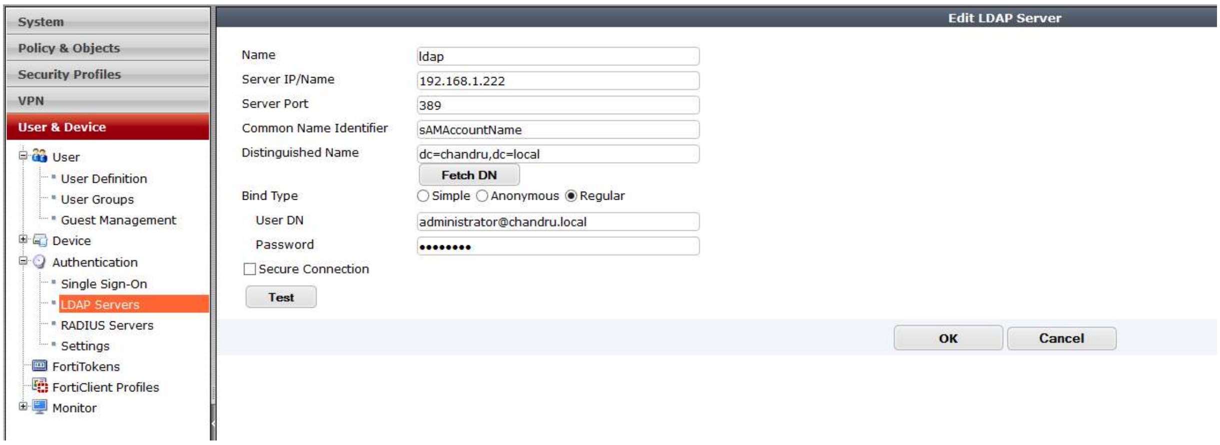
User based authentication on FSSO, using LDAP and FSSO agent on advanced mode.

Applicable Firmware version: v5.0 and v5.2

Requirements:

User based authentication required on FSSO, so different users get different profiles through policy. Need to integrate FortiGate with LDAP, install FSSO agent (with DC Agent) on the server with advanced mode and set user filter from FortiGate FSSO configuration using LDAP.

Integrate FortiGate with LDAP:



Edit LDAP Server

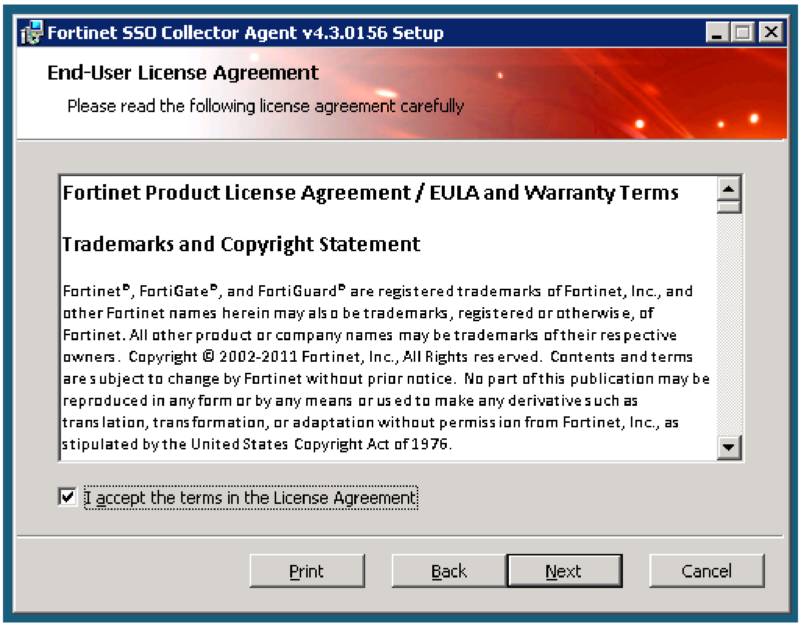
Name	ldap
Server IP/Name	192.168.1.222
Server Port	389
Common Name Identifier	sAMAccountName
Distinguished Name	dc=chandru,dc=local
	Fetch DN
Bind Type	○ Simple ○ Anonymous ● Regular
User DN	administrator@chandru.local
Password	••••••••

□ Secure Connection

```
config user ldap
   edit "ldap"
      set server "192.168.1.222"
      set cnid "sAMAccountName"
      set dn "dc=chandru,dc=local"
      set type regular
      set username "administrator@chandru.local"
      set password XYZ
   next
end
```

Install FSSO agent on the Server on Advanced mode:

1) Accept the agreement.



Fortinet SSO Collector Agent v4.3.0156 Setup

End-User License Agreement

Please read the following license agreement carefully

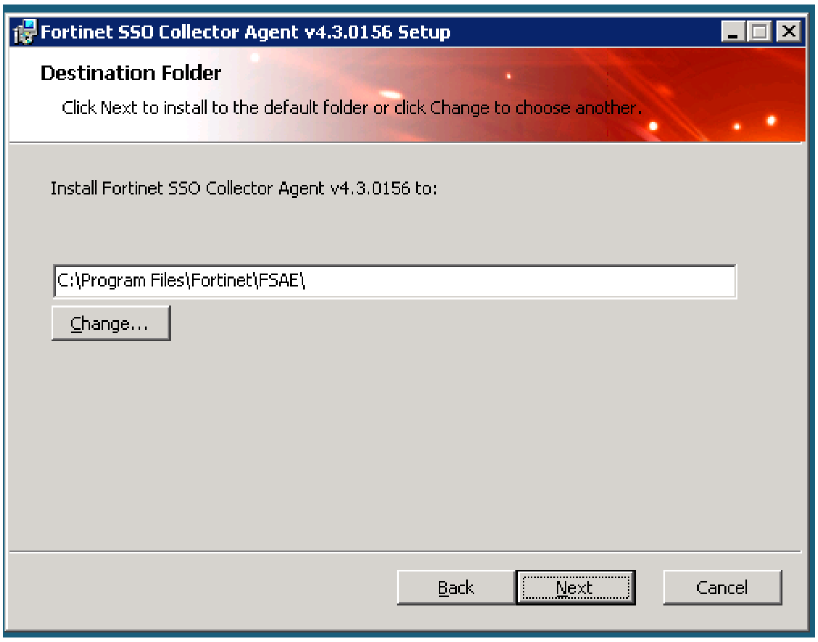
Fortinet Product License Agreement / EULA and Warranty Terms

