Abstract
Organizations that use SAP® need a way to manage user accounts and access rights. Identity Manager, a part of the Dell One Identity products from Dell Software, makes it easy to manage user identities, privileges and security across the enterprise, including SAP. This technical brief details how.

Introduction
Identity Manager simplifies user administration for the SAP R/3 environment and integrates with SAP/HR and SAP/OM to provide a trusted and authoritative source for valuable organizational information. Identity Manager helps you set up and manage user accounts, groups, roles, profile assignments and transactions. All the attributes of those objects are synchronized with the central database through connectors, enabling Identity Manager to access other target systems.

In addition to streamlining user administration, Identity Manager helps you achieve your security and compliance goals. It can be used to define rules that maintain and monitor compliance with regulatory requirements and automatically deal with rule violations. Identity Manager helps ensure separation of duty (SoD), and provides full auditing.

SAP solutions and architecture
Solutions
SAP is the global market leader in enterprise applications software. Its offerings include:

- **Analytical applications**—SAP offers a suite of analytical applications that are custom-designed for different industries. Because these applications turn business data into business intelligence, they give businesses an advantage. These solutions are able to take key performance indicators (KPIs) into account and check the performance of the business against sector KPIs.

- **Governance, risk and compliance (GRC)**—These modules include automation of risk management and compliance for both small to medium businesses (SMBs) and global enterprises. Other solutions aid businesses to set sustainability goals and track their achievements against these.
SAP has three architecture levels: client, application and database.

• **Business Objects (BO)**—BO links closely to the Analytical Application suite and enables businesses to plan to grow their existing IT systems to meet their future business needs. SAP offer solutions to collate information across the organization and to leverage existing investments from vendors such as Microsoft and IBM.

• **Financial management**—SAP offers cash flow management in modular solutions that can be customized to meet the needs of any size business.

• **Customer relationship management (CRM)**—SAP CRM tools provide brand management, e-marketing and loyalty management to help businesses stay focused on their customers.

• **Supply chain management**—This software allows businesses to plan, distribute and transport supplies, as well as to adapt to a constantly changing market.

**Architecture**

SAP has three architectural levels: client, application and database, as shown in Figure 1.

• **Client**—The most used SAP client is SAP GUI. This C or C++ based program allows access to the application server(s) and is used to display and modify SAP data. The communication with the SAP application server is established upon the DIAG protocol, which allows communication only between SAP GUI and the application server(s).

• **Application**—The client layer communicates with the application server, which is the core of the SAP deployment. The application layer is responsible for each process operation within the different layers of an SAP system—it is the “brain” of the system. The application server is not a single service installed on an operating system; it is deployed as multiple instances of the processing system on various servers.

All business logic of an SAP system is implemented in Advanced Business Application Programming Language (ABAP) programs, which are executed on the application server. This execution happens in a dedicated runtime environment called a kernel. The kernel consists of multiple processes, such as transfer processes or spool processes, which can be distributed over different servers for different purposes. The data is compressed during transmission, which is not the case when using protocols for access like RFC to the SAP application server.

• **Database**—The application server in turn communicates with the database layer. All SAP system data is stored and managed in a database, such as a Microsoft SQL Server database or an Oracle database. The database is kept on a separate server, mainly for performance reasons but for security.

---

**Figure 1. SAP has three architecture levels: client, application and database.**
To summarize:
1. The client communicates with the application server.
2. The application server does all the processing and makes calls to the database.
3. Data is passed back to the application server.
4. More processing is done before the results are sent to the client.

SAP base administration

Clients
A SAP system always contains multiple clients, which separate the data of individual users. Each client owns regular user data individually. Because of this structure, it is easily possible to host multiple organizations on one single SAP system, without risking or granting cross-client access to sensitive data. Changes to the system configuration have immediate effect on each hosted client.

The selection of the intended client is entered during login to the system. Each client owns an individual client number, which has to be entered at login.

User management
ABAP authorization protects transactions, programs, and services in SAP systems from unauthorized access. The administrator assigns authorizations to users to control which actions each user can execute in the SAP system after he or she has logged onto the system and authenticated.

To access Business Objects or execute SAP transactions, which are both protected by authorization objects (which are explained below), a user requires corresponding authorizations. The authorizations represent instances of generic authorization objects and are defined depending on the activity and responsibilities of the employee. The authorizations are combined in an authorization profile that is associated with a role. The user administrators then assign the corresponding roles using the user master record, so that the user can use the appropriate transactions for his or her tasks.

ABAP authorization protects transactions, programs, and services in SAP systems from unauthorized access.
Figure 3 shows the authorization components and their relationships.

- **User master record**—The user master record enables the user to log onto the SAP system and access the functions and objects in it within the limits of the authorization profiles specified in the role. The user master record contains all information about the corresponding user, including the authorizations. Changes to a user master record take effect when the user next logs onto the system. Users who are already logged on are not immediately affected by the changes.

- **Composite role**—This consists of any number of single roles.

- **Single role**—This is created with the role administration tool and allows the automatic generation of an authorization profile. The role contains the authorization data and the logon menu for the user.

- **Generated authorization profile**—This is generated in role administration from the role data.

- **Manual authorization profile**—To minimize the editing effort if you are using authorization profiles, do not usually enter single authorizations in the user master record, but rather authorizations combined into authorization profiles. Changes to the authorization rights take effect for all users whose user master record contains the profile the next time they log on to the system. Users who are already logged on are not immediately affected by the changes.

- **Composite profile**—This consists of any number of authorization profiles.

- **Authorization object**—Authorization objects control what actions users can perform within the system. An authorization object can contain up to ten fields that are related by “AND” operators, allowing complex tests for multiple conditions. For an authorization check to be successful, all field values of the authorization object must be appropriately entered in the user master record. Authorization objects are divided into classes for comprehensibility. An object class is a logical combination of authorization objects and corresponds, for example, to an application such as financial accounting or human resources.

- **Authorization field**—This field contains the value that you define. It is connected to
the data elements stored with the ABAP dictionary. You can specify any number of single values or value ranges for an authorization field. You can also allow all values, or allow an empty field as a permissible value.

Changing an authorization affects all users whose authorization profile contains these authorizations. As a system administrator, you can edit authorizations in the following ways:

- You can extend and change the SAP defaults with role administration.
- You can change authorizations manually. These changes take effect for the relevant users as soon as you activate the authorization.

The programmer of a function decides whether, where and how authorizations are to be checked. The program determines whether the user has sufficient authorization for a particular activity. To do this, it compares the field values specified in the program with the values contained in the authorizations of the user master record.

**SAP user administration**

To perform user administration, you first create a user master record for each user, with which the users can log on to the SAP system. Using the user master record, assign one or more roles to the users, which determine the activities in the user menu and which authorizations the user has.

User master records are client-specific, so you need to maintain separate user master records for each client in the SAP system.

A SAP client can be configured across multiple SAP systems. You cannot transport user master records. Instead, you can copy them using a client copy, or use Central User Administration to distribute the user master records from the central system to the child systems.

**Central User Administration (CUA)**

Central User Administration (CUA) simplifies user maintenance in environments with multiple systems. One specific SAP client is promoted to be the master, and other clients are connected and assigned as subordinates to this master. These clients do not necessarily have to reside on the same SAP system.

It is worth noting that not all clients need to have a role in a CUA infrastructure. Individual clients may stay independent and keep their own user management repository.

Logical systems are created in a CUA for each client. Each of these logical systems represents one client. One logical system is selected to take over the role of a master, and the other logical systems act as subordinate logical systems.

**Figure 4.** You must maintain separate user master records for each client in the SAP system.
During the creation and configuration of a CUA infrastructure, all accounts and permission/entitlement objects are transferred and loaded from the subordinate logical systems to the master system. Changes to the core master set of accounts or permission/entitlement objects and their assignments are synchronized periodically to the designated subordinate logical system.

A master SAP account record is held in a master SAP client, and CUA maintains user master data towards child SAP clients. The information is asynchronously distributed to the child systems. In theory you should have an overview of all user data in the entire system landscape.

User account records are distributed asynchronously by the CUA between the application systems and its embedded clients.

The CUA topology runs as a hub and spoke service. One system in the Central User Administration is defined as the central or master system and is linked with every child system bi-directionally. Child systems have no link to each other.

SAP User Maintenance
SAP User Maintenance enables the creation, modification, disabling and deletion of accounts, as well as the assignment of permissions. To access User Maintenance, either following the path Tools —> Administration —> User Maintenance (as shown in Figure 6) or execute the transaction code “su01”.

The CUA topology runs as a hub and spoke service.
The first User Maintenance screen displays the mask shown in Figure 7.

**Account types**

SAP is aware of the following account types:

- **Dialog (A)**—This is the most common account type. It is typically generated for employees who work actively with SAP GUI or the Web Portal of SAP. During a logon of this type, the system checks the validity of passwords, initial values and multiple logons.
- **System (B)**—These accounts are typically used for internal communication or background operations, since they do not allow a dialog logon, such as SAP GUI. Furthermore, no checks on password or initial values are processed. Passwords are changed by administrative accounts.
- **Communication (C)**—This account type also does not allow dialog logons. It is typically used for communication between SAP systems or with third-party software via RFC.
- **Reference (L)**—Reference accounts are used as a kind of template for accounts with similar permissions. A logon is not possible with a reference account.
- **Service (S)**—A service account is used for anonymous logons of multiple users. Multiple dialog logons are possible. The system does not execute checks on passwords. Passwords are changed by administrative accounts.

**Permissions**

In SAP, permissions are controlled by an assignment of roles, profiles and groups to an SAP account. While direct assignments of profiles and groups have an unlimited duration, an account owns the permissions assigned via a role only for the specified duration. Multiple single roles can be grouped in a cumulative role so you can assign a cumulative role to an account instead of assigning multiple single roles.
Figure 8 displays an SAP account with assigned roles in the display mode of transaction “su01”.

Effective permissions
The previous section describes how a SAP account gains basic permissions. This section explains how the specific coherence of a role to an entitlement (such as the ability to write to a specific data field) is implemented in SAP.

First, it is important to understand the elements of a permission:
- **Transactions**—Programs.
- **Activities**—Activities are defined procedures which can be executed on a data set in SAP by an ABAP program. A simple example might be the entering of a new submission. If an ABAP program or function is able to enter a new data set record to SAP, it has to check in the code whether the account has the appropriate permissions to execute the “enter submission” program.

Transactions, activities and fields are system-wide objects, which mean they are valid cross-client.

The smallest available element in an entitlement definition is the entitlement object. It merges transactions, activities and fields. This object also contains information about which activities are allowed to be executed and which transactions and fields are assigned to it. An object can contain a maximum of 10 elements. One entitlement object is valid system-wide (cross-client).

The assignment of concrete values to the elements of an entitlement object is client-specific. These client-specific entitlement objects are also called distinct entitlement objects. A profile may contain up to 1000 distinct entitlement objects. Multiple profiles establish a single role, multiple single roles, or a cumulative role.

Figure 8. An SAP account with roles assigned
Identity Manager allows synchronization from SAP/HR and SAP/OM, as well as synchronization to SAP R/3 via Identity Manager Connector for SAP R/3.

<table>
<thead>
<tr>
<th>System</th>
<th>Client</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transaction&lt;br&gt;Transaction Field&lt;br&gt;Activity Activity Field&lt;br&gt;Activity Field Transaction</td>
<td>Entitlement Object 1&lt;br&gt;Entitlement Object 1 (distinct) Profile 1 Role 1</td>
</tr>
<tr>
<td>Field</td>
<td></td>
</tr>
<tr>
<td>Activity Activity Field Transaction</td>
<td>Entitlement Object 2&lt;br&gt;Entitlement Object 2 (distinct)</td>
</tr>
<tr>
<td>Field</td>
<td></td>
</tr>
<tr>
<td>Activity Activity Field Transaction Field</td>
<td>Entitlement Object 3&lt;br&gt;Entitlement Object 3 (distinct) Profile 2 Role 2</td>
</tr>
</tbody>
</table>

**Figure 9. Entitlement objects in SAP**

Figure 9 displays the single elements up to the indenture level "single role" with its scope and possible accumulations.

**CUA-managed access permissions**
A system entitlement in the context of CUA always refers to a specific logical system—that is, a client. An account created in the CUA without entitlement assignments is not able to log on to any CUA subordinate logical system. Only the assignment of entitlements enables accounts to log on.

**Role assignment in a CUA**
The assignment of single or cumulative roles to an account always requires the specification of the logical systems.

---

**Identity Manager Connector for SAP R/3**
Identity Manager allows synchronization from SAP/HR and SAP/OM, as well as synchronization to SAP R/3 via Identity Manager Connector for SAP R/3. The synchronization supports all the attributes and structural relationships of SAP user accounts, groups, profiles, roles and activity groups with Identity Manager as a central repository for the full and secure automation of administrative tasks and application security. In order to maintain the SAP user accounts, additional information required (such as available company addresses, Start menus or user types) is also read from the SAP system.
The connector is the technical basis for the automation of the standard processes for creating, deleting and editing the account and access permission objects in SAP R/3.

Identity Manager allows the administration of new groups, profiles, roles and activity groups, but usually these SAP objects are maintained in SAP directly and only synchronized into the central repository of Identity Manager. Only the data available in SAP R/3 is read into Identity Manager in order to assign the corresponding permissions to the SAP user accounts.

Architecture
Identity Manager synchronizes SAP bi-directionally. Only the BAPIs and RFC elements provided by SAP need to be activated in the connected SAP systems. Thus only the elements provided by SAP are used for communicating with the SAP systems. The exchange of data between the Identity Manager repository and the SAP systems is executed agentlessly; only a routing server operates as a secure transaction by http or by ftp or over an OLE-DB provider. The synchronization can be either time-driven or event-driven.

SAP certification
To ensure all functionalities implemented within the Identity Manager Connector for SAP, Identity Manager was certified by SAP on August 23, 2011. For more information, see the SAP Partner Information Center.

Technical interfaces
Identity Manager uses the SAP .NET connector for SAP for accessing SAP and supports all versions from SAP R/3 4.6 to Netweaver 7.11.

Identity Manager provides a business application programming interface (BAPI) coded in APAB and certified by SAP, which needs to be transported to an SAP system in order to use the connector. Since the BAPI is SAP-certified and shipped as a SAP transport file, it can be distributed by the standard SAP transport mechanisms.

This ABAP code is provided to:
- Retrieve data that is not provided by standard BAPIs of SAP, such as providing lists for synchronization, handling of analysis authorization and structural profile and maintain the PAS infrastructure
- Abstract the differences of SAP versions

On top of that layer, the Identity Manager process orchestration engine is used to execute provisioning and synchronization tasks.

Figure 10. Identity Manager uses the SAP .NET connector for SAP for accessing SAP. (Source: SAP, Marketplace Online)
Benefits of Identity Manager

Unified administration and security

Identity Manager empowers organizations to manage accounts and access permissions from a single instance by unifying disparate and sometimes disconnected entities in the IT landscape.

Although employees often have more than just one user account, SAP supports only a SAP account-centric approach, which cannot handle employees having multiple user accounts.

Identity Manager, on the other hand, provides a comprehensive approach that can manage logically disconnected SAP accounts and connect those SAP accounts to employee identities. This provides a full, business-driven view of the complete organization as well as IT-relevant data derived from the managed SAP systems.

Identity Manager provides integrated management of SAP, regardless of the complexity of the SAP infrastructure. In fact, the more complex the SAP system, the more benefits you gain by externalizing user and access permissions into Identity Manager.
Requests for SAP user accounts or assignment of permissions in various clients can be integrated in the IT Shop, the self-service interface of Identity Manager.

**Process integration**

The following SAP R/3 processes can be integrated in Identity Manager via the connector:

- Automatic creation of an SAP user account for an employee
- Automatic creation of an SAP user account for an employee through enabling a request or assigning a resource or through membership of a structural unit
- Automatic deletion after a grace period when an employee leaves the company
- Automatic changes to the SAP user account for change of name, relocation or transfer of assignment within the organization
- Full synchronization of the objects described, above including manual or automatic resolution of conflicts. Full synchronization means that equal status exists in Identity Manager and SAP R/3 with regard to the objects managed in Identity Manager. This means that differences such as:
  - An object exists in SAP R/3 but not yet in Identity Manager (it was created by bypassing Identity Manager)
  - An object exists in Identity Manager but not in the target environment (either it was deleted by bypassing Identity Manager, or the creation of the object was aborted). These objects, are collected and dealt with manually. A rule can also be defined to execute automatic creation or deletion in Identity Manager or in SAP R/3.

Requests for SAP user accounts or assignment of permissions in various clients can be integrated in the IT Shop, the self-service interface of Identity Manager. The accounting cost for the user accounts and permissions can be integrated in the Cost Management module.

Through a full synchronization, either of the following can take place:

- The creation of all SAP R/3 user accounts in Identity Manager
- The creation of only those accounts in SAP R/3 known objects in Identity Manager.

You can also specify whether only new objects are affected or whether all features of the objects already recognized in both systems are incorporated.

Some screenshots can be found in Appendix A.
Organizations operating User Maintenance up to date with a CUA are specifically forced to evaluate alternative solutions to replace their CUA for various reasons:

- The CUA concept has not yet specifically been “sunsetted” by SAP, but SAP shipped the last version of the CUA with SAP NetWeaver 7.1 and stopped any further investments in development and support.
- Customers are forced to switch theoretically to SAP Identity Management System.
- Feedback from the field shows us a huge gap of quality, functions and features between SAP IDM and Identity Manager.
- Organizations meanwhile identify and understand the value and benefit of an overall IDM concept regardless of any IT infrastructure focus.
- Any integration of non-SAP platforms, systems application and/or technology to be connected to is not core competence of SAP.

Structural profiles
With Identity Manager, you can manage existing structural profiles and assign structural profiles to user accounts either directly or with IT Shop request/approval workflows, which support compliance and access governance. Specifically, the SAP connector enables you to view and manage SAP HR structural profiles. Access levels can be defined in personnel master data or the organization chart to define structural profiles for the SAP HCM module. Access can be represented in terms of the organizational tree and can also be bound to dates.

Analysis authorization
With the Netweaver 7.0 platform SAP introduced new authorization management for their data warehouse product. Before that, the creation of profiles or roles for defining “who has access to which report” in combination with “which data is the user allowed to see in a report” was quite complex. This complexity is reduced by this new functionality.

Identity Manager allows the assignment of analysis authorization to user accounts.

Special processes with SAP R/3
In addition to connectors, pre-defined processes are fundamental components of Identity Manager. This applies particularly to the creating, editing and deleting of an employee and the subsequent effects on the configurations in SAP. For example, company address data in an SAP user account will be automatically computed from an employee’s location information.

SAP single sign-on with Dell SAP SSO
SAP supports single sign-on with Active Directory over the Secure Network Communications (SNC) protocol. This requires a special SAP GUI on the SAP side, provided by Dell Software with Authentication Services for SAP. Furthermore, a mapping of the SAP user account with an ADS user account must be stored in SAP for each user.

Since both user accounts are known to Identity Manager, Identity Manager automatically generates the corresponding mapping. Single sign-on is therefore ensured without the need for any additional maintenance in SAP administration.

License management
SAP user licensing is usually carried out on the basis of a “system measurement.” This means that an employee can have several SAP user accounts in various SAP clients, but only the most-privileged account requires an SAP license. All the other user accounts can be identified as “multi-client users” and contain a reference to the user account that is licensed.

Based on the significance of SAP roles, groups and profiles, Identity Manager will determine the most significant SAP account of an employee and assign the proper license to the user account. The results of an SAP license measurement within Identity Manager can be published into the SAP system environment and will ensure proper licensing with SAP.
Locking of non-active users
A widely used scenario is the process of locking user accounts that have not been logged on to the system for a certain period (of typically 90 or 100 days). Using Identity Manager you can configure this process to be scheduled daily and lock user accounts by changing the respective attributes (typically using the SAP user attributes U_Flag and Gltgb).

Special features for synchronization with SAP CUA
If there is a Central User Administration (CUA) System in place, Identity Manager needs only a connection to the CUA system. The management of users and permission within all connected clients is done by the Application Link Enabling (ALE) distribution model of SAP R/3. An existing CUA will minimize the implementation time for complex SAP environments, providing real value with a fully integrated and managed SAP environment that can include several SAP systems.

Auditing and reporting
You can use the audit function from Identity Manager to:
• Define rules for any employee assignments
• Evaluate the risk of possible rule violations
• Specify mitigating controls
• Initiate regular or spontaneous rule checks
• Detailed testing of edit permissions for employees within an SAP client (using SAP functions)
• Evaluate rule violations with differing criteria
• Create reports about rules and rule violations

Based on this information, you can make corrections to data in Identity Manager and transfer them to the connected target systems. The integrated report function in Identity Manager can be used to provide the information for the appropriate tests.

Support for the RFC call RFCReadTable
Using the Identity Manager connector supports the RFC call RFCReadTable which enables easy reading any data from SAP tables that are enabled for being read by RFC. Many tables are enabled by default, and additional tables can be enabled using the SAP GUI.

Figure 14. The SAP GRC module executes rules only on single independent SAP accounts.
Critical access and segregation of duties (SoD)

SAP’s rule checking
Compliance rule checking, segregation of duty and company policies are necessary to ensure corporate compliance. The following are several simple rule examples:

• An employee may not obtain two entitlements A and B at the same time.
• Only employees with a particular department can have a particular permission.
• Every user account has to have a manager assigned to it.

SAP provides a Governance, Risk and Compliance (GRC) module for rule checks. This framework executes rules, which have to be configured up front within SAP (see Figure 14).

The main disadvantage of the SAP GRC module is that rules are executed on single independent SAP accounts, without any reference to business dependencies within the SAP system landscape. Any relationship to other SAP accounts, such as a superordinate employee identity, is not included in GRC rule calculations; therefore the risk is high that violations will not be detected.

Identity Manager’s rule checking
Identity Manager closes this gap by including the SAP account relationships to employee identities within the Identity Manager repository, as illustrated in Figure 15.

The biggest advantage is the exploration of rule conflicts on the business level, which would have never been noticed by a singular rule check execution on single SAP accounts. The more target systems managed, the greater the benefit this approach provides.

For example, in one customer situation, an SAP GRC rule execution claimed only 634 violations, whereas Identity Manager was able to prove 16,993 violations within the same application infrastructure across individual accounts and entitlement assignments, focusing on the organizationally logical superordinate employee identity.

Any relationship to other SAP accounts is not included in GRC rule calculations; therefore the risk is high that violations will not be detected.

Figure 15. Identity Manager includes the SAP account relationships to employee identities.
Identity Manager’s rule checking by profile, role and user

The Identity Manager connector can also read all the information from SAP required to define GRC “abilities,” or fine-grained permissions in SAP. An ability is defined by transactions and authorization objects (such as whether a user can create an invoice) and value definitions for attributes of an authorization objects (for example, the user can create invoices only for customers A and B). Those fine-grained permissions are the defining elements of a profile, which can be assigned to user account or first combined with roles and then assigned to user accounts.

Identity Manager reads:
- All base data in SAP that is required to create abilities
- The fine-grained definition of profiles

Based on this information, critical access and SoD rules can be defined and a check for rule violations by profile, role and user can be executed. Some screenshots can be found in Appendix B.

Identity Manager’s checking of effective user edit permissions

Apart from the rule-checking options already described, Identity Manager offers very detailed checking of effective user edit permissions for the target system SAP. By linking SAP users to employees, combinations of SAP authorizations that an employee obtains via different SAP users can be checked. Potentially dangerous SAP authorizations and combinations of them can easily be recognized this way and the necessary action taken.

SAP authorizations are tested on the basis of permitted transactions for an SAP user and the associated authorization objects. To do this you have to define the transactions and authorization objects you want to check as SAP functions in Identity Manager. Use compliance rules to check whether the SAP functions are permitted in this combination for an employee. An SAP role matches an SAP function if the SAP profile for that SAP role contains at least one of the transactions that are defined in the SAP function. To do this, the SAP profile must have all the authorization objects for this transaction. If a function element with a list of several instances is defined for an authorization object, the SAP profile matches the SAP function if it has at least one of these instances.

All SAP groups, SAP roles and SAP profiles that have either of the following authorizations are determined by the SAP function shown in Figure 16:

![Figure 16. Identity Manager offers detailed checking of effective user edit permissions for the target system SAP](image-url)
• Transaction 1 with authorization object 1, function elements 1 AND 2
• Transaction 2 with authorization objects 2, 3 AND 4 and function elements 3, 4, 5, 6, 7 AND 8, where function element 8 has the instance “DOKU-BG-DD” OR “DOKU-BG-B”.

Authorization editor
Identity Manager’s Authorization Editor (see Figure 17) allows you to create specific SAP rules in terms of GRC. The look and feel is similar to the SAP GRC module. Use the Authorization Editor to set up the SAP function authorization definition. To do this, group transactions and authorization objects together that should be covered by the SAP function.

Identity Manager creates the configuration authorization objects in the context of the executing SAP Account.

Cross-platform SoD and compliance
Companies have different requirements for regulating internal and external employee access to company resources. They also have to demonstrate that they adhere to legal requirements. Such requirements can be defined as policies and identity audits. For example, access to “strictly confidential” files should be prevented in directories that can be accessed by “Everyone”; perhaps user accounts that are not members of a particular Active Directory group should be prevented from accessing a particular file directory; or administrative permissions for one employee in different platforms or applications are contradicting administrative policies.

Identity Manager enables you to manage these company policies and to conducts identity audits to assess the risk involved. Assuming the appropriate data is stored in the Identity Manager database, Identity Manager discovers all company resources that violate your company policies.

You can also define rules and policies for the purpose of providing reports that do not have any connection with Identity Manager. Adherence to company rules and policies is checked regularly using scheduled tasks. You can incorporate company policies into your regular company resource attestation to decide on further handling. Risk assessment can be run for all company policies. Different reports and statistics provide you with an overview of violated policies.

Identity Manager is able to execute SoD rules and conflict definitions (company policies) cross-platform, to set different individual conditions of individual accounts in the context of the organization and business-related compliance rules originating from the business object “Employee Identity” regardless of the underlying technology.

Identity Manager’s Authorization Editor allows you to create specific SAP rules in terms of GRC.

Figure 17. Identity Manager’s Authorization Editor
Identity Manager makes it possible for every employee in a given department to have the same permissions consistently.

Other functions based on the Identity Manager architecture

- **Administrative options with Identity Manager**—Identity Manager provides a comprehensive role management module which can be used to assign technical SAP roles and profiles to user by defining business roles and assigning role memberships. The role management capabilities do not allow just the definition of business roles; they also allow organizational structures to be mapped in Identity Manager, through which permissions managed in SAP can be administered on a role basis. This makes it possible for every employee in a given department to have the same permissions consistently; even a change of department is automatically changed and logged according to the role definition. Through the specification of the SAP systems and the clients in Identity Manager, several SAP systems can be simultaneously managed independent of each other. This lets standard processes be uniformly established in all environments.

- **Abstraction of the role description for the administration and the IT Shop**—SAP permissions usually have very technical descriptions that are not easy for end users to interpret. Moreover, several permissions are often required to execute tasks in SAP. With Identity Manager, several SAP permissions (even across clients) can be taken at an abstraction level and combined into SAP “products.” These SAP products can then be directly assigned to the employees or granted according to affiliation with an organizational unit.

At the same time, instead of offering the end user unidentifiable/unclear permissions in the IT Shop, this abstraction can be used to offer identifiable products with descriptions that are comprehensible for the end user.
• **Flexibility through the use of process chains**—Identity Manager uses process chains, which can be composed of any number of individual steps that are connected together. Process chains are stored in the Identity Manager repository. A very simple mechanism allows customized requirements to be displayed as process images.

• **Employee Self Service**—Employee Self Service can the following tasks:
  - Requesting, authorizing and setting up an SAP R/3 user account, or deleting it
  - Requesting, authorizing and subsequent assignment of a permission in SAP R/3, or deleting it

• **Risk management**—SAP groups and user accounts are integrated in the risk management functionality of Identity Manager. Each entitlement can be assigned a risk index. Based on a schedule the risk index of the user account is calculated from the risk indices of the assigned entitlements. Also calculated is the risk index of identities (employees) based on the risk indices of the entitlements assigned to user accounts related with the identity. Therefore, at any time each manager knows the risk index of his or her direct reports.

• **Audit trail and reporting**—All the information on SAP is available for the comprehensive reporting engine in Identity Manager. Reports can be requested on an ad-hoc or subscription basis. Subscribed reports are created by schedule and then sent by email or stored in a file system. And since all changes can be stored in Identity Manager using the TimeTrace engine, reports can be used to provide the historic information on all changes in terms of “in which period was a user assigned to a role.”

• **Status tracking**—Identity Manager provides a smooth architecture for tracking the status of all provisioning processes activated. Activities comprising several steps can be combined into a status step and linked with a “master process.” Even non-technical users are therefore continuously aware of all the process steps they have activated. Of course this information can be altered to suit specific organizational requirements in order to respond quickly and flexibly to special needs.

**Synchronized objects**

Objects read from an SAP system
- List of clients
- Available license definitions
- SAP BI users (BI systems only)
- SAP BI analysis authorizations (BI systems only)
- Structural profiles (HR systems only)
- External IDs

Objects read per client
- User accounts
- Groups
- Single profiles
- Composite profiles and their single profiles
- Single roles and their profiles
  - Transactions, authorization objects and field values that define a profile (for SoD checks)
  - All lookup data required for field values (for creation of abilities used in SoD or critical access checks (USOBT, USOBJ) and related tables;
- Composite roles and their single roles
- Start menus
- Company entries
- Cost centers
- Printers

**Provisioning objects**
- Create, update and delete user accounts (attributes) Assign profiles and roles to (or remove them from) user accounts (including validity range)
- Assign analysis authorizations to user accounts
- Assign structural profiles to (or remove them from) user accounts

**Remarks**
- Provisioning and reading works with SAP Central User Administration as well.
- Exception: licensing is not implemented for CUA.

---

SAP groups and user accounts are integrated in the risk management functionality of Identity Manager.
Delivering business value

Scenario 1: User lifecycle management at a large bank
A large bank was struggling to manage employee permissions and access rights that change on a regular basis. Now, Identity Manager delivers automated and timely user provisioning for employees based on their membership to business units. This ensures that employee access is managed without providing more or less access and permission than needed in any given position.

The key benefits this customer has achieved with the Identity Manager Connector for SAP are:
- Provisioning SAP user accounts with appropriate access permissions for new employees on time and within a staged SAP environment
- Ensuring compliance by providing only the necessary access permissions based on the business unit membership of the moved employee
- Optimizing the value of licenses with SAP by de-provisioning SAP user accounts immediately when an employee leaves the company keeping all historic attribute values and permission assignments within the Identity Manager database for reporting in case of internal or external audits

Scenario 2: Enhancing business roles with SAP for a large financial services company
A financial services company needed to manage roles and provide a front end for access requests from end users. Identity Manager’s IT Shop was an ideal solution, providing a simple, intuitive interface for users to request access to the SAP system, SharePoint and other systems.

With Identity Manager as a single point of access to the end user, complex business roles are managed and the access for a particular role is automated by kicking off the necessary approval workflow before access is granted.

The key benefits this customer achieved with Identity Manager are:
- Allowing end users themselves to request access as needed
- Automating the approval process so that it is more efficient, documented, and reportable for audit purposes
- Managing roles as a dedicated set of distributed permissions assigned to user accounts within several systems

Identity Manager delivers automated and timely user provisioning for employees based on their membership to business units.
Appendix A: Screenshots of SAP user management in Identity Manager

Figure 19. SAP user account overview

Figure 20. SAP user account master data
Figure 21. SAP user account login data

Figure 22. SAP user account communication data
Figure 23. SAP user account defaults

Figure 24. SAP user account license information
Figure 25. SAP user account SNC mapping (SSO with Active Directory)

Figure 26. SAP entitlement (composite role, single role, composite profile, single profile) overview
Figure 27. SAP entitlement master data

Figure 28. SAP entitlement, assignment of user accounts
Figure 29. SAP defined rights

Figure 30. SAP maintains SoD rules
For More Information

© 2013 Dell, Inc. ALL RIGHTS RESERVED. This document contains proprietary information protected by copyright. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose without the written permission of Dell, Inc. (“Dell”).

Dell, Dell Software, the Dell Software logo and products—as identified in this document—are registered trademarks of Dell, Inc. in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners.

The information in this document is provided in connection with Dell products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Dell products. EXCEPT AS SET FORTH IN DELL’S TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, DELL ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL DELL BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF DELL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Dell makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Dell does not make any commitment to update the information contained in this document.

About Dell Software
Dell Software helps customers unlock greater potential through the power of technology—delivering scalable, affordable and simple-to-use solutions that simplify IT and mitigate risk. The Dell Software portfolio addresses five key areas of customer needs: data center and cloud management, information management, mobile workforce management, security and data protection. This software, when combined with Dell hardware and services, drives unmatched efficiency and productivity to accelerate business results. www.dellsoftware.com.

If you have any questions regarding your potential use of this material, contact:

Dell Software
5 Polaris Way
Aliso Viejo, CA 92656
www.dellsoftware.com
Refer to our Web site for regional and international office information.