
How to Configure Wi-Fi Access Point Authentication

<https://campus.barracuda.com/doc/46205802/>

Configure Wi-Fi Access Point authentication for the Barracuda NextGen Firewall X-Series to be able to use the authentication information contained in the syslog stream of supported Wi-Fi access points.

Supported Wi-Fi Access Points

- Aerohive (login and logout)
- Ruckus (login and logout)
- Aruba (login only)

Before You Begin

To authenticate connecting users, you must enable syslog streaming on the access point. For more information, see:

- [Wi-Fi AP Authentication Aerohive Configuration](#)
- [Wi-Fi AP Authentication Ruckus Wireless Configuration](#)
- [Wi-Fi AP Authentication Aruba Configuration](#)

Configure Wi-Fi Access Point Authentication

1. Go to the **USERS > External Authentication** page.
2. Click the **Wi-Fi** tab.
3. Select **Enable Wi-Fi Access Point Authentication** to enable integration with Wi-Fi.
4. In the **Auto Logout After** file, enter the timeout in hours. Enter 0 to disable the timeout.
5. Click **Add** to add a Wi-Fi endpoint. The **Add External Authentication Wi-Fi AP Endpoint** window opens.
6. In the **IP/Subnet** field, enter the IP address or network for your Wi-Fi access point. E.g., 10.0.33.1 or 10.0.33.0/24
7. Select the **Protocol** used by the Wi-Fi access point to send the syslog.
8. (SSL only) Enter the Subject Alternative Name of the SSL certificate.
9. (SSL only) Select the SSL certificate from the dropdown. You can upload or create certificates using the Certificate Manager. For more information, see [How to Use and Manage Certificates with the Certificate Manager](#).
10. Select the manufacturer of your Wi-Fi access point from the **AP Model** dropdown.
11. Click **Save**.
12. Depending on the protocols used by the Wi-Fi AP endpoints, enter the **UDP, TCP, or SSL Listen Ports**.


AUTHENTICATION SERVICES

DC Agent TS Agent Active Directory NTLM LDAP RADIUS **Wi-Fi** OCSF

Enable Wi-Fi Access Point Authentication: Yes No
Enable Terminal Server Agent service as external directory service. Default: No

Auto Logout After: hours
Timeout in hours for automated logout. Default: 0 (disabled).

Wi-Fi AP Endpoints:

Source IP	Protocol	SubAltName	AP Model	Action
172 . 16 . 0 . 233	SSL	test	Aerohive	Edit 

UDP Listen Port:

TCP Listen Port:

SSL Listen Port:

13. Click **Save**.

Wi-Fi Access Point authentication is now configured and can be used for wireless connections.

Figures

1. wifi_ap_01.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.