In this lesson, 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.

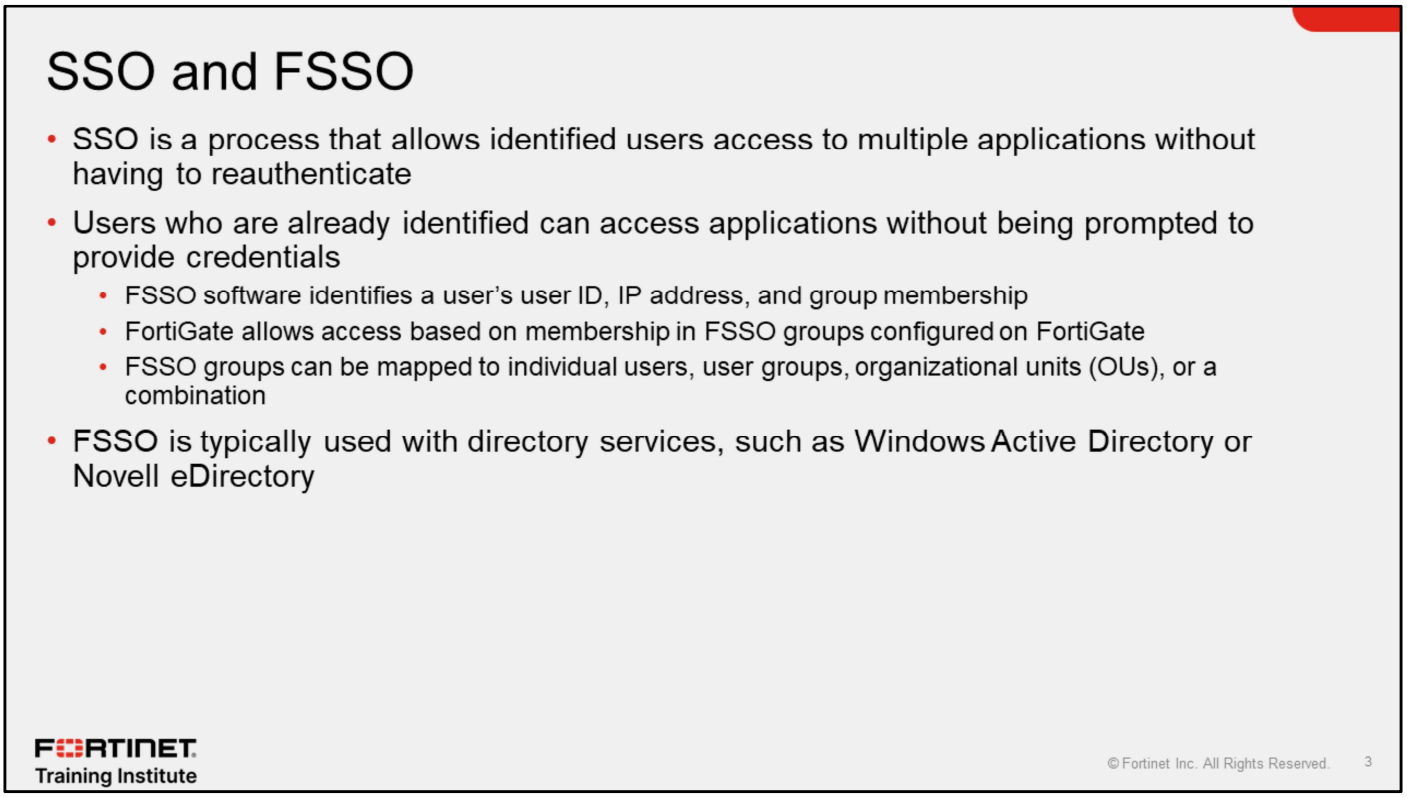
Objectives

- Install FSSO in DC agent mode
- Install collector agent
- Troubleshoot FSSO login issues

FORTINET Training Institute

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in understanding SSO concepts, you will be able to more effectively understand FSSO methods.



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.

FSSO is typically used with directory service networks, such as Windows Active Directory or Novell eDirectory.

FSSO Deployment and Configuration

Microsoft Active Directory (AD)

- Domain controller (DC) agent mode
- Polling mode:
  - Collector agent-based
  - Agentless
- Terminal server (TS) agent
  - Enhances login capabilities of a collector agent or FortiAuthenticator
  - Gathers logins for Citrix and terminal servers where multiple users share the same IP address

Novell eDirectory

- eDirectory agent mode
- Uses Novell API or LDAP setting

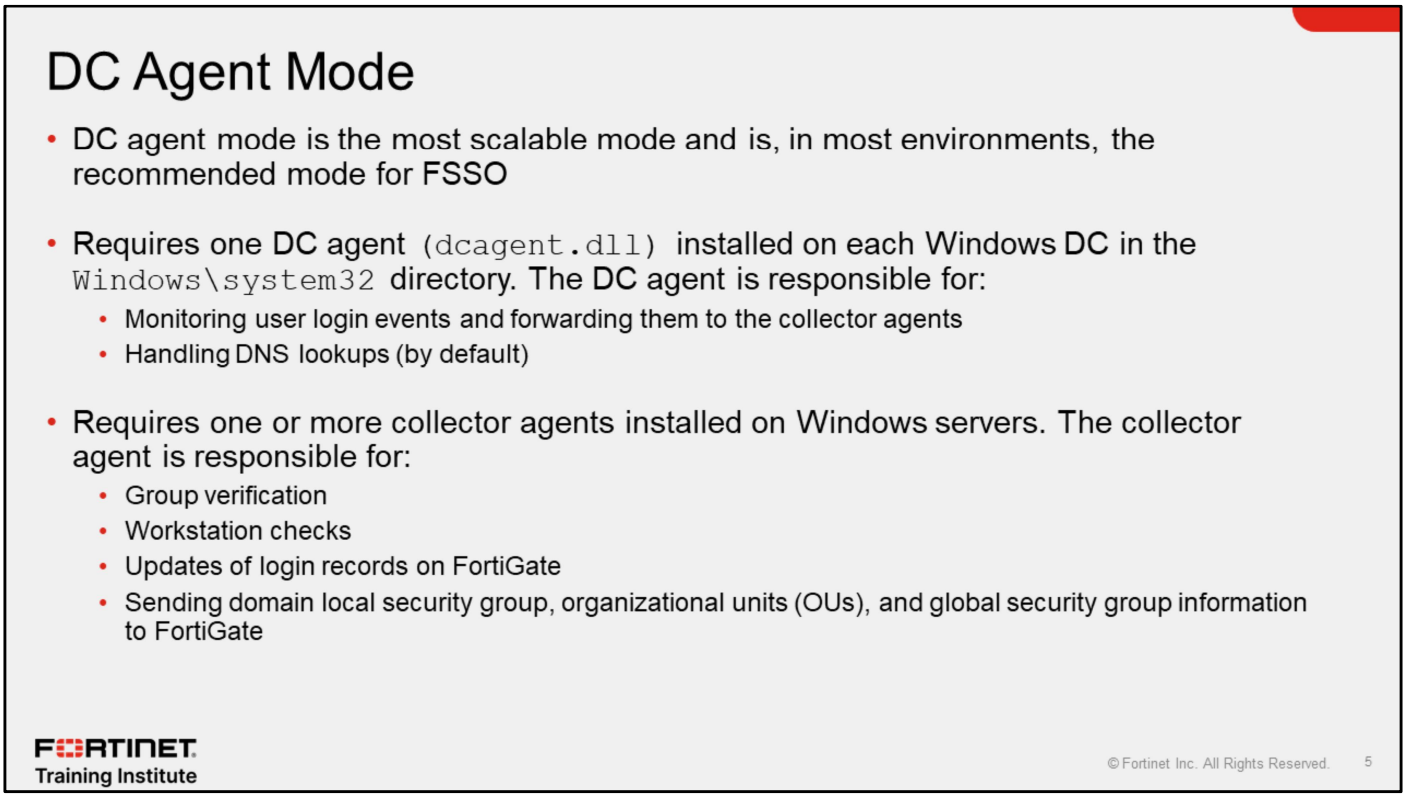
FORTINET Training Institute

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

FSSO for Windows Active Directory (AD) uses a collector agent. Domain controller (DC) agents may also be required, depending on the collector agent working mode. There are two working modes that monitor user sign-on activities in Windows: DC agent mode and polling mode. 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.

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.

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.



DC agent mode is considered the recommended mode for FSSO.

DC agent mode requires:

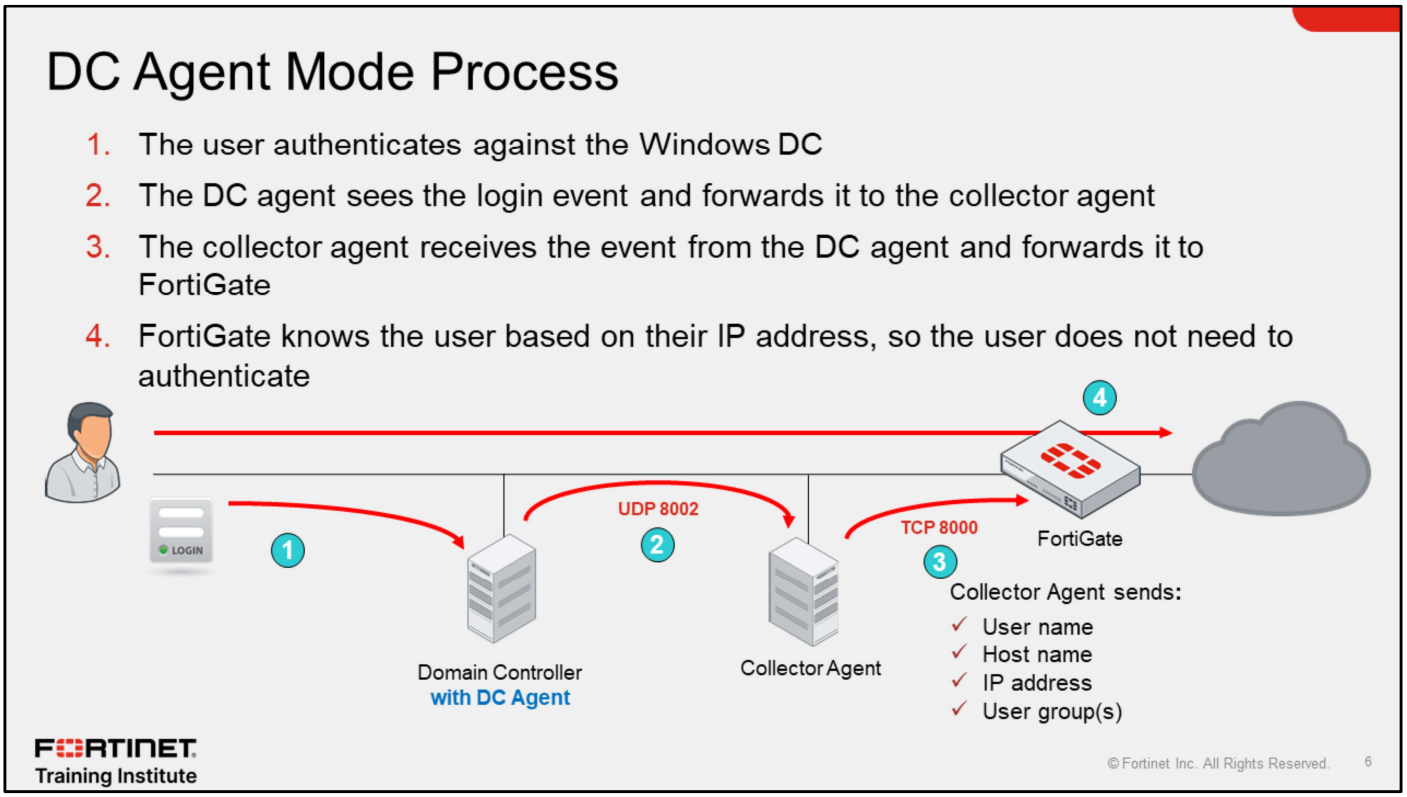
- One DC agent installed on each Windows DC
  If you have multiple DCs, this means that you need multiple DC agents. DC agents monitor and forward user login events to the collector agents.

