

مكتبة الالخ نم FTD ثدحل نمآ لماكت نيوكت نمآ ثدح لصوم ربع نامأال ةباحس يف

تايوتحمل

[ةمدقملا](#)

[ةيساسأال تابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكملا](#)

[نيوكتلا](#)

[ةحصللا نمققحتلا](#)

[اهالصل او عا طخأال فاشكتسا](#)

ةمدقملا

يف مكتبتلا" ىل نامأال ثادحأ لاسرال Cisco Secure FTD نيوكت ةيفيك دنتسملا اذه فصيفي (SEC) "نامأال ثدح لصوم" مادختساب (SCC) "نامأال ةباحس

ةيساسأال تابلطتملا

تابلطتملا

ةيلاتلا عيضاوملاب ةفرعم كيذل نوكت ناب Cisco ي صوت:

- Cisco نم (FTD) ةيامحل رادج ديدعت نع نمآال عافدل
- Linux (CLI) رماوأ رطس ةهجاو

ةمدختسملا تانوكملا

ةيلاتلا ةيдамلا تانوكملا وجماربل تارادصل ىل دنتسملا اذه يف ةدراول تامولعمل دنتست:

- Cisco Secure FTD، 7.6 رادصل
- Ubuntu 24.04 ةغيص لدان

ةصاخ ةيلمعم ةئيبي يف ةدوجوملا ةزهجأال نم دنتسملا اذه يف ةدراول تامولعمل عاشنإ مت تناك اذإ. (يضايرتفا) حوسمم نيوكتب دنتسملا اذه يف ةمدختسملا ةزهجأال عيمجت أدب رمايأال لمحتمل ريثأتلل كمهف نم دكأتف، ليغشتلا ديق كتكتبش

نيوكتلا

SCC: ةومجم ةباوب ىل لوخدل ليحست 1. ةوطخل



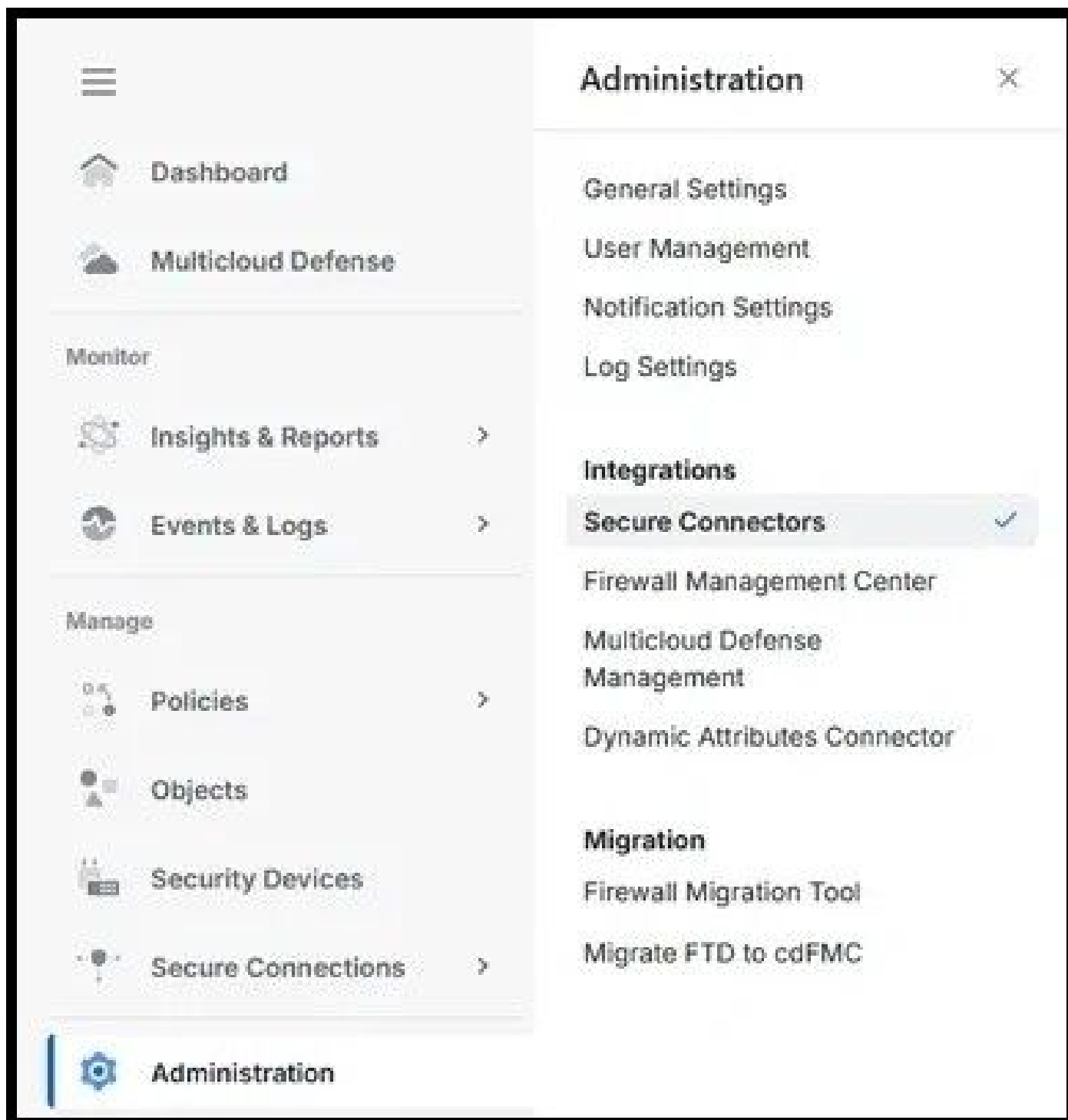
CONNECTING TO SECURITY CLOUD CONTROL (US)