Trademarks and Copyright Statement

Fortinet®, FortiGate®, and FortiGuard® are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be trademarks, registered or otherwise, of Fortinet. All other product or company names may be trademarks of their respective owners. Copyright © 2002-2011 Fortinet, Inc., All Rights reserved. Contents and terms are subject to change by Fortinet without prior notice. No part of this publication may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from Fortinet, Inc., as stipulated by the United States Copyright Act of 1976.

☑ I accept the terms in the License Agreement

2) Change the location if you require, however make sure you have the default location :



Fortinet SSO Collector Agent v4.3.0156 Setup

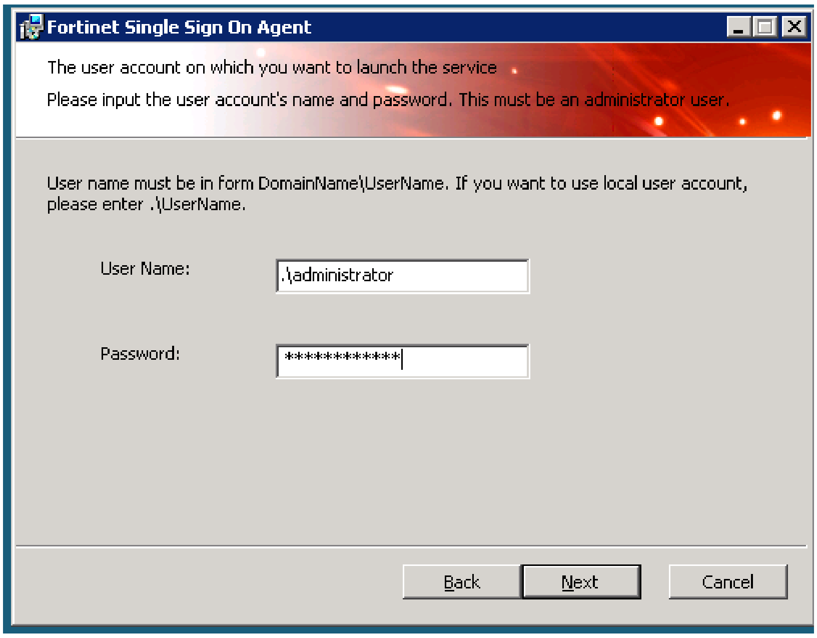
Destination Folder

Click Next to install to the default folder or click Change to choose another.

Install Fortinet SSO Collector Agent v4.3.0156 to:

C:\Program Files\Fortinet\FSAE\

3) Enter the domain admin credentials



The user account on which you want to launch the service

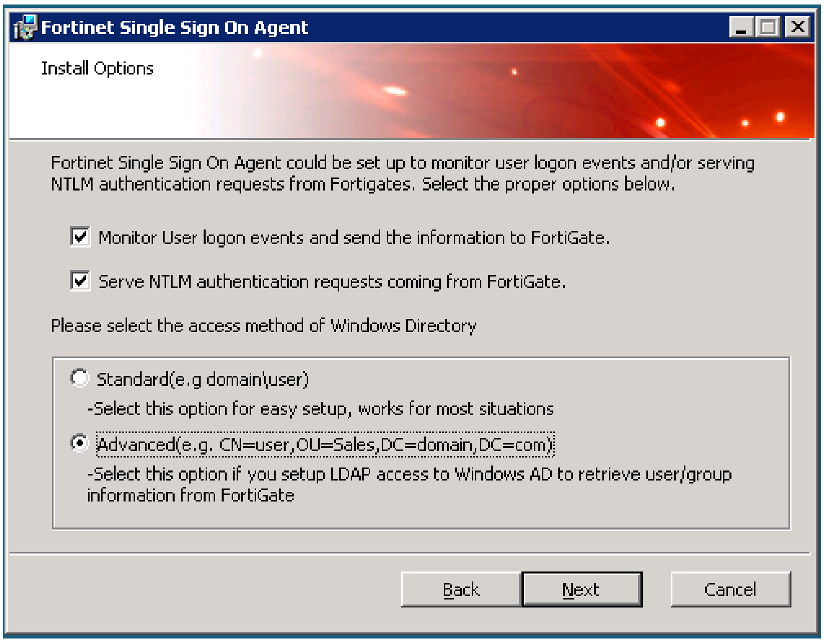
Please input the user account's name and password. This must be an administrator user.

User name must be in form DomainName\UserName. If you want to use local user account, please enter .\UserName.

User Name: .\administrator

Password: ************

4) Select the Advanced Mode



Install Options

Fortinet Single Sign On Agent could be set up to monitor user logon events and/or serving NTLM authentication requests from Fortigates. Select the proper options below.

