HP OpenView Select Identity

Software Version: 4.10

New Information About Select Identity 4.10

Document Release Date: November 2006
Software Release Date: November 2006

Legal Notices

Warranty

Hewlett-Packard makes no warranty of any kind with regard to this document, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

A copy of the specific warranty terms applicable to your Hewlett-Packard product can be obtained from your local Sales and Service Office.

Restricted Rights Legend

Use, duplication, or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause in DFARS 252.227-7013.

Hewlett-Packard Company
United States of America

Rights for non-DOD U.S. Government Departments and Agencies are as set forth in FAR 52.227-19(c)(1,2).

Copyright Notices

This product includes software developed by the Apache Software Foundation (http://www.apache.org/). Portions Copyright (c) 1999-2003 The Apache Software Foundation. All rights reserved.

HP OpenView Select Identity (OVSI) uses software from the Apache Jakarta Project including:

- Commons-beanutils
- Commons-collections
- Commons-logging
- Commons-digester
- Commons-httpclient
- Element Construction Set (ecs)
- Jakarta-poi
- Jakarta-regexp
- Logging Services (log4j)

Additional third party software used by HP OpenView Select Identity includes:

- JasperReports developed by SourceForge
- iText (for JasperReports) developed by SourceForge
- BeanShell
- Xalan from the Apache XML Project
- Xerces from the Apache XML Project
- Java API for XML Processing from the Apache XML Project

Trademark Notices

Unix® is a registered trademark of The Open Group.

This product includes software provided by the World Wide Web Consortium. This software includes xml-apis. Copyright © 1994-2000 World Wide Web Consortium, (Massachusetts Institute of Technology, Institute National de Recherche en Informatique et en Automatique, Keio University). All Rights Reserved. http://www.w3.org/Consortium/Legal/

Intel and Pentium are trademarks or registered trademarks of Intel Corporation in the United States, other countries, or both.

AMD and the AMD logo are trademarks of Advanced Micro Devices, Inc.

BEA and WebLogic are registered trademarks of BEA Systems, Inc.

VeriSign is a registered trademark of VeriSign, Inc. Copyright © 2001 VeriSign, Inc. All rights reserved.

Support

Please visit the HP OpenView support web site at:

http://www.hp.com/managementsoftware/support

This web site provides contact information and details about the products, services, and support that HP OpenView offers.

HP OpenView online software support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valuable support customer, you can benefit by using the support site to:

- Search for knowledge documents of interest
- Submit enhancement requests online
- Download software patches
- Submit and track progress on support cases
- Manage a support contract
- Look up HP support contacts
- Review information about available services
- Enter 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 log in. Many also require a support contract.

To find more information about access levels, go to:

http://www.hp.com/managementsoftware/access_level

To register for an HP Passport ID, go to:

http://www.managementsoftware.hp.com/passport-registration.html

New Information About Select Identity 4.10

This document provides information about Select Identity that became available after its product documentation was completed and immediately prior to actual release of the product.

In general, this information will be incorporated into the product documentation during the next release cycle.

This document contains the following topics:

Administrative Permission Definitions

When configuring administrative roles, whether during role creation or modification, you assign permissions to a role by selecting from numerous individual permissions and levels of authority. Each selection grants permission (authority) to view, create, delete, or change certain types of information (users, services, resources, roles, and contexts, for example).

There are four default administrative roles in Select Identity:

- **End User:** The minimum level of access, conferring only individual self-service permissions. This role is intended for non-administrative accounts.
- **Workflow Approver:** This role solely and specifically confers the right to approve provisioning operations during a workflow that includes approval actions.
- **Configuration Approver:** This role solely and specifically confers the right to approve configuration changes made anywhere in the system, if Configuration Change Management is enabled.
- **Concero Sys Admin:** The top-level administration role, with the widest-ranging permissions.

You can develop custom administrative roles consisting of varied and targeted access to system functional areas and data selections. This section provides a brief reference for each permission, as a series of tables by permission type.

Requests Permissions

Sets the permissions for users to view, terminate, approve, reject or retry requests.

Permission	Description
User Request Status List	Permits the user to view, terminate, and retry requests.

Permission	Description
User Request	Access the User Request Status List page.
Request Worklist	View, modify, approve, or reject requests.
Approval	Access to the **Approval** button on User Request Status List page.

Reports Permissions

Determines the specific reports users are allowed to access. Users given access to a report get permission to add, view, modify, run, schedule and delete the report. Partial access cannot be given.

Permission	Description
Audit Reports	Create different kinds of audit reports.
Audit Service Report	Access to the Audit Service report.
User Audit Report	Access to the Audit User report.
Audit User Summary Report	Access to the Audit User Summary report.
Audit User Creation Report	Access to the Audit User Creation report.
Audit User Creation Summary Report	Access to the Audit User Creation Summary report.
Audit User Deletion Report	Access to the Audit User Deletion report.
Audit User Deletion Summary Report	Access to the Audit User Deletion Summary report.
Audit User Termination Report	Access to the Audit User Termination report.
Audit User Termination Summary Report	Access to the User Termination Summary report.
Audit User Password Report	Access to the Audit User Password report.
Audit User Password Summary Report	Access to the Audit User Password Summary report.
Audit User Login Report	Access to the Audit User Login report.
Set Hint Audit Report	Access to the Audit Hint report.
Set Hint Audit Summary Report	Access to the Audit Hint Summary report.
Resource Users Configuration Report	Access to the Resource Users Configuration report.
Resource Entitlements Configuration Report	Access to the Resource Entitlements Configuration report.
Resource Reconciliation Reports	Access to the Resource Reconciliation Reports report.

Configuration Reports

Determine authority to view and create various kinds of configuration report for the system.

Permission	Description
User Configuration Report	Access to the User Configuration report.
User Configuration Summary Report	Access to the User Configuration Summary report.
User Configuration Detail Report	Access to the User Configuration Detail report.
Admin Configuration Report	Access to the Admin Configuration report.

Service Studio Permissions

Determine the authority an administrator has to manage assigned services. Administrators may be given permission to create, modify, and delete service forms, service roles, and context groups. Administrators may also be given permission to reconcile services and set service attribute properties for assigned services.

Connector Permissions

Authority to manage connectors for the services assigned to the administrator. Administrators can view, deploy, modify, or delete according to the permissions granted.

Permission	Description
View Connector	View the details of a connector.
Deploy Connector	Deploy a connector.
Modify Connector	Modify a connector.
Delete Connector	Remove a connector from the available list of connectors when the connector is no longer being used by any resource.

Resource Permissions

Manage resources for applications and data stores within assigned services. Administrators may view, deploy, modify, delete, and copy resources. Additionally administrators can view attribute fields and modify attribute field mapping based on permissions given.

Permission	Description
View Resource	View the details of a resource.
Deploy Resource	Deploy a new resource.
Modify Resource	Change the options associated with a system resource on which your products and services rely.

Permission	Description
Delete Resource	Remove a resource from Select Identity. Resources may be deleted if no users or services are associated with the resource.
Copy Resource	Create a new resource by using an existing resource and modifying its options.
View Resource Attributes	View the list of attributes associated with a resource.
Modify Resource Attribute Mapping	Change the how resource field attributes are mapped to Select Identity field attributes so that reconciliation updates the data correctly.
Modify Service Role	Modify the service role details.
Delete Service Role	Remove a service role.
View Service Role	See details associated with a service role.

Service Permissons

Determines the authority an administrator has to manage assigned services. Administrators may be given permission to create, modify, and delete service forms, service roles, and context groups. Administrators may also be given permission to reconcile services and set service attribute properties for assigned services.

Permission	Description
Add Service	Create a new service.
Modify Service	Change services associated with a user.
Copy Service	Create a new service by using an existing service definition and modifying its options.
Delete Service	Remove a service from Select Identity (if no users are subscribed to the service).
View Service	View the basic information page of service
Set Service Attribute Values	Add, modify, or delete values for service attributes for a service.
View Service Attribute Values	View the assigned values for service attributes of a service.
Set Service Attribute Properties	Define the settings for a service attribute.
View Service Attribute Properties	See the settings defined for service attributes.
Create Form	Add a new form to Select Identity.
Create Form (Multi-page)	Add a new form consisting of multiple pages of attribute fields to Select Identity.
Modify Form	Change the attribute fields for an existing form.

Delete Form	Remove a form from the list of available forms.
View Form	View the settings of an existing form.
Create Service Role	Define a new service role to attach views and workflows to a request event. This permission also allows you to set fixed/ optional values for attributes associated with the service role.

Permission	Description
Create Context	Define a new context for a service role.
Modify Context	Modify a service role context.
Delete Context	Remove selected context user groups. All dependencies must also be removed.
View Context	See the details of a defined context.
Reconcile Service	Perform service reconciliation, which updates users of a service following changes to a service.

Notification Permissions

View, add, copy, and delete notification templates for assigned services.

Permission	Description
View Notification Template	View the content of a notification template.
Add Notification Template	Create a new notification template.
Copy Notification Template	Define a new notification template by using an existing notification template as a starting point.
Modify Notification Template	Change the details of a notification template.
Delete Notification Template	Remove a notification template from the list of available notification templates.

External Calls Permissions

Manage external calls by viewing, adding, modifying, and deleting calls.

Permission	Description
View Call	See the external call settings.
Add New Call	Create a new external call.
Modify Call	Change the settings of an existing external call.
Delete Call	Remove an external call.

Workflow Studio Permissions

Add, copy, view, modify, and delete workflow diagrams.

Permission	Description
Add Workflow Template	Create a new workflow template.
Copy Workflow Template	Create a new workflow template by using an existing workflow template as a starting point.
View Workflow Template	View the contents of a workflow template.
Modify Workflow Template	Change the contents within a workflow template.
Delete Workflow Template	Remove a workflow template.

Attributes Permissions

Add, view, modify, map and delete attribute fields.

Permission	Description
Add Attributes	Create a new attribute if the attribute does not already exist.
View Attributes	View the details of an existing attribute definition.
Modify Attributes	Modify an existing attribute.
Delete Attributes	Remove an attribute.

Tools Permissions

Determines the authority an administrator has to manage administrative roles, modify hint questions and challenge/response policies, the ability to perform bulk uploads, user imports and reconciliation, configuration change, rules, server management, system security, and the ability to import or export configurations.

Admin Roles Permissions

Manage administrator roles by viewing, adding, copying, modifying, and or deleting roles.

Permission	Description
View Admin Roles	View details, including permissions, associated with defined administrator roles.
Add Admin Roles	Create a new administrator role and define permissions available to that administrator role.
Copy Admin Roles	Create a new administrator role by using an existing administrator role as a starting point.
Modify Admin Roles	Change the role description and permissions associated with an administrator role.
Delete Admin Roles	Remove an administrator role.

Challenge/Response Permissions

Modify hint questions and hint policies by setting the parameters for standard and personal hints.

Permission	Description
Modify Challenge/ Response	Change the questions that an end-user would be required to answer to modify their password.

User Import Permissions

Import users from external resources into HP OpenView Select Identity. Administrators may schedule user import jobs, schedule service assignment, and view services assigned based on the permissions given.

Permission	Description
Schedule User Import	Configure Select Identity to import user accounts from resource files on a scheduled date.
User Import List	View the status of previously scheduled user import tasks.
Schedule Services Assignment	Schedule a time to assign services to existing users.
Service Assignment List	View the status of all scheduled service assignments.

Reconciliation Permissions

Create and manage reconciliation jobs. Permission may be granted to add, view, modify, and delete reconciliation jobs. Administrators may also be given permission to view the tasks of any job being processed for services assigned.

Permission	Description
Add New Reconciliation Job	Schedule a new reconciliation task.
View Automated Job	View the details of a scheduled reconciliation task.
Modify Automated Job	Change the details of a scheduled reconciliation task.
Delete Automated Job	Remove a scheduled reconciliation task.
View Task Status	View the status of all reconciliation tasks.

Bulk Operations Permissions

Add, view, modify, and delete bulk jobs that provision or move large numbers of users. Administrators may also be given permission to view the task of any job being processed.

Permission	Description
Add New Automate Job	Schedule a new bulk job.
View Automated Job	View the details of a scheduled bulk job.

Modify Automated Job	Change the details of a scheduled bulk job.
Delete Automated Job	Remove a scheduled bulk job.
View Task Status	View the status of all bulk jobs.
Bulk Move User Task	View the status of all bulk tasks.

Configurations Permissions

Import and export XML files used to move configurations from one instance of HP OpenView Select Identity to another. Administrators may also export XML configuration files, make changes, and then import the files back into the same instance.

Permission	Description
Export Configuration	Create configuration export files.
Import Configuration	Import configuration information into Select Identity.
Manage Migration Policy	Change the object migration security settings.
View Migration Policy	View the object migration security settings.
Manage Import Sources	Change the configuration import file directory, certificate, and encryption settings.
View Import Sources	View the configuration import file directory, certificate, and encryption settings.
Manage Export Destinations	Change the configuration import file directory, certificate, and encryption settings.
View Export Destinations	View the configuration export file directory, certificate, and encryption settings.

Configuration Change Management Permissions

Manage migration policy, sources, and destinations.

Permission	Description
Configuration Change Management	Enable and disable configuration change approval by function type.
Approve Configuration Change	Approve configuration change requests.
Manage Configuration Change Requests	Retry and terminate configuration change requests.

Rules Permissions

Upload, view, modify, and delete rules

Permission	Description
Add Rule	Add a rule file to Select Identity.
Modify Rule	Change a rule file.
View Rule	View a rule file.
Delete Rule	Remove a rule file from Select Identity.

Server Management Permissions

View the status of servers used by Select Identity.

Permission	Description
Server Instance List	View the server instance list.

System Security Permissions

Change system encryption key settings.

Permission	Description
Security Setup	Change system encryption key settings.

User Management Permissions

Add, view, modify, disable, enable, delete, and transfer user accounts, service memberships and user authorities within the proper user group context and assigned services. Administrators may also receive permission to view resources assigned to users, reset passwords, move user accounts and terminate users within assigned services.

Permission	Description
View User Resource Profile	View user's account associated with resource attributes.
View Service Membership	View **Service Subscription** tab, which lists the services associated with a user.
Add New User	Create users.
Modify Service Membership	Change service membership for a user's account.
Enable Service Membership	Enable service membership for a user's account.
Disable Service Membership	Disable service membership for a user's account.
Delete Service Membership	Remove service membership for a user's account.
Add Account	Add secondary accounts to a user.

Permission	Description
Enable Account	Enable another user's account.
Disable Account	Disable another user's account.
Delete Account	Remove another user's account.
Enable All Services	Enable all services for other users.
Disable All Services	Disable all services for other users.
Reset Password	Reset all passwords for other users.
Terminate User	Terminate other users.
Add Service	Add services to a user's account.
Modify User Profile	Change other users' attributes.
View User Profile	View other user profiles.
Manage User Expiration	Set user expiration dates and terminate users.
Move User	Move a user from current context to another context.
Transfer Accounts	Transfer the accounts of one user to another user.
View User Subscription Report	View the User Subscription report.
View User Resource Report	View the User Resource report.
View User Audit Report	View the User Audit report.
Change Username	Change Select Identity user names.