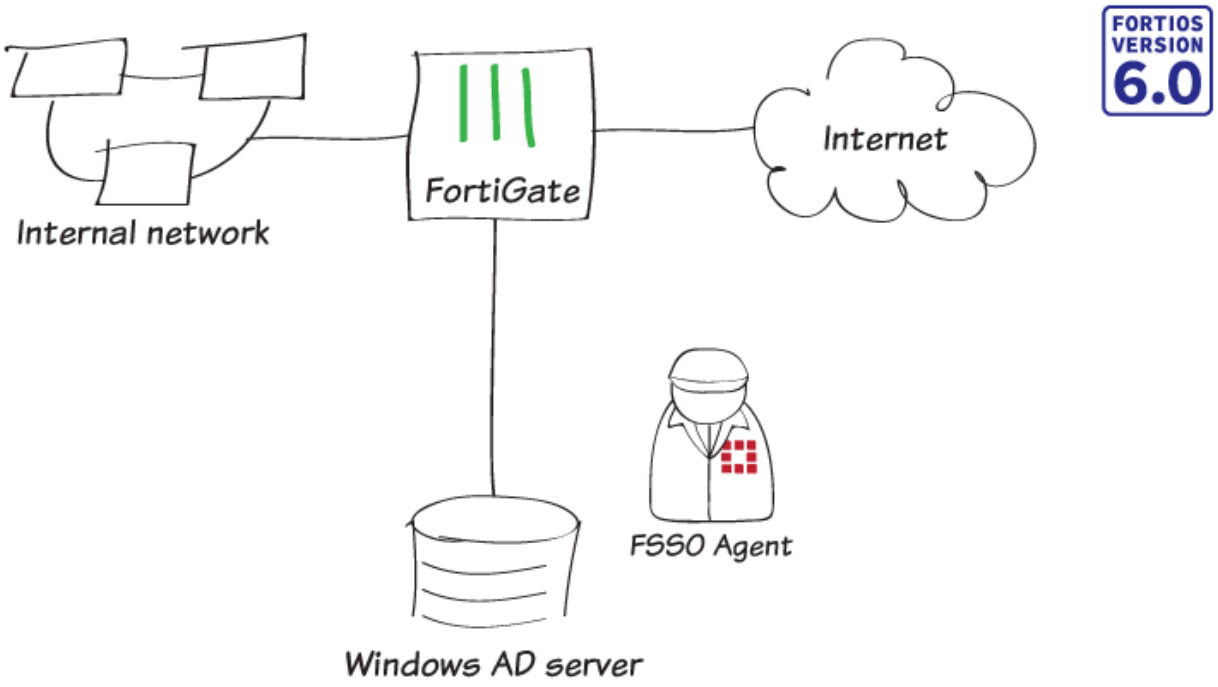
Authentication

This section contains information about authenticating users and devices.

Agent-based FSSO for Windows AD



In this recipe, you use agent-based Fortinet single sign-on (FSSO) to allow users to login to the network once with their Windows AD credentials and seamlessly access all appropriate network resources.

This example uses the FSSO agent in advanced mode. The main difference between advanced and standard mode is the naming convention used when referring to username information. Standard mode uses Windows convention: Domain\Username. Advanced mode uses LDAP convention: CN=User, OU=Name, DC=Domain.

