

# Sun Java™ System Identity Synchronization für Windows Versionshinweise

Version 1 2004Q3

Teilenummer 817-7850

---

Diese Versionshinweise enthalten wichtige Informationen, die bei der Herausgabe von Sun Java™ System Identity Synchronization für Windows 1 2004Q3 vorlagen. Hier werden neue Funktionen, Verbesserungen, bekannte Einschränkungen und Probleme, technische Hinweise und andere Informationen behandelt, die Sie vor der Installation und Verwendung von Sun Java System Identity Synchronization für Windows lesen sollten.  
1 2004Q3 (Identity Synchronization für Windows).

Diese Versionshinweise sind in die folgenden Abschnitte aufgegliedert:

- [Änderungsprotokoll](#)
- [Grundlegendes zu Identity Synchronization für Windows 1 2004Q3](#)
- [In dieser Version behobene Fehler](#)
- [Wichtige Informationen](#)
- [Bekannte Probleme und Einschränkungen](#)
- [Dateien für Neuverteilung](#)
- [Problemmeldungen und Feedback](#)
- [Weitere Informationen über Sun](#)

Diese Dokumentation verweist auf URLs zu Produkten von Drittanbietern, unter denen Sie weitere zugehörige Informationen finden.

---

**HINWEIS** Sun übernimmt keine Verantwortung für die Verfügbarkeit der in diesem Dokument erwähnten Websites von Drittanbietern. Sun unterstützt keine Inhalte, Werbung, Produkte oder andere Materialien, die auf oder mithilfe von solchen Sites oder Ressourcen erhältlich sind, und übernimmt diesbezüglich keine Haftung. Sun ist nicht verantwortlich oder haftbar für tatsächliche oder angebliche Schäden oder Verluste, die durch oder in Verbindung mit der Verwendung von derartigen Inhalten, Waren oder Dienstleistungen (bzw. das Vertrauen darauf) entstehen, die auf oder mithilfe von derartigen Sites oder Ressourcen verfügbar sind.

---

---

# Änderungsprotokoll

**Tabelle 1** Revisionsverlauf

Datum	Beschreibung der Änderungen
30. September 2004	Erste Veröffentlichung der Versionshinweise.

---

## Grundlegendes zu Identity Synchronization für Windows 1 2004Q3

Identity Synchronization für Windows bietet bidirektionale Kennwortsynchronisierung zwischen den folgenden Verzeichnissen:

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

Bei der Synchronisierung von Sun Java System Directory Server (Directory Server) und Windows 2000/2003 Active Directory können Sie alle Identity Synchronization für Windows-Komponenten unter Solaris™ Operating System und den Windows 2000 Server-Betriebssystemumgebungen installieren und ausführen. Beim Synchronisieren von Directory Server und Windows NT müssen Sie die Windows NT-Komponenten in der Windows NT-Umgebung ausführen.

Themen in diesem Abschnitt:

- [Neuheiten in dieser Version](#)
- [Hardware- und Softwareanforderungen](#)

# Neuheiten in dieser Version

## Neue Funktionen

Identity Synchronization für Windows 1 2004Q3 enthält folgende neue Funktionen:

- **Benutzer löschen:** Sie können die Synchronisierung von Benutzereintragslöschungen von Sun Java System Directory Server mit Active Directory und von Active Directory mit Sun Java System Directory Server konfigurieren und aktivieren.
- **Active Directory Failover:** Unterstützung für die Angabe zusätzlicher Active Directory-Server bei Failover während der bedarfsgesteuerten Authentifizierung. Mithilfe dieser Funktion authentifiziert das Identity Synchronization für Windows Directory Server-Plug-In Benutzer für Active Directory, wenn ihr Kennwort sich in Active Directory geändert hat. In Version 1.0 war dies nicht möglich, d. h., wenn der primäre Active Directory-Server nicht verfügbar war, schlug die Durchsatzauthentifizierung für Active Directory vom Identity Synchronization für Windows Directory Server-Plug-In fehl und der Benutzer konnte sich nicht für Directory Server authentifizieren. Dieser Fall trat nur ein, wenn der Benutzer sein Kennwort für Active Directory geändert hatte und sich zum ersten Mal nach Änderung des Kennworts für Directory Server authentifizieren wollte.
- **Benutzerobjektklassen für Active Directory:** Für Active Directory-Schemainformationen können Sie eine beliebige geeignete Objektklasse (user oder eine Erweiterung) verwenden. (In Version 1.0 konnte nur die Objektklasse user verwendet werden.)
- **Unterstützung für Windows 2003 Server Active Directory:** Sie können nun Identity Synchronization für Windows 1 2004Q3 installieren und konfigurieren und Kennwörter sowie Attribute mit Active Directory auf einer Windows 2003 Server Standard- oder Enterprise Edition-Plattform ausführen.
- **Zusätzliche Objektklassenunterstützung für die Benutzersynchronisierung:** Sie können Attributzuordnungen für Attribute in zusätzlichen und strukturellen Objektklassen definieren. Für Active Directory wird der Satz zusätzlicher Klassen durch Ihre Auswahl von Haupt- bzw. strukturellen Objektklassen beschränkt. In Directory Server können Sie eine beliebige andere Objektklasse verwenden.
- **Migration:** Erlaubt die Migration von der Version 1.0 oder Version 1.0 SP1 auf Version 1 2004Q3.
- **Unterstützung der Solaris 9 x86-Plattform:** Identity Synchronization für Windows unterstützt die Solaris 9 x86-Plattform vollständig.

- **Linkusers- und resync-Befehlszeilenvorgang:** Die Funktion des linkusers-Befehls wurde mit dem resync-Befehl vereint. Den resync-Befehlszeilenoptionen wurden drei Optionen hinzugefügt. Bei den Befehlen handelt es sich um:
  - `-f <linkusers.cfg>` – die Verknüpfungsdatei (wurde zuvor im Befehl `linkusers` verwendet)
  - `-k --nur Benutzer verknüpfen`
  - `-i NEW_LINKED_USERS` – das Kennwort neu verknüpfter Benutzer zurücksetzen. Dieser Befehl entspricht den Befehlen `ALL_USERS` und `NEW_USERS`, mit Ausnahme von Benutzern, die in Directory Server verknüpft sind.

Weitere Informationen über diese neue Funktion finden Sie im *Identity Synchronization for Windows Installation and Configuration Guide*.

---

**HINWEIS** Da Microsoft Windows NT voraussichtlich im Dezember 2004 einstellt, behebt Identity Synchronization für Windows 1 2004Q3 zwar Fehler in Verbindung mit Windows NT, unterstützt jedoch keine neuen Funktionen für diese Plattform.

Weitere Informationen finden Sie im Abschnitt „Windows Life Cycle Support“ unter folgendem URL: [http://support.microsoft.com/default.aspx?scid=fh;\[ln\];LifeWin](http://support.microsoft.com/default.aspx?scid=fh;[ln];LifeWin)

---

## Produktänderungen

Folgende Produktänderungen wurden in der Version 1 2004Q3 vorgenommen:

- **Installation:** Da Sun Java Enterprise System 2 2004Q2 Sun Java System Message Queue Enterprise Edition und Sun Java System Directory Server installiert (die beide für Identity Synchronization für Windows 1 2004Q3 erforderlich sind), müssen Sie Sun Java Enterprise System auf Ihren Solaris-Systemen vor der Installation von Identity Synchronization für Windows 1 2004Q3 installieren.

Zuvor installierte Identity Synchronization für Windows Version 1.0 Sun Java System Message Queue 3.0.1 (Message Queue). Die Version 1 2004Q3 nimmt diese Installation nicht vor.

- **Neuer Name für Produkt und Dokumentation:** Das Identity Synchronization für Windows-Produkt sowie die Produktdokumentation wurden von *Sun ONE Identity Synchronization für Windows* in *Sun Java System Identity Synchronization für Windows* umbenannt.

## Leistungsverbesserungen

Die Synchronisierungsleistung wurde erheblich verbessert.

## Änderungen in der Dokumentation

**Neuer Name für Produkt und Dokumentation:** Das Sun Java System Identity Synchronization für Windows-Produkt sowie die Produktdokumentation wurden von *Sun ONE Identity Synchronization für Windows* in *Sun Java System Identity Synchronization für Windows* umbenannt.

# Hardware- und Softwareanforderungen

## Betriebssystemanforderungen

In der folgenden Tabelle sind die Betriebssystemanforderungen für diese Version von Identity Synchronization für Windows beschrieben:

**Tabelle 2** Solaris-Anforderungen

Komponente	Solaris™-Anforderungen
Core-Komponenten	Solaris 8™ für UltraSPARC® (32-Bit und 64-Bit) Solaris 9™ SPARC® Platform Edition (32-Bit und 64-Bit) Solaris 9™ Operating System (x86 Platform Edition für Pentium II oder höher) IA-32
Konnektoren für Sun Java™ System Directory Server und für Windows Active Directory	Solaris 8 für UltraSPARC (32-Bit und 64-Bit) Solaris 9 für SPARC-Plattformen (32-Bit und 64-Bit) Solaris 9™ Operating System (x86 Platform Edition für Pentium II oder höher) IA-32
Sun Java™ System Directory Server-Plug-In	Solaris 8 für UltraSPARC (32-Bit und 64-Bit) Solaris 9 für SPARC-Plattformen (32-Bit und 64-Bit) Solaris 9™ Operating System (x86 Platform Edition für Pentium II oder höher) IA-32

**Tabelle 3**    Windows-Anforderungen

Komponente	Windows-Anforderungen
Core	Windows 2000 Server SP4 Windows 2000 Advanced Server SP4 Windows Server 2003 Standard oder Enterprise Edition
Konnektoren für Sun Java™ System Directory Server und für Windows Active Directory	Windows 2000 Server SP4 Windows 2000 Advanced Server SP 4 Windows Server 2003 Standard oder Enterprise Edition
Sun Java™ System Directory Server-Plug-In	Windows 2000 Server SP4 Windows 2000 Advanced Server SP 4 Windows Server 2003 Standard oder Enterprise Edition
NT-Konnektoren und Plug-Ins (Unterkomponenten)	Windows Primary Domain Controller NT 4.0 Server SP 6A (nur für x86)
Synchronisierung mit Active Directory auf Windows 2003 Standard und Enterprise Server	Windows Server 2003 Standard Edition (mit aktuellen Sicherheitsupdates) Windows Server 2003 Enterprise Edition (mit aktuellen Sicherheitsupdates)

Hardwareanforderungen

Ihre Hardware (alle Plattformen) muss zum Ausführen von Identity Synchronization für Windows folgende Mindestanforderungen erfüllen:

- Etwa 400 MB Speicherplatz für eine Mindestinstallation
- Mindestens 512 MB RAM für Server, die eine Identity Synchronization für Windows-Komponente ausführen (vorzugsweise 1 GB RAM)

Sun Java SystemSoftwareanforderungen

Zum Ausführen von Identity Synchronization für Windows müssen folgende Sun Java System-Softwarekomponenten installiert sein:

- Sun Java System Message Queue Enterprise Edition Version 3.5 SP 1 (ehemals Sun ONE Message Queue)  
  
Message Queue Enterprise Edition Version 3.5 SP 1 muss vor der Installation von Identity Synchronization für Windows bereits installiert sein. Es wird außerdem empfohlen, Message Queue Enterprise Edition Version 3.5 SP 1 vor Sun Java System Directory Server 5 2004Q2 zu installieren.

Um den Identity Synchronisation für Windows-Core-Server in einer *vorhandenen* Sun Java System Message Queue-Installation zu installieren, müssen Sie Message Queue Enterprise Edition 3.5 SP1 verwenden. Bei Installation des Identity Synchronisation für Windows-Core-Servers in einer unzulässigen Version von Message Queue treten Synchronisierungsfehler auf.

- Sun Java System Directory Server Version 5 2004Q2 oder höher

Voraussetzung für die Installation von Identity Synchronisation für Windows 1 2004Q3 ist die Ausführung von Directory Server 5 2004Q2 (5.2 Patch 2).

Weitere Informationen zur Installation des Solaris-Pakets bzw. zu den anzuwendenden Patches finden Sie unter [Wichtige Informationen](#) in den [Sun Java System Directory Server 5 2004Q2 Release Notes](#).

Weitere Informationen zur komprimierten Archivinstallation (ZIP-Installation), zum Anwenden von Patches und zu bekannten Fehlern in der ZIP-Aktualisierung finden Sie in den [Installation Notes](#) in den [Sun One Directory Server 5.2 Release Notes](#).

Eine Liste der durch Directory Server 5.2 Patch 2 behobenen Fehler (dies gilt für die Behebung wichtiger Fehler) finden Sie im nachfolgend angegebenen Dokument bzw. in den jeweiligen README-Dateien zu sämtlichen angewendeten Patches: [Sun Java System Directory Server 5 2004Q2 Release Notes](#).

Auf jedem Directory Server-Master, -Replikat und -Hub Ihres Systems muss ein Directory Server-Plug-In (Unterkomponente) installiert sein.

Aktuelle Informationen über Patches, die unter Umständen für die Installation von Directory Server 5 2004Q2 unter Solaris erforderlich sind, finden Sie im *Sun Java System Directory Server 5 2004Q2 Installation and Migration Guide* und den *Sun Java System Directory Server 5 2004Q2 Release Notes* auf folgender Website:

[http://docs.sun.com/db/coll/DirectoryServer\\_04q2](http://docs.sun.com/db/coll/DirectoryServer_04q2)

- Sun Java System Directory Server 5 2004Q2 Retro Change Log-Patch

Zur Behebung eines Problems mit der Directory Server Retro Change Log- und der Löschfunktion in Identity Synchronisation für Windows 1 2004Q2 muss ein Patch auf Sun Java System Directory Server 5 2004Q2 installiert werden. Die Einzelheiten der Patchnummer für spezifische Systemumgebungen lauten wie folgt:

- Für das Solaris Sparc-Paketformat: Patchnummer 117907-02 oder höher
- Für komprimierte Archivinstallationen von Solaris Sparc: Patch 5077789
- Für das Solaris X86 Package-Format: Patchnummer 117908-02 oder höher
- Für komprimierte Archivinstallationen von Solaris X86: Patch 5077789
- Für komprimierte Windows-Archivinstallationen: Patch 5077789

Weitere Informationen über diese Patches und über ihre Aktualisierung in der Directory Server-Umgebung finden Sie in der Datei `README.patch` im Downloadverzeichnis von Identity Synchronization für Windows:

`<download_root>/patches/directory/README.patch`

- **Java Runtime Environment**

Mit diesem Produkt wird kein J2SE Java Runtime Environment (JRE) mitgeliefert.

