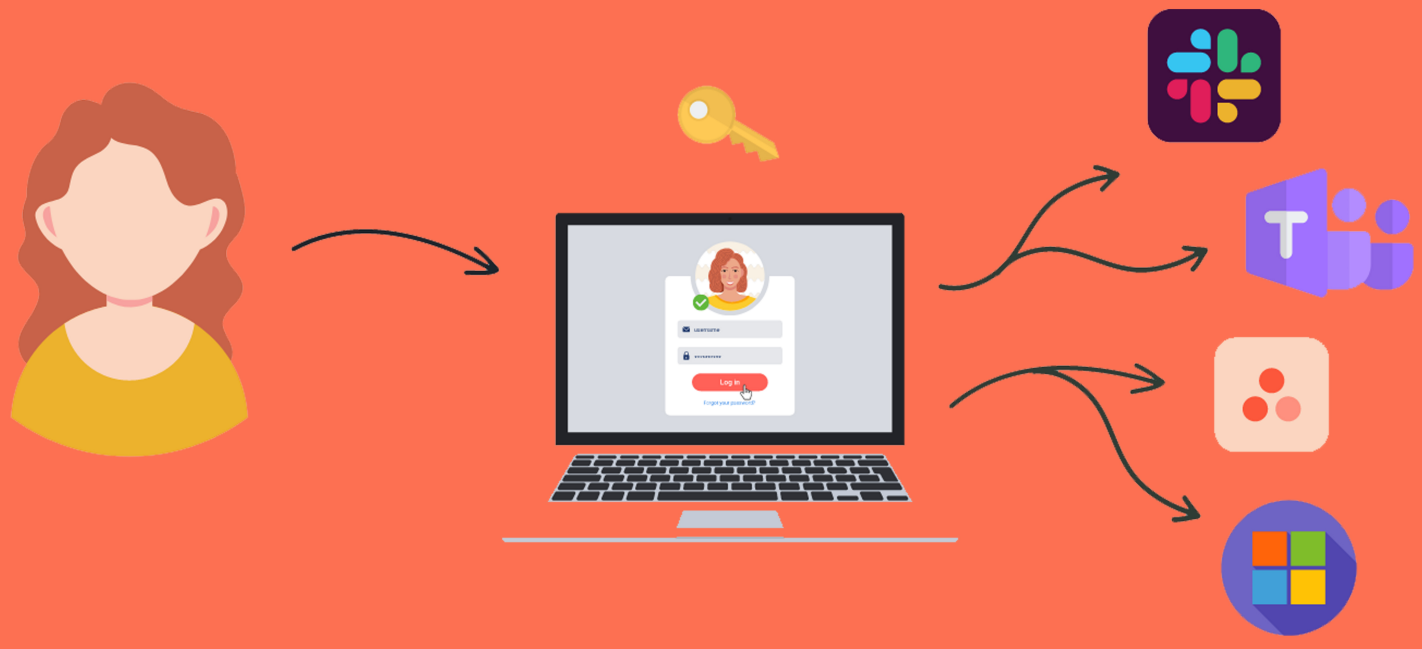
FORTINET®

FortiGate Single Sign-On

FSSO v.1

All You Need To Know

1 Complete Lab



ManiPahlavanzadeh

Ref.: Fortinet Documents

Fortinet Single Sign-On (FSSO) v.1

Mani Pahlavanzadeh
mani.pahlavan@gmail.com
ManiPahlavanzadeh

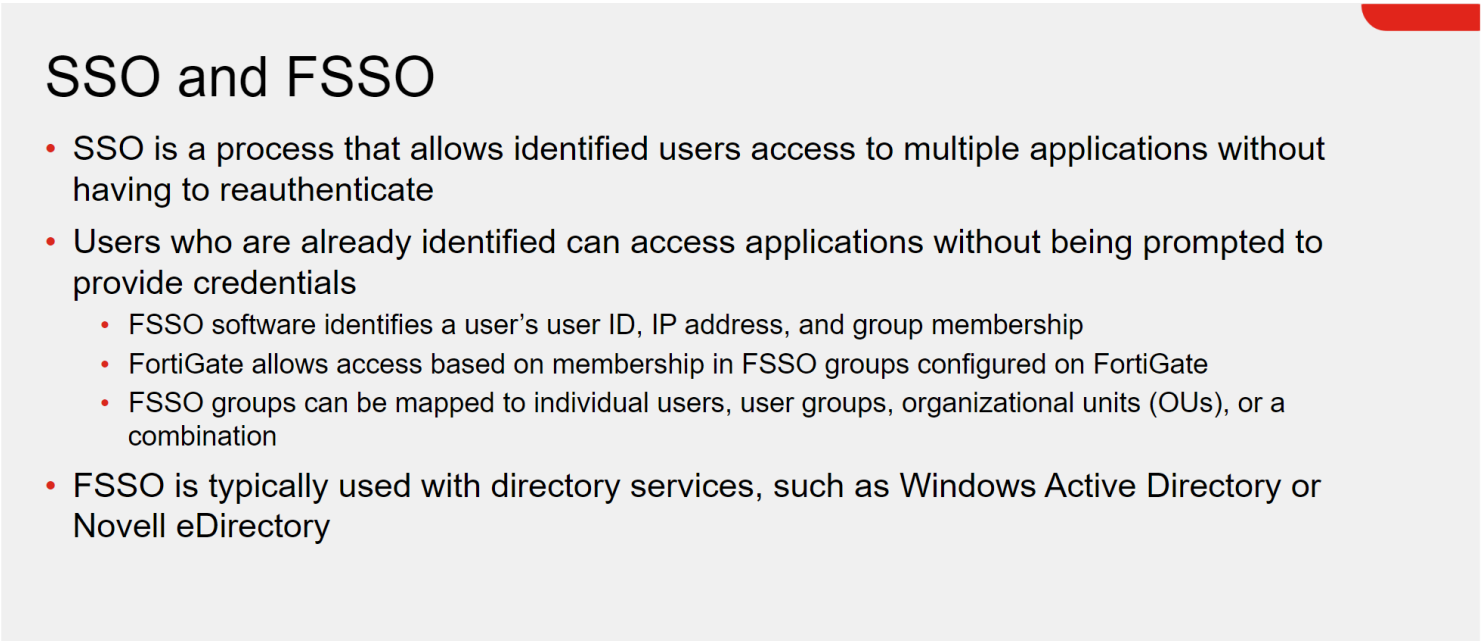
After completing this document, you will be able to achieve these objectives about FortiGate Methods of Firewall Authentication:

- SSS and FSSO
- FSSO Deployment and Configuration
- DC Agent Mode
    - What is the DC Agent Mode?
    - DC Agent Mode Process
- Polling Mode
    - Collector Agent-based Polling Mode
    - Collector Agent-based Polling Mode options
    - Collector Agent-based Polling Mode process
    - Agentless Polling Mode
    - Agentless Polling Mode process
- Comparing Modes
- Additional FSSO AD Requirements
- FSSO Configuration
    - FSSO Configuration – Agentless Polling Mode
    - FSSO Configuration – Collector Agent-Based Polling or DC Agent Mode
    - FSSO Agent Installation
    - FSSO Collector Agent Installation Process
    - DC Agent Installation Process
    - FSSO Collector Agent Configuration (Group Filter, Ignored User List, Collector Agent Timers, …)
- AD Group Support
- Troubleshooting Tips for FSSO
- FSSO Log Messages on FortiGate
- Log Messages on FSSO Collector Agent
- Currently Logged-on Users
- Checking Connection to FortiGate
- FSSO Additional CLI Commands
- Verification in Polling Mode
- LAB: Configuring FortiGate for FSSO Authentication

Fortinet Single Sign-On (FSSO)

In this document, you will learn about Fortinet single sign-on (FSSO). When you use this feature, your users don't need to log on each time they access a different network resource. By demonstrating competence in understanding SSO concepts, you will be able to more effectively understand FSSO methods.

SSO and FSSO



SSO is a process that allows users to be automatically logged in to every application after being identified, **regardless of platform, technology, and domain**. FSSO is a **software** agent that enables FortiGate to identify network users for security policies or for VPN access, without asking for their username and password. When a user logs in to a directory service, the **FSSO agent** sends FortiGate the username, the IP address, and the list of groups that the user belongs to. FortiGate uses this information to maintain a local database of usernames, IP addresses, and group mappings.

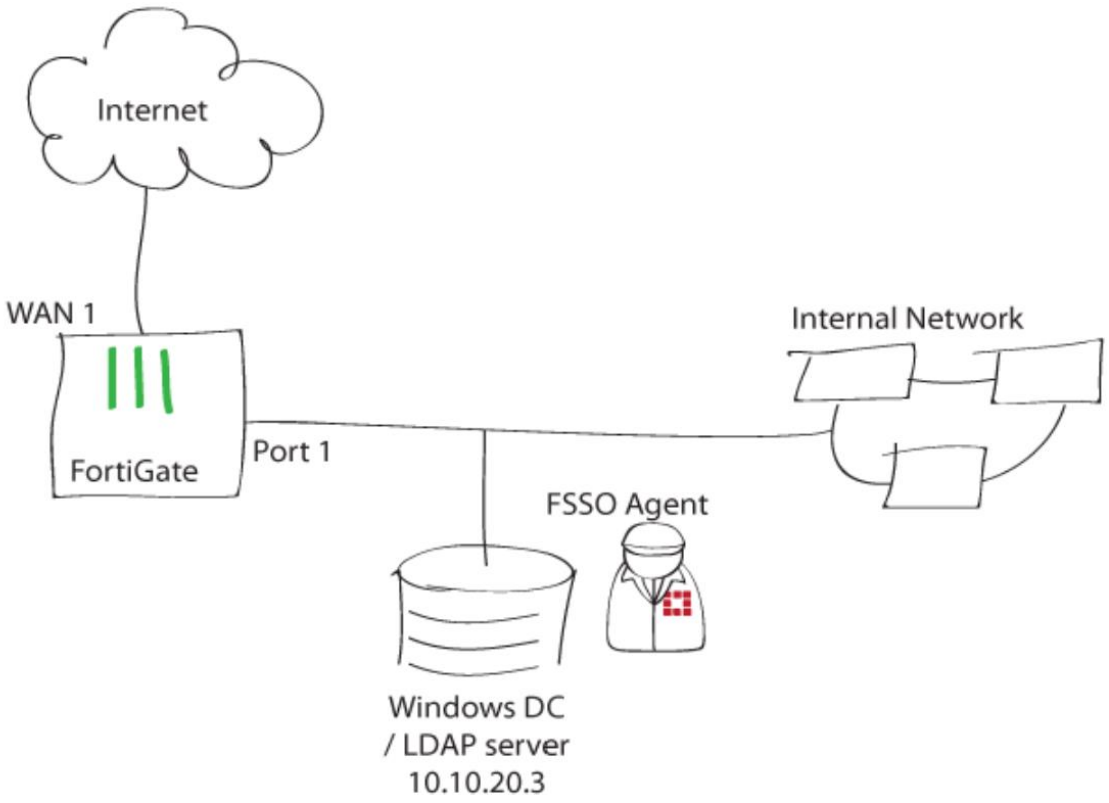
Because the domain controller authenticates users, FortiGate does not perform authentication. When the user tries to access network resources, FortiGate selects the appropriate security policy for the destination. If the user belongs to one of the permitted user groups, the connection is allowed.

FortiOS can provide single sign-on capabilities to Windows AD, Citrix, VMware Horizon, Novell eDirectory, and Microsoft Exchange users with the help of FSSO agent software installed on these networks. The agent software sends information about user logons to the FortiGate unit. With user information such as IP address and user group memberships from the network, FortiGate security policies can allow authenticated network access to users who belong to the appropriate user groups without requesting their credentials again.

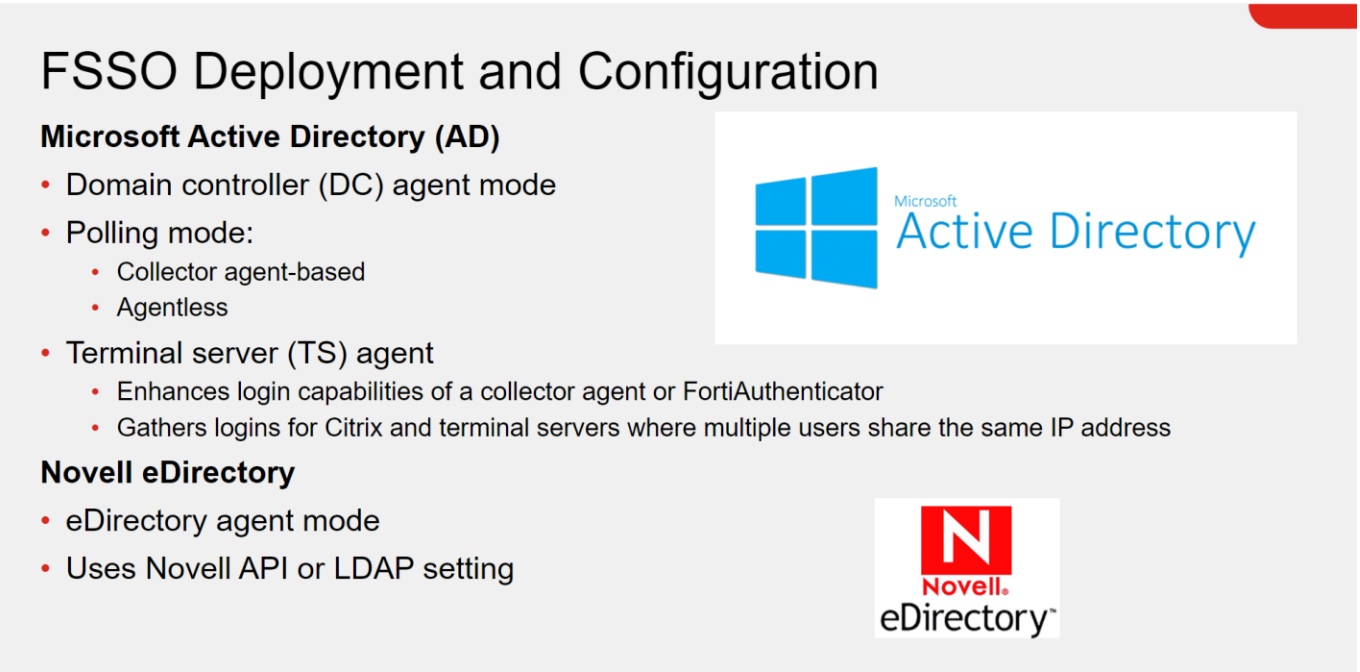
Fortinet Single Sign-On (FSSO), through agents installed on the network, monitors user logons and passes that information to the FortiGate unit. When a user logs on at a workstation in a monitored domain, FSSO:

- **Detects the logon event and records the workstation name, domain, and user,**
- **Resolves the workstation name to an IP address,**
- **Determines which user groups the user belongs to,**
- **Sends the user logon information, including IP address and groups list, to the FortiGate unit,**
- **Creates one or more log entries on the FortiGate unit for this logon event as appropriate.**

When the user tries to access network resources, the FortiGate unit selects the appropriate security policy for the destination. If the user belongs to one of the permitted user groups associated with that policy, then the connection is allowed, otherwise the connection is denied.



FSSO Deployment and Configuration



How you deploy and configure FSSO depends on the server that provides your directory services.

Microsoft Active Directory (AD)

There are two working modes that monitor user sign-on activities in Windows:

- **DC agent mode** ➔ uses a Collector Agent. **The Domain Controller (DC) agent** must be installed on every domain controller when you use DC Agent mode. The DC agents monitor user logon events and pass the information to the **Collector Agent**, which stores the information and sends it to the FortiGate unit.

- **Polling mode**
  - **Collector Agent-Based**
  - **Agentless**: FortiGate also offers a polling mode that does not require a collector agent, which is intended for simple networks with a minimal number of users.

❖ **Terminal Server (TS) Agent:** There is another kind of DC agent that is used exclusively for Citrix and terminal services environments: terminal server (TS) agents. TS agents require the Windows Active Directory collector agent or FortiAuthenticator to collect and send the login events to FortiGate.

Novell eDirectory

The **eDirectory agent** is installed on a Novell network to monitor user sign-ons and send the required information to FortiGate. It functions much like the collector agent on a Windows AD domain controller. The agent can obtain information from the Novell eDirectory using either the **Novell API** or **LDAP**.

The Terminal Server (TS) agent can be installed on a Citrix, VMware Horizon 7.4, or Windows Terminal Server to monitor user logons in real time. It functions much like the DC Agent on a Windows AD domain controller.

DC Agent Mode

DC agent mode is the most scalable mode and is, in most environments, the recommended mode for FSSO.

DC agent mode requires:

• **One DC agent installed on each Windows DC:** If you have multiple DCs, this means that you need multiple DC agents. DC agents monitor and forward user login events to the collector agents. DC Agent should be installed on each Windows DC in the **`Windows\system32`** directory.

We will learn about how we can install DC Agent on a Windows DC later in this document.

The DC Agent is responsible for:

- Monitoring user login events and forwarding them to the Collector Agent
- Handling DNS lookups (by default)

• **A collector agent, which is another FSSO component:**

The collector agent is installed on a Windows server that is a member of the domain you are trying to monitor. It consolidates events received from the DC agents, then forwards them to FortiGate.

The Collector Agent is responsible for:

- Group verification,
- Workstation checks,
- Updates of login records on FortiGate,
- The FSSO Collector Agent can send domain local security group, organizational units (OUs), and global security group information to FortiGate devices,
- It can also be customized for DNS lookups.

When the user logs on, the DC agent intercepts the login event on the domain controller. It then resolves the DNS of the client, and sends it to the collector agent.

The collector agent receives it and then performs a DNS resolution in order to check if the IP of the user has changed.

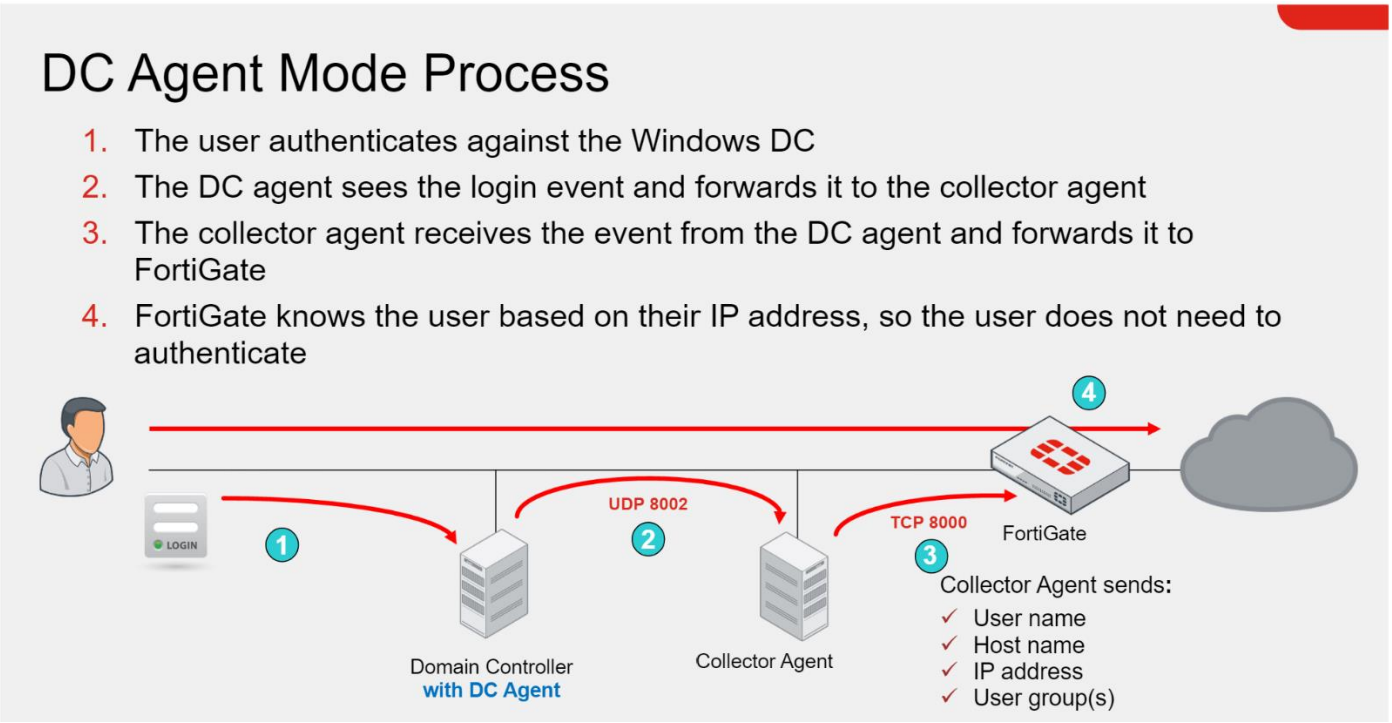
In some configurations, double DNS resolution is a problem. In this case, you may configure a registry key on the domain controller that hosts the DC agent in order not to resolve the DNS:
donot_resolve = (DWORD) 1 at HKLM/Software/Fortinet/FSAE/dcagent

---

A **FortiAuthenticator device** can act much like a CA, collecting Windows AD user logon information and sending it to the FortiGate device. It is particularly useful in large installations with several FortiGate units.

❖ The CA communicates with the FortiGate over TCP port 8000 and it listens on UDP port 8002 for updates from the DC agents.

DC Agent Mode Process



This slide shows the process of information passing between DC agents, the collector agent, and a FortiGate configured for FSSO authentication.

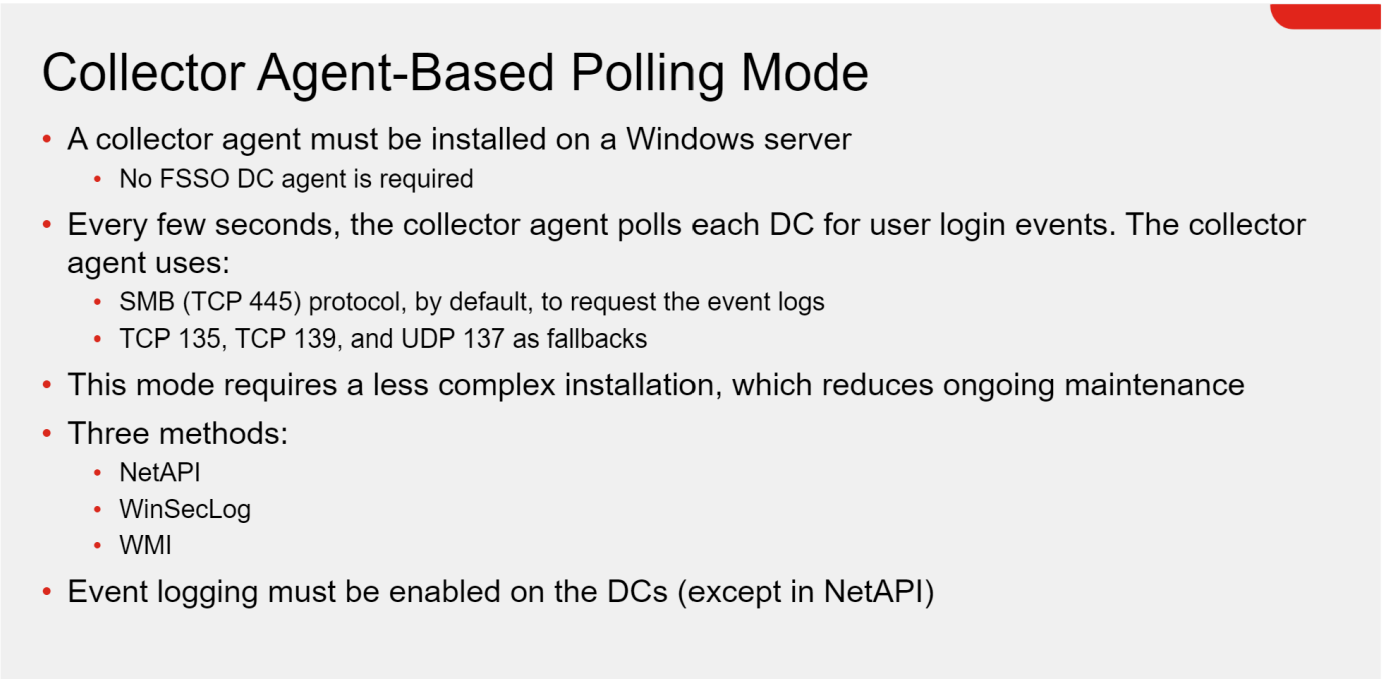
1. When users authenticate with the DC, they provide their credentials.

2. The DC agent sees the login event, and forwards it to the collector agent. (DC agent monitors and forwards user login events to the collector agent)

3. The collector agent aggregates all login events and forwards that information to FortiGate. The information sent by the collector agent contains the username, host name, IP address, and user group(s). The collector agent communicates with FortiGate over TCP port 8000 (default) and it listens on UDP port 8002 (default), for updates from the DC agents. The ports are customizable.

4. FortiGate learns from the collector agent who the user is, their IP address, and some of the AD groups that the user is a member of**. When a user tries to access the internet, FortiGate compares the source IP address to its list of active FSSO users**. Because the user in this case has already logged in to the domain, and FortiGate already has their information, FortiGate doesn't prompt the user to authenticate again. **Rather it allows or denies the traffic based on the matching firewall policy.**

Polling Mode – Colloctor Agent-Based



Polling mode can be:

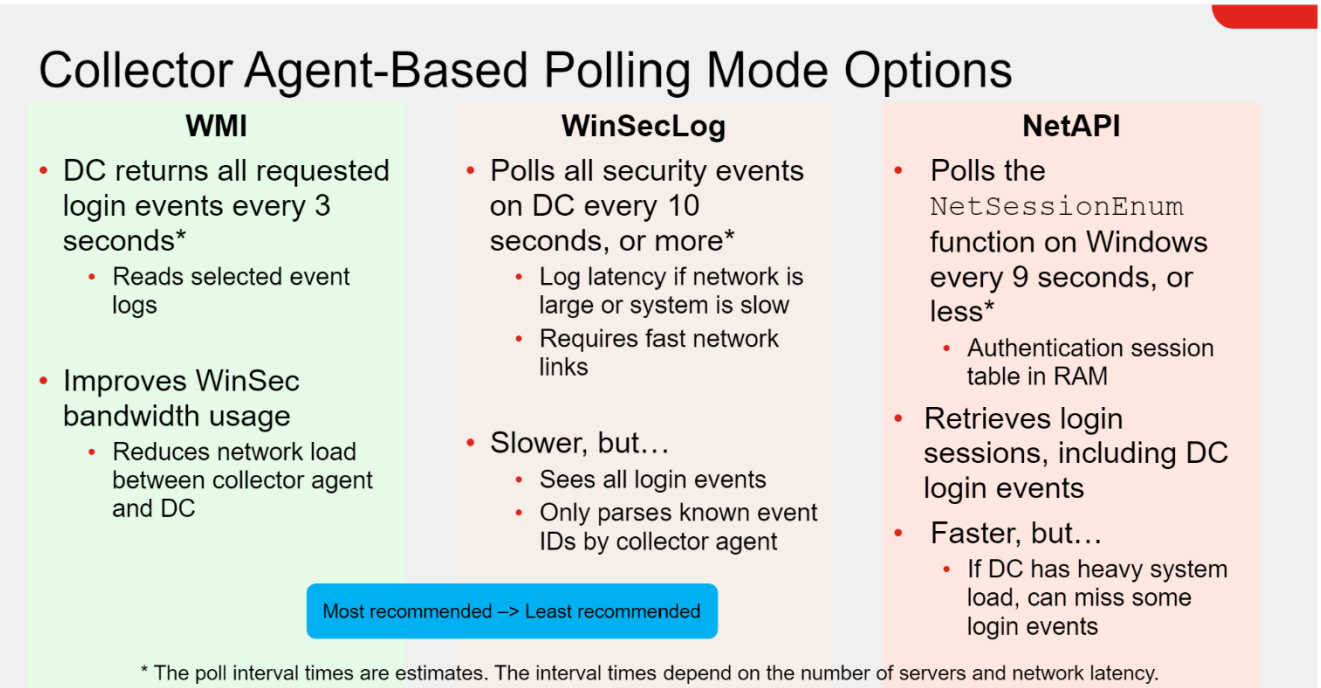
- Collector agent-based or
- Agentless

First, you'll look at the collector agent-based polling mode.

Like DC agent mode, collector agent-based mode **requires a collector agent** to be installed on a Windows server, but **it doesn't require DC agents** to be installed on each DC. In collector agent-based polling mode, the collector agent must be more powerful than the collector agent in DC agent mode, and it also generates unnecessary traffic when there have been no login events.

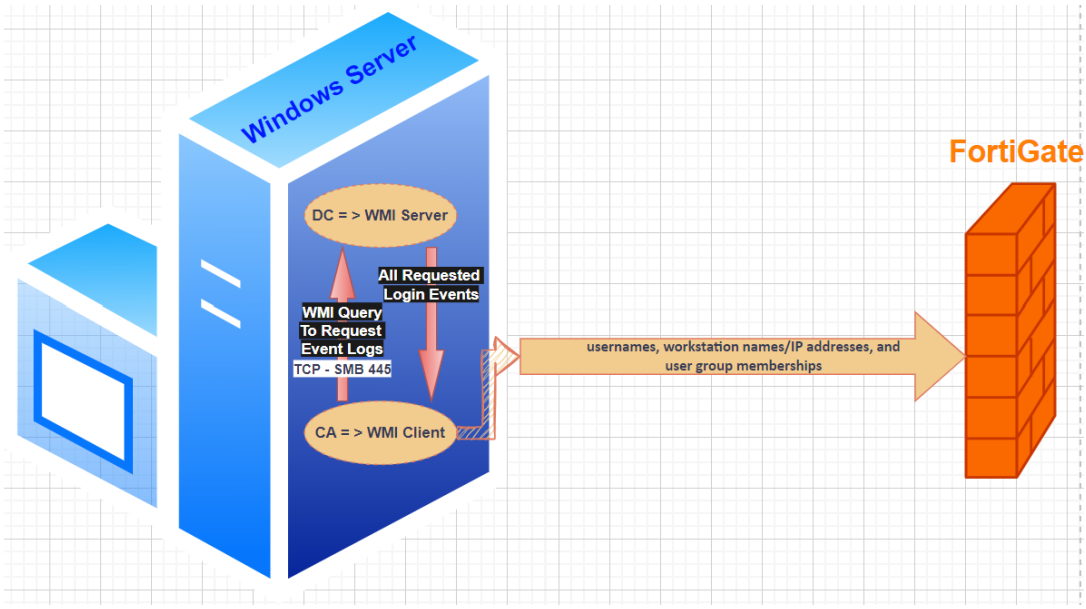
In Windows Event Log Polling, the most commonly deployed polling mode, the collector agent uses the **SMB (TCP port 445)** protocol to periodically request event logs from the domain controllers. Other methods may gather information differently, but after the login is received by the collector agent, the collector agent parses the data and builds the user login database, which consists of usernames, workstation names/IP addresses, and user group memberships. This information is then ready to be sent to FortiGate.

Collector Agent-Based Polling Mode Options



Collector Agent-based polling mode *has three methods (or options)* for collecting login information. The order on the slide from left to right shows most recommend to least recommended:

• **WMI:** (Windows Management Instrumentation) is a Windows API that gets system information from a Windows server. The DC returns all requested login events every almost 3 seconds. The **collector agent is a WMI client** and sends WMI queries for user login events to the **DC, which, in this case, is a WMI server**. The collector agent doesn't need to search security event logs on the DC for user login events; instead, the DC returns all requested login events. This reduces network load between the collector agent and DC.



• **WinSecLog:** polls **all** the security event logs from the DC every almost 10 seconds or more. It doesn't miss any login events that have been recorded by the DC because events are not normally deleted from the logs. There can be some delay in FortiGate receiving events if the network is large or system is slow and, therefore, writing to the logs is slow. It also requires that the audit success of specific event IDs is recorded in the Windows security logs.

• **NetAPI:** polls temporary sessions created on the DC when a user logs in or logs out and calls the **NetSessionEnum** function on Windows every 9 seconds or less. It's faster than the WinSec and WMI methods; however, it can miss some login events if a DC is under heavy system load. This is because sessions can be quickly created and purged from RAM, before the agent has a chance to poll and notify FortiGate.

Event ID?

1. FSSO Collector Agent with Windows Security Event Log polling mode supports the following Windows Event IDs:

- Windows 2008/2012/2016/2019 Event IDs: **4768, 4769*, 4776, 4624, 4770 **.**
- Windows 2003 Event IDs: **672, 673*, 680, 528, 540 **.**

* Some Event IDs are not supported alone and they required another event to correlate the login information. For example:

- Event 4769 requires 4768.
- Event 673 requires 672.

