Sage Alerting Systems
Regarding EAS equipment access rules, FCC 26-38

The FCC has issued a Report and Order that requires changes in how EAS equipment is accessed. While this document provides guidance on implementing the password portion of these rules, it is not a replacement for the official regulations. You should read and understand the Report and Order portion of this document: https://docs.fcc.gov/public/attachments/FCC-26-38A1.pdf

The specific rules changes are noted in Appendix A of the FCC R&O. The rules take effect 60 days after their publication in the Federal Register. The rules are part of good cybersecurity practices and there is no reason to wait 60 days to start implementing the new requirements in the Report and Order.

The best practices now required by the FCC for EAS can also be followed for any other aspect of your business, including access to other elements of your broadcast chain.

This document assumes that your ENDEC is on at least Rev 96 of the ENDEC software. Older versions of the software are **not** compliant with the 2023 FCC rules, such as CAP priority, and do not contain current FEMA validation certificates.

The FCC has three categories in its new rules: passwords, updates, and network access. Our comments and suggestions are below.

Passwords

- Have strong passwords of at least 15 characters – the ENDEC allows up to 20.
- Strong passwords are usually defined as a combination of upper and lower case letters, digits, and special characters. Note that there is currently a problem with using the ampersand (&) and plus (+) keys, do not use these on the ENDEC. This will be corrected in an upcoming release. As long as you avoid using those characters, you can create strong passwords for the ENDEC.
- Change your password if you think it has been compromised. Sage also recommends that you change the password when an authorized user leaves your company. The ENDEC supports role-based user IDs for easier management. We recommend you configure a separate account and password for each user.
- Do not use the same password for other equipment or services.
- Do not use dictionary words, call signs, user names, frequencies, or station branding in your password. Avoid reusing passwords across different services. There are techniques for choosing a password that is memorable but not easily guessable. Search online for them.
- Sage recommends that you never use HTTP to access the ENDEC remotely, especially when building new users and changing passwords. You can disable HTTP by using the Menu > Network > Disable HTTP menu on the front panel, or the “Disable HTTP” check box on ENDECSetD. Make

sure you have HTTPS access to your ENDEC before you disable HTTP. Also, see the section below on Server Certificates.

- Note that the ENDEC will not allow you to use its “call sign” or the “user name” as part of your password.
- If you lock yourself out of your ENDEC when changing passwords, you can reset users and passwords from the front panel, Menu > Network > Reset Web Users. This will reset only the user names and passwords to the factory defaults. The ENDEC will remind you at login that one or more of your user/password accounts is using default credentials. The new FCC rules require that you change the password and not use the factory defaults.

Updates

- Install security updates promptly.
- You can sign up for email notifications at https://www.sagealertingsystems.com/support.htm

Firewalls

- The FCC says “Use a network firewall or comparable network segmentation practice that limits remote management access to authorized devices and authorized users.”
- Do not allow uncontrolled access to the ENDEC, or any other part of your broadcast equipment. Use a VPN, a firewall with an appropriate set of rules, or a variety of other network protections.
- The ENDEC has a setting to add additional login access restrictions. This allows you to specify a list of addresses or subnets that can log in to the ENDEC with a browser. Using a web browser, access the ENDEC, click the “Access Control” button, then select “Computers” from the selection box and add your list. If you lock yourself out, you can clear the list at the front panel, with Menu > Network > Reset Whitelist.

Server Certificates

HTTPS uses a server certificate to allow your browser to make sure that the server (in this case, the ENDEC), is the expected device. ENDEC has its own webserver TLS (sometimes called SSL) certificate that is used to authenticate and encrypt communication via HTTPS between your browser and the ENDEC. The built-in default certificate provides adequate encryption, but because it is self-signed, your browser will display a variety of different warnings about it.

To eliminate browser warnings about the default certificate, you can use the Certificates page to create a custom server certificate set to the IP address(es) that you use to access the ENDEC. This certificate will be self-signed, so you will need to manually add it to the trusted root store in your PC. Because the process varies by browser and operating system, we recommend searching for "install self-signed certificates for [your browser]" for specific instructions.

In corporate or university environments, you can upload a valid certificate and intermediates signed by a CA that your computer is already configured to trust.

Once you have tested HTTPS access to your ENDEC, you can disable HTTP from the front panel (Menu > Network > Disable HTTP), or the “Disable HTTP” check box on ENDECSetD.

Sage is currently developing a step-by-step guide for common browsers, which will be posted to our FAQ page in the near future.