National Information Assurance Partnership


TM

# Common Criteria Evaluation and Validation Scheme Validation Report

## Perceptive Software, Inc., ImageNow v5.42 SP3 and WebNow v3.42

**Report Number:** **CCEVS-VR-06-0056**
**Dated:** **10 January 2007**
**Version:** **1.0**

**National Institute of Standards and Technology**
**Information Technology Laboratory**
**100 Bureau Drive**
**Gaithersburg, MD 20899**
**6740**

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

## ACKNOWLEDGEMENTS

### Validation Team

Shaun Gilmore
Santosh Chokhani
Common Criteria Evaluation and Validation Scheme

### Common Criteria Testing Laboratory

Science Applications International Corporation
Columbia, Maryland

# Table of Contents

# 1 Executive Summary

The evaluation of the Perceptive Software ImageNow v5.42 SP3 and WebNow v3.42 commenced on 01-05-06 and was completed on 15 November 2006. The Perceptive Software ImageNow v5.42 SP3 and WebNow v3.42 evaluation was performed by Science Applications International Corporation (SAIC) in the United States. The evaluation was conducted in accordance with the requirements drawn from the Common Criteria CCv2.3, Part 2, and Part 3 Evaluation Assurance Level 2 augmented with ALC_FLR.2 and AVA_MSU.1 requirements.

The Perceptive Software ImageNow v5.42 SP3 and WebNow v3.42 product identified in this Validation Report has been evaluated at an accredited testing laboratory using the Common Methodology for IT Security Evaluation (Version 2.3) for conformance to the Common Criteria for IT Security Evaluation (Version 2.3). This Validation Report applies only to the specific versions of the Perceptive Software ImageNow v5.42 SP3 and WebNow v3.42 products. The evaluation has been conducted in accordance with the provision 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 produced. This Validation Report is not an endorsement of the Perceptive Software ImageNow v5.42 SP3 and WebNow v3.42 products by any agency of the U.S. Government and no warranty of the product is either expressed or implied.

Science Applications International Corporation (SAIC) is certified by the NIAP validation body for laboratory accreditation. The CCTL has presented CEM work units and rationale that are consistent with the CC [Common Criteria], the CEM [Common Evaluation Methodology] and CCEVS publication number 4 Guidance to CCEVS Approved Common Criteria Testing Laboratories. The CCTL evaluation team concluded the requirements from Common Criteria CCv2.3, Part 2 and Part 3 Evaluation Assurance Level 2 augmented with ALC_FLR.2 and AVA_MSU.1 requirements have been met.

The TOE is a document imaging, management and workflow solution based on a client/server architecture that provides a user the ability to scan, file, retrieve, print, fax or distribute electronic objects. Because the TOE can support widespread imaging within an entire network, it provides security auditing, thorough security management functionality, and secure data transfer when accessing stored images via WebNow or the ImageNow Client.

The TOE offers users the flexibility of deployment options and configurations that allow choices for distributed document capture, indexing, storage and management capabilities. ImageNow can simultaneously manage scanning along with the importing of object data from multiple sources, such as fax servers, mail servers, or a network location.

The TOE allows images to be indexed and tracked by 20 different data elements and six user-defined index values. An unlimited number of keywords can be assigned to a document, enabling the user to retrieve specific information. ImageNow also has a LearnMode to ‘learn’ the host application screen. From the host application screen, a user retrieves the desired transaction. The user presses the ImageNow icon from the windows system tray and ImageNow retrieves all associated documents linked to the current displayed transaction. The toolbars in ImageNow provide the user with the ability to annotate key points on the document without altering original integrity, distribute the document via print, fax, or e-mail, and view multiple documents that are linked to the current displayed document.

## Interpretations

This evaluation used the Common Criteria for Information Technology Security Evaluation Parts 2 and 3, Version 2.3, August 2005. The evaluation started in January 2006; therefore no additional interpretations existed to be applied.

# 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 CCTLs or candidate CCTLs using the Common Evaluation Methodology (CEM) for 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 and candidate 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 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;
- The organizations and individuals participating in the evaluation.

