SAP BASIS and Security Administration

An Article From thespot4sap LTD

Contents

1.0 Introduction 2
2.0 SAP Security Components – The Big Picture 2
  2.1 SAP Authorization Concept 3
  2.2 Composite Profiles 4
  2.3 User Ids 4
  2.4 Authorizations 4
3.0 Security Configuration in SAP 4
  3.1 User Authentication 4
  3.2 Creating and Assigning Authorization Profiles 5
  3.3 Auditing and Monitoring 6
  3.4 Administration and Maintenance 9

SAP BASIS and Security Administration

1.0 Introduction

SAP has done nothing less than change the entire systems landscape for enterprises. The benefits it can bring have led to widespread adoption across the globe. One of the key benefits SAP brings to an enterprise is the ability to integrate the data both within the enterprise, and between it and it's partners / competitors. In many cases organizations today are both partners and competitors at the same time. Think of wholesalers and distributors, SAP and Oracle, AT&T and BT, or two oil giants who have an upstream joint venture. These companies use SAP to integrate process between themselves for their mutual benefit. This ability to integrate, however, brings with it a particular risk – that of exposing their data to the un-authorized outside world.

Entire companies have been built up around highly guarded intellectual property and process secrets ... and could easily fall if this was breached. Therefore, keeping the security of the organization intact is one of the vital aspects of any SAP implementation.

SAP BASIS addresses all security issues by incorporating an authorization module. With increased potential for security breaches in the computer systems around the world, BASIS consultants face a tough task of maintaining the integrity and administering the security of SAP systems. Interoperability features of a SAP system makes this task a bit more difficult.

2.0 SAP Security Components – The Big Picture

SAP security in form of discrete components as

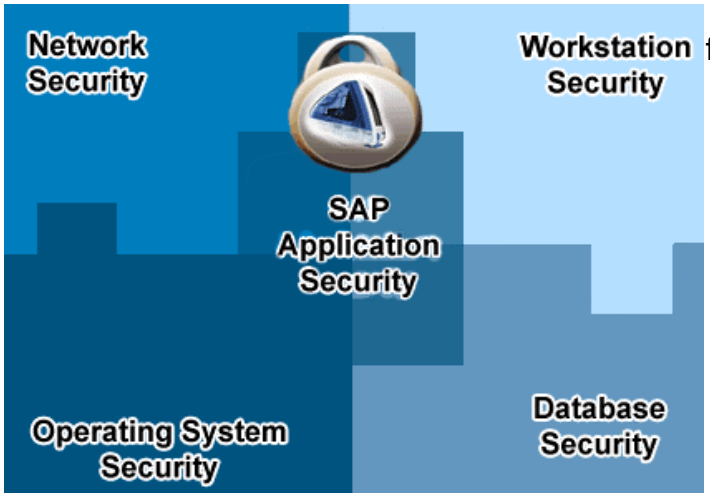

Figure 1

Tight security is required for each of the above components (Network, Workstation, Operating System and Database) as a breach made in one area can compromise the entire system.

The scope of this article is SAP Application Security, which can be achieved with the help of SAP's BASIS security application through the concept of authorization.

In SAP, security is administered for objects (profiles and authorizations). Users are only authorized to see or change the parts of the system required by their respective job responsibilities.

2.1 SAP Authorization Concept

The SAP authorization concept is based upon the logical relationship between a user ID and the range of system authorizations with which it can be associated. The architecture of the authorization system is based upon the utilization of several individuals but related logical components: Profiles, Objects, Fields, and Authorizations. The user ID refers exclusively to profiles. Each profile grants a set of specific system access authorizations to user. Figure 2 illustrates the hierarchical authorization concept in SAP.

