Sun Microsystems, Inc.

Sun Java™ System Identity Manager v5.0

Security Target V2.4

Debra Baker

July 29, 2005

CYGNACOM SOLUTIONS

Suite 5200♦7925 Jones Branch Drive♦McLean, VA 22102-3305♦703 848-0883♦Fax 703 848-0985

Revision History:

Date:	Version:	Author:	Description
06/25/2003	0.1	Debra Baker	First Draft of LPM ST
07/15/2003	0.2	Debra Baker	Second draft of LPM ST
07/17/2003	0.3	Debra Baker	Updated TOE description
08/05/2003	0.4	Debra Baker	Added FMT_SMF.1 (CCIMB 065), added cryptographic SFRs
08/13/2003	0.5	Debra Baker	Update to TOE Description
08/14/2003	0.6	Debra Baker	Updated Rationale to map to cryptographic functions
08/18/2003	1.0	Debra Baker	Made version 1.0 to prepare for NIAP
08/26/2003	1.1	Debra Baker	Updated section 7
09/15/2003	1.2	Debra Baker	Update to version of ST references
01/06/2004	1.3	Debra Baker	Updates from ST evaluation
02/13/2004	1.4	Debra Baker	Updates from ST evaluation
03/9/2004	1.5	Debra Baker	Updates from ST evaluation
09/9/2004	1.5.1	Debra Baker	Product name updates
11/23/2004	2.0	Debra Baker	SFR revisions
1/17/2005	2.1	Debra Baker	Updates throughout
3/24/2005	2.2	Debra Baker	Update to reflect evaluated configuration
4/4/2005	2.3	Debra Baker	Update to reflect evaluator comments
7/29/2005	2.4	Debra Baker	Update to reflect evaluator comments

TABLE OF CONTENTS

SECTION **PAGE**

Table of Tables and Figures

Table or Figure **Page**

1 Security Target Introduction

1.1 Security Target Identification

TOE Identification:	Sun Java™ System Identity Manager v5.0
TOE Part Number:	817-7804-05
ST Title:	Sun Java™ System Identity Manager v5.0 Security Target
ST Version:	Version 2.4
ST Authors:	Debra Baker
ST Date:	July 29, 2005
Assurance Level:	EAL2
Strength of Function:	SOF Basic
Registration:	<To be filled in upon registration>
Keywords:	Resources, Identification, Authentication, Access Control, Security Target, and Security Management

1.2 Security Target Overview

This Security Target (ST) defines the Information Technology (IT) security requirements for Sun Java™ System Identity Manager v5.0. Sun Java™ System Identity Manager (IDM) is an identity management system that enables IDM authorized administrators to securely and efficiently manage access to accounts and resources. IDM is a server application that provides a consistent interface for system administrators to update user account and other configuration information in many target systems of various kinds.

1.3 Common Criteria Conformance

The TOE is Part 2 conformant, Part 3 conformant, and meets the requirements of Evaluation Assurance Level (EAL) 2 from the Common Criteria Version 2.2.

1.4 Document Organization

The main sections of an ST are the ST Introduction, Target of Evaluation (TOE) Description, TOE Security Environment, Security Objectives, IT Security Requirements, TOE Summary Specification, and Rationale.

Section 2, the TOE Description, describes the product type and the scope and boundaries of the TOE.

Section 3, TOE Security Environment, identifies assumptions about the TOE's intended usage and environment and threats relevant to secure TOE operation.

Section 4, Security Objectives, defines the security objectives for the TOE and its environment.

Section 5, IT Security Requirements, specifies the TOE Security Functional Requirements (SFR), Security Requirements for the IT Environment, and the Security Assurance Requirements.

Section 6, TOE Summary Specification, describes the IT Security Functions and Assurance Measures.

Section 7, Protection Profile (PP) Claims, is not applicable, as this product does not claim conformance to any PP.

Section 8, Rationale, presents evidence that the ST is a complete and cohesive set of requirements and that a conformant TOE would provide an effective set of IT security countermeasures within the security environment. The Rationale has three main parts: Security Objectives Rationale, Security Requirements Rationale, and TOE Summary Specification Rationale.

Section 9, Acronyms, provide definitions of acronyms used in the ST.

Section 10, References, provide references to applicable documents.

2 TOE DESCRIPTION

2.1 Product Type

Sun Java™ System Identity Manager (IDM) is a server application that provides a consistent interface for system administrators to update user account and other configuration information in many target systems of various kinds such as applications, mainframes, databases, directory services (LDAP), operating systems, ERP systems, and messaging platforms. With role and rule based provisioning, this solution automates the routine, yet often complex, activities associated with granting, managing, and revoking user access privileges.

2.2 TOE Physical Boundary and Scope of the Evaluation

The TOE Physical Boundary and the evaluated configuration includes the following:

- Sun Java™ System Identity Manager V5.0 running on Microsoft Windows 2000;
- Sun Java™ System Identity Manager Administrator/User Interface running on the same machine.

The TOE includes the IDM Server and the IDM Administrator/User Interface and the physical boundary consists of these software components. The TOE does not include the underlying operating system (OS) software and hardware of the system hosting the TOE. The third party relational database is not included in the TOE. The interface of the third party database is not included as part of the TOE. The TOE also does not include the third-party encryption software that is used to provide a trusted communication path between users and the TOE. The Web Services Engine is not part of the TOE. Note again please that in the evaluated configuration, all TOE components run on the same machine running Microsoft Windows 2000.

2.3 TOE Logical Boundaries and Functionality

The TOE encompasses the following components of the Sun Java™ System Identity Manager product:

- IDM Server,
- Administrator/User Interface.

As described in sections 2.3 and 5.3 respectively, the data store and OS are not part of the TOE. The main security service provided by Sun Java™ System Identity Manager is to manage user identities. The IDM server maintains information on users and the resources they can access. It provides a single interface for authorized administrators to grant, manage, and revoke user access privileges.

Sun Java™ System Identity Manager provides the following security functions:

- **Security Audit –**IDM provides the ability to audit the following events: generated accounts, approved requests, failed access attempts, password changes and resets, self provisioning activities, and administration of configuration data. IDM provides a utility for searching, sorting, ordering, and viewing audit records.
- **User Data Protection/Access Control –**IDM provides access control through the enforcement of the Sun Java™ System Identity Manager Access Control Policy. The IDM

Access Control Policy is based on user roles also described as user capabilities in the Administrator's Guide. This functionality is specified using security attributes in user records in the IDM Data Store.

- **User Identification and Authentication –** The Sun Java™ System Identity Manager provides user identification and authentication through the use of user accounts and the enforcement of password policies. In addition, IDM provides the capability to automatically generate passwords that meet the rules of the password policy.
- **Security Management –**IDM provides security management through the use of the Administrator Interface and User Interface.

2.4 TOE Security Environment

It is assumed that there will be no untrusted users or software on the IDM host. IDM relies upon the underlying operating system platform to provide reliable time stamps. The evaluated configuration of IDM was tested on the following platform with the IT environment resources listed:

OS: Microsoft Windows 2000 Server SP4

Application Server: Apache Tomcat Version 4.1.27 (with JDK 1.4.2)

Database: MySQL™ 4.0.16 .

System:

Dell OptiPlex GX270

P4 2.4 GHz.

1GB RAM

40 GB HD

3 TOE Security Environment

This section identifies secure usage assumptions and threats to security. There are no organizational security policies.

3.1 Assumptions

This section contains assumptions regarding the security environment and the intended usage of the TOE.

Item	Assumption	Description
1	A.NoUntrusted	It is assumed that the administrator will follow administrator guidance for installing and maintaining the TOE, including ensuring that there will be no untrusted users and no untrusted software on the IDM Server host.
2	A.Time	It is assumed that the underlying operating system provides reliable time stamps.

3.2 Threats

The TOE must counter the following threats to security:

Item	Threat	Description
1	T.Abuse	An undetected compromise of the TOE may occur as a result of an authorized user of the TOE (intentionally or otherwise) performing actions the individual is not authorized to perform.
2	T.BadPassword	Users may not select good passwords on their own, allowing attackers to guess their passwords and obtain unauthorized access to the TOE.
3	T.Mismanage	Authorized administrators may make errors in the management of security functions and TSF data, if administrative tools are not provided. Administrative errors may allow attackers to gain unauthorized access to resources protected by the TOE.
4	T.Privil	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.
5	T.Undetect	Attempts by an attacker to violate the security policy may go undetected.
6	T.Walkaway	A user may leave his workstation without logging out.

4 Security Objectives

4.1 Security Objectives for the TOE

The security objectives for the TOE are as follows:

Item	Objective	Description
1	O.Access	The TOE must allow authorized users to access only appropriate TOE functions and data.
2	O.Admin	The TOE must provide the functionality to enable an authorized user to effectively manage the TOE and its security functions.
3	O.Audit	The TOE must record audit records for data accesses and use of the system functions.
4	O.IDAuth	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.
5	O.ManageData	The TOE must be able to store and maintain properties of users and resources.
6	O.PasswordGen	The TOE must support automatic generation of passwords.
7	O.PasswordQual	The TOE must be able to specify password quality parameters such as password history, minimum length, and numbers of types of characters.
8	O.Reauthenticate	The TOE must be able to require the user to be re-authenticated.
9	O.Roles	The TOE must support multiple administrative roles.