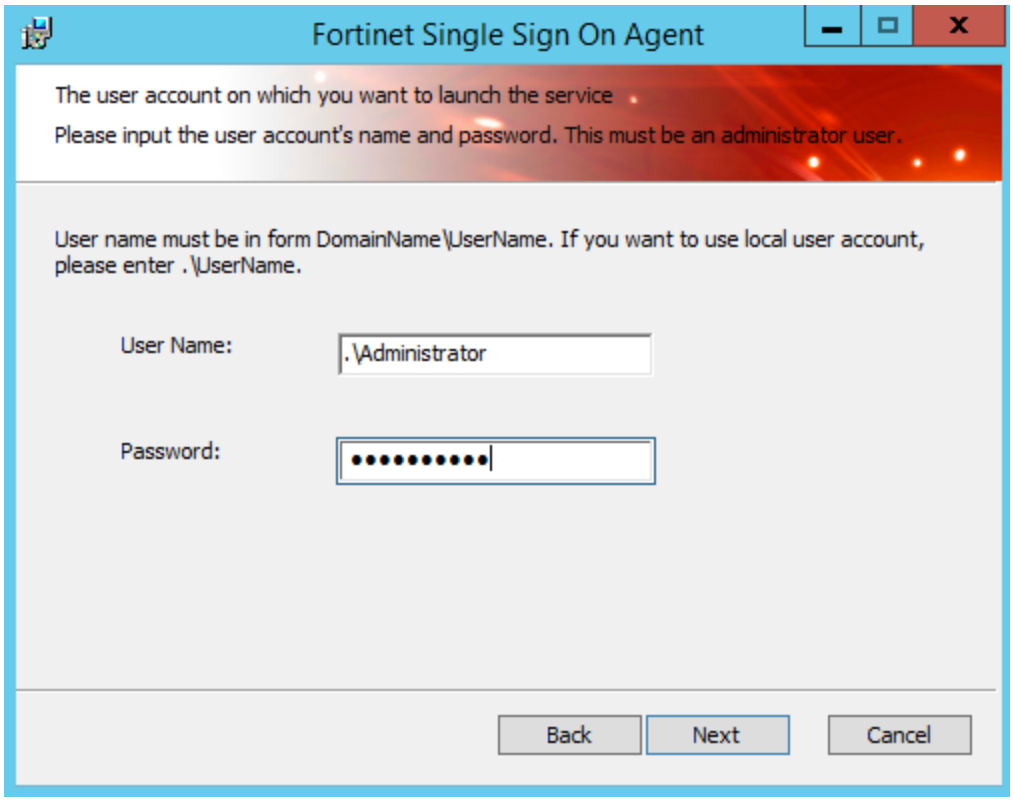
Standard mode supports device names up to 15 characters long. Advanced mode supports device names longer than 15 characters.

Advanced mode is required for multi-domains environments.

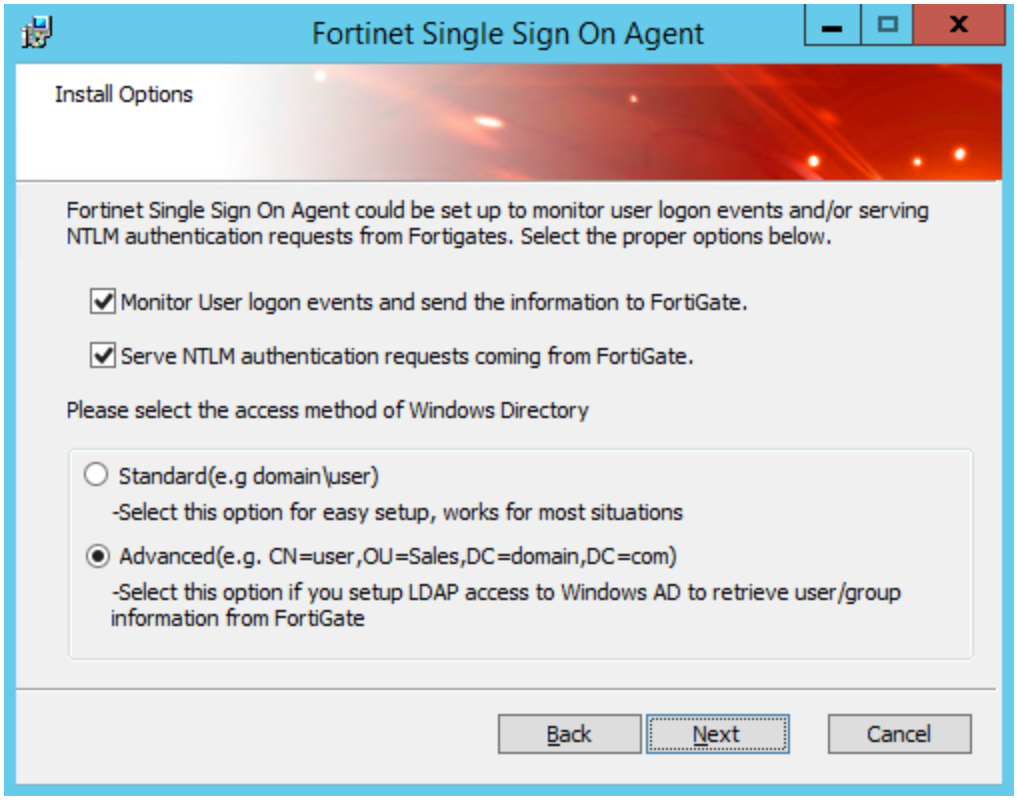
Installing the FSSO agent

Connect to the Windows AD server and download the FSSO agent from Fortinet Support.

