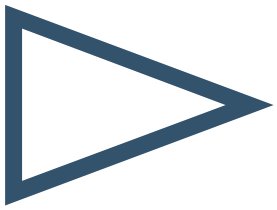


# BMC® Remedy® Action Request System® with Premium Encryption Security v8.1

## Security Target

Version 0.07

24 January 2014

# Document Revision History

| Date | Revision | Author | Changes made |
|---|---|---|---|
| 1/4/13 | 0.01 | Catherine Skrbina | Initial Draft |
| 2/4/13 | 0.02 | Catherine Skrbina | Revised Draft. Class FDP erroneously reflected in Class FIA section. |
| 5/17/13 | 0.03 | Chandra Bridges | Revised Draft. Addressed evaluator comments. |
| 5/22/13 | 0.04 | Chandra Bridges | Revised Draft. Changes to Figure 1 and related information. |
| 6/7/13 | 0.05 | Chandra Bridges | Revised Draft. Addressed evaluator comment. |
| 4/10/13 | 0.06 | Mark Gauvreau | Change to TOE name and version # |
| 24/1/14 | 0.07 | TM | Addressed evaluator comments |

# TABLE OF CONTENTS

# 1 SECURITY TARGET INTRODUCTION

This section presents Security Target (ST) identification information and an overview of the ST for *BMC Remedy Action Request System with Premium Encryption Security v8.1* (hereinafter referred to as *BMC Remedy AR System or 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 (TOE Security Environment section).
- A set of security objectives and a set of security requirements to address the security problem (Security Objectives and IT Security Requirements sections, respectively).

The IT security functions provided by the TOE that meet the set of requirements in the TOE Summary Specification section.

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 Security Target, TOE, and CC identification

| | |
|---|---|
| **ST Title:** | BMC Remedy Action Request System with Premium Encryption Security v8.1 Security Target |
| **ST Version:** | Version 0.07 |
| **ST Date:** | January 24, 2014 |
| **TOE Identification:** | BMC Remedy Action Request System with Premium Encryption Security v8.1 (English version) |
| **TOE Developer** | BMC Software, Inc. |
| **Evaluation Sponsor** | BMC Software, Inc. |
| **CC Identification:** | Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4, September 2012 |

## 1.2 Conformance claims

This ST and the TOE it describes are conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, Version 3.1, Revision 4, September 2012
  - Part 2 Extended
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, Version 3.1, Revision 4, September 2012
  - Part 3 Conformant

This ST and the TOE it describes are conformant to the following package:

- EAL2+ Conformant

## 1.3 Hardware requirements

The hardware requirements for any given environment depend on the size and amount of activity expected. This section describes minimum and recommended requirements, suitable for a small organization. In most cases, BMC recommends that an analysis of the organization's needs be performed to determine the hardware requirements for the installation.

For complete information about hardware that is compatible with AR System, refer to the *Action Request System Compatibility and Support* document in the Product Availability and Compatibility pages of the Customer Support website at http://www.bmc.com/support. BMC Software recommends that customers check the websites of the suppliers of the platforms and supporting components in use at their site to verify that they are still supported. Platforms that are no longer supported by the vendor are not supported by BMC Software. Common Criteria customers should also read the *BMC Remedy AR System Installation* information before installing BMC Remedy AR System.

The minimum and recommended hardware requirements for a server running AR System or BMC Remedy Mid Tier (mid tier) are:

| **Minimum** | **Recommended** |
|---|---|
| 512 MB of available RAM | 1 GB of available RAM |
| 800 MB of available hard disk space | 2 GB of available hard disk space |
| 2.8 GHz processor | 2.8 GHz processor |

Note: If you use a mid tier, BMC Remedy strongly recommends that you install it on a separate server, with the same minimum and recommended requirements as an AR System Server. If, however, you do combine a mid tier and an AR System installation on the same server, see the recommendations below concerning that server's minimum and recommended hardware requirements.

The hardware requirements for a single server running both AR System and the BMC Remedy Mid Tier are:

| **Minimum** | **Recommended** |
|---|---|
| 1 GB of available RAM | 2 GB of available RAM |
| 1.5 GB of available hard disk space | 4 GB of available hard disk space |
| 2.8 GHz processor | 2.8 GHz processor |

The minimum requirements for BMC Remedy Developer Studio are:

- Pentium 4-class
- 1.3 GHz or higher
- 512 MB memory
- 100 MB of free disk space

The basic AR System hardware requirements increase when you install applications that run on top of AR System. The following table displays the minimum and recommended hardware requirements for an AR System Server and one complex application in a production environment, on a Microsoft® Windows®-based server. Note: Each additional complex application requires an additional 2 GB of disk space. Also, 64-bit servers must run against 64-bit databases.

| **Minimum** | **Recommended** |
|---|---|
| 2 GB of available RAM | 4 GB of available RAM |
| 4 GB of available hard disk space | 8 GB of available hard disk space |
| Dual 3 GHz processor | Dual 3 GHz processor |

## 1.4 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.

### 1.4.1 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:

1) 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.
2) 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.**
3) The selection operation is used to select one or more options provided by the CC in stating a requirement. Selections are denoted by *underlined italicized text.*
4) Iterated functional components are given unique identifiers by appending a lower case letter to the component name, short name, and functional element name from the CC, i.e., FMT_MTD.1.1a and FMT_MTD.1.1b

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

5) Plain *italicized text* is used to introduce the names of TOE components and specific concepts.
6) ***Bold italicized text*** is used for emphasis.

### 1.4.2 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), perform an operation. |
| **External IT entity** | Any IT product or system, untrusted or trusted, outside of the TOE that interacts with the TOE. |
| **Form** | A fundamental building block in AR System. It is composed of a collection of fields. A field contains a unit of information such as an employee's first name or location. |
| **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) Scope of Control (TSC) 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 operational environment of the TOE. |
| **Subject** | An entity within the TSC that causes operations to be performed. |
| **TSC** | A set of interactions that can occur with or within a TOE and are subject to the rules of the TSP. |
| **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. |
| **TSP** | A set of rules that regulate how assets are managed, protected, and distributed within a TOE. |
| **User** | Any entity (human user or external IT entity) outside the TOE that interacts with the TOE. |

### 1.4.3 Acronyms

The following acronyms are used in this ST:

| | |
|---|---|
| **API** | Application Programming Interface |
| **ARDBC** | Action Request System Database Connectivity |
| **AREA** | Action Request System External Authentication |
| **AR System** | BMC Remedy Action Request System |
| **CC** | Common Criteria |
| **CEM** | Common Evaluation Methodology |
| **CM** | Configuration Management |
| **CSEC** | Communications Security Establishment Canada |
| **CVE** | Common Vulnerabilities and Exposures |
| **DAC** | Discretionary Access Control |
| **DSO** | Distributed Server Option |
| **EAL** | Evaluation Assurance Level |
| **FDP** | User Data Protection |
| **FIA** | Identification and Authentication |
| **FMT** | Security Management |
| **FPT** | Protection of the TSF |
| **FSP** | Functional Specification |
| **GUI** | Graphical User Interface |
| **HLD** | High-Level Design |
| **ISO** | International Standards Organization |
| **ISO 15408** | Common Criteria 2.3 ISO Standard |
| **IT** | Information Technology |
| **JRE** | Java Runtime Environment |
| **JSP** | Java Server Pages |
| **LDAP** | Lightweight Directory Access Protocol |
| **MOF** | Management of Functions |

| | |
|---|---|
| **MTD** | Management of TSF Data |
| **OS** | Operating System |
| **OSP** | Organization Security Policy |
| **PP** | Protection Profile |
| **SAR** | Security Assurance Requirement |
| **SDK** | Software Development Kit |
| **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 Functionality |
| **TSFI** | TSF Interface |
| **TSP** | TOE Security Policy |
| **UAU** | User Authentication |
| **UDP** | User Data Protection |

## 1.5 TOE overview

AR System provides a consolidated Service Process Management platform for automating and managing Service Management business processes. With its request-centric, workflow-based architecture, AR System is optimized for efficiencies in Service Management business process delivery, and includes pre-built functionality for notifications, escalations, and approvals. AR System is compatible with existing IT infrastructures, and includes various integration capabilities, including support for Web Services. This evaluation did not cover the service process management functions but focused on the IA-enabled capabilities related to the definition and use of that function.

# 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 applications that automate business processes. It also gives customers with or without programming experience the ability to design and customize workflow-based applications to automate business processes. Using AR System, nonprogrammers can build powerful business workflow applications and deploy them simultaneously in web, Windows, UNIX®, and Linux® environments. One of the most common uses of AR System is to automate internal service desks.

The following table identifies the AR System components and versions 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 | *BMC Remedy AR System, AR System Server, AR System server* |
| BMC Remedy Premium Encryption Security | *Premium Security, Encryption Security* |
| BMC Remedy Approval Server | *Approval server* |
| BMC Remedy Email Engine | *Email Engine* |
| BMC Remedy Flashboards Server | *Flashboards server* |
| Server Configuration plug-in | *Server Configuration plug-in* |
| Web Services plug-in | *Web Services plug-in* |
| Action Request System External Authentication LDAP plug-in | *AREA LDAP plug-in* |
| Action Request System Database Connectivity plug-in | *ARDBC plug-in* |
| BMC Remedy Mid Tier | *BMC Remedy Mid Tier, the mid tier* |
| BMC Remedy Developer Studio | *Developer Studio* |
| BMC Remedy Data Import | *BMC Remedy Data Import* |
| BMC Remedy Mid Tier Configuration Tool | *Mid Tier Configuration Tool* |
| BMC Remedy Distributed Server Option | *DSO* |
| BMC Remedy Assignment Engine | *Assignment Engine* |
| BMC Atrium Integrator | *Atrium Integrator* |

### 2.1.1 Physical scope and boundary

The TOE consists of BMC Remedy Action Request System (AR System), with BMC Remedy Premium Encryption Security. The TOE is the base BMC Remedy AR System platform and does not include workflow-based applications that are developed and run on the platform. AR System consists of server and client components. Table 2 lists the components of AR System that are included in the TOE.

The TOE does not include the hardware, database, operating systems, email servers, or directory service protocols with which 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.

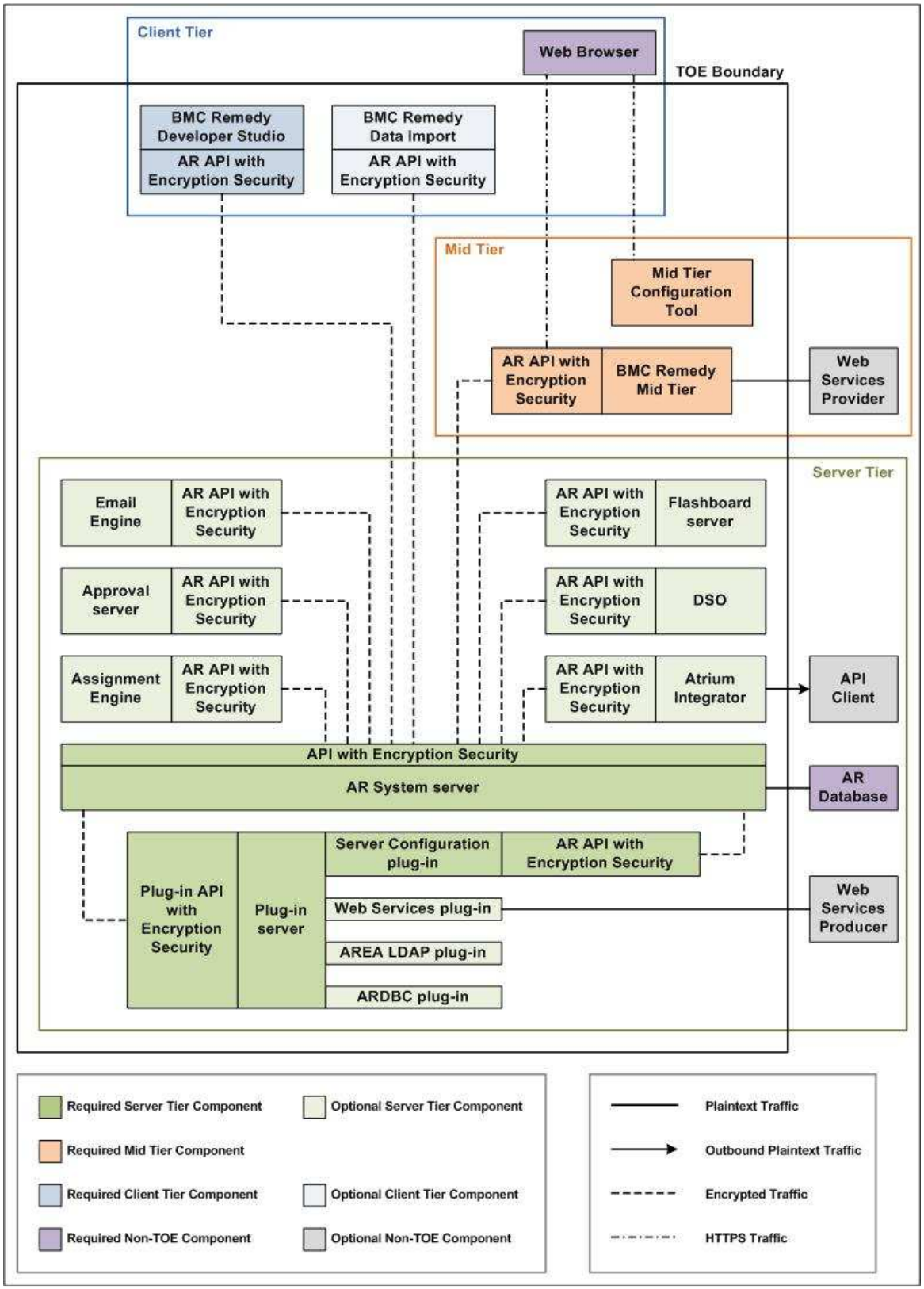
The TOE architecture provides mechanisms for its own self-protection, including:

