Sun ONE™ Identity Synchronization for Windows Release Notes

Version *1.0 SP1*

Part Number 817-6262

These release notes contain important information available at the time of the release of Sun ONE™ Identity Synchronization for Windows Version 1.0 SP1. 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 Version 1.0 SP1 (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 product documentation.

These release notes contain the following sections:

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
June 21, 2004	Minor corrections to content. Added note to “Installing the Service Pack” and removed reference to Calendar Server tool in “How to Report Problems and Provide Feedback” section.
April 26, 2004	Initial version of these Service Pack 1 release notes.

About Identity Synchronization for Windows, Version 1.0 SP1

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

- Sun Java™ System Directory Server 5.2 and Windows 2000/2003 Active Directory
- Sun Java™ System Directory Server 5.2 and Windows NT SAM Registry

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

NOTE Identity Synchronization for Windows 1.0 SP1 supports synchronization with the Windows 2003 platform, but *cannot be installed on* a Windows 2003 server (see “Known Issues and Limitations” on page 44). Active Directory connectors and subcomponents must be installed on Solaris or on Windows 2000 Server or Advanced Server.

For more information about synchronizing with Active Directory, refer to the *Sun ONE Identity Synchronization for Windows 1.0 Installation and Configuration Guide.*

This section includes:

What's New in This Release

Identity Synchronization for Windows 1.0 SP1 is provided to fix several known product issues. For a detailed description of these issues, see "Bugs Fixed in This Release" on page 5.

This service pack does not contain any new features or performance enhancements.

Hardware and Software Requirements

The hardware requirements for this release of Identity Synchronization for Windows are as follows:

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

The operating system requirements are provided in the following tables:

Table 2 Solaris Operating System Requirements

Component	Solaris Requirement
Core	Solaris 8™ for UltraSPARC® (32-bit and 64-bit) Solaris 9™ SPARC® Platform Edition (32-bit and 64-bit)
Sun Java™ System Directory Server connectors and Active Directory connectors	Solaris 8 for UltraSPARC (32-bit and 64-bit) Solaris 9 for SPARC platforms (32-bit and 64-bit)
Sun Java™ System Directory Server plugin	Solaris 8 for UltraSPARC (32-bit and 64-bit) Solaris 9 for SPARC platforms (32-bit and 64-bit)

Table 3 Windows Operating System Requirements

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

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 plugin (subcomponent).

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

Synchronizing with Active Directory on Windows 2003

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

- You cannot install any of the Identity Synchronization for Windows components on a Windows 2003 operating system.
- You must install an Active Directory connector using the Identity Synchronization for Windows graphical user interface-based (GUI) installer.

NOTE Active Directory connectors will work with Active Directory on Windows 2003.

- You use the same procedures to create directory sources, global catalogs, and synchronization scopes for Windows 2003 that you used for Active Directory on Windows 2000.
- You must install the Active Directory Certificate manually for each Active Directory connector synchronizing a source on Windows 2003. Use the instructions provided in the "Retrieving the Active Directory CA Certificate Using certutil" section of the "Configuring Security" chapter in the *Sun ONE Identity Synchronization for Windows Version 1.0 Installation and Configuration Guide.*
- On Windows 2003, the default password policy enforces strict passwords, which is not the default password policy on Windows 2000.

NOTE If you do not have to enforce password policies, instructions for disabling the Windows 2003 password policy are provided in "Changing Password Policies on Active Directory" on page 24.

If you enforce password policies on Windows or on Directory Server, read the information provided in "Compatibility Issues: Password Policies" on page 15 to understand how password policies can affect synchronization results between Active Directory and Directory Server.

Bugs Fixed in This Release

The following table describes the bugs fixed in Identity Synchronization for Windows 1.0 SP1:

Table 4 Bugs Fixed in This Release

Bug Number	Description
4995351	Identity Synchronization for Windows maps wrong attribute
4987742	`resync` misses entries due to race condition
4939484	`linkusers` command may never exit

Identity Synchronization for Windows maps wrong attribute. (*4995351*)

This service pack corrects a problem that occurred when like values were not mapped to each other, such as `cn <--> displayname` and `uid <--> cn`.

The following example illustrates this problem:

Active Directory		Directory Server
displayName	<-->	cn
cn	<-->	uid

This problem occurred when you transferred attributes from Active Directory to Directory Server. The mappings would become mismatched so the `displayname` would be mapped to `uid` instead of the stated `cn` attribute.

`resync` can miss entries due to race condition. (*4987742*)

This service pack corrects a situation in which the `resync` source connector was occasionally sending refresh actions before the destination connector was ready to receive them, which was causing the first few entries to be missed.

`linkusers` command may never exit. (*4939484*)

This service pack fixes the `linkusers` command so it exits appropriately.

Important Information

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

Installing the Service Pack

This section explains how to install Identity Synchronization for Windows1.0 SP1. The information is organized into the following sections:

NOTE Before installing Identity Synchronization for Windows 1.0 SP1, be sure to read the "Preparing for Installation" chapter in the *Sun ONE™ Identity Synchronization for Windows 1.0 Installation and Configuration Guide*.

References to *core* or *instance* within this publication should be understood to mean *Identity Synchronization for Windows core* and *Identity Synchronization for Windows instance* — unless specifically indicated otherwise within the text.

An *instance* is any machine on which an Identity Synchronization for Windows connector or subcomponent (plugin) is installed.

NOTE *Identity Synchronization for Windows 1.0 SP1 is a binary patch and does not provide any installation capabilities.* You must be sure to install the core, any connectors, and subcomponents using the version 1.0 binaries before you follow the 1.0 SP1 installation instructions provided in this section.

If you install additional connectors or subcomponents to an existing 1.0 SP1 deployment, you will have to repeat the 1.0 SP1 installation steps for the newly added components only.

Overview

For this service pack, each installation must have one (or can have a combination of two) of the following sections (core and/or instance), where each section refers to a specific part of the deployed file system's topology:

- **The <*core*> section** is subordinate to a <*server_root*> and can exist in one location only:
  - **On Windows**: The default <*server_root*> is `C:\Program Files\Sun\MPS`
  - **On Solaris**: The default <*server_root*> is `/var/Sun/mps`

  The easiest way to find the precise location of the <*core*> section is to use the system Console.

When you start the Console and select the Identity Synchronization for Windows (isw-<*hostname*>) task, the associated panel reveals the <*core*> section's "server root." In addition, the <*core*> section's host name will be shown in the task name (which is the text to the right of the literal beginning with "isw-"). You deploy (tar or unzip) the service pack's core file on the core machine, within its <*server_root*> file system.

- **The <*instance*> section** also is subordinate to the <*server_root*> but, unlike the <core> section, the <instance> section can exist on multiple machines.
  - **On Windows**: C:\Program Files\Sun\MPS\
  - **On Solaris**: /var/Sun/mps/

  It is important to recognize that Identity Synchronization for Windows 1.0 SP1 packaging processes *do not know* the <*instance*> name.

  For example, if a machine named dirserver.example.com possessed an installed instance of Identity Synchronization for Windows, a path named <*server_root*>/isw-dirserver (where dirserver.sun is the instance directory under <*server_root*>) would exist in the dirserver.example.com's file system. This area of the file system is called (collectively) the installation's <*instance*> directory. The <*instance*> directory must be the current working directory when you deploy (tar or unzip) the service pack's instance files.

Installing the Software

Use the following procedure to install Identity Synchronization for Windows 1.0 SP1:

1. Download the Identity Synchronization for Windows service pack (into a temporary location) from:

   http://www.sun.com/software/download/inter_ecom.html

2. Unpack the patch file as follows:
   - **On Windows**: unzip IdentitySyncForWindows_1.0_SP1-Windows.zip
   - **On Solaris**: tar -xvf IdentitySyncForWindows_1.0_SP1-Solaris.tar

   The patch file contents will be unpacked into a subdirectory called idsync_1.0_sp1, which will be created in the location where you unpacked the file. (See Table 5 and Table 6 for a list of the patch file contents provided in the zip and tar files, respectively.)

