

STORMSHIELD



OVA DEPLOYMENT GUIDE Version 2

Document last updated: July 25, 2024 Reference: sls-en-deployment guide ova



Table of contents

Change log	3
Getting started	4
Requirements	5
Deploying SLS OVA Selecting an OVA Selecting a Name and Folder Selecting a Computing Resource Reviewing the Template Details Selecting Storage Selecting Networks Wrapping up the Configuration	6 7 8 8 9 9
Activating SLS 1 Accessing the SLS user interface 2 Getting the SLS Hardware Key 2 Registering the SLS product 2 Downloading the SLS license (.pak file) 2 Installing the license 2 Changing the "admin" user password 2 Updating SLS to the latest patch 2	LO 10 10 11 11 12 13
Getting logs from an SNS firewall Adding a new device on SLS Configuring logs retrieval Getting the logs through standard Syslog Getting the logs through Syslog-TLS	L4 14 15 15 15
Getting logs from SES Evolution Adding a new device on SLS Configuring logs retrieval Getting the logs through standard Syslog Getting the logs through Syslog-TLS	L8 18 19 19 20
Getting logs from external sources 2 Downloading the external sources archive on MyStormshield 2 Adding an external source application on SLS 2 Further reading 2	22 22 22 22





Change log

Date	Description
July 25, 2024	New section for External Sources support
July 4, 2024	New document





Getting started

Welcome to the Stormshield Log Supervisor OVA version 2 Deployment Guide.

This guide discusses the steps and considerations for deploying the SLS OVA on the VMWare ESXi server.

With the SLS OVA, you can use:

- Virtualization to transform data centers into simplified cloud computing infrastructures and use flexible and reliable IT services. VMware vSphere virtualizes and aggregates the underlying physical hardware resources across multiple systems and provides pools of virtual resources to the data center.
- Managed Infrastructure to utilize large collections of infrastructures such as CPUs, storage, and networking as a seamless and dynamic operating environment without worrying about the complexity of a data center.

For a better assessment of this guide, we expect you to have a basic understanding of the VMware vSphere and its core services.

In the documentation, Stormshield Log Supervisor is referred to in its short form SLS, Stormshield Network Security in its short form SNS, and Stormshield Endpoint Security Evolution in its short form SES Evolution.

🕒 IMPORTANT

This document covers only SLS version 2 deployments.





Requirements

Compatibility

For more information about the SLS Life Cycle management policy and compatibilities, refer to the **Product life cycle Log Supervisor** guide.

Minimum recommended specifications

- CPU: Quad-core
- RAM: 7GB
- Disk space: 169GB

1 NOTES

- These recommended specifications <u>only apply</u> to launch SLS on a new installation. If you are updating your SLS, these recommended specifications <u>may not apply</u>. For updating your SLS, please refer to the <u>Update Guide</u>.
- The chosen specifications must be consistent with the infrastructure in which SLS will be deployed and the amount of sources and logs that SLS will manage.



Deploying SLS OVA

Selecting an OVA

- Download the provided SLS .ova file from your MyStormshield personal area, in Downloads
 > Downloads > Stormshield Log Supervisor > Firmware.
- 2. Log in to your vSphere client.
- 3. Click the Host and Cluster icon.
- 4. Select the required resource pool to install the OVA.
- 5. Right-click the required resource pool and click Deploy OVF Template.



- 6. Select the Local file option.
- 7. Click Choose files, browse the OVA file and click Next.

%) C	eploy OVF Template	(?) H
1	Select template	Select template Select an OVF template.	
2	Select name and location		
3	Select a resource	Enter a URL to download and install the OVF package from the Internet, or browse to a location accession from your computer such as a local hard drive a network share or a CD/D/D drive.	ible
4	Review details	initia your computer, such as a local hard drive, a network share, or a CD/DVD drive.	
5	Select storage	○ URL	
6	Ready to complete		
		Local file	
		Browse 1 file(s) selected, click Next to validate	
		A Use multiple selection to select all the files associated with an OVF template (.ovf, .vmdk, etc.)	
		Back Next Finish Cance	а),





Selecting a Name and Folder

- 1. Enter a Virtual machine name.
- 2. Select a target location for the virtual machine and click Next.

