STORMSHIELD

GUIDE
STORMSHIELD ENDPOINT SECURITY EVOLUTION

SAAS DEPLOYMENT GUIDE
Version 2.6.2

Table of contents

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

1. Getting started

Welcome to the Stormshield Endpoint Security Evolution SaaS deployment guide.

This document contains technical information specific to the SaaS version of the product, and is aimed at Managed Security Service Providers (MSSPs).

The SES Evolution security solution offers organizations of all sizes comprehensive protection for user workstations and servers. Installed on your customers' workstations and servers, the SES Evolution agent protects them from known and unknown attacks, as well as intrusions, in a transparent manner for users.

As an MSSP, you configure the agent from an administration console, and you to manage the SES Evolution backoffice for each of your customers.

In the administration console, you can configure security policies and also read event logs generated by workstations and servers in order to monitor their operation.

SES Evolution also has a public REST API. It is not enabled by default. For more information on the public API, refer to the section Enabling and managing SES Evolution's public API.

2. Understanding the architecture

The diagram below shows the main connections between the various components of the SES Evolution architecture in SaaS mode:

- Stormshield manages and controls SES Evolution backoffices for end customers. The set of backoffice components dedicated to a customer is called a *tenant*. Our *Cloud Services* department administers machines through specific accounts.

- The MSSP has a workstation on which the SES Evolution administration console is installed. From this workstation, he/she connects separately to each customer's tenant to carry out the day-to-day tasks of administering and monitoring the SES Evolution solution.

- Each customer retrieves their own logs and SES Evolution security policy. Optionally, they can use an administration console to log into their own tenant.

All the flows below use TCP port 443.
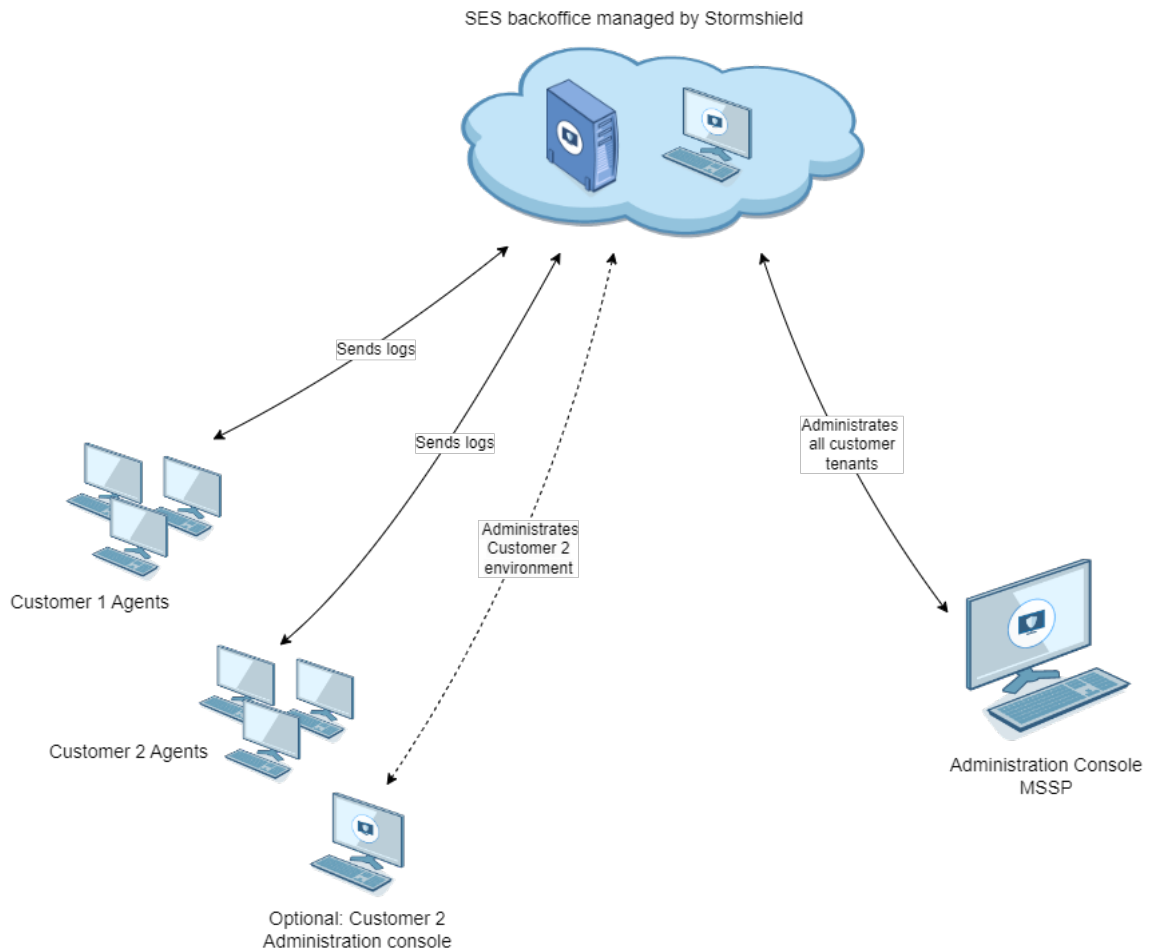
3. Configuring SES Evolution to manage multiple tenants

As the MSSP, you are responsible for administering and monitoring the SES Evolution agent pool for several customers. From a single workstation, you can connect to any of the customer's tenants via the SES Evolution administration console. To do this, you need to create local accounts on your workstation, then install the administration console for an initial tenant, and finally declare the console for additional tenants.

