HP OpenView Select Identity

Connector for Netegrity Siteminder

Connector Version: 3.7

Installation and Configuration Guide

Document Release Date: March 2006
Software Release Date: March 2006

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

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notices

Select Identity 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 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
- SOAP developed by the Apache Software Foundation
- JavaMail from SUN Reference Implementation
- Java Secure Socket Extension (JSSE) from SUN Reference Implementation
- Java Cryptography Extension (JCE) from SUN Reference Implementation
- JavaBeans Activation Framework (JAF) from SUN Reference Implementation

Trademark Notices

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

Contents

1 Introduction 7

About HP OpenView Select Identity. 7

About Connectors 7

About Netegrity SiteMinder Connector 7

2 Installing the Connector 9

System Requirements 9

Installation Procedure 10

Extract the Contents of Schema File 10

Deploy the Connector on Application Server 10

Configure the Application Server 11

Configure SiteMinder 12

Configure the Connector with OVSI 18

3 Uninstalling the Connector. 21

A Sample Images 23

1 Introduction

This chapter gives an overview of the HP OpenView Select Identity connector for Netgrity SiteMinder. An HP OpenView Select Identity connector allows you to provision users and manage identities on resource_system. At the end of this chapter, you will be able to know about:

- the benefits of HP OpenView Select Identity
- the role of a connector
- the connector for Netgrity SiteMinder

About HP OpenView Select Identity

HP OpenView Select Identity (OVSI) provides a new approach to identity management. It helps you manage the entire identity lifecycle of an enterprise application. By using OVSI, you can automate the process of provisioning and managing user accounts and access privileges across platforms, applications, and corporate boundaries. OVSI communicates with the enterprise information system through connectors, and automates the tasks of identity management. The enterprise information system, which is also referred to as **resource**, can be a database, a directory service, or an ERP package, among many others.

About Connectors

You can establish a connection between a resource and OVSI by using a connector. A connector is resource specific. It is installed on the system where OVSI is installed. The combination of OVSI and connector helps you perform a set of tasks on the resource to manage identity. A connector can be **unidirectional** or **bidirectional**. A unidirectional connector helps you manage identities from OVSI, but if any change takes place in resource, it cannot communicate that back to OVSI. On the other hand, a bidirectional connector can reflect the changes made on resource back to OVSI. This property of bidirectional connectors is known as **reverse synchronization**.

About Netegrity SiteMinder Connector

The Netegrity SiteMinder connector — hereafter referred to as SiteMinder connector — enables OVSI to perform the following tasks in SiteMinder:

- Add, update, and remove users
- Retrieve user attributes

- Enable and disable users
- Verify a user's existence
- Change user passwords
- Reset user passwords
- Retrieve all entitlements
- Retrieve a list of supported user attributes
- Grant and revoke entitlements to and from users

It is a unidirectional connector and pushes changes made to user data in the OVSI database to the target SiteMinder server and its configured user store (such as Sun ONE Directory Server). The mapping file defines how OVSI fields are mapped to SiteMinder fields.

➤ This connector can be used with OVSI 4.0 and 3.3.1

2 Installing the Connector

SiteMinder connector comprises of a Resource Adapter Archive (RAR) file and a Schema file, which are listed in Table 1 below.

Table 1 SiteMinder Connector Files

Serial Number	File Name	Description
1.0	`NetSmConnector.rar`	It contains the RAR file (the binaries).
2.0	`NetSmSchema.jar`	It contains the mapping files and a sample `WebAgent.conf` file.

These files are located in the Netegrity SiteMinder directory on the Select Identity Connector CD.

System Requirements

The SiteMinder connector is supported in the following environment:

Table 2 Platform Matrix for SiteMinder connector

Select Identity Version	Application Server	Database
3.0.2	WebLogic 8.1.2 on Windows 2000	SQL Server 2000
	WebLogic 8.1.2 on Windows 2003	SQL Server 2000
	WebLogic 8.1.2 on Solaris 9	Oracle 9i
	WebLogic 8.1.2 on HP-UX 11i	Oracle 9i
3.3	WebLogic 8.1.4 on Windows 2003	SQL Server 2000

Table 2 Platform Matrix for SiteMinder connector

Select Identity Version	Application Server	Database
3.3.1	WebLogic 8.1.4 on Windows 2003	SQL Server 2000
	WebLogic 8.1.5 on RedHat Enterprise Linux AS Release 3.0	Oracle 10g
4.0	The SiteMinder connector is supported on all the platform configurations of Select Identity 4.0.	

This connector is supported with Netegrity SiteMinder, version 5.5, on
Windows 2000 and Solaris 8.

Installation Procedure

Perform the following tasks to achieve successful installation of SiteMinder connector.

1 Extract the Contents of Schema File

2 Deploy the Connector on Application Server

3 Configure the Application Server

4 Configure SiteMinder

5 Configure the Connector with OVSI

Extract the Contents of Schema File

After deploying the connector on application server, you must extract the contents of schema file (`NetSmSchema.jar`) on the OVSI system. Ensure that the `CLASSPATH` environment variable in the application server startup script references the `Schema` subdirectory.

Deploy the Connector on Application Server

You must deploy the RAR file (`NetSmConnector.rar`) of the connector on an application server. Before deploying the RAR file, you must copy it to a local directory from the connector CD. Refer to *HP OpenView Select Identity Deployment Guide* for more information on deploying a connector on application server.

Configure the Application Server

You must copy SiteMinder Java Application Program Interfaces (API) JAR files to the application server. You must also copy the SiteMinder shared libraries to the application server. These libraries are called by the SiteMinder agent APIs, which are used by the connector for provisioning. After that, you must set the application server's `CLASSPATH` and `LD_LIBRARY_PATH` environment variables to reference the files. Perform the following steps to configure the application server.

