Security Certifications for IoT Devices

AFFINITY IoT SECURITY LABS
CERTIFIED SECURE

DISTINGUISH YOUR PRODUCTS
with an Independent Security Lab Evaluation

Gain a Competitive Advantage through Certification

Open Standard Evaluation Criteria
(see other side)

Static and Dynamic Evaluation available

PERMANENTLY PUBLISH
Product Security Certifications on the Web

Demonstrate your commitment to security

Leverage security features in your marketing collateral

Provide instant access to evaluation results on packaging

YOUR CLIENTS NEED

Secure products but are not security experts

WE PROVIDE

Assurance through open, independent, and objective product evaluation

Comprehensive evaluation across 20 different criteria

YOU RECEIVE product-specific

Security Rating Graphics ready for marketing

Security Rating Certificate

Permanent Evaluation web page

AFFINITY IoT SECURITY LABS
CERTIFIED SECURE

"Affinity IoT Security Labs provides our customers with the assurance that our products contain the right set of features for secure deployment."

-- IoT Product Manager

"Security Certification provides a cost-effective way to differentiate our product line in a competitive marketplace."

-- IoT Marketing Rep

COSTS:*

Static Evaluation:
$995 + expenses

Dynamic Evaluation:
$1,995 + expenses

***Contract Required**

Show your customers your commitment to security –
Contact us today to register your products for Security Certification!

Evaluation Criteria for Security Certification

Affinity IoT Security Labs is an independent laboratory that evaluates interconnectable products and certifies them exclusively in regards to the following specific categories and criteria. Static evaluation relies on documentary evidence, whereas Dynamic evaluation relies on testing the product/device. Dynamic criteria are always negative during Static evaluation.

Critical Criteria	**Static/Dynamic**
1. Does the product require a login to access administrative features?	S
2. Does the product enforce strong password requirements?	S
3. Is it possible to easily update the product software?	S
4. Does the product support automated software updates?	S
5. Does the product validate and reject unacceptable inputs?	D
6. Does the product support secure administrative access?	S
7. Does the product fail safely?	D
Important Criteria	
8. Does the product feature anti-robot brute-force protection?	D
9. Does the product support multi-factor authentication?	S
10. Does the product allow administrative accounts to be created?	S
11. Does the product allow the default administrative accounts to be removed/disabled?	S
12. Does the product encrypt the information that it stores?	S
13. Does the product encrypt its communications with other devices?	S
14. Does the product authenticate other devices and components it interacts with?	S
15. Does the product authenticate the update server?	S
16. Does the product fully redact its make, model, and software version in non-admin comms?	D
17. Does the product securely log access events?	D
Valuable Criteria	
18. Does the product verify downloaded software updates via digital signature?	S
19. Does the product feature any DoS resistance features?	D
20. Does the product resist physical tampering?	D

Security Score

The security score is calculated by aggregating the sum of positive answers, weighted by category:

- Critical Criteria: 5 points
- Important Criteria: 2 points
- Valuable Criteria: 1 point

The resulting aggregate score is divided by the maximum possible score of 58, multiplied by 10, and rounded to the nearest integer, producing an integer score in the range of 0-10.

Security Rating

The Security Rating is based on the Security Score as follows: