

# **HP OpenView Select Identity**

**Connector for  
IBM Lotus Notes/Domino,  
Versions 5.0.8, 5.0.10, 6.0.3, and 6.5.1**

## **Installation and Configuration Guide**

**Connector Version: 3.4  
Select Identity Version: 3.3.1**



**August 2005**

© 2005 Hewlett-Packard Development Company, L.P.

## Legal Notices

### Warranty

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

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

### Restricted Rights Legend

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

Hewlett-Packard Company  
United States of America

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

### Copyright Notices

© 2005 Hewlett-Packard Development Company, L.P.

No part of this document may be copied, reproduced, or translated into another language without the prior written consent of Hewlett-Packard Company. The information contained in this material is subject to change without notice.

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

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 (C) 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](http://www.waveset.com)). Portions Copyright © 2003 Waveset Technologies, Inc. 6034 West Courtyard Drive, Suite 210, Austin, Texas 78730. All rights reserved.

Portions Copyright (c) 2001-2004, Gaudenz Alder. All rights reserved.

## Trademark Notices

HP OpenView Select Identity is a trademark of Hewlett-Packard Development Company, L.P. Microsoft, Windows, the Windows logo, and SQL Server are trademarks or registered trademarks of Microsoft Corporation.

Sun™ workstation, Solaris Operating Environment™ software, SPARCstation™ 20 system, Java technology, and Sun RPC are registered trademarks or trademarks of Sun Microsystems, Inc. JavaScript is a trademark of Sun Microsystems, Inc., used under license for technology invented and implemented by Netscape.

This product includes the Sun Java Runtime. This product includes code licensed from RSA Security, Inc. Some portions licensed from IBM are available at <http://oss.software.ibm.com/icu4j/>.

IBM, DB2 Universal Database, DB2, WebSphere, and the IBM logo are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group.

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

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

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

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

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

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

## Support

Please visit the HP OpenView web site at:

**<http://www.managementsoftware.hp.com/>**

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

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

**<http://support.openview.hp.com/>**

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

- Search for knowledge documents of interest
- Submit and track progress on support cases
- Manage a support contract
- Look up HP support contacts
- Review information about available services
- Enter discussions with other software customers
- Research and register for software training

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

To find more information about access levels, go to:

**[http://support.openview.hp.com/access\\_level.jsp](http://support.openview.hp.com/access_level.jsp)**

To register for an HP Passport ID, go to:

**<https://passport2.hp.com/hpp/newuser.do>**

# contents

<b>Chapter 1</b>	<b>Understanding the Connector</b>	<b>8</b>
<b>Chapter 2</b>	<b>Installing the Connector</b>	<b>13</b>
	System Requirements	14
	Deploying on the Web Application Server	15
	Installing the Agent on the Domino Server	17
	Configuring Domino Security Settings	18
	Installing the Agent on Windows	21
	Installation Using the Wizard	23
	Manual Installation	26
	Installing the Agent on Solaris	26
	Installation Using the Wizard	27
	Manual Installation	30
	Configuring the Agent	31
	Configuring the Reverse Synchronization Agent in Domino	33
	On Domino 5.0.x	33
	On Domino 6.x	36
	Configuring Password Synchronization in Domino 5.0.x	38
	Configuring Password Synchronization in Domino 6.x	40
	Upgrading Users' Mail Templates	42
	Administrator Initiated Upgrade	42
	User Initiated Upgrade	43
	Changing Passwords Using the Web Client	43
	Starting the Agent	44

<b>Chapter 3</b>	<b>Understanding the Mapping Files</b> .....	45
	User Attributes .....	46
	Reverse Synchronization .....	55
<b>Chapter 4</b>	<b>Configuring the Connector</b> .....	58
	Internationalization Support .....	58
	Connector Deployment .....	60
<b>Chapter 5</b>	<b>Uninstalling the Connector</b> .....	66
	Uninstalling the Connector from WebLogic .....	66
	Uninstalling the Domino Agent .....	67

# Understanding the Connector

The Domino connector enables HP OpenView Select Identity to manage user data in IBM Lotus Notes/Domino systems. This connector is a two-way 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. This is called **reverse synchronization**. The mapping files, which are included with the connector, control how Select Identity fields are mapped to Domino fields.

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

- Access levels
- Entitlements
- Roles
- User groups

The following describes how the connector works for each provisioning operations:

- **Adding 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 using the Notes client. When a Domino administrator creates a user on the Domino Administrator Console, he or she must manually send the ID file to the user. The Domino connector has automated 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. See [page 47](#) for a description of the mapping file attribute, or see [Step 1 on page 31](#) for a description of this property in the `Properties.ini` file.

Also, when creating users in Select Identity that will be provisioned on a Domino server, keep the following guidelines in mind:

- The Domino server allows only one ACCESS LEVEL to be specified for a user at a time. Therefore, when creating users in Select Identity, specify only one access level.
- ENTITLEMENT, ROLE, and Group are multivalued 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 when creating the user.

- **Modifying a User—**

The connector can modify all the attributes on the Domino server except for the `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; only changes to the user's HTTP password are synchronized with Select Identity. This function resets the user's HTTP password, and the user must specify this new password while using the Notes Web Interface.

The Notes client uses ID files, which are provided by the administrator, that have different passwords in them. However, users can log in to their mailbox using their old passwords. 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 that 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**, then click **Yes** to continue.
- e** Select **Check password**.

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

<b>Field</b>	<b>Enter</b>
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.

- g Complete the following to enable password verification on each server with which these users authenticate:
- Click the **Configuration** tab and open each Server document.
  - Click the **Security** tab.
  - In the "Check passwords on Notes IDs" field, select **Enabled**.

To disable password verification for an individual user, complete 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**, then click **Yes** to continue.
- d Select **Don't check password**, then click **OK**.

To disable password verification for a server, complete 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**.

# Installing the Connector

The Domino connector is packaged in the following files:

- `DominoConnector.rar` — contains the binaries for the connector
- `Dominoschema.jar` — 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.
- `Manual_DominoSetup.zip` — contains the files for the Domino agent on Windows platforms
- `Manual_DominoSetup.tar` — contains the files for the agent on Solaris platforms
- `DominoSetup.zip` — contains the GUI-based installer for the agent on Windows platforms

- `DominoSetup.tar` — contains the GUI-based installer for the agent on Solaris platforms
- `PasswordSync_5_0_X.zip` — contains the template file for Domino 5.0.x on Windows
- `PasswordSync_5_0_X.tar` — contains the template file for Domino 5.0.x on Solaris
- `PasswordSync_6_5_1.zip` — contains the template file for Domino 6.5.x on Windows
- `PasswordSync_6_5_1.tar` — contains the template file for Domino 6.x on Solaris

These files are located in the `Domino` directory on the Select Identity Connector CD.

