

# Sun™ ONE Identity Synchronization for Windows 1.0 Release Notes

Version 1.0

816-6395-10

December 2003

---

These release notes contain important information available at the time of the Version 1.0 release of Sun™ Open Net Environment (Sun ONE) Identity Synchronization for Windows. New features and enhancements, known limitations and problems, technical notes, and other information are addressed here. Read this document before you begin using Sun ONE Identity Synchronization for Windows 1.0 (Identity Synchronization for Windows).

The most up-to-date version of these release notes can be found at the Sun ONE documentation web site: <http://docs.sun.com/prod/sunone>. Check the web site prior to installing and setting up your software and then periodically thereafter to view the most up-to-date release notes and manuals.

These release notes contain the following sections:

- [Revision History](#)
- [About Identity Synchronization for Windows, Version 1.0](#)
- [Identity Synchronization for Windows](#)
- [Accessing the Product Documentation](#)
- [Hardware and Software Requirements](#)
- [New Information](#)
- [Known Issues](#)
- [How to Report Problems and Provide Feedback](#)
- [Additional Sun Resources](#)

---

# Revision History

**Table 1**    Revision History

Date	Description of Changes
December 2003	Initial product release.
November 14, 2003	Reorganized and edited text, added new information
October 17, 2003	Reformatted with new templates, reorganized information, bug updates
September 25, 2003	Beta 2 release.
March 23, 2003	Initial Beta release.

---

---

## About Identity Synchronization for Windows, Version 1.0

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

- Sun™ ONE Directory Server and Windows 2000 Active Directory
- Sun ONE Directory Server and Windows NT SAM Registry

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

---

# Identity Synchronization for Windows

Features provided in this initial release of Identity Synchronization for Windows include:

- Supports both the 32-bit and 64-bit versions of Directory Server on Solaris.
- Supports Multi-Master Directory Server deployments and has enhanced SSL configuration features.
- Includes the `idsync` command line utility, which incorporates several command line utilities that are run as subcommands.
- Requires a configuration password, which protects sensitive information such as credentials and encryption keys while they are stored in Directory Server and in-transit over the network.
- Includes enhanced support for deployments with multiple Windows domains. For more information, refer to the *Sun™ ONE Identity Synchronization for Windows Installation and Configuration Guide*.

