Data File

Stormshield Data Kernel

Stormshield Data Mail

Stormshield Data Team

Stormshield Data Shredder

Stormshield Data Sign

Import from master

CRL configuration (continued)

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

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

Main menu

Stormshield Data Kernel - Revocation controller

General settings

	☐ Not visible
☐ Do not control the revocation state	☒ Cannot be modified by the user
CRLs default validity period (days) 7	☐ Cannot be modified by the user
Protocols: Activate revocation lists downloads with the following protocols:	
☒ HTTP (web)	☒ Cannot be modified by the user
☒ HTTP secured by SSL	☒ Cannot be modified by the user
☒ LDAP (directory access)	☒ Cannot be modified by the user
☒ LDAP secured by SSL	☒ Cannot be modified by the user
☒ FILE (file copy)	☒ Cannot be modified by the user

Issuers

 RootCA	☒ Prohibit adding issuers
Delete	☐ Prohibit deleting this issuer from the list
Add database authority: Add	
Add an external issuer: Add	
☐ Do not control the revocation state	☐ Cannot be modified by the user
Validity length (days) 7	

CRL configuration (continued)

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

Revocation lists downloading rule:



Download at the first encryption operation (recommended) ▼

Custom distribution points:

Enter in order of priority

http://%IP_SDAM:port/rootcrl/rootca.crl



☐ 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

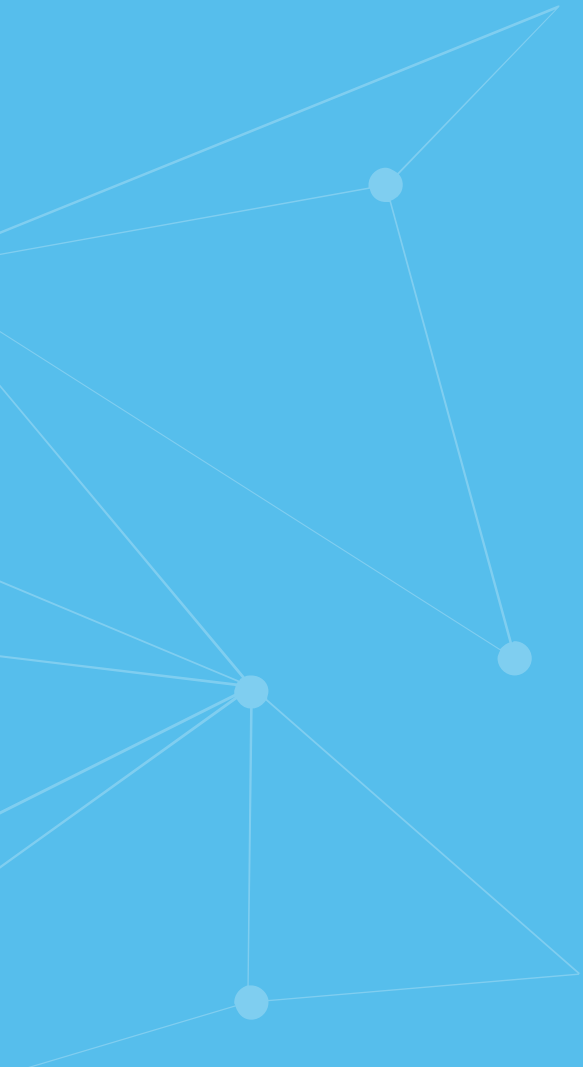
☐ Cannot be deleted

☐ Cannot be modified

☐ Cannot be deleted

Confirm operation:

Apply modifications

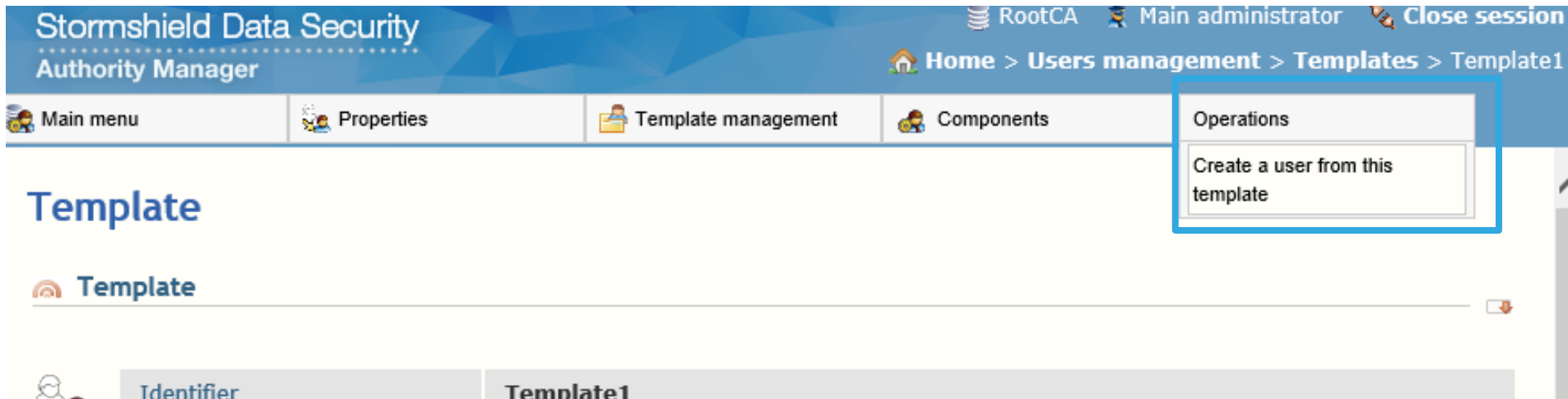


Creating SDS user accounts

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**

The screenshot displays the Stormshield Data Security Authority Manager web interface. The top navigation bar includes the product name, user information (RootCA, Main administrator), and a session close button. A breadcrumb trail shows the path: Home > Users management > Users. Below this, a horizontal menu contains several options: Main menu, Special users, Users creation, Users management, Certificates management, and LDAP. The LDAP option is highlighted, and a sub-menu is visible with the option LDAP Synchronization. The main content area is titled 'Users list' and shows a status message: 'The database contains 0 user of which 0 is special'. Below the message is a search bar with a dropdown menu containing letters A through Z, and a 'Search criteria' input field.

