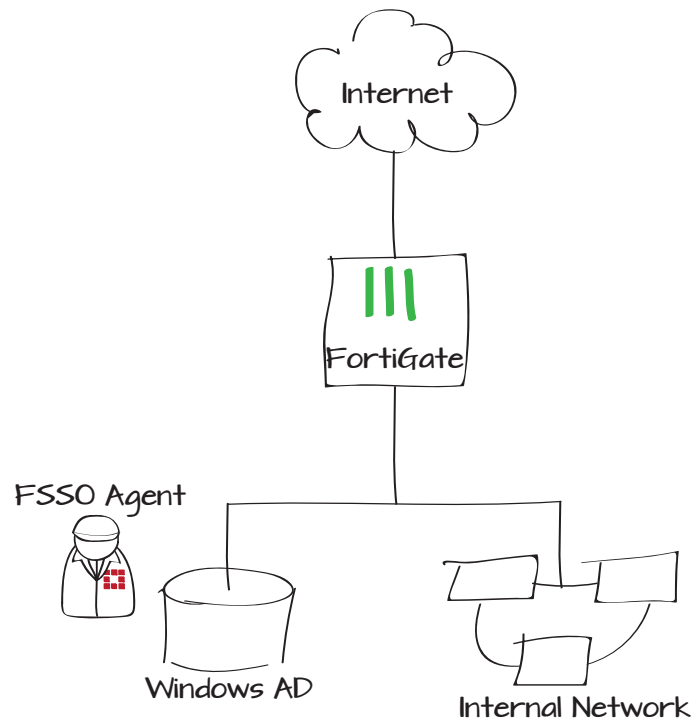


Providing Single Sign-On for a Windows AD network with a FortiGate

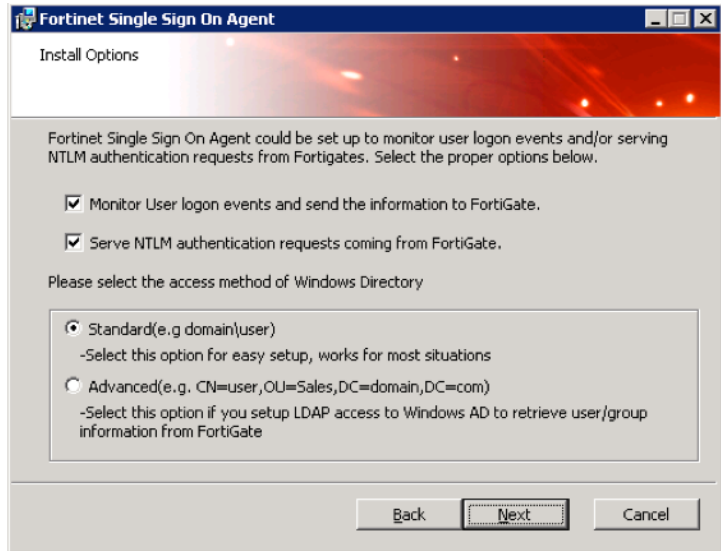
This example uses the Fortinet Single Sign-On (FSSO) Collector Agent to integrate a FortiGate unit into the Windows AD domain.