8	D	eploy OVF Template		? Þ
~	1	Select template	Select name and location Enter a name for the OVF and select a deployment location	
	2	Select name and location		
	3	Select a resource	Name SLS	
	4	Review details	Filter Browse	
	5	Select storage	Select a datacenter or folder.	
	6	Ready to complete	SLS-Server	
			Back Next Finish	Cancel

Selecting a Computing Resource

1. Select the destination resource for the virtual machine and click Next.

Deploy OVF Template		? H
1 Select template 2 Select name and location	Select a resource Select where to run the deployed template.	
3 Select a resource	Filter Browse	
4 Review details	Select a host or cluster or resource pool or vapp.	
5 Select storage	a B Transform	
6 Ready to complete	C SLS-Server	
	Back Next Finish	Cancel





Reviewing the Template Details

1. Review the details of the OVA and click Next.

8	Deploy OVF Template (?)		
* *	1 Select template 2 Select name and location	Review details Verify the template	e details.
~	3 Select a resource	Product	Stormshield Log Supervisor
	4 Review details	Version	1.0.0
	5 Select storage	Publisher	② No certificate present
	6 Select networks	Download size	Unknown
	7 Ready to complete	Size on disk	Unknown (thin provisioned) 100.0 GB (thick provisioned)
			Back Next Finish Cancel

Selecting Storage

- 1. Select the virtual disk format:
 - Select the **Eager Zeroed Thick Provision** format to allocate the storage and clear all the data inside the disk array immediately.
 - Select the Lazy Zeroed Thick Provision format to allocate the storage immediately, and clear all the data of the disk array only on demand.
 - Select the **Thin Provision** format to allocate the storage and clear the data of the disk array only on demand.
- 2. Select a VM Storage Policy from the drop-down menu.
- 3. Select a datastore to deploy the virtual machine and click Next.

()			
Select template Select storage Select location to store the files for the deployed template.			
elect virtual disk format. Thin provision			
Show datastores from Storage DRS clusters 🚯			
Filter Datastores Datastore Clusters			
🕒 🌾 📑 (Q Filter 🗸			
Name Status VM storage policy Capacity Free			
C (2 menute strate stra			
C 2 united ap 82 mon 8 tons - 1 19 40 7 18			
C C anticità aj Al Journ A A tornal - 1 Th Hold CA			
C (2) carfred big AL shore A (4) former - (4.16) (37.16.0)			
■			
M 16 Objects 🕒 Copy 🗸			
H 16 Objects Back Next Finish			





Selecting Networks

 On the IP Allocation Settings section, select the IP allocation option for the virtual machine and click Next. If IP addresses are not distributed via a DHCP server, you must set the IP address while accessing the SLS instance. For more information, refer to Accessing the SLS user interface.

🍘 Deploy OVF Template	Deploy OVF Template		
 1 Select template 2 Select name and location 	Select networks Select a destination network t	or each source network.	
✓ 3 Select a resource	Source Network	Destination Network	
✓ 4 Review details			
✓ 5 Select storage			
6 Select networks			
7 Ready to complete			
	IP Allocation Settings		
	IP protocol: IPv4	IP allocation: DHCP 🔹 🗊	
		Back Next Finish Cance	

Wrapping up the Configuration

- 1. **Review** the configuration before creating a virtual machine. Click **Back** before finalizing the configuration if necessary.
- 2. Click **Finish** to create the virtual machine.

🍘 Deploy OVF Template	Deploy OVF Template (?)		
 1 Select template 2 Select name and location 	Ready to complete Review configuration data.		
✓ 3 Select a resource	Name	Stormshield Log Supervisor	
4 Review details	Source VM name	Stormshield Log Supervisor	
6 Select networks	Download size	Unknown	
 7 Ready to complete 	Size on disk Folder	CI & Source	
	Resource	SLS-Server	
	 Storage mapping 	1	
	Network mapping	0	
	 IP allocation settings 	IPv4, DHCP	
		Back Next Finish Cancel	



Activating SLS

Accessing the SLS user interface

- 1. Select the required virtual machine and go to Actions >> Power >> Power On.
- 2. Note down its IP address. If it is not displayed, see the instructions below.
- 3. Enter the IP address in a web browser (example: https://10.45.3.95).
- 4. Log in to the SLS user interface. The default credentials are *admin* (username) and *changeme* (password).

If you need to get or set the IP address of the SLS instance:

- 1. Open a VM Console. The default credentials are *li-admin* (username) and *changeme* (password).
- 2. Retrieve the IP address by using the "ip a" command. Define the IP address by using the "change-ip" command, then the "systemctl reboot" command.

