



STORMSHIELD



HOW TO

STORMSHIELD ENDPOINT SECURITY

APPLYING A SECURITY POLICY TO YOUR ACTIVE DIRECTORY

Product concerned: SES

Date: November 29, 2018

Reference: [ses-en-how_to_apply_a_security_policy_to_your_AD](#)



Table of contents

How to apply a security policy to your Active Directory	3
How to import Active Directory groups into the Environment Manager	3
How policy priority works	3
How to apply a policy	4
How to change a policy	5

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



How to apply a security policy to your Active Directory



This document applies to versions 7.2 and higher of Stormshield Endpoint Security.

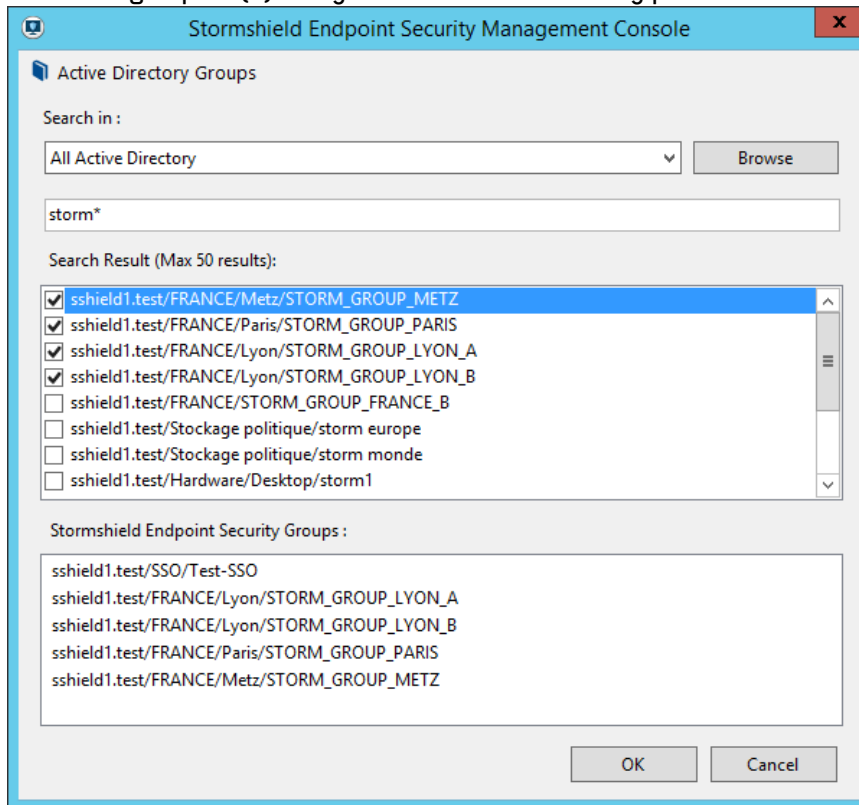
Warning

You must specify to use Active Directory during SES installation, otherwise this procedure is not possible.

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

How to import Active Directory groups into the Environment Manager

1. From the SES Management Console, in the second pane of the Environment Manager, click on  to toggle to see the computers.
2. Click on  to search the Active Directory.
3. Enter the first letters of the group/Organizational Units(s) you want, followed by an asterisk, in the search field, and click on Enter.
4. Select the group/OU(s) that you wish to link to security policies. Click on **OK**.



How policy priority works

In **Environment Manager**, you can apply security policies to each item of the environment.

Policies are prioritized in a bottom up fashion (computer policy takes priority over group which takes priority over OU, etc.).



The hierarchy can be seen clearly if you click on the computer in question. In the following example, the active policies are applied directly to the C3 computer (indicated by white background), so the inherited policies are not applied (indicated by crossed out text).