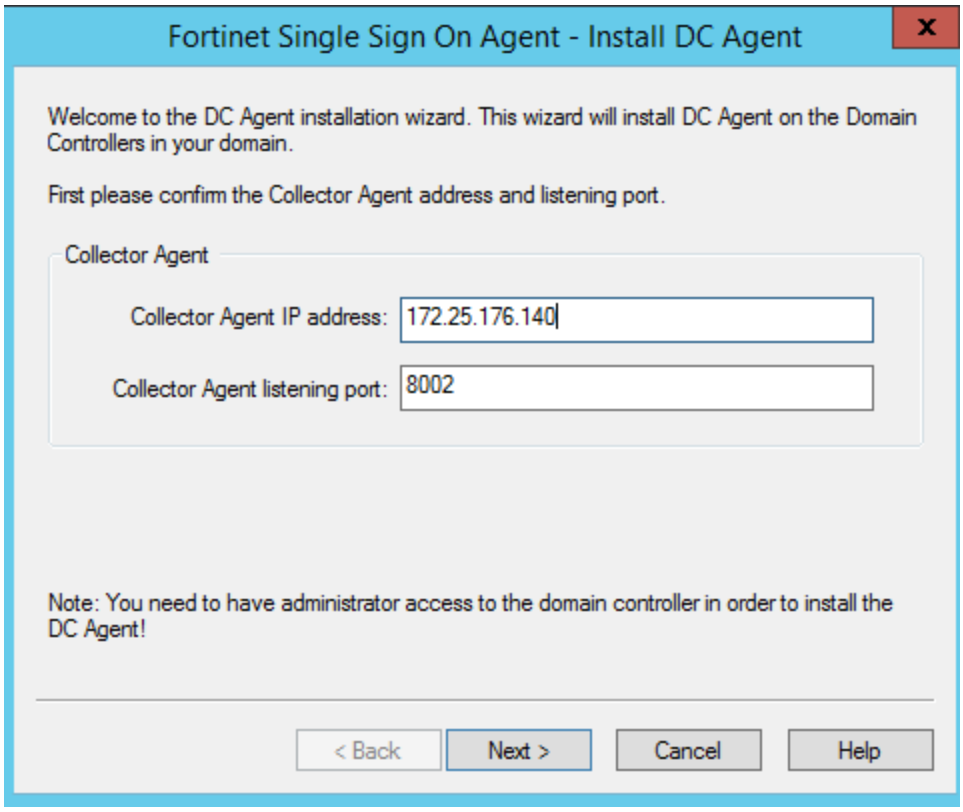
1. To install the agent, open the installer file and use the installation wizard.
2. Set a **User Name** and **Password** for the FSSO domain administrator.