Getting the SLS Hardware Key

Once connected to the SLS user interface for the first time, it is requested to activate SLS with a license provided by Stormshield, which contains the details of the purchased product, the number of sources it can handle, and the license's expiration date.

The license refers to the Hardware Key of the solution, which is unique. You can find it here:

×,	System Settings / Licenses					
ø	Licenses	Hardware Key: XXXX-XXXX-XXXX-XXXX	xx-xxxxx-xxxxx-xx	••••••••••••••••••••••••••••••••••••••	Upload License	
Ø	i Trial Version					×
Q	Please be aware that your	system is running on a trial version with limited ac	ccess to features.			
٩	License Overview					
B						
¢	Licenses		Allocated	Remaining	Days Remaining	
	SIEM Data Sources		5	3	15	

Registering the SLS product

You must contact your Stormshield reseller or partner to obtain an SLS product. Then, register it in your MyStormshield personal area. You will be prompted to enter your SLS Hardware Key and SLS Serial Number. For more information, refer to the **Registering products** guide.





Downloading the SLS license (.pak file)

Download the license (*.pak* file) from your **MyStormshield** personal area. For more information, refer to the **Downloading a product's license file** page.

Installing the license

1. On SLS, go to 🕸 Settings >> System Settings in the navigation bar on the left and click License.

(Z)	System				
ø	Ch	r		17	
⊘	System Monitor	System Settings	Licenses	Updates	
ø					
٩	Open Door	Backup and Resore	Plugins	B Sync	
B					
\$	User Accounts				
	Configuration				
1	Knowledge Base				
	System Settings				

2. Click Upload License > SIEM.



- 3. Browse to the file containing the License Key.
- 4. Go through the END USER LICENSE AGREEMENT (EULA).



5. Click Submit if you agree with the terms and conditions of the EULA.

R)	System Settings / Licenses	New SIEM License
0	Licenses	Hardware key:
Ø	i) Trial Version	X000X-X0XX-X00XX-X0XXX-X0XXX-X0XXX-X0XXX
Q	Please be aware that your system is running on a trial version with lin	* License File:
۹	License Overview	Select License File to import Browse
E		EULA:
\$	Licenses	END USER LICENSE AGREEMENT (EULA)
	SIEM Data Sources	IF YOU OBTAIN A LICENSE TO USE OUR PRODUCTS OR SERVICES (THE "PRODUCTS") THEN IN ADDITION TO THE PROVISIONS OF THE "STORMSHIELD GENERAL TERMS OF SERVICE", THESE ADDITIONAL TERMS WILL APPLY TO YOUR USE OF THE PRODUCT. IF THERE ARE ANY
	SIEM License	DISCREPANCIES BETWEEN THE "STORMSHIELD GENERAL TERMS" AND THESE ADDITIONAL TERMS, THESE ADDITIONAL TERMS WILL PREVAIL.
	License Details Company information	The terms of the End User License Agreement
	Customer: Stormshield	This End User License Agreement (the "Agreement") is an agreement between the person, company or organization (the "Licensee") that has obtained a license for the PRODUCTS and Stormshield (the "Licenser") Bu installing and/or using the PRODUCTS the Licensee accents the license accents the license acting
	No. Of Sources: 5	PRODUCTS and agrees to the terms of this Agreement. The terms of the Agreement will govern new and/
	Validity Period: 2024/06/11 To 2024/07/10	or updated versions of the PRODUC Is installed according to the Licensor's instructions or in connection with an error correction.
C	Uploaded on: 2024/06/11 16:17:10	DEFINITIONS
Q •	Uploaded by: Stormshield	"Confidential Information" shall mean the PRODUCTS, all Documentation, all information data, \checkmark
0		I accept the terms of the End User License Agreement EULA
8		
Ξ		Cancel Submit

Changing the "admin" user password

For security reasons, you must change the default password of the "admin" user.

- 1. Go to \mathcal{R} User >> My Preferences in the navigation bar on the left.
- 2. In the Account tab, enter changeme in the Current Password field.
- 3. Enter the new password and confirm it.
- 4. Click Change Password.

	Change Password	Date Format: 2024/06/27 V
	Current Password: password	Time Format:
	New Password: password Retype New Password:	Current User Time: 09:06:31
Q	password	API Access Key
Q •	Change Password	Access Key:
0	My Preferences	C O
8	Logout	







Updating SLS to the latest patch

1. Identify the current SLS version installed. On SLS, click on O Help > About SLS in the navigation bar on the left and look for the version number.

