

How to Configure MSAD Authentication

<https://campus.barracuda.com/doc/96026646/>

Microsoft Active Directory (MSAD) is a directory service that allows authentication and authorization of network users. On the Barracuda CloudGen Firewall you can configure MSAD as an external authentication scheme. MSAD is included with all Windows Server operating systems as of the Windows 2000 Server. For MSAD authentication, you can also configure the Barracuda DC Agent, which allows transparent authentication monitoring with the Barracuda CloudGen Firewall and Microsoft® domain controllers. The MSAD authentication service can handle a maximum of 20 AD servers at a time. MSAD authentication fetches the user principal name (UPN) and returns it in the USER attribute field during authentication. The UPN is then applied to filtering and firewall rules. For attributes to match, e.g., in VPN client-to-site filtering, the UPN format in AD must be *user@domain.com*.

Before You Begin

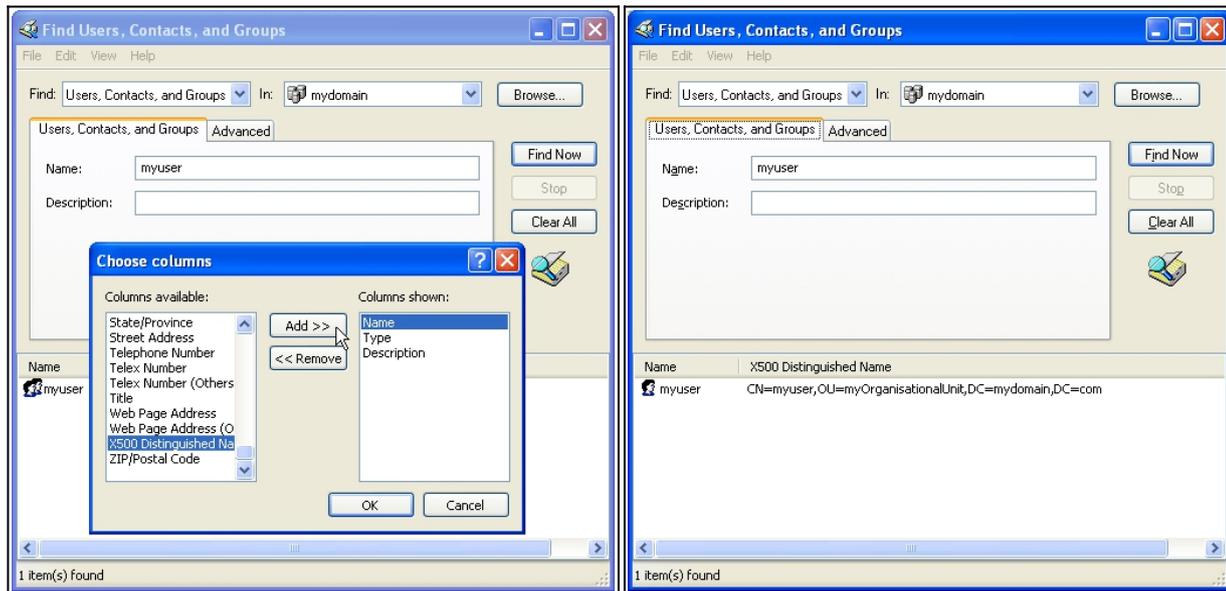
Deactivate Kerberos Pre-authentication

If MSAD is running in native mode on a Windows 2003 Server domain, you must deactivate Kerberos pre-authentication for each user.

Gather Group Information

To use services such [URL Filter](#), [VPN](#), or [Firewall Authentication and Guest Access](#), you might need to gather group information. The distinguished name (DN) containing the group information is needed for external authentication using MSAD and LDAP (see also [How to Configure LDAP Authentication](#)). To gather group information from MSAD:

1. Go to **My Network Places > Search Active Directory**.
2. Select the searching domain.
3. Enter the name of the user you are searching for and click **Find Now**.
4. After you have found the user, add the **X500 Distinguished Name** column.
 - Select **View > Choose columns**.
 - Select **X500 Distinguished Name**.
 - Click **Add**.