3. For the **Install Options**, select **Advanced** to use advanced mode instead of standard.

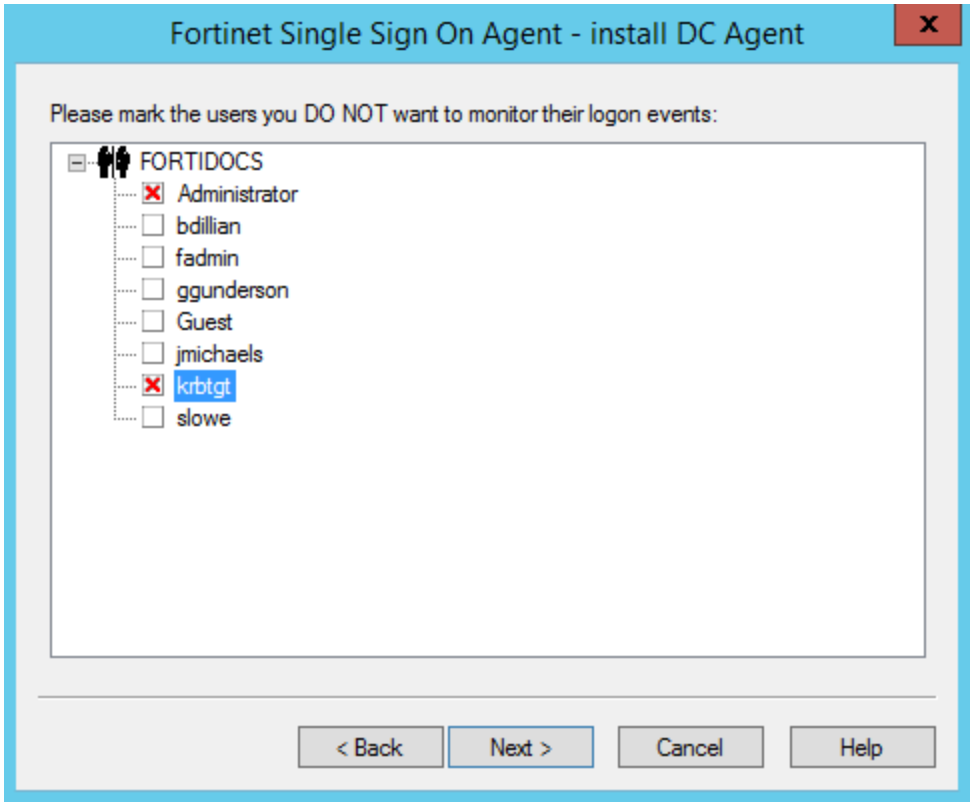


4. After installing the FSSO agent, run **Install DC Agent**.
5. Set the **Collector Agent IP address** and the **Collector Agent listening port**.