SLS 2.■.	
This product is created by Logpoint for Stormshield	

2. Check the version release notes to see if a newer SLS version is available. If so, refer to the Update Guide to install it.





Getting logs from an SNS firewall

Adding a new device on SLS

1. On SLS, go to 🕸 Settings >> Configuration >> Devices and click Add.

(Z)	é B	АСК	Devices			
	0	ADD	🕄 ADD BULK DEVICES 🛛 🛓 IMF	PORT 🕘 JOBS		
0		S.N.	Name	Addresses	Device Groups	Log Collection Policies
Ø		1	E16-000	10.00.001		stormshield
ø		2	And the second	10.01		stormshield
٩		3	localhost	127.0.0.1,::1	linux	
B						
愈						

- 2. Enter the Name of the device.
- 3. In the IP address(es) field, enter the IP address of the SNS firewall.
- 4. In the Log Collection Policy field, select stormshield.
- 5. Choose the correct **Time Zone**.
- 6. Click Submit.

CREATE DEVICE		00
DEVICE INFORMATION -		
Name:	Alpha	
Device Address(es):	The second secon	
Device Groups:		
Log Collection Policy:	stormshield ×	
Distributed Collector:		
Time Zone:	(GMT+01:00) Brussels, Copenhagen, Madrid, Paris	Ŧ
RISK VALUES		
Confidentiality:	Minimal	Ŧ
Integrity:	Minimal	Ŧ
Availability:	Minimal	Ŧ
	Submit	Cancel



Configuring logs retrieval

You can choose to either get the logs from the SNS firewall through standard Syslog or more securely through Syslog-TLS.

Getting the logs through standard Syslog

Configuring a standard Syslog connection on the SNS firewall

- 1. On SNS, go to Configuration > Notifications > Logs Syslog IPFIX > Syslog.
- Select the object representing the IP address of the SLS instance or create a new object if one has not been created yet.
- 3. Select the appropriate protocol (TCP or UDP).
- 4. Select the port number. The default listening port is 514. You can retrieve the Syslog listening port by using the "change-syslog-port" command on a VM console. Note that using this command toggles the port between 514 and 601. Use it again if necessary.
- 5. Select the format.
- 6. **Apply** the configuration.

I NOTIFICATIONS / LOGS - SYSLOG - IPFIX									
LOCAL STOR	LOCAL STORAGE SYSLOG IPFIX								
SYSLOG PROF	ILES	Details							
Status Name									
Enabled SLS Name: SLS									
	Syslog Profile 1	Comments:	SLS						
Disabled Syslog Profile 2 Disabled Syslog Profile 3		Syslog server:	SLS_Server						
		Protocol:	UDP						
		Port:	syslog	· 5.					
		Certification authority:	Syslog-CA	* X					
		Server certificate:	sls.syslog	* ×					
		Client certificate:		* X					
		Format:	RFC5424	•					

Getting the logs through Syslog-TLS

Downloading SNS Certificate Identity

- 1. On SNS, go to Configuration > Objects > Certificates and PKI.
- 2. Create a Server Identity with RSA as Key type.





3. Download the Server Certificate identity as a P12 file.

SOBJECTS / CERTIFICATES /	ND PKI		
🔍 Enter a filter 🔹 Filte	r: all 💌 🗶 🖉 📔	+ Add • × Revoke = Actions •	📮 Download 🕶 👁 Check usage
sslvpn-full-default-authority openvpnserver openvpnclient CA_for_SMC_VPN_tunnels Bravo.stormshield.eu Charlie.stormshield.eu Delta.stormshield.eu	ج ج ج ج	DETAILS REVOCATION (CRL Validity Issued: Expires:	Certificate CRL as PEM file CRL as PIM file Seb 16 12:43:29 2021 GMT Feb 14 12:43:29 2031 GMT
SSL proxy default authority CA_for_SMC_VPN_tunnels Syslog-CA Ssl.syslog	م م م	Issued for	C=AW,ST=test state,L=test city,0=Te

Extract the key from the certificate

On a terminal emulator, use the following commands. Customize the *.p12*, *.key* and *.crt* file names to match your case.

```
~/ SYSLOG-TLS ]$ openssl pkcs12 -in syslog2.sls.local.p12 -out
syslog2.sls.local.key -nocerts
Enter Import Password:
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
~/SYSLOG-TLS ]$ openssl pkcs12 -in syslog2.sls.local.p12 -out
syslog2.sls.local.crt -nokeys -clcerts
Enter Import Password:
~/SYSLOG-TLS ]$ openssl rsa -in syslog2.sls.local.key -out syslog2.sls.local-
unprotected.key
Enter pass phrase for syslog2.sls.local.key:
writing RSA key
```

Importing the SNS Certificate Identity on SLS

On SLS, go to ⁽²⁾ Settings >> System Settings >> System Settings.