- Encrypted communications between components of the TOE
- Controlled access to all AR System data and controlled objects by means of security attributes associated with the human user (user name and group membership) and object permissions associated with all AR System controlled objects
- Required identification and authentication of all users, control of session establishment, and association of the user security attributes with the session
- Security roles including authorized administrator and authorized subadministrator
- Limitation of the management of the TSF to the authorized security roles
- Authentication of automated TOE server components (application servers)
- Audit data generation, including user identity association

In addition to its own mechanisms for self protection, the components of the TOE are dependent upon features of their operational environment as summarized in each component description below.

AR System is built on a multi-tiered architecture (Figure 1) that includes the server tier, the mid tier, and the client tier. In addition to a three-tier deployment model, the architecture may include a two-tier deployment model such as a server tier and a mid tier.

## Figure 1. BMC Remedy AR System multi-tiered architecture



#### 2.1.1.1 Server tier

The server tier consists of the AR System Server, along with several *application servers* that provide specialized functionality, including the Approval Server, the Email Engine, the Flashboards server, and the Assignment Engine. These application servers provide commonly used services to AR System applications, such as workflow approvals, automated notifications, and graphics that illustrate system status and history. The Server Configuration plug-in will be installed with the AR System Server, and is used to issue API calls to the AR System Server for configuration. If the Action Request System External Authentication (AREA) LDAP plug-in or the AR System Database Connectivity (ARDBC) plug-in is used, it is also part of the server tier. If the Web Services plug-in is used, it is also a part of the server tier. The Distributed Server Option (DSO) enables administrators to automatically transfer requests between AR System Servers and to keep requests synchronized across multiple AR System Servers.

**BMC Remedy Action Request System Server.** The BMC Remedy Action Request System Server (AR System Server) is a required component that is the core of AR system. The AR System Server is a set of processes that run on the host machine. The server implements workflow and controls workflow logic, controls user access to AR System and the database from AR System client applications, and controls the flow of AR System data into and out of the database. All APIs and server objects that make up AR System, including forms, menus, active links, filters, and escalations, are installed with the AR System Server executable.

The AR System Server can be installed on UNIX, Linux, or Windows platforms. The AR System Server database abstraction layer makes the AR System database-independent, so it can operate with most popular databases, such as Oracle®, MySQL, 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), which includes both C and Java® API libraries. The server and its API libraries implement the majority of the security functionality. In addition, the server processes are protected by operating system access rights to the computer that hosts the AR System Server. The server executables, configuration files, log files, and other associated files are protected by operating system file and directory permissions set by the administrator. The AR System Server is also protected by controlled physical access to the facilities housing the server tier and mid tier components of the TOE.

**Server Configuration plug-in.** The Server Configuration plug-in is a separate instance of the ARDBC plug-in that will be installed with the AR System Server. which will issue API calls to the AR System Server. All communication to the AR System Server will be encrypted using the BMC Remedy Premium Encryption Security.

**BMC Remedy Approval Server.** The Approval Server is an application server component that adds approval functions to existing applications to automate business rules. The Approval Server is a set of pre-defined AR System workflow that can be added to any AR System application. It routes business requests that require approval, such as manager approval of employee expenses, software and hardware change requests, and so on, along a defined path to gather the required approvals or rejections.

The evaluation addressed the limits on the security-related configuration of the Approval Server and its functions, but those functions were not more deeply analyzed.

The Approval Server runs as an AR System plug-in, and communicates with the AR System Server through the plug-in server. The plug-in server is an AR System Server process and is protected by operating system access rights to the computer that hosts the AR System and plug-in server processes. The Approval Server executables, configuration files, log files, and other associated files are protected by operating system file and directory permissions set by the administrator, as well as by controlled physical access to the facilities housing the server tier and mid tier components of the TOE.

**BMC Remedy Email Engine.** The Email Engine is an application server component that provides email access to the 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 email engine does not serve as an email exchange; it is simply an integration conduit between an email exchange server (like Microsoft Exchange™, or UNIX mbox) and AR System. The Email Engine communicates directly with the 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 Java Runtime Environment (JRE) must be installed on the same platform as the Email Engine.

The Email Engine runs as a process. The process is protected by operating system access rights to the computer that hosts the Email Engine. The Email Engine executables, configuration files, log files, and other associated files are protected by operating system file and directory permissions set by the administrator, as well as by controlled physical access to the facilities housing the server tier and client tier components of the TOE. The administrator can configure the Email Engine to use SSL when communicating with the SMTP or MAPI mail server.

***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.***

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

The Flashboards server runs as a process. The process is protected by operating system access rights to the computer that hosts the Flashboards server. The Flashboards server executables, configuration files, log files, and other associated files are protected by operating system file and directory permissions set by the administrator, as well as by controlled physical access to the facilities housing the server tier and mid tier components of the TOE.

**BMC Remedy Distributed Server Option.** The BMC Remedy Distributed Server Option (DSO) server is a separate process that runs on the same host machine as the AR System Server to provide geographically distributed data and data redundancy between AR System Servers. The DSO server is associated with one AR System Server. To the DSO server, the associated AR System Server is the local or source AR System Server. All other AR System Servers, whether they reside on the same host as the DSO server or on a different host, are considered remote AR System Servers. Each DSO server can transfer data from a form on its local AR System Server to a form on a remote AR System Server, or to a form on its local AR System Server.

The DSO server process is protected by operating system access rights to the computer that hosts the DSO server processes. Its executables, configuration files, log files, and other associated files are protected by operating system file and directory permissions set by the administrator, as well as by controlled physical access to the facilities housing the server tier and mid tier components of the TOE.

**BMC Atrium Integrator.** The BMC Atrium Integrator (Atrium Integrator) will be installed with the BMC Remedy Action Request System Server but does not need to be used. This tool is primarily meant for use in integrations, to populate the AR server with information from outside the system.

**BMC Remedy Premium Encryption Security.** BMC Remedy Premium Encryption Security (Encryption Security) is sold and installed separately from AR System. It must be included in evaluated configuration of the TOE. It can be configured to use a FIPS-certified encryption algorithm. It has not been independently FIPS-validated, yet it includes the RSA BSAFE Crypto-J JCE Provider Module, version 4.0 – CMVP certificate number 1048. The FIPS-certified RSA BSAFE module is used for the Java API, which includes the mid-tier component. When installed and configured, encryption of network communications between AR System components is provided. Encryption Security is installed and operates on the server tier, the mid tier, and the client tier. Encryption Security libraries are installed on all computers running any component of the TOE. The library files and log files are protected by operating system access control rights on each computer where the product is installed.

**Action Request System External Authentication (AREA) LDAP plug-in.** The AREA LDAP plug-in is a component that allows the administrator to configure external authentication by using the Lightweight Directory Access Protocol (LDAP). If configured, the AREA LDAP plug-in passes the user name and password to the network directory service or other LDAP authentication service, which authenticates the user and returns the authentication result. The AREA LDAP plug-in passes the authentication result to the AR System Server.

The plug-in server is an AR System Server process and is protected by operating system access rights to the computer that hosts the AR System and plug-in server processes. The AREA LDAP plug-in executables, plug-in configuration files, plug-in log files, and other associated files are protected by operating system file and directory permissions set by the administrator, as well as by controlled physical access to the facilities housing the server tier and mid tier components of the TOE. The administrator can configure the AREA LDAP plug-in to use SSL when communicating with the LDAP directory service.

***To protect the password when the AREA LDAP plug-in is used, the administrator must configure the plug-in to use SSL.***

**Action Request System Database Connectivity (ARDBC) plug-in.** The ARDBC plug-in is a component that allows the administrator to configure interaction with an external (non-AR System) data source from within AR System. (The access control of such external data is the responsibility of that external data source. The evaluated configuration does not include any external data source for the ARDBC plug-in to interact with and therefore this component is unused in the evaluated configuration.) Protection of communications between the ARDBC plug-in and the external data source is determined by the external data source.

**BMC Remedy Assignment Engine.** The Assignment Engine is an application server component that assigns service and help desk requests to individuals automatically. The Assignment Engine runs as a process on the same computer as the AR System Server. A related set of AR System workflow includes processes and rules for auto-routing requests and auto-identification of request type and recipient, for example, assigning a request for printer repair to a member of the hardware support team. Administrators configure forms, processes, and rules for the Assignment Engine by using the Assignment Engine Administration Console (a form).

The evaluation addressed the limits on the security-related configuration of the Assignment Engine and its functions, but those functions were not more deeply analyzed.

The Assignment Engine process is protected by operating system access rights to the computer that hosts the Assignment Engine and AR System Server processes. Its executables, configuration files, log files, and other associated files are protected by operating system file and directory permissions set by the administrator, as well as by controlled physical access to the facilities housing the server tier and mid tier components of the TOE.

**AR Database. (The database is not included in the TOE.)** A relational database is a required component of the environment. The database is accessed by the AR System Server only. It can be installed on any machine 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.

The database is protected by operating system discretionary access control as determined by the administrator. In addition, the assumptions placed on the operational environment assure that the database has had all current, applicable security patches applied, and that the administrator configures inherent database security mechanisms to their most restrictive settings that will still permit TOE functionality and interoperability.

**Web Services Producer (The Web Services Producer is not included in the TOE.)** The Web Services plug-in will consume the web services provided by the Web Services Producer.

**API Client (The API Client is not included in the TOE.)** The API Client is any external application/tool that will query the AR server using the Atrium Integrator.

#### 2.1.1.2 Mid tier

**BMC Remedy Mid Tier.** BMC Remedy Mid Tier (mid tier) can be installed on either UNIX or Windows, which works with a web server to enable access to the AR System through a web browser. The web server and the 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. The mid tier communicates with the AR System Server through the AR System Java API interface.

The Mid Tier is a Java-based application that works together with a web server and a JSP engine in a Java run-time environment. The web server, the components of the Java environment, and well as the Mid Tier executables, configuration files, log files, and other associated files are protected by operating system file and directory permissions set by the administrator. They are also protected by controlled physical access to the facilities housing the server tier and mid tier components of the TOE. The mid tier relies on the associated web server to provide encrypted communication (https) with browsers.

The mid tier provides access to mid tier-related system management functions by way of the BMC Remedy Mid Tier 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 2.0.x or higher, BEA WebLogic, 9.2 or higher, IBM Websphere 6.1 or higher, JBoss 4.0.2 or higher, Oracle Application Server 10G (R2) or higher, Microsoft IIS 6.0 or higher, and Tomcat 7.0) or higher. The mid tier communicates with the web server through a JSP engine. To protect the password when using a browser to access AR System, the administrator must 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 Tomcat 7.0 is used. The mid tier communicates with the JSP engine by means of JSP servlets.
- Java SDK/JRE v1.6.0_31 or higher. (The Java SDK is not included in the TOE.) The Java SDK provides the runtime environment for the JSP servlets that make up the mid tier.

**BMC Remedy Mid Tier Configuration Tool**. The BMC Remedy Mid Tier Configuration tool, which is a .jsp script, is installed as part of the mid tier. It does not access the AR System Server. Rather, it forms a browser based interface to the mid tier configuration file, named configproperties.

