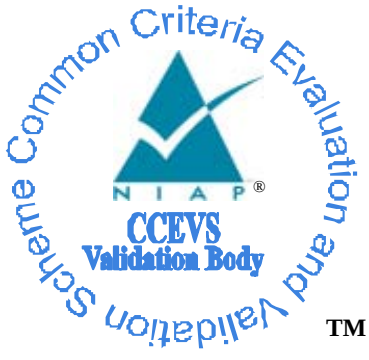
National Information Assurance Partnership



TM

Common Criteria Evaluation and Validation Scheme Validation Report

Applied Identity ID-Enforce

Report Number: **CCEVS-VR-VID10272-2008**

Dated: **October 6, 2008**
Version: **2.0**

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 6757
Fort George G. Meade, MD 20755-6757

ACKNOWLEDGEMENTS

Validation Team

Paul Bicknell
Jean Hung
MITRE Corporation
Bedford, Massachusetts

Common Criteria Testing Laboratory

SAIC, Inc.
Columbia, Maryland

Table of Contents

List of Tables

1 Executive Summary

The evaluation of *Applied Identity ID-Enforce Hardware Appliance (models 5000, 7000, and 10000) with ID-Enforce Gateway, Version 3.3, including the ID-Enforce Client (ID-Mark, v3.3), and the Identisphere Manager (ID-Policy, v3.3)* also known as *Applied Identity ID-Enforce* was performed by SAIC, in the United States and was completed in September 2008. The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) process and scheme. The criteria against which the *Applied Identity ID-Enforce Hardware Appliance (models 5000, 7000, and 10000) with ID-Enforce Gateway, Version 3.3, including the ID-Enforce Client (ID-Mark, v3.3), and the Identisphere Manager (ID-Policy, v3.3)* TOE was judged are described in the Common Criteria for Information Technology Security Evaluation, Version 2.3 and International Interpretations effective on 12, January 2007. The evaluation methodology used by the evaluation team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 2.3.

Science Applications International Corporation (SAIC) determined that the evaluation assurance level (EAL) for the product is the EAL 2 family of assurance requirements. The product, when configured as specified in the installation guides and user guides, satisfies all of the security functional requirements stated in the *Applied Identity ID-Enforce Security Target*.

This Validation Report applies only to the specific version of the TOE 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. This Validation Report is not an endorsement of the *Applied Identity ID-Enforce Hardware Appliance (models 5000, 7000, and 10000) with ID-Enforce Gateway, Version 3.3, including the ID-Enforce Client (ID-Mark, v3.3), and the Identisphere Manager (ID-Policy, v3.3)*product by any agency of the US Government and no warranty of the product is either expressed or implied.

The technical information included in this report was obtained from the *Evaluation Technical Report for Applied Identity ID-Enforce Hardware Appliance (models 5000, 7000, and 10000) with ID-Enforce Gateway, Version 3.3, including the ID-Enforce Client (ID-Mark, v3.3), and the Identisphere Manager (ID-Policy, v3.3)* (ETR) Parts 1 and 2 produced by SAIC.

1.1 Evaluation Details

Evaluated Product:	**Applied Identity ID-Enforce Hardware Appliance (models 5000, 7000, and 10000) with ID-Enforce Gateway, Version 3.3, including the ID-Enforce Client (ID-Mark, v3.3) and the Identisphere Manager (ID-Policy, v3.3)**

