National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

Sybase Incorporated

Sybase IQ User Administration v12.6

Report Number: CCEVS-VR-05-0084

Dated: 11 February 2005

Version: 1.0

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 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team

Nicole M. Carlson (Lead)
Daniel P. Faigin

The Aerospace Corporation
El Segundo, California

Common Criteria Testing Laboratory

Science Applications International Corporation (SAIC)

Columbia, Maryland

Table of Contents

1. EXECUTIVE SUMMARY

This report documents assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Sybase Inc.'s Sybase IQ User Administration product, version 12.6. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America, and was completed in December 2004. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by SAIC. The evaluation determined that the product is both **Common Criteria Part 2 Extended and Part 3 Conformant**, and meets the assurance requirements of EAL 3 augmented with ALC_FLR.2. The product is not conformant with any published Protection Profiles. All security functional requirements are derived from Part 2 of the Common Criteria or expressed in the form of Common Criteria Part 2 requirements.

The Sybase IQ User Administration product (the TOE) provides two functions that serve as extensions to the Sybase Adaptive Server Anywhere product, which is in the IT environment and was not covered by this evaluation:

1. The TOE can set and reset a user's password expiration date

2. The TOE can check that a user's password expiration date has not yet passed.

Though other functionality is present in the underlying product, the evaluation covered *only* these two User Administration functions.

During this validation, the validators monitored the activities of the SAIC evaluation team, provided guidance on technical issues and evaluation processes, reviewed successive versions of the Security Target, reviewed selected evaluation evidence, reviewed test plans, reviewed intermediate evaluation results (i.e., the CEM work units), and reviewed successive versions of the ETR and test reports. The validator determined that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements defined in the Security Target (ST). Therefore, the validator concludes that the SAIC findings are accurate, the conclusions justified, and the conformance claims correct.

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, 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 conduct security evaluations.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring 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's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated;
- The Security Target (ST), describing the security features, claims, and assurances of the product;
- The conformance result of the evaluation;
- Any Protection Profile to which the product is conformant;
- The organizations participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	Sybase IQ User Administration Version 12.6
Protection Profile	None
Security Target	*Sybase IQ User Administration Security Target, version 1.0, February 8, 2005*
Evaluation Technical Report	*Evaluation Technical Report for the Sybase IQ User Administration Version 12.6:* • *Part 1 (Non-Proprietary), Version 1.0, February 9, 2005* • *Part 2 (Propriety), Version 1.0, February 8, 2005*
Conformance Result	Part 2 Extended and Part 3 Conformant, EAL 3 augmented with ALC_FLR.2
Sponsor	Sybase, Incorporated
Developer	Sybase, Incorporated
Evaluators	Science Applications International Corporation (SAIC)
Validator	The Aerospace Corporation

3. SECURITY POLICY

The Sybase IQ User Administration suite provides security functions related to password expiration, although the product itself *does not* provide full password expiration policy enforcement. Specifically, the product permits the setting, resetting, and testing of the password expiration date. It does not provide enforcement of password expiration; said enforcement only occurs when these functions are utilized in the context of a full password expiration implementation.

4. ASSUMPTIONS

4.1. Usage Assumptions

Administrators are assumed to be non-hostile, appropriately trained and follow all administrator guidance.

4.2. Environmental Assumptions

It is assumed that there are no general-purpose computing capabilities (e.g., compilers or user applications) available on DBMS servers, other than those services necessary for the operation, administration and support of the DBMS.

It is also 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.

Lastly, it is assumed that the IT environment provides support commensurate with the expectations of the TOE. This is achieved by using evaluated products (or products in evaluation at the time of the writing of this VR) in the environment. The expectations of the TOE with respect to the security provided by the IT environment are captured in the ST in the environmental objectives, but *were not* verified by the evaluation.

5. ARCHITECTURAL INFORMATION

This TOE is extremely simple, as it provides only two functions in a single subsystem. These functions are designed as a set of stored procedures and supporting database tables (which are actually stored in the IT environment). These stored procedures are used to configure the security functions of the TOE; they may also be invoked by the hosting product to invoke the security functions of the TOE.