4.2 Security Objectives for the Environment

4.2.1 Security Objectives for the IT Environment

The security objectives for the IT environment are as follows:

Item	Objective	Description
1E	OE.Time	The underlying operating system must provide reliable time stamps.

4.2.2 Security Objectives for Non-IT Security Environment

The Non-IT security objectives are as follows:

Item	Objective	Description
2N	ON.NoUntrusted	The authorized administrator must install the TOE and maintain it according to administrator guidance, including ensuring that there are no untrusted users and no untrusted software on the IDM Server host.

5 IT Security Requirements

5.1 Conventions

The following formatting conventions apply to the TOE Security Functional Requirements and the Requirements for the IT Environment.

The CC allows several operations to be performed on functional requirements; *refinement*, *selection*, *assignment*, and *iteration* as defined in Common Criteria, Part 1, section 4.4.1.3.2.

Each of these operations are defined as follows:

a) Iteration: allows a component to be used more than once with varying operations.

b) Assignment: allows the specification parameters;

c) Selection: allows the specification of one or more elements from a list; and

d) Refinement: allows the addition of details

This ST indicates which text is affected by each of these operations in the following manner:

- *Iterations* are identified with a dash number "-#" following the component identifier. "*" refers to all iterations of a component.
- *Assignments* and *Selections* specified by the ST author are in **[*italicized bold text*]**.
- *Refinements* in the form of additions to the CC text are specified in ***<u>italicized bold and underlined text</u>***.
- *Application notes* provide additional information for the reader, but do not specify requirements. Application notes are denoted by *italicized text.*

5.2 TOE Security Functional Requirements

The TOE security functional requirements are listed in Table 5-1. They are all taken from Part 2 of the Common Criteria and there are no explicitly stated requirements.

Table 5-1 – Security Functional Components for the TOE

Security Functionality	Item	Component	Component Name
Security Audit	1	FAU_GEN.1	Audit data generation
	2	FAU_GEN.2	User identity association
	3	FAU_SAR.1	Audit review
	4	FAU_SAR.2	Restricted audit review
	5	FAU_SAR.3*	Selectable audit review
	6	FAU_SEL.1	Selective audit
	7	FAU_STG.1	Protected audit trail storage
User Data Protection/Access Control	8	FDP_ACC.1	Subset access control
	9	FDP_ACF.1	Security attribute based access control

Security Functionality	Item	Component	Component Name
Identification and Authentication	10	FIA_ATD.1	User attribute definition
	11	FIA_SOS.1	Verification of secrets
	12	FIA_SOS.2	TSF Generation of secrets
	13	FIA_UAU.2	User authentication before any action
	14	FIA_UAU.6	Re-authenticating
	15	FIA_UID.2	User identification before any action
Security Management	16	FMT_MOF.1	Management of security functions behaviour
	17	FMT_MSA.1	Management of security attributes
	18	FMT_MSA.3	Static attribute initialisation
	19	FMT_MTD.1	Management of TSF data
	20	FMT_SMF.1	Specification of management functions
	21	FMT_SMR.1	Security roles

5.2.1 Class FAU: Security Audit

FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the **[*not specified*]** level of audit; and

c) **[*the following auditable events:***

- ***generated accounts,***
- ***approved requests,***
- ***failed access attempts,***
- ***password changes and resets,***
- ***self provisioning activities, and***
- ***administration of configuration data*.]**

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST: **[*no other information*]**

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.2 User identity association

Hierarchical to: No other components.

FAU_GEN.2.1 The TSF shall be able to associate each auditable event with the identity of the user that caused the event.

Dependencies: FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification

FAU_SAR.1 Audit review

Hierarchical to: No other components.

FAU_SAR.1.1 The TSF shall provide **[*Report Administrator*]** with the capability to read **[*all audit information within the Report Administrator's scope of control*]** from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.2 Restricted audit review

Hierarchical to: No other components.

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

Dependencies: FAU_SAR.1 Audit review

Application Note for Iterations of FAU_SAR.3 (below): IDM uses different parameters for searching, sorting, and ordering. The following three iterations address each of these parameter sets in turn. This capability is provided through the Audit Log reports functionality. IDM type is defined as the following: Select an IDM object type, such as a user or resource. (Refer to page-level Help for a detailed list of types)

FAU_SAR.3-1 Selectable audit review ***- searching***

Hierarchical to: No other components.

FAU_SAR.3.1-1The TSF shall provide the ability to perform **[*searches*]** of audit data based on **[*organizations, IDM type, actions, result equals, subject, interface, server, account id, message, resource, object name, attribute changes, Client IP, Session IP, report timeline, maximum number of records*].**

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.3-2 Selectable audit review***- sorting***

Hierarchical to: No other components.

FAU_SAR.3.1-2The TSF shall provide the ability to perform **[*sorting*]** of audit data based on **[*administrator report, role report, user report, usage report, AuditLogReport*].**

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.3-3 Selectable audit review *- ordering*

Hierarchical to: No other components.

FAU_SAR.3.1-3The TSF shall provide the ability to perform **[*ordering*]** of audit data based on **[*timestamp, subject, action, type of object modified, object name, resource (account), ID, result (success or failure*].**

Dependencies: FAU_SAR.1 Audit review

FAU_SEL.1 Selective audit

Hierarchical to: No other components.

FAU_SEL.1.1 The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes:

a) [*event type,*]

b) [*Account Management, IDM login/logout, Password Management, Resource Management, Role Management, Security Management, Task Management, Change outside Identity Manager, IDM configuration Management*].

Dependencies: FAU_GEN.1 Audit data generation
FMT_MTD.1 Management of TSF data

FAU_STG.1 Protected audit trail storage

Hierarchical to: No other components.

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.1.2 The TSF shall be able to **[*prevent*]** unauthorized modifications to the audit records in the audit trail.

Dependencies: FAU_GEN.1 Audit data generation

5.2.2 Class FDP: User Data Protection

FDP_ACC.1 Subset access control

Hierarchical to: No other components

FDP_ACC.1.1 The TSF shall enforce the **[*Table 5-2 – Sun Java™ System Identity Manager Access Control Policy*]** on **[*Subjects and Objects listed in Table 5-2*]**.

Dependencies: FDP_ACF.1 Security attribute based access control

Table 5-2 – Sun Java™ System Identity Manager Access Control Policy

Subjects with the following Capabilities	Objects	Operations among subjects and objects
Account Administrator	**Accounts**	▪ List Accounts, ▪ Find Users, ▪ Extract to File, ▪ Load from File, ▪ Load from Resource
	Passwords	▪ Change My Password, ▪ Change My Answers, ▪ Change User Password, ▪ Reset User Password
	Approvals	▪ Awaiting Approval, ▪ Previously Approved, ▪ Previously Rejected
	Tasks	▪ Find Tasks, ▪ All Tasks, ▪ Run Tasks
Approver	**Passwords**	▪ Change My Password, ▪ Change My Answers
	Approvals	▪ Awaiting Approval, ▪ Previously Approved, ▪ Previously Rejected
Capability Administrator	**Passwords**	▪ Change My Password, ▪ Change My Answers
	Approvals	▪ Awaiting Approval, ▪ Previously Approved, ▪ Previously Rejected
Change Password Administrator	**Accounts**	▪ List Accounts, ▪ Find Users
	Passwords	▪ Change My Password, ▪ Change My Answers, ▪ Change User Password
	Tasks	▪ Find Tasks, ▪ All Tasks, ▪ Run Tasks
Import/Export Administrator	**Passwords**	▪ Change My Password, ▪ Change My Answers

Subjects with the following Capabilities	Objects	Operations among subjects and objects
	Tasks	▪ Find Tasks, ▪ All Tasks, ▪ Run Tasks, ▪ Schedule Tasks
	Reports	▪ Run Reports, ▪ Manage Reports
	Resources	▪ List Resources
	Configure	▪ Import Exchange File
Password Administrator	**Accounts**	▪ List Accounts, ▪ Find Users
	Passwords	▪ Change My Password, ▪ Change My Answers, ▪ Change User Password, ▪ Reset User Password
	Tasks	▪ Find Tasks, ▪ All Tasks, ▪ Run Tasks
Remedy Integration Administrator	**Passwords**	▪ Change My Password, ▪ Change My Answers
	Tasks	▪ Find Tasks, ▪ All Tasks, ▪ Run Tasks
	configure	▪ Remedy Integration
Report Administrator	**Passwords**	▪ Change My Password, ▪ Change My Answers
	Reports	▪ Run Reports, ▪ Manage Reports
	Risk Analysis	▪ Run Risk Analysis Reports ▪ Manage Reports
	Configure	▪ Audit Events
Reset Password Administrator	**Accounts**	▪ List Accounts, ▪ Find Users
	Passwords	▪ Change My Password, ▪ Change My Answers, ▪ Reset User Password

Subjects with the following Capabilities	Objects	Operations among subjects and objects
	Tasks	▪ Find Tasks, ▪ All Tasks, ▪ Run Tasks
Resource Administrator	**Passwords**	▪ Change My Password, ▪ Change My Answers
	Tasks	▪ Find Tasks, ▪ All Tasks, ▪ Run Tasks
	Resources	▪ List Resources, ▪ List Resources Groups, ▪ Examine Account Index
Role Administrator	**Passwords**	▪ Change My Password, ▪ Change My Answers
	Tasks	▪ Find Tasks, ▪ All Tasks, ▪ Run Tasks
	Roles	▪ List Roles, ▪ Find Roles
Security Administrator	**Accounts**	▪ List Accounts, ▪ Find Users
	Passwords	▪ Change My Password, ▪ Change My Answers, ▪ Change User Password, ▪ Reset User Password
	Tasks	▪ Find Tasks, ▪ All Tasks, ▪ Run Tasks
	Reports	▪ Run Reports, ▪ Manage Reports
	Resources	▪ List Resources
	Configure	▪ Policies ▪ Login
Waveset Administrator	**Passwords**	▪ Change My Password, ▪ Change My Answers
	Approvals	▪ Awaiting Approval, ▪ Previously Approved, ▪ Previously Rejected

Subjects with the following Capabilities	Objects	Operations among subjects and objects
	Tasks	▪ Find Tasks, ▪ All Tasks, ▪ Run Tasks, ▪ Schedule Tasks
	Reports	▪ Run Reports, ▪ Manage Reports
	Resources	▪ List Resources
	Risk Analysis	▪ Run Risk Analysis Reports, ▪ Manage Reports
	Configure	▪ Audit Events, ▪ Email Templates, ▪ Form and Process Mapping ▪ Servers

FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

FDP_ACF.1.1 The TSF shall enforce the **[Table 5-2 - *Sun Java™ System* Identity *Manager* Access Control Policy]** to objects based on the following: **[*Subjects with Capabilities, Objects, and Operations listed in Table 5-2*]**.

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [**Owner-controlled access control attributes on objects]**.

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **[*no additional rules*]**.

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the **[*no additional explicit denial rules*]**.

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization.

5.2.3 Class FIA: Identification and Authentication

FIA_ATD.1 User attribute definition

Hierarchical to: No other components.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

- **[*User Identity;***
- ***Selected Policy;***
- ***Roles;***
- ***Organization;***
- ***Resources;***
- ***Resource Groups;***
- ***Resource Attributes;***
- ***Administrative role(s) user can assume (see Table 5-2)*].**

Dependencies: No dependencies.

FIA_SOS.1 Verification of secrets

Hierarchical to: No other components.

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet **[*the rules of the password policy*]**

Dependencies: No dependencies.

FIA_SOS.2 TSF Generation of secrets

Hierarchical to: No other components.

FIA_SOS.2.1 The TSF shall provide a mechanism to generate secrets that meet **[*the rules of the password policy*]*.***

FIA_SOS.2.2 The TSF shall be able to enforce the use of TSF generated secrets for **[*Manage User Access Function*]*.***

Dependencies: No dependencies.

FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: FIA_UID.1 Timing of identification.

FIA_UAU.6 Re-authenticating

Hierarchical to: No other components.

FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions **[*configurable session time out*]**.

Dependencies: No dependencies.

FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1

FIA_UID.2.1 The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: No dependencies.

5.2.4 Class FMT: Security Management (FMT)

FMT_MOF.1 Management of security functions behaviour

Hierarchical to: No other components.

FMT_MOF.1.1 The TSF shall restrict the ability to **[*determine the behavior of, disable, enable, and modify the behavior of*]** the functions **[*related to the selection of which events are to be audited (see FAU_SEL.1.1) and audit (see FAU_GEN.1.1)*]** to **[*the Report Administrator*].**

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles.

FMT_MSA.1-1 Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1-1 The TSF shall enforce the **[Table 5-2 - *Sun Java™ System* Identity *Manager Access Control Policy*]** to restrict the ability to **[*query, modify, delete,* [*create, rename, disable, update, enable, import, unlock, view*]]** the security attributes **[*user*]** to **[*Account Administrator*]**.

Dependencies: [FDP_ACC.1 Subset access control or
FDP_IFC.1 Subset information flow control]
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles.

FMT_MSA.1-2 Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1-2The TSF shall enforce the **[Table 5-*2* – *Sun Java™ System* Identity *Manager* Access Control Policy]** to restrict the ability to **[*query, modify, delete,* [or *create*]]** the security attributes **[*roles*]** to **[*Role Administrator*]**.

Dependencies: [FDP_ACC.1 Subset access control or
FDP_IFC.1 Subset information flow control]

FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles.

FMT_MSA.1-3 Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1-3 The TSF shall enforce the **[Table 5-*2* – *Sun Java™ System* Identity *Manager* Access Control Policy]** to restrict the ability to **[*query, modify, delete,* [*or create*]]** the security attributes **[*resource*]** to **[*Resource Administrator*]**.

Dependencies: [FDP_ACC.1 Subset access control or
FDP_IFC.1 Subset information flow control]
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MSA.3 Static attribute initialisation

Hierarchical to: No other components.

FMT_MSA.3.1 The TSF shall enforce the **[Table 5-*2* – *Sun Java™ System* Identity *Manager* Access Control Policy]** to provide **[*restrictive*]** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the **[*roles identified in* Table 5-*2* – *Sun Java™ System* Identity *Manager* Access Control Policy]** to specify alternative initial values to override the default values when an object or information is created.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles.

FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1 The TSF shall restrict the ability to **[*change default*, *query, modify, delete,* [*see operations specified in Table 5-3*]]** the **[*TSF Data as specified in Table 5-3*]** to **[*the role as specified in Table 5-3-*]**.

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles.

Table 5-3 – Management of TSF Data

Role	Allowed Operations on TSF Data (Management Functions)
Account Administrator	The Account Administrator can: ▪ Create users in controlled organizations ▪ Change and reset user passwords ▪ Discover user accounts ▪ Manage approvals ▪ Schedule, view, and delete tasks
Approver	The Approver can approve creation of user accounts
Capability Administrator	The Capability Administrator can manage capabilities (rights)
Change Password Administrator	The Change Password Administrator can change user account passwords
Import/Export Administrator	The Import/Export Administrator can import and export IDM objects into and out of the IDM Repository
Password Administrator	The Password Administrator can change and reset user account passwords.
Remedy Integration Administrator	The Remedy Integration Administrator can manage events to be captured by Remedy
Report Administrator	The Report Administrator can: ▪ Create, edit, and delete reports ▪ Set audit event limits
Reset Password Administrator	The Reset Password Administrator can reset user account passwords
Resource Administrator	The Resource Administrator can: ▪ Create, edit, and delete resources ▪ Define resource approvers ▪ Scan resources ▪ View risk analysis reports
Role Administrator	The Role Administrator can: ▪ Create, edit, and delete roles ▪ Define role approvers ▪ Scan roles ▪ View risk analysis reports
Security Administrator	The Security Administrator can: ▪ Create, edit, and delete organizations ▪ Create, edit, and delete authorized administrators
Waveset Administrator	The Waveset Administrator can: ▪ Customize email notification ▪ Schedule tasks

FMT_SMF.1 Specification of management functions

Hierarchical to: No other components.

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: **[**

- ***determine the behavior of, disable, enable, and modify the behavior of the functions related to the selection of which events are to be audited (see FAU_SEL.1.1) and audit (see FAU_GEN.1.1)
(see FMT_MOF.1),***
- ***query, modify, delete, create, rename the security attributes user identity (see FMT_MSA.1-1),***
- ***query, modify, delete, or create the security attributes roles (see FMT_MSA.1-2),***
- ***query, modify, delete, or create the security attributes resource (see FMT_MSA.1-3),***
- ***change_default, query, modify, delete, clear create as specified in Table 5-3 the TSF Data as specified in Table 5-3 (See FMT_MTD.1)*]**.

Dependencies: No Dependencies.

FMT_SMR.1 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1 The TSF shall maintain the roles **[*see roles identified in* Table 5-2 *– Sun Java™ System* Identity *Manager* Access Control Policy]**.

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of identification.

5.3 Strength of Function

The overall strength of function requirement is SOF-Basic. The strength of function requirement applies to FIA_SOS.1 and FIA_SOS.2. The SOF claims for FIA_SOS.1 and FIA_SOS.2 are SOF-Basic. The strength of the "secrets" mechanism is consistent with the objectives of authenticating users (O.IDAUTH). In addition, O.PasswordGen and O.PasswordQual are consistent with the SOF-Basic claim.

5.4 TOE Security Assurance Requirements

The Security Assurance Requirements for the TOE are the assurance components of Evaluation Assurance Level 2 (EAL2) taken from Part 3 of the Common Criteria. None of the assurance components is refined. The assurance components are listed in Table 5-4 - EAL2 Assurance Components.

Table 5-4 – EAL2 Assurance Components

Item	Component	Component
1	ACM_CAP.2	Configuration items
2	ADO_DEL.1	Delivery procedures
3	ADO_IGS.1	Installation, generation, and start-up procedures
4	ADV_FSP.1	Informal functional specification

5	ADV_HLD.1	Descriptive high-level design
6	ADV_RCR.1	Informal correspondence demonstration
7	AGD_ADM.1	Administrator guidance
8	AGD_USR.1	User guidance
9	ATE_COV.1	Evidence of coverage
10	ATE_FUN.1	Functional testing
11	ATE_IND.2	Independent testing – sample
12	AVA_SOF.1	Strength of TOE security function evaluation
13	AVA_VLA.1	Developer vulnerability analysis

Further information on these assurance components can be found in the Common Criteria for Information Technology Security Evaluation (CCITSE) Part 3.

5.5 Security Requirements for the IT Environment

Security Functional Components for the IT Environment are listed in Table 5-5 below.

Table 5-5 – Security Functional Components for the IT Environment

	Item	Component	Component Name
Protection of the TOE Security Functions	22	FPT_STM.1	Reliable time stamps

5.5.1 Class FPT: Protection of the TSF

FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

FPT_STM.1.1 **Refinement:** The ***IT environment*** shall be able to provide reliable time stamps for its own use.

Dependencies: No dependencies.

6 TOE Summary Specification

6.1 IT Security Functions

The following describe the IT Security Functions in the Sun Java™ System Identity Manager.

Table 6-1. – Security Functional Requirements mapped to Security Functions

SFRs	Security Class	Sub-functions
FAU_GEN.1	Security Audit	SA-1
		SA-2
FAU_GEN.2	Security Audit	SA-3
FAU_SAR.1	Security Audit	SA-4
FAU_SAR.2	Security Audit	SA-5
FAU_SAR.3	Security Audit	SA-6
FAU_SEL.1	Security Audit	SA-7
FAU_STG.1	Security Audit	SA-8
FDP_ACC.1	Access Control	AC-1
FDP_ACF.1	Access Control	AC-1
FIA_ATD.1	User Identification and Authentication	UIA-1
FIA_SOS.1	User Identification and Authentication	UIA-2
FIA_SOS.2	User Identification and Authentication	UIA-3
FIA_UAU.2	User Identification and Authentication	UIA-4
FIA_UAU.6	User Identification and Authentication	UIA-5
FIA_UID.2	User Identification and Authentication	UIA-6
FMT_MOF.1	Security Management	SM-1
FMT_MSA.1-1	Security Management	SM-2
FMT_MSA.1-2	Security Management	SM-3
FMT_MSA.1-3	Security Management	SM-4
FMT_MSA.3	Security Management	SM-5

SFRs	Security Class	Sub-functions
FMT_MTD.1	Security Management	SM-6
FMT_SMF.1	Security Management	SM-7
FMT_SMR.1	Security Management	SM-8

Security Function: Security Audit Function	
Sub-function ID	**Sub-function description**
SA-1	IDM generates the following types of audit events: ▪ startup and shutdown of audit functions ▪ *generated accounts,* ▪ *approved requests,* ▪ *failed access attempts,* ▪ *password changes and resets,* ▪ *self provisioning activities, and* ▪ *administration of configuration data.* (FAU_GEN.1)
SA-2	The following information is recorded for all events: ▪ Date and time of event, ▪ Type of event, ▪ Subject identity, and ▪ Success or failure of event. (FAU_GEN.1)
SA-3	IDM will associate each auditable event with the identity of the user that caused the event. (FAU_GEN.2)
SA-4	IDM provides the report administrator with the capability to read all audit information within the Report Administrator's scope of control from the audit records. (FAU_SAR.1)
SA-5	IDM prohibits all users read access to the audit records, except those that have been granted explicit read access. (FAU_SAR.2)
SA-6	IDM provides the ability to perform searches, sorting, and ordering of the audit data, based on organizations to include, IDM type, actions, result, subject, interface, server, account id, message, resource, attribute changes, report timeline, and the maximum number of records. This capability is provided through the Audit Log reports functionality. IDM type is defined as the following: Select a IDM object type, such as a user or resource. (Refer to page-level Help for a detailed list of types) (FAU_SAR.3)
SA-7	IDM is able to include or exclude auditable events from the set of audited events based on specific attributes. (FAU_SEL.1)
SA-8	IDM is able to prevent modifications to the audit records. (FAU_STG.1)

Security Function: Access Control	
Sub-function ID	**Sub-function description**
AC-1	IDM enforces the IDM User Access Policy (See Table 5-2 - Sun Java™ System Identity Manager Access Control Policy) (FDP_ACC.1) (FDP_ACF.1)

Security Function: User Identification and Authentication Function	
Sub-function ID	**Sub-function description**
UIA-1	IDM maintains the following information for each user: user identity, selected policy, roles, organization, resources, resource groups, resource attributes, and administrative roles users can assume. (FIA_ATD.1)
UIA-2	IDM requires that user passwords meet the rules of the password policy (See Table 6-2 – Password Policy Rules). (FIA_SOS.1)
UIA-3	IDM provides a mechanism to generate and enforce passwords that meet the rules of the password policy (See Table 6-2 – Password Policy Rules). (FIA_SOS.2)
UIA-4	IDM requires each user to successfully authenticate with a password before being allowed any other actions. (FIA_UAU.2)
UIA-5	IDM requires the user to re-authenticate when the session times out. (FIA_UAU.6)
UIA-6	IDM requires each user to identify himself/herself before being allowed to perform any other actions. (FIA_UID.2)

Security Function: Security Management Function	
Sub-function ID	**Sub-function description**
SM-1	IDM restricts the ability to determine the behavior of, disable, enable, and modify the behavior of the functions related to the selection of which events are to be audited (see FAU_SEL.1.1) and the audit function (see FAU_GEN.1.1) to the Report Administrator. (FMT_MOF.1)
SM-2	IDM restricts the ability to query, modify, delete, create, and rename the user identity attributes to the Account Administrator. (FMT_MSA.1-1)
SM-3	IDM restricts the ability to query, modify, delete, or create the role attributes to the Role Administrator. (FMT_MSA.1-2)
SM-4	IDM restricts the ability to query, modify, delete, or create the resource attributes to the Resource Administrator. (FMT_MSA.1-3)
SM-5	IDM provides restrictive default values for security attributes as specified in Table 5-2 - Sun Java™ System Identity Manager Access Control Policy and allows the Account Administrator to specify alternative initial values. (FMT_MSA.3)
SM-6	IDM restricts the ability to access data as specified in Table 5-2 - Sun Java™ System Identity Manager Access Control Policy. (FMT_MTD.1)

Security Function: Security Management Function	
Sub-function ID	**Sub-function description**
SM-7	IDM provides the following security management functions: - determine the behavior of, disable, enable, and modify the behavior of the functions related to the selection of which events are to be audited (see FAU_SEL.1.1) - audit (see FAU_GEN.1.1) (see FMT_MOF.1), - query, modify, delete, create, rename the security attributes user identity (see FMT_MSA.1-1), - query, modify, delete, or create the security attributes roles (see FMT_MSA.1-2), - query, modify, delete, or create the security attributes resource (see FMT_MSA.1-3), - change_default, query, modify, delete, clear create the TSF Data as specified in Table 5-3 (See FMT_MTD.1)]. (FMT_SMF.1)
SM-8	IDM maintains the roles: • See roles listed in Table 5-2 • End User. (FMT_SMR.1)

The variables used to define password policy rules in the evaluated configuration are listed in the table below.

Table 6-2 – Password Policy Rules

Rule	Description
Minimum Alpha	Minimum number of alphabetic characters
Minimum Numeric	Minimum number of numeric characters
Minimum Uppercase	Minimum number of upper case characters
Minimum Lowercase	Minimum number of lower case characters
Minimum Special	Minimum number of special characters
Maximum Repetitive	Maximum number of consecutive grouping of identical characters ex. abcabcabc
Maximum Sequential	Maximum number of consecutive identical characters
Minimum Begin Alpha	Minimum number of alphabetic characters at the beginning of the password
Minimum Begin Numeric	Minimum number of numeric characters at the beginning of the password
Password History Policy	Number of previous passwords to be checked against new passwords
Words not Allowed	Words that are not allowed
User Attributes not Allowed	User attributes that are not allowed (such as account ID, email, firstname, fullname, and lastname)

6.2 SOF Claims

The following IT Security Functions are realized by probabilistic or permutational mechanisms:

- UIA-2 – IDM requires that user passwords meet the rules of the password policy
(See Table 6-2 – Password Policy Rules). (FIA_SOS.1)
- UIA-3 – IDM provides a mechanism to generate and enforce passwords that meet the rules of the password policy
(See Table 6-2 – Password Policy Rules). (FIA_SOS.2)

Within UIA-2 and UIA-3, the methods used to provide difficult-to-guess passwords are probabilistic.

The SOF claim for all of these IT security functions is SOF-Basic. The SOF analysis is included in the rationale in Section 8 of this document.

6.3 Assurance Measures

The Sun Java™ System Identity Manager satisfies the assurance requirements for Evaluation Assurance Level EAL2.

The following items are provided as evaluation evidence to satisfy the EAL2 assurance requirements:

Table 6-3 - Assurance Measures

Item	Security Assurance Requirement	How Satisfied
1	ACM_CAP.2	CVS listings provided by the vendor
2	ADO_DEL.1	Sun Java™ System Identity Manager procedures at website address http://www.sun.com/service/online
3	ADO_IGS.1	Sun Java™ System Identity Manager Installation 5.0 Sun Java™ System Identity Manager Release Notes 5.0
4	ADV_FSP.1	Sun Java™ System Identity Manager Administration 5.0 Sun Java™ System Identity Manager Technical Deployment 5.0 Sun Java™ System Identity Manager Technical Reference 5.0 Sun Java™ System Identity Manager Release Notes 5.0
5	ADV_HLD.1	Sun Java™ System Identity Manager Administration 5.0 Sun Java™ System Identity Manager Technical Deployment 5.0 Sun Java™ System Identity Manager Technical Reference 5.0 Sun Java™ System Identity Manager Release Notes 5.0
6	ADV_RCR.1	Sun Java™ System Identity Manager Technical Reference 5.
7	AGD_ADM.1	Sun Java™ System Identity Manager Administration guide Sun Java™ System Identity Manager Installation guide Sun Java™ System Identity Manager Technical Deployment Guide Sun Java™ System Identity Manager Technical Reference
8	AGD_USR.1	Sun Java™ System Identity Manager Administration guide Sun Java™ System Identity Manager Installation guide Sun Java™ System Identity Manager Technical Deployment Guide

Item	Security Assurance Requirement	How Satisfied
9	ATE_COV.1	Sun Java™ System Identity Manager CC Tests
10	ATE_FUN.1	Sun Java™ System Identity Manager CC Tests
11	ATE_IND.2	Evaluator Test Plan
12	AVA_SOF.1	Security Target
13	AVA_VLA.1	Sun Java System Identity Manager Vulnerability Assessment, December 2004

7 PP Claims

The Sun Java™ System Identity Manager Security Target was not written to address any existing Protection Profile.

8 RATIONALE

8.1 Security Objectives Rationale

8.1.1 Threats to Security

Table 8-1 shows that all the identified threats to security are countered by Security Objectives for the TOE or IT Environment.

Table 8-1. - All Threats to Security Countered

Item	Threat Name	Threat Description	Security Objective
1	T.Abuse	An undetected compromise of the TOE may occur as a result of an authorized user of the TOE (intentionally or otherwise) performing actions the individual is not authorized to perform.	1-O.Access 3-O.Audit 4-O.IDAuth 1E-OE.Time
2	T.BadPassword	Users may not select good passwords on their own, allowing attackers to guess their passwords and obtain unauthorized access to the TOE.	6-O.PasswordGen 7-O.PasswordQual
3	T.Mismanage	Authorized administrators may make errors in the management of security functions and TSF data, if administrative tools are not provided. Administrative errors may allow attackers to gain unauthorized access to resources protected by the TOE.	2-O.Admin 5-O.ManageData 10O.Roles
4	T.Privil	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.	1-O.Access 4-O.IDAuth
5	T.Undetect	Attempts by an attacker to violate the security policy may go undetected.	3-O.Audit
6	T.Walkaway	A user may leave his workstation without logging out.	9-O.Reauthenticate

T.Abuse: An undetected compromise of the TOE may occur as a result of an authorized user of the TOE (intentionally or otherwise) performing actions the individual is not authorized to perform. T.Abuse is countered by:

- O.Access: The TOE must allow authorized users to access only appropriate TOE functions and data. This is provided by access controls that limit the actions an individual is authorized to perform.
- O.Audit: The TOE must record audit records for data accesses and use of the system functions. This objective counters this threat by requiring the TOE to audit attempts for data accesses and use of TOE functions.
- O.IDAuth: The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data. This objective provides for authentication of users prior to any TOE data access.
- OE.Time: The underlying operating system must provide reliable time stamps. This objective provides for a reliable way to correlate audit records to reconstruct a potential compromise.

T.BadPassword: Users may not select good passwords on their own, allowing attackers to guess their passwords and obtain unauthorized access to the TOE. T.BadPassword is countered by:

- O.PasswordGen: The TOE must support automatic generation of passwords. This objective counters this threat by eliminating the need for users to create their own passwords.
- O.PasswordQual: The TOE must be able to specify password quality parameters such as password history, minimum length, and numbers of types of characters. This objective enables the authorized administrator to specify checks for bad password qualities.

T.Mismanage: Authorized administrators may make errors in the management of security functions and TSF data, if administrative tools are not provided. Administrative errors may allow attackers to gain unauthorized access to resources protected by the TOE. T.Mismanage is countered by:

- O.Admin: The TOE must provide the functionality to enable an authorized user to effectively manage the TOE and its security functions. Administrative tools make it easier for authorized administrators to correctly manage the TOE.
- O.ManageData: The TOE must be able to store and maintain properties of users and resources.
- O.Roles: The TOE must support multiple administrative roles. Multiple administrative roles can be used to enforce separation of duty, so that one authorized administrator can catch errors made by another authorized administrator.

T.Privil: An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data. T.Privil is countered by:

- O.Access: The TOE must allow authorized users to access only appropriate TOE functions and data. This objective builds upon the O.IDAuth objective by only permitting authorized users to access TOE functions.
- O.IDAuth: The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data. This objective provides for authentication of users prior to any TOE function access.

T.Undetect: Attempts by an attacker to violate the security policy may go undetected. T.Undetect is countered by:

- O.Audit: The TOE must record audit records for data accesses and use of the system functions. This objective records attempts to violate the security policy.

T.Walkaway: A user may leave his workstation without logging out. T.Walkaway is countered by:

- O.Reauthenticate: The TOE must be able to require the user to be reauthenticated. Requiring reauthentication prevents an attacker from walking up to an unattended workstation and performing activities using the identity of the user who left the workstation unattended.

8.1.2 Assumptions

Table 8-2 shows that all of the assumptions are addressed by either security objectives for the IT or Non-IT environment security objectives. Table 8-3 is included as a consistency check that all security objectives for the environment map to corresponding threats and assumptions.

Table 8-2. – All Assumptions Addressed

Item	Name	Assumption	Objective
1	A.NoUntrusted	It is assumed that the administrator will follow administrator guidance for installing and maintaining the TOE, including ensuring that there will be no untrusted users and no untrusted software on the IDM Server host	2N-ON.NoUntrusted
2	A.Time	It is assumed that the underlying operating system provides reliable time stamps.	1E-OE.Time

A.NoUntrusted: It is assumed that the administrator will follow administrator guidance for installing and maintaining the TOE, including ensuring that there will be no untrusted users and no untrusted software on the IDM Server host. A.NoUntrusted is covered by:

- ON.NoUntrusted: The authorized administrator must install the TOE and maintain it according to administrator guidance, including ensuring that there are no untrusted users and no untrusted software on the IDM Server host.

A.Time: It is assumed that the underlying the operating system provides reliable time stamps. A.Time is covered by:

- OE.Time: The underlying operating system must provide reliable time stamps. This objective provides for reliable time stamps.

Table 8-3. - Mapping of Security Objectives for the Environment to Threats and Assumptions

No.	Objective Name	Threat/Policy/Assumption
1E	OE.Time	2-A.Time
2N	ON.NoUntrusted	1-A.NoUntrusted

8.2 Security Requirements Rationale

8.2.1 Functional Requirements

Table 8-4 shows that all of the security objectives for the TOE are satisfied.

Table 8-4. - All Objectives for the TOE Met by Functional Components

Item	Objective	Objective Description	Security Functional Requirement
1	O.Access	The TOE must allow authorized users to access only appropriate TOE functions and data.	4-FAU_SAR.2 Restricted Audit review 8-FDP_ACC.1 Subset access control 9-FDP_ACF.1Security attribute based access control 13-FIA_UAU.2 User authentication before any action 16-FIA_UID.2 User identification before any action 17-FMT_MOF.1 Management of security functions behaviour 20-FMT_MTD.1 Management of TSF Data
2	O.Admin	The TOE must provide the functionality to enable an authorized user to effectively manage the TOE and its security functions.	3-FAU_SAR.1 Audit review 5-FAU_SAR.3 Selectable Audit Review 6-FAU_SEL.1 Selective audit 7-FAU_STG.1 Protected audit trail storage 17-FMT_MOF.1 Management of security functions behaviour 18-FMT_MSA.1 Management of security attributes 19-FMT_MSA.3 Static attribute initialisation 20-FMT_MTD.1 Management of TSF Data 21-FMT_SMF.1 Specification of management functions
3	O.Audit	The TOE must record audit records for data accesses and use of the system functions.	1-FAU_GEN.1 Audit data generation 2-FAU_GEN.2 User identity association 6-FAU_SEL.1Selective audit 7-FAU_STG.1 Protected audit trail storage 23-FPT_STM.1 Reliable time stamps
4	O.IDAuth	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.	13-FIA_UAU.2 User authentication before any action 14-FIA_UAU.6 Re-authenticating 16-FIA_UID.2 User identification before any action
5	O.ManageData	The TOE must be able to store and maintain properties of users and resources.	10-FIA_ATD.1 User attribute definition 20-FMT_MTD.1 Management of TSF data 21-FMT_SMF.1 Specification of management functions
6	O.PasswordGen	The TOE must support automatic generation of passwords.	12-FIA_SOS.2 TSF generation of secrets

Item	Objective	Objective Description	Security Functional Requirement
7	O.PasswordQual	The TOE must be able to specify password quality parameters such as password history, minimum length, and numbers of types of characters.	11-FIA_SOS.1 Verification of secrets 12-FIA_SOS.2 TSF generation of secrets
8	O.Reauthenticate	The TOE must be able to require the user to be reauthenticated.	14-FIA_UAU.6 Re-authenticating
9	O.Roles	The TOE must support multiple administrative roles.	22-FMT_SMR.1 Security roles

O.Access: The TOE must allow authorized users to access only appropriate TOE functions and data. O.Access is addressed by:

- FAU_SAR.2 Restricted audit review, which requires that access to audit data be restricted to authorized users.
- FDP_ACC.1 Subset access control, which requires that the TSF enforce access controls on operations between controlled subjects in the TSC and controlled objects within the TSC.
- FDP_ACF.1 Security attribute based access control, which requires the TSF enforce access controls based on specified security attributes. In addition, the TSF can explicitly authorize and deny access to specified subjects.
- FIA_UAU.2 User authentication before any action, which requires each user to be successfully authenticated before allowing access to the TOE.
- FIA_UID.2 User identification before any action, which requires that users be successfully identified before allowing access to the TOE.
- FMT_MOF.1 Management of security functions behaviour, which restricts the ability to disable, enable, and modify functions to authorized users.
- FMT_MTD.1 Management of TSF data, which specifies the management of TSF Data according to assigned roles.

O.Admin: The TOE must provide the functionality to enable an authorized user to effectively manage the TOE and its security functions. O.Admin is addressed by:

- FAU_SAR.1 Audit review, which requires that the auditor be able to read audit records.
- FAU_SAR.3 Selectable Audit Review, which requires that the TSF will provide the ability to search, sort, and order audit data.
- FAU_SEL.1 Selective audit, which requires the TOE to provide authorized users with the ability to include or exclude auditable events from the set of audited events.
- FAU_STG.1 Protected audit trail storage, which requires the audit log be protected from unauthorized deletion and modifications to the audit log will be detected.
- FMT_MOF.1 Management of security functions behaviour, which requires that the auditor be able to manage the behavior of the audit tools.
- FMT_MSA.1 Management of security attributes, which requires only authorized users can query, modify, and delete specified security attributes.

- FMT_MSA.3 Static attribute initialization, which requires the TSF enforce access control for specified default values of security attributes.
- FMT_MTD.1 Management of TSF Data, which specifies the management of TSF Data according to assigned roles.
- FMT_SMF.1 Specification of management functions, which requires the TSF be capable of performing the specified security management functions.

O.Audit: The TOE must record audit records for data accesses and use of the system functions. O.Audit is addressed by:

- FAU_GEN.1 Audit data generation, which requires the ability to audit specified events.
- FAU_GEN.2 User identity association, which requires the ability to associate an auditable event with a specific user.
- FAU_SEL.1 Selective audit, which requires the TOE to provide authorized users with the ability to include or exclude auditable events from the set of audited events.
- FAU_STG.1 Protected audit trail storage, which requires the audit log be protected from unauthorized deletion and modifications to the audit log will be detected.
- FPT_STM.1 Reliable time stamps, which requires that a reliable time stamp be available to record in the audit record.

O.IDAuth: The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data. O.IDAuth is addressed by:

- FIA_UAU.2 User authentication before any action, which requires each user to be successfully authenticated before allowing access to the TOE.
- FIA_UAU.6 Re-authenticating, which requires that the TSF reauthenticate the user under the specified conditions.
- FIA_UID.2 User identification before any action, which requires that users be successfully identified before allowing access to the TOE.

O.ManageData: The TOE must be able to store and maintain properties of users and resources. O.ManageData is addressed by:

- FIA_ATD.1 User attribute definition, which requires that the TSF maintain security attributes of users.
- FMT_MTD.1 Management of TSF data, which specifies the management of TSF Data according to assigned roles.
- FMT_SMF.1 Specification of management functions, which requires the TSF be capable of performing the specified security management functions.

O.PasswordGen: The TOE must support automatic generation of passwords. O.PasswordGen is addressed by:

- FIA_SOS.2 TSF generation of secrets, which requires that the TSF provide a mechanism to generate passwords.

O.PasswordQual: The TOE must be able to specify password quality parameters such as password history, minimum length, and numbers of types of characters. O.PasswordQual is addressed by:

- FIA_SOS.1 Verification of secrets, which requires that the TSF provide a mechanism to verify that passwords meet the rules of the password policy.
- FIA_SOS.2 TSF generation of secrets, which requires that the TSF be able to enforce the use of generated passwords that meet the rules of the password policy.

O.Reauthenticate: The TOE must be able to require the user to be reauthenticated. O.Reauthenticate is addressed by:

- FIA_UAU.6 Re-authenticating, which requires that the TSF reauthenticate the user under the specified conditions.

O.Roles: The TOE must support multiple administrative roles. O.Roles is addressed by:

- FMT_SMR.1 Security roles, which requires that the TSF maintain multiple administrative roles.

8.2.2 Dependencies

Table 8-5 shows the dependencies between the functional requirements. All dependencies are satisfied. Dependencies that are satisfied by a hierarchical component are denoted by an (H) following the dependency reference.

Table 8-5. - Dependencies Satisfied

No.	Component	Component Name	Dependencies	Reference
1	FAU_GEN.1	Audit data generation	FPT_STM.1	23
2	FAU_GEN.2	User identity association	FAU_GEN.1 FIA_UID.1	1 16H
3	FAU_SAR.1	Audit Review	FAU_GEN.1	1
4	FAU_SAR.2	Restricted audit review	FAU_SAR.1	3
5	FAU_SAR.3	Selectable audit review	FAU_SAR.1	3
6	FAU_SEL.1	Selective audit	FAU_GEN.1 FMT_MTD.1	1 20
7	FAU_STG.1	Protected audit trail storage	FAU_GEN.1	1
8	FDP_ACC.1	Subset access control	FDP_ACF.1	9
9	FDP_ACF.1	Security attribute based access control	FDP_ACC.1 FMT_MSA.3	8 19
10	FIA_ATD.1	User attribute definition	None	None
11	FIA_SOS.1	Verification of secrets	None	None
12	FIA_SOS.2	TSF Generation of secrets	None	None
13	FIA_UAU.2	User authentication before any action	FIA_UID.1	16 (H)
14	FIA_UAU.6	Re-authenticating	None	None
15	FIA_UID.2	User identification before any action	None	None
16	FMT_MOF.1	Management of security functions behaviour	FMT_SMF.1 FMT_SMR.1	21 22
17	FMT_MSA.1	Management of security attributes	FDP_ACC.1 FMT_SMF.1 FMT_SMR.1	8 21 22
18	FMT_MSA.3	Static attribute initialisation	FMT_MSA.1 FMT_SMR.1	18 22
19	FMT_MTD.1	Management of TSF data	FMT_SMF.1 FMT_SMR.1	21 22
20	FMT_SMF.1	Specification of management functions	None	None
21	FMT_SMR.1	Security roles	FIA_UID.1	16 (H)
22	FPT_STM.1	Reliable time stamps	None	None

8.2.3 Strength of Function Rationale

As described by the Common Criteria Evaluation Methodology (CEM), Version 2.2, Section B.8, Strength of function analysis is only performed on probabilistic or permutational functions. The analysis assumes that the probabilistic or permutational security function is implemented flawlessly and that the security function is used during attack within the limits of its design and implementation. A SOF rating reflects the attack, described in terms of attack potential, against which the probabilistic or permutational security function is designed to protect. To perform the SOF analysis, first the attack potential is calculated, using assumptions from the Security Target and the guidance documentation about TOE implementation, protections and interaction with other systems and human users. Next the attack potential is mapped to the rating of vulnerabilities and the SOF rating is determined.

The following factors are considered to calculate the attack potential required to exploit a vulnerability; factors are considered for identifying a vulnerability and then exploiting that vulnerability:

- Identification
  - Time taken to identify
  - Specialist technical expertise
  - Knowledge of the TOE design and operation
  - Access to the TOE
  - IT hardware/software or other equipment required for analysis
- Exploitation
  - Time taken to exploit
  - Specialist technical expertise
  - Knowledge of the TOE design and operation
  - Access to the TOE
  - IT hardware/software or other equipment required for exploitation

Each of these factors is discussed in section B.8.2.2 of the CEM and that discussion is not repeated here.

The only security mechanism that is realized by a probabilistic or permutational implementation is the identification and authentication function, specifically the password policy, which is used to meet the FIA_SOS.1 and FIA_SOS.2 requirements. The password is specified according to a specific policy that is provided in a guidance document addendum for the evaluated configuration, i.e., this ST. The administrative policy for the TOE evaluated configuration requires that passwords meet the following:

- Minimum length of 8,
- At least one special character,
- At least one numeric character,
- At least one uppercase and one lowercase character
- 30 day expiration date
- Must not be a common word, a word in any existing password dictionaries, or a word easily guessed (such as “password”).

For the TOE, the operating environment includes the following assumptions:

- The administrator is trusted to correctly configure the TOE.

- It is assumed that there will be no untrusted users and no untrusted software on the system hosting the TOE.
- It is assumed that users will protect their authentication data.

Given these assumptions, the only possible attack would be to guess a user's password in order to access the system as an authorized user.

Analysis was performed using the following assumptions as a worst-case scenario for guessing an authorized user password:

- It is assumed that attackers are layman who would have access to commonly available password crackers, particularly those that use dictionary and exhaustive search attacks.
- It is assumed that the environment provides protections such that passwords could not be captured en route to the TOE, therefore the analysis covers only those attacks that guess passwords or retrieve them from the TOE through some vulnerability; the scope of the SOF analysis is the TOE.
- Only password cracker attacks are considered; other types of password attacks such as social engineering or key logging are not considered, since such attacks are outside the scope of the TOE.
- It is assumed that the attacker would first use a dictionary attack that would include common strategies for guessing passwords such as selecting a user login name, pAsSwOrD, simple transformations for common words, etc.
- Motivation of the attacker is not considered as part of this analysis because the system is multi-purpose and there is no way of knowing the value of the assets protected by the TOE. It is assumed that the value of the assets is low and therefore motivation on the part of the attacker is moderate to low.
- It is assumed that there is a 30-day time limit on the attacker, since passwords expire after 30 days.

A SOF rating reflects the attacker, described in terms of attack potential, against which the probabilistic or permutational security function is designed to protect. To determine a SOF rating for the I&A functionality, the attack potential was calculated by the following method: Using Table 3 from the CEM Annex B, a numerical score for attack potential was calculated and then Table 4 from the CEM Annex B was used to translate the number into a qualitative attack potential and an SOF rating.

The attack potential, given this set of assumptions, is defined in the table below, using the format included in Table 3, Section B.8.2.3 of the CEM:

Attack Potential Calculation for Guessing Passwords

Factor	Range	Identifying Value	Exploiting Value
Elapsed Time	One month	3	5
Expertise	Layman	0	0
Knowledge of TOE	Public	2	2
Access to TOE	One month	3	6
Equipment	Standard	1	2

Total		9	15

Based on the attack potential calculation for identifying passwords (score of 9) and exploiting guessed passwords (score of 15), the attack potential for identifying and for exploiting the vulnerability maps to SOF-basic, as shown by Table 4 for CEM Annex B, included below:

Table 4 from CEM Annex B, section B.8.2.3

Range of Values	Resistant to attack with attack potential of:	SOF rating
<10	No rating	No rating
10 – 17	Low	Basic
18 – 24	Moderate	Medium
>25	High	High

The password space is calculated as follows:

Standard password crackers on the market advertise the ability to try 15 million passwords per second. An 8-character password consisting of 94 available characters results in time required to crack the password as:

94^8 / 15,000,000 per second = 406,379,292 seconds to crack the password

or

4,703 days to crack the password

Since the maximum number days that any password is valid is 30 days, the SOF-basic strength level is sufficient to meet the objectives of the TOE given the security environment described in the ST.

8.2.4 Assurance Requirements

Evaluation Assurance Level EAL2 was chosen to provide a basic level of assurance due to the low level threat of malicious attacks.

8.2.5 Rationale that IT Security Requirements are Internally Consistent and Mutually Supportive

The IT Security Requirements are internally consistent. There are no requirements that conflict with one another. When different IT security requirements apply to the same event, operation, or data there is no conflict between the security requirements. The requirements mutually support each other to apply to the event, operation, or data.

For auditing, each of the SFRs build on the others. For example, FAU_SAR.1 states that the TSF shall provide the Report Administrator with the capability to read all audit information from the audit records. FAU_SAR.2 builds on FAU_SAR.1 by stating the TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access. Audit records are generated for many events that involve other requirements, such as login, policy check failures, and management functions and all of these related requirements are consistent with the audit requirements.

Together FDP_ACC.1 and FDP_ACF.1 provide User Data Protection. FDP_ACC.1 defines the IDM Access Control Policy. FDP_ACF.1 specifies that the TSF enforce access based upon security attributes and named groups of attributes. The roles listed in Table 5-2 (FDP_ACC.1) are also referenced in FMT_SMR.1.

Login processing brings in elements of many requirements, but all in a complementary way. FIA_UID.2 requires that the user be identified before allowing any other operations and FIA_UAU.2 requires that the user be authenticated before allowing any other operations. FIA_SOS defines the strength of the authentication.

The management requirements (FMT_) are related to many of the mechanisms involved with other requirements. FMT_MSA.1 enforces the IDM Access Control Policy (FDP_ACC.1). In many cases, the other mechanisms will enforce the settings made through management functions. Installation mechanisms (see ADO_IGS.1) rely on management functions. The Administrator Guidance (see AGD_ADM) documents the management functions.

8.2.6 Requirements for the IT Environment

Table 8-6 shows that all of the security objectives for the IT environment are satisfied.

Table 8-6. - All Objectives for the IT Environment Met by Security Functional Requirements

Item	Objective	Objective Description	Requirement for the IT Environment	Component Title
1	OE.Time	The underlying operating system must provide reliable time stamps.	FPT_STM.1	Reliable time stamps

OE.Time The underlying operating system must provide reliable time stamps. OE.Time is addressed by:

- FPT_STM.1 Reliable time stamps, which requires that time stamps be provided by the IT environment.

Table 8-7 shows the security functional requirements for the TOE map to the security objectives of the TOE.

Table 8-7. - Mapping of Security Functional Requirements for the TOE to Security Objectives

Item.	Requirement	Component Name	Objective
1	FAU_GEN.1	Audit data generation	3-O.Audit
2	FAU_GEN.2	User identity association	3-O.Audit
3	FAU_SAR.1	Audit Review	2-O.Admin
4	FAU_SAR.2	Restricted Audit Review	1-O.Access
5	FAU_SAR.3	Selectable Audit Review	2-O.Admin
6	FAU_SEL.1	Selective audit	2-O.Admin 3-O.Audit

Item.	Requirement	Component Name	Objective
7	FAU_STG.1	Protected audit trail storage	2-O.Admin 3-O.Audit
8	FDP_ACC.1	Subset access control	1-O.Access
9	FDP_ACF.1	Security attribute based access control	1-O.Access
10	FIA_ATD.1	User attribute definition	5-O.ManageData
11	FIA_SOS.1	Verification of secrets	7-O.PasswordQual
12	FIA_SOS.2	TSF Generation of secrets	6-O.PasswordGen 7-O.PasswordQual
13	FIA_UAU.2	User authentication before any action	1-O.Access 4-O.IDAuth
14	FIA_UAU.6	Re-authenticating	4-O.IDAuth 9-O.Reauthenticate
15	FIA_UID.2	User identification before any action	1-O.Access 4-O.IDAuth
16	FMT_MOF.1	Management of security functions behaviour	1-O.Access 2-O.Admin
17	FMT_MSA.1	Management of security attributes	2-O.Admin
18	FMT_MSA.3	Static attribute initialisation	2-O.Admin
19	FMT_MTD.1	Management of TSF data	1-O.Access 2-O.Admin 5-O.ManageData
20	FMT_SMF.1	Specification of management functions	2-O.Admin 5-O.ManageData
21	FMT_SMR.1	Security roles	10-O.Roles

Table 8-8 below shows the security functional requirements for the IT Environment map to the security objectives of the IT Environment.

Table 8-8. – Mapping of SFRs for the IT Environment to Security Objectives

Item	Requirement	Component Name	Objective
22	FPT_STM.1	Reliable time stamps	1E-OE.Time

8.3 TOE Summary Specification Rationale

8.3.1 IT Security Functions

The table below shows that the IT Security Functions in the TOE Summary Specification (TSS) address all of the TOE Security Functional Requirements.

