TECHNICAL NOTE

STORMSHIELD MULTI-LAYER COLLABORATIVE SECURITY

SDS EASY: EMBEDDING A SNS PKI IN A SDS CLIENT

Product concerned: SNS 2.4 and higher - SDS Suite v9.1.1 and higher

Date: July 2016

Reference: mlcs-en_SDS_Easy_Embedding_SNS_PKI_in_SDS_technical_note

Table of contents

Introduction

The aim of this document is to describe the setup of a PKI (Public Key Infrastructure) hosted on a Stormshield Network firewall for workstations that use the Stormshield Data Security Suite solution.

SNS firewalls do indeed build in functions that allow managing certificate authorities (CAs), associated CRLs, (Certificate Revocation Lists), CRLDPs (CRL Distribution Points) as well as user certificates.

Managing the PKI on the firewall therefore makes it possible for the organization to do without the creation of one or several servers dedicated to these functions and the potential implementation of an external LDAP directory or Microsoft Active Directory infrastructure.

Requirements

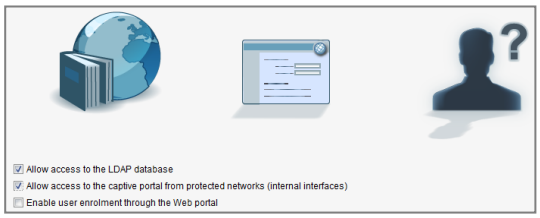
- Workstation: SDS Suite in v9.1.1 or higher,
- SNS firewall in version 1.1 or higher (the automatic verification of CRLs from SDS Suite only operates from v2.4 of SNS upwards).

Configuring the SNS firewall

Creating an internal LDAP directory

If your firewall already has an internal LDAP directory, skip straight to the paragraph Enable the captive portal.

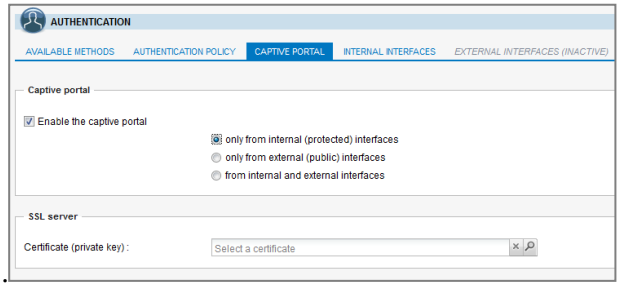
1. In the menu **Configuration** > **Directory configuration**, click on **Create an internal LDAP directory** then click on **Next.**
2. Enter the following mandatory fields:
   - **Organization**: name of your company (e.g.: MyCompany),
   - **Domain**: your company's DNS domain (e.g.: mycompany.org),
   - **Password**: password that allows the firewall to log on to the directory or to log on from an LDAP browser.
3. Validate by clicking on **Next**.
4. Select the 2 checkboxes:
   - **Allow access to the LDAP database**: this will allow - with an appropriate filter rule - LDAP requests from user workstations equipped with SDS Suite,
   - **Allow access to the captive portal from protected networks (internal interfaces)**: this option makes the authentication portal accessible from the internal network. CRL verification requests to the firewall will therefore be allowed.



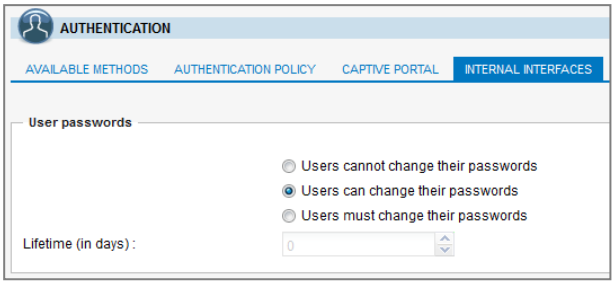
Enabling the captive portal

If you have created your internal directory following the procedure described in the chapter Create the internal directory, the captive portal will already have been enabled. In this case, you can skip directly to the paragraph Create the CA for user certificates.

1. In the *Captive portal* tab of the **Users** > **Authentication** menu, check **Enable the captive portal** and select **Only from internal (protected) interfaces**



2. In the **User passwords** panel of the *Internal interfaces* tab, select the option **Users can change their passwords** to allow users to modify their passwords from the captive portal.

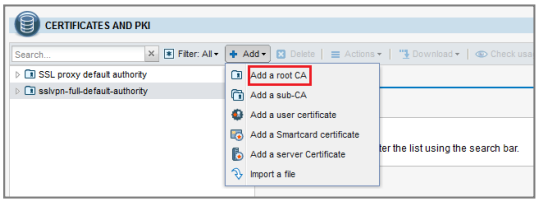


3. Confirm by clicking on **Apply**.The captive portal can now be accessed at the address *https://firewall_ip_address/auth/*.

NOTE
In the method that Stormshield recommends, the captive portal is useful only for making the CRL accessible to SDS Suite clients. In the alternative method, it is necessary for user enrollment.

Creating the CA for user certificates

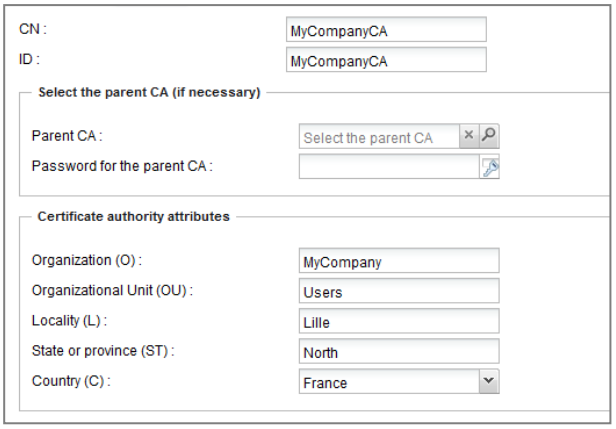
1. In the menu **Objects** > **Certificates and PKI**, click on **Add** and select **Add a root CA**.



2. Fill in the fields in the wizard:

Step 1:

- **CN**: enter a name that allows you to identify your certificate authority,
- **ID**: the name entered in the CN field is suggested by default,
- **Organization (O)**. Example: the name of your company,
- **Organizational Unit (OU)**. Example: the name of the CA user's department,
- **Locality (L)**: city in which your organization is located,
- **State or province (ST)**: state or province in which your organization is located,
- **Country (C)**: country in which your organization is located.

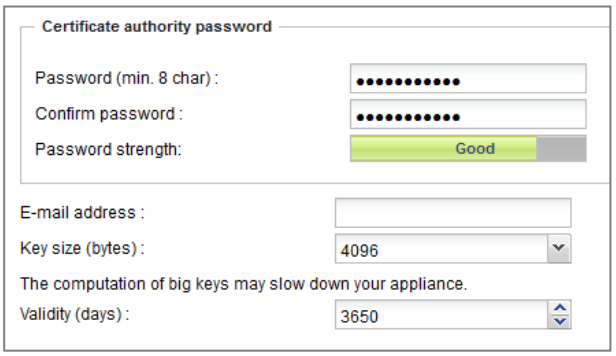


Step 2 :

- **Password**: enter a password of at least 8 characters in order to protect access to your CA's private key. You will be asked for this password every time you create or modify a user certificate,

  WARNING
  The firewall will not save this password. If you forget your password, the CA can no longer be used to sign certificates.

- **Key size**: (4096 bits by default),
- **Validity** (3650 days by default).



Step 3 :

Indicate the URI of the CRLDP (CRL distribution point). This URI will be found in each certificate signed by the CA.

Since the CRL will be hosted on the firewall, it will be in the following form:

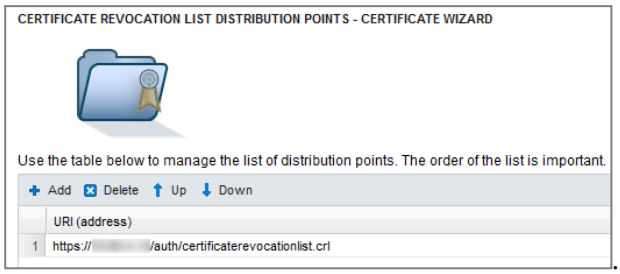
- **https://***firewall_ip_address*/**auth**/*certificaterevocationlist.crl*

or

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

REMARK

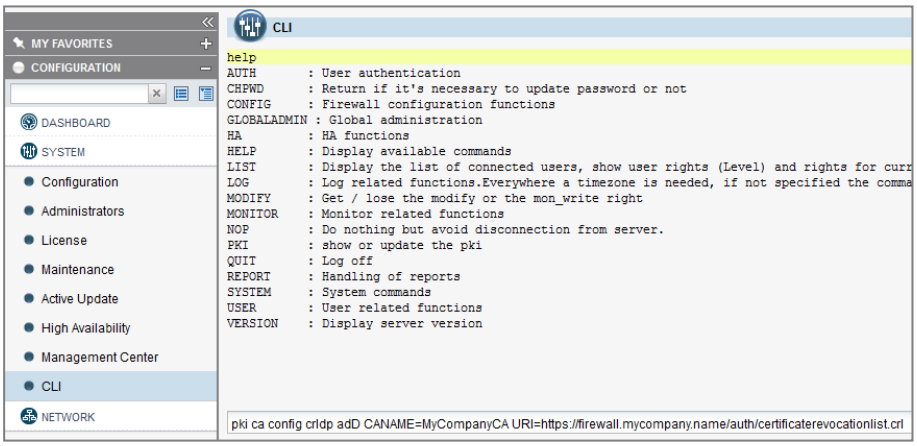
Choosing a URI that indicates the firewall's DNS name means that this name must be entered in an internal DNS server that can be accessed from SDS Suite clients.



After creating the CA, CRLDPs can no longer be added via the web administration interface (e.g.: adding a CRLDP hosted in another network zone, modifying a DNS name or the firewall's DNS alias). CRLDPs can therefore be modified using only CLI commands:

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

Example:



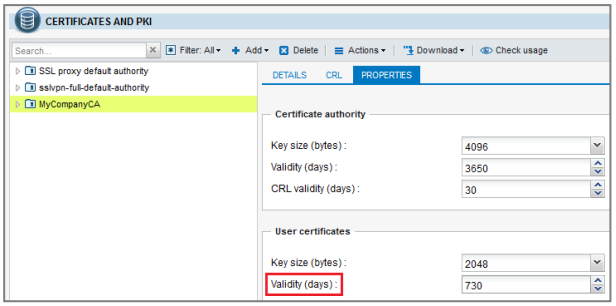
3. The last screen in the wizard will show a summary of the CA's settings. Confirm the creation by clicking on **Finish**.

Modifying CA settings

The CA creation wizard does not allow modifying the validity of user certificates (365 days by default) that were signed by the same CA.

However, this operation may be carried out by editing the properties of the CA after it has been created.

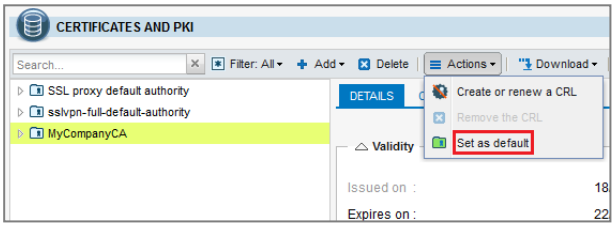
Select the CA in the left column, then click on the *Configuration* tab and modify the field **Validity (days)** in the **User certificates** panel in order to assign the recommended validity of 730 days (2 years):



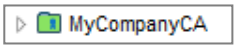
This value will then be applied every time the user certificate creation wizard is launched.

Defining the CA as the default CA for the LDAP directory

1. Select the CA from the left panel, then click on **Actions** and select **Set as default**.



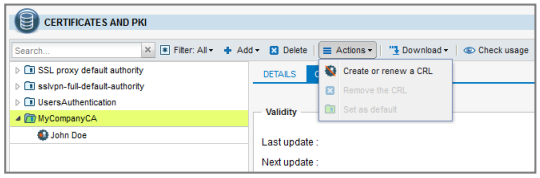
2. Confirm the operation by clicking on **Yes**.

The CA will now be identified by a green symbol 

indicating that it is the CA used by default to encrypt user certificates in the LDAP directory.

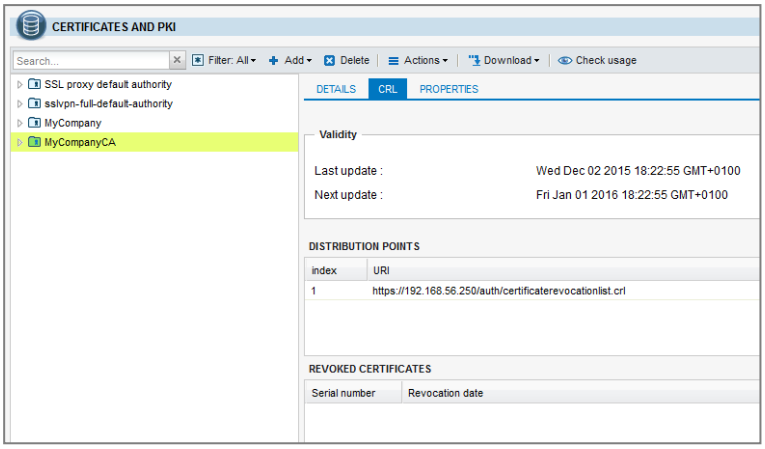
Creating the CRL

1. In the menu **Objects** > **Certificates and PKI**, select the CA then expand the menu **Actions** and click on **Create or renew a CRL:**



2. You need to enter the password that protects the CA, and then finish the operation by clicking on **Create or renew a CRL**.

The CRL will then be initialized (dates of the last and next update). It can be viewed in the CA's *CRL* tab.



