

# Sun Java™ System Identity Synchronization for Windows 发行说明

版本 1 2004Q3

文件号码 817-7855

---

本说明包含了在 Sun Java™ System Identity Synchronization for Windows 1 2004Q3 发行时可用的重要信息。介绍了新功能和增强功能、已知的限制和问题、技术说明及其它信息。在使用 Sun Java System Identity Synchronization for Windows 1 2004Q3 (Identity Synchronization for Windows) 之前，请阅读本文档。

本发行说明包含以下各节：

- [修订历史](#)
- [关于 Identity Synchronization for Windows 1 2004Q3](#)
- [本版本中已修复的错误](#)
- [重要信息](#)
- [已知问题和限制](#)
- [可重新分配的文件](#)
- [如何报告问题和提供反馈](#)
- [其它 Sun 资源](#)

本文档中引用了第三方 URL 并提供了附加的相关信息。

---

## 注意

Sun 对本文档中提及的第三方网站的可用性概不负责。对于此类站点或资源直接或间接提供的任何内容、广告、产品或其它资料，Sun 不作任何担保，也不承担任何责任。对于此类站点或资源直接或间接提供的任何此类内容、物品或服务导致的、或与其使用或可靠性相关的任何实际的或声称的损害或损失，Sun 亦不承担任何责任。

---

---

# 修订历史

**表 1**      修订历史

| 日期              | 变更说明    |
|-----------------|---------|
| 2004 年 9 月 30 日 | 发行说明初版。 |

---

---

## 关于 Identity Synchronization for Windows 1 2004Q3

Identity Synchronization for Windows 提供了下列目录之间的双向密码同步：

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

同步 Sun Java System Directory Server (Directory Server) 和 Windows 2000/2003 Active Directory 时，可以在 Solaris™ Operating System 和 Windows 2000 Server 操作系统环境中安装和运行所有 Identity Synchronization for Windows 组件。同步 Directory Server 和 Windows NT 时，则必须在 Windows NT 环境中运行 Windows NT 组件。

本节包括：

- [本版本中的新功能](#)
- [硬件和软件要求](#)

# 本版本中的新功能

## 新功能

Identity Synchronization for Windows 1 2004Q3 中的新功能包括：

- **用户删除：**可以配置和启用从 Sun Java System Directory Server 到 Active Directory 以及从 Active Directory 到 Sun Java System Directory Server 的用户条目删除操作的同步。
- **Active Directory 故障转移：**支持在即时请求的验证期间，指定用于故障转移的附加 Active Directory 服务器。当用户的密码已在 Active Directory 上更改时，Identity Synchronization for Windows Directory Server 插件可使用此功能向 Active Directory 证明用户的身份。在版本 1.0 中，这是不可能的。因此，如果主 Active Directory 服务器不可用，则从 Identity Synchronization for Windows Directory Server 插件到 Active Directory 的通过验证将失败，用户无法通过 Directory Server 验证。仅当用户在 Active Directory 上更改了其密码并在此次密码更改之后首次进行 Directory Server 验证时，才会出现这种情况。
- **用于 Active Directory 的用户对象类：**可将任何适当的对象类（User 或扩展名）用于 Active Directory 模式信息。（在版本 1.0 中，仅可使用 User 对象类。）
- **Windows 2003 Server Active Directory 支持：**现在可以安装和配置 Identity Synchronization for Windows 1 2004Q3，并与运行于 Windows 2003 Server 标准版或企业版平台上的 Active Directory 进行密码和属性同步。
- **对于用户同步的附加对象类支持：**可为辅助和结构对象类中的属性定义属性映射。对于 Active Directory，辅助类集将受用户所选择的主 / 结构对象类的限制。在 Directory Server 中，可使用任何其它对象类。
- **移植：**允许从版本 1.0 或 1.0 SP1 移植到版本 1 2004Q3。
- **Solaris 9 x86 平台支持：**Identity Synchronization for Windows 完全支持 Solaris 9 x86 平台。
- **Linkusers 和 resync 命令行操作：**linkusers 命令的功能现在已经与 resync 命令合并。resync 命令行选项现在又添加了三个选项。对应命令为：
  - `-f <linkusers.cfg> --` 链接文件（原来在 linkusers 命令中使用）
  - `-k --` 仅链接用户
  - `-i NEW_LINKED_USERS --` 重设新链接的用户的密码。除了对在 Directory Server 中链接的用户之外，此命令与 ALL\_USERS 和 NEW\_USERS 命令相同。

有关此新功能的详细信息，请参阅《*Identity Synchronization for Windows 安装和配置指南*》。

---

## 注意

由于 Windows NT 预计将于 2004 年 12 月被 Microsoft 完全 EOL，所以 Identity Synchronization for Windows 1 2004Q3 会修复与 Windows NT 相关的错误，但不会支持该平台的新功能。

有关其它信息，请参阅以下位置的 Windows Life Cycle Support:  
[http://support.microsoft.com/default.aspx?scid=fh;\[ln\];LifeWin](http://support.microsoft.com/default.aspx?scid=fh;[ln];LifeWin)

---

## 产品变更

以下是本产品 1 2004Q3 版本的变更：

- **安装：**因为 Sun Java Enterprise System 2 2004Q2 安装了 Sun Java System Message Queue 企业版和 Sun Java System Directory Server（此二者都是 Identity Synchronization for Windows 1 2004Q3 必需的），所以必须在安装 Identity Synchronization for Windows 1 2004Q3 前将 Sun Java Enterprise System 安装到 Solaris 系统中。

以前，Identity Synchronization for Windows 版本 1.0 曾安装了 Sun Java System Message Queue 3.0.1 (Message Queue)，但现在版本 1 2004Q3 没有安装。

- **重新确定产品和文档的品牌：**Identity Synchronization for Windows 产品和产品文档的品牌已从 *Sun ONE Identity Synchronization for Windows* 重新确定为 *Sun Java System Identity Synchronization for Windows*。

## 性能改进

同步性能已显著改善。

## 文档更改

**重新确定产品和文档的品牌：**Sun Java System Identity Synchronization for Windows 产品和产品文档的品牌已从 *Sun ONE Identity Synchronization for Windows* 重新确定为 *Sun Java System Identity Synchronization for Windows*。

# 硬件和软件要求

## 操作系统要求

以下各表描述了本版本 Identity Synchronization for Windows 的操作系统要求:

表 2        Solaris 要求

| 组件   | Solaris 要求   |
|--|--|
| 核心组件   | Solaris 8™ for UltraSPARC® （32 位和 64 位）<br>Solaris 9™ SPARC® 平台版 （32 位和 64 位）<br>Solaris 9™ 操作系统 （x86 Platform Edition for Pentium II 或更高版本） IA-32 |
| 用于 Sun Java™ System Directory Server 和 Windows Active Directory 的连接器 | Solaris 8 for UltraSPARC （32 位和 64 位）<br>Solaris 9 for SPARC 平台 （32 位和 64 位）<br>Solaris 9™ 操作系统 （x86 Platform Edition for Pentium II 或更高版本） IA-32  |
| Sun Java™ System Directory Server 插件                                 | Solaris 8 for UltraSPARC （32 位和 64 位）<br>Solaris 9 for SPARC 平台 （32 位和 64 位）<br>Solaris 9™ 操作系统 （x86 Platform Edition for Pentium II 或更高版本） IA-32  |

表 3        Windows 要求

| 组件   | Windows 要求   |
|--|--|
| 核心   | Windows 2000 Server SP4<br>Windows 2000 Advanced Server SP4<br>Windows Server 2003 标准版或企业版             |
| 用于 Sun Java™ System Directory Server 和 Windows Active Directory 的连接器 | Windows 2000 Server SP4<br>Windows 2000 Advanced Server SP 4<br>Windows Server 2003 标准版或企业版            |
| Sun Java™ System Directory Server 插件                                 | Windows 2000 Server SP4<br>Windows 2000 Advanced Server SP 4<br>Windows Server 2003 标准版或企业版            |
| NT 连接器和插件 （子组件）  | Windows Primary Domain Controller NT 4.0 Server SP 6A<br>（仅限 x86）                                      |
| 要与 Windows 2003 标准版和企业版服务器上的 Active Directory 进行同步                   | Windows Server 2003 Standard Edition （具有最新的安全更新）<br>Windows Server 2003 Enterprise Edition （具有最新的安全更新） |

## 硬件要求

要运行 Identity Synchronization for Windows，硬件（所有平台）必须满足以下最低要求：

- 最小安装所需的大约 400 MB 磁盘空间
- 运行任何 Identity Synchronization for Windows 组件的服务器需要的至少 512 MB RAM。（最好具有 1 GB 的 RAM）

## Sun Java System 软件要求

要运行 Identity Synchronization for Windows，必须安装下列 Sun Java System 软件组件：

- Sun Java System Message Queue Enterprise Edition 3.5 SP 1 版本（以前为 Sun ONE Message Queue）

Message Queue Enterprise Edition 3.5 SP 1 版本必须在安装 Identity Synchronization for Windows 前进行安装。而且，还建议先安装 Message Queue Enterprise Edition 3.5 SP 1 版本，然后再安装 Sun Java System Directory Server 5 2004Q2。

要在现有的 Sun Java System Message Queue 安装基础上安装 Identity Synchronization for Windows 核心，必须使用 Message Queue Enterprise Edition 3.5 SP1。尝试在不适当的 Message Queue 版本上安装 Identity Synchronization for Windows 核心将导致同步失败。

- Sun Java System Directory Server 版本 5 2004Q2 或更高版本

要安装 Identity Synchronization for Windows 1 2004Q3，必须运行 Directory Server 5 2004Q2（5.2 修补程序 2）

有关适用的 Solaris Package 安装程序或修补程序的详细信息，请参阅《[Sun Java System Directory Server 5 2004Q2 发行说明](#)》中的[重要信息](#)。

有关压缩归档 (ZIP) 安装、如何进行修补及压缩升级版中的已知问题的详细信息，请参阅《[Sun One Directory Server 5.2 发行说明](#)》中的[安装说明](#)。

要获得 Directory Server 5.2 修补程序 2（用于重要错误修复）修复的错误列表或查看所有应用的修补程序的各个 README 文件，请参阅：《[Sun Java System Directory Server 5 2004Q2 发行说明](#)》。

必须在部署中的每一 Directory Server 主服务器、副本服务器和集线器上安装 Directory Server 插件（子组件）。

有关在 Solaris 上安装 Directory Server 5 2004Q2 可能必需的修补程序的最新信息，请参阅《[Sun Java System Directory Server 5 2004Q2 Installation and Migration Guide](#)》及《[Sun Java System Directory Server 5 2004Q2 发行说明](#)》，这两个文档位于以下网站：

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

- Sun Java System Directory Server 5 2004Q2 Retrochangelog 修补程序

要更正 Directory Server Retrochangelog 以及 Identity Synchronization for Windows 1 2004Q2 中“删除”功能的问题，必须在 Sun Java System Directory Server 5 2004Q2 中安装一个修补程序。特定于您的环境系统的修补程序编号详细信息为：

- 对于 Solaris Sparc 软件包格式：修补程序编号为 117907-02 或更高
- 对于 Solaris Sparc 压缩的归档安装：修补程序 5077789
- 对于 Solaris X86 软件包格式：修补程序编号为 117908-02 或更高
- 对于 Solaris X86 压缩的归档安装：修补程序 5077789
- 对于 Windows 压缩的归档安装：修补程序 5077789

有关这些修补程序及如何将它们更新到 Directory Server 环境的详细信息，请参阅文件 README.patch，该文件位于 Identity Synchronization for Windows 下载目录：  
<download\_root>/patches/directory/README.patch

- Java Runtime Environment

J2SE Java Runtime Environment (JRE) 不随本产品一起提供。

- 必须安装 JRE 1.4.2\_04（或更高版本）才能在 Solaris 或 Windows Active Directory 上运行 Identity Synchronization for Windows 安装程序。也可安装 J2SE v 1.4.2\_04 SDK，其性能比 JRE 有所改进。
- 在 Windows NT 上必须安装 JRE 1.4.1\_03（或更高版本）。

另外，在安装 Identity Synchronization for Windows 之前必须在 Solaris 上将 JAVA\_HOME 设置为 1.4.2\_04 JRE（或更高版本），否则安装程序可能会报告未设置 JAVA\_HOME。

# 本版本中已修复的错误

下表描述了 Identity Synchronization for Windows 1 2004Q3 中已修复的错误：

表 4      Identity Synchronization for Windows 1 2004Q3 中已修复的错误

| 错误编号            | 说明   |
|-----------------|--|
| <b>安装 / 卸载</b>  |  |
| 4881466         | 在 7676 以外的端口上有现有 Message Queue 实例时安装 “核心” 组件会失败。   |
| 4829497         | 卸载程序未删除所有文件和文件夹。   |
| 4820869         | 在 Windows 上，重新安装 “核心” 组件前必须先重新启动系统。  |
| 4916789         | 为安装在同一 Server_Root 上的副本生成了重复 Directory Server 插件 ID。   |
| 5035406         | 使用 JRE 而非 JDK 时，在基于 Solaris 的机器上安装 “核心” 失败。  |
| 4880807         | runInstaller.sh 和 runUninstaller.sh 不支持 -nodisplay 选项。   |
| 5030928         | 安装程序不支持主主机和故障转移主机的不同证书。  |
| 5037157         | 在进行 “仅限 DS 插件” 安装后，卸载脚本不存在。  |
| 5050554         | 在 “-nodisplay” 模式下启动安装程序需要变量 DISPLAY。  |
| 4915192         | 不能在仅限 SSL 的 Directory Server 上安装连接器。   |
| 5052509         | 基于文本的卸载脚本不删除所有与 Identity Synchronization 相关的软件包。   |
| 4937341         | 无法在基于 Windows 的系统中使用 “添加 / 删除” 选项卸载 Identity Synchronization for Windows。                        |
| 5056685         | NT 插件卸载程序不删除密码过滤器 DLL （需要删除此过滤器，以便 Windows 启动时不加载该 DLL，确保该 DLL 已删除）。不删除此过滤器过去曾导致在重新安装组件的过程中出现问题。 |
| 4988901         | 对于某些安装程序面板，单击 “上一步” 按钮时不显示正确面板。  |
| 5030567         | 在 NT Connector 安装期间，安装程序不正确显示说明已经安装了 NT Connector 所有子组件的情况的提示性文本。                                |
| 5036330         | 安装期间，如果修改 “为管理域输入唯一的描述性名称 ...” 字段中描述性文本的默认值，则安装操作失败。   |
| 5041518         | 安装子组件期间单击 “上一步” 按钮，则错误显示 “连接器端口” 面板。   |
| 5048953/5049733 | 如果 JAVA_HOME 值包含引号，则卸载操作失败。  |
| 5050691         | 安装 “核心” 期间，“MQ 配置” 窗口显示有关系统中安装的 MQ 版本的错误消息。显示 “空”。   |
| 5057716         | 尽管成功卸载插件，但是 Directory Server 插件软件包及其注册表条目均未从系统中删除。   |
| 5071574         | Directory Server 连接器不接受有效端口号 (65535)。  |



**表 4** Identity Synchronization for Windows 1 2004Q3 中已修复的错误 (续)

| 错误编号                                 | 说明   |
|--------------------------------------|--|
| 5079602                              | nt_dll_registrar 不将“通知软件包”的值强制为 REG_MULTI_SZ。                              |
| <b>密码同步</b>                          |  |
| 4845844                              | Idsync resync 命令在同步时，从 Directory Server 创建用户到 NT 失败。                       |
| 4937502                              | 连接器在频繁失去网络连接后可能停止同步。   |
| 4939825                              | Directory Server 连接器不删除已修改条目的循环检测属性。                                       |
| 4906752                              | Sun Directory Server 中其后快速跟随有一个 modrdn 操作的用户创建操作不同步。                       |
| 4933861                              | 使用合成属性时，如果在“idsync resync -c -o Sun”后开始同步，NT Connector 显得过于活跃。             |
| 4941200                              | 只有大小写发生变化时，重命名的用户条目不进行同步。  |
| 4893525                              | 与 Active Directory 服务器之间的网络连接被终止时，属性修改丢失。                                  |
| 5019327                              | Directory Server 连接器通过对象类来同步用户，该对象类被设置为同步对象类类型的子类。                         |
| 4995351                              | Identity Synchronization for Windows 映射了不正确的属性。                            |
| 5036025                              | 修改 SUL 然后尝试同步用户导致 NullPointerException 错误（在日志文件中报告），而且连接器停止响应。             |
| 5054654                              | 突然复位或关闭连接器时，NT 密码的更改丢失。  |
| <b>Sun Java System Message Queue</b> |  |
| 4881240                              | 在 Solaris 上，不能使用安装在用户目录中的现有 Message Queue。                                 |
| <b>常规</b>                            |  |
| 4943564/4939730                      | Userpassword 不是可选属性。   |
| 4994145                              | 与不可用主机间的 Directory Server 插件测试连接过于频繁。                                      |
| 5041435                              | 启用“密码历史”选项后，密码更新即时请求会使 Directory Server 无法作出响应。                            |
| 4939859                              | 源连接器是 Windows NT 时，Idsync linkusers/resync 会忽略 LDAP 过滤器选项。                 |
| 4987742                              | resync 因竞争情况而不处理所有条目。  |
| 5048362                              | 不自动删除来自日志消息的换行符。   |
| 4925575                              | Active Directory 连接器安装程序不进行确保域与证书域相匹配的检查。                                  |
| 4901486                              | 以前，Identity Synchronization for Window 1 2004Q3 不支持多个 Active Directory 森林。 |
| <b>控制台常规错误</b>                       |  |
| 5040094                              | “objectclass=<some oc>”报告了一个无效过滤器错误。                                       |
| 5030704                              | 无法从“控制台”修改“活动”目录源的 resync 时间间隔。  |
| 5026929                              | 无法为强制创建属性指定默认值。  |
| 4941238                              | 日志查看器不正确解析日志记录。  |

表 4 Identity Synchronization for Windows 1 2004Q3 中已修复的错误 (续)

| 错误编号     | 说明  |
|----------|---|
| 5026198  | 已改正 “日志” 窗口中的拼写错误。  |
| 5044529  | 控制台命令 <code>prepds</code> 对仅限 SSL 的 Directory Server 不起作用。                              |
| 5008697  | 编辑 <code>cn</code> 映射时向列表中添加其它项，而不是更新现有项。   |
| 50134407 | 可以创建与现有目录源同名的目录源。不显示错误消息，也无法删除该目录源。   |
| 5026198  | 已改正 “控制台” 的 “日志” 窗口中存在的拼写错误。  |
| 5044529  | 控制台命令 <code>prepds</code> 对仅限 SSL 的 Directory Server 不起作用。                              |
| 5045350  | 修改现有创建属性后，值无法设置为 < 无 >。   |
| 4921889  | 再次选择 “查看” 下的 “树” 选项时，“控制台” 不能返回正常树视图。   |
| 连接器      |   |
| 4988028  | 缺失 <code>usnchanged</code> 属性上有 “Java 运行时间例外” (RTE)。                                    |
| 命令行实用程序  |   |
| 5015766  | 将空密码传递到 <code>idsync changepw</code> 导致无法后续访问配置注册表。                                     |
| 4986303  | 命令行界面没有为 <code>-h</code> 、 <code>-p</code> 、 <code>-D</code> 和 <code>-s</code> 选项提供默认值。 |
| 5038195  | 配置后缀无效时， <code>resetconn</code> 不提供相应的错误消息。   |
| 5019543  | 配置后缀无效时， <code>printstat</code> 不提供相应的错误消息。   |
| 5024148  | <code>resetconn</code> 不删除连接器 Message Queue 证书。   |
| 4941125  | 当源是 Sun 且已同步合成属性时， <code>resync</code> 会更新同步用户。   |
| 4939484  | <code>linkusers</code> 命令可能始终不退出。   |
| 5015575  | 在命令行提示符后执行 “c” 命令时，CLI 操作不停止。   |
| 5062028  | 安装具备 SSL 的 “核心” 时，命令行提示符停止响应。(CLI 上端口的默认值为 SSL 端口。)                                     |

---

# 重要信息

本节包括核心产品文档中未包含的最新信息。包括以下主题：

- [安装说明](#)
- [兼容性问题](#)
- [系统或应用程序失败时执行数据恢复](#)
- [Identity Synchronization for Windows 1 2004Q3 的文档更新](#)
- [在装有防火墙的环境中运行 Identity Synchronization for Windows](#)

## 安装说明

在安装 Identity Synchronization for Windows 1 2004Q3 前，请务必阅读 《Sun Java™ System Identity Synchronization for Windows 1 2004Q3 安装和配置指南》中的“准备安装”一章。

### 使用 Windows 2003 Server

- 现在，可以使用 Windows 2003 Server 标准版或企业版作为安装和配置 Identity Synchronization for Window 1 2004Q3 的平台。
- 在 Windows 2003 Server 上，默认的密码策略将强制使用严格的密码，但 Windows 2000 中的默认密码策略并非如此。

### *Windows 2003 Server 问题*

在对“用户必须在下次登录时更改密码”的处理上，**Windows 2003 Server 与 Windows 2000 不同。**  
**(4997513)**

在 Windows 2003 上，会默认设置用户必须在下次登录时更改密码标志，但在 Windows 2000 上却并非如此。

如果在已设置“用户必须在下次登录时更改密码”标志的情况下在 Windows 2000/2003 上创建用户，则在 Directory Server 上创建的用户不使用密码。这些用户在下次登录 Active Directory 时会被强制要求更改密码，从而使他们在 Directory Server 上的密码失效，并且会在这些用户下次进行 Directory Server 验证时强制执行即时请求同步。

除非用户在 Active Directory 上更改其密码，否则将无法通过 Directory Server 验证。

# 兼容性问题的兼容性

使用特定“远程控制台”产品访问 Identity Synchronization for Windows 控制台时产生的兼容性问题。  
(5077227)

尝试使用 PCAnywhere 10.x 或 Remote Administration2.1 查看 Identity Synchronization for Windows 控制台时，可能会出现问题。（但 PCAnywhere 9.2 版本不会引起问题。）如果问题一直存在，请删除 Remote Administration 软件。或者，可选择使用 VNC，目前它在显示 Identity Synchronization for Windows 控制台时尚不会引起任何问题。

## 系统或应用程序失败时执行数据恢复

如果出现硬件或应用程序故障，可能必须从某些已同步的目录源中的备份恢复数据。

但是，完成数据恢复后，还必须执行一个附加过程，以确保同步可以正常继续。

一般而言，连接器维护有关传播到信息队列的最新更改的信息。

此数据（称为连接器状态）用于确定连接器必须从其目录源读取的后续更改。如果某个已同步目录源的数据库是从备份恢复的，则连接器状态可能不再有效。

基于 Windows 的连接器（Active Directory 或 Windows NT）还维护一个内部数据库。此数据库为已同步数据源的副本，用于确定连接的数据源中发生了哪些变化。显而易见，一旦从备份恢复连接的 Active Directory 源或 Windows NT 系统，则该内部数据库将不再有效。

通常，idsync resync 命令可用于重新填充恢复的数据源。

注意

重新同步不能用于同步密码，但有一个例外。如果重新同步数据源是 Windows（而且 SUL 列表仅包括 Active Directory 系统），-i ALL\_USERS 选项可用于使 Sun Java Systems Directory Server 系统中的密码无效。

但是，使用 idsync resync 并不是在每种情况下都是合理选项。

警告

在执行下述任何步骤之前，请确保同步已停止。

## 双向同步

建议过程是（根据同步设置）使用带有相应的修改人设置的 idsync resync 命令。resync 操作的目标应该是恢复的目录源。

## 单向同步

如果恢复的数据源为同步目标，则可以遵循与双向同步相同的过程。

如果恢复的数据源为同步源，则仍然可以使用 `idsync resync` 重新填充恢复的目录源。不需要更改 Identity Synchronization for Windows 配置中的同步流动设置，`idsync resync` 允许使用 `-o <Windows|Sun>` 选项独立于已配置的流动对同步流动进行设置。

请考虑下列示例情况：

在 Sun Java Systems Directory Server 和 Active Directory 之间建立了双向同步

- 必须从备份恢复 Microsoft Active Directory 服务器的数据库。
  - 在 Identity Synchronization for Windows 中，为 SUL “AD” 配置了此 “Active Directory 源”。
  - 在此 “Active Directory 源” 与 “Sun Directory Server 源” 之间建立了修改、创建和删除的双向同步。
1. 停止同步 `idsync stopsync -w - -q -`
  2. 重新同步 “Active Directory 源” 并重新同步修改、创建和删除：`idsync resync -c -x -o Sun -l AD -w - -q -`
  3. 重新启动同步 `idsync startsync -w - -q -`

## 目录源特定恢复过程

### *Microsoft Active Directory*

如果可从备份恢复 Active Directory，则请遵循双向同步或单向同步章节中描述的过程。

但是，可能有必要在出现严重故障之后使用不同的域控制器。此时，请遵循下列步骤更新 Active Directory Connector 的配置：

1. 启动 Identity Synchronization for Windows 管理控制台。
2. 选择 “配置” 选项卡。
3. 展开 “目录源” 节点。
4. 选择适当的 “Active Directory 源”。
5. 单击 “编辑控制器 ...”
6. 选择新的域控制器。

建议您将选定的域控制器作为该域的 NT PDC FSMO 角色属主

7. 保存配置。

8. 停止运行 Active Directory Connector 的主机上的 Identity Synchronization 服务。
9. 删除 <serverroot>/isw-<hostname>/persist/ADPxxx 之下的所有文件（但不删除目录），其中 xxx 是 Active Directory Connector 标识符的编号部分（例如，若 Active Directory Connector 标识符为 CNN100，则为 100）。
10. 启动运行 Active Directory Connector 的主机上的 Identity Synchronization 服务。
11. 遵循单向同步或双向同步章节中基于您的同步流动的步骤。

## Sun Java System Directory Server

Retro Changelog 数据库或拥有同步用户的数据库（或这两者）均可受严重故障的影响。

1. Retro-Changelog 数据库。

Retro- Changelog 数据库中可能出现了 Directory Server 连接器无法处理的更改。只有备份包含某些未处理的更改时，恢复 Retro Changelog 数据库才有意义。这可通过将 <serverroot>/isw-<hostname>/ADPxxx/accessor.state 文件中最新的条目与备份中的最后一个 changenumber 进行比较来实现。如果 accessor.state 中的值大于或等于备份中的 changenumber，则没有必要恢复数据库，但应重新创建数据库。

重新创建 Retro-Changelog 数据库之后，请确保运行 idsync prepds 或在 Identity Synchronization for Windows 管理控制台“Sun 目录源”窗口中单击“准备 Directory Server”。

Directory Server 连接器将会检测到已重新创建了 Retro-Changelog 数据库并将一条警告消息记录到日志中。可以忽略此消息，不会出现安全问题。

2. 已同步的数据库。

如果没有可用于已同步数据库的备份，则必须重新安装 Directory Server 连接器。

如果可从备份恢复已同步数据库，则请遵循双向同步或单向同步章节中描述的过程。

## Identity Synchronization for Windows 1 2004Q3 的文档更新

可通过浏览器访问 Identity Synchronization for Windows 联机文档文件。另外，也可下载整个文档集（HTML 格式）。

在下载此文件后，请将其提取到以下位置：

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

ServerRoot 是 Sun Java System Administration Server 的位置。实际的 ServerRoot 路径将视用户的平台、安装和配置而定。ServerRoot 目录包含 startconsole 程序。

然后，便可以直接从 `<ServerRoot>/manual/en/isw/index.html` 访问该文档集，或者通过从“帮助”菜单选择“文档主页”，从“服务器控制台”访问。

## 在装有防火墙的环境中运行 Identity Synchronization for Windows

可在装有防火墙的环境中运行 Identity Synchronization for Windows。本节描述了必须暴露在防火墙外的那些服务器端口，如下所示：

- [Message Queue 要求](#)
- [安装程序要求](#)
- [核心组件要求](#)
- [控制台要求](#)
- [连接器要求](#)
- [Directory Server 插件要求](#)

### Message Queue 要求

默认情况下，Message Queue 为所有服务（其端口映射程序除外）使用动态端口。要通过防火墙访问 Message Queue Broker，对于所有服务，代理程序都应使用固定端口。

安装核心后，必须设置 `imq.<service_name>.<protocol_type>.port` 代理程序配置属性。特别是，必须设置 `imq.ssljms.tls.port` 选项。有关详细信息，请参阅《*Sun Java™ System Message Queue Administrator's Guide*》。

### 安装程序要求

Identity Synchronization for Windows 安装程序必须能与充当配置目录的 Directory Server 通信。

- 如果要安装 Active Directory 连接器，则安装程序必须能够联系 Active Directory 的 LDAP 端口（端口 389）。
- 如果要安装 Directory Server 连接器或 Directory Server 插件（子组件），则安装程序必须能够联系 Active Directory 的 LDAP 端口（默认端口 389）。

### 核心组件要求

Message Queue、系统管理器和命令行界面必须能够联系存储 Identity Synchronization for Windows 配置的 Directory Server。

## 控制台要求

Identity Synchronization for Windows 控制台必须能够联系下列项目：

- Active Directory （通过 LDAP （端口 389）或 LDAPS （端口 636））
- Active Directory 全局目录 （通过 LDAP （端口 3268）或 LDAPS （端口 3269））
- 每一个 Directory Server （通过 LDAP 或 LDAPS）
- Sun Java System Administration Server
- Message Queue

## 连接器要求

所有连接器都必须能够与 Message Queue 通信。另外：

- Active Directory 连接器必须能够通过 LDAP （端口 389）或 LDAPS （端口 636）访问“Active Directory 域控制器”。
- Directory Server 连接器必须能够通过 LDAP （默认端口 389）或 LDAPS （默认端口 636）访问 Directory Server。

## Directory Server 插件要求

每个 Directory Server 插件都必须能够联系 Directory Server 连接器的服务器端口，此端口是在安装该连接器时选择的。在 Directory Server Master 副本中运行的插件必须能够连接到 Active Directory 的 LDAP （端口 389）或 LDAPS （端口 636）。在其它 Directory Server 副本中运行的插件必须能够联系 Master 的 Directory Server LDAP 或 LDAPS 端口。



---

# 已知问题和限制

本节包含了 Identity Synchronization for Windows 1 2004Q3 已知问题的列表。涉及以下产品区域：

- [安装和卸载](#)
- [连接器和插件](#)
- [控制台和命令行](#)
- [密码同步](#)
- [Sun Java System Message Queue](#)
- [常规问题](#)

## 安装和卸载

有关手动擦除产品注册表的说明。 **(5050004)**

如果需要从产品注册表中删除对 Identity Synchronization for Windows 的引用，请遵循 《*Identity Synchronization for Windows 安装和配置指南*》中的第 7 章 “如果 1.0 卸载失败应采取何种措施” 中针对 Windows NT 和 Windows 2000 平台介绍的过程。

如果核心安装在名称内有空格的目录中，则 **Solaris** 脚本将不会工作。 **(4801643)**

如果将 Identity Synchronization for Windows 核心安装在路径名内有空格的目录中，则 Solaris 上的命令行脚本将不会工作。

如果 “基本 DN” 包含空格，则 **Message Queue Broker** 将无法启动。 **(4892332 和 4892490)**

请勿将核心安装在含有空格的后缀上，否则 Message Queue Broker 将无法进行验证。

有现有 **Message Queue** 实例时安装核心的副作用。 **(4882194)**

有现有 Message Queue Broker 实例时安装核心会影响该现有实例。例如，对一个现有配置进行了如下修改：

- `/etc/imq/imqbrokerd.conf` 文件被修改为在启动时自动启动代理程序，这将使从 `/etc/init.d/imq` 脚本启动的其它代理程序实例在系统重新启动时不会启动。

### **Message Queue Broker 最小需要 512MB 内存。(4819519)**

Message Queue Broker 需要最小 512 MB 的内存。由于代理程序是作为核心的一部分安装的，所以安装核心的机器至少应有 1GB 的 RAM。

### **从“多目录服务器”实例安装中卸载插件会删除卸载程序。(4916035)**

如果两个 Directory Server 实例具有相同的文件系统安装根（例如 `/usr/sunone/servers/slapd-foxhead` 和 `/usr/sunone/servers/slapd-foxhead2`），则将无法卸载多个插件。

*解决方法：*

1. 打开 Directory Server 控制台（用于安装插件的 Directory Server）。
2. 单击“配置”选项卡。
3. 双击 Plugins 文件夹，展开插件树。
4. 单击 `pswsync` 并取消选中“启用插件”复选框。
5. 重新启动 Directory Server。

### **如果在完成前取消安装并再次尝试重新安装，则 Active Directory 连接器的性能将不确定。(5038905)**

如果安装程序在进行到配置连接器时被取消，然后再次执行，则不可安装连接器选项。

*解决方法*

从命令行提示符运行 `idsync resetconn`，复位连接器的配置，然后重新运行安装程序以重新安装连接器。有关运行 `idsync resetconn` 命令的详细信息，请参阅《*Sun Java System Identity Synchronization for Windows 安装和配置指南*》。

### **在卸载产品时，与产品相关的注册表主键未被删除。(5045237)**

执行核心卸载后，产品注册文件中的 Sun Java System Identity Synchronization for Windows 相关节点未被删除。要成功地重新安装产品，必须手动从产品注册表主键中删除这些节点。有关删除这些产品注册表主键的详细信息，请参阅《*Identity Synchronization for Windows 安装和配置指南*》。这种情况只在 Solaris 8 中发生。

如果在未连接到配置注册表的情况下卸载“核心”，则 Identity Synchronization for Windows 相关引用会显示在“控制台”中。(5049700)

如果在对 Identity Synchronization for Windows 执行盲卸载（即未连接到配置注册表）后启动“控制台”，会显示一条错误消息。

### **“temp”目录（记录安装日志的目录）可能是一个隐藏目录。(5051905)**

在某些 Window 系统上，`C:\Documents and Settings > Administrator > Local Settings` 文件夹可能是一个隐藏文件夹。

### 解决方法

要查看 Local Setting 文件夹和 Temp 子文件夹，应选择 “Windows 资源管理器” 选项显示隐藏的文件。或者，在命令提示符后键入 `cd %TEMP` 或 `cd %TMP`，以查看目录中与安装相关的日志文件。然后，便可用 “记事本” 查看这些日志。

### 如果根后缀包含空格，则 Message Queue Broker 验证便会失败。(4892903)

由于 Message Queue 的限制，Identity Synchronization for Windows 配置必须存储在不含任何空格的根后缀中。

### 解决方法

在安装 “核心” 前，创建新的根后缀以存储 Identity Synchronization for Windows 配置。

### 在 Directory Server 插件安装失败之后，“待执行”列表显示该插件安装已完成。(5081912)

在某些情况下，尽管插件安装实际上已经失败，但 “待执行” 列表可能显示已经安装 Directory Server 插件。

### 卸载连接器期间，卸载程序不能精确显示要恢复的磁盘空间。(5081823)

卸载连接器时，卸载程序不精确地显示 0 字节（卸载过程后将恢复的字节数）。查看磁盘空间的属性时，实际恢复的磁盘空间大小不会为零。

### 安装程序不强制您将组件安装在 Directory Server 插件安装目录所在的目录中。(5080178)

如果 Directory Server 插件是在机器上安装的第一个组件，则该特定机器上所有后续的组件都必须安装在同一安装目录（Directory Server 插件所在的目录）中。但在安装过程中，安装程序并不强求满足此条件。

### 卸载组件时，卸载程序可能显示错误信息。(5079489)

当从并未安装 “核心” 组件的机器卸载连接器时，安装程序会错误地报告正在卸载 “核心” 组件。可忽略此消息。

### 如果在配置目录不存在的情况下执行卸载过程，则不删除 Identity Synchronization for Windows 控制台引用。(5077156)

选中 “卸载产品而不卸载配置目录” 选项时，Sun Server Console 保留所有对 Identity Synchronization for Windows 控制台的引用。卸载产品之后，Identity Synchronization for Windows 的图标仍存在于拓扑树中。尝试显示控制台时出错。有关删除控制台引用的详细信息，请参阅《Identity Synchronization for Windows 安装和配置指南》第 8 章中的 “手动卸载控制台” 一节。

### 卸载并不删除 “server-root/isw-\*/lib” 目录和 jar 文件。(5038284)

卸载操作不删除包含 \*.jar 文件的 lib 目录。这些文件和目录必须手动删除。

**取消安装操作和重新安装时，Active Directory 连接器的性能不确定。(5038905)**

安装 Active Directory 连接器时，如果突然取消安装操作，然后试图重新安装连接器，则 Active Directory 连接器将错误地显示状态“已安装”。试图安装时，此状态不发生变化且不会发生同步操作，也不可能重新安装 Active Directory 连接器。

**解决方法**

必须运行 `idsync resetconn` 命令以重新安装连接器。有关运行 `idsync resetconn` 命令的详细信息，请参阅《*Identity Synchronization for Windows 安装和配置指南*》。

**在安装有 Sun Java Enterprise System 3 的 Directory Server 5.2p3 上安装 Identity Synchronization for Windows 失败。(5092530)**

不能为 Directory Server 5.2 P3（或更高版本）安装核心 Identity Synchronization for Windows 产品。Identity Synchronization for Windows 1 2004Q3 仅将 Sun Java Enterprise System 3 (Directory Server 5.2 P3) 作为数据同步源支持。

**在备用主服务器上安装 Directory Server 插件后，安装列表仍会提示安装该插件。(5096593)**

“待执行”列表几乎总是很精确，但有时可能不能报告所需的步骤，也不能识别出某些步骤已执行。例如，可能不总是反映出已安装或需要安装哪些 Directory Server 插件。

**在 FAT32 系统上安装的 Identity Synchronization for Windows 没有 ACL。(5097751)**

在 FAT32 格式的设备上安装 Identity Synchronization for Windows 后，到 ACL 中查看文件夹和文件时发现 ACL 不存在。建议不要在非 NTFS 分区上安装。

**使用 Directory Server 压缩版时，仅卸载插件可能会失败。(5101589)**

试图执行仅卸载插件操作时，如果使用 Directory Server 的压缩存档软件包，则该操作会失败。

**出现提示后如果使用多字节的管理员名称，则安装操作会失败。(5109332)**

如果输入了多字节 LDAP 管理员名称，则在“核心”安装过程中出现提示时，该操作将失败。将显示消息“安装程序无法上载模式文件 `/var/opt/isw/SUNWisw/misc/40so-psw.out.ldif`。有关详细信息请查看安装程序的日志文件”。安装进程将被中断，并且对话框窗口会突然终止。

**解决方法**

确保使用默认的“admin”LDAP 管理名称进行安装，以避免出现此问题。如果上一安装失败，请重新启动安装程序并使用默认的管理员名称重新安装“核心”。可能会显示消息“已在机器上找到核心文件”。可安全地忽略此消息。继续完成安装操作。

## 连接器和插件

### 删除预先存在的条目会启动 NT 连接器同步。 (4864009)

带有现有 Windows 用户（Active Directory 或 NT）的安装必须在开始同步前，运行 `idsync resync` 命令，以防止性能不确定（如现有 Windows 用户随时被同步到 Directory Server）。

### 如果连接器处于非活动状态，则重新启动它们。 (4938309)

如果中心错误日志报告了一条类似于连接器 [CNN100] 无响应已长达 10 分钟的消息，则可能必须停止并重新启动正在运行连接器的 Identity Synchronization for Windows 守护进程 / 服务程序。

#### 解决方法

- 在 Solaris 上，先后发出 `/etc/init.d/isw stop` 和 `/etc/init.d/isw start` 命令。
- 在 Windows 上，重新启动 Sun Java System Identity Synchronization for Windows 服务程序。

### 为 Directory Server 插件启用“加密套接字层”后重新启动 Directory Server。 (4944804)

为 Directory Server 插件（子组件）启用“加密套接字层” (SSL) 并将 Active Directory CA 证书添加到 Directory Server 的证书数据库后，必须重新启动 Directory Server，否则“即时请求”同步可能会在验证已更改了 Active Directory 上密码的用户时失败（请参阅样例日志消息）。

### 如果 Active Directory 搜索超时，管理员应提高搜索限制。 (4881182)

如果 Active Directory 错误日志报告某连接器出现超时错误，请使用 Windows 2000 资源工具包的 `ntdsutil` 来增加最大搜索超时，如下所示：

```
C:\>cdif>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
```

**Sun Java System Directory Server 不会处理没有用 ;binary 子类型来创建的二进制值属性。(5029226)**

某些属性（如 userCertificate）的创建实例需要 ;binary 选项。Identity Synchronization for Windows 可同步这些属性的值，但不会在创建时设置 ;binary 选项。这可能会使客户与 Sun Java System Directory Server 间的通信出现问题。如果没有用二进制选项创建某属性，而客户机请求具有二进制选项的属性，则 Sun Java System Directory Server 不会返回此属性。

**Identity Synchronization for Windows 不会在创建 user\_name 属性时验证所用的字符数。(5021886)**

对于“user\_name”属性，NT SAM 的限制为 20 个字符，而 Sun Java Directory Server 对创建用户名时使用的字符数没有限制。映射到 NT SAM 上“user\_name”属性的条目尽管成功地从 NT SAM 流动到了 Sun Java Directory Server，但也不能使用。在 NT SAM 上编辑或查看该条目的属性时，会显示错误消息。

## 控制台和命令行

如果“Retro 更改日志”数据库文件被重新创建、破坏或缺失，请运行 `idsync prepds`。(4921114 和 4832355)

如果“Retro 更改日志”(RCL)数据库曾被删除或破坏，则 Directory Server 或 Directory Server 连接器将发出警告消息。出现这些消息时，必须重新创建 Retro Changelog 并重新运行 `idsync prepds` 命令，然后才能恢复同步。

选择新的命名上下文后，为“基本 DN”选择的“浏览”按钮不会更改。(4944711)

如果从控制台将 Identity Synchronization for Windows 配置为使用一个以上 Directory Server 源和两个以上 Active Directory (AD) 源，则在配置新的“同步用户列表”(SUL)时，为基本 DN 显示出的供选择的“浏览”按钮可能不能准确反映正确的 Directory Server 或 Active Directory 源。

### 解决方法

将“基本 DN”名称手动键入“基本 DN”字段。

控制台模式主机应指向配置目录。(4877996)

指定模式主机时，建议仅使用核心配置目录。请勿使用独立的 Directory Server 或任何其它远程配置目录。

“控制台状态”窗口不提供用于查看日志文件的 508 访问权限。(4874361)

“控制台状态”窗口中的“日志文件查看器”不允许通过无鼠标的界面查看日志文件。

### 解决方法

要查看日志文件，请将文件复制到喜欢的文本编辑器（在“控制台日志查看器”之外）中。

Message Queue 的控制台状态不能正确指示系统组件的实际状态。(4937312)

如果“控制台”和 MessageBroker 之间的网络连接中断，则“控制台”可能无法正确报告系统组件的状态。

### 解决方法

如果出现网络问题，请务必重新启动“控制台”。也可执行 `idsync printstat` 命令来更加准确地查看消息队列的状态。

在添加新的 Directory Server 数据源时，尽管 Directory Server 已经准备就绪，仍出现一条消息提示用户准备 Directory Server。(5029558)

创建新 Sun Java System Directory Server 源时，始终会提示用户准备 Directory Server 源。如果已经准备了目录源，则可安全地单击“否”选项。

执行 CLI 命令 `resetconn` 时，显示消息“正在重设 ...”。重设密码失败，并且所有关于 Directory Server 源、配置等的信息都被删除。(5039655)

执行 `resetconn` 命令行功能时，“控制台”不应运行。如果在执行该命令前未退出“控制台”，则会显示“正在重设 ...”消息。此时，应退出“控制台”并重新启动它。

**“startsync”命令无法执行。显示错误消息“启动某些已请求目录源的同步失败 ...”。(5050443)**

某些情况下（例如内存不足），即使某些组件无法开始同步，命令行或管理控制台也可能会报告“开始同步”已经成功。遇到同步问题时，请查看错误日志以寻找与内存相关的消息。

**在单值属性具有多个值的情况下，参数化属性失败。(5069907)**

为单值属性指定多个值而不是单个值时，同步失败。将这些值保存到 Directory Server 时，将出现错误或警告消息。

**执行 `idsync` 命令时，在屏幕上以明文形式显示密码。(4900126)**

输入密码时，`idsync` 命令提示输入绑定和配置密码时，它们以明文形式显示而且不加密。

#### 解决方法

为了避免密码显示在屏幕上，可将每个密码都存储到一个受保护的文件中，然后将其重定向到命令行。如果为任何密码参数提供了“-”选项，`idsync` 命令会按照各选项在命令行中出现的顺序提示输入相应密码值。例如，如果管理员密码为 `adminPw`，配置密码为 `configPw`，则应创建具有下列内容的文件 (`passwords.txt`):

```
adminPw
configPw
```

然后执行 `idsync printstat -w - -q - < passwords.txt` 来运行该命令。

**加载日志文件时出错。(5091787)**

某些情况下，当在“状态”选项卡的“控制台”中加载 `audit.log` 文件时，可能会显示下面的错误消息：“因为未知错误而无法检索日志条目。需要重新启动管理员服务器。”

#### 解决方法

访问并随后试图加载该文件时，将加载 `audit.log` 文件。

**Prepds 在移植时会在 MMR 设置中显示一条错误消息。(5093124)**

在复制环境中进行移植时，`idsync prepds` 可能会错误地报告模式复制已失败。（例如，错误消息可能如下：“在 `ldap://preferred.example.com:389`，首选 Sun Java System Directory Server 将模式更改复制到在 `ldap://secondary.example.com:389` 的备用 Sun Java(TM) System Directory Server 失败。请检查复制设置”）。此时，请使用同一参数重新运行 `idsync prepds`。仅当第二次运行 `idsync prepds` 出现同样的错误消息时查看复制设置。



**使用 Reflection X 10.0 访问“控制台”可能无效。(5095013)**

某些对话框可能不可用，原因是按钮或文本框不可见，也不能调整对话框的大小。

**“控制台”中的“日志”消息显示被破坏的多字节字符。(6174184)**

仅当使用多字节同步用户列表名或要同步多字节后缀时，才在日志中报告多字节字符。要正确查看日志消息，请在显示 UTF-8 编码文档的查看器中打开日志文件 (/var/opt/SUNWisw/logs/central/error.log)。

**配置密码被更改后，startsync 和 stopsync 命令不能正常起作用。将显示一条错误消息。(6175396)**

使用 idsync changepw 命令更改了 Identity Synchronization for Windows 配置密码并且未重启机器时，idsync startsync 和 stopsync 命令不能正常起作用。这两个命令将显示类似以下的消息：“接收的消息未加密”，并返回退出代码 1。

虽然显示了此错误消息，但却进行了开始 / 停止同步操作。要对此进行验证，请运行 idsync printstat 命令。但为了避免出现此问题，请确保每次更改配置密码后重启机器。

## 密码同步

**密码策略问题。(4834865 和 4811572)**

不同目录上使用的密码策略可以导致同步错误。如密码长度以及必需的最大和最小字符数。管理员必须手动更改不兼容的密码策略，使其与其它系统的密码策略相一致。

**同时修改的相应属性或密码可能不会正确同步。(4854183 和 4808601)**

在两个目录源之间同步某条目的过程中，如果同时对某一属性进行了多项修改，则该属性可能不会正确同步。例如，假设各事件的顺序如下。

- John Smith 在 Active Directory (AD) 中将其电话号码更改为 555-1111。
- 这一更改将传播至 Directory Server；但是，在此更改到达之前，管理员在 Directory Server 中错误地将 John Smith 的电话号码设置为 555-1112。
- 然后，在 Active Directory 中进行的更改被应用于 Directory Server，John Smith 的电话号码被设置为 555-1111。
- 同样，在 Directory Server 中进行的更改被传播到 AD，John Smith 的电话号码被设置为 555-1112。

这两个目录源交换了值并变成了不同步。

同样，如果几乎同时在 Active Directory (AD) 和 Directory Server 上修改用户密码，在某些情况下密码也可能不会正确同步。

在负荷较小的系统中，只有在相差数秒之内发生的多个密码修改才会不同步。即使在 AD 密码被设置为 Directory Server 值之后再修改它也会发生此种情况，但是一般不太可能在 AD 密码被设置为 Directory Server 值后的几毫秒内就必须修改它。

#### **使用 Active Directory 的“用户必须在下次登录时更改密码”功能。(4827180)**

如果管理员在 Active Directory (AD) 上更改了用户的密码并指定“用户必须在下次登录时更改密码”，则在用户登录并更改其密码之前，密码更改不会同步到 Directory Server。

在下列环境下，用户验证会失败：

1. 用户在 AD 上更改了其密码。（该密码传播到 Directory Server，Directory Server 密码无效）。
2. 管理员重设用户密码，并设置“用户必须在下次登录时更改密码”标志。
3. 如果用户尝试使用来自 #1 或 #2 的密码登录到 Directory Server，则该登录尝试将失败。更改 AD 或 Directory Server 中的密码将更新 Directory Server 密码值。

#### **在已启用 7 位检查插件的 NT 或 Active Directory 中指定非 ASCII 密码将使密码无法同步到 Directory Server。(4817344)**

在 Directory Server 上，对于 userpassword 属性值，默认情况下将启用 7 位检查插件（子组件）。请参阅：<http://docs.sun.com/source/816-6699-10/pluginattr.html>

如果将非纯 7 位元的密码从 Windows 同步到 Directory Server，然后为 userpassword 属性值启用并配置此插件，则同步将失败。

必须谨慎对待具有非 ASCII 字符的同步密码，因为密码值的字符编码方法不是持续不变的。因此，Windows 端的客户机和 Directory Server 客户机在更改密码时（以及在验证时）必须使用相同的字符编码方法，否则操作会失败。

#### **不支持多密码值。(4807350)**

不支持多用户密码值。

#### **重新启动系统管理器时，Resync 不自动恢复 resync 进程。(5077660)**

执行 resync 命令并重新启动系统管理器时，resync 不自动恢复和重新启动该进程。

#### **执行重新同步时，创建属性可能会被删除。(5085134)**

#### **对某个属性进行并行更新不能被同步。(5077760)**

为某个属性添加值时，如果几乎同时也在为相应远程目录条目中的同一属性添加不同的值，则会出现此问题。该属性可能不会被同步。

执行重新同步时，即使重新同步操作已中止，**Directory Server** 连接器也未收到链接操作。(4985505)

执行 `resync -c -o Sun` 时，在 Active Directory 中创建新用户之后，“链接”操作被发送到 Directory Server。尽管 `resync` 操作已中止，Directory Server 连接器仍未收到这些“链接”操作。当前，这些“链接”操作与所有 `resync/linkusers` 操作发布于同一临时 MQ 主题中。

由于 **Directory Server Retro-Change Log** 插件中的一个已知问题而无法将删除的条目从 **Directory Server** 同步到 **Active Directory**。(5077814)

Directory Server Retro-ChangeLog 插件可能无法在插件条目中为删除的条目存储 `dspswuserlink`。如果发生这种情况，则不会将 Directory Server 条目的已删除条目同步到 Active Directory。

#### 解决方法

要解决此问题，请确保已经用解决此问题的修补程序更新 Directory Server。有关解决此问题需要的修补程序的信息，请参阅 [“Sun Java System Directory Server 5 2004Q2 Retrochangelog 修补程序”](#) 一节。

## Sun Java System Message Queue

**系统管理器无法连接到 Message Queue。(4907711)**

系统管理器无法连接到 Message Queue，且 Message Queue 已打开。

#### 解决方法

重新启动安装核心的 Identity Synchronization for Windows 服务程序 / 守护进程。

**增加 Message Queue Broker 用于部署 100K+ 用户的最大内存。(4924939)**

Identity Synchronization for Windows 将 Message Queue Broker 配置为在默认情况下使用最大 512 MB 内存，该内存足够供大多数安装使用。但是，对于安装容量超过 100K 的用户，则应将最大内存增加到至少 1 GB 才能确保获得最佳性能。对于超过 200K 的用户的部署，请将内存增加到 2 GB。

如果在 *Solaris* 上安装 Identity Synchronization for Windows 核心，则请使用下列步骤来提高 Message Queue Broker 的内存限制：

1. 发布以下命令，停止 Message Queue Broker：

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

2. 编辑 `/etc/imq/imqbrokerd.conf` 文件，将当前默认内存设置 `-Xmx512m` 更改为 `-Xmx1024m` 以获得 1 GB 内存，或更改为 `-Xmx2048m` 以获得 2 GB 内存。

3. 发布以下命令，启动 Message Queue Broker：

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

如果在 Windows 2000 上安装 Identity Synchronization for Windows 核心，则请使用下列步骤来提高 Message Queue Broker 的内存限制：

1. 使用 Windows Services Management 控制台，停止 Message Queue Broker 服务程序。
2. 在 `<installation-root>/isw-<machine-name>/imq/bin` 目录，从命令行发出 `imqsvcadmin query` 命令。其输出将与下列内容相似：

```
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. 将此命令产生的输出保存到文件中。
4. 通过发出 `imqsvcadmin remove` 命令来卸载 Message Queue Broker 服务程序。
5. 必须先重新启动安装核心的 Windows 2000 机器，然后才能继续进行。
6. 在 `<installation-root>/isw-<machine-name>/imq/bin` 目录，使用已保存的先前发出 `imqsvcadmin query` 命令产生的输出，发出以下命令。例如：

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

其中：

- `-args` 参数用 Broker Args 字段填充。
- `-jrehome` 参数用 JREHome 字段填充。
- 要将内存增加到 1 GB，请使用 `-vmargs -Xmx1024m`。
- 仅限 64 位 Java VM：要将内存增加到 2 GB，请使用 `-vmargs -Xmx2048m`。  
32 位 Java VM 的最大内存值为 `-Xmx1750m`

7. 使用 Windows Services Management 控制台，启动 Message Queue Broker 服务程序。

**启动和停止 Message Queue Broker。 (4809493)**

在 Windows 上，Message Queue Broker 作为服务程序运行，管理员可通过服务程序控制面板来控制 Message Queue Broker 服务程序。

要启动和停止该代理程序，必须在安装核心后重新启动机器，因为如果不重新启动 Windows，服务程序管理进程便无法看到所需的 IMQ\_JAVAHOME 环境变量。仅当安装了具有核心的 Message Queue（即，未使用预先存在的 Message Queue）时，此种情况才适用。

请使用以下命令：

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

**不支持在未安装核心的机器上使用 Message Queue。 (4943576)**

Identity Synchronization for Windows “核心”组件和 Message Queue 必须安装在同一主机上。

## 常规问题

**即使同步成功开始，错误仍可存在。 (4814324)**

即使 idsync startsync 获得成功，也应查看中心错误日志，验证连接器是否能够连接到其目录源。

**对于 MMR 配置，强烈建议将配置目录和目录源放入单独的 Directory Server 实例中。 (4943470 和 4943480)**

在“多主复制” (MMR) 配置中，Sun 强烈建议将配置目录和目录源放在单独的 Directory Server 实例中，并且在安装 Identity Synchronization for Windows 前配置复制协议。

如果将同一 Directory Server 实例指定为配置目录和首选的 Directory Server（用户数据），并在安装 Identity Synchronization for Windows 后创建“复制协议”，则 Identity Synchronization for Windows 核心安装所创建的模式元素可能会被删除。如果发生此种情况，则 Identity Synchronization for Windows 将不会运行。

**解决方法**

要在意外删除该模式元素的情况下更新模式：

1. 将 40so-psw.ldif 文件（其中仅包含安装软件包的“配置注册表”的模式对象）复制到 Directory Server 实例的“模式目录”。
2. 更改 40so-psw.ldif 文件名。  
如果在启动时处理 40so-psw.ldif，则模式中的某些引用将不会被加载（结果：服务器不启动）。
3. 将重命名的文件复制到两个主服务器的“模式目录”中。（从服务器一方看，模式尚未通过协议更改，因为模式条目的更改序列号仍保持不变）。

### 应在 Directory Server 中为链接操作过程中使用的属性创建索引。(4814412)

使用 `idsync resync` (`-f <filename>` 选项) 链接用户时, 该命令在 Directory Server 中搜索与 Active Directory 或 Windows NT 用户相匹配的用户。应为 `idsync resync` 操作中使用的每一个 Directory Server 属性创建等同索引。

### 中心记录器无法关闭。(4945507 和 4933217)

尽管 Identity Synchronization for Windows 中心记录器 (记录日志到文件、syslog 或两者) 似乎允许关闭记录功能, 但它会继续记录到先前指定的位置。

例如, 如果从控制台指定记录到 syslog (文件记录功能已关闭), 然后关闭 syslog 记录功能, 则程序会继续记录到 syslog。如果从控制台指定记录到文件 (syslog 记录功能已关闭), 然后禁用文件记录功能, 则程序会继续记录到文件日志。

如果取消选中 “将日志写入文件” 且从未使用过 syslog, 则会出现相同情况。此时, 程序会继续将日志写入目录。

重新启动 Identity Synchronization for Windows 服务程序对此没有任何影响 — 记录会继续进行。

### “同步用户列表” 的 “浏览” 按钮可能无法正常使用。(4944348)

如果从 “同步用户列表” (SUL) 创建向导或编辑面板浏览查找 “基本 DN”, 则建议仔细检验通过 “浏览” 按钮得到的基本 DN。在某些情况下, 该按钮会浏览错误的目录并得到无效的基本 DN。

### 禁用 Active Directory 上的用户帐户。(4943785)

如果用户使某用户帐户无效然后在 Active Directory (AD) 上更改了密码, 则其将无法使用新密码通过 AD 验证。但是, 在禁用 AD 上的用户帐户后, 他们仍然能够通过 Sun Java System Directory Server 登录。

### 更改配置目录端口。(4941271)

如果更改了当前用作 Identity Synchronization for Windows 配置目录的 Sun Java System Directory Server, 则还必须调整 Identity Synchronization for Windows 配置, 使软件识别端口更改, 否则 “系统管理器” 和 Message Queue Broker 将不会运行。

#### 解决方法

1. 在 `<imq_installroot>\imq\var\instances\psw-broker\props\config.properties` 中修改端口。  
例如 `imq.user_repository.ldap.server=<host>\:<port>`
2. 在 `<isw_installroot>\resources\SystemManagerBootParams.cfg` 中修改端口  
例如 `<Parameter name="manager.configReg.hostPort" value="<port>" />`
3. 重新启动 Message Queue Broker 服务程序 / 守护进程。
4. 重新启动 Identity Synchronization for Windows 服务程序 / 守护进程。

### 对不同的多值属性的支持受到限制。(4987930 和 4807260)

因为结果不确定，所以对于同步不同的多值属性，Identity Synchronization for Windows 仅提供有限支持。有以下限制：

- 多值属性中的各值将作为一个单元进行同步。例如，如果将单个值添加到已具有四个值的多值属性中，则所有五个值都将作为一个单元进行同步，而且相应远程属性的值也会设置为这五个值。
- 如果链接有预先存在的用户，其属性不会自动同步。如果多值属性有所更改，则远程目录源的属性值将被本地目录源的值改写。例如，如果将电话号码添加到某条目在 Active Directory (AD) 内的先前为空的 telephoneNumber 属性中，则 Directory Server 内相应条目的 telephoneNumber 属性将被设置为此新值，改写任何现有值。
- 对多值属性的并行更新可能不会同步。在向某多值属性添加值时，如果几乎同时又将另一不同的值添加到相应远程目录条目的该多值属性中，则该属性可能不会同步。对于单值属性亦是如此。
- 修改或重命名 cn 属性时，cn 在 Directory Server 上属于多值属性类型，在 AD 上却是单值属性类型。AD 使用此属性类型（及其值）为重命名或修改的人员条目生成新 DN。由于连接器不知道在构造新 DN 时应使用多值 cn 中的哪一个值来构造新 DN，所以默认情况下它将发送第一个值。由于第一个值通常不正确，所以 AD 重命名或修改会失败。

如果在 deleteoldrdn 标志设置为 0，且 rdn 组件属性类型为 cn 时指定重命名操作 (ldap modrdns)，该项操作会在 AD 端失败。例如，如果下面条目存在，且在 Directory Server 和 AD 上都同步，

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

如果重命名 Directory Server 上的条目并将 deleteoldrdn 标志设置为 0，则 Identity Synchronization for Windows 会将 Directory Server 端的条目更改为

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

但重命名会在 AD 端失败，因为条目将被创建为：

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

从而导致类似于以下内容的错误消息（在审计日志中）：

```
[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)
```

要成功执行此操作，必须设置标志 deleteoldrdn=1。请按照以下 LDAP 示例中的修改说明操作，以成功执行重命名操作：

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

- 在使用更改类型 modify 和模式 add 修改 cn 属性时，如果添加了多个 cn 属性类型，或者如果已存在 cn 属性类型而又添加了一个新的 cn 属性类型，则 modify 操作将失败。例如，如果 Directory Server 和 AD 中都有以下 cn 条目，

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

并对该条目应用以下 LDAP 修改说明，

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

Directory Server 条目将更改为

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

但是，modify 操作在 AD 端会失败，因为 AD 端是单值的。审计日志中会出现前一例中曾注明的不同错误消息，因为连接器不能区分重命名或修改操作。

### Active Directory 将说明性属性视为单值，即使 AD 模式将其描述为多值。(4938940)

如果使用多值说明性属性将条目添加到 Directory Server，则 Active Directory (AD) 连接器 audit.log 中将出现以下 DSID-031D0809 错误：

```
[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)
```

该条目将存在于 Directory Server 而非 AD 中。

此问题似乎是 Active Directory 的缺陷。有关详细信息，请参阅 Microsoft 知识库中的以下文章 (286760)：

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



### 解决方法

将该条目从 Directory Server 中删除，将说明性属性定义为单值属性，然后重新添加该条目。

另外，请勿为“定义创建属性映射和值”对话框中的说明初始化多个属性。

### “安全套接字层”证书不可信时，插件不发出任何错误消息。(4924027 和 4924705)

在“多主复制”(MMR)配置中，如果在 Identity Synchronization for Windows 插件（子组件）使用“加密套接字层”(SSL)进行通信时，发生导致失败的 SSL 问题，而插件未提供错误消息，则在运行该插件的 Directory Server 的证书数据库中，对等服务器证书的一个 CA 证书（其中，对等服务器可为首选的主服务器、备用主服务器或 Active Directory）很可能缺失。

可使用 `idsync certinfo` 命令行实用程序来确定缺失的证书。此实用程序确定哪个数据库需要哪些证书（产品期望使用哪些证书）。

### 在 Sun Java System Directory Server 中创建的用户应包括“同步用户列表”过滤器中的所有属性。(4900568)

如果要将创建操作从 Sun Java System Directory Server 同步到 Windows，且 Directory Server “同步用户列表”(SUL)定义中含有过滤器，然后又尝试创建具有与 SUL 过滤器不符的属性值的条目，则该条目创建操作不会传播，因为 SUL 中没有这些属性。而且，由于原始创建操作未被传播，所以 Windows 端将没有该 Directory Server 条目。

### 解决方法

发生这种情况时，会记录一条警告，而管理员则必须运行 `idsync resync -c -o Sun`，以在 Windows 上创建 Directory Server 条目。

如果修改该条目使其属性与 SUL 过滤器相符，则对该条目的修改会传播到 Windows 端。

### NetBIOS 导致即时请求同步延迟。(4876741)

当 Directory Server 插件的即时请求密码同步功能正与 AD 通话时，在 Windows 2000 上使用 Directory Server 和核心组件配置同步两个 Active Directory (AD) 域的尝试会导致同步延迟。对 AD 执行的多数查询通常需要几毫秒的时间。信息包跟踪标识了一些可疑的 NBNS（NetBIOS 名称服务程序）信息包。

### 解决方法

要解决这一问题，必须访问 Directory Server 机器上的 TCP/IP 设置并通过 TCP/IP 禁用 NetBIOS。

### 消息总线使用的 Identity Synchronization for Windows 名称空间（主题）。(4827081)

- ConConfig\_100
- CntrlLog\_100
- SysMgr\_100

- PSW\_AuditLoggingTopic
- PSW\_ErrorLoggingTopic
- PSW\_LinkAuditLoggingTopic

另外，

- 对于系统中的每一个连接器，都将有 CNN1XX\_100 主题（如 CNN100\_100、CNN101\_100 和 CNN102\_100）。
- 对于系统中的每一个“同步用户列表” (SUL)，都将有基于 SUL 名称的主题。（例如，名为 *people* 的 SUL 会有一个名为 *people\_100* 的主题。）

从“全局目录”或“配置目录”对话框指定主机可能需要一些时间。**(4826109 和 4812651)**

如果指定了一个不可解析的主机，则不会显示任何指示工作进程的进度指示器（如忙指针或状态栏）。

**NT 用户名必须唯一。(4825636)**

如果要在 Directory Server 中创建要流动到 NT 的用户，则必须确保映射到 USER\_NAME 的 Directory Server 属性的各值均是唯一的。

**建议用户使用访问控制列表 (ACL) 来保护 XML 配置文件。(4812824)**

请对 XML 配置文件使用文件级保护。这些文件可能包含明文密码值，所以应使用其系统上提供的机制（如文件级 ACL）来保护它们。

**支持“同步用户列表”和数据库关系。(4811577)**

Identity Synchronization for Windows 仅支持单个 Directory Server 数据库。必须将所有“同步用户列表”放在单个 Directory Server 数据库之下。

**日志数目可无限增长。(4807451)**

除非保存或删除旧日志，否则 Identity Synchronization for Windows 中每种日志文件类型的数目都会无限增长（每天增一）。

日志以下列格式命名：

- audit\_YYYY\_MM\_DD.log
- error\_YYYY\_MM\_DD.log

将保存以下日志：

- 审计
- 错误

这些日志位于：

- 在 **Solaris** 上：/var/opt/SUNWsw/logs
- 在 **Windows** 上：<install-root>/isw-<machine-name>/logs

### 具有特殊字符的条目将不会从 **Directory Server** 同步到 **Active Directory**。(4816867)

Identity Synchronization for Windows 无法解析特殊字符（由于映射限制），Active Directory (AD) 也无法创建用户（由于 uid 中使用了一个或多个特殊字符）。

AD 控制台不允许创建以下“用户登录名”：

- 包含以下特殊字符之一："/ [ ] : | < > ; ? % \$ ^ & \* ( ) ! @ # - + = ~ `
- 超过 20 个字符
- 以句点结尾或包括逗号
- 包含范围 1-31 内的字符（不可打印的字符）

### useraccountcontrol 属性默认值使非用户 **Active Directory** 对象类无法创建。(5043156)

如果为新用户选择的对象类不允许 useraccountcontrol 属性，则无法在 Active Directory 中创建用户。如果用户对对象类或任何其它用户衍生的对象类允许在 Active Directory 中使用 useraccountcontrol 属性，则此限制不适用。

#### 解决方法

使用 Directory Server 控制台编辑配置用户。查找并删除 useraccountcontrol 属性。

例如：

```
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
```

还要编辑对 useraccountcontrol 属性的所有引用，特别是在 Active Directory 全局模式的 pswCreationAttributeDefaultRef 属性中。

例如：

```
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
```

### 不对默认值进行任何验证。(5051725)

可为属性指定默认值，并且可在创建属性时将默认值应用到目录条目（请参阅《*Sun Java System Identity Synchronization for Windows 安装和配置指南*》中的“创建属性”）。当前，不对用户指定的属性值进行任何验证。为单值属性指定多个值将导致条目同步期间的对象创建失败。在指定属性值时，请确保所指定的值与贵企业的 LDAP 模式相符。

### 如果用户出现在“同步用户列表”(SUL)中，则对修改的处理将不一致。(4970664)

如果用户因修改而进入任何“同步用户列表”(SUL)的范围内（例如，SUL 具有过滤器“l=Austin”，且用户被修改，其属性 l 被设置为 Austin），则 Sun Java System Identity Synchronization for Windows 在 Active Directory 中和 Sun Java System Directory Server 中处理此用户更新的方式不同：

- 如果用户更新发生在 Active Directory 中，则 Identity Synchronization Directory Server Connector 将创建相应用户。
- 如果用户更新发生在 Sun Java System Directory Server 中，则 Active Directory 中不会创建相应用户。运行 `resync -c -o Sun` 可帮助解决此问题。

### 从选择用于同步的对象类继承的、具有结构对象类的条目也被同步。(5046861)

例如，如果选择了 `organizationalperson` 对象类，则具有 `inetorgperson` 对象类的用户也会被同步，因为 `inetorgperson` 是 `organizationalperson` 的子类。

要防止此种情况发生，请给 SUL 加上一个排除子类的过滤器：  
(!(objectclass=inetorgperson))

使用 `resync` 来同步删除的条目时，这通常会引起问题，因为子类也会被删除。例如，对于 Active Directory，`computer` 对象类是从用户继承的，且 `computer` 条目可能会被删除，因为它们没有相应的 Directory Server 条目。要防止 `computer` 条目被同步，请给 SUL 加上一个排除它的过滤器：  
(!(objectclass=computer))

### 日志文件在到期日期之后不自动删除。(5069020)

未删除存在时间超过指定删除天数的日志文件。

### 默认的创建属性值可能配置不正确或者未通过验证逻辑。(5066657)

如果 Directory Server 和 Active Directory 数据源的某个创建属性名称相同，则向其中的一个源添加默认值时会自动向另一个源添加相同的默认值。

#### 解决方法

在控制台删除创建属性映射和创建属性，然后重新添加。保存之前，请执行以下操作：如果映射属性的名称相同，而且属性的语法 (OID)，即 Active Directory 和 Directory Server 的模式相同：

- 请确保为各属性添加不同的默认值。（都没有值也会导致此问题。）

---

**注意** 如果各默认值完全相同，则可能不会出现此问题。如果各默认值相同，则如果不先删除然后再重新添加创建属性和映射，便无法将它们分隔。

---

**useraccountcontrol 属性的默认值阻止了非用户 Active Directory 对象类的创建。(5043156)**

如果为新用户选择的对象类不允许使用 useraccountcontrol 属性，则无法在 Active Directory 中创建用户。用户对象类或任何其它用户衍生对象类允许在 Active Directory 中使用 useraccountcontrol 属性，并且不受此限制影响。

**无法用具有强制属性的扩展类映射 InetOrgperson。(5091959)**

例如，显示以下错误消息：“未为 Active Directory 属性 mail 指定任何 Sun 映射或值”，其中 mail 为强制属性且 mail 被映射到 Sun 的 mail 属性。

**《Identity Synchronization for Windows 安装和配置指南》未提及有关“下一步”按钮和“摘要”窗格的信息。(5104768)**

《Identity Synchronization for Windows 安装和配置指南》规定在每次调用后都必须使用“安装摘要”窗格上的“关闭”按钮退出向导。但是，该窗格上没有“关闭”按钮选项。在“安装摘要”窗格中，必须单击“下一步”按钮，该按钮可移动到说明其余将执行的安装和配置步骤的窗格。对于所有非“核心”安装操作，此窗格将显示“已完成”按钮，单击它时会退出向导。对于“核心”安装，此窗格将显示“下一步”按钮，单击该按钮时会转到一个提示您是否要启动控制台的窗格。可在此窗格中使用“已完成”按钮退出安装程序。

**WAN 支持限制。(5097751)**

可在一定条件限制下在“广域网”(WAN)环境中部署 Identity Synchronization for Windows。

除 Directory Server 插件外，所有 Identity Synchronization for Windows 组件都必须安装在同一 LAN 中（例如，在同一机器上），即不应有任何通过 WAN 的 Message Queue 通信。这些组件可在带有 Directory Server 或 Active Directory 域控制器的 WAN 中通信。

WAN 的性能取决于等待时间和链接速度。我们建议每个连接器和它所管理的目录间的连接速度至少为 T1 (1.544Mbps)，且等待时间不超过 300MS。在 Active Directory 和 Directory Server 被 WAN 分开的部署中，将 Directory Server 连接器与 Directory Server 安装在同一 LAN 中并使 Active Directory 连接器通过 WAN 与 Active Directory 通信可获得更好的性能。

---

## 可重新分配的文件

Sun Java System Identity Synchronization for Windows 1 2004Q3 不包含任何可以重新分配的文件。

---

## 如何报告问题和提供反馈

如果使用 Sun Java System Identity Synchronization for Windows 时遇到问题，请使用以下机制之一与 Sun 客户支持人员联系：

- 要获得 Sun 软件支持联机服务，请访问以下站点：

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

此站点包含到知识库、联机支持中心、产品跟踪器以及维护程序和联系支持人员的电话号码的链接。

- 与维护合同相关的本地服务电话号码

为使我们能够更好地帮助解决问题，请在联系支持人员时准备好以下信息：

- 问题描述，包括问题出现时的情况及其对操作的影响
- 计算机类型、操作系统版本和产品版本，包括可能影响问题的所有修补程序和其它软件
- 用于重现问题的方法的详细步骤
- 所有错误日志或内核转储

## Sun 欢迎您提出宝贵意见

Sun 非常愿意改进其文档，并欢迎您提出意见和建议。请使用基于 web 的表单向 Sun 提供反馈：

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

请在相应字段中提供完整的文档标题和文件号码。文件号码可在书的标题页或文档的顶部找到，通常为七位或九位的数字。例如，这些 Identity Synchronization for Windows 版本 1 2004Q3 发行说明的文件号码为 817-7855。

---

## 其它 Sun 资源

以下 Internet 位置提供了有用的 Sun Java System 信息:

- Sun Java System Identity Synchronization for Windows 1 2004Q3 的文档  
[http://docs.sun.com/coll/Sl\\_IdSyncForWin\\_1.0](http://docs.sun.com/coll/Sl_IdSyncForWin_1.0)
- Sun Java System 文档  
<http://docs.sun.com/prod/sunone>
- Sun Java System 专业服务  
<http://www.sun.com/service/sunps/sunone>
- Sun Java System 软件产品和服务  
<http://www.sun.com/software>
- Sun Java System 软件支持服务  
<http://www.sun.com/service/sunone/software>
- Sun Java System 支持和知识库  
<http://www.sun.com/service/support/software>
- Sun 支持和培训服务  
<http://training.sun.com>
- Sun Java System 咨询和专业服务  
<http://www.sun.com/service/sunps/sunone>
- Sun Java System 开发者信息  
<http://sunonedev.sun.com>
- Sun 开发者支持服务  
<http://www.sun.com/developers/support>
- Sun Java System 软件培训  
<http://www.sun.com/software/training>
- Sun 软件数据表  
<http://www.sun.com/software>

---

版权所有 © 2004 Sun Microsystems, Inc.。保留所有权利。

Sun Microsystems, Inc. 拥有本文档所述产品中包含技术的相关知识产权。特别是包括（但不限于）列于 <http://www.sun.com/patents> 的一项或多项美国专利以及一项或多项其它专利或正在美国和其它国家/地区申请的专利。

SUN 专有技术资产/机密。

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

请根据许可证条款使用。

此发布内容中可能含有由第三方开发的资料。

某些部分可能源自 Berkeley BSD 系统，已获得加利福尼亚大学的许可。

Sun、Sun Microsystems、Sun 徽标、Java 和 Solaris 是 Sun Microsystems, Inc. 在美国和其它国家/地区的商标或注册商标。所有 SPARC 商标的使用均已获得许可，它们是 SPARC International, Inc. 在美国和其它国家/地区的商标或注册商标。

---

版权所有 © 2004 Sun Microsystems, Inc.。 Inc. Tous droits réservés.

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

Propriété de SUN/CONFIDENTIEL.

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

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

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

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

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