National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Common Criteria Evaluation and Validation Scheme
Validation Report

U. S. Government Protection Profile Anti-Virus Applications for Workstations In Basic Robustness Environments, Version 1.0

Report Number: CCEVS-VR-05-0090
Dated: 10 February 2005
Version 1.1

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validator

James Brosey
Tom Murphy
Mitretek Systems
3150 Fairview Park Drive South
Falls Church, Virginia 22042

Common Criteria Testing Laboratory

Evaluation Team
COACT, Inc
Rivers Ninety Five
9140 Guilford Road, Suite G
Columbia, MD 21046-2587

TABLE OF CONTENTS

1. EXECUTIVE SUMMARY

This report documents the NIAP Validators' assessment of the CCEVS evaluation of the Basic Robustness Anti-Virus Protection Profile, version 1.0. It presents the evaluation results, their justifications, and the conformance result.

The evaluation of the U. S. Government Protection Profile Anti-Virus Applications for Workstations in Basic Robustness Environments, Version 1.0, was performed by COACT, Inc., CAFÉ Lab CCTL in the United States and was completed on 7 January 2005. The Protection Profile (PP) identified in this Validation Report has been evaluated at an accredited testing laboratory using the Common Methodology for IT Security Evaluation (Version 2.2) for conformance to the APE requirements of the Common Criteria for IT Security Evaluation (Version 2.2).

This Validation Report applies only to the specific version of the PP as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced. The information contained in this Validation Report is not an endorsement of the U. S. Government Protection Profile Anti-Virus Applications for Workstations In Basic Robustness Environments, Version 1.0, dated January 6, 2005 by any agency of the U.S. Government and no warranty of the PP is either expressed or implied.

The COACT, Inc., CAFÉ Lab evaluation team concluded that the Common Criteria requirements for a PP Evaluation have been met.

The technical information included in this report was obtained from the U. S. Government Protection Profile Anti-Virus Applications for Workstations In Basic Robustness Environments, Version 1.0, dated January 6, 2005 produced by the U.S. Government and the Basic Robustness Anti-Virus Application Protection Profile Evaluation Technical Report, dated January 6, 2005, Document No. E2-1104-005(5) produced by COACT, Inc., CAFÉ Lab.

2. IDENTIFICATION

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level
(EAL) 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desire a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP CCEVS' Validated Products List.

2.1. PP Identification

The following information completely identifies the Protection Profile:

Evaluation Identifiers for U. S. Government Protection Profile Anti-Virus Applications for Workstations In Basic Robustness Environments, Version 1.0	
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Evaluation Technical Report	Basic Robustness Anti-Virus Application Protection Profile Evaluation Technical Report, dated January 6, 2005, Document No. E2-1104-005(5)
Conformance Result	Part 2 extended, Part 3 conformant
Version of CC	CC Version 2.2 [1], [2], [3], and all applicable NIAP CCEVS and International Interpretations effective on November 23, 2004
Version of CEM	CEM Version 2.2 [5], and all applicable NIAP CCEVS and International Interpretations effective on November 23, 2004
Sponsor	DISA
Developer	ARTEL, Inc. and COACT, Inc
Evaluator(s)	COACT, Inc Brian Pleffner Christa Lanzisera Diann Vechery Chris Pleffner
Validator(s)	NIAP CCEVS James Brosey Tom Murphy

2.2. PP Overview

The "U. S. Government Protection Profile Anti-Virus Applications for Workstations In Basic Robustness Environments" specifies the minimum-security requirements for Anti-Virus Applications (i.e., the Target of Evaluation (TOE)) used on workstations in the US Government in Basic Robustness Environments. The Anti-Virus Application provides protection against viruses coming into the workstation from network connections and/or removable media, and is considered sufficient protection for environments where the likelihood of an attempted compromise is low. This profile establishes the requirements necessary to achieve the security objectives of the Target of Evaluation (TOE) and its environment.

An Anti-Virus application scans content being introduced onto the workstation for viruses. The content may be introduced via removable media (e.g., CDs) inserted into the workstation or via incoming network traffic (e.g., HTML, e-mail attachments, FTP). Anti-Virus applications provide:

- Real-time scanning (to detect viruses as they are entering the system),
- On-demand scans (especially useful for scanning removable media), and
- Scheduled scans (backup mechanism in case a virus is introduced in a way that escaped detection).

Viruses may be file-based or memory-based (i.e., the virus itself does not have to be written to the workstation disk via the file system in order to execute – an example is CodeRed). To detect memory-based viruses, Anti-Virus applications may scan incoming network traffic or scan application memory space (or both). File-based scans must be able to detect viruses contained within compressed files.