**Table 1: Evaluation Identifiers**

| Item | Identifier |
|---|---|
| Evaluation Scheme | United States NIAP Common Criteria Evaluation and Validation Scheme |
| Target of Evaluation | The TOE consists of the Perceptive Software ImageNow v5.42 SP3 and WebNow v3.42 |
| Security Target | Perceptive Software, Inc. ImageNow v5.42 SP3 and WebNow v3.42 Security Target Version 1.0, 10 January 2007 |
| Evaluation Technical Report | Evaluation Technical Report For Perceptive Software, Inc. ImageNow v5.42 SP3 and WebNow v3.42 Part 1 Version 3.0, 10 January 2007 |
| Conformance Result | EAL 2 augmented with ALC_FLR.2 and AVA_MSU.1 |
| Sponsor | Perceptive Software, Inc.<br>22701 W. 68th Terr<br>Shawnee, KS 66226 |
| Common Criteria Testing Lab (CCTL) | Science Applications International Corporation<br>7125 Columbia Gateway Drive, Suite 300<br>Columbia, MD 21046-2554 |
| CCEVS Validator(s) | Shaun Gilmore<br>National Security Agency<br><br>Santosh Chokhani<br>Orion Security Solutions |

# 3 TOE Security Services

The security services provided by the TOE are summarized below:

## 3.1 Security audit

ImageNow generates an audit record for audit mechanism start-up and shutdown events, as well as viewing, deleting, and re-indexing images. Each audit record includes the date and time of the event, type of event, subject identity, the IP and MAC addresses where the event occurred, and the outcome of the event. An Owner can review the audited records and can select the auditable events. In addition, ImageNow provides audit selection capabilities for reviewing audit data. The audit events are stored on the underlying operating system. The Information Technology (IT) environment provides a reliable timestamp for audit use and the protection of the audit records.

## 3.2 User data protection

ImageNow enforces rules-based access control on users and groups. The Owner or Manager has the ability to grant access (known as privileges) on the drawer objects that contain document pages.

## 3.3 Identification and authentication

ImageNow maintains a list of security attributes for users and requires users to be authorized prior to granted access to protected functions as security attributes are associated to users. The TOE relies on the IT environment to authenticate users using user and password mechanisms provided by directory services

## 3.4 Security management

ImageNow restricts the ability to manage user security policy rules. This is accomplished in a manner similar to that employed to control access to drawers – global privileges are required to successfully perform specific security management and other TOE functions. ImageNow provides the functions necessary for effective management of the security functions and all actions are accomplished on the Client with the exception of auditing, as that is accomplished via the ISA console.

# 4 Assumptions

## 4.1 Physical Security Assumptions

It is assumed that appropriate security is provided within the environment of the TOE for the value of the IT assets protected by the TOE and the value of the stored, processed, and transmitted information.

## 4.2 Personnel Security Assumptions

It is assumed that authorized administrators are non-hostile, appropriately trained and follow all administrator guidance.

# 5 Architectural Information

The TOE is comprised of the following components: ImageNow Server (which contains ISA, Intool, the ImageNow database, and the Object Storage Manager, OSM), ImageNow Client, and WebNow.

## 5.1 ImageNow Server

The ImageNow Server subsystem contains the following modules: OSM, ImageNow database, ISA, and Intool. The ImageNow Server provides all user authorization, document capture, indexing, retrieval, and workflow functions and includes the ImageNow Server Administrator (ISA) to manage services, logging, and auditing. Although the ImageNow Server provides the overriding security functionality, the only function where the Owner (i.e., highest level administrator) must log on to ISA directly is to manage the logs (i.e., audit). All other security management functions are handled on the ImageNow Client.

### 5.1.1 OSM

The documents are stored in the Object Storage Manager (OSM) as document objects. The OSM requires a high capacity and high availability storage system, such as Redundant Array of Independent Disks (RAID) 5. The OSM needs to be directly accessible by the ImageNow Server. The OSM can be installed on a separate server because the object store for the scanned images and other documents can grow quite large.

### 5.1.2 ImageNow Database

The ImageNow database stores the metadata of each document. ImageNow includes an embedded database in one of its evaluated configurations. Third party databases can be used in additional supported evaluated configuration to provide the same functionality.

