Australian Government
Department of Defence

Australasian Information Security Evaluation Program

Certification Report

Certificate Number: 2008/50

16 Dec 2008

Version 1.0

Amendment Record

Version	Date	Description
1.0	29/1/2009	Public release.

Executive Summary

1 The target of evaluation (TOE) is the Passlogix v-GO Access Accelerator Suite Version 6.0 which consists of five Passlogix V-GO Products that make up the Sign-On Platform. It is also sold under the following brand name: Oracle Enterprise Single Signon Suite. The products are identical and are all manufactured by Passlogix, only the brand name is different.

2 The TOE is a middleware product that allows the user to authenticate once, with subsequent automatic detection and handling by the TOE of requests for user credentials from other applications. The TOE also provides features for password reset, suspending or closing inactive sessions and bridging strong authentication using a variety of different authentication mechanisms to applications within the enterprise.

3 This report describes the findings of the IT security evaluation of the TOE to the Common Criteria (CC) evaluation assurance level EAL3 augmented with basic flaw remediation (ALC.FLR.1). The report concludes that the product has met the target assurance level of EAL3 augmented with ALC.FLR.1 and that the evaluation was conducted in accordance with the relevant criteria and the requirements of the Australasian Information Security Evaluation Program (AISEP). The evaluation was performed by stratsec and was completed on 15 November 2008.

4 With regard to the secure operation of the TOE, the Australasian Certification Authority (ACA) recommends that the TOE is:

a) used only in its evaluated configuration;

b) operated according to the administrator guidance (Refs [3][4][5][6][7]);

c) configured so that the self service password reset quiz questions and answers are not researchable; and

d) is checked daily for self service password reset brute force attacks.

5 This report includes information about the underlying security policies and architecture of the TOE, and information regarding the conduct of the evaluation.

6 It is the responsibility of the user to ensure that the TOE meets their requirements. For this reason, it is recommended that a prospective user of the TOE refers to the Security Target at Ref [1], and reads this Certification Report prior to deciding to purchase the product.

Table of Contents

Chapter 1 - Introduction

1.1 Overview

7 This chapter contains information about the purpose of this document and how to identify the Target of Evaluation (TOE).

1.2 Purpose

8 The purpose of this Certification Report is to:

a) report the certification of results of the IT security evaluation of the TOE, Passlogix v-GO Access Accelerator Suite Version 6.0, against the requirements of the Common Criteria (CC) evaluation assurance level EAL3, and

b) provide a source of detailed security information about the TOE for any interested parties.

9 This report should be read in conjunction with the TOE's Security Target (Ref [1]) which provides a full description of the security requirements and specifications that were used as the basis of the evaluation.

1.3 Identification

10 Table 1 provides identification details for the evaluation. For details of all components included in the evaluated configuration refer to section 2.6.1 Evaluated Configuration.

Table 1: Identification Information

Item	**Identifier**
Evaluation Scheme	Australasian Information Security Evaluation Program (AISEP)
TOE	Passlogix v-GO Access Accelerator Suite Version 6.0
Software Version	VGO Single SignOn (SSO), version 6.0 VGO Authentication Manager (AM), version 6.0 VGO Provisioning Manager (PM), version 6.0 VGO Session Manager (SM), version 6.0 VGO Self Service Password Reset (SSPR), version 6.0 V-GO single sign on platform includes the following components: AM 6.0 ROLLUP D

	PM 6.0 ROLLUP D SM 6.0 ROLLUP E SSO 6.0 ROLLUP E SSPR 6.0 ROLLUP D Oracle Branded: ESSO Authentication Manager 10.1.403 ESSO Provisioning Gateway 10.1.403 ESSO Kiosk Manager 10.1.403 ESSO Logon Manager 10.1.403 ESSO Password Reset 10.1.403
Security Target	Passlogix v-GO Access Accelerator Suite Version 6.0
Evaluation Level	EAL3
Evaluation Technical Report	Evaluation Technical Report for Passlogix V-GO Sign-On Platform Product Suite, Version 6.0
Criteria	CC Version 2.3, August 2005, with interpretations as of 14 August 2007
Methodology	Common Criteria, Common Methodology for Information Technology Security Evaluation, Evaluation Methodology August 2005 Version 2.3 CCMB-2005-08-004 with interpretations as of 14 August 2007
Conformance	CC Part 2 Conformant CC Part 3 Augmented with Basic Flaw Remediation. (ALC.FLR.1)
Sponsor	Passlogix.Inc. 75 Broad Street, Suite 815 New York, NY 10004
Developer	Passlogix.Inc. 75 Broad Street, Suite 815 New York, NY 10004
Evaluation Facility	stratsec Deakin House, 1/50 Geils Court DEAKIN ACT 2603, AUSTRALIA

Chapter 2 - Target of Evaluation

2.1 Overview

11 This chapter contains information about the Target of Evaluation (TOE), including: a description of functionality provided; its architecture components; the scope of evaluation; security policies; and its secure usage.