- Zum Ausführen des Identity Synchronization für Windows-Installationsprogramms unter Solaris oder Windows Active Directory müssen Sie JRE 1.4.2\_04 (oder höher) ausführen. Sie können auch J2SE v 1.4.2\_04 SDK installieren, das eine bessere Leistung als JRE besitzt.
- Unter Windows NT müssen Sie JRE 1.4.1\_03 (oder höher) installieren.

Außerdem müssen Sie `JAVA_HOME` auf ein 1.4.2\_04 JRE (oder höher) unter Solaris festlegen, bevor Sie Identity Synchronization für Windows installieren. Andernfalls meldet das Installationsprogramm unter Umständen `JAVA_HOME` als nicht festgelegt.

---

# In dieser Version behobene Fehler

In der nachfolgenden Tabelle werden die in Identity Synchronization für Windows 1 2004Q3 behobenen Fehler beschrieben:

**Tabelle 4** Behobene Fehler in Identity Synchronization für Windows 1 2004Q3

Fehlernummer	Beschreibung
<b>Installation/Deinstallation</b>	
4881466	Die Installation der Core-Komponenten bei einer vorhandenen Message Queue-Instanz an einem anderen Port als 7676 ist fehlgeschlagen.
4829497	Vom Deinstallationsprogramm wurden nicht alle Dateien und Ordner entfernt.
4820869	Unter Windows hätte das System vor dem erneuten Installieren der Core-Komponenten neu gestartet werden müssen.
4916789	Es wurden duplizierte Directory Server-Plug-In-IDs für Replikate erzeugt, die in demselben <code>Server_Root</code> -Verzeichnis installiert sind.
5035406	Die Installation des Core-Servers ist bei Verwendung von JRE statt JDK auf Solaris-Computern fehlgeschlagen.
4880807	<code>runInstaller.sh</code> und <code>runUninstaller.sh</code> unterstützten keine <code>-nodisplay</code> -Option.



**Tabelle 4** Behobene Fehler in Identity Synchronization für Windows 1 2004Q3 (*Fortsetzung*)

<b>Fehlernummer</b>	<b>Beschreibung</b>
5030928	Das Installationsprogramm unterstützte keine unterschiedlichen Anmeldedaten für primäre und Failover-Hosts.
5037157	Das Deinstallationsskript ist nach einer reinen DS-Plug-In-Installation nicht vorhanden.
5050554	Zum Starten des Installationsprogramms im „-nodisplay“-Modus war ein gültiger DISPLAY-Wert erforderlich.
4915192	Installieren des Konnektors auf einem Nur-SSL-Directory Server war nicht möglich.
5052509	Das textbasierte Deinstallationsskript hat nicht alle zu Identity Synchronization gehörenden Pakete entfernt.
4937341	Die Deinstallation von Identity Synchronization für Windows mit der Option zum Hinzufügen bzw. Entfernen auf Windows-Systemen schlug fehl.
5056685	Die Kennwortfilter-DLL wurde vom NT-Plug-In-Deinstallationsprogramm nicht entfernt (erforderlich, damit Windows beim Start die DLL nicht lädt, um sicherzustellen, dass sie entfernt wurde). Dies führte bei der Neuinstallation der Komponente zu Problemen.
4988901	Einige Fenster des Installationsprogramms zeigten nach Klicken auf die Schaltfläche „Zurück“ nicht das entsprechende Fenster an.
5030567	Bei der NT-Konnektorinstallation zeigte das Installationsprogramm den vorgeschlagenen Text, dass alle Teilkomponenten für den NT-Konnektor bereits installiert sind, nicht ordnungsgemäß an.
5036330	Bei der Installation wurde der Standardwert für den beschreibenden Text im Feld für die Eingabe eines aussagekräftigen, eindeutigen Namens für die Administrationsdomäne geändert. Der Installationsvorgang ist fehlgeschlagen.
5041518	Fälschlicherweise wurde beim Klicken auf die Schaltfläche „Zurück“ während der Installation der Teilkomponenten das Fenster für den Konnektor-Anschluss angezeigt.
5048953/ 5049733	Der Deinstallationsvorgang schlug fehl, wenn der Wert JAVA_HOME Anführungszeichen enthielt.
5050691	Bei der Installation des Core zeigt das Fenster für die MQ-Konfiguration eine falsche Meldung in Bezug auf die auf dem System installierte MQ-Version an. Es zeigte „null“ an.
5057716	Weder das Directory Server-Plug-In-Paket noch die entsprechenden Registrierungseinträge werden vom System entfernt, obwohl das Plug-In erfolgreich deinstalliert wurde.
5071574	Für den Directory Server-Konnektor wurde keine gültige Portnummer (65535) akzeptiert.
5079602	Der nt_dll_registrar erzwang für „Benachrichtigungspakete“ nicht REG_MULTI_SZ.
<b>Kennwortsynchronisierung</b>	
4845844	Der Befehl <code>Idsync resync</code> schlug fehl. Es wurden bei der Synchronisierung keine Benutzer von Directory Server auf NT angelegt.
4937502	Konnektoren können die Synchronisierung bei häufiger Unterbrechung der Netzwerkverbindung anhalten.

**Tabelle 4** Behobene Fehler in Identity Synchronization für Windows 1 2004Q3 (*Fortsetzung*)

<b>Fehlernummer</b>	<b>Beschreibung</b>
4939825	Der Directory Server-Konnektor hat kein Schleifenerkennungsattribut für geänderte Einträge entfernt.
4906752	Das Anlegen eines Benutzers, auf das unmittelbar ein modrdn-Vorgang in Sun Directory Server folgte, wurde nicht synchronisiert.
4933861	NT-Konnektor zeigte übermäßige Aktivität beim Starten der Synchronisierung nach einem „idsync resync -c -o Sun“-Befehl und Verwendung synthetischer Attribute.
4941200	Umbenannte Benutzereinträge wurden nicht synchronisiert, wenn nur die Groß- bzw. Kleinschreibung geändert wurde.
4893525	Attributänderungen gingen bei Beenden der Netzwerkverbindung zum Active Directory Server verloren.
5019327	Der Directory Server-Konnektor synchronisiert Benutzer, wobei die Objektklasse auf die Unterklasse des synchronisierten Objektklassentyps festgelegt ist.
4995351	Identity Synchronization für Windows ordnete ein falsches Attribut zu.
5036025	Das Ändern von SULs und der anschließende Versuch, Benutzer zu synchronisieren, führte zu einem NullPointerException-Fehler (der in den Protokolldateien gemeldet wurde). Der Konnektor antwortet nicht mehr.
5054654	Die am Kennwort unter NT vorgenommenen Änderungen gingen verloren, als der Konnektor zurückgesetzt oder abrupt heruntergefahren wurde.

#### **Sun Java System Message Queue**

4881240	Unter Solaris konnte eine vorhandene Meldungswarteschlange nicht verwendet werden, wenn sie in einem Benutzerverzeichnis installiert war.
---------	---

#### **Allgemein**

4943564 / 4939730	<i>Benutzerkennwort</i> war kein optionales Attribut.
4994145	Das Directory Server-Plug-In prüfte die Verbindung zu nicht verfügbaren Hosts zu häufig.
5041435	Bedarfsgesteuerte Kennwortaktualisierung hielt den Directory Server vom Antworten ab, wenn die Option „Kennwortchronik“ aktiviert war.
4939859	„Idsync linkusers/resync“ ignorierte LDAP-Filteroption, wenn der Quellkonnektor Windows NT war.
4987742	<i>resync</i> verarbeitete nicht alle Einträge aufgrund einer Race-Bedingung.
5048362	Zeilenwechsel in Protokollmeldungen wurden nicht automatisch entfernt.
4925575	Das Installationsprogramm für Active Directory-Konnektor hat nicht geprüft, ob die Domäne mit der Zertifikatsdomäne übereinstimmt.
4901486	Mehrere Active Directory-Strukturen wurden von Identity Synchronization für Windows 1 2004Q3 zuvor nicht unterstützt.

**Tabelle 4** Behobene Fehler in Identity Synchronization für Windows 1 2004Q3 (*Fortsetzung*)

<b>Fehlernummer</b>	<b>Beschreibung</b>
<b>Konsole allgemein</b>	
5040094	„objectclass=<some oc>“ meldete einen ungültigen Filter.
5030704	Das <code>resync</code> -Intervall für die Active Directory-Quelle von der Konsole konnte nicht geändert werden.
5026929	Der Standardwert für die obligatorischen Erstellungsattribute konnte nicht festgelegt werden.
4941238	Die Protokollanzeige hat den Protokolldatensatz falsch analysiert.
5008697	Statt das vorhandene Element zu aktualisieren, wurde der Liste bei der Bearbeitung der cn-Zuordnung ein weiteres Element hinzugefügt.
50134407	Eine Verzeichnisquelle konnte mit demselben Namen erstellt werden wie eine bereits vorhandene Verzeichnisquelle. Es wurde weder eine Fehlermeldung angezeigt noch konnte die Verzeichnisquelle gelöscht werden.
5026198	Typografische Fehler im Protokollfenster der Konsole wurden korrigiert.
5044529	Der Konsolenbefehl „preps“ funktionierte auf einem Nur-SSL-Directory-Server nicht.
5045350	Beim Ändern eines vorhandenen Erstellungsattributs konnte der Wert nicht auf <Kein> festgelegt werden.
4921889	Nach erneuter Auswahl der Option zum Anzeigen der Struktur zeigte die Konsole nicht wieder die normale Strukturansicht an.
<b>Konnektor</b>	
4988028	Java Run Time Exception (RTE) bei nicht vorhandenem <code>usnchanged</code> -Attribut.
<b>Befehlszeilen-Dienstprogramme</b>	
5015766	Durch Übergabe eines leeren Kennworts an <code>idsync changepw</code> ist ein anschließender Zugriff auf die Konfigurationsregistrierung nicht möglich.
4986303	Die Befehlszeilenschnittstelle (CLI) stellte keine Standardwerte für die Optionen <code>-h</code> , <code>-p</code> , <code>-D</code> und <code>-s</code> zur Verfügung.
5038195	Der Befehl <code>resetconn</code> gab bei ungültigem Konfigurationssuffix keine entsprechende Fehlermeldung aus.
5019543	Der Befehl <code>printstat</code> gab bei ungültigem Konfigurationssuffix keine entsprechende Fehlermeldung aus.
5024148	Der Befehl <code>resetconn</code> löschte die Anmeldedaten für die Meldungswarteschlange des Konnektors nicht.
4941125	Der Befehl <code>resync</code> aktualisierte synchronisierte Benutzer, sofern die Quelle Sun ist und synthetische Attribute synchronisiert wurden.
4939484	Der Befehl <code>linkusers</code> wird möglicherweise nie beendet.
5015575	Der CLI-Vorgang wurde nicht angehalten, wenn der Befehl „c“ an der Eingabeaufforderung ausgeführt wurde.
5062028	Die Eingabeaufforderung reagierte nicht mehr, als der Core mit SSL installiert wurde. (Bei dem Standardwert für den Port auf der CLI handelte es sich um den SSL-Port.)

# Wichtige Informationen

In diesem Abschnitt finden Sie die aktuellsten Informationen, die nicht in der eigentlichen Produktdokumentation enthalten sind. Es werden die folgenden Themen behandelt:

- [Installationshinweise](#)
- [Kompatibilität](#)
- [Datenwiederherstellung bei einem System- oder Anwendungsfehler](#)
- [Aktualisierung der Identity Synchronization für Windows 1 2004Q3-Dokumentation](#)
- [Ausführen von Identity Synchronization für Windows in einer Firewall-Umgebung](#)

## Installationshinweise

Lesen Sie vor dem Installieren von Identity Synchronization für Windows 1 2004Q3 das Kapitel zur Installationsvorbereitung im *Sun Java™ System Identity Synchronization für Windows 1 2004Q3 Installation and Configuration Guide*.

### Arbeiten mit Windows 2003 Server

- Sie können nun Windows 2003 Server Standard oder Enterprise Edition als Plattform für die Installation und Konfiguration von Identity Synchronization für Windows 1 2004Q3 verwenden.
- Auf dem Windows 2003 Server erzwingt die Standardkennwortrichtlinie sichere Kennwörter und entspricht damit nicht der Standardkennwortrichtlinie unter Windows 2000.

### *Probleme mit Windows 2003 Server*

**Das Verhalten von Windows 2003 Server für das Kennzeichen „Benutzer muss das Kennwort bei der nächsten Anmeldung ändern“ unterscheidet sich von Windows 2000. (4997513)**

Unter Windows 2003 wird das Kennzeichen Benutzer muss das Kennwort bei der nächsten Anmeldung ändern standardmäßig gesetzt, was unter Windows 2000 nicht der Fall ist.

Wenn Sie unter Windows 2000/2003 Benutzer mit festgelegtem Kennzeichen „Benutzer muss das Kennwort bei der nächsten Anmeldung ändern“ erstellen, werden die Benutzer auf Directory Server ohne Kennwort erstellt. Beim nächsten Anmelden der Benutzer bei Active Directory werden sie gezwungen, ihr Kennwort zu ändern. Dadurch werden ihre Kennwörter auf Directory Server ungültig und es wird bei der nächsten Authentifizierung dieser Benutzer für Directory Server eine bedarfsgesteuerte Synchronisierung erzwungen.

Die Benutzer können sich erst wieder für Directory Server authentifizieren, wenn sie ihr Kennwort in Active Directory geändert haben.