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 Mid Tier Configuration tool is installed on the same computer and in the same directory structure as the BMC Remedy Mid Tier. Therefore, it relies on the same discretionary access control settings in the operating system that are used to protect the Mid Tier.

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

**Web Services Provider (The Web Services Provider is not included in the TOE.)** The BMC Remedy Mid Tier will produce web services which will be consumed by external agents (Web Service Provider).

#### 2.1.1.3 Client tier

The AR System client tier includes BMC Remedy Developer Studio, BMC Remedy Data Import, and a Web Browser. All communication between the Client Tier (Web Browser) and the Mid Tier will be performed using https after the web server has been configured properly.

**BMC Remedy Developer Studio**. BMC Remedy Developer Studio is an AR System development tool that runs on top of a Java-based development platform. It is used to develop or customize AR System workflow and applications, including assigning permissions to AR System controlled objects. It provides a graphical interface to the application's forms, fields, and workflow rules. BMC Remedy Developer Studio communicates directly with the AR System Server through the AR System Java API interface.

BMC Remedy Developer Studio is installed on computers used by AR System authorized administrators and authorized subadministrators. Its executables, configuration files, log files, and other associated files are protected by operating system file and directory permissions set on the computer where it is installed.

**BMC Remedy Data Import.** BMC Remedy Data Import is a client tool that enables AR System administrators to transfer data from an external source into a database form. Import runs on top of a Java-based development platform and communicates directly with the AR System Server through the AR System API interface.

BMC Remedy Data Import is installed on computers used by AR System authorized administrators. Its executables, configuration files, log files, and other associated files are protected by operating system file and directory permissions set on the computer where it is installed.

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

Users can access AR System applications and forms to which they have permission with a web browser. Administrators can access all forms, including interfaces such as the User, Group, Roles, and AR System Administration: Server Information (Server Information) forms, with a browser. Web pages are written in JSP and rendered in JavaScript and HTML.

***To secure the user password when using the mid tier, the administrator must configure the web server to only allow https access.***

BMC supports AR System compatibility with multiple operating system platforms, databases, and other third-party applications. To achieve a timely validation, BMC limited the Operational Environment for Common Criteria testing to the platforms and third-party applications described in the tables below. Table 2 describes the AR System components that are included in the evaluated configuration, along with their dependencies and the underlying

environment for each component. Table 3 describes the environment components used and to be tested in the evaluated configuration. For complete information about operating systems, databases, and other applications that are compatible with AR System, see the *BMC Remedy AR System Compatibility Matrix.*

## Table 2. AR System components

| TOE component | Dependency | Version | Underlying environment |
|---|---|---|---|
| BMC Remedy Action Request System Server | A database | 8.1.00 | Microsoft Windows Server 2008 R2<br>Sun Solaris 10<br>Microsoft SQL Server 2008 R2<br>Oracle 11g |
| Server Configuration plug-in | AR System Server | 8.1.00 | Same as AR System Server platform |
| Web Services plug-in | AR System Server | 8.1.00 | Same as AR System Server platform |
| BMC Atrium Integrator | AR System Server | 8.1.00 | Same as AR System Server platform |
| BMC Remedy Premium Encryption | AR System Server | 8.1.00 | Microsoft Windows Server 2008 R2<br>Sun Solaris 10 |
| BMC Remedy Mid Tier and Configuration Tool | AR System Server<br>Web server<br>Servlet Engine<br>Java SDK/JRE<br>Browser | 8.1.00 | Microsoft Windows Server 2008 R2<br>Sun Solaris 10<br>Tomcat 7.0 or higher<br>Java SDK/JRE 1.6.0_31<br>Internet Explorer 9 and 10 and<br>Mozilla Firefox, latest |
| BMC Remedy Developer Studio | AR System Server<br>Java SDK/JRE | 8.1.00 | Windows XP<br>Java SDK/JRE 1.6.0_31 |
| BMC Remedy Data Import | AR System Server<br>Java SDK/JRE | 8.1.00 | Windows XP<br>Java SDK/JRE 1.6.0_31 |
| BMC Remedy Email Engine | AR System Server<br>Java SDK/JRE<br>An email exchange server | 8.1.00 | Same as AR System Server platform<br>Java SDK/JRE 1.6.0_31<br>Microsoft Exchange<br>(Windows Server 2008 R2) |
| BMC Remedy Approval Server | AR System Server | 8.1.00 | Same as AR System Server platform |
| BMC Remedy Flashboards Server | BMC Remedy Mid Tier<br>AR System Server | 8.1.00 | Same as AR System Server platform |
| BMC Remedy Distributed Server Option | AR System Server | 8.1.00 | Same as AR System Server platform |
| AREA LDAP plug-in | AR System Server<br>LDAP directory service | 8.1.00 | Same as AR System Server platform<br>Microsoft Active Directory<br>(Windows Server 2008 R2) |
| ARDBC plug-in | AR System Server | 8.1.00 | Same as AR System Server platform |
| BMC Remedy Assignment Engine | AR System Server | 8.1.00 | Same as AR System Server platform |

## Table 3. Operational environment components

| Environment component | Dependency | Optional Y/N | Version | Underlying environment |
|---|---|---|---|---|
| Operating system | None | N | Microsoft Windows Server 2008 R2<br>Sun Solaris 10 | As appropriate |
| Database | Operating system<br>AR System Server | N | Oracle 11G (R2) or higher<br>Microsoft SQL Server 2008 R2 | As appropriate |
| Web server | Operating system | N | Tomcat 7.0 or higher | As appropriate |
| Servlet Engine | Web Server<br>Java SDK/JRE | N | Tomcat 7.0 or higher<br>Java SDK/JRE 1.6.0_31 | As appropriate |
| Java SDK/JRE | Operating system | N | Java SDK/JRE 1.6.0_31 | As appropriate |
| An email exchange server | Operating system | Y | Microsoft Exchange<br>(Windows Server 2008 R2) | As appropriate |
| LDAP directory service | Operating system | Y | Microsoft Active Directory<br>(Windows Server 2008 R2) | As appropriate |
| Web Browser | BMC Remedy Mid Tier<br>AR System Server | N | Microsoft Internet Explorer 9 and 10<br>Mozilla Firefox, latest | As appropriate |

The BMC Remedy Action Request System TOE does not include the following components. However, these components can be used in the TOE's operational environment and accessed by TOE clients as application objects, when so configured, subject to TOE access control policies.

- BMC Atrium Configuration Management Database
- BMC Atrium Integration Engine
- BMC Remedy Asset Management
- BMC Remedy Change Management
- BMC Remedy Service Desk (includes BMC Remedy Incident Management and BMC Remedy Problem Management)
- BMC Service Level Management
- BMC Service Request Management

### 2.1.2 Logical scope and boundary

The TOE logical boundary consists of the security functionality of the BMC Remedy AR System, including the BMC Remedy AR System components listed in Table 2 and BMC Remedy AR System Encryption described in Table 1.

The TOE provides the following security functions:

- Security Audit Data Generation
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF

#### 2.1.2.1 Security Audit Data Generation

AR System provides the ability to audit all interaction between clients and the AR System Server, and between the AR System Server and the database, including API calls between clients and server, SQL requests from the AR System Server to the database server, user authentication attempts, and several other log types. The administrator can also configure the BMC Remedy Premium Encryption Security to report audit data to a log file. The TOE relies on the operational environment to store and protect the audit data. It also relies on the TOE environment to provide an appropriate time stamp for use in the audit records. The TOE can be configured to store the audit records in a form, in which case, the audit records are reviewed using the BMC Client interfaces; or they can be stored in files on the OS directory. When the audit records are stored in files on the OS, the audit records are reviewed using the log viewer provided with the TOE or with a text editor provided by the TOE environment.

#### 2.1.2.2 Cryptographic Support

AR System provides encryption technology for encryption of API communications with the AR System Server. Standard level encryption is installed with the AR System Server, but ***for the evaluated configuration, the administrator must install BMC Remedy Premium Encryption Security***. This product provides enhanced encryption using an administrator-configurable selection of FIPS-certified or non-FIPS-certified algorithms. In the evaluated configuration, only the FIPS-certified selection is configured.

The Encryption Security includes the RSA BSAFE Crypto-J JCE Provider Module, version 4.0 – Certificate number 1048. When configured, Encryption Security causes all clients, the mid tier, and the server tier components 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. Communication and data between the separate parts of the TOE are also secured from unauthorized disclosure or modification using encryption between the client and the mid tier, between the client and the server, and between the mid tier and the server.

Note: The evaluated configuration relies on the 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. 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 administrator is required to configure SSL for these two elements of the evaluated configuration.

#### 2.1.2.3 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. The AR System Server enforces access control at each level of access.

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.

#### 2.1.2.4 Identification and Authentication

AR System identifies users by the user name, which is stored in AR System. By default, users who access BMC Remedy based solutions through the AR System browser interface 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.

AR System prompts the user for a user name and password.

- If AR System is not configured to use external authentication, the AR System Server searches for the user name in the User form. If a match is found, the AR System Server compares the password entered by the user with that stored in the User form. If the user name and password both match, the user is authenticated.
- If AR System is configured for external authentication, the user name and password entered are passed to the operating system (Windows or UNIX) or to an LDAP server in the operational environment. 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 the AR System Administration: Server Information form, accessed through the AR System browser interface.

***In the evaluated configuration, the administrator must configure 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. The administrator must configure AR System to prevent access by guest users.

#### 2.1.2.5 Security Management

The TOE provides administrators with interfaces to manage security policy and its implementation in the AR System Administration Console, BMC Remedy Developer Studio, and the BMC Remedy Mid Tier 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, BMC Remedy based applications, and other external clients.

All user access definition and management is performed through forms that are accessible to Authorized administrators through the AR System browser. 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 (except those assigned to the Public group), and Authorized administrators or Authorized subadministrators add

permissions as needed. Authorized administrators can set default permissions and specific permissions on objects in AR System, and Authorized subadministrators can set specific permissions to objects where assigned.

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 the groups Administrator and Subadministrator. Members of the Administrator group have the security role Authorized administrator. Members of the Subadministrator group have the security role Authorized subadministrator.

Configuration of application servers, including application server passwords, is controlled by Authorized administrators using the AR System Administration: Server Information form and other forms accessible to the administrator through the AR System browser interface. Many settings managed in the AR System Administration: Server Information form are stored in the server configuration file (ar.cfg on Windows or ar.conf on UNIX). The administrator must protect this and other configuration files from tampering by setting the appropriate directory permissions and file settings. In addition to the file protections assumed to be provided by the operational environment, application service passwords stored in configuration files are obfuscated using DES.

#### 2.1.2.6 Protection of the TSF

The evaluated configuration includes application servers that automate commonly used workflow functions. These include the Approval Server, the Email Engine, the mid tier, the Flashboards server, DSO, and the Assignment Engine. The evaluated configuration also includes the AREA LDAP plug-in.

These application servers communicate directly with the AR System Server, and their access to the AR System Server is controlled by the application server passwords. There is an internal password, which is preset and not published, and in addition the administrator must set the appropriate application server passwords at installation time. If an application server attempts to connect to the AR System Server but does not pass the correct password, the connection fails.

These passwords can be changed by the Authorized administrator for additional security, by using the AR System Administration: Server Information form. The application server passwords include the *Application Service Password*, used by the Approval Server, the Email Engine, the Flashboards server, and the Assignment Engine; the *Mid-Tier Administration Password*, used by the mid tier, the *plug-in Server Local and Target Passwords*, used by the plug-in service and the AR System Server during AREA LDAP authentication, and the DSO Local Password. In addition, there is a Remote Workflow Local Password that controls access by workflow originating in other AR System Servers. ***For the evaluated configuration, it is recommended that the selected application server passwords must be at least six characters long.***

### 2.1.3 Functionalities excluded from the evaluated TOE

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.

Additional functionality is provided by the following applications and they may be used in the operational environment of the TOE and accessed by the TOE clients as application objects, when so configured, subject to TOE access control policies. However, as applications that run on the AR System platform they are not part of the TOE and are not included in the evaluated configuration.

- BMC Atrium Configuration Management Database
- BMC Atrium Integration Engine
- BMC Remedy Asset Management
- BMC Remedy Change Management
- BMC Remedy Service Desk (includes BMC Remedy Incident Management and BMC Remedy Problem Management)
- BMC Service Level Management
- BMC Service Request Management
- BMC Migrator

# 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 operational environment with a basic level of risk to identified assets. The assurance requirements of EAL2+ 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.