### 5.1.3 ISA

The ImageNow Server Administration (ISA) is the administrator console used to control the ImageNow Server. ISA enables an Owner, or a Manager or User given ISA privilege, to manage ImageNow Server on Microsoft Windows. Using ISA, users with the appropriate privileges can customize ImageNow Server configuration (.ini) files, manage and mirror storage locations, and monitor, audit, instant message, and disconnect users. ISA also provides a way to supervise specific ImageNow Clients or groups for auditing purposes, view all database tables, workflow queues, and locked documents, and monitor the number of user licenses being used compared with the number of licenses available. ISA can also be used to view real-time interaction between users and ImageNow Server for real-time troubleshooting, as well as view, save, print, and e-mail server log files using the Log and Activity Viewers.

### 5.1.4 Intool

This command-line tool is provided as a tool that provides information about the Owner outside of ISA. This tool provides a mechanism to change the Owner if needed. Intool provides many of the options available in ISA for ImageNow Servers running on UNIX platforms.

### 5.1.5 Auditing Scripts

ImageNow Server contains an auditing script called apply_cc_audit. This script establishes the auditing claimed in this evaluation.

## 5.2 WebNow

The WebNow component is a separate browser-based interface that works seamlessly with the ImageNow Server to provide web-based access to the stored images via a Secure Sockets Layer (SSL) over standard TCP/IP. The WebNow Server application enables users to view and work with ImageNow documents using a Web browser. The WebNow component enables ImageNow functionality to be used over a highly distributed Wide Area Network (WAN).

Users access WebNow from their client computer by supplying a URL to WebNow in a web browser. From their browser connection to WebNow, users can view and search documents stored in ImageNow, and participate in workflows created in the ImageNow Client. User permissions are set in the ImageNow Client.

### 5.3 ImageNow Client

The Client is a desktop interface that provides access to all ImageNow functions such as document capture, viewing, searching, indexing documents, and creating and participating in workflows. Users are created and permissions are granted using ImageNow Client.

ImageNow Client connects directly to the ImageNow Server Scanning, and indexing operations are conducted in the ImageNow Client. Third, Perceptive Software's LearnMode technology exists only in the ImageNow Client.

The Individual TOE components are depicted below.

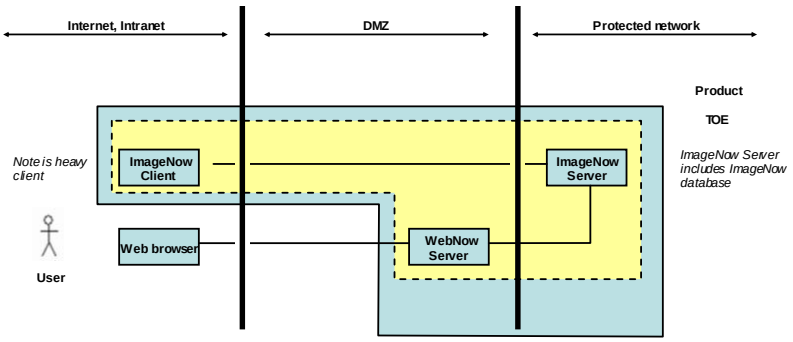



**Figure 1: TOE boundary**

In Figure 1, the communication between the ImageNow Server and the ImageNow Client, and the ImageNow Server and WebNow should be protected as deemed necessary. The TOE can be configured to use a Perceptive Software, Inc. implementation of 3DES over TCP/IP to help make the links more secure. However, that implementation has not been FIPS or otherwise certified. As such, this ST assumes that the links would be protected to the degree necessary by available external means (e.g., physical network protection or some VPN technology). Note that in a closed enterprise network enclave it may be the case that, if the network users are suitably trusted not to actively attempt to circumvent the security mechanisms of the TOE, the network communications would not need to be protected.