2.2 Description of the TOE

12 The TOE is the Passlogix v-GO Access Accelerator Suite Version 6.0 developed by Passlogix.Inc. It's primary role is to allow the user to authenticate once with subsequent automatic detection and handling by the TOE of requests for user credentials from other applications. The TOE also provides features for password reset, suspending or closing inactive sessions and bridging strong authentication using a variety of different authentication mechanisms to applications within the enterprise.

13 The TOE is a set of interrelated software applications that run in an MS Windows environment that can be described in terms of the following components:

a) VGO SSO, which responds to requests for user credentials from any Windows, Web or Mainframe/Host application. SSO allows the user to authenticate once, with subsequent automatic detection and handling by the TOE of requests for user credentials from other applications. The remaining four products in the VGO SignOn Platform are add-ons to SSO.

b) VGO AM enables organisations to bridge strong authentication to all of their applications, including smart cards, biometrics and Entrust authenticators. Users can employ different authenticators at different times and with different applications.

c) VGO PM provides the ability for an administrator to automatically provision VGO SSO with a user's ID and password by using a provisioning system. An administrator is able to add, modify and delete IDs and passwords for particular applications within the provisioning system and have the changes reflected in VGO SSO.

d) VGO Session Manager (SM) provides a solution that addresses the needs of traditional Single SignOff in a kiosk environment. VGO SM has a clientside agent that suspends or closes inactive sessions and seamlessly shuts down all applications.

e) VGO Self Service Password Reset (SSPR) enables users to reset their own Windows domain passwords without the intervention of administrative or helpdesk personnel. It provides end users with an alternative means of authenticating themselves by taking a quiz comprising a series of passphrase questions.

14 A detailed description of the TOE architecture is available in the Security Target.(Ref[1])

2.3 Security Policy

15 The TOE Security Policy (TSP) is a set of rules that defines how the information within the TOE is managed and protected. The Security Target (Ref [1]) contains no explicit security policy statements.

2.4 TOE Architecture

16 The TOE's major architectural components are described in the Security Target (Ref [1]).

2.5 Clarification of Scope

17 The scope of the evaluation includes only the v-GO SSO application suite. The operating system layer and hardware devices (including proximity readers/cards) were not evaluated. The TOE does not implement authentication or encryption functionality directly; however in the evaluated configuration it does rely on the IT environment through the use of Microsoft Windows authentication and the Microsoft Cryptographic API. In providing security functionality, the TOE relies on the underlying operating system to provide correct details of the site/application requiring authentication to the TOE. As such, if the operating system provides incorrect details to the TOE, the TOE may not behave as expected. It should be noted that a human user would also be fooled in such cases.

2.5.1 Evaluated Functionality

18 The TOE evaluated security functionality is described in detail in the Security Target (Ref [1]).

19 The security functions are

a) Security Audit

b) User Data Protection

c) Identification and authentication

d) Security management

e) Protection of the TSF

f) TOE Access

2.5.2 Non-evaluated Functionality

20 Potential users of the TOE are advised that some functions and services have not been evaluated as part of the evaluation. Potential users of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration; Australian Government users should refer to Australian Government ICT Security Manual (ISM) (Ref [2]) for policy relating to using an evaluated product in an un-evaluated configuration. New Zealand Government users should consult the Government Communications Security Bureau (GCSB).

2.6 Usage

2.6.1 Evaluated Configuration

21 This section describes the configurations of the TOE that were included within scope of the evaluation. The assurance gained via evaluation applies specifically to the TOE in these defined evaluated configuration(s). Australian Government users should refer to Australian Government ICT Security Manual(ISM) (Ref [2]) to ensure that configuration(s) meet the minimum Australian Government policy requirements. New Zealand Government users should consult the Government Communications Security Bureau (GCSB).