## Kompatibilität

### **Kompatibilitätsprobleme beim Verwenden bestimmter Remotekonsolenprodukte für den Zugriff auf die Identity Synchronization für Windows-Konsole. (5077227)**

Bei dem Versuch, die Identity Synchronization für Windows-Konsole mit PCAnywhere 10.x oder Remote Administration 2.1 anzuzeigen, können Probleme auftreten. (PCAnywhere Version 9.2 verursacht hingegen keine Fehler.) Bestehen die Probleme weiter, entfernen Sie die Remoteverwaltungssoftware. Alternativ kann VNC verwendet werden. Es sind diesbezüglich keine Probleme beim Anzeigen der Identity Synchronization für Windows-Konsole bekannt.

## Datenwiederherstellung bei einem System- oder Anwendungsfehler

Bei einem Hardware- oder Anwendungsfehler kann eine Wiederherstellung der Daten von einer Datensicherung in einigen synchronisierten Verzeichnisquellen erforderlich werden.

Nach der Datenwiederherstellung ist jedoch ein zusätzlicher Vorgang erforderlich, um sicherzustellen, dass die Synchronisierung normal fortgesetzt werden kann.

Die Konnektoren speichern in der Regel Daten über die letzte an die Meldungswarteschlange weitergegebene Änderung.

Mit diesen als Konnektorstatus bezeichneten Daten wird die nachfolgende Änderung bestimmt, die der Konnektor von seiner Verzeichnisquelle aus lesen muss. Wird die Datenbank einer synchronisierten Verzeichnisquelle von einer Sicherung wiederhergestellt, ist der Konnektorstatus unter Umständen nicht mehr gültig.

Windows-Konnektoren (Active Directory oder Windows NT) verwalten ebenfalls eine interne Datenbank. Bei dieser Datenbank handelt es sich um eine Kopie der synchronisierten Datenquelle. Mit ihr wird bestimmt, was sich in der verbundenen Datenquelle geändert hat. Es lässt sich leicht erkennen, dass die interne Datenbank nicht mehr gültig ist, sobald die verbundene Active Directory-Quelle oder das Windows NT-System von einer Sicherung wiederhergestellt wurde.

Im Allgemeinen kann die wiederhergestellte Datenquelle mit dem Befehl `idsync resync` wieder mit Daten gefüllt werden.

---

**HINWEIS** Eine Neusynchronisierung kann mit einer Ausnahme nicht zum Synchronisieren von Kennwörtern verwendet werden. Mit der Option `-i ALL_USERS` werden Kennwörter in Sun Java Systems Directory Server-Systemen ungültig, wenn die Datenquelle für die Neusynchronisierung Windows ist (und die SUL-Liste nur Active Directory-Systeme enthält).

---

Die Option `idsync resync` ist jedoch nicht für alle Situationen geeignet.

---

**VORSICHT** Stellen Sie vor dem Ausführen der unten beschriebenen Schritte sicher, dass die Synchronisierung angehalten wurde.

---

## Bidirektionale Synchronisierung

Als Vorgehensweise wird die Verwendung des Befehls `idsync resync` mit den entsprechenden Modifiziereinstellungen (den Synchronisierungseinstellungen entsprechend) empfohlen. Das Ziel des resync-Vorgangs sollte die wiederhergestellte Verzeichnisquelle sein.

## Unidirektionale Synchronisierung

Handelt es sich bei der wiederhergestellten Datenquelle um ein Synchronisierungsziel, können Sie dieselbe Vorgehensweise wie für die bidirektionale Synchronisierung wählen.

Wenn es sich bei der wiederhergestellten Datenquelle um eine Synchronisierungsquelle handelt, kann der Befehl `idsync resync` nach wie vor zum erneuten Füllen der wiederhergestellten Verzeichnisquelle verwendet werden. Es ist nicht erforderlich, die Einstellungen für den Synchronisierungsfluss in der Identity Synchronization für Windows-Konfiguration zu ändern. Mit `idsync resync` können Sie den Synchronisierungsfluss mit der Option `-o <Windows|Sun>` unabhängig von den festgelegten Synchronisierungsrichtungen konfigurieren.

Betrachten Sie das folgende Szenario als Beispiel:

Zwischen einem Sun Java Systems Directory Server und Active Directory wird eine bidirektionale Synchronisierung eingerichtet.

- Die Datenbank eines Microsoft Active Directory Server muss von einer Sicherung wiederhergestellt werden.
  - In Identity Synchronization für Windows wird diese Active Directory-Quelle für die SUL „AD“ konfiguriert.
  - Zwischen dieser Active Directory-Quelle und einer Sun Directory Server-Quelle wird eine bidirektionale Synchronisierung für Änderungs-, Erstellungs- und Löschvorgänge eingerichtet.
1. Synchronisierung anhalten: `idsync stopsync -w - -q -`
  2. Neusynchronisierung der Active Directory-Quelle und Neusynchronisierung von Änderungs-, Erstellungs- und Löschvorgängen: `idsync resync -c -x -o Sun -l AD -w - -q -`
  3. Synchronisierung neu starten: `idsync startsync -w - -q -`

## Verzeichnisquellenspezifische Wiederherstellungsvorgänge

### *Windows Active Directory*

Wenn Active Directory von einer Sicherung wiederhergestellt werden kann, führen Sie die im Abschnitt zur bidirektionalen bzw. unidirektionalen Synchronisierung beschriebenen Schritte aus.

Nach einem schwerwiegenden Fehler muss jedoch unter Umständen ein anderer Domänencontroller verwendet werden. Führen Sie in diesem Fall die Schritte zur Aktualisierung der Konfiguration des Active Directory-Konnektors aus:

1. Starten Sie die Identity Synchronization für Windows-Verwaltungskonsole.
2. Wählen Sie die Registerkarte „Konfiguration“.
3. Erweitern Sie den Verzeichnisquellenknoten.
4. Wählen Sie die entsprechende Active Directory-Quelle.
5. Klicken Sie auf „Controller bearbeiten...“
6. Wählen Sie den neuen Domänencontroller.  
  
Es wird empfohlen, den ausgewählten Domänencontroller als NT PDC FSMO-Rolleninhaber der Domäne festzulegen.
7. Speichern Sie die Konfiguration.

8. Halten Sie den Dienst *Identity Synchronization* auf dem Host an, auf dem der Active Directory-Konnektor ausgeführt wird.
9. Löschen Sie alle Dateien (jedoch nicht die Verzeichnisse) unter `<serverroot>/isw-<hostname>/persist/ADPxxx`, wobei xxx der aus Zahlen bestehende Teil des Active Directory-Konnektorbezeichners ist (Beispiel: 100, wenn der Active Directory-Konnektorbezeichner CNN100 lautet).
10. Starten Sie den Dienst *Identity Synchronization* auf dem Host, auf dem der Active Directory-Konnektor ausgeführt wird.
11. Führen Sie je nach Synchronisierungsfluss die Schritte im Abschnitt für die unidirektionale bzw. die bidirektionale Synchronisierung aus.

### *Sun Java System Directory Server*

Durch einen schwerwiegenden Fehler kann entweder die Retro Change Log-Datenbank oder die Datenbank mit den synchronisierten Benutzern (oder beides) beeinträchtigt werden.

#### 1. Retro Change Log-Datenbank

In der Retro Change Log-Datenbank sind unter Umständen Änderungen vorhanden, die der Directory Server-Konnektor nicht verarbeiten konnte. Eine Wiederherstellung der Retro Change Log-Datenbank ist nur sinnvoll, wenn die Sicherung einige nicht verarbeitete Änderungen enthält. Vergleichen Sie dazu den letzten Eintrag in der Datei `<serverroot>/isw-<hostname>/ADPxxx/accessor.state` mit der letzten Änderungsnummer in der Sicherung. Ist der Wert in `accessor.state` größer oder gleich der Änderungsnummer in der Sicherung, ist eine Wiederherstellung der Datenbank nicht erforderlich. Sie sollte aber neu erstellt werden.

Stellen Sie nach erneuter Erstellung der Retro Change Log-Datenbank sicher, dass `idsync prepds` ausgeführt wird, oder klicken Sie im Fenster der Sun Directory-Quelle der Identity Synchronization für Windows-Verwaltungskonsolle auf „Directory Server vorbereiten“.

Der Directory Server-Konnektor erkennt, dass die Retro Change Log-Datenbank neu erstellt wurde, und protokolliert eine Warnmeldung. Diese Meldung können Sie bedenkenlos ignorieren.

#### 2. Synchronisierte Datenbank

Ist für die synchronisierte Datenbank keine Sicherung verfügbar, muss der Directory Server-Konnektor neu installiert werden.

Wenn die synchronisierte Datenbank von einer Sicherung wiederhergestellt werden kann, führen Sie die im Abschnitt zur bidirektionalen bzw. unidirektionalen Synchronisierung beschriebenen Schritte aus.



# Aktualisierung der Identity Synchronization für Windows 1 2004Q3-Dokumentation

Auf die Dateien der Identity Synchronization für Windows-Online-Dokumentation können Sie über einen Browser zugreifen. Außerdem können Sie die gesamte Dokumentation im HTML-Format herunterladen.

Laden Sie diese Datei herunter und extrahieren Sie sie in folgendes Verzeichnis:

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

ServerRoot ist der Speicherort des Sun Java System Administration Server. Der tatsächliche ServerRoot-Pfad hängt von Ihrer Plattform, Installation und Konfiguration ab. Das ServerRoot-Verzeichnis enthält das startconsole-Programm.

Anschließend können Sie direkt vom Verzeichnis `<ServerRoot>/manual/en/isw/index.html` auf die Dokumentation zugreifen.

Oder wählen Sie zum Öffnen des Dokumentationssatzes auf der Serverkonsole den Befehl „Startseite der Dokumentation“ im Menü „Hilfe“.

## Ausführen von Identity Synchronization für Windows in einer Firewall-Umgebung

Sie können Identity Synchronization für Windows in einer Firewall-Umgebung ausführen. In diesem Abschnitt wird beschrieben, welche Serverports Sie durch die Firewall offen legen müssen:

- [Message Queue-Anforderungen](#)
- [Installationsprogrammanforderungen](#)
- [Core-Komponentenanforderungen](#)
- [Konsolenanforderungen](#)
- [Konnektoranforderungen](#)
- [Directory Server-Plug-In-Anforderungen](#)

## Message Queue-Anforderungen

Standardmäßig verwendet Message Queue dynamische Ports für alle Dienste mit Ausnahme der Portzuordnung. Um durch eine Firewall auf den Message Queue-Broker zuzugreifen, sollte der Broker für alle Dienste feste Ports verwenden.

Nach Installation des Core müssen Sie die Brokerkonfigurationseigenschaften `img.<Dienstname>.<Protokolltyp>.port` festlegen. Legen Sie insbesondere die Option `img.ssljms.tls.port` fest. Weitere Informationen finden Sie im *Sun Java™ System Message Queue Administrator's Guide*.

## Installationsprogrammanforderungen

Das Identity Synchronization für Windows-Installationsprogramm muss mit dem Directory Server als Konfigurationsverzeichnis kommunizieren können.

- Bei Installation eines Active Directory-Konnektors muss das Installationsprogramm in der Lage sein, den LDAP-Port (Port 389) von Active Directory zu kontaktieren.
- Wenn Sie einen Directory Server-Konnektor oder ein Directory Server-Plug-In (Unterkomponente) installieren, muss das Installationsprogramm Kontakt zum LDAP-Port (Standardport 389) von Directory Server aufnehmen können.

## Core-Komponentenanforderungen

Message Queue, der Systemmanager und die Befehlszeilenschnittstelle müssen den Directory Server erreichen können, auf dem die Identity Synchronization für Windows-Konfiguration gespeichert ist.

## Konsolenanforderungen

Die Identity Synchronization für Windows-Konsole muss folgende Komponenten erreichen können:

- Active Directory über LDAP (Port 389) oder LDAPS (Port 636)
- Active Directory Global Catalog über LDAP (Port 3268) oder LDAPS (Port 3269)
- Jeden Directory Server über LDAP oder LDAPS
- Sun Java SystemAdministration Server
- Message Queue

## Konnektoranforderungen

Alle Konnektoren müssen in der Lage sein, mit Message Queue zu kommunizieren. Darüber hinaus bestehen folgende Anforderungen:

- Der Active Directory-Konnektor muss auf den Active Directory-Domänencontroller über LDAP (Port 389) oder LDAPS (Port 636) zugreifen können.
- Der Directory Server-Konnektor muss auf Directory Server über LDAP (Standardport 389) oder LDAPS (Standardport 636) zugreifen können.

## Directory Server-Plug-In-Anforderungen

Jedes Directory Server-Plug-In muss den Serverport des Directory Server-Konnektors, der bei Installation des Konnektors ausgewählt wurde, erreichen können. Plug-Ins, die in Directory Server Master-Replikaten ausgeführt werden, müssen in der Lage sein, eine Verbindung zu LDAP (Port 389) oder LDAPS (Port 636) von Active Directory herzustellen. Die Plug-Ins, die in anderen Directory Server-Replikaten ausgeführt werden, müssen die Directory Server-LDAP- oder LDAPS-Ports des Masters erreichen können.

---

# Bekannte Probleme und Einschränkungen

Dieser Abschnitt enthält eine Liste der bekannten Probleme in Identity Synchronization für Windows 1 2004Q3. Die folgenden Produktbereiche wurden hierbei berücksichtigt:

- [Installation und Deinstallation](#)
- [Konnektoren und Plug-Ins](#)
- [Konsole und Befehlszeile](#)
- [Kennwortsynchronisierung](#)
- [Sun Java System Message Queue](#)
- [Allgemeine Probleme](#)

# Installation und Deinstallation

## **Anweisungen zum manuellen Bereinigen der Produktregistrierung. (5050004)**

Wenn Sie Verweise auf Identity Synchronization für Windows aus der Produktregistrierung entfernen müssen, verwenden Sie die in Abschnitt „*What to Do if the 1.0 Uninstallation Fails*“ im Kapitel 7 des *Identity Synchronization for Windows Installation and Configuration Guide* beschriebene Vorgehensweise für die Windows NT- und Windows 2000-Plattform.