Scanning is performed against "signatures" of known viruses. A signature is a known pattern indicative of a virus. To combat new viruses, vendors update and make available a file of signatures (often referred to as DAT files) on a frequent basis. The Anti-Virus application must be able to import updated signatures as necessary. A message digest is used to verify the integrity of the imported signature file on the individual workstations executing the Anti-Virus application.

When a file-based virus is detected, a configured action (or ordered list of actions) is performed to isolate and/or eliminate the virus. The actions available include:

- Clean the virus from the file,
- Quarantine the file,
- Rename the file,
- Delete the file, and
- No action (allow the virus to remain in the file).

When a memory-based virus is detected, the virus is prevented from further execution. The mechanism used to accomplish this is dependent on the type of scanning being performed. Possible mechanisms include discarding incoming network traffic that contains the virus, or terminating a process that has the virus present in its memory space.

An alert message is generated on the screen of the workstation informing the user of the workstation about the virus and the action performed. This alert remains on the screen until acknowledged by the user (or the user ends the session).

In the past, new viruses have been known to propagate themselves to additional platforms via email. Some instances have used self-contained mail functionality. Conformant TOEs must prevent unauthorized processes (i.e., Trojan) from sending email (via SMTP) from the workstation.

Conformant TOEs will be used in Enterprise environments. To support this usage, centralized control and monitoring is required. A Central Administrator must be able to remotely configure the TOE on all network-attached workstations within the Central Administrator's domain. At a minimum, the configuration options that are only made available to the Central Administrator include:

- Configuration of the actions to be taken when file-based viruses are detected,
- Frequency of scheduled scans,
- Depth of scans (for compressed files), and
- File types to be included and/or excluded from scans.

Copies of all audits (including alert messages) from the network-attached workstations are sent to a central management system, where they can be reviewed by the Central Administrator. Audit buffers are provided on the workstations to account for temporary interruptions in connectivity between the workstation and central collection system.

An alert message is generated to the Central Administrator (if a session is active at the time the audit information is received by the central collection system) informing him/her about detection of a virus and the action performed. This alert remains on the screen until acknowledged by the Central Administrator (or the session is ended).

Workstations may not be network-attached (i.e., stand-alone). In those situations, the local administrator for the workstation assumes the privileges of the Central Administrator for that workstation.

The Central Administrator is able to electronically transfer signature files to the network-attached workstations in the domain. Stand-alone workstations depend on physical transfer of the signature files.

Signature files are expected to be updated frequently. The updates originate with the vendor of the Anti-Virus application, and distribution of the updates occurs in several stages.

A TOE conformant to the PP satisfies the specified functional requirements, as well as the Basic Robustness assurance requirements that are expressed in PP Section 5.3 TOE Security Assurance Requirements. The assurance requirements were originally based upon Evaluated Assurance Level (EAL) 2 requirements augmented from part 3 of the Common Criteria with Flaw Remediation (ALC_FLR.2), and Misuse-Examination Guidance (AVA_MSU.1). These augmented assurance requirements were deemed necessary by NSA to provide the level of assurance appropriate for basic robustness environments. For more detail information on the assurance requirements, reference Section 5.3 of the PP.

2.3. IT Security Environment

The TOE described in the PP is intended to operate in Enterprise environments having the security functional requirements equivalent to those required by a basic level of robustness.

A Basic Robustness TOE is considered sufficient for low threat environments or where compromise of protected information will not have a significant impact on mission objectives. This implies that the motivation of the threat agents will be low in environments that are suitable for TOEs of this robustness. In general, basic robustness results in “good commercial practices” that counter threats based in casual and accidental disclosure or compromise of data protected by the TOE.

Basic robustness allows processing of data at a single sensitivity level in an environment where users are cooperative and threats are minimum. Authorized users of the TOE are cleared for all information managed by the TOE, but may not have the need-to-know authorization for all of the data. Hence, the risk that significant damage will be done due to compromise of data is low.

The TOE in and of itself is not of sufficient robustness to protect information of such criticality that the integrity or secrecy is critical to the survival of the enterprise.

The PP has allocated many of the Security Functional Requirements necessary for Basic Robustness compliance to the IT environment. Although this is acceptable for the PP itself, the users of TOEs compliant to the PP should be aware that to achieve an enterprise environment equivalent to Basic Robustness, the Security Functional Requirements allocated to the IT environment must be integrated.

