

Oracle® Fusion Middleware

Installation and Configuration Guide for Identity Synchronization
for Windows 6.0

11g Release 1 (11.1.1.7.0)

E28963-01

January 2013

Covers installation and configuration information for Oracle
Identity Synchronization for Windows.

Oracle Fusion Middleware Installation and Configuration Guide for Identity Synchronization for Windows
6.0, 11g Release 1 (11.1.1.7.0)

E28963-01

Copyright © 2001, 2013, Oracle and/or its affiliates. All rights reserved.

Primary Author: Gina Cariaga

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

Contents

1 Understanding the Product

1.1	Product Features	1-2
1.2	System Components	1-3
1.2.1	Watchdog Process.....	1-4
1.2.2	Core.....	1-4
1.2.3	Connectors	1-6
1.2.4	Connector Subcomponents	1-6
1.2.5	Message Queue	1-7
1.3	System Components Distribution	1-8
1.3.1	Core.....	1-8
1.3.2	Directory Server Connector and Plug-in.....	1-8
1.3.3	Active Directory Connector	1-9
1.3.4	Windows NT Connector and Subcomponents.....	1-10
1.4	How Identity Synchronization for Windows Detects Changes in Directory Sources...	1-10
1.4.1	How Directory Server Connectors Detect Changes	1-11
1.4.2	How Active Directory Connectors Detect Changes	1-11
1.4.3	How Windows NT Connectors Detect Changes.....	1-12
1.4.4	Propagating Password Updates	1-13
1.4.5	Reliable Synchronization	1-15
1.5	Deployment Example: A Two-Machine Configuration	1-16
1.5.1	Physical Deployment	1-17
1.5.2	Component Distribution.....	1-18

2 Preparing for Installation

2.1	Installation Overview	2-1
2.1.1	Installing Core	2-3
2.1.2	Configuring the Product.....	2-3
2.1.3	Preparing the Directory Server	2-3
2.1.4	Installing Connectors and Configuring Directory Server Plug-In	2-4
2.1.5	Synchronizing Existing Users	2-4
2.2	Configuration Overview	2-5
2.2.1	Directories	2-5
2.2.2	Synchronization Settings	2-5
2.2.3	Object Classes.....	2-6
2.2.4	Attributes and Attribute Mapping.....	2-6

2.2.5	Synchronization User Lists.....	2-7
2.3	Synchronizing Passwords With Active Directory.....	2-8
2.3.1	Enforcing Password Policies	2-9
2.4	Configuring Windows for SSL Operation.....	2-13
2.5	Installation and Configuration Decisions.....	2-14
2.5.1	Core Installation.....	2-14
2.5.2	Core Configuration.....	2-14
2.5.3	Connector Installation and Configuring the Directory Server Plug-In	2-15
2.5.4	Using the Command-Line Utilities	2-15
2.6	Installation Checklists	2-16

3 Installing Core

3.1	Before You Begin.....	3-1
3.2	Starting the Installation Program	3-2
3.2.1	On Solaris SPARC.....	3-2
3.2.2	On Solaris x86.....	3-2
3.2.3	On Windows.....	3-2
3.2.4	On Red Hat Linux.....	3-3
3.3	Installing Core	3-3
3.3.1	To Install Identity Synchronization for Windows Core Components Using the Installation Wizard	3-4

4 Configuring Core Resources

4.1	Configuration Overview	4-1
4.2	Opening the Identity Synchronization for Windows Console.....	4-2
4.2.1	To Open Identity Synchronization for Windows Console	4-3
4.3	Creating Directory Sources.....	4-6
4.3.1	To Create Directory Sources.....	4-6
4.3.2	Creating a Sun Java System Directory Source	4-6
4.3.3	Preparing Sun Directory Source	4-12
4.3.4	Creating an Active Directory Source	4-15
4.3.5	Creating a Windows NT SAM Directory Source	4-22
4.4	Selecting and Mapping User Attributes	4-24
4.4.1	Selecting and Mapping Attributes	4-24
4.4.2	Creating Parameterized Default Attribute Values.....	4-27
4.4.3	Changing the Schema Source.....	4-27
4.5	Propagating User Attributes Between Systems.....	4-29
4.5.1	Specifying How Object Creations Flow.....	4-30
4.5.2	Specifying How Object Modifications Flow	4-34
4.5.3	Specifying Configuration Settings for Group Synchronization	4-42
4.5.4	Configuring and Synchronizing Account Lockout and Unlockout	4-44
4.5.5	Specifying How Deletions Flow	4-46
4.6	Creating Synchronization User Lists.....	4-47
4.6.1	To Identify and Link User Types Between Servers	4-48
4.7	Saving a Configuration	4-52
4.7.1	To Save your Current Configuration from the Console Panels	4-52

5 Installing Connectors

5.1	Before You Begin.....	5-1
5.2	Running the Installation Program.....	5-2
5.2.1	To Restart and Run the Installation Program.....	5-2
5.3	Installing Connectors.....	5-3
5.3.1	Installing the Directory Server Connector.....	5-3
5.3.2	Installing an Active Directory Connector.....	5-9
5.3.3	Installing the Windows NT Connector.....	5-12

6 Synchronizing Existing Users and User Groups

6.1	Post-Installation Steps Based on Existing User and Group Populations.....	6-2
6.2	Using idsync resync.....	6-2
6.2.1	Resynchronizing Users or Groups.....	6-2
6.2.2	Linking Users.....	6-3
6.2.3	idsync resync Options.....	6-4
6.3	Checking Results in the Central Log.....	6-6
6.4	Starting and Stopping Synchronization.....	6-6
6.4.1	To Start or Stop Synchronization.....	6-6
6.5	Resynchronized Users/Groups.....	6-7
6.6	Starting and Stopping Services.....	6-7

7 Removing the Software

7.1	Planning for Uninstallation.....	7-1
7.2	Uninstalling the Software.....	7-2
7.2.1	Uninstalling Connectors.....	7-2
7.2.2	To Uninstall Core.....	7-3
7.3	Uninstalling the Console Manually.....	7-4
7.3.1	From Solaris or Linux Systems.....	7-4
7.3.2	From Windows Systems.....	7-5

8 Configuring Security

8.1	Security Overview.....	8-1
8.1.1	Specifying a Configuration Password.....	8-2
8.1.2	Using SSL.....	8-2
8.1.3	Requiring Trusted SSL Certificates.....	8-2
8.1.4	Generated 3DES Keys.....	8-3
8.1.5	SSL and 3DES Keys Protection Summary.....	8-3
8.1.6	Message Queue Access Controls.....	8-4
8.1.7	Directory Credentials.....	8-5
8.1.8	Persistent Storage Protection Summary.....	8-5
8.2	Hardening Your Security.....	8-6
8.2.1	Configuration Password.....	8-6
8.2.2	Creating Configuration Directory Credentials.....	8-6
8.2.3	Message Queue Client Certificate Validation.....	8-7
8.2.4	Message Queue Self-Signed SSL Certificate.....	8-7

8.2.5	Access to the Message Queue Broker	8-7
8.2.6	Configuration Directory Certificate Validation	8-7
8.2.7	Restricting Access to the Configuration Directory	8-7
8.3	Securing Replicated Configurations	8-8
8.4	Using idsync certinfo.....	8-10
8.4.1	Arguments	8-10
8.4.2	Usage	8-10
8.5	Enabling SSL in Directory Server	8-11
8.5.1	To Enable SSL in Directory Server	8-11
8.5.2	Retrieving the CA Certificate from the Directory Server Certificate Database	8-12
8.5.3	Retrieving the CA Certificate from the Directory Server (using dsadm command on Solaris platform) 8-12	
8.6	Enabling SSL in the Active Directory Connector	8-13
8.6.1	Retrieving an Active Directory Certificate.....	8-13
8.6.2	Adding Active Directory Certificates to the Connector's Certificate Database.....	8-14
8.7	Adding Active Directory Certificates to Directory Server.....	8-15
8.7.1	To Add the Active Directory CA certificate to the Directory Server Certificate Database 8-15	
8.8	Adding Directory Server Certificates to the Directory Server Connector	8-16
8.8.1	To Add the Directory Server Certificates to the Directory Server Connector	8-16

9 Understanding Audit and Error Files

9.1	Understanding the Logs.....	9-1
9.1.1	Log Types.....	9-2
9.1.2	Reading the Logs	9-4
9.2	Configuring Your Log Files.....	9-5
9.2.1	To Configure Logging for Your Deployment.....	9-5
9.3	Viewing Directory Source Status.....	9-7
9.3.1	To View the Status of your Directory Sources.....	9-7
9.4	Viewing Installation and Configuration Status.....	9-8
9.4.1	To View the Remaining Steps of the Installation and Configuration Process.....	9-8
9.5	Viewing Audit and Error Logs	9-9
9.5.1	To View Your Error Logs.....	9-9
9.6	Enabling Auditing on a Windows NT Machine.....	9-10
9.6.1	To Enable Audit Logging on Your Windows NT Machine.....	9-10

A Using the Identity Synchronization for Windows Command Line Utilities

A.1	Common Features.....	A-1
A.1.1	Common Arguments to the Idsync Subcommands.....	A-1
A.1.2	Entering Passwords.....	A-3
A.1.3	Getting Help	A-3
A.2	Using the idsync command	A-4
A.2.1	Using certinfo	A-5
A.2.2	Using changepw	A-6
A.2.3	Using importcnf	A-7
A.2.4	Using prepds	A-7
A.2.5	Using printstat.....	A-10

A.2.6	Using resetconn.....	A-11
A.2.7	Using resync	A-11
A.2.8	Using groupsync.....	A-13
A.2.9	Using accountlockout.....	A-14
A.2.10	Using dspluginconfig.....	A-14
A.2.11	Using startsync.....	A-15
A.2.12	Using stopsync	A-15
A.3	Using the forcepwchg Migration Utility	A-16
A.3.1	To Execute the forcepwchg Command line Utility.....	A-16
B	Identity Synchronization for Windows LinkUsers XML Document Sample	
B.1	Sample 1: linkusers-simple.cfg.....	B-1
B.2	Sample 2: linkusers.cfg.....	B-2
C	Running Identity Synchronization for Windows Services as Non-Root on Solaris	
C.1	Running Services as a Non-root User	C-1
C.1.1	To Run services as a Non-root User.....	C-1
D	Defining and Configuring Synchronization User Lists for Identity Synchronization for Windows	
D.1	Understanding Synchronization User List Definitions.....	D-1
D.2	Configuring Multiple Windows Domains	D-3
D.2.1	To Configure Multiple Windows Domains	D-3
E	Identity Synchronization for Windows Installation Notes for Replicated Environments	
E.1	Configuring Replication.....	E-1
E.1.1	To Configure any Replication Topology	E-2
E.2	Configuring Replication Over SSL	E-2
E.2.1	To Configure Directory Servers Involved in Replication so that all Replication Operations Occur Over an SSL Connection	E-2
E.3	Configuring Identity Synchronization for Windows in an MMR Environment.....	E-3
E.3.1	To Configure Identity Synchronization for Windows in an MMR Environment.....	E-3

Preface

This guide covers installation and configuration information for Oracle Identity Synchronization for Windows.

Who Should Use This Book

If you are installing Directory Server Enterprise Edition software for evaluation purposes only, put this guide aside for now, and see *Evaluation Guide for Oracle Directory Server Enterprise Edition*.

This Installation Guide is for administrators deploying Directory Server Enterprise Edition, Directory Service Control Center, and Identity Synchronization for Windows software. This document also covers configuration of Identity Synchronization for Windows.

Before You Read This Book

Review pertinent information in the *Release Notes for Oracle Directory Server Enterprise Edition*.

If you are deploying Directory Server Enterprise Edition software in production, also review pertinent information in the *Deployment Planning Guide for Oracle Directory Server Enterprise Edition*.

Readers installing Identity Synchronization for Windows should be familiar with the following technologies:

- Directory Server
- Microsoft Active Directory or Windows NT authentication
- Lightweight Directory Access Protocol (LDAP)
- Java technology
- Extensible Markup Language (XML)
- Public-key cryptography and Secure Sockets Layer (SSL) protocol
- Intranet, extranet, and Internet security
- The role of digital certificates in an enterprise

Examples Used in This Guide

For consistency, the same example data is used throughout this guide. Replace these values with the appropriate values for your system.

Variable	Values used in examples
Suffix (SUFFIX_DN)	dc=example,dc=com
Instance path (INSTANCE_PATH)	For Directory Server: /local/dsInst/ For Directory Proxy Server: /local/dps/
Hostnames (HOST)	host1,host2,host3
Port (PORT)	LDAP: Default for root: 389. Default for non-root: 1389 SSL default: Default for root: 636. Default for non-root: 1636

Oracle Directory Server Enterprise Edition Documentation Set

This documentation set explains how to use Oracle Directory Server Enterprise Edition to evaluate, design, deploy, and administer directory services. In addition, it shows how to develop client applications for Directory Server Enterprise Edition. The Oracle Fusion Middleware Directory Server Enterprise Edition Documentation Library is available at http://docs.oracle.com/cd/E29127_01/index.htm.

The following table lists the documents that make up the Directory Server Enterprise Edition documentation set.

Document Title	Contents
<i>Release Notes for Oracle Directory Server Enterprise Edition</i>	Contains the latest information about Directory Server Enterprise Edition, including known problems.
<i>Evaluation Guide for Oracle Directory Server Enterprise Edition</i>	Introduces the key features of this release. Demonstrates how these features work and what they offer in the context of a deployment that you can implement on a single system.
<i>Deployment Planning Guide for Oracle Directory Server Enterprise Edition</i>	Explains how to plan and design highly available, highly scalable directory services based on Directory Server Enterprise Edition. Presents the basic concepts and principles of deployment planning and design. Discusses the solution life cycle, and provides high-level examples and strategies to use when planning solutions based on Directory Server Enterprise Edition.
<i>Installation Guide for Oracle Directory Server Enterprise Edition</i>	Explains how to install the Directory Server Enterprise Edition software. Shows how to configure the installed software and verify the configured software.
<i>Upgrade and Migration Guide for Oracle Directory Server Enterprise Edition</i>	Provides instructions for upgrading versions 11.1.1.3, 7.x, and 6 installations, and instructions for migrating version 5.2 installations.
<i>Administrator's Guide for Oracle Directory Server Enterprise Edition</i>	Provides command-line instructions for administering Directory Server Enterprise Edition. For hints and instructions about using the Directory Service Control Center, DSCC, to administer Directory Server Enterprise Edition, see the online help provided in DSCC.

Document Title	Contents
<i>Reference for Oracle Directory Server Enterprise Edition</i>	Introduces technical and conceptual foundations of Directory Server Enterprise Edition. Describes its components, architecture, processes, and features.
<i>Man Page Reference for Oracle Directory Server Enterprise Edition</i>	Describes the command-line tools, schema objects, and other public interfaces that are available through Directory Server Enterprise Edition. Individual sections of this document can be installed as online manual pages.
<i>Developer's Guide for Oracle Directory Server Enterprise Edition</i>	Shows how to develop directory client applications with the tools and APIs that are provided as part of Directory Server Enterprise Edition.
<i>Troubleshooting for Oracle Directory Server Enterprise Edition Guide</i>	Provides information for defining the scope of the problem, gathering data, and troubleshooting the problem areas by using various tools.
<i>Release Notes for Identity Synchronization for Windows 6.0</i>	Provides the latest information for installing, migrating, and upgrading Identity Synchronization for Windows 6.0 SP1.
<i>Deployment Planning Guide for Identity Synchronization for Windows 6.0</i>	Provides general guidelines and best practices for planning and deploying Identity Synchronization for Windows.
<i>Installation and Configuration Guide for Identity Synchronization for Windows 6.0</i>	Describes how to install and configure Identity Synchronization for Windows.

Related Reading

The SLAMD Distributed Load Generation Engine is a Java application that is designed to stress test and analyze the performance of network-based applications. This application was originally developed by Sun Microsystems, Inc. to benchmark and analyze the performance of LDAP directory servers. SLAMD is available as an open source application under the Sun Public License, an OSI-approved open source license. To obtain information about SLAMD, go to <http://www.slamd.com/>. SLAMD is also available as a java.net project. See <https://slamd.dev.java.net/>.

Java Naming and Directory Interface (JNDI) supports accessing the Directory Server using LDAP and DSML v2 from Java applications. For information about JNDI, see <http://www.oracle.com/technetwork/java/jndi/index.html>. The *JNDI Tutorial* contains detailed descriptions and examples of how to use JNDI. This tutorial is at <http://download.oracle.com/javase/jndi/tutorial/>.

Identity Synchronization for Windows uses Message Queue with a restricted license. Message Queue documentation is available at <http://www.oracle.com/technetwork/indexes/documentation/index.html>.

Identity Synchronization for Windows works with Microsoft Windows password policies.

- Information about password policies for Windows 2003, is available in the Microsoft documentation (<http://technet.microsoft.com/en-us/windowsserver/default.aspx>) online.

- Information about the Microsoft Certificate Services Enterprise Root certificate authority, is available in the Microsoft support documentation (<http://support.microsoft.com/default.aspx?scid=kb;en-us;247078>) online.
- Information about configuring LDAP over SSL on Microsoft systems, is available in the Microsoft support documentation (<http://support.microsoft.com/default.aspx?scid=kb;en-us;321051>) online.

Redistributable Files

Directory Server Enterprise Edition does not provide any files that you can redistribute.

Default Paths and Command Locations

This section explains the default paths used in documentation, and provides locations of commands on different operating systems and deployment types.

Default Paths

The table in this section describes the default paths that are used in this document. For complete descriptions of the files installed, see Chapter 1, *Directory Server Enterprise Edition File Reference*, in *Reference for Oracle Directory Server Enterprise Edition*.

Placeholder	Description	Default Value
<i>install-path</i>	Represents the base installation directory for Directory Server Enterprise Edition software.	When you install from a zip distribution using unzip, the <i>install-path</i> is the <i>current-directory/dsee7</i> .
<i>instance-path</i>	Represents the full path to an instance of Directory Server or Directory Proxy Server. Documentation uses <i>/local/dsInst/</i> for Directory Server and <i>/local/dps/</i> for Directory Proxy Server.	No default path exists. Instance paths must nevertheless always be found on a <i>local</i> file system. On Solaris systems, the <i>/var</i> directory is recommended:
<i>serverroot</i>	Represents the parent directory of the Identity Synchronization for Windows installation location	Depends on your installation. Note that the concept of a <i>serverroot</i> no longer exists for Directory Server and Directory Proxy Server.
<i>isw-hostname</i>	Represents the Identity Synchronization for Windows instance directory	Depends on your installation
<i>/path/to/cert8.db</i>	Represents the default path and file name of the client's certificate database for Identity Synchronization for Windows	<i>current-working-dir/cert8.db</i>
<i>serverroot/isw-hostname/linebreaklogs/</i>	Represents the default path to the Identity Synchronization for Windows local log files for the System Manager, each connector, and the Central Logger	Depends on your installation
<i>serverroot/isw-hostname/linebreaklogs/central/</i>	Represents the default path to the Identity Synchronization for Windows central log files	Depends on your installation

Command Locations

The table in this section provides locations for commands that are used in Directory Server Enterprise Edition documentation. To learn more about each of the commands, see the relevant man pages. See also "Software Layout for Directory Server Enterprise Edition" in the *Reference for Oracle Directory Server Enterprise Edition*.

Command	Zip Distribution
certutil	<i>install-path/bin/certutil</i>
dpadm	<i>install-path/bin/dpadm</i>
dpconf	<i>install-path/bin/dpconf</i>
dsadm	<i>install-path/bin/dsadm</i>
dscagent	<i>install-path/bin/agent</i>
dscmon	<i>install-path/bin/dscmon</i>
dscreg	<i>install-path/bin/dscreg</i>
dscsetup	<i>install-path/bin/dscsetup</i>
dsconf	<i>install-path/bin/dsconf</i>
dsmig	<i>install-path/bin/dsmig</i>
dsutil	<i>install-path/bin/dsutil</i>
entrycmp	<i>install-path/bin/entrycmp</i>
fildif	<i>install-path/bin/fildif</i>
idsktune	At the root of the unzipped zip distribution
insync	<i>install-path/bin/insync</i>
ldapmodify	<i>install-path/dsrk/bin/ldapmodify</i>
ldapsearch	<i>install-path/dsrk/bin/ldapsearch</i>
repldisc	<i>install-path/bin/repldisc</i>

Typographic Conventions

The following table describes the typographic conventions that are used in this book.

Typeface	Meaning	Example
AaBbCc123	The names of commands, files, and directories, and onscreen computer output	Edit your <code>.login</code> file. Use <code>ls a</code> to list all files. <code>machine_name% you have mail.</code>
AaBbCc123	What you type, contrasted with onscreen computer output	<code>machine_name% su</code> Password:
<i>aabbcc123</i>	Placeholder: replace with a real name or value	The command to remove a file is <code>rm filename</code> .

Typeface	Meaning	Example
<i>AaBbCc123</i>	Book titles, new terms, and terms to be emphasized	Read Chapter 6 in the <i>User's Guide</i> . A <i>cache</i> is a copy that is stored locally. Do <i>not</i> save the file. Note: Some emphasized items appear bold online.

Shell Prompts in Command Examples

The following table shows the default UNIX system prompt and superuser prompt for shells that are included in the Oracle Solaris OS. Note that the default system prompt that is displayed in command examples varies, depending on the Oracle Solaris release.

Shell	Prompt
Bash shell, Korn shell, and Bourne shell	\$
Bash shell, Korn shell, and Bourne shell for superuser	#
C shell	machine_name%
C shell for superuser	machine_name#

Symbol Conventions

The following table explains symbols that might be used in this book.

Symbol	Description	Example	Meaning
[]	Contains optional arguments and command options.	ls [-l]	The -l option is not required.
{ }	Contains a set of choices for a required command option.	-d {y n}	The -d option requires that you use either the y argument or the n argument.
\${ }	Indicates a variable reference.	\${com.sun.javaRoot}	References the value of the com.sun.javaRoot variable.
-	Joins simultaneous multiple keystrokes.	Control-A	Press the Control key while you press the A key.
+	Joins consecutive multiple keystrokes.	Ctrl+A+N	Press the Control key, release it, and then press the subsequent keys.
>	Indicates menu item selection in a graphical user interface.	File > New > Templates	From the File menu, choose New. From the New submenu, choose Templates.

Documentation, Support, and Training

See the following web sites for additional resources:

- Documentation (<http://www.oracle.com/technetwork/indexes/documentation/index.html>)
- Support (<http://www.oracle.com/us/support/systems/index.html>)
- Training (<http://education.oracle.com>)

Oracle Software Resources

Oracle Technology Network

(<http://www.oracle.com/technetwork/index.html>) offers a range of resources related to Oracle software:

- Discuss technical problems and solutions on the ODSEE Discussion Forum (<http://forums.oracle.com/forums/forum.jspa?forumID=877>) and the Directory Services blog (<http://blogs.oracle.com/directoryservices/>).
- See the latest announcements on the Directory Services blog (<http://blogs.oracle.com/directoryservices/>).
- Download ODSEE 11g Example Files (<http://www.oracle.com/technetwork/middleware/id-mgmt/learnmore/odsee11113-examples-350399.zip>).

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit

<http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> or visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> if you are hearing impaired.

Part I

Installing

Sun Java System Identity Synchronization for Windows allows passwords and other specified user attributes to flow between Sun Java System Directory Server and other systems.

This part of the guide explains how to install and configure Identity Synchronization for Windows for use in a production environment.

For the latest information about new features and about enhancements in this release of Identity Synchronization for Windows, see the *Release Notes for Oracle Directory Server Enterprise Edition*.

Note: User interfaces that are depicted in this document are subject to change in future versions of the product.

This part includes the following chapters:

- [Chapter 1, "Understanding the Product"](#) describes Identity Synchronization for Windows product features, system components and their distribution, command-line utilities, and deployment examples.
- [Chapter 2, "Preparing for Installation"](#) describes the installation and configuration processes and information you need to know when preparing to install the product.
- [Chapter 3, "Installing Core"](#) explains how to use the Identity Synchronization for Windows installation program and how to install its Core component.
- [Chapter 4, "Configuring Core Resources"](#) explains how to add and configure Core resources by using the Console.
- [Chapter 5, "Installing Connectors"](#) provides instructions for installing the Identity Synchronization for Windows Connectors and Directory Server Plug-ins.
- [Chapter 6, "Synchronizing Existing Users and User Groups"](#) explains how to link and resynchronize existing users and user groups for new Identity Synchronization for Windows installations.
- [Chapter 7, "Removing the Software"](#) explains how to remove Identity Synchronization for Windows, including how to prepare for the uninstallation and how to uninstall the Console manually.
- [Chapter 8, "Configuring Security"](#) describes how to configure a secure system. This chapter covers how to harden security, secure replicated configurations, enable SSL, and add Active Directory CA certificates to certificate databases.

- [Chapter 9, "Understanding Audit and Error Files"](#) provides information about audit and error logging, including instructions on how to set logging levels, how to view and understand your log files, and directory source status.
- [Appendix A, "Using the Identity Synchronization for Windows Command Line Utilities"](#) shows how to use command-line utilities to perform various tasks.
- [Appendix B, "Identity Synchronization for Windows LinkUsers XML Document Sample"](#) provides sample `Linkusers` XML configuration files that you can use to customize your deployment.
- [Appendix C, "Running Identity Synchronization for Windows Services as Non-Root on Solaris"](#) explains how to run Identity Synchronization for Windows services as a `non-root` user on the Solaris operating system.
- [Appendix D, "Defining and Configuring Synchronization User Lists for Identity Synchronization for Windows"](#) provides information about Synchronization User List definitions and multiple domain configurations.
- [Appendix E, "Identity Synchronization for Windows Installation Notes for Replicated Environments"](#) provides an overview of the steps required to configure and secure a multimaster replication deployment.

Understanding the Product

Oracle Identity Synchronization for Windows 6.0 SP1 provides bidirectional password and user attributes synchronization between Sun Java System Directory Server and the following:

- Windows 2000 or Windows 2003 Server Active Directory
- Windows NT SAM Registry

Identity Synchronization for Windows 6.0 SP1 supports Sun Directory Server 7.0, 6.3, 6.2, 6.1, 6.0, and 5.2 Patch 5.

Oracle Identity Synchronization for Windows handles synchronization events in these ways:

- **Securely.** It does not send passwords "in the clear," and it restricts system access to administrators only.
- **Robustly.** It keeps directories synchronized, even when individual components are temporarily unavailable.
- **Efficiently.** It uses synchronization methods that place very little load on your directory servers.

Note: Before you install Sun Java System Identity Synchronization for Windows version 6.0 SP1, you *must* read the *Release Notes for Identity Synchronization for Windows 6.0 Service Pack 1*. This Technical Note provides additional installation instructions that help you to install Identity Synchronization for Windows for Directory Server Enterprise Edition 7.0.

Sun Java System Identity Synchronization for Windows version 6.0 SP1 is not bundled with the Sun Directory Server Enterprise Edition 7.0 release. You can download the Identity Synchronization for Windows software from http://www.sun.com/software/products/directory_srvr_ee/get.jsp.

You should also familiarize yourself with the concepts described in this chapter, which includes the following topics:

- [Product Features](#)
- [System Components](#)
- [System Components Distribution](#)

- [How Identity Synchronization for Windows Detects Changes in Directory Sources](#)
- [Deployment Example: A Two-Machine Configuration](#)

1.1 Product Features

Oracle Identity Synchronization for Windows provides the following features and functionality:

- **Bidirectional password synchronization.** Enables you to synchronize user passwords between the following directory sources:
 - Sun Java System Directory Server and Windows Active Directory
 - Sun Java System Directory Server and Windows NT

Synchronizing passwords allows users to access applications using these directory sources for login authentication, so users only have to remember a single password. In addition, when users have to apply periodic password updates, they only have to update their password in one location.

- **Bidirectional user attributes synchronization.** Enables you to create, modify, and delete selected attributes in one directory environment and propagate the values automatically to the other directory environment.
- **Bidirectional user account creation synchronization.** Enables you to create or delete a user account in one directory environment and automatically propagate the new account to the other directory environment.
- **Bidirectional group synchronization.** Enables you to synchronize the creation or deletion of a group, and association or disassociation of users with that group between Directory Server and Active Directory sources.
- **Bidirectional object deletions, activations, and inactivations.** Enable you to control the flow of object deletions, activations, and inactivations between Directory Server and Active Directory sources.
- **Bidirectional account lockout and unlockout synchronization.** Enables you to synchronize account lockout and unlockout between Directory Server and Active Directory sources.
- **Synchronization with multiple domains.** Enables you to synchronize with multiple Active Directory and Windows NT domains, and with multiple Active Directory forests.
- **Centralized system auditing.** Enables you to monitor from a single-centralized location, installation and configuration status, the day-to-day system operations, and any error conditions related to your deployment.

You are not required to modify entries in Windows directories or to change the applications using the directories.

If you are using Identity Synchronization for Windows to synchronize between Directory Server and Active Directory, you do not need to install any components in the Windows operating system.

If you are synchronizing between Directory Server and Windows NT, you must install the product's NT component in the Windows NT operating system.

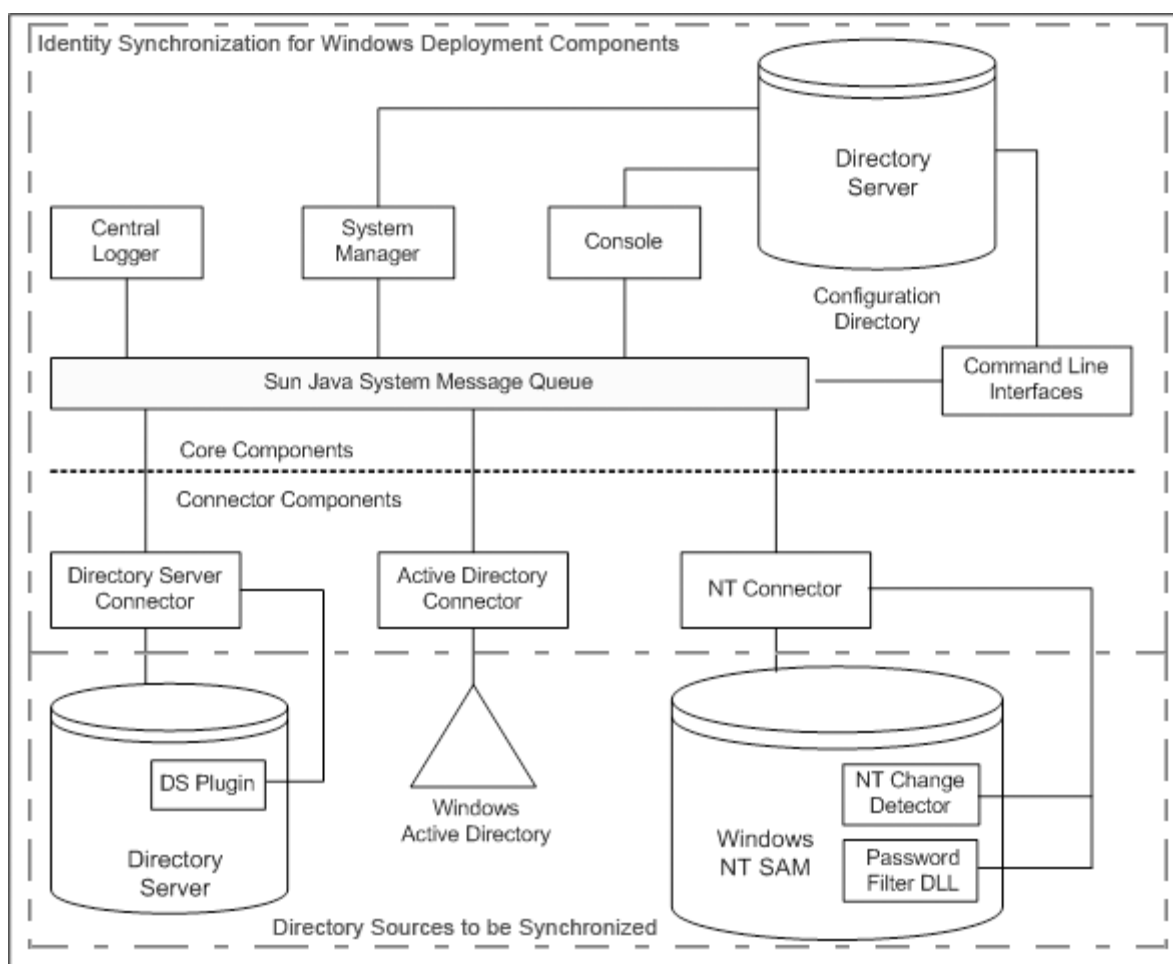
Note: The following features are not available for Windows NT:

- Bidirectional group synchronization
 - Bidirectional object deletions, activations, and inactivations
 - Bidirectional account lockout and unlockout synchronization
-

1.2 System Components

The following figure shows that Identity Synchronization for Windows consists of a set of Core components and any number of individual connectors and connector subcomponents. These system components allow for the synchronization of password and user attribute updates between Sun Java System Directory Server (Directory Server) and Windows directories.

Figure 1-1 System Components



This section defines and describes these Identity Synchronization for Windows components:

- [Watchdog Process](#)
- [Core](#)

- [Connectors](#)
- [Connector Subcomponents](#)
- [Message Queue](#)

1.2.1 Watchdog Process

The *Watchdog* is an Identity Synchronization for Windows Java technology-based process (Java process) that starts, restarts, and stops individual background Java processes. The Watchdog launches and monitors the central logger, system manager, and connectors. The Watchdog does not monitor subcomponents, Message Queue, or the Identity Synchronization for Windows Console.

The Watchdog is installed where you install the Core components and it can be started as a Solaris software daemon, Red Hat Linux daemon, or a Windows service.

1.2.2 Core

When you install Identity Synchronization for Windows, you install the *Core* component first, then configure it to match your environment.

The Core component consists of the following components:

- [Configuration Directory](#)
- [Console](#)
- [Command-Line Utilities](#)
- [System Manager](#)
- [Central Logger](#)

1.2.2.1 Configuration Directory

Identity Synchronization for Windows *stores* its configuration data in a Directory Server configuration directory. The program does not install a configuration directory.

The Console, system manager, command-line utilities, and the installer all read and write the product's configuration data to and from the configuration directory, including the following:

- Installation information about each component's health
- Configuration information for every directory, domain, connector, and Directory Server Plug-in
- Connector status
- Synchronization settings that describe the direction of user or group creations, deletions, and attribute modifications
- Attributes to be synchronized and attribute mappings between Active Directory and Directory Server or Windows NT and Directory Server
- Synchronization User Lists (SULs) in each directory topology
- Log settings

1.2.2.2 Console

Identity Synchronization for Windows provides a Console that centralizes all of the product's component configuration and administration tasks.

You can use the Console to do the following:

- Configure directory sources to be synchronized
- Define mappings for user entry attributes to be synchronized, in addition to passwords
- Specify which users and attributes within a directory or domain topology will or will not be synchronized
- Monitor system status
- Start and stop synchronization

1.2.2.3 Command-Line Utilities

Identity Synchronization for Windows also provides command-line utilities that enable you to perform the following tasks directly from the command line:

- Display certificate information based on your configuration and Secure Sockets Layer (SSL) settings
- Change the Identity Synchronization for Windows configuration password
- Configure the Directory Server Plug-in for a specified Directory Server source
- Prepare a Sun Java System Directory Server source for use by Identity Synchronization for Windows
- Display the steps that you must perform to complete the installation or configuration process, and view the status of installed connectors, the system manager, and Message Queue
- Reset connector states in the configuration directory to *uninstalled*
- Synchronize and link existing users in two directories, and pre-populate directories as part of the installation process
- Enable or disable account lockout
- Enable or disable group synchronization
- Start and stop synchronization

For a detailed description of the product's command-line utilities and how to use them, see [Appendix A, "Using the Identity Synchronization for Windows Command Line Utilities"](#).

1.2.2.4 System Manager

The Identity Synchronization for Windows system manager is a separate Java process that does the following:

- Leverages the product's back-end networked facilities to dynamically deliver configuration updates to connectors
- Keeps the status of each connector and all connector subcomponents
- Coordinates `idsync` `resync` operations that are used to initially synchronize two directories

1.2.2.5 Central Logger

Connectors may be installed so that they are widely distributed across remote geographical locations. Therefore, having all logging information centralized is of great administrative value. This centralization allows the administrator to monitor

synchronization activity, detect errors, and evaluate the health of the entire system from a single location.

Administrators can use the central logger logs to perform these tasks:

- Verify that the system is running correctly
- Detect and resolve individual component and system-wide problems
- Audit individual and system-wide synchronization activity
- Track a user's password synchronization between directory sources

The two types of logs are as follows:

- **Audit log.** Provides information about the system's day-to-day activities, which includes events such as a user's password being synchronized between directories. You can control the level of information that is logged in the audit log by increasing or decreasing the detail provided in the log messages.
- **Error log.** Provides information about conditions that are qualified as severe errors and warnings. All error log entries are worthy of attention, so you cannot prevent errors from being logged. If an error condition takes place, it will always be documented in the error log.

Note: Identity Synchronization for Windows also writes all error log messages to the audit log to facilitate correlation with other events.

1.2.3 Connectors

A *connector* is a Java process that manages the synchronization process in a single data source type. A connector detects user changes in the data source and publishes these changes to remote connectors over Message Queue.

Identity Synchronization for Windows provides the following directory-specific connectors. These connectors bidirectionally synchronize user attributes and password updates between directories and domains.

- **Directory Server Connector.** Supports a single root suffix (for example, suffix/database) in a Directory Server.
- **Active Directory Connector.** Supports a single instance in a Windows 2000 or Windows 2003 Server Active Directory source. You can use multiple connectors for additional domains.
- **Windows NT Connector.** Supports a single domain on Windows NT.

Note: The Watchdog is installed where you install a connector, and it starts, restarts, and stops the connectors. For more information, see [Watchdog Process](#).

1.2.4 Connector Subcomponents

A *subcomponent* is a lightweight process or library that runs separately from the connector. Connectors use subcomponents to access native resources that cannot be accessed remotely, such as capturing passwords inside Directory Server or Windows NT.

The following connector subcomponents are configured or installed with the directory being synchronized and communicate with the corresponding connector over an encrypted connection.

- [Directory Server Plug-In](#)
- [Windows NT Connector Subcomponents](#)

Note: Active Directory Connectors do not require subcomponents.

1.2.4.1 Directory Server Plug-In

The Directory Server Plug-in is a subcomponent of the Directory Server Connector. You configure the Directory Server Plug-in on each Directory Server being synchronized.

This Plug-in does the following:

- Enhances the Directory Server Connector's change-detection features by storing encrypted passwords in the retro changelog
- Provides bidirectional support for user attribute and password synchronization between Active Directory and Directory Server (see [Using On-Demand Password Synchronization to Obtain Clear-Text Passwords](#))

Note: Identity Synchronization for Windows used to support only two-way multimaster replication (MMR). Now, the Directory Server Plug-in is also functional in *N*-way MMR environments.

1.2.4.2 Windows NT Connector Subcomponents

If your installation requires synchronization with Windows NT SAM Registries, the Identity Synchronization for Windows installation program installs the following in the Primary Domain Controller (PDC) along with the Windows NT Connector:

- **Change Detector.** Detects user entry and password change events by monitoring the Security Log, then passes the changes to the Connector
- **Password Filter DLL.** Captures password changes made on the Windows NT Domain Controller and passes these securely to the NT Connector.

1.2.5 Message Queue

Identity Synchronization for Windows uses Oracle Message Queue (Message Queue), a persistent message queue mechanism with a publish and subscribe model, to propagate attribute and password changes between directory sources. Message Queue also distributes administrative and configuration information to the connectors managing synchronization for those directory sources.

Message Queue is an enterprise messaging system that implements the Java Message Service open standard. This specification describes a set of programming interfaces that provide a common way for Java applications to create, send, receive, and read messages in a distributed environment.

Message Queue consists of message publishers and subscribers that exchange messages using a common message service. This service is composed of one or more dedicated message brokers that control access to the message queue, maintain information about active publishers and subscribers, and ensure that messages are delivered.

Message Queue does the following:

- Establishes a system of trust between connectors
- Simplifies security access controls for all components
- Facilitates end-to-end encryption of passwords
- Ensures that all password update messages are delivered
- Reduces connector-to-connector communication complexity and security risks
- Enables a central authority to distribute configuration information
- Allows for the aggregation of all connector logs in a central location

1.3 System Components Distribution

Before you can develop an effective deployment, you must understand how Identity Synchronization for Windows components are organized and how the product operates. This section discusses the following:

- [Core](#)
- [Directory Server Connector and Plug-in](#)
- [Active Directory Connector](#)
- [Windows NT Connector and Subcomponents](#)

When you understand the basic concepts described in this section and in [Deployment Example: A Two-Machine Configuration](#), you should be able to extrapolate the information to create deployment strategies for more complex, sophisticated scenarios. Such scenarios might be mixed Active Directory and Windows NT environments or multiserver environments.

1.3.1 Core

Note: Install Oracle Message Queue 3.6 Enterprise Edition on the same machine where you are planning to install Core.

Install all Core components only once in any of the supported operating system's directory servers. Identity Synchronization for Windows installs Administration Server on your machine if it is not already installed.

1.3.2 Directory Server Connector and Plug-in

You can install Directory Server Connectors on any of the supported operating systems. You are not required to install a Directory Server Connector on the same machine where the Directory Server that is being synchronized is running. However, one Directory Server Connector must be installed for each configured Directory Server source.

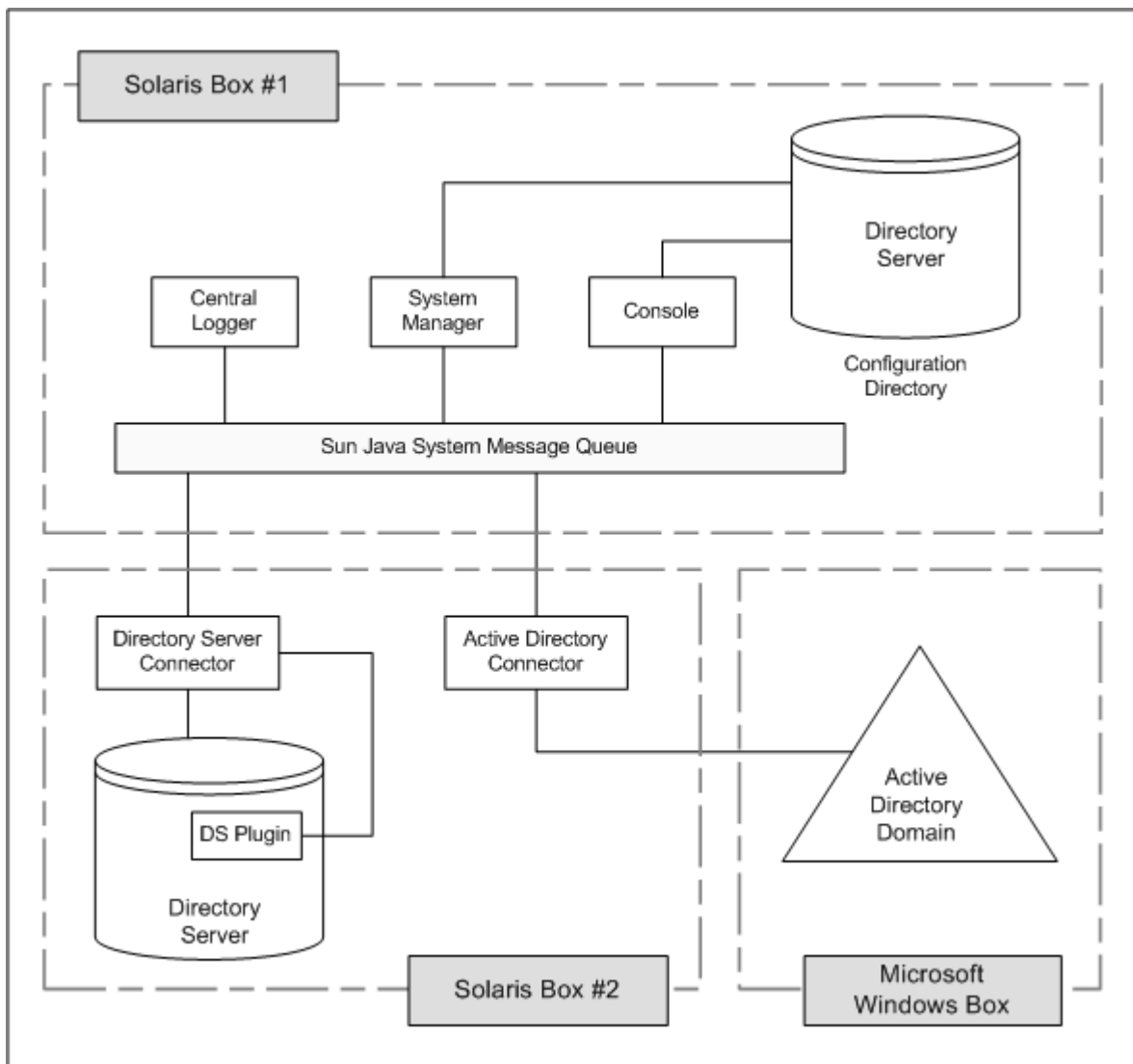
You must configure the Directory Server Plug-in on every host where a Directory Server that is to be synchronized resides.

Note: A single Directory Server Connector is installed for each Directory Server source. However, Directory Server Plug-ins should be configured for each master, hub, and consumer replica to be synchronized.

1.3.3 Active Directory Connector

You can install Active Directory Connectors on any of the supported operating systems. You are not required to install an Active Directory Connector on a machine running Windows. However, one Active Directory Connector must be installed for each Active Directory domain. See the following figure for a sample distribution of components.

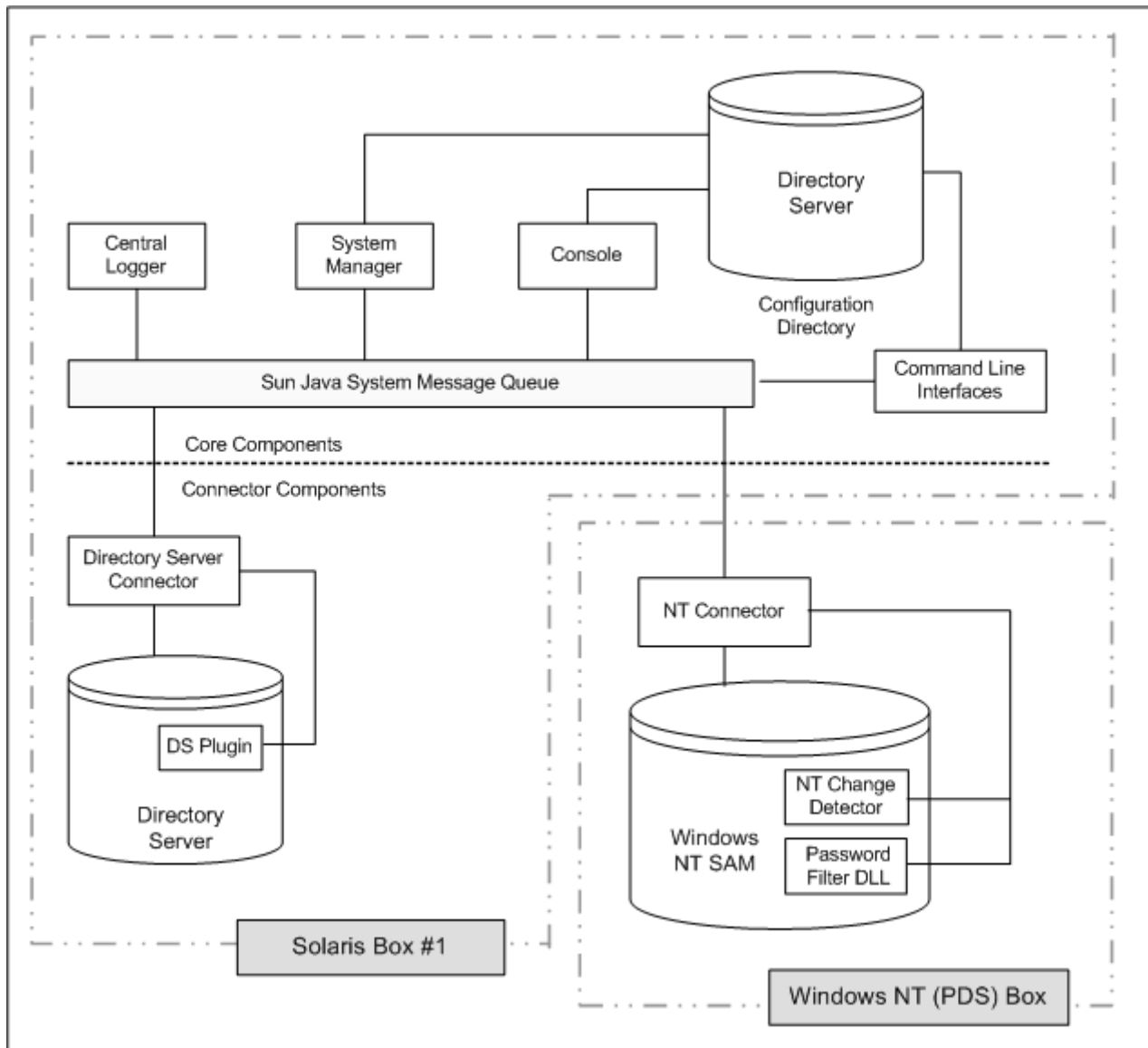
Figure 1-2 Directory Server and Active Directory Component Distribution



1.3.4 Windows NT Connector and Subcomponents

To synchronize with Windows NT SAM Registries, you must install the Windows NT Connector in the Primary Domain Controller (PDC). The installation program also installs the two NT Connector subcomponents, the Change Detector and the Password Filter DLL, along with the Connector in the PDC of the NT domain. A single NT Connector synchronizes users and passwords for a single NT domain. See the following figure for a sample distribution of components.

Figure 1-3 Directory Server and Windows NT Component Distribution



1.4 How Identity Synchronization for Windows Detects Changes in Directory Sources

This section explains how user entry and password changes are detected by Sun Java System Directory Server (Directory Server), Windows Active Directory, and Windows NT Connectors.

The information is organized as follows:

- [How Directory Server Connectors Detect Changes](#)
- [How Active Directory Connectors Detect Changes](#)
- [How Windows NT Connectors Detect Changes](#)
- [Propagating Password Updates](#)
- [Reliable Synchronization](#)

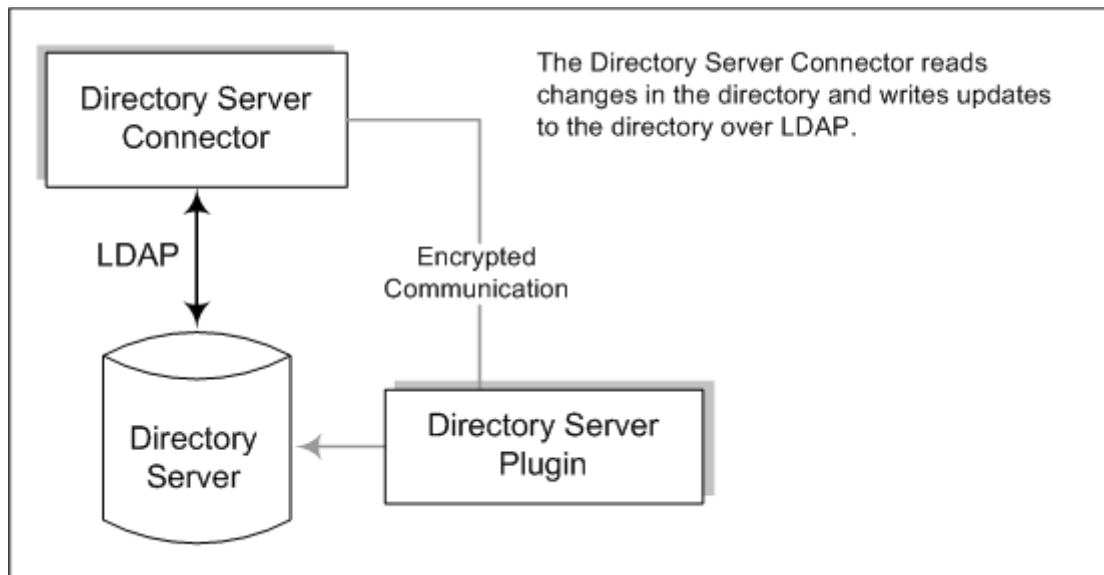
1.4.1 How Directory Server Connectors Detect Changes

The Directory Server Connector examines the Directory Server retro changelog over LDAP to detect user entry and password change events. The Directory Server Plug-in helps the Connector do the following:

For more information about retro changelog, see *Replication and the Retro Change Log Plug-In in Reference for Oracle Directory Server Enterprise Edition*.

- Capture clear-text passwords by encrypting them and then making them available in the retro changelog. Without the Plug-in, only hashed passwords appear in the retro changelog, and hashed passwords cannot be synchronized.
- Perform on-demand password synchronization with Active Directory. No Identity Synchronization for Windows components need to be installed in a Windows topology (See [Using On-Demand Password Synchronization to Obtain Clear-Text Passwords](#)).

Figure 1-4 How Directory Server Connectors Detect Changes



1.4.2 How Active Directory Connectors Detect Changes

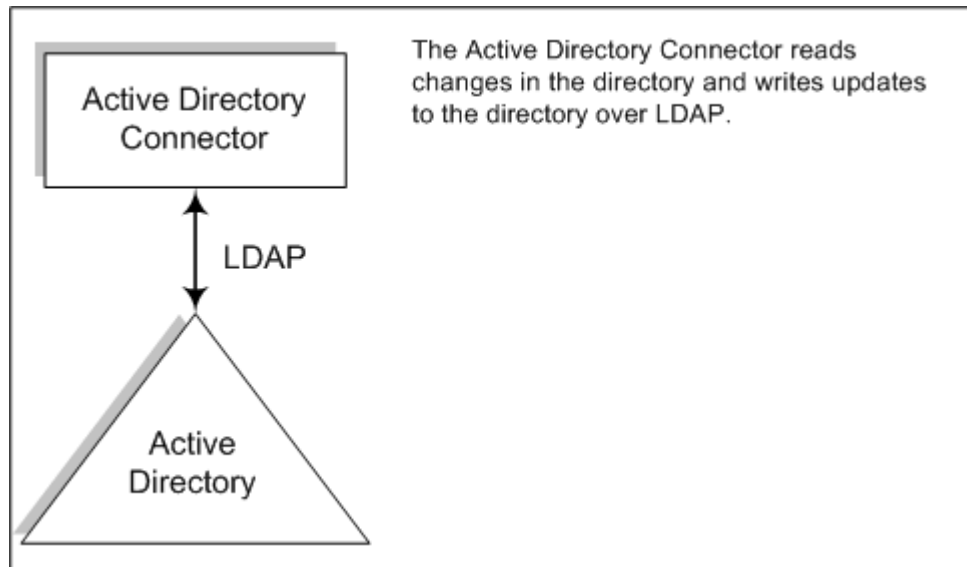
The Windows 2000/2003 Server Active Directory Connector detects user entry and password changes by examining the Active Directory `USNChanged` and `PwdLastSet` attribute values.

Unlike the Directory Server's retro changelog, when you change attributes in an entry, Active Directory does not report which attributes changed. Instead, Active Directory

identifies entry changes by incrementing the `USNchanged` attribute. To detect changes to individual attributes, an Active Directory Connector uses an in-process database called the *object cache*. The object cache stores a hashed copy of each Active Directory entry, which allows the Connector to determine exactly which attributes were modified in the entry.

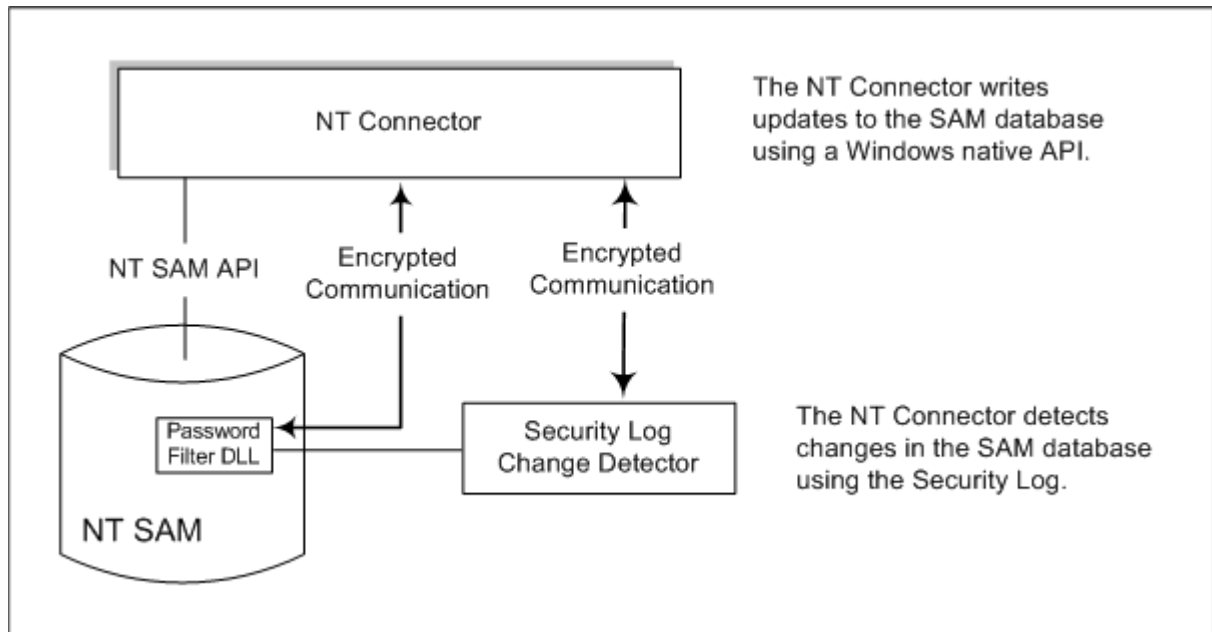
You are not required to install Active Directory Connectors on Windows. These connectors can also run on other operating systems such as Solaris or Red Hat Linux, and detect or make changes remotely over LDAP.

Figure 1-5 How Active Directory Connectors Detect Changes



1.4.3 How Windows NT Connectors Detect Changes

The Windows NT Connector detects user entry and password changes by examining the Security Log for audit events about user objects. Auditing must be enabled or Identity Synchronization for Windows cannot read log messages from Windows NT machine. To verify that audit logging is enabled, see [Enabling Auditing on a Windows NT Machine](#).

Figure 1-6 How Windows NT Connectors Detect Changes

For a description of the Change Detector and the Password Filter DLL subcomponents, see [Windows NT Connector Subcomponents](#).

1.4.4 Propagating Password Updates

This section explains two ways to obtain clear-text passwords. Clear-text passwords are needed to propagate password changes between Windows and Directory Server sources.

1.4.4.1 Using the Password Filter DLL to Obtain Clear-Text Passwords

Windows NT Connectors must obtain clear-text passwords to propagate password updates to the Sun Java System Directory Server. However, you cannot extract clear-text passwords from a Windows directory. By the time passwords are stored in the directories, the passwords have already been encrypted.

Windows NT provides a Password Filter DLL interface that allows components to capture clear-text passwords before they are stored in a directory permanently.

1.4.4.2 Using On-Demand Password Synchronization to Obtain Clear-Text Passwords

While Active Directory supports the same password filter as Windows NT, you must install the Password Filter DLL on every domain controller (not the Primary Domain Controller used by Windows NT). Because this can be a significant installation burden, Identity Synchronization for Windows uses a different approach, called *on-demand password synchronization*, to synchronize password changes from Active Directory to Directory Server.

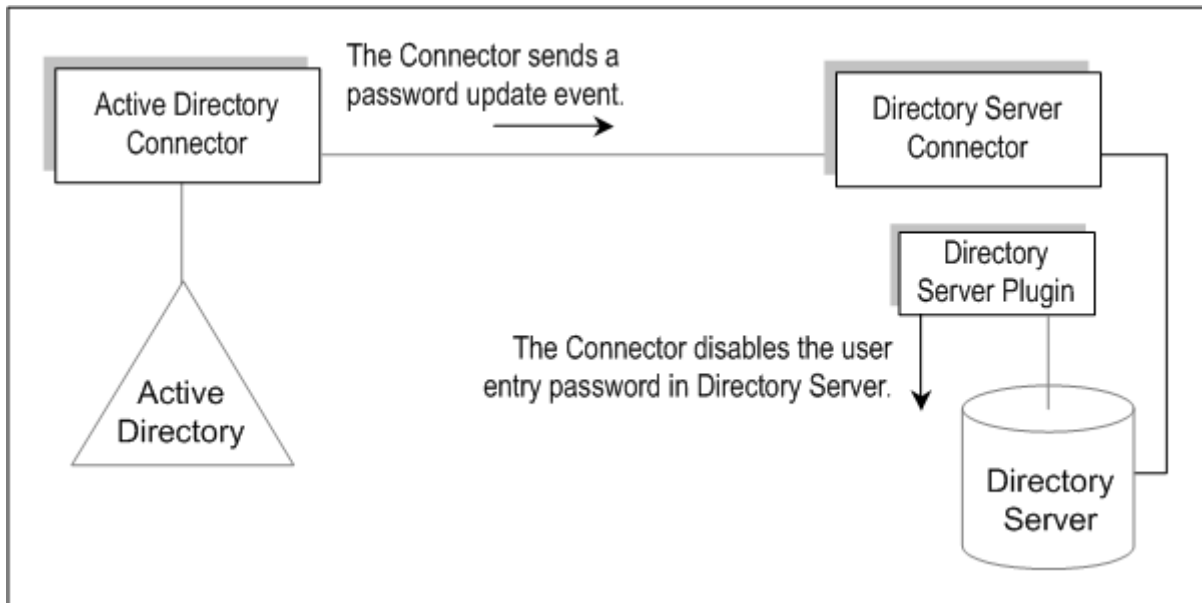
On-demand password synchronization provides a method to obtain new password values on Directory Server when users try to login after their password change on Windows 2000/2003.

On-demand password synchronization also allows you to synchronize passwords on Active Directory without using the Password Filter DLL.

The on-demand password synchronization process is as follows:

1. The user presses Ctrl-Alt-Del on a machine running Windows and changes his or her password. The new passwords are stored in Active Directory.
2. The Active Directory Connector polls the system at scheduled intervals.

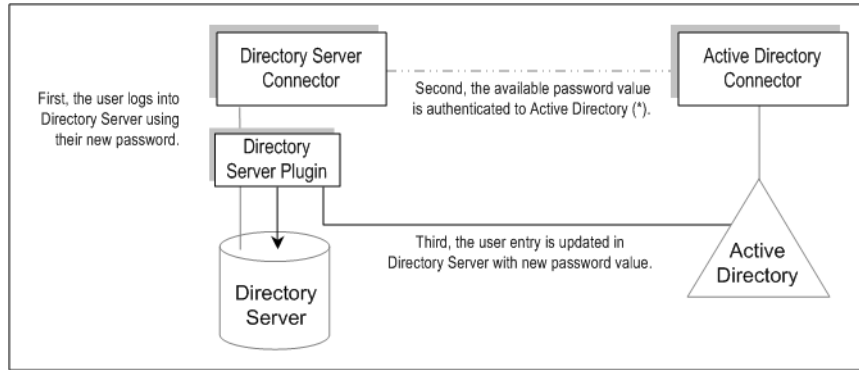
When the Connector detects the password change, based on changes made to the `USNchanged` (Update Sequence Number) and `PwdLastSet` attributes, the Connector publishes a message on Message Queue about the password change. The message is transferred on an SSL-encrypted channel.



3. The Directory Server Connector receives the password change message from Message Queue (over SSL).
4. The Directory Server Connector sets the user entry's `dspswvalidate` attribute to `true`, which invalidates the old password and alerts the Directory Server Plug-in of the password change.
5. When the user tries to log in, using an LDAP application (such as Portal Server) to authenticate against the Directory Server, the Sun Java System Directory Server Plug-in detects that the password value in the Directory Server entry is invalid.
6. The Directory Server Plug-in searches for the corresponding user in Active Directory. When the Plug-in finds the user, the Plug-in tries to bind to Active Directory using the password provided when the user tried logging in to Directory Server.

Note: On-demand password synchronization requires that the application use simple authentication against Directory Server instead of using a more complex authentication mechanism, such as SASL Digest-MD5.

7. If the bind against Active Directory succeeds, the Directory Server Plug-in sets the password and removes the invalid password flag from the user entry on Directory Server allowing the user to log in.



Note: If user authentication fails, the user entry password remains in Directory Server and the passwords on Directory Server and Active Directory are not the same until the user logs in with a valid password, one that authenticates to Active Directory.

1.4.5 Reliable Synchronization

Identity Synchronization for Windows takes many precautions to ensure that you do not lose user change events, even when components become temporarily unavailable. Identity Synchronization for Windows' reliability is similar to the TCP network protocol. TCP guarantees that even over a loosely and intermittently connected network, it will eventually deliver all data in order. Data sent during a temporary network outage is queued while the network is down and re-delivered after connectivity is restored. Identity Synchronization for Windows will eventually detect and apply user change events if one of the following components becomes temporarily unavailable:

- Connector
- Directory Server
- Message Queue
- Active Directory domain controller
- Windows NT Primary Domain Controller
- System manager
- Configuration directory

If one of these components is not available, Identity Synchronization for Windows will delay synchronization until the affected component is available and contains all changes, even to passwords. This version of Identity Synchronization for Windows does not support Sun Cluster software or other true high-availability solutions. Because users do not interact with Identity Synchronization for Windows directly, high availability is not usually required. If you experience a catastrophic failure, you can reinstall Identity Synchronization for Windows components and use the `idsync resync` command to resynchronize all directory sources.

In most situations, when a component is unavailable, the program queues synchronization events and applies them only when the component becomes available. There are two exceptions to this process:

- In a multimaster replication (MMR) Directory Server environment, external changes to Windows users can be synchronized to the preferred or secondary Directory Servers.

If the preferred Directory Server is unavailable, the Directory Server Connector will apply changes to one of the available secondary servers from the MMR topology.

- While the Active Directory Connector can communicate with a single Active Directory domain controller only, the Directory Server Plug-in can fail between all Active Directory domain controllers while performing on-demand password synchronization. This point is where failover is most important. If the Directory Server Plug-in cannot contact an Active Directory domain controller to verify a user's new password, the user cannot log in to Directory Server.

1.5 Deployment Example: A Two-Machine Configuration

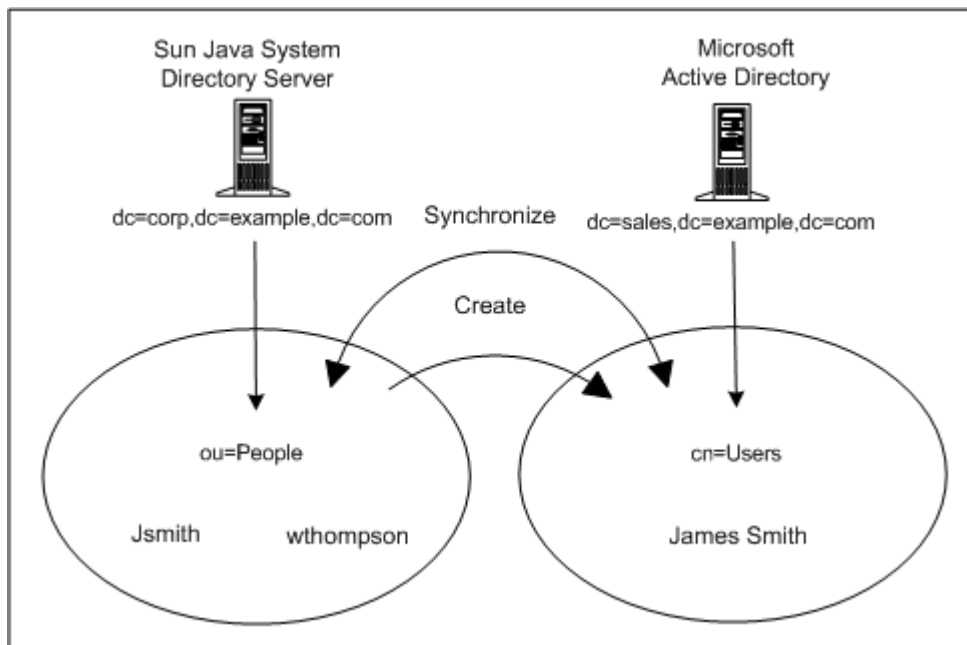
This section describes a deployment scenario in which Identity Synchronization for Windows is used to synchronize user object creation and bidirectional password modification operations between Directory Server and Active Directory sources.

The deployment scenario consists of two machines:

- A machine running a Sun Java System Directory Server (host name: corp.example.com)
- A machine running Active Directory on a Windows 2000 Server (host name: sales.example.com)

Note: Even though Windows NT is not used in this scenario, Identity Synchronization for Windows also supports synchronization with NT domains.

The following figure illustrates the synchronization requirements (node structures with associated attribute values) used for this deployment scenario.



The two goals for this scenario are as follows:

- To synchronize user passwords bidirectionally between the *user subtrees* (*ou=people* in Directory Server and *cn=users* in Active Directory), which means that whenever a user password changes in either directory, the password change is synchronized to the associated user in the other directory.

For example, if you change the password for *uid=Jsmith* in the *ou=people* container in the Directory Server, the new password should automatically be synchronized to *cn=James Smith* in the *cn=users* container in Active Directory.

- To synchronize user object creation operations from the Directory Server *people* subtree to the Active Directory *user* subtree only.

For example, if you create a new user *uid=WThompson* in the *ou=People* container with a specified set of attributes, Identity Synchronization for Windows will create a new account *cn=William Thompson* in the *cn=Users* container with the same set of attributes in Active Directory.

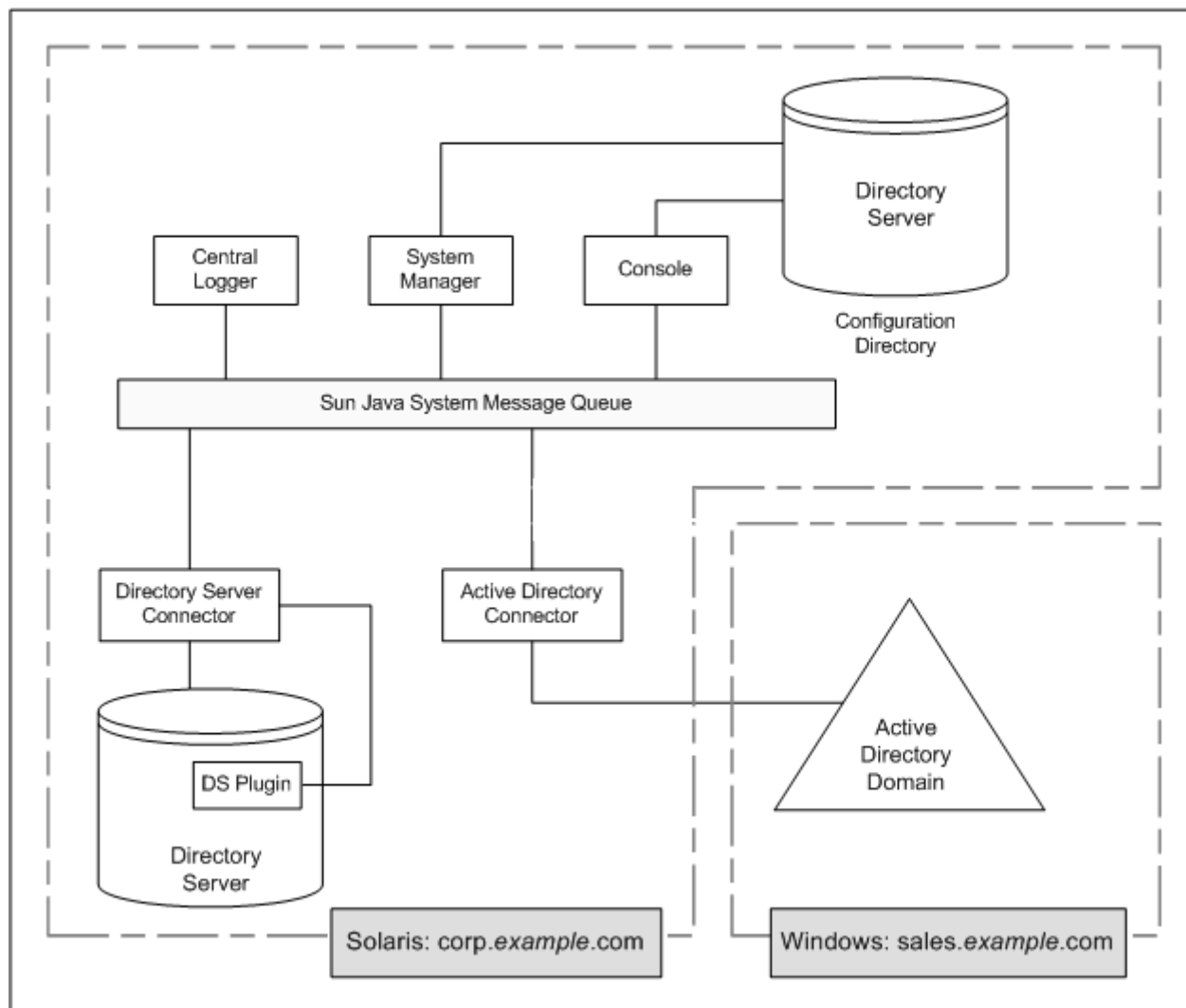
Note: Identity Synchronization for Windows supports multiple synchronization sources of the same type. For example, you can have more than one Directory Server in a deployment or multiple Active Directory domains.

Creation, modification, and deletion synchronization settings are global for the entire set of directories, and cannot be specified for individual directory sources. If you synchronize user object creations from Directory Server to Active Directory, user object creations will propagate from *all* Directory Servers to *all* Active Directory domains and Windows NT domains configured in the installation.

1.5.1 Physical Deployment

The following figure illustrates how all the product's components are physically deployed on a single Solaris system, while the Active Directory domain resides in a separate Active Directory domain controller where no components have been installed.

Figure 1-7 Directory Server and Active Directory Scenario



1.5.2 Component Distribution

`corp.example.com` is a machine where Directory Server is installed on a Solaris operating system. The root suffix for the Directory Server instance being synchronized is `dc=corp,dc=example,dc=com`.

This topology contains the following:

- Identity Synchronization for Windows Core components
- Identity Synchronization for Windows Directory Server Connector
- Identity Synchronization for Windows Directory Server Plug-in
- Identity Synchronization for Windows configuration directory (located in a different Directory Server instance than the one being synchronized)

`sales.example.com` is the Active Directory domain being synchronized.

Preparing for Installation

Before installing Identity Synchronization for Windows 6.0 SP1 or before migrating from Sun Java System Identity Synchronization for Windows 1 2004Q3 SP1 to version 6.0 SP1, familiarize yourself with the installation and configuration process.

For information about the Identity Synchronization for Windows installation requirements, see *Release Notes for Identity Synchronization for Windows 6.0 Service Pack 1*.

Identity Synchronization for Windows can also be installed in French, German, Spanish, Japanese, Korean, Simplified Chinese, and Traditional Chinese languages. All the languages are bundled in the same distribution.

For multilingual support for Identity Synchronization for Windows, use the UTF-8 encoding.

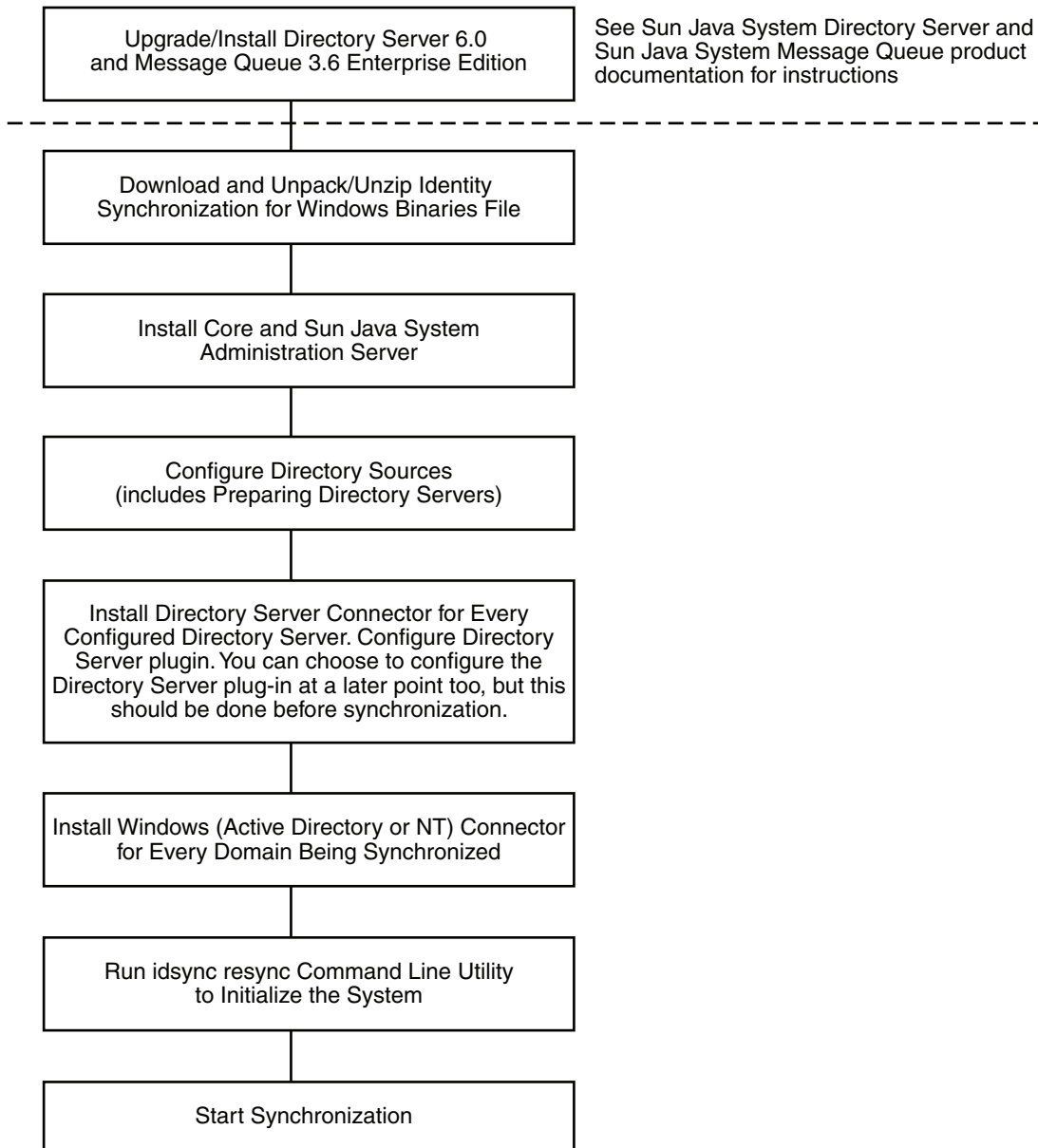
This chapter covers the following topics:

- [Installation Overview](#)
- [Configuration Overview](#)
- [Synchronizing Passwords With Active Directory](#)
- [Configuring Windows for SSL Operation](#)
- [Installation and Configuration Decisions](#)
- [Installation Checklists](#)

2.1 Installation Overview

This section illustrates a single-host installation procedure for Identity Synchronization for Windows.

Figure 2-1 Single-host installation procedure



Some components must be installed in a particular order, so be sure to read all installation instructions carefully.

Identity Synchronization for Windows provides a "To Do" list, which is displayed throughout the installation and configuration process. This information panel lists all of the steps that you must follow to successfully install and configure the product.

Figure 2-2 To Do List for Identity Synchronization for Windows Installation and Configuration

This is a list of remaining installation and configuration steps:

- ✓ **1** : Install the Identity Synchronization core components.
- 2** : Create an initial configuration using the product's console or by migrating from a previous installation using 'idsync importcnf'.
- 3** : Prepare every Sun Directory Server included in this configuration by using the console or the 'idsync prepsds' command.
- 4** : Install connectors for every configured directory source.
- 5** : After installing each Sun Directory Server connector, configure the Sun Directory Server plugin on every master and on every read-only replica by using the console or the "idsync dspluginconfig" command.
- 6** : Run 'idsync resync' to establish links between existing Directory Server and Windows users.
- 7** : Start synchronization using the console or the 'idsync startsync' command.

As you go through the installation and configuration process, all completed steps in the list are grayed-out as shown in Figure 6-2.

The rest of this section provides an overview of the installation and configuration process.

2.1.1 Installing Core

When you install Core, you will be installing the following components:

- **Sun Java System Administration Server.** Configures the Directory Server Plug-in and provides the administration framework.
- **Console.** Provides a centralized location for performing all of the product's component configuration and administration tasks.
- **Central logger.** Centralizes all audit and error logging information in a central location.
- **System manager.** Delivers configuration updates to connectors dynamically and maintains the status of each connector.
- Instructions for installing Core are provided in [Chapter 3, "Installing Core"](#)

2.1.2 Configuring the Product

After installing Core, use Console to initially configure the directory sources to be synchronized and other characteristics of the deployment, all from a centralized location.

Instructions for configuring directory resources are provided in [Chapter 4, "Configuring Core Resources"](#).

2.1.3 Preparing the Directory Server

Before you can install Directory Server Connectors, you must prepare a Sun Java System Directory Server source for every preferred and secondary Directory Server that is being synchronized.

You can perform this task from the Console, or from the command line by using the `idsync prepds` subcommand.

Instructions for preparing Directory Server are provided in [Preparing Sun Directory Source](#).

2.1.4 Installing Connectors and Configuring Directory Server Plug-In

You can install any number of connectors depending on the number of configured directories in your topology. Both the Console and the installation program use the directory label to associate a connector with the directory that is synchronized. The following table describes the label naming conventions.

Table 2-1 Label Naming Conventions

Connector Type	Directory Source Label	Subcomponent
Directory Server Connector	root suffix or suffix/database	Directory Server Plug-in Configure one Plug-in in every Directory Server (master or consumer) for the root suffix being synchronized.
AD Connector	Domain name	None
NT Connector	Domain name	(Automatically installed with the Windows NT Connector) Change Detector and Password Filter DLL subcomponents are installed together in the same installation. You must install the Windows NT Connector using the graphical user interface (GUI) installer.

Table 2-2 Label Naming Examples

Connector Name	Directory Source
CNN100	SunDS1 on ou=isw_data1
CNN101	AD1
CNN102	SunDS1 on ou-isw_data2
CNN103	SunDS2

Instructions for installing and configuring Connectors are provided in [Chapter 3, "Installing Core"](#)

2.1.5 Synchronizing Existing Users

After installing the connectors, plug-ins, and subcomponents, you must run the `idsync resync` command-line utility to bootstrap deployments with existing users. This command uses administrator-specified matching rules to do the following:

- Link existing entries (for more information about *linking users*, see [Linking Users](#))
- Populate an empty directory with the contents of a remote directory
- Bulk-synchronize attribute values (including passwords) between two existing user populations, where entries in both the Windows and Directory Server directories are uniquely identified and linked to each other

Instructions for synchronizing existing users in your deployment are provided in [Chapter 6, "Synchronizing Existing Users and User Groups"](#).

2.2 Configuration Overview

After installing the product, you must configure the product deployment, which includes doing the following:

- Configuring the directories and global catalogs to be synchronized
- Specifying synchronization settings for attribute modifications and object activations/inactivations
- Specifying settings for group synchronization
- Specifying settings for account lockout and unlockout synchronization
- (optional) Specifying synchronization settings for user entry creations and deletions between the configured directories

This section provides an overview of the following configuration element concepts:

- Directories
- Synchronization Settings
- Object classes
- Attributes and Attribute Mapping
- Synchronization User Lists

Note: Some related configuration instructions appear in [Chapter 4, "Configuring Core Resources"](#).

2.2.1 Directories

A directory represents the following:

- A single root suffix (suffix/database) in one or more Sun Java System Directory Servers
- A single Active Directory domain in a Windows 2000 or Windows 2003 Server Active Directory forest
- A single Windows NT domain

You can configure any number of each directory type.

2.2.2 Synchronization Settings

You use synchronization settings to control the direction in which object creations, object deletions, passwords and other attribute modifications are propagated between Directory Server and Windows directories. Synchronization flow options are as follows:

- From Directory Server to Active directory/Windows NT
- From Active directory/Windows NT to Directory Server
- Bidirectionally

Note: In a configuration that includes Active Directory and Windows NT, it is not possible to save a configuration that specifies different synchronization settings for creations or modifications between Windows NT and Directory Server, and between Active Directory and Directory Server.

2.2.3 Object Classes

When you configure resources, you will specify which entries to synchronize based on their *object class*. Object classes determine which *attributes* will be available to synchronize for both Directory Server and Active Directory.

Note: Object classes are not applicable for Windows NT.

Identity Synchronization for Windows supports two types of object classes:

- **Structural object classes.** Every entry that's created or synchronized from the selected Directory Server must have at least one structural object class. Choose a structural object class from the drop-down menu. (Defaults to `inetorgperson` on Directory Server and to `User` on Active Directory.)
- **Auxiliary object classes.**
 - Directory Server allows you to select one or more object classes from the Available Auxiliary Object Classes list to augment the selected structural class. The structural class provides additional attributes for synchronization.
 - Active Directory is more restrictive with the auxiliary object class. Attributes on all valid auxiliary object classes for the selected structural object class will be available for synchronization.

For instructions on configuring object classes and attributes, see [Chapter 4, "Configuring Core Resources"](#)

2.2.4 Attributes and Attribute Mapping

Attributes hold descriptive information about a user entry. Every attribute has a label and one or more values, and follows a standard syntax for the type of information that can be stored as the attribute value.

You can define attributes from the Console. See [Chapter 4, "Configuring Core Resources"](#).

2.2.4.1 Attribute Types

Identity Synchronization for Windows synchronizes *significant* and *creation* user attributes, as follows:

- **Significant attributes.** Synchronized between Directory Server and Windows directories whenever the attributes are modified according to specified modification synchronization settings.
- **Creation attributes.** Synchronized between Directory Server and Windows directories whenever a new user is created, according to specified object creation synchronization settings.

Mandatory creation attributes are attributes that are considered "mandatory" to successfully complete a creation action in the target directory. For example, Active

Directory expects that both `cn` and `samaccountname` have valid values upon creation. On the Directory Server side, if you are configuring `inetorgperson` of a `user` object class, Identity Synchronization for Windows will expect `cn` and `sn` as mandatory attributes for a creation.

A creation attribute default updates the target directory creation attribute with a default value *only* when there is no value in the attribute propagated from the originating directory. (Creation attribute defaults can be based on other attribute values. See [Parameterized Attribute Default Values](#))

Note: Significant attributes are automatically synchronized as creation attributes but not the other way around. Creation attributes are only synchronized during user creations.

2.2.4.2 Parameterized Attribute Default Values

Identity Synchronization for Windows allows you to create *parameterized* default values for creation attributes using other creation or significant attributes.

To create a parameterized default attribute value, you embed an existing creation or significant attribute name, preceded and followed by percent symbols (`%attribute_name%`), in an expression string. For example, `homedir=/home/%uid%` or `cn=%givenName%. %sn%`.

When you create these attribute default values, follow these guidelines:

- You can use multiple attributes in a creation expression (`cn=%givenName% %sn%`), but the attributes in `% attribute_name%` must have single values.
- If `A=0`, `B` can have one default value only.
- You can use the backslash symbol (`\\`) for quoting (for example, `diskUsage=0\\%`).
- Do not use expressions that have cyclic substitution conditions (for example, `sn=%uid%` and `uid= %sn%`).

2.2.4.3 Mapping Attributes

After you define the attributes to synchronize, map the attribute names between the Directory Server and Active Directory/Windows NT systems to synchronize them to each other. For example, you must map the Sun `inetorgperson` attribute to the Active Directory `user` attribute.

You use attribute maps for both significant and creation attributes, and you must configure attribute maps for all "mandatory creation attributes" in each directory type.

2.2.5 Synchronization User Lists

You create Synchronization User Lists (SULs) to define specific users in both the Directory Server and Windows directories to be synchronized. These definitions enable synchronization of a flat Directory Information Tree (DIT) to a hierarchical directory tree.

The following concepts are used to define a Synchronization User List:

- **Base DN**(not applicable to Windows NT). Includes all users in that DN unless another SUL is more specific or unless excluded by a filter.

- **Filter.** Uses attributes in the user's entry to exclude users from synchronization or to separate users with the same base DN into multiple SULs. This filter uses LDAP filter syntax.
- **Creation expression** (not applicable to Windows NT). Constructs the DN where new users are created, for example, `cn=%cn%, ou=sales, dc=example, dc=com`, where `%cn%` is replaced with the value of `cn` from the existing user entry. A creation expression must end with the base DN.

An SUL includes two definitions; where each definition identifies the group of users to be synchronized in the topology terms of the directory type.

- One definition identifies which Directory Server users to synchronize (for example, `ou=people, dc=example, dc=com`).
- The other definition identifies the Windows users to synchronize (for example, `cn=users, dc=example, dc=com`).

When you are preparing to create SULs, ask yourself the following questions:

- Which users will be synchronized?
- Which users are excluded from synchronization?
- Where should new users be created?

See [Appendix D, "Defining and Configuring Synchronization User Lists for Identity Synchronization for Windows"](#) for detailed information about creating SULs.

2.3 Synchronizing Passwords With Active Directory

The default password policy on Windows 2000 was changed on Windows 2003 to enforce strict passwords by default.

Identity Synchronization for Windows services must occasionally create entries that do not have passwords, for example, during a `resync -c` from Directory Server to Active Directory. Consequently, if password policies are enabled on Active Directory (on Windows 2000 or 2003) or on Directory Server, user creation errors can result.

Although you do not have to disable password policies on Active Directory or Directory Server, you need to understand the issues associated with enforcing their password policies.

The following installation information is important if you will be synchronizing passwords with Active Directory on Windows 2003 Server Standard or Enterprise Edition:

- If you are installing on Windows, you can install the Active Directory Connector on the Solaris OS, Red Hat Linux, or Windows.

Note: Active Directory Connectors will work with Active Directory on both Windows 2000 and Windows 2003 Server.

- You use the same procedures to create directory sources, global catalogs, and Synchronization User Lists for Windows 2003 Server that you used for Active Directory on Windows 2000.
- On Windows 2003 Server, the default password policy enforces strict passwords, which is not the default password policy on Windows 2000.

2.3.1 Enforcing Password Policies

This section explains how the password policies for Active Directory on Windows 2000, Windows 2003 Server, and Sun Java System Directory Server can affect synchronization results.

If you create users on Active Directory (or Directory Server) that meet the required password policies for that topology, the users may be created and synchronized properly between the two systems. If you have password policies enabled on both directory sources, the passwords must meet the policies of both directory sources or the synchronized user creations will fail.

- If you enable the password policy features on Active Directory, you should enable a similarly configured or matched password policy on Directory Server.
- If you cannot create a consistent password policy in both Active Directory and Directory Server, you should enable password policies in the directory source that you consider to be the authoritative source for passwords and user creations. However, user creations will not work as expected in some cases because of certain password policy configurations.

Note: Identity Synchronization for Windows does not synchronize password expiration.

This section discusses the following:

- [Directory Server Password Policies](#)
- [Active Directory Password Policies](#)
- [Creating Accounts Without Passwords](#)
- [Example Password Policies](#)
- [Error Messages](#)

2.3.1.1 Directory Server Password Policies

If you create users in Active Directory with passwords that violate the Directory Server password policy, those users will be created and synchronized in Directory Server, but the entries will be created without a password. The password will not be set until the new user logs in to Directory Server, which triggers on-demand password synchronization. At this time the login will fail because the password violates the Directory Server password policy.

To recover from this situation, do one of the following:

- Force users to change their password the next time they log in to Active Directory.
- Change the user password in Active Directory, making sure that the new password meets Directory Server password policy requirements.

2.3.1.2 Active Directory Password Policies

If you create users in Active Directory that do not match the Active Directory password policy, those users *will* be created in Directory Server.

- Active Directory actually creates users "temporarily" and then deletes the entries if the password does not meet the password policy requirements. Consequently, the Active Directory Connector sees this temporary ADD and creates users in Directory Server. The users will not have a password in Directory Server, so no one will be

able to log in as those users. In addition, these entries will not be linked to a valid entry in Active Directory. If deletions are synchronized from Active Directory to Directory Server, the temporarily created users will be deleted automatically.

- Users are created without a password in Directory Server. Directory Server does not enforce the password policy for user creations unless the entries contain a password.

The preferred method from recovering this situation is to synchronize deletions from Active Directory to Directory Server. Alternatively, you can remove the users from Directory Server and then add them to Active Directory with a password that follows Active Directory password policies. This method ensures that the users are created in Directory Server and are properly linked. Directory Server users will have their password invalidated when they log in to Active Directory for the first time and change it.

- If you do not delete the user from Directory Server, and then try to add the Active Directory user again with a new password, the ADD to Directory Server will fail because the user already exists in Directory Server. The entries will not be linked, and you will have to run the `idsync resync` command to link the two separate accounts.

If you run the `idsync resync` command, you must reset the passwords for the accounts in Active Directory that were linked to entries in Directory Server. Resetting the passwords invalidates those passwords in Directory Server, which then forces on-demand synchronization to update the Directory Server passwords the next time users authenticate to Directory Server with their new Active Directory password.

2.3.1.3 Creating Accounts Without Passwords

In certain circumstances, such as resynchronization, Identity Synchronization for Windows must create accounts without passwords.

2.3.1.3.1 Directory Server When Identity Synchronization for Windows creates entries in Directory Server without a password, it sets the `userpassword` attribute to `{PSWSYNC}*INVALID*PASSWORD*`. The user will not be able to log in to Directory Server until you reset the password. One exception is when you run `resync` with the `-i NEW_USERS` or `NEW_LINKED_USERS` option. In this case, `resync` will invalidate the new user's password, triggering on-demand password synchronization the next time the user logs in.

2.3.1.3.2 Active Directory When Identity Synchronization for Windows creates entries in Active Directory without a password, it sets the user's password to a randomly chosen, strong password that meets Active Directory password policies. In this case, a warning message is logged, and the user will not be able to log in to Active Directory until you reset the password.

The following tables show some scenarios that you might encounter as you work with Identity Synchronization for Windows.

This section describes how password policies affect synchronization and resynchronization.

These tables do not attempt to describe all possible configuration scenarios because system configurations differ. Use this information as a guideline to help ensure that passwords will remain synchronized.

Table 2–3 *How Password Policies Affect Synchronization Behavior*

Scenario	Results					
	User Originally Created In	User Meets Password Policy In	User Created In	Directory Server	Active Directory	Comments
Active Directory	Yes	Yes	Yes	Yes	Yes	
	Yes	No	Yes (see Comments)	No	No	User will be created in Directory Server. However, if deletions are synchronized from Active Directory to Directory Server, this user will be deleted immediately. See Active Directory Password Policies information.
	No	Yes	Yes	Yes	Yes	See Active Directory Password Policies information.
Directory Server	No	No	Yes (see Comments)	No	No	Users will be created in Directory Server. However, if deletions are synchronized from Active Directory to Directory Server, this user will be deleted immediately. See Active Directory Password Policies information.
	Yes	Yes	Yes	Yes	Yes	
	Yes	No	Yes	No	No	
	No	Yes	No	No	No	
	No	No	No	No	No	

Table 2–4 How Password Policies Affect Resynchronization Behavior

Scenario	Result		
	Resync Command	User Meets Password Policy In	Active Directory
resync -c -o Sun	N/A	Yes	User will be created in Active Directory but will not be able to log in. See Creating Accounts Without Passwords .
	N/A	No	User will be created in Active Directory but will not be able to log in. See Creating Accounts Without Passwords .
resync -c -i NEW_USERS NEW_LINKED_ USERS	Yes	N/A	User will be created in Directory Server, and the user's passwords will be set when the user first logs in. See Creating Accounts Without Passwords .
	No	N/A	User will be created in Directory Server but cannot log in because the password violates the Directory Server password policy. See Creating Accounts Without Passwords .
resync -c	Yes	N/A	User will be created in Directory Server but cannot log in until a new password value is set in Active Directory or Directory Server. See Creating Accounts Without Passwords .
	No	N/A	User will be created in Directory Server but cannot log in until a new password value is set in Active Directory or Directory Server. See Creating Accounts Without Passwords .

2.3.1.4 Example Password Policies

This section states example password policies for Active Directory and Directory Server.

2.3.1.4.1 Directory Server Password Policies

- User must change password after reset
- User may change password
- Keep 20 passwords in history
- Password expires in 30 days
- Send warning 5 days before password expires
- Check password syntax: Password minimum length is 7 characters

2.3.1.4.2 Active Directory Password Policies

- Enforce Password History: 20 days
- Maximum Password Age: 30 days
- Minimum Password Age: 0 days
- Minimum Password Length: 7 characters
- Passwords must meet complexity requirements: Enabled

2.3.1.5 Error Messages

Check the central logger `audit.log` file on the Core system for the following error message:

Unable to update password on DS due to password policy during on-demand synchronization:

```
WARNING 125 CNN100 hostname "DS Plugin (SUBC100):
unable to update password of entry 'cn=John Doe,ou=people,o=sun',
reason: possible conflict with local password policy"
```

Note: For more information about password policies for Windows 2003, see [http://technet.microsoft.com/en-us/library/cc782657\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc782657(WS.10).aspx)

For more information about password policies for Sun Java System Directory Server, see Chapter 7, *Directory Server Password Policy*, in *Administrator's Guide for Oracle Directory Server Enterprise Edition*.

2.4 Configuring Windows for SSL Operation

If you are planning to propagate password changes from Directory Server to Windows Active Directory, you must configure each Active Directory to use SSL and install the high-encryption pack.

The Identity Synchronization for Windows Active Directory Connector installer can automatically setup SSL in the Active Directory Connector if you enable LDAP over SSL in Active Directory. You can automatically obtain a certificate from a Microsoft Certificate Services Enterprise Root certificate authority as described in

<http://support.microsoft.com/default.aspx?scid=kb;en-us;q247078>
(<http://support.microsoft.com/default.aspx?scid=kb;en-us;q247078>)

However, LDAP over SSL can more easily be configured, as described in the technical note at <http://support.microsoft.com/default.aspx?scid=kb;en-us;321051>
(<http://support.microsoft.com/default.aspx?scid=kb;en-us;321051>)

In this case, if you decided to require trusted certificates for SSL communication, you must manually install the certificate in the Connector's certificate database as described in [Enabling SSL in the Active Directory Connector](#).

2.5 Installation and Configuration Decisions

This section provides installation and configuration summaries and details the choices you make when deploying Identity Synchronization for Windows. Read all of the information in this section, and complete the installation checklists before you begin the installation process.

2.5.1 Core Installation

You must provide the following information when you install Core:

- **Configuration directory host and port.** Specify the configuration directory host and port for the Directory Server instance on which Identity Synchronization for Windows configuration information will be stored.

You can specify an SSL port as the configuration directory port. If you do, you must identify the port as an SSL port during the installation process.
- **Root suffix.** Specify the root suffix for the configuration directory. All configuration information is stored under this suffix.
- **Administrator's name and password.** Specify credentials for accessing the configuration Directory Server.
- **Configuration password.** Specify a secure password to protect sensitive configuration information.
- **File system directory.** Specify the location in which to install Identity Synchronization for Windows. You must install Core in the same directory as a Directory Server Administration Server.
- **Unused port number.** Specify an available port number for the Message Queue instance.
- **Administration Server.** Specify administration server administrator's user name and password if it already exists on Directory Server.

2.5.2 Core Configuration

You must provide the following information when you configure Core:

- **Sun Java System Directory schema.** Specify the Directory Server data that you want to load from the configuration directory.
- **User object class (for Directory Server only).** Specify the user object class that will be used to determine user types. Identity Synchronization for Windows derives a list of attributes (including password attributes) based on this object class. This list is populated from the schema.
- **Synchronized attributes.** Specify user entry attributes to be synchronized between the Directory Server and Windows directory sources.
- **Modifications, creations, and deletions flow.** Specify how you want modifications, creations, and deletions to be propagated between Directory Server and Windows directory sources.
 - From Directory Server to Active directory/Windows NT
 - From Active directory/Windows NT to Directory Server
 - Bidirectionally

Specify whether to synchronize object activations and inactivations if they are propagated between Directory Server and Windows directory sources, and specify a method for synchronizing these objects.

- **Global catalogs.** Specify global catalogs (repositories for Active Directory topological and schema information).
- **Active Directory schema controller.** Specify the fully qualified domain name (FQDN) of the Active Directory schema source to be retrieved from the Windows global catalog.
- **Configuration Directory.** Specify the Directory Server that stores the Identity Synchronization for Windows configuration.
- **Active Directory source.** Specify the sources used to synchronize Active Directory domains.
- **Windows NT Primary Domain Controller.** Specify the Windows NT domains to be synchronized and the name of the Primary Domain Controller for each domain.
- **Synchronization User Lists.** Use LDAP DIT and filter information to specify the users to be synchronized on Directory Server, Active Directory, and Windows NT.
- **Sun Java System Directory Servers.** Specify Directory Server instances that store users to be synchronized.

2.5.3 Connector Installation and Configuring the Directory Server Plug-In

You must provide the following information when you install the connectors and the Directory Server Plug-in:

- **Configuration directory host and port.** Specify the configuration directory host and port for the Directory Server instance on which Identity Synchronization for Windows configuration information will be stored.
- **Root suffix.** Specify the root suffix for the configuration directory. Use the root suffix specified during Core installation.
- **Administrator's name and password.** Specify credentials for accessing the configuration Directory Server.
- **Configuration password.** Specify a secure password to protect sensitive configuration information.
- **File system directory.** Specify the location in which to install Identity Synchronization for Windows. All components installed on the same machine must have the same installation path.
- **Directory sources:** Specify the directory source for which you want to install the connector or plug-in.

When you are installing Directory Server and Windows NT Connectors, you must specify an unused port.

When you are installing the Directory Server Connector and Plug-in, you must specify the host, port, and credentials for the Directory Server that corresponds to that Connector and Plugin.

2.5.4 Using the Command-Line Utilities

Identity Synchronization for Windows enables you to perform a variety of tasks from the command line using the `idsync` script with the following subcommands:

- `certinfo` — Displays certificate information based on your configuration and SSL settings.
- `changepw` — Changes the Identity Synchronization for Windows configuration password.
- `prepsds` — Prepares a Sun Java System Directory Server source for use by Identity Synchronization for Windows.
- `printstat` — Prints the status of installed connectors, the system manager, and Message Queue.

You can also use the `printstat` command to display a list of the remaining installation and configuration steps you have to perform to complete the installation process.

- `resetconn` — Resets connector states in the configuration directory to *uninstalled* only in cases of hardware or uninstaller failure.
- `resync` — Resynchronizes and links existing users, and pre-populates directories as part of the installation process.
- `dspluginconfig` — Configures or unconfigures the Directory Server Plug-in.
- `groupsync` — Enables or disables group synchronization.
- `accountlockout` — Enables or disables account lockout feature.
- `startsync` — Starts synchronization.
- `stopsync` — Stops synchronization.

See [Appendix A, "Using the Identity Synchronization for Windows Command Line Utilities"](#) for detailed information about these utilities.

2.6 Installation Checklists

Use these checklists to prepare for the installation process. Print the checklists and record the appropriate information before installing Identity Synchronization for Windows.

Table 2-5 Core Installation Checklist

Required Information	Entry
Configuration directory host and port	
Root suffix for the configuration directory (such as <code>dc=example,dc=com</code>)	
File system directory in which to install Identity Synchronization for Windows	
Configuration directory server administrator's name and password	
Secure configuration password to protect sensitive configuration information	
Port number for the Message Queue instance	
User name and password for the Administration Server	

Table 2–6 Core Configuration Checklist

Required Information	Entry
Active Directory global catalog (when appropriate)	
Directory Server schema server	
Directory Server user structural and auxiliary object classes	
Synchronized attributes	
Flow for user entry creations	
Flow for user entry modifications	
Flow for user entry activations and inactivations	
Flow for user entry deletions	
Sun Java System Directory Server directory sources	
Active Directory	
Synchronization User Lists	
Windows source filter creation expression	
Sun Java System source filter creation expression	
User name and password for the Administration Server	

Connector and Directory Server Plug-in Installation Checklist

Required Information	Entry
Configuration directory host and port	
Root suffix for the configuration directory	
File system directory in which to install the connector	
Configuration Directory Server administrator's name and password	
Secure configuration password to protect sensitive configuration information	
Directory sources	
Unused port for Directory Server and Windows NT	
Host, port, and credentials for the Directory Server corresponding to the Connector and Plug-in	

Linking Users Checklist

Required Information	Entry
Synchronization User Lists to be linked.	
Attributes used to match equivalent users	
XML configuration file	

Resynchronization Checklist

Required Information	Entry
Synchronization User List selection	
Synchronization source	
Create a user entry automatically if a corresponding user is not found at the destination directory source?	
Invalidate Directory Server passwords?	
Synchronize only those users that match the specified LDAP filter and are in the selected SULs?	

Installing Core

This chapter explains how to use the Identity Synchronization for Windows installation program and how to install the Identity Synchronization for Windows Core component.

The information is organized into the following sections:

- [Before You Begin](#)
- [Starting the Installation Program](#)
- [Installing Core](#)

3.1 Before You Begin

Before starting the Identity Synchronization for Windows installation process:

- Read [Chapter 2, "Preparing for Installation"](#) that contains important information, such as installation prerequisites, checklists, and administrator privilege requirements.
- A Java Runtime Environment (JRE) is not provided with this product. If necessary, you can download a Java Development Kit from the following location:

<http://www.oracle.com/technetwork/java/index.html> or
<http://www.java.com>

You must install JRE 1.5.0_09 or later to run the Identity Synchronization for Windows installation program on your Solaris, Linux, or Windows 2000/2003 systems.

Note: If Directory Server 6.x is installed with Java ES, JRE 1.5.0_09 is already installed on your computer.

- **On Windows systems only:** You must close any open Service Control Panel windows before starting Core installation, or the installation will fail.
- **On Solaris systems:** Do not install Message Queue and Identity Synchronization for Windows in the same directory.
- **On Red Hat Linux systems:** Do not install Message Queue and Identity Synchronization for Windows in the same directory.

3.2 Starting the Installation Program

This section explains how to download, unpack (or unzip), and run the Identity Synchronization for Windows installation program on the following platforms:

- [On Solaris SPARC](#)
- [On Solaris x86](#)
- [On Windows](#)
- [On Red Hat Linux](#)

3.2.1 On Solaris SPARC

Use the following steps to prepare and run the Identity Synchronization for Windows installation program on a Solaris SPARC operating system.

3.2.1.1 To Run Identity Synchronization for Windows on Solaris SPARC

1. Log in as root.
2. Change to the directory on the delivery media for Solaris SPARC containing the installation program, `DSEE_Identity_Synchronization_for_Windows`.
3. Type `./runInstaller.sh` to execute the installation program.

To run the installation program in text-based mode, type the following.

```
./runInstaller.sh -nodisplay
```

When you run the `runInstaller.sh` program, Identity Synchronization for Windows automatically masks passwords so they will not be echoed in the clear.

3.2.2 On Solaris x86

3.2.2.1 To Prepare and Run Identity Synchronization for Windows on Solaris x86

1. Log in as root.
2. Change to the directory on the delivery media for Solaris x86 containing the installation program, `DSEE_Identity_Synchronization_for_Windows`.
3. Type `./runInstaller.sh` to execute the installation program.

To run the installation program in text-based mode, type the following.

```
./runInstaller.sh -nodisplay
```

When you run the `runInstaller.sh` program, Identity Synchronization for Windows automatically masks passwords so they will not be echoed in the clear.

3.2.3 On Windows

Use the following steps to prepare and run the Identity Synchronization for Windows installation program on a Windows operating system:

3.2.3.1 To Run Identity Synchronization for Windows on Windows

1. Log in as an Administrator.

2. Change to the directory on the delivery media for Windows containing the installation program, `DSEE_Identity_Synchronization_for_Windows`.
3. Type `setup.exe` to execute the installation program.

The Identity Synchronization for Windows installation wizard is displayed.

Note: Installing Core in the Administration Server root, makes the Identity Synchronization for Windows wizard detect most of the information required for installation, such as directory paths and names, and complete certain fields in the wizard panels automatically.

If any of the information is missing or incorrect, you can enter the required information manually.

Continue to the next section for Core installation instructions.

3.2.4 On Red Hat Linux

Use the following steps to prepare and run the Identity Synchronization for Windows installation program on a Red Hat Linux operating system:

3.2.4.1 To Prepare and Run Identity Synchronization for Windows on Linux

1. Log in as root.
2. Change to the directory on the delivery media for Red Hat containing the installation program, `DSEE_Identity_Synchronization_for_Windows`.
3. Type `./installer.sh` to execute the installation program.

To run the installation program in text-based mode, type the following.

```
./installer.sh -nodisplay
```

When you run the `installer.sh` program, Identity Synchronization for Windows automatically masks passwords so they will not be echoed in the clear.

3.3 Installing Core

This section explains the process for installing the Identity Synchronization for Windows Core on Solaris, Linux, and Windows operating systems.

Before you install Core, you should be aware of the following requirements:

- **On Solaris systems:** You must have root privileges to install and run Solaris services.
- **On Red Hat Linux systems:** You must have root privileges to install and run Linux services.
- **On Windows 2000/2003 systems:** You must have Administrator privileges to install Identity Synchronization for Windows.

Note: You must install the program as root, but after installation you can configure the software to run Solaris and Linux services as a non-root user. (See [Appendix B, "Identity Synchronization for Windows LinkUsers XML Document Sample"](#))

You must install Core into a directory that has an existing server root managed by an Administration Server (version 5 2004Q2 or higher) or the installation program will fail. (You can install Administration Server using the Directory Server 5 2004Q2 installation program.)

Note: With Identity Synchronization for Windows 6.0 SP1, the installer checks for an existing Sun Java System Administration Server. If it is not installed, the installer will install Sun Java System Administration Server as a part of Core installation.

3.3.1 To Install Identity Synchronization for Windows Core Components Using the Installation Wizard

1. When the Welcome screen is displayed, read the information provided and then click Next to proceed to the Software License Agreement panel.
2. Read the license agreement, then select
 - **Yes (Accept License)** to accept the license terms and go to the next panel.
 - **No** to stop the setup process and exit the installation program.
3. The Configuration Location panel is displayed, specify the configuration directory location.

Figure 3–1 Specifying the Configuration Directory Location

Core Install: Configuration Location

Specify information about the configuration directory and root context where the Sun Java(TM) System Identity Synchronization for Windows will be stored or is already stored.

Configuration Directory Host:

Configuration Directory Port: Secure Port

Configuration Root Suffix:

Provide the following information:

- **Configuration Directory Host:** Enter the fully qualified domain name (FQDN) of a Sun Java System Directory Server instance (affiliated with the local Administration Server) where Identity Synchronization for Windows configuration information will be stored.

You can specify an instance on the local machine or an instance that is running on a different machine.

Identity Synchronization for Windows allows Administration Server to access the remotely installed instance of Directory Server.

Note: To avoid warnings about invalid credentials or host names, be sure to specify a host name that is DNS-resolvable to the machine on which the installation program is running.

- **Configuration Directory Port:** Specify the port where the configuration directory is installed. (*Default port is 389*)

To enable secure communication, enable the Secure Port option and specify an SSL port. (*Default SSL port is 636*).

Once the program determines that the configuration directory is SSL-enabled, all Identity Synchronization for Windows components will use SSL to communicate with the configuration directory.

Note: Identity Synchronization for Windows encrypts sensitive configuration information before sending it to the configuration Directory Server.

However, if you want additional transport encryption between the Console and configuration directory, be sure to enable SSL for both Administration Server and the configuration Directory Server. Then, configure a secure connection between the Administration Server to which you will be authenticating the Directory Server Console. (For information, see the *Sun Java System Administration Server 5 2004Q2 Administration Guide*).

Sun Java System Administration Server installed (and configured) as a part of the core components, is installed in a non-SSL mode.

- **Configuration Root Suffix:** Select a root suffix from the menu in which to store the Identity Synchronization for Windows configuration.

Note: If the program could not detect a root suffix, and you have to enter the information manually (or if you change the default value), you must click Refresh to regenerate a list of root suffixes. You must specify a root suffix that exists on the configuration Directory Server.

4. Click Next to open the Configuration Directory Credentials panel.

Figure 3–2 Specifying the Administrator Credentials

Core Install: Configuration Directory Credentials

You must specify administrative credentials to access the configuration Directory Server.

Administrator User ID:

Administrator Password:

5. Enter the configuration directory Administrator's user ID and password.
 - If you specify `admin` as the user ID, you will not be required to specify the User ID as a DN.
 - If you use any other user ID, then you must specify the ID as a full DN. For example, `cn=Directory Manager`.

Note: If you are not using SSL to communicate with the configuration directory (see [Installing Core](#)), these credentials will be sent without encryption.

6. When you are finished, click Next to open the Configuration Password panel.

Figure 3–3 Specifying a Configuration Password

Core Install: Configuration Password

Please provide a password that will be used to encrypt sensitive parts of the configuration. Remember this password because it must be supplied when you use the console, use the command line utilities, or install other components.

Configuration Password:

Confirm Password:

7. You must enter and confirm a password that will be used to encrypt sensitive configuration information, such as credentials. When you are done, click Next.

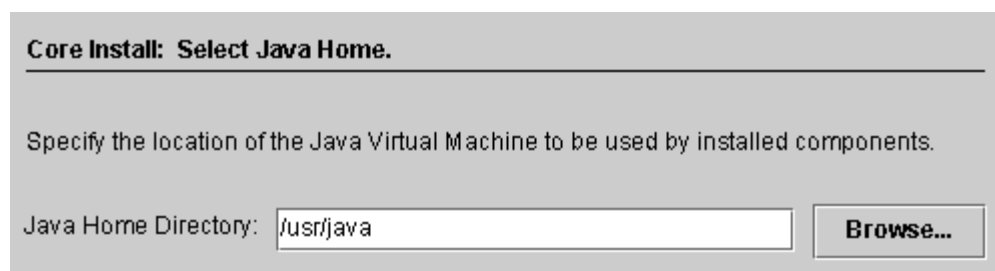
Note: Be sure to remember this password as it will be required whenever you want to

- Access the Identity Synchronization for Windows Console
- Create or edit a configuration
- Install components
- Run any of the command line utilities

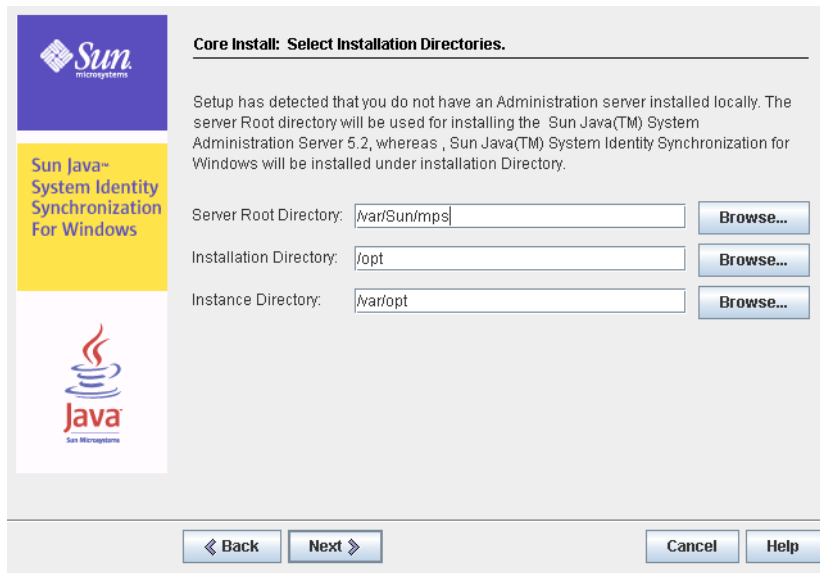
For information about changing the configuration password see [Using changepw](#).

The Select Java Home panel is displayed (see [Installing Core](#)). The program automatically inserts the location of the Java Virtual Machine directory to be used by the installed components.

Figure 3–4 *Specifying the Java Home Directory*



8. Verify the Java Home Directory (must be a JDK/JRE 1.5.0_09 or later):
 - If the location is satisfactory, click Next to proceed to the Select Installation Directories panel ([Installing Core](#)).
 - If the location is not correct, click Browse to search for and select a directory where Java is installed, for example:
 - **On Solaris** : /var/java
 - **On Linux**: /usr/bin/java
 - **On Windows**: C:\Program Files\j2sdk1.5

Figure 3–5 Specifying the Installation Directories

9. Enter the following information in the text fields provided or click Browse to search for and select available directories:
 - **Server Root Directory:** Specify the path and directory name of the Administration Server installation server root. The Console will be installed in this location.
 - **Installation Directory** (*available only when you are installing Core on Solaris or Linux*): Specify the path and directory name of the installation directory. Core binaries, libraries, and executable will be installed in this directory.
 - **Instance Directory** (*available only when you are installing Core on Solaris or Linux*): Specify the path and directory name of the instance directory. Configuration information that changes (such as log files) will be stored in this directory.

Note: There is only one server root directory available on Windows operating systems, and all products will be installed in that location.

Note: If an Administration Server corresponding to the Configuration Directory Host and Port number provided in step 3 is not found, the installer Administration Server will install the Administration Server as part of the core installation. The default port number for the Administration Server port assigned would be the configuration directory port plus one.

10. Click Next to proceed to the Message Queue Configuration panel.

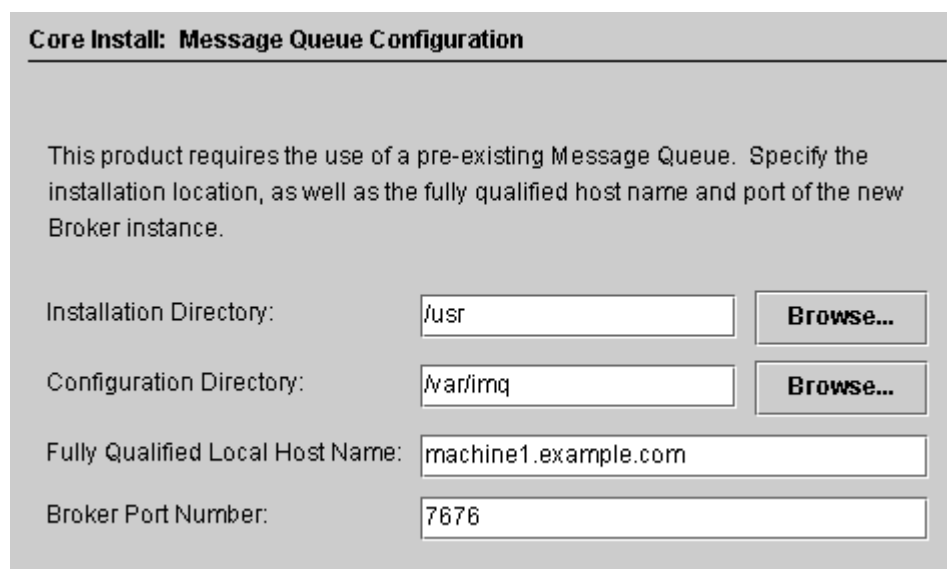
Note: You should have installed Message Queue 3.6 Enterprise Edition before starting the Identity Synchronization for Windows installation.

On Solaris systems: Do not install Message Queue and Identity Synchronization for Windows in the same directory.

On Linux system: Do not install Message Queue and Identity Synchronization for Windows in the same directory.

On Windows systems: You must close any open Service Control Panel windows before continuing, or the Core installation will fail.

Figure 3–6 Configuring Message Queue



Core Install: Message Queue Configuration

This product requires the use of a pre-existing Message Queue. Specify the installation location, as well as the fully qualified host name and port of the new Broker instance.

Installation Directory:

Configuration Directory:

Fully Qualified Local Host Name:

Broker Port Number:

11. Enter the following information in the text fields provided or click Browse to search for and select available directories:
 - **Installation Directory:** Specify the path of the Message Queue installation directory.
 - **Configuration Directory:** Specify the path and directory name of the Message Queue instance directory.
 - **Fully Qualified Local Host Name :** Specify the fully qualified domain name (FQDN) of the local host machine. (There can only be one Message Queue broker instance running per host.)
 - **Broker Port Number :** Specify an unused port number for the Message Queue broker to use. (*Default port is 7676*)
12. Click Next and the Ready to Install panel is displayed.

This panel provides information about the install, such as the directory where Core will be installed and how much space is required to install Core.

- If the displayed information is satisfactory, click Install Now to install the Core component (where the installation program installs the binaries, files, and packages).
- If the information is not correct, click Back to make changes.

An "Installing" message is displayed briefly, and then the Component Configuration panel is displayed while the installation program adds configuration data to the specified configuration Directory Server. This operation includes: a) creating a Message Queue broker instance, b) creating a Message Queue broker instance, and c) uploading deployment-specific configuration information to the configuration directory.

This operation will take several minutes and may pause periodically, so do not be concerned unless the process exceeds ten minutes. (Watch the progress bar to monitor the installation program's status.)

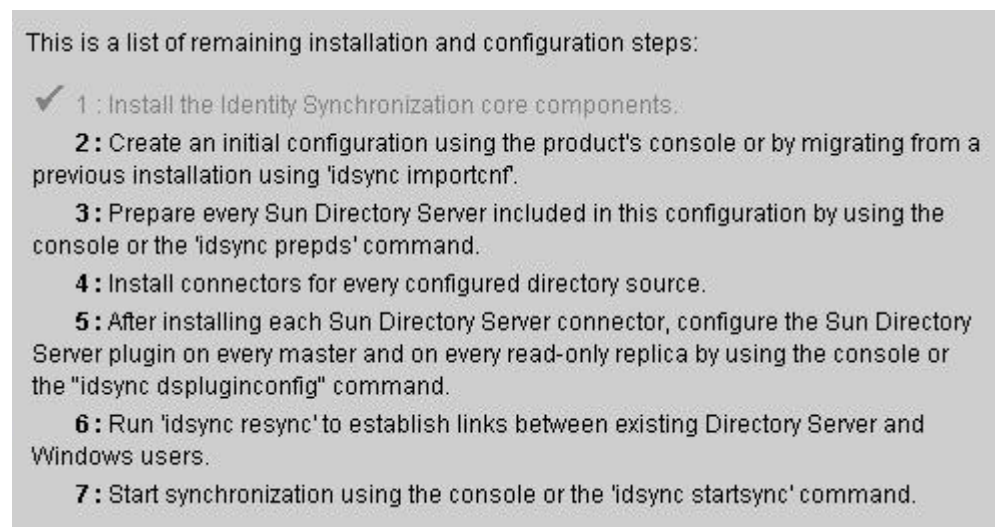
13. When the component configuration operation is complete, the Installation Summary panel is displayed to confirm that Identity Synchronization for Windows installed successfully.

You can click the Details button to see a list of the files that have been installed, and where they are located.

14. Click Next and the program will determine the remaining steps you must perform to successfully install and configure Identity Synchronization for Windows.

A "Loading..." message, and then a Remaining Installation Steps panel each display briefly, and then the following panel ([Installation Overview](#)) is displayed. This panel contains a "To Do" list of the remaining installation and configuration steps. (You also can access this panel from the Console's Status tab.)

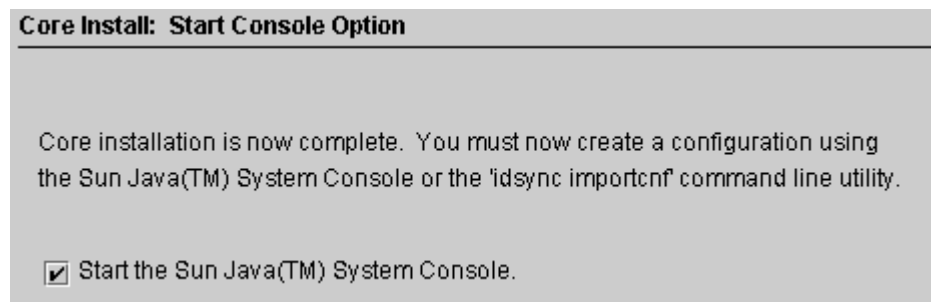
Figure 3–7 To Do List for Identity Synchronization for Windows Installation and Configuration



The "To Do" panel will re-display throughout the installation and configuration process. The program greys-out all completed steps in the list.

Up to this point, the To Do list will contain a generic list of steps. After you save a configuration, the program provides a list of steps that are customized for your deployment (for example, which connectors you must install).

15. After reading the list of steps, click Next and the Start Console Option panel is displayed to indicate you have finished the Core installation.

Figure 3–8 Starting the Console

16. Next, you must configure the Core component, which you can do from the Sun Java System Console (*the Start the Sun Java System Console option is enabled by default*).

If you are migrating from Identity Synchronization for Windows version 1.0 or SP1 to Sun Java System Identity Synchronization for Windows 6.0 SP1, you can import an exported version 1.0 or SP1 configuration XML document using the `idsync importcnf` command line utility.

17. Click Finished.

18. If you elected to use the Console, the Sun Java System Console Login dialog box is displayed (see [Installing Core](#)).

Figure 3–9 Logging into the Console

You must enter the following information to log into the Console:

- **User ID:** Enter the Administrator's user ID you specified when you installed the Administration Server on your machine.
- **Password:** Enter the Administrator's password specified during Administration Server installation.
- **Administration URL:** Enter the Administration Server's current URL location using the following format:

`http://hostname.your_domain.domain:port_number`

Where *hostname.your_domain.domain* is the computer host name you selected when you installed Administration Server, and *port_number* is the port you specified for Administration Server.

19. After providing your credentials, click OK to close the dialog box.
20. You will then be prompted for the configuration password. Enter the password and click OK.

When the Sun Java System Server Console window is displayed, you can start configuring Core. Continue to [Chapter 4, "Configuring Core Resources"](#) for instructions.

Configuring Core Resources

You must initially configure the Core resources immediately after installing the Identity Synchronization for Windows Core.

This chapter explains how to add and configure these resources using the Console, and is organized into the following sections:

- [Configuration Overview](#)
- [Opening the Identity Synchronization for Windows Console](#)
- [Creating Directory Sources](#)
- [Selecting and Mapping User Attributes](#)
- [Propagating User Attributes Between Systems](#)
- [Creating Synchronization User Lists](#)
- [Saving a Configuration](#)

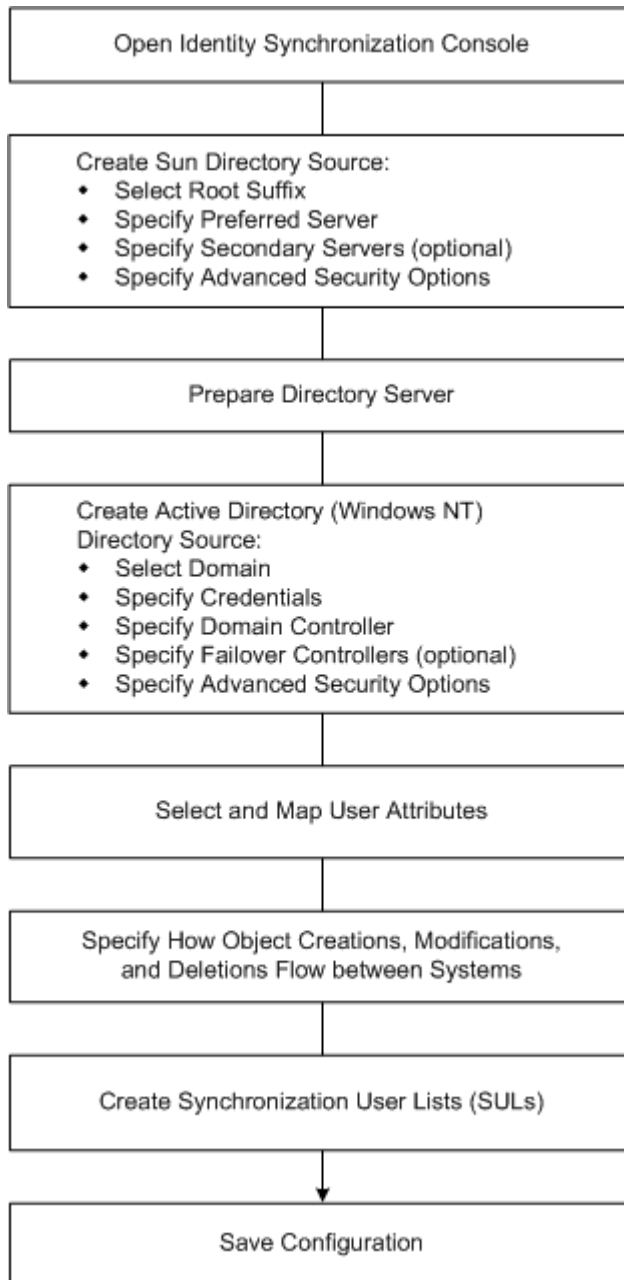
Note: To effectively configure Core resources you must know how to configure and operate Directory Server and Active Directory.

You are not required to configure these resources in a particular order (unless specifically noted in the text); however, using the configuration order presented in this chapter until you become more familiar with the product can save time and prevent errors.

4.1 Configuration Overview

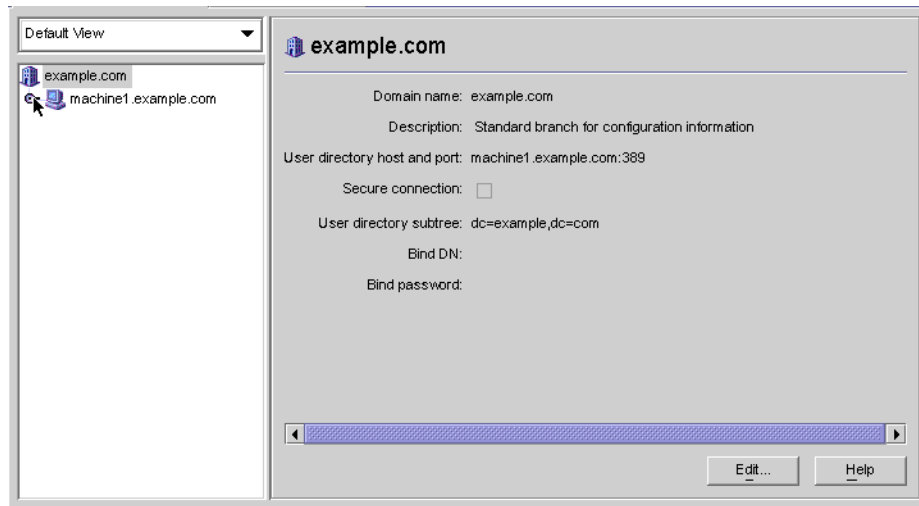
This section illustrates the steps you will use to configure the Core resources for your deployment.

Figure 4–1 Configuring Core Resources for Your Deployment



4.2 Opening the Identity Synchronization for Windows Console

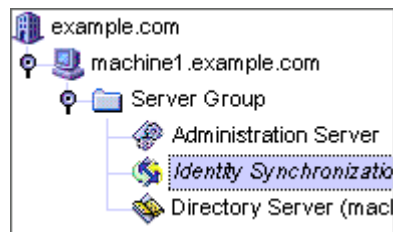
The Sun Java System Server Console window lists all of the servers and resources under your control and provides information about your system.

Figure 4–2 Sun Java System Server Console

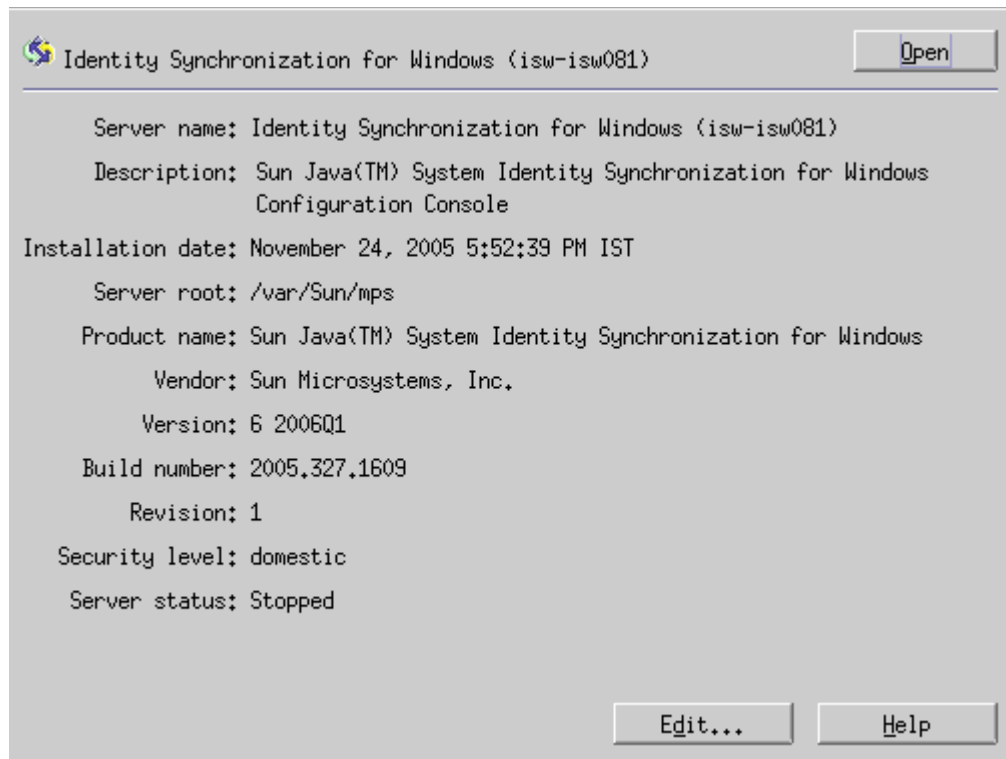
Note: If you have not logged into the Sun Java System Server Console yet, return to [Figure 3–9](#) for instructions.

4.2.1 To Open Identity Synchronization for Windows Console

1. On the Servers and Applications tab, select the hostname node in the navigation tree that contains the Server Group to which the Identity Synchronization for Windows instance belongs.
2. Expand the Server Group node and select the Identity Synchronization for Windows node.

Figure 4–3 Expanding the Server Group

The information panel changes to provide information about Identity Synchronization for Windows and your system.

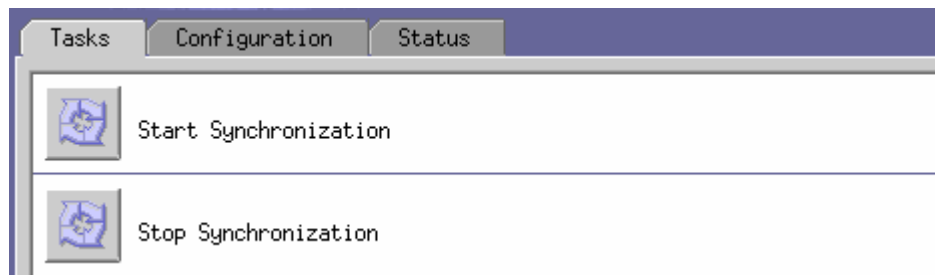
Figure 4–4 Information Panel

3. Click the Open button (located in the upper-right corner of the panel).

Note: The Edit button (located at the bottom of the panel) enables you to edit the Server name and Description.

4. You will be prompted to enter the configuration password that you specified during Core installation. Enter the password and click OK.

The Identity Synchronization for Windows Console is displayed, as follows:

Figure 4–5 Console: Tasks Tab

This window contains three tabs:

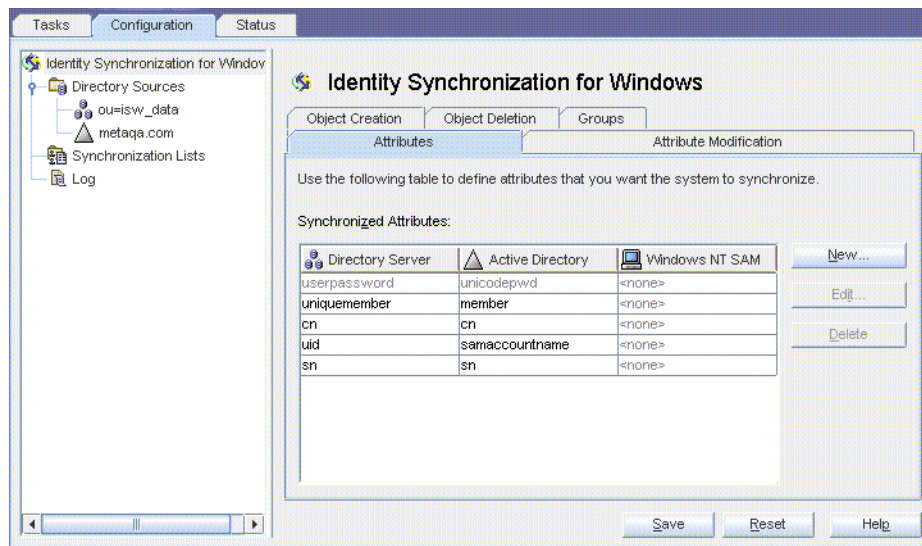
- **Tasks (Default):** Use this tab to stop and start synchronization between your Sun and Windows systems. (Information about starting and stopping services is provided in [Starting and Stopping Synchronization](#))

Note: Do not confuse starting and stopping Synchronization Services with starting and stopping Windows services.

To start or stop Windows services, you must do so from the Windows Console by selecting Start > Console > Administrative Tools > Computer Management > Services.

- **Configuration:** Use this tab to configure your systems for synchronization.
 - **Status:** Use this tab to do the following: a) monitor the status of system components (such as Connectors), b) view the audit and error logs generated by Identity Synchronization for Windows during configuration and synchronization, and c) update and check the installation and configuration To Do list.
5. Select the Configuration tab.

Figure 4–6 Console: Configuration Tab



The Configuration panel consists of the following tabs:

- **Attributes:** Use this tab to specify the attributes you want to synchronize between systems.

Attribute Modification: Use this tab to specify how passwords, attribute modifications, and object disablements are propagated between systems.

Object Creation: Use this tab to specify how newly created passwords and attributes are propagated between systems, and to specify initial values for the objects created by Identity Synchronization for Windows during synchronization.

Object Deletion: Use this tab to specify how deleted passwords and attributes are propagated between systems.

You must configure at least one Sun Java System Directory Server directory source, and at least one Windows server directory source (either Active Directory or Windows NT). Proceed to the next section for instructions.

4.3 Creating Directory Sources

4.3.1 To Create Directory Sources

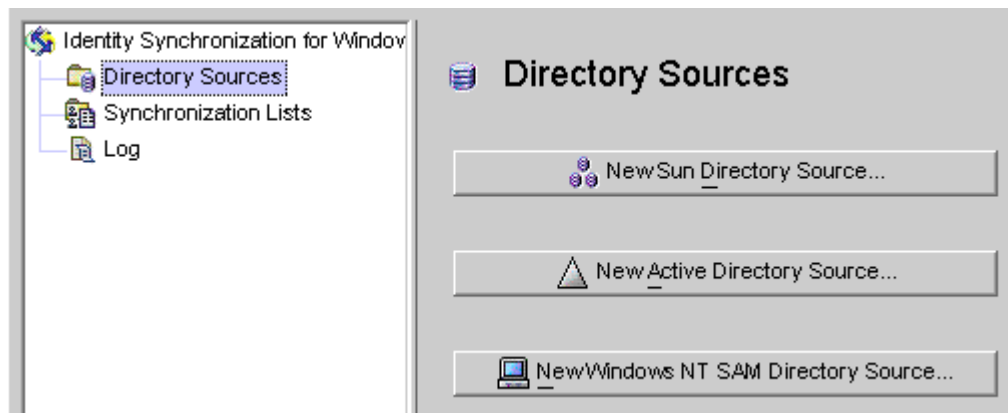
You must create directory sources in the following order (based on which sources you will be synchronizing).

1. [Creating a Sun Java System Directory Source](#)
2. [Preparing Sun Directory Source](#)
3. [Creating an Active Directory Source](#)
4. [Creating a Windows NT SAM Directory Source](#)

Note: At minimum, you must configure at least one Sun Java System Directory source and at least one Windows directory source (Active Directory and/or NT SAM).

Select the Directory Sources node in the navigation tree and the Directory Sources panel is displayed.

Figure 4–7 Accessing the Directory Sources Panel



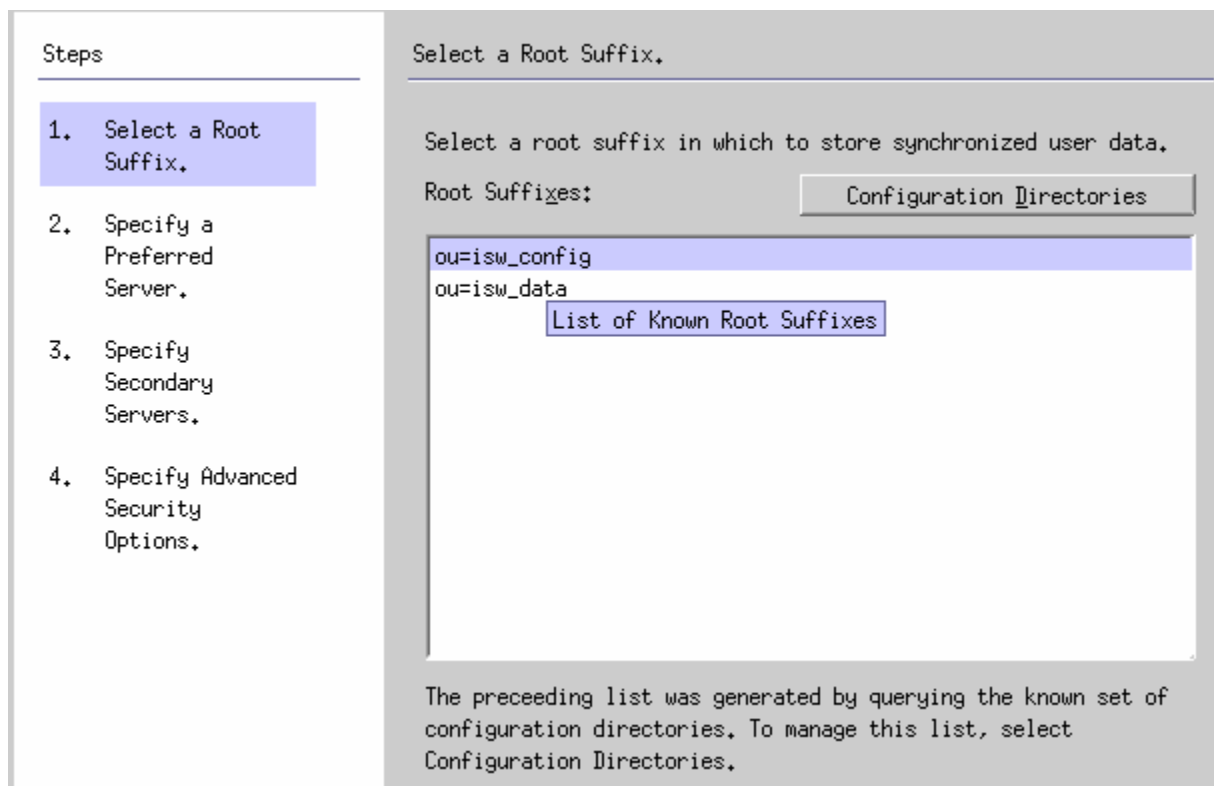
4.3.2 Creating a Sun Java System Directory Source

Each Sun Java System directory source is associated with a Connector and set of Plug-ins that can be deployed in a replication scenario involving multiple servers. The Directory Server Connector is capable of synchronizing changes from Windows directory source to the preferred server (master). In case, the preferred server is down, the changes will failover to the secondary server in the configured secondary servers list in a sequential manner till the preferred server comes up. Directory Server replication will replicate changes made from the preferred server (master) to other preferred secondary servers configured in the topology. Any Directory Server Plug-in can handle password validity checks from Windows directory sources and users can change passwords at any server.

4.3.2.1 To Create a New Sun Java System Directory Source

1. Click the New Sun Directory Source button to invoke the Define Sun Java System Directory Source wizard.

Figure 4–8 Selecting a Root Suffix



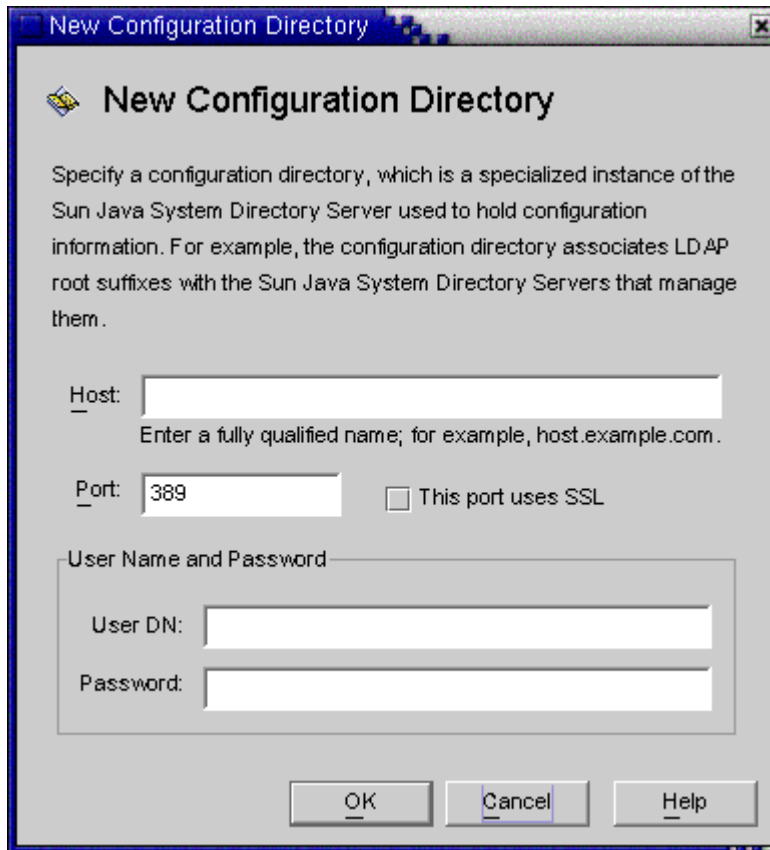
The program queries a known set of configuration directory sources and displays existing root suffix (also referred to as *naming contexts*) in the list pane.

By default, the program knows about the configuration directory where you installed the product, and the root suffixes known by the configuration directory will be listed in the list pane.

2. Select the root suffix where your users are located from the list pane. (If several root suffixes are listed, select the one where your users are located.) Click Next.

If the root suffix you want to synchronize with is not affiliated with a configuration directory registered with Identity Synchronization for Windows, then you must specify a new configuration directory, as follows:

- a. Click the Configuration Directories button to specify a new configuration directory.
- b. When the Configuration Directories dialog box is displayed ([Use one of the following methods to select a preferred server:](#)), click the New button to open the New Configuration Directories dialog box.

Figure 4–9 Selecting a New Configuration Directory

- c. Enter the following information, and then click OK to save your changes and close the dialog box.

Host: Enter the fully qualified host name.

For example: **machine1.example.com**

Port: Enter a valid, unused LDAP port number. (Default is 389)

Enable the This port uses SSL box if Identity Synchronization for Windows is using an SSL (Secure Socket Layer) port to communicate with the configuration directory.

User DN: Enter your Administrator's (bind) distinguished name. For example, **uid=admin,ou=Administrators,ou=TopologyManagement,o=NetscapeRoot**

Password: Enter your Administrator's password.

The wizard will query the specified configuration directory to determine all of the directory servers managed by that directory.

Note: Identity Synchronization for Windows only supports one root suffix per Sun Java System Directory Server source.

Editing and Removing Configuration Directories

You can also use the Configuration Directories dialog box to manage your list of configuration directories, as follows:

Select a configuration directory from the list pane, and then click the Edit button. When the Edit Configuration Directories dialog is displayed, you can change the Host, Port, Secure Port, User Name, and Password parameters.

Select a configuration directory from the list pane, and then click Remove to delete the directory from the list.

- d. Click OK to close the Configuration Directories dialog box and the newly selected configuration directory's root suffixes are displayed in the list pane.

By default, Directory Server creates a root suffix whose prefix corresponds to the components of the machine's DNS domain entry. It uses the following suffix:

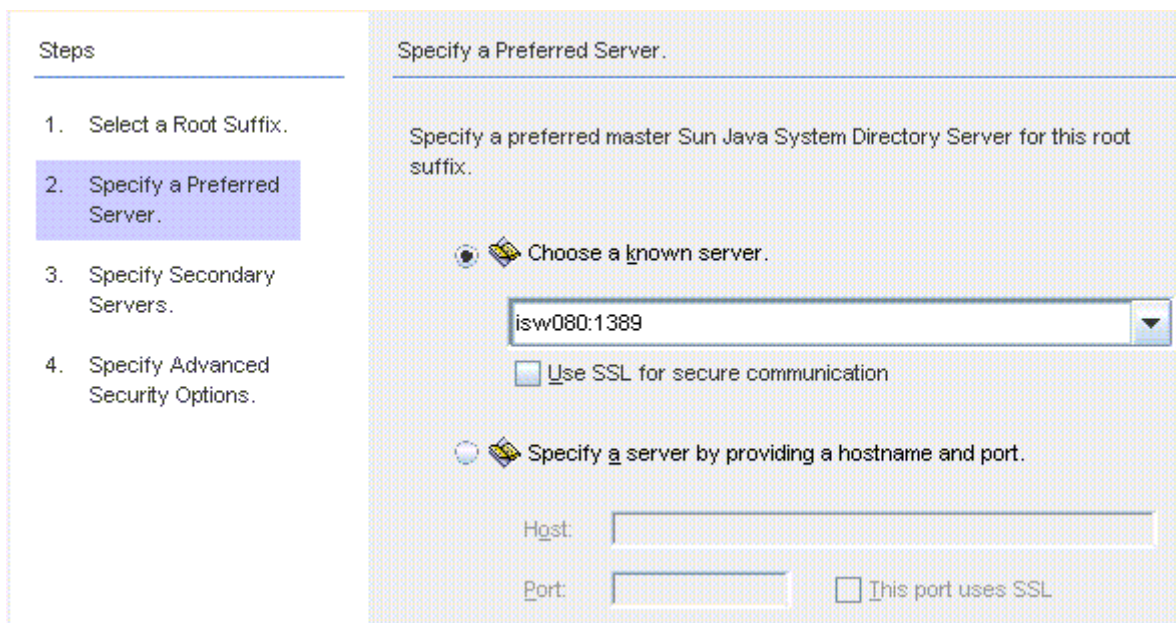
`dc=your_machine's_DNS_domain_name`

That is, if your machine domain is *example.com*, then you should configure the suffix `dc=example`, `dc=com` for your server. The entry named by the chosen suffix must already exist in the directory.

- e. Select the root suffix, and click Next.

The Specify Preferred Servers panel is displayed (see [Creating a Sun Java System Directory Source](#)).

Figure 4–10 Specifying a Preferred Server



Identity Synchronization for Windows uses the preferred Directory Server to detect changes made at any Directory Server master. The preferred server also acts as the primary location where changes made on Windows systems are applied to the Sun Java System Directory Server system.

If the preferred master server fails, the secondary server can store these changes until the preferred server (master) comes back online.

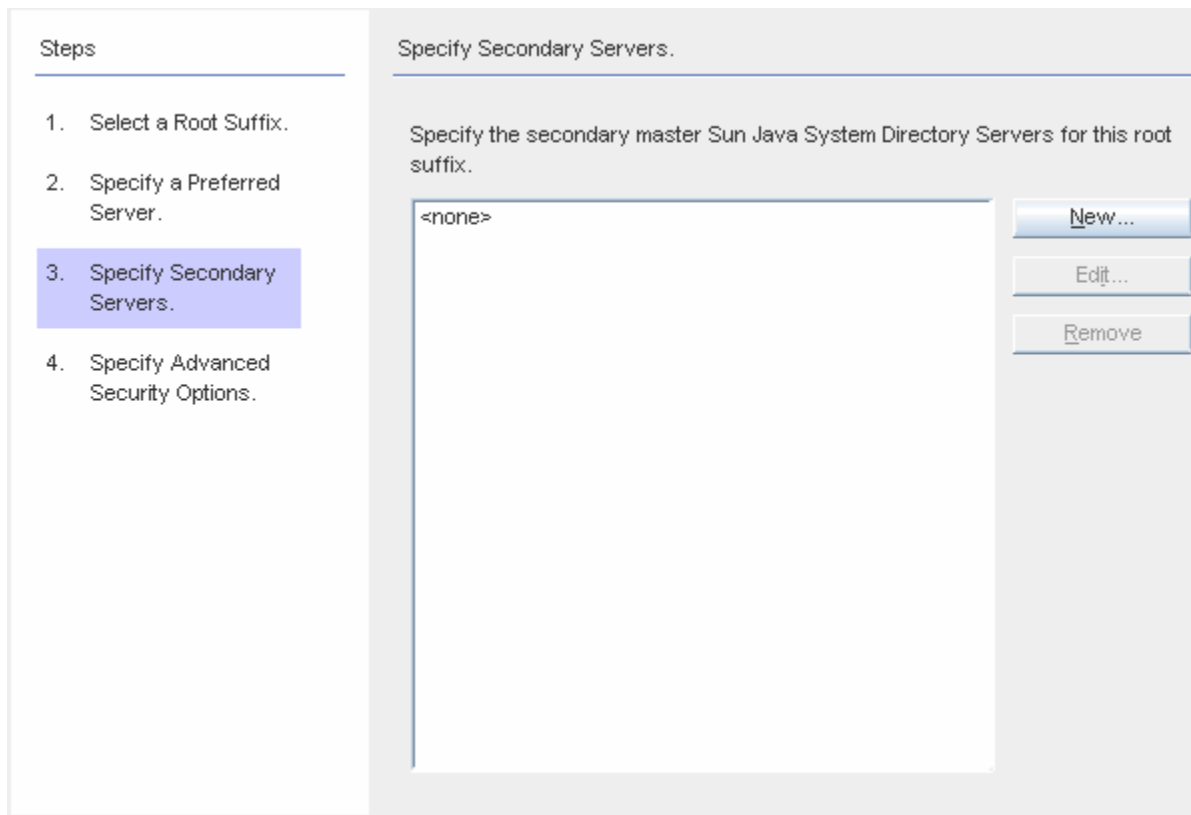
3. Use one of the following methods to select a preferred server:
 - Select the Choose a Known Server option, and then select a server name from the drop-down list.

Note: The Directory Server must be running to appear in the list. If the server is down temporarily, select the Specify a Server by Providing a Hostname and Port option, and then enter the server information manually.

Enable the Use SSL for secure communication box if you want the Directory Server to communicate using SSL. However, if you enable this feature there are some additional setup steps you must perform after installation. For more information, see [Enabling SSL in Directory Server](#)

- Select the Specify a Server By Providing a Hostname and Port option, and then type the server's Host name and Port into the text fields.
Select the This Port Uses SSL checkbox if the port you specified uses SSL.
4. Click Next and the Specify a Secondary Server panel is displayed.

Figure 4–11 *Specifying the Secondary Servers for Failover Support*



You can add, edit, or delete the Secondary Servers:

- a. Click the New button to display the Add Sun Directory Source dialog box. Enter the host name, port, user DN, password, and then click OK. For more information on these fields, see [Enter the following information, and then click OK to save your changes and close the dialog box.](#)
- b. Click the Edit button to display the Edit Sun Directory Source dialog box. Enter the host name, port, user DN, password, and then click OK. For more

information on these fields, see [Enter the following information, and then click OK to save your changes and close the dialog box.](#)

- c. From the Secondary Servers list, select the server you want to delete and click the Remove button.
5. To specify the secondary Directory Servers, select a server name from list, and then click Next.

Note: ■ The Directory Server must be running or the server name will *not* appear in list.

- Do not use the same host name and port for both the preferred and the secondary servers in a Sun directory source.
- If you enable the Secure Port feature, there are additional setup steps you must perform after installation. For more information, see [Enabling SSL in Directory Server](#)

If you do not want to specify a secondary server, click Next.

6. If you want to use secure SSL communication, *read the notes below*, and then enable one or both of the following options:

Figure 4–12 Specifying Advanced Security Options

Steps	Specify Advanced Security Options.
1. Select a Root Suffix.	
2. Specify a Preferred Server.	
3. Specify Secondary Servers.	
4. Specify Advanced Security Options.	<p><input type="checkbox"/> Require trusted SSL certificates</p> <p><i>This option only applies to SSL communication between the directory server connector and the directory server.</i></p> <p><input type="checkbox"/> Use SSL for plugin to Active Directory communication</p> <p>WARNING: Before enabling this setting, be sure you read and understand the security information provided in the product documentation. Also, you can use the 'idsync certinfo' command line utility to get specific information about the certificates required to configure SSL for your system.</p>

Note: You must install the Directory Server Plug-in on each Directory Server (any master, replica, or hub) where users will bind or where passwords will be changed.

When the Directory Server Plug-in synchronizes passwords and attributes to Active Directory, it must bind to Active Directory to search for users and their passwords. In addition, the Plug-in writes log messages to the central log and into the Directory Server's log. By default these communications are not accomplished over SSL.

- To encrypt channel communication only or to encrypt channel communication and use certificates to ensure participants' identity verification between Directory Server and the Directory Server Connector, enable the Require Certificates for SSL box.

Clear the checkbox if you do not want to trust certificates.

- To use secure SSL communication between the Directory Server Plug-in and Active Directory, enable the Use SSL for Plug-in to Active Directory communication box.

If you enable these features, then additional setup is required after installation. See [Enabling SSL in Directory Server](#)

- You can use the use the `idsync certinfo` command line utility to determine which certificates you must add for each Directory Server Plug-in and/or Connector certificate database. See [Using certinfo](#)
- If your primary and secondary Directory Servers are part of a multimaster replication (MMR) deployment, refer to [Appendix E, "Identity Synchronization for Windows Installation Notes for Replicated Environments"](#)

7. When you are finished with the Specify Advanced Security Options panel, click Finish.

The program adds the selected directory sources to the navigation tree under Directory Sources, and the Prepare Directory Server Now? dialog is displayed.

You must prepare the Directory Server to be used by Identity Synchronization for Windows. You can choose to perform this task now, or you can do it later — but you must prepare the Directory Server before you install the Connectors. (Instructions for installing Connectors are provided in [Chapter 5, "Installing Connectors"](#)).

- If you want to prepare the Directory Server now, click Yes to open the wizard, and then proceed to the next section, [Preparing Sun Directory Source](#)
- If you prefer to perform this process later, click No and proceed to [Creating an Active Directory Source](#).

4.3.3 Preparing Sun Directory Source

This section explains how to prepare Sun Directory source for use by Identity Synchronization for Windows.

Preparing the Directory Server:

- Creates the Retro-Changelog database and access control instance available on the preferred host
- Creates the Connector user and user access control instance available on the preferred host
- Creates an equality index on the preferred and secondary hosts

Note: ■ As an alternative to using the Console, you can use the `idsync prepds` command line utility to prepare the Directory Server. For more information, see [Using prepds](#).

- To prepare the Directory Server using the `idsync prepds` command line utility, you must know which hosts and suffixes you will be using and you must have Directory Manager's credentials.

You can use the Prepare Directory Server wizard to prepare the Directory Server.

Figure 4–13 Entering Your Directory Manager Credentials

Steps

1. Specify Directory Manager Credentials.
2. Specify Preparation Configuration.
3. Preparation Status.

Specify Directory Manager Credentials.

To prepare the Sun Java System Directory Server for use by Sun Java System Identity Synchronization for Windows, you must provide Directory Manager credentials.

Preferred Host : machine1.example.com:389

Directory Manager User Name :

Directory Manager Password :

Secondary Host :

Directory Manager User Name :

Directory Manager Password :

Note: To access this wizard, use one of the following methods:

- When the Prepare Directory Server Now? dialog box is displayed, click the Yes button.
 - When the Sun Directory Sources panel is displayed (on the Configuration tab), click the Prepare Directory Server button.
-

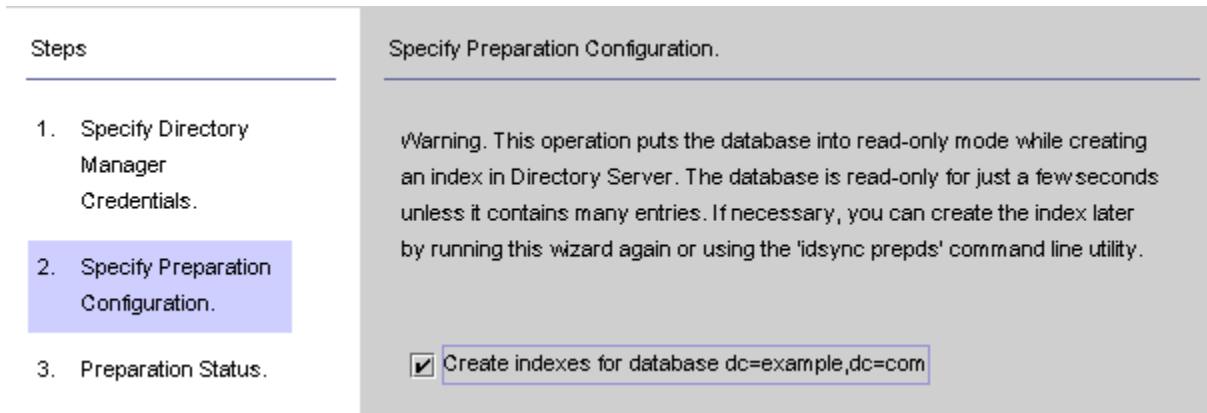
4.3.3.1 To Prepare your Directory Server Source

1. Enter the following credentials for the Directory Manager account.
 - **Directory Manager User Name**
 - **Directory Manager Password**

If you are using a secondary host (MMR configurations), then the Secondary Host options will be active and you must specify credentials for these hosts too.

- When you are done, click Next and the Specify Preparation Configuration panel is displayed.

Figure 4–14 *Specifying the Preparation Configuration*



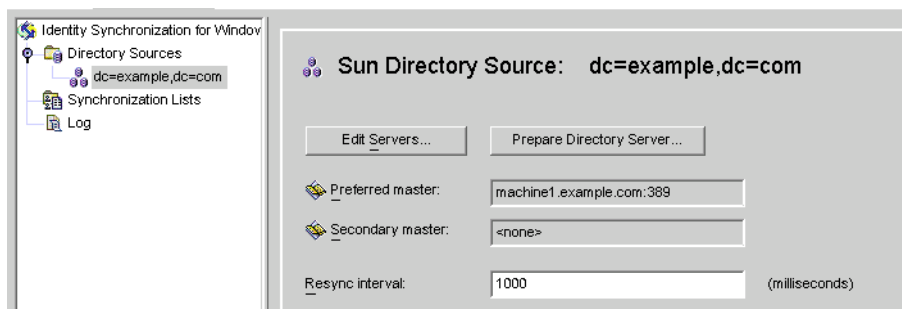
Read the warning, and then decide whether to create the Directory Server indexes now or later.

Note: ■ This operation can take some time, depending on the size of your database.

- While your database is in read-only mode, any attempts to update information in the database will fail.
 - Taking your database offline enables you to create the indexes much faster.
 - To create the indexes now, enable the Create indexes for database box, and then click Next.
 - To create the indexes later (either manually or by running this wizard again) clear the Create indexes for database box, and then click Next.
-

- The Preparation Status panel is displayed to provide information about the Directory Server preparation progress.
 - When a SUCCESS message is displayed at the bottom of the message pane, click Finish.
 - If error messages display, you must correct the problem(s) reported before you can continue. Check the error logs (see the Status tab) for more information.
- Return to the Configuration tab in the Console. Select the Sun Directory source node in the navigation tree to view the Sun Directory Source panel.

Figure 4–15 Sun Directory Source Panel



From this panel, you can perform the following tasks:

- Edit servers:** Click this button to reopen the Define Sun Java System Directory Source panel where you can change any of the server configuration parameters. If necessary, review the instructions provided for [Creating a Sun Java System Directory Source](#).

Note: If you recreate the Retro-Changelog database for the preferred Sun directory source, the default access control settings will not allow the Directory Server Connector to read the database contents.

To restore the access control settings for new the Retro-Changelog database, run `idsync prepds` or click the Prepare Directory Server button after selecting the appropriate Sun directory source in the Console.

- Prepare Directory Server:** Click this button and follow the instructions for [Preparing Sun Directory Source](#) to prepare a Directory Server.

If anything changes on the Directory Server after you initially prepare the server (for example, if an index is deleted or you lose the Retro-Changelog database), you can re-prepare the server.

- Resync interval:** Specify how often you want the Directory Server Connector to check for changes. (Default is 1000 milliseconds)
- Add a Directory Server directory source for each user population in your Sun Java System Directory Server enterprise that you want to synchronize.

When you are finished, you must create at least one Windows directory source:

- To create an Active Directory source, continue to the next section, [Creating an Active Directory Source](#).
- To create a Windows NT directory source, continue to [Creating a Windows NT SAM Directory Source](#)

4.3.4 Creating an Active Directory Source

You should add an Active Directory directory source for each Windows domain in your network that you want to synchronize.

Each Active Directory deployment has at least one global catalog that knows about all the global information across all Active Directory domains. To access the global

catalog, the rights assigned to a normal user are sufficient unless you change the default permissions.

Note: It is possible for each Active Directory server to be a global catalog and a deployment can have multiple global catalogs, but you only need to specify one global catalog.

4.3.4.1 To Configure and Create Windows Active Directory Servers in a Network

Perform these steps if there are Windows Active Directory servers in your network:

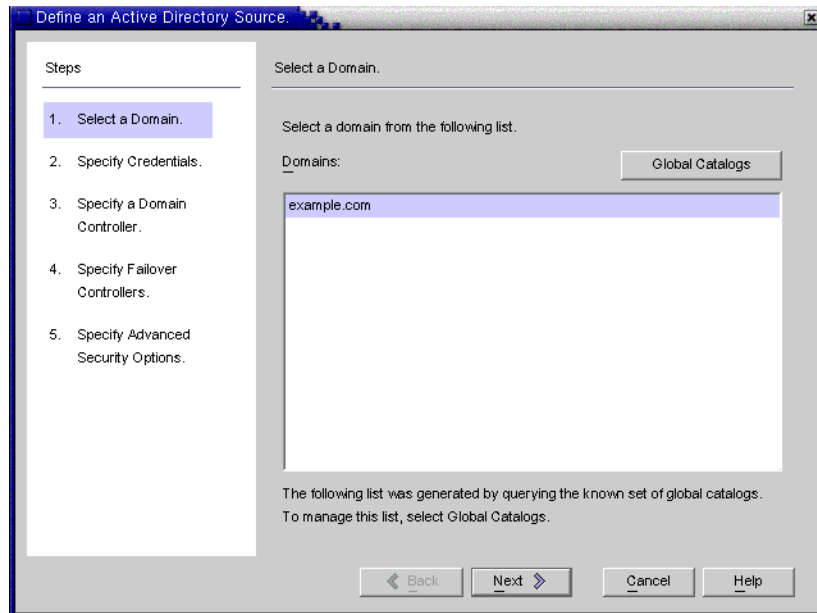
1. Select the Directory Sources node in the navigation tree, and then click the New Active Directory Source button on the Directory Sources panel.

The Windows Global Catalog dialog box is displayed.

Figure 4–16 Windows Global Catalog



2. Enter the following information and then click OK:
 - **Host:** Enter the fully qualified host name of the machine that holds the global catalog for the Active Directory forest.
For example: **machine2.example.com**
 - **This port uses SSL:** Enable this option if Identity Synchronization for Windows is using an SSL port to communicate with the global catalog.
 - **User DN:** Enter your fully qualified Administrator's (bind) distinguished name. (Any credentials that enable you to browse the schemas and determine which Active Directory domains are available on your system will suffice.)
For example: **cn=Administrator,cn=Users,dc=example,dc=com**
 - **Password:** Enter a password for the specified user.
3. The Define Active Directory Source wizard is displayed, as follows.

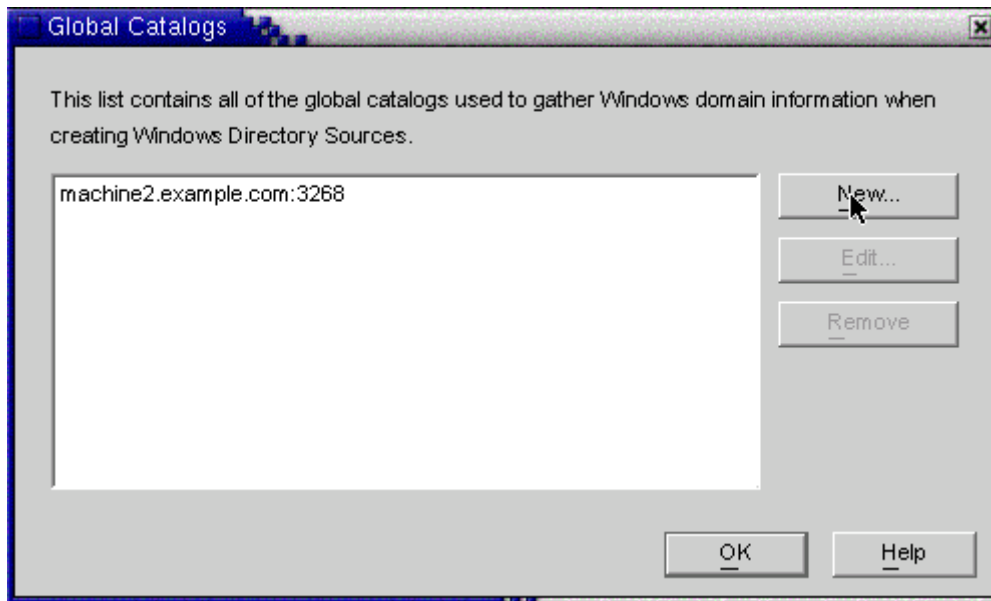
Figure 4–17 Define an Active Directory Source Wizard

This wizard queries the Active Directory global catalog to determine what other domains exist, and displays those domains in the Domains list pane.

4. Select a name from the list pane to specify an Active Directory domain and click OK.

If the domain you want to use is not displayed in the list, you must add the global catalog that knows about that domain using the following steps:

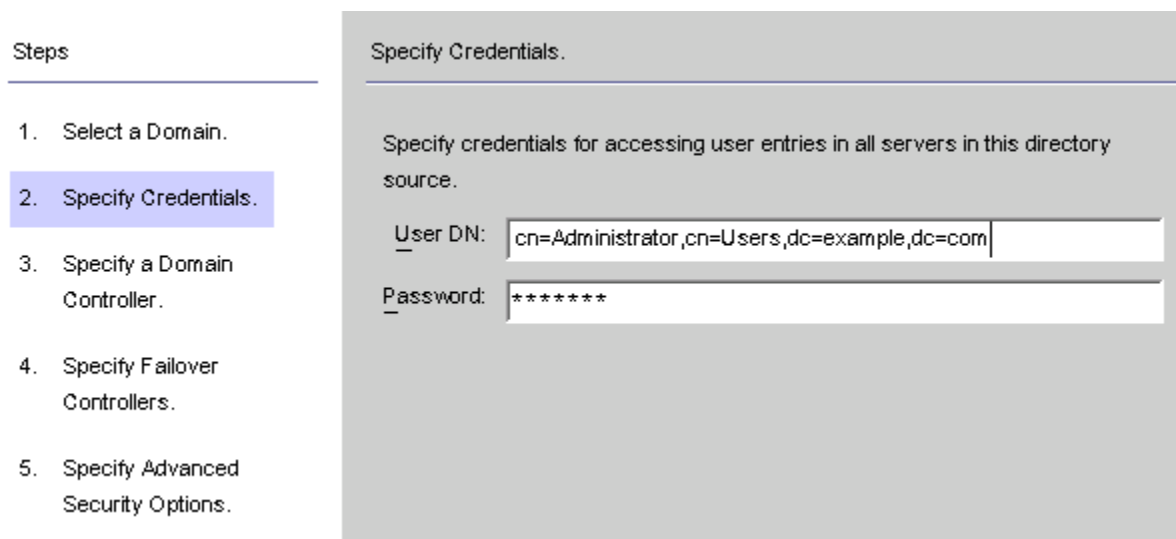
- a. Click the Global Catalogs button and the Global Catalogs wizard is displayed.

Figure 4–18 Specifying a New Global Catalog

- b. Click the New button.

- c. When the Windows Global Catalog dialog box is displayed, provide the global catalog's Host name and your Directory Source credentials (as described in Step 2), and then click OK
 - d. The new global catalog and port, are displayed in the Global Catalogs list panel. Select the catalog name, and then click OK.
 - e. Repeat these steps if you want to add more global catalogs (domains) to the system.
 - f. When you are done, click the Next button in the Select a Domain pane.
5. When the Specify Credentials panel is displayed, review the value in the User DN field.

Figure 4–19 *Specifying Credentials for This Active Directory Source*



If the program did not automatically enter the Administrator's distinguished name in the User DN field (or you do not want to use the Administrator's credentials) enter a User DN and password manually.

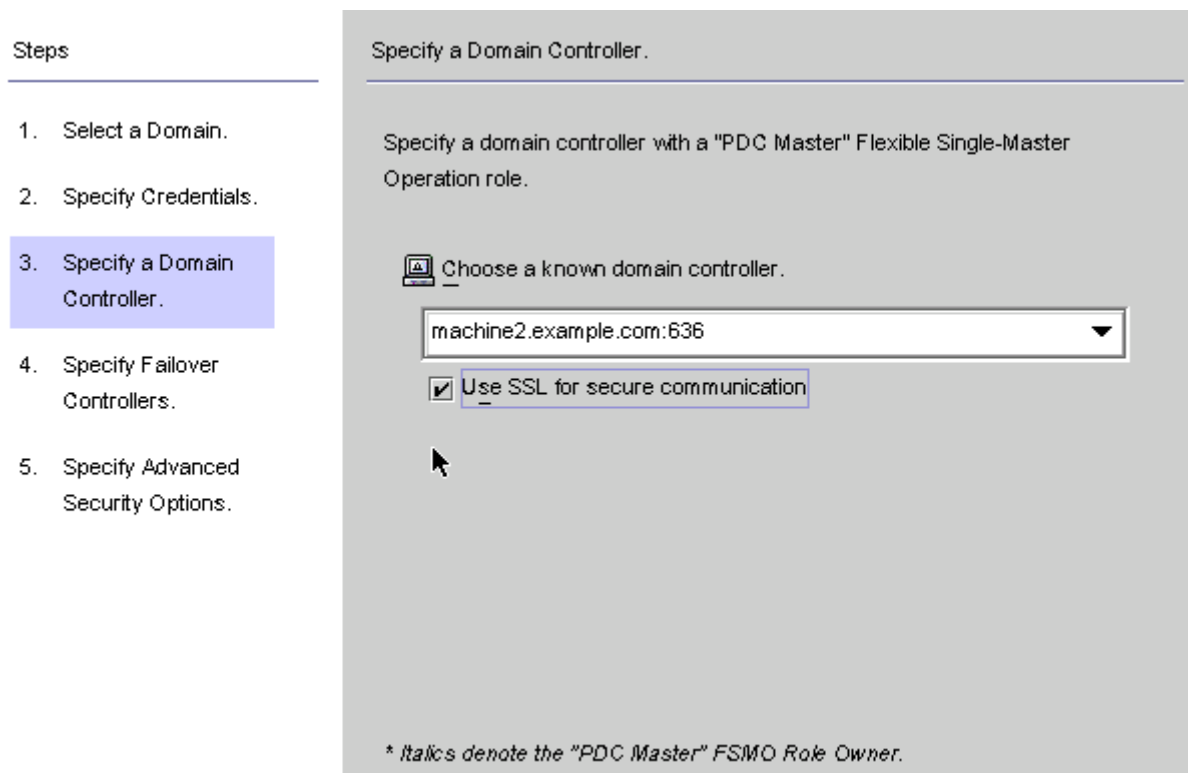
When configuring an Active Directory source, you must provide a user name and password that the Active Directory Connector can use to connect to Active Directory.

Note: The Connector requires specific access rights. Minimum rights will depend on the direction of synchronization, as follows:

- If you are configuring synchronization flow from Active Directory to Directory Server only, then the user provided for the Active Directory Connector does not require many special privileges. A normal user with the extra privilege to "Read All Properties" in the domain being synchronized will suffice.
 - If you are configuring synchronization flow from Directory Server to Active Directory, then the Connector user must have more privileges because, synchronization changes the user entries in Active Directory. In this setup, the Connector user must have either the "Full Control" privilege or be a member of the Administrators group.
-

- Click Next to open the Specify a Domain Controller panel.

Figure 4–20 *Specifying a Domain Controller*



Use this panel to select a controller to synchronize within the specified domain. (The domain controller is similar in concept to a Directory Server's preferred server.)

If the selected Active Directory domain has multiple domain controllers, select the domain controller with the Primary Domain Controller flexible single master operation (FSMO) role for synchronization.

By default, password changes made at all domain controllers will be replicated immediately to the Primary Domain Controller FSMO role owner, and if you select this domain controller, Identity Synchronization for Windows will synchronize these password changes immediately to the Directory Server.

In some deployments, the `AvoidPdcOnWan` attribute may be set in the Windows registry because there is a significant network "distance" to the PDC, which will delay synchronization significantly. (See *Microsoft Knowledge Base Article 232690* for more information.)

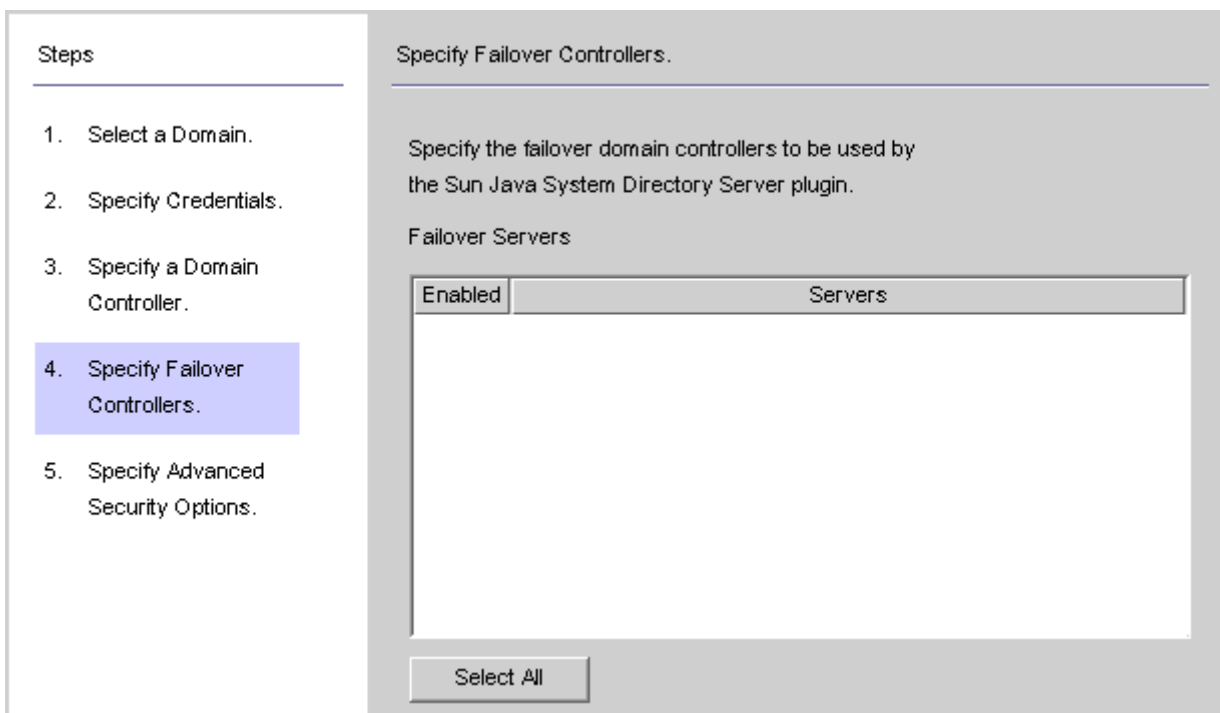
- Select a domain controller from the drop-down list.
- If you want the Identity Synchronization for Windows Connector to communicate with the domain controller over a secure port, enable the Use a Secure Port box.

Note: The program automatically installs the CA certificate in the Active Directory Connector if you are using Microsoft certificate server. If you are not, then you must manually add the CA certificate in the Active Directory Connector (see [Enabling SSL in the Active Directory Connector](#) change your flow settings after initial configuration these procedures apply as well).

9. When you are done, click Next.

The Specify Failover Controllers panel is displayed (see [Creating an Active Directory Source](#)). You can use this panel to specify any number of failover domain controllers.

Figure 4–21 *Specifying Failover Controllers*



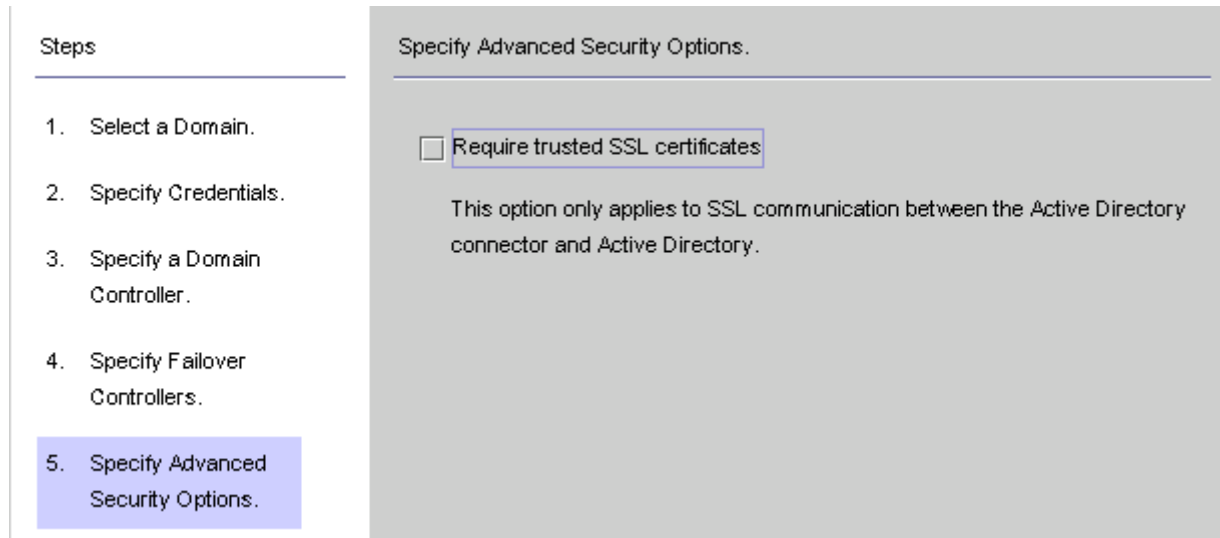
The Active Directory Connector communicates with only one Active Directory domain controller, and Identity Synchronization for Windows does not support failover changes applied by that Connector. However, the Directory Server Plug-in will communicate with any number of domain controllers when validating password changes to Directory Server.

If Directory Server tries connecting to an Active Directory domain controller and that domain controller is not available, Directory Server will iteratively try connecting to the failover domain controller(s) specified.

10. Select one or more of the server names listed in the Failover Servers list pane (or click the Select All button to specify all of the servers in the list), and then click Next.
11. The Specify Advanced Security Options panel is displayed.

The Require trusted SSL certificates option is active (available for selection) only if you enabled the Use SSL for Secure Communication box on the Specify a Domain Controller panel.

Figure 4–22 Specifying Advanced Security Options



- If the Require trusted SSL certificate box is disabled (*Default setting*), the Active Directory Connector will connect to Active Directory over SSL and does not verify that it trusts the certificates passed by Active Directory.

Disabling this option simplifies the setup process because you do not have to put an Active Directory Certificate in the Active Directory certificate database.

- If you enable the Require trusted SSL certificate box, the Active Directory Connector will connect to Active Directory over SSL and it must verify that it trusts the certificates passed by Active Directory.

Note: You must add Active Directory Certificates to the Active Directory Connector's certificate database. For instructions, see [Adding Active Directory Certificates to the Connector's Certificate Database](#).

12. When you are finished with the Advanced Security Options panel, click the Finish button.

The program adds the newly specified Active Directory source to the navigation tree under Directory Sources.

13. Select the Active Directory source node to view the Active Directory Source panel.

Figure 4–23 Active Directory Source Panel

△ Active Directory Source: example.com

Edit Controller...

Domain Controller: machine2.example.com:389

Resync interval: 1000 (milliseconds)

Directory Source Credentials

User DN: cn=Administrator,cn=Users,dc=example,dc=com

Password: *****

From this panel, you can perform the following tasks:

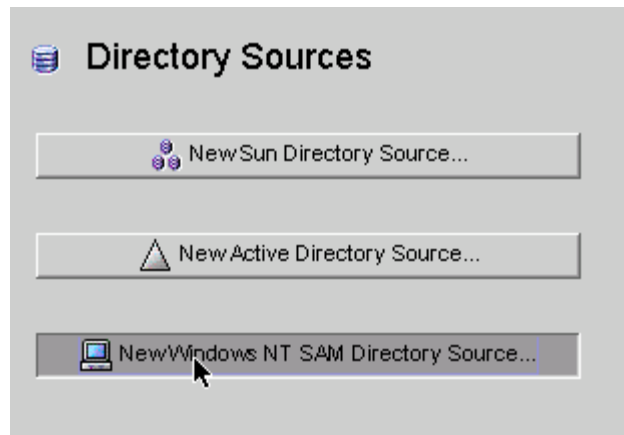
- **Edit Controllers:** Click this button to reopen the Specify a Domain Controller panel where you can change any of the domain controller configuration parameters. If necessary, review the instructions provided for [Creating an Active Directory Source](#).
- **Resync Interval:** Specify how often you want the Active Directory Connector to check for changes. (Default is 1000 milliseconds)
- **Directory Source Credentials:** Change the specified User DN and/or password.

4.3.5 Creating a Windows NT SAM Directory Source

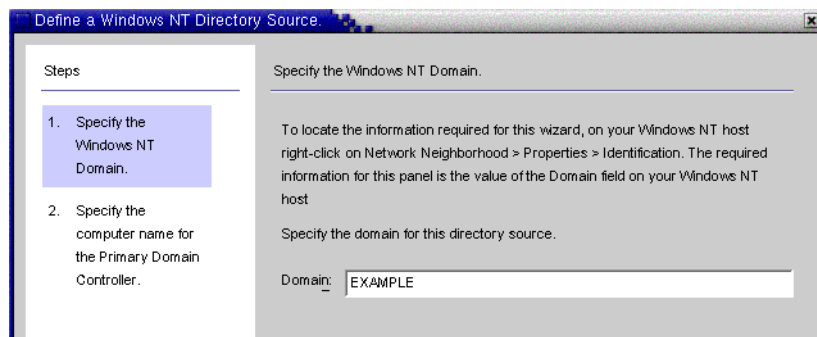
This section explains how to create a Windows NT SAM Directory Source where you can deploy Identity Synchronization for Windows.

4.3.5.1 To Deploy Identity Synchronization for Windows on Windows NT

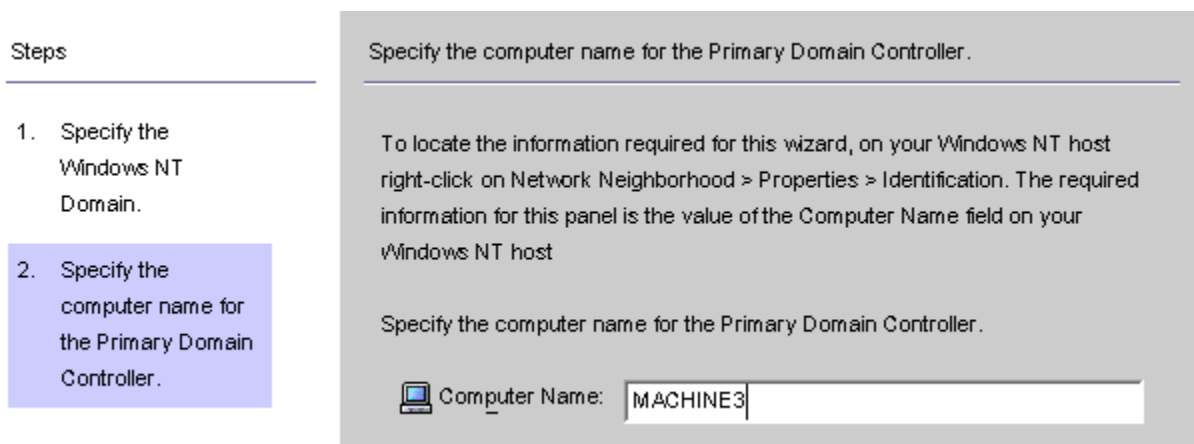
1. Select the Directory Sources node in the navigation tree, and then click the New Windows NT SAM Directory Source button.

Figure 4–24 Directory Sources Panel

2. When the Define a Windows NT SAM Directory Source panel is displayed, follow the instructions for locating the Windows NT domain name, and enter the unique NT directory source domain name in the Domain field. When you are done, click Next.

Figure 4–25 Specifying a Windows NT SAM Domain Name

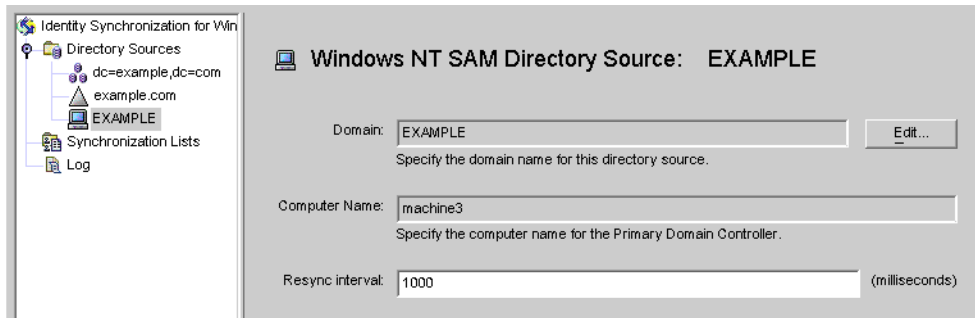
3. When the Specify the Computer Name for the Primary Domain Controller panel is displayed, follow the instructions for locating the Primary Domain Controller computer name, and enter the information in the Computer Name field.

Figure 4–26 Specifying a Name for the Primary Domain Controller

4. Click Finish.

The program adds the newly specified Windows NT SAM directory source to the navigation tree under Directory Sources. Select the new directory source node to view the Windows NT SAM Source panel.

Figure 4–27 Windows NT SAM Directory Source Panel



From this panel, you can perform the following tasks:

- *Edit:* Click this button to reopen the Specify a Domain Controller panel where you can change any of the domain controller configuration parameters. If necessary, review the instructions provided for [Creating an Active Directory Source](#).
 - *Resync interval:* Specify how often you want Identity Synchronization for Windows to check for changes made on Windows NT. (Default is 1000 milliseconds)
5. Add a Windows NT directory source for each Windows NT machine in your network.

When you are finished creating Windows NT SAM directory sources, you are ready to create and map attributes to be synchronized, continue to [Selecting and Mapping User Attributes](#)

4.4 Selecting and Mapping User Attributes

After you have created and configured your Directory Server and Windows directory sources, you must decide which user attributes you want to synchronize and then map those attributes between systems.

The information in this section is organized as follows:

- [Selecting and Mapping Attributes](#)
- [Creating Parameterized Default Attribute Values](#)
- [Changing the Schema Source](#)

4.4.1 Selecting and Mapping Attributes

There are two types of attributes:

- **Significant:** Attributes that are synchronized between systems when you create or modify user entries.
- **Creation:** Attributes that are synchronized between systems only when you create user entries.

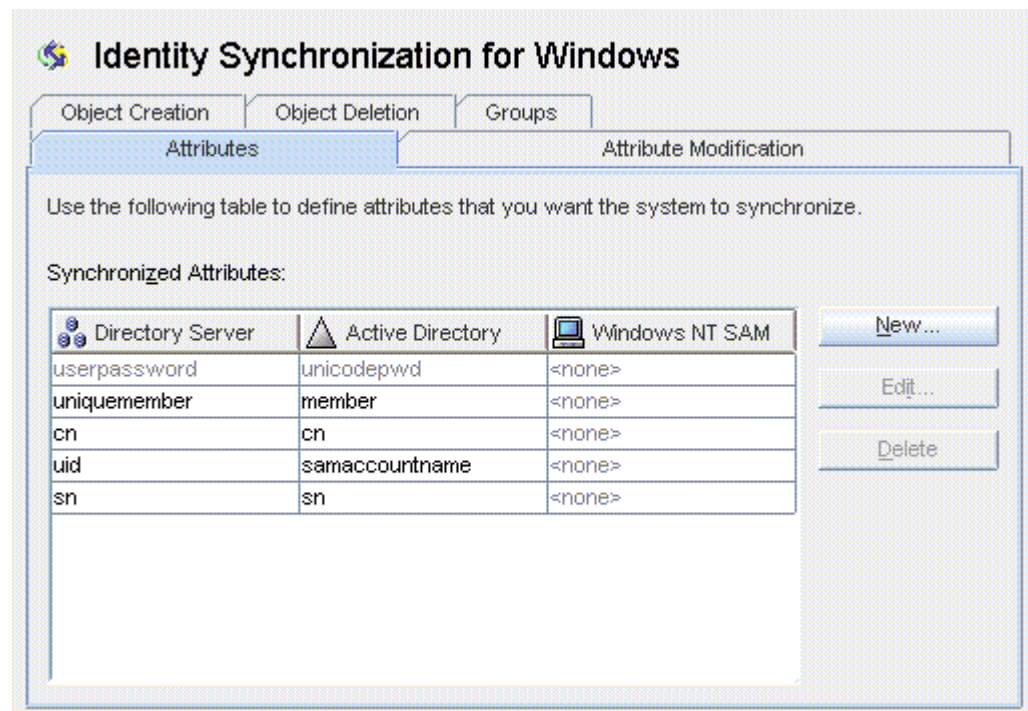
Some creation attributes are *mandatory* based on the schema used for each platform. These attributes are required for password synchronization and they must be mapped to Directory Server attributes to successfully create a user object class entry on the Active Directory server.

This section explains how to select user attributes for synchronization and how to map these attributes (one-to-one) so that when you specify an attribute for Directory Server the equivalent attribute will display in your Active Directory and/or Windows NT environment (and vice versa), and the companion Windows attributes will have their values synchronized.

4.4.1.1 To Select and Map Attributes for Synchronization

1. Select the Identity Synchronization for Windows node at the top of the navigation tree.

Figure 4–28 Attributes Tab

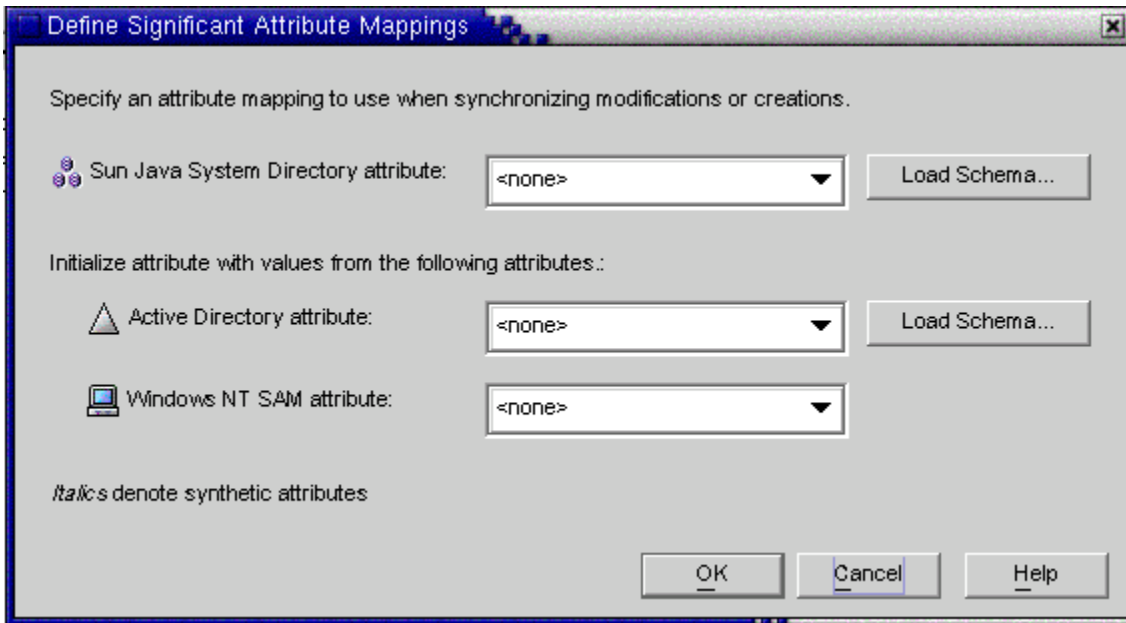


Note: When the Group Synchronization feature has been enabled, the *uniquemember* (Directory Server) attribute and *member attribute* (Active Directory) are internally mapped and would be indicated as shown in the console.

2. Select the Attributes tab and then click the New button.

The Define Significant Attribute Mappings dialog box is displayed. Use this dialog box to map attributes from Directory Server to your Windows Systems (Active Directory and/or Windows NT).

Figure 4–29 Defining Significant Attribute Mappings



Note: Which creation attributes are mandatory for Directory Server (or for Active Directory) will depend on the objectclass configured for your Sun-side (or Active Directory-side) user entries.

The program automatically uses *inetOrgPerson* as the default objectclass for Directory Server, and you loaded the Active Directory schema when you specified the global catalog. So you do not use the Load Schema buttons unless you want to change the default schema.

If you want to change the default schema source, see [Changing the Schema Source](#)

3. Select an attribute from the Sun Java System attribute drop-down list (for example *cn*), and then select the equivalent attribute from the Active Directory attribute and/or Windows NT SAM attribute drop-down menus.
4. When you are finished, click OK.
5. To designate additional attributes, repeat steps 2 through step 4.

A finished Synchronized Attributes table might look something like the following example, which shows the *userpassword*, *cn*, and *telephonenumber* Directory Server attributes mapped to *unicodepwd*, *cn*, and *telephonenumber* Active Directory attributes.

Figure 4–30 Completed Synchronized Attributes Table

Directory Server	Active Directory	Windows NT SAM
<i>userpassword</i>	<i>unicodepwd</i>	<i>user_password</i>
<i>cn</i>	<i>cn</i>	<none>
<i>telephonenumber</i>	<i>telephonenumber</i>	<none>

4.4.2 Creating Parameterized Default Attribute Values

Identity Synchronization for Windows allows you to create *parameterized* default values for attributes using other creation or significant attributes.

To create a parameterized default attribute value, you embed an existing creation or significant attribute name—preceded and followed by percent symbols (`% attribute_name %`)—in an expression string. For example, `homedir=/home/%uid%` or `cn=%givenName% %sn%`.

When you create these attribute values:

- You can use multiple attributes in a creation expression (`cn=%givenName% %sn%`).
- If A=0, then B can have one default value only.
- You can use the backslash symbol (`\\`) for quoting (for example, `diskUsage=0\\%`).
- Do not use expressions that have cyclic substitution conditions (for example, if you specify `description=%uid%`, you cannot use `uid=%description%`.)

Note: When Group Synchronization is enabled, the following are important:

1. The creation expression supported at Active Directory is `cn=%cn%`.
2. The creation expression must contain valid attribute names belonging to the group objectclass also since the creation expression is common to both user as well as the group.

For example: The attribute `sn` is not part of the `groupofuniqueNames` objectclass at the Directory Server. Hence the following creation expression would be invalid for a group object. (Though it would work fine for user.)

```
cn=%cn%. %sn%
```

3. The attribute used in the creation expression must be provided with a value for every user/group entry created. The value maybe provided using the command line interface, if the console does not have the provision.
-

4.4.3 Changing the Schema Source

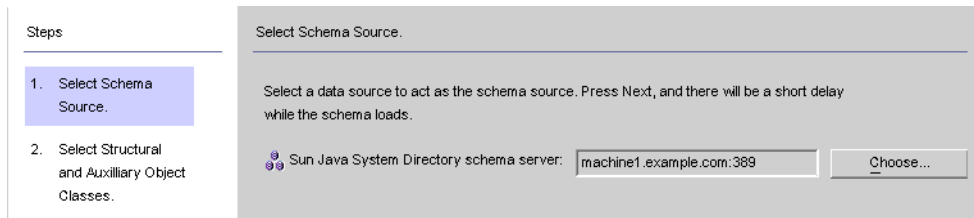
The program automatically provides default schema sources, but allows you to change the default schema.

4.4.3.1 To Change the Default Schema Source

1. Click the Load Schema button on the Define Significant Attribute Mappings dialog box.

The Select Schema Sources panel is displayed.

Figure 4–31 Selecting Schema Sources



Use this panel to specify from which Sun Java System Directory Server schema server you want to read the schema. This schema contains the object classes that are available on your system, and object classes define which attributes are available for users on your system.

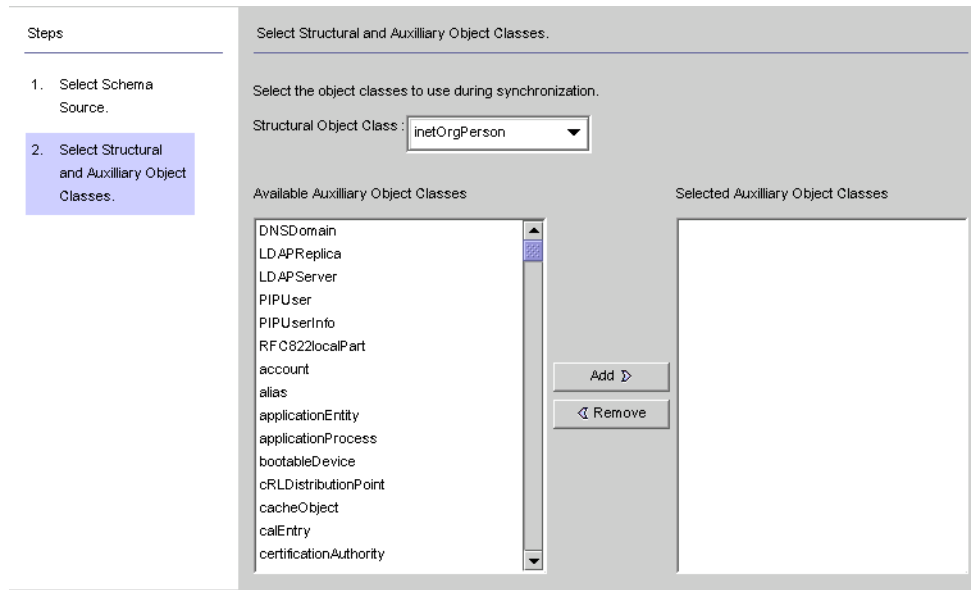
The program adds your configuration directory to the Sun Java System Directory schema server field by default.

2. To select a different server, click the Choose button.

The Select a Sun Schema Host dialog box is displayed. This dialog box contains a list of the configuration directories that gather administrative information about your directory sources.

From this dialog box, you can:

- Create new configuration directories and add them to the list.
Click New, and when the New Configuration Directory dialog box displays; specify a Host, Port, User DN, and Password. Click OK when you are done.
 - Edit existing directories.
Click Edit, and when the Edit Configuration Directory dialog box displays, you can change the Host, Port, User DN, and/or Password. Click OK when you are done.
 - Remove directories from the list.
Select a directory name from the list and then click the Remove button.
3. Select a server from the list and click OK when you are done. (Generally, one of your Sun synchronization host(s) is a good choice as a schema source.)
 4. Click the Next button and the Select Structural and Auxiliary Object Classes panel is displayed.

Figure 4–32 Selecting Structural and Auxiliary Object Classes

Use this panel to specify the object classes to synchronize, as follows:

- **Structural Object Class:** Every entry that is created or synchronized from the selected Directory Server must have at least one structural object class.
- **Auxiliary Object Classes:** These object classes augment the selected structural class and provide additional attributes for synchronization.

To specify structural and auxiliary object classes:

- a. Select a structural object class from the drop-down list. (*Default is inetorgperson.*)
- b. Select one or more object classes from the Available Auxiliary Object Classes list pane, and then click Add to move your selection(s) to the Selected Auxiliary Object Classes list pane.

The selected object class(es) determine which Directory Server source attributes will be available for selection as significant or creation attributes. The object class(es) also determine the mandatory creation attributes.

To delete selections from the Selected Auxiliary Object Classes list, click the object class name and then click the Remove button.

- c. When you are done, click Finish and the program loads the schema and selected object classes.

4.5 Propagating User Attributes Between Systems

After you create and map the user attributes you want to synchronize, you must tell Identity Synchronization for Windows how to propagate (flow) the attribute creations, modifications, and deletions between your Directory Server and Windows Systems.

By default, Identity Synchronization for Windows:

- Synchronizes from Windows to Directory Server only
- Synchronizes the password attribute only (unless you specified significant attributes in the previous section)

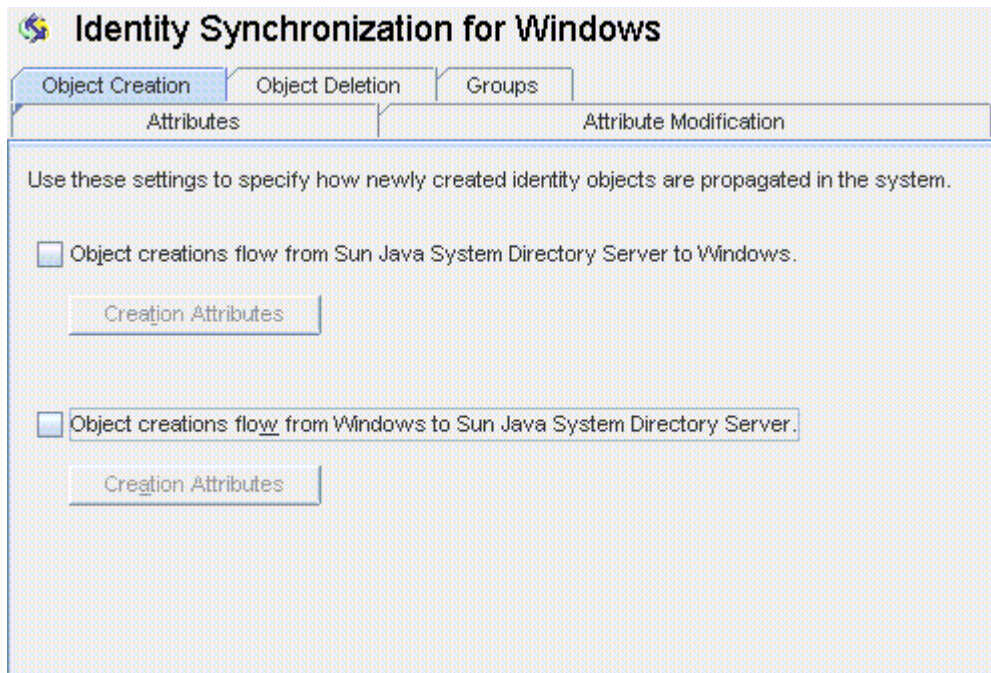
- Does not synchronize the creation or deletion of entries
- This section explains how to configure attribute synchronization between systems. The information is organized as follows:
- [Specifying How Object Creations Flow](#)
 - [Specifying How Object Modifications Flow](#)
 - [Specifying Configuration Settings for Group Synchronization](#)
 - [Configuring and Synchronizing Account Lockout and Unlockout](#)
 - [Specifying How Deletions Flow](#)

4.5.1 Specifying How Object Creations Flow

4.5.1.1 To Specify How Object Creations Should Flow Between Directory Server and Active Directory Systems

1. Click the Object Creation tab.

Figure 4–33 *Selecting and Propagating Creations*



2. You can enable or disable the flow of creations as follows:
 - Enable **Object creations flow from Sun Java System Directory Server to Windows** to propagate creations from the Directory Server environment to your Windows servers.
 - Enable **Object creations flow from Windows to Sun Java System Directory Server** to propagate creations from the Windows environment to your Directory Servers.
 - Enable both options for bidirectional flow.

- Disable both options to prevent user creations from propagating from one system to the other. (Default).
3. To add, edit, or delete creation attributes to synchronize between systems, click the Creation Attributes button located under the selected option(s).

The Creation Attribute Mappings and Values dialog box displays.

Figure 4-34 Creation Attributes Mappings and Values: Directory Server to Windows

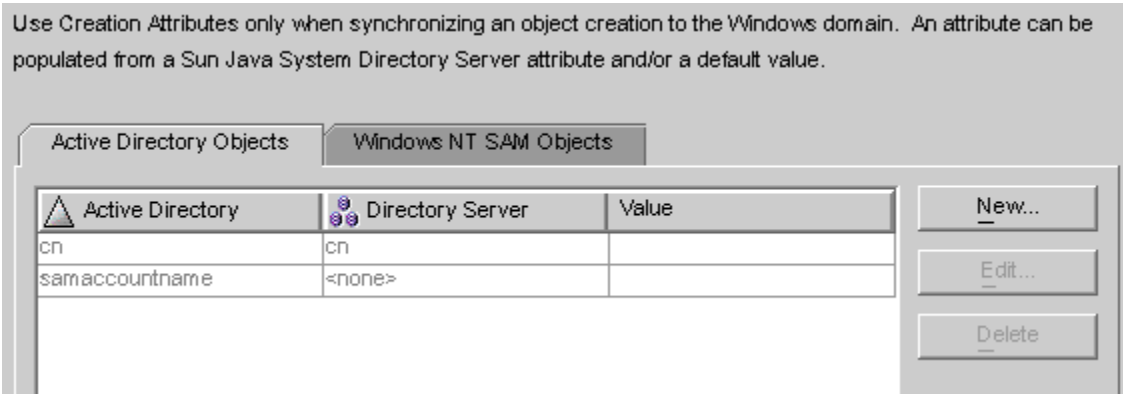
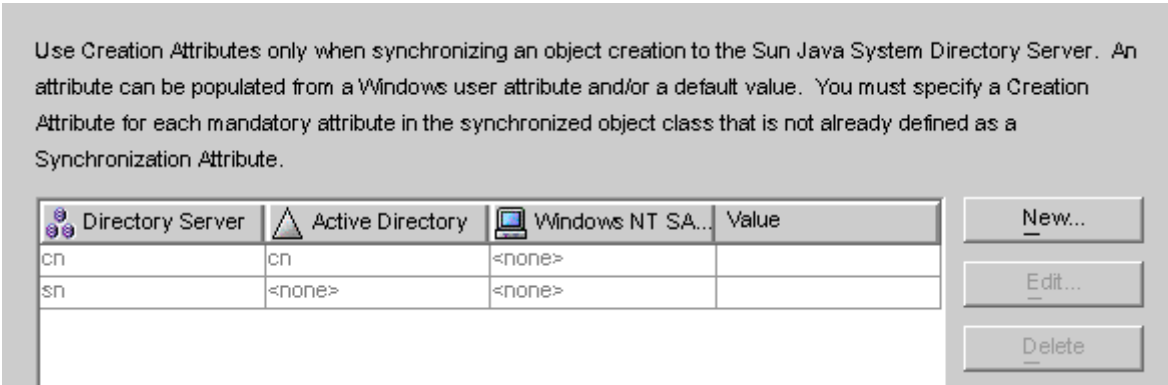


Figure 4-35 Creation Attributes Mappings and Values: Windows to Directory Server



You can use either of the dialog boxes to specify new creation attributes, edit, or delete existing attributes. For more information, see [Specifying New Creation Attributes](#).

Note: To satisfy schema constraints regarding required attributes for user object classes, you may have to specify additional attributes to flow through the system during a user creation.

Additional attributes are not necessary if you specified the required attributes as *modification* attributes (as described in [Selecting and Mapping User Attributes](#)).

4.5.1.2 Specifying New Creation Attributes

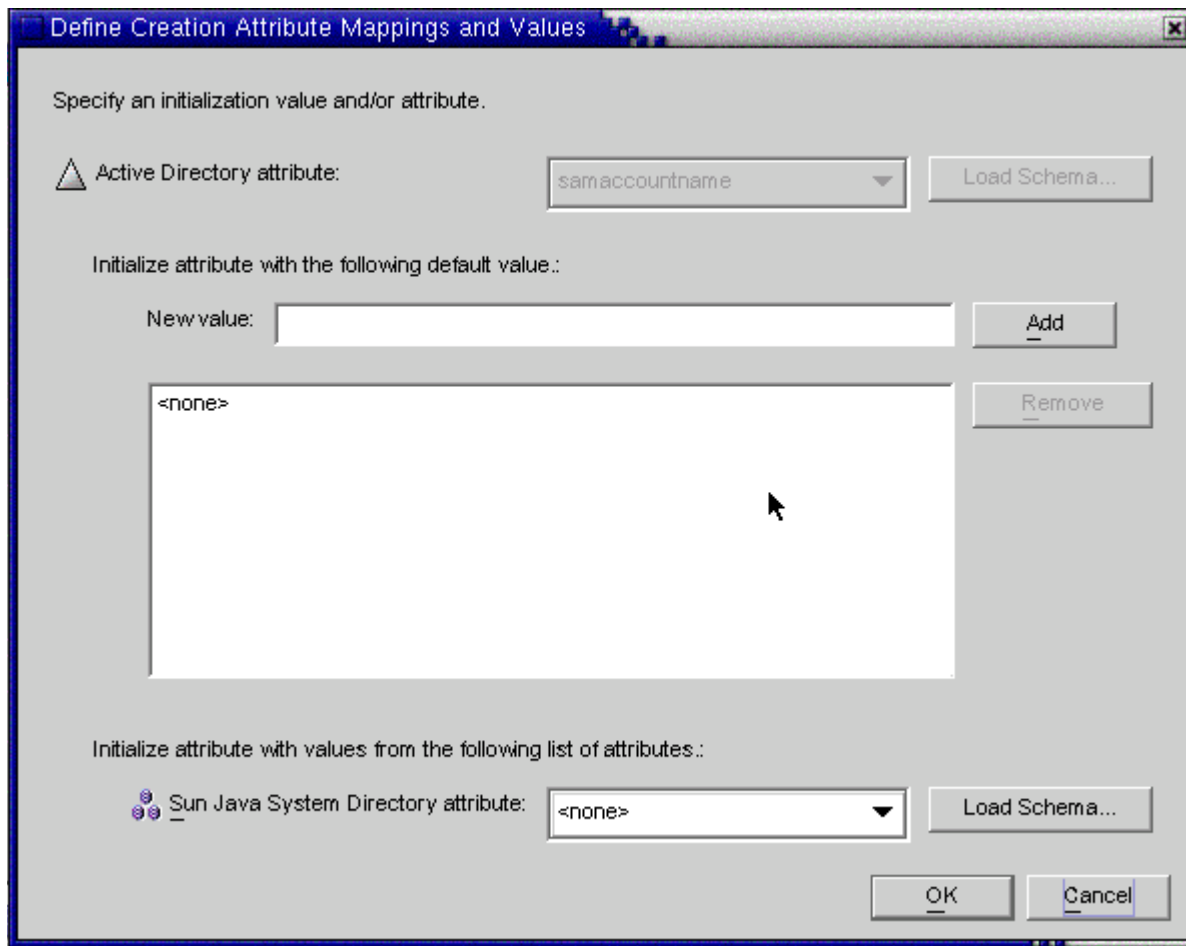
The following instructions explain how to add and map creation attributes from Active Directory to Directory Server. (The procedure for adding and mapping creation

attributes flowing from Directory Server to Windows and from Windows to Directory Server is similar.)

4.5.1.2.1 To Specify New Creation Attributes

1. Click the New button in the Creation Attribute Mappings and Values dialog box. The Define Creation Attribute Mappings and Values dialog box is displayed.

Figure 4–36 Defining Creation Attribute Mappings and Values



2. Select an attribute value from the Active Directory attribute drop-down list.

Figure 4–37 Selecting a New Active Directory Attribute



Identity Synchronization for Windows allows you to initialize an attribute with multiple values— if the attribute itself accepts multiple values.

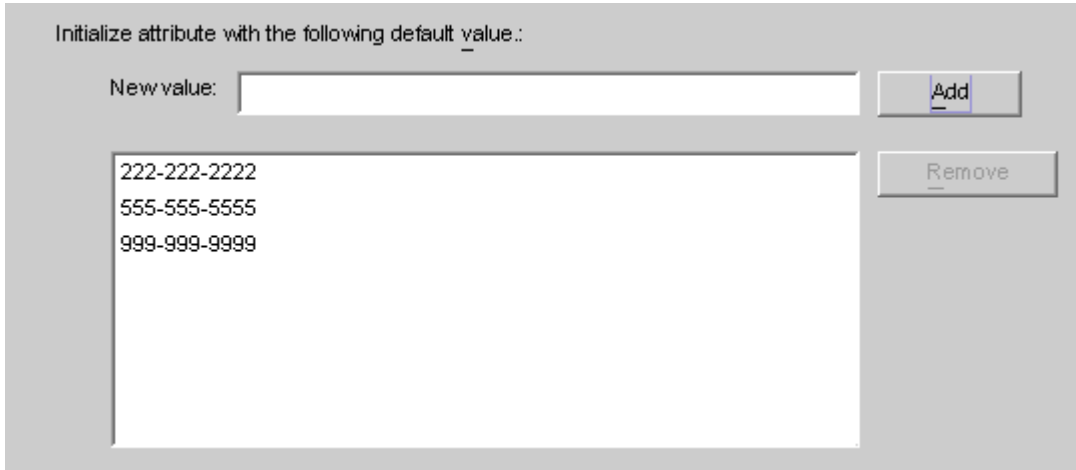
For example, if your company has three fax telephone numbers, you can specify the `facsimiletelephonenumber` attribute for both Sun Java System Directory Server and Active Directory, and specify the three numbers.

You must know which attributes will accept multiple values. If you try adding multiple values to an attribute that does not accept them, an error will result during runtime when the program attempts to create the object.

- 3. Enter a value in New value field and click Add.

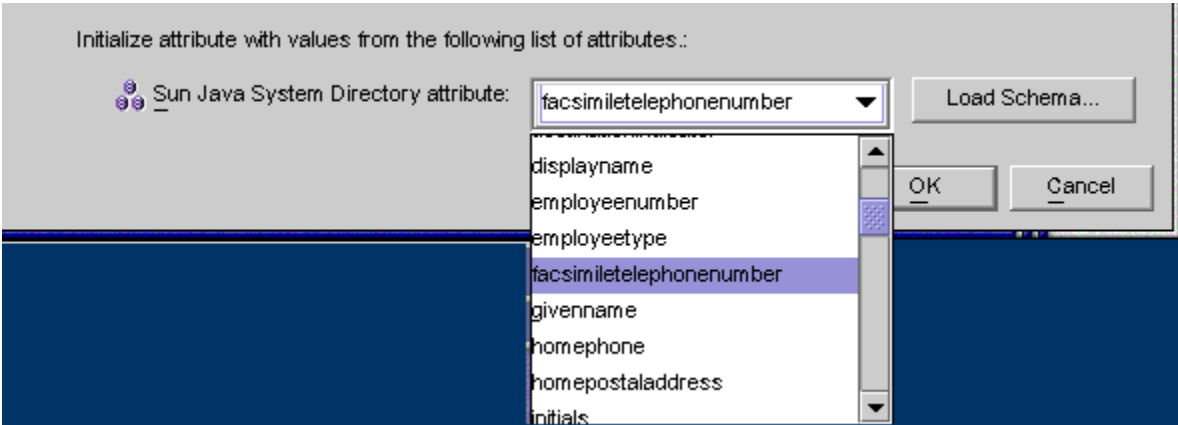
The program adds the attribute value to the list pane. Repeat this step as many times as necessary to add multiple attribute values.

Figure 4-38 Specifying Multiple Values for a Creation Attribute



- 4. To map the attribute to Directory Server, select an attribute name from the Directory Server attribute drop-down list.

Figure 4-39 Mapping the Directory Server Attribute



- 5. When you are finished, click OK.

Based on the example, the finished Creation Attributes and Mappings table would look like the one in the following figure.

Figure 4–40 Completed Creation Attributes and Mappings Table

 Active Directory	 Directory Server	Value
cn	cn	
samaccountname	<none>	
facsimiletelephonenumber	facsimiletelephonenumber	[222-222-2222,555-555-55...

- To designate additional attributes, repeat these steps.

4.5.1.3 Editing Existing Attributes

4.5.1.3.1 To Edit Creation Attributes Mapping or Values

- Select the Object Creation tab, and click on the Creation Attributes button located under the selected creation option.
- When the Creation Mappings and Values dialog box is displayed, select the attribute from the table, and then click the Edit button.

The Define Creation Mappings and Values dialog box is displayed.

- Use the drop-down menus to change the existing mapping between Directory Server and Active Directory (or Windows NT).

For example, if you have Sun Java System Directory Server's homephone attribute mapped to Active Directory's othertelephone attribute. You could use the Active Directory attributes drop-down list to change the mapping to homephone.

- You can also add or remove attribute values:
 - To add a value, enter the information in the New Value field and click Add.
 - To remove a value, select the value from the list pane and click Remove.
- When you are done, click OK to apply your changes and close the Define Creation Mappings and Values dialog box.
- Click OK again to close the Creation Mappings and Attributes dialog box.

4.5.1.4 Removing Attributes

4.5.1.4.1 To Remove Creation Attributes Mapping or Values

- Select the Object Creation tab, and click the Creation Attributes button located under the selected creation option.
- When the Creation Mappings and Values dialog box is displayed, select the attribute from the table, and then click the Delete button.

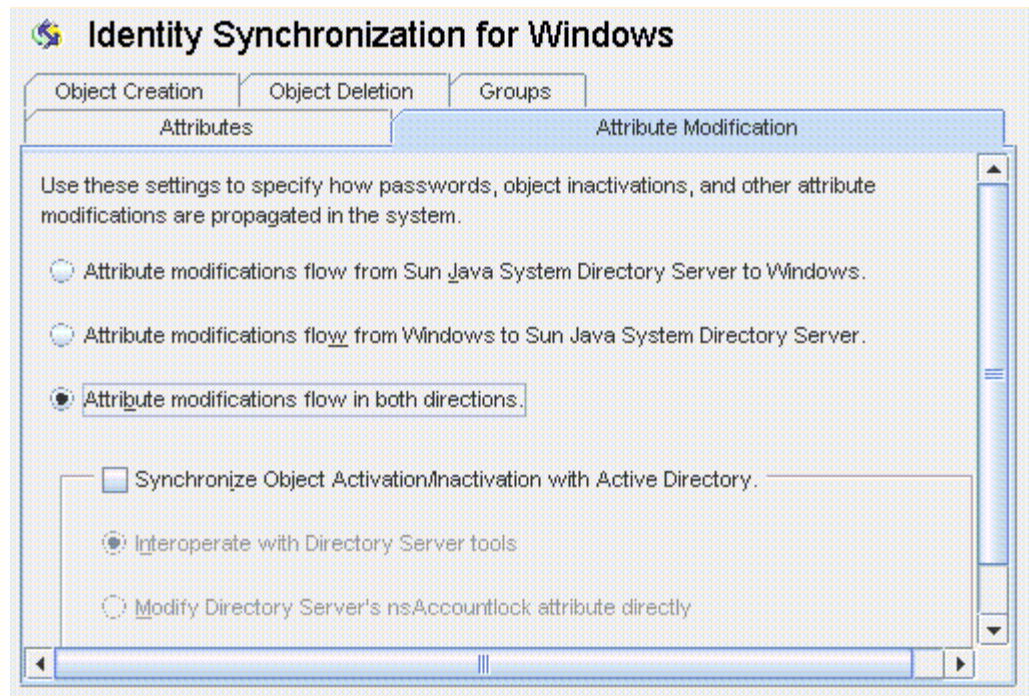
The attribute is removed from the table immediately.

- When you are done, click OK to close the Creation Mappings and Attributes dialog box.

4.5.2 Specifying How Object Modifications Flow

Use the Attribute Modification tab to control how modifications made to user attributes and passwords will be propagated (flow) between your Sun and Windows systems.

Figure 4–41 Attribute Modification Tab



You use this tab to configure the following:

- Specify the direction in which modifications flow between Directory Server and Windows directory sources.
- Control whether object activations and inactivations (*enables* and *disables* on Active Directory) will be synchronized between Directory Server and Active Directory sources, and specify the method in which user accounts are activated and inactivated.

Note: You cannot synchronize account statuses with Windows NT directory sources.

4.5.2.1 Specifying Direction

Select one of the following buttons to control how changes made in the Directory Server and Windows environments will be propagated between systems.

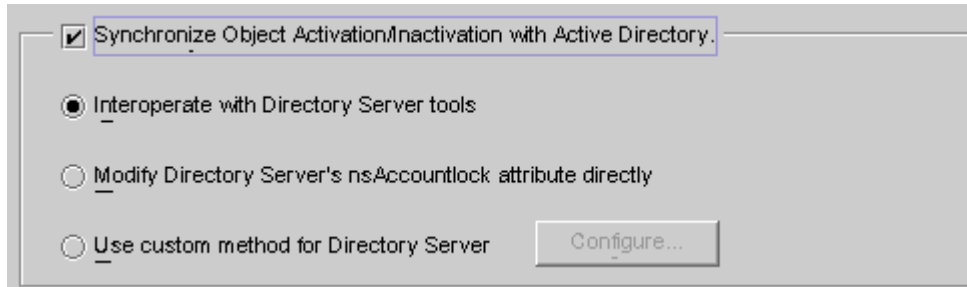
- **Attribute modifications flow from Sun Java System Directory Server to Windows:** Propagates changes made in the Directory Server environment to your Windows servers.
- **Attribute modifications flow from Windows to Sun Java System Directory Server (Default):** Propagates changes made in the Windows environment to your Directory Servers.
- **Attribute modifications flow in both directions :** Propagates changes bidirectionally (from one environment to the other environment).

4.5.2.2 Configuring and Synchronizing Object Activations and Inactivations

If you enable the Synchronize Object Activations/Inactivations with Active Directory box you can synchronize object activations and inactivations (known as *enables* and *disables* on Active Directory) between Directory Server and Active Directory sources.

Note: You cannot synchronize activations and inactivations with Windows NT directory sources.

Figure 4–42 Synchronizing Object Activations and Inactivations



4.5.2.2.1 To Synchronize Object Activations/Inactivations:

1. Enable the Synchronize Object Inactivations between Directory Server & Active Directory box.
2. Enable one of the following buttons to specify how Identity Synchronization for Windows will detect and synchronize object activations and inactivations:
 - [Interoperating with Directory Server Tools](#)
 - [Modifying Directory Server's NsAccountLock Attribute Directly](#)

Note: These options are mutually exclusive.

- [Using a Custom Method for Directory Server](#)

4.5.2.2.2 Interoperating with Directory Server Tools Select this option if you use the Directory Server Console or command line tools to activate/inactivate an object. With this option selected Identity Synchronization for Windows cannot set or remove the `nsAccountLock` attribute directly. In addition, the program cannot detect objects that have been inactivated using other roles such as `cn=nsdisabledrole, database suffix` or roles that nest within other roles, such as `cn=nsdisabledrole, database suffix` or `cn=nsmanageddisabledrole, database suffix`.

- To activate objects, Identity Synchronization for Windows will remove the `cn=nsmanageddisabledrole, database suffix` value from the `nsroledn` attribute.
- To inactivate objects, Identity Synchronization for Windows will add the `cn=nsmanageddisabledrole, database suffix` value to the `nsroledn` attribute.

Note: If you enable the Interoperate with Directory Server Tools option, Identity Synchronization for Windows cannot set or remove the nsAccountLock attribute directly. In addition, Identity Synchronization for Windows cannot detect objects have been inactivated using other roles.

For example, cn=nsdisabledrole, *database suffix* or roles that nest within other roles such as cn=nsdisabledrole, *database suffix* or cn=nsmanageddisabledrole, *database suffix*.

Interoperating with Directory Server Tools describes how Identity Synchronization for Windows detects and synchronizes object activations/inactivations when you enable the Interoperate with Directory Server Tools option.

Table 4–1 Interoperating with Directory Server Tools

Activations	Inactivations
Identity Synchronization for Windows detects an activation only when the cn=nsmanageddisabledrole, <i>database suffix</i> role is removed from the object.	Identity Synchronization for Windows detects an inactivation only when the entry's nsroledn attribute includes the cn=nsmanageddisabledrole, <i>database suffix</i> role.
When synchronizing an object activation from Active Directory, Identity Synchronization for Windows activates the object by removing the cn=nsmanageddisabledrole, <i>database suffix</i> role from the object.	When synchronizing an object inactivation from Active Directory, Identity Synchronization for Windows inactivates the object by adding the cn=nsmanageddisabledrole, <i>database suffix</i> role to the object.

4.5.2.2.3 Modifying Directory Server's nsAccountLock Attribute Directly Use this method when Directory Server activations and inactivations are based on Directory Server's operational attribute, nsAccountLock.

Note: When the Modify Directory Server's nsAccountLock attribute option is enabled, Identity Synchronization for Windows will not detect objects that are activated/inactivated using the Directory Server Console or command line utilities.

This attribute controls object states as follows:

- When nsAccountLock=true, the object is inactivated and the user cannot log in.
- When nsAccountLock=false (or has no value), the object is activated.

Modifying Directory Server's nsAccountLock Attribute Directly describes how Identity Synchronization for Windows detects and synchronizes object activations/inactivations when you enable the Modify Directory Server's nsAccountLock Attribute Directly option.

Table 4–2 Modifying Directory Server's nsAccountLock Attribute Directly

Activation	Inactivation
Identity Synchronization for Windows detects an inactivated object only when the nsAccountLock attribute is set to true .	Identity Synchronization for Windows detects an activated object only when the nsAccountLock attribute is absent or set to false .

Table 4–2 (Cont.) Modifying Directory Server's nsAccountLock Attribute Directly

Activation	Inactivation
When synchronizing an object inactivation from Active Directory, Identity Synchronization for Windows removes the nsAccountLock attribute.	When synchronizing an object activation from Active Directory, Identity Synchronization for Windows sets the nsAccountLock attribute to true .

4.5.2.2.4 Using a Custom Method for Directory Server Use this method when Directory Server activations and inactivations are controlled exclusively by an external application such as Sun Java System Access Manager (formerly Sun JES Identity Server).

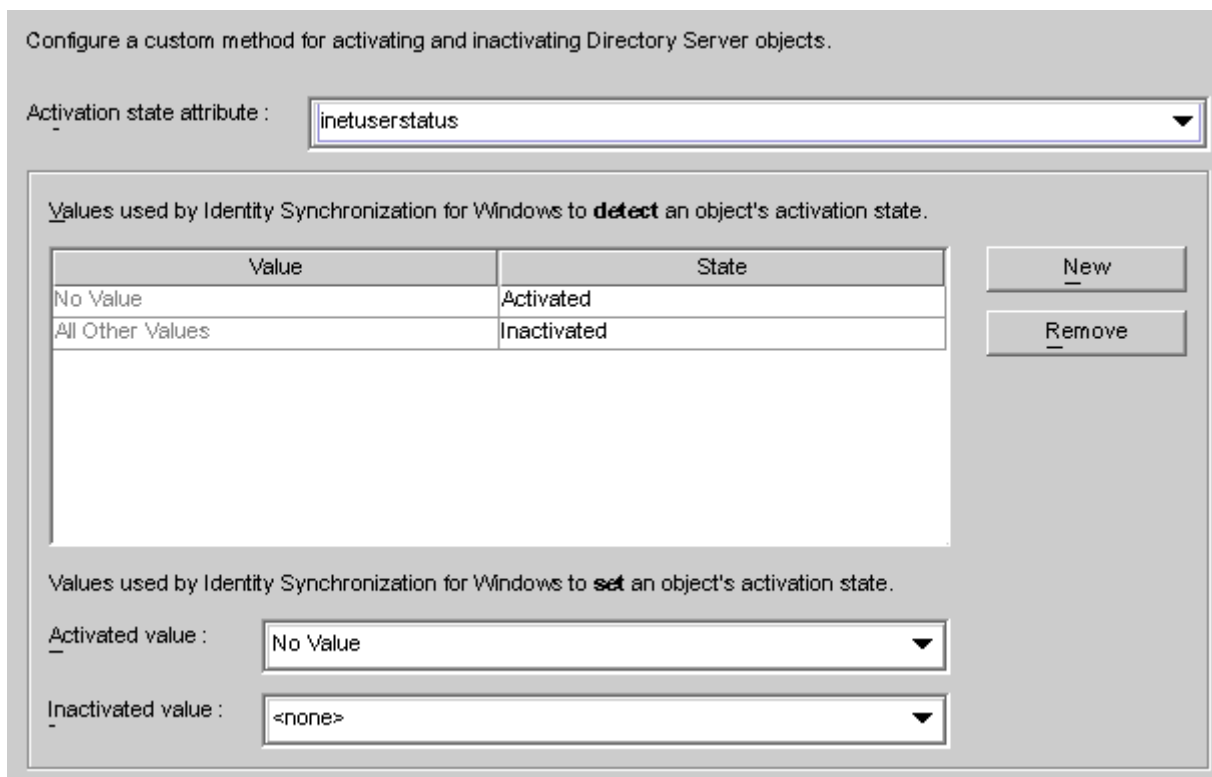
When you configure a custom method for Directory Server, you must specify the following:

- How Identity Synchronization for Windows will detect that the external application has activated or inactivated an object in Directory Server.
- How Identity Synchronization for Windows will activate or inactivate the object when synchronizing from Active Directory to Directory Server.

Note: If you enable the Use custom method for Directory Server option, Identity Synchronization for Windows cannot lock objects out of the directory unless access to the directory is controlled by an external application, such as Access Manager.

To configure a Custom method for activations and inactivations, click the Configure button and the Configure Custom Method for Directory Server dialog box is displayed.

Figure 4–43 Configuring a Custom Method for Activations and Inactivations



This dialog contains the following features:

- **Activation state attribute drop-down list** : Use this list to specify an attribute that Identity Synchronization for Windows will use to synchronize activations and inactivations between Directory Server and Active Directory.

The list contains all attributes in the schema for the currently selected Directory Server structural and auxiliary objectclasses.

- **Value and State table**: Use this table to specify when values associated with the selected attribute are activated or inactivated.

- **Value column**: Use this column (in conjunction with the New and Remove buttons) to specify attribute values that will be used to indicate active or inactive states.

The program automatically provides two values in this column:

No Value: Where the Activation state attribute has no value.

All Other Values: Where the Activation state attribute has a value, but that value is not specified in this Value and State table.

- **State column**: Use this column to specify whether the Value entry (in the same row) corresponds to an object that is activated or inactivated.

Value	State	Result
No Value	Activated	If the attribute is missing or does not have a value, Identity Synchronization for Windows detects the object as activated.

Value	State	Result
	Inactivated	If the attribute is missing or does not have a value, Identity Synchronization for Windows detects the object as inactivated.
<i>user-defined</i> values	Activated	If the attribute has the <i>user-defined</i> attribute, Identity Synchronization for Windows detects the object as activated.
	Inactivated	If the attribute has the user-defined attribute, Identity Synchronization for Windows detects the object as inactivated.
All Other Values	Activated	If the attribute has a value, but that value is not specified in the table, Identity Synchronization for Windows detects the object as activated.
	Inactivated	If the attribute has a value, but that value is not specified in the table, Identity Synchronization for Windows detects the object as inactivated.

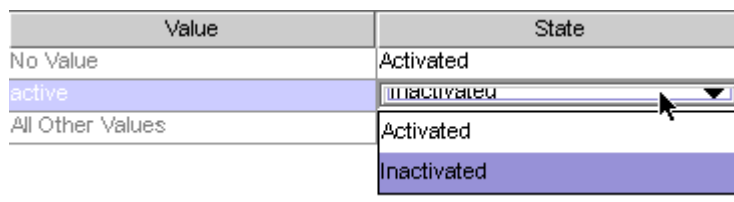
- **New button:** Click this button to add new entries to the Value column.
- **Remove button:** Select an entry in the Value column, and then click this button to remove that entry.
- **Activated value and Inactivated value drop-down lists:** Use these two lists to specify values that Identity Synchronization for Windows will use to *set* an object's state.

Synchronizing Activations and Inactivations

4.5.2.2.5 To Configure Identity Synchronization for Windows to Detect and Synchronize Object States between Directory Server and Active Directory 1. Select an attribute from the Activation state attribute drop-down list.

2. Click the New button to add attribute values to the Value column of the table.
3. Click in the State column next to each of the Value entries and when the drop-down list is displayed, select Activated or Inactivated.

Figure 4-44 Selecting a State



For example, if you were using Access Manager:

4. Select the **inetuserstatus** attribute from the Activation state attribute drop-down list.
5. Click the New button and enter **active**, **inactive**, and **deleted** attribute values to the Value column of the table.
6. Click in the State column and select Activated or Inactivated for each value as follows:
 - **No Value:** Activated

- **active:** Activated
- **inactive:** Inactivated
- **deleted:** Inactivated
- **All Other Values:** Inactivated

Based on this example, [Using a Custom Method for Directory Server](#) describes how Identity Synchronization for Windows will detect and synchronize activations/inactivations when you enable the Use Custom Method for Directory Server option (using the `inetuserstatus` example).

Value	State	Result
No Value	Activated	If the <code>inetuserstatus</code> attribute is missing or does not have a value, Identity Synchronization for Windows detects the object as activated.
active	Activated	If the attribute is active Identity Synchronization for Windows detects the object as activated.
inactive	Inactivated	If the attribute value is inactive Identity Synchronization for Windows detects the object as inactivated.
deleted	Inactivated	If the attribute value is deleted Identity Synchronization for Windows detects the object as inactivated.
All Other Values	Inactivated	If the attribute has a value, but that value is not specified in the table, Identity Synchronization for Windows detects the object as inactivated.

Setting Activations and Inactivations

As you populate the Value and State table with entries, Identity Synchronization for Windows automatically populates the **Activated value** and **Inactivated value** drop-down lists as follows:

- The Activated value list contains all values with an Activated status (for example **No Value** and **active**).
- The Inactivated value list contains all values with an Inactivated status (for example **inactive** and **deleted**).
- Neither list will contain the All Other Values value.

Select a value from the Activated value and/or the Inactivated value drop-down lists to specify how Identity Synchronization for Windows will activate and/or inactivate an object when synchronizing from Active Directory.

- **Activated value:** Controls the object's active state.

No Value: If the object contains the active value, Identity Synchronization for Windows will set the state to activated in Directory Server.

active: If the object contains the active value, Identity Synchronization for Windows will set the state to activated in Directory Server.

- **Inactivated value:** Controls the object's active state.

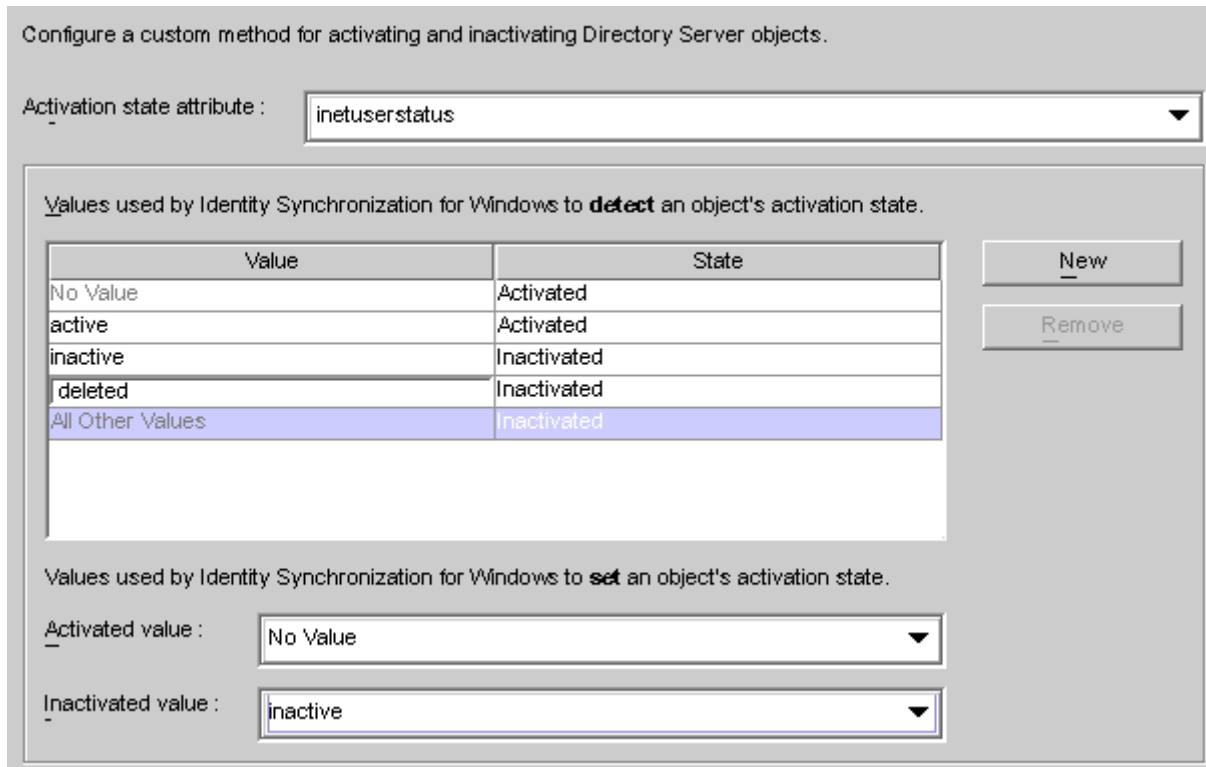
inactive or **deleted**: Identity Synchronization for Windows will set the object's state to inactive in Directory Server.

none: Not a valid setting. You must select a value.

Note: You must specify an Inactivated value or your configuration will be invalid.

Using a Custom Method for Directory Server illustrates a completed Configure Custom Method for Directory Server dialog box.

Figure 4-45 Example: Completed Dialog



4.5.3 Specifying Configuration Settings for Group Synchronization

If you enable Group Synchronization between Directory Server and Active Directory, you can synchronize the creation of groups, deletion of groups, and the membership changes within that group .

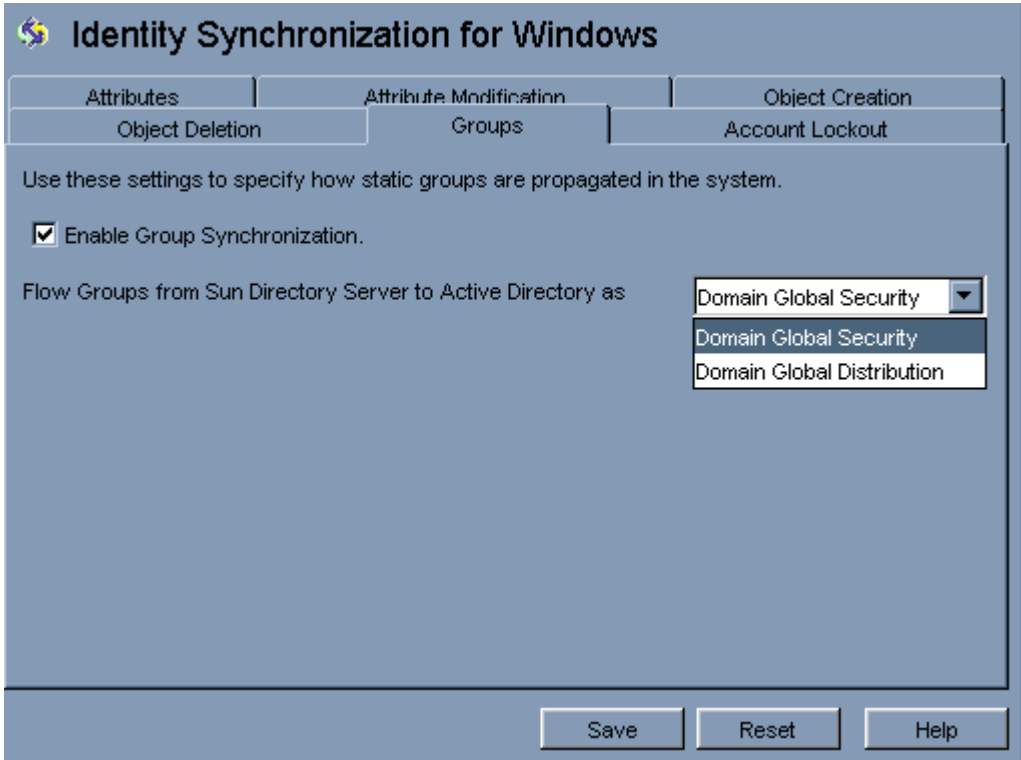
Note: Group Synchronization is not supported on Windows NT directory sources.

4.5.3.1 To Synchronize Groups:

1. Under the Groups tab, select the Enable Group Synchronization check box.
2. Select one of the following Group Synchronization methods to specify how Identity Synchronization for Windows will detect and synchronize various groups:

- *Domain Global Security*
- *Domain Global Distribution*

Figure 4–46 *Enable Group Synchronization*

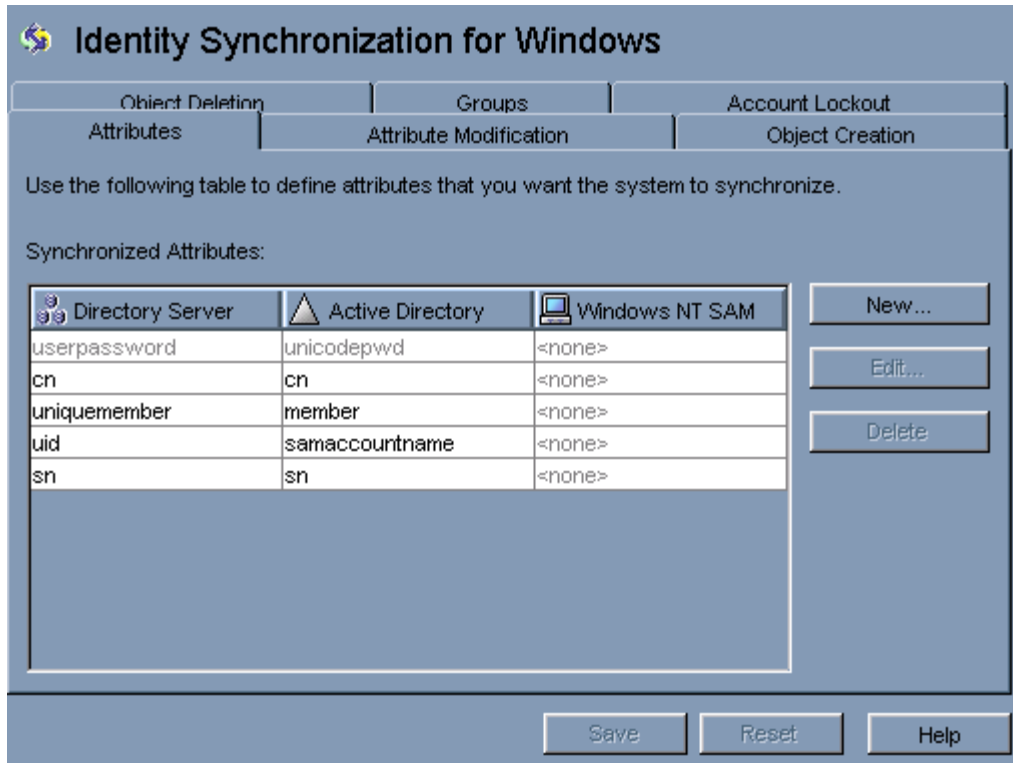


Note: For more information about Domain Global Security, Domain Global Distribution, and Active Directory; see the Microsoft Active Directory documentation.

4.5.3.2 Configure Identity Synchronization for Windows to Detect and Synchronize Groups Related Changes between Directory Server and Active Directory

You do not need to map any attribute manually for the group synchronization. When you press Save, Identity Synchronization for Windows maps the attributes automatically.

Figure 4–47 Attribute Mapping for Group Synchronization



-
- Note:**
1. Do not modify the mapping between the *userpassword* and *unicodepwd* attributes.
 2. To disable the group synchronization, deselect the Disable Group Synchronization check box.
 3. Alternatively, you can enable or disable group synchronization using command line `idsync groupsync`. For more information, see [Appendix A, "Using the Identity Synchronization for Windows Command Line Utilities"](#).
-

4.5.4 Configuring and Synchronizing Account Lockout and Unlockout

To enable the Account Lockout feature, you must do the following:

- Make the Password policies same on both Active Directory and Directory Server.
- Enable Account Lockout.
- Map certain attributes, which are different in Directory Server and in Active Directory

Identity Synchronization for Windows can synchronize the following events between Active Directory and Directory Server:

- Lockout events from Active Directory to Directory Server
- Lockout events from Directory Server to Active Directory
- Manual unlockout events from Active Directory to Directory Server
- Manual unlockout events from Directory Server to Active Directory

Note: Account lockout and unlockout synchronization is not supported on Windows NT directory servers.

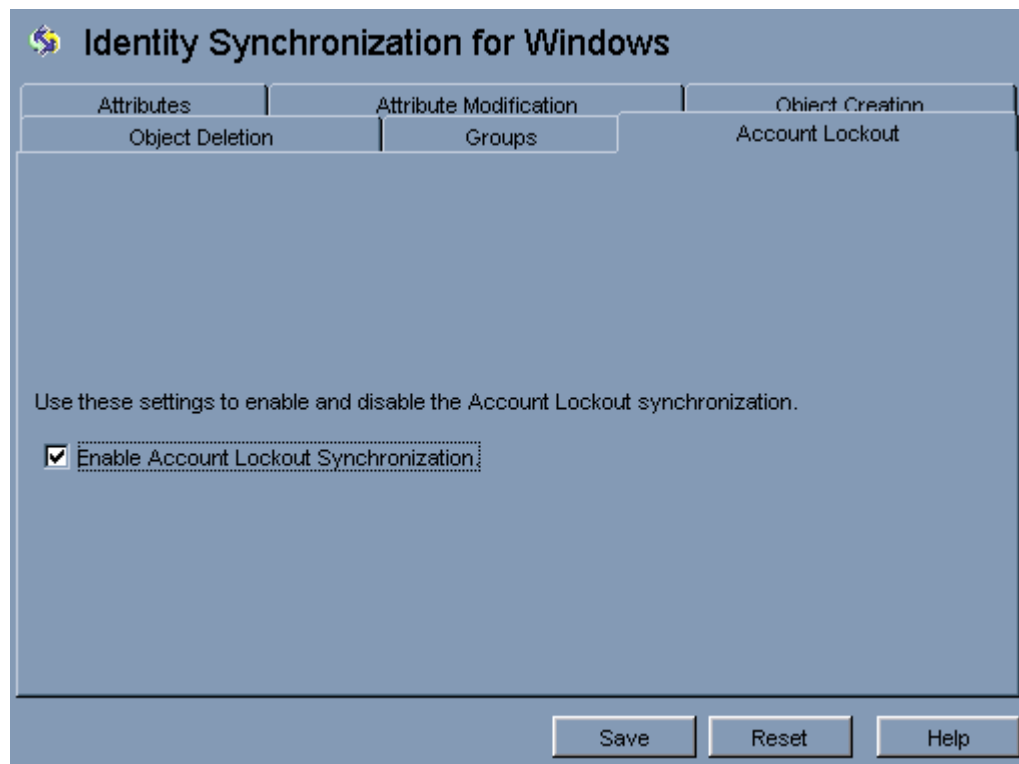
4.5.4.1 Prerequisites for Account Lockout

The attribute `lockoutDuration` should be set to the same value at both the places before enabling the account lockout feature. Make sure that the system time is also uniform across the distributed setup. Otherwise, the lockout events can expire if the `lockoutDuration` is less than the difference in the system dates.

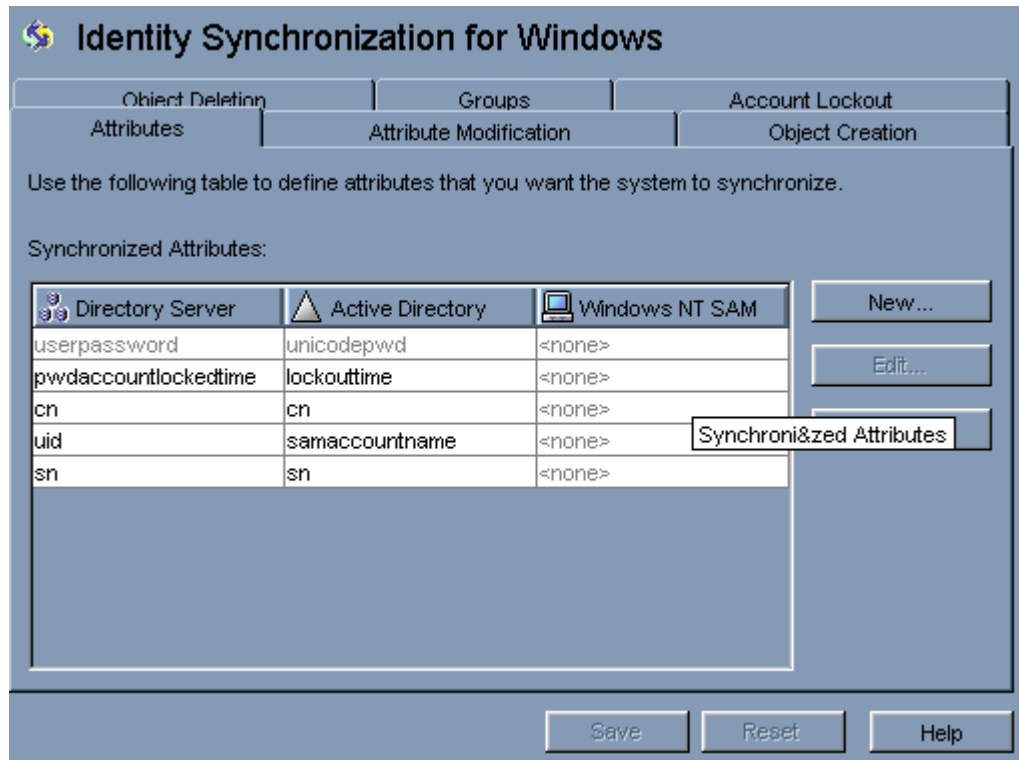
Note: Set the symmetric password policy at both ends. For example, if the password policy at Active Directory signifies a permanent lockout then the same password policy should be set at Directory Server.

4.5.4.2 Using the Account Lockout Feature

Enable Account Lockout Synchronization between Directory Server and Active Directory.



No explicit mapping of the `pwdaccountlockedtime` (Directory Server) and `lockoutTime` (AD) attributes is required to enable account lockout. Select Enable Account Lockout Synchronization from the Account Lockout tab in Identity Synchronization for Windows configuration panel.



Note: You can enable or disable the account lockout synchronization using command line tool `idsync accountlockout`. For more information, see [Appendix A, "Using the Identity Synchronization for Windows Command Line Utilities"](#).

4.5.5 Specifying How Deletions Flow

Use Object Deletions tab to specify how deleted user entries should flow between Directory Server and Active Directory systems.

Note: You cannot specify Object Deletions flow for Windows NT.

4.5.5.1 To Specify how Deleted Entries Flow Between Directory Server and Active Directory Systems

1. Select the Identity Synchronization for Windows node at the top of the navigation pane, and then click the Object Deletion tab.

Figure 4–48 Propagating User Entry Deletions



2. Enable or disable the flow of deletions as follows:
 - Enable **Object deletions flow from Sun Java System Directory Server to Active Directory** to propagate deletions from the Sun Directory Server environment to your Active Directory servers.
 - Enable **Object deletions flow from Active Directory to Sun Java System Directory Server** to propagate deletions from the Active Directory environment to your Sun Directory Servers.
 - Enable both options for bidirectional flow.
 - Disable both options to prevent user deletions from propagating from one system to the other (*Default setting*).

4.6 Creating Synchronization User Lists

A Synchronization User List (SUL) specifies which users in Active Directory and Sun Directory Server will be synchronized. Every entry in the SUL passes through the Connector and is evaluated against the constraints you configured for that SUL.

Each SUL contains two elements, one to identify which Directory Server users to synchronize and one to identify which Windows users to synchronize.

Note: To synchronize users in a Directory Server with multiple Active Directory domains, you must define one SUL for each Active Directory domain.

For more information about defining and configuring SULs (including components of a definition, how to define multiple SULs, how multiple SULs are processed, and how to configure multiple Windows domain support) refer to [Appendix D, "Defining and Configuring Synchronization User Lists for Identity Synchronization for Windows"](#)

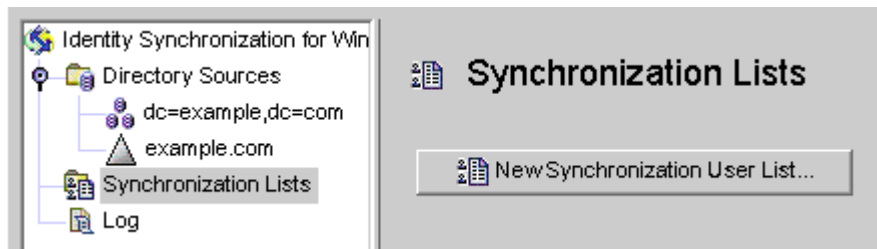
Both of the SUL elements contain three definitions that identify which users to synchronize:

- **Base DN:** Location of the users to be synchronized (not applicable for NT)
- **Naming attribute:** Attribute used for newly created users (creation expression) (not applicable for NT)
- **Filter:** Excludes specified users from synchronization

4.6.1 To Identify and Link User Types Between Servers

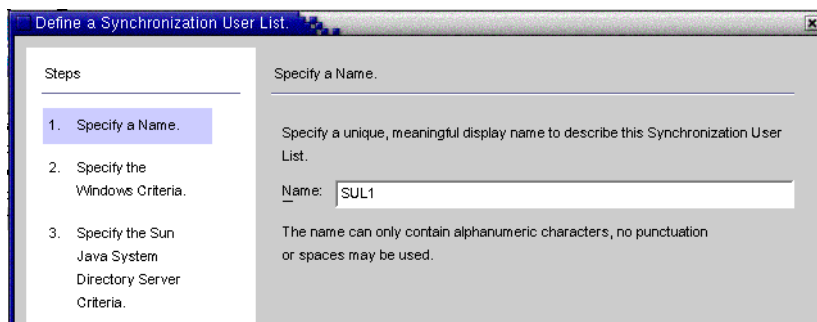
1. Select the Synchronization User Lists node in the navigation tree, and then click New Synchronization User List button.

Figure 4–49 *Creating a New Synchronization User List*



The Define a Synchronization User List wizard is displayed.

Figure 4–50 *Specifying a Name for Your SUL*

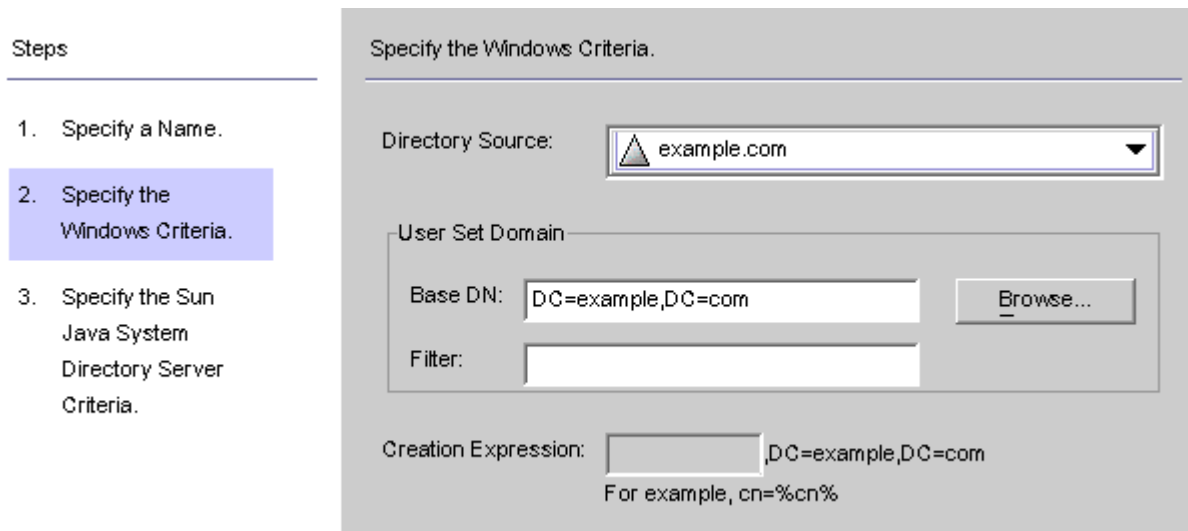


The program default for your first Synchronization User List is *SUL1*.

- If the default name is acceptable, click Next.

- If you want to use a different name, type a different name into the Name field and then click Next.
 - Do not use spaces or any kind of punctuation in the SUL name.
 - You must specify a name that is unique within the system.
- The Windows Criteria panel is displayed.

Figure 4–51 Specifying the Windows Criteria



2. Select a Windows Directory Source from the drop-down list.

Note: You cannot edit the Active Directory or Directory Server directory sources included in this SUL after you click the Finish button to create the SUL. When the Group Synchronization feature is enabled, the creation expression would be `uid=%uid%` or `cn=%cn%` in the Sun Java System Directory Server Criteria panel.

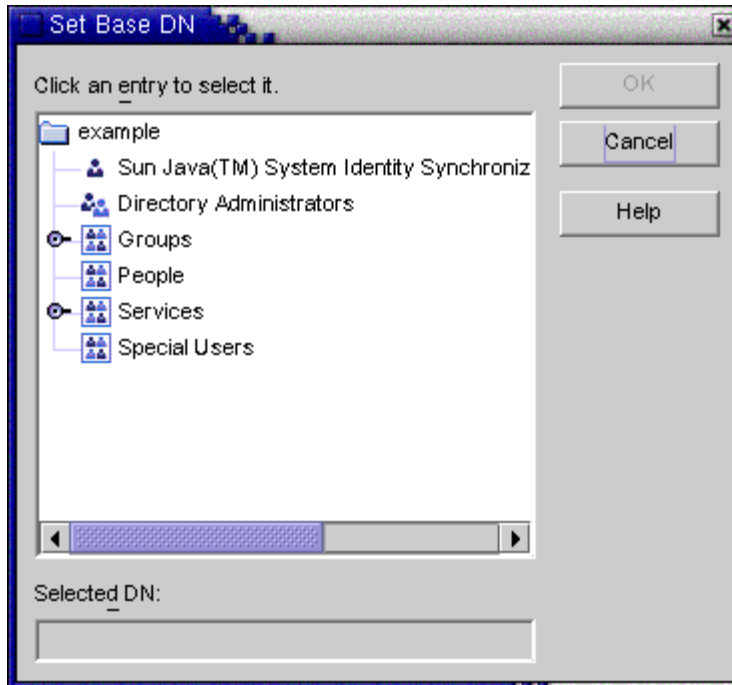
3. *A User Set Domain* is the set of all the users to be synchronized. Enter the User Set Domain's Base DN, using one of the following methods:
 - Type the name into the text field (for example, **DC=example,DC=com**).
 - Click the Browse button, to open the Set Base DN dialog box so you can look for, and select a Base DN.

All users under the specified Base DN will be included in this SUL, unless you explicitly exclude them using a filter.

Note: Base DNs and creation expressions are not allowed for Windows NT machines.

You cannot edit the Active Directory or Directory Server directory sources included in this SUL after you click the Finish button to create the SUL. When the Group Synchronization feature is enabled, then the creation expression should be `uid=%uid%` in the Sun Java System Directory Server Criteria panel.

Figure 4-52 Selecting a Base DN



4. You can enter an equality, a presence, or a substring Filter to specify which users in this base DN are synchronized. For example, if you are using the same base DN for multiple synchronization user lists, you may want to use a filter to distinguish between them.

The equality filter syntax is similar to LDAP query syntax, except that equality substrings allow *, &, |, =, ! characters only. For example, you can use the following filter to exclude the Administrator from your SUL:

(!(cn=Administrator))

The program should populate the Creation Expression field automatically.

Note: A creation expression defines the parent DN and naming attribute used when new entries are propagated from Active Directory to Directory Server.

A creation expression is not allowed for Sun directories unless you configured user attribute creations to flow from Active Directory to Directory Server. For more information, see [Specifying How Object Creations Flow](#).

5. If the creation expression is missing or you want to change the existing entry, you can enter a creation expression for all Windows Active Directory synchronization user lists; for example:

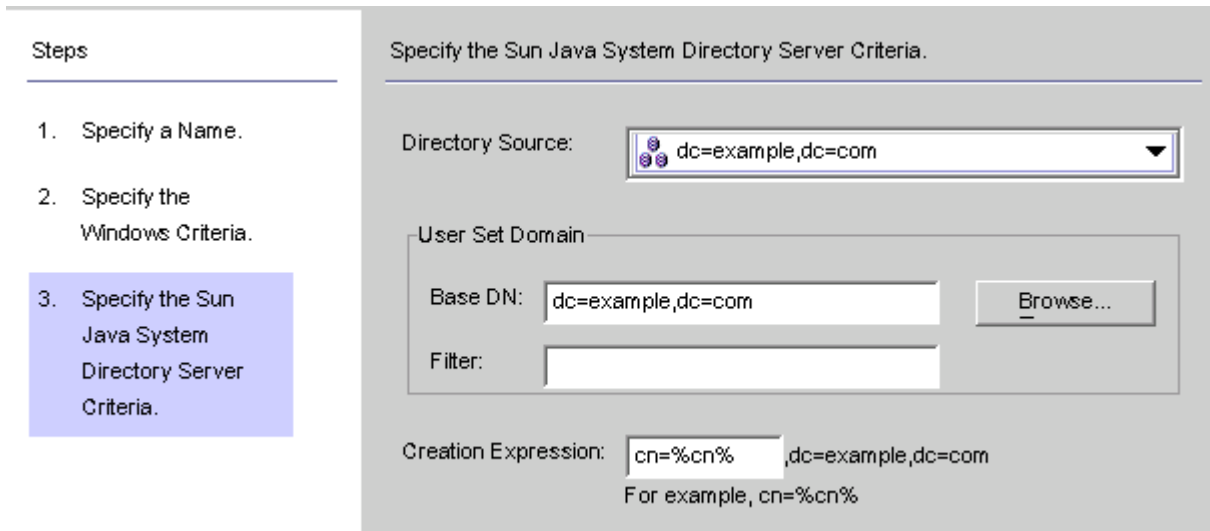
cn=%cn% ,c1=users,dc=example,dc=com

If you are going to change the creation expression, you must select an attribute that you will be synchronizing. If necessary, go back to the Object Creation tab and use the Creation Attribute button to add and map this attribute.

6. Click Next to specify the Sun Java System Directory Server criteria.

- When the Specify the Sun Java System Directory Server Criteria panel is displayed repeat Step 2 through Step 5 to provide the Directory Server criteria.

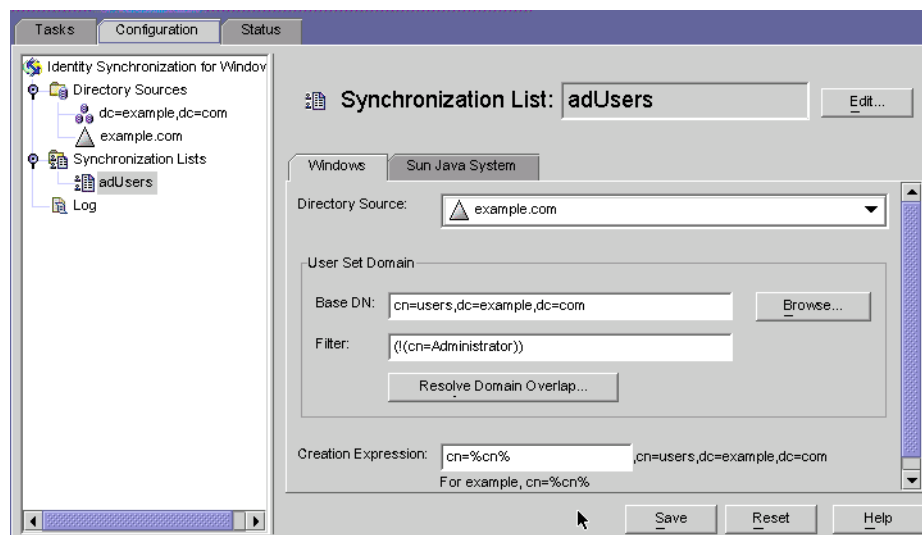
Figure 4–53 *Specifying Directory Server Criteria*



Note: You cannot edit the Active Directory or Directory Server directory sources included in this SUL after you click the Finish button to create the SUL.

- When you are done, click Finish.
- The program adds your new SUL node to the navigation tree and the Synchronization User List panel is displayed on the Configuration Tab.

Figure 4–54 *Synchronization List Panel*



- In cases where a user matches multiple lists, click the Resolve Domain Overlap button to define a preference for the synchronization user list.

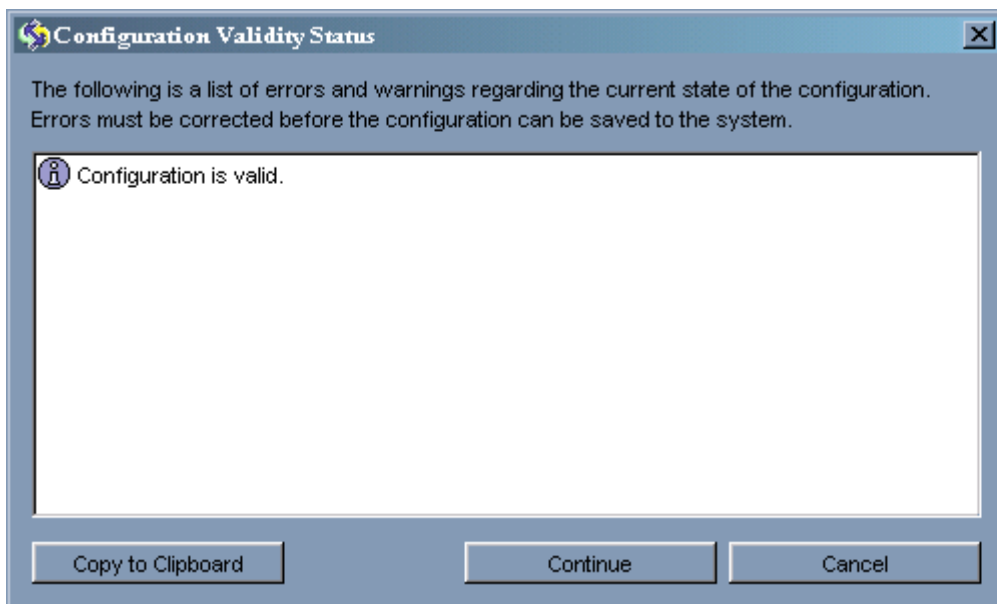
11. Create a Synchronization User List that includes every directory source in your network except for the Directory Server.

4.7 Saving a Configuration

4.7.1 To Save your Current Configuration from the Console Panels

1. Click Save to store your settings at this point.
2. The Configuration Validity Status window is displayed as the program evaluates your configuration settings.

Figure 4–55 Configuration Validity Status Window



This panel confirms that your configuration is valid or identifies configuration problems that must be fixed.

Saving your configuration may take a few minutes because the program rewrites the information out to the configuration directory and notifies the system manager.

The system manager (a Core component) is responsible for distributing your configuration settings out to the components that need the information.

Note: Configuration validation errors are red and warnings are yellow.

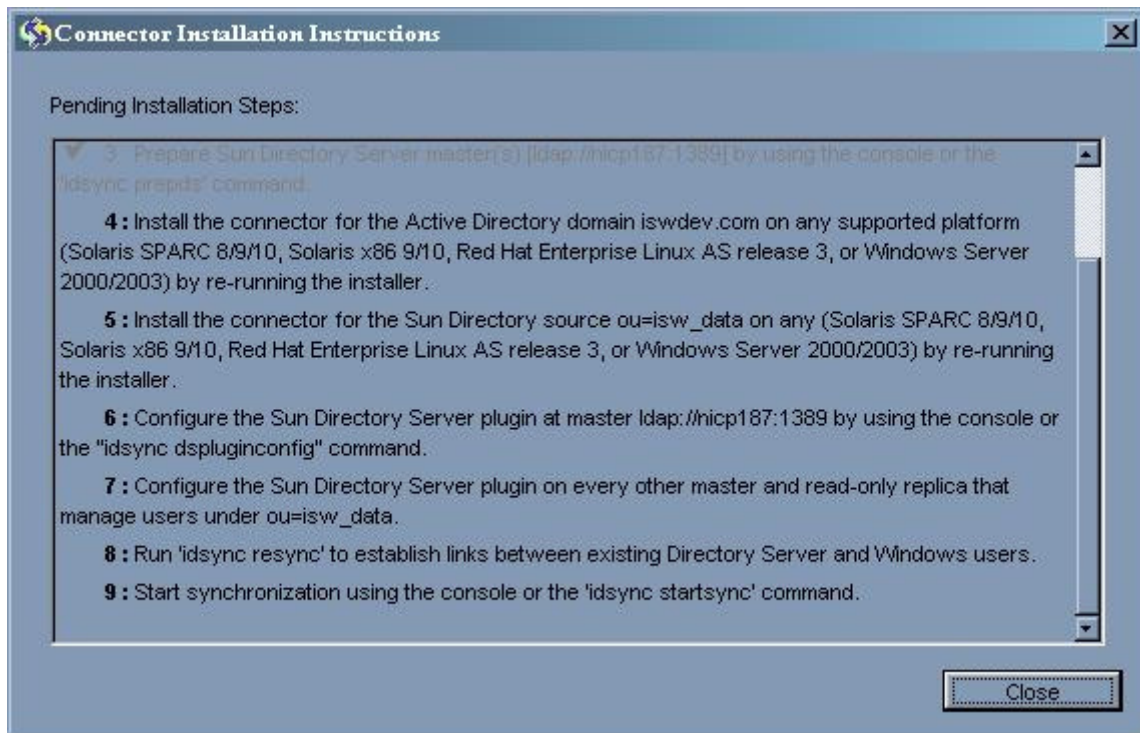
- You cannot save a configuration with errors.
 - You can save configurations with warnings, but it is better to try and clear the warnings first.
-

3. If your configuration is valid, click Continue to save the configuration.

A Connector Installation Instructions dialog box is displayed, giving instructions about how to proceed with installing the Identity Synchronization for Windows Connectors and subcomponents.

This list has now been updated with a To Do list that is customized for your deployment. (Up to this point, the steps were generic.) Note that you can also access and update the To Do list from the Status tab on the Identity Synchronization for Windows Console.

Figure 4-56 Instructions for Installing the Connectors



4. Read the information carefully and click OK.

After finishing the initial Core configuration, you are ready to install the Identity Synchronization for Windows Connectors and subcomponents. Continue to [Chapter 1, "Understanding the Product"](#) for instructions.

Installing Connectors

This chapter provides instructions for installing the Identity Synchronization for Windows Connectors. The information is organized as follows:

- [Before You Begin](#)
- [Running the Installation Program](#)
- [Installing Connectors](#)

Identity Synchronization for Windows uses Connectors to synchronize user passwords between directory sources, and uses subcomponents to enhance the Connector's change-detection and bidirectional synchronization support.

5.1 Before You Begin

Before starting the Connector configuring process, you should be aware of the following:

- Close the Console before starting the installation process. If the Console is open when you are installing a Connector, the program perceives a conflict about which component is adding configuration data to the server and generates an error message.
- Active Directory Connectors do not have subcomponents.
- Windows NT Connectors and subcomponents are installed simultaneously.
- You can install Directory Server or Active Directory Connectors on the same machine where you installed Core or you can install Connectors on another machine. (The Windows NT Connector must be installed on the Primary Domain Controller (PDC) of the domain being synchronized.)
- If you are installing the Connector on the same machine as Core, the program automatically installs the Connector in the same directory as Core.
- If you are installing the Connector on a different machine, the program will prompt you to specify the configuration directory information supplied during the Core installation.

You must run the installation program each time you install a Connector.

For example, if you are installing a Directory Server Connector and an Active Directory Connector, you will run the installation program twice after the Core is installed.

5.2 Running the Installation Program

Repeat the following steps each time you install a Connector.

5.2.1 To Restart and Run the Installation Program

1. Run the installation program again on the machine where you want to install the Connector, as follows:
 - **On Solaris:** Change to the `installer` directory and then type `./runInstaller.sh` to execute the installation program.

Note: To run the installation program in text-based mode, type `./runInstaller.sh -nodisplay`.

When you run the `runInstaller.sh` program, Identity Synchronization for Windows automatically masks passwords so they will not be echoed in the clear.

 - **On Linux:** Change to the `installer` directory and then type `./installer.sh` to execute the installation program.

Note: To run the installation program in text-based mode, type `./installer.sh -nodisplay`.

When you run the `installer.sh` program, Identity Synchronization for Windows automatically masks passwords so they will not be echoed in the clear.

 - **On Windows:** Change to the `installer` directory and then type `setup.exe` to execute the installation program.
2. When the Welcome screen is displayed, read the information provided and then click Next to proceed to the Software License Agreement panel.
3. Read the license agreement, then select
 - **Yes (Accept License)** to accept the license terms and go to the next panel.
 - **No** to stop the setup process and exit the installation program.
4. The Sun Java System Directory Server panel is displayed. Specify the configuration directory location as follows:
 - **Configuration Directory Host:** Enter the fully qualified domain name (FQDN) of a Sun Java System Directory Server instance (affiliated with an Administration Server) where Identity Synchronization for Windows configuration information is stored. You must specify the same instance that you specified during the Core installation.
 - **Configuration Directory Port** (*Defaults to port 389*): Specify a port for the configuration directory. You can leave the port set to the default or change to a different, available port.

To enable SSL (Secure Socket Layer) between Core and the configuration directory, enable the Secure Port option and specify an SSL port (*default SSL port is 636*). Enabling this option prevents sensitive information from being passed in the clear over the network.

- **Configuration Root Suffix:** Select the root suffix that you specified during the Core installation from the menu. The Identity Synchronization for Windows configuration will be stored in this root suffix.

Note: If the program could not detect a root suffix, and you enter the server information manually, you must click Refresh to repopulate the list of root suffixes.

5. Click Next to open the Configuration Directory Credentials panel.
6. Enter the configuration directory Administrator's user ID and password.
 - If you specify `admin` as the user ID, you will not be required to specify the User ID as a DN.
 - If you use any other user ID, then you must specify the ID as a full DN. For example, `cn=Directory Manager`.

Note: These credentials will be sent without encryption unless you enabled SSL in.

7. Click Next to open the Configuration Password panel where you must enter the configuration password you specified when you installed Core.

Also, if Core has not been installed on this machine, you will be prompted to provide the location of the Java Home directory (see [Installing Core](#)).

8. When you are finished, click Next.

Note: At this point, the installation process becomes specific to the type of Connector you are installing.

5.3 Installing Connectors

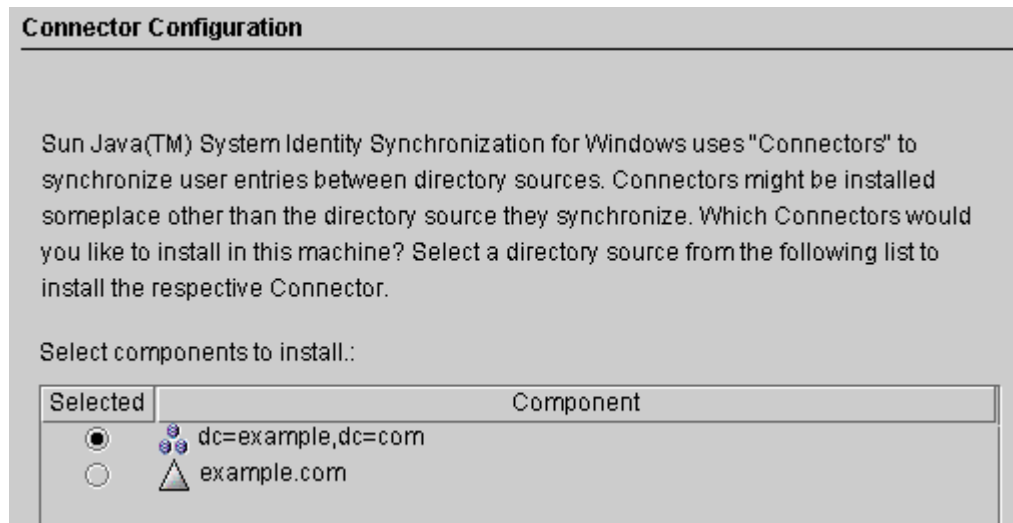
This section explains how to install the three types of Identity Synchronization for Windows Connectors, as follows

- [Installing the Directory Server Connector](#)
- [Installing an Active Directory Connector](#)
- [Installing the Windows NT Connector](#)

Note: You are not required to install Connectors in any particular order, but do not attempt to install any Connectors simultaneously.

5.3.1 Installing the Directory Server Connector

After completing the steps described in [Running the Installation Program](#)

Figure 5–1 Selecting the Directory Server Connector

The Select components to install list contains only those Connector components that have not yet been installed. For example, after you install the Directory Server Connector (`dc=example,dc=com`), the program will remove the entry from the list pane.

The following table contains some example directory source entries.

Table 5–1 Directory Source Examples

Directory Source	Example Entry
Sun Java System Directory Server	<code>dc=example,dc=com</code>
Windows Active Directory	<code>example.com</code>
Windows NT SAM	<code>EXAMPLE</code>

5.3.1.1 To Install the Directory Server Connector

1. Enable the button next to the Directory Server Connector component and then click Next.

The Directory Server Connector Credentials panel is displayed.

Directory Server Connector Credentials

Enter the directory manager credentials for the Sun Java(TM) System Directory Server(s) associated with the connector being installed.

Primary: ldap://machine1.example.com:389

Primary Directory Server User DN:

Primary Directory Server Password:

Secondary: none

Secondary Directory Server User DN:

Secondary Directory Server Password:

Note: The program automatically completes the User DN fields with your fully qualified Directory Manager distinguished name, but you can change the information if necessary.

Enter the following information:

- **Primary Directory Server User DN:** If necessary, change the default user DN by entering a fully qualified Directory Manager distinguished name.
- **Primary Directory Server Password:** Enter your Directory Manager password.

If you are using a secondary master, the Secondary Directory Server User Name and Password fields will be active. The program automatically completes the Directory Manager DN field with the same entries provided for the Primary Directory Server User DN and Password fields. You can change this information if necessary.

The program will verify that the Directory Server was prepared and ready to synchronize data. When you prepared Directory Server ([Preparing Sun Directory Source](#)), the program creates an account that the Connector will use to connect to Directory Server (for example, `uid=PSWConnector,suffix`).

2. Click Next to proceed to the Connector Port Configuration pane.

Connector Port Configuration

Some Sun Java(TM) System Identity Synchronization for Windows Connectors require a TCP/IP port number. You must specify a TCP/IP server port number to enable communication between the Connector and its subcomponent(s). You must specify a port number that is not being used by any other applications on this machine.

Fully Qualified Local Host Name:

Connector Port Number:

3. Enter the Fully Qualified Local Host Name with the domain and an available port number where the Connector will listen. (Specifying a port already in use will result in an error message.)
4. Click Next and the Ready to Install pane is displayed to provide information about the Connector's installation location and how much disk space is required for the installation. When you are ready, click the Install Now button.

Ready to Install.

Product: Identity Synchronization for Windows

Location: /opt/SUNWisw

Space Required: 3.51 MB

Sun Java(TM) System Identity Synchronization for Windows Connector

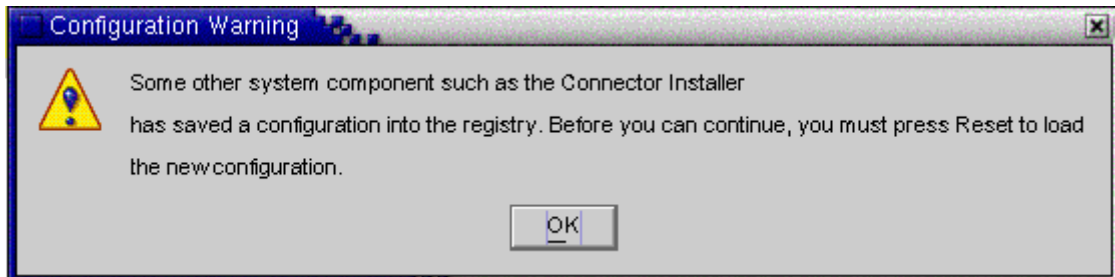
Note: If you installed Core on the local machine, the Ready to Install pane will indicate that zero space is required to install the Connector. This situation occurs because the Core installation has already installed the Connector binaries. Because there are no additional binaries to install, no additional space is required.

If you are installing the Connector on a machine other than where you installed Core, then the Ready to Install pane will indicate how much space is required to complete the Connector installation on the local machine.

The Connector installation is accomplished in two steps:

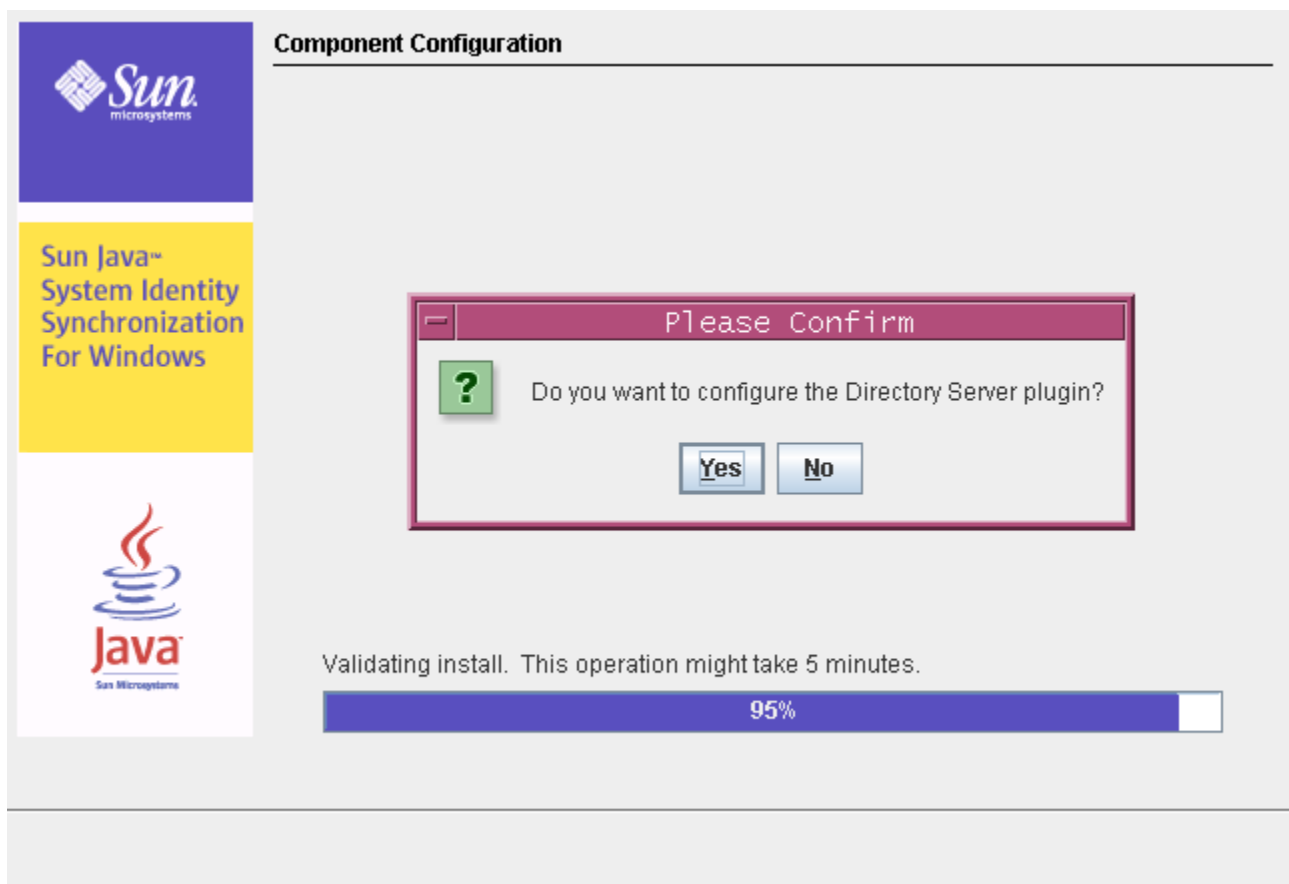
- An Installing pane is displayed, with a progress bar, while the program installs the binaries.
- Next, the Component Configuration pane displays a progress bar. This step takes several minutes to complete.

Note: If you did not close the Console before starting the installation, the following warning displays ([Installing the Directory Server Connector](#)). Click Reset in the Console to reload the Connector's configuration settings.



When both steps are complete, an Installation Summary pane is displayed.

Note: Directory Server plugin gets configured for preferred and secondary hosts (if any).

The image shows a "Component Configuration" window. On the left side, there is a vertical sidebar with three sections: a purple section with the Sun Microsystems logo, a yellow section with the text "Sun Java™ System Identity Synchronization For Windows", and a white section with the Java logo. The main area of the window is titled "Component Configuration" and contains a smaller dialog box titled "Please Confirm". This dialog box has a green question mark icon and asks, "Do you want to configure the Directory Server plugin?". Below the question are "Yes" and "No" buttons. At the bottom of the main window, there is a progress bar that is 95% full, with the text "Validating install. This operation might take 5 minutes." above it.

-
-
- Note:**
1. Clicking Yes configures the Directory Server plugin in all the hosts (preferred and secondary).
 2. Clicking No enables you to configure the plugin later using command line `idsync dspluginconfig`. For more information, see [Appendix A, "Using the Identity Synchronization for Windows Command Line Utilities"](#).
-
-

5. Click the Details button if you want to review the installation log.
 - **On Solaris:** Installation logs are written to `/var/sadm/install/logs/`
 - **On Linux:** Installation logs are written to `/var/sadm/install/logs/`
 - **On Windows:** Installation logs are written to the `%TEMP%` directory, which is usually a subdirectory of the `Local Settings` folder located under `C:\Documents and Settings\Administrator`

Note: On some Windows systems (such as Windows 2000 Advanced Server), the `Local Settings` folder is a hidden folder.

To view this folder and the `Temp` subdirectory, open your Windows Explorer and select `Tools > Folder Options` from the menu bar. When the Folder Options dialog box is displayed, select the `View` tab and enable the `Show Hidden Files` option.

6. Click Next to display the "To Do list" panel, which shows the list of successfully completed and pending steps.

This is a list of remaining installation and configuration steps:

- ✓ 1 : Install the Identity Synchronization core components.
- ✓ 2 : Create an initial configuration using the product's console or by migrating from a previous installation using `'idsync importcnf'`.
- ✓ 3 : Prepare Sun Directory Server master(s) [`ldap://isw080:1389`] by using the console or the `'idsync prepds'` command.
- ✓ 4 : Install the connector for the Sun Directory source `ou=isw_data` on any (Solaris SPARC 8/9/10, Solaris x86 9/10, Red Hat Enterprise Linux AS release 3, or Windows Server 2000/2003) by re-running the installer.
- ✓ 5 : Configure the Sun Directory Server plugin at master `ldap://isw080:1389` by using the console or the `"idsync dspluginconfig"` command.
- 6 : Install the connector for the Active Directory domain `metaqa.com` on any supported platform (Solaris SPARC 8/9/10, Solaris x86 9/10, Red Hat Enterprise Linux AS release 3, or Windows Server 2000/2003) by re-running the installer.
- 7 : Configure the Sun Directory Server plugin on every other master and read-only replica that manage users under `ou=isw_data`.
- 8 : Run `'idsync resync'` to establish links between existing Directory Server and Windows users.
- 9 : Start synchronization using the console or the `'idsync startsync'` command.

7. When you are done with the panel, click Finished.

After installing the Directory Server Connector, you can install other Connectors that you configured when you configured the resources ([Chapter 4, "Configuring Core Resources"](#)):

- Install additional Directory Server Connectors: Restart the installation program (using the instructions in [Running the Installation Program](#)) and then repeat [Enable the button next to the Directory Server Connector component and then click Next.](#) through [When you are done with the panel, click Finished.](#).
- Install an Active Directory Connector: Go to [Installing an Active Directory Connector](#).
- Install a Windows NT Connector: Go to [Installing the Windows NT Connector](#).

5.3.1.2 Configuring Identity Synchronization for Windows Plug-in when Chained Suffix exists

This configuration is needed only when the chained suffix exists in the Directory Server instance where Identity Synchronization for Windows Plug-in is installed. If Identity Synchronization for Windows Plug-in is not configured to search on chained suffix, MODIFY and BIND operations performed on the Directory Server where the Identity Synchronization for Windows Plug-in is installed, will fail.

In the Directory Server instance where the chained suffix is created, perform the following operations:

Execute the following LDIF script using `ldapmodify` utility:

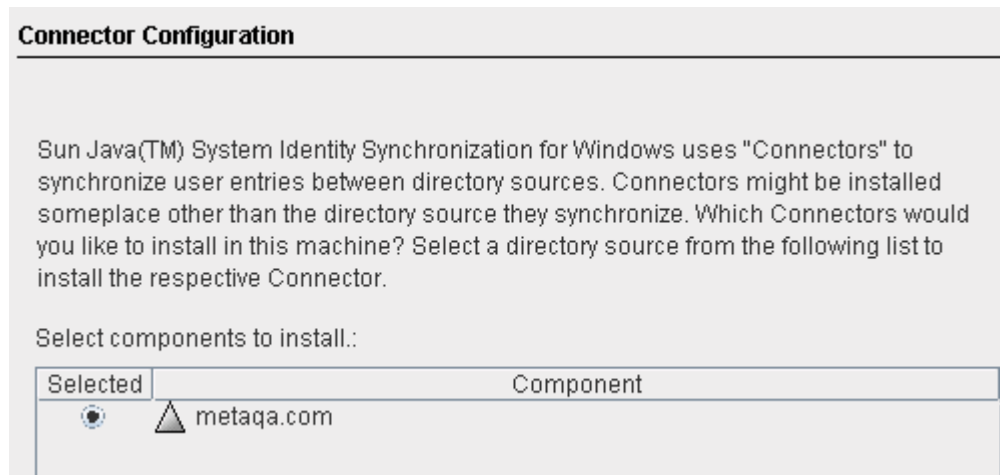
```
dn: cn=config,cn=chaining database,cn=plugins,cn=config
changetype: modify
add: nspossiblechainingcomponents
nspossiblechainingcomponents: cn=pswsync,cn=plugins,cn=config
```

You can perform the similar operation by using the following procedure:

1. Select the Configuration tab.
2. Click the Data node that displays in the left pane.
3. Select the Chaining tab in the right pane.
4. Add Identity Synchronization for Windows Plug-in (`cn=pswsync,cn=plugins,cn=config`) to the components that are allowed to chain.
5. Save the changes and exit.

5.3.2 Installing an Active Directory Connector

After you install the Directory Server Connector and if you have other configured Connectors to install, the installation program will give you the option of installing the Connectors before you see the Connector Configuration pane.

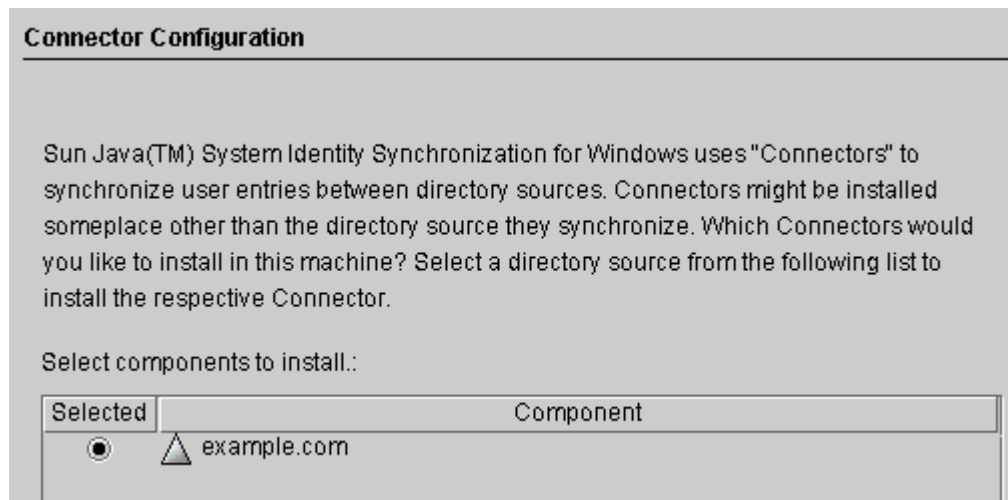
Figure 5–2 Selecting the Connector

The component list contains only those Connector components that have not yet been installed. For example, if you already installed the Directory Server Connector (`dc=example,dc=com` in this case), it will not be listed.

5.3.2.1 To Install an Active Directory Connector

1. Enable the Connector button and click Next.

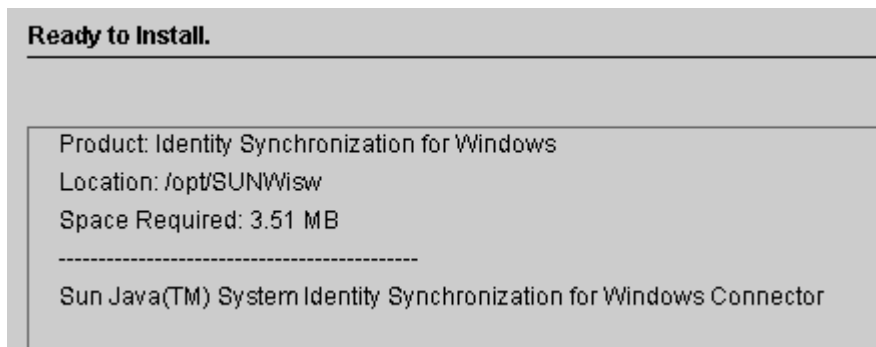
The Connector Configuration panel displays.



The Select components to install list contains only those Connector components that have not yet been installed. For example, after you install the Directory Server Connector (`dc=example,dc=com` in this case), the program will remove the entry from this list pane.

2. Enable the button next to the Active Directory component and then click Next.

The Ready to Install pane is displayed to provide information about the Connector's installation location and how much disk space is required for the installation.



Note: If you installed Core on the local machine, the Ready to Install pane will indicate that zero space is required to install the Connector. This situation occurs because the Core installation has already installed the Connector binaries. Because there are no additional binaries to install, no additional space is required.

If you are installing the Connector on a machine other than where you installed Core, then the Ready to Install pane will indicate how much space is required to complete the Connector installation on the local machine.

3. When you are ready, click the Install Now button.

An Installing pane is displayed, with a progress bar, while the program installs the binaries, and then an Installation Summary pane is displayed to confirm the installation is finished.

4. Click the Details button if you want to review the installation log.
 - **On Solaris:** Installation logs are written to `/var/sadm/install/logs/`
 - **On Linux:** Installation logs are written to `/var/sadm/install/logs/`
 - **On Windows:** Installation logs are written to the `%TEMP%` directory, which is a subdirectory of the `Local Settings` folder located under `C:\Documents and Settings\Administrator`

Note: On some Windows systems (such as Windows 2000 Advanced Server), the `Local Settings` folder is a hidden folder.

To view this folder and the `Temp` subdirectory, open your Windows Explorer and select `Tools > Folder Options` from the menu bar. When the Folder Options dialog box is displayed, select the `View` tab and enable the `Show Hidden Files` option.

5. Click Next to display the "To Do list" panel, which shows the list of successfully completed and pending steps.

This is a list of remaining installation and configuration steps:

- ✓ 1 : Install the Identity Synchronization core components.
- ✓ 2 : Create an initial configuration using the product's console or by migrating from a previous installation using 'idsync importcnf'.
- ✓ 3 : Prepare Sun Directory Server master(s) [ldap://isw080:1389] by using the console or the 'idsync prepds' command.
- ✓ 4 : Install the connector for the Active Directory domain metaqa.com on any supported platform (Solaris SPARC 8/9/10, Solaris x86 9/10, Red Hat Enterprise Linux AS release 3, or Windows Server 2000/2003) by re-running the installer.
- ✓ 5 : Install the connector for the Sun Directory source ou=isw_data on any (Solaris SPARC 8/9/10, Solaris x86 9/10, Red Hat Enterprise Linux AS release 3, or Windows Server 2000/2003) by re-running the installer.
- ✓ 6 : Configure the Sun Directory Server plugin at master ldap://isw080:1389 by using the console or the "idsync dspluginconfig" command.
- 7 : Configure the Sun Directory Server plugin on every other master and read-only replica that manage users under ou=isw_data.
- 8 : Run 'idsync resync' to establish links between existing Directory Server and Windows users.
- 9 : Start synchronization using the console or the 'idsync startsync' command.

6. When you are done with the panel, click Finished to exit the installation program.
After installing the Active Directory Connector, you can install other Connectors that you configured when you configured resources ([Chapter 4, "Configuring Core Resources"](#)):
 - Install additional Active Directory Connectors: Restart the installation program (see [Running the Installation Program](#)) and then repeat through.
 - Install a Windows NT Connector: Go to [Installing the Windows NT Connector](#).
 - Install additional Directory Server Connectors: Restart the installation program (using the instructions in [Running the Installation Program](#)) and then repeat [Enable the Connector button and click Next.](#) through [When you are done with the panel, click Finished to exit the installation program..](#)

5.3.3 Installing the Windows NT Connector

You must install the Windows NT Connector on the Primary Domain Controller (PDC) of the domain you configured.

5.3.3.1 To Install a Windows NT Connector and the NT subcomponents

1. Enable the Windows NT Connector button and click Next.
2. When the Connector Port Configuration pane is displayed, enter the Fully Qualified Local Host Name with the domain and an available port number where the Connector will listen. (Specifying a port already in use will result in an error message.)
3. When you are done, click Next.

The Ready to Install pane is displayed to provide information about the Connector's installation location and how much disk space is required.

4. When you are ready, click the Install Now button.

The Connector installation is accomplished in two steps:

- An Installing pane is displayed, with a progress bar, while the program installs the binaries.
- Next, the Component Configuration pane displays a progress bar. This step takes several minutes to complete.

Note: If you did not close the Console before starting the installation, a warning displays (see [Installing the Directory Server Connector](#)). Click Reset in the Console to reload the Connector's configuration settings.

When both steps are complete, an Installation Summary pane is displayed.

5. Click the Details button if you want to review the installation log.

Installation logs are written to the %TEMP% directory, which is C : \TEMP on most Windows NT systems.

6. Click Close to exit the installation program.

After installing the Windows NT Connector, you can install other Connectors that you configured when you configured resources ([Chapter 4, "Configuring Core Resources"](#)):

- To install additional Windows NT Connectors, restart the installation program. For more information, see [Running the Installation Program](#) and then repeat [Enable the Connector button and click Next](#).through [When you are done with the panel, click Finished to exit the installation program](#).
- To install Directory Server Connector, refer to [Installing the Directory Server Connector](#).
- To install Active Directory Connector, refer to [Installing an Active Directory Connector](#).

Synchronizing Existing Users and User Groups

The Identity Synchronization for Windows command line utility provides the `idsync resync` subcommand to bootstrap deployments with existing users or groups. This command uses administrator-specified matching rules to link existing entries, to populate an empty directory with the contents of a remote directory, or to bulk-synchronize attribute values (including passwords) between two existing user and group populations.

This chapter explains how to use the `idsync resync` subcommand and synchronize existing users and groups for new Identity Synchronization for Windows installations. In addition, this chapter provides instructions for starting and stopping synchronization and services. The information is organized as follows:

- [Using `idsync resync`](#)
- [Checking Results in the Central Log](#)
- [Starting and Stopping Synchronization](#)
- [Starting and Stopping Services](#)

Note: You must finish installing Core and the Connectors before trying to synchronize existing users.

For more information about the `idsync resync` subcommand, see [Appendix A, "Using the Identity Synchronization for Windows Command Line Utilities"](#)

Synchronizing Existing Users and User Groups summarizes the post-installation steps to follow based on existing user and group populations:

6.1 Post-Installation Steps Based on Existing User and Group Populations

Table 6–1 Post-Installation Steps Based on Existing User Populations

Users Exist In	Directory Server	Post-Installation Steps	Do NOT Synchronize Existing Users
No	No	None	None
No	Yes	Run <code>idsync resync -o Sun -c</code> to create existing Directory Server users in Windows.	None
Yes	No	Run <code>idsync resync -c</code> to create existing Windows users in Directory Server.	Run <code>idsync resync -u</code> to populate the connector's local cache of user entries.
Yes	Yes	Run <code>idsync resync -f <filename> -k</code> to link the users only, and then run <code>idsync resync -o Sun</code> to resynchronize existing users from Directory Server.	Run <code>idsync resync -u</code> to populate the connector's local cache of user entries.

Note: If Group Synchronization is enabled then the groups are synchronized in the same way as the users are synchronized.

6.2 Using `idsync resync`

This section explains the synchronizing processes, describes the proper syntax for using the `idsync resync` subcommand, and explains how to verify that the processes completed successfully. The information is organized as follows:

- [Resynchronizing Users or Groups](#)
- [Linking Users](#)
- [idsync resync Options](#)
- [Checking Results in the Central Log](#)

6.2.1 Resynchronizing Users or Groups

You need to resynchronize the user entries when two directory sources become out of sync. Use the `idsync resync` command to create users, user groups, and synchronize user and user group attributes in two directory sources. Specifically, you can use the `idsync resync` command to populate an empty Directory Server with the existing Active Directory or Windows NT SAM domain users.

The `idsync resync` command can be used in any of the following ways:

- If there are users that exist on Directory Server and Windows, you must run the `idsync resync` command to synchronize those users.
- If you do not want to synchronize existing users to Directory Server, then run `idsync resync` with the `-u` argument, which updates the object cache only and does not synchronize the Windows' entries to Directory Server.

- If you have existing Windows users and do not run `idsync resync`, then changes to these users may or may not be propagated; and depending on flow settings, these users might even be automatically created in Directory Server. You must run `idsync resync` again, even if you have already run the command.

Note: You cannot use the `idsync resync` command to synchronize passwords (except to invalidate Directory Server passwords to force on-demand password synchronization in an Active Directory environment).

When the Group Synchronization feature is enabled, both the users as well as the groups associated with the users are synchronized between the data sources configured. No additional options are required while using the `resync` command for Group Synchronization.

6.2.2 Linking Users

After populating Active Directory and Directory Server with users and installing the Active Directory and Directory Server Connectors (before starting synchronization), you must use the `idsync resync` command to ensure that all existing users are *linked* in the two directory sources.

What is *linking*? Identity Synchronization for Windows correlates the same user on Directory Server and on Windows by storing the following unique, immutable identifiers:

- The `dspswuserlink` attribute of each Directory Server user entry
- The `objectguid` attribute for each Active Directory user
- A combination of the domain name and the RID for each Windows NT SAM user

Storing this immutable identifier allows Identity Synchronization for Windows to synchronize other key identifiers, such as `uid` and `cn`. The `dspswuserlink` attribute is populated when:

- Identity Synchronization for Windows creates a new user in Directory Server (after a new user is synchronized from Windows or by running `idsync resync -c`)
- Identity Synchronization for Windows creates a new user on Windows (after synchronizing a new user from Directory Server or by running `idsync resync -c -o Sun`)
- You run `idsync resync -c -f` to link entries that already exist on Directory Server and Windows as described in this chapter.

To link existing users, you must provide rules for matching users between the two directories. For example, to link a user entry in two directories, both the first names and last names must match in both directory entries.

Linking user entries and resolving data conflicts could be described as more art than science. There are many reasons why the `idsync resync` subcommand might fail to link two users in opposing directory sources and depends to a large extent on the consistency of the data in the linked directories.

One strategy for using `idsync resync` is to use the `-n` argument, which runs the operation in "safe mode" so you can preview the effects of an operation with no actual changes. Running in safe mode allows you to refine the linking criteria gradually until you find an optimum set of user matching criteria.

However, you should be aware that there is a balance to be achieved through linkage accuracy and linkage coverage.

For example, if both directory sources contain an employee ID or social security number, you might begin with linking criteria that includes this number only. You might think that to improve linkage accuracy, you should include a last name attribute in the criteria as well. However, you could lose linkages because entries that would have matched on ID alone did not match because there were inconsistent last name values in the data. You will have to go through a data cleansing process for entries that fail to link.

Note: If Group Synchronization is enabled then the groups are linked in the same way as the users are linked.

6.2.3 idsync resync Options

The `idsync resync` command accepts the following options.

Table 6–2 *idsync resync Usage*

Argument	Meaning
<code>-a <ldap-filter></code>	Specifies an LDAP filter to limit the entries to be synchronized. The filter will be applied to the source of the resynchronization operation. For example, if you specify <code>idsync resync -o Sun -a "uid=*" </code> all Directory Server users that have a <code>uid</code> attribute will be synchronized to Active Directory.
<code>-l <sul-to-sync></code>	Specifies individual Synchronization User Lists (SULs) to resynchronize Note: You can specify multiple SUL IDs to resynchronize multiple SULs or, if you do not specify any SUL IDs, the program will resynchronize all of your SULs.
<code>-o (Sun Windows)</code>	Specifies the source of the resynchronization operation <ul style="list-style-type: none"> ■ Sun: Sets attribute values for Windows entries to corresponding attribute values in Sun Java System Directory Server directory source entries. ■ Windows: Sets attribute values for Sun Java System Directory Server entries to corresponding attribute values in Windows directory source entries. <p>(Default is Windows)</p>
<code>-c</code>	Creates a user entry automatically if the corresponding user is not found at destination <ul style="list-style-type: none"> ■ Randomly generates a cryptographically secure password for users created in Active Directory or Windows NT. ■ Automatically creates a special password value (<code>{PSWSYNC}*INVALID PASSWORD*</code>) for users created in Directory Server (unless you specify the <code>-i</code> option) <p>Note: Identity Synchronization for Windows will attempt to create users even if you have not configured creations in that direction. For example, if you have not configured Identity Synchronization for Windows to synchronize from Windows to Sun (or vice versa), but you specify the <code>-c</code> argument, Identity Synchronization for Windows will try to create users that are not found.</p>

Table 6–2 (Cont.) idsync resync Usage

Argument	Meaning
-i (ALL_USERS NEW_USERS)	Resets passwords for user entries synchronized in a Sun directory source, forcing password synchronization within the current domain for those users the next time the user password is required. <ul style="list-style-type: none"> ■ ALL_USERS: Forces on-demand password synchronization for all synchronized users ■ NEW_USERS: Forces on-demand password synchronization for newly created users only
-u	Updates the object cache. This argument updates the local cache of user entries for a Windows directory source only, which prevents existing Windows users from being created in Directory Server. If you use this argument, Windows user entries are not synchronized with Directory Server user entries. This argument is valid only when the resync source is Windows.
-x	Deletes all destination user entries that do not match a source entry.
-n	Runs in safe mode so you can preview the effects of an operation with no actual changes.

Table 6–3 Will idsync resync invalidate the user's password on Directory Server?

	User has an entry on Active Directory and on Directory Server that is linked.	User has an entry on Active Directory and on Directory Server that are not linked.	User has an entry on Active Directory, but not on Directory Server.
-i ALL_USERS	Yes	Yes	Yes
-i NEW_USERS	No	No	Yes
No -i value	No	No	No

The following table provides examples to illustrate the results of combining different arguments (The -h, -p, -D, -w, -, and -s arguments are defaulted and have been omitted for brevity).

Table 6–4 idsync resync Usage Samples

Arguments	Result
idsync resync	Displays a <code>resync</code> usage statement.
idsync resync -i ALL_USERS	Invalidates the passwords of all users to force on-demand password synchronization (valid in Active Directory environments only). In mixed environments (with both Active Directory and NT domains), you must explicitly list Active Directory SULs.
idsync resync -c -i NEW_USERS	Creates users that are not found on Directory Server and invalidates their passwords to force on-demand password synchronization. Use this command to populate an empty Directory Server instance with existing Windows users.

Table 6–4 (Cont.) *idsync resync Usage Samples*

Arguments	Result
<code>idsync resync</code>	Displays a <code>resync</code> usage statement.
<code>idsync resync -c -l SUL_sales -l SUL_finance</code>	Creates all existing Active Directory users on Directory Server for the <code>SUL_sales</code> and <code>SUL_finance</code> SULs only (but does not force on-demand password synchronization).
<code>idsync resync -n</code>	Runs in safe mode so you can preview the effects of the <code>resync</code> operation with no actual changes.
<code>idsync resync -o Sun -a "(sn=Smith)"</code>	Synchronizes all Directory Server users with the last name (<code>sn</code>) Smith, on Windows.
<code>idsync resync -u</code>	Updates the object cache for Windows Connectors only to prevent existing users from being created in Directory Server. No users are actually synchronized.
<code>idsync resync -f link.cfg</code>	Links unlinked users based on linking criteria specified in the <code>link.cfg</code> file. Identity Synchronization for Windows does not create or modify users, but the Directory Server passwords of newly linked users will be set to the Active Directory users' passwords.

Note: When you use `idsync resync` to link users, be aware that you should use indexes for the operation. Non-indexes can affect performance.

If there are multiple attributes in the `UserMatchingCriteria` set, and at least one of them is indexed, then performance will probably be acceptable. However, if there are no indexes in `UserMatchingCriteria`, then performance will be unacceptable with a large directory.

6.3 Checking Results in the Central Log

The results of all `idsync resync` operations are reported in a special central log named `resync.log`. This log lists all of the users that were properly linked and synchronized, those that failed to link, and those that were previously linked.

Note: Some pre-existing special Active Directory users (such as Administrator and Guest) might appear in this log as failures.

6.4 Starting and Stopping Synchronization

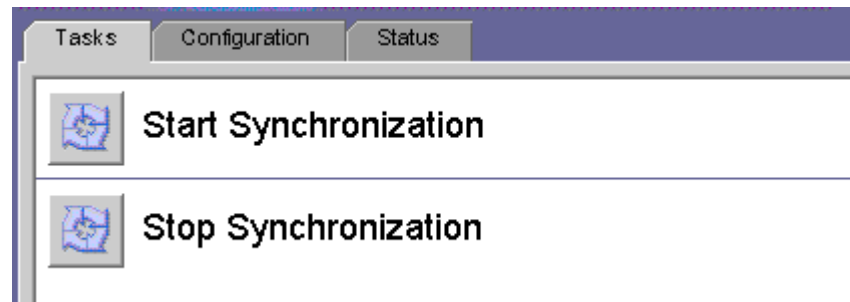
Starting and stopping synchronization *does not* start or stop individual Java processes, daemons, or services. Once you begin synchronization, stopping synchronization only pauses the operation. When you restart synchronization, the program resumes synchronization from where it stopped and no changes will be lost.

6.4.1 To Start or Stop Synchronization

1. In the Sun Java System Server Console navigation pane, select the Identity Synchronization for Windows instance.

2. When the Identity Synchronization for Windows pane is displayed, click the Open button in the upper right corner.
3. When you are prompted, enter the configuration password.
4. Select the Tasks tab.

Figure 6–1 Starting and Stopping Synchronization



- To start synchronization, click Start Synchronization.
- To stop synchronization, click Stop Synchronization.

Note: You can also start and stop synchronization using the `idsync startsync` and `idsync stopsync` command line utilities. For detailed instructions, see [Using startsync](#) and [Using stopsync](#)

6.5 Resynchronized Users/Groups

To resynchronize groups, the Group Synchronization feature must be enabled either through the console or through the command line interface.

To know about how to enable the Group Synchronization feature, see [Specifying Configuration Settings for Group Synchronization](#)

6.6 Starting and Stopping Services

Identity Synchronization for Windows and Message Queue are installed as *daemons* on Solaris and Linux, and as *services* on Windows. These processes start automatically when the system boots, but you can also start and stop them manually, as follows:

- **On Solaris:** From the command line,
 - Enter `/etc/init.d/isw start` to start all Identity Synchronization for Windows processes.
 - Enter `/etc/init.d/isw stop` to stop all Identity Synchronization for Windows processes.
 - Enter `/etc/init.d/imq start` to start the Message Queue broker.
 - Enter `/etc/init.d/imq stop` to stop the Message Queue broker.
- **On Linux:** From the command line,
 - Enter `/etc/init.d/isw start` to start all Identity Synchronization for Windows processes.

- Enter `/etc/init.d/isw stop` to stop all Identity Synchronization for Windows processes.
- Enter `/etc/init.d/imq start` to start the Message Queue broker.
- Enter `/etc/init.d/imq stop` to stop the Message Queue broker.
- On Windows, use one of the following methods.
 - From the Windows Start menu:**
 1. Select Start > Settings > Control Panel > Administrative Services.
 2. When the Administrative Services dialog box is displayed, double-click the Services icon to open the Services dialog box.
 3. Select Identity Synchronization for Windows and then select Action > Start (or Stop) from the menu bar. Repeat for iMQ Broker.

From the command line:

Enter the `net` command to control the services.

Note: Pause 30 seconds after stopping the Identity Synchronization for Windows daemon/service before starting it again. Connectors can take several seconds to cleanly shut themselves down.

Removing the Software

This section contains procedures for removing Identity Synchronization for Windows 6.0 SP1 in the following sections:

- [Planning for Uninstallation](#)
- [Uninstalling the Software](#)
- [Uninstalling the Console Manually](#)

7.1 Planning for Uninstallation

Before removing the software keep in mind the following points:

- You must uninstall subcomponents and the Directory Server Plug-in before you uninstall their associated connectors, and uninstall all the connectors before Core. (The Active Directory Connector does not have any subcomponents to uninstall.)

Failure to uninstall one of these components in the proper order will prevent you from selecting and uninstalling the other components. For example, if you do not uninstall the connectors first, you cannot select Core for uninstallation.

- You must uninstall the Directory Server Plug-in before you uninstall Core.

Uninstalling Core first will remove the Plug-in bits without unregistering them from the Directory Server, which prevents the Directory Server from starting unless you manually remove `cn=pswsync`, `cn=plugins`, `cn=config`.

- In replicated environments with replicas (in addition to primary and secondary servers) you must uninstall the Directory Server Plug-in and then restart the servers.
- The order in which you uninstall connectors does not matter.
- After uninstalling a Sun Java System Directory Server or Windows Connector, you must perform some additional steps to reinstall the Connector on a different machine or to use a different server port.

In this case, you must uninstall and reinstall all of the corresponding subcomponents, and restart the Identity Synchronization for Windows daemon/service where Core is installed (see [Starting and Stopping Services](#)).

- You must run the `uninstall.cmd` script (located in the `isw-hostname` directory) on Windows 2000 and NT platforms. (You must run this batch file as Administrator.)
- You must run the `runUninstall.sh` script (located in the installation directory, `/opt/SUN/isw`, by default) on the Solaris or Linux operating systems. (You must run this script as root.)

Note: You must follow the instructions for uninstalling product components and subcomponents *explicitly*, and verify that you have uninstalled all components successfully.

7.2 Uninstalling the Software

Your system may contain any or all of the following Identity Synchronization for Windows components:

- Active Directory Connectors
- Directory Server Connectors and Plug-ins
- Core

Your Windows NT system may contain the Windows NT Connector and subcomponents.

Use `runUninstaller.sh` (Solaris), `uninstaller.sh` (Linux), or `uninstall.cmd` (Windows) to remove all connectors and subcomponents and then remove Core (if installed).

This section provides instructions for the following:

- [Uninstalling Connectors](#)
- [To Uninstall Core](#)

7.2.1 Uninstalling Connectors

7.2.1.1 To Uninstall the Connectors

1. Start the uninstaller program (`runUninstaller.sh` on Solaris, `uninstaller.sh` on Linux, or `uninstall.cmd` on Windows).
These programs are located in the installation directory (which is the `/opt/SUNWisw` directory by default).
2. At the Welcome screen click Next.
3. Enter the Configuration Directory Host name and Port number.
 - Select the root suffix of the configuration directory. (If necessary, click Refresh to see the list of suffixes.)
 - For secure communication between the uninstall program and the configuration directory server, enable the Secure Port box and specify the Directory Server's SSL port number.
4. Enter your administrator's name and password for the configuration directory.
5. Select the connector(s) to be uninstalled.

Note: The selected connectors *must* be present on the target host.

6. Click Next to perform further uninstallation related tasks.
7. A summary window appears. Please follow the instructions presented in this window.

- **On Solaris systems:** Uninstallation logs are written to `/var/sadm/install/logs/`
- **On Linux systems:** Uninstallation logs are written to `/var/sadm/install/logs/`
- **On Windows systems:** Uninstallation logs are written to the `%TEMP%` directory, which is a subdirectory of the `Local Settings` folder located in `C:\Documents and Settings\Administrator`

Note: On some Windows systems such as Windows 2000 Advanced Server, the `Local Settings` folder is a hidden folder. To view this folder and the `Temp` subdirectory:

Open your Windows Explorer and select `Tools > Folder Options` from the menu bar. When the `Folder Options` dialog box is displayed, select the `View` tab and enable the `Show Hidden Files` option.

8. Click `Close` to exit the program.
9. If there are no other connectors installed on the target host, then you can safely remove the `isw-hostname` folder.
10. Repeat [Uninstalling Connectors](#) for all hosts where connectors are installed.

7.2.2 To Uninstall Core

Note: You must uninstall the `Directory Server Plug-in` before you uninstall `Core`.

Uninstalling `Core` before the `Plug-in` removes the `Plug-in` bits without unregistering them from the `Directory Server`, which will prevent the `Directory Server` from starting unless you manually remove `cn=pswsync`, `cn=plugins`, `cn=config`.

Use the following instructions to uninstall `Core`:

1. Start the uninstaller program:
 - On **Windows** machines:
 - a. Click `Start`, and then choose `Settings > Control Panel`.
 - b. Double-click `Add/Remove Programs`.
 - c. In the `Add/Remove Programs` window, select `name="ProductName" content="Identity Synchronization for Windows"`, then click `Remove`.
2. Start the uninstaller.
 - On Solaris, execute `runUninstaller.sh`.
 - On Linux, execute `uninstaller.sh`.
 - On Windows, execute `uninstall.cmd`.

These programs are located in the installation directory (which is the `/opt/SUNWiwsw` directory on Solaris and `/opt/sun/iwsw` directory on Linux by default).

3. In the Welcome screen click Next.
4. Enter the Configuration Directory Host name and Port number.
 - a. Select the root suffix of the configuration directory. (If necessary, click Refresh to see the list of suffixes.)
 - b. For secure communication between the uninstall program and the configuration directory server, enable the Secure Port box and specify the Directory Server's SSL port number.
5. Enter your administrator's name and password for the configuration directory.
6. Select Core to be uninstalled and click Next.
7. Enter the configuration directory URL, click Refresh, and select the appropriate root suffix from the drop-down list.
8. Click Next to perform further uninstallation related tasks.
9. A summary window appears. Please follow the instructions presented in this window.
 - a. **On Solaris systems:** Uninstallation logs are written to `/var/sadm/install/logs/`
 - b. **On Linux systems:** Uninstallation logs are written to `/var/sadm/install/logs/`
 - c. **On Windows systems:** Uninstallation logs are written to the `%TEMP%` directory, which is a subdirectory of the `Local Settings` folder located under
`C:\Documents and Settings\Administrator`
On some Windows systems (such as Windows 2000 Advanced Server), the `Local Settings` folder is a hidden folder.
To view this folder and the `Temp` subdirectory:
Open your Windows Explorer and select `Tools > Folder Options` from the menu bar. When the Folder Options dialog box is displayed, select the `View` tab and enable the `Show Hidden Files` option.
10. Click Close to exit the program.

7.3 Uninstalling the Console Manually

After you have removed all other Identity Synchronization for Windows components, you may have to manually uninstall the Console.

7.3.1 From Solaris or Linux Systems

7.3.1.1 To Uninstall the Console from Solaris or Linux

1. Delete the following subtree from the configuration directory:
`cn=Sun Java (TM) System Identity Synchronization for Windows,
cn=server_group,cn=hostname,`

`ou=domain_name, o=netscaperoot`

2. For all console installations, remove all of the `.jar` files with an *isw* prefix from the following directory:

`serverroot/server/java/jars`

7.3.2 From Windows Systems

7.3.2.1 To Uninstall the Console from a Windows Active Directory or NT system

1. Delete the following subtree from the configuration directory:

`cn=Sun Java (TM) System Identity Synchronization for Windows,
cn=server_group, cn=hostname,
ou=domain_name, o=netscaperoot`

2. For all console installations, remove all of the `.jar` files with an *isw* prefix from the following directory:

`serverroot/server/java/jars`

Configuring Security

This chapter provides important information about configuring security for your deployment. The information is organized as follows:

- [Security Overview](#)
- [Hardening Your Security](#)
- [Securing Replicated Configurations](#)
- [Using idsync certinfo](#)
- [Enabling SSL in Directory Server](#)
- [Enabling SSL in the Active Directory Connector](#)
- [Adding Active Directory Certificates to Directory Server](#)
- [Adding Directory Server Certificates to the Directory Server Connector](#)

Note: This chapter assumes that you are familiar with the basic concepts of public-key cryptography and Secure Sockets Layer (SSL) protocol, and that you understand the concepts of intranet, extranet, Internet security, and the role of digital certificates in an enterprise. If you are new to these concepts, please refer to the security-related appendixes of the *Managing Servers with iPlanet Console 5.0* manual.

8.1 Security Overview

Passwords are sensitive information; therefore, Identity Synchronization for Windows takes security precautions to ensure that user and administrative password credentials used to access the directories being synchronized are not compromised.

This section covers the following security methodologies:

- [Specifying a Configuration Password](#)
- [Using SSL](#)
- [Generated 3DES Keys](#)
- [SSL and 3DES Keys Protection Summary](#)
- [Message Queue Access Controls](#)
- [Directory Credentials](#)
- [Persistent Storage Protection Summary](#)

This security approach aims to prevent the following events from taking place:

- An eavesdropper intercepting a clear text password over the network
- An attacker manipulating a connector to change a user's password to a value of their choosing, which is equivalent to capturing the user's clear text password
- An attacker gaining access to a privileged component of Identity Synchronization for Windows
- An unprivileged user recovering a password from a file stored on disk.
- An intruder recovering a password from a hard disk that was removed from one of the components of the system. This could be a password being synchronized, or it could be a system password that is used to access a directory.

8.1.1 Specifying a Configuration Password

To protect sensitive information while it is stored in the product's configuration directory and while it is transferred over the network, Identity Synchronization for Windows uses a *configuration password*. You (the administrator) specify a configuration password when you install Core, and you must provide this password when you open the Console or run the Identity Synchronization for Windows installation program.

Note: The system manager must access the configuration password before passing it to the connector; consequently, the system manager stores this password in its initialization file.

File system access controls prevent non-privileged users from accessing the system manager's initialization file. The Identity Synchronization for Windows installation program does not enforce a password policy for this password.

To increase security when you select a configuration password, see [Hardening Your Security](#).

8.1.2 Using SSL

You can configure Identity Synchronization for Windows to use LDAP over SSL everywhere that components use LDAP. All access to Message Queue is protected with SSL.

You must use SSL between the Active Directory Connector and Active Directory when you are synchronizing from Directory Server to Active Directory.

8.1.3 Requiring Trusted SSL Certificates

By default, connectors configured to use SSL will accept any SSL certificate that the server (i.e. Directory Server or Active Directory) returns — which includes untrusted, expired, and invalid certificates. All network traffic between the connector and server will be encrypted, but the connector will not detect a server that is impersonating the true Active Directory or Directory Server.

To force the connector to accept only trusted certificates, use the Console to enable the Require trusted SSL certificates option on the Specify Advanced Security Options panel of the Directory Source Configuration wizard (see [Creating an Active Directory Source](#)). After enabling this option, you must add the appropriate CA certificates to the connector's certificate database as reported by `idsync certinfo`.

8.1.4 Generated 3DES Keys

A 3DES key generated from the configuration password is used to secure all sensitive information in the product's configuration directory. With the exception of log messages, all messages to the Message Queue are encrypted with per-topic 3DES keys. Messages sent between connectors and subcomponents are encrypted with per session 3DES keys. The Directory Server Plug-in encrypts all user password changes with a 3DES key.

8.1.5 SSL and 3DES Keys Protection Summary

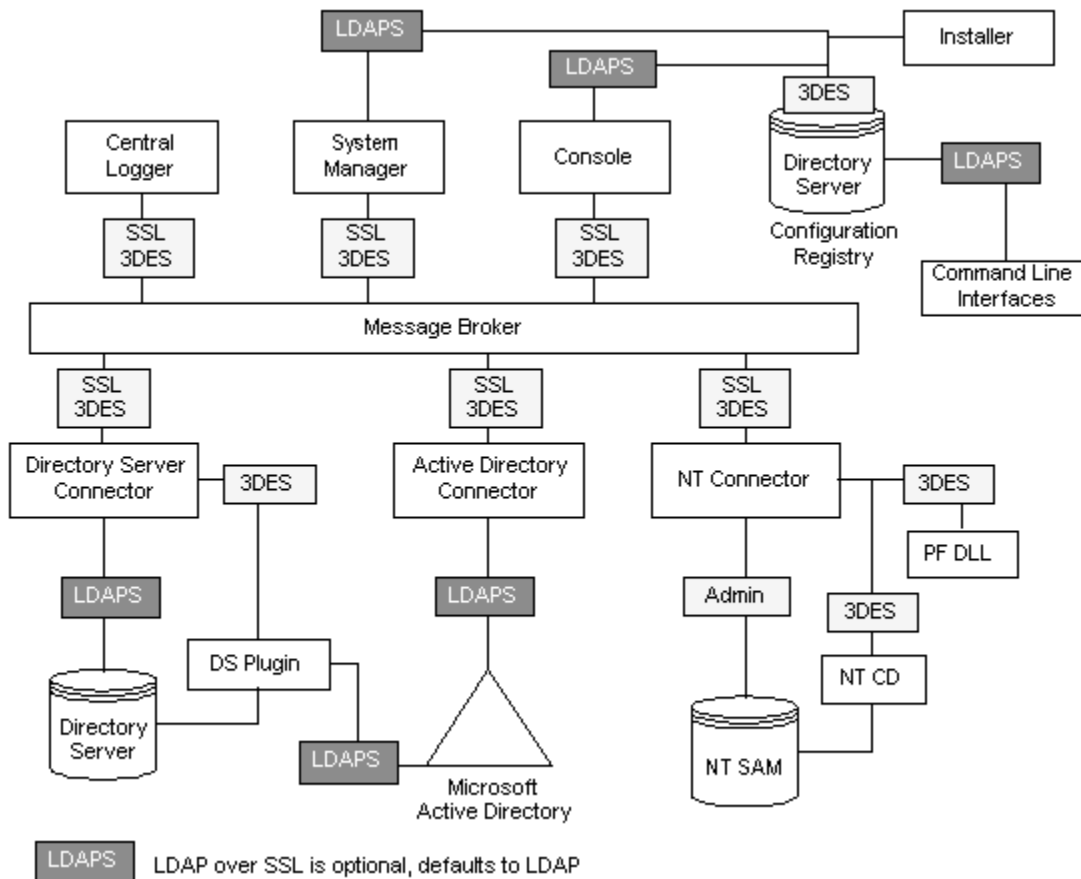
[SSL and 3DES Keys Protection Summary](#) summarizes how Identity Synchronization for Windows protects sensitive information that is sent over the network.

Table 8–1 Protecting Sensitive Information Using Network Security

Use this Protection Method	Between the Following Information Types:
LDAP over SSL (optional)	<ul style="list-style-type: none"> ▪ Directory Server Connector and Directory Server, Active Directory Connector and Active Directory ▪ Directory Server Plug-in and Active Directory ▪ Command line interfaces and the product's configuration directory ▪ Console and the product's configuration directory ▪ Console and Active Directory Global Catalog ▪ Console and Active Directory domains or Directory Servers being synchronized ▪ Message Queue broker and the product's configuration directory ▪ Connectors, system manager, central logger, command line interfaces, and Console may authenticate the Message Queue over LDAPS ▪ Installer and the Configuration Directory Server ▪ Installer and Active Directory ▪ Installer and the Directory Server being synchronized
Encrypted with 3DES keys (default)	<ul style="list-style-type: none"> ▪ Directory Server Connector and Directory Server Plug-in (all data) ▪ Windows NT Connector, Windows NT Password Filter DLL, and Windows NT Change Detector (all data) ▪ All sensitive information in the product's configuration directory ▪ All messages sent between connectors and subcomponents (encrypted with per-session 3DES keys) ▪ All (non-log) messages sent over Message Queue

[SSL and 3DES Keys Protection Summary](#) contains an overview of the security features discussed in this section.

Figure 8–1 Security Overview for Identity Synchronization for Windows



8.1.6 Message Queue Access Controls

Identity Synchronization for Windows uses Message Queue's access control to prevent unauthorized access to message subscription and publishing, allowing each connector to trust messages that it receives.

Unique username and passwords known only to Message Queue and to the connector are provided to access the Message Queue broker. Each message sent over the Message Queue is encrypted with a per topic 3DES key, which protects the message contents and prevents outsiders who do not know the topic key from sending meaningful messages. These measures prevent (a) an attacker from sending falsified password synchronization messages to connectors and (b) an attacker from impersonating a connector and receiving actual password updates.

Note: By default, clients of the Message Queue, such as the connectors and system manager, accept any SSL certificate that the Message Queue broker returns. See [Hardening Your Security](#) for more information to enhance Message Queue certificate validation and other Message Queue-related security issues.

8.1.7 Directory Credentials

Privileged credentials are required by the connectors to change passwords in Active Directory and the Directory Servers being synchronized. These privileged credentials are encrypted before they are stored in the product's configuration directory.

8.1.8 Persistent Storage Protection Summary

[Persistent Storage Protection Summary](#) summarize how Identity Synchronization for Windows protects sensitive information that is stored on disk.

Table 8–2 Persistent Storage Protection

Persistent Storage	Confidential Information	Protection
Product's Configuration Stored in a Configuration Directory Server	Credentials for accessing the directories and per Message Queue topic 3DES keys are stored in the product's configuration directory.	All sensitive information stored in the product's configuration directory is encrypted with a 3DES key that is generated from the configuration password. See Hardening Your Security for recommendations to further protect the product's configuration directory.
Directory Server Retro Changelog	The Directory Server Plug-in captures password changes and encrypts them before writing them to the Directory Server Retro Changelog.	The Directory Server Plug-in encrypts all user password changes with a 3DES key that is unique to each deployment.
Message Queue Broker Persistent Storage	The Message Queue broker stores password synchronization messages sent between all connectors.	With the exception of log messages, all persisted messages are encrypted with per-topic 3DES keys.
Message Queue Broker Directory Credentials	The Message Queue broker authenticates users against the product's configuration directory. It connects to the configuration directory using the directory administrative user name and password provided during Core installation.	The directory password is stored in a passfile, which is protected with file system access controls.
System Manager Boot File	The system manager's boot file contains information for accessing the configuration. This includes the configuration password and the directory administrative user name and password provided during Core installation.	This file is protected with file system access controls.
Connectors and Central Logger Boot Files	Each connector as well as the central logger have an initial configuration file with credentials for accessing the Message Queue.	These files are protected with file system access controls.
Directory Server Plug-in Boot Configuration	The Plug-in's configuration, stored in <code>cn=config</code> , includes credentials for connecting to the connector.	The <code>cn=config</code> subtree is protected with ACIs and the <code>dse.ldif</code> file, which mirrors this tree, is protected with file system access controls.
NT Password Filter DLL and NT Change Detector Boot Configuration	The NT subcomponent's configuration, which is stored in the Windows registry, includes credentials for connecting to the connector.	If access to the PDCs registry is not secure, these registry keys can be protected with access controls.
Windows Connector's Object Cache	Windows connectors store hashed user passwords in the connector's object cache.	The passwords are not stored in the clear but encrypted with MD5 hashes. These database files are protected with file system access controls. (see Hardening Your Security)

8.2 Hardening Your Security

This section depicts potential security weaknesses in the current release of the product and recommendations as to how to extend and harden security outside the product's default configuration. It includes the following:

- [Configuration Password](#)
- [Creating Configuration Directory Credentials](#)
- [Message Queue Client Certificate Validation](#)
- [Message Queue Self-Signed SSL Certificate](#)
- [Access to the Message Queue Broker](#)
- [Configuration Directory Certificate Validation](#)
- [Restricting Access to the Configuration Directory](#)

8.2.1 Configuration Password

The configuration password is used to protect sensitive configuration information but the installation program does not enforce any password policy for this password; be sure that this password follows some strict guidelines choose a complex password that is not easily guessed and follow standard policy guidelines for strong passwords.

For example, it should be at least eight characters long, include upper case letters, lower case letters, and non-alphanumeric characters. It should not include your name, initials, or dates.

8.2.2 Creating Configuration Directory Credentials

To access the Directory Server where the product's configuration directory resides, your credentials must be in the Configuration Administrators group. However, if you need to create credentials other than *admin* for any reason, consider the following:

The installation program requires you to provide credentials for a user stored in the Console administrative subtree. However, the Core installation program will not expand users other than *admin* into "uid=admin, ou=Administrators, ou=TopologyManagement, o=NetscapeRoot". Therefore, you must specify the entire DN during Core installation.

8.2.2.1 To Create a New User Other Than *admin*

1. Create a user in:

```
ou=Administrators, ou=TopologyManagement, o=NetscapeRoot
```

2. Add the new credentials to the Configuration Administrators group.
3. Set ACIs to allow only this user or all users in the Configuration Administrators group to access the Directory Server where the product's configuration directory is stored.
4. Specify entire DN during Core installation.

For more information about managing access controls in the Directory Server, see Chapter 6, *Directory Server Access Control*, in *Administrator's Guide for Oracle Directory Server Enterprise Edition*

8.2.3 Message Queue Client Certificate Validation

By default, clients of the Message Queue, such as the connectors and system manager, accept any SSL certificate that the Message Queue broker returns.

8.2.3.1 To Validate the Message Queue Client Certificate

1. To override this setting and force Message Queue clients to validate the Message Queue broker's certificate, edit:

```
installation_root /resources/WatchList.properties
```

2. Add the following to the JVM arguments of each process in `Watchlist.properties`:

```
-Djavax.net.ssl.trustStore=keystore_path-DimqSSLIsHostTrusted=false
```

3. Restart the Identity Synchronization for Windows daemon or service.

The `javax.net.ssl.trustStore` property should point to a JSEE keystore that trusts the broker certificate, for example, `/etc/imq/keystore` can be used on the machine where Core was installed because this is the same keystore used by the broker.

8.2.4 Message Queue Self-Signed SSL Certificate

By default, the Message Queue broker uses a self-signed SSL certificate. To install a different certificate, use the `keytool` utility that ships with Java to modify the broker's keystore (`/var/imq/instances/isw-broker/etc/keystore` on Solaris, `/var/opt/sun/mq/instances/isw-broker/etc/keystore` on Linux, and `mq_installation_root /var/instances/isw-broker/etc/keystore` on Windows 2000). The alias of the certificate must be `imq`.

8.2.5 Access to the Message Queue Broker

By default, the Message Queue uses dynamic ports for all services except for its port mapper. To access the broker through a firewall or restrict the set of hosts that can connect to the broker, the broker should use fixed ports for all services.

This can be achieved by setting the `imq.service_name protocol_type .port` broker configuration properties. Refer to the *Sun Java System Message Queue Administration Guide* for more information.

8.2.6 Configuration Directory Certificate Validation

The system manager accepts any certificate when connecting to the product's configuration directory over SSL; the Message Queue broker accepts any certificate when connecting to the product's configuration directory over SSL. Currently, there is no way to make either the system manager or the Message Queue broker validate the product's configuration directory SSL certificates.

8.2.7 Restricting Access to the Configuration Directory

When Core is installed, the process of adding information to the Directory Server where the product's configuration directory is stored does not include adding any access control information. To restrict access to only configuration Administrators, the following ACI can be used:

```
(targetattr = "*")
(target = "ldap://ou=IdentitySynchronization,
ou=Services,dc=example,dc=com")
(version 3.0;acl "Test";deny (all)
(groupdn != "ldap://cn=Configuration Administrators,
ou=Groups, ou=TopologyManagement, o=NetscapeRoot");)
```

For more information about managing access controls in the Directory Server, see Chapter 6, *Directory Server Access Control*, in *Administrator's Guide for Oracle Directory Server Enterprise Edition*

8.3 Securing Replicated Configurations

Deployments connecting to Directory Servers using replication follow the same rules identified in [Security Overview](#). This section gives an example replicated configuration and explains how to enable use of SSL in this configuration.

Note: For an overview of planning, deploying, and securing replicated configurations see [Appendix D, "Defining and Configuring Synchronization User Lists for Identity Synchronization for Windows"](#)

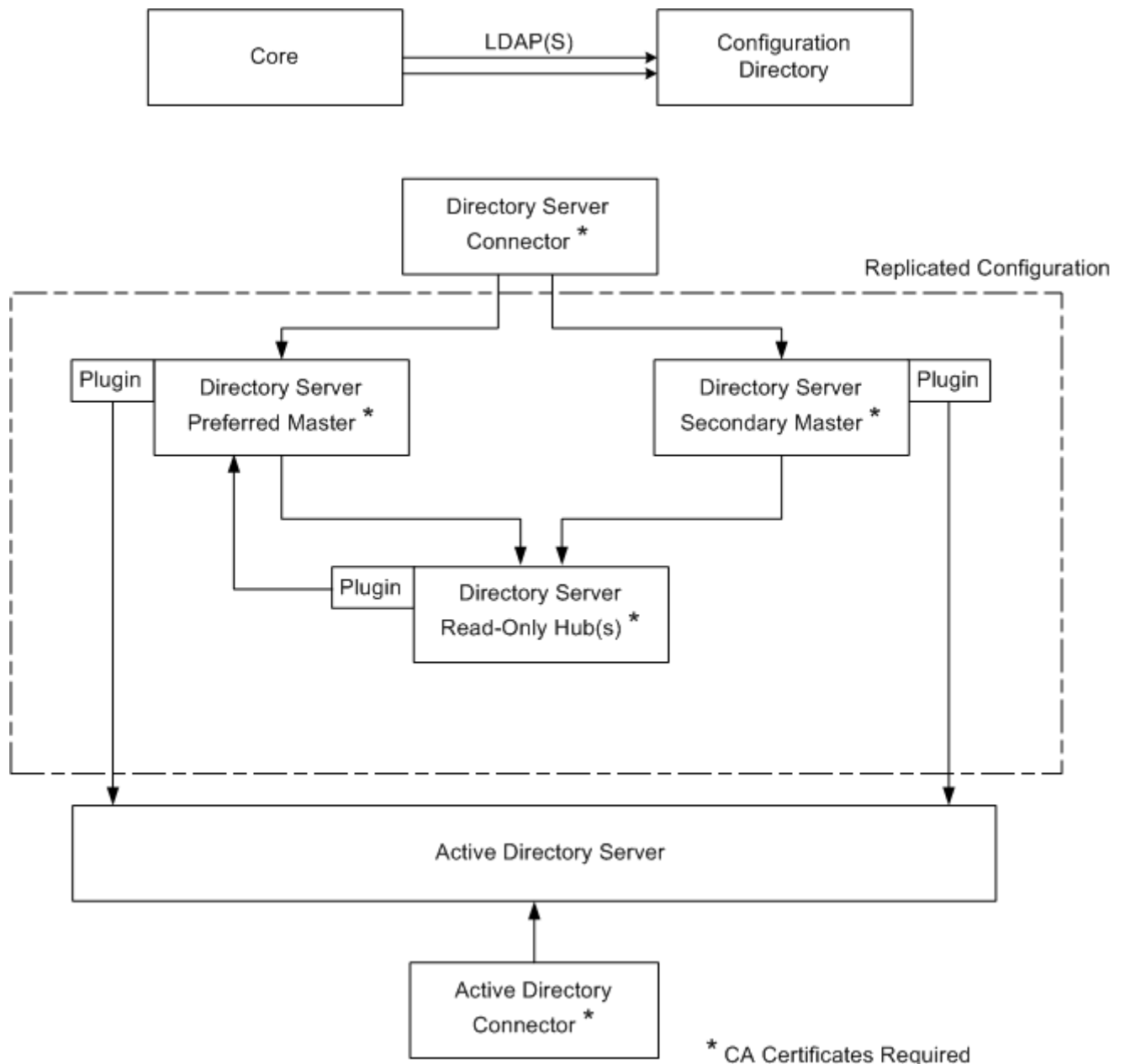
[Securing Replicated Configurations](#) lists the configuration components requiring CA certificates and identifies which certificates are required where.

Table 8–3 *Securing Replicated Configurations*

Component	Required CA certificates
Preferred Directory Server Replicated Master	Active Directory System
Secondary Directory Server Replicated Master	Active Directory System
Read-only Directory Server Hub(s)	Preferred Directory Server Replicated Master Secondary Directory Server Replicated Master
Directory Server Connector	Preferred Directory Server Replicated Master Secondary Directory Server Replicated Master
Active Directory Connector	Active Directory System

Replicated configuration shows Identity Synchronization for Windows installed in an MMR configuration, where there are two replicated Directory Server masters with multiple Directory Server read-only hubs or consumers. Each Directory Server has a Plug-in and there is only one Directory Server Connector, one Active Directory system, and one Active Directory Connector.

Figure 8-2 Replicated Configuration



When the Directory Server source is configured for SSL, you must make sure that both the preferred and secondary Directory Server certificates are trusted by the replica Directory Server. This is true for every Directory Server Plug-in of type `other` that you install on a system with a Directory Server hub or read-only replica.

Note: Directory Server Plug-ins have access to the same CA certificates as its associated Directory Server.

The above diagram is specific to two Directory Server masters. But you can extend this to contain multiple masters.

8.4 Using idsync certinfo

Use the `idsync certinfo` utility to determine what certificates are required based on the current Identity Synchronization for Windows SSL settings. Execute `idsync certinfo` to retrieve information about what certificates are required in each certificate database.

Note: You must be sure that when you are configuring the Directory Server source for SSL, both the preferred and secondary Directory Server source certificates are trusted by the replica Directory Server for all Directory subcomponents or Plug-ins.

If Identity Synchronization for Windows tries to establish SSL connections (with the trust all certificates setting enabled), and the server's hostname does not match the hostname provided in the certificate presented by the server during the SSL negotiation phase, the Identity Synchronization for Windows Connector will refuse to establish the connection.

The directory source hostname in the Identity Synchronization for Windows configuration must always match the hostname embedded in the certificate used by that directory source.

8.4.1 Arguments

Arguments describes the arguments you can use with the `idsync certinfo` subcommand.

Table 8–4 *certinfo Arguments*

Argument	Description
-h <i>CR-hostname</i>	Specifies the configuration directory hostname. This argument defaults to the values specified during Core installation.
-p <i>CR-port-no</i>	Specifies the configuration directory LDAP port number. (<i>Default is 389</i>)
-D <i>bind-DN</i>	Specifies the configuration directory bind distinguished name (DN). This argument defaults to the values specified during Core installation.
-w <i>bind-password</i> -	Specifies the configuration directory bind password. The - value reads the password from standard input (STDIN).
-s <i>rootsuffix</i>	Specifies the configuration directory rootsuffix. Where rootsuffix is a distinguished name such as <code>dc=example,dc=com</code> . This argument defaults to the values specified during Core installation.
-q <i>configuration_password</i>	Specifies the configuration password. The - value reads the password from standard input (STDIN).

8.4.2 Usage

The following example uses `idsync certinfo` to search for system components designated to run under SSL communications. The results of this example identifies two connectors (CNN101 and CNN100) and provides instructions as to where to import the appropriate CA certificate.

```
: \Program Files\Sun\MPS\isw-
hostname\bin idsync certinfo -h
```

```

CR-hostname -p 389 -D
"cn=Directory Manager" -w dirmanager -s dc=example,dc=com
-q password
Connector: CNN101
Certificate Database Location: C:\Program Files\Sun\MPS\isw-
hostname\etc\CNN101
Get 'Active Directory CA' certificate from Active Directory
and import into Active Directory Connector certificate db
for server ldaps://
hostname.example.com:636
Connector: CNN100 Certificate Database Location:
C:\Program Files\Sun\MPS\isw-
hostname\etc\CNN100
Export 'Directory Server CA' certificate
from Directory Server certificate db and
import into Directory Server Connector certificate db
ldaps://hostname.example.com:636
Export 'Active Directory CA' certificate
from Active Directory Server
hostname.example.sun.com:389
and import into Directory Server Server certificate db
for server ldaps://hostname.example.com:638
SUCCESS

```

8.5 Enabling SSL in Directory Server

Follow these steps to enable SSL in a Directory Server using a self-signed certificate.

Note: These abbreviated procedures are for your convenience. Refer to the *Administrator's Guide for Oracle Directory Server Enterprise Edition* for more information.

- On Windows, use the `certutil` version bundled with Identity Synchronization for Windows 6.0 SP1 within the `ISW-host-name\shared\bin` folder.
 - On Solaris, `certutil` is installed in `/usr/sfw/bin` by default.
 - On Linux, `certutil` is installed in `/opt/sun/private/bin` by default.
-
-

8.5.1 To Enable SSL in Directory Server

Refer to the following procedure to enable SSL in Directory Server:

1. Create a DS instance

```

/opt/SUNWdsee/ds6/bin/dsadm create -p non-ldap-port-P
ldap-secure-port <DS-server-root>/slapd-<hostname>

```

2. Start the instance

```

/opt/SUNWdsee/ds6/bin/dsadm start
<DS-server-root>/slapd-<hostname>

```

3. Create a self-signed certificate

```
/opt/SUNWdsee/ds6/bin/dsadm add-selfsign-cert -S "cn=<machine
name with domain>,O=<preferred root
suffix>" /<DS-server-root>/slapd-<hostname>/<certificate name>
```

Where S = Create an individual certificate and add it to database, the second variable represents the path of Directory Server instance and the last variable is for the certificate alias.

4. Set the server properties to this certificate

```
/opt/SUNWdsee/ds6/bin/dsconf set-server-prop -p non-ldap-port
ssl-rsa-cert-name:<certificate name>
```

5. Restart the DS

```
/opt/SUNWdsee/ds6/bin/dsadm restart
/<DS-server-root>/slapd-<hostname>/
```

6. Now stop the DS and remove the default certificate (this ensures that the above generated certificate will be the default certificate)

```
/opt/SUNWdsee/ds6/bin/dsadm stop
/<DS-server-root>/slapd-<hostname>/
```

7. Now remove the default certificate

```
/opt/SUNWdsee/ds6/bin/dsadm remove-cert
/<DS-server-root>/slapd-<hostname>/ defaultCert
```

where the first variable represents the slapd-path and the second variable represents the alias of the certificate. In case you want to export the above default certificate, following is the command

```
/opt/SUNWdsee/ds6/bin/dsadm export-cert -o /<any
path>/slapd-cert.export /<DS-server-root>/slapd-<hostname>/
<original default cert alias>
```

where o=output file (/<any path>/slapd-cert.export), the second variable represents the slapd-path and the third variable represents the certificate alias.

8.5.2 Retrieving the CA Certificate from the Directory Server Certificate Database

Ensure that you have enabled SSL in Directory Server. To export the Directory Server certificate to a temporary file so that you can import it into the certificate database of the Directory Server Connector, issue the following command:

```
<ISW-server-root>\shared\bin\certutil.exe -L -d .
-P slapd-hostname- -n server-cert -a \> C:\s-cert.txt
```

ISW-server-root is the path where ISW-hostname directory is present.

These examples are run in the alias directory immediately below the server root. Otherwise, Directory Server will not find the certificate database.

8.5.3 Retrieving the CA Certificate from the Directory Server (using dsadm command on Solaris platform)

Ensure that you have enabled SSL in Directory Server. To retrieve the CA certificate issue the following command:

```
/opt/SUNWdsee/ds6/bin/dsadm export-cert -o /<any path>
/slapd-cert.export /<DS-server-root>/slapd-<hostname>/
<original default cert alias>
```


8.6 Enabling SSL in the Active Directory Connector

Identity Synchronization for Windows *automatically* retrieves Active Directory SSL certificates over SSL and imports them into the Connector's certificate database using the same credentials you provided for the Connector.

However; if an error occurs (for example, invalid credentials or no SSL certificates were found), you can retrieve an Active Directory CA certificate and add it to the Connector certificate database. See the following sections for instructions:

- [Retrieving an Active Directory Certificate](#)
- [Adding Active Directory Certificates to the Connector's Certificate Database](#)

8.6.1 Retrieving an Active Directory Certificate

If an error occurs, you can use `certutil` (a program that ships with Windows 2000/2003) or LDAP to retrieve an Active Directory certificate, as described in the following sections.

Note: The `certutil` command discussed in this section is *not* the same as the `certutil` command that ships with the Directory Server and discussed previously in this publication.

8.6.1.1 Using Window's Certutil

8.6.1.1.1 To Retrieve an Active Directory Certificate Using the `certutil` program

1. Run the following command from the Active Directory machine to export the certificate.

```
C:\>certutil -ca.cert cacert.bin
```

2. You can then import the `cacert.bin` file into a certificate database.

8.6.1.2 Using LDAP

8.6.1.2.1 To Retrieve an Active Directory Certificate using LDAP 1. Execute the following search against Active Directory:

```
ldapsearch -h CR-hostname -D administrator_DN -w administrator_password
-b "cn=configuration,dc=put,dc=your,dc=domain,dc=here" "cacertificate=*
```

Where the `administrator_DN` might look like:

```
cn=administrator,cn=users,dc=put,dc=your,dc=domain,dc=here
```

In this example, the domain name is: `put.your.domain.name.here`.

Several entries will match the search filter. You probably need the entry using `cn=Certification Authorities, cn=Public Key Services` in its DN.

2. Open a text editor and cut the first value of the first CA certificate attribute (it should be a base64 encoded text block). Paste that value (text block) into the text

editor (only the value). Edit the contents, so that none of the lines start with white space.

3. Add-----BEGIN CERTIFICATE----- before the first line and -----END CERTIFICATE----- after the last line. See the following example:

```
-----BEGIN CERTIFICATE-----
MIIDvjCCA2igAwIBAgIQDgoyk+Tu14NGoQnxhmNHLjANBgk
qhkiG9w0BAQUFADCBjjEeMBwGCSqGSIb3DQEJARYPYmVydG
9sZEBzdW4uY29tMQswCQYDVQGEwJVUzELMAkGA1UECBMCV
FgxDzANBgNVBACtBkF1c3RpbjEzMBCGA1UEChMQU3VuIE1p
Y3Jvc3lzdGVtczEQMA4GA1UECXMHaVBSYw51dEUMBIGA1U
EAXMLUmVzdGF1cmFudHMwHhcNMDIwMTExMDE1NDU5WjcNMT
IwMTExMDA1OTQ2WjCBjjEeMBwGCSqGSIb3DQEJARYPYmVyd
G9sZEBzdW4uY29tMQswCQYDVQGEwJVUzELMAkGA1UECBMCV
FgxDzANBgNVBACtBkF1c3RpbjEzMBCGA1UEChMQU3VuIE1p
Y3Jvc3lzdGVtczEQMA4GA1UECXMHaVBSYw51dEUMBIGA1U
EAXMLUmVzdGF1cmFudHMwXDNANBgkqhkiG9w0BAQEFAANLAD
BIAkEAYekZa8gwwhw3rLk3eV/12St1DVUsg31L0u3CnB8cM
HQZXLgiUgtQ0hm2kpZ4nEhwCAHhFLD3iThIP4BGWQFjcwID
AQABo4IBnjjCAAZowEwYJKwYBBAGCNxQCBAYeBABDAEEwCwY
DVR0PBAQDAgFGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0OBB
YEFJ5Bgt6Oypq7T8Oyk4LH6ws2d/IMIIBMgYDVR0fBIIBK
TCCASUwgdOggdCggc2GgcpsZGFwOi8vL0N0PVJlc3RhdXJh
bnRzLENOPWRvd210Y2hlcixDTj1DRFAsQ049UHVibGljJTJl
wS2V5JTlWU2Vydm1jZXMsQ049U2Vydm1jZXMsQ049Q29uZm
lndXJhdGlvbixEQz1yZXN0YXVyYW50cyxEQz1jZW50cmFsL
RPXN1bixEQz1jb20/Y2Vydg1maWVhdGVScXZvY2F0aW9u
TG1zdD9iYXNlP29iamVjdGNsYXNzPWNSSTERpc3RyaWJ1dG1
vb1BvaW50ME2gS6BjHkdodHRwOi8vZG93aXRjaGVyLnJlc3
RhdXJhbnRzLmNlbnRyYWwuc3VuLmNvbS9DZXJ0RW5yb2xsL
1Jlc3RhdXJhbnRzLmNybDAQBgkrBgEeAYI3FQEEAwIBADAN
BgkqhkiG9w0BAQUFAANBAL5R9R+ONDdVHWu/5Sd9Tn9dpXN
8oegjs88ztv1HD6XSTDzGTuaaVebSZV3I+ghSInsgQbH0gW
4fGRwaI BvePI4=
-----END CERTIFICATE-----
```

4. Save the certificate into a file (such as ad-cert.txt).
5. You can then import that file (for example, ad-cert.txt) into a certificate database. Continue to the next section, [Adding Active Directory Certificates to the Connector's Certificate Database](#)

8.6.2 Adding Active Directory Certificates to the Connector's Certificate Database

Use this procedure only if you enabled SSL for the Active Directory Connector after installing the Connector or if invalid credentials were provided during installation.

8.6.2.1 To Add Active Directory Certificate to the Connector's Certificate Database

1. On the machine where the Active Directory Connector is installed, stop the Identity Synchronization for Windows service/daemon.
2. Retrieve the Active Directory CA certificate using one of the following methods:
 - [Using Window's Certutil](#)
 - [Using LDAP](#)
3. Assuming the Active Directory Connector has connector ID CNN101 (see logs/central/error.log for a mapping from connector ID to the directory

source it manages), go to its certificate database directory on the machine where it was installed, and import the certificate file:

- If the certificate was retrieved using `certutil`, type:

```
<ISW-server-root>\shared\bin\certutil.exe -A -d . -n ad-ca-cert -t C,, -i \cacert.bin
```

- If the certificate was retrieved using LDAP, type:

```
<ISW-server-root>\shared\bin\certutil.exe -A -d . -n ad-ca-cert \ -t C,, -a -i \ad-cert.txt
```

ISW-server-root is the path where ISW-hostname directory is present

On Solaris, the certificate can be imported using the `dsadm` command in the following manner:

```
/opt/SUNWdsee/ds6/bin/dsadm add-cert -C <DS-server-root>/slapd-<hostname>/ ad-ca-cert cacert.bin
```

where `ad-ca-cert` is the name of the certificate assigned after the import and `cacert.bin` is the certificate about to be imported

4. Restart the Identity Synchronization for Windows service/daemon.

Note: Because the Directory Server `certutil.exe` is installed automatically when you install Directory Server, you will not be able to add a CA certificate to a connector installed on a machine with no Directory Server.

At a minimum, you must install the Sun Java System Server Basic Libraries and Sun Java System Server Basic System Libraries from the Directory Server package on the server where the Active Directory Connector is installed. (You do not have to install the Administration Server or Directory Server components.)

In addition, be sure to select the JRE subcomponent from the Console (to ensure your ability to uninstall).

8.7 Adding Active Directory Certificates to Directory Server

Note: Make sure that you have enabled SSL in Directory Server.

8.7.1 To Add the Active Directory CA certificate to the Directory Server Certificate Database

1. Retrieve the Active Directory CA certificate using one of the following methods:
 - [Using Window's Certutil](#)
 - [Using LDAP](#)
2. Stop Directory Server.
3. Import `cacert.bin` into the `<DS-server-root>\slapd-hostname\alias` folder on Windows and for Solaris and Linux import it into `<DS-server-root>/slapd-hostname/alias` directory.

4. On the machine where Directory Server is installed, import the Active Directory CA certificate as follows:

- If the certificate was retrieved using `certutil`, type:

```
<ISW_server_root>\shared\bin\certutil.exe -A -d .
-P slapd-hostname- -n ad-ca-cert -t C,, -i \cacert.bin
```

- If the certificate was retrieved using LDAP, type:

```
<ISW_server_root>\shared\bin\certutil.exe -A -d .
-P slapd-hostname- -n ad-ca-cert -t C,, -a -i \ad-cert.txt
```

`ISW-server-root` is the path where `ISW-hostname` directory is present

- If the certificate was retrieved using the `dsadm` command (on Solaris), type:

```
/opt/SUNWdsee/ds6/bin/dsadm add-cert -C <DS-server-root>
/slapd-<hostname>/ ad-ca-cert cacert.bin
```

Where `ad-ca-cert` is the name of the certificate assigned after the import and `cacert.bin` is the certificate about to be imported

5. Start Directory Server.

8.8 Adding Directory Server Certificates to the Directory Server Connector

If you enable SSL communication between the Directory Server Plug-in and Active Directory, then you must add the Active Directory CA Certificate to the certificate database of each Directory Server master.

8.8.1 To Add the Directory Server Certificates to the Directory Server Connector

1. On the machine where the Directory Server Connector is installed, stop the Identity Synchronization for Windows service/daemon.
2. Retrieve the Directory Server CA certificate.
3. Assuming the Directory Server Connector has connector ID `CNN100` (see `logs/example/error.log` for a mapping from connector ID to the directory source it manages), go to its certificate database directory on the machine where it was installed, and import the `cacert.bin` file:

```
<ISW_server_root>\shared\bin\certutil.exe -A -d . -n ds-cert -t C,, -i
C:\s-cert
```

`ISW-server-root` is the path where `ISW-hostname` directory is present.

4. Restart the Identity Synchronization for Windows service/daemon.

Understanding Audit and Error Files

Identity Synchronization for Windows provides information about the installation and configuration status, the day-to-day system operations, and any error conditions that are related to your deployment.

This chapter explains how to access and understand this information in the following sections:

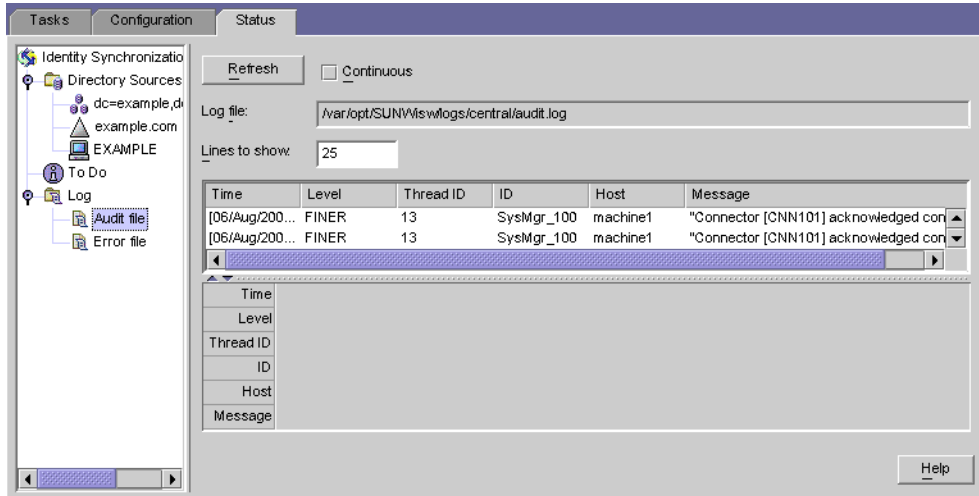
- [Understanding the Logs](#)
- [Configuring Your Log Files](#)
- [Viewing Directory Source Status](#)
- [Viewing Installation and Configuration Status](#)
- [Viewing Audit and Error Logs](#)
- [Enabling Auditing on a Windows NT Machine](#)

9.1 Understanding the Logs

You can view various types of information from the Status tab of the Identity Synchronization for Windows Console.

If you select one of the following nodes in the navigation tree pane (on the left), the content presented on the Status tab changes to provide specific information about that item.

- **Directory Source:** Select a directory source node (such as `dc=example,dc=com`) to view status information about that directory source.
- **To Do:** Select this node for a list of the steps you must complete to successfully install and configure Identity Synchronization for Windows (the program greys-out all completed steps).
- **Audit File:** Select this node for information about day-to-day system operations (including error conditions).
- **Error File:** Select this node for information about error conditions on your system. (The Error log essentially acts as a filter in which only the error entries are displayed.)



9.1.1 Log Types

This section describes the different kinds of logs that are available for Identity Synchronization for Windows:

- [Central Logs](#)
- [Local Component Logs](#)
- [Local Windows NT Subcomponent Logs](#)
- [Directory Server Plug-in Logs](#)

9.1.1.1 Central Logs

As long as Identity Synchronization for Windows components can access Message Queue, all audit and error messages will be logged in the Identity Synchronization for Windows central logger. Consequently, these central logs (which include messages from all components) are the primary logs to monitor.

The centralized logs are located on the machine where Core is installed, in the following directories:

- **On Solaris:** `/var/opt/SUNWisisw/logs`
- **On Linux:** `/var/opt/sun/isw/logs`
- **On Windows:** `installation_root/isw-machine_name/logs/central/`

Table 9–1 Log Types for Identity Synchronization for Windows

Log Name	Description
<code>error.log</code>	Warning and Severe messages are reported here.
<code>audit.log</code>	A superset of <code>error.log</code> that includes messages about each synchronization event.
<code>resync.log</code>	Messages generated by the <code>resync</code> command are reported here.

Each central log also includes information about each component ID. For example,

```
[2003/03/14 14:48:23.296 -0600] INFO 13
"System Component Information:
SysMgr_100 is the system manager (CORE);
```

```
console is the Product Console User Interface;
CNN100 is the connector that manages
[example.com (ldaps:// server1.example.com:636)];
CNN101 is the connector that manages
[dc=example,dc=com (ldap:// server2.example.com:389)];"
```

In addition to the central logger, each component has its own local logs. You can use these local logs to diagnose problems with the connector if it cannot log to the central logger.

9.1.1.2 Local Component Logs

Each connector, the system manager, and the central logger have the following local logs:

Table 9-2 Local Logs

Log Name	Description
<code>audit.log</code>	A superset of <code>error.log</code> that includes messages about each synchronization event. These messages are also written to the central <code>audit.log</code> .
<code>error.log</code>	Warning and Severe messages are reported here. These messages are also written to the central <code>error.log</code> .

These local logs are located in the following subdirectories:

- **On Solaris:** `/var/opt/SUNWisw/logs`
- **On Linux:** `/var/opt/sun/isw/logs`
- **On Windows:** `installation_root/isw-machine_name/logs/central/`

The `sysmgr` and `clogger100` (central logger) directories are on the machine where Core is installed.

Identity Synchronization for Windows rotates these local component logs daily by moving the current log to a log file that includes the date, as follows:

```
audit_2004_08_06.log
```

Note: By default, Identity Synchronization for Windows deletes connector logs after ten days. You can extend this period by editing the `com.sun.directory.wps.logging.maximumDaysToKeepOldLogs` value in the `Log.properties` file and restarting the service daemon.

9.1.1.3 Local Windows NT Subcomponent Logs

The following Windows NT subcomponents also have local logs:

- Windows NT Change Detector DLL
- Password Filter DLL

These subcomponent logs are located in the `SUBC1XX` (for example, `SUBC100`) subdirectories of the following directory:

```
installation_root/isw-machine_name/logs/
```

Identity Synchronization for Windows limits these files to 1 MB in size, and keeps only the last 10 logs.

9.1.1.4 Directory Server Plug-in Logs

The Directory Server Plug-in logs information through the Directory Server connector to the central log and through the Directory Server logging facility. Consequently, local Directory Server Plug-in log messages will also be saved in the Directory Server error log.

Directory Server saves information into the error log from other Directory Server Plug-ins and components. To identify messages from the Identity Synchronization for Windows Directory Server Plug-in, you can filter out lines containing the `isw` string.

By default, only minimal Plug-in log messages are displayed in the error log. For example:

```
[14/Jun/2004:17:08:36 -0500] - ERROR<38747> - isw - conn=-1
op=-1 msgId=-1 - Plug-ins unable to establish connection to DS Connector
at attila:1388, will retry later
```

9.1.1.4.1 To Change the Verbosity Level of the Error Logs You can change the default verbosity level of the Directory Server error log through DSCC as follows:

1. Log in to Directory Service Control Center.
2. On the Directory Servers tab page, click the server whose log level you want to configure.
3. Select the Server Configuration tab, then the Error Logging tab.
4. In the General > Additional Items to Log section, select Plug-Ins.
5. Click Save.

You can enable plug-in logging using the command line.

```
$ dsconf set-log-prop errors level:err-plugins
```

For more information about Directory Server logging, refer to Chapter 14, *Directory Server Logging*, in *Administrator's Guide for Oracle Directory Server Enterprise Edition*.

9.1.2 Reading the Logs

Every log message includes the following information:

- **Time:** Indicates when (time and date) the log entry was generated. For example:

```
[13/Aug/2004:06:14:36:753 -0500]
```

- **Level:** Indicates the severity and verbosity of the log message. Identity Synchronization for Windows uses the following log levels:

Table 9–3 Log Levels

Log Level	Description
INFO	These messages provide a minimum amount of information about each action so you can see that the system is running correctly. For example, you can see when a change is detected and when synchronization occurs. These messages are always logged to the audit log.
FINE	These messages contain more information about an action as it travels through the system.
FINER	These messages contain even more information about an action as it travels through the system. Turning the logging level to FINER for all components may impact performance.
FINEST	These messages contain the most information about an action as it travels through the system. Turning the logging level to FINEST for all components may significantly impact performance.

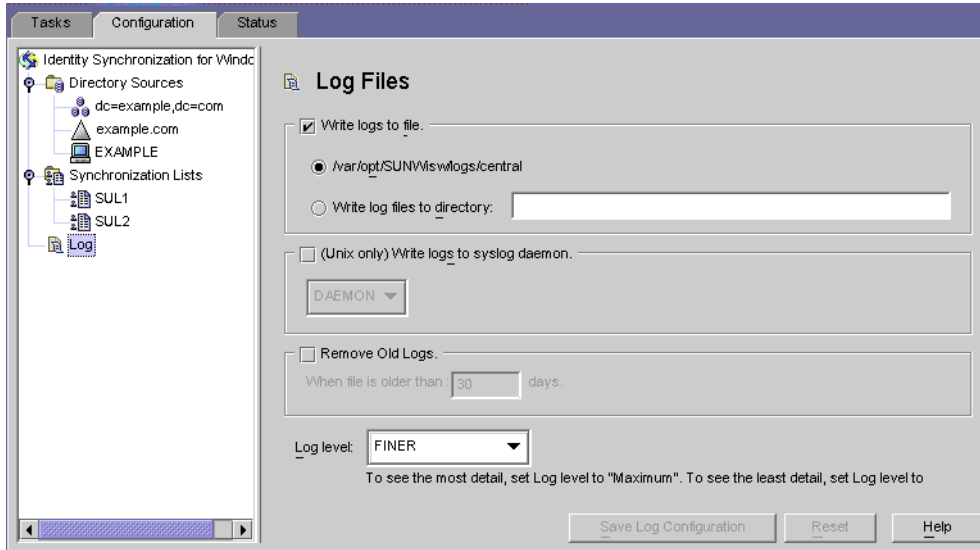
- **Thread ID:** Displays the Java thread ID of the function causing the event.
- **ID:** Identifies the component (console, system manager, and so forth.) causing the event.
- **Host:** Displays the name of the host causing the event.
- **Message:** Displays audit or error information associated with the event. Some examples include:

```
"Resetting Central Logger configuration ..."  
"System manager is shutting down."  
"Processing request (ID=ID_number  
from the console to stop synchronization."
```

9.2 Configuring Your Log Files

9.2.1 To Configure Logging for Your Deployment

1. Open the Console and select the Configuration tab.
2. In the navigation tree pane, and expand nodes until you see the Logs node.
3. Select the Logs node and the Log Files panel is displayed on the Configuration tab.



4. Use the Log Files pane to configure your log files, as follows:
 - **Write logs to file.** Enable this option to write logs to a file on the Core host. After selecting this option you can:
 - Enable the default log directory and file (for example, `/var/opt/SUNWswlogs/central`), or
 - Enable the Write log files to directory option, and then specify a path and file name for the log file.

Note: The Console does not verify whether a specified log file location actually exists. The central logger will try to create the log directory if it does not exist. Consequently, there is no indication that you specified and saved a nonexistent log location until you try to view the logs. After several attempts to view the logs, a message displays to report the Console's inability to find logs at the specified location.

- **On Solaris Only** — *Write logs to syslog daemon:* Enable this option if Identity Synchronization for Windows resides on a Solaris platform. Use the drop-down list to select a category for writing the log. (*Default is DAEMON*)

Note: When you select this option, Identity Synchronization for Windows logs everything to the syslog; however, the syslog is configured by default to log WARNING and SEVERE messages only.

To configure syslog to log INFO messages, edit `/etc/syslog.conf` and change the following line:

```
*.err;kern.debug;daemon.notice;mail.crit /var/adm/messages
```

to

```
*.err;kern.debug;daemon.notice;daemon.info;mail.crit
/var/adm/messages
```

After making this change, you must restart the syslog daemon as follows:

```
/etc/init.d/syslog stop ; /etc/init.d/syslog start
```

To enable FINE, FINER, and FINEST logging, include `daemon.debug` in the semicolon separated list.

- **Remove Old Logs:** The number of log files will continue to grow (one per day) indefinitely. To avoid running out of disk space, enable this option and specify when the program can delete old logs from the central log file.
 For example, if you specify 30 days, Identity Synchronization for Windows will delete all files when they become 31 days old.
 - **Log Level.** Use the drop-down list to select the level of detail you want to see in your system logs. (Review [Reading the Logs](#))
5. Click the Save Log Configuration button to create log files based on the selected options.

9.3 Viewing Directory Source Status

9.3.1 To View the Status of your Directory Sources

1. From the Identity Synchronization for Windows Console, select the Status tab.
2. In the navigation tree pane, expand the Directory Source node, and then select the directory source node (such as `dc=example,dc=com`).

The Status tab content changes to provide information related to the selected directory source.



Note: When viewing the Directory Source status you are essentially viewing the status of the connector associated with that Directory Source.

Click Update to refresh the information on this tab. The following information is provided on the Status tab:

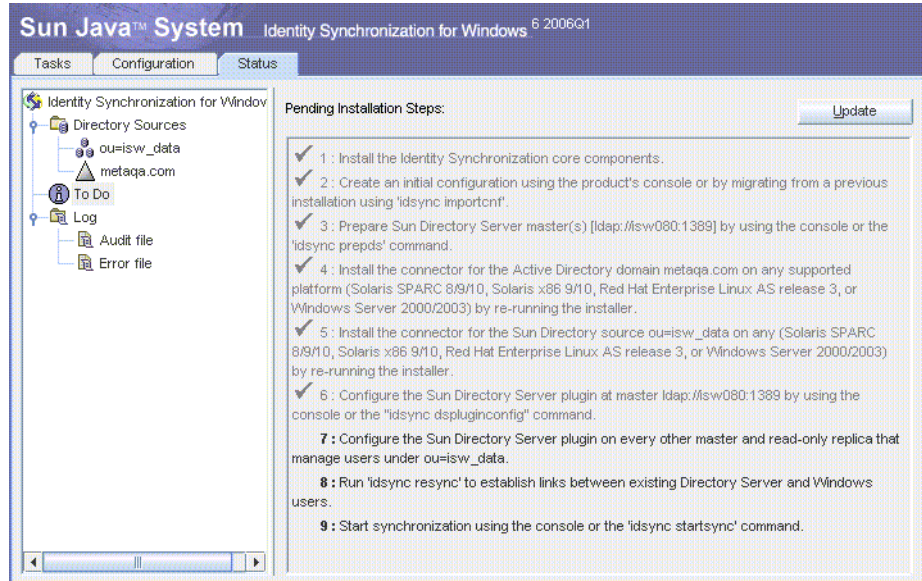
- **State:** Reflects the current state of the directory source. Valid states include:
 - Uninstalled:** The connector has not been installed.
 - Installed:** The connector is installed, but is not ready for synchronization because it has not received its runtime configuration yet. If the connector remains in this state for more than a minute, something is probably wrong.
 - Ready:** The connector is ready for synchronization, but it is currently not synchronizing any objects. A connector remains in the Ready state if synchronization has not been started or if synchronization has been started but not all subcomponents have established connections with the connectors.
 - Syncing:** The connector is synchronizing objects. There might still be errors, so consult the error log if you notice that changes are not synchronized.
- **Active:** Indicates whether the directory source is active or down.
- **Last Communication:** Indicates the time of the last response from this directory source's connector.

9.4 Viewing Installation and Configuration Status

9.4.1 To View the Remaining Steps of the Installation and Configuration Process

1. From the Identity Synchronization for Windows Console, select the Status tab.
2. In the navigation tree pane, expand the To Do node.

The Status tab content changes to provide a checklist of the installation and configuration steps (for example, see [Viewing Directory Source Status](#)).



3. Click the Update button (upper right) to refresh the list.

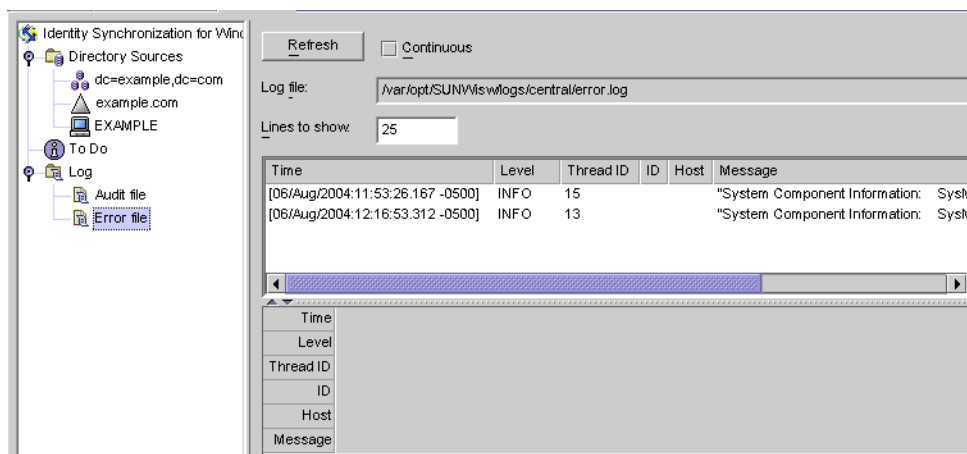
Completed steps will be check-marked and greyed-out. You must complete the remaining steps to successfully complete the installation and configuration process.

9.5 Viewing Audit and Error Logs

9.5.1 To View Your Error Logs

1. From the Identity Synchronization for Windows Console, select the Status tab.
2. In the navigation tree pane, expand the Audit File or the Error File node.

The Status tab content changes to display the current logs.



Click Refresh to load the latest audit or error information.

The following information is provided on the Status tab:

- **Continuous:** Updates and displays the latest audit or error information constantly.
- **Log File:** Displays the full path name of the audit or error log being read; for example:
`C:\Program Files\Sun\MPS\isw-hostname\logs\central\audit.log`
- **Lines to show:** Specifies how many audit or error entries to display. (*Default is 25.*)

9.6 Enabling Auditing on a Windows NT Machine

If you have a Windows NT machine in your deployment, verify that auditing is enabled or Identity Synchronization for Windows cannot log messages from that machine.

9.6.1 To Enable Audit Logging on Your Windows NT Machine

1. From the Windows NT Start menu, select Programs> Administrative Tools> User Manager for Domains.
2. When the User Manager dialog box is displayed, select Policies> Audit from the menu bar.
The Audit Policy dialog box is displayed.
3. Enable the Audit These Events button and then enable the Success and Failure boxes.
4. Click OK to close the dialog box.
These settings will remain in effect until you change them again.

Part II

Appendixes

Using the Identity Synchronization for Windows Command Line Utilities

Identity Synchronization for Windows enables you to perform a variety of tasks from the command line. This appendix explains how to execute the Identity Synchronization for Windows command line utilities to perform different tasks. The information is organized into the following sections:

- [Common Features](#)
- [Using the `idsync` command](#)
- [Using the `forcepwchg` Migration Utility](#)

A.1 Common Features

The Identity Synchronization for Windows command line utilities share the following features:

- [Common Arguments to the `Idsync` Subcommands](#)
- [Entering Passwords](#)
- [Getting Help](#)

A.1.1 Common Arguments to the `Idsync` Subcommands

This section describes the arguments (options) that are common to most of the command line utilities. The information is organized into the following tables:

- **Common Arguments to the `Idsync` Subcommands:** Describes the following arguments, which are common to all of the `idsync` subcommands (*except `prepds`*) and migration tools.

```
-D bind-DN -w bind-password | - [-h Configuration Directory-hostname]  
[-p Configuration Directory-port-no] [-s rootsuffix] [-Z] [-P cert-db-path]  
[-m secmod-db-path]
```

Note: Brackets [] indicate optional arguments.

The Identity Synchronization for Windows installation program automatically writes default values to the `-h`, `-p`, `-D`, and `-s` arguments based on the information you provide during installation. However, you can specify a different value on the command line to override a defaulted value.

To support multibyte characters, Identity Synchronization for Windows base64-encodes the default values for `-s rootsuffix` and `-D bind-DN` in the command line interface (CLI) environment file. The `rootsuffix` default should not be changed. The `bind DN` default can be overridden on the command line or updated with the appropriate base64-encoded value in the CLI environment file.

- **Common Arguments for Accessing the Configuration Directory Server using SSL:** Describes optional arguments that provide information about securely accessing the Configuration Directory Server using Secure Socket Layer (SSL). These arguments are also common to all of the `idsync` subcommands and the migration tools.
- **Common Arguments Related to Configuration Directory:** Describes arguments related to the configuration directory. These arguments are common to two or more `idsync` subcommands and migration tools.

Table A-1 Arguments Common to All Subcommands

Argument	Description
<code>-h</code> <i>Configuration Directory-hostname</i>	Specifies the configuration directory hostname. This argument defaults to the values specified during Core installation.
<code>-p</code> <i>Configuration Directory-port</i>	Specifies the configuration directory LDAP port number.
<code>-D</code> <i>bind-DN</i>	Specifies the configuration directory bind distinguished name (DN). This argument defaults to the values specified during Core installation.
<code>-w</code> <i>bind-password</i> <code>-</code>	Specifies the configuration directory bind password. The <code>-</code> value reads the password from standard input (STDIN).
<code>-s</code> <i>rootsuffix</i>	Specifies the configuration directory rootsuffix. Where <code>rootsuffix</code> is a distinguished name such as <code>dc=example,dc=com</code> . This argument defaults to the values specified during Core installation.
<code>-q</code> <i>configuration_password</i> <code>-</code>	Specifies the configuration password. The <code>-</code> value means the password will be read from standard input (STDIN). This argument is <i>mandatory</i> for all subcommands except <code>preps</code> .

Table A-2 SSL-Related Arguments Common to All Subcommands

Argument	Description
<code>-Z</code>	Specifies that SSL be used to provide secure communication. Provides certificate-based client authentication when connecting to the configuration directory accessing the command line interface or the preferred/secondary Directory Servers.

Table A-2 (Cont.) SSL-Related Arguments Common to All Subcommands

Argument	Description
-P <i>cert-db-path</i>	Specifies the path and file name of the client's certificate database. This certificate database must contain the CA certificate used to sign the Directory Server's certificate database. If you specify -Z but do not use -P, the <i>cert-db-path</i> defaults to <i>current-working-directory/cert8.db</i> . Note: If Identity Synchronization for Windows does not find the certificate database file in the specified directory, the program creates an *empty* database in that directory, which consists of three files: <i>cert8.db</i> , <i>key3.db</i> , and <i>secmod.db</i> .
-m <i>secmod-db-path</i>	Specifies the path to the security module database. For example: <i>/var/Sun/MPS/slaped-serverID/secmod.db</i> Specify this argument only if the security module database is in a different directory than the certificate database itself.

Table A-3 Configuration Directory Arguments

Argument	Description
-a <i>ldap_filter</i> Use with <i>forcepwchg</i> and <i>resync</i> subcommands	Specifies the LDAP filter to use when retrieving users from the source SULs, and allows the operation to retrieve a focused subset of users from the directory source, prior to determining whether the users fall within the specified SULs.
-f <i>filename</i> Use with <i>export10cnf</i> , <i>importcnf</i> , and <i>resync</i> subcommands	Specifies the name of a Configuration XML Document file.
-n Use with <i>forcepwchg</i> , <i>importcnf</i> , and <i>resetconn</i> subcommands	Runs in safe mode so you can preview the effects of an operation with no actual changes.

A.1.2 Entering Passwords

Wherever a password argument is required (such as -w *bind-password* or -q *configuration_password*), you can use the "-" argument to tell the password program to read the password from STDIN.

If you use the "-" value for multiple password options, *idsync* will prompt you for passwords based on the arguments' order.

In this case, the program would expect the *bind-password* first, and then for the *configuration-password*.

A.1.3 Getting Help

You can use one of the following commands to display usage information about *idsync* or any of its subcommands in the command Console:

- **-help**
- **--help**
- **-?**

For usage information

- About `idsync` (including a list of valid subcommands), type one of the preceding help options at a command prompt and click Return.
- About a subcommand, type the subcommand followed by a help option at a command prompt and click Return.

A.2 Using the `idsync` command

You use the `idsync` command and subcommands to execute the Identity Synchronization for Windows command line utility.

Note: The `idsync` command converts all DN-valued arguments (such as bind DN or suffix name) from the character set specified for that window to UTF-8 before sending the arguments to Directory Server.

Do not use backslashes as escape characters in suffix names.

To specify UTF-8 characters on Solaris and on Linux, your terminal window must have a locale based on UTF-8. Make sure that the environmental variable's `LC_CTYPE` and `LANG` are set correctly.

Unless specifically noted otherwise, you can run the `idsync` command with subcommands using either of the following methods:

- **From Solaris:**
 1. Open a terminal window and **cd** to the `/opt/SUNWiwsw/bin` directory.
 2. Type the `idsync` command with one subcommand, as follows


```
idsync subcommand
```
- **From Linux:**
 1. Open a terminal window and **cd** to the `/opt/sun/isw/bin` directory.
 2. Type the `idsync` command with one subcommand, as follows


```
idsync subcommand
```
- **From Windows:**
 1. Open a Command Window and **cd** to the `install_path\isw-hostname\bin` directory.
 2. Type the `idsync` command with one subcommand, as follows


```
idsync subcommand
```

[Using the `idsync` command](#) lists all of the `idsync` utility subcommands and their purpose:

Table A-4 Quick Reference to `idsync` Subcommands

Subcommand	Purpose
<code>certinfo</code>	Displays certificate information based on your configuration and SSL settings (see Using <code>certinfo</code>)

Table A-4 (Cont.) Quick Reference to `idsync` Subcommands

Subcommand	Purpose
<code>changepw</code>	Changes the Identity Synchronization for Windows configuration password (see Using <code>changepw</code>)
<code>importcnf</code>	Imports an exported Identity Synchronization for Windows version 1.0 configuration XML document (see Using <code>importcnf</code>)
<code>prepds</code>	Prepares a Sun Java System Directory Server source for use by Identity Synchronization for Windows (see Using <code>prepds</code>)
<code>printstat</code>	Displays a list of steps you must perform to complete the installation/configuration process. Also provides the status of installed connectors, the system manager, and the Message Queue (see Using <code>printstat</code>)
<code>resetconn</code>	Resets connector states in the configuration directory to <i>uninstalled</i> (see Using <code>resetconn</code>)
<code>resync</code>	Links and resynchronizes existing users or groups and pre-populates directories as part of the installation process (see Using <code>resync</code>)
<code>groupsync</code>	Synchronizes group information between users and groups from one directory source to another (see Using <code>groupsync</code>)
<code>accountlockout</code>	Synchronizes account lockout and unlockout between Directory Server and Active Directory sources (see Using <code>accountlockout</code>)
<code>dspluginconfig</code>	Configures and unconfigures Directory Server plugin on a specified host (see Using <code>dspluginconfig</code>)
<code>startsync</code>	Starts synchronization (see Using <code>startsync</code>)
<code>stopsync</code>	Stops synchronization (see Using <code>stopsync</code>)

A.2.1 Using `certinfo`

You can use the `certinfo` subcommand to display certificate information based on your configuration and SSL settings. This information can help you determine which certificates must be added for each connector and/or Directory Server Plug-in certificate database.

To display certificate information, open a terminal window (or Command Window) and type the **`idsync certinfo`** command as follows:

```
idsync certinfo [bind-DN] -w bind-password | -
[-h Configuration Directory-hostname] [-p Configuration Directory-port-no]
[-s rootsuffix] -q configuration_password [-Z]
[-P cert-db-path] [-m secmod-db-path]
```

Note: Because the `certinfo` subcommand does not have access to the connectors' and Directory Server's certificate databases, some of the required steps it lists might have already been performed.

For example:

```
idsync certinfo -w admin-password -q configuration-password
```

Note: For detailed information about the `certinfo` arguments, review [Common Arguments to the Idsync Subcommands](#).

A.2.2 Using `changepw`

You can use the `changepw` subcommand to change the Identity Synchronization for Windows configuration password.

A.2.2.1 To Change the Configuration Password for Identity Synchronization for Windows:

1. Stop all Identity Synchronization for Windows processes (for example, System Manager, Central Logger, Connectors, Console, Installers/Uninstallers).
2. After stopping all the processes, back up the `ou=Services` tree by exporting the configuration directory to `ldif`.
3. Type the `idsync changepw` command as follows:

```
idsync changepw [-D bind-DN] -w bind-password | -
[-h Configuration Directory-hostname] [-p Configuration Directory-port-no]
[-s rootsuffix] -q configuration_password
[-Z] [-P cert-db-path] [-m secmod-db-path]
-b new_password | - [-y]
```

For example:

```
idsync changepw -w admin password -q old config password -b -q new config
password
```

The following arguments are unique to `changepw`:

Argument	Description
<code>-b password</code>	Specifies a new configuration password. The <code>-</code> value reads the password from standard input (STDIN).
<code>[-y]</code>	Does not prompt for command confirmation.

4. Respond to the messages that display in the terminal window. For example,

```
Are you sure that want to change the configuration password (y/n)? yes
Before restarting the system -
you must edit the $PSWHOME/resources/SystemManagerBootParams.cfg file
and change the 'deploymentPassword' to the new value.
```

```
SUCCESS
```

5. You must modify the `SystemManagerBootParams.cfg` file before restarting the system.

The `SystemManagerBootParams.cfg` file in `$PSWHOME/resources` (where `$PSWHOME` is the *isw-installation directory*) contains the configuration password the system manager uses to connect to the configuration directory.

For example, you would change the password value as follows:

From: `Parameter name="manager.configReg.deploymentPassword" value="oldpassword" /`

To: `Parameter name="manager.configReg.deploymentPassword" value="newpassword" /`

6. If the program reports any errors, restore the configuration directory using the `ldif` from [Using `changepw`](#) and then try again. The most likely reason for an

error is that the Directory Server hosting the configuration directory became unavailable during the password change.

A.2.3 Using `importcnf`

After installing Core ([Chapter 3, "Installing Core"](#)), use the `idsync importcnf` subcommand to import your exported Identity Synchronization for Windows version 1.0 or 1.1 (SP1) configuration XML file, which contains Core configuration information.

To import your version 1.0 configuration XML file, open a terminal window (or Command Window) and type the **`idsync importcnf`** command as follows:

```
idsync importcnf [-D bind-DN] -w bind-password | -
[-h Configuration Directory-hostname] [-p Configuration Directory-port-no]
[-s rootsuffix] -q configuration_password [-Z] [-P cert-db-path]
[-m secmod-db-path] -f filename [-n]
```

For example:

```
idsync importcnf -w admin_password -q configuration_password -f "MyConfig.cfg"
```

The following arguments are unique to `importcnf`:

Table A-5 *idsync importcnf Arguments*

Argument	Description
<code>-f filename</code>	Specifies the name of your configuration XML document.
<code>-n</code>	Runs in safe mode so you can preview the effects of an operation with no actual changes.

Note: For detailed information about other `importcnf` arguments, review [Common Arguments to the Idsync Subcommands](#).

After importing the version 1.0 configuration XML file, you must run `prepds` on all Directory Server sources configured for synchronization, (see [Using prepds](#) connectors and subcomponents).

A.2.4 Using `prepds`

You use the console or `prepds` subcommand to prepare a Sun Java System Directory Server source for use by Identity Synchronization for Windows. You must run `prepds` before installing the Directory Server Connector.

Running the `idsync prepds` subcommand applies the appropriate ACI to the `cn=changelog` entry, which is the root node of the Retro-Changelog database.

If you are preparing a *preferred master* Directory Server for use by Identity Synchronization for Windows, you must provide *Directory Manager* credentials.

The Directory Manager user is a special user on Directory Server who has full rights anywhere inside the Directory Server instance. (ACI does not apply to Directory Manager users.)

For example, only the Directory Manager can set the access control for the Retro-Changelog database, which is one of the reasons why Identity Synchronization for Windows requires Directory Manager credentials for the preferred master server.

Note: If you recreate the Retro-Changelog database for the preferred Sun directory source for any reason, the default access control settings will not allow the Directory Server Connector to read the database contents.

To restore the access control settings for the Retro-Changelog database, run `idsync prepds` or click the Prepare Directory Server button after selecting the appropriate Sun directory source in the Console.

You can configure your system to automatically remove (or *trim*) Changelog entries after a specified period of time. From the command line, modify the `nsslapd-changelogmaxage` configuration attribute in `cn=Retro Changelog Plug-in`, `cn=plugins`, `cn=config`:

```
nsslapd-changelogmaxage: IntegerTimeunit
```

Where:

- **Integer** is a number.
- **Timeunit** is *s* for seconds, *m* for minutes, *h* for hours, *d* for days, or *w* for weeks. (There should be no space between the Integer and Timeunit variables.)

For example, `nsslapd-changelogmaxage: 2d`

For more information, see the "Managing Replication" chapter in the Sun Java System Directory Server 5 2004Q2 Administration Guide.

- You can use *Administrative* credentials to prepare a *secondary* server.

Be sure to plan your Identity Synchronization for Windows configuration *before* running `idsync prepds` because you must know which hosts and suffixes you will be using.

Running `idsync prepds` on a Directory Server suffix where the Directory Server Connector and Plug-in are already installed, configured, and synchronizing will result in a message asking you to install the Directory Server Connector. Disregard this message.

To prepare a Sun Java System Directory Server source, open a terminal window (or a Command Window) and type the **`idsync prepds`** command as follows:

For single host:

```
idsync prepds [-h <hostname>] [-p <port>] [-D <Directory Manager DN>] -w  
<password>  
-s <database suffix> [-x] [-Z] [-P <cert db path>] [-m <secmod db path>]
```

For multiple hosts:

```
idsync prepds -F <filename of Host info> -s <root suffix> [-x] [-Z]  
[-P <cert db path>] [-m <secmod db path>] [-3]
```


For example:

```
isw-hostname\bin>idsync prepds -F isw-hostname\samples\Hosts.xml \
-s ou=isw_data
```

Note: The `-h`, `-p`, `-D`, `-w`, and `-s` arguments are redefined (as described in the following table) for the `prepds` subcommand only. In addition, the `-q` argument does not apply.

Using `prepds` describes the arguments that are unique to `idsync prepds`.

Table A-6 *prepds Arguments*

Argument	Description
<code>-h name</code>	Specifies the DNS name of the Directory Server instance serving as the preferred host.
<code>-p port</code>	Specifies port number for Directory Server instance serving as preferred host. (Default is 389.)
<code>-j name (optional)</code>	Specifies the DNS name of the Directory Server instance serving as the secondary host (applicable in a Sun Java System Directory Server 5 2004Q2 multimaster replicated (MMR) environment).
<code>-r port (optional)</code>	Specifies a port for the Directory Server serving as the secondary host (applicable in a Sun Java System Directory Server 5 2004Q2 multimaster replicated (MMR) environment). (Default is 389)
<code>-D dn</code>	Specifies the distinguished name of the Directory Manager user for the preferred host.
<code>-w password</code>	Specifies a password for the Directory Manager user for the preferred host. The - value reads the password from standard input (STDIN).
<code>-E admin-DN</code>	Specifies the distinguished name of the Directory Manager user for the secondary host.
<code>-u password</code>	Specifies a password for the Directory Manager user for the secondary host. The - value reads the password from standard input (STDIN).
<code>-s rootsuffix</code>	Specifies the root suffix to use for adding an index (root suffix where you will be synchronizing users). Note: The database name of the Preferred and Secondary hosts may vary, but the suffix will not. Consequently, the program can find the database name of each host and use it to add the indexes.
<code>-x</code>	Does not add equality and presence indexes for <code>dspswuserlink</code> attribute to the database.
<code>-F filename of Host info</code>	Specifies the filename containing the host information in case of multiple hosts environment.

If you are running `idsync prepds` in a replicated environment, (for example, where you have a preferred master, a secondary master, and two consumers), you only need to run `idsync prepds` once for the preferred and secondary masters.

A.2.4.1 To run `idsync prepds`

1. Ensure that Directory Server replication is up and running (if applicable.)
2. Run `idsync prepds` from the Console or from the command line, for example:

```
idsync prepds -h M1.example.com -p 389 -j M2.example.com -r 389.
```

Running the `idsync prepds` command on M1 accomplishes the following:

- Enables and extends the RCL to capture more attributes (`dspswuserlink` and so forth)

RCL is required on M1 only.

- Extends schema.
- Adds `uid=pswconnector, suffix` user with ACIs.
- Adds indexes to the `dspswuserlink` attribute, which puts Directory Server in read-only mode temporarily until the indexing is done.

You can add indexes later to avoid downtime, but you must add indexes *before* installing the Directory Server Connector.

Adds indexes on M2.

Note: ■ Replication ensures that Identity Synchronization for Windows copies schema information and the `uid=pswconnector` from the preferred master to the secondary master and both consumers.

- You must install the Directory Server Connector once. You must install the Directory Server Plug-in in *all* directories.
 - Indexing is required on the preferred and the secondary masters only. (Replication does not push the indexing configuration from the preferred master to the secondary master.)
-
-

A.2.5 Using `printstat`

You can use the `printstat` subcommand to:

- Display a list of the remaining steps you have to perform to complete the installation and configuration process.
- Print the status of installed connectors, the system manager, and the Message Queue.

Possible status settings include:

- **Uninstalled.** The connector is not installed.
- **Installed.** The connector is installed, but not ready for synchronization because it has not received its runtime configuration yet.
- **Ready.** The connector is ready for synchronization, but is not synchronizing any objects yet.
- **Syncing.** The connector is synchronizing objects.

To print the status of installed Connectors, the System Manager, and the Message Queue open a terminal window (or a Command Window) and enter the **`idsync printstat`** command as follows:

```
idsync printstat [-D bind-DN] -w bind-password | -
[-h Configuration Directory-hostname] [-p Configuration Directory-port-no]
[-s rootsuffix] -q configuration_password [-Z]
[-P cert-db-path] [-m secmod-db-path]
```

For example:

```
idsync printstat -w admin password -q configuration password
```

A.2.6 Using `resetconn`

You can use the `resetconn` subcommand to reset connector states in the configuration directory to *uninstalled*. For example, if a hardware failure prevents you from uninstalling a connector, use `resetconn` to change the connector's status to *uninstalled* so you can reinstall that connector.

Note: The `resetconn` subcommand is intended to be used only in the event of hardware or uninstaller failures.

To reset the state of connectors from the command line, open a terminal window (or a Command Window) and type the **idsync resetconn** command as follows:

```
idsync resetconn [-D bind-DN] -w bind-password\> | -
[-h Configuration Directory-hostname] [-p Configuration Directory-port-no]
[-s rootsuffix] -q configuration_password [-Z] [-P cert-db-path]
[-m secmod-db-path] -e directory-source-name [-n]
```

For example:

```
idsync resetconn -w admin password -q configuration_password -e
"dc=example,dc=com"
```

[Using `preps`](#) describes the arguments that are unique to `resetconn`:

Table A-7 *idsync resetconn Arguments*

Argument	Description
<code>-e dir-source</code>	Specifies the name of the directory source to reset.
<code>-n</code>	Runs in safe mode so you can preview the effects of an operation with no actual changes.

Note: `idsync printstat` can be used to find directory source names.

For detailed information about the other `resetconn` arguments, review [Common Arguments to the Idsync Subcommands](#).

A.2.7 Using `resync`

You can use the `resync` subcommand to bootstrap deployments with existing users. This command uses administrator-specified matching rules to

- Link existing entries
- Populate an empty directory with the contents of a remote directory
- Bulk-synchronize attribute values between two existing user populations
- Bulk-synchronize existing groups and the users associated with the groups (when the group synchronization feature is enabled).

Note: For more detailed information about linking and synchronizing users, see [Chapter 1, "Understanding the Product"](#).

To resynchronize existing users and to pre-populate directories, open a terminal window (or a Command Window) and type the `idsync resync` command as follows:

```
idsync resync [-D bind-DN] -w bind-password | -
[-h Configuration Directory-hostname] [-p Configuration Directory-port-no]
[-s rootsuffix] -q configuration_password [-Z] [-P cert-db-path]
[-m secmod-db-path] [-n] [-f xml filename for linking] [-k] [-a ldap-filter]
[-l sul-to-sync] [-o Sun | Windows] [-c] [-x]
[-u] [-i ALL_USERS | NEW_USERS | NEW_LINKED_USERS]
```

For example:

```
idsync resync -w admin password -q configuration_password
```

Using `resync` describes the arguments that are unique to `resync`:

Table A–8 *idsync resync Usage*

Argument	Meaning
<code>-f filename</code>	Creates links between unlinked user entries using one of the specified XML configuration files provided by Identity Synchronization for Windows (see Appendix B, "Identity Synchronization for Windows LinkUsers XML Document Sample")
<code>-k</code>	Creates links between unlinked users only (does not create users or modify existing users)
<code>-a ldap-filter</code>	Specifies an LDAP filter to limit the entries to be synchronized. The filter will be applied to the source of the resynchronization operation. For example, if you specify <code>idsync resync -o Sun -a "uid=*"</code> all Directory Server users that have a <code>uid</code> attribute will be synchronized to Active Directory.
<code>-l sul-to-sync</code>	Specifies individual Synchronization User Lists (SULs) to resynchronize Note: You can specify multiple SUL IDs to resynchronize multiple SULs or, if you do not specify any SUL IDs, the program will resynchronize all of your SULs.
<code>-o (Sun Windows)</code>	Specifies the source of the resynchronization operation <ul style="list-style-type: none"> ▪ Sun: Sets attribute values for Windows entries to corresponding attribute values in Sun Java System Directory Server directory source entries. ▪ Windows: Sets attribute values for Sun Java System Directory Server entries to corresponding attribute values in Windows directory source entries. (Default is Windows)
<code>-c</code>	Creates a user entry automatically if the corresponding user is not found at destination <ul style="list-style-type: none"> ▪ Randomly generates a password for users created in Active Directory or Windows NT ▪ Automatically creates a special password value (<code>(PSWSYNC)*INVALID PASSWORD*</code>) for users created in Directory Server (unless you specify the <code>-i</code> option)

Table A-8 (Cont.) `idsync resync` Usage

Argument	Meaning
<code>-i</code> (<code>ALL_USERS</code> <code>NEW_USERS</code> <code>NEW_LINKED_USERS</code>)	Resets passwords for user entries synchronized in the Sun directory sources, forcing password synchronization within the current domain for those users the next time the user password is required. <ul style="list-style-type: none"> ■ ALL_USERS: Forces on-demand password synchronization for all synchronized users ■ NEW_USERS: Forces on-demand password synchronization for newly created users only ■ NEW_LINKED_USERS: Forces on-demand password synchronization for all newly created and newly linked users
<code>-u</code>	Only updates the object cache. No entries are modified. This argument updates the local cache of user entries for a Windows directory source only, which prevents pre-existing Windows users from being created in Directory Server. If you use this argument, Windows user entries are not synchronized with Directory Server user entries. This argument is valid only when the resync source is Windows.
<code>-x</code>	Deletes all destination user entries that do not match a source entry.
<code>-n</code>	Runs in safe mode so you can preview the effects of an operation with no actual changes.

Note: ■ Run `idsync resync` with no arguments to view a usage statement.

- For detailed information about the `resync` arguments, review [Common Arguments to the Idsync Subcommands](#).
- For more information about resynchronizing existing users, review [Chapter 1, "Understanding the Product"](#).

After running `resync`, check the `resync.log` file in the central `audit log`. If errors result, consult *Troubleshooting Guide for Oracle Directory Server Enterprise Edition*.

A.2.8 Using `groupsync`

You can use the `groupsync` subcommand to synchronize groups between Active Directory and Directory Server.

To enable or disable the Group Synchronization, type `idsync groupsync` command.

For example:

```
idsync groupsync -{e/d} -D <bind DN> -w <bind password> [-h <CD hostname>]
[-p <CD port no>] -s <rootsuffix> [-Z] -q <configuration password> -t <AD group
type>
```

Table A-9 `groupsync` arguments

Argument	Meaning
<code>-{e/d}</code>	Select <code>e</code> for enabling, and <code>d</code> for disabling the group synchronization.

Table A-9 (Cont.) groupsync arguments

Argument	Meaning
-t	Specifies the group type at Active Directory. For example, it can be selected as either of "distribution" or "security"

A.2.9 Using accountlockout

You can use the `accountlockout` subcommand to synchronize account lockout and unlockout between Active Directory and Directory Server.

To enable or disable the account lockout, type **`idsync accountlockout`** command.

For example:

```
idsync accountlockout -(e/d) -D <Directory Manager DN> -w <bind-password>
-h <Configuration Directory-hostname> -p <Configuration Directory-port-no>
-s <rootsuffix> [-Z] [-P <cert db path>] [-m <secmod db path>]
-q <configuration password> -t <max lockout attempts>
```

Table A-10 accountlockout arguments

Argument	Meaning
<i>-(e/d)</i>	Select e for enabling , and d for disabling the account lockout synchronization.
-t	Specifies the maximum number of lockout attempts that Active Directory Connector performs.

A.2.10 Using dspluginconfig

You can use the `dspluginconfig` subcommand to configure or unconfigure Directory Server plugin on a specified Directory Server data source.

To configure or unconfigure the Directory Server plugin, type **`idsync dspluginconfig`** command.

For example:

```
idsync dspluginconfig -(C/U) -D <bind DN> -w <bind password | ->
[-h <CD hostname>] [-p <CD port no>] [-s <configuration suffix>]
[-Z] [-P <cert db path>] [-m <secmod db path>] [-d <ds plugin hostname>]
[-r <ds plugin port>] [-u <ds plugin user>] [-x <ds plugin user password>]
[-o <database suffix>] [-q <configuration password | ->]
```

Table A-11 dspluginconfig arguments

Argument	Meaning
<i>-(C/U)</i>	Select C for configuring and U for unconfiguring the Directory Server plugin.
-d	Host name of the Directory Server data source where the plugin needs to be configured
-r	Port number of the Directory Server data source where the plugin needs to be configured
-u	Administrator of the Directory Server data source where the plugin needs to be configured
-x	Password of the administrator of the Directory Server data source where the plugin needs to be configured

Table A-11 (Cont.) `dspluginconfig` arguments

Argument	Meaning
<code>-o</code>	Data suffix of the Directory Server data source.

A.2.11 Using `startsync`

You can use the `startsync` subcommand to start synchronization from the command line.

To start synchronization, open a terminal window (or a Command Window) and type the **`idsync startsync`** command as follows:

```
idsync startsync [-D bind-DN] -w bind-password | -
[-h Configuration Directory-hostname] [-p Configuration Directory-port-no]
[-s rootsuffix] -q configuration_password [-Z]
[-P cert-db-path] [-m secmod-db-path]
```

For example:

```
idsync startsync -w admin password -q configuration_password
```

[Using `startsync`](#) describes the arguments that are unique to `startsync`.

Table A-12 `idsync startsync` Arguments

Argument	Description
<code>[-y]</code>	Does not prompt for command confirmation.

Note: For detailed information about the other `startsync` arguments, review [Common Arguments to the Idsync Subcommands](#).

A.2.12 Using `stopsync`

You can use the `stopsync` subcommand to stop synchronization from the command line.

To stop synchronization, open a terminal window (or a Command Window) and type the **`idsync stopsync`** command as follows:

```
idsync stopsync [-D bind-DN] -w bind-password | -
[-h Configuration Directory-hostname] [-p Configuration Directory-port-no]
[-s rootsuffix] -q configuration_password [-Z]
[-P cert-db-path] [-m secmod-db-path]
```

For example:

```
idsync stopsync -w admin password -q configuration_password
```

Note: For detailed information about the `stopsync` arguments, review [Common Arguments to the Idsync Subcommands](#).

A.3 Using the forcepwchg Migration Utility

Users who change their passwords during migration will have different password in Windows NT and the Directory Server. You can use the `forcepwchg` utility to require a password change for users who changed their passwords during the Identity Synchronization for Windows version 1.0 to version 6.0 SP1 migration process.

Note: The `forcepwchg` utility ships with Windows packages only.

Before using `forcepwchg` you must verify the following:

- Be sure you do not configure the 7-bit check Plug-in in Directory Server to enforce 7-bit values for the `userpassword` attribute. Do this using the Directory Server console.
- Be sure that the client you are using for authentication translates the value from your locale to UTF-8 correctly. (For example, the `-i` option for the `ldapsearch` shipped with Directory Server).

A.3.1 To Execute the `forcepwchg` Command line Utility

1. Open a Command Prompt window and `cd` to the Windows migration directory on the host where you are performing the migration. (The Identity Synchronization for Windows 1.0 NT components such as connector, Change Detector DLL, and Password Filter DLL must be installed on the PDC host.)
2. From the migration directory, type

```
java -jar forcepwchg.jar [-n] [-a] [-t <
time_specification\>]
```

For example,

```
forcepwchg.jar -n -a forcepwchg.jar -t 33m
```

[Using the forcepwchg Migration Utility](#) describes the arguments that are unique to `forcepwchg`:

Option	Description
-n	Specifies <i>preview mode</i> . In the preview mode, the utility prints out the names of all normal users except: <ul style="list-style-type: none"> ■ Built-in accounts (Administrator and Guest) if you specify the <code>-a</code> argument. ■ Users who changed passwords during the time specified using the <code>-t</code> argument. <p>In preview mode, any user can execute <code>forcepwchg</code>. In non-preview mode, only the Administrator can execute <code>forcepwchg</code>.</p>
-a	Requires all users (except Administrator and Guest) to change their passwords. You cannot use this argument if you are using the <code>-t</code> argument.

Option	Description
<code>-t <i>time_specification</i></code>	<p>Forces all users who changed passwords in the past <i>time_specification</i> to change their passwords. Where <i>time_specification</i> can have the following form:</p> <ul style="list-style-type: none"><li data-bbox="675 323 1247 350">■ <i>number</i>: Number of seconds (for example, <code>-t 30</code>)<li data-bbox="675 365 1289 392">■ <i>number m</i>: Number of minutes (for example, <code>-t 25m</code>)<li data-bbox="675 407 1247 434">■ <i>number h</i>: Number of hours (for example, <code>-t 6h</code>) <p>For example, if you specify <code>forcepwchg -t 6h</code>, all users who changed passwords within the last six hours will be required to change their password again.</p>
<code>-?</code>	Prints out usage information.

Identity Synchronization for Windows LinkUsers XML Document Sample

This appendix provides two sample XML configuration documents that you can use with the `idsync resync` subcommand to link existing users in your deployment.

Both of the following files are available in the `samples1` subdirectory where you installed Core:

- [Sample 1: linkusers-simple.cfg](#) (an example of a common and simple configuration)
- [Sample 2: linkusers.cfg](#) (a more-complex configuration example that shows the full power of specifying linking criteria)

You can modify the samples to suit your environment. Both files contain comments that explain how to modify the samples to link your users — including how to link users in multiple SULs.

B.1 Sample 1: linkusers-simple.cfg

```
<!--
  Copyright 2004 Sun Microsystems, Inc. All rights reserved
  Use is subject to license terms.
--\>
<!--
  This xml file is used to link Windows and
  Sun Directory Server users from the commandline.
  It is passed to the 'idsync resync'
  script as the -f option. This is a simple file
  that links users in the SUL1 synchronization user list
  that have the same login name, that is the Directory Server
  uid attribute matches the Active Directory
  samaccountname attribute. For more complex
  matching rules, see the linkusers.cfg sample.
--\>

<UserLinkingOperationList\>
  <UserLinkingOperation parent.attr="UserLinkingOperation"
sulist="SUL1"\>
    <UserMatchingCriteria parent.attr="UserMatchingCriteria"\>
      <AttributeMap parent.attr="AttributeMap"\>
        <AttributeDescription parent.attr="SunAttribute"
name="uid"/\>
        <AttributeDescription parent.attr="WindowsAttribute"
name="samaccountname"/\>
      </AttributeMap\>
```

```

    </UserMatchingCriteria\>
  </UserLinkingOperation\>
</UserLinkingOperationList\>

```

B.2 Sample 2: linkusers.cfg

```

<?xml version ="1.0" encoding="UTF-8"?\>
<!--

    Copyright 2004 Sun Microsystems, Inc.
    All rights reserved
    Use is subject to license terms.
--\>
<!--
    This xml file is used to link Windows
    and Sun Directory Server users from
    the command line. It is passed to the
    \qidsync resync\q script as the -f option.
--\>
<!--
    The following parameters allowLinkingOutOfScope:
    if true, then Windows users can be
    linked to Sun Directory Server users
    that are outside of the users\q Synchronization
    User List. Default is false.
--\>
<UserLinkingOperationList allowLinkingOutOfScope="false"\>

<!--
    UserLinkingOperation encapsulates the configuration
    of a single SUL to link. It includes the SUL ID
    and a list of attributes to match.
    A separate UserLinkingOperation must
    be specified for each SUL being linked.
--\>
<UserLinkingOperation parent.attr="UserLinkingOperation" sulid="SUL1"\>

<!--
    UserMatchingCriteria encapsulates a
    list of attributes that must match for a user to be linked. --\>
<!--
    For two users to match using this UserMatchingCriteria,
    they must have the same givenName and the same sn. --\>
<UserMatchingCriteria parent.attr="UserMatchingCriteria"\>
  <AttributeMap parent.attr="AttributeMap"\>
    <AttributeDescription parent.attr="SunAttribute" name="sn"/\>
    <AttributeDescription parent.attr="WindowsAttribute" name="sn"/\>
  </AttributeMap\>    <AttributeMap parent.attr="AttributeMap"\>
    <AttributeDescription parent.attr="SunAttribute" name="givenName"/\>
    <AttributeDescription parent.attr="WindowsAttribute"
name="givenName"/\>    </AttributeMap\></UserMatchingCriteria\>

<!--
    Multiple UserMatchingCriteria can be specified for a single SUL.
    They are treated as a logical OR. In this example,
    the givenName\qs and sn\qs must match (see above)) OR
    (the employee(Number|ID) must match),

```

```

    for the user to be linked. Notice that attribute
    that is specified, employeeNumber,
    is the name of the DS attribute. --\>
<!--
    This UserMatchingCriteria is commented out because
    employeeNumber is not an indexed attribute in DS.
    All attributes used in a UserMatchingCriteria
    should be indexed.
    <UserMatchingCriteria parent.attr="UserMatchingCriteria"\>
      <AttributeMap parent.attr="AttributeMap"\>
        <AttributeDescription parent.attr=
          "SunAttribute" name="employeeNumber"/\>
        <AttributeDescription parent.attr=
          "WindowsAttribute" name="employeeID"/\>
      </AttributeMap\>
    </UserMatchingCriteria\>
  --\>
</UserLinkingOperation\>
<!--
    When multiple SULs are linked, a separate UserLinkingOperation
    is specified for each.
    As shown here, each UserLinkingOperation can use different
    UserMatchingCriteria: in this example, users in SUL2 are
    only linked if their sn and employeeNumber match.
    Note: this UserLinkingOperation is currently
    commented out because the example configuration
    only has a single SUL.
    <UserLinkingOperation parent.attr="UserLinkingOperation" sulid="SUL2"\>
      <UserMatchingCriteria parent.attr="UserMatchingCriteria"\>
        <AttributeMap parent.attr="AttributeMap"\>
          <AttributeDescription parent.attr="SunAttribute" name="sn"/\>
          <AttributeDescription parent.attr="WindowsAttribute" name="sn"/\>
        </AttributeMap\>
        <AttributeMap parent.attr="AttributeMap"\>
          <AttributeDescription parent.attr=
            "SunAttribute" name="employeeNumber"/\>
          <AttributeDescription parent.attr=
            "WindowsAttribute" name="employeeID"/\>
        </AttributeMap\>
      </UserMatchingCriteria\>
    </UserLinkingOperation\>
  --\>
</UserLinkingOperationList\>

```

Running Identity Synchronization for Windows Services as Non-Root on Solaris

You must have `root` privileges to install and to run Identity Synchronization for Windows services on Solaris and Red Hat systems.

However, after installing the product you can configure the software to run the program services as a `non-root` user.

C.1 Running Services as a Non-`root` User

Note: To run services as `non-root`, you must change the permissions for all directories under the Identity Synchronization for Windows instance directory. The *default* directory is `/var/opt/SUNWisw`.

C.1.1 To Run services as a Non-`root` User

Although you must be `root` to install and to run Identity Synchronization for Windows services, you can configure the software to run the program services as a `non-root` user.

1. Use the UNIX `useradd` command to create a user account for Identity Synchronization for Windows.

You also can use a `nobody` user to run services. The remaining examples in this procedure assume you created a user called `iswuser`.

2. To install a Sun Java System Directory Server Connector, you must choose a non-privileged port for the Connector during installation.

For example, ports larger than 1024 are acceptable. Port 1389 is recommended for LDAP when the server is running as a `non-root` user. Port 1636 is recommended for LDAP over SSL.

Note: You must execute all commands in the remaining steps as `root`.

3. After installing all components, execute the following command to stop Identity Synchronization for Windows:

```
/etc/init.d/isw stop
```

4. You must update the ownership of the instance directory. For example, if you installed the product in `/var/opt/SUNWisw`.

```
chown -R iswuser /var/opt/SUNWisw
```

```
chown -R iswuser /opt/SUNWisw
```

5. In a text editor, open the `/etc/init.d/isw` file and replace the following line:

```
"$EXEC_START_WATCHDOG" "$JAVA_PATH" "$INSTALL_DIR" "$CONFIG_DIR"
```

with the following:

```
su iswuser -c "$EXEC_START_WATCHDOG '$JAVA_PATH' '$INSTALL_DIR' '$CONFIG_DIR' "
```

6. Execute the following command to restart the service:

```
/etc/init.d/isw start
```

7. Execute the following command to verify that the components are running using the assigned user's userid:

```
ps -ef | grep iswuser
```

Defining and Configuring Synchronization User Lists for Identity Synchronization for Windows

This appendix provides supplemental information about Synchronization User List (SUL) definitions and explains how to configure multiple domains. The information is organized as follows:

- [Understanding Synchronization User List Definitions](#)
- [Configuring Multiple Windows Domains](#)

D.1 Understanding Synchronization User List Definitions

Every Synchronization User List (SUL) contains two definitions — one to identify which Directory Server users to synchronize and the other to identify which Windows users to synchronize.

Each definition identifies which users in a directory to synchronize, which users to exclude from synchronization, and where to create new users.

Note: The objectclasses you select using the Identity Synchronization for Windows Console also determine which users will be synchronized. The program synchronizes only those users that have the selected objectclass, which includes any users that have a subclass of the selected objectclass.

For example, if you select the `organizationalPerson` objectclass, then Identity Synchronization for Windows will synchronize users with the `inetOrgPerson` objectclass because it is a subclass of the `organizationalPerson` objectclass.

[Understanding Synchronization User List Definitions](#) describes the components of an SUL definition:

Table D-1 SUL Definition Components

Component	Definition	Applicable		
		Sun	AD	NT
Base DN	<p>Defines the parent LDAP node of all users to be synchronized.</p> <p>A Synchronization User List base DN includes all users in that DN — unless the users are excluded by the Synchronization User List's filter or the user's DN is matched in a more specific Synchronization User List. For example, <code>ou=sales,dc=example,dc=com</code>.</p>	Yes	Yes	No
Filter	<p>Defines an LDAP-like filter used to include or exclude users from a Synchronization User List. The filter can include the <code>&</code>, <code> </code>, <code>!</code>, <code>=</code>, and <code>*</code> operators. The <code>\>=</code> and <code><=</code> operators are not supported. All comparisons are done using case-insensitive string comparisons.</p> <p>For example, <code>(&(employeeType=manager)(st=CA))</code> will include managers in California only.</p>	Yes	Yes	Yes
Creation Expression	<p>Defines the parent DN and naming attribute of newly created users (applicable only when you enable creates).</p> <p>The creation expression must include the base DN of the Synchronization User List. For example, <code>cn=%cn%,ou=sales,dc=example,dc=com</code>. (Where the <code>%cn%</code> token is replaced with a value from the user entry being created.)</p>	Yes	Yes	No

Note: To synchronize users in a Sun Java System Directory Server with multiple Active Directory domains, you must define at least one SUL for each Active Directory domain.

When Group Synchronization is enabled, the following are important:

1. The creation expression supported at Active Directory is `cn=%cn%`.
2. The creation expression must contain valid attribute names belonging to the group objectclass since the creation expression is common to both user as well as group.

For example:

The attribute `sn` is not part of the `groupofuniqueNames` objectclass at the Directory Server. Hence the following creation expression would be invalid for a group object. (Though it would work fine for user.)

```
cn=%cn%.%sn%
```

3. The attribute used in the creation expression must be provided with a value for every user/group entry created. If the value is not provided then the user/group object will not synchronize and an appropriate message will be logged in the central log.

When you define multiple SULs, Identity Synchronization for Windows determines membership in an SUL by iteratively matching each SUL definition. The program examines the SUL definitions with more-specific base DNs first. For example, the program tests a match against `ou=sales,dc=example,dc=com` before testing `dc=example,dc=com`.

If two SUL definitions have the same base DN and different filters, then Identity Synchronization for Windows cannot determine automatically which filter should be tested first, so you must use the Resolve Domain Overlap feature to order the two SUL definitions. If a user matches the base DN of an SUL definition but does not match any filters for that base DN, then the program will exclude that user from synchronization — even if that user matches the filter for a less-specific base DN.

D.2 Configuring Multiple Windows Domains

To support synchronizing multiple Windows domains to the same Directory Server container (such as `ou=people,dc=example,dc=com`), Identity Synchronization for Windows uses "synthetic" Windows attributes that contain domain information.

- For Active Directory domains, Identity Synchronization for Windows sets the `activedirectorydomainname` attribute to the Active Directory domain name (such as `east.example.com`) before synchronizing the entry to the Directory Server.
- For Windows NT domains, Identity Synchronization for Windows sets the `user_nt_domain_name` attribute to the Windows NT domain name (such as `NTEXAMPLE`) before synchronizing the entry to the Directory Server.

While these attributes do not actually appear in the Windows user entries, they are available for synchronization in the Identity Synchronization for Windows Console and can be mapped to a Directory Server user attribute. Once Identity Synchronization for Windows maps the domain attributes, they will be set in the Directory Server entries during synchronization and can be used in Synchronization User List (SUL) filters.

The following example illustrates how Identity Synchronization for Windows uses these attributes. This example assumes that three Windows domains (two Active Directory domains and one Windows NT domain) will be synchronized with a single Directory Server instance.

D.2.1 To Configure Multiple Windows Domains

1. Users in the Active Directory `east.example.com` domain will be synchronized to the Directory Server in `ou=people,dc=example,dc=com`.
2. Users in the Active Directory `west.example.com` domain will be synchronized to the Directory Server in `ou=people,dc=example,dc=com`.
3. Users in the Windows NT `NTEXAMPLE` domain will be synchronized to the Directory Server in `ou=people,dc=example,dc=com`.

When you create or modify a Directory Server user, the program uses the SUL filters to determine in which Windows domain to synchronize the user (because each Directory Server SUL has the same base DN, `ou=people,dc=example,dc=com`). The `activedirectorydomainname` and `user_nt_domain_name` attributes make constructing these filters easy.

To construct a filter from the Attributes tab on the Console:

4. Map the Directory Server `destinationindicator` attribute to the Active Directory `activedirectorydomainname` attribute and to the Windows NT `user_nt_domain_name` attribute.
5. Configure one SUL for each Windows domain as follows:

EAST_SUL

Sun Java System Directory Server definition

```
Base DN:   ou=people,dc=example,dc=com
Filter:    destinationindicator=east.example.com
Creation Expression:  cn=%cn%,ou=people,dc=example,dc=com
```

Active Directory definition (east.example.com)

```
Base DN:   cn=users,dc=east,dc=example,dc=com
Filter:    <none>
Creation Expression:  cn=%cn%,cn=users,dc=east,dc=example,dc=com
```

WEST_SUL

Sun Java System Directory Server definition

```
Base DN:ou=people,dc=example,dc=com
Filter: destinationindicator=west.example.com
Creation Expression:  cn=%cn%,ou=people,dc=example,dc=com
```

Active Directory definition (west.example.com)

```
Base DN:   cn=users,dc=west,dc=example,dc=com
Filter:<none>
Creation Expression:  cn=%cn%,cn=users,dc=west,dc=example,dc=com
```

NT_SUL

Sun Java System Directory Server definition

```
Base DN:   ou=people,dc=example,dc=com
Filter:    destinationindicator=NTEXAMPLE
Creation Expression:  cn=%cn%,
ou=people,dc=example,dc=com
```

Windows NT definition (NTEXAMPLE)

```
Base DN:   NA
Filter:    <none>
Creation Expression:  NA
```

Notice that each Directory Server SUL definition has the same base DN and creation expression, but the filters indicate the domain of the corresponding Windows user entry.

To further illustrate how these settings allow Directory Server user entries to synchronize with separate Windows domains, consider this test case:

6. Create `cn=Jane Test, cn=users, dc=east, dc=example, dc=com` in the Active Directory `east.example.com` domain.
7. Identity Synchronization for Windows creates the user entry `cn=Jane Test, ou=people, dc=example, dc=com` in the Directory Server with `destinationindicator=east.example.com`.
8. Modify the `cn=Jane Test, ou=people, dc=example, dc=com` entry in the Directory Server.
9. Because Jane Test's `destinationindicator` attribute is `east.example.com`, her entry will match the EAST_SUL Synchronization User List filter, and the

modification will be synchronized to the `east.example.com` Active Directory domain.

This example assumes that Identity Synchronization for Windows is synchronizing user creations from Windows to the Directory Server. If this is not the case, you can run the `idsync resync` command to set the `destinationindicator` attribute.

Note: When you use `idsync resync -f` in a deployment with multiple SULs, you probably will have to set the `allowLinkingOutOfScope` option to `true` in the linking configuration file. See [Appendix B, "Identity Synchronization for Windows LinkUsers XML Document Sample"](#)

The example uses an existing attribute in `inetorgperson`, `destinationIndicator`, which might be used for other purposes. If this attribute is already in use or a you select a different objectclass, you must map some attribute in the user's Directory Server entry to the `user_nt_domain_name` and/or the `activedirectorydomainname` attribute(s). The Directory Server attribute you choose to hold this value must be in the objectclass you are using for the rest of the attribute mapping configuration.

If there are no unused attributes to hold this domain information, you must create a new objectclass to include a new domain attribute and all other attributes you will be using with Identity Synchronization for Windows.

Identity Synchronization for Windows Installation Notes for Replicated Environments

Identity Synchronization for Windows 6.0 SP1 supports synchronizing users in a single replicated suffix.

Note: This appendix summarizes procedures used to configure and secure a multimaster replication (MMR) deployment. The information is taken directly from the *Administrator's Guide for Oracle Directory Server Enterprise Edition* — and is not Identity Synchronization for Windows - specific.

Designing and implementing an MMR deployment is *complex*. Refer to the *Deployment Planning Guide for Oracle Directory Server Enterprise Edition* to plan your deployment and the *Administrator's Guide for Oracle Directory Server Enterprise Edition* to implement the deployment.

This appendix is organized into the following sections:

- [Configuring Replication](#)
- [Configuring Replication Over SSL](#)

E.1 Configuring Replication

Note: In multimaster replication (MMR) environments, Identity Synchronization for Windows allows you to specify a preferred and secondary master servers for any given Sun directory source.

Directory Server supports n-way MMR (where you can change the replicated database at any of the 'n' masters configured). When you install the plug-in at the preferred master, you must select the *Other* host type and enter Directory Server instance's parameters manually during plug-in installation.

The following steps assume you are replicating a single suffix. If you are replicating more than one suffix, you may configure them in parallel on each server. In other words, you may repeat each step to configure replication on multiple suffixes.

E.1.1 To Configure any Replication Topology

1. Define a replication manager entry on all servers except single masters (or use the default replication manager on all servers.)
2. On all servers containing a dedicated consumer replica:
 - a. Create an empty suffix for the consumer replica.
 - b. Enable the consumer replica on the suffix through the replication wizard.
 - c. Optionally, configure the advanced replica settings.
3. On all servers containing a hub replica, if applicable:
 - a. Create an empty suffix for the hub replica.
 - b. Enable the hub replica on the suffix through the replication wizard.
 - c. Optionally, configure the advanced replica settings.
4. On all servers containing a master replica:
 - a. Choose or create a suffix on one of the masters that will be the master replica.
 - b. Enable the master replica on the suffix through the replication wizard.
 - c. Optionally, configure the advanced replica settings.
5. Configure the replication agreements on all supplier replicas, in the following order:
 - a. Between masters in a multimaster set.
 - b. Between masters and their dedicated consumers.
 - c. Between masters and hub replicas.

Optionally, you can configure fractional replication at this stage.

6. Configure replication agreements between the hub replicas and their consumers.
7. For multimaster replication, initialize all masters from the same master replica containing the original copy of the data. Initialize the hub and consumer replicas.

E.2 Configuring Replication Over SSL

Note: In this procedure, all references are chapters in the *Administrator's Guide for Oracle Directory Server Enterprise Edition*.

E.2.1 To Configure Directory Servers Involved in Replication so that all Replication Operations Occur Over an SSL Connection

1. Configure both the supplier and consumer servers to use SSL.
Refer to Chapter 11, "Managing Authentication and Encryption" for details.

Note:

- Replication over SSL will fail if the supplier server certificate is an SSL server-only certificate that cannot act as a client during an SSL handshake.
- Replication over SSL is currently unsupported with self-signed certificates.

2. If replication is not configured for the suffix on the consumer server, enable it as described in Chapter 8, "Enabling a Consumer Replica."
3. Follow the procedure in Chapter 8, "Advanced Consumer Configuration," to define the DN of the certificate entry on the consumer as another replication manager.
4. If replication is not configured for the suffix on the supplier server, enable it as described in Chapter 8, "Enabling a Hub Replica" or "Enabling a Master Replica."
5. On the supplier server, create a new replication agreement to send updates to the consumer on the secure SSL port. Follow the procedure in Chapter 8, "Creating Replication Agreements," for detailed instructions. Specify a secure port on the consumer server and select the SSL option of either using a password or a certificate. Enter a DN for the SSL option that you chose, either a replication manager or a certificate.

After you finish configuring the replication agreement, the supplier will send all replication update messages to the consumer over SSL and will use certificates if you chose that option. Customer initialization will also use a secure connection if performed through the console using an agreement configure for SSL.

E.3 Configuring Identity Synchronization for Windows in an MMR Environment

E.3.1 To Configure Identity Synchronization for Windows in an MMR Environment

1. From the Identity Synchronization for Windows Console, specify a preferred master and secondary master servers for the suffix to be synchronized. (Review [Creating a Sun Java System Directory Source](#))

You do not have to provide information about other Directory Servers in your topology.

2. Prepare the preferred master and secondary master servers from the Console or using the `idsync prepds` command line utility. (Review [Preparing Sun Directory Source](#))

If you use the command line utility, you should prepare both servers in a single invocation by specifying arguments for both the preferred and secondary servers.

3. Install the Directory Server Connector for the suffix replicated between these directories. (Review [Installing the Directory Server Connector](#))
4. Configure the Directory Server Plug-in on the preferred master, the secondary masters, and every other Directory Server instance that manages users in the replicated suffix (Review [Using dspluginconfig](#))