1. Create a directory named `SiteMinderConnectorLib` in the Select Identity home directory.
2. Copy the SiteMinder Java API JAR files, which are distributed with SiteMinder, to the `SiteMinderConnectorLib` subdirectory. These files are:

   — `Smjavaagentapi.jar`

   — `Smjavasdk2.jar`

   The default location of these files on the SiteMinder system is `C:\Program Files\Netegrity\SiteMinder\SDK\java\`.
3. Add the JAR files to the application server startup script. Here is an example:

   ```
   set CLASSPATH=%WEBLOGIC_CLASSPATH%;
   %POINTBASE_CLASSPATH%;%JAVA_HOME%\jre\lib\rt.jar;
   %WL_HOME%\server\lib\webservices.jar;
   c:\SelectIdentity\SiteMinderConnectorLib\smjavaagentapi.jar;
   c:\SelectIdentity\SiteMinderConnectorLib\smjavasdk2.jar;
   %CLASSPATH%
   ```
4. Copy the following files to the folder `SiteMinderConnectorLib` subdirectory.

   — `smagentapi.dll`

   — `smjavaagentapi.dll`

   These files can be copied from the SiteMinder system, where they typically reside in `C:\Program Files\Netegrity\SiteMinder\SDK\bin\`.
5. On Solaris, copy the following files to a directory on the server:

   — `libsmagentapi.so`

   — `libsmjavaagentapi.so`

   For the steps 4 and 5, set `PATH` or `LD_LIBRARY_PATH` environment variables appropriately in the WebLogic startup script.

   For example, in the WebLogic startup script, add the following line:

   For .so files:
   `export LD_LIBRARY_PATH=/opt/si/weblogic/sysArchive/SiteMinderConnectorLib:$LD_LIBRARY_PATH`

   For .dll files:
   `set PATH = C:\Select_Identity\SiteMinderConnectorLib;%PATH%`

   Then, set the `LD_LIBRARY_PATH` environment variable to this directory. This environment variable should be available for use by the application server.
   For example, in the WebLogic startup script, locate the following line:

   ```
   export LD_LIBRARY_PATH=/opt/si/weblogic/sysArchive/
   SiteMinderConnectorLib:$LD_LIBRARY_PATH
   ```

On UNIX, use colon (:) to separate library paths. On Windows, use semicolon (;).

Configure SiteMinder

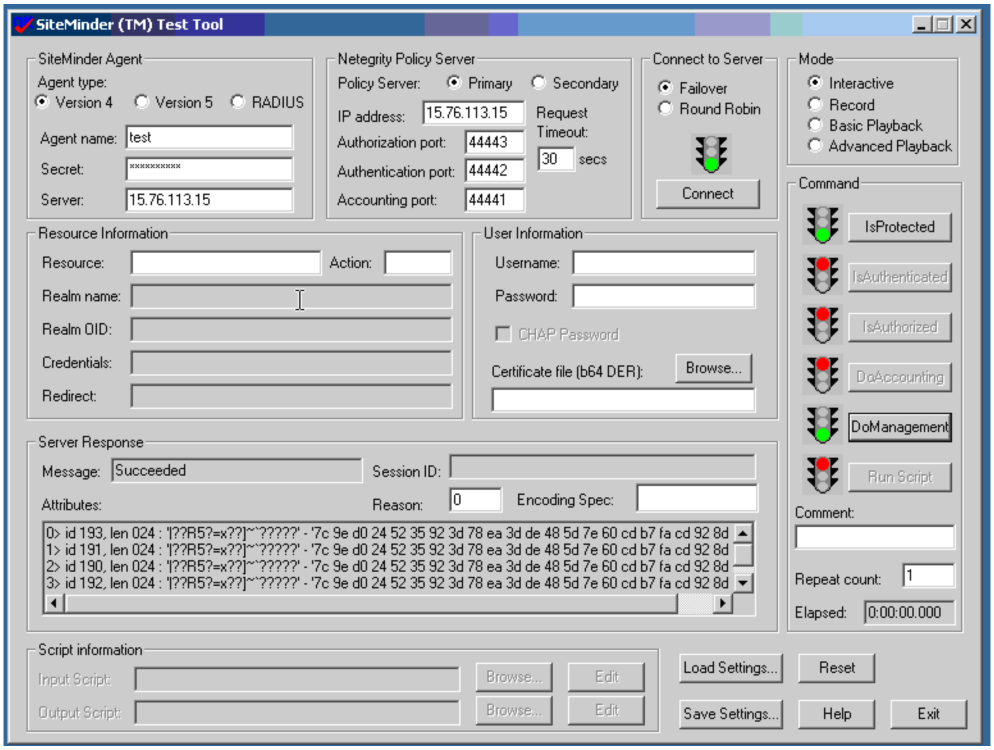
The SiteMinder connector manages users in SiteMinder using the SiteMinder Java DMS APIs.

In this section, the following configurations are assumed.

- SiteMinder Policy Server 5.5 Service Pack 3 (RC21) and SDK on Solaris 8 or Windows 2000 Server
- SiteMinder WebAgent configured for the following web servers:
  - iPlanet 6.0 on HP-UX11i, Solaris 9, and Windows
  - Microsoft IIS on Windows
- iPlanet Directory Server 5.1 on Solaris 9 or Windows, which acts as the user directory

To configure SiteMinder for use with the connector:

1 Verify that SiteMinder Policy Server and WebAgent are installed and functioning correctly. On the SiteMinder Policy Server, select **Start** → **Program Files** → **SiteMinder** → **SiteMinder Test Tool**.



