How to Configure MSAD Authentication

https://campus.barracuda.com/doc/48202902/

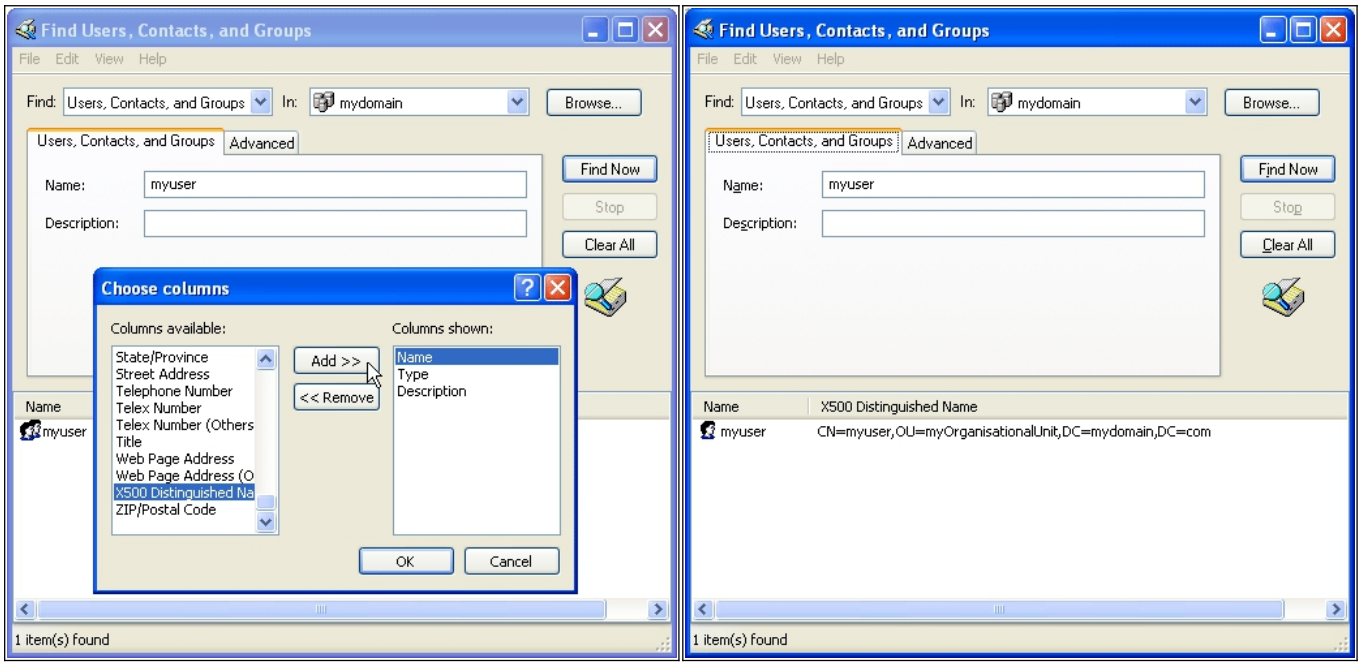
Microsoft Active Directory (MSAD) is a directory service that allows authentication and authorization of network users. On the Barracuda NextGen Firewall F-Series you can configure MSAD as an external authentication scheme. MSAD is included with all Windows Server operating systems since Windows 2000 Server. For MSAD authentication, you can also configure the Barracuda DC Agent, which allows transparent authentication monitoring with the Barracuda NextGen Firewall F-Series and Microsoft® domain controllers.

Before you begin

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

To use services such FTP, 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.

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.
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 / password** fields, enter the Distinguished Name (DN) and password of a user with permission to search the Active Directory and to view group information. For example: `CN=search,OU=development,DC=domain,DC=local`
8. 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 BaseDN lookup. If possible, add an OU= entry to your BaseDN.
9. When using NTLM authentication, enable **Use MSAD-groups with NTLM** to periodically synchronize user groups from MSAD and let the Barracuda NextGen Firewall F-Series handle them offline .
10. When using MSAD-groups with NTLM, enable **Cache MSAD-groups** to reduce network traffic and load on the MSAD server.
11. 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 (prepended * and appended *).

12. Select **Use SSL** when establishing the connection to the LDAP directory using SSL.
13. Select **Follow referrals** to search the MSAD global catalog and follow LDAP referrals.
14. Click **OK**.
15. If group information is queried from a different authentication scheme, select the scheme from the **User Info Helper Scheme** list.
16. 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=foo`

    In this example, User01 does not have the *SSL* pattern in its group membership string and will not match in group-based limitations.
17. Click **OK**.
18. Click **Send Changes** and **Activate**.

MSAD authentication through the remote management tunnel

To allow remote F-Series 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 Azure AD

MSAD authentication against an Azure AD is possible, when the Azure AD 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 Azure AD - Configure Secure LDAP.

Figures

1. add_col.png
2. col_inf.png