8 CHAPTER

User Management and Security in SAP Environments

Security is increasingly being considered one of the key points to boost electronic commerce over the Web. SAP has always established security as one of the critical topics both for the implementation and correct deployment of SAP Solutions and any of the SAP Web-enabled applications. Every professional involved in modern SAP projects is aware that leveraging security technology and measures and a sound security policy is mandatory.

The information stored in the systems we support ranks among a company's most important and valuable assets. Moreover, addressing security during and after a SAP implementation not only protects valuable business information; it ensures continuous and stable systems operations.

Most of the concepts around the SAP and SAP NetWeaver security infrastructure are based on the sound security services typically available in R/3 systems plus the latest security technology. Therefore, this chapter first includes an introduction to traditional SAPs and other general security concepts and options and the second part of the chapter deals with the user administration and the role and authorization concept.

The chapter then takes a deeper approach into Single Sign-On Solutions, the SNC (Secure Network Communications) interface, Digital Signatures, Data Encryption, Public Key Infrastructure (PKI) technologies, and Privacy protection for user data. There are additional sections explaining available security options for user authentication such as cookies, X.509 certificates for Internet connections, standards such as HTTP-SSL (Secure Service Layer), and new Web security services.

It is impossible to cover in one chapter all the topics around the SAP NetWeaver and Java technologies security options. Should you need additional information, you can find comprehensive security documentation at the SAP Service Marketplace in the quick link *Security* (service.sap.com/security).

With the SAP NetWeaver Security Infrastructure, based on market standards, SAP has set in place a full range of security measures and technologies so that business data integrity and privacy are protected against unauthorized access. Security is more than ever increasingly important considering how data and business processes expand beyond intranet levels into Web collaborative scenarios often quite transparent to end users.

With these and many other considerations, SAP and its partners provide a full range of security services to make SAP Solutions a secure place to do business.

Objectives of SAP security are as follows:

- Set up private communication channels.
- Use strong authentication mechanisms.
- Implement group concept in Java.
- Provide evidence of business transactions.
- Enforce auditing and logging.

Among these objectives the security services available for SAP environments are as follows:

- The use of client and server certificates for user *authentication*
- Single Sign-On solutions to access the full range of SAP components and solution
- The *role-based* concept, which involves activity groups and authorizations
- Deployment of firewalls between systems and networks, as well as secure protocols such as HTTPS (HTTP over SSL)
- SNC (Secure Network Communications) and SSF (Secure Store and Forward) for compliance with security standards

Before discussing the specifics of available options and implementation considerations for SAP security, the following sections introduce readers to common security concepts as well as to the background of traditional SAP Security Services from the R/3 age, most of which still apply and have evolved into newer scenarios.

Overview of Security Concepts

Traditional SAP implementation projects usually considered security just as the design and realization of the authorization concept. At the *application level* the authorization concept (user masters, profiles, authorizations, activity groups, roles) is key to provide access to needed transactions and ensure secure access to sensitive data and as such is extremely important within the SAP security infrastructure. However, systems within mySAP Business Suite applications and SAP NetWeaver do have many other *levels* that could be attacked, and therefore a consistent security strategy must also consider all these other layers and components of the SAP systems.

Security can be defined from two different perspectives that have in common the objective of protecting the company systems and information assets. These two perspectives are as follows:

- *Security* as the protection measures and policies against *unauthorized accesses* by illegitimate users (both internal and external). An internal attack is considered when a SAP user tries to access or perform functions for which he or she is not allowed.
- *Security* as protection measures against hardware, software, or any other type of environmental *failures* (disasters, fires, earthquakes, and others) using safety technologies (backup/restore/disaster recovery/standby systems/archiving and so on).

In this chapter only the first perspective is dealt with: explaining some of the most common and practical concepts of SAP security components and security infrastructure from the first perspective to protect SAP systems from unauthorized accesses. It must be noted that a global security policy includes other "non-SAP" related components that can be defined as "peripheral security," such as the measures that must be taken to protect workstations, servers, and networks from the many types of outside attacks (e.g., viruses, denial of services, password cracking, sniffers).

Security Policy Basics

Companies must implement some type of security policy to protect their assets, but also they are required to comply with their country's legal obligations, business agreements, and industry laws and regulations. For instance, many countries have some forms of laws for protecting confidential data of employees. It is also very important to keep all financial records for tax authorities. And in terms of business partners, it is of great importance to ensure the confidentiality of commercial agreements with vendors or customers.

Modern information systems and technologies are both the means and the containers of the strategic and operative business information. They are the known but hidden treasures of companies, and companies need to keep their treasures secure.

The *Security Policy* is the set of procedures, standards, roles, and responsibilities covering and specifying all the security and organizational measures that companies must follow to protect their business from threats and vulnerabilities. An approach to security will have the objective of building a strong security policy and should start by assessing a risk analysis to implement, monitor, and enforce such policy. It is important to realize that security implementation never ends and must be continually updated, reviewed, communicated, implemented, monitored, and enforced.

The security strategy and risk analysis must first consider these basic issues:

a. *What is to be protected?* Companies must identify those assets—such as critical information (customer list, employee personal data, contracts), hardware, software, intangibles (hours of operation, cost of nonrevenue, nonproduction) or others—that require some type and some degree of protection against unwanted and unauthorized access, which could damage or destroy to some degree such assets.

b. *Which are the possible threats?* The second security issue is to identify the possible sources of attack and the degree of vulnerability of infrastructure. Threats are of different type and nature and sometimes unknown. They are often intentional, but can also be unintentional. They can be external threats or can be internal (for instance, by other geographical locations or by burned-out or frustrated employees).

c. *What protection measures can be taken?* Finally, the risk analysis and the security policy must identify the best security measures to implement and enforce such policy efficiently. Measures can be standard measures included in the information system capabilities, additional and external security infrastructure, and behavioral rules. For instance, a basic and strong security measure is the *password* that users must provide to access systems; however, it is almost impossible with technical means to know whether someone told his or her password to someone else.

Efficiency in security policy means that measures do not include awkward procedures that would obstruct or make users' jobs more difficult. Security policies always follow a principle of controls, which means that the security strategy must approach the balance between risks and control measures.

As indicated, security is a continuous process due to the fact that new assets, new threats, or new technology can be identified as well as some threats or assets that are obsolete and no longer need protection. These facts will make the security policy a living entity that also includes the retraining of employees.

In the following sections, the SAP security infrastructure is discussed so that you can better identify threats and vulnerabilities as well as the standard and nonstandard measures that can be applied to better protect and secure your assets.

Risks and Vulnerabilities

The increasing need for broad and open connectivity within complex SAP system landscapes and the increasing number of components within the architecture combined with options for external communications increase the risk of being attacked.

Systems are more vulnerable when a security policy is either insufficient or nonexistent. In these cases people trust that standard measures will be enough, but normally this is not the case.

The following is a brief list of threat types:

- External network attacks to set systems unavailable
- External password cracking attacks
- Internal sabotage to set systems unavailable
- Internal attacks for collecting confidential data
- Unintentional internal attacks or misbehavior
- Trojan programs
- Intentional internal breach of security policy
- Unintentional breach of security policy
- Unknown attacks

The main point is that the greater the number of risks and the fewer security measures in place, the greater the vulnerability of systems and therefore company assets.

Basic Security Processes

The following sections introduce some of the basic processes that are common when dealing with security and that you will find referenced continuously during this chapter.

Authentication

Authentication is the process that is used for verifying that users, programs, or services are actually who they say they are. Authentication is the cornerstone of any security infrastructure or technology.

SAP's standard User Authentication verifies a user's identity through the use of logon passwords. (Unsuccessful logon attempts will cause the session to terminate and activate user locks.) As standard security measures, SAP provides several login profile parameters and an initial set of password rules that you can expand on according to your needs. Standard security measures already provide a moderate to high degree of protection. User Authentication applies mainly at the presentation level, but a breach will affect other layers as well.

Limitations on SAP standard authentication pertain to the legal export rules of different countries regarding encryption software and algorithms. SAP included SNC in the kernel to overcome these limitations.

Additional security measures to raise your system to the highest protection level include the following:

- Using external security products that support encryption. Any such products however must be SNC compliant (see the discussion later in this chapter on SNC).
- Using techniques such as client certificates or logon tickets for Web User Authentication security. However, these methods can only work if other security layers, such as the network and Internet, are also properly protected over secure protocols such as SSL.

Further references for SAP user authentication can be found on the SAP online help, the Security Guide, and the SNC user's guide, which can be found at http://service.sap.com/security.

Smart-Card Authentication

SAP's standard smart-card authentication allows a "safer" authentication process. The users use cards, "smart cards," instead of passwords to log on to the security system. No password information is transmitted over the communication lines. Because the smart cards are often protected with a password or PIN, it is much more difficult for someone to compromise a user's authentication information.

The use of hardware devices such as smart cards is normally configured using an external security system based on the SNC interface.

The smart cards that can be used for login into the SAP Enterprise Portal are actually holders of the private keys of users, so the cards work as digital certificates that authenticate the holder.

Authorization

Authorization is the process that is used for determining what accesses or privileges are allowed for users. Authorizations are enforced by means of *access controls*, which are in charge of restricting user accesses.

SAP's User Authorization Concept

SAP's standard User Authorization secures user access to business data and transactions, ensuring that only preauthorized users gain access to data and processes. User authorizations are defined by Authorization administrators in coordination with key business users in authorization profiles that are stored in the SAP user master records. An initial set of authorization profiles is predefined by SAP; you can modify/add to these profiles and you can use the Profile Generator to create new profiles automatically based on user activity information. Authorization applies to the application level mainly, but remote communications, operating system commands, and the Change and Transport System must also be taken into account.

The SAP authorization system is very comprehensive but difficult to implement fully to achieve the strictest security standards. It is difficult to implement and maintain because it has a great deal of organizational projects in which users, key users, managers, and technical consultants are involved. Therefore, it is necessary to audit and monitor critical system authorizations. The SAP online documentation as well as the SAP security guide provides a good basic understanding and methodology for implementing the authorization concept.

You can increase the security level of SAP's User Authorization system by including well-defined developing standards along with a quality control that filters programs that do not implement the necessary security and authorization checks.

Privacy

Privacy is the process that can be used for ensuring that data or information sent over a network or communication line is not accessed or read by unauthorized persons. A usual way of granting privacy is by using *cryptography* technology. Both authorization and privacy ensure the confidentiality of data and information.

Within SAP landscapes *privacy* can be considered the highest security level that can be set by technological means and can be enforced by means of digital signatures, digital envelopes, and the use of the SNC and SSF components.

Integrity

Integrity is the process that verifies that nothing or nobody modifies data from a source to a target. Similar to the privacy within mySAP landscapes, *integrity* can be enforced by means of digital signatures, digital envelopes, and the use of the SNC and SSF components.

Proof of Obligation

Obligation or proof of obligation is necessary for confirming and guaranteeing that a business message is correct so it can be considered a business transaction between business partners. For this reason in electronic commerce there must be enough security mechanisms to guarantee the *nonrepudiation* of business messages.

Auditing

Auditing is the process of collecting and analyzing security data for verifying that the security policy and rules are complied with. *Accounting* is a way of measuring and/or restricting the use of system resources and as such is a form of authorization.

Cryptography

Cryptography is the technique based on mathematical algorithms and other methods to encode data and thus prevent data from being read or disclosed. Cryptography is commonly defined as the science of secret writing.

SAP's encrypted communications secure the exchange of critical data. This is an important security aspect in e-commerce communications. You can use SAP's SNC (Secure Network Communications) or SSF (Secure Store and Forward) solutions and the SSL (Secure Sockets Layer) protocol to encrypt the data being transferred via HTTPS connections. Data encryption ensures that the data being exchanged are secured end-to-end and protected from being intercepted.

SAP does not directly include encryption software within their solutions but provides the possibility of external security products that are compliant with SNC and SSF so it can be used for authentication, for single sign-on, for digital signatures and envelopes, and so on.

If security measures are not taken seriously, the manipulation and disclosure of information or digital documents is relatively easy with the aid of the current technology. Most of the advanced security measures are based on cryptography technologies. The following sections discuss common topics in modern cryptography applied to information technology.

Public Key Cryptography

Public key cryptography is based on mathematical functions of one direction, meaning that it is impossible to observe the results.

With this type of system each user that originates communications or messages has two keys:

- A private one (secret)
- A public one that is distributed to their communication partners

Every message that is sent with public key can only be decrypted using the private key.

Let’s consider an example of how this system works. Suppose that these keys are the keys for a wooden box: from one of the keys there is only a master copy that you have securely kept; from the other one you have as many copies as you want and you give them to all people who want to communicate with you. The messages are boxes that have two locks (one opens with the secret key and the other one opens with the public one), with the special feature that if the box is closed using one of the keys it can only be opened using the other one.

Because of this procedure each communication partner has its own private key and the public keys from other partners.

If a person (sender A) wants to send a private message to another person (receiver B), the procedure would be as follows: it will introduce the message in a box that would be locked with the public key of the receiver so that only the receiver will be able to open it with his or her private key.

Then there is the following question: once the message is received, how does the receiver know that the message comes from the person (sender A) and not from another person that has his or her public key? This is the type of problem that digital signatures try to solve.

Digital Signatures

Digital signatures are special appendixes that are added to the digital documents to show the authenticity of the origin and the integrity of those documents.

A digital signature is equivalent to the traditional hand-written signatures on paper documents. When someone tries to modify a handwritten signature illegally, there are usually clues that can be detected by physical means. This is usually what guarantees the authenticity and integrity of data and information contained.

The digital signature must guarantee the same elements although using technological means. The first important point is that each digital signature will be different in every document. Otherwise it could be easy to copy and falsify digital signatures. For this reason the digital signature will depend on the document that is being signed using a mathematical function. This mathematical relationship allows for later verification of the validity and authenticity of the document.

The impossibility to falsify any type of digital signature is based on using characteristics or knowledge owned by the sender (the one that signs). Every time a person uses its analogical (handwritten) signature it generates a very similar graphic using its inherent graphological characteristics. In the case of digital signatures the signatory uses its secret private key. This is a very secure mechanism because even if the message is intercepted and someone wants to modify its content, he or she must also modify the signature and that cannot be done without knowing the secret private key.

To guarantee the security of digital signatures, the following points must be applied:

- Digital signatures must be unique: only the signatory can generate them.
- They cannot be falsified: in order to distort the signature the criminal should resolve very complex mathematical algorithms (considered computational safe).
- Verifiable: they should be easily verifiable by the receiver or by a competent authority.
- Nondeniable: the signatory cannot deny its own signature.
- Feasible: digital signatures should be easily generated by the signatory.

Several different protocols based on private key cryptography were proposed in standard organizations. However, currently it has been concluded that the public key cryptography is safer. Digital signatures in use and according to the aforementioned characteristics are based on the RSA signature and the DSS signature (Digital Signature Standard).

In certain countries digital signatures can be used legally as if they were handwritten. In terms of security this means proof of obligation and nonrepudiation. For this reason the use of digital signatures based on public key infrastructure can raise the system to a high degree of security.

Cryptography in SAP Systems

Since release 4.0 of SAP Basis R/3 in 1998, SAP systems have included the SSF (Secure Store and Forward) as a mechanism for protecting some of the data within the system. The SAP applications can use the SSF layer for securing the integrity, authenticity, and privacy of certain data. The key point of the SSF is that the data are still protected when they leave the SAP systems. The first applications using SSF are as follows:

- Production planning–process industry
- Product data management
- ArchiveLink II

SAP is committed to providing further applications that support SSF. SSF uses digital signature and *digital envelopes* for securing data. The digital signature identifies the sender and ensures the data integrity whereas the digital envelope ensures that the message can only be opened by the receiver.

