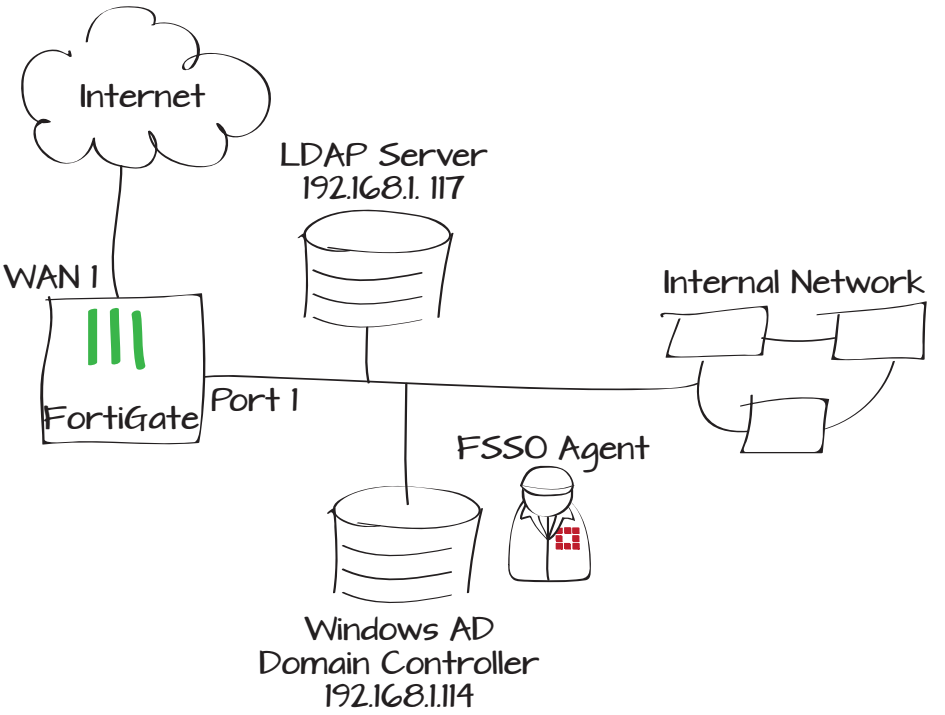
Providing Single Sign-On for Windows AD with LDAP

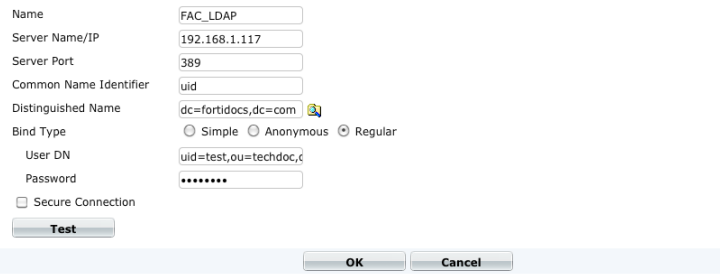
A logged-on Windows user can be automatically authenticated on a FortiGate unit through Fortinet Single Sign-On. Some Windows AD systems use an external LDAP server. FSSO can also accommodate this configuration.

1. Configuring access to the LDAP server
2. Configuring the DC agent as an FSSO agent
3. Configuring a group filter on the FSSO agent
4. Creating an FSSO user group and adding AD user groups
5. Creating a security policy to allow the FSSO user group access
6. Results



Configuring access to the LDAP server

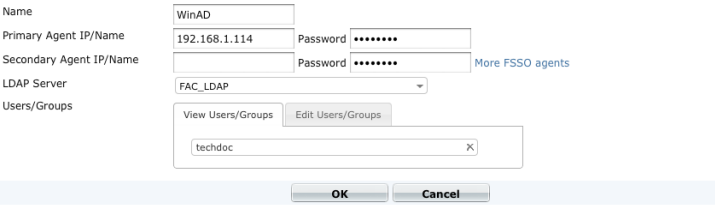
Go to **User & Device > Authentication > LDAP Servers** and enter the information needed to connect the FortiGate unit to the external LDAP server.