Creating the recovery account

The recovery account is a specific account with the purpose of allowing the decryption of data belonging to a user whose private key may no longer be available.

This account can be configured in four steps (the first three are described in this chapter):

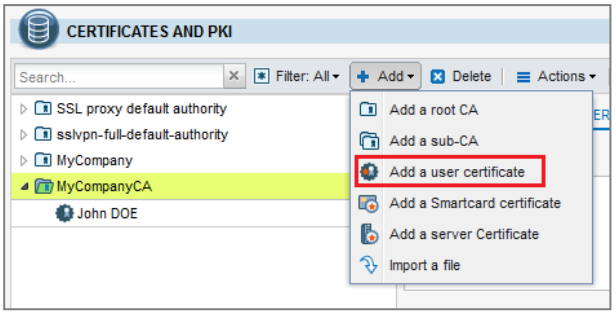
- creation of the recovery account on the firewall,
- creation of the recovery account's certificate.
- export of this certificate (in *.crt* format, without the private key),
- import of the recovery key in SDS Suite. This step is described in the paragraph Configuration of the recovery account in SDS Suite.

Creating the recovery account in the internal LDAP directory

1. In the **Users** menu, click on **Add user** and enter the mandatory fields in the *account* tab:
   - **Identifier (login):** data.recovery in the example,
   - **Last name:** recovery in the example,,
   - **First name:** data in the example,
   - **E-mail address**: data.recovery@mycompany.org in the example.
2. Click on **Apply** to confirm the creation.
3. A window will appear asking you to initialize the password. Enter the user's password twice and confirm.

Creating the recovery account's certificate

1. In the menu **Objects** > **Certificates and PKI**, select the default CA then expand the menu **Add** and select **Add user certificate:**



2. Fill in the fields in the wizard:

Properties of the user certificate

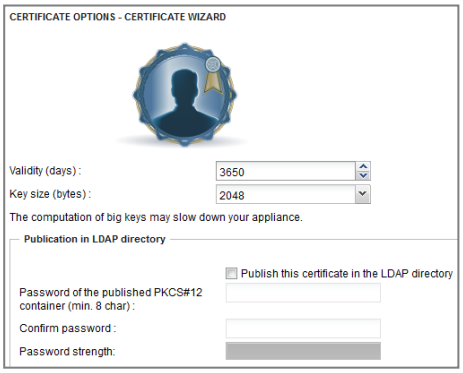
- **Name(CN):** Data recovery in the example,
- **ID:** the name of the user is suggested by default (Data.recovery in the example),
- **E-mail address**: data.recovery@mycompany.org in the example.

Options of the certificate (screen 1)

In the **Authority password** field, indicate the password of the default CA.

Options of the certificate (screen 2)

- **Validity**: indicate the same validity as the CA's (3650 days by default),
- You are advised against selecting the *Publication in LDAP directory* checkbox



Summary

Click on **Finish** to confirm the creation of the certificate.

NOTE
The recovery account must not be modified. If it has been modified, the recovery must also be modified on all SDS Suite clients.

Exporting the recovery account's certificate

1. Select the certificate of the recovery account then expand the **Download** menu and select **Certificate in DER format**.

2. Enter then confirm a password to protect the certificate and click on **Download the certificate**. Save it on your administration workstation and/or on a removable device so that you can import it on the client workstation.

Creating accounts and certificates without enrollment (recommended method)

This chapter sets out the method recommended by Stormshield and explains the following steps:

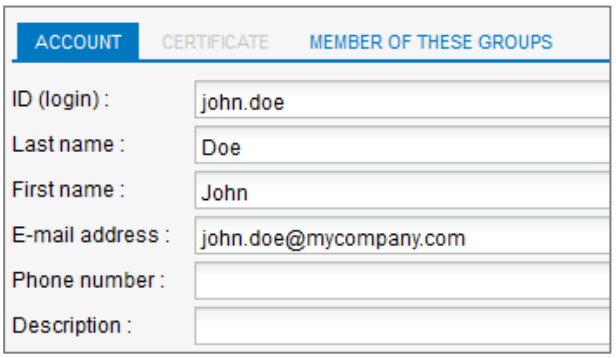
- creating an internal LDAP directory,
- creating and managing the CA,
- adding and deleting user certificates,
- publishing new certificates in the LDAP directory,
- CRL updates,
- creating a user in the Stormshield Data Security client,
- declaring the firewall's LDAP directory in the SNS user's address book.

Configuring the SNS firewall

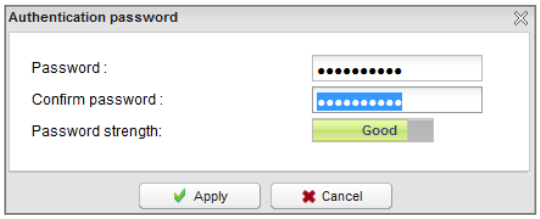
Creating a user and his certificate

Creating a user

1. In the **Users** menu, click on **Add user** and enter the mandatory fields in the *account* tab:
   - **Identifier (login)**
   - **Last name**
   - **First name**
   - **E-mail address** (required for creating the user's certificate)



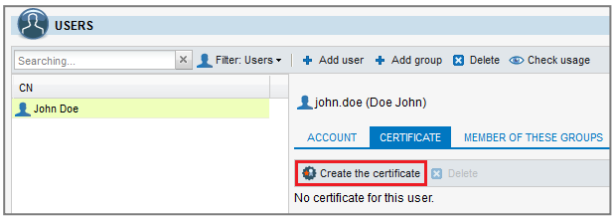
2. Click on **Apply** to confirm the creation.
3. A window will appear asking you to initialize the password. Enter the user's password twice and confirm:



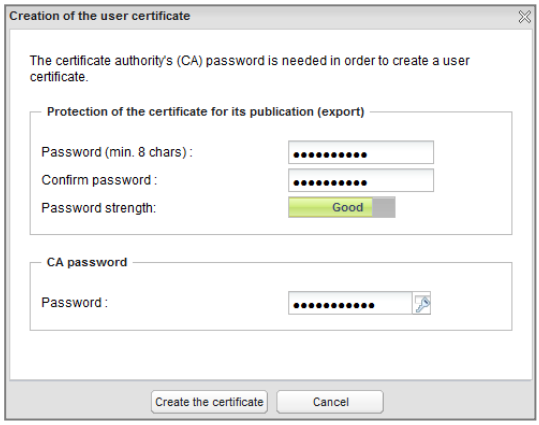
4. Give the user his identifier and this password so that he can modify it later from the authentication portal.

Creating the user's certificate and publishing it in the directory

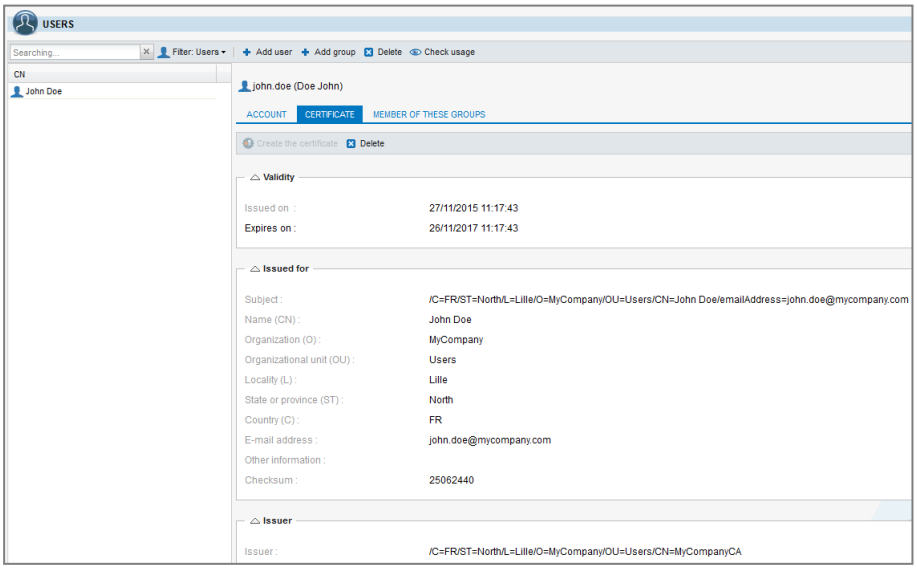
1. Select the user account created earlier and click on **Create certificate** (*Certificate* tab).



2. Indicate a password that will be used to protect the certificate. This password is completely different from the user password. You will be asked for it when exporting the certificate. Next, enter the CA password and click on **Create certificate**:



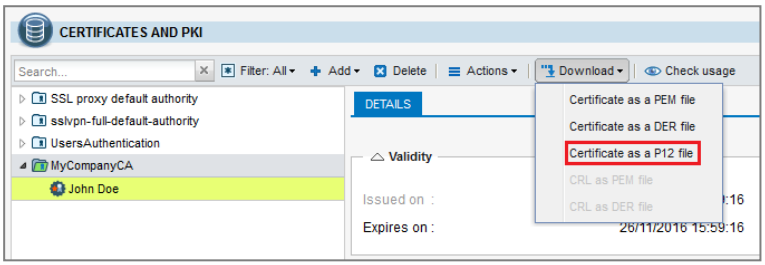
The certificate will be automatically published in the LDAP directory; its details can be viewed in the user's *Certificate* tab:



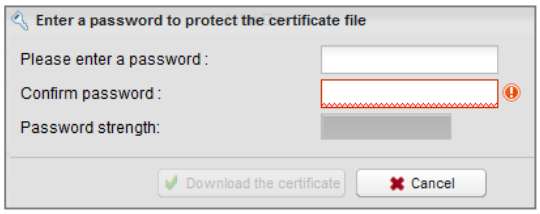
NOTE
Creating the certificate in the LDAP directory automatically involves the creation of the user's private key.

Exporting a user's certificate and private key

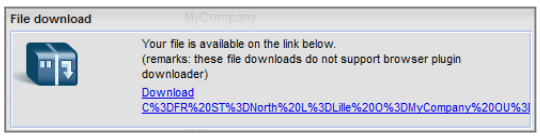
1. In the menu **Objects** > **Certificates and PKI**, select the certificate to be exported, then expand the menu **Download** and select **Certificate in P12 format:**



2. Enter the password that protects the certificate (password initialized during the creation of the certificate) and confirm by clicking on **Download the certificate**:



3. Click on the hypertext link and save the file (".p12" extension) on your administration workstation:



IMPORTANT
This file in PKCS#12 format is an encrypted file that contains the user's certificate and private key. It must therefore be sent through secure channels.

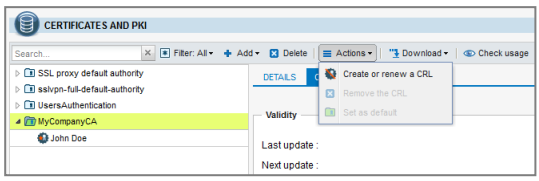
Updating and publishing the CRL

Querying the CRL is a critical point during the use of a Stormshield Data Security client: cryptographic operations may indeed be compromised if the CRL is not up to date. This update takes place automatically during the revocation of a certificate from the menu **Certificates and PKI** if the option **Create CRL after revocation** has been selected (this operation is described in the paragraph Revoke a user certificate and update the CRL).

However, the CRL has to be updated manually in the following cases:

- deletion of a user certificate from the **Users** menu,
- if the CRL has expired or is about to expire.

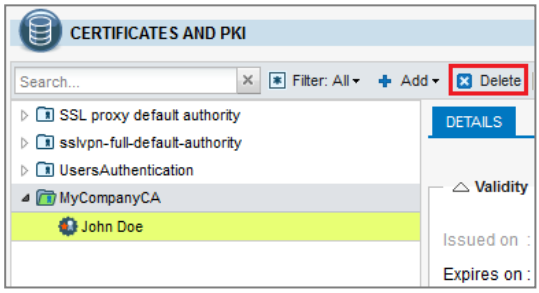
To manually update the CRL, select the CA in the menu **Objects** > **Certificates and PKI**, then expand the menu **Actions** and click on **Create or renew a CRL:**



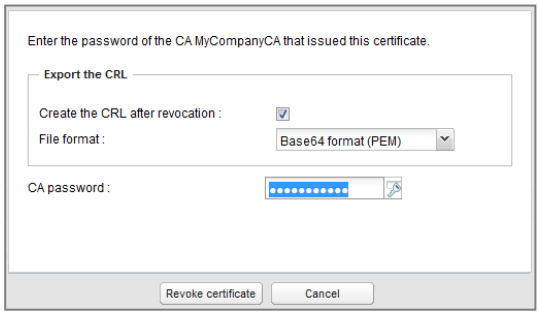
The validity of the CRL will then be modified accordingly. Since the CRL is stored directly on the firewall, it will be updated automatically without the need for a manual republication.

Revoking a user certificate and updating the CRL

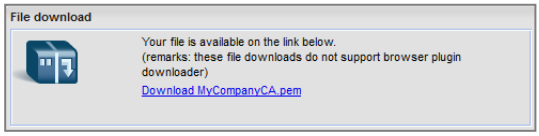
1. From the menu **Objects** > **Certificates and PKI**, select the user certificate to be revoked, then click on **Delete**.



