# National Information Assurance Partnership

TM

# Common Criteria Evaluation and Validation Scheme
# Validation Report

# CA Identity Manager r12.5

**Report Number: CCEVS-VR-VID10341-2010**
**Version 1.0**
**July 27, 2010**

**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**

# Table of Contents

# 1 Executive Summary

The Target of Evaluation (TOE) is r12.5 of the CA Identity Manager with the IMr12.5CommonCriteriaPatch applied. The TOE was evaluated by the Booz Allen Hamilton Common Criteria Test Laboratory (CCTL) in the United States and was completed in July 2010. The evaluation was conducted in accordance with the requirements of the Common Criteria, Version 3.1 Revision 2 and the Common Methodology for IT Security Evaluation (CEM), Version 3.1 Revision 2. The evaluation was for Evaluation Assurance Level 3 (EAL3) augmented with ALC_FLR.1 (Basic Flaw Remediation) and ASE_TSS.2 (TOE Summary Specification). The evaluation was consistent with National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site (www.niap.ccevs.org).

CA Identity Manager (IM) is an integrated identity management platform that automates the creation, modification, suspension or deletion of user identities and their access to enterprise resources. Through these functions, Identity Manager manages diverse user populations on a range of enterprise systems, from mainframes to web applications over a single tool. Identity Manager also provides TOE users with the functionality to manage and delegate Password Management, Provisioning/Deprovisioning, and Identity Administration to the level deemed necessary.

The CA Identity Manager product, when configured as specified in the installation guides and user guides, satisfies all of the security functional requirements stated in the TOE's Security Target.

Although the vendor has asserted that they tested the cryptography used in this product, the cryptography is not FIPS-certified, nor was it analyzed or tested for conformance to cryptographic standards during this evaluation.

The technical information included in this report was largely derived from the Evaluation Technical Report and associated test reports produced by the evaluation team. The *CA Identity Manager 12.5 Security Target version 2.0, dated 21 June 2010* identifies the specific version and build of the evaluated TOE. This Validation Report applies only to that ST and is not an endorsement of the CA Identity Manager product by any agency of the US Government and no warranty of the product is either expressed or implied.

# 2 Evaluation Details

| | |
|---|---|
| **Evaluated Product** | CA Identity Manager r12.5 with the *IMr12.5CommonCriteriaPatch* applied |
| **Sponsor & Developer** | CA, Inc., Framingham, MA |
| **CCTL** | Booz Allen Hamilton, Linthicum, Maryland |
| **Completion Date** | July 2010 |
| **CC** | *Common Criteria for* |

| | |
|---|---|
| | *Information Technology Security Evaluation*, Version 3.1 Revision 2, September 2007 |
| **Interpretations** | None. |
| **CEM** | *Common Methodology for Information Technology Security Evaluation*, Version 3.1 Revision 2, September 2007 |
| **Evaluation Class** | EAL3 Augmented ALC_FLR.1 and ASE_TSS.2 |
| **Description** | The TOE is the Identity Manager r12.5 software with the *IMr12.5CommonCriteriaPatch* applied, which is a security software product developed by CA, Inc. |
| **Disclaimer** | The information contained in this Validation Report is not an endorsement of the Identity Manager product by any agency of the U.S. Government, and no warranty of the Access Control product is either expressed or implied. |
| **PP** | None |
| **Evaluation Personnel** | Chris Gugel<br>John Schroeder<br>Jeremy Sestok<br>Amit Sharma<br>Mark Wozar |
| **Validation Body** | NIAP CCEVS |

## 2.1 Threats to Security

Table 2 summarizes the threats that the evaluated product addresses.

**Table 2 – Threats**

| |
|---|
| TOE users could gain electronic access to protected resources by attempting to establish a connection that they are not permitted to perform. |
| A TOE user may incorrectly install or configure the TOE, or install a corrupted TOE resulting in ineffective security mechanisms. |
| A malicious user or process may view audit records, cause audit records to be lost or modified, or prevent future audit records from being recorded, thus masking a TOE user's action. |
| A malicious user could eavesdrop on network traffic to gain unauthorized access to TOE data. |
| Users whether they be malicious or non-malicious, could gain unauthorised access to the TOE by bypassing identification and authentication countermeasures. |
| A user may masquerade as a TOE user or an authorized IT entity to gain access to data or TOE resources. |
| Users could gain unauthorised access to the TOE or its data stores by bypassing identification and authentication requirements. |

# 3 Identification

The product being evaluated is CA Identity Manager r12.5 with the IMr12.5CommonCriteriaPatch applied.

# 4 Security Policy

## 4.1 User Data Protection

When a TOE user attempts to access the TOE, Identity Manager uses their role information to determine the tasks available for them to access. Within these tasks, the TOE user's scope, determined by the policy that assigned them their role information or an explicit authorization, is used to determine the scope of control of the TOE user's available operations. Compliance support can be used to define mutually exclusive roles or preconditions for a TOE user being assigned a role. In this manner, explicit denial of operations can be established.

Independently of this process, TOE users can be delegated the ability to be workflow approvers for specific tasks. TOE users have workflow approver roles that determine what types of tasks they can approve, and delegation of this approval is determined by role and scope information. Workflow is essentially an information flow that forces tasks to be approved at certain points before their execution. If workflow is enabled for the TOE and applies to a certain tasks, the information flow will apply to that task as long as it has at least one approver assigned to.

The third means by which TOE data is protected is via the Task Execution Web Service. An authorized TOE user can run a web service application to perform a batch of automated commands on the TOE. The credentials of the TOE user running the application are sent to the TOE and checked against a separate access control list (ACL) stored in the Identity Manager database before the web service application can be run.

Provisioning roles are the process by which endpoint user accounts are assigned to an endpoint. A provisioning role identifies the type of endpoint account that will be created (such as a Unix account). The privileges assigned to that account are based on account templates. For example, an account template can be defined for a DBA, attached to a Unix account provisioning role, and then this role can applied to all DBA endpoint users by assigning the role to them. Provisioning roles and account templates are created by a TOE user with the appropriate task privileges.

Once an endpoint user account has been assigned to an endpoint via provisioning, it's the responsibility of that endpoint to protect its data from unauthorized access. A TOE user who accesses that endpoint should only be allowed to perform operations allowed to them by the initial provisioning assignment.

## 4.2 Identification and Authentication

The TOE provides TOE users with a username and password to authenticate to the TOE and stores their e-mail address so they can perform tasks which require authentication by answering a pre-defined security verification question. The TOE contains a configurable password policy mechanism to ensure that TOE user passwords are sufficiently secure for a given deployment. It also stores a password recovery question and answer in case of forgotten password. Other security attributes which pertain to TOE users are the enabled/disabled state of their account, the admin roles to which they belong, and the scope of task access they're assigned. A certain set of self-management tasks are referred to as public tasks due to the fact that authentication to the TOE is performed by answering a pre-defined security verification question. All other tasks require username/password authentication.

The Task Execution Web Service (TEWS) relies on a simple directory-based authentication to allow access to the TOE's web service API. When a web service application is run against the TOE, the taskContext value of the SOAP request identifies the TOE user running the application and contains their username credential, which is used to identify and authorize their actions. In the evaluated configuration, the TEWS interface requires a third party application to authenticate users prior to granting access to the interface. The user will then provide their identity to the TOE for identification and to determine access control restrictions. Thus, TEWS interface will only identify a user that has already been granted access to the interface by the third party application. The identity provided to the TOE does not have to match the one provided to the third party application, nor will the identity provided to the TOE be authenticated. Therefore, the TEWS interface is expected to only be used by a user that has been assigned all privileges of the TOE in the evaluated configuration.

**NOTE:** *Although it was not validated through the evaluation, the vendor has asserted that the TOE can have the TEWS interface protected by CA SiteMinder. This would allow for TOE users to have their TOE identity be authenticated by SiteMinder, and then have all actions on the TOE be associated with their authenticated TOE identity.*

Password policies can be defined by a TOE user with the appropriate task privileges. Options such as password length, composition (such as "at least one number"), and regular expression formatting can be applied. When a password policy is applied to an environment, the TOE forces TOE user passwords to comply with the policy before they can proceed.

When an endpoint has been configured by the TOE's provisioning capabilities, they enforce the provisioned identification and authentication policies as if they had been configured directly on that endpoint (without using the TOE as an intermediary). Access to endpoints, therefore, is governed by the native I&A of the endpoints themselves.

## 4.3 Security Management

The TOE provides management capabilities through the User Console that are used remotely by TOE users. The capability to manage various attributes is limited by the allowed tasks and authorized scope of TOE users. For example, one degree of scope can be authority to perform a task on behalf of all members of a particular group. Another can be for a TOE user to modify only his/her own attributes.

Management functions of the TOE are accomplished via performing tasks. Roles are given a set of tasks they are authorized to perform and the TOE associates TOE users with one or more of these roles. TOE users are taken from the user store, which is defined as an LDAP directory using the XML Directory Configuration File during initial setup of the TOE.

Like performing any other management function, groups are defined by a TOE user with the appropriate task privilege. Groups can be based on a static set of members, a dynamic LDAP query that changes the group membership as the user store changes, or by aggregating multiple existing groups.

During initial configuration of the TOE, the default values for new pieces of TOE data are restrictive by default. For example, a new TOE user won't be assigned scope over all other TOE users by default on the Create User Task page. However, any TOE user with the ability to create data (as defined by the available tasks in table 6-11) in the Identity Manager database can override these default values.

There is a superuser account on the TOE by default, but in the evaluated configuration it will only be used in the initial configuration and then disabled. The TOE contains a number of default roles, but custom roles can be defined as well by combining policies (to determine membership conditions and scope of operations) and tasks.

Provisioning is managed by TOE users with Create/Modify Endpoint tasks assigned to them. This allows TOE users to apply account templates to endpoints and perform provisioning. Once an endpoint is created, endpoint user accounts are configured on it by managing provisioning roles and account templates.