# 6 Documentation

Following is a list of the evaluation evidence, each of which was issued by the developer (and sponsor):

### Design documentation

| Document | Version | Date |
|---|---|---|
| Perceptive Software, Inc.<br>ImageNow Functional Specification for<br>Common Criteria Evaluation<br>of ImageNow 5.42 | Version 1.2 | 14 September 2006 |

| | | |
|---|---|---|
| Perceptive Software, Inc.<br>ImageNow High-Level Design for<br>Common Criteria Evaluation of<br>ImageNow 5.42 | Version 1.4 | 14 September 2006 |

**Guidance documentation**

| Document | Version | Date |
|---|---|---|
| ImageNow Administrator Guide<br>for ImageNow 5.4x | | 6 February 2006 |
| ImageNow End-User Guide for<br>ImageNow 5.4x | | 6 February 2006 |
| ImageNow Server Administration (ISA) Guide<br>for ImageNow 5.4x | | 27 March 2006 |
| ImageNow WebNow Guide for<br>WebNow 3.4x | | 27 March 2006 |

**Configuration Management documentation**

| Document | Version | Date |
|---|---|---|
| ImageNow Perceptive Software,<br>Configuration Management | Version 1.4 | 3 July 2006 |

**Delivery and Operation documentation**

| Document | Version | Date |
|---|---|---|
| ImageNow, Perceptive Software, Inc.<br>Delivery and Ops: Delivery Procedures | Version 1.4 | 18 October 2006 |
| ImageNow, Perceptive Software, Inc.,<br>ImageNow Installation Guide for<br>ImageNow 5.42x | Version 1.3 | 9 January 2007 |
| ImageNow, Perceptive Software, Inc.<br>WebNow Installation Guide for<br>WebNow 3.4 | | 16 March 2006 |

**Life Cycle documentation**

| Document | Version | Date |
|---|---|---|
| Perceptive Software, Inc.<br>Life Cycle Support – Flaw Remediation | | 31 May 2006 |

**Test documentation**

| Document | Version | Date |
|---|---|---|
| Test Cases For Common Criteria Evaluation<br>of ImageNow 5.42x and WebNow 3.42x, | Version 1.1 | 30 October 2006 |

**Vulnerability Assessment documentation**

| Document | Version | Date |
|---|---|---|
| Vulnerability Assessment | Version 1.1 | 14 September 2006 |

**Security Target**

| Document | Version | Date |
|---|---|---|
| Perceptive Software, Inc.<br>ImageNow v5.42 SP3 and WebNow v3.42 | | |

# 7 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team.

## 7.1 Developer Testing

Perceptive's approach to security testing for the TOE was security functional requirement based. Essentially, Perceptive developed a set of test cases that corresponded to a security functional requirement. Each set of test case(s) was subdivided into security functions and each test procedure targeted the specific security behavior associated with that security function. The test procedures were designed to be exercised manually using the subsystem interfaces. The general testing philosophy and goal for each of the functional areas described in the ST is outlined below.

**Security Audit**
The goal of these test procedures was to test the generation of audit records and the association of audit records with the identity of the user that caused the event; as well as success or failure.

**User Data Protection**
The goal of these test procedures was to demonstrate how the TOE can control access to objects where the objects are the Drawers. Each object had an access control list (ACL) that included the user ID, group information, and permissions/privileges.

**Identification and Authentication**
The goal of these test procedures was to test how the TOE defined users in terms of security attributes that included user name (user ID), group ID, and privileges. The IT environment was relied on to authenticate the user's ID. The test procedures further demonstrated how the TOE offerd no TSF-mediated functions until the user was identified and authenticated.

**Security Management**
The goal of these test procedures was to test how the TOE provided the ISA console to the Owner and Manger to read audit records and the ImageNow Client to an Owner and Manager that can be used to manage the TSF. The tests also demonstrated how the TOE maintains Owner, Manager, and user roles.

## 7.2 Evaluation Team Independent Functional Testing

This section summarizes the team's test coverage analysis approach. The correspondence between security functions and interfaces is clearly defined in the functional specification and need not be repeated here.

The team test cases are categorized according to the security function. The evaluation team tests were derived based on perceived gaps or areas of weakness in the developer's test suite based on the preceding coverage and depth analyses. Although the developer's testing was considered adequate, the evaluators also analyzed and tested each of the security functions as defined in the Security Target and as outlined below.

