Lab Report: Fortinet Single Sign-On (FSSO) Configuration

Fortinet Infrastructure - FortiOS 7.2

Submitted by:

Sama Yousef

DPEI

Date: November 28, 2024

Contents

Abstract

This report details the steps, configuration, and testing results of Fortinet Single Sign-On (FSSO) integration. It covers configuring FortiGate to monitor and control user authentication, utilizing transparent user identification methods, and verifying the functionality through both GUI and CLI tools.

1 Objective of the Lab

The goal of this lab is to configure and test Fortinet Single Sign-On (FSSO) for user authentication. The specific objectives include:

- Reviewing the Single Sign-On (SSO) configuration on FortiGate.
- Testing transparent or automatic user identification through simulated user logon events.
- Monitoring SSO status and operations using the FortiGate GUI and CLI.

2 Topology

The lab utilizes the following components:

- **Local-FortiGate:** Configured to enable SSO and monitor user logon activities.
- **Local-Client VM:** Runs a Python script to simulate user logon events.
- **TrainingDomain:** Demonstrates integration with the FSSO authentication system.

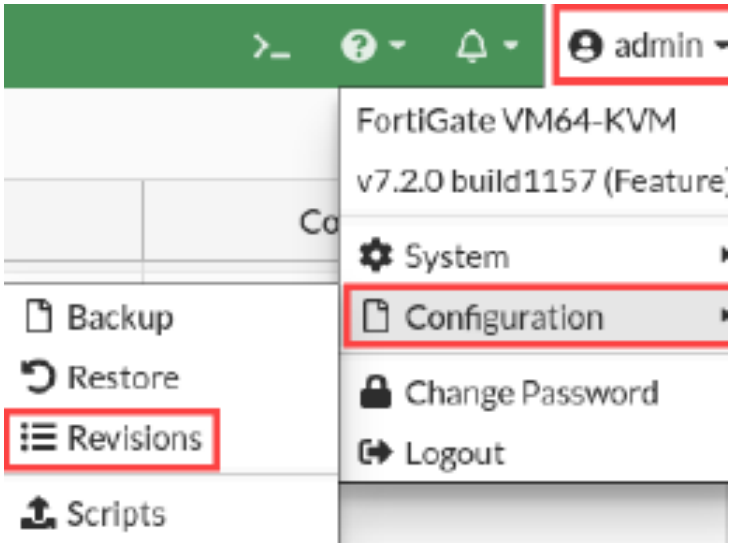
3 Components Used

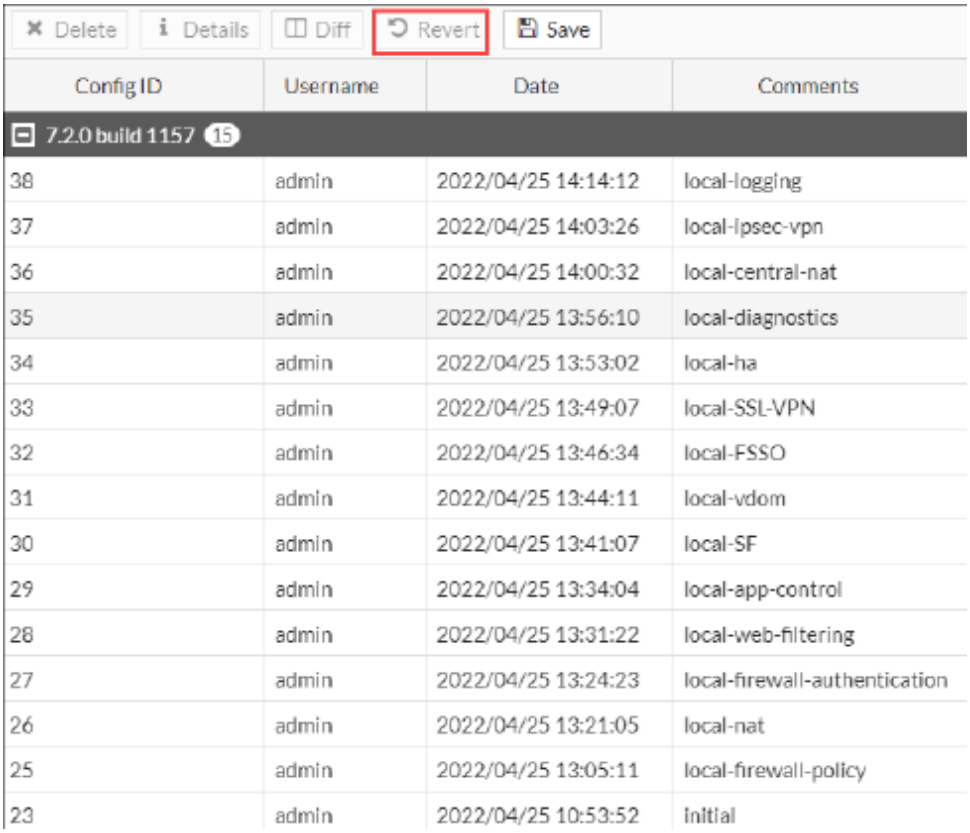
- **FortiGate Device:** Configured with SSO policies.
- **Local-Client VM:** Used for generating logon events via a Python script.
- **Python Script:** Simulates user logon activities and generates events for FSSO.

