Table of Contents

The Anti-Virus Certification Criteria Overview................................................................. 1
Desktop/Server Overview......................................................................................................... 1
Desktop/Server Requirements ................................................................................................. 1
  Anti-Virus Testing .................................................................................................................. 1
  Administrative Functions ....................................................................................................... 2
  Logging .................................................................................................................................. 2
The Anti-Virus Certification Criteria Overview

Products and services certified by the ICSA Labs Anti-Virus Product Certification program are able to prevent the end user from becoming infected by in-the-wild and other computer malware. The Anti-Virus Certification Criteria is geared for products and services that detect computer malware prior to causing an infection. The requirements comprising the criteria are intended to ensure the proper detection of computer malware before doing any damage to the host system.

The Anti-Virus Certification Criteria consists of primary and secondary modules, an addendum, and a glossary. To attain ICSA Labs Anti-Virus Certification, the Certification Candidate must completely satisfy all requirements in one of the primary modules. Testing against a secondary module, such as the Cleaning module, is optional. The Anti-Virus Certification Test Suites Matrix contains a matrix that the primary modules refer to. Finally, the Glossary module, which does not contain requirements, has definitions for terms appearing in the primary and secondary criteria modules as well as in the addendum.

The primary modules are identified by the type of anti-virus product or service being tested and are chosen by the vendor-customer prior to submitting their product or service for testing. The primary modules correspond to a particular type of anti-virus product or service: Desktop/Server, Gateway, Groupware, or Managed Services – ASP. There is currently one secondary module, called the Cleaning module. As with choosing a primary module, testing against the secondary module is elected by the vendor-customer prior to submitting their product or service for testing.

Desktop/Server Overview

This module is targeted at Anti-Virus products designed to protect individual desktops, laptops, and/or servers of residential users and organizations from malicious code infection. The Anti-Malware software and current product updates are installed and maintained on individual desktops, laptops, and servers. Anti-Virus products satisfying the requirements in this module have the capability to:

- Detect malware on-demand;
- Detect and prevent the replication of viruses on-access;
- Report no false positives;
- Log the results of malware detection attempts;
- Perform necessary administrative functions.

Desktop/Server Requirements

Anti-Virus Testing

- AN1 – On-Demand Detection – While in its Default Configuration, the Certification Candidate must demonstrate through On-Demand testing that it Detects Malware according to the Anti-Virus Certification Test Suites Matrix for Desktop/Server Certification Candidates.
Anti-Virus Desktop / Server Detection Certification
Criteria Version 4.1

- AN2 – On-Access Detection – While in its Default Configuration, the Certification Candidate must demonstrate through On-Access testing that it Detects Malware according to the Anti-Virus Certification Test Suites Matrix for Desktop/Server Certification Candidates.

- AN3 – On-Access Replication Prevention – While in its Default Configuration, the Certification Candidate must demonstrate through On-Access testing in accordance with the Anti-Virus Certification Test Suites Matrix for Desktop/Server Certification Candidates that it prevents the execution and replication of Malware.

- AN4 – No False Positives – While in its Default Configuration, the Certification Candidate must demonstrate through testing that no Entity is falsely identified as containing malware.

- AN5 – Administrative Functions Testing – The Certification Candidate must demonstrate through testing that its Administrative Functions work properly at all times regardless of the how the Certification Candidate is configured.

Administrative Functions
- AD1 – Administrative Interface – The Certification Candidate must include an Administrative Interface from which the Administrative Functions are accessible.

- AD2 – Administrative Functions – The Certification Candidate must include Administrative Functions to:
  A. Enable and disable the Detection of Malware;
  B. Retrieve and apply the latest Engine and Signatures over the Internet;
  C. Review Required Log Data.

Logging
- LO1 – Malware Detection Required Log Events – The Certification Candidate must have the capability to log the results of all Malware Detections.

- LO2 – Required Log Data – All Required Log Events must include all resulting actions taken in a Log.

- LO3 – Log Data Presentation – All Required Log Data presented in a Log must be presented in a human readable format.
Refer to the Anti-Virus Certification Test Suites Matrix which maps Certification Candidate types to the Malware collections they must be tested against for detection and cleaning testing.

ii Same as i.

iii Same as i.

iv Refer to LO2 in this module.

v Refer to LO1 in this module and, when applicable, to LO4 in the Cleaning Module.

vi Same as iv.