3.1 Requirements

For each of the tenants you administer, you must have the following elements sent by e-mail by Stormshield:

- The login and password of the account(s) created by Stormshield for your tenants,
- The public DNS name of the SES Evolution backend for your tenants,
- The URL of the Stormshield authentication portal where you can log in to access your tenants.

3.2 Creating local accounts

1. In your infrastructure, on the workstation on which you wish to install the SES Evolution administration console, create local accounts corresponding to those transmitted by Stormshield. Use the password and password policy sent by Stormshield.
   There are two possible account types. The account names below are examples:
   - *Admin*: Used to run the SES Evolution Installation Center and declare new instances of the administration console. There is only one *Admin* account for all your tenants.
   - *Firstname.Lastname* (optional): Used to run the administration console to perform day-to-day pool administration tasks. There are as many *Firstname.Lastname* accounts as there are console administrators.

   If you have a single account (*Admin*), this latter will be used for both console installation and daily tasks. However, Stormshield recommends using a *Firstname.Lastname* account for each SES Evolution administrator.

2. Add the *Admin* account to the local system administrators using the `lusrmgr.msc` command or the following command line:

```
$BuiltinUsersSid =
[System.Security.Principal.SecurityIdentifier]::new
([System.Security.Principal.WellKnownSidType]::BuiltinUsersSid,
$null)

$BuiltinAdminsSid =
[System.Security.Principal.SecurityIdentifier]::new
([System.Security.Principal.WellKnownSidType]::BuiltinAdministrato
rsSid, $null)


New-LocalUser -UserMayNotChangePassword -AccountNeverExpires -
PasswordNeverExpires -Name "Admin" -Description "Admin Console" -
FullName "Admin" -Password (Read-Host -AsSecureString)

# (enter Admin password here)

Add-LocalGroupMember -Sid $BuiltinUsersSid -Member Admin

Add-LocalGroupMember -Sid $BuiltinAdminsSid -Member Admin
```

3.3 Installing the administration console for the first tenant

1. On the same workstation, run *SES_Evolution_Installation_Center_vxxx.exe* as user *Admin*.
   - or -
   If the workstation is on a domain, run the following command:
   `SES_Evolution_Installation_Center_vxxx.exe -NoDomainCheck`.

2. Select **Add a new component to an existing installation**, then **Console**.

3. Enter the DNS name of the backend provided by Stormshield.
   The console is installed and a shortcut created on the public Windows Desktop.

4. Open the console as *Admin* to ensure correct connection to the backend.

5. In the **Users > Users and groups** panel, ensure that your *Firstname.Lastname* accounts for this tenant are declared and have been assigned a role.

6. Rename the shortcut on the Windows Desktop to identify this first tenant.

Throughout the remainder of this document, we refer to customer 1's environment as the primary environment.

3.4 Declaring the administration console for additional tenants

1. On the same workstation, launch a command prompt as the *Admin* user and run the following command:
   ```
   EsInstaller.exe -NoDomainCheck -RegisterConsole -BackendAddress
   <Tenant2_Backend_DNS_Name> -ShortcutPath
   "C:\Users\Public\Desktop\SES Evolution Console - Tenant2.lnk".
   ```

   where:

Parameter	Description
-NoDomainCheck	Use only if the machine belongs to an Active Directory domain.
-RegisterConsole	Registers a new console linked to another SES Evolution backend.
-BackendAddress	Specifies the public DNS name of the additional tenant's backend.
-ShortcutPath	Indicates the path and name of the shortcut on the public Windows Desktop.

   After about ten seconds, a new console shortcut appears on the public Windows Desktop. If not, check the installation center logs in *AppData/Local/Temp*, or the backend logs on the second tenant. For more information, see the *Administration guide*.

2. Using the new shortcut, open the console as *Admin* to ensure correct connection to the backend.

3. In the **Users > Users and groups** panel, ensure that your *Firstname.Lastname* accounts for this tenant are declared and have been assigned a role.

4. Repeat this procedure for any additional tenants you wish to administer.

5. (Optional) After this procedure, Stormshield recommends you disable the *Admin* account, so as not to leave any privileged accounts unused on your workstation. You can re-enable it if you need to install a console for a new tenant.

Throughout the remainder of this document, we refer to additional customer environments as secondary environments.

3.5 Knowing best practices

- If you add or delete users in the SES Evolution administration console, inform the Stormshield Cloud Services team so that they can also be added or deleted on the tenant.

- Do not change the password of local Windows accounts used to log into SES Evolution without first informing the Stormshield Cloud Services team. Indeed, the password must also be changed on the tenant.

- Before deploying changes to a customer's pool, make sure you do so from the administration console linked to the customer's tenant.

3.6 Using the administration console

Use of the administration console is described in detail in the *Administration guide*.

3.7 Updating the administration console

When you receive the notification, update the SES Evolution administration console as follows in order to synchronize its version with the backend:

- Start the **primary environment** console.
  It will be updated automatically, and will also allow secondary environments to function properly.

3.8 Uninstalling the administration console

To uninstall the administration console when it is configured with multiple tenants, open a ticket with Stormshield technical support, which will guide you through the process.

4. Further reading

Additional information and answers to questions you may have about SES Evolution are available on the Documentation website and in the Stormshield knowledge base (authentication required).

STORMSHIELD

documentation@stormshield.eu

All images in this document are for representational purposes only, actual products may differ.

Copyright © Stormshield 2024. All rights reserved. All other company and product names contained in this document are trademarks or registered trademarks of their respective companies.