- 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, and FortiGate updates of login records. 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`



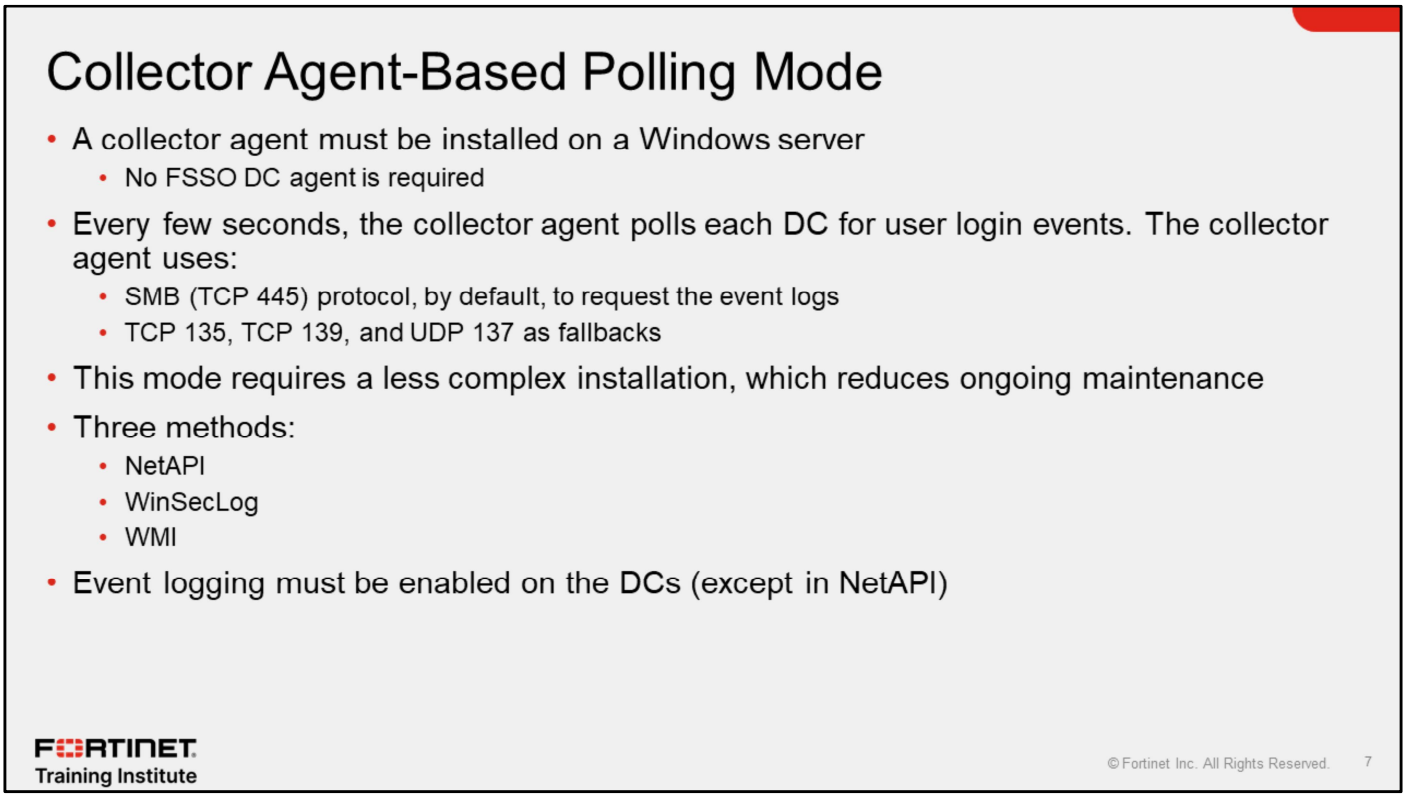
This slide shows the process of information passing between DC agents, the collector agent, and a FortiGate configured for FSSO authentication.

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.

3. The collector agent aggregates all login events and forwards that information to FortiGate. The information sent by the collector agent contains the user name, 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.

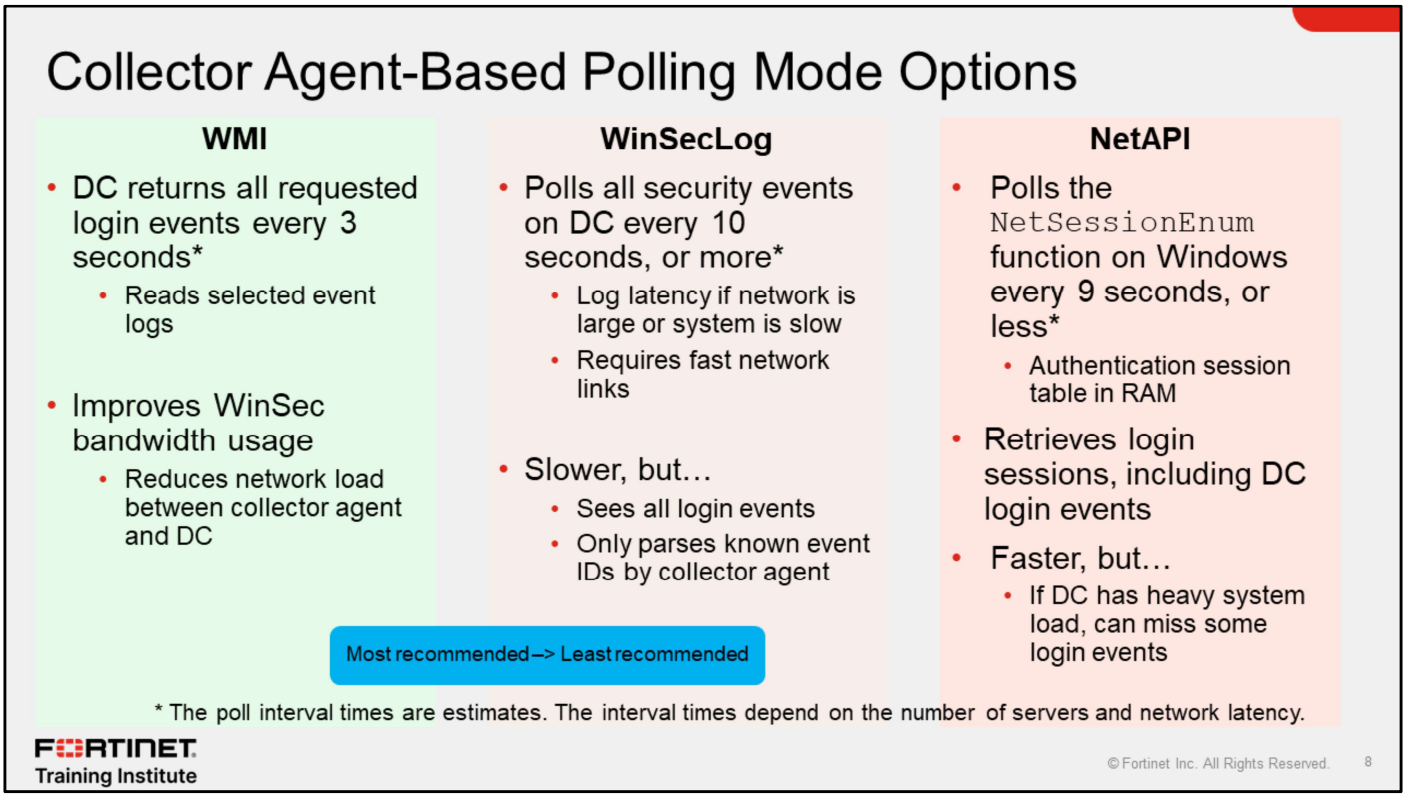
4. FortiGate learns from the collector agent who the user is, their IP address, and some of the AD groups that the user is a member of. When a user tries to access the internet, FortiGate compares the source IP address to its list of active FSSO users. Because the user in this case has already logged 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 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.

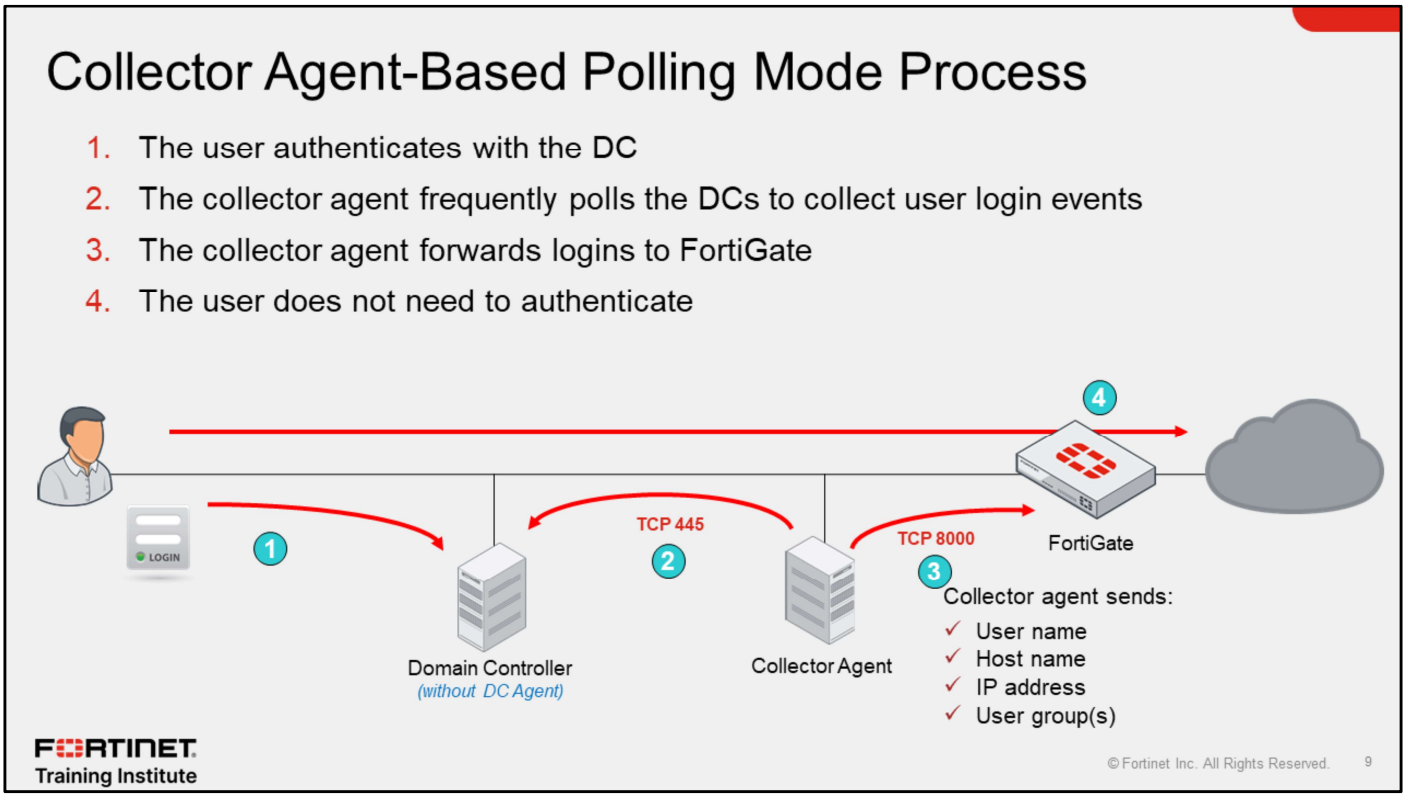


As previously stated, collector agent-based polling mode has three methods (or options) for collecting login information. The order on the slide from left to right shows most recommend to least recommended:

- **WMI**: is a Windows API that gets system information from a Windows server. The DC returns all requested login events. 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. 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 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. 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.



