



Sun Java™ System  
Identity Installation Pack 2005Q4M3 SP4  
Versionshinweise

Sun Microsystems, Inc.  
4150 Network Circle  
Santa Clara, CA 95054  
USA

Teilenummer: 820-4367-10

Copyright © 2007, 2008 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, USA Alle Rechte vorbehalten.

Rechte der US-Regierung – Kommerzielle Software. Nutzer in Regierungsbehörden unterliegen der Standard-Lizenzvereinbarung von Sun Microsystems Inc. sowie den relevanten Bestimmungen der FAR mit Zusätzen.

Die Nutzung unterliegt Lizenzvereinbarungen.

Diese Ausgabe kann von Drittanbietern entwickelte Bestandteile enthalten.

Sun, Sun Microsystems, das Sun-Logo, Java, SunTone, The Network is the Computer, We're the dot in .com und iForce sind Marken oder eingetragene Warenzeichen von Sun Microsystems, Inc., in den USA und anderen Ländern.

UNIX ist ein eingetragenes Warenzeichen in den USA und in anderen Ländern und exklusiv durch X/Open Company, Ltd. lizenziert.

Dieses Produkt unterliegt den US-amerikanischen Exportgesetzen und kann außerdem von den Export- oder Importgesetzen anderer Länder betroffen sein. Die Verwendung im Zusammenhang mit Nuklearwaffen, Raketenwaffen, chemischen und biologischen Waffen, im nuklear-maritimen Bereich oder durch in diesem Bereich tätige Endbenutzer, direkt oder indirekt, ist strengstens untersagt. Der Export oder Rückexport in Länder, die einem US-Embargo unterliegen, oder an Personen und Körperschaften, die auf der US-Exportausschlussliste stehen, einschließlich (jedoch nicht beschränkt auf) der Liste nicht zulässiger Personen und speziell ausgewiesener Staatsangehöriger, ist strengstens untersagt.

Waveset, Waveset Lighthouse und das Waveset-Logo sind Marken von Waveset Technologies, einer 100%igen Tochtergesellschaft von Sun Microsystems, Inc.

Copyright © 2000 The Apache Software Foundation. Alle Rechte vorbehalten.

Bei Weiterverteilung des Quellcodes müssen oben stehender Copyright-Hinweis, diese Liste von Bedingungen und folgender Haftungsausschluss beibehalten werden. Bei Weiterverteilung in binärer Form müssen oben stehender Copyright-Hinweis, diese Liste von Bedingungen und folgender Haftungsausschluss in der Dokumentation bzw. anderen mit der Distribution ausgelieferten Materialien reproduziert werden. Dieses Produkt umfasst Software, die von der Apache Software Foundation (<http://www.apache.org/>) entwickelt wurde.

Copyright © 2003 AppGate Network Security AB. Alle Rechte vorbehalten.

Copyright © 1995-2001 The Cryptix Foundation Limited. Alle Rechte vorbehalten.

Bei Weiterverteilung des Quellcodes müssen der Copyright-Hinweis, diese Liste von Bedingungen und folgender Haftungsausschluss beibehalten werden. Bei Weiterverteilung in binärer Form müssen oben stehender Copyright-Hinweis, diese Liste von Bedingungen und folgender Haftungsausschluss in der Dokumentation bzw. anderen mit der Distribution ausgelieferten Materialien reproduziert werden.

DIESE SOFTWARE WIRD VON CRYPTIX FOUNDATION LIMITED UND MITARBEITERN OHNE MÄNGELGEWÄHR BEREITGESTELLT UND ALLE AUSGESPROCHENEN ODER STILLSCHWEIGENDEN GARANTIEN, EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GARANTIE DER VERMARKTBARKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, WERDEN ABGELEHNT. IN KEINEM FALL SIND CRYPTIX FOUNDATION LIMITED ODER MITARBEITER FÜR IRGENDWELCHE DIREKTEN, INDIREKTEN, ZUFÄLLIGEN, SPEZIELLEN, EXEMPLARISCHEN SCHÄDEN ODER FOLGESCHÄDEN HAFTBAR (EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF, BEREITSTELLUNG VON ERSATZGÜTERN ODER -DIENSTLEISTUNGEN, NUTZUNGSAusFALL, VERLUST VON DATEN ODER PROFIT ODER GESCHÄFTSUNTERBRECHUNG), GANZ GLEICH, WIE DIESE VERURSACHT WURDEN UND WELCHER HAFTUNGSTHEORIE SIE UNTERLIEGEN, SEI DIES VERTRAG, GEFÄHRDUNGSHAFTUNG, DELIKTHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER SONSTIGES), DIE AUF IRGEND EINE WEISE DURCH DIE BENUTZUNG DIESER SOFTWARE ENTSTEHEN, SELBST WENN DIE MÖGLICHKEIT SOLCHER SCHÄDEN MITGETEILT WURDE.

Drittanbietermarken, Handelsnamen, Produktnamen sowie Logos, die in diesem Dokument enthalten sind, sind möglicherweise Marken oder eingetragene Warenzeichen ihrer jeweiligen Eigentümer.

# Inhalt

---

## **Hinweise zu Identity Installation Pack 2005Q4M3 SP4**

Installation . . . . .	7
Unterstützte Software und Umgebungen . . . . .	7
Betriebssysteme . . . . .	8
Anwendungsserver . . . . .	8
Browser . . . . .	8
Repository-Datenbankserver . . . . .	9
Sun Identity Manager Gateway . . . . .	9
Unterstützte Ressourcen . . . . .	9
Webserver . . . . .	12
Nicht mehr unterstützte Software . . . . .	12
API-Unterstützung . . . . .	13
Verworfen API . . . . .	14
Ende der Gültigkeitsdauer . . . . .	14
Ende der Gültigkeitsdauer (End of Service Life, EOSL) für den Software-Support . . . . .	14

## **Identity Installation Pack 2005Q4M3 SP4 - Funktionen**

Neue Funktionen und behobene Fehler für diese Version . . . . .	17
Administratorbenutzeroberfläche . . . . .	17
Überprüfung . . . . .	18
Passwortsynchronisation . . . . .	18
Abstimmung . . . . .	20
Berichte . . . . .	20
Ressourcen . . . . .	21
Scheduler . . . . .	22
Weitere behobene Probleme . . . . .	22
Bekannte Probleme . . . . .	22

## **Frühere Funktionen und Fehlerkorrekturen**

Frühere Funktionen . . . . .	27
Installation und Aktualisierung . . . . .	27
Administratorbenutzeroberfläche und Benutzeroberflächen . . . . .	28
Formulare . . . . .	30
Gateway . . . . .	31
HTML Display Components . . . . .	31
Identity Auditor . . . . .	31
Identity Manager SPE . . . . .	32

Lokalisierung	33
Protokollierung	34
Abstimmung	34
Berichte	34
Repository	35
Ressourcen	36
Rollen	45
Sicherheit	46
Server	48
SOAP	49
Ansichten	50
Workflow	50
In früheren Versionen behobene Fehler	51
Installation und Aktualisierung	51
Administratorbenutzeroberfläche	51
Business Process Editor	53
Formulare	53
Identity Auditor	54
Identity Manager SPE	54
Anmelden	54
Passwortsynchronisation	55
Abstimmung	55
Berichte	55
Repository	56
Ressourcen	57
Abstimmung	63
Repository	63
Rollen	63
Sicherheit	63
Server	65
SOAP	65
Workflow	65
Weitere behobene Probleme	65
<b>Hinweise zur Installation und Aktualisierung</b>	
Installationshinweise	67
Hinweise zur Aktualisierung	68
Schritt 1: Aktualisierung der Identity Manager-Software	69
Schritt 2: Aktualisierung des Sun Identity Manager Gateway	70
Manuelle Aufrüstung von Identity Manager	71

## Erweiterungen und Korrekturen der Dokumentation

Informationen zur Softwaredokumentation von Identity System . . .	75
Navigation in der Onlinedokumentation . . . . .	76
<i>Install Pack Installation</i> . . . . .	77
Korrekturen . . . . .	77
Zusätzliche Informationen . . . . .	84
Identity Manager Upgrade . . . . .	87
Zusätzliche Informationen . . . . .	87
Identity Manager Administration Guide . . . . .	88
Zusätzliche Informationen . . . . .	88
Korrekturen . . . . .	94
<i>Identity Manager Workflows, Forms, and Views</i> . . . . .	95
Kapitel 1: Workflows . . . . .	95
Kapitel 2: Workflow Services . . . . .	95
Kapitel 3: Formulare . . . . .	97
Kapitel 4: FormUtil Methods . . . . .	97
Kapitel 5: Ansichten . . . . .	98
Kapitel 6: XPRESS Language . . . . .	103
Kapitel 8: HTML Display Components . . . . .	104
<i>Identity Manager Technical Deployment Overview</i> . . . . .	109
Prozessausführung . . . . .	109
Anhang A, Konfigurationsobjekte bearbeiten . . . . .	117
Identity Manager 6.0 Resources Reference . . . . .	117
Access Manager Adapter . . . . .	118
Active Directory Adapter . . . . .	118
BridgeStream SmartRoles-Adapter . . . . .	118
ClearTrust-Adapter . . . . .	119
Datenbanktabellen-Adapter . . . . .	119
Flat File Active Sync-Adapter . . . . .	120
HP OpenVMS-Adapter . . . . .	120
JMS Listener-Adapter . . . . .	120
LDAP-Adapter . . . . .	121
Mainframe-Adapter (ACF2, Natural, RACF, Top Secret) . . . . .	124
Oracle/Oracle ERP-Adapter . . . . .	126
SAP-Adapter . . . . .	129
Skript-JDBC-Adapter . . . . .	134
Shell-Skript-Adapter . . . . .	135
Siebel CRM-Adapter . . . . .	135
Sun Java System Access Manager-Adapter . . . . .	137
Sun Java System Communications Services-Adapter . . . . .	139
Top Secret-Adapter . . . . .	139

Kapitel 3: Aktionen zu Ressourcen hinzufügen . . . . .	139
Identity Manager Tuning, Troubleshooting, and Error Messages .	140
Zusätzliche Informationen . . . . .	140
Korrekturen . . . . .	140
Identity Manager Deployment Tools . . . . .	141
Korrekturen . . . . .	141
Arbeiten mit HelpTool . . . . .	141
Index der Onlinehilfe neu erstellen . . . . .	142
Dokumentationsindex neu erstellen . . . . .	143
<b>Verworfen APIs</b>	
Verworfen Konstruktoren . . . . .	145
Verworfen Methoden und Felder . . . . .	146

# Hinweise zu Identity Installation Pack 2005Q4M3 SP4

---

Lesen Sie vor der Installation oder Aufrüstung der Sun Java™ System Identity Installation Pack-Software den Abschnitt „Hinweise zur Installation und Aktualisierung“ auf Seite 67.

## Installation

---

Verwenden Sie Identity Installation Pack 2005Q4M3 zur Installation von Sun Java™ System Identity Manager, Sun Java™ System Identity Auditor und Sun Java™ System Identity Manager Service Provider Edition (SPE) in einer neuen Umgebung oder als Aktualisierung.

Sie können Identity Manager, Identity Auditor und Identity Manager SPE von Identity Manager v5.0 oder einem der Service Packs bis zu 5.0 SP6 aktualisieren. Wenn Sie eine ältere Version von Identity Manager verwenden, müssen Sie zuerst auf Identity Manager v5.0 aufrüsten.

Detaillierte Anweisungen zur Produktinstallation finden Sie unter *Identity Manager Upgrade* und *Identity Install Pack Installation*.

**Hinweis** Die niedrigste unterstützte Java-Version ist 1.4.2.

## Unterstützte Software und Umgebungen

---

In diesem Abschnitt werden die Softwareprodukte und Umgebungen aufgelistet, die mit der Identity-Produktsoftware kompatibel sind:

- Betriebssysteme
- Anwendungsserver
- Browser
- Datenbankserver
- Java Runtime-Umgebung
- Sun Identity Manager Gateway
- Unterstützte Ressourcen
- Webserver

**Hinweis** Da die Entwickler der Softwareprodukte häufig neue Versionen, Aktualisierungen und Korrekturen herausbringen, sind die hier veröffentlichten Informationen häufig Änderungen unterworfen. Lesen Sie deshalb vor der Installation die jeweiligen Versionshinweise.

## Unterstützte Software und Umgebungen

### Betriebssysteme

- AIX 4.3.3, 5.2, 5L v5.3
- HP-UX 11i v1, 11i v2
- Microsoft Windows 2000 SP3 oder höher
- Microsoft Windows 2003
- Solaris 8, 9, 10 Sparc und x86d
- Red Hat Linux Advanced Server 2.1
- Red Hat Linux Enterprise Server 3.0, 4.0
- Novell SuSE Linux Enterprise Server 9 SP1

### Anwendungsserver

Der Anwendungsserver, den Sie mit Identity Manager verwenden, muss Servlet 2.2 unterstützen und mit der enthaltenen Java-Plattform installiert werden, sofern nicht folgendermaßen angemerkt:

- Apache Tomcat
  - Version 4,1.x (mit JDK 1.4.2)
  - Version 5.0.x (mit JDK 1.4.2)
- BEA WebLogic® Express 8.1 (mit JDK 1.4.2)
- BEA WebLogic® Server™ 8.1 (mit JDK 1.4.2)
- IBM WebSphere® 6.0
- IBM WebSphere® Application Server - Express Version 5.1.1 (mit JDK 1.4.2)
- Sun™ ONE Application Server 7
- Sun Java™ System Application Server Platform Edition 8
- Sun Java™ System Application Server Platform Edition und Enterprise Edition 8.1

**Hinweis** Wenn Ihr derzeitiger Anwendungsserver JDK 1.4.2 nicht unterstützt, erkundigen Sie sich beim Hersteller vor der Installation von Identity Installation Pack 2005Q4M3 SP4 über die Aufrüstung auf eine geeignete Version.

### Browser

- Microsoft Internet Explorer 5.x oder höher
- Safari v2.0 oder höher für Mac OS X 10.4.2 oder höher
- Mozilla 1.78 (mit JRE 1.5)
- Firefox 1.04, 1.05, 1.06 (mit JRE 1.5)

### Repository-Datenbankserver

- IBM® DB2® Universal Database für Linux, UNIX®, und Windows® (Version 7.x, 8.1, 8.2)
- Microsoft SQL Server™ 2000
- MySQL™ 4.1
- Oracle 9i® und Oracle Database 10g, 10gR1 und 10gR2®

### Sun Identity Manager Gateway

Wenn Sie Windows Active Directory, Novell NetWare, Novell GroupWise, Exchange 5.5, Remedy, Lotus Domino oder RSA ACE/Server einrichten möchten, müssen Sie vorher Sun Identity Manager Gateway installieren.

### Unterstützte Ressourcen

Diese Ressourcen werden von der Identity-Produktsoftware unterstützt.

#### CRM (Customer Relationship Management)

- Siebel 6.2, 7.0.4, 7.7, 7.8

#### Datenbanken

- IBM® DB2® Universal Database for Linux, UNIX® und Windows® (7.x, 8.1, 8.2)
- Microsoft® Identity Integration Server (MIIS) 2003
- Microsoft SQL Server 2000
- MySQL™ 4.1.x, 5.x
- Oracle® 8i, 9i, 10g Release 1, 10g Release 2
- Sybase Adaptive Server® 12.x

#### Verzeichnisse

- LDAP v3
- Microsoft® Active Directory® 2000, 2003
- Novell® eDirectory unter Novell NetWare 5.1, 6.0
- Open LDAP
- Sun™ ONE Directory Server 4.x
- Sun Java™ System Directory Server 5 2004Q2, 2005Q1

## Unterstützte Software und Umgebungen

### Hinweise

- Identity Manager wird auf Sun™ ONE Directory Server und Open LDAP getestet. LDAP-Server, die v3 unterstützen, können deshalb ohne Änderungen des Ressourcenadapters ausgeführt werden.
- Bei Sun Java™ System Directory Server 5 2005Q1 muss ein Patch für das Plug-In „retro changelog“ von Directory Server installiert werden, wenn Sie ActiveSync verwenden. Das Patch ist nur für die „regelmäßige“ Replikation erforderlich (nicht für die MMR-Replikation).

### Enterprise Resource Planning (ERP)

- Oracle Financials auf Oracle Applications 11.5.9, 11.5.10, 12
- Peoplesoft® PeopleTools 8.1 bis 8.4.2 mit HRMS 8.0 bis 8.8
- SAP® R/3 v4.5, v4.6
- SAP® R/3 Enterprise 4.7 (SAP BASIS 6.20)
- SAP® NetWeaver Enterprise Portal 2004 (SAP BASIS 6.40)
- SAP® NetWeaver Enterprise Portal 2004s (SAP BASIS 7.00)
- mySAP ERP ECC 5.0 (SAP 5.0)

### Help Desk

- Remedy® Help Desk 4.5, 5.0

### Messaging-Plattformen

- Blackberry RIM Enterprise Server 4+ (verwendet Generic Windows Script Adapter)
- Sun Java System Messaging und Calendar Service
- Lotus Notes® 5.0, 6.5, 6.5.4 (Domino)
- Microsoft® Exchange 5.5, 2000, 2003
- Novell® GroupWise 5.x, 6.0

**Hinweis** Microsoft Exchange 2000 und 2003 werden von Microsoft Windows Active Directory 2000 und 2003 verwaltet.

### Message-Queue

- JMS Message Queue Listener

### Betriebssysteme

- HP OpenVMS 7.2
- HP-UX 11.0, 11i v1, 11i v2
- IBM AIX® 4.3.3, 5.2, 5L v5.3
- IBM OS/400® V4r3, V4r5, V5r1, V5r2, V5r3, V5r4
- Microsoft Windows® NT® 4.0
- Microsoft Windows® 2000, 2003
- Generic Windows Script Adapter (verwendet Gateway)
- Red Hat Linux 8.0, 9.0
- Red Hat Linux Advanced Server 2.1
- Red Hat Linux Enterprise Server 3.0, 4.0
- Sun Solaris™ 8, 9, 10
- SuSE Enterprise 9

### Sicherheitsmanager

- ActivCard® 5.0
- eTrust CA-ACF2® Security
- Natural
- IBM RACF®
- Scripted Host
- INISafe Nexess 1.1.5
- RSA® SecurID® 5.0, 6.0
- RSA® SecurID® 5.1, 6.0 für UNIX
- eTrust CA-Top Secret® Security 5.3

### Steuerung des Webzugriffs

- IBM Tivoli® Access Manager 4.x, 5.1
- Netegrity® Siteminder® 5.5
- RSA® ClearTrust® 5.0.1
- Sun™ ONE Identity Server 6.0, 6.1, 6.2
- Sun™ Java System Identity Server 2004Q2
- Sun™ Java System Access Manager 6 2005Q1, 7 2005Q4

## Unterstützte Software und Umgebungen

### Webserver

**Hinweis** Die Integration zwischen einem Anwendungsserver und Webserver ist für Identity Manager nicht erforderlich. Die Auswahl eines Webservers bietet einen besseren Lastenausgleich und eine erhöhte Sicherheit (über das HTTPS-Protokoll).

- Apache 1.3.19
- iPlanet 4.1
- Microsoft Internet Information Server (IIS) 4.0, 5.0
- Sun™ ONE Web Server 6

### Nicht mehr unterstützte Software

Identity Manager unterstützt in Zukunft folgende, als Anwendungsserver, Datenbank-Repositorys und verwaltete Ressourcen verwendete Softwarepakete nicht mehr. Die Unterstützung wird nur bis zur nächsten Hauptversion von Identity Manager bereitgestellt. Wenden Sie sich bei Fragen zu neueren Versionen dieser Softwarepakete an Ihren Kundendienstmitarbeiter.

#### Datenbankserver

- Oracle 8i
- IBM DB2 Universal Database für Linux, UNIX und Windows 7.0

#### Betriebssysteme

- Solaris 7

#### Ressourcen

- Microsoft Exchange 5.5
- IBM DB2 7.0

### Offizieller Support für den NT4-Ressourcenadapter

Da in unseren letzten Versionen stets neue und verbesserte Funktionen implementiert wurden, wird die Unterstützung älterer Versionen in Zukunft eingestellt. Die Pläne für die Einstellung der Unterstützung beruhen darauf, dass Microsoft das Betriebssystem NT 4.0 nicht mehr unterstützt. Sun stellt die Unterstützung von Windows NT ein, die NT-Adapterfunktionalität wird jedoch weiterhin unterstützt. Kunden, die das Betriebssystem Windows NT verwenden, erhalten seit Ende 2006 keinen Support mehr.

## API-Unterstützung

Die Identity Manager v6.0-API (Schnittstelle für die Anwendungsprogrammierung, API) enthält eine beliebige öffentliche Klasse (und eine beliebige öffentliche oder geschützte Methode oder ein Feld einer öffentlichen Klasse), die in der folgenden Tabelle angegeben wird.

API-Typ	Klassennamen
Sitzung	com.waveset.msgcat.* com.waveset.util.* com.waveset.object.* com.waveset.exception.* com.waveset.expression.* com.waveset.config.* com.waveset.session.SessionUtil com.waveset.session.ScriptSession com.waveset.session.SessionFactory com.waveset.session.Session com.waveset.session.UserViewConstants
Adapter	com.waveset.adapter.* com.waveset.util.Trace
Richtlinie	com.waveset.policy.PolicyImplementation com.waveset.policy.StringQualityPolicy
Vorgang	com.waveset.task.Executor com.waveset.task.TaskContext
UI	com.waveset.ui.FormUtil com.waveset.ui.util.RequestState com.waveset.ui.util.html.*
Workflow	com.waveset.provision.WorkflowServices com.waveset.session.WorkflowServices com.waveset.workflow.WorkflowApplication com.waveset.workflow.WorkflowContext

## Ende der Gültigkeitsdauer

Identity Manager SPE enthält außerdem die in der folgenden Tabelle aufgeführten öffentlichen Klassen.

API-Typ	Klassennamen
SPE	com.sun.idm.idmx.api.IDMXContext com.sun.idm.idmx.api.IDMXContextFactory com.sun.idm.idmx.auditor.* com.sun.idm.idmx.txn.TransactionPersistentStore com.sun.idm.idmx.txn.TransactionQuery com.sun.idm.idmx.txn.TransactionSummary

Diese Klassen sind die einzigen Klassen, die offiziell unterstützt werden. Wenn Sie Klassen verwenden, die in diesen Tabellen nicht angezeigt werden, fragen Sie den Kundendienst, ob eine Migration zu einer unterstützten Klasse erforderlich ist.

## Verworfen API

“Verworfen APIs” auf Seite 145 enthält alle Identity Manager-APIs (Application Programming Interfaces), die in dieser Version verworfen wurden. Außerdem werden deren Nachfolger aufgelistet, falls verfügbar.

## Ende der Gültigkeitsdauer

---

Unsere Produkte werden immer entsprechend den höchsten Qualitätsansprüchen unserer Kunden entwickelt. Da in unserer letzten Version (Identity Manager v6) stets neue und verbesserte Funktionen implementiert wurden, wird die Unterstützung älterer Versionen in Zukunft eingestellt. Führen Sie deshalb so schnell wie möglich eine Migration durch, damit Sie keine Versionen verwenden, die von uns nicht mehr unterstützt werden.

## Ende der Gültigkeitsdauer (End of Service Life, EOSL) für den Software-Support

Vor dem Ende der Gültigkeitsdauer (End of Service Life, EOSL) wird Support in zwei Phasen angeboten, der vollständigen und der beschränkten Support-Phase. Die Zeitdauer des vollständigen Supports ist je nach Produkt verschieden. In Tabelle 1 finden Sie eine nach Produkten geordnete Liste der vollständigen und beschränkten Support-Phasen.

## **Vollständige Support-Phase**

Während der vollständigen Support-Phase stellt Sun Software-Support gemäß des zwischen dem Kunden und Sun abgeschlossenen Support-Vertrages (einschließlich geltender Service-Aufstellungen) bereit. Siehe: <http://www.sun.com/service/servicelist/>. Nach Ankündigung des Endes der Gültigkeitsdauer für ein Softwareprodukt haben Kunden keinen Zugang mehr zu Software-Aktualisierungen und -Aufrüstungen für dieses Softwareprodukt.

## **Beschränkte Support-Phase**

Während der beschränkten Support-Phase stellt Sun Software-Support gemäß des zwischen dem Kunden und Sun abgeschlossenen Support-Vertrages (einschließlich geltender Service-Aufstellungen) bereit. Siehe: <http://www.sun.com/service/servicelist/>. Kunden haben jedoch keinen Anspruch auf das Einsenden von Problembereichten und den Erhalt neuer Patches von Sun. Wie nach dem Ende der vollständigen Support-Phase auch haben Kunden Nach Ankündigung des Endes der Gültigkeitsdauer für ein Softwareprodukt keinen Zugang mehr zu Software-Aktualisierungen und -Aufrüstungen für dieses Softwareprodukt.

## **Hinweise zum Ende der Gültigkeitsdauer für Identity Manager-Produkte**

Genauere Datumsangaben werden unten aufgelistet. Wenden Sie sich bei Fragen zur Aufrüstung auf Identity Manager 6.0 (2005Q4M3) an Ihren Kundendienstmitarbeiter.

- Identity Manager 2005Q4M3 wird bis zum 25. Mai 2008 vollständig und bis zum 25. Mai 2012 beschränkt unterstützt.
- Identity Manager 2005Q3M1 mit Identity Manager 5.5 und Identity Auditor 1.5 (einschließlich aller Service Packs) wird bis zum 11. August 2007 vollständig und bis zum 11. August 2011 beschränkt unterstützt.
- Identity Manager 5.0 (einschließlich aller Service Packs) wird bis zum 11. August 2007 vollständig und bis zum 11. August 2011 beschränkt unterstützt.
- Identity Manager 2005Q3M3 wird bis Oktober 2006 unterstützt. Es sind keine weiteren Service Packs geplant.
- Identity Manager 2005Q1M3 wird bis März 2006 unterstützt. Es sind keine weiteren Service Packs geplant.
- Lighthouse 4.1 (einschließlich aller Service Packs) wird bis März 2006 unterstützt. Es sind keine weiteren Service Packs geplant.
- Lighthouse 4.0 (einschließlich SP1) wird seit September 2004 nicht mehr unterstützt.

## **Ende der Gültigkeitsdauer**

- Lighthouse 3.1 (einschließlich aller Service Packs) wird seit September 2004 nicht mehr unterstützt.
- Lighthouse 2.0 (einschließlich aller Patches) wird seit Mai 2004 nicht mehr unterstützt.
- Lighthouse 1.x (einschließlich 1.6) wird seit Mai 2004 nicht mehr unterstützt.

# Identity Installation Pack 2005Q4M3 SP4 - Funktionen

---

Lesen Sie vor der Installation oder Aufrüstung der Sun Java™ System Identity Installation Pack-Software den Abschnitt „Hinweise zur Installation und Aktualisierung“ dieser Versionshinweise und andere Dokumentationen, die für das aktuelle Identity Manager 2005Q4M3 Service Pack bereitgestellt wurden.

## Neue Funktionen und behobene Fehler für diese Version

---

Dieser Abschnitt enthält eine Zusammenfassung und Details zu neuen Funktionen für Identity Installation Pack 2005Q4M3 SP4. Detaillierte Informationen finden Sie in den jeweiligen Abschnitten dieses Kapitels.

### Administratorbenutzeroberfläche

- Nach Anzeige von **Serveraufgaben** wird die Spalte **Startzeit** auf der Registerkarte **Aufgaben verwalten** nun in der richtigen chronologischen Reihenfolge sortiert. Zuvor wurde die Spalte **Startzeit** nicht fehlerlos sortiert. (ID-16783).
- Bei der Benutzersuche auf der Registerkarte **Konten auflisten** (Konten > Konten auflisten) werden die Benutzer jetzt nur noch einmal pro Organisation aufgeführt. Zuvor konnte derselbe Benutzer in den Suchergebnissen mehrmals pro Organisation aufgeführt werden. (ID-16795).  
Ein weiteres Problem bezüglich der Kontenstrukturtable auf der Registerkarte zum Auflisten der Konten ist im Abschnitt *Bekannte Probleme* auf Seite 22 beschrieben.
- Bei einer Suche nach Benutzern in der Kontenstrukturtable gibt das Manager-Attribut des gefundenen Benutzers jetzt den vollständigen Namen des Managers an. Zuvor wurde nur die Manager-ID angezeigt. (ID-14645).
- Die Spalte **Status** auf der Seite **Benutzerpasswortergebnisse ändern** wurde entfernt. Darüber hinaus wurde die Spalte **Status** von den folgenden Seiten entfernt: **Ergebnis von Antworten ändern**, **Alle Ergebnisse ändern** und **Ergebnis von Passwort ändern**. Die Spalte **Status** enthielt keine Daten und war unnütz. (ID-16889).
- Der Feldtypwert **DatePicker** in Formularen kann jetzt gelöscht werden. (ID-17022).
- Die Tabelle **Genehmigung steht an** kann nun sortiert werden. Zuvor konnten Benutzer mit anstehenden Genehmigungen die Tabelle nicht sortieren. Stattdessen wurde die Meldung „Ergebnisseite kann nicht formatiert werden, keine Aufgaben-ID oder kein Ergebnis“ angezeigt. (ID-17304).

## Neue Funktionen und behobene Fehler für diese Version

- Die Textanzeigekomponente kann jetzt in Eingabefeldern `autocomplete="off"` darstellen, wenn die Anzeigeeigenschaft `autocomplete` auf `off` gesetzt wurde. (Durch Setzen der Eigenschaft `autocomplete` auf `off` wird verhindert, dass Webbrowser Berechtigungsdaten von Benutzern auf deren Computern speichern.)  
Sie können diese Anpassung in XPRESS durch Hinzufügen der Anzeigeeigenschaft vornehmen. Alle anderen Werte außer `off` verhindern, dass das Attribut `autocomplete` dargestellt wird. (Dies entspricht dem Verhalten beim Nichtsetzen dieser Eigenschaft.) (ID-17045).
- Für die folgenden Seiten wurde eine site-übergreifende Skriptsicherheitslücke gefunden und korrigiert (ID-17241):
  - `task/taskLaunch.jsp`
  - `user/processLaunch.jsp`
  - `user/requestLaunch.jsp`

## Überprüfung

- Überwachungsdatensätze für die Rollenerstellung enthalten jetzt im Bereich **Ändern** des Überprüfungsberichts zusätzliche Informationen zur betreffenden Rolle (z. B. zugewiesene Ressourcen, untergeordnete und übergeordnete Rollen und Rollenattribute). (ID-16327).

## Passwortsynchronisation

- Eine Änderung des Verhaltens in Microsoft Windows Server 2003 SP2 hat eine Änderung an der PasswordSync-DLL (`lhpwic.dll`) von Identity Manager erforderlich gemacht. In SP2 können von Windows an PasswordSync gesendete Benachrichtigungen über Passwortänderungen falsch formatierte Rechnerkontendaten enthalten. Dadurch kann PasswordSync einen Ausnahmefehler verursachen. Auch die LSASS-Komponente von Microsoft (Local Security Authority Subsystem) kann schließlich hängen bleiben und einen Neustart des Domänencontrollers erforderlich machen.

Da Rechnerkontendaten nicht von PasswordSync verarbeitet werden (es werden nur Benutzerkonten verarbeitet), wurde die PasswordSync-DLL dahin gehend aktualisiert, dass sämtliche Benachrichtigungen über Änderungen an Rechnerkonten bei Empfang umgehend verworfen werden.

Windows-Rechnerkonten enden mit einem Dollarzeichen (\$). Beachten Sie deshalb, dass PasswordSync keine auf \$ endenden Konten verarbeitet. Dies gilt auch für Benutzerkonten, die mit \$ enden. (ID-17245).

## Neue Funktionen und behobene Fehler für diese Version

- Das PasswordSync-Nachverfolgungsprotokoll wurde aktualisiert. Wenn PasswordSync/JMS eine Benachrichtigung über eine Passwortänderung von Windows Active Directory an Identity Manager weiterleitet und der Benutzer in Identity Manager nicht vorhanden ist, wird im Protokoll eine entsprechende Meldung aufgezeichnet. Zuvor löste PasswordSync unter diesen Umständen ohne Erklärung einen Nullzeiger-Ausnahmefehler aus. (ID-16920).
- Das Booten eines Active Directory-Domänencontrollers im Modus "Directory Service Restore" verursacht keine ständigen Hochfahrzyklen mehr, wenn PasswordSync (lhpwic.dll) abstürzt. (ID-16695).
- PasswordSync wurde dahin gehend aktualisiert, dass "out of handle"-Fehler auf Active Directory-Domänencontrollern verhindert wird, auf denen PasswordSync (lhpwic.dll) ausgeführt wird. Wenn Rechnerkonten in einer Domäne aktualisiert werden, sendet der Domänencontroller fälschlicherweise eine Benachrichtigung über eine Passwortänderung an die PasswordSync-DLL von Identity Manager. Folglich wurden Such-Handles nicht ordnungsgemäß von der DLL geschlossen. (ID-16495).

Auch: Ein weiteres Problem bezüglich PasswordSync, das Speicherlecks verursachte, wurde behoben. (ID-16827).

- Wenn die PasswordSync-DLL einen Ausnahmefehler auslöst, wird durch einen Eintrag in der Windows-Registry eine Speicherabzugsdatei generiert.

**Schlüsselname:** dumpFilebase

**Typ:** REG\_SZ

Dieser Schlüssel sollte dem Windows-Domänencontroller, auf dem PasswordSync ausgeführt wird, hinzugefügt werden. Setzen Sie den Registrierungsschlüssel auf den vollständig qualifizierten Pfad des Verzeichnisses, in dem der Speicherabzug generiert werden soll. Beispiel: c:\temp

Wenn der Registrierungswert festgelegt ist, wird bei jedem Ausnahmefehler während einer Passwortverarbeitung ein Speicherabzug geschrieben.

**Hinweis:** Unter Windows 2000 Server (jedes Service-Pack) müssen Sie auch DbgHelp.dll (erhältlich von Microsoft) im konfigurierten Verzeichnis installieren. Verwenden Sie mindestens Version 5.1 dieser Datei. Diese Datei steht unter folgender URL zum Download zur Verfügung:

<http://www.microsoft.com/whdc/DevTools/Debugging/default.msp>

Wenn DbgHelp.dll nicht installiert ist, werden unter Windows 2000 keine Speicherabzüge generiert.

## Neue Funktionen und behobene Fehler für diese Version

Die Speicherabzugsdateien werden nach folgendem Schema benannt:

```
lhpwic-JahrMonatTag-StundeMinute-xxxxx.dmp
```

Dabei ist `JahrMonatTag` das Datum des Speicherabzugs, `StundeMinute` die Uhrzeit des Speicherabzugs (im 24-Stunden-Format) und `xxxxx` die Thread-Nummer der Anwendung.

Beachten Sie, dass Speicherabzugsdateien manuell gelöscht werden müssen! Je nach der Größe des Windows-LSASS-Prozesses (Local Security Authority Subsystem) können diese Dateien zwischen 20 und über 100 MB groß sein. Wenn diese Dateien nicht gelöscht werden, kann der Speicherplatz auf Systeme mit geringer Festplattengröße mit der Zeit aufgebraucht werden. (ID-17552).

## Abstimmung

- Bei einer Abstimmung mit Suche nach Konten-ID kann ein Nullzeiger-Ausnahmefehler ausgelöst werden. Dieses Problem wurde behoben. (ID-17186).

## Berichte

- Die folgenden Ereignisse werden nun in Überprüfungsprotokollberichten wie Berichten über die tägliche Aktivität aufgenommen:
  - Versuche, Benutzer ohne Benutzer-ID oder Passwort zu erstellen
  - Versuche, Benutzer mit einer nicht existierenden Rolle zu erstellen (sowie Versuche, einem vorhandenen Benutzer eine solche Rolle zuzuweisen)
  - Versuche, Benutzer unter Verstoß gegen die Konten-ID-Richtlinie zu erstellen
  - Versuche, Benutzer zu erstellen und einer nicht zugänglichen Ressource zuzuweisen (sowie Versuche, einem vorhandenen Benutzer eine solche Ressource zuzuweisen)
  - Versuche, nicht vorhandene Benutzer zu löschen

Diese Ereignisse werden auch in das Systemprotokoll aufgenommen.

Zuvor wurden erfolglose Versuche, Benutzer zu erstellen oder zu löschen, ausschließlich in das Systemprotokoll geschrieben. (ID-13284).

- Identity Manager unterstützt jetzt bei Verwendung einer Oracle-Datenbank als Identity Manager-Repository den CLOB-Datentyp für `acctAttrChanges`.

Der Vorteil der Verwendung des CLOB-Datentyps (anstatt des Standarddatentyps `VARCHAR(4000)`) besteht darin, dass damit viel mehr Änderungen protokolliert werden können. Dadurch werden aber aufgrund der proprietären Natur der CLOB-Zugriffsroutinen Abfragen dieser Spalte verkompliziert.

Wenn mehr Änderungen protokolliert werden sollen, müssen Sie den Spaltentyp von `log.acctAttrChanges` auf CLOB (von `VARCHAR(4000)`) und das Attribut `maxLogAcctAttrChangesLength` des Konfigurationsobjekts `RepositoryConfiguration` entsprechend ändern. (ID-15326).

### Ressourcen

- Der Solaris-Ressourcenadapter erzwingt nun, dass Benutzer ihre Passwörter bei der nächsten Anmeldung ändern. Um diese Funktion zu aktivieren, fügen Sie `expirePassword` in die Spalte "Identity System-Benutzerattribut" der Schemazuordnung und `force_change` in die Spalte "Ressourcen-Benutzerattribut" ein. Dieser Attributtyp muss auf „String“ gesetzt werden. (ID-17032, ID-17146)
- Der Oracle-Ressourcenadapter wurde aktualisiert und bietet jetzt ausführlichere Fehlermeldungen für den Fall, dass ein Zuständigkeitsbereich nicht vom Adapter hinzugefügt, geändert oder gelöscht werden kann. Jetzt gibt der Adapter den Zuständigkeitsbereich an, der nicht aktualisiert werden konnte. (ID-16656).
- Der Sun Access Manager-Ressourcenadapter kann nun im SSL-Modus mit Access Manager verbunden werden. Bisher haben Administratoren beim Testen der Ressourcenadapter-Konfiguration den Fehler „AuthContext cannot be created“ erhalten. (ID-16454).
- Das Microsoft ADSI-Gateway wurde aktualisiert. Wenn zur Authentifizierung einer Benutzeranmeldung bei Identity Manager eine Active Directory-Ressource genutzt wird, wird der Benutzer nun in der Benutzeroberfläche von Identity Manager dazu aufgefordert, sein Passwort zu ändern, sofern sein Windows-Passwort abgelaufen ist. Bisher wurde der Benutzer lediglich in einer Fehlermeldung darauf aufmerksam gemacht, dass sein Passwort abgelaufen ist. (ID-16681).
- Die Unterstützung für den Zugriff auf Remedy-Server wurde geändert. Das Gateway ist nicht mehr von Version 4.5 der Remedy API-Bibliotheken abhängig. Die Kunden müssen jetzt Remedy-Bibliotheken in das Gateway-Verzeichnis kopieren. Sie finden diese Bibliotheken auf dem Remedy-Server. (ID-17361, ID-16551)
- Mit diesem Service-Pack bietet Identity Manager Unterstützung für Remedy Version 6.3 und 7.0. Diese Versionen unterscheiden sich jedoch erheblich im Hinblick auf Beispieldaten, Standardwerte und die Konfiguration neuer Systeme. So ist beispielsweise der Name des „Ticket“-Schemas in Version 6.3 HPD:HelpDesk. In Version 7.0 wurde er in HPD:Help Desk geändert. (ID-17361, ID-14611)
- Bei der Konfiguration von Active Directory-Ressourcen können Sie jetzt in den Eigenschaften für die Ressourcenauthentifizierung eine Domäne angeben. In Umgebungen mit mehreren Domänen oder zahlreichen Hierarchien sollten Administratoren eine Domäne angeben, damit Anmeldungen in der richtigen Active Directory-Domäne authentifiziert werden. Wenn keine Domäne angegeben ist, kann ein Benutzer schon nach einem einzigen fehlgeschlagenen Anmeldeversuch gesperrt werden. Dies ist darauf zurückzuführen, dass der Benutzer pro Domäne, die eine Vertrauensbeziehung zur Primärdomäne unterhält, einen Passwortfehler sammeln kann. (ID-16603).
- Ein Problem mit dem SecurId Unix-Ressourcenadapter wurde behoben. Vor der Problembehebung wurden durch eine Änderung des Vor- oder Nachnamens eines Benutzers dessen Benutzergruppen aus der SecurId-Ressource gelöscht. (ID-16914).

## Bekannte Probleme

### Scheduler

- Der Scheduler wurde dahin gehend aktualisiert, dass die Ausgabe des Systemprotokolleintrags (syslog) 'EVNT00', `LockedByAnother` unterdrückt wird. In Cluster-Umgebungen wurde diese Meldung extrem häufig an das Protokoll ausgegeben. (ID-15714).
- Der Scheduler wurde dahin gehend aktualisiert, dass die Wahrscheinlichkeit, dass zwei Instanzen von Identity Manager denselben Workflow gleichzeitig abarbeiten, herabgesetzt wird. Vor dieser Aktualisierung waren Cluster-Umgebungen mit mehreren auf dasselbe Repository zugreifenden Schemulern für dieses Problem anfällig. (ID-16500).

### Weitere behobene Probleme

16382

## Bekannte Probleme

---

- In der Kontenstrukturtable auf der Registerkarte **Konten auflisten** (Konten > Konten auflisten) wird die Spalte **Manager** nicht angezeigt. (Nur die Spalten **Name**, **Nachname** und **Vorname** werden angezeigt.)

Um dieses Problem zu beheben, bearbeiten Sie das Konfigurationsobjekt `UserUIConfig` mithilfe des Business Process-Editors.

Suchen Sie das Element `<AppletColumns>` und fügen Sie folgendes XML-Couplet ans Listenende an:

```
<Object name="idmManager">
  <Attribute name="label" value="UI_ATTR_MANAGER"/>
</Object>
```

Speichern Sie die Änderungen, und starten Sie den Anwendungsserver neu. (ID-17710).

- Die einzige Möglichkeit, in der Administratoroberfläche eine erfolgte Delegation rückgängig zu machen (**Genehmigungen > Eigene Genehmigungen delegieren**), besteht in der Einstellung desselben Werts für das End- und das Startdatum (oder durch Einstellen auf ein Datum in der Vergangenheit). (ID-16790, ID-16799)

- TaskScheduleViewer formatiert das Startdatum nicht in der Weise, die für einen Eintrag erforderlich ist. Folglich müssen Sie bei Bearbeitung eines Aufgabenplans das Startdatum korrigieren. (ID-5675).

- Wenn ein Benutzer eine Antwort auf eine Authentifizierungsfrage eingibt, werden die eingegebenen Zeichen standardmäßig mit Sternchen (\*) maskiert. Dies verhindert in einigen Eingabemethodeneditoren (IMEs) jedoch die Eingabe komplexer Zeichen wie beispielsweise japanischer Kanji-Zeichen.

Damit Benutzer Antworten auf Authentifizierungsfragen unter Verwendung eines Eingabemethodeneditors eingeben können, müssen Sie über die Debugging-Seite im Benutzerformular für die Anmeldefrage den Wert der Eigenschaft `secret` auf `false` setzen.

```
<Property name="secret" value="false"/>
```

**Hinweis:** Da die Antworten auf Authentifizierungsfragen nun als Klartext auf dem Bildschirm mitlesbar sind, stellt diese Einstellungsänderung ein Sicherheitsrisiko dar. Die Antworten werden jedoch weiterhin verschlüsselt gespeichert. (ID-7424).

- Einige Konfigurationsoptionen in der Identity Manager-Administratorbenutzeroberfläche werden in Identity Manager SPE nicht verwendet (ID-10843). Hierzu gehören:
  - Konfigurationsoptionen für den Ressourcenassistenten: Ausschließen von Kontoregeln, Genehmigern und Organisationen
  - Rollenattribute
- FireFox 1.5 zeigt einige Identity Manager-Formulare nicht ordnungsgemäß an. So führt der Browser beispielsweise im Formular zum Bearbeiten von Benutzern, das Registerkarten enthält, an Beschriftungen keine Zeilenumbrüche durch. Dadurch wird alles nach rechts verschoben (ID-13109).
- Das Kontrollkästchen „Nur Benutzer melden, deren Benutzername“ ist in Benutzer- und Benutzerfragenberichten zweimal aufgeführt. Ein Kontrollkästchen besitzt IHelp-Funktionalität, das andere Kontrollkästchen jedoch nicht. Bei einzelner Verwendung geben beide Kontrollkästchen jedoch die richtigen Daten zurück. (ID-13155).
- Bei der Protokollierung in SPE erzeugen Endbenutzerseiten der HTTP-Fehlerstatus 500. Das kann darauf hinweisen, dass in der SPE-Konfiguration mehrere Chiffrierschlüssel vorhanden sind. Dieses Problem kann von einem während der Aktualisierung von Identity Manager neu generiertem Chiffrierschlüssel verursacht worden sein.

Zwischenlösung: Verwenden Sie die Chiffrierschlüssel (EncryptionKeys) aus dem SPE-Konfigurationsverzeichnis und exportieren Sie neu aus Identity Manager. (ID-13162).
- Wenn ein Wert für ein E-Mail-Benutzerattribut einmal gesetzt wurde, kann er nicht mehr gelöscht werden. Er kann zwar geändert, aber nicht mehr auf null zurückgesetzt werden. (ID-13164).

## Bekannte Probleme

- Wenn Sie zum Ändern der Variable `showSuperAndSubRoles` von 0 auf 1 ein Rollenformular ändern und dann eine Objektdefinitionsdatei einer übergeordneten Rolle importieren, die untergeordnete Rollen von der Registerkarte **Konfigurieren** enthält, werden diese untergeordneten Rollen nicht dahingehend geändert, dass sie den Abschnitt `<SuperRoles>` enthalten. Wenn Sie jedoch eine übergeordnete Rolle auf der grafischen Benutzeroberfläche von Identity Manager erstellen, werden die von dieser übergeordneten Rolle referenzierten untergeordneten Rollen aktualisiert. (ID-15053).

Dieses Problem kann bei Rollen auftreten, die außerhalb von Identity Manager erstellt wurden und Referenzen zu vorhandenen Rollen (entweder untergeordnete oder übergeordnete Rollen) enthalten, die sich bereits auf dem System befinden.

Beim Importieren dieser Rollen werden die Rollen, die sich bereits auf dem System befinden, nicht bezüglich der neuen Beziehungen aktualisiert; die Referenzintegrität ist somit nicht gewährleistet. Wenn Sie Rollen auf diese Weise importieren, prüfen und ggf. korrigieren Sie die Referenzintegrität mittels `RoleUpdater`.

**Zwischenlösung:** Siehe die Erläuterungen zu ID-15482 unter „Rollen“.

- Die Sperreigenschaften von Microsoft SQL Server 2000 können bei hoher Auslastung von Identity Manager Deadlock-Fehler verursachen. (ID-16068).

**Zwischenlösung:** Rüsten Sie im systemeigenen Modus von Microsoft SQL Server 2000 auf Microsoft SQL Server 2005 auf.

Microsoft SQL Server 2005 (mit der neuen Funktion *Snapshot Isolation*) wurde mit Identity Manager unter hoher Auslastung getestet und zeigt nicht die gleichen Deadlock-Probleme wie SQL Server 2000.

Einige Benutzer haben mit der folgenden Änderung von `READ_COMMITTED_SNAPSHOT` in der Datenbank positive Erfahrungen gemacht:

```
ALTER DATABASE dbname SET READ_COMMITTED_SNAPSHOT ON  
</quote>
```

- Wegen Interoperabilitätsproblemen zwischen WebSphere-Datenquellen und Oracle JDBC-Treibern müssen Oracle-Kunden, die WebSphere-Datenquellen mit Identity Manager verwenden wollen, Oracle 10g R2 und den entsprechenden JDBC-Treiber verwenden. (Der Oracle9 JDBC-Treiber funktioniert nicht mit WebSphere-Datenquellen und Identity Manager.) Wenn Sie eine Oracle-Version vor 10g R2 haben und nicht auf Oracle 10g R2 aktualisieren können, müssen Sie das Identity Manager-Repository so konfigurieren, dass Verbindungen zur Oracle-Datenbank mithilfe des JDBC-Treibermanagers von Oracle (und nicht mit WebSphere-Datenquellen) hergestellt werden. (ID-16167).

Weitere Informationen finden Sie unter der folgenden URL:

<http://www-1.ibm.com/support/docview.wss?uid=swg21225859>

- Einige Worte im Bildschirm „Benutzer bearbeiten“ können im Mehrsprachenmodus umgebrochen dargestellt werden. (ID-16054).

**Zwischenlösung:** Um zu gewährleisten, dass Wörter in Tabellen ohne Umbruch angezeigt werden, müssen Sie Folgendes zur Datei `$WSHOME/styles/customStyle.css` hinzufügen:

```
table.Tab2TblNew td {
background-image:url(../images/tabs/level2_deselect.jpg);
background-repeat:repeat-x;background-position:left top;
background-color:#C4CBD1;
border:solid 1px #8f989f;
white-space:nowrap;
}

table.Tab2TblNew td.Tab2TblSelTd {
border-bottom:none;
background-image:url(../images/tabs/level3_selected.jpg);
background-repeat:repeat-x;background-position:left bottom;
background-color:#F2F4F3;
border-left:solid 1px #8f989f;
border-right:solid 1px #8f989f;
border-top:solid 1px #8f989f;
white-space:nowrap;
}
```

## **Bekannte Probleme**

# Frühere Funktionen und Fehlerkorrekturen

---

## Frühere Funktionen

---

In diesem Abschnitt werden Funktionen beschrieben, die mit früheren Service-Packs für Identity Installation Pack 2005Q4M3 eingeführt wurden.

### Installation und Aktualisierung

- Wenn Sie SQL Server 2000 SP4 als Repository mit dem JDBC-Treiber von Microsoft verwenden, müssen Sie mit dem SQL Server 2000-Treiber für den for JDBC SP3-Treiber arbeiten. (ID-9917).
- Das Systemattribut `waveset.serverId` wurde hinzugefügt. Mit diesem Attribut können Sie eindeutige Servernamen setzen, wenn Ihr Deployment mehrere Identity Manager-Instanzen enthält, die auf ein Repository auf einem einzigen physischen Server zeigen. (ID-11578).
- Identity Manager unterstützt jetzt als Repository Oracle Database 10g Release2®. (ID-12908).
- Das Installationsprogramm unterstützt jetzt die Aufrüstung von Installationen, die das Konfigurator-Standardkonto umbenannt, gelöscht oder deaktiviert haben. Das Installationsprogramm fordert Sie zur Eingabe des korrekten Benutzernamens und des Passworts auf, mit deren Hilfe die Datei `update.xml` während der Nachverarbeitung des Aufrüstungsvorgangs importiert werden kann. Wenn der Benutzername oder das Passwort falsch eingegeben wurden, haben der Benutzer maximal drei Versuche, das richtige Passwort einzugeben. Der Fehler wird im Textfeld dahinter angezeigt. (ID-13006).

Bei der manuellen Installation müssen Sie die Flags `-U <Benutzername> -P <Passwort>` angeben, damit die Berechtigungsnachweise an die Prozedur `UpgradePostProcess` übergeben werden können.

- Identity Manager wird auf Rechnern ohne Grafikkarte ordnungsgemäß installiert. (ID-14258).

# Administratorbenutzeroberfläche und Benutzeroberflächen

- Die Fenster **Konfigurieren > Server > Servereinstellungen bearbeiten/Standardservereinstellungen bearbeiten** enthalten jetzt die Registerkarte „E-Mail-Vorlagen“. Diese Registerkarte enthält die standardmäßige bzw. serverweise einzustellende SMTP-Hostvariable, die alle E-Mail-Vorlagen mit der Variable  $\$(smtpHost)$  standardmäßig verwenden. Diese Registerkarte verwendet darüber hinaus die Serverkonfigurationsvariable, wenn das Feld „SMTP-Host“ leer ist. (ID-3574).
- Wenn Sie im Bildschirm „Benutzer suchen“ auf „Abfrage zurücksetzen“ klicken, werden die Namensliste und die Ergebnisbeschränkung jetzt auf den Anfangszustand zurückgesetzt. (ID-8961)
- Die Seiten „Benutzerpasswort ändern“ und „Benutzerpasswort zurücksetzen“ in der Administratorbenutzeroberfläche von Identity Manager enthalten jetzt Menüoptionen für Suchtypen. Dazu gehören **beginnt mit**, **enthält**, und **ist** als Operatoren, um nach Benutzern zu suchen, deren Passworte geändert oder zurückgesetzt werden müssen. (ID-8965).
- Die Debug-Seite bietet jetzt die Optionen **export default** und **export all**. Diese Optionen funktionieren ähnlich wie die Konsolenoptionen. Der einzige Unterschied besteht darin, dass bei den Optionen auf der Debug-Seite der Name der exportierten Datei nicht ausgewählt werden kann. Stattdessen erstellt Identity Manager eine Datei namens `export<date>.xml`, die Sie von der Debug-Seite aus speichern können. (ID-9270).
- Es wird jetzt der Import von E-Mail-Vorlagen mit „Kopie an“-Feldern unterstützt. (ID-9768).
- Auf der Seite „Identity-Attribute“ gibt es jetzt einen Passwortbereich, in dem der Status der Passwörterstellung in Bezug auf Identity-Attribute beschrieben wird. Sie können Identity Manager so konfigurieren, dass Passwörter neuen Benutzern aufgrund eines Standardwertes (z.B. einer Regel) oder einer Identity System-Kontorichtlinie, die Passwörter erzeugt, zugewiesen werden. (ID-10274, 12560).
- Es wurden Fehlermeldungen im Zusammenhang mit dem Bearbeiten von Richtlinien überarbeitet. (ID-12187).
- Identity Manager enthält jetzt das Standardattribut „Manager“, das eine Manager-Mitarbeiter-Beziehung unterstützt. Diese Information wird im Identity Manager-Benutzerobjekt gespeichert. Weitere Informationen finden Sie im Abschnitt *Erweiterungen und Korrekturen der Dokumentation* dieser Versionshinweise. (ID-12416).
- Identity-Attribute können jetzt aufgrund vorheriger Änderungen an Ressourcen (Berarbeitungs- oder Erstellungsoperationen) konfiguriert werden. (ID-12678) Wenn sich Ressourcen seit der letzten Speicherung von Identity-Attributen in der Administratorbenutzeroberfläche von Identity Manager geändert haben, wird auf

der Seite „Identity-Attribute“ die folgende Meldung angezeigt: „Seit dem letzten Speichern der Identity-Attribute wurde mindestens eine Ressource geändert. Wenn diese Änderungen die Identity-Attribute betreffen, sollten sie auf der Seite „Identity-Attribute aus Ressourcenänderungen konfigurieren“ aufgenommen werden. Identity Manager enthält einen Verweis auf die Seite „Identity-Attribute konfigurieren“ (auf der Seite „Ressourcen ändern“), mit dessen Hilfe Sie Attribute aus den Schemazuordnungen geänderter Ressourcen auswählen können, um sie als Quelle bzw. Ziel für Identity-Attribute zu verwenden.

Nach dem Speichern einer Ressource im Ressourcenassistent oder auf der Seite „Kontoattribute“ zeigt Identity Manager eine Seite an, in der Sie gefragt werden, ob Sie Identity-Attribute aufgrund kürzlich vorgenommener Ressourcenänderungen konfigurieren möchten. Klicken Sie auf **Ja**, um zur Seite „Identity-Attribute aus Ressourcenänderungen konfigurieren“ zu gehen. Klicken Sie auf **Nein**, um zur Ressourcenliste zurückzukehren.

Klicken Sie auf **Diese Frage nicht mehr wiederholen**, um diese Seite zu deaktivieren. Dadurch wird diese Seite durch Setzen der Eigenschaft `idm_showMetaViewFromResourceChangesPage` des angemeldeten Benutzers deaktiviert.

- MultiSelect-Objekte sortieren jetzt die verfügbaren Werte, wenn die Eigenschaften `noApplet=true` und `sorted=true` gesetzt sind. (ID-12823).
- Änderungen an Konfigurationsobjekten, die eine statische Liste enthalten, wurden von der Kontostrukturtable nicht erkannt. So wurden beispielsweise die von einem Administrator kontrollierten Organisationen von einer Regel ermittelt, die eine statische Liste von einem Konfigurationsobjekt abrief. Zuvor musste der Server neu gestartet werden, damit Änderungen am Konfigurationsobjekt erkannt werden konnten. Jetzt enthält die Strukturtable Änderungen an Konfigurationsobjekten, wenn sich Benutzer aus der aktuellen Sitzung ab- und dann wieder anmelden. (ID-14442).
- Der DatePicker kann jetzt einen Datumszeitraum besitzen, mit dessen Hilfe nur bestimmte Datumsangaben aus dem Kalender ausgewählt werden können. (ID-10100)
- Die Vorlagen „Serverkonfiguration“ und „E-Mail ändern“ wurden geändert, damit Administratoren entscheiden können, ob auf dem SMTP-Server SSL oder Authentifizierung durchgeführt werden sollte. (ID-12465).
- Die Seite `continueLogin.jsp` zeigt Meldungen jetzt ordnungsgemäß an. (ID-13193).
- Die folgenden Änderungen wurden an Identity Manager 7.1 Identity Manager Integrated Development Environment vorgenommen, sodass nun Unterstützung für Identity Manager Version 2005Q4M3 SP3 besteht: (ID-14089, 15211).

## Frühere Funktionen

- Der Identity Manager-Debugger ist jetzt standardmäßig aktiviert.  
Bei Bereitstellung für die Produktion sollten Sie die Systemkonfigurationseigenschaft auf `serverSettings.default.debugger.enabled=false` setzen.
- Der Identity Manager-Debugger unterstützt jetzt das Setzen von Haltepunkten in Regelbibliotheken.
- Für die Passwortsynchronisation im Direktmodus muss `SimpleRpcHandler` in der Datei `web.xml` konfiguriert sein. `SimpleRpcHandler` stört bestimmte `RemoteSession`-Aufrufe. Wenn Sie die Passwortsynchronisation nicht im Direktmodus verwenden und Probleme mit `RemoteSession`-Aufrufen feststellen, können Sie die `SimpleRpcHandler`-Konfiguration aus dem `rpcrouter2`-Servlet entfernen. Dadurch beheben Sie die Probleme mit `RemoteSession`.

Ändern Sie diese Einträge in `web.xml`:

```
<init-param>
<param-name>handlers</param-name>
<param-
value>com.waveset.rpc.SimpleRpcHandler,com.waveset.rpc.Passwor
dSyncHandler</param-value>
</init-param>
```

in Folgendes ab:

```
<init-param>
<param-name>handlers</param-name>
<param-value>com.waveset.rpc.PasswordSyncHandler</param-value>
</init-param>
```

Wenn Sie `RemoteSession` und die Passwortsynchronisation im Direktmodus verwenden möchten, konfigurieren Sie ein separates Servlet für die Behandlung von `RemoteSession`-Aufrufen.

- Es wurde ein Problem behoben, bei dem ein Organisationsobjekt nicht freigegeben wurde, wenn ein Benutzer mit unzureichenden Zugriffsrechten versuchte, dieses zu löschen. (ID-14942).

## Formulare

- In Formularen funktioniert die Methode `<set>` innerhalb von `<Expansion>` jetzt ordnungsgemäß. (ID-9617).
- Meldungen zu Verifizierungsregeln werden jetzt im Gebietschema des Clients und nicht dem des Servers angezeigt. (ID-12780).

## Gateway

- Das Gateway läuft jetzt sowohl mit vmware-Abbildern unter Windows 2000 SP4 und Windows 2003 SP1. (ID-12826).

## HTML Display Components

- Die Anzeigeklasse „DatePicker“ besitzt die neue Eigenschaft `strict`. Wenn diese Eigenschaft gesetzt ist, werden manuell eingegebene Daten überprüft. (ID-11037).
- Sie können die erzwungene Erstellung des Endbenutzermenüs jetzt deaktivieren, indem Sie die Eigenschaft `doNotRegenerateEndUserMenu` im Formular „Endbenutzermenü“ setzen. (ID-11327).
- Die Komponente `SortingTable` unterstützt jetzt die Eigenschaften `align`, `valign` und `width` der untergeordneten Komponenten, die bei der HTML-Ausgabe die jeweilige Tabelle enthalten. Zur Anzeige von Fehlermeldungen, Warnhinweisen und Informationsmeldungen in Formularen steht darüber hinaus die `InlineAlert`-Komponente zur Verfügung. (ID-12560).
- Die Strukturtabellenkomponente unterstützt jetzt veränderliche Tabellenspaltenbreiten. Mit CSS können Sie die Spaltenbreiten der Benutzerliste und der Ressourcenlistentabellen auf einen absoluten Pixelwert oder einen Prozentsatz einstellen. Sie können darüber hinaus Tabellenspaltenbreiten mit der Maus durch Klicken und Ziehen der Begrenzung der entsprechenden Spaltenüberschrift ändern. (ID-11474).

**Hinweis** In Firefox/Mozilla und anderen Gecko-basierten Browsern kann die Größenänderung von Spalten dazu führen, dass Text markiert wird. Dieses Problem tritt nicht mit Internet Explorer oder Safari auf, da das DHTML-Verhalten beim Ereignis „onselectstart“ unterdrückt werden kann.

## Identity Auditor

- Überprüfungsrichtlinien können jetzt so konfiguriert werden, dass nur eine beschränkte Anzahl an Ressourcen abgefragt wird. (ID-9127).
- Die Ressourcen „Datenbanktabelle“ und „Microsoft Identity Information Server“ nutzen jetzt die für diese beiden Ressourcen angegebenen benutzerspezifischen Formulare. (ID-10302)
- Der Titel von Benutzerzugriffsberichten wird jetzt ordnungsgemäß angezeigt. (ID-11538).
- Die Aufgabe „Zugriffsabfrage“ funktioniert jetzt mit dynamischen Organisationen. (ID-12437).

## Frühere Funktionen

- Die Benutzeransichtsoption „CallViewValidators (UserViewConstants.OP\_CALL\_VIEW\_VALIDATORS)“ kann auf die Strings „true“ oder „false“ gesetzt werden, um während der Bereitstellung das Prüfen von Überprüfungsrichtlinien zu aktivieren/deaktivieren. (ID-12757).
- Bei einer Aufrüstung wird die E-Mail-Vorlage „Zugriffsprüfungshinweis“ nicht mehr überschrieben (ID-13216)

## Identity Manager SPE

Mit Identity Manager SPE 2005Q4M3 SP1 wurden die folgenden neuen Funktionen eingeführt. Ausführliche Informationen zu diesen Funktionen finden Sie in den Dokumenten *Identity Manager Service Provider Edition Administration Addendum* und *Identity Manager SPE Deployment*.

### Erweiterte Endbenutzerseiten

Es stehen jetzt erweiterte Endbenutzerseiten zur Verfügung. Die Beispielseiten enthalten die folgenden Funktionen:

- An- und Abmeldung mit Authentifizierung mittels geheimer Fragen
- Registrierung und Einschreibung
- Ändern von Benutzernamen und Passwörtern
- Geheime Authentifizierungsfragen und Bearbeiten von Benachrichtigungsadressen
- Behandlung vergessener Benutzernamen und Passwörter
- Benachrichtigung per E-Mail
- Überprüfung

Diese Seiten können für Ihr spezielles Deployment angepasst werden. Sie können Folgendes anpassen:

- Erscheinungsbild
- Konfigurationsoptionen (z.B. die Anzahl fehlgeschlagener Anmeldeversuche)
- Hinzufügen und Entfernen von Seiten

### Richtlinien zu Passwörtern und Konto-IDs

Für Identity Manager SPERessourcenkonten existieren jetzt Richtlinien zu Konto-ID und Passwörtern. Diese Richtlinien werden mit der gleichen Richtlinieninfrastruktur wie bei Identity Manager implementiert. (ID-12556).