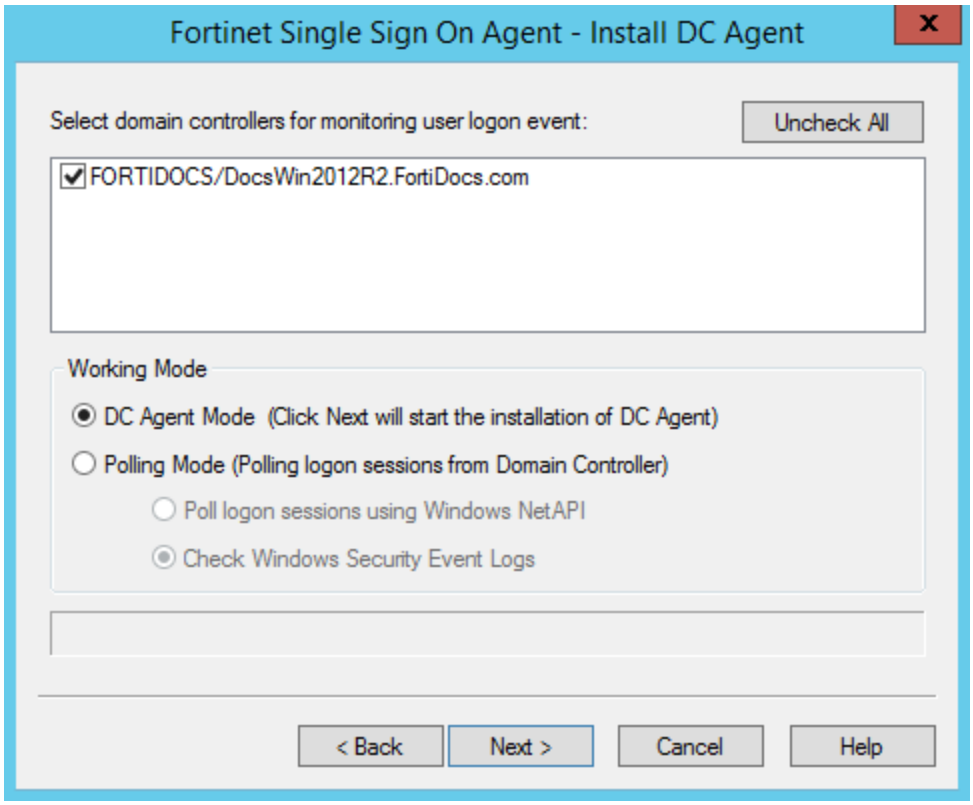


6. Select the domain you wish to monitor.

7. Exclude any users that you don't want to monitor, including the administrator.



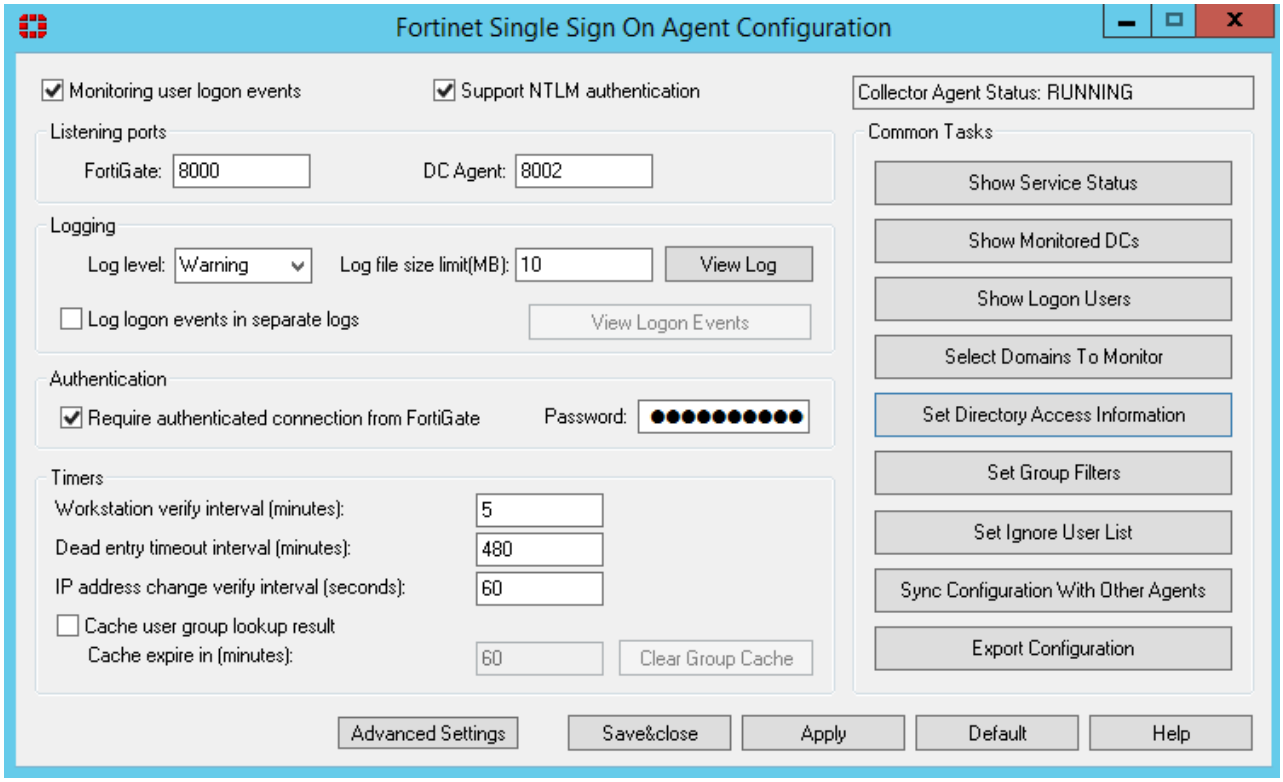
8. Set **Working Mode** to **DC Agent Mode**



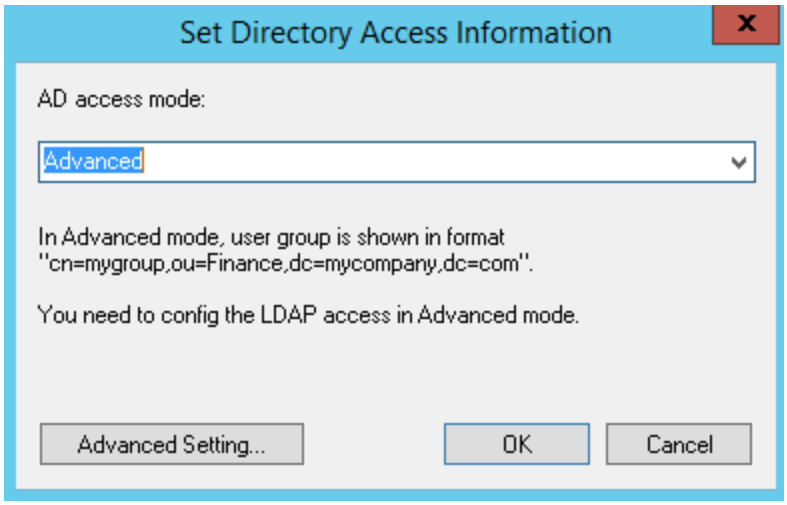
9. Restart your server to apply all changes.

Configuring the FSSO agent

1. To configure the settings for your network, open the FSSO agent. You can use the default for most settings.



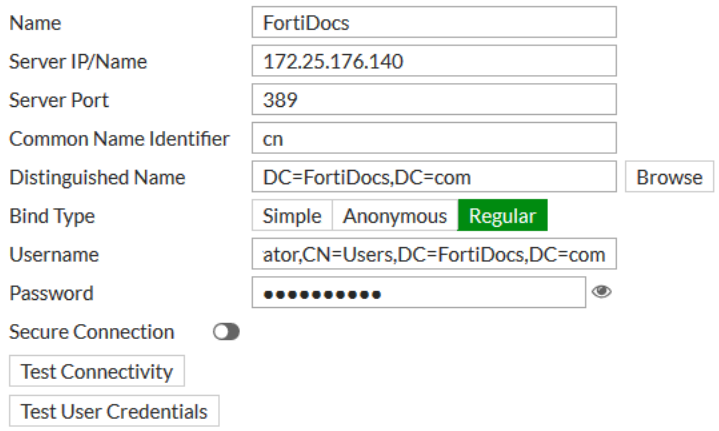
2. Select **Set Directory Access Information**. Set **AD access mode** to **Advanced**.



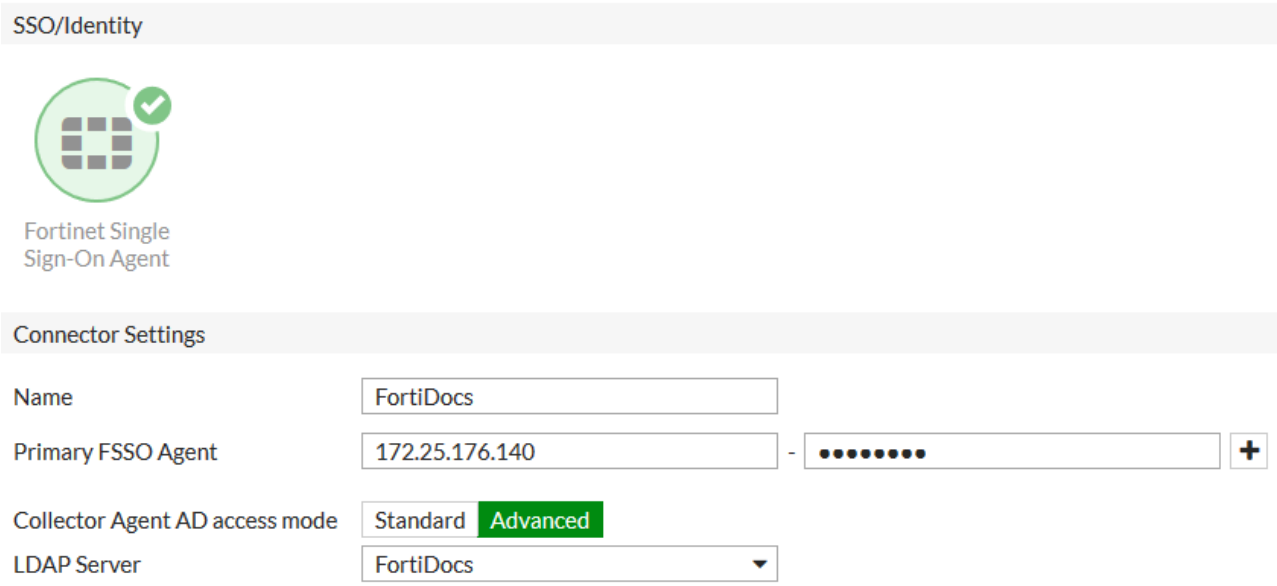
Setting up your FortiGate for FSSO

Because you have installed FSSSO in advanced mode, you need to configure LDAP to use with FSSO.

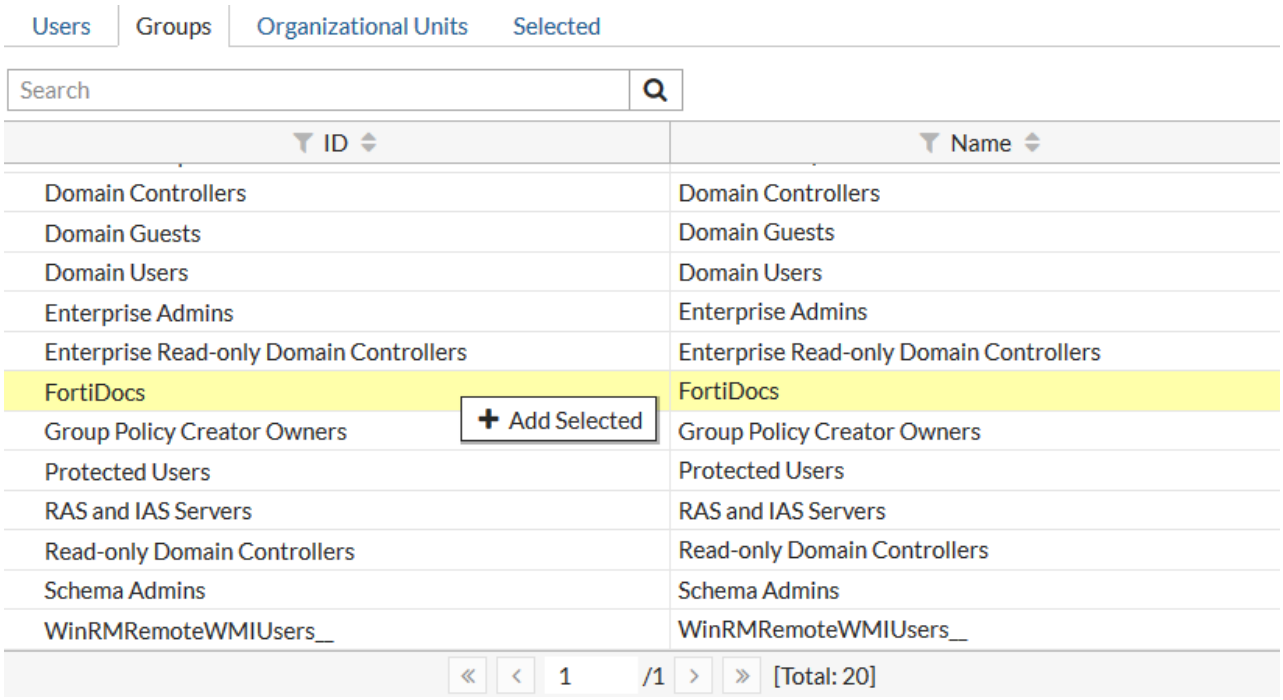
1. To configure the LDAP service, go to **User & Device > LDAP Servers** and select **Create New**.
2. Enter all information about your LDAP server. Select **Test Connectivity**. If your information is correct, **Connection status** is **Successful**.



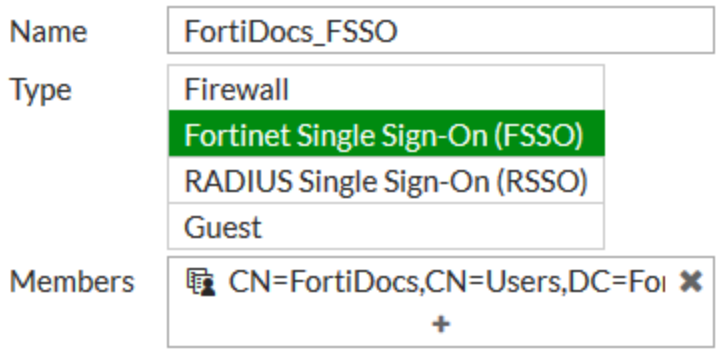
3. Create a Fabric Connector to the FSSO agent by going to **Security Fabric > Fabric Connectors** and select **+ Create New**.
4. Under **SSO/Identity**, select **Fortinet Single Sign-On Agent**.
5. Set the **Name** and enter the IP address and password for the **Primary FSSO Agent**.
6. Set **Collector Agent AD access mode** to **Advanced** and set **LDAP Server** to the new LDAP service.



