HP Select Identity Software

Connector for IBM Lotus Notes/Domino

Connector Version: 4.01

Installation and Configuration 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

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

This product includes software developed by the Apache Software Foundation (http://www.apache.org/).

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

- OpenSPML Toolkit from OpenSPML.org
- JGraph developed by JGraph
- Hibernate from Hibernate.org
- BouncyCastle engine for keystore management, bouncycastle.org

This product includes software developed by Teodor Danciu (http://jasperreports.sourceforge.net). Portions Copyright © 2001-2004 Teodor Danciu (teodord@users.sourceforge.net). All rights reserved.

Portions Copyright © 1994-2004 Sun Microsystems, Inc. All Rights Reserved.

This product includes software developed by the Waveset Technologies, Inc. (www.waveset.com). Portions Copyright © 2003 Waveset Technologies, Inc. 6034 West Courtyard Drive, Suite 210, Austin, Texas 78730. All rights reserved.

Portions Copyright © 2001-2004, Gaudenz Alder. All rights reserved.

Trademark Notices

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

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

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

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

Oracle® is a registered US trademark of Oracle Corporation, Redwood City, California

UNIX® is a registered trademark of The Open Group.

Support

You can visit the HP software support web site at:

http://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 an active support contract.

To find more information about support access levels, go to:

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

Contents

1 Documentation Map

This chapter describes the organization of HP Select Identity connector documentation and provides necessary information on how to use the documentation set to install and configure the connectors.

Figure 1 illustrates the documentation map for HP Select Identity connector. For a list of available product documentation, refer to the Table 1.

Figure 1 Documentation Map

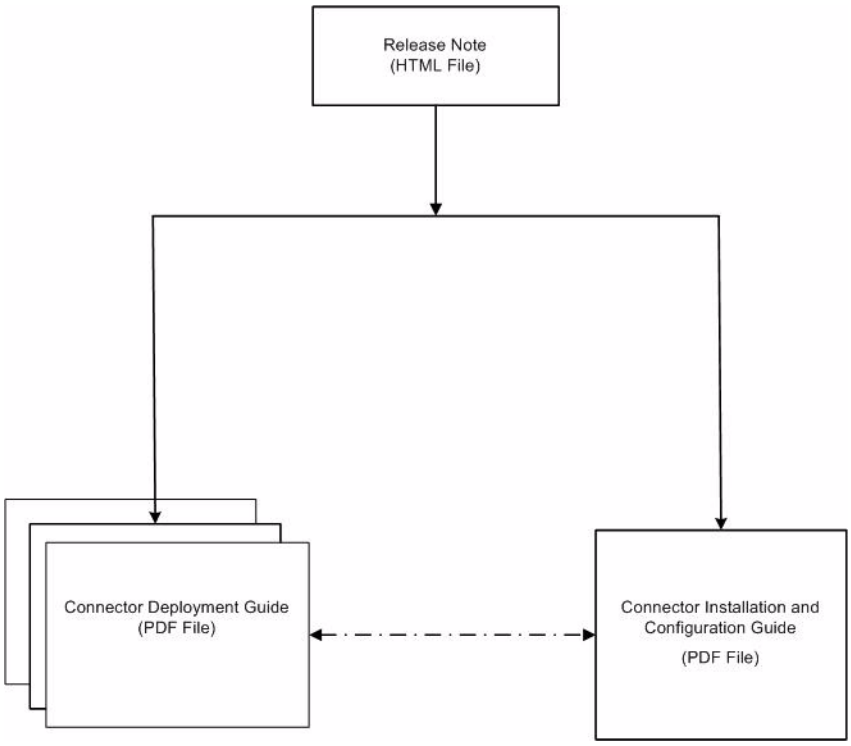


Table 1 Connector Documentation

Document Title and Filename	Contents	Location
Release Note `Domino Connector v4.01 Release Note.htm`	This file contains necessary information on new features of the connector, enhancements, known problems or limitations, and support information.	`/Docs/` subdirectory under the connector directory.
Connector Deployment Guide (for Select Identity 4.20) `connector_deploy_SI4.20.pdf`	Connector deployment guides provide detailed information on: • Deploying a connector on an application server. • Configuring a connector with Select Identity. Refer to these guides when you need generic information on connector installation.	`/Docs/` root directory on the product's CD media.
Connector Deployment Guide (for Select Identity 4.10-4.13) `connector_deploy_SI4.13.pdf`		
Connector Deployment Guide (for Select Identity 4.0-4.01) `connector_deploy_SI4.pdf`		
Connector Deployment Guide (for Select Identity 3.3.1) `connector_deploy_SI3.3.1.pdf`		
Connector Installation and Configuration Guide `Domino_guide.pdf`	Connector installation and configuration guide provides installation instructions for a specific connector. It contains resource specific configuration details.	`/Docs/` subdirectory under the connector directory.

2 Introduction

This chapter gives an overview of the HP Select Identity connector for IBM Lotus Notes/Domino. An HP Select Identity connector for IBM Lotus Notes/Domino enables you to provision users and manage identities on Domino server. At the end of this chapter, you will be able to know about:

- The benefits of HP Select Identity.
- The role of a connector.
- The connector for IBM Lotus Notes/Domino.

About HP Select Identity

HP Select Identity provides a new approach to identity management. Select Identity helps you automate the process of provisioning and managing user accounts and access privileges across platforms, applications, and corporate boundaries. Select Identity 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 Select Identity by using a connector. A connector is resource specific. The combination of Select Identity 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 Select Identity, but if any change takes place in resource, it cannot communicate that back to Select Identity. On the other hand, a bidirectional connector can reflect the changes made on resource back to Select Identity. This property of bidirectional connectors is known as **reverse synchronization**.

About the Domino Connector

The connector for IBM Lotus Notes/Domino — hereafter referred to as the Domino connector — enables Select Identity to manage user data in IBM Lotus Notes/Domino systems. This connector is a bidirectional connector and pushes changes made to user data in the Select Identity database to the target Domino server. It also enables the agent on the Domino server to send password updates back to Select Identity. The mapping files, which are included with the connector, control how Select Identity fields are mapped to Domino fields.

This connector can be used with Select Identity version 3.3.1-4.20.

The Domino connector supports provisioning the following for users on the Domino server:

- Access levels
- Entitlements
- Roles
- User groups

The following list describes the operations supported by the connector and how the connector works for each provisioning operation:

- Add a User—
  This functionality adds a user on the Domino server. You can set all of the attributes in the Domino server for the user. This is controlled through configuration of the mapping file.

  An ID file is required for the user to log on to the Domino server by using the Notes client. When a Domino administrator creates a user on the Domino Administrator Console, the administrator must manually send the ID file to the user. The Domino connector automates this process.

  When the user is created, the ID file is mailed to the user's mailbox (as specified by the default mail account in Domino server). If an alternative email address is specified for the user (by mapping the `AltEmailAddress` attribute in the mapping file), the ID file is also mailed to that address. If the `AltEmailAddress` value is not provided in the mapping file, the connector searches for the value in the `Properties.ini` file, which is installed with the connector's agent on the Domino server.

  Also, while creating users in Select Identity that will be provisioned on a Domino server, follow the guidelines given below:

  — While creating a user, specify only one access level because the Domino server allows only one ACCESS LEVEL to be specified for a user at a time.

  — ENTITLEMENT, ROLE, and Group are multivalue components of the entitlement (for example, a user can belong to zero or more of these attributes). Therefore, you can select any combination of these components while creating the user.

  — You must assign an ACCESS LEVEL before assigning an ENTITLEMENT or ROLE.

  You can use the connector to add both a Notes user or a non-Notes user (a Domino user without Notes privilege and id file).

- Modify a User—
  The connector can modify all the attributes on the Domino server except UserID and Password attributes.

  Also, when changing user entitlements in Select Identity for users who are provisioned in Domino, make sure you select only one ACCESS LEVEL. (You may want to remove the ACCESS LEVEL previously selected before adding a new one.)

- Disable Service Membership—
  This removes all entitlements assigned to the user by the Select Identity Service on the Domino server.

- Enable Service Membership—
  This restores all entitlements removed by the Disable Service Membership functionality.

- Delete Service Membership—
  This removes user from the Domino server.
- Disable All Services—
  This functionality disables the user in all Select Identity Services to which he or she is provisioned. This prevents the user from logging in to the Domino server.
- Enable All Services—
  This restores and enables the user for all Services disabled by Disable All Service. On the Domino server, the user can log on to the system once the action completes.
- Reset Password—
  The Domino connector can manage HTTP passwords only. The changes to the user's HTTP password are synchronized with Select Identity. This function resets user's HTTP password, and the user must specify this new password while using the Notes Web Interface.

  The connector cannot change the Notes client password. The Notes client uses ID files, which are provided by the administrator, that have different passwords. Users can log in to their mailboxes by using their old passwords. However, you can prevent this by setting the `Check passwords on Notes IDs` property to **`YES`** in the server security settings.

  To enable password verification for Notes users, you must enable password verification for users and servers:

  a Make sure that the Administration Process is set up on the server and you have at least Author access and the User Modifier role in the Domino Directory.

  b From the Domino Administrator, click the **People & Groups** tab using a network connection to the Domino Directory.

  c Select each Person document for which you want to enable password checking.

  d Choose **Actions - Set Password Fields**, and then click **Yes** to continue.

  e Select **Check password**.

  f Complete these fields, and then click **OK**:

Field	**Enter**
Required change Interval	Number of days during which users must provide a new password. The default is 0, which does not require users to change their passwords and ignores any entry in the Grace period field.
Grace period	Number of days after a required change interval that users have to change their passwords. The default is 0, which allows users an unlimited amount of time to change their passwords after the change interval expires. A value between 3 and 7 days is recommended.

  Perform the following instructions to enable password verification on each server with which these users authenticate:

  a Click the **Configuration** tab and open each Server document.

  b Click the **Security** tab.

  c In the Check passwords on Notes IDs field, select **Enabled**.

To disable password verification for an individual user, perform the following steps. When you disable password verification for a user, Domino does not check passwords for the user even if password verification is enabled for the server.

a. From the Domino Administrator, click the **People & Groups** tab using a network connection to the Domino Directory.

b. Select each Person document for which you want to disable password verification.

c. Choose **Actions - Set Password Fields**, and then click **Yes** to continue.

d. Select **Don't check password**, and then click **OK**.

To disable password verification for a server, perform these steps. When you disable password verification for a server, Domino does not check passwords for any users who access the server, even if the user has password verification enabled.

a. From the Domino Administrator, click the **Configuration** tab and open the Server document.

b. Click the **Security** tab.

c. In the Check passwords on Notes IDs field, select **Disabled**.

The following list describes some additional features of the Domino connector:

- The Domino connector supports creation of non-Notes user.
- Connector provides the option of specifying the value of certifier id file name and certifier password as part of resource creation or as user attributes. This enables the use of multiple certifier ID files to create users.
- The connector exposes a function called `Process()`, which could be invoked from a workflow external call. This function checks if a given group can accommodate more users. If the group is full, the `Process()` function creates a new group and returns the newly created group name. Refer to the Appendix B for more details on the this functionality.

Overview of Installation Tasks

Before you start installing the connector, you must ensure that system requirements and all the installation prerequisites are met. Refer to the Table 2 for an overview of installation tasks.

Table 2 Organization of Tasks

Task Number	Task Name	Reference
1	Install the connector on the Select Identity server.	See Installing the Connector on page 15.
	— Meet the system requirements.	See System Requirements on page 16.
	— Extract contents of the Schema file (file that contains the mapping files for the connector) to location on the Select Identity server.	See Extracting Contents of the Schema File on page 17.
	— Install the Resource Adapter Archive (RAR) of the connector on an application server.	See Installing the Connector RAR on page 17.
2	Installing the agent for Domino connector.	See Installing the Agent on page 19.
3	Configure the connector with the Select Identity server.	See Configuring the Connector with Select Identity on page 43.

3 Installing the Connector

The Domino connector is packaged in the following files, which are located in the `Domino` directory of the Select Identity Connector CD: .

Table 3 Domino Connector Files

Serial Number	File Name	Description
1	• `DominoConnector_420.rar` for WebSphere • `DominoConnector_420WL9.rar` for WebLogic	It contains the binaries for the connector
2	`Dominoschema.jar`	It contains the following mapping files: • `dominouser.properties` — maps the Select Identity user attributes to those on the Domino server • `dominogroup.properties` — maps the Select Identity group attributes to those on the Domino server; note that group provisioning is not currently supported, though this file must be extracted during installation • `domino.xsl` — maps attributes on the Domino server to attributes on the Select Identity server. This file is used by the agent during reverse synchronization.
3	`Manual_DominoSetup.zip`	It contains the files for the Domino agent on Windows platforms.
4	`Manual_DominoSetup.tar`	It contains the files for the agent on Solaris platforms.
5	`DominoSetup.zip`	It contains the GUI-based installer for the agent on Windows platforms.
6	`DominoSetup.tar`	It contains the GUI-based installer for the agent on Solaris platforms.

Table 3 Domino Connector Files

Serial Number	File Name	Description
7	`PasswordSync_6_5_1.zip`	It contains the template file for Domino 6.5.x on Windows.
8	`PasswordSync_6_5_1.tar`	It contains the template file for Domino 6.5.x on Solaris.
9	`ConnectorExt.jar`	Use this file while using the connector with versions of Select Identity prior to 4.10.

System Requirements

The Domino connector is supported in the following environment:

Table 4 Platform Matrix for Domino connector

Select Identity Version	Application Server	Database
3.3.1	WebLogic 8.1.4 on Windows 2003	Microsoft SQL Server 2000
	WebSphere 5.1.1 on HP-UX 11i	Oracle 9i
4.0-4.20	The Domino connector is supported on all the platform configurations of Select Identity 4.0-4.20.	

The Domino connector and agent are supported in the following environment:

- Domino 6.5.1 on Solaris 9
- Domino 6.5.1,6.5.3, and 6.5.4 on Windows (2000/2003/XP)

The agent must be installed on the system where the Domino server is running.

To use this connector on versions of Select Identity prior to 4.10, add the `ConnectorExt.jar` file (available in the connector folder) to the application server classpath.

The Domino connector is internationalized and able to operate with languages that are supported by the Java Unicode specification. If you wish to use the connector on non-English platforms, make sure that the following prerequisites are met:

- The Select Identity server should be configured for internationalization. Refer to the *HP Select Identity Installation Guide* for details.
- The resource must be configured to support local language characters.

Extracting Contents of the Schema File

The Schema file of the connector contains necessary mapping information to map resource attributes to Select Identity. Extract contents of the `Dominoschema.jar` file to a directory that is in the application server `CLASSPATH`. Refer to the *HP Select Identity Connector Deployment Guide* for detailed instruction to extract contents of the Schema file.

Installing the Connector RAR

To install the RAR file of the connector (such as `DominoConnector_420.rar`) on the Select Identity server, you must copy the file to a local subdirectory on the Select Identity server, and then deploy on the application server. Refer to the *HP Select Identity Connector Deployment Guide* for detailed information on deploying a RAR file on an application server.

While deploying the RAR on WebSphere, enter the JNDI Pool Name as **`eis/DominoConnector`**.

4 Installing the Agent

The Domino connector is an agent-based connector. The agent is a suite of services and support files deployed on the resource.

You must install the agent on the system where the Domino server is running. In the resource system, you must set the `JAVA_HOME` environment variable to the <*Java Home*> location.For example, if Java is installed at `C:\JRE`, set `JAVA_HOME = C:\JRE`.

Also, you must have `notes.jar` in your `CLASSPATH` and the Domino install directory in `CLASSPATH` and `PATH`.
For example, if the Domino server is installed on `C:\Lotus` and `notes.jar` file is in `C:\Lotus\Domino`, the `CLASSPATH` variable must include the following:
`C:\Lotus\Domino\notes.jar; C:\Lotus\Domino`

and the `PATH` variable must include the following:

`C:\Lotus\Domino`

Perform the following tasks to install the agent:

1. Configure Domino Security Settings — Perform this task to enable reverse synchronization. This must be performed before installing the agent.
2. Install the Agent on Windows — Perform this task to install the agent (by using a wizard or manually) on Windows
3. Install the Agent on Solaris — Perform this task to install the agent (by using a wizard or manually) on Solaris
4. Configure the Agent — Perform this task to provide the settings in the agent's configuration files; you must perform this procedure
5. Configure the Reverse Synchronization Agent in Domino — Perform this task to configure Domino to use the reverse synchronization feature of the agent
6. Configure Password Synchronization in Domino 6.5.x — Perform this task to enable reverse (password) synchronization for Domino 6.5.*x*. This must be performed after the agent is installed
7. Upgrade Users' Mail Templates — Perform this task to enable Domino to use the new template file for all new users, which is necessary for reverse synchronization.
8. Change Passwords Using the Web Client — Perform this task to enable users to synchronize user passwords with the Select Identity server.
9. Start the Agent — Perform this task to start the agent on Windows and Solaris

Configure Domino Security Settings

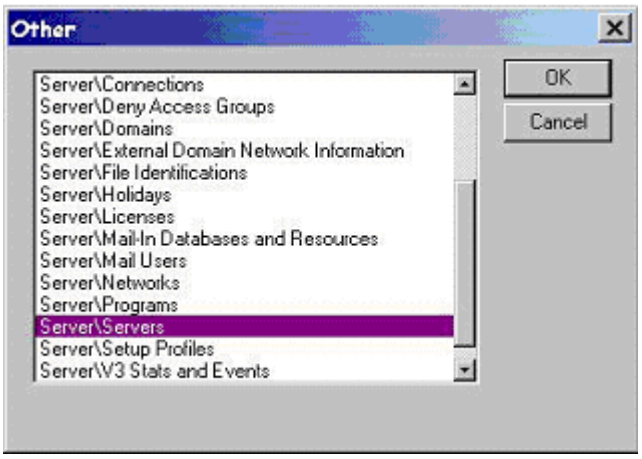
The following procedure describes how to configure security settings on the Domino server running on Windows or Solaris. You must perform these steps to run the Java-based agent for reverse synchronization.

1 Verify that the Domino server is running.

2 Launch the Domino Administrator.

3 Modify the security settings for the server. Perform the following steps.

Select **View** → **Server** → **Other**. The Other dialog box appears.



d Select **Server/Servers** from the list, and then click **OK**. The Domino Address Book - Server/Servers dialog box appears.

e Click **Edit Server**.

f Select the **Security** tab.

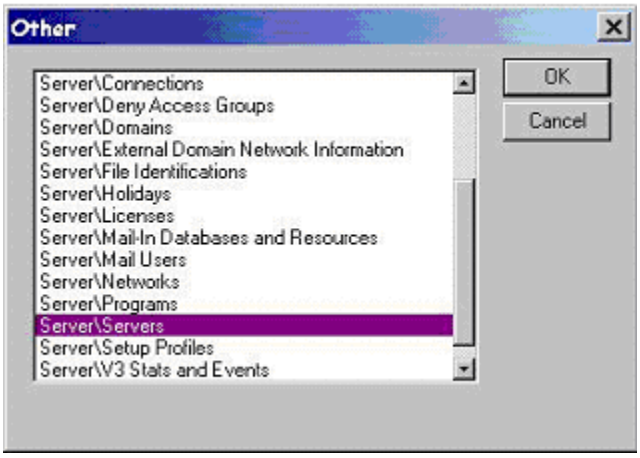
g Navigate to the Server Access section on the Security tab, and then select the **users listed in all trusted directories** option. In the And section, select the account (*server_name/domain_name*), for example, sicfpc07/hpqcorp, admin/hpqcorp, siadmin/hpqcorp.

h Locate the Programmability Restrictions section of the Security tab and edit the following settings to include the Administrator account and Server account (*server_name/domain_name*) on the Domino server:

- Run Unrestricted methods and operations
- Run Restricted Lotus script/Java Agents

4 Perform the following steps to modify the preferred `Notes.ini` settings

Select **View** → **Server** → **Other**. The Other dialog box appears.



i Select **Server/Servers** from the list, and then click **OK**. The Domino Address Book - Server/Servers dialog box appears.

j Select **Configuration** → **Servers** → **Configurations**.

k Select the server name.

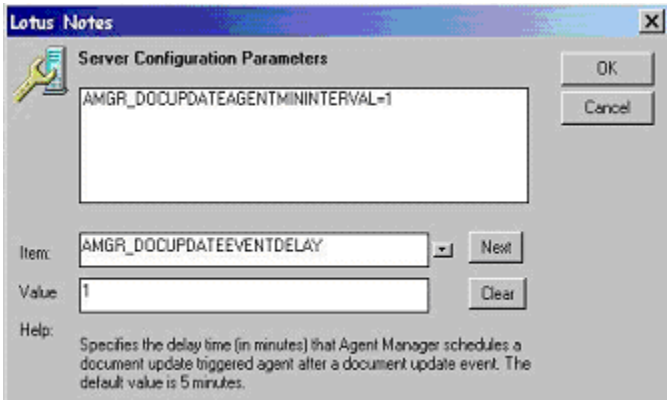
l Click **Edit Configuration**.

m Click the **NOTES.INI Settings** tab.

n Click **Set/Modify Parameters**.

o Specify `1` as the value of AGMR_DOCUPDATEAGENTMININTERVAL, and then click **Add**.

p Specify `1` as the value of AGMR_DOCUPDATEEVENTDELAY, and then click **Add**.

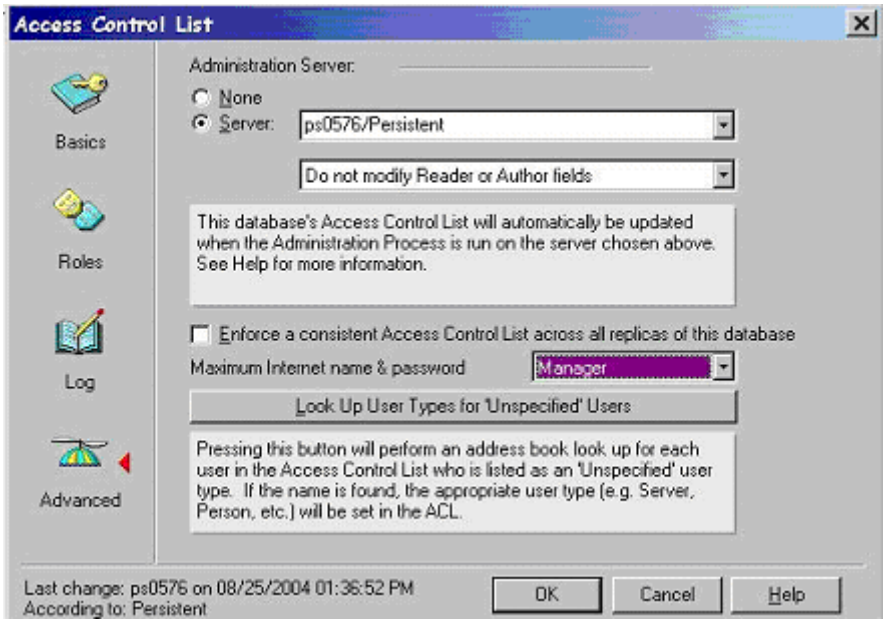


q Click **OK** to close the dialog.

r Save your settings, and then close the Other dialog.

5 To set access control settings, which enable the connector to perform operations related to roles and entitlements, perform the following steps:

a Select **File** → **Database** → **Access Control**. The Access Control List dialog box appears.



b Click **Advanced** on the left side of the dialog.

c Select **Manager** from the Maximum Internet name & password drop-down list.

d Click **OK** to close the dialog.

Install the Agent on Windows

You can install the agent by using the installation wizard or by manually copying files to the server. After you install the agent on Windows, the following folders and files are available:

install_dir\	`startDominoApp.cmd`	Starts the agent.
install_dir\bin\	`dominoapp.jar`	The main application JAR file. This file is included in the `CLASSPATH`.
	`connagents.jar`	The JAR file containing the Domino agents.
install_dir\config\	`commons-logging.properties`	The configuration file for the logging libraries in `commons-logging.jar`. This file is included in the `CLASSPATH`.
	`log4j.properties`	The configuration file for the logging libraries in `log4j-1.4.8.jar`. This file is included in the `CLASSPATH`.

install_dir\lib\	commons-logging.jar	Logging libraries. This file is included in the CLASSPATH.
	log4j-1.2.8.jar	Logging libraries. This file is included in the CLASSPATH.
	xercesImpl.jar	Xerces XML parser libraries. This file is included in the CLASSPATH.
	xmlParserAPIs.jar	Xerces XML parser libraries. This file is included in the CLASSPATH.

The properties.ini and opAttributes.properties files are automatically copied to the directory in which the Notes.jar file resides. This directory is specified during the agent installation.

Installation Using the Wizard

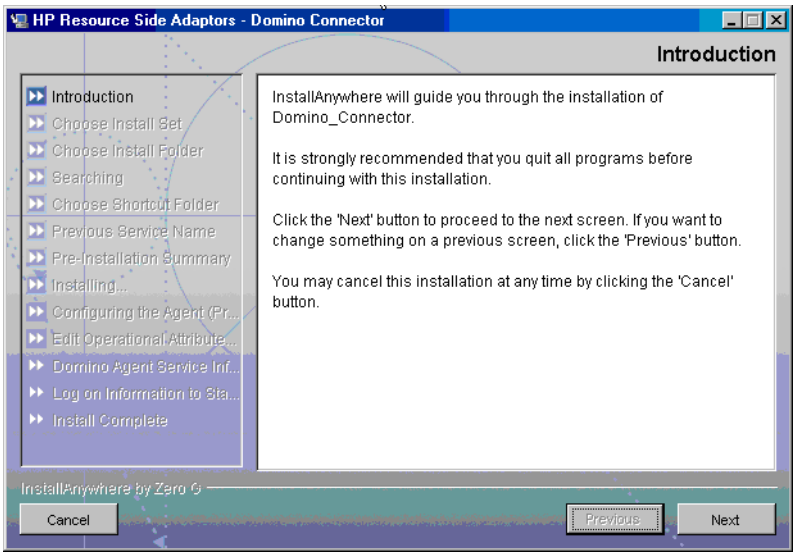
Complete the following steps to run the installation wizard, which installs the agent. Also, note that you can install the agent as a console application or as a service.

Before running the installation wizard, ensure that the log4j-1.2.8.jar file resides in the *JREDIR*\lib\ext directory, where *JREDIR* is the Java Runtime Environment (JRE) that will be used by the wizard. For example, if the JRE resides in C:\Program Files\Java\j2re1.4.1_04, verify that the log4j-1.2.8.jar file resides in C:\Program Files\Java\j2re1.4.1_04\lib\ext.

Also, ensure that this JRE is included in the Path system variable.

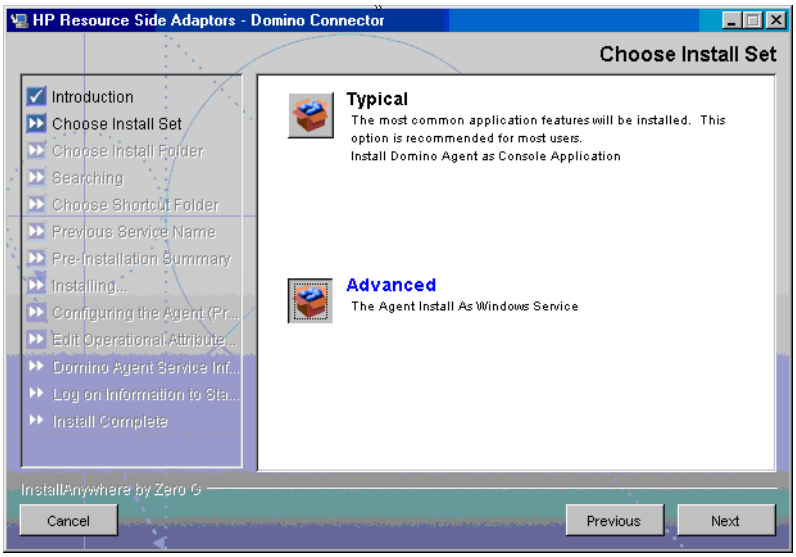
1 Extract all the files from the DominoSetup.zip file.

2 Run the installation wizard (install.exe). The following popup appears:

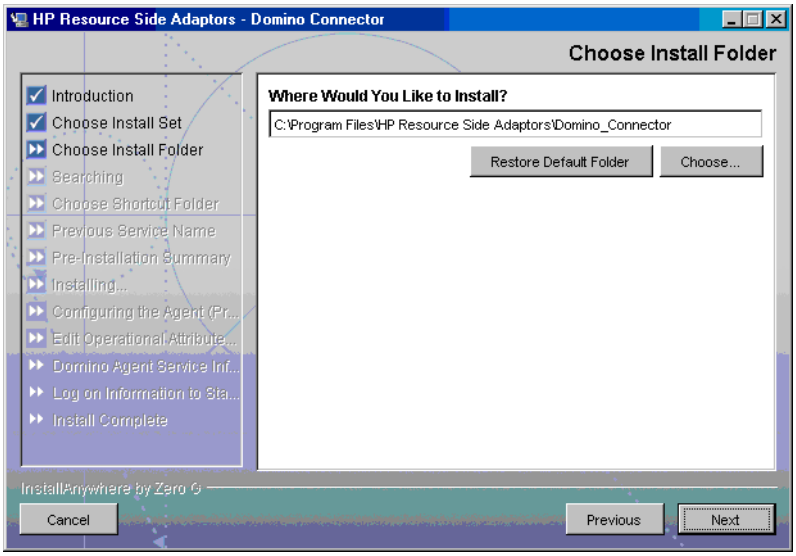


3 Click **Next** to proceed.

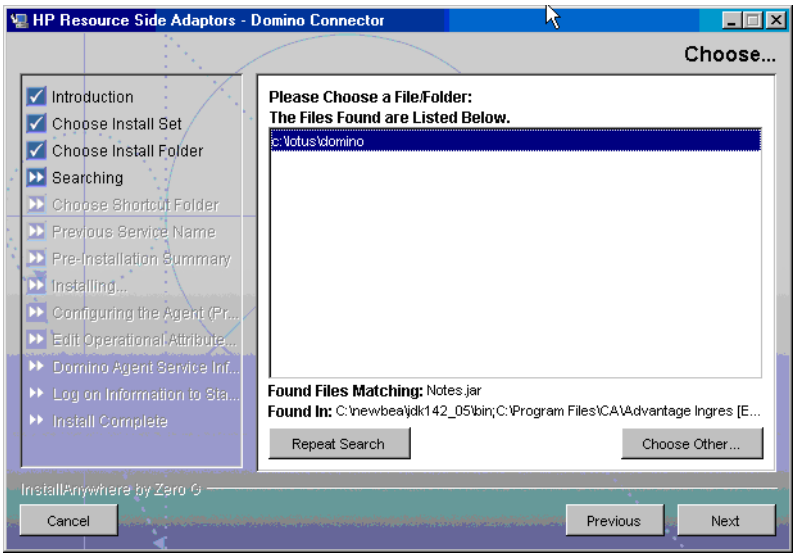
4 Select the mode of installation. If you wish to install the agent as a service, select the **Advanced** option. Then, click **Next**.



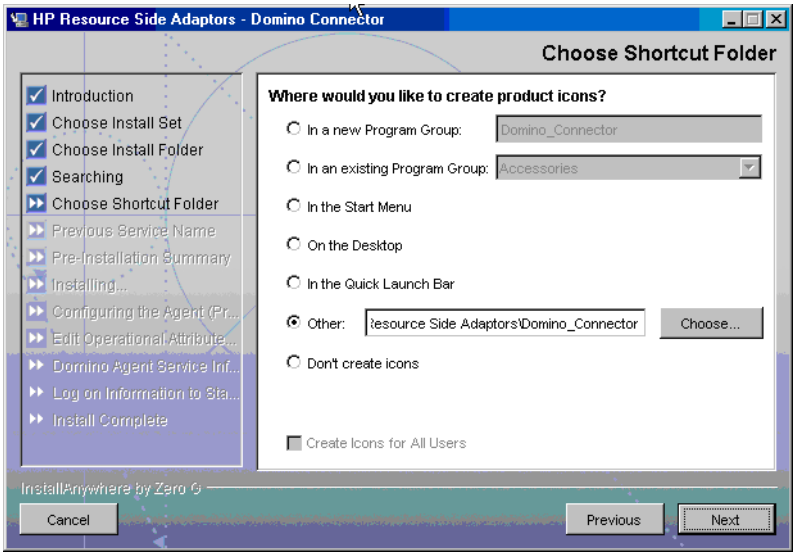
5 Specify an installation directory, and then click **Next**.



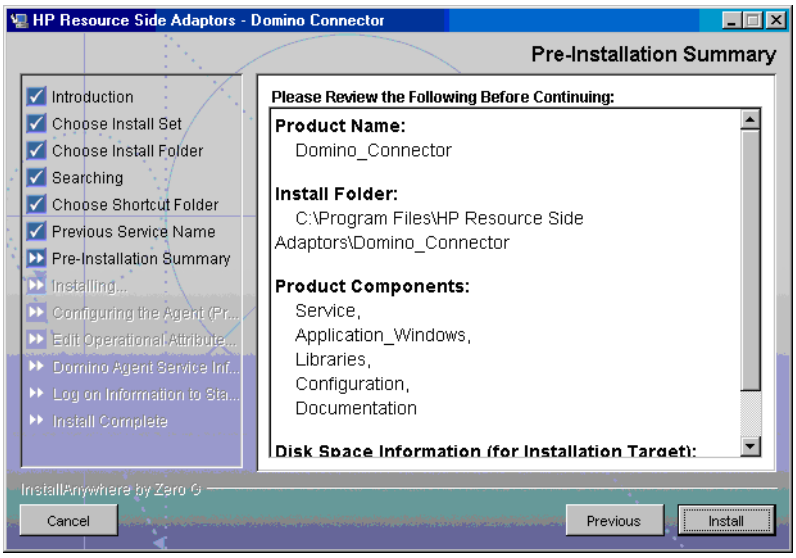
6 Provide the location to the `Notes.jar` file, and then click **Next**.



7 Specify where the product icons will be installed, and then click **Next**.

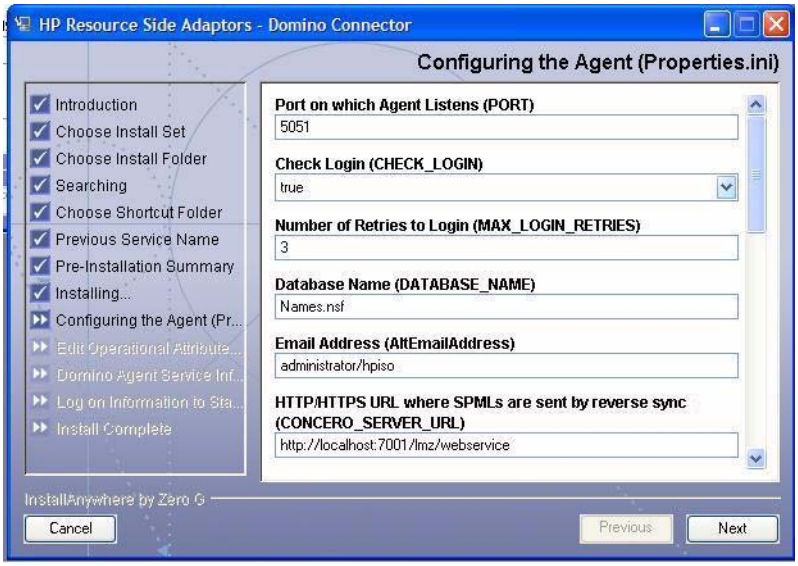


8 Verify the pre-installation summary. If you wish to make changes, click **Previous,** and then edit the chosen options. To install the agent, click **Install**.

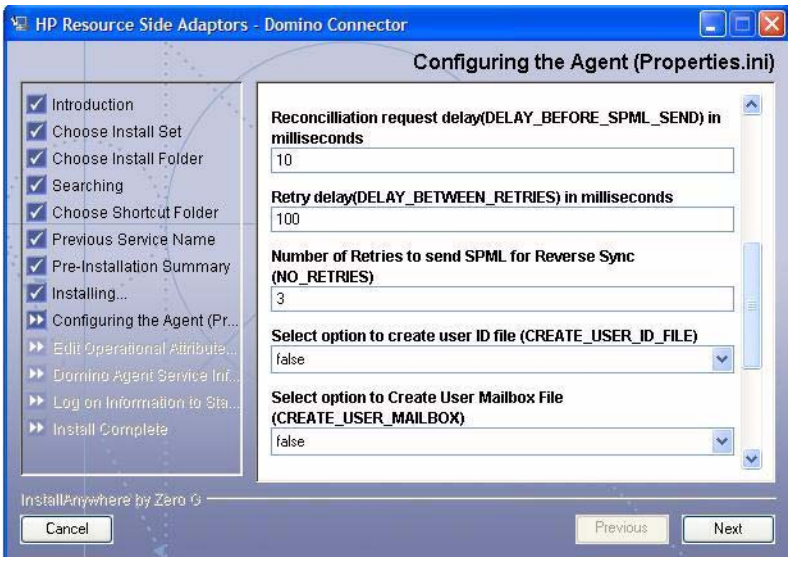


9 If you chose to install the agent as a service, continue with the installation as follows:

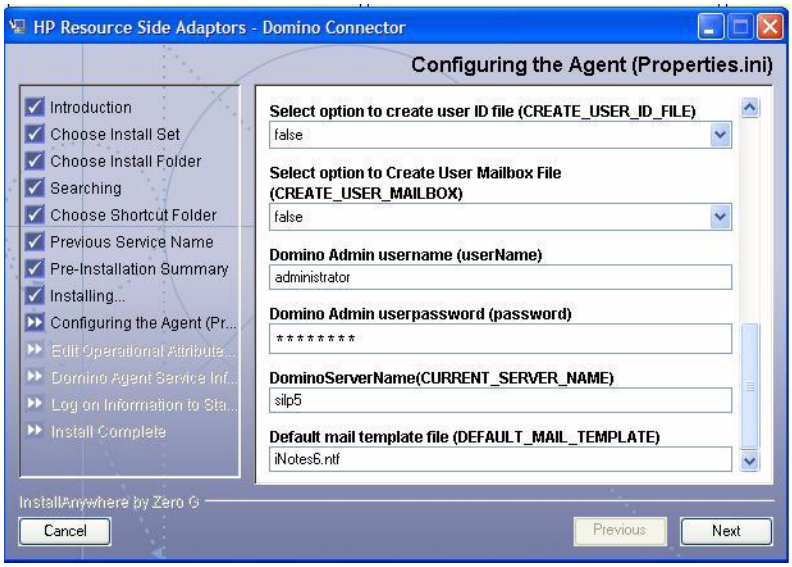
a Configure the agent by providing attribute values that will be stored in the `properties.ini` file. See step 1 on page 34 for more information on these properties.



This is the middle half of the dialog box:



This is the bottom half of the dialog box:

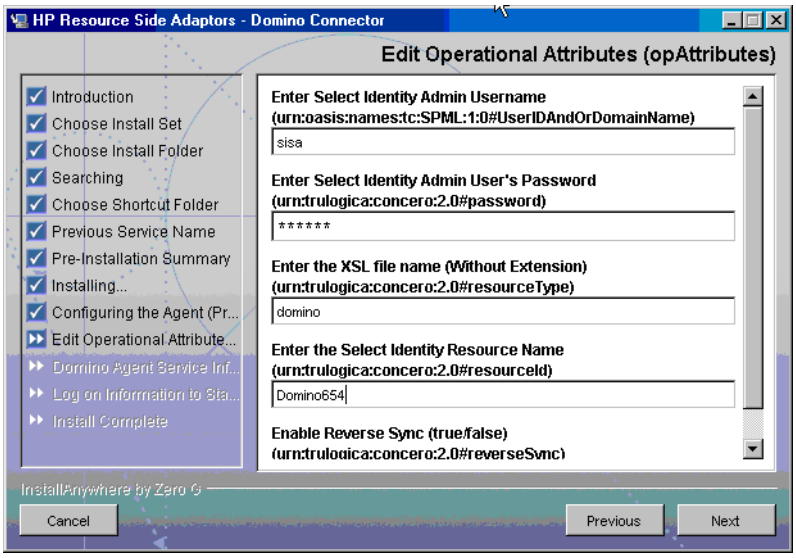


The administrative username/ password used here should be the same as that will be used to create resource in Select Identity as this is also used to block cyclic request of the events

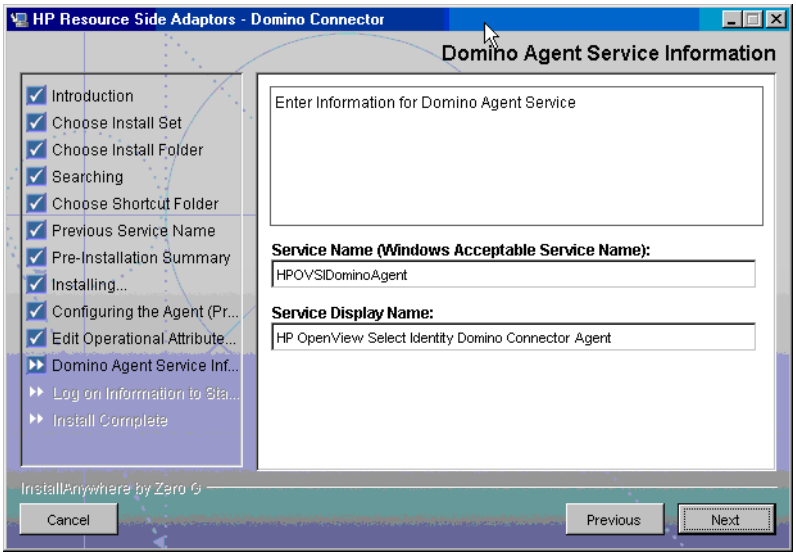
You must use this user only to create a Select Identity resource for the Domino connector. If you use this user to perform any operation directly on Domino resource, the change will not be synchronized back to Select Identity

Click **Next**.

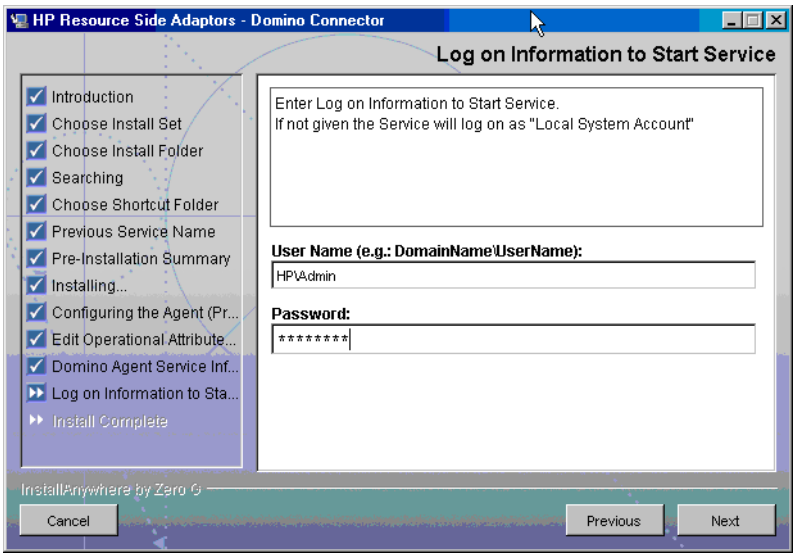
b Configure the agent by providing attribute values that will be sent during reconciliation requests and stored in the `opAttributes.properties` file. See step 2 on page 35 for information on these attributes



c Specify the name and display name of the service for the Domino agent; the display name will be used to register the service with the Windows system. Then, click **Next**.



d Specify the Windows log on information (user name and password), which will be used by the Domino agent to run as a service, and then click **Next**.



10 When the installation wizard completes, click **Done** on the Install Complete dialog to close the installation program

The `properties.ini` and `opAttributes.properties` files are automatically copied to the directory chosen in the step 6 on page 24.

Manual Installation

Perform the following to install the agent on Windows:

1 Edit the `CLASSPATH` environment variable to append the installation folder of the Domino server and the location of the `Notes.jar` file. Also, ensure that the `bin` folder of the JDK is included in the PATH environment variable.

For example, if the Domino server is installed in `C:\Lotus` and the JDK resides in `C:\jdk141_05`, the `CLASSPATH` variable should include the following:

`C:\Lotus\Domino\Notes.jar;C:\Lotus\Domino;`
`C:\jdk141_05\bin;`

2 Copy the `Manual_DominoSetup.zip` file from the Select Identity Connector CD to a folder on the Domino server.

3 Extract the `Manual_DominoSetup.zip` file to a folder where you wish to install the Domino agent.

4 Move the `Properties.ini` and `opAttributes.properties` files from the *<Domino Connector Agent Directory>*`\config` folder to the installation folder of the Domino server (such as `C:\Lotus\Domino`).

Reset Domino Administrator Password and Select Identity Administrator Password

If the password of Domino Administrator is not written or you want to reset it in the Properties.ini file for some reason.You can verify in the Properties file that there is no password or there is your existing password in encrypted password format.

You can re-enter the Domino Administrator password without reinstalling the agent in the file `Properties.ini` by running the command line based utility as follows:

***<Domino Connector agent Directory>*\bin>passwordEncrypt.cmd -r respwd**

The following output appears.

```
C:\Program Files\HP Resource Side
Adaptors\Domino_Connector\bin>passwordEncrypt.cmd -r Welcome1 0 [main] INFO
connagents.PasswordEncDec  - Entering PasswordEncDec() >10 [main] INFO
connagents.PasswordEncDec  - Number of arguments = :2 >350 [main] INFO
connagents.PasswordEncDec  - Resource Properties should be modified >350
[main] INFO connagents.PasswordEncDec  - Entering  encryptPass... >470 [main]
INFO connagents.PasswordEncDec  - Encrypted Password.. >>>>>>>>>>>>>>>520
[main] INFO connagents.PasswordEncDec  - Writing to file >520 [main] INFO
connagents.PasswordEncDec  - Password written Successfully>C:\Program
Files\HP Resource Side Adaptors\Domino_Connector\bin>
```

You can re-enter the Select Identity Administrator (typically sisa) password without reinstalling the agent in the file `opAttriutes.ini` by running the command line based utility as follows:

***<Domino Connector agent Directory>*\bin>passwordEncrypt.cmd -s sisapasswd**

The following output appears.

```
C:\Program Files\HP Resource Side
Adaptors\Domino_Connector\bin>passwordEncrypt.cmd -s abc123
0 [main] INFO connagents.PasswordEncDec  - Entering PasswordEncDec()
>10 [main] INFO connagents.PasswordEncDec  - Number of arguments = :2
>350 [main] INFO connagents.PasswordEncDec  - Resource Properties should be
modified
>350 [main] INFO connagents.PasswordEncDec  - Entering  encryptPass...
>470 [main] INFO connagents.PasswordEncDec  - Encrypted Password..
>>>>>>>>>>>>>>>520 [main] INFO connagents.PasswordEncDec  - Writing to file
>520 [main] INFO connagents.PasswordEncDec  - Password written Successfully
>C:\Program Files\HP Resource Side Adaptors\Domino_Connector\bin>
```

Install the Agent on Solaris

You can install the agent using the installation wizard or by manually copying files to the server.

After you install the agent on Solaris, the following directory structure and files are available:

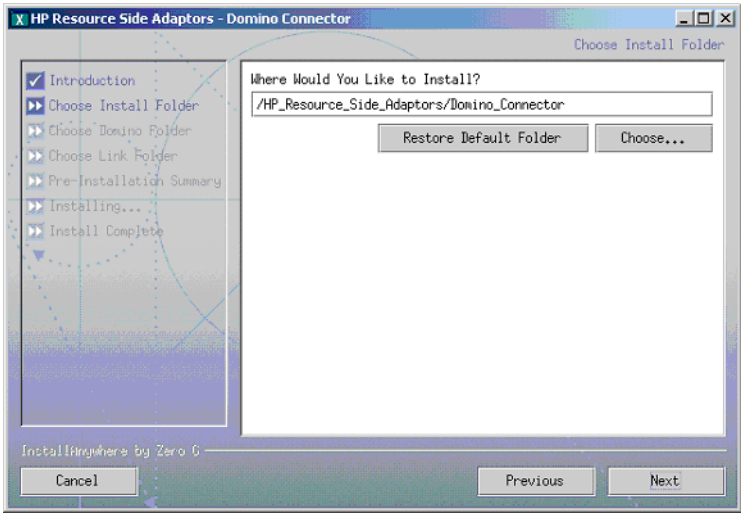
install_dir/	`startDominoApp.sh`	Starts the agent.
install_dir/bin/	`dominoapp.jar`	The main application JAR file. This file is included in the CLASSPATH.
	`connagents.jar`	The JAR file containing the Domino agents.

install_dir/config/	commons-logging.properties	The configuration file for the logging libraries in commons-logging.jar. This file is included in the CLASSPATH.
	log4j.properties	The configuration file for the logging libraries in log4j-1.4.8.jar. This file is included in the CLASSPATH.
install_dir/lib/	commons-logging.jar	Logging libraries. This file is included in the CLASSPATH.
	log4j-1.2.8.jar	Logging libraries. This file is included in the CLASSPATH.
install_dir/lib/	xercesImpl.jar	Xerces XML parser libraries. This file is included in the CLASSPATH.
	xmlParserAPIs.jar	Xerces XML parser libraries. This file is included in the CLASSPATH.
install_dir/logs/		Contains log files generated by the agent.

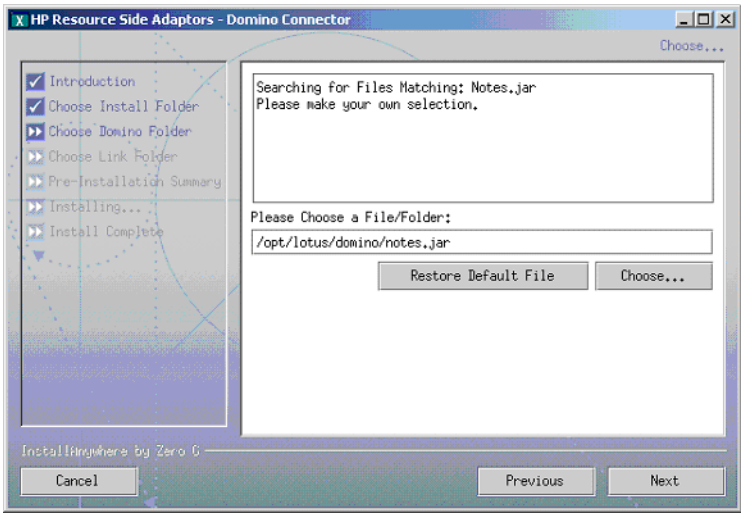
Installation Using the Wizard

Complete the following steps to run the installation wizard, which installs the agent:

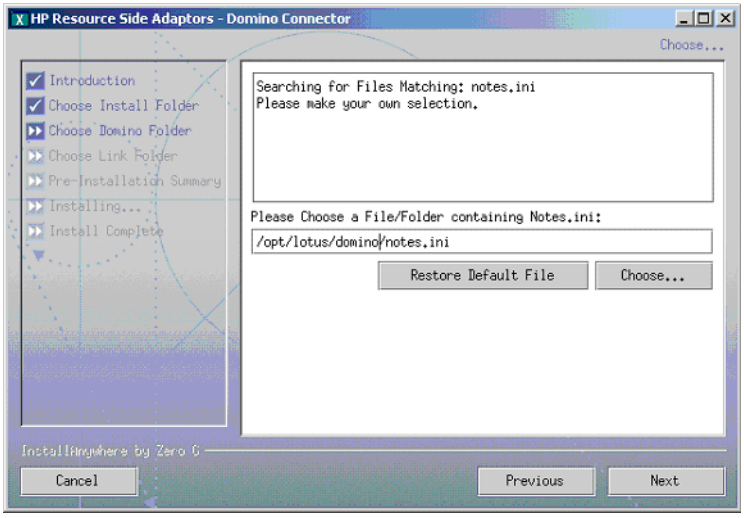
1. Export the display from the Solaris system to any Windows system.
2. Extract `install.bin` from the `DominoSetup.tar` file.
3. Run the installation program (`install.bin`). The Introduction dialog appears.
4. Click **Next** to proceed.
5. Select the mode of installation, and then click **Next**.
6. Specify an installation directory, and then click **Next**.



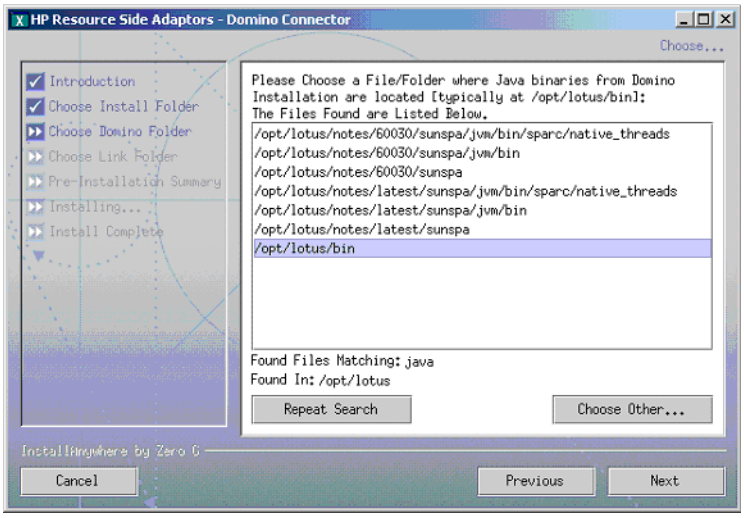
7 Provide the location to the `Notes.jar` file, and then click **Next**.



8 Provide the location to the `Notes.ini` file, and then click **Next**.



9 Select the location of the Domino binaries, and then click **Next**.



10 Verify the pre-installation summary. If you wish to make changes, click **Previous,** and then edit the chosen options. To install the agent, click **Install**.

11 When the installation procedure completes, click **Done** on the Install Complete dialog to close the installation program.

Manual Installation

Complete the following steps to install the agent on the Domino server:

1 Log on to the Solaris system as the same user who installed the Domino server.

2 Export the `CLASSPATH` environment variable and ensure that it includes the path to the Domino installation directory, the path to the `Notes.jar` file, and the path to the JDK `bin` directory.

For example, if Domino is installed in `/usr/lotus` and the JDK resides in `/usr/jdk141_05`, the `CLASSPATH` variable includes the following:

`/usr/lotus/Domino/Notes.jar: /usr/lotus/Domino: /usr/jdk141_05/bin:`

3 Copy the `Manual_DominoSetup.tar` (on UNIX) file from the Select Identity Connector CD to a directory on the Domino server.

4 Extract the contents of the file, which creates the required directory structure.

5 Move the `Properties.ini` and `opAttributes.properties` files from the directory to the Domino Data Directory, which is typically `/usr/lotus/notesdata` or `/lotus/notesdata`.

Configure the Agent

Complete the following steps to configure the agent after installation:

1 Modify the `Properties.ini` file to configure the agent with the necessary access information. This file resides in the Domino Data Directory. The following table describes the properties to be set in the file:

Property	Default	Description
PORT	5051	The port number on which the agent will be listening for requests.
CHECK_LOGIN	true	Whether the agent should verify the logon credentials with the Domino server.
CONCERO_ SERVER_URL	http:// myserver:7001/lmz/ webservice	URL to the Web Service on the Select Identity server, which listens for reverse notifications. Typically, the format of the URL is **http://*server*:*port*/lmz/webservice**.
AltEmailAddress	CN=Administrator /O=Domain	The administrator's email address. When a user is added, the ID files will be emailed to this account if the user model does not have this property.
MAX_LOGIN_ RETRIES	3	Number of retries for the entering logon credentials.
DATABASE_ NAME	Names.nsf	Database name for reverse notification. The modification details are retrieved from this database.
userName	dominoAdmin	The administrative user name on the Domino server. This parameter is used if the agent is installed as a service on Windows.
password	dominoAdminPassw ord	The administrative user's password; this value is encrypted. This parameter is used if the agent is installed as a service on Windows.
CREATE_USER_ MAILBOX_FILE	true	Whether the agent should create a mail file while creating a user.

Property	Default	Description
CREATE_USER_ ID_FILE	true	Whether the agent should create an ID file while creating a user.
DELAY_BEFORE_S PML_SEND	10	The delay in milliseconds before sending SPML requests to the Select Identity server.
NO_RETRIES	3	The number of retries for sending reconciliation SPML requests.
DELAY_BETWEEN _RETRIES	100	The number of milliseconds for which the agent should wait before retrying a request.
DEFAULT_MAIL_T EMPLATE	iNotes6.ntf	Notes template which will be assigned to newly created user if the CREATE_USER_ MAILBOX_FILE option is set to true.
CURRENT_SERVE R_NAME	myDominoServer	Name of the Domino server

Here are the contents of an example `Properties.ini` file:

```
password=rO0ABXNyADhjb20udHJ1bG9naWNhLmNvbm5lY3RvcnMuc2VjdXJpdHkuY2lwaGVy
LkVuY3J5cHRlZE9iamVjdNqDhpyY550aAgAESQAOaVBhZGRpbmdMZW5ndGhaAAxwYWRkaW5nV
mFsdWVMAApvRW5jcnlwdGVkdAASTGphdmEvbGFuZy9PYmplY3Q7TAAJc0FsZ29Vc2VkdAASTG
phdmEvbGFuZy9TdHJpbmc7eHAAAAABAHVyAAJbQqzzF/
gGCFTgAgAAeHAAAAAQamu1EgfWnzVk2URUZ4FcXnQABDNERVM=
userName= dominoAdmin
CREATE_USER_MAILBOX_FILE=false
CREATE_USER_ID_FILE=false
CHECK_LOGIN=true
DELAY_BEFORE_SPML_SEND=10
#PASSWORDREQUEST_KEY_FIELD=FullName
CONCERO_SERVER_URL=http://localhost:7001/lmz/webservice
AltEmailAddress=administrator/hpiso
CURRENT_SERVER_NAME=myDominoServer
PORT=5051
DELAY_BETWEEN_RETRIES=100
DATABASE_NAME=Names.nsf
DEFAULT_MAIL_TEMPLATE=iNotes6.ntf
NO_RETRIES=3
MAX_LOGIN_RETRIES=3
DATABASE_NAME=Names.nsf
NO_RETRIES=3
MAX_LOGIN_RETRIES=3
```

2 Modify the `opAttributes.properties` file, which provides operational attributes that are sent to the Select Identity server during reverse synchronization requests. This file also resides in the Domino Data Directory. The file must contain the following:

- Logon credentials —
  Set the urn:oasis:names:tc:SPML:1:0#UserIDAndOrDomainName and urn:trulogica:concero:2.0#password keys to provide the user name and password needed to authenticate with the Select Identity server.
- The name of the Domino resource in Select Identity —
  Set the urn:trulogica:concero:2.0#resourceId key to the name of the Domino resource.
- The reverse synchronization key —
  Set the urn:trulogica:concero:2.0#reverseSync key to **`true`**.
- The reverse synchronization type —
  Set the urn:trulogica:concero:2.0#resourceType to **`domino`**. This is the name of the XSL file (`domino.xsl`, without the .xsl extension), which provides reverse mappings for the agent to send data back to Select Identity (reverse synchronization).

Here are contents of an example `opAttributes.properties` file:

```
urn:trulogica:concero:2.0#reverseSync=true
urn:trulogica:concero:2.0#resourceId=Domino654
urn:oasis:names:tc:SPML:1:0#UserIDAndOrDomainName=sisa
urn:trulogica:concero:2.0#resourceType=domino
urn:trulogica:concero:2.0#password={ENC:1:Er4nwCXxNR3fwRu3z+
 Otrefg2ODKzAKwL/OFMBHo/
 +kFoqIJOYb5cqeBgXncfkc9SLbodtSvhYMoADVhiGKt9wQWozSs7Hx6l
 edEI1QOvnGEetI3JoRO8zwvK4kx/
 KO9MqVdFrAlpe3f26GooGrfFr0OgEn94Ed0bJpdfKsnRFo=}
```

3 *On Windows:*
Edit the `startDominoApp.cmd` file to replace the $domino_home string with the absolute path to the folder containing the `Notes.jar` file. For example, this file might reside in `C:\Lotus\Domino`.

4 *On Solaris:*
Edit the `log4j.properties` file, which resides in the `config` subdirectory of the installation directory, to replace the <DOMINO_AGENT_INSTALL_PATH> string with the absolute path to the agent's installation directory (where the contents of the `Manual_DominoSetup.tar` file were extracted).

5 *On Solaris:*
Edit the `startDominoApp.sh` file to ensure that the following variables are set according to the Domino server installation:

Variable	Default Value	Description
DOMINO_LIBRARY_PATH	/var/lotus/notes/65010/sunspa	Location of the Domino libraries (including `Notes.jar`)
DOMINO_JAVA_PATH	/var/lotus/bin	Location of the Java executable used by Domino
NOTES_DATA_DIRECTORY	/usr/local/notesdata	Location of the Notes components (such as `Notes.ini`)
COMMANAGER_PATH	/export/home/notes/Select_Identity	Location of the directory where the contents of the `Manual_DominoSetup.tar` file where extracted

6 *On Solaris:*
Copy `connagent.jar` from `<Domino Connector Agent Directory>/bin` to the system where the Domino Administration client is installed.

Configure the Reverse Synchronization Agent in Domino

Perform the following steps to create an Add/Modify agent in Domino, which performs reverse synchronization:

1 Launch the Lotus Domino Designer.

2 Open the Domain Address Book database by completing these steps:

a Select **File** → **Database** → **Open**.

b Enter the following information:

Server: Choose the server, which is typically *machineName/D\domainName* (local is the default).

Database: Specify ***Domino* Address Book**.

File: Specify **names.nsf** (you can browse to *install_dir*\Data\ Names.nsf).

3 Locate Shared Code, and then click **Agent** → **New Agent**.

4 Provide the following information:

— On the first tab:

Name: Specify any name.

Trigger: Select **On Event**.

Runtime: Select **After Documents are created and modified**.

— On the second tab:

Set runtime security level: Select **(2) Allow restricted operations**.

Default Access for Viewing and running the agent: Select **All readers and above enabled**.

Imported Java: Select **Action** → **Run**, then provide the following information:

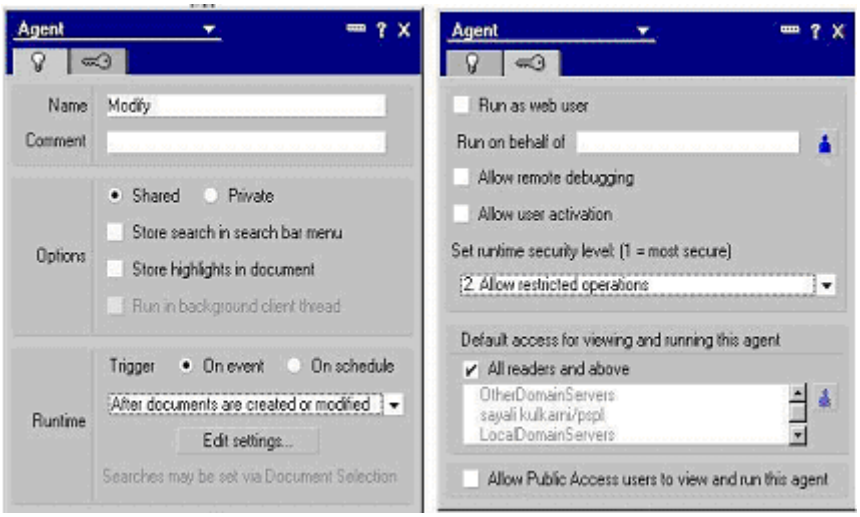
— Click **Import Class Files**.

— Enable **Archive** in Show Files.

— Browse to the folder where the resource-side components are installed.

— In the `bin` folder, select `connagent.jar` and click **Add/Replace Files**.

Enter the base class for Add/Modify Agent as **[com/trulogica/domino/connagents/AddModifyHandler.class]**.



5 Save and close the window.

6 Ensure that the agent is enabled.

Complete the following steps to create a Delete agent:

1 Open the Admin Requests (6) database (such as `admin4.nsf` in Domino Designer).

2 In Recent Databases' for the selected database, locate Shared Code, and then click **Agent** → **New Agent**.

3 Provide the following information:

— On the first tab:

Name: Specify **`DeleteAgent`** or any name.

Trigger: Select **On Event**.

Runtime: Select **After Documents are created and modified**.

— On the second tab:

Set runtime security level: Select **(2) Allow restricted operations**.

Default Access for Viewing and running the agent: Select **All readers and above enabled**.

Imported Java: Select **Action** → **Run**, then provide the following information:

— Click **Import Class Files**.

— Enable **Archive** in Show Files.

— Browse to the folder where the resource-side adapter is installed.

— In the `bin` folder, select `connagent.jar` and click **Add/Replace Files**.

— Enter the base class for Delete agent as **`[com/trulogica/domino/connagents/DeleteEventHandler.class]`**.

4 Save and close the agent.

5 Ensure that the DeleteAgent is enabled.

Configure Password Synchronization in Domino 6.5.*x*

Perform the following steps to configure the Select Identity agent in Domino 6.5.x:

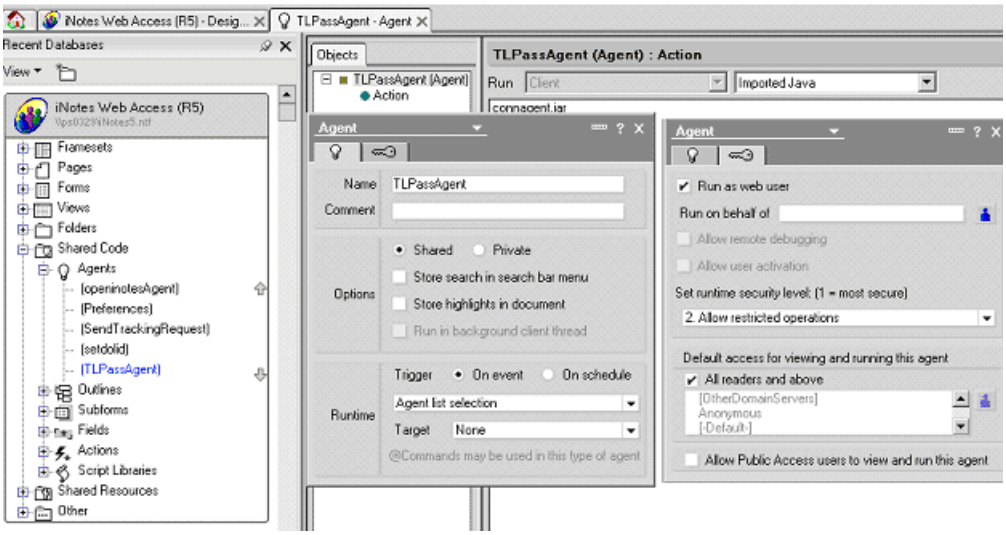
1. Replace the `Form5.nsf` and `Form6.nsf` files that reside in the `\Domino\Data\iNotes` folder with the `Form5.nsf` and `Form6.nsf` files provided by Select Identity. The new files are packaged in `PasswordSync_6_5_1.zip` (for Windows) or `PasswordSync_6_5_1.tar` (for UNIX) on the CD.

   If the `Form`*X*`.nsf` file that resides in `\Domino\Data\iNotes` was previously modified by an administrator, contact your Select Identity representative. Replacing this file with the one provided by Select Identity will overwrite the changes.

2. Launch Domino Designer by selecting **Start** → **Programs** → **Lotus Applications** → **Lotus Domino Designer**.
3. Open the Domain Address Book database by selecting **File** → **Database** → **Open**. The Open Database dialog is displayed.
4. Enter the following information:
   - Choose the correct server (typically *machine_name/domain_name*) from the Server list.
   - Select **iNotes Web Access (R5)** from the Database list if using the Forms5 template, or select **Domino Web Access (6)** if using the Forms6 template.
   - Ensure that **`iNotes5.ntf`** is specified in the Filename field if using the Form5 template, or ensure that **`iNotes6.ntf`** is specified if using the Form6 template.
5. Select **Recent Databases** → **Shared Code** → **Agents** → **New Agent**. The Agent properties dialog is displayed.
6. Enter the following information:
   - On the first tab:
     - Specify any name, such as **`TLPassAgent`**, in the Name field.
     - Select the **Shared** option.
     - Select **On Event** for the Trigger setting.
     - Select **Agent List Selection** for the Runtime setting.
     - Select **None** for the Target setting.
   - On the second tab:
     - Select the **Run as web user** option.
     - Select **2 Allow Restricted operations** for the Set runtime security level setting.
     - Select **All readers and above enabled** for the Default Access for Viewing and running the agent setting.

The following illustrates the settings:



7 Select **Imported Java** from the Action drop-down list, then provide this information:

- Click **Import Class Files**.
- Enable **Archive** in Show Files.
- Browse to the agent's installation folder, select **connagents.jar**, and then click **Add/Replace Files**.
- Set the base class to **`[com/trulogica/domino/connagents/PwChange.class]`**.

8 Close Domino Designer.

Upgrade Users' Mail Templates

Activating password synchronization for Domino users requires that the users migrate to the new (modified) iNotes template. They must also use the iNotes Web Interface to change their Internet password. There are two ways to migrate the user mail template; however, user interaction is required whichever method is used.

Administrator Initiated Upgrade

As the Administrator, you can perform the following steps to initiate the migration of legacy users to the new iNotes template:

1 Open the Domino Administrator.

2 Select the users to migrate from the People list.

3 Right-click and select **Upgrade**. A new form is displayed.

4 Click the **Software Distribution** tab.

5 In the New mail template file name field, enter the path to the new iNotes template provided by Select Identity (`iNotes5.ntf` if using iNotes 5 on Domino 6.5.*x* or `iNotes6.ntf` if using iNotes 6 on Domino 6.5.*x*).

6 Send the mail.

7 Inform the user of the following steps, which he or she must perform after receiving the email:

— Open the Notes mail client.

— Open the mail received from the administrator.

— Click the **Upgrade** button. This initiates the upgrade process.

— Provide the Notes ID password when prompted.

The user's mailbox will be migrated to the new iNotes template.

User Initiated Upgrade

Users can perform the following steps to migrate their mailboxes to the new iNotes template. Instruct the users to perform the following steps:

1 Open his or her mailbox using the Notes client program.

2 Select **File** → **Database** → **Replace Design**, then select the Template Server to the Domino Server.

3 Select the **Show Advanced templates** option.

4 Complete one of the following steps based on the version of Domino:

— If using iNotes 5 on Domino 6.5.*x*, select **iNotes Web Access**. `iNotes5.ntf` is displayed next to the About button.

— If using iNotes 6 on Domino 6.5.*x*, select **Domino Web Access**. `iNotes6.ntf` is displayed next to the About button.

5 Click the **Replace** button to migrate the mailbox to the selected iNotes template.

Change Passwords Using the Web Client

After you configure the default user template (by replacing `iNotes5.ntf` or `iNotes6.ntf`), users can perform the following steps to synchronize their passwords with the Select Identity server. Instruct your users to log on to the iNotes Web Access interface and change their passwords, enabling Domino to save the new Internet passwords. Before sending this procedure to users, substitute your values for variables in the procedure, such as the Domino server name.

Provide the following steps to your users:

1 Launch Internet Explorer and load the following URL:

http://*domino_server_name*/mail/*username*.nsf

where *username* is the user's name in Domino/Notes. The Network Password page is then displayed.

2 Enter your user name (short name) and Password. The iNotes Web Access page is displayed.

3 Click **Preferences**.

4 Click **Save and Close** to close the Preferences page. You are returned to the iNotes Web Access page.

5 Again, click **Preferences**.

6 Click **Change** under Change Internet Password.

7 On the Change Password dialog, enter your old password and a new password. Then, close the dialog.

8 Close the Preferences page.

9 Click **Logout** to log out of the iNotes Web Access pages.

Start the Agent

On Windows:
To start the agent as a service, perform the following steps:

1 From the Start menu, click **Run**, type **`services.msc`** in the Open text box, and then click **OK**. The Services window appears.

Alternatively, from the Start menu, click **Settings** → **Control Panel**. In the Control Panel window, double-click **Administrative Tools**, and then double-click **Services**.

2 Locate the Domino agent service (the service name will appear as specified in step c on page 28) in the Services window and right-click on it to start the service.

To start the domino agent as a console application, run the `startDominoApp.cmd` file from the Command Prompt. When prompted, provide the Domino Administrator's user name and password. To stop the agent at any time, enter **`Exit`** in the Command Prompt window running the agent.

On Solaris:
Start the agent by running the following command from the command line:

```
sh startDominoApp.sh
```

When prompted, provide the Domino Administrator's user name and password.

5 Configuring the Connector with Select Identity

This chapter describes the procedure to configure the Domino connector with Select Identity and the connector specific parameters that you must provide while configuring the connector with Select Identity.

Configuration Procedure

After you deploy the connector RAR on application server, you must configure the connector with Select Identity. Perform the following steps to configure the Domino connector with Select Identity.

1 Add a New Connector

2 Add a New Resource

3 Map Attributes

Add a New Connector

Add a new connector in Select Identity by using the user interface. While adding the connector, do the following:

- In the Connector Name text box, specify a name for the connector.
- In the Pool Name text box, enter **`eis/DominoConnector`**.
- Select **`No`** for the Mapper Available section.

Refer to the *HP Select Identity Connector Deployment Guide* for detailed information on adding a new connector in Select Identity.

Add a New Resource

Add a new resource in Select Identity that uses the newly added connector. Refer to the *HP Select Identity Connector Deployment Guide* for detailed instructions on adding a resource in Select Identity.Refer to the following table while entering the parameters in the Basic Information and the Access Information pages

Table 5 Resource Configuration Parameters

Field Name	Sample Values	Description	Comment
Resource Name	Domino_server	Name given to the resource.	
Connector Name	Domino	The newly deployed connector.	Known as Resource Type on Select Identity 3.3.1.
Authoritative Source	Yes	Whether this resource is a system that is considered to be the authoritative source for user data in your environment. Specify **Yes** if the connector is enabled for reverse synchronization. If the resource is not authoritative, the resource can only modify user entitlements during reverse synchronization.	
Associate to Group	Selected	Whether the system uses the concept of groups. For this connector, select this option.	Applicable only for Select Identity 3.3.1.
Server Name	PSO111	The NETBIOS name of the Domino server.	
Agent Port	5003	The port on which the agent is running on the Domino server.	
UserName	Administrator	Administrative account on the Domino server.	
Password	Password123	Internet password corresponding to the administrative account.	

Table 5 Resource Configuration Parameters (cont'd)

Field Name	Sample Values	Description	Comment
Notes Base Dir	*On Windows:* C:\Lotus\Notes\Data *On UNIX:* /usr/local/notesdata	The Notes data directory. User ID files are created here.	
Domino Certifier ID File	*On Windows:* C:\Lotus\Domino\data\cert.id *On UNIX:* /usr/local/notesdata/cert.id	The Certifier ID that is used to provision users. Note that Domino servers support hierarchical Certifiers.	This field is optional. You can leave this field empty and specify the Domino Certifier ID filename at the time of user creation.
Domino Certifier ID Password	Certpassword	The password corresponding to the specified Certifier.	This field is optional. You can leave this field empty and specify the Domino Certifier ID password at the time of user creation.
Address Book DB File	names.nsf	The Domino Address Book on which all operations are to be performed.	
Is Notes User	yes	Specfies if the users added to the Domino resource are Notes users or not.	The value specified here takes preference over the value specified during user creation.
User Attributes Mapping File Name	dominouser.properties	Name of the domino user properties file used for mapping attributes.	The default value is `dominouser.properties`. You can change the default value if you use some other customized properties file.