Besides those features the Secure Store and Forward includes others that are relevant and important for electronic transactions:

- SSF is asynchronous: the creation, transmission, reception, process, and confirmation of business transactions are different steps that can take place at different times without locking or affecting the applications in charge of the process.
- Independence of the transport so that it should be possible to use different transfer mechanisms such as public networks, Internet, online services, magnetic disks, and so on as well as different protocols and communication services such as HTTP, FTP, e-mail, and EDI.

In order to perform these functions SSF requires the use of a third-party security product. Since release 4.5 of SAP R/3, the system has included the SAPSECULIB (SAP Security Library) as default provider for SSF services. SAPSECULIB is a software solution, but the functionality is limited to digital signatures. In order to support specific cryptographic hardware such as smart cards or for supporting digital envelopes, SSF needs to be complemented by an external product that must be certified by SAP.

To use digital signatures effectively, it is necessary to maintain a public key infrastructure (PKI). Because there is no accepted worldwide PKI, it is required for this infrastructure to be established in a secure provider domain.

Digital signatures are available in SAP systems and the SAP Business Connector and XI and can be used to secure business documents in SAP environments.

SAP's standard digital signatures authenticate the SAP systems data that are being transmitted and ensure that the senders (signatories) can be clearly determined. The subsequently assigned *digital envelope* ensures that the data contents will only be visible to the intended recipients. On SAP systems digital signatures are based on SSF.

Single Sign-On (SSO)

With SAP's standard Single Sign-On solution, users only need to enter their passwords once when they initially log on to the security system or the operating system. The security system then generates "credential" information so that the users can later automatically log on to other systems, such as R/3 or other mySAP Business Suite components, without any password information being transmitted over the communication lines.

With SAP R/3 and further with the SAP Web Application Server systems, there are many possibilities for Single Sign-On, although not all of them provide the same level of service. Some of these are as follows:

- External security product compliant with the SNC interface
- Use of central administration
- Trusted systems
- Microsoft Windows security provider
- Cookies
- Client certificates (X.509)

- Integration with LDAP servers
- SAP logon tickets

You can find extensive information on Single Sign-On solution on the security page of the SAP Service Marketplace (http://service.sap.com/security) and in the online documentation, as well as a set of SAP Notes.

LDAP

LDAP is the abbreviation of **L**ightweight **D**irectory **A**ccess **P**rotocol. A directory access protocol provides defined criteria to search, read, or write within a directory. Known for a long time (e.g., Novel Directory Services NDS, Netscape Directory Server) directories are having a comeback with the introduction of PKIs that require a LDAP server to store users and certificates and have them accessible for search and verification requests. Microsoft introduced LDAP functionality with Windows 2000 and its ability to use Active Directory Services.

Originating from the OSI Directory Access Protocol (DAP) introduced to the Internet community in August 1991, the X.500 Lightweight Directory Access Protocol is specified in RFC1777 from March 1995 as a read-only access protocol to the X.500 protocol suite (LDAP v2). The lightweight is derived from the fact that this directory access protocol provides read-only access to the main topics, variables, or features using TCP or other transport. This means that not all accessible values are represented using LDAP and that the corresponding layer is the transport layer bypassing much of the session/presentation overhead required for DAP. An update of LDAP can be found in RFC2251 from December 1997, which specifies LDAP v3 that has, in addition to other enhancements, writing capabilities within the directory.

Secure Socket Layer Protocol (SSL)

HTTP is the default protocol for transferring files on the World Wide Web. HTTP transports Web sites as plain-text files. So it is possible that a third party having access to the network can read or alter the data sent. The protocol has no proper mechanisms to ensure authentication and confidentiality for the data. For that purpose SSL encryption can be used. The HTTPS protocol transfers HTTP over an SSL connection. HTTPS offers options to encrypt the data and to identify the other party by its digital certificate.

SSL/HTTPS provides confidentiality and integrity of the data transmitted and authentication of the user.

- Confidentiality is ensured through strong encryption. So the information transmitted cannot be decrypted by anyone else and the intended recipient and is unreadable to third parties.
- Data integrity ensures that a third party did not alter data sent through the network.
- Authentication is provided through digital certificates that are very difficult to falsify.

When an HTTPS communication is set up, client and server first agree on a protocol version and define the encryption algorithms. Then they authenticate each other and use encryption techniques to generate the session information.

The following sections provide an overview over the steps required to set up a HTTPS connection:

1. The client sends a request to the SSL-enabled server.
2. The server sends its public key and its certificate to the client.
3. The client checks if the certificate of the server was signed by a certificate authority whom the client trusts. Otherwise the client will abort the connection to the server.
4. The client compares the information from the certificate with those it just received about the server: domain name and public key. If the information matches, the client accepts the server as authenticated. At this point the server might request a certificate from the client as well.
5. The client creates a session key, encrypts it with the public key of the server, and sends it to the server.
6. The server receives the session key and encrypts it with its private key.
7. Client and server use the session key to encrypt and decrypt the data they send and receive.

SAP Security Infrastructure

As indicated previously, SAP systems security often is only seen as the implementation of the authorization/role concept. However, SAP solutions based on open, multitiered client/server and Web-based architecture include many components that can exchange or are used for exchanging data and information with other components, applications, or systems. Each of the elements needed for the communication and exchange of information is a layer of the SAP security infrastructure also known as a security service.

Security must be addressed at all these layers. Here is an introduction to each of them; these will be further covered in following sections:

- The presentation level is represented by all forms of front ends used for accessing SAP systems. This is typically the SAP GUI for Windows although other options are available, such as the SAP GUI for HTML, SAP Enterprise Portals, the SAP GUI Shortcuts, and other front ends that can be programmed with the SAP Automation and other utilities. At the presentation level the main security service is the *user authentification*.
- The application level includes the application logic that is run by the ABAP programs. The role-based and authorization concept is the main security service located at this level.
- The SAP databases are the containers of all the business information as well as the metadata, data models, and object repository. SAP databases must be protected against unauthorized accesses, which can come from direct or remote accesses. It is very important to recognize and protect the most critical system tables. This is the level of data access protection.
- The network is the de facto backbone of computing, and there is no business or collaborative application that can work without it. SAP solutions and systems are a

complex set of networked servers and applications both inside and outside the companies and as such the network is the enabler that must be protected. Since SAP R/3 release 3.1G the system includes the SNC interface that can be complemented with third-party security products to further enhance and protect the SAP network communications. The network is located at the access security level.

- Remote communications. The natural openness of the SAP systems and the endless possibilities of communicating and exchanging data between them and other systems require a security analysis from the point of view of external or remote communications mainly on the areas of the RFC and CPIC protocols, which are used in other interfacing techniques such as the BAPIs.
- Internet. The Internet represents the biggest opportunity and natural marketplace for e-business and at the same time the riskiest place if security measures are not in place. More and more SAP solutions are extensively based on Web technology and they are Internet enabled. Internet security is very extensive and would require a book on its own. In case of SAP systems care, must be taken to use firewalls; protect ITS, SAP WAS, or SAP Enterprise Portal servers; and use SNC and other cryptographic technologies.
- Operating system. SAP solutions include naturally a large collection of software applications. Access protection to SAP files and directories as well as the operating system commands must be also be in place.

Security must also address the overall system landscape: development system, quality assurance system, productive system, and any connected complementary system whether belonging to the SAP Business Framework architecture or not. Security also implies the Change and Transport System.

All security aspects on SAP systems components are based on restricting the access to each of the system's layers to authorized users or authorized external systems only.

A security infrastructure must also include all the logging and auditing possibilities because these mechanisms are required for monitoring and enforcing the security policy.

What Type of Security Is Standard on SAP Systems?

SAP NetWeaver and the mySAP Business Suite systems include many security features, the majority of which are not often applied in most customer's installations. On one hand, it is easy to think that in order to reach SAP systems you must first leak into the network, the operating system, or the database. And whereas somehow this is true it is also true that if internal threats are considered, then standard security measures will certainly not be enough.

The SAP Basis Middleware (R/3) as well as the SAP Web Application Server includes basic and generic security measures based mostly on passwords for user authentication as well as the authorization concept for user access to business data and transactions. SAP Basis comes with other powerful security features, such as support for Secure Network Communications (SNC), Secure Store and Forward (SSF), and digital signatures and allows the use of external security products, Single Sign-On solutions, smart cards, and many other options to suit the needs of the most exigent businesses and chief security officers.

How Can SAP Security Be Improved?

If you understand the security components and infrastructure, there is a lot you can do to improve SAP systems security without compromising normal users' operation.

You can improve security by

- Designing and implementing a secure systems infrastructure by means of firewalls and setting password policies and parameters
- Setting the most appropriate values for security-related instance profile parameters
- Using external security products
- Establishing a security policy and efficiently communicating it
- Creating a security checklist that can be periodically tested either manually or automatically so you can evaluate the efficiency of your security policy
- Enforcing the security policy by means of logging and auditing
- Monitoring security alerts and locating threats
- Establishing a procedure for constant update of the security policies

The Multilayer SAP Security Infrastructure

Layers of the SAP security infrastructure must interoperate to form a cohesive security strategy. This interoperation cannot happen unless you understand what each layer is supposed to do. We explore these functions in the following sections.

Security at the Presentation Level

Presentation-level security addresses all forms of front ends used for accessing SAP systems. This is typically the SAP GUI, though other options are available, such as the SAP GUI for HTML, SAP GUI for Java, the SAP GUI shortcuts, the SAP Enterprise Portal, and other front ends or logon programs that can be programmed with SAP Automation and other utilities. The primary security service at the presentation level is User Authentication. When security fails at this level it is typically because

- The security policy is weak, not well communicated or enforced, or not existing at all.
- The profile parameters that enforce basic security measures are not set.
- You have not changed the passwords of standard users.
- Basic protection measures at the workstation are not taken.
- You have not implemented advanced security methods such as SNC, Single Sign-On, client certificates that allows encryption, or smart login devices.
- Security auditing and monitoring is scarce.

As a result you see unauthorized users logging in with privileged user accounts, many unsuccessful logon attempts, or users using other persons' accounts.

Once I was starting a security analysis for a customer and he gave me access to a PC. I asked him for a username and password to enter the SAP systems (they had many systems) and he went out a few minutes to ask someone else for a username. When he came back I had successfully logged into every SAP system using the well-known privileged user and password. I said, "What SAP instance do you want me to stop?"

It is mainly the job of the Basis administrators and User administrators together with the IT department and the security manager to define a clear authentication policy, to set in place all the standard SAP security measures, and if needed to add any advanced measures to protect the system at the presentation level.

Application-Level Security

Security at this level addresses the application logic that is run by the ABAP programs. Here the main security service is the User Authorization concept, which grants or denies access to business objects and transactions based upon a user's authorization profiles. When security fails at this level it is typically because

- The authorization system has been poorly implemented.
- Critical authorizations have not been defined.
- Local development did not include appropriate authority checks.
- Administration of authorizations and profiles are not properly distributed and protected.
- The user and authorization information system is rarely used.

As a result you see unintentional transaction executions by unauthorized users, performance problems, display or modification of confidential information by unauthorized users, or even deletion of important data.

Several times it happened to me that a user that was not supposed to have such an authorization had unintentionally deleted or changed parts of the number range table (NRIV) and due to the legal implications of this we had to make a point-in-time recovery of the whole system.

It is the Application administrators' job to define which users have access to what data and transactions. These definitions must later be technically implemented by the User and Authorization administrators. It is also very important that every developer follows a programming methodology that includes security checks.

Security at the Database Level

The SAP systems databases are the container for all the business information as well as the metadata, data models, and object repository. These databases must be protected against unauthorized accesses. At this level security services must grant access protection to SAP systems data. When security fails at this level it is typically because

- Standard passwords have not been changed.
- Access to the operating system is not properly protected.
- Remote access to the database is not secure.
- Auditing has not been activated on critical tables.
- The authorization system at SAP level is poorly implemented.

As a result you see modifications at the database level that compromise systems integrity and consistency, uncontrolled access to confidential information below the application level, or systems unavailability.

In one of my customer installations the operator (who additionally did not understand very good English) started a tablespace reorganization instead of adding a new data file to a tablespace. The system was stopped for some hours.

It is the job of the Database administrators together with the OS system managers and the Basis administrators to take appropriate security measures at this level. Some of the measures are changing the passwords of privileged DB users, protecting SAPDBA with expert mode, restricting external remote access to read-only mode, auditing critical tables, setting correctly the S_TABU_DIS authorization object.

Operating System–Level Security

Security services must guarantee access protection to SAP files and directories as well as the operating system commands and programs. At this level security services are provided by the operating system features themselves. When security fails at this level it is typically because

- Permissions on files and directories are not properly set.
- The password and user policy at the OS level is static and widely known.
- Logging and monitoring is scarce.

As a result you see deletion of important system and application files, software malfunctions, or system unavailability.

I have seen a system operator deleting critical system files like the database files by mistake that were fully unprotected. A restore and recovery was necessary in order to have the system up and running again.

It is the job of the Operating System manager to implement security measures at the operating system and to monitor the main log files of the audit system. Measures include implementing a security password policy at user level, taking care not to create unnecessary users or services, monitoring SETUID programs, setting ACLs (Access Control Lists) in critical files and directories, and protecting external commands from being executed from SAP.

Network-Level Security

Networks are the de facto backbones of computing. There is no business or collaborative application that can work without one. SAP systems based on a client/server architecture are no exception. With release 3.1G SAP Basis (R/3), SAP systems included the SNC interface (Secure Network Connections), which can and in most cases should be complemented with third-party security products to further protect network communications. When security fails at this level it is typically because

- There are too many unprotected network services.
- Network topology is poorly designed.
- There is little or no network monitoring.

- Routers, filters, or firewalls are not correctly configured.
- SAP router configuration is not properly set.
- There is no automatic intrusion detection system.
- Data are not traveling in encrypted form.

As a result you see users or programs trying to log on to unauthorized systems like hackers, users logging on to the wrong servers, unbalanced system loads, or even sniffing.

One example of security violations in the network environment is when end users log on directly to the database server when this has an administrative instance. Another one I have seen many times is when the *rlogin* service is completely unprotected and users have logged on through the network and stopped the wrong servers.

It is the Network administrators' responsibility to design and implement a security network topology that takes into consideration an automatic monitoring and intrusion detection system.

Transport System–Level Security

SAP has provided the TMS (Transport Management System) as an environment for coordinated customizing and team development that protects the modification of objects and settings across a SAP landscape. Unfortunately the TMS is a facet of the SAP enterprise that is often undersecured.

When security fails at this level it is typically because

- System landscape settings are not properly configured.
- Repairs are freely allowed.
- There are no filters that control which objects are being transported.
- Authorizations are not completely implemented.
- Transport monitoring is not a periodic task.

As a result you see software failures, transport of copied programs without security checks, or problems when upgrading your system.

It is the task of the Basis administrator together with users in charge of customizing and developers to properly set the system to basic security standards and to define a security policy that makes sure that there is some type of filtering and monitoring within the transport system.

Secure Network Communications (SNC)

SAP's standard Secure Network Communications provides protection for the communication links between the distributed components of a SAP system. SNC is built on the SAP WAS kernel based on standard GSS API V2 and allows you to increase the level of your SAP security via external security products (e.g., Single Sign-On, smart-card authentication, and encrypted communications). SNC can raise your system to high security standards because it can cover several layers such as the presentation (authentication and Single Sign-On) layer, the remote communications layer, the network layer, and even the Internet layer.