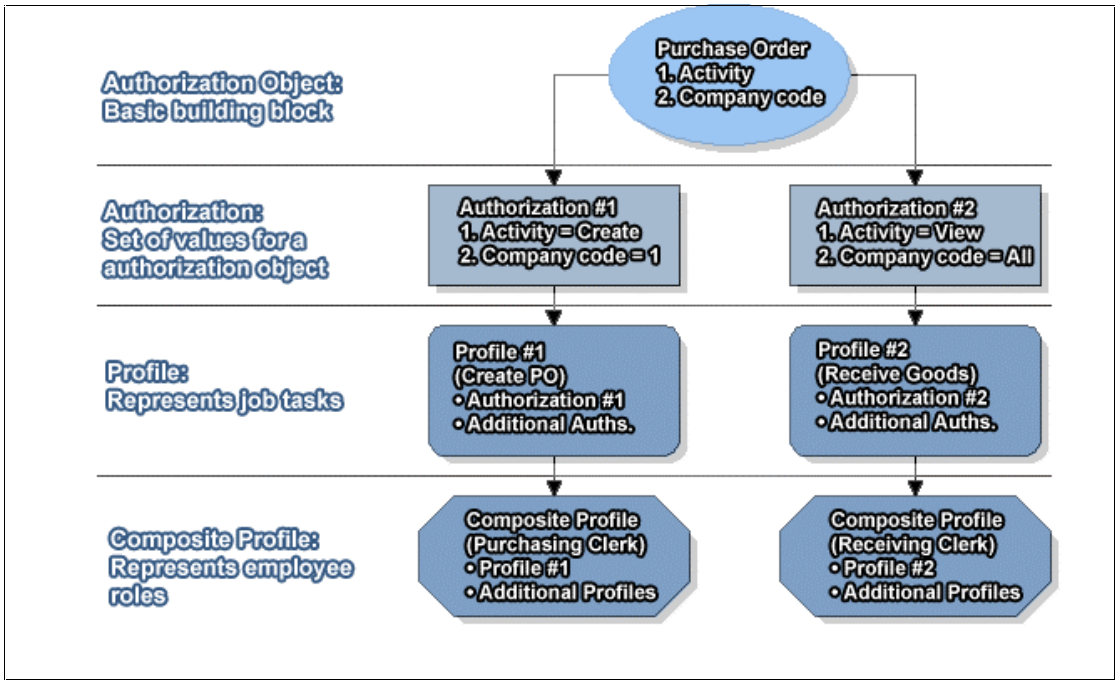

Figure 2

2.2 Composite Profiles

Composite profiles refer to the various employee roles available in the corporation (for instance: Purchasing / Receiving Clerk or Accounts Agent). As the name suggests, composite profiles may contain multiple user IDs necessary to perform all the business operations associated with a particular role. A composite profile may encapsulate another composite profile(s). In practice, a model composite profile should be recognized for each possible role in the organization, which may be used to produce hybrid composite profiles. The over-existence of the hybrids can defy the very purpose of composite profiles and they should be created only when specific needs arise.

2.3 User Ids

User ids allow access to SAP applications. Each user must have a corresponding profile specifically assigned. In many situations, multiple composite profiles can be assigned to a user ID, depending on the role(s) an individual user is responsible for, in the business processes.

2.4 Authorizations

Authorizations are the key building blocks of SAP security. Authorization is the process of assigning values to fields present in authorization objects. In SAP, access to all system functionality is achieved through a complex array of authorizations. Sometimes users find that they lack the necessary authorizations to perform a certain function in the system, in which case the message: "You are not authorized..." is displayed at the bottom of the screen.

An authorization process may ask for second associated authorization process which in turn asks for third and so on. For example, the task of paying a vendor invoice may require 10 different authorizations.

3.0 Security Configuration in SAP

Security configuration and administration in SAP is a multi-phase process. Four key security components are required to ensure the adequate security, privacy, and integrity of information. The phases are as follows:

3.1 User Authentication

The first phase comprises confirmation of user identity and results in authentication of user. Unauthorized access to SAP system is prevented through

this initial check. This ensures system integrity by regulating secure access through genuine user authentication.

3.2 Creating and Assigning Authorization Profiles

A Profile Generator (PG) is used to automatically generate and assign authorization profiles. This tool was released with SAP version 3.1g and above. The administrator can also create authorization profiles manually.