---

## Accessing the Product Documentation

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
```

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.

# Hardware and Software Requirements

The following hardware and software are required for this release of Identity Synchronization for Windows.

**Table 2** Hardware and Software Requirements

Component	Solaris Requirement	Windows Requirement
Core	Solaris 8™ for UltraSPARC® (32-bit and 64-bit)	Windows 2000 Server SP4
	Solaris 9™ SPARC® Platform Edition (32-bit and 64-bit)	Windows 2000 Advanced Server SP4
Sun ONE Directory Server and Active Directory connectors	Solaris 8 for UltraSPARC (32-bit and 64-bit)	Windows 2000 Server SP4
	Solaris 9 for SPARC platforms (32-bit and 64-bit)	Windows 2000 Advanced Server SP 4
Sun ONE Directory Server plug-in	Solaris 8 for UltraSPARC (32-bit and 64-bit)	Windows 2000 Server SP4
	Solaris 9 for SPARC platforms (32-bit and 64-bit)	Windows 2000 Advanced Server SP 4
NT connectors and plug-ins (subcomponents)		Windows Primary Domain Controller NT 4.0 Server SP 6A (x86 only)

NOTES

A Java Runtime Environment (JRE) is not provided with this product. You must install JRE 1.4.1\_03 (or later) to run the Identity Synchronization for Windows installer.

You must install Directory Server version 5.2 for the Directory Server plug-in (subcomponent).

If you want to install the Identity Synchronization for Windows core on an existing Sun™ ONE Message Queue installation, you must be using Sun ONE Message Queue (Message Queue) version 3.0.1 SP2 (or later). Using an improper version of Message Queue will cause synchronization failures.

---

# New Information

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

- [Installation Notes](#)
- [Compatibility Issues](#)
- [Running Identity Synchronization for Windows in a Firewalled Environment](#)

## Installation Notes

Before installing Identity Synchronization for Windows 1.0, be sure to read the “Preparing for Installation” chapter provided in the *Sun™ ONE Identity Synchronization for Windows 1.0 Installation and Configuration Guide*.

## Compatibility Issues

An incompatibility exists between Directory Server 5.2 and Identity Synchronization for Windows 1.0. You must install Windows 2000 SP 4 to run Identity Synchronization for Windows components, but this service pack does not support Directory Server 5.2.

---

<b>NOTE</b>	This compatibility issue only applies to configurations where Directory Server 5.2 is running on Windows 2000 and Directory Server is the source for user synchronizations.
-------------	---

---

For more information, and a workaround, see [Compatibility issue between Identity Synchronization for Windows 1.0 and Sun ONE Directory Server 5.2 on Windows 2000 SP4. \(4943652\)](#) on page 20.

# 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™ ONE 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 ONE 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

This section describes known issues in Identity Synchronization for Windows 1.0 and their workarounds.

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

## Installation and Uninstallation

**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.
- The `/etc/imq/passfile` file was modified to include the configuration registry password, which prevented clients of other broker instances from using this passfile for LDAP authentication. You must create separate passfiles for all conflicting broker instances.
- A keystore for the broker was created, which affected other broker instances that used a pre-existing keystore.



**Installing core with an existing Message Queue instance on a port other than 7676. (4881466)**

You cannot change the port number in the installer because the option is greyed out. (*Solaris only*)

**Workaround**

To change the port number,

1. Modify the `/usr/share/lib/imq/props/broker/default.properties` file prior to running the core installer.
2. Set the `imq.portmapper.port` property to the port where the private Message Queue broker instance is to run.

---

**NOTE** Identity Synchronization for Windows does not use an existing Message Queue broker instance. The software reuses Message Queue bits but creates a private broker instance.

---

**Uninstaller does not remove all files and folders. (4829497)**

The Identity Synchronization for Windows uninstaller does not remove all files and folders.

**Workaround**

After uninstalling Identity Synchronization for Windows, reboot the machine. Check the following directories under the installation home and manually remove any remaining files or folders:

- `imq` directory
- `log` directories (if Directory Server plug-ins (subcomponents) or NT plug-ins were installed)
- `lib` directory

**On Windows only, you must reboot the machine before reinstalling core. (4820869)**

If you install and then uninstall core on a machine, you must reboot before attempting to reinstall core on the machine again. The reinstaller displays a dialog to remind you to reboot the machine.

**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.

**Duplicate Directory Server plug-in IDs are generated for replicas installed on the same server root. (4916789)**

When you install Directory Server plug-ins (subcomponents) on multiple replicas that all reside in the same server-root, log files for each plug-in will be generated in a common directory. This condition can make it difficult for engineers and customers to analyze plug-in log files.

**Workaround**

Use the following procedure to change the logging directory for each plug-in:

1. Create the log directory. (Sun recommends using *<Identity Synchronization Installation Root>/logs/<SUBC\_ID>/<replica\_instance\_name>*.)
2. Open the Directory Server console and click on the Directory tab.
3. Open the *cn=config, cn=pswsync, cn=plugins, cn=config* entry.
4. Change the *logDirectory* attribute value to the directory you created in step 1, and then click OK.
5. Restart Directory Server.

**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 *pswsync* and uncheck the *Enable plugin* checkbox.
5. Restart Directory Server.

# 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 ONE 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

## 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 AD sources.

### *Workaround*

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

**Console does not support SSL-only directory servers. (4918013)**

The console will not detect servers operating in SSL-only mode. Servers involved in synchronization must listen on a non-SSL port or listen on both SSL and non-SSL ports. This problem does not apply to servers that were configured exclusively through the Sun ONE Directory Server Console.

**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).

## Password Synchronization

**Password changes on NT might be lost during connector reset or when the connector is down. (4822655)**

Password changes on NT can be lost during a connector reset or while the connector is down. Consequently, passwords can get out-of-sync between Directory Server and Windows NT.

*Workaround*

After starting synchronization in a Windows NT environment, do not stop it. Also, do not stop the Identity Synchronization for Windows service where the NT connector is installed.

**Password policy issues. (4834865 and 4811572)**

Identity Synchronization for Windows does not support password synchronization between directory services that have incompatible password policies because Identity Synchronization for Windows does not map one directory's password policy to another.

It is possible for password policies used on different systems to cause synchronization errors between incompatible hosts. Examples include password length and minimum maximum required characters. Administrators must change the incompatible password policy manually to match that of other systems. Password history is kept in Directory Server.

**Users can change passwords using clear text password values only. (4807342)**

You can change passwords using clear text password values only. Identity Synchronization for Windows does not support setting passwords to prehashed values.

### **Possible misuse of dspassword. (4878012)**

Both the Identity Synchronization for Windows plug in and the Directory Server connector use the dspassword attribute to store the reversible encrypted password temporarily.

The Identity Synchronization for Windows plug-in adds or removes this attribute whenever a user's password has to be changed. Next, Directory Server evaluates whether to make the password change; however, due to limitations in the Directory Server access control model, it is possible for a user to change only the dspassword attribute without changing his password.

This situation does not cause any problems in the Directory Server connector because the connector checks to see if the credential seen in the Retro Change Log (1) can be decrypted and (2) validated, but it is still possible for any user to manipulate the dspassword attribute.

Administrators must ensure that write access is the same for the userpassword attribute and the dspassword attribute, or the system may reject valid password changes.

### **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 AD 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.

**idsync resync can fail to create users from Directory Server to NT. (4845844)**

Passwords are not propagated when you resynchronize users from Directory Servers to Windows NT. Consequently, the NT connector will not receive the password attribute for each of the resynchronized users and, in this case, the NT connector will not assign a password value. However, certain users may not synchronize because this may not satisfy the minimum password length policy.

**Workaround**

To resynchronize all of the users, you must permit blank passwords.

**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 login," the password change will not be synchronized to Directory Server until the user logs on and changes their password.

A user bind will fail to log in 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 login" 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.

# Sun ONE 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:

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

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 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 `imqsvcadmin 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 `imqsvcadm query` command issued earlier. For example:

```
imqsvcadm 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`.
  - To increase the memory to 2 GB, use `-vmargs -Xmx1024m'`.
7. Use the Windows Services Management console to start the Message Queue broker service.

#### **On Solaris, you cannot use an existing Message Queue installed in a user directory. (4881240)**

The Message Queue installation that is bundled with the installer always mandates the installation location. If you try to use an existing Message Queue installed in a different directory, Message Queue will not work because the Identity Synchronization for Windows installer always looks for files under hard-coded directories. For example, it always looks for the `accesscontrol.properties` file under `"/etc/imq/"` on Solaris.

#### **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 does not support using Message Queue on a computer where core is not installed.

## 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 make or modify replication agreements *before* you install Identity Synchronization for Windows.

If you install the configuration directory and the primary Directory Server source on the same Directory Server on the same machine, the configuration data and the source data will be located under the same suffix (for example, `dc=example,dc=com`). With this configuration, when you create a Replication Agreement *after* installing Identity Synchronization for Windows, the object classes created by the Identity Synchronization for Windows core installation will be deleted and 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 in `idsync linkusers` should be indexed in Directory Server. (4814412)**

`idsync linkusers` searches Directory Server for users that match Active Directory/NT users. Every Directory Server attribute used in an `idsync linkusers` operation should be indexed for equality.

**Identity Synchronization for Windows 1.0 only supports a single Active Directory forest. (4901486)**

Identity Synchronization for Windows does not support domains in multiple Active Directory forests. The product supports domains in a single forest only.

**Identity Synchronization for Windows does not synchronize user deletions. (no bug number)**

Identity Synchronization for Windows supports synchronizing user creations and modifications between Active Directory, Windows NT, and Directory Server, but it does not synchronize entry deletion. User entries deleted in any of these directory sources will not be deleted in the corresponding remote directory source.

**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 ONE Directory Server.

If an administrator disables an AD account, they also must change the password if they want the user to be locked-out of Directory Server.

## Compatibility issue between Identity Synchronization for Windows 1.0 and Sun ONE Directory Server 5.2 on Windows 2000 SP4. (4943652)

---

**NOTE** This issue only applies to configurations running Sun ONE Directory Server 5.2 on Windows 2000 where Directory Server will be the source for user synchronizations.

---

An incompatibility exists between Identity Synchronization for Windows 1.0 and Directory Server 5.2. Identity Synchronization for Windows requires you to install Windows 2000 service pack 4, but the service pack does not support Directory Server 5.2.

### *Workaround:*

Sun recommends having two separate systems running Windows 2000:

1. On one system, use Directory Server 5.2 on a separate Windows 2000 SP3, which can be used for user synchronization.
2. On an another system running Windows 2000 SP 4, install Identity Synchronization for Windows core and a connector for Directory Server.

## Changing the configuration directory port. (4941271)

If you change the port for a Sun ONE 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 `<installroot>\imq\var\instances\psw-broker\props\config.properties`.  
For example, `imq.user_repository.ldap.server=<host>\:<port>`
2. Modify the port in `<installroot>\resources\SystemManagerBootParams.cfg`  
For example, `<Parameter name="manager.configReg.hostPort" value="<port>" />`
3. Reboot (Windows) or restart the Message Queue broker and System Manager on Solaris.

## Unlike multi-valued attributes are not supported in release 1.0. (4807260)

Identity Synchronization for Windows 1.0 supports synchronizing multi-valued attributes with a few restrictions. The values in a multi-valued attribute are 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. That is, the values of the corresponding remote attribute will be set to these five values.

Synchronizing multi-valued attributes has the following caveats:

- 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, 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.

**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.

**userpassword must be an optional attribute. (4943564 and 4939730)**

If you configure Identity Synchronization for Windows to use a user-defined objectclass from a Sun ONE Directory Server schema, the userpassword attribute must be *optional* or Identity Synchronization for Windows will not work properly.

**No error message from plug-in when Secure Sockets Layer certificate is not trusted. (4924027 and 4904705)**

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 ONE Directory Server should include all attributes in Synchronized Users List filters. (4900568)**

If you are synchronizing creates from Sun ONE 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.

**Attribute modification lost after losing connectivity to Active Directory. (4893525)**

Attribute modifications may fail to synchronize to Active Directory (AD) if the entry was being processed as a user creation when the AD network interface became disabled.

**Workaround:**

If you see an error similar to the following, you can use `idsync linkusers` to manually link the user from AD to Directory Server.

```
audit.log:[21/Jul/2003:10:10:55.906 -0500] SEVERE 18 CNN101 qa19 "Unable to create
user "cn=BDSAD-3408-0557,cn=users,dc=qa21,dc=com" at ldaps://qa21.qa21.com:636. LDAP
add operation failed. Error code: 68, reason: 00000524: UpdErr: DSID-031A0AE5,
problem 6005 (ENTRY_EXISTS), data 0
```

**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.

**Using the command line to import the Configuration XML file sets displayName as Directory. (4821768 and 4812964)**

You must use an accurate display name in `idsync importcnf.cfg` files. The `displayName` attribute on `SynchronizationHost` in the `idsync importcnf` file must be the database suffix for Directory Server, the domain name for Active Directory, and the NETBIOS domain name for Windows NT.

If you use the console user interface to import Identity Synchronization for Windows configuration sets, the interface forces you to specify a domain name as the directory source name, but importing through the command line does not.

When you import configuration sets through the command line, the directory source name will be set to the *directory* (for example, `<SunDirectory Source displayName="DS">`). Consequently, you must be sure to specify a *domain name* as the `displayName`.

**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 1.0 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:

- `isw-<machine-name>/logs/`
- `$HOME/.mcc`



**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.

---

## How to Report Problems and Provide Feedback

If you have problems with Sun ONE 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

To assist in reporting problems, Sun provides the `capture_environment.pl` tool, a Perl script that captures the current Identity Synchronization for Windows environment, including the `ics.conf` file, log files, calendar database files, platform information, and core files (if available). These files can be useful to Identity Synchronization for Windows development to debug problems.

**To run the `capture_environment.pl` tool:**

1. If necessary, download the `capture_environment.pl` tool from customer support.
2. If necessary, install Perl and add it to your path. (If you cannot install Perl, see the instructions in the `capture_environment.pl` file that describe how to manually create a snapshot of your Identity Synchronization for Windows environment.)
3. Login (or become) `root` on UNIX systems or an Administrator on Windows 2000 systems.
4. Run the `capture_environment.pl` tool. The tool copies the files to a directory named `archive_directory`. On UNIX systems, it places all files into a tar file named `tar_file`. On Windows 2000 systems, however, you must manually add the files in `archive_directory` to a Zip file.
5. Send the `tar_file` or Zip file to customer support.

## Sun Welcomes Your Comments

Sun is interested in improving its documentation and welcomes your comments and suggestions. Email your comments to Sun at this address:

[docfeedback@sun.com](mailto:docfeedback@sun.com)

Please include the part number (816-6395-10) and the full title of the document (*Identity Synchronization for Windows 1.0 Release Notes*) in the subject line of your email.

---

# Additional Sun Resources

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

- **Documentation for Sun ONE Identity Synchronization for Windows**  
[http://docs.sun.com/coll/S1\\_IdSyncForWin\\_1.0](http://docs.sun.com/coll/S1_IdSyncForWin_1.0)
- **Sun ONE Documentation**  
<http://docs.sun.com/prod/sunone>
- **Sun ONE Professional Services**  
<http://www.sun.com/service/sunps/sunone>
- **Sun ONE Software Products and Service**  
<http://www.sun.com/software>
- **Sun ONE Software Support Services**  
<http://www.sun.com/service/sunone/software>
- **Sun ONE Support and Knowledge Base**  
<http://www.sun.com/service/support/software>
- **Sun Support and Training Services**  
<http://www.sun.com/supporttraining>
- **Sun ONE Consulting and Professional Services**  
<http://www.sun.com/service/sunps/sunone>
- **Sun ONE Developer Information**  
<http://sunonedev.sun.com>
- **Sun Developer Support Services**  
<http://www.sun.com/developers/support>
- **Sun ONE Software Training**  
<http://www.sun.com/software/training>
- **Sun Software Data Sheets**  
<http://www.sun.com/software>

---

Copyright © 2003 Sun Microsystems, Inc. All rights reserved.

Sun, Sun Microsystems, the Sun logo, Solaris, Java and the Java Coffee Cup logo are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries. Use of Identity Synchronization for Windows is subject to the terms described in the license agreement accompanying it.

