Troubleshoot Active Directory Users Missing from the Umbrella Dashboard

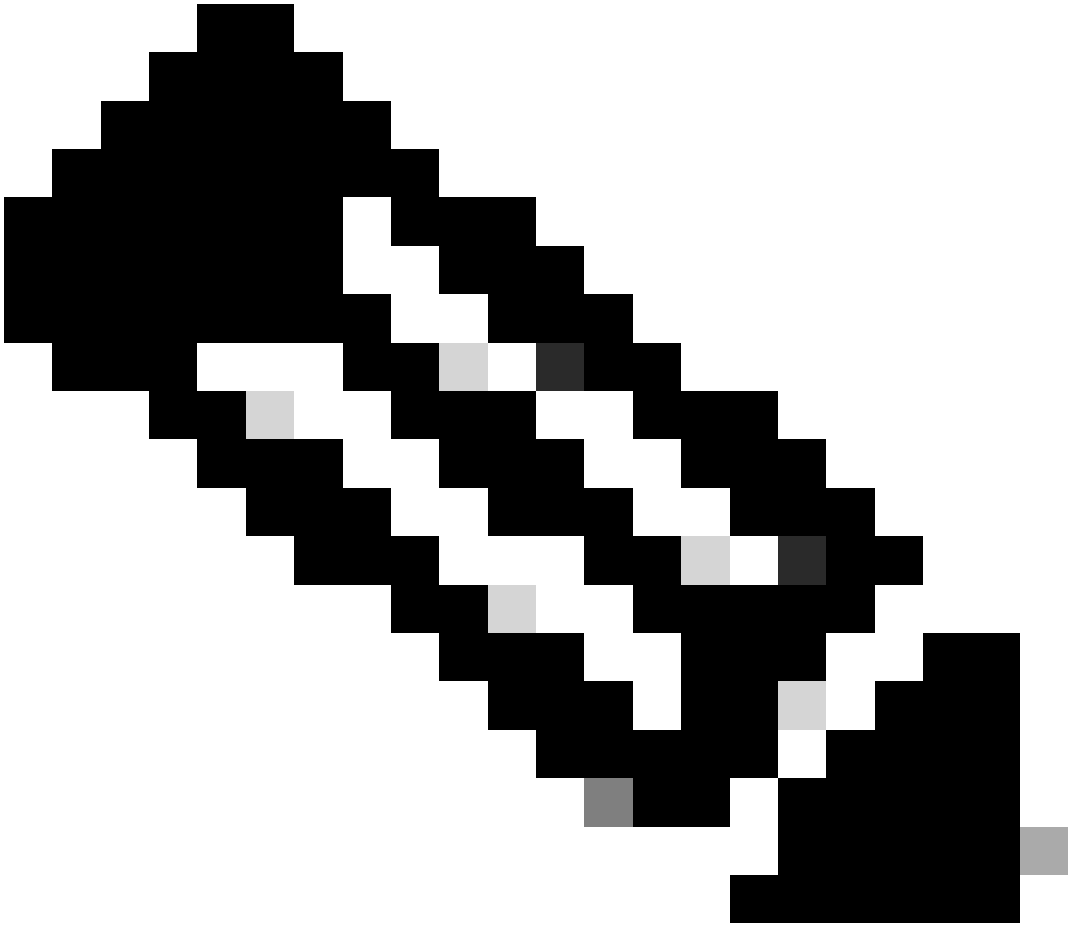
Contents

Introduction

This document describes how to troubleshoot Active Directory (AD) users that are missing from the Umbrella dashboard.

Overview

The OpenDNS Connector runs a sync against Active Directory to return a list of AD users, groups, and computers. This list is then posted securely to the Umbrella dashboard so they can be used for policies and reporting.