- 2. On the Syslog tab, import the Certificate (.crt file) and the Key (.key file).
- 3. Save.

SYSTEM SETTINGS				0 8
General	Þ	TLS		
SMTP	►	Certificate:		Browse
NTP	•	Key:		Browse
SNMP	×	SLS Certificates ba	ive already been installed	
HTTPS	•			
Syslog	Þ	SEQUENCE NUMBE	ERING	
Support Connection	►	Add sequence r	numbers on log received from syslog collector	
Modes of Operation	•	COLLECTOR		
SSH Key Pair for li-admin	•	Message Length:	12	
Lockout Policy	•			1KB / 64KB
Enrichment	•			
Data Privacy Module	•		Save	Cancel

Configuring a Syslog-TLS connection on the SNS firewall

- 1. On SNS, go to Configuration > Notifications > Logs Syslog IPFIX > Syslog.
- 2. Select the object representing the IP address of the SLS instance or create a new object if one has not been created yet.
- 3. Choose *TLS* Protocol.
- 4. Fill in the certificate information.
- 5. Select *legacy_long* format.
- 6. Apply the configuration.

NOTIFIC/	ATIONS / LOGS - SYSLOG - I	PFIX			
LOCAL STOP	RAGE SYSLOG IPFIX				
SYSLOG PROP	FILES	Details			
Status	Name	Details			
💽 Enabled	SLS	Name:	SLS		
🗇 Disabled	Syslog Profile 1	Comments:	SLS		
🕁 Disabled	Syslog Profile 2	Syslog server:	SLS Server	-	100
⊕ Disabled	Syslog Profile 3	Protocol:	TLS		•
		Port:	syslog-tls	-	000
		Certification authority:	Syslog-CA		>
		Server certificate:	sls.syslog		>
		Client certificate:			>
		Format:	legacy_long		•



Getting logs from SES Evolution

Adding a new device on SLS

1. On SLS, go to 🕸 Settings >> Configuration >> Devices and click Add.

(Z)	€ B	АСК	Devices			
	0	ADD	🕄 ADD BULK DEVICES 🛛 🛓 IMF	PORT 🕘 JOBS		
0		S.N.	Name	Addresses	Device Groups	Log Collection Policies
Ø		1	214-000	10.00.001		stormshield
ø		2	And and a second	10.01		stormshield
٩		3	localhost	127.0.0.1,::1	linux	
B						
\$						

- 2. Enter the Name of the device.
- 3. In the **IP address(es)** field, enter he IP addresses of each machine that hosts an SES Agent handler that communicates with SLS.
- 4. In the Log Collection Policy field, select stormshield.
- 5. Choose the correct **Time Zone**.
- 6. Click Submit.

CREATE DEVICE		00
DEVICE INFORMATION -		
Name:	Alpha	
Device Address(es):	The second secon	
Device Groups:		
Log Collection Policy:	stormshield 🗙	
Distributed Collector:		
Time Zone:	(GMT+01:00) Brussels, Copenhagen, Madrid, Paris	T
RISK VALUES		
Confidentiality:	Minimal	Ŧ
Integrity:	Minimal	Ŧ
Availability:	Minimal	T
	Submit	Cancel





Configuring logs retrieval

You can choose to either get the logs from SES Agent handlers through **standard Syslog** or more securely through **Syslog-TLS**.

Getting the logs through standard Syslog

Configuring a TCP or UDP connection on the Agent handler

- 1. On the SES Evolution administration console, go to the **Agent handlers** menu and click the + icon.
- 2. Enter the Name of the Agent handler group.
- 3. In the Address field, enter the IP address of the SLS instance.
- 4. Select the appropriate Protocol (TCP or UDP).
- 5. Enter the **Port** number. The default listening port is *514*. You can retrieve the Syslog listening port by using the "change-syslog-port" command on a VM console. Note that using this command toggles the port between *514* and *601*. Use it again if necessary.
- 6. In the **Transfer type** field, choose Non-Transparent-Framing.
- 7. In the Message content field, choose Raw JSON.
- 8. Click Save in the upper banner.