** By default, the Collector Agent is using a subset of events. Which event IDs are monitored is configurable with '**Windows Security Event ID to poll**' under Advanced settings:

- **0** - polls: **672, 680, 4768, 4776** - this is the **default** subset.
- 1 - polls: 672, **673**, 680, 4768, **4769**, 4776.
- 2 - polls: 672, 673, 680, 4768, 4769, 4776, **4624** (EventID 4624 was added to default polling in Windows 2016 for better support of MacOS and newer Windows server platforms).

2. FortiGate (FGT) has an integrated poller as well. Its local polling mode also uses the Windows Security Event logs, however, currently the supported event subset is smaller.

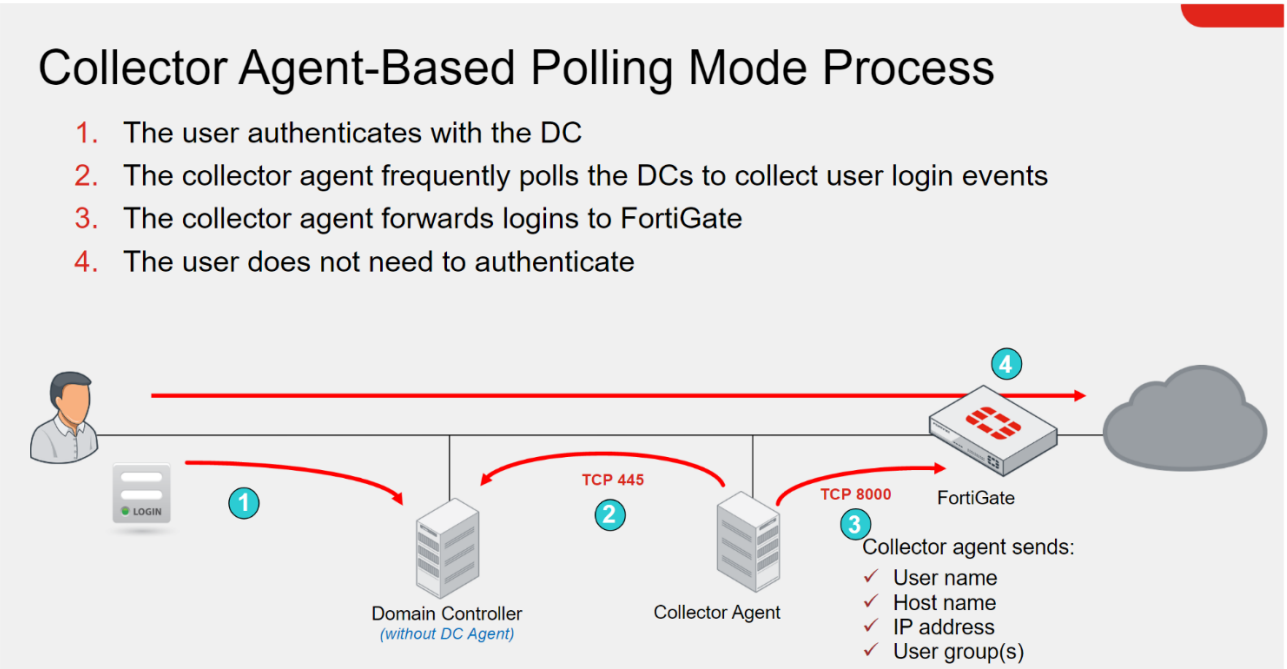
- Windows 2008/2012/2016/2019 Event IDs: **4768, 4769, 4776.**
- Windows 2003 Event IDs: **672, 673.**

3. FortiAuthenticator supports the following event IDs:

- Windows 2008/2012/2016/2019 Event IDs: **4768, 4769*, 4624*, 4770*, 4776.**
- Windows 2003 Event IDs: **672, 673*, 674*, 680, 528*, 540*.**

* Support for these events is available by enabling under the **Fortinet Single Sign-On (FSSO) section -> SSO -> General -> Enable Windows event log polling** (e.g., domain controllers/Exchange servers) **[Configure Events]**.

Collector Agent-Based Polling Mode Process



This slide shows an example of FSSO using the collector agent-based polling mode. This example includes a DC, a collector agent, and FortiGate, but the DC doesn't have the dcagent (or, alternatively, dcagent.dll) installed.

1. The user authenticates with the DC, providing their credentials.

2. The collector agent periodically (every few seconds) polls **TCP port 445** of each DC directly, to ask if anyone has logged in.

3. The collector agent sends login information to FortiGate over **TCP port 8000**. This is the same information that is sent in DC agent mode.

4. When user traffic arrives at FortiGate, FortiGate already knows which users are at which IP addresses, and no repeated authentication is required.

Polling Mode – AgentLess

Agentless Polling Mode

- Similar to agent-based polling, but FortiGate polls instead
- Doesn't require an external DC agent or collector agent
  - FortiGate collects the data directly
- Event logging must be enabled on the DCs
- More CPU and RAM required by FortiGate
- Support for polling option WinSecLog only
  - FortiGate uses the SMB protocol to read the event viewer logs
- Fewer available features than collector agent-based polling mode
- FortiGate doesn't poll workstation
  - Workstation verification is not available in agentless polling mode

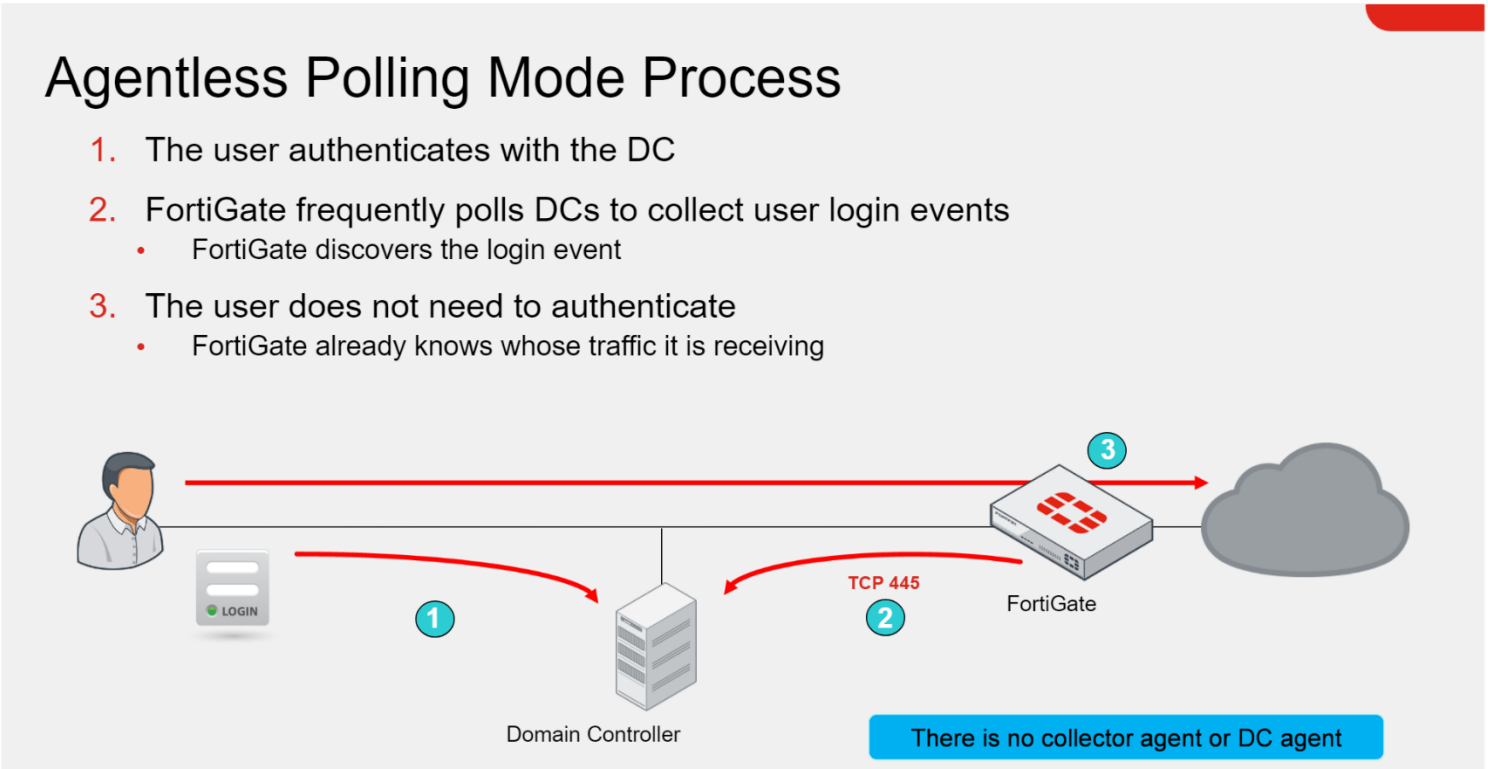
You can deploy FSSO without installing an agent (Neither DC agent nor Collector agent). FortiGate polls the DCs directly, instead of receiving login information indirectly from a collector agent. For Windows AD networks, FortiGate devices can also provide SSO capability by directly polling Windows Security Event log entries on Windows DC for user log in information. This configuration does not require a CA or DC agent.

Because FortiGate collects all of the data itself, agentless polling mode **requires greater system resources**, and **it doesn't scale as easily**. (More CPU and RAM required by FortiGate)

Agentless polling mode operates in a similar way to WinSecLog, but with only two event IDs: 4768 and 4769. Because there's no collector agent, FortiGate uses the **SMB protocol** to read the event viewer logs from the DCs. Event Logging must be enabled on the DCs.

In Agentless polling mode, FortiGate acts as a collector. It is responsible for polling on top of its normal FSSO tasks but does not have all the extra features, such as workstation checks, that are available with the external collector agent, it means FortiGate doesn't poll workstation. (Workstation verification is not available in Agentless polling mode)

Agentless Polling Mode Process



This slide shows how communication is processed without agents. (There is no collector agent or DC agent.)

1. User authenticates with the DC.

2. FortiGate polls the DC TCP port 445 to collect user login events. FortiGate registers a login event, obtaining the username, the host name, and the IP address. FortiGate then queries for the user's user group or groups.

3. When the user sends traffic, FortiGate already knows whose traffic it is receiving; therefore, the user does not need to authenticate.

Comparing Modes

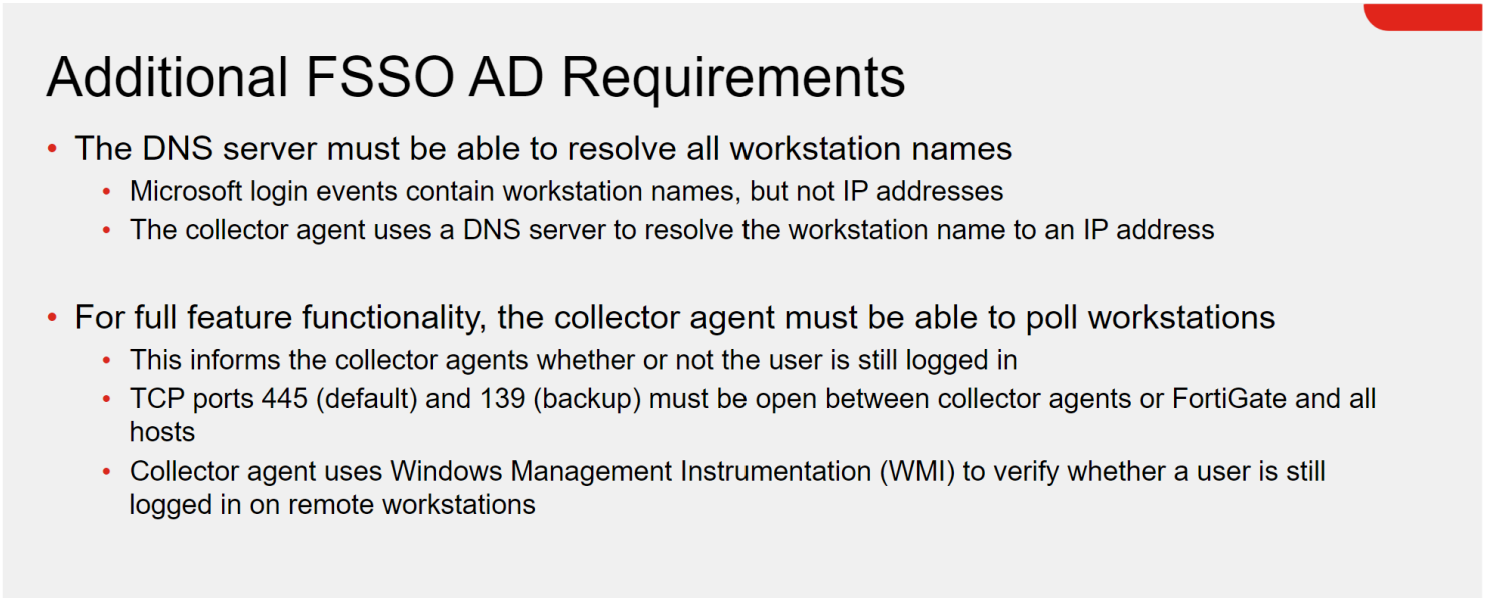
Comparing Modes

	DC agent mode	Polling mode
Installation	Complex—multiple installations (one per DC). Requires reboot.	Easy—one or no installations. No reboot required.
DC agent required	Yes	No
Resources	Shares with DC agents	Has own resources
Scalability	Higher	Lower
Redundancy	Yes	Yes
Level of confidence	Captures all logins	Might miss a login (NetAPI), or have a delay (WinSecLog)

This table summarizes the main differences between **DC agent mode** and **polling mode**.

- DC agent mode is more complex. It requires not only a collector agent, but also a DC agent for each monitored domain controller.
- However, it is also more scalable because the work of capturing logins is done by the DC agents who pass their information directly to the collector.
- In polling mode, the collector needs to query every domain controller, every few seconds. So, with each DC that is added, the number of queries grows.
- If you want to add a second collector agent for redundancy in polling mode, both collector agents need to query every DC individually.
- In DC agent mode, the DC agent just has to collect the log once, and send a copy of the necessary information to all the collector agents. In comparison, if you use polling mode, some login events might be missed or delayed, depending on the polling option used.
- You do not have to install a collector agent on the DC, you can install it on any Windows machine on the network.

Additional FSSO AD Requirements



Regardless of the collector method you choose, some FSSO requirements for your AD network are the same:

• Microsoft Windows login events have the **workstation name and username, but not the workstation IP address**. When the collector agent receives a login event, it queries a DNS server to resolve the IP address of the workstation. So, FSSO requires that you have your own DNS server. If a workstation IP address changes, DNS records must be updated immediately in order for the collector agent to be aware of the change and report it to FortiGate.

In Collector Agent-based polling mode, **Collector-Agent** is the responsible for DNS Resolution.

• For full feature functionality, collector agents need connectivity with all workstations. Since a "**monitored event log**" is not generated on logout, the collector agent (depending on the FSSO mode) must use a different method to verify whether users are still logged in. So, each user workstation is polled to see if users are still there. By default, all currently supported versions of FSSO collector agent use **WMI** to verify whether a user is still logged in on remote workstations.

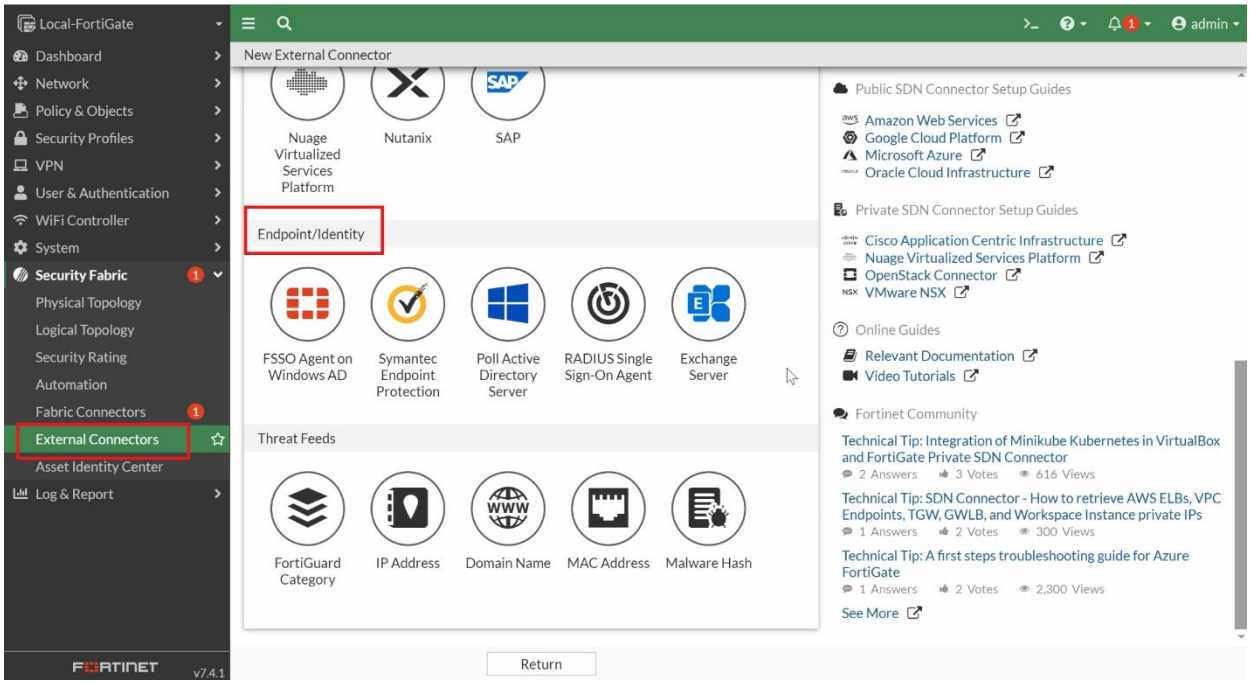
• The DC agent, when the user logs in, intercepts the login event on the domain controller. It then resolves the DNS of the client, and sends it to the collector agent. The collector agent receives the DNS and then performs a DNS resolution in order to check whether the IP address of the user has changed.

In DC Agent mode, **DC-Agent** is the responsible for DNS Resolution.

FSSO Configuration

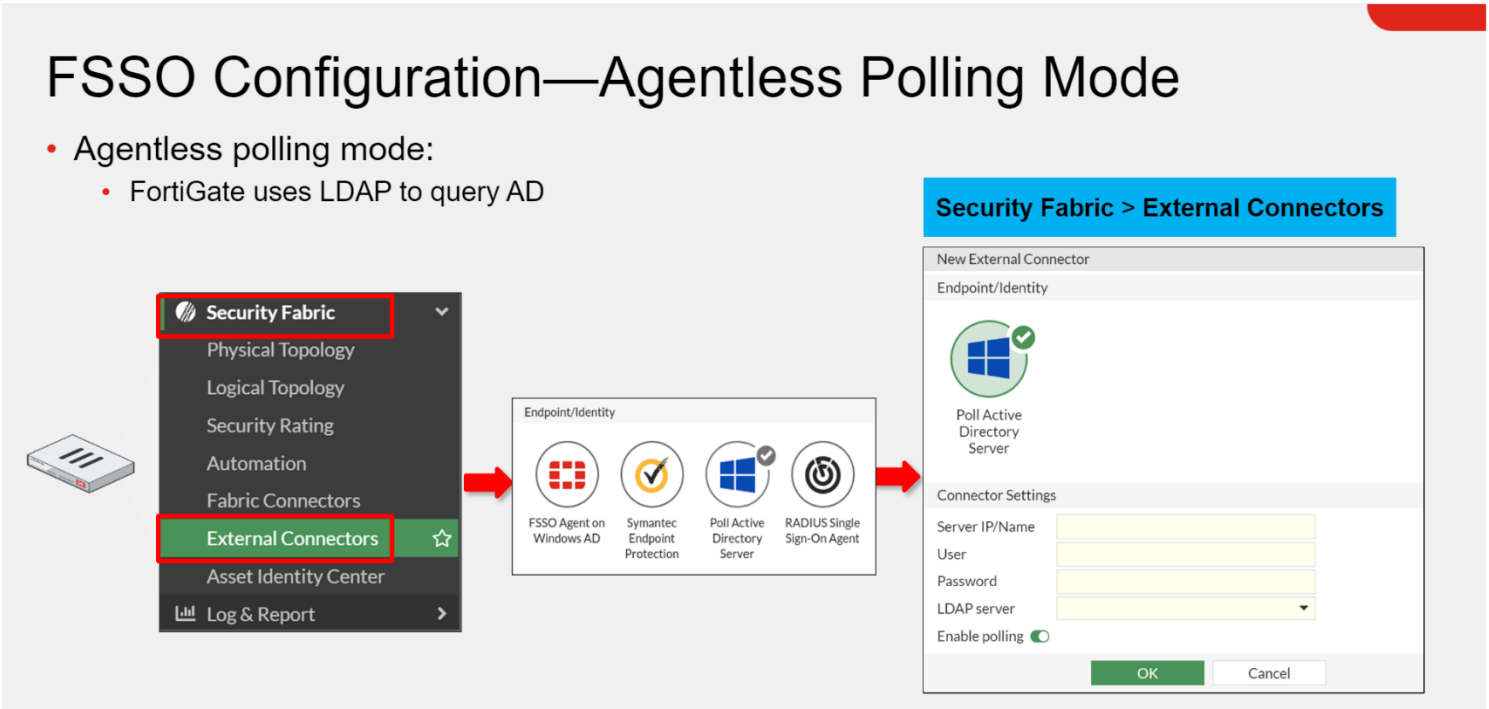
To configure FSSO on a FortiGate, go to ***Security Fabric*** **>** ***External Connectors***.

When creating a new connector, several options for connectors are available under **Endpoint/Identity**:



- **FSSO Agent on Windows AD**
  For most FSSO Agent-based deployments, this connector option will be used. Specify either Collector Agent or Local as User Group Source to collect user groups from the Collector Agent, or to match users to user groups from a LDAP server.
- **Poll Active Directory Server**
  This connection option directly polls Windows Security Event log entries on Windows DC for user log in information.
- **RADIUS Single Sign-On Agent**
  FortiGate can authenticate users who have authenticated on a remote RADIUS server by monitoring the RADIUS accounting records forwarded by the RADIUS server to the FortiGate.
- **Exchange Server connector**
  FortiGate collects information about authenticated users from corporate Microsoft Exchange Servers.
- **Symantec endpoint connector**
  This connector uses client IP information from Symantec Endpoint Protection Manager (SEPM) to assign dynamic IP addresses on FortiOS.

FSSO Configuration – Agentless Polling Mode



FortiGate FSSO configuration is straightforward.

If FortiGate is acting as a collector for agentless polling mode, you must select **Poll Active Directory Server** and configure the IP addresses and AD administrator credentials for each DC.

FortiGate uses **LDAP** to query AD to retrieve user group information. For this to happen, you must add the LDAP server to the **Poll Active Directory Server** configuration.

FSSO polling connector agent installation

This topic gives an example of configuring a local FSSO agent on the FortiGate. The agent actively pools Windows Security Event log entries on Windows Domain Controller (DC) for user log in information. The FSSO user groups can then be used in a firewall policy.

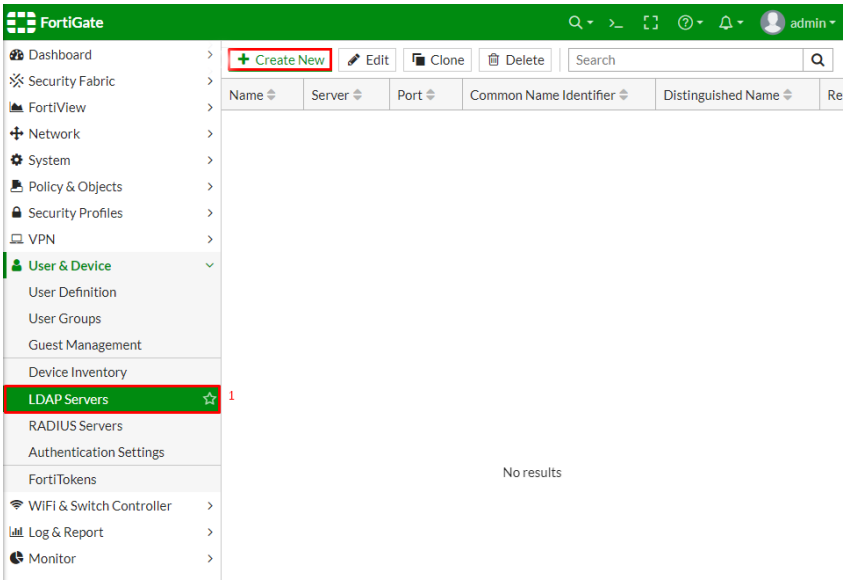
This method does not require any additional software components, and all the configuration can be done on the FortiGate.

To configure a local FSSO agent on the FortiGate:

1. **Configure an LDAP server on the FortiGate**
2. **Configure a local FSSO polling connector**
3. **Add the FSSO groups to a policy**

Configure an LDAP server on the FortiGate

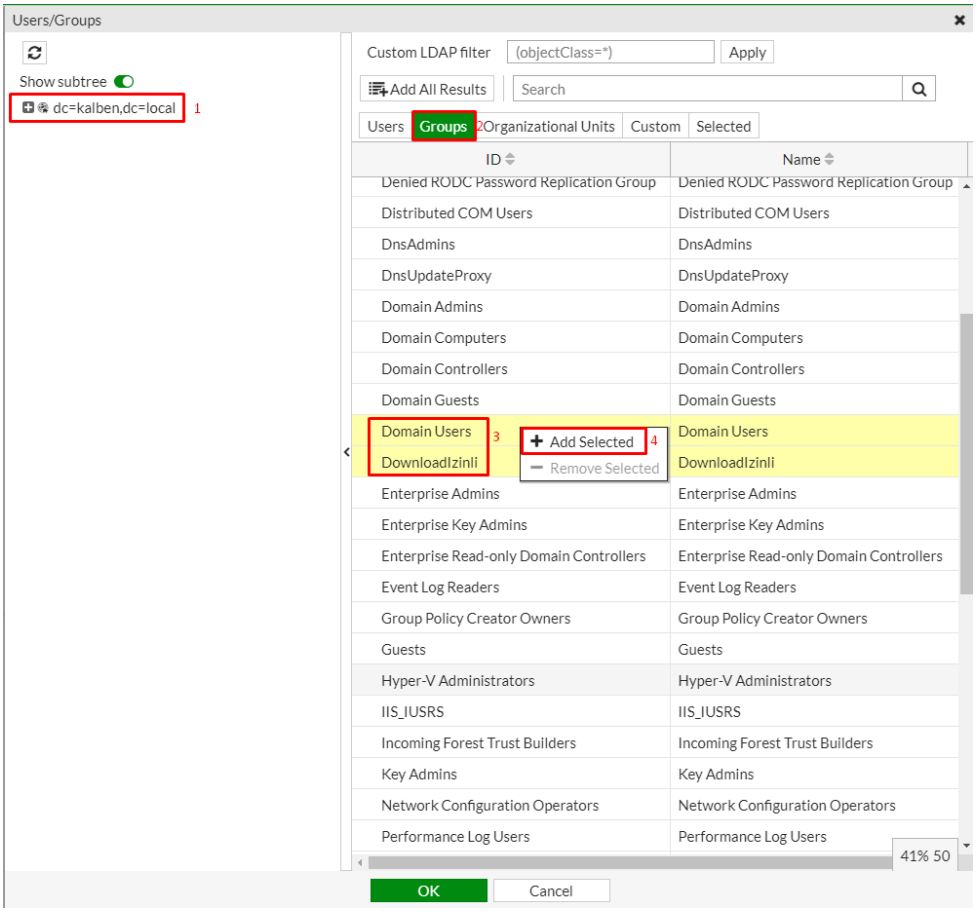
Refer to Configuring an LDAP server in my Firewall Authentication document. The connection must be successful before configuring the FSSO polling connector.

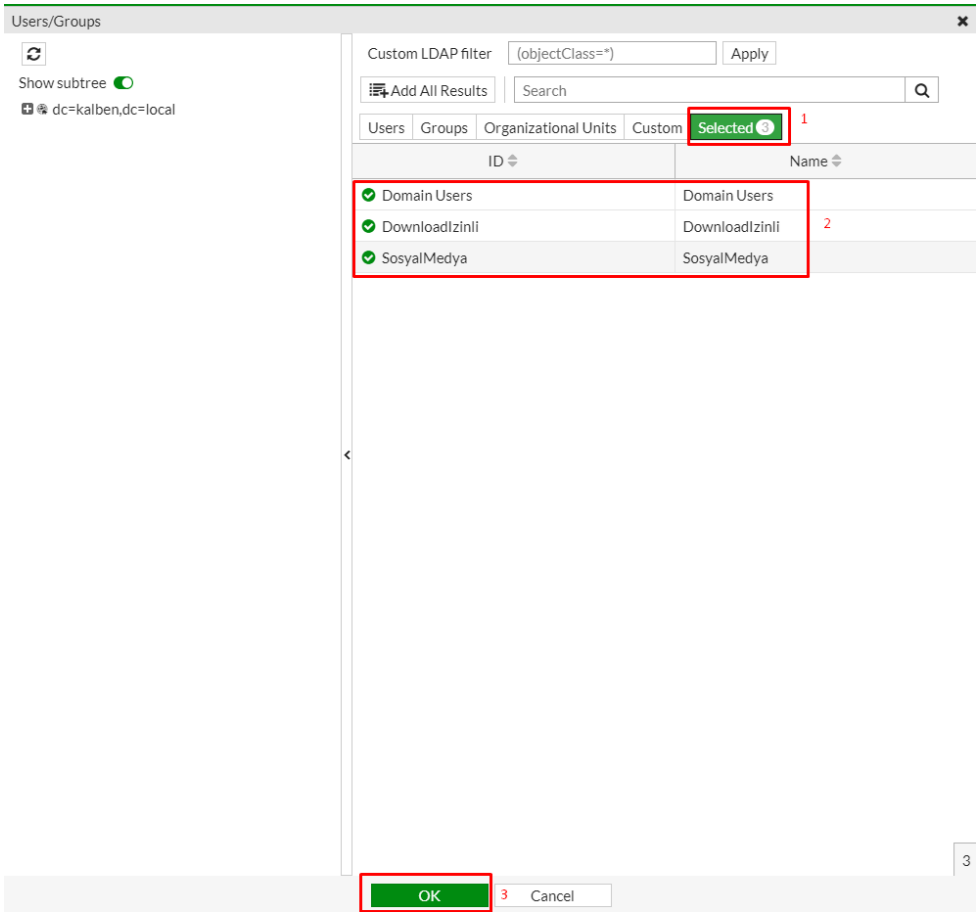


Configure a local FSSO polling connector

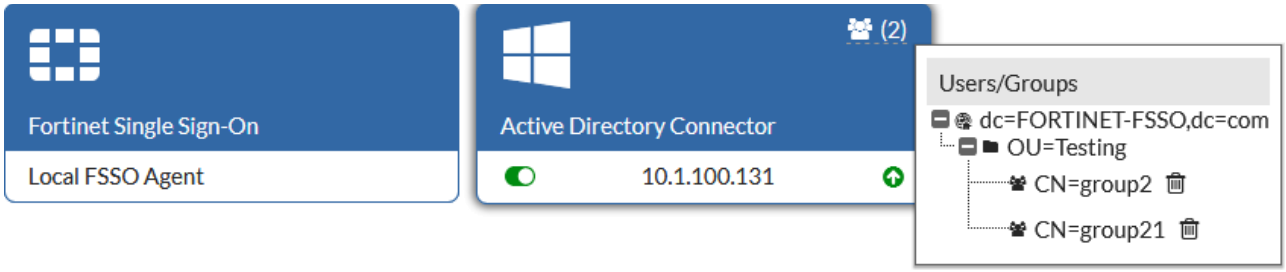
To configure a local FSSO polling connector:

1. Go to ***Security Fabric*** > ***External Connectors*** and click ***Create New***.
2. In the ***Endpoint/Identity*** section, select ***Poll Active Directory Server***.
3. Fill in the required information.
4. For ***LDAP Server***, select the server you just created.
5. Configure the group settings:
    1. For ***Users/Groups***, click ***Edit***. The structure of the LDAP tree is shown in the *Users/Groups* window.
    2. Click the ***Groups*** tab.
    3. Select the required groups, right-click on them, and select ***Add Selected***. Multiple groups can be selected at one time by holding the CTRL or SHIFT keys. The groups list can be filtered or searched to limit the number of groups that are displayed.
    4. Click the ***Selected*** tab and verify that the required groups are listed. To remove a group, right-click and select *Remove Selected*.
    5. Click *OK* to save the group settings.