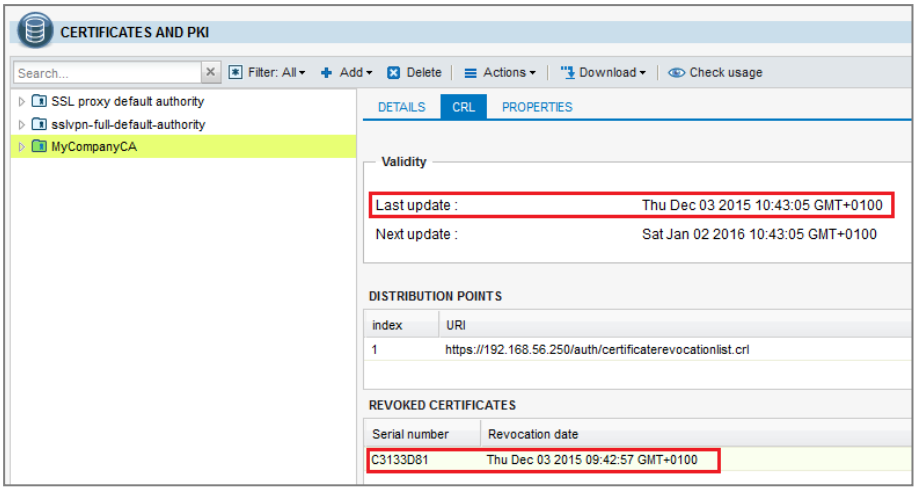
2. Check that **Create CRL after revocation** has been selected: this will allow the automatic update of the CRL at the end of the certificate revocation process.
3. Enter the CA's password and confirm the deletion by clicking on **Revoke the certificate**:



4. Enter the CA's password again to update the CRL and click on **Create or renew a CRL**.
5. You can now download the CRL, which has been updated so that it can be published on distribution points other than the firewall:

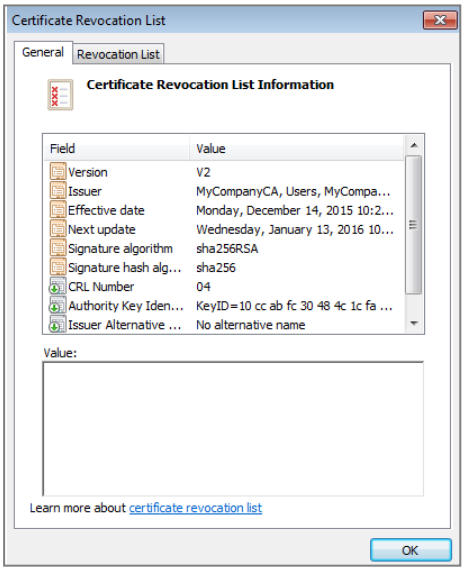


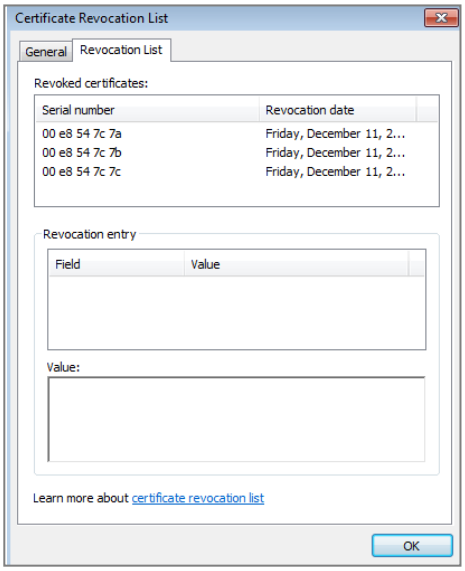
Information about the CRL immediately reflects the fact that the certificate has been revoked.



Since the CRL is stored directly on the firewall, it will be updated automatically without the need for a manual republication.

The CRL retrieved from the CRDLP (**https://***firewall_dns_name*/**auth**/*certificaterevocationlist.crl* or **https://***firewall_ip_address*/**auth**/*certificaterevocationlist.crl*) allows checking that the certificate has indeed been revoked:

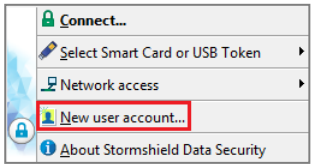




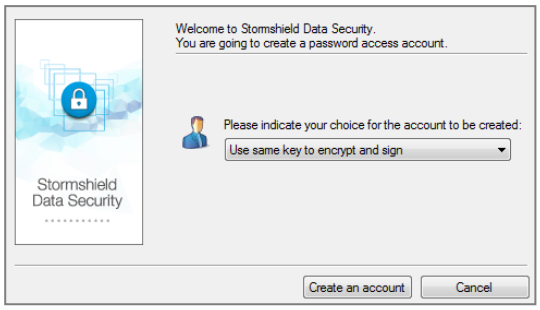
Configuring the SDS software suite

Creating a new user in SDS Suite

1. Right-click on the  icon found in the taskbar of the user workstation and select the menu **New user**:



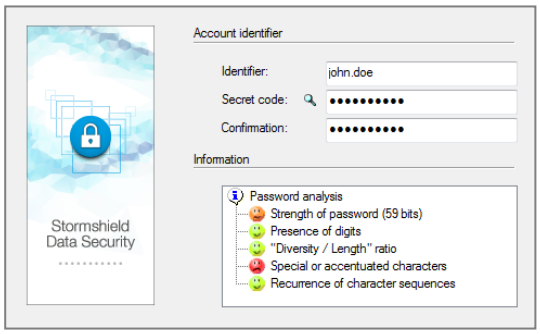
2. Select the option **Use a single key for encrypting and signing** then click on **Create an account**:



3. Identifier of the account

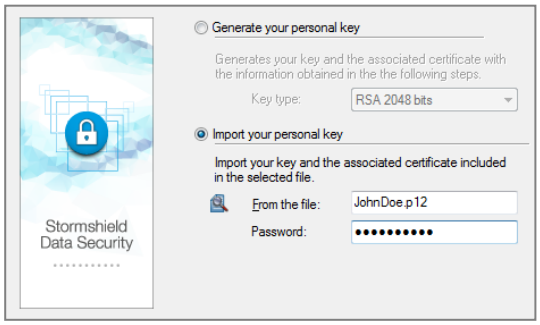
Fill in the three mandatory fields:

- **Identifier**: this connection identifier has to be the same as the one entered in the firewall's LDAP directory (john.doe in the example).
- **Personal code**: the user enters a strictly personal password that will be used for protecting his SDS Suite account. This password is not in any way linked to the one that protects his private key.
  Criteria for this password's complexity are displayed in the **Information** window.
- **Confirmation**: the user must confirm the chosen password.



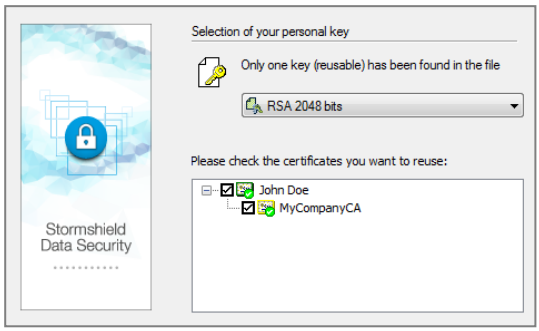
4. Personal key

Select the option **Import your personal key** and select the PKCS#12 file (".p12" extension) containing the user's certificate and private key. Enter the password that protects this certificate and confirm by clicking on **Next**:

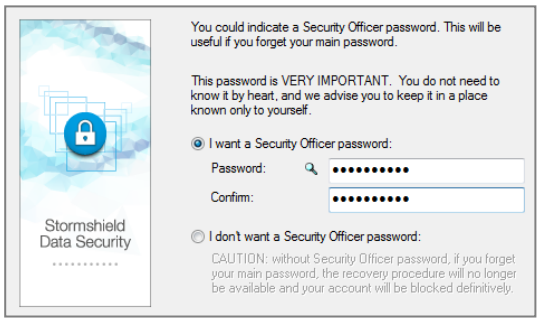


NOTE

The CA certificate is also suggested during an import. Ensure that the user and CA certificate checkboxes have been selected.



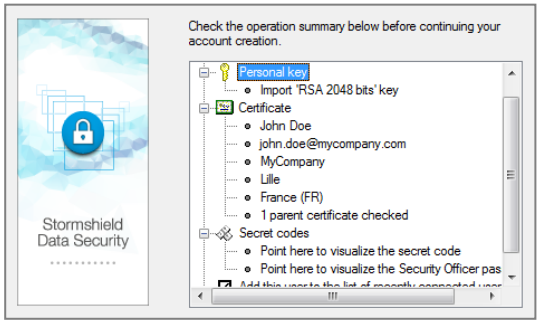
5. Validate by clicking on **Next**.
6. The wizard will then offer to create a backup password that will allow finding the password to the user account in the event it gets lost. You are strongly advised to create this backup password. Enter and confirm this password. Validate by clicking on **Next**:



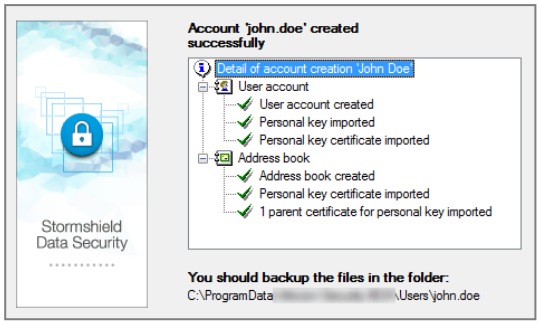
IMPORTANT

Without a backup password, the user's password cannot be retrieved if it is lost. You are therefore strongly advised to create a backup password.

7. When you see the screen providing a summary of the user account, confirm by clicking on **Finish**.



8. The creation of the local directory will be launched automatically and the last screen will give a summary of the operations performed:



9. Click on **Quit** to close the wizard.

Adding the firewall's directory in the SDS Suite address book.

Referencing an LDAP directory in the local address book makes it possible to indicate to SDS Suite that this directory must always be queried when sending or receiving e-mail.

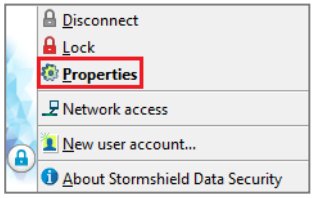
Connecting the user to SDS Suite

1. Right-click on the SDS Suite icon found in the taskbar and select the menu **Connect...**:

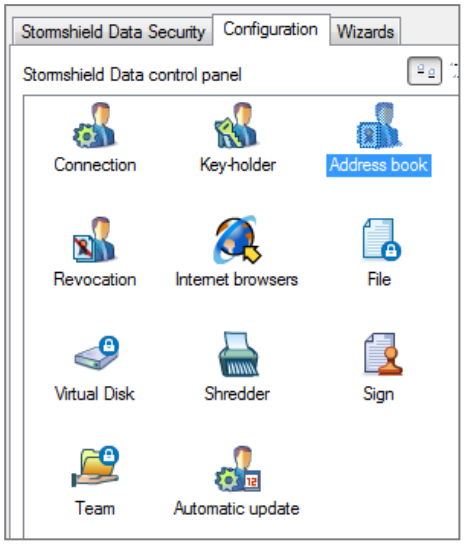
2. Enter the user's password and click on **Confirm**:

Adding the firewall's LDAP directory

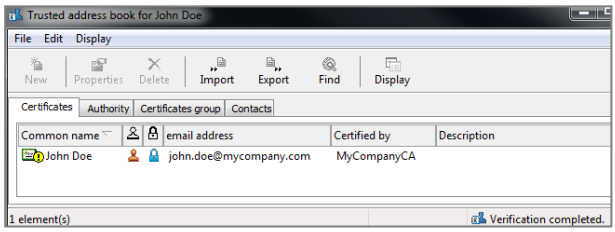
1. After logging on, right-click again on the SDS Suite icon found in the taskbar and select the menu **Properties**:



2. In the *Configuration* tab of the user properties window, double-click on the **Directory** icon:



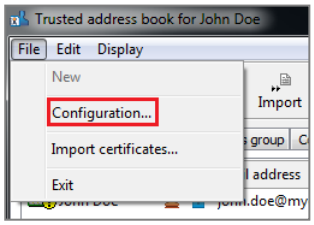
The contents of the user's local directory will be shown:



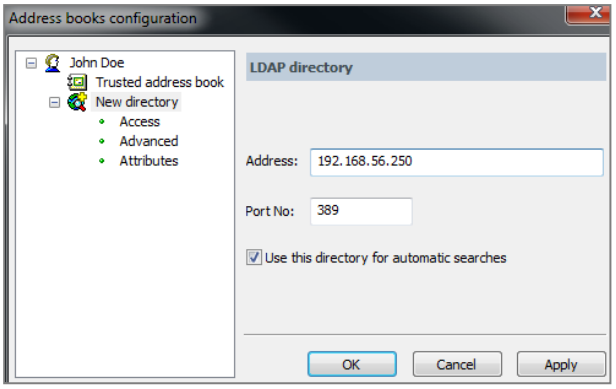
NOTE

In the example, the  symbol indicates that the listed certificate needs to be used carefully as the CRL could not be looked up.