22 The TOE is comprised of the software components identified in the Security Target (Ref [1]).

2.6.2 Delivery Procedures

23 When placing an order for the TOE, purchasers should make it clear to their supplier that they wish to receive the evaluated product.

2.6.3 Distribution of Product on Compact Disc

24 In general, clients will download the product themselves from the Extranet. If they request a physical delivery, the Passlogix Office Manager will download the product from the Extranet and ensure product integrity by confirming the hash value. Then the Passlogix Office Manager will burn the ISO onto CD(s) which is then silk-screened with the product name and logo and labelled with the appropriate version number. The CD(s) is/are shipped inside a custom Passlogix CD mailer that is sealed with a sticker. The mailer containing the CD(s) is then shipped inside a sealed FedEx package via overnight delivery with delivery receipt signature required.

2.6.4 Distribution of Product via Passlogix portal

25 Approved customers and partners with appropriate access rights can download the product from the Passlogix portal. Membership to this secure site is private. When account information has been submitted, the

portal administrator is notified and the application is subjected to a screening procedure. If the application is authorised, proper access rights are assigned and notification is sent to the applicant with details on how to access the portal. Each account holder is assigned an individual user ID and password, and specific access rights dependent on their role.

2.6.5 Customer Distribution

26 Passlogix assigns product download rights to the approved technical and management contacts at each customer site. Access to purchased products and subsequent product updates are available for download for the duration of the maintenance agreement.

2.6.6 Channel Partner Distribution

27 Passlogix assigns product download rights to the approved Channel Partner management and technical contacts. Access to all Passlogix products resold by the channel partner is available for download for the duration of the reseller license agreement.

2.6.7 OEM Partner Distribution

28 Passlogix assigns product download rights to the approved OEM Partner management and technical contacts. OEM partners are only allowed to download their own self-branded products. OEM partners do not have access to Passlogix-branded products, or access to other OEM-branded products.

2.6.8 Oracle ESSO Delivery Model

29 The Oracle branded ESSO product is released to Oracle customers through the Oracle Technology Network (OTN), which is Oracle’s largest community of developers, DBAs, and architects using Oracle products and industry-standard technologies. Members collaborate via OTN. The membership to the OTN site is free. The OTN site is password protected and once the customer is a valid member, he/she will login to the OTN site at this location: http://www.oracle.com/admin/account/index.html The Oracle ESSO software downloads are free, and each comes with a Development License that allows customers to use full version of the ESSO products only while developing and prototyping their applications (or for strictly self-educational purposes). In some cases certain downloads (such as Beta releases) have licenses with slightly different terms. Customers can buy Oracle ESSO product with full-use licenses at any time from the sales representative. Oracle ESSO product is currently available for download at this location on the OTN:

30 http://www.oracle.com/technology/software/products/ias/htdocs/101401.html

2.6.9 Determining the Evaluated Configuration

31 To ensure the integrity and authenticity of the product downloaded by the client, Passlogix utilises Hash Tab Shell Extension version 1.9, a publicly available utility that displays the MD5, SHA1 and CRC-32 hashes of a file’s contents. The hashes are posted along with the other download information such as product title and description and are reproduced in Table 2 and Table 3. The client is then able to check the hash after downloading.

32 When a product is released, it is posted to the Extranet for availability. Prior to making it publicly available, it is downloaded on a remote computer to ensure it is a fully functioning product. Once validated on the remote machine, the Hash Tab utility is run and the various hash values are generated. The hash values are then posted to the product description page on the Extranet and the product is made available for client downloads. After downloading the product, clients can then run their own utility to generate hashes and ensure a complete and successful download.

TOE Verification Hashes Table 2.

Toe Component	MD5	Sha1
v-GO AM - v6.00 Rollup D.zip	fdff736958daa966f570734e7a8bb031	25789bc93c181226d381be97990e68c3469a1735
v-GO PM - v6.00 Rollup D.zip	32dbea57880671de4d1b39f546e9131b	5df17e8fa1384524e0e0e4fdbf8840eabc7e0246
v-GO SM - v6.00 Rollup E.zip	bba1b2ebe323d990d2fcd76417169176	9fa0ec79c688f3c5ab8bcdea8bc9a8f503192ede
v-GO SSO - v6.00 Rollup E.zip	c93caa68dc58827ddcf22a8aa3011606	1a14b7760485cb7c722bf333d027e0b8c5937ae7
v-GO SSPR - v6.00 Rollup D.zip	cf510593be5116c3d285a45ffc272107	5dbec02f5a5de49b0086b0a725e056830ed92a61

Oracle Branding Verification Hashes Table 3.