NOTE The following files are common to all zip / tar files:

```
COPYRIGHT.txt
INSTALL.txt
LICENSE.txt
README.txt
THIRDPARTYLICENSEREADME.txt
```

Table 5 Windows Patch Files in IdentitySyncForWindows_1.0_SP1-Windows.zip

IdentitySyncForWindows_1.0_SP1-Windows.core.zip	IdentitySyncForWindows_1.0_SP1-Windows.instance.zip
isw-server2004.100.1537.jar isw2004.100.1537.jar isw2004.100.1537_en.jar	common.jar connector.jar install.jar manager.jar registry.jar setBuild.jar ui.jar watchdog.jar

Table 6 Solaris Patch Files (IdentitySyncForWindows_1.0_SP1-Solaris.tar)

IdentitySyncForWindows_1.0_SP1-Solaris.core.tar	IdentitySyncForWindows_1.0_SP1-Solaris.instance.tar
• **In the bin/isw/admin/servlets/ directory**: isw-server2004.100.1537.jar • **In the java/jars/ directory**: isw2004.100.1537.jar isw2004.100.1537_en.jar	**In the lib/ directory**: common.jar connector.jar install.jar manager.jar registry.jar setBuild.jar ui.jar watchdog.jar

3. Check one level below the *<server_root>* and verify that all of the files unpacked successfully (compare to the listings in Table 5 and Table 6).

4. Stop synchronization using one of the following methods.

   - **On Windows**: From the Identity Synchronization for Windows Console, select the Status tab and click the Stop Synchronization Task button. Close the Console.
   - **On Solaris**: From the command line, type

     `/var/Sun/mps/isw-<instance>/bin/idsync stop`

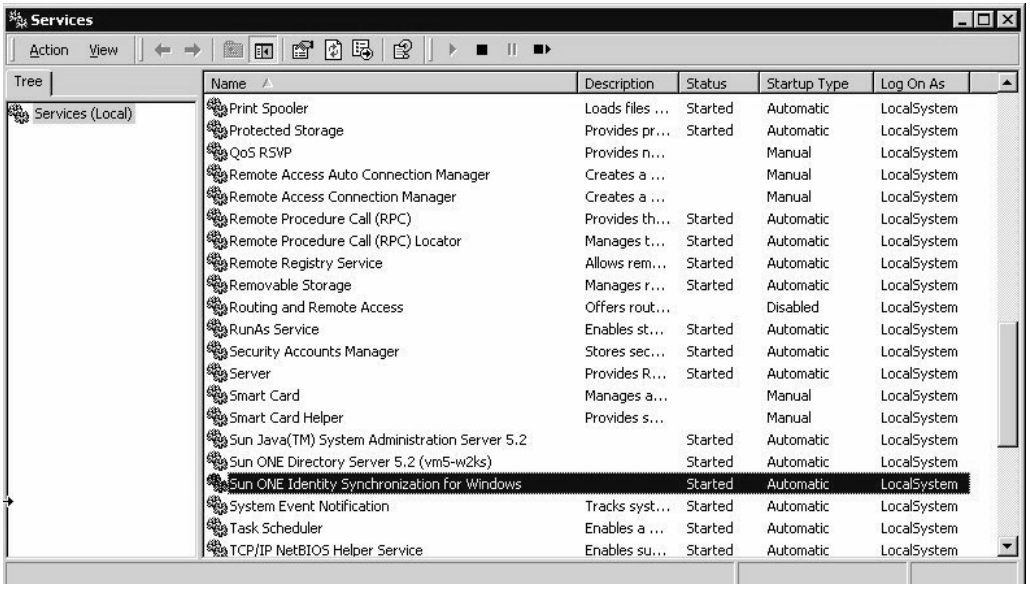
5. Stop all services (daemons) on each machine in your deployment topology (Active Directory, NT, and Solaris) as follows:

   - **On Windows**: Select Start -> Settings -> Control Panel -> Administrative Tools -> Services to open the Services dialog box. Select Sun ONE Identity Synchronization for Windows from the list and click the Stop icon on the toolbar to stop all corresponding services. (See Figure 1.)
   - **On Solaris**: From the command line, type the following command to stop the system manager:

     `/etc/init.d/isw stop`

NOTE Remember, it is possible to have services started but not engaged.

Figure 1 Services Dialog Box



6. Use the `db2ldiff` utility to backup the existing configuration directory and all file systems on which you have Identity Synchronization for Windows installed.

   NOTE For detailed information about the `db2ldiff` utility, refer to Chapter 4 of the *Sun ONE Directory Server 5.2 Administration Guide.*

   This service pack and the `setBuild` utility both make changes to the configuration directory during installation, so be sure to backup and preserve your current configuration.

   If you need to revert the system's state to its condition prior to the service pack installation, perform the following backups before you proceed to the next step:

   - Backup the contents of the Identity Synchronization for Windows configuration directory. Be sure to include `o=NetscapeRoot` and the `ou=services,<SUL suffix>` of the managed Synchronized Users List(s).
   - Backup the Sun ONE Directory Server and Windows Active Directory and / or NT SAM Registry.
   - Backup all files that reside at the core's `<server-root>`.
   - Backup all files that reside at every instance root.

7. For the installation where core is installed, deploy the core zip (or tar) file from the current working directory (core's `<server_root>`) using one of the following methods:

   - **On Windows**:

     ```
     cd C:\Program Files\Sun\MPS
     unzip <path_to_idsync_1.0_sp1>\IdentitySyncForWindows_1.0_SP1-Windows.core.zip
     ```

     NOTE If you use a zip utility, unzip the Windows core files into the `<server_root>` directory for that system.

   - **On Solaris**:

     ```
     cd /var/Sun/mps/
     tar -xvf <path_to_idsync_1.0_sp1>/IdentitySyncForWindows_1.0_SP1-Solaris.core.tar
     ```

     If you are asked whether to replace all files, select Yes to All to extract the service pack files and place them under `/var/Sun/mps//isw-<hostname>`. (See "Solaris Patch Files (`IdentitySyncForWindows_1.0_SP1-Solaris.tar`)" on page 9 for more information.)

8. For all other instance installations (*any machine on which Identity Synchronization for Windows connectors or subcomponents are installed*), deploy the instance zip (or tar) file only from the instance working directory (<*server_root*>/isw-<*hostname*>) using one of the following methods:

   - **On Windows**:

     ```
     cd C:\Program Files\Sun\MPS\isw-<hostname>
     unzip <path_to_idsync_1.0_sp1>\IdentitySyncForWindows_1.0_SP1-Windows.instance.zip
     ```

     NOTE If you use a zip utility, unzip the Windows core files into the <*server_root*>/isw-<*hostname*> directory for that system.

   - **On Solaris**:

     ```
     cd /var/Sun/mps/isw-<hostname>
     tar -xvf <path_to_idsync_1.0_sp1>/IdentitySyncForWindows_1.0_SP1-Solaris.instance.tar
     ```

   If you are asked whether to replace all files, select Yes to All.

You are now ready to run the setBuild utility. Continue to the next section for instructions.

Using the setBuild Utility

After installing the Identity Synchronization for Windows 1.0 SP1 files, you must modify the system's configuration so it will start using the new files. Some of these files employ a naming nomenclature that embeds a build number into the file name. You use the setBuild command line utility to tell the synchronization system to start using the newer versioned files. The utility locates the new files and subsequently changes the configuration to reflect those new names.

Because the setBuild utility modifies the configuration, the utility requires credentials that permit you to modify the configuration registry. Generally, these credentials are the same credentials used to configure the system through the GUI (such as the credentials specified to start the Console). In addition, you must tell the utility where the configuration registry resides. For example,

```
ou=services, o=example.com
```

NOTE You must run the setBuild utility from the server that hosts the Identity Synchronization for Windows' core and you must start the configuration directory server.

1. Run the `setBuild` command as follows:

   ```
   cd isw-<hostname>/lib
   java -jar setBuild.jar -h <hostname> -D <bind dn> -w <password>
                          [-p <port number> [-v]
                          [-x <localInstanceHostname>]
   ```

   Where:

-h	Specifies the hostname of the machine that possesses the configuration registry.
-D	Specifies the `bind as` dn to use when connecting.
-w	Specifies which password to use when binding. **Note**: Specifying the "`-`" value (without the quotes) tells the `setBuild` utility to solicit the password from "standard in," once the routine begins executing. Avoid entering a password directly on the command line because you cannot prevent someone from discovering the password's value. It would be easy for someone to inspect the your command history or use a "`ps`" type command to view running processes and their associated parameters.
-p	Specifies the port number on which to reach the configuration repository. If you omit the `-p` option, the command line utility assumes that it should connect to the configuration repository using the default LDAP port (389).
-v	Informs the command line utility to be verbose in its interaction and reporting. This additional information can help you determine the cause of any failure encountered by the utility.
-x	Helps the utility determine the value of the local instance host's name. In most cases, the utility can resolve the local host's name on its own, but the `setBuild` utility's methods cannot determine the instance name 100 percent of the time (especially when the local instance host is known/reachable under multiple IP addresses). If you use this parameter to specify the instance host's name, the utility will not attempt to guess (possibly erroneously) the instance host's name.

2. If prompted, provide the Directory Manager or Administrative password.
3. Restart the Admin Server on the core machine.
4. To start services (daemons), use one of the following methods:
   - **For Windows**: Return to the Services dialog (Select Start -> Settings -> Control Panel -> Administrative Tools -> Services) and start services on all of the instance machines.
   - **For Solaris**: When services are running on all instance machines, then you can start services on the core machine(s). (Usually done by typing **`/etc/initial/isw start`** or from the Services dialog box.)

5. To verify a successful installation, open the Identity Synchronization for Windows Console. From the Console tree, select Identity Synchronization for Windows, click the Open button, and log in.

   From this point, you should see that the product's version title now contains the SP1 suffix.

6. Select the Tasks tab and click Start Synchronization Task.

7. Select the Status tab and check the logs to verify that synchronization is working properly.

Uninstalling the Service Pack

If necessary, you can use the following procedure to remove this service pack from a machine:

1. Stop synchronization. (See Step 4 on page 10.)

2. Stop all services (daemons). (See Step 5 on page 10.)

3. Restore the back-ups you made of the file system during the service pack installation process onto the core machine.

4. Restore the configuration repository from the back-up you made during the installation process.

5. Restart all services (daemons). (See Step 4 on page 13.)

6. Verify the version number in the Identity Synchronization for Windows Console.

7. Restart synchronization. (See Step 6 on page 14.)

Compatibility Issues: Password Policies

As mentioned previously, the default password policy on Windows 2003 has been changed to enforce strict passwords by default, which was not the default for Windows 2000.

Identity Synchronization for Windows services must occasionally create entries that do not require passwords. Consequently, if you have password policies enabled on Active Directory (on Windows 2003 or 2000) or on Directory Server, user creation errors can result.

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

This section is organized as follows:

- "Enforcing Password Policies" on page 15: If you must enforce password policies on Windows or on Directory Server, read the information provided in this section to understand how password policies can affect synchronization results between Active Directory and Directory Server.
- "Changing Password Policies on Active Directory" on page 24: If you do not have to enforce password policies, skip to this section for the instructions you need to disable the Windows 2003 default password policy.

Enforcing Password Policies

This section explains how the password policies for Active Directory on Windows 2003, Windows 2000, and Sun ONE Directory Server version 5.2 can affect synchronization results.

The information is organized as follows:

Overview

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

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

The next three sections contain tables that describe some different scenarios you might encounter. You can use this information as a guideline to help ensure that passwords will remain synchronized. (These tables do not attempt to describe all possible configuration scenarios because system configurations differ.)

NOTE For more information about password policies for Windows 2003, go to `http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/deployguide/en-us/dsscc_aut_xbby.asp`

For more information about password policies for Directory Server 5.2, go to `http://docs.sun.com/source/816-6698-10/useracct.html`

Enforcing Password Policies on Active Directory Only

Table 7 describes different scenarios for an Active Directory only password policy using the following specifications:

- Enforce Password History: 20
- Max Password Age: 30
- Min Password Age: 0
- Min Password Length: 7
- Passwords must meet complexity requirements: Enabled

Table 7 Example Scenarios: Password Policy on Active Directory Only

Scenario (Based on Direction of Flow)	Password Meets Policy Requirements	Results
From Active Directory to Directory Server	Yes	Users are created on Active Directory and Directory Server, and link properly.
From Active Directory to Directory Server	No	Users are created on Directory Server but cannot be created on Active Directory. Users are not linked. See "Important Notes" on page 22 for more information.
From Active Directory to Directory Server during `idsync resync -c -i NEW_USERS`	Not Applicable	Users that exist on Active Directory are created on Directory Server and the passwords are invalidated to force on-demand synchronization. The user passwords will be updated in Directory Server the next time those users log into Directory Server.
From Directory Server to Active Directory	Yes	Users are created on Directory Server and Active Directory, and link properly.
From Directory Server to Active Directory	No	Users are created on Directory Server but cannot be created on Active Directory.
From Directory Server to Active Directory during `idsync resync -c`	Not Applicable	Users that exist on Directory Server cannot be created on Active Directory because the entries do not contain a password. To create users, the entries must contain passwords and the passwords must meet the Active Directory password policy. See "Important Notes" on page 22 for more information.

Enforcing Password Policies on Active Directory and Directory Server

Table 8 describes different scenarios for Active Directory and Directory Server password policy examples using the following specifications:

- **For Active Directory**:
  - Enforce Password History: 20
  - Max Password Age: 30
  - Min Password Age: 0
  - Min Password Length: 7
  - Passwords must meet complexity requirements: Enabled

- **For Directory Server**:
  - User must change password after reset
  - User May Change Password
  - Keep 20 passwords in history
  - Password expires in 30 days
  - Send warning 5 days before password expires
  - Check password syntax: Password min length is 7

Table 8 Example Scenarios: Password Policy on Active Directory and Directory Server

Scenario (Based on Direction of Flow)	Password Meets Policy Requirements	Results
From Active Directory to Directory Server	Yes	Users are created on Active Directory and Directory Server, and link properly.
From Active Directory to Directory Server	No	Users are created on Directory Server with no password but cannot be created on Active Directory. Users are not linked. See "Important Notes" on page 22 for more information.
From Active Directory to Directory Server during `idsync resync -c -i NEW_USERS`	Not Applicable	Users that exist on Active Directory are created in Directory Server and the passwords are invalidated to force on-demand synchronization. The user passwords will be updated in Directory Server the next time those users log into Directory Server — if the passwords meet the password policy requirements on both Active Directory and Directory Server. **Note**: If you create users on Active Directory but do not select the User must change password at next login option, the users will be created on Directory Server. However, their passwords will be invalidated immediately because the users will not be forced to change their passwords the next time they log into Active Directory.
From Directory Server to Active Directory	Yes	Users are created on Directory Server and Active Directory, and link properly.
From Directory Server to Active Directory	No	Users are not created on Directory Server or Active Directory.
From Directory Server to Active Directory during `idsync resync -c`	Not Applicable	Users that exist on Directory Server will not be created on Active Directory because the entry you are trying to create on Active Directory does not contain a password and does not comply with the password policy.

Enforcing Password Policies on Directory Server Only

Table 9 describes different scenarios for a Directory Server only password policy using the following specifications:

- User must change password after reset
- User May Change Password
- Keep 20 passwords in history
- Password expires in 30 days
- Send warning 5 days before password expires
- Check password syntax: Password min length set to 7

Table 9 Example Scenarios: Password Policy on Directory Server Only

Scenario (Based on Direction of Flow)	Password Meets Policy Requirements	Results
From Active Directory to Directory Server	Yes	Users are created on Active Directory and Directory Server, and link properly. Users on Directory Server are created 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. **Note**: If you create users on Active Directory but do not select the User must change password at next login option, the users will be created on Directory Server. However, their passwords will be invalidated immediately because the users will not be forced to change their passwords the next time they log into Active Directory.

Table 9 Example Scenarios: Password Policy on Directory Server Only

Scenario (Based on Direction of Flow)	Password Meets Policy Requirements	Results
From Active Directory to Directory Server	No	Users are created on Active Directory and Directory Server and link properly. Users are created on Directory Server with no password. The users are created on Directory Server because the entries are initially created without a password, which does not trigger the password policy. Users will not be able to authenticate to Directory Server unless they log into Active Directory first. When these users log into Active Directory, they will be forced to change their password, which invalidates their passwords on Directory Server and forces on-demand synchronization the next time they authenticate to Directory Server. If users authenticate to Directory Server with a password from Active Directory that does not meet the password policy on Directory Server, the on-demand synchronization will authenticate to Active Directory and get a successful authentication back. On-demand synchronization will then try to update the password in Directory Server, but fail because the password will not meet Directory Server password policy requirements. The return code will be `LDAP Error Code 53 (DSA is unwilling to perform)` **Note**: If you create users on Active Directory but do not select the User must change password at next login option, the users will be created on Directory Server. However, their passwords will be invalidated immediately because the users will not be forced to change their passwords the next time they log into Active Directory.

Table 9 Example Scenarios: Password Policy on Directory Server Only

Scenario (Based on Direction of Flow)	Password Meets Policy Requirements	Results
From Active Directory to Directory Server during `idsync resync -c -i NEW_USERS`	Not Applicable	Users that exist on Active Directory are created in Directory Server with an invalidated password. (The `-i` option forces this action for `resync`). The invalidated password forces on-demand synchronization the next time those users authenticate to Directory Server. If users change their passwords on Active Directory to something that does not meet the password policy on Directory Server, the following note applies: **Note**: If you create users on Active Directory but do not select the User must change password at next login option, the users will be created on Directory Server. However, their passwords will be invalidated immediately because the users will not be forced to change their passwords the next time they log into Active Directory.
From Directory Server to Active Directory	Yes	Users are created on Directory Server and Active Directory, and link properly.
From Directory Server to Active Directory	No	Users are not created on Directory Server or Active Directory.
From Directory Server to Active Directory during `idsync resync -c`	Not Applicable	Users that exist on Directory Server but not on Active Directory will be created without a password. The administrator will have to reset the user passwords so they can log in to Active Directory the first time. If users change their passwords the first time they log in to Active Directory, they will invalidate their password on Directory Server and force on-demand synchronization the next time they authenticate to Directory Server. If users change their passwords on Active Directory to something that does not meet the password policy on Directory Server, the following note applies: **Note**: If you create users on Active Directory but do not select the User must change password at next login option, the users will be created on Directory Server. However, their passwords will be invalidated immediately because the users will not be forced to change their passwords the next time they log into Active Directory.

Important Notes

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

- Active Directory actually creates users “temporarily” and then deletes the entries if the password does not meet the password policy requirements. Consequently, the Active Directory connector sees this temporary `ADD` and creates users on the Directory Server side. The users will not have a password in Directory Server, so no one will be able to log in as the user. In addition, these entries will not be linked to a valid entry in Active Directory. If you try to run the `idsync resync -c` command, the entries will not be created in Active Directory because they do not have a password.
- If you specify a password policy on Directory Server, user entries are still created without a password. Directory Server does not enforce the password policy for user creations unless the entries contain a password.

There are several ways to recover from this situation.The preferred method is to remove the user from Directory Server and then add them to Active Directory with a valid password for the Active Directory password policies. This method ensures that the users are created on Directory Server and linked properly. Users on Directory Server will have their password invalidated when they log into Active Directory for the first time and change their passwords.

- If you do not delete the user from Directory Server, and then try to add the Active Directory user again with a new password, the `ADD` to Directory Server will fail because the user already exists on Directory Server. The entries will not be linked together and you will have to run a `idsync linkusers` command to link the two separate accounts.
- If you run the `idsync linkusers` command, you must be sure to reset the passwords for the accounts on Active Directory that were linked to entries on Directory Server. Resetting the passwords invalidates those passwords on Directory Server, which then forces on-demand synchronization to update the Directory Server password the next time the user authenticates to Directory Server with their new Active Directory password.
- If you run `idsync resync` with the `-c` option, the users that exist on Directory Server will not be created on Active Directory because there are no passwords available and the entry you are trying to create does not comply with the Active Directory password policy.

  To work around this problem,

  a. Set the Active Directory password policy’s Minimum Password Length to 0.

  b. Disable the Password must meet complexity requirements option.

  c. Run the following command to create existing Directory Server users on Active Directory with no passwords:

  ```
  idsync resync -h <hostname> -p port -D {directory manager} -w {password} -s
  o=idsconfig -q {configuration password} -o Sun -c
  ```

d. Set your Active Directory password policy back to their default settings.

e. Reset the user passwords on Active Directory, and set the flag that requires users to change their passwords the next time they log in. When the users log into Active Directory and change their passwords, the passwords will be invalid on Directory Server and force the on-demand synchronization the next time the users authenticate to Directory Server.

Error Messages

Check the central logger `audit.log` file on the core system for the following error messages:

- **`User not created on AD from DS with password policy`**:

```
INFO 63 CNN100 hostname "The agent is sending the following inbound action to MQ:
Type: CREATE SUL: lab3 {Data Attrs: [ADD telephonenumber: 212-121-1212] [ADD
userpassword: ****] [ADD mail: johndoe@sun.com]} {Other Attrs: nsuniqueid:
1b525981-926a11d8-80d880f1-73703f99 givenname: John sn: Doe uid: jdoe cn: John Doe
dn: uid=jdoe,ou=people,o=sun changenumber: 72}." (Action ID=CNN100-FC04B2476F-53,
SN=2)

INFO 47 CNN101 hostname "LDAP operation on entry cn=John
Doe,ou=people,dc=idsync,dc=com failed at ldaps://w2003.idsync.com:636, error(53):
LDAP server is unwilling to perform (0000052D: SvcErr: DSID-031A0FBC, problem 5003
(WILL_NOT_PERFORM), data 0)." (Action ID=CNN100-FC04B2476F-53, SN=7)

SEVERE 47 CNN101 hostname "Unable to create user "cn=John
Doe,ou=people,dc=idsync,dc=com" at ldaps://w2003.idsync.com:636. LDAP add operation
failed. Error code: 53, reason: 0000052D: SvcErr: DSID-031A0FBC, problem 5003
(WILL_NOT_PERFORM), data 0" (Action ID=CNN100-FC04B2476F-53, SN=8)
```

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

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

Changing Password Policies on Active Directory

To change the Active Directory Windows 2003 password policy so Identity Synchronization will work correctly, you must change the Windows password policies as follows:

- Change Minimum Password Length to `0` (zero) `characters`.
- Change Password must meet complexity requirements to Disabled.

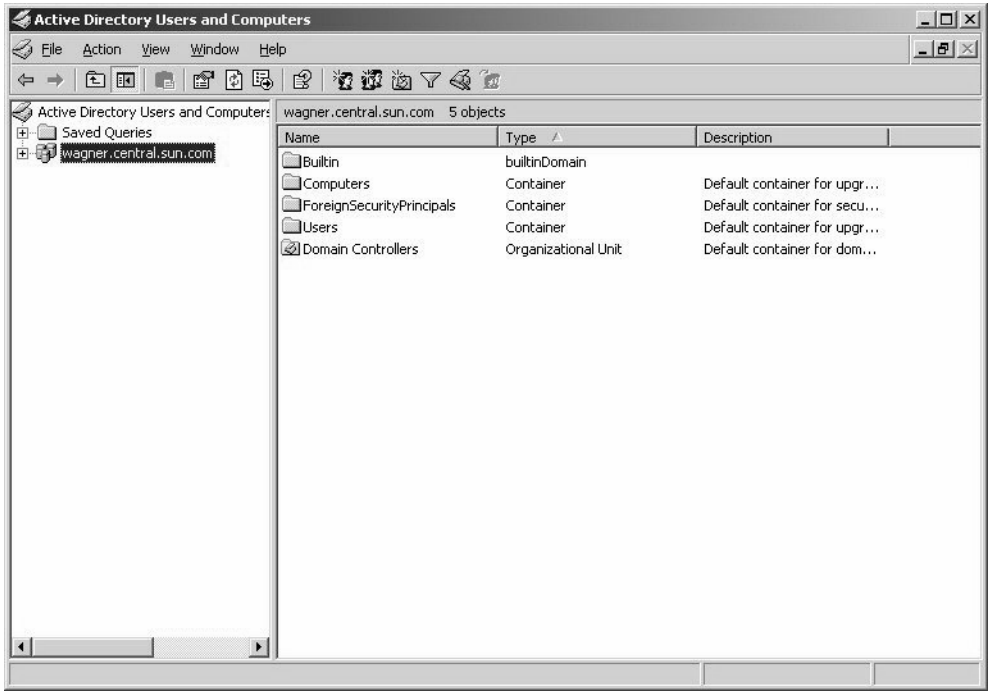
NOTE For Windows 2000 Active Directory environments, the system's default values for these rules are already compatible with Identity Synchronization for Windows' requirements.

