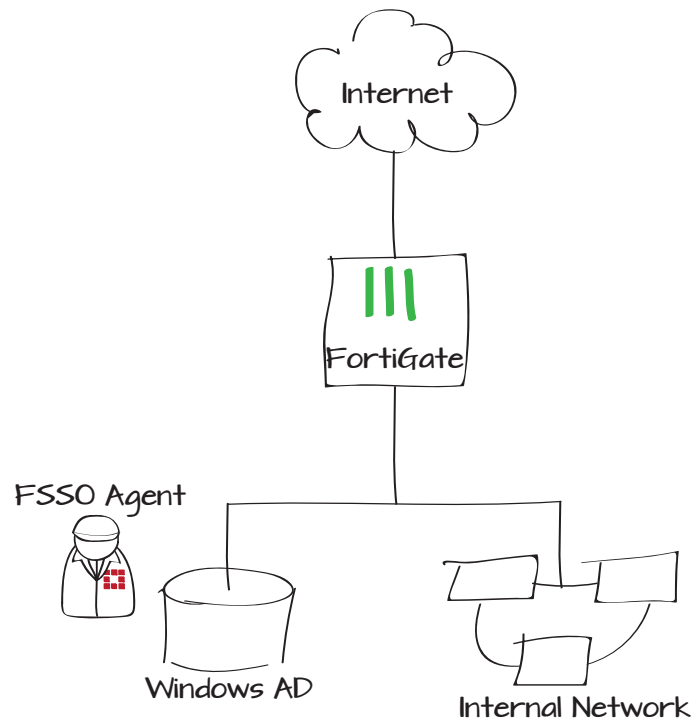


# Providing Single Sign-On for a Windows AD network with a FortiGate

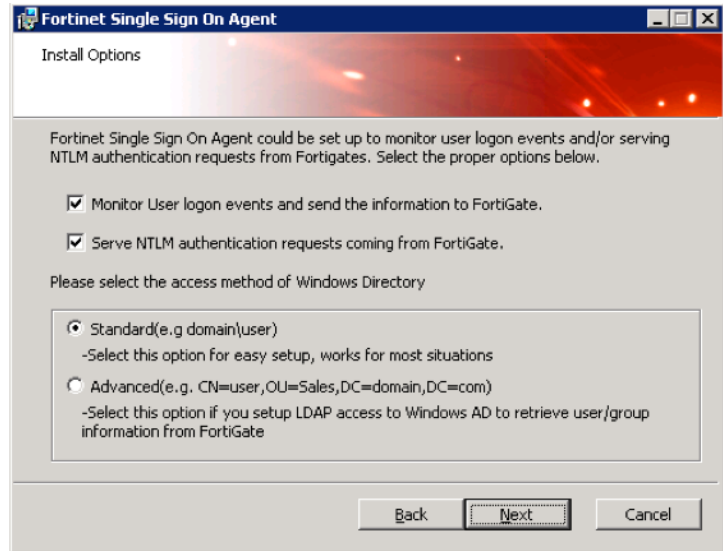
This example uses the Fortinet Single Sign-On (FSSO) Collector Agent to integrate a FortiGate unit into the Windows AD domain.

1. Installing the FSSO Collector Agent
2. Configuring the Single Sign-on Agent
3. Configuring the FortiGate unit to connect to the FSSO agent
4. Adding a FSSO user group
5. Adding a firewall address for the internal network
6. Adding a security profile that includes an authentication rule
7. Results

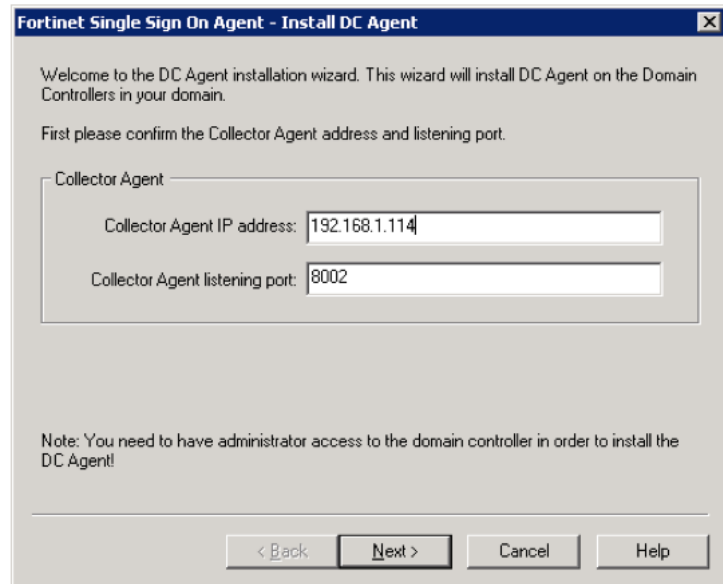


## Installing the FSSO Collector Agent

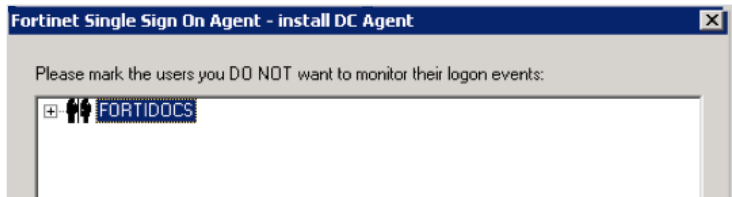
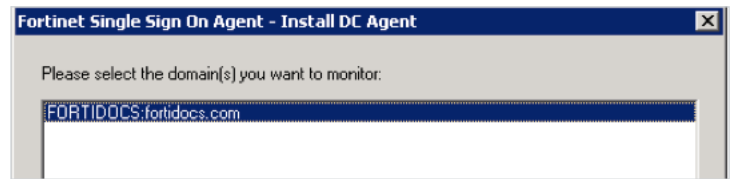
Run the setup for the Fortinet SSO Collector Agent. After logging in, configure the agent settings.



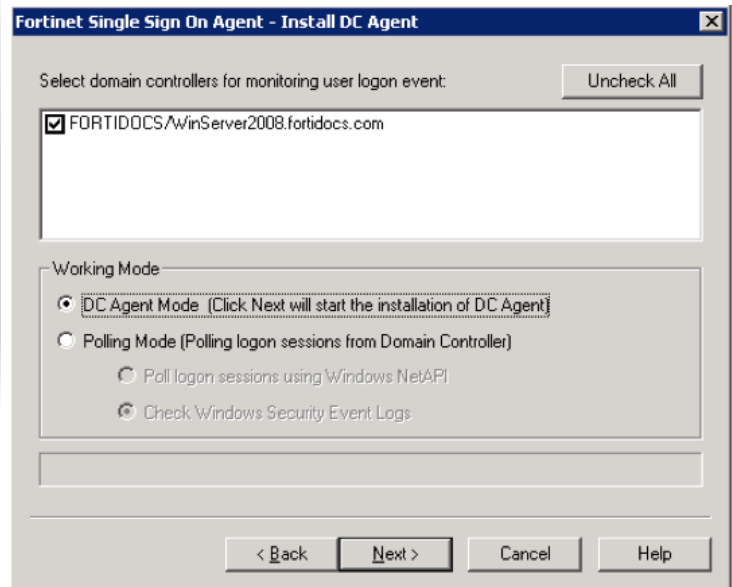
Add the Collector Agent address information.



Select the domains to monitor, and any users whose activity you do not wish to monitor.