SiteMinder (TM) Test Tool

SiteMinder Agent

Agent type: ● Version 4 ○ Version 5 ○ RADIUS

Agent name: test

Secret: **********

Server: 15.76.113.15

Netegrity Policy Server

Policy Server: ● Primary ○ Secondary

IP address: 15.76.113.15

Authorization port: 44443

Authentication port: 44442

Accounting port: 44441

Request Timeout: 30 secs

Connect to Server: ● Failover ○ Round Robin

Mode: ● Interactive ○ Record ○ Basic Playback ○ Advanced Playback

User Information: □ CHAP Password

Server Response

Message: Succeeded

Reason: 0

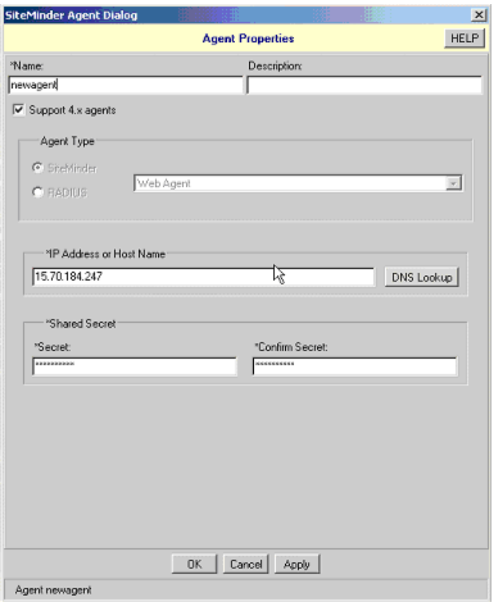
Attributes:

```
0> id 193, len 024 : '|??R5?=x??]~`?????' - '7c 9e d0 24 52 35 92 3d 78 ea 3d de 48 5d 7e 60 cd b7 fa cd 92 8d
1> id 191, len 024 : '|??R5?=x??]~`?????' - '7c 9e d0 24 52 35 92 3d 78 ea 3d de 48 5d 7e 60 cd b7 fa cd 92 8d
2> id 190, len 024 : '|??R5?=x??]~`?????' - '7c 9e d0 24 52 35 92 3d 78 ea 3d de 48 5d 7e 60 cd b7 fa cd 92 8d
3> id 192, len 024 : '|??R5?=x??]~`?????' - '7c 9e d0 24 52 35 92 3d 78 ea 3d de 48 5d 7e 60 cd b7 fa cd 92 8d
```

Repeat count: 1

Elapsed: 0:00:00.000

2 Verify that the **Support 4.x agents** option, which is required by the DMS APIs, is selected as shown in the following snapshot. This can be viewed by clicking the agent properties in the SiteMinder user interface.



SiteMinder Agent Dialog

Agent Properties

*Name: newagent

Description:

☑ Support 4.x agents

Agent Type: ● SiteMinder ○ RADIUS — Web Agent

*IP Address or Host Name: 15.70.184.247

*Shared Secret

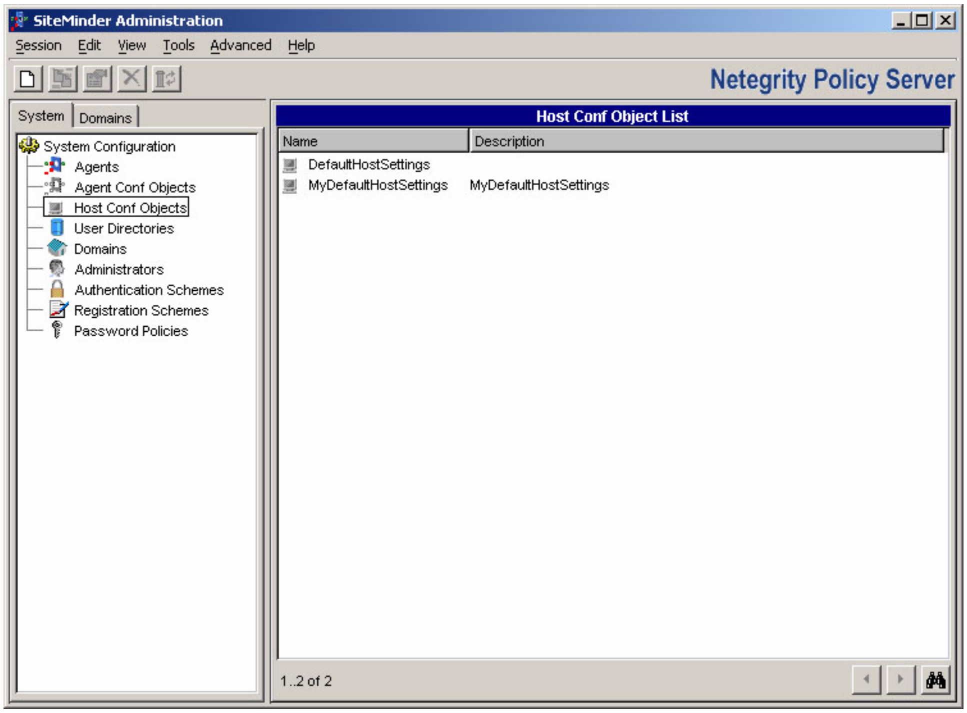
*Secret: **********

*Confirm Secret: **********

Agent newagent

3 To execute the APIs on the Select Identity server, register the Select Identity host system as a trusted host in the SiteMinder Policy Server's database. Complete these steps to do so:

a Create a Host-Config-Object in the SiteMinder interface and specify the Policy Server IP address there. For example, in the following snapshot, the TestHostConfigObject Host-Config-Object was created by duplicating the default host object and updating the Policy Server information.