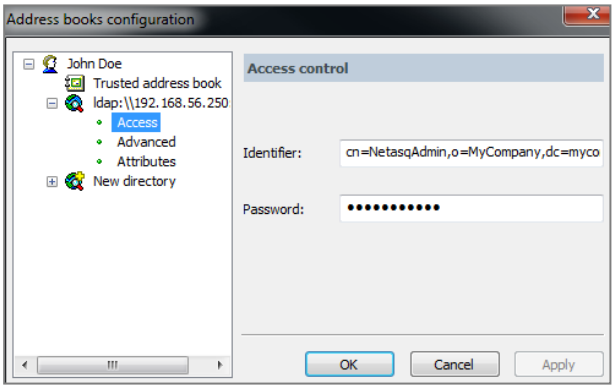
3. Expand the **File** menu and select **Configuration...** :



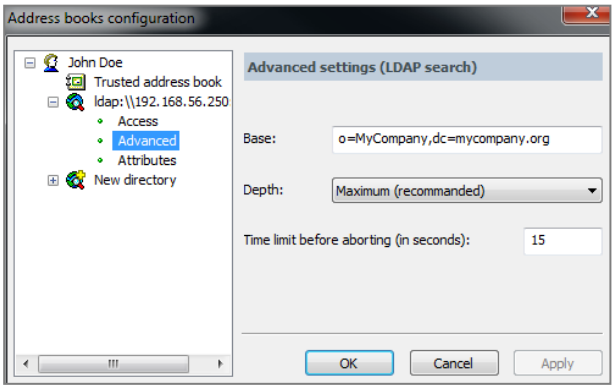
4. In the directory configuration window, click on **Add a directory** and enter the firewall's IP address (192.168.56.250 in the example) or DNS name (this name must then be entered in a DNS server that SDS Suite clients can contact). Leave the port entered by default (LDAP/389) and select **Use this directory for automatic searches**:



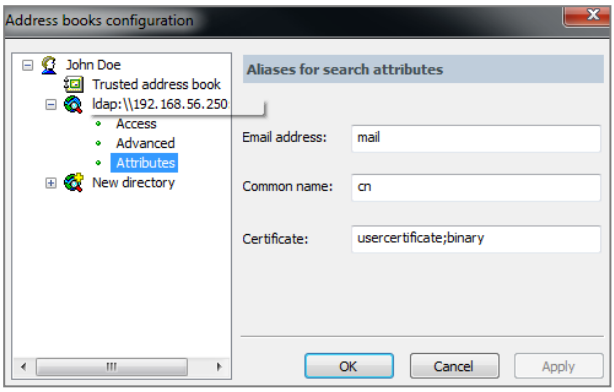
5. Click on **Apply**.
6. In the properties of the LDAP added, select **Access** and fill in both fields:
   - **Login**: Distinguished Name (DN) of the user allowed to browse the directory (NetasqAdmin). It will resemble the following: cn=NetasqAdmin, o=Organisation, dc=Domain (example : cn=NetasqAdmin,o=MyCompany,dc=mycompany.org)
   - **Password**: enter the password used during the creation of the LDAP directory on the firewall.



7. In the properties of the LDAP directory, select **Advanced** and fill in the **Base** field corresponding to the Base DN that stores certificates on the firewall. It will resemble the following: o=Organisation,dc=Domain (example: o=MyCompany,dc=mycompany.org).



8. In the properties of the LDAP directory, select **Attributes** and check that the fields contain the following values:
   - **Email address**: *mail*,
   - **Common name**: *cn*,
   - **Certificate**: *usercertificate;binary*.



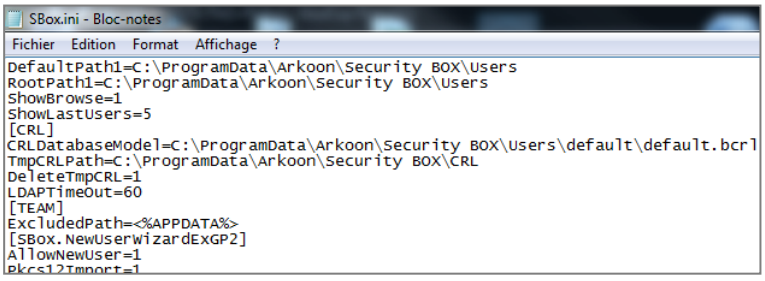
9. Click on **OK** to confirm the creation of the LDAP directory in the user's address book.

Adding certificates of e-mail peers automatically

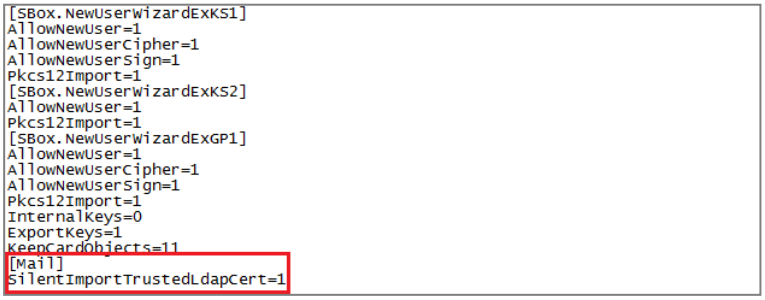
It is possible to configure the LDAP directory in such a way that peer certificates contained in it are automatically added to the SDS Suite local directory when e-mails are sent to them.

To do so, the SDS Suite configuration file *sbox.ini* must be modified as follows:

1. Edit the *sbox.ini* file found in the Kernel folder of the SDS Suite installation path (C:\Program Files\Arkoon\Security BOX\Kernel\ in the example).



2. Create a [Mail] section, add a field "SilentImportTrustedLdapCert" and assign the value "1" to it:

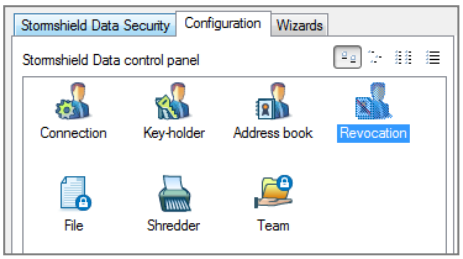


3. Save the changes and close the file.

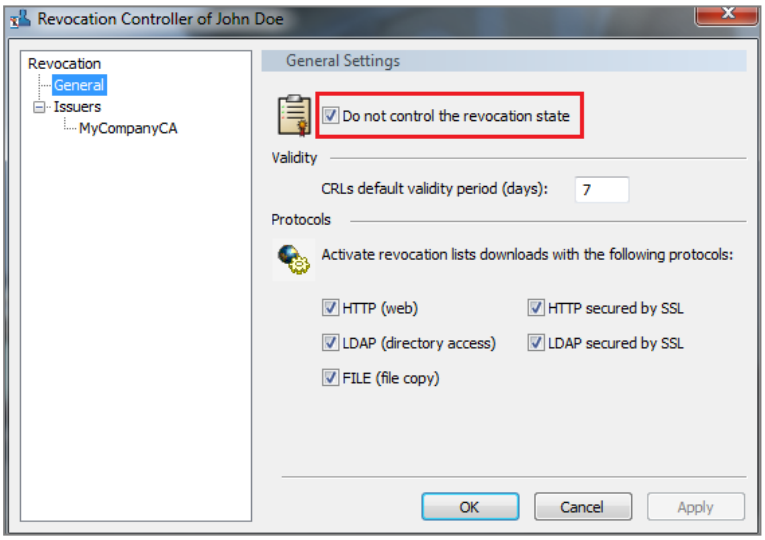
Enabling / Disabling certificate revocation control

When the version of the Stormshield Network firewall firmware hosting the CRL is lower than 2.4, certificate revocation control on the SDS client needs to be disabled.

1. Right-click on the SDS Suite icon found in the taskbar and select the menu **Properties**:
2. In the *Configuration* tab, double-click on the menu **Revocation**:



3. Select the checkbox "Do not control the revocation state" located in the **Revocation** > **General** menu. Apply and confirm:



NOTE
Remember to unselect this checkbox when the Stormshield Network firewall hosting the CRL has firmware in at least version 2.4.

Importing the firewall's certificate into the client workstation's trusted certificates

When the SDS Suite client performs an automatic check of the CRL status, it logs on in HTTPS to the CRLDP hosted on the SNS firewall, which is when the firewall's certificate will be presented. In order for this check to run smoothly, the firewall's certificate must therefore be imported into the Windows trusted certificate management console.

Retrieving the firewall's certificate

From Internet Explorer

1. In the browser's address bar, enter the address for connecting to the firewall's administration interface: **https://***firewall_ip_address*/**admin** or **https://***firewall_dns_name*/**admin.**

   REMINDER
   Choosing a URI that indicates the firewall's DNS name means that this name must be entered in an internal DNS server that can be accessed from SDS Suite clients.

2. When the firewall authentication page appears, click on the security report area located to the right of the browser's address bar.
3. In the security report window, click on **View certificates**.
4. In the *Details* tab, click on **Copy to a file...**
5. Click on **Next**,
6. Leave the suggested default format: **DER encoded binary X.509 (.CER)**, then click on **Next**.
7. Click on **Browse** to select a location to save the file, then enter a name for the file and click on **Save.**
8. Click on **Next** then on **Finish**.
9. Confirm the message "**The export was successful**".
10. Close the window showing details of the certificate by clicking on **OK.**

From Mozilla Firefox

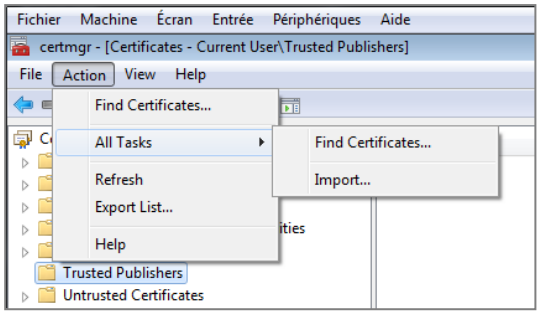
1. In the browser's address bar, enter the address for connecting to the firewall's administration interface: **https://***firewall_ip_address*/**admin** or **https://***firewall_dns_name*/**admin.**

   REMINDER
   Choosing a URI that indicates the firewall's DNS name means that this name must be entered in an internal DNS server that can be accessed from SDS Suite clients.

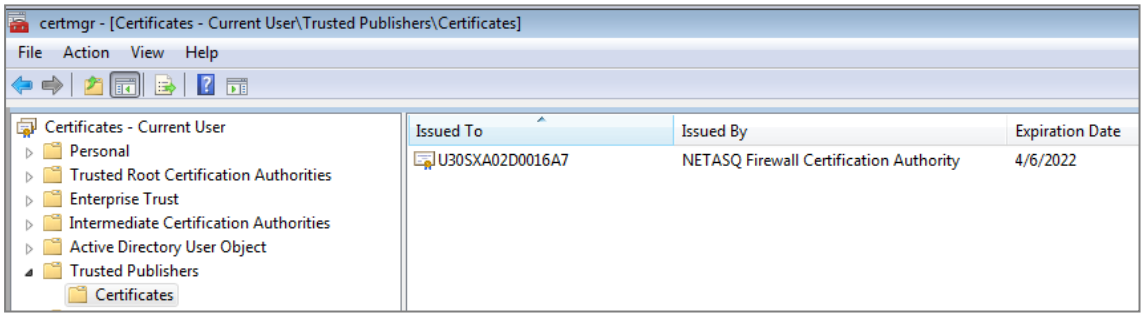
2. When the firewall authentication page appears, click on the security report area (padlock) located to the left of the browser's address bar.
3. In the security report window, click on ">" then on the **More information** button.
4. Click on **View certificate**.
5. In the *Details* tab, click on **Export...**
6. Select a location to save the file, then enter a name for the file (leave the extension ".crt" suggested by default) and click on **Save.**
7. Close the window showing details of the certificate by clicking on **Close.**
8. Close the security report window using the button. 

Importing this certificate into the client workstation's trusted certificate management console

1. In the Windows **Start** > **Run** menu, enter *certmgr.msc* then confirm by clicking on **OK** in order to run the certificate management console.
2. In the menu to the left of the console, select the store **Trusted Publishers** > **Certificates**.
3. Click on the **Action** > **All tasks** > **Import...** menu.



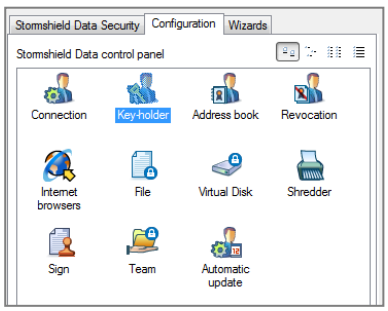
4. Select the firewall's certificate, exported earlier through your internet browser, then click on **Next**.
5. Confirm your choice of the certificate store (**Trusted Publishers**) by clicking on **Next.**
6. Confirm the import by clicking on **Finish**.
7. A message will confirm that the certificate was correctly imported. Your firewall's certificate will now appear in the store. It can be identified through your firewall's serial number (or its DNS name if it has one).



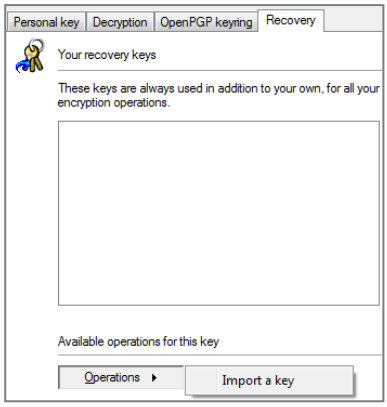
Importing the recovery key in SDS Suite

IMPORTANT
The recovery key must be imported into the SDS Suite client before any data is encrypted. Indeed, data encrypted before the installation of the recovery key may not be retrieved if the user loses his private key.

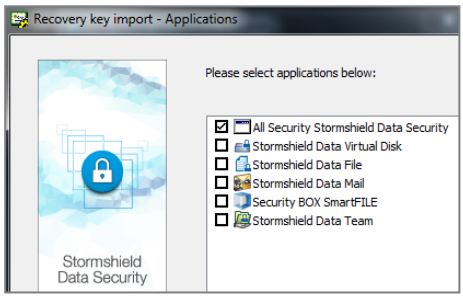
1. Right-click on the SDS Suite icon found in the taskbar and select the menu **Properties**:
2. In the *Configuration* tab, double-click on the menu **Keyring**.



3. Select the *Recovery* tab and click on **Import a key**.

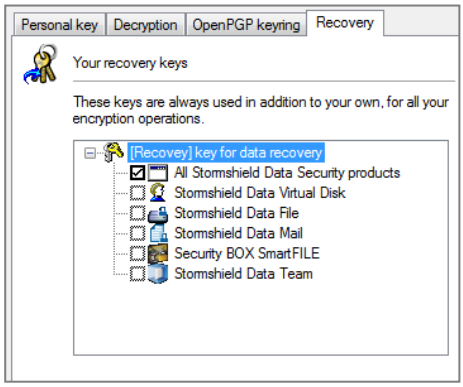


4. Select the recovery account's certificate.
5. Indicate the applications for which you wish to use this recovery key by selecting the checkbox **All Stormshield Data Security products**:



6. Click on **Finish** to confirm the operation.

The recovery key has now been declared for the SDS Suite user account:



Using the recovery account

In the event a user loses his private key, the recovery account may allows the user to decrypt his data.

