How to Configure MSAD DC Client Authentication

https://campus.barracuda.com/doc/79463354/

The Barracuda DC Agent is the connector between various Barracuda Networks products and Microsoft domain controllers to transparently monitor user authentication. You can install the Barracuda DC Agent either on the domain controller or on a dedicated Windows PC on the office network. The Barracuda DC Agent periodically checks the domain controller for login events and to obtain a record of authenticated users. The IP addresses of authenticated users are mapped to their username and group context. The list of authenticated users is provided to the firewall, allowing true single sign-on capabilities.

Before You Begin

Before you configure MSAD DC Client authentication, you must install the Barracuda DC Agent on the Microsoft Active Directory server.

For more information, see Barracuda DC Agent for User Authentication.

Configure the MSAD DC Client

Configure MSAD DC Client settings on the Barracuda CloudGen Firewall:

1. Go to **CONFIGURATION > Configuration Tree > Box > Infrastructure Services > Authentication Service**.
2. In the left menu, click **MSAD DC Client**.
3. Click **Lock**.
4. Set **Activate Scheme** to **Yes**.
5. Set **Auto Logout After** to the number of hours after which a user is automatically logged out. If the client receives the IP address via DHCP, sync this value with the DHCP lease timeout.
6. In the **Server Setting** table, add all Microsoft Active Directory servers running the Barracuda DC Agent.
7. For each entry, specify the **IP Address** of the Active Directory server running the DC Agent.
8. Enter the **TCP Port** of the Active Directory server running the DC Agent (default: port 5049).
9. If group information is queried from a different authentication scheme, select the scheme from the **User Info Helper Scheme** list.
10. Click **OK**.
11. 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.
12. Click **Send Changes** and **Activate**.

Remove the User from the User Database

On the **FIREWALL > Users** page, right-click on the user and click **Logout Selected**. The user must now re-authenticate on the domain controller, for example, by accessing a network share or by logging into his/her workstation.

Figures

1. dc_client_auth.gif