Users/Groups
Show subtree
dc=kalben,dc=local
1
Custom LDAP filter
(objectClass=*)
Apply
Add All Results
Search
Users
Groups
2Organizational Units
Custom
Selected
ID
Name
Denied RODC Password Replication Group
Distributed COM Users
DnsAdmins
DnsUpdateProxy
Domain Admins
Domain Computers
Domain Controllers
Domain Guests
Domain Users
3
Add Selected
4
Remove Selected
DownloadIzinli
Enterprise Admins
Enterprise Key Admins
Enterprise Read-only Domain Controllers
Event Log Readers
Group Policy Creator Owners
Guests
Hyper-V Administrators
IIS_IUSRS
Incoming Forest Trust Builders
Key Admins
Network Configuration Operators
Performance Log Users
41% 50
OK
Cancel


Users/Groups
Show subtree
dc=kalben,dc=local
Custom LDAP filter
(objectClass=*)
Apply
Add All Results
Search
Users
Groups
Organizational Units
Custom
Selected
1
ID
Name
Domain Users
DownloadIzinli
SosyalMedya
2
3
OK
3
Cancel

6. Click ***OK*** to save the connector settings.
7. Go back to ***Security Fabric*** > ***External Connectors***.
8. There should be two new connectors:



- The ***Local FSSO Agent*** is the backend process that is automatically created when the first FSSO polling connector is created.
- The ***Active Directory Connector*** is the front-end connector that can be configured by FortiGate administrators.

To verify the configuration, hover the cursor over the top right corner of the connector; a popup window will show the currently selected groups. A successful connection is also shown by a green up arrow in the lower right corner of the connector.

If you need to get log in information from multiple DCs, then you must configure other Active Directory connectors for each additional DC to be monitored.

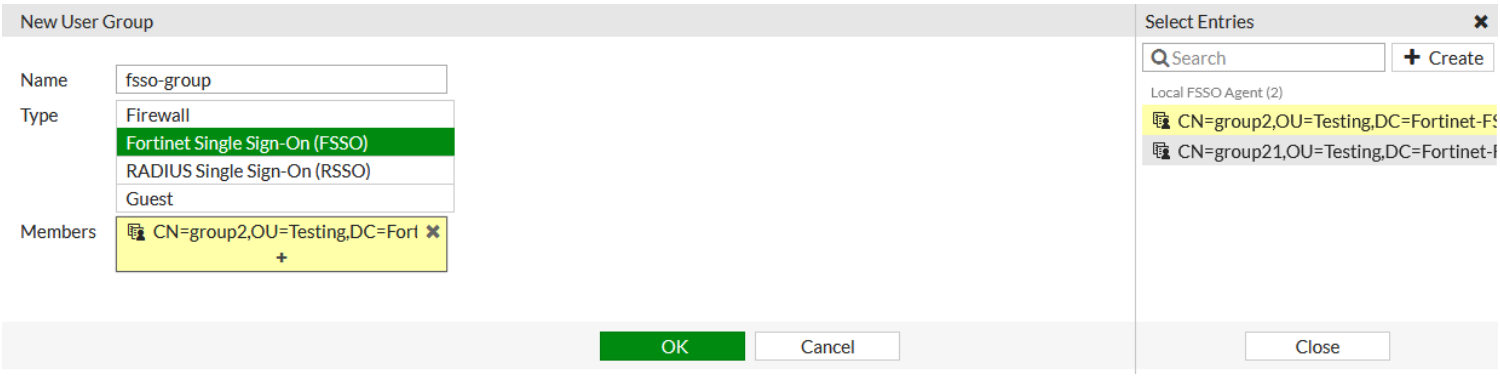
Add the FSSO groups to a policy

FSSO groups can be used in a policy by either:

- **adding them to the policy directly**, or
- **by adding them to a local user group and then adding the group to a policy**.

To add the FSSO groups to a local user group:

1. Go to ***User & Authentication*** **>** ***User Groups*** and click ***Create New***.
2. Enter a name for the group in the ***Name*** field.
3. Set the ***Type*** to ***Fortinet Single Sign-On (FSSO)***.
4. In the ***Members*** field, click the ***+*** and add the FSSO groups.



5. Click ***OK***.
6. Add the local FSSO group to a policy.

To add the FSSO groups directly to a firewall policy:

1. Go to ***Policy & Objects*** > ***Firewall Policy*** and click ***Create New***.
2. In the ***Source*** field, click the +. In the *Select Entries* pane, select the ***User*** tab.
3. Select the FSSO groups.
4. Configure the remaining settings as required.
5. Click ***OK***.

Troubleshooting

If an authenticated AD user cannot access the internet or pass the firewall policy, verify the local FSSO user list:

```
# Diagnose debug authd fsso list
----FSSO logons----
IP: 10.1.100.188 User: test2 Groups: CN=group2,OU=Testing,DC=Fortinet-
FSSO,DC=COM Workstation: MemberOf: CN=group2,OU=Testing,DC=Fortinet-
FSSO,DC=COM
Total number of logons listed: 1, filtered: 0
----end of FSSO logons----
```

1. Check that the group in ***MemberOf*** is allowed by the policy.
2. If the expected AD user is not in list, but other users are, it means that either:
   - The FortiGate missed the log in event, which can happen if many users log in at the same time, or
   - The user's workstation is unable to connect to the DC, and is currently logged in with cached credentials, so there is no entry in the DC security event log.

3. If there are no users in the local FSSO user list:

A. Ensure that the local FSSO agent is working correctly:

```
# diagnose debug enable
# diagnose debug authd fsso server-status
```

```
Server Name                          Connection Status    Version            Address
-----------                          -----------------    -------            -------
FGT_A (vdom1) # Local FSSO Agent        connected      FSAE server 1.1      127.0.0.1
```

The connection status must be `connected`.

B. Verify the Active Directory connection status:

```
# diagnose debug fsso-polling detail 1
AD Server Status (connected):
ID=1, name(10.1.100.131),ip=10.1.100.131,source(security),users(0)
port=auto username=Administrator
read log eof=1, latest logon timestamp: Fri Jul 26 10:36:20 2019

polling frequency: every 10 second(s) success(274), fail(0)
LDAP query: success(0), fail(0)
LDAP max group query period(seconds): 0
LDAP status: connected

Group Filter: CN=group2,OU=Testing,DC=Fortinet-
FSSO,DC=com+CN=group21,OU=Testing,DC=Fortinet-FSSO,DC=COM
```

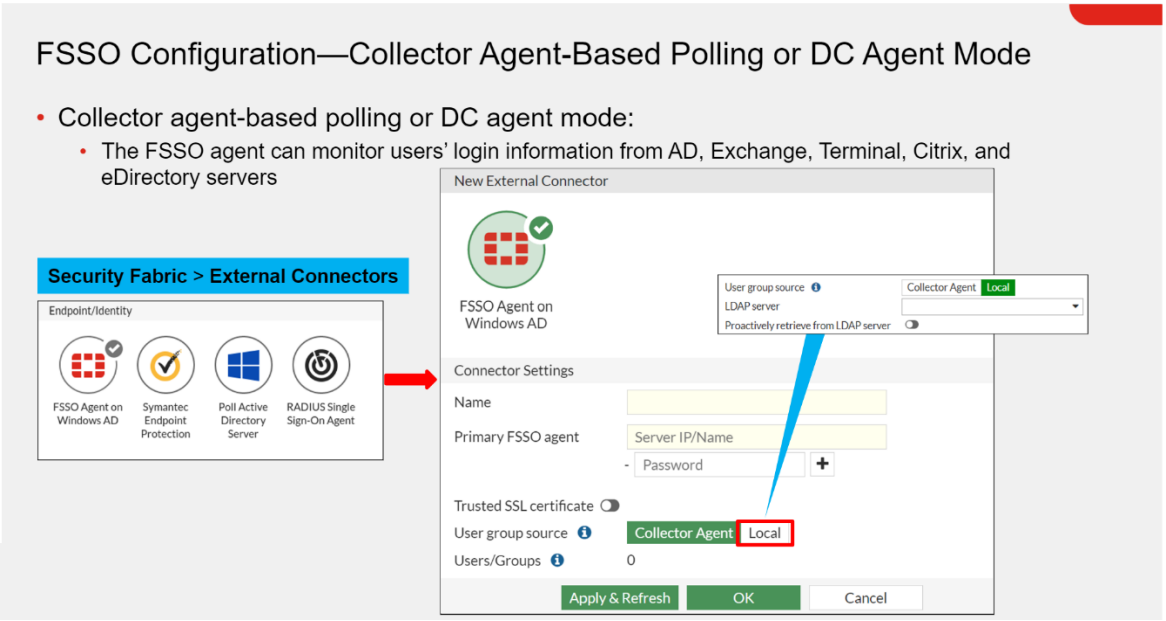
If the polling frequency shows successes and failures, that indicates sporadic network problems or a very busy DC. If it indicates no successes or failures, then incorrect credentials could be the issue.

If the LDAP status is connected, then the FortiGate can access the configured LDAP server. This is required for AD group membership lookup of authenticated users because the Windows Security Event log does not include group membership information. The FortiGate sends an LDAP search for group membership of authenticated users to the configure LDAP server.

FortiGate adds authenticated users to the local FSSO user list only if the group membership is one of the groups in Group Filter.

FSSO Configuration

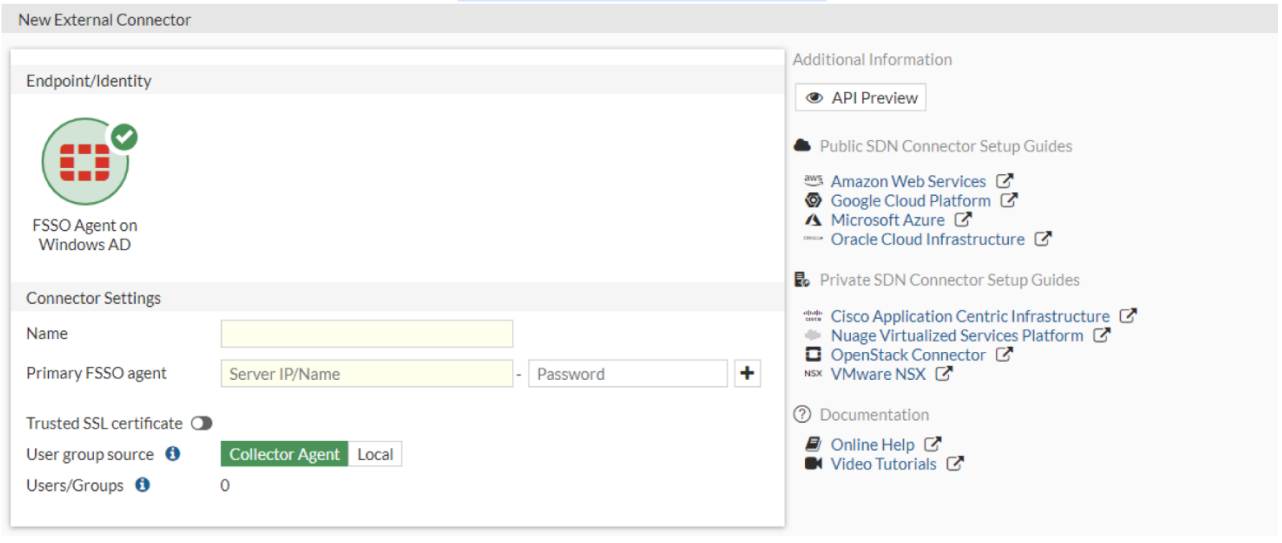
Collector Agent-Based Polling or DC Agent Mode



If you have collector agents, using either the DC agent mode or the collector agent-based polling mode, you must select **FSSO Agent on Windows AD** and configure the IP address and password for each collector agent. (Maybe you have more than on Collector Agent for Redundancy)

To create an FSSO agent connector in the GUI:

1. Go to ***Security Fabric*** > ***External Connectors***.
2. Click ***Create New***.
3. In the Endpoint/Identity section, click **FSSO Agent on Windows AD**.



4. Fill in the ***Name***
5. Set the ***Primary FSSO Agent*** to the **IP address of the FSSO Collector Agent**, and enter its **password**
6. Optionally, add more FSSO agents by clicking the plus icon.
7. Optionally, enable ***Trusted SSL certificate*** and select or import a certificate.
8. Select the ***User group source***: ***Collector Agent*** ***or*** ***Local***

The **FSSO Collector Agent** can access Windows AD in one of two modes:

• **Collector Agent:** You create group filters on the collector agent. You can set FortiGate to Collector Agent mode, and the collector agent can still use Advanced mode to access nested groups. ➔ User groups will be pushed to the FortiGate from the collector agent.

• **Local:** You create group filters on FortiGate, using the LDAP server. If you set FortiGate to Local mode, you must set the collector agent to Advanced mode, otherwise the collector agent does not recognize the group filter sent by FortiGate and does not pass down any user logins. ➔ User groups will be specified in the FortiGate unit's configuration.

9. Click *OK*.

Local

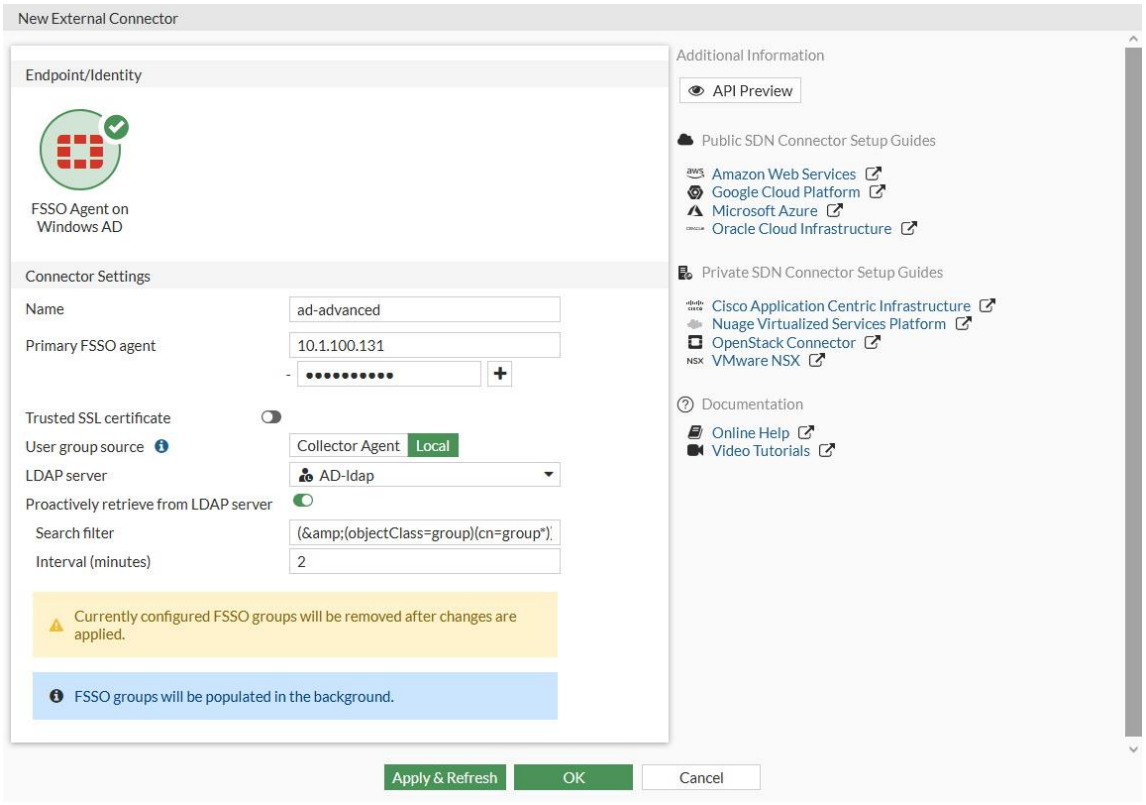
Create the FSSO collector that updates the AD user groups list

To create an FSSO agent connector in the GUI:

1. Go to *Security Fabric > External Connectors*.
2. Click *Create New*.
3. In the *Endpoint/Identity* section, click *FSSO Agent on Windows AD*.
4. Fill in the *Name*
5. Set the *Primary FSSO Agent* to the IP address of the FSSO Collector Agent, and enter its password.
6. Set the *User Group Source* to ***Local***.
7. Set the *LDAP Server* to one you created before. (*AD-ldap* server)
8. Enable *Proactively Retrieve from LDAP Server*.
9. Set the *Search Filter* to *(&(objectClass=group)(cn=group*))*.

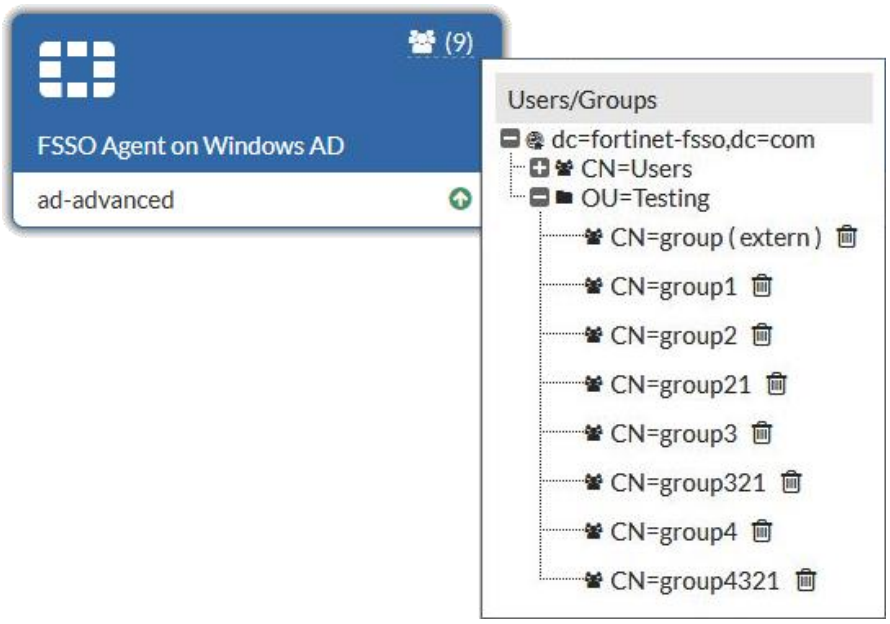
The default search filter retrieves all groups, including Microsoft system groups. In this example, the filter is configured to retrieve *group1*, *group2*, etc, and not groups like *grp199*.
The filter syntax is not automatically checked; if it is incorrect, the FortiGate might not retrieve any groups.

10. Set the *Interval (minutes)* to configure how often the FortiGate contacts the remote AD LDAP server to update the group information.



11. Click *OK*.

12. To view the AD user groups that are retrieved by the FSSO agent, hover the cursor over the group icon on the fabric

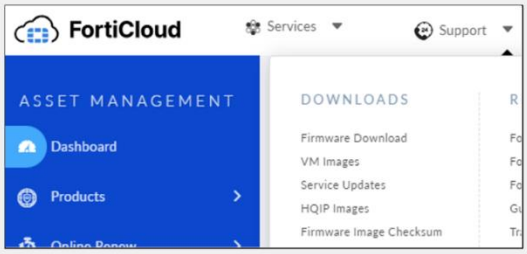


FSSO Agent Installation

FSSO Agent Installation

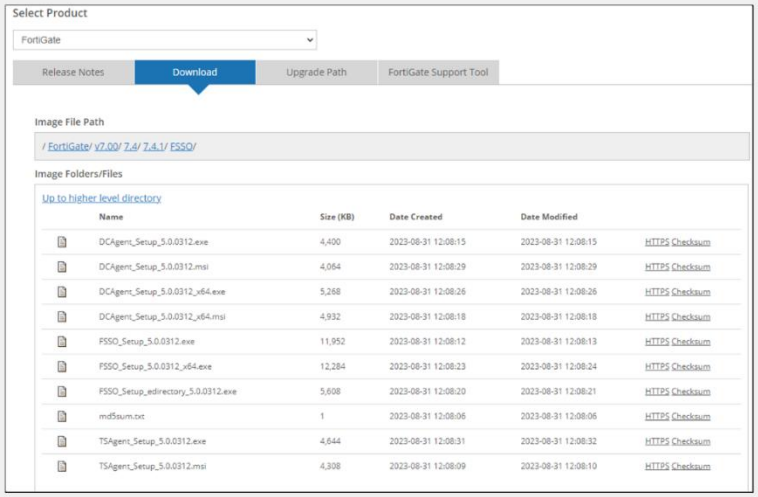
1. Visit the Fortinet support website:
   - https://support.fortinet.com
2. Click **Support** > **Firmware Download**
3. Select **FortiGate**, then click **Download**.
4. Click **v7.00** > **7.4** > **7.4.1** > **FSSO**

   Example image below:



Available agents:

- DC agent: DCAgent_Setup
- CA for Microsoft servers: FSSO_Setup
- CA for Novell: FSSO_Setup_edirectory
- TS Agent: TSAgent_Setup



The FSSO agents are available on the **Fortinet Support website**. **(https://support.fortinet.com)**

There you will find the following:

- The DC agent (DCAgent_Setup)
- The collector agent for Microsoft servers: FSSO_Setup
- The collector agent for Novell directories: FSSO_Setup_edirectory
- The terminal server agent (TSagent) installer for Citrix and terminal servers: TSAgent_Setup

Also, for each agent, there are two versions:

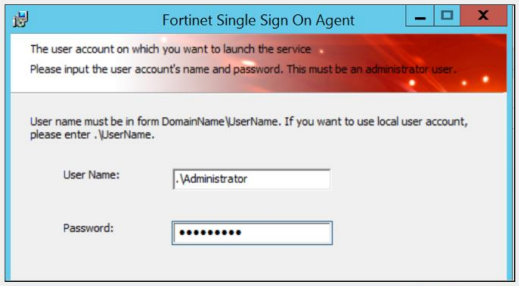
- the executable (.exe)
- Microsoft Installer (.msi)

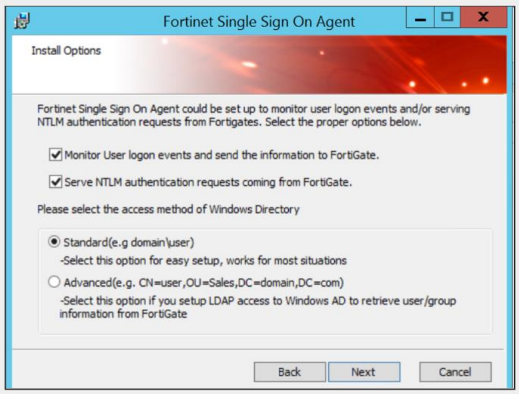
Notice that <u>you do not need</u> to match the FSSO version with your exact FortiGate firmware version. When installing FSSO, grab the latest collector agent for your major release. <u>You do however, need</u> to match the DC agent version to the collector agent version.

FSSO Collector Agent Installation Process

FSSO Collector Agent Installation Process

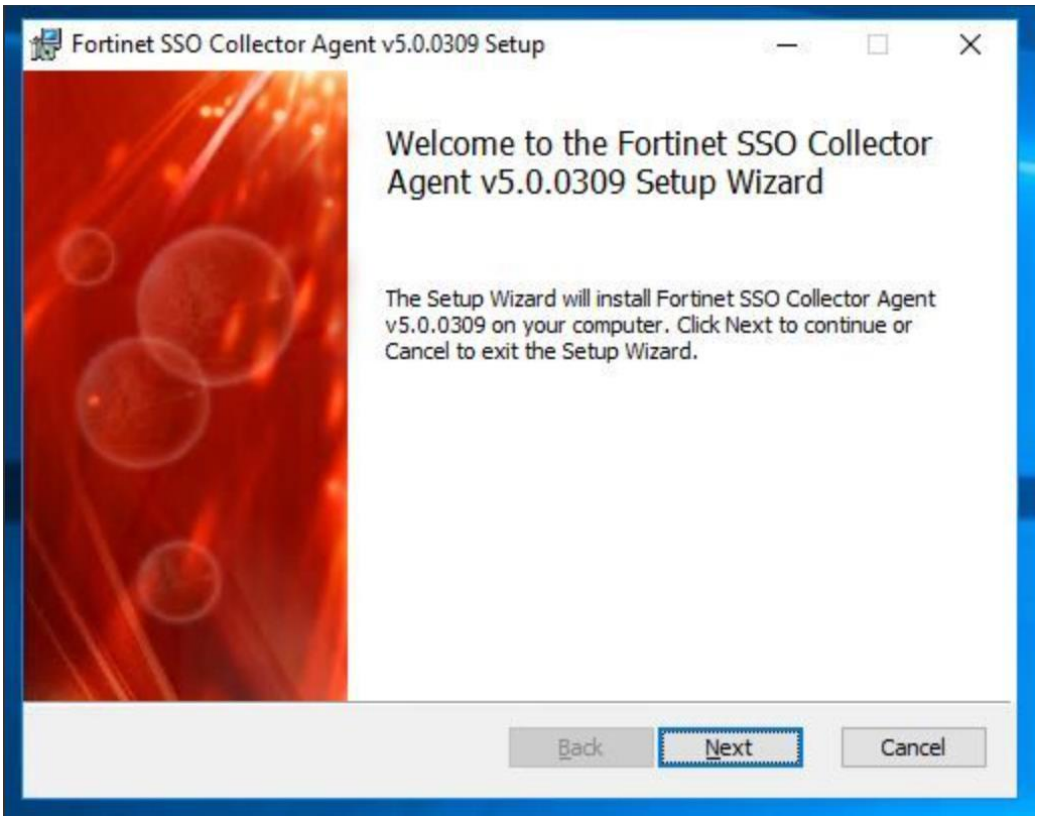
1. Run the installation process as `Administrator`
2. Enter the user name in the following format:
   - `DomainName\UserName`
3. Configure the collector agent for:
   - Monitoring logins
   - NTLM authentication
   - Directory access
4. Optionally, launch the DC agent installation wizard before exiting the collector agent installation wizard

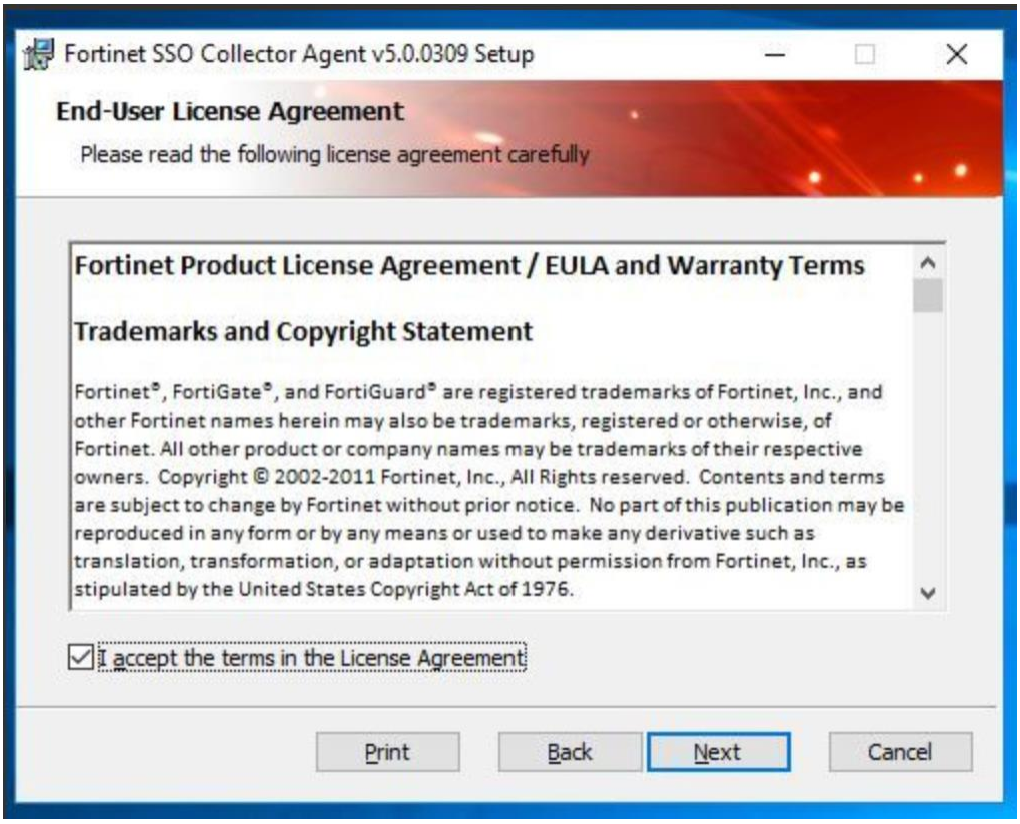




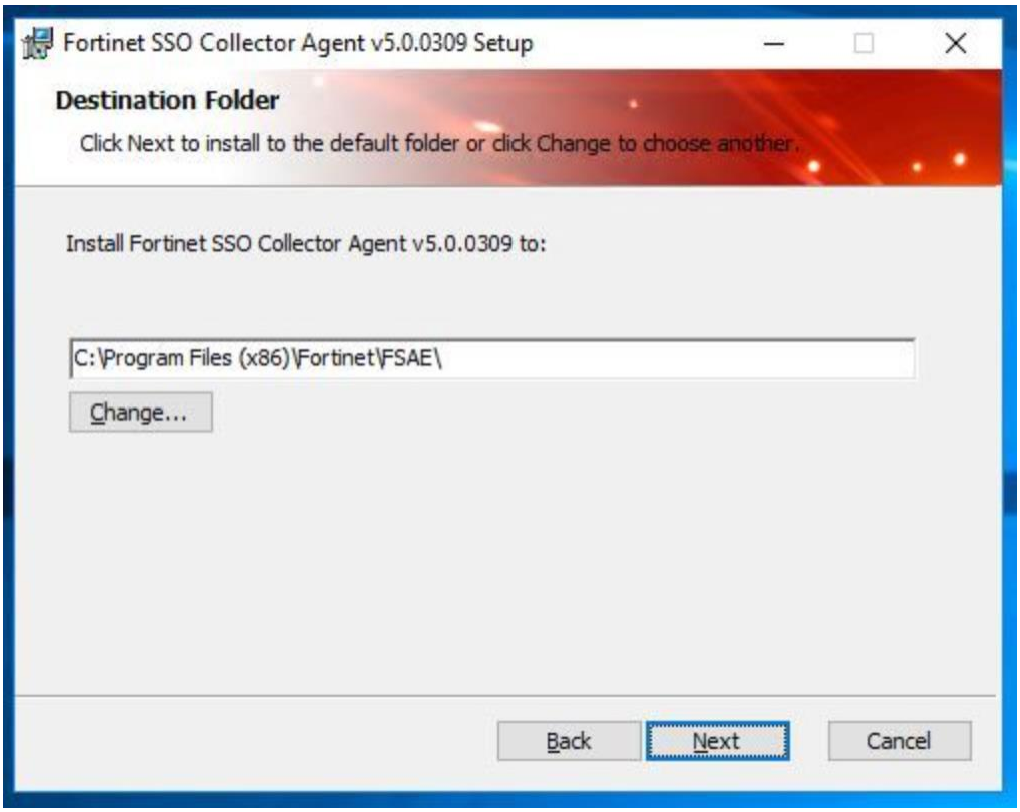
After you've downloaded the **collector agent**, run the installation process as Administrator and follow these steps in the installation wizard: (Run the FSSO_Setup file with administrator privileges)

1. Read and accept the license agreement.

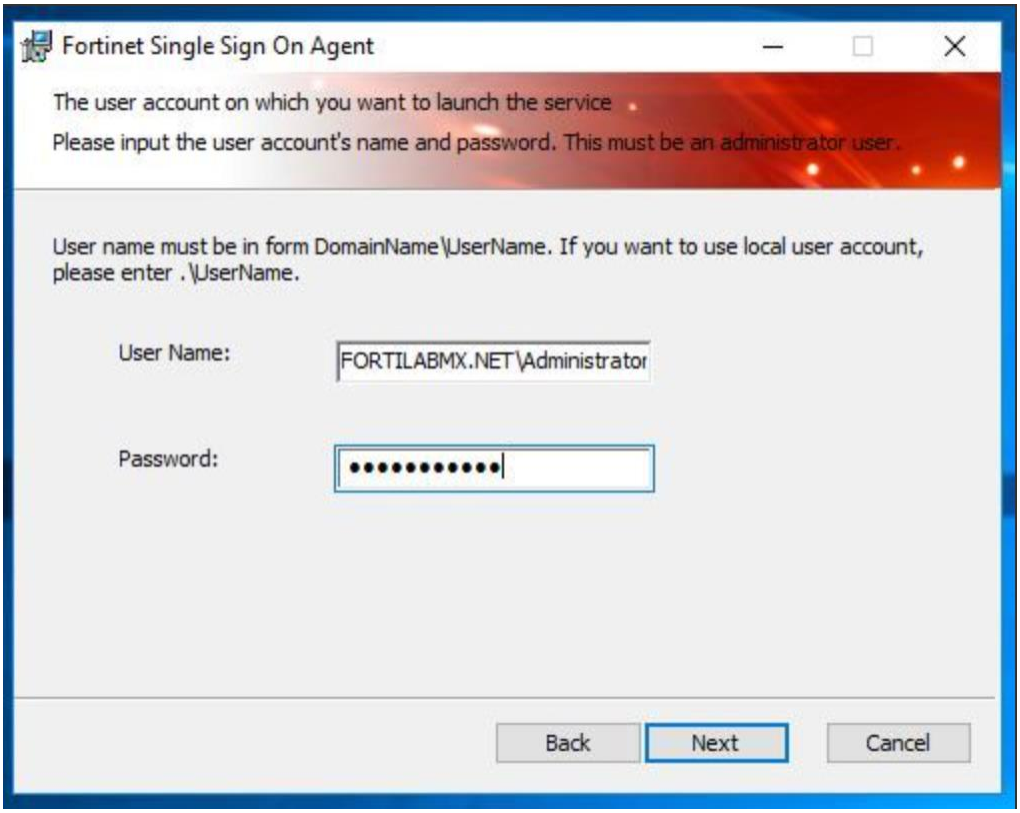




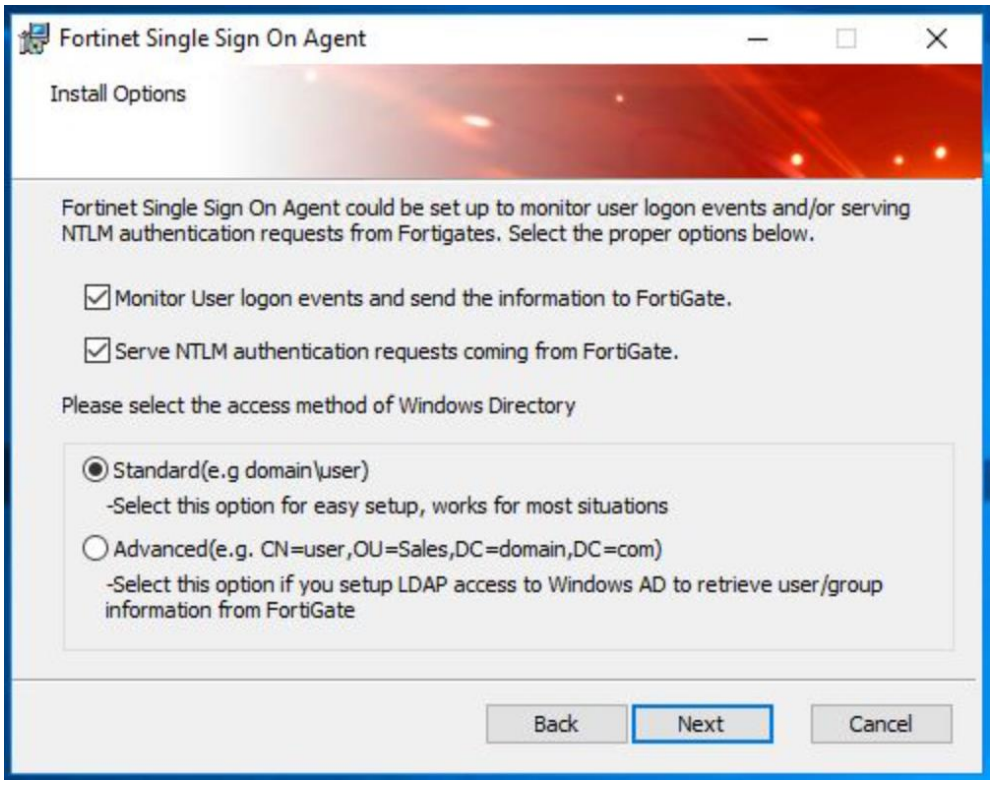
2. Optionally, change the installation location. The default folder is named **FSAE** (Fortinet Server Authentication Extension).



