
How to Configure MSAD DC Client Authentication

<https://campus.barracuda.com/doc/72516164/>

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.

Do not install the Barracuda DC Agent on Windows server domain controllers that are configured to use NTLM.

For more information, see [Barracuda DC Agent for User Authentication](#).

Configure the MSAD DC Client

Configure the CloudGen Firewall to communicate with the Barracuda DC Agent and specify the domain controllers where the Barracuda DC Agent is installed.

1. Go to **USERS > External Authentication**.
2. Click the **DC Agent** tab.
3. Set **Enable Single Sign-On** to **Yes**.
4. In the **Domain Controller IP** field, enter the IP address of the domain controller running the DC Agent. The CloudGen Firewall polls the DC Agent to obtain the list of users authenticated against this domain controller.
5. Enter the **DC Agent Listening Port**. Default: 5049.
6. In the **Synchronization Interval** field, specify the time interval in seconds at which the firewall should poll the DC Agent for the list of authenticated users. The recommended value is 15 seconds.
7. Click **Add**.
8. Enter the username in the **Exempt User Name** field to exclude specific domain users. You can use Perl-compatible regular expression (PCRE) pattern-matching notation, such as `\w` for any alphanumeric character or `\W` for any non-alphanumeric character.
9. Click **Add**.

DC Agent | TS Agent | Active Directory | NTLM | LDAP | RADIUS | Wi-Fi

Enable Single Sign-On: Yes No
Enable to provide Single Sign-On for authenticated LDAP domain users. Applicable for

Auto Logout After: hours
Timeout for automated logout. 0 disables automated logout. Default: 24

Domain Controller IP	DC Agent Listening Port	Synchronization Interval	
	5049	5	Add
10.0.10.11	5049	15	

DC Agent Listening Port. Default: 5049
Synchronization Interval. Default: 15

Exempt Group

Add

Specify exempted groups, all the users belonging to will be treated as unauthenticated for policies, logs and reports.

Remove the User from the User Database

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

Figures

1. dc-agent.gif
2. dc_user.png

© Barracuda Networks Inc., 2019 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.