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

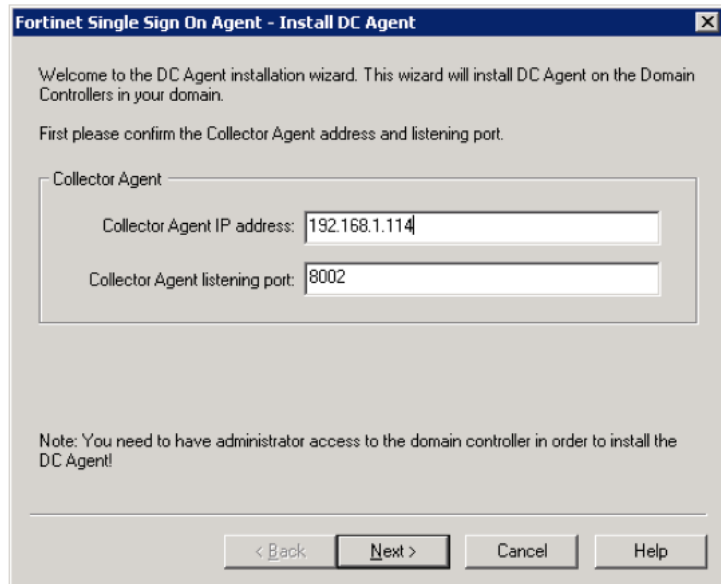


Installing the FSSO Collector Agent

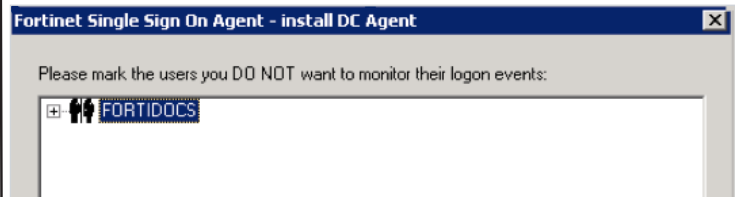
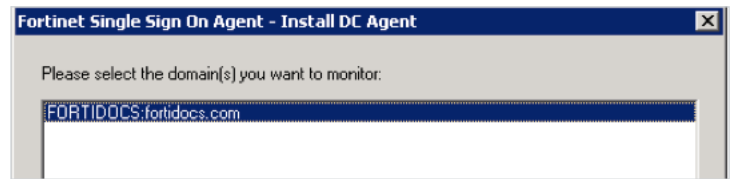
Run the setup for the Fortinet SSO Collector Agent. After logging in, configure the agent settings.



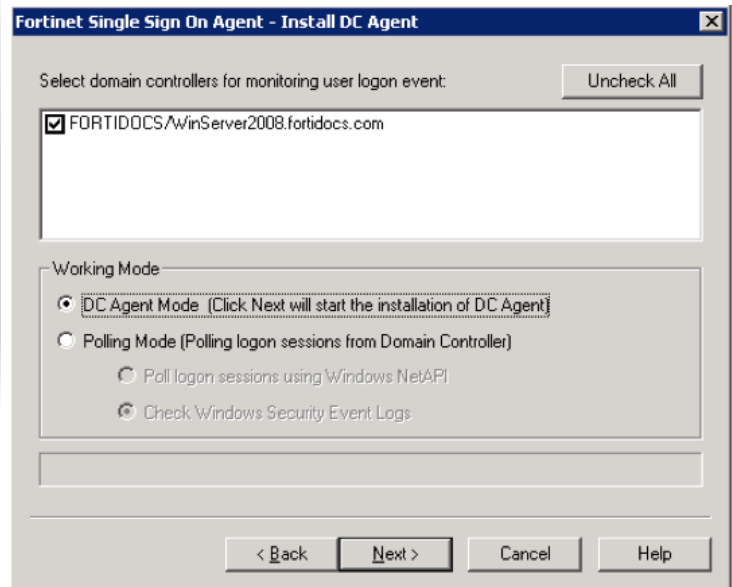
Add the Collector Agent address information.



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



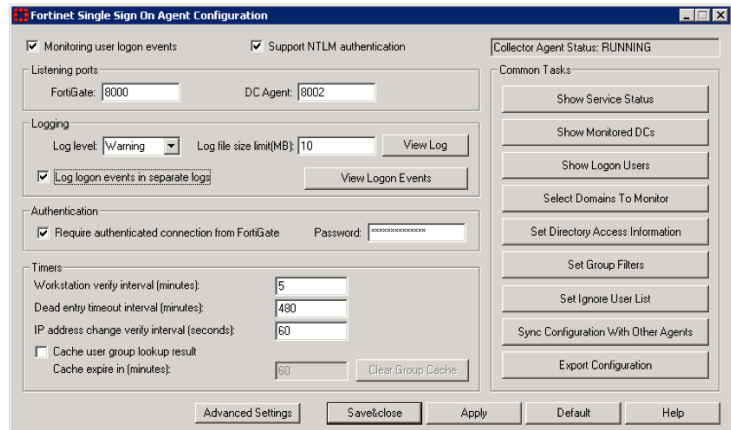
Set the working mode and complete the installation.



Configuring the Single Sign-on Agent

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

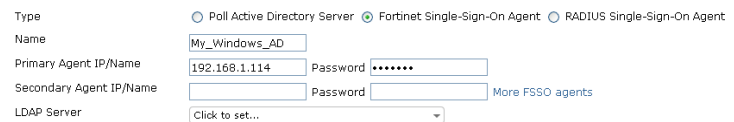
You will also enter this password when configuring the FSSO on the FortiGate unit.



Configuring the FortiGate unit to connect to the FSSO agent

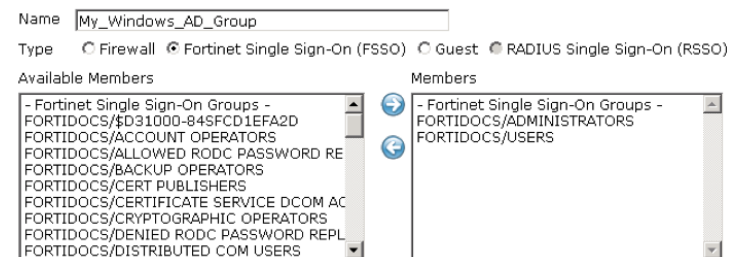
On the FortiGate unit, go to **User & Device > Authentication > Single Sign-On**.

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...

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

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