Sponsor & Developer:	Applied Identity, Inc. 456 Montgomery, Suite 400 San Francisco, CA 94104
CCTL:	Science Applications International Corporation Common Criteria Testing Laboratory 7125 Columbia Gateway Drive, Suite 300 Columbia, MD 21046
Completion Date:	August 2008
CC:	Common Criteria for Information Technology Security Evaluation, Version 2.3
Interpretations:	There were no applicable interpretations used for this evaluation.
CEM:	Common Methodology for Information Technology Security Evaluation, Version 2.3
Evaluation Class:	EAL 2
Description	The *Applied Identity ID-Enforce Hardware Appliance (models 5000, 7000, and 10000) with ID-Enforce Gateway, Version 3.3, including the ID-Enforce Client (ID-Mark, v3.3), and the Identisphere Manager (ID-Policy, v3.3)* is a system which is designed primarily to protect resources located on a protected network from users on an untrusted network. The client application (i.e., ID-Mark) allows the network users to interact with the TOE in order to access the resources it protects, and the Identisphere Manager (ID-Policy v3.3) application offers a Graphical User Interface (GUI) that may be used by the network administrator, in lieu of the native tools provided by the LDAP server itself, to define the user access policies stored in the LDAP server. The appliances include the external Ethernet ports used to communicate with the untrusted network, protected network, a dedicated management network and console port for direct serial connection of a terminal computer for TOE management, and a high availability port used to connect a failover appliance for redundancy. The Applied Identity ID-Enforce Gateway, Version 3.3, consists of a pre-installed version 2.6 Linux Operating System that provides the functions to control user access to protected network resources and also implements a Command-Line Interface (CLI), which provides the local authorized administrator the interfaces to configure the TOE. The ID-Enforce Client (ID-Mark, v3.3) allows network users

	to authenticate to the TOE in order to access the resources the TOE protects. The TOE can be configured to allow access to network resources without requiring an authenticated user session and in those cases the client is not necessary. The Identisphere Manager (ID-Policy, v3.3) application offers a Graphical User Interface (GUI) that may be used by the network administrator, in lieu of the native tools provided by the LDAP server itself, to define the user access policies stored in the LDAP server.
Disclaimer	The information contained in this Validation Report is not an endorsement of the *Applied Identity ID-Enforce Hardware Appliance (models 5000, 7000, and 10000) with ID-Enforce Gateway, Version 3.3, including the ID-Enforce Client (ID-Mark, v3.3), and the Identisphere Manager (ID-Policy, v3.3)*product by any agency of the U.S. Government and no warranty of the *Applied Identity ID-Enforce Hardware Appliance (models 5000, 7000, and 10000) with ID-Enforce Gateway, Version 3.3, including the ID-Enforce Client (ID-Mark, v3.3), and the Identisphere Manager (ID-Policy, v3.3)* product is either expressed or implied.
PP:	none
Evaluation Personnel	Dawn Campbell Gary Grainger
Validation Team:	Paul Bicknell Jean Hung

1.2 Interpretations

The Evaluation Team determined that there were no NIAP Interpretations applicable to this evaluation:

1.3 Threats to Security

The following are the threats that the evaluated product addresses:

Table 1 - Threats

Threat	TOE Threats
T.ACCESS	Users may be able to access network resources for which they are not authorized.

Threat	TOE Threats
T.ACCOUNT	Users might not be accountable for management of the TOE and access to controlled network resources.

2 Identification

The product being evaluated is *Applied Identity ID-Enforce Hardware Appliance (models 5000, 7000, and 10000) with ID-Enforce Gateway, Version 3.3 including the ID-Enforce Client ID-Mark v3.3 and the Identisphere Manager (ID-Policy v3.3).*

3 Security Policy

Table 1 - Policies

None	The ST does not define security policies for this TOE

4 Assumptions

4.1 Personnel Assumptions

The following personnel assumptions are identified in the Security Target:

Table 2 – Personnel Assumptions

A.MANAGE	It is assumed that the TOE and its IT environment will be installed, configured, and managed in accordance with applicable security management guidance.
A.NOEVIL	It is assumed that all administrators regardless of individual authority will be appropriately trusted not to intentionally attempt to exceed their authority using either physical or logical means.

4.2 Physical Assumptions

The following physical assumptions are identified in the Security Target:

Table 3 – Physical Assumptions

A.LOCATE	It is assumed that the TOE and its IT environment will be located such that the IT environment can deliver security policies to the TOE and such that the TOE can effectively control the resources it is intended to protect without the risk of bypassing the TOE altogether in order to access the resources to be protected.
A.PHYSICAL	It is assumed that the TOE and its IT environment will be physically protected from tampering.