The TOE is layered on top of Sybase IQ, which is not part of the TOE. The Sybase IQ product provides relational database technology designed as an extended version of Sybase Adaptive Server Anywhere (ASA). Sybase IQ is a decision support server designed for data warehousing that has (in turn) been designed around the Sybase Adaptive Server Anywhere core product. Adaptive Server Anywhere (under separate evaluation as of the time of publication) is itself an application that runs on top of a general purpose operating system, and depends on the services exported by the operating system to function. The hardware upon which the operating system runs is completely transparent to this chain of applications.

Figure 1 provides an overview of the architecture of Sybase IQ User Administration.

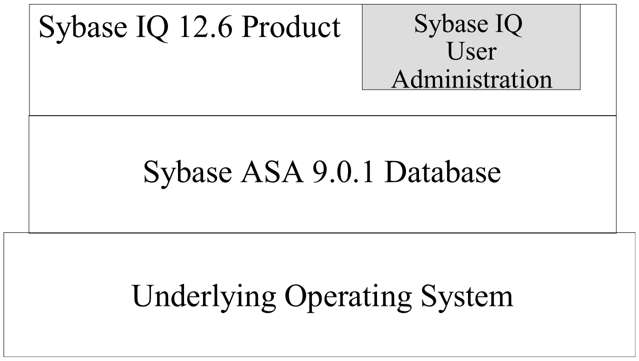
Sybase IQ 12.6 Product
Sybase IQ User Administration
Sybase ASA 9.0.1 Database
Underlying Operating System

Figure 1: Architectural Overview of Sybase IQ UA

6. DOCUMENTATION

The following documentation was used as evidence for the evaluation of the Sybase IQ User Administration Version 12.6:[1]

6.1. Design documentation

Document	Version	Date
Sybase IQ User Administration Design Specification	v2.0	12 October 2004
Sybase IQ User Administration Functional Specification	v1.0	1 June 2004
IQ User Administration Correspondence	v2.0	13 October 2004

6.2. Guidance documentation

Document	Version	Date
Sybase IQ 12.6 System Administration Guide	None	July 2004
Sybase IQ 12.6 Common Criteria Evaluation Road Map	None	3 November 2004
Sybase IQ 12.6 Reference Manual	None	November 2004
Sybase IQ 12.6 Utility Guide	None	June 2004

6.3. Configuration Management and Lifecycle documentation

Document	Version	Date
Sybase IQ Configuration Management Plan	v 0.30	22 November 2004
Sybase IQ Life Cycle Plan	V 0.3	10 September 2004
Sybase Manual Release Guide, Document # 35580-01-0100-15	None	None
Videotape of development facility	None	18 November 2004

[1] This documentation list is extracted from the Evaluation Technical Report, Part 1, developed by SAIC.

6.4. Delivery and Operation documentation

Document	Version	Date
Sybase IQ Delivery and Operation procedures	v 0.1	1 June 2004
Supplement for Installing Sybase IQ for Common Criteria Configuration, Document ID: DC00230-01-1260-01	None	20 November 2004
Sybase IQ Installation & Configuration Guide 12.6 Linux, DC10083	None	None
Sybase IQ Installation & Configuration Guide 12.6 Sun Solaris, DC30066	None	None
Sybase IQ Installation & Configuration Guide 12.6 Windows, DC30056	None	None
Sybase IQ Installation & Configuration Guide 12.6 HP-UX, DC39500	None	None

6.5. Test documentation

Document	Version	Date
Sybase IQ Test Specification	V3.0	17 November 2004
Sybase IQ Test Coverage Analysis	V2.0	17 November 2004
Sybase Design Mapping	V1.0	17 November 2004
Actual Test Results	V1.0	3 November 2004

6.6. Vulnerability Assessment documentation

Document	Version	Date
Sybase IQ – User Administration Vulnerability Analysis	V0.2	22 November 2004

6.7. Security Target

Document	Version	Date
Sybase IQ User Administration Security Target	V1.0	8 February 2005

7. IT PRODUCT TESTING

7.1. Developer Testing

Evaluator analysis of the developer's test plans, test scripts, and test results indicate that the developer's testing is adequate to satisfy the requirements of EAL3, augmented with AVA_VLA.2.

The developer's tests were non-automated, and consisted of sixteen manual tests, on all four underlying operating systems. These verified the basic functionality of the TOE, and exercised the parameters and verified the exception conditions documented in the user and administrative guidance.

For each of the developer tests, the evaluators analyzed the test procedures to determine whether the procedures were relevant to, and sufficient for the function being tested. They also verified that the test documentation showed results that were consistent with the expected results for each test script.

7.2. Evaluator Testing

7.2.1. Functional Testing

In addition to developer testing, the CCTL conducted its own suite of tests. Two configurations of the TOE were tested:

- Sybase IQ UA v.12.6 running in an environment consisting of Sybase IQ 12.6 (an extension of ASA version 9.0.1) running on Windows 2000 SP3

- Sybase IQ UA v.12.6 running in an environment consisting of Sybase IQ 12.6 (an extension of ASA version 9.0.1) running on Solaris 2.8

The CCTL installed ASA and Sybase IQ on the systems listed, and followed the installation procedures for Windows and Solaris. The CCTL reran fourteen of sixteen developer tests, as well as running their own suite of tests. These tests identified no failures of the functions in the TOE. Testing was witnessed by a representative of the validation team.

7.2.2. Vulnerability Testing

The evaluators developed vulnerability test to address both management and TOE access security functions, as well as expanding upon the public search for vulnerabilities provided to the team by the sponsor. These tests identified no vulnerabilities in the specific functions provided by the TOE.

8. EVALUATED CONFIGURATION

The TOE may only be purchased as part of the full Sybase IQ product, version 12.6; that is, there is no distinct product in the Sybase product catalog denoted "Sybase IQ User Administration." This evaluation covers *only those functions* provided to set, reset, and test the password expiration date. The remaining functions of the full Sybase IQ product, *including all database functionality,* are part of the IT environment.

To use the product in the evaluated configuration, the product must be configured as specified in the *Supplement for Installing Sybase IQ for Common Criteria Configuration*, Document ID: DC00230-01-1260-01, November 20, 2004,

Sybase IQ is an extended version of Sybase Adaptive Sever Anywhere product, version 9.0.1. For the purposes of this evaluation, the set of underlying operating systems for Sybase IQ/ASA included Microsoft Windows 2000, XP and Server 2003, Sun Solaris 8, HP-UX, and Redhat Linux Advanced Server 2.1.

9. RESULTS OF THE EVALUATION

The evaluation was conducted based upon the Common Criteria (CC), Version 2.1, dated August 1999 [1,2,3,4]; the Common Evaluation Methodology (CEM), Version 1.0, dated August 1999 [6]; and all applicable International Interpretations in effect on 1 April 2004. The evaluation confirmed that the Sybase IQ User Administration product is compliant with the Common Criteria Version 2.1, functional requirements (Part 2), Part 2 extensions, and assurance requirements (Part 3) for EAL3 augmented with AVA_VLA.2. The details of the evaluation are recorded in the CCTL's evaluation technical report, Evaluation Technical Report for the Sybase IQ User Administration v12.6, Part 1 (Non-Proprietary) and Part 2 (Proprietary). The product was evaluated and tested against the claims presented in the Sybase IQ User Administration Security Target v1.0, 8 February 2005.

The validator followed the procedures outlined in the Common Criteria Evaluation Scheme publication number 3 for Technical Oversight and Validation Procedures. The validator has observed that the evaluation and all of its activities were in accordance with the Common Criteria, the Common Evaluation Methodology, and the CCEVS. The validator therefore concludes that the evaluation team's results are correct and complete.

The following evaluation results are extracted from the non-proprietary Evaluation Technical Report provided by the CCTL.

9.1. Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Sybase IQ User Administration product that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

9.2. Evaluation of the Configuration Management Capabilities (ACM)

The evaluation team applied each EAL 3 ACM CEM work unit. The ACM evaluation ensured the TOE is identified such that the consumer is able to identify the evaluated TOE. The evaluation team ensured the adequacy of the procedures used by the developer to accept, control and track changes made to the TOE implementation, design documentation, test documentation, user and administrator guidance, security flaws and the CM documentation. To support the ACM evaluation, the evaluation team received Configuration Management (CM) records from Sybase.

9.3. Evaluation of the Delivery and Operation Documents (ADO)

The evaluation team applied each EAL 3 ADO CEM work unit. The ADO evaluation ensured the adequacy of the procedures to deliver, install, and configure the TOE securely. The evaluation team ensured the procedures addressed the detection of modification while in transit. The evaluation team followed the Configuration Guide to test the installation procedures to ensure the procedures result in the evaluated configuration.

9.4. Evaluation of the Development (ADV)

The evaluation team applied each EAL 3 ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification and a high-level design document. The evaluation team also ensured that the correspondence analysis between the design abstractions correctly demonstrated that the lower abstraction was a correct and complete representation of the higher abstraction.

9.5. Evaluation of the Guidance Documents (AGD)

The evaluation team applied each EAL 3 AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. Both of these guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

9.6. Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each EAL 3 ALC CEM work unit. The evaluation team ensured the adequacy of the developer procedures to protect the TOE and the TOE documentation during TOE development and maintenance to reduce the risk of the introduction of TOE exploitable vulnerabilities during TOE development and maintenance. To support the ALC evaluation, the evaluation team received a video recording of the security measures at Sybase to support the documented measures.

In addition to the EAL 3 ALC CEM work units, the evaluation team applied the ALC_FLR.2 work units from the CEM supplement. The flaw remediation procedures were evaluated to ensure that flaw reporting procedures exist for managing flaws discovered in the TOE.

9.7. Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each EAL 3 ATE CEM work unit. The evaluation team ensured that the TOE performed as described in the design documentation and demonstrated that the TOE enforces the TOE security functional requirements. Specifically, the evaluation team ensured that the vendor test documentation sufficiently addresses the security functions as described in the functional specification and high level design specification. The evaluation team performed a sample of the vendor test suite, 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.

9.8. Vulnerability Assessment Activity (AVA)

The evaluation team applied each EAL 3 AVA CEM work unit. The evaluation team ensured that the TOE does not contain exploitable flaws or weaknesses in the TOE based upon the developer strength of function analysis, the developer vulnerability analysis, the developer misuse analysis, and the evaluation team's misuse analysis and vulnerability analysis, and the evaluation team's performance of penetration tests.

9.9. Summary of Evaluation Results

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 a subset of the vendor tests suite, the independent tests, and the penetration test also demonstrated the accuracy of the claims in the ST.

10. VALIDATOR COMMENTS

The validators note that this is an *extremely limited* TOE: it sets, resets, and tests a password expiration date. Users of this product must be clear that, in and of itself, the product provides *no* enforcement function (i.e., a wrapping application must invoke the product as part of a full implementation of a password expiration mechanism).

11. SECURITY TARGET

Sybase IQ User Administration Security Target, version 1.0, February 8, 2005

12. GLOSSARY

ASA	Adaptive Server Anywhere
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Criteria Testing Laboratory
CEM	Common Evaluation Methodology
CM	Configuration Management
CMP	Configuration Management Plan
DoD	Department of Defense
DBMS	Database Management Server
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards & Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
PP	Protection Profile
SAIC	Science Applications International Corporation
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

TSFI	TOE Security Function Interface
VR	Validation Report

13. BIBLIOGRAPHY

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated August 1999, Version 2.1.

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

[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 1999, Version 2.1.

[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 1999, version 1.0.

[7] Sybase IQ User Administration Security Target, v1.0, 8 February 2005

[8] Evaluation Technical Report for the Sybase IQ User Administration, v1.0, 8 February 2005. Part 1 (Non-Proprietary); Part 2 (Proprietary).

[9] Evaluation Team Test Plan For The Sybase Adaptive Server IQ User Administration, ETR Part 2 Supplement (SAIC and Sybase Proprietary), Version 2.0, November 17, 2004.