3. SECURITY POLICY

The Basic Robustness Anti-Virus Application Protection Profile provides these security services:

Anti-Virus

When a file-based virus is detected, a configured action (or ordered list of actions) is performed to isolate and/or eliminate the virus. The actions available include:

- Clean the virus from the file,
- Quarantine the file,
- Rename the file,
- Delete the file, and
- No action (allow the virus to remain in the file).

When a memory-based virus is detected, the virus is prevented from further execution. The mechanism used to accomplish this is dependent on the type of scanning being performed.

Audit

The audit functionality required is to generate audits when security-relevant events occur, store the audit information on the local system, transmit the audit information to a central management system, generate alarms for designated events, and audit review.

Protection of audit data in the audit trail involves the TOE and the Operating System (OS). The TOE controls the insertion of audit events into the audit log and the deletion of audit events from the audit log.

Cryptographic Operations

Integrity of the signature files is verified by a message digest calculated for the file.

Management

Audits and alerts are monitored from a central management system. Audit buffers are provided on the workstations to account for temporary interruptions in connectivity between the workstation and central collection system. Alert messages are generated to report the detection of a virus and the action performed. An alert remains on the screen until acknowledged by the Central Administrator (or the session is ended).

Protection of the TOE

Protection of the TOE is required to ensure the TOE security services are not bypassed or tampered with. The TOE and the OS cooperatively provide this service.

The environment for the Basic Robustness Anti-Virus Application Protection Profile is expected to provide these security services to achieve Basic Robustness. The Operating System on which the TOE executes provides these services.

Audit

The environment provides basic file protection services for the audit log.

Data Protection

Data protection services ensure the objects used by the TOE are not available for re-use by other processes or users.

Protection of the TOE

Protection of the TOE is required to ensure the TOE security services are not bypassed or tampered with.

Secure Communications

Between separate portions of the TOE, secure communication is provided by the IT Environment.

3.1. Threats to Security

The Protection Profile identified the following Threats:

Threat	Description of Threat
T.ACCIDENTAL_ADMIN_ERROR	An administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.
T.AUDIT_ COMPROMISE	A user or process may gain unauthorized access to the audit trail and cause audit records to be lost or modified, or prevent future audit records from being recorded, thus masking a security relevant event.
T.MASQUERADE	A user or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources.
T.POOR_DESIGN	Unintentional errors in requirements specification or design of the TOE may occur, leading to flaws that may be exploited by a casually mischievous user or program.
T.POOR_IMPLEMENTATION	Unintentional errors in implementation of the TOE design may occur, leading to flaws that may be exploited by a casually mischievous user or program.
T.POOR_TEST	Lack of or insufficient tests to demonstrate that all TOE security functions operate correctly (including in a fielded TOE) may result in incorrect TOE behavior being discovered thereby causing potential security vulnerabilities.
T.RESIDUAL_DATA	A user or process may gain unauthorized access to data through reallocation of memory used by the TOE to scan files or process administrator requests.
T.TSF_COMPROMISE	A user or process may cause, through an unsophisticated attack, TSF data or executable code to be inappropriately accessed (viewed, modified, or deleted).
T.UNATTENDED_SESSION	A user may gain unauthorized access to an unattended session.
T.UNIDENTIFIED_ACTIONS	Failure of the authorized administrator to identify and act upon unauthorized actions may occur.
T.VIRUS	A malicious agent may attempt to introduce a virus onto a workstation via network traffic or removable media to compromise data on that workstation, or use that workstation to attack additional systems.

3.2. Policies

The Operational Security Policies defined for the TOE are as follows:

Policy	Policy Description
P.ACCESS_BANNER	The system shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the system.
P.ACCOUNTABILITY	The authorized users of the TOE shall be held accountable for their actions within the TOE.
P.CRYPTOGRAPHY	Only NIST FIPS validated cryptography (methods and implementations) are acceptable for key management (i.e.; generation, access, distribution, destruction, handling, and storage of keys) and cryptographic services (i.e.; encryption, decryption, signature, hashing, key exchange, and random number generation services)
P.MANUAL_SCAN	The authorized users of the workstations shall initiate manual anti-virus scans of removable media (e.g., floppy disks, CDs) introduced into the workstation before accessing any data on that removable media.
P.ROLES	The TOE shall provide an authorized administrator role for secure administration of the TOE. This role shall be separate and distinct from other authorized users.

4. ASSUMPTIONS

Secure Usage Assumptions

The specific conditions below are assumed to exist in a PP-compliant TOE environment.

