

A large, abstract graphic on the left side of the page, consisting of several overlapping, curved, semi-transparent shapes in shades of gray, creating a layered, organic effect.

Additional Installation Instructions for Sun Java System Identity Synchronization for Windows 6.0

November 2009

This technical note contains the following sections:

- “Obtaining Sun Java System Identity Synchronization for Windows 6.0” on page 2
- “Supported Platforms and System Requirements” on page 2
- “Sun Java System Identity Synchronization for Windows 6.0 Installation Recommendations” on page 3

Obtaining Sun Java System Identity Synchronization for Windows 6.0

Sun Java System Identity Synchronization for Windows 6.0 is no longer bundled with the Directory Server Enterprise Edition software. You can download the Identity Synchronization for Windows software from http://www.sun.com/software/products/directory_srvr_ee/get.jsp.

For a detailed installation procedure, once you have downloaded the binaries, refer to the *Sun Java System Identity Synchronization for Windows 6.0 Installation and Configuration Guide*.

Supported Platforms and System Requirements

Sun Java System Identity Synchronization for Windows 6.0 is supported on the platforms listed here.

Note – Installing Sun Java System Identity Synchronization for Windows 6.0 on an unsupported platform will have unpredictable results.

Certain operating systems require additional service packs or patches, as shown in the following tables:

Operating System	Supported OS Versions	Architecture	Additional Required Software
Solaris Operating System	Solaris 10 Operating System for UltraSPARC®, and x86 (Pentium) architectures	64-bit	No additional software is required.
	Solaris 10 Operating System for x86 (Pentium) architectures	64-bit	
	Solaris 9 Operating System for SPARC architectures	64-bit	No additional software is required.
	Solaris 9 Operating System for x86 architectures	32-bit	
Red Hat Linux	Red Hat Advanced Server 4.0	32-bit and 64-bit	No additional software is required.
Microsoft Windows	Windows 2003 Server Enterprise and Standard Edition	32-bit	Latest security updates

Note – Windows Server 2008 is not a supported installation platform for Sun Java System Identity Synchronization for Windows 6.0. So, although you can synchronize with Active Directory 2008 data, installing Sun Java System Identity Synchronization for Windows 6.0 on Windows Server 2008 is not supported.

Identity Synchronization for Windows Requirements for Windows NT

The following table lists operating system requirements for Windows NT components and connectors.

Operating System	Supported OS Versions	Additional Required Software
Microsoft Windows	Windows NT 4.0 Server Primary Domain Controller, x86 architectures	Service Pack 6A

Sun Java System Identity Synchronization for Windows 6.0 Installation Recommendations

There are certain known issues with the installation of Sun Java System Identity Synchronization for Windows 6.0. These issues can be avoided, or alleviated, by following the recommendations that are provided in this section.

Identity Synchronization for Windows Patches and Hot Fixes

After you have installed Sun Java System Identity Synchronization for Windows 6.0 and before you perform the linking process, you should contact Sun Service Support to obtain the latest patches and hot fixes for this product.

For a comprehensive list of the known issues in Sun Java System Identity Synchronization for Windows 6.0, refer to [Chapter 6, “Identity Synchronization for Windows Bugs Fixed and Known Problems,” in *Sun Directory Server Enterprise Edition 7.0 Release Notes*](#).

NSS Security Patch

On Solaris 10 systems, the latest NSS security patches (3.12.4 and later) conflict with the NSS libraries that are installed with Sun Java System Identity Synchronization for Windows 6.0. If you install Sun Java System Identity Synchronization for Windows 6.0 after you have installed the NSS security patch, the Identity Synchronization for Windows installation effectively overwrites the NSS patch installation.

To work around this, reinstall the NSS security patch after you have installed .

The latest NSS security patch also causes problems if you restart the Directory Server from the console. The effect of this issue is that you are unable to access information through the console, and unable to log into or out of the console.

To work around this issue, you *must* set the following environment variable after you have installed the NSS patch and before you start the Directory Server or Identity Synchronization for Windows:

```
NSS_STRICT_NOFORK=DISABLED
```

This variable makes the new NSS libraries function in a manner that is similar to the previous version of the libraries, and no untoward issues should occur with Sun Java System Identity Synchronization for Windows 6.0.

In addition, if you are running Sun Java System Directory Server Enterprise Edition 6.x and using the Administration Server Console 5.2, you must create the following symbolic links manually before you install Identity Synchronization for Windows.

```
$ cd /var/mps/serverroot/lib
$ ln -s /usr/lib/mps/secv1/libnssutil3.so libnssutil3.so
$ ln -s /usr/lib/mps/secv1/libnssdbm3.so libnssdbm3.so
$ ln -s /usr/lib/mps/secv1/libsqlite3.so libsqlite3.so
```

These links are required for the Administration Server to function correctly.

Sun Java System Message Queue

Sun Java System Identity Synchronization for Windows 6.0 delivers a version of Message Queue that is no longer supported. The workaround for this depends on the version of Message Queue that you have installed.

- If you are running a version of Message Queue other than 3.7 update 1 (the version that is provided with Java Enterprise System 5 update 1), you need to do the following:
 1. Uninstall Message Queue.
 2. Install and configure the version of Message Queue that is provided with Java Enterprise System 5 update 1 (3.7 update 1).
 3. Run the following commands to create a dummy Message Queue license file:

```
$ mkdir /etc/imq/lic
$ touch /etc/imq/lic/imqbrokerun.lic
```
 4. If you are running the Solaris Operating System, you can then patch the Message Queue installation up to update 2, by using Solaris update patching.
 5. Install Sun Java System Identity Synchronization for Windows 6.0.
- If you are running Solaris 10u7 or above, you have Message Queue 3.7 update 1 installed by default. In this case, you can skip steps 1 and 2 in the previous procedure and simply create the dummy Message Queue license file before you install Identity Synchronization for Windows.

Note – Message Queue 3.7 update 1 or later is supported. Message Queue 4.x is not supported at this stage.

Group Synchronization

If you use Sun Java System Identity Synchronization for Windows 6.0 to synchronize groups, you *must* use the following configuration:

- Map the following Directory Server (DS) attributes to Active Directory (AD):
 - DS cn to AD cn
 - DS uid to AD samaccountname
- Define the creation expression as follows:
 - For Directory Server: uid=%uid%, sync_base
 - For Active Directory: cn=%cn%, sync_base
- In Directory Server, specify the uid attribute as the RDN for synchronized groups.

In spite of this configuration, group synchronization still has the following limitations:

- Concurrent modifications of a specific attribute is not supported with synchronized groups.
- Synchronization of nested groups fails.
- Group synchronization fails if the user entries that belong to a group are not at the same level as the sync base.

For example, if your sync base is ou=employees, dc=example, dc=com, the user DN must be uid=user-1, ou=employees, dc=example, dc=com. If the user DN is of the form uid=user-2, ou=sales, ou=employees, dc=example, dc=com, the ou=sales branch between the user and the sync base causes group synchronization to fail.

- If you create new users in Directory Server, and add those users to an existing group, the users must also be created in the corresponding connector before the synchronization of that group between Directory Server and Active Directory will work.

For additional limitations regarding synchronized groups, please see CR 6740714 and CR 6728372 (“[Known Problems and Limitations in Identity Synchronization for Windows](#)” in *Sun Directory Server Enterprise Edition 7.0 Release Notes*).

Note – Most of the group limitations described in the *Sun Directory Server Enterprise Edition 7.0 Release Notes* are fixed in the latest Identity Synchronization for Windows hot fix.

Synchronization With Active Directory 2008

Synchronization between Sun Directory Server 7.0 and Active Directory 2008 is supported, with the following restrictions:

- Fine-grained password policies.

These are supported, as long as the service complies with the configuration described here.

Active Directory, up to and including version 2003, uses Group Policy (GPO) that is global and domain-wide. The password policy and account lockout settings are therefore global in nature. In Active Directory 2008, domain level, fine-grained PSOs (password setting objects) can be configured for individual users or groups.

Identity Synchronization for Windows requires the password policy and account lockout settings to be uniform between Active Directory and Directory Server. This uniformity must include the PSOs, to avoid unpredictable behavior. Specifically, the following PSO attributes must have the same values in Active Directory and Directory Server:

- `msDS-LockoutThreshold` Determines how many failed password attempts are allowed before locking out a user account.
 - `msDS-LockoutObservationWindow` Determines the time after which a bad password counter is reset.
 - `msDS-LockoutDuration` Determines how long an account is locked out after too many failed password attempts.
- Read-only domain controllers.

These are not supported. Identity Synchronization for Windows uses a failover server for all operations. Unlike Directory Server read-only replicas, a read-only domain controller cannot be a part of the Active Directory failover setup.

A Directory Server replica uses a password plug-in that redirects all writable requests to the masters. This functionality cannot be provided in Active Directory, as there is no such plug-in.

Note – Windows Server 2008 is not a supported installation platform for Sun Java System Identity Synchronization for Windows 6.0. So, although you can synchronize with Active Directory 2008 data, installing Sun Java System Identity Synchronization for Windows 6.0 on Windows Server 2008 is not supported. For more information, see [“Supported Platforms and System Requirements” on page 2](#).

Windows 2008 does not alleviate the current group synchronization restrictions that are described in [“Group Synchronization” on page 4](#).

Using SUL Filters

If you specify different filters for Active Directory and Directory Server in the Synchronization User List (SUL), you might have unpredictable results. You must use the same filters for Active Directory and for Directory Server.

Copyright 2009 Sun Microsystems, Inc. All rights reserved. Sun Microsystems, Inc. has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more U.S. patents or pending patent applications in the U.S. and in other countries.

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

This distribution may include materials developed by third parties.

Parts of the product may be derived from Berkeley BSD systems, licensed from the University of California. UNIX is a registered trademark in the U.S. and other countries, exclusively licensed through X/Open Company, Ltd.

Sun, Sun Microsystems, the Sun logo, the Solaris logo, the Java Coffee Cup logo, docs.sun.com, Java, and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. or its subsidiaries in the U.S. and other countries.

All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and other countries. Products bearing SPARC trademarks are based upon an architecture

developed by Sun Microsystems, Inc.

The OPEN LOOK and Sun™ Graphical User Interface was developed by Sun Microsystems, Inc. for its users and licensees. Sun acknowledges the pioneering efforts of Xerox in researching and developing the concept of visual or graphical user interfaces for the computer industry. Sun holds a non-exclusive license from Xerox to the Xerox Graphical User Interface, which license also covers Sun's licensees who implement OPEN LOOK GUIs and otherwise comply with Sun's written license agreements.

Products covered by and information contained in this publication are controlled by U.S. Export Control laws and may be subject to the export or import laws in other countries. Nuclear, missile, chemical or biological weapons or nuclear maritime end uses or end users, whether direct or indirect, are strictly prohibited. Export or reexport to countries subject to U.S. embargo or to entities identified on U.S. export exclusion lists, including, but not limited to, the denied persons and specially designated nationals lists is strictly prohibited.

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

821-0816

Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 U.S.A.

