HOW TO

STORMSHIELD ENDPOINT SECURITY

RENEWING THE SES ROOT CERTIFICATE AUTHORITY

Product concerned: SES

Date: June 07, 2019

Reference: ses-en-how_to_renew_the_root_certificate_authority

Table of contents

In the documentation, Stormshield Endpoint Security is referred to in its short form: SES.

Renewing the SES root certificate authority

This document applies to versions 7.2.26 of Stormshield Endpoint Security and above.

Digital certificates allow servers, consoles and agents in an SES pool to authenticate themselves during communications. All specific certificates for each component are issued by the same trusted root certificate authority.

The root certificate authority has an approximate lifetime of ten years, after which the certificate will be considered expired and components that use certificates issued by this root authority will not be able to communicate with one another. The trusted root certificate authority must therefore be renewed BEFORE its certificate expires.

In this document, we will explain the process of renewing this certificate and the various phases that need to be followed in order to ensure that components in the pool can continue to communicate.

Getting started

The certificate renewal process must take place in several stages spaced out over several months. It is important that you comply with the periods recommended by Stormshield to avoid overloading servers or disrupting agents' connections.

There are three phases to follow in this process:

Phase 1: Preparation	Six months before expiration (the administration console will indicate this when the configuration is deployed)	This phase aims to prepare SES servers for the renewal of the root authority so that they can prepare new certificates for agents by spreading out the task over six months. The length of this period also helps to ensure that agents that are usually offline would be able to retrieve their new certificates during this phase.
Phase 2: Deployment of the new root certificate authority	One month before expiration (the administration console will indicate this when the configuration is deployed)	During this phase, the new root authority takes effect and all components will use their new certificates. This phase must be launched as late as possible to ensure that most agents have retrieved their new certificates.
Phase 3: Purge of old certificates	Several months after the root authority has been changed (optional step)	This phase is to be conducted when all agents in the pool have logged on to the server and retrieved their certificates.

Phase 1- Preparation

About six months before the root authority's certificate expires, a new root authority must be generated in order to start issuing new agent certificates.

The new root authority must be generated on the main SES server:

1. Run the *gen_root.bat* SES file as an administrator. This file is located in the SES server's main folder (*C:\Program Files (x86)\Stormshield\Stormshield Endpoint Security Server* by default).

2. Move the mouse cursor to generate random numbers so that symmetric keys can be issued securely.
   Two files will be generated in the server's main folder:
   - *new_root.pem* (about 6 KB)
   - *new_rootcert.pem* (about 2 KB)

     Both of these files make up the new root authority.
3. If there are several servers in the pool, copy both of these files in the main folder of each server.

The servers in the pool will start generating new agent certificates and distributing them once the following conditions have been met:

- When the server has new root certificates
- When there are fewer than 182 days left before the root authority expires (six months)

The distribution of new certificates may increase the servers' load, so to avoid this issue, each server will generate only one new agent certificate at a time. If several agents simultaneously request updates for their certificates, only one request will be accepted. The other agents' requests will be denied, and they will have to resubmit their requests later.

After the phase 1 operations have been performed, the console message asking the user to follow the certificate renewal procedure will no longer appear during deployment in the environment.

Phase 2 - Deployment of the new root certificate authority

Ensure that you follow the recommendations below:

- This phase must not be conducted more than a month before the expiration of the root authority's certificate — if this operation is performed too early, communication between agents and servers will be disrupted until this period begins.
- As the replacement of certificates will increase the SES servers' load, you are advised to perform this operation during off-peak periods.
- This operation must be conducted on all servers in the pool at the same time.

Changing the root authority on all SES servers

To change the root authority:

1. Run the *switch_cert.bat* file as an administrator. This file is located in the SES server's main folder (*C:\Program Files (x86)\Stormshield\Stormshield Endpoint Security Server* by default).
2. The command file will request confirmation; type Yes to confirm. If anything else is typed, the command will be aborted.

Updating console certificates

WARNING
New console certificates must be imported for each console user.

Once the root authority has been changed, the console certificate must be generated from the new authority.

To do so:

1. Run the *gen_console.bat* file as an administrator. This file is located in the SES server's main folder (*C:\Program Files (x86)\Stormshield\Stormshield Endpoint Security Server* by default).
2. Follow the procedure; you will be asked to enter a new password twice. You are strongly advised against using non-ASCII characters in the password.
3. Once you have completed the procedure, retrieve the *new_console.sr12* file and copy it to the host on which the console is installed. If the console is on the server, there is no need to copy the file.
4. Open the console and import the new certificate through the **Configuration** > **Secure connections** menu.
5. Enter the password in the **Passphrase** field.

The certificate can then be deployed in the environment again.

Updating the key database

This operation needs to be performed only if file encryption, full disk encryption or removable device encryption is or was used in the pool.

As the key database uses the root authority to encrypt the data that it contains, its certificate must also be updated.

1. From a server, retrieve the files *old_root.pem* and *root.pem* located in the server's main folder (*C:\Program Files (x86)\Stormshield\Stormshield Endpoint Security Server* by default).
2. Run DBInstaller from a workstation on which a console has been installed.
3. Select the **Encryption key database maintenance** menu.
4. Enter the login credentials for the instance on which the key database has been installed (srkey).
5. Select the option **Change certificate authority**.
6. Move the *old_root.pem* file to **Old value**.
7. Move the *root.pem* file to **New value**.

Reconnecting agents

Agents that have already retrieved certificates issued by the new authority will automatically switch to the new certificate the next time they log on to the server.

Servers will experience discernibly heavier traffic as each agent will attempt to log on for the first time using its old certificate, the connection will be denied, and the agent will set up a new connection using the new certificate.

If an agent fails to obtain its new certificate during phase 1, it will retrieve a new certificate from the SES certificate server in the same way that a newly installed agent will retrieve its certificate.

> WARNING
> The process of retrieving certificates through the SES certificate server will consume a great amount of server resources and only one certificate can be generated at a time. If there are many agents in this situation, connection errors may arise as the certificate server will deny simultaneous certificate requests. The agent will regularly attempt this operation several times until it retrieves a certificate that would allow it to communicate with its server.

After the phase 2 operations have been performed, the console message asking the user to follow the certificate renewal procedure will no longer appear during deployment in the environment.

Phase 3 - Purge of old certificates

This phase must not be conducted as long as there are still agents that have not retrieved a new certificate. Any communication between servers and isolated agents that have not been updated will be cut off without the possibility of backtracking, which will involve manual operations including the shutdown of affected agents.

This phase makes it possible to delete old root certificates from the servers in the pool.

To do so:

1. Run the *cleanup_cert.bat* file as an administrator. This file is located in the SES server's main folder (*C:\Program Files (x86)\Stormshield\Stormshield Endpoint Security Server* by default).
2. The command file will request confirmation; type Yes to confirm. If anything else is typed, the command will be aborted.

Purging certificates will permanently delete all traces of previous certificates.

documentation@stormshield.eu