- Certifier ID File name and Certifier ID Password fields are mandatory fields to create a Notes user.
- If you use the same Certifier ID File for all users, you must provide the values of Certifier ID File name and Certifier password during resource creation. Otherwise, you must specify these values every time you create a new user.

Map Attributes

After successfully adding a resource for Domino connector, you must map the resource attributes to Select Identity attributes. Add new attributes to Select Identity if necessary. Refer to the *HP Select Identity Connector Deployment Guide* for more information on mapping and creating attributes. While mapping the attributes, refer to the following table for Domino connector attribute mapping information.

You must map the `ShortName` attribute to the `UserName` attribute in Select Identity.

Table 6 Domino Mapping Information

Select Identity Resource Attribute	Domino User Attribute	Label on Domino UI	Description
ShortName	ShortName	Short name/UserID (on the Basics tab)	Primary key for the connector, and this is a mandatory attribute.
Password	Password	(not available in UI)	This is a mandatory attribute.
AltEmail Address	AltEmail Address	(not available in UI)	An alternative email address where Select Identity will send the user's ID file.
FirstName	FirstName	First name (on the Basics tab)	Note that the FullName attribute is automatically generated by the Domino server by combining the FirstName, MiddleName, and LastName attributes. Do not set the FullName attribute; this will cause an error and unpredictable behavior.
MiddleInitial	MiddleInitial	Middle initial (on the Basics tab)	
LastName	LastName	Last name (on the Basics tab)	
Title	Title	Personal title (on the Basics tab)	
JobTitle	JobTitle	Job title (in Work Details on the Work tab)	
CompanyName	CompanyName	Company (in Work Details on the Work tab)	

Table 6 Domino Mapping Information (cont'd)

Select Identity Resource Attribute	Domino User Attribute	Label on Domino UI	Description
Manager	Manager	Manager (in Work Details on the Work tab)	
OfficePhone Number	OfficePhone Number	Office phone (in Work Details on the Work tab)	
CellPhone Number	CellPhone Number	Cell phone (in Work Details on the Work tab)	
OfficeCity	OfficeCity	City (in Company Information on the Work tab)	
OfficeState	OfficeState	State/Province (in Company Information on the Work tab)	
City	City	City (on the Home tab)	
State	State	State/province (on the Home tab)	
Zip	Zip	Zip/postal code (on the Home tab)	
HomePostal Address	HomePostal Address	Street address (on the Home tab)	
HomePhone Number	PhoneNumber	Home phone (on the Home tab)	
Comment	Comment	Comment (on the Miscellaneous tab)	
(not mapped by default)	Suffix	Generational qualifier (on the Basics tab)	
(not mapped by default)	CheckPassword	Boolean for Change Password (on the Basics tab)	
(not mapped by default)	MailSystem	Mail System (on the Mail tab)	
(not mapped by default)	MailDomain	Domain (on the Mail tab)	

Table 6 Domino Mapping Information (cont'd)

Select Identity Resource Attribute	Domino User Attribute	Label on Domino UI	Description
(not mapped by default)	MailServer	Mail Server (on the Mail tab)	
(not mapped by default)	MailFile	Mail file (on the Mail tab)	
(not mapped by default)	MailAddress	Forwarding address (on the Mail tab)	
(not mapped by default)	Internet Address	Internet address (on the Mail tab)	
(not mapped by default)	Message Storage	Format preference for incoming mail (on the Mail tab)	
(not mapped by default)	Encrypt IncomingMail	Encrypt incoming mail (on the Mail tab)	
(not mapped by default)	ccMail Location	CC Mail Location (on the Mail tab)	
(not mapped by default)	ccMailUser Name	CC Mail Username (on the Mail tab)	
(not mapped by default)	Department	Department (in Work Details on the Work tab)	
(not mapped by default)	EmployeeID	Employee ID (in Work Details on the Work tab)	
(not mapped by default)	Location	Location (in Work Details on the Work tab)	
(not mapped by default)	OfficeFAX PhoneNumber	FAX phone (in Work Details on the Work tab)	
(not mapped by default)	PhoneNumber_6	Pager number (in Work Details on the Work tab)	
(not mapped by default)	Assistant	Assistant (in Work Details on the Work tab)	
(not mapped by default)	OfficeStreet Address	Street address (in Company Information on the Work tab)	

Table 6 Domino Mapping Information (cont'd)

Select Identity Resource Attribute	Domino User Attribute	Label on Domino UI	Description
(not mapped by default)	OfficeZIP	Zip/postal code (in Company Information on the Work tab)	
(not mapped by default)	OfficeCountry	Country (in Company Information on the Work tab)	
(not mapped by default)	OfficeNumber	Office Number (in Company Information on the Work tab)	
(not mapped by default)	Country	Country (on the Home tab)	
(not mapped by default)	HomeFAXPhone Number	FAX phone (on the Home tab)	
(not mapped by default)	Spouse	Spouse (on the Home tab)	
(not mapped by default)	Children	Children (on the Home tab)	
(not mapped by default)	PersonalID	Personal ranking (on the Corporate Hierarchy Information tab)	
(not mapped by default)	x400Address	Other X.400 address (on the Miscellaneous tab)	
(not mapped by default)	Calendar Domain	Calendar domain (on the Miscellaneous tab)	
(not mapped by default)	WebSite	Web page (on the Miscellaneous tab)	
(not mapped by default)	PublicKey	Notes certified public key (on the Notes Certificates tab)	
(not mapped by default)	Certificate	Internet certificate (on the Internet Certificates tab)	

Table 6 Domino Mapping Information (cont'd)

Select Identity Resource Attribute	Domino User Attribute	Label on Domino UI	Description
(not mapped by default)	Owner	Owners (on the Administration tab)	
(not mapped by default)	AltFullName	Alternate FullName (on the Administration tab)	
(not mapped by default)	AltFullName Sort	Alternate FullName Sort (on the Administration tab)	
(not mapped by default)	LocalAdmin	Administrators (on the Administration tab)	
(not mapped by default)	Password Digest	Password digest (on the Administration tab)	
(not mapped by default)	Password ChangeDate	Password Change date (on the Administration tab)	
(not mapped by default)	Password Change Interval	Password Change Interval (on the Administration tab)	
(not mapped by default)	PasswordGrace Period	Password Change Grace Period (on the Administration tab)	
(not mapped by default)	ClientType	Notes client license (on the Administration tab)	
(not mapped by default)	Profiles	Setup profile(s) (on the Administration tab)	
(not mapped by default)	AvailableFor DirSync	Foreign directory synch allowed (on the Administration tab)	
(not mapped by default)	NetUserName	Network account name (on the Administration tab)	

Table 6 Domino Mapping Information (cont'd)

Select Identity Resource Attribute	Domino User Attribute	Label on Domino UI	Description
(not mapped by default)	ProposedAlt CommonName	Proposed alternate common name (on the Administration tab)	
(not mapped by default)	ProposedAlt OrgUnit	Proposed alternate unique organizational unit (on the Administration tab)	
(not mapped by default)	Proposed AltFull NameLanguage	Proposed alternate name language (on the Administration tab)	
(not mapped by default)	Sametime Server	Sametime server (on the Administration tab)	
(not mapped by default)	CertifierIDFile	(not available in UI)	The Certifier ID that is used to provision users. Note that Domino servers support hierarchical Certifiers.
(not mapped by default)	CertifierIDPwd	(not available in UI)	The password corresponding to the specified Certifier.
(not mapped by default)	IsNotesUser	(not available in UI)	Specfies if the user is a Notes user or not.

After mapping the attributes, you can use the connector to create a service, or you can associate the connector with an existing service. Refer to the *Service Studio* chapter of the *HP Select Identity Administration Online Help* for information on Select Identity services.

Reverse Synchronization

The agent can send changes made to user attributes on the Domino server to the Select Identity server. The agent sends an SPML request to the Select Identity server that contains the attribute changes. The names of the attributes in the SPML request are defined by Domino. To transform the attribute names to Select Identity attribute names, the request is parsed by Select Identity using the `domino.xsl` file.

The `dominouser.properties` file contains generic Domino attributes that are typically used when a user is created. As described above, you can configure this file to include or exclude attributes. Any addition or deletion of attributes in `dominouser.properties` must also be made in `domino.xsl`. Each block in `domino.xsl` corresponds with each attribute entry in `dominouser.properties`.

If the following mapping is added to `dominouser.properties`:

SI_RESOURCE_ATTRIBUTE|*DOMINO_ATTRIBUTE*

You must add the following block to `domino.xsl`:

```
<xsl:when test="$ATTRNAME ='DOMINO_ATTRIBUTE' ">
  <xsl:call-template name="AttributeBuilder">
    <xsl:with-param name="DSMLELEMENT" select="$DSMLELEMENT"/>
    <xsl:with-param name="ATTRNAME" select="'
     SI_RESOURCE_ATTRIBUTE' "/>
    <xsl:with-param name="ATTRVALUE" select="$ATTRVALUE"/>
    <xsl:with-param name="MODIFYFLAG" select="$MODIFYFLAG"/>
  </xsl:call-template>
</xsl:when>
```

where *DOMINO_ATTRIBUTE* represents the attribute passed from the Domino server and *SI_RESOURCE_ATTRIBUTE* represents the attribute defined by Select Identity and displayed in the resource attributes list.

The XSL file is case sensitive; attributes must be specified exactly as they exist in Select Identity and on the resource. For example, if the mail attribute is defined in Domino, you must specify **`mail`**, not **`Mail`** or **`MAIL`**, and so on.

The following is an example. The mail attribute is added to `dominouser.properties`, as follows:

`Email|mail`

Then, the following block is added to `domino.xsl`:

```
<xsl:when test="$ATTRNAME = 'mail'">
<xsl:call-template name="AttributeBuilder">
<xsl:with-param name="DSMLELEMENT" select="$DSMLELEMENT"/>
<xsl:with-param name="ATTRNAME" select="'Email'"/>
<xsl:with-param name="ATTRVALUE" select="$ATTRVALUE"/>
<xsl:with-param name="MODIFYFLAG" select="$MODIFYFLAG"/>
</xsl:call-template>
</xsl:when>
```

where **`mail`** represents the attribute passed from the Domino server and **`Email`** represents the attribute in Select Identity.
For composite attributes defined in the `dominouser.properties` file, such as [First Name] [Last Name], you must provide two attribute name-value pairs in the `domino.xsl` file. For example, for the following entry in `dominouser.properties`:

```
[First Name] [Last Name]|displayname
```

The XSL file must contain the following:

```
<xsl:when test="$ATTRNAME = 'displayname'">
  <xsl:choose>
    <xsl:when test="contains($ATTRVALUE, ' ')">
      <!-- First Name is before space char -->
      <xsl:call-template name="AttributeBuilder">
        <xsl:with-param name="DSMLELEMENT" select="$DSMLELEMENT"/>
        <xsl:with-param name="ATTRNAME" select="'First Name'"/>
        <xsl:with-param name="ATTRVALUE"
         select="substring-before($ATTRVALUE, ' ')"/>
        <xsl:with-param name="MODIFYFLAG" select="$MODIFYFLAG"/>
      </xsl:call-template>
      <!-- Last Name is after space char -->
      <xsl:call-template name="AttributeBuilder">
```

```
        <xsl:with-param name="DSMLELEMENT" select="$DSMLELEMENT"/>
        <xsl:with-param name="ATTRNAME" select="'Last Name'"/>
        <xsl:with-param name="ATTRVALUE"
         select="substring-after($ATTRVALUE, ' ')"/>
        <xsl:with-param name="MODIFYFLAG" select="$MODIFYFLAG"/>
      </xsl:call-template>
    </xsl:when>
    <xsl:otherwise>
      <!-- If no space, take the whole string as First Name -->
      <xsl:call-template name="AttributeBuilder">
        <xsl:with-param name="DSMLELEMENT" select="$DSMLELEMENT"/>
        <xsl:with-param name="ATTRNAME" select="'First Name'"/>
        <xsl:with-param name="ATTRVALUE" select="$ATTRVALUE"/>
        <xsl:with-param name="MODIFYFLAG" select="$MODIFYFLAG"/>
      </xsl:call-template>
    </xsl:otherwise>
  </xsl:choose>
</xsl:when>
```

6 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 Select Identity.
- Delete the connector from application server.

See *HP Select Identity Connector Deployment Guide* to know more on deleting the connector from Select Identity and application server.

Uninstalling the Domino Agent

You can uninstall the agent manually or by using the wizard. You must use the uninstallation wizard if the agent has been installed with the help of the wizard, or perform the manual steps if the agent has been installed manually.

