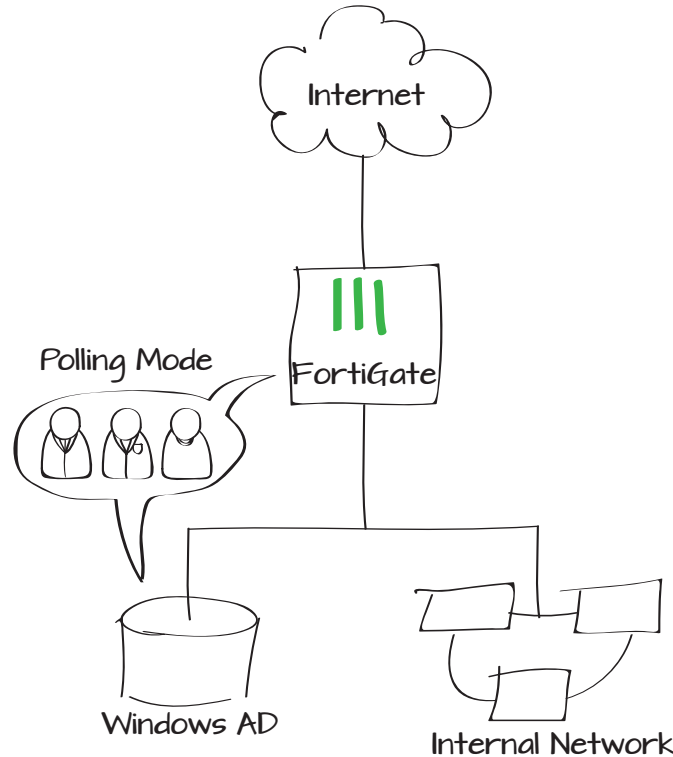


# Fortinet Single Sign-On in Polling Mode for a Windows AD network

This example uses Active Directory Polling to establish Fortinet Single Sign-On (FSSO) for a Windows AD Domain Controller, without requiring a FortiAuthenticator or a Collector Agent running on the Windows AD Domain to act as an intermediary between the FortiGate and the domain.

1. Adding the LDAP Server to the FortiGate
2. Configuring the FortiGate unit to poll the Active Directory
3. Adding an FSSO user group
4. Adding a firewall address for the internal network
5. Adding a security policy that includes an authentication rule
6. Results



## Adding the LDAP Server to the FortiGate

In the FortiGate web interface, go to **User & Device > Authentication > LDAP Servers**. Add your LDAP server details.

## Configuring the FortiGate unit to poll the Active Directory

Next, go to **User & Device > Authentication > Single Sign-On**.

For the **Type**, select **Poll Active Directory Server**. Enter the IP, username and password, and select the LDAP server you added previously. Ensure **Enable Polling** is checked.

## Adding an FSSO user group

Go to **User & Device > User > User Groups**, and add the desired AD member groups to the group.

Name	<input type="text" value="FAC_LDAP"/>
Server IP/Name	<input type="text" value="192.168.1.117"/>
Server Port	<input type="text" value="389"/>
Common Name Identifier	<input type="text" value="uid"/>
Distinguished Name	<input type="text" value="dc=fortidocs,dc=com"/>
Bind Type	<input type="radio"/> Simple <input type="radio"/> Anonymous <input checked="" type="radio"/> Regular
User DN	<input type="text" value="ou=techdoc,dc=fortidocs,dc=com"/>
Password	<input type="password" value="*****"/>

Type	<input checked="" type="radio"/> Poll Active Directory Server <input type="radio"/> Fortinet Single-Sign-On Agent <input type="radio"/>
Server IP/Name	<input type="text" value="192.168.1.117"/>
User	<input type="text" value="Example_Admin"/>
Password	<input type="password" value="*****"/>
LDAP Server	<input type="text" value="FAC_LDAP"/>
Enable Polling	<input checked="" type="checkbox"/>
Users/Groups	<div><input type="button" value="View Users/Groups"/> <input type="button" value="Edit Users/Groups"/></div> <div><input checked="" type="checkbox"/> DC=fortidocs,DC=com</div>

Name	<input type="text" value="My_Windows_AD_Group"/>
Type	<input type="radio"/> Firewall <input checked="" type="radio"/> Fortinet Single Sign-On (FSSO) <input type="radio"/> Guest <input checked="" type="radio"/> RADIUS Single Sign-On (RSSO)
Available Members	<div><input checked="" type="checkbox"/> - Fortinet Single Sign-On Groups - FORTIDOCs/31000-845FCD1EFA2D FORTIDOCs/ACCOUNT OPERATORS FORTIDOCs/ALLOWED RODC PASSWORD RE FORTIDOCs/BACKUP OPERATORS FORTIDOCs/CERT PUBLISHERS FORTIDOCs/CERTIFICATE SERVICE DCOM AC FORTIDOCs/CRYPTOGRAPHIC OPERATORS FORTIDOCs/DENIED RODC PASSWORD REPL FORTIDOCs/DISTRIBUTED COM USERS</div>
Members	<div><input checked="" type="checkbox"/> - Fortinet Single Sign-On Groups - FORTIDOCs/ADMINISTRATORS FORTIDOCs/USERS</div>

## Adding a firewall address for the internal network

Go to **Firewall Objects > Address > Addresses**, and create an internal network address to be used by the policy.

## Adding a security policy that includes an authentication rule

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

Create a **User Identity** policy and add an authentication rule to allow your FSSO group to access the internet.

Category  Address  IPv6 Address  Multicast Address

Name

Color [Change]

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

Create New Edit Delete

User/Group	Destination Address	Service	Schedule	UTM Security	Traffic Shaping
My_Windows_AD_Group	all	ALL	always	-	
ANY	all	ALL	always	-	

Skip this policy for unauthenticated user

Disclaimer

Customize Authentication Messages

## Results

Go to **Log & Report > Traffic Log > Forward Traffic**. When users log into the Windows AD network, the FortiGate will automatically poll the domain for their account information, and record their traffic.

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 (content.mkt931.com)
15:45	ADMINISTRATOR (192.168.1.114)	00:0c:29:4b:d7:cc	74.121.50.17 (www.msft.com)
15:07	TWHITE (192.168.1.116)	Lab test system 2	207.46.206.78 (mscr.microsoft.com)
15:07	TWHITE (192.168.1.116)	Lab test system 2	207.46.206.78 (mscr.microsoft.com)
15:04	TWHITE (192.168.1.116)	Lab test system 2	63.251.85.33 (m.webt.com)
15:04	TWHITE (192.168.1.116)	Lab test system 2	63.251.85.33 (m.webt.com)
15:04	TWHITE (192.168.1.116)	Lab test system 2	63.251.85.33 (m.webt.com)

<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		