Assumption	Assumption Description
A.AUDIT_BACKUP	Administrators will back up the audit files and monitor disk usage to ensure audit information is not lost.
A.NO_EVIL	Administrators are non-hostile, appropriately trained, and follow all administrator guidance.
A.PHYSICAL	It is assumed that appropriate physical security is provided within the domain for the value of the IT assets protected by the TOE and the value of the stored, processed, and transmitted information.
A.SECURE_COMMS	It is assumed that the IT environment will provide a secure line of communications between distributed portions of the TOE and between the TOE and remote administrators.
A.SECURE_UPDATES	Administrators will implement secure mechanisms for receiving and validating updated signature files from the Anti-Virus vendors, and for distributing the updates to the central management systems.

5. ARCHITECTURAL INFORMATION

The PP does not dictate a specific TOE architecture. The TOE may be completely software based.

The TOE is intended to be used on workstations in a trusted network configuration, as illustrated in Figure 1. The Firewall/Guard at the boundary of the trusted network represents one or more systems that perform protection services for the trusted network as a whole. It is assumed that protocols commonly used to transport viruses, such as SMTP, HTTP, and FTP, are screened at the Firewall/Guard function. This provides a "defense in depth" since the TOE (executing on the workstations) performs similar functions.

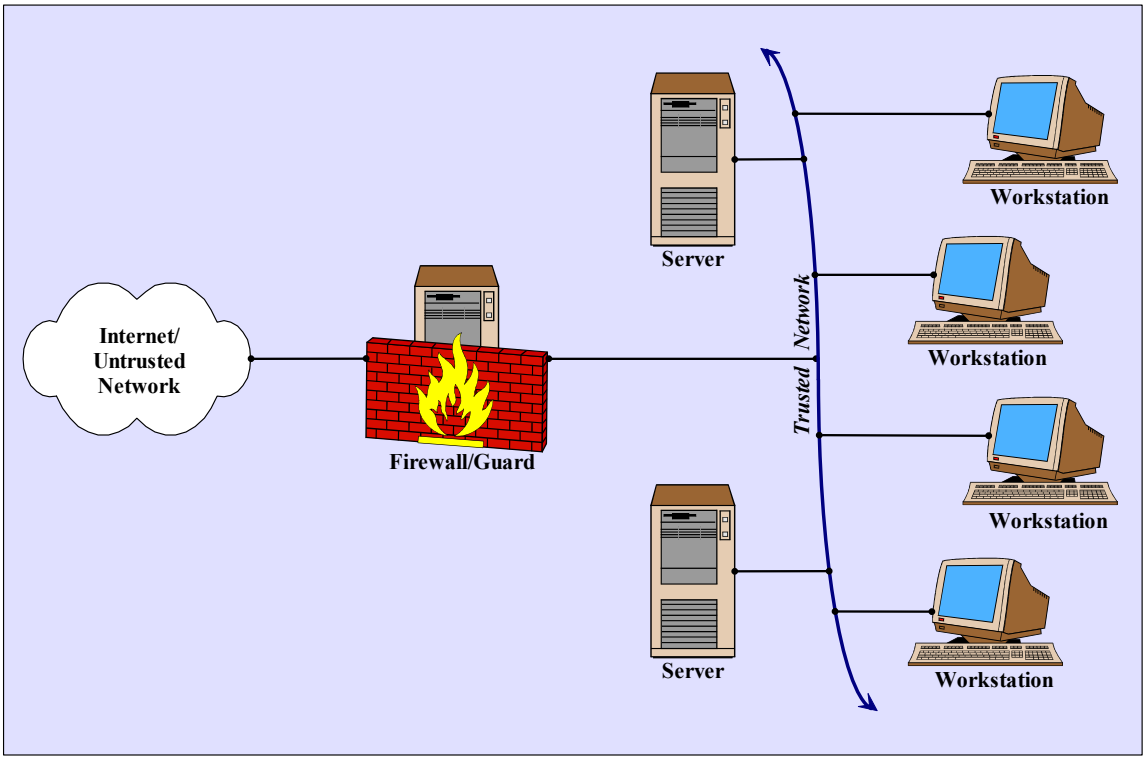

Figure 1 – Network Environment of the TOE

It is expected that Anti-Virus applications may be executing on both the servers (e.g., network attached storage, email servers, web servers) and workstations within the trusted network. The PP does not address the servers; instead, it focuses on workstations.

On the workstations, the Anti-Virus application executes on top of the operating system to perform its scanning, reaction, and logging functions. The management functions of the Central Administrator for a conformant TOE may execute on a separate system from the portion of the TOE performing virus scanning on workstations. Access to those management functions may be remote via HTTP.