Remote Communications–Level Security

The natural openness of the SAP systems and the endless possibilities of communicating with and exchanging data between SAP and other systems require stringent security analysis from the point of view of external or remote communications mainly in the areas of the RFC and CPIC protocols, which are used in other interfacing techniques such as ALE or BAPIs.

When security fails at this level it is typically because

- The authorization system is poorly implemented for remote communications.
- RFC communications include the passwords in their definitions.
- There is scarce monitoring at the gateways.
- OS and network security is also weak.
- No encryption software has been used.

As a result you see unexpected connections or program executions from other systems, software failures, or access to confidential information.

It is the job of Basis administrators together with Network administrators and developers to implement standard security measures to avoid leaving holes at the remote communication level.

Some standard measures are as follows: do not create more RFC destinations than those necessary, include AUTHORITY-CHECK within the programs that can be remotely called, protect table RFCDES, use standard interface techniques, provide periodic monitoring of the gateway server, and ensure that the *secinfo* file exits.

Document Transfer–Level Security

SAP security services must guarantee the integrity, confidentiality, and authenticity of any type of business documents such as electronic files, mail messages, and others. At this level SAP provides Secure Store and Forward (SSF) mechanisms, which include digital signatures and digital envelopes based on public key technology. And these mechanisms can be deployed using external security services like digital certificates and digital envelopes.

When security fails at this level it is typically because

- Certificates and encryption are not used/implemented.
- Private keys are not properly protected.
- There is scarce tracing and monitoring.

As a result you see documents intercepted by unauthorized persons or access to confidential information.

It is the job of the Basis administrators and expert security consultants with the help of the legal department to define and implement secure mechanisms like encryption methods for protecting the secure transfer of documents.

Introduction to SSF (Secure Store and Forward)

SAP's standard Secure Store and Forward provides the required support to protect SAP systems data and documents as independent data units. You can use the SSF functions to "wrap" SAP systems data in secure formats before the data are transmitted over insecure communications links. These secure formats are based on public and private keys using cryptographic algorithms.

While SAP provides a Security Library (SAPSECULIB) as a software solution for digital signatures as well as standard support for SSF in certain application modules such as PDM or ArchiveLink, a high degree of protection is achieved only when private keys are secured using hardware devices such as smart cards.

Despite the fact that the communication infrastructure might be well protected, it is also necessary to protect the private keys that are used in digital signatures and envelopes because if this information is intercepted, the cryptographical strategy will be useless.

This includes SAP components such as the application servers when these act as the senders of the messages and therefore hold the private keys.

In addition to the risk that exists in case the private key falls into the wrong hands, it must also be considered that criminals can be interested in sabotaging the communications and could modify the public keys repository for the partners with whom the company system communicates.

Protecting Private Keys

There are two main ways for storing and protecting private keys:

- *Via hardware.* The best solution for protecting SAP users' private keys is the use of an individual smart card for every user. With this there is no way to reveal the private key that the smart card holds. Additionally users must be identified in their smart cards using biometric means (such as a fingerprint, the eyeprint, etc.) or by the use of a secret number such as a PIN, a password, a question that only the user knows, and so on. Users are responsible for securing their cards.

  If this method of protecting private keys is selected, companies should develop a communication campaign so that users are informed of the importance of not sharing or letting others use their smart cards.

  From the point of view of the server and in order to improve performance, the recommendation is the use of a crypto box instead of a smart card.
- *Via software.* The software solution is not as safe as when specific hardware is used. If a file holding the keys is used, then it is very important to protect this file from unauthorized accesses.

Protecting Public Keys

If the security products use an address book for holding the public keys just in the case of the private keys, then the files must be protected from unauthorized access or modifications.

An alternative is to use certificates that are issued by a trusted Certification Authority (CA) to grant the authenticity of those certificates.

There are several countries that have regulated the use of cryptography and digital signatures. However, these rules or laws frequently generate a big amount of controversy and even change. Some countries already accept the digital signatures as a valid proof of obligation and therefore digital signatures can be used for secure business.

Internet-Level Security

A critical component is what I call the "Internet level," which addresses the interactions that take place between a SAP system and browsers, Web servers, SAP Web Application Server, ITS, SAP EP, firewalls, and so on.

When security fails at this level it is typically because

- Secure protocols are not properly set.
- Encryption and certificates are not used.
- Remote debugging of ITS is not disabled.
- Service files are not protected.
- Firewalls and authentication might not be properly configured.
- Security measures at Web servers are weak.
- Monitoring is scarce.

As a result you see many types of attacks on Web servers that might make systems unavailable or compromise critical information.

There are thousands of Internet security incidents and break-ins reported; some of them make the CNN headlines. There are dozens of books and hundreds of Web sites covering security, hacking, and protection software. You could start at http://www.securitynews.org.

It is the job of the Basis administrator, Network administrator, and Web administrator to set in place a system design for implementing the best security measures that protect against attacks to the SAP systems that are tightly connected to the Internet.

A comprehensive security strategy limits access at each of these security layers to only authorized users and/or authorized external systems. It also accounts for the overall *system landscape*: development systems, quality assurance system, productive system, and the transport system that operates between them as well as any connected complementary systems whether they belong to the SAP NetWeaver infrastructure architecture or not. You want to be sure that certain protective procedures are set in place to guard against insecure programs or Trojan horses that may travel from one system to another.

Logging and Auditing

Last but not least, a security infrastructure must include robust *logging and auditing* capabilities; the mechanisms you will need to monitor and enforce your security policies. Logging and monitoring address the efficiency of the security measures and the capacities of the system for detecting weaknesses, vulnerabilities, and any other security problem. There are logging and auditing facilities in the SAP security infrastructure at every level. These facilities are implemented mainly in the Security Audit Log, the Audit Info System (AIS), the security alerts within CCMS, and the Users and Authorization Info System (SUIM). These tools are complemented by other logging facilities such as those available at operating system level, database auditing statements, network and Internet monitoring and management, and others.

The difficulty for monitoring the whole SAP security infrastructure is that there is no single tool for doing that automatically although the evolution of the CCMS and the AIS tools make us think that it might happen.

You can find extensive information and checklists for auditing security in the diverse SAP Security Guides at the SAP Service Marketplace (http://service.sap.com/security).

SAP Trust Center Services

The focus of the SAP Trust Center Service is to provide global one-step authentication and digital signature technology for enabling collaborative business scenarios. The trust infrastructure relies on already existing business relationships between SAP and its customers. The SAP Trust Center provides more trust than any other existing trust center because these do not typically rely on existing business relationships. This service provides a smooth migration from password-based authentication to certificate-based authentication.

The Trust Center Service works with the customer's internal Portal to distribute digital certificates—called SAP Passports—to individual users. The SAP Passport is based on the X.509 certificate standard and enables data to be encrypted and transmitted safely over intranets and open Internet connections. SAP customers using the Trust Center Services can be sure that only authorized partners and employees are accessing information and conducting business in Marketplaces.

If SAP users wish to apply for a SAP Passport when they log on to their Portal, their UID and password is used. The Portal Server transfers the user as well as the company's identity to the Web browser of the user. The Web browser then automatically generates an asymmetric public/private key pair. After receiving and verifying the certificate request containing the user's and the company's identity and the public key from the Web browser, the Portal Server approves the certificate request with its digital signature. The Web browser then sends the approved certificate request to the SAP Trust Center Service. The SAP Trust Center Service verifies the certificate request against the agreed naming convention. Then the Trust Center Service Certification Authority (CA) creates a X.509 certificate and transfers the certificate back to the Web browser. The SAP Passport is now ready for use.

Management of Users, Authorizations, and Roles

The users of the SAP systems are defined internally within the same SAP systems and there is no need for user management at the operating system or database level, except for those special users defined in the standard installations, such as <sid>adm, SAPServices<adm>, ora<dbsid>, or others, depending on the operating system and database platform.

The users are defined and maintained, and the security of the system is enforced in the user master records with the use of the SAP authorizations and role concept.

The following sections deal with the general management of user master records and the most important available fields and options, just on the SAP Web Application Server with the ABAP engine.

But the main concern for system administrators and project managers when implementing the SAP solutions is how to enforce the right security methods for users' access to the business information. As we have seen in the first part of this chapter, the SAP system provides a comprehensive and flexible way to protect data and transactions against unauthorized use.

In the user master records, users are assigned one or more *roles* and *authorization profiles*. These authorization profiles are made of a set of *authorizations*, which give access privileges for the different elements of the system. Further down, authorizations refer to *authorization objects*, which contain a range of permitted values for different system or business entities within SAP systems.

Managing roles, profiles, and authorizations is a complex and time-consuming task within SAP implementation projects and later maintenance and support. SAP has designed a tool that reduces the time needed for implementing and managing the authorizations, thus decreasing the implementation costs. This tool is known as the *Role Maintenance* based on the classical *Profile Generator*. The Profile Generator is a SAP utility available since release 3.0F of the R/3 Basis kernel, with the goal of making easier the configuration and management of authorizations, profiles, and roles. It can be used for automatically creating roles, authorizations, and profiles and assigning them easily to users. The definition of profiles using the Profile Generator is based on the possibility of grouping functions by *roles* (known as *activity groups* in releases of SAP Basis before 4.6C) in a company menu. This menu will be generated using customizing settings and will only include those functions selected by the customers. *Roles* form a set of tasks or activities that can be performed in the system, such as running programs, transactions, and other functions that generally represent a job description or job role.

In the following sections, all the concepts are introduced with some practical examples dealing with the process of granting access rights and protecting the system elements. A final section of the chapter covers the topic of organizing the user master record management from the point of view of tasks involved in granting access rights to the users.

Overview of User Administration

As a SAP administrator or support personnel, user handling should not be of major concern if certain rules and guidelines are followed from the beginning of the project. This, however, does not apply to authorization and role maintenance, which are matters of joint projects and efforts between the SAP functional and technical people. The reason is that usually SAP system managers do not have to deal with such things as granting access to certain users for specific general ledger accounts, cost centers, or production plants. It is the role of the customization specialists, developers, or business consultants to define entities that should be protected by means of authorization objects and to assign or create the corresponding roles or profiles.

This task is really important, and it might become a puzzle that can take a lot of time to solve, depending on the degree of security protection desired and the number of users and modules being implemented.

The easy part of user administration deals with such things as creating user master records, changing passwords, helping users define their own default values, and organizing the user maintenance tasks.

Managing User Master Records

Similar to the rest of the SAP systems based on the SAP WAS for ABAP, where there is a material master, a vendor master, and so on, the user administrative and management functions also have a user master. The *user master records* define the user accounts for enabling access to the system. They contain other screens with additional fields apart from the user ID, some of which are just for information purposes (but are nevertheless important) and others that can make life easier for both users and administrators.

The user master records contain all the access information needed by the system to validate a user logon and assign users access rights to the system, such as passwords, roles, and authorization profiles.

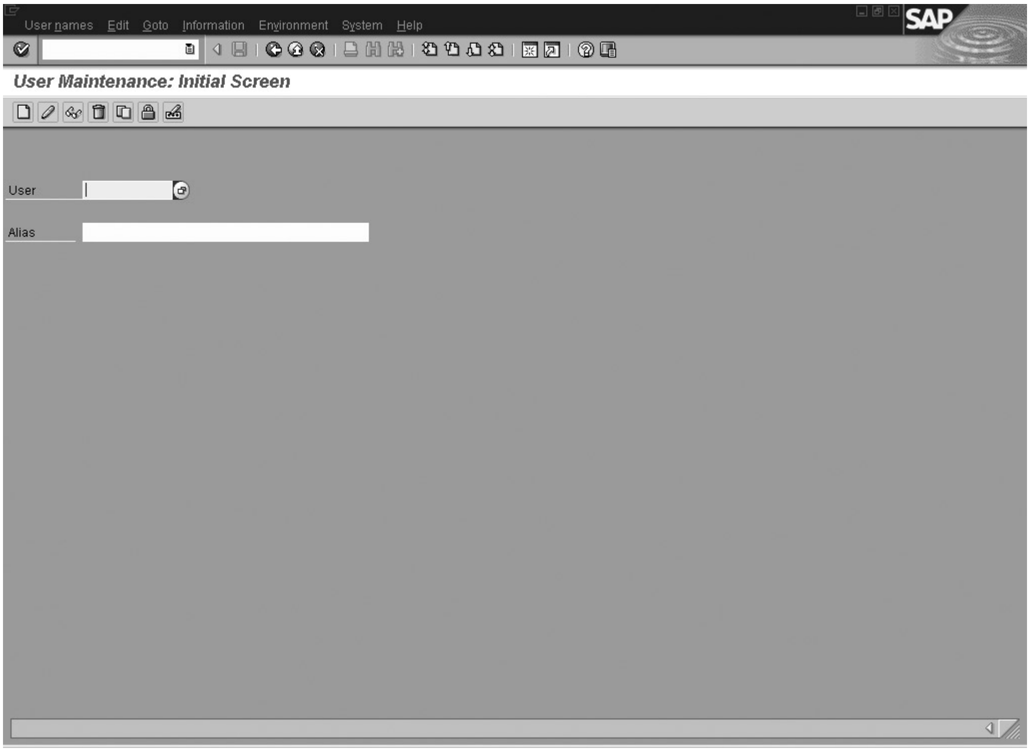
There is a lot of extra information in a user master record, including which start menu the users will see when they first log on, what printer is assigned by default, and the addresses and phone numbers of users. Some of the fields are just for information purposes, whereas others have a direct effect on the working environment for the users.

To reach the user maintenance functions via menu options, from the SAP Easy Access menu select Tools | Administration | User Maintenance | Users, or type the transaction code SU01 in the command field. Figure 8-1 shows the user maintenance initial screen.

This screen shows the input field for specifying an individual user for which to perform administrative actions.

To find a particular user when you don't know the proper user ID, you can select the possible entries list arrow and then click on the List icon on the dialog box.

To perform functions over a group of users, the system includes some options under the menu Environment | Mass Changes. This is introduced in a later section.