**Security Audit**
The evaluation team determined multiple gaps in vendor testing that needed to be verified through independent analysis in terms of audit functionality. Namely, the evaluation team tested and confirmed that the TSF shall provide the capability for the Owner and the Manager to read the audit logs; that the TSF only provides the Owner and the Manager the capability to read the audit logs; and that the TSF shall generate audit records for unsuccessful auditable events. There was one detailed test case run for each of the audit functionality cases described.

**User Data Protection**

The evaluation team determined that the vendor test procedures are thorough in ensuring all users are subjected to the access control policies before access to the TOE and its data is granted. The evaluation team did not identify additional functional tests for this security function.

**Identification and Authentication**
There was one additional test case run by the evaluation team to completely test the I&A functionality of the product. The additional test case ensured that the TSF maintains security attributes for users.

**Security Management**
Two additional security management test cases were added to the vendor test suite and verified by the evaluation team. The evaluation team tested that a normal user cannot access the ISA or perform security management functions, unless explicitly granted access and that a normal user cannot create or manage users, unless explicitly granted access.

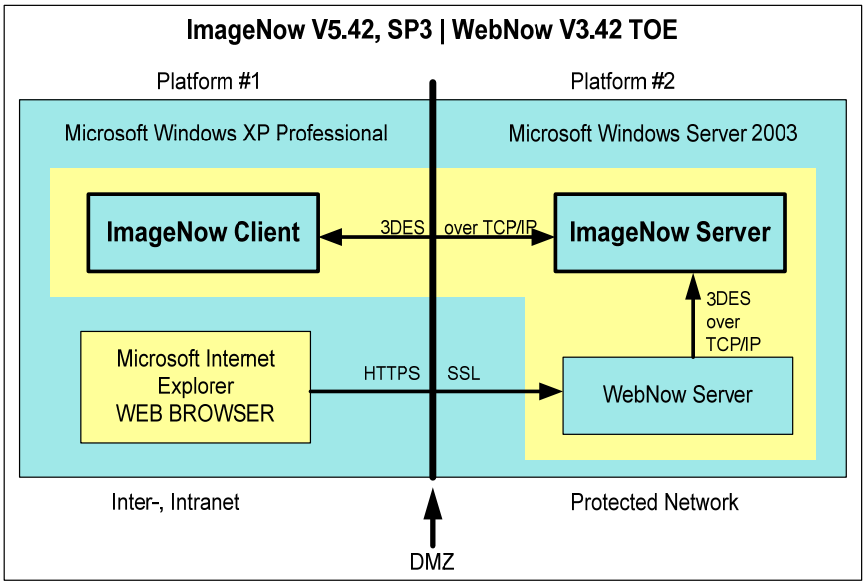
### 7.3 Evaluation Team Independent Penetration Testing

The evaluators also executed a number of tests to determine whether the TOE is vulnerable to attacks aimed at bypassing the security functions or subverting the basic protection mechanisms. The evaluation team also did an open source vulnerability search to ensure the vulnerability analysis did not miss any well-known vulnerability. The public domain search determined there were no security alerts or advisories for the product. The evaluation team independently identified and tested two potential vulnerabilities and determined in both cases that the vulnerability was properly mitigated by the product.

## 8 Evaluated Configuration

The TOE was made available at the Vendor facility in Shawnee, KS. The evaluation team followed the procedures in the ImageNow Installation Guide document and WebNow Installation Guide to download the software and install the TOE on the test platforms.

The evaluation team exercised all manual developer and independent tests against the evaluated configuration of the TOE running on the Windows platforms where the following diagram depicts the test configuration and the hardware and software components are summarized in the subsequent sections. The Vendor ran all of the test cases on the supported operating systems on the Windows and Solaris platforms.




**Hardware**

The following hardware is necessary to create the test configurations as depicted above:

- Windows Platform (ImageNow Server and ImageNow Client)
    - Any x86 machine that that is certified as Windows 2000, Windows XP, or Windows 2003 compatible (including a suitable monitor for the operating system that supports 1280 x 1024 SVGA screen resolution). The machines used for testing were Dell Optiplex GX620, P4, 3ghz with 1GB of RAM.
    - At least 1GB hard disk. The hard drive was a 37 GB.