6. DOCUMENTATION

U. S. Government Protection Profile Anti-Virus Applications for Workstations in Basic Robustness Environments, Version 1.0.

7. RESULTS OF THE EVALUATION

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted in accordance with the APE sections in the Common Criteria, Version 2.2; CEM, Version 2.2, and all applicable NIAP CCEVS and International Interpretations in effect on November 23, 2004.

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of the APE assurance component. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer of the issue that needed to be resolved or the clarification that needed to be made to the particular evaluation evidence.

The Evaluation Team accomplished this by providing Comments or Work Pack Assessment Tables for an evaluation activity that recorded the Evaluation Team's evaluation results and that the Evaluation Team provided to the developer. The Evaluation Team also communicated with the developer by telephone and electronic mail. If applicable, the Evaluation Team re-performed the work unit or units affected. In this way, the Evaluation Team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict. No constraints or assumptions were identified in performing this evaluation.

In this way, the Evaluation Team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict.

Chapter 4, Evaluation Results, in the Evaluation Team's ETR, states: "The U. S. Government Protection Profile Anti-Virus Applications for Workstations in Basic Robustness Environments was successfully evaluated."

Chapter 5, Conclusions, in the Evaluation Team's ETR, states: "The US Government Protection Profile Anti-Virus Applications for Workstations in Basic Robustness Environments has satisfied the requirements of the APE Assurance Requirements. The PP was assessed against the requirements as stated in the Common Methodology for Information Technology Security Evaluation Part 2, Version 2.2."

8. VALIDATION COMMENTS/RECOMMENDATIONS

The PP evaluation precedes the certification and publication of the U.S. Government Protection Profile for Single-level Operating Systems in Environments Requiring Basic Robustness, Version 0.3, dated 29 January 2004, which at the time of certification was under development.

The Validation Team observed that the evaluation and all of its activities were performed in accordance with the CC, the CEM, and CCEVS practices. The Validation Team agrees that the CCTL presented appropriate rationales to support the evaluation results presented in Section 4

and the Conclusions presented in Section 5 of the Basic Robustness Anti-Virus Application Protection Profile Evaluation Technical Report, dated January 6, 2005, Document No. E2-1104-005(5). The Validation Team considered the findings of the evaluation team and the sections provided in this document. The Validation Team, therefore, concludes that the evaluation and PASS result for the U. S. Government Protection Profile Anti-Virus Applications for Workstations in Basic Robustness Environments; Version 1.0 is complete and correct.

9. ACRONYMS

AM	Assurance Maintenance
BR CIM	Basic Robustness Consistency Instruction Manual
CC	Common Criteria
CM	Configuration Management
CMVP	Cryptographic Module Validation Program
DISA	Defense Information Services Agency
DoD	Department of Defense
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standard
FOUO	For Official Use Only
FTP	File Transfer Protocol
GIG	Global Information Grid
HTTP	Hypertext Transport Protocol
I&A	Identification and Authentication
ID	Identification
IGS	Installation, Startup and Generation
IP	Internet Protocol
IT	Information Technology
LAN	Local Area Network
NIAP	National Information Assurance Partnership
NIPRNet	Non-classified Internet Protocol Router Network
NIST	National Institute of Standards and Technology
NSA	National Security Agency
PP	Protection Profile
PUB	Publication
RFC	Request for Comments
SFP	Security Function Policy

SIPRNet	Secret Internet Protocol Router Network
SOF	Strength of Function
SMTP	Simple Message Transfer Protocol
SSL	Secure Socket Layer
ST	Security Target
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TP	Trusted Path
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy
UDP	User Datagram Protocol

10. BIBLIOBRAPHY

The Validation Team used the following documents to produce this Validation Report:

[1] *Common Criteria for Information Technology Security Evaluatio*n, version 2.2, January 2004, Part 1

[2] *Common Criteria for Information Technology Security Evaluatio*n, version 2.2, January 2004, Part 2

[3] *Common Criteria for Information Technology Security Evaluatio*n, version 2.2, January 2004, Part 3

[4] *Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Guidance to Validation Teams of IT Security Evaluations, Scheme Publication #3*, Version 1.0, February 2002.

[5] *Common Evaluation Methodology for Information Technology Security Evaluation* – Evaluation Methodology, version 2.2, January 2004.

[6] U. S. Government Protection Profile Anti-Virus Applications for Workstations In Basic Robustness Environments, Version 1.0, dated January 5, 2005

[7] *Basic Robustness Anti-Virus Application Protection Profile Evaluation Technical Report*, dated January 6, 2005, Document No. E2-1104-005(5)