

Sun Java™ System Identity Synchronization for Windows Release Notes

Version 1 2004Q3

Part Number 817-6202-05

These release notes contain important information available at the time of the release of Sun Java™ System Identity Synchronization for Windows 1 2004Q3. New features and enhancements, known limitations and problems, technical notes, and other information are addressed here. Read this document before you begin using Sun Java System Identity Synchronization for Windows 1 2004Q3 (Identity Synchronization for Windows).

These release notes contain the following sections:

- [Revision History](#)
- [About Identity Synchronization for Windows 1 2004Q3](#)
- [Bugs Fixed in This Release](#)
- [Important Information](#)
- [Known Issues and Limitations](#)
- [Redistributable Files](#)
- [How to Report Problems and Provide Feedback](#)
- [Additional Sun Resources](#)

Third-party URLs are referenced in this document and provide additional, related information.

NOTE	Sun is not responsible for the availability of third-party Web sites mentioned in this document. Sun does not endorse and is not responsible or liable for any content, advertising, products, or other materials that are available on or through such sites or resources. Sun will not be responsible or liable for any actual or alleged damage or loss caused by or in connection with the use of or reliance on any such content, goods, or services that are available on or through such sites or resources.
-------------	---

Revision History

Table 1 Revision History

Date	Description of Changes
30 September 2004	Initial release of the Release Notes.

About Identity Synchronization for Windows 1 2004Q3

Identity Synchronization for Windows provides bidirectional password synchronization between the following directories:

- Sun Java™ System Directory Server and Microsoft Windows 2000/2003 Active Directory
- Sun Java System Directory Server and Windows NT SAM Registry

When synchronizing Sun Java System Directory Server (Directory Server) and Windows 2000/2003 Active Directory, you can install and run all Identity Synchronization for Windows components on the Solaris™ Operating System and Windows 2000 Server operating system environments. When synchronizing Directory Server and Windows NT, you must run the Windows NT components in the Windows NT environment.

This section includes:

- [What's New in This Release](#)
- [Hardware and Software Requirements](#)

What's New in This Release

New Features

New features in Identity Synchronization for Windows 1 2004Q3 include:

- **User Deletes:** You can configure and enable the synchronization of user entry deletions from Sun Java System Directory Server to Active Directory, and from Active Directory to Sun Java System Directory Server.
- **Active Directory Failover:** Support for specifying additional Active Directory servers for failover during on-demand authentication. This feature is used by the Identity Synchronization for Windows Directory Server plug-in to authenticate users to Active Directory when their password has changed on Active Directory. In version 1.0 this was not possible, thus if the primary Active Directory server was unavailable then pass-through authentication to Active Directory from the Identity Synchronization for Windows Directory Server plug-in would fail and the user could not authenticate to the Directory Server. This condition would occur only if the user had changed their password on Active Directory and was authenticating to the Directory Server for the first time since this password change.
- **User Objectclasses for Active Directory:** You can use any appropriate objectclass (User or an extension) for Active Directory schema information. (In version 1.0, you could only use the User objectclass.)
- **Windows 2003 Server Active Directory Support:** You can now install and configure Identity Synchronization for Windows 1 2004Q3 and, synchronize passwords and attributes with Active Directory running on a Windows 2003 Server Standard or Enterprise Edition platform.
- **Additional Objectclass Support for User Synchronization:** You can define attribute maps for attributes in auxiliary and structural object classes. For Active Directory, the auxiliary classes set is restricted by your choice of main/structural objectclass. In Directory Server, you can use any other objectclass.
- **Migration:** Allows you to migrate from the version 1.0 or version 1.0 SP1 to version 1 2004Q3.
- **Solaris 9 x86 Platform Support:** Identity Synchronization for Windows fully supports the Solaris 9 x86 platform.
- **Linkusers and resync Command Line operation:** The linkusers command's functionality has now been merged with the resync command. Three options are now added to the resync command line options. The commands are:
 - `-f <linkusers.cfg> --` the linking file (used previously in the linkusers command)

- `-k` -- only link users
- `-i NEW_LINKED_USERS` -- reset the password of newly linked users. This is the same as `ALL_USERS` and `NEW_USERS` command except for users that are linked in the Directory Server.

For more information on this new feature, see the *Identity Synchronization for Windows Installation and Configuration Guide*.

NOTE Because Windows NT is expected to be fully EOL'ed by Microsoft in December 2004, Identity Synchronization for Windows 1 2004Q3 will fix bugs related to Windows NT but will not support new features for that platform.

See Windows Life Cycle Support at the following location for additional information: [http://support.microsoft.com/default.aspx?scid=fh;\[ln\];LifeWin](http://support.microsoft.com/default.aspx?scid=fh;[ln];LifeWin)

Product Changes

The following changes were made to the product for the version 1 2004Q3 release:

- **Installation:** Because Sun Java Enterprise System 2 2004Q2 installs Sun Java System Message Queue Enterprise Edition and Sun Java System Directory Server (both of which are required for Identity Synchronization for Windows 1 2004Q3), you must install Sun Java Enterprise System on your Solaris systems before installing Identity Synchronization for Windows 1 2004Q3.

Previously, Identity Synchronization for Windows version 1.0 installed Sun Java System Message Queue 3.0.1 (Message Queue) but version 1 2004Q3 does not.

- **Product and Documentation Rebranding:** The Identity Synchronization for Windows product and product documentation have been rebranded from *Sun ONE* Identity Synchronization for Windows to *Sun Java System* Identity Synchronization for Windows.

Performance Enhancements

Synchronization performance has been improved significantly.

Changes to the Documentation

Product and Documentation Rebranding: The Sun Java System Identity Synchronization for Windows product and product documentation have been rebranded from *Sun ONE* Identity Synchronization for Windows to *Sun Java System* Identity Synchronization for Windows.

Hardware and Software Requirements

Operating System Requirements

The following tables describe the operating system requirements for this release of Identity Synchronization for Windows:

Table 2 Solaris Requirements

Component	Solaris Requirement
Core Components	Solaris 8™ for UltraSPARC® (32-bit and 64-bit) Solaris 9™ SPARC® Platform Edition (32-bit and 64-bit) Solaris 9™ Operating System (x86 Platform Edition for Pentium II or later) IA-32
Connectors for Sun Java™ System Directory Server and for Windows Active Directory	Solaris 8 for UltraSPARC (32-bit and 64-bit) Solaris 9 for SPARC platforms (32-bit and 64-bit) Solaris 9™ Operating System (x86 Platform Edition for Pentium II or later) IA-32
Sun Java™ System Directory Server plug-in	Solaris 8 for UltraSPARC (32-bit and 64-bit) Solaris 9 for SPARC platforms (32-bit and 64-bit) Solaris 9™ Operating System (x86 Platform Edition for Pentium II or later) IA-32

Table 3 Windows Requirements

Component	Windows Requirement
Core	Windows 2000 Server SP4 Windows 2000 Advanced Server SP4 Windows Server 2003 Standard or Enterprise Edition
Connectors for Sun Java™ System Directory Server and for Windows Active Directory	Windows 2000 Server SP4 Windows 2000 Advanced Server SP 4 Windows Server 2003 Standard or Enterprise Edition
Sun Java™ System Directory Server plug-in	Windows 2000 Server SP4 Windows 2000 Advanced Server SP 4 Windows Server 2003 Standard or Enterprise Edition
NT connectors and plug-ins (subcomponents)	Windows Primary Domain Controller NT 4.0 Server SP 6A (for x86 only)
To Synchronize with Active Directory on Windows 2003 Standard and Enterprise Server	Windows Server 2003 Standard Edition (with latest security updates) Windows Server 2003 Enterprise Edition (with latest security updates)

Hardware Requirements

Your hardware (all platforms) must meet the following minimum requirements to run Identity Synchronization for Windows:

- Approximately 400 MB of disk space for a minimal installation
- A minimum of 512 MB of RAM for servers running any Identity Synchronization for Windows component. (1 GB of RAM preferred)

Sun Java System Software Requirements

To run Identity Synchronization for Windows, you must install the following Sun Java System software components:

- Sun Java System Message Queue Enterprise Edition version 3.5 SP 1 (formerly Sun ONE Message Queue)

Message Queue Enterprise Edition version 3.5 SP 1 must be installed prior to installing Identity Synchronization for Windows. It is also recommended that you install Message Queue Enterprise Edition version 3.5 SP 1 prior to installing Sun Java System Directory Server 5 2004Q2.

To install the Identity Synchronization for Windows core on an *existing* Sun Java System Message Queue installation, you must be using Message Queue Enterprise Edition 3.5 SP1. Trying to install Identity Synchronization for Windows core on an improper version of Message Queue will cause synchronization failures.

- Sun Java System Directory Server version 5 2004Q2 or higher

To install Identity Synchronization for Windows 1 2004Q3 you must be running Directory Server 5 2004Q2 (5.2 Patch 2)

For more information on the Solaris Package installation or the patches to be applied, refer to [Important Information](#) in the [Sun Java System Directory Server 5 2004Q2 Release Notes](#).

For more information on the Compressed Archive (ZIP) installation, how to patch, and known bugs in the zip upgrade, refer to [Installation Notes](#) in the [Sun One Directory Server 5.2 Release Notes](#).

For a list of bugs fixed by Directory Server 5.2 Patch 2 (for the important bug fixes) or see the individual READMEs of all applied patches:

[Sun Java System Directory Server 5 2004Q2 Release Notes](#).

You must install a Directory Server plug-in (subcomponent) on every Directory Server master, replica, and hub in your deployment.

For the latest information about patches that may be required to install Directory Server 5 2004Q2 on Solaris, refer to the *Sun Java System Directory Server 5 2004Q2 Installation and Migration Guide* and the *Sun Java System Directory Server 5 2004Q2 Release Notes*, which can be found at the following web site:

http://docs.sun.com/db/coll/DirectoryServer_04q2

- Sun Java System Directory Server 5 2004Q2 Retrochangelog Patch

To correct an issue with the Directory Server Retrochangelog and the Delete functionality in Identity Synchronization for Windows 1 2004Q2, a patch must be installed on the Sun Java System Directory Server 5 2004Q2. The patch number details for systems specific to your environment are:

- For Solaris Sparc Package Format: Patch Number 117907-02 or higher
- For Solaris Sparc Compressed Archive Installations: Patch 5077789
- For Solaris X86 Package Format: Patch Number 117908-02 or higher
- For Solaris X86 Compressed Archive Installations: Patch 5077789
- For Windows Compressed Archive Installations: Patch 5077789

For more details on these patches and how to update them to the Directory Server environment, see the `README.patch` file located in the Identity Synchronization for Windows download directory:
<download_root>/patches/directory/README.patch

- **Java Runtime Environment**
A J2SE Java Runtime Environment (JRE) is not provided with this product.
 - You must install JRE 1.4.2_04 (or later) to run the Identity Synchronization for Windows installer on Solaris or Windows Active Directory. You can also install the J2SE v 1.4.2_04 SDK which has performance improvements over the JRE.
 - You must install JRE 1.4.1_03 (or later) on Windows NT.

Also, you must set `JAVA_HOME` to a 1.4.2_04 JRE (or later) on Solaris before installing Identity Synchronization for Windows or the installer might report `JAVA_HOME` as not set.

Bugs Fixed in This Release

The following table describes the bugs fixed in Identity Synchronization for Windows 1 2004Q3:

Table 4 Fixed Bugs in Identity Synchronization for Windows 1 2004Q3

Bug Number	Description
Installation/Uninstallation	
4881466	Installing Core components with an existing Message Queue instance on a port other than 7676 had failed.
4829497	Uninstallation program did not remove all files and folders.
4820869	On Windows, the system had to be restarted prior to reinstalling the Core components.
4916789	Duplicate Directory Server plug-in IDs were generated for replicas installed on the same <code>Server_Root</code> .
5035406	Installation of Core failed on Solaris-based machines when JRE was used instead of JDK.
4880807	<code>runInstaller.sh</code> and <code>runUninstaller.sh</code> did not support a <code>-nodisplay</code> option.
5030928	Installation program did not support different credentials for primary and failover hosts.
5037157	Uninstall script not present after a “DS plug-in only” installation.
5050554	Starting the installation program in ‘ <code>-nodisplay</code> ’ mode required a viable <code>DISPLAY</code> .
4915192	Installing the connector on SSL-only Directory Server was not possible.

Table 4 Fixed Bugs in Identity Synchronization for Windows 1 2004Q3 (*Continued*)

Bug Number	Description
5052509	Text based uninstalling script did not remove all the Identity Synchronization related packages.
4937341	Uninstalling Identity Synchronization for Windows using the Add/Remove option on Windows-based systems did not work.
5056685	NT plug-in uninstallation program did not remove the password filter DLL (required so that Windows does not to load the DLL when it starts up, ensuring that the DLL is deleted). This had caused problems during reinstallation of the component.
4988901	Some of the panels of the installation program did not display the correct panel when the 'Back' button was clicked.
5030567	During NT Connector installation, the installation program did not correctly display a suggestive text that all sub-components for the NT connector was already installed.
5036330	During installation, when the default value for the descriptive text in the 'Enter some descriptive, unique name for the administration domain...' field was modified, the installation operation had failed.
5041518	The Connector port panel was be displayed in error when the Back button was clicked during the installation of the sub-components.
5048953/ 5049733	When the JAVA_HOME value contained quotes, the uninstallation operation failed.
5050691	During installation of the Core, the MQ Configuration window displayed an incorrect message related to the MQ version installed on the system. It had displayed 'null'.
5057716	The Directory Server plug-in package nor its registry entries were removed from the system although the plug-in was sucessfully uninstalled.
5071574	A valid port number (65535) was not accepted for the Directory Server connector.
5079602	The nt_dll_registrar did not force 'Notification Packages' to REG_MULTI_SZ.

Password Synchronization

4845844	Idsync resync command had failed to create users from Directory Server to NT, on synchronization.
4937502	Connectors can stop synchronizing after frequent loss of network connectivity.
4939825	Directory Server connector did not remove loop detection attribute for modified entries.
4906752	User creation quickly followed by a modrdn operation in the Sun Directory Server was not synchronized.
4933861	NT Connector showed excess activity when synchronization was started after an 'idsync resync -c -o Sun' if synthetic attributes were used.
4941200	User entries that were renamed were not synchronized when only case was changed.
4893525	Attribute modifications were lost when network connection to the Active Directory server was terminated.

Table 4 Fixed Bugs in Identity Synchronization for Windows 1 2004Q3 (*Continued*)

Bug Number	Description
5019327	Directory Server connector synchronizes users with objectclass set to the subclass of the synchronized objectclass type.
4995351	Identity Synchronization for Windows mapped incorrect attribute.
5036025	Modifying SULs and then attempting to synchronize users had resulted in a NullPointerException error (reported in the log files) and the connector stopped responding.
5054654	The changes made to the password on NT were lost when the connector was reset or shutdown abruptly.
Sun Java System Message Queue	
4881240	On Solaris, an existing Message Queue could not be used when installed in a user directory.
General	
4943564 / 4939730	<i>Userpassword</i> was not an optional attribute.
4994145	The Directory Server plug-in tested connection to unavailable hosts too frequently.
5041435	On-demand password update stopped the Directory Server from responding if the 'Password History' option was enabled.
4939859	Idsync linkusers/resync ignored LDAP filter option if the source connector was Windows NT.
4987742	<i>resync</i> did not process all the entries due to race condition.
5048362	Newline characters from log messages were not automatically removed.
4925575	Active Directory connector installer did not check to make sure the domain matched the certificate domain.
4901486	Multiple Active Directory forests was previously not supported by Identity Synchronization for Window 1 2004Q3.
Console General	
5040094	"objectclass=<some oc>" had reported an invalid filter error.
5030704	The <i>resync</i> interval for the Active directory source from the Console could not be modified.
5026929	Default value for mandatory creation attributes could not be specified.
4941238	Log viewer incorrectly parsed the log record.
5008697	Another item was added to the list when the cn mapping was edited instead of updating the existing item.
50134407	A directory source could be created with the same name as an existing directory source. No error message was displayed nor the directory source could be deleted.
5026198	Typographical errors that existed in the Log window of the Console have been corrected.
5044529	The Console preps did not work for SSL-only Directory Server.

Table 4 Fixed Bugs in Identity Synchronization for Windows 1 2004Q3 (*Continued*)

Bug Number	Description
5045350	When an existing creation attribute was modified, the valued could not be set to <none>.
4921889	When the View Tree option was selected again, the Console did not return to the normal tree view.
Connector	
4988028	Java Run Time Exception (RTE) on missing usunchanged attribute.
Command Line Utilities	
5015766	Passing empty password to <code>idsync changepw</code> makes subsequent access to configuration registry impossible.
4986303	Command line interface did not provide default values for the <code>-h</code> , <code>-p</code> , <code>-D</code> , and <code>-s</code> options.
5038195	<code>resetconn</code> did not provide an appropriate error message if the configuration suffix was invalid.
5019543	<code>printstat</code> did not provide an appropriate error message if the configuration suffix was invalid.
5024148	<code>resetconn</code> did not delete the connector Message Queue credentials.
4941125	<code>resync</code> updated in-sync users if the source is Sun and synthetic attributes were synchronized.
4939484	<code>linkusers</code> command may never exit.
5015575	The CLI operation did not stop when the 'c' command was executed on the command line prompt.
5062028	Command line prompt stopped responding when the Core was installed with SSL. (The default value for the port on the CLI was the SSL port.)

Important Information

This section contains the latest information that is not contained in the core product documentation. This section includes the following topics:

- [Installation Notes](#)
- [Compatibility Issues](#)
- [Performing Data Recovery When System or Application Fails](#)
- [Documentation Updates for Identity Synchronization for Windows 1 2004Q3](#)
- [Running Identity Synchronization for Windows in a Firewalled Environment](#)

Installation Notes

Before installing Identity Synchronization for Windows 1 2004Q3, be sure to read the “Preparing for Installation” chapter provided in the *Sun Java™ System Identity Synchronization for Windows 1 2004Q3 Installation and Configuration Guide*.

Using Windows 2003 Server

- You can now use Windows 2003 Server Standard or Enterprise edition as a platform for installing and configuring Identity Synchronization for Window 1 2004Q3.
- On Windows 2003 Server, the default password policy enforces strict passwords, which is not the default password policy on Windows 2000.

Windows 2003 Server Issues

Windows 2003 Server behavior for ‘user must change pw at next login’ is different from Windows 2000. (4997513)

On Windows 2003 the user must change pw at next login flag is set by default, which is not the case on Windows 2000.

When you create users on Windows 2000/2003 with the ‘user must change pw at next login’ flag set, users will be created on Directory Server with no password. The next time the users log into Active Directory, they will be forced to change their password, which will invalidate their passwords on Directory Server and force on-demand synchronization the next time those users authenticate to Directory Server.

Until users change their password on Active Directory they will not be able to authenticate to Directory Server.

Compatibility Issues

Compatibility issues when using certain Remote Console products to access the Identity Synchronization for Windows console. (5077227)

Problems could occur when attempting to view the Identity Synchronization for Windows console using PCAnywhere 10.x or Remote Administration2.1. (However, PCAnywhere version 9.2 may not cause errors.) If problems persist, remove the remote administration software. Alternatively, VNC could be used; it is not known to cause any issues displaying the Identity Synchronization for Windows console.

Performing Data Recovery When System or Application Fails

In case of a hardware or application failure it may be necessary to restore the data from a backed up in some of the synchronized directory sources.

After completing the data recovery, however, it is necessary to perform an additional procedure to ensure that the synchronization can proceed normally.

The connectors - in general - maintain information about the last change propagated to the message queue.

This data - referred as the connector state - is used to determine the subsequent change the connector has to read from its directory source. If the database of a synchronized directory source is restored from a backup, then the connector state may no longer be valid.

Windows-based connectors (Active Directory or Windows NT) also maintain an internal database. This database is a copy of the synchronized data source, and is used to determine what has changed in the connected data source. It is easy to see that the internal database will no longer be valid once the connected Active Directory source or Windows NT system is restored from a backup.

In general, the `idsync resync` command can be used to repopulate the recovered data source.

NOTE	Resynchronization cannot be used to synchronize passwords with one exception. The <code>-i ALL_USERS</code> option can be used to invalidate passwords in Sun Java Systems Directory Server systems if the resynchronization data source is Windows (and the SUL list includes only Active Directory systems).
-------------	--

Using `idsync resync`, however, may not be an acceptable option in every situation.

CAUTION Before executing any of the steps detailed below, make sure that synchronization is stopped.

Bidirectional synchronization

The recommended procedure is to use the `idsync resync` command with the appropriate modifier settings (according to the synchronization settings). The target of the `resync` operation should be the recovered directory source.

Unidirectional synchronization

If recovered data source is a synchronization destination, then the same procedure can be followed as for bidirectional synchronization.

If recovered data source is a synchronization source, then `idsync resync` can still be used to repopulate the recovered directory source. There is no need to change the synchronization flow settings in the Identity Synchronization for Windows configuration, `idsync resync` allows setting synchronization flow independent of the configured flows using the `-o <Windows|Sun>` option.

Consider the following scenario as an example:

Bidirectional synchronization is setup between a Sun Java Systems Directory Server and Active Directory

- The database of a Microsoft Active Directory server has to be recovered from a backup.
 - In Identity Synchronization for Windows, this Active Directory Source is configured for the SUL 'AD'
 - Bidirectional synchronization for modifies, creates and deletes is setup between this Active Directory Source and a Sun Directory Server Source.
1. Stop synchronization `idsync stopsync -w - -q -`
 2. Resynchronize Active Directory Source and resynchronize modifies, creations and deletes:
`idsync resync -c -x -o Sun -l AD -w - -q -`
 3. Restart synchronization `idsync startsync -w - -q -`

Directory Source Specific Recovery Procedures

Microsoft Active Directory

If Active Directory can be restored from a backup, then follow the procedures described in the bidirectional or unidirectional synchronization sections.

It may become necessary, however, to use a different domain controller after a critical failure. In this case, follow these steps to update the configuration of the Active Directory Connector:

1. Start the Identity Synchronization for Windows management console.
2. Select the Configuration tab.
3. Expand the Directory Sources node.
4. Select the appropriate Active Directory Source.
5. Click Edit controller...
6. Select the new domain controller.
It is recommended to make the selected domain controller the NT PDC FSMO role owner of the domain
7. Save the configuration.
8. Stop the Identity Synchronization service on the host where the Active Directory Connector is running.
9. Delete all the files (but not the directories) under
`<serverroot>/isw-<hostname>/persist/ADPxxx`, where xxx is the number portion of the Active Directory Connector identifier (for example, 100 if the Active Directory Connector identifier is CNN100).
10. Start the Identity Synchronization service on the host where the Active Directory Connector is running.
11. Follow the steps based on your synchronization flow in the unidirectional or the bidirectional synchronization sections.

Sun Java System Directory Server

Either the Retro Changelog database or the database with synchronized users (or both) can be affected by a critical failure.

1. Retro-Changelog Database.

There may have been changes in the Retro- Changelog database that the Directory Server connector could not process. Restoring the Retro Changelog database only makes sense if the backup contains some unprocessed changes. This can be done by comparing the most recent entry in the `<serverroot>/isw-<hostname>/ADPxxx/accessor.state` file with the last changenumber in the backup. If the value in `accessor.state` larger or equal than the changenumber in the backup, then it is not necessary to restore the database, but the database should be recreated.

After the Retro-Changelog database is recreated, make sure that you run `idsync preps` or click Prepare Directory Server from the Sun Directory Source window in the Identity Synchronization for Windows management console.

The Directory Server connector will detect that the Retro-Changelog database is recreated and log a warning message. You can safely ignore this message.

2. Synchronized Database.

If there is no backup available for the synchronized database, then the Directory Server connector has to be reinstalled.

If the synchronized database can be restored from a backup, then follow the procedures described in the bidirectional or unidirectional synchronization sections.

Documentation Updates for Identity Synchronization for Windows 1 2004Q3

You can access the Identity Synchronization for Windows online documentation files via a browser. In addition, you can download the entire documentation set, in HTML format.

After downloading this file, extract it to the following location:

```
<ServerRoot>/manual/en/isw
```

The ServerRoot is the location of the Sun Java System Administration Server. The actual ServerRoot path depends on your platform, your installation, and your configuration. The ServerRoot directory contains the `startconsole` program.

You can then access the documentation set directly from `<ServerRoot>/manual/en/isw/index.html` or from the Server Console by selecting Documentation Home from the Help menu.

Running Identity Synchronization for Windows in a Firewalled Environment

You can run Identity Synchronization for Windows in a firewalled environment. This section describes which server ports you must expose through the firewall, as follows:

- [Message Queue Requirements](#)
- [Installer Requirements](#)
- [Core Component Requirements](#)
- [Console Requirements](#)
- [Connector Requirements](#)
- [Directory Server Plug-in Requirements](#)

Message Queue Requirements

By default, Message Queue uses dynamic ports for all services except for its port mapper. To access the Message Queue broker through a firewall, the broker should use fixed ports for all services.

After installing the core, you must set the `imq.<service_name>.<protocol_type>.port broker` configuration properties. Specifically, you must set the `imq.ssljms.tls.port` option. Refer to the *Sun Java™ System Message Queue Administrator's Guide* for more information.

Installer Requirements

The Identity Synchronization for Windows installer must be able to communicate with the Directory Server acting as the configuration directory.

- If you are installing an Active Directory connector, the installer must be able to contact Active Directory's LDAP port (port 389).
- If you are installing a Directory Server connector or a Directory Server plug-in (subcomponent), the installer must be able to contact the Directory Server's LDAP port (default port 389).

Core Component Requirements

The Message Queue, system manager, and command line interface must be able to reach the Directory Server where the Identity Synchronization for Windows configuration is stored.

Console Requirements

The Identity Synchronization for Windows console must be able to reach the following:

- Active Directory over LDAP (port 389) or LDAPS (port 636)
- Active Directory Global Catalog over LDAP (port 3268) or LDAPS (port 3269)
- Each Directory Server over LDAP or LDAPS
- Sun Java System Administration Server
- Message Queue

Connector Requirements

All connectors must be able to communicate with Message Queue. In addition:

- The Active Directory connector must be able to access the Active Directory Domain Controller via LDAP (port 389) or LDAPS (port 636).
- The Directory Server connector must be able to access Directory Server(s) via LDAP (port 389 default) or LDAPS (port 636 default).

Directory Server Plug-in Requirements

Each Directory Server plug-in must be able to reach the Directory Server connector's server port, which was chosen when the connector was installed. Plug-ins running in Directory Server Master replicas must be able to connect to Active Directory's LDAP (port 389) or LDAPS (port 636). The plug-ins running in other Directory Server replicas must be able to reach the Master's Directory Server LDAP or LDAPS ports.

Known Issues and Limitations

This section contains a list of the known issues with Identity Synchronization for Windows 1 2004Q3. The following product areas are covered:

- [Installation and Uninstallation](#)
- [Connectors and Plug-Ins](#)
- [Console and Command Line](#)
- [Password Synchronization](#)
- [Sun Java System Message Queue](#)
- [General Issues](#)

Installation and Uninstallation

Instructions for manually scrubbing the product registry. (5050004)

If you need to remove references to Identity Synchronization for Windows from the product registry, use the procedures described for the Windows NT and Windows 2000 platform in Chapter 7, “*What to Do if the 1.0 Uninstallation Fails*” section of the *Identity Synchronization for Windows Installation and Configuration Guide*.

Solaris scripts will not work if you install core in a directory with spaces in its name. (4801643)

The command line scripts on Solaris will not work if you install Identity Synchronization for Windows core in a directory with a space in its pathname.

Message Queue broker cannot start if the Base DN contains spaces. (4892332 and 4892490)

Do not install core on a suffix containing spaces or the Message Queue broker will fail to authenticate.

Side-effects of installing core with an existing Message Queue instance. (4882194)

Installing core with an existing Message Queue broker instance can affect the existing instance. For example, an existing configuration was modified as follows:

- The `/etc/imq/imqbrokerd.conf` file was modified to start the broker automatically on start-up, which prevented other broker instances launched from `/etc/init.d/imq` script from being launched on reboot.

Message Queue broker requires a minimum of 512MB of memory. (4819519)

The Message Queue broker requires a minimum of 512 MB of memory. Because the broker is installed as part of core, the machine where core is installed should have at least 1GB of RAM.

Uninstalling plug-ins if a multi-Directory Server instance installation removes the uninstaller. (4916035)

You cannot uninstall multiple plug-ins if two Directory Server instances have the same file system installation root (for example, `/usr/sunone/servers/slapd-foxhead` and `/usr/sunone/servers/slapd-foxhead2`).

Workaround:

1. Open the Directory Server console (for the Directory Server where you installed the plug-in).
2. Click on the Configuration tab.
3. Double-click on the `Plugins` folder to expand the plug-in tree.
4. Click on `pwsync` and uncheck the Enable plug-in checkbox.
5. Restart Directory Server.

Indeterminate behavior of Active Directory connector if installation is cancelled before completion and when attempted to reinstall again. (5038905)

If the installation program is cancelled while it is configuring the connector and when the installation program is executed again, the connector option is not available for installation.

Workaround

Run the `idsync resetconn` from the command-line prompt to reset the connector's configuration, and then re-run the installer to re-install the connector. For details on running `idsync resetconn` command, see the *Sun Java System Identity Synchronization for Windows Installation and Configuration Guide*.

Registry keys pertaining to the product are not removed when the product is uninstalled. (5045237)

After performing an uninstallation of core, the Sun Java System Identity Synchronization for Windows related nodes in the product registry file are not removed. To successfully reinstall the product, you must manually remove the nodes from the product registry keys. For more details on removing these product registry keys, see the *Identity Synchronization for Windows Installation and Configuration Guide*. This situation only occurs on Solaris 8.

Identity Synchronization for Windows related references are displayed in the Console when the Core is uninstalled without connecting to the config registry. (5049700)

An error message is displayed when the Console is started after performing a blind uninstallation (without connecting to the config registry) of Identity Synchronization for Windows.

The 'temp' directory, where install logs are logged could be a hidden directory. (5051905)

The under C:\ Documents and Settings > Administrator > Local Settings folder could be a hidden folder on some Window systems.

Workaround

To view Local Setting folder and Temp subfolder, the Windows Explorer option Show Hidden files should be selected. Alternately, type either `cd %TEMP` or `cd %TMP` on the command prompt to view installation related log files in the directory. The logs can then be viewed using Notepad.

Authentication to Message Queue broker fails if the root suffix contains spaces. (4892903)

The Identity Synchronization for Windows configuration must be stored in root suffix that does not have any spaces due to a limitation of Message Queue.

Workaround

Create a new root suffix to store the Identity Synchronization for Windows configuration before installing Core.

After a failed Directory Server plug-in installation, the To Do list displays that the installation of the plug-in is complete. (5081912)

In certain scenarios, the To Do list may display that the Directory Server plug-in has been installed although the installation of the plug-in actually failed.

During the uninstallation of a connector, the uninstallation program does not accurately display the disk space it will recover. (5081823)

The uninstallation program inaccurately displays 0 bytes (as the number of bytes it will recover after the uninstallation procedure), when uninstalling a connector. When the properties of the disk space is viewed, the actual disk space size recovered will not be zero.

Installation program does not enforce you to install components in the same directory where the Directory Server plug-in installation directory is located. (5080178)

If the Directory Server plug-in is the first component installed on a machine, then all succeeding component installations, on that particular machine, must be installed in the same installation directory (of the Directory Server plug-in). However, the installation program does not enforce this criteria during installation.

Uninstallation program may display incorrect information when uninstalling components. (5079489)

When a connector is uninstalled from a machine where the Core component is not installed, then the installer incorrectly reports that it is uninstalling the Core component. This message can be ignored. Identity Synchronization for Windows console references is not removed if a uninstallation procedure is performed when the configuration directory does not exist. (5077156)

When the option to uninstall the product without the configuration directory is selected, then the Sun Server Console retains all references to the Identity Synchronization for Windows console. After uninstalling the product, the icon for the Identity Synchronization for Windows will still exist in the topology tree. On attempting to display the console, an error occurs. For more information on removing the console's references, see Chapter 8, in the "Uninstalling the Console Manually" section of the *Identity Synchronization for Windows Installation and Configuration Guide*.

Uninstallation does not remove the 'server-root/isw-*/lib' directory and the jar files. (5038284)

The uninstallation operation does not remove the `lib` directory containing the `*.jar` files. These files and the directory must be manually deleted.

Indeterminate behaviour of Active Directory connector when the installation operations is cancelled and reinstalled. (5038905)

When installing the Active Directory connector if the installation operation is cancelled abruptly and then a re-installation of the connector is attempted, the Active Directory connector displays an incorrect status as 'Installed'. This status does not change and the synchronization operation does not occur nor a reinstallation of the Active Directory connector is possible - when attempted.

Workaround

You must run the `idsync resetconn` command to reinstall the connector. For details on running the `idsync resetconn` command, see the *Identity Synchronization for Windows Installation and Configuration Guide*.

Identity Synchronization for Window installation fails on Directory Server 5.2p3 installed with Sun Java Enterprise System 3. (5092530)

You cannot install the core Identity Synchronization for Windows product against Directory Server 5.2 P3 or higher. Identity Synchronization for Windows 1 2004Q3 will support Sun Java Enterprise System 3 (Directory Server 5.2 P3) as a data synchronization source only.

The installation list prompts to install the Directory Server Plug-in on the secondary master even after installation. (5096593)

The To Do list is almost always accurate, but sometimes it might fail to report the required steps nor does it not recognize that some steps have already been performed. For instance, it may not always reflect which Directory Server plug-ins have been or need to be installed.

Identity Synchronization for Windows installation on FAT32 system does not have ACLs. (5097751)

After installing Identity Synchronization for Windows on a FAT32 formatted drive and when the you check ACLs for the folders and files, the ACLs do not exist. It is recommended to avoid installing on non-NTFS partitions.

Plug-in only uninstallation may fail when using the Directory Server zip version. (5101589)

When attempting to perform a plug-in only uninstallation operation, the operation fails when the compressed archive package of the Directory Server is used.

Connectors and Plug-Ins

Deleting a pre-existing entry starts NT connector synchronization. (4864009)

Installations with existing Windows users (Active Directory or NT) must run an `idsync resync` command before starting synchronization to prevent undefined behaviors (such as existing Windows users being synchronized to Directory Server at any time).

Restart connectors if they are inactive. (4938309)

If the central error log reports a message similar to `No response from connector [CNN100] for 10 minutes`, you might have to stop and restart the Identity Synchronization for Windows daemon/service where the connector is running.

Workaround

- On Solaris, issue the `/etc/init.d/isw stop` and then `/etc/init.d/isw start` commands.
- On Windows, restart the Sun Java System Identity Synchronization for Windows service.

Restart Directory Server after enabling Secure Sockets Layer for the Directory Server plug-in. (4944804)

You must restart Directory Server after enabling Secure Sockets Layer (SSL) for the Directory Server plug-in (subcomponent) and adding the Active Directory CA certificate to the Directory Server's certificate database or OnDemand synchronization may fail trying to authenticate a user whose password changed on Active Directory (see sample log messages).

If Active Directory searches time out, administrators should increase search limit. (4881182)

If the Active Directory error log reports a time-limit-exceeded error for a connector, use `ntdsutil` from the Windows 2000 resource kit to increase the maximum search time out, as follows:

```
C:\idif>ntdsutil
ntdsutil: ldap policies
ldap policy: connections
server connections: set creds example.sun.com administrator password
server connections: connect to server matar
Binding to matar as user(administrator) in domain(example.sun.com) ...
Connected to matar as user(administrator) in domain(example.sun.com) ...
```

```
server connections: quit
ldap policy: show values
```

Policy	Current (New)
MaxPoolThreads	4
MaxDatagramRecv	1024
MaxReceiveBuffer	10485760
InitRecvTimeout	120
MaxConnections	5000
MaxConnIdleTime	900
MaxActiveQueries	20
MaxPageSize	1000
MaxQueryDuration	120
MaxTempTableSize	10000
MaxResultSetSize	262144
MaxNotificationPerConn	5

```
ldap policy: Set InitRecvTimeout to 2400
ldap policy: Commit Changes
```

Binary-valued attributes created without the ;binary subtype will not be processed by Sun Java System Directory Server. (5029226)

Certain attributes such as `userCertificate` require the `;binary` option at the instance of creation. Identity Synchronization for Windows can synchronize the values of such attributes, but it does not set the `;binary` option at creation time. This may cause problems for clients communicating with the Sun Java System Directory Server. Sun Java System Directory Server does not return such an attribute if the attribute was created without the binary option and the client requests the attribute with the binary option.

Identity Synchronization for Windows does not validate the number of characters used when creating the `user_name` attribute. (5021886)

NT SAM has a limit of 20 characters for the `'user_name'` attribute, however, Sun Java Directory Server does not have a restriction on the number of characters used create the user name. The entry mapped to `'user_name'` attribute on NT SAM cannot be used although the sucessfully flows from NT SAM to Sun Java Directory Server. An error message is displayed when the properties of the entry is edited or viewed on the NT SAM.

Console and Command Line

Run `idsync prepds` if Retro Change Log database files are re-created, corrupted, or missing. (4921114 and 4832355)

If the Retro Change Log (RCL) database is ever deleted or corrupted, the Directory Server or the Directory Server connector will issue warning messages. When you see these messages, you must re-create the Retro Changelog and rerun the `idsync prepds` command before synchronization will resume.

Browse button choices for Base DN may not change after choosing a new naming context. (4944711)

If you configure Identity Synchronization for Windows from the console to use more than one Directory Server source and more than two Active Directory (AD) sources, when you configure a new Synchronized Users List (SUL), the Browse button choices presented for the base DN may not accurately reflect the proper Directory Server or Active Directory sources.

Workaround

Manually type the Base DN name into the Base DN field.

Console schema host should point to configuration directory. (4877996)

When specifying a schema host, it is recommended that you use the core configuration directory only. Do not use a stand-alone Directory Server or any other remote configuration directory.

Console Status window does not provide 508 accessibility for viewing log files. (4874361)

The Log File Viewer in the Console Status window does not permit a mouseless interface to view the log files.

Workaround

To view the log files, copy the files to a preferred text editor (outside of the Console Log Viewer).

Console status for Message Queue does not correctly indicate the actual status of the system components. (4937312)

If the network connectivity is interrupted between the Console and MessageBroker, the Console may incorrectly report the status of system components.

Workaround

If network problems occur, make sure that you restart the Console. You could also execute the `idsync printstat` command to receive a more accurate view of the message queue status.

A message is prompted to prepare the Directory Server although the Directory Server has already been prepared, when adding a new Directory Server data source. (5029558)

Whenever you create a new Sun Java System Directory Server source, you will be prompted to prepare the Directory Server source. If you have already prepared the directory source you can safely click the 'No' option.

A message 'Resetting...' is displayed, when the CLI command `resetconn` is executed. Reset password fails and all information about the Directory Server source, configuration, and so on are removed. (5039655)

The Console should not be running when the `resetconn` command-line function is executed. If you do not exit the Console prior to executing the command, the "Resetting..." message is displayed. You should now exit the Console and restart it.

The 'startsync' command fails to execute. The error 'Failed to start synchronization for some of the requested directory sources...' message is displayed. (5050443)

Under certain conditions (for example in case of insufficient memory), it is possible that the command line or the management console reports that "Start synchronization" was successful even if some components could not start synchronization. If you encounter synchronization issues, check the error log for memory related messages.

Parameterized attribute fails in case of multiple values for single-value attributes. (5069907)

The synchronization fails when multiple values are specified instead of a single value for single-value attributes. An error nor a warning message will be displayed when the values are being saved to the Directory Server.

When the `idsync` command is executed, passwords are displayed in clear text on the screen. (4900126)

When the `idsync` command prompts for the bind and config passwords, on entering the passwords, they are displayed as clear text and are not encrypted.

Workaround

To avoid passwords being displayed on the screen, store each password in a protected file and then redirect it to the command line. If the '-' option is provided for any password argument, the `idsync` command prompts for the password values in the order the options appear on the command line. For example, if the administrator password is `adminPw` and the configuration password is `configPw`, then create a file (`passwords.txt`) whose contents are:

```
adminPw
configPw
```

And then execute `idsync printstat -w - -q - < passwords.txt` to run the command.

Error while loading log files. (5091787)

In some cases, while loading the `audit.log` file in the Console in the Status tab, this error could be displayed: 'Cannot retrieve log entries due to unknown error. Admin server may need to be restarted.'

Workaround

The `audit.log` file will be loaded, when it is accessed, on subsequent attempts to load the file.

Prepds displays an error message in MMR setup on migration. (5093124)

During migration of a replicated environment, `idsync prepds` may incorrectly reports that schema replication has failed. (For example, the error message could be: "The preferred Sun Java System Directory Server at `ldap://preferred.example.com:389` failed to replicate schema changes to secondary Sun Java(TM) System Directory Server at `ldap://secondary.example.com:389`. Check the replication settings.'). In this case, run `idsync prepds` with the same arguments again. Investigate the replication settings only if the second run of `idsync prepds` results in the same error message.

Using Reflection X 10.0 to access the Console may not be usable. (5095013)

Some of the dialog boxes may not be unusable because the buttons or text boxes cannot be viewed nor can the dialog boxes be resized.

Password Synchronization

Password policy issues. (4834865 and 4811572)

It is possible for password policies used on different directories to cause synchronization errors. Examples include password length and minimum maximum required characters. Administrators must change the incompatible password policy manually to match that of other systems.

Corresponding attributes or passwords that are modified concurrently may not synchronize properly. (4854183 and 4808601)

If an entry that is being synchronized between two directory sources and concurrent modifications are made to an attribute, the attribute may not be synchronize properly. For example, consider this sequence of events.

- John Smith changes his telephone number to 555-1111 in Active Directory (AD).
- This change is propagated to Directory Server; but before this change arrives, an administrator erroneously sets John Smith's telephone number to 555-1112 in Directory Server.

- Next, the change made in Active Directory is applied to Directory Server and John Smith's telephone is set to 555-1111.
- Likewise, the change made in Directory Server is propagated to AD, and John Smith's telephone number is set to 555-1112.

The two directory sources have swapped values and have become unsynchronized.

Similarly, if a user's password is modified on Active Directory (AD) and Directory Server at approximately the same time, the password may not synchronize properly in certain situations.

Under lightly loaded systems, the password modifications would have to occur within a few seconds of each other to become out of sync. Although this situation can occur even if the AD password is modified *after* it was set to the Directory Server value, it is unlikely — the AD password would have to be modified within a few milliseconds of being set to the Directory Server value.

Working with Active Directory's "user must change password at next login" function. (4827180)

If an administrator changes a user's password on Active Directory (AD) and specifies "user must change password at next logon," the password change will not be synchronized to Directory Server until the user logs on and changes their password.

A user authentication will fail under these circumstances:

1. A user changes their password on AD. (The password is propagated to Directory Server and the Directory Server password is invalidated).
2. The administrator resets the user's password and sets the "user must change password at next logon" flag.
3. If the user tries to log into Directory Server using the password from #1 or #2, the log on attempt will fail. Changing the password in AD or Directory Server will update the Directory Server password value.

Specifying a non-ASCII password in NT or Active Directory with the 7-bit check plug-in enabled will prevent the password from synchronizing to Directory Server. (4817344)

On Directory Server, the 7-bit check plug-in (subcomponent) is enabled for userpassword attribute values by default. See: <http://docs.sun.com/source/816-6699-10/pluginattr.html>

If you synchronize passwords from Windows to Directory Server that are not 7-bit clean and then you enable and configure this plug-in for userpassword attribute values, synchronization will fail.

You must be careful about synchronizing passwords with non-ASCII characters because the character encoding of the password value is not persisted. Therefore, Windows-side clients and Directory Server clients must use the same character encoding when changing passwords (and in cases of authentication) or the operation will fail.

Multiple password values are not supported. (4807350)

Multiple user password values are not supported.

Resync does not automatically resume the resync process when the system manager is restarted. (5077660)

When the resync command is executed and the system manager is restarted, resync does not automatically recover and restart the process.

When resynchronization is performed, creation attributes may get deleted. (5085134)**Concurrent updates to an attribute do not get synchronized. (5077760)**

This issue occurs if a value is added to an attribute at approximately the same time a different value is also added to the attribute in a corresponding remote directory entry. The attribute may not get synchronized.

When performing resynchronization, the link actions are not received by the Directory Server connector even if the resynchronization operation had aborted. (4985505)

When the `resync -c -o Sun` is executed, LINK actions are sent to the Directory Server after new users are created in Active Directory. These LINK actions are not received by the Directory Server connector although the resync operation has aborted. Currently, these LINK actions are published on the same temporary MQ topic that all resync/linkusers actions are published.

Deleted entries may not get synchronized from Directory Server to Active Directory due to a known issues in Directory Server Retro-Change Log plug-in. (5077814)

The Directory Server Retro-ChangeLog plug-in may fail to store the `dspswuserlink` in the plug-in entry for a deleted entry. If this occurs, synchronization for the deleted entry of the Directory Server entry to Active Directory does not occur.

Workaround

To resolve this issue, make sure you have updated the Directory Server with the patch that resolves this issue. For information on the patches required to resolve this issue, see the [“Sun Java System Directory Server 5 2004Q2 Rectrochangelog Patch”](#) section.

Sun Java System Message Queue

System manager cannot connect to Message Queue. (4907711)

The system manager cannot connect to Message Queue and the Message Queue is up.

Workaround

Restart the Identity Synchronization for Windows service/daemon where the core is installed.

Increase Message Queue broker's maximum memory for deployments of 100K+ users. (4924939)

Identity Synchronization for Windows configures the Message Queue broker to use a maximum of 512 MB of memory by default, which is sufficient for most installations. However, for installations larger than 100K users, you should increase the maximum memory to at least 1 GB to ensure optimal performance. For deployments of more than 200K users, increase the memory to 2 GB.

If the Identity Synchronization for Windows core is installed on *Solaris*, use the following steps to increase Message Queue broker's memory limit:

1. Issue the following command to stop the Message Queue broker:
2. Edit the `/etc/imq/imqbrokerd.conf` file to change the current default memory setting of `-Xmx512m` to `-Xmx1024m` for 1 GB of memory or `-Xmx2048m` for 2 GB of memory.
3. Issue the following command to start the Message Queue broker:

```
/etc/init.d/imq stop
```

```
/etc/init.d/imq start
```

If the Identity Synchronization for Windows core is installed on *Windows 2000*, use the following steps to increase Message Queue broker's memory limit:

1. Using the Windows Services Management console, stop the Message Queue broker service.
2. From the `<installation-root>/isw-<machine-name>/imq/bin` directory, issue the `imqsvcadm query` command from the command line. The output will be similar to the following:

```
Service iMQ Broker is installed.
```

```
Display name: iMQ Broker
```

```
Start Type: Automatic
```

```
Binary location: C:\sunone\servers\isw-example\imq\in\imqbrokersvc
```

```
JREHome: c:/j2sdk1.4.2/jre/
```

```
VM Args: -Xmx512m
```

```
Broker Args: -passfile
```

```
"C:/sunone/servers/isw-example/imq/etc/passfile.properties"
```

```
-DimqConnectionType=TLS -port 7676 -name psw-broker
```

3. Save the output from this command to a file.
4. Uninstall the Message Queue broker service by issuing the `imqsvcadm remove` command.

5. Before you can proceed, you must restart the Windows 2000 machine where core was installed.
6. From the `<installation-root>/isw-<machine-name>/imq/bin` directory, issue the following command using the output you saved from the `imqsvcadmin query` command issued earlier. For example:

```
imqsvcadmin install -jrehome c:/j2sdk1.4.2/jre/ -vmargs -Xmx1024m -args
"-passfile C:/sunone/servers/isw-example/imq/etc/passfile.properties
-DimqConnectionType=TLS -port 7676 -name psw-broker"
```

Where:

- The `-args` argument is filled in from the `Broker Args` field.
- The `-jrehome` argument is filled in with the `JREHome` field.
- To increase the memory to 1 GB, use `-vmargs -Xmx1024m`.
- Only for 64bit Java VM: to increase the memory to 2 GB, use `-vmargs -Xmx2048m`
The highest memory value for a 32bit Java VM is `-Xmx1750m`

7. Use the Windows Services Management console to start the Message Queue broker service.

Starting and stopping Message Queue broker. (4809493)

On Windows, the Message Queue broker runs as a service, and administrators can control the Message Queue broker service through the service control panel.

To start and stop the broker, you must reboot the machine after installing the core because the service manager process cannot see the required `IMQ_JAVAHOME` environment variable until Windows is rebooted. This situation applies only if you installed Message Queue with the core (i.e. a pre-existing Message Queue was not used).

Use the following commands:

```
/etc/init.d/imq( stop or start)
```

No support for using Message Queue on a machine where core is not installed. (4943576)

Identity Synchronization for Windows Core components and Message Queue must be installed on the same host.

General Issues

Errors can still exist when synchronization starts successfully. (4814324)

Even if `idsync startsync` returns success, you should check the central error log to verify that the connectors were able to connect to their directory sources.

Strongly recommend putting configuration directory and directory source in separate Directory Server instances for an MMR configuration. (4943470 and 4943480)

In a Multi-Master Replication (MMR) configuration, Sun strongly recommends that you put the configuration directory and directory source in separate Directory Server instances, and that you configure replication agreements *before* you install Identity Synchronization for Windows.

If you designate the same Directory Server instance as the configuration directory and the preferred Directory Server (user data), and you create Replication Agreements after installing Identity Synchronization for Windows, the schema elements created by the Identity Synchronization for Windows core installation may be deleted. If this happens, then Identity Synchronization for Windows will not run.

Workaround

To update the schema if you accidentally erase it:

1. Copy the `40so-psw.ldif` file (which contains the schema objects for the Configuration Registry for the install package only), to the Schema Directory of the Directory Server instance.
2. Change the `40so-psw.ldif` file name.

Some references in the schema are not loaded when the `40so-psw.ldif` is processed at start-up (consequence: the server does not start up).

3. Copy the renamed file to the Schema Directory of both masters. (From the server's point of view, the schema has not been changed over the protocol because the schema entry's change sequence number will remain the same).

Attributes used during linking operation should be indexed in the Directory Server. (4814412)

When linking users using `idsync resync (-f <filename> option)`, the command searches the Directory Server for users that match Active Directory or Windows NT users. Every Directory Server attribute used in an `idsync resync` operation should be indexed for equality.

Central logger cannot be turned off. (4945507 and 4933217)

Although the Identity Synchronization for Windows central logger (which logs to files, the syslog, or both) appears to allow you to turn off logging, the central logger will continue to log to the previously specified location.

For example, if you specify syslog logging from the console (with file logging turned off) and then turn off syslog logging, the program will continue logging to syslog. If you specify file logging from the console (with syslog logging turned off) and then disable file logging, the program will continue logging to the file log.

The same behavior occurs if the “Write logs to file” is unchecked and syslog was never used. In this case, the program continues writing logs to the directory.

Restarting the Identity Synchronization for Windows service has no effect — logging will continue.

Synchronization User List Browse button may not function properly. (4944348)

If you browse for a Base DN from the Synchronization User List (SUL) creation wizard or editor panel, it is advisable to double-check the base DN derived by using the Browse button. In some cases, the button will browse the wrong directory and result in an invalid base DN.

Disabling user accounts on Active Directory. (4943785)

If a user invalidates a user account and changes the password on Active Directory (AD), they will not be able to authenticate via AD using the new password. However, after disabling a user account on AD, they will still be able to log-in through Sun Java System Directory Server.

Changing the configuration directory port. (4941271)

If you change the port for a Sun Java System Directory Server that is currently being used as an Identity Synchronization for Windows configuration directory, you also must adjust the Identity Synchronization for Windows configuration so the software recognizes the port change or the System Manager and Message Queue broker will not work.

Workaround

1. Modify the port in
`<img_installroot>\img\var\instances\psw-broker\props\config.properties.`
 For example, `img.user_repository.ldap.server=<host>\:<port>`
2. Modify the port in `<isw_installroot>\resources\SystemManagerBootParams.cfg`
 For example, `<Parameter name="manager.configReg.hostPort" value="<port>" />`
3. Restart the Message Queue broker service/daemon.
4. Restart the Identity Synchronization for Windows service/daemon.

Support for unlike, multi-valued attributes is limited. (4987930 and 4807260)

Identity Synchronization for Windows provides only limited support for synchronizing unlike, multi-valued attributes because the results are undefined. The following restrictions apply:

- The values in a multi-valued attribute will be synchronized as a unit. For example, if you add a single value to a multi-valued attribute that already has four values, then all five values will be synchronized as a unit and the values of the corresponding remote attribute will be set to these five values.
- When pre-existing users are linked, their attributes will not be synchronized automatically. When a multi-valued attribute changes, the values of the attribute at the remote directory source will be overwritten with the values of the local directory source. For example, if you add a telephone number to an entry's previously empty `telephoneNumber` attribute in Active Directory (AD), then the `telephoneNumber` attribute for the corresponding entry in Directory Server will be set to this new value, overwriting any existing values.
- Concurrent updates to a multi-valued attribute might not be synchronized. If you add a value to a multi-valued attribute at approximately the same time that a different value is added to the multi-valued attribute in the corresponding remote directory entry, then the attribute might become out-of-sync. This situation is also true for single-valued attributes.
- When modifying or renaming the `cn` attribute, the `cn` is a multi-valued attribute type on Directory Server, but a single-valued attribute type on AD. AD uses this attribute type (and its value) to generate new DNs for the person entries to be renamed or modified. Because the connector does not know which value in a multi-valued `cn` should be used to construct the new DN, the connector sends the first value by default. Because the first value is generally not the correct value, the AD rename or modification fails.

If you specify renames (`ldap modrdns`) with `deleteoldrdn` flag set to 0 and the `rdn` component attribute type as `cn`, the operation will fail on the AD side. For example, if the following entry exists and is synchronized on both Directory Server and AD,

```
cn=old rdn, ou=example.com
cn=old rdn
```

and you rename the entry on Directory Server and set the `deleteoldrdn` flag to 0, Identity Synchronization for Windows will change the entry on the Directory Server side to

```
cn=new rdn, ou=example.com
cn= old rdn
cn= new rdn
```

but the rename will fail on the AD side because the entry will be created as:

```
cn=old rdn, ou=example.com not cn=new rdn, ou=example.com
```

resulting in an error message (found in the audit log) similar to the following:

```
[30/Jan/2004:16:41:14.831 -0600] WARNING 16 CNN100 dragon "The action does not have a
single value for attribute cn. The corresponding user at the remote repository might not
have been created with a corresponding attribute value, the attribute might have
multiple values, or cn is not a significant or creation attribute for this directory
source. See audit log for more information" (Action ID=CNN101-FA6784B526-787, SN=1)
```

For this operation to succeed, you must set the flag `deleteoldrdn=1`. Use the following example LDAP modification instructions to perform the rename operation successfully:

```
dn: cn=old rdn, ou=example.com
changetype: modrdn
newrdn: cn=new rdn
deleteoldrdn: 0
```

- When modifying a `cn` attribute using the `modify changetype` and `add` mode, if you add more than one `cn` attribute type *or* if a `cn` attribute type already exists and you add a new `cn` attribute type, the `modify` operation will fail. For example, if the following `cn` entry exists in both Directory Server and AD,

```
cn=example1, ou=example.com
cn=example1
```

You use the following LDAP modification instructions on the entry,

```
dn: cn=example1, ou=example.com
changetype: modify
add: cn
cn: new value
```

the Directory Server entry will change to

```
cn=example1, ou=example.com
cn=example1
cn=new value
```

However, the `modify` operation will fail on the AD side because AD is single-valued. The same error message noted in the previous case will display in the audit log, because the connector cannot distinguish between a rename or a modification.

Active Directory treats description attributes as single-valued even though AD schema describes them as multi-valued. (4938940)

When you add entries to Directory Server using a multi-valued description attribute, the following DSID-031D0809 error will result in the Active Directory (AD) connector `audit.log`:

```
[16/Oct/2003:10:02:54.998 -0500] SEVERE 29 CNN101 dragon "Unable to create user
"cn=Aaccf Amar1072,cn=users,dc=example,dc=sun,dc=com" at
ldaps://starlingvm0.example.sun.com:636. LDAP add operation failed. Error code: 19,
reason: 00002081: AtrErr: DSID-031D0809, #1: 0: 00002081: DSID-031D0809, problem 1005
(CONSTRAINT_ATT_TYPE), data 0, Att d (description)
" (Action ID=CNN100-F841CDBF2A-2568, SN=8)
```

The entry will exist in Directory Server but not in AD.

This issue appears to be an Active Directory defect. For more information, refer to the following article in Microsoft's knowledge base (286760):

<http://support.microsoft.com/default.aspx?scid=kb/en-us/286760&Product=win2000>

Workaround

Remove the entry from Directory Server, make the description attribute single-valued, and re-add the entry.

In addition, do not initialize more than one attribute for description in the Define Creation Attribute Mappings and Values dialog box.

No error message from plug-in when Secure Sockets Layer certificate is not trusted. (4924027 and 4924705)

In a Multi-Master Replication (MMR) configuration, if an Identity Synchronization for Windows plug-in (subcomponent) is communicating using Secure Sockets Layer (SSL) and an SSL problem causes a failure, if the plug-in does not provide error messages a CA certificate of the *peer* server's certificate (where the *peer* can be a preferred master, a secondary master, or an Active Directory) is probably missing from the certificate database of the Directory Server on which the plug-in is running.

You can use the `idsync certinfo` command line utility to identify missing certificates. This utility identifies which certificates are required in which database (which certificates the product expects).

Users created in Sun Java System Directory Server should include all attributes in Synchronized Users List filters. (4900568)

If you are synchronizing creates from Sun Java System Directory Server to Windows and the Directory Server Synchronized User List (SUL) definitions include filters, then try to create an entry with attribute values that do not match the SUL filter, the entry creation will not be propagated because the attributes are not in the SUL. And, because the original create was not propagated, the Directory Server entry will not be found on the Windows side.

Workaround

When this situation occurs, a warning will be logged and the administrator must run `idsync resync -c -o Sun` to create the Directory Server entry on Windows.

If you modify the entry so that the attributes match the SUL filter, modifications made to the entry will be propagated to the Windows side.

On-demand sync delay caused by NetBIOS. (4876741)

An attempt to synchronize two Active Directory (AD) domains using a Directory Server and core components configuration on Windows 2000, caused a delay when the Directory Server plug-in's on-demand password synchronization function was talking to AD. Most queries against AD normally take a few milliseconds. A packet trace identified some suspicious NBNS (NetBIOS Name Service) packets.

Workaround

To solve the problem, you must access the TCP/IP settings on the Directory Server machine and disable NetBIOS over TCP/IP.

Identity Synchronization for Windows namespaces (topics) used by message bus. (4827081)

- ConConfig_100
- CntrlLog_100
- SysMgr_100
- PSW_AuditLoggingTopic
- PSW_ErrorLoggingTopic
- PSW_LinkAuditLoggingTopic

In addition,

- For each connector in the system, there will be a CNN1XX_100 topic (such as CNN100_100, CNN101_100, and CNN102_100).
- For each Synchronization User List (SUL) in the system, there will be a topic based on the SUL name. (For example, an SUL named *people* will have a topic named *people_100*.)

Specifying a host from the Global Catalog or Configuration Directory dialog may take some time. (4826109 and 4812651)

When you specify a host that is not resolvable, no progress indicator (such as a cursor busy or status bar) displays to indicate that something is working.

NT user names must be unique. (4825636)

When creating a user in Directory Server to flow to NT, you must ensure that the Directory Server attribute mapped to `USER_NAME` has unique values.

Advise users to secure XML configuration files using access control lists (ACLs). (4812824)

Use file-level protection for the XML configuration files. These files may contain cleartext password values so you should secure them using mechanisms provided on their system — such as file-level ACLs.

Supported Synchronization User List and database relationship. (4811577)

Identity Synchronization for Windows only supports a single Directory Server database. You must include all Synchronization User Lists under a single Directory Server database.

Number of logs can grow without bounds. (4807451)

Unless you save or delete old logs, the number of each log file type in Identity Synchronization for Windows will grow without bounds (one per day).

Logs are named in the following format:

- audit_YYYY_MM_DD.log
- error_YYYY_MM_DD.log

The following logs are kept:

- audit
- error

These logs are located in:

- **On Solaris:** /var/opt/SUNWisw/logs
- **On Windows:** <install-root>/isw-<machine-name>/logs

Entry with special characters will not synchronize from Directory Server to Active Directory. (4816867)

Either Identity Synchronization for Windows cannot resolve the special characters (due to mapping restrictions) or Active Directory (AD) cannot create the user because one or more special characters were used in the uid.

The AD console does not allow you to create a “user logon name” that

- Contains any of the following special characters: `"/ [] : | < > ; ? % $ ^ & * () ! @ # - + = ~ ``
- Exceeds 20 characters
- Ends with a period or include commas
- Includes characters in the range 1-31, which are non-printable characters.

useraccountcontrol attribute default prevents creation of non-user Active Directory objectclass. (5043156)

Users cannot be created in Active Directory if the selected objectclass for the new users does not allow the `useraccountcontrol` attribute. This limitation does not apply to scenarios where the user objectclass or any other user-derived objectclasses allows the `useraccountcontrol` attribute in Active Directory.

Workaround

Edit the configuration user using the Directory Server console. Find and remove the `useraccountcontrol` attribute.

For example:

```
dn: cn=130,ou=AttributeDescriptions,cn=active[2],ou=GlobalConfig,ou=1.1,ou=IdentitySynchronization,ou=Services,dc=central,dc=sun,dc=com
pswVersion: 2
pswName: useraccountcontrol
pswSyntax: 1.3.6.1.4.1.1466.115.121.1.5
pswValue: 512
pswPreferCreationAttributeDefaultToAction: false
cn: 130
objectClass: pswattributedescription
objectClass: top
```

Edit all references to `useraccountcontrol` attribute too, specifically, in the `pswCreationAttributeDefaultRef` attribute of the Active Directory global schema.

For example:

```
dn: cn=127,ou=ActiveDirectory,ou=Globals,cn=active[2],ou=GlobalConfig,ou=1.1,ou=IdentitySynchronization,ou=Services,dc=central,dc=sun,dc=com
```

No validation is done for default values. (5051725)

Default values can be specified for the attributes and it can be applied to the directory entries when the attributes are created (see “Creation Attributes” in the *Sun Java System Identity Synchronization for Windows Installation and Configuration Guide*). Currently no validation is performed on the attribute values you specify. Specifying multiple values for attributes that are single-valued will result in object creation failure during synchronization of the entries. When specifying attribute values, make sure that the values you specify conform to the LDAP schema of your enterprise.

Inconsistent handling of modifications if the user appears in the Synchronization User List (SUL). (4970664)

If a user gets into the scope of any Synchronization User List (SUL) as a result of a modification (for example, SUL has a filter ‘`l=Austin`’ and user is modified to have the attribute `l` set to Austin), then Sun Java System Identity Synchronization for Windows treats this user update differently in Active Directory and Sun Java System Directory Server:

- If the user update occurred in Active Directory, then the Identity Synchronization Directory Server Connector will create the corresponding user.
- If the user update occurred in Sun Java System Directory Server, then the corresponding user is not created in Active Directory. Running `resync -c -o Sun` can help to work around this issue.

Entries that have a structural objectclass that inherit from the objectclass selected to synchronize gets synchronized too. (5046861)

For example, if the `organizationalperson` objectclass is selected, then users with the `inetorgperson` objectclass will also be synchronized because `inetorgperson` is a subclass of `organizationalperson`.

To prevent this from occurring, include a filter on the SUL that excludes the subclass:

```
(!(objectclass=inetorgperson))
```

This will normally cause a problem when using `resync` to synchronize deleted entries because subclasses will also be deleted. For example, with Active Directory the `computer` objectclass inherits from `user`, and `computer` entries might get deleted because they do not have a corresponding Directory Server entry. To prevent the `computer` entries from being synchronized include a filter on the SUL that excludes it:

```
(!(objectclass=computer))
```

Log files are not automatically removed after their expired date. (5069020)

Log files that are older than the specified number of days for removal are not removed.

Default creation attribute values could be incorrectly configured or fail validation logic. (5066657)

If a creation attribute name is the same for Directory Server and the Active Directory data source, then adding default values to one automatically adds the same defaults to the other source.

Workaround

Remove the creation attribute map and creation attributes in the console and add them again.

Before saving, do this:

If the names of the mapped attributes are the same and the syntaxes (OIDs) of the attributes is the schemas of Active Directory and Directory Server are the same:

- Ensure that default values that you add for the attributes are not the same. (Neither having a value is also going to cause this problem.)

NOTE	If the defaults are exactly the same, then this problem may not occur. If they are the same, they cannot be separated without removing and then re-adding the creation attributes and maps.
-------------	---

The `useraccountcontrol` attribute's default prevents creation of non-user Active Directory objectclass. (5043156)

Users cannot be created in Active Directory if the selected objectclass for new users does not allow the `useraccountcontrol` attribute. The `user` objectclass or any other user-derived objectclasses allow the `useraccountcontrol` attribute in Active Directory and will not be affected by this limitation.

Unable to map InetOrgperson with a extended class which has a mandatory attribute. (5091959)

For instance, an error message is displayed: 'No Sun mappings or values are specified for Active Directory attribute `mail`,' where `mail` is the mandatory attribute and `mail` is mapped to Sun's `mail` attribute.

The Identity Synchronization for Windows Installation and Configuration Guide does not mention about the Next button and the Summary pane. (5104768)

The *Identity Synchronization for Windows Installation and Configuration Guide* states at the end of each invocation, that you must exit the wizard using a Close button on the Installation Summary pane. However, the Close button option does not exist on the pane. From the Installation Summary pane, you must click the Next button which moves to a pane describing the remaining installation and configuration steps to be performed. For all non-Core installation operations, this pane has a Finished button which when clicked, exits the wizard. For Core installation, this pane has the Next button which when clicked takes you to a pane prompting whether or not you would like to start the console. From this pane, you can exit the installation program using the Finished button.

WAN support limitations. (5097751)

Identity Synchronization for Windows can be deployed in a Wide Area Network (WAN) environment with certain restrictions.

With the exception of the Directory Server plug-in, all Identity Synchronization for Windows components must be installed on the same LAN (for example, on the same machine), that is, no Message Queue traffic should travel across the WAN. These components can communicate over a WAN with Directory Servers or Active Directory domain controllers.

Performance over the WAN depends on latency and link speeds. We recommend having at least a T1 (1.544Mbps) connection and no more than 300MS latency between each connectors and the directory it manages. In a deployment where Active Directory and the Directory Server are separated by a WAN, better performance can be achieved by installing the Directory Server connector on the same LAN as the Directory Server and having the Active Directory connector communicate with Active Directory across the WAN.

Redistributable Files

Sun Java System Identity Synchronization for Windows 1 2004Q3 does not contain any files that you can redistribute.

How to Report Problems and Provide Feedback

If you have problems with Sun Java System Identity Synchronization for Windows, contact Sun customer support using one of the following mechanisms:

- Sun Software Support services online at

<http://www.sun.com/service/sunone/software>

This site has links to the Knowledge Base, Online Support Center, and ProductTracker, as well as to maintenance programs and support contact numbers.

- The telephone dispatch number associated with your maintenance contract

So that we can best assist you in resolving problems, please have the following information available when you contact support:

- Description of the problem, including the situation where the problem occurs and its impact on your operation
- Machine type, operating system version, and product version, including any patches and other software that might be affecting the problem
- Detailed steps on the methods you have used to reproduce the problem
- Any error logs or core dumps

Sun Welcomes Your Comments

Sun is interested in improving its documentation and welcomes your comments and suggestions. Use the web-based form to provide feedback to Sun:

<http://www.sun.com/hwdocs/feedback/>

Please provide the full document title and part number in the appropriate fields. The part number can be found on the title page of the book or at the top of the document, and is usually a seven or nine digit number. For example, the part number of these Identity Synchronization for Windows Version 1 2004Q3 Release Notes is 817-6202-05.

Additional Sun Resources

Useful Sun Java System information can be found at the following Internet locations:

- Documentation for Sun Java System Identity Synchronization for Windows 1 2004Q3
http://docs.sun.com/coll/S1_IdSyncForWin_1.0
- Sun Java System Documentation
<http://docs.sun.com/prod/sunone>
- Sun Java System Professional Services
<http://www.sun.com/service/sunps/sunone>
- Sun Java System Software Products and Service
<http://www.sun.com/software>
- Sun Java System Software Support Services
<http://www.sun.com/service/sunone/software>
- Sun Java System Support and Knowledge Base
<http://www.sun.com/service/support/software>
- Sun Support and Training Services
<http://training.sun.com>
- Sun Java System Consulting and Professional Services
<http://www.sun.com/service/sunps/sunone>
- Sun Java System Developer Information
<http://sunonedev.sun.com>

- **Sun Developer Support Services**
<http://www.sun.com/developers/support>
- **Sun Java System Software Training**
<http://www.sun.com/software/training>
- **Sun Software Data Sheets**
<http://www.sun.com/software>

Copyright © 2004 Sun Microsystems, Inc. All rights reserved.

Sun Microsystems, Inc. has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed at <http://www.sun.com/patents> and one or more additional patents or pending patent applications in the U.S. and in other countries.

SUN PROPRIETARY/CONFIDENTIAL.

U.S. Government Rights - Commercial software. Government users are subject to the Sun Microsystems, Inc. standard license agreement and applicable provisions of the FAR and its supplements.

Use is subject to license terms.

This distribution may include materials developed by third parties.

Portions may be derived from Berkeley BSD systems, licensed from U. of CA.

Sun, Sun Microsystems, the Sun logo, Java and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and other countries.

Copyright © 2004 Sun Microsystems, Inc. Tous droits réservés.

Sun Microsystems, Inc. détient les droits de propriété intellectuelle relatifs à la technologie incorporée dans le produit qui est décrit dans ce document. En particulier, et ce sans limitation, ces droits de propriété intellectuelle peuvent inclure un ou plus des brevets américains listés à l'adresse <http://www.sun.com/patents> et un ou les brevets supplémentaires ou les applications de brevet en attente aux Etats - Unis et dans les autres pays.

Propriété de SUN/CONFIDENTIEL.

L'utilisation est soumise aux termes du contrat de licence.

Cette distribution peut comprendre des composants développés par des tierces parties.

Des parties de ce produit pourront être dérivées des systèmes Berkeley BSD licenciés par l'Université de Californie.

Sun, Sun Microsystems, le logo Sun, Java et Solaris sont des marques de fabrique ou des marques déposées de Sun Microsystems, Inc. aux Etats-Unis et dans d'autres pays.

Toutes les marques SPARC sont utilisées sous licence et sont des marques de fabrique ou des marques déposées de SPARC International, Inc. aux Etats-Unis et dans d'autres pays.