Generating a new user certificate and its associated private key

Delete the previous user certificate and update the CRL (see Revoking a user certificate and updating the CRL).

In a configuration that does not use enrollment:

1. Generate a new certificate and its key.
2. Export the certificate and its key in PKCS#12 format (see Exporting a user's certificate and private key).

In a configuration that uses enrollment:

1. The user submits a new certificate request through the authentication portal (menu **Certificates** > **Request your certificate**, accessible after authentication on the portal).
2. The administrator will validate this request in the menu **User** > **Enrollment** (see Validating a user and certificate creation request).
3. The user will then retrieve his certificate and key from the authentication portal.
4. He will save them in PKCS#12 format and store this format in a secure location.

Creating a recovery user in SDS Suite

On the client workstation, follow the method described in the chapter Creating a new SDS user in order to create the recovery account in SDS Suite.

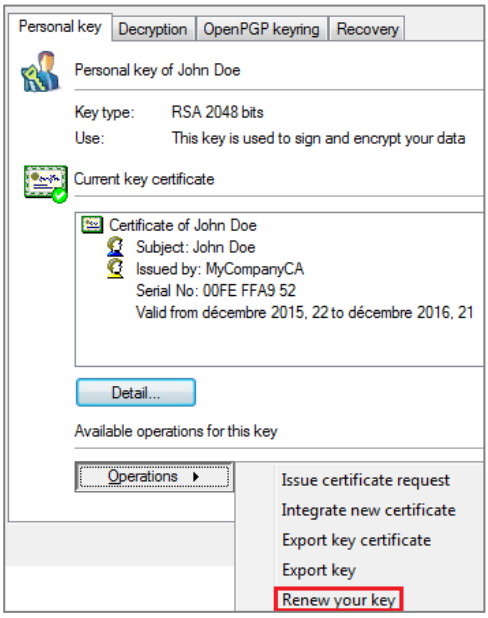
Decrypting the user's data using the recovery account

Logging on to SDS Suite using the recovery account will enable the manual decryption of the user's data.

NOTE
This decryption operation must be carried out with all the SDS Suite modules that the user had used to encrypt his data (File, Mail, etc).

Renewing the user's key

1. The user logs on to the SDS Suite client using his personal account.
2. In the *Personal key* tab in the **Keyring** menu of the SDS Suite client, expand the **Operations** menu and select **Renew your key**.



3. Next, select the option **Import your personal key**, select the PKCS#12 file containing the new user key and enter the password that protects the file.

Encrypting data using the recovery account

The user can now encrypt his data again.

NOTE
This encryption operation must be carried out with all the SDS Suite modules that the user had used to encrypt his data (File, Mail, etc).

Creating accounts and certificates through enrollment (alternative method)

This chapter covers an alternative method that allows the enrollment of users through the authentication portal. However, this solution has the major disadvantage of not offering any key escrow solution for users' private keys on the firewall.

In the event a user loses his private key, it will therefore be impossible to retrieve it and the user's encrypted data will become inaccessible as well. Only a recovery account would allow retrieving data encrypted by a user who has lost his private key. This method also forces users to ensure that they store their private keys in a secure location.

NOTE
Since enrollment does not function with a Microsoft Active Directory, only the use of an internal LDAP directory will be described in this document.

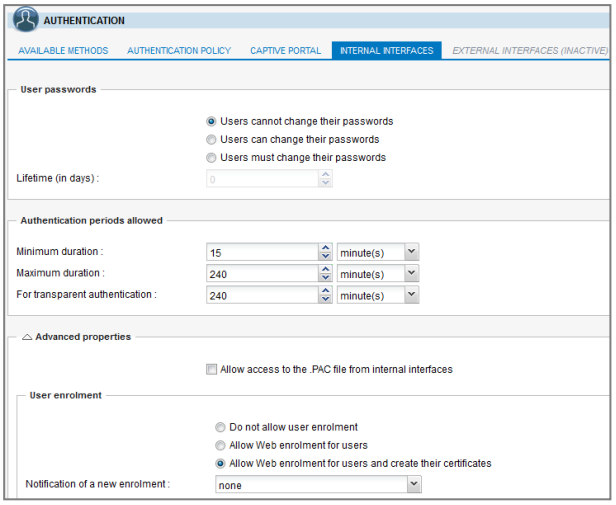
The steps presented for this method are the following:

- creating an internal LDAP directory,
- enabling enrollment,
- creating and managing the CA,
- creating a recovery account and its certificate on the firewall,
- signing certificates created after user requests through the captive portal,
- publishing certificates in the LDAP directory,
- updating the CRL,
- creating a user in the Stormshield Data Security client,
- declaring the firewall's LDAP directory in the SDS user's address book.
- importing the recovery key in SDS Suite.

Configuring the SNS firewall

Enabling enrollment and certificate signing requests

1. In the *Internal interfaces* tab, in the menu **User** > **Authentication**, expand the **Advanced properties** panel and select **Allow web enrolment for users and create their certificate**.



2. Confirm by clicking on **Apply**.

NOTE

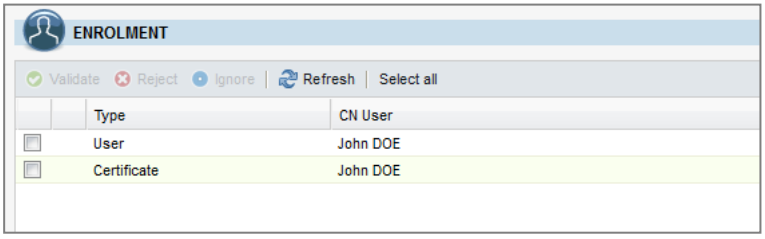
If you want a group of e-mail recipients to be notified of every enrollment request (**Notification of a new enrolment** field), this group needs to be created beforehand in the *Recipients* tab in the menu **Notifications** > **E-mail alerts**.

Approving enrollment requests

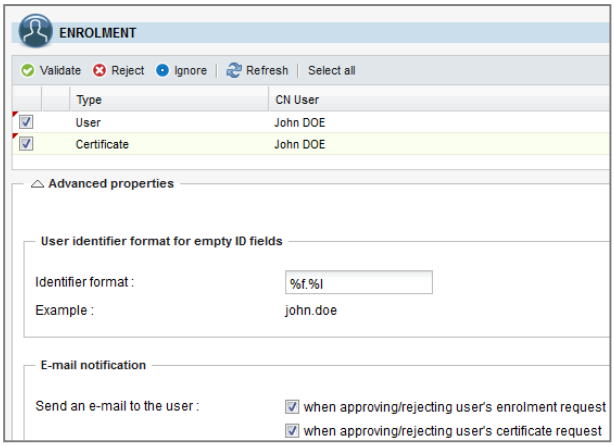
Every request to create a user and certificate submitted through the authentication portal must be validated by an administrator of the firewall. The user and his certificate will then be automatically published in the firewall's internal LDAP directory.

Validating a user and certificate creation request

The **Users** > **Enrollment** menu shows the various requests to create users and sign certificates pending approval:



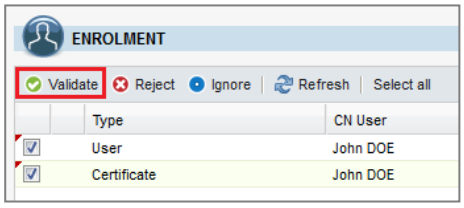
1. Select the checkboxes of the user creation and certificate requests that need to be approved,
2. In the **Advanced properties** panel, indicate the format to be used for creating the user's login. For a *firstname.lastname* format (lowercase only), select *%f.%l*. The example under the window will dynamically display the format applied:



NOTE

The user can be alerted to the approval or rejection of his requests by selecting the relevant checkboxes in the **Advanced properties** panel:
Send an e-mail to the user: during the approval of his enrollment request
Send an e-mail to the user: during the approval of his certificate request

3. Click on **Approve**:



4. Then click on Apply at the bottom of the window then on **Save** in the confirmation message,
5. Enter the password of the CA in order to sign the user certificate,
6. The user and his certificate will be automatically published in the firewall's LDAP directory.

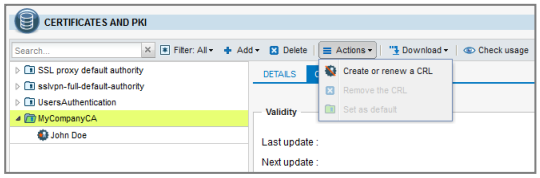
Updating and publishing the CRL

Querying the CRL is a critical point during the use of a Stormshield Data Security client: cryptographic operations may indeed be compromised if the CRL is not up to date. This update takes place automatically during the revocation of a certificate from the menu **Certificates and PKI** if the option **Create CRL after revocation** has been selected (this operation is described in the paragraph Revoke a user certificate and update the CRL).

However, the CRL has to be updated manually in the following cases:

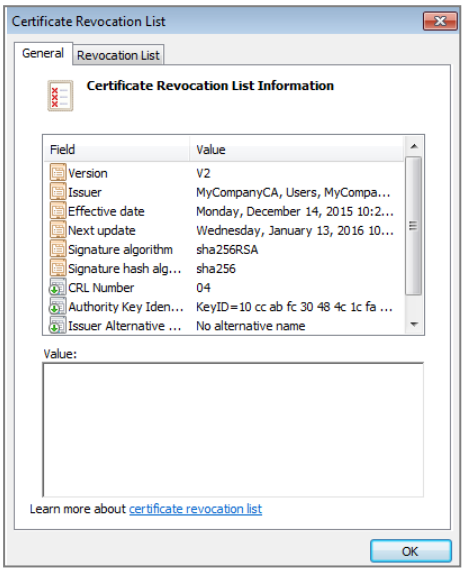
- deletion of a user certificate from the **Users** menu,
- if the CRL has expired or is about to expire.

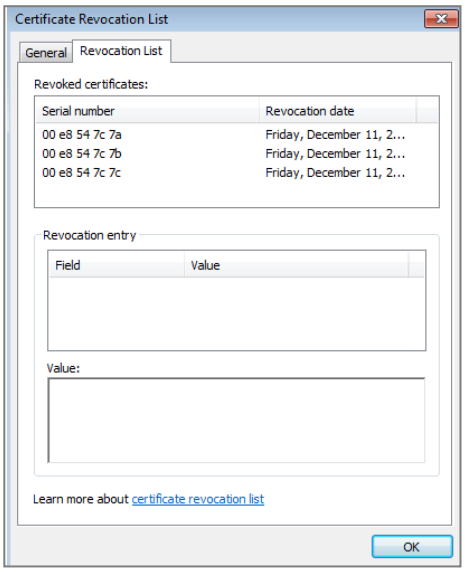
To manually update the CRL, select the CA in the menu **Objects** > **Certificates and PKI**, then expand the menu **Actions** and click on **Create or renew a CRL:**



The validity of the CRL will then be modified accordingly. Since the CRL is stored directly on the firewall, it will be updated automatically without the need for a manual republication.

The CRL retrieved from the captive portal (**https://***firewall_dns_name*/**auth**/ or **https://***firewall_ip_address*/**auth** then **Certificate** > **Your company's certificate revocation list**) makes it possible to check that the certificate has indeed been revoked:



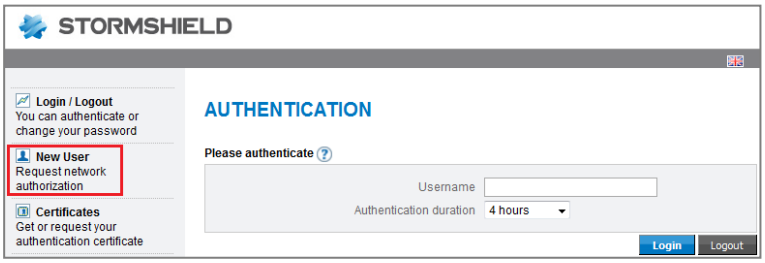


Enrolling a user

In this chapter, requests to enroll, retrieve and back up certificates are carried out by the SDS Suite user.

Requesting enrollment

The user logs on to the firewall's web authentication portal using a URL resembling: https://*firewall_ip_address*/auth/ in order to submit his account creation request and clicks on the **New user** menu on the left:



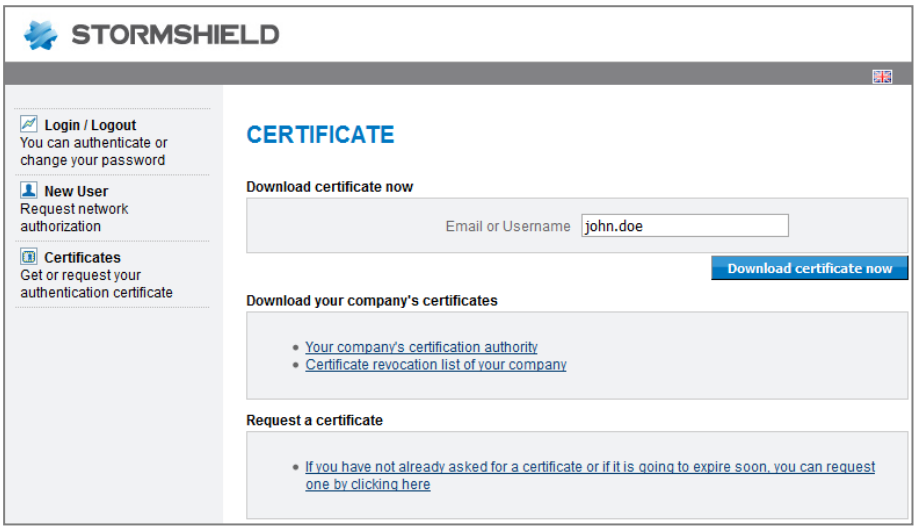
The user then fills in the mandatory fields in the request form (**First name**, **Last name**, **E-mail address**, **Password**) and confirms his request by clicking on **Submit information...**

His request for the creation of an account and the signing of the associated certificate will then be submitted to a firewall administrator for validation. The validation of this request will be covered in the chapter Approval of enrollment requests by an administrator.

