Configure Users, Groups, and Computers from Active Directory to Sync with OpenDNS Connector Service

Contents

Introduction

This document describes how to sync users, groups, and computers from Active Directory with the OpenDNS Connector service.

Overview

As part of its operation the OpenDNS Connector service syncs a list of users, groups and computers from Active Directory using the LDAP protocol. This article describes how to check that the **OpenDNS_Connector** account has the correct permissions to read those objects.

Each object (users/groups/computers) in Active Directory has ACL security permissions associated with it, and each object must allow the OpenDNS_Connector user account to read its attributes.

Note: This article assumes that the normal pre-requisites for the 'OpenDNS_Connector' account have already been checked. If AD Users/Groups are missing from the Dashboard please see this article first:
AD users/groups missing from Umbrella Dashboard.

Default permissions

By default all authenticated users can read the properties of users/groups/computers, so the OpenDNS_Connector user does not require any extra permissions to do the LDAP sync.

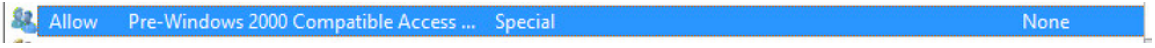
The *default permissions* are normally set as follows:

1) The 'Pre-Windows 2000 Compatible Access' group is assigned read (read all properties) permissions on the domain for 'Descendant User Objects', 'Descendant Group Objects' and 'Descendant Computer Objects'.

You can double-check this as follows:

- Open Active Directory Users and Computers
- Click on **'View'** and check the **'Advanced Features'** option.
- Right-click on the Domain object and select **'Properties'** then **'Security > Advanced'**

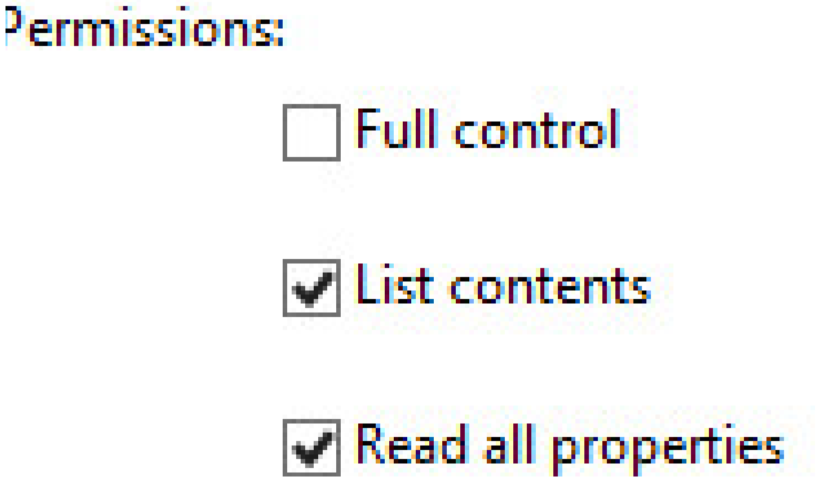
- Select the **'Pre Windows 2000 Compatible Access'** entry with **'Special'** permissions:



Allow Pre-Windows 2000 Compatible Access ... Special None

115011616667

- Click **'Edit'** to see these permissions in detail.
- Select **'Descendant User objects'** in the Applies to section
- Look for these permissions:



Permissions:

□ Full control

☑ List contents

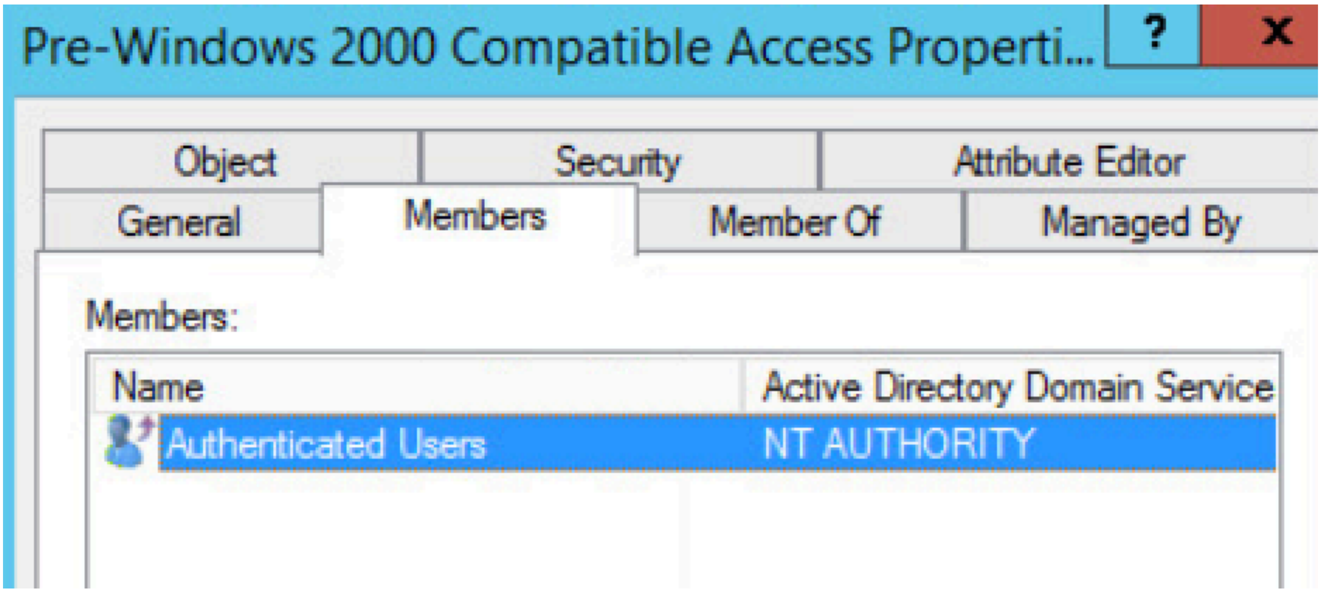
☑ Read all properties

115011616687

- Repeat these steps for **'Descendant Group objects'** and **'Descendant Computer objects'**

2) The All 'Authenticated Users' group is a member of **'Pre-Windows 2000 Compatible Access'** group which provides these settings to all users.

- Right-click on the **Pre-Windows 2000 Compatible Access** group, which is normally in the Builtin AD container.
- Select **'Properties'** and go to the **'Members'** tab.
- Check if **'Authenticated Users'** is listed.



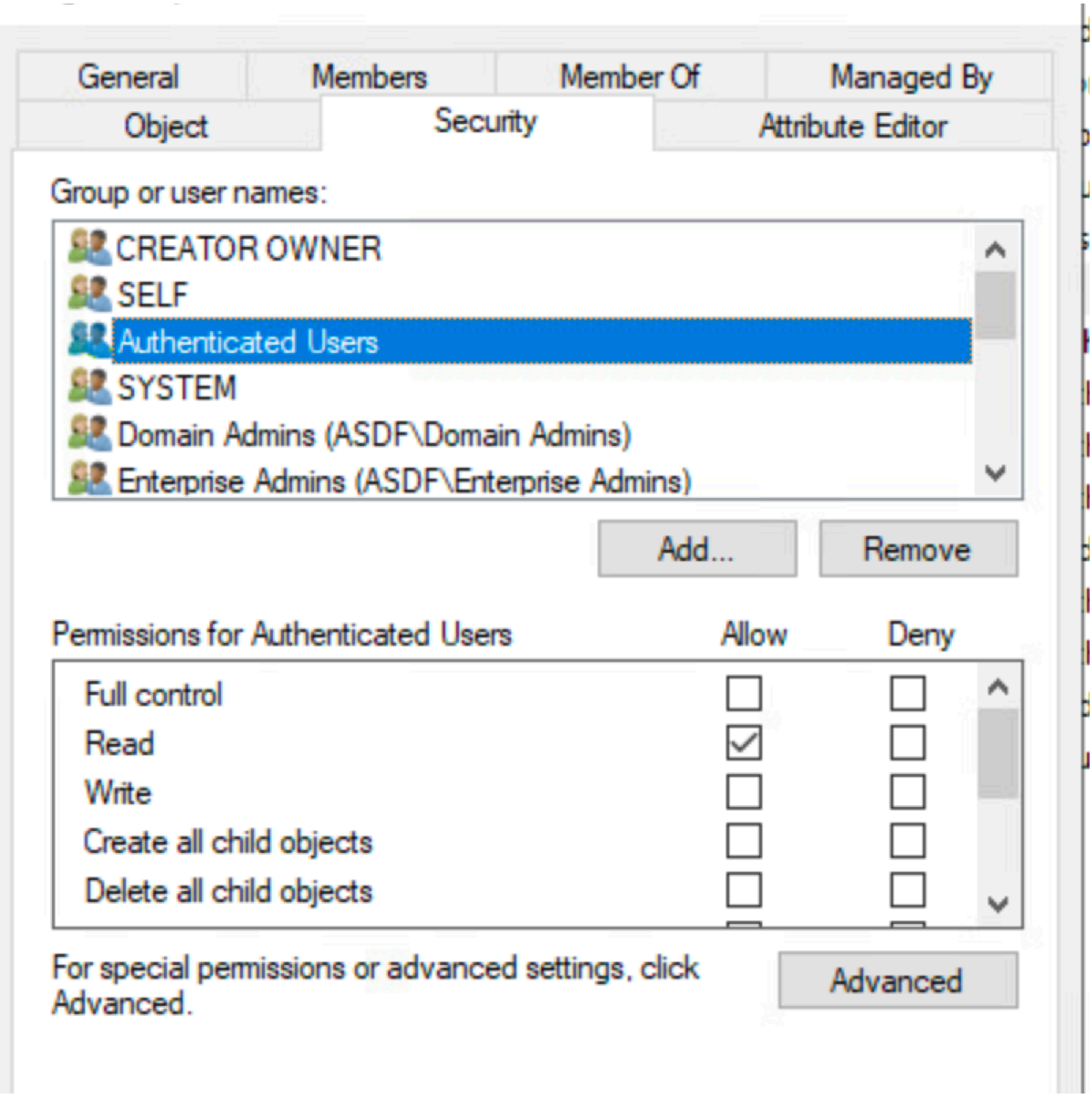
Members:

Name	Active Directory Domain Service
Authenticated Users	NT AUTHORITY

115011616707

However, in some AD environments this permissions model could have been changed and authenticated users have been removed. This could manifest itself as some users being missing from the Umbrella Dashboard, or group memberships being incorrect. If this is the case, add the OpenDNS_Connector user to this group, restart the connector service and the missing items show up in Umbrella.

In some Rare Cases this still does not address the issue. If you find this to be the case, check the groups security tab in active directory, make sure you see authenticated users listed here with a check in read access. If this is not checked, then check it off and restart the connector service to see if the group members show up. Additionally if they find this security setting missing from all groups they need to apply the changes to all groups globally in bulk.



Group or user names:

- CREATOR OWNER
- SELF
- Authenticated Users
- SYSTEM
- Domain Admins (ASDF\Domain Admins)
- Enterprise Admins (ASDF\Enterprise Admins)

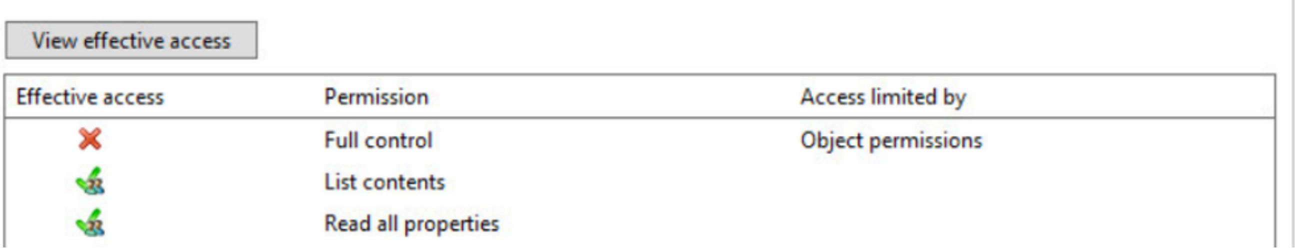
Permissions for Authenticated Users	Allow	Deny
Full control	□	□
Read	☑	□
Write	□	□
Create all child objects	□	□
Delete all child objects	□	□

For special permissions or advanced settings, click Advanced.

View effective access

You can use the Windows **'Effective Access'** tool to see if the OpenDNS_Connector user is able to read a particular object which is missing (or which has incorrect group membership).

- Open Active Directory Users and Computers
- Click on **'View'** and check the **'Advanced Features'** option.
- Find the user object and right-click to select **'Properties'**
- Go to the **'Security > Advanced > Effective Access'** (this can say **'Effective Permissions'**)
- Click on '**Select a user'** then select the **'OpenDNS_Connector'** user account.
- Click 'OK' then **'View Effective Access'**
- Make sure the connector user is able to **read all properties**:



Effective access	Permission	Access limited by
✗	Full control	Object permissions
✓	List contents	
✓	Read all properties	

115011616727

Setting OpenDNS_Connector LDAP permissions

The 'Delegate Control' wizard in AD is a quick way to assign the necessary permissions to the 'OpenDNS_Connector' user:

1) Go to Administrative Tools and open the Active Directory Users and Computers snap-in.
2) Right click on the domain that includes the OpenDNS_Connector and select "**Delegate Control...**", then click Next.
3) Add the **OpenDNS_Connector** user, then click Next.
4) Select "**Read all user information**" and click Next. [See picture 3.]
7) Click **Finish**. [See picture 6.]

Note: These steps can fail if inheritance is disabled on some objects. For those objects you need to set the permissions manually.

userPerms script

The attached powershell script is another method to get the permissions of a specific object (eg. user) in AD. Please include the output of this script when contacting Umbrella Technical support.