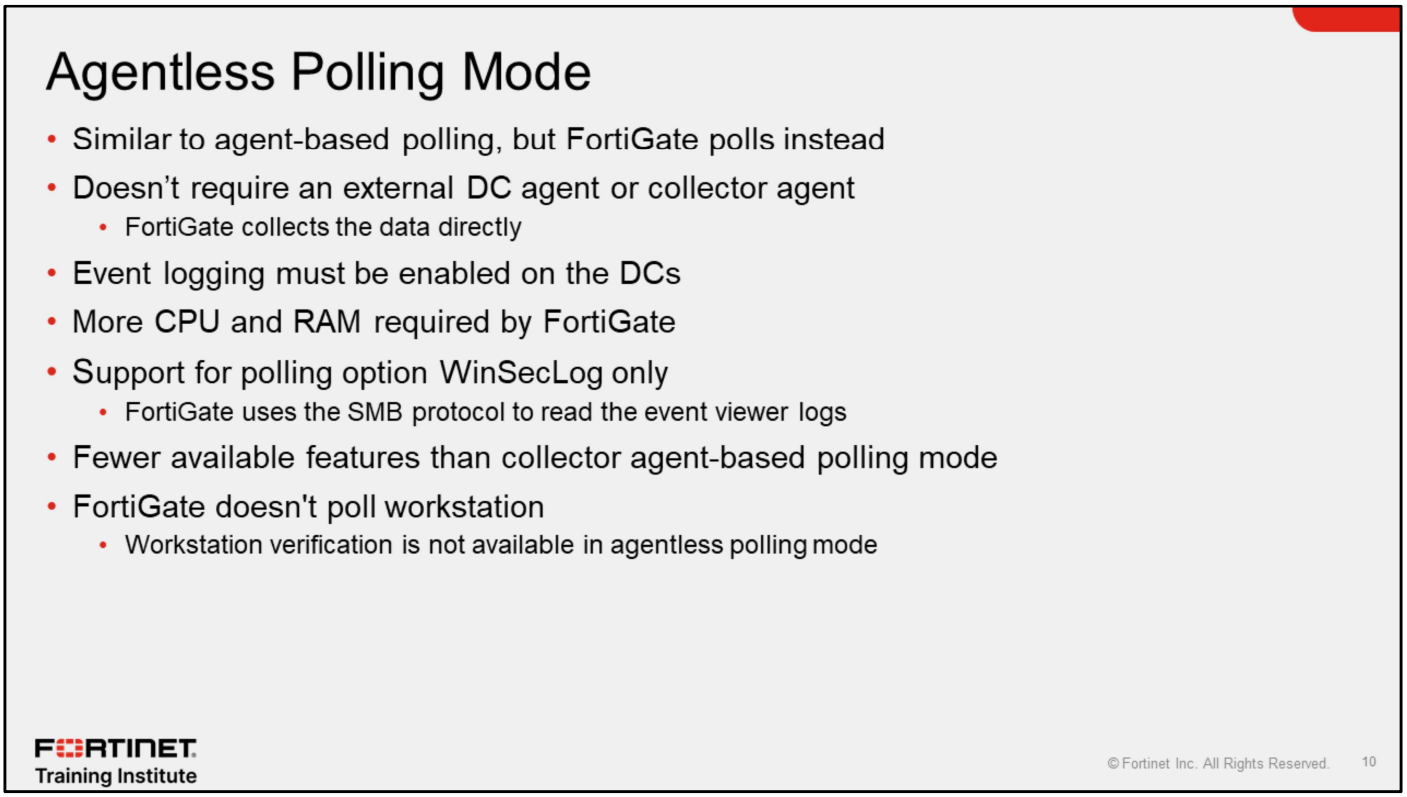
This slide shows an example of FSSO using the collector agent-based polling mode. This example includes a DC, a collector agent, and FortiGate, but the DC doesn't have the dcagent (or, alternatively, dcagent.dll) installed.

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.

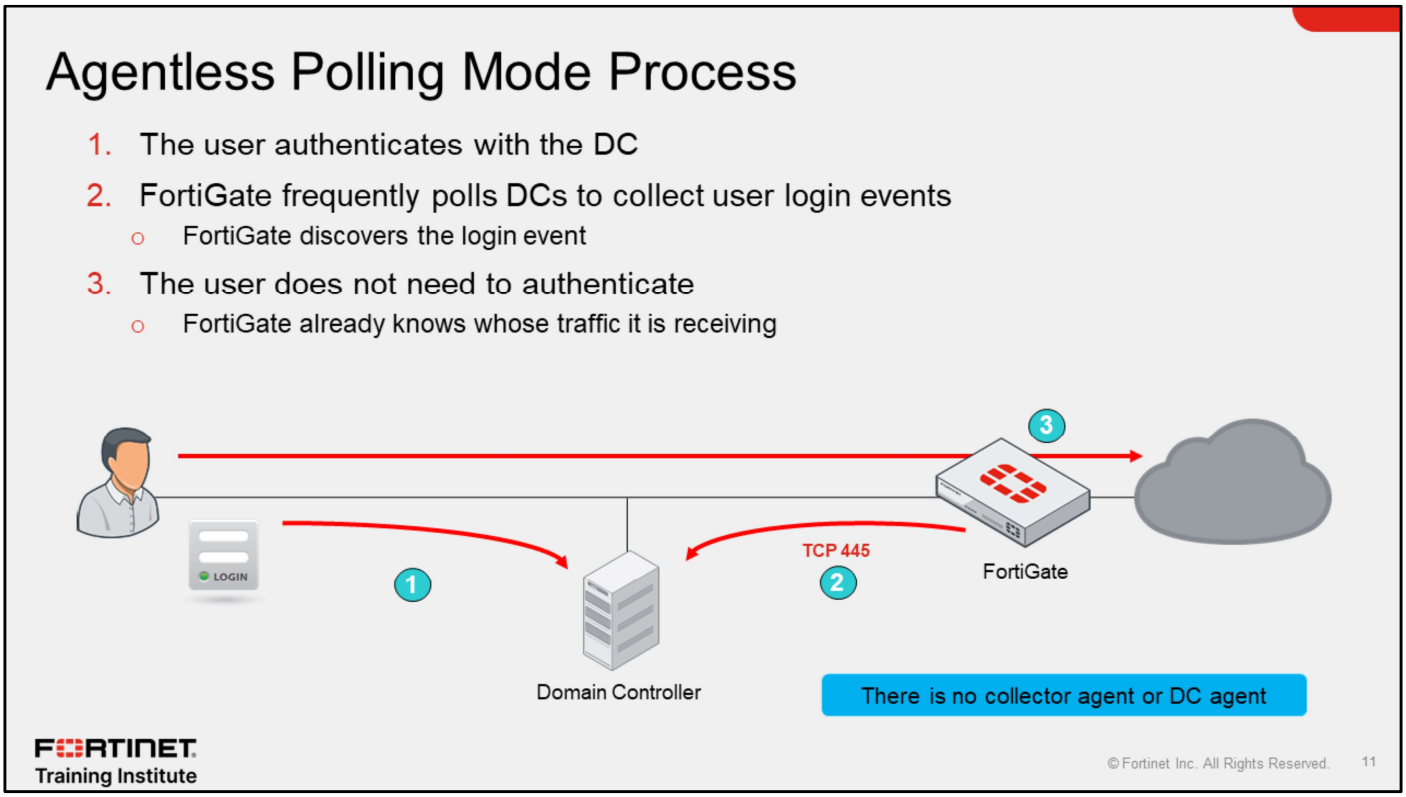


You can deploy FSSO without installing an agent. FortiGate polls the DCs directly, instead of receiving login information indirectly from a collector agent.

Because FortiGate collects all of the data itself, agentless polling mode requires greater system resources, and it doesn't scale as easily.

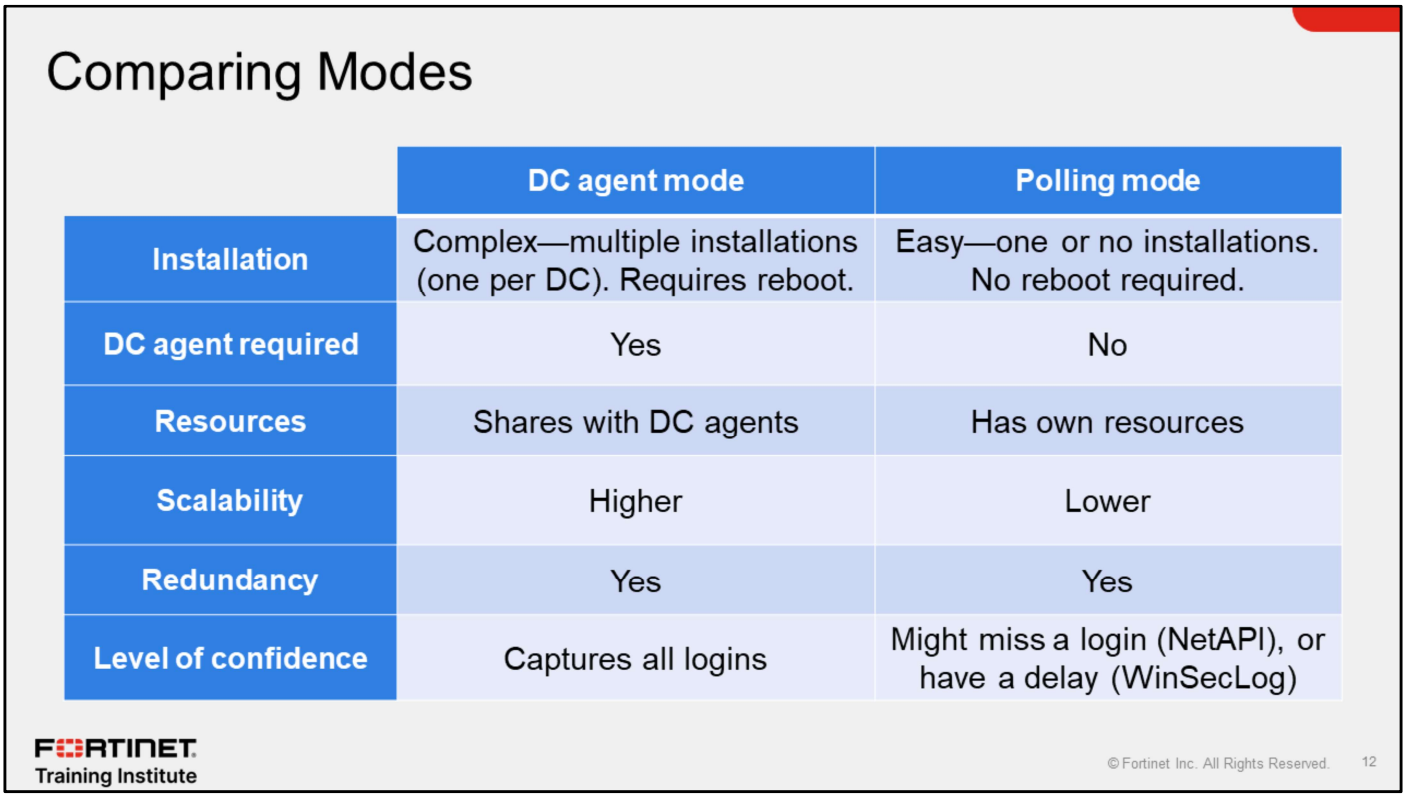
Agentless polling mode operates in a similar way to WinSecLog, but with only two event IDs: 4768 and 4769. Because there's no collector agent, FortiGate uses the SMB protocol to read the event viewer logs from the DCs.

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.



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 user name, 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.