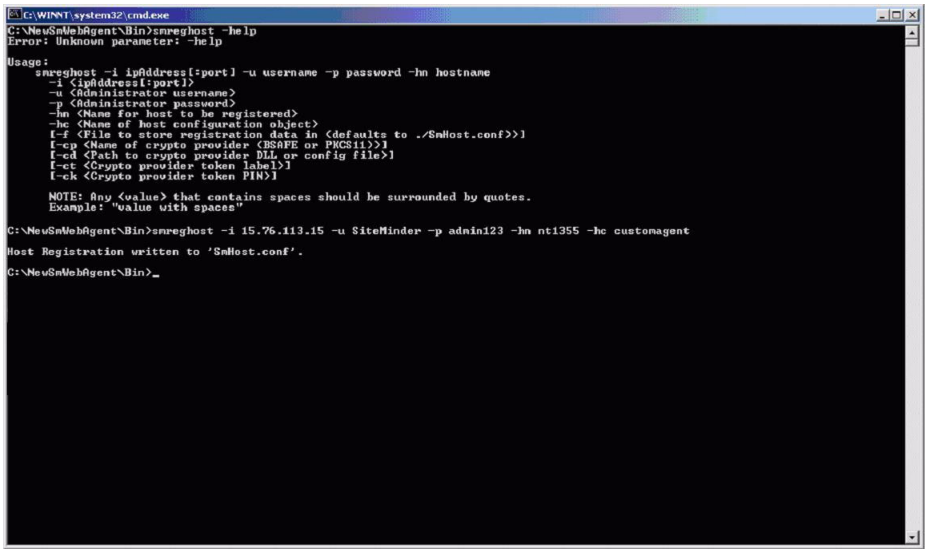


Host Conf Object List

Name	Description
DefaultHostSettings	
MyDefaultHostSettings	MyDefaultHostSettings

1..2 of 2

b Using the `smreghost` utility from an existing WebAgent installation or the WebAgent software, run the utility on the Select Identity server by specifying the Policy Server IP address, SiteMinder administrative login, password, current host name, and the name of the Host-Config-Object that was created above.



```
C:\NewSmWebAgent\Bin>smreghost -help
Error: Unknown parameter: -help

Usage:
    smreghost -i ipAddress[:port] -u username -p password -hn hostname
      -i <ipAddress[:port]>
      -u <Administrator username>
      -p <Administrator password>
      -hn <Name for host to be registered>
      -hc <Name of host configuration object>
      [-f <File to store registration data in <defaults to ./SmHost.conf>>]
      [-cp <Name of crypto provider <BSAFE or PKCS11>>]
      [-cd <Path to crypto provider DLL or config file>]
      [-ct <Crypto provider token label>]
      [-ck <Crypto provider token PIN>]

      NOTE: Any <value> that contains spaces should be surrounded by quotes.
      Example: "value with spaces"

C:\NewSmWebAgent\Bin>smreghost -i 15.76.113.15 -u SiteMinder -p admin123 -hn nt1355 -hc customagent

Host Registration written to 'SmHost.conf'.

C:\NewSmWebAgent\Bin>_
```

If the Select Identity server is on a Windows system, use this utility from the Windows WebAgent software. If the Select Identity server is on Linux, use the utility from the Linux WebAgent software.

The output of this command is written to a file called `SmHost.conf`.

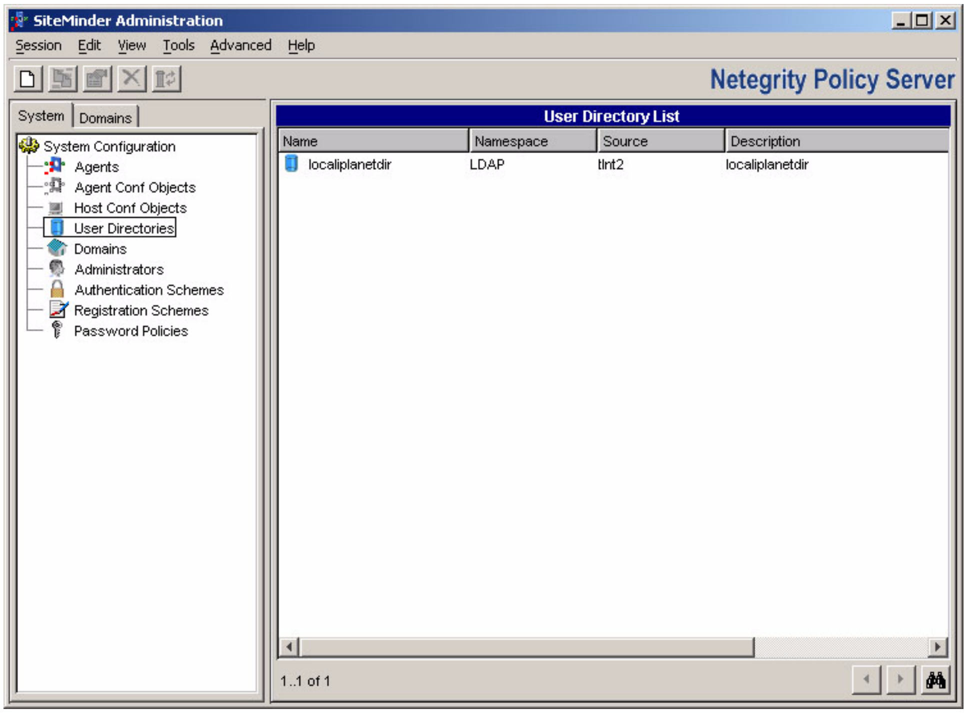
4 Locate the `WebAgent.conf` file that was extracted from the `NetSmSchema.jar` file. It typically resides in `SI_home/com/trulogica/truaccess/connector/netSm/`. Update the `WebAgent.conf` file from values in the generated `SmHost.conf` file. Specifically, update the variables for the host name, default agent name, and policy server IP address. Here are example values:

```
hostname="nt1325"
defaultagentname="test"
maxsocketsperport="20"
minsocketsperport="2"
newsocketstep="2"
requesttimeout="10"
policyserver="15.76.113.15, 44441, 44442, 44443"
sharedsecret="{RC2}mLog6JDcu3TzSNE457J+bRdL2QigyQrDbTbevbg4WQz3U
vvbKdyQnoFmuiUCoZp1H/fp7epKZMhEZQP+OBNJJc6OTrCnkvOkpR35Vts5Nnnx
rLhra3B2umee+eDWC3zIKAXJ6sHGWqJgUiMN+PIVlmks9uDSn2HmrUfdLl0FBVBs
Ztjto+vHNXy8eQefhqkr"
```