When a TOE user has rights revoked, the action will be processed as soon as the task is completed. This is enforced on the TOE user upon the next page loaded in the User Console.

## 4.4 Security Audit

When the TOE is first configured, an audit settings file is created to define the types of events that will be audited by the TOE and the conditions under which they're audited. Audit records are stored in the Audit DB and contain the fields shown in Tables 6-3 and 6-4. This includes, among other data, the timestamp of the event, subject identity, and outcome of the event.

When a task is performed by the TOE, it is composed as a series of events. For example, performing the Modify Admin Role Members/Administrators task can involve one or more of the following events: AddGrantorOnAccessRoleEvent, AssignAccessRoleEvent, RemoveGrantorOnAccessRoleEvent, and RevokeAccessRoleEvent. These events are the audit events which are entered into the Audit DB as audit records.

Audit review is performed in the Operational Environment because the TOE lacks the capability to review audit data natively. The Operational Environment must therefore be configured in a manner that allows for only authorized individuals to review or modify the audit trail.

The TOE relies on the underlying operating system to provide accurate time stamps to be used for audit records.

## 4.5 Cryptographic Support

The TOE uses AES encryption with 256-bit keys that the vendor asserts operates in accordance with FIPS PUB 197. Encryption is performed when directories and environments are exported, when new TOE user passwords are created, and when database fields configured as “encrypt on write” are written to. To secure communications between the TOE and the TOE user web browser, the application server on which the TOE is installed must be configured for HTTPS.

Although the vendor has asserted that all cryptography for this product has been tested, testing of specific cryptographic algorithms was not conducted as part of this evaluation.

## 4.6 Protection of TSF

The TOE relies on the host operating system to provide reliable timestamps for audit records.

## 4.7 Trusted Path/Channels

The Operational Environment shall provide a path for communication between the TSF and remote TOE users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification and disclosure. The Operational Environment shall allow initial communication to the trusted path by remote TOE users, and it shall require the use of the trusted path for initial TOE user authentication and all other TSF mediated actions by the TOE user. This is accomplished by configuring the environmental application server to use HTTPS for remote browser sessions.

## 4.8 Provisioning

The Provisioning function of the TOE is a subset of the activities performed by the User Data Protection security function. Account templates are defined, provisioning roles are assigned, and endpoint users are given provisioning roles through the same mechanism that admin roles are created and assigned.

Applications called connectors translate provisioning commands issued by the TOE into the format used by the endpoints. Depending on the application type, some connectors are installed directly on the endpoints themselves, while others are installed on a central environment server.

Once endpoints are provisioned, their access control and authentication mechanisms are no longer the responsibility of the TOE. A provisioned endpoint does not require communication with the TOE (unless further provisioning is required) because it acts as if it was configured locally by an administrator. This allows the operational environment to function in its intended manner if the TOE itself is in a failed state. In the evaluated configuration, the user store used by the Provisioning Server is the same logical user store used by the Application Server. This allows endpoint accounts and roles to be provisioned and assigned to TOE users without the need to introduce an additional mapping between multiple user stores.

### 4.9 Work Flow

The Workflow function of the TOE enforces the FDP_ACC.1(2), FDP_ACF.1(2) , FDP_IFC.1, and FDP_IFF.1 requirements. It is also a subset of the activities performed by the User Data Protection security function. A TOE user with Create or Modify Admin Task privileges is able to designate workflow approval steps for that task based on the events that occur as part of the task. These events are the same events which are audited. These TOE users also determine who can approve those steps.

When a task requires action from an approver to continue; that action is considered a work item. The TOE allows TOE users with delegation roles to give their work items to other TOE users. A TOE user with the ability to modify tasks can reassign work items for that task to different TOE users.

When multiple TOE users are capable of approving a single work item, it's possible for one TOE user to reserve the work item so that they can prevent the others from approving or rejecting it.

Workflow is defined as an information flow for the TOE in the sense that the work item flows through multiple subjects until final approval, at which point the task is performed. The information flow will not be performed unless the TOE is enabled for workflow, a task is associated with a workflow process, and the workflow process designates at least one approver for the given task. Explicit authorization of this information flow is defined by the workflow process applied to the task, which indicates the events which require approval and the set of TOE users which must do so in order for the events to proceed.

# 5 Assumptions

### 5.1 Personnel Assumptions

**Table 1 – Personnel Assumptions**

| |
|---|
| One or more TOE users will be assigned to install, configure and manage the TOE. |
| Users responsible for management of the operational environment exercise due diligence to update the TOE with the latest patches (e.g., OS and database) so they are not susceptible to network attacks. |
| TOE users are not careless, willfully negligent, or hostile and will follow and abide by the instructions provided by the organization's guidance documentation. |

### 5.2 Physical Assumptions

**Table 3 – Physical Assumptions**

| |
|---|
| The TOE and the endpoints the TOE will monitor and manage are located on a network that is isolated from any other network. No connections exist to other networks. |

# 6 Clarification of Scope

The TOE includes all the code that enforces the policies identified (see section 4).