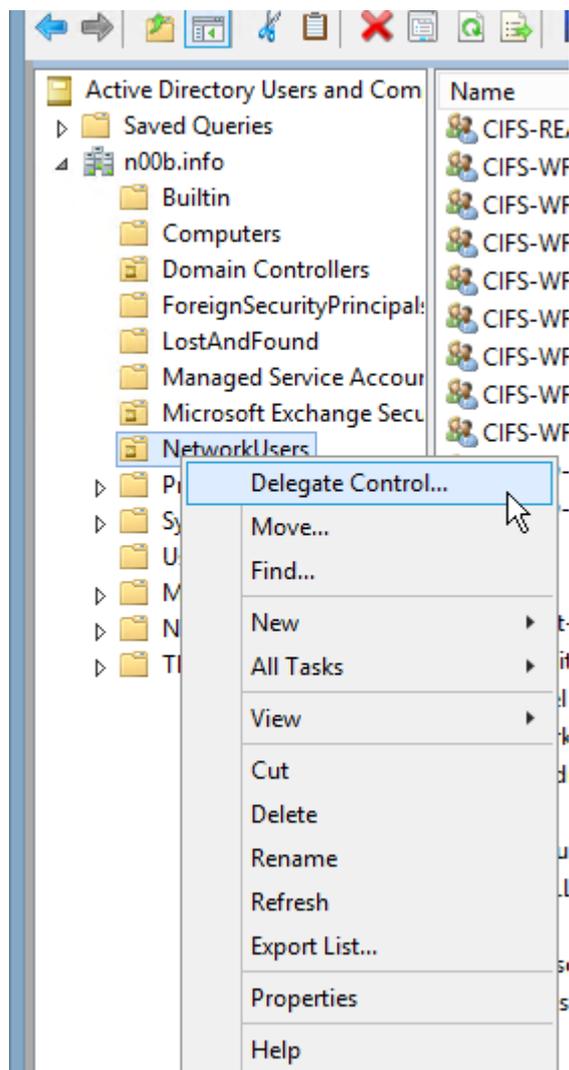


The DN is displayed in the search results.

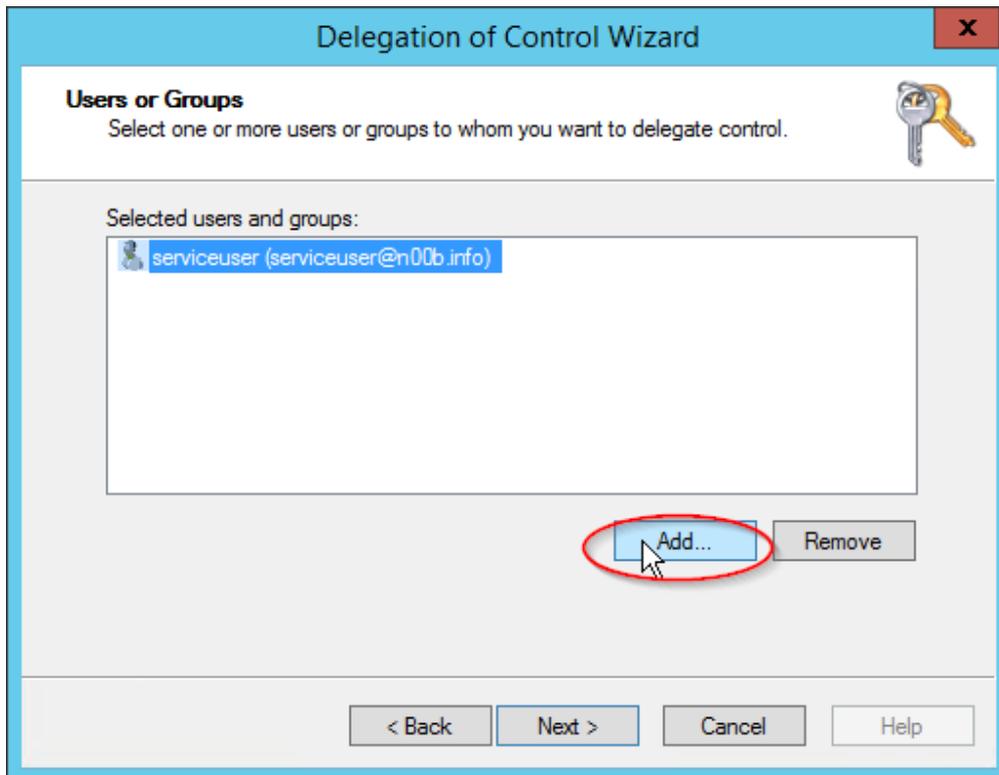
Delegate a Service User

You must delegate the 'serviceuser' to **Read all user information** in the specific OU:

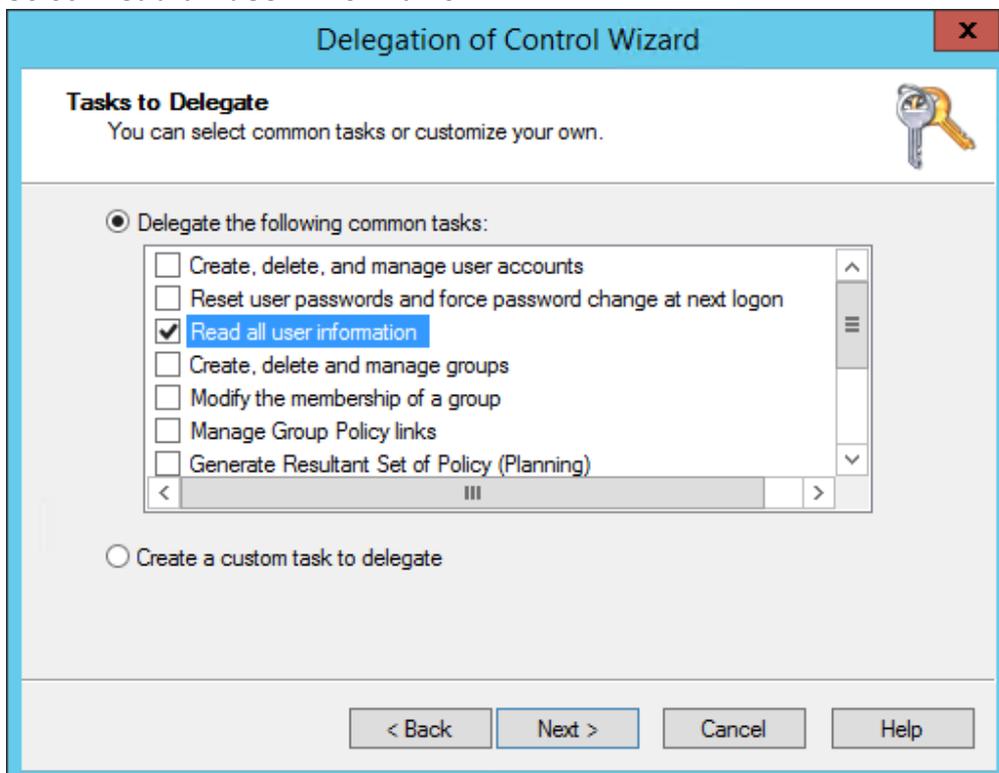
1. Select the OU: in this example **NetworkUsers**.
2. Select **Delegate Control**.



3. **Add** your 'serviceuser'.



4. Click **Next**.
5. Select **Read all user information**.



6. Click **Next**.
7. Click **Finish**.

Configure MSAD Authentication

1. Go to **CONFIGURATION > Configuration Tree > Box > Infrastructure Services > Authentication Service**.
2. In the left navigation pane, select **MSAD Authentication**.
3. Click **Lock**.
4. Enable MS Active Directory as external directory service.
5. In the **Basic** table, add an entry for the domain controller.
 - (optional) In case you want to provide MSAD-group access information to the HTTP proxy via MSCHAP, set **Use MSAD-groups with NTLM** to **Yes** in the **Basic** window.
6. Enter the name and IP address or hostname of the primary domain controller, without the domain suffix. Hostnames must be DNS-resolvable.
7. In the **Active Directory Searching User** field, enter the Distinguished Name (DN) of the 'serviceuser' (a user with permission to search the Active Directory and to view group information). For example: CN=username,OU=development,DC=domain,DC=local or: DOMAIN\username or: username@domain.local
8. In the **Active Directory Searching User Password** field, enter a password for the user with permission to search the Active Directory.

The password can consist of small and capital characters, numbers, and non-alphanumeric symbols, except the hash sign (#).
9. In the **Base DN** field, specify where to search for user information. Define the Base DN as specific as possible in order to increase the speed of the lookup and avoid timeouts.

If you enter the domain in this field (e.g.: DC=xyz,DC=com), Active Directory may refuse the Base DN lookup. If possible, add an OU= entry to your Base DN.
10. When using NTLM authentication, enable **Use MSAD-groups with NTLM** to periodically synchronize user groups from MSAD and let the Barracuda CloudGen Firewall handle them offline.
11. When using MSAD-groups with NTLM, enable **Cache MSAD-groups** to reduce network traffic and load on the MSAD server.

