

How to Configure RADIUS Authentication

<https://campus.barracuda.com/doc/53248691/>

Remote Access Dial-In User Service (RADIUS) is a networking protocol providing authentication, authorization, and accounting. The Barracuda NextGen Firewall F-Series can use RADIUS authentication for IPsec, Client-to-Site, and SSL VPN.

Before You Begin

When using RADIUS for OTP authentication (eg., LinOTP, privacyIDEA) you must enable the option **Always use Session Password** in the NextGen Admin **Client Settings**, otherwise authentication will fail. For more information, see [NextGen Admin Settings](#).

Configure RADIUS Authentication

To configure RADIUS for external authentication with the Barracuda NextGen Firewall F-Series,

1. Go to **CONFIGURATION > Configuration Tree > Box > Infrastructure Services > Authentication Service**.
2. In the left navigation pane, select **RADIUS Authentication**.
3. Click **Lock**.
4. From the **Configuration Mode** menu on the left, select **Advanced View**.
5. Enable RADIUS as external directory service.
6. In the **Radius Server Address / Port** fields, enter the IP address and port of the RADIUS server (default: port 1812).
7. In the **Radius Server Key** section, define the pre-shared secret to authorize requests.
The pre-shared secret can consist of small and capital characters, numbers, and non alpha-numeric symbols, except backslashes and the hash sign (#).
8. From the **Group Attribute Delimiter** list, you can select how groups are delimited in a list. To explicitly specify a delimiter character, select the **Other** checkbox and enter the character in the **Group Attribute Delimiter** field.
9. From the **Group Attribute Usage** list, you can select the group information that is used (e.g.: CN=..., OU=..., DC=...). You can select:
 - **All** (default) – Complete string
 - **First** – Only the first group
 - **Last** – Only the last group
10. If group information is queried from a different authentication scheme, select the scheme from the **User Info Helper Scheme** list.
11. Enter the NAS identifier, IP address, and port if your RADIUS servers requires you to set NAS credentials.

12. Enable **OTP preserves State** if a One-Time Password server (e.g., Symantec VIP Enterprise Gateway 9.0) requires the RADIUS response to contain the 'State' attribute.
13. Click **Send Changes** and **Activate**.

RADIUS 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. By default, this rule is disabled.

© 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.