The evaluated configuration of the TOE includes the CA Identity Manager r12.5 product that is comprised of the following:

- Servers
    - Identity Manager Application Server
    - Identity Manager Provisioning Server
- User Store
    - CA Directory (user store and provisioning directory)
- Connectors
    - Java Connector Server
    - Connectors

## 6.1 System Requirements

The following minimum components are required for the system that will host the Identity Manager servers:

**Hardware Components**

- CPU – one of the following:
    - Intel Core 2 Duo (or equivalent), 2 GHz
    - Dual-core SPARC, 1.5 GHz
- Memory: 4 GB
- Available disk space: 5 GB

**Software Components**

- Operating System: one of the following
    - Windows Server 2003 SP2
    - Windows Server 2003 R2 SP2
    - Windows Server 2008 (32-bit)
    - Solaris 9
    - Solaris 10
- ODBC Database: one of the following
    - Oracle 10g R2
    - Microsoft SQL Server 2005
- Application Server: JBoss 4.2.3 or WebLogic 9.2.3 for Solaris 10

> ***Note:*** *These hardware requirements take into account the requirements of the Application Server that must be installed on the system where Identity Manager is installed. The Provisioning Server will run on the same machine and the requirements for the Application Server are sufficient to accomplish this.*

In the evaluated configuration, the TOE will consist of one machine running the Application Server and another running the Provisioning Server, which includes the Java Connector Server. CA Directory will be used for the combined User Store and Provisioning Directory, and a third party application server is required to be installed on the Application Server prior to Identity Manager's installation.

In addition to the environmental components listed above, the following non-TOE software is required to run the TOE:

- TLS v1.0 implementation
- Transport standards HTTP, and FTP implementations
- SMTP implementation
- Web browser software

# 7 Architectural Information

The TOE's boundary has been defined in Figure 1.

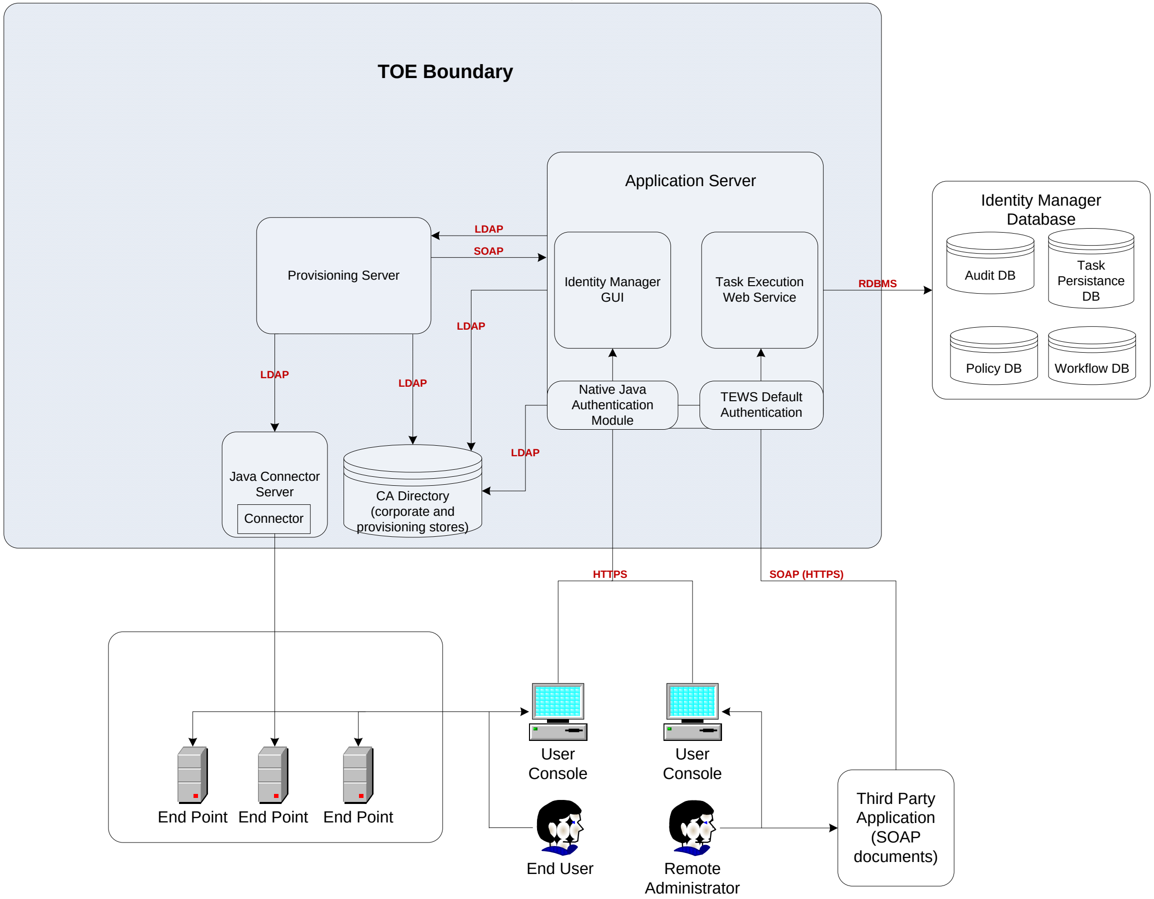

**Figure 1 – CA Identity Manager r12.5 TOE Boundary**

## 7.1 TOE Components

### 7.1.1 Identity Manager Application Server

The Identity Manager Application Server executes tasks within Identity Manager. The J2EE Identity Manager application includes the Identity Manager Management Console and the Identity Manager User Console. It is also the primary interface to the environmental data stores, which assist in auditing and applying the tasks that are executed.