Note: Profile Generator can be retroactively installed in SAP versions 3.0f and above.

The authorization objects can be selected using the SAP Profile Generator. Administrators can automatically generate authorization profiles for function-specific access to SAP users after configuring initial settings.

The entire authorization functionality of SAP signifies a new approach to authorization. The administrator can define user authorization based on SAP functions. Based on the selected function, the PG groups objects in administrator-created authorization profiles.

Authorization profiles created by a Profile Generator are based on the given authorizations. It also speeds up the process and simplifies administrator/user communication facilitating both the administrator and users to use the same SAP function terminology. To auto-generate an Authorization profile, an Activity Group needs to be created.

Activity Groups contain simple profiles and usually represent employee or job roles. They are user-defined and allow administrator to organize and maintain system activities. Activity group when used as an information database reduces data entry time. Administrators can define activity groups in two steps:

1. Selecting the criteria, such as access controls.
2. Dividing the activities into appropriate groups.

For example, activities can be organized by functions, such as human resources, payroll, or administration or by job classes, such as computer programming activities, or accounting activities. A combination of function-specific activity and job-specific activity can also be implemented.

Security implementation with the new Profile Generator is based on the creation of activity groups or a collection of linked or associated activities, such as tasks, reports, and transactions.

Consider a business situation involving a company, ABC Inc. faced with transaction security hiccups in business dealings with its dealers. To address this problem, the company can create authorization profiles for its dealers using the profile generator features. This can be done by implementing the following instruction set:

Instruction 1: A dealer activity group should be created. Name this activity group as **Dealer.**

Instruction 2: All dealer-specific business transactions should be included in the activity group.

Instruction 3: Generate an **authorization profile** for Dealers.

Instruction 4: Assign Dealer to a **"new user"** or in your system and update master records.

Following this procedure will ensure complete functional access to the new user using the system as Dealer.

3.3 Auditing and Monitoring

In this subsequent phase, a track of the authorizations created (previous phase) is kept. Detailed accounts of system events are used to record the actions of a user corresponding to that unique user account identifier. Auditing/Monitoring activities should be in compliance with enterprise's overall IT strategy and should be performed on a weekly, monthly, quarterly, and yearly basis.

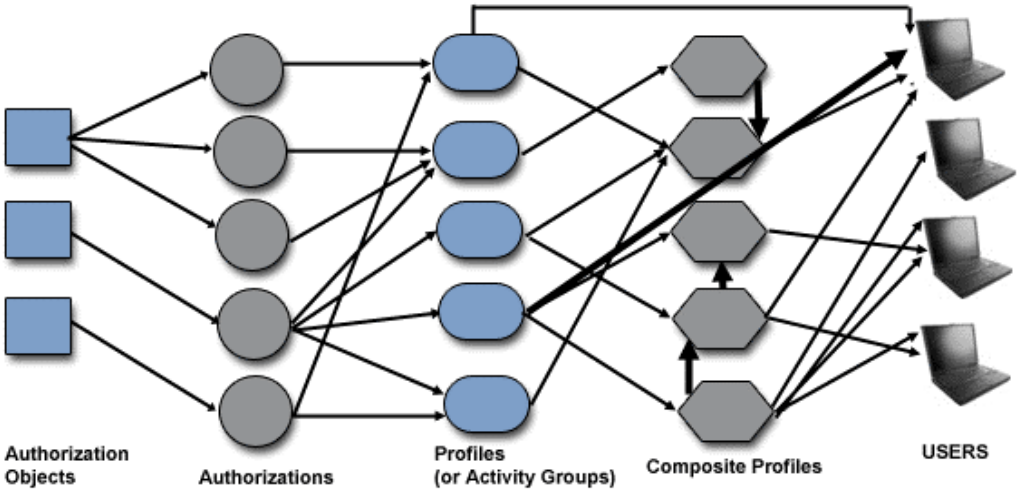

Figure 3

There are some key tasks that should be included in a monitoring plan. The following reviews should be a part of an ideal monitoring plans.