## **Gleichzeitiges Ausführen von Active Sync and Identity Manager SPE Sync**

Active Sync- und SPE-Synchronisierungen sind jetzt auf dem gleichen Identity Manager-Server ausführbar, dürfen jedoch nicht auf der gleichen Ressource ausgeführt werden. (ID-12178).

## **Getrennte Benutzer- und Konfigurationsverzeichnisse für LDAP**

Benutzer- und Konfigurationsinformation können jetzt in jeweils eigenen LDAP-Instanzen gespeichert werden. Diese Instanzen werden während der Anfangskonfiguration ausgewählt. (ID-12548).

## **Integration mit Access Manager**

Sie können zur Authentifizierung auf Endbenutzerseiten von Identity Manager SPE jetzt Sun Java System Access Manager 7 2005Q4 verwenden. Access Manager stellt sicher, dass nur authentifizierte Benutzer Zugriff auf die Endbenutzerseiten haben.

## **Sonstige Korrekturen**

- Identity Manager SPE setzt jetzt die Transaktionsverarbeitung fort, wenn ein Dienst abnormal beendet wird, z.B. wenn der Anwendungsserver mit einem „Out-of-memory“-Fehler (nicht genügend Speicher) abbricht. (ID-14579).
- Identity Manager SPE-Transaktionen unterstützen jetzt konfigurierbare Konsistenzebenen zur Benutzeraktualisierung. Vorhandene Transaktionsdatenbanken müssen um eine zusätzliche Spalte (`userId VARCHAR (N)`) erweitert werden, wobei `N` groß genug sein muss, um die erwartete Maximallänge eines Identity Manager SPE Benutzer-DNs plus zusätzlich 8 Zeichen enthalten zu können. Diese Datenbankänderung wird beim Ausführen der Aufrüstungskripten nicht automatisch vorgenommen. (ID-13830).

## **Lokalisierung**

- Als Authentifizierungsfragen verwendete Meldungsschlüssel werden auf der Ergebnisseite jetzt ordnungsgemäß angezeigt. (ID-13076).

### Protokollierung

- Active Sync-Ereignisse werden jetzt im Systemprotokoll aufgezeichnet. (ID-12446).
- Das Ändern der Authentifizierungsfragen von Benutzern wird jetzt in den Überwachungsprotokollen aufgezeichnet. (ID-13082).
- Direkte und indirekte Methodenaufrufe können jetzt verfolgt werden. (ID-13436)  
Das ist dann nützlich, wenn Fehler gesucht werden, die auf einer Ebene unter einer bestimmten Eintrittsmethode auftreten. Zum Aktivieren dieser Funktion müssen Sie die Verfolgungsebene für einen Gültigkeitsbereich mithilfe des `subcalls`-Bezeichners setzen (siehe folgendes Beispiel):

```
trace 4,subcalls=2  
com.waveset.recon.ReconTask$WorkerThread#reconcileAccount
```

Dies verfolgt die Methode `reconcileAccount()` auf Ebene 4 und alle Unteraufrufe auf Ebene 2.

- Im Planer auftretende Fehler werden jetzt im Systemprotokoll aufgezeichnet und nicht mehr im `TaskSchedule`-Objekt gespeichert. (ID-14261).

### Abstimmung

- Die Aufgabendefinition „Benachrichtigung über das Abstimmungsende“ wird erfolgreich ausgeführt, wenn sie als „Nachabstimmungs-Workflow“ angegeben wird (ID-9259)
- Wenn eine große Anzahl an `Account`-Objekten existiert (diese werden im Ergebnis von Abstimmungen und Bereitstellungen erstellt), kann die Leistung bei Abstimmungen und Bereitstellungen drastisch abnehmen.  
Um dies zu beheben, sollte für die Spalte „name“ der Tabelle „account“ im Repository ein Index erstellt werden. Einige Skripts, die dazu dienen, befinden sich im Beispielverzeichnis. `account_index.sqlserver` ist für Microsoft SQL Server, `account_index.sql` für alle anderen Datenbanken bestimmt. (ID-14478).

### Berichte

- Identity Manager erstellt jetzt beim Erstellen und Ändern von Fähigkeiten Überprüfungsereignisse. (ID-9734).
- Identity Manager bietet jetzt im Feld **Wählen Sie die Identity Manager - Attribute aus, die für die Benutzer angezeigt werden sollen** eine neue Rollenoption. Durch Auswahl dieser Option für neue bzw. vorhandene Berichte wird im betreffenden Bericht eine kommaseparierte Liste mit Rollen angezeigt. (ID-9777).

- Sie können jetzt eine Liste mit Attributen angeben, die in CSV- und PDF-Berichten in einer eigenen Spalte angezeigt werden soll. Wenn Sie keine Liste angeben, werden alle Attribute in einer einzelnen Spalte namens „Überwachbare Attribute“ angezeigt. (ID-10468).
- Der Gültigkeitsbereich der folgenden Berichtstypen wird standardmäßig auf die vom angemeldeten Administrator kontrollierten Organisationen abgestimmt, es sei denn, es wurden explizit eine oder mehrere Organisationen ausgewählt, für die der betreffende Bericht gelten soll: (ID-12116).
  - Admin-Rolle - Zusammenfassung
  - Administrator-Zusammenfassung
  - Rollenzusammenfassung
  - Zusammenfassender Bericht zu Benutzerfragen
  - Benutzerzusammenfassung

Zur Unterstützung dieser Funktion wurde die Komponente „Organisationsumfang“ von einer `Select`- in eine `MultiSelect`-Komponente umgewandelt.

- Zwei neue Berichte unterstützen die integrierten Manager-Mitarbeiter-Beziehungen: „Eigene direkte Berichte - Zusammenfassung“, „My Direct Employee Summary“, „My Direct and Indirect Employee Summary“ und „My Direct Reports Individual“. (ID-12416, ID-12689)
- Der Ressourcenbenutzerbericht erzeugt CSV- und PDF-Dateien jetzt ordnungsgemäß. (ID12509, 13701)
- Bei der Erstellung, Änderung und Löschung von Admin-Rollen wird nun Überwachungsprotokollierung unterstützt. (ID-12514).
- Benutzerberichte enthalten jetzt ein Suchattribut, damit Berichte, die auf dem Manager eines Benutzers basieren, leichter ausgeführt werden können. (ID-12689).
- In Benutzerberichten erscheint die Konto-ID einer Ressource für alle Konten der Ressource in einer Liste, deren Einträge durch Semikolon getrennt sind.(ID-12820) Indirekt über eine Rolle oder Ressourcengruppe zugewiesene Konten und Ressourcen sind ebenfalls aufgeführt. Wenn nur ein Ressourcenkonto vorhanden ist, wird die Konto-ID nur angezeigt, wenn sie nicht gleich der Konto-ID von Identity Manager ist.
- Spaltentitel werden in PDF-Berichten jetzt ordnungsgemäß angezeigt. (ID-12794).
- Die Generierung zu langer `TaskTemplate`-Namen (d.h. länger als `MAX_NAME_LENGTH`) wurde behoben. (ID-13790).

## Repository

- Identity Manager unterstützt jetzt als Repository Oracle Database 10g Release2®. (ID-12908).

## Frühere Funktionen

- SQL Server 2005 wird nun als Repository unterstützt. (ID-14755) Gehen Sie wie folgt vor, um diese Version von SQL Server zu verwenden.
  1. Laden Sie den JDBC-Treiber für SQLServer 2005 (Version 1.2) von der Microsoft-Website herunter.
  2. Archivieren Sie die vorherige Version des Treibers, die sich im Verzeichnis `$WSHOME/WEB-INF/lib` befindet. Ersetzen Sie dann die alte Version durch den Treiber `sqljdbc.jar` in demselben Verzeichnis.
  3. Öffnen Sie das Datenbankerstellungsskript. Es kann günstig sein, beim Erstellen der Datenbank folgende Zeilen auszukommentieren:

```
ALTER DATABASE waveset SET READ_COMMITTED_SNAPSHOT ON
GO
```

Informationen zu diesen Zeichenketten entnehmen Sie bitte der Dokumentation zu SQL Server 2005.
  4. Zum Setzen des Repositorys mit den Befehlen `lh setup` oder `lh setRepro` verwenden Sie folgende Einstellungen:

```
type = SQLServer
jdbc driver = com.microsoft.sqlserver.jdbc.SQLServerDriver
url = jdbc:sqlserver://Rechnername:Port;DatabaseName=waveset
```

Rechnernamen und Port müssen Sie in der URL durch die gültigen Einstellungen ersetzen.
- Das IDM-Repository wird jetzt schneller initialisiert. (ID-14937).

## Ressourcen

### Neue Ressourcen

Seit Identity Manager 2005Q4M3 werden die folgenden neuen Ressourcen unterstützt: Weitere Informationen finden Sie im *Identity Manager Resources Reference Addendum*.

- HP OpenVMS (ID-8556)
- BridgeStream SmartRoles (ID-12262)
- OS/400 v4r5, v5r2, v5r3, and v5r4 (5.2, 5.3, and 5.4).
- Shell-Skript (ID-11906, ID-9866)
- Skript-JDBC (ID-7540)
- Siebel 7.8
- Realm-Unterstützung in Sun Java System Access Manager (ID-12414)

### Allgemein

- Identity Manager unterstützt jetzt das Speichern binärer Kontoattribute. Folgende Adapter unterstützen diese Funktion: (ID-8851, 12665).
  - Active Directory
  - LDAP
  - Flat File Active Sync
  - Datenbanktabelle
  - Skript-JDBC
  - Sun Java System Communications Services

Active Directory unterstützt jetzt die Binärattribute `thumbnailPhoto` (Windows 2000 Server und neuer) und `jpegPhoto` (Windows 2003). Die anderen Adapter unterstützen jetzt Attribute wie `jpegPhoto`, `audio` und `userCertificate`.

Identity Manager löst eine Ausnahme aus, wenn binäre oder komplexe Attribute an Ressourcen gesendet werden, die Binärattribute nicht unterstützen.

Binärattribute sollten so klein wie möglich gehalten werden. Wenn Sie ein Binärattribut laden, das zu groß ist (z.B. 200 KB), kann es sein, dass eine Fehlermeldung auftritt, die Sie darauf hinweist, dass die maximal zulässige Datenpaketgröße überschritten wurde. Wenden Sie sich an den Kundendienst, wenn Sie größere Attribute verwalten müssen.

- Ressourcenagent-Adaptoren besitzen jetzt das optionale Ressourcenattribut, das das Halten von Verbindungen bei Blockoperationen unterstützt: `RA_HANGTIMEOUT`. Dieses Attribut gibt die Zeitdauer (in s) an, bevor eine Anforderung an das Gateway außerhalb der Vorgabezeit liegt und als aufgehangen interpretiert wird. Der Standardwert ist 0, was bedeutet, dass nicht auf eine aufgehängene Verbindung geprüft wird. (ID-12455).
- Änderungen an `AttrParse`-Objekten werden jetzt wirksam, ohne dass Identity Manager neu gestartet werden muss. (ID-12516).
- An `AttrParse` wurde Leistungsverbesserungen vorgenommen. Der normale Parserprozess löst nicht mehr für jedes Zeichen im Puffer einen Ausnahmefehler aus (und fängt diesen auch nicht mehr ab). (ID-13384).
- Identity Manager unterstützt jetzt Verbindungen zu Mainframe-Ressourcen über die Emulator-Klassenbibliothek von Attachmate Reflection for the Web. Informationen zur Einrichtung dieses Leistungsmerkmals finden Sie im Abschnitt *Erweiterungen und Korrekturen der Dokumentation* dieser Versionshinweise. (ID-14815).

### Active Sync

- Der Active Sync-Assistent ist jetzt vollständiger lokalisiert. (ID-10504).
- Das System unterstützt jetzt wiederholte Versuche von Active Sync an Ressourcen. Zum Aktivieren dieses Leistungsmerkmals erweitern Sie den XML-Code der Ressource um zwei Ressourcenattribute der Form:

```
<ResourceAttribute name="syncRetryCountLimit" type="string"
multi="false" facets="activesync" value="180"/>
<ResourceAttribute name="syncRetryInterval" type="string"
multi="false" facets="activesync" value="10000"/>
```

`syncRetryCountLimit` gibt an, wie oft die Aktualisierung versucht werden soll. `syncRetryInterval` gibt an, wie lange (in Millisekunden) zwischen den Wiederholungen gewartet werden muss. Diese Werte erscheinen danach bei der ActiveSync-Konfiguration als benutzerspezifische Ressourceneinstellungen. Sie sollten einen Anzeigenamen (`displayName`) angeben. Verwenden Sie dafür einen benutzerspezifischen Katalogschlüssel, wenn dieser Name lokalisiert angezeigt werden soll. (ID-11255).

- Die Maximalanzahl der in einer ActiveSync-Ressource konfigurierten Active Sync-Protokolle wird jetzt ordnungsgemäß eingehalten. (ID-11848).

### Domino

- Sie können jetzt Domino-Benutzer ohne ID-Datei oder E-Mail-Adresse, aber mit einem Eintrag im Domino-Verzeichnis erstellen. (ID-11201).
- Auf Domino 6.x-Ressourcen können Sie jetzt Konten deaktivieren, ohne eine Liste mit Verweigerungsgruppen erstellen zu müssen. Wenn keine Verweigerungsgruppen angegeben sind, nutzt Identity Manager zum Aktivieren bzw. Deaktivieren auf der Domino-Ressource das Attribut „CheckPassword“. Der Wert 2 deaktiviert ein Konto. (ID-12088).
- Beim Domino-Ressourcenadapter rufen gleichzeitige Aktualisierungen von HTTPPassword mit mehreren Benutzern mithilfe der API `NSFNoteComputeWithForm()` keinen Gateway-Fehler “-551” mehr hervor. (ID-12466).

### Verzeichnis

- Identity Manager bietet jetzt einen skalierbareren Mechanismus zum Bearbeiten großer Attribute von Ressourcenobjekten. Beispielformulare zur Verwendung dieser Methode zum Verwalten von LDAP-Gruppen finden Sie in der Datei `sample/forms/LDAPgroupScalable.xml`. (ID-9882).
- Der LDAP-Ressourcenadapter verwendet jetzt den JSSE-Provider direkt. (ID-9958) Die niedrigste unterstützte Java-Version auf Identity Manager ist jetzt 1.3. Dadurch können für die SSL-Kommunikation bei Domino., LDAP- und

NDS SecretStore-Ressourcenadaptern Sicherheitsfremdanbieter verwendet werden. Sie können Bibliotheken von Sicherheitsfremdanbietern mithilfe der Datei `java.security` registrieren.

Weitere Informationen finden Sie unter

<http://java.sun.com/j2se/1.4.2/docs/guide/security/CryptoSpec.html#ProviderInstalling>.

- LDAP-Gruppen, deren Namen Vorwärts-Schrägstriche enthalten, können jetzt bearbeitet werden. (ID-9872).

Das Konfigurationsattribut

`LdapJndiConnectionFactory.alwaysUseNames`-Eigenschaft wurde zur Datei `Waveset.properties` hinzugefügt.

Standardmäßig ist diese Eigenschaft aktiviert. Wenn sie aktiviert ist, werden alle String-Namen mithilfe des `NameParsers` des Kontexts in einen Namenstring eingelesen. Dadurch werden Probleme mit JNDI-Escapezeichen vermieden. Diese Option ist nur sinnvoll, wenn die Option `LdapJndiConnectionFactory.wrapUnpooledConnections` auf „true“ gesetzt ist.

Sie benötigen JVM 1.4 oder neuer, wenn dieser Wert explizit auf „true“ gesetzt werden soll oder Sie mit dem „true“-Wert arbeiten wollen Wegen eines Problems mit JNDI können in früheren JVM-Versionen Umbenennungsoperationen fehlschlagen, wenn diese Option aktiviert ist.

- Der LDAP-Adapter generiert für ein neues Konto keinen unzulässigen Distinguished Name (DN) mehr. (ID-10951).  
Die `escape`-Methode in `com.sun.idm.util.ldap.DnUtil` kann jetzt in Formularen verwendet werden, um Werte, die in Identitätsvorlagen von Ressourcenadaptern im LDAP DN-Format eingefügt werden sollen, zu überspringen. Als Alternative kann eine `accountId`-Richtlinie mit aktivierter Option „LDAP-DN-Format verlangen“ verwendet werden, um LDAP DNs, die z.B. durch Benutzer, ActiveSync oder Abstimmungsrichtlinien in Identity Manager eingegeben werden, zu validieren.
- Der Standardwert für das ActiveSync-Attribut **Zu synchronisierende Objektklassen** auf LDAP-Ressourcen ist jetzt standardmäßig `inetorgperson`. (ID-11644).
- Die Leistung des `LDAPActiveSync`-Suchfilters, mit dem Änderungsprotokolle nach Änderungen durchsucht werden, wurde optimiert. Der Filterteil (`objectClass=changelogEntry`) wurde vom Standardsuchfilter entfernt. (ID-11722).

Sie können die alte Funktionsweise wiederherstellen, indem Sie das Ressourcenattribut **Remove objectClass from Search Params Filter** mit dem Wert „false“ wie folgt zur Ressourcendefinition hinzufügen:

## Frühere Funktionen

```
<ResourceAttribute name="Remove objectClass from Search Params
Filter" displayName="Remove objectClass from Search Params
Filter" facets="activesync" value="false">
</ResourceAttribute>
```

Hinweis: Sie können diese Einstellung nicht von der GUI aus ändern.

- Die Änderung von LDAP-Gruppenmitgliedschaften nutzt jetzt einzelne Hinzufüge- und Entfernungsvorgänge, anstatt die gesamte Gruppe zu ändern (d. h. das gesamte Attribut `uniqueMember` wurde ersetzt). (ID-13035).
- Der LDAP-Adapter kann so konfiguriert werden, dass der Vorgang "VLV Sort" an einem anderen Wert als `uid` erfolgt. (ID-13321) Zum Ändern dieses Werts fügen Sie Folgendes in die Ressourcendefinition ein:

```
<ResourceAttribute name="vlvSortAttribute" displayName="VLV Sort
Attribute" description="VLV Sort Attribute"
value="myValue"></ResourceAttribute>
```

- Das Active Directory-Attribut `PasswordNeverExpires` kann jetzt auch während einer Aktualisierung gesetzt werden. (ID-13710).
- Der NDS Active Sync-Adapter fragt Änderungen nicht mehr basierend auf der Eigenschaft „`lastModifiedTimeStamp`“ des Benutzerobjekts ab. Dieses Attribut wurde bei jeder Benutzeran- und -abmeldung aktualisiert. Zur Behebung dieses Problems wird der letzte geänderte Wert jetzt aufgrund der Eigenschaft „`lastModifiedTimestamp`“ der in der Schemazuordnung definierten Benutzerattribute berechnet. Wenn „`lastModifiedTimestamp`“ eines Attributs größer als das Highwater Mark des Adapters ist, meldet das Gateway diesen Benutzer dem Server als geändert. (ID-13896)
- Es wurde ein Problem behoben, aufgrund dessen neu erstellte NDS-Benutzer keinen Zugriff auf ihre Home-Verzeichnisse hatten. (ID-14208).
- Zeitüberschreitungen beim Active Directory-Datenabruf verursachen kein vorzeitiges Ende von Abstimmungsvorgängen mehr. (ID-14564)
- Es wurde ein Problem behoben, durch das sich der Active Directory Active Sync-Adapter aufhängt, weil Verbindungen zum Gateway nicht geschlossen werden. (ID-14597).
- Der LDAP-Adapter erlaubt der Aktivierungskurzmethode `nsaccountlock` die Verwendung von Logik, die bei der Deaktivierung von LDAP-Benutzern deren An- und Abwesenheit berücksichtigt. (ID-14925) Weitere Informationen hierzu finden Sie im Abschnitt *Erweiterungen und Korrekturen der Dokumentation* dieser Versionshinweise.

## Oracle ERP

- Der Oracle ERP-Adapter wurde zur Unterstützung von Überprüfungsfunktionen um mehrere Attribute erweitert. (ID-11725) Genauere Informationen hierzu finden Sie im Abschnitt *Erweiterungen und Korrekturen der Dokumentation* dieser Versionshinweise.
- Der Oracle ERP-Adapter schließt jetzt Oracle-Datenbankzeiger. Vorher wurde dadurch der folgende Fehler verursacht: (ID-12222).
- In Formularen für Oracle ERP-Adapter kann die Methode `listResourceObjects` der Klasse `com.waveset.ui.FormUtil` jetzt die spezifischen Zuständigkeitsbereiche eines Benutzers zurückgeben und so gefiltert werden, dass entweder alle oder nur die aktiven Zuständigkeitsbereiche zurückgegeben werden. (ID-12629).

Die übergebenen Optionen sind:

- `key id` - (String) Die ID der Ressource, deren Zuständigkeitsbereiche zurückgegeben werden
- `activeRespsOnly` - (String) „true“ oder „false“. Der Standardwert ist „false“.
- Der Oracle ERP-Adapter bietet jetzt das Schlüsselwort `sysdate` bzw. `SYSDATE`. Sie können dieses Schlüsselwort mit `to_date` zur Angabe eines Ablaufdatums (in der lokalen Zeit eines Oracle E-Business Suite-Servers, EBS) für einen Zuständigkeitsbereich verwenden. (ID-12709).
- Der Oracle ERP-Adapter von Identity Manager bietet jetzt das neue Kontoattribut `employee_number`. Dieses Attribut stellt eine Mitarbeiternummer (`employee_number`) aus der Tabelle `per_people_f` dar. Weitere Informationen hierzu finden Sie im Abschnitt *Erweiterungen und Korrekturen der Dokumentation* dieser Versionshinweise. (ID-12710).
- Das Aktualisieren des Zuständigkeitsbereiches eines Oracle ERP-Kontos mithilfe des Oracle ERP-Adapter aktualisiert keine anderen, zu diesem Konto gehörigen Zuständigkeitsbereiche mehr. (ID-13889) Infolgedessen wird nur der Oracle ERP-Überprüfungszeitstempel für den geänderten Zuständigkeitsbereich aktualisiert. Die Oracle ERP-Überprüfungszeitstempel für die anderen Konto-Zuständigkeitsbereiche bleiben unverändert.
- Zur Schema-Zuordnung für den Oracle ERP-Adapter wurde das Attribut „`person_fullname account`“ hinzugefügt. Im Oracle ERP-Benutzerformular dient dieses Attribut zur Anzeige des Felds „Personenname“. Dieses Feld ist schreibgeschützt und zeigt den vollständigen Namen eines Benutzers an, wenn ein Oracle ERP-Konto mit einem Oracle HR-System, das mit Mitarbeiternummern arbeitet, verknüpft ist. (ID-14675).
- Der Oracle ERP-Adapter verhindert jetzt das Löschen von Ressourcenkonten-Verknüpfungen, wenn eine Oracle ERP-Ressource während einer vollständigen Abstimmung nicht zugänglich ist. (ID-14960) (Eine Ressource kann aus vielen Gründen, z.B. wegen nicht ordnungsgemäßer Konfiguration der Ressourcenverbindung, unzugänglich sein.)

## Frühere Funktionen

- Der Oracle ERP-Adapter unterstützt jetzt Oracle E-Business Suite 12. Nähere Informationen finden Sie unter *Erweiterungen und Korrekturen der Dokumentation* in diesen Versionshinweisen. (ID-15062, 16705).
- Der Oracle ERP-Adapter wurde zur Unterstützung von Kontingentausführungen um das Kontoattribut `npw_number` erweitert. (ID-16507).

## SAP und SAP HR

- Sie können den SAP HR-Adapter jetzt für die Verarbeitung von IDOCs beliebiger Meldungstypen konfigurieren. Vorher konnten nur IDOCs vom Typ HRMD\_A verarbeitet werden. (ID-12120).
- Die SAP- und SAP HR-Adapter enthalten jetzt drei neue Ressourcenattribute, die Parameter zum Wiederholen einer SAP-Operation nach Netzwerkfehlern verfügbar machen. (ID-12579) Diese Attribute sind:
  - SAP-BAPI-Wiederholungen - gibt an, wie oft der betreffende Vorgang wiederholt werden soll.
  - SAP-Verbindungswiederholungen - gibt an, wie oft der Versuch der Verbindungsherstellung zum SAP-Server wiederholt werden soll.
  - Intervall für SAP-Verbindungswiederholungen - gibt an, wie lange (in ms) gewartet werden soll, bis der Versuch der Verbindungsherstellung zum SAP-Server wiederholt wird.
- Bei der Verwendung des CUA.Modus auf SAP-Ressourcen können Passwörter jetzt als nicht abgelaufen gesetzt werden. (ID-13355).
- Der SAP-Adapter erzeugt keine JCO\_ERROR\_FUNCTION\_NOT\_FOUND-Ausnahme mehr, wenn das SAP-System das PASSWORD\_FORMAL\_CHECK-Funktionsmodul nicht enthält. (ID-14663).
- Der SAP-Adapter meldet den Status deaktivierter Konten jetzt ordnungsgemäß. (ID-14834).
- Aktivitätsgruppen (Rollen) und Profile können in einer CUA-Umgebung nun mit einem Anfangs- und Enddatum aktualisiert werden. (ID-15613).

Für Rollen ordnen Sie dem `activityGroups`-Attribut im Adapter Folgendes zu:

```
CUA->directLocalActivityGroupObjects
```

Für Profile ordnen Sie `profiles` Folgendes zu:

```
CUA->directLocalProfileObjects
```

- Der SAP-Adapter unterstützt jetzt die Aktualisierung des ALIAS-Felds in SAP. Die Attributzuordnung in der Schemakonfiguration ist ALIAS->USERALIAS. (ID-16320).

## UNIX

- UNIX-basierte Adapter enthalten jetzt das Ressourcenattribut „Ausgangsverzeichnis-Basis“. Wenn es vorhanden ist, hat die Einstellung dieses Attributs Vorrang vor der des Ausgangsverzeichnisses auf der nativen Ressource, auf der das Konto erstellt werden soll. Die Einstellung für diesen Wert ist der eigentliche Attributwert gefolgt von der `Konto-ID`. Wenn in den Kontenattributen des Benutzers ein Ausgangsverzeichnis angegeben ist, so hat dieses jedoch Vorrang gegenüber der Einstellung in „Ausgangsverzeichnis-Basis“. (ID-8587).
- Über „Ressourcentyp-Richtlinie“ können Sie jetzt Standardwerte für Zeitüberschreitungen festlegen. Darüber hinaus können Sie mit der Eigenschaft `maxWaitMilliseconds` auch die Abfragefrequenz steuern, die der Skript-Adapter von Identity Manager verwendet, wenn er auf das Abschließen einer Aufgabe durch eine Ressource wartet. (ID-11906).
- Solaris- und Linux-Adapter liefern jetzt Anmeldeinformationen des letzten Jahres. (ID-12182).
- Beim Anzeigen von Kontoinformationen von einer mit NIS konfigurierten Solaris-Ressource werden mit dem Gruppennamen anstatt der numerischen Gruppen-ID Informationen zur Gruppenmitgliedschaft angezeigt. (ID-12667)
- Die Solaris-, AIX-, HP-UX-, Red Hat Linux- und SuSE Linux-Ressourcenadapter wurden um zwei Ressourcenattribute erweitert: Default Primary Group und Login Shell. (ID-15034).

## Sonstige Adapter

- Mit dem RACF-Ressourcenadapter können Sie jetzt Dataset-Regeln direkt überwachen, statt sie von Identity Manager verwalten zu lassen. Dadurch können Sie Dataset-Regeln erstellen, die sich von den Identity Manager-nativen Regeln unterscheiden. (ID-10446).