4 Steps of the Lab

4.1 Prerequisite Configuration

1. Restore the `local-FSSO` configuration file on Local-FortiGate using the GUI.





Config ID	Username	Date	Comments
7.2.0 build 1157 (15)			
38	admin	2022/04/25 14:14:12	local-logging
37	admin	2022/04/25 14:03:26	local-ipsec-vpn
36	admin	2022/04/25 14:00:32	local-central-nat
35	admin	2022/04/25 13:56:10	local-diagnostics
34	admin	2022/04/25 13:53:02	local-ha
33	admin	2022/04/25 13:49:07	local-SSL-VPN
32	admin	2022/04/25 13:46:34	local-FSSO
31	admin	2022/04/25 13:44:11	local-vdom
30	admin	2022/04/25 13:41:07	local-SF
29	admin	2022/04/25 13:34:04	local-app-control
28	admin	2022/04/25 13:31:22	local-web-filtering
27	admin	2022/04/25 13:24:23	local-firewall-authentication
26	admin	2022/04/25 13:21:05	local-nat
25	admin	2022/04/25 13:05:11	local-firewall-policy
23	admin	2022/04/25 10:53:52	initial

4.2 Review the FSSO Configuration

1. Log in to the Local-FortiGate GUI.

2. Navigate to **Security Fabric ¿ External Connectors**.
3. Review the **TrainingDomain** connector's configuration and confirm its status.

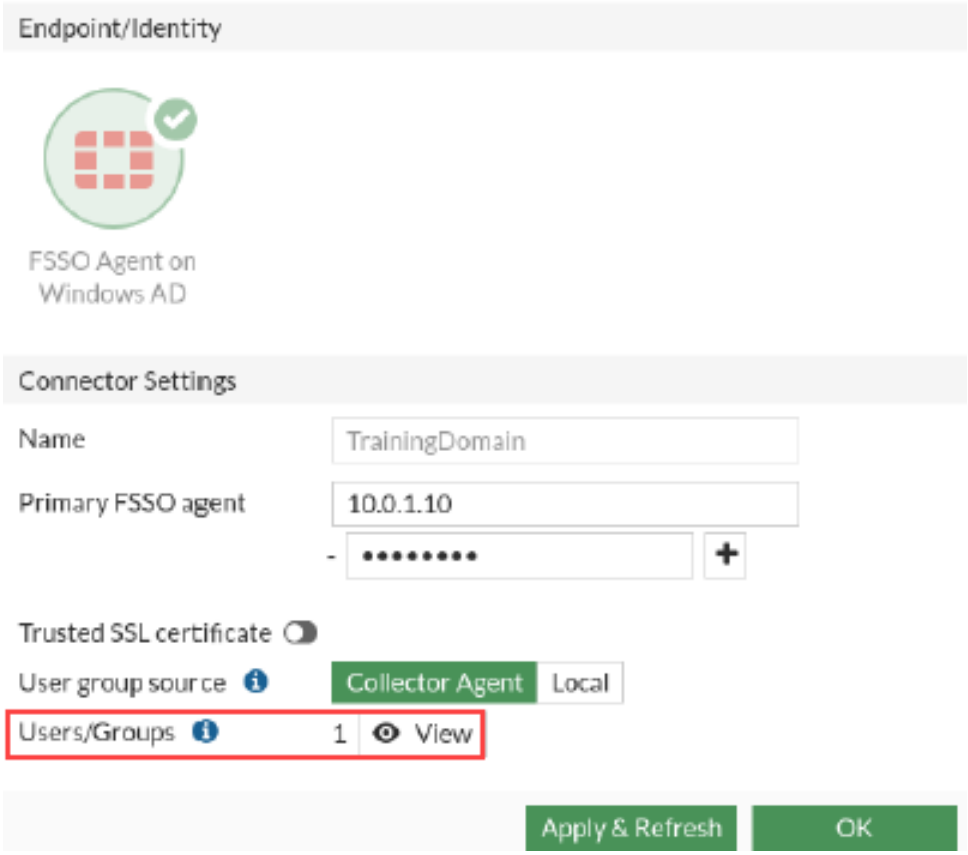
4.3 Simulate User Logon Events

1. On the Local-Client VM, run the Python script to generate simulated logon events:

```
cd Desktop/FSSO/
python2 fssoreplay.py -l 8000 -f sample.log
```