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

LDAP Synchronization

Users list

The database contains 0 user of which 0 is 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

Creating users via LDAP (continued)

Click on To associate or use to create users

Stormshield Data Security
Authority Manager

RootCA Main administrator %HOSTNAME_LDAP:389 Close session

Home > Users management > Users > LDAP Synchronization

Main menu

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

Main menu

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=stotrmshiedl,dc=corp

Filter

(Objectclass=person)

Depth

Searching:

☒ entire tree under the base

☐ one level under the base

☐ base only

Confirm operation:

Search

Caution, this operation may take several minutes.

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.

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

☒ Publish generated certificate in the LDAP directory

 Certificates already published on the LDAP server

☐ Keep
☐ Delete
☒ Replace certificates that have the same usages and the same issuer

User account configuration

 Use as template

Template1

Validation

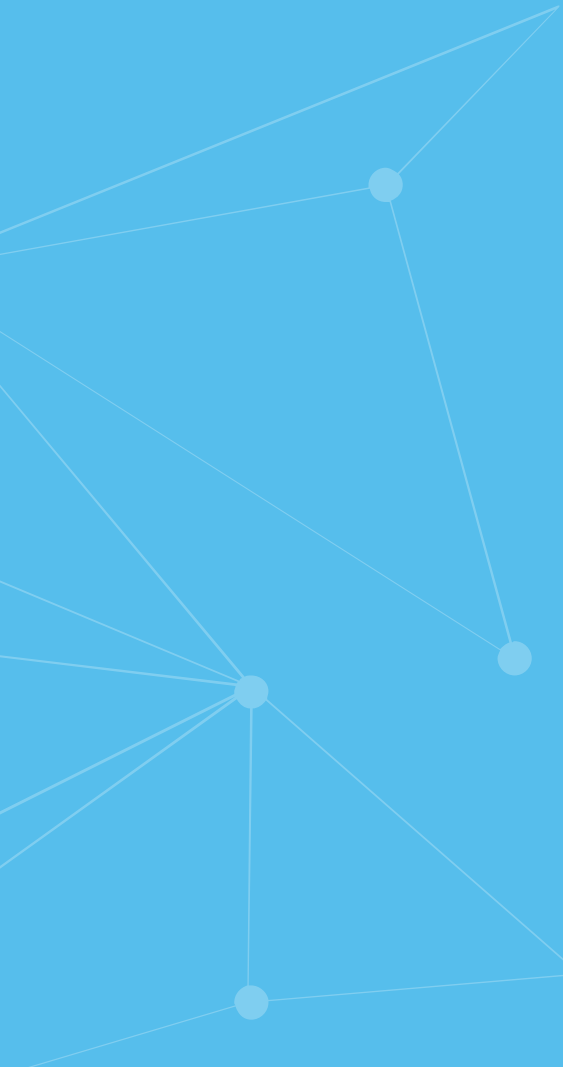
 The following operations will be performed:

- 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



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**

The screenshot shows the 'Users list' page in the Stormshield Data Security Authority Manager. The top navigation bar includes 'Main menu', 'Special users', 'Users creation', 'Users management', and 'Certificates management'. The breadcrumb trail is 'Home > Users management > Users'. A status message indicates 'The database contains 3 users of which 2 are special'. Below this is a table with columns A through Z for search criteria. The table shows 3 selected users: 'Policy Signatory', 'Recovery Account', and 'test1'. The 'test1' user is highlighted with a blue box, showing the email 'test1@stormshield.com'. The footer text reads 'Stormshield Data Authority Manager 9.13.931 - Copyright © 1996-2017 Stormshield'.

Search criteria	
Users 1 - 3 of 3 found	3 selected users
Policy Signatory	☒
Recovery Account	☒
test1	☒

The screenshot shows the 'User management' page for the user 'test1'. The top navigation bar includes 'Main menu', 'Properties', 'User management', and 'Keys and certificates'. The breadcrumb trail is 'Home > Users management > Users > test1'. The 'User management' tab is active, and the 'Distribute account' option is highlighted with a blue box. Below this, the user's details are displayed in a table:

Identifier	test1
Template	Template1

Below the user details is the 'Identity' section, which displays a table of user attributes:

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

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)

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):

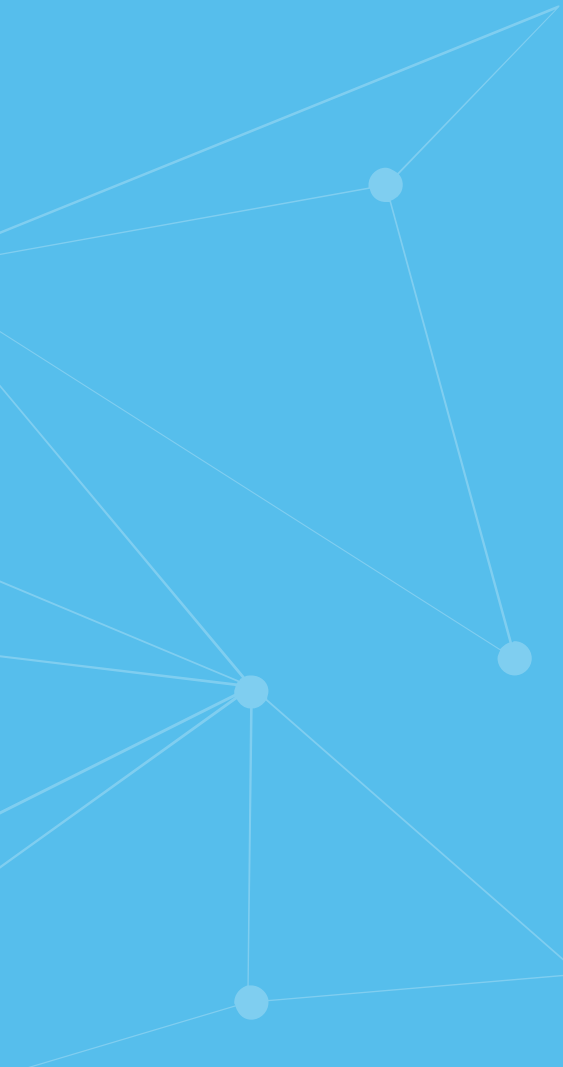
Subject:

Text:

Confirm operation:

Distribute account

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

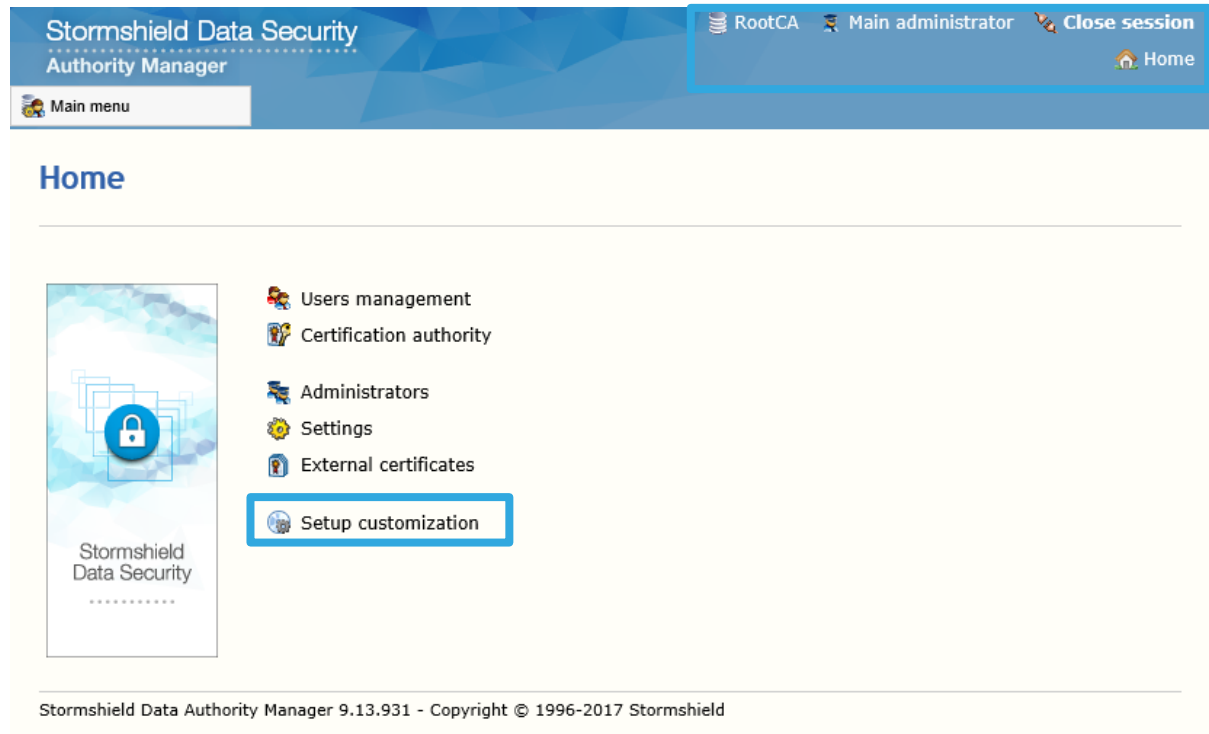


Installing the client workstation

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

Stormshield Data Security
Authority Manager

RootCAMain administratorClose session
Home > Setup customization > General settings

Main menu

Stormshield Data Security Suite: General settings

User connection

	Authorize a connection ☒ In password mode ☐ In card mode
Shutting down Windows	☐ 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: ...
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: ...
Backup folder	In the Stormshield Data Security connection window: ☐ Do not display the pathname of the second users accounts search folder 
Contextual menu	☐ 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: ☐ Do not display the "Browse" item
Command line utility	In the SBCMD.EXE command line utility: ☐ Ignore a secret code supplied on the command line. User must enter his/her secret code.

Configuring the setup (continued)

Check the option
Prohibit account creation

Stormshield Data Security
Authority Manager

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

Main menu

Account creation

	New accounts	☒ Prohibit account creation
	Self-certified certificates	Validity length of self-certified certificates generated by Stormshield Data Security: - when creating an account: years - when renewing a key: 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>]]

Address book

	LDAP search	In an LDAP search launched from the address book: ☐ Do not append '*' to the search criteria ☐ Do not include the search filter "usercertificate;binary"
---	-------------	---

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**

Revocation controller

CRL download

Maximum time limit for a CRL download in LDAP:

120 seconds

Maximum time limit for a CRL download via HTTP:

120 secondes

Miscellaneous

License key

In the "About" window:

☒ Do not show license key

Adding settings to the SBox.ini file

File containing the settings to add or merge

Select a file:

Browse...

⚠

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".

Confirm operation:

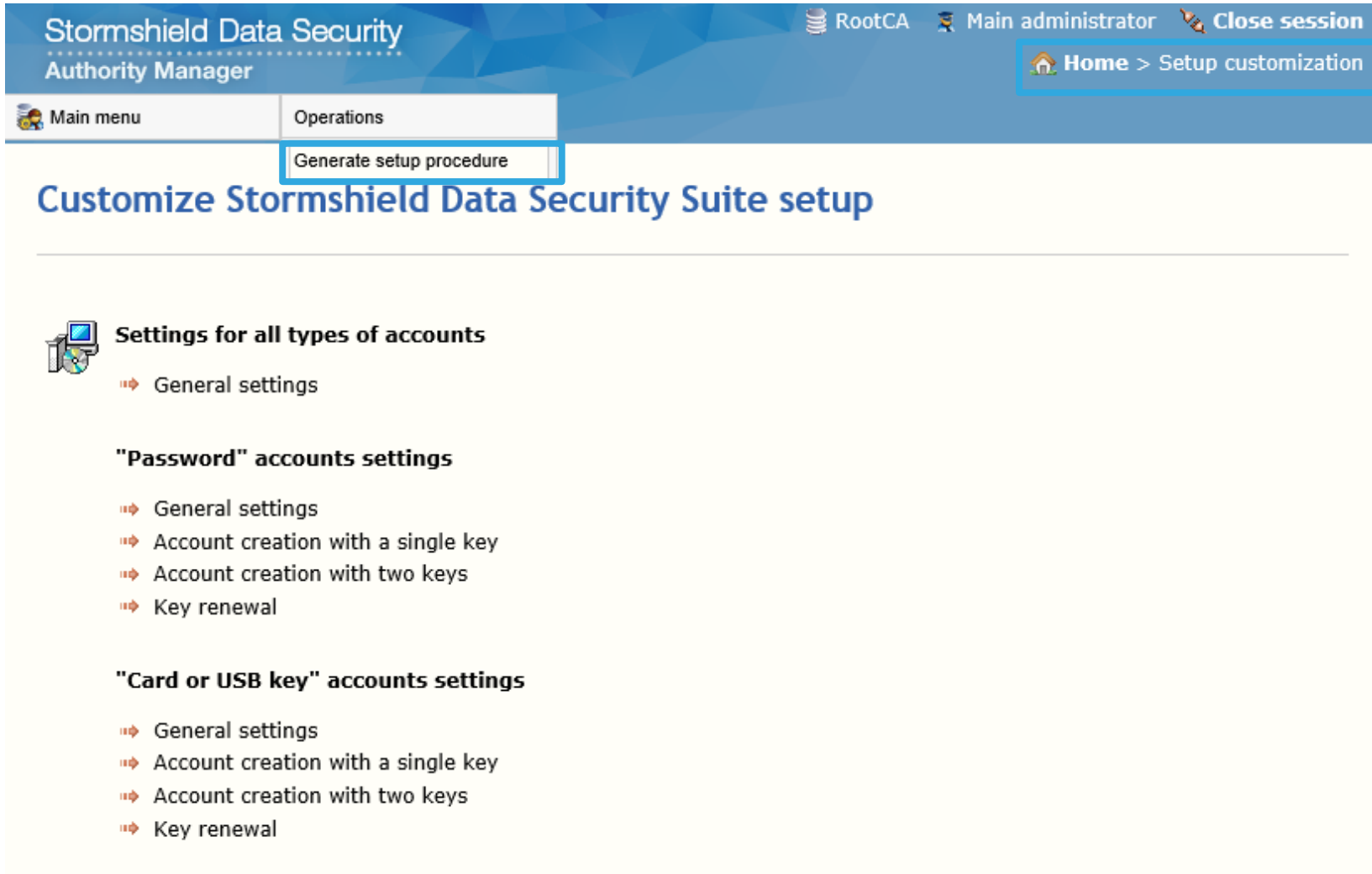
Apply modifications

STORMSHIELD

131

Generating the installation file

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



The screenshot displays the Stormshield Data Security Authority Manager web interface. The top navigation bar includes the title 'Stormshield Data Security Authority Manager', user information 'RootCA Main administrator', and a 'Close session' button. A breadcrumb trail shows 'Home > Setup customization'. The left sidebar contains a 'Main menu' and an 'Operations' menu where 'Generate setup procedure' is highlighted. The main content area is titled 'Customize Stormshield Data Security Suite setup' and lists configuration options for different account types: 'Settings for all types of accounts', 'Password accounts settings', and 'Card or USB key accounts settings'. Each category has a list of sub-options with expandable icons.

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

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)

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 - EFGDFGF

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:

Generating setup procedure

The customized setup procedure of Stormshield Data Security Suite will be generated in the folder C:\SBMData\rootca\MSITarget.

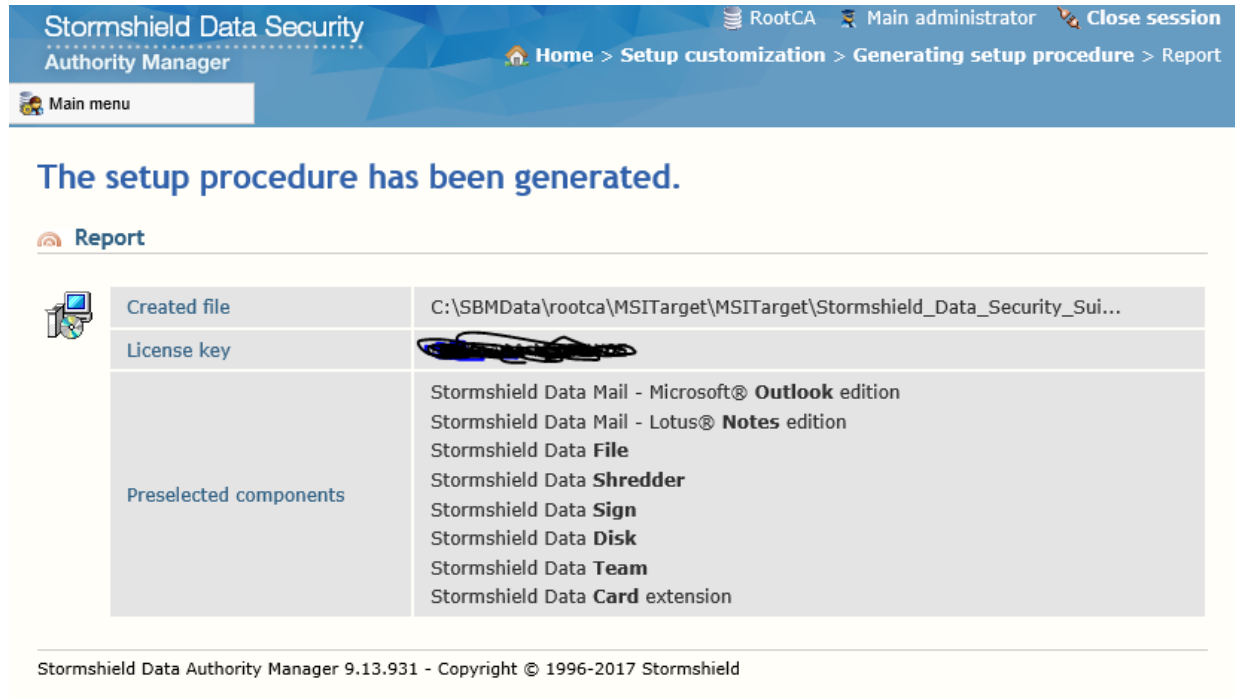
Caution, this operation may take several minutes.