Configuring the DC agent as an FSSO agent

Go to **User & Device > Authentication > Single Sign-On** to enter the information the FortiGate unit needs to access the DC agent.

Select the LDAP Server. In Users/Groups use the Edit Users/Groups tab to select user groups from the LDAP tree.

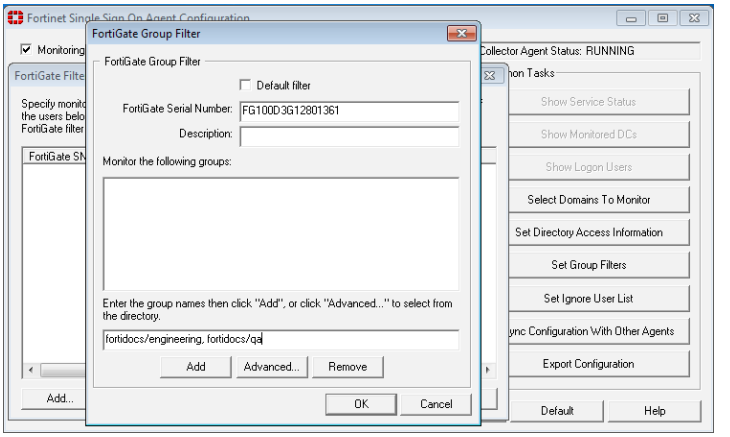


Configuring a group filter on the FSSO agent

Log on to the Windows server where the DC agent is installed. Go to **All Programs > FortiNet > Fortinet Single Sign On Agent > Configure Fortinet Single Sign On Agent**.

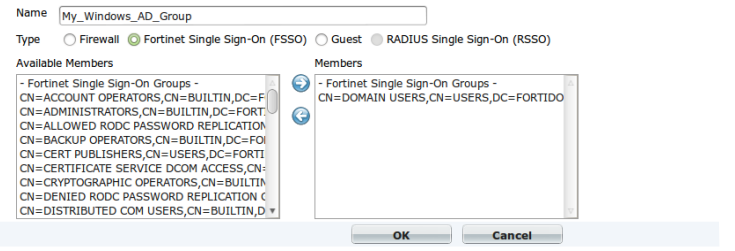
Select **Set Group Filters**. Select **Add**. Enter the FortiGate unit serial number and specify which user groups the DC agent should monitor for the FortiGate unit. Select **Add** again.

To avoid adversely affecting the FortiGate unit's performance, configure the filter to send information only for the groups you intend to authenticate.



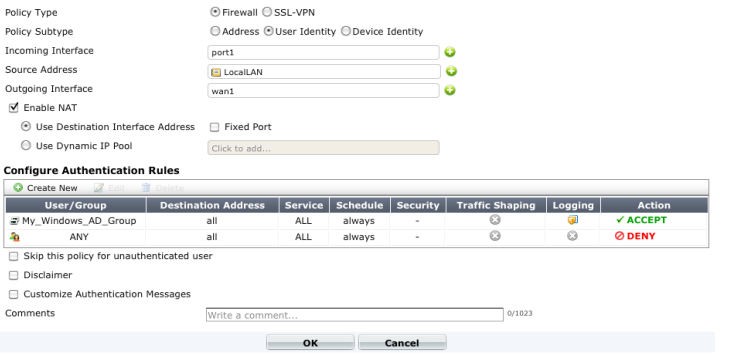
Creating an FSSO user group and adding AD user groups

.Go to **User & Device > User > User Groups**. Create a Fortinet Single Sign-On group and select which Windows AD groups to include as members.



Creating a security policy to allow the FSSO user group access

Create identity-based security policies that use the FSSO user group that you created.



Results

The Windows AD user, having authenticated at logon, does not have to authenticate again to connect to the Internet.