## 3.2 Environmental assumptions

The environmental assumptions identified in Table 4 are required to ensure the security of the TOE:

### Table 4. 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.OPERATIONAL_ENVIRONMENT_ LOCKED_DOWN | All supporting operational environment components (such as the operating system, database, web browser, web server, email server, and LDAP server) have had all current security patches (if applicable) applied, and the Authorized Administrator has configured the inherent component security mechanisms to their most restrictive settings that will still permit TOE functionality and interoperability. Any such patch must not interfere with the correct functioning of AR System Server's interfaces to the supporting operational environment components. | Connectivity |
| A.EXTERNAL_ AUTHENTICATION | The TOE environment may provide authentication mechanisms, as described in Table 11 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 |

| Assumption | Description | Aspect |
|---|---|---|
| A.PLATFORM_SUPPORT | The underlying platform(s) upon which the TOE executes and all other components in the operational environment including the operating system, database, email server and LDAP server will provide reliable functionality including correct hardware operation and functionality, and correct platform software operation. | Physical |
| A.TIME | The operational environment will provide reliable system time. | Connectivity |
| A.SECURE_ COMMUNICATION | The TOE operational environment will provide the ability to configure SSL communications where appropriate. | Connectivity |

## 3.3 Threats

Table 5 lists threats to the resources to be protected by the TOE. The threat agents 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 the Security Objectives section.

### Table 5. Threats

| Threat | Description |
|---|---|
| T.ACCOUNT | A user might be able to repudiate their use of privileged functions protected by the TSF. |
| T.UNAUTH_ACCESS | An unauthorized user or subject might gain access to user data protected by the TOE or TSF 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 6.

### Table 6. Security objectives for the TOE

| Security Objective | Description |
|---|---|
| O.ACCOUNTABLE | The TSF must ensure that requests to invoke controlled interfaces are audited so that those users can be held accountable for their actions. |
| 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. |
| O.ENCRYPT | The TOE must protect the confidentiality of its API communications through encryption. |

## 4.2 Security objectives for the environment

This section identifies and describes the security objectives for the environment, as shown in Table 7.

### Table 7. Security objectives for the environment

| Objective | Description |
|---|---|
| OE.OPERATIONAL_ ENVIRONMENT_LOCKED_DOWN | Those responsible for the TOE must ensure that the all associated supporting components in the operational environment (such as the operating system, database, web browser, web server, email server, and LDAP server) have had all current patches applied, and are configured in the most restrictive way that will still allow TOE access to all supporting operational environment components. They must also assure that any future security patches do not interfere with the correct functioning of AR System Server's interface to the supporting operational environment components. |
| 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. |

| Objective | Description |
|---|---|
| OE.PHYSICAL | Those responsible for the TOE must ensure that the host computer system(s) containing the AR System Server and database 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 operational environment must ensure that it provides reliable platform functions, including correct hardware operation and functionality, and correct platform software operation and functionality. |
| OE.EXTERNAL_AUTHENTICATION | The TOE operational environment may 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 operational environment must provide correct system time. |
| OE.SECURE_COMMUNICATION | The TOE operational environment must provide SSL communications. |
| OE.AUDIT_PROTECTION | The TOE operational environment must protect audit information. |

# 5 IT SECURITY REQUIREMENTS

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

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 operational environment meet its security objectives (e.g., configuration management, testing, and vulnerability assessment).

These requirements are discussed separately in the following subsections

## 5.1 Extended requirements definition

This ST contains an extended requirement component to address the authentication requirements for internal components of the TOE, collectively described as *application servers*. 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 this extended requirement. 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 this extended requirement. Existing families in the FPT class did not provide coverage of authentication for internal TOE components and as such the APP family was defined and is used for this purpose.

## 5.2 Application server authentication (FPT_APP_EXP)

Family Behavior: This family defines a requirement for ensuring that separate parts of the TOE are identified and authenticated before allowing TOE data to flow to those separate parts of the TOE. This family includes only one component FPT_APP_EXP.1.

Management Activity: The following actions should be considered for FMT – management of the application service password.

Audit Activity: The following actions should be auditable (FAU) – failure to authenticate an application server.

| **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 Functional Requirements

The TOE satisfies the SFRs delineated in Table 8,

### Table 8. TOE security functional requirements

| Functional component ID | Functional component name |
|---|---|
| Class FAU: Security audit | |
| FAU_GEN.1 | Audit data generation |
| FAU_GEN.2 | User identity association |
| FAU_SAR.1 | Audit review |
| Class FCS: Cryptographic support | |
| FCS_CKM.1 | Cryptographic key generation |
| FCS_CKM.4 | Cryptographic key destruction |
| FCS_COP.1 | Cryptographic operation |
| Class FDP: User data protection | |
| FDP_ACC.1 | Subset access control |
| FDP_ACF.1 | Security attribute based access control |
| Class FIA: Identification and authentication | |
| FIA_ATD.1 | User attribute definition |
| FIA_SOS.1 | Verification of secrets |
| FIA_UAU.2 | User authentication before any action |
| FIA_UAU.5 | Multiple authentication mechanisms |
| FIA_UID.2 | User identification before any action |
| FIA_USB.1 | User-subject binding |
| Class FMT: Security management | |
| FMT_MOF.1 | Management of security functions behavior |
| FMT_MSA.1 | Management of security attributes |
| FMT_MSA.2 | Secure security attributes |
| FMT_MSA.3 | Static attribute initialization |
| FMT_MTD.1 | Management of TSF data |
| FMT_SMF.1 | Specification of management functions |
| FMT_SMR.1 | Security roles |
| Class FPT: Protection of the TSF | |
| FPT_APP_EXP.1 | Application server authentication |
| FPT_ITT.1 | Basic internal TSF data transfer protection |
| Class FTA: TOE Access | |
| FTA_TSE.1 | TOE session establishment |

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

### 5.3.1 Class FAU: Security audit

| FAU_GEN.1 | Audit data generation |
|---|---|
| Hierarchical to: | No other components |
| FAU_GEN.1.1 | The TSF shall be able to generate an audit record of the following auditable events:<br>Start-up and shutdown of the audit functions;<br>All auditable events for the *not specified* level of audit; and<br>[the following events:<br>FCS_COP.1 — Failure of cryptographic operation, the type of cryptographic operation, and success and failure of self test operation<br>FCS_CKM.1 — Failure of the key generation activity<br>FCS_CKM.4 — Failure of the key destruction activity<br>FDP_ACF.1 — Successful requests to perform an operation on an object covered by the SFP<br>FIA_UID.2 – Unsuccessful use of the login mechanism, including the user name provided.<br>FMT_SMF.1 — Use of the management functions<br>FMT_SMR.1 — Modifications of the group of users that are part of a role.<br>FPT_APP_EXP.1 – Unsuccessful use of the authentication mechanism<br>FIA_UAU.2 – Any unsuccessful use of the authentication mechanism]. |
| FAU_GEN.1.2 | The TSF shall record within each audit record at least the following information:<br>Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and<br>For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [no other audit relevant information**].** |
| Dependencies: | FPT_STM.1 Reliable time stamps |

Application Note: While the TOE provides the functions to generate security audit events and also functions to display or review those generated events, the TOE depends upon its host operational environment to store and protect that data from inappropriate access.

| FAU_GEN.2 | User identity association |
|---|---|
| Hierarchical to: | No other components |
| FAU_GEN.2.1 | For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event. |
| Dependencies: | FAU_GEN.1<br>FIA_UID.1 |

| FAU_SAR.1 | Audit review |
|---|---|
| Hierarchical to: | No other components |
| FAU_SAR.1.1 | The TSF shall provide [authorized users] with the capability to read [all information] from the audit records in the audit trail. |
| FAU_SAR.1.2 | The TSF shall provide the audit records in a manner suitable for the user to interpret the information. |
| Dependencies: | FAU_GEN.1 |

## 5.3.2 Class FCS: Cryptographic support

| FCS_CKM.1 | Cryptographic key generation |
|---|---|
| Hierarchical to: | No other components |
| 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 [1024 or 2048] that meet the following: [ANSI X9.31]. |
| Dependencies: | FCS_COP.1 Cryptographic operation<br>FCS_CKM.4 Cryptographic key destruction |

| FCS_CKM.4 | Cryptographic key destruction |
|---|---|
| Hierarchical to: | No other components |
| FCS_CKM.4.1 | The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [zeroization] that meets the following: [ FIPS 140-2] |
| Dependencies: | FCS_CKM.1 Cryptographic key generation |

| FCS_COP.1 | Cryptographic operation |
|---|---|
| Hierarchical to: | No other components |
| FCS_COP.1.1 | The TSF shall perform [FIPS mode encryption and decryption of API communications] in accordance with a specified cryptographic algorithm [AES CBC ] and cryptographic key sizes [128 bit or 256 bit] that meet the following [FIPS-197]. |
| Dependencies: | FCS_CKM.1 Cryptographic key generation<br>FCS_CKM.4 Cryptographic key destruction |

## 5.3.3 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<br><br>[Subjects: Sessions representing the user;<br><br>Objects: AR System controlled objects (applications, forms, fields, data records (requests), active links, active link guides, web services, packing lists, flashboards, and flashboards variables);<br><br>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:<br><br>[Subjects: User name, group membership, and licenses; |

| FDP_ACF.1 | Security attribute based access control |
|---|---|
| | Objects: Permission list and unique object identifier.] |
| FDP_ACF.1.2 | The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:<br>1. [Access is granted if any one of the following is true: 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, or any group that is included in a computed group that is contained in the object's permission list. In this case, the user can perform operations according to the following rules: |

| Permission type | Object type(s) | Operation(s) |
|---|---|---|
| Visible | application or active link | read and execute |
| Visible | form | read |
| Hidden | application or active link guides | execute |
| Hidden | form | create or delete operations, as controlled by the related application or workflow |
| View | field | read |
| Change | field | read and modify |
| Permission granted | active link | read and execute |
| Permission granted | flashboards or flashboards variable | read operations as allowed by form and field permissions associated with the flashboard |
| Hidden or Visible | web service | read |
| Subadministrator | applications, forms, packing lists | read, modify and delete |

2. 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:
    a) 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.
    b) 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.
    c) 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.
    d) 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.1.3 | The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [<br>1. Members of the Administrator group have full access and can perform all operations on all AR System controlled objects except as restricted by FDP_ACF.1.4.<br>2. Members of the Subadministrator group have full administrator access to a subset of existing objects only: those they create and those an Authorized Administrator has delegated to the subadministrator. They can perform all operations, but only on the designated subset of AR System controlled objects.] |
| FDP_ACF.1.4 | The TSF shall explicitly deny access of subjects to objects based on the following additional rules [a user must hold an appropriate license (i.e. read license, write license, fixed write license) to perform a corresponding operation on a protected object]. |
| Dependencies | FDP_ACC.1 Subset access control |

| FDP_ACF.1 | Security attribute based access control |
|---|---|
| | FMT_MSA.3 Static attribute initialization |

### 5.3.4 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, password, and group membership]. |
| Dependencies: | No dependencies |

| FIA_SOS.1 | Verification of secrets |
|---|---|
| Hierarchical to: | No other components |
| FIA_SOS.1.1 | The TSF shall provide a mechanism to verify that secrets meet [an administrator-defined password policy based on the following characteristics:<br>Blank passwords are not allowed,<br>Passwords cannot match the login name,<br>The user cannot use the old password when changing the password,<br>Must be a minimum number of 8 characters,<br>Must include at least one uppercase alphabetic character,<br>Must include at least one lowercase alphabetic character,<br>Must include at least one non-alphanumeric (special) character,<br>Password shall have a maximum lifetime, configurable by the authorized administrator. |
| Dependencies: | No dependencies |

Application Note: FIA_SOS.1 is enforced by the TSF on passwords attributes maintained by the TOE in the User Form. It is assumed that the operational environment enforces its own password restrictions on user passwords.

| FIA_UAU.2 | User authentication before any action |
|---|---|
| Hierarchical to: | FIA_UAU.1 |
| FIA_UID.2.1 | The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user. |
| Dependencies: | FIA_UID.1 User identification before any action |

| FIA_UAU.5 | Multiple authentication mechanisms |
|---|---|
| Hierarchical to: | None |
| FIA_UAU.5.1 | The TSF shall provide [local authentication using username/password stored locally, and external authentication via the Operating System or an external LDAP service] to support user authentication. |
| FIA_UID.5.2 | The TSF shall authenticate any user's claimed identity according to the [configured authentication method – ARS, OS, AREA:<br>If the TOE is configured for local authentication (ARS), then the TSF will authenticate the user based on the username and password stored in the User Form.<br><br>If the TOE is configured for external authentication via the operating system (OS), then the TSF will cooperate with the underlying OS to authenticate the users based on username and password stored and controlled by the AR System Server component underlying OS. |

| | |
|---|---|
| | If the TOE is configured for external authentication through an AREA LDAP service (AREA), then the TSF will cooperate with the external remote AREA LDAP service to have the user authenticated using username and password attributes stored and controlled by the external LDAP service. When authentication chaining is enabled, the first mechanism that has a matching user account will be used. |
| 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 group membership]. |
| 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 |