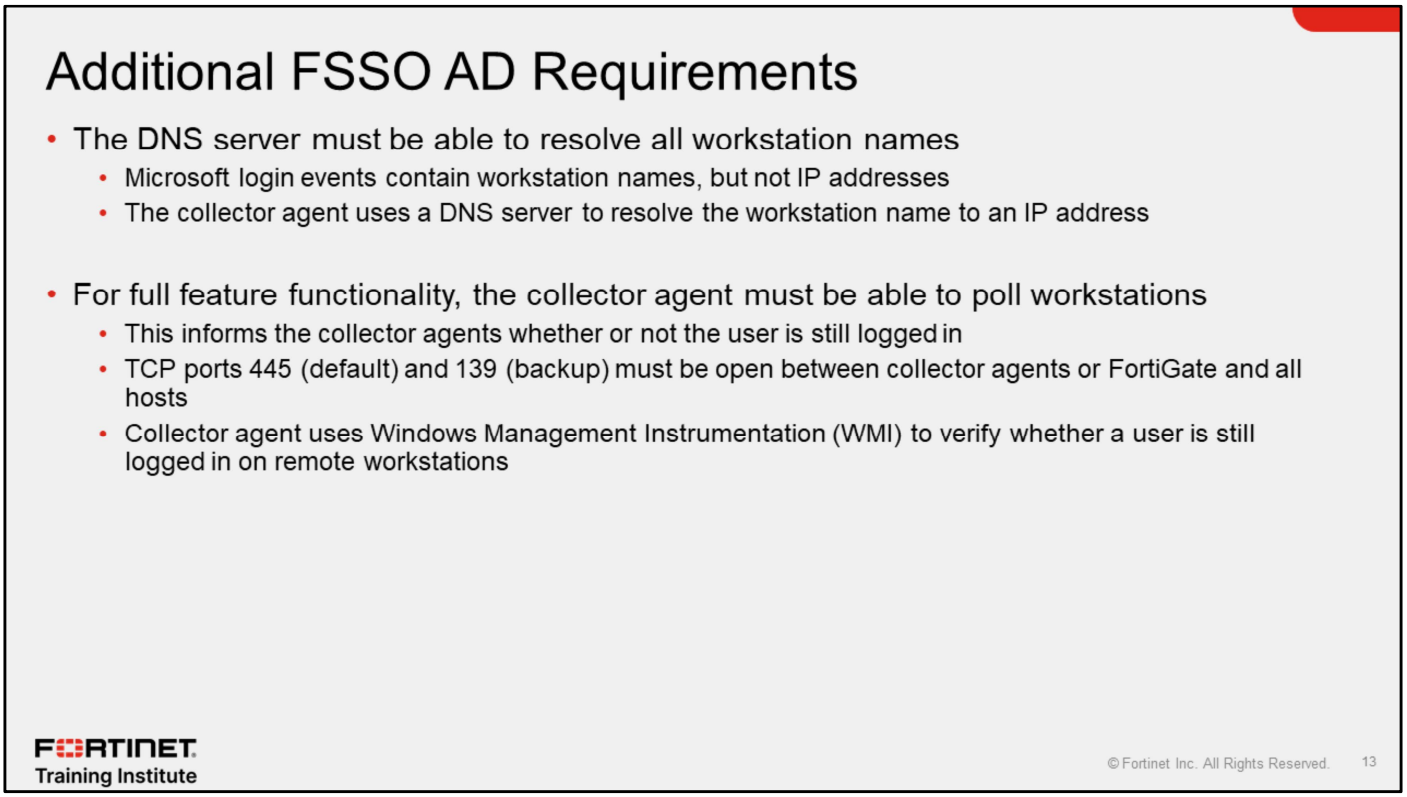
This table summarizes the main differences between DC agent mode and polling mode.

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.



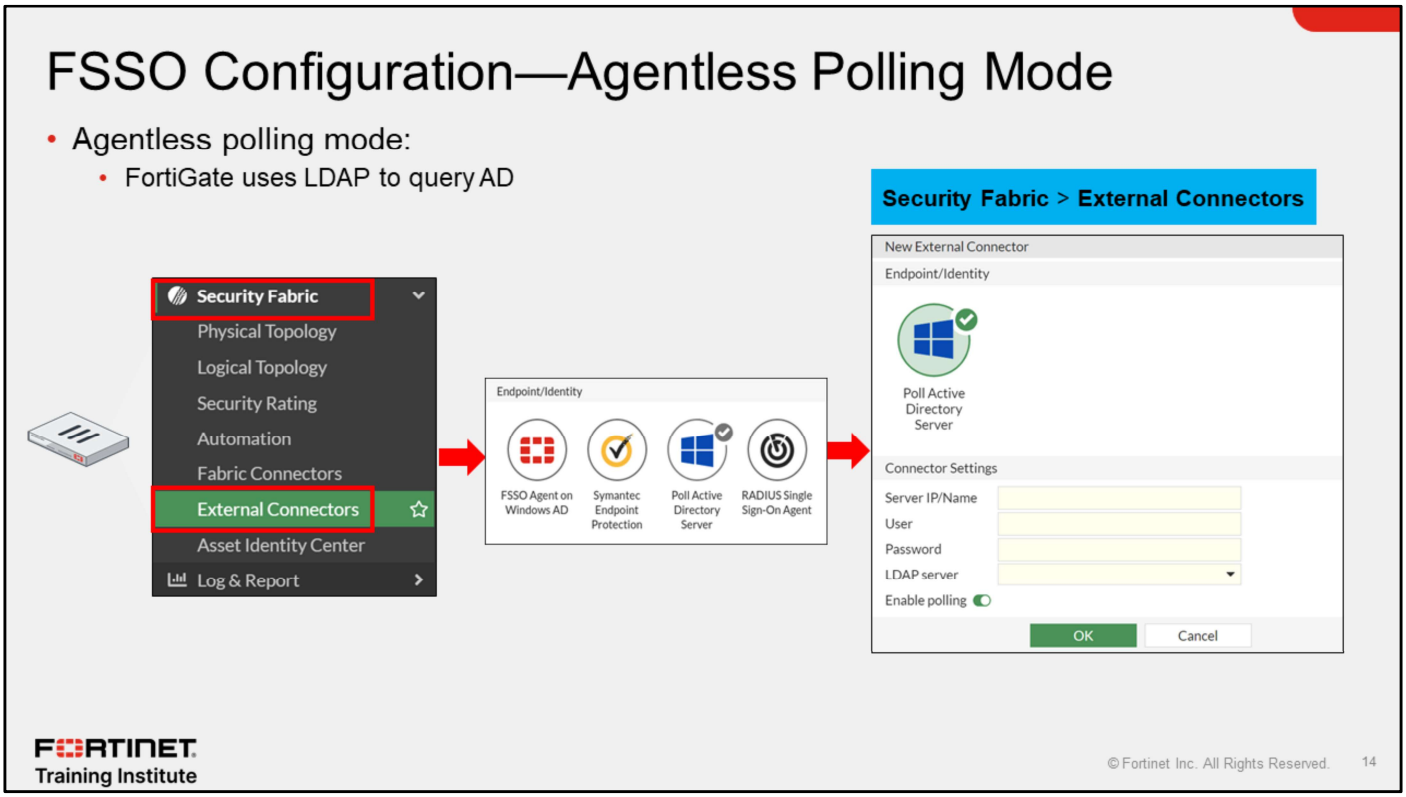
Regardless of the collector method you choose, some FSSO requirements for your AD network are the same:

- 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.

- 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.

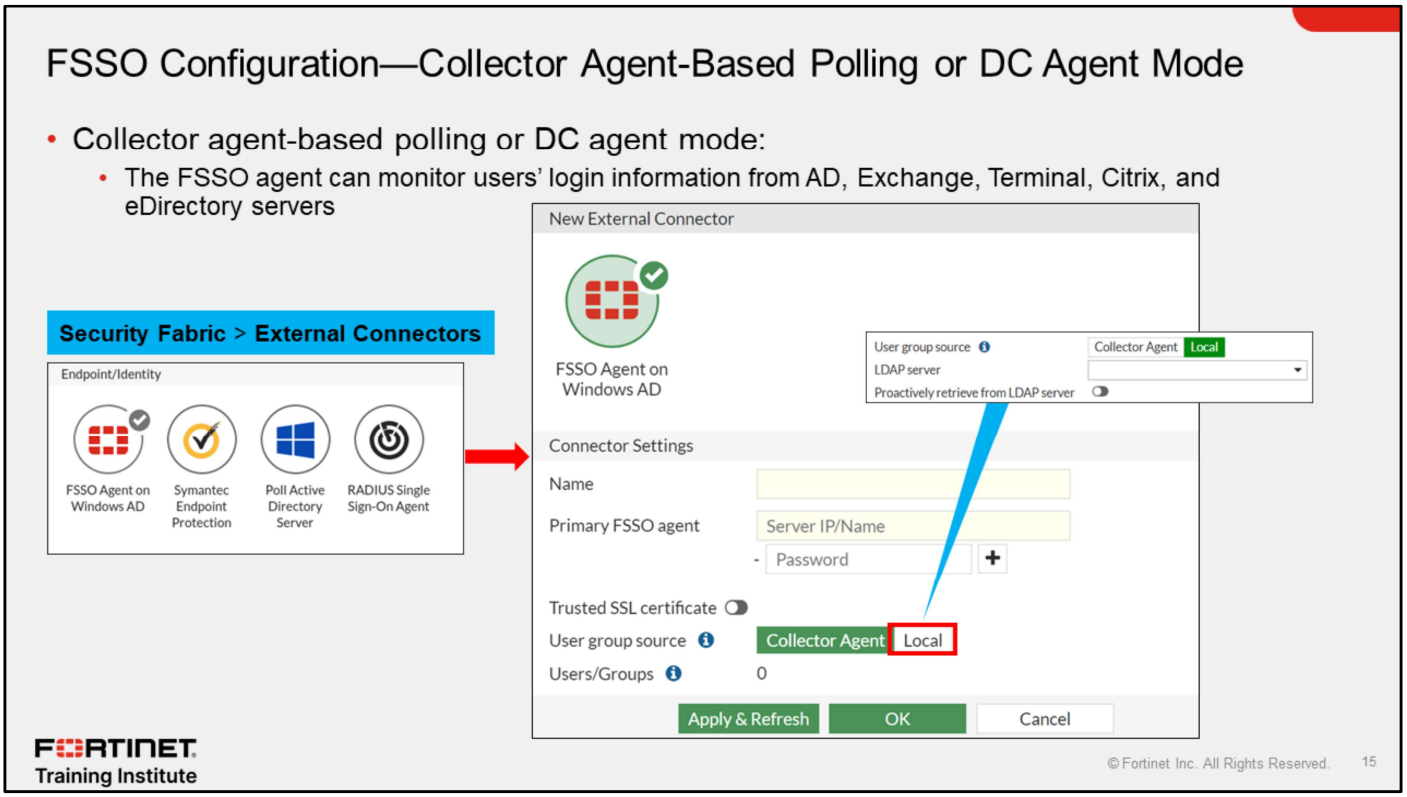
  The collector agent receives the DNS and then performs a DNS resolution in order to check whether the IP address of the user has changed.



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.



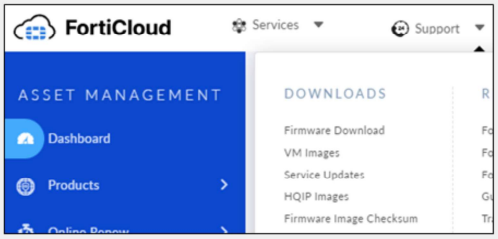
If you have collector agents, using either the DC agent mode or the collector agent-based polling mode, you must select **Fortinet Single-Sign-On Agent** and configure the IP address and password for each collector agent.

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.
- **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.

FSSO Agent Installation

1. Visit the Fortinet support website:
   - https://support.fortinet.com
2. Click **Support** > **Firmware Download**

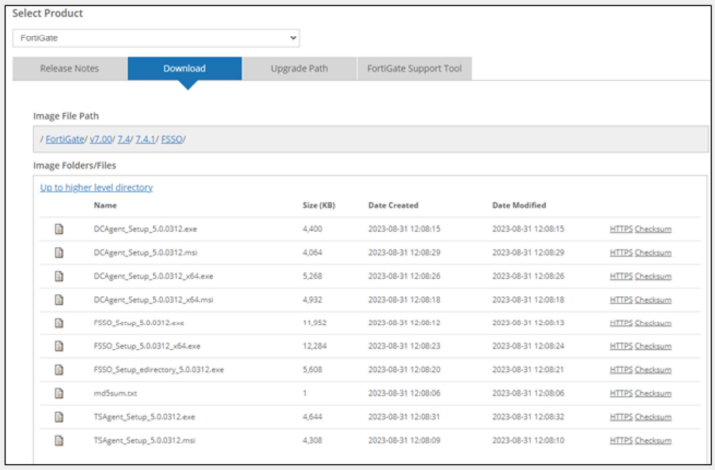


Available agents:

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

3. Select **FortiGate**, then click **Download**.
4. Click **v7.00** > **7.4** > **7.4.1** > **FSSO**

   Example image below:



FORTINET Training Institute

 16

The FSSO agents are available on the Fortinet Support website. There you will find the following:

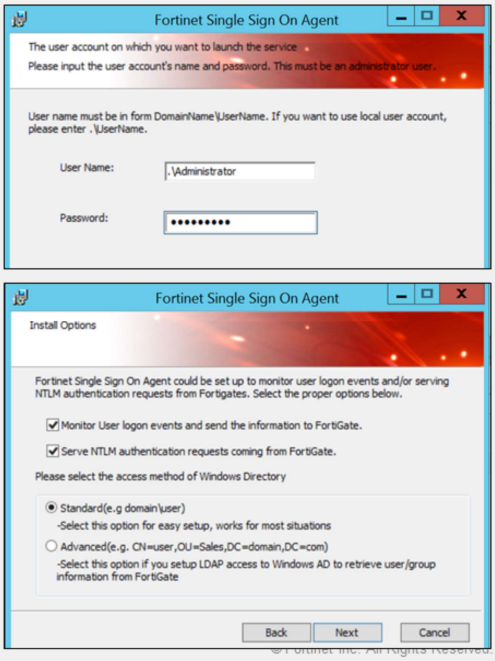
- The DC agent
- The collector agent for Microsoft servers: FSSO_Setup
- The collector agent for Novell directories: FSSO_Setup_edirectory
- The terminal server agent (TSagent) installer for Citrix and terminal servers: TSAgent_Setup

Also, for each agent, there are two versions: the executable (`.exe`) and Microsoft Installer (`.msi`).