4.3 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made; and meets them with only a certain level of assurance (EAL 2 in this case).
- As with all EAL 2 evaluations, this evaluation did not specifically search for vulnerabilities that were not "obvious" (as this term is defined in the CC and CEM); or seriously attempt to find counters to them; nor find vulnerabilities related to objectives not claimed in the ST.
- Encryption of communications using either SSL or TLS between the Appliance and the Client and between the LDAP Server is required. The evaluation team did verify that communication between these components is encrypted. Testing confirmed the presence of encrypted communication. However, the cryptography used in this product was not analyzed or tested to conform to cryptographic standards during this evaluation.

5 Architectural Information

The *Applied Identity ID-Enforce Hardware Appliance (models 5000, 7000, and 10000) with ID-Enforce Gateway, Version 3.3, including the ID-Enforce Client (ID-Mark, v3.3), and the Identisphere Manager (ID-Policy, v3.3)* is a system that is designed primarily to protect resources located on a protected network from users on an untrusted network. Policies can be defined using the ID-Policy component; which are then enforced by the ID-Enforce Gateway software located on the appliance. The ID-Mark allows users to authenticate to the appliance portion of the TOE in order to access protected resources. Policies can be defined which allow unauthenticated users to access specific resources. In these cases the use of ID-Mark is not required.

TOE Components:

- **ID-Enforce 5000, 7000, and 10000 Hardware Appliances** – The hardware appliance includes the external Ethernet ports used to communicate with the untrusted network, protected network, a dedicated management network and console port for direct serial connection of a terminal computer for TOE management, and a high availability port used to connect a failover appliance for redundancy.
- **ID-Enforce Gateway** - The software component, executing within the hardware appliance, provides the functions to control user access to protected network resources and implement a Command-Line Interface (CLI), which provides the local authorized administrator the interfaces to configure the TOE.
- **ID-Enforce Client** – Optional client component design specifically for use with the ID-Enforce Gateway.
- **Identisphere Manager** – An optional application that can be used to define user access policies.

IT Environment:

- Simple Network Management Protocol (SNMP) server – an optional component to receive alerts generated by the ID-Enforce Gateway v3.3 server. Note that the specific capability to generate alerts is not claimed in this Security Target and hence is not a subject of the evaluation.
- System Log (SYSLOG) server – required to store the audit records generated by the TOE before the (local) records are overwritten.
- Authentication Servers (i.e., Lightweight Directory Access Protocol (LDAP), RSA) – required to provide/store the user credentials (for both authentication and access) used by the TOE in making network access control decisions and by the authentication servers in order to authenticate users.
- Network Time Protocol (NTP) or Time Server – required to provide the reliable timestamp used by the TOE.
- Terminal application - a local system connected directly to the TOE for local administration. Access to the CLI can be accomplished by one of the following ways:
    - A direct connection to the ID-Enforce serial console port.
    - A network connection to the High Availability port using SSH. This connection should only be used during configuration and should subsequently be disconnected or used to facilitate the High Availability feature.
    - A network connection to protected, untrusted, or managed ports using SSH. This requires explicit policy configuration to allow such access.

  Note that accessing the CLI via one of the network connection is recommended only if the connected network is dedicated and isolated for that purpose. Reliance on SSH is not recommended, since the SSH implementation is not FIPS certified, and is not subject to security claims in this Security Target. *As such, the evaluated configuration includes only the use of direct serial connections and/or dedicated isolated networks for the purpose of accessing the CLI.*
- Operating system (Windows ME, Windows 2000 Server or Professional, Windows XP, or Windows Server 2003) – required to host any ID-Mark client applications.

6 Documentation

Following is a list of useful documents supplied by the developer and shipped with the product.