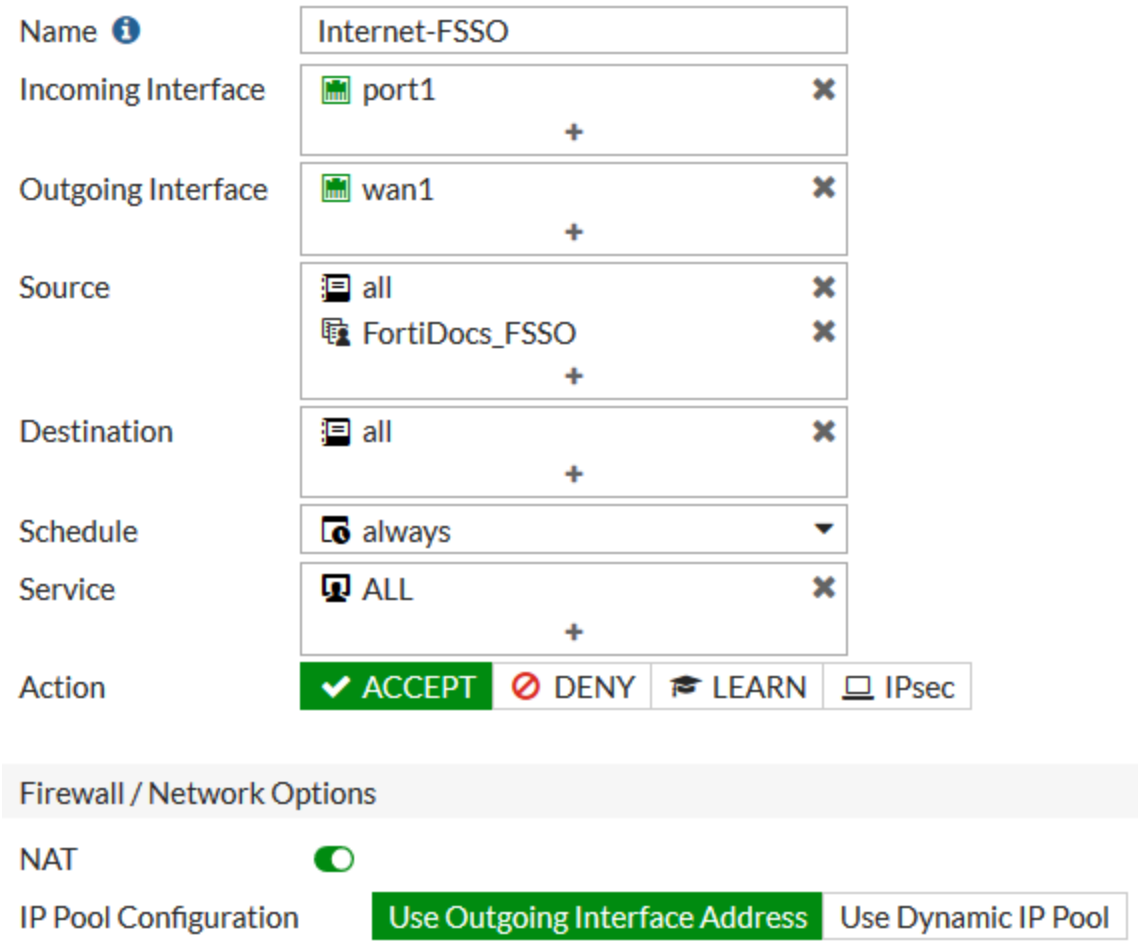
7. Your FortiGate displays information retrieved from the AD server. Select **Groups**, then right-click the FSSO group and select **+ Add Selected**.
8. Select **Selected**.
   The FSSO group is shown.



9. To create a user group for FSSO users, go to **User & Device > User Groups** and select **Create New**.
10. Enter a group **Name** and set **Type** to **Fortinet Single Sign-On (FSSO)**. Add the FSSO users to **Members**.



11. To create a policy for FSSO users, go to **Policy & Objects > IPv4 Policy** and select **Create New**.
12. For **Source**, set **User** to the FSSO user group.



Results

Log into a computer on the domain and access the Internet. The FortiGate uses FSSO for authentication and doesn't require your credentials to be entered again.

On the FortiGate, go to **Monitor > Firewall User Monitor** and select **Show all FSSO Logons**.