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

FSSO Collector Agent Installation Process

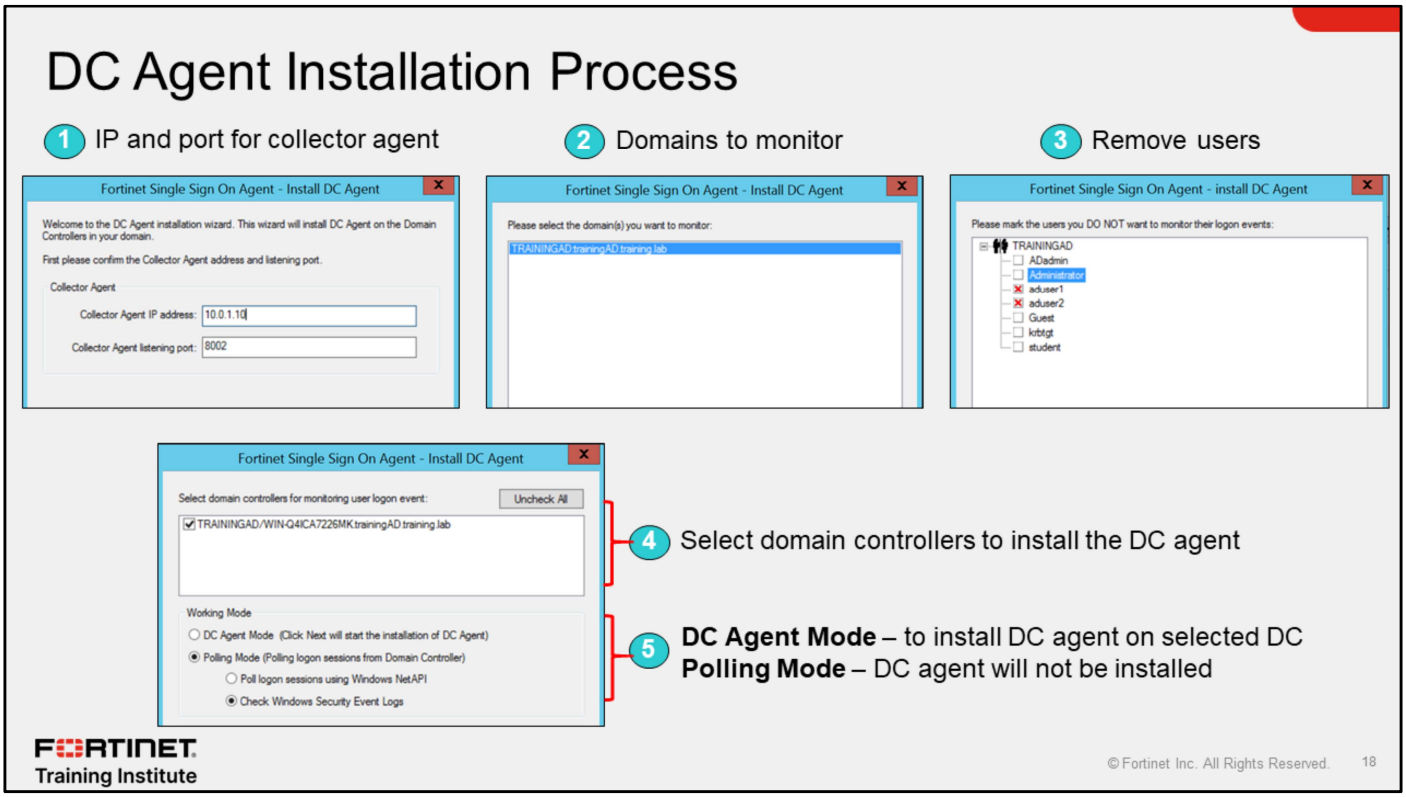
1. Run the installation process as `Administrator`
2. Enter the user name in the following format:
   - `DomainName\UserName`
3. Configure the collector agent for:
   - Monitoring logins
   - NTLM authentication
   - Directory access
4. Optionally, launch the DC agent installation wizard before exiting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



FORTINET Training Institute

After you've downloaded the collector agent, run the installation process as Administrator and follow these steps in the installation wizard:

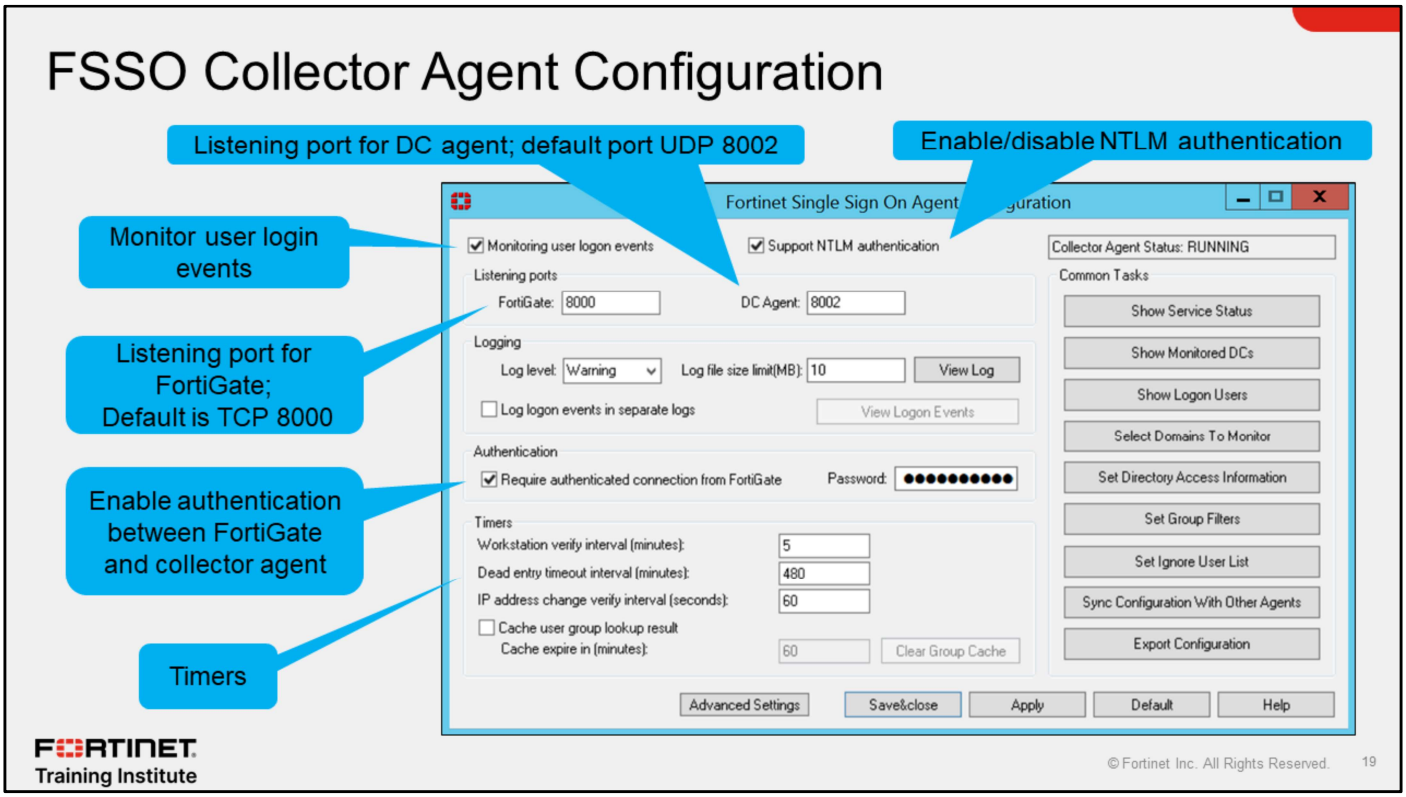
1. Read and accept the license agreement.
2. Optionally, change the installation location. The default folder is named `FSAE` (Fortinet Server Authentication Extension).
3. Enter the username. By default, the agent uses the name of the currently running account; however, you can change it using the format: **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 lesson.
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.



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

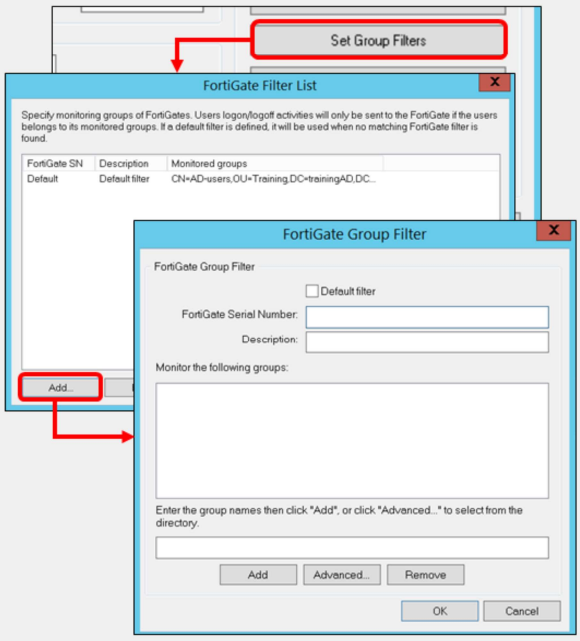


On the FSSO agent configuration GUI, you can configure settings such as:

- 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

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



FORTINET Training Institute

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.

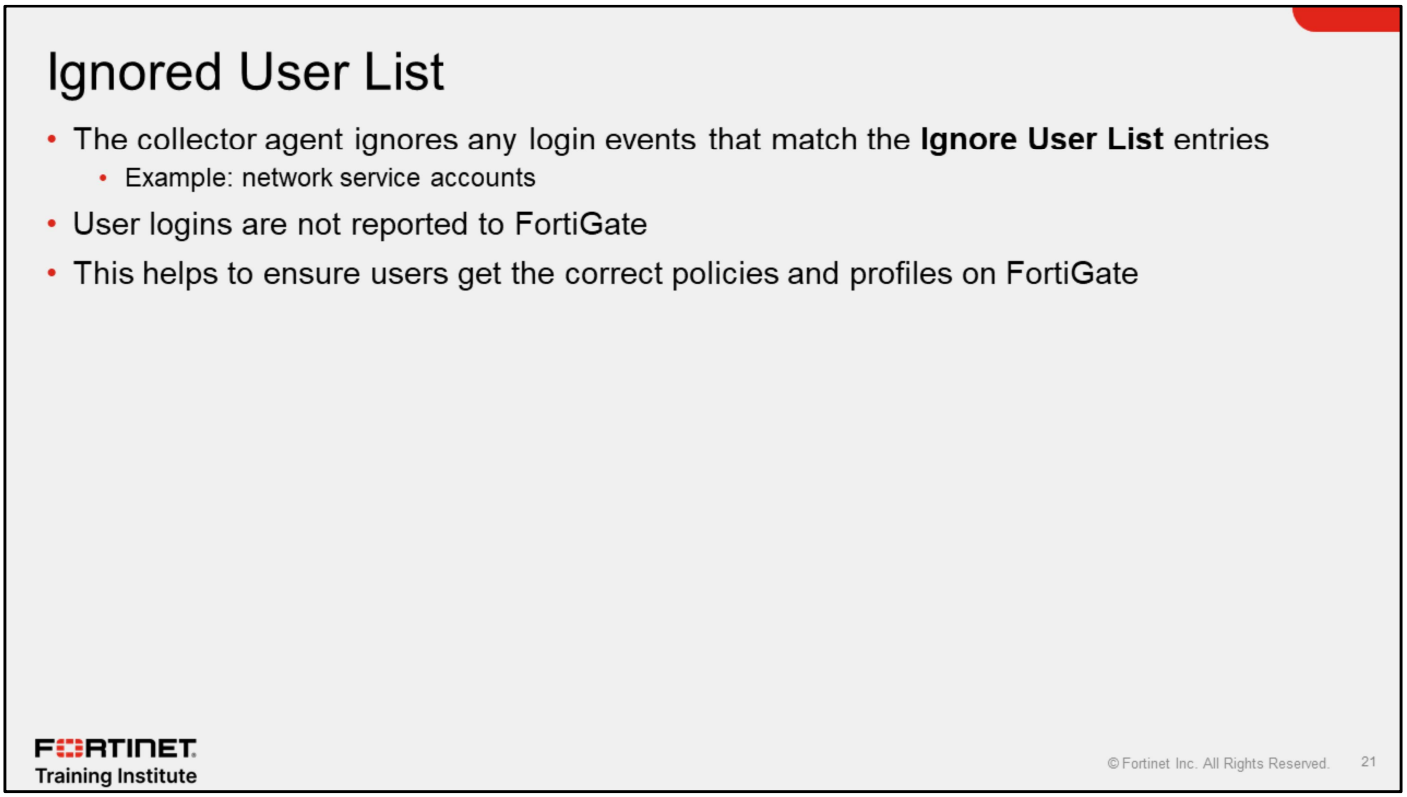
Monitoring the entire group list in a large AD structure is highly inefficient, and a waste of resources. Most FSSO deployments need group segmentation (at least four or five groups), with the intention of assigning varying levels of security profile configurations to the different groups, using identity-based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