## **Solaris-Skripts funktionieren nicht, wenn Sie den Core in einem Verzeichnis speichern, dessen Name Leerzeichen enthält. (4801643)**

Die Befehlszeilen-Skripts funktionieren unter Solaris nicht, wenn Sie den Identity Synchronization für Windows-Core in einem Verzeichnis speichern, dessen Pfadname ein Leerzeichen enthält.

## **Message Queue-Broker kann nicht starten, wenn der Basis-DN Leerzeichen enthält. (4892332 und 4892490)**

Installieren Sie den Core nicht mit einem Suffix, der Leerzeichen enthält. Andernfalls tritt bei der Authentifizierung durch den Message Queue-Broker ein Fehler auf.

## **Nebeneffekte beim Installieren des Core mit einer vorhandenen Message Queue-Instanz. (4882194)**

Durch Installieren des Core mit einer vorhandenen Message Queue-Broker-Instanz kann die vorhandene Instanz beeinträchtigt werden.

Eine vorhandene Konfiguration wurde beispielsweise wie folgt geändert:

- Die Datei `/etc/imq/imqbrokerd.conf` wurde geändert, sodass der Broker beim Start automatisch startet. Dadurch wurde verhindert, dass andere Broker-Instanzen, die vom Skript `/etc/init.d/imq` gestartet wurden, beim Neustart gestartet werden können.

## **Message Queue-Broker erfordert mindestens 512 MB Speicherplatz. (4819519)**

Der Message Queue-Broker erfordert mindestens 512 MB Speicherplatz. Da der Broker als Bestandteil des Core installiert wird, sollte der Rechner, auf dem der Core installiert ist, mindestens 1 GB RAM aufweisen.

## **Deinstallation von Plug-Ins bei Entfernen des Deinstallationsprogramms durch eine Installation mehrerer Directory Server-Instanzen. (4916035)**

Mehrere Plug-Ins können nicht deinstalliert werden, wenn zwei Directory Server-Instanzen dasselbe Installationsrootverzeichnis für das Dateisystem besitzen (z. B.

`/usr/sunone/servers/slapd-foxhead` und `/usr/sunone/servers/slapd-foxhead2`).

*Umgehung des Problems*

1. Öffnen Sie die Directory Server-Konsole (für den Directory Server, auf dem Sie das Plug-In installiert haben).
2. Klicken Sie auf die Registerkarte „Konfiguration“.
3. Doppelklicken Sie auf den Ordner `Plug-Ins`, um die Plug-In-Struktur zu erweitern.
4. Klicken Sie auf `pswsync` und deaktivieren Sie das Kontrollkästchen „Plug-In aktivieren“.
5. Starten Sie Directory Server neu.

**Unbestimmtes Verhalten des Active Directory-Konnektors, wenn die Installation vorzeitig beendet wird und eine Neuinstallation versucht wird. (5038905)**

Wird das Installationsprogramm abgebrochen, während der Konnektor konfiguriert wird, steht bei erneuter Ausführung des Installationsprogramms die Konnektor-Option für die Installation nicht zur Verfügung.

*Umgehung*

Führen Sie an der Eingabeaufforderung den Befehl `idsync resetconn` aus, um die Konfiguration des Konnektors zurückzusetzen. Führen Sie anschließend das Installationsprogramm erneut aus, um den Konnektor neu zu installieren. Weitere Informationen zum Ausführen des Befehls `idsync resetconn` finden Sie im *Sun Java System Identity Synchronization für Windows Installation and Configuration Guide*.

**Zum Produkt gehörende Registrierungsschlüssel werden bei der Deinstallation nicht entfernt. (5045237)**

Nach der Deinstallation des Core werden die zu Sun Java System Identity Synchronization für Windows gehörenden Knoten in der Produktregistrierungsdatei nicht entfernt. Um das Produkt erfolgreich zu deinstallieren, müssen Sie die Knoten manuell aus den Produktregistrierungsschlüsseln löschen. Weitere Informationen zum Löschen dieser Produktregistrierungsschlüssel finden Sie im *Identity Synchronization für Windows Installation and Configuration Guide*. Diese Situation tritt nur unter Solaris 8 auf.

**Mit Identity Synchronization für Windows verbundene Referenzen werden in der Konsole angezeigt, wenn der Core ohne Verbindung zur Konfigurationsregistrierung deinstalliert wird. (5049700)**

Es wird eine Fehlermeldung angezeigt, wenn die Konsole nach einer blinden Deinstallation (ohne Verbindung zur Konfigurationsregistrierung) von Identity Synchronization für Windows gestartet wird.

**Das Temp-Verzeichnis, in dem Installationsprotokolle gespeichert werden, kann ein verborgenes Verzeichnis sein. (5051905)**

In einigen Windows-Systemen kann das Verzeichnis unter C:\ Dokumente und Einstellungen > Administrator > Lokale Einstellungen verborgen sein.

*Umgehung*

Zum Anzeigen des Verzeichnisses Lokale Einstellungen und des Unterverzeichnisses Temp wählen Sie die Windows Explorer-Option Versteckte Dateien anzeigen. Alternativ können Sie an der Eingabeaufforderung auch entweder `cd %TEMP` oder `cd %TMP` eingeben, um die Protokolldateien der Installation im Verzeichnis anzuzeigen. Die Protokolldateien können dann mit Notepad angezeigt werden.

**Die Authentifizierung für Message Queue schlägt fehl, wenn das Rootsuffix Leerzeichen enthält. (4892903)**

Aufgrund einer Einschränkung von Message Queue muss die Identity Synchronisation für Windows-Konfiguration in einem Rootsuffix ohne Leerzeichen gespeichert werden.

*Umgehung*

Erstellen Sie ein neues Rootsuffix, um die Identity Synchronisation für Windows-Konfiguration vor dem Installieren des Core zu speichern.

**Nach einer fehlgeschlagenen Directory Server-Plug-In-Installation zeigt die Aufgabenliste an, dass die Installation des Plug-Ins abgeschlossen ist. (5081912)**

In bestimmten Fällen zeigt die Aufgabenliste mitunter an, dass das Directory Server-Plug-In installiert wurde, obwohl die Installation eigentlich fehlschlug.

**Bei der Deinstallation eines Konnektors zeigt das Deinstallationsprogramm nicht präzise an, wie viel Speicherplatz wiederhergestellt wird. (5081823)**

Das Deinstallationsprogramm zeigt bei der Deinstallation eines Konnektors fälschlicherweise 0 Byte (als Anzahl Byte, die nach der Deinstallation wiederhergestellt sind) an. Beim Anzeigen der Eigenschaften des Speichers wird der tatsächliche wiederhergestellte Speicherplatz nicht mit null angegeben.

**Das Installationsprogramm erzwingt die Installation von Komponenten nicht in demselben Verzeichnis, in dem sich das Installationsverzeichnis des Directory Server-Plug-Ins befindet. (5080178)**

Wurde das Directory Server-Plug-In als erste Komponente auf einem Computer installiert, müssen alle nachfolgenden Komponenten auf diesem bestimmten Computer in demselben Installationsverzeichnis (des Directory Server-Plug-Ins) installiert werden. Das Installationsprogramm erzwingt diese Kriterien bei der Installation jedoch nicht.

### **Das Deinstallationsprogramm zeigt mitunter falsche Informationen beim Deinstallieren von Komponenten an. (5079489)**

Wird ein Konnektor auf einem Computer deinstalliert, auf dem die Core-Komponente nicht installiert ist, meldet das Installationsprogramm fälschlicherweise, dass es die Core-Komponente deinstalliert. Diese Meldung kann ignoriert werden. Verweise auf die Identity Synchronization für Windows-Konsole werden nicht entfernt, wenn ein Deinstallationsvorgang durchgeführt wird und das Konfigurationsverzeichnis nicht vorhanden ist. (5077156)

Wird die Option zum Deinstallieren des Produkts ohne Konfigurationsverzeichnis ausgewählt, behält die Sun Server-Konsole alle Verweise auf die Identity Synchronization für Windows-Konsole bei. Nach Deinstallation des Produkts ist das Symbol für Identity Synchronization für Windows nach wie vor in der Verzeichnisstruktur vorhanden. Beim Versuch, die Konsole anzuzeigen, tritt ein Fehler auf. Weitere Informationen zum Entfernen der Verweise auf die Konsole finden Sie im Abschnitt zum manuellen Deinstallieren der Konsole in Kapitel 8 des *Identity Synchronization for Windows Installation and Configuration Guide*.

### **Bei der Deinstallation werden das Verzeichnis `server-root/isw-*/lib` und die `jar`-Dateien nicht entfernt. (5038284)**

Beim Deinstallieren wird das Verzeichnis `lib` mit den `*.jar`-Dateien nicht entfernt. Diese Dateien sowie das Verzeichnis müssen manuell gelöscht werden.

### **Unbestimmtes Verhalten des Active Directory-Konnektors, wenn der Installationsvorgang abgebrochen und eine Neuinstallation durchgeführt wird. (5038905)**

Wenn die Installation des Active Directory-Konnektors abrupt abgebrochen und dann versucht wird, den Konnektor erneut zu installieren, wird vom Active Directory-Konnektor ein falscher Status angegeben, nämlich ‚Installiert‘. Dieser Status bleibt unverändert und es wird weder die Synchronisierung durchgeführt noch ist die Neuinstallation des Active Directory-Konnektors möglich.

#### *Umgehung*

Zur Neuinstallation des Konnektors muss der Befehl `idsync resetconn` ausgeführt werden. Weitere Informationen zum Ausführen des Befehls `idsync resetconn` finden Sie im *Identity Synchronization for Windows Installation and Configuration Guide*.

### **Die Identity Synchronization für Windows-Installation schlägt bei Directory Server 5.2p3 fehl (Installation mit Sun Java Enterprise System 3). (5092530)**

Die Installation des Identity Synchronization für Windows-Core-Produkts ist bei Directory Server 5.2 P3 oder höher nicht möglich. Identity Synchronization für Windows 1 2004Q3 unterstützt Sun Java Enterprise System 3 (Directory Server 5.2 P3) nur als Datensynchronisierungsquelle.

**In der Installationsliste wird auch nach der Installation eine Aufforderung zur Installation des Directory Server-Plug-Ins auf dem sekundären Master ausgegeben. (5096593)**

Die Aufgabenliste ist nahezu immer richtig, in einigen wenigen Fällen werden jedoch möglicherweise die erforderlichen Schritte nicht angegeben bzw. es wird nicht erkannt, dass einige Schritte bereits durchgeführt wurden. So geht aus der Aufgabenliste beispielsweise nicht immer hervor, welche Directory Server-Plug-Ins bereits installiert wurden und welche installiert werden müssen.

**Bei der Identity Synchronization für Windows-Installation auf einem FAT32-System sind keine ACLs (Access Control Lists, Zugriffsteuerungslisten) vorhanden. (5097751)**

Wenn nach der Installation von Identity Synchronization für Windows auf einem Laufwerk mit FAT32-Formatierung versucht wird, in den ACLs nach Ordnern und Dateien zu suchen, ist dies nicht möglich, da keine ACLs vorhanden sind. Von der Installation auf anderen Partitionen als NTFS-Partitionen wird abgeraten.

**Bei Verwendung der ZIP-Version von Directory Server ist die ausschließliche Plug-In-Deinstallation unter Umständen nicht möglich. (5101589)**

Wenn versucht wird, nur die Plug-Ins zu deinstallieren, schlägt dieser Vorgang fehl, wenn hierfür das komprimierte Archivpaket von Directory Server verwendet wird.

**Installation schlägt fehl, wenn nach Aufforderung ein Multibyte-Administratorname verwendet wird. (5109332)**

Falls während der auf den Core bezogenen Installation nach Aufforderung ein Multibyte-LDAP-Administratorname eingegeben wird, schlägt der Vorgang fehl. Die Fehlermeldung „The installer cannot upload the schema file /var/opt/isw/SUNWisw/misc/40so-psw.out.ldif. Check the installer's log file for further details. (Das Installationsprogramm kann die Schemadatei /var/opt/isw/SUNWisw/misc/40so-psw.out.ldif nicht laden. Weitere Informationen finden Sie in der Protokolldatei des Installationsprogramms)“ wird angezeigt. Der Installationsvorgang wird abgebrochen und das Dialogfeld wird abrupt geschlossen.

*Umgehung*

Stellen Sie sicher, dass Sie für den Installationsvorgang den standardmäßigen LDAP-Administrationsnamen „admin“ verwenden, damit dieses Problem nicht auftritt. Falls eine vorherige Installation fehlgeschlagen ist, starten Sie das Installationsprogramm neu und installieren Sie den Core unter Verwendung des standardmäßigen Administrationsnamens erneut. Möglicherweise wird die Meldung „Core files have been found on your machine (Auf Ihrem Computer wurden Core-Dateien gefunden.)“ angezeigt. Diese Meldung kann bedenkenlos ignoriert werden. Sie können mit dem Installationsvorgang fortfahren.



# Konnektoren und Plug-Ins

**Durch Löschen eines bereits vorhandenen Eintrags wird die NT-Konnektorsynchronisierung gestartet. (4864009)**

Installationen mit vorhandenen Windows-Benutzern (Active Directory oder NT) müssen vor der Synchronisierung den Befehl `idsync resync` ausführen, um undefiniertes Verhalten zu verhindern (z. B. vorhandene Windows-Benutzer werden jederzeit mit Directory Server synchronisiert).

**Neustart inaktiver Konnektoren. (4938309)**

Wenn das zentrale Fehlerprotokoll eine Meldung wie Keine Antwort von Konnektor [CNN100] seit 10 Minuten anzeigt, müssen Sie unter Umständen den Identity Synchronization für Windows-Dämon bzw. Dienst anhalten und neu starten, auf dem der Konnektor ausgeführt wird.

## Umgehung

- Führen Sie unter Solaris den Befehl `/etc/init.d/isw stop` und anschließend den Befehl `/etc/init.d/isw start` aus.
- Starten Sie unter Windows den Sun Java System Identity Synchronization für Windows-Dienst neu.