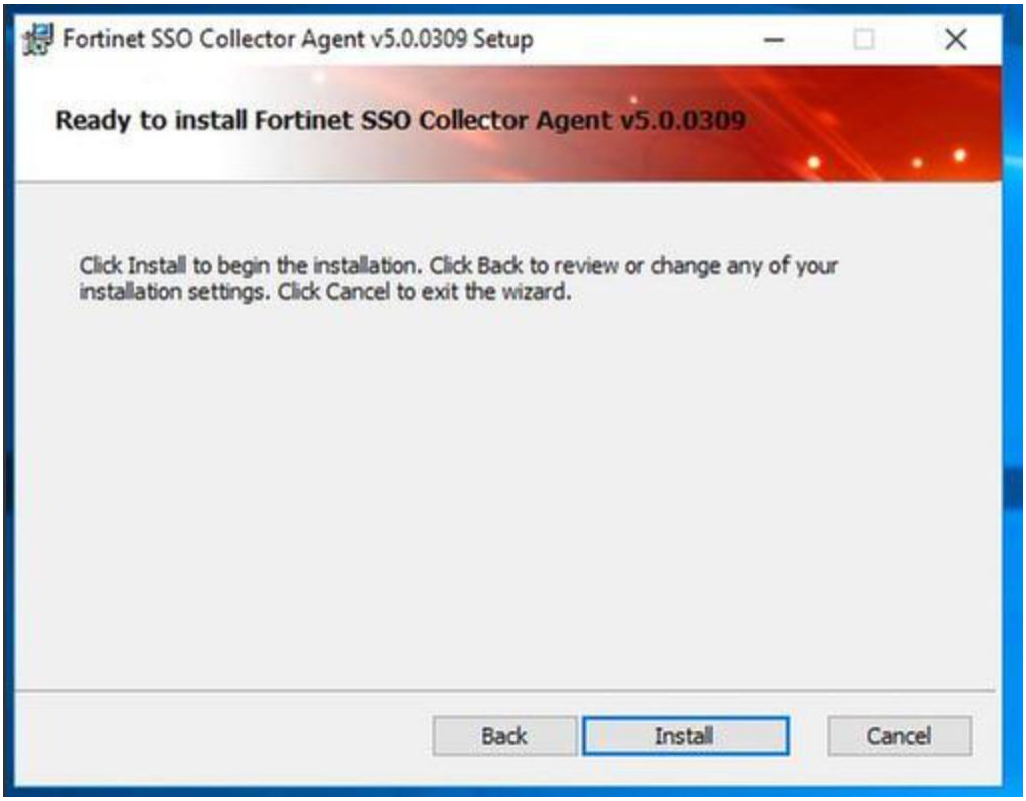
3. Enter the username. By default, the agent uses the name of the currently running account; however, you can change it using the format: DomainName\UserName.

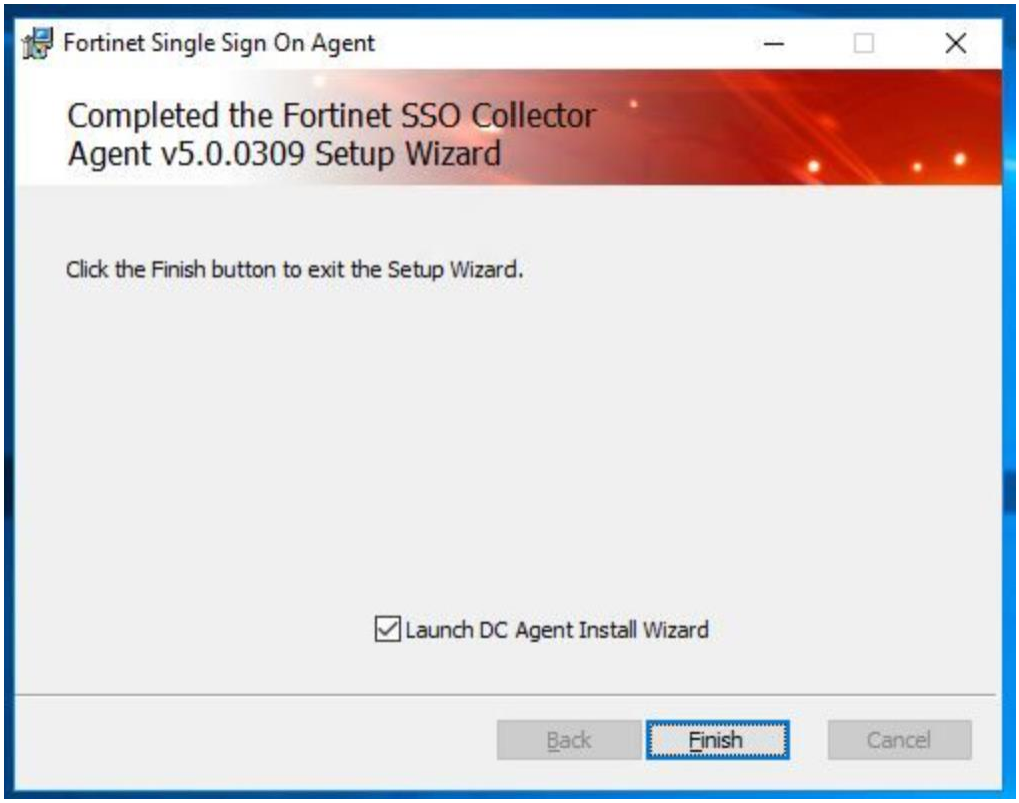


4. Alternatively, configure your collector agent for monitoring, NTLM authentication, and directory access. These options are also customizable after installation. **Although the default is Standard mode**, when doing new FSSO setups it is always a best practice to install in **Advanced mode**. You will look at some of the advantages in this document.

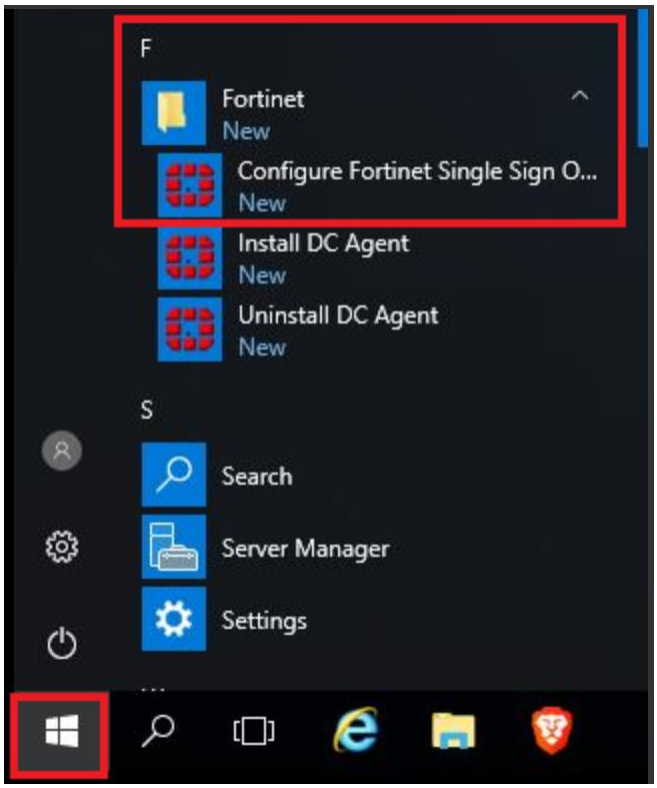


5. If you want to use **DC agent mode**, make sure that Launch DC Agent Install Wizard is selected. This automatically starts the DC agent installation.

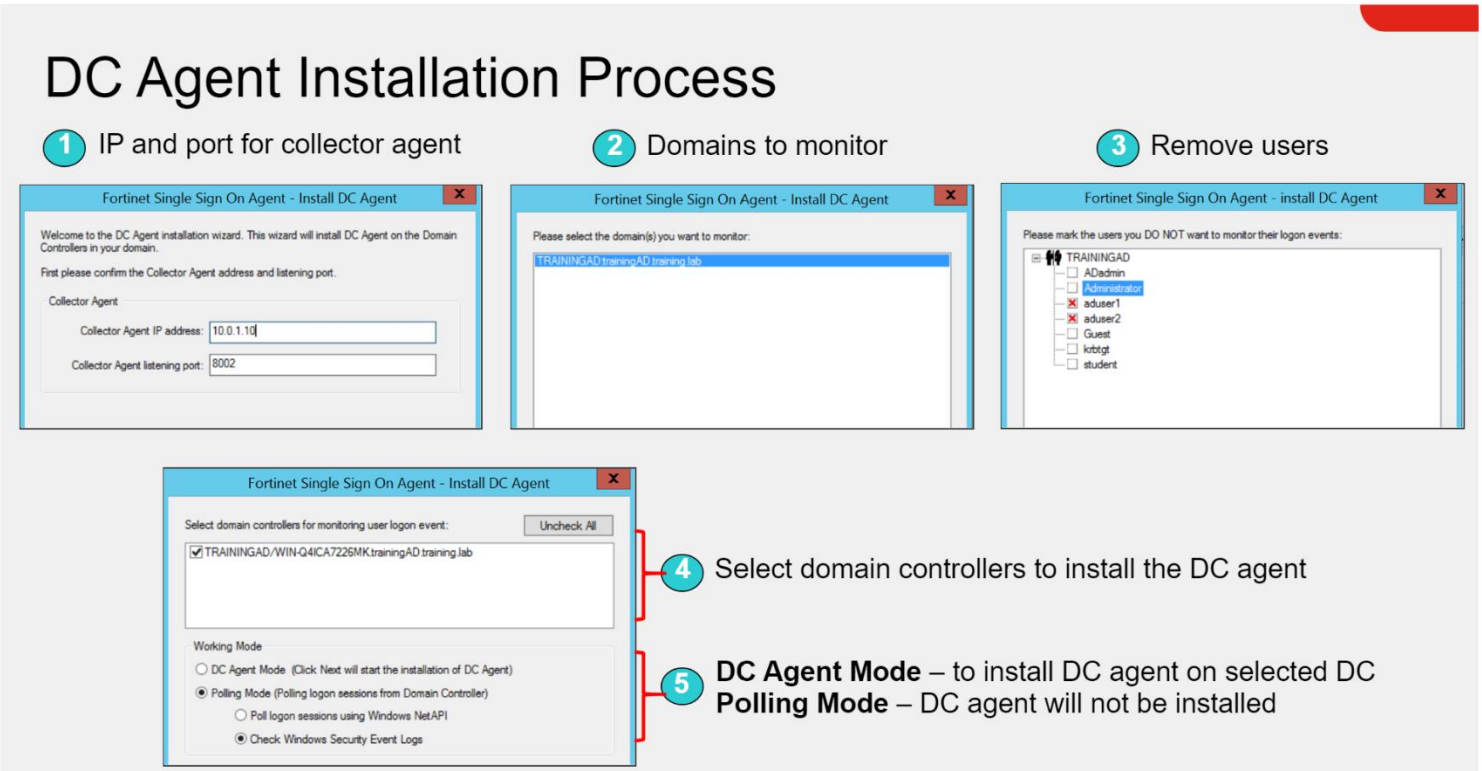




FSSO-CA is installed in the server and can be found in the following directory:

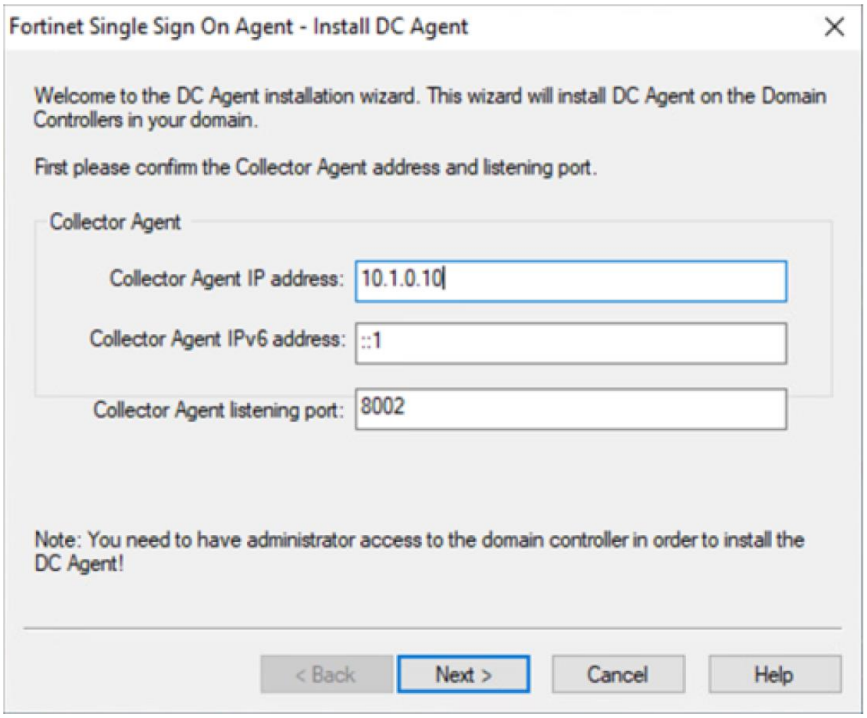


DC Agent Installation Process



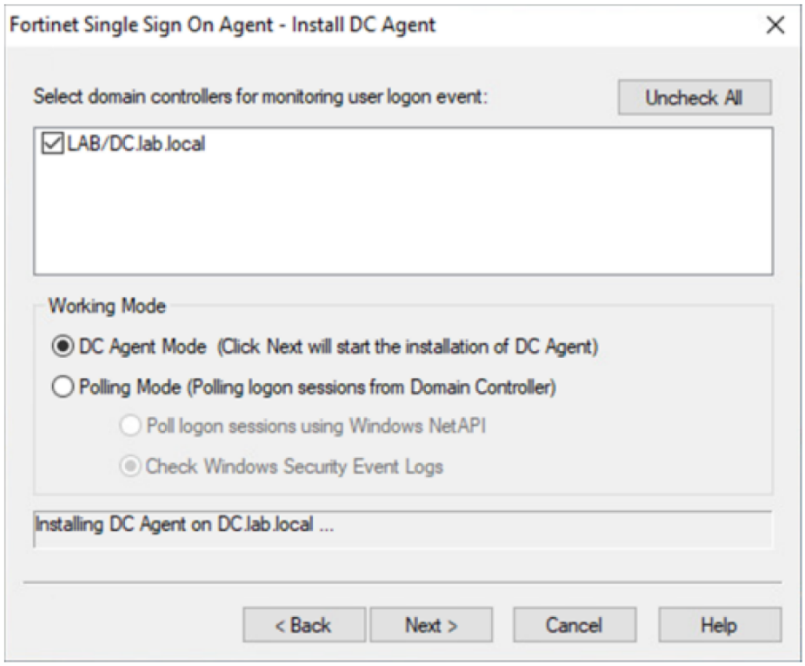
If you have just installed the **collector agent** and you selected **Launch DC Agent Install Wizard**, the installation process for domain controller agent (DC Agent) automatically starts.

1. Enter the IP address for the collector agent. Optionally, you can customize the listening port, if the default value is already used by another service.



2. Select the **domains** to monitor. If any of your required domains are not listed, you should check 2 settings:

- Cancel the wizard and set up the correct trusted relationship with the domain controller. Then, run the wizard again.
- Note that this could also be a result of using an account without all the necessary permissions.



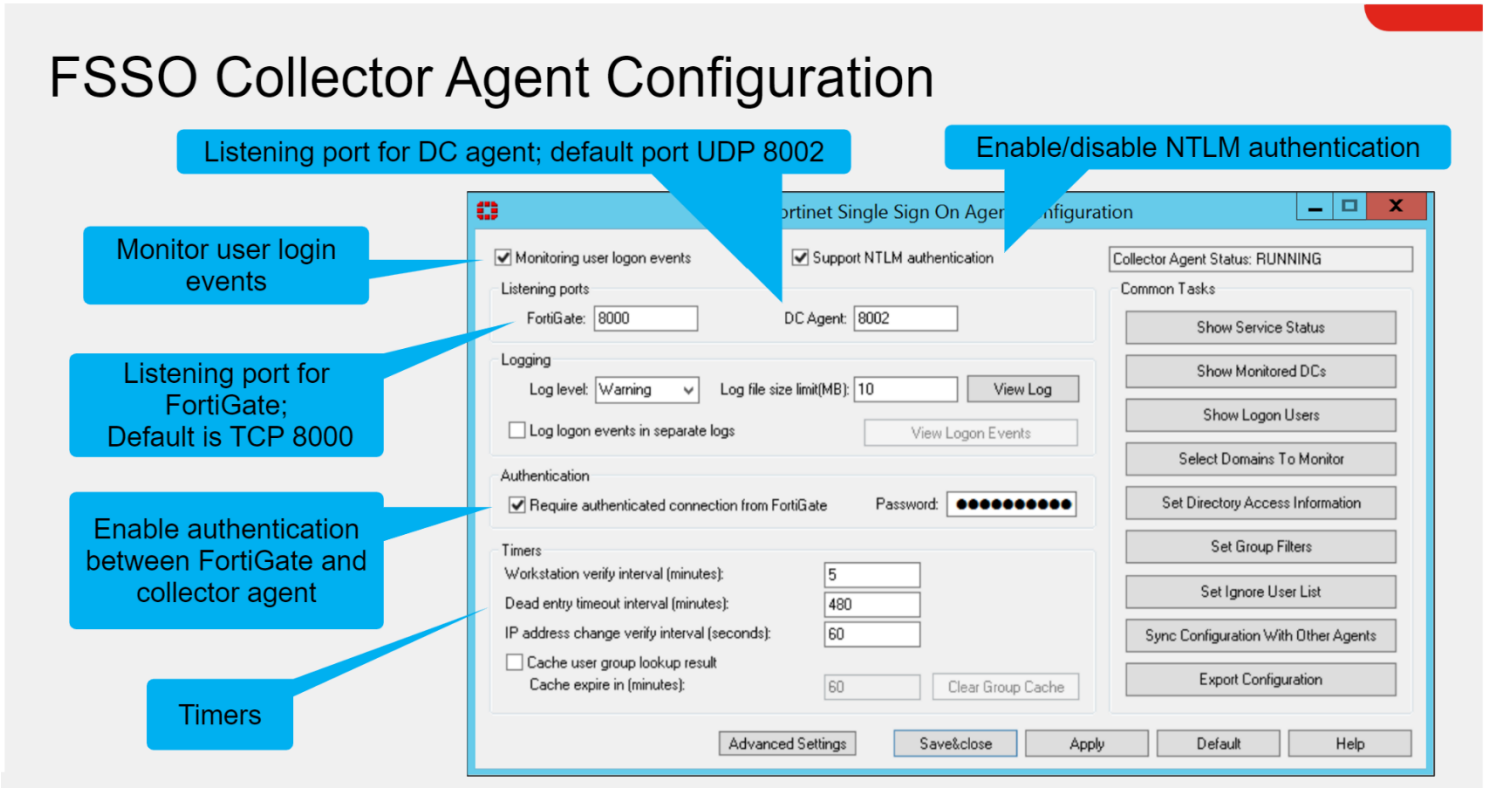
3. Optionally, select users that you do not want to monitor; these users' login events are not recorded by the collector and therefore are not passed to FortiGate. While these users are still able to generate login events to the domain, when they are detected by the collector agent, they are discarded so as to not interfere with the logged in user. This is especially useful in environments with a centrally managed antivirus solution, or a scheduled backup service that uses an AD account to start. These accounts can create login events for the collector agent that overwrite existing user logins. This may result in FortiGate applying the incorrect policies and profiles based on the overriding account. You can also customize the option to ignore users after installation is complete.

4. Optionally, clear the checkboxes of domain controllers that you don't want to install the DC agent on**. Remember, for DC agent mode FSSO, at least one domain controller must have the DC agent installed**. Also remember that installing the DC agent requires a reboot of the DC before it will start gathering login events. You can add or remove the DC agent to DCs at any time after the installation is complete.

5. Select **DC Agent Mode** as the working mode. If you select **Polling Mode**, the DC agent will not be installed.

Finally, the wizard requests a system reboot.

FSSO Collector Agent Configuration



On the FSSO agent configuration GUI, you can configure settings such as:

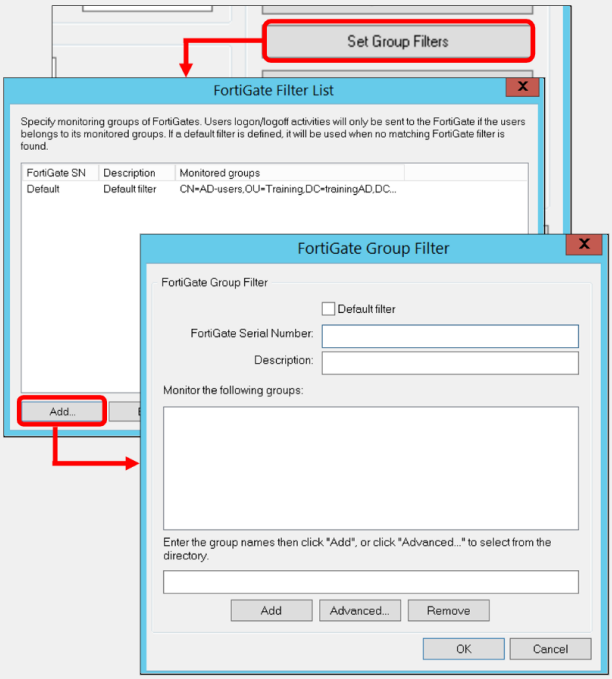
- The listening port for the communication with the DC agents (UDP)
- The listening port for the communication with FortiGate (TCP)
- NTLM authentication support
- Password authentication between the collector agent and FortiGate
- Timers

➔ I want to explain some of the Collector Agent's options.

Group Filter

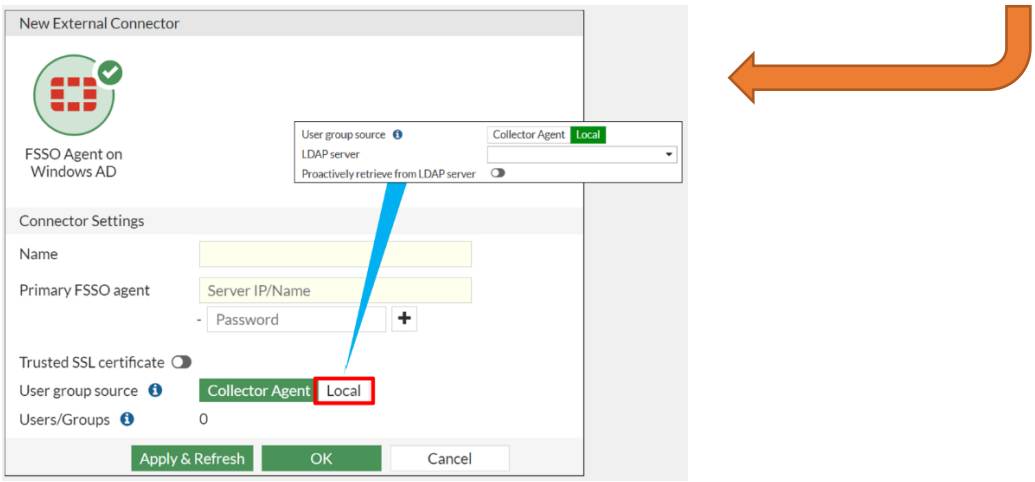
Group Filter

- The FSSO collector agent manages FortiGate group filters
- FortiGate group filters control which user's login information is sent to that FortiGate device
  - Filters are tied to the FortiGate serial number
- You can set filters for groups, OUs, users, or a combination



When configuring FSSO, administrators have the ability to specify which user groups will be monitored by FSSO.

The **Group Filter** can be defined either locally on FortiGate or directly on FSSO Collector Agent.



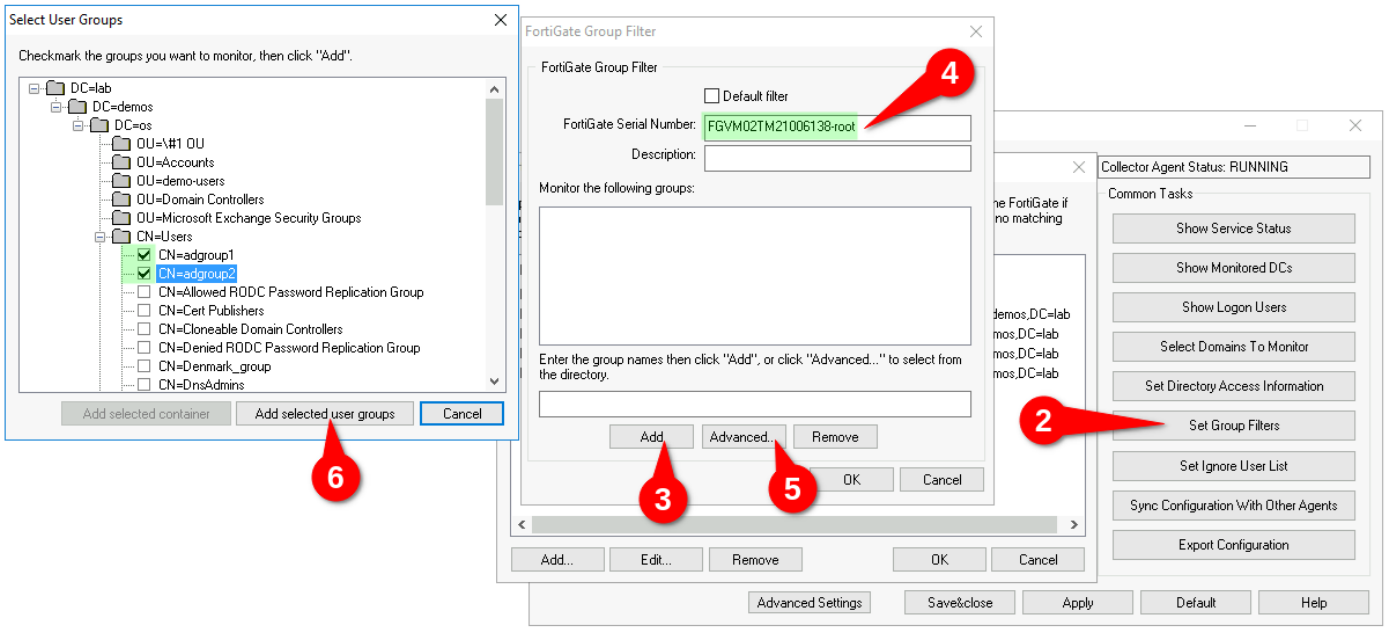
While in general the group filter should be defined locally on FortiGate, there are situations where the group filter needs to be defined on the FSSO Collector Agent.

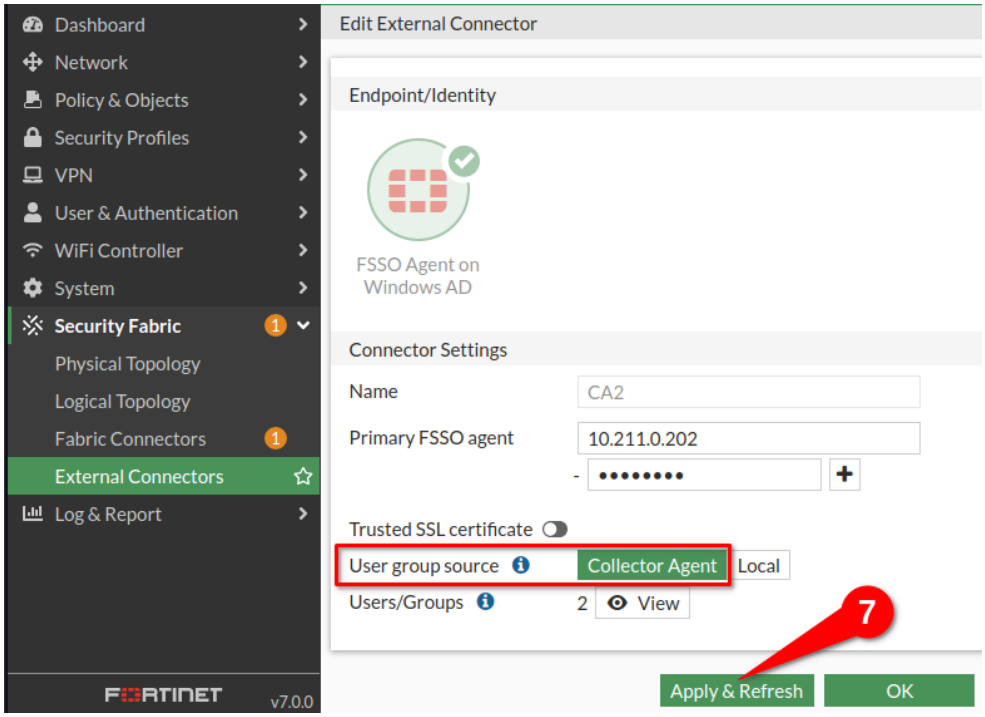
The most common use cases for group filters defined on Collector Agent are:

- FortiGate does not have connectivity to the LDAP server. (We cannot select **Local** option)
- The Collector Agent will be serving many FortiGates, each with an identical group filter.

Configuration:

1. Open FSSO Collector Agent Configuration Utility.
2. Select the '**Set Group Filter**' button.
3. Select the '**Add**' button to create a new group filter.
4. Type the Serial Number and VDOM name of the FortiGate into the FortiGate Serial Number field. This value must be specified in format **<SN>-<VDOM>**.
   Note: VDOM name 'root' has to be specified even when VDOM functionality is not enabled on the target FortiGate.
5. Select the '**Advanced**' button to open the LDAP tree browser.
6. Select user groups to monitor by FSSO and confirm the selection by selecting '**Add selected user groups**'.
   Note: It is necessary to select the Organizational Units icons in order to expand the LDAP tree.
7. To reflect the change on FortiGate, navigate to Security Fabric > External Connectors > [the FSSO Collector], ensure the User group source is set to **Collector Agent**, and select the 'Apply&Refresh' button.





‘Group Filter’ Overview:

The FSSO collector agent allows you to configure a FortiGate group filter, which actively controls what user login information is sent to each FortiGate device. So, you can define which groups the collector agent passes to individual FortiGate devices.

Monitoring the entire group list in a large AD structure is highly inefficient, and a waste of resources. Most FSSO deployments need group segmentation (at least four or five groups), with the intention of assigning varying levels of security profile configurations to the different groups, using identity-based policies.

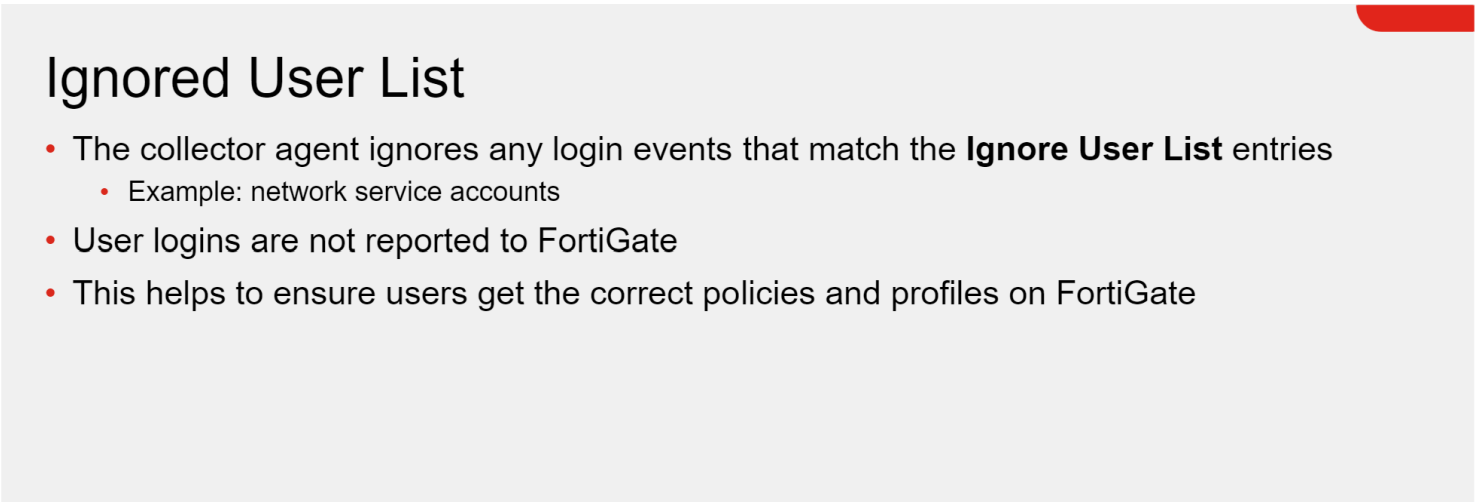
Group filters also help to limit the traffic sent to FortiGate. The maximum number of Windows AD user groups allowed on FortiGate depends on the model. Low-end FortiGate models support **256** Windows AD user groups. Mid-range and highend models can support **more groups**. This is per VDOM, if VDOMs are enabled on FortiGate.

You can filter on FortiGate instead of the collector agent, but only if the collector agent is operating in **advanced mode**. In this case, the collector agent uses the list of groups you selected on FortiGate as its group filter for that device.

The filter list is initially empty. At a minimum, you should create a default filter that applies to all FortiGate devices without a defined filter. The default filter applies to any FortiGate device that does not have a specific filter defined in the list.

Note that if you change the AD access mode from **Standard** to **Advanced** or **Advanced** to **Standard**, you must recreate the filters because they vary depending on the mode.

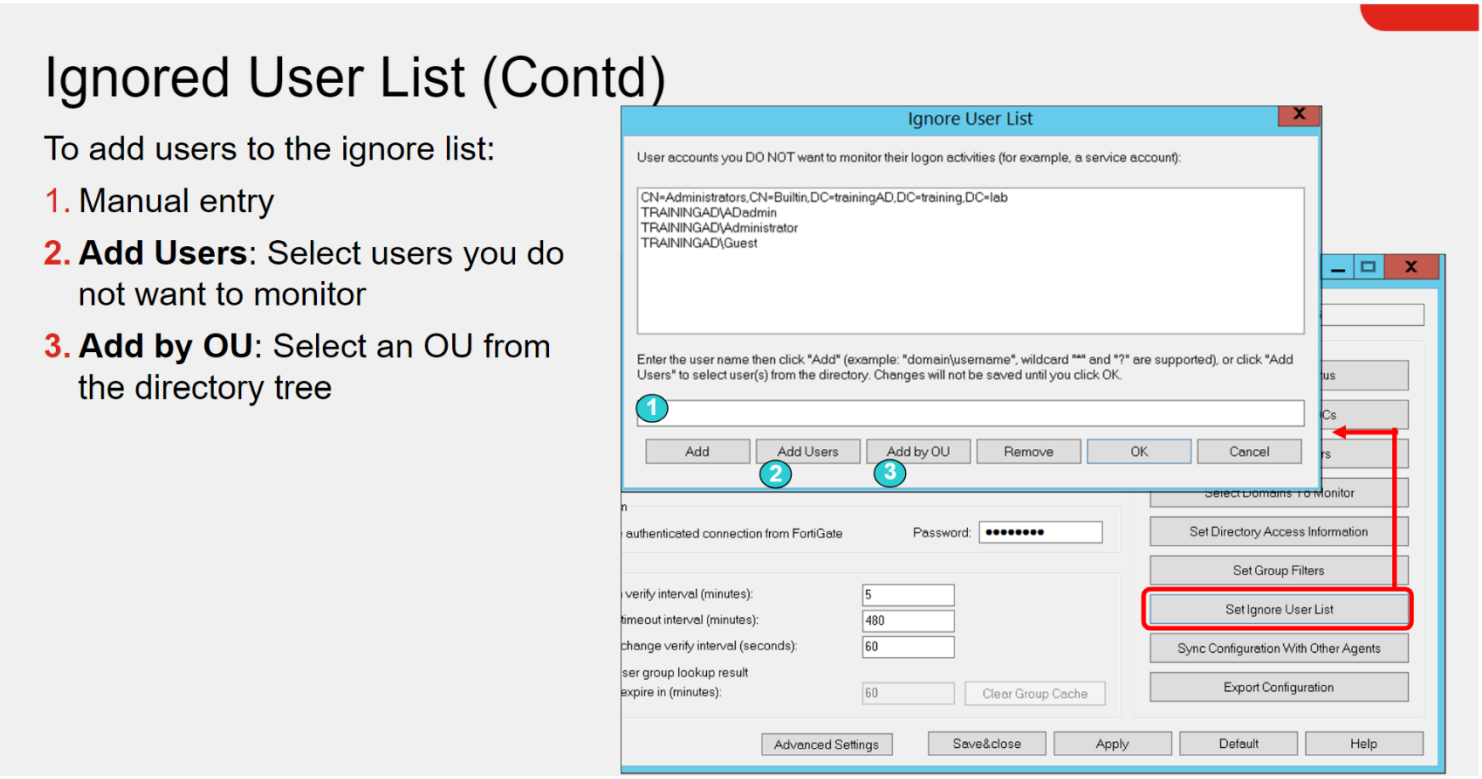
Ignored User List (So Important)



The FSSO collector agent ignores any login events that match the Ignore User List entries. Therefore, these login events are not recorded by the collector agent, nor are they reported to FortiGate. It is a good practice to add all network service accounts to the Ignore User List. Service accounts tend to overwrite user login events, and create issues with identity-based policy matching.

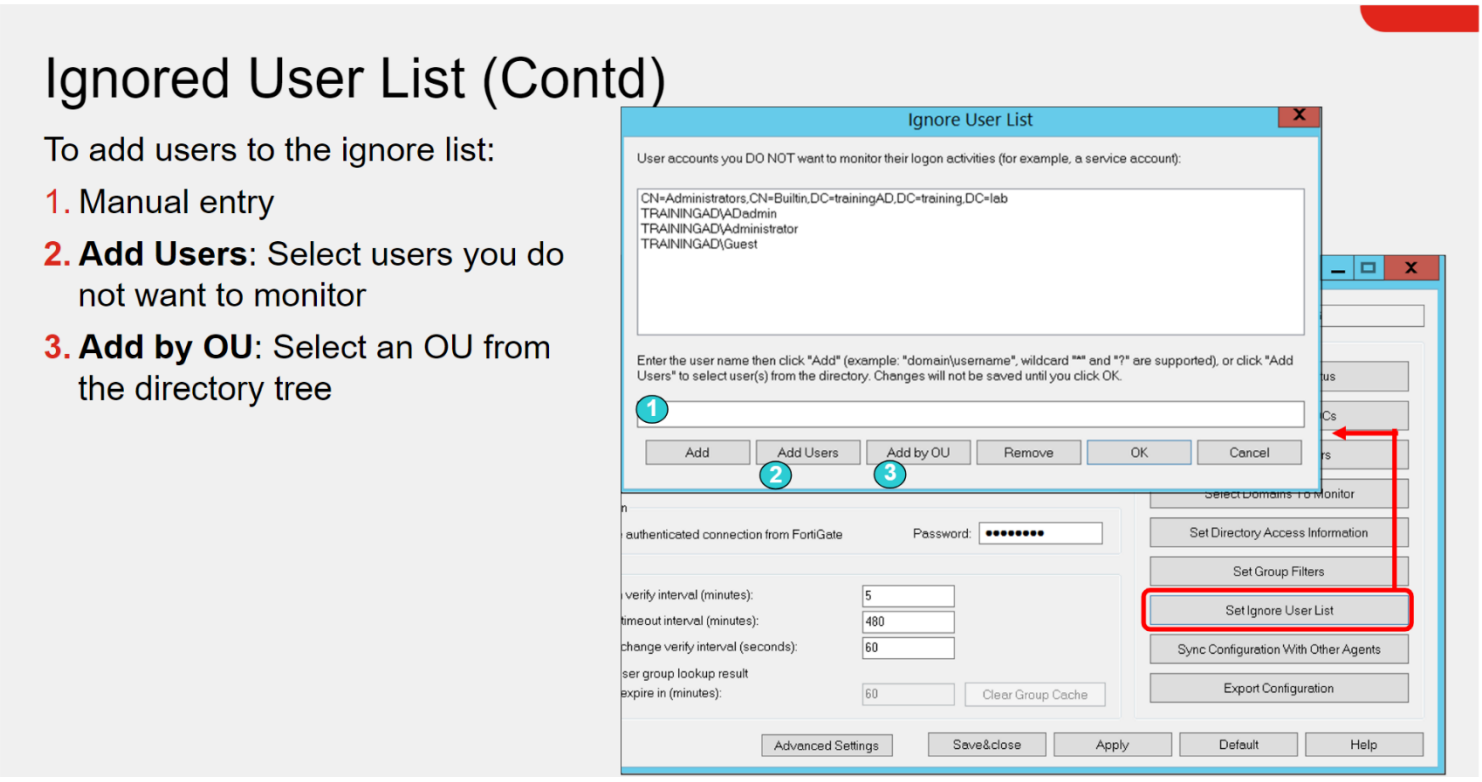
In principle, **FSSO Collector Agents capture all (user) account logins generated on monitored Domain Controllers**, whether in polling mode or DC Agent mode. This includes service accounts and admin accounts as well.
In addition, **FSSO only accounts for one user per IP** (except for terminal servers and the specific Terminal Server Agent), and the Collector Agent will overwrite an existing login on an IP if another login event on the same IP is observed.
This means, for FSSO to work as expected, it is necessary to exclude certain accounts to prevent login information from being overwritten. Generally, service accounts and some admin accounts need to be excluded to prevent them from overwriting valid user logins when a login event is triggered by a service account or admin. FSSO Collector Agent provides the '**Ignore User List**' option for this purpose.

Configuration:



A. From the Start menu, select **Programs -> Fortinet -> Fortinet Single Sign On Agent** and configure Fortinet Single Sign On Agent.

B. In the Common Tasks section, select 'Set Ignore User List'. The current list of ignored users is displayed:



C. You can add users to the Ignore Users List in the following ways:

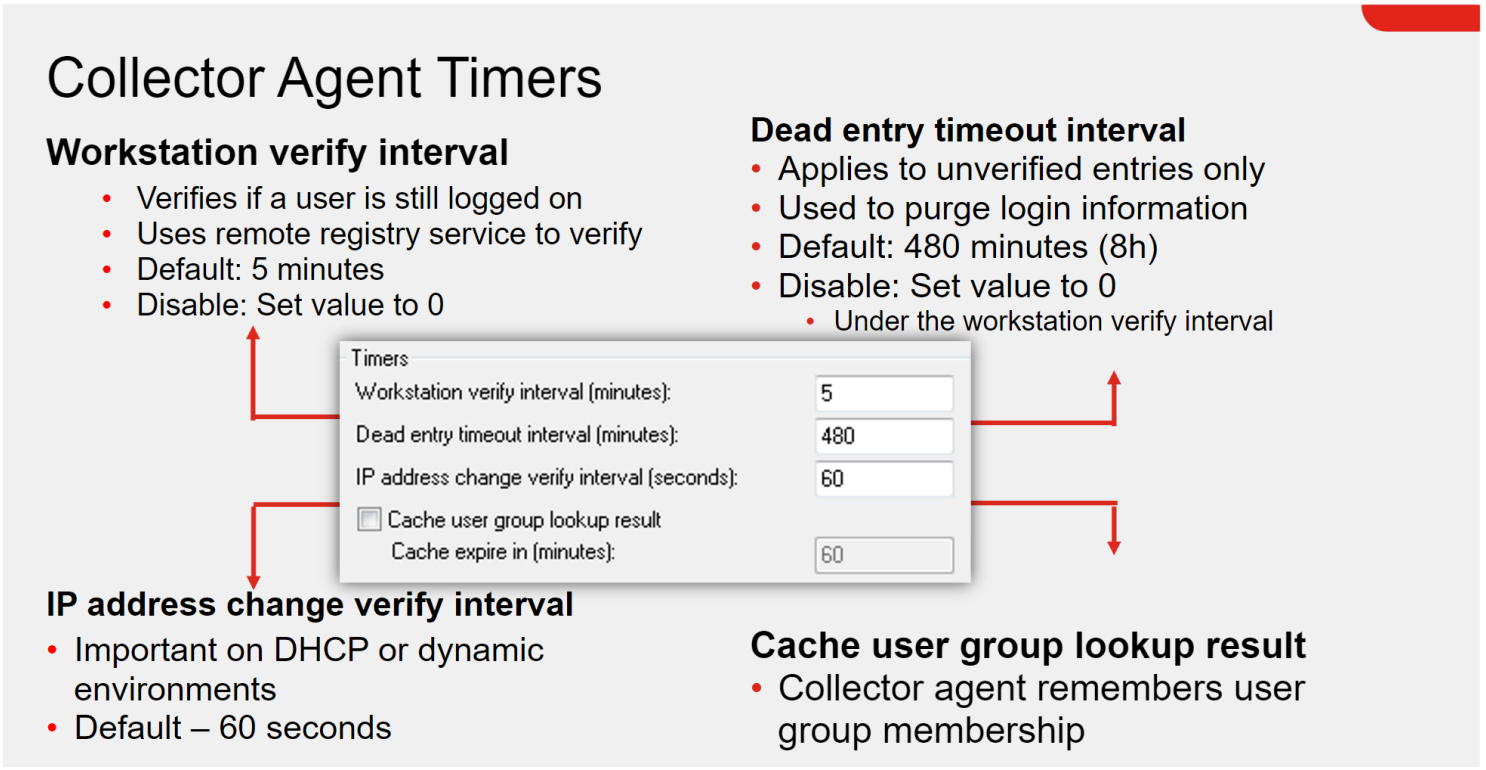
1. Manually enter the username: Enter the username in the appropriate format (AD or LDAP syntax), then select **'Add'**. An 'Add Ignore Users' window is displayed; checkmark the users that are not to be monitored (so will be actively ignored by FSSO Collector Agent), then select **'Add'**.

2. Click *Add Users*, and then choose the users you do not want to monitor: An 'Add Ignore Users' window is displayed; checkmark the users that are not to be monitored (so will be actively ignored by FSSO Collector Agent), then select **'Add'**.

3. Click Add by OU, and then select an OU from the directory tree. Be aware that, all users under the selected OU are added to the Ignore User List: an 'Add Ignore Users by OU' window is displayed, select an OU from the directory tree, then select **'Add'**. All users under the selected OU will be added to the Ignore User List.

D. Select **OK**. The FSSO Collector Agent might **restart**; currently, logged-on user information will be maintained through the process.

Collector Agent Timers (So Important)



The FSSO collector agent timers play an important role in ensuring the correct operation of FSSO.

Now, you'll take a look at each one and how they work.

Workstation verify interval (minutes):

Microsoft Windows does not provide reliable logoff event monitoring tools. In order to verify that a user is still logged on to the same station, the Collector agent needs to connect to each authenticated station and verify that. The default timer value is **every 5 minutes**.

To work properly **ports tcp/139 and tcp/445** need to be available on stations together with Remote Registry service.

To disable this check set the value to **0**.

Take into account that station verification process works in batches. This means the Collector agent should finish a previous verification job before it will activate this timer.

If Collector Agent cannot contact station, it will change user status to UNKNOWN but it will not invalidate user permissions until 'Dead entry timeout interval' will be met or until new logon event will not be detected from the same IP address. If it does connect, it verifies the user and the status remains OK. To facilitate this verification process, you should set the remote registry service to auto start on all domain member PCs.

Dead entry timeout interval (minutes):

This setting applies only to entries with an unverified status. When an entry is not verified, the collector starts this timer. It's used to age out the entry. When the timer expires, the login is removed from the collector. From the perspective of FortiGate, there is no difference between entries that are OK and entries that are not verified. Both are considered valid.

The default is **480 minutes (8 hours)**.

Dead entries usually occur because the computer is unreachable (in standby mode or disconnected, for example) but the user has not logged off.

Disable Dead entry timeout by settings it to **0**.

When it is disabled, the user will stay with 'logged in' status forever. However, a new logon event (either from the same user or a different user) from the same workstation will overwrite/refresh the record.

IP address change verify interval (seconds):

This setting checks the IP addresses of logged in users and updates FortiGate when a user's IP address changes. **This timer is especially important in DHCP or dynamic environments to prevent users from being locked out if they change IP address**.

FSSO periodically checks the IP addresses of logged-in users and updates the FortiGate unit when user IP addresses change.

This timer is especially important in DHCP environments or dynamic environments when mobile users may change their IP address as they move from one location (floor) to another together with their laptop (mobile device).

FSSO relies heavily on DNS for IP resolves. Make sure to allow dynamic updates and configured DHCP server to update DNS whenever client IP address change.

IP address verification prevents users from being locked out if they change IP addresses.

Enter **0** to disable IP address checking if static IP addresses are used. By default, the Collector agent verifies **every 60 seconds** that IP is the same.

User/Groups cache expiration interval (minutes):

This setting caches the user group membership for a defined period of time. It is not updated, even if the user changes group membership in AD. (FSSO will 'remember' user group membership information until expired and will not updated it even if the change group membership is changed in AD).

Example

With the default setting of every 5 minutes, the Collector agent will:

1. Perform an IP address lookup to get the correct IP address, also detect whether IP addresses have been changed.
2. Check whether it can connect to port 139 or 445 of the remote machine. If not, set status to UNKNOWN, go to step 5.
3. Try to open the registry of the remote machine. If failed, set status to UNKNOWN, and go to step 5.
4. Check whether the user's registry hive still exists under HKEY_USERS. If still exists, set status to USER_LOGON. If not, set status to USER_LOGOFF.
5. If the status is:
   - UNKNOWN, do nothing (the entry will be removed in 8 hours).
   - USER_LOGOFF, the entry will be removed right away and FortiGate will be informed.
   - USER_LOGON if:
     - IP didn't change, the entry will be kept.
     - IP changed, need to update FortiGate with new IP address.

AD Access Mode Configuration

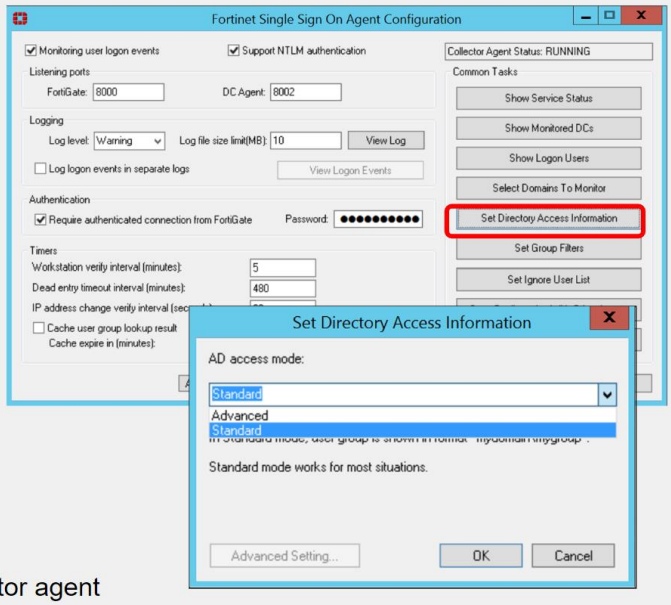
AD Access Mode Configuration

Standard access Mode

- Windows convention:
  - `Domain\groups`
- Firewall policy to groups
  - Nested group is not supported
- Group filters at collector agent

Advanced access Mode

- LDAP convention user names:
  - `CN=User,OU=Name,DC=Domain`
- Firewall policy to users, groups, and OUs
  - Supports nested or inherited groups
- Group filtering:
  - FortiGate as an LDAP client, or group filter on collector agent
  - Filter groups defined on FortiGate



Another important FSSO setting is **AD access mode**. You can set the AD access mode by clicking **Set Directory Access Information**. The AD access mode specifies how the collector agent accesses and collects the user and user group information.

There are two modes that you can use to access AD user information:

- **Standard Mode**
- **Advanced Mode**

The main difference between modes is the naming convention used:

- **Standard** mode uses the Windows convention, NetBios: `Domain\groups`

  The FSSO Collector Agent receives group information from the Collector agent in the **domain\user format**. In this mode, the monitored groups are specified on the Collector Agent.

- **Advanced** mode uses the LDAP convention: `CN=User, OU=Name, DC=Domain`

  The FSSO Collector Agent obtains user group information using LDAP. The benefit of this method is that it is possible to nest groups within groups. The group information is in standard LDAP format "CN=myGroup, OU=myOrganizationUnit, DC=myDomain". In this mode the monitored groups are specified on the FortiGate.

Advanced mode supports nested or inherited groups; that is, users can be members of subgroups that belong to monitored parent groups. Additionally, in advanced mode, FortiGate firewall policies can be applied to individual users, user groups, and OUs.

In comparison, in standard mode, you can have a firewall policy with a security profile which can apply to user groups but not to individual users.

In advanced mode, you can configure FortiGate as an LDAP client and configure the group filters on FortiGate. You can also configure group filters on the collector agent.

If the LDAP on the collector agent fails, it doesn't matter what the LDAP on FortiGate says, FSSO won't work. If FortiGate LDAP fails, but the LDAP on the collector agent is still running, FortiGate may not be able to collect logs, but the collector agent still collects logs. So, it is recommended that you create filters from the collector agent.

It is necessary for the Collector Agent and FortiGate to have the same Directory Access mode, or the connection between them might fail.

Even though Standard mode is the default mode of operation, sometimes it is necessary to switch to Advanced mode in order to comply to company polices or authenticate nested groups.

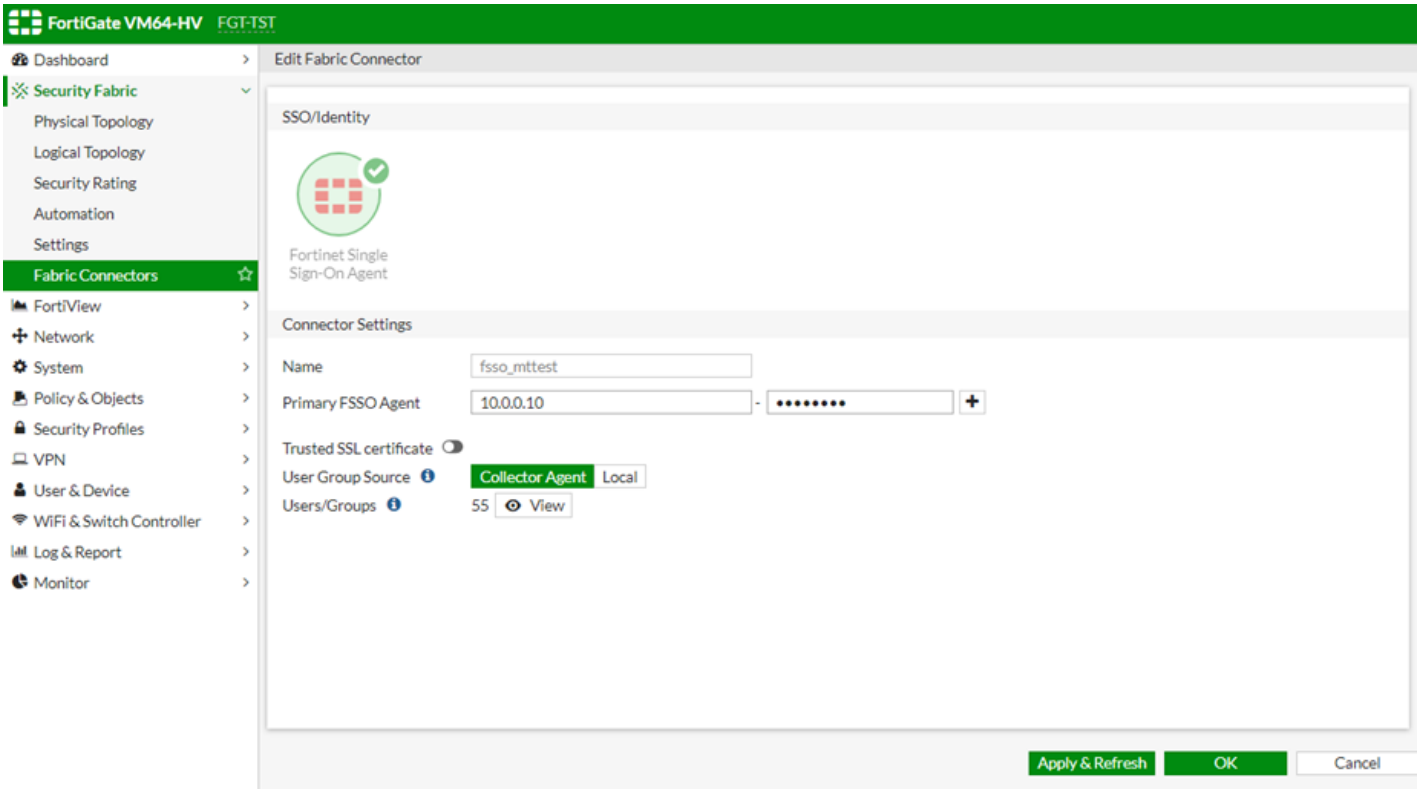
How to switch FSSO operation mode from Standard Mode to Advanced Mode???

On Collector Agent

1. On the Collector Agent (CA) open the Fortinet Single Sign-On Agent Configuration console and click **Set Directory Access Information** button.
2. Select required mode and apply changes by clicking **'ok'** button.
3. If any filters have been configured, remove old filters by clicking Set Group Filters and then selecting filters and pressing 'remove' button.
4. After group filter is specified, FSSO service should be restarted automatically.

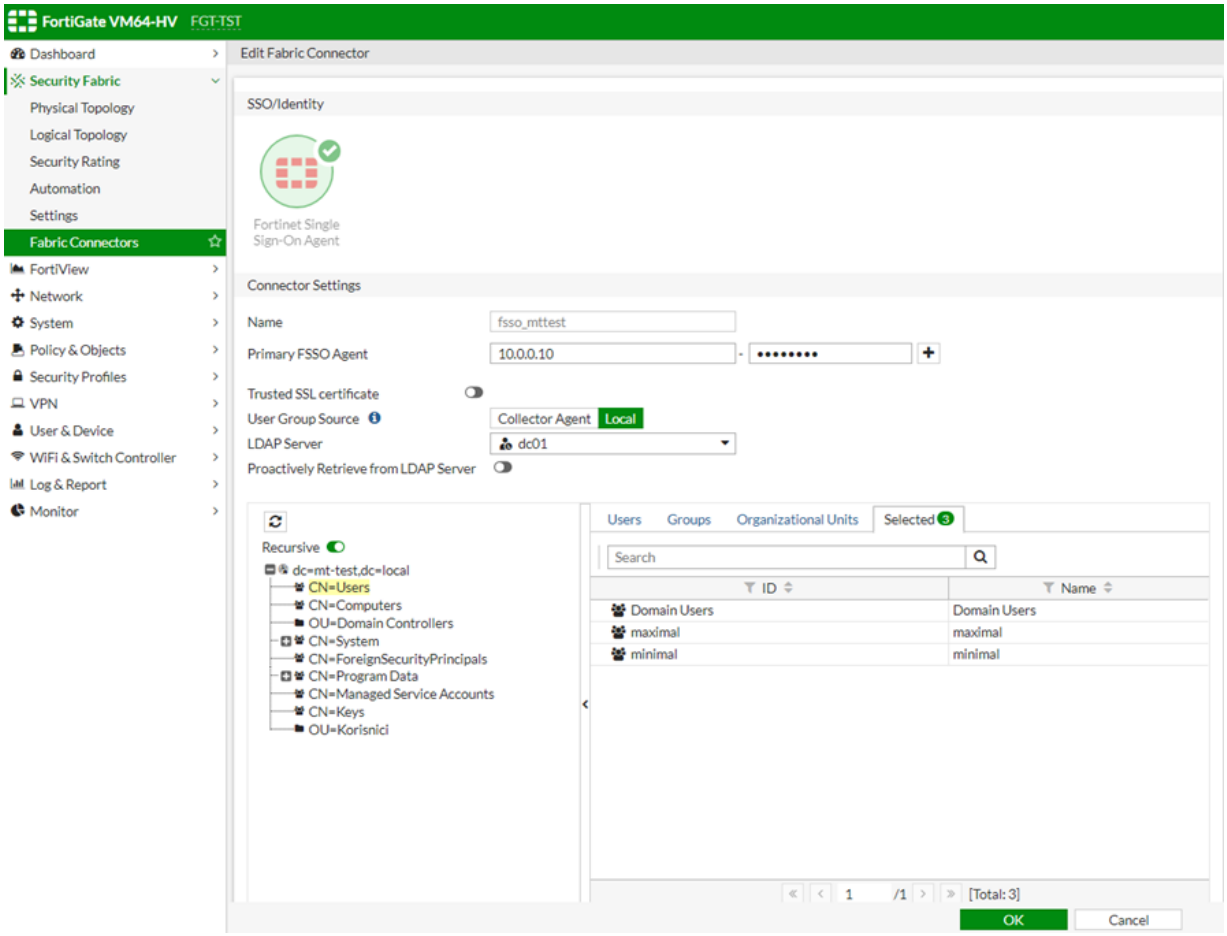
On FortiGate

1. On the FortiGate, go to **Security Fabric -> Fabric Connectors** and edit the FSSO entry.
2. To use the group filter specified on the FSSO collector agent, change the User Group Source to **Collector Agent**. Save the setting with 'OK' and if needed afterwards 'Apply & Refresh'.



After selecting 'Apply & Refresh' button, the groups specified on FSSO CA group filter should be seen.

3. To specify a group filter on the FortiGate, change the User Group Source to **Local**.
Select one of the preconfigured LDAP server entries from the FortiGate and select which groups, users or OUs it is required to filter.



Difference between User Group Source: Collector Agent and Local

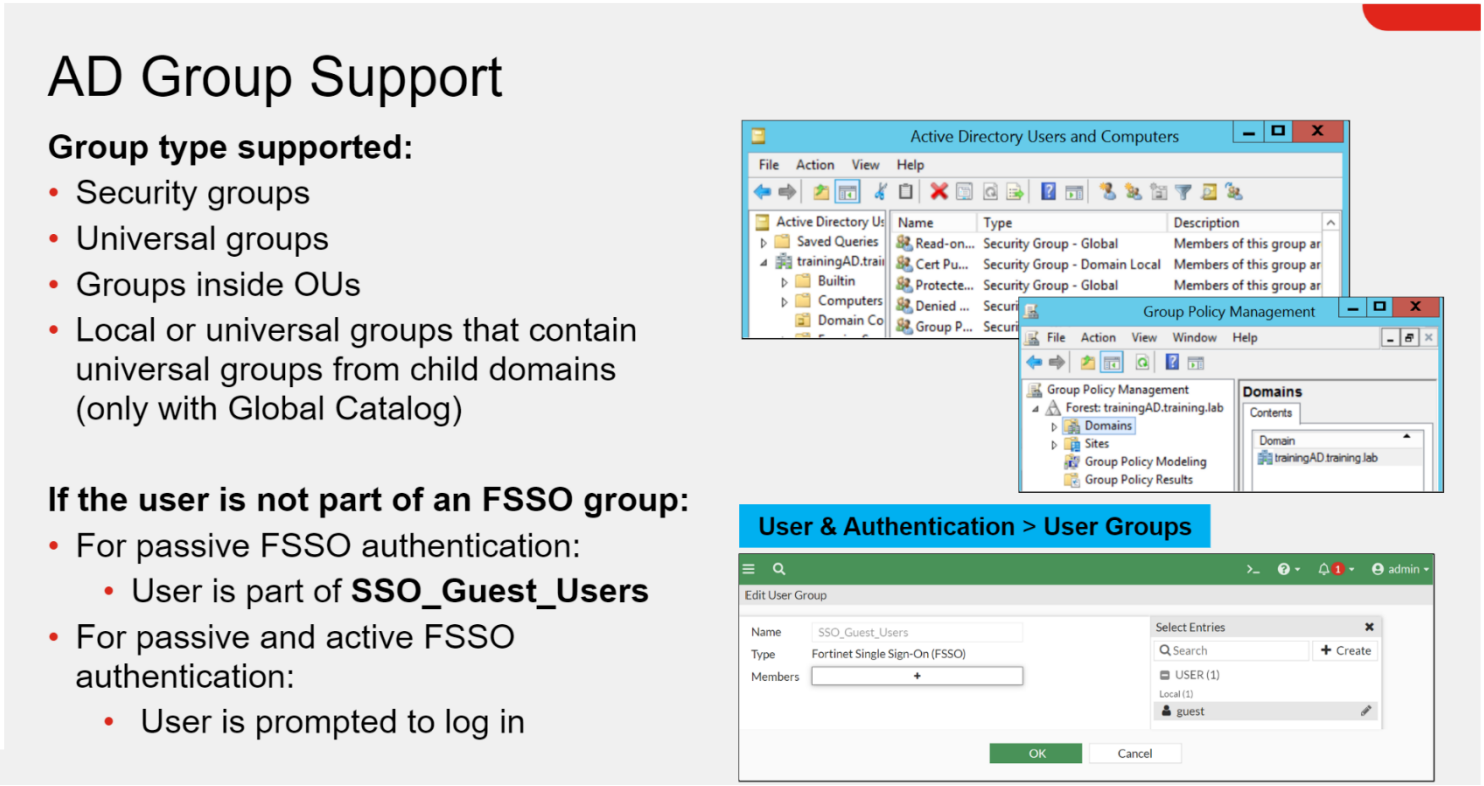
Collector Agent:

- Usually selected when FSSO Collector Agent is configured in **Standard mode**.
- Means that the Group Filter for users is specified on the Collector Agent

Local:

- Usually selected when FSSO Collector Agent is configured in **Advanced mode**.
- Means that the Group Filter for users is specified on the Fortigate.

AD Group Support



In AD settings, not all group types are supported. AD settings support filtering groups only from:

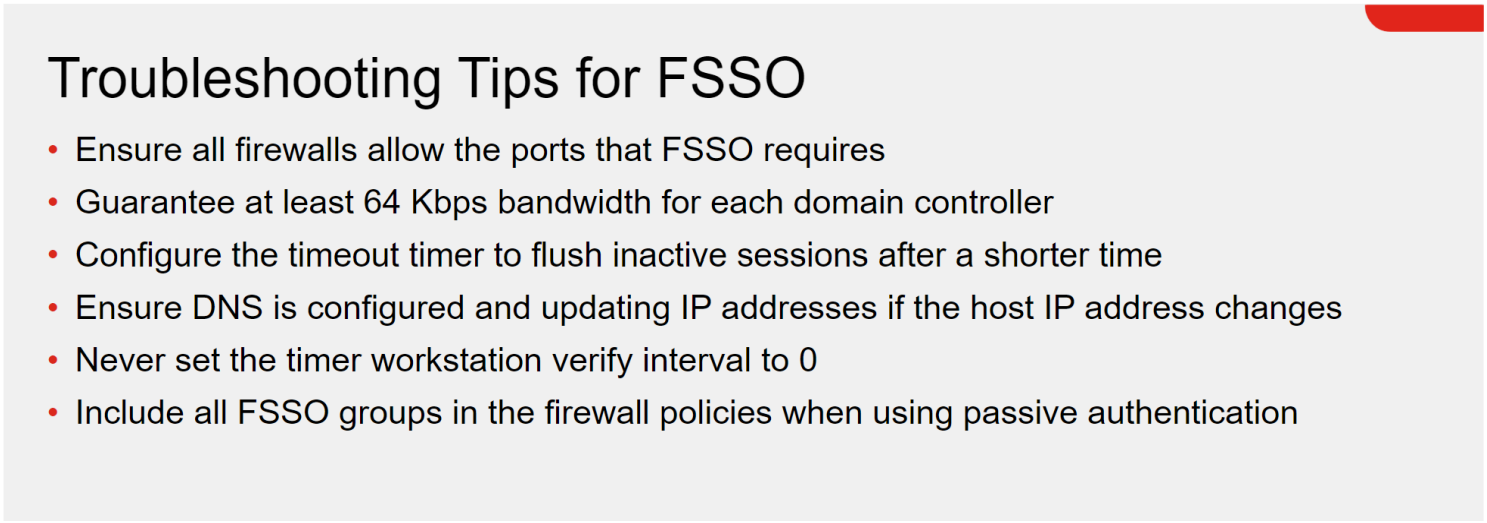
- Security groups
- Universal groups
- Groups inside OUs
- Local or universal groups that contain universal groups from child domains (only with Global Catalog)

All FortiGate configurations include a user group called **SSO_Guest_Users**. When only passive authentication is used, all the users that do not belong to any FSSO group are automatically included in this guest group.

This allows an administrator to configure limited network access to guest users that do not belong to the Windows AD domain.

However, if both passive and active authentication are enabled for specific traffic, you cannot use SSO_Guest_Users, because traffic from IP addresses not on the FSSO user list must be prompted to enter their credentials.

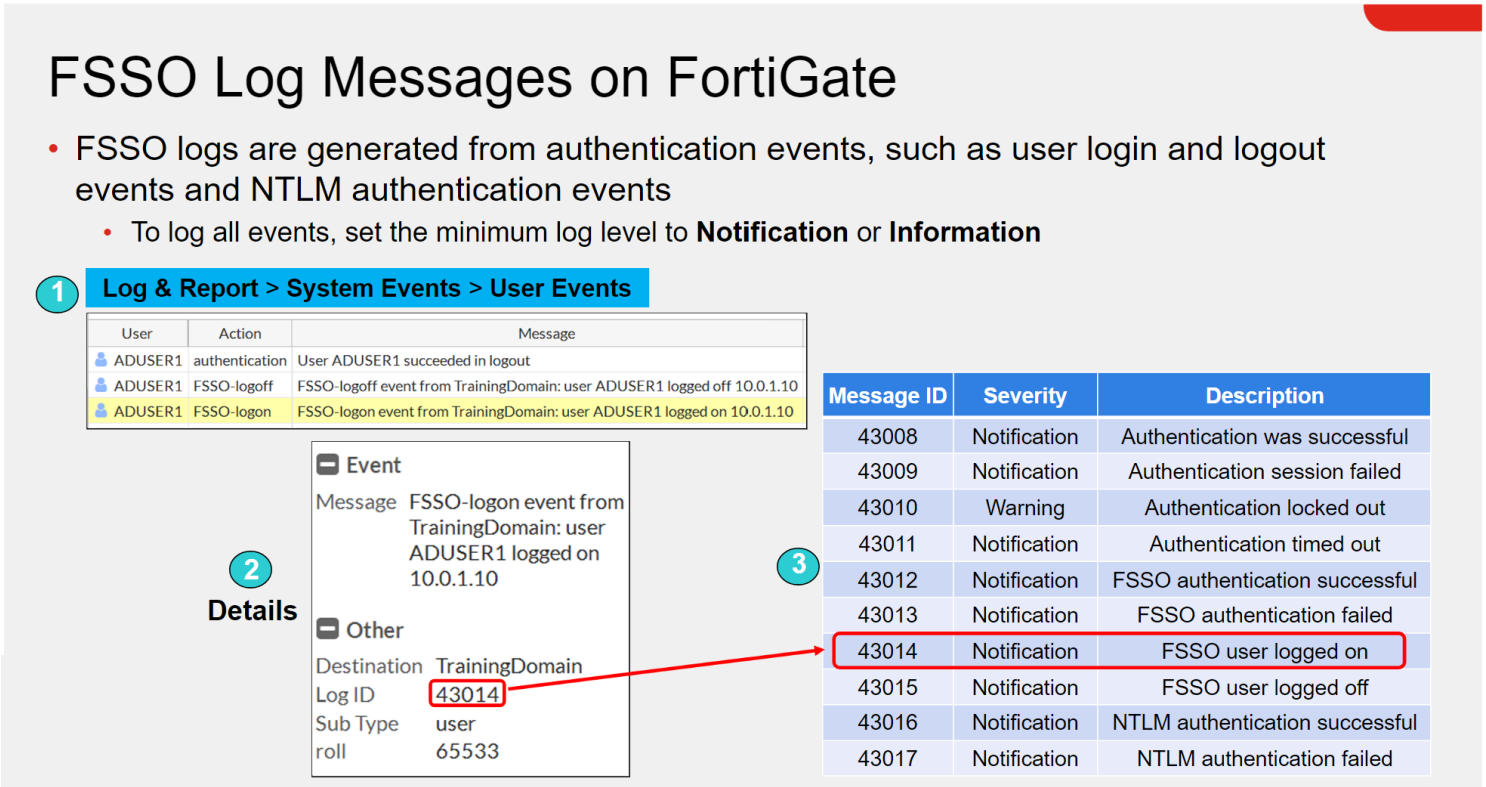
Troubleshooting Tips for FSSO



Begin with the following tips, which are useful in many FSSO troubleshooting situations:

- FSSO has a number of required ports that you must allow through all firewalls, or connections will fail. These include **ports 139** (workstation verification), **445** (workstation verification and event log polling), **389** (LDAP), and **445 and 636** (LDAPS).
- Configure traffic shaping to have a **minimum guaranteed bandwidth of 64 Kbps** for each domain controller. If there is insufficient bandwidth, some FSSO information might not reach FortiGate.
- In an all-Windows environment, flush inactive sessions. Otherwise, a session for a nonauthenticated machine may be sent as an authenticated user. This can occur if the DHCP lease expires for the authenticated user with the collector agent being able to verify that the user has logged out. Ensure DNS is configured correctly and is updating IP addresses, if workstation IP addresses change.
- Never set the workstation verify interval to 0. This prevents the collector agent from deleting stale entries, which means that they can be removed only by a new event overwriting them. This can be especially dangerous in environments where FSSO and non-FSSO users share the same DHCP pool.
- When using passive authentication only, include the group of guest users (SSO_Guest_User) in a policy and give them access. Associate their group with a security policy. If you use active authentication as a backup, ensure you do not add SSO_Guest_User to any polices. SSO_Guest_User and active authentication are mutually exclusive.

FSSO Log Messages on FortiGate



FSSO-related log messages are generated from authentication events. These include **user login** and **user logout** events, and **NTLM authentication events**. These log messages are central to network accounting policies, and can also be useful in troubleshooting issues.

To ensure you log all the events needed, set the minimum log level to **Notification** or **Information**. Firewall logging requires Notification as a minimum log level. The closer the log level is to Debug level; the more information is logged.

FortiOS FSSO log messages

There are two types of FortiOS log messages:

- **Firewall**
- **Event**

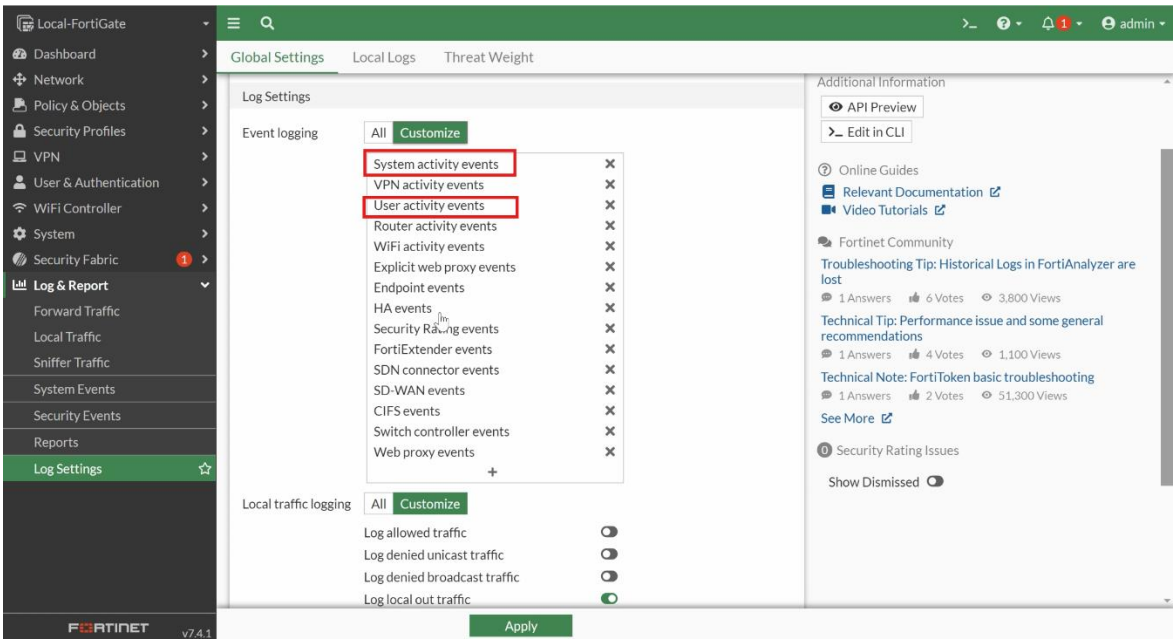
FSSO-related log messages are generated from authentication events.

To enable event logging:

1. Go to **Log & Report > Log Settings**.
2. In **Event Logging**, select:

System activity event	**All system-related events, such as ping server failure and gateway status.**
User activity event	**All administration events, such as user logins, resets, and configuration updates.**

3. Optionally you can enable any or all of the other logging event options.
4. Select **Apply**.

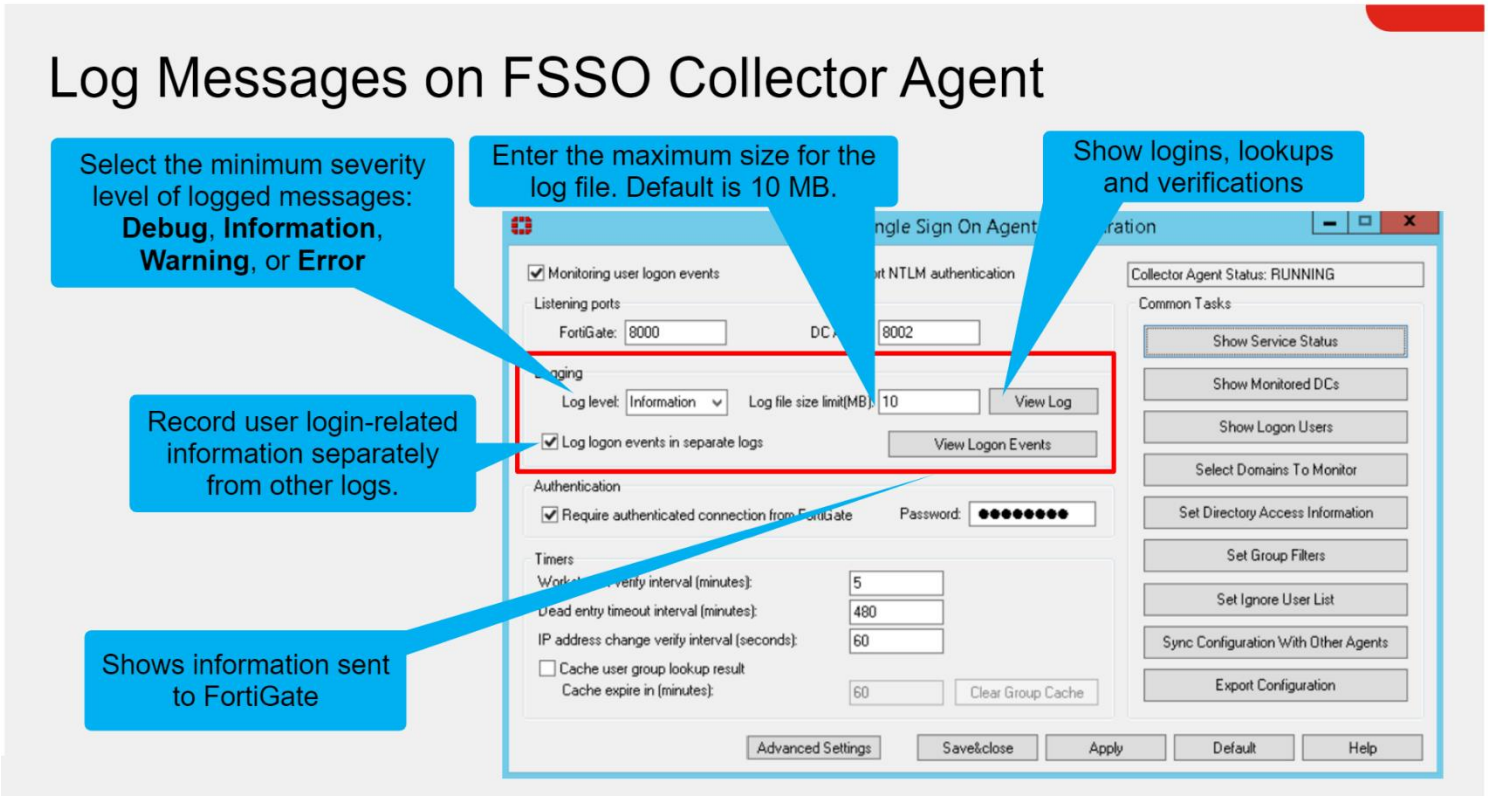


List of FSSO related log messages:

Message ID	Severity	Description
43008	Notification	Authentication was successful
43009	Notification	Authentication session failed
43010	Warning	Authentication locked out
43011	Notification	Authentication timed out
43012	Notification	FSSO authentication was successful
43013	Notification	FSSO authentication failed
43014	Notification	FSSO user logged on
43015	Notification	FSSO user logged off
43016	Notification	NTLM authentication was successful
43017	Notification	NTLM authentication failed

To learn more about Log&Report in FortiGate, take a look at this link:
https://docs.fortinet.com/document/fortigate/7.4.3/administration-guide/738890/log-and-report

Log Messages on FSSO Collector Agent



When troubleshooting FSSO agent-based deployments, you might want to look at the log messages generated directly on the FSSO collector agent.

The **Logging** section of the FSSO collector agent allows the following configurations:

- **Log level:** Select the minimum severity level of logged messages. Includes these levels:
  - ✓ **Debug:** the most detailed log level. Use it when actively troubleshooting issues.
  - ✓ **Information:** includes details about login events and workstation checks. This is the recommended level for most troubleshooting.
  - ✓ **Warning:** the default level. It provides information about failures.
  - ✓ **Error:** lists only the most severe events.

- **Log file size limit (MB):** Enter the maximum size for the log file in MB. The default is 10.

- **View Log:** View all FSSO agent logs.

- **Log login events in separate logs: Record user login-related information separately from other logs**. The information in this log includes: data received from DC agents, user login/logout information, workstation IP change information, and data sent to FortiGate devices. When selected, a summary of events sent and removed from FortiGate is listed under View login Events, while all other information remains under View Log.

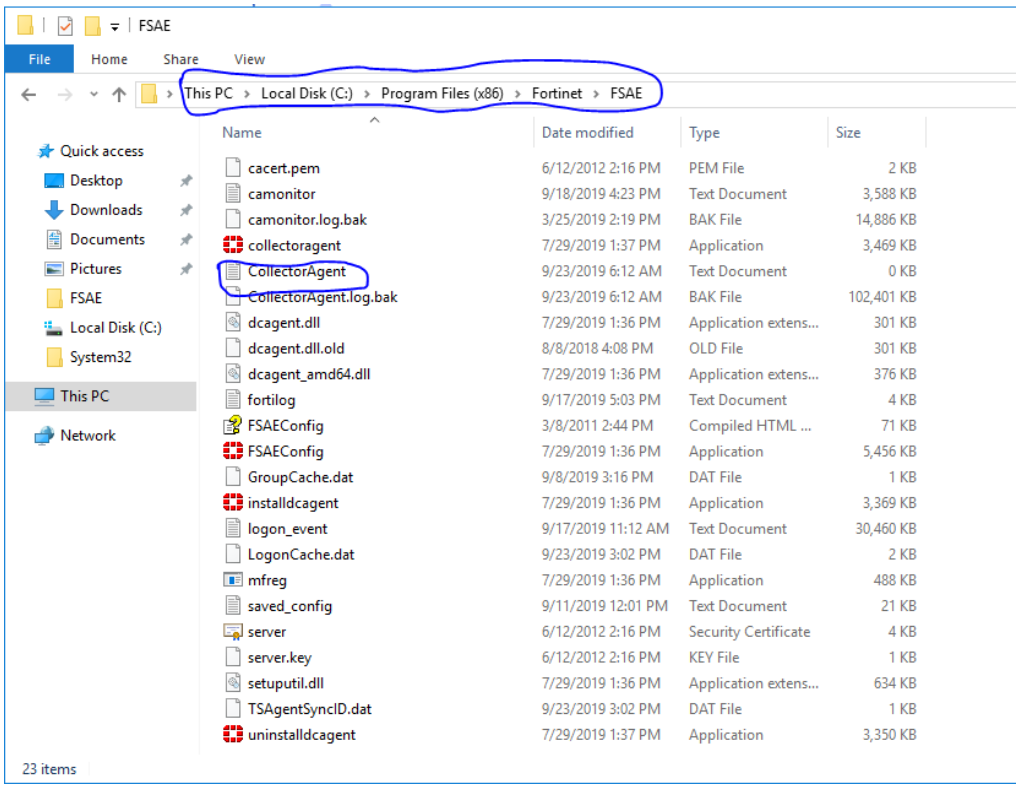
• **View login Events:** If Log login events in separate logs is enabled, you will can view user login-related information.

Best Practice:

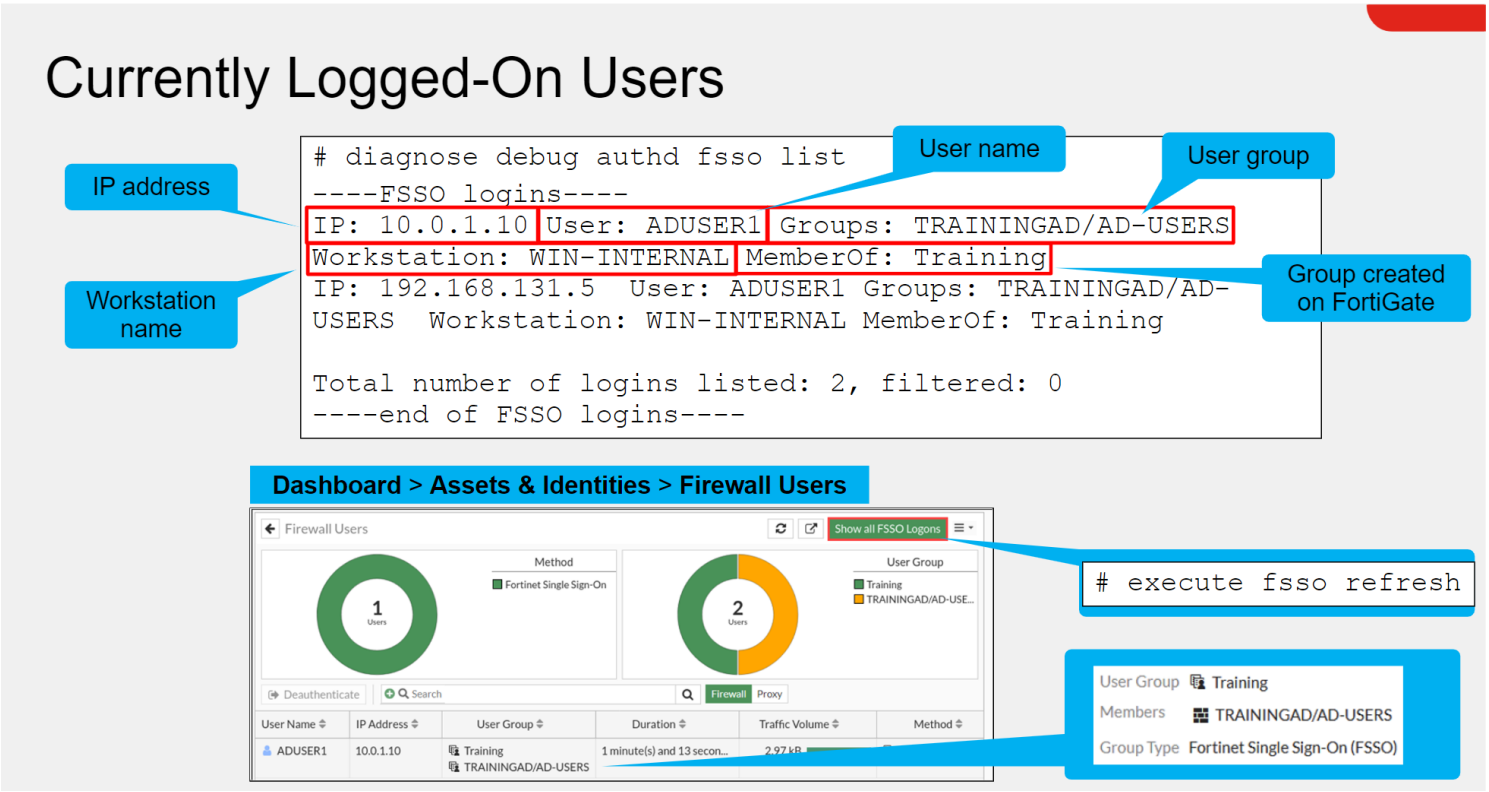
When FSSO collector agent is installed on any member server or domain controller, the Logging level needs to be changed to **'Debug'** and the size needs to be increased **100MB** (or more if the number of users is more).

To see the View Log, click on View Logs. It will open with notepad.

After changing the log level and set the required size, the log file will be available at:
C:\>Program files or Program(x64) \fortinet\FSAE\CollectorAgent.txt



Currently Logged-on Users



If applying the tips from the previous topic didn't solve your FSSO issues, you may need to apply some **debug** commands.

To display the list of FSSO users that are currently logged in, use the CLI command:

diagnose debug authd fsso list

For each user, the username, user group, IP address, and the name of the workstation from which they logged in shows. The MemberOf section shows the group that was created on the firewall, to which you mapped the AD group. The same group should show in the **User group** screen on the GUI. (**Dashboard > Assests & Identities > Firewall Users**)

Also, use **execute fsso refresh** to manually refresh user group information from any directory service servers connected to FortiGate, using the collector agent.

Checking Connection to FortiGate

Connection to FortiGate

- Check connectivity between collector agent and FortiGate

```
# diagnose debug authd fsso server-status

 Server Name    Connection Status      Version                Address
-----------     -----------------     -------                -------
TrainingDomain   connected             FSAE server 1.1        10.0.1.10
```

To show the status of communication **between FortiGate and each collector agent**, you can use the CLI command: **diagnose debug authd fsso server-status**

Additional Commands

Additional Commands

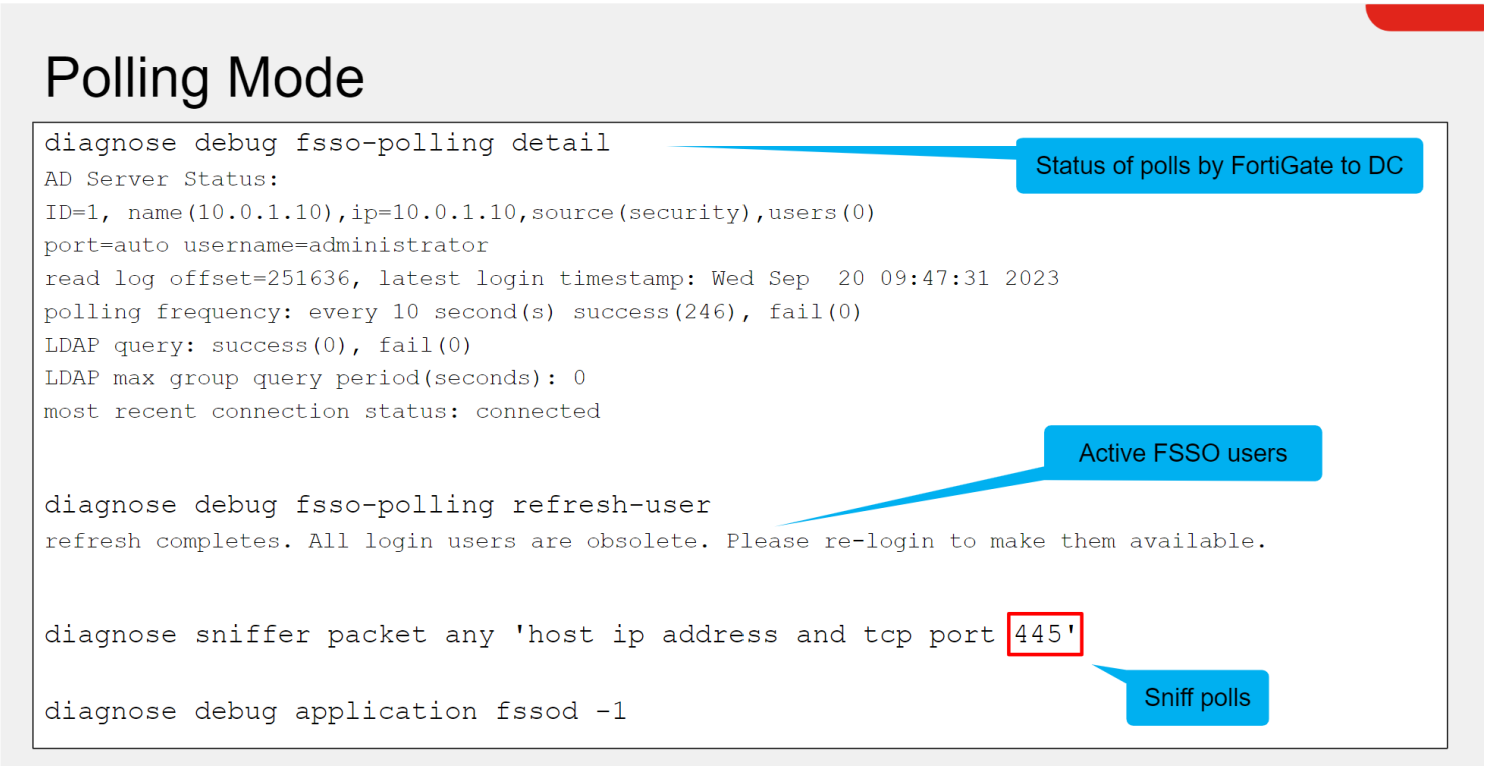
```
# diagnose debug authd fsso <…>

       filter  - Filters used for list or clear logins
       list    - Show currently logged on users
       refresh-groups - Refresh group mapping
       summary        - Summary of currently logged on users
       clear-logons   - Delete cached login status
       refresh-logons - Resynchronize login database
       show-address   - Show FSAE dynamic addresses
       server-status  - Show FSSO agent connection status

# diagnose firewall auth clear -  Clears all filtered users
# diagnose firewall auth filter-  Filter specific group, id, and so on
# diagnose firewall auth list  -  List authenticated users
# diagnose firewall auth mac   -  Authenticated MAC users
# diagnose firewall auth ipv6  -  Authenticated IPv6 users
```

Also, available under **diagnose debug authd fsso** are commands for clearing the FortiGate cache of all currently logged in users, filtering the display of the list of logged in users, and refreshing the login and user group information.

Polling Mode



The command **`diagnose debug fsso-polling detail`** displays status information and some statistics related to the polls done by FortiGate on each DC in **agentless polling**. If the `read log offset` is incrementing, FortiGate is connecting to and reading the logs on the domain controller. If the `read log offset` is incrementing but you are not getting any login events, check that the group filter is correct and that the domain controller is creating the correct event IDs.

The command **`diagnose debug fsso-polling refresh-user`** flushes information about all the active FSSO users.

In agentless polling mode, FortiGate frequently polls the event viewer to get the login events. You can sniff this traffic on port 445.

Also, there is a specific FortiGate daemon that handles polling mode. It is the **`fssod`** daemon. To enable agentless polling mode real-time debug, use the **`diagnose debug application fssod -1`** command.

LAB

Fortinet Single Sign-On Configuration

In this exercise, you will configure FortiGate for FSSO and test user authentication. The lab uses a demo environment to emulate the behavior of an active FSSO DC agent from the Local-Client VM using a Python script. Therefore, you will not configure a DC agent to send logon events from the Local-Client VM.

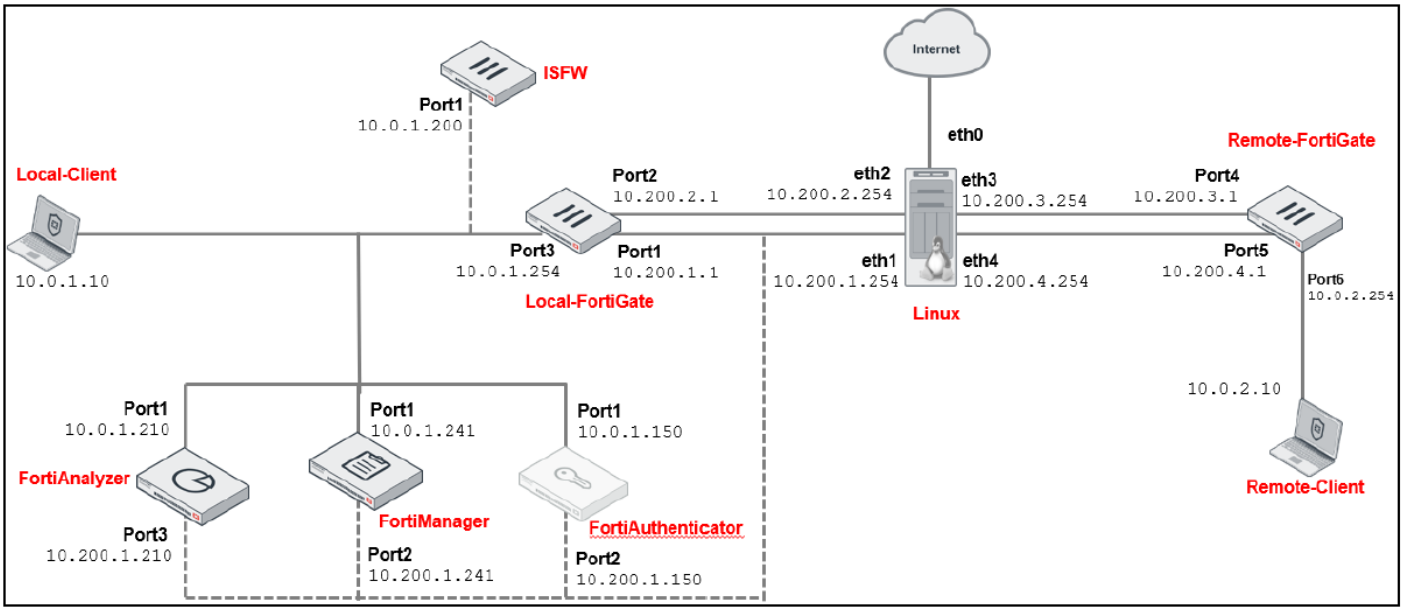
Objectives

- Review the FSSO configuration on FortiGate
- Test the transparent or automatic user identification by generating user logon events
- Monitor the FSSO status and operation

We have an exercise in this LAB:

Configuring FortiGate for FSSO Authentication

LAB Topology:



In a real-world environment, you must configure FortiGate to identify users by polling their logon events using an FSSO agent, and you must install and configure a collector agent. FSSO agents are available on the Fortinet Support website (http://support.fortinet.com).

For FortiGate to communicate and poll information from the FSSO collector agent, you must assign the polled user to a firewall user group, and then add the user group as a source on a firewall policy.

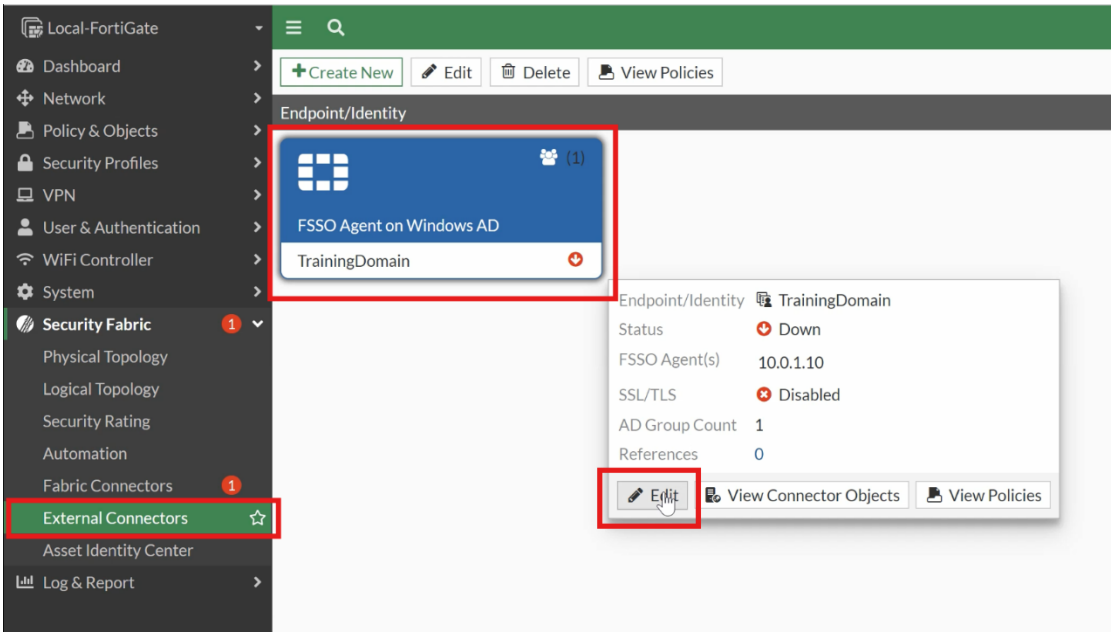
Finally, you can verify the user logon event that FortiGate collects. This event is generated after a user logs in to the Windows Active Directory domain. Therefore, no firewall authentication is required.

Review the FSSO Configuration on FortiGate

You will review the FSSO configuration and FSSO user groups on FortiGate. FSSO allows FortiGate to automatically identify the users who connect using SSO. Then, you will add FSSO user groups to the firewall policies.

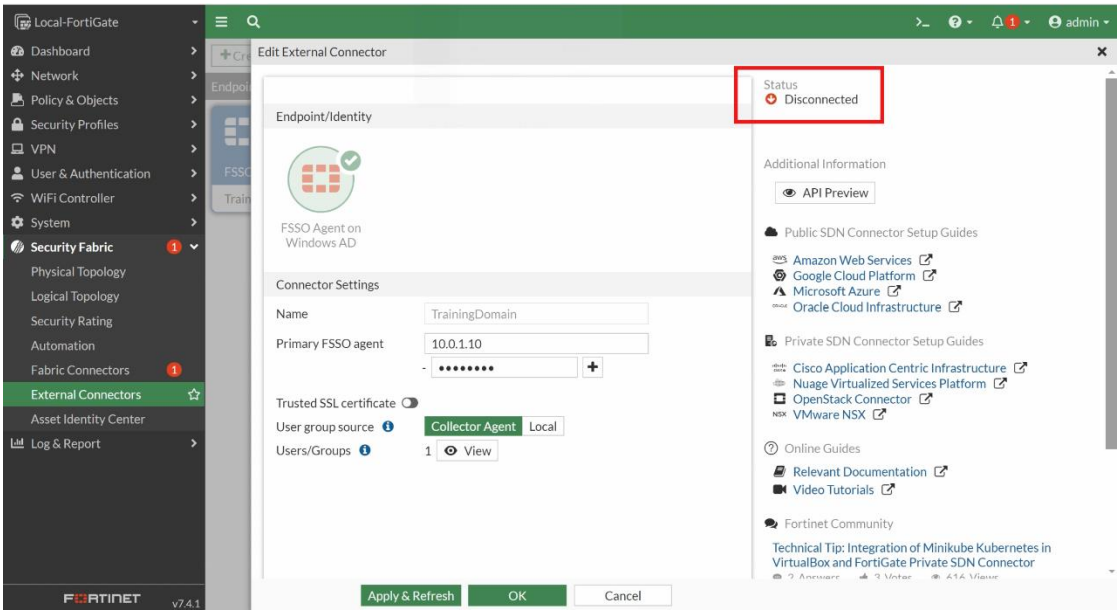
To review the FSSO server and FSSO user group configuration on FortiGate

1. Connect to the Local-FortiGate GUI, and then log in with the username admin and password password.
2. Click **Security Fabric** > **External Connectors**.
3. Select **TrainingDomain**, and then click **Edit**.



4. In the upper-right corner, review the **Endpoint/Identity** status, and see that the status is **Disconnected**.

5. Leave the browser window open.



To run a script to simulate a user logon event

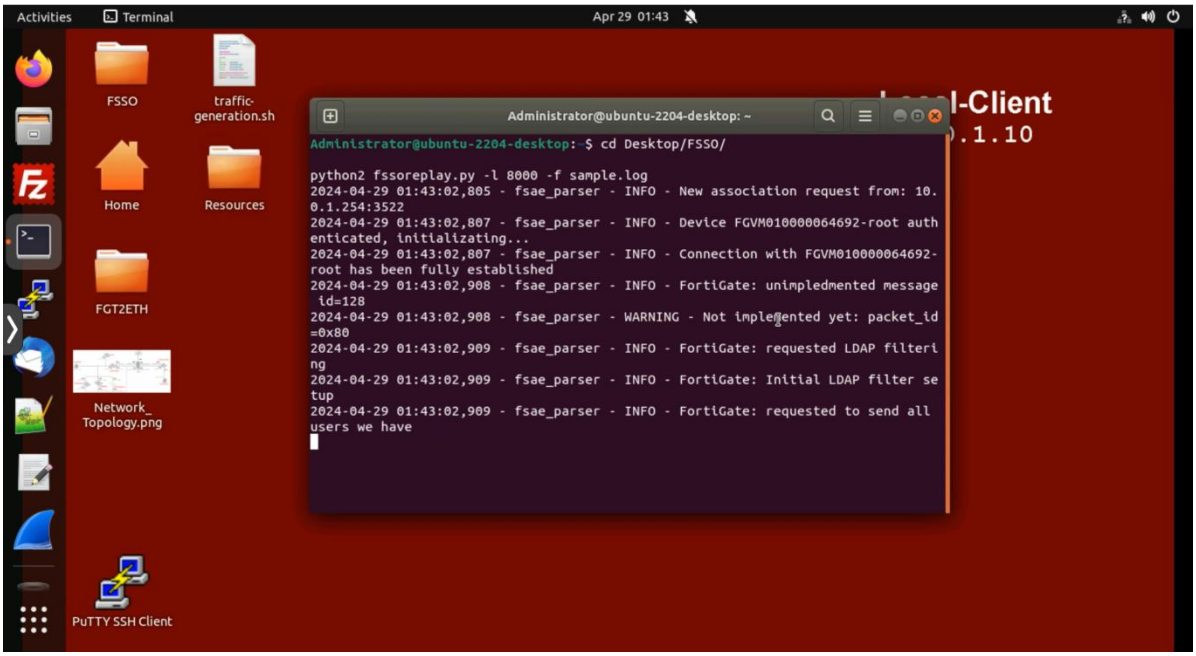
1. On the Local-Client VM, open a terminal window, and then enter the following commands to simulate a user logon event:

```
cd Desktop/FSSO/

python2 fssoreplay.py -l 8000 -f sample.log
```

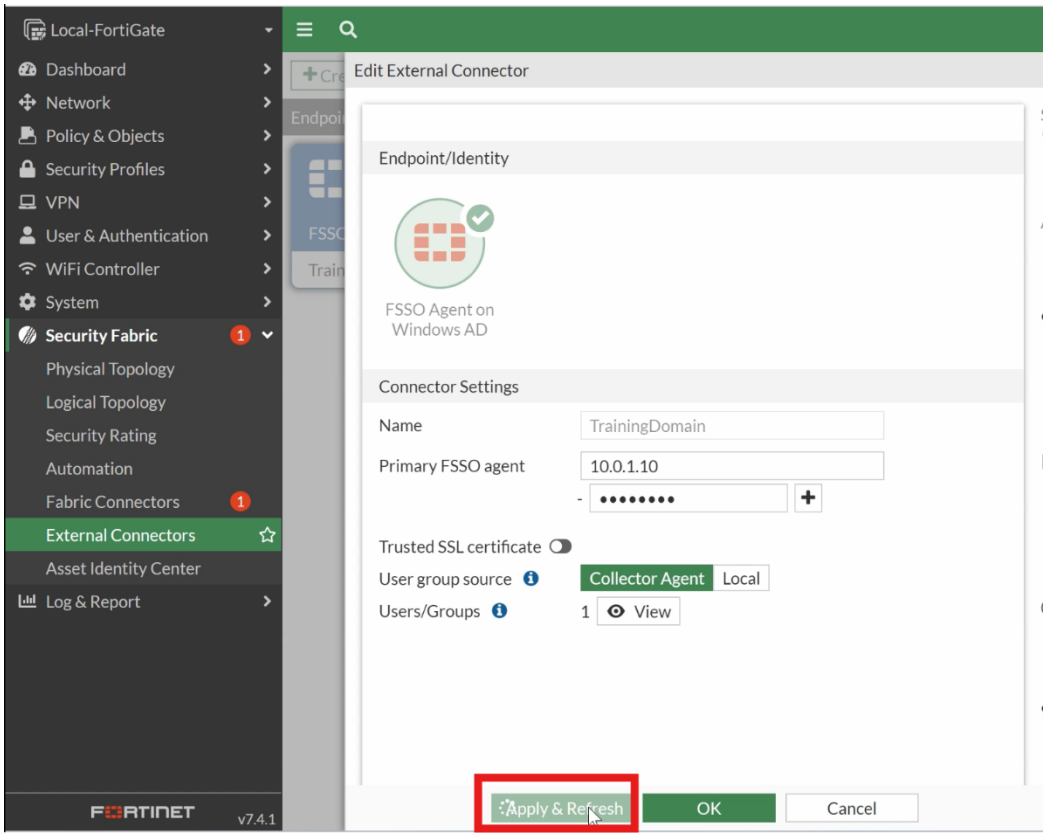
2. Keep the terminal window open.

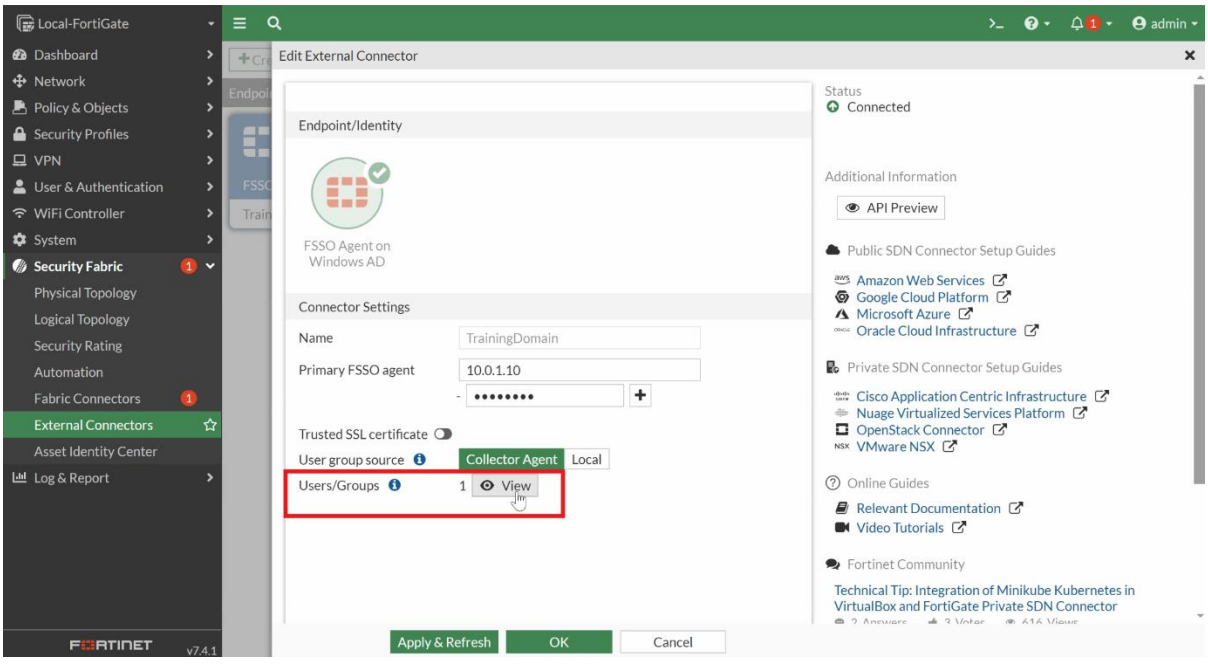
The script continues to run in the background.



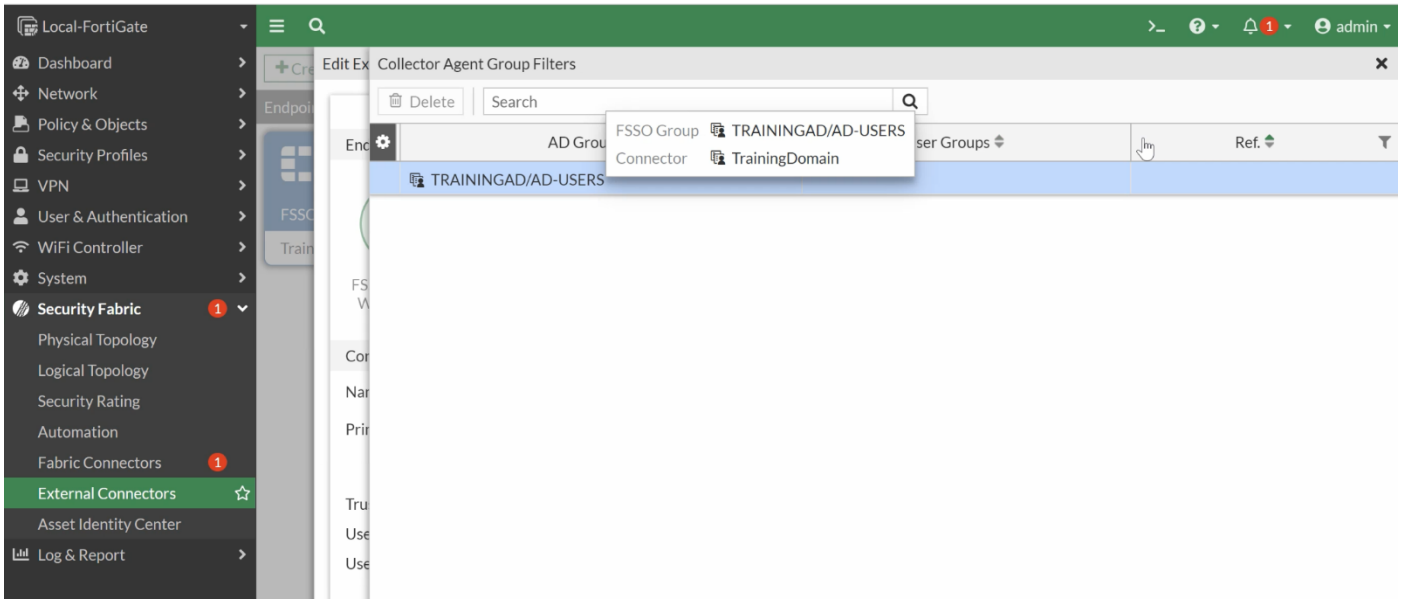
To review the FSSO connection and FSSO user groups

1. Continuing in the **TrainingDomain** window, click **Apply & Refresh**.
2. Select **TrainingDomain**, and then click **Edit**.
3. In the **Users/Groups** field, click **View**.





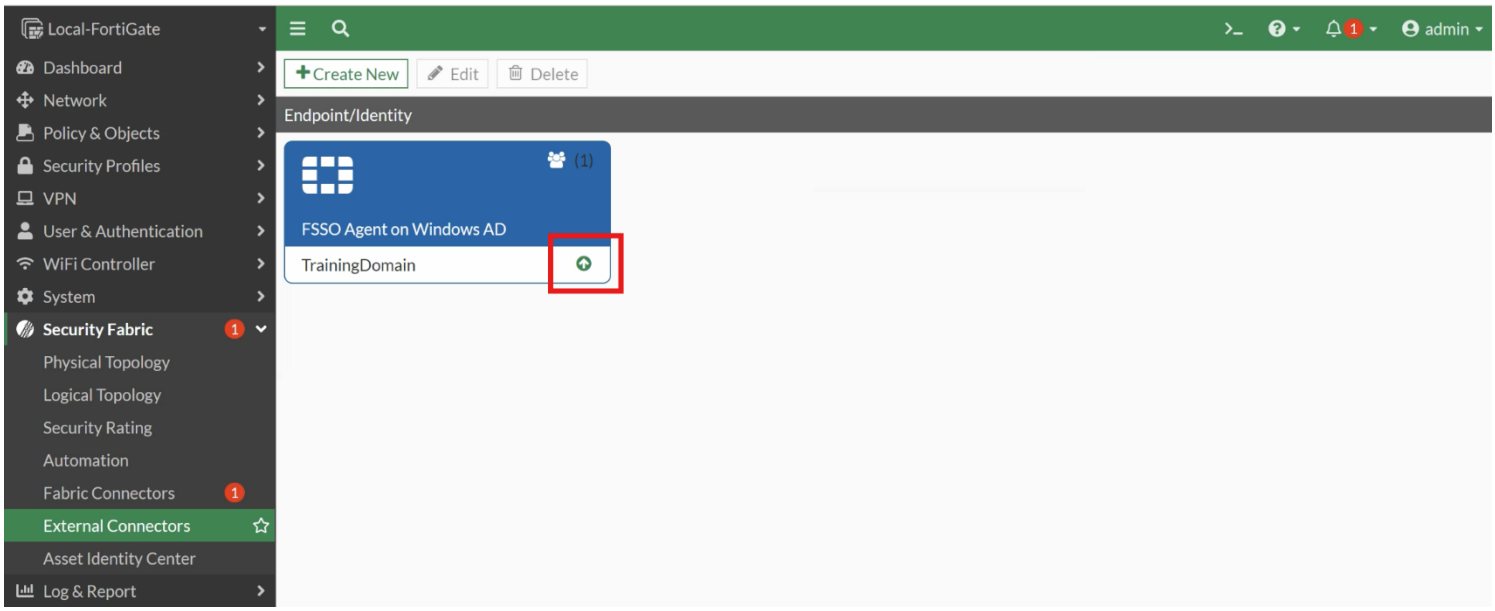
The **TRAININGAD/AD-USERS** monitored group is displayed.



4. Click **X** to close the **Collector Agent Group Filters** window.

5. Click **OK**.

A green up arrow confirms that the communication with the FSSO collector agent is up.



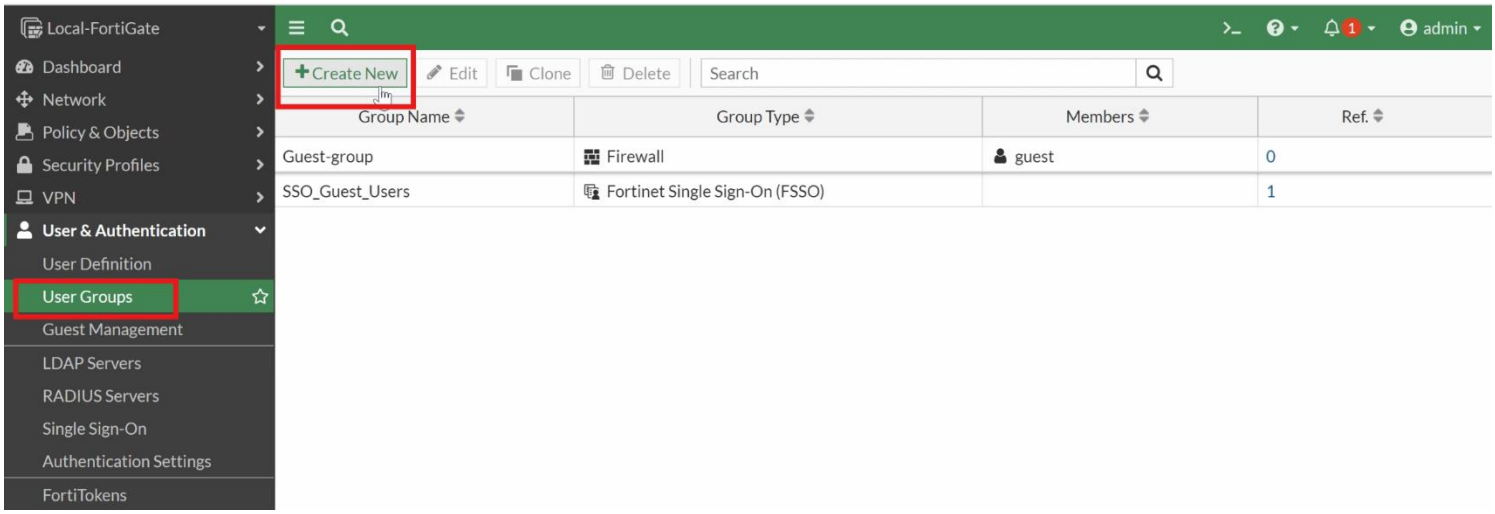
To assign the FSSO user to an FSSO user group

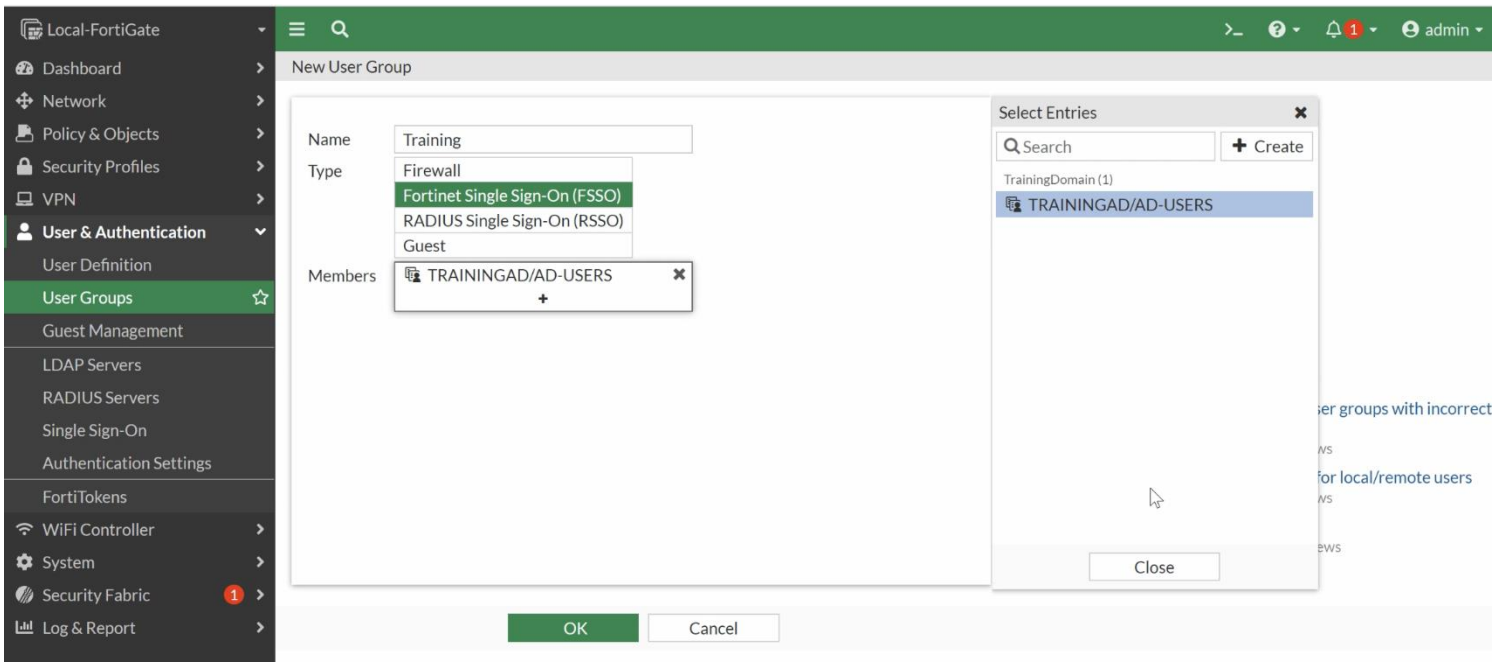
1. Continuing on the Local-FortiGate GUI, click **User & Authentication** > **User Groups**.

2. Click **Create New**, and then configure the following settings:

Field	Value
Name	Training
Type	Fortinet Single Sign-On (FSSO)
Members	TRAININGAD/AD-USERS

The FSSO user is automatically listed because of the selected group type—FSSO.





3. Click **OK**.

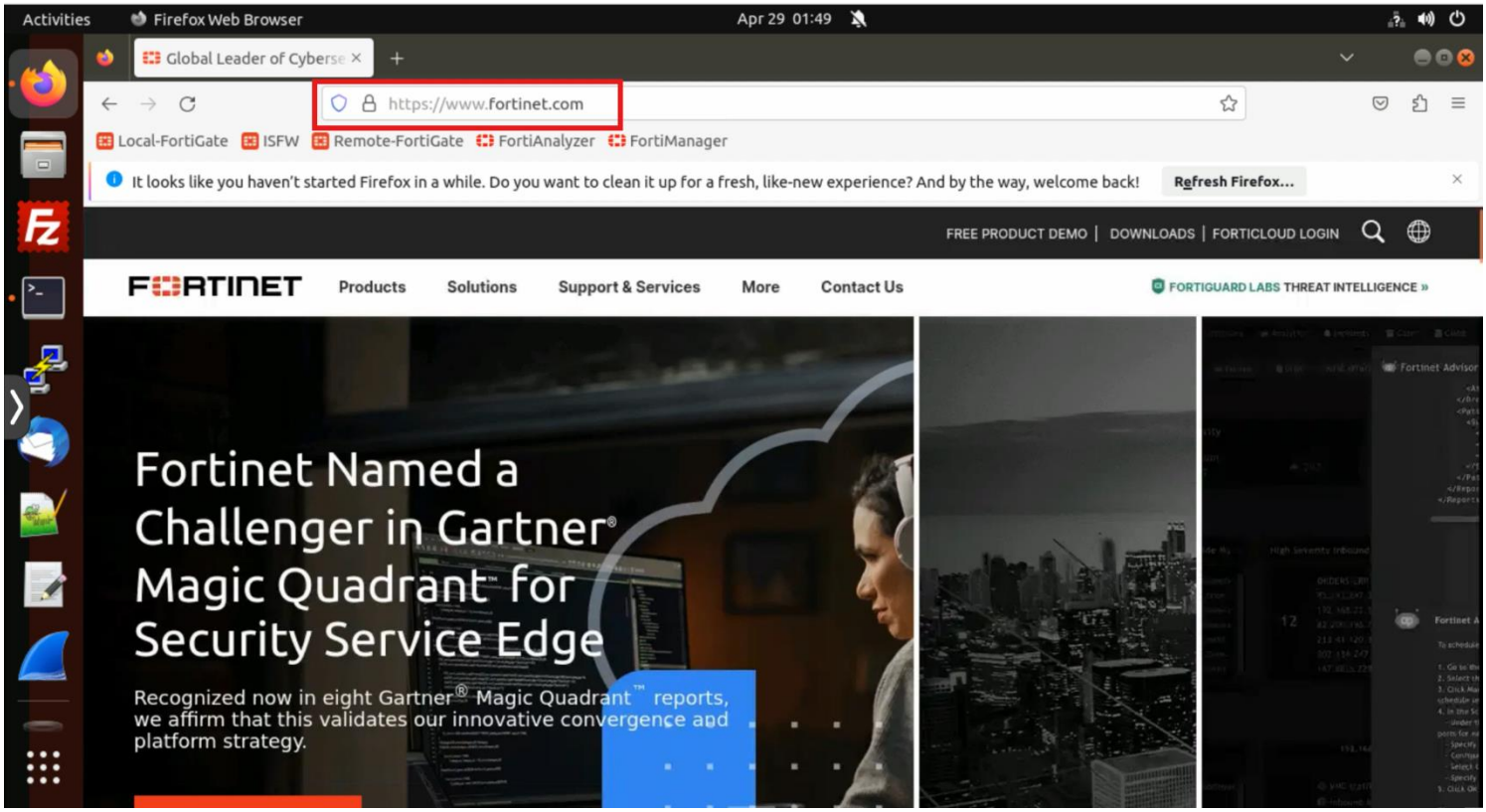
Assign FSSO Users to a Firewall Policy

You will assign your FSSO user group as a source in a firewall policy. This allows you to control access to network resources based on user identity.

To test the connection without assigning the FSSO user group to a firewall policy

1. On the Local-Client VM, open a new browser, and then go to https://www.fortinet.com.

You can see that all users can access the Fortinet website.