Using System Logs and Security Audit Logs
The system log records critical information important events. Each individual application server maintains local log files to which the information is written periodically. The security audit log records areas such as successful and unsuccessful dialog log-on attempts, RFC log-on attempts, changes to user master records, and transaction starts.

Reviewing User Activity
All SAP system users must be continuously monitored so that their problems can be rectified as soon as they occur. The timely attention to user problems can reduce administration overheads.

For example, if a SAP administrator wants to check for unrecognizable user Ids or the users trying to use non-permitted transactions, administrator can execute transaction AL08 and review user activity.

Monitoring User access in BASIS User Group
The BASIS users in a SAP system have access to sensitive areas of an organization. Therefore it is vital to monitor their access. Following instructions can be performed to check the access of BASIS User group.

Instruction Set

- Enter transaction SUIM to view Repository Information of the system.
- Follow the Menu Path:
    - User **>** Lists of users (according to selection criteria) **>** user IDS (Double Click).

Monitoring Change Requests
All change requests need to be properly reviewed and controlled prior to being applied. This formal process needs to be detailed enough to ensure that separation of duties and other control features are not breached. Strong integration knowledge of the SAP system is required for this review. Critical profiles, authorizations, and transactions need to be identified and treated even more carefully.

Checking Important Default SAP Profiles

Administrators must check that default profiles act a template for user defined profiles and are not directly used in production. Default profiles contain values, which apply to all application servers. These include: SAP_ALL, SAP_NEW, S_A.ADMIN, S_A.CUSTOMIZ, S_A.DEVELOP, S_A.DOKU, S_A.SYSTEM, S_A.USER, S_ENT_IMG_GE, S_WF_ALL, and P_ALL.

Changing Default SAP User ID's

SAP comes with some pre-configure clients (independent business units). They are client 000, 001 and 066 in the non-IDES system. In the IDES system, client 800 is the default client. SAP installation process automatically creates default user Ids and their corresponding passwords. SAP administrators must ensure that they are not used to access the system. The following table explains default user Ids in various SAP clients.

User Ids	Client Name	User Function
SAP*	000 and 001	SAP* denotes the default super user and has all administrative powers.
DDIC	000 and 001	DDIC user is responsible for the maintenance of the ABAP/4 Dictionary and the software logistics.
EarlyWatch	066	The EarlyWatch user has access only to monitoring and performance data.

Instruction Set

- Change all default passwords and verifying the password change by logging into various client areas.
- Assign SAP* to the Super user group.
  - Enter transaction SE16.
  - Enter SAP* into the field called BNAME.
  - Click "Execute" and verify.
- As a final step, check that the secret super user has been created (with a different user ID and password). All of the authorizations assigned to SAP* should then be removed (an empty profile list followed by a password change.

Auditing Information System (AIS)
SAP Audit Information System (AIS) serves as a centralized repository for reports, queries, and views of interest to auditors. It is designed to address the overall system configuration as well as SAP business processes and their related control features, providing audit and security practitioners with the critical information they need to conduct effective reviews of their SAP systems. SAP administrators can use AIS for security auditing. The AIS plays a supportive role in providing security services for SAP systems. The primary function of AIS is auditing but auditing features can derive the measures that help in developing the security policy for SAP systems.

3.4 Administration and Maintenance

A successful security set up of a SAP system concludes with proper management and administration of user IDs, password resetting, audit trails, audit logs, access control list, and personnel responsibilities.

Security administration in SAP includes maintenance of the overall SAP security environment using the SAP Profile Generator, creating user-level activity groups and creating user master records.

The concept of SAP security is flexible as well as complex. SAP has a multi-layered integrated framework. To ensure adequate protection, security measures must be factored into all layers of the SAP infrastructure. With client/server architecture, SAP systems include many components that exchange information, each of which constitutes a layer of the SAP security infrastructure. Security is often not a priority in an implementation and as a result, the default security is not strong. SAP security functionality could be enhanced using various measures as discussed above.

Enterprises must develop a security strategy to ensure a secure and functional SAP system. A business critical application like SAP needs continuous monitoring and improvement of its security features.