Retrieving the certificate

When the user's request has been approved by an administrator, he will be able to retrieve his certificate from the firewall's authentication portal.

The user can log on to the authentication portal (https://*firewall_ip_address*/auth/) using his user name and password, click on the **Certificates** menu on the left, enter his user name (*john.doe* in the example) and click on **Download the certificate**:



NOTE
With the enrollment method, the user's certificate and private key will be created and stored in the user's Internet browser (the private key will never be saved on the firewall). Since this operation can only be carried out once, it is important that you immediately save the certificate and private key in a secure location, and delete them from the browser when the connection to the SDS Suite client has been validated for the user.

Saving the user certificate

On the client workstation, go to the web browser's certificate store in order to save the certificate:

Firefox:

1. Go to the *Certificates* tab in the **Settings > Advanced** menu and click on **Show certificates**,
2. Select the user's certificate,
3. Click on **Save**,
4. Select a secure backup location, select the PKCS12 format, give a name to the certificate and click on **Save**,
5. Enter a backup password for the certificate and validate.

Internet Explorer:

1. Go to the *Contents* tab in the **Internet options** menu and click on **Certificates**,
2. Select the user's certificate,
3. Click on **Export** then on **Next**,
4. Select **Yes, export the private key** then the format **Private information exchange - PKCS#12**,

5. Enter a name for this certificate,
6. Enter a backup password for the certificate,
7. Select a secure backup location, click on **Save** and validate.

Next, delete the certificate and its key from the Internet browser.

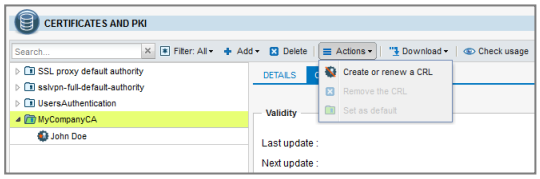
Updating and publishing the CRL

Querying the CRL is a critical point during the use of a Stormshield Data Security client: cryptographic operations may indeed be compromised if the CRL is not up to date. This update takes place automatically during the revocation of a certificate from the menu **Certificates and PKI** if the option **Create CRL after revocation** has been selected (this operation is described in the paragraph Revoke a user certificate and update the CRL).

However, the CRL has to be updated manually in the following cases:

- deletion of a user certificate from the **Users** menu,
- if the CRL has expired or is about to expire.

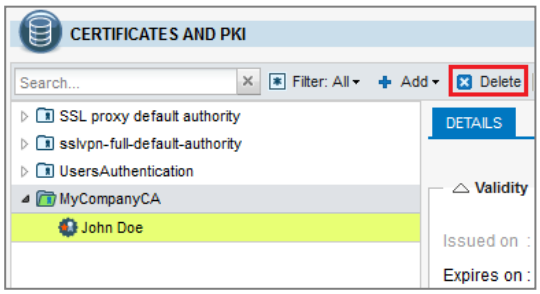
To manually update the CRL, select the CA in the menu **Objects** > **Certificates and PKI**, then expand the menu **Actions** and click on **Create or renew a CRL:**



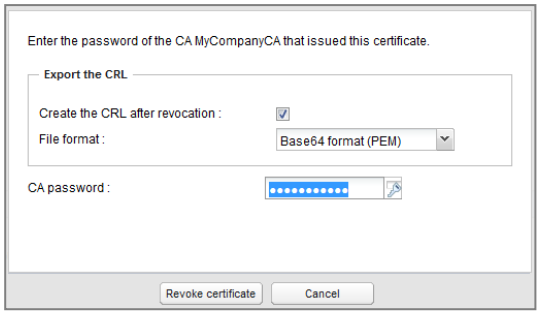
The validity of the CRL will then be modified accordingly. Since the CRL is stored directly on the firewall, it will be updated automatically without the need for a manual republication.

Revoking a user certificate and updating the CRL

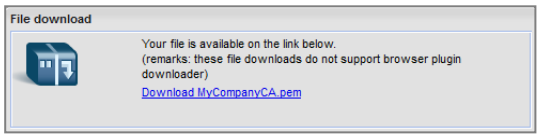
1. From the menu **Objects** > **Certificates and PKI**, select the user certificate to be revoked, then click on **Delete**.



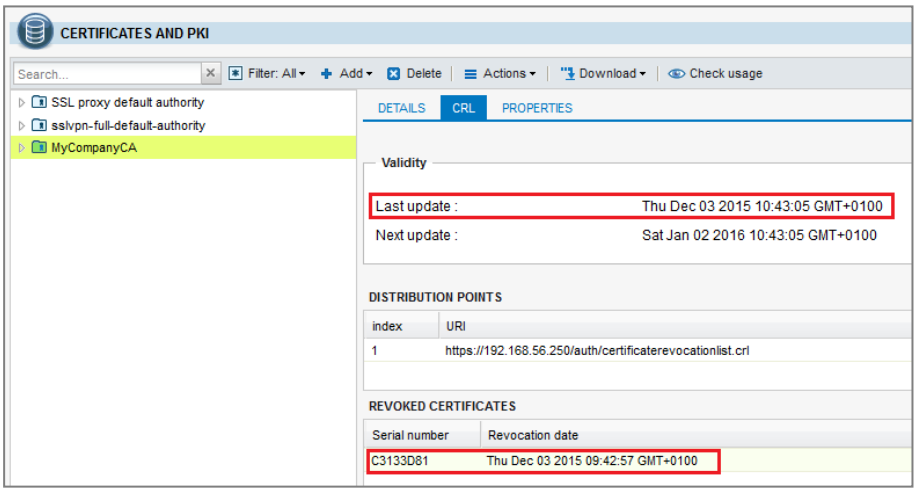
2. Check that **Create CRL after revocation** has been selected: this will allow the automatic update of the CRL at the end of the certificate revocation process.
3. Enter the CA's password and confirm the deletion by clicking on **Revoke the certificate**:



4. Enter the CA's password again to update the CRL and click on **Create or renew a CRL**.
5. You can now download the CRL, which has been updated so that it can be published on distribution points other than the firewall:

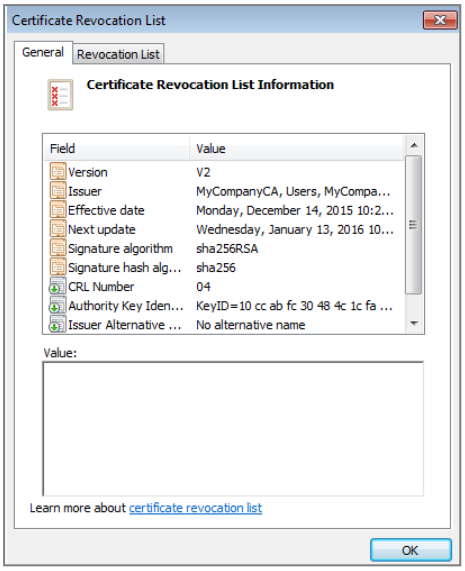


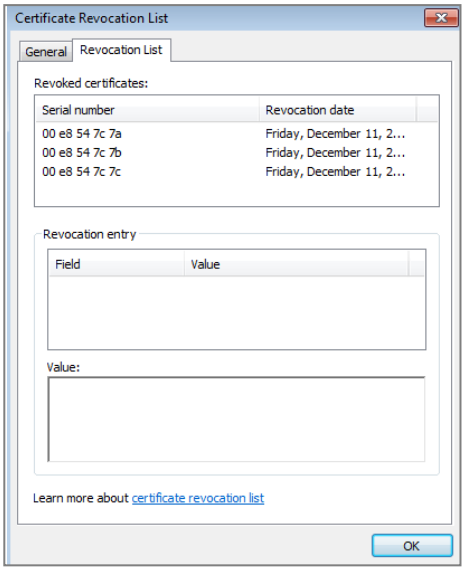
Information about the CRL immediately reflects the fact that the certificate has been revoked.



Since the CRL is stored directly on the firewall, it will be updated automatically without the need for a manual republication.

The CRL retrieved from the captive portal (**https://***firewall_dns_name*/**auth**/ or **https://***firewall_ip_address*/**auth** then **Certificate** > **Your company's certificate revocation list**) makes it possible to check that the certificate has indeed been revoked:

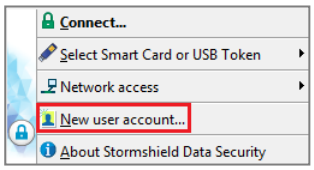




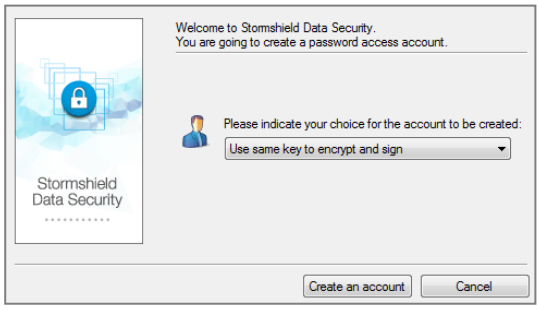
Configuring the SDS software suite

Creating a new user in SDS Suite

1. Right-click on the  icon found in the taskbar of the user workstation and select the menu **New user**:



2. Select the option **Use a single key for encrypting and signing** then click on **Create an account**:



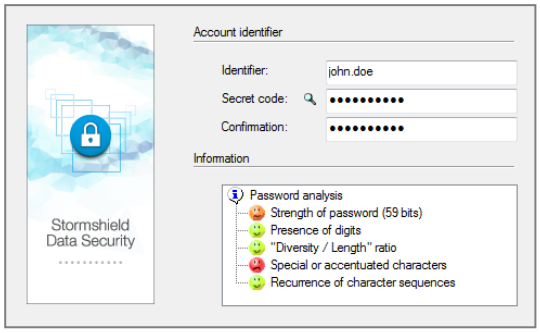
3. Identifier of the account

Fill in the three mandatory fields:

- **Identifier**: this connection identifier has to be the same as the one entered in the firewall's LDAP directory (john.doe in the example).
- **Personal code**: the user enters a strictly personal password that will be used for protecting his SDS Suite account. This password is not in any way linked to the one that protects his private key.

Criteria for this password's complexity are displayed in the **Information** window.

- **Confirmation**: the user must confirm the chosen password.



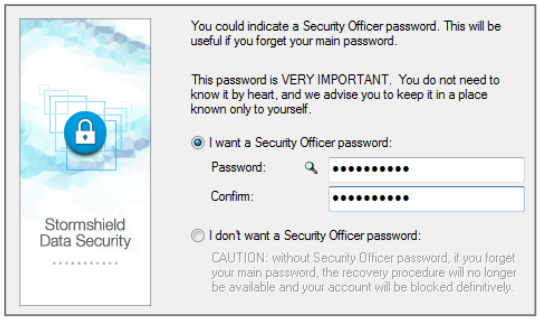
4. Personal key

Select the option **Import your personal key** and select the PKCS#12 file (".p12" extension) containing the user's certificate and private key. Enter the password that protects this certificate and confirm by clicking on **Next**:

NOTE

The CA certificate is also suggested during an import. Ensure that the user and CA certificate checkboxes have been selected.

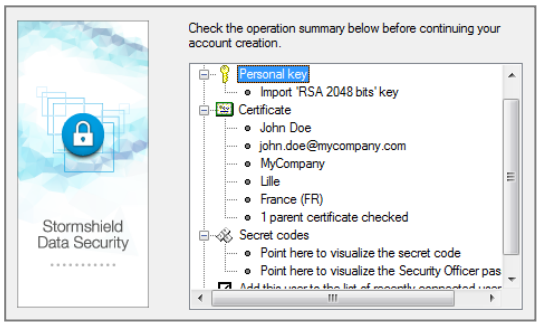
5. Validate by clicking on **Next**.
6. The wizard will then offer to create a backup password that will allow finding the password to the user account in the event it gets lost. You are strongly advised to create this backup password. Enter and confirm this password. Validate by clicking on **Next**:



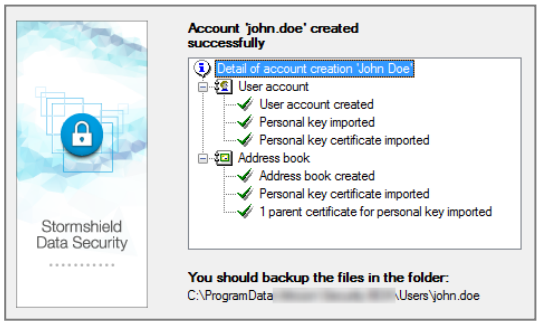
IMPORTANT

Without a backup password, the user's password cannot be retrieved if it is lost. You are therefore strongly advised to create a backup password.

7. When you see the screen providing a summary of the user account, confirm by clicking on **Finish**.



8. The creation of the local directory will be launched automatically and the last screen will give a summary of the operations performed:



9. Click on **Quit** to close the wizard.

Adding the firewall's directory in the SDS Suite address book.

Referencing an LDAP directory in the local address book makes it possible to indicate to SDS Suite that this directory must always be queried when sending or receiving e-mail.

