



# Pocket Guide

Configure SF-OS to use LDAP 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: Create the LDAP group (optional).....	4
Step 2: Configure LDAP authentication .....	5
Step 3: Select LDAP as Authentication Server .....	6
<b>Results</b> .....	<b>6</b>
<b>Copyright Notice</b> .....	<b>7</b>

## Scenario

This guide describes how to integrate Sophos XG Firewall (SF-OS) with LDAP (Lightweight Directory Access Protocol) to authenticate users.

## Prerequisites

- You must have read-write permissions on the SF-OS Admin Console for the relevant features.
- You will need the following LDAP parameters during the integration:
  - LDAP server IP address and port
  - LDAP version
  - LDAP administrator username and password (If Anonymous Login is disabled)
  - Authentication Attribute is used to perform user search. By default, LDAP uses UID attribute to identify user entries.
  - Group Name Attribute, Display Name Attribute, Email Address Attribute and Expire Date Attribute

## Configuration

- Log in to the SF-OS Admin Console.

### Step 1: Create the LDAP group [optional]

By default LDAP users are added to the Default group of SF-OS. If you do not want to add them to the Default group, create a new LDAP group in SF-OS. The group is synchronized with the LDAP server at the time of each user's first login.

- Go to **Configure > Authentication > Groups** and click **Add**.
- Set **Group Type** to **Normal** to log in using the client device; or to **Clientless** to perform access control through IP address.
- You can create, or choose the Policies.
- To override a user's group policy, create or choose **Remote Access** and **Clientless** policies.

Note: **Remote Access**: To deny SSL VPN access, select No Policy Applied.

- **Login restriction** allows access from any or specified nodes.

Click **Save**.

The screenshot shows the 'Authentication' configuration page in the SF-OS Admin Console, specifically the 'Groups' tab. The page is titled 'Authentication' and has a navigation bar with tabs for 'Servers', 'Services', 'Groups', 'Users', 'One-Time Password', 'Captive Portal', and 'Guest Users'. The 'Groups' tab is selected. The main content area is divided into several sections:

- Group Name \***: A text input field containing 'LDAP\_Server'.
- Description**: A text area with the placeholder text 'Description'.
- Group Type \***: A dropdown menu set to 'Normal'.
- Policies**: A section with several dropdown menus, each with an information icon (i):
  - Surfing Quota \***: 'Unlimited Internet Access'
  - Access Time \***: 'Allowed all the time'
  - Network Traffic**: '100 MB Total Data Transfer policy'
  - Traffic Shaping**: 'Extremely Limited User'
  - Remote Access \***: 'No Policy Applied'
  - Clientless \***: 'No Policy Applied'
- Quarantine Digest \***: Radio buttons for 'Enable' (selected) and 'Disable'.
- MAC Binding**: Radio buttons for 'Enable' (selected) and 'Disable'.
- L2TP \***: Radio buttons for 'Enable' (selected) and 'Disable'.
- PPTP \***: Radio buttons for 'Enable' (selected) and 'Disable'.
- Login Restriction\***: Radio buttons for 'Any Node', 'Selected Nodes', and 'Node Range' (selected). Below this are two text input fields: 'From IP' (172.16.16.80) and 'To IP' (172.16.16.90), with '(IPv4 Address)' text to the right.

At the bottom of the page, there are two buttons: 'Save' and 'Cancel'.

Step 2: Configure LDAP authentication

- Go to **Configure > Authentication > Servers** and click **Add**.
- Set **Server Type** to **LDAP Server**.
- The default **Port** is based on the **Connection Security** that you select. Change the port number, if required.
- For **Connection Security** options **SSL/TLS** or **STARTTLS**, select **Validate Server Certificate**, if required.
- **Client Certificate** is set to the default certificate, change if required.
- Click **Get Base DN** to retrieve it from the LDAP directory.
- To use an attribute other than the default **UID**, enter the **Authentication Attribute**.

The screenshot shows the 'Servers' configuration page in SF-OS. The 'Server Type' is set to 'LDAP Server'. The 'Server Name' is 'LDAP\_Server', 'Server IP/Domain' is '172.16.16.80', and 'Port' is '636'. 'Version' is set to '3'. 'Anonymous Login' and 'Validate Server Certificate' are checked. 'Connection Security' is set to 'SSL/TLS'. 'Client Certificate' is 'ApplianceCertificate'. 'Base DN' is 'dc=sophos, dc=com'. 'Authentication Attribute' is 'UID', 'Display Name Attribute' is 'LDAP', 'Email Address Attribute' is 'mail', 'Group Name Attribute' is 'GID', and 'Expiry Date Attribute' is 'Date'. At the bottom, there are buttons for 'Test Connection', 'Save', and 'Cancel'.

Note:

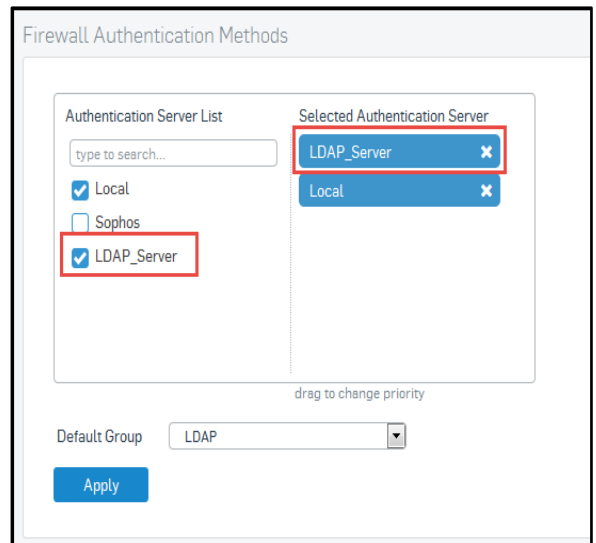
For **Connection Security** option **Simple**, **username** and **password** are communicated in plain text between SF-OS and LDAP.

Click **Save**.

### Step 3: Select LDAP as Authentication Server

- Go to **Configure > Authentication > Services**
- Within **Firewall Authentication Methods**, go to the **Authentication Server List** and select the **LDAP Server** you have configured in Step 2.
- In the **Selected Authentication Server** list, drag the selected **LDAP server** to the top. This **LDAP server** will act as the primary authentication server.

Click **Apply**.



## Results

You have integrated SF-OS with LDAP. All users will be authenticated by this LDAP server.

## 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.