Table 8-9. – Mapping of the TOE Functional Requirements to TOE Summary Specification

Item	Functional Component	Functional Requirement	Requirement is met by:	
			Security Function Ref. No	Rationale
1	FAU_GEN.1	Audit data generation	SA-1	Specifies the types of events to be audited.
			SA-2	Specifies the information to be recorded in an audit record.
2	FAU_GEN.2	User identity association	SA-3	Each auditable event is associated with the identity of the user that caused the event.
3	FAU_SAR.1	Audit Review	SA-4	Specifies who has the capability to read information from the audit records.
4	FAU_SAR.2	Restricted Audit Review	SA-5	Specifies that only specific users have read access to the audit records.
5	FAU_SAR.3	Selectable audit review	SA-6	Specifies that the IDM Administrator Interface provides the ability to perform searches, sorting, and ordering of the audit data, based on various criteria.
6	FAU_SEL.1	Selective audit	SA-7	Specifies that the IDM Administrator Interface provides the ability to include or exclude auditable events from the set of audited events based on specific attributes.
7	FAU_STG.1	Protected audit trail storage	SA-8	The IDM Administrator Interface is able to prevent modifications to the audit records.
8	FDP_ACC.1	Subset access control	AC-1	Specifies that the IDM Administrator Interface enforces the IDM User Access Policy.
9	FDP_ACF.1	Security attribute based access control	AC-1	Specifies the subjects and objects controlled under the IDM User Access Policy.
10	FIA_ATD.1	User attribute definition	UIA-1	Specifies the security attributes maintained for each user.
11	FIA_SOS.1	Verification of secrets	UIA-2	Specifies that user passwords meet the rules of the password policy.
12	FIA_SOS.2	TSF Generation of secrets	UIA-3	Specifies that the IDM Administrator Interface provides a mechanism to generate passwords that meet the rules of the password policy.
13	FIA_UAU.2	User authentication before any action	UIA-4	Specifies that the IDM Administrator Interface requires each user to successfully authenticate with a password before being allowed any other actions.
14	FIA_UAU.6	Re-authenticating	UIA-5	Specifies that the IDM Administrator Interface requires the user to re-authenticate under certain conditions.

Item	Functional Component	Functional Requirement	Requirement is met by:	
			Security Function Ref. No	Rationale
15	FIA_UID.2	User identification before any action	UIA-6	Specifies that the IDM Administrator Interface requires each user to identify himself/herself before being allowed to perform any other actions.
16	FMT_MOF.1	Management of security functions behaviour	SM-1	Specifies that that the IDM Administrator Interface restricts the ability to determine the behavior of, disable, enable, and modify the behavior of the functions related to the selection of which events are to be audited (see FAU_SEL.1.1) and the audit function (see FAU_GEN.1.1) to the Report Administrator.
17a	FMT_MSA.1-1	Management of security attributes	SM-2	Specifies that the IDM Administrator Interface restricts the ability to query, modify, or delete the user name and password policy attributes to the Account Administrator.
17b	FMT_MSA.1-2	Management of security attributes	SM-3	Specifies that the IDM Administrator Interface restricts the ability to query, modify, or delete the organization attribute to the Security Administrator.
17c	FMT_MSA.1-3	Management of security attributes	SM-4	Specifies that the IDM Administrator Interface restricts the ability to query, modify, delete, or create the resource attribute to the Resource Administrator.
18	FMT_MSA.3	Static attribute initialisation	SM-5	Specifies that the IDM Administrator Interface provides restrictive default values for security attributes and the Account Administrator can specify alternative initial values.
19	FMT_MTD.1	Management of TSF data	SM-6	Specifies that the IDM Administrator Interface restricts the ability to access data.
20	FMT_SMF.1	Specification of management functions	SM-7	Specifies the security management functions provided by the IDM Administrator Interface.
21	FMT_SMR.1	Security roles	SM-8	Specifies the roles maintained by the IDM Administrator Interface.

8.3.2 Assurance Measures

The assurance measures rationale shows how all assurance requirements are satisfied. The rationale is provided in Table 8-10.

Table 8-10. – Assurance Measures Rationale

Item	Component	Evidence Requirements	How Satisfied	Rationale
1	ACM_CAP.2	CM Documentation	CVS listings provided by the vendor	Shows the CM system is being used. Configuration Item List(s) is comprised of a list of the source code files and version numbers is comprised of a list of design documents with version numbers is comprised of test documents with version numbers user and administrator documentation with version numbers
2	ADO_DEL.1	Delivery Procedures	Sun Java™ System Identity Manager procedures at website address http://www.sun.com/service/online	Provides a description of all procedures that are necessary to maintain security when distributing the TOE software to the user's site.
3	ADO_IGS.1	Installation, generation, and start-up procedures	Sun Java™ System Identity Manager Installation 5.0	Provides detailed instructions on how to install IDM.
			Sun Java™ System Identity Manager Release Notes 5.0	Provides guidance on new features of Sun Java™ IDM 5.0.
4	ADV_FSP.1	Functional Specification	Sun Java™ System Identity Manager Administration 5.0 Sun Java™ System Identity Manager Technical Reference 5 Sun Java™ System Identity Manager Technical Deployment Guide, V 5	Describes the TSF interfaces and TOE functionality.
			Sun Java™ System Identity Manager Release Notes 5.0	Provides guidance on new features of Sun Java™ IDM 5.0.

Item	Component	Evidence Requirements	How Satisfied	Rationale
5	ADV_HLD.1	High-Level Design	Sun Java™ System Identity Manager Administration 5.0 Sun Java™ System Identity Manager Technical Reference 5 Sun Java™ System Identity Manager Technical Deployment Guide, V 5	Describes the TOE subsystems and their associated security functionality.
			Sun Java™ System Identity Manager Release Notes 5.0	Provides guidance on new features of Sun Java™ IDM 5.0.
6	ADV_RCR.1	Representation Correspondence	Sun Java™ System Identity Manager Representation Correspondence Table, version 1.0	Provides the following two dimensional mappings: 1. TSS and functional specification; 2. functional specification and high-level design
7	AGD_ADM.1	Administrator Guidance	Sun Java™ System Identity Manager Administration 5.0	Describes how to administer the TOE securely.
			Sun Java™ System Identity Manager Technical Deployment 5.0	Provides guidance on customizing IDM Forms and Views. Provides guidance on configuring IDM ActiveSync Adapters. Provides guidance on using the IDM Business Process Editor graphical interface.
			Sun Java™ System Identity Manager Technical Reference 5.0	Provides guidance on using the XPRESS language, identifies attributes, and describes the configuration of IDM with a firewall or proxy server.
			Sun Java™ System Identity Manager Installation 5.0	Provides detailed instructions on how to install IDM.
8	AGD_USR.1	User Guidance	Sun Java™ System Identity Manager Administration 5.0	Describes how to administer the TOE securely.
			Sun Java™ System Identity Manager Technical Deployment 5.0	Provides guidance on customizing IDM Forms and Views.

Item	Component	Evidence Requirements	How Satisfied	Rationale
			Sun Java™ System Identity Manager Installation 5.0	Provides detailed instructions on how to install IDM.
9	ATE_COV.1	Test Coverage Analysis	Sun Java™ System Identity Manager CC Tests	Shows correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.
10	ATE_FUN.1	Test Documentation	Sun Java™ System Identity Manager CC Tests	Test documentation includes test plans and procedures and expected and actual results.
11	ATE_IND.2	TOE for Testing	Evaluator Test Plan and test results.	The TOE will be provided for testing.
12	AVA_SOF.1	SOF Analysis	Security Target	Provides a rationale that each mechanism identified in the ST as having an SOF meets or exceeds the minimum strength level specified there.
13	AVA_VLA.1	Vulnerability Analysis	Sun Java System Identity Manager Vulnerability Assessment, December 2004	Provides an analysis of the TOE deliverables for obvious ways in which a user can violate the TSP, including the disposition of obvious vulnerabilities.

8.4 PP Claims Rationale

Not applicable. There are no PP claims.

8.5 Strength of Function Rationale

As stated in section 6.2, there are some security functions based on probabilistic methods. The strength of this TOE is SOF-Basic. A strength of SOF-Basic is consistent with protecting the TOE’s assets from unsophisticated attackers with access to standard equipment and public information. See section 5.3 for the objectives that SOF supports.

The specific “strength” required of the methods used to provide difficult-to-guess are defined in Table 6-2 Password Policy Rules. This maps to Security Functions: AI-UIA-2 and AI-UIA-3.

9 ACRONYMS

CC	Common Criteria [for IT Security Evaluation]
EAL	Evaluation Assurance Level
GUI	Graphical User Interface
ID	Identifier
IT	Information Technology
IDM	Sun Java™ System Identity Manager
SF	Security Function
SFP	Security Function Policy
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy

10 References

CCITSE	Common Criteria for Information Technology Security Evaluation, CCIMB-2004-01-002, Version 2.2, January 2004
IDM_Administration_5_0.pdf	Sun Java™ System Identity Manager Administration 5.0 Part No: 817-7804-05
IDM_Installation_5_0.pdf	Sun Java™ System Identity Manager Installation 5.0 Part No: 817-7803-05
IDM Release_Notes_5_0.pdf	Sun Java™ System Identity Manager Release Notes 5.0 Part No: 817-7988-01
IDM_Technical_Deployment_5_0.pdf	Sun Java™ System Identity Manager Technical Deployment Part No: 817-7805-05
IDM_Technical_Reference_5_0.pdf	Sun Java™ System Identity Manager Technical Reference - Part No: 817-7806-05