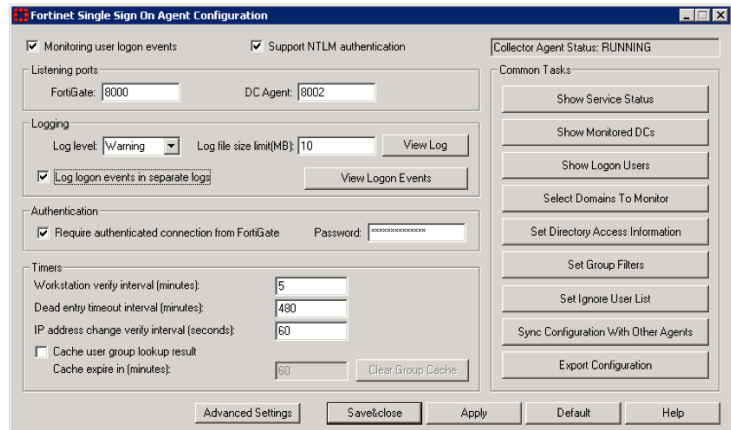
Set the working mode and complete the installation.



## Configuring the Single Sign-on Agent

If required, select Require authenticated connection from FortiGate, and add a password.

You will also enter this password when configuring the FSSO on the FortiGate unit.



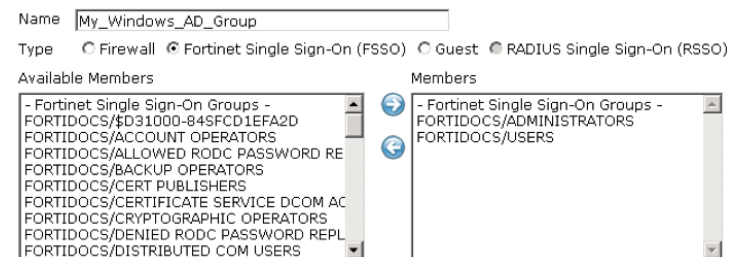
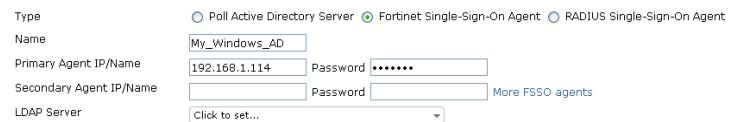
## Configuring the FortiGate unit to connect to the FSSO agent

On the FortiGate unit, go to **User & Device > Authentication > Single Sign-On**.

Enter this password used configuring the FSSO on the FortiGate unit in the previous step.

## Adding a FSSO user group

On the FortiGate unit, go to **User & Device > User > User Groups**.



## Adding a firewall address for the internal network

Go to **Firewall Objects > Address > Addresses**.

## Adding a security profile that includes an authentication rule

Go to **Policy > Policy > Policy**.

Add an accept user identity security policy and add the new FSSO group.

Category  Address  IPv6 Address  Multicast Address

Name

Color

Type

Subnet / IP Range

Interface

Show in Address List

Comments  0/255

Policy Type  Firewall  VPN

Policy Subtype  Address  User Identity  Device Identity

Incoming Interface

Source Address

Outgoing Interface

Enable NAT

Use Destination Interface Address  Fixed Port

Use Dynamic IP Pool

Use Central NAT Table

Enable Web cache

Enable WAN Optimization

### Configure Authentication Rules

User/Group	Destination Address	Service	Schedule	UTM Security	Traffic Shaping
My_Windows_AD_Group	all	ALL	always	-	<input checked="" type="button" value="x"/>
ANY	all	ALL	always	-	<input checked="" type="button" value="x"/>

- Skip this policy for unauthenticated user
- Disclaimer
- Customize Authentication Messages

# Results

Go to **Log & Report > Traffic Log > Forward Traffic**. As users log into the Windows AD system, the FortiGate collects their connection information.

Select an entry for more information.

