

KB LEVEL: NOC	KB ARTICLE	KB NUMBER: KB-NOC-2019-02-27-01
	<i>Configure Fortigate 300E for the Single Sign On Feature</i>	

KB Category:	Internal / NOC / Configuration / Firewall		
Author:	Ian John Lastimoso	Date:	February 27, 2019

Problem Description:	Different SSO configuration for FortiGate 300E
Symptoms and Cause of the issue:	Different FortiOS for each FortiGate units

Procedures:

I. SERVER CONFIGURATION

1. Install Fortinet Single Sign on Agent inside the Domain Controller
2. Setup Password on the Application. **Note:** That the password that will be entered on the application itself must be the same with the password that will be inputted On the Firewall. (See Picture below for reference)

3. Creation of FSSO_USERS inside the Active Directory

Name	Type	Description
FSSO_AVA	Security Group...	
FSSO_AVA_TLs	Security Group...	
FSSO_EMPREL	Security Group...	
FSSO_EXEC	Security Group...	
FSSO_FINANCE	Security Group...	
FSSO_MANAGERS	Security Group...	
FSSO_MAYO	Security Group...	
FSSO_QUORA_ENG	Security Group...	
FSSO_QUORA_INT	Security Group...	
FSSO_RECRUIT	Security Group...	
FSSO_UIPATH	Security Group...	
FSSO_WV	Security Group...	
FSSO_WV_TLs	Security Group...	

KB LEVEL: NOC	KB ARTICLE	KB NUMBER: KB-NOC-2019-02-27-01
	<i>Configure Fortigate 300E for the Single Sign On Feature</i>	

II. FIREWALL CONFIGURATION

1. **Access Fortigate 300E** *https:172.22.0.74:10443*
2. **Once Logged-In, Navigate to USER & DEVICE > LDAP SERVERS.** This can be found on the left side panel of the page
3. **From LDAP Servers, Click on Create New.** (See picture below for reference)

Edit LDAP Server

Name	<input type="text"/>
Server IP/Name	<input type="text"/>
Server Port	<input type="text" value="389"/>
Common Name Identifier	<input type="text" value="cn"/>
Distinguished Name	<input type="text"/> <input type="button" value="Browse"/>
Bind Type	<input type="button" value="Simple"/> <input type="button" value="Anonymous"/> <input type="button" value="Regular"/>
Username	<input type="text"/>
Password	<input type="password"/> <input type="button" value="Show"/>
Secure Connection	<input type="checkbox"/>
<input type="button" value="Test Connectivity"/>	

Here's an example on what to be filled out

Name: LDAP_1
 Server IP/Name: 172.22.1.1
 Port: 389
 Common Name Identifier: sAMAccountName
 Distinguished Name: DC= openaccess,DC=bpo
 Bind Type: Regular

Note: At the end of this configuration, Make sure to Click on "Test Connectivity" it should display an "Successful" notification on the bottom right side.

4. **Next is Navigate to Users & Device > Single Sign-on > Create New.** Please see picture below for reference.

KB LEVEL: NOC	KB ARTICLE	KB NUMBER: KB-NOC-2019-02-27-01
	<i>Configure Fortigate 300E for the Single Sign On Feature</i>	

New Single Sign-On Server

Type

Poll Active Directory Server
Fortinet Single-Sign-On Agent
RADIUS Single-Sign-On Agent

Name

Primary FSSO Agent

Server IP/Name

-

Password

+

Collector Agent AD access mode

Standard **Advanced**

LDAP Server

Apply & Refresh

OK

Cancel

Name: G2_LDAP

Type: Fortinet Single Sign-On Agent

Primary FSSO Agent: 172.22.1.1

Password: "Password that has been set on to your LDAP and Fortinet Agent inside the Domain Controller"

LDAP Server: "The created LDAP Server based on 3"

Verification:

1. **Navigate to Users & Device > Single Sign-on > The created FSSO > Double Click on the account**

Edit Single Sign-On Server

Name

G2_LDAP

Primary FSSO Agent

172.22.1.1

-

.....

+

Collector Agent AD access mode

Standard **Advanced**

LDAP Server

G2_LDAP1

Users

Groups

Organizational Units

Selected 10

2. **Click on Groups > Note: We should be able to see the created FSSO Groups based on the Server Configuration Step 3.**

KB LEVEL: NOC	KB ARTICLE	KB NUMBER: KB-NOC-2019-02-27-01
	<i>Configure Fortigate 300E for the Single Sign On Feature</i>	

Edit Single Sign-On Server

Primary FSSO Agent
172.22.1.1
-
.....
+

Collector Agent AD access mode
Standard
Advanced

LDAP Server
G2_LDAP1

Refresh
Recursive
DC=openaccess,DC=bpo

Users
Groups
Organizational Units
Selected 10

Search
Q

ID	Name
FSSO_ADORE_TLs	FSSO_ADORE_TLs
FSSO_ADORE	FSSO_ADORE
FSSO_AVA_TLs	FSSO_AVA_TLs
FSSO_AVA	FSSO_AVA
FSSO_MANAGERS	FSSO_MANAGERS
FSSO_QUORA_ENG	FSSO_QUORA_ENG
FSSO_QUORA_INT	FSSO_QUORA_INT
FSSO_RECRUIT	FSSO_RECRUIT
FSSO_WV_TLs	FSSO_WV_TLs
FSSO_WV	FSSO_WV

OK
Cancel