As opposed to online group retrieval, offline group caching, which performs nested group lookup, also fetches all group information for a user before applying filtering. Online group retrieval just reads up to 16k bytes of group information as a concatenated FQDN string. However, for both online group retrieval and offline group caching, after filtering users the group string is restricted and truncated to a max. of 8k bytes.
12. Use **Offline Sync [m]** to specify the interval of the synchronization in minutes of the offline database of the MSAD-groups, if enabled.

| Basic | |
|---------------------------------|---|
| Domain Controller Name | <input type="text" value="ad01"/> |
| Domain Controller IP | <input type="text" value="10.0.40.3"/> |
| Active Directory Searching User | <input type="text" value="CN=serviceuser,OU=NetworkUsers,DC=n00b,DC=info"/> |
| AD Searching User Password | Current <input type="password"/> |
| | New <input type="password" value="•••••"/> |
| | Confirm <input type="password" value="•••••"/> |
| | Strength <input type="text" value=""/> |
| Base DN | <input type="text" value="OU=NetworkUsers,DC=n00b,DC=info"/> |
| Use MSAD-groups with NTLM | <input type="text" value="Yes"/> |
| Cache MSAD-groups | <input type="text" value="Yes"/> |
| Offline Sync [m] | <input type="text" value="15"/> |

13. With **Timeout [s]** you can specify the timeout in seconds for requests to the MASD server.
14. To search additional LDAP attributes for mail addresses, enter a comma-separated list of LDAP attributes in the **Additional Mail Fields**.

Specify a comma-separated list of meta-directory field names that should also be searched for a mail address. Only LDAP attributes are allowed, no spaces and no GUI description fields. If you are not sure, use an LDAP browser. All additional fields are searched via a pattern search (prefixed * and suffixed *).

15. Select **Use SSL** when establishing the connection to the LDAP directory using SSL.

Using SSL is strongly recommended for Windows 10 servers in order to bypass security vulnerabilities related to LDAP channel binding on Active Directory domain controllers and LDAP signing.

For certificate verification to work, the LDAPS server name must be DNS resolvable. When using hostnames (recommended as used in certificates for SSL communication), you must create a host firewall rule to match the traffic because the dynamic network object is no longer pre-filled with the authentication server address. For more information, see [Host Firewall](#).
16. Select **Follow referrals** to search the MSAD global catalog and follow LDAP referrals. It is recommended to enable this setting.
17. Specify **Max. Hops for Referrals** to define the maximum number of LDAP referrals to be used.
18. Enable **Check Domain Name** to let your CloudGen Firewall additionally check the domain name of the user who tries to authenticate. This setting is recommended if you have more than one domain in your network.
19. Set **Add User-DN as Group name** to **yes** if you want to add the user distinguished name to the list of groups.

The group added to the list of groups does not need to exist. This setting allows you to enhance filtering.

20. Click **OK**.
21. If group information is queried from a different authentication scheme, select the scheme from the **User Info Helper Scheme** list.
22. In the **Group Filter Patterns** table, you can add patterns to filter group information from the directory service.
Example:
 - **Group Filter Pattern:** *SSL*
 - **User01:** CN=foo, OU=bar, DC=foo-bar, DC=foo
 - **User02:** CN=SSL VPN, DC=foo-bar, DC=fooIn this example, User01 does not have the *SSL* pattern in its group membership string and will not match in group-based limitations.
23. Click **OK**.
24. Click **Send Changes** and **Activate**.

MSAD Authentication through the Remote Management Tunnel

To allow remote CloudGen Firewalls to connect to the authentication server through the remote management tunnel, you must activate the outbound **BOX-AUTH-MGMT-NAT** host firewall rule. Per default this rule is disabled.

MSAD Authentication against Microsoft Entra ID

MSAD authentication against Microsoft Entra ID is possible when Entra ID is configured to use secure LDAP. Use the **Active Directory Searching User** and **Base DN** as supplied by Microsoft.

For more information, see the Microsoft article [Entra ID - Configure Secure LDAP](#).

Figures

1. add_col.png
2. col_inf.png
3. msad_user1.png
4. msad_user2.png
5. msad_user3.png
6. msad_conf.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.