### 5.3.5 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 [<br>Identification and Authentication mechanism, including configuring external authentication<br>Access limits for anonymous users<br>Management of AR System Server information settings<br>Security audit]<br>to [the Authorized Administrator(s)]. |
| Dependencies: | FMT_SMF.1 Specification of management functions<br>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 [<br>Access control attributes associated with users, including user name, groups, and group membership<br>The permission list of AR System controlled objects<br>Mapping of groups to AR System roles |

| | |
|---|---|
| | to [the Authorized administrator(s), or to Authorized subadministrators]. |
| Dependencies: | FDP_ACC.1 Subset access control<br>FMT_SMR.1 Security roles<br>FMT_SMF.1 Specification of management functions |

| **FMT_MSA.2** | **Secure security attributes** |
|---|---|
| Hierarchical to: | No other components |
| FMT_MSA.2.1 | The TSF shall ensure that only secure values are accepted for [user authentication data]. |
| Dependencies: | FDP_ACC.1 Subset access control<br>FMT_MSA.1 Management of security attributes<br>FMT_SMR.1 Security roles |

| **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 administrator(s)] 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<br>FMT_SMR.1 Security roles |

| **FMT_MTD.1** | **Management of TSF data** |
|---|---|
| Hierarchical to: | No other components |
| FMT_MTD.1.1a | The TSF shall restrict the ability to change_default, modify the [user password of other users and the application server passwords] to [Authorized administrators] |
| FMT_MTD.1.1b | The TSF shall restrict the ability to *modify* the [minimum length, complexity requirements and validity period of user passwords] to [Authorized administrators] |
| FMT_MTD.1.1c | The TSF shall restrict the ability to *modify* the [encryption security policy, the data key algorithm, the data key expire interval, the public key algorithm, and the public key expire interval] to [Authorized administrators] |
| FMT_MTD.1.1d | The TSF shall restrict the ability to *modify* [a user own password] to [the non-administrative user that owns the password]. |
| Dependencies: | FMT_SMR.1 Security roles<br>FMT_SMF.1 Specification of Management Functions |

Application Note: The restrictions of FMT_MTD.1.1b apply only to user passwords maintained by the TOE.

| **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: [<br>Manage the GRP_ACC_CTRL SFP, including:<br>Individual human user security attributes<br>AR System groups and AR System roles<br>AR System controlled object permission lists<br>Manage the identification and authentication mechanism<br>Limit access by anonymous users |

| | |
|---|---|
| | Manage AR System Server Information settings<br>Manage the application server passwords<br>Manage encryption settings<br>Manage the minimum length and complexity requirements of user passwords<br>Manage the maximum validity period of user passwords<br>Manage the audit mechanism]. |
| Dependencies: | No Dependencies |

| **FMT_SMR.1** | **Security roles** |
|---|---|
| Hierarchical to: | No other components |
| FMT_SMR.1.1 | The TSF shall maintain the roles [<br>Authorized administrators;<br>Authorized subadministrators;<br>Authorized non-administrators.] |
| FMT_SMR.1.2 | The TSF shall be able to associate users with roles. |
| Dependencies | FIA_UID.1 Timing of identification |

### 5.3.6 Class FPT: Protection of the TSF

| **FPT_ITT.1** | **Basic internal TSF data transfer protection** |
|---|---|
| Hierarchical to: | No other components |
| FPT_ITT.1.1 | The TSF shall protect TSF data from *disclosure, modification* when it is transmitted between separate parts of the TOE. |
| Dependencies | No dependencies |

| **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 | None |

Application Note: Application servers subject to these extended SFRs are not considered external (machine) users subjects to FIA_UAU.2. They are TOE components that must be mutually authenticated in order to exchange information with the AR System Server.

### 5.3.7 Class FTA: TOE access

| **FTA_TSE.1** | **TOE session establishment** |
|---|---|
| Hierarchical to: | No other components |
| FTA_TSE.1.1 | The TSF shall be able to deny session establishment based on [a user password which has not been changed for a period of time that exceeds an authorized administrator configured validity period]. |
| Dependencies | No dependencies |

## 5.4 TOE Security Assurance Requirements

The TOE satisfies the SARs delineated in Table 9,

### Table 9. TOE security assurance requirements

| Assurance component ID | Assurance component name |
|---|---|
| Class ADV: Development | |
| ADV_ARC.1 | Security architecture description |
| ADV_FSP.2 | Complete functional specification |
| ADV_TDS.1 | Basic modular design |
| Class AGD: Guidance documents | |
| AGD_OPE.1 | Operational user guidance |
| AGD_PRE.1 | Preparative procedures |
| Class ALC: Life-cycle support | |
| ALC_CMC.2 | Production support, acceptance procedures and automation |
| ALC_CMS.2 | Problem tracking CM coverage |
| ALC_DEL.1 | Delivery procedures |
| ALC_FLR.2 | Flaw remediation |
| Class ATE: Tests | |
| ATE_COV.1 | Analysis of coverage |
| ATE_FUN.1 | Functional testing |
| ATE_IND.2 | Independent testing – sample |
| Class AVA: Vulnerability assessment | |
| AVA_VAN.2 | Focused vulnerability analysis |

### 5.4.1 Class ADV: Development

| ADV_ARC.1 | Security architecture description |
|---|---|
| ADV_ARC.1.1D | The developer shall design and implement the TOE so that the security features of the TSF cannot be bypassed. |
| ADV_ARC.1.2D | The developer shall design and implement the TSF so that it is able to protect itself from tampering by untrusted active entities. |
| ADV_ARC.1.3D | The developer shall provide a security architecture description of the TSF. |
| ADV_ARC.1.1C | The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document. |
| ADV_ARC.1.2C | The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs. |
| ADV_ARC.1.3C | The security architecture description shall describe how the TSF initialization process is secure. |
| ADV_ARC.1.4C | The security architecture description shall demonstrate that the TSF protects itself from tampering. |
| ADV_ARC.1.5C | The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality. |
| ADV_ARC.1.1E | The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. |
| Dependencies | ADV_FSP.1<br>ADV_TDS.1 |

| ADV_FSP.2 | Complete functional specification |
|---|---|
| ADV_FSP.2.1D | The developer shall provide a functional specification. |
| ADV_FSP.2.2D | The developer shall provide a tracing from the functional specification to the SFRs. |
| ADV_FSP.2.1C | The functional specification shall completely represent the TSF. |
| ADV_FSP.2.2C | The functional specification shall describe the purpose and method of use for all TSFI. |
| ADV_FSP.2.3C | The functional specification shall identify and describe all parameters associated with each TSFI. |
| ADV_FSP.2.4C | For each SFR-enforcing TSFI, the functional specification shall describe the SFR-enforcing actions associated with the TSFI. |
| ADV_FSP.2.5C | For each SFR-enforcing TSFI, the functional specification shall describe direct error messages resulting from processing associated with the SFR-enforcing actions. |
| ADV_FSP.2.6C | The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification. |
| Dependencies | ADV_TDS.1 |

| ADV_TDS.1 | Basic modular design |
|---|---|
| ADV_TDS.1.1D | The developer shall provide the design of the TOE. |
| ADV_TDS.1.2D | The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design. |
| ADV_TDS.1.1C | The design shall describe the structure of the TOE in terms of subsystems. |
| ADV_TDS.1.2C | The design shall identify all subsystems of the TSF. |
| ADV_TDS.1.3C | The design shall describe the behavior of each SFR-supporting or SFR non-interfering TSF subsystem in sufficient detail to determine that it is not SFR-enforcing. |
| ADV_TDS.1.4C | The design shall summarize the SFR-enforcing behavior of the SFR-enforcing subsystems. |

| | |
|---|---|
| ADV_TDS.1.5C | The design shall provide a description of the interactions among SFR-enforcing subsystems of the TSF, and between the SFR-enforcing subsystems of the TSF and other subsystems of the TSF. |
| ADV_TDS.1.6C | The mapping shall demonstrate that all TSFIs trace to the behavior described in the TOE design that they invoke. |
| Dependencies | ADV_FSP.2 |

### 5.4.2 Class AGD: Guidance documents

| **AGD_OPE.1** | **Operational user guidance** |
|---|---|
| AGD_OPE.1.1D | The developer shall provide operational user guidance. |
| AGD_OPE.1.1C | The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings. |
| AGD_OPE.1.2C | The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner. |
| AGD_OPE.1.3C | The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate. |
| AGD_OPE.1.4C | The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF. |
| AGD_OPE.1.5C | The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation. |
| AGD_OPE.1.6C | The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfill the security objectives for the operational environment as described in the ST. |
| AGD_OPE.1.7C | The operational user guidance shall be clear and reasonable. |
| AGD_OPE.1.1E | The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. |
| Dependencies | ADV_FSP.1 |

| **AGD_PRE.1** | **Preparative procedures** |
|---|---|
| AGD_PRE.1.1D | The developer shall provide the TOE including its preparative procedures |
| AGD_PRE.1.2C | The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures |
| AGD_PRE.1.2C | The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST |
| AGD_PRE.1.1E | The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence |
| AGD_PRE.1.2E | The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation |
| Dependencies | No dependencies. |

### 5.4.3 Class ALC: Life-cycle support

| **ALC_CMC.2** | **Production support, acceptance procedures and automation** |
|---|---|
| ALC_CMC.2.1D | The developer shall provide the TOE and a reference for the TOE. |
| ALC_CMC.2.2D | The developer shall provide the CM documentation. |
| ALC_CMC.2.3D | The developer shall use a CM system. |
| ALC_CMC.2.1C | The TOE shall be labeled with its unique reference. |
| ALC_CMC.2.2C | The CM documentation shall describe the method used to uniquely identify the configuration items. |
| ALC_CMC.2.3C | The CM system shall uniquely identify all configuration items. |
| ALC_CMC.2.1E | The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. |
| Dependencies | ALC_CMS.1 |

| **ALC_CMS.2** | **Problem tracking CM coverage** |
|---|---|
| ALC_CMS.2.1D | The developer shall provide a configuration list for the TOE. |
| ALC_CMS.2.1C | The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; the parts that comprise the TOE; the implementation representation; and security flaw reports and resolution status. |
| ALC_CMS.2.2C | The configuration list shall uniquely identify the configuration items. |
| ALC_CMS.2.3C | For each TSF relevant configuration item, the configuration list shall indicate the developer of the item. |
| ALC_CMS.2.1E | The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. |
| Dependencies | No dependencies |

| **ALC_DEL.1** | **Delivery procedures** |
|---|---|
| ALC_DEL.1.1D | The developer shall document procedures for delivery of the TOE or parts of it to the consumer. |
| ALC_DEL.1.2D | The developer shall use the delivery procedures. |
| ALC_DEL.1.1C | The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer. |
| ALC_DEL.1.1E | The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. |
| Dependencies | No dependencies |

| **ALC_FLR.2** | **Delivery procedures** |
|---|---|
| ALC_FLR.2.1D | The developer shall document and provide flaw remediation procedures addressed to TOE developers. |
| ALC_FLR.2.2D | The developer shall establish a procedure for accepting and acting upon all reports of security flaws and requests for corrections to those flaws. |
| ALC_FLR.2.3D | The developer shall provide flaw remediation guidance addressed to TOE users. |
| ALC_FLR.2.1C | The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE. |
| ALC_FLR.2.2C | The flaw remediation procedures shall require that a description of the nature and effect of each security |

| | |
|---|---|
| | flaw be provided, as well as the status of finding a correction to that flaw. |
| ALC_FLR.2.3C | The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws. |
| ALC_FLR.2.4C | The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users. |
| ALC_FLR.2.5C | The flaw remediation procedures shall describe a means by which the developer receives from TOE users reports and enquiries of suspected security flaws in the TOE. |
| ALC_FLR.2.6C | The procedures for processing reported security flaws shall ensure that any reported flaws are remediated and the remediation procedures issued to TOE users. |
| ALC_FLR.2.7C | The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws. |
| ALC_FLR.2.8C | The flaw remediation guidance shall describe a means by which TOE users report to the developer any suspected security flaws in the TOE. |
| ALC_FLR.2.1E | The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. |
| Dependencies | No dependencies |