## System Requirements

The Domino connector is supported in the following environment:

Select Identity Version	Application Server	Database
3.0.2	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 Solaris 9	Oracle 9i
	WebLogic 8.1.4 on Red Hat Enterprise Linux 3.0	SQL Server 2000
3.3.1	WebLogic 8.1.4 on Windows 2003	SQL Server 2000
	WebSphere 5.1.1 on HP-UX 11i	Oracle 9i

Also, the J2SE Developer Kit (JDK) version 1.4 must be installed on the application server.

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

- Domino 5.0.8 on Windows 2000
- Domino 5.0.10 on Windows 2000
- Domino 6.0.3 on Solaris 9
- Domino 6.5.1 on Windows 2000 and Solaris 9

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 OpenView Select Identity Installation and Configuration Guide* for more information.
- The resource should be configured to support local language characters.

See [Internationalization Support](#) on page 58 for more information.

## Deploying on the Web Application Server

To install the Domino connector on the Select Identity server, complete these steps:

- 1 Create a subdirectory in the Select Identity home directory where the connector's RAR file will reside. For example, you could create the `C:\Select_Identity\connectors` folder on Windows. (A connector subdirectory may already exist.)
- 2 Copy the `DominoConnector.rar` file from the Select Identity Connector CD to the connector subdirectory.
- 3 Create a schema subdirectory in the Select Identity home directory where the connector's mapping file(s) will reside. For example, you could create the `C:\Select_Identity\schema` folder. (This subdirectory may already exist.)
- 4 Extract the contents of the `Dominoschema.jar` file (on the Select Identity Connector CD) to the schema subdirectory.

- 5 Ensure that the CLASSPATH environment variable in the WebLogic server startup script references the schema subdirectory.
- 6 Start the application server if it is not currently running.
- 7 Log on to the WebLogic Server Console.
- 8 Navigate to *My\_domain* → **Deployments** → **Connector Modules**.
- 9 Click **Deploy a New Connector Module**.
- 10 Locate and select the `DominoConnector.rar` file from the list. It is stored in the connector subdirectory.
- 11 Click **Target Module**.
- 12 Select the **My Server** (your server instance) check box.
- 13 Click **Continue**. Review your settings.
- 14 Keep all default settings and click **Deploy**. The Status of Last Action column should display **Success**.
- 15 Modify the mapping files as needed. The mapping files are described in [Understanding the Mapping Files on page 45](#).
- 16 To configure reverse synchronization on the server, extract the `domino.xsl` file from the `Dominoschema.jar` file to the Select Identity home directory. This file maps user attributes on the Windows server to attributes in Select Identity.

Because the attributes in the `domino.xsl` file are based on those in the `dominouser.properties` and `dominogroup.properties` files, you must modify the `domino.xsl` file to reflect changes made to these files ([Step 15](#)).

After installation, refer to [Configuring the Connector on page 58](#) for information about registering and configuring the connector in Select Identity.



# Installing the Agent on the Domino Server

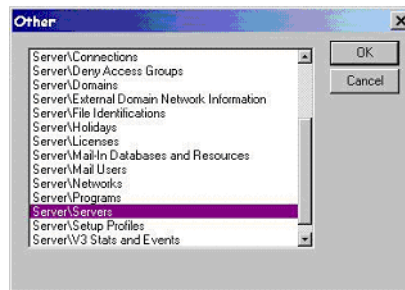
This is an agent-based connector. The agent is a suite of Services and support files deployed on the resource. The following procedures are provided in this section:

- [Configuring Domino Security Settings on page 18](#) — Enables reverse synchronization; this must be performed before installing the agent
- [Installing the Agent on Windows on page 21](#) — Installs the agent (using a wizard or manually) on Windows
- [Installing the Agent on Solaris on page 26](#) — Installs the agent (using a wizard or manually) on Solaris
- [Configuring the Agent on page 31](#) — Provides settings in the agent's configuration files; you must perform this procedure
- [Configuring the Reverse Synchronization Agent in Domino on page 33](#) — Configures Domino to use the reverse synchronization feature of the agent
- [Configuring Password Synchronization in Domino 5.0.x on page 38](#) — Enables reverse (password) synchronization for Domino 5.0.x; this must be performed after the agent is installed
- [Configuring Password Synchronization in Domino 6.x on page 40](#) — Enables reverse (password) synchronization for Domino 6.x; this must be performed after the agent is installed
- [Upgrading Users' Mail Templates on page 42](#) — Enables Domino to use the new template file for all new users, which is necessary for reverse synchronization, then provides procedures to migrate existing users to the new template
- [Changing Passwords Using the Web Client on page 43](#) — Provides a procedure to enable users to synchronize user passwords with the Select Identity server.
- [Starting the Agent on page 44](#) — Provides the command to start the agent on Windows and Solaris

## Configuring Domino Security Settings

The following procedure describes how to configure security settings on the Domino server (versions 5.0.8, 5.0.10, and 6.5.1) running on Windows or Solaris. You must complete these steps to run the agent, which is Java-based, for reverse synchronization.

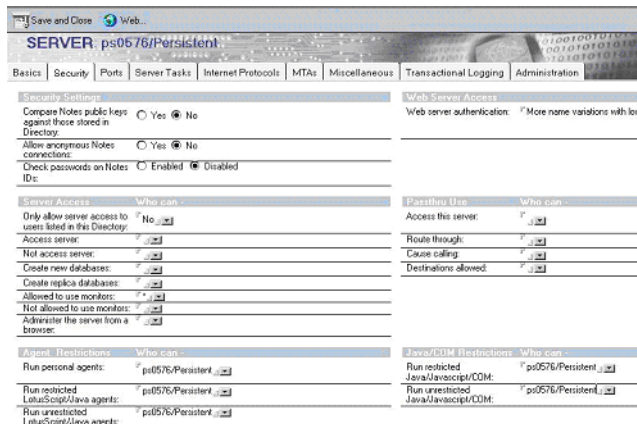
- 1 Verify that the Domino server is running.
- 2 Launch the Domino Administrator.
- 3 Modify the security settings for the server, as follows:
  - a Select **View** → **Server** → **Other**. The Other dialog is displayed.