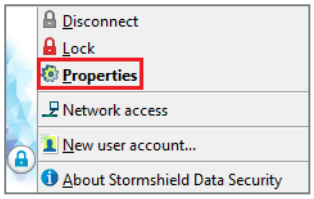
Connecting the user to SDS Suite

1. Right-click on the SDS Suite icon found in the taskbar and select the menu **Connect...**:

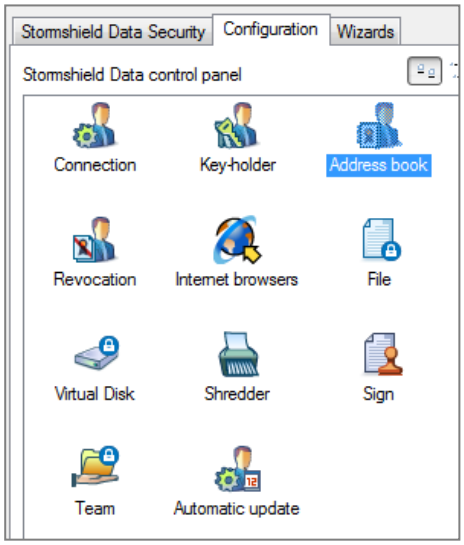
2. Enter the user's password and click on **Confirm**:

Adding the firewall's LDAP directory

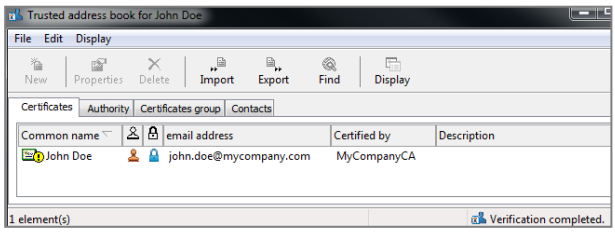
1. After logging on, right-click again on the SDS Suite icon found in the taskbar and select the menu **Properties**:



2. In the *Configuration* tab of the user properties window, double-click on the **Directory** icon:



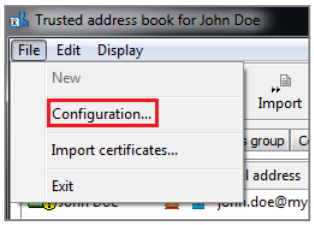
The contents of the user's local directory will be shown:



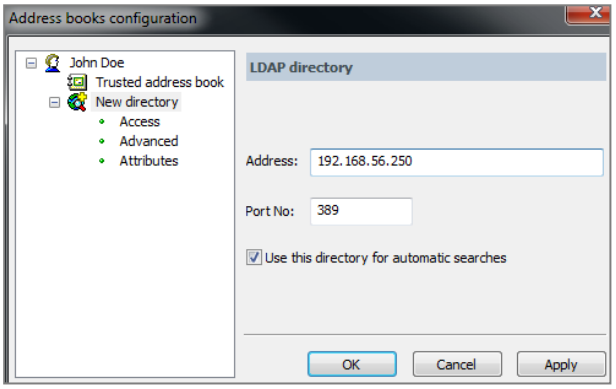
NOTE

In the example, the  symbol indicates that the listed certificate needs to be used carefully as the CRL could not be looked up.

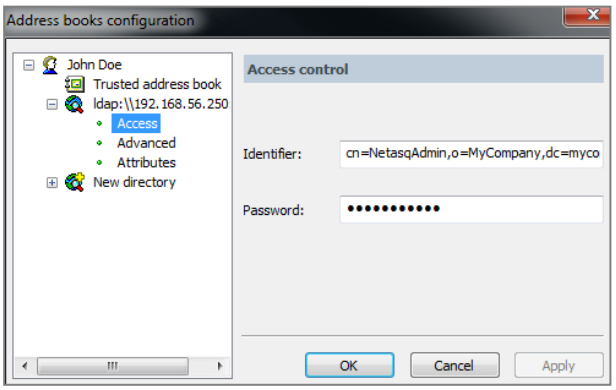
3. Expand the **File** menu and select **Configuration...** :



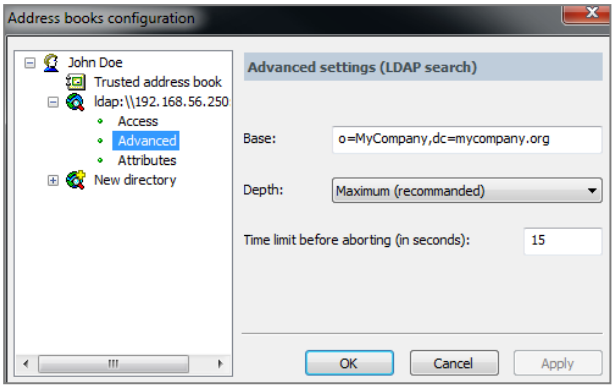
4. In the directory configuration window, click on **Add a directory** and enter the firewall's IP address (192.168.56.250 in the example) or DNS name (this name must then be entered in a DNS server that SDS Suite clients can contact). Leave the port entered by default (LDAP/389) and select **Use this directory for automatic searches**:



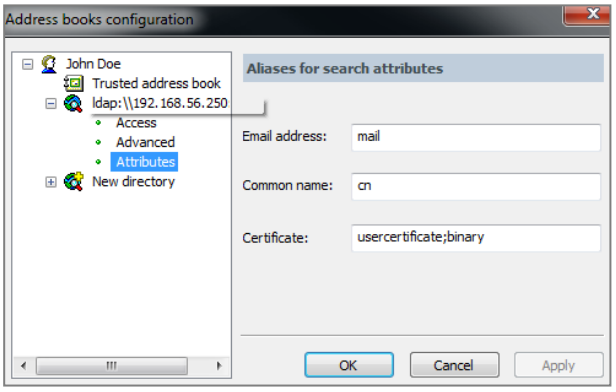
5. Click on **Apply**.
6. In the properties of the LDAP added, select **Access** and fill in both fields:
   - **Login**: Distinguished Name (DN) of the user allowed to browse the directory (NetasqAdmin). It will resemble the following: cn=NetasqAdmin, o=Organisation, dc=Domain (example : cn=NetasqAdmin,o=MyCompany,dc=mycompany.org)
   - **Password**: enter the password used during the creation of the LDAP directory on the firewall.



7. In the properties of the LDAP directory, select **Advanced** and fill in the **Base** field corresponding to the Base DN that stores certificates on the firewall. It will resemble the following: o=Organisation,dc=Domain (example: o=MyCompany,dc=mycompany.org).



8. In the properties of the LDAP directory, select **Attributes** and check that the fields contain the following values:
   - **Email address**: *mail*,
   - **Common name**: *cn*,
   - **Certificate**: *usercertificate;binary*.



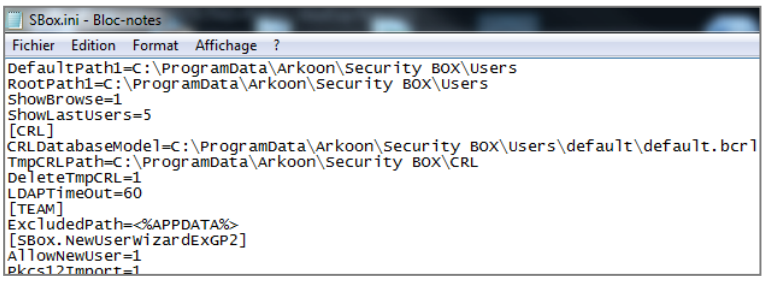
9. Click on **OK** to confirm the creation of the LDAP directory in the user's address book.

Adding certificates of e-mail peers automatically

It is possible to configure the LDAP directory in such a way that peer certificates contained in it are automatically added to the SDS Suite local directory when e-mails are sent to them.

To do so, the SDS Suite configuration file *sbox.ini* must be modified as follows:

1. Edit the *sbox.ini* file found in the Kernel folder of the SDS Suite installation path (C:\Program Files\Arkoon\Security BOX\Kernel\ in the example).



2. Create a [Mail] section, add a field "SilentImportTrustedLdapCert" and assign the value "1" to it:

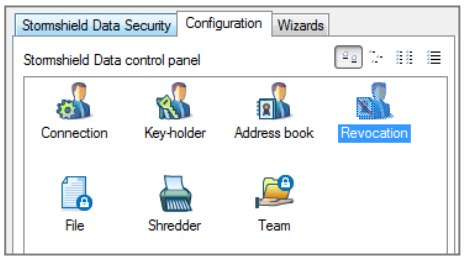
```
[SBox.NewUserWizardExKS1]
AllowNewUser=1
AllowNewUserCipher=1
AllowNewUserSign=1
Pkcs12Import=1
[SBox.NewUserWizardExKS2]
AllowNewUser=1
Pkcs12Import=1
[SBox.NewUserWizardExGP1]
AllowNewUser=1
AllowNewUserCipher=1
AllowNewUserSign=1
Pkcs12Import=1
InternalKeys=0
ExportKeys=1
KeepCardObjects=11
[Mail]
SilentImportTrustedLdapCert=1
```

3. Save the changes and close the file.

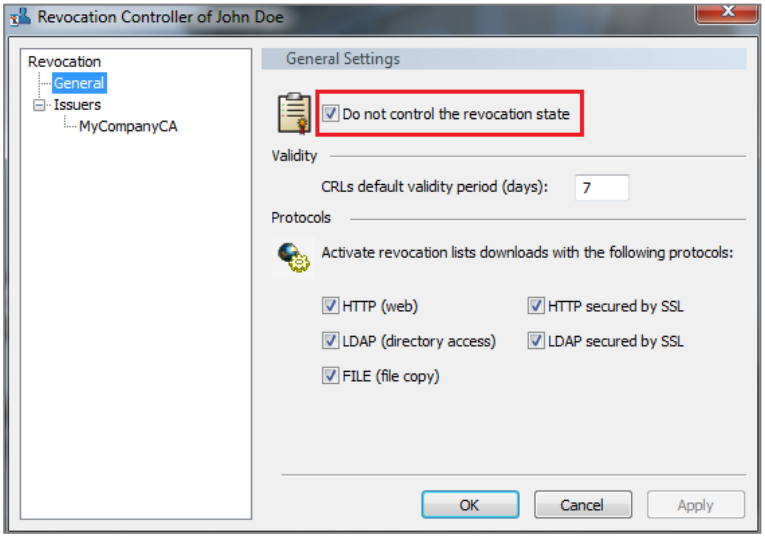
Enabling / Disabling certificate revocation control

When the version of the Stormshield Network firewall firmware hosting the CRL is lower than 2.4, certificate revocation control on the SDS client needs to be disabled.

1. Right-click on the SDS Suite icon found in the taskbar and select the menu **Properties**:
2. In the *Configuration* tab, double-click on the menu **Revocation**:



3. Select the checkbox "Do not control the revocation state" located in the **Revocation** > **General** menu. Apply and confirm:



NOTE
Remember to unselect this checkbox when the Stormshield Network firewall hosting the CRL has firmware in at least version 2.4.

Importing the firewall's certificate into the client workstation's trusted certificates

When the SDS Suite client performs an automatic check of the CRL status, it logs on in HTTPS to the CRLDP hosted on the SNS firewall, which is when the firewall's certificate will be presented. In order for this check to run smoothly, the firewall's certificate must therefore be imported into the Windows trusted certificate management console.

Retrieving the firewall's certificate

From Internet Explorer

1. In the browser's address bar, enter the address for connecting to the firewall's administration interface: **https://***firewall_ip_address*/**admin** or **https://***firewall_dns_name*/**admin.**

   REMINDER
   Choosing a URI that indicates the firewall's DNS name means that this name must be entered in an internal DNS server that can be accessed from SDS Suite clients.

2. When the firewall authentication page appears, click on the security report area located to the right of the browser's address bar.
3. In the security report window, click on **View certificates**.
4. In the *Details* tab, click on **Copy to a file...**
5. Click on **Next**,
6. Leave the suggested default format: **DER encoded binary X.509 (.CER)**, then click on **Next**.
7. Click on **Browse** to select a location to save the file, then enter a name for the file and click on **Save.**
8. Click on **Next** then on **Finish**.
9. Confirm the message "**The export was successful**".
10. Close the window showing details of the certificate by clicking on **OK.**

From Mozilla Firefox

1. In the browser's address bar, enter the address for connecting to the firewall's administration interface: **https://***firewall_ip_address*/**admin** or **https://***firewall_dns_name*/**admin.**

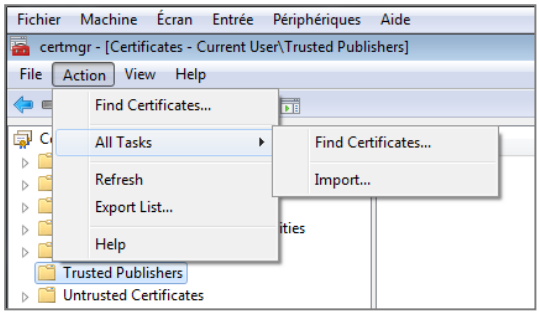
   REMINDER
   Choosing a URI that indicates the firewall's DNS name means that this name must be entered in an internal DNS server that can be accessed from SDS Suite clients.

