SAP NetWeaver® Identity Management Identity Center

White Paper

September 2007

SAP NetWeaver®
Identity Management 7.0 - Identity Center

Table of contents

Executive summary

As companies face the challenge of managing identity information, they must implement a technology solution that will help them strengthen business relationships, meet regulatory requirements and create efficiencies that sustain financial viability.

SAP NetWeaver Identity Management is a suite of products that helps organizations handle the complex requirements of identity management by offering provisioning, workflow, password management, reconciliation and meta directory functionality in a single, vendor-neutral software solution. SAP NetWeaver Identity Management's modular approach allows an organization to deploy the entire identity management stack all at once or deploy the components in phases to meet the organization's need for process management and cost control.

Building on the features supplied with the Identity Center, managers can provide value and return on investment and achieve buy-in from senior executives. The Identity Center reduces the cost of managing your applications and enables you to deploy new applications in a timely manner.

The architecture of the Identity Center is designed to provide maximum flexibility, scalability and security in a single software solution. This allows identity management across multiple applications and databases both within the organization and in an extranet environment.

The Identity Center offers a complete range of identity management functions:

- Workflow
- Rules- and roles-based provisioning
- Meta directory
- Password management
- Audit and monitoring

Identity Center

Background

Corporations today face increasing complexity and accelerating global, economic, and technological change. Historically, the goal of IT departments has been to deploy new applications, maintain and manage networks, and ensure that only employees had access to valuable corporate assets. Today, however, customers and partners expect similar access, and in many cases businesses are requiring partners to use corporate systems for information, resource planning and asset allocation planning. This bilateral push and pull across the traditional perimeters of business and business relationships has blurred the line marking where the enterprise ends and where customers and partners begin. Adding to these challenges is the growing number of internal and external systems any one organization may have and the increasing number of people whose details must be added to, deleted from and managed within these systems. As a result, identity management has become a key concern for all members of the business community.

In addition to the increased demand for data access, new regulatory compliance requirements call for a high level of corporate vigilance in tracking and auditing this data. Two prominent examples of these requirements are the Health Insurance Portability and Accountability Act (HIPAA) and the Sarbanes-Oxley Act. Both of these laws mandate tight control of corporate information, strict accountability for data access, and secure maintenance of personal identity information. The administration is required to prove that they are in control of access to applications. This proof will require reports to be produced showing who is allowed access, and who granted this access, as well as proving that previous employees no longer have access to the applications.

As companies face the challenge of managing identity information, they must implement a technology solution that will help them strengthen business relationships, meet regulatory requirements and create efficiencies that sustain financial viability.

In most organizations today, there is an abundance of applications that are unaware of each other, and each of these maintains its own set of identity data. This data includes, but is not necessarily limited to, authentication and authorization information for the application. The organization spends heavily on resources to maintain all this duplicated identity information. There is always a risk that this information is wrong, which may result in people getting access to information and applications for which they are not authorized.

Purpose

The Identity Center is used to provide control of all identities within the organization, not only for employees, but also for contractors, customers, partners and other identities that need to access the organization's applications.

Using the Identity Center will improve the overall quality of the identity information within the organization. The solution proves who has been granted access, and who approved the access. It can be configured to connect to any number of different applications, and to ensure that the identity information is correctly updated in each of these applications. In addition, the web-based workflow can be used to define an approval process before access is granted or other operations are performed.

Highlights

The Identity Center includes features for streamlining processes, automating redundant tasks and providing comprehensive views of current and historical information. This enables organizations to make quicker business decisions, save vital corporate resources and move ahead of the competition.

Roles- and rules-based provisioning and workflow

Automating workflows and provisioning tasks reduces the many time-consuming manual jobs of IT administrators. A single source for information flow makes it possible to produce a detailed audit supplying security personnel with information including the date and time an account was created or updated, the user who authorized the account, and the content of the account before it was changed.

When users leave an organization, the workflow process can be configured to disable and delete user accounts, with the appropriate authorizations in a specified time frame. Deprovisioning is of immeasurable value for organizations that employ short-term contractors, provide guest accounts for visitors, or wish to avoid the risks associated with orphaned accounts in general. Adding workflows, tasks and escalation procedures to the deprovisioning process provides intelligence to assure business rules are followed even during disable and delete events.

Comprehensive reporting, auditing and logging

The Identity Center's extensive and customizable audit trails report the number of transactions, transactions in the queue and details on users and accounts, among other information. Organizations can supplement the built-in reports supplied with the product with third-party database reporting tools to gain an even deeper insight into current and historical data.

The Identity Center includes the necessary state information as well as historical information to generate the necessary reports to prove compliance.

Password management

The Identity Center supports password synchronization, taking great care not to expose the passwords.

The Identity Center enables password recovery both from the workflow web interface and by using a specialized kiosk solution.

Reconciliation

As important as provisioning is ensuring that the actual state matches the provisioned state. In many cases, a system administrator may change the access control directly into an application, to give a person with urgent need to this application access. However, this may violate organizational security, and reconciliation will detect any such changes. If inconsistencies are found, this may trigger a workflow process to reset data to a consistent state, or a report may be generated and sent to a manager.

Integration with Microsoft Identity Integration Server (MIIS)

The integration with the Identity Center and MIIS extends the MIIS solution by offering web-based request and approval processes reflecting the company's business processes.

For details, see the white paper *SAP NetWeaver Identity Management Identity Center - MIIS Integration*.

System architecture

The architecture of the Identity Center is designed to provide maximum flexibility, scalability and security in a single software solution. This allows identity management across multiple applications and databases both within the organization and in an extranet environment. The Identity Center manages all of its activities from a core database and supports both Microsoft SQL Server and Oracle. All components in the solution interact with the database to ensure that all identity management activities are properly executed.

Some characteristics of the architecture:

- **Technology independence.** The Identity Center can run both on Microsoft Windows and Unix/Linux platforms, using either Oracle or Microsoft SQL Server as the central repository. Any type of repository can be accessed.
- **Persistence and fault tolerance.** The Identity Center has strong focus on persistence and fault tolerance. This ensures that no data is lost or corrupted if system failures (such as network problems or power glitches) occur. A persistent state is always kept in the identity store.
- **Optimized data handling.** The Identity Center has several mechanisms for ensuring optimized handling of large amounts of data. The advanced delta mechanism is used to ensure that only changed data is written to the target repositories, while event agents can be used when reading data, to ensure that only changes are read.
- **Non-intrusive.** Using the Identity Center to retrieve information from applications is non-intrusive. In many cases, there is no need to make any changes at all to existing applications to get access to the data.

The architecture of the Identity Center can be illustrated in the following way:

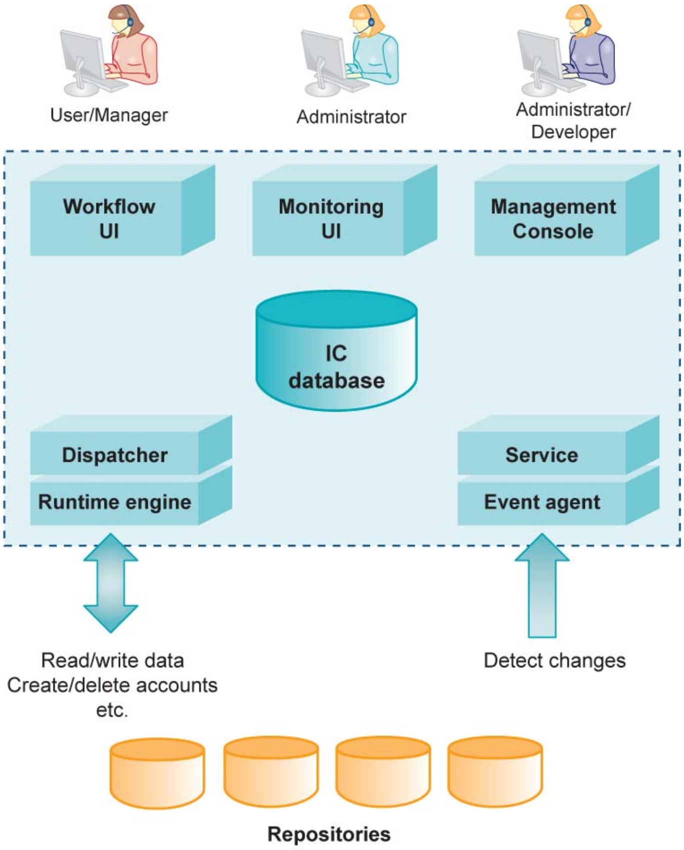


Figure 1: System architecture

The Identity Center consists of the following components:

- **IC database:** All information about provisioning/workflow tasks and jobs, the identity store, scheduling information, state information and audit/logs is kept in this passive store.
- **Dispatcher / Runtime engine:** These components act as local or remote agents for the Identity Center and are responsible for processing both provisioning and synchronization tasks. They are also responsible for performing reconciliation and bootstrapping. Multiple pairs of dispatcher/runtime engines can be used and dedicated to running specific types of jobs.
- **Service / Event agent:** An event agent can be configured to take action based on changes in different types of repositories such as directory servers, message queues or others. The event agent will detect changes and submit information to the Identity Center. The dispatcher will then initiate execution of a given job. This mechanism is optional and its only purpose is to initiate synchronization based on changes in repositories in addition to the scheduled operations.
- **Workflow UI:** The Workflow web interface is used for all end-user registration/self service, password resets and approval of tasks.
- **Monitoring UI:** The Monitoring web interface is used to provide an overview of the system status, audit and logs during daily operations.
- **Management console:** The Design user interface is used for configuring the Identity Center, including provisioning/workflow tasks and jobs.

Identity store

The identity store of the Identity Center is based on a relational database, but has a dynamic data schema, which allows for new attributes to be added to entries on the fly, even automatically, if this is desired.

The data within the identity store is based on entries, and can be arranged in a hierarchy. All changes are transaction based, so if any error or data violation occurs, all changes are rolled back.

A powerful feature of the identity store is the ability to save old values of data, either a number of days or a number of revisions, which can be defined on a per-attribute basis. Events can be defined on any attributes or entry, which can fire up a task whenever an attribute or entry is added, modified or deleted.

To avoid data synchronization, it is possible to leave data in its original repositories with a pointer to the data directly from the identity store. When a user or process requests the data, the Identity Center will retrieve it automatically and transparently.

Expiry time can be defined on any attribute value, and upon expiry the attribute is automatically deleted. At this time, any defined events will be executed. This can for example be used for time-limited privileges.

The Identity Center supports a multi-master attribute model. This includes attribute precedence; if the same attribute is present in multiple repositories, it is possible to define that one repository has precedence over the others.

Main features of the Identity Center

The Identity Center offers a complete range of identity management functions:

- Workflow
- Provisioning
- Password management
- Meta directory
- Logging and reporting
- Regulatory compliance

Workflow

The Identity Center enables businesses to automate the identity management process in accordance with company policies and procedures. Provisioning is the process of automatically executing pre-configured tasks in a specified order. Workflow is the process of breaking down the business operations into provisioning tasks.

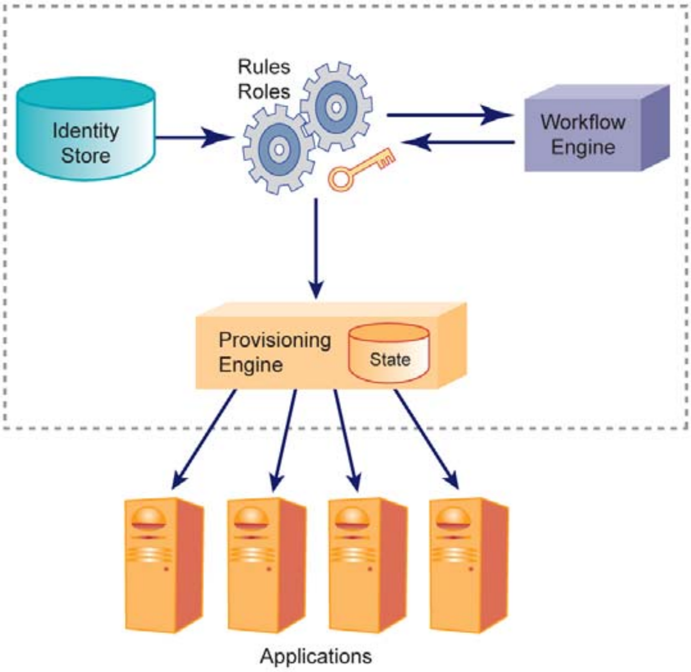


Figure 2: The workflow process

The Identity Center's workflow is designed and configured through a feature-rich graphical user interface and is tightly integrated with the identity store. A workflow is started every time a provisioning request is initiated. The Identity Center workflow can be used to:

- Collect identity information from the specific individuals.
- Enforce single- or multi-stage approvals from authorized personnel.
- Generate notifications to designated users when manual actions need to be performed, or report the outcome of completed tasks.
- Execute new workflow tasks (such as notifications and escalation) when pre-defined time-outs are reached.

Approvals

Approvals are an important part of the workflow process, performed either in sequence or in parallel. Each approver may also be required to add additional information about the user being approved.

Approvals are configured as part of the workflow tasks. Approvals can be used as a manual step in a workflow or as a way to collect identity information.

The authorization mechanism enables routing of approvals to the appropriate persons. When identity information is collected, attributes can be configured as mandatory or optional.

Approvals can be used in several ways:

- A workflow can be set up to make sure all necessary information is available before a user is provisioned to a connected system.
- Approvals can be used as work orders for a manual operation such as "order cell phone" or "assign office space".
- Approvals can be configured so that one out of a number of users could approve a request and/or a series of approvals must be given before the workflow can continue.

Provisioning

The Identity Center has powerful provisioning mechanisms, based on a task hierarchy. All provisioning operations are configured from the management console, which provides facilities for debugging and error tracking. During provisioning, all changes are stored in the database, ensuring data consistency.

Roles- and rules-based provisioning

When implementing a provisioning solution, you can use two different provisioning mechanisms:

- Roles-based provisioning
- Rules-based provisioning

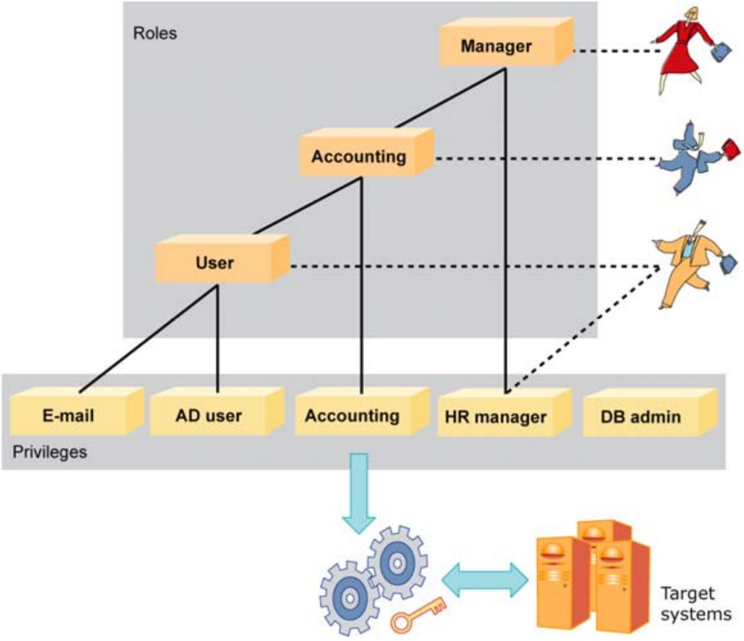


Figure 3: Roles- and rules-based provisioning

Roles-based provisioning

The Identity Center supports the use of roles to assign privileges to users. A role hierarchy can be defined where each role can be assigned any number of privileges.

By assigning one or more roles to a user, the necessary provisioning is done automatically for this user, to grant access or set other information in the required applications. When roles are removed from a user, deprovisioning will ensure that the privileges are removed.

Normally, only a limited number of roles should be defined, and these should be used to handle 80% of the privilege assignments. To handle the remaining 20%, rules should be the preferred method, although direct assignments are also possible.

The use of temporary roles is also supported for cases where a role should be assigned for a limited time. Consultants or contractors often work with the organization for a limited time, and for security (and compliance) reasons it is important to ensure that their accounts are removed when they are no longer in use. For this purpose, a role can be defined with a time limit, and when this time limit is reached, the account is automatically deprovisioned.

Rules-based provisioning

Some users need privilege assignments which do not easily fit into the roles. These can be assigned by defining rules. In this case, if a user entry matches a given set of rules, a privilege is assigned and thereby also the required provisioning.

Rules in the workflow process are used to transform business decisions into actions performed on connected systems, according to predefined rules. This removes unnecessary human interactions in the user and profile administration process.

Flexible rules can be defined to achieve branching in a workflow process. For example, it can be based on location: *If location is New York, add user to server X. If location is Los Angeles, add user to server Y.* In this way the management process is simplified - a manager can initiate provisioning and let the system make all the logical decisions that follow.

In a more complex example, a provisioning task creates mailboxes in Microsoft Exchange. Rules are defined to create the mailbox in the server at the closest location and to select the server with the least load (using the API).

Explicit and implicit provisioning

There are two ways to initiate provisioning:

- Explicit provisioning
- Implicit provisioning

Explicit provisioning

Provisioning and workflow can be initiated explicitly, for example a user requesting a resource from the web interface. This can also (if authorized) be done on behalf of other users.

In addition, external applications can initiate provisioning and workflow.

Implicit provisioning

It is possible to assign specific tasks to attributes and entries within the identity store. This means that whenever a value changes within the identity store, this will automatically start provisioning. This can for example be used to provision access control based on change of location for a user.

Delegating provisioning tasks

The right to execute provisioning can be delegated to users in two ways:

- Self-service
- Delegated administration

Self-service management

The Identity Center's authorization mechanism can be configured to allow end-users to execute a set of tasks that influence *their own* system profile. This may include changing profile attributes, requesting an account or creating access rights settings.

End-users may be granted rights to reset passwords and synchronize them across applications (reducing the need for remembering multiple passwords). Also, it is possible to give the users the rights to request access to new applications or order non-IT resources. This reduces administration costs as well as the costs associated with helpdesk operations.

Delegated administration

As part of the configuring task properties, administrators can delegate user administration and profile management to business units, partners, customers and others. This is accomplished using the authorization mechanism in the workflow.

In addition to enabling internal employees to do their job more efficiently, it gives customers, partners and other external users the possibility to manage their own accounts. Giving non-IT users the possibility of managing access rights and user profiles also reduces administrative costs, provides timely access to essential resources and helps employees perform more efficiently.

Password management

Password management is an important part of identity administration. This is an expensive task for most organizations since it usually requires a help desk staff to respond to requests about forgotten passwords in different systems. While maintaining security is always a priority, a balance must be struck between secure password handling and simplicity for end users.

There are different methods for password management:

- **Automatic:** Passwords are set automatically from an authoritative system to other systems in the enterprise. This is accomplished by adding password-change trapping mechanisms that will set the changed password in designated systems. This is often referred to as password synchronization.
- **Self-service**: Passwords are changed and reset by end-users. In such cases the end-user can change his or her password in a central system normally accessed through a web interface. To resolve forgotten passwords, end-users can be authorized by requesting other information which is specific to this user and by which the user can be identified.
- **Delegated:** Passwords are set or reset by authorized persons for other end-users. This will normally be done by managers or help desk persons through a web interface.

The Identity Center offers functionality for supporting all three scenarios. Password trapping will support password changes in Microsoft Active Directory only.

Password recovery

Many helpdesk calls concern forgotten passwords. The Identity Center includes a kiosk solution for resetting lost passwords.

A user who forgets his/her password can log on with a given user name and reach the Workflow's password recovery task without gaining access to any other resources. This provides a secure way for recovering passwords without assistance from a helpdesk or another internal service desk.

The kiosk solution is implemented by creating a new policy in Active Directory connected to a single account that is used for reaching the password recovery task. The security settings of the policy prevent the user from opening other web pages, or starting other programs. After recovering the password, the user logs out and logs in again using his/her normal user name and the recovered password.

Meta directory

The core component of the Identity Center is the identity store, which serves as the central repository for all identity information in the organization.

To build a central repository of organization-wide identity data, the meta solution goes through the process of extracting, normalizing, synchronizing, joining, transforming and publishing all identity data contained in the existing repositories, thus creating a uniform view of the data. The identity store that results from this process is a vital part of the organization's infrastructure, which is then used for other business applications, such as provisioning or authentication.

The identity data collected from the various data sources is joined to create unique entries for each user (who may be an employee, customer, partner or other user as defined by the organization). The synchronized data may then be transported back to the identity repository of each application. This maintains data integrity between the identity store and each application, ensuring that each user is uniformly identifiable across all applications.

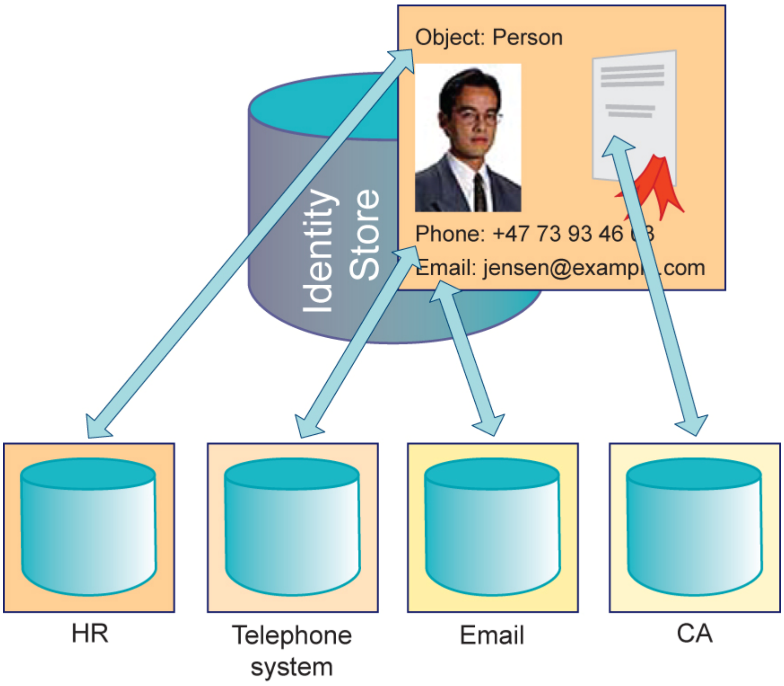


Figure 4: The meta solution

The Identity Center offers a meta solution that is robust, flexible, and technology independent with support for high availability and load balancing. It does not require any changes in the existing infrastructure or investment in expensive proprietary interfaces. Therefore it stands out as an efficient meta solution that provides administrative cost savings, enhanced data integrity and increased information security.

Reconciliation

A highly refined process of data reconciliation is essential when sharing identity information between multiple applications across a large organization, as well as playing an important role in proving regulatory compliance. The Identity Center provides this reconciliation by managing the exchange of identity data between applications, and between those applications and the identity store.

While the Identity Center provides a single interface for making updates across all applications, data changes can still originate from any single application's source. For example, a local administrator can edit key data directly in an application, creating an account without the identity management system being aware of this. Such changes are sometimes called "wild cowboy" operations, and require that reconciliation takes place between the "source" (in this case the identity store) and the "target" (the application that was accessed directly by the administrator).

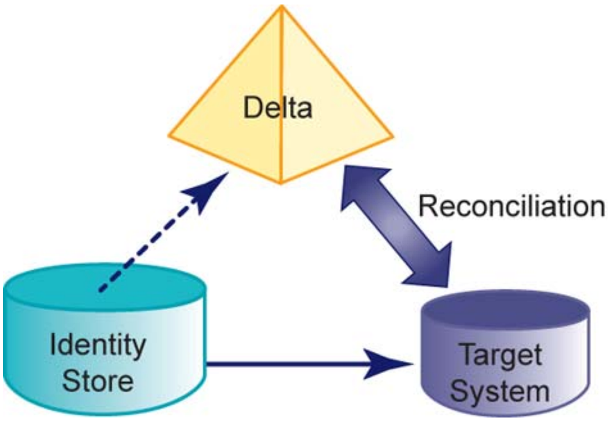


Figure 5: Reconciliation

When differences are detected, the two systems must be adjusted. It must then be decided which of the systems should be the master. Is the source or target data correct?

There are several ways to handle this:

- Data inconsistencies can be reported to administrators, who may then perform manual adjustments.
- Company policy says that source data is deemed authoritative and target data should be adjusted automatically.
- Company policy says that target data is deemed authoritative and source data should be adjusted automatically.
- Workflow tasks may be defined and initiated for each scenario. These tasks can include approvals and decision processes to ensure that the correct action is taken.

The last alternative is recommended for adjusting the data, but this decision rests with the individual organization.

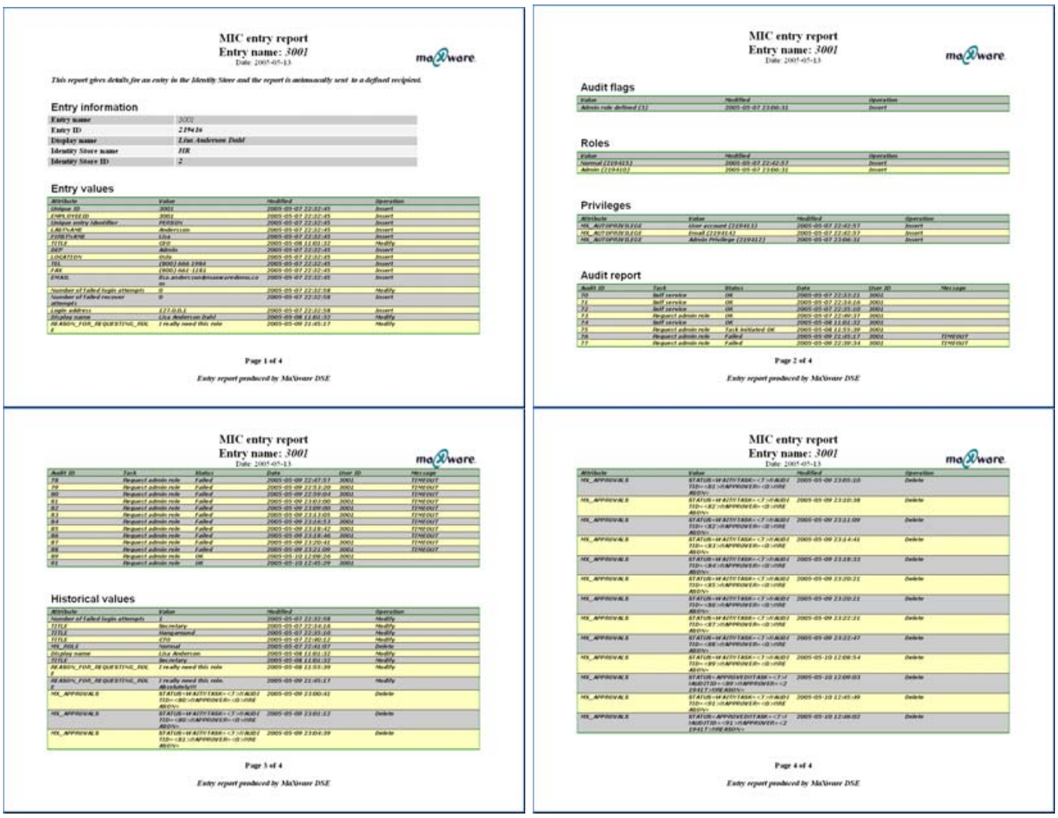
When a provisioning system is put into production, all connected repositories need to be reconciled with authoritative data ("bootstrapping"). This uses the same mechanisms described for reconciliation.

Logging and reporting

The requirements for proving regulatory compliance are becoming increasingly important; management must prove that they are in control of their organization, especially for IT systems. This means proving that the right people are allowed in, while others are kept out. For this purpose, the Identity Center can be used to set up a provisioning system for granting and denying access to the applications within the organization. In addition, the Identity Center provides auditing and logging features that can be used to document compliance.

Basic reporting

A set of templates for generating reports is delivered with the Identity Center. It is easy to produce reports for other purposes. One example is reporting on a single individual, showing the current values, as well as any historical values. It is also possible to report on roles and privileges, to see who has which roles, and who has been granted which privileges.



MIC entry report
Entry name: 3001
Date: 2005-05-13

This report gives details for an entry in the Identity Store and the report is automatically sent to a defined recipient.

Entry information

Entry name	3001
Entry ID	219416
Display name	Lisa Anderson Dahl
Identity Store name	HR
Identity Store ID	2

Entry values

Page 1 of 4

Entry report produced by MaXware DSE

Audit flags

Roles

Privileges

Audit report

Page 2 of 4

Historical values

Page 3 of 4

Page 4 of 4

Figure 6: Reports

System report

The system report feature of the Identity Center allows you to automatically generate a complete report as a Microsoft Word document. This contains all configuration information for the whole or any part of the Identity Center.

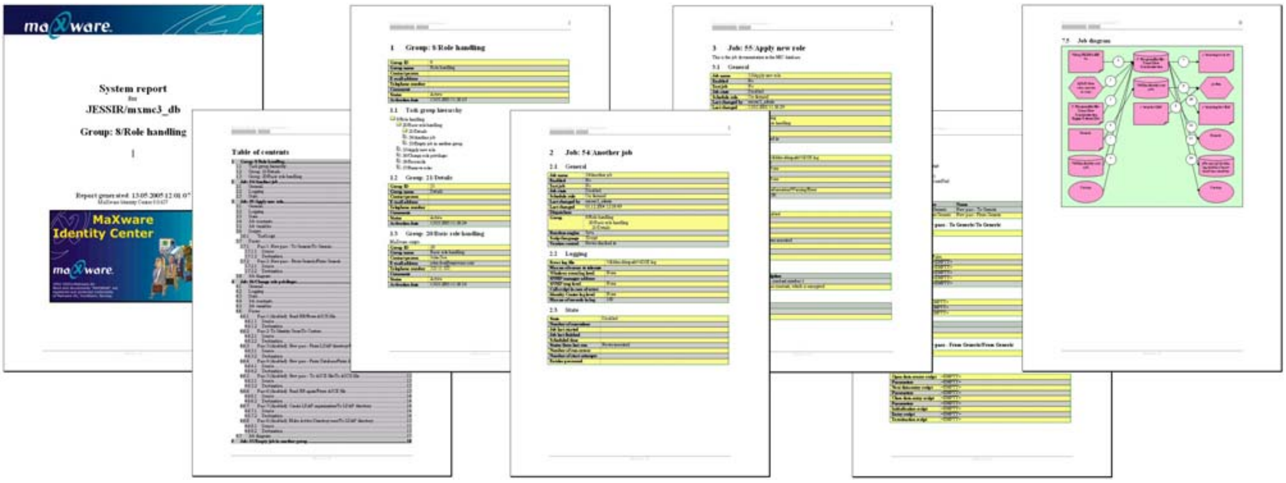


Figure 7: System report

Regulatory compliance

As a result of many financial frauds, the US Congress passed the Sarbanes-Oxley Act of 2002[1]. The purpose of this act is to increase the level of financial and operational discipline within organizations by placing higher demands on corporate executives.

The Act gives no details on how to implement the procedures, but the following issues are important:

- Rules must be defined to specify who has access to what information as well as who is authorized to grant such access.
- It must be possible, as well as simple, to generate reports verifying that the existing system access controls follow the governance rules established by the organization. Part of the quarterly or yearly report will be confirming compliance with the defined rules.
- Also, it must also be possible to verify who had access to what and who was authorized by whom to do what at any given point in time.

One important issue is that it must be possible to define and implement rules for segregation of duties. An example of this is that a corporate manager with rights to approve a new supplier should not at the same time be allowed to issue purchase orders for this supplier. This is to avoid the temptation for the manager to pass business to a company with whom he/she has personal or family ties.

More information can be found in the white paper *Achieving Sarbanes-Oxley compliance*.

Implementing the access control policy

The Access Control Policy is a set of statements defined by the corporate governance. This document is used to implement provisioning using the roles and rules mechanism in the Identity Center. The rules and roles will drive the provisioning engine, which will also keep track of the state of all the provisioned accesses.

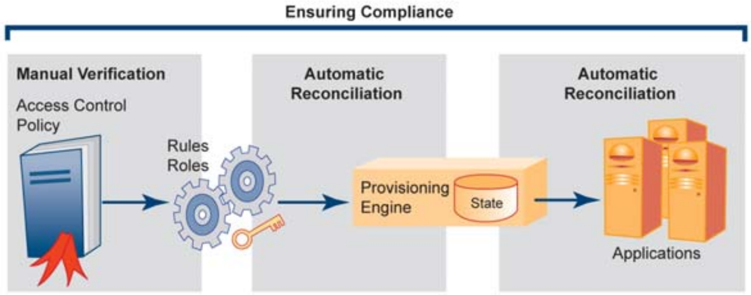


Figure 8: Implementing access control policy

To prove compliance, it is important to be able to verify that the accesses granted in the applications match the access control policy. Using the Identity Center, this can be achieved in several steps.

Going from right to left, automatic reconciliation can be performed between the applications and the provisioning engine state information. This reconciliation may automatically perform some repairs, while other defects may be taken to workflow, or as defect reports.

[1] Information about Sarbanes-Oxley can be found at www.sarbanes-oxley.com.

The rules and roles can be reconciled with the provisioning engine, again producing defect reports. Finally, manual verification must be done between the access control policy and the defect reports.

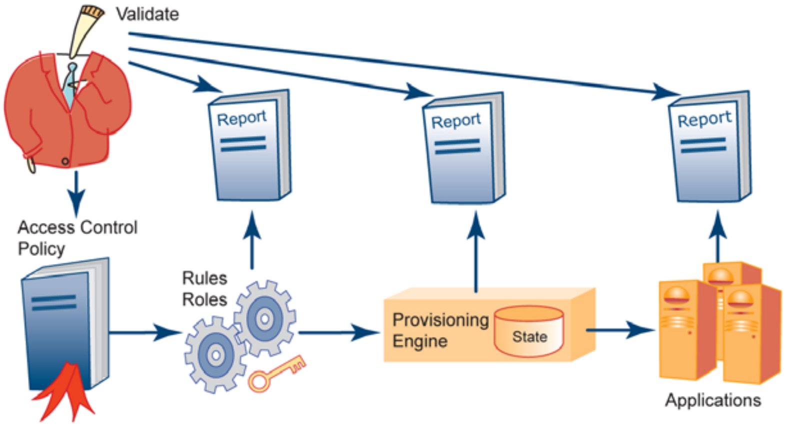
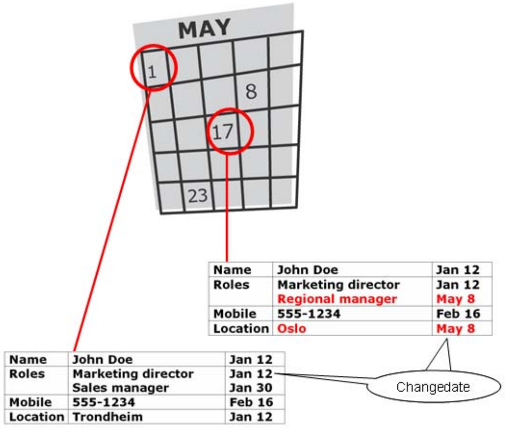


Figure 9: Ensuring compliance

Showing historical values

The Identity Center's identity store contains the previous values of the data. By using the web-based monitoring interface, it is simple to retrieve data for any given date to see what an entry looked like at that time.



Name	John Doe	Jan 12
Roles	Marketing director	Jan 12
	Regional manager	May 8
Mobile	555-1234	Feb 16
Location	Oslo	May 8

Name	John Doe	Jan 12
Roles	Marketing director	Jan 12
	Sales manager	Jan 30
Mobile	555-1234	Feb 16
Location	Trondheim	Jan 12

Figure 10: Attribute history

In the above example, one can see the information about John Doe on May 1st and on May 17th. It will also show the dates when the various attributes were changed.

Specifications

Technical specifications

This section contains the technical specifications for the Identity Center:

Operating system:	Configuration user interface: Windows: Microsoft Windows NT 4 (SP6) or newer. Java: Java2 RTE version 1.4 or later. Runtime environment: Windows: Windows NT 4 (SP6) or newer. Java: Java2 RTE version 1.4 or later. Monitoring and operations interface: Web server supporting PHP version 4.3.3 or newer. Workflow module: Web server supporting PHP version 4.3.3 or newer.
Identity Center database:	Microsoft SQL Server 2000 or newer. Oracle 9 or newer.
Programming:	VBScript, using the Microsoft VBScript control. JScript, using the Microsoft JavaScript control (Windows runtime engine) or Rhino (Java runtime engine). Perl, using ActivePerl from ActiveState.
Supported character sets:	T.61, UTF-8, ANSI, Unicode, DBCS Other character sets by scripting
Templates supplied:	Some of the templates supplied: Microsoft Exchange Microsoft Active Directory Microsoft Active Directory Application Mode (ADAM) General LDAP Lotus Domino/Notes Sun ONE Directory Server Injoin Directory Services (IDS) Audit trail report General CSV file handling InetOrgPerson handling Change-log handling from various systems, including Oracle, Active Directory and Sun ONE

This information is subject to change without notice.

Connector overview

Connector		Description
Directory servers	LDAP version 3[2]	The Identity Center can read and write the LDAP version 3 format. The simple-paged result is implemented, making it possible to read a large amount of data from a directory. The LDAP URL is used for retrieving data. Support for Secure Sockets Layer (SSL) or Kerberos authentication and encryption when communicating with a directory server that supports this.
	LDAP version 2[3]	The Identity Center reads and writes LDAP version 2. It has mechanisms for bypassing the size and time limits imposed by the server, by performing multiple searches for the information. As there is no standard way of indicating the character set in LDAP version 2, the Identity Center can be configured to use T.61, UTF-8 or ANSI, which are the formats most widely used. The LDAP URL[4] is used for retrieving data, and allows for setting up complex searches in a directory.
Databases		The Identity Center uses either an ADO[5] connection string or a JDBC[6] URL to access databases. This can also be used to access ODBC data sources, such as Microsoft Access, Microsoft Excel, FoxPro and others. An SQL "SELECT" statement is used to retrieve the data, giving the user full control of which data to retrieve.
ASCII files		The ASCII interface is used to handle simple comma-separated ASCII (CSV) files. Most applications have the ability to export and import CSV files, and this format can be used if no other means of accessing the application's data is available. The CSV format is fairly compact, and can also be used for transporting data over e-mail or FTP. CSV files with or without CSV headers can be handled. It is also possible to handle ASCII files with fixed record lengths.
LDIF and DSML files	LDIF[7]	The LDIF format is "[…] a file format suitable for describing directory information or modifications made to directory information". This may be used for exporting data from a directory server that is not directly accessible. The LDIF file can then be transported, for example using e-mail, before being processed by the Identity Center. The Identity Center can then perform verifications and quality assurance of this LDIF file before processing it.

[2] Lightweight Directory Access Protocol v 3, RFC2251

[3] Lightweight Directory Access Protocol v 2,RFC1777

[4] Defined in RFC2255

[5] ActiveX Data Objects, http://www.microsoft.com/data/ado/

[6] Java Database Connectivity, http://java.sun.com/j2se/1.3/docs/guide/jdbc/spec2/jdbc2.1.frame.html

[7] LDAP Data Interchange Format, RFC2849

Connector		Description
	DSML[8]	DSML is a markup language for representing directory services in XML. DSML helps XML-based applications make better use of directories. With a recognized standard, applications can be written to make use of DSML and capture the scalability, replication, security and management strengths of directory services. The Identity Center can produce DSML data from any source or joined data.
Microsoft Windows domain		The Identity Center can read and write directly to the Microsoft Windows user database. This makes it possible for the Identity Center to create objects based on Windows NT users, but also to create Windows users whenever they appear in the directory. ***Note:*** Platform specific.
XML recordset		The Identity Center can produce an XML recordset based on a selection in the data source. It is also able to process an XML recordset file. ***Note:*** Platform specific.
Generic/script		If none of the above interfaces is usable, it is also possible to write a COM object for handling the data source. This can be written in VB, C or any programming language, and will be plugged into the Identity Center pass. The Java runtime engine also supports connectors created in plug-in Java classes.

[8] Directory Services Markup Language, http://www.dsml.org