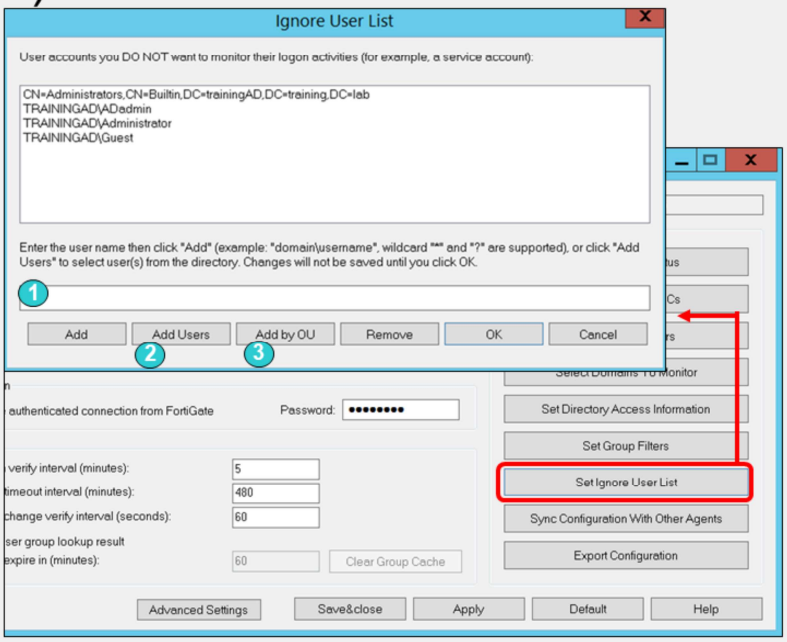
The FSSO collector agent ignores any login events that match the **Ignore User List** entries. Therefore, these login events are not recorded by the collector agent, nor are they reported to FortiGate.

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.

Ignored User List (Contd)

To add users to the ignore list:

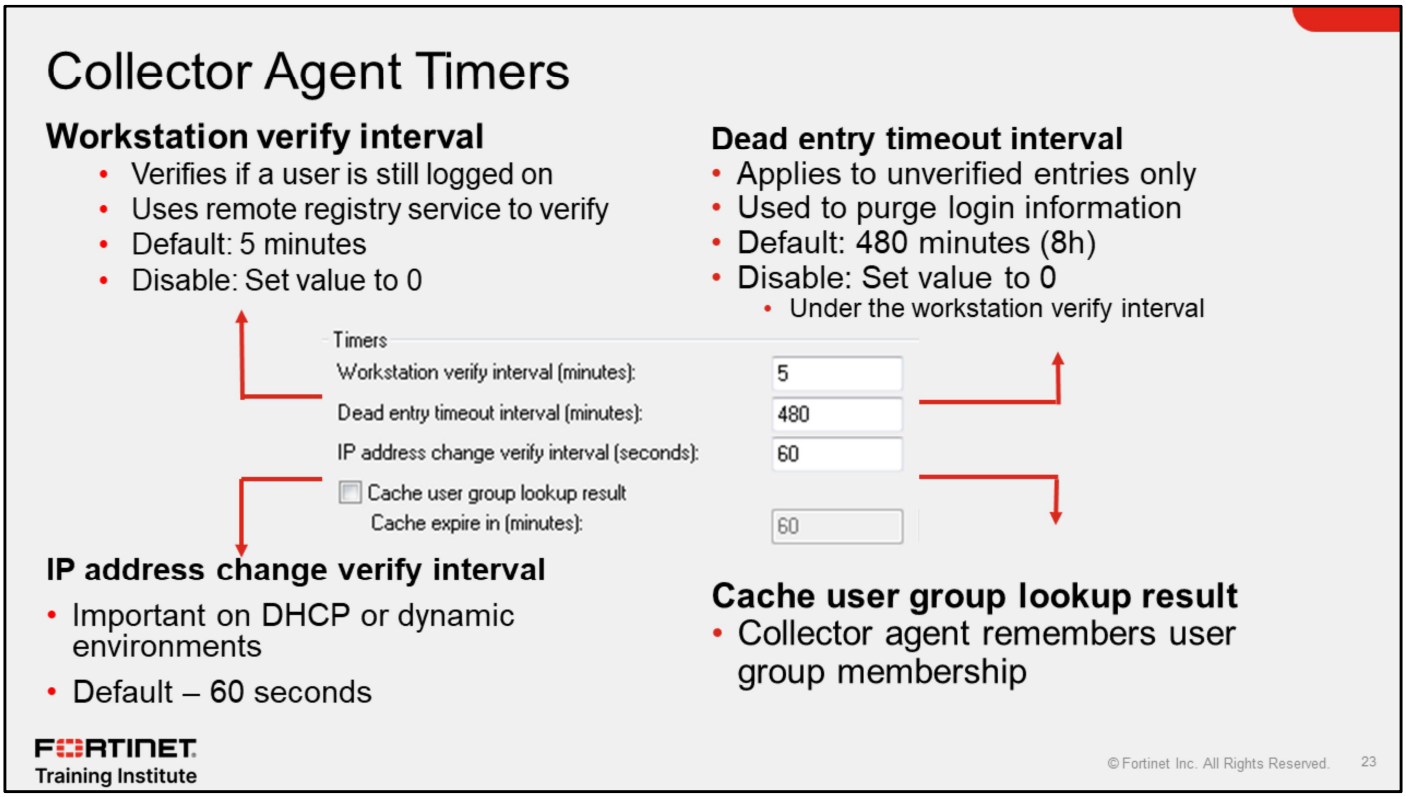
1. Manual entry
2. **Add Users**: Select users you do not want to monitor
3. **Add by OU**: Select an OU from the directory tree



FORTINET Training Institute

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

- Manually enter the username.
- Click **Add Users**, and then choose the users you do not want to monitor.
- 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**.



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**. This setting controls when the collector agent connects to individual workstations on port 139 (or port 445), and uses the remote registry service to verify if a user is still logged in to the same station. It changes the status of the user under **Show login User**, to **not verified** when it cannot connect to the workstation. 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**. 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.

- **IP address change verify interval**. 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. The domain DNS server should be accurate; if the DNS server does not update the affected records promptly, the collector agent's IP information is inaccurate.

- **Cache user group lookup result**. 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.

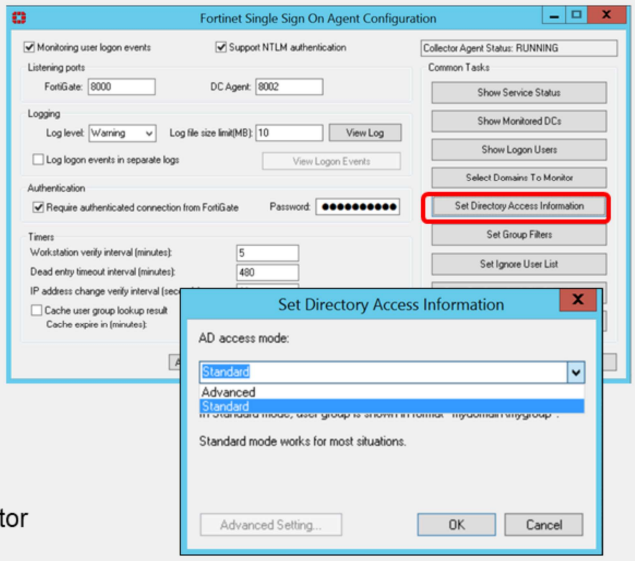
AD Access Mode Configuration

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



FORTINET Training Institute

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** and **Advanced**.

The main difference between modes is the naming convention used:
- **Standard** mode uses the Windows convention, NetBios: `Domain\groups`
- **Advanced** mode uses the LDAP convention: `CN=User`, `OU=Name`, `DC=Domain`

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.

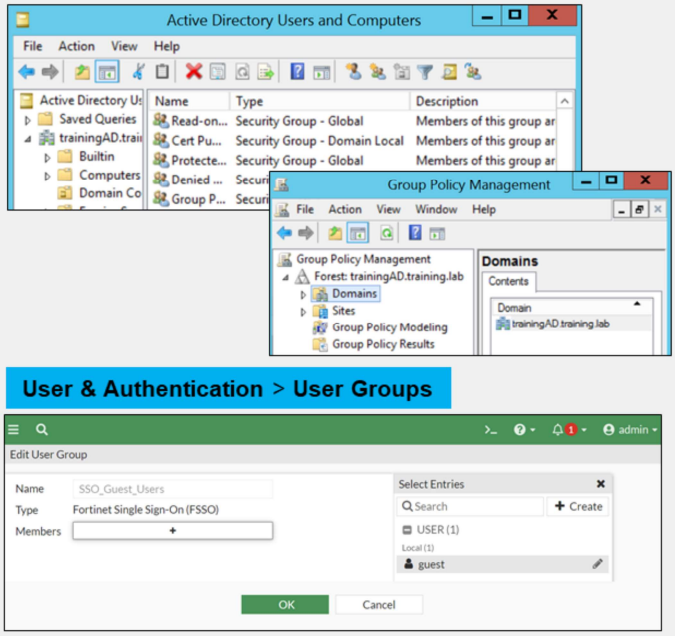
AD Group Support

Group type supported:

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

If the user is not part of an FSSO group:

- For passive FSSO authentication:
  - User is part of **SSO_Guest_Users**
- For passive and active FSSO authentication:
  - User is prompted to log in



User & Authentication > User Groups

FORTINET Training Institute

 25

In AD settings, not all group types are supported. AD settings supports 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.

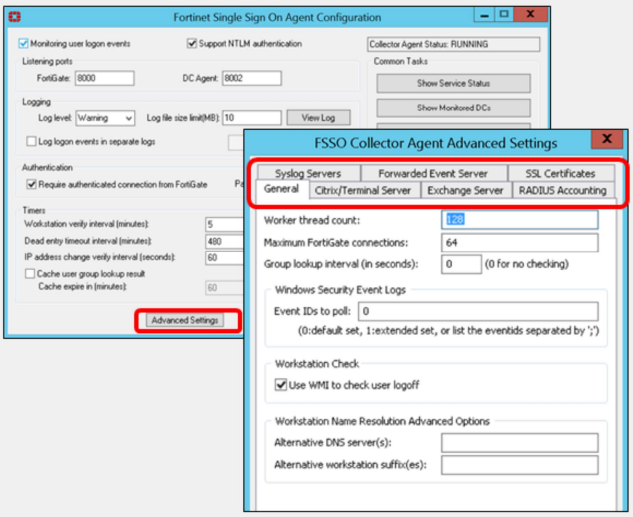
However, if both passive and active authentication are enabled for specific traffic, you cannot use **SSO_Guest_Users**, because traffic from IP addresses not on the FSSO user list must be prompted to enter their credentials.