☑ Monitor User logon events and send the information to FortiGate.

☑ Serve NTLM authentication requests coming from FortiGate.

Please select the access method of Windows Directory

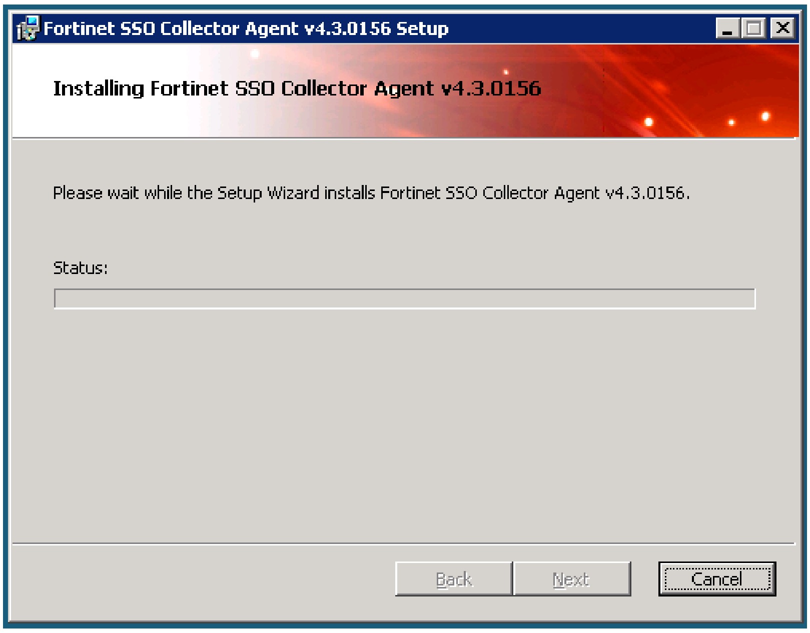
○ Standard(e.g domain\user)

-Select this option for easy setup, works for most situations

● Advanced(e.g. CN=user,OU=Sales,DC=domain,DC=com)

-Select this option if you setup LDAP access to Windows AD to retrieve user/group information from FortiGate

5) **Proceed to next to install the Agent**



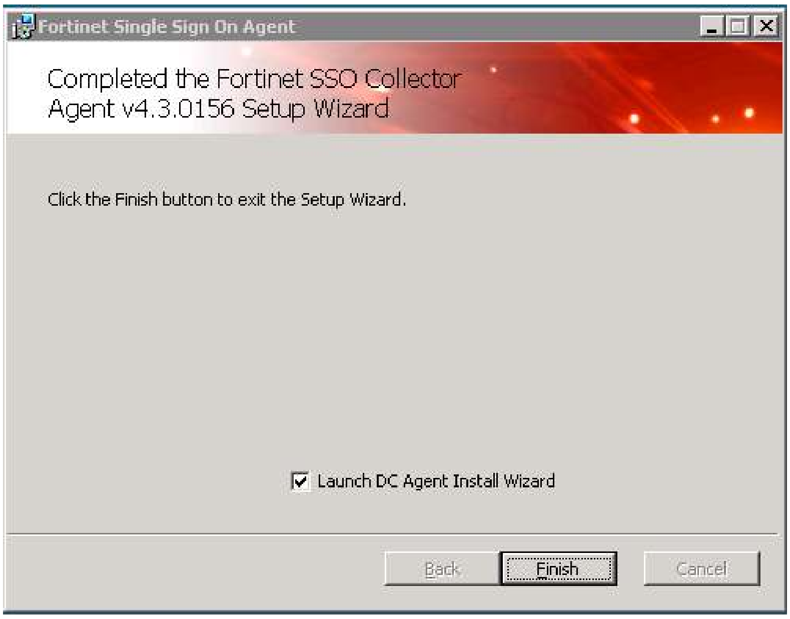
Fortinet SSO Collector Agent v4.3.0156 Setup

Installing Fortinet SSO Collector Agent v4.3.0156

Please wait while the Setup Wizard installs Fortinet SSO Collector Agent v4.3.0156.

Status:

6) **Install the DC Agent when it tries to launch**



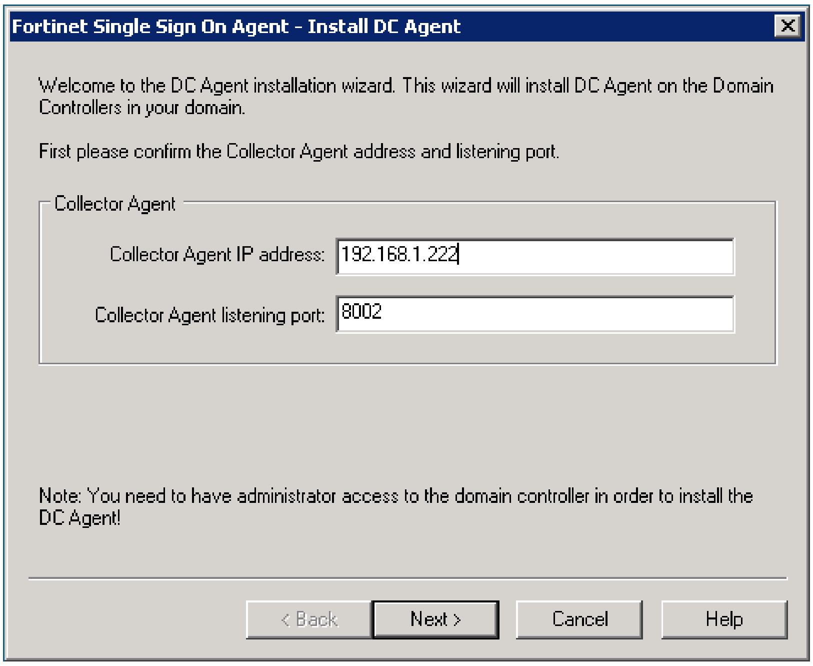
Fortinet Single Sign On Agent

Completed the Fortinet SSO Collector Agent v4.3.0156 Setup Wizard

Click the Finish button to exit the Setup Wizard.