Security Cloud Sign On

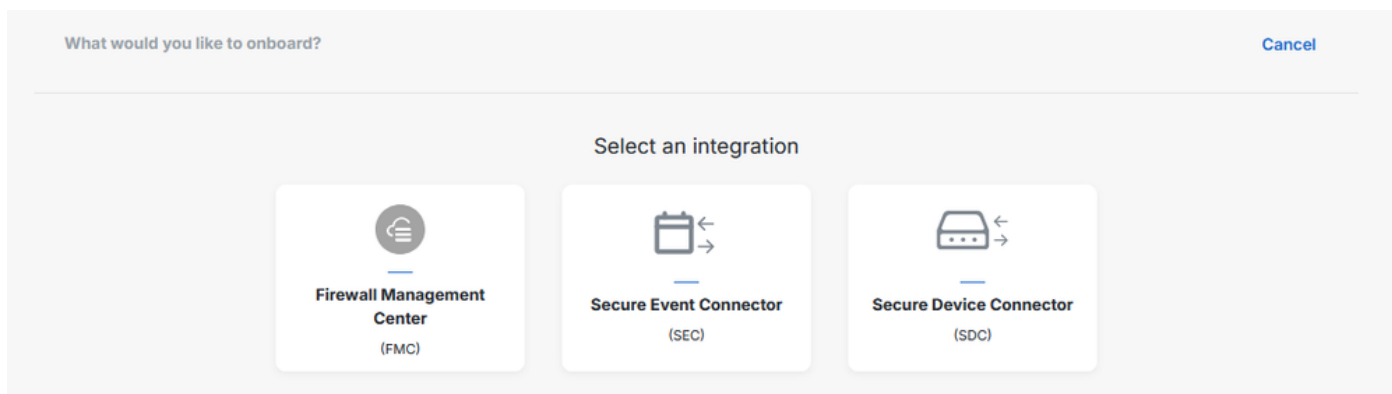
Email

Continue

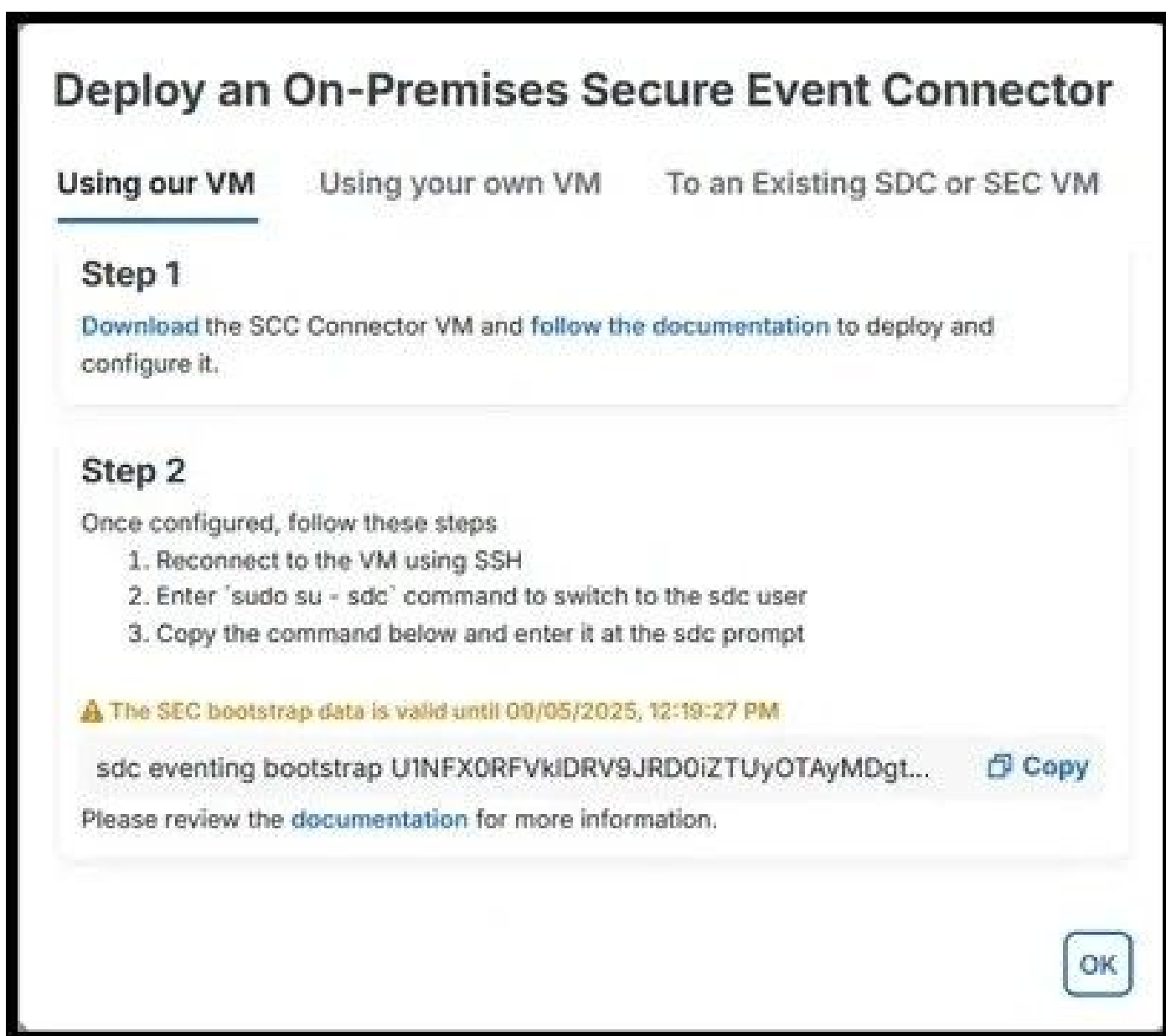
ةنمآلا تالصولل او ةرادإلا رتخأ ،رسيألا بنألا ةمئاق نم 2. ةوطخلا



شرح لصوم رتخاو ديدج لصوم مضل دئاز زم ر قوف رقنا ،يولعلال نميال بانجال ىلع 3. ةوطخلال نم:



بـولـطـمـال راـيـخـال إـلـى اـدائـتـسـا هـلـي غـشـت دـي هـمـت و لـصـومـال تـي بـثـل تـا و طـخـال مـدخـتـسـا 4. ة و طـخـال
بـ"دو جـوم SEC VM و SDC إـلـى" و "كـب صـاخـال (VM) يـرهـا ظـال زـاهـجـال مـادخـتـسـا" نـيـب