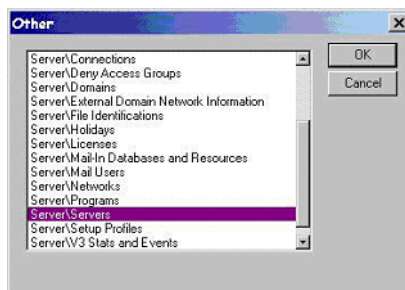
- b Select **Server/Servers** from the list and click **OK**. The Domino Address Book - Server/Servers dialog is displayed.
- c Click **Edit Server**.
- d Select the **Security** tab.
- e Navigate to the Server Access section on the Security tab and select the **users listed in all trusted directories** option. In the And section, select the account (*server\_name/domain\_name*).
- f If you are running Domino 5.0.8 and 5.0.10, locate the Agents Restriction 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 personal agents
  - Run restricted LotusScript/Java agents
  - Run unrestricted LotusScript/Java agents

- Run restricted Java/JavaScript/COM
- Run unrestricted Java/JavaScript/COM

The following illustrates the Domino 5.0.x security settings:

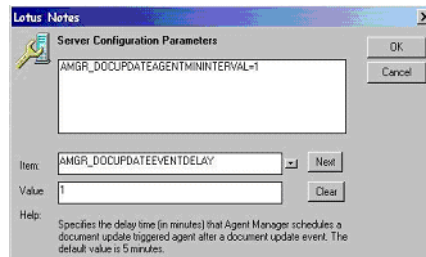


- g If you are running Domino 6.5.1 on Windows, locate the Programmability Restrictions section of the Security tab and edit the following settings to include the Administrator account and Server account (*server\_name/domain\_name*) on the Domino server:
  - Run Unrestricted methods and operations
  - Run Restricted Lotus script/Java Agents
- 4 Modify the preferred `Notes.ini` settings, as follows:
  - a Select **View** → **Server** → **Other**. The Other dialog is displayed.



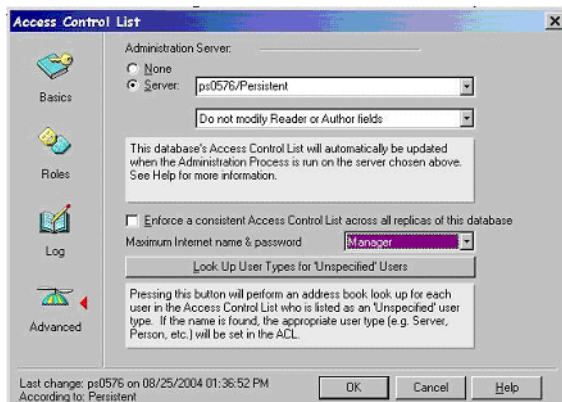
- b Select **Server/Servers** from the list and click **OK**. The Domino Address Book - Server/Servers dialog is displayed.

- c Select **Configuration** → **Servers** → **Configurations**.
- d Select the server name.
- e Click **Edit Configuration**.
- f Click the **NOTES.INI Settings** tab.
- g Click **Set/Modify Parameters**.
- h Specify **1** as the value of **AGMR\_DOCUPDATEAGENTMININTERVAL** and click **Next** (on 5.x) or **Add** (on 6.x).
- i Specify **1** as the value of **AGMR\_DOCUPDATEEVENTDELAY** and click **Next** (on 5.x) or **Add** (on 6.x).



- j Click **OK** to close the dialog.
- k Save your settings and close the Other dialog.

- 5 To set access control settings, which enable the connector to perform operations related to roles and entitlements, complete these steps:
  - a Select **File** → **Database** → **Access Control**. The Access Control List dialog is displayed.



- 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.

## Installing the Agent on Windows

You can install the agent 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:

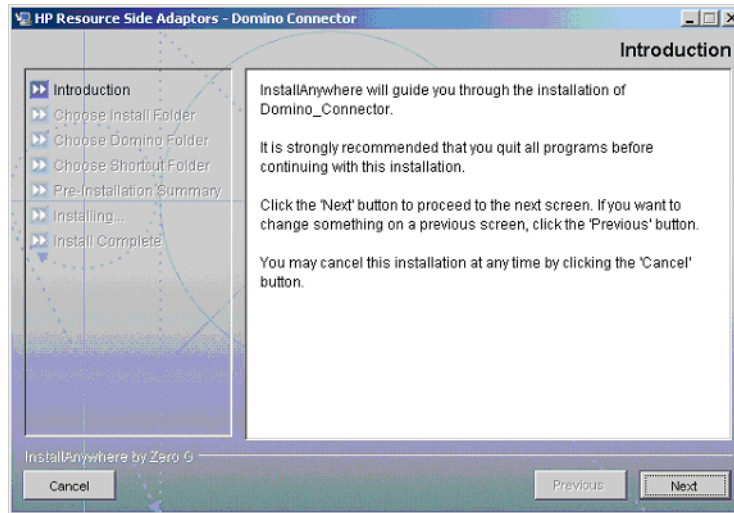
<code>install_dir\</code>	<code>startDominoApp.cmd</code>	Starts the agent.
<code>install_dir\bin\</code>	<code>dominoapp.jar</code>	The main application JAR file. This file is included in the CLASSPATH.
	<code>connagents.jar</code>	The JAR file containing the Domino agents.

<i>install_dir\config\</i>	commons-logging.properties	<b>The configuration file for the logging libraries in commons-logging.jar. This file is included in the CLASSPATH.</b>
	log4j.properties	<b>The configuration file for the logging libraries in log4j-1.4.8.jar. This file is included in the CLASSPATH.</b>
<i>install_dir\lib\</i>	commons-logging.jar	<b>Logging libraries. This file is included in the CLASSPATH.</b>
	log4j-1.2.8.jar	<b>Logging libraries. This file is included in the CLASSPATH.</b>
	xercesImpl.jar	<b>Xerces XML parser libraries. This file is included in the CLASSPATH.</b>
	xmlParserAPIs.jar	<b>Xerces XML parser libraries. This file is included in the CLASSPATH.</b>

## Installation Using the Wizard

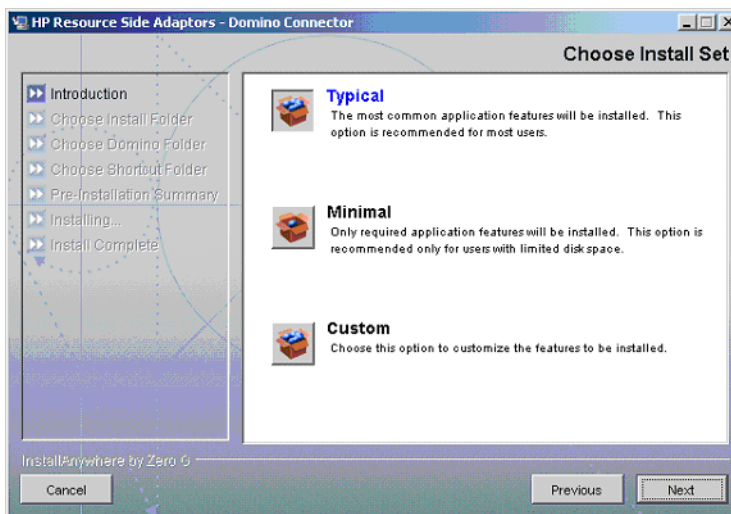
Complete the following steps to run the installation wizard, which installs the agent:

- 1 Extract `install.exe` from the `DominoSetup.zip` (for Windows) or `DominoSetup.tar` (for UNIX) file.
- 2 Run the installation wizard (`install.exe`). The following dialog displays:

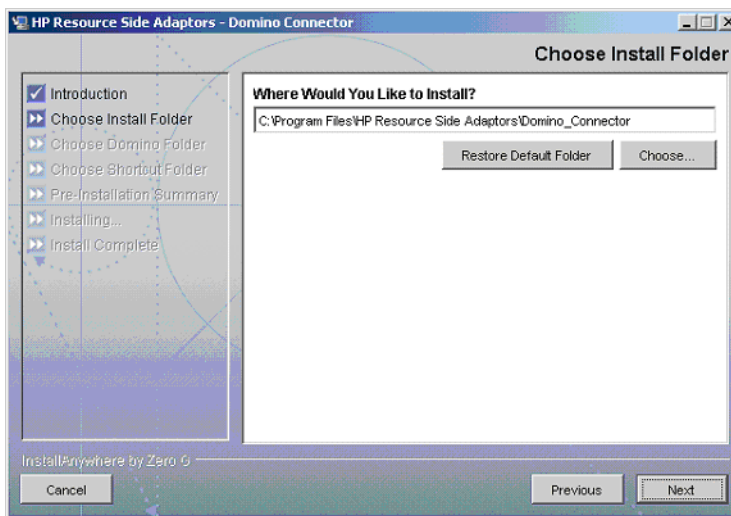


- 3 Click **Next** to proceed.

- 4 Select the mode of installation, then click **Next**.

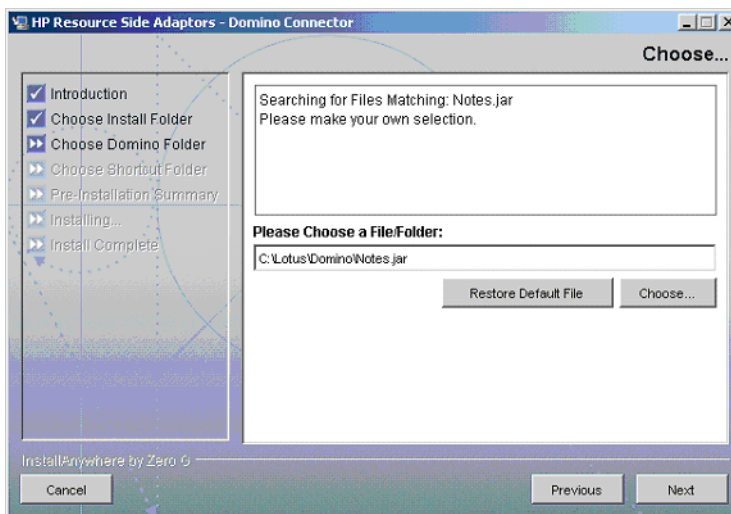


- 5 Specify an installation directory, then click **Next**.

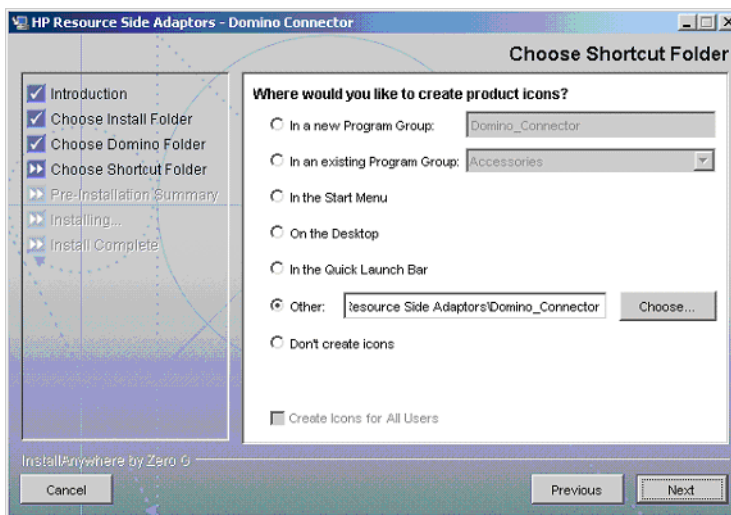




- 6 Provide the location to the Notes . jar file, then click **Next**.



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



- 8 Verify the pre-installation summary. If you wish to make changes, click **Previous** and edit the chosen options. To install the agent, click **Install**.
- 9 When the installation wizard completes, click **Done** on the Install Complete dialog to close the installation program.

## 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 `DominoAgent.zip` file from the Select Identity Connector CD to a folder on the Domino server.
- 3 Extract the `DominoAgent.zip` file to a folder where you wish to install the Domino agent. A folder named `DominoAgent` is created.
- 4 Move the `Properties.ini` and `opAttributes.properties` files from the `DominoAgent\config` folder to the installation folder of the Domino server (such as `C:\Lotus\Domino`).

## Installing 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:

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

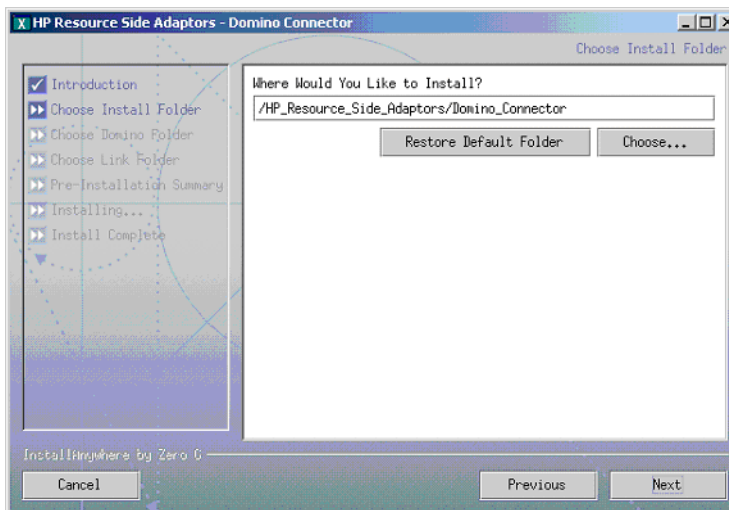
<i>install_dir/config/</i>	<code>commons-logging.properties</code>	The configuration file for the logging libraries in <code>commons-logging.jar</code> . This file is included in the CLASSPATH.
	<code>log4j.properties</code>	The configuration file for the logging libraries in <code>log4j-1.4.8.jar</code> . This file is included in the CLASSPATH.
<i>install_dir/lib/</i>	<code>commons-logging.jar</code>	Logging libraries. This file is included in the CLASSPATH.
	<code>log4j-1.2.8.jar</code>	Logging libraries. This file is included in the CLASSPATH.
	<code>xercesImpl.jar</code>	Xerces XML parser libraries. This file is included in the CLASSPATH.
	<code>xmlParserAPIs.jar</code>	Xerces XML parser libraries. This file is included in the CLASSPATH.

## Installation Using the Wizard

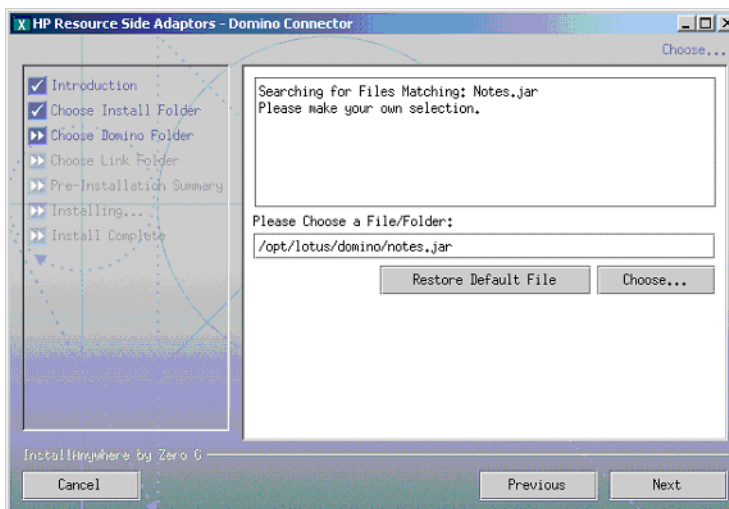
Complete the following steps to run the installation wizard, which installs the agent:

- 1 Export the display from the Solaris system to any Windows system.
- 2 Run the installation wizard (`install.bin`), which is located in the `CDROM_Installers/Disk1/InstData/Solaris/NoVM` directory on the CD. The Introduction dialog displays.
- 3 Click **Next** to proceed.
- 4 Select the mode of installation, then click **Next**.

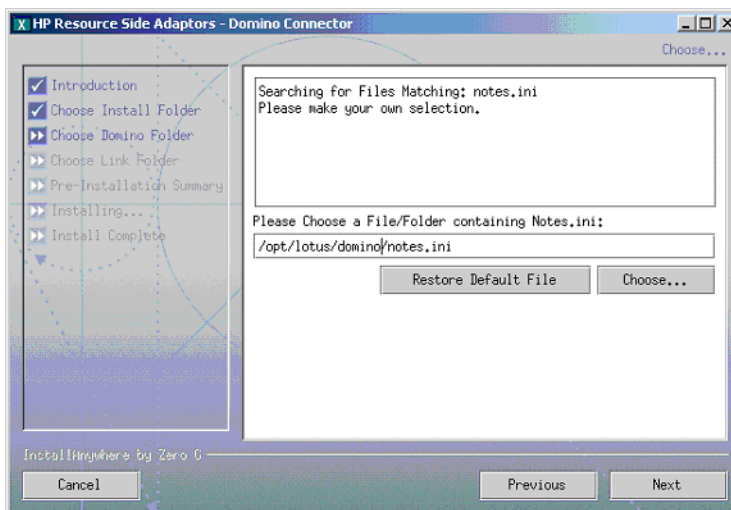
5 Specify an installation directory, then click **Next**.



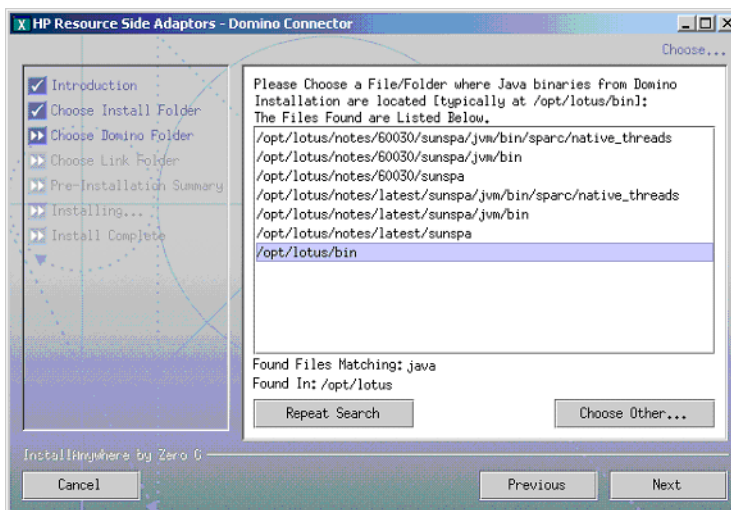
6 Provide the location to the Notes.jar file, then click **Next**.



- 7 Provide the location to the `Notes.ini` file, then click **Next**.



- 8 Select the location of the Domino binaries, then click **Next**.



- 9 Verify the pre-installation summary. If you wish to make changes, click **Previous** and edit the chosen options. To install the agent, click **Install**.
- 10 When the installation wizard 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 will include the following:

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

- 3 Copy the Manual\_DominoSetup.zip (on Windows) or 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.

## Configuring 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 set in the file:

Property	Default	Description
PORT	5002	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 <b>http://server.port/lmz/webservice</b> .
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.

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

```
PORT=5003
CHECK_LOGIN=true
CONCERO_SERVER_URL=http://domino_svr1:7001/lmz/webservice
AltEmailAddress=CN=Administrator/O=Domain
MAX_LOGIN_RETRIES=3
DATABASE_NAME=Names.nsf
```

- 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:conceroc:2.0#password` keys to provide the user name and password need to authenticate with the Select Identity server.
  - **The name of the Domino resource in Select Identity —**  
Set the `urn:trulogica:conceroc:2.0#resourceId` key to the name of the Domino resource.
  - **The reverse synchronization key —**  
Set the `urn:trulogica:conceroc:2.0#reverseSync` key to `true`.
  - **The reverse synchronization type —**  
Set the `urn:trulogica:conceroc:2.0#reverseType` 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:oasis:names:tc:SPML:1:0#UserIDAndOrDomainName=sisa
urn:trulogica:conceroc:2.0#password=abc123
urn:trulogica:conceroc:2.0#resourceId=Domino510
urn:trulogica:conceroc:2.0#reverseSync=true
urn:trulogica:conceroc:2.0#reverseType=domino
```

- 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 `DominoAgent.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	<code>/var/lotus/notes/65010/sunspa</code>	Location of the Domino libraries (including <code>Notes.jar</code> )
DOMINO_JAVA_PATH	<code>/var/lotus/bin</code>	Location of the Java executable used by Domino
NOTES_DATA_DIRECTORY	<code>/usr/local/notesdata</code>	Location of the Notes components (such as <code>Notes.ini</code> )
COMMANAGER_PATH	<code>/export/home/notes/Select_Identity</code>	Location of the directory where the contents of the <code>DominoAgent.tar</code> file were extracted

**6** *On Solaris:*

Copy `connagent.jar` from `DominoAgent/bin` to the system where the Domino Administration client is installed.

## Configuring the Reverse Synchronization Agent in Domino

The following sections provide instructions to configure Domino to use the agent for reverse synchronization.

### On Domino 5.0.x

Complete the following steps to create an Add/Modify agent in Domino:

- 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 Agents and select **Create a New Agent**.**4** Provide the following information:

**Name:** Specify *TAgent* or any name.

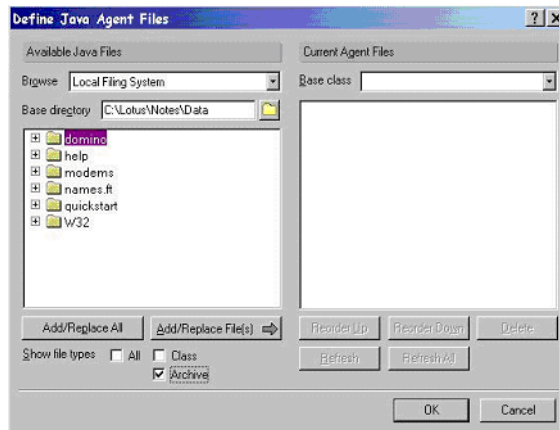
**Shared Agent:** Leave this unchecked.

**When should this Agent run on:** Select **If Documents Have Been Created or Modified?**.

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

- Click **Import Class Files**.
- Enable **Archive** in Show Files.
- Browse to the folder where the resource-side components are installed.
- Under the `bin` folder, select `connagent.jar` and click **Add/Replace Files**.

- Enter the base class for Add/Modify Agent as `[com/trulogica/domino/cnagents/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 Administration Requests (5) database (such as `admin4.nsf` in Domino Designer).
- 2 Locate Agents and select **Create a New Agent**.
- 3 Provide the following information:

Name: Specify `DeleteAgent` or any name.

Shared Agent: Leave this option unchecked.

When should this Agent run on: Select **If Documents Have Been Created or Modified?**.

Imported Java: Select **Action** → **Run**, then provide this 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 `cnagent.jar` and click **Add/Replace Files**.
- Enter the base class for Delete agent as `[com/trulogica/domino/cnagents/DeleteEventHandler.class]`.

- 4 Save and close the window.
- 5 Ensure that the agent is enabled.

## On Domino 6.x

Complete the following steps to create an Add/Modify agent in Domino:

- 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, then click **Agent** → **New Agent**.
- 4 Provide the following information:
  - On the first tab:
 

Name: Specify any name.

Trigger: Select **On Event**.

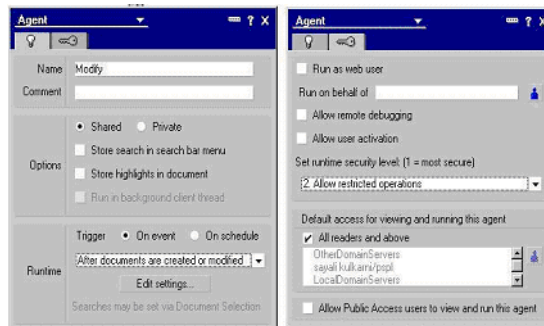
Runtime: Select **After Documents are created and modified**.
  - On the second tab:
 

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/truologica/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, 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/truologica/domino/connagents/DeleteEventHandler.class]`.
- 4 Save and close the agent.
  - 5 Ensure that the DeleteAgent is enabled.

## Configuring Password Synchronization in Domino 5.0.x

The following procedure configures the agent installed on the Domino 5.0.8 and 5.0.10 server, enabling the agent to perform password synchronization.

- 1 Replace the `Form5.nsf` file that resides in the `\Domino\Data\iNotes` folder with the `Form5.nsf` file provided by Select Identity. The new `Form5.nsf` file is packaged in `PasswordSync_5_0_X.zip` (for Windows) or `PasswordSync_5_0_X.tar` (for UNIX) on the CD.
  - ▶ If the `Form5.nsf` file that resides in `\Domino\Data\iNotes` was previously modified by an administrator, contact your HP OpenView Select Identity representative. Replacing this file with the one provided by Select Identity will overwrite the changes.
- 2 Start the Domino server by selecting **Start** → **Programs** → **Lotus Applications** → **Lotus Domino Server**.
- 3 Launch Domino Designer by selecting **Start** → **Programs** → **Lotus Applications** → **Lotus Domino Designer**.
- 4 Open the `iNotesMail` and `C&S` template.
- 5 Select **File** → **Database** → **Open**. This displays the Open Database dialog.
- 6 Enter the following information on this dialog:
  - For Server, enter `local`.
  - For Database, enter `iNotes Mail and C&S`.
  - Ensure that `iNotes5.nsf` is listed in the Filename field.
- 7 Select **View** → **Agents**, which displays the agent dialog.
- 8 Click **New Agent**.

- 9 Provide the following information in the dialog:
  - Specify any name, such as **TAPassAgent**, in the Name field.
  - Select the **Shared** option.
  - Select **Manual from agent list** for the When should this Agent run on? setting.
  - Select **runonce at command** for the Which document should it act on? setting.
  - 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 click **Add/Replace Files**.
    - Set the base class to `[com/truologica/domino/connagents/PwChange.class]`.
- 10 Save the settings and close the dialog.
- 11 On the agent window, enable **Web Agent**.
- 12 Ensure that the Runtime Security Level option is set to **2. Allow restricted Operations**.
- 13 Close Domino Designer.

## Configuring Password Synchronization in Domino 6.x

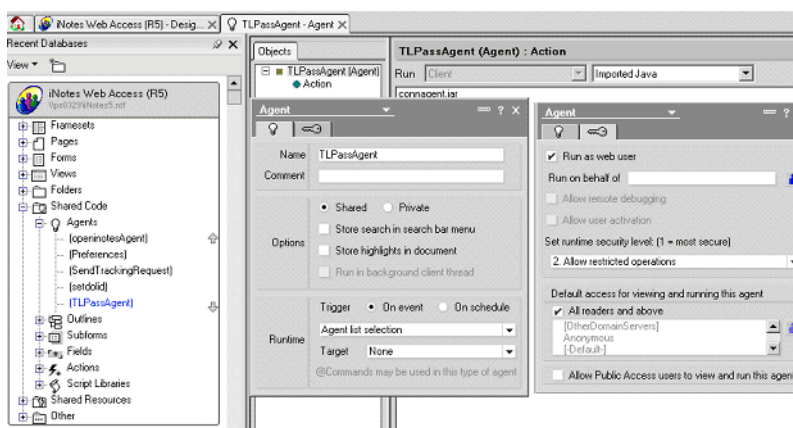
Complete the following steps to configure the Select Identity agent in Domino 6.0.8 or 6.5.1:

- 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 `FormX.nsf` file that resides in `\Domino\Data\iNotes` was previously modified by an administrator, contact your HP OpenView 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 `TAPassAgent`, 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 click **Add/Replace Files**.
  - Set the base class to `[com/truologica/domino/connagents/PwChange.class]`.
- 8 Close Domino Designer.

## Upgrading Users' Mail Templates

To enable Domino to use the new template file for all new users, edit the `Notes.ini` file located in `C:\Lotus\Domino` to change the `DefaultMailTemplate` entry. Replace `mail50.ntf` with the name of the iNotes template (`iNotes5.ntf` or `iNotes6.ntf`). Therefore, the entry will look like this:

```
DefaultMailTemplate=iNotes6.ntf
```

Then, perform the procedures in this section only if you have created users on the Domino server using `Select Identity` prior to configuring Domino to use the new template (`iNotes5.ntf` or `iNotes6.ntf`).

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 5.0.x or Domino 6.x or `iNotes6.ntf` if using iNotes 6 on Domino 6.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 5.x, select **iNotes Mail and C&S** from the list. `iNotes5.ntf` is displayed next to the About button.
  - If using iNotes 5 on Domino 6.x, select **iNotes Web Access**. `iNotes5.ntf` is displayed next to the About button.
  - If using iNotes 6 on Domino 6.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.

## Changing 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.

## Starting the Agent

*On Windows:*

Start the agent by entering `startDominoApp.cmd` from a 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.

## Understanding the Mapping Files

The Domino connector is deployed with the following mapping files, which map user and group account additions and modifications from Select Identity to the Domino server (forward mapping):

- `dominouser.properties`
- `dominogroup.properties`

These files contain the attributes required by the resource.

In addition, the Domino connector provides the `domino.xml` file, which maps attributes in Domino to those in Select Identity (reverse mapping). Configure this file if you wish to support reverse synchronization.

When you deploy a resource through the Resources pages on the Select Identity client, you can review these files.



Note that the `dominogroup.properties` file is installed with the Domino connector and must be present on the system, but group provisioning is not supported at this time.

You can create attributes that are specific to Select Identity using the Attributes pages on the Select Identity client. You can then use these attributes to associate Select Identity user accounts with system resources by mapping the attributes in the mapping files described in this chapter. This

process becomes necessary because, for example, a single attribute “username” can have a different definition on three different resources, such as “login” for UNIX, “UID” for a database, and “userID” on a Windows server.

## User Attributes

You do not need to edit the `dominouser.properties` file unless you want to map additional attributes to your resource. If attributes and values are not defined in the mapping files, they cannot be saved to the resource through Select Identity. The `dominouser.properties` file is a text file that maps each Select Identity user attribute to an attribute on the resource; the attributes are delimited by `|`. Consider this excerpt:

```
UserId|UserId
```

The Select Identity user attribute is named `UserId` and it is mapped to the `UserId` attribute on the Domino resource. In this case, the attributes have the same name, though often they do not.

Attributes can be concatenated. The attribute names and the separators must not contain the `|` delimiter. For concatenation, the format is as follows:

```
[<SI Attribute>]<separator>[<SI Attribute>] |<Resource Attribute>
```

as in this example:

```
[addr1] [addr2] |HomePostalAddress
```

where `addr1` and `addr2` are attributes in Select Identity. They are concatenated to form the value of the `HomePostalAddress` attribute on the resource. A space is used as a separator between the two Select Identity attributes.

The `dominouser.properties` file provides the mandatory mappings that must be configured for Select Identity to provision users on the Domino server. The primary key is `UserId`; this Domino attribute must be mapped to a Select Identity attribute in order for user information to be stored on the Domino server. It should be the first entry in `dominouser.properties`.

You can edit the Select Identity resource attributes; they reflect the identity information as seen in Select Identity. The physical resource attributes are literal attributes of user accounts on Domino. These attributes cannot be

changed. The following table provides a list of all Domino attributes that you can map if you wish to provision users with this information. Here is a description of the columns provided in the table:

- **Select Identity Resource Attribute**— The attribute used by the Domino connector, as defined in the mapping file.
- **Domino User Attribute** — The attribute name on the Domino server.
- **Label on Domino UI** — The name of the property on the Domino UI that corresponds to the attribute on the Domino server.
- **Description** — A description of the attribute and any noteworthy information needed when assigning values to the attribute.

The mandatory attributes that are mapped by default are noted.

<b>Select Identity Resource Attribute</b>	<b>Domino User Attribute</b>	<b>Label on Domino UI</b>	<b>Description</b>
UserId	UserId	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)	
MiddleInitial	MiddleInitial	Middle initial (on the Basics tab)	
LastName	LastName	Last name (on the Basics tab)	

<b>Select Identity Resource Attribute</b>	<b>Domino User Attribute</b>	<b>Label on Domino UI</b>	<b>Description</b>
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)	
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)	



<b>Select Identity Resource Attribute</b>	<b>Domino User Attribute</b>	<b>Label on Domino UI</b>	<b>Description</b>
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)	
(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)	

<b>Select Identity Resource Attribute</b>	<b>Domino User Attribute</b>	<b>Label on Domino UI</b>	<b>Description</b>
(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)	

<b>Select Identity Resource Attribute</b>	<b>Domino User Attribute</b>	<b>Label on Domino UI</b>	<b>Description</b>
(not mapped by default)	OfficeStreet Address	Street address (in Company Information on the Work tab)	
(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)	

<b>Select Identity Resource Attribute</b>	<b>Domino User Attribute</b>	<b>Label on Domino UI</b>	<b>Description</b>
(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)	
(not mapped by default)	Owner	Owners (on the Administration tab)	
(not mapped by default)	AltFullName	Alternate FullName (on the Administration tab)	

<b>Select Identity Resource Attribute</b>	<b>Domino User Attribute</b>	<b>Label on Domino UI</b>	<b>Description</b>
(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)	

<b>Select Identity Resource Attribute</b>	<b>Domino User Attribute</b>	<b>Label on Domino UI</b>	<b>Description</b>
(not mapped by default)	Profiles	Setup profile(s) (on the Administration tab)	
(not mapped by default)	AvailableForDirSync	Foreign directory synch allowed (on the Administration tab)	
(not mapped by default)	NetUserName	Network account name (on the Administration tab)	
(not mapped by default)	ProposedAltCommonName	Proposed alternate common name (on the Administration tab)	
(not mapped by default)	ProposedAltOrgUnit	Proposed alternate unique organizational unit (on the Administration tab)	

<b>Select Identity Resource Attribute</b>	<b>Domino User Attribute</b>	<b>Label on Domino UI</b>	<b>Description</b>
(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)	

## 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.



Note that 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>

```

# Configuring the Connector

After you deploy the connector on the application server, you must configure Select Identity to use the connector by deploying it in the Select Identity client. The following provides an overview of the procedures you must complete in order to deploy your connector. It also provides connector-specific information you must provide when configuring Select Identity to use the connector.

## Internationalization Support

If you installed the connector on non-English platforms, familiarize yourself with the information in this section before deploying and configuring the connector. Internationalization support provided by the connector includes the following capabilities and limitations:

- When entering user attributes to provision (in the Select Identity client), you can enter local language characters except for the following attributes:
  - UserName
  - Password
  - Email

The following shows Chinese characters used in attribute values:

用户属性	
FirstName	中文
UserName	OraEvf003
Password	***** [No expiration ]
GUID	E19A27C5-C66E-4F60-11DD-363488491677
Email	yilei.zhang@hp.com
Business Phone	null
Home Phone	null
Address 1	地址1
Country	中国ABC
Gen_Ora_118N_KEY	OraEvf003

- Reverse synchronization of local language characters is supported. When provisioning users on the LDAP resource, you can enter local language characters as input data. These characters are reconciled with Select Identity through SPML communication. However, the following user attributes must contain English characters:
  - UserName
  - Password
  - Email
- The attribute names on the resource cannot contain non-English characters. Thus, you cannot include non-English characters in the mapping file. The following shows attributes contained in a mapping file; only English attribute names are shown.

Resource Name=Gen_Ora_118N				
<< < 页 1 / 1 > >>				总记录数: 10
Name	Min Length	Max Length	Attribute Mapped To	Authoritative
Address	0	255	Addr1	N
Country	0	255	Country	N
E-Mail	0	255	Email	N
FirstName	0	255	FirstName	N
Gen_Ora_118N_ENTITLEMENTS	1	255	Gen_Ora_118N_ENTITLEMENTS	Y
Gen_Ora_118N_KEY	1	255	Gen_Ora_118N_KEY	Y
Password	0	255	Password	N
PhOffice	0	255	PhBus	N
UserName	0	255	UserName	N
phHome	0	255	PhHome	N

- Non-English entitlements are not supported by the connector.

- All configuration and property file names must be in English.
- The exception messages from the resource are in English only.
- The log messages are in English only.
- The Select Identity resource name, which is included in the reverse synchronization configuration of the agent, must be in English.

## Connector Deployment

Complete the following steps to deploy and configure the connector:

- 1 Register the connector with Select Identity by clicking the **Deploy New Connector** button on the Connectors home page. Complete this procedure as described in the “Connectors” chapter of the *HP OpenView Select Identity Administrator Guide*.

After you deploy the connector, the connector properties will look similar to this:

[Home](#) > [Connectors](#) > [View Connector : DominoConnector](#)

Connector Information	
* Connector Name:	DominoConnector
* Pool Name:	eis/DominoConnector

- 2 Deploy a resource that uses the newly created connector. On the Resources home page, click the **Deploy New Resource** button. When configuring the resource, refer to the following table for parameters specific to this connector:

Field Name	Sample Values	Description
Resource Name	Domino_server	Name given to the resource.
Resource Type	Domino	The connector that was deployed in <a href="#">Step 1</a> .

Field Name	Sample Values	Description
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 <b>No</b> 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.
Server Name	PSO111	The NETBIOS name or IP address 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.
Notes Base Dir	<i>On Windows:</i> C:\Lotus\Notes\Data <i>On UNIX:</i> /usr/local/notesdata	The Notes data directory. User ID files are created here.
Domino Certifier ID File	<i>On Windows:</i> C:\Lotus\Domino\data\cert.id <i>On UNIX:</i> /usr/local/notesdata/cert.id	The Certifier ID that is used to provision users. Note that Domino servers support hierarchical Certifiers.

Field Name	Sample Values	Description
Domino Certifier ID Password	Certpassword	The password corresponding to the specified Certifier.
Address Book DB File	names.nsf	The Domino Address Book on which all operations are to be performed.

Complete the steps in this procedure as described in the “Resources” chapter of the *HP OpenView Select Identity Administrator Guide*. After you deploy the resource for the connector, the Basic Info page of the resource properties will look similar to this:

Resource Information	
* Resource Name:	Domino651w
Resource Description:	<pre> domino resource on windows 6.5.1 t1nt2 </pre>
* Resource Type:	DominoConnector
* Authoritative Source:	Yes
* Delete User:	Yes
Reconciliation Workflow:	ReconciliationDefaultProcess
Resource Owner:	sis
* Resource Id:	1414

The Additional Info page will look similar to this:

Resource Information	
Resource Name:	Domino651w
<input checked="" type="checkbox"/> Manage User	
Associate to Group:	<input checked="" type="checkbox"/>

The Access Info page will look similar to this:

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

- 3** Create attributes that link Select Identity to the connector. For each mapping in the connector's mapping file, create an attribute using the Attributes capability on the Select Identity client. Refer to the "Attributes" chapter in the *HP OpenView Select Identity Administrator*

*Guide* for more information. After you create the attributes for the connector, the View Attributes page for the resource will look similar to this:

(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

- 4 Create a Service that will use the newly created resource. To do so, click the **Deploy New Service** button on the Services home page. Complete this procedure as described in “Services” of the *HP OpenView Select Identity Administrator Guide*. You will reference your new resource created in **Step 2** while creating this service.

If you are enabling reverse synchronization, configure the Service as follows:

- When selecting the Business Relationship, choose the **ReconciliationDefaultProcess** workflow for the **RECONCILIATION:Add Service** and **RECONCILIATION:Delete Service Membership** request events. For **RECONCILIATION:Add Service**, use the user addition view.



- In the user addition view, specify mandatory attributes that are guaranteed to be passed by the reverse synchronization request when adding a user. If you specify a mandatory attribute that is not passed by the resource, the user will be created in Select Identity but reverse synchronization will not succeed.
- When specifying the context, obtain the value from the add request issued by the resource. For example, if the context is Country and the value is US, the <addRequest> element in the reverse synchronization request should have an attribute called country and a value of US. If the context attribute is not present in the add user request, the user will be created in Select Identity but will not be assigned to a Service.

## Uninstalling the Connector

If you need to uninstall a connector from Select Identity, make sure that the following are performed:

- All resource dependencies are removed.
- The connector is deleted through the Connectors home page on the Select Identity client.

## Uninstalling the Connector from WebLogic

Perform the following to delete the Domino connector from the Select Identity server:

- 1 Log on to the WebLogic Server Console.
- 2 Navigate to *My\_Domain* → **Deployments** → **Connector Modules**.
- 3 Click the delete icon next to the connector that you want to uninstall.
- 4 Click **Yes** to confirm the deletion.
- 5 Click **Continue**.

# Uninstalling the Domino Agent

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

- 1 Delete the home directory of the agent.
- 2 Delete the `opAttributes.properties` and `Properties.ini` files from `C:/Lotus/Domino`.
- 3 Remove the `Forms5.nsf` or `Forms6.nsf` file that was copied during installation.
- 4 Delete the password synchronization agent that was created in Domino Designer.