☑ Launch DC Agent Install Wizard

7) You need to specify the Collector agent which the DC agent will talk to, if this is the same server, then leave the default



Welcome to the DC Agent installation wizard. This wizard will install DC Agent on the Domain Controllers in your domain.

First please confirm the Collector Agent address and listening port.

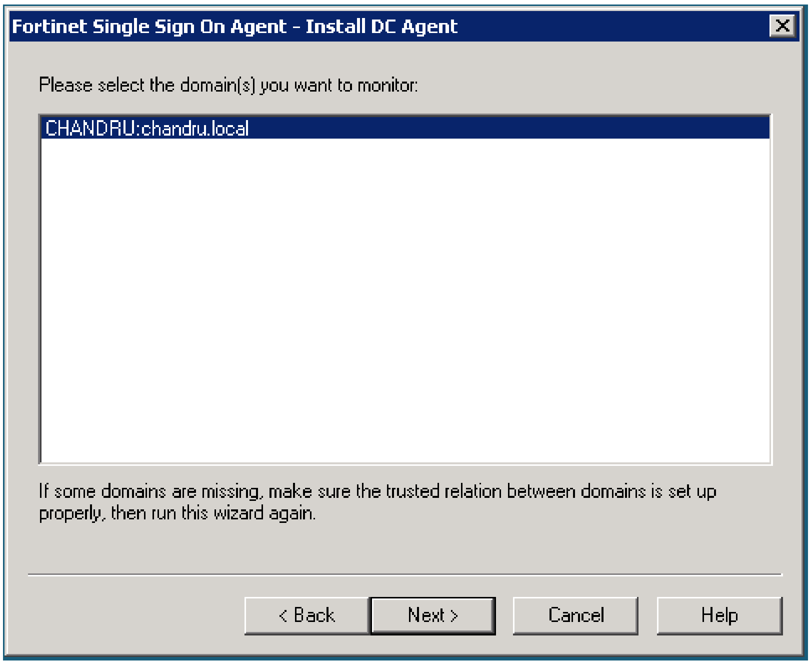
Collector Agent

Collector Agent IP address: 192.168.1.222

Collector Agent listening port: 8002

Note: You need to have administrator access to the domain controller in order to install the DC Agent!

8) Select the Domain to monitor and click Next

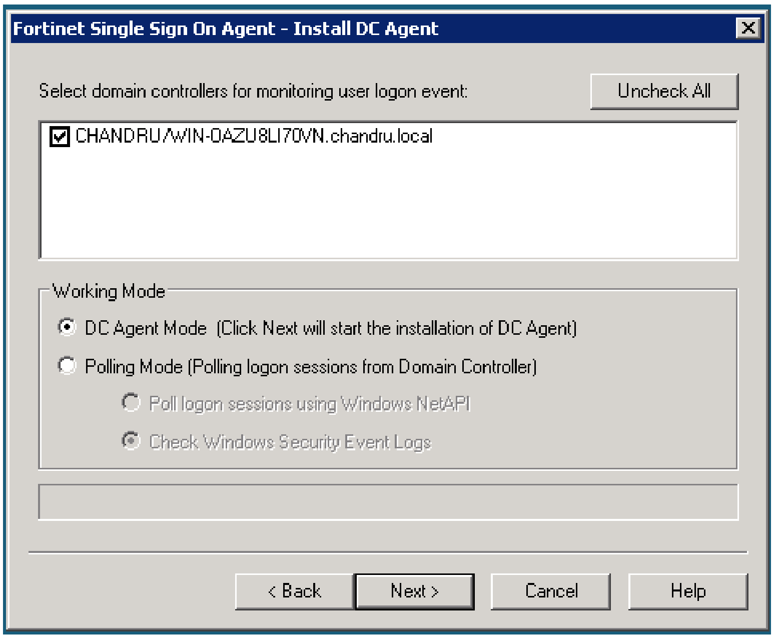


Please select the domain(s) you want to monitor:

CHANDRU:chandru.local

If some domains are missing, make sure the trusted relation between domains is set up properly, then run this wizard again.

9) In the Domain to monitor, select the DC Agent mode



Fortinet Single Sign On Agent - Install DC Agent

Select domain controllers for monitoring user logon event:

☑ CHANDRU/WIN-0AZU8LI70VN.chandru.local

Working Mode

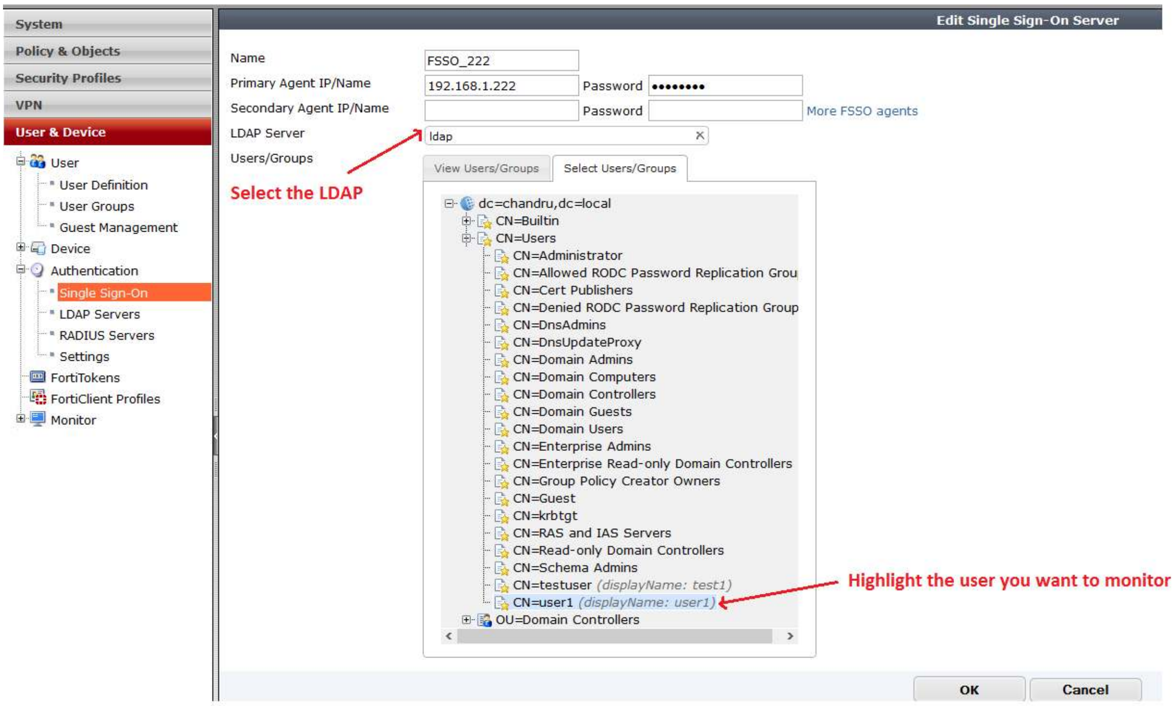
● DC Agent Mode (Click Next will start the installation of DC Agent)

○ Polling Mode (Polling logon sessions from Domain Controller)

○ Poll logon sessions using Windows NetAPI

● Check Windows Security Event Logs

Once the FSSO agent with DC agent is installed successfully, configure FortiGate FSSO by selecting LDAP server to filter the users



Edit Single Sign-On Server

Name: FSSO_222

Primary Agent IP/Name: 192.168.1.222 Password: ••••••••

Secondary Agent IP/Name: Password:

LDAP Server: ldap

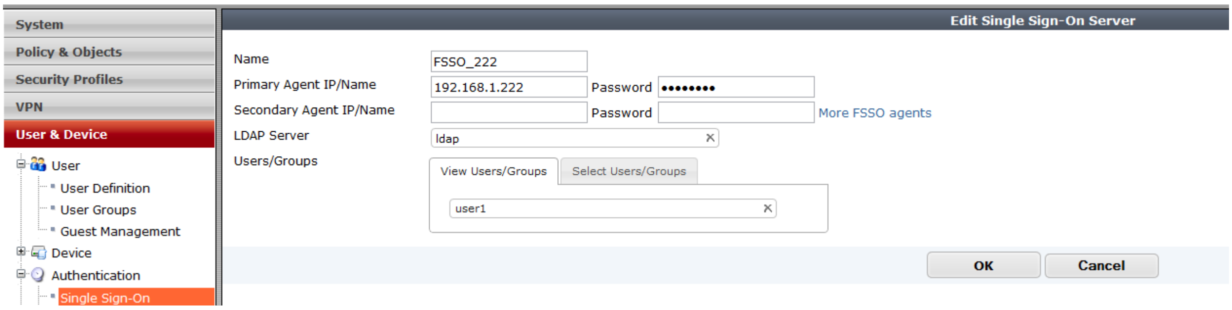
Users/Groups:

Select the LDAP

```
dc=chandru,dc=local
  CN=Builtin
  CN=Users
    CN=Administrator
    CN=Allowed RODC Password Replication Grou
    CN=Cert Publishers
    CN=Denied RODC Password Replication Group
    CN=DnsAdmins
    CN=DnsUpdateProxy
    CN=Domain Admins
    CN=Domain Computers
    CN=Domain Controllers
    CN=Domain Guests
    CN=Domain Users
    CN=Enterprise Admins
    CN=Enterprise Read-only Domain Controllers
    CN=Group Policy Creator Owners
    CN=Guest
    CN=krbtgt
    CN=RAS and IAS Servers
    CN=Read-only Domain Controllers
    CN=Schema Admins
    CN=testuser (displayName: test1)
    CN=user1 (displayName: user1)
  OU=Domain Controllers
```

