HP Select Identity

Software Version: 4.20

Concepts Guide

Document Release Date: September 2007
Software Release Date: September 2007

Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Copyright Notices

Trademark Notices

Support

You can visit the HP software support web site at:

www.hp.com/go/hpsoftwaresupport

HP Software online support provides an efficient way to access interactive technical support tools. As a valued support customer, you can benefit by using the support site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract.

To find more information about access levels and HP Passport, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

Contents

1 About this Guide

Welcome to the *HP Select Identity Concepts Guide*.

This document is here to help you learn and use HP Select Identity (Select Identity). From it, you can discover the conceptual foundations of Select Identity and master the skills you need to get the most from Select Identity.

However, this guide does *not* include detailed procedures that involve the Select Identity graphical user interface. That information is in the extensive online help system, described below.

Structure

The *HP Select Identity Concepts Guide* provides an increasingly detailed look at the concepts and rationale behind Select Identity. You will also find an overview and examples of how Select Identity is customarily deployed.

This material should be especially helpful if you are new to Select Identity, if you want to get an overview of the deployment process, or if you want to better understand the logic of what Select Identity does and why.

Audience

This guide is not for everyone. It was written with the following readers in mind:

- Organizational decision makers who need an in-depth understanding of Select Identity, what it offers to their business, and what is involved in its deployment.
- Identity management design architects who need to fully understand the concepts behind Select Identity.
- System administrators and business unit administrators who want to better understand.
- User administrators, who are charged with the daily task of adding, changing, and removing users.
- Help desk users who want to upgrade their understanding of Select Identity and prepare for greater responsibility.

Assumptions

You should be aware that this document makes several important assumptions about you and your situation:

- You should have a working knowledge of the general field of identity management.

Getting Help

Select Identity comes with the following online help systems that you access, based on user logon, from the Select Identity graphical user interface:

- *HP Select Identity Administration Online Help* (available to Administrators only)
- *HP Select Identity My Identity Online Help* (available to all users)
- *HP Select Identity Workflow Studio Online Help* (available to Administrators only)

Other Select Identity Documentation

This is not the only source for Select Identity information. You can find all of the following documents on the Select Identity product CD:

- *HP Select Identity Administration Guide* - Provides detailed information on how to design, implement, and deploy an identity management solution using Select Identity.
- *HP Select Identity Connector Developer Guide* - Provides a technical reference for developing custom connectors.
- *HP Select Identity External Call Developer Guide* - Describes how to create, register, and use external calls.
- *HP Select Identity Installation Guide* - Includes all available platform and migration information and describes how to install and setup Select Identity on a Web application server.
- *HP Select Identity Web Services Guide* - Provides a technical reference for developing and using web service requests in SPML.
- *HP Select Identity Addendum* (if provided) and the Release Notes accompanying the software - Contain late-breaking information about Select Identity.

2 Welcome to Select Identity

Introduction

Select Identity is focused on simplifying and automating the tasks associated with managing identity, including provisioning of accounts and entitlements, approval workflows, delegation of administrative rights, enforcement of security policy, and reporting.

It mitigates the limitations of the traditional role and rule based identity management by taking a more highly abstracted approach. Select Identity provides a service-based approach to managing identity, matching identity management to the real-world business processes in your organization. This reduces deployment times and management costs, enables great scalability, and improves security.

Putting Select Identity to work means using people, processes, and technologies to support the creation, maintenance, and termination of a digital identity for people, services and other entities, and to ensure their secure access to services, systems and applications.

What Select Identity Can Do for You

Select Identity automates the process of provisioning and managing user accounts and entitlements across platforms, applications, and corporate boundaries. Select Identity simplifies identity management because its approach mirrors the business processes in your organization.

By deploying Select Identity, you can anticipate lower help desk loads and costs, faster provisioning with fewer errors, better compliance with regulatory demands, and improved security of your essential business data.

Why Select Identity?

Modern organizations of all types, from industry to government, from education to finance, face a growing need to support job sharing, telecommuting, geographically dispersed teams, joint ventures, and so on. In addition, efficient and productive interaction among customers, partners, suppliers, and employees increasingly relies on access to relevant and often sensitive information from both internal and external sources. The need extends beyond individuals, as teams, task forces, and so on form swiftly to deal with specific challenges, and just as quickly dissolve.

You and your organization have probably experienced a surge in the need to quickly deploy new resources, and to rapidly adapt to changes in the enterprise and the global environment in which you operate.

Supporting new business configurations, managing the ebb and flow of users, and the rapid evolution of business processes is a growing challenge. Meanwhile, widespread and flexible access to data and services create greater opportunities for security lapses.

And increasingly, shareholders, legislators, and regulators demand accountability and transparent corporate governance. It is no longer merely desirable to implement effective security and access measures. They are essential to protect corporate reputations and assets from hackers, fraudsters, accounting scandals, law suits, and punitive regulation.

All too often, business people are unaware of the sophistication and potential consequences of the network-based attacks that can be launched from outside as well as inside the network, especially where there is high staff turnover, workforce reductions, involuntary reassignments, corporate mergers, and so on.

But the scale and complexity of managing access to important resources impedes the efficiency and effectiveness of an organization. Not surprisingly, users experience delays in access to necessary resources. Mistakes, such as orphan accounts, creep in. Users dodge the system by writing passwords down, rather than go to the trouble of requesting new ones when they're forgotten.

In the end, business managers, IT operations, and call-desk staff simply cannot accept the results: a flood of help-desk calls regarding trivial matters, suboptimal use of business resources, and the lurking shadow of security lapses.

Tackling the Challenge

To cope, organizations must develop a comprehensive identity management strategy.

In many cases, a multitude of different systems and processes have grown organically as the enterprise has evolved. While adequate at the time, these methods typically don't scale well, offer uncertain security safeguards, and become exponentially complex as the number of users, groups, and resources expands.

Identity management can become as much the problem as the solution.

A proper answer to the challenge, that is, a truly effective identity management solution, must meet the following five cornerstone requirements:

- **Identification (also called Authentication)**

  The ability to unequivocally establish the identity of an individual or system so that electronic credentials may be issued to them and relied upon. That is, to establish that "you are who you say you are."

- **Authorization**

  The ability to associate an individual or system with entitlements to certain applications, systems, and services. That is, to grant permission to access some things, and implicitly deny permission to access others.

- **Access**

  The ability to enforce managed access to systems and services for authorized individuals, applications and systems. This could range from a simple access control lists on routers and firewalls, to a comprehensive privilege-management infrastructure system.

- **Accountability**

  The ability to document all changes to the identity management system so that any irregularities can be detected and resolved, and to conform to audit requirements.

- **Adaptability**

  The ability to easily support rapid changes in the organization, its processes, its affiliations, and its personnel in a comprehensive and cost-effective way.

Approaches to Identity Management

All identity management systems define a framework through which the system will organize identity information and execute management processes. The most common model is Role-Based Access Control (RBAC), which uses the concept of a **role** to organize users and entitlements. Select Identity employs a higher level abstraction, called a **service**, and a complementary concept called **context**.

About Role-Based Access Control (RBAC)

Role Based Access Control (RBAC) has been the traditional model for identity management systems. It was originally conceived to address the problem of access management within individual applications. It has since been extended to the identity management realm, providing a management framework that spans multiple applications, organizations and business processes.

At a high level, RBAC provides a reasonably flexible model. Roles can span a great breadth of responsibilities, or be focused on a specific task. This definition is generally up to a role administrator, and requires a real knowledge of the business and how business is done across multiple resources.

RBAC can offer effective identity management when job functions are relatively well structured and static. However, in a large highly dynamic organization, it is difficult to design a manageable and extensible suite of roles.

Few members of a modern enterprise have a single role. A quality assurance manager may also be a part of a support escalation team, as well as coordinator of the corporate charitable giving campaign. If he or she changes jobs, some roles will change, others may not. An RBAC solution may not easily support such changes.

In addition, someone in a “Manager” role in Texas may have most of the access permissions of a “Manager” in California, but with a few exceptions. Typically, rules are established to handle the exceptions, which mitigates the problem. Rules, however, are difficult to create and maintain, and can be hard to test.

For these reasons, it can be difficult and expensive to adapt a pure RBAC solution to a corporate reorganization or merger. As the system grows and changes, roles are likely to proliferate, and it can become difficult to modify or add rules without unintended side effects.

Finally, compliance with current business regulations, such as the Sarbanes-Oxley Act, requires a secure infrastructure and strong auditing capabilities. Few pure RBAC solutions can offer this.

About Select Identity

Select Identity brings two simple but pivotal ideas to identity management — services and context. These ideas offer new ways to think about identity management, and dramatically extend the capabilities of other solutions.

The following brief descriptions merely introduce these important ideas, which are covered in greater detail later:

Services

Select Identity introduces the concept of **services** to align identity and access management with business processes. Fundamentally, services represent the processes, systems and applications that are used by your customers, partners, and employees.

This approach makes it much easier to manage dynamic changes in the resources and processes of an enterprise, both internal and external.

A service in Select Identity encapsulates all of the resources, entitlements, workflows, policies and other identity management elements related to a single business service. Select Identity provides a mechanism to partition or group these elements in various ways, to accommodate the differing needs and rights of diverse users.

Through the concept of services, Select Identity uses the workings of a business as an organizational model for identity management. Resources are organized into business services. A number of resources — such as email, SAP, LDAP, and a database — can be associated with a single service, and multiple different services may share the same resources.

Select Identity organizes identity management tasks according to the company's business processes rather than its structure; accordingly, roles are subordinate to services. This creates substantial efficiencies and benefits.

Context

Context is a dynamic way to group users based on the value of a specific attribute in the user identity profile.

For example, suppose the identity profile includes an attribute called `Residency`, which contains the country of an employee's residence. Employees, then, naturally fall into groups based on the value of that attribute, such as `Italy`, `China`, `India`, or `Canada`. Each of these groups is a context.

When the value of that attribute changes, perhaps when an employee moves, Select Identity checks to see which context the user now belongs in. It makes appropriate adjustments to his or her resources and entitlements, based on what is granted under the new context.

In terms familiar to the RBAC model, context allows the dynamic assignment of identities to roles. That is a potent extension. Context teamed with services create a powerful and dynamic approach to identity management.

Benefits of Select Identity

Select Identity offers several key benefits that enhance every aspect of your identity management solution.

Select Identity improves security, helps ensure regulatory compliance, raises efficiency and productivity, and substantially decreases administrative costs for the complex or extended enterprise. It lets you easily manage the entire identity life cycle — from provisioning, through maintenance, to termination — from a “single pane of glass”.

Select Identity automates the process of provisioning and managing user accounts and entitlements across platforms, applications, and even across corporate boundaries.

Unlike some identity management implementations, which can become practically fossilized over time, Select Identity adapts easily to change. By separating user identities from entitlements, Select Identity sidesteps the entanglement of two independent matters.

Creation of a service is a one-time task, and a service can easily be made available to the appropriate population. Moreover, a service can be modified and adapted over time to meet changing conditions.

Select Identity offers unparalleled usability and scalability. Together with robust workflow management, user self service, audit capability, reporting, and delegated administration capabilities, Select Identity offers a comprehensive identity management solution.

Select Identity's Capabilities

Select Identity offers a sophisticated set of identity management capabilities to provide simplicity, standardization, modularity and integration to solve the complex issues of identity management within large-scale or even global organizations:

- **Provisioning** – Automates the creation, modification, and deletion of accounts and entitlements on information systems across the enterprise.
- **Workflow** – Automates the processes required for provisioning users, including any necessary approvals.
- **User Self Service** – Lets end users initiate, modify, or terminate access to services, change passwords, set password hints, and update general identity information through a simple web browser interface.
- **Administrative Delegation** – Lets you delegate administrative rights among multiple tiers of functional departments, customers, and partners.
- **Password and Profile Management** – Lets you define and enforce password policy. You can manage, synchronize and distribute password and user profile information across and between disparate information systems.
- **Audit and Reporting** – Select Identity creates a secure infrastructure as a foundation for attaining compliance with Sarbanes-Oxley and other regulatory standards. Select Identity also provides standardized reporting on actions and user account activity. Teamed with HP Select Audit, you can quickly achieve document conformance.
- **Scalable and resilient** – Takes even heavy workloads in stride.
- **User Import** – Import existing users, profile information and entitlements.
- **Extensible Connector Architecture** – Ensure provisioning connectivity to your present and future IT environment.
- **Variable Entitlements** – Handle exceptions to role-based entitlements assignment without the burden of more roles or rules.
- **Change Management** – Implement identity management change at the velocity of business, and technology changes.
- **Industry Standards based** – Ensure interoperability with systems and technologies throughout the enterprise - Select Identity is a 100-percent J2EE application that works with a number of directory servers, several mainstream operating systems, commonly used database servers, business integration tools, and Microsoft Exchange Server. It also works with enterprise applications such as PeopleSoft, SAP, and others. Check with your HP representative for a current list of supported platforms and integrations.

- **Synchronization** – Keep identity data synchronized throughout your infrastructure.
- **Web-based Access** — Along with the primary user interface, which this document focuses on, you can use the Web Services web-based interface. See the *HP OpenView Select Identity Web Services Developer Guide* for more information.

Usage Scenarios: an Overview

At the most basic level, Select Identity will let you map any suite of roles to the service model, thereby mimicking the capabilities of general RBAC solutions.

However, Select Identity can easily deal with role changes, while at the same time incorporating process change and delegation of that change. This mitigates many of the slower role-based access challenges.

In the beginning, you may decide to deploy a simple role-based model. Over time, you can easily migrate and evolve to more optimal or complex models as required. The combination of the service model and dynamic, context-based role assignment gives you tremendous flexibility.

Furthermore, you can scale business processes dynamically using Select Identity's extensive delegation across all functions, not just roles alone. You can manage services independently, and more specifically, delegate ownership of services and roles. This lets you start by managing parts of the business or business processes with more fine-grained control, while leaving other parts under a more general model.

The remainder of this section outlines a few scenarios to illustrate some of Select Identity's possibilities.

New User

When a new employee comes into the organization, there are a number of provisioning actions that have to occur. For example, a new employee needs to be assigned an email address, a Windows account, and be given access to the wages and benefits systems, to the employee portal, and so on. The list is long and complex.

It is important that a new user be fully provisioned as quickly and efficiently as possible, to get the user productive, and to not over-tax IT. Many organizations, however, labor to assure that all the details have been accounted for when a new user comes in.

With Select Identity, it is possible to automate the entire process. You can automatically create user accounts, generate passwords, provision access to multiple resources, and otherwise be assured that all necessary actions and approvals happen in an orderly and efficient way.

User Moves

Over time, users move between different organizations, locations, or jobs. For many organizations, this scenario applies to both single users as well as groups.

When a user moves, all his or her previous entitlements must be checked to see if they are still valid in the target organization. Entitlements that are no longer required must be removed for compliance purposes. To maintain productivity, it is essential that the user be provisioned as quickly as possible in their new situation.

In most identity management solutions, moving a user or a group of users can be a complex operation that requires coding to ensure that all entitlements are correctly updated. The situation becomes even more difficult if the change is not based on the organizational structure – for example, when a user merely changes location.

Because Select Identity's approach does not necessarily mirror organizational hierarchy, it is typically simpler to deploy a dynamic implementation. Users are automatically assigned to roles through their context. For example, when the user moves to a new locale, the change to his or her HR records triggers a cascade of appropriate changes to their access rights.

Termination of an Account

Over time, people within an organization acquire access to a wide range of resources and entitlements. Often, these resources are geographically dispersed, and under the auspices of multiple subunits of the company.

When a person leaves the organization, it can be difficult to identify and terminate all the associated accounts and entitlements. The existence of these "orphan accounts" is a significant window of vulnerability that is hard to detect and close.

With Select Identity in place, when a user terminates, their entitlements can be automatically revoked, and their various accounts can optionally be disabled or deleted.

Termination can also be scheduled. For example, when a contract worker is added to the system, you can immediately create a termination date corresponding to the worker's end date. This includes termination of the worker's email account, database account, and whatever other accounts were granted. This forestalls the security risks that arise from orphan accounts.

Mergers and Acquisitions

Sometimes an enterprise needs to integrate a previously independent business unit or a new acquisition.

The employees of the acquired or merged company may continue to need access to many of the same resources, and to continue using some of the business processes of their original organization.

In addition, you may also need to implement variations in the processes of the parent organization to accommodate the new acquisition.

The same scenario applies to extending the management system from an initial deployment to new groups in the company, so they can access the existing services and resources.

Using a typical identity management system, it would be a major undertaking to implement the new organization in a way that can be managed consistently with the existing organization and accommodate the customizations required for the new group. You would need to define, implement, and test a whole new set of roles, rules, workflows, and so on.

Select Identity groups the definitions of these management objects into a single entity known as a service. You can create a new service based on a copy of an existing service, and then customize it based on a particular situation. The new service can then be populated through a bulk load of the new users. Select Identity automatically calculates and applies all the necessary provisioning actions for each user.

Because the acquired company or business unit is being integrated into the parent company, you can anticipate that existing processes, workflows, and so on are likely to be similar. Through minor changes to items such as workflow approvals and entitlements, or the addition of acquired resources, Select Identity can swiftly accommodate the new group.

Changing Resources

When you add, upgrade or retire applications or resources, or change an existing resource that is used and shared by one or more business processes, it can be hard to unravel all the consequences of the change. You need to know how the change affects existing workflows, roles, rules and forms. This is particularly true when you need to associate roles and rules with the resource.

You need a way to link all these identity management objects, and manage their relationships. Without knowing the full effects of a change, you could encounter costly and time-consuming problems that impede your progress.

Because a service encapsulates all of the resources, entitlements, workflows, policies and other identity management elements related to a single business service, you can immediately see the effect of a planned resource change.

If the new resource requires a new attribute that is not already defined in Select Identity, then you will need to modify relevant views to include the new attributes.

Changing Entitlements

changing your resources usually requires you to change entitlements that may be optionally or directly assigned to users. This can be a labor-intensive, lengthy, and error-prone process.

Select Identity lets you quickly add optional entitlements without any coding effort. Select Identity automatically generates forms based on optional and required attributes.

Managing entitlements during a resource change involves two basic steps in Select Identity:

1. Add the new attributes in the definition of the resource.
2. Specify the fixed and optional entitlements in the root service role of the service. (Service roles are detailed later; for now, just remember that a service role carries the entitlements for part or all of service.)

The fixed and optional entitlements of a service are inherited throughout a service hierarchy.

You can add further customization to subordinate roles as required to handle requirements that are specific to those roles. The forms are automatically generated and specific to the service.

Managing Complex and Dynamic Environments

In many cases, you need to organize users in hierarchies other than the one depicted on the company organizational chart.

Most solutions on the market today align RBAC to one hierarchy that is defined at the beginning of a deployment. Often this is a basic organizational hierarchy based on an existing directory deployment or HR model. There may also be some customization through abstract roles or rules to deal with exceptions. While this allows for a potentially rapid deployment early on, issues will eventually arise when the organization needs to manage a different hierarchy.

In a pure RBAC solution, the role hierarchy is often tightly coupled to a single model, typically an organizational hierarchy. Such tight coupling limits the value of roles, because it is difficult to define role hierarchies based on other attributes such as location, title or function.

Other hierarchies can be created by using extensive rules, but the cost is high, and you can wind up with multiple inconsistent hierarchies.

Select Identity uses one consistent service hierarchy regardless of how the enterprise chooses to organize users — by location, function, organization, or some other way.

Select Identity lets you easily create multiple different hierarchies based on context attributes such as location, department, function, and so on, without any need for special coding or programming. This also lets you easily deploy delegation models based on different hierarchies.

3 Select Identity's Service-Based Model

This chapter focuses on the most important concept in Select Identity — the idea of a **service**.

This concept sets Select Identity apart from other identity management solutions, and understanding it is essential to a successful deployment. Those who are steeped in the concepts and methodologies of other identity management models, such as RBAC, will find a rewarding challenge in learning about Select Identity.

Why Services?

People in any organization engage in many different business processes and services. Examples are abundant:

- Employees need access to compensation and benefits services.
- Corporate accountants need access to financial information and related applications.
- Managers need to be able to update employee performance records.

Each service or process uses applications or resources that require unique entitlements, often specific to a user's particular needs. Provisioning new users, or injecting new services, can involve the addition of multiple new relationships, and potentially a new set of exception rules. These tasks have a high potential for errors and accidental security lapses, and are apt to generate a flurry of notification messages of occasionally dubious value.

Select Identity's service-based model aligns identity and access management with business processes. This makes it much easier to manage all the business users and their entitlements to access business resources, both internal and external.

A service, as defined by Select Identity, encapsulates all of the resources, entitlements, workflows, policies and other identity management elements related to a single business service. This high-level abstraction greatly simplifies the job of managing the complex relationships inherent in the domain.

The service-based model makes it easy to handle routine changes, such as when an employee gets promoted. More importantly, it makes it easy to take on more challenging problems, such as when a department is created, split, or merged with another. Most dramatically, Select Identity's service-based model lets you tackle truly monumental tasks, like a corporate merger, with a set of tools that greatly accelerate and simplify the transition.

The Three Keys to Services

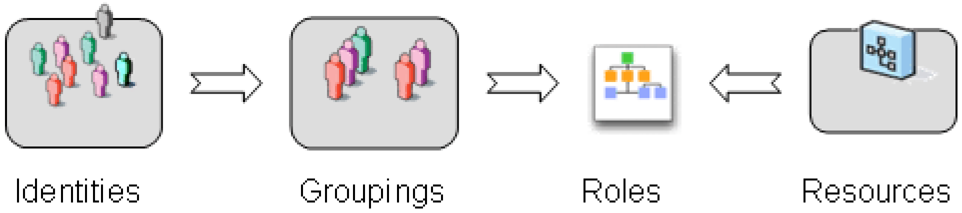
There are three keys to understanding services:

- Systems, processes, and applications are organized in **Services**.
- Users are organized in high-level logical **Contexts**.
- Access to services is controlled by **Service Roles**.

About Services

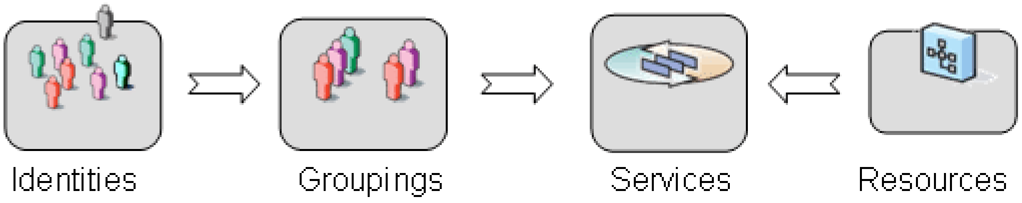
In RBAC solutions, the pivotal concept is the role. A role links groups of users with their entitlements on the appropriate **resources**, which are systems or applications that record and use identify information to govern their usage.

Figure 1 The role defines the resources and entitlements for a group of users.



In Select Identity, the pivotal concept is the service. A service links groups of users with their entitlements on the appropriate resources.

Figure 2 A service defines the resources and entitlements for a group of users.



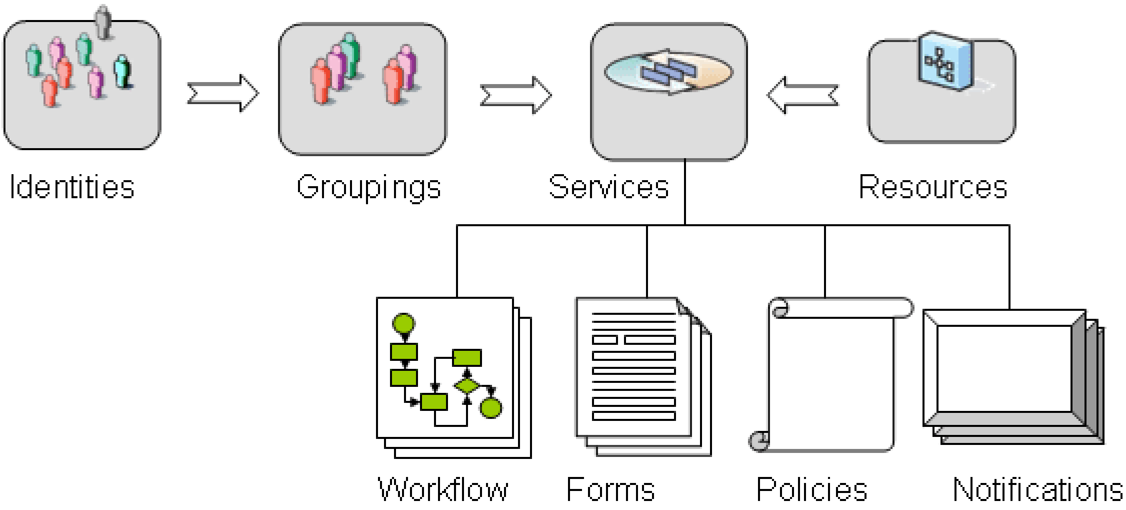
The difference is in the inherent power of the model.

It would be possible, though probably not terribly helpful, to map services directly onto RBAC-style roles. In that case, there would be little, if any, difference between the models. But the concept of a service adds many capabilities that are not available in a role.

Services incorporate a number of management capabilities:

- **Workflows** – for approvals, provisioning, and user registrations
- **Forms** – for input of user attributes
- **Policies** – to define security, exclusions and password settings
- **Notifications** – for alerts, updates and verifications

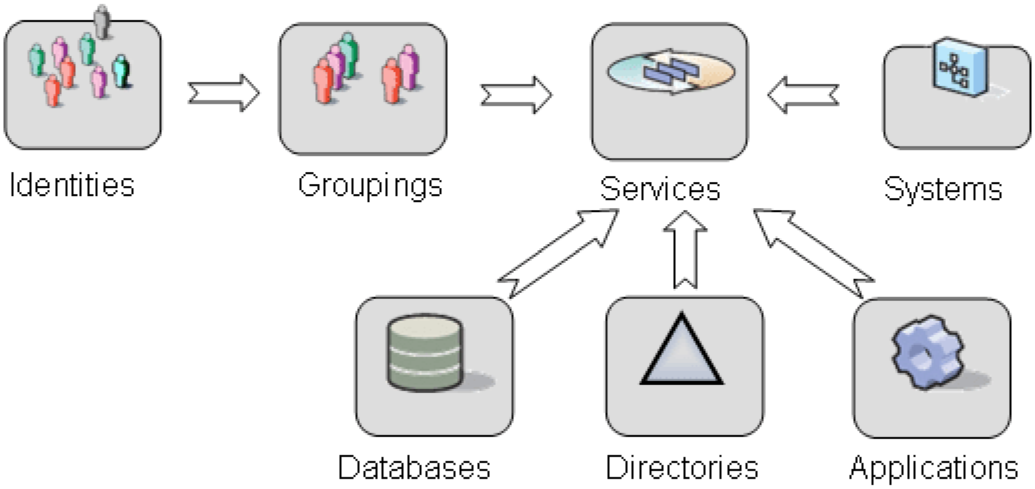
Figure 3 A service incorporates important aspects of identity management.



A service can entail any number of different resources:

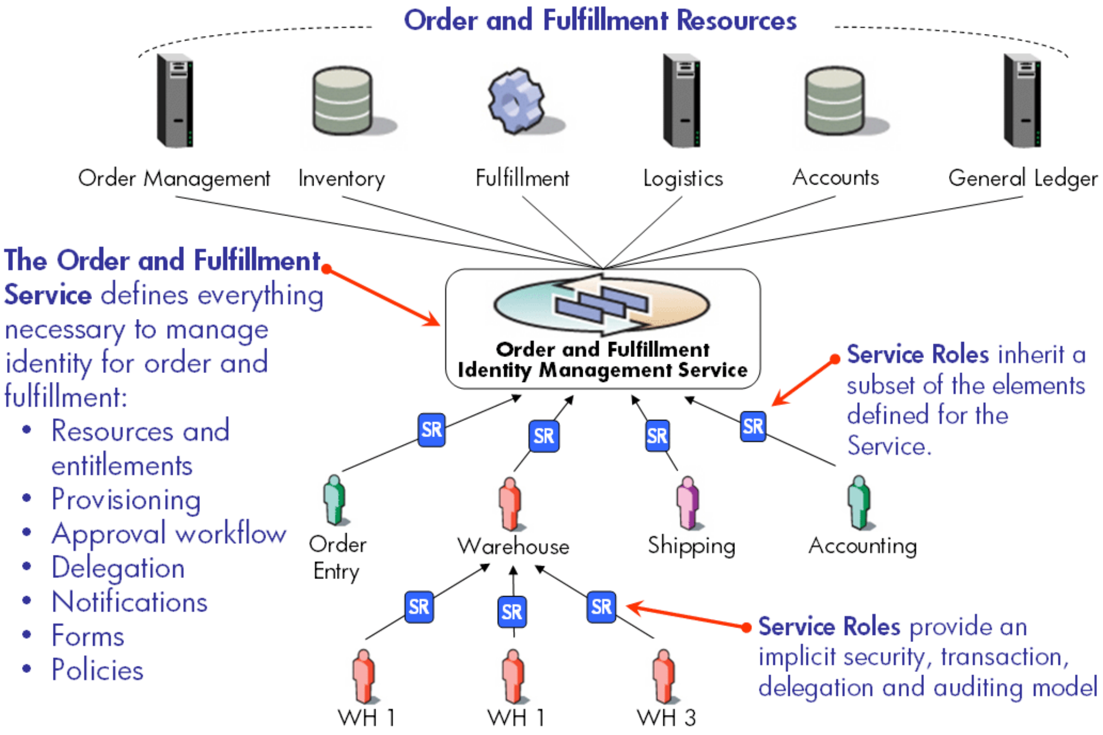
- Databases
- Directories
- Applications
- Web services
- Messaging systems
- Operating systems
- Portals
- Network devices
- Role-based security systems
- Even non-digital components can be ticketed with the help desk, so that IT staff is prompted to do manual provisioning.

Figure 4 Multiple resources associated with a single service. Multiple services can also share resources.



The next diagram shows a larger example to illustrate these points. It represents a typical order and fulfillment process within a large organization. Select Identity uses a loose (rather than tight) coupling of groups, roles and resources within its service-based management. Loose coupling means that the various user groups or roles are connected at a higher level of abstraction – an identity provisioning service. In this example the service is called the Orders and Fulfillment identity management service, and this corresponds exactly to the business process.

Figure 5 A typical Order Fulfillment identity management service



The Order and Fulfillment Service defines everything necessary to manage identity for order and fulfillment:

- Resources and entitlements
- Provisioning
- Approval workflow
- Delegation
- Notifications
- Forms
- Policies

Service Roles inherit a subset of the elements defined for the Service.

Service Roles provide an implicit security, transaction, delegation and auditing model

User groups gain access to the resources indirectly through the Order and Fulfillment identity management service. So a new warehouse worker who registers for access to the Order and Fulfillment service, and is then provisioned with all the entitlements needed to perform his or her warehouse duties. A shipping agent also registers once for access to the service, but is provisioned and controlled using a different service role (see About Service Roles on page 24).

Each service role uses a subset of the functionality in the Order and Fulfillment Service, and each has different entitlements, workflow, policies, and so on.

The key advantage of this is that the overall Order and Fulfillment identity management service already has definitions of all resources and entitlements, all provisioning and approval workflows, delegation options, notifications, forms and policies within it.

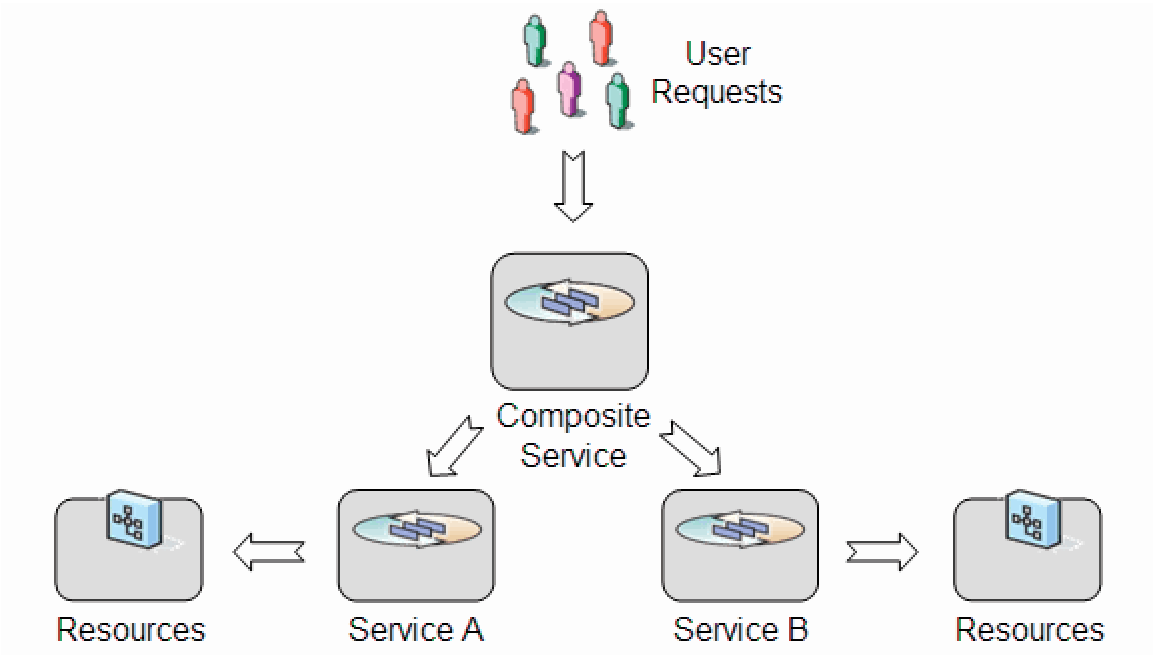
This creates a system that streamlines changes, and ensures consistent change management.

Defining a new service role within this identity management service is simple. IT staff and expert security administrators are not required, and you do not need modeling tools to understand and test a new role or rule definition.

Additionally, you can use the composite service feature in Select Identity to combine two or more services into a single unit. By creating composite services, you streamline the process of service subscription by providing the capability of using one request with one workflow to update multiple, common attributes.

For example, if new employees need subscriptions to five different services, you can create a composite service that contains the five services. Instead of subscribing to each individual service, the employees can subscribe or be subscribed to the five services through the one composite service request and workflow approval.

Figure 6 A composite service



About Contexts

A context defines a logical grouping of users, based on the value of an identity profile attribute that you select. A user's membership in a context — or exclusion from it — depends on the value of the context attribute in his or her identity profile.

To determine if an individual is a member of a given context, Select Identity compares the value of the context attribute in his or her identity profile with the value defined for the context. If there is a match, the user is *ipso facto* a member of that context.

For example, imagine a payroll service, which varies depending on the country in which the service user resides. You can create contexts for England, India, and China that are dependent on the `Country` attribute of an employee. In this example, the value of the employee's `Country` attribute determines his or her context, which ultimately determines which resources they can access and their entitlements.

By assigning context membership based on attributes, a change to an identity profile can cause a change to the context of that identity in a given service. In turn, based on the new context, the user may be granted access to a different set of resources and entitlements.

Contexts can also be structured hierarchically. For example, in service for a transportation company, you might define a parent context called `Driver`, with different child contexts for `Long-Haul` and `Local` drivers. Members of a given context share workflows, notifications, attributes and resources specific to that context.

A user's context ultimately determines the rights and permissions that he or she receives, based on the service role — such as `Long-Haul Driver` — associated with the user's context.

About Service Roles

A service identifies specific systems and applications as its resources; a context groups users according to value of the context attribute. Now, members of a given context need to access resources within the service with specific entitlements.

It is the **service role** that links members of a given context to specific entitlements within a service. In this way, service roles are the control points that govern access rights for the various administrators and users.

The concept of context, paired with service roles, gives Select Identity a great ability to adapt to business process changes.

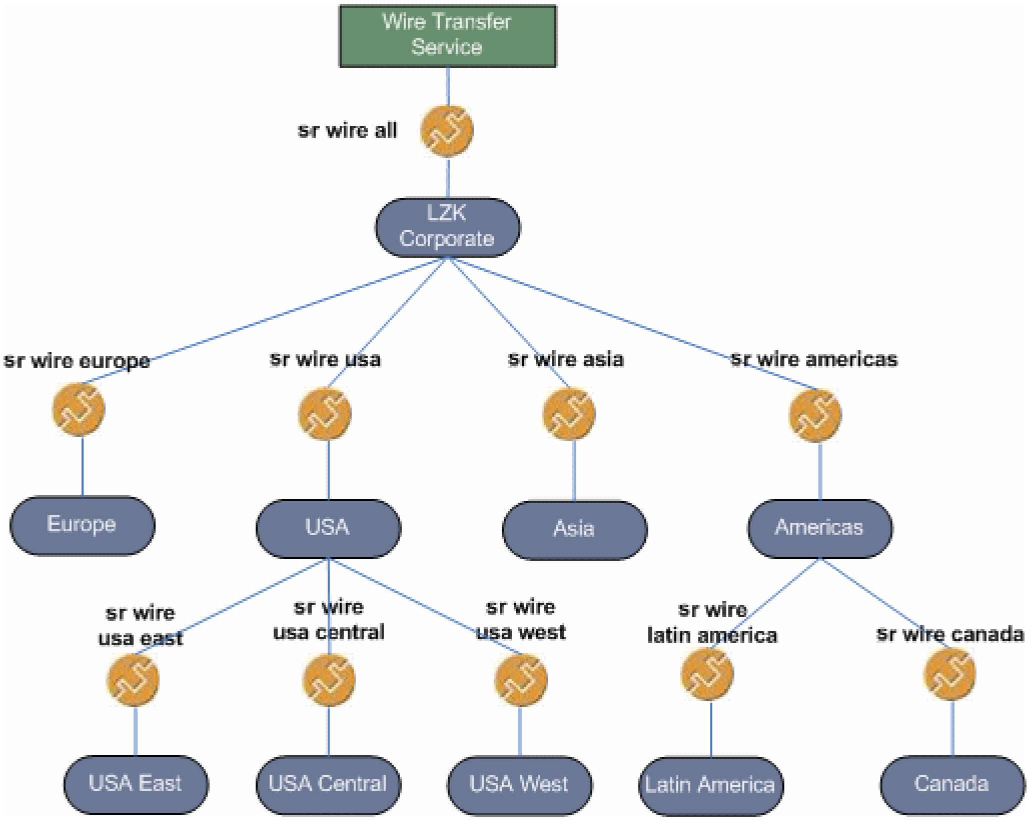
When you define a service, one of the key steps is to define the hierarchy of service roles for that service. Each service role has a specific purpose. It offers its members access to the resources of the service, and grants specific entitlements on those resources. Each tier of service roles below the root inherits from the root.

Fixed attribute inheritance is *additive*, so the child always gets the parent's attributes, plus any additional fixed attributes defined at the child level. Optional attribute inheritance is *subtractive*. That is, what is optional at the child level must be a subset of the optional values specified at the parent level (which could be, potentially, the exact same optional values).

The hierarchy of service roles creates a secure way to share services across different companies or locations. You can use contexts to determine who can manage which users across various companies or locations.

Figure 7 illustrates a simple service role hierarchy.

Figure 7 Service Role Hierarchy



The root service role at LZK Corporate defines the full set of entitlements for the Wire Transfer service. Lower levels in the hierarchy inherit from the parent service role, but each child has generally more restricted optional or available entitlements than its parent, and the same fixed entitlements. (See Fixed and Optional Entitlements on page 29 for details)

This kind of hierarchy can represent real service roles within the organization. It also protects the privacy and security of those roles, because any entitlement that is not granted to a parent can not be granted to a child.

4 The Core Concepts of Select Identity

Previous chapters set up a framework of knowledge, to help you understand the big picture and the fundamental structure of Select Identity.

This chapter provides more detail about many of the concepts that were introduced earlier. Specifically, it explains the following concepts in more depth:

- Services
- Service roles
- Contexts
- Administrative roles
- Resource management
- Workflow management
- Configuration approval
- User management
- Request management
- Security management and reporting
- Configuration replication

Services, Service Roles, and Contexts

Chapter 3, Select Identity's Service-Based Model, introduced you to the terms and concepts that Select Identity calls **Services**, **Service Roles**, and **Contexts**. These are the most fundamental and important ideas in Select Identity.

Services

In Select Identity, a service corresponds directly to an actual business process or service. In a single object, a service encapsulates all of the identity management elements related to the actual service:

- Resources
- Entitlements
- Workflows
- Policies
- Provisioning
- Delegation

- Notification
- Forms

For example, you may have a service, such as Customer Support, that includes all of the identity management components related to your help desk, including Customer Relationship Management and Internet Support portal systems.

Service Roles

A service role is a Select Identity abstraction that defines how a logical grouping of users will access a subset of a Select Identity service's entitlements. For example the `Sales` service could have three service roles: `East`, `Central`, and `West`. These service roles can be subdivided as well. For example, the service role `West` could contain two subordinate service roles: `Northwest` and `Southwest`. A service can contain an unlimited number of levels of service roles.

A service is generally accessed in different ways by different users. For example, a warehouse foreman and an accountant will have very different needs from an Order Processing and Fulfillment service. These differing needs call for different service roles.

Service roles create a secure framework that gives users of a service access to everything relevant to their contexts. You need to define and create service roles that will fulfill the requirements of the various users of a service.

When creating a service role, you assign workflow processes and notification policies that pertain to that service role. Each service role may have its own set of Entitlements, a subset of the Entitlements defined for the service. You can also define attributes that are fixed for users who access the service under the service role.

Service roles are hierarchical. The top level — or "root" — service role defines the full set of entitlements. Lower levels in the hierarchy inherit from the root service role. Each child has more restricted optional entitlements than its parent, and the same, or more, fixed entitlements. This allows a secure way for services to be shared across various users, geographies, or even across different companies.

But merely defining service roles alone is not enough. You need a mechanism to associate each service role with its intended users.

Contexts

A Select Identity context is a logical grouping of users with access to a particular service through a specific service role. A context serves two essential functions:

- First, a context defines a group of users who share an identifying attribute in their profiles.

  For example, in the "Benefits" service, you might have one context called "`US Employees`", one called "`Argentina Employees`", and one called "`Japan Employees`". Each group is made up of employees who share a specific value for the "`CountryOfResidence`" attribute of their profiles.

  In an Order Processing and Fulfillment service, you might define a "`Warehouse`" context and an "`Accounting`" context, whose members are assigned according to the value of the "`Job Title`" attribute in their profiles.

  A Select Identity administrator manages groups of users by their context attribute value.

- Second, a context links its members to one or more service roles.

  Each context has one service role assigned to it. This means that when the user of a service is identified as a member of a given context, that user gets provisioned to the service based on the service role assigned to that context.

Summarizing then, when a user is assigned to a service, his or her identity attributes determine which context the user belongs in. The context determines which service roles apply to its members.

Thus, when a user is assigned to a service, he or she automatically obtains appropriate entitlements to the service resources based on his or her context attribute.

At some later date, the user's attributes may change. For example, suppose a user is a member of a service that determines context membership based on the "CountryOfResidence" attribute. If he or she emigrates to a different country, the value of that attribute changes. Select Identity automatically terminates their membership in the original context, and makes them a member of a different context, based on their new "CountryOfResidence". The user automatically obtains access appropriate to the service role for that context.

See the *HP Select Identity Administration Guide* to learn about using wildcards in specifying the context variable.

Fixed and Optional Entitlements

An **entitlement** is an abstraction of the resource privileges granted to a user. Entitlements are resource-specific, and can be account IDs, role memberships, group memberships, and access rights and privileges. Entitlements are also called privileges, permissions, or access rights.

Select Identity lets you offer sets of entitlements based on the service role. Entitlements can either be fixed or optional.

A service role belongs to the service in which it was created. The entitlements available to any service role are defined either at the service level or attribute level. A service role can assign one or more entitlements belonging to the service, but it cannot assign an entitlement that does not belong to its service. In other words, the entitlements that are available in a given service role level are strictly prescribed by the parent service role or attributes.

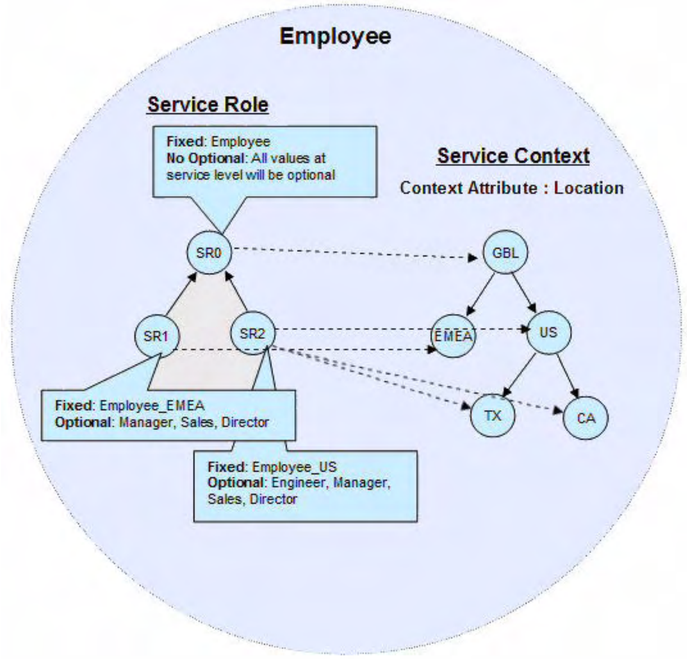
A fixed entitlement is an entitlement automatically granted to certain users, as determined by the context (and thus, the service role) associated with their identity. Any fixed entitlement is automatically inherited by a child service role created within the service. All children service roles will inherit it.

An optional entitlement is an entitlement that is available to certain users as determined by the service role and context associated with their identity. Users have the option to choose or not choose the entitlement.

Optional entitlements can be defined in the service role. The root service role inherits all optional entitlements defined at the service level if there is no definition at its level. A child service role inherits optional entitlements from its parent service role if there is no definition at its level. But a child can only get a subset (perhaps all) of the optional entitlements defined in a parent service role level.

For example, suppose your business has an `Employee Service` and every user in this service needs to have `Employee` entitlements for a certain resource. Users in the US region require the `Employee US` entitlements, and may also have one or more of the following entitlements: `Engineer`, `Manager`, `Sales`, or `Director`. Users in Europe, Middle East, and Africa (EMEA) region require the `Employee EMEA` entitlement, and may also have one or more of the following entitlements: `Sales`, `Manager`, or `Director`. Figure 8 on page 30 illustrates this entitlement setup, and shows how a service role is attached to a service context.

Figure 8 Example of Employee Service and Entitlements


Employee
Service Role
Fixed: Employee
No Optional: All values at service level will be optional
Service Context
Context Attribute : Location
SR0
GBL
SR1
SR2
EMEA
US
TX
CA
Fixed: Employee_EMEA
Optional: Manager, Sales, Director
Fixed: Employee_US
Optional: Engineer, Manager, Sales, Director

Now, users belonging to the US context have `Employee` and `Employee US` entitlements automatically. Administrators can choose to select from `Engineer`, `Manager`, `Sales`, or `Director` entitlements. Users who belong to the `TX` (Texas, US) or `CA` (California, US) contexts are similar.

To recap, all possible entitlements are defined at the service level. Within that set of entitlements, service roles determine which are fixed and which are optional.

By default, the root service role has all of the optional entitlements existing on the service. You can constrain the entitlements in different service roles to suit different context groups of users. Service roles are structured in a hierarchy of parents and children. Children receive all fixed entitlements and a subset of the optional entitlements available to the parent. Children can never have more optional entitlements than their parent.

The concept of fixed and optional values is also applied to attributes other than entitlements. You can fix a value or constrain a list of values for any attribute except as follows:

- The globally unique identifier (`GUID`) and `UserName`. attributes can not be fixed or constrained.
- If the attribute type is `Password`, or the primitive type is `Date`, it can not be fixed or optional.

Service level constraints are set for each attribute on the **Service Attribute Values** page. The constraints are applied to the entire service, not just one service role.

Administrative Roles

An administrative role determines the capabilities and actions that are available to an administrator within Select Identity.

Administrative roles are made available through an administrative service. That is, a user gets administrative rights when he or she is assigned to an administrative service.

You can add users to an administrative service, who will serve as Select Identity administrators. When assigning a user to an administrative service, you choose the following:

- The intended user
- The administrative service
- One or more administrative roles, which specify the set of available capabilities and actions
- One, several, or all services
- For each service, a subset of context values, or `All Contexts`.

Select Identity provides four basic administrative roles that reflect the capabilities and actions that are performed within the system. You can use these roles as they come, edit them, or create your own to better reflect your business needs. The four base roles are as follows:

- **End-User** – designates someone who is simply a user of the services provided by Select Identity. All users have at least this role, which grants a default set of permissions. You can change the default permissions by modifying this role. The End-User role is technically an administrative role, but it typically has no administrative privileges beyond managing details of the user's profile.
- **Workflow Approver** – designates someone who is authorized to approve changes to user accounts. Select Identity automatically grants this role to users assigned any approval task. A user with this role can approve user account additions, modifications, or deletions for those users within the approver's context.
- **Configuration Approver** – designates someone who is authorized to approve configuration changes to Select Identity. See Configuration Approval on page 36 and the *HP Select Identity Administration Guide* for more information.
- **Concero Sys Admin** – designates someone who has full access to all configuration and administrative features of Select Identity; this level of access should be restricted to at most a very small group of people.

Additional roles that you might add could include the following examples:

- *Workflow Engineer* – to designate someone who performs this specific identity management task
- *User Administrator* – to designate someone who is allowed to manage users
- *Resource Administrator* – to designate someone who is allowed to manage resources
- *Access Manager* – to designate someone who is authorized to grant groups of users (contexts) access to services

Someone with an administrative role can also delegate his or her permissions to another administrator. This is commonly done to accommodate vacations and other extended absences.

> An administrative role can not be restricted to manage a particular service.
>
> On the other hand, an administrative service can define a specific administrative role for its users, by setting that role as a fixed value.

Service Roles in an Administrative Service

Select Identity lets you create a hierarchy of administrators, by defining service roles within an administrative service. Each lower level in the service role hierarchy has more restricted capabilities. This makes it possible to shift some management responsibilities and tasks more deeply into the organization, to free up higher level staff. You can assign any range of management permissions to internal users, customers, and partners as needed and appropriate.

Resource Management

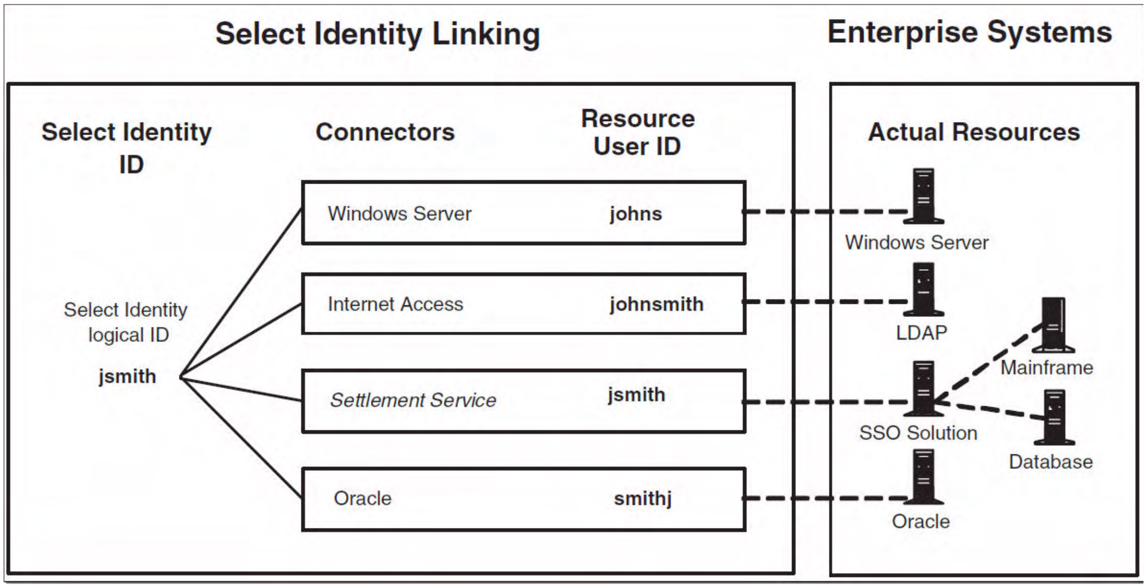
Resources in the Select Identity system represent the applications, databases, and directories that Select Identity provisions. Resources in a typical environment might be Windows Server Systems, or Oracle databases.

Select Identity views a resource as a repository of user data, in which accounts and entitlements can be created, modified, and deleted.

You must deploy a **connector** for each type of resource in your environment. A connector enables Select Identity to interact with a resource. Later sections of this guide cover connectors in detail. After the connectors for each resource type are deployed, the resources on which your products and services rely can be configured.

Select Identity maps virtual user identities to the identities contained in the data stores of your systems. The end result is that no matter how many resources you have in your environment, Select Identity creates a single, unified view of a user that spans all the resources that may contain user identity information.

Figure 9 Select Identity Linking Example



As illustrated in Figure 9, you may offer services to your customers that rely on a database, such as Oracle, or a Windows Server. After you deploy these resources within Select Identity, the end user — John Smith — accessing the service has one logical Select Identity identity — `jsmith` — which maps to the user accounts on both the Oracle system and the Windows Server.

With connectors deployed, you simply provide the addresses of the machines in your environment and Select Identity creates the bridge to each data store. Select Identity then uses administrative authority to access each user data repository in each resource as each service requires.

In Select Identity, the concept of identity is enterprise-wide. If a user leaves the company, transfers to a different division, or changes jobs, Select Identity tracks all the various resources where he or she has accounts and entitlements, and can act appropriately.

Synchronizing Identity Data among Resources

Suppose a person changes his or her name upon marriage. To manage such an event, Select Identity makes it possible for the change to be entered once, and have it propagated to all the resources associated with that user.

To make this possible, Select Identity defines two classes of resources:

- An authoritative resource contains accurate data about one or more key aspects of a user's identity. This data is taken to be reliable as a matter of convention. A typical example of an authoritative resource is a human resources server containing employee data; the data in it is treated as trustworthy.
- A non-authoritative resource typically needs to stay synchronized with regard the key aspects of a user's identity that originate at the authoritative resource, and may also contain less essential or resource-specific identity data. A typical example would be a UNIX® resource or account which contains the person's first and last name (from the authoritative resource), as well as the shell and home directory.

Select Identity uses authoritative resources to update non-authoritative resources about changes in key user attributes, as when a user's name changes upon marriage. See the *HP Select Identity Administration Guide* for more details.

It can also synchronize other user attributes among non-authoritative resources, if you correctly set an attribute's synchronization properties (see the *HP Select Identity Administration Guide* for details). For example, if the UNIX user changes his shell, Select Identity can be updated correspondingly. This process is called account reconciliation, and it lets you keep account data synchronized between various resources.

Account reconciliation provides the ability to automatically update and synchronize Select Identity accounts with changes made to those accounts externally. An administrator can configure Select Identity to reconcile changes made on a resource so that the account on the resource and the account in Select Identity are synchronized. Select Identity can reconcile changes made to both authoritative and non-authoritative resources.

For example, you may want to ensure that an attribute, such as `LastName`, is changed in Select Identity only if the change occurs in a human resources application (an authoritative resource). A user's permissions or entitlements, however, may be updated from a non-authoritative resource if the synchronization properties of the relevant attributes are set to allow it. Select Identity allows updates from both types of resources. Select Identity can automatically reconcile account data with that resource on a regular basis. You can set the frequency to whatever makes sense for your organization — monthly, weekly, daily, or hourly, or even every few minutes.

Reconciliation is explained in detail in the *HP Select Identity Administration Guide*.

Workflow Management

Workflow is the process by which user requests for service access are approved and provisioned by Select Identity.

For example, when an employee is promoted to manager, the employee needs access to the company's HCM system to manage other employees. To support these new responsibilities, the employee must be granted new entitlements. Before giving the employee access to these systems, upper-level management must approve the access requests and the employee must be created in the supporting systems.

These provisioning events include the addition and removal of accounts and can require any number of approval steps. Each step can include a call to individuals or external systems for validation and approval. A step may require that email notifications be sent to one or more addresses.

A workflow in Select Identity has the following features and functions:

- Automates the approval and provisioning processes.
- Supports synchronous and asynchronous calls to external systems to obtain information or initiate actions that are outside the Select Identity system.
- Permits context-based workflow selection, which lets you assign different authorization processes to different groups of users.
- Allows sequential and parallel processing of steps.
- Supports group approval processing.
- Provides escalation for overdue approvals.
- Provides control over user profile attributes pushed to resource.
- Support for arbitrary logic, branching and custom function.s

You can automate workflows of this sort by using the **Workflow Studio** in Select Identity. **Workflow Studio** lets you create workflow templates that model particular sequences of approvals and provisioning for different situations.

Workflow templates also let you track the progress of a system event through the Request Status pages.

Workflow Studio is a flexible tool that simplifies workflow creation, using a graphical interface.

Full information about using the workflow studio can be found in the online help.

Configuration Approval

Use the configuration approval features to regulate high-risk changes to the configuration of Select Identity itself. Through configuration approval, you can establish an approval workflow for Select Identity configuration changes.

Using configuration approval is not required, but is highly recommended. Without configuration approval, administrators can make unregulated large-scale changes to key system settings such as attributes, rules, and services. Select Identity configuration approval setup is flexible, and allows you to establish the appropriate level of control within your organization.

User Management

The user management features of Select Identity give you centralized control over user identities, including accounts, entitlements and profile information. You can manage the complete identity life cycle, from creation to termination.

Users are added to the system through the registration process defined for a service, possibly a self-registration page. The workflow and service role that you have assigned to each context determines how this process takes place.

A Select Identity administrator can create and manage user accounts through the **Users** tab, which permits the following actions:

- Add, modify, and terminate user accounts, and view account attributes.
- Add, view, enable, disable, or delete a user’s membership in a service.
- Enable and disable all services for a user
- Reset a user’s account password
- Manage a user’s expiration

Furthermore, you can disable a user’s accounts for a buffer period prior to actual deletion. In addition, you can set up temporary users whose accounts expire on a schedule. There is more information about how passwords are managed in the section, Passwords and Attributes on page 38.

User Self-management

Select Identity provides advanced facilities to allow user self-service and self-administration. This helps you avoid significant costs in help desk operations.

A user can perform several important tasks, such as the following:

- Viewing and updating his or her account profile
- Change or synchronize his or her password
- Change password hints
- Request access to a new service, or removal from one
- Delegate his or her administrative role, if applicable

Password Management

Select Identity gives you comprehensive password management. You define and enforce password policies that suit your organization, including defining what constitutes a valid password, password expiration, lock-out policies, challenge-and-response questions, and so on.

Provisioning

As part of user management, you can automate creation, maintenance, and revocation of accounts and entitlements.

For complete control, you can define provisioning dependencies that Select Identity will follow. Provisioning is a transactional operation, with automated rollback. You can configure a provisioning retry action in the workflow.

Select Identity can employ asynchronous communication with resources, and uses the open standard J2EE Connector Architecture (JCA) for provisioning enterprise resources.

Multiple User Identities for a Single User

An individual user may need multiple identity accounts for a resource. Users may have multiple accounts on a resource based on their role, and want to consolidate and manage these accounts at person level in Select Identity.

Select Identity lets you easily consolidate and manage multiple user-IDs for a user:

- You can group multiple resource accounts for a person into a multiple-user-ID account containing primary and secondary identities.
- You can manage (add, modify, or delete) entitlements of a person based on roles.
- You can transfer accounts from one person to another, and terminate a single account, or all of a user's resource accounts.

In addition, multiple-user-ID accounts let you support situations where a person's multiple accounts on a resource are maintained independently of each other on the resource, but need to be linked externally using Select Identity.

Attribute Management

In Select Identity, an attribute is a data item, or field, that helps define an identity profile. For each identity, each attribute has a corresponding value. For example, an attribute called `EmployeeNumber` would contain the employee number of a user.

All identities in a Select Identity implementation share the same attributes, but each specific identity has a unique combination of attribute values. You can define whatever attributes you need in order to generate a user profile that satisfies your requirements. The attributes you define can reflect any identity data your implementation requires.

Select Identity uses attributes to manage accounts and services. More specifically, Select Identity uses the value of the attributes you specify to determine a user's context in various services. The context links the user to a service role, which ultimately provides the user access to the correct resources and entitlements.

An attribute in Select Identity can be mapped to similar but differently named identity fields in various resources. For example, an attribute in Select Identity called `EmployeeNumber` could be mapped to an identity field called `empnum` on a resource.

If an authoritative resource informs Select Identity that a user's `EmployeeNumber` has changed, Select Identity can use the resource attribute mapping to propagate the change to the `empnum` field of the resource.

Attributes are also used to automatically generate forms, for provisioning, and for data validation. Some attribute values may be generated automatically, and some attributes may be constrained to predetermined values.

Passwords and Attributes

Select Identity manages and synchronizes multiple passwords used throughout an enterprise. The key to managing multiple passwords lies in attribute management. You can create as many attributes as you need to properly provision user-related data into a resource. A resource's password is simply another attribute in Select Identity, which can be pushed to the resource during account creation and reset activities.

Select Identity ships with one password attribute – `Password`. This attribute cannot be removed as it is used for authentication into Select Identity itself. It can also be used to push the same password to any number of resources, thus synchronizing Select Identity with the resources.

However, you can create multiple password attributes, one for each resource, if necessary. Each password attribute must have a unique text name and contain its own password policy, such as minimum and maximum characters permitted, or whether the password should be auto-generated to a corporate standard.

Once a password attribute is used to provision a user, Select Identity tracks that password for the life of the user's identity in Select Identity. Subsequent password reset requests will display all password attributes for the user, thus any resource using that password attribute will be synchronized. This mapping of password attribute to resource can be 1:1 or 1: many.

External Calls

Select Identity workflow processes and attributes support the ability to interact with an external processes or system. This functionality is known as external calls. An external call invokes a function that you create using Java APIs that are part of Select Identity. You write your external call to interact with a program or system outside of Select Identity.

External calls let you integrate approval processes with other business processes and systems. You can use external calls to perform the following kinds of actions:

- Approver selection — executes an external program to retrieve a list of workflow approvers
- Value generation — generates the values of an attribute
- Value constraint — provides a list of possible values for an attribute
- Value validation — validates the value of an attribute
- Value verification — verifies the value is what was previously saved. This is used to verify passwords.
- Certification management — lets you retrieve a certificate from an external system
- SPML request filter — invoked before a reconciliation request is processed
- Workflow action — performs a task as part of a workflow, so that you can integrate approval processes with external processes and systems
- Perform some direct operation to resource

- Update attributes during workflow

Once created, external calls are managed through the Select Identity interface.

For complete information about how to design, develop, and use external calls, refer to the *HP Select Identity External Call Developer Guide*.

Notifications

The **notifications** section of the Select Identity user interface lets you define the content of email notices that are sent to users and administrators when a system event occurs.

These messages are useful at different stages in a workflow process. For example, it is often desirable to send email to a user for events like account approval, rejection, or modification, or to confirm changes to an account password or hint. Similarly, you are likely to want to send email to an administrator when an account requires approval, or when an account has not been reviewed within a specified period of time.

Wholesale Addition of Users

Select Identity gives you two ways to add numerous users to Select Identity at once:

- One way, called **user import**, lets you draw on user data from existing resources to quickly populate Select Identity with users, and assign them to services based on their attributes and current entitlements.

  User import is primarily used when setting up new Select Identity installations.

- The other way, called **bulk add** or **bulk move**, lets you quickly add multiple new users to Select Identity, assign them to services based on their attributes, and provision them on the appropriate resources.

  Bulk add is primarily used to add new users to an existing Select Identity installation.

The key difference between the two centers on how the new users are provisioned:

- With user import, the new users are already provisioned on your resources before the job starts.
- With bulk add, Select Identity provisions the new users as part of the job.

Request Status

When user accounts are added to the system, you can view status and approval process details by using the **Request Status** capability.

Request status lets you view the workflow steps, color-coded to indicate which have been executed, not executed, or are waiting approval.

Select Identity provides a default report template for displaying workflow information. You can also create your own XML template for viewing details specific to your environment. See the Workflow Studio online help for details.

Security Management and Audit Reporting

You can check on all account management processes by using audit and configuration reports. Use audit reports to monitor regular account interaction. Use configuration reports to display current information related to the setup of the Select Identity system.

Select Identity gives you a detailed audit log of all system events., with built-in reporting against database and audit logs. Select Identity caches identity and audit data, so you can generate historical reports.

You can customize your reports with regard to scheduling and data selection. Your reports are automatically filtered by context, so that an administrator sees only data relevant to users he or she manages.

Configuration Replication

Select Identity lets you configure your system in one environment, and then replicate that configuration in another environment.

To accomplish this, you export the key components of the source system, such as services, attributes, and resources. You can then import those elements into your target system.

This facility lets you easily move from a test environment to a production environment.

For more detail, see the *HP Select Identity Administration Guide*.

A Integrating Select Identity with Other HP Identity Center Applications

This Appendix describes supported integration pairings between Select Identity and other Identity Center applications, namely HP Service Desk and HP Select Audit as of Release 4.10.

Select Identity can be configured alongside Service Desk and Select Audit so that each product is enhanced by exchanging data with the other. See the *HP Select Identity Installation Guide* for instructions on how to set up integration in Select Identity.

Select Identity–Service Desk Integration

This section provides information about the integration of Select Identity with Service Desk 4.5, service pack 13.

Integration of the Select Identity password management feature with Service Desk enables Service Call tickets in Service Desk to be automatically updated by Select Identity. This provides tracking of issues and enforcement of Service Level Agreements (SLAs) in Service Desk.

If the two applications are not integrated, a Reset Password Service Call opened in Service Desk must be handled by manually activating the `ResetPassword` process using Select Identity. The ResetPassword process in Select Identity is not managed by Service Desk for enforcing Service Level Agreements (SLAs).

Functional Scenarios

The following sections provide example use-case scenarios for Select Identity:Service Desk integration. In essence, password management requests can be initiated either from Select Identity or Service Desk.

The password management functions are listed below for reference:

- **Change password**: The user changes his or her password.
- **Reset password**: An administrator performs a delegated password change on the user's behalf.
- **Forget password**: Either the system resets the password with an auto-generated password, or the user is able to enter a new password. This depends on the value assigned to the `TruAccess.properties` item named `com.hp.ovsi.forgetpassword.autogenerate` (if set to "true," the system auto-generates the password).

Password Management Request from Select Identity Triggers New Service Call in Service Desk

When a Select Identity end user or system administrator submits a password management request (reset or change password, or retrieve forgotten password), this automatically opens a new Service Call in Service Desk, and also updates the status at various stages of the Service Desk workflow in Select Identity. This occurs whether the request is submitted via the Select Identity GUI or via a Web Services request. The Service Call is updated with `Completed` status at the end of the workflow.

Reset Password Request from Service Desk and Corresponding Updates of Service Call Status at Various Stages of Select Identity Workflow

When a Service Desk Customer Service Representative (CSR) opens or updates a new Service Call for password management, the Select Identity `Reset Password` page opens and the CSR performs the request directly in Select Identity. The status of the Service Call is updated at various stages of the Service Desk workflow in Select Identity. The Service Call is updated with `Completed` status at the end of the workflow.

Accessing the Select Identity Request Status Page from Service Desk

A Service Desk CSR can access the **Request Status** page in Select Identity, to check the status of the request corresponding to a Service Call for password resets.

Select Identity-Select Audit Integration

Select Identity can be configured with Select Audit so that the two applications are able to perform the following:

- Pass Select Identity request, transaction, configuration, and maintenance data into Select Audit for compliance auditing in Sarbanes-Oxley, HIPAA, and other regulatory settings.
- Incorporate data from the Select Identity XML audit data stream into a wide range of reports.
- Allow Select Identity administrators to view audit reports in Select Audit, depending on the access rights they have for Select Identity configuration reports. The Select Audit reports filter by the managed service and the context of the Select Identity administrator; you can only see reports for users and services you manage.

➤ Refer to the Select Audit documentation for detailed instructions on how to perform configuration steps in Select Audit. This documentation provides summary information only about how to set up integration from the Select Audit side.

B An Overview of the Select Identity Architecture

Introduction

An identity management system must meet several challenging demands common to all enterprise software solutions.

- It must scale to manage not only all the employee users of a business, but also the users that represent the business' partners, vendors, contractors, and customers.
- It must scale not only in terms of its performance, but also in terms of its manageability as its utilization increases in size and complexity. Since an enterprises information systems are its lifeblood, access to these systems is a business-critical function and drives the need for reliability of an identity management system.
- Finally, the wide variety of systems, organizations and business processes creates the requirement for maximum flexibility for enterprise-class identity management systems.

This appendix describes the technical architecture of Select Identity, with a particular emphasis on its enterprise effectiveness. This appendix provides a detailed look at the technologies and architecture that make up the Select Identity system.

This appendix discusses three architectural aspects of Select Identity:

- Platform architecture
- Deployment architecture
- System architecture

Platform Architecture

The Select Identity system was designed from the beginning to manage identities in very large, complex, extended enterprise environments. To support the demands of such an environment, Select Identity uses a number of technologies to enhance its scalability, reliability and extensibility.

J2EE

Select Identity uses J2EE (Java 2 Platform, Enterprise Edition) as its platform, because of its open standards portability, providing greater hardware and software choice for customers, and its enterprise-class scalability, reliability and extensibility. The J2EE platform also provides a robust set of APIs to other enterprises systems including databases (JDBC), directories (JNDI), messaging services (JMS). Select Identity runs on the leading J2EE application servers including BEA WebLogic, IBM WebSphere and JBoss.

Leveraging the J2EE platform, Select Identity provides a robust set of options to enhance scalability for large and extended enterprises. Select Identity is able to use standard web application scalability technologies and techniques, such as load balancing, concurrency and parallel processing, to ensure that Select Identity scales with the needs of the business on user, resource, geographic and corporate dimensions.

J2EE natively supports event-driven transaction processing. Select Identity uses J2EE's transaction support to provide enhanced reliability features, such as rollback and multi-phase commit.

Transaction processing ensures that identity management task are performed reliably, correctly and completely.

For example, when provisioning a new user, Select Identity treats the creation of all the user's accounts and entitlements across multiple resources as a single transaction and can roll back the transaction if it fails to successfully complete for any reason.

This ensures the integrity of external system data and prevents the inconvenience and expense of half-provisioned users. When the reason for failure is resolved, Select Identity will retry the transaction.

Using J2EE's web service architecture, Select Identity is very flexible in extending its functionality to meet the needs of the business. For example, in an environment where a web single-sign-on (SSO) application is deployed to provide common authentication capabilities, Select Identity's internal authentication service (which is used when users and administrators log into the Select Identity system) can be swapped out for the SSO.

In addition, and of great significance, Select Identity uses J2EE's extensive API set for accessing external systems, to provide connectors to enterprises resources.

Relational Database

Select Identity uses a relational database to store user information, internal system information, and an audit log. This is a significant architectural advantage to identity management systems that are built on a directory, since relational database systems provide native support for transactions, backup and restore, distributed processing and data warehousing.

While directories provide fast record retrieval, they do not support the data relationship mapping and reliability features that are standard in most relational database products. It should be noted, however, that Select Identity does support the ability to provision directories. In that context, a directory is treated like any other enterprise resource. Select Identity can be deployed on JDBC-addressable database systems, including Oracle, Microsoft SQL Server and IBM DB2.

User Interface

Select Identity embraces a full-function graphical user interface (GUI) philosophy. All user and administrator actions can be performed from the graphical user interface, eliminating the need to manually script, code or edit configuration files. This philosophy greatly enhances ease of use and reduces deployment time. In addition to the GUI, API access is provided for batch-oriented activities such as importing users.

The Select Identity interface is automatically personalized to the user, displaying only those functions that the user is allowed to perform.

A significant benefit of Select Identity's thin client approach is that there is no client software to manage or administer. This simplifies the deployment of patches and new version updates. In addition, Select Identity's web-based client enables ubiquitous access, via the Internet or dial-up. This is a significant benefit in emergency contingency planning. To maintain security, Select Identity uses SSL to secure the web client's interaction with the Select Identity server.

Finally, the Select Identity web client is firewall-friendly, using standard ports to access the server.

Select Identity was designed for extended enterprise deployment, so its user interface is optimized for scale. For example, when presenting a large list of items to an administrator, Select Identity breaks the list into manageable pages, and provides powerful searching options.

Security

With any identity management product, security is a primary concern. Select Identity encrypts application data both in storage and in transit. For in-storage encryption, Select Identity uses the standard hashing algorithm, `SHA-256`. For data in-transit, information is secured using SSL.

Depending on corporate policy, the server and client can be mutually authenticated. In both in-storage and in-transit cases, Select Identity can support other encryption and authentication technologies.

Deployment Architecture

As with any enterprise software, ease of deployment is a critical success factor for an identity management system. Deploying an identity management system is particularly complicated due its pervasive role within the business: an identity management system must integrate with a wide variety of applications, databases and directories to enable provisioning and identity-related processes. These resources can span organizational boundaries, geographic locations, and hardware/software platforms.

J2EE Connector Architecture

Select Identity uses the J2EE Connector Architecture (JCA) to provide an open standards-based approach to accessing enterprise resources. JCA is the Java standard for connectivity to enterprise information systems. Like all J2EE components, it was designed for enterprise scale and manageability. With JCA, connectors to enterprise applications can be created and used by any number of J2EE applications, not just Select Identity.

Select Identity furnishes a robust set of connectors to provide broad coverage of enterprise resources, and offers new connectors as they become available.

Select Identity is able to take advantage of JCA's built-in support for transaction pooling to maximize transaction throughput and improve system performance. Transaction pooling manages connections to resources, optimizing the reuse of existing connections wherever possible in order to ensure resource availability. This feature minimizes the performance impact on enterprise resources of Select Identity connectors.

Agent-Enabled Connectors

There has been considerable debate regarding the merits of agent-based and agent-less connectors in identity management systems. Agent-based connectors reside with a resource (typically on the same host), processing requests from the identity management system and notifying the identity management system of relevant changes within the resource that may require provisioning or synchronization actions on other resources.

The difficulty with agent-based connectors is in managing their day-to-day operations, since they live independently of the identity management system and require their own administrative effort. This is particularly burdensome as the number of resources managed by the identity management system increases.

An alternative to agent-based connectors is the “agent-less” connector, which resides in the identity management system and passes along identity-related updates to resources. Agent-less connectors have the advantage of being tightly integrated with and administered within the identity management system. By consolidating connectors with the identity management system itself, deployment and maintenance is greatly simplified.

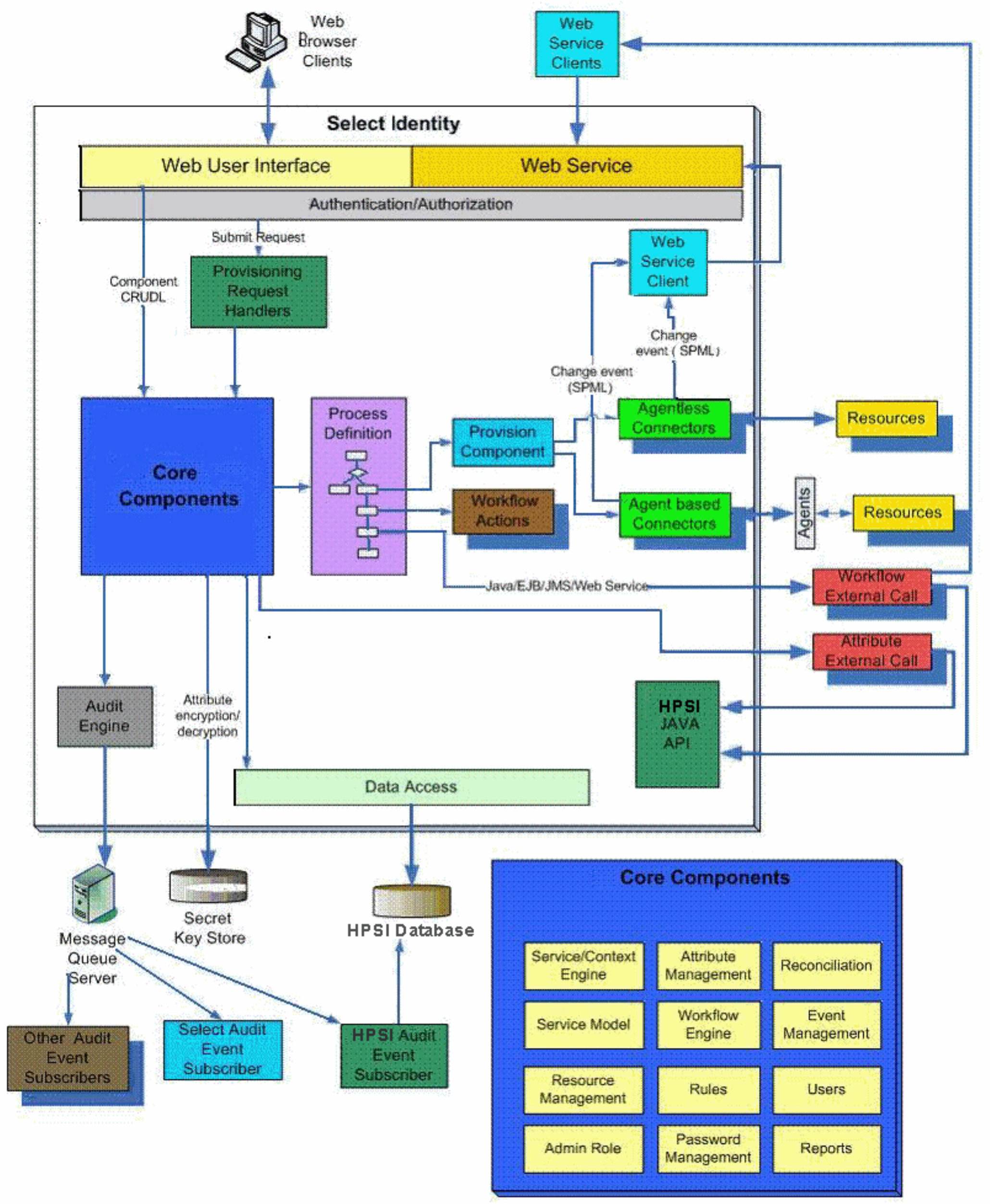
The downside of this approach is that agent-less connectors are optimized for communication in one direction — *from* the identity management system *to* a resource.

When changes to an identity within a resource must be propagated to other resources, an agent-based connector is better suited to the task. For that reason, Select Identity employs an “agent-enabled” connector model, which accommodates both agent-based and agent-less connectors depending on the requirements of the resource and business processes.

System Architecture

Select Identity is an event-driven, J2EE application that enables clustering, failover, multi-phase commit, and asynchronous operation. The following illustration provides a high-level view of the Select Identity system and its components.

Figure 10 Select Identity Architecture



All requests to and from the system use the HTTP protocol. User accounts use one virtual ID to access back-end systems and services and are governed by Select Identity system functions and actions. Accounts are also governed by attributes and entitlements based on the access requirements of the company's products and services.

The Context Engine and Identity Business Process Services components of the Select Identity architecture are particularly useful to administrators and personnel responsible for deploying and maintaining the Select Identity system. These components contain the functions that administrators use most.

Select Identity core components include the following:

- **Service / Context Engine** – Assembles the hierarchy of services and service roles. Filters groupings based on context user groups.
- **Attribute Management** – Facilitates the configuration and setup of attributes in a service, e.g., the definition, characters that make up an attribute and any constraints that apply.
- **Reconciliation** – Reports on the consistency of a user's identity data in multiple resources. Synchronizes any change that occurred on a field designated to sync in or out such as a telephone number change, by replicating it in all the applicable resources and / or the Select Identity database.
- **Service Mode**l – Provides an abstraction layer that allows change management of users' belonging to a service so that it is more dynamic and flexible. With Select Identity's service model, users and groups are not tied tightly to resources or systems, unlike other identity management products in the market.
- **Workflow Engine** – Provides a facility to create, modify, and delete the process steps used in provisioning one or more users.
- **Event Management** – Determines what workflow process or view applies to an event, e.g., add a user.
- **Resource Management** –Captures the definition and details about the resource, whether or not it is authoritative, and allows the administrator to verify connection to the resource.
- **Rules** – Allows for the creation, modification, viewing, and deletion of rules that determine how information is imported and exported throughout the reconciliation process.
- **Users** – Permits management of users in a service. This includes creation, modification, and deletions of user accounts. Users are assigned to services that are subscribed to them, and attributes that apply to these services also apply to the user account.
- **Admin Role** – Defines a role for one or more users to administer one or more service accounts. Multiple Administrator Roles may be created to handle the varied administration needs of any one company.

Glossary

actions

Actions are associated with workflow activities. Actions invoke functions provided by the Select Identity workflow engine or external applications. For example, actions can log information to a file, set a variable to be used later in the workflow, call an external process to provision a user in Select Identity, or store data in a database.

activities

An activity represents a step in a process represented by a workflow template. Activities are the core components of workflow templates; the actions defined in activities do the work necessary to provision users. An activity can contain actions that, for example, set workflow variables, track approvals, start a sub-workflow, send email, and call external applications.

AD

Active Directory

administrative (admin) service

A service used by the Select Identity System Administrator to add approvers. A separate service for administrators eliminates the need to add administrators each time for every service for which they are responsible. Administrators can thus manage user approval requests from numerous services.

agent

A connector that allows for reverse data flow from the SI data store to the enterprise resource. This permits bidirectional replication.

agent-based connector

A two-way connector interface. There are two components: the connector that resides in the same system as Select Identity, and the agent, which resides in the same system as the resource. The agent listens for changes made in the resource, and contacts the resource about changes made in Select Identity.

agentless connector

A one-way connectors. Connectors reside in the Select Identity server and perform communication brokering with the resource.

application invocation

Use the Application Invocation workflow action to call a Select Identity application. Select Identity provides many applications that you can use. You can also develop your own customized applications within Select Identity.

Apply Move Policy option

A Select Identity feature that may be used during reconciliation when changing a user's context. Enabling the Apply Move Policy allows Select Identity to change the user's attributes according to the service role and service-level attribute move policy for each affected service during reconciliation.

approval process

The process of approving the association, modification, or revocation of entitlements for an identity. This process is automated via workflow templates.

approver

A Select Identity administrator who approves user management requests. Approvers must have an admin role that provides approver-level privileges.

asynchronous invocation

An activity or action property that allows the workflow to continue processing a request before an invoked application completes its operation. This property can help reduce request processing bottlenecks.

asymmetric key

A key, or key-pair, that contains a public key and a private key. The public key is used to encrypt; and the private key is used to decrypt. The private key can also be used to sign, but the public key can be used only to verify the signature. The private key is kept secret, while the public key may be widely distributed.

attribute

A data field, containing a value, that helps define an object in Select Identity, such as a service or an identity profile. For example, an attribute could be "department" with possible values of "IT," "sales," or "support." Single-valued attributes allow users to enter or select one valid value for the attribute. Multi-valued attributes allow the selection of more than one valid value.

attribute mapping

The process of associating the name of a resource attribute with that of its corresponding Select Identity attribute. This facilitates and maintains the integrity of data exchange between the two.

audit

A record of events, transactions, configuration changes, and other data about the use, operation, and maintenance of a system.

audit report

A report that presents audit data so that it is organized and readable.

authentication

Verification of the credentials associated with an identity, such as a password and user ID combination, to prevent improper access.

authoritative resource

A resource that has been designated as the “authority” for identity information. Select Identity accounts can be reconciled against accounts in an authoritative source.

authorization

Real-time enforcement of an identity’s entitlements. Authentication is a prerequisite for authorization.

auto discovery

The process of adding user accounts to Select Identity for a specified Service by importing them from a data file.

block

A set of related activities within a workflow. Blocks have two purposes, to define information to be shared by a subset of activities (block-level properties) and to provide block-level reporting. For example, you might define a block that submits an approval request, waits for the response, and returns the status of the request to the workflow. Think of a block as a subprocess within a workflow.

block form

A form specifically associated with a block in a workflow. For example, a workflow could have different forms for each of its approval blocks, each form showing a different set of user attributes.

block view

A view associated with a specific block in a workflow. For example, a workflow could have several views for each of its approval blocks, each showing a different set of user attributes.

business process engine

A system component that serves up all Workflow, Reconciliation, Policy, Forms, Tiered Access, Audit and Report features.

business relationship

see the definition for service role.

business service

A product, facility, or essential business process offered or used by an organization to support day-to-day operations. Examples include online banking services, customer support process, and IT infrastructure offerings such as email, calendaring, and network access. See also: service

Business Service Identity Management (BSIM)

A new, dynamic, and scalable approach to identity management within and between enterprises. BSIM automates the process of provisioning and managing user accounts and access privileges across platforms, applications, and corporate boundaries.

certificate

A digitally signed statement from an entity, the issuer, saying that the public key and information of another entity, the subject) has some specific value.

certificate authority (CA)

An organization or entity that issues digital certificates for use by other parties, and guarantees that the key contained in the certificate belongs to the person, server, organization, or other entity noted in the certificate.

certificate revocation list (CRL)

A list of revoked or cancelled certificates.

challenge and response

A method of supplying alternate authentication credentials, typically used when a password is forgotten. Select Identity challenges the user with a question and, if the answer is correct, resets the password to a random value and sends email to the user.

challenge question

A question designed to elicit very specific information about the person seeking system access. These are most commonly used as a secure fail-safe when a password is lost. Examples are "What is your mother's maiden name" or "Which city were you born in?" Standard challenge questions are preset questions that all users must answer to reset their password. This is usually written by the Select Identity System Administrator as part of setting a challenge/ response policy.   A preset question written by the user and stored with its answer in that user's profile. It must be answered by the user to reset his or her password. Users write their personal challenge question or questions at initial log on after they receive a user name and password. Typical question could include "What year did I graduate from college?" or "What is my pet's name?"

class path

A setting that specifies the directory location of important system files.

cluster

A group of servers that function as a single entity, for example by operating as a jBoss AS, BEA WebLogic, or IBM WebSphere Web application server. This term is also used to refer to a group of user accounts, known specifically as a user cluster.

communication endpoints

The point of termination for the communication link.

composite service

A mechanism for grouping services so that they can be accessed as a unit. For example, users who register for a composite service actually have access to multiple services as a result of registering.

Concero sys admin

A special-purpose administrative role that confers the highest level of entitlements and access.

Configuration Approver

A special-purpose administrative role that confers the privilege of approving configuration management changes in systems where this feature is enabled. Only users who have this role can approve changes to the system's configuration.

configuration management

The configuration management feature establishes an approval workflow for Select Identity configuration changes.

configuration report

Configuration reports provide current system information for user, administrator, and service management activities.

configurations

The configurations capability enables you to import and export Select Identity settings and configurations, such as workflows, resources, services and attributes. This is useful when moving from a test to a production environment.

connectors

Connectors are programs that enable various databases and applications to be accessed by Java application servers that run on the J2EE platform from Sun Microsystems. They enable Select Identity to access an enterprise application and communicate with the system resources that contain your identity profile information. SI comes with several predefined connectors to support data access with backend data stores. For example, a J2EE connector is included that communicates with the Select Identity system resources that contain your identity profile information.

context

A logical grouping of users who are able to access a service.

context attribute

A common attribute that groups users so that they can access a service through a specific service role. For example, an East context groups users with an East attribute so that they can assume the East service role in the XYZ Service.

context engine

A system component that retrieves data according to a service/users context definition.

credential

Information that is used for validation of a person's identity for security and access control purposes. Examples are a user name, password, challenge/response questions, digital certificates, and biometrics.

data file

An SPML file that enables you to define user accounts to be added to Select Identity through Auto Discovery or Reconciliation.

data services template

A specification that provides protocols for the query and modification of data attributes related to a Principal, and exposed by a data service. The protocols are also provided for subscribing to notification related to those attributes and sending and receiving those notifications. Additionally, some guidelines, common XML attributes and data types are defined for data services.

default workflow templates

Select Identity provides default workflow templates, each of which is an example of a common workflow process. You can assign the default templates to service roles to avoid having to build new workflow templates each time. You can use these templates as they are, or you can copy them, rename them, and modify them as you wish. See also workflow templates.

delegated administration

user identity management functions performed by an administrator on behalf of end users. See also self-service.

delegated registration

Account registration performed by an administrator on behalf of another person.

deployment

To install and start software, hardware, capabilities, or services so that they begin to function as intended in the business environment.

disable

To put something out of use without deleting it, usually on a temporary basis. User accounts and services can be disabled in Select Identity, for example.

EAR file

Enterprise Archive; a compressed file format for storing application packages such as Select Identity.

enable

To reinstate something that has been previously disabled, such as a user account, or to put a feature or setting into operation.

encryption

The process of encoding a message so that it can be read only by the sender and the intended recipient.

end user

A role assigned by default to every user in Select Identity. The end user role allows access to the Self Service pages, but conveys no administrative rights.

entitlement

Entitlements are resource-specific privileges granted to an identity. They can be account IDs, role memberships, group memberships, and access rights and privileges. Entitlements are also considered permissions, or access rights.

event handler

Notification templates or workflow templates associated with a particular system event. Notification templates are notification event handlers; workflow templates are request event handlers.

event manager

A system that provides for an event handler interface to process all system events such as sending out e-mail notifications or executing workflows associated with a particular system event. Notification templates are notification event handlers. Workflow templates are request event handlers.

exclusion rule

A rule that handles exceptions. An exclusion rule excludes a set of users with a common attribute or entitlement values from being subscribed to specified services, granted specific entitlements, or allowed particular attribute values. Exclusion rules can be invoked in any workflow by using an external call.

export

To format and store data for use by other applications or systems.

external call

A programmatic call to a third-party application or system for validating accounts or constraining attribute values.

fixed attribute

An attribute automatically granted to certain users as determined by the service role and context associated with their identity.

fixed entitlement

An entitlement automatically granted to a certain users as determined by the service role and context associated with their identity.

form

An electronic document used to capture information from end users. Forms are used by Select Identity for information capture and system operation in many business processes. Most Select Identity forms consist of a subset of service attribute fields in a presentation view that allows certain logical groups users to enter values. For example, you could define a form for administrators to add users, a form for administrators to grant user entitlements, another form for users to modify their own profile, and so on.

function

A grouping of Select Identity permissions.

HSM

Hardware security module.

identity

A set of data relating to a specific individual within a system, including their personal details, contact information, and access privileges to various resources and services. Some identities are special-purpose, such as a system administrator.

identity management (IdM)

Identity management is a set of processes, tools, and agreements among organizations and individuals. It enables people, systems and services to access resources to achieve business objectives.

identity provider (IdP)

An identity provider or IDP is a web site that authenticates a user before the user is sent off to a federated web site. It is possible for a web site to function as an IDP as well as SP.

import

To read, reformat, and store data from another application or system.

JCA

Java Connection Architecture

JDBC

Java Database Connectivity

JDK

Java Developer Kit

JMS

Java Messaging Service

JNDI

Java Naming Directory Interface

key

A piece of information that specifies how plain text is transformed into cipher text, or vice versa during decryption.

key rotation

The scheduled process of changing a Select Identity security key and optionally re-encrypting data with the new key.

keystore

A database of keys and certificates. The private keys are associated with a certificate chain, which authenticates the corresponding public key. Certificates are from trusted entities.

keystore alias

A case-insensitive name assigned to a keystore entry. All keystore entries (key and trusted certificate entries) are accessed via unique aliases.

LDAP

Lightweight Directory Access Protocol

LDIF

Lightweight Directory Interchange Format

Liberty Identity Federation Framework (ID-FF)

Popular open standard federation protocol developed by the Liberty Alliance Project, an alliance of more than 150 companies, nonprofit and government organizations from around the globe. The consortium is committed to developing an open standard for federated network identity.

Lightweight Directory Access Protocol (LDAP)

A software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network. An LDAP directory can be distributed among many servers. LDIF is used to synchronize each LDAP directory.

Lightweight Directory Interchange Format (LDIF)

An ASCII file format used to exchange data and enable the synchronization of that data between Lightweight Directory Access Protocol (LDAP) servers called Directory System Agents (DSAs).

logging.properties file

A text file that defines how Select Identity logs messages and exceptions.

mutual authentication

A method to establish two-way secure communication between clients and servers using digital certificates that conform to the standards defined by the X.509 Public Key Infrastructure (PKI). Each client and the server (communication endpoints) must present a valid certificate, issued for the purpose of authenticating either a client or the server, respectively. This certificate is trusted by the other endpoint and has not been revoked.

name-value pair

A name-value pair is combination of an attribute identifier (field name) and the value of that attribute for a specific object. An example of an attribute-name-value pair for a person would be Name: John Smith.

notification

A message sent when a system event occurs, typically via email. You configure and set up Notifications in Select Identity using a template that controls the information sent in the notification message.

notification template

A notification template defines the format and content of standard e-mail messages automatically sent by Select Identity when certain types of system event occur, such as a user’s account request approval, an account deletion, or a password reset.

OASIS

Organization for the Advancement of Structured Information Standards. A not-for-profit, international consortium that drives the development, convergence, and adoption of e-business standards. The consortium produces Web services standards for security, e-business, and standardization efforts in the public sector and for application-specific markets.

optional entitlement

An entitlement available to certain users as determined by the service role and context associated with their identity. Users have the option of choosing the entitlement.

password reset

Setting a password to a system-generated value.

password validation function

Function that validates the password value against a predefined set of parameters; for example 6-12 alphanumeric characters, at least two numerals, and so forth.

password verification function

Function that verifies the password against a list of authorized passwords.

permission

A permission that allows a user to perform an administrative task within Select Identity.

persistent variable

A variable that is persisted after an instance is passivated. To extend the variable life cycle to the entire instance, you must create the variable to be persistent. This enables the variable to be created before a wait activity, and it will be accessible after the workflow instance resumes. To make a variable persistent, precede the name with $. For example, the $retryCount variable is persistent while retryCount is not.

policy

A set of regulations set by an organization to assist in managing some aspect of its business. For example, policy may determine the type of internal and external information resources that employees can access.

pre-defined variables

Variables for administrator names, user names, and email addresses. These variables enable the system to supply the appropriate information based on the action and the user performing the action.

primary user

The user ID in a user cluster that serves as the Select Identity login name. All other user accounts in the cluster are associated with it as secondary accounts.

profile

A group of descriptive attributes associated with an identity, such as name, address, title, company, or cost center.

profile attributes

Descriptive attributes associated with an identity, such as name, address, title, company, or cost center.

properties

A name-value pair where the value is a string. Properties define constant data when the template is created. Property values do not change at runtime. A global property is shared by all the activities within a workflow instance. The first time you set a property, you initialize its type. Specified properties can be read by external applications using the Workflow API provided by Select Identity. They can also be referenced by a report template to show relevant information in a status report. Some property names are defined by the workflow engine. Use these properties when defining activities and blocks. When you create a workflow template, you must assign values to properties. These property values instruct the workflow how to operate. For example, if you assign a value of three to the joinCount property, the workflow waits for three approvers to join the workflow before it exits the approval block.

reconciliation

The process by which Select Identity accounts are synchronized with a system resource. Account data is added to the Select Identity system from an SPML data file.

reconciliation recovery

The process of using the Select Identity user interface to manually retry or resubmit a reconciliation task. Retrying a task recovers the task, starting from the last failure or stuck point, and retries the record. The status of the original task or record is overwritten with the latest execution result. Resubmitting a task starts a new task from the beginning with an exact copy of the data from the old task. The new task has its own records and report. The records that were left in process during the previous job are terminated.

reconciliation rule

A rule that defines operations to be performed on a user account. Reconciliation rules perform these operations based on eligibility criteria. The actions specified in the rule are only applied if the user meets the qualification criteria. Reconciliation rules can be invoked during reconciliation as defined on the resource reconciliation policy or by a workflow external call.

reconciliation termination

The process of using the Select Identity user interface to manually stop the processing of a reconciliation task. Completed tasks are unaffected. Tasks that have not been processed are terminated.

registration

The process of requesting access to one or more resources. Registration is generally performed by an end user seeking resource access, or by an administrator registering a user on a user's behalf.

request

An event within Select Identity initiating the addition, modification, or removal of a user account.

request event

Whenever a user account is added, modified or removed, it is registered within Select Identity as a request event.

resource

Any single application or information repository that is part of your Select Identity BSIM solution. Resources typically include applications, directories, and databases that store identity information.

role

A simple abstraction that associates entitlements with identities. A role is an aggregation of entitlements, and is usually organized by job function.

rule

An XML file used by Select Identity to control system behavior. For information on the type of rules used in Select Identity, see reconciliation rule and exclusion rule.

secondary user

An account other than the primary user in a user cluster.

security repository

A file that stores logical keys, making physical keys transparent to client.

self-service

The ability to securely allow end users to manage identity and service access on their own behalf.

self-signed (signing) certificate

An identity certificate that is signed by its creator and signed off by its creator as legitimate.

service attribute

A set of attributes and values that are available for or required by a Service. Attributes are created and managed through the Attributes pages.

service attribute properties

Settings that determine how fields are displayed in forms.

service attribute values

Restrict the values that a user or approver can select from in a form.

service form

A restricted form of a service that is valid for a group of users. Forms enable you to define a subset of service registration fields, change field names, reorder fields, and mask field values for specific users.

service role

A Select Identity abstraction that defines how a logical grouping of users will access a subset of a Select Identity service's entitlements. For example XYZ Service could have three business relationships: East, Central, and West. These business relationships can be subdivided as well, for example the business relationship West could contain two more granular business relationships: Northwest and Southwest. A service can contain an unlimited number of levels of business relationships.

SHA

Secure Hash Algorithm

single sign-on (SSO)

A session/authentication process that permits a user to enter one set of credentials (name and password) in order to access multiple applications. A Web SSO is a specialized SSO system for web applications.

SOAP

Simple Object Access Protocol

SPML

Service Provisioning Markup Language

SPML data file

A server-parsed XML file used to add and provision accounts in Select Identity. For reconciliation, SPML data files can be generated from both non-authoritative and authoritative resources. Typically, one SPML file is generated for each resource. The SPML file contains changes for a specific period to user account information, such as additions, deletions, or changes. The files are uploaded into Select Identity, and the user account information in Select Identity is updated during reconciliation.

SSO

single sign-on

subject certificate

A certificate that identifies the client or server, requires authentication, and is stored in the keystores on both the client and the server.

symmetric key

A symmetric key is also referred to as a secret key, which is used for both encryption and decryption. The sender and receiver of a message share a single, common key that is used to encrypt and decrypt the message.

terminate

Removing a user's account from Select Identity, so that it no longer exists.

transition

A transition provides a link from one activity to another. There are two kinds of transitions—conditional and unconditional. Using an unconditional transition to link two activities means that the second activity is always executed after the first. With a conditional transition, a certain condition must first be met before the next activity is executed. For example, you can define a transition that only allows the workflow to progress if at least two administrators approve a request.

TruAccess.properties file

A text file that contains numerous Select Identity configuration settings that you can customize.

trust store

A file that stores the corresponding self-signed or signing certificates which are used to verify the subject certificates.

URI

Uniform Resource Identifier

user cluster

A group of user IDs consisting of one primary user account and multiple associated secondary accounts. This is the mechanism used to enable a single person whose identity is managed in Select Identity to have several user accounts on multiple resources.

user import

The process of adding user accounts for a specified Select Identity service by copying them into the database from a data file.

Wait activity

The Wait Activity check box is selected if the activity you are creating requires an action to occur before moving forward to the next activity (e.g. approver approves/rejects an account request).

wait instance

When a running workflow instance hits a wait activity, it is suspended until it is reactivated by an external source. The suspended workflow instance is called a wait instance.

WAR file

Web Archive file; a compressed format for packaging multiple files. Has the extension .war and is used by servlets.

Web application server

A computer or group of computers configured to provide infrastructure for Interned-based data and communication transactions.

Web Services

An XML-based request framework using the Service Provisioning Markup Language (SPML) to provide customizable user management functions in Select Identity.

Web Services Definition Language (WSDL)

An XML format for describing network services as a set of endpoints operating on messages containing either document-oriented or procedure-oriented information. The operations and messages are described abstractly, and then bound to a concrete network protocol and message format to define an endpoint. Related concrete endpoints are combined into abstract endpoints (services). WSDL is extensible to allow description of endpoints and their messages regardless of what message formats or network protocols are used to communicate.

WfMC

Workflow Management Commission

workflow

The process by which requests are completed in Select Identity, including the various levels of approval needed for different types of request. Workflows are depicted in the form of a process flow, defined in a workflow template created in Workflow Studio. Requests can be tracked using the workflow to ascertain their current state of completion in detail.

Workflow Approver Role

A default Administrative role that grants permission to approve user provisioning workflow operations.

workflow external call

A "subroutine" that is called during the workflow process. This could be an external application invocation such as a small custom application that calls external processes outside of the normal workflow process.

workflow studio

The functionality that enables you to create and manage workflow templates.

Workflow Studio Editor

The Select Identity capability with a special graphical user interface that enables you to create and manage workflow templates.

WSDL

Web Services Definition Language

XML Processing Description Language (XPDL)

When you save a workflow template, it is saved in the Select Identity repository as an Extensible Markup Language (XML) file. Its format is the XML Processing Description Language (XPDL) as defined by the Workflow Management Coalition (WfMC).

XPDL

XML Processing Description Language

Index