5 Configure SiteMinder such that it knows the user password attribute name in the configured LDAP User Store.

a On the left side of the window, select the configured user store.

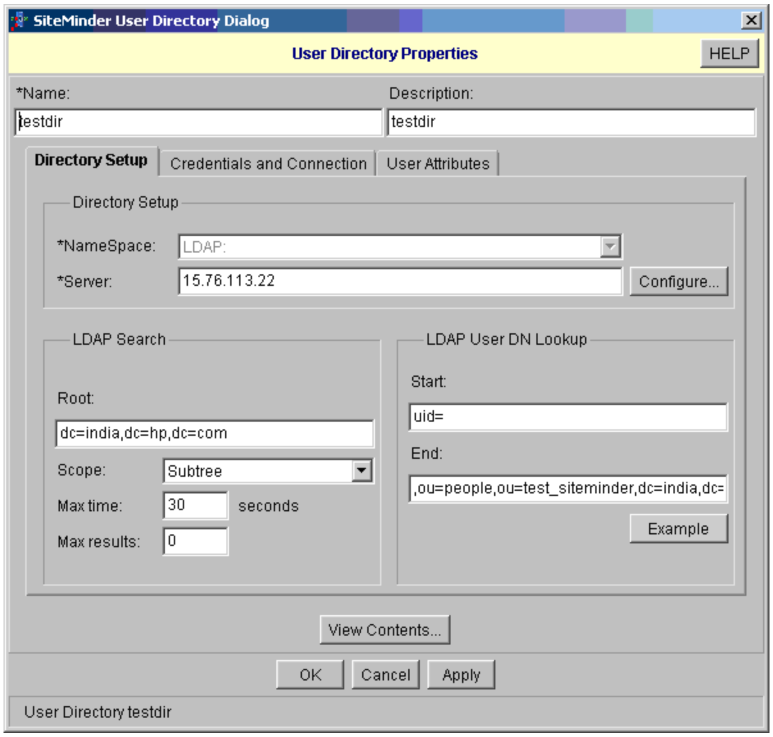
b Right-click to view the User Directory Properties dialog.



User Directory List

Name	Namespace	Source	Description
localiplanetdir	LDAP	tlnt2	localiplanetdir

c Configure the Directory Setup tab as shown in the following snapshot:



SiteMinder User Directory Dialog
User Directory Properties
HELP
Directory Setup
Credentials and Connection
User Attributes
Configure...
Example
View Contents...
OK
Cancel
Apply

*Name: testdir

Description: testdir

Directory Setup

*NameSpace: LDAP:

*Server: 15.76.113.22

LDAP Search

Root: dc=india,dc=hp,dc=com

Scope: Subtree

Max time: 30 seconds

Max results: 0

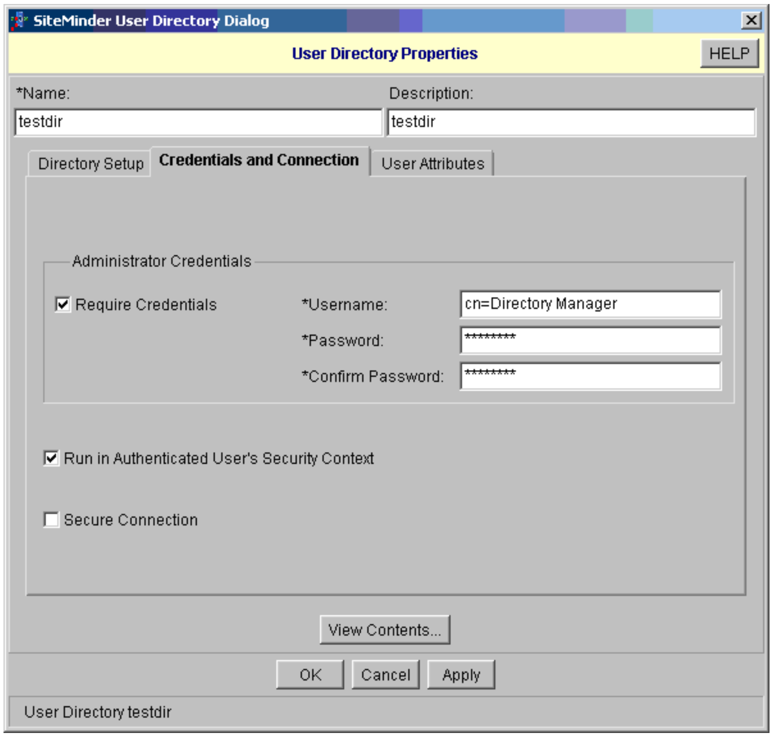
LDAP User DN Lookup

Start: uid=

End: ,ou=people,ou=test_siteminder,dc=india,dc=

User Directory testdir

d Configure the Credentials and Connection tab as shown here:



SiteMinder User Directory Dialog
User Directory Properties
HELP
Directory Setup
Credentials and Connection
User Attributes
View Contents...
OK
Cancel
Apply

*Name: testdir

Description: testdir

Administrator Credentials

☑ Require Credentials

*Username: cn=Directory Manager

*Password: *********

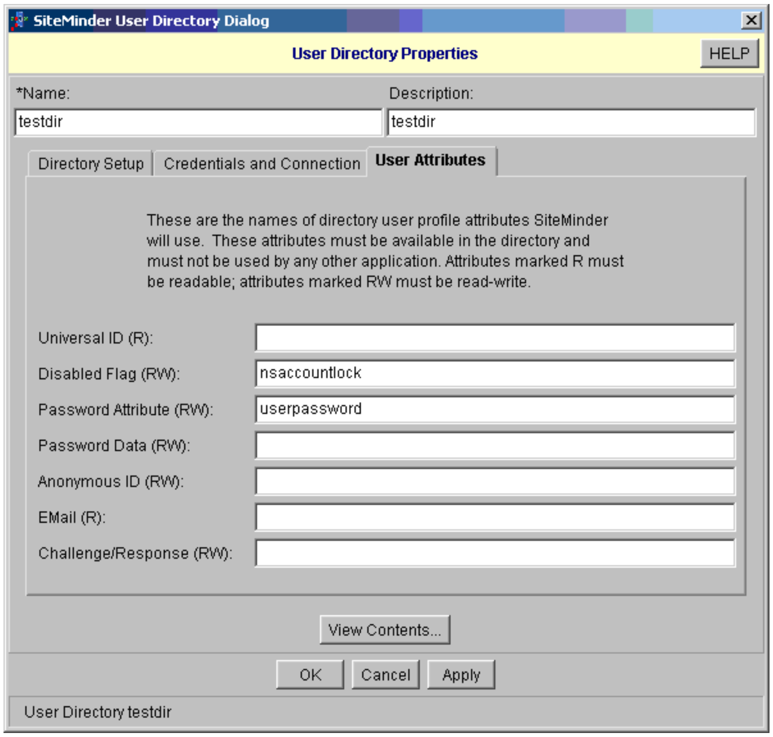
*Confirm Password: *********

☑ Run in Authenticated User's Security Context

☐ Secure Connection

User Directory testdir

e Configure the User Attributes tab as shown here:


SiteMinder User Directory Dialog
User Directory Properties
HELP
Directory Setup
Credentials and Connection
User Attributes
View Contents...
OK
Cancel
Apply

*Name: testdir

Description: testdir

These are the names of directory user profile attributes SiteMinder will use. These attributes must be available in the directory and must not be used by any other application. Attributes marked R must be readable; attributes marked RW must be read-write.

Universal ID (R):	
Disabled Flag (RW):	nsaccountlock
Password Attribute (RW):	userpassword
Password Data (RW):	
Anonymous ID (RW):	
EMail (R):	
Challenge/Response (RW):	

User Directory testdir

For troubleshooting connectivity and configuration of the Policy Server, WebAgent, and LDAP User Store, execute the sample Java programs that are provided with the SiteMinder SDK. View the log files for details. The return code and error message may help to troubleshoot any issue that might arise.

Configure the Connector with OVSI

After deploying the connector to an application server, you must configure it with Select Identity. To achieve successful configuration, you must perform the following steps.

1. Add a new connector – Add a new connector on OVSI. Refer to *HP OpenView Select Identity Connector Deployment Guide* for information on adding a new connector. While adding the connector, under Current Resource Connectors section in Manage Connectors page, do the following:

   — In the Connector Name text box, specify a name for the connector.

   — In the Pool Name text box, enter **`eis/NetSm`**

   — Under Mapper Available section, select **No.**

2. Add a new resource – You must add a new resource to OVSI that uses the newly added connector. Refer to *HP OpenView Select Identity Connector Deployment Guide* for the instruction to add a new resource to OVSI. While entering the resource parameters for SiteMinder connector, refer to the table below.

Table 3 Resource Configuration Parameters

Field Name	Sample Values	Description
Resource Name	*SiteMinder*	Name given to the resource.
Resource Type	*SiteMinder*	The connector that was deployed in step 1.
Authoritative Source	*No*	Whether this resource is a system that is considered to be the authoritative source for user data in your environment. You must specify **No** because the connector cannot synchronize account data with the Select Identity server.
Associate to Group	*Selected*	Whether the system uses the concept of groups. For this connector, select this option.
SiteMinder Admin	*SiteMinder*	SiteMinder superuser account name.
Admin Password	*Admin123*	SiteMinder superuser password.
SiteMinder User Directory	*SiteMinder LDAP_User_Store*	Name of the user directory as configured in SiteMinder.
SiteMinder Root Organizational Unit	*ou=smtesting*	The name of the node in the LDAP user store. (Additional OUs are provided below this level.)
OrgUnit Object Class	*top, organizationalunit*	Object class of the Org Unit in LDAP user store.
Group Object Class	*top, groupofuniquenames*	Object class of the groups in LDAP user store.
Group Suffix	*ou=Groups*	Group suffix name. This is one level below the "SiteMinder Root Organizational Unit" in the LDAP user store.
User Object Class	*top, person, organizationalperson, inetorgperson*	Object class of the user entry in LDAP user store.
User Suffix	*ou=People*	User suffix name. This is one level below the "SiteMinder Root Organizational Unit" in the LDAP user store.
Mapping File	*netsm.xml*	The attribute mapping XML file.