Highlight the user you want to monitor

Once you select the user and click OK, you will see the user will be available



Name: FSSO_222

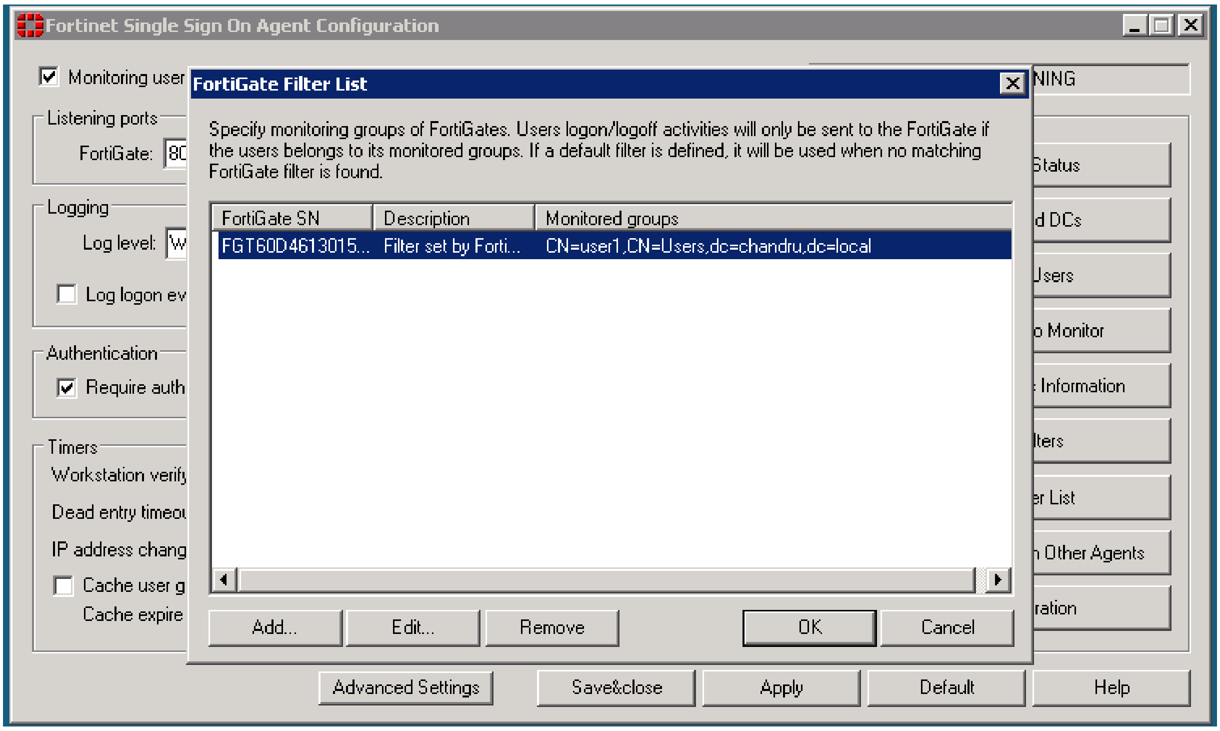
Primary Agent IP/Name: 192.168.1.222 Password: ••••••••

Secondary Agent IP/Name: Password:

LDAP Server: ldap

Users/Groups: user1

The same user will be reflecting on the FSSO agent once it synchronizes

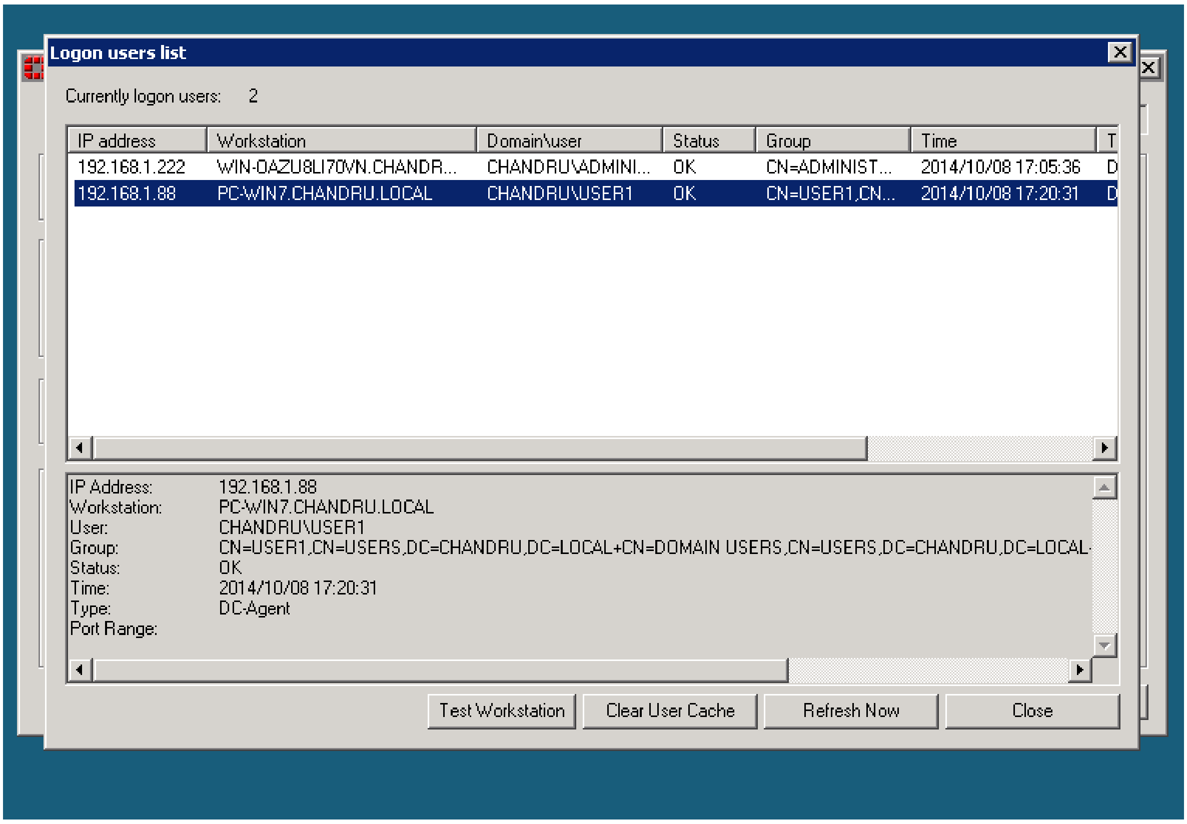


FortiGate Filter List

Specify monitoring groups of FortiGates. Users logon/logoff activities will only be sent to the FortiGate if the users belongs to its monitored groups. If a default filter is defined, it will be used when no matching FortiGate filter is found.