**Neustart von Directory Server nach Aktivieren des Secure Sockets Layer für das Directory Server-Plug-In. (4944804)**

Nach Aktivieren von Secure Sockets Layer (SSL) für das Directory Server-Plug-In (Unterkomponente) und Hinzufügen des Active Directory CA-Zertifikats zur Zertifikatsdatenbank von Directory Server müssen Sie Directory Server neu starten. Andernfalls tritt bei der bedarfsgesteuerten Synchronisierung unter Umständen ein Fehler bei der Authentifizierung eines Benutzers auf, dessen Kennwort in Active Directory geändert wurde (siehe Beispielprotokollmeldungen).

**Falls es bei Suchen in Active Directory zu Zeitüberschreitungen kommt, sollte das Suchlimit von Administratoren erhöht werden. (4881182)**

Wenn das Active Directory-Fehlerprotokoll einen Zeitüberschreitungsfehler für einen Konnektor ausgibt, verwenden Sie den Befehl des Windows 2000 Resource Kit `ntdsutil` zur maximalen Erhöhung des Zeitlimits wie folgt:

```
C: dif>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
```

**Attribute mit Binärwerten, die ohne den Untertyp „;binary“ erstellt wurden, werden von Sun Java System Directory Server nicht verarbeitet. (5029226)**

Bestimmte Attribute wie `userCertificate` erfordern die Option „;binary“ zum Zeitpunkt der Erstellung. Identity Synchronization für Windows kann die Werte dieser Attribute zwar synchronisieren, setzt die Option „;binary“ jedoch nicht auf die Erstellungszeit. Für Clients, die mit Sun Java System Directory Server kommunizieren, können daraus Probleme entstehen. Sun Java System Directory Server gibt ein solches Attribut nicht zurück, wenn das Attribut ohne die Option „;binary“ erstellt wurde und der Client das Attribut mit der Option „;binary“ anfordert.

**Identity Synchronization für Windows prüft die beim Erstellen des Attributs `user_name` verwendete Anzahl Zeichen nicht. (5021886)**

Unter NT SAM sind 20 Zeichen für das Attribut `user_name` zulässig. Im Gegensatz dazu besitzt Sun Java Directory Server keine solche Einschränkung für die Erstellung des Benutzernamens. Der dem Attribut `user_name` unter NT SAM zugeordnete Eintrag kann nicht verwendet werden, obwohl er erfolgreich von NT SAM an Sun Java Directory Server übergeben wird. Wenn die Eigenschaften des Eintrags unter NT SAM bearbeitet oder angezeigt werden, wird eine Fehlermeldung ausgegeben.

## Konsole und Befehlszeile

**Führen Sie den Befehl `idsync prepds` aus, wenn Retro Change Log-Datenbankdateien neu erstellt werden, beschädigt oder nicht vorhanden sind. (4921114 und 4832355)**

Sobald die Retro Change Log-Datenbank (RCL) gelöscht oder beschädigt wird, gibt Directory Server oder der Directory Server-Konnektor Warnungen aus. Wenn diese Warnungen angezeigt werden, müssen Sie die Retro Change Log-Datei neu erstellen und den Befehl `idsync prepds` erneut ausführen, bevor die Synchronisierung wieder aufgenommen wird.

**Die Auswahl der Schaltfläche „Durchsuchen“ für Basis-DN ändert sich nach Wahl eines neuen Namenskontexts nicht. (4944711)**

Wenn Sie Identity Synchronization für Windows von der Konsole aus auf mehr als eine Directory Server-Quelle und mehr als zwei Active Directory (AD)-Quellen konfigurieren, zeigt die Auswahl der Schaltfläche „Durchsuchen“ für die Basis-DN beim Konfigurieren einer neuen synchronisierten Benutzerliste (Synchronized Users List, SUL) unter Umständen die entsprechenden Directory Server- oder Active Directory-Quellen nicht richtig an.

### *Umgehung*

Geben Sie den Basis-DN-Namen manuell in das Basis-DN-Feld ein.

**Der Schemahost der Konsole sollte auf das Konfigurationsverzeichnis verweisen. (4877996)**

Beim Festlegen eines Schemahosts wird empfohlen, nur das Core-Konfigurationsverzeichnis zu verwenden. Verwenden Sie keinen eigenständigen Directory Server oder ein anderes Konfigurationsverzeichnis auf einem Remote-Computer.

**Das Fenster „Konsolenstatus“ bietet keinen 508-Zugang für die Anzeige von Protokolldateien. (4874361)**

Die Protokolldateianzeige im Fenster „Konsolenstatus“ erlaubt keine Schnittstelle ohne Maus zur Anzeige von Protokolldateien.

### *Umgehung*

Um die Protokolldateien anzuzeigen, kopieren Sie sie in einen beliebigen Texteditor (außerhalb der Konsolenprotokollanzeige).

**Der Konsolenstatus für Message Queue gibt den tatsächlichen Status der Systemkomponenten nicht korrekt wieder. (4937312)**

Wenn die Netzwerkverbindung zwischen der Konsole und MessageBroker unterbrochen wird, gibt die Konsole den Status der Systemkomponenten unter Umständen falsch wieder.

#### *Umgehung*

Wenn Netzwerkprobleme auftreten, starten Sie die Konsole unbedingt neu. Sie können auch den Befehl `idsync printstat` ausführen, um eine genauere Anzeige des Meldungswarteschlangenstatus zu erhalten.

**Beim Hinzufügen einer neuen Directory Server-Datenquelle fordert eine Meldung zur Vorbereitung des Directory Server auf, obwohl der Directory Server bereits vorbereitet wurde. (5029558)**

Bei jedem Erstellen einer neuen Sun Java System Directory Server-Quelle werden Sie zur Vorbereitung der Directory Server-Quelle aufgefordert. Wenn Sie die Verzeichnisquelle bereits vorbereitet haben, können Sie bedenkenlos auf „Nein“ klicken.

**Beim Ausführen des CLI-Befehls „resetconn“ wird die Meldung „Resetting... (Wird zurückgesetzt...)“ angezeigt. Das Zurücksetzen des Kennworts schlägt fehl, und es werden alle Daten über die Directory Server-Quelle, Konfiguration usw. gelöscht. (5039655)**

Wenn die Befehlszeilenfunktion `resetconn` ausgeführt wird, sollte die Konsole nicht aktiv sein. Wenn Sie die Konsole nicht vor dem Ausführen des Befehls beenden, wird die Meldung „Resetting... (Wird zurückgesetzt...)“ angezeigt. Beenden Sie nun die Konsole und starten Sie sie neu.

**Beim Ausführen des Befehls „startsync“ tritt ein Fehler auf. Die Fehlermeldung „Failed to start synchronization for some of the requested directory sources... (Synchronisation konnte für einige angeforderte Verzeichnisquellen nicht gestartet werden)“ wird angezeigt. (5050443)**

Unter bestimmten Bedingungen (z. B. bei unzureichendem Arbeitsspeicher) kann es vorkommen, dass die Befehlszeile oder die Managementkonsole einen erfolgreichen Start der Synchronisierung meldet, auch wenn einige Komponenten die Synchronisierung nicht starten konnten. Prüfen Sie bei Synchronisierungsproblemen das Fehlerprotokoll auf Meldungen, die sich auf den Speicherplatz beziehen.

**Ein Attribut mit Parametern schlägt fehl, wenn mehrere Werte für einwertige Attribute angegeben sind. (5069907)**

Die Synchronisierung schlägt fehl, wenn für einwertige Attribute statt eines Wertes mehrere Werte angegeben sind. Beim Speichern der Werte auf dem Directory Server wird weder ein Fehler noch eine Warnmeldung angezeigt.

**Beim Ausführen des idsync-Befehls werden die Kennwörter unverschlüsselt auf dem Bildschirm angezeigt. (4900126)**

Wenn der Befehl `idsync` zur Eingabe der `bind`- und `config`-Kennwörter auffordert, werden diese bei der Eingabe unverschlüsselt als Text angezeigt.

*Umgehung*

Um zu verhindern, dass Kennwörter auf dem Bildschirm angezeigt werden, speichern Sie jedes Kennwort in einer geschützten Datei und leiten Sie diese dann an die Befehlszeile weiter. Wenn die „-“-Option für ein Kennwortargument angegeben wird, fordert der `idsync`-Befehl zur Eingabe der Kennwortwerte in der Reihenfolge auf, in der die Optionen in der Befehlszeile angezeigt werden. Lautet das Administratorkennwort beispielsweise `adminPw` und das Konfigurationskennwort `configPw`, erstellen Sie eine Datei (`kennwort.txt`) mit folgendem Inhalt:

```
adminPw
```

```
configPw
```

Führen Sie anschließend `idsync printstat -w - -q - < kennwort.txt` für den Befehl aus.

**Fehler beim Laden von Protokolldateien. (5091787)**

In einigen Fällen wird beim Laden der Datei `audit.log` über die Registerkarte mit dem „Status“ der Konsole ein Fehler ausgegeben, der in etwa wie folgt lautet: ‚Protokolleinträge konnten aufgrund eines unbekannten Fehlers nicht abgerufen werden. Der Admin-Server muss möglicherweise neu gestartet werden.‘

*Umgehung*

Wenn zu einem späteren Zeitpunkt versucht wird, die Datei zu laden, wird die Datei `audit.log` bei Zugriff geladen.

**Durch den Befehl „preps“ wird bei der MMR-Einrichtung während der Migration eine Fehlermeldung ausgegeben. (5093124)**

Bei der Migration einer replizierten Umgebung wird von `idsync preps` unter Umständen fälschlicherweise gemeldet, dass die Schemareplikation fehlgeschlagen ist. (Die Fehlermeldung könnte beispielsweise wie folgt lauten: ‚Der bevorzugte Sun Java System Directory Server unter `ldap://preferred.example.com:389` konnte die am sekundären Sun Java(TM) System Directory Server unter `ldap://secondary.example.com:389` vorgenommenen Schemaänderungen nicht replizieren. Überprüfen Sie die Replikationseinstellungen.‘) Führen Sie in diesem Fall `idsync preps` mit denselben Argumenten erneut aus. Sie müssen die Replikationseinstellungen nur dann überprüfen, wenn die zweite Ausführung von `idsync preps` zu derselben Fehlermeldung führt.

**Wenn Reflection X 10.0 für den Zugriff verwendet wird, kann die Konsole möglicherweise nicht verwendet werden. (5095013)**

Einige der Dialogfelder können möglicherweise nicht verwendet werden, da die Schaltflächen oder Textfelder nicht angezeigt werden können und die Größe der Dialogfelder nicht geändert werden kann.

### **In den Protokollmeldungen der Konsole werden beschädigte Multibytezeichen angezeigt. (6174184)**

Es werden nur dann Multibytezeichen im Protokoll gemeldet, wenn in der synchronisierten Benutzerliste ein Multibyte-Name verwendet oder ein Multibytesuffix synchronisiert wird. Öffnen Sie die Protokolldatei (`/var/opt/SUNWiw/logs/central/error.log`) in einem Anzeigeprogramm, das UTF-8-codierte Dokumente anzeigen kann, um die Protokollmeldungen ordnungsgemäß anzuzeigen.

### **Die Befehle „startsync“ und „stopsync“ werden nicht ordnungsgemäß ausgeführt, wenn das Konfigurationskennwort geändert wurde. Es wird eine Fehlermeldung angezeigt. (6175396)**

Wenn das Identity Synchronization für Windows-Konfigurationskennwort mit dem Befehl `idsync changepw` geändert und der Computer nicht neu gestartet wurde, werden die Befehle `idsync startsync` und `stopsync` nicht ordnungsgemäß ausgeführt. Die Befehle zeigen eine Meldung an wie beispielsweise „The received message was not encrypted. (Die erhaltene Nachricht war nicht verschlüsselt)“ und geben den Beendigungscode 1 aus.

Obwohl die Fehlermeldung angezeigt wird, wird der Vorgang zum Starten bzw. Anhalten der Synchronisierung nicht ausgeführt. Führen Sie den Befehl `idsync printstat` aus, um dies zu überprüfen. Stellen Sie jedoch sicher, dass der Computer nach jedem Ändern des Konfigurationskennworts neu gestartet wird, damit dieses Problem nicht auftritt.

## Kennwortsynchronisierung

### **Probleme mit der Kennwortrichtlinie. (4834865 und 4811572)**

Durch Kennwortrichtlinien, die in verschiedenen Verzeichnissen verwendet werden, können Synchronisationsfehler entstehen. Ein Beispiel sind die Kennwortlänge und die mindestens erforderlichen und höchstens zulässigen Zeichen. Eine nicht kompatible Kennwortrichtlinie muss von Administratoren manuell geändert werden, damit sie mit den Richtlinien anderer Systeme übereinstimmt.

### **Zusammengehörige Attribute oder Kennwörter, die gleichzeitig geändert werden, werden unter Umständen nicht ordnungsgemäß synchronisiert. (4854183 und 4808601)**

Wenn ein Eintrag, der zwischen zwei Verzeichnisquellen synchronisiert wird, und gleichzeitig Änderungen an einem Attribut vorgenommen werden, wird das Attribut unter Umständen nicht ordnungsgemäß synchronisiert. Schauen Sie sich dazu folgendes Beispiel an:

- Peter Becker ändert seine Telefonnummer in Active Directory (AD) in 551111.
- Diese Änderung wird an den Directory Server weitergegeben. Bevor die Änderung dort ankommt, legt ein Administrator Peter Beckers Telefonnummer in Directory Server fälschlicherweise auf 551112 fest.

- Als Nächstes wird die in Active Directory vorgenommene Änderung in Directory Server übernommen und Peter Beckers Telefonnummer wird auf 551111 festgelegt.
- Ebenso wird die in Directory Server vorgenommene Änderung in Active Directory übernommen und Beckers Telefonnummer wird auf 551112 festgelegt.

Die beiden Verzeichnisquellen haben die Werte getauscht und sind nicht mehr synchronisiert.

Ähnlich verhält es sich, wenn das Kennwort eines Benutzers in Active Directory (AD) und Directory Server etwa zur gleichen Zeit geändert wird. Das Kennwort wird dann unter Umständen in bestimmten Situationen nicht ordnungsgemäß synchronisiert.

