HP OpenView Select Access

Integration Paper for Microsoft Active Directory Application Mode (ADAM) Server

Software Version Tested Against: 6.0

for Windows Operating Systems

February 2005

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

HP OpenView Select Access includes software developed by third parties. The software HP OpenView Select Access uses includes:

- The OpenSSL Project for use in the OpenSSL Toolkit.
- Cryptographic software written by Eric Young.
- Cryptographic software developed by The Cryptix Foundation Limited.
- JavaService software from Alexandria Software Consulting.
- Software developed by Claymore Systems, Inc.
- Software developed by the Apache Software Foundation.

- JavaBeans Activation Framework version 1.0.1 © Sun Microsystems, Inc.
- JavaMail, version 1.2 © Sun Microsystems, Inc.
- SoapRMI, Copyright © 2001 Extreme! Lab, Indiana University.
- cURL, Copyright © 2000 Daniel Stenberg.
- Protomatter Syslog, Copyright © 1998-2000 Nate Sammons.
- JClass LiveTable, Copyright © 2002 Sitraka Inc.

For expanded copyright notices, see HP OpenView Select Access `<install_path>/3rd_party_license` directory.

All other product names are the property of their respective trademark or service mark holders and are hereby acknowledged.

Trademark Notices

Java™ is a US trademark of Sun Microsystems, Inc.

HP-UX Release 10.20 and later and HP-UX Release 11.00 and later (in both 32 and 64-bit configurations) on all HP 9000 computers are Open Group UNIX 95 branded products.

Intel®, Pentium®, and Itanium® are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux® is a U.S. registered trademark of Linus Torvalds.

Microsoft®, Windows, Windows NT®, and Windows XP®, are U.S. registered trademarks of Microsoft Corporation.

Unix® is a registered trademark of The Open Group.

All other product names are the property of their respective trademark or service mark holders and are hereby acknowledged.

Support

Please visit the HP OpenView web site at:

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

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

You can also go directly to the support web site at:

http://support.openview.hp.com/

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 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 the following URL:

http://support.openview.hp.com/access_level.jsp

To register for an HP Passport ID, go to:

https://passport.hp.com/hpp2/newuser.do

contents

1

Understanding Your Select Access Integration

Select Access is an integral part HP's comprehensive Identity Management suite. It delivers a full solution for complex access management across the enterprise. Select Access:

- Automates access control and identity life-cycle management for profiles stored in a Microsoft Active Directory Application Mode (ADAM) repository.
- Extends the enterprise through federation.
- Delegates management to business owners and the end users themselves.

Along with robust workflow, user self-service, reporting, and delegated administration capabilities, Select Access is the most comprehensive access control system available. Select Access simplifies your ability to secure ADAM identity access to corporate resources.

Assumptions in this Document

This document assumes the following:

- That you have a complete knowledge of how a user service directory varies from that of other LDAP 3.0-compliant deployments.

- That you have ADAM installed and running on your network.
- That you understand the features and functions of Select Access.

Integrating Select Access with ADAM

For organizations that have integrated their network applications with ADAM, Select Access offers you the ability to protect those applications via the same user service directory with which you are already integrated. Because ADAM is a user service directory, not a system service directory, you need to understand where the most critical integration points lie. Specific integration points unique to this deployment are discussed below.

Understanding the Key Components of this Integration

To use ADAM as the identity and policy repository for Select Access, you need to ensure that ADAM's schema is compatible with Select Access. This requires that you understand:

- How schemas are set up and the order in which schemas need to be referenced. Reference order is critical to ensuring that day-to-day operations of the directory remain intact.
- The importance of SSL and why HP recommends you enable SSL-based communications between ADAM and Select Access.
- The importance of adding the `organizationUnit` object class, if the entry does not already exist. Select Access uses this object to store group information. However, if you already have users stored in your ADAM repository, this entry typically should exist.
- Why a user with an administrative role must create a new identity for "manager" if one does not already exist. Without this identity, Select Access cannot read/write to the ADAM repository.
- The fact that Select Access does not use Microsoft's SSPI. Therefore, a user ID must be created.

- How to use the Select Access Policy Builder—the Java GUI that provides you with a view of all identities in your ADAM repository as well as all corporate assets that you want to protect with Select Access. The combination is displayed as a hierarchical matrix which can be easily expanded and contracted to facilitate quick navigation and simply manage your access and authentication policies.

For a complete overview of all Select Access components, refer to the *HP OpenView Select Access 6.0 Installation Guide*.

2

Integration Tasks

To ensure Select Access and ADAM function properly as a unit, you must follow a specific series of steps to integrate them correctly. Table 1 summarizes the steps you need to perform to configure and delegate all authentication and authorization responsibilities to Select Access.