لـي غـشـت دـي هـمـت مـا ظـن لـو كـوتـورب ذـي فـنـت مـتـي اـمـدـنـع ة لـثـامـم ة لـاسـر رـهـظـت 5. ة و طـخـال
حـا جـنـب رـتـويـبـمـكـال

```
2025-06-09 05:41:56 [INFO] Bootstrap package processed successfully
2025-06-09 05:41:56 [INFO] Default AWS Region is us-west-2
2025-06-09 05:42:00 [INFO] Scanning for next available TCP port starting with 10125
2025-06-09 05:42:00 [INFO] TCP port found and set to 10125
2025-06-09 05:42:00 [INFO] Scanning for next available UDP port starting with 10025
2025-06-09 05:42:00 [INFO] UDP port found and set to 10025
2025-06-09 05:42:00 [INFO] Scanning for next available Netflow port starting with 10425
2025-06-09 05:42:00 [INFO] Netflow port found and set to 10425

WARNING! Your credentials are stored unencrypted in '/var/lib/sdc/.docker/config.json'.
Configure a credential helper to remove this warning. See
https://docs.docker.com/go/credential-store/

5a99d0351c1ae91cd790dcf18ee1d0594d37fcfaf5a1725473eed042342a567
2025-06-09 05:42:06 [INFO] The SEC is up and running - You should be all set to go
2025-06-09 05:42:08 [INFO] Your SEC has been successfully bootstrapped! Please verify that everything is working within
the SCC UI, and thank you for being a customer
sdc@lcorream-sdc:~$
```

SCC: لخدم ي ف ذفنم ل تامولعم رهظت ،هزيهجتو لصومل رشن درجم ب. 6 ةوطخل

CDO_cisco-lcorream-cdo-us_swz1we-SEC_a3889708-0844-4110-a1e8-641bf17374a6

Details

ID	a3889708-0844-4110-a1e8-641bf17374a6
Tenant ID	77cbf34d-91e0-4b2a-a7a8-2597430ce7ce
Version	202407211709
IP Address	19.0.0.10
TCP Port	10125
UDP Port	10025
NetFlow Port	10425

إلى م ث تاسايسلإلى لقتنا Cisco، نم (FMC) نمآال ةيامحل رادج ةرادا زكرم ي ف. 7 ةوطخل
هولي محت متي يذلا (ةزهجال) زاهجال عم قفاوتمل جهنل رتخأ. لوصول ي ف مكحتل
ل: لجستل م ث ديزمل رتخأ. 8 ةوطخل



Firewall Management Center

Policies / Access Control / Policy Editor

Overview

Analysis

Policies

Devices

Objects

Integrations

[Return to Access Control Policy Management](#)

FTD-Policy

Packets

→

✓ Prefilter Rules

→

○ Decryption

→

✓ Security Intelligence

→

✓ Identity

→

✓ Access Control

→

More

Type to search

Advanced Settings

HTTP Responses

Inheritance Settings

Logging

	Name	Action	Source	
			Zones	Networks
☐				

syslog هېښنت تفضاًو ددحم syslog هېښنت رايځ مادختساب لاسرالال نېكمتب مق 9. ةوطخلال نم اهيلع لوصحلال متيئالال ذفنمال تامولعمو (IP) تنرتنلال لوكوتورب ناوئع مدختسأ. ديډج SCC لخدم في SEC لوصوم

Create Syslog Alert Configuration



Name

SEC-Connector

Host

19.0.0.10

Port

10025

Facility

CONSOLE (ALERT)



Severity

ALERT



Tag

Cancel

Save

ثادحألا لاسرإل ةيدرفل دءاوقل لىدءءب مق ،لوصولا ف مكءءل ءهن لىل ةدوعل 10 ةوطءل
للى syslog مداء لىل

Logging settings for Rule 12: PC-to-Internet

☒ Log at beginning of connection

☒ Log at end of connection

☒ Log Files

 File Policy

FTDv-Malware/File



Send Connection Events to:

☒ Firewall Management Center

☒ Syslog server

(Using default syslog configuration in Access Control Logging)

[> Show overrides](#)

Discard

Confirm

عدبب ةيامحل رادجل حامسلل FTD ىلع اهؤارج مت يتل تاريخيغتال رشنب مق 11. ةوطخلل
ثادحلاليچست.

ةحصلال نم ققحتال

تالچسل او ثادحلالي ل لقتنا ، ثادحلالي لچست ءارج او حاجنبتاريخيغتال ذيفنت نم ققحتلل
ثادحلالي ةيؤر نم دكأتو SCC ةباوب يف ثادحلالي لچستو

Clear Time Range After 06/03/2025 11:40:01			
+ Views View 1			
	Date/Time	Device Type	Event Type ⓘ
⊕	Jun 5, 2025, 11:49:17	FTD	Connection
⊕	Jun 5, 2025, 11:49:18	FTD	Connection
⊕	Jun 5, 2025, 11:49:46	FTD	Connection
⊕	Jun 5, 2025, 11:49:46	FTD	Connection
⊕	Jun 5, 2025, 11:49:59	FTD	Connection
⊕	Jun 5, 2025, 11:50:02	FTD	Connection
⊕	Jun 5, 2025, 11:50:10	FTD	Connection
⊕	Jun 5, 2025, 11:50:47	FTD	Connection
⊕	Jun 5, 2025, 11:51:08	FTD	Connection
⊕	Jun 5, 2025, 11:51:15	FTD	Connection
⊕	Jun 5, 2025, 11:51:23	FTD	Connection
⊕	Jun 5, 2025, 11:51:38	FTD	Connection
⊕	Jun 5, 2025, 11:51:40	FTD	Connection

اهحال صاوعاطخال فاشكتسا

ةكرح قباط تيال ةرادال ةهجاو مادختساب زاهجال يلع ةمزح طاقثال ليغشتب مق FTD، يف syslog رورم ةكرح طاقثال لجا نم SEC الى لقتنت تيال تانايبال رورم

> capture-traffic

Please choose domain to capture traffic from:
0 - eth0

1 - Global

Selection? 0

Warning: Blanket capture may cause high CPU usage and reduced throughput, use selective filtering to reduce network traffic.
Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options: host 19.0.0.10 port 10025
Starting traffic capture, press ctrl + c to exit (Maximum 1,000,000 packets will be captured)
HS_PACKET_BUFFER_SIZE is set to 4.
tcpdump: can't parse filter expression: syntax error
Exiting.

> capture-traffic

Please choose domain to capture traffic from:

0 - eth0

1 - Global

Selection? 0

Warning: Blanket capture may cause high CPU usage and reduced throughput, use selective filtering to reduce network traffic.
Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options: host 19.0.0.10 and port 10025
Starting traffic capture, press ctrl + c to exit (Maximum 1,000,000 packets will be captured)
HS_PACKET_BUFFER_SIZE is set to 4.
10:43:00.191655 IP firepower.56533 > 19.0.0.10.10025: UDP, length 876
10:43:01.195318 IP firepower.56533 > 19.0.0.10.10025: UDP, length 1192
10:43:03.206738 IP firepower.56533 > 19.0.0.10.10025: UDP, length 809
10:43:08.242948 IP firepower.56533 > 19.0.0.10.10025: UDP, length 1170

مق. يره اظلال زاهجلا ىلع تنرتنلا اب لاصتا رفوت نم دكأت، SEC ل يره اظلال زاهجلا نم
نكمي اهحالص او عا طخألا فاشكتسا ةمزح عاشنإل، sdc troubleshooting رملأل ليغشتب
صخشتلال نم ديزم ىلع لوصحلل lar.log فلم نم ققحتلل اهمادختسا.

ةمچرتل هذه ل و ح

ةيلآل ا تاي ن ق ت ل ا ن م ة و م ج م ا د خ ت س ا ب د ن ت س م ل ا ا ذ ه Cisco ت م چ ر ت م ل ا ع ل ا ا ح ن ا ع م ج ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل ا و ا م ك ة ق ي ق د ن و ك ت ن ل ة ي ل آ ة م چ ر ت ل ض ف ا ن ا ة ط ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب Cisco ي ل خ ت . ف ر ت ح م م چ ر ت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة م چ ر ت ل ا ع م ل ا ح ل ا و ه ي ل ا ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا م چ ر ت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا د ن ت س م ل ا