The Application Server is ultimately responsible for determining the privileges available to a TOE user and allowing the user to access only the parts of the TOE that he/she has been authorized to access.

### 7.1.2 Identity Manager Provisioning Server

The Provisioning Server manages accounts on endpoint systems. In the evaluated configuration, Identity Manager will support provisioning, so this is a required component.

***Note**: The Provisioning Directory must be installed on a CA Directory Server before installing the Provisioning Server. In the evaluated configuration, this Provisioning Directory will be the same logical CA Directory Server instance as the corporate user store.*

The Provisioning Server is the server that manages additional accounts that are assigned to an endpoint user. When a provisioning role is assigned to an endpoint user, the Provisioning Server creates accounts on endpoints that meet the requirements of the role. For example, if a provisioning role is assigned to a user that includes an LDAP account template, the Provisioning Server assigns an LDAP account to the user. Basic management of provisioning roles and activities are accomplished through administrative use of the User Console. The Provisioning Server contains a Provisioning Manger GUI that allows for advanced management of provisioning functionality, but these features will not be subject to evaluation.

### 7.1.3 CA Directory (user store and provisioning directory)

An Identity Manager implementation must include a user store that contains the identities that Identity Manager maintains. It is used for the purposes of authenticating to the TOE and delivering information to the internal security model, which then authorizes access to protected data. Typically, this is an existing user store that an enterprise uses to store information about its users, such as employees and customers. In the evaluated configuration, this will be an instantiation of CA Directory.

When provisioning is used (as it is in the evaluated configuration), Identity Manager also requires a provisioning directory that includes global users, which are associated with accounts on endpoints such as LDAP, Oracle, and SAP.

To provide options for managing users and automatic provisioning of additional accounts for those users, Identity Manager coordinates two user stores:

- The Identity Manager corporate directory, the user store maintained by Identity Manager. Typically, this is an existing store that contains the user identities that a company needs to manage.
  The user store can be an LDAP directory or a relational database.
  In the Management Console, the admin installing the TOE must create an Identity Manager Directory object to connect to the user store and to describe the user store objects that Identity Manager will maintain.

- The Provisioning Directory, the user store maintained by the Provisioning Server. It is an instance of CA Directory and includes global user accounts, which associate users in the Provisioning Directory with accounts on endpoints such as LDAP, Oracle, and SAP.
  Only some users have a corresponding global user account. The users are known as endpoint users. When a user receives a provisioning role, the Provisioning Server creates a global user in the Provisioning Directory, designating them as an endpoint user.

In the evaluated configuration, these two user stores will be the same logical instance of CA Directory. The corporate directory would traditionally be regarded as a component of the operational environment. However, the setup of the TOE will incorporate this directory into the TOE in order to manage provisioning. This is why the corporate directory cannot be considered to be part of the environment in this situation.

### 7.1.4 Connectors

A connector is the software interface to an endpoint. The Provisioning Server uses the connector to communicate with the endpoint. It translates Provisioning Server actions into changes on the endpoint, such as "Create a new dba level account on an Oracle endpoint."

Examples of endpoints are LDAP server, Oracle database, or SAP enterprise software.

Connectors work with multiple endpoints. For example, if there are many UNIX workstation endpoints in the environment, there could be one UNIX connector on the Connector Server that is able to manage these workstations from a centralized point. Another connector might handle all connectors that request Windows accounts.

A Connector Server is a Provisioning Server component that manages connectors. All connectors will have a component that runs on and the Connector Server. However, some connectors also have a component that must be present on the managed endpoint in order for provisioning to be accomplished. For this evaluation, all connectors are within the scope, but the communication between connector components on the Connector Server and those that also run remotely will not be evaluated.

There are two types of connector servers:

- The Java Connector Server (JCS) manages connectors written in Java
- The C++ Connector Server (CCS) manages connectors written in C++

Note that for this evaluation, the JCS is the only connector service which is within the scope of the evaluation. The CCS has been listed only for informational purposes and will not be evaluated. The TOE has no assurance of the integrity of these agents. Because they are installed on systems that are outside the TOE boundary, an administrator has no capability to protect these agents from modification.

# 8 Documentation

The following end user documents were reviewed as part of the evaluation:

1. **CA Identity Manager r12.5 Security Target v2.0**
2. **CA Identity Manager Administration Guide r12.5**
3. **CA Identity Manager Standard Connector Guide 12.5**
4. **CA Identity Manager Provisioning Reference Guide**
5. **CA Identity Manager Configuration Guide r12.5**
6. **CA Identity Manager Release Notes r12.5**

# 9 TOE Acquisition

The NIAP-certified CA Identity Manager product is acquired via normal sales channels, and digital delivery of the TOE is coordinated with the end customer by CA Technologies.

