BMC Remedy
Action Request System 6.3
Security Target

Version 4.5
March 28, 2007
Part number: 60658

Prepared by:
BMC Software, Inc.
1030 W. Maude Avenue
Sunnyvale, CA 94085

Restricted Rights Legend

Table of Contents

List of Figures

List of Tables

1 SECURITY TARGET INTRODUCTION

This section presents Security Target (ST) identification information and an overview of the ST for *BMC Remedy Action Request System 6.3* (formerly Remedy Action Request System 6.3 and hereinafter referred to as *AR System*).

An ST contains the information technology (IT) security requirements of an identified Target of Evaluation (TOE) and specifies the functional and assurance security measures offered by that TOE to meet stated requirements. An ST principally defines:

- A security problem expressed as a set of assumptions about the security aspects of the environment, a list of threats that the product is intended to counter, and any known rules with which the product must comply (Section 3, TOE Security Environment).
- A set of security objectives and a set of security requirements to address the security problem (Sections 4 and 5, Security Objectives and IT Security Requirements, respectively).
- The IT security functions provided by the TOE that meet the set of requirements (Section 6, TOE Summary Specification).

The structure and content of this ST comply with the requirements specified in the Common Criteria (CC), Part 1, Annex C, and Part 3, Chapter 5.

1.1 ST and TOE identification

This section provides information needed to identify and control this ST and its TOE. This ST targets Evaluation Assurance Level (EAL) 3.

ST Title:	BMC Remedy Action Request System 6.3 Security Target
ST Version:	4.5
Authors:	BMC Software, Inc. (Anand Ahire/Virginia Hupp), SAIC, Computer Sciences Corporation Common Criteria Testing Laboratory
TOE Identification:	BMC Remedy Action Request System 6.03.00/6.3, patch 18 (see version numbering explanation below)
CC Identification:	Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005
Keywords:	BMC, Remedy, Action Request System, AR System, workflow, application server, Business Service Management (BSM)
Publication Date:	March 28, 2007

With regard to the TOE identification, in AR System release numbering, the second position of the release number represents the minor release version. In a minor release, the second position of the version number is sometimes displayed with the leading and trailing zeroes, and sometimes without them. Both displays represent the same version number. For example, version number 6.03.00 represents the same release version as version number 6.3.

1.2 References

The following CC documentation was used to prepare this ST:

CC_PART1	Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated August 2005, version 2.3, CCMB-2005-08-001.
CC_PART2	Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated August 2005, version 2.3, CCMB-2005-08-002.
CC_PART3	Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated August 2005, version 2.3, CCMB-2005-08-003.
CEM	Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, dated August 2005, version 2.3, CCMB-2005-08-004.

1.3 Conventions, terminology, and acronyms

This section identifies the formatting conventions used to convey additional information and terminology. It also defines terminology and the meanings of acronyms used throughout this ST.

1.3.1 Conventions

This section describes the conventions used to denote Common Criteria operations on security functional components and to distinguish text with special meaning.

CC_PART2 defines the approved set of operations that can be applied to functional requirements: *assignment, refinement*, *selection,* and *iteration.* In this ST, these operations are indicated as follows:

a) The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Showing the value in square brackets [assignment_value] indicates an assignment.

b) The refinement operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text.**

c) The selection operation is used to select one or more options provided by the CC in stating a requirement. Selections are denoted by <u>*underlined italicized text.*</u>

d) Iterated functional components are given unique identifiers by appending to the component name, short name, and functional element name from the CC an iteration number inside parentheses, i.e., FMT_MTD.1.1(1) and FMT_MTD.1.1

In addition, the following general conventions are also used in this document:

a) Plain *italicized text* is used to introduce the names of TOE components and specific concepts.

b) ***Bold italicized text*** is used for emphasis.

1.3.2 Terminology

In the CC, many terms are defined in Section 2.3 of Part 1. The following terms are a subset of those definitions:

Authentication data Information used to verify the claimed identity of a user.

Authorized user A user who can, in accordance with the TOE Security Policy (TSP[1]), perform an operation.

External IT entity Any IT product or system, untrusted or trusted, outside of the TOE that interacts with the TOE.

Human user Any person who interacts with the TOE.

Identity A representation (e.g., a string) uniquely identifying an authorized user, which can either be the full or abbreviated name of that user or a pseudonym.

Object An entity within the TOE Security Function (TSF[2]) Scope of Control (TSC[3]) that contains or receives information and upon which subjects perform operations.

Role A predefined set of rules establishing the allowed interactions between a user and the TOE.

Security functional components Express security requirements intended to counter threats in the assumed operating environment of the TOE.

Subject An entity within the TSC that causes operations to be performed.

User Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.

[1] TSP – A set of rules that regulate how assets are managed, protected, and distributed within a TOE, as defined in the CC, Part 1, version 2.3:

[2] TSF - A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

[3] TSC - The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.

1.3.3 Acronyms

The following acronyms are used in this ST:

AR System	BMC Remedy Action Request System 6.3
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Evaluation Methodology for Information Technology Security
CM	Configuration Management
EAL	Evaluation Assurance Level
FDP	User Data Protection CC Class
FIA	Identification and Authentication CC Class
FMT	Security Management CC Class
FPT	Protection of the TSF
FSP	Functional Specification
HLD	High-Level Design
ISO	International Standards Organization
ISO 15408	Common Criteria 2.3 ISO Standard
IT	Information Technology
MOF	Management of Functions
MTD	Management of TSF Data
OSP	Organization Security Policy
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SM	Security Management
SMR	Security Management Roles
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy
UAU	User Authentication
UDP	User Data Protection

1.4 TOE overview

AR System is a development and delivery platform that makes it easy for administrators to design and develop customized business applications, even without programming experience. AR System enables the rapid development of applications that incorporate flexible, business-oriented workflow rules and rich graphical user interfaces. AR System combines a form-based environment, workflow modules commonly used in automating service processes, an easy-to-use development interface, and client and database APIs to allow administrators to automate service request-oriented business processes on top of legacy database systems.

AR System also functions as the underlying platform for the BMC Remedy IT Service Management (ITSM) Suite of applications, which includes BMC Remedy Help Desk, BMC Remedy Change Management, BMC Remedy Asset Management and BMC Remedy Service Level Agreements. *(The ITSM Suite is not part of the evaluated configuration.)*

1.5 Common Criteria conformance claim

This TOE is conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, Version 2.3, August 2005, ISO/IEC 15408-2.
    - Part 2 Conformant
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, Version 2.3, August 2005, ISO/IEC 15408-3.
    - Part 3 Conformant.
    - Evaluation Assurance Level 3 (EAL3)

2 TOE DESCRIPTION

This section provides context for the TOE evaluation by identifying the product type and describing the evaluated configuration.

2.1 Product type and evaluated component names

The AR System is a development and runtime platform used to build custom applications that automate business processes. It also provides the platform for the BMC Remedy ITSM Suite. It gives administrators with or without programming experience the ability to design and customize workflow-based applications to easily automate business processes.

The following table identifies the AR System components and versions that are included in the evaluated configuration. The "abbreviated name" is used in this Security Target for discussion purposes.

Table 1: AR System component names

AR System component name	Abbreviated name
BMC Remedy Action Request System Server 6.3, patch 18	*AR System server*
BMC Remedy Approval Server 6.3 (no patch)	*Approval server*
BMC Remedy Email Engine 6.3, patch 18	*Email Engine*
BMC Remedy Flashboards® Server 6.3 (no patch)	*Flashboards server*
Action Request System External Authentication LDAP Plug-in 6.3, patch 18	*AREA LDAP Plug-in*
BMC Remedy Mid Tier 6.3, patch 18	*Mid Tier, the mid tier*
BMC Remedy Administrator 6.3, patch 18	*BMC Remedy Administrator*
BMC Remedy User 6.3, patch 18	*BMC Remedy User*
BMC Remedy Import 6.3, patch 18	*Import*
BMC Remedy Alert 6.3, patch 18	*Alert*
BMC Remedy Configuration Tool 6.3, patch 18	*Configuration Tool*

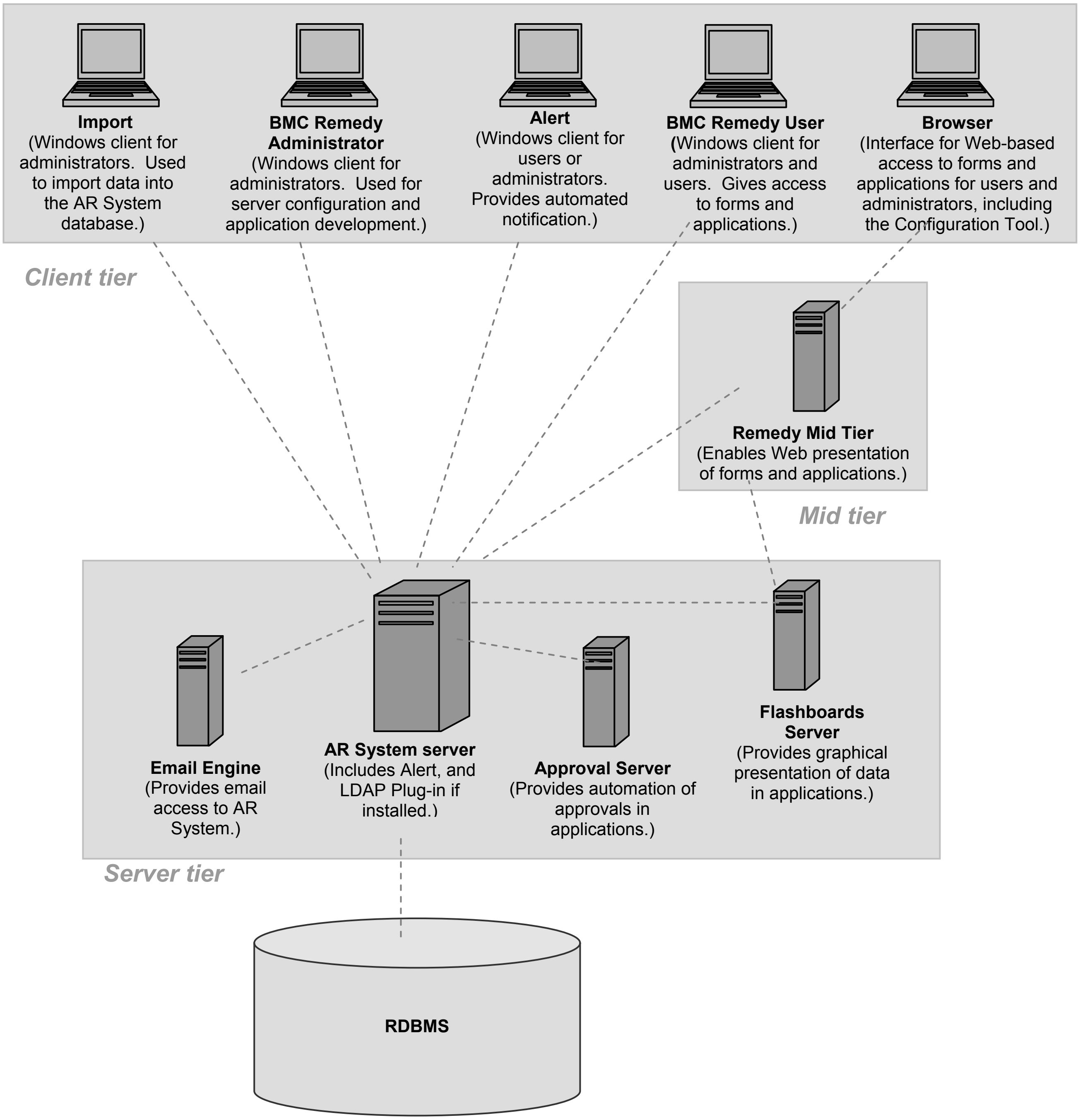
2.1.1 Physical scope and boundary

The AR System consists of server and client components that can be combined to create the types of access the consumer wants to enable. Certain components are required for all AR System installations, while other components are optional, as described in Section 2.1.1.1. The TOE consists of all permutations of required and optional components described in this section.

The TOE does not include the hardware, database, operating systems, email servers, or directory service protocols with or on which the TOE components run, and also does not include third-party components of the mid tier, such as a web server, JSP servlet engine, or browser. However, these components are described in this section where required, to illustrate the physical scope and boundary of the TOE.

The AR System is built on a multi-tiered architecture (see Figure 1) that includes the server tier, the mid tier, and the client tier.

Figure 1: AR System multi-tiered architecture


Import
(Windows client for administrators. Used to import data into the AR System database.)
BMC Remedy Administrator
(Windows client for administrators. Used for server configuration and application development.)
Alert
(Windows client for users or administrators. Provides automated notification.)
BMC Remedy User
(Windows client for administrators and users. Gives access to forms and applications.)
Browser
(Interface for Web-based access to forms and applications for users and administrators, including the Configuration Tool.)
Client tier
Remedy Mid Tier
(Enables Web presentation of forms and applications.)
Mid tier
Email Engine
(Provides email access to AR System.)
AR System server
(Includes Alert, and LDAP Plug-in if installed.)
Approval Server
(Provides automation of approvals in applications.)
Flashboards Server
(Provides graphical presentation of data in applications.)
Server tier
RDBMS

2.1.1.1 Server Tier

The server tier consists of AR System server, along with several optional *application servers* that provide specialized functionality, including Approval Server, Email Engine, and the Flashboards Server. These application servers provide commonly used services that administrators can incorporate into their customized applications, such as workflow approvals, automated notifications, and graphics that illustrate system status and history. If the Action Request System External Authentication (AREA) LDAP Plug-in *(AREA LDAP plug-in)* is used, it is also part of the server tier.

AR System server. The AR System server is a required component that is the core of the AR system. AR System server is a set of processes that run on the server host machine. It implements workflow and controls workflow logic, controls user access to the AR System and the database from AR System client applications, and controls the flow of AR System data into and out of the database. The AR System server installation also provides all APIs and server objects that make up the AR System, including forms, menus, active links, filters, and escalations.

AR System server can be installed on UNIX or Windows. The AR System server database abstraction layer makes the AR System database-independent, so it can operate with most popular databases, such as Oracle, Sybase, Informix, Microsoft SQL Server, and IBM DB2.

The server processes have no direct user interface. They communicate with AR System clients and the application servers through an application programming interface (API).

Approval server. The Approval Server is an optional application server component that adds approval functions to existing applications. This server provides a standard approach to adding an approval process to an AR System workflow application. This allows AR System developers to quickly and easily include approval functionality in applications, without having to develop their own approval system. It also allows them to implement a standard approach for approvals, so that AR System users do not have to figure out different approval mechanisms for each application. The Approval Server communicates directly with AR System server through the AR System API interface.

Email Engine. The Email Engine is an optional application server component that provides email access to AR System server, and is available for all supported platforms. The Email Engine enables applications to send notifications through email to users, and to have users submit AR System requests using an email client. This engine does not serve as an email exchange; it is simply an integration conduit between an email exchange server (such as Microsoft Exchange, or UNIX mbox) and AR System. The Email Engine communicates directly with AR System server through the AR System API interface. It communicates with the email exchange server using IMAP4, SMTP, POP3, MAPI, or MBOX protocols. A supported Java SDK with JRE must be installed on the same platform as the Email Engine.

Only outgoing Email Engine functionality, for the purpose of sending notifications, is included in the evaluated configuration. Submission and modification of requests through the Email Engine is not included in the evaluated configuration.

Flashboards server. Flashboards is an optional application server component that consists of a server, forms, and GUI components. Flashboards provides graphics, such as pie charts and bar graphs, based on underlying AR System data. With Flashboards, the AR System administrator develops graphics within BMC Remedy Administrator as part of an application. Users see color graphics as part of the user interface. These graphics pull data in real time from AR System server or from the *Flashboards server*, which in turn gets the data from the AR System server.

Flashboards forms and limited functionality are automatically installed with AR System server and their use is optional. Full functionality, including the use of flashboards that display historical data, requires licensing the Flashboards Server.

Flashboards requires Mid Tier to be installed. This is because the mid tier is used to construct the graphical presentation of the Flashboards graphics. The Flashboards Server communicates with AR System server through the AR System C API, and with the mid tier by means of the AR System Java API. The mid tier presents flashboards to the client in HTML format. The mid tier generates charts, converts them to HTML format, and then presents them to the client.

Alert. Alert consists of a server component and a client-side component. The server functionality for Alert is part of AR System server and is installed automatically with AR System server. Alert can be configured to display the alert list in BMC Remedy User or in a browser.

Action Request System External Authentication (AREA) LDAP Plug-in. The AREA LDAP plug-in is an optional component that allows the administrator to configure external authentication by using the Lightweight Directory Access Protocol (LDAP). If configured, it accesses network directory services or other authentication services to verify the user login name and password. The AREA LDAP plug-in extends the AR System functionality to access directory services using the LDAP protocol. ***To protect the password when the AREA LDAP plug-in is used, the administrator must configure the plug-in to use SSL.***

A database. (The database is not included in the TOE.) A relational database is a required component of the IT environment. The database sits below the server tier and is accessed by AR System server only. It can be installed on any machine that is accessible to the AR System server.

The AR System server communicates with the database using the AR System database abstraction layer and the database API of the database in use. At installation, the AR System server installer creates, or updates, an AR System database and a series of tables in the database that make up a data dictionary where form, filter, escalation, and other definitions are stored. The actual structure of the AR System database varies depending on the underlying relational database.

2.1.1.2 Mid Tier

Mid Tier. Mid Tier is optional middleware, installed on either UNIX or Windows, which works with a web server to enable AR System access through a web browser. The web server and Mid Tier can be installed on a separate machine with network access to the AR System server machine, or all can be installed on the same machine. One Mid Tier can permit access to multiple AR System servers, and one AR System server can be served by multiple Mid Tiers. Mid Tier communicates with AR System server through the AR System Java API interface.

Mid Tier also provides some administrator access to Mid Tier-related system management functions by way of the Configuration Tool, which runs in a browser. The following supporting components must be installed on the mid tier platform:

- **A supported web server. (The web server is not included in the TOE.)** Supported web servers include Apache, Websphere, Weblogic, SunONE, and IIS. Mid Tier communicates with the web server through the JSP engine. ***To protect the password when using a browser to access AR System, the administrator should configure the Web server to only allow https access.***
- **A supported Java Server Pages (JSP) engine. (The JSP engine is not included in the TOE.)** ***For this evaluation ServletExec 5.0 is used.*** Mid Tier communicates with the JSP engine by means of JSP servlets.
- **Java SDK/JRE v1.4.2 or above. (The Java SDK is not included in the TOE.)** The Java SDK provides the runtime environment for the JSP servlets that make up Mid Tier.

The Configuration Tool. When the Mid Tier is installed, the administrator uses the Configuration Tool to configure the Mid Tier. The Configuration Tool is a .jsp script that is installed with Mid Tier. It does not access the AR System server. Rather, it forms a browser based interface to the Mid Tier configuration file, named config.properties. Administrators use the Configuration Tool to configure Mid Tier access to AR System servers and for other Mid Tier configuration settings. The Configuration Tool is accessed by entering the correct URL in a browser, and it requires a password to log in and change configuration settings.

The administrator must change the Configuration Tool password from the default to a unique password as soon as the Mid Tier installation is complete.

2.1.1.3 Client tier

The AR System client tier includes BMC Remedy Administrator, BMC Remedy User, Import, Alert, and, if Mid Tier is installed, a browser.

BMC Remedy Administrator. BMC Remedy Administrator is a required component. It is installed on Windows only, so at least one Windows client machine is required to administer and license any AR System server (UNIX or Windows). BMC Remedy Administrator is used to administer and configure AR System servers, and to develop AR System applications. One copy of BMC Remedy Administrator can be used to manage multiple AR System servers. It provides a graphical interface to the application's forms, fields, and workflow rules. Developers use BMC Remedy Administrator for application development. Administrators use it for managing the system, including some aspects of controlling security, as well as for customizing and changing BMC Remedy solutions. BMC Remedy Administrator communicates directly with AR System server through the AR System API interface.

BMC Remedy User. BMC Remedy User is a required component if Mid Tier is not installed. BMC Remedy User is installed on Windows and serves two functions. For administrators, it provides access to the User and Group forms that manage user access control, as well as access to other administrative forms. For users, it provides access to the AR System applications from client machines, to submit and modify requests and search the database. BMC Remedy User communicates directly with AR System server through the AR System API interface.

BMC Remedy User and BMC Remedy Administrator are both typically installed on client machines used by administrators. BMC Remedy User is also required for user access to the AR System in configurations that do not include Mid Tier. If Mid Tier is installed, then BMC Remedy User is optional for user access to the AR System. The administrator can optionally configure the AR System to allow authorized administrators to manage the User and Group forms from a browser, if Mid Tier is installed.

Import. Import is installed with BMC Remedy Administrator. Import is an optional client tool that enables AR System administrators to transfer data from an external source into a database form. Import communicates directly with AR System server through the AR System API interface.

Alert. The Alert client is an optional component installed on Windows that provides notifications to users about new AR System transactions, such as when a ticket has been assigned to a user, when a ticket has been escalated, and so on. The purpose of the Alert client is to prompt the user by means of a sound, a window, or a flashing icon, to check the alert list in BMC Remedy User or in a browser.

A supported web browser. (The browser is not included in the TOE.) When Mid Tier is installed, a supported web browser must be installed on client workstations that will access the AR System through the mid tier. Supported web browsers include Internet Explorer, Netscape, and Mozilla. The browser communicates with the mid tier by means of http or https. ***To protect the password when using a browser to access AR System, the administrator should configure the Web server to only allow https access.***

When the mid tier is installed, users can access AR System applications with a browser instead of BMC Remedy User. Web pages are written in JSP and rendered in JavaScript and HTML.

T***o secure the user password when using Mid Tier, the administrator should configure the web server to only allow https access.***

2.1.1.4 Environment configuration for the evaluated configuration

BMC supports AR System 6.3 compatibility with multiple operating system platforms, databases, and other third-party applications. To achieve a timely validation, BMC limited the IT Environment for Common Criteria testing to the platforms and third-party applications described in Table 2: AR System components and their environments. For complete information about operating systems, databases, and other applications that are compatible with AR System 6.3, see the *AR System 6.3 Compatibility Matrix*, which is available at http://www.bmc.com/support_home.

Table 2: AR System components and their environments

TOE component	Dependency	Optional Y/N	Identification-Version	Underlying environment
BMC Remedy Action Request Server (AR System server)	A database	N	6.03.00	o Microsoft Windows 2003. o Sun Solaris 9.
Database (not evaluated)	None	N	o Oracle 9i R2. o Sybase Adaptive Server Enterprise 12.5.3 o MS SQL Server 2000.	As appropriate
BMC Remedy Mid Tier and Configuration Tool	o AR System server o Web server o Servlet Engine o Java SDK/JRE o Browser	Y	6.03.00	Same as AR System server platforms. Also see Web server, Servlet Engine, Java SDK/JRE
Web server (not evaluated)	None	o N if Mid Tier installed. o N/A if Mid Tier not installed.	o Sun ONE 6.1 o Microsoft Internet Information Server 6	As appropriate
Servlet Engine (not evaluated)	o Web Server o Java SDK/JRE	o N if Mid Tier installed. o N/A if Mid Tier not installed.	o Servlet Exec 5	As appropriate

TOE component	Dependency	Optional Y/N	Identification-Version	Underlying environment
Java SDK/JRE (not evaluated)	Web Server	o N if Mid Tier or Email Engine installed. o N/A if Mid Tier and Email Engine not installed.	o Sun Java SDK 1.4.2, 1.4.2+	As appropriate
BMC Remedy User	AR System server	o Y if Mid Tier installed. o N if Mid Tier not installed.	6.03.00	Windows 2000, 2003, XP
BMC Remedy Administrator	AR System server	N	6.03.00	Windows 2000, 2003, XP
BMC Remedy Alert	AR System server	Y	6.03.00	Windows 2000, 2003, XP
BMC Remedy Email Engine	o AR System server o Java SDK/JRE o An email exchange server	Y	6.03.00	Same as AR System server platforms
An email exchange server	None	Y	Any mail server using SMTP or MAPI standard protocols.	As appropriate
BMC Remedy Approval Server	AR System server	Y	6.03.00	Same as AR System server platforms
BMC Remedy Flashboards	o Mid Tier o AR System server	Y	6.03.00	Same as AR System server platforms
AREA LDAP Plug-in	o AR System server o LDAP directory service (optional)	Y	6.03.00	Same as AR System server platforms

TOE component	Dependency	Optional Y/N	Identification-Version	Underlying environment
LDAP directory service	None	Y	Any directory service using the LDAP standard protocol.	As appropriate
Web Browser (not evaluated)	o Mid Tier o AR System server	o N if Mid Tier installed. o N/A if Mid Tier not installed.	o Microsoft Internet Explorer 6.x	As appropriate

2.1.2 Logical scope and boundary

The TOE logical boundary consists of the security functionality of the AR System, including the optional BMC Remedy components described in Table 1.

The TOE provides the following security features:

- Cryptographic support: FCS
- User data protection: FDP
- Identification and authentication: FIA
- Security management: FMT
- Protection of the TSF: FPT (explicitly stated requirement)

FCS (Cryptographic support)

AR System provides optional encryption technology for encryption of API communications with the AR System server. When configured, AR System standard encryption causes all clients, the Mid Tier and the application servers to use public/private key technology to negotiate a secret session key when they initiate a session with the AR System server, and to encrypt all API calls to the server. This protects the user security attributes during network transmission. ***For the evaluated configuration, the administrator must configure BMC Remedy encryption to be turned on.***

Application server passwords are encrypted before they are stored in the appropriate configuration file, using the DES algorithm in combination with a proprietary AR System data manipulation.

FDP (User data protection):

Access to AR System data is controlled by the use of *access control groups*. A user's inclusion within a group, or groups, is established by the administrator in accordance with the locally specified access control policy (*GRP_ACC_CTRL*). AR System allows the administrator to set group-based permissions on various types of *AR System controlled objects*. This allows the administrator to control access at multiple levels, including applications and the components of applications, and data at the level of forms (tables), requests (rows) and fields (columns.) Groups further determine the type of operational access that group members have at each level, including view, modify, create, delete, execute, and no access. AR System server enforces access control at each level of access.

In AR System 6.3, the concept of *AR System roles* is introduced. AR System Roles allow an administrator designing an application to assign access control to application objects by AR System role, and each role is mapped to an access control group. In this way, when the application is distributed to local systems, access control by groups is maintained across a distributed network having differing group names that support similar roles. In this document, the term "AR System roles" is used to refer to this method of assigning permissions in AR System, while the term "roles" refers to the CC concept of a defined relationship governing the allowed interactions between a user and the TOE.

FIA (Identification and authentication):

AR System identifies users by the user name, which is stored in AR System. Users who access Remedy based solutions through BMC Remedy User or a web browser are prompted for a user name and password by AR System, and must be identified and authenticated before they can access the system. After identification and authentication, the user name is then used as part of every AR System server request, since no action can be taken unless a valid user name is associated with it.

In the evaluated configuration, AR System must be configured to use external authentication. In this configuration, AR System prompts the user for a user name and password. The user name and password entered are passed to the operating system (Windows or UNIX) or to an LDAP server. The operating system or LDAP server matches the user name, and authenticates the password, before the user can access the AR System. In this case, the user name assigned in AR System must match the user name in the external authenticating environment exactly. Configuring AR System to use external authentication is controlled from BMC Remedy Administrator.

In the evaluated configuration, the administrator must also configure the AR System to prevent anonymous access. There are two parts to this configuration. The administrator must replace the default administrator account and password with an administrator-designated administrator account and password. Also, the administrator must configure AR System to prevent access by guest users.

FMT (Security management):

The TOE provides administrators with interfaces to manage security policy and its implementation in BMC Remedy Administrator, BMC Remedy User, and the Configuration Tool. These clients allow the administrator to manage server objects and system configuration settings, and to control access to AR System by human users, Remedy based applications, and other external clients.

All user access definition and management is performed through forms that are accessible to authorized administrators in BMC Remedy User or through a browser, if the mid tier is configured to display forms. Policy management and implementation are controlled through the use of access control groups and security role definitions and privileges. Access control groups are the basis by which all user access is granted. Access control in AR System is additive. Each user starts out with no access to AR System controlled objects, and administrators add permissions as needed. Administrators can set default permissions and specific permissions on objects in AR System.

Roles, including security roles, are specified in the AR System by membership in groups. The AR System reserves eight group IDs for special group definitions with associated access privileges, including Administrator and Subadministrator.

Configuration of application servers, including application server passwords, is controlled by a combination of menu options in BMC Remedy Administrator, by forms accessible to the administrator through BMC Remedy User, and by settings in the ar.cfg (Windows) or ar.conf (UNIX) file.

FPT (Protection of the TSF):

The evaluated configuration includes optional application servers that automate commonly used workflow functions. These include the Approval Server, the Email Engine, Mid Tier, and Flashboards Server. The evaluated configuration also includes the optional AREA LDAP plug-in.

These optional application servers communicate directly with AR System server, and their access to AR System server is controlled by the application server passwords. If an application server attempts to connect to AR System server but does not pass the correct password, the connection fails.

These passwords can be changed by the administrator for additional security, by using BMC Remedy Administrator. These include the *Application Service Password*, used by the Approval Server, the Email Engine, and the Flashboards Server; the *Mid-Tier Administration Password*, used by Mid Tier, and the *Plug-in Server Local and Target Passwords*, used by the plug-in service and the AR System server during AREA LDAP authentication. In addition, there is a Remote Workflow Local Password that controls access by workflow originating in other AR System servers.

For the evaluated configuration, if using any of these optional components, the administrator must change the appropriate password(s) using BMC Remedy Administrator. The selected password must be at least six characters long.

3 TOE SECURITY ENVIRONMENT

3.1 Secure usage assumptions

This section describes the security aspects of the environment in which the TOE is intended to be used and the manner in which it is expected to be employed. The statement of the TOE security environment defines:

- Threats that the product is designed to counter.
- Assumptions made on the operational environment and the method of use intended for the product.

BMC Remedy Action Request System has been developed for an operating environment with a medium level of risk to identified assets. The assurance requirements of EAL 3 and the minimum strength of function of SOF-basic were chosen to be consistent with that level of risk

The operational environment must be managed in accordance with assurance requirement documentation for delivery, operation, and user/system administrator guidance. The following specific conditions are assumed to exist in an environment where this TOE is employed.

3.1.1 Environment assumptions

The environmental assumptions delineated in Table 3 are required to ensure the security of the TOE:

Table 3: Environmental assumptions

Assumption	Description	Aspect
A.DAC	The host platform operating system of the TOE environment will provide discretionary access control (DAC) to protect TOE executables and TOE data.	Connectivity
A.DB_LOCKED_DOWN	The component database has had all current security patches (if applicable) applied, and the Authorized Administrator has configured the inherent database security mechanisms to their most restrictive settings that will still permit TOE functionality and interoperability. Any such patch does not interfere with the correct functioning of AR System server's interface to the database.	Connectivity

Assumption	Description	Aspect
A.EXTERNAL_ AUTHENTICATION	The TOE environment will provide authentication mechanisms, as described in section 6.1.2, Table 12: Types of external authentication, and these mechanisms will function correctly and accurately.	Connectivity
A.INSTALL	The TOE software has been delivered, installed, and set up in accordance with documented delivery and installation/setup procedures and the evaluated configuration.	Personnel
A.MANAGE	There will be one or more competent Authorized Administrators assigned to manage the TOE and the security functions it performs. Procedures will exist for granting Authorized Administrators access to the TSF.	Personnel
A.NO_EVIL_ADM	An Authorized Administrator is not careless, willfully negligent, nor hostile, and will follow and abide by the instructions provided by the Administrator documentation.	Personnel
A.PEER_ASSOCIATION	Any other systems with which the TOE communicates are assumed to be under the same management control and operate under the same security policy constraints. This includes the network. (The network operates under the same constraints and resides within a single management domain.)	Physical
A.PHYSICAL_PROTECT	The processing resources of the TOE will be located within facilities providing controlled access to prevent unauthorized physical access.	Physical
A.PLATFORM_SUPPORT	The underlying platform(s) upon which the TOE executes will provide reliable functionality including correct hardware operation and functionality, and correct platform software operation.	Physical
A.TIME	The operating environment will provide reliable system time.	Connectivity
A.SECURE_ COMMUNICATION	The TOE IT environment will provide the ability to configure SSL communications where appropriate.	Connectivity
A.CONNECT	Any network resources used for communication between TOE components will be adequately protected from unauthorized access.	Connectivity

3.2 Threats

3.2.1 Threats addressed by the TOE

Table 4 identifies the threats to the TOE. The threats to the TOE are considered to be unauthorized users with public knowledge of how the TOE operates and who possess the skills and resources to alter TOE configuration settings, or parameters, or both. The threat agents do not have physical access to the TOE. Mitigation to the threats is through the objectives identified in Section 4, Security Objectives.

Table 4: Threats addressed by the TOE

Threat	Description
T.UNAUTH_ACCESS	An unauthorized user or subject might gain access to system data to view, modify, or delete that data, or execute system applications or modify system applications in order to disrupt, or otherwise hinder, business operations.
T.EXCEED_PRIV	Human users of the TOE might attempt to view, modify, or delete TOE objects, or execute or modify applications for which they do not have the prescribed authority, as specified by local policy, in order to disrupt, or otherwise hinder, business operations.
T.MANAGE	Administrators of the TOE might not have utilities sufficient to effectively manage the security functions of the TOE, as specified by local security policy.

4 SECURITY OBJECTIVES

The purpose of the security objectives is to address all of the security concerns, and to show which security concerns are addressed by the TOE, and which are addressed by the environment. Threats can be directed against the TOE or the security environment or both. Therefore, the CC identifies two categories of security objectives:

- Security objectives for the TOE
- Security objectives for the environment

4.1 Security objectives for the TOE

This section identifies and describes the security objectives for the TOE, as shown in Table 5.

Table 5: Security objectives for the TOE

Security Objective	Description
O.AUTHORIZATION	The TSF must ensure that only authorized users and applications gain access to the TOE and its resources.
O.DISCRETIONARY_ACCESS	The TSF must limit access to named objects maintained by the TOE to users or applications with authorization and appropriate privileges. The TSF must allow authorized users to specify which users can access their objects and the actions performed on the objects.
O.MANAGE	The TSF must provide all of the functions and facilities necessary to support the Authorized Administrators that are responsible for the management of TOE security.

4.2 Security objectives for the non-IT environment

This section identifies and describes the security objectives for the non-IT environment.

Table 6: Security objectives for the non-IT environment

Objective	Description
OE.DB_LOCKED_DOWN	Those responsible for the TOE must ensure that the associated database has had all current patches applied, and is configured in the most restrictive way that will still allow TOE access to the database. They must also assure that any future security patches do not interfere with the correct functioning of AR System server's interface to the database.

Objective	Description
OE.INSTALL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner that is consistent with IT security, with documented delivery and installation/setup procedures, and with the evaluated configuration.
OE.PERSON	Authorized administrators of the TOE shall be properly trained and competent in the configuration and usage of the TOE, and will follow the guidance provided. These users are not careless, negligent, or hostile.
OE.PHYSICAL	Those responsible for the TOE must ensure that the host computer system(s) containing the AR System server, database, BMC Remedy Administrator, and other installed optional TOE components are protected from physical attack.
OE.PEER_ASSOCATION	Those responsible for the TOE must ensure that the systems with which the TOE communicates, including the network, are operated under the same management control and security policies as the TOE.
OE.DAC	Those responsible for the host platform operating system of the TOE environment must ensure that it provides discretionary access control (DAC) to protect TOE executables and TOE data.
OE.PLATFORM_SPT	Those responsible for the TOE operating environment must ensure that it provides reliable platform functions, including correct hardware operation and functionality, and correct platform software operation and functionality.

4.3 Security objectives for the IT environment

This section identifies and describes the security objectives for the IT environment.

Table 7: Security objectives for the IT environment

Objective	Description
OE.EXTERNAL_AUTHENTICATION	The TOE operating environment must provide authentication mechanism(s) to authenticate identified users of the TOE. Those responsible for the TOE must ensure that such external authentication mechanisms function accurately and correctly.
OE.TIME	The TOE operating environment must provide correct system time.

Objective	Description
OE.SECURE_COMMUNICATION	The TOE operating environment must provide the ability to configure SSL communications.
OE.SEP	The TOE operating environment shall provide mechanisms to isolate the TOE Security Functions (TSF) and assure that TSF components cannot be tampered with or bypassed.

5 IT SECURITY REQUIREMENTS

This section defines the IT security requirements that shall be satisfied by the TOE or its environment.

The CC divides TOE security requirements into two categories:

- Security functional requirements (SFRs) (such as identification and authentication, security management, and user data protection) that the TOE and the supporting evidence need to satisfy to meet the security objectives of the TOE.
- Security assurance requirements (SARs) that provide grounds for confidence that the TOE and its supporting IT environment meet its security objectives (e.g., configuration management, testing, and vulnerability assessment).

These requirements are discussed separately in the following subsections.

5.1 TOE security functional requirements

The TOE satisfies the SFRs delineated in Table 8.

Table 8: TOE security functional requirements

Functional component ID	Functional component name
Cryptographic support (FCS)	
FCS_COP.1	Cryptographic operation
FCS_CKM.1	Cryptographic key generation
FCS_CKM.4	Cryptographic key destruction
User data protection (FDP)	
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
Identification and authentication (FIA)	
FIA_ATD.1	User attribute definition

Functional component ID	Functional component name
FIA_UID.2	User identification before any action
FIA_USB.1	User-subject binding
Security management roles (FMT)	
FMT_MOF.1	Management of security functions behavior
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialization
FMT_SMF.1	Specification of management functions
FMT_SMR.1	Security roles
Protection of the TSF (FPT)	
FPT_APP_EXP.1	Application server authentication

The remainder of this section contains a description of each component and lists any related dependencies.

5.1.1 Class FCS: Cryptographic support

FCS_COP.1	**Cryptographic operation**
Hierarchical to:	No other components
FCS_COP.1.1(1)	The TSF shall perform [encryption and decryption of API communications] in accordance with a specified cryptographic algorithm [DES] and cryptographic key sizes [56 bits] that meet the following [the DES algorithm as implemented by OpenSSL].
FCS_COP.1.1(2)	The TSF shall perform [encryption and decryption of application service passwords and the Configuration Tool password for file storage] in accordance with a specified cryptographic algorithm [DES in combination with a proprietary BMC data manipulation algorithm] and cryptographic key sizes [24-bit proprietary BMC key in combination with a data manipulation algorithm] that meet the following [DES as implemented by OpenSSL and data manipulation algorithms as implemented by OpenSSL and BMC].
Dependencies:	FCS_CKM.1 Cryptographic key generation FCS_CKM.4 Cryptographic key destruction FMT_MSA.2 Secure security attributes

FCS_CKM.1	**Cryptographic key generation**
FCS_CKM.1.1	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [RSA] and specified cryptographic key sizes [672] that meet the following: [the RSA algorithm as implemented by OpenSSL].
Hierarchical to:	No other components
Dependencies:	FCS_COP.1 Cryptographic operation FCS_CKM.4 Cryptographic key destruction FMT_MSA.2 Secure security attributes

FCS_CKM.4	**Cryptographic key destruction**
FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [freeing of the data structure] that meets the following: [List of standards: none]
Hierarchical to:	No other components
Dependencies:	FCS_CKM.1 Cryptographic key destruction FMT_MSA.2 Secure security attributes

5.1.2 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 [GRP_ACC_CTRL SFP] on [Subjects: Users and the session representing the user; Objects: AR System controlled objects (applications, forms, fields, data records (requests), active links, active link guides, web services, packing lists, and Flashboards data sources); Operations: Read, modify, create and delete, and execute, as appropriate to the object type.]
Dependencies:	FDP_ACF.1 Security attribute-based access control

FDP_ACF.1	**Security attribute based access control**
Hierarchical to:	No other components
FDP_ACF.1.1	The TSF shall enforce the [GRP_ACC_CTRL SFP] to objects based on the following: [Subjects: Users and the session representing the user;

	Objects: AR System controlled objects (applications, forms, fields, data records (requests), active links, active link guides, web services, and Flashboards data sources); Attributes: User name and group membership of the user, and object permission types Visible, Hidden, View, Change, permission granted, and none, as defined in the permission list of the AR System controlled object.]
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [Access is granted if any one of the following is true: 1) The user is a member of one of the following explicit groups: a. Administrator group – Members of the Administrator group have full access and can perform all operations on all AR System controlled objects. b. Subadministrator group – Members of the Subadministrator group have full administrator access to a subset of existing objects only (forms, applications, packing lists, and related workflow). They can perform all operations, but only on the designated subset of AR System controlled objects. c. Customize group – Members of the Customize group can customize the layout of their view of forms for which they have Visible permission, as described below (view and modify operations). 2) The user is a member of any group that is also contained in the AR System controlled object's permission list, or of any group that is mapped to an AR System role that is contained in the object's permission list. In this case, the user can perform operations according to the following rules: a. Permission type Visible, object type application or active link guide: read and execute operations. b. Permission type Visible, object type form: read operations. c. Permission type Hidden, object type application or active link guides: execute operations. d. Permission type Hidden, object type form: read, create or delete operations, as controlled by the related application or workflow. e. Permission type View, object type field: read operations. f. Permission type Change, object type field: read and modify operations.

	g. Permission granted, object type active link: read and execute operations. h. Permission granted, object type Flashboards data source: read operations as allowed by form and field permissions associated with the flashboard. i. Permission type Hidden or Visible, object type web service: read operations.
FDP_ACF.1.3	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [Access to requests (records) is controlled by the use of the implicit groups Submitter, Assignee, Assignee Group, or an administrator-created dynamic group, as follows: 1) The Submitter group is in the Request ID field (field ID 1) of the record, and the user name is in the Submitter field (field ID 2) of the record. In this case the user is a member of the implicit group Submitter, and can perform read or modify operations on the record, according to the permissions granted. 2) The Assignee group is in the Request ID field, and the user name is in the Assigned To field (field ID 4) of the record. In this case the user is a member of the implicit group Assignee, and can perform read or modify operations on the record, according to the permissions granted. 3) The Assignee Group group is in the Request ID field, and the user is a member of a group that is listed in the Assignee Group field (field ID 112) of the record, or is a member of a group that is mapped to an AR System role that is listed in field 112 of the record, or the user's user name is listed in field 112 of the record. In these cases the user is a member of the implicit group Assignee Group, and can perform read or modify operations on the record, according to the permissions granted. 4) A dynamic group is in the Request ID field, and the user is a member of a group that is listed in that dynamic group field (field IDs 60000-60999) of the record, or is a member of a group that is mapped to an AR System role that is listed in that dynamic group field of the record, or the user's user name is listed in that dynamic group field of the record. In this case the user is a member of that implicit dynamic group, and can perform read or modify operations on the record, according to the permissions granted.]
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

5.1.3 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 name and group membership].
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

FIA_USB.1	**User-subject binding**
Hierarchical to:	No other components
FIA_USB.1.1	The TSF shall associate the following user security attributes with subjects acting on behalf of that user: [user name and password].
FIA_USB.1.2	The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [At session initialization, AR System shall associate the values of the security attributes user name and password with the session.]
FIA_USB.1.3	The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [the user security attributes associated with the session shall not be changed during the session.]
Dependencies	FIA_ATD.1 User attribute definition

5.1.4 Class FMT: Security management

FMT_MOF.1	**Management of security functions behavior**
Hierarchical to:	No other components
FMT_MOF.1.1	The TSF shall restrict the ability to *determine the behavior of, disable, enable, modify the behavior of* the functions [1) Identification and Authentication mechanism, including configuring external authentication 2) Management of user names, groups, and user membership in

	groups 3) Mapping of groups to AR System roles 4) Management of AR System controlled object permissions 5) Limit of access by anonymous users 6) Management of AR System Server information settings 7) Management of application server passwords to [the AR System administrator(s) in the Administrator group, or to subadministrators in the Subadministrator group where assigned].
Dependencies:	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles

FMT_MSA.1	**Management of security attributes**
Hierarchical to:	No other components
FMT_MSA.1.1	The TSF shall enforce the [GRP_ACC_CTRL SFP] to restrict the ability to *change_default, modify, delete, [create, view]* the security attributes [1) Access control attributes associated with users, including user name, groups, and group membership 2) The permission list of AR System controlled objects 3) Mapping of groups to AR System roles] to [the AR System administrator(s) in the Administrator group, or to subadministrators in the Subadministrator group where assigned].
Dependencies:	FDP_ACC.1 Subset access control FMT_SMR.1 Security roles FMT_SMF.1 Specification of management functions

FMT_MSA.3	**Static attribute initialization**
Hierarchical to:	No other components
FMT_MSA.3.1	The TSF shall enforce the [GRP_ACC_CTRL SFP] to provide *restrictive* default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow the [Authorized Administrators within the Administrator or Subadministrator access control group] 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_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: [1) Manage the GRP_ACC_CTRL SFP, including: a. Individual human user security attributes b. AR System groups and AR System roles c. AR System controlled object permission lists 2) Manage the identification and authentication mechanism 3) Limit access by anonymous users 4) Manage AR System server Information settings 5) Manage the application server passwords 6) Manage encryption settings].
Dependencies:	No Dependencies

FMT_SMR.1	**Security roles**
Hierarchical to:	No other components
FMT_SMR.1.1	The TSF shall maintain the roles [1) Authorized administrators within the Administrator access control group; 2) Authorized subadministrators within the Subadministrator access control group.]
FMT_SMR.1.2	The TSF shall be able to associate users with roles.
Dependencies	FIA_UID.1 Timing of identification

5.2 Explicitly stated requirements for the TOE

The following table describes explicitly stated security functional requirements for the TOE.

5.2.1 Class FPT: Protection of the TSF

FPT_APP_EXP.1	**Application server authentication**
Hierarchical to:	No other components
FPT_APP_EXP.1.1	The TSF shall be able to identify and authenticate authorized application servers that act as part of the TOE for the transfer of TOE data and the execution of workflow within the TOE.
Dependencies	No dependencies

5.3 TOE security assurance requirements

Table 9 identifies the security assurance components drawn from CC Part 3 Security Assurance Requirements EAL3. The SARs are not iterated or refined from Part 3.

Table 9: EAL3 assurance requirements

Assurance class	Assurance components
Configuration Management (ACM)	Authorization controls (ACM_CAP.3)
	TOE CM coverage (ACM_SCP.1)
Delivery and Operations (ADO)	Delivery procedures (ADO_DEL.1)
	Installation, generation, and start-up procedures (ADO_IGS.1)
Development (ADV)	Informal functional specification (ADV_FSP.1)
	Security enforcing high-level design (ADV_HLD.2)
	Informal correspondence demonstration (ADV_RCR.1)
Guidance Documents (AGD)	Administrator guidance (AGD_ADM.1)
	User guidance (AGD_USR.1)
Life Cycle Support (ALC)	Identification of security measures (ALC_DVS.1)
Tests (ATE)	Analysis of coverage (ATE_COV.2)
	Testing: High-level design (ATE_DPT.1)
	Functional testing (ATE_FUN.1)
	Independent testing – sample (ATE_IND.2)
Vulnerability Assessment (AVA)	Examination of guidance (AVA_MSU.1)
	Strength of TOE security function evaluation (AVA_SOF.1)
	Developer vulnerability analysis (AVA_VLA.1)

5.4 Security requirements for the IT environment

The following table describes the security requirements for the IT environment. The CC components in this section are refined as indicated to reflect the fact that they are requirements for the IT environment. The refinements to the requirements FIA_UAU.2 and FIA_UID.2 also reflect the fact that the TOE relies on the IT environment to authenticate the user by checking user name and password, before the user can take any action within the TOE.

Table 10: Security requirements for the IT environment

Functional component ID	Functional component name
User data protection (FDP)	
FDP_ITT.1	Basic internal transfer protection
Identification and authentication (FIA)	
FIA_ATD.1	User attribute definition
FIA_UAU.2	User authentication before any action
FIA_UID.2	User identification before any action
Protection of the TSF (FPT)	
FPT_SEP.1	Domain separation
FPT_STM.1	Reliable time stamp

5.4.1 User data protection (FDP)

5.4.1.1 Basic internal transfer protection (FDP_ITT.1)

5.4.1.1.1 FDP_ITT.1.1

The **IT Environment** shall enforce the [locally specified SSL communication policy] to prevent the *disclosure* of user data when it is transmitted between physically-separated parts of the TOE, where appropriate.

5.4.2 Identification and authentication (FIA)

5.4.2.1 User attribute definition (FIA_ATD.1)

5.4.2.1.1 FIA_ATD.1.1

The **IT environment** shall maintain the following list of security attributes belonging to individual users:

- [User name
- Password (authentication data)]

5.4.2.2 User authentication before any action (FIA_UAU.2)

5.4.2.2.1 FIA_UAU.2.1

The TSF shall require each user to be successfully authenticated **by the IT Environment** before allowing any other TSF-mediated actions on behalf of that user.

5.4.2.3 User identification before any action (FIA_UID.2)

5.4.2.3.1 FIA_UID.2.1

The TSF shall require each user to **be successfully identified by the IT environment** before allowing any other TSF-mediated action on behalf of that user.

5.4.3 Protection of the TSF (FPT)

5.4.3.1 Domain separation (FPT_SEP.1)

5.4.3.1.1 FPT_SEP.1.1

The **IT environment** shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

5.4.3.1.2 FPT_SEP.1.2

The **IT environment** shall enforce separation between the security domains of subjects in the **IT environment.**

5.4.3.2 Reliable time stamp (FPT_STM.1)

5.4.3.2.1 FPT_STM.1.1

The **IT environment** shall be able to provide reliable time stamps for use **by the TSF**.

5.5 SFRs with SOF declarations

This ST makes a claim of SOF-Basic for the following security functional requirement:

- FPT_APP_EXP.1 – Application server authentication

6 TOE SUMMARY SPECIFICATION

This section presents an overview of the security functions implemented by the TOE and the Assurance Measures applied to ensure their correct implementation.

6.1 TOE security functions

6.1.1 Cryptographic support—TSF_FCS

AR System provides a feature called BMC Remedy Encryption for encryption of API communications with the AR System server. AR System standard level encryption is installed with the AR System server, and must be configured by the administrator. When configured, AR System standard encryption causes the AR System server to generate a public and private key pair at startup, using the RSA key-generation algorithm. A new public/private key pair is regenerated at intervals, based on a configurable timeout. When any client (including the Mid Tier or an application server) connects to the AR System server, the C API carries out a key negotiation between client and server. This results in a secret session key which is used to encrypt all API calls to the server, using the DES algorithm. The secret session key is also subject to a configurable timeout. This functionality protects the user security attributes during network transmission. AR System uses encryption algorithms provided by OpenSSL.

All Windows-based GUI clients, all command-line clients, the Approval server and the Plug-in server utilize the C API for communication with the AR System server. AR System components that utilize the Java API, including the Mid Tier, the Email Engine, and the Flashboards server, pass all API calls through a JNI layer, where they are converted to the C API. Since all communication with the AR System server must come through the C API, all components implement this encryption functionality when the session is initiated.

Application server passwords and the Configuration Tool password are encrypted before they are stored in the appropriate configuration file. In this case, the DES algorithm is combined with a proprietary AR System algorithm to generate the encrypted password. Because the encryption methodology is proprietary and internal to AR System code, no external key generation or destruction method is required. Components that implement encryption of application server passwords include the AR System server, the Mid Tier Configuration Tool, the Flashboards installation script, and the Email Engine installation script. Components that implement decryption of the application service passwords include AR System server and Plug-in server, the Mid Tier, the Flashboards server, the Email Engine, and the Approval server. The Mid Tier Configuration Tool decrypts the Configuration Tool password.

Note: The evaluated configuration relies on the IT Environment to ensure that user authentication data is protected when it must be transmitted outside the TOE. This includes communication between a browser and the Mid Tier, if the Mid Tier is in use. It also includes communication between the Plug-in service and an LDAP directory server, if AREA LDAP is used for external authentication. For this reason the security requirement FDP_ITT.1 is placed on the IT environment and the administrator is required to configure SSL for these two elements of the evaluated configuration.

6.1.2 User data protection–TSF_FDP

Functional requirement FDP_ACC.1 (Subset access control)

User access to AR System is controlled at multiple levels. This section describes user access control for AR system controlled objects and data. See the section "Identification and Authentication—TSF_FIA" for a description of overall AR System access.

User access to AR System controlled objects and data is granted and controlled by making all users members of access control groups, and then granting the appropriate type of permission to the appropriate groups or to AR System roles, which are mapped to groups. The object permission type determines whether the user can read, modify, create, delete or execute the object.

Group or AR System role permissions can be set for all AR System controlled objects, including applications, forms (tables), requests (records or rows), fields (columns), active links and active link guides (application and workflow control), web services, and Flashboards data sources.

(The object types filter, filter guide, and escalation are only accessible to administrators and subadministrators, and are only executed by AR System server, and therefore do not require permissions. Menus are objects that are only associated with fields and access to them is therefore controlled by the associated field's permissions. While packing list permissions can be assigned, such permissions are not used for access control, since packing lists are only accessible to administrators and subadministrators. For users, access is controlled to the AR System controlled objects contained in the packing list instead.)

The above functionality satisfies FDP_ACC.1.1 by enforcing access control to AR System controlled objects based on group membership.

Functional requirement FDP_ACF.1 (Security attribute based access control)

A user's inclusion within a group, or groups, is established by the administrator in accordance with the locally specified access control policy (GRP_ACC_CTRL). Similarly, AR System roles allow an administrator designing an application to enforce the locally specified access control policy across a distributed network having differing group names that support similar roles.

Users are made members of groups by means of the User form. This form is only accessible to members of the Administrator group. Users are not given membership in AR System roles directly. Instead, when the application is distributed, the administrator must map a local AR System explicit group to each of the application's AR System roles. Thus when permission is granted to an AR System role, the user's access to the object is determined by the user's group membership. AR System roles are mapped to groups by means of the Roles form, which is only accessible to members of the Administrator group.

When a user attempts to access an AR System controlled object, AR System server verifies the group or AR System role permissions set for the object against the user's group memberships, which are listed in the User form along with the user name, to determine if access to the object is granted. Users have access to the object if they are members of a single group with access, even if they are members of other groups that are not given access.

Object permission types determine what type of operational access a user has to an object, application, or workflow. Permission types in AR System include Visible/Hidden, View/Change, and permission or no permission. The possible permission types vary with the object type, as shown in the following table.

Table 11: AR System controlled object permission types

Access type	Relevant objects	Description
No permission	All objects	Members of the group have no access to the object.
Visible	Applications Forms Active link guides	Members of the group have permission to view or select the object in the object list in BMC Remedy User or in a browser, or can select the object from the home page. Visible permission gives read access to forms, and read and execute access to applications and active link guides.
Hidden	Applications Forms Active link guides	Members of the group have access to the object through workflow, but the object does not appear in the object list in BMC Remedy User, and cannot be selected on the home page or opened in a browser. Through workflow, Hidden permission gives execute access to applications and active link guides, and read access to forms that are part of the application or workflow.
Visible/Hidden	Web services	Although the Visible/Hidden icon appears and either can be selected, permissions for Web services are the same whether you choose Visible or Hidden. To publish a web service, you give permission to the group Public. This grants read access to the web service for members of the group Public.
View	Fields	Members of the group have permission to view (read) the field and its contents.
Change	Fields	Members of the group have permission to view and change (read and modify) the field contents.
Permission	Active links Flashboards data sources	Members of the group have access to the object. For active links, this allows for execute operations. For Flashboards, this permission grants access to the flashboard.

Access to requests (row-level access) is granted by the user’s membership (usually dynamically assigned) in one or more of the implicit groups Submitter, Assignee, Assignee Group, or any customer-created dynamic group, as described below.

There are two types of groups in AR System – explicit and implicit. Explicit groups are those to which users must be explicitly assigned by an authorized administrator. When a user is assigned to an explicit group, the user is granted access to all items to which the group is granted access. Implicit groups are those that depend on specific user circumstance and situations; users are not directly assigned to implicit groups. Membership in an implicit group is based on specific conditions, such as the contents of certain fields within each request (record). This field content is usually controlled by the application or workflow.

There are three predefined explicit administration groups. They are:

- Administrator: Members of the Administrator group have full and unlimited access to AR System, and thus can perform all operations on all object types. (Members of this group must have a Fixed Write license, or else the group membership will be ignored.)

- Subadministrator: Members of the Subadministrator group have administrator access to a limited set of objects to which the group has been given specific access, such as an application and its related forms and active link guides. They can perform all operations on all object types, but only within the assigned set of related objects. (Members of this group must have a Fixed Write license, or else the group membership will be ignored.)

- Customize: Members of the Customize group can modify the layout of their view of forms to which they have Visible permission by means of membership in another group (such as Public).

Membership in implicit groups changes dynamically based on the content of certain fields in the record, and is used to grant access to requests (row-level access.) For the Assignee, Submitter and Assignee Group groups, the field content that determines group membership is usually entered by the application or workflow. The reserved implicit groups are:

- Public: All users are part of public.

- Assignee: The user name in the Assigned To field (a core required field with field ID 4) of the record has operation access as determined by permission type granted to the Assignee group in the Request ID field of the record.

- Submitter: The user name in the Submitter field (a core required field with field ID 2) of the record has create access when submitting a new request, and operation access as determined by permission type granted to the Submitter group in the Request ID field of the record for existing requests.

- Assignee Group: For requests containing the Assignee Group field (field ID 112) all members of the groups listed in the record’s Field 112, members of groups mapped to any AR System roles listed in the record’s field 112, or users directly listed in the record’s field 112, have operation access as defined by permission type granted to the Assignee Group group in the Request ID field of the record.

In addition to the reserved groups, AR System allows the administrator to create the following types of groups:

- Regular: Regular groups are explicit groups that the administrator creates, according to roles needed for the application and within the organization.

- Dynamic: Dynamic groups are implicit groups created by the administrator (reserved field IDs 60000-60999.) They can be used to grant row-level access in the same way as the Assignee Group.

- Computed: Computed groups are explicit groups. The administrator can use a formula to assign other specific groups and individual users to a computed group. Members of a group that is part of a computed group, or users that are direct members of a computed group, have operation access to objects as determined by permission type.

The functionality described above satisfies the functional requirements FDP_ACF.1.1, FDP_ACF.1.2, FDP_ACF.1.3 and FDP_ACF.1.4 by controlling access of subjects to objects on the basis of security attributes and according to a set of rules, and by using permission type to control the type of operation access, in order to enforce the locally specific access control policy (GRP_ACC_CTRL SFP).

Note: Although licensing is not a component of access control, it can affect whether users are able to perform an operation that they have been granted permission to perform. For example, in most cases, if a user is a member of a group with Change permission to a field, but the user has not been granted a write license, then they will not be able to change the field. Also, each member of the group Administrator and Subadministrator must have a Fixed write license. The administrator can configure AR System to allow users with a Read license to perform limited write actions, including creating records and modifying their own (submitted) records.

6.1.3 Identification and authentication – (TSF_FIA)

Functional requirement FIA_ATD.1 (User attribute definition)

The user name and group membership attributes are stored in the User Form in AR System. Since the evaluated configuration uses external authentication (see the subsection Functional requirement FIA_UID.2, below) users' passwords are not stored in the AR System. The security attributes user name and group membership are used by AR System server when checking access to AR System controlled objects, as described in section 6.1.1.

The above functionality satisfies the functional requirement FIA_ATD.1.1 by maintaining the user name and group membership security attributes.

Functional requirement FIA_UID.2 (User identification before any action)

The AR System uses a hierarchical access control scheme to protect information from unauthorized access. If users are denied permission at any level, they cannot proceed to the next level. The first level of access is to the AR System server. Users are presented with a login dialog box, and must identify themselves by user name, and enter their password along with an *authentication string* (as described in Table 12) if required. The user name and password must be successfully authenticated before the user can perform any action within AR System. The login dialog box is presented by all Windows components of the client tier, including BMC Remedy Administrator, BMC Remedy User, Import, and Alert. The Mid Tier also presents a login window to users logging in with a browser.

For this evaluation, the AR System must use external authentication as the method to authenticate users. There are three types of external authentication. Two of the three methods use the field Authentication String, found in the login dialog box. For authentication by the Windows domain or by an LDAP server, the contents of this field are used to identify the authentication domain or service, respectively. The field is not used if AR System is using UNIX for external authentication. Depending on the system configuration, users can be authenticated by the methods shown in Table 12:

Table 12: Types of external authentication

External authentication method	Description
To the Operating System (UNIX only)	The AR System server authenticates the user name and password against the operating system's /etc/passwd (or equivalent) file. The authentication string field is not used when authenticating to the UNIX operating system.
To the server domain (Windows NT/2000)	The AR System server passes login authentication information to the Windows NT/2000/XP server domain. In this case, the Windows logon domain of the user must be entered in the Authentication String field. That value will determine which Windows domain the AR System server will send the login authentication information to.
To an LDAP server using the AREA Plug-in service	To use this mechanism, the AR System administrator must install the Action Request System External Authentication (AREA) LDAP plug-in. If configured, the AR System server will provide the AREA service the login information provided by the user: user name, password, and authentication string. In this case, the authentication string is used to identify the authentication service. When this method is used, AR System server waits for a configurable period of time for a response from the AREA LDAP plug-in when making an external authentication call.

When using external authentication, the AR System server requests the external system to authenticate the password entered by the user against their Windows NT/UNIX/LDAP login password instead of maintaining an AR System specific password. To configure this, the administrator must take all three of the following actions:

- Ensure that the AR System user name and the operating system user name are identical;
- In BMC Remedy User, leave the Password field in the User form blank in AR System server;
- In BMC Remedy Administrator, select the Cross Ref Blank Password check box in the Configuration tab of the Server Information dialog box.

Guest users are those users who are not "recognized" users (i.e., not listed in the User form). AR System allows administrators to control whether guest users are allowed to access AR System. ***In the evaluated configuration, guest users are not allowed.***

The functionality described above satisfied the functional requirement FIA_UID.2.1 by requiring users to be identified before they can take any other action in the AR System.

Functional requirement FIA_USB.1 (User-subject binding)

When the user supplies a user name and password at the login dialog box, and is successfully authenticated, the user name and password are stored for use by the API during the user's session. All requests to the AR System server for any user action are made through the AR System API, and every request made through the AR System API to the AR System server must have a valid, authenticated identification attached. The AR System API stores the user name and password at the time the user's session is initiated, and it maintains this information for the duration of the session.

The functionality described above satisfies FIA_USB.1.1 by associating the security attributes user name and password with the user's session. It satisfies FIA_USB.1.2 by associating these user security attributes with the session at session initialization. It satisfies FIA_USB.1.3 by maintaining the user security attributes without change throughout the session.

6.1.4 Security management roles – (TSF_FMT)

In AR System, authorized administrators use various options in BMC Remedy User, BMC Remedy Administrator, and the Configuration Tool to manage access control and other aspects of security policy.

Functional requirement FMT_MOF.1 (Management of security functions behavior)

The AR System supports the use of the authorized administrator role to manage users and access control groups, as well as all other aspects of the AR System server and TOE management and configuration. A user is associated with the authorized administrator role by membership in the Administrator access control group.

Authorized administrators use BMC Remedy User to create and manage user names and group membership by accessing the User and Group forms from the object list in BMC Remedy User. Only members of the Administrator group have access to the User and Group forms in BMC Remedy User; these forms do not appear in the object list for other users. Authorized administrators access the Roles form in BMC Remedy User to map each AR System role to an explicit group. Only members of the Administrator group have access to the Roles form.

Authorized administrators use BMC Remedy Administrator to develop applications, and to manage and configure AR System administration security settings and functions. Only Members of the Administrator and Subadministrator groups can run BMC Remedy Administrator. The "Server information" dialog provides the administrative interface for authorized administrators to set or modify server settings for AR System server and the application servers, including configuring external authentication, changing application server passwords, and limiting access by anonymous users. Subadministrators can view the server information settings, but cannot change them.

Authorized administrators and subadministrators also use BMC Remedy Administrator to manage object permissions. Administrators can assign and remove permissions for all AR System controlled object types. Subadministrators can only view objects to which they have been granted subadministrator permission, and can assign and remove permissions for those objects only.

Mid Tier is managed through the Configuration Tool, which is a JSP servlet hosted by the mid tier. Access to the Configuration Tool is controlled by the Configuration Tool password. Administrators can change this password in the Configuration Tool. ***In the evaluated configuration, the administrator must change the Configuration Tool password from the default after completing installation of the Mid Tier.***

AR System also supports the role of authorized subadministrator, by membership in the explicit group Subadministrator. Subadministrators can administer forms to which they have been given access, and can create, delete and modify (including granting object permissions) the filters, active links, and escalations connected to those forms. They can also view, but not change, AR System server information.

The functionality described above satisfies the functional requirement FMT_MOF.1.1, by restricting the ability to determine the behavior of, disable, enable and modify the behavior of the TSF to authorized administrators and subadministrators.

Functional requirement FMT_MSA.1 (Management of security attributes)

Administrators and subadministrators must manage the appropriate permissions to AR System controlled objects (applications, forms, fields, requests, active links, active link guides, web services, and Flashboards data sources) according to the GRP_ACC_CTRL security policy. They do so by maintaining the access control attributes associated with users (user name, groups and group membership) in the User and Group forms in BMC Remedy User, and by assigning and revoking permissions to AR System controlled objects in BMC Remedy Administrator. Administrators can also change the default permissions for each object type in Remedy Administrator.

Only members of the Administrator group have access to the User and Group forms, where they can view, create, delete and modify user names, groups, and group membership. Only members of the Administrator group have access to the Roles form, where they can map AR System roles to explicit groups. Only members of the Administrator group have access to all AR System controlled objects. Members of the Subadministrator group can manage only those AR System controlled objects to which they have been granted subadministrator rights by the administrator.

The functionality described above satisfies the functional requirement FMT_MSA.1.1, by restricting the ability to view, create, delete, modify and change the default settings for the security attributes user name and group membership, and the permission lists of AR System controlled objects, to authorized administrators and subadministrators.

Functional requirement FMT_MSA.3 (Static attribute initialization)

Access control in AR System is additive. By default, new objects have no permissions, and administrators must add them. Also by default, each user starts out as a member of no explicit groups, and administrators add group membership as needed.

Administrators can set default group permissions to object types, so that new objects are created with the default permissions.

The functionality described above satisfies the functional requirements FMT_MSA.3.1 and FMT_MSA.3.2 by providing restrictive default values for object permissions and group membership, and by allowing authorized administrators to change these defaults.

Functional requirement FMT_SMF.1 (Specification of management functions)

Administrators use the security functionality provided in BMC Remedy User to manage individual human user security attributes including user name and group membership, group definition, and mapping of AR System roles to groups. Administrators use the security functionality provided in Remedy Administrator to manage AR System controlled object permissions. These functions work together to implement user access control and the GRP_ACC_CTRL SFP.

Administrators also use BMC Remedy Administrator to manage the security configuration of AR System. This includes managing the identification and authentication mechanism and settings, such as configuring external authentication and limit of access by anonymous users. It also includes changing the application server passwords. The application servers are part of the TOE, and are identified internally when they connect to AR System server. The administrator can change the default (hidden) password to ensure that only known instances of the application servers can connect to AR System server in their environment. These passwords are set in AR System server by using BMC Remedy Administrator, and are set for each application server by editing the appropriate form in BMC Remedy User. The application server passwords are:

- Application Service Password – Used by Email Engine, Approval Server, and Flashboards Server when connecting to AR System server.
- Mid Tier Administration Password – Used by Mid Tier when connecting to AR System server.
- Plug-in Server Local Password – Used by the AREA LDAP plug-in when connecting to AR System server.

For the evaluated configuration, the administrator must change these passwords from the default if the components in question are installed.

Administrators manage the configuration of standard encryption by using a text editor to modify the server configuration file ar.cfg (Windows) or ar.conf (UNIX). This file is located in the *<AR_System_install>*/CONF directory, where *<AR_System_install>* is the directory where the AR System server is installed. The administrator must set access control rights to prevent modification of this file by any users other than the administrator and the AR System server.

The functionality described above satisfies the functional requirement FMT_SMF.1.1, by providing the interfaces to manage the security management functions of the TOE.

Security functional requirement FMT_SMR.1 (Security Roles)

AR System supports the security roles authorized administrator and authorized subadministrator. Administrators associate the users with these two roles by assigning group membership for the users to the Administrator or the Subadministrator group. Administration control over components such as the Email Engine and the Approval Server is done by setting the appropriate administrator group access information for those product forms.

The functionality described above satisfies the security requirements FMT_SMR.1.1 and FMT_SMR.1.2 by maintaining the roles of authorized administrator and authorized subadministrator, and by the ability to associate users with these roles.

6.1.5 Protection of the TSF (TSF_FPT)

The TOE includes several optional application servers that, if installed, act as part of the TOE to carry out workflow operations. These include the Approval0 Server, the Email Engine, Flashboards Server, Mid Tier, and the AREA LDAP Plug-in.

Explicitly defined functional requirement FPT_APP_EXP.1 (Application server authentication)

If installed, each application server connects to AR System server using the AR System API. This occurs as part of workflow; there is no direct user interface to the application servers. Administrators configure the application servers by modifying the appropriate forms in BMC Remedy User, and by editing appropriate configuration settings in BMC Remedy Administrator or (for Mid Tier) in the Configuration Tool.

The application servers are part of the TOE and are identified internally when they connect to AR System server. At connect time, AR System server checks the password passed from the application server against the appropriate application server password set by the administrator. If the passwords do not match, the application server cannot connect to AR System server and the operation fails. The AR System server uses the Plug-in Server Target password to authenticate itself to the plug-in server in the same way, when external authentication is configured to use the AREA LDAP plug-in.

The functionality described above satisfies the explicit functional requirement FPT_APP_EXP.1.1 by ensuring that the TOE can internally identify and authenticate application servers that are part of the TOE.

6.2 Assurance measures

The TOE satisfies CC EAL3 assurance requirements. This section identifies the Configuration Management, Delivery and Operation, Life Cycle Support, Delivery and Operation, Design Documentation, Guidance Documentation, Test Documentation, and Vulnerability Assessment

Assurance Measures applied by BMC Software, Inc. (BMC) to satisfy the CC EAL3 assurance requirements.

6.2.1 Configuration management (CM)

The CM documentation describes the processes and procedures that are followed, and automated tools that are utilized, in the tracking and monitoring of changes to the CM items and the generation of the TOE. The configuration management measures applied by BMC ensure that configuration items are uniquely identified. BMC ensures that changes to the implementation representation are controlled and that TOE-associated configuration item modifications are properly controlled. BMC performs configuration management on the TOE implementation representation, design, tests, vulnerability analysis, delivery, installation, user and administrator guidance, lifecycle, and the CM documentation. These activities are documented in:

- *Action Request System 6.3 Configuration Management Guide*, version 2.0.

The configuration management measures satisfy the following assurance requirements:

- ACM_CAP.3
- ACM_SCP.1

6.2.2 Life cycle support

BMC ensures the adequacy of the procedures used during the development and maintenance of the TOE. BMC includes security controls on the development environment that are adequate to provide the confidentiality and integrity of the TOE design and implementation that is necessary to ensure the secure operation of the TOE. BMC achieves this through the use of documented procedures. These procedures are documented in:

- *Action Request System 6.3 Configuration Management Guide*, version 2.0.

The process assurance measures satisfy the following assurance requirements:

- ALC_DVS.1

6.2.3 Delivery and operation

BMC provides documentation that explains how the TOE is delivered, the carriers utilized, and the procedures that are followed to maintain security when distributed to the user's site. BMC's installation procedures describe the steps used for the secure installation, generation, and start-up of the TOE along with configuration settings to secure the TOE privileges and functions. These procedures are documented in:

- *Action Request System 6.3 Installing AR System*
- *BMC Remedy Action Request System 6.3 Sales Orders and Delivery Guide*, version 1.

The delivery and operation assurance measure satisfies the following Assurance requirements:

- ADO_DEL.1
- ADO_IGS.1

6.2.4 Design documentation

BMC provides design documentation that identifies and describes the external interfaces and the decomposition of the TOE into subsystems. The design documentation consists of the following documents:

- ADV_FSP.1: *The BMC Remedy Action Request System 6.3 Functional Specification*, Version 2.2, describes all the external interfaces of the TSF. The description includes the purpose and method of use of the interface, applicable parameters, effects, error messages, and exceptions as appropriate.
- ADV_HLD.2: The *BMC Remedy Action Request System 6.3 High Level Design*, Version 2.2, decomposes the TOE into TSP-enforcing and other subsystems. Each subsystem will describe the purpose and method of use of all interfaces to the subsystems of the TSF. The description includes the purpose and method of use of the interface, applicable parameters, effects, error messages, and exceptions as appropriate.
- ADV_RCR.1: The way that this correspondence is evident within the design documentation is:
  - ST-TSS to FSP: The AR System Correspondence Matrix identifies the interfaces that provide the security functions as described in the ST.
  - FSP to HLD: The AR System Correspondence Matrix identifies the interfaces of the subsystems that provide the security functions as described in the FSP.

The Design assurance measure satisfies the following Assurance requirements

- ADV_FSP.1
- ADV_HLD.2
- ADV_RCR.1

6.2.5 Guidance documentation

BMC provides administrator guidance on how to utilize the TOE security functions, the interfaces available to the administrator, and warnings to authorized administrators about actions that can compromise the security of the TOE. The procedures, included in the administrator guidance, describe the steps necessary to operate AR System in accordance with the evaluated configuration, detailing how to establish and maintain the secure configuration, and assumptions about the environment.

The user guidance describes the procedures to use the TOE security-related functions and the interfaces that are available to the non-administrative users.

The administrator and user guidance is documented in:

- *Action Request System 6.3 Concepts Guide*
- *Action Request System 6.3 Configuring AR System*
- *Action Request System 6.3 Optimizing and Troubleshooting AR System*
- *Action Request System 6.3 C API Reference Guide*
- *Action Request System 6.3 Database Reference Guide*
- *Action Request System 6.3 Developing AR System Applications – Basic*
- *Action Request System 6.3 Developing AR System Applications – Advanced*
- *Action Request System 6.3 Remedy Email Engine Guide*
- *Remedy Approval Server 6.3 Guide for Users and Administrators*
- *Action Request System 6.3 Error Messages Guide*
- *Action Request System 6.3 Release Notes*
- *Action Request System 6.3 Remedy Flashboards Administrator's Guide*
- *BMC Remedy Action Request System 6.3 Documentation Addendum*, Version 1.1

The Guidance assurance measure satisfies the following Assurance requirements

- AGD_ADM.1
- AGD_USR.1

6.2.6 Test documentation

BMC provides test documentation that describes how each of the TOE security functions is tested, as well as the actual results of applying the tests. The test documentation consists of the following documents:

- *BMC Remedy Action Request System 6.3 Test Plan and Test Cases*, Version 1.2.

The Tests assurance measure satisfies the following assurance requirements:

- ATE_COV.2: The Test Cases document describes the test cases for each of the security-relevant interfaces of the TOE. The descriptions indicate which tests are used to satisfy the test cases identified for each interface.
- ATE_DPT.1: The Test Cases document includes more detailed test case descriptions that show that the tests are sufficient to demonstrate that the TSF operates in accordance with the high-level design, and that all of the corresponding interfaces are appropriately exercised.
- ATE_FUN.1: The Test Plan describes the security functions to be tested, how to successfully test all of them, the expected results, and the actual test results after exercising all of the tests.
- ATE_IND.2: The TOE and test documentation will be available for independent testing.

6.2.7 Strength of TOE security functions and vulnerability assessment

6.2.7.1 Evaluation of misuse

The Evaluation Team's misuse analysis will demonstrate that the administrative and user guidance completely addresses managing the TOE in a secure configuration.

6.2.7.2 Strength of TOE security functions and Vulnerability Analysis

The claim made in this Security Target is SOF-Basic. The only probabilistic or permutational function on which the strength of authentication mechanisms depends is the set of application server passwords, which control access to AR System server by non-user components of the TOE. The strength of TOE security function analysis demonstrates that the SOF claims made in the ST for all probabilistic or permutation mechanisms are correct.

The strength of TOE security function analysis is provided in the Section 8.5 of this ST.

AR System's vulnerability assessment provides the status of each identified vulnerability and demonstrates that each one cannot be exploited in the intended environment and that AR System is resistant to obvious penetration attacks.

The vulnerability analysis is documented in:

- *BMC Remedy Action Request System Vulnerability Analysis*, Version 1.

The Vulnerability Assessment assurance measure satisfies the following assurance requirements:

- AVA_MSU.1
- AVA_SOF.1
- AVA_VLA.1

7 PROTECTION PROFILE (PP) CLAIMS

The TOE does not claim conformance to a PP.

8 RATIONALE

This section demonstrates the completeness and consistency of this ST by providing justification for the following:

Traceability: The security objectives for the TOE and its environment are explained in terms of threats countered and assumptions met. The SFRs are explained in terms of objectives met by the requirement. The traceability is illustrated through matrices that map the following:

- Security objectives to threats encountered (Table 13)
- Environmental objectives to assumptions met (Tables 14 and 15)
- TOE SFRs to objectives met (Tables 16 and 17)
- IT Environment SFRs to objectives met (Table 18)
- TOE SFRs to TOE Security Functions (Table 19)

Assurance level: A justification is provided for selecting an EAL3 level of assurance for this ST (Section 8.3).

SOF: A rationale is provided for the SOF level chosen for this ST (Section 8.5).

Dependencies A mapping is provided as evidence that all dependencies are met (Tables 20 and 21).

8.1 Security objectives rationale

This section demonstrates that all security objectives for the TOE are traced back to aspects of the identified threats to be countered by the TOE, and that all objectives for the IT and non-IT environments are traced back to assumptions for the IT and non-IT environments.

Table 13: Security objectives rationale for the TOE

Objective	Threat	Rational
O.AUTHORIZATION	T.UNAUTH_ACCESS	O.AUTHORIZATION helps to mitigate the threat T.UNAUTH_ACCESS by requiring the TOE to allow only authorized users and applications access to the TOE.
O.DISCRETIONARY_ ACCESS	T.EXCEED_PRIV	O.DISCRETIONARY_ACCESS helps to mitigate the threat T.EXCEED_PRIV by using DAC as a mechanism to limit access to TOE objects or applications.

Objective	Threat	Rational
O.MANAGE	T.UNAUTH_ACCESS T.EXCEED_PRIV T.MANAGE	O.MANAGE mitigates the threat T.UNAUTH_ACCESS by requiring the TOE to provide the administrative functionality to manage the TOE to prevent unauthorized access. It mitigates the threat T.EXCEED_PRIV by the same provisions. It mitigates the threat T.MANAGE by providing all of the functions and facilities necessary to support authorized administrators and subadministrators responsible for management of TOE security.

Table 14: Security objectives rationale for the non-IT environment

Objective	Assumption	Rational
OE.DB_LOCKED_ DOWN	A.DB_LOCKED_ DOWN	OE.DB_LOCKED_DOWN meets the assumption A.DB_LOCKED_DOWN. This environmental objective ensures that the component database has had all current security patches applied, and that the authorized administrator has configured the database security mechanism(s) to their most restrictive settings that will still permit TOE functionality and interoperability. It also requires the administrator to ensure that any such patch does not interfere with the correct functioning of AR System server's interface to the database.
OE.INSTALL	A.INSTALL	OE.INSTALL meets the assumption A.INSTALL, by requiring that those responsible for the TOE must make sure that the TOE software is delivered, installed, managed, and operated in accordance with documented delivery and installation/setup procedures, and in accordance with the evaluated configuration.
OE.PERSON	A.NO_EVIL_ADM A.MANAGE	The objective OE.PERSON meets the assumptions A.MANAGE and A.NO_EVIL_ADMIN. OE.PERSON ensures that the TOE is operated in a

Objective	Assumption	Rational
		secure manner by personnel who are not careless, negligent, or hostile, which addresses the assumption A.NO_EVIL_ADM. OE.PERSON also ensures that there are authorized administrators of the TOE and they are properly trained and competent, which addresses the A.MANAGE assumption.
OE.PHYSICAL	A.PHYSICAL_ PROTECT	OE.PHYSICAL meets the environmental assumption A.PHYSICAL_PROTECT, by requiring that the TOE be located within facilities providing controlled access, to prevent unauthorized physical access.
OE.PEER_ ASSOCIATION	A.PEER_ ASSOCIATION	OE.PEER_ASSOCIATION meets the environmental assumption A. PEER_ASSOCIATION, by requiring that the other systems that communicate with the TOE are under the same security and management controls as the TOE.

Table 15: Security objectives rationale for the IT environment

Objective	Assumption	Rational
OE.DAC	A.DAC	OE.DAC meets the assumption A.DAC. This objective for the IT environment specifies that the host platform operating system must provide discretionary access control (DAC) to protect the TOE executables and data.
OE.EXTERNAL_ AUTHENTICATION	A.EXTERNAL_ AUTHENTICATION	OE.EXTERNAL_AUTHENTICATION meets the assumption A.EXTERNAL _AUTHENTICATION, by requiring that the IT environment must provide mechanisms for authentication of TOE users, and that those responsible for the TOE must ensure that the external Authentication mechanism functions correctly and accurately.
OE.PLATFORM_SPT	A.PLATFORM_ SUPPORT	OE.PLATFORM_SPT meets the assumption A.PLATFORM_SUPPORT, by requiring that the underlying hardware and software of the TOE operating

Objective	Assumption	Rational
		environment provide reliable functionality.
OE.TIME	A.TIME	The IT environment objective OE.TIME meets the assumption A.TIME, by requiring that the operating environment of the TOE must provide reliable system time.
OE.SECURE_ COMMUNICATION	A.SECURE_ COMMUNICATION A.CONNECT	OE.SECURE_COMMUNICATION meets the assumption A.SECURE_COMMUNICATION by requiring that the TOE operating environment must provide the ability to configure SSL communications. This ability also helps to meet the assumption A.CONNECT, by providing the ability to protect communication between TOE components and third-party components, where SSL can be configured.
OE.SEP	A.CONNECT	The objective OE.SEP helps to meet the assumption A.CONNECT, by requiring that the TOE operating environment shall provide mechanisms to isolate the TOE security functions and ensure that TSF components cannot be tampered with or bypassed.

8.2 Security requirements rationale

8.2.1 Rationale for TOE security requirements

This section provides evidence demonstrating that the security objectives of the TOE are satisfied by the security requirements. The following two tables provide the security requirement to security objective mapping and a rationale to justify the mapping.

Table 16: Security functional requirements rationale for the TOE

SFR	Rationale
FCS_COP.1(1), FCS_CKM.1, and FCS_CKM.4	FCS_COP.1(1), FCS_CKM.1 and FCS_CKM.4 work together to help ensure that only authorized users can access the TOE, by protecting user security attributes from discovery by unauthorized or malicious users. These SFRs trace back to and aid in meeting the following objective: O.AUTHORIZATION.
FCS_COP.1(2)	FCS_COP.1(2) helps ensure that only authorized applications can access the TOE, by protecting the application server passwords and the Configuration Tool password from discovery by unauthorized or malicious users. This SFR traces back to and aids in meeting the following objective: O.AUTHORIZATION
FDP_ACC.1	FDP_ACC.1 ensures that there is an access control policy covering access requests to TOE objects. This SFR traces back to and aids in meeting the following objective: O.DISCRETIONARY_ACCESS.
FDP_ACF.1	FDP_ACF.1 ensures that access control is based on a correlation of user group membership and permissions to TOE objects. This SFR traces back to and aids in meeting the following objectives: O.DISCRETIONARY_ACCESS.
FIA_ATD.1	FIA_ATD.1 requires that the TOE maintain the security attributes user name and group membership. This SFR traces back to the objective O.AUTHORIZATION. It works with the TOE security requirements FIA_UID.2 and FIA_USB.1 to meet the objective O.AUTHORIZATION, by providing the association between user names and group membership.
FIA_UID.2	FIA_UID.2 requires a user be identified before any access to the TOE is allowed. This SFR traces back to the objective O.AUTHORIZATION. It works together with the TOE security requirements FIA_ATD.1 and FIA_USB.1 to meet the objective O.AUTHORIZATION.
FIA_USB.1	FIA_USB.1 requires that the TOE shall associate the security attributes user name and password with subjects acting on behalf of the user. This SFR traces back to the objective O.AUTHORIZATION. It works with the TOE security requirements FIA_ATD.1 and FIA_UID.2 to meet the objective O.AUTHORIZATION, by assuring that the user's access rights can be checked at each access to the TOE.
FMT_MOF.1	FMT_MOF.1 ensures that Authorized Administrator(s) can manage all aspects of the TOE security functions. This SFR traces back to and aids in meeting the following objectives: O.MANAGE.
FMT_MSA.1	FMT_MSA.1 ensures that that Authorized Administrator(s) can manage all security attributes associated with user access, object permissions, and administrator and application access. This SFR traces back to and aids in meeting the following objective: O.MANAGE.

SFR	Rationale
FMT_MSA.3	FMT_MSA.3 ensures that restrictive default values are used for security attributes and that only Authorized Administrator(s) can change the default values. This SFR traces back to and aids in meeting the following objectives: O.MANAGE.
FMT_SMF.1	Ensures that the management functions to be provided for by the TOE are specified. This SFR traces back to, and aids in meeting the following objectives: O. O.MANAGE.
FMT_SMR.1	Ensures that the capabilities of the Authorized Administrator(s) are based on their role (privilege level). This SFR traces back to and aids in meeting the following objectives: O.MANAGE.
FPT_APP_EXP.1	FPT_APP_EXP.1 is an explicitly stated requirement for the TOE. It ensures that only authorized application servers that are part of the TOE can connect to AR System server when executing workflow. This SFR traces back to and aids in meeting the following objective: O.AUTHORIZATION.

Table 17: TOE SFR mappings to objectives

TOE security functional requirement	O.AUTHORIZATION	O.DISCRETIONARY_ACCESS	O.MANAGE
FCS_COP.1	X		
FCS_CKM.1	X		
FCS_CKM.4	X		
FDP_ACC.1		X	
FDP_ACF.1		X	
FIA_ATD.1	X		
FIA_UID.2	X		
FIA_USB.1	X		
FMT_MOF.1			X
FMT_MSA.1			X
FMT_MSA.3			X

TOE security functional requirement	O.AUTHORIZATION	O.DISCRETIONARY_ACCESS	O.MANAGE
FMT_SMF.1			X
FMT_SMR.1			X
FPT_APP_EXP.1	X		

8.2.2 Rationale for explicitly stated requirements for the TOE

This ST contains explicitly stated requirements to address the authentication requirements for internal components of the TOE, collectively described as *application servers*, when accessing the AR System server.

Application servers are subjects that can execute workflow and manipulate controlled objects in the TOE. Application servers are not directly accessed or controlled by human users of the TOE, but rather are automatically activated as part of applications and workflow, as programmed by authorized administrators of the TOE. Therefore the CC Requirements that address user identification and authentication (Class FIA) do not apply.

The Class FPT was chosen for these explicitly stated requirements. FPT is concerned with protection of the TSF. Since application server authentication is a method of TSF self-protection, this class was deemed appropriate for these explicitly stated requirements.

The CC component FPT_SEP.1, TSF domain separation, was considered for this functionality. While the use of an internal authentication mechanism to control access to the AR System server and protection of the TOE data could be considered establishing a protected domain for the TOE, FPT_SEP.1 is concerned with modification of the TSF data itself, rather than general access to the TOE or protection of TOE data. Since no other components of the FPT class address the function of controlling internal application component access to another component of the TOE, explicitly stated requirements were defined.

8.2.3 Rationale for IT environment security requirements

This section provides evidence indicating which security objectives for the IT Environment are satisfied by the security requirements for the IT Environment. The following table provides the security requirement to security objective mapping for the IT environment, and a rationale to justify the mapping.

Table 18: Security functional requirements rationale for the IT environment

SFR	Rationale
FDP_ITT.1	FDP_ITT.1 requires that the IT environment enforce the locally specified SSL communication policy to prevent the disclosure of user data when it is transmitted between physically separated parts of the TOE and required components of the IT Environment. This requirement traces back to and meets the objective OE.SECURE_COMMUNICATION, allowing the administrator to configure SSL to protect TOE user password transmission to and from third party applications where necessary.
FIA_ATD.1	FIA_ATD.1 requires that the IT environment maintain a list of the user security attributes user name and password. This requirement traces back to the objective OE.EXTERNAL_AUTHENTICATION. It works with the environmental requirements FIA_UAU.2 and FIA_UID.2, and with the TOE SFRs FIA_ATD.2 and FIA_UID.2, to meet the objective OE.EXTERNAL_AUTHENTICATION.
FIA_UAU.2	FIA_UID.2 and FIA_UAU.2 require that a user be identified and authenticated before any access to the TOE is allowed. FIA_UAU.2 traces back to the objective OE.EXTERNAL_AUTHENTICATION. It works with the environmental requirements FIA_ATD.1 and FIA_UID.2 to help meet the objective OE.EXTERNAL_AUTHENTICATION.
FIA_UID.2	FIA_UID.2 and FIA_UAU.2 require that a user be identified and authenticated before any access to the TOE is allowed. FIA_UID.2 traces back to the objective OE.EXTERNAL_AUTHENTICATION. It works with the environmental requirements FIA_ATD.1 and FIA_UAU.2 to help meet the objective OE.EXTERNAL_AUTHENTICATION.
FPT_SEP.1	FPT_SEP.1 requires that the IT environment shall maintain a security domain that protects it from interference and tampering by untrusted subjects. This requirement traces back to and meets the security objective OE.SEP, to assure that TSF components, including AR System configuration files, cannot be tampered with or bypassed.
FPT_STM.1	FPT_STM.1 requires that the environment provide correct system time. This SFR traces back to and meets the following objective: OE.TIME. Correct system time is essential for the correct measurement and functioning of timeouts related to external authentication when using the AREA LDAP plug-in.

8.3 Rationale for assurance level

This ST contains the assurance requirements from the CC EAL3 assurance package and is based on good commercial development practices. This ST has been developed for a generalized environment with a medium level of risk to the assets. The security environment in which the TOE operates assumes physical protection. AR System 6.3 provides a level of protection that is appropriate for IT environments that require secure automated change management, such as the distribution of application updates and patches throughout an enterprise. As such, it is believed that EAL3 provides an appropriate level of assurance in the security functions offered by the TOE.

8.4 Rationale for TOE summary specification

This section demonstrates that the TSFs and assurance measures meet the SFRs.

8.4.1 TOE security functional requirements

The specified TSFs work together to satisfy the TOE SFRs. Table 19 provides a mapping of SFRs to the TSFs to show that each SFR is captured within a security function.

Table 19: Mapping of SFRs to security functions

SFR	Name	TSF
FCS_COP.1	Cryptographic operation	TSF_COP
FCS_CKM.1	Cryptographic key generation	TSF_COP
FCS_CKM.4	Cryptographic key destruction	TSF_COP
FDP_ACC.1	Access control policy	TSF_FDP
FDP_ACF.1	Security attribute-based access control	TSF_FDP
FIA_ATD.1	User attribute definition	TSF_FIA
FIA_UID.2	User identification	TSF_FIA
FIA_USB.1	User-subject binding	TSF_FIA
FMT_MOF.1	Management of security functions behavior	TSF_FMT
FMT_MSA.1	Management of security attributes	TSF_FMT
FMT_MSA.3	Static attribute initialization	TSF_FMT
FMT_SMF.1	Specification of management functions	TSF_FMT
FMT_SMR.1	Security roles	TSF_FMT
FPT_APP_EXP.1	Application server authentication	TSF_FPT

8.4.2 TOE assurance requirements

This ST contains the assurance requirements from the CC EAL3 assurance package and is based on good commercial development practices. This ST has been developed for a generalized environment with a medium level of risk to the assets. The security environment in which the TOE operates assumes physical protection. AR System provides a level of protection that is appropriate for IT environments that implement IT applications such as Help Desk and Asset Management. As such, it is believed that EAL3 provides an appropriate level of assurance in the security functions offered by the TOE.

8.5 Rationale for strength of function claim

The rationale for the TOE Strength of Function described in this section satisfies the SOF-Basic claim. SOF-Basic is chosen because the TOE strength of function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential. In addition, SOF-basic is sufficient to meet the objectives of the TOE given the security environment described in this ST.

The SOF-Basic claim is made for the explicitly stated security functional requirements for the TOE under FPT_APP_EXP.1, with regard to the application server passwords and the Configuration Tool password, as described in section 6.1.4. The application server passwords include the Mid Tier Administration Password, the Application Service Password, the Plug-in Server Local and Target Passwords, and the Remote Workflow Local Password. In the evaluated configuration, the administrator is required to change each application server password from the default password, and to assign a new password of at least six characters.

The valid range of values for each password can consist of any alpha-numeric character or any of 32 symbols (described below). Passwords are case-sensitive, and in the evaluated configuration, the minimum password length is six characters. Also, access to AR System server by the application servers and by mid tier-based applications is not done directly through a user interface, but requires an API-based application to be programmed that will use the application server in question. Access to the Configuration Tool is by entering the Configuration Tool Password in the Configuration Tool Password window, which is presented in a browser.

According to the CEM guidance for SOF claims, patterns of human usage must be taken into consideration when estimating password vulnerability. Assuming that in a worst case scenario, the administrator chooses a password comprising only six characters, the average total time to guess the correct password can be estimated by:

52 alpha characters (26 uppercase + 26 lowercase)
10 digits (0 through 9)
+ 32 special characters (`,~,!,@,#,$,%,^,&,*,(,),-,_,=,+,[,],{,},\,|,;,:,’,”,,,., <,>,/,?)
94 possible values

94^6 = (94*94*94*94*94*94) = 689,869,781,056 possible passwords.

An attacker would typically need to execute such workflow (689,869,781,056 / 2) = 344,934,890,528 times, prior to entering the correct password. Assuming that a proficient or expert person could write an AR System application using the AR System API to test passwords at the rate of 1,000 guesses per second, a successful attack would typically require (344,934,890,528 / 3,600,000) = 95,815 hours. This equals (95,815 / 24) = 3,992 days, or (3,992 / 365) = 10.93 years.

According to the Common Evaluation Methodology Section A.8.2.3, Table 3, this attack path would therefore not be exploitable within a time scale that would be useful to an attacker, and therefore the claim of SOF-Basic is satisfied.

8.6 Rationale for SFR and SAR dependencies

Table 20 is a cross-reference of the functional components, their related dependencies, and whether the dependency was satisfied. SFRs for the IT environment are marked with "(ITE)" in the Functional Component ID column. Those not so marked are SFRs for the TOE.

Table 20: SFR dependency status

Functional component ID	Functional component name	Dependencies	Satisfied
FCS_COP.1.1(1)	Cryptographic operation	FCS_CKM.1 FCS_CKM.4 FCS_MSA.2	Yes. Yes. No, see notes following table.
FCS_COP.1.1(2)	Cryptographic operation	FCS_CKM.1 FCS_CKM.4 FCS_MSA.2	No, see notes following table.
FCS_CKM.1	Cryptographic key generation	FCS_COP.1 FCS_CKM.4 FCS_MSA.2	Yes. Yes. No, see notes following table.
FCS_CKM.4	Cryptographic key destruction	FCS_CKM.1 FCS_MSA.2	Yes. No, see notes following table.
FDP_ACC.1	Subset access control	FDP_ACF.1	Yes
FDP_ACF.1	Security attribute-based access control	FDP_ACC.1 FMT_MSA.3	Yes Yes
FDP_ITT.1 (ITE)	Basic internal transfer protection	FDP_ACC.1	No, see notes following table.
FIA_ATD.1	User attribute definition	No dependencies	N/A
FIA_ATD.1 (ITE)	User attribute definition	No dependencies	N/A
FIA_UAU.2 (ITE)	User authentication before any action	FIA_UID.1	Yes, by FIA_UID.2 for the IT environment. FIA_UID.2 is hierarchical to FIA_UID.1.

Functional component ID	Functional component name	Dependencies	Satisfied
FIA_UID.2	User identification before any action	No dependencies	N/A
FIA_UID.2 (ITE)	User identification before any action	No dependencies	N/A
FIA_USB.1	User-subject binding	FIA_ATD.1	Yes
FMT_MOF.1	Management of security functions behavior	FMT_SMR.1 FMT_SMF.1	Yes Yes
FMT_MSA.1	Management of security attributes	FDP_ACC.1 FMT_SMR.1 FMR_SMF.1	Yes Yes Yes
FMT_MSA.3	Static attribute initialization	FMT_MSA.1 FMT_SMR.1	Yes Yes
FMT_SMF.1	Specification of management functions	No dependencies	N/A
FMT_SMR.1	Security roles	FIA_UID.1	Yes, by FIA_UID.2, which is hierarchical to FIA_UID.1.
FPT_SEP.1 (ITE)	Domain separation	No dependencies	N/A
FPT_STM.1 (ITE)	Reliable time stamp	No dependencies	N/A
FPT_APP_EXP.1	Application server authentication	FMT_MSA.1 FMT_SMR.1	Yes Yes

Notes:

- **FMT_MSA.2**—FCS_COP.1.1(1), FCS_CKM.1 and FCS_CKM.4 are present to handle the protection of API calls only, which in turn protects the user security attributes during network transmission. Since external authentication requires that the user name and password must be the same as the password in the external authenticating system (LDAP directory service or operating system), the definition of secure passwords for users is determined by the locally specified access control policy for the environment. This is in accordance with the assumption A.PEER_ASSOCIATION. Therefore, FMT_MSA.2 is not necessary to satisfy FCS_COP.1.1(1), FCS_CKM.1, and FCS_CKM.4.

- **FCS_CKM.1, FCS_CKM.4, and FMT_MSA.2**—FCS_COP.1.1(2) is present to handle the protection of application server passwords only, when they are stored in AR System configuration files. Because the encryption methodology is proprietary and internal to AR System code, no external key generation or destruction method is required. Therefore, FCS_CKM.1 and FCS_CKM.4 are not necessary to satisfy FCS_COP.1.1(2). Also in this case, secure security attributes are ensured by the secure usage assumptions for the environment. The evaluated configuration requires that the administrator impose a minimum password length of six characters for application server passwords. This is in accordance with the environment assumption A.INSTALL. The Strength of Function rationale provides a clear definition of these secure values and why they are considered secure. Also, the relevant configuration files must be protected by setting the appropriate file and directory permissions. This is in accordance with the environment assumptions A.DAC and A.CONNECT. Therefore, FMT_MSA.2 is not necessary to satisfy FCS_COP.1.1(2).

- **FDP_ACC.1 for the IT Environment**—FDP_ITT.2 is present only to require that SSL can be configured in third party applications where required for the evaluated configuration. This is to assure that the IT environment protects the user data while providing authentication in support of the TOE SFRs FDP_ACC.1 and FDP_ACF.1. The environmental objective OE.DAC carries the assumption that the access to the IT Environment is determined by the locally specified access control policy for the environment. Therefore, it is not necessary to place a specific requirement for FDP_ACC.1 on the IT Environment.

As can be seen by Table 20 and the explanatory notes, all required Security Functional Requirement dependencies have been met.

The SAR dependencies identified in the CC have been met by this ST as shown in Table 21:

Table 21: EAL 3 SAR dependencies

Assurance component ID	Assurance component name	Dependencies	Satisfied
ACM_CAP.3	Authorization controls	ALC_DVS.1	Yes
ACM_SCP.1	TOE CM coverage	ACM_CAP.3	Yes
ADO_DEL.1	Delivery procedures	No dependencies	N/A
ADO_IGS.1	Installation, generation, and startup procedures	AGD_ADM.1	Yes
ADV_FSP.1	Informal functional specification	ADV_RCR.1	Yes
ADV_HLD.2	Security enforcing high-level design	ADV_FSP.1	Yes
ADV_RCR.1	Informal correspondence demonstration	No dependencies	N/A
AGD_ADM.1	Administrator guidance	ADV_FSP.1	Yes
AGD_USR.1	User guidance	ADV_FSP.1	Yes
ALC_DVS.1	Identification and security measures	No dependencies	N/A
ATE_COV.2	Evidence of coverage	ADV_FSP.1 ATE_FUN.1	Yes Yes
ATE_DPT.1	Testing: High-level design	ADV_HLD.1 ATE_FUN.1	Yes Yes
ATE_FUN.1	Functional testing	No dependencies	N/A

Assurance component ID	Assurance component name	Dependencies	Satisfied
ATE_IND.2	Independent testing – sample	ADV_FSP.1 AGD_ADM.1 AGD_USR.1 ATE_FUN.1	Yes Yes Yes Yes
AVA_MSU.1	Examination of guidance	ADO_IGS.1 ADV_FSP.1 AGD_ADM.1 AGD_USR.1	Yes Yes Yes Yes
AVA_SOF.1	Strength of TOE security function evaluation	ADV_FSP.1 ADV_HLD.1	Yes Yes
AVA_VLA.1	Developer vulnerability analysis	ADV_FSP.1 ADV_HLD.1 AGD_ADM.1 AGD_USR.1	Yes Yes Yes Yes

8.7 Internal consistency and mutually supportive rationale

The set of security requirements provided in this ST form a mutually supportive and internally consistent whole for the following reasons:

- The choice of security requirements is justified as shown in Sections 8.2 and 8.4. The choice of SFRs and SARs is based on the assumptions about the objectives for, and the threats to, the TOE and the security environment. This ST provides evidence that the security objectives counter threats to the TOE, and that physical, personnel, and procedural assumptions are satisfied by security objectives for the TOE environment.
- The security functions of the TOE satisfy the SFRs as shown in Table 19. All SFR and SAR dependencies have been satisfied or rationalized as shown in Tables 20 and 21, and described in Section 8.6.
- The SFRs and SARs presented in Section 5 and justified in Sections 8.2 and 8.4 are internally consistent. There is no conflict between security functions, as described in Section 2 and Section 6, and the SARs to prevent satisfaction of all SFRs.