Im folgenden Beispiel wird mit der „after create“-Regel anstatt der Identity Manager-Standardregel von `<user id>.**` die Dataset-Regel von `<user id>.test1.**` erstellt.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE ResourceAction PUBLIC "waveset.dtd" "waveset.dtd">
<ResourceAction name="create after action">
  <ResTypeAction restype="RACF">
    <act>
      var TSO_PROMPT = "READY";
      var TSO_MORE = "****";
      var cmd1 = "addsd ""+identity+".test1.**"
owner("""+identity+""") [enter]";
      var result1 = hostAccess.doCmd(cmd1, TSO_PROMPT, TSO_MORE);
    </act>
  </ResTypeAction>
</ResourceAction>
```

## Frühere Funktionen

- Der RACF-Adapter unterstützt jetzt Suchfilter für `listAllObjects`. (ID-10895).
- Sie können in Siebel jetzt Objekte erstellen und aktualisieren, die eine Navigation durch eine Hierarchie mit Business-Komponenten erfordern. Weitere Informationen hierzu finden Sie im Abschnitt *Erweiterungen und Korrekturen der Dokumentation* in diesen Versionshinweisen. (ID-11427).
- Die Methode `isPickListAttribute` im Siebel-Adapter wird vom Verfolgungssystem nicht mehr fälschlicherweise als `isMVGAttribute` erkannt. (ID-11471).
- Bei SecurId-Ressourcen wird das Attribut „Clients“ jetzt als optionales Attribut behandelt. (ID-11509).
- Der Flat File Active Sync-Adapter zeigt jetzt im Active Sync-Protokoll (falls aktiviert) einen Warnhinweis an, wenn ein Fehler auftritt, der für Synchronisierungszwecke eine `diff`-Aktion verhindert. (ID-12484).
- Wenn Sie Identity Manager zur Bereitstellung für eine RSA Clear Trust 5.5.2-Ressource konfigurieren, sind zur SSL-Kommunikation im Gegensatz zu früheren Clear Trust-Versionen keine weiteren Bibliotheken erforderlich. (ID-12499).
- Im Datenbanktabellenassistent können Sie keine Tabellen mehr konfigurieren, für die Sie keine Zugriffsrechte besitzen. (ID-12643).
- Der Siteminder LDAP-Adapter führt jetzt die folgenden Operationen auch dann ordnungsgemäß aus, wenn Siteminder-Benutzer aufgrund fehlgeschlagener Anmeldungen gesperrt wurden. (ID-12824).
  - aktivieren
  - disable
  - Expire password (mit Aktivierung/Deaktivierung)
  - Unexpire password (mit Aktivierung/Deaktivierung)
- Der RACF-Adapter sucht für jeden einzelnen in `listAllObjects` aufgeführten Benutzer keine lange Zeichenkette mehr. Dadurch wird diese Funktion bei einer großen Benutzeranzahl schneller. (ID-12829).
- Kontingenteinstellungen sind für temporäre Tablespace nicht zulässig. Wenn in Oracle 10gR2 versucht wird, solche Einstellungen vorzunehmen, kommt es zu einer SQL-Ausnahme. (ID-12843).

Bislang legte der Ressourcenadapter für temporäre Tablespace ein Kontingent fest, auch wenn das Kontoattribut `oracleTempTSQuota` nicht zugeordnet wurde. Dieses Verhalten wurde geändert. Wenn Sie das Attribut `oracleTempTSQuota` zuordnen, ändert sich das Verhalten nicht. Wenn Sie die Zuordnung löschen, wird für temporäre Tablespace dagegen kein Kontingent festgelegt.

Löschen Sie für Oracle 10gR2-Ressourcen das Attribut `oracleTempTSQuota` aus dem Ressourcenadapter.

- Identity Manager setzt vor dem Löschen eines Benutzers mit sicherem ID jetzt Admin-Zugriffsrechte (falls vorhanden) zurück. (ID-13053).
- Es wurde ein Problem behoben, das beim Ausführen einer Abstimmung auf VMS auftrat. (ID-13425).
- SecurID für UNIX-Adapter führt bei der Zusammenarbeit mit RSA jetzt UTF-8-Codierung und -Decodierung aus. (ID-13451).
- Der Shell-Skript-Adapter erkennt jetzt Fehler, die von einer Ressourcenaktion während des Erstellens von Benutzern und Aktualisierens von Funktionen generiert wurden. (ID-13465)
- Beim Erstellen eines Kontos auf einer Windows NT-Ressource über den Windows NT-Ressourcenadapter wird auf der Ergebnisseite „Benutzer erstellen“ die folgende Fehlermeldung nicht mehr angezeigt: “Error requiring password: put\_PasswordRequired(): 0X80004005:E\_FAIL”. (ID-13618).
- Zum Datenbanktabellenadapter wurde der neue Ressourcenkonfigurationsparameter „enableEmptyString“ hinzugefügt. Damit wird in zeichenbasierten Spalten, die im Tabellenschema als ungleich null definiert wurden, anstatt eines NULL-Wertes das Schreiben eines Leerstrings ermöglicht. Diese Option hat keinen Einfluss darauf, wie Strings für Oracle-basierte Tabellen geschrieben werden. (ID-13737).
- Der Shell-Skript-Adapter unterstützt jetzt die Umbenennungs-, Deaktivierungs- und Aktivierungsfunktionen. (ID-14472).
- Der Skript-JDBC-Adapter aktualisiert jetzt Attribute ordnungsgemäß, deren ursprünglicher Wert null war, die aber auf einen Wert ungleich null gesetzt werden. (ID-14655).

## Rollen

- Mithilfe von Rollen und Ressourcengruppen können Benutzern jetzt einzeln oder in Kombinationen auf einer Ressource mehrere Konten zugewiesen werden. Weitere Informationen hierzu finden Sie im Abschnitt *Erweiterungen und Korrekturen der Dokumentation* dieser Versionshinweise. (ID-6684).

## Frühere Funktionen

- Beim Importieren von Rollen, die Verknüpfungen zu vorhandenen übergeordneten Rollen enthalten, aktualisiert Identity Manager jetzt die vorhandenen Rollen mit den Verknüpfungen zu den neu importierten Rollen. (ID-15482).

Identity Manager erkennt und erstellt Verknüpfungen von vorhandenen übergeordneten Rollen zu den untergeordneten Rollen, die darauf verweisen. Bei einer Aufrüstung führt Identity Manager die Klasse RoleUpdater aus, die zum Reparieren von Rollen dient.

Sie können Rollen außerhalb des Upgrade-Prozesses aktualisieren, indem Sie die Datei RoleUpdater.xml unter sample/forms/RoleUpdater.xml neu importieren. Identity Manager fügt während der Aufrüstung oder beim Importieren von RoleUpdater.xml standardmäßig die Verknüpfungen für untergeordnete Rollen hinzu.

Um diese neue Funktion zu deaktivieren, setzen Sie das RoleUpdater-Attribut `nofixsubrolelinks` auf „true“. Zum Beispiel:

```
<MapEntry key="nofixsubrolelinks" value="true" />
```

Weitere Informationen zum automatischen Aktualisieren von Rollen während des Imports finden Sie unter ID-15053 im Abschnitt „Bekannte Probleme“.

## Sicherheit

- Benutzer mit der Berechtigung „Genehmiger“ können alle zukünftigen Genehmigungsanforderungen für einen bestimmten Zeitraum an einen oder mehrere Benutzer, die keine Identity Manager-Genehmiger sind, delegieren. Die Delegation ist mithilfe dreier Methoden möglich: (ID-8485).
  - Endbenutzer-Hauptmenü - Link „Genehmigungen delegieren“
  - Registerkarte „Genehmigungen“ - Unterregisterkarte „Eigene Genehmigungen delegieren“
  - Admin - Benutzerkonto erstellen/bearbeiten/anzeigen - Abschnitt „Sicherheit“
- Die Passwörterzeugung funktioniert jetzt ordnungsgemäß und schlägt erwartungsgemäß fehl, wenn Passwörter nicht ordnungsgemäß generiert wurden. (ID-12275).
- Identity Manager bietet jetzt den Authentifizierungstyp „EndUserLibrary“. Die Fähigkeit „EndUser“ (AdminGroup) kann jetzt Bibliotheken mit dem Authentifizierungstyp „EndUserLibrary“ anzeigen und deren Inhalt auflisten. (ID-12469).

Setzen Sie `authType="EndUserLibrary"` und vergewissern Sie sich, dass Parameter „MemberObjectGroup“ der Bibliothek auf „All“ gesetzt ist.
- Identity Manager-Benutzer Sitzungen mit mehreren gleichzeitigen Anmeldungen ausführen. Sie können dies so einschränken, dass nur noch eine Sitzung pro Anmeldeanwendung möglich ist. Hierzu ändern Sie den Wert des

Konfigurationsattributs „security.authn.singleLoginSessionPerApp“ im Systemkonfigurationsobjekt. Dieses Attribut ist ein Objekt, das wiederum ein Attribut pro Anmeldeanwendung enthält (z. B. für die Administratoroberfläche, die Benutzeroberfläche oder BPE). Ändern Sie den Wert dieses Attributs auf „true“, damit für jeden Benutzer nur noch eine einzige Anmeldesitzung möglich ist. (ID-12778).

Wenn dies gewünscht ist, können sich Benutzer mit mehreren Sitzungen gleichzeitig anmelden. Es bleibt jedoch nur die letzte Anmeldesitzung aktiv und gültig. Wenn der Benutzer versucht, unter einer ungültigen Sitzung eine Aktion auszuführen, wird die Sitzung automatisch beendet.

- Von Administratoren durchgeführte Endbenutzer-Passwortänderungen, die über SPML oder andere Verfahren durchgeführt wurden, werden nicht in der Passwortabfolge aufgezeichnet. Es stehen nun zwei Möglichkeiten zur Verfügung, die Anwendung so zu konfigurieren, dass ein Passwort in der Historie des Benutzers gespeichert wird. Nur eine Methode ist erforderliche. (ID-13029).

- Ansichtsoption (hat Vorrang, sofern vorhanden oder „true“). Setzen Sie das Attribut savePasswordHistory im Zielformular. Beispiel:

```
<Field name="savePasswordHistory">
  <Default>
    <Boolean>true</Boolean>
  </Default>
</Field>
```

- Schalten Sie das Verhalten der gewünschten Schnittstelle mit der folgenden Systemkonfigurationseinstellung um. Sofern noch nicht vorhanden, muss diese dem Systemkonfigurationsobjekt hinzugefügt werden.

```
<Attribute name="security">
  <Object>
    <Attribute name="admin">
      <Object>
        <Attribute name="changePassword">
          <Object>
            <Attribute name="Administrator Interface">
              <Object>
                <Attribute name="savePasswordHistory">
                  <Boolean>true</Boolean>
                </Attribute>
              </Object>
            </Attribute>
          </Object>
        </Attribute>
      </Object>
    <Attribute name="Command Line Interface">
      <Object>
        <Attribute name="savePasswordHistory">
          <Boolean>true</Boolean>
        </Attribute>
      </Object>
    </Object>
  </Object>
</Attribute>
```

## Frühere Funktionen

```
</Attribute>
<Attribute name="IVR Interface">
  <Object>
    <Attribute name="savePasswordHistory">
      <Boolean>>false</Boolean>
    </Attribute>
  </Object>
</Attribute>
<Attribute name="SOAP Interface">
  <Object>
    <Attribute name="savePasswordHistory">
      <Boolean>>true</Boolean>
    </Attribute>
  </Object>
</Attribute>
<Attribute name="User Interface">
  <Object>
    <Attribute name="savePasswordHistory">
      <Boolean>>false</Boolean>
    </Attribute>
  </Object>
</Attribute>
</Object>
</Attribute>
</Object>
</Attribute>
....
```

## Server

- Von TaskInstance abgeleitete Objekte wie z.B. Genehmigungen werden jetzt bei Beendigung einer Aufgabe ordnungsgemäß gelöscht. (ID-3258).
- Identity Manager benötigt jetzt Zugriff auf das Verzeichnis tmp. (ID-7804) Wenn Ihr Anwendungsserver eine Sicherheitsrichtlinie verwendet, müssen Sie folgende Berechtigung festlegen:

```
permission java.io.FilePermission "$(java.io.tmpdir)$(/)*",
"read,write,delete";
```

- Die Seite „Benutzer suchen“ kann jetzt tief verschachtelte Hierarchien vieler Organisationen verarbeiten. (ID-10352).
- In Cluster-Umgebungen erzeugt eine fehlgeschlagene Anmeldung auf den Endbenutzerseiten keinen Serialisierungsausnahmefehler mehr. (ID-10556).
- Server lösen keine Failover-Mechanismen mehr an sich selbst aus und beenden Ihre eigenen Aufgaben, wenn die Verarbeitung von Aufgabeninformationen zu lange dauert. (ID-10920).

- Erweiterte Benutzerattribute werden jetzt ordnungsgemäß aus Benutzerobjekten gelöscht. (ID-11721).
- ResourceConnectionManager wird jetzt über das bevorstehende Herunterfahren des Systems informiert. Deswegen braucht der Server nicht mehr auf Zeitüberschreitungen von SSH-Verbindungen zu warten, bevor er beendet wird. (ID-12214).
- Es wurde ein Problem behoben, durch das auf der Seite „Aufgaben verwalten“ für Benutzer in untergeordneten Organisationen, die keinen administrativen Zugriff auf übergeordnete Organisationen haben, der Fehler „no cache error“ ausgelöst wurde. (ID-12288).
- Die Verarbeitung von Begrenzungszeichen wird jetzt zwischen eckigen Klammern unterdrückt. Als Folge davon werden jetzt alle zwischen eckigen Klammern erkannten Zeichen als Index oder Filter interpretiert. Hinweis: Gegenwärtig existiert kein Verfahren zum Umschalten nach Erkennung der schließenden eckigen Klammer „]“. (ID-12384).
- Das Beenden von Aufgabeninstanzen wird jetzt als Terminate-Aktion anstatt Modify-Aktion protokolliert. (ID-12791).
- Benutzeraktionen können an Benutzern ausgeführt werden, nachdem Ressourcen, die diesen Benutzern direkt zugewiesen waren, gelöscht wurden. (ID-14806).

## SOAP

- Die SPML-Unterstützung wurde erweitert, sodass jetzt neben Personen auch Rollen und Ressourcengruppen unterstützt werden. (ID-8850).
- Die neue Fähigkeit „SPMLAccess“ ermöglicht den Kontenadministratorzugriff auf die SPML-Schnittstelle. (ID-10854).
- Der SPML-Server gibt jetzt Fehler für Anforderungen zurück, die Filter mit noch nicht implementierten Operatoren enthalten. (ID-11343).
- Die SPML-Schnittstelle von Identity Manager bietet den Anmeldeparameter „login ExtendedRequest“, mit dessen Hilfe sich Benutzer als Administrator anmelden können. Ab dieser Version bietet die SPML-Schnittstelle auch einen Parameter „loginUser ExtendedRequest“, mit dessen Hilfe Benutzern eine Sitzung für die Selbstbereitstellung zugewiesen werden kann. Dieser „loginUser ExtendedRequest“ unterstützt die Anmeldung mit Passwort oder mit Antworten auf Sicherheitsfragen. (ID-12103).

# Ansichten

- Die Benutzeransicht bietet jetzt das folgende Steuerattribut: (ID-4383).  
`accounts[Resname].waveset.forceUpdate`  
Hierbei ist **Resname** der Name der Ressource. Der Wert dieses Attributs ist eine Liste mit Ressourcenkontenattributen, die immer dann zur Aktualisierung an eine Ressource gesendet werden, wenn ein Benutzer geändert wird.
- Die Ansichten für Ressourcenkonten (DeprovisionViewer, DisableViewer, EnableViewer, PasswordViewer, RenameUserViewer, ReprovisionViewer und UnlockViewer) unterstützen jetzt zwei neue Optionen zum Abrufen von Ressourcenkontenattributen für Benutzer: (ID-10176).
  - › `fetchAccounts` – (Boolean) Wenn dieser Parameter auf „true“ gesetzt ist, enthält die Ansicht Kontenattribute für die dem Benutzer zugewiesenen Ressourcen.
  - › `fetchAccountResources` – eine Liste mit Ressourcennamen, die abgerufen werden können. Wenn hier nichts angegeben ist, verwendet Identity Manager alle zugewiesenen Ressourcen.

# Workflow

- Bei der Ausführung von Workflows wird keine „checkReference“-Warnung mehr ausgegeben. (ID-10802).
- Wenn Meldungen mithilfe von `notification.redirect` in eine Datei umgeleitet werden, wird diese Datei jetzt mithilfe der Methode `emailNotifier.contentCharset` geschrieben. Diese Methode dient auch zum Erstellen von E-Mails aus Meldungen. Dadurch kann die Datei auch Zeichen enthalten, die nicht im ISO-8859-1-Zeichensatz enthalten sind. (ID-10331, 14984).
- Workflow-Meldungen enthalten ausführlichere Informationen, wenn ein Genehmiger Arbeitseinheiten genehmigt oder ablehnt, die bereits genehmigt bzw. abgelehnt wurden. (ID-11045).
- Identity Manager bietet jetzt den Workflow-Dienst `auditPolicyScan`. Sie können diesen Workflow-Dienst dazu nutzen, Benutzer auf der Grundlage der ihnen zugewiesenen Richtlinien nach Verstößen gegen Überprüfungsrichtlinien abzufragen. Wenn dem betreffenden Benutzer keine Richtlinie zugewiesen ist, wird die seiner Organisation zugewiesene Richtlinie (falls vorhanden) verwendet. Weitere Informationen hierzu finden Sie im Abschnitt *Erweiterungen und Korrekturen der Dokumentation* dieser Versionshinweise. (ID-12589).
- Der Authentifizierungstyp „RoleAdminTask“ wurde zur Aufgabendefinition „Rolle verwalten“ und der Authentifizierungstyp „ResourceAdminTask“ zur Aufgabendefinition „Ressource verwalten“ hinzugefügt. (ID-12768).

## In früheren Versionen behobene Fehler

---

Dieser Abschnitt beschreibt Fehler, die seit Identity Installation Pack 2005Q4M3 behoben wurden.

### Installation und Aktualisierung

- Bei einer Aufrüstung wird die E-Mail-Vorlage „Zugriffsprüfung“ nicht mehr überschrieben. (ID-13216).

### Administratorbenutzeroberfläche

- Wenn Sie für das Benutzerapplet-Menü eine neue Benutzeraktion konfigurieren, werden Textschlüssel jetzt ordnungsgemäß angezeigt. (ID-8400).
- Identity Manager behandelt jetzt Hilfeanzeigen, die Fehler auslösten, weil sie Sonderzeichen enthielten, ordnungsgemäß. (ID-8747).
- Wenn das Attribut „singleLoginSessionPerApp“ einer Anmeldeanwendung auf „true“ gesetzt ist, verhält sich Identity Manager wie folgt: Benutzer können sich an der gleichen Anwendung mehrmals anmelden. Die aktive und gültige Sitzung ist jedoch die, bei der sich der Benutzer zuletzt angemeldet hat. Wenn der betreffende Benutzer als der gleiche Identity Manager-Benutzer während einer anderen Anmeldesitzung eine Aufgabe ausführen will, wird er automatisch abgemeldet und die Sitzung wird beendet. (ID-9543).
- Wenn ein Benutzer direkt einer Organisation zugewiesen ist und eine UserMemberRule diesen Benutzer der gleichen Organisation zuweist, wird der betreffende Benutzer in der Liste nicht mehr dupliziert. (ID-10410).
- Die Seite „Sitzungstimeout für die Anmeldung“ kann jetzt lokalisiert werden und wird in der vom Gebietsschema des Benutzers angegebenen Sprache angezeigt. (ID-10571).
- Das Beispielformular zur LDAP-Passwortsynchronisierung (sample/forms/LDAPPasswordActiveSyncForm.xml) setzt jetzt das Feld `waveset.password` anstatt `password.password` und `password.confirmpassword`. (ID-11660).
- Die Administratorbenutzeroberfläche von Identity Manager generiert keine Fehler mehr, wenn Suchergebnisse einen Benutzernamen mit einfachem Anführungszeichen enthalten und dieser Name in einem Link für einen nachfolgend auszuführenden Befehl verwendet wird. (ID-11123).
- MultiSelect-Komponenten zeigen jetzt einfache Zeichenfolgen ordnungsgemäß an. (ID-11979).

## In früheren Versionen behobene Fehler

- Identity Manager zeigt jetzt eine korrekte Fehlermeldung an, wenn Sie versuchen, einen Ressourcenobjekttyp zu bearbeiten, der keine Aktualisierungen unterstützt. (ID-12242).
- Beim Auflisten von Ressourcen mithilfe der Strukturtabelle werden jetzt Knoten mit Namen, die Unterstriche enthalten, ordnungsgemäß aufgeklappt. (ID-12478).
- Die Online-Hilfe zeigt jetzt die richtigen Hilfeseiten an, wenn im ActiveSync-Konfigurationsteilmenü Optionen, die nicht im Assistenten verfügbar sind, ausgewählt werden. (ID-12597).
- Benutzer können im französischen Gebietsschema jetzt ordnungsgemäß gelöscht werden. (ID-12642).
- Strukturtabelle, Kontoseite und die Seite „Suchergebnisse“ zeigen jetzt als Managername von Identity Manager ein unaufgelöstes Manager-Attribut in Klammern an. Bei jeder Benutzeraktualisierung versucht Identity Manager, dieses Manager-Attribut aufzulösen. Wenn das Attribut aufgelöst werden kann, entfernt Identity Manager die Klammern und führt am neuen Wert eine Beschränkungsüberprüfung aus. (ID-12726).
- Der Link im Anmeldefenster für eine anonyme Benutzeranmeldung zeigt jetzt auf die neue Endbenutzer-Arbeitseinheitentabelle. (ID-12816).
- Schaltflächen der TabPanel-Komponente können jetzt positioniert werden. (ID-12797).
- Identity Manager konvertiert jetzt E-Mail-Vorlagen mit der Standarddatei mail.example.com in die neue Variablenfunktionalität der Serverkonfiguration. (ID-12720).
- Passwortfelder werden jetzt bedingt angezeigt, wenn die Identity Manager-Benutzeroberfläche das LH-Anmeldemodul nicht enthält und dem betreffenden Benutzer eine Admin-Rolle zugewiesen ist. (ID-12692).
- Identity Manager zeigt Ressourcengruppenlisten, auf die über die Registerkarte „Ressourcen“ zugegriffen wird, jetzt in der Reihenfolge an, in der die Listen gespeichert wurden. (Bisher wurden die Ressourcen sortiert.) (ID-14117).
- Wenn Sie über die Seite „Rollen finden“ Rollen suchen, die in vielen Organisationen vorkommen, wird jetzt kein Objektgruppenfehler mehr angezeigt. (ID-15303).
- Beim Aufheben von Zuweisungen von Ressourcenkonten zu Benutzern mithilfe der Funktion „Benutzer bearbeiten“ wird das Feld SITUATION im Kontenindex für alle Klassen jetzt ordnungsgemäß aktualisiert. (ID-15310).
- Über Registerkarte „Rollen“ > Rollen finden > Menü „Genehmiger“ können jetzt Benutzer mit der Fähigkeit „Genehmigungsbeauftragter für Regeln“ angezeigt werden. (ID-15373).
- Es wurde ein Problem behoben, durch das Internet Explorer bei URLs mit mehr als 2000 Zeichen fehlschlug. (ID-15801).

## In früheren Versionen behobene Fehler

- Wenn Sie Internet Explorer 6 oder 7 mit Sicherheitsupdate 912812 verwenden, müssen Sie nicht mehr auf ein Multioptionsfeld doppelklicken, um das Feld zu markieren, oder auf ein Element doppelklicken, um dieses zu verschieben. (ID-15824).
- Wenn Sie im ActiveSync-Eingabeformular für `IAPI.cancel` den Wert `true` angeben und damit alle anstehenden Aktualisierungen abrechnen, die für den verarbeiteten Benutzer erkannt wurden, ist die Benutzeransicht nach der Verarbeitung nicht mehr gesperrt. (ID-15912).
- Eine Benutzersuche mit Auswahl der Option für Benutzerorganisationen und anderen Suchoptionen ergibt nun gültige Resultate. (ID-16076).
- Die Liste der Genehmiger auf der Seite „Rollen finden“ ist nun sortiert. (ID-16392).
- Die DatePicker-Komponente funktioniert für alle Zeitzonen ordnungsgemäß. (ID-16618).

## Business Process Editor

- Sie können für manuelle Aktionen bei Zeitüberschreitungen negative Werte (in s) anzeigen und bearbeiten. (ID-9715).
- Die Auswahl von **Attribut in Identity Manager-Repository speichern** bei der Bearbeitung eines MetaView-Attributs funktioniert jetzt ordnungsgemäß. (ID-12396).

## Formulare

- Identity Manager bietet neue LDAP-Beispielformulare zum Erstellen und Aktualisieren von Gruppen für nicht eindeutige Mitgliedernamen. (ID-8831).
- MultiSelect-Komponenten behandeln Elemente mit identischen Beschriftungen (Anzeigenamen) jetzt ordnungsgemäß (ID-10964).
- Der Standardwert für die maximal zulässige Länge einer Textkomponente ist jetzt unbegrenzt (früher betrug die Maximallänge 256 Zeichen) (ID-11995).
- Die Gruppenfelder „NTForm“ und „NDSUserForm“ implementieren die ListObjects-Regel jetzt ordnungsgemäß. (ID-12301).
- Ressourcenassistenten für Host-Adapter verwalten die affinityAdmin-Felder jetzt optimaler und vermeiden so Duplikationen und Nulleinträge. (ID-12024).
- Das LDAP-Formular zum Aktualisieren von Gruppen ignoriert keine Änderungen mehr, wenn die Net-Mitgliedschaft gleich bleibt. (ID-12162).
- Die Methode `listResourceObjects` von `com.waveset.ui.FormUtil` führt definierte Filter jetzt ordnungsgemäß aus. Weitere Informationen zu dieser Methode finden Sie in JavaDocs. (ID-14422).

### Identity Auditor

- Die Richtlinienüberprüfung bei der Benutzererstellung erstellt keine zusätzlichen Aufgabeninstanzen mehr. (ID-10489).

### Identity Manager SPE

- Beim Erstellen eines Ressourcenkontos speichert Identity Manager SPE die Werte von Ressourcenattributen ab, wenn die Ressource heruntergefahren ist. Wenn der betreffende Benutzer das nächste Mal in Identity Manager SPE bearbeitet wird, wird das Konto auf der jeweiligen Ressource erstellt, wenn sie verfügbar ist. (ID-11168).
- Sie können verfolgte Ereignisse jetzt in SPE deaktivieren, indem Sie „Erfassung verfolgter Ereignisse aktivieren“ auf der Seite **Service Provider > Hauptkonfiguration bearbeiten** auswählen. Darüber hinaus können Sie auf der gleichen Seite das Erfassen verfolgter Ereignisdaten für jeden Zeitraum selektiv deaktivieren. Wie bei allen Einstellungen auf dieser Seite auch müssen die geänderten Konfigurationsobjekte erst in das SPE-Hauptverzeichnis exportiert werden, bevor sie wirksam werden. (ID-12033).
- Die SPE-Methode „IDMXContext deleteObjects“ löscht jetzt Objekte ordnungsgemäß aus dem Verzeichnisspeicher. (ID-11251).
- Das Prüf-Teilsystem der Service Provider Edition löst beim Schließen von Containern keinen Nullzeiger-Ausnahmefehler mehr aus. (ID-12845).
- IDMXUserViewer löste früher einen Nullzeiger-Ausnahmefehler aus, wenn ein zu den in einer Ansicht angegebenen Eigenschaften zugehöriges Formular keine Ziele enthielt oder die den Ansichtsbehandlungsmethoden (create/checkin/checkout/refresh) übergebene Optionszuordnung null war. (ID-12861).
- Über LDAP gelöschte Attribute werden jetzt propagiert, sobald eine ausgefallene Ressource wieder zur Verfügung steht. (ID-15471).

### Anmelden

- Das Aufrufen einer benutzerdefinierten Aufgabe während der Anmeldung verlangsamt die Anmeldung nicht mehr übermäßig. (ID-12377).
- Identity Manager protokolliert jetzt fehlgeschlagene Administrator-Anmeldeversuche ordnungsgemäß für Benutzer, die keine Fähigkeiten, Organisationen oder Fähigkeiten/Organisationen besitzen. (ID-12497).

## Passwortsynchronisation

- Die Anwendung zum Konfigurieren der Passwortsynchronisation (Configure.exe) kürzt JMS-Eigenschaften beim Lesen vom Repository nicht mehr am Gleichheitszeichen (=). (ID-12658).
- Die Bibliothek `passwordsync.dll` gibt bei Verbindungsfehlern jetzt die richtige Fehlermeldung aus. Diese Änderung beseitigt auch eventuell von Behandlungsroutinen verursachte Speicherlecks nach dem Fehlschlagen von Verbindungen. (ID-15451).
- Passwörter mit Zeichen, die außerhalb des 7-Bit-ASCII-Bereichs liegen, werden vor der Verschlüsselung jetzt richtig in UTF-8 codiert. (ID-15829).

## Abstimmung

- Abstimmungen werden nicht mehr gestoppt, wenn Ressourcen doppelte Benutzer haben. (ID-14949).
- Um unnötige Abstimmungsfehler zu vermeiden, werden einige nicht eindeutige Kontoübereinstimmungen während einer Abstimmung nun als bevorzugte Übereinstimmung behandelt. (ID-14965).
- Abstimmungen werden nicht mehr gestoppt, wenn alle Ressourceninformationen durch eine Benutzernormalisierung von einem Benutzer entfernt werden. (ID-15028).

## Berichte

- Die Abfrage nach inaktiven Windows 2000 / Active Directory-Konten (eine Aufgabe in der oberen Menüleiste „Risikoanalyse“) wird jetzt erfolgreich abgeschlossen. (ID-11148).
- Sie können den Ressourcenbenutzerbericht jetzt mit mehreren Benutzern verwenden. (ID-11420).
- Wenn ein delegierter Administrator einen Benutzerbericht ausführt, werden Benutzer, die aufgrund einer UserMembersRule-Regel Mitglieder einer Organisation sind, jetzt einbezogen. (ID-11871).
- Bei Auswahl eines Ressourcennamens für die Y-Achse eines Einsatzberichts wird dieser Wert jetzt in der Abfrage verwendet. (ID-12035).
- Der Gültigkeitsbereich der folgenden Berichtstypen wird standardmäßig auf die vom angemeldeten Administrator kontrollierten Organisationen abgestimmt, es sei denn, es wurden explizit eine oder mehrere Organisationen ausgewählt, für die der betreffende Bericht gelten soll: Zur Unterstützung dieser Funktion wurde die Komponente „Organisationsumfang“ von einer Select- in eine MultiSelect-Komponente umgewandelt. (ID-12116).

## In früheren Versionen behobene Fehler

- Identity Manager protokolliert jetzt Änderungen von LDAP-Gruppenmitgliedschaften ordnungsgemäß. (Es sind jetzt sowohl alte als auch neue Werte enthalten.) (ID-12163).
- Im UTF-8-Zeichensatz und mit Multibyte-Text codierte CSV-Berichte können nun für die Anzeige in Anwendungen angepasst werden, die keine UTF-8-Kodierung unterstützen, z. B. Microsoft Excel. (ID-13574, 15407).
- Bei per E-Mail versendeten PDF-Berichten werden nun die Einstellungen für Schriftart und Schriftarteinbettung, die auf einer beliebigen Ebene festgelegt wurden, richtig beachtet. (ID-15328).
- Die HTML-Tags `<b></b>` werden jetzt aus den folgenden PDF-Berichten entfernt: (ID-15408).
  - Alle Admin-Rollen
  - Alle Administratoren
  - Alle Rollen
- Zur Angabe eines Werts für das X-Achsenattribut sind nun Formulare für Einsatzberichte erforderlich. (ID-15777).

## Repository

- Das Identity Manager-Repository führt jetzt die Oracle-Abwicklung für die BLOB-Spalten aus. Die Beispielskripten für Oracle definieren jetzt die Spalte xml als Datentyp BLOB (statt als LONG VARCHAR). Bei neuen Installationen werden alle Tabellen mit BLOB-xml-Spalten erstellt. Während einer Aufrüstung besitzen nur neue Tabellen eine BLOB-xml-Spalten. Die übrigen Tabellen können jedoch in BLOBs konvertiert werden, indem die angemerkten Änderungen in einem Aufrüstungsskript ausgeführt werden. (Bei großen Deployments kann dieser Aufrüstungsprozess einige Stunden dauern). Sie sollten auf den neuesten Oracle JDBC-Treiber aufrüsten, um mit BLOBs eine optimale Leistung zu erhalten. (ID-11999).
- Das Repository von Identity Manager wurde dahin gehend geändert, dass für Microsoft SQL Server 2000 spezifische Deadlock-Fehler verhindert werden. Das Repository verwendet jetzt anstatt des Namens die ID von LAST\_MOD\_ITEM, wenn der zuletzt geänderte Wert eines Typs ausgewählt wird. (ID-12297).
- Bei langsamen Oracle-Datenbanksystemen kann es nicht mehr vorkommen, dass angehaltene Aufgaben auf mehreren Schemata gleichzeitig ausgeführt werden. (ID-15372).
- Durch die Entfernung einer Rolle von einem Benutzer in einer ähnlichen Gruppe von Benutzern werden die Repository-Einträge anderer Benutzer nicht mehr beeinträchtigt. Zudem wird dadurch auch nicht mehr verhindert, diese Benutzer beim Suchen nach einer Rolle zu lokalisieren. (ID-15584).

## Ressourcen

### Gateway

- Gateway-Abstürze ereignen sich nicht mehr, wenn die Identity Manager-APIs direkt ohne den Zugriff auf die Identity Manager-Oberfläche verwendet werden. (ID-12481).

### Allgemein

- In Passwörtern können jetzt einfache Anführungszeichen verwendet werden. (ID-10043).
- Ressourcenassistenten für Host-Adapter verwalten die affinityAdmin-Felder jetzt optimaler und vermeiden so Duplikationen und Nulleinträge. (ID-12024).
- Active Sync-Prozesse, die auf einem Websphere-Cluster mit dem Starttyp „Automatisch mit Failover“ laufen, hängen sich nicht mehr auf. (ID-12540).
- Für einige Ressourcenadapter werden nun Ausschlussregeln angewendet, bevor Benutzer im Rahmen der Abstimmung abgerufen werden. Dadurch können bestimmte Benutzer ausgeschlossen werden und es kann verhindert werden, dass Fehler von der Ressource erzeugt werden. Darüber hinaus kann die Leistung für eine große Anzahl von Benutzern verbessert werden. (ID-14436).
- Identity Manager beachtet nun für eine Ressource die Kombinationseinstellung deny, ignore von unterstützten Funktionen. Bei Auswahl von **ignore** wird die Aktion nicht ausgeführt, sie wird jedoch in einigen Fällen u. U. in Form einer Meldung auf der GUI angezeigt. (ID-14948).
- Wenn in der Systemkonfiguration gemeinsame Ressourcen für den Gebrauch bei der Anmeldung festgelegt wurden und die Anmeldung einer gemeinsamen Ressource fehlschlägt, schlagen Anmeldungen nicht mehr fehl, solange sich im Stapel des Anmeldemoduls eine andere Ressource befindet, bei der es sich nicht um eine gemeinsame Ressource handelt und für die andere Authentifizierungseigenschaften benötigt werden als für die vorherigen Anmeldemodul-Ressourcen. (ID-15047).
- Active Sync wird nicht mehr weiter ausgeführt, wenn „Konten ohne Übereinstimmung erstellen“ auf „true“ eingestellt ist und die zulässige Fehleranzahl überschritten wird. (ID-15662).

### Verzeichnisse

- Der Active Directory-Ressourcenadapter löst bei Angabe eines ungültigen Verschlüsselungstyps jetzt einen Ausnahmefehler aus. Gültige Werte sind nichts (leer), „keiner“, „kerberos“ und „ssl“. (ID-9011).
- Identity Manager fasst jetzt LDAP-Verbindungen in einem Pool zusammen. (ID-10219).
- Die Verwaltung von „Nicht-im-Büro“-Attributen eines Active Directory-Benutzers (Exchange) mit aktivierter E-Mail schlägt nicht mehr fehl, wenn `msExchHideFromAddressLists` auf „true“ gesetzt ist. Darüber hinaus wurde der Active Directory-Beispielbenutzer aktualisiert, damit Identity Manager keine „Nicht-im-Büro“-Attribute anzeigt, wenn `msExchHideFromAddressLists` aktiviert ist. (ID-12231).
- Die Active Sync-Verarbeitung von LDAP-Änderungsprotokollen behandelt jetzt MODIFY-Änderungstypen ohne Werte. (ID-12298).
- Verbindungen werden beim Abfragen von Ressourcenobjekten nun vom `ADSIResourceAdapter` geschlossen. (ID-15098).
- Identity Manager liest keine Kontoattribute mehr, die ausschließlich für den Schreibzugriff vorgesehen sind, von einem LDAP-Verzeichnis oder Active Directory (ID-15838).

### Mainframe

- Beim RACF-Adapter ruft eine Änderung in DFLTGRP jetzt ein Hinzufügen (falls erforderlich) von DFLTGRP zu den GROUPS hervor, um zu gewährleisten, dass DFLTGRP als neue Standardgruppe eingestellt werden kann. (ID-9987).
- Verbindungen mit dem Mainframe-Ressourcenadapter werden jetzt ordnungsgemäß in Pools zusammengefasst und verursachen kein Aufhängen von Mainframe-Operationen mehr. (ID-12388).
- Die zum Erstellen eines Natural-Ressourcenadapters verwendete Terminalemulation ermöglicht Benutzernamen mit 8 Zeichen Länge und ohne Tabulatorzeichen jetzt die Auswahl des Attributs „Copy Links“. (ID-12503).
- Der standardmäßige RACF-Mechanismus `AttrParse` zum Angeben von Benutzern wurde erweitert und kann nun eine große Anzahl von „CLASS AUTHORIZATIONS“ und Vorlagenbenutzern mit Gruppeneinträgen wie „GROUP SYS1 USER CONNECTION NOT INDICATED“ bearbeiten. (ID-15021).
- Wenn das Ressourcenaffinitätskonto in RACF ungenügende Berechtigungen zum Anzeigen eines Benutzers hat, zeigt Identity Manager eine entsprechende Fehlermeldung an. (ID-15331).
- Zum Löschen von RACF-Konten fragt das System jetzt mithilfe einer Suchmaske die Dataset-Profile des Benutzers ab, sucht das Dataset sequenziell über diese Profile ab und löscht die einzelnen Datasets (anstatt sie mit `DELDSD.**` gemeinsam zu löschen). (ID-15413).

## In früheren Versionen behobene Fehler

- Durch das Löschen eines RACF-Attributs in einem Formular wurde das Attribut für den Benutzer in Identity Manager beim Übermitteln des Formulars nicht gelöscht (nichts geschah). Jetzt wird das Attribut in Identity Manager gelöscht. (ID-15971).
- Der Top Secret-Ressourcenadapter ist nun in der Lage, `ASUSPEND`, `PSUSPEND`, `VSUSPEND` und `XSUSPEND` bei der Aktivierung und Deaktivierung von Benutzern richtig zu bearbeiten. (ID-16295)
- Es wurde ein Problem im Top Secret-Adapter behoben, durch das unvollständige Benutzerattribute geladen wurden. (ID-16334).

## Oracle und Oracle ERP

- Während einer Sitzung mit dem Oracle-Ressourcenadapter werden alle Oracle-Zeiger auch beim Auftreten von Ausnahmefehlern geschlossen. (ID-10357).
- Bei Oracle- und Oracle ERP-Ressourcenadaptern, die mit Oracle RAC-Umgebungen Verbindungen mithilfe eines Thin-Treibers herstellen, sollte das folgende Format verwendet werden: (ID-10875).  