Advanced Settings

Citrix/Terminal Server
- Terminal server (TS) agent mode: monitors user logins in real time
- Requires a collector agent
  - No polling support from FortiGate

RADIUS Accounting
- Notify the firewall upon login and logout events

Syslog Servers
- Notify the firewall upon login and logout events



FORTINET Training Institute

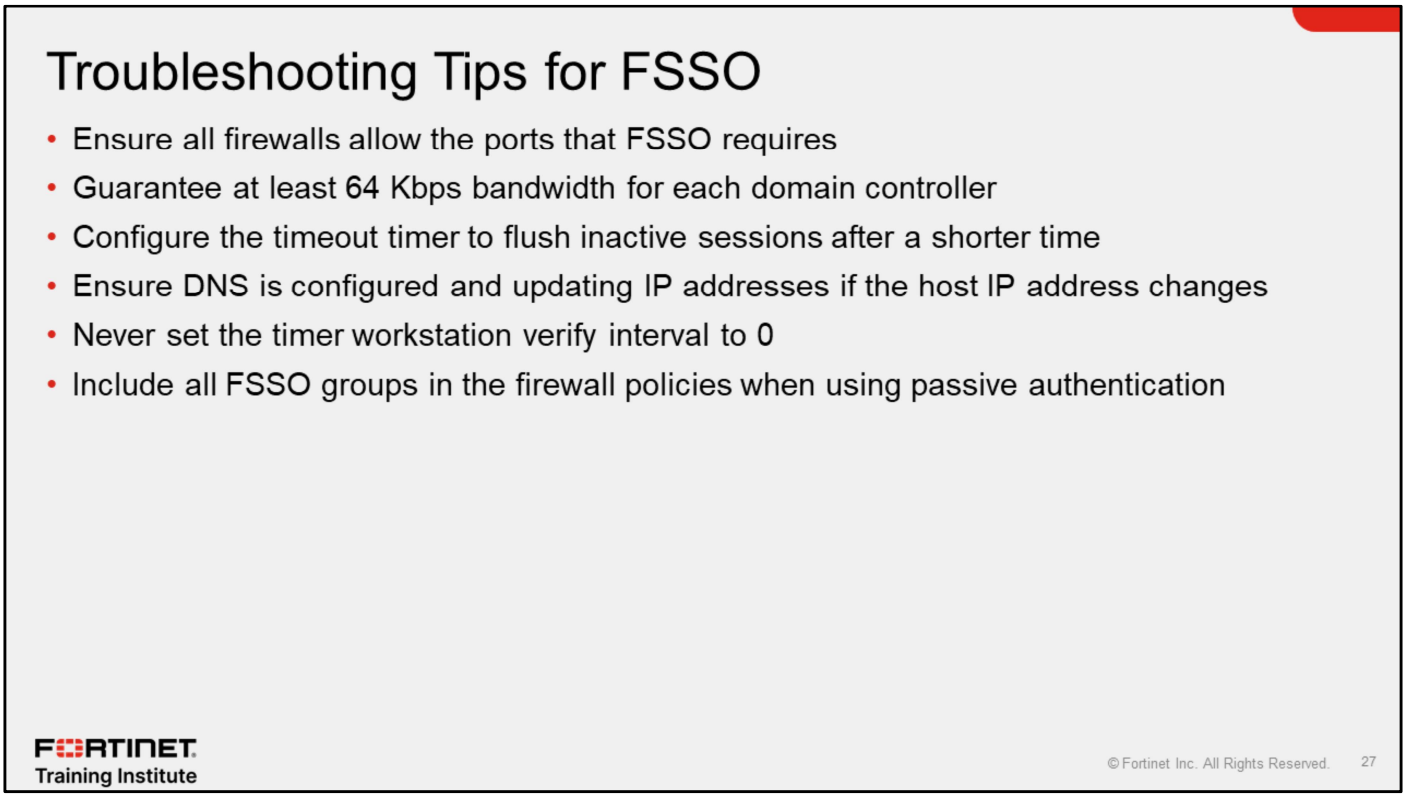
Depending on your network, you might need to configure advanced settings on your FSSO collector agent.

Citrix servers support FSSO. TS agent mode allows the server to monitor user logins in real time. The TS agent is like a DC agent, it also needs the collector agent to collect and send the login events to FortiGate. It then uses the same ports to report the logins back to the collector agent.

The collector agent on its own can get accurate login events from Citrix servers only if each user has their own IP address. If multiple users share the same IP address, the TS agent is required to report the user, the IP address, and the source port range assigned to that user to the collector agent. The TS agent cannot forward logs directly to FortiGate; the logs first have to be gathered by a collector. This does not work with polling from FortiGate.

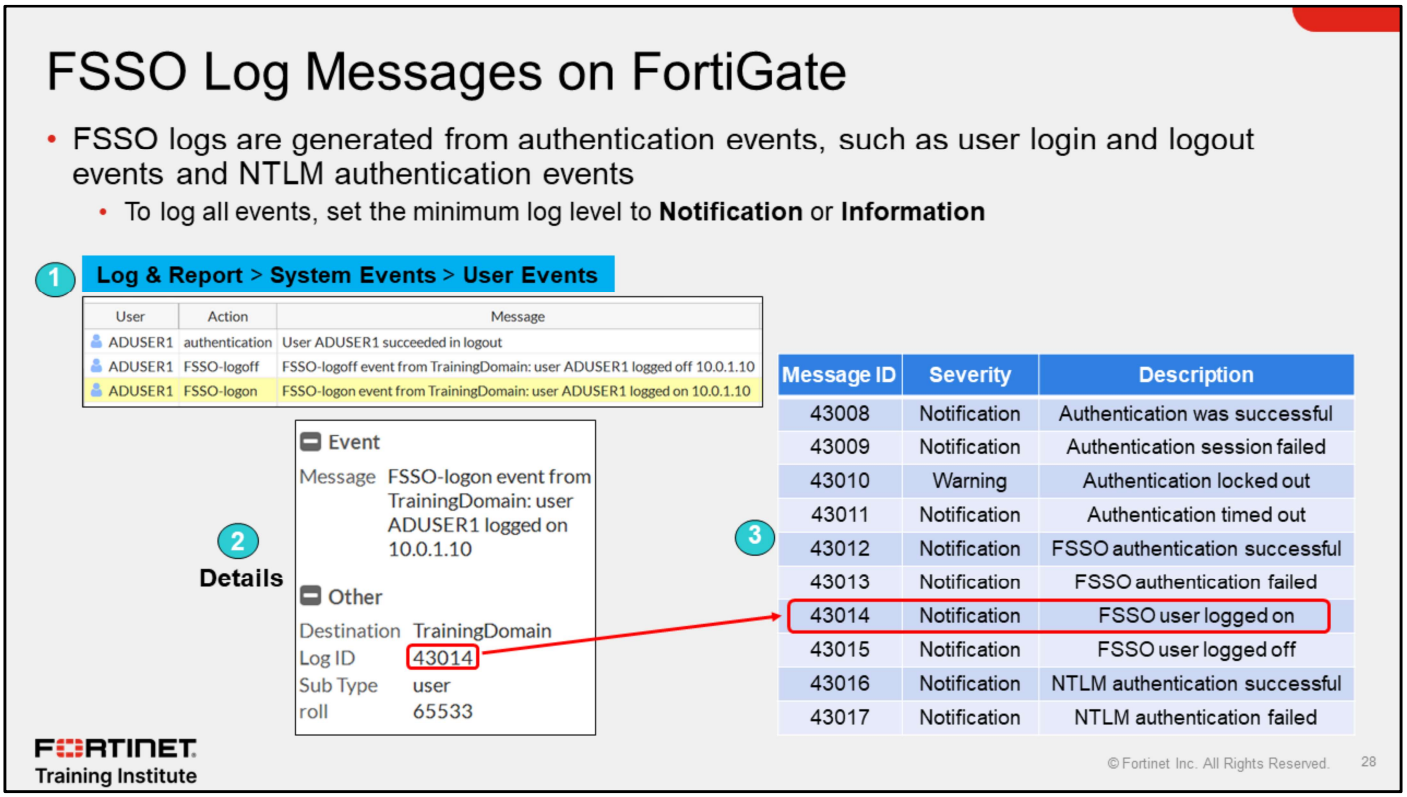
A RADIUS server configured as a RADIUS-based accounting system can interact in your network by sending accounting messages to the collector agent. The FSSO collector agent also supports integration with syslog servers, for the same purpose.

You can configure which event IDs are polled for Windows security event logs in the **Event IDs to poll** field.



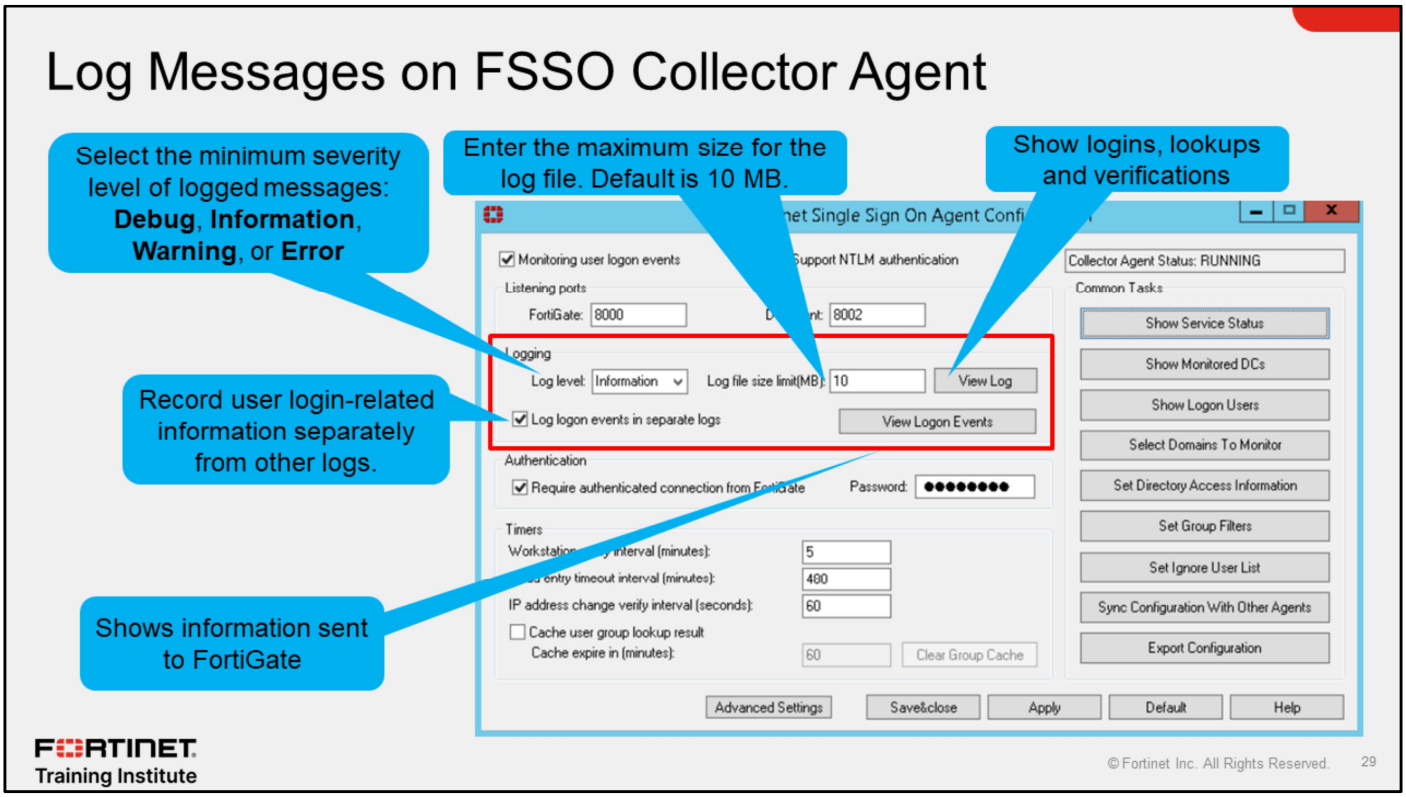
Begin with the following tips, which are useful in many FSSO troubleshooting situations:

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

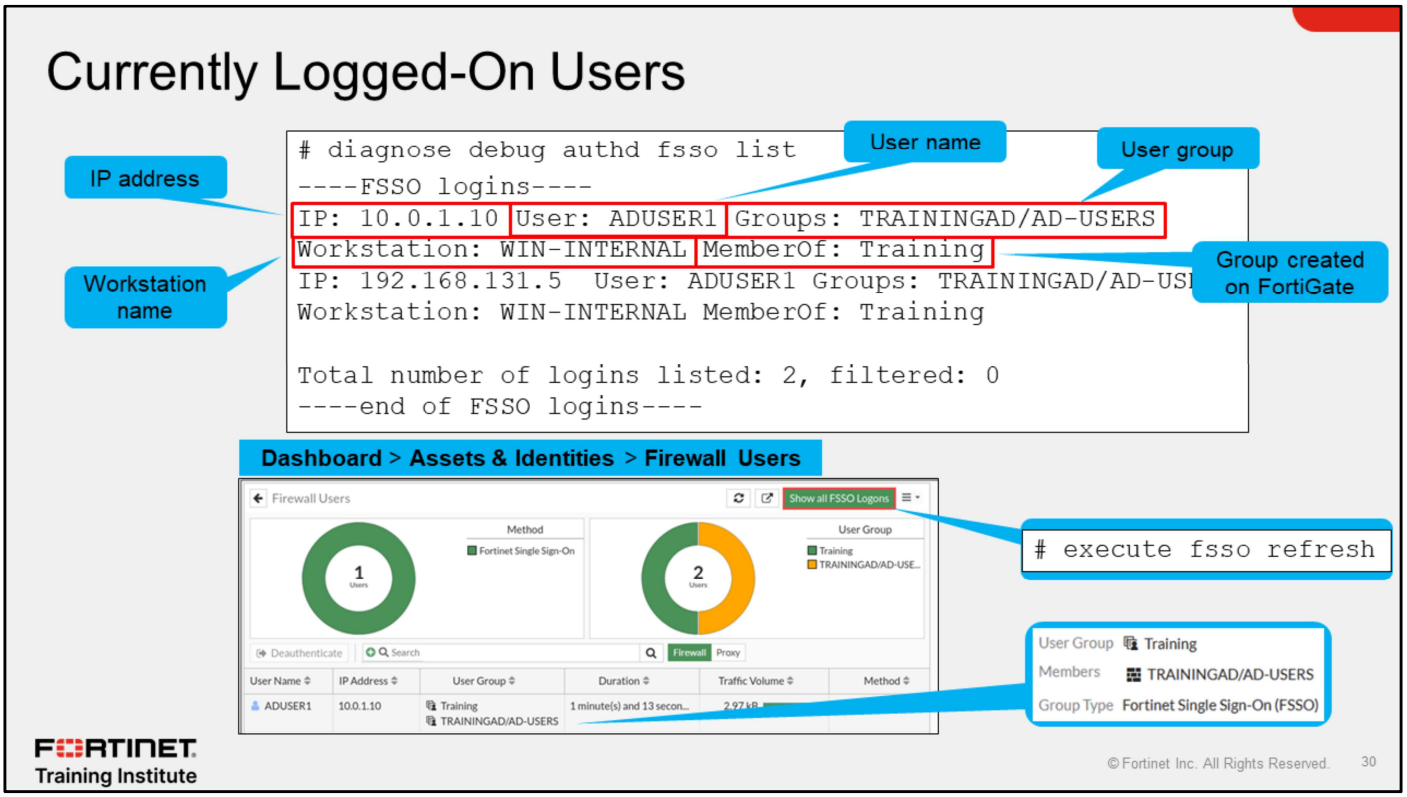
To ensure you log all the events needed, set the minimum log level to **Notification** or **Information**. Firewall logging requires **Notification** as a minimum log level. The closer the log level is to **Debug** level, the more information is logged.



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.



If applying the tips from the previous slide 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 user name, 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.

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

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
```

FORTINET Training Institute

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

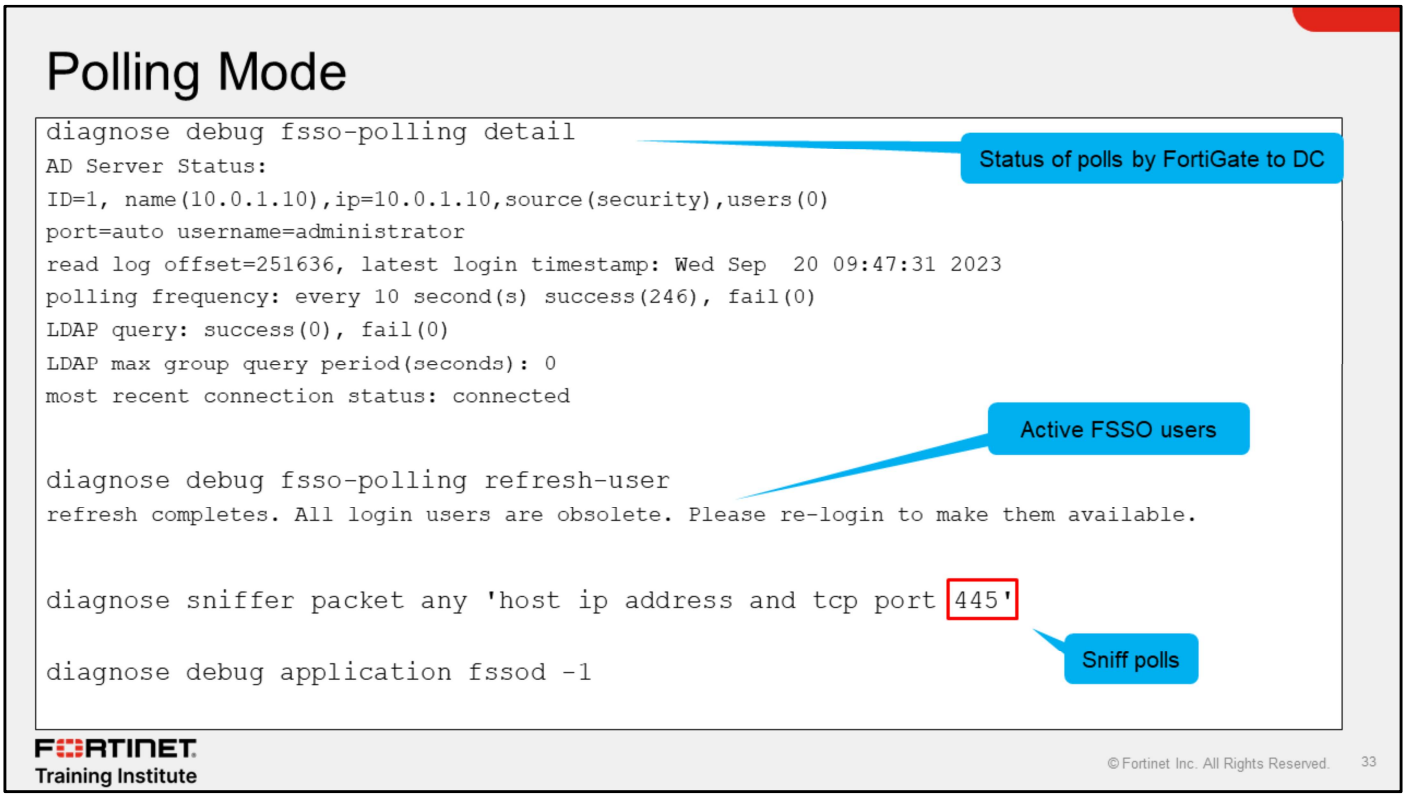
```
# diagnose debug authd fsso <…>

       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
```

FORTINET Training Institute

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.



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.

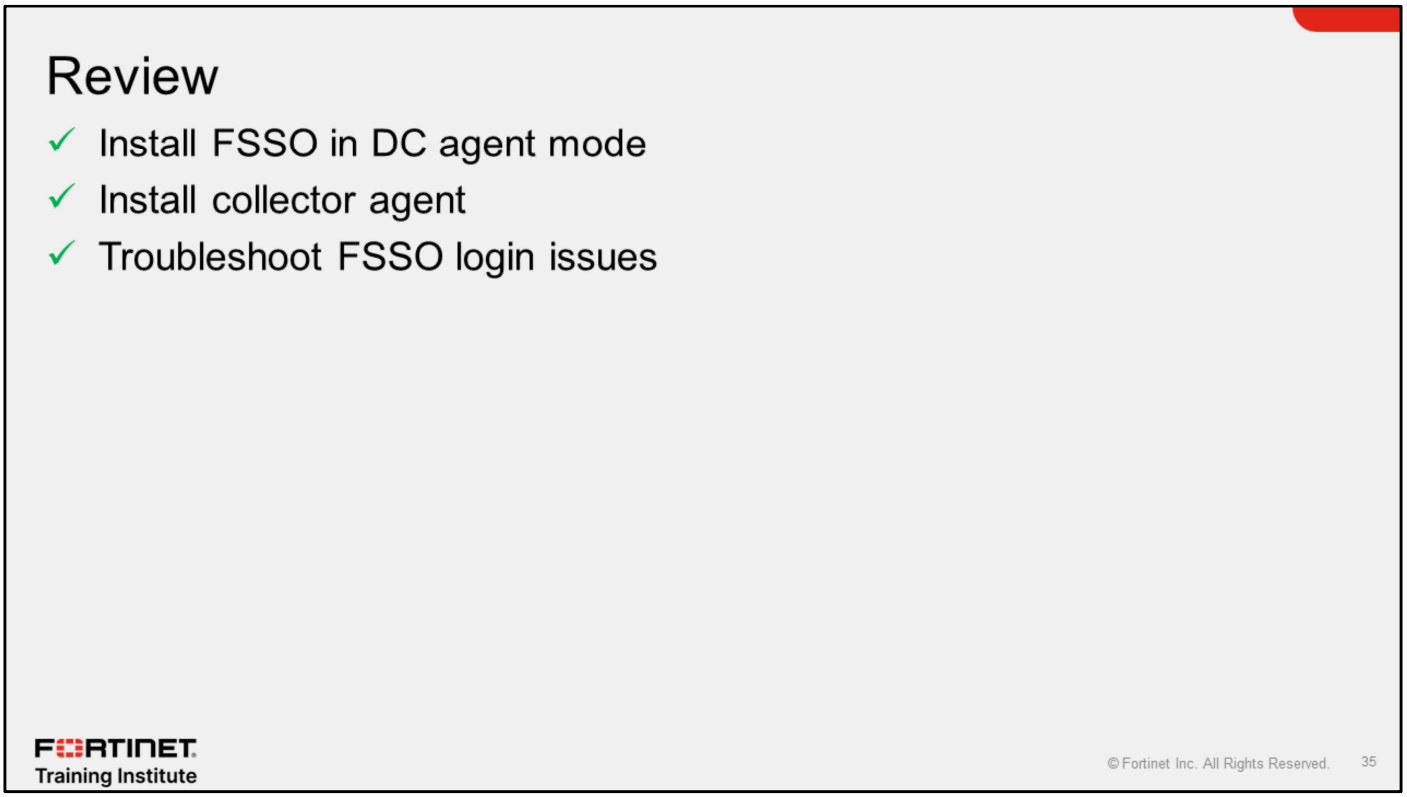
Knowledge Check

1. Which mode is recommended for FSSO deployments?
   - ✓ A. DC agent mode
   - B. Polling mode: Agentless

2. Which naming conventions does the FSSO collector agent use to access the Windows AD in standard access mode?
   - ✓ A. Windows convention—NetBios: `Domain\groups`
   - B. LDAP convention: `CN=User,OU=Name,DC=Domain`

3. Which FSSO mode requires more FortiGate system resources (CPU and RAM)?
   - A. Collector agent-based polling mode
   - ✓ B. Agentless polling mode

FORTINET Training Institute



This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned how to use FSSO so that your users don’t need to log in each time they access a different network resource.