Toe Component	MD5	Sha1
ESSO Authentication Manager 10.1.403.zip	35f8978e6b6326e1a1a849c69f20507e	06ccb033466cb9a8a666b6f00100df26651696b5
ESSO Kiosk Manager 10.1.403.zip	b5bd79696a5bbad74a35c7de28e103ce	b6e5a0844f6ad25947e8466aed6637531475ac09
ESSO Logon Manager 10.1.403.zip	beb8439301bafcffe060f6a30ec7d009	337b685cf1cc9e377a9bec420b30dbfdb334b43e
ESSO Password Reset 10.1.403.zip	d927178bc9609d4ddfdc524719ac7f82	fe7cbdd27ce8d4152429a7f9306613537628194b
ESSO Provisioning Gateway - v10.1.403.zip	89f391c54cd27e19db7beee3289f0cf7	4681756989e2838e2f2e54bf217c1725550bf968

2.6.10 Documentation

33 It is important that the TOE is used in accordance with guidance documentation in order to ensure secure usage. The following documentation is provided by the developer:

a) V-GO Single Sign-On Installation and Setup Guide, version 6.00(Ref [3]).

b) V-GO Authentication Manager Installation and Setup Guide, version 6.0 (Ref [4]).

c) V-GO Provisioning Manager Installation and Setup Guide, version 6.0 (Ref [5]).

d) V-GO Session Manager Installation and Setup Guide, version 6.00(Ref [6]).

e) V-GO Self-Service Password Reset Client Installation and Setup Guide, version 6.00 (Ref [7]).

2.6.11 Secure Usage

34 The evaluation of the TOE took into account certain assumptions about it's operational environment. These assumptions must hold in order to ensure the security objectives of the TOE are met.

35 The following assumptions were made:

a) The TOE will be located within controlled access facilities, which will prevent unauthorised physical access.

b) The IT Environment will protect network communication to and from the TOE from unauthorised disclosure or modification.

c) The TOE will be installed, configured, managed and maintained in accordance with its guidance documentation by administrators who are well trained and not hostile.

Chapter 3 - Evaluation

3.1 Overview

36 This chapter contains information about the procedures used in conducting the evaluation and the testing conducted as part of the evaluation.

3.2 Evaluation Procedures

37 The criteria against which the Target of Evaluation (TOE) has been evaluated are contained in the Common Criteria for Information Technology Security Evaluation (Refs [8] [9] [10]). The methodology used is described in the Common Methodology for Information Technology Security Evaluation (CEM) (Ref [11]). The evaluation was also carried out in accordance with the operational procedures of the Australasian Information Security Evaluation Program (AISEP) (Refs [12][13][14][15]) In addition, the conditions outlined in the Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security (Ref[16]) were also upheld.

3.3 Functional Testing

38 To gain confidence that the developer's testing was sufficient to ensure the correct operation of the TOE, the evaluators analysed the evidence of the developer's testing effort. This analysis included examining test coverage, test plans and procedures and comparing expected and actual results. The evaluators drew upon this evidence to perform a sample of the developer tests in order to verify that the evaluator's test results were consistent with those recorded by the developers.

3.4 Penetration Testing

39 The developer performed a vulnerability analysis of the TOE in order to identify any obvious vulnerability in the product and to show that the vulnerabilities were not exploitable in the intended environment of the TOE. This analysis included a search for possible vulnerability sources in publicly available information.

Chapter 4 - Certification

4.1 Overview

40 This chapter contains information about the result of the certification, an overview of the assurance provided by the level chosen, and recommendations made by the certifiers.

4.2 Certification Result

41 After due consideration of the conduct of the evaluation as witnessed by the certifiers and of the Evaluation Technical Report (Ref [17]) the Australasian Certification Authority certifies the evaluation of Passlogix v-GO Access Accelerator Suite performed by the Australasian Information Security Evaluation Facility, stratsec.

42 Stratsec has found that Passlogix v-GO Access Accelerator Suite upholds the claims made in the Security Target (Ref [1]) and has met the requirements of the Common Criteria (CC) evaluation assurance level EAL3.

