

---

# REDLINE

## TAKING THINGS TO THE NEXT LEVEL

---



We're pleased to announce that Redline has received full FIPS (Federal Information Processing Standard) 140-2 Level 2 certification for the following RDL-3000 products:

- Ellipse
- Edge
- Elte-MT

The FIPS Publication 140-2, is a U.S. government

computer security standard used to validate cryptographic modules. Redline has been awarded certificate **#2636** which includes both hardware and software components. To operate in a FIPS-compliant mode, a Redline radio requires:

- RDL-3000 Software v3.1
- A FIPS-enabled option key
- An ECDSA (Elliptic Curve Digital Signature Algorithm) certificate.

### CERTIFIED — NOT JUST COMPLIANT

Certification is an important factor to consider when selecting any networking gear that will be used to create secure communications environments. A product can be compliant — meaning that the manufacturer believes that the product meets the requirements, or it can be certified — meaning that the manufacturer had the product independently tested by a third party to a set of security requirements.

The FIPS 140-2 publication is a joint effort by the United States' National Institute of Standards and Technology (NIST), and the Communications Security Establishment (CSEC) for the Canadian government. FIPS 140-2 describes the requirements to ensure secure transmission of classified information and services over a network. The process of achieving FIPS 140-2 certification is managed through the Cryptographic Module Validation Program (CMVP), headed by NIST. Products must undergo a set of rigorous tests to certify that modules meet FIPS 140-2 standards. This process provides a stringent third-party guarantee of FIPS 140-2 compliance and gives the buyer assurance that they are getting the security for which they paid. Additionally, FIPS 140-2 certification is a mandatory security requirement for all US and Canadian Federal government agency purchases,

including the military.

Not only was Redline one of the first vendors to achieve FIPS 140-2 certification for broadband wireless systems, but Redline has included built-in security features in our products that go above and beyond what's required for certification.

### SECURITY FOR YOUR WIRELESS SYSTEM

The shared nature of wireless systems and deployment scenarios can leave broadband wireless systems vulnerable to a variety of malicious attacks if security measures are not given priority in the network planning stage. Advance planning is crucial as it is extremely difficult to apply patch solutions to a deployed product and achieve the level of protection necessary for defending against these attacks.

Successful broadband wireless security implementations depend on:

- Selecting manufacturers who have considered security measures early in the product design phase.
- Working with vendors who have a track record of architecting and deploying secure broadband wireless networks.