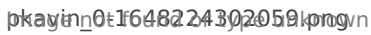
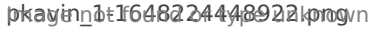


Troubleshooting FSSO Agent Install

Description	This article describes why Fortinet Single Sign-On (FSSO) stops working after upgrading to FSSO Collector Agent 5.0.0290.
Scope	FortiGate, FSSO, Collector Agent
Solution	<p>It has been noticed Fortinet Single Sign-On Agent service appears to be stopped, however, when trying to restart the service, it stops again shortly after.</p> <p>If it is verified the FSSO CA debug logs, an error 'cannot bind to UDP socket' can be found.</p> <p></p> <p>Starting FSSO Collector Agent build 5.0.0290, the FSSO Collector Agent includes a Syslog service that runs on UDP port 514.</p> <p>If UDP port 514 is already in use by another application/service/server on the Windows machine running the FSSO Collector Agent, this error while running FSSO - 'cannot bind to UDP socket' can be seen.</p> <p>To verify the same, open command prompt, run as administrator. Enter command '<i>netstat -abo</i>', this will show Active Connections along with the listening port number.</p> <p>On FSSO Agent build 5.0.0290 and later, under Advanced Settings -> Syslog source list -> Uncheck 'Enable this feature', since it is also using port 514.</p> <p>After disabling the FSSO Collector Agent's Syslog functionality, the FSSO Collector Agent should start successfully.</p> <p></p>

Description

This article describes why FortiGate cannot connect to FSSO Agent on Windows server 2019 and how to resolve the issue.

Scope

FortiGate v7.2.1, FSSO Collector Agent.

Solution

As an example in this article, an External Connector on FortiGate 7.2.1 has been configured using an FSSO Agent on a Windows AD connector.

matanaskovic_0_1660919587463.png

The configuration was working, but suddenly FSSO communication between FortiGate and FSSO Collector Agent 5.0.0306 has stopped.

FortiGate connects to the Collector Agent by default via port TCP/8000. Verify the Collector Agent is listening on port TCP/8000 in the Windows Firewall.

matanaskovic_1_1660919620231.png

matanaskovic_2_1660919636954.png

From FortiGate, double-check to see if the FSSO CA is listening and to additionally verify that it is connected using telnet connection:

matanaskovic_3-1660919668489.png

Using debug command for verifying FSSO server status, 'waiting for retry' can still be seen as the Connection Status.

matanaskovic_4-1660919694805.png

- commands in picture
- diagnose debug enable
- diagnose debug authd fsso server-status

For further troubleshooting FSSO CA on Windows server, run the following debug application authd command.

diagnose debug application authd -1

Debug messages will be on for 30 minutes.

```
photon-kvm12 (root) # diagnose debug enable
```

```
photon-kvm12 (root) # authd_timer_run: 2 expired
```

```
authd_epoll_work: timeout 5000
```

```
authd_timer_run: 1 expired
```

```
authd_epoll_work: timeout 990
```

```
authd_timer_run: 1 expired
```

```
authd_epoll_work: timeout 10000
```

```
authd_epoll_work: timeout 10000
```

```
Server challenge:
```

```
    f9 57 20 05 7a 00 6d 50 42 7b a5 48 02 5d cf 37
```

```
MD5 response:
```

```
    d5 08 03 a2 66 f1 ad 2b 0c 9a 6f 9b a5 d1 e9 1c
```

```
authd_epoll_work: timeout 9990
```

```
_process_auth[FSSO-Collector Agent]: server authentication failed, aborting
```

```
disconnect_server_only[FSSO-Collector Agent]: disconnecting
```

```
authd_epoll_work: timeout 9990
```

```
diag deb disauthd_timer_run: 1 expired
```

```
authd_epoll_work: timeout 9980
```

```
authd_epoll_work: timeout 9980
```

```
Server challenge:
```

```
    19 58 fc 28 4b 3a 66 7c 2c 0e 09 62 96 56 76 45
```

```
MD5 response:
```

73 b5 03 1b b8 64 21 c8 82 7e 8d 10 e6 2b c3 99

authd_epoll_work: timeout 9970

**_process_auth[FSSO-Collector Agent]: server authentication failed, aborting
disconnect_server_only[FSSO-Collector Agent]: disconnecting**

authd_epoll_work: timeout 9960

After trying to re-enter or change the FSSO Agent password that is in use for communication between FortiGate and FSSO Collector Agent, finally communication is established.

Make sure the password is less than 15 characters. The FSSO collector agent can only accept passwords up to 15 characters in length.

The status will then show as 'Connected' and will be possible to verify once again using a debug command.

matanaskovic_0_1661436846730.png

matanaskovic_5_1660919765998.png

Identify the user account used to run the Fortinet Single Sign On process service and validate the permissions of the user account, it must belong to Administrators and/or Domain Admins groups:

adminaccountcredentials.png

the account should be admin or in admin group.png

If it still does not work after confirming that the password is the same on both FortiGate and the Collector agent, try to uninstall and reinstall the Collector agent.

To uninstall the collector agent in Windows, go to **Add or Remove programs** under **System Settings**. Find the FSSO Collector agent and uninstall it.

To reinstall the collector agent, refer to [Technical Tip: How to install the FSSO Collector Agent](#).

After it is installed again, configure the FSSO collector agent and try to connect it again to the FortiGate.

The status should then show as 'Connected'.

Revision #1

Created 4 December 2024 21:41:37 by ColtM

Updated 4 December 2024 21:42:43 by ColtM