



Pocket Guide

Configure SFOS to use LDAP server for authentication

Product: Sophos XG Firewall

Contents

Scenario	3
Prerequisites	3
Configuration	4
Step 1: Create the LDAP group (optional).....	4
Step 2: Configure LDAP authentication	5
Step 3: Select LDAP as Authentication Server	6
Result	7
Copyright Notice	8

Scenario

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

Prerequisites

- You must have read-write permissions on the SFOS 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 SFOS Admin Console.

Step 1: Create the LDAP group [optional]

By default LDAP users are added to the Default group of SFOS. If you do not want to add them to the Default group, create a new LDAP group in SFOS. 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 SFOS Admin Console, specifically the 'Groups' tab. The page is titled 'Authentication' and has several tabs: Servers, Services, Groups (selected), Users, One-Time Password, Captive Portal, and Guest Users. The main configuration area is divided into two sections: 'Group Information' and 'Policies'.

Group Information:

- Group Name *: LDAP_Server
- Description: Description
- Group Type *: Normal

Policies:

- 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 *: Enable Disable
- MAC Binding: Enable Disable
- L2TP *: Enable Disable
- PPTP *: Enable Disable
- Login Restriction*: Any Node Selected Nodes Node Range

At the bottom of the Login Restriction section, there are two input fields: 'From IP' with the value '172.16.16.80' and 'To IP' with the value '172.16.16.90'. A note '(IPv4 Address)' is visible next to the To IP field.

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**.

Servers	Services	Groups	Users	One-Time Password	Captive Portal
Server Type	LDAP Server				
Server Name *	LDAP_Server				
Server IP/Domain *	172.16.16.80				
Port *	636				
Version *	3				
Anonymous Login *	<input checked="" type="checkbox"/>				
Connection Security *	SSL/TLS				
Validate Server Certificate	<input checked="" type="checkbox"/>				
Client Certificate	ApplianceCertificate				
Base DN *	dc=sophos, dc=com				Get Base DN
Authentication Attribute *	UID				
Display Name Attribute	LDAP				
Email Address Attribute	mail				
Group Name Attribute *	GID				
Expiry Date Attribute *	Date				
Test Connection Save Cancel					

Note:

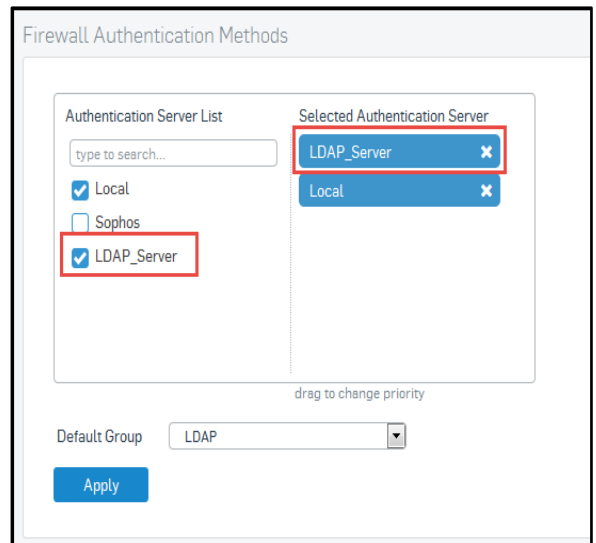
For **Connection Security** option **Simple**, **username** and **password** are communicated in plain text between **SFOS** and **LDAP**.

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**.



Result

You have integrated **SFOS** 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.