### 5.4.4 Class ATE: Tests

| **ATE_COV.1** | **Analysis of coverage** |
|---|---|
| ATE_COV.1.1D | The developer shall provide an analysis of the test coverage |
| ATE_COV.1.1C | The analysis of the test coverage shall demonstrate the correspondence between the tests in the test documentation and the TSFIs in the functional specification |
| ATE_COV.1.2C | The analysis of the test coverage shall demonstrate that all TSFIs in the functional specification have been tested |
| ATE_COV.1.1E | The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence |
| Dependencies | ADV_FSP.2<br>ATE_FUN.1 |

| **ATE_FUN.1** | **Functional testing** |
|---|---|
| ATE_FUN.1.1D | The developer shall test the TSF and document the results. |
| ATE_FUN.1.2D | The developer shall provide test documentation. |
| ATE_FUN.1.1C | The test documentation shall consist of test plans, expected test results and actual test results. |
| ATE_FUN.1.2C | The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests. |
| ATE_FUN.1.3C | The expected test results shall show the anticipated outputs from a successful execution of the tests. |
| ATE_FUN.1.4C | The actual test results shall be consistent with the expected test results. |
| ATE_FUN.1.1E | The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. |
| Dependencies | ATE_COV.1 |

| **ATE_IND.2** | **Independent testing - sample** |
|---|---|
| ATE_IND.2.1D | The developer shall provide the TOE for testing. |

| ATE_IND.2 | Independent testing - sample |
|---|---|
| ATE_IND.2.1C | The TOE shall be suitable for testing. |
| ATE_IND.2.2C | The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF. |
| ATE_IND.2.1E | The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. |
| ATE_IND.2.2E | The evaluator shall execute a sample of tests in the test documentation to verify the developer test results. |
| ATE_IND.2.3E | The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified. |
| Dependencies | ADV_FSP.2<br>AGD_OPE.1<br>AGD_PRE.1<br>ATE_COV.1<br>ATE_FUN.1 |

### 5.4.5 Class AVA: Vulnerability assessment

| AVA_VAN.2 | Focused vulnerability analysis |
|---|---|
| AVA_VAN.2.1D | The developer shall provide the TOE for testing. |
| AVA_VAN.2.1C | The TOE shall be suitable for testing. |
| AVA_VAN.2.1E | The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. |
| AVA_VAN.2.2E | The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE. |
| AVA_VAN.2.3E | The evaluator shall perform an independent vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design, security architecture description and implementation representation to identify potential vulnerabilities in the TOE. |
| AVA_VAN.2.4E | The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Enhanced-Basic attack potential. |
| Dependencies | ADV_ARC.1<br>ADV_FSP.2<br>ADV_TDS.1<br>AGD_OPE.1<br>AGD_PRE.1 |

# 6 TOE SUMMARY SPECIFICATION

This section presents an overview of the security functions implemented by the TOE.

## 6.1 TOE security functions

### 6.1.1 Security Audit Data Generation

AR System provides the capability to record actions taken by users and administrators through a variety of logging options. AR System Server logs are managed from the Log Files tab of the AR System Administration: Server Information form. The administrator can control the location of the audit data and can enable and disable the audit function via the Server Information Form; the TOE will generate an audit record when audit logging is enabled and disabled. The log data can be written to a file and stored, to a form in AR System and saved, or viewed as it is generated (and stored later.). When log data is written to a form, access is controlled by permissions on the logging form, managed by the administrator. In this case, data is viewed by opening the log form in the AR System browser interface. If the audit data is sent to a file, the administrator must protect these files by setting the appropriate directory and file level access controls in the environment. The administrator views and may save these log files by using a text editor. If the audit data is viewed as it is generated, the AR System Log Display (arlogdisplay.exe) is used and the files can be saved to a file for storage and accessed after they are generated to display, search, or edit the content.

The administrator can direct the output for different types of logging into a single file or log form to collate information. All log entries are marked with a reliable timestamp indicating the time and date of the entry and each entry indicates the type of event, the identity of the subject making the change, and the outcome of the event (success or failure). The timestamp is obtained from the environment. Each log file records the startup and end of logging activity.

For example, the API log tracks all API calls to the server, and the SQL log tracks all AR System Server SQL requests that send and retrieve data to and from the database server. By combining these two logs any server API communication and database transaction can be detected, including:

- Successful and unsuccessful requests to perform an operation on an object covered by the access control policy (GRP_ACC_CTRL SFP).
- Use of the management functions managed in the AR System Administration: Server Information form, such as setting or changing the identification and authentication mechanism, limiting access by anonymous, changing the application server passwords, managing the encryption settings, and configuring the minimum length, complexity, and validity period of user passwords.
- Modifications to the user security attributes by changes to the User, Group, and Roles forms or the permission list of any controlled object.
- The encryption key exchange at session startup, and at key expiration.

The User log records all connection attempts to the server, and therefore can record unsuccessful login attempts, including the username provided, by both human and application service users. This log can also detect an unsuccessful binding of user security attributes to a subject because in the case of an unsuccessful binding, no username would be provided with the login attempt.

The logging configuration options for the API, SQL, and User logs do not allow the administrator to select which type of events are audited. When enabled, these logs capture all activity between the server and all components of the client tier, the mid tier and the server tier.

The administrator can configure the BMC Remedy Premium Encryption Security to report information to a log file by setting an environment variable on the computer where encryption functions are to be traced. This setting includes administrator-configurable log levels. Encryption Security reports the failure of encryption and decryption operations, including the operation type and the failure of key generation activity, to a log file.

Logging by the Encryption Security also includes a self-test functionality for the FIPS-certified AES algorithm in accordance with the FIPS requirement to periodically validate the encryption library. For the encryption algorithms AES and RSA, the self test performs a known answer test (KAT). If the self test fails the library goes into self-test failed mode and does not perform any other cryptographic function. In this case the server will not carry out any communications until the problem is corrected.

The administrator must protect the Encryption Security log files by setting the appropriate directory and file level access controls in the environment. The administrator views these log files by using a text editor.

The functionality described above satisfies the FAU_GEN.1, FAU_GEN.2, and FAU_SAR.1 functional requirements by recording the occurrence of security relevant modifications to the system to include the nature of the modification, the time and date, and the identity of the entity making the change.

### 6.1.2 Cryptographic Support

The TOE includes BMC Remedy Premium Encryption Security for encryption of communications between all components and the AR System Server: Standard Security is built into the AR System API, but ***for the evaluated configuration, the administrator is required to install BMC Remedy Premium Encryption Security***. Premium Security provides a FIPS-compliant configuration option.

In the evaluated configuration, BMC Remedy Premium Encryption Security must be configured in this encryption mode: *AES CBC w*ith a 128 bit or 256-bit key for data encryption and a 2048-bit modulus for the RSA key exchange. It uses SHA-256 for message authentication. This option supports premium FIPS 140-2 encryption requirements.

The Java plug-in server and the Java API use the RSA Crypto-J 4.0 FIPS-140 jsafeJCEFIPS.jar cryptographic module, following the procedures specified in the RSA BSAFE Crypto-J Cryptographic Module Security Policy (CMVP Certificate number 1048). This module is also installed on and used by the AR System Java API clients, including BMC Remedy Mid Tier, BMC Remedy Developer Studio, the BMC Remedy Flashboards server, and BMC Remedy Email Engine, for all communication with the AR System Server. The Java plug-in server and its plug-ins, also uses this module for communication with the AR System Server.

The AREA LDAP plug-in uses the FIPS compliant Network Security Services (NSS) version 3.11.4 (CMVP Certificate number 815). LDAP libraries provided by Mozilla when it establishes a session with the LDAP directory service in the environment. The RSA key generation algorithm conforms to ANSI X9.31. The LDAP plug-in is an LDAP client, so AR System does not control the encryption policies that are used when an LDAP plug-in session is established with the LDAP directory service in the environment.

When configured, AR System Premium Encryption causes the AR System Server to generate a public and private key pair at startup, using the selected 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 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 selected 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 API calls from the encryption module library to perform key zeroization to destroy ephemeral keys used for encrypted communication.

Because all communication with the AR System Server must come through the API, all components implement this encryption functionality when the session is initiated with the AR System Server.

The functionality described above satisfies the FCS_COP.1, FCS_CKM.1, and FCS_CKM.4 functional requirements by encrypting and decrypting AR System communications according to specified FIPS mode (AES CBC) algorithms and using specified cryptographic key sizes, by generating cryptographic keys according to a specified algorithm and key sizes, and by destroying cryptographic keys by freeing of the data structure.

**Note:** The evaluated configuration relies on the 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. 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 administrator is required to configure SSL for these two elements of the evaluated configuration – satisfying the objective: OE.SECURE_COMMUNICATION.

### 6.1.3 User Data Protection

#### 6.1.3.1 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 Identification and Authentication—TSF_FIA section 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, packing lists, flashboards, and flashboards variables. (Packing lists are only used at design time in BMC Remedy Developer Studio by authorized administrators and authorized subadministrators where assigned, to organize related workflow objects when creating an application. Flashboards variables define the data that is represented by the graphical object in the flashboard. Access is controlled at the level of the flashboard and the flashboard variable. The user must have permission to flashboard to see the flashboard object at all, and to the flashboard variables to see the graphical depiction of the data.)

(Some other AR System object types, including filters, filter guides, and escalations, are only accessible to administrators and subadministrators, and are only executed by the 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 permissions.)

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

#### 6.1.3.2 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. Only members of the Administrator group have permission to add users to groups in the User form. 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, the AR System Server checks the group or AR System role permissions in the permission list of 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. Each access-controlled server object has a name that is unique among its type (for example, no two active links can have the same name) and also a unique id. The server uses the object type and the name or ID to identify the object.

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[1]. The possible permission types vary with the object type, as shown in Table 11.

[1] "No permission" is the absence of all permission on an object when no permission has been defined for the object.

## Table 10. 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<br>Forms<br>Active link guides | Members of the group have permission to view or select the object in the object list in the AR System browser interface, 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<br>Forms<br>Active link guides | Members of the group have access to the object through workflow, but the object cannot be opened in the AR System browser. Through workflow, Hidden permission gives execute access to applications and active link guides, and read, create, or delete 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<br>Flashboards<br>Flashboards variables | 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. For flashboards variables, this permission grants access to the data being depicted in 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 two predefined explicit administration groups:

- 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.)

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. When the administrator creates a new user, that user is automatically part of the Public group. Therefore, a new user has access to any objects for which the administrator has granted permissions to 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 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).

Licensing affects 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 record. 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.

### 6.1.4 Identification and Authentication

#### 6.1.4.1 Functional requirement FIA_ATD.1 (User attribute definition)

The user name and group membership attributes are stored in the User Form in AR System. If AR System is not configured for external authentication, the user's password is also stored in the User Form, using a 128-bit MD5 one-way salted hash, which is retrieved using the API. In this case, users can change their AR System passwords by using the Change Password link on the AR System Home Page. If AR System is configured to use external authentication, the users' AR System password is blank – triggering AR System to use the configured external authentication. The security attributes user name and group membership are used by the AR System Server when checking access to AR System controlled objects.

In the User form the TOE stores information about the users including user name, user password, user group, and license type; it uses these attributes to authenticate and authorize user access to protected objects. When the TOE is configured for external authentication, the TOE also maintains an LDAP mapping of LDAP groups that are defined in the LDAP server to user group defined in AR System. The above functionality satisfies the functional requirement FIA_ATD.1.1 by maintaining the user name, password, and group membership security attributes.

#### 6.1.4.2 Functional requirement FIA_SOS.1 (Verification of secrets)

The AR System provides a password complexity mechanism that allows the authorized administrator to configure a password policy via the User Password Management Configuration form. This form allows the administrator to set any of the following restrictions:

- Blank passwords are not allowed,
- Password cannot match the login name,
- The user cannot use the old password when changing the password,
- Must be a minimum number of 8 characters,
- Must include at least one uppercase alphabetic character,
- Must include at least one lowercase alphabetic character,
- Must include at least one non-alphanumeric (special) character,
- Password shall have a maximum lifetime, configurable by the authorized administrator.

The above functionality satisfies the functional requirement FIA_SOS.1.1 by ensuring that the user password meets complexity requirements as specified by the authorized administrator. Note that the password complexity requirements defined by FIA_SOS.1 apply to user passwords maintained by the TOE in the User Form; FIA_SOS.1 does not apply to password maintained by the external authentication servers that may be used by the TOE. Password complexity requirements do not apply to the Application Service Passwords.