Date/Time	Src	Device	Dst
15:49	ADMINISTRATOR (192.168.1.114)	00:0c:29:4b:d7:cc	204.246.169.91 (cont...
15:45	ADMINISTRATOR (192.168.1.114)	00:0c:29:4b:d7:cc	74.121.50.17 (www.p...
15:07	TWHITE (192.168.1.116)	Lab test system 2	207.46.206.78 (mscr...
15:07	TWHITE (192.168.1.116)	Lab test system 2	207.46.206.78 (mscr...
15:04	TWHITE (192.168.1.116)	Lab test system 2	63.251.85.33 (m.webt...
15:04	TWHITE (192.168.1.116)	Lab test system 2	63.251.85.33 (m.webt...
15:04	TWHITE (192.168.1.116)	Lab test system 2	63.251.85.33 (m.webt...

<b>Dst</b>	204.246.169.91 (content.mkt931.com)	<b>Virtual Domain</b>	root
<b>Received</b>	92	<b>Source Country</b>	Reserved
<b>Src NAT IP</b>	172.20.120.123	<b>Sent / Received</b>	292 B / 92 B
<b>Device Type</b>	Windows PC	<b>Duration</b>	10
<b>Sent</b>	292	<b>Src NAT Port</b>	9803
<b>Application Details</b>		<b>Group</b>	My_Windows_AD_Group
<b>Device</b>	00:0c:29:4b:d7:cc	<b>Service</b>	HTTP
<b>Protocol</b>	6	<b>byod_name</b>	
<b>User</b>	ADMINISTRATOR	<b>Destination Country</b>	United States
<b>Identity Index</b>	1	<b>Dst Port</b>	80
<b>roll</b>	65372	<b>Status</b>	close
<b>Timestamp</b>	Tue May 7 15:59:49 2013	<b>Tran Display</b>	snat
<b>OS Name</b>	Windows	<b>Sequence Number</b>	1607872
<b>Policy ID</b>	9	<b>Src Interface</b>	port1
<b>Src</b>	ADMINISTRATOR (192.168.1.114)	<b>Sent Packets</b>	7
<b>OS Version</b>	Vista	<b>Level</b>	notice
<b>Src Port</b>	9803	<b>Log ID</b>	13
<b>Sub Type</b>	forward	<b>Threat</b>	
<b>Received Packets</b>	2	<b>Date/Time</b>	15:59:49 (Tue May 7 15:59:49 2013)
<b>Dst Interface</b>	wan1		
<b>Dst</b>	207.46.206.78 (mscr.microsoft.com)	<b>Virtual Domain</b>	root
<b>Received</b>	3202	<b>Source Country</b>	Reserved
<b>Src NAT IP</b>	172.20.120.123	<b>Sent / Received</b>	609 B / 3.13 KB
<b>Device Type</b>	Windows PC	<b>Duration</b>	5
<b>Sent</b>	609	<b>Src NAT Port</b>	50608
<b>Application Details</b>		<b>Group</b>	My_Windows_AD_Group
<b>Device</b>	Lab test system 2	<b>Service</b>	HTTP
<b>Protocol</b>	6	<b>byod_name</b>	Lab test system 2
<b>User</b>	TWHITE	<b>Destination Country</b>	United States
<b>Identity Index</b>	1	<b>Dst Port</b>	80
<b>roll</b>	65372	<b>Status</b>	close
<b>Timestamp</b>	Tue May 7 15:59:07 2013	<b>Tran Display</b>	snat
<b>OS Name</b>	Windows	<b>Sequence Number</b>	1607691
<b>Policy ID</b>	9	<b>Src Interface</b>	port1
<b>Src</b>	TWHITE (192.168.1.116)	<b>Sent Packets</b>	7
<b>OS Version</b>	7	<b>Level</b>	notice
<b>Src Port</b>	50608	<b>Log ID</b>	13
<b>Sub Type</b>	forward	<b>Threat</b>	
<b>Received Packets</b>	7	<b>Date/Time</b>	15:59:07 (Tue May 7 15:59:07 2013)
<b>Dst Interface</b>	wan1		