

How to Configure Additional Authentication Schemes

<https://campus.barracuda.com/doc/79463365/>

On the Barracuda CloudGen Firewall, you can introduce additional authentication schemes, for example, to configure a second proxy server in your network with an alternative authentication server. There is no limit to the number of authentication schemes that you can add.

References to additional schemes are not checked for integrity. Keep in mind that schemes may be deleted even though they are used by VPN users.

Configure an Additional Authentication Scheme

1. Go to **CONFIGURATION > Configuration Tree > Box > Infrastructure Services > Authentication Service**.
2. Click **Lock**.
3. In the left menu, click **Additional Schemes**.
4. In the **Schemes** section, click **+** to add an entry for the additional authentication scheme.
5. Enter a **Name** for the additional authentication scheme.
6. Enable the scheme to start the authentication processes.
7. Select the scheme from the **Method** list.
8. Configure the settings applicable to the selected scheme:
 - o **MSNT Settings** – For information on the settings in this section, see [How to Configure MSNT Authentication](#).
 - o **MSAD Settings** – For information on the settings in this section, see [How to Configure MSAD Authentication](#).
 - o **RADIUS Settings** – For information on the settings in this section, see [How to Configure RADIUS Authentication](#).
 - o **LDAP Settings** – For information on the settings in this section, see [How to Configure LDAP Authentication](#).
 - o **RSA-ACE Settings** – For information on the settings in this section, see [How to Configure RSA-ACE SecurID Authentication](#).
 - o **CloudGen Firewall Local Authentication Settings** – For information on the settings in this section, see: [How to Configure NGF Local Authentication](#).
 - o **TACACS+ Settings** – For information on the settings in this section, see [How to Configure TACACS+ Authentication](#).
 - o **OSCP Settings** – For information on the settings in this section, see [How to Configure OSCP Validation](#).
9. In the **Filter Settings** section, select the scheme from the **User Info Helper Scheme** list if group information is queried from a different authentication scheme. For example, select **LDAP** if RADIUS is used for identity verification but group information must be queried from an LDAP directory.

10. 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.

11. Click **OK**.

12. Click **Send Changes** and **Activate**.

© 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.