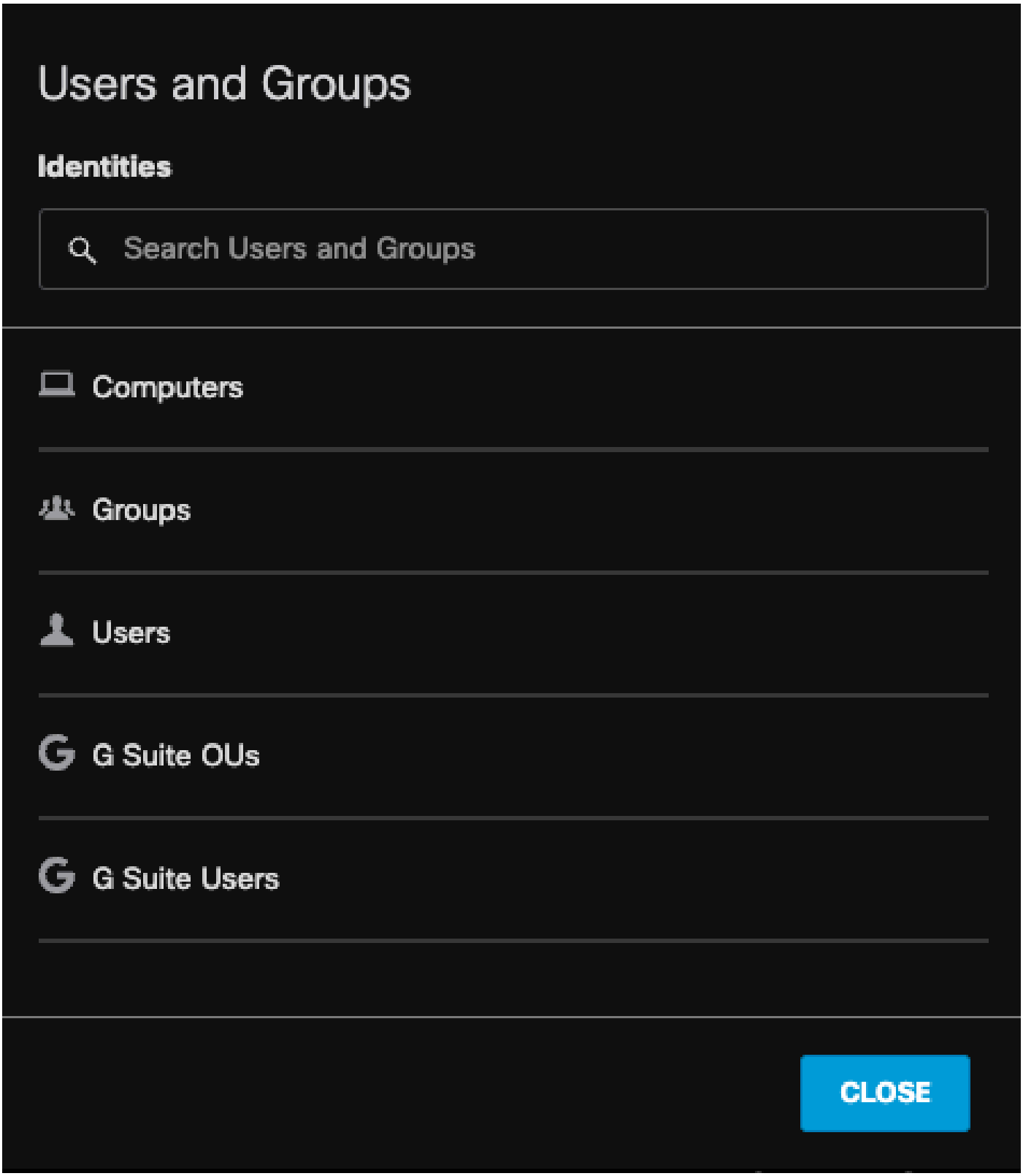


Note: If you are using version 1.1.24 or higher of the Connector software, it is possible to specify which AD groups are synced to Umbrella.

You can check which objects have been synced to the Dashboard by navigating to **Deployments > Core Identities > Users and Groups**.

Scenario 1 - All Users and Groups Missing From the Dashboard

If all users are missing from the Identities tab, this indicates that the AD sync has not occurred.



26022106541844

Potential causes include:

- The Active Directory integration has not been configured, or the OpenDNS Connector is not installed. For more information, see the Active Directory Identity Integrations documentation.
- The OpenDNS connector is unable to contact the Domain Controller on the required ports.
- There is a permissions error that prevents the OpenDNS_Connector user from reading the directory via LDAP.
- There is a problem with the OpenDNS_Connector user account (which is used for the sync). The

password entered during connector installation could be incorrect or the account might be locked out.
- The OpenDNS connector service is installed but not working. The most common cause is that **ldifde.exe** (used to perform the AD sync via LDAP) is not installed (most commonly it is included in the AD LDS role), notably when the Connector is installed on a machine other than a Domain Controller. Please view the pre-requisites for non-DC installation.
- The **C:\CiscoUmbrellaADGroups.dat** file exists, but is empty or has an incorrect format.

For more information, please contact Cisco Umbrella support with the Connector logs.

Scenario 2 - Newly Created Users/Groups Missing From the Dashboard

The Connector frequently syncs with Active Directory to determine if there have been any changes to the directory using LDAP. If there has been a recent change, a full LDAP sync is then performed. It can take several hours for new users/groups to take effect in the Dashboard.

If new users are never appearing, it could be due to:

- The **OpenDNS_Connector** account does not have permission for **'replicating directory changes'** which is required for us to monitor changes in AD. Ensure that the **OpenDNS_Connector** is a member of the **'Enterprise Read-Only Domain Controllers'** group to assign the correct permissions.
- The connector was able to sync previously but is now unable to. See the steps in this article to resolve the issue.

Scenario 3 - Specific AD Objects Are Missing From the Dashboard

We recommend that you create your own AD groups for use within Umbrella policies.
Domain Admins and several other "default" groups are excluded from the sync. Many well-known groups associated with background software (such as Exchange, SQL, and WSUS) are also excluded from the AD sync.

If the **C:\CiscoUmbrellaADGroups.dat** file exists, verify that it specifies an AD group that includes the missing AD objects.

Scenario 4 - AD Sync is Working but Some AD Objects Are Not Synced

Check that the OpenDNS_Connector user has permission to **"Read"** information from the objects that are missing. In Active Directory, all objects (including users, groups, and computers) have their own ACL permissions to determine who can read their attributes. For more information please check this article: Permissions Troubleshooting

If the **C:\CiscoUmbrellaADGroups.dat** file exists, verify that it specifies an AD group that includes the non-synced AD objects.

Scenario 5 - Certain Built-in AD Groups and Roles Are Not Visible in the Cisco Umbrella Policy Wizard

After deploying Umbrella Active Directory integration components, specifically the AD Connector, you find that certain built-in AD groups are not found in the Umbrella Policy wizard.

However, non-built-in AD groups, AD users, and AD computers are still found in the Umbrella Policy wizard as expected. The AD Connector purposely does not import built-in AD groups to the Umbrella API. As such, it is expected that you are not be able to define policies for these groups. Please refer to this Knowledge Base article for more details: Why are certain built-in Active Directory groups not displaying in the Umbrella Policy wizard?