3 Map the attributes – You must map the Select Identity attributes to the attributes of the resource. While mapping the attributes, refer to the following table for resource specific mapping information.

Table 4 SiteMinder Mapping Information

Select Identity Resource Attribute	Connector Attribute	SiteMinder Attribute	Description
User Name	Username	uid	Unique field
Password	Password	userpassword	User's password
First Name	Firstname	givenname	First name
Last Name	Lastname	sn	Surname
Email	Email	mail	Email ID
Common Name	Firstname	cn	Common name
AccountLockStatus	AccountLockStatus	nsaccountlock	The default value provided in the mapping file

Create the `AccountLockStatus` attribute on Select Identity. This attribute is used internally by the connector to enable or disable the user in the SiteMinder LDAP user store. If a user is disabled, he or she cannot log in to the Sun ONE directory resource. The mapping file contains an attribute called `nsaccountlock` to which you have to map this attribute. Refer to *Service Studio* chapter of *HP OpenView Select Identity Administrator Guide* for information adding a new attribute to OVSI.

4 Associate the newly created resource to a service. Refer to *Service Studio* chapter of *HP OpenView Select Identity Administrator Guide* for more information on service.

➤

- The `nsaccountlock` attribute should not be included in the Service attributes. It is for internal use by the connector and should be specified in the resource attribute mappings.
- Do not add the `AccountLockStatus` attribute to any Service view; it is for internal use by the connector.

3 Uninstalling the Connector

If you want to uninstall a connector from Select Identity, perform the following steps:

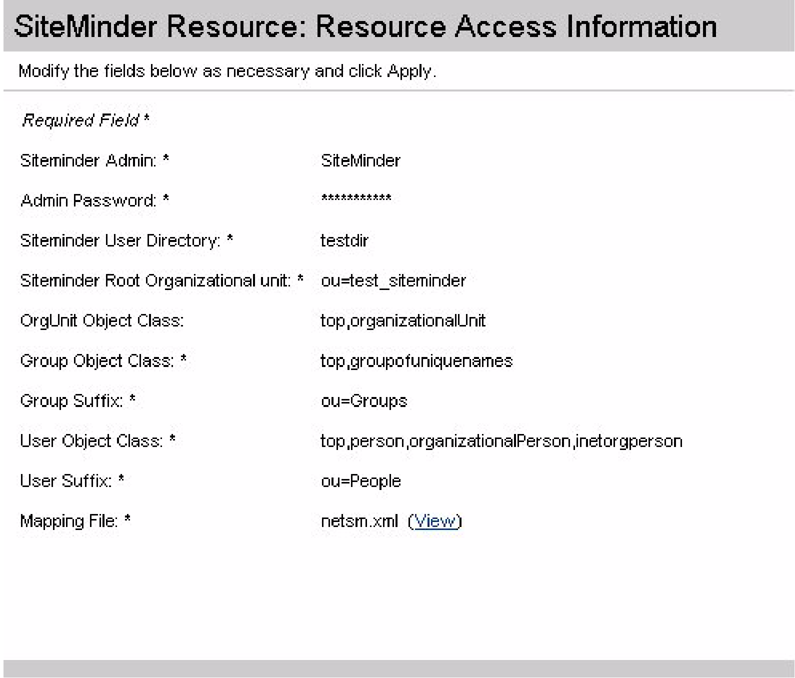
- Remove all resource dependencies.
- Delete the connector from the Select Identity Connectors pages.
- Uninstall the connector from application server.

See *HP OpenView Select Identity Deployment Guide* to know more on uninstalling the connector from application server.

A Sample Images

This chapter illustrates some sample screenshots of HP OVSI when SiteMinder connector in deployed on it.

- HP OVSI 4.0 displays the Resource Access Information page in the following format, when a SiteMinder resource is deployed on it.



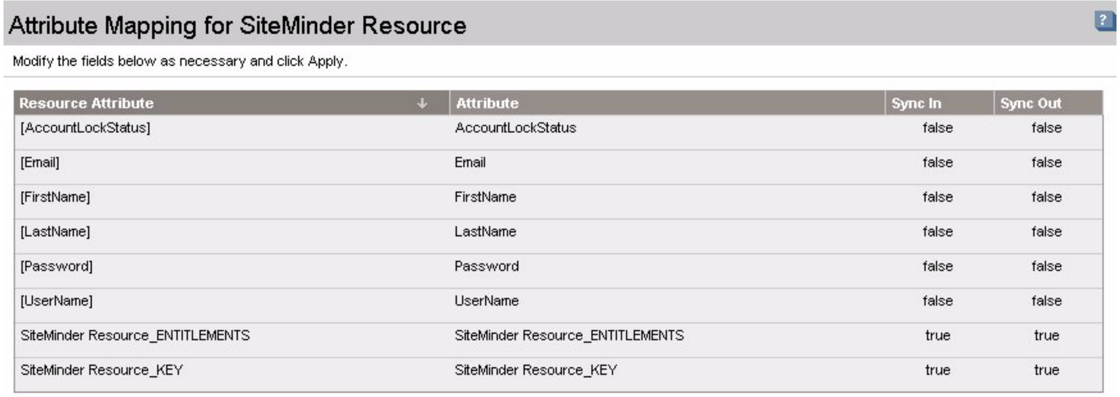
SiteMinder Resource: Resource Access Information

Modify the fields below as necessary and click Apply.