The Active Directory connectors provided by Identity Synchronization for Windows 1.0 SP1 can be used for synchronization with Active Directory on Windows 2003.

Use the following procedure to change the complexity and minimum password length rules:

1. Select Start -> Settings -> Administrative Tools -> Active Directory Users and Computers to open the Active Directory Users and Computers window. (See Figure 2.)

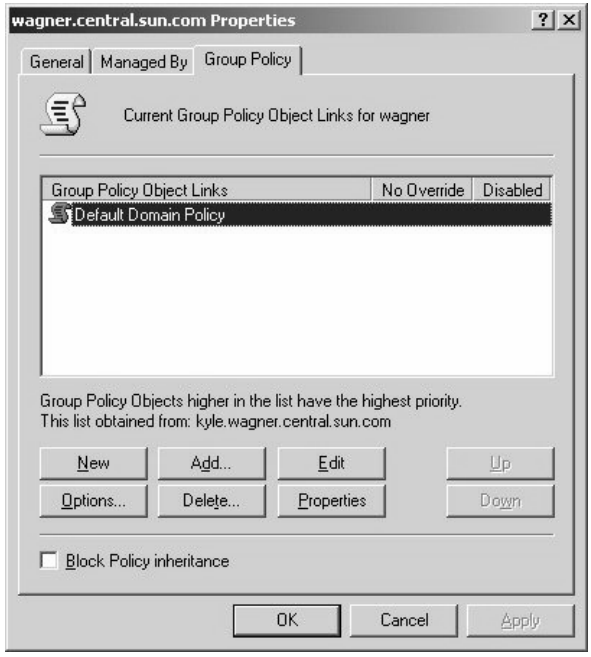
Figure 2 Active Directory Users and Computers Window



2. Right-click on your domain name in the left pane and select Properties from the pop-up menu.

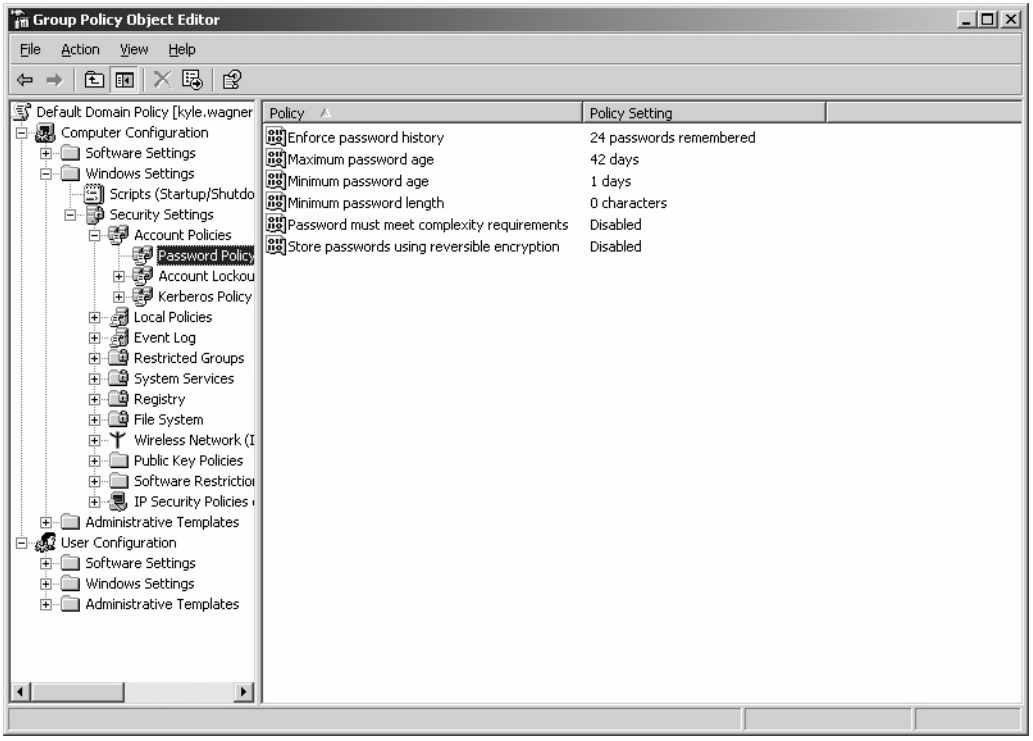
3. When the <*domain_name*> Properties dialog box is displayed, select the Default Domain Policy (as shown in Figure 3) and then click Edit.

Figure 3 <*domain_name*> Properties Dialog Box



4. When the Group Object Policy window displays (Figure 4), select Computer Configuration -> Windows Settings -> Security Settings -> Account Policies -> Password Policy.

Figure 4 Group Object Policy Window



5. Click the Password Policy icon located in the right pane (see Figure 4).
6. In the left pane, change the following policies so Identity Synchronization for Windows services can create entries that do not require passwords:
   - **Password must meet complexity requirements**: Change to `Disable` so Active Directory will not require passwords.
   - **Minimum password length**: Change to `0` (zero) `characters` so Active Directory will not require passwords with a minimum number of characters.
7. Close all windows and dialog boxes.

8. Run one of the following applications, which force the policy changes to take effect immediately:

   - **For a Windows 2003 operating system**: `gpupdate.exe`
   - **For a Windows 2000 operating system**:
     `secedit /refreshpolicy machine_policy /enforce`

NOTE For additional information about Windows Password Policies, refer to the following sources:

Apply or Modify Password/Group Policy in Windows 2003
`http://www.microsoft.com/resources/documentation/windowsserv/2003/standard/proddocs/en-us/password_grouppolicy.asp`

Using Secedit.exe to Force Group Policy to Be Applied Again - Windows 2000 Servers
Microsoft KB #227448

A Description of the Group Policy Update Utility - Windows 2003 Servers
Microsoft KB #298444

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

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 plugin (subcomponent), the installer must be able to contact 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 Plugin Requirements

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

Documentation Updates for Identity Synchronization for Windows 1.0 SP1

Detailed instructions for uninstalling Identity Synchronization for Windows version 1.0 manually are provided in the following three sections:

- "Manually Uninstalling Core and Instances from Windows 2000" on page 29
- "Manually Uninstalling Core and Instances from Solaris" on page 34
- "Manually Uninstalling an Instance from Windows NT" on page 40

NOTE The uninstallation instructions provided in this section are for uninstalling version 1.0 only.

Manually Uninstalling Core and Instances from Windows 2000

Use the instructions provided in this section to manually uninstall Core from a Windows 2000 machine.

NOTE In this section, Identity Synchronization for Windows locations are described in the following manner:

<*server_root*>\isw-<*hostname*>

Where <*server_root*> represents the parent directory of the Identity Synchronization for Windows installation location. For example, if you installed Identity Synchronization for Windows in `C:\Program Files\Sun\mps\isw-`*`example`*, the <*server_root*> would be `C:\Program Files\Sun\mps`.

1. Stop all Identity Synchronization for Windows java processes using one of the following methods:

   - Select Start -> Settings -> Control Panel -> Administrative Tools -> Services to open the Services window. In the right pane, right-click on Sun ONE Identity Synchronization for Windows and select Stop.
   - Open a Command Prompt window and type the following command:

     `net stop "Sun ONE Identity Synchronization for Windows"`

   - If the preceding methods do not work, you can use the following steps to stop the java processes manually:

     a. Open the Services window, right-click on Sun ONE Identity Synchronization for Windows, and select Properties.

     b. From the General tab in the Properties window, select Manual from the Startup type drop-down menu.

