



CCT MARK TEST REPORT SUMMARY

IBM

Virtual Infrastructure Access Services
Version 5.5b

VENDOR DETAILS	TEST LABORATORY DETAILS
IBM UK Ltd	West Coast Labs
PO Box 41, North Harbour Portsmouth, PO6 3AU	William Knox House, Britannic Way, Llandarcy, Swansea, SA10 6EL
Telephone Number: +44 (0) 1926 880892	Telephone Number: +44 (0) 1792 324000

Test Report Summary Issue Date: 28/06/07
--

Further details about the claims tested are included in the Information Assurance Claims Document (CCT Mark Certificate Number 2006/06/0024) published on the CCT Mark website (www.cctmark.gov.uk)

1 Test Result

- 1.1. The CSIA claims testing of the Virtual Infrastructure Access Services during June 2007 by West Coast Labs concluded that the security functionality claims made within the IA Claims Document [ICD] are valid for this IS Product.

2 References

[ICD] The IA Claims Document published for the Virtual Infrastructure Access Services version 5.5b published on the CCT Mark website.

[SHOWCASE] There was no administration guide as West Coast Labs tested against a SHOWCASE environment that was preconfigured by IBM.

[TLG] This report has been compiled using the CCT Mark Test Laboratory Guide Issued v2.3.0.doc.

[VIAS] West Coast Labs were supplied with a document entitled "The VIA Showcase access instruction – Client Side" which demonstrated how to access the product. Version number 1, document creation date: 5th January 2007

3 Scope of Testing

- 3.1. The Virtual Infrastructure Access Services version 5.5b was tested using the Test Method version 1.3 supplied by West Coast Labs included in, and against the claims made in the [ICD].
- 3.2. The following features of Virtual Infrastructure Access Services version 5.5b were not tested under the CCT Mark Scheme:
 - RSA SecurID Testing

- Client Operating Systems other than Windows XP
- IBM Java version 5
- Internet Browsers other than Internet Explorer
- Client specific applications.
- IBM Professional Services.

3.3. The version of the IBM Virtual Infrastructure Access Service tested by West Coast Labs was 5.5b that is hosted on their SHOWCASE environment.

3.4. The Claims Tests were conducted at West Coast Labs' premises in Llandarcy and at IBM's Birmingham Road facility in Warwick. Testing was conducted at both locations with some witnessing also being performed in Warwick.

3.5. The following platform combinations were used:

Operating System	Version
Red Hat Enterprise Linux (ES)	3 Update 8
Microsoft Windows Server Standard Edition	2003
IBM Java 2 JRE	1.4.1-8
IBM Java 2 SDK	1.4.1-9
IBM HTTP Server	1.3.28
IBM MQ Series	6.0.0
IBM DB2	8.2 FP5
IBM Tivoli Directory Server (includes GSKit 7.0.1.16)	5.0 FP3
IBM WebSphere Portal Enable for Multiplatforms	5
IBM Virtual Infrastructure Access Services	5.5b

3.6. For each client used, the operating system was

Operating System	Browser	Version
Windows XP SP2 with Sun's Java Runtime environment JRE 1.4.2 installed (version 1.4.2_14 build b05) and the KB884020_x86_enu Windows patch installed	Internet Explorer	6.0.2900.2180.xp_sp_sp2_rtm.040803-2185

4 Ease of Use

4.1. Installation of the product:

4.1.1 The testing was conducted using IBM's SHOWCASE environment that has been pre-set up in IBM's Warwick facility. It is recommended by IBM that their technical services personnel are involved in any installation and initial configuration due to the complexity of the solution.

4.1.2 From the client side, installation involved following some printed instructions provided by IBM, and was limited to altering the hosts file on the Windows client, downloading and installing the Java Runtime Environment and then connecting to a web page.

4.2. Notes for an administrator:

4.2.1 The administrator should note that with any internet facing security product it is important for system administrators and network personnel to always follow the recommended set up and hardening procedures.

4.2.2 West Coast Labs also recommend that products that do not include firewall or IPS technology as part of the core functionality should

always be protected by a firewall and/or signature/anomaly based IPS solution.

- 4.2.3 It is important to note that the backend servers providing VIA services should have user control policies implemented that are consistent with an organisation's security policy – for example if users are not allowed to download and install software from the internet on their desktop machines, they should not be allowed to do so on the backend servers.
- 4.2.4 It should also be noted that an administrator can potentially have separate passwords to get into the main VIA environment and then into the VIA Administration web interface – if a change is required, both should be changed simultaneously as it is currently possible to use a direct URL entry to get into the VIA Admin web interface without being tunnelled via VIA.
- 4.2.5 It is important to note that the hardware configuration tested might not be acceptable to an Accreditor, as currently VLANS provide no recognised security separation. Furthermore, the CCT Mark process has not tested the security of VLANS in its testing.
- 4.2.6 It is also important to note that SHOWCASE is a publicly accessible demonstration environment and that an installation into a customer site may vary from what was tested.
- 4.2.7 It is recommended by IBM that their technical services personnel are involved in any installation and initial configuration due to the complexity of the solution.
- 4.2.8 With any internet facing security product it is important for system administrators and network personnel to always follow the recommended set up and hardening procedures.

5 **Quality of User and Administration Documentation**

- 5.1. West Coast Labs were supplied with a document entitled “The VIA Showcase access instruction – Client Side” [VIAS] which demonstrated how to access the product.
- 5.2. The engineers that conducted the testing were briefed on the functionality of the product by IBM technical staff. IBM provided an engineer at Warwick to provide technical support to the WCL testing engineer on site during the testing period.

6 **Resistance to Publicly Known Vulnerabilities**

- 6.1. Given the scope of the SHOWCASE environment, a selection of vulnerabilities were targeted against the public IP addresses of the servers, and each was found to repel the attempt.

7 **Validation of Existing Assurance Certificates**

- 7.1. Not applicable

8 **Disclaimer**

CSIA Claims Testing is not a guarantee of freedom from security vulnerabilities. There remains a probability that exploitable security vulnerabilities may exist in the IS Product, IS Service or the Information Systems environment supporting the IS Product or IS Service. The issue of a Test Report Summary is not an endorsement of a product or service.

This Test Report Summary serves solely to summarise the results of the testing carried out for the CCT Mark Scheme and should not be taken as an endorsement or otherwise of the IS product or IS Service.

9 Abbreviations

CCT	CSIA Claims Tested Mark
IA	Information Assurance
ICD	Information Assurance Claims Document
IS	Information Systems
VLANS	Virtual Local Area Networks
VIA	Virtual Infrastructure Access
LDAP	Lightweight Directory Access Protocol
SSO	Single Sign-On
HTTP	Hypertext Transfer Protocol
SSL	Secure Sockets Layer
WCL	West Coast Labs
IP	Internet Protocol