43 Certification is not a guarantee of freedom from security vulnerabilities.

4.3 Assurance Level Information

44 EAL3 provides assurance by an analysis of the security functions, using a functional and interface specification, guidance documentation, and the high-level design of the TOE, to understand the security behaviour.

45 The analysis is supported by independent testing of the TOE security functions, evidence of developer testing based on the functional specification and high-level design, selective independent confirmation of the developer test results, strength of function analysis, and evidence of a developer search for obvious vulnerabilities (e.g. those in the public domain).

46 EAL3 also provides assurance though the use of development environment controls, TOE configuration management, and evidence of secure delivery procedures.

4.4 Recommendations

47 Not all of the evaluated functionality present in the TOE may be suitable for Australian and New Zealand Government users. For further guidance, Australian Government users should refer to Australian Government ICT Security Manual (ISM) (Ref [2]) and New Zealand Government users should consult the Government Communications Security Bureau (GCSB).

48 In addition to ensuring that the assumptions concerning the operational environment are fulfilled and the guidance document is followed (Ref [3][4][5][6][7]), the ACA also recommends that users and administrators do not use researchable questions and answers when constructing the Self Service Password Reset (SSPR) quiz.

49 During the evaluation the evaluators determined that the following points should be considered when deploying v-GO Access Accelerator Suite Version 6.0

a) It should be noted that user accounts do not have to be locked out in order to use v-go self service password reset. As such it is recommended that the administrator should review the self service password reset management logs daily in order to detect brute force attacks against the SSPR.

b) In some configurations of the environment it is possible to bypass the TOE encryption settings, particularly in domain environments. The bypass may not be apparent to the end user or administrator, i.e. the configuration can appear to show encryption is enabled when it is not. As such, the evaluators recommend that the administrators of the TOE verify that the encryption is enabled through other means, particularly for the synchronisation of user credentials to Active Directory.

Annex A - References and Abbreviations

A.1 References

[1] Passlogix V-GO Sign-On Platform Product Suite Version 6.0, Security Target Version 1.0, November 16 2008.

[2] Australian Government ICT Security Manual (ISM) 2008 Defence Signals Directorate, (available at www.dsd.gov.au).

[3] V-GO Single Sign-On Installation and Setup Guide, version 6.00

[4] V-GO Authentication Manager Installation and Setup Guide, version 6.0

[5] V-GO Provisioning Manager Installation and Setup Guide, version 6.0

[6] V-GO Session Manager Installation and Setup Guide, version 6.00

[7] V-GO Self-Service Password Reset Client Installation and Setup Guide, version 6.00

[8] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model (CC), Version 2.3, August 2005, CCMB-2005-08-001, Incorporated with interpretations as of 2007-8-14

[9] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements (CC), Version 2.3, August 2005, CCMB-2005-08-002, Incorporate with interpretations as of 2007-8-14

[10] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements (CC), Version 2.3, August 2005, CCMB-2005-08-003, Incorporate with interpretations as of 2007-8-14

[11] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology (CEM), Version 2.3, August 2005, CCMB-2005-08-004, Incorporated with interpretations as of 2007-8-14

[12] AISEP Publication No. 1 – Program Policy, AP 1, Version 3.1, 29 September 2006, Defence Signals Directorate.

[13] AISEP Publication No. 2 – Certifier Guidance, AP 2. Version 3.1, 29 September 2006, Defence Signals Directorate.

[14] AISEP Publication No. 3 – Evaluator Guidance, AP 3. Version 3.1, 29 September 2006, Defence Signals Directorate

[15] AISEP Publication No. 4 – Sponsor and Consumer Guidance, AP 4. Version 3.1, 29 September 2006, Defence Signals Directorate

[16] Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, May 2000

[17] Evaluation Technical Report for Passlogix V-GO Sign-On Platform Product Suite, Version 6.0, 16 November 2008.

A.2 Abbreviations

AISEF	Australasian Information Security Evaluation Facility
AISEP	Australasian Information Security Evaluation Program
CC	Common Criteria
CEM	Common Evaluation Methodology
DSD	Defence Signals Directorate
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GCSB	Government Communications Security Bureau
ISM	Australian Government ICT Security Manual
PP	Protection Profile
SFP	Security Function Policy
SFR	Security Functional Requirements
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy