



# Pocket Guide

Configure SF-OS to use AD Server for authentication

Product: Sophos XG Firewall

## Contents

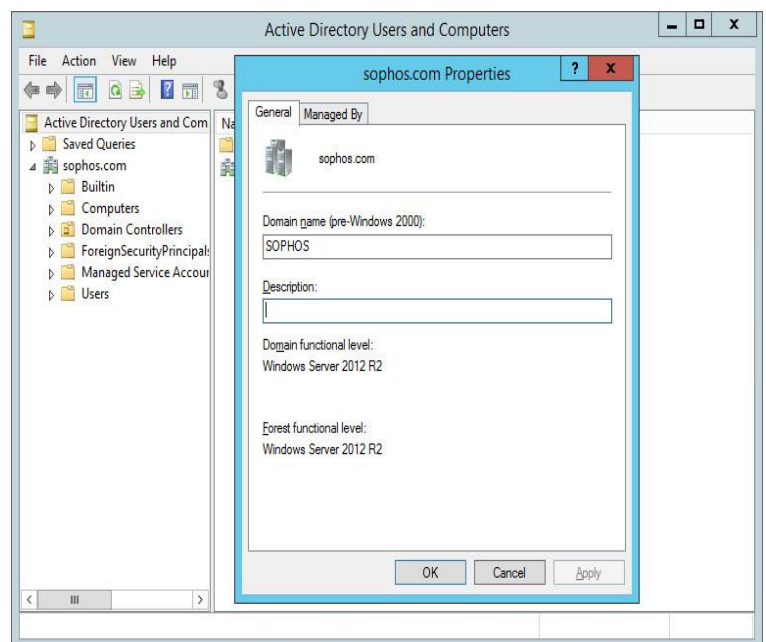
<b>Scenario</b> .....	<b>3</b>
<b>Prerequisites</b> .....	<b>3</b>
<b>Configuration</b> .....	<b>4</b>
Step 1: Configure Active Directory .....	4
Step 2: Select AD as the Primary Authentication Method .....	5
<b>Results</b> .....	<b>5</b>
<b>Suggested Reading</b> .....	<b>6</b>
<b>Copyright Notice</b> .....	<b>7</b>

## Scenario

This guide describes how to integrate Sophos XG Firewall (SF-OS) with Windows Active Directory (AD) to authenticate users based on groups, domains and organizational units listed within the Active Directory Server (ADS).

## Prerequisites

- You must have read-write permissions on the SF-OS Admin Console for the relevant features.
- You will need the following SF-OS and AD parameters during the integration:
  - IP address of the SF-OS interface connected to ADS
  - IP address of ADS
  - Administrator username and password for ADS
- To get the following parameters, log in to ADS as Admin. Go to **Start > Programs > Administrative Tools > Active Directory Users and Computers**.
  - NetBIOS domain name
  - FQDN (example: sophos.com)
  - Search DN (example: dc=sophos, dc=com)



## Configuration

Log in to the SF-OS Admin Console.

### Step 1: Configure Active Directory

- Go to **Configure > Authentication > Servers** and click **Add**.
- Set **Server Type** to **Active Directory**.
- Enter the **NetBIOS Domain**, **Display Name Attribute** and **Email Name Attribute** from the ADS.
- The **default Port** is based on the **Connection Security** option that you select. Change the port number, if required.
- For **Connection Security** options **SSL/TLS** or **STARTTLS**, select **Validate Server Certificate**, if required.

The screenshot shows the 'Add External Server' configuration page in the SF-OS Admin Console. The page has a navigation bar at the top with 'Servers', 'Services', 'Groups', 'Users', 'One-Time Password', 'Captive Portal', 'Guest Users', 'Clientless Users', 'STAS', and a user profile 'admin' (Sophos Test Account). The main form is titled 'Add External Server' and contains the following fields:

- Server Type: Active Directory (dropdown)
- Server Name \*: Sophos
- Server IP/Domain \*: 172.16.16.50
- Port \*: 389
- NetBIOS Domain \*: test
- ADS Username \*: Administrator
- Password \*: [masked]
- Connection Security \*: Simple (dropdown)
- Display Name Attribute: Enter Display Name Attribute
- Email Address Attribute: mail
- Domain Name \*: sophos.com
- Search Queries \*: dc=sophos,dc=com (with Add, Remove, Move Up, Move Down actions)

At the bottom of the form, there are three buttons: 'Test Connection', 'Save', and 'Cancel'.

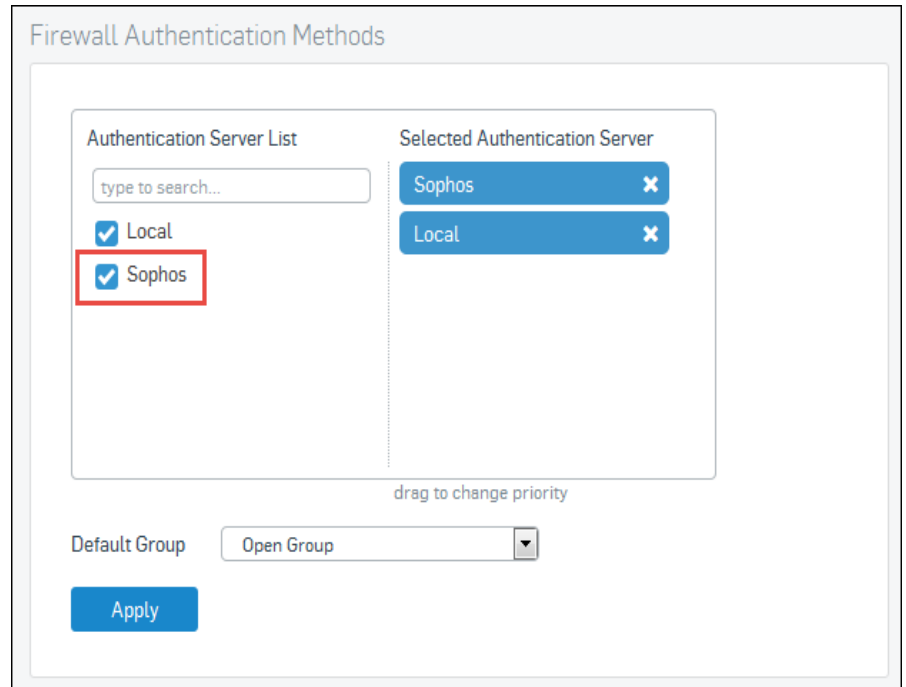
Note:

For **Connection Security** option **Simple**, **username** and **password** are communicated in plain text between SF-OS and ADS.

Click **Save**.

## Step 2: Select AD as the Primary Authentication Method

- Go to **Configure > Authentication > Services**.
- Within **Firewall Authentication Methods**, go to the **Authentication Server List** and select the ADS you have configured in Step 1.
- In the **Selected Authentication Server** list, drag the selected ADS to the top position. This ADS will act as the primary authentication server.



### Note:

The default authentication server (Local) is SF-OS.

Click **Apply**.

## Results

You have configured ADS as your primary authentication server. All users will be authenticated by this ADS.

## **Suggested Reading**

Import Active Directory Groups using Wizard.

## Copyright Notice

Copyright 2015-2016 Sophos Limited. All rights reserved.

Sophos is a registered trademark of Sophos Limited and Sophos Group. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise unless you are either a valid licensee where the documentation can be reproduced in accordance with the license terms or you otherwise have the prior permission in writing of the copyright owner.