

Matt Elkington

From: Check Point Support <support@checkpoint.com>
Sent: 20 March 2025 18:50
To: Steven Meadows
Cc: Matt Elkington; Steven Meadows
Subject: [EXTERNAL]SR#6-0004227433 Please supply the script mentioned in sk180507 [ref: 00D2009OX.1500J50CqcWM:ref]

Cyber Security Notice: This email originated from outside of the organisation. Do not click links or open attachments unless you recognise the sender and know the content is safe.



CHECK POINT™

Check Point Technical Services

Hi Steven,

Thanks for the update, **the proper script uploaded to the sftp account, please check sftp section.**

-For R81.20 and lower versions:

1. Close all SmartConsole windows.
2. Take the Gaia Snapshot/backup of the Management Server:
 1. In Gaia Portal, navigate to click "**Maintenance**" > "**Snapshot Management**".
 2. In the Snapshot Management section, click "**New**".
 3. In the "**Name**" field, enter a name for the image.
 4. **Optional:** In the "**Description**" field, enter a description for the image.
 5. Click **OK**.
3. Copy the TAR file to the Management Server (each server in Management High Availability) to some directory (for example, /var/log/).
4. Connect to the command line on the Management Server (each server in Management High Availability).
5. Log in to the Expert mode.
6. Extract the TAR archive:

```
cd /var/log/
```

```
tar xvf <Name of TAR File>
```

7. Go to the sub-directory with the script:

```
cd <Name of Sub-Directory>
```

8. Assign the 'execute' permission to the files:

```
chmod -v +x RunAccessClient.sh
```

```
chmod -v +x AccessClient.jar
```

9. Run the script to enable all Trusted CAs:

Important - Ignore the internal notes from this script.

- On a Security Management Server:

```
./RunAccessClient.sh -a fixOrphanTrustedCAs
```

- On a Multi-Domain Security Management Server:

```
./RunAccessClient.sh -a fixOrphanTrustedCAs -d <IP Address of Domain  
Management Server>
```

10. Connect with SmartConsole to your Security Management Server or Domain Management Server.

11. **Optional:** In SmartDashboard, disable unwanted Trusted CAs.

12. In SmartConsole, install the Access Control policy on the Security Gateway / Cluster object.

13. On the Management Server, remove the sub-directory with the script:

```
rm -i /var/log/<Name of Sub-Directory>/*
```

```
cd /var/log/
```

```
rmdir -v <Name of Sub-Directory>
```

I will go ahead and close this case since required file/scripts uploaded to the sftp account, please see sftp section.

Regards,

William Awad

Technical Services Chat Engineer

[CCSM]

Check Point Software Technologies

Toll-Free: +1 (888) 361-5030

Office hours: Mon-Fri 9:00a-6:00p US Central

For immediate assistance or any questions outside of my working hours, please feel free to reach out via our [Support Hotline](#) or [Chat](#).

For escalation purposes only, please contact:

Ken Savage – Team Manager savage@checkpoint.com

[Global Escalation Path](#) | [Global Support Phone Numbers](#)

SR Number: 6-0004227433



ref:!00D2009OX.!500J50CqcWM:ref