Confirm operation:

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



Stormshield Data Security Authority Manager

RootCA Main administrator Close session

Home > Setup customization > Generating setup procedure > Report

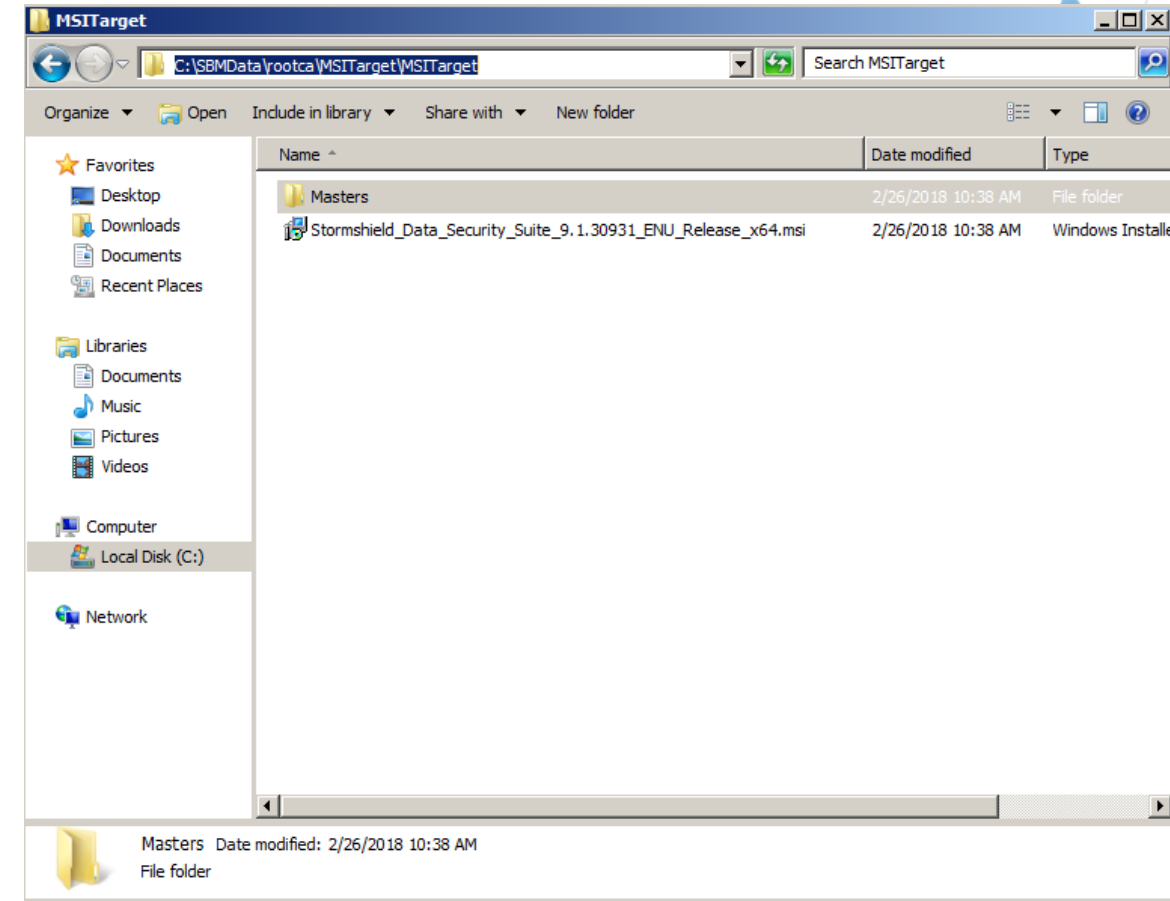
Main menu

The setup procedure has been generated.

Report

Created file	C:\SBMData\rootca\MSITarget\MSITarget\Stormshield_Data_Security_Sui...
License key	[redacted]
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



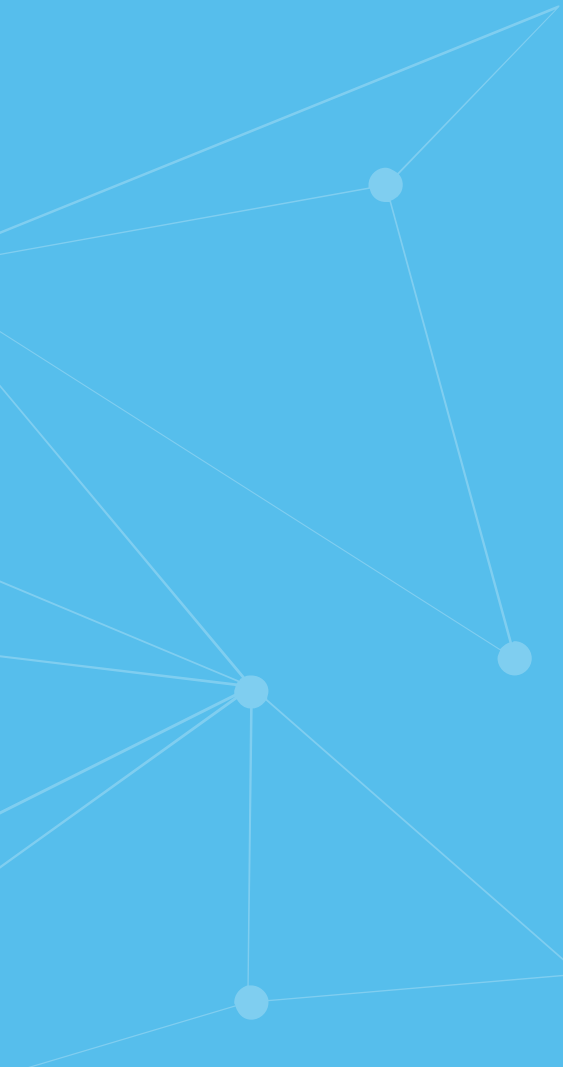
You can rename the customized setup file if you wish to, for example Custom_SDS_file.msi

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+

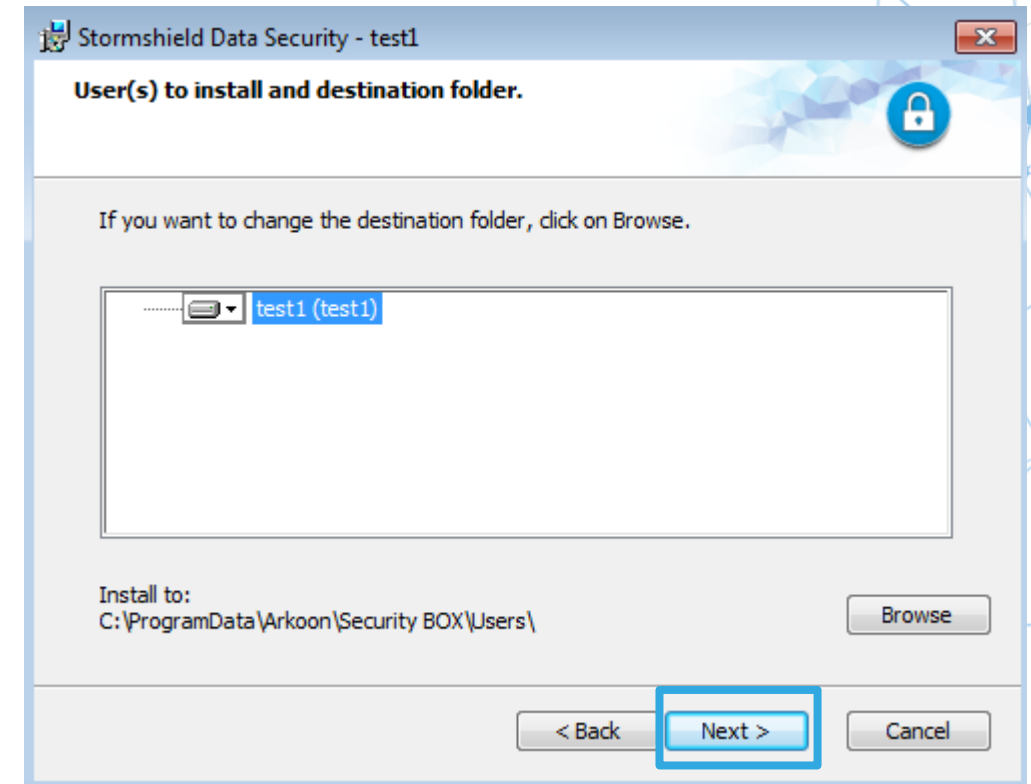
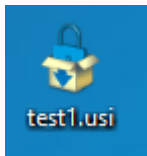