#### 6.1.4.3 Functional requirements FIA_UAU.2 (User authentication before any action), FIA_UAU.5 (Multiple authentication mechanisms) and 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. At each of the user accessible external interfaces, users must enter their username and password to be authenticated. At the BMC Remedy client interfaces (BMC Remedy Developer Studio for example), 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) if required. The user name and password must be successfully authenticated before the user can perform any action within AR System.

User passwords are stored in the User form. By default, AR System authenticates users at login time by comparing the user-supplied user name and a hash of the user password to the attributes stored in the User form (internal authentication). With internal authentication, the Authentication String field of the login dialog box is not used.

AR System can also be configured to use external authentication, in which case the user name and password are stored in the User form, but the password is blank, which triggers AR System to rely on the environment to authenticate the user. 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 10.

## Table 11. 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 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 provides to 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, the 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. The AREA LDAP plug-in returns the authentication result obtained from the environment to the AR System Server. |

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 the User form, leave the Password field blank;
- In the AR System Administration: Server Information form, select the Cross Ref Blank Password check box in the EA tab.

Guest users are those users who are not listed in the User form. For the evaluated configuration, the administrator must configure AR System to disallow guest users, by deselecting the Allow Guest Users checkbox in the Configuration tab of the AR System Administration: Server Information form.

The functionality described above satisfies the functional requirements FIA_UAU.2 and FIA_UID.2.1 by requiring users to be identified and authenticated before they can take any other action in the AR System.

### 6.1.4.4 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.

### 6.1.4.5 Functional requirement FTA_TSE.1 (TOE session establishment)

Authorized administrators use the User Password Management Configuration form to configure the expiration time for user passwords for all users, as well as the number of warning days before the password expires, and the number of days after expiration until the user is disabled. If the user attempts to log in after the password is expired, the user cannot be authenticated and a session is not established.

The functionality described in this section satisfies FTA_TSE.1.1 by preventing the establishment of a user session after the configured validity period.

### 6.1.5 Security Management

Authorized administrators use various options in the AR System Administration: Server Information form in the AR System browser interface, and in the Mid Tier Configuration Tool to manage access control and other aspects of security policy.

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

AR System supports the use of the authorized administrator role to manage all 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 the AR System Administration: Server Information form to set or modify server settings for the AR System Server and the application servers. This includes determining the behavior of, enabling, disabling, and modifying the behavior of external authentication; enabling or disabling access by anonymous (guest) users, determining the behavior of, and enabling or disabling other settings in the AR System Server information form. Authorized administrators access the AR System Administration: Server Information form through the AR System browser interface. They can open the form directly, or navigate to it by using the AR System Administration Console link on the administrator's AR System home page. Non-administrators do not see this link on the AR System home page and do not have permission to the AR System Administration: Server Information form.

The 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.***

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.

#### 6.1.5.2 Functional requirement FMT_MSA.1 (Management of security attributes)

Administrators maintain the access control attributes associated with users (user name, groups and group membership) in the User and Group forms. Administrators also map AR System roles to groups by using the Roles form. The User, Group, and Roles forms are accessed through the AR System browser interface.

Only members of the Administrator group have full access to the User form, where they can view, create, delete, and modify user names and group membership. Only members of the Administrator group have access to the Group form, where they can view, create, delete, and modify groups. Only members of the Administrator group have access to the Roles form, where they can map AR System roles to explicit groups.

Administrators and subadministrators use BMC Remedy Developer Studio to develop AR System applications and to manage the appropriate permissions (Visible, Hidden, View, Change, and permission granted, as appropriate) to AR System controlled objects (applications, forms, fields, requests, active links, active link guides, web services, flashboards, and flashboards variables) according to the GRP_ACC_CTRL security policy. 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. Administrators use BMC Remedy Developer Studio to assign subadministrator permissions to applications, forms, and packing lists. Only Members of the Administrator and Subadministrator groups can log into an AR System Server with BMC Remedy Developer Studio; therefore only these roles can create and manage AR System applications and object permissions. Administrators can also change the default permissions for each object type in BMC Remedy Developer Studio.

Administrators, and subadministrators where designated by the administrator, use BMC Remedy Developer Studio to add an Assignee Group or dynamic group field to a form where required for row-level access control. The Request ID, Submitter, and Assigned To fields are core fields included in every form; administrators, and subadministrators where designated, use BMC Remedy Developer Studio to configure the use of these fields on any given form.

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, the permission lists of AR System controlled objects and the mapping of groups to AR System roles to authorized administrators and subadministrators where applicable.

#### 6.1.5.3 Functional requirement FMT_MSA.2 (Secure security attributes)

If user passwords are stored in AR System, the authorized administrator sets the password management policies by editing the User Password Management Configuration form. Only authorized administrators have permission to make modifications to or see settings in this form. The administrator can define password policies for user passwords, include minimum length, complexity requirements, and the maximum validity period.

The functionality described above satisfies the functional requirement FMT_MSA.2 by ensuring that only secure values are accepted for user passwords.

#### 6.1.5.4 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 the Public group, and administrators add group membership as needed. New users are automatically members of the Public group, and as such have access to any object for which the administrator has assigned permission to the group Public.

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.

#### 6.1.5.5 Functional requirement FMT_MTD.1 (Management of TSF data)

Only authorized administrators have full permissions to the User form where user passwords are stored, and therefore only authorized administrators can change the password for any user. A user can change his or her own password by using the Change Password link on the AR System Home Page. This link opens the User Password Change form, which acts as a dialog box to accept the user's current and new passwords. When the user clicks Save in the User Password Change form, workflow inserts the user's new password in the User form. For this reason, users have Hidden permission to the User form. Users are further restricted by row-level access control and field permissions to view only certain fields in only their own entry in the User form.

Only authorized administrators can manage the policies that enforce password restrictions. This includes setting the password minimum length, complexity requirements, and validity period. To do so, the administrator uses the User Password Management Configuration form to set global password policies. The administrator can also configure the same password policy for individual users by using the Password Management section on the User form.

Only authorized administrators can set and change the application server passwords by using the Connection Settings tab of the AR System Administration: Server Information form. Only authorized administrators can configure the encryption key timeout, which is controlled by the Key Expire Interval field on the Encryption tab of the AR System Administration: Server Information form. Non-administrators do not have permission to the AR System Administration: Server Information form.

The functionality described above satisfies the functional requirements FMT_MTD.1 by restricting management of global user password policies, user passwords, and application server passwords to the authorized administrator, and by restricting users to manage only their own password.

#### 6.1.5.6 Functional requirement FMT_SMF.1 (Specification of management functions)

Administrators use the security functionality provided in the AR System 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 BMC Remedy Developer Studio 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 the AR System Administration: Server Information form, accessed through The AR System browser interface, 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.

Administrators use the User Password Management Configuration form and the Password Management section of the User form to configure user password security policies, including setting the minimum length and complexity requirements of user passwords, and the maximum validity period of user passwords.

Administrators use the Connection Settings tab of the AR System Administration: Server Information form to set the application server passwords. The application servers are part of the TOE, and are identified internally when they connect to the AR System Server. The application server passwords are:

- Application Service Password – Used by Email Engine, Approval Server, the Flashboards server, and the Assignment Engine when connecting to the AR System Server.
- Mid Tier Administration Password – Used by the mid tier when connecting to the AR System Server.
- Plug-in Server Local Password – Used by the AREA LDAP plug-in when connecting to the AR System Server.
- DSO Local Password – Used by the DSO process when connecting to the AR System Server. The local DSO process uses this password to connect to its local AR System Server. A remote DSO process is configured on the remote AR System Server to use the target server's local password. The administrator configures both sides of the DSO connection with the name and password of the target server by using the Connection Settings tab of the AR System Administration: Server Information form.

Administrators manage the configuration of BMC Remedy Premium Encryption Security by using the Encryption tab of the AR System Administration: Server Information form. Administrators configure Encryption Security to report information to a log file by setting an environment variable on the computer where encryption functions are to be traced. This setting includes administrator-configurable log levels.

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.

#### 6.1.5.7 Functional requirement FMT_SMR.1 (Security roles)

AR System supports the security roles authorized administrator and authorized subadministrator.

Administrators associate the users with the authorized administrator and authorized subadministrator roles by assigning group membership for the users to the Administrator or the Subadministrator group, respectively. Authorized administrators have full access to all AR System controlled objects and functionality. 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.

AR System also supports the role of authorized subadministrator, by membership in the explicit group Subadministrator. Authorized subadministrators can administer forms to which they have been given access by an authorized administrator, and can create, delete and modify (including granting object permissions) the filters, active links, and escalations connected to those 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.

### 6.1.6 Protection of the TSF

The TOE includes several application servers that act as part of the TOE to carry out workflow operations. These include the Approval Server, the Email Engine, the Flashboards server, the Assignment Engine, the mid tier, and the AREA LDAP plug-in.

#### 6.1.6.1 Extended functional requirement FPT_APP_EXP.1 (Application server authentication)

If installed, each application server connects to the 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 editing appropriate configuration settings in the AR System Administration: Server Information form or (for the mid tier) in the Mid Tier Configuration Tool.

The application servers are part of the TOE and they initiate contact with the AR System Server. They are identified internally and authenticate themselves when they connect to the AR System Server. At connect time, the 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 the 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 plug-in server is the only component to which the AR System Server initiates contact.

The functionality described above satisfies the extended 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.

#### 6.1.6.2 Functional requirement FPT_ITT.1 (Basic internal TSF data transfer protection)

AR System supports encryption of network communications between all components of the client tier, mid tier, and server tier, and the AR System Server. FPT_ITT.1 does not apply to the traffic between the TOE and the external AREA LDAP server or between the web browser (not included in the TOE) and the mid tier; this traffic is protected by the operational environment. The *BMC Remedy Action Request System Common Criteria Supplemental Guide* requires the use of AES for these communications; however, the TOE does not control them.

FPT_ITT.1 applies to communication between the TOE, or the API communications. To protect the internal transfer of TSF data between components of the TOE, the administrator must install the selected BMC Remedy Premium Encryption Security on the AR System Server computer and on any computer running a client tier, mid tier, or server tier component of AR System. The administrator must also set the Security Policy setting on the Encryption tab of the AR System: Server Information form to Required.

# 7 PROTECTION PROFILE (PP) CLAIMS

There are no Protection Profile claims in this Security Target.

# 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 countered
- Environmental objectives to assumptions met
- TOE SFRs to objectives met
- TOE SFRs to TOE Security Functions

### Assurance level

A justification is provided for selecting an EAL2+ level of assurance for this ST.

### Dependencies

A mapping is provided as evidence that all dependencies are met.

## 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 environment are traced back to assumptions for the environments.

**Table 12. Environment to objective correspondence**

| | T.ACCOUNT | T.UNAUTH_ACCESS | T.EXCEED_PRIV | T.MANAGE | A.OPERATIONAL_ENVIRONMENT_ LOCKED_DOWN | A.INSTALL | A. NO_EVEIL_ADM | A.MANAGE | A.PHYSICAL_PROTECT | A.PEER_ASSOCIATION | A.DAC | A.EXTERNAL_AUTHENTICATION | A.PLATFORM_SUPPORT | A.TIME | A.SECURE_COMMUNICATION |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **O.ACCOUNTABLE** | X | | | | | | | | | | | | | | |
| **O.AUTHORIZATION** | | X | | | | | | | | | | | | | |
| **O.DISCRETIONARY_ACCESS** | | | X | | | | | | | | | | | | |
| **O.ENCRYPT** | | X | | | | | | | | | | | | | |
| **O.MANAGE** | | X | X | X | | | | | | | | | | | |
| **OE.OPERATIONAL_ENVIRONMENT_ LOCKED_DOWN** | | | | | X | | | | | | | | | | |
| **OE.INSTALL** | | | | | | X | | | | | | | | | |
| **OE. PERSON** | | | | | | | X | X | | | | | | | |
| **OE.PHYSICAL** | | | | | | | | | X | | | | | | |
| **OE.PEER_ASSOCIATION** | | | | | | | | | | X | | | | | |
| **OE. DAC** | | | | | | | | | | | X | | | | |

| | T.ACCOUNT | T.UNAUTH_ACCESS | T.EXCEED_PRIV | T.MANAGE | A.OPERATIONAL_ENVIRONMENT_ LOCKED_DOWN | A.INSTALL | A. NO_EVEIL_ADM | A.MANAGE | A.PHYSICAL_PROTECT | A.PEER_ASSOCIATION | A.DAC | A.EXTERNAL_AUTHENTICATION | A.PLATFORM_SUPPORT | A.TIME | A.SECURE_COMMUNICATION |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **OE.EXTERNAL_AUTHENTICATION** | | | | | | | | | | | | X | | | |
| **OE.PLATFORM_SPT** | | | | | | | | | | | | | X | | |
| **OE.TIME** | | | | | | | | | | | | | | X | |
| **OE.SECURE_COMMUNICATION** | | | | | | | | | | | | | | | X |
| **OE.AUDIT_PROTECTION** | | | | | | | | | | | | | X | | |