```
jdbc:oracle:thin:@(DESCRIPTION=(LOAD_BALANCE=on)(ADDRESS=(PROTOCOL=TCP)(HOST=host01)(PORT=1521))(ADDRESS=(PROTOCOL=TCP)(HOST=host02)(PORT=1521))(ADDRESS=(PROTOCOL=TCP)(HOST=host03)(PORT=1521))(CONNECT_DATA=(SERVICE_NAME=PROD)))
```
- Oracle ERP kann optional Konten, die vom Kontoiterator und den `listObjects`-Schnittstellen zurückgegeben werden, durch Setzen des Ressourcenattributs `activeAccountsOnly` auf `TRUE` beschränken. Der Standardwert ist `FALSE`. Ist er auf `FALSE` gesetzt, werden alle Konten der betreffenden Ressource zurückgegeben. Ist er `TRUE`, werden nur Konten zurückgegeben, bei denen `SYSDATE` (der aktuelle Zeitpunkt) zwischen `START_DATE` und `END_DATE` liegt. (ID-12303).
- Die Oracle ERP-Adapter wurden entsprechend aktualisiert, damit `PreparedStatements` konsistenter geschlossen werden und somit die Anzahl geöffneter Zeiger verringert wird. (ID-12564).

## SAP

- Der SAP-Adapter behandelt jetzt Fälle, in denen von der Methode `listAllObjects()` duplizierte Aktivitätsgruppen zurückgegeben werden. (ID-7776).
- Der SAP-Adapter kann jetzt temporäre generierte Passwörter im `WavesetResult`-Objekt zurückzugeben, wenn der Adapter das betreffende Passwort nicht als nicht abgelaufen setzen konnte. Dies tritt unter den folgenden Bedingungen auf:

## In früheren Versionen behobene Fehler

- es wird die Änderung eines Administratorpassworts angefordert und `expirePassword = false`
- das gewünschte Passwort entspricht nicht den SAP-Passwortrichtlinien

Dieser Fehler tritt höchstwahrscheinlich dann auf, wenn sich das gewünschte Passwort bereits in der SAP-Passwortabfolge befindet.

Das Ressourcenattribut `Bei Fehler temporäre SAP-Passwörter zurückgeben` wurde erstellt, um diese Fähigkeiten zu aktivieren, funktioniert jedoch zurzeit noch nicht. (ID-12185).

- Der SAP-Adapter überprüft das gewünschte Passwort eines Benutzers jetzt sicherer gegen sein aktuelles Passwort, wenn das Administratorpasswort geändert werden soll und das Flag `expirePassword` auf „false“ gesetzt ist. Dadurch wird eine Fehlerbedingung verhindert, wenn das gewünschte Passwort und das aktuelle Passwort des Benutzers gleich sind. (ID-12447).
- Durch das Schreiben von SAP-Aktivitätsgruppen und -Profilen in eine CUA-Umgebung (CUA, Central User Administration) wird eine neue Tabellenzeile nicht mehr in zwei Zeilen aufgeteilt, wenn die Daten durch ein Semikolon getrennt sind. (ID-14371).

## UNIX

- Die UNIX-Adapters bieten eine grundlegende `sudo`-Initialisierung und -Zurücksetzung. Wenn jedoch eine Ressourcenaktion definiert wird und im Skript einen Befehl enthält, für den eine `sudo`-Autorisierung erforderlich ist, müssen Sie den Befehl `sudo` zusammen mit dem UNIX-Befehl eingeben. (So müssen Sie beispielsweise `sudo useradd` statt lediglich `useradd` eingeben.) Befehle, die `sudo` erfordern, müssen auf der nativen Ressource angemeldet werden. Sie können diese Befehle mithilfe von `visudo` registrieren. (ID-10206).
- Die Red Hat Linux- und SuSE Linux-Adapters füllen bei Massenprozessen wie z.B. „Aus Ressource importieren“ und „In Datei exportieren“ jetzt die Primärgruppe, Sekundärgruppe sowie die letzten Anmeldefelder. (ID-11627).  
Wenn die Schema-Zuordnung anweist, dass das letzte Anmeldefeld verfolgt werden soll, kann sich der betreffende Massenprozess beträchtlich verlangsamen, weil der Adapter für jeden Benutzer einzeln die Informationen der letzten Anmeldung abrufen muss.
- Sie können jetzt das Attribut `time_last_login_resource` auf Solaris-, HP-UX- und Linux-Adaptoren zu Attributnamen, die nicht dem Standardwert (letzte Anmeldezeit) entsprechen, zuordnen. (ID-11692).
- Wenn Sie für eine Solaris NIS-Serverressource ein Ressourcenobjekt erstellen, unter „Benutzer“ mehrere Konten auswählen und dann auf Speichern klicken, werden der Gruppendatei im NIS-Passwortquellverzeichnis des verwalteten NIS-Server nun alle Konten hinzugefügt. Dieser Vorgang konnte zuvor nur bei der Auswahl eines Kontos richtig ausgeführt werden. (ID-15085).

## In früheren Versionen behobene Fehler

- Identity Manager fügt für Solaris NIS nicht mehr das `netid`-Ziel hinzu, das nicht benötigt wurde und in den Protokollen Fehlermeldungen verursacht hat. (ID-15503).
- Identity Manager verhindert für Solaris NIS nicht mehr den Gebrauch des Befehls `sudo`, wenn das Verzeichnis, in dem sich die Solaris NIS-Vorlagendateien `passwd`, `shadow` und `group` befinden, vom Administrator schreibgeschützt wurde. (ID-15505).
- Für Solaris NIS werden keine Konten mehr partiell erstellt, wenn die primäre Standardgruppe entweder vollständig fehlt oder deren Name in der Gruppendatei nicht gefunden werden kann. (ID-15509).
- Das Generieren von IDs für Solaris NIS-Benutzer bzw. -Gruppen schlug fehl, wenn in der Ausgangsumgebung keine Benutzer oder Gruppen vorhanden waren. Dieser Fehler wurde korrigiert. Die Vorlagendateien `passwd` und `group` befinden sich jetzt nicht mehr im Verzeichnis `/etc`. (ID-15510).
- Wenn für Solaris NIS zwei Konten nacheinander erstellt werden — wobei für das erste Konto eine Shell angegeben ist, aber für das zweite nicht (entweder ist es in der Datei `defadduser` nicht definiert oder die Datei `defadduser` ist nicht vorhanden) —, wird das zweite Konto nicht mehr mit der Shell des ersten erstellt. (ID-15511).
- Bei Solaris NIS wird nun die Datei `/usr/sadm/defadduser` als optionale Quelle für Standardwerte für neu erstellte Konten verwendet. In vorherigen Versionen von Identity Manager griff das System zum Festlegen der Standard-Primärgruppe neuer Identity Manager-Benutzer auf ein falsches Element dieser Datei zu. Jetzt wird die Standard-Primärgruppe richtig durch das Element `defgname` gesetzt. Dieser Standardwert für die Primärgruppe wird vom Ressourcenattribut **Standardmäßige Primärgruppe** überschrieben, das seinerseits von dem Kontenattribut mit demselben Namen überschrieben wird. (ID-15512).
- Identity Manager speichert die verschlüsselten Solaris NIS- und HP-UX NIS-Passwörter bei der Aktualisierung eines Kontos nicht mehr in den NIS-Vorlagendateien `passwd` und `shadow`. Der Platzhalterwert „x“ wird nun in der Datei `passwd` gespeichert. (ID-15593).
- Ein Problem, durch das es möglich war, auf Solaris NIS-Ressourcen Gruppen mit dem Namen oder der ID einer bereits vorhandenen Gruppe zu erstellen, wurde behoben. (ID-15755).
- Beim Löschen eines Benutzers von einer Solaris-Ressource liefert Identity Manager nicht mehr ein fälschlicherweise positives Ergebnis, wenn der Benutzer gerade bei der Ressource angemeldet ist und der Löschvorgang misslingt. (ID-15761).

### Andere

- Der SecurID-UNIX-Adapter verarbeitet Benutzerknotenattribute von Identity System bei Änderung der Standardnamen ordnungsgemäß. (ID-10521).
- Wenn Sie mit einer Active Sync-Ressource für PeopleSoft-Komponenten arbeiten, die die Komponentenschnittstelle LH\_AUDIT\_RANGE\_COMP\_INTF verwenden, müssen Sie an der Ressource Änderungen vornehmen, wenn Sie die Komponentenschnittstelle LH\_AUDIT\_RANGE\_COMP\_INTF weiterhin nutzen möchten. (ID-11226).

Vergewissern Sie sich, dass Ihre Ressource ein Ressourcenattribut `auditLegacyGetUpdateRows` besitzt und dieses auf „true“ gesetzt ist.

```
<ResourceAttribute name="auditLegacyGetUpdateRows"
  value="true"
  displayName="Use Legacy Get Update Rows"
  type="boolean"
  multi="false"
  facets="activesync" >
</ResourceAttribute>
```

- Sie können jetzt Sun Access Manager Organization-Objekte aus dem Identity Manager-Ressourcenapplet löschen. (Identity Manager löscht anschließend alle untergeordneten Objekte ohne Bestätigung.) (ID-11516).
- Beim Verwalten von SecurID-Benutzern unterstützt Identity Manager jetzt drei Token pro Benutzer. (ID-11723).
- Beim Datenbanktabellenadapter werden Datenbankverbindungen jetzt so schnell wie möglich während der Iteration und des Pollings geschlossen, um zu verhindern, dass nicht verwendete Verbindungen unnötig gehalten werden. (ID-11986).
- Der JMS Listener-Adapter schlägt auf Websphere 6.0 nicht mehr fehl. Durch den Übergang von asynchroner zu synchroner Meldungsverarbeitung funktioniert der JMS Listener jetzt auf J2EE-Servern, die asynchrone JMS-Meldungsverarbeitung innerhalb von Internetanwendungen verhindern. Die Polling-Frequenz muss jetzt für JMS Listener-Ressourcen definiert werden. (ID-12654).
- Die SecurID-Adapter erzwingen die RSA-Voraussetzung, dass das Standard-Anmeldeattribut nur aus englischen Einzelbytezeichen bestehen kann. (ID-13805)
- Passwörter mit Zeichen, die außerhalb des ASCII-7-bit-Bereichs liegen, werden nun vom Gateway richtig eingestellt (Erstellung und Aktualisierung), wenn Identity Manager mit Tivoli Access Manager und Active Directory bereitgestellt wird. (ID-15006).
- Die Ausgabe von Lösch-Skripten, die mit einem Fehler zurückgegeben werden, werden jetzt vom Shell Script-Adapter abgefangen und gemeldet. (ID-15340).
- Der Datenbanktabellenadapter ermöglicht die Angabe des Ressourcenparameters **Rethrow all SQLExceptions**. Wenn diese Option nicht aktiviert ist, werden bei SQL-Anweisungen, die SQLExceptions mit einem Fehlercode 0 erzeugen, diese Ausnahmen abgefangen und unterdrückt. (ID-15390).
- Ein Problem, das bei Verwendung von Active Sync und der PeopleSoft-Ressource Deadlocks verursachte, wurde behoben. (ID-16109).

## Abstimmung

- Durch Setzen einer `ControlledOrganizationRule` in der Admin-Rolle eines Benutzer wird der Start der Reconciler-Dämons nicht mehr verhindert. (ID-12695).

## Repository

- Fehlermeldungen wie `com.waveset.util.InternalError: Länge der Zusammenfassungs-Zeichenfolge (2185) überschreitet die maximale Länge (2048)` treten beim Speichern von Benutzern oder anderen Objekten nicht mehr auf. (ID-12492).

## Rollen

- Rollennamen, die Apostrophe enthalten, werden beim Bearbeiten von Rollen nicht mehr abgeschnitten. (ID-8806).
- Identity Manager behandelt das Hinzufügen bzw. Entfernen von zugewiesenen Gruppen durch Rollenattribute jetzt ordnungsgemäß. (ID-10832).
- Rollen, die in Identity Manager 5.0 erstellt wurden und Unterrollen anderer Rollen waren, enthalten jetzt Verknüpfungen auf ihre übergeordneten Rollen. (ID-11477).
- Bei der Umbenennung einer Ressource referenzieren Rollenattribute jetzt weiter korrekt die jeweilige Ressource. (ID-11689).
- Wenn `waveset.roles` nur eine Rolle enthält, kann diese durch Massenaktionen entfernt werden. (ID-14568).
- Das System aktualisiert unter- und übergeordnete Rollen während einer `SaveAs`-Aktion jetzt ordnungsgemäß. (ID-16010).

## Sicherheit

- Sie können die ausführlichen, in HTML-Kommentaren enthaltenen Debugging-Informationen unterdrücken, indem Sie die Eigenschaft `ui.web.disableStackTraceComments` in der Datei `Waveset.properties` auf „true“ setzen. Wenn Sie von einer früheren Identity Manager-Version aufrüsten, müssen Sie diese Eigenschaft zur Datei `config/Waveset.properties` hinzufügen. Die Eigenschaft wird ignoriert (was dem Setzen der Eigenschaft auf „false“ entspricht), wenn sie sich nicht in der Eigenschaftendatei befindet. (ID-10499)
- Anonyme Benutzer können jetzt auf verschiedene Objekttypen wie Regeln zugreifen, ohne das verworfene Attribut `endUserAccess` im Systemkonfigurationsobjekt setzen zu müssen. (ID-11248).

## In früheren Versionen behobene Fehler

- Zur Konfiguration dieser Version für eine Bereitstellung für eine Clear Trust 5.5.2-Ressource müssen Sie die Datei `ct_admin_api.jar` von der Clear Trust 5.5.2-Installations-CD installieren. Für die SSL-Kommunikation benötigen Sie keine zusätzlichen Bibliotheken. (ID-12449).
- Während der Erstellung von Admin-Rollen behandelt Identity Manager jetzt das Einbeziehen und Ausschließen aller Objekttypen ordnungsgemäß. (ID-12491).
- Administratoren mit den folgenden Fähigkeiten haben jetzt Zugriff auf die Seite „Ressourcen auflisten“: (ID-12647).
  - Ressourcen-Passwort-Administrator
  - Ressourcenpasswortänderungs-Administrator
  - Ressourcenpasswortzurücksetzungs-Administrator
  - Active Sync-Ressourcenadministrator ändern
  - Active Sync-Ressourcenadministrator steuern
  - Abstimmungs-Administrator
  - Abstimmungsanforderungs-Administrator
- Sie können einer Passworthistorie eines Benutzers nun beim Erstellen eines Benutzers Passwörter hinzufügen. (ID-15179).
- Genehmiger, die nicht die Organisation an der Hierarchiespitze kontrollieren, können keine vorher genehmigten bzw. abgelehnten Genehmigungsanforderungen anzeigen. (ID-15271)
- Wenn ein Benutzer, der in Besitz noch ausstehender Arbeitselemente ist, gelöscht wird, stellt Identity Manager nun wie folgt sicher, dass die Arbeitselemente nicht verloren gehen: (ID-15868).
  - Wenn ein ausstehendes Arbeitselement delegiert und der Delegierende nicht gelöscht wurde, wird das ausstehende Arbeitselement an den Delegierenden zurückgegeben; der Delegierende ist dann der neue Inhaber des Arbeitselements.
  - Wenn ein ausstehendes Arbeitselement delegiert und der Delegierende auch gelöscht wurde oder wenn ein ausstehendes Arbeitselement nicht delegiert wurde, schlägt jeder Löschvorgang fehl, bis das ausstehende Arbeitselement des Benutzers entweder aufgelöst oder zu einem anderen Benutzer weitergeleitet wurde.

## Server

- Der Anwendungsserver stürzt bei der Verwendung von Oracle OCI-Treibern mit SSL nicht mehr ab. (ID-7109)
- Bei der Anmeldung im Endbenutzermenü wird kein „Null pointer“-Ausnahmefehler mehr ausgelöst, wenn der Identity Manager-Benutzer eine Rolle auf einer Ressource besitzt, in der dieser Benutzer nicht existiert. (ID-12379).
- Die Sitzung wird jetzt während Erweiterungen und Ableitungen ordnungsgemäß konfiguriert, wenn das Erstellen von Ressourcenkonten in Massenaktionen verarbeitet wird. (ID-16181).
- Unter bestimmten Umständen war es möglich, dass eine geplante Aufgabe für eine bestimmte Startzeit von mehreren Servern verarbeitet wurde. Dies kommt nun nicht mehr vor. (ID-16318).

## SOAP

SPML 1.0-Aufrufe können jetzt durch `debug/callTimer.jsp` überwacht werden. Der Aufruf der obersten Ebene (die Methode `doRequest()` von „`com.waveset.rpc.SpmlHandler`“) ist zur Ermittlung der SOAP/SPML-Leistung äußerst nützlich. Die Zeitdauern der einzelnen SPML-Methoden (z.B. `addRequest`) werden zur Überwachung ebenfalls gemessen. (ID-8463).

## Workflow

- Unter bestimmten Umständen konnte ein abgelaufenes Arbeitselement ohne Fehlermeldung bearbeitet werden. Jetzt wird ein Fehler zurückgegeben, der angibt, dass das Arbeitselement nicht mehr gültig ist. (ID-15439).
- Die Workflow-Variable `WF_ACTION_ERROR` wird jetzt beim Auftreten von Fehlern im Remedy-Ressourcenadapter richtig gesetzt. (ID-16360).
- Für weitergeleitete Genehmigungen können jetzt benutzerspezifische E-Mail-Vorlagen (`emailTemplate`) verwendet werden. Sie müssen die gewünschte Vorlage in den Genehmigungsprozessen nach ID angeben. (ID-16468)

## Weitere behobene Probleme

6496, 8586, 8739, 8958, 8960, 9936, 10235, 10475, 10483, 10832, 11232, 11642, 11767, 11979, 12135, 12203, 12234, 12274, 12368, 12377, 12464, 12483, 12510, 12585, 12611, 12614, 12673, 12967, 13054, 13338, 13434, 13965, 14044, 14178, 14334, 14792, 14874, 14893, 14899, 15036, 15073, 15219, 15474, 16107, 16282, 16389, 16395, 16610, 17346

## **In früheren Versionen behobene Fehler**

# Hinweise zur Installation und Aktualisierung

---

## Installationshinweise

---

- Sie müssen Identity Installation Pack unter HP-UX manuell installieren.
- Zur Ausführung von Identity Manager unter Tomcat 4.1.x müssen Sie die JSSE Jar-Dateien von der Sun-Website <http://java.sun.com/products/jsse/index-103.html> herunterladen und diese in das Verzeichnis `idm\WEB-INF\lib` kopieren.
- Zur Ausführung von Sun Identity Manager Gateway unter Windows NT muss das Zusatzmodul Microsoft Active Directory Client installiert sein. Den DSClient können Sie von <http://support.microsoft.com/default.aspx?scid=kb;en-us;Q288358> herunterladen.
- Die folgenden JAR-Dateien wurden aufgrund von Problemen mit der Lizenzierung entfernt. (ID-9338) Diese JAR-Dateien sind für folgenden Ressourcenadapter erforderlich. Jedes Element enthält unten Informationen zum Abrufen der JAR-Dateien vom Hersteller.

Adapter: OS400ResourceAdapter

URL: <http://jt400.sourceforge.net>

Projekt: JTOpen

JAR: `jt400.jar`

Version: 2.03

Adapter: ONTDirectorySmartAdapter

URL: <http://my.opennetwork.com>

Projekt: Directory Smart

JARs: `dsclass.jar`, `DSUtils.jar`

Version: entf.

# Hinweise zur Aktualisierung

---

Vor dem Aufrüsten von Identity Manager sollten Sie in der Installationsanleitung für Ihren Anwendungsserver nach anwendungsserverspezifischen Anweisungen suchen. Dieser Abschnitt enthält eine Zusammenfassung der Aufgaben, die Sie zum Aufrüsten von Identity Manager von Version 6.0 auf Version 6.0 SP4 ausführen müssen. Weitere Informationen finden Sie im Handbuch *Identity Manager 6.0 Upgrade*.

Sie können von den folgenden früheren Versionen auf Identity Installation Pack 2005Q4M3 SP4 aufrüsten:

- Identity Manager 6.0 (alle Service Pack-Ebenen)
- Identity Auditor 1.7 (alle Service Pack-Ebenen)

**Hinweis** Wenn für Ihre aktuelle Identity Manager -Installation viele individuelle Anpassungen erforderlich sind, sollten Sie sich mit Sun Professional Services in Verbindung setzen, die Sie bei der Planung und Ausführung der Aufrüstung unterstützen.

Verwenden Sie zum Aufrüsten von Identity Manager die folgenden Informationen und Anleitungen:

**Hinweis** In einigen Umgebungen (wie z.B. HP-UX) kann es sein, dass Sie die alternative (manuelle) Aktualisierung durchführen müssen. Wenn dies der Fall ist, müssen Sie zum Abschnitt *Manuelle Aufrüstung von Identity Manager* gehen.

**Hinweis** Identity Manager 6.0 verwendet ein Schema, das neue Tabellen für Aufgaben, Gruppen und Organisationen sowie die syslog-Tabelle enthält. Sie müssen diese neuen Tabellen erstellen und ihre vorhandenen Daten in diese Tabellen kopieren. Weitere Informationen finden Sie in *Schritt 2: Aufrüsten des Repository-Datenbankschemas* im Abschnitt *Erweiterungen und Korrekturen der Dokumentation* dieses Dokuments.

**Hinweis** Wenn Sie die E-Mail-Vorlage „Zugriffsprüfungshinweis“ in Identity Manager Version 6.0 bearbeitet haben, müssen Sie diese vor der Aufrüstung von Identity Manager entweder gesondert abspeichern oder die Vorlage nach der Aufrüstung noch einmal neu bearbeiten. (Die Aufrüstung überschreibt die Vorlage mit den Standardwerten.) (ID-13216).

# Schritt 1: Aktualisierung der Identity Manager-Software

Verwenden Sie zum Aufrüsten von Identity Manager die folgenden Informationen und Anleitungen:

### Hinweise:

- In einigen Umgebungen (wie z.B. HP-UX) kann es sein, dass Sie die alternative (manuelle) Aktualisierung durchführen müssen. Wenn dies der Fall ist, müssen Sie zum Abschnitt *Manuelle Aufrüstung von Identity Manager* gehen.
- In UNIX-Umgebungen müssen Sie sich vergewissern, dass das Verzeichnis `/var/opt/sun/install` existiert und nicht schreibgeschützt ist.
- Während der Aktualisierung werden Sie gefragt, in welchem Verzeichnis Ihr Anwendungsserver installiert ist
- Alle vorher installierten Hotfixes werden im Verzeichnis `$WSHOME/patches/HotfixName` archiviert:
- Die in den folgenden Schritten angegebenen Befehle gelten für eine Windows-Installation und einen Tomcat-Anwendungsserver. Je nach Umgebung können sich die von Ihnen zu verwendenden Befehle von den hier angegebenen unterscheiden.

So aktualisieren Sie Identity Manager:

1. Fahren Sie den Anwendungsserver herunter.
2. Wenn in Ihrem System das Sun Identity Manager Gateway auf dem Identity Manager-Server ausgeführt wird, müssen Sie den Gateway-Dienst mit dem folgenden Befehl herunterfahren:  

```
gateway -k
```
3. Führen Sie den Befehl `install` aus, um den Installationsvorgang zu beginnen. Identity Manager zeigt ein Begrüßungsfenster an.
4. Klicken Sie auf **Weiter**. Identity Manager zeigt das Fenster „Select Installation Directory“ an. Klicken Sie auf „Upgrade“ und dann auf „Next“.
5. Geben Sie das Identity Manager-Installationsverzeichnis ein (oder klicken Sie auf **Browse**, um es zu suchen), und klicken Sie dann auf **Next**.

## Hinweise zur Aktualisierung

6. Zum Starten der Aktualisierung klicken Sie auf **Weiter**.  
Identity Manager zeigt das Fenster „Installation Summary“ an.

**Hinweis** Weitere Informationen zur Installation finden Sie, wenn Sie auf **Details** klicken. Je nachdem, wieviele Informationen während des Installationsvorganges erfasst wurden, kann es sein, dass nicht alle hier aufgeführten Meldungen angezeigt werden. Weitere Informationen finden Sie in der Protokolldatei (unter „Details“). Klicken Sie auf **Close**, um das Installationsprogramm zu beenden, wenn die Installation abgeschlossen ist.

7. Entfernen Sie alle compilierten Identity Manager-Dateien aus dem Arbeitsverzeichnis des Anwendungsservers.
8. Verlagern Sie eventuell vorhandene Hotfix-Klassendateien aus dem Verzeichnis `WEB-INF/classes` in das Verzeichnis `patches\HotfixName`, falls das der Aufrüstungsvorgang nicht bereits erledigt hat.

## Schritt 2: Aktualisierung des Sun Identity Manager Gateway

Wenn das Sun Identity Manager Gateway auf einem anderen, über Netzwerk zugänglichen System ausgeführt wird, müssen Sie es wie folgt aufrüsten.

1. Melden Sie sich bei dem Windows 2000-System an, auf dem das Sun Identity Manager Gateway installiert ist.
2. Wechseln Sie in das Verzeichnis, in dem das Gateway installiert ist.
3. Fahren Sie den Gateway-Dienst durch Eingeben des folgenden Befehls herunter:  
`gateway -k`
4. Bei Windows 2000-Systemen (oder neueren Betriebssystemversionen) müssen Sie alle Instanzen des MMC-Plugins „Dienste“ beenden.
5. Löschen Sie die vorhandenen Gateway-Dateien.
6. Wenn Sie das neu aufrüstete Gateway auf einem System installieren, auf dem nicht der Identity Manager-Server läuft müssen Sie die Datei `gateway.zip` aus dem Verzeichnis, in dem das Installationsabbild entpackt wurde, kopieren.
7. Entpacken Sie die Datei `gateway.zip` in das Verzeichnis, in dem das Gateway installiert war.
8. Geben Sie den folgenden Befehl ein, um den Gateway-Dienst zu starten:  
`gateway -s`

Sie können das Gateway durch Ausführen der folgenden Schritte starten oder stoppen:

1. Öffnen Sie die Windows-Systemsteuerung.
2. Öffnen Sie „Dienste“. (In Windows 2000 befindet sich die Option „Dienste“ unter „Verwaltung“.)
3. Wählen Sie Sun Identity Manager Gateway.
4. Klicken Sie auf **Starten** oder **Stoppen**.

## Manuelle Aufrüstung von Identity Manager

---

In einigen Umgebungen kann es sein, dass Sie die Aufrüstung manuell durchführen müssen und dafür nicht das Installations- und Aufrüstungsprogramm von Identity Manager verwenden können.

### Hinweise:

- Vergewissern Sie sich, dass die Umgebungsvariable `JAVA_HOME` gesetzt ist.
- Stellen Sie sicher, dass sich das Verzeichnis `bin` im Verzeichnis `JAVA_HOME` im Pfad befindet.
- Alle vorher installierten Hotfixes werden im Verzeichnis `%WSHOME%/patches/HotfixName` archiviert:
- Stellen Sie vor der Aufrüstung das interne Konfiguratorkonto wieder her, sodass es „Configurator“ und Importfunktionalität besitzt. Darüber hinaus muss das Passwort für dieses Konto „configurator“ lauten. Setzen Sie nach der Aufrüstung das Konfiguratorkonto auf den Zustand zurück, den es vor der Aufrüstung besaß. Falls erforderlich, müssen Sie dieses Konto umbenennen und das Passwort ändern, bevor Sie es wieder in Ihrer Produktionsumgebung nutzen können.

Folgen Sie diesen Schritten, um Identity Manager manuell aufzurüsten:

1. Fahren Sie den Anwendungsserver und das Sun Identity Manager Gateway herunter.
2. Geben Sie die folgende Befehlsfolge ein:

#### Unterstützte Windows-Plattformen:

- a. Setzen der Umgebungsvariablen:

```
set SPPATH=Pfad zu den Service Pack-Dateien
set WSHOME=Pfad zum Identity Manager-Installationsverzeichnis
ODER -Staging-Verzeichnis
set TEMP=Pfad zum temporären Verzeichnis
```

## Manuelle Aufrüstung von Identity Manager

### b. Ausführen der Vorverarbeitung:

```
mkdir %TEMP%
cd /d %TEMP%
jar -xvf %SPPATH%\IDPAK2005Q4M3_SP4.jar \
WEB-INF\lib\idm.jar \ WEB-INF\lib\idmcommon.jar \
WEB-INF\lib\idmformui.jar
set TEMPLIBPTH=%TEMP%\WEB-INF\lib
set CLASSPATH=%TEMPLIBPTH%\idm.jar;\
%TEMPLIBPTH%\idmcommon.jar;%TEMPLIBPTH%\idmformui.jar
java -classpath %CLASSPATH% -Dwaveset.home=%WSHOME%
com.waveset.install.UpgradePreProcess
```

### c. Software-Installation:

```
cd %WSHOME%
jar -xvf %SPPATH%\IDM.jar
```

### d. Ausführen der Nachverarbeitung:

```
java -classpath %CLASSPATH% -Dwaveset.home=%WSHOME%
com.waveset.install.UpgradePostProcess
```

## Unterstützte UNIX-Plattformen:

### a. Setzen der Umgebungsvariablen:

```
export SPPATH=Pfad zu den entpackten Service Pack-Dateien
export WSHOME=Pfad zum Identity Manager-Installationsverzeichnis
ODER -Staging-Verzeichnis
export TEMP=Pfad zum temporären Verzeichnis
```

### b. Ausführen der Vorverarbeitung:

```
mkdir $TEMP
cd $TEMP
jar -xvf $SPPATH/IDPAK2005Q4M3_SP4.jar \
WEB-INF/lib/idm.jar WEB-INF/lib/idmcommon.jar \
WEB-INF/lib/idmformui.jar
CLASSPATH=$TEMP/WEB-INF/lib/idm.jar:\
$TEMP/WEB-INF/lib/idmcommon.jar:\
$TEMP/WEB-INF/lib/idmformui.jar
java -classpath $CLASSPATH -Dwaveset.home=$WSHOME \
com.waveset.install.UpgradePreProcess
```

### c. Software-Installation:

```
cd $WSHOME
jar -xvf $SPPATH/IDM.jar
```

### d. Ausführen der Nachverarbeitung:

```
java -classpath $CLASSPATH -Dwaveset.home=$WSHOME
com.waveset.install.UpgradePostProcess
```

## Manuelle Aufrüstung von Identity Manager

3. Wechseln Sie in das Verzeichnis `$WSHOME/bin/solaris` bzw. `$WSHOME/bin/linux` und setzen Sie dann für die Dateien im Verzeichnis die Zugriffsrechte so, dass sie ausführbar sind.
4. Bei der Installation in ein Staging-Verzeichnis müssen Sie für das Deployment in Ihrem Anwendungsserver eine `.war`-Datei erstellen.

**Hinweis** Spezifische Anweisungen für verschiedene Anwendungsserver finden Sie in den entsprechenden Abschnitten unter *Sun Java™ System Identity Manager Installation*.

5. Entfernen Sie die Identity Manager-Dateien aus dem Arbeitsverzeichnis des Anwendungsservers.
6. Verlagern Sie eventuell vorhandene Hotfix-Klassendateien aus dem Verzeichnis `WEB-INF/classes` in das Verzeichnis `patches\HotfixName`, falls das der Aufrüstungsvorgang nicht bereits erledigt hat.
7. Starten Sie den Anwendungsserver.
8. Aktualisieren Sie die Identity Manager-Datenbank Ausführliche Anweisungen finden Sie im obigen Abschnitt *Schritt 2: Aktualisierung des Sun Identity Manager Gateway*.
9. Rüsten Sie das Sun Identity Manager Gateway auf und starten Sie es dann neu Ausführliche Anweisungen finden Sie im obigen Abschnitt *Schritt 2: Aktualisierung des Sun Identity Manager Gateway*.

## **Manuelle Aufrüstung von Identity Manager**

# Erweiterungen und Korrekturen der Dokumentation

---

## Informationen zur Softwaredokumentation von Identity System

---

Die Identity System-Softwaredokumentation finden Sie auf der Identity Install Pack-CD in Form mehrerer (.pdf)-Dateien, die Sie in Acrobat Reader öffnen können. Zu dieser Version gibt es die folgenden Dokumentationen.

### Identity System-Software

#### *Install Pack Installation*

(Identity\_Install\_Pack\_Installation\_2005Q4M3.pdf) – Beschreibt die Installation und Aktualisierung der Identity System-Software.

### Identity Manager

- *Identity Manager Administration* (IDM\_Administration\_2005Q4M3.pdf) - Enthält eine Einführung in die Administratorbenutzeroberfläche und Benutzeroberfläche von Identity Manager.
- *Identity Manager Upgrade* (IDM\_Upgrade\_2005Q4M3.pdf) – Enthält Informationen zur Planung und Ausführung von Aufrüstungen.

**Hinweis** Für *Identity Manager Technical Deployment* und *Identity Manager Technical Reference* wurde die Dokumentation in dieser Version folgendermaßen neu organisiert:

- *Identity Manager Technical Deployment Overview* (IDM\_Deployment\_Overview\_2005Q4M3.pdf) – Konzeptüberblick über das Identity Manager-Produkt (einschließlich Objektarchitekturen) mit einer Einführung in grundlegende Produktkomponenten.
- *Identity Manager Workflows, Forms, and Views* (IDM\_Workflows\_Forms\_Views\_2005Q4M3.pdf) – Referenzmaterialien und Informationen zur Vorgehensweise, die beschreiben, wie die Identity Manager Workflows, Formulare und Ansichten verwendet werden. Hierzu gehören Informationen zu den Tools zum Anpassen dieser Objekte.
- *Identity Manager Deployment Tools* (IDM\_Deployment\_Tools\_2005Q4M3.pdf) – Referenzmaterialien und Informationen zur Vorgehensweise, die beschreiben, wie verschiedene Identity Manager-Bereitstellungstools verwendet werden. Hierzu gehören Regeln und Regelbibliotheken, allgemeine Aufgaben und Prozesse, Wörterbuchunterstützung und die SOAP-basierte Webdienstoberfläche vom Identity Manager-Server.

## Navigation in der Onlinedokumentation

- **Identity Manager Resources Reference** ([IDM\\_Resources\\_Reference\\_2005Q4M3.pdf](#)) – Referenzmaterialien und Informationen zur Vorgehensweise, die beschreiben, wie Kontoinformationen aus einer Ressource geladen und in Sun Java™ System Identity Manager synchronisiert werden. Zusätzliche Adapter sind in der Datei [ResourcesRef\\_Addendum\\_2005Q4M3SP1.pdf](#) dokumentiert.
- **Identity Manager Audit Logging** ([IDM\\_Audit\\_Logging\\_2005Q4M3.pdf](#)) – Referenzmaterialien und Informationen zur Vorgehensweise, die beschreiben, wie Kontoinformationen aus einer Ressource geladen und in Sun Java™ System Identity Manager synchronisiert werden.
- **Identity Manager Tuning, Troubleshooting, and Error Messages** ([IDM\\_Troubleshooting\\_2005Q4M3.pdf](#)) – Referenzmaterialien und Informationen zur Vorgehensweise, welche die Fehlermeldungen und Ausnahmen von Identity Manager beschreiben und Anweisungen für die Ablaufverfolgung und Behandlung von Probleme enthalten, die während der Arbeit auftreten können.

## Identity Auditor

*Identity Auditor Administration* ([IDA\\_Administration\\_2005Q4M3.pdf](#)) - Enthält eine Einführung in die Identity Auditor Administratorbenutzeroberfläche.

## Identity Manager Service Provider Edition

- **Identity Manager Service Provider Edition Administration Addendum** ([SPE\\_Administration\\_Addendum\\_2005Q4M3SP1.pdf](#)) - Enthält eine Einführung in die Funktionen von Identity Manager SPE.
- **Identity Manager Service Provider Edition Deployment** ([SPE\\_Deployment\\_2005Q4M3\\_SP1.pdf](#)) - Enthält Informationen zur Bereitstellung von Identity Manager SPE.

## Navigation in der Onlinedokumentation

---

Über die Acrobat-Textmarken können Sie Dokumentationen navigieren. Klicken Sie auf den Namen eines Abschnitts im Textmarkenbereich, um zum entsprechenden Abschnitt im Dokument zu springen.

Die gesamte Identity Manager-Dokumentation kann in jeder Identity Manager-Installation angezeigt werden. Navigieren Sie hierzu in Ihrem Webbrowser zu `idm/doc`.

# ***Install Pack Installation***

---

## **Korrekturen**

### **Vorwort**

Fehlerhafte Querverweise auf Anhang H vom Abschnitt „How to Find Information in this Guide“ wurden entfernt. (ID-12369).

### **Kapitel 1: Before You Install**

- Microsoft Exchange 5.5 wurde als unterstützte Ressource aus der Tabelle „Supported Resources“ entfernt. Es wurde verworfen. (ID-12682).
- Lotus Notes® 6.5.4 (Domino) wurde als unterstützte Ressource zur Tabelle „Supported Resources“ hinzugefügt. (ID-12226).
- JDK 1.5 wurde in mehreren Fällen als unterstützte Java-Version hinzugefügt. (ID-12984).
- ERP Systems SAP-Informationen in der Tabelle „Supported Resources“ wurden geändert in: (ID-12635).
  - SAP® R/3 v4.5, v4.6
  - SAP® R/3 Enterprise 4.7 (SAP BASIS 6.20)
  - SAP® NetWeaver Enterprise Portal 2004 (SAP BASIS 6.40)
  - SAP® NetWeaver Enterprise Portal 2004s (SAP BASIS 7.00)
- Red Hat-Informationen in der Tabelle „Supported Resources“ wurden geändert in:
  - Red Hat Linux Advanced Server 2.1
  - Red Hat Linux Enterprise Server 3.0, 4.0
- Unter „Supported Software and Environments“ wurden der Abschnitt „Repository Database Servers“ und die folgenden Informationen hinzugefügt: (ID-12425).
  - IBM® DB2® Universal Database for Linux, UNIX®, und Windows® (Version 7.x, 8.1, 8.2)
  - Microsoft SQL Server™ 2000
  - MySQL™ 4.1
  - Oracle 9i® und Oracle Database 10g, 10gR1 und 10gR2®

### **Kapitel 2: Installing Identity Installation Pack for Tomcat**

Das Kapitel unterstützt jetzt den Anwendungsserver Apache Tomcat (Versionen 4.1.x oder 5.0.x).

### Kapitel 4: Installing Identity Installation Pack for WebSphere

- Dieses Kapitel beschreibt jetzt die Installation von Websphere 5.1 Express und 6.0. (ID-12655, 12656) Zu den angegebenen Punkten wurden folgende Hinweise und Informationen hinzugefügt:

**Hinweis** Der folgende Schritt ist für die Installation von Identity Installation Pack 6.0 oder höher nicht erforderlich.

4. Wechseln Sie in das Staging-Verzeichnis und löschen Sie folgende Dateien, falls vorhanden:

```
WEB-INF\lib\cryptix-jce-provider.jar  
WEB-INF\lib\cryptix-jce-api.jar
```

25. Laden Sie die neueste Version des Package `jlog` von WebSphere unter der folgenden URL herunter:

```
http://www.alphaworks.ibm.com/tech/loggingtoolkit4j
```

**Hinweis** Das Package `jlog` ist jetzt in WebSphere 6.0 enthalten. Sie brauchen dieses nur für frühere Versionen herunterzuladen.

- Da Sie JDK 1.4.2 für diese Version installieren müssen, ist der Abschnitt *For JDK 1.3.x*: nicht mehr gültig. In diesem Kapitel muss der Abschnitt *For JDK 1.4* jetzt *For JDK 1.4.2* lauten.

### Kapitel 7/8: Installing Identity Installation Pack for Sun ONE/Sun Java System Application Server 7/8

- Unter „Installation Steps > Step 5“ wurden die folgenden korrigierten Informationen hinzugefügt: Edit the server.policy File > example permissions: (ID-12292).

```
permission java.io.FilePermission  
"/opt/SUNWappserver/domains/domain1/applications/j2ee-modules/  
idm/config/tracel.log", "read,write,delete";
```

```
permission java.io.FilePermission "$(java.io.tmpdir)$(/)*",  
"read,write,delete";
```

- Unter „Installation Steps > Step 5“ wurden die folgenden Informationen hinzugefügt: Edit the server.policy File > example permissions:

Wenn Sie die Identity Manager Service Provider Edition nutzen möchten, müssen Sie zu den obigen server.policy-Einträgen das folgende Zugriffsrecht hinzufügen.

```
permission java.lang.RuntimePermission "shutdownHooks";
```

## Kapitel 14: Uninstalling Applications

`_Version_` wurde aus dem Syntaxbeispiel unter „Remove the Software > On UNIX > Step 3“ entfernt. (ID-7762)

## Kapitel 15: Installing The Applications (Manual Installation)

Das Syntaxbeispiel unter „Installation Steps > Step 3“: Configure the Identity Install Pack Index Database Connection > Non-Xwindows Environments > Step 3 wurde folgendermaßen korrigiert: (ID-5821).

3. Set your license key with the following commands:

```
cd idm/bin
./lh license set -f LicenseKeyFile
```

## Anhang A: Index Database Reference

Die Zeile zur Beschreibung von SQL Server wurde abgeändert in:

Ihre Auswahl:	Geben Sie Folgendes ein
<p>SQL Server</p> <p><b>Standardwerte für den Microsoft SQL Server 2005 JDBC-Driver:</b></p> <ul style="list-style-type: none"> <li>• <b>URL:</b> "jdbc:sqlserver://host.your.com:1433;DatabaseName=dbname"</li> <li>• <b>JDBC Driver:</b> com.microsoft.sqlserver.jdbc.SQLServerDriver</li> <li>• <b>Connect as User:</b> waveset</li> </ul> <p>Für den Microsoft SQL Server 2000 JDBC-Treiber verwenden Sie folgende Werte:</p> <ul style="list-style-type: none"> <li>• <b>URL:</b> "jdbc:microsoft:sqlserver://host.your.com:1433;DatabaseName=dbname;SelectMethod=Cursor"</li> <li>• <b>JDBC Driver:</b> com.microsoft.jdbc.sqlserver.SQLServerDriver</li> <li>• <b>Connect as User:</b> waveset</li> </ul>	<p>Geben Sie den Pfad zur Index-Datenbank und das bei der Einrichtung der Datenbank gewählte Passwort an.</p> <p><b>Hinweis:</b> Alle Verbindungen zu SQL Server müssen über denselben JDBC-Treiber erfolgen. Dies gilt für das Repository und sämtliche Ressourcenadapter, die SQL Server-Konten oder -Tabellen verwalten oder benötigen, einschließlich: Microsoft SQL-Adapter, Microsoft Identity Integration Server-Adapter, Database Table-Adapter, Scripted JDBC-Adapter und alle auf diesen Adaptern beruhenden benutzerdefinierten Adapter. Bei dem Versuch, unterschiedliche Treiberversionen zu verwenden, treten Konfliktfehler auf.</p>

## **Anhang C: Configuring Data Sources for Identity Manager**

- Mehrere IOP URLs werden nicht unterstützt. (ID-12499) Die folgenden falschen Informationen unter „Configuring a WebSphere Data Source for Identity Manager > Configuring a Websphere 5 Data Source > Configure the DataSource in a Websphere Cluster“ wurden entfernt:

Wenn in der Eigenschaft **BOOTSTRAP\_ADDRESS** der Anwendungsserver nicht derselbe Anschluss angegeben ist, kann `java.naming.provider.url` mehrere URLs angeben. Beispiel:

```
iiop://localhost:9812,iiop://localhost:9813.
```

- Alle noch in WebSphere Version 5 verwendeten `j2c.properties` sind in WebSphere Version 6 nun Bestandteil der Datei `resources.xml`. Es wurden Informationen über die Konfiguration einer Websphere 5.1/6.x-Datenquelle und die Konfiguration der 6.x-Authentifizierungsdaten hinzugefügt. Informationen zur Konfiguration von Websphere 4.x-Datenquellen wurden entfernt. (ID-12767) Die Änderungen betreffen die folgenden Abschnitte:

### **Konfiguration eines JDBC Providers**

Mit der Administrationskonsole von WebSphere können Sie einen neuen JDBC Provider konfigurieren.

1. Klicken Sie auf die Registerkarte **Ressourcen** im linken Teilfenster, um eine Liste mit Ressourcentypen anzuzeigen.
2. Klicken Sie auf **JDBC-Provider**, um eine Tabelle der konfigurierten JDBC-Provider anzuzeigen.
3. Klicken Sie auf die Schaltfläche **Neu** über der Tabelle konfigurierter JDBC-Provider.
4. Wählen Sie aus der Liste der JDBC-Datenbanktypen den JDBC-Typ sowie den Implementierungstyp aus. Klicken Sie auf „Weiter“.

In diesem Beispiel werden Oracle, der Oracle JDBC-Treiber und Verbindungs-Pooling für Datenquellen verwendet.

5. Fahren Sie mit der Konfiguration allgemeiner Parameter fort.
  - Geben Sie den Namen an.
  - Geben Sie im Feld **Classpath** den JAR-Pfad an, der den JDBC-Treiber enthält. Zur Angabe eines Oracle Thin-Treibers sollten Sie beispielsweise einen Pfad, der dem folgenden ähnelt, eingeben:

```
/usr/WebSphere/AppServer/installedApps/idm/idm.ear/idm.war/WEB-INF/lib/oraclejdbc.jar
```

**Hinweis** Sie können den JAR-Pfad zum JDBC-Treiber mithilfe der Administrationskonsole angeben. Wählen Sie aus dem Menü **Umgebung** den Eintrag **WebSphere-Variable**. Wählen Sie in diesem Teilfenster zuerst **Zelle, Knoten** und **Server**, für die diese Umgebungsvariable definiert werden soll. Geben Sie dann den JAR-Pfad als Wert dieser Variable an.

- Geben Sie im Feld **Implementierungs-Klassenname** den vollständig qualifizierten Namen der JDBC-Treiberklasse an.
  - Für den Oracle Thin ist dieser Wert  
`oracle.jdbc.pool.OracleConnectionPoolDataSource.`
  - Für den db2 jcc-Treiber ist dieser Wert  
`com.ibm.db2.jcc.DB2ConnectionPoolDataSource.`
- Sie können auch den Namen, die Beschreibung des Providers oder andere ausgewählte Parameter ändern.

Klicken Sie auf die Schaltfläche **OK** unter der Tabelle, wenn Sie diesen Vorgang abgeschlossen haben. Im rechten Teilfenster sollte jetzt der neu hinzugefügte Provider angezeigt werden.

Informationen zur Konfiguration einer Datenquelle, die diesen JDBC-Provider nutzt finden Sie unter "Point the Identity Manager Repository to the Data Source".

## Konfiguration einer Websphere JDBC-Datenquelle

1. Mit der Administrationskonsole von WebSphere können Sie eine Datenquelle mit einem vorhandenen JDBC Provider definieren. Information zur Konfiguration eines neuen JDBC-Providers für Identity Installation Pack finden Sie unter "Konfiguration eines JDBC-Providers".

Vor dem Abschluss der Konfiguration einer Datenquelle müssen Sie Authentifizierungsdaten konfigurieren. Diese Aliasnamen enthalten Berechtigungsnachweise, die beim Herstellen einer Verbindung mit DBMS verwendet werden.

### Konfiguration der 5.1-Authentifizierungsdaten

1. Klicken Sie auf die Registerkarte **Sicherheit** im linken Teilfenster, um eine Liste von Sicherheitskonfigurationstypen anzuzeigen.
2. Klicken Sie auf die Registerkarte **JAAS-Konfiguration** im linken Teilfenster, um eine Liste von JAAS-Konfigurationstypen anzuzeigen.
3. Klicken Sie auf die Registerkarte **J2C-Authentifizierungsdaten** im linken Teilfenster. Im rechten Teilfenster wird eine Tabelle mit Authentifizierungsdaten angezeigt.
4. Klicken Sie auf die Schaltfläche **Neu** über der Authentifizierungsdatentabelle. Im rechten Teilfenster wird eine Tabelle mit allgemeinen Eigenschaften, die konfiguriert werden müssen, angezeigt

## Install Pack Installation

5. Konfigurieren Sie die allgemeinen Eigenschaften für den neuen Authentifizierungsdateneintrag. Bitte beachten Sie Folgendes:
  - **Alias** ist der Name, der in der Auswahlliste immer dann angezeigt wird, wenn DBMS-Berechtigungs-nachweise für eine Datenquelle konfiguriert werden.
  - **Benutzer-ID** ist der Benutzername, der zum Herstellen der Verbindung mit DBMS verwendet wird.
  - **Passwort** ist das Passwort, das zum Herstellen der Verbindung mit DBMS verwendet wird.

Konfigurieren Sie als Nächstes die Datenquelle.

### Konfiguration der 6.x-Authentifizierungsdaten

1. Klicken Sie auf **Sicherheit > Globale Sicherheit**.
2. Klicken Sie unter „Authentifizierung“ auf **JAAS-Konfiguration > J2C-Authentifizierungsdaten**. Das Teilfenster **J2C-Authentifizierungsdaten** wird angezeigt.
3. Klicken Sie auf **Neu**.
4. Geben Sie einen eindeutigen Aliasnamen, eine gültige Benutzer-ID, ein gültiges Passwort und (optional) eine Kurzbeschreibung ein.
5. Klicken Sie auf **OK** oder **Anwenden**. Benutzer-ID und Passwort müssen nicht validiert werden.
6. Klicken Sie auf **Speichern**.

**Hinweis** Der neue Eintrag wird zwar angezeigt, ohne dass der Anwendungsserver, der in der Datenquellendefinition verwendet werden soll, neu gestartet werden muss, wird jedoch erst nach einem Neustart des Servers wirksam.

### Konfiguration der Datenquelle

**Hinweis** Informationen zur Konfiguration von Datenquellen im Websphere 5.x-Cluster finden Sie unter “Configure the DataSource in a Websphere Cluster”.

1. Klicken Sie auf die Registerkarte **Ressourcen** im linken Teilfenster, um eine Liste mit Ressourcentypen anzuzeigen.
2. Klicken Sie auf **JDBC-Provider**, um eine Tabelle der konfigurierten JDBC-Provider anzuzeigen.
3. Klicken Sie auf den Namen eines JDBC-Providers in der Tabelle. Im rechten Teilfenster wird eine Tabelle mit allgemeinen Eigenschaften für den ausgewählten JDBC-Provider angezeigt.

4. Gehen Sie nach unten zur Tabelle mit zusätzlichen Eigenschaften. Klicken Sie auf **Datenquellen**. Im rechten Teilfenster wird eine Tabelle mit Datenquellen für den ausgewählten JDBC-Provider angezeigt.

**Hinweis** Bitte beachten Sie das Feld **Gültigkeitsbereich** am oberen Rand der WebSphere-Administrationskonsole. Vergewissern Sie sich, dass die Felder **Knoten** und **Server** leer sind, sodass die Zelleninformationen zur Konfiguration unter den Schaltflächen **Neu** und **Löschen** angezeigt werden.

5. Klicken Sie auf die Schaltfläche **Neu** über der Datenquellentabelle. Im rechten Teilfenster wird eine Tabelle mit allgemeinen Eigenschaften, die zu konfigurieren sind, angezeigt.
6. Konfigurieren Sie die allgemeinen Eigenschaften für die neuen Datenquelle. Bitte beachten Sie Folgendes:
  - **JNDI-Name** ist der Pfad zur Datenquelle (DataSource-Objekt) im Verzeichnisdienst. Sie müssen den gleichen Wert wie beim Argument `-f` in `setRepo -tdbms -iinitCtxFac -ffilepath` angeben.
  - **Container-verwaltete Fortdauer** muss nicht markiert werden, da Identity Installation Pack keine Enterprise Java Beans (EJBs) verwendet.
  - **Komponentenverwaltetes Authentifizierungs-Alias** zeigt auf die Berechtigungsnachweise, die beim Zugriff auf die DBMS, auf die das DataSource-Objekt zeigt, verwendet werden.
  - Wählen Sie aus der Liste den Aliasnamen aus, der den passenden Satz an DBMS-Berechtigungsnachweisen enthält. Weitere Informationen finden Sie unter *Konfiguration der 5.1-Authentifizierungsdaten*.
  - Der Parameter **Containerverwaltetes Authentifizierungs-Alias** wird nicht verwendet. Setzen Sie diesen Wert auf `(keines)`. Identity Installation Pack stellt eine eigene Verbindung zur DBMS, auf die das betreffende DataSource-Objekt zeigt, her.
  - Klicken Sie auf **OK**, wenn Sie dieses Teilfenster konfiguriert haben. Die Seite „Datenquellen“ wird angezeigt.
7. Klicken Sie auf das DataSource-Objekt, das Sie erzeugt haben. Gehen Sie dann zur Tabelle mit zusätzlichen Eigenschaften im unteren Teil. Klicken Sie auf den Link **Benutzerdefinierte Eigenschaften**.  
Im rechten Teilfenster wird eine Tabelle DBMS-spezifischer Eigenschaften angezeigt.
8. Konfigurieren Sie die benutzerdefinierten Eigenschaften für dieses DataSource-Objekt. Klicken Sie auf den Link der gewünschten Eigenschaft, um ihren Wert einzustellen. Bitte beachten Sie Folgendes:
  - **URL** ist die einzige erforderliche Eigenschaft. Diese Datenbank-URL identifiziert die Datenbankinstanz und enthält die Parameter `driverType`, `serverName`, `portNumber` und `databaseName`. Einige dieser Parameter können Sie auch als individuelle Eigenschaften angeben.

## Install Pack Installation

- In diesem Beispiel ist **driverType** auf „thin“ gesetzt.
  - Beim Parameter **serverName** kann ein Hostname (oder eine IP-Adresse) angegeben werden.
  - **databaseName** ist normalerweise ein kurzer Datenbankname.
  - **portNumber** ist für Oracle standardmäßig auf 1521 gesetzt.
  - **preTestSQLString** kann auf einen Wert wie z.B. SELECT 1 FROM USEROBJ gesetzt werden. Diese SQL-Abfrage bestätigt, dass die USERJOB-Tabelle existiert und auf diese zugegriffen werden kann.
9. Sie können in der Tabelle „Zusätzliche Eigenschaften“ auch auf den Link **Verbindungs-Pool** klicken, wenn Sie diese Eigenschaften zur Leistungsoptimierung konfigurieren möchten.

## Anhang E: Configuring JCE

Ein Hinweis muss wie folgt lauten:

**Hinweis** Da Sie JDK 1.4.2 für diese Version installieren müssen, muss bei allen unterstützten Umgebungen jetzt JCE 1.2 enthalten sein. Außerdem sind die Informationen in diesem Anhang nicht mehr gültig.

## Zusätzliche Informationen

### Kapitel 1: Before You Install

- Unter „Setup Task Flow > Bullet Install and configure the Identity Install Pack software“ wurde der folgende Hinweis hinzugefügt: (ID-8431).

**Hinweis** Unix- bzw. Linux-Systeme:

- Bei der Installation von Identity Installation Pack, Versionen 5.0 - 5.0 SP1 muss das Verzeichnis `/var/tmp` vorhanden sein und für den Benutzer, der das Installationsprogramm ausführt, Schreibzugriff besitzen.
- Bei der Installation von Identity Installation Pack, Version 5.0 SP2 oder höher muss das Verzeichnis `/var/opt/sun/install` vorhanden sein und für den Benutzer, der das Installationsprogramm ausführt, Schreibzugriff besitzen.
- Zu „Prerequisite Tasks > Set Up an Index Database > Setting Up SQL Server > Step 3b“ wurde der folgende Hinweis hinzugefügt: (ID-11835).

**Hinweis** Folgende Dateien müssen sich im Verzeichnis `$WSHOME/WEB-INF/lib` befinden:

```
db2jcc  
db2jcc_license_cisuz.jar or db2jcc_license_cu.jar
```

- Unter Supported Software and Environments > Application Servers wurden die folgenden Informationen hinzugefügt: (ID-12385).

**Hinweis** Ihr aktuell installierter Anwendungsserver muss UTF-8 unterstützen.

## Kapitel 2: Installing Identity Installation Pack for Tomcat

- Unter „Installation Steps > Step 1: Install the Tomcat Software > Installing on UNIX“ wurden die folgenden Schritte hinzugefügt: (ID-12487).

2. Kopieren Sie die Dateien `mail.jar` und `activation.jar` in das Verzeichnis `./tomcat/common/lib`. Diese Dateien finden Sie unter:

```
http://java.sun.com/products/javamail
http://java.sun.com/products/beans/glasgow/jaf.html
```

- Unter „Installation Steps > Step 1: Install the Tomcat Software > Installing on UNIX“ wurden die folgenden Schritte hinzugefügt: (ID-12462).

3. Bei der Konfiguration von Tomcat zur Unterstützung von UTF-8 müssen Sie das Attribut `URIEncoding="UTF-8"` zum Element `connector` in der Datei `TOMCAT DIRconf/server.xml` hinzufügen. Beispiel:

```
<!-- Define a non-SSL Coyote HTTP/1.1 Connector on the port
specified during installation -->
<Connector port="8080"
    maxThreads="150"
    minSpareThreads="25"
    maxSpareThreads="75"
    enableLookups="false" redirectPort="8443"
    acceptCount="100" debug="0" connectionTimeout="20000"
    disableUploadTimeout="true"
    URIEncoding="UTF-8" />
```

4. Bei der Konfiguration von Tomcat zur Unterstützung von UTF-8 müssen Sie in den Optionen der Java Virtual Machine den Parameter `-Dfile.encoding=UTF-8` hinzufügen.

## Kapitel 13: Updating Identity Manager

Zum Identity Manager Upgrade wurde ein Querverweis hinzugefügt, damit Benutzer besser vollständige Upgrade-Informationen finden können. (ID-12366).

### Kapitel 15: Installing The Applications (Manual Installation)

Unter „Installation Steps > Step 2: Install the Application Software“ wurde der folgende Hinweis hinzugefügt: (ID-8344).

**Hinweis** Ab Version 5.0 SP3 befinden sich die Adapterklassen jetzt in der Datei `idmadapter.jar`. Wenn Sie benutzerdefinierte Adapter nutzen, kann es sein, dass Sie den Java-CLASSPATH aktualisieren müssen.

### Anhang B: Configuring MySQL

Unter „Configuring MySQL > Step 3: Start the MySQL process“ wurden die folgenden Informationen hinzugefügt: (ID-12461).

Wenn dieser Prozess noch nicht gestartet wurde, können Sie MySQL wie folgt registrieren und starten.

Windows: Wenn das MYSQL nicht im Verzeichnis `c:\mysql` installiert wird, müssen Sie eine Datei namens `c:\my.cnf` mit dem folgenden Inhalt erstellen:

```
[mysqld]
basedir=d:/mysql/
default-character-set=utf8
default-collation=utf8_bin
```

Installieren und starten Sie diesen Dienst unter Windows:

```
cd <MySQL_Install_Dir>/bin
mysqld-nt --install
net start mysql
```

### Anhang C: Configuring Data Sources for Identity Manager

Unter „Configuring a WebSphere Data Source for Identity Manager > Point the Identity Manager Repository to the Data Source“ wurden folgende Informationen hinzugefügt: (ID-12071).

8. Lassen Sie das Repository auf ein neues Verzeichnis zeigen. Beispiel:

```
lh -Djava.ext.dirs=$JAVA_HOME/jre/lib/ext:$WAS_HOME/lib setRepo
-tdbms -iinitCtxFac
-ffilepath -uiiop://localhost:bootstrap_port
-Uusername
-Ppassword
-toracle icom.ibm.websphere.naming.WsnInitialContextFactory -
fDataSourcePath
```

Im obigen Beispiel kann `DataSourcePath` auf `jdbc/jndiname` gesetzt sein. `bootstrap_port` ist das Port für die Bootstrap-Adresse des WebSphere-Servers.

Die Option `-Djava.ext.dirs` fügt zum CLASSPATH alle JAR-Dateien in den WebSphere-Verzeichnissen `lib/` und `java/jre/lib/ext/` hinzu. Dies ist erforderlich, damit der Befehl „setrepo“ ordnungsgemäß funktioniert.

Ändern Sie die Option `-f` so, dass sie mit dem Wert, den Sie bei der Konfiguration der Datenquelle im Feld **JNDI-Name** angegeben haben, übereinstimmt. Weitere Informationen zu diesem Befehl finden Sie in der Referenz zum Befehl „setrepo“.

# Identity Manager Upgrade

---

## Zusätzliche Informationen

### Kapitel 1: Upgrade Overview

Zum Abschnitt *Example Upgrade* wurde folgender Punkt hinzugefügt: (ID-12467).

Lassen Sie beim Bearbeiten des Felds „SuperRoles“ im Rollenformular äußerste Vorsicht walten. SuperRoles können verschachtelte Rollen sein. Die Felder „SuperRoles“ und „SubRoles“ weisen Verschachtelungen von Rollen und deren zugehörigen Ressourcen bzw. Ressourcengruppen auf. Wenn sie auf einen Benutzer angewendet wird, enthält die betreffende SuperRole die zugehörigen Ressourcen mit den dafür vorgesehenen SubRoles (Unterrollen). Das Feld „SuperRole“ wird angezeigt, um auf die Rollen hinzuweisen, die die angezeigte Rolle enthalten.

### Kapitel 3: Develop the Upgrade Plan

Zum Abschnitt „Upgrade the Environment Upgrade From Identity Manager 5.x to 6.x“ wurde der folgende Abschnitt hinzugefügt. (ID-12361).

#### Schritt 2: Aufrüsten des Repository-Datenbankschemas

Identity Manager 6.0 verwendet ein Schema, das neue Tabellen für Aufgaben, Gruppen und Organisationen sowie die `syslog`-Tabelle enthält. Sie müssen diese neuen Tabellen erstellen und ihre vorhandenen Daten in diese Tabellen kopieren.

**Hinweis** Vor dem Aufrüsten des Repository-Schemas sollten Sie von allen Repository-Tabellen Sicherungskopien erstellen.

## Identity Manager Administration Guide

1. Identity Manager speichert Objekte in zwei Tabellen. Sie können zum Ändern von Schemen die im Verzeichnis `sample` befindlichen Beispiel-Skripten nutzen.

Zum Aufrüsten der Repository-Tabellen dient das Skript

`sample/upgradeto2005Q4M3.Datenbankname.`

- Hinweis** Die Aufrüstung von MySQL-Datenbanken ist ziemlich kompliziert. Weitere Informationen hierzu finden Sie unter `sample/upgradeto2005Q4M3.mysql.`

## Identity Manager Administration Guide

---

### Zusätzliche Informationen

- Wenn Sie Sunrise konfiguriert haben und einen Benutzer erstellen, wird ein Arbeitselement erstellt, das auf der Registerkarte **Genehmigungen** angezeigt wird. Durch Genehmigung dieses Elements wird das Sunrise-Datum überschrieben und das Konto erstellt. Wenn Sie das Element ablehnen, wird der Erstellvorgang für das Konto abgebrochen.
- Bei der Planung der Abstimmung können Sie jetzt den Namen einer Regel angeben, die den Zeitplan anpasst. Die Regel kann beispielsweise Abstimmungen für Samstag auf den folgenden Montag verlegen. (ID-11391).

### Kapitel 4: Administration

- Es wurden Informationen zur Delegierung von Genehmigungsfähigkeiten hinzugefügt. (ID-12754).

#### Delegierung von Genehmigungen

Wenn Sie über Genehmigerfähigkeiten verfügen, können Sie zukünftige Genehmigungsanforderungen für einen bestimmten Zeitraum an einen oder mehrere Benutzer (die „Delegierten“) delegieren. Diese müssen hierzu keine Genehmigerfähigkeiten besitzen.

Es werden lediglich zukünftige Genehmigungsanforderungen delegiert. Bereits vorhandene Elemente (die Elemente unter „Wartet auf Genehmigung“) müssen Sie über die Weiterleitungsfunktion separat weiterleiten.

Klicken Sie zum Einrichten einer Delegierung auf die Registerkarte **Eigene Genehmigungen delegieren** im Bereich **Genehmigungen**.

### Hinweise

- Sie können auf die Delegierungsfunktion zugreifen, wenn Sie aufgrund einer Ihrer zugewiesenen Fähigkeiten das Delegierungsrecht für WorkItem, eine von dessen authType-Erweiterungen (Approval, OrganizationApproval, ResourceApproval, RoleApproval, usw.) oder einen benutzerdefinierten Subtyp haben, der WorkItem oder einen von dessen authTypes erweitert.
- Sie können Genehmigungen auch über die Formularregisterkarte Sicherheit der Seiten zum Erstellen, Bearbeiten und Anzeigen von Benutzern sowie über das Hauptmenü der Benutzeroberfläche delegieren.

Während des Delegierungszeitraums können die Delegierten Anforderungen in Ihrem Namen genehmigen. In delegierten Genehmigungsanforderungen ist der Name des Delegierten enthalten.

### Überwachungsprotokolleinträge für Anforderungen

Überwachungsprotokolleinträge für genehmigte und abgelehnte Genehmigungsanforderungen enthalten den Namen des Delegierenden (d. h. Ihren Namen), wenn die Anforderung delegiert wurde. Änderungen an den Angaben zu den Delegiertengenehmigern eines Benutzers werden beim Erstellen oder Ändern eines Benutzers im Detailabschnitt des Überwachungsprotokolleintrags protokolliert.

## Kapitel 5: Configuration

- Es wurden Informationen zur Konfiguration von Identity-Attributen beim Erstellen bzw. Aktualisieren einer Ressource hinzugefügt. (ID-12606).

### Identity-Attribute aus Ressourcenänderungen konfigurieren

Identity-Attribute bestimmen, in welchem Verhältnis Attribute auf Ressourcen zueinander stehen. Das Erstellen oder Ändern einer Ressource kann sich daher auf diese Attributbeziehungen auswirken.

Beim Speichern einer Ressource zeigt Identity Manager die Seite „Identity-Attribute konfigurieren?“ an. Hier können Sie wahlweise:

- weiter zur Seite „Identity-Attribute aus Ressourcenänderungen konfigurieren“ gehen und dort Attribute konfigurieren. Klicken Sie auf **Ja**, um fortzufahren.
- zur Ressourcenliste zurückkehren Klicken Sie auf **Nein**, um zurückzugehen.
- diese Seite für zukünftige Ressourcenaktualisierungen deaktivieren. Klicken Sie auf **Diese Frage nicht mehr wiederholen**, um diese Seite zu deaktivieren.

**Hinweis** **Diese Frage nicht mehr wiederholen** ist nur für Benutzer mit der Fähigkeit, die Metaansicht zu ändern, sichtbar.

### Die Seite „Identity-Attribute konfigurieren? wieder aktivieren“

Wenn die Seite „Identity-Attribute konfigurieren?“ deaktiviert ist, können Sie sie auf eine der folgenden Weisen reaktivieren:

- Bearbeiten Sie über die Debugging-Funktionen von Identity Manager das WSUser-Objekt des angemeldeten Benutzers. Ändern Sie den Wert der Eigenschaft `idm_showMetaViewFromResourceChangesPage` auf `true`.
- Fügen Sie dem Benutzerformular (z. B. dem Formular mit Registerkarten) ein Feld wie das folgende hinzu, und ändern Sie anschließend über die Seite zum Bearbeiten von Benutzern den Wert dieser Einstellung:

```
<Field name="accounts[Lighthouse].properties.displayMetaViewPage">  
  <Display class="Checkbox">  
    <Property name="label" value="Display Meta View?"/>  
  </Display>  
</Field>
```

### Konfiguration von Attributen

Auf der Seite „Identity-Attribute konfigurieren“ (aus „Ressourcen ändern“) können Sie Attribute aus den Schemazuordnungen geänderter Ressourcen auswählen, um sie als Quelle bzw. Ziel für Identity-Attribute zu verwenden. In einigen Fällen ist es nicht möglich, Attribute in der Spalte „Quelle“ bzw. „Ziel“ auszuwählen. Sie können ein Attribut nicht als Quelle auswählen, wenn es:

- in der Schemazuordnung als verschlüsselt gekennzeichnet ist
- in der Schemazuordnung ausschließlich für Schreibzugriff gekennzeichnet ist

Sie können ein Attribut nicht als Ziel auswählen, wenn:

- es ein global gespeichertes Identity-Attribut mit demselben Namen gibt. Wenn es beispielsweise ein globales Identity-Attribut namens „Vorname“ gibt, ist die Zieloption „Vorname“ ausgewählt und kann nicht abgewählt werden.
- es in der Schemazuordnung ausschließlich für Lesezugriff gekennzeichnet ist.
- die Funktionen der Ressource zum Erstellen und Aktualisieren von Konten deaktiviert sind oder die Ressource diese Funktionen nicht unterstützt.

### Kapitel 7: Sicherheit

- Dem Abschnitt „Configuring Authentication for Common Resources“ wurde der folgende Hinweis hinzugefügt: (ID-16805).

Alle in einer Gruppe gemeinsamer Ressourcen aufgeführten Ressourcen müssen auch in der Definition des Anmeldemoduls enthalten sein. Wenn eine vollständige Liste gemeinsamer Ressourcen nicht auch in der Definition des Anmeldemoduls enthalten ist, funktioniert das Leistungsmerkmal der gemeinsamen Ressourcen nicht ordnungsgemäß.
- Es wurden Informationen zum Anmelden bei gleichzeitigen Sitzungen hinzugefügt. (ID-12778).

#### Begrenzen von Sitzungen mit mehreren gleichzeitigen Anmeldungen

Standardmäßig können Identity Manager-Benutzer Sitzungen mit mehreren gleichzeitigen Anmeldungen ausführen. Sie können dies so einschränken, dass nur noch eine Sitzung pro Anmeldeanwendung möglich ist. Hierzu ändern Sie den Wert des Konfigurationsattributs `security.authn.singleLoginSessionPerApp` im Systemkonfigurationsobjekt. Dieses Attribut ist ein Objekt, das wiederum ein Attribut pro Anmeldeanwendung enthält (z. B. für die Administratoroberfläche, die Benutzeroberfläche oder BPE). Ändern Sie den Wert dieses Attributs auf `true`, damit für jeden Benutzer nur noch eine einzige Anmeldesitzung möglich ist.

In diesem Fall kann sich der Benutzer zwar bei mehreren Sitzungen anmelden, es bleibt jedoch nur die jeweils letzte Sitzung aktiv und gültig. Wenn der Benutzer versucht, unter einer ungültigen Sitzung eine Aktion auszuführen, wird die Sitzung automatisch beendet.

### Kapitel 8: Reporting

Im Abschnitt „Summary Reports“ enthält die Beschreibung von Benutzerberichten jetzt die Fähigkeit, Benutzer nach Managerrollen zu suchen: (ID-12690).

- **Benutzer** -- Anzeigen von Benutzern, die ihnen zugewiesenen Rollen und die ihnen zugänglichen Ressourcen. Bei der Definition eines Benutzerberichtes können Sie festlegen, welche Benutzer nach Namen, zugehörigem Manager, Rolle, Organisation oder Ressourcenzuweisung im Bericht enthalten sein sollen.

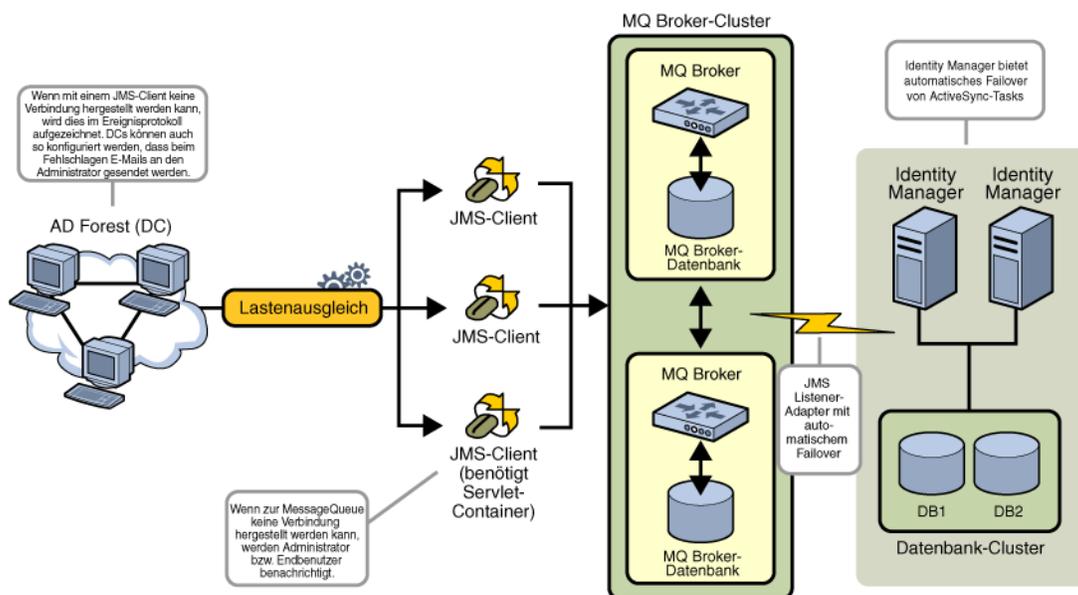
## Kapitel 10: PasswordSync

- Es wurden Anweisungen zur Konfiguration von Windows-PasswordSync mit einem Sun JMS-Server hinzugefügt. Weitere Informationen finden Sie im Dokument *Configuring PasswordSync with a Sun JMS Server*, das diesen Versionshinweisen beiliegt. (ID-11788).
- Es wurde der folgende neue Abschnitt zur Beschreibung der Hochverfügbarkeitsarchitektur mit Failover für PasswordSync hinzugefügt. (ID-12634).
- Es wurde ein Abschnitt hinzugefügt, der die Implementierung von PasswordSync ohne Java Messaging Server beschreibt. (ID-14974).

### Failover-Deployment für Windows PasswordSync

Die PasswordSync-Architektur eliminiert einzelne fehlerhafte Stellen im Windows-Deployment für die Passwort-Synchronisierung für Identity Manager.

Wenn Sie jeden Active Directory Domain Controller (ADC) so konfigurieren, dass er mit einem von mehreren JMS-Clients über eine Auslastungsverteilung (siehe folgende Abbildung) eine Verbindung herstellt, können die JMS-Clients Nachrichten an einen Cluster aus Message Queue Brokern senden. Dieser gewährleistet, dass beim Ausfall von Message-Queues keine Nachrichten verloren gehen.



**Hinweis** Für Ihren Message Queue-Cluster ist höchstwahrscheinlich eine Datenbank erforderlich, um die Nachrichten-Persistenz zu gewährleisten. (Anweisungen zur Konfiguration eines Message Queue Broker-Clusters finden Sie in der Produktdokumentation Ihres Anbieters.)

Der Identity Manager-Server, auf dem ein für das automatische Failover konfigurierter JMS Listener-Adapter läuft, kontaktiert den Message Queue Broker-Cluster. Obwohl der Adapter zur gleichen Zeit nur in einer Instanz von Identity Manager ausgeführt wird, beginnt er beim Ausfall des primären ActiveSync-Servers mit dem Suchen nach Passwortnachrichten auf einem sekundären Identity Manager-Server und teilt Passwortänderungen untergeordneten Ressourcen mit.

### Implementierung von PasswordSync ohne Java Messaging Service

Zur Implementierung von PasswordSync ohne JMS müssen Sie das Konfigurationsprogramm mit dem folgenden Flag aufrufen:

```
Configure.exe -direct
```

bei Angabe des Flags `-direct` zeigt das Konfigurationsprogramm die Registerkarte „Benutzer“ an. Konfigurieren Sie PasswordSync gemäß den in „Configuring PasswordSync“ aufgeführten Anweisungen. Dabei gelten folgende Ausnahmen:

- Konfigurieren Sie keine Parameter in den Registerkarten „JMS-Einstellungen“ und „JMS-Eigenschaften“.
- Geben Sie in der Registerkarte „Benutzer“ das Konto und das Passwort an, das zum Herstellen einer Verbindung zu Identity Manager verwendet wird.

Wenn Sie PasswordSync ohne JMS implementieren, brauchen Sie keinen JMS Listener-Adapter zu erstellen. Deswegen können Sie die in „Deploying PasswordSync“ angegebenen Anweisungen überspringen. Wenn Sie Benachrichtigungen einrichten wollen, kann es sein, dass Sie den Workflow „Benutzerpasswort ändern“ modifizieren müssen.

**Hinweis** Wenn Sie das Konfigurationsprogramm danach ohne Angabe des Flags `-direct` ausführen, benötigt PasswordSync zur Konfiguration JMS. Starten Sie das Anwendungsprogramm mit dem Flag `-direct` neu, um JMS erneut zu umgehen.

# Korrekturen

## Kapitel 5: Ressourcen

In der Tabelle für benutzerdefinierte Ressourcenklassen wurde die benutzerdefinierte Ressourcenklasse für den ClearTrust-Ressourcenadapter wie folgt berichtigt: (ID-12681).

```
com.waveset.adapter.ClearTrustResourceAdapter
```

## Kapitel 10: PasswordSync

Im Abschnitt „Configuring PasswordSync“ unter „JMS Settings Dialog“ wurde die Beschreibung für „Queue Name“ wie folgt berichtigt:

- **Queue Name** specifies the Destination Lookup Name for the password synchronization events. (ID-12621).

## lh-Referenz

Die Befehlssyntax wurde entsprechend aktualisiert, um anzuzeigen, dass nach angegebenen Optionen ein Leerzeichen folgen muss. (ID-12798).

Bei Verwendung der Option `-p` sollte aus Sicherheitsgründen *Password* als Pfad zu einer Textdatei, die ein Passwort enthält, angegeben werden, anstatt das Passwort direkt in der Befehlszeile einzugeben.

## Beispiele

- `lh com.waveset.session.WavesetConsole`
- `lh console`
- `lh console -u $user -p Pfad_zu_Passwort.txt`
- `lh setup -U Administrator -P Pfad_zu_Passwort.txt`
- `lh setRepo -c -A Administrator -C Pfad_zu_Passwort.txt`
- `lh setRepo -t LokaleDateien -f $WSHOME`

## Der license-Befehl

### Syntax

```
license [Optionen] { Status | set {Parameter} }
```

### Optionen

- `-U Benutzername` (wenn das Configurator-Konto umbenannt wurde)
- `-P Pfad_zu_Passwort.txt` (wenn das Configurator-Passwort geändert wurde)

Die Parameter für die Option `set` müssen im Format `-f Datei` angegeben werden.

# Identity Manager Workflows, Forms, and Views

---

## Kapitel 1: Workflows

Die Erläuterung manueller Aktionen in diesem Kapitel muss die folgenden Informationen enthalten:

Ist das Attribut `itemType` eines Arbeitselements auf „wizard“ gesetzt, umgeht das Arbeitselement beim Prüfen der WorkItem-Ansicht standardmäßig das Abrufen weiterleitender Genehmiger. Weist „itemType“ einen anderen Wert als „wizard“ auf, ruft Identity Manager die weiterleitenden Genehmiger weiterhin ab, es sei denn, `CustomUserList` ist als Eigenschaft des in der manuellen Aktion verwendeten Formulars auf „true“ gesetzt. (ID-10777).

Fügen Sie hierzu den folgenden Code in das Formular ein:

```
<Formular>
  <Properties>
    Property name="CustomUserLists" value="true"/>
  </Properties>
```

## Kapitel 2: Workflow Services

- Die Argumenttabelle für die Workflow-Dienstsitzung `createView` ist falsch. In der folgenden Tabelle werden die für diesen Dienst verfügbaren Argumente beschrieben.

Name	Erforderlich	Gültige Werte	Beschreibung
<code>op</code>	ja	<code>createView</code>	
<code>viewid</code>	ja		Legt den Typ der Ansicht fest, die erstellt werden soll.
<code>options</code>	nein		Ansichtsspezifische Optionen. Die übergebenen Werte gelten nur für die verwendete Ansicht. Die häufigste Ansicht ist die Benutzeransicht (UserView). Sie finden die Optionen in <code>session.UserViewConstants</code> . Optionskonstanten für einfachere Ansichten sollten in der Datei <code>Viewer.java</code> deklariert werden. Die in Workflows am zweithäufigsten verwendete Ansicht ist <code>ProcessViewer</code> , gefolgt von <code>PasswordViewer</code> , <code>DisableViewer</code> , <code>EnableViewer</code> und <code>RenameViewer</code> . Diese haben nur vergleichsweise wenig Optionen.

## Identity Manager Workflows, Forms, and Views

- Identity Manager bietet die Methode `checkStringQualityPolicy` der Workflow-Dienste, die den Wert einer betreffenden Zeichenkette gegen die geltenden Zeichenfolgen-Richtlinien prüft. (ID-12428, 12440).

Name	Erforderlich	Gültige Werte	Beschreibung
<code>policy</code>	ja		Gibt die Richtlinie (für Zeichenfolgen) an
<code>map</code>	nein		Zeigt eine Aufstellung der Zeichen (Map), die eine Zeichenkette nicht enthalten darf. <code>returnNull</code> -- (optional) Bei <code>true</code> gibt die Methode bei erfolgreicher Ausführung ein Nullobjekt zurück.
<code>value</code>	ja		Gibt den Inhalt der zu überprüfenden Zeichenkette an. (Objekt)
<code>pwdhistory</code>	nein		Führt die früheren Passwörter eines Benutzers in Großbuchstaben und verschlüsselt auf.
<code>owner</code>	ja		Gibt den Benutzer an, der der Eigentümer der zu überprüfenden Zeichenkette ist.

Diese Methode gibt ein `checkPolicyResult`-Objekt zurück. Der Wert `true` gibt an, dass die betreffende Zeichenkette den Test gegen die geltenden Richtlinien bestanden hat. Diese Methode gibt eine Fehlermeldung zurück, wenn die Zeichenkette den Test nicht bestanden hat. Wenn die Option `returnNull` im Parameter `map` auf `true` gesetzt ist, gibt die Methode bei erfolgreicher Ausführung ein Nullobjekt zurück.

- Identity Manager bietet jetzt den Workflow-Dienst `auditPolicyScan` (ID-12615). Dieser Workflow-Dienst dient dazu, Benutzer auf der Grundlage der ihnen zugewiesenen Richtlinien nach Verstößen gegen Überprüfungsrichtlinien abzufragen. Wenn dem betreffenden Benutzer keine Richtlinie zugewiesen ist, wird von Identity Manager die seiner Organisation zugewiesene Richtlinie (falls vorhanden) verwendet.

Diese Methode übernimmt ein Argument, `view`, das die Benutzeransicht des angegebenen Benutzers festlegt. Sie gibt die Workflow-Variable `checkPolicyResult` zurück. Diese Variable enthält eines von Folgendem:

- Liste der Verletzungen
- Nullwert, wenn keine Verletzungen vorliegen

## Kapitel 3: Formulare

Identity Manager kann erforderliche Attribute in der Schemazuordnung einer Ressource kennzeichnen. Im Formular „Benutzer bearbeiten“ sind diese Attribute mit einem \* (Sternchen) gekennzeichnet. Standardmäßig zeigt Identity Manager ein Sternchen nach dem auf den Attributnamen folgenden Textfeld an. (ID-10662).

Gehen Sie folgendermaßen vor, um die Positionierung des Sternchens anzupassen:

1. Öffnen Sie mit Identity Manager BPE oder einem XML-Editor Ihrer Wahl das Konfigurationsobjekt „Komponenteneigenschaften“.
2. Fügen Sie `EditForm.defaultRequiredAnnotationLocation=left` zum Tag `<SimpleProperties>` hinzu.  
Gültige Werte für `defaultRequiredAnnotationLocation` sind `left`, `right` und `none`.
3. Speichern Sie die Änderungen, und starten Sie den Anwendungsserver neu.

## Kapitel 4: FormUtil Methods

- Identity Manager bietet die FormUtil-Methode `checkStringQualityPolicy`, die den Wert einer betreffenden Zeichenkette gegen die geltenden Zeichenfolgen-Richtlinien prüft. (ID-12428, 12440).  
**checkStringQualityPolicy**(LighthouseContext s, String policy, Object value, Map map, List pwdhistory, String owner)

Parameter	Beschreibung
<i>LighthouseContext</i>	Der Lighthouse-Kontext des aktuellen Benutzers.
<i>policy</i>	(Erforderlich) Gibt den Namen der Richtlinien an, gegen die die betreffende Zeichenkette geprüft wird.
<i>value</i>	(Erforderlich) Gibt den zu überprüfenden Zeichenketteninhalt an.
<i>map</i>	(Optional) Zeigt eine Aufstellung der Zeichen, die eine Zeichenkette nicht enthalten darf. <code>returnNull</code> -- (optional) Bei <code>true</code> gibt die Methode bei erfolgreicher Ausführung ein Nullobjekt zurück.
<i>pwdhistory</i>	(Optional) Führt die früheren Passwörter eines Benutzers in Großbuchstaben und verschlüsselt auf.
<i>owner</i>	(Erforderlich) Gibt den Benutzer an, der der Eigentümer der zu überprüfenden Zeichenkette ist.

## Identity Manager Workflows, Forms, and Views

Diese Methode gibt `true` zurück, wenn die betreffende Zeichenkette den Test gegen die geltenden Richtlinien bestanden hat. Diese Methode gibt eine Fehlermeldung zurück, wenn die Zeichenkette den Test nicht bestanden hat. Wenn die Option `returnNull` im Parameter `map` auf `true` gesetzt ist, gibt die Methode bei erfolgreicher Ausführung ein Nullobjekt zurück.

- Identity Manager bietet jetzt die FormUtil-Methode `controlsAtLeastOneOrganization`. (ID-9260).

**controlsAtLeastOneOrganization**(LighthouseContext `s`, List organizations)  
throws WavesetException {

Ermittelt, ob ein aktuell authentifizierter Benutzer die auf der Liste einer oder mehrerer Organisationsnamen (Objektgruppen) angegebenen Organisationen kontrolliert. Die Liste unterstützter Organisationen enthält auch die Organisationen, die durch Auflisten aller Objekte vom Typ `ObjectGroup` zurückgegeben werden.

Parameter	Beschreibung
<code>s</code>	Der Lighthouse-Kontext (die Sitzung) des aktuellen Benutzers.
<code>organizations</code>	Eine Liste eines oder mehrerer Organisationsnamen. Die Liste unterstützter Organisationen enthält auch die Organisationen, die durch Auflisten aller Objekte vom Typ <code>ObjectGroup</code> zurückgegeben werden.

Diese Methode gibt Folgendes zurück:

`true` – Der aktuell authentifizierte Identity Manager-Benutzer kontrolliert Organisationen in der Liste.

`false` – Der aktuell authentifizierte Identity Manager-Benutzer kontrolliert keine Organisationen in der Liste.

## Kapitel 5: Ansichten

### Kontotypen

Diese Identity Manager-Version bietet Unterstützung zur Zuordnung mehrerer Konten zu Benutzern auf einer Ressource mit *Kontotypen*. (ID-12697) Sie können jetzt wahlweise beim Zuweisen von Ressourcen zu Benutzern einen Kontotyp einer Ressource zuordnen. Dabei gelten jedoch die folgenden Einschränkungen:

- Jeder Ressource kann nur ein einziger Kontotyp zugewiesen werden.
- Benutzer können normalerweise nur einen Kontotyp besitzen.

Vor dem Zuweisen eines Kontotyps zu einer Ressource ist dieser Typ zunächst von einem Administrator zu definieren. Es muss darüber hinaus auch eine Identity-Regel definiert werden (Beispiele für Identity-Regeln finden Sie in `samples/identityRules.xml` for examples).

Identity Manager verwendet zum Zuweisen einer Regel zu einem Kontotyp den Untertyp `IdentityRule`. Diese Regel generiert die benötigten `Konten-IDs`. (Diese Regeln funktionieren ähnlich wie Identitätsvorlagen, sind jedoch in XPRESS implementiert und greifen auf die `LighthouseContext-API` zu).

Informationen darüber, wie Sie mit der Administratorbenutzeroberfläche von Identity Manager Kontotypen zu Ressourcen zuweisen, finden Sie im *Identity Manager Administration*.

### Auslassen des Kontotyps

Wenn der Kontotyp in einer Ressource weggelassen wird, weist Identity Manager den Standardkontotyp zu. Dies gewährleistet eine Abwärtskompatibilität. Wenn jedoch für keine Ressource ein Kontotyp definiert ist, wird diese Funktion deaktiviert.

Der Standardkontotyp nutzt die Identitätsvorlage. Sie können jedoch auch angeben, dass statt der Identitätsvorlage ein Standardtyp verwendet werden soll.

Der Standardkontotyp ist insofern speziell, als dass der Benutzer mehrere Konten dieses Typs zuweisen kann. In der Praxis ist das Zuweisen mehrerer Konten des gleichen Typs jedoch oft nicht sinnvoll.

### Änderungen in Ansichten

Die folgenden Änderungen, die an Identity Manager-Ansichten vorgenommen wurden, unterstützen Kontotypen.

- Die Ressourcenansicht besitzt jetzt das Attribut `accountType` (Liste). Jeder Eintrag ist ein Objekt mit dem Attribut `identityRule`, das die Regel, die zur Erstellung der `accountIds` für diesen Typ verwendet wurde, enthält.
- Das Attribut `resources` der Rollen- und Anwendungsansicht erlaubt jetzt die Verwendung qualifizierter Ressourcenzuweisungen. Die Syntax dieser qualifizierten Zuweisungen ist `<Ressourcenname>|<Kontotyp>`.
- Die Benutzeransicht enthält jetzt das Attribut `waveset.resourceAssignments`, das qualifizierte Ressourcenzuweisungen akzeptiert. (`waveset.resources` enthält nur unqualifizierte Referenzen.) Sie können alle diese Attribute ändern; in der Praxis ist es jedoch sinnvoll, nur `waveset.resourceAssignment` für Aufrüstungen und `waveset.resources` zum Schreibschutz zu ändern.)

Der Zugriff auf diese Objekte im Attribut `accounts` der Benutzeransicht hat sich nach dem Hinzufügen dieser neuen Funktion nicht geändert. Zur Indizierung der `accounts`-Liste sollten qualifizierte Ressourcennamen verwendet werden. So wählt das Konstrukt `accounts[Resource|Typ]` das Konto für diese Ressourcen- und Typkombination aus. Wenn Sie keinen Typ angeben, können Sie auf diese Objekte trotzdem noch mit `accounts[Resource]` zugreifen.

- Zugehörige Ansichten wie z.B. „Bereitstellung aufheben“ und „Passwort ändern“ nutzen diese Adressierungsart ebenfalls. Die Objekte in dieser Liste besitzen jetzt auch ein neues Attribut namens `accountType`, das den Kontotyp des Ressourcenkontos enthält.

### Ansicht „Delegierte Genehmiger“

In dieser Ansicht können Sie einen oder mehrere Identity Manager-Benutzer als delegierte Genehmiger für einen vorhandenen Genehmiger zuweisen. Dadurch können Genehmiger ihre Genehmigungsfähigkeiten einen bestimmten Zeitraum lang an Benutzer delegieren, die selbst keine Genehmiger sind. Zu den Attributen der höchsten Stufe gehören: (ID-12754).

**Hinweis** Außer dem Attribut „name“ enthält die Benutzeransicht die gleichen Attribute. Diese neuen Attribute sind im Namensraum `accounts[Lighthouse]` enthalten.

#### **name**

Der Benutzer, der Genehmigungen delegiert.

#### **delegateApproversTo**

Gibt an, an welchen Benutzer Genehmigungen delegiert werden sollen. Zu den gültigen Werten zählen „manager“, „selectedUsers“ oder „delegateApproversRule“.

#### **delegateApproversSelected**

- Wenn `selectedUsers` den Wert `delegateApproversRule` hat, werden hier die ausgewählten Benutzernamen aufgeführt.
- Wenn `delegatedApproversRule` den Wert `delegateApproversTo` hat, ist hier die ausgewählte Regel angegeben.
- Wenn `manager` den Wert `delegateApproversTo` hat, besitzt dieses Attribut keinen Wert.

#### **delegateApproversStartDate**

Das Datum, an dem die Delegierung von Genehmigungsfähigkeiten beginnen soll. Standardmäßig ist dieses Datum auf 12:01 des jeweiligen Tages gesetzt.

### delegateApproversEndDate

Das Datum, an dem die Delegation von Genehmigungsfähigkeiten enden soll. Standardmäßig ist dieses Datum auf 23:59 des jeweiligen Tages gesetzt.

Die Dokumentation zu Rollenansichten wurde wie folgt aktualisiert. (ID-12390).

### Rollenansicht

Dient zum Definieren von Rollenobjekten in Identity Manager.

Ist die Ansicht aktiviert, ruft sie den Workflow „Rolle verwalten“ auf. Standardmäßig speichert dieser Workflow lediglich die Ansichtsänderungen im Repository. Er enthält jedoch auch Ausgangspunkte für Genehmigungen und andere benutzerspezifische Anpassungen.

In der folgenden Tabelle sind die Attribute der höchsten Ebene für diese Ansicht aufgeführt.

Attribut	Bearbeitbar?	Datentyp	Erforderlich
name	Lesen/Schreiben	String	Ja
resources	Lesen/Schreiben	Liste	Nein
applications	Lesen/Schreiben	Liste	Nein
roles	Lesen/Schreiben	Liste	Nein
assignedResources	Lesen/Schreiben	Liste	Nein
notifications	Lesen/Schreiben	Liste	Nein
approvers	Lesen/Schreiben	Liste	Nein
properties	Lesen/Schreiben	Liste	
organizations	Lesen/Schreiben	Liste	Ja

Tabelle 1. Attribute für Rollenansichten

#### name

Der Name der Rolle. Entspricht dem Name des Role-Objekts im Identity Manager-Repository.

#### resources

Die Namen der lokal zugewiesenen Ressourcen.

#### applications

Die Namen der lokal zugewiesenen Anwendungen (Ressourcengruppen).

## Identity Manager Workflows, Forms, and Views

### roles

Die Namen der lokal zugewiesenen Rollen.

### assignedResources

Flache Liste aller zugewiesenen Ressourcen über Ressourcen, Anwendungen und Rollen.

Attribut	Bearbeitbar?	Datentyp
resourceName		String
name		String
attributes		Object

#### resourceName

Der Name der zugewiesenen Ressource.

#### name

IDer Ressourcenname oder die Ressourcen-ID (ID bevorzugt).

#### attributes

Die charakteristischen Eigenschaften der Ressource. Alle Unterattribute sind vom Datentyp „String“ und können bearbeitet werden.

Attribut	Beschreibung
name	Name des Ressourcenattributs
valueType	Typ des für dieses Attribut gesetzten Wertes. Zulässige Werte: Rule, text oder none.
requirement	Typ des von diesem Attribut gesetzten Wertes. Zulässige Werte: Regel, Text, Keiner, Wert, Mit Wert kombinieren, Mit Wert entfernen, Mit Wert kombinieren, vorhandenen Wert löschen, Autoritativ auf Wert setzen, Autoritativ mit Wert kombinieren, Autoritativ mit Wert kombinieren, vorhandenen Wert löschen.
rule	Ein Regelname, wenn „valueType“ auf „rule“ gesetzt ist.
value	Ein Wert, wenn „valueType“ auf „text“ gesetzt ist.

Tabelle 2. Attributoptionen (Rollenansicht)

- `notifications` -- Listet die Namen der Administratoren auf, die die Zuweisung dieser Rolle zu einem Benutzer genehmigen müssen.
- `approvers` -- Die Namen der Administratoren, die die Zuweisung dieser Rolle zu einem Benutzer genehmigen müssen.
- `properties` -- In dieser Regel gespeicherte benutzerdefinierte Eigenschaften.
- `organizations` -- Die Liste der Organisationen, in denen die Rolle verfügbar ist.
- Die Ansichten zu Ressourcenkonten (Ansichten „Benutzerbereitstellung aufheben“, „Deaktivieren“, „Aktivieren“, „Passwort“, „Benutzer umbenennen“, „Erneut bereitstellen“, and „Sperrung aufheben“) unterstützen jetzt zwei neue Optionen, mit denen Ressourcenkontenattribute für Benutzer abgerufen werden können. (ID-12482).
  - `fetchAccounts` – (Boolean) Wenn dieser Parameter auf „true“ gesetzt ist, enthält die Ansicht Kontenattribute für die dem Benutzer zugewiesenen Ressourcen.
  - `fetchAccountResources` – Ressourcennamen, die abgerufen werden können. Wenn hier nichts angegeben ist, werden alle zugewiesenen Ressourcen verwendet.

Diese Optionen können am Einfachsten als Formulareigenschaften gesetzt werden. (Weitere Informationen finden Sie in der Erläuterung der Ansicht „WorkItem List“ im Kapitel „Views“ in diesem Handbuch).

## Kapitel 6: XPRESS Language

- Die Funktion `instanceOf` ist gegenwärtig im Kapitel „XPRESS Language“ nicht dokumentiert. Diese Funktion ermittelt, ob ein Objekt eine Instanz des im Parameter `name` angegebenen Typs ist. (ID-12700).

`name` – Das Objekt, gegen das geprüft wird.

Diese Funktion gibt je nachdem, ob das Unterausdrucksobjekt eine Instanz des im Parameter `name` angegebenen Typs ist, den Wert 1 oder 0 („true“ oder „false“) zurück.

Der folgende Ausdruck gibt 1 zurück, da `ArrayList` ein List-Objekt ist.

```
<instanceof name="List">  
  <new class="java.util.ArrayList"/>  
</instanceof>
```

## Kapitel 8: HTML Display Components

- Die Beschreibung der Komponente `SortingTable` wurde wie folgt geändert:  
Dient zum Erstellen einer Tabelle, deren Inhalt nach Spaltenüberschrift sortiert werden kann. Der Inhalt dieser Tabelle wird durch untergeordnete Komponenten bestimmt. Erstellen Sie eine untergeordnete Komponente pro Spalte (definiert mit der Eigenschaft `columns`). Spalten sind in der Regel in einer `FieldLoop` enthalten.  
Diese Komponente unterstützt bei der Ausgabe der Tabellenzellen die Eigenschaften `align`, `valign` und `width` der untergeordneten Komponenten. (ID-12606).
- Identity Manager stellt jetzt die Anzeigekomponente `InlineAlert` bereit. (ID-12606).  
Diese zeigt ein Fehler-, Warn-, Erfolgs- oder Informationsdialogfeld an und befindet sich normalerweise am oberen Seitenrand. Durch Definition von untergeordneten Komponenten vom Typ `InlineAlert$AlertItem` können mehrere Meldungen in einem Hinweisdialgfeld angezeigt werden.  
Zu den Eigenschaften für diese Anzeigekomponente gehören:
  - `alertType` – Der Typ der anzuzeigenden Meldung. Diese Eigenschaft bestimmt die verwendeten Stile und Grafiken. Zulässige Werte sind „error“, „warning“, „success“ und „info“. Der Standardwert für diese Eigenschaft ist „info“. Diese Eigenschaft gilt nur für `InlineAlert`.
  - `header` – Der für das Hinweisdialgfeld anzuzeigende Titel. Dies kann entweder eine Zeichenfolge (String) oder ein Message-Objekt sein. Diese Eigenschaft gilt für `InlineAlert` oder `InlineAlert$AlertItem`.
  - `value` – Die anzuzeigende Meldung. Dies kann entweder eine Zeichenfolge (String) oder ein Message-Objekt sein. Diese Eigenschaft gilt für `InlineAlert` oder `InlineAlert$AlertItem`.
  - `linkURL` – Eine optionale URL, die am unteren Rand des Hinweisdialgfeldes angezeigt wird. Diese Eigenschaft gilt für `InlineAlert` oder `InlineAlert$AlertItem`.
  - `linkText` – Text für `linkURL`. Dies kann entweder eine Zeichenfolge (String) oder ein Message-Objekt sein. Diese Eigenschaft gilt für `InlineAlert` oder `InlineAlert$AlertItem`.
  - `linkTitle` – Titel für `linkURL`. Dies kann entweder eine Zeichenfolge (String) oder ein Message-Objekt sein. Diese Eigenschaft gilt für `InlineAlert` oder `InlineAlert$AlertItem`.

### Beispiele

#### Meldung mit einem Hinweis

```
<Field>
  <Display class="InlineAlert">
    <Property name="alertType" value="warning"/>
    <Property name="header" value="Data not Saved"/>
    <Property name="value" value="The data entered is not yet saved.
      Please click Save to save the information."/>
  </Display>
</Field>
```

#### Meldung mit mehreren Hinweisen

alertType sollte nur innerhalb der Eigenschaft InlineAlert definiert werden. Sie können für InlineAlert\$AlertItems andere Eigenschaften definieren.

```
<Field>
  <Display class="InlineAlert">
    <Property name="alertType" value="error"/>
  </Display>
  <Field>
    <Display class="InlineAlert$AlertItem">
      <Property name="header" value="Server Unreachable"/>
      <Property name="value" value="The specified server could not
        be contacted. Please view the logs for more information."/>
      <Property name="linkURL" value="viewLogs.jsp"/>
      <Property name="linkText" value="View logs"/>
      <Property name="linkTitle" value="Open a new window with
        the server logs"/>
    </Display>
  </Field>
  <Field>
    <Display class="InlineAlert$AlertItem">
      <Property name="header" value="Invalid IP Address"/>
      <Property name="value" value="The IP address entered is
        in an invalid subnet. Please use the 192.168.0.x subnet."/>
    </Display>
  </Field>
</Field>
```

## Identity Manager Workflows, Forms, and Views

- Identity Manager stellt jetzt die Azeigekomponente `Selector` bereit. (ID-12729).

Diese stellt ein Feld mit einem oder mehreren Werten (wie bei `Text`- oder `ListEditor`-Komponenten) mit darunter liegenden Suchfeldern bereit. Nach einem Suchvorgang zeigt Identity Manager Ergebnisse unter den Suchfeldern an und schreibt die Ergebnisse in das Wertefeld.

Im Gegensatz zu anderen Container-Komponenten besitzt `Selector` einen Wert (Das Feld, das mit den Suchergebnissen gefüllt wird). Bei den enthaltenen Feldern handelt es sich normalerweise um Suchkriterienfelder. `Selector` implementiert eine Eigenschaft zur Anzeige des Inhalts der Suchergebnisse.

Zu den Eigenschaften gehören:

- `fixedWidth` – Legt fest, ob die Komponente eine feste Breite haben soll (das gleiche Verhalten wie bei `MultiSelect`). (Boolean)
- `multivalued` – Legt fest, ob der Wert ein List-Objekt oder ein String ist. (Der Wert dieser Eigenschaft bestimmt, ob für den Wert ein `ListEditor`- oder Textfeld ausgegeben wird). (Boolean)
- `allowTextEntry` – Legt fest, ob Einträge aus der bereitgestellten Liste ausgewählt werden müssen oder manuell eingegeben werden können. (Boolean)
- `valueTitle` – Eine Beschriftung für die `value`-Komponente. (String)
- `pickListTitle` – Eine Beschriftung für die `picklist`-Komponente. (String)
- `pickValues` – die verfügbaren Werte in der `picklist`-Komponente (ist dieser Wert null, wird die Picklist nicht angezeigt). (List)
- `pickValueMap` – eine Matrix mit Beschriftungen für die Werte der Picklist. (Map oder List)
- `sorted` – Legt fest, dass die Werte in der Picklist sortiert werden sollen (bei mehreren und unsortierten Werten wird die Werteliste ebenfalls sortiert). (Boolean)
- `clearFields` – Die Felder, die beim Klicken auf die Schaltfläche „Löschen“ zurückgesetzt werden sollen. (List)

Die folgenden Eigenschaften gelten nur für Komponenten mit mehreren Werten:

- `ordered` – Legt fest, dass die Wertereihenfolge wichtig ist. (Boolean)
- `allowDuplicates` – Legt fest, ob die Werteliste Duplikate enthalten kann. (Boolean)
- `valueMap` – eine Matrix mit Beschriftungen für die Werte in der Liste. (Map)

Die folgenden Eigenschaften gelten nur für Komponenten mit einem Wert:

- `nullLabel` – Die Beschriftung, die für einen Nullwert verwendet werden soll. (String)
- Die Beschreibungen der `Select`- und `MultiSelect`-Komponenten wurden zur Erläuterung der Eigenschaft `caseInsensitive` wie folgt geändert. (ID-13364).

### MultiSelect-Komponente

Zeigt ein MultiSelection-Objekt an, das von Identity Manager als zwei nebeneinander liegende Textauswahlschlüsselfelder dargestellt wird, in denen eine bestimmte Anzahl an Werten vom einen Feld in das andere Feld verschoben werden kann. Die Werte im linken Feld werden von der Eigenschaft `allowedValues` definiert. Diese Werte werden oft dynamisch durch Aufruf einer Java-Methode wie z.B. `FormUtil.getResources` abgerufen. Die Werte im rechten Mehrfachauswahlfeld werden aus dem aktuellen Wert des zugehörigen Anzeigeattributs eingelesen, das durch den Feldnamen definiert ist.

Sie können die Formulartitel für jedes Feld in diesem MultiSelection-Objekt mithilfe der Eigenschaften `availableTitle` und `selectedTitle` setzen.

Wenn Sie eine MultiSelect-Komponente wünschen, die kein Applet verwendet, müssen Sie die Eigenschaft `noApplet` auf „true“ setzen.

**Hinweis** Wenn Identity Manager auf einem System mit Safari-Browser läuft, müssen Sie alle Formulare mit MultiSelect-Komponenten entsprechend benutzerspezifisch anpassen, um die Option „noApplet“ setzen zu können. Stellen Sie diese Option wie folgt ein:

```
<Display class="MultiSelect">  
  <Property name="noApplet" value="true"/>  
  ...
```

Zu den Eigenschaften für diese Anzeigekomponente gehören:

- `availableTitle` – Der Titel für das Feld der verfügbaren Werte.
- `selectedTitle` – Der Titel für das Feld der ausgewählten Werte.
- `ordered` – Legt fest, ob ausgewählte Einträge in der Liste nach oben oder unten bewegt werden können. Ein `true`-Wert legt fest, dass zum Bewegen ausgewählter Einträge nach oben bzw. unten zusätzliche Schaltflächen angezeigt werden.
- `allowedValues` – Die Werte im linken Feld des MultiSelection-Objekts. Dieser Wert muss eine Stringliste sein. **Hinweis:** Das Element `<Beschränkungen>` kann zum Einlesen von Werten in dieses Feld verwendet werden, ist jedoch verworfen.
- `sorted` – Legt fest, dass die Werte in beiden Feldern alphabetisch sortiert werden sollen.
- `noApplet` – Legt fest, ob die MultiSelect-Komponente mithilfe eines Applets oder zwei HTML-Standardauswahlfeldern implementiert wird. Der Standardwert ist `Applet`, da Applets lange Wertelisten besser verarbeiten können. Information zur Verwendung dieser Option auf Systemen mit Safari-Browser finden Sie im vorherigen Hinweis.

## Identity Manager Workflows, Forms, and Views

- `typeSelectThreshold` – (nur verfügbar, wenn `noApplet` auf „true“ gesetzt ist.) Legt fest, ob ein Type-ahead-Auswahlfeld unter der Liste `allowedValue` angezeigt wird. Wenn die Anzahl der Einträge im linken Auswahlfeld den von dieser Eigenschaft festgelegten Grenzwert erreicht, erscheint unter dem Auswahlfeld ein zusätzliches Texteingabefeld. Bei der Eingabe von Zeichen in dieses Textfeld werden im Auswahlfeld automatisch passende Einträge angezeigt, falls diese existieren. Wenn Sie beispielsweise `w` eingeben, geht das Auswahlfeld zum Eintrag, der mit `w` beginnt.
- `width` – Die Breite für das Feld der ausgewählten Werte (in Pixeln). Die Standardwert beträgt 150.
- `height` – Die Höhe für das Feld der ausgewählten Werte (in Pixeln). Die Standardwert beträgt 400.
- `caseInsensitive` -- Ermöglicht das Durchführen von Operationen, die Groß- und Kleinschreibung ignorieren.

### Select-Komponente

Zeigt ein Einfachauswahlobjekt an. Werte für das Listefeld müssen von der Eigenschaft `allowedValues` bereitgestellt werden.

Zu den Eigenschaften für diese Anzeigekomponente gehören:

- `allowedValues` – Die Liste auswählbarer Werte zur Anzeige im Listefeld.
- `allowedOthers` – Wenn dieser Wert gesetzt ist, werden Anfangswerte, die nicht in der `allowedValues`-Liste enthalten waren, akzeptiert und „stillschweigend“ in die Liste aufgenommen.
- `autoSelect` – Wenn dieser Wert auf `true`, gesetzt ist, wird der erste Wert in der Liste `allowedValues` durch diese Eigenschaft automatisch ausgewählt, wenn der Anfangswert für das Feld null ist.
- `caseInsensitive` -- Ermöglicht das Durchführen von Operationen, die Groß- und Kleinschreibung ignorieren.
- `multiple` – Wenn dieser Wert auf `true` gesetzt ist, können mehrere Werte ausgewählt werden.
- `nullLabel` – Legt den Text fest, der oben in der Liste angezeigt wird, wenn kein Wert ausgewählt ist.
- `optionGroupMap` – Ermöglicht die Ausgabe von Optionen in Gruppen mithilfe des Tags `<optgroup>`. Formatieren Sie die Map so, dass die Schlüssel der Maps die Gruppenlabels und die Elemente Listen auswählbarer Einträge sind. (Werte müssen zur Eigenschaft `allowedValues` gehören, um ausgegeben werden zu können.)
- `size` – (optional) Die Maximalanzahl der anzuzeigenden Zeilen. Wenn die Zeilenanzahl diesen Wert überschreitet, wird eine Bildlaufleiste hinzugefügt.
- `sorted` – Wenn dieser Wert auf `true` gesetzt ist, werden die Werte in der Liste sortiert.

○ `valueMap` – Ordnet Rohwerten angezeigten Werten zu.

Die Komponente unterstützt die Eigenschaften `command` und `onChange`.

- Die Erläuterung zur `DatePicker`-Komponente beschreibt die folgenden neuen Eigenschaften. (ID-14802).

Die HTML-Komponente `DatePicker` ermöglicht jetzt die Auswahl getrennter Datumsangaben. Sie können einen Datumszeitraum angeben, mit dessen Hilfe bestimmte Datumsangaben aus dem Kalender ausgewählt werden können.

`DatePicker` implementiert die folgenden beiden neuen Eigenschaften:

`SelectAfter` -- Beschränkt die auswählbaren Datumsangaben, die im Kalender angezeigt werden, auf Datumsangaben am oder nach dem eingegebenen Datum. Der Wert dieser Eigenschaft kann ein Datumsstring oder ein Java `Date`-Objekt sein.

```
<Property name="SelectAfter" value="**/**/****"/>
```

`SelectBefore` -- Beschränkt die auswählbaren Datumsangaben, die im Kalender angezeigt werden, auf Datumsangaben am oder vor dem eingegebenen Datum. Der Wert dieser Eigenschaft kann ein Datumsstring oder ein Java `Date`-Objekt sein.

```
<Property name="SelectBefore" value="**/**/****"/>
```

Bei Verwendung eines Formulars, das das Tag `<Display class="DatePicker">` implementiert, müssen diese Variablen zum Formular hinzugefügt werden, um den Datumszeitraum zu definieren. Wenn Sie diese Eigenschaften nicht einstellen, wird der Kalender nicht für auswählbare Datumsangaben beschränkt.

## Identity Manager Technical Deployment Overview

---

Die folgenden Erläuterungen zu zugehörigen Workflows, Formularen und JSPs gehören zum Überblick über die Architektur von *Identity Manager Technical Deployment Overview* (ID-7332).

### Prozessausführung

Wenn ein Benutzer Daten in einem Feld auf einer Seite eingibt und auf Speichern klickt, verarbeiten die Workflow- und Formularkomponenten die Daten gemeinsam.

Jede Seite in Identity Manager hat zugehörige Ansichten, Workflows und Formulare, welche die Datenverarbeitung übernehmen. Diese Workflow-, Ansichts- und Formularzuweisungen werden in den folgenden zwei Tabellen aufgelistet.

### Identity Manager-Prozesse für die Benutzeroberfläche

Die folgenden Tabellen enthalten die Formulare, Ansichten, Workflows und JSPs der Prozesse, die von diesen Seiten der Identity Manager-Benutzeroberfläche eingeleitet werden:

Benutzeroberfläche wieder aktivieren	Formular	Ansicht	Workflow
Hauptmenü	<ul style="list-style-type: none"> <li>• endUserMenu</li> <li>• Endbenutzermenü (Standard)</li> </ul>	Benutzer Die Ansicht ist schreibgeschützt. Auf dieser Seite können keine Änderungen vorgenommen werden	Kein
Passwort ändern	<ul style="list-style-type: none"> <li>• endUserChangePassword</li> <li>• Formular für die Passwortänderung (Standard)</li> </ul>	Passwort	<ul style="list-style-type: none"> <li>• changeUserPassword</li> <li>• Benutzer-Passwort ändern (Standard)</li> </ul>
Andere Kontoattribute ändern	<ul style="list-style-type: none"> <li>• endUserForm</li> <li>• Endbenutzerformular (Standard)</li> </ul>	Benutzer	Benutzer aktualisieren
Prozess-Status prüfen	<ul style="list-style-type: none"> <li>• endUserTaskList</li> <li>• Endbenutzeraufgabenliste (Standard)</li> </ul>	Liste Die Ansicht enthält Informationen zu den TaskInstance-Objekten, die vom Benutzer gestartet werden	Kein
Prozess-Status Diese Seite wird von der TaskViewResults-Klasse generiert	Kein	Kein	Kein
Verfügbare Prozesse	<ul style="list-style-type: none"> <li>• endUserLaunchList</li> <li>• Endbenutzerstartliste (Standard)</li> </ul>	Liste Die Ansicht enthält Informationen zu den TaskDefinition-Objekten, auf die der Benutzer zugreifen kann	Kein

## Identity Manager Technical Deployment Overview

Benutzeroberfläche wieder aktivieren	Formular	Ansicht	Workflow
Prozess starten Startet eine ausgewählte Aufgabendefinition	Von der Aufgabendefinition definiert	Prozess	Kein
Antworten auf Authentifizierungsfragen ändern	<ul style="list-style-type: none"> <li>• changeAnswers</li> <li>• Benutzerantworten ändern (Standardformular)</li> </ul>	ChangeUserAnswers	Kein
Selbsterkennung Kann nur mit vorhandenen Ressourcenkonten verbunden werden	<ul style="list-style-type: none"> <li>• selfDiscovery</li> <li>• Selbsterkennung (Standard)</li> </ul>	Benutzer	Benutzer aktualisieren
Posteingang	<ul style="list-style-type: none"> <li>• endUserWorkItemList</li> <li>• Endbenutzerarbeitselement (Standardliste)</li> </ul>	Liste Die Ansicht enthält Informationen zu Arbeitselementen, die dem aktuellen Benutzer direkt angehören	Kein
Posteingang-Element bearbeiten	Wird vom Arbeitselement angegeben oder automatisch generiert	WorkItem	Kein

### Prozesse der Administratorbenutzeroberfläche

Die folgenden Tabellen enthalten die Formulare, Ansichten, Arbeitsabläufe und JSPs der Prozesse, die von diesen Seiten der Identity Manager-Administratorbenutzeroberfläche eingeleitet werden:

## Identity Manager Technical Deployment Overview

Seite der Administratorbenutzeroberfläche	Formular	Ansicht	Workflow
Organisation erstellen und bearbeiten	<p>Zuordnung der Systemkonfiguration</p> <p>Je nach Kontext kann es sich um verschiedene Formulare handeln. Hierzu gehören:</p> <ul style="list-style-type: none"> <li>• Organisationsformular</li> <li>• Formular zum Umbenennen von Organisationen</li> <li>• Formular für Verzeichnisverbindungen</li> <li>• Formular für virtuelle Organisationen</li> <li>• Formular zum Aktualisieren von virtuellen Organisationen</li> </ul>	Org	Kein
Benutzer erstellen	<ul style="list-style-type: none"> <li>• userForm</li> <li>• Benutzer (Standardformular mit Registerkarten)</li> </ul>	Benutzer	<ul style="list-style-type: none"> <li>• createUser</li> <li>• Benutzer erstellen (Standard)</li> </ul>
Benutzer aktualisieren	<ul style="list-style-type: none"> <li>• userForm</li> <li>• Benutzer (Standardformular mit Registerkarten)</li> </ul>	Benutzer	<ul style="list-style-type: none"> <li>• updateUser</li> <li>• Benutzer aktualisieren (Standard)</li> </ul>
Ressourcenkonten des Benutzers deaktivieren	<ul style="list-style-type: none"> <li>• disableUser</li> <li>• Benutzer deaktivieren (Standard)</li> </ul>	Deaktivieren	<ul style="list-style-type: none"> <li>• disableUser</li> <li>• Benutzer deaktivieren (Standard)</li> </ul>
Benutzer umbenennen	<ul style="list-style-type: none"> <li>• renameUser</li> <li>• Benutzer umbenennen (Standardformular)</li> </ul>	RenameUser	<ul style="list-style-type: none"> <li>• renameUser</li> <li>• Benutzer umbenennen (Standard)</li> </ul>
Ressourcenkonten des Benutzers aktualisieren	<ul style="list-style-type: none"> <li>• reprovisionUser</li> <li>• Erneut bereitstellen (Standardformular)</li> </ul>	Erneut bereitstellen	<ul style="list-style-type: none"> <li>• updateUser</li> <li>• Benutzer aktualisieren (Standard)</li> </ul>

## Identity Manager Technical Deployment Overview

Seite der Administratorbenutzeroberfläche	Formular	Ansicht	Workflow
Sperre der Ressourcenkonten für den Benutzer aufheben	<ul style="list-style-type: none"> <li>• unlockUser</li> <li>• Sperre für Benutzer aufheben (Standard)</li> </ul>	Sperre aufheben	<ul style="list-style-type: none"> <li>• unlockUser</li> <li>• Sperre für Benutzer aufheben (Standard)</li> </ul>
Ressourcenkonten des Benutzers löschen	<ul style="list-style-type: none"> <li>• deprovisionUser</li> <li>• Aufheben der Bereitstellung (Standardformular)</li> </ul>	Bereitstellung aufheben	<ul style="list-style-type: none"> <li>• deleteUser</li> <li>• Benutzer löschen (Standard)</li> </ul>
Benutzer-Passwort ändern Verwendet denselben Workflow wie die Endbenutzer-GUI, jedoch ein anderes Formular	<ul style="list-style-type: none"> <li>• changePassword</li> <li>• Benutzerpasswort ändern (Standardformular)</li> </ul>	ChangeUser Password	<ul style="list-style-type: none"> <li>• changeUserPassword</li> <li>• Benutzer-Passwort ändern (Standard)</li> </ul>
Benutzerpasswort zurücksetzen	<ul style="list-style-type: none"> <li>• resetPassword</li> <li>• Benutzerpasswort zurücksetzen (Standardformular)</li> </ul>	ResetUserPassword	<ul style="list-style-type: none"> <li>• changeUserPassword</li> <li>• Benutzer-Passwort ändern (Standard)</li> </ul>
Mein Passwort ändern Ansicht, Formular und Workflow wie beim Ändern des Endbenutzerpassworts, jedoch andere JSP	<ul style="list-style-type: none"> <li>• endUserChangePassword</li> <li>• Formular für die Passwortänderung (Standard)</li> </ul>	Password	<ul style="list-style-type: none"> <li>• changeUserPassword</li> <li>• Benutzer-Passwort ändern (Standard)</li> </ul>
Meine Antworten ändern Ansicht und Formular wie beim Ändern der Endbenutzerantworten, jedoch andere JSP	<ul style="list-style-type: none"> <li>• changeAnswers</li> <li>• Benutzerantworten ändern (Standardformular)</li> </ul>	ChangeUserAnswers	Kein
Genehmigungen	<ul style="list-style-type: none"> <li>• workItemList</li> <li>• Arbeitselemente (Standardliste)</li> <li>• Standardformular enthält Bestätigung des Arbeitselements</li> </ul>	WorkItemList	Kein

## Identity Manager Technical Deployment Overview

Seite der Administratorbenutzeroberfläche	Formular	Ansicht	Workflow
Arbeitselement bearbeiten Das Einchecken der Ansichtsergebnisse für Arbeitselemente in der Wiederaufnahme des erstellenden Workflow, wobei kein Workflow für den Eincheckvorgang des Arbeitselements erstellt wurde.	Wird vom Arbeitselement angegeben oder automatisch generiert	WorkItem	Kein
Aufgabe starten Startet eine ausgewählte Aufgabendefinition	Von der Aufgabendefinition definiert	Prozess	Kein
Geplante Aufgaben erstellen und aktualisieren	Keine Systemkonfigurationszuordnung, Standardformular für den Aufgabenzeitplan, kombiniert mit dem Formular für die Aufgabendefinition  Dieses Formular wird aus den Formularen für die Aufgabendefinition und dem Aufgabenzeitplan als Wrapper generiert	TaskSchedule	Kein

## Identity Manager Technical Deployment Overview

Seite der Administratorbenutzeroberfläche	Formular	Ansicht	Workflow
Rolle zum Erstellen und Bearbeiten	Keine Systemkonfigurationszuordnung Die Standardformulare für die Rolle und das Umbenennen der Rolle sind kontextabhängig	Rolle	<ul style="list-style-type: none"> <li>• manageRole</li> <li>• Rolle verwalten (Standard)</li> </ul>
Ressource bearbeiten	Keine Systemkonfigurationszuordnung, kontextabhängig, mögliche Formulare: <ul style="list-style-type: none"> <li>• Ressourcenkontopasswort ändern</li> <li>• Ressourcenkontopasswort zurücksetzen</li> <li>• Ressourcenrichtlinien bearbeiten</li> <li>• Ressource umbenennen</li> <li>• Ressourcenassistent &lt;Ressourcentyp&gt;</li> <li>• Ressourcenassistent.</li> </ul> Ermöglicht typspezifische Assistentenformulare, standardmäßig der Ressourcenassistent	Ressource	<ul style="list-style-type: none"> <li>• manageResource</li> <li>• Ressource verwalten (Standard)</li> </ul>
Fähigkeit bearbeiten	changeCapabilities, Benutzerfunktionen ändern (Standardformular)	ChangeUser Capabilities	Kein

## JSPs (Java Server Pages) und ihre Rolle in Identity Manager

Die folgenden Tabellen beschreiben die System-JSPs und deren Seiten für die Administratorbenutzeroberfläche und Benutzeroberfläche.

### JSPs für die Identity Manager-Benutzeroberfläche

wieder aktivieren	Zugewiesene JSP
Hauptmenü	user/main.jsp
Passwort ändern	user/changePassword.jsp
Andere Kontoattribute ändern	user/changeAll.jsp
Prozess-Status prüfen	user/processStatusList.jsp
Prozess-Status	user/processStatus.jsp
Verfügbare Prozesse	user/processList.jsp