The "Evaluated Configuration for CA Identity Manager r12.5" document, which provides the recommendations and secure usage directions for the TOE as derived from testing. This includes how to apply the *IMr12.5CommonCriteriaPatch* patch.

# 10 IT Product Testing

The test team's test approach is to test the security mechanisms of the CA Identity Manager r12.5 by exercising the external interfaces to the TOE and viewing the TOE behavior on the platform. Each TOE external interface is to be described in CA design documentation (e.g., FSP) in terms of the relevant claims on the TOE that can be tested through the external interface. The ST, TOE Design (TDS), Functional Specification (FSP), Security Architecture (ARC) and the vendor's test plans will be used to demonstrate test coverage of all EAL3 requirements for all *security relevant* TOE external interfaces. TOE external interfaces that will be determined to be *security relevant* are interfaces that

- change the security state of the product,
- permit an object access or information flow that is regulated by the security policy,
- are restricted to subjects with privilege or behave differently when executed by subjects with privilege, or
- invoke or configure a security mechanism.

Security functional requirements will be determined to be *appropriate* to a particular interface if the behavior of the TOE that supported the requirement could be invoked or observed through that interface.

The evaluation team will create a test plan that contains a sample of the vendor functional test suite, and supplemental functional testing of the vendors' tests. Booz Allen will also perform vulnerability assessment and penetration testing.

## 10.1 TEST METHODOLOGY

### 10.1.1 Vulnerability Testing

The evaluation team created a set of vulnerability tests to attempt to subvert the security of CA Identity Manager r12.5. These tests were created based upon the evaluation team's review of the vulnerability analysis evidence and independent research. The Evaluation Team conducted searches for public vulnerabilities related to the TOE. A few notable resources consulted include securityfocus.com, the cve.mitre.org, and the nvd.nist.gov.

Upon the completion of the vulnerability analysis research, the team had identified several generic vulnerabilities upon which to build a test suite. These tests were created specifically with the intent of exploiting these vulnerabilities within the TOE or its configuration.

The team tested the following areas:

- Eavesdropping on Communications

  In this test, the evaluators manually inspected network traffic to and from the TOE in order to ensure that no useful or confidential information could be obtained by a malicious user on the network. This test was specialized for the following interfaces:
  - Web (HTTPS)
  - Application Server – Provisioning Server
  - Provisioning Server - Endpoint
- Port Scanning

  Remote access to the TOE should be limited to the standard TOE interfaces and procedures. This test attempted to find ways to bypass these standard interfaces of the TOE and open any other vectors of attack.
- Buffer Overflow / Format String / Unexpected Input Attack

  In this attack, the evaluators attempted to discover and exploit any software errors that do not appropriately handle various non standard inputs. The evaluators attempted to inject known malicious inputs into the various TOE interfaces. These malicious inputs form 3 categories.
  - Buffer Overflows: In this case, larger and larger inputs are injected to try to overflow a buffer and corrupt the program stack.
  - Format Strings: In this case, format strings are injected to attempt to see if they are not handled correctly by the program.
  - Special Characters: In this case, unexpected special characters are injected in an attempt to induce non standard behavior.
- Vulnerability Scanner (Nessus)

  This test used the Nessus Vulnerability scanner to test any and all open interfaces on any applicable systems of the TOE. The scanner probes a wide range of vulnerabilities that includes but is not limited to the following:

| | | |
|---|---|---|
| Backdoors | Gain root remotely | RPC |
| CGI abuses | General | Settings |

| | | |
|---|---|---|
| Denial of Service | Miscellaneous | SMTP Problems |
| Finger abuses | Netware | SNMP |
| Firewalls | NIS | Untested |
| FTP | Port scanners | Useless services |
| Gain a shell remotely | Remote file access | |

- TCP Malformed Packet Flooding

  This test attempted to shutdown TOE resources by flooding the network with large amounts of malformed tcp packets.
- Unauthenticated Access / Directory Traversal Attack

  This test used “URL hacking” to attempt to access protected TOE resources by injecting unexpected input into requests that were sent to the TOE. This was done using two different approaches to URL exploitation.
  - The first part attempted to access protected TOE resources as an unauthenticated outsider.
  - The second part attempted to access local TOE resources that should be protected from any remote access (unauthenticated and authenticated).
- SQL Injection / Cross Site Scripting Attack / Cross Site Request Forgery

  This test executed automated SQL Injection and Cross Site Scripting attacks against the TOE. The evaluators determined any fields or variables that could be prone to attack. They then used a scanner, which contained a large database of standard strings that are used for testing SQL Injection and Cross Site Scripting issues. These strings were input into the various fields and variables and the output was analyzed for inconsistencies.
- Web Server Vulnerability Scanner (Nikto)

  This test used the Nikto web server vulnerability scanner to test for any known vulnerabilities that could be present in the TOE’s web interfaces. This scanner probed a wide range of vulnerabilities that included the following:

| | |
|---|---|
| File Upload. | Denial of Service. |
| Interesting File / Seen in logs. | Command Execution / Remote Shell. |
| Misconfiguration / Default File. | SQL Injection. |
| Information Disclosure. | Authentication Bypass. |
| Injection (XSS/Script/HTML). | Software Identification |
| Remote File Retrieval | Remote source inclusion. |

- Vulnerability Scanner (Retina)

  This test uses the Retina Vulnerability scanner to test any and all open interfaces on any applicable systems of the TOE.