Perform the following steps on the Domino server to uninstall the agent by using wizard:

1. Go to the `Uninstall_Domino_Connector` directory under the agent home directory and double-click the uninstallation wizard file.
2. Click **Uninstall** on the wizard.
3. When the Uninstall Complete screen appears, click **Done**.

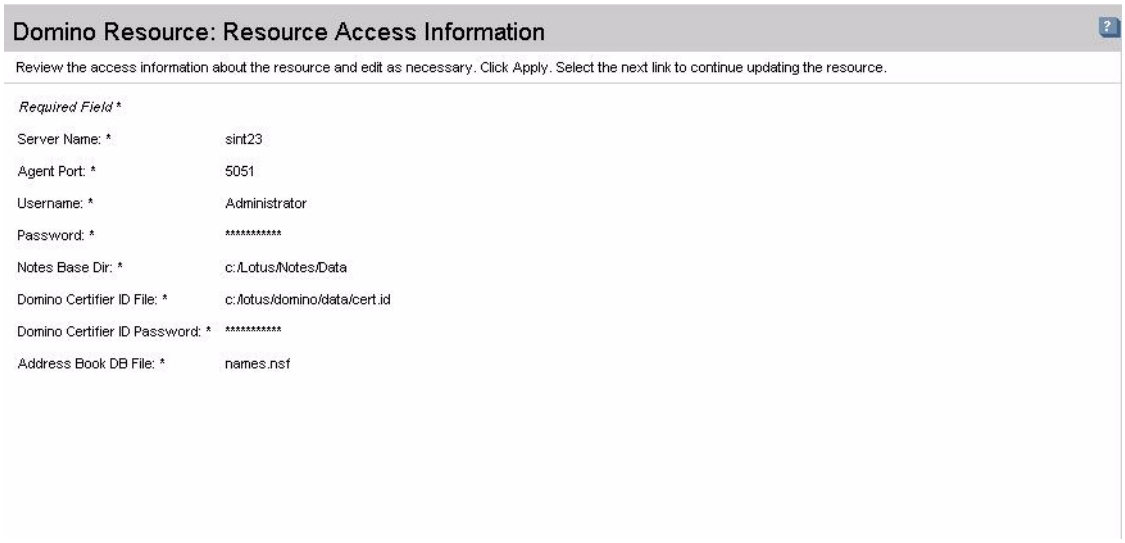
Perform the following steps on the Domino server to delete the agent manually:

1. Stop the agent.
2. Delete the home directory of the agent.
3. Delete the `opAttributes.properties` and `Properties.ini` files from `C:/Lotus/Domino`.
4. Remove the `Forms5.nsf` or `Forms6.nsf` file that was copied during installation.
5. Delete any AddModify, Delete, and Password synchronization agents that were created in the Domino Designer.

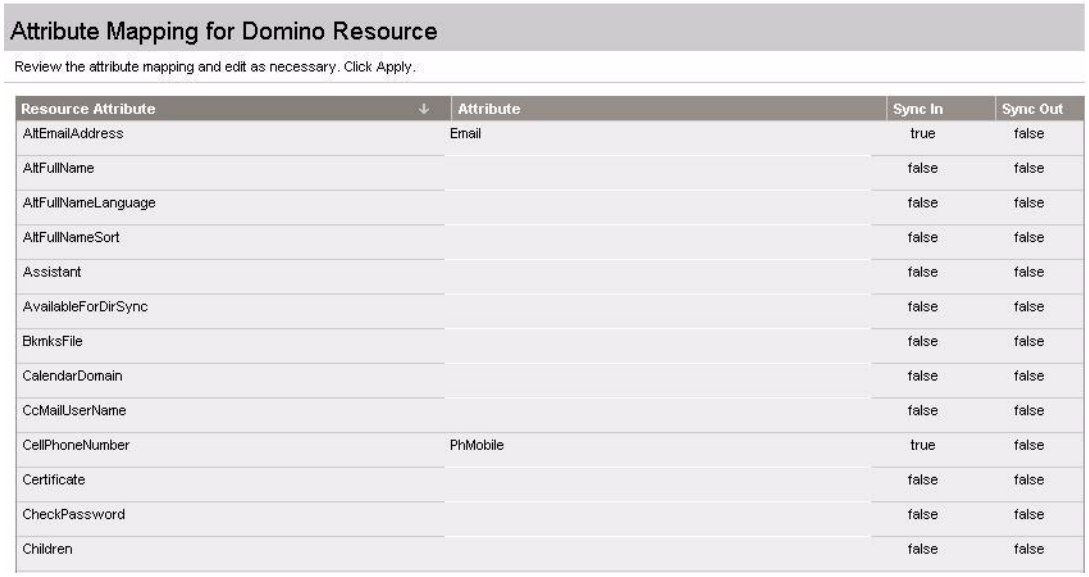
A Sample Images

This chapter illustrates some sample images of Select Identity when Domino connector is deployed on it.

- Select Identity 4.0 displays the Resource Access Information page in the following format, when a domino resource is deployed on it.



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

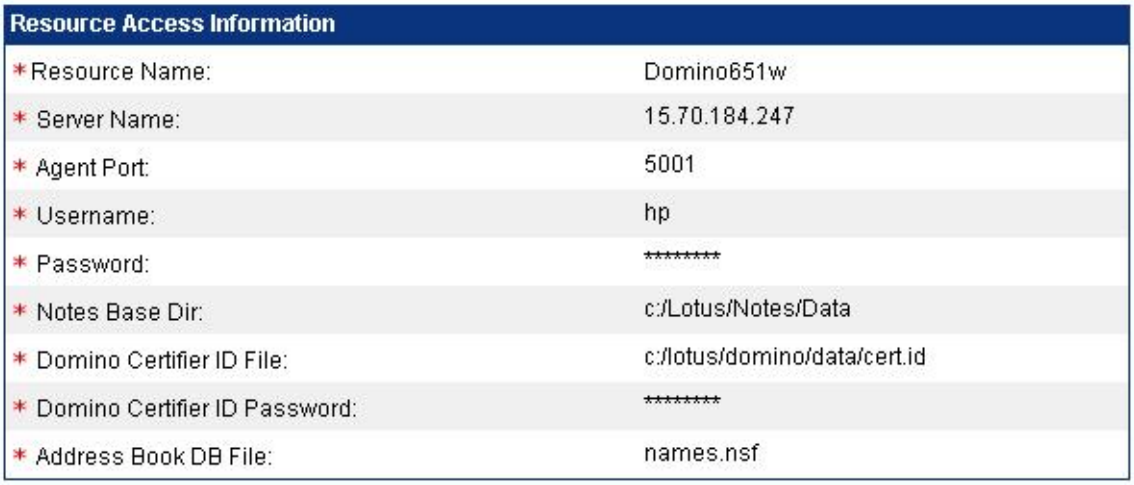


Attribute Mapping for Domino Resource

Review the attribute mapping and edit as necessary. Click Apply.

Resource Attribute ↓	Attribute	Sync In	Sync Out
AltEmailAddress	Email	true	false
AltFullName		false	false
AltFullNameLanguage		false	false
AltFullNameSort		false	false
Assistant		false	false
AvailableForDirSync		false	false
BkmksFile		false	false
CalendarDomain		false	false
CcMailUserName		false	false
CellPhoneNumber	PhMobile	true	false
Certificate		false	false
CheckPassword		false	false
Children		false	false

- Select Identity 3.3.1 displays the Resource Access Information page in the following format, when a domino resource is deployed on it.



Resource Access Information

* Resource Name:	Domino651w
* Server Name:	15.70.184.247
* Agent Port:	5001
* Username:	hp
* Password:	********
* Notes Base Dir:	c:/Lotus/Notes/Data
* Domino Certifier ID File:	c:/lotus/domino/data/cert.id
* Domino Certifier ID Password:	********
* Address Book DB File:	names.nsf

- Select Identity 3.3.1 displays the View Attribute page in the following format, when a domino resource is deployed on it and resource attributes are mapped to Select Identity 3.3.1.

(Resource Name=Domino651w)

Page 1 of 1 Total Records:22

Name	Min Length	Max Length	Attribute Mapped To	Authorative
AltEmailAddress	0	255	Email	N
CellPhoneNumber	0	255	PhMobile	N
City	0	255	City	N
Comment	0	255	Comment	N
CompanyName	0	255	Company	N
Domino651w_ENTITLEMENTS	1	255	Domino651w_ENTITLEMENTS	Y
Domino651w_KEY	1	255	Domino651w_KEY	Y
FirstName	0	255	FirstName	N
HomePhoneNumber	0	255	PhHome	N
homePostalAddress	0	255	HomePostalAddress	N
JobTitle	0	255	JobTitle	N
LastName	0	255	LastName	N
manager	0	255	manager	N
MiddleInitial	0	255	MiddleInitial	N
OfficeCity	0	255	OfficeCity	N
OfficePhoneNumber	0	255	PhBus	N
OfficeState	0	255	OfficeState	N
Password	0	255	Password	N
State	0	255	State	N
Title	0	255	Title	N
UserId	0	255	UserName	N
Zip	0	255	Zip	N

B Group Availability Checking Functionality to Accommodate Domino Users

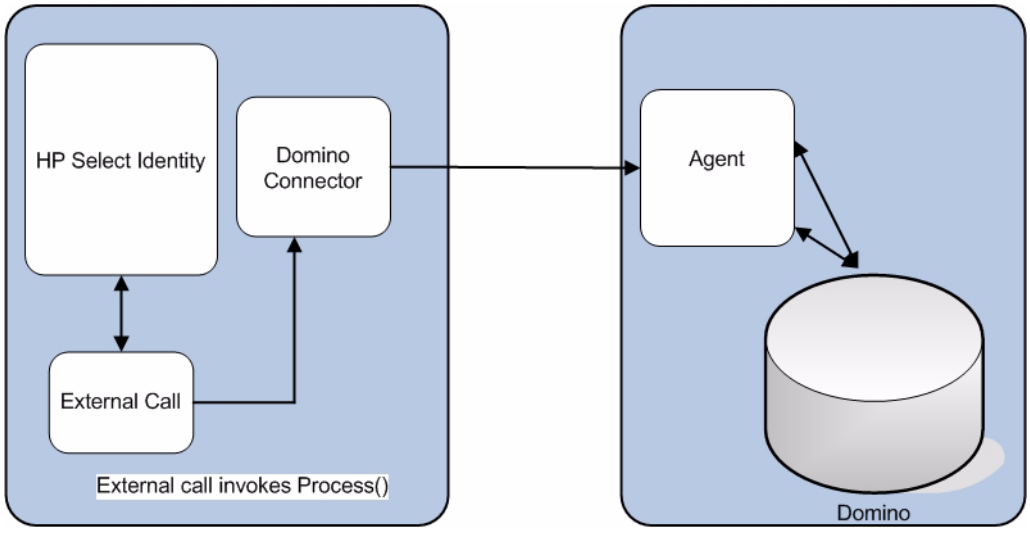
Domino server limits the maximum size of a plain text field (for example, `group Members` field) to 64KB per (non summary) text limit. This limit is encountered by Domino developers in their API calls. To counter this, the `Process()` function is provided in the form of an independent function, which can be executed by an external call (which needs to be developed). This function checks if a group can accommodate more users, creates a new group, links it to the existing group, and returns that group name when the limit is reached.

The Domino Connector is enhanced to expose a function that can be invoked to verify if the group has reached the specified limit of members. This function checks if a given group is available for more users to be assigned to it, create a new group if it is full, and returns this group id.

This limit can be specified by setting `MAX_GROUP_CAPACITY` property in the `Properties.ini` file (default setting is 64k), which is present in the Domino install folder.

If the number of members in the group is lesser than `MAX_GROUP_CAPACITY`, the same group name is returned.

If the number of members in the group is greater than or equal to `MAX_GROUP_CAPACITY`, a new group is created and linked to the existing group and the group name is returned. The name of the new group will be created by appending 1 to the existing group name. For example, if the existing group name is `GROUP` , the new group name will be `GROUP1`.If the `GROUP1` already exists and is full, the new group name will be `GROUP11`, and so on.



This feature can be invoked by writing an external call to invoke `Process()` function by passing appropriate information as explained below:

Instance of `TAConnector`, for example – `t`, is passed and it is cast to `TAConnectorExtIntf`.

The following is a sample code snippet in the external call:

```
TAConnectorExtIntf conn = (TAConnectorExtIntf) t;


SIGenConnectorRequest req = new SIGenConnectorRequest();
JCAUserModel userModel = new JCAUserModel();
userModel.setUserId("Sample user id");  // sample value used
req.setUserModel(userModel);
JCAEntitlementModel entModel = new JCAEntitlementModel("Core Group Id"); /
/ sample used
req.setEntModel(entModel);
req.setOperation("CHECK_AND_CREATE_GROUP");

conn.process(req);
```

The connector will check if the group is available, create a new one if necessary, and return it back to the `entModel` instance:

```
req.getEntModel().getId()
```