The screenshot shows the Stormshield Environment Manager interface. On the left, the 'Environment' tree is expanded, showing the hierarchy: Environment > Active Directory > sshield2.test > Kuala Lumpur > R&D > C3-W7-32-ATH-20. The 'C3-W7-32-ATH-20' computer is selected, and its details are shown on the right. The 'Policies linked' tab is active, showing a list of policies linked to the computer. The policies are categorized into Dynamic Agent Configuration, Static Agent Configuration, Security, and Encryption. The 'Security' category shows four links: 1. NewPreprodSecu, 2. PreProdSecu, 3. quarantine, and 4. DefaultSecurityPolicy. The 'quarantine' policy is highlighted with a red box, and a red line connects it to the 'quarantine_file' condition in the 'Security' list. The 'DefaultSecurityPolicy' is also highlighted with a red box, and a red line connects it to the 'DefaultSecurityPolicy' condition in the 'Security' list. The 'Encryption' category shows 0 links.

Link order	Condition	Policy Name	Inherited from
1	(true)	DefaultDynamicAgentPolicy	Environment

Link order	Condition	Policy Name	Inherited from
1	(true)	DefaultStaticAgentPolicy	Environment

Link order	Condition	Policy Name	Inherited from
1	(true)	NewPreprodSecu	
2	(true)	PreProdSecu	R&D
3	quarantine_file	quarantine	Kuala Lumpur
4	(true)	DefaultSecurityPolicy	Environment

Link order	Condition	Policy Name	Inherited from
1	(true)	DefaultSecurityPolicy	Environment

- Moving a computer with policies that are directly linked (not inherited - white background) into a new OU does not change the active policy. You can remove policies that are directly linked by selecting the active policy and **Remove**.
- Moving a computer with an inherited policy into a new OU automatically changes the inherited security policy to the new OU (and loses the previous one).
- Groups are slightly different because they do not inherit a policy.
 - They can be 'invisible' with no policy: members are linked to the OU policy above them.
 - They can be directly linked to a policy: members are linked to this groups policy (unless they also have a directly linked policy).

Groups can be useful to override (or not) the OU policy for several computers (more easily visible and reproducible than applying separate policies to individual computers).

How to apply a policy

In **Environment Manager**, select the item on which you want to apply the policy. Choose the **Policy name** and the **Condition** under which it will apply.

The screenshot shows the Stormshield Environment Manager interface. On the left, the 'Environment' tree is expanded, showing the hierarchy: Environment > Active Directory > enfant1.sshield1.test > sshield1.test > sshield2.test. The 'sshield2.test' computer is selected, and its details are shown on the right. The 'Policies linked' tab is active, showing a list of policies linked to the computer. The policies are categorized into Dynamic Agent Configuration, Static Agent Configuration, Security, and Encryption. The 'Security' category shows two links: 1. quarantine_file and 2. (true). The 'quarantine_file' policy is highlighted with a blue box, and a blue line connects it to the 'quarantine' condition in the 'Security' list. The '(true)' policy is also highlighted with a blue box, and a blue line connects it to the 'DefaultSecurityPolicy' condition in the 'Security' list. The 'Encryption' category shows 0 links.

Link order	Condition	Policy Name	Inherited from
1	(true)	DefaultStaticAgentPolicy	Environment

Link order	Condition	Policy Name	Inherited from
1	quarantine_file	quarantine	
2	(true)	DefaultSecurityPolicy	Environment

Link order	Condition	Policy Name	Inherited from
1	(true)	DefaultSecurityPolicy	Environment



How to change a policy

A computer with inherited policies needs to be moved to the new OU using Active Directory. The SES policy change is then automatic.

A computer (or group) with directly applied policies can be modified in the **Policies linked** tab.

Click on the arrow ▼ and choose the policy and condition that apply, or Add a new one, or

Remove using + Add ✕ Remove.

You could have 2 active policies: one for when the machine is connected, and a different one for when it is disconnected.

Security - 3 link(s)			
+ Add - Remove ↕ ↑ ↓ ↕			
Link order	Condition	Policy Name	Inherited from
1	(connected) ▼	testpolicy ▼	
2	(disconnected) ▼	DefaultSecurityPolicy ▼	



STORMSHIELD

documentation@stormshield.eu

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

Copyright SkyRecon Systems 2018. All rights reserved. All other company and product names contained in this document are trademarks or registered trademarks of their respective companies.