Table 1 Integrating Select Access with ADAM

Setup Task	Details
Step 1: Install ADAM and create a new partition instance.	1 Run `adamsetup.exe` from a command prompt or double-click `adamsetup.exe` in Windows Explorer. 2 Create a new partition instance. 3 Verify that you have a new partition instance. Select Access needs this partition instance to load its schema and policy directory entries
Step 2: Add the Active Directory and Select Access schemas. Note: If you already added the Active Directory schema to your ADAM directory server, you may only need to add the Select Access schema. This depends on how much of the entire set of the Active Directory schema you added and how much customization you did to it. You can examine the `ad_schema.ldf` file and compare it to your current ADAM schema. The path to the schema files is: `\Select Access\Schema\ADAM`	1 Back up your directory server. Do this before you add any new schema elements. 2 To go to a command prompt, do one of the following: • Click **Start → Programs → ADAM → ADAM Tools Command Prompt** • At a DOS command prompt, change directories to `\Windows\ADAM`. 3 At the command prompt, type `ldifde.exe` to set the Active Directory and Select Access schemas in this order: • `ad_schema.ldf` (Active Directory schema) • `sa_schema.ldf` (Select Access schema)

Table 1 Integrating Select Access with ADAM (cont'd)

Setup Task	Details
Step 3: Set up ADAM to use SSL so you can set a user's password through the Select Access Policy Builder.	For details, refer to your Microsoft documentation. Although it is not recommended, you can change the directory server behavior using the `dsmgmt.exe` command in the ADAM Tools command prompt. Refer to the ADAM technical reference manual for instructions.
Step 4: If no users/groups exist, create an entry that uses the `organizationUnit` object. Note: If users/groups exist, skip to the next step.	1 Click **Start** → **Programs** → **ADAM** → **ADAM ADSI Edit**. 2 Using the `organizationUnit` object, create a group named `Users`.

Table 1 Integrating Select Access with ADAM (cont'd)

Setup Task	Details
Step 5: Create an administrator profile for Select Access. This profile allows the Select Access system to log into ADAM as needed.	Creating an Administrator Profile for Select Access on page 15.
Step 6: If you want to use the ADAM directory as both your Select Access Policy Store and as a source of user data, configure the Administration Server and Directory Server.	1 Run the setup tool. 2 Click **Next** on the Welcome screen. 3 Click **Next** on the list of detected components screen. The Administration Server's setup wizard appears. 4 Click the **Configure** button. The Administrator setup screen appears. 5 Configure the Select Access administrator credentials and click **Next**. The Directory Server setup screen appears 6 Use the credentials of your newly created "manager" profile. Note: In the **Login Name** field, type the user ID you configured in Step 5. For example, "cn=manager." For details, see Step 4 in To create an Administrator Profile for Select Access on page 16. 7 In the **Password** field, type the password you configured for that identity. Select Access uses these credentials each time it logs into the ADAM directory.

Table 1 Integrating Select Access with ADAM (cont'd)

Setup Task	Details
Step 7: If you only want to use ADAM as a source of user data, configure the new user store using the Policy Builder.	1 Start the Policy Builder. 2 Click **Tools** → **Identity Location Configuration**. 3 Click **Add**. 4 Type the detailed information for the ADAM directory and click **OK**. For more information, see the *Policy Builders Guide*.

Creating an Administrator Profile for Select Access

An entity profile for Select Access is not part of ADAM by default. The most important elements are:

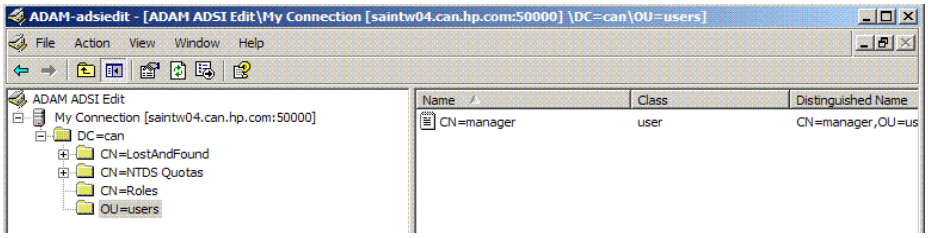
- The role to which it is assigned (that is, role)
- The login credentials Select Access uses to log in

Why you need an Administrator Profile

An administrator profile gives Select Access the ability to act as the ADAM administrator. This allows Select Access to log in and manage user profiles and authentication/authorization policies accordingly. The creation of this profile is a vital step in the integration of these two products.

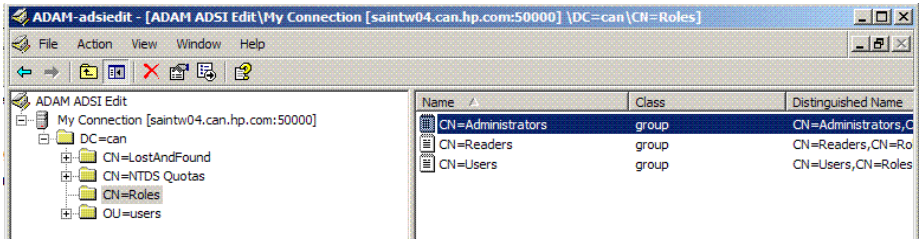
To create an Administrator Profile for Select Access

1 Create a `cn=manager` entry in the `OU=users` container..

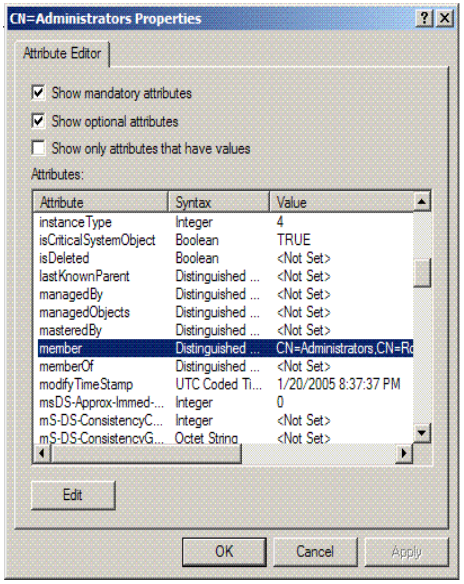


2 Do the following to add this entity profile as a member of the `Administrators` role:

a Click **CN=Roles**

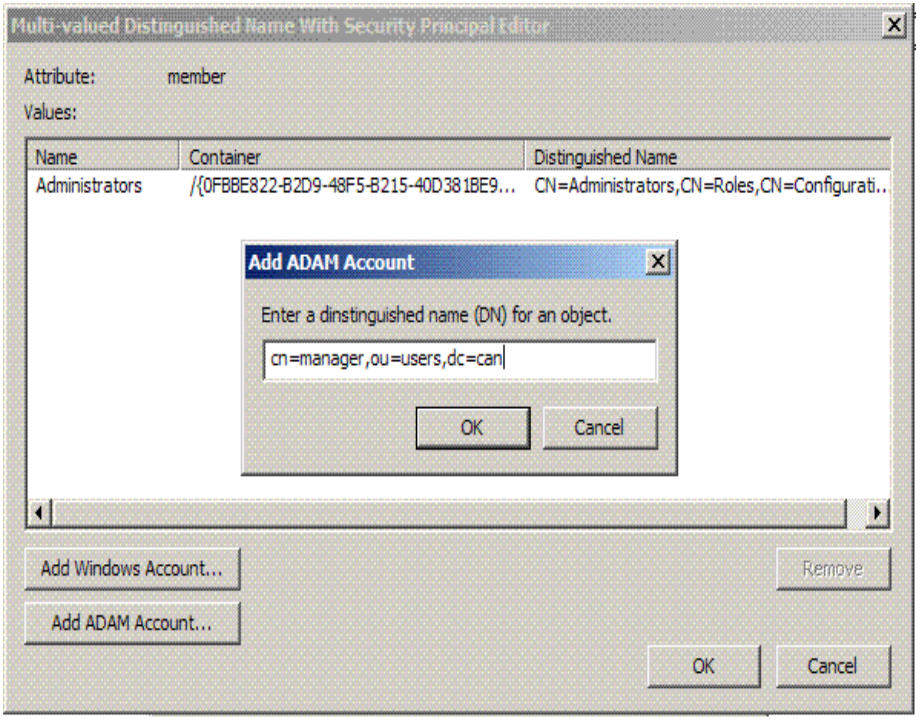


b Right-click the **cn=administrator** entry, and then click **Properties**. The CN-Administrator Properties dialog box appears.



c In the CN-Administrator Properties dialog box, click **Edit**. The Multi-valued Distinguished Name With Security Principal Editor dialog box appears.

d In the Multi-valued Distinguished Name with Security Principal Editor dialog box, click **Add ADAM Account**. To set your newly created `cn=manager` entry as an administrator role, edit the members attributes and type the required information.



3 Do the following to create a password for the entity profile for Select Access.

a Right-click the newly created `cn=manager` entry in the `OU=users` directory entry.

b Click **Reset Password**. The Reset Password dialog box appears.

c Type and confirm a new password.