- Applied Identity ID-Enforce User's Guide, v3.3
- Applied Identity ID-Enforce Quick Start Guide v3.3

- Applied Identity ID-Policy 3.3

The security target used is:

- Applied Identity ID-Enforce Security Target V1.0, September 29, 2008

7 IT Product Testing

The evaluation team applied each EAL 2 ATE CEM work unit. The evaluation team ensured that the TOE performed as described in the functional specification and as stated in the TOE security functional requirements. The evaluation team performed the entire vendor test suite over two platforms, and devised an independent set of team test and penetration tests. The vendor tests, team tests, and penetration tests substantiated the security functional requirements in the ST. The tests were conducted using:

- The Applied Identity ID-Enforce Hardware Appliance (models 5000 and 10000) with the ID-Enforce Gateway, Version 3.3, software pre-installed.
- The ID-Enforce Client (ID-Mark, v3.3) and the Identisphere Manager (ID-Policy, v3.3) Software installed on Windows XP (same machine) located on the untrusted network
- SecureCRT terminal application with direct connection to ID-Enforce serial console port to access the CLI
- LDAP, RSA, SYSLOG and NTP Servers located on the trusted network

The developer test suite was examined and found to provide adequate coverage of the security functions; where the vendor test suite provided insufficient coverage, the evaluation team devised additional test cases to adequately test the security functions.

The entire developer tests were run and the results were found to be consistent with the results generated by the developer.

No vulnerabilities in the TOE were found during a search of vulnerability databases.

8 Evaluated Configuration

The evaluated configuration is one or two Applied Identity ID-Enforce Hardware Appliances each with the ID-Enforce Gateway software pre-installed. One appliance configuration is standalone mode and two is High-Availability mode. The High-Availability (HA) mode provides failover functionality in case one of the appliances was to lose connection or otherwise fail. In addition there are Bridged and Routed modes however the functionality in these modes are the same except that Bridged mode permits policies to be configured that deny access based on mac addresses (i.e MAC Filtering). The 10000 model was tested in Bridged mode with two appliances connected and configured for High-Availability. Model 5000 was tested as standalone in routed mode before configuring a second appliance for HA testing (also in routed mode). The evaluated configuration also included one ID-Enforce Client (ID-Mark, v3.3) and the Identisphere Manager (ID-Policy,

v3.3). Software installed on Windows XP (same machine) located on the untrusted network. SSL or TLS must be configured for the connection to the LDAP Server and between ID-Mark and the ID-Enforce Gateway appliance. The evaluated configuration excludes a second Client WebAuth. This client is intended to allow web-based access to the appliance via login web page. This feature must be disabled by creating a global policy preventing access to the HTTPS port 443. A secure communication channel between the Identisphere Manager (ID-Policy) and the LDAP server acting as the policy store must be ensured. ID-Policy could be hosted on the same computer as the server. If not, it is necessary that either the SSL or TLS protocol is used for connectivity between the ID-Policy and the server.

9 Results of the Evaluation

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's performance of the vendor tests suite, the independent tests, and the penetration test also demonstrates the accuracy of the claims in the ST.

10 Validator Comments/Recommendations

The validation team observed that the evaluation was performed in accordance with the CC, the CEM, and CCEVS practices. The Validation team agrees that the CCTL presented appropriate rationales to support the Results presented in Section 5 of the ETR and the Conclusions presented in Section 6 of the ETR.

The validation team, therefore, recommends that the evaluation and Pass result for the identified TOE be accepted.

11 Annexes

Not applicable.

12 Security Target

The security target for this product's evaluation is **Applied Identity ID-Enforce, version 1.0 dated September 29, 2008**.

13 Glossary

There were no definitions used other than those used in the CC or CEM.

14 Bibliography

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

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated August 2005, Version 2.3.

[2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated August 2005, Version 2.3.

[3] Common Criteria for Information Technology Security Evaluation – Part 2: Annexes, dated August 1999, Version 2.1.

[4] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated August 2005, Version 2.3.

[5] Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, dated 1 November 1998, version 0.6.

[6] Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology, dated August 2005, version 2.3.

[7] Evaluation Technical Report for Applied Identity ID-Enforce Hardware Appliance (models 5000, 7000, and 10000) with ID-Enforce Gateway, Version 3.3 including the ID-Enforce Client ID-Mark v3.3 and the Identisphere Manager (ID-Policy v3.3) Part II, version 1.0, August 29, 2008

[8] Security Target for Common Criteria: Applied Identity ID-Enforce, version 1.0, September 29, 2008.

[9] NIAP Common Criteria Evaluation and Validation Scheme for IT Security, Guidance to Common Criteria Testing Laboratories, Version 2.3, August 2005