Bei System mit geringer Auslastung müssten die Kennwortänderungen im Abstand von wenigen Sekunden vorgenommen werden, damit sie nicht mehr synchronisiert sind. Obwohl eine solche Situation auch auftreten kann, wenn das Active Directory-Kennwort *nach* Festlegen auf den Directory Server-Wert geändert wird, ist dies unwahrscheinlich. Das Active Directory-Kennwort müsste innerhalb weniger Millisekunden geändert werden, nachdem es auf den Directory Server-Wert festgelegt wurde.

#### **Arbeiten mit der Active Directory-Funktion „Benutzer muss Kennwort bei der nächsten Anmeldung ändern“ (4827180)**

Ändert ein Administrator das Kennwort eines Benutzers in Active Directory (AD) und gibt die Option „Benutzer muss das Kennwort bei der nächsten Anmeldung ändern“ an, wird die Kennwortänderung erst mit Directory Server synchronisiert, wenn der Benutzer sich anmeldet und das Kennwort ändert.

Unter folgenden Umständen schlägt eine Benutzerauthentifizierung fehl:

1. Ein Benutzer ändert sein Kennwort in Active Directory. (Das Kennwort wird von Directory Server übernommen und das Directory Server-Kennwort wird ungültig.)
2. Der Administrator setzt das Kennwort des Benutzers zurück und setzt das Kennzeichen „Benutzer muss das Kennwort bei der nächsten Anmeldung ändern“.
3. Versucht der Benutzer sich bei Directory Server mit dem in Schritt 1 oder 2 festgelegten Kennwort anzumelden, schlägt die Anmeldung fehl. Durch Ändern des Kennworts in Active Directory oder Directory Server wird der Directory Server-Kennwortwert aktualisiert.

**Durch Angabe eines nicht-ASCII-Kennworts in NT oder Active Directory mit aktiviertem 7-Bit-Prüf-Plug-In wird verhindert, dass das Kennwort mit Directory Server synchronisiert wird. (4817344)**

In Directory Server wird das 7-Bit-Prüf-Plug-In (Unterkomponente) für Benutzerkennwort-Attributwerte standardmäßig aktiviert. Siehe auch <http://docs.sun.com/source/816-6699-10/pluginattr.html>

Wenn Sie Kennwörter von Windows in Directory Server synchronisieren, die nicht 7-Bit betragen, und dieses Plug-In anschließend aktivieren und für Benutzerkennwort-Attributwerte konfigurieren, schlägt die Synchronisation fehl.

Seien Sie vorsichtig beim Synchronisieren von Kennwörtern mit nicht-ASCII-Zeichen, da die Zeichenkodierung des Kennwortwerts nicht dauerhaft ist. Daher müssen Windows-seitige Clients und Directory Server-Clients beim Ändern von Kennwörtern (und bei Authentifizierungen) die gleiche Zeichenkodierung verwenden. Andernfalls schlägt der Vorgang fehl.

**Mehrere Kennwortwerte werden nicht unterstützt. (4807350)**

Mehrere Kennwortwerte werden nicht unterstützt.

**Mit dem resync-Befehl wird nicht automatisch der Prozess zur Neusynchronisation wieder aufgenommen, wenn der Systemmanager neu gestartet wird. (5077660)**

Wird der resync-Befehl ausgeführt und der Systemmanager neu gestartet, wird die Neusynchronisation nicht automatisch wiederhergestellt und der Prozess neu gestartet.

**Bei Durchführung einer Neusynchronisation werden mitunter Erstellungsattribute gelöscht. (5085134)**

**Gleichzeitige Aktualisierungen eines Attributs werden nicht synchronisiert. (5077760)**

Dieses Problem tritt auf, wenn ein Wert zu einem Attribut hinzugefügt wird und etwa gleichzeitig ein anderer Wert zu dem Attribut in einem entsprechenden Remoteverzeichniseintrag hinzugefügt wird. Das Attribut wird unter Umständen nicht synchronisiert.

**Beim Durchführen einer Neusynchronisation werden die LINK-Aktionen nicht vom Directory Server-Konnektor empfangen, auch wenn der Neusynchronisationsvorgang abgebrochen wurde. (4985505)**

Wenn `resync -c -o Sun` ausgeführt wird, werden die LINK-Aktionen an den Directory Server gesendet, nachdem neue Benutzer in Active Directory angelegt wurden. Diese LINK-Aktionen werden nicht vom Directory Server empfangen, obwohl der Resync-Vorgang abgebrochen wurde. Momentan werden die LINK-Aktionen in demselben MQ-Thema veröffentlicht wie alle `resync/linkusers`-Aktionen.



**Aufgrund eines bekannten Problems im Directory Server Retro Change Log-Plug-In werden in Directory Server gelöschte Einträge unter Umständen nicht mit Active Directory synchronisiert. (5077814)**

Das Directory Server Retro Change Log-Plug-In speichert den `dspswuserlink` möglicherweise nicht im Plug-In-Eintrag für einen gelöschten Eintrag. In diesem Fall wird keine Synchronisation für den gelöschten Eintrag des Directory Server-Eintrags mit Active Directory durchgeführt.

*Umgehung*

Um dieses Problem zu beheben, muss der Directory Server mit dem entsprechenden Patch aktualisiert werden. Informationen darüber, welche Patches zur Behebung des Problems erforderlich sind, finden Sie im Abschnitt „[Sun Java System Directory Server 5 2004Q2 Retro Change Log-Patch](#)“.

## Sun Java System Message Queue

**Der Systemmanager kann keine Verbindung zu Message Queue herstellen. (4907711)**

Der Systemmanager kann keine Verbindung zu Message Queue herstellen, obwohl Message Queue aktiv ist.

*Umgehung*

Starten Sie den Identity Synchronization für Windows-Dienst bzw. -Dämon, auf dem der Core installiert ist, neu.

**Erhöhen Sie den Maximumspeicher des Message Queue-Brokers für Installationen mit über 100.000 Benutzer. (4924939)**

Identity Synchronization für Windows konfiguriert Message Queue-Broker standardmäßig auf maximal 512 MB Speicher, was für die meisten Installationen ausreicht. Für Installationen, die mehr als 100.000 Benutzer umfassen, sollten Sie den maximalen Speicher auf mindestens 1 GB erhöhen, um eine optimale Leistung zu gewährleisten. Für Installationen von über 200.000 Benutzern erhöhen Sie den Speicher auf 2 GB.

Führen Sie bei Installation des Identity Synchronization für WindowsCore unter *Solaris* folgende Schritte aus, um die Speicherbeschränkung des Message Queue-Brokers zu erhöhen:

1. Geben Sie den folgenden Befehl aus, um den Message Queue-Broker anzuhalten:

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

2. Bearbeiten Sie die Datei `/etc/imq/imqbrokerd.conf`, um die aktuelle Speicherstandardeinstellung von `-Xmx512m` auf `-Xmx1024m` für 1 GB Speicher bzw. auf `-Xmx2048m` für 2 GB Speicher zu ändern.

3. Geben Sie den folgenden Befehl aus, um den Message Queue-Broker zu starten:

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

Führen Sie bei Installation des Identity Synchronization für Windows-Core unter *Windows 2000* folgende Schritte aus, um die Speicherbeschränkung des Message Queue-Brokers zu erhöhen:

1. Halten Sie den Message Queue-Brokerdienst mit der Managementkonsole der Windows-Dienste an.
2. Führen Sie im Verzeichnis `<Installationsroot>/isw-<Computername>/imq/bin` in der Befehlszeile den Befehl `imqsvcadm query` aus. Die Ausgabe sieht etwa so aus:  
  
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. Speichern Sie die Ausgabe dieses Befehls in eine Datei.
4. Deinstallieren Sie den Message Queue-Brokerdienst durch Ausführen des Befehls `imqsvcadm remove`.
5. Bevor Sie fortfahren können, müssen Sie den Windows 2000-Computer, auf dem der Core installiert wurde, neu starten.
6. Führen Sie im Verzeichnis `<Installationsroot>/isw-<Computername>/imq/bin` den folgenden Befehl unter Verwendung der aufgrund des Befehls `imqsvcadm query` gespeicherten Ausgabe aus. Zum Beispiel:

```
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"
```

Dabei gilt:

- Das Argument `-args` wird durch das Feld `Broker.Args` ausgefüllt.
- Das Argument `-jrehome` wird durch das Feld `JREHome` ausgefüllt.
- Um den Speicher auf 1 GB zu erhöhen, verwenden Sie den Befehl `-vmargs -Xmx1024m`.
- Nur für 64-Bit-Java VM: Um den Speicher auf 2 GB zu erhöhen, verwenden Sie den Befehl `-vmargs -Xmx2048m`.  
Der höchste Speicherwert für eine 32-Bit-Java VM ist `-Xmx1750m`

7. Starten Sie den Message Queue-Brokerdienst mit der Managementkonsole der Windows-Dienste.

### **Starten und Anhalten des Message Queue-Brokers (4809493)**

Unter Windows wird der Message Queue-Broker als Dienst ausgeführt und Administratoren können den Message Queue-Brokerdienst über die Dienstsysteemsteuerung steuern.

Zum Starten und Anhalten des Brokers müssen Sie den Rechner nach Installation des Core neu starten, da der Dienst-Manager-Prozess die erforderliche Umgebungsvariable `IMQ_JAVAHOME` erst nach Neustart von Windows erkennen kann. Diese Situation tritt nur ein, wenn Sie Message Queue mit dem Core installiert haben (d. h., es wurde kein bereits vorhandenes Message Queue verwendet).

Verwenden Sie die folgenden Befehle:

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

### **Keine Unterstützung für die Verwendung von Message Queue auf einem Computer, auf dem der Core nicht installiert ist. (4943576)**

Identity Synchronization für Windows-Core-Komponenten und Message Queue müssen auf demselben Host installiert sein.

## Allgemeine Probleme

**Wenn die Synchronisation erfolgreich startet, können nach wie vor Fehler vorhanden sein. (4814324)**

Auch wenn die Befehle `idsync startsync` Erfolg vermelden, sollten Sie das zentrale Fehlerprotokoll prüfen, um festzustellen, ob die Konnektoren eine Verbindung zu ihren Verzeichnisquellen herstellen konnten.

**Es wird dringend empfohlen, das Konfigurationsverzeichnis und die Verzeichnisquelle für eine MMR-Konfiguration in separate Directory Server-Instanzen zu speichern. (4943470 und 4943480)**

Es wird in einer Multimaster Replication (MMR)-Konfiguration dringend empfohlen, das Konfigurationsverzeichnis und die Verzeichnisquelle in separate Directory Server-Instanzen zu speichern und Replikationsvereinbarungen *vor* der Installation von Identity Synchronization für Windows zu konfigurieren.

Wenn Sie dieselbe Directory Server-Instanz als Konfigurationsverzeichnis und als bevorzugten Directory Server (Benutzerdaten) bestimmen und nach der Installation von Identity Synchronization für Windows Replikationsvereinbarungen erstellen, werden unter Umständen die von der Identity Synchronization für Windows-Core-Installation erstellten Schemaelemente gelöscht. In diesem Fall wird Identity Synchronization für Windows nicht ausgeführt.

### *Umgehung*

So aktualisieren Sie das Schema, wenn Sie es versehentlich gelöscht haben:

1. Kopieren Sie die Datei `40so-psw.ldif` (die die Schemaobjekte für die Konfigurationsregistrierung nur für das Installationspaket enthält) in das Schemaverzeichnis der Directory Server-Instanz.
2. Benennen Sie die Datei `40so-psw.ldif` um.

Einige Referenzen im Schema werden nicht geladen, wenn die Datei `40so-psw.ldif` beim Hochfahren verarbeitet wird (Folge: der Server fährt nicht hoch).

3. Kopieren Sie die umbenannte Datei in das Schemaverzeichnis beider Master. (Aus der Sicht des Servers wurde das Schema gegenüber dem Protokoll nicht geändert, da die Änderungsreihenfolgennummer des Schemaeintrags gleich bleibt.)

**Während des Verknüpfungsvorgangs verwendete Attribute sollten in Directory Server indiziert werden. (4814412)**

Beim Verknüpfen von Benutzern mit `idsync resync` (-f <dateiname> Option) durchsucht der Befehl den Directory Server nach Benutzern, die Active Directory- oder Windows NT-Benutzern entsprechen. Jedes Directory Server-Attribut sollte in einem „idsync resync“-Vorgang aus Gleichheitsgründen indiziert werden.

**Die zentrale Protokollierung lässt sich nicht ausschalten. (4945507 und 4933217)**

Obwohl die zentrale Protokollierung von Identity Synchronization für Windows (die Daten in Dateien, im Systemprotokoll oder beidem protokolliert) Ihnen anscheinend das Ausschalten der Protokollierung erlaubt, wird die Protokollierung in den zuvor festgelegten Speicherort fortgesetzt.

Wenn Sie z. B. in der Konsole die Protokollierung in das Systemprotokoll festlegen (wobei die Dateiprotokollierung deaktiviert ist) und anschließend die Systemprotokollprotokollierung ausschalten, setzt das Programm die Protokollierung in das Systemprotokoll fort. Wenn Sie die Dateiprotokollierung von der Konsole aus angeben (wobei die Systemprotokollprotokollierung deaktiviert ist) und anschließend die Dateiprotokollierung deaktivieren, setzt das Programm die Protokollierung in das Dateiprotokoll fort.

Dasselbe Verhalten tritt auf, wenn die Option „Write logs to file (Protokolle in Datei schreiben)“ deaktiviert ist und das Systemprotokoll nie verwendet wurde. In diesem Fall schreibt das Programm die Protokolle weiterhin in das Verzeichnis.

Das Neustarten des Identity Synchronization für Windows-Dienstes hat keine Wirkung – die Protokollierung wird fortgesetzt.

**Die Schaltfläche zum Durchsuchen der synchronisierten Benutzerliste funktioniert unter Umständen nicht ordnungsgemäß. (4944348)**

Wenn Sie vom Erstellungsassistenten der synchronisierten Benutzerliste (SUL) oder dem Editorfenster aus nach einem Basis-DN suchen, ist es ratsam, den durch Verwenden der Schaltfläche „Durchsuchen“ abgeleiteten Basis-DN gründlich zu prüfen. In einigen Fällen wird durch die Schaltfläche das falsche Verzeichnis durchsucht, was zu einem ungültigen Basis-DN führt.

**Deaktivieren von Benutzerkonten in Active Directory (4943785)**

Wenn ein Benutzer ein Benutzerkonto löscht und das Kennwort in Active Directory (AD) ändert, kann er sich über Active Directory nicht anhand des neuen Kennworts authentifizieren. Bei Deaktivierung eines Benutzerkontos in Active Directory ist jedoch nach wie vor eine Anmeldung über Sun Java System Directory Server möglich.

**Ändern des Konfigurationsverzeichnisports (4941271)**

Wenn Sie den Port für einen Sun Java System Directory Server ändern, der momentan als Identity Synchronization für Windows-Konfigurationsverzeichnis verwendet wird, müssen Sie die Identity Synchronization für Windows-Konfiguration entsprechend anpassen, damit die Software die Portänderung erkennt. Andernfalls funktioniert der Systemmanager oder Message Queue-Broker nicht.

## Umgehung

1. Ändern Sie den Port im Verzeichnis  
`<imq_installroot>\imq\var\instances\psw-broker\props\config.properties.`  
Zum Beispiel: `imq.user_repository.ldap.server=<Host>\:<Port>`
2. Ändern Sie den Port in `<isw_installroot>\resources\SystemManagerBootParams.cfg.`  
Zum Beispiel: `<Parameter name="manager.configReg.hostPort" value="<port>" />`
3. Starten Sie den Message Queue-Brokerdienst bzw. -dämon neu.
4. Starten Sie den Identity Synchronization für Windows-Dienst bzw. -Dämon neu.

### Die Unterstützung für ungleiche, mehrwertige Attribute ist beschränkt. (4987930 und 4807260)

Identity Synchronization für Windows bietet nur begrenzte Unterstützung für die Synchronisierung ungleicher mehrwertiger Attribute, da die Ergebnisse nicht definiert sind. Es gelten folgende Einschränkungen:

- Die Werte in einem mehrwertigen Attribut werden als Einheit synchronisiert. Wenn Sie beispielsweise einem mehrwertigen Attribut, das bereits vier Werte besitzt, einen einzelnen Wert hinzufügen, werden alle fünf Werte als Einheit synchronisiert und die Werte des entsprechenden remote Attributs werden auf diese fünf Werte gesetzt.
- Beim Verknüpfen bereits vorhandener Benutzer werden die entsprechenden Attribute nicht automatisch synchronisiert. Ändert sich ein mehrwertiges Attribut werden die Werte des Attributs an der remote Verzeichnisquelle mit den Werten der lokalen Verzeichnisquelle überschrieben. Wenn Sie beispielsweise dem zuvor leeren Attribut `telephoneNumber` eines Eintrags in Active Directory (AD) eine Telefonnummer hinzufügen, wird das Attribut `telephoneNumber` für den entsprechenden Eintrag in Directory Server auf diesen neuen Wert festgelegt und bereits vorhandene Werte werden überschrieben.
- Gleichzeitige Aktualisierungen eines mehrwertigen Attributs werden unter Umständen nicht synchronisiert. Wenn Sie einem mehrwertigen Attribut etwa zur gleichen Zeit einen Wert hinzufügen wie ein anderer Wert dem mehrwertigen Attribut in dem entsprechenden remote Verzeichniseintrag hinzugefügt wird, dann ist das Attribut möglicherweise nicht mehr synchronisiert. Dieser Fall gilt auch für einwertige Attribute.
- Wenn Sie das Attribut `cn` ändern oder umbenennen, ist das Attribut `cn` in Directory Server ein mehrwertiger Attributtyp und in Active Directory ein einwertiger Attributtyp. Active Directory verwendet diesen Attributtyp (und seinen Wert) zur Generierung neuer DNs für die umzubenennenden und zu ändernden Personeneinträge. Da der Konnektor nicht weiß, welcher Wert eines mehrwertigen `cn`-Attributs für die Erzeugung des neuen DNs verwendet werden soll, sendet er standardmäßig den ersten Wert. Da der erste Wert im Allgemeinen nicht der richtige ist, schlägt die Umbenennung oder Änderung in Active Directory fehl.

Wenn Sie Umbenennungen (`ldap modrdns`) mit dem `deleteoldrdn`-Kennzeichen auf 0 und dem `rdn`-Komponentenattributtyp als `cn` festlegen, schlägt der Vorgang auf Seiten von Active Directory fehl. Ist beispielsweise der folgende Eintrag vorhanden und sowohl in Directory Server als auch in Active Directory synchronisiert

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

und Sie benennen den Eintrag in Directory Server um und setzen das `deleteoldrdn`-Kennzeichen auf 0, ändert Identity Synchronization für Windows den Eintrag in Directory Server in

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

Die Umbenennung in Active Directory schlägt allerdings fehl, da der Eintrag wie folgt erstellt wurde:

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

Dies führt zu einer Fehlermeldung (im Überwachungsprotokoll), die in etwa wie folgt aussieht:

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

Damit dieser Vorgang erfolgreich ausgeführt wird, setzen Sie das Kennzeichen `deleteoldrdn=1`. Führen Sie den Umbenennungsvorgang anhand der folgenden Anweisungen zum Ändern von LDAP aus:

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

- Wenn Sie ein `cn`-Attribut anhand des `modify`-Änderungstyps und des `add`-Modus ändern und mehr als einen `cn`-Attributtyp hinzufügen *oder* wenn ein `cn`-Attributtyp bereits vorhanden ist und Sie einen neuen `cn`-Attributtyp hinzufügen, schlägt der Vorgang `modify` fehl. Beispiel: Der folgende `cn`-Eintrag ist sowohl in Directory Server als auch Active Directory vorhanden:

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

Sie verwenden die folgenden LDAP-Änderungsanweisungen für diesen Eintrag:

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

In diesem Fall wird der Directory Server-Eintrag wie folgt geändert:

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

Allerdings schlägt der modify-Befehl auf der Active-Directory-Seite fehl, da Active Directory einwertig ist. Im Überwachungsprotokoll wird dieselbe Fehlermeldung angezeigt wie im vorhergehenden Beispiel, da der Konnektor nicht zwischen Umbenennung und Änderung unterscheiden kann.

### **Active Directory behandelt Beschreibungsattribute als einwertig, obwohl sie im Active Directory-Schema als mehrwertig beschrieben sind. (4938940)**

Wenn Sie mithilfe eines mehrwertigen Beschreibungsattributs Einträge zu Directory Server hinzufügen, wird der folgende DSID-031D0809-Fehler in der Überwachungsdatei audit.log des Active Directory-Konnektors ausgegeben:

```
[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)
```

Der Eintrag ist zwar in Directory Server, nicht aber in Active Directory vorhanden.

Das Problem scheint ein Active-Directory-Fehler zu sein. Weitere Informationen erhalten Sie im folgenden Artikel der Microsoft Knowledge Base (286760):

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

### *Umgehung*

Entfernen Sie den Eintrag aus Directory Server, ändern Sie das Beschreibungsattribut in einwertig und fügen Sie den Eintrag erneut hinzu.

Initialisieren Sie außerdem nur maximal ein Beschreibungsattribut im Dialogfeld „Define Creation Attribute Mappings and Values (Erstellungsattributzuordnungen und -werte definieren)“.



### **Keine Fehlermeldung vom Plug-In bei nicht vertrauenswürdigen Secure Sockets Layer-Zertifikat (4924027 und 4924705)**

Wenn in einer Multimaster Replication (MMR)-Konfiguration ein Identity Synchronization für Windows-Plug-In (Unterkomponente) mithilfe von Secure Sockets Layer (SSL) kommuniziert und ein SSL-Problem zu einem Fehler führt, das Plug-In jedoch keine Fehlermeldungen ausgibt, fehlt vermutlich ein CA-Zertifikat des *Peer*-Server-Zertifikats (wobei der *Peer* ein bevorzugter Master, ein sekundärer Master oder ein Active Directory sein kann) in der Zertifikatdatenbank des Directory Server, auf dem das Plug-In ausgeführt wird.

Verwenden Sie zum Ermitteln fehlender Zertifikate das `idsync` `certinfo`-Befehlszeilen-Dienstprogramm. Dieses Dienstprogramm ermittelt, welche Zertifikate in welcher Datenbank erforderlich sind (d. h. welche Zertifikate das Produkt erwartet).

### **In Sun Java System Directory Server erstellte Benutzer sollten alle Attribute in SUL-Filtern enthalten. (4900568)**

Wenn Sie erstellte Daten von Sun Java System Directory Server in Windows synchronisieren und die Definitionen der synchronisierten Benutzerliste (SUL) Filter umfassen, versuchen Sie einen Eintrag mit Attributwerten zu erstellen, die dem SUL-Filter nicht entsprechen. Der erstellte Eintrag wird nicht weitergegeben, da sich die Attribute nicht in der synchronisierten Benutzerliste befinden. Da der ursprünglich erstellte Eintrag nicht weitergegeben wird, ist der Directory Server-Eintrag in Windows nicht vorhanden.

#### *Umgehung*

Wenn dieser Fall eintritt, wird eine Warnung protokolliert und der Administrator muss den Befehl `idsync resync -c -o Sun` ausführen, um den Directory Server-Eintrag in Windows zu erstellen.

Wenn Sie den Eintrag so ändern, dass die Attribute mit dem SUL-Filter übereinstimmen, werden an dem Eintrag vorgenommene Änderungen an Windows weitergegeben.

### **Von NetBIOS verursachte bedarfsgesteuerte Synchronisationsverzögerung (4876741)**

Der Versuch, zwei Active Directory-Domänen mithilfe einer Directory Server- und Core-Komponenten-Konfiguration unter Windows 2000 zu synchronisieren, verursachte eine Verzögerung bei der Kommunikation der bedarfsgesteuerten Synchronisationsfunktion des Directory Server-Plug-Ins mit Active Directory. Die meisten an Active Directory gerichteten Abfragen erfordern wenige Millisekunden. Durch eine Paketverfolgung wurden einige verdächtige NBNS-Pakete (NetBIOS Name Service) erkannt.

#### *Umgehung*

Zur Behebung des Problems müssen Sie auf die TCP/IP-Einstellungen auf dem Directory Server-Computer zugreifen und NetBIOS über TCP/IP deaktivieren.

**Identity Synchronization für Windows-Namespaces (Themen) wurden vom Meldungsbus verwendet. (4827081)**

- ConConfig\_100
- CntrlLog\_100
- SysMgr\_100
- PSW\_AuditLoggingTopic
- PSW\_ErrorLoggingTopic
- PSW\_LinkAuditLoggingTopic

Darüber hinaus bestehen folgende Anforderungen:

- Für jeden Konnektor im System ist ein CNN1XX\_100-Thema vorhanden (z. B. CNN100\_100, CNN101\_100 und CNN102\_100).
- Für jede synchronisierte Benutzerliste (SUL) im System ist ein Thema basierend auf dem SUL-Namen vorhanden. (Zum Beispiel: Eine synchronisierte Benutzerliste mit dem Namen *Personen* besitzt ein Thema namens *Personen\_100*.)

**Das Angeben eines Hosts im Dialogfeld für den globalen Katalog oder das Konfigurationsverzeichnis dauert eine Weile. (4826109 und 4812651)**

Wenn Sie einen nicht auflösbaren Host angeben, erscheint keine Fortschrittsanzeige (ein entsprechender Cursor oder eine Statusleiste) als Hinweis darauf, dass ein Vorgang verarbeitet wird.

**NT-Benutzernamen müssen eindeutig sein. (4825636)**

Stellen Sie beim Erstellen eines Benutzers in Directory Server zur Weitergabe an NT sicher, dass das dem Wert `USER_NAME` zugeordnete Directory Server-Attribut eindeutige Werte besitzt.

**Weisen Sie Benutzer an, XML-Konfigurationsdateien mithilfe von Zugriffssteuerungslisten (ACLs) zu sichern. (4812824)**

Verwenden Sie für die XML-Konfigurationsdateien den Schutz auf Dateiebene. Da diese Dateien unter Umständen unverschlüsselte Kennwortwerte enthalten, sollten Sie sie anhand der in Ihrem System verfügbaren Mechanismen sichern, z. B. ACLs auf Dateiebene.

**Unterstützte synchronisierte Benutzerliste (SUL) und Datenbankbeziehungen (4811577)**

Identity Synchronization für Windows unterstützt nur eine einzige Directory Server-Datenbank. Daher müssen Sie alle synchronisierten Benutzerlisten (SULs) in einer einzigen Directory Server-Datenbank speichern.

**Die Anzahl der Protokolle steigt unter Umständen unbegrenzt. (4807451)**

Sofern Sie alte Protokolle nicht speichern oder löschen, steigt die Anzahl der einzelnen Protokolldateitypen in Identity Synchronization für Windows unbegrenzt (ein Protokoll pro Tag).

Protokolle besitzen folgendes Format:

- audit\_JJJJ\_MM\_TT.log
- error\_JJJJ\_MM\_TT.log

Es werden folgende Protokolle gespeichert:

- audit (Überwachung)
- error (Fehler)

Diese Protokolle befinden sich in folgendem Verzeichnis:

- **Unter Solaris:** /var/opt/SUNWsw/logs
- **Unter Windows:** <Installationsroot>/isw-<Rechnername>/logs

**Ein Eintrag mit Sonderzeichen wird in Directory Server nicht mit Active Directory synchronisiert. (4816867)**

Entweder kann Identity Synchronization für Windows die Sonderzeichen (aufgrund von Zuordnungsbeschränkungen) nicht auflösen oder Active Directory (AD) kann den Benutzer nicht anlegen, da mindestens ein Sonderzeichen in der Benutzer-ID verwendet wird.

Die Active Directory-Konsole erlaubt Ihnen nicht, einen Benutzeranmeldenamen mit folgenden Eigenschaften zu erstellen:

- Enthält eines der folgenden Sonderzeichen: " / [ ] : | < > ; ? % \$ ^ & \* ( ) ! @ # - + = ~ `
- Überschreitet 20 Zeichen.
- Endet mit einem Punkt oder enthält Kommata.
- Enthält Zeichen im Bereich 1-31, die nicht druckbare Zeichen sind.

### **Der useraccountcontrol-Attributstandard verhindert die Erstellung einer benutzerfremden Active Directory-Objektklasse. (5043156)**

In Active Directory können keine Benutzer angelegt werden, wenn die für die neuen Benutzer ausgewählte Objektklasse das Attribut `useraccountcontrol` nicht zulässt. Diese Einschränkung gilt nicht für Szenarien, in denen die Benutzer-Objektklasse oder eine andere benutzerabgeleitete Objektklasse das Attribut `useraccountcontrol` in Active Directory zulässt.

#### *Umgehung*

Bearbeiten Sie den Konfigurationsbenutzer mithilfe der Directory Server-Konsole. Suchen und entfernen Sie das Attribut `useraccountcontrol`.

Zum Beispiel:

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

Bearbeiten Sie außerdem alle Verweise auf das Attribut `useraccountcontrol`, insbesondere im Attribut `pswCreationAttributeDefaultRef` des globalen Schemas von Active Directory.

Zum Beispiel:

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

### **Für Standardwerte wird keine Überprüfung durchgeführt. (5051725)**

Standardwerte können für die Attribute angegeben werden und können beim Erstellen der Attribute auf die Verzeichniseinträge angewendet werden. (Weitere Informationen finden Sie im Abschnitt „Creation Attributes“ des *Sun Java System Identity Synchronization für Windows Installation and Configuration Guide*). Momentan wird keine Überprüfung der von Ihnen angegebenen Attributwerte durchgeführt. Durch Angabe mehrerer Werte für einwertige Attribute schlägt die Objekterstellung bei der Synchronisation der Einträge fehl. Stellen Sie bei der Angabe von Attributwerten sicher, dass die angegebenen Werte dem LDAP-Schema Ihres Unternehmens entsprechen.

### **Änderungen werden inkonsistent behandelt, wenn der Benutzer in der synchronisierten Benutzerliste (SUL) erscheint. (4970664)**

Wenn ein Benutzer als Folge einer Änderung in den Bereich einer synchronisierten Benutzerliste (SUL) gerät (die SUL besitzt z. B. einen Filter „l=Austin“ und der Benutzer wird geändert, sodass das Attribut „l“ auf „Austin“ eingestellt wird), behandelt Sun Java System Identity Synchronization für Windows diese Benutzeraktualisierung in Active Directory und Sun Java System Directory Server unterschiedlich:

- Wird die Benutzeraktualisierung in Active Directory vorgenommen, erstellt der Identity Synchronization Directory Server-Konnektor den entsprechenden Benutzer.
- Geschieht die Benutzeraktualisierung in Sun Java System Directory Server, wird der entsprechende Benutzer in Active Directory nicht erstellt. Mit dem Befehl `resync -c -o` Sun kann das Problem möglicherweise umgangen werden.

### **Einträge mit einer strukturellen Objektklasse, die von der zum Synchronisieren ausgewählten Objektklasse erben, werden ebenfalls synchronisiert. (5046861)**

Ist zum Beispiel die Objektklasse `organizationalperson` ausgewählt, werden auch die Benutzer mit der Objektklasse `inetorgperson` synchronisiert, da die Objektklasse `inetorgperson` eine Unterklasse der erstgenannten Klasse ist.

Um dies zu verhindern, fügen Sie in die synchronisierte Benutzerliste einen Filter ein, der die Unterklasse ausschließt:

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

Dadurch wird in der Regel ein Problem verursacht, wenn Sie den Befehl `resync` zur Synchronisation gelöschter Einträge verwenden, da die Unterklassen ebenfalls gelöscht werden. In Active Directory erbt die Objektklasse `computer` beispielsweise von der Objektklasse „user“, und Einträge der Objektklasse `computer` werden unter Umständen gelöscht, da sie keinen entsprechenden Directory Server-Eintrag besitzen. Um zu verhindern, dass die Einträge der Objektklasse `computer` synchronisiert werden, fügen Sie einen Filter in die synchronisierte Benutzerliste (SUL) ein, der die Klasse ausschließt:

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

### **Protokolldateien werden nach Ablauf ihres Gültigkeitsdatums nicht automatisch gelöscht. (5069020)**

Protokolldateien, die älter sind als die für die Entfernung angegebene Anzahl von Tagen, werden nicht entfernt.

**Standardwerte für Erstellungsattribute konnten nicht richtig konfiguriert werden oder haben die Überprüfungslogik nicht bestanden. (5066657)**

Lautet der Name eines Erstellungsattributs für die Directory Server- und die Active Directory-Datenquelle gleich, werden beim Hinzufügen von Standardwerten zu einer Quelle der anderen Quelle die gleichen Werte hinzugefügt.

*Umgehung*

Löschen Sie die Zuordnung des Erstellungsattributs und die Erstellungsattribute in der Konsole und fügen Sie sie erneut hinzu. Führen Sie vor dem Speichern folgende Schritte aus: Wenn die Namen der zugeordneten Attribute übereinstimmen und die Syntax (OIDs) der Attribute den Schemata von Active Directory und Directory Server entsprechen:

- Stellen Sie sicher, dass die für die Attribute hinzugefügten Standardwerte nicht identisch sind. (Dieses Problem tritt auch auf, wenn keine Quelle einen Wert aufweist.)

---

**HINWEIS** Sind die Standardwerte absolut identisch, tritt dieses Problem unter Umständen nicht auf. Wenn die Werte identisch sind, können sie nur getrennt werden, indem die Erstellungsattribute und Zuordnungen entfernt und anschließend erneut hinzugefügt werden.

---

**Der useraccountcontrol-Attributstandard verhindert die Erstellung einer benutzerfremden Active Directory-Objektklasse. (5043156)**

In Active Directory können keine Benutzer angelegt werden, wenn die für die neuen Benutzer ausgewählte Objektklasse das Attribut `useraccountcontrol` nicht zulässt. Die Benutzer-Objektklasse oder eine andere benutzerabgeleitete Objektklasse lassen das Attribut `useraccountcontrol` in Active Directory zu und sind von dieser Einschränkung nicht betroffen.

**InetOrgperson kann nicht mit einer erweiterten Klasse zugewiesen werden, die ein obligatorisches Attribut aufweist. (5091959)**

Es wird beispielsweise eine Fehlermeldung ausgegeben, die in etwa wie folgt lautet: ‚Keine Sun-Zuordnungen oder -Werte für Active Directory-Attribut `mail` angegeben‘; hierbei ist `mail` das obligatorische Attribut und `mail` wird dem Sun-Mail-Attribut zugeordnet.

**Im Identity Synchronization for Windows Installation and Configuration Guide werden die Schaltfläche „Weiter“ und der Bereich „Zusammenfassung“ nicht erwähnt. (5104768)**

Im *Identity Synchronization for Windows Installation and Configuration Guide* wird am Ende jedes Aufrufs angegeben, dass der Assistent über eine Schaltfläche mit der Bezeichnung „Schließen“ im Bereich mit der Installationszusammenfassung beendet werden muss. Es gibt in diesem Bereich jedoch keine Schaltfläche mit dieser Bezeichnung. Sie müssen im Bereich mit der Installationszusammenfassung auf die Schaltfläche „Weiter“ klicken, um zu einem Bereich zu gelangen, in dem die noch auszuführenden Installations- und Konfigurationsschritte erläutert werden. Bei allen nicht auf den Core bezogenen Installationsvorgängen weist dieser Bereich eine Schaltfläche mit der Bezeichnung „Fertig“ auf. Wenn hierauf geklickt wird, wird der Assistent beendet. Bei auf den Core bezogenen Installationsvorgängen ist in diesem Bereich die Schaltfläche „Weiter“ vorhanden. Wenn Sie darauf klicken, gelangen Sie zu einem Bereich, in dem Sie gefragt werden, ob die Konsole aufgerufen werden soll. Von diesem Bereich aus können Sie das Installationsprogramm über die Schaltfläche „Fertig“ beenden.

**Einschränkungen bei der WAN-Unterstützung. (5097751)**

Identity Synchronization für Windows kann als Wide Area Network-(WAN-)Umgebung mit bestimmten Einschränkungen bereitgestellt werden.

Mit Ausnahme des Directory Server-Plug-Ins müssen sämtliche Identity Synchronization für Windows-Komponenten im selben LAN (Local Area Network), also beispielsweise auf demselben Computer, installiert werden, da kein Message Queue-Datenverkehr über das WAN übermittelt werden sollte. Diese Komponenten können über ein WAN mit Directory Server-Instanzen oder Active Directory-Domänencontrollern kommunizieren.

Die Leistung über das WAN hängt von Latenzzeit und Linkgeschwindigkeit ab. Wir empfehlen mindestens eine T1-Verbindung (1,544 MBit/s) und eine Latenzzeit von höchstens 300 ms zwischen den einzelnen Konnektoren und dem verwalteten Verzeichnis. In einer Bereitstellung, bei der Active Directory und Directory Server durch ein WAN getrennt sind, lässt sich bessere Systemleistung erzielen, wenn der Directory Server-Konnektor im selben LAN wie Directory Server installiert wird und die Kommunikation zwischen dem Active Directory-Konnektor und Active Directory über das WAN erfolgt.

---

# Dateien für Neuverteilung

Sun Java System Identity Synchronization für Windows 1 2004Q3 enthält keine Datei für eine Neuverteilung.

---

## Problemmeldungen und Feedback

Wenn Sie mit Sun Java System Identity Synchronization für Windows Probleme haben, wenden Sie sich an die Kundenunterstützung von Sun. Dazu stehen Ihnen folgende Möglichkeiten zur Verfügung:

- Sun-Softwaresupport unter:

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

Auf dieser Website finden Sie Links zur Knowledge Base, zum Online Support Center, zum ProductTracker wie auch zu Wartungsprogrammen und Kontaktinformationen für die Kundenunterstützung.

- Die auf Ihrem Wartungsvertrag angegebene Telefonnummer.

Damit wir Sie optimal beraten können, halten Sie bitte die folgenden Informationen bereit, wenn Sie sich an die Kundenunterstützung wenden:

- Beschreibung des Problems, einschließlich der Situation, in der das Problem auftrat, sowie seine Auswirkungen auf Ihre Arbeit.
- Rechnertyp, Betriebssystem- und Produktversion, einschließlich sämtlicher Patches und anderer Software, die mit dem Problem in Zusammenhang stehen könnten.
- Zur Nachvollziehung des Problems eine ausführliche Beschreibung der einzelnen Schritte und Vorgehensweisen, die zu dem Problem geführt haben.
- Sämtliche Fehlerprotokolle oder Kernspeicherauszüge.



## Kommentare sind willkommen

Sun möchte seine Dokumentation laufend verbessern. Ihre Kommentare und Vorschläge sind daher immer willkommen. Verwenden Sie das webbasierte Formular, um uns Ihr Feedback mitzuteilen:

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

Tragen Sie den vollständigen Titel der Dokumentation und die vollständige Teilenummer in die entsprechenden Felder ein. Sie finden die Teilenummer auf der Titelseite des Buchs oder oben auf dem Dokument. Dabei handelt es sich in der Regel um eine sieben- oder neunstellige Nummer. Die Teilenummer dieser Identity Synchronization für Windows Version 1 2004Q3-Versionshinweise lautet beispielsweise 817-7850.

---

## Weitere Informationen über Sun

Nützliche Informationen über Sun Java System finden Sie unter den folgenden Internet-Adressen:

- Dokumentation zu Sun Java System Identity Synchronization für Windows 1 2004Q3  
[http://docs.sun.com/coll/S1\\_IdSyncForWin\\_1.0](http://docs.sun.com/coll/S1_IdSyncForWin_1.0)
- Sun Java System-Dokumentation  
<http://docs.sun.com/prod/sunone>
- Professionelle Dienste für Sun Java System  
<http://www.sun.com/service/sunps/sunone>
- Sun Java System-Softwareprodukte und -dienste  
<http://www.sun.com/software>
- Sun Java System-Softwaresupport  
<http://www.sun.com/service/sunone/software>
- Sun Java System-Support und -Knowledge Base  
<http://www.sun.com/service/support/software>
- Sun-Support und -Schulungen  
<http://training.sun.com>
- Sun Java System-Beratung und professionelle Dienste  
<http://www.sun.com/service/sunps/sunone>
- Sun Java System-Informationen für Entwickler  
<http://sunonedev.sun.com>

- Sun-Supportdienste für Entwickler  
<http://www.sun.com/developers/support>
- Sun Java System-Softwareschulungen  
<http://www.sun.com/software/training>
- Sun-Softwaredatenblätter  
<http://www.sun.com/software>

---

Copyright © 2004 Sun Microsystems, Inc. Alle Rechte vorbehalten.

Sun Microsystems, Inc., ist Inhaber der Urheberrechte für die Technologie, die in den in diesem Dokument beschriebenen Produkten verwendet wird. Diese Urheberrechte können insbesondere und ohne Einschränkungen eines oder mehrere der unter <http://www.sun.com/patents> aufgelisteten US-Patente und weitere Patente oder angemeldete Patente in den USA und anderen Ländern einschließen.

SUN URHEBERRECHTLICH/VERTRAULICH.

Rechte der US-Regierung – Kommerzielle Software. Regierungsbenutzer unterliegen der standardmäßigen Lizenzvereinbarung von Sun Microsystems, Inc., sowie den anwendbaren Bestimmungen der FAR und ihrer Zusätze.

Die Verwendung unterliegt Lizenzbestimmungen.

Diese Ausgabe kann von Drittanbietern entwickelte Bestandteile enthalten.

Teile davon leiten sich möglicherweise aus den Berkeley BSD-Systemen ab und sind lizenziert von der University of California.

Sun, Sun Microsystems, das Sun-Logo, Java und Solaris sind Marken oder eingetragene Marken von Sun Microsystems, Inc. in den USA und anderen Ländern. Alle SPARC-Warenzeichen werden unter Lizenz verwendet und sind Warenzeichen oder eingetragene Warenzeichen von SPARC International, Inc., in den USA und anderen Ländern.