*Required Field **

Siteminder Admin: *	SiteMinder
Admin Password: *	***********
Siteminder User Directory: *	testdir
Siteminder Root Organizational unit: *	ou=test_siteminder
OrgUnit Object Class:	top,organizationalUnit
Group Object Class: *	top,groupofuniquenames
Group Suffix: *	ou=Groups
User Object Class: *	top,person,organizationalPerson,inetorgperson
User Suffix: *	ou=People
Mapping File: *	netsm.xml (View)

- HP OVSI 4.0 displays the View Attribute page in the following format, when a SiteMinder resource is deployed on it and resource attributes are mapped to HP OVSI 4.0.

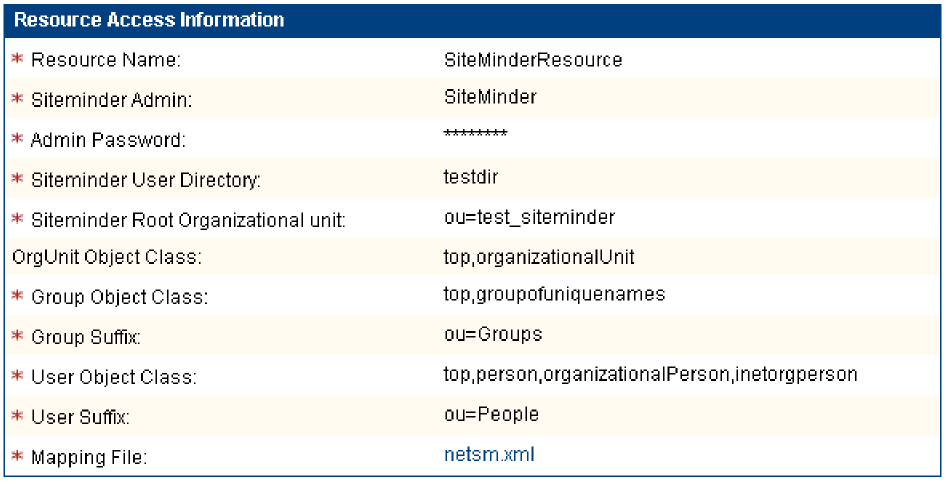


Attribute Mapping for SiteMinder Resource

Modify the fields below as necessary and click Apply.

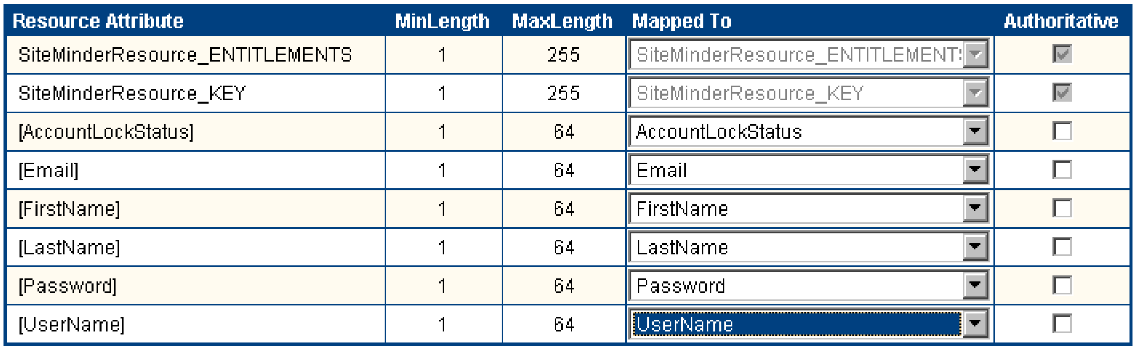
Resource Attribute ↓	Attribute	Sync In	Sync Out
[AccountLockStatus]	AccountLockStatus	false	false
[Email]	Email	false	false
[FirstName]	FirstName	false	false
[LastName]	LastName	false	false
[Password]	Password	false	false
[UserName]	UserName	false	false
SiteMinder Resource_ENTITLEMENTS	SiteMinder Resource_ENTITLEMENTS	true	true
SiteMinder Resource_KEY	SiteMinder Resource_KEY	true	true

- HP OVSI 3.3.1 displays the Resource Access Information page in the following format, when a SiteMinder resource is deployed on it.



Resource Access Information	
* Resource Name:	SiteMinderResource
* Siteminder Admin:	SiteMinder
* Admin Password:	********
* Siteminder User Directory:	testdir
* Siteminder Root Organizational unit:	ou=test_siteminder
OrgUnit Object Class:	top,organizationalUnit
* Group Object Class:	top,groupofuniquenames
* Group Suffix:	ou=Groups
* User Object Class:	top,person,organizationalPerson,inetorgperson
* User Suffix:	ou=People
* Mapping File:	netsm.xml

- HP OVSI 3.3.1 displays the Map Attribute page in the following format, when a SiteMinder resource is deployed on it and resource attributes are mapped to HP OVSI 3.3.1.



Resource Attribute	MinLength	MaxLength	Mapped To	Authoritative
SiteMinderResource_ENTITLEMENTS	1	255	SiteMinderResource_ENTITLEMENT	☑
SiteMinderResource_KEY	1	255	SiteMinderResource_KEY	☑
[AccountLockStatus]	1	64	AccountLockStatus	□
[Email]	1	64	Email	□
[FirstName]	1	64	FirstName	□
[LastName]	1	64	LastName	□
[Password]	1	64	Password	□
[UserName]	1	64	UserName	□