**Software**

- The following software is required to be installed on the machines used for the test:
- TOE Software
    - ImageNow v5.42 and WebNow v3.42. The ImageNow component was updated to address an issue with auditing so testing was completed with ImageNow v5.42 SP3 and WebNow v3.42
- IT Environment Software
    - Microsoft Windows 2000, 2003, or XP Professional, version SP2.
        - The evaluator installed the ImageNow Server on Windows 2003 Service Pack 1 Version 5.2 R2, Build 3790.SRV03_SP1_RTM.050324-1447
        - The evaluator installed the ImageNow client and WebNow on Windows XP Professional Version 5.1 Service Pack 2, Build 2600.XPSP_SP2_GDR.050301-1519
    - Required applications
        - ImageNow Server
            - Adobe Flashplayer and Active X
            - Apache Tomcat 5.0
            - MS SQL Server 2000
            - J2SE Development Kit 5.0 Update 9

        - J2SE Runtime Environment 5.0 Update 9
    - ImageNow Client and WebNow.
        - Adobe Download Manager
        - Adobe Reader 7.0.7
        - Broadcom Gigabit Intergrated Controller
        - Intel (R) Graphics Media Excel Driver
        - Live Update 2.6
        - Macro Media Flash Player 8
        - Symantec AntiVirus
        - Windows Installer 3.1 (KB893803)

# 9 Validator Comments

The TOE developer and sponsor, and the Evaluation Team are commended for their effort in developing tests for the Perceptive Software ImageNow v5.42 SP3 and WebNow v3.42 products. All test plans were clear, complete, and comprehensible.

Although the ST states the Sun Microsystems Solaris 8, 9 and 10 as supported platforms no evaluation team tests were run to verify any security claims associated with the Sun operating systems. The evaluation team did receive vendor test results and reviewed them for completeness and correctness however no independent verification of those results were performed.

It is important to emphasize that the distributed TOE components should contain FIPS validated cryptographic algorithm protection with a FIPS validated key management scheme. However, the links are encrypted with an algorithm that is not FIPS certified and was not tested during the evaluation. Furthermore, there is no information on the key management scheme utilized. The protection of these links is a critical component to the security of the product but there are no security claims for these protections.

# 10 Security Target

Perceptive Software, Inc. ImageNow v5.42 SP3 and WebNow v3.42 Security Target Version 1.0, 10 January 2007

# 11 List of Acronyms

| | |
|---|---|
| CC | Common Criteria |
| CCEVS | Common Criteria Evaluation and Validation Scheme |
| CCTL | Common Evaluation Testing Laboratory |
| CEM | Common Evaluation Methodology |
| EAL | Evaluation Assurance Level |
| ETR | Evaluation Technical Report |
| MFD | Multifunction Device |
| NIAP | National Information Assurance Partnership |
| NIST | National Institute of Standards & Technology |
| NSA | National Security Agency |
| PP | Protection Profile |
| ST | Security Target |
| TOE | Target of Evaluation |
| TSF | TOE Security Function |
| TSFI | TOE Security Function Interface |

.

# 12 Bibliography

The validation team used the following documents to prepare the validation report.


1. Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 2.3, August 2005.
2. Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 2.3, August 2005.
3. Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements, Version 2.3, August 2005.
4. Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 2.3, August 2005.
5. Part 2: Evaluation Methodology, Supplement: ALC_FLR - Flaw Remediation, Version 1.1, February 2002, CEM-2001/0015R
6. Evaluation Technical Report for Perceptive ImageNow v5.42 SP3 and WebNow v3.42 Final ETR Part 2, Proprietary.
7. Perceptive Software, Inc., ImageNow v5.42 SP3 and WebNow v3.42 Security Target, Version 1.0, 10 January 2007.
8. NIAP Common Criteria Evaluation and Validation Scheme for IT Security, Guidance to Common Criteria Testing Laboratories, Version 1.0, March 20, 2001.


# 13 Interpretations

This evaluation used the Common Criteria for Information Technology Security Evaluation Parts 2 and 3, Version 2.3, August 2005. The evaluation started in January 2006; therefore no additional interpretations existed to be applied.