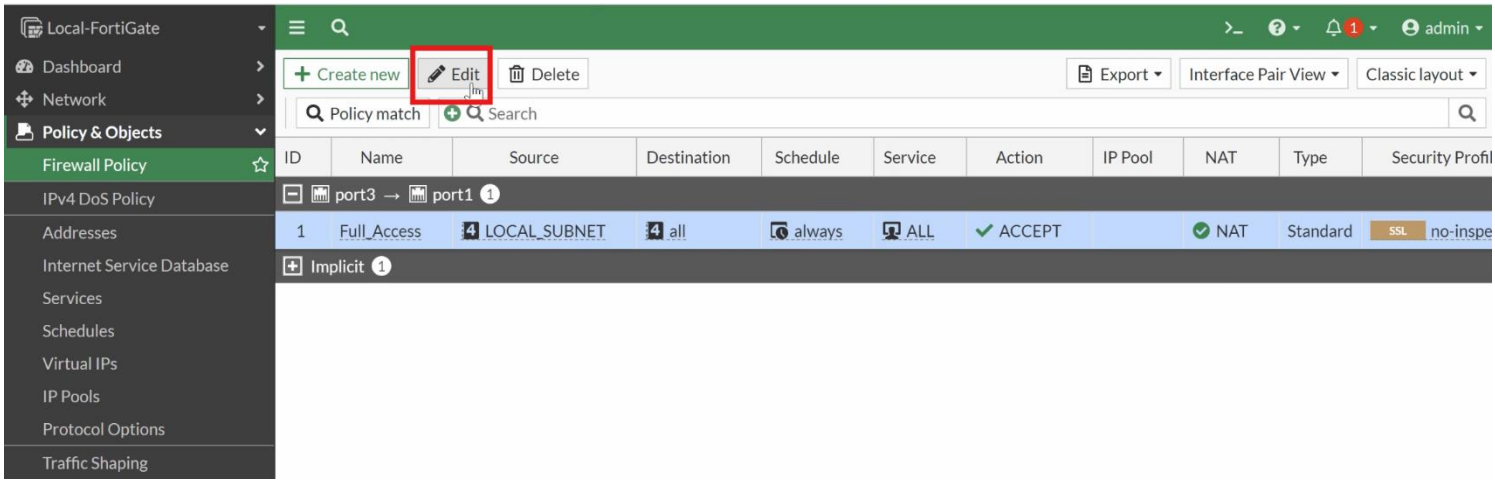
To add the FSSO user group to your firewall policy

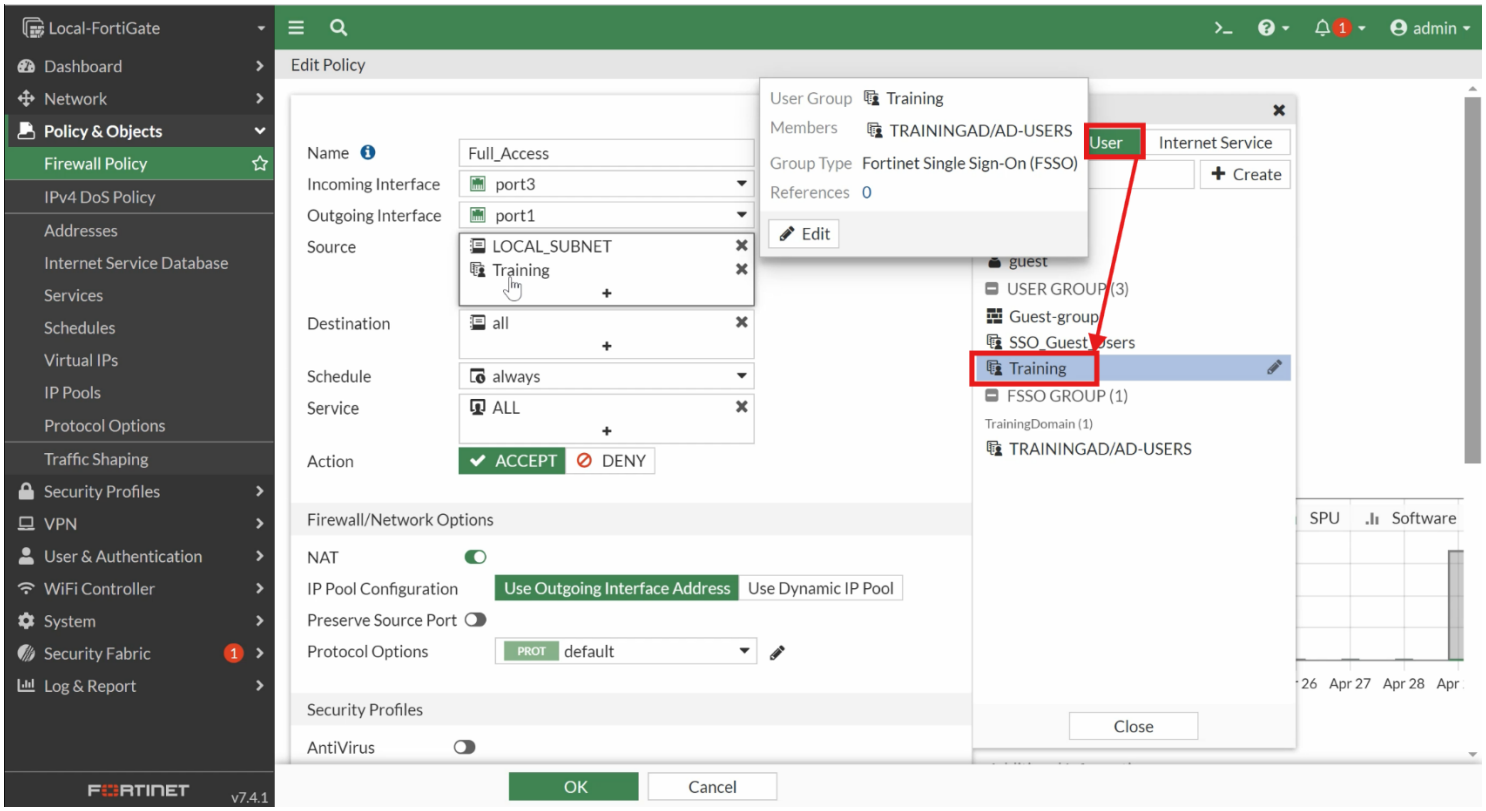
1. Return to the browser where you are logged in to the Local-FortiGate GUI, and then click **Policy & Objects** > **Firewall Policy**.

2. Edit the **Full_Access** firewall policy.

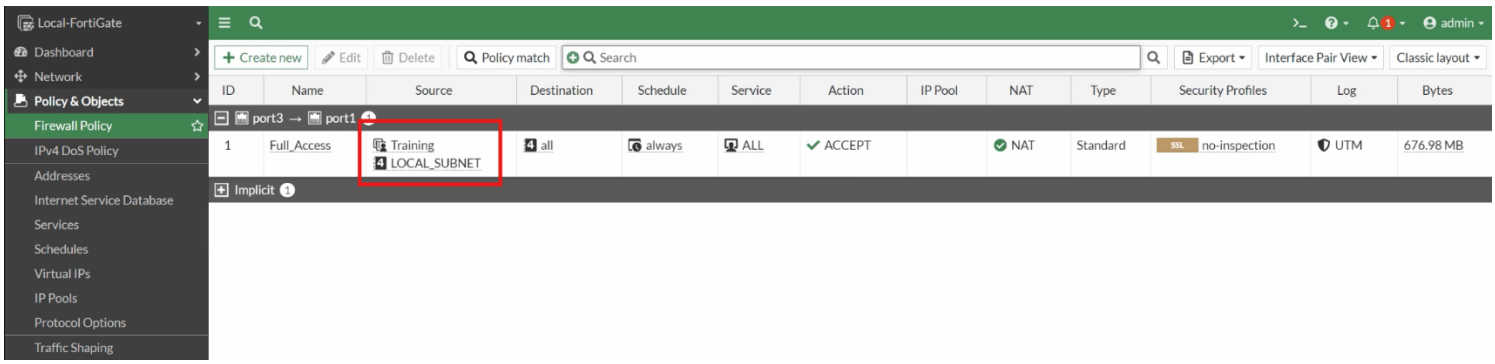
3. In the **Source** field, click **LOCAL_SUBNET**.

4. In the **Select Entries** section, select **User**, and then add the **Training** group.





5. Click **Close**, and then click **OK**.

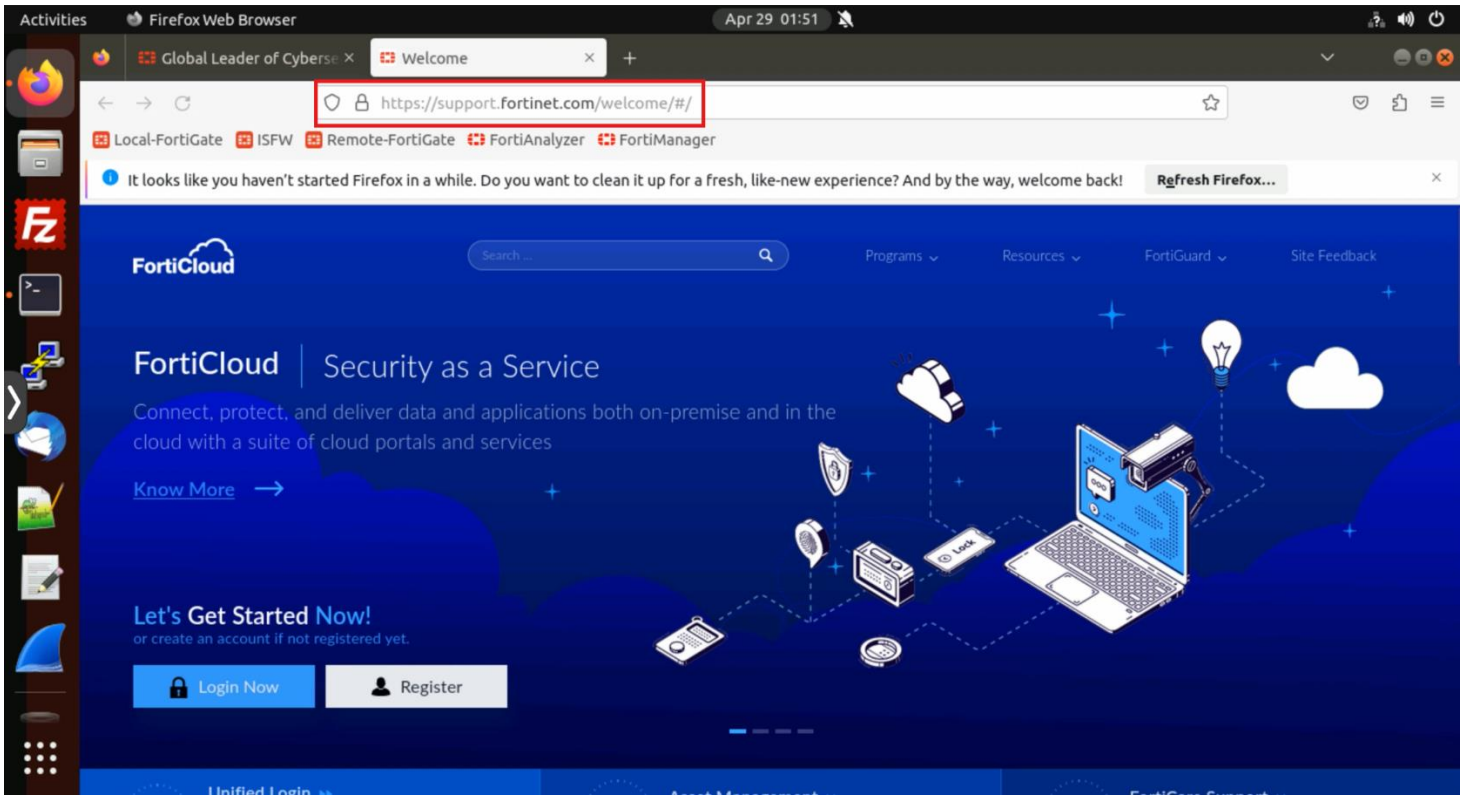


Test FSSO

After a user logs in, they are automatically identified based on their IP address. As a result, FortiGate allows the user to access network resources as policy decisions are made. You will test FSSO.

To test the connection after assigning the FSSO user to the firewall policy

1. On the Local-Client VM, open a new browser tab, and then go to http://support.fortinet.com.



The Python script that is running on the Local-Client VM is already sending user logon events with the following information:

- **user**: aduser1
- **IP**: 10.0.1.10

In this case, the website loads successfully because aduser1 belongs to the configured user group on a firewall policy.

To review the connection status between the FSSO collector agent and FortiGate

1. On the Local-FortiGate CLI, log in with the username admin and password password.
2. Enter the following commands to show the connection status between FortiGate and each collector agent:

```
diagnose debug enable

diagnose debug authd fsso server-status
```

3. Observe the CLI output.

Your FortiGate is connected to the FSSO collector agent.

```
Local-FortiGate #
Local-FortiGate # diagnose debug enable

Local-FortiGate # diagnose debug authd fsso server-status

Local-FortiGate #
Server Name                    Connection Status     Version              Address
-----------                    -----------------     -------              -------
TrainingDomain                 connected             FSAE server 1.1      10.0.1.10

Local-FortiGate #
Local-FortiGate #
Local-FortiGate #
```

To monitor communication between the FSSO collector agent and FortiGate

1. Continuing on the Local-FortiGate CLI, log in with the username admin and password password.
2. Enter the following commands:

```
diagnose debug enable

diagnose debug application authd 8256
```

```
Local-FortiGate #
Local-FortiGate # diagnose debug enable

Local-FortiGate #
Local-FortiGate # diagnose debug application authd 8256
Debug messages will be on for 30 minutes.

Local-FortiGate #
```

3. On the Local-Client VM, on a terminal window, press Ctrl+C to stop the script, and then enter the following command again to simulate a user logon event:

```
python2 fssoreplay.py -l 8000 -f sample.log
```

4. View the output of the diagnose command.

```
Local-FortiGate #
Local-FortiGate #
Local-FortiGate # diagnose debug enable

Local-FortiGate #
Local-FortiGate # diagnose debug application authd 8256
Debug messages will be on for 30 minutes.

Local-FortiGate # fsae_io_ctx_process_msg[TrainingDomain]: received heartbeat 100074
fsae_io_ctx_process_msg[TrainingDomain]: received heartbeat 100075
fsae_io_ctx_process_msg[TrainingDomain]: received heartbeat 100076
_event_error[TrainingDomain]: error occurred in epoll_in: Success
disconnect_server_only[TrainingDomain]: disconnecting
_event_error[TrainingDomain]: error occurred in epoll_err: Success
disconnect_server_only[TrainingDomain]: disconnecting
_event_error[TrainingDomain]: error occurred in epoll_err: Success
disconnect_server_only[TrainingDomain]: disconnecting
connected_state[TrainingDomain]: entering CONNECTED state (vfid=0)
_send_pending_requests[TrainingDomain]: need_gai=0 need_gli=1
fsae_io_ctx_process_msg[TrainingDomain]: received heartbeat 100002
[_process_logon:1079]: ADUSER1 (10.0.1.10, 0) logged on from TrainingDomain.
[_process_logon:1122]: ADUSER1 (10.0.1.10, 0) from TrainingDomain exists.
fsae_io_ctx_process_msg[TrainingDomain]: received heartbeat 100004
fsae_io_ctx_process_msg[TrainingDomain]: received heartbeat 100005
fsae_io_ctx_process_msg[TrainingDomain]: received heartbeat 100006
fsae_io_ctx_process_msg[TrainingDomain]: received heartbeat 100007
```

You generated a logon event on the Local-Client VM using the script, and it was forwarded to FortiGate.

5. Enter the following command to stop the debug process:

```
diagnose debug reset
```

To display the FSSO logon events

1. Continuing on the Local-FortiGate VM, enter the following command:

```
diagnose debug authd fsso list
```

2. Review the output, which shows the FSSO logon events.

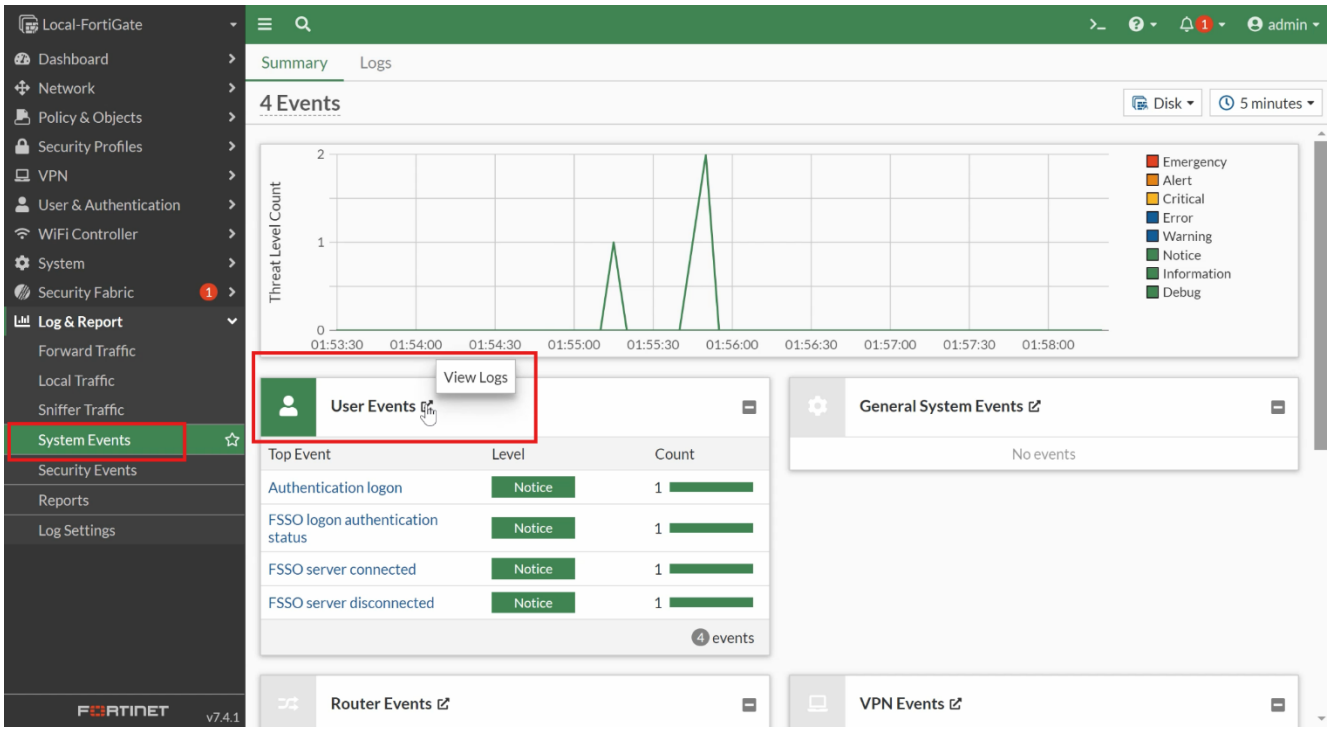
```
Local-FortiGate #
Local-FortiGate #
Local-FortiGate # diagnose debug authd fsso list
----FSSO logons----
IP: 10.0.1.10  User: ADUSER1  Groups: TRAININGAD/AD-USERS  Workstation: C7280677811.TRAININGAD.TRAINING.LAB MemberOf: Training TRAININGAD/AD-USERS
Total number of logons listed: 1, filtered: 0
----end of FSSO logons----

Local-FortiGate #
```

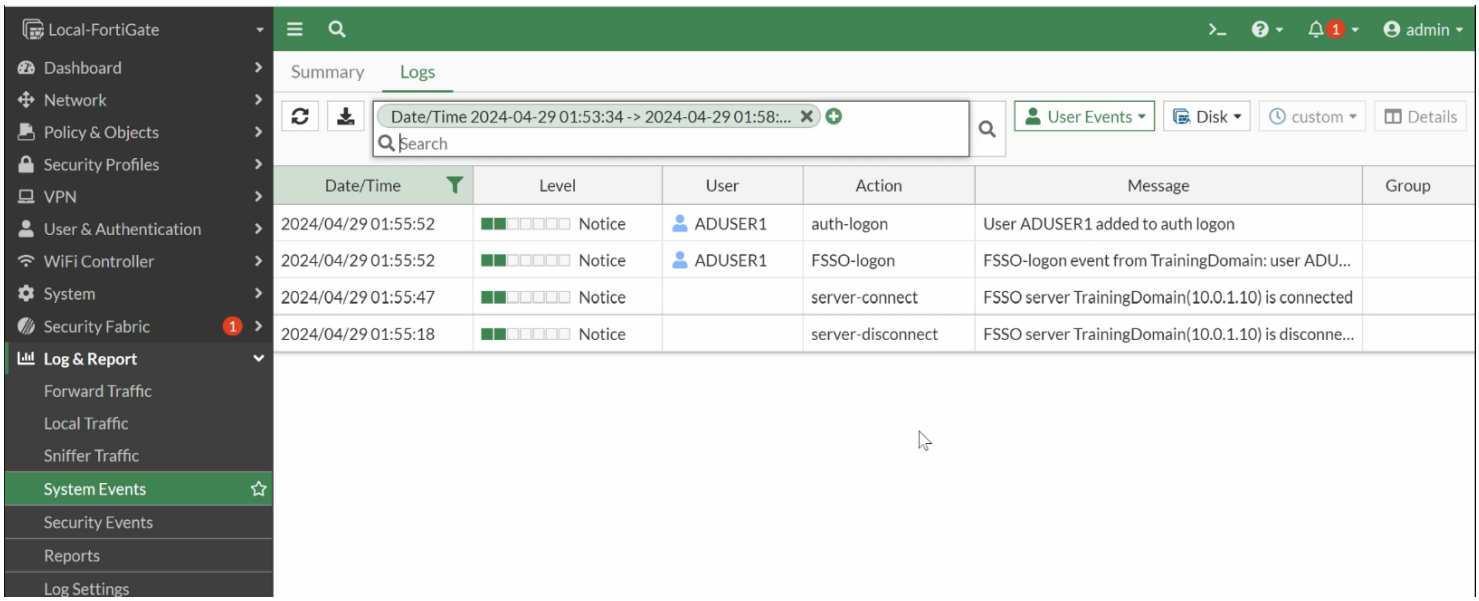
To review the user event logs

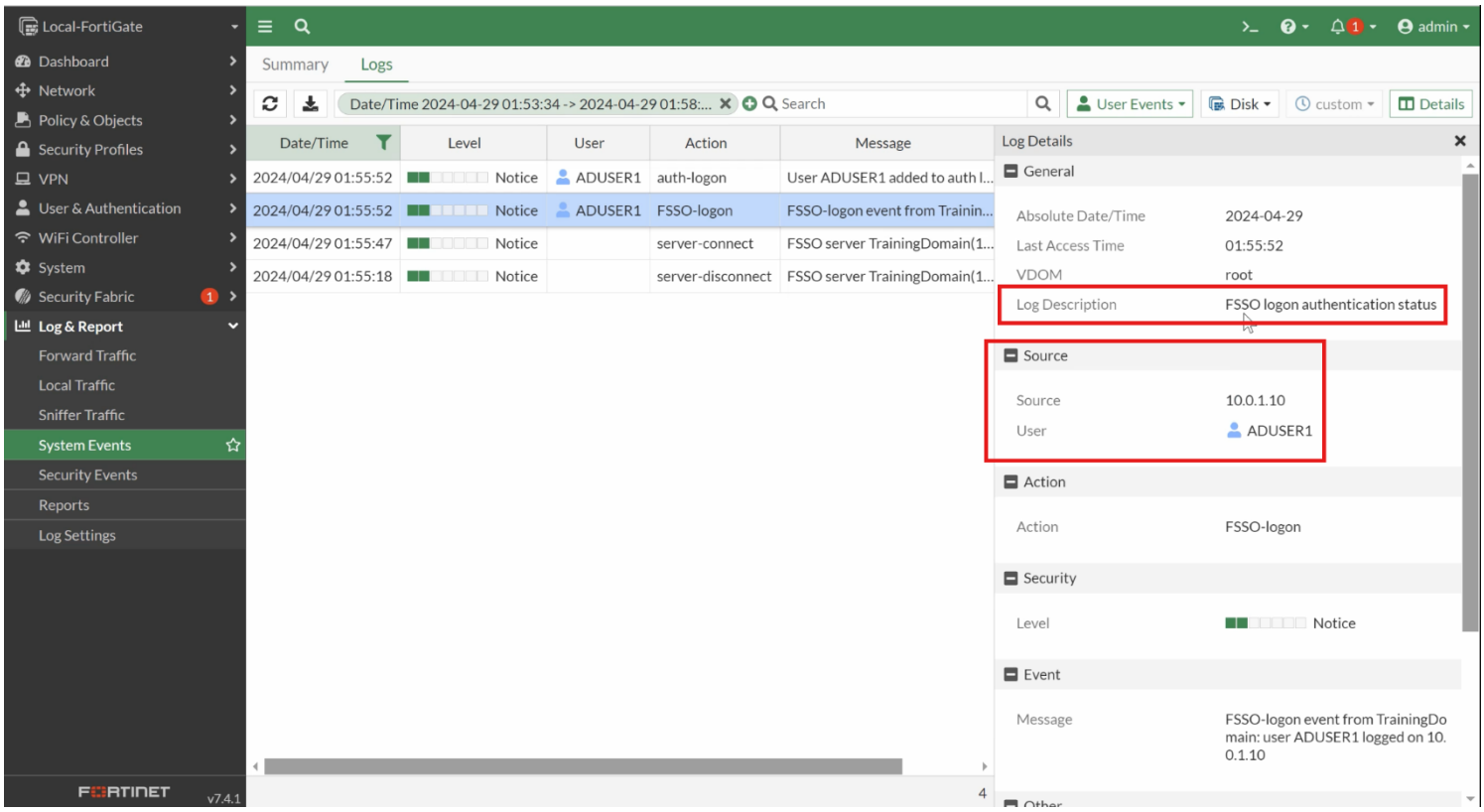
1. Connect to the Local-FortiGate GUI, and then log in with the username admin and password password.

2. Click **Log & Report** > **System Events**, and then in the **User Events** widget, click the **View Logs** arrow.



3. Select a log, and then click **Details** to view more information about it.

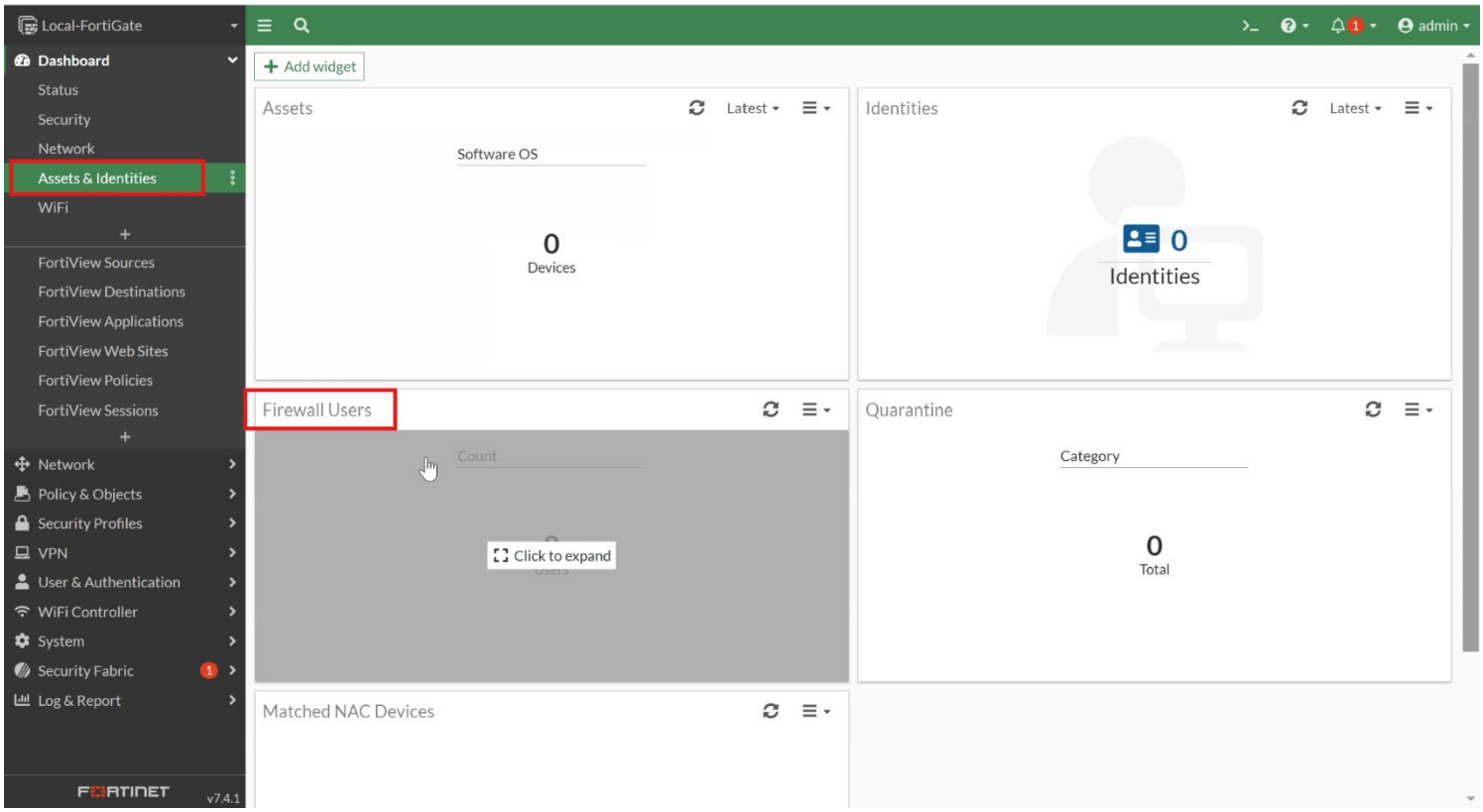


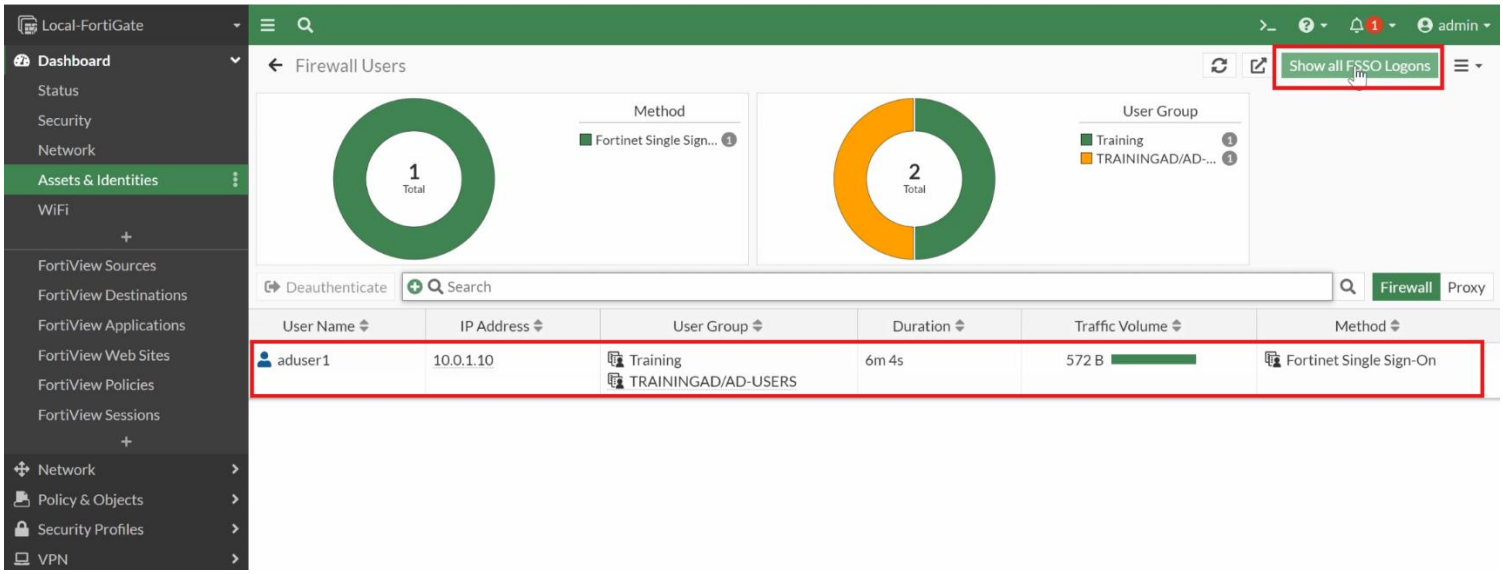


To monitor FSSO logon events

1. Continuing on the Local-FortiGate GUI, click **Dashboard** > **Assets & Identities**, and then double-click **Firewall Users** to expand it to full screen.

2. Click **Show all FSSO Logons**, and then click **Refresh** if the user's details don't appear.






FORTINET