   NOTE Although you can view java processes (such as `pswwatchdog.exe`) from the Windows Task Manager, you cannot determine which processes are specifically related to Identity Sychronization for Windows. For this reason, do not stop processes from the Windows Task Manager.

2. Stop the Message Queue (for a Core uninstallation only) using one of the following methods:

   - In the Services window, right-click on iMQ Broker in the right pane and select Stop.
   - Open a Command Prompt window and type the following command:

     `net stop "iMQ Broker"`

   - If the preceding methods do not work, you can use the following steps to stop Message Queue manually:

     a. Open the Services window, right-click on iMQ Broker and select Properties.

     b. From the General tab in the Properties window, select Manual from the Startup type drop-down menu.

3. Remove the Directory Server plugin as follows:

   a. Open the Directory Server Console and select the Configuration tab.

   b. In the left pane, expand the Plugins node and select the pswsync node.

c. In the right pane, uncheck the Enable plug-in check box.

d. Click Save to save your changes.

e. From the Console, locate and remove the following entry from the Configuration Directory:

`cn=pswsync,cn=plugins,cn=config`

f. Stop Directory Server, using one of the following methods:

- In the Services window, right-click on Sun ONE Directory Server 5.2 in the right pane and select Stop.
- Open a Command Prompt window and type the following command:

  `net stop slapd-<myhostname>`

g. Open the Windows Explorer to locate and remove the plugin binary:

`<server_root>\lib\psw-plugin.so`

h. Restart Directory Server.

4. Open a Command Prompt window and type **`regedit`** to open the Registry Editor window.

Important – Back up your current registry file before proceeding to Step 5.

a. In the Registry Editor, select the top node (My Computer) in the left pane.

b. Select Registry -> Export Registry File from the menu bar.

c. When the Export Registry File dialog box is displayed, specify a name for the file and select a location in which to save the backup registry.

5. In the Registry Editor, select Edit -> Delete from the menu bar and remove the following Identity Synchronization for Windows keys from the Windows Registry:

- All entries under `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Identity Synchronization for Windows`
- All `CurrentControlSet` and `ControlSet` (such as `ControlSet001`, `ControlSet002`, and so forth) entries under `HKEY_LOCAL_MACHINE\SYSTEM\*`, which includes the following entries (if they exist):
  - `...\Control\Session Manager\Environment\PSWHOME`
  - `...\Services\Eventlog\Application\Sun ONE Identity Synchronization for Windows`

- ...\Services\Sun ONE Identity Synchronization for Windows
- ...\Services\iMQBroker

6. Back-up (copy and rename) the current productregistry file located in C:\WINNT\system32.
7. Edit the C:\WINNT\system32 productregistry file to remove the following tags:

NOTE

- For best results, use an XML editor. Alternatively, you can use a standard text editor.
- Some of the following components may not be included in your file.
- You must delete the beginning tag (<compid>), ending tag (<\compid>), and all contents in-between both tags). Ellipses are used in the following list to represent any additional text and/or tags that are included as part of these tags. (See the example page 33.)

- <compid>Identity Synchronization for Windows . . . </compid>
- <compid>Core . . . </compid>
- <compid>unistaller . . . </compid>
- <compid>wpsyncwatchdog . . . </compid>
- <compid>sentenv . . . </compid>
- <compid>Create DIT . . . </compid>
- <compid>Extend Schema . . . </compid>
- <compid>resources . . . </compid>
- <compid>CoreComponents . . . </compid>
- <compid>Connector . . . </compid>
- <compid>DSConnector . . . </compid>
- <compid>Directory Server Plugin . . . </compid>
- <compid>DSSubcomponents . . . </compid>
- <compid>ObjectCache . . . </compid>
- <compid>ObjectCacheDLLs . . . </compid>
- <compid>ADConnector . . . </compid>

The following is a <compid> tag sample. Remove <compid>, </compid>, and all text and tags in-between.

```
<compid>Identity Synchronization for Windows
    <compversion>1.0
          <uniquename>Identity Synchronization for Windows</uniquename>
           <compinstance>1
                    <children>
                        <compref>ADConnector
                            <instance>1
                                <version>1.0</version>
                            </instance>
                        </compref>
                        <compref>DSSubcomponents
                        . . .

        </compinstance>
    </compversion>
</compid>
```

8. Remove the Identity Synchronization for Windows installation folder located at *<server_root>*\isw-*<hostname>*.

   For example, C:\Program Files\Sun\mps\isw-example

9. Clean up the configuration directory as follows:

   a. From a Command Prompt window, run the ldapsearch command against the configuration directory where Identity Synchronization for Windows Core is installed to locate the Identity Synchronization for Windows Console subtree.

   NOTE ldapsearch is located in *<server_root>*\shared\bin\ldapsearch.

   For example, C:\Program Files\Sun\mps\shared\bin\ldapsearch

   ```
   ldapsearch -D "cn=directory manager" -w <my_password> -b o=netscaperoot
   "(nsnickname=isw)" dn
   ```

   The resulting entry should be similar to the following (note that the entry will always end with *o=NetscapeRoot*):

   ```
   "cn=Sun ONE Identity Synchronization for Windows,cn=server group,
   cn=myhost.mydomain.com,ou=mydomain.com,o=NetscapeRoot"
   ```

b. Use the Directory Server Console to remove the Identity Synchronization for Windows Console subtree you found and all subtrees below it.

10. Clean up the Identity Synchronization for Windows configuration registry as follows:

a. From a a Command Prompt window, run the following `ldapsearch` command to locate the Identity Synchronization for Windows configuration registry in Directory Server:

```
ldapsearch -D "cn=directory manager" -w <my_password> -b "dc=my,dc=domain"
"(&(objectclass=iplanetservice)(ou=IdentitySynchronization))" dn
```

The resulting entry should be similar to the following:

```
"ou=IdentitySynchronization,ou=Services,dc=my,dc=domain"
```

b. Use the Directory Server Console to remove the configuration registry subtree you found, including all subtrees below it.

11. Clean up all other Console-related files as follows:

a. Remove all Console jar files located in `<server_root>\java\jars\isw*`
For example, `C:\Program Files\Sun\mps\java\jars\isw*`

b. Remove all Console servlet jar files located in `\<directory_server_install_root>\bin\isw\`
For example, `C:\SunOne\Servers\bin\isw\`

12. Restart your machine for all changes to take effect.

Manually Uninstalling Core and Instances from Solaris

Use the instructions provided in this section to manually uninstall Core from a Solaris machine.

NOTE In this section, Identity Synchronization for Windows locations are described in the following manner:

`<server_root>/isw-<hostname>`

Where `<server_root>` represents the parent directory of the Identity Synchronization for Windows installation location. For example, if you installed Identity Synchronization for Windows in `/var/Sun/mps/isw-example`, the `<server_root>` would be `/var/Sun/mps`.

---

1. Stop all Identity Synchronization for Windows java processes by typing **/etc/init.d/isw stop** into a terminal window.