  The scanner probes a wide range of vulnerabilities that includes but is not limited to the following:

| | | |
|---|---|---|
| Accounts | DoS | Service Control |
| Anti-Virus | IP Services | Spyware |
| Backdoors | Registry | Web Services |
| CGI Scripts | Remote Access | CVE Issues |
| Database Issues | RPC Services | SecurityFocus BID Issues |

- Soap/JMS Testing
  This test attempts to exercise the web services interface of the product using a third party tool in an attempt to discover any vulnerabilities that could be presented by these services. It also attempts to discover any other unknown web services that could be used for a side channel attack.
- HTTP Soap Brute Force
  This test attempts to brute force SOAP/XML requests to uncover hidden methods against the TOE web server using the metasploit framework tool.
- Direct Database Access
  The TOE uses a database to store all of its security related data. The way it is designed, the TOE should perform all direct interaction to and from the backend database and no user should have any access to it. This test attempts to access the database directly and bypass these normal access procedures.

### 10.1.2 Vulnerability Results

The following lists any issues that were discovered as a result of the vulnerability testing process. These issues along with the related guidance for mitigation have been included in the "Evaluated Configuration for CA Identity Manager 12.5" addendum to the product Administrator Guidance. These issues have been broken up into the following categories:

#### 10.1.2.1 Fixed in CC Version Based on Testing Results

- **Cross Site Scripting Vulnerability**
  There existed a cross site scripting vulnerability in the user-name field of the Identity Manager UI.
  At the login screen, a user-name and password are sent via HTTP Post to the server for authentication. If the credentials are incorrect, the user is sent back to the login screen with the previously entered user-name already filled out.
  The problem was that the site did not filter any characters that were sent with the user-name and sent them back exactly as entered. Therefore, by entering in special characters, the HTML control flow could be broken and javascript could be embedded in the page.
  The vendor had fixed this issue in a later release of the product and the fix was back-ported to the CC version as a solution to this vulnerability. The issue no longer exists in the CC version of the product.

- **LDAP Special Character Injection**
  Identity Manager does not properly filter the use of the '*' character in user Id's (or user fields) managed by the product. In this scenario, attempts to specify that user directly (such as in role-member rules or in TEWS transactions) could match different users or multiple users and produce unintended or malicious behavior.
  The vendor developed a Common Criteria Patch that includes a full fix for this issue. The issue no longer exists in the CC version of the product.

- **ASCII Escape Vulnerability**
  Identity Manager handles escaped ASCII values (in hexadecimal) inconsistently throughout the system. In this attack vector, a malicious user creates an independent user id that is equivalent to another user in the system except using ASCII escaped values (i.e. user='\75\73\65\72'). When an administrator attempts to delete the malicious user in this case, the valid user is the one that is actually deleted and the administrator is unable to delete the malicious user through the IM UI.
  The vendor developed a Common Criteria Patch that includes a full fix for this issue. The issue no longer exists in the CC version of the product.

#### 10.1.2.2 Mitigated Via Configuration

- **Apache Axis Administrative console**
  There exists a web administrative console ('/idm/axis2-admin') that comes with the Apache Axis platform that can be used to provide status and configuration of web services. It also provides the capability to upload and deploy new web services. If compromised, this could allow for remote execution of Java code. The console has a built-in authentication mechanism; however, the credentials defined for it are static and equivalent across Identity Manager installations.
  IM administrators are instructed to change the password value for this console as part of the IM installation.

- **Unauthenticated JSP Pages**
  There exist several jsp pages that are available to unauthenticated users in the IM user console path. These are as follows:
  /idm/status.jsp – provides information about started IM user environments
  /idm/ping.jsp – provides server and system information including java versions and raw system paths
  /idm/logging.jsp – provides the ability to set the logging verbosity for several IM audit logs (including 'off')
  Administrators are instructed to remove these jsp pages before deploying Identity Manager

- **Unauthenticated Web-Services Interface (TEWS)**
  The TEWS interface allows for SOAP execution of IM tasks exposed through web services at the URL '/idm/TEWS6/<env_name>'. This interface does not enforce password authentication of users. The context in which a particular task is run can be specified using a user-name only. All tasks available to the Identity Manager user console can be executed through this interface.
  IM administrators will be instructed to enable environmental authentication enforcement on this console through the application server (Jboss or Weblogic).