2. When the firewall authentication page appears, click on the security report area (padlock) located to the left of the browser's address bar.
3. In the security report window, click on ">" then on the **More information** button.
4. Click on **View certificate**.
5. In the *Details* tab, click on **Export...**
6. Select a location to save the file, then enter a name for the file (leave the extension ".crt" suggested by default) and click on **Save.**

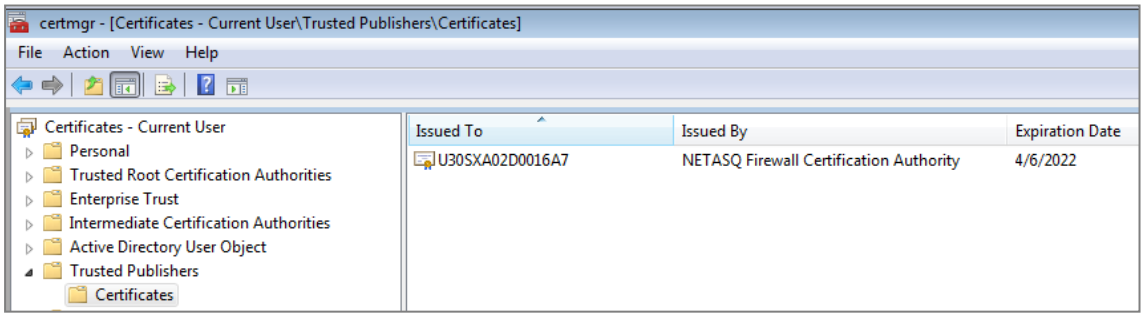
7. Close the window showing details of the certificate by clicking on **Close.**
8. Close the security report window using the button.

Importing this certificate into the client workstation's trusted certificate management console

1. In the Windows **Start** > **Run** menu, enter *certmgr.msc* then confirm by clicking on **OK** in order to run the certificate management console.
2. In the menu to the left of the console, select the store **Trusted Publishers** > **Certificates**.
3. Click on the **Action** > **All tasks** > **Import...** menu.



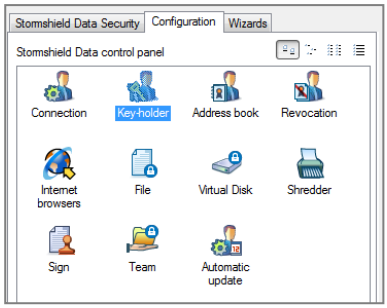
4. Select the firewall's certificate, exported earlier through your internet browser, then click on **Next**.
5. Confirm your choice of the certificate store (**Trusted Publishers**) by clicking on **Next.**
6. Confirm the import by clicking on **Finish**.
7. A message will confirm that the certificate was correctly imported. Your firewall's certificate will now appear in the store. It can be identified through your firewall's serial number (or its DNS name if it has one).



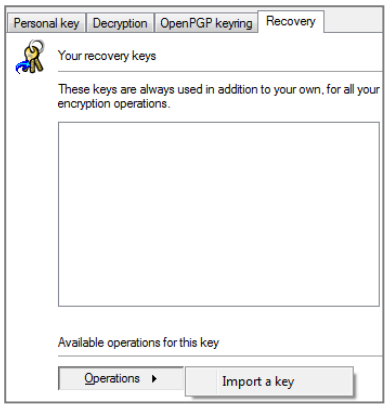
Importing the recovery key in SDS Suite

IMPORTANT
The recovery key must be imported into the SDS Suite client before any data is encrypted. Indeed, data encrypted before the installation of the recovery key may not be retrieved if the user loses his private key.

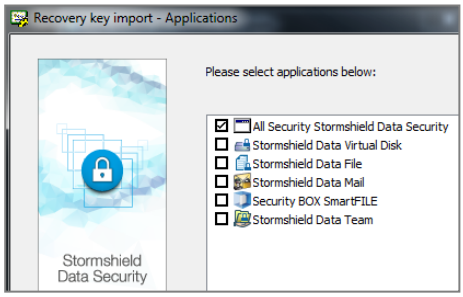
1. Right-click on the SDS Suite icon found in the taskbar and select the menu **Properties**:
2. In the *Configuration* tab, double-click on the menu **Keyring**.



3. Select the *Recovery* tab and click on **Import a key**.

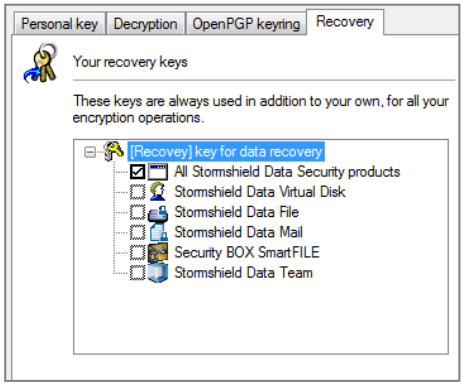


4. Select the recovery account's certificate.
5. Indicate the applications for which you wish to use this recovery key by selecting the checkbox **All Stormshield Data Security products**:



6. Click on **Finish** to confirm the operation.

The recovery key has now been declared for the SDS Suite user account:



Using the recovery account

In the event a user loses his private key, the recovery account may allows the user to decrypt his data.

Generating a new user certificate and its associated private key

Delete the previous user certificate and update the CRL (see Revoking a user certificate and updating the CRL).

In a configuration that does not use enrollment:

1. Generate a new certificate and its key.
2. Export the certificate and its key in PKCS#12 format (see Exporting a user's certificate and private key).

In a configuration that uses enrollment:

1. The user submits a new certificate request through the authentication portal (menu **Certificates** > **Request your certificate**, accessible after authentication on the portal).
2. The administrator will validate this request in the menu **User** > **Enrollment** (see Validating a user and certificate creation request).
3. The user will then retrieve his certificate and key from the authentication portal.
4. He will save them in PKCS#12 format and store this format in a secure location.

Creating a recovery user in SDS Suite

On the client workstation, follow the method described in the chapter Creating a new SDS user in order to create the recovery account in SDS Suite.

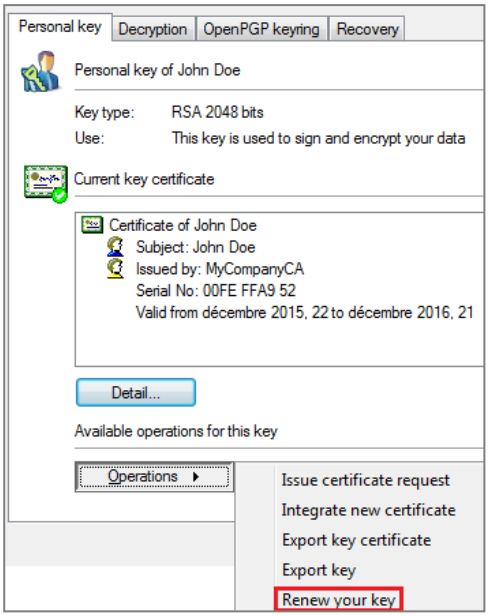
Decrypting the user's data using the recovery account

Logging on to SDS Suite using the recovery account will enable the manual decryption of the user's data.

NOTE
This decryption operation must be carried out with all the SDS Suite modules that the user had used to encrypt his data (File, Mail, etc).

Renewing the user's key

1. The user logs on to the SDS Suite client using his personal account.
2. In the *Personal key* tab in the **Keyring** menu of the SDS Suite client, expand the **Operations** menu and select **Renew your key**.



3. Next, select the option **Import your personal key**, select the PKCS#12 file containing the new user key and enter the password that protects the file.

Encrypting data using the recovery account

The user can now encrypt his data again.

NOTE
This encryption operation must be carried out with all the SDS Suite modules that the user had used to encrypt his data (File, Mail, etc).

Key life cycles

Recaps of general points

In this document, users' keys and certificates have a lifetime of two years where the certificate authority is defined for a period of 10 years. For security reasons, it is indeed not advisable to issue certificates with lifetimes equal to that of the CA that signed them.

Stormshield Network firewalls do not allow renewing expired certificates (the CA keeps the private key and its new signature by default): a new certificate associated with a new key must therefore be generated for the user.

NOTE
Since the recovery key was created with a lifetime of the same duration as the CA's by default (10 years in the example), this key will remain valid after the expiry of the user's certificate and does not require renewal in the SDS Suite client.

What should I do if a user certificate expires or is revoked?

Generating a new certificate and its associated private key

In a configuration that does not use enrollment:

1. Generate a new certificate and its key.
2. Export the certificate and its key in PKCS#12 format.

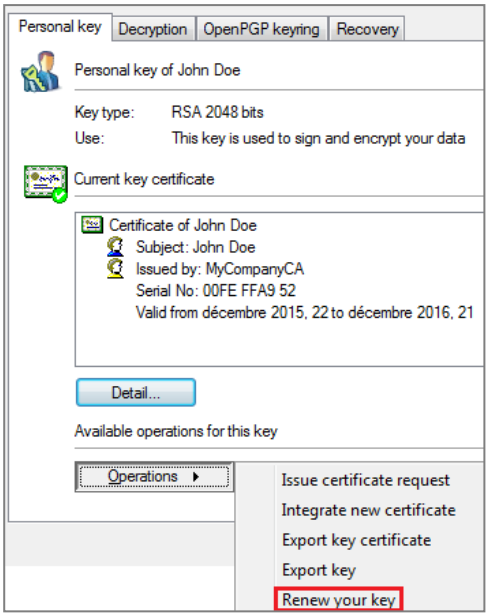
In a configuration that uses enrollment:

1. The user submits a new certificate request through the authentication portal (menu **Certificates** > **Request your certificate**, accessible after authentication on the portal).
2. The administrator will then validate this request in the menu **User > Enrollment**.
3. The user will retrieve his certificate and its key in PKCS#12 format.
4. He will save them in PKCS#12 format and store this format in a secure location.

Renewing the certificate and its private key in SDS Suite

Installing the new key

1. The user logs on to the SDS Suite client using his personal account.
2. In the *Personal key* tab in the **Keyring** menu of the SDS Suite client, expand the **Operations** menu and select **Renew your key**.



3. Next, select the option **Import your personal key**, select the PKCS#12 file containing the new key and enter the password that protects the file.

Transcrypting user data

After updating his key in SDS Suite, the user must:

1. Manually decrypt his data using each of the modules used: File, Mail, etc (SDS Suite automatically selects the former key, which will still be present).
2. Manually encrypt his data again using each of the modules concerned (SDS Suite will then automatically select the user's most recent key).

What should I do when the CA's expiry date approaches?

When the CA's expiry date approaches, you will need to anticipate its expiry by redefining a new trust chain and by updating all SDS Suite clients:

1. Create a new CA defined by default for users.
2. Generate user certificates defined by this new CA.
3. Import new certificates on SDS clients (see Renewing certificates and private keys in SDS Suite).
4. Transcrypt each user's data (see Renewing certificates and private keys in SDS Suite).

Configuring automatic backups of the firewall

This chapter describes how to configure automatic backups of the firewall in the Stormshield cloud. Automatically backing up a configuration makes it possible to restore the firewall's configuration partially or totally in the event of a wrong move or a disaster.

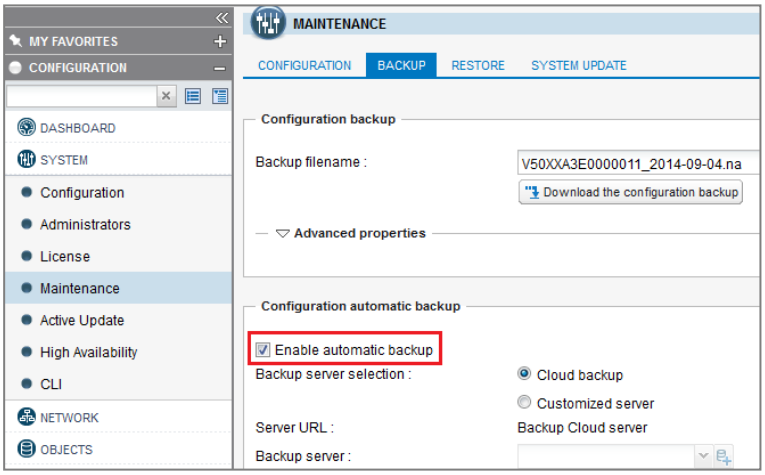
Do note that only the method recommended by Stormshield (without enrollment) will enable the restoration of users' private keys from an automatic backup of the firewall.

Automatically backing up the configuration of the firewall in the Stormshield cloud

The **Cloud backup** option allows sending backups of the firewall directly to your secure area (https://mystormshield.eu). The last 5 backups (daily, weekly or monthly) of your appliance will be stored and accessible in the same way.

Enabling automatic backups

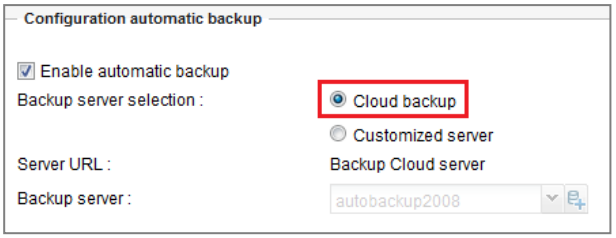
1. Select the *Backup* tab in the module **Configuration > System > Maintenance**.
2. In the *Automatic configuration backup* screen, select **Automatic Database Backup**.



Selecting Stormshield Network Cloud Backup

To enable automatic backups to the **Stormshield Network Cloud backup** service, select the value "Cloud backup" for the field **Backup server**. Backups will then be saved in your secure area (https://mystormshield.eu) and will be identifiable by the firewall's serial number. So for this feature, there is no need to enter a login and password in the **Preferences** module.

NOTE
The SN Cloud Backup feature can be found on all Stormshield Network firewalls. However, this service is only available to firewalls covered by a valid maintenance contract.



Only two complementary fields need to be entered:

- **Backup frequency**: select one of the three frequencies suggested (every day, every week or every month).
- **Backup file password (optional)**: enter a password that will be used for protecting this backup file. You will be asked for this password whenever you use this file to restore a configuration.

Automatically backing up the firewall configuration on a customized HTTP/HTTPS server

For further detail on the configuration of automatic backups from the firewall to a customized HTTP/HTTPS server, please refer to the Technical Note *Automatic Backups* available in your secure area.

documentation@stormshield.eu