



## District managed systems that can directly impact ENA Air Wi-Fi functionality.

If a large number of users within your network begin experiencing issues related to your ENA Air Wi-Fi service, there are some common systems that may be impacting your overall wireless and wired LAN performance.

**DHCP:** Each wireless device on your ENA Air Wi-Fi network will obtain one IP address, which it will retain on each access point (AP) with which it interacts regardless of the client's location within the site or building. Essentially, the device should never change its IP address even if it's roaming across multiple APs unless the DHCP lease timer has expired. If devices are changing IP addresses, please check the following:

- Verify the DHCP server is operational (i.e., responding), the scope for the wireless VLAN has been configured properly, and the DHCP leases have been logged by the server.
- Verify if the DHCP scope is oversubscribed for the network or wireless VLAN.
- It is recommended that DHCP lease timers be set within 8–24 hours on wireless networks. Verify your DHCP lease timers and adjust accordingly. Very short lease times will induce more DHCP network traffic, but long lease timers can induce oversubscription.
- Verify if the DHCP server logs contain errors. If they do, note the time stamps, and then correlate the DHCP logs with the incident date/time. Specifically look for errors that relate to duplicate IPs (e.g., IP address contention) or IP fragmentation errors (e.g., datagram reassembly).
- If duplicate IP addresses are detected, check for rogue DHCP servers (e.g., consumer routers that may have been brought into the facility by a staff member).

**Network & Firewall:** Your district's Internet access, WAN, and firewall are assessed and reviewed prior to the installation of ENA Air. As with any Wi-Fi/LAN service, these services can impact your ENA Air network in various ways. If you begin experiencing issues, please verify the following:

- Verify if the local LAN is experiencing a LAN loop or broadcast storms.
- Verify if the local LAN switch ports are properly configured to support the wireless VLANs.
- Verify if the aggregate WAN ingress is experiencing any saturation issues.
- Verify if the Internet access for the district is experiencing any saturation issues.
- Verify if any recent firewall or content filtering changes have been made on the network. If they have been, reverse those changes and verify if the issues remain.
- Verify if any switch ports connected to APs, inter-switch links, or routers are down or have errors.

**DNS:** Wireless devices will use your local DNS to complete name resolution unless DNS settings are statically set on the device. Should devices experience name resolution issues (e.g., timeouts or page not available errors), please check the following:

- Try to browse via the webpage's IP address instead of its URL.
- Verify the DNS servers are up and operational, especially the primary/authoritative DNS servers.
- Verify if users can access webpages when using an alternate DNS (e.g., Google's DNS is 8.8.8.8 and 8.8.4.4). This requires the firewall to allow outbound UDP and TCP 53 connections on the wireless VLAN.
- Verify the local DNS server is capable of resolving to an alternate DNS server for assistance with queries. This typically is an external DNS server (i.e., ISP DNS) that resolves queries the local server cannot resolve. If it is capable, verify you can reach that external DNS server.
- Verify the DNS server logs for errors. If there are errors, note the time stamps, and then correlate the DNS logs with the wincident date/time.

**RADIUS or Active Directory (AD):** Wireless devices may use your local RADIUS or AD server for authentication, authorization, and accounting. Should devices experience issues authenticating or accessing network content/resources, please check the following.

- Verify the user account within RADIUS and validate the privileges assigned or associated with the user.
- Verify the user account is not disabled due to excessive failed authentication attempts.
- Verify the RADIUS server is properly configured for the EAP authentication methods required.
- Verify the RADIUS server certificate has not expired.
- Verify the RADIUS server and client have the correct system date/time, since many certificate-related checks require accurate time.
- Verify the RADIUS server logs for errors. If there are errors, note the time stamps, and then correlate RADIUS logs with the incident date/time.
- Verify the wireless AP and RADIUS server have been configured with the same shared secret.
- Verify that excessive latency doesn't exist between the wireless AP and RADIUS server across a WAN link, which can cause authentication delays and timeouts.
- Verify the user account within AD and validate the privileges assigned or associated with the user.
- Review the AD server logs for errors and note the time stamps to correlate AD logs with the connectivity incident date/time.

Visit [help.ena.com](http://help.ena.com) to access help documentation and tutorials for ENA Air on the **ENA Help Center**.

### CONTACT US TODAY!

For more information about ENA Air, contact your ENA account service manager or visit our website at [www.ena.com](http://www.ena.com).

General Inquiries: 866-615-1101 | [info@ena.com](mailto:info@ena.com)

ENACTAC 888-612-2880 | [support@ena.com](mailto:support@ena.com)



Education Networks of America