FortiGate SN	Description	Monitored groups
FGT60D4613015...	Filter set by Forti...	CN=user1,CN=Users,dc=chandru,dc=local

Domain workstation logged into the domain and created logon event on DC, the same information available on FSSO agent logon user list



Currently logon users: 2

IP address	Workstation	Domain\user	Status	Group	Time	T
192.168.1.222	WIN-0AZU8LI70VN.CHANDR...	CHANDRU\ADMINI...	OK	CN=ADMINIST...	2014/10/08 17:05:36	D
192.168.1.88	PC-WIN7.CHANDRU.LOCAL	CHANDRU\USER1	OK	CN=USER1,CN...	2014/10/08 17:20:31	D

```
IP Address:     192.168.1.88
Workstation:    PC-WIN7.CHANDRU.LOCAL
User:           CHANDRU\USER1
Group:          CN=USER1,CN=USERS,DC=CHANDRU,DC=LOCAL+CN=DOMAIN USERS,CN=USERS,DC=CHANDRU,DC=LOCAL-
Status:         OK
Time:           2014/10/08 17:20:31
Type:           DC-Agent
Port Range:
```

On FortiGate you can see the same user:

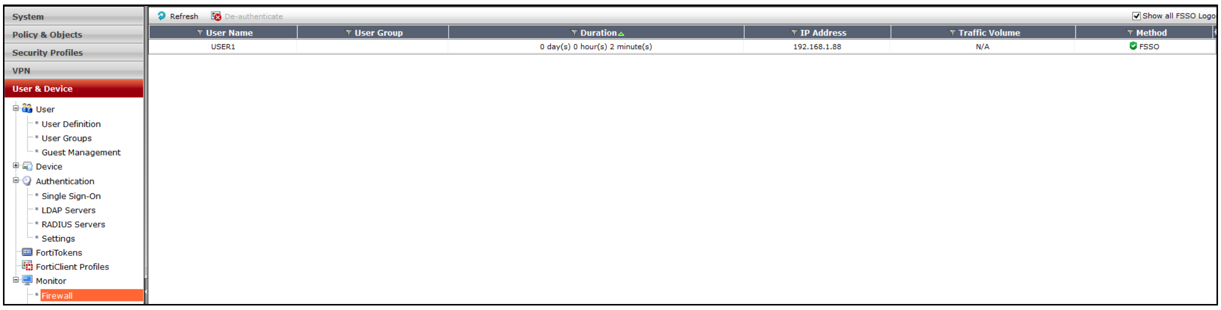
FGT60D4613015643 # diagnose debug authd fsso list

----FSSO logons----

IP: 192.168.1.88 User: USER1 Groups: CN=USER1,CN=USERS,DC=CHANDRU,DC=LOCAL Workstation: PC-WIN7.CHANDRU.LOCAL

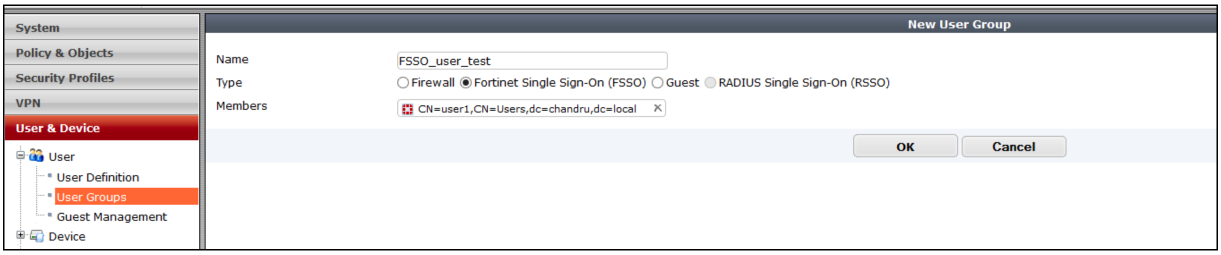
Total number of logons listed: 1, filtered: 0

----end of FSSO logons----



User Name	User Group	Duration	IP Address	Traffic Volume	Method
USER1		0 day(s) 0 hour(s) 2 minute(s)	192.168.1.88	N/A	FSSO

Create group on FortiGate and add the user1 to the group to authenticate to the policy