Agent handlers > New gro	oup (SLS-AHAN	DLERSES)				
+ Add	Agent handler g	group settings				
New group (SLS-AHANDLERSES) SLS-AHANDLERSES	Name New group (SLS-AHANDLERSES)					
	Syslog servers					
	Add a ser Enabled	Description				
	Address	1945-69-00		Message content	Raw JSON	\sim
	Protocol	ТСР	\sim	Message language	English	~
	Port	514		Maximum message size		
	Transfer type	Non-Transparent-Framing	\sim	Minimum log severity	Warning	\sim

Page 19/24





Getting the logs through Syslog-TLS

Generating and importing the Certificate Identity on SLS

- 1. On the host system used to generate certificates, generate a PEM X.509 certificate.
- 2. On SLS, go to 🕸 Settings >> System Settings >> System Settings.



3. On the Syslog tab, import the Certificate (.crt file) and the Key (.key file).

4. Save.

SYSTEM SETTINGS				00
General	•	TLS		
SMTP	•	Certificate:		Browse
NTP	•	Key:		Browse
SNMP	•			
HTTPS	•	SLS Certificates ha	ave already been installed	
Syslog	Þ	SEQUENCE NUMB	ERING	
Support Connection	►	Add sequence	numbers on log received from syslog collector	
Modes of Operation	•	COLLECTOR		
SSH Key Pair for li-admin	•	Message Length:	12	
Lockout Policy	•			1KB / 64KB
Enrichment	•			
Data Privacy Module	•		Save	Cancel



Importing the Root Certificate Authority

On each machine that hosts an SES Agent handler that communicates with SLS, install the root certificate in the Trusted root certification authorities or Third-party root certificate authorities certificate store.

Configuring a TCP/TLS connection on the Agent handler

- 1. On the SES Evolution administration console, go to the **Agent handlers** menu and click the + icon.
- 2. Enter the Name of the agent handler group.
- 3. In the Address field, enter the IP address of the SLS instance.
- 4. Select the *TCP/TLS* **Protocol**.
- 5. Enter the **Port** 6514.
- 6. In the Transfer type field, choose Non-Transparent-Framing.
- 7. In the Message content field, choose Raw JSON.
- 8. Click Save in the upper banner.

Agent handlers > New gro	oup (S	LS-AHANI	DLERSES)						
+ Add	Age	nt handler g	roup settings						
New group (SLS-AHANDLERSES) SLS-AHANDLERSES	Name New group (SLS-AHANDLERSES)								
	Syslog servers + Add a server								
		Enabled	Description						
		Address	104540-50		Message content	Raw JSON	\sim		
		Protocol	TCP/TLS	~	Message language	English	\sim		
			Reminder: The root certification authority and intermediate		Maximum message size				
			certification authorities of the Syslog Server must be imported in the certificate store of each agent handler computer.		Minimum log severity	Warning	, ~		
		Port	6514						
		Transfer type	Non-Transparent-Framing	~					





Getting logs from external sources

Downloading the external sources archive on MyStormshield

- 1. Download the "Applications SLS External Sources" archive from your MyStormshield personal area in Downloads > Downloads > Stormshield Log Supervisor > Resources.
- 2. Extract the content of the archive.
- 3. Find the application file .pak you want.

Adding an external source application on SLS

1. On SLS, go to 🕸 Settings >> System Settings >> Applications and click Import.

(Z)	BACK SLS Applications						
	±.0	IPORT 🥑 JOBS		search	0		
0	S.N.	Name	Description	Version	Actions		
Ø	1	ThreatIntelligence	This package contains Threat Intelligence Enrichment Source, Threat Intel Analytics, and Threat Intelligence process command.	6.1.2	İ		
Q	2	GEOIP	This package contains GEOIP EnrichmentSource and GEOIP Process Plugin.	5.2.0	Î		
٩	3	JSONParser	This package contains JSONParser process commands	5.0.2	İ		
Đ	4	MitreDatasetUpdater	This application contains the Mitre Dataset Updater plugin.	6.2.0	İ		
愈	5	StringConcat	This package contains String Concat process plugin	1.0.1	î		
	6	CSVEnrichmentSou	This package contains pluggable CSVEnrichmentSource.	5.2.1	İ		

2. Browse to the application .pak file and click Upload.

IMPORT NEW APPLICATION			8
Application:	Select a File to import		Browse
		Upload	Cancel









Additional information and answers to questions you may have about SLS are available in the **Stormshield knowledge base** (authentication required).









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.