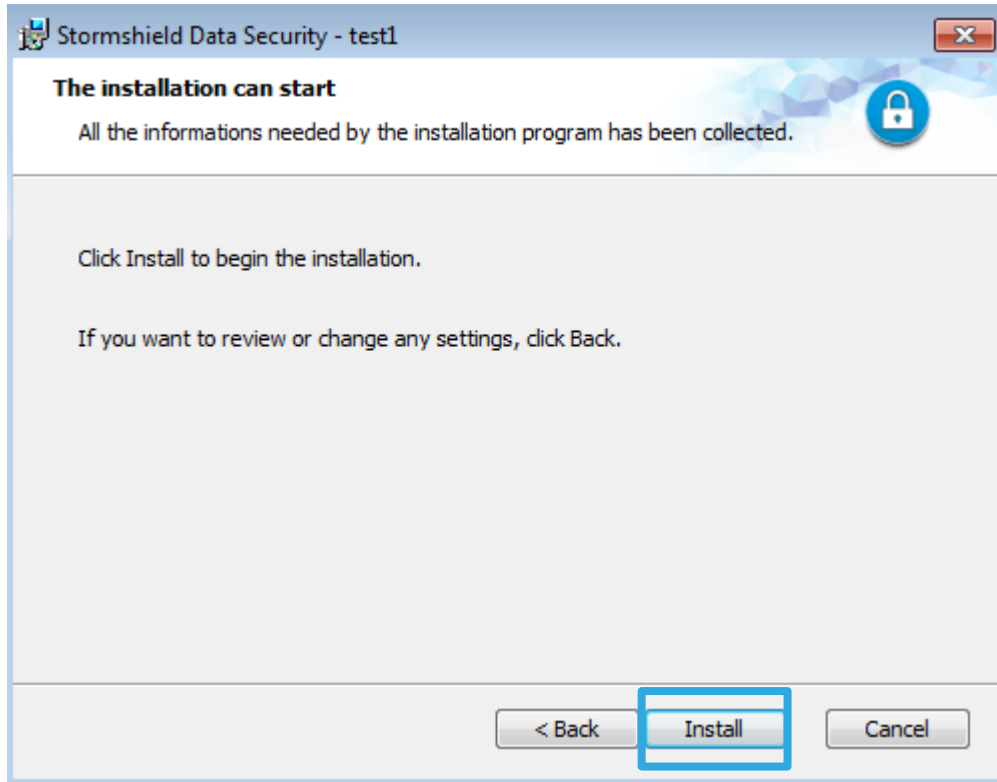
Installing the SDS account

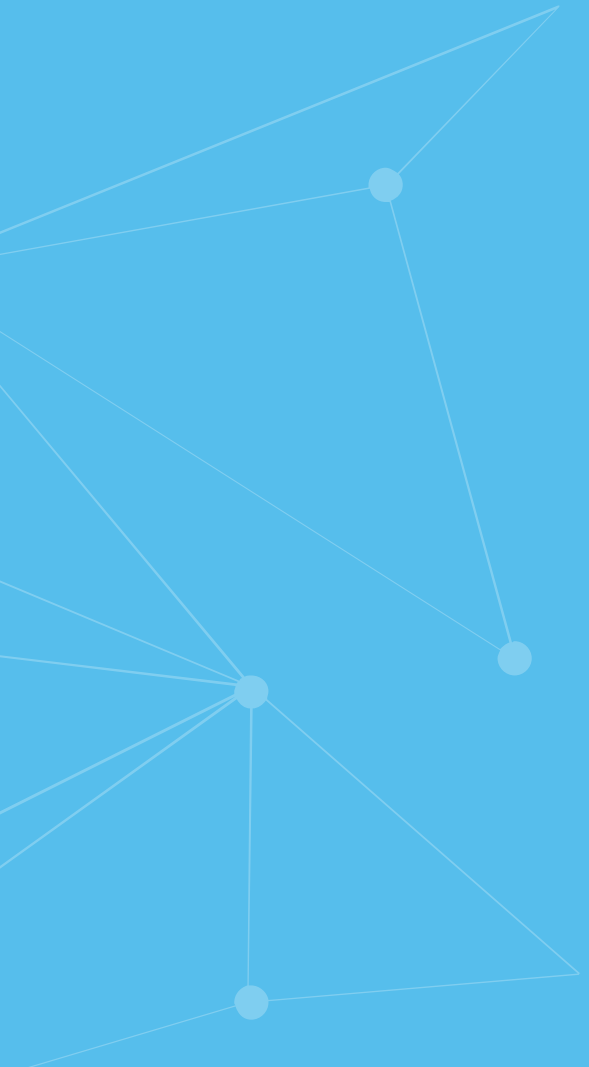
Installing the SDS account

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



Installing the SDS account (continued)





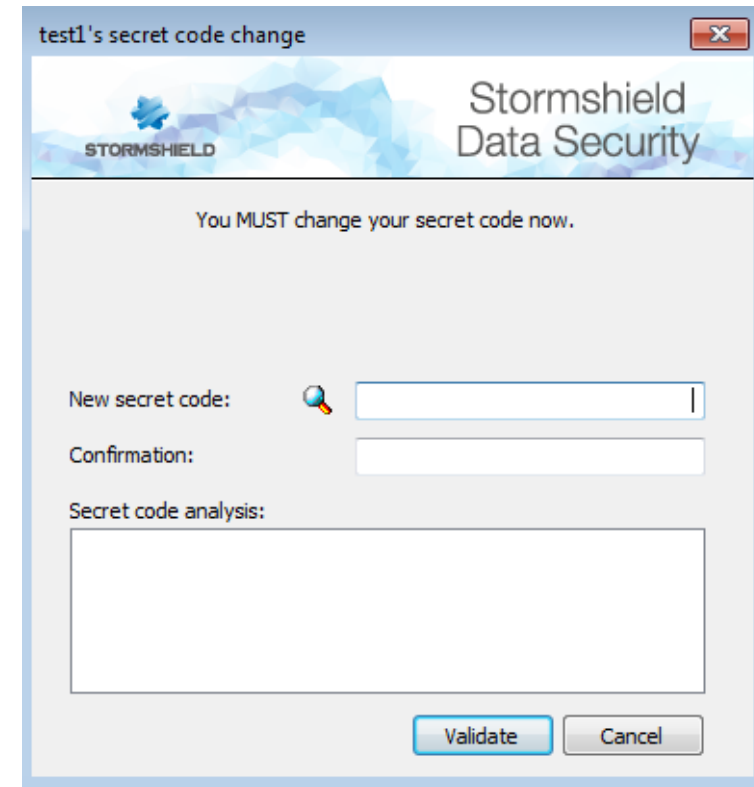
Initial connection

Initial connection

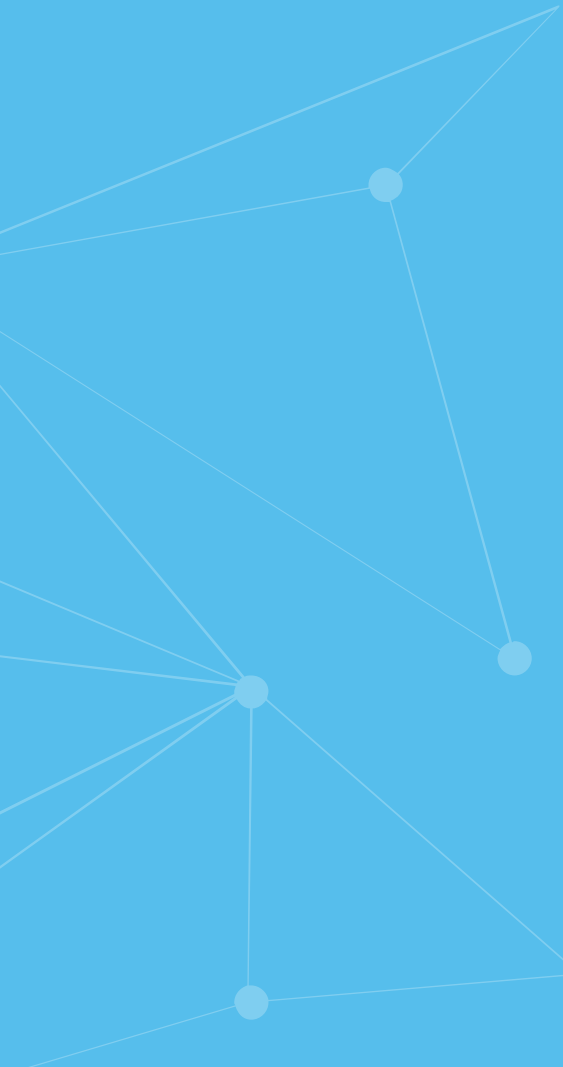
The user icon displayed on the left indicates that the account exists on the workstation. Enter the user's initial password. After the initial connection, the user will be asked to change his initial password.



