

Forcepoint Data Security Posture Management

Powered by **Getvisibility**

Setup LDAP AD Scan



Report

Forcepoint
April 23, 2024

Table of Contents

INTRODUCTION	2
STEPS:	2
DEFINITIONS	3

Introduction

This feature gathers permissions and access rights for groups, users, and other entities (trustees) on an LDAP server. When used with a corresponding CIFS/SMB server, users can review file permissions and access from the DDC/FDC UI and analytics.

Steps:

1. Go to **Administration > Data Sources > LDAP**

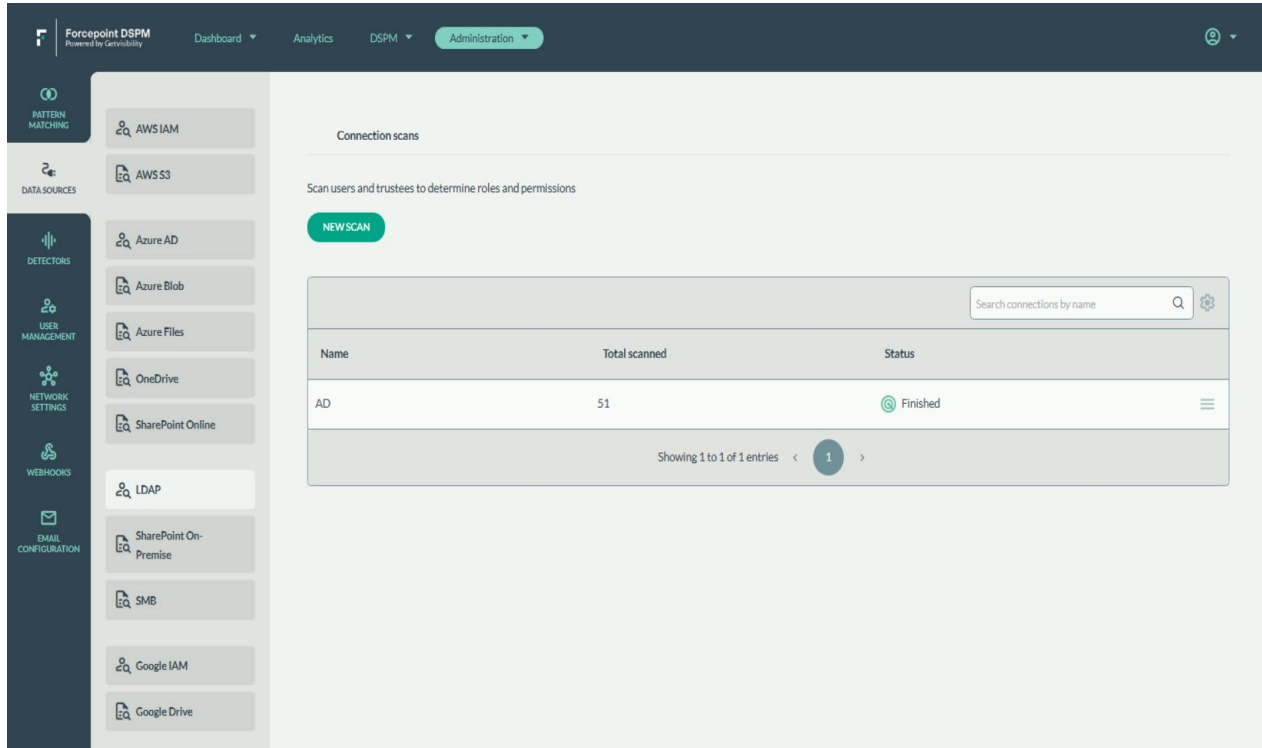


Figure 1.

2. Select **New Scan**.
3. Enter the following details of the LDAP to scan and select **SAVE**.

The screenshot shows a 'New LDAP scan share' dialog box with the following fields and values:

- Name: [Empty]
- Username: admin@domain.com
- Password: [Empty]
- IP Address: 0.0.0.0
- Certificate (optional): [Empty]
- Port: 389
- Inactivity: 90
- Search base: DC=aws-gv,DC=local
- Data Owner: Select user
- Geographic Location: Select countries

Buttons: CANCEL, SAVE

Figure 2.

Definitions

- **Name:** Give a name to the scan to identify it later
- **Username:** The user must be an admin level and have access to all the LDAP utilities to be scanned. The username should be entered in the format user@domain.com
- **Password:** Password for the admin user
- **IP Address:** The IP Address of the server where the LDAP is installed
- **Certificate (Optional):** If the server you wish to scan uses LDAPS (LDAP over SSL/TLS) enter your certificate text here. Otherwise leave it blank
- **Port:** 389 is the default port for LDAP, however for Secure LDAP 636 is used.
- **Inactivity:** This defines inactive users. Default is 90 days
- **Search:** This is the point in the LDAP directory where DDC will start searching from.
- **Data Owner:** Select from the drop-down.
- **Geographical location:** Select from the drop-down.