User Maintenance: Initial Screen

User

Alias

FIGURE 8-1 Initial screen for user management (Copyright by SAP AG)

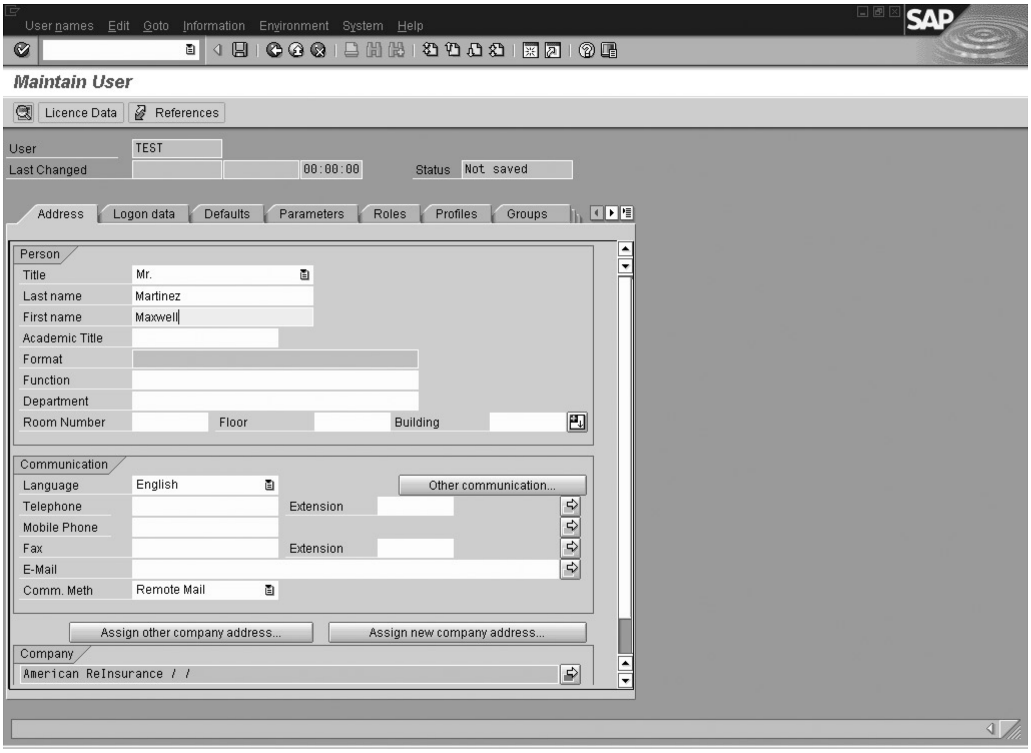
Creating Users

From the User Maintenance initial screen, as shown in Figure 8-1 there are many options available. Normally, the input field for the user field is empty, except if you have been working in other user management functions previously in the same session.

User master records are client dependent, which means that they are separately defined for each client in the SAP system. For example, if user *FREDSMITH* is defined on client 003, but not on client 005, he won't be able to log on in client 005.

To create a user master record you have two options: either define it completely from scratch or copy it from another user or from a reference user you had previously defined. The next list explains both methods.

- *Creating new users from scratch.* From the User Maintenance menu, enter the name for the new user and click on the Create icon, or with the right mouse button select the F8 function key, or select User Names | Create from the menu bar. Figure 8-2 shows a screen similar to the one you will get. The system displays the different sections of the user master records within the different tabstrips. You might get additional tabstrips if you have security interfaces installed, such as with an SNC compatible product.



Maintain User

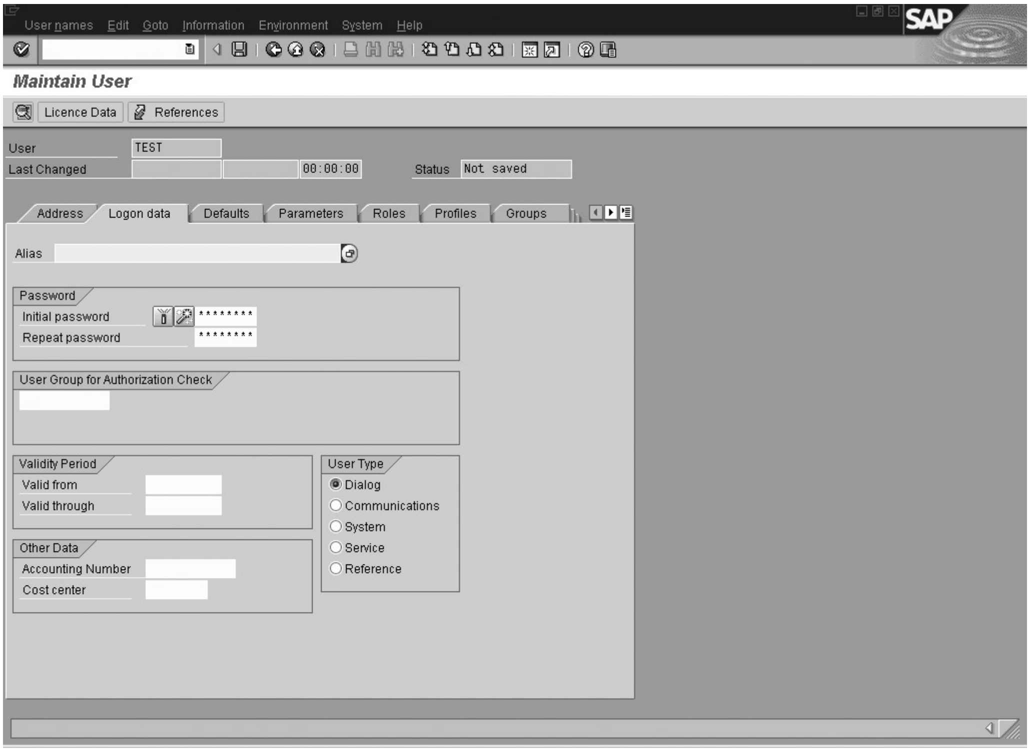
User TEST
Last Changed 00:00:00
Status Not saved

Person
Title Mr.
Last name Martinez
First name Maxwell
Academic Title
Format
Function
Department
Room Number Floor Building

Communication
Language English
Telephone Extension
Mobile Phone
Fax Extension
E-Mail
Comm. Meth Remote Mail

Company
American ReInsurance / /

FIGURE 8-2 Creating users from scratch (Copyright by SAP AG)



User TEST
Last Changed 00:00:00
Status Not saved

Alias

Password
Initial password ********
Repeat password ********

User Group for Authorization Check

Validity Period
Valid from
Valid through

Other Data
Accounting Number
Cost center

User Type
● Dialog
○ Communications
○ System
○ Service
○ Reference

FIGURE 8-3 Logon data (Copyright by SAP AG)

The first data the system displays corresponds to the Address information. Here the Last Name is a mandatory field that must be completed to go to other sections. You can move back and forth between tabstrips by clicking on them. However, any mandatory fields on these tabstrips must be completed before you can move to another section.

The most important mandatory field is the password, located under the Logon Data tabstrip, as shown in Figure 8-3. Enter or generate a password in the Initial Password field and retype it in the second field (verification field). Also you can optionally enter the user group for authorization check, or select it from the list of available groups by clicking on the possible list entries arrow.

Users themselves can maintain information corresponding to Address, Defaults, and Parameters by selecting System | User Profile | Own Data if they have the required authorizations.

When mandatory fields are completed, you can save the user by clicking on the Save icon. It is important, however, to assign at least some authorization profiles or role to the users; otherwise they won't be able to perform any task.

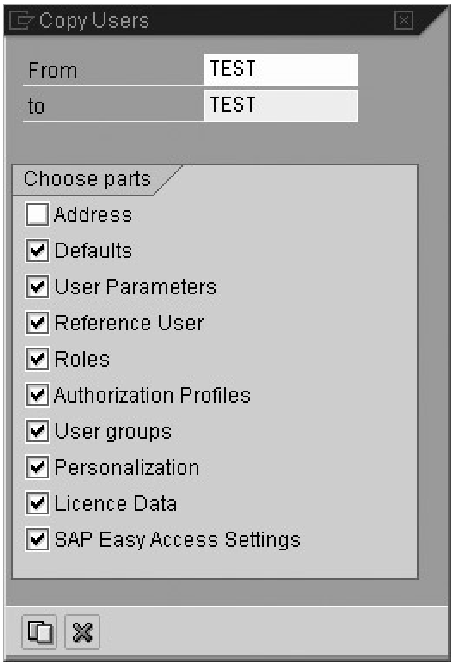
After a user has been created, any modification to the user master fields is performed by entering the user ID in the User input field of the initial User Maintenance screen and clicking on the Change icon on the application toolbar.

- *Copying users from reference master records.* Instead of defining the SAP users one by one from scratch, it is usually better to define some template user master records and to create new users by copying these templates and changing only some of the fields. Doing it this way reduces the time needed to create users, especially at the beginning of the system life. These models or reference users can be regular SAP system users. For example, suppose your company is implementing a SAP R/3 Enterprise for managing the sales and distribution, the materials management, and the finances. Possibly there will be users who just take orders in the system, others doing accounting work, and others with different tasks. In these cases, you can create a reference user for the sales module and use that user master record as a reference for creating the rest. The same process can be done for the users of other modules.

  To create a new user by copying from a reference user, from the initial user maintenance screen, enter the name of the new user in the input field and press the Copy function button from the application toolbar. The system displays a dialog box similar to the one shown in Figure 8-4.

  As you can see from Figure 8-4, you can decide what parts of the user master record to copy. You might want to copy just the profiles or just the address, in case you want to reuse any of the company address, or even just the defaults. In any case, you will have to specify a new password for the new user. The other values for the following screens can be modified just as if you were creating a new user. To modify any input field value, just write over the field while in Overwrite mode.

FIGURE 8-4 Dialog box for copying users (Copyright by SAP AG)



From TEST
to TEST

Choose parts

□ Address
☑ Defaults
☑ User Parameters
☑ Reference User
☑ Roles
☑ Authorization Profiles
☑ User groups
☑ Personalization
☑ Licence Data
☑ SAP Easy Access Settings

User Master Records Fields

Whether you are creating or modifying user master records, the SAP system screens for the user maintenance transaction show several input fields.

There are many, and some of the most important fields are the following:

- *Initial password.* The password for the first logon with the user ID. The password must be entered twice in a verification field, to make sure there were no typing errors. The next section explains password management from the point of view of the administrator. For an introduction and guide for users, refer to the section on password rules in Chapter 5.
- *User group.* Located under the Groups tabstrip, the name of the user master record groups to which this user can be assigned. This is a useful field for dividing user maintenance among groups or for performing changes on all users belonging to a group. For example, you can create user administrator master records in charge of a particular group but not of others. Before you can assign a group, it must have been created first.
- *User type.* Located on the Logon Data tabstrip, there are five user types available, each of which provides special access privileges depending on the type of processing. The normal interactive or ordinary user must be of type *Dialog*, which is the default. Other types of users are
  - *System*, which provides access privileges for processing background jobs and for internal RFC calls.
  - *Communication*, which is used for communication between systems not requiring dialog, such as ALE, RFC, or the TMS.
  - *Service*, a very special type of user, which can be assigned to a large group of anonymous users, which allows multiple logons.
  - *Reference*, which is an additional user type for assigning additional and identical authorizations to users. No online access to the system is allowed with this type of users. A user can only be assigned to a user type.
- *Validity period.* In this optional field, administrators can enter a period of time in which the user ID is valid. Although this field is often left empty, it can be very useful within a security policy, especially when setting accounts for occasional users such as external consultants or business partners.
- *Other data: accounting number.* You can enter in this optional field any name or number you want to assign to a user as his or her user account. It can be unique for each user or can be shared by a group of users. This field is useful when working with the SAP user accounting system, which performs statistics of the usage of the system. If you want to get individual usage statistics, you could enter the same user ID name into this field. For group statistics, a possibility is to enter the cost center, the department name, and so forth. If you leave it blank, the accounting statistics for the user will be assigned to a collective *No account* category.
- *Roles.* In the roles tab page, you can enter any number of predefined roles, which is one collective way of assigning specific authorizations to users for accessing SAP systems. Formerly this was known as *task profile*.

- *Profiles.* A profile gives the user the permission to access specific system functions. *Profiles* are made of a group of authorizations and authorization objects. Profiles can be simple or composite. Composite profiles are groups of profiles (either simple or composite).

SAP systems include a large number of predefined roles and profiles matching most common user needs for the different SAP application modules and also for the development and system management functions. To get the list of predefined roles you can click on the possible entries arrow of the input field for profile. Looking for specific predefined profiles can be done by either looking in the application documentation or by searching the implementation guide (IMG). There are other ways to search for profiles by tracing authorizations and then using the authorization information system.

The system provides facilities for creating your own roles and profiles, using the Role Maintenance and the Profile Generator, when the predefined profiles or roles are not enough.

Available Defaults and Options for User Master Records

After the first initial screen for user maintenance, the system provides additional screens for entering other user information. You can set, for example, the default printer for a user, the user's address, and values for user field defaults (parameters). The three available screens are Address, Defaults, and Parameters. These subscreens are accessed by clicking on the corresponding tabstrip within the User Maintenance screen.

Users can set their own values and defaults by themselves in the System | User Profile | Own Data menu. The following sections show the available options that can be set by users.

Specifying User Address

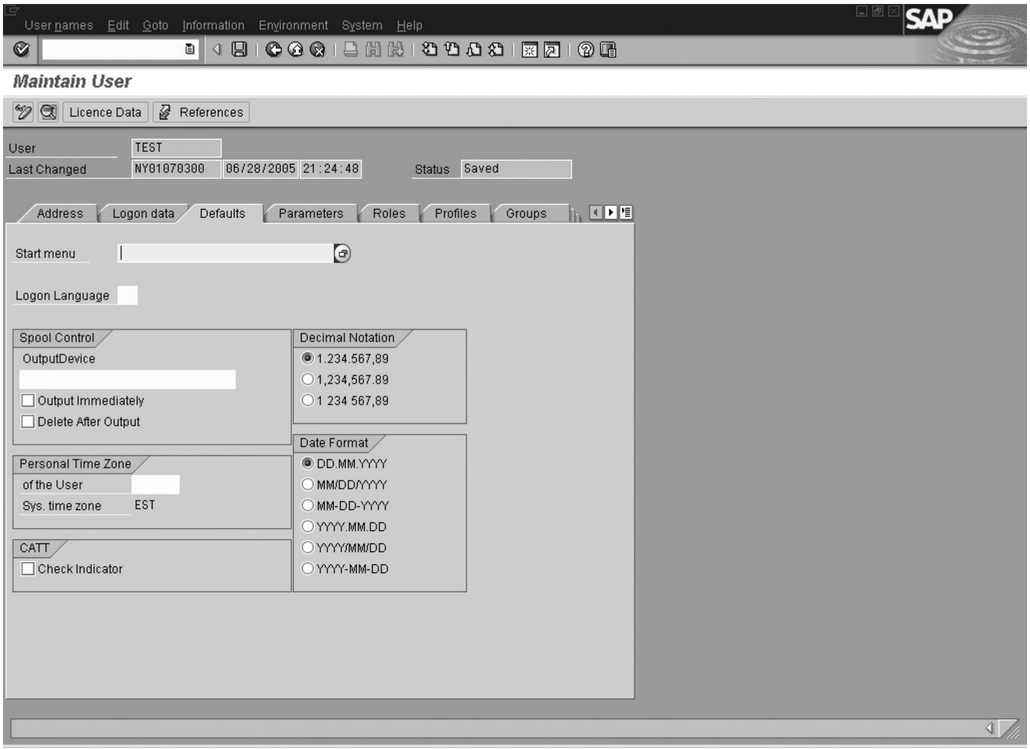
The information in user addresses is only used by the SAP system for documentation purposes. It can be very useful, however, for system administrators when trying to locate a user by her or his name, phone number, and so on. Often companies assign user IDs using letters and numbers which are coded so that it is easier to locate or assign user IDs to system users. The address data for a user includes three main information boxes, corresponding to *Person*, *Communication*, and *Company*. Some of the most important fields in those boxes are as follows:

- *Last Name.* In this field you must enter the surname of the user. This is a mandatory field that has an additional use when using the SAP Business Workplace.
- *Telephone No., Fax, and E-mail.* These fields can be used for entering the phone number, fax number, and e-mail address, which are important, especially the fax and the e-mail, when connecting the SAP systems with external fax systems or Internet e-mail.
- *Company.* You can also enter and maintain the company information for users.

Setting User Default Values

Administrators or users by themselves can set some fixed or default values for some common functions or input fields that they find often while working in SAP systems. Figure 8-5 shows an example of this screen. Here, you can set the following:

- *Start menu.* You can set the name of the menu or the transaction, which will be started automatically when a user logs on.



User TEST
Last Changed NY01070300 06/28/2005 21:24:48 Status Saved

Start menu

Logon Language

Spool Control
OutputDevice
☐ Output Immediately
☐ Delete After Output

Personal Time Zone
of the User
Sys. time zone EST

CATT
☐ Check Indicator

Decimal Notation
● 1.234.567,89
○ 1,234,567.89
○ 1 234 567,89

Date Format
● DD.MM.YYYY
○ MM/DD/YYYY
○ MM-DD-YYYY
○ YYYY.MM.DD
○ YYYY/MM/DD
○ YYYY-MM-DD

FIGURE 8-5 Maintaining user default values (Copyright by SAP AG)

- *Logon language.* Setting this field for a user will overwrite the system default when the user logs on. If the language field for the initial logon window of the SAP system is empty, the language specified in this field is used.
- *The default printer for a user.* This is assigned in the Output Device field. You can click on the possible entries arrow to display a list of printers.
- *The output controller check boxes.* These are particularly important for handling user print requests. Check the box next to Print immediately to have a print job sent directly to the printer; otherwise, it will just send it to the output controller where users can print it later. Setting the box next to Delete after output tells the system to delete the job from the spool database after it has been printed.
- *The format for date and decimal points.* The last check box, CATT, is used for special test functions within the computer-aided test tool provided in the SAP system. For information on CATT, look it up in the SAP online documentation.

Setting User Default Values for Parameters

The parameters that can be set on this screen match some fields of the SAP systems. Setting default values using these parameters offers the advantage that every time a user is presented with a screen containing any of those fields, the value is automatically entered in the input field.

This concept is explained in Chapter 5. Remember that at any time users can overwrite those values or change the parameter values by selecting System | User Profile | Own Data.

The parameter screen has two fields:

- *Parameter ID* refers to the parameter ID, which you can find using the technical information for the field (remember: place your cursor on the field, press F1 and then Technical Info). You can also list the available parameters by clicking on the possible entries arrow next to the parameter input field.
- In the Value field, enter the value you want to assign as the default any time a SAP screen presents that field.

Managing User Groups

User groups within the SAP user maintenance functions basically serve as a way to divide administration tasks. To reach the user group screen, from the initial user maintenance, select Environment | User Groups and then you can either Maintain or Display them.

User groups are just assigned a name. So the only two basic functions to perform are either *create* a group or *delete* a group. To create or delete a group, position the cursor over the group name and click on the corresponding function button.

Clients 000 and 001 include a special privilege group, SUPER, which is normally assigned to superusers SAP* and DDIC. To delete the group SUPER, users need special authorization.

Modifying User Master Records

Changes to user master records can be performed by the system administrator with the corresponding authorization or by the users themselves to their own address, defaults, or parameters values. Normal privileged users cannot change, for example, their roles or authorization profiles. They can do that only if they have additional access rights to perform that operation.

The modifications made to a user master record (like a password, a locking, a time period validity, etc.) are only effective the next time a user logs on. Current logged-on users are not affected by those changes. But administrators can make some changes to the users' access permission by modifying and then activating authorizations and profiles.

Changes made to profiles are not effective until the users log on again; however, a modified and reactivated authorization has an immediate effect, even on logged-on users. So, for instance, if an authorization has been changed and then activated, it will immediately affect all users with profiles containing that authorization.

Deleting Users

To delete a single user master record, just enter it in the input box of the initial user maintenance screen and press DELETE on the application toolbar.

Locking and Unlocking Users

Administrators can temporarily set a lock in user master records that prevents a particular user from logging on to the SAP system. To lock a user, enter the user name in the input field and select the Lock/Unlock button on the application toolbar, or select User Names | Lock/Unlock from the main menu. Locking and unlocking functions work in a toggle fashion. A lock won't have an effect on users who are currently logged on.

The system also enters automatic locks in user master records after 12 consecutive unsuccessful logon attempts. The default value is 12, but administrators can change that by setting an instance profile parameter. Refer to the section on technical details at the end of this chapter.

A user who has been automatically locked out by the system because of unsuccessful logon attempts is also automatically unlocked by the system at midnight. However, a manual lock on a user master record will remain in place until you explicitly delete it.

Making Modifications to a Group of Users

The SAP system includes many functions to perform over a group of users. The options available are as follows:

- *Deleting, creating, locking, and unlocking several users from the current client.* From the initial User Maintenance screen, select Environment | Mass Changes. In the new screen you select users by using the possible entries list box, or by Address or Authorization criteria.
- *Modifying profiles or roles for all selected users.* To do this, select Environment | Mass Changes. First select the users in the Mass Change initial screen manually or by using criteria, and then click on the Change button on the application toolbar. You can not only modify profiles, but many other information for the group of users which can be applied to all of them at the same time, such as validity period, user type, defaults, and so on.

User Information System

The user maintenance functions of the SAP system include a comprehensive information system where you can look up, display, and analyze the users, profiles, or authorizations of the system. The system permits extensive navigation among the information: from users to profiles, from there to authorizations, and so on.

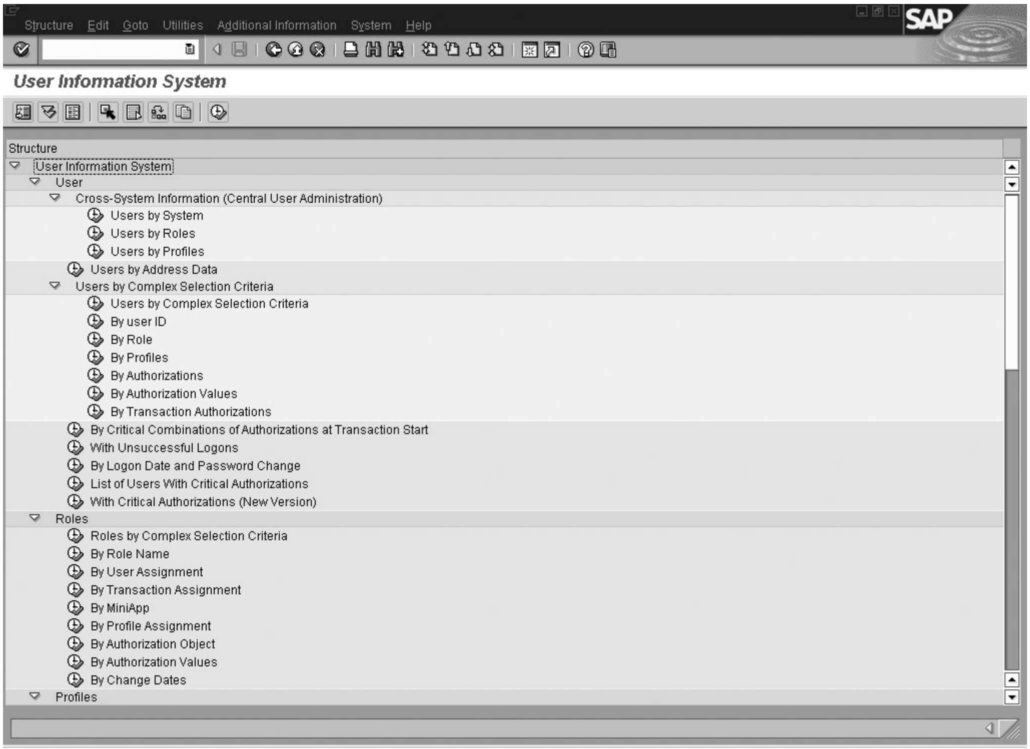
To reach the user and authorization information system, from the main user maintenance menu, select Information | Information System. The system displays a report tree corresponding to the authorization information system. These report trees contain several folders, each of which contains different reports. Figure 8-6 shows this report tree. By running different reports from the report tree folders, you can get a list of users, profiles, objects, authorizations, and so forth. The system presents several selection screens to permit searching for different criteria.

Another very useful report collection is the Change Documents folder reports, which can be used for displaying any modifications made to authorizations, users, or profiles and tells who did the modification.

Password Management

To change a password for a user, click the Change Password pushbutton on the application toolbar from the initial user maintenance screen. The system will display the New Password dialog box where you have to enter the password twice to verify that you didn't make any typing mistakes.

When system managers change the password for other users, the system requests these users to enter the new password when they log on. Administrators can change their



User Information System

Structure

- User Information System
  - User
    - Cross-System Information (Central User Administration)
      - Users by System
      - Users by Roles
      - Users by Profiles
    - Users by Address Data
    - Users by Complex Selection Criteria
      - Users by Complex Selection Criteria
      - By user ID
      - By Role
      - By Profiles
      - By Authorizations
      - By Authorization Values
      - By Transaction Authorizations
    - By Critical Combinations of Authorizations at Transaction Start
    - With Unsuccessful Logons
    - By Logon Date and Password Change
    - List of Users With Critical Authorizations
    - With Critical Authorizations (New Version)
  - Roles
    - Roles by Complex Selection Criteria
    - By Role Name
    - By User Assignment
    - By Transaction Assignment
    - By MiniApp
    - By Profile Assignment
    - By Authorization Object
    - By Authorization Values
    - By Change Dates
  - Profiles

Figure 8-6 Authorization info system report tree (Copyright by SAP AG)

passwords and other users' passwords as many times as they wish; however, normal privileged users can only change their passwords once a day.

By default and right from installation, there are some standard requirements concerning passwords. Some of the restrictions are set up in the system code and cannot be changed, while others can be changed as required by setting some instance profile parameters or by configuring system tables.

For example, system administrators might decide to set up a minimum password length or enter a character string as a nonpermitted password.

On the other hand, passwords are not case sensitive, so uppercase and lowercase passwords or a mix and match of both cases behave exactly the same.

Password Restrictions and Requirements

The passwords restrictions and requirements are as follows:

- The password cannot be the word *pass*.
- Minimum password length is set by default to three characters. Administrators can change this setting by specifying a greater value in the instance profile parameter

login/min_password_lng. If you change this parameter, be sure to do it in the common DEFAULT.PFL so that it has effect on every instance of the SAP system. Maximum password length is always set to eight characters.

- You can also specify the minimum number of digits, letters or special characters, by specifying a number value in the profile parameters *login/min_password_digits*, *login/min_password_letters*, or *login/min_password_specials*.
- The first character of a password cannot be an exclamation point (!) or a question mark (?).
- When a user changes his or her password, he or she may not use any of the last five passwords.
- Administrators can decide to forbid certain strings to be used as passwords. Users will receive an error message in the status bar when specifying a password that has been forbidden by the administrator. The process of forbidding passwords is explained later.
- A password cannot begin with three identical characters. For example, *aaamy* and *bbbyou* are invalid passwords.
- A user must change his or her password if there is an expiration date in the user master account and the date has arrived. System managers can decide how frequently the users must enter new passwords. To enforce password changes, set the instance profile parameter *login/password_expiration_time* with a value indicating the number of days after which a password must be changed. For example, if the profile parameter is set to 30, users will be requested to change their password every month. To leave the passwords without limit, the default value *0* is used for this parameter.

With the previous restrictions and other user master records rules, the process of logging on to SAP systems based on SAP WAS requires some more work for the system code to do besides checking the password. For instance, when a user tries to log on with a correct password, the system first checks whether the user is locked. If the user is locked either manually by the system manager or automatically after 12 unsuccessful logon attempts or by a system upgrade, the system displays an error message.

If the user is not locked, then the system checks whether the current password has expired. In this case, the system requests the user to enter a new password.

Restricting Password Strings

System administrators can forbid passwords or password strings by entering them in the table USR40. This is useful, for example, to avoid the use of passwords that start with similar words as the name of the company, the river that crosses nearby, and so forth. Table USR40 is maintained with standard table maintenance transactions such as SM30 (System | Services | Table Maintenance | Extended Table Maintenance).

To specify a nonpermitted password string, you can enter the typical wildcards, * and ?, where the * substitutes a group of characters, and the ?, a single character. Figure 8-7 shows an example of this table with some of the forbidden password strings. In this example, all passwords starting with the characters *SAP*, containing *R3*, or ending with *2005* are forbidden. This table is client independent and, therefore, the password restrictions are applied to any system client.

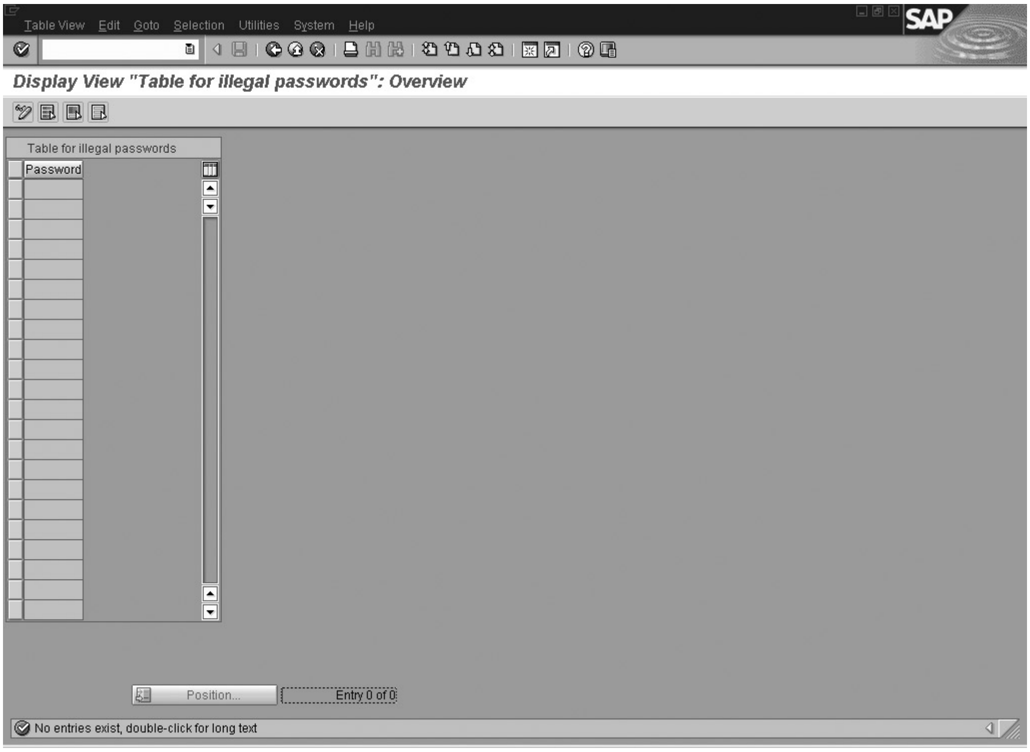


Table View Edit Goto Selection Utilities System Help
SAP
Table for illegal passwords
Password
Position...

Display View "Table for illegal passwords": Overview

Entry 0 of 0

No entries exist, double-click for long text

FIGURE 8-7 Maintaining forbidden password character strings in table USR40 (Copyright by SAP AG)

Managing SAP System Superusers

The SAP WAS system includes in the default installation two special users: DDIC and SAP*. These users have special privileges and must be protected to avoid unauthorized access. System administrators should consider a good strategy for managing the superusers of SAP systems for security reasons and to ensure system integrity.

The standard installation creates the system clients 000, 001, and 066. The SAP* and DDIC users are created in clients 000 and 001 with standard names and passwords.

User SAP*

SAP* is the standard SAP system superuser, and it's the only system user who does not require a user master record because it's defined in the code itself. When a new client is created for doing a client copy, SAP* is created by default in the new client with a standard password *PASS* and unlimited access rights. In the standard installation, SAP* has the password 06071992 in clients 000 and 001.

The special properties of the SAP* user can be deactivated. To deactivate the properties of the SAP* superuser, you must create a user master record for it, in which case it will have just the authorizations given in the profiles of the user master record.

If a user master record exists for SAP* and then it is deleted, it recovers the special properties assigned by the system code and has the password *PASS* again. When SAP* does not have a user master record, the password is always *PASS*; it cannot be changed, and it's not subject to any authorization check.

Some of the measures to protect SAP* are as follows:

- Change the password in client 000 and 001.
- Create a user master record for SAP* in 000, 001, 066, and the possible new clients you create in the system.
- Turn off the special status of SAP* by setting the instance profile parameter *login/no_automatic_user_sapstar* to a value greater than zero in the common default profile, DEFAULT.PFL. If the parameter is set, then SAP* has no special default properties. If there is no SAP* user master record, then SAP* cannot be used to log on. Be sure to have a user master record for SAP* even when this parameter is set because, if the parameter is reset to the value *0*, the system will again allow the logins by SAP* with the password *PASS*.
- Having a user master record, SAP* behaves like any other user subject to authorization checks. Its password can be changed.
- Create your own superuser account in each system client. This is explained in the next section.
- Delete all profiles from the SAP* profile list so that it has no authorizations.
- Be sure that SAP* is assigned to the user group SUPER, which protects the master records from being deleted by anyone not having authorization to delete SUPER master records. The user group SUPER has special status in the user maintenance profiles as delivered by the system. Users within this group can only be maintained or deleted by new superusers, as defined by the SAP standard authorization profiles.

Defining a New Superuser

Defining a new superuser just requires giving him or her a superuser profile with all authorizations in the user master record. The standard profile with full authorization, which is the only one needed to define a new superuser to replace SAP*, is the SAP_ALL profile. SAP_ALL contains all SAP authorizations, including the new authorizations as released in the SAP_NEW profile. SAP_NEW is a standard profile that ensures upward compatibility in access privileges. It's the way to protect users against authorization problems after a new system upgrade. If the upgrade of the system includes new access tests, this profile ensures the inclusion of those new authorization objects needed to validate the new access tests.

User DDIC

User DDIC (from *data dictionary*) is the maintenance user for the ABAP dictionary and for software logistics. It's the user required to perform special functions in system upgrades. Like SAP*, user DDIC is a user with special privileges.

The user master record for user DDIC is automatically created in clients 000 and 001 when you install your SAP system. It has, by default, the password 19920706. Its difference from SAP* is that it has its own user master record.

To secure DDIC against unauthorized use, you must change the password for the user in clients 000 and 001 in your SAP system. User DDIC is required for certain installation and setup tasks in the system, so you should not delete DDIC.

The Authorization System in SAP WAS

The authorization system of the SAP system is the general term that groups all the technical and management elements for granting access privileges to users to enforce the SAP system security.

An *access privilege* is permission to perform a particular operation in the SAP system. Access privileges in SAP systems are granted to users by assigning them authorizations, profiles or roles. By entering such roles and profiles in user master records, you enable users to use the system.

The main features and concepts of the SAP authorization system can be summarized as follows:

- The authorization system is based on complex system objects with multiconditional testing of system access privileges. The authorization system tests multiple conditions before granting users the permission to perform a task in the system. A multiconditional access test is defined in an authorization object. A multiconditional testing is, for example, to allow users to create, display, or delete information from one purchasing center, but only display information in another purchasing center. The following list shows this concept:

User	Purchasing Center	Permissions
FREDSMITH	001	Create, Delete, Display
FREDSMITH	002	Display
JGALPJR	002	Create, Delete, Display

- The authorization system uses authorization profiles and roles, together with the Role Maintenance (former Profile Generator) tool, to make the maintenance of the user master records easier. Authorization profiles are groups of authorizations. Instead of entering every authorization in the user master records, administrators only have to enter either roles, profiles, or both.
- Authorization profiles can be either simple or composite. Composite profiles contain other profiles.
- The authorization system uses an activation method. When authorization or profiles are created or modified, they must be activated to become effective.
- The SAP authorization system provides mechanisms for the distribution of the maintenance tasks related with users and access privileges, such as assigning authorizations, roles, activating profiles, managing new authorizations, and so on. These tasks can be done by a single superuser or they can be divided among several administrators.

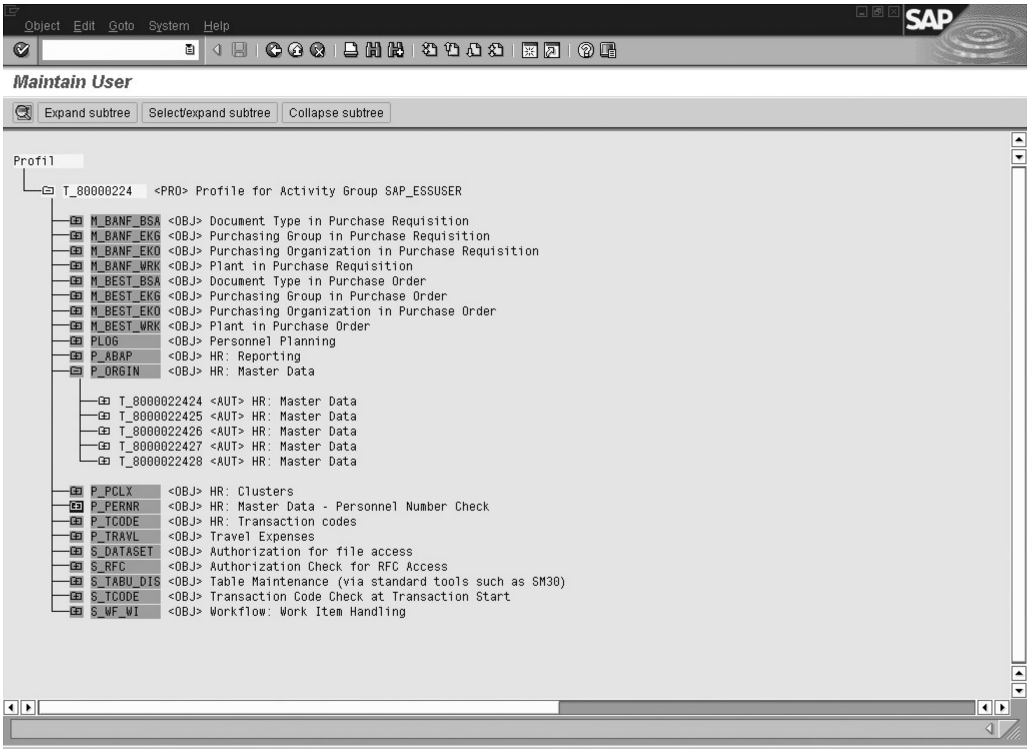
SAP systems include many predefined authorizations, profiles, and roles that cover most of the usual needs for assigning access privileges to users. Before creating a new role or profile, you should try to use an existing predefined one.

The complex objects of the SAP authorization system are structured in a hierarchical but flexible way, as shown in Figure 8-8. The next section introduces the main elements of the authorization system.

In order to aid understanding of the authorization system, basic concepts are explained first. Then the manual procedure for creating profiles and authorizations is introduced, and finally the Role Maintenance tool and how to work with it are covered.

Authorization Profiles

An authorization profile contains a group of authorizations, that is, a group of access privileges. Profiles are assigned to users in the user master records. A profile could represent a simple job position since it defines the tasks for which a user has access privileges. Every profile might have as many access privileges (authorizations) as desired. Profiles can contain authorization objects and authorizations.



```
Profil
  T_80000224   <PRO> Profile for Activity Group SAP_ESSUSER
      M_BANF_BSA <OBJ> Document Type in Purchase Requisition
      M_BANF_EKG <OBJ> Purchasing Group in Purchase Requisition
      M_BANF_EKO <OBJ> Purchasing Organization in Purchase Requisition
      M_BANF_WRK <OBJ> Plant in Purchase Requisition
      M_BEST_BSA <OBJ> Document Type in Purchase Order
      M_BEST_EKG <OBJ> Purchasing Group in Purchase Order
      M_BEST_EKO <OBJ> Purchasing Organization in Purchase Order
      M_BEST_WRK <OBJ> Plant in Purchase Order
      PLOG       <OBJ> Personnel Planning
      P_ABAP     <OBJ> HR: Reporting
      P_ORGIN    <OBJ> HR: Master Data
          T_8000022424 <AUT> HR: Master Data
          T_8000022425 <AUT> HR: Master Data
          T_8000022426 <AUT> HR: Master Data
          T_8000022427 <AUT> HR: Master Data
          T_8000022428 <AUT> HR: Master Data
      P_PCLX     <OBJ> HR: Clusters
      P_PERNR    <OBJ> HR: Master Data - Personnel Number Check
      P_TCODE    <OBJ> HR: Transaction codes
      P_TRAVL    <OBJ> Travel Expenses
      S_DATASET  <OBJ> Authorization for file access
      S_RFC      <OBJ> Authorization Check for RFC Access
      S_TABU_DIS <OBJ> Table Maintenance (via standard tools such as SM30)
      S_TCODE    <OBJ> Transaction Code Check at Transaction Start
      S_WF_WI    <OBJ> Workflow: Work Item Handling
```

FIGURE 8-8 Hierarchy of authorization system (Copyright by SAP AG)

Changing the list or contents of the authorizations inside a profile affects all users that are given that profile when this is activated. It becomes effective the next time the user logs on. The change is not effective for users currently logged on.

Composite Profiles

Composite profiles are sets of authorization profiles, both simple and composite. A composite profile can contain an unlimited number of profiles. They can be assigned to users just as profiles in the user master records are.

Composite profiles are suitable for users who have different responsibilities or job tasks in the system. These profiles are sometimes known as *reference* profiles for assigning a larger group of access privileges and having the possibility to better match users with several responsibilities.

Making modifications to any of the profiles in the list included in the composite profile directly affects the access privileges of all users having that composite profile in the user master record.

When displaying profiles on the different SAP screens, there is a description indicating whether the profile is simple or composite.

Authorizations

The SAP system uses authorizations to define the permitted values for the fields of an authorization object. An authorization might contain one or more values for each field of the authorization object.

An authorization object is like a template for testing access privileges, consisting of authorization fields that finally define the permitted values for the authorization. Both authorization objects and fields are explained in the next two sections.

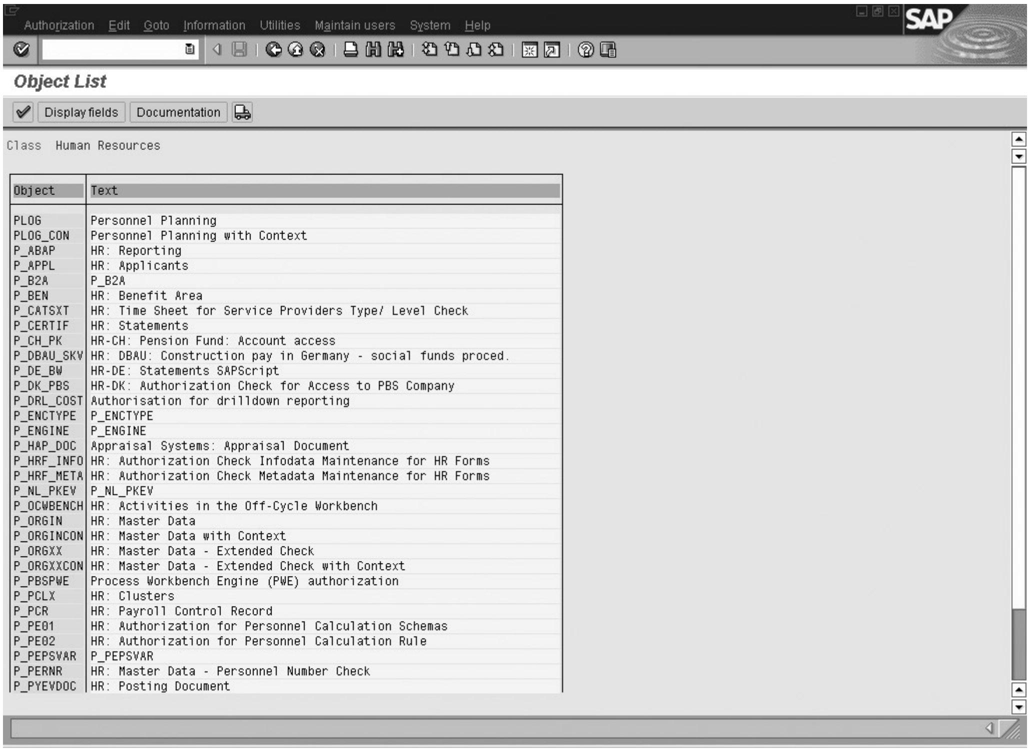
An authorization is identified with the name of an authorization object and the name of the authorization created for the object. An authorization can have many values or ranges of values for a single field. It is also possible to authorize for every value (by entering an asterisk, *) or for none (by leaving the field blank). In the example shown in Figure 8-9, you can see that for the object, *Batch processing: Batch administrator*, there are several authorizations. Each of these authorizations can have different values for the authorization fields within the object.

Authorizations are entered in authorization profiles with the corresponding authorization object. When an authorization is changed and then activated, it immediately affects all users having a profile containing that authorization in their user master records.

The technical names for authorizations and authorization objects have a maximum of 12 positions, but usually they are displayed in the system using short descriptive texts. For customer-created authorizations, the only name restriction is to not place an underscore in the second position of the technical name. Additionally, every customer-created system object should comply with SAP standard style guide and begin either with a *Z* or a *Y* to distinguish it from the SAP original objects, thus avoiding the possibility of being overwritten by a system upgrade.

Authorization Objects

An *authorization object* identifies an element or object within the SAP system that needs to be protected. These objects work like templates for granting access rights by means of authorization fields that allow for performing complex tests of access privileges. An


Authorization Edit Goto Information Utilities Maintain users System Help
Object List
Display fields
Documentation

Class Human Resources

Object	Text
PLOG	Personnel Planning
PLOG_CON	Personnel Planning with Context
P_ABAP	HR: Reporting
P_APPL	HR: Applicants
P_B2A	P_B2A
P_BEN	HR: Benefit Area
P_CATSXT	HR: Time Sheet for Service Providers Type/ Level Check
P_CERTIF	HR: Statements
P_CH_PK	HR-CH: Pension Fund: Account access
P_DBAU_SKV	HR: DBAU: Construction pay in Germany - social funds proced.
P_DE_BW	HR-DE: Statements SAPScript
P_DK_PBS	HR-DK: Authorization Check for Access to PBS Company
P_DRL_COST	Authorisation for drilldown reporting
P_ENCTYPE	P_ENCTYPE
P_ENGINE	P_ENGINE
P_HAP_DOC	Appraisal Systems: Appraisal Document
P_HRF_INFO	HR: Authorization Check Infodata Maintenance for HR Forms
P_HRF_META	HR: Authorization Check Metadata Maintenance for HR Forms
P_NL_PKEV	P_NL_PKEV
P_OCWBENCH	HR: Activities in the Off-Cycle Workbench
P_ORGIN	HR: Master Data
P_ORGINCON	HR: Master Data with Context
P_ORGXX	HR: Master Data - Extended Check
P_ORGXXCON	HR: Master Data - Extended Check with Context
P_PBSPWE	Process Workbench Engine (PWE) authorization
P_PCLX	HR: Clusters
P_PCR	HR: Payroll Control Record
P_PE01	HR: Authorization for Personnel Calculation Schemas
P_PE02	HR: Authorization for Personnel Calculation Rule
P_PEPSVAR	P_PEPSVAR
P_PERNR	HR: Master Data - Personnel Number Check
P_PYEVDOC	HR: Posting Document

FIGURE 8-9 Example of authorization list for an authorization object (Copyright by SAP AG)

authorization object can contain a maximum of 10 authorization fields. Users are permitted to perform a system function only after passing the test for every field in the authorization object. The verification against the field contents is done with the logical AND operator. With this mechanism, the system can perform multiconditional tests.

As with authorizations, when maintaining authorization objects, the system does not display the names but descriptive text for each object.

Authorization objects are grouped in object classes belonging to different application areas that are used to limit the search for objects, thus making it faster to navigate among the many SAP system objects.

SAP predefined authorization objects should not be modified or deleted, except if instructed by the SAP support personnel or a SAP note. Deleting or changing standard authorization objects can cause severe errors in the programs that check those objects.

Before an authorization object is modified, all authorizations defined for that object must first be deleted.

If you want to use the OR logic to give users access to certain functions, you can define several authorizations for the same object, each time with different values. In the user master records, you assign each of these profiles, which are linked with the OR login. So, when the system tests whether the user has access privileges, it checks each authorization to see if the assigned values comply with the access condition. The system allows access with the first authorization that passes the test.

Authorization Fields

Authorization fields identify the elements of the system that are to be protected by assigning them access tests. An authorization field can be, for example, a user group, a company code, a purchasing group, a development class, or an application area. There is one authorization field that is found in most authorization objects which is the *Activity*. The Activity field in an authorization object defines the possible actions that could be performed over a particular application object. For example, activity *03* is always *Display*, so if an authorization contains two fields such as *company code* and *activity* and if the company code field is * (meaning all company codes), the user with that authorization can only display the company codes.

The list of standard activities in the system is held on the SAP standard table TACT, which can be displayed using standard transactions such as SM30 (Extended Table Maintenance), or SE16 (Data Browser).

The relationship between the authorization objects and the activities is held in table TACTZ. Not all authorization objects have the Activity authorization field. Authorization fields are the components of authorization objects as stated previously. And also, fields are part of the standard ABAP function call AUTHORITY-CHECK.

When maintaining authorizations, the system does not display the real names (technical names) for the fields; instead it shows a description for each field. Table TOBJ contains the fields that are associated with each authorization object; this is how the SAP system knows which fields belong to an authorization object. The fields in an object are associated with data elements in the ABAP data dictionary.

Authorization fields are not maintained from the user maintenance menu, but have to be defined within the development environment. Normally users do not need to change standard authorization fields, except if adding or modifying system elements and they want those elements to be tested with authorizations.

Roles

Roles form a set of tasks or activities that can be performed in the system, such as running programs, transactions, as well as access to Web sites, files and other functions that generally represent job roles. When you assign roles to users, the system will automatically present a specific menu for that role when the users log on to the SAP system.

The roles and the information they include are what makes the profiles able to be automatically generated.

Roles are the basic components needed for working with the Role Maintenance tool (transaction PFCG), based on the Profile Generator, which uses them to generate authorization profiles. You can also access the Role Maintenance tool, by clicking on the Create Role button on the application toolbar from the initial SAP Easy Access screen.

Roles resemble a job description, such as sales representative, accountant, treasurer, system administrator, and so on. Roles can include as many single system activities as needed. Single system activities can be transactions, reports and access to other types of objects such as Web sites, files, BSPs, and others.

Role administrators select transactions or reports from a menu tree or can select authorizations and save this information as an activity group. This selection is used by the profile generator for determining the necessary authorizations and generating the profiles, which can then be assigned to users.

You can also assign roles to organizational objects, such as organizational units, jobs, positions, users, and so on. This can be done with the Organizational Management pushbutton, but you will only see this function if you have defined what it's known as an active plan variant, which is configure through the Customizing of HR. Please refer to the SAP online help for guidance on how to set up Roles for Organizational Management in HR.

User master records can be assigned to one or more roles. When this type of assignment takes place, the updating of the user master records can be performed manually or automatically by running a background job. When this happens, the system combines the functions in the user menu when she or he logs on.

Roles can be temporarily assigned to users, which means that they can have multiple validity periods that cannot overlap. Date dependency assignment of profiles to user master records can be enforced by scheduling background jobs for that purpose.

User Buffers

User buffers are special areas (tables) containing all the authorizations for the user. These buffers are specific for individual users, and are actually built when the users log on, based on the authorizations contained in the profiles included in the user master record. When users try to perform activities in the system, the application programs and transaction are checked against the authorization objects and values contained within the user buffer.

The number of entries in the user buffer can be controlled using the profile parameter *auth/new_buffering*.

You can see the context of the user buffer by selecting Tools | Administration | Monitor | User Buffer from the main menu, or by running transaction SU56.

The Activation Concept in Profiles and Authorizations

The authorization system allows two versions of authorizations or profiles: an active version and a modified, or maintenance, version. A new or modified authorization or profile cannot be used until it has been activated, since user master records can only contain active versions of profiles.

The activation concept is useful for preventing mistakes when creating new authorizations or modifying existing ones, since the maintenance versions will not affect the system. It is also helpful for dividing the maintenance tasks among several users. For example, some users can define or edit authorizations, while an activation administrator can be in charge of activating the maintenance versions previously created.

The system verification for access privileges is only performed against active versions. Active versions are the only ones that have real effect in the system. When administrators create or modify an authorization or a profile, then they are working with a maintenance version. In this state, the system displays the status *Revised* in the header of the authorization or profile being modified. When the activation is performed, the maintenance version becomes the active one and replaces automatically the existing version if it exists. The system changes the status to *Active*.

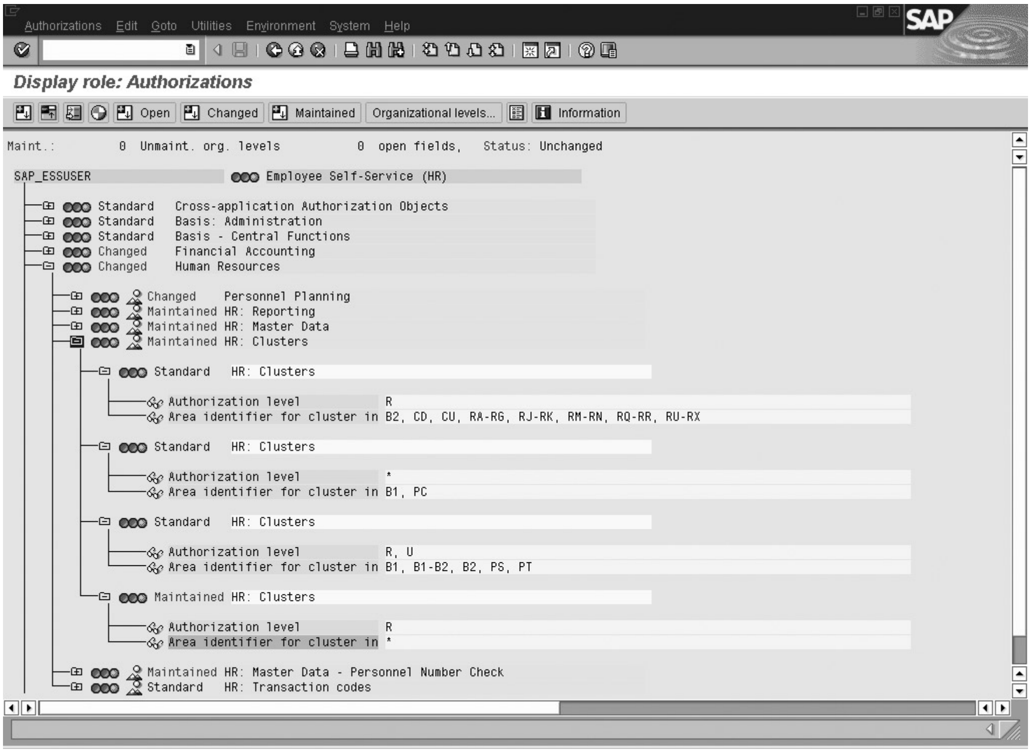
Working with the Role Maintenance Tool

The Role Maintenance tool is an evolution of the Profile Generator available in releases of SAP R/3 since 4.6 that aids in facilitating the management of roles, user authorizations, and profiles. Previous to the Role Maintenance and Profile Generator, there was a great deal of effort involved in the implementation and support of the authorization concept, and this was a costly activity within projects.

The Role Maintenance tool was designed by SAP with the objective of reducing the time needed for implementing and managing the user menus and authorizations associated with a job description, thus decreasing the implementation costs. SAP recommends using the Role Maintenance and Profile Generator to set up authorizations.

Using the Role Maintenance is very different from manual profile management, where authorization objects must be selected, authorizations defined, and profiles created to be assigned to users later. With the Role Maintenance, the management of profiles and authorizations is based on the functions and tasks that users will perform with the SAP systems, and the Profile Generator is in charge of selecting and grouping the authorization objects (Figure 8-10).

The definition of roles with the Role Maintenance is based on grouping functions or tasks user menu that generates the profiles and authorizations selected by the customers.



Display role: Authorizations

```
Maint.:        0  Unmaint. org. levels         0  open fields,   Status: Unchanged

SAP_ESSUSER                 Employee Self-Service (HR)

   Standard   Cross-application Authorization Objects
   Standard   Basis: Administration
   Standard   Basis - Central Functions
   Changed    Financial Accounting
   Changed    Human Resources

      Changed    Personnel Planning
      Maintained HR: Reporting
      Maintained HR: Master Data
      Maintained HR: Clusters

         Standard   HR: Clusters

            Authorization level            R
            Area identifier for cluster in B2, CD, CU, RA-RG, RJ-RK, RM-RN, RQ-RR, RU-RX

         Standard   HR: Clusters

            Authorization level            *
            Area identifier for cluster in B1, PC

         Standard   HR: Clusters

            Authorization level            R, U
            Area identifier for cluster in B1, B1-B2, B2, PS, PT

         Maintained HR: Clusters

            Authorization level            R
            Area identifier for cluster in *

      Maintained HR: Master Data - Personnel Number Check
      Standard   HR: Transaction codes
```

FIGURE 8-10 Assigning authorizations to the new profile (Copyright by SAP AG)

As introduced in a previous section, *roles* form a set of tasks or activities that can be performed in the system, such as running programs, transactions, and other functions that generally represent job roles. SAP systems already include a very large number of predefined roles that can be freely selected, or copied and then modified to accommodate specific needs.

In summary, the Role Maintenance tool and the Profile Generator

- Can be used to automatically create profiles and assign them easily to users
- Only select and use the necessary authorization objects, avoiding excessive validations in the system and thereby improving performance
- Facilitate functional communication between security or the authorization administrator and end users or consultants
- Make defining and maintaining authorization profiles easier

The Role Maintenance and Profile Generator can be accessed from the initial SAP Easy Access screen by clicking on the Create Role pushbutton on the application toolbar; or, from the main menu tree by selecting Tools | Administration | User Maintenance | Role Administration | Roles or alternatively by entering transaction code PFCG in the command field.

The following sections introduce how the Role Maintenance works, how to configure it, and a basic example of creating roles and using automatically generated profiles to assign those roles to user master records.

How the Role Maintenance Works

Based on a job role, or group of tasks that represents what the users are trying to perform, administrators can identify and select the transactions, reports, or values that are required for users to pass the authorization checks.

Using the Role Maintenance and Profile Generator tool, the administrator creates roles with functions and tasks, associated to SAP transactions, reports, and other object types, that automatically will create a generate profiles and select the required authorizations, and sets authorization values or let the administrator maintain those values for the authorization objects that correspond to the specific functions selected.

Once roles are created, the Profile Generator is in charge of retrieving all the authorization objects for the selected transactions. This is accomplished using special check tables.

The Profile Generator then creates the profile or profiles, and then the roles can be assigned to the user master record. The user master record is then updated by a direct assignment, which automatically assigns the generated profiles as well. This assignment can be also performed via a batch job. Once the assignment is done, when the users log on, their user buffer will contain the corresponding authorization that will allow them to pass the authorization checks required for performing their usual jobs.

Configuring the Profile Generator

Before using the Role Maintenance, you have to configure the Profile Generator for the first time. The steps required to configure and work with the Profile Generator tool are the following:

1. *Activate the Profile Generator.* The activation of the Profile Generator is based on the instance profile parameter *auth/no_check_in_some_cases* = *Y*. If this value is

not set, users won't be able to see the Authorization pushbutton within the role maintenance screen. This is the default value since R/3 Basis release 4.0. This profile parameter tells the system to allow certain authorization checks to be ignored in a program. With this setting the profiles will only contain the necessary authorizations. For example, if the installation includes only one company code, administrators don't want to worry about setting authorizations for company code.

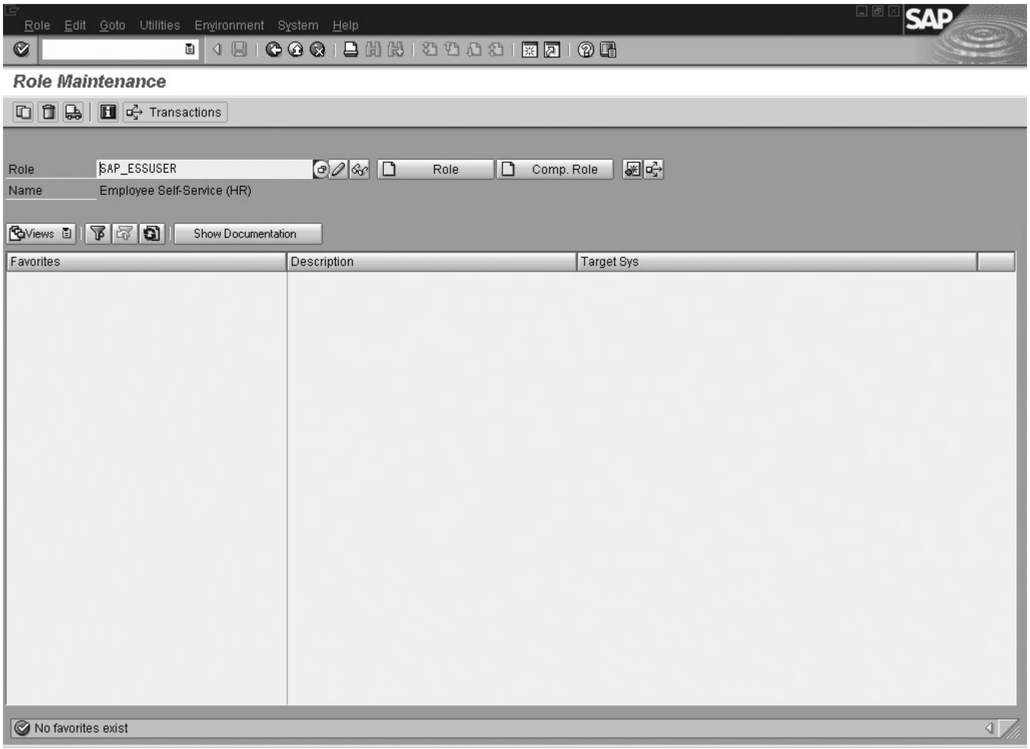
2. *Set up the initial copy of Profile Generator configuration tables.* You must run transaction SU25 to transfer the SAP transactions and authorization objects from SAP tables USOBT and USOBX to the customer tables USOBT_C and USOBX_C. You can then maintain these tables using transaction SU24. Table USOBT includes the relation between the transactions and the authorization objects. If it is a new installation, just click on the button next to option 1, *Initially fill the customer tables*. If you are upgrading from a previous release, you must use the lower options, but first look up the most recent information concerning your release in the online documentation.
3. *Maintain the scope of authorization object checks in transactions.* This is performed using transaction SU24 (also the last button on the screen for transaction SU25) in order to maintain customer tables USOBX_C (transactions and authorization objects) and USOBT_C (proposed values for authorization objects). This is not a mandatory step, but can be used by customers to maintain their own authorization checks as well as to assign SAP authorization objects to custom transactions. You can also maintain the assignment for a single transaction, and enforce or suppress the authorization check for any transaction. Additionally, it is possible to maintain the field assignments for the transactions. In any case there is always the possibility of comparing these settings with the SAP standard settings. The purpose of this transaction is for the administrator to be able to maintain the scope of authorization checks in transactions by
    - Assigning the authorization objects that are relevant to a transaction
    - Assigning default values and organizational level defaults for authorization object fields

Basic Concepts for Working with Roles

Access the Role Maintenance screen by clicking on the Create Role pushbutton in the initial screen of the SAP Easy Access, or enter transaction PFCG in the command field. The system will display a screen like the one in Figure 8-11.

Role maintenance includes three different views, which you can select from the initial screen by choosing Goto | Settings:

- The Simple Maintenance View is used only to maintain the Role menu.
- The Basic Maintenance View allows additional functions for defining and maintaining roles, not only for maintaining the menu, but also the profile and authorizations.
- The Complete View includes all the functions for the basic maintenance plus the organizational management link and the workflow. This is the more comprehensive view that can display all the assignments for a role. This view is tightly related



Role Maintenance

Role SAP_ESSUSER
Name Employee Self-Service (HR)

Favorites	Description	Target Sys

No favorites exist

FIGURE 8-11 Role Maintenance initial screen in complete view (Copyright by SAP AG)

to the personnel development HR application, so it is useful for users working in organizational management.

When implementing structural authorizations, that is, roles linked with HR organizational management, roles are assigned to *agents*. There are several types of agents, being the most common the *user master record;* however, there are other types of organizational agents that can be created within the Human Resource module, such as *organizational units*, *positions*, *jobs*, *persons*, or *work centers*.

Creating Roles

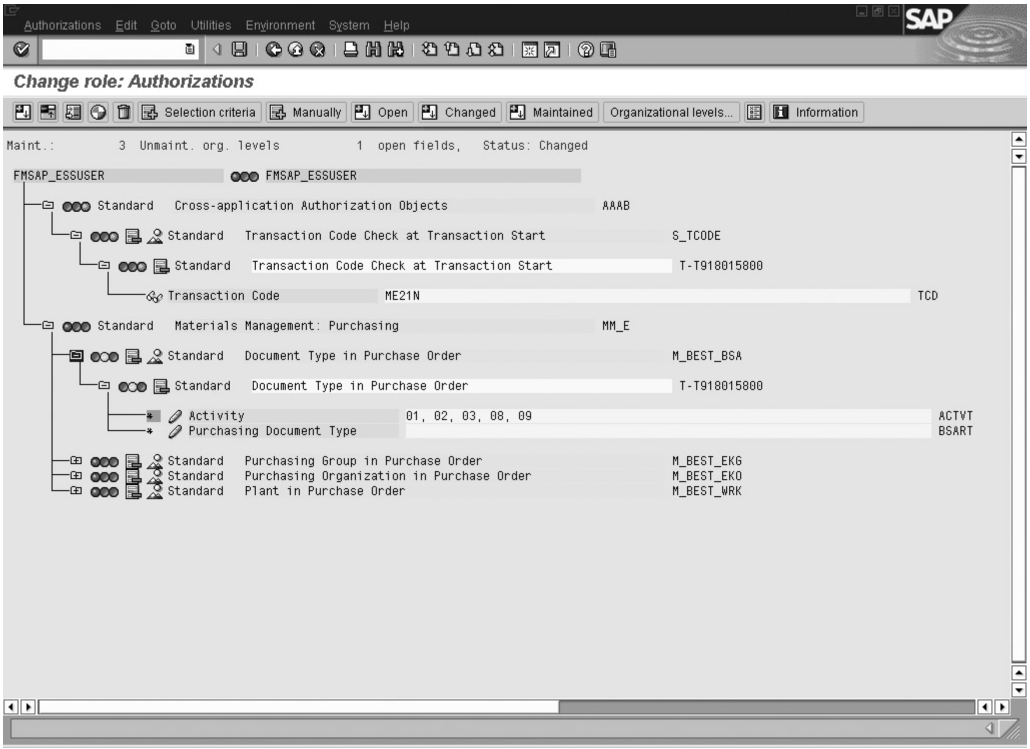
The basic steps for creating a new role are, in a simplified way:

1. Enter a role name in the input field and press the Create pushbutton to the right of the name or the Comp. Role if wishing to create a composite role. Remember to follow the naming convention, starting the role name with Z_ or Y_.
2. Save the role, click on the Menu tabstrip and select the transactions from the SAP menu, from other role, or insert individual transactions or objects by clicking on the corresponding pushbutton. The process is very easy and intuitive.

3. Next, go to the Authorizations tab, and enter a profile name, or let the system propose one for you. Click on Change Authorization Data. The system will present the Change Role: Authorization screen. Complete the authorizations for chosen activities: those marked with an orange light.
4. Select Authorizations | Generate the Profiles.
5. Assign the role to users and press User Comparison to transfer profiles to the user master record.

The following example shows how to create a simple role for the purchasing department users, providing them with authorizations for creating purchasing orders when the vendor is known (transaction code ME21) and for changing and displaying purchasing orders (transaction codes ME22 and ME23). These are the steps:

1. Access the main Role Maintenance screen by entering transaction code PFCG in the command field. The system will display the Role Maintenance initial screen.
2. Enter the name for the activity group, and click the Create icon located to the right of the name. Enter a description, or even some sort of documentation in the space provided at the bottom of the screen.
3. Click on the Menu tabstrip. The system will display the main Change Roles screen, full of options to create a menu for this specific role. In this case, we will do it from a standard SAP menu.
4. Click on the From the SAP Menu pushbutton located on the right of the screen. The system will show a dialog box with the standard SAP Menu tree. In our example, click on the plus signs on Logistics, Materials Management, Purchasing, Purchase Order, Create. Finally, mark the square box next to Vendor/Supplying Plant Known. On the same level as Create and below, mark the square box next to Change and Display. Save your selection by clicking on the Transfer icon.
5. You will return to the previous screen. The next step is to maintain the Authorizations, by clicking on the Authorizations tabstrip. Click on the small icon to the right of the Profile Name field, so that the system will propose a profile name. Then click on the Change Authorization Data pushbutton in the lower part of the screen. Save the role.
6. Next, the system first displays a new screen where you have to maintain the organizational levels. In this case, these are the Purchasing Group, Purchasing Organization, and Plant. You can input simple values or ranges, or enter a wildcard such as * to indicate all organizations. Fill in the fields or click on the Full Authorization pushbutton if you want to allow authorization on all organizational levels and save it. The system will display the Change Role: Authorizations screen, as shown in Figure 8-12.
7. Expand the nodes by clicking on the folders or by positioning the cursor on the line and clicking on the Expand icon. Notice how the browser view is presented in four levels: authorization object class, authorization object, authorizations, and field values. The system automatically selects the objects and values according to the previous selections. Select Utilities | Technical Names On to display the familiar authorization objects. Notice also how the Profile Generator tool has selected the


Authorizations Edit Goto Utilities Environment System Help
SAP
Change role: Authorizations
Selection criteria
Manually
Open
Changed
Maintained
Organizational levels...
Information

```
Maint.:        3  Unmaint. org. levels        1  open fields,   Status: Changed

FMSAP_ESSUSER              FMSAP_ESSUSER
  Standard   Cross-application Authorization Objects           AAAB
    Standard   Transaction Code Check at Transaction Start            S_TCODE
      Standard   Transaction Code Check at Transaction Start          T-T918015800
        Transaction Code      ME21N                                          TCD
  Standard   Materials Management: Purchasing                  MM_E
    Standard   Document Type in Purchase Order                        M_BEST_BSA
      Standard   Document Type in Purchase Order                      T-T918015800
        * Activity                01, 02, 03, 08, 09                         ACTVT
        * Purchasing Document Type                                           BSART
    Standard   Purchasing Group in Purchase Order                     M_BEST_EKG
    Standard   Purchasing Organization in Purchase Order              M_BEST_EKO
    Standard   Plant in Purchase Order                                M_BEST_WRK
```

FIGURE 8-12 Activity group browser view (Copyright by SAP AG)

authorization object S_TCODE (authorization for transaction start) and provided it with the values of the selected transactions.

8. You have to maintain all pending authorizations before you can generate the complete profile. The maintenance status of the authorizations at every level is shown using traffic lights: green indicates that all values are maintained, yellow that there is some value that is not yet maintained, and red that at least an organizational level is missing. In order to maintain pending or open values, you can click on the individual level so the system will display a new dialog box for entering required field values.

   Or, you can click on a traffic light and maintain all outstanding fields below, or assign full authorizations. For this example, you can assign complete authorizations for the subtree by clicking the stoplight on the *Standard: Document type in purchase order* line. On the dialog box, click the Enter icon.

9. Next, click the Generate icon on the application toolbar. If you did not define previously, the system will display a dialog box for entering the profile name and a short text. You can keep the proposed system name or change it to your own standards. Continue by pressing ENTER. The system will now generate the profile.

10. Go back to the initial activity group maintenance screen. The screen will show green traffic lights for both Menu and Authorizations. Now assign this profile to one or more user master records by clicking on the User tabstrip.
11. In this part of the role maintenance, you could simply assign this role to one or several users, or associated with other type of agents, by clicking on the Organizational Management pushbutton (you will only see this pushbutton if in complete view). Enter the name of the user or users you want to assign the new created role.
12. If you want the profiles to be transferred to the actual user master records, click the User Comparison pushbutton. The system will display the use comparison program.

You can verify that the role and profiles have been effectively transferred by looking up the user master records using transaction SU01. There is the possibility of running a general report for updating all user masters and pending assignments of activity groups by using transaction PFUD.

The Role Maintenance and Profile Generator tools include many additional functions to facilitate the creation and maintenance of roles, authorizations and profiles, such as using single roles as templates, collections of authorization objects that can be included within roles.

Tracing Authorizations

The SAP system includes some options to find the authorization for any transaction or function a user performs in the system. This is quite useful when looking for an authorization denial problem or when defining profiles when you want to specify exactly what authorization objects a particular transaction checks. The two methods available in SAP systems for finding authorizations are the authorization check transaction (SU53) and using the system trace.

The *system trace* is a more general-purpose tool used mainly by developers or system administrators which can provide a great detail of information and can be used to trace other user sessions.

Transaction SU53 is more specific for authorization error analysis but can only be used for the current user sessions. However, SU53 is a faster and more direct method for finding an authorization denial problem. Transaction SU53 can be accessed from the menu System | Utilities | Display Authorization Check.

Using the System Trace for Tracing Authorizations

The SAP system includes extensive tracing and debugging utilities. You can find more information about tracing in Chapter 10. This section covers just the simple process of activating and displaying a trace concerning authorization checks.

To start the system trace, from the main menu select Tools | Administration | Monitor | Traces | System Trace. The system displays the available trace options and switches, one of which is the Authorization Check. Make sure you mark the check box next to Authorization Check.

To limit the trace to your own user ID or another user ID, enter the name of the user ID you want to trace in the General Filter field by clicking on the possible entries arrow and then selecting it from the list.

To activate and start the tracing process, select Trace On from the application toolbar. The trace will start recording every system function you or the entered user performs. So, if you are looking for an authorization problem or just want to find a particular authorization check, open a new session and go to the screen, function, or transaction you want to analyze.

Once you are finished you should stop the system trace. Go back to the session where you activated the trace, and if you are on the tracing screen, stop the trace by selecting Trace Off.

Now you should look at the trace file generated. To analyze the trace click on the Analysis pushbutton on the application toolbar, and enter the criteria for the analysis.

The trace file contains the authorization objects, authorization fields, and values that have been tested while you have been performing system functions. Authorization tests are displayed in the following format:

```
<Authorization object>:<Field>=<Value tested>
```

But you can display a more legible view of the authorization check by clicking over the entry.

Using the SU53 Transaction

The transaction SU53 can be used to analyze a function when getting the error *You are not authorized to* in the status bar. When you get this message, enter SU53 or /NSU53 in the command field. Alternatively, you can select System | Utilities | Display Authorization Check from any SAP screen. The system will display the authorization object and value for which you were not authorized.

Transaction SU53 can also be used from any of your open sessions and not only from the one in which you got the authorization error message. However, you cannot use SU53 to analyze other users' authorization errors. In those cases, administrators should instruct users to reproduce the error and then to enter the transaction SU53 in the command field to receive information about the authorization error messages they got.

Organizing the Maintenance of the Authorization System

The SAP authorization system offers many options for organizing the administration of users, authorizations, and profiles, making it quite flexible when defining roles. Depending on the type, size, and security restrictions, an installation can have a single superuser for all users and authorization system maintenance to several decentralized administrators with different maintenance functions and limited authorizations.

SAP recommends that for enforcing maximum system security customers divide the maintenance of the user and authorization system among three types of users:

- *User administrators.* They are in charge of creating and modifying user master records. User administrators can set user parameters, edit the list of assigned profiles, and so forth. User administrators cannot create or activate roles, authorizations or profiles. User administrators can be further divided by assigning them authorization maintenance to certain user groups.

- *Authorization administrators.* These users are able to define or modify roles, authorizations and profiles; however, they are not permitted to activate authorizations or profiles. Authorization administrators only work with *active* versions of authorizations and profiles.
- *Activation administrators.* They are in charge of activating profiles and authorizations. This type of administrator is no longer able to change the authorizations or profiles but can only activate existing revised versions of profiles and authorizations.

Dividing the maintenance responsibilities among different administrators can increase the security of the system against unwanted actions over user master records, authorizations, and profiles. Another advantage is the decentralization of the user administration. In big installations with hundreds of users, it can be a good practice to divide up user maintenance functions by department, building, regional office, and so forth.

To implement these administrative roles, the superuser uses authorizations to limit which user groups are maintained by user administrators and which authorizations and profiles can be maintained or activated by which administrators. Because the superuser can limit and restrict the access rights, the decentralized administrators do not need to be high-level technical staff. They can be normal company users.

As a superuser, you can define new profiles for these administrators using the standard S_A.ADMIN profile as a template and changing the allowed field values corresponding to authorization objects such as *user group, authorizations, authorization profiles*, and mainly setting the Activity field values.

Refer to the SAP online documentation in the "Users and Authorization" help file for details on setting values for dividing up administrative roles.

Creating New Authorization Checks

Although the SAP Web Application Server systems includes virtually all authorization objects and checks to test whether users can access the system functions, customers might add new development objects and functions to extend the system capabilities. In such cases, customers might also need to include a new authorization check.

SAP provides several ways to include new authorization checks for custom-developed objects or transactions, the most important being:

- By programming the authorization check using the ABAP standard statement AUTHORITY-CHECK
- By assigning authorization groups to tables, maintaining table TDDAT, and using authorization object S_TABU_DIS
- By using authorization object S_PROGRAM and using program authorization groups by maintaining table TPGP

For specific details about these procedures, please refer to the SAP online documentation.