- **Unauthenticated IM Management Console**
  There exists an Identity Manger administrative web console at the web address '/idmmanage' that does not have any authentication mechanism attached to it by

default. This console allows for the management of IM directories and environments. It includes functionality such as:

- The ability to promote any IM user to a System Manager
- The ability to enable/disable workflow, email notifications, and web-services (TEWS)

IM administrators will be instructed to enable environmental authentication enforcement on this console through the application server (Jboss or Weblogic).

#### 10.1.2.3 Additional Guidance for Security

- **The Use of HTTP over SSL/TLS**
  The Identity Manager Web interface should be accessed using HTTPS only. Administrators should be aware that standard HTTP is required to be enabled for notifications from the Provisioning Server (which are encrypted using payload encryption). However, standard users/administrators should not use the non-secure HTTP implementation. The use of standard HTTP would expose user passwords to network interception.

- **Trusted Certificates**
  All implementations of SSL/TLS in use by Identity Manager should be configured using valid certificates signed by a trusted certificate authority. The use of self-signed certificates could expose users to Man-In-the-Middle attacks resulting in credential theft.

# 11 Results of the Evaluation

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) process and scheme. The evaluation demonstrated that the CA Identity Manager r12.5 TOE meets the security requirements contained in the Security Target.

The criteria against which the CA Identity Manager r12.5 TOE was judged are described in the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 2, September 2007. The evaluation methodology used by the evaluation team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 2, September 2007. The Booz Allen Hamilton Common Criteria Test Laboratory determined that the evaluation assurance level (EAL) for the CA Identity Manager r12.5 TOE is EAL 3. The TOE, configured as specified in the installation guide, satisfies all of the security functional requirements stated in the Security Target.

The evaluation was completed in July 2010.

# 12 Validator Comments/Recommendations

The Validation team agrees that the CCTL presented appropriate rationales to support the results and conclusions presented in the ETR. The validation team therefore recommends that the evaluation results be accepted and recommends a Pass result for the TOE identified in section 3 of this document.

# 13 Security Target

The security target for this product's evaluation is *CA Identity Manager r12.5 Security Target version 2.0, dated June 21, 2010.*

# 14 List of Acronyms

| Acronym | Definition |
|---|---|
| ACL | Access Control List |
| AES | Advanced Encryption Standard |
| CC | Common Criteria |
| CS | Connector Server |
| DB | Database |
| IM | Identity Manager |
| IT | Information Technology |
| JIAM | Java Identity and Access Management |
| LDAP | Lightweight Directory Access Protocol |
| OS | Operating System |
| PP | Protection Profile |
| RDBMS | Relational Database Management System |
| SOAP | Simple Object Access Protocol |
| ST | Security Target |
| TEWS | Task Execution Web Services |
| TLS | Transport Layer Security |
| TOE | Target of Evaluation |
| TSF | TOE Security Function |
| XML | Extensible Markup Language |

# 15 Terminology

| Term | Definition |
|---|---|
| Account Template | A preconfigured set of privileges which can be assigned to an endpoint user's account on an endpoint during provisioning. |
| Admin Role | A subset of available administrative activities that can be defined and assigned to a TOE user. |
| Administrator | A TOE user who is assigned as an administrator of a group is able to control the membership of that group. |
| Connector | A piece of code that translates provisioning commands issued by Identity Manager into commands that can be interpreted by an endpoint. |
| Endpoint | A computer on the enterprise network that can have its accounts managed by Identity Manager. This can be system-based (i.e. a UNIX endpoint) or application-based (i.e. an LDAP endpoint) |

| Term | Definition |
|---|---|
| Endpoint User | A user on the enterprise network that interacts with endpoints managed by the TOE. If an endpoint user has the ability to interact with the TOE, then they are also considered a TOE user. |
| Identity Manager | An integrated identity management platform that automates the creation, modification, suspension or deletion of user identities and their access to enterprise resources. |
| Management Console | The administrative interface which is used only in the initial configuration of Identity Manager. |
| Policy | A collection of one or more conditions for a role that combine to determine whether or not a user is assigned that role and what their scope within it is. |
| Provisioning | The act of using Identity Manager to create or modify user accounts on an endpoint as if an administrator on that endpoint was directly configuring it. |
| Provisioning Role | A set of account templates that are applied to a set of endpoints which can be defined and assigned to end users. |
| TOE User | Any trusted user on the TOE. All TOE users are capable of some administrative functionality (self-management at the very least). |
| User | A generic term to refer to all individuals belonging to an IT enterprise environment. All users are at the very least endpoint users, but can potentially be TOE users as well. |
| User Console | The administrative interface which is used to configure Identity Manager during its operation. |
| Workflow | The process of requiring approval to changes made in the configuration of Identity Manager. |

# 16 Bibliography

1. Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 3.1 Revision 2.
2. Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, Version 3.1 Revision 2.
3. Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, Version 3.1 Revision 2.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 2.
5. CA Identity Manager r12.5 Security Target version 2.0, June 21, 2010
6. Evaluation Technical Report for a Target of Evaluation “CA Identity Manager r12.5 Security Target version 2.0” Evaluation Technical Report v2.0 dated 2 July 2010.