   If the preceding command does not stop all of the java processes, type the following:

   /usr/ucb/ps -gauxwww | grep java

   kill -s SIGTERM *<process IDs from preceding command>*

2. Stop Message Queue as follows:

   a. At the prompt, type the following command to stop the Message Queue broker:

      /etc/init.d/imq stop

   b. To stop any remaining imq processes, type:

      * **ps -ef | grep imqbroker**

      * **kill -s SIGTERM *<process IDs from preceding command>***

   c. Use one of the following methods to uninstall the broker packages and directories:

      - Use the Message Queue broker uninstall script (located in the Identity Synchronization for Windows instance directory on the host where you installed core) to uninstall the broker. Type the following:

        /*<server_root>*/isw-*<hostname>*/imq_uninstall

      - Manually uninstall the packages and directories as follows:

        Use the pkgrm: command to remove these packages:

SUNWaclg	SUNWiqum	SUNWiqjx
SUNWiqlen	SUNWxsrt	SUNWiqu
SUNWjaf	SUNWiqfs	SUNWjhrt
SUNWiqdoc	SUNWiquc	SUNWiqsup
SUNWiqr	SUNWjmail	

        Use the rm -rf command to remove these directories:

        ```
        rm -rf /etc/imq
        rm -rf /var/imq
        rm -rf /usr/bin/imq*
        ```

3. To remove the Identity Synchronization for Windows Solaris packages run `pkgrm <packageName>` for each of the packages listed in Table 10.
(For example, **`pkgrm SUNWidscm SUNWidscn SUNWidscr SUNWidsct SUNWidsoc`**)

Table 10 Solaris Packages to Remove

Package Name	Description
SUNWidscm	Sun ONE Directory Server Identity Synchronization package for Core components and Connectors.
SUNWidscn	Sun ONE Directory Server Identity Synchronization package for Console help files.
SUNWidscr	Sun ONE Directory Server Identity Synchronization package for Core Components.
SUNWidsct	Sun ONE Directory Server Identity Synchronization package for Connectors.
SUNWidsoc	Sun ONE Directory Server Identity Synchronization package for Object Cache.

To verify that all of the packages were removed, type the following:

```
pkginfo | grep -i "Identity Synchronization"
```

NOTE Run the `pkgrm <packageName>` command again if there are still existing packages due to dependencies.

4. Remove Director Server plugin as follows:
   a. Open the Directory Server Console and select the Configuration tab.
   b. In the left pane, expand the Plugins node and select the pswsync node.
   c. In the right pane, uncheck the Enable plug-in check box.
   d. Click Save to save your changes.
   e. From the Directory Server Console, locate and remove the following entry from the Configuration Directory:

      `cn=pswsync,cn=plugins,cn=config`

   f. Stop Directory Server.
   g. To remove the plugin binary, type

      `rm -f /<server_root>/lib/psw-plugin.so`

   h. Restart Directory Server.
5. Back-up (copy and rename) the current `productregistry` file located in `/var/sadm/install/productregistry`.

6. Manually edit the `productregistry` file in `/var/sadm/install/productregistry` to remove the following entries (*if present*):

NOTE

- For best results, use an XML editor. Alternatively, you can use a standard text editor.
- Some of the following components may not be included in your file.
- You must delete the beginning tag (`<compid>`), ending tag (`<\compid>`), and all contents in-between both tags). Ellipses are used in the following list to represent any additional text and/or tags that are included as part of these tags. (See the example on page 38.)

- `<compid>Identity Synchronization for Windows . . . </compid>`
- `<compid>Core . . . </compid>`
- `<compid>unistaller . . . </compid>`
- `<compid>wpsyncwatchdog . . . </compid>`
- `<compid>sentenv . . . </compid>`
- `<compid>Create DIT . . . </compid>`
- `<compid>Extend Schema . . . </compid>`
- `<compid>resources . . . </compid>`
- `<compid>CoreComponents . . . </compid>`
- `<compid>Connector . . . </compid>`
- `<compid>DSConnector . . . </compid>`
- `<compid>Directory Server Plugin . . . </compid>`
- `<compid>DSSubcomponents . . . </compid>`
- `<compid>ObjectCache . . . </compid>`
- `<compid>ObjectCacheDLLs . . . </compid>`
- `<compid>SUNWidscr . . . </compid>`
- `<compid>SUNWidscm . . . </compid>`
- `<compid>SUNWidsct . . . </compid>`
- `<compid>SUNWidscn . . . </compid>`
- `<compid>SUNWidsoc . . . </compid>`
- `<compid>ADConnector . . . </compid>`

The following is a example <compid> tag. Remove <compid>, </compid>, and all text and tags in-between.

```
<compid>Identity Synchronization for Windows
    <compversion>1.0
          <uniquename>Identity Synchronization for Windows</uniquename>
           <compinstance>1
                    <children>
                        <compref>ADConnector
                            <instance>1
                                <version>1.0</version>
                            </instance>
                        </compref>
                        <compref>DSSubcomponents
                        . . .

        </compinstance>
    </compversion>
</compid>
```

7. Remove the following Identity Synchronization for Windows directories and files:

   a. From the installation location, type

      rm -rf /<*server_root*>/isw-<*hostname*>

   b. Remove the bootstrap files by typing

      rm -rf /etc/init.d/isw

8. Clean up the configuration directory as follows:

   a. Run the following ldapsearch command against the configuration directory where Identity Synchronization for Windows core is installed to locate the Identity Synchronization for Windows Console subtree:

      ldapsearch -D "cn=directory manager" -w <*my_password*> -b o=netscaperoot "(nsnickname=isw)" dn

---

NOTE ldapsearch is located in Directory Server's <*server_root*>/shared/bin/ldapsearch
For example, var/Sun/mps/shared/bin/ldapsearch

The resulting entry should be similar to the following (note that the entry will always end with *o=NetscapeRoot*):

```
"cn=Sun ONE Identity Synchronization for Windows,cn=server group,
cn=myhost.mydomain.com,ou=mydomain.com,o=NetscapeRoot"
```

b. Use the Directory Server Console to remove the Identity Synchronization for Windows Console subtree and all subtrees below it.

9. Clean up the Identity Synchronization for Windows configuration registry as follows:

a. Run the following `ldapsearch` command to locate the Identity Synchronization for Windows configuration registry in Directory Server:

```
ldapsearch -D "cn=directory manager" -w <my_password> -b "dc=my,dc=domain"
"(&(objectclass=iplanetservice)(ou=IdentitySynchronization))" dn
```

The resulting entry should be similar to the following:

```
"ou=IdentitySynchronization,ou=Services,dc=my,dc=domain"
```

b. Use the Directory Server Console to remove the Identity Synchronization for Windows configuration registry and all subtrees below it.

10. Clean up all other Console-related files as follows:

a. Remove all Console jar files by typing:

`rm -rf <server_root>/java/jars/isw*`
For example, `/var/Sun/mps/java/jars/isw*`

b. Remove all Console servlet jar files by typing:

`rm -rf <server_root>/bin/isw/`
For example, `/var/Sun/mps/bin/isw/`

11. Restart your machine for all changes to take effect.

Manually Uninstalling an Instance from Windows NT

Use the instructions provided in this section to manually uninstall an instance from a Windows NT machine.

NOTE In this section, Identity Synchronization for Windows locations are described in the following manner:

<server_root>\isw-*<hostname>*

Where *<server_root>* represents the parent directory of the Identity Synchronization for Windows installation location. For example, if you installed Identity Synchronization for Windows in C:\Program Files\Sun\mps\isw-*example*, the *<server_root>* would be C:\Program Files\Sun\mps.

1. Stop all Identity Synchronization for Windows java processes (core and instance installations) using one of the following methods:
   - Select Start -> Settings -> Control Panel -> Administrative Tools -> Services to open the Services window. In the right pane, right-click on Sun ONE Identity Synchronization for Windows and select Stop.
   - Open a Command Prompt window and type the following command:

     net stop "Sun ONE Identity Synchronization for Windows"
   - If the preceding methods do not work, use the following steps to stop the java processes manually:
     a. Open the Services window, right-click on Sun ONE Identity Synchronization for Windows, and select Properties.
     b. From the General tab in the Properties window, select Manual from the Startup type drop-down menu.

NOTE Although you can view java processes (such as pswwatchdog.exe) from the Windows Task Manager, you cannot determine which processes are specifically related to Identity Sychronization for Windows. For this reason, do not stop processes from the Windows Task Manager.

2. Stop the Change Detector service using one of the following methods:

   - In the Services window, right-click on Sun ONE NT Change Detector Service in the right pane and select Stop.
   - Open a Command Prompt window and type the following command:

     net stop "Sun ONE NT Change Detector Service"

   - If the preceding methods do not work, use the following steps to stop the Change Detector Service manually:

     a. Open the Services window, right-click on Change Detector Service and select Properties.

     b. From the General tab in the Properties window, select Manual from the Startup type drop-down menu.

3. Restart your Windows NT computer.

4. You must remove Identity Synchronization for Windows registry keys. Open a Command Prompt window and type **regedit** to open the Registry Editor window.

   Important – Back up your current Windows registry file before proceeding to Step 5.

   a. In the Registry Editor, select the top node (My Computer) in the left pane.

   b. Select Registry -> Export Registry File from the menu bar.

   c. When the Export Registry File dialog box is displayed, specify a name for the file and select a location in which to save the backup registry.

5. In the Registry Editor, select Edit -> Delete from the menu bar and remove the following Identity Synchronization for Windows keys from the Windows Registry:

   - All entries under `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Identity Synchronization for Windows`
   - All `CurrentControlSet` and `ControlSet` (such as `ControlSet001`, `ControlSet002`, and so forth) entries under `HKEY_LOCAL_MACHINE\SYSTEM\*`, which includes the following entries (if they exist):
     - `...\Control\Session Manager\Environment\PSWHOME`
     - `...\Services\Eventlog\Application\Sun ONE Identity Synchronization for Windows`
     - `...\Services\Sun ONE Identity Synchronization for Windows`
     - `...\Services\iMQBroker`
   - The `HKEY_LOCAL_MACHINE\SOFTWARE\Sun Microsystems\PSW`

6. Modify (***do not delete***) the following registry key:

   a. Select the following registry key entry in the left pane:

      `HKEY_LOCAL_MACHINE\SYSTEM\\CurrentControlSet\\CONTROL\\LSA`

   b. In the right pane, right-click on the Notification Packages value and select Modify.

   c. Change the `PASSFLT` value to `FPNWCLNT`.

7. Back-up (copy and rename) the current `productregistry` file located in `C:\WINNT\system32`.

8. Edit the `C:\WINNT\system32` `productregistry` file to remove the following tags:

NOTE

- For best results, use an XML editor. Alternatively, you can use a standard text editor.
- Some of the following components may not be included in your file.
- You must delete the beginning tag (`<compid>`), ending tag (`<\compid>`), and all contents in-between both tags). Ellipses are used in the following list to represent any additional text and/or tags that are included as part of these tags. (See the example on page 33.)

- `<compid>Identity Synchronization for Windows . . . </compid>`
- `<compid>Core . . . </compid>`
- `<compid>unistaller . . . </compid>`
- `<compid>wpsyncwatchdog . . . </compid>`
- `<compid>sentenv . . . </compid>`
- `<compid>Create DIT . . . </compid>`
- `<compid>Extend Schema . . . </compid>`
- `<compid>resources . . . </compid>`
- `<compid>CoreComponents . . . </compid>`
- `<compid>Connector . . . </compid>`
- `<compid>DSConnector . . . </compid>`
- `<compid>Directory Server Plugin . . . </compid>`
- `<compid>DSSubcomponents . . . </compid>`
- `<compid>ObjectCache . . . </compid>`

- <compid>ObjectCacheDLLs . . . </compid>
- <compid>ADConnector . . . </compid>

The following is a example <compid> tag. Remove <compid>, </compid>, and all text and tags in-between.

```
<compid>Identity Synchronization for Windows
    <compversion>1.0
          <uniquename>Identity Synchronization for Windows</uniquename>
           <compinstance>1
                    <children>
                        <compref>ADConnector
                            <instance>1
                                <version>1.0</version>
                            </instance>
                        </compref>
                        <compref>DSSubcomponents
                        . . .

        </compinstance>
    </compversion>
</compid>
```

9. Remove the Identity Synchronization for Windows installation folder located at *<server_root>*\isw-*<hostname>*.

For example, C:\Program Files\Sun\mps\isw-example

NOTE You must edit the Windows registry as described in Step 8 before proceeding to Step 10.

10. Remove the Password Filter DLL.

Locate the passflt.dll file in the C:\winnt\system32 folder, and rename the file to **passflt.dll.old**.

11. Restart your machine for all changes to take effect.

Known Issues and Limitations

This section explains issues and limitations identified after the initial release of Identity Synchronization for Windows version 1.0.

NOTE For a description of previously reported issues and limitations (and available workarounds) for Identity Synchronization for Windows version 1.0, refer to the "Known Issues" section of the *Sun ONE Identity Synchronization for Windows Version 1.0 Release Notes*, which are available at the following Internet location:

`http://docs.sun.com/coll/S1_IdSyncForWin_1.0`

Avoid using the deny (all) ACI on entries that are subordinate to an SUL's Base DN. (*5009673*)

It is important to be aware of the use and impact of access control instructions (ACIs) on a directory branch that is subordinate to the Directory Server suffix (such as, dc=mydomain,dc=com) that is targeted for user synchronization.

You use the Identity Synchronization for Windows `prepds` command to add a special user (`uid=PSWConnector,dc=mydomain,dc=com`) to the base directory suffix; however, this command does not override existing ACIs that are subordinate to the directory suffix if the ACIs are more restrictive.

For example, if DN dc=mydomain,dc=com is the database suffix targeted for user synchronization, then all users under this suffix will normally be available for synchronization. However, if a branch DN such as dc=myusers,dc=mydomain,dc=com has a more-restrictive ACI, these users may not be available for synchronization.

Specifically, a more-restrictive ACI could be in the following form:

```
aci: (targetattr=*) (version 3.0;acl "my aci"; deny(all) (userdn="ldap:///all");)
```

Workaround:
You must reduce the level restriction or add the PSWConnector user as an exception to the rule. For example,

```
aci: (targetattr=*) (version 3.0;acl "my aci"; deny(all) (userdn="ldap:///all" and not
userdn="uid=PSWConnector,dc=mydomain,dc=com");)
```

NOTE For more information about troubleshooting ACIs, read the "Managing Access Control" and "Managing Log Files" chapters in the *Sun ONE Directory Server 5.2 Administration Guide*.

Message Queue will not start with "bad file magic number." (*4997872*)

If Message Queue will not start, check the log files for an entry similar to the following:

```
[20/Feb/2004:08:10:21 CST] [B1060]: Loading persistent data...
[20/Feb/2004:08:10:21 CST] ERROR [B4031]: Failed to load destinations from store:
java.io.StreamCorruptedException: C:\sunone\servers\isw-vwin2k\imq\var\instances
sw-broker?lestore†estination: Bad file magic number: 0; Expecting: 1431677610
[20/Feb/2004:08:10:21 CST] ERROR [B3000]: Could not open persistent message store:
com.sun.messaging.jmq.jmsserver.util.BrokerException: Failed to load destinations from
store:
java.io.StreamCorruptedException: C:\sunone\servers\isw-vwin2k\imq\var\instances
sw-broker?lestore†estination:
Bad file magic number: 0; Expecting: 1431677610
```

Workaround:
Invoke the following command:

```
imqbrokerd.exe -name psw-broker -reset store -reset messages
```

Because some synchronization events will be removed from the system, you are advised to perform a `resync` operation after executing this command.

A rename operation will fail on Directory Server if the RDN differs in case only. (*4985027*)

During a user rename operation, if the only difference between the old Relative Distinguished Name (RDN) component and the new RDN is the case, Active Directory will rename the user, but Directory Server will not.

For example, if you try to rename **cn=Upper Case, dc=somesuffix** to **cn=upper case, dc=somesuffix**, the operation will fail on Directory Server. There must be some other difference in the RDN for the operation to complete successfully on Directory Server.

Missing the `-P` option in `certutil` examples. (*4960968*)

The `certutil` examples provided in Chapter 10: "Configuring Security" of the *Sun ONE Identity Synchronization for Windows Installation and Configuration Guide Version 1.0*, should include the **`-P`** option, as follows:

```
C:\Program Files\Sun\MPS\shared\bin\certutil.exe -N -d . -P slapd-hostname-
C:\Program Files\Sun\MPS\shared\bin\certutil.exe -d . -P slapd-hostname- -S -n server-cert
-s "cn=hostname.example.com,c=us" -x -t CTu,,
C:\Program Files\Sun\MPS\shared\bin\certutil.exe -L -d . -P slapd-hostname-
```

Redistributable Files

Sun ONE Identity Synchronization for Windows 1.0 SP1 does not contain any files that can be redistributed.

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

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 1.0 SP1 Release Notes is 817-6262.

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
- 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://training.sun.com
- 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://wwws.sun.com/software