In this example: **DC** stands for Domain Component. An attribute used to represent domain levels.

aws-gv is the name of the first-level domain.

local is the top-level domain.

Together, **DC=aws-gv,DC=local** represents the domain **aws-gv.local**.

4. Back on the **LDAP connections** page, From the burger menu, select **Start trustee scan**.

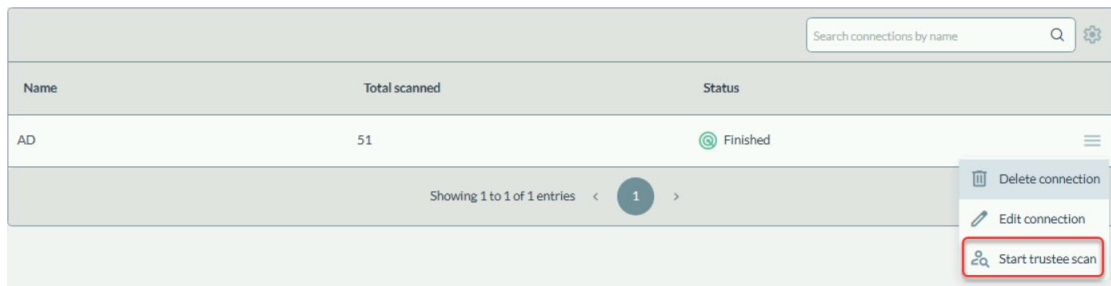


Figure 3.

DDC has now begun discovering trustees and assessing permissions on files. An overview of the results can be found on the **Explore Trustees** page.

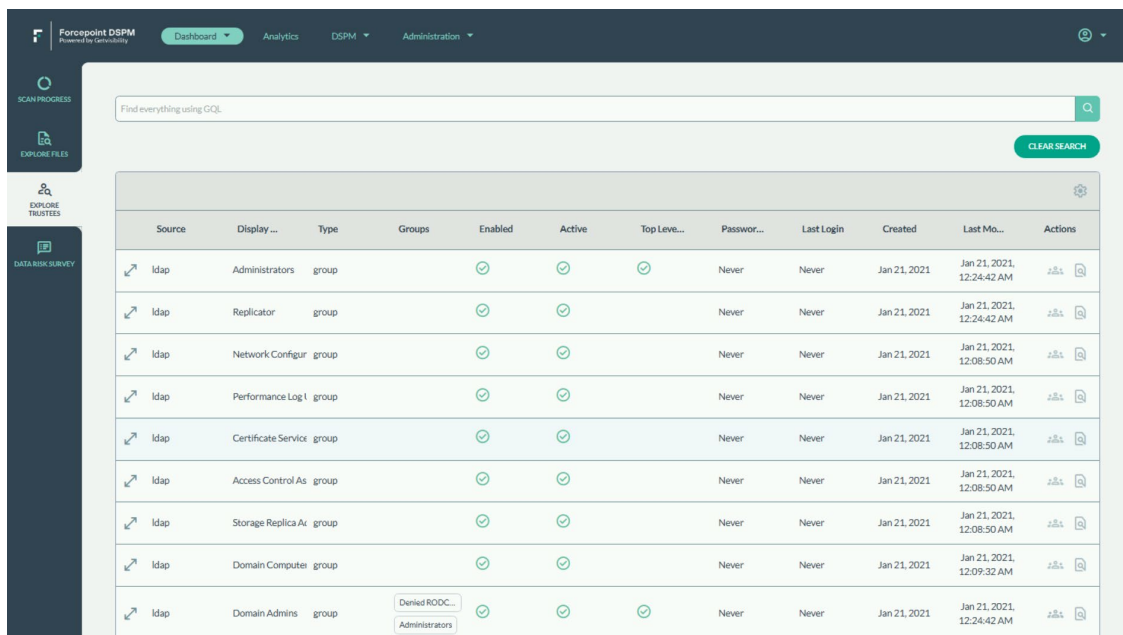


Figure 4.



forcepoint.com/contact

About Forcepoint

Forcepoint simplifies security for global businesses and governments. Forcepoint's all-in-one, truly cloud-native platform makes it easy to adopt Zero Trust and prevent the theft or loss of sensitive data and intellectual property no matter where people are working. Based in Austin, Texas, Forcepoint creates safe, trusted environments for customers and their employees in more than 150 countries. Engage with Forcepoint on www.forcepoint.com, [Twitter](#) and [LinkedIn](#).