## Table 13. Security objectives rational for the TOE

| Objective | Threat | Rationale |
|---|---|---|
| O.ACCOUNTABLE | T.ACCOUNT | O.ACCOUNTABLE mitigates the T.ACCOUNT threat by ensuring that security relevant changes to configuration are documented and are attributable in a non-reputable fashion to the entity responsible for the modification. |
| 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. |
| O.ENCRYPT | T.UNAUTH_ACCESS | O.ENCRYPT helps to mitigate the threat T.UNAUTH_ACCESS by requiring that all TSF data flowing between the TOE components is encrypted. |
| O.MANAGE | T.UNAUTH_ACCESS<br>T.EXCEED_PRIV<br>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 rational for the environment

| Objective | Assumption | Rationale |
|---|---|---|
| OE.OPERATIONAL_ ENVIRONMENT_LOCKED_ DOWN | A.OPERATIONAL_ENVIRONMENT_ LOCKED_DOWN | OE.OPERATIONAL ENVIRONMENT_LOCKED_DOWN meets the assumption A.OPERATIONAL_ ENVIRONMENT_LOCKED_DOWN. This environmental objective ensures that all supporting operational environment components (such as the operating system, database, web browser, web server, email server, and LDAP server have had all current security patches applied, and that the authorized administrator has configured the supporting operational component(s) 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 the AR System Server's interface to the supporting operational component(s). |
| 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<br>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 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. |
| OE.DAC | A.DAC | OE.DAC meets the assumption A.DAC. This objective for the operational 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 operational 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 platform(s) upon which the TOE executes and all other components in the operational environment including the operating system, database, email server and LDAP server will provide reliable functionality including correct hardware operation and functionality, and correct platform software operation. |
| OE.TIME | A.TIME | The environment objective OE.TIME meets the assumption A.TIME, by requiring that the operational environment of the |

| Objective | Assumption | Rationale |
|---|---|---|
| | | TOE must provide reliable system time. |
| OE.SECURE_ COMMUNICATION | A.SECURE_ COMMUNICATION | OE.SECURE_COMMUNICATION meets the assumption A.SECURE_COMMUNICATION by requiring that the TOE operational environment must provide the ability to configure SSL communications. |
| OE.AUDIT_ PROTECTION | A.PLATFORM_ SUPPORT | OE.AUDIT_PROTECTION meets the assumption A.PLATFORM_SUPPORT by requiring that the operational environment store and protect the audit trail from inappropriate access. |

## 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.

**Table15. Security functional requirements rationale for the TOE**

| SFR | Rationale |
|---|---|
| FAU_GEN.1, FAU_GEN.2, and FAU_SAR.1 | FIA_GEN.1, FAU_GEN.2, and FAU_SAR1 work together to ensure that privileged actions that are performed by a user are traceable and attributable to a user of the system. These SFRs trace back to and aid in meeting the following objective: O.ACCOUNTABLE |
| FCS_COP.1, FCS_CKM.1, and FCS_CKM.4 | FCS_COP.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 objectives: O.AUTHORIZATION and O.ENCRYPT |
| 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 objective: 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_SOS.1, FIA_UAU.2, FIA_UID.2 and FIA_USB.1 to meet the following objective by providing the association between user names and group membership: O.AUTHORIZATION |
| FIA_SOS.1 | FIA_SOS.1 ensures that user passwords confirm to a complexity scheme established by the authorized administrator via the User Password Management Configuration form. This SFR traces back to the objective O.AUTHORIZATION. It works with the TOE security requirements FIA_ATD.1, FIA_UAU.2, FIA_UID.2, and FIA_USB.1 to meet the objective: O.AUTHORIZATION |
| FIA_UAU.2, and FIA_UAU.5 | FIA_UAU.2 requires a user to be successfully authenticated before any access to the TOE is allowed. FIA_UAU.5 requires the TSF to provide multiple methods of user authentication. These SFRs trace back to the objective O.AUTHORIZATION. They work together with the TOE security requirements FIA_ATD.1, FIA_SOS.1, FIA_UID.2 and FIA_USB.1 to meet the objective: O.AUTHORIZATION |
| 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, FIA_SOS.1, FIA_UAU.2 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, FIA_SOS.1, FIA_UAU.2 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 |

| SFR | Rationale |
|---|---|
| | 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 objective: 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 |
| FMT_MSA.2 | FMT_MSA.2 ensures that the TOE only accepts secure values for locally managed user defined passwords. This SFR traces back to and aids in meeting the objective: O.MANAGE |
| 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 objective: O.MANAGE |
| FMT_MTD.1 | Ensures that TSF data, in the form of passwords, can be effectively managed by an authorized administrator. This SFR traces back to, and aids in meeting the following objective: 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 objective: 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 objective: O.MANAGE |
| FPT_APP_EXP.1 | FPT_APP_EXP.1 is an extended requirement for the TOE. It ensures that only authorized application servers that are part of the TOE can connect to the AR System Server when executing workflow. This SFR traces back to and aids in meeting the following objective: O.AUTHORIZATION |
| FPT_ITT.1 | Ensures that data transferred between application servers and the AR System remains protected from disclosure and modification. This is accomplished by use of AES encryption to protect API communications between separate parts of the TOE. This SFR traces back to and aids in meeting the following objectives: O.AUTHORIZATION and O.ENCRYPT |
| FTA_TSE.1 | Ensures that when user passwords have exceeded an age defined by the Authorized Administrator, the user is denied the ability to establish a session. This SFR traces back to, and aids in meeting the following objective: O.AUTHORIZATION |

## Table 16. Objective to requirement correspondence

| TOE security functional requirement | O.ACCOUNTABLE | O.AUTHORIZATION | O.DISCRETIONARY_ACCESS | O.MANAGE | O.ENCRYPT |
|---|---|---|---|---|---|
| FAU_GEN.1 | X | | | | |
| FAU_GEN.2 | X | | | | |
| FAU_SAR.1 | X | | | | |
| FCS_COP.1 | | X | | | X |
| FCS_CKM.1 | | X | | | X |
| FCS_CKM.4 | | X | | | X |
| FDP_ACC.1 | | | X | | |
| FDP_ACF.1 | | | X | | |
| FIA_ATD.1 | | X | | | |
| FIA_SOS.1 | | X | | | |
| FIA_UAU.2 | | X | | | |
| FIA_UAU.5 | | X | | | |
| FIA_UID.2 | | X | | | |
| FIA_USB.1 | | X | | | |
| FMT_MOF.1 | | | | X | |
| FMT_MSA.1 | | | | X | |
| FMT_MSA.2 | | | | X | |
| FMT_MSA.3 | | | | X | |
| FMT_MTD.1 | | | | X | |
| FMT_SMF.1 | | | | X | |
| FMT_SMR.1 | | | | X | |
| FPT_APP_EXP.1 | | X | | | |
| FPT_ITT.1 | | X | | | X |
| FTA_TSE.1 | | X | | | |

### 8.2.2 Rationale for extended requirements

This ST contains an extended requirement 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 this extended requirement. 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 this extended requirement. Existing families in the FPT class did not provide coverage of authentication for internal TOE components and as such the APP family was defined and is used for this purpose.

Since no other component of the CC addresses the function of controlling internal application component access to another component of the TOE, an extended requirement was defined.

## 8.3 Rationale for assurance level

EAL2+ was selected as the assurance level because the TOE is a commercial product whose users require a moderate level of independently assured security. AR System is targeted at a relatively benign environment with good physical access security and competent administrators. Within such environments, it is assumed that attackers will have an attack potential that can be characterized as basic. AR System provides a level of protection that is appropriate for operational environments that implement IT applications such as Help Desk and Asset Management. As such, it is believed that EAL2+ 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 17 provides a mapping of SFRs to the TSFs to show that each SFR is captured within a security function.

**Table 17. Mapping of SFRs to security functions**

| SFR | Name | TSF |
|---|---|---|
| FAU_GEN.1 | Audit data generation | Security Audit Data Generation |
| FAU_GEN.2 | User identity association | Security Audit Data Generation |
| FAU_SAR.1 | Audit data review | Security Audit Data Generation |
| FCS_COP.1 | Cryptographic operation | Cryptographic Support |
| FCS_CKM.1 | Cryptographic key generation | Cryptographic Support |
| FCS_CKM.4 | Cryptographic key destruction | Cryptographic Support |
| FDP_ACC.1 | Access control policy | User Data Protection |
| FDP_ACF.1 | Security attribute-based access control | User Data Protection |
| FIA_ATD.1 | User attribute definition | Identification and Authentication |
| FIA_SOS.1 | Verification of secrets | Identification and Authentication |

| SFR | Name | TSF |
|---|---|---|
| FIA_UAU.2 | User authentication before any action | Identification and Authentication |
| FIA_UID.2 | User identification before any action | Identification and Authentication |
| FIA_UAU.5 | Multiple authentication mechanisms | Identification and Authentication |
| FIA_USB.1 | User-subject binding | Identification and Authentication |
| FMT_MOF.1 | Management of security functions behavior | Security Management |
| FMT_MSA.1 | Management of security attributes | Security Management |
| FMT_MSA.2 | Secure security attributes | Security Management |
| FMT_MSA.3 | Static attribute initialization | Security Management |
| FMT_SMF.1 | Specification of management functions | Security Management |
| FMT_SMR.1 | Security roles | Security Management |
| FPT_APP_EXP.1 | Application server authentication | Protection of the TSF |
| FPT_ITT.1 | Basic internal TSF data transfer protection | Protection of the TSF |
| FTA_TSE.1 | TOE session establishment | Identification and Authentication |

## 8.5 Requirement dependency rationale

Table  is a cross-reference of the functional components, their related dependencies, and whether the dependency was satisfied.

### Table 18. SFR dependency status

| Functional component ID | Functional component name | Dependencies | Satisfied |
|---|---|---|---|
| FAU_GEN.1 | Audit data generation | FPT_STM.1 | No, see notes following table. |
| FAU_GEN.2 | User identity association | FAU_GEN.1<br>FIA_UID.1 | Yes<br>Yes |
| FAU_SAR.1 | Audit review | FAU_GEN.1 | Yes |
| FCS_COP.1 | Cryptographic operation | FCS_CKM.1<br>FCS_CKM.4 | Yes<br>Yes |
| FCS_CKM.1 | Cryptographic key generation | FCS_COP.1<br>FCS_CKM.4 | Yes<br>Yes |
| FCS_CKM.4 | Cryptographic key destruction | FCS_CKM.1 | Yes |
| 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<br>Yes |
| FIA_ATD.1 | User attribute definition | No dependencies | N/A |
| FIA_SOS.1 | Verification of secrets | No dependencies | N/A |
| FIA_UAU.2 | User authentication before any action | FIA_UID.1 | Yes, by FIA_UID.2, which is hierarchical to FIA_UID.1. |
| FIA_UAU.5 | Multiple authentication mechanisms | No dependencies | N/A |
| FIA_UID.2 | 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<br>FMT_SMF.1 | Yes<br>Yes |
| FMT_MSA.1 | Management of security attributes | FDP_ACC.1<br>FMT_SMR.1<br>FMR_SMF.1 | Yes<br>Yes<br>Yes |

| Functional component ID | Functional component name | Dependencies | Satisfied |
|---|---|---|---|
| FMT_MSA.2 | Secure security attributes | FDP_ACC.1 | Yes |
| | | FMT_MSA.1 | Yes |
| | | FMT_SMR.1 | Yes |
| FMT_MSA.3 | Static attribute initialization | FMT_MSA.1 | Yes |
| | | FMT_SMR.1 | Yes |
| FMT_MTD.1 | Management of TSF data | FMT_SMR.1 | Yes |
| | | FMT_SMF.1 | 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_APP_EXP.1 | Application server authentication | FMT_MSA.1 | Yes |
| | | FMT_SMR.1 | Yes |
| FPT_ITT.1 | Basic internal TSF data transfer protection | No dependencies | N/A |
| FTA_TSE.1 | TOE session establishment | No dependencies | N/A |

Note: **FPT_STM.1 -** The TOE generates the reliable timestamp for audit records it creates based on time data obtained from the underlying operating system. This is covered by OE.TIME.

## 8.6 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. 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. All SFR dependencies have been satisfied or rationalized.
- The SFRs are internally consistent. There is no conflict between security functions and the SARs to prevent satisfaction of all SFRs.

*442598*