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

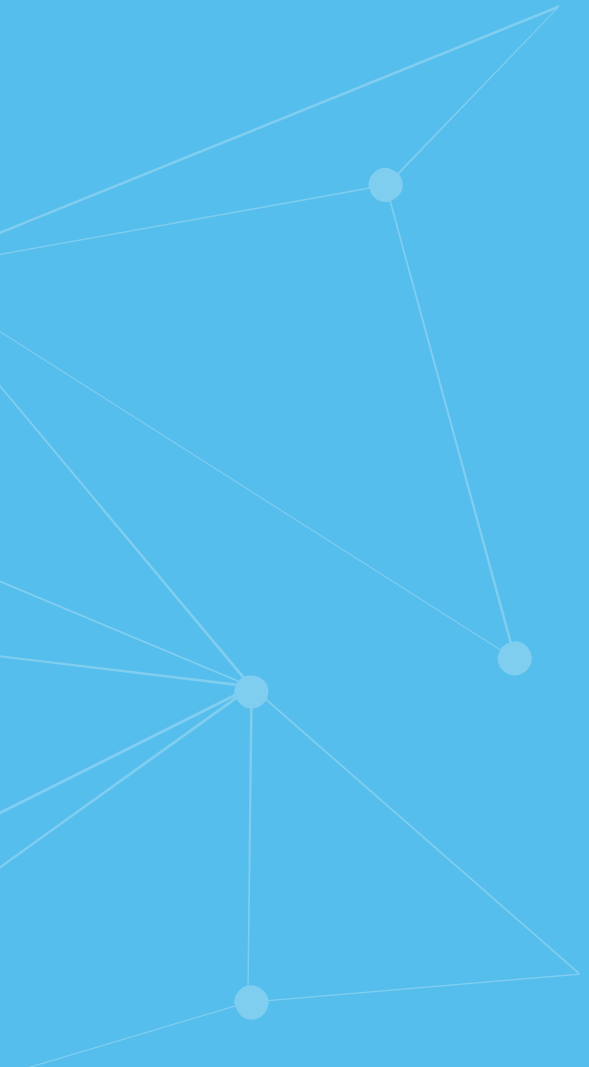
- Manually creating a disk volume on the computer %HOSTNAME_CLIENT1 with an automatic mount
- %USERNAME_CLIENT1 manually creating a disk volume on a USB drive shared with %USERNAME_CLIENT2 with manual editing

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

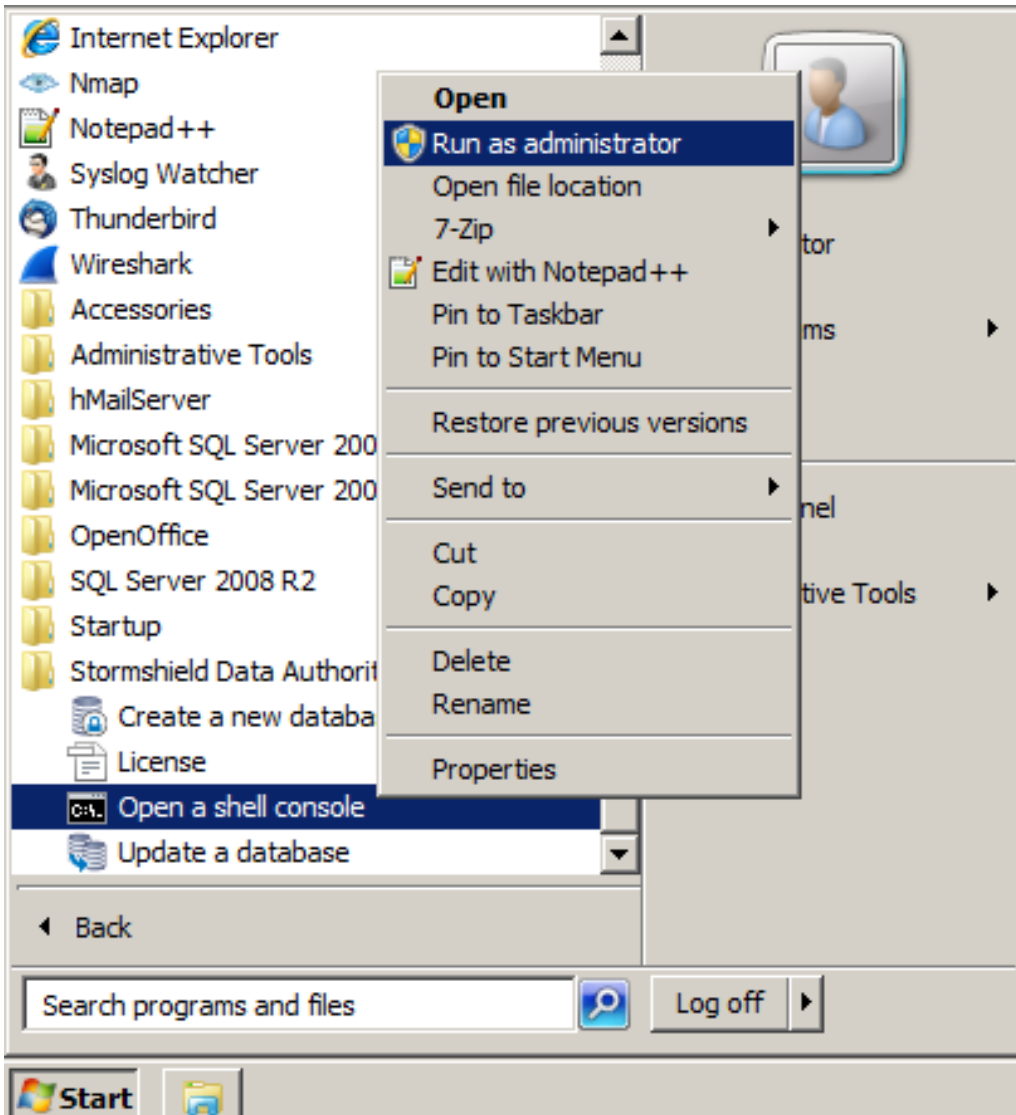
Contacts

- 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