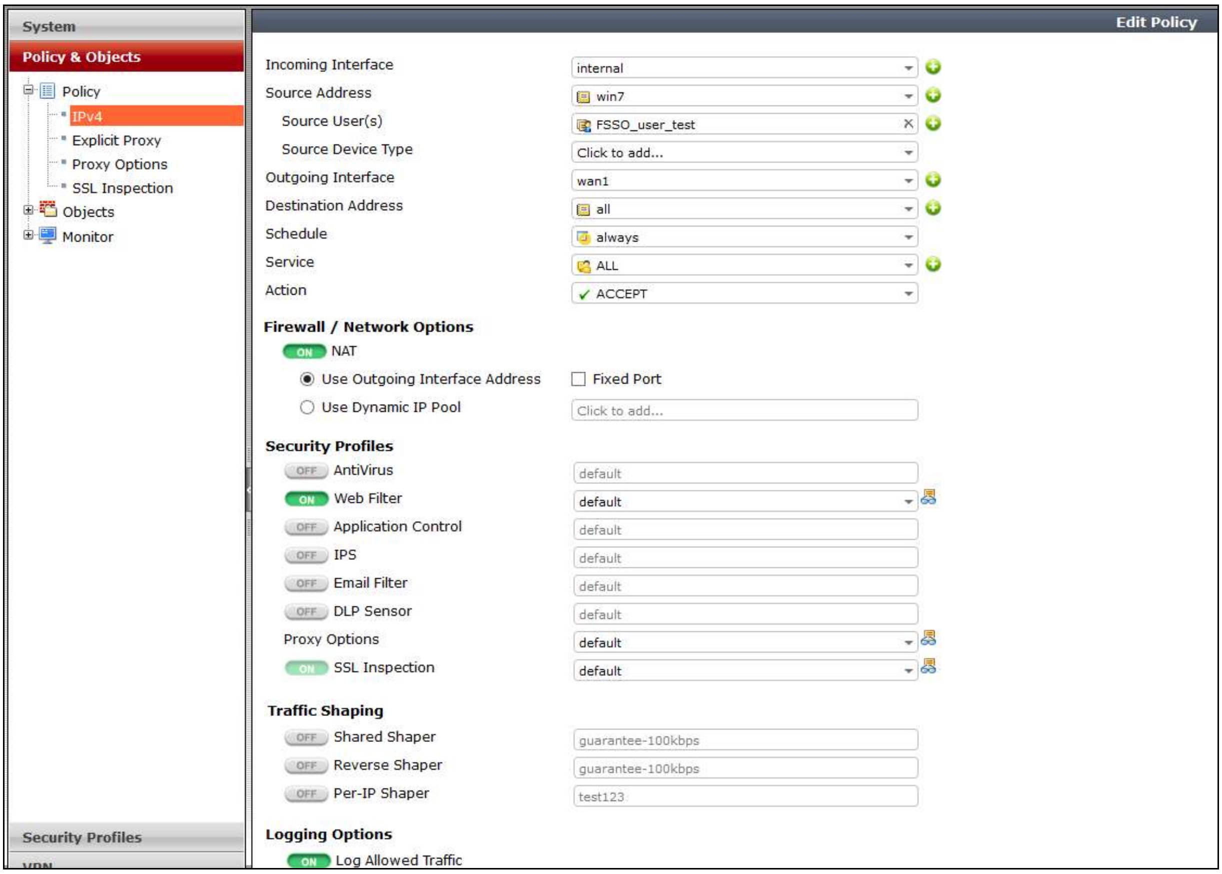


New User Group

Name: FSSO_user_test

Type: ○ Firewall ● Fortinet Single Sign-On (FSSO) ○ Guest ○ RADIUS Single Sign-On (RSSO)

Members: CN=user1,CN=Users,dc=chandru,dc=local ✕



Edit Policy

Incoming Interface	internal
Source Address	win7
Source User(s)	FSSO_user_test
Source Device Type	Click to add...
Outgoing Interface	wan1
Destination Address	all
Schedule	always
Service	ALL
Action	✓ ACCEPT

Firewall / Network Options

ON NAT

● Use Outgoing Interface Address □ Fixed Port

○ Use Dynamic IP Pool Click to add...

Security Profiles

OFF AntiVirus	default
ON Web Filter	default
OFF Application Control	default
OFF IPS	default
OFF Email Filter	default
OFF DLP Sensor	default
Proxy Options	default
ON SSL Inspection	default

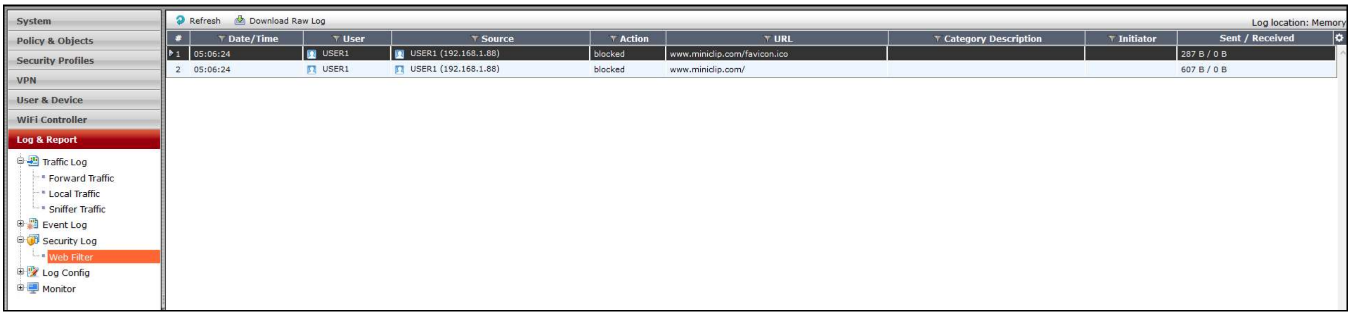
Traffic Shaping

OFF Shared Shaper	guarantee-100kbps
OFF Reverse Shaper	guarantee-100kbps
OFF Per-IP Shaper	test123

Logging Options

ON Log Allowed Traffic

Sample Web Filter logs for the user



Log location: Memory

#	Date/Time	User	Source	Action	URL	Category Description	Initiator	Sent / Received
1	05:06:24	USER1	USER1 (192.168.1.88)	blocked	www.miniclip.com/favicon.ico			287 B / 0 B
2	05:06:24	USER1	USER1 (192.168.1.88)	blocked	www.miniclip.com/			607 B / 0 B