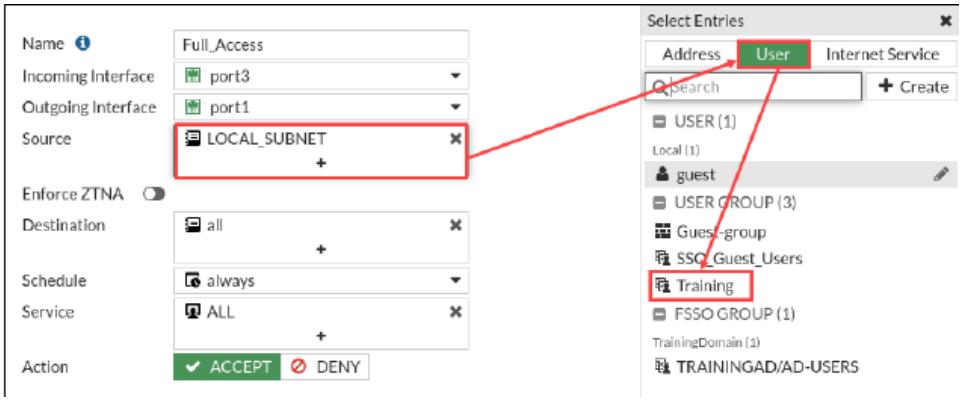
4.4 Create and Assign FSSO User Group

1. Create a new FSSO user group (`Training`) under **User & Authentication ¿ User Groups**.
2. Add the simulated user (`aduser1`) to this group.



4.5 Assign Firewall Policy

1. Edit an existing firewall policy to include the `Training` group as the source.
2. Save the policy and apply changes.



4.6 Test SSO Authentication

1. Verify unrestricted access to the Fortinet website without FSSO policies.
2. Assign the FSSO group to the firewall policy and retest access.

4.7 Monitor FSSO Operations

1. Use CLI commands to validate SSO functionality and monitor logon events:

```
diagnose debug authd fsso server-status
diagnose debug application authd 8256
```

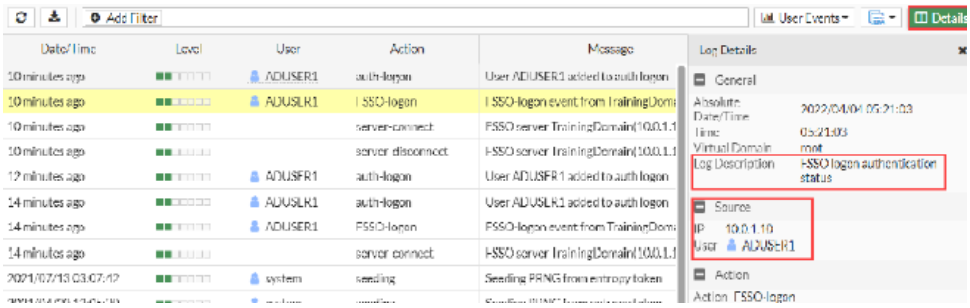
5 Testing the Lab

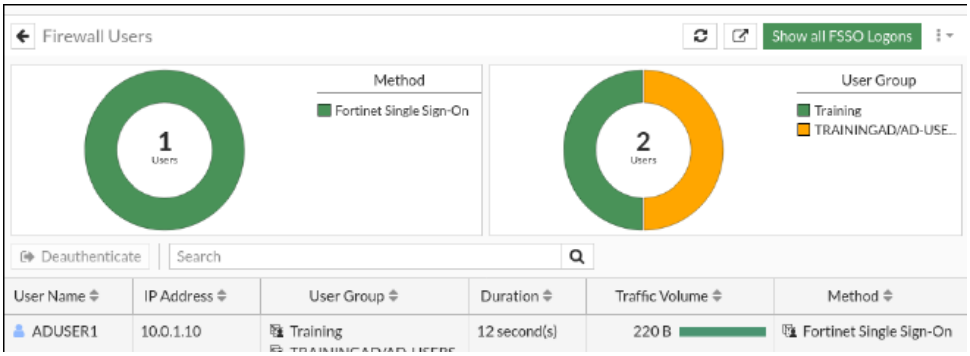
5.1 Scenario 1: Unrestricted Access Without FSSO Policies

All users can access resources such as the Fortinet website.

5.2 Scenario 2: Restricted Access with FSSO Policies

Only users within the `Training` group are allowed access to specified resources.





5.3 Monitoring

Simulated logon events are captured using CLI diagnostic tools, and FSSO logons are displayed in the FortiGate GUI.

6 Results

6.1 Configuration Success

- FSSO successfully configured on FortiGate.
- Users were correctly assigned to the FSSO user group.

6.2 Testing Outcomes

- Access controlled successfully based on user identity.
- Only authorized users in the `Training` group were allowed access.

6.3 Monitoring Results

- Logon events were captured and displayed in the FortiGate GUI.
- CLI diagnostics confirmed real-time communication between the simulated FSSO collector agent and FortiGate.

7 Conclusion

The lab successfully demonstrated the integration of FSSO with FortiGate, showcasing its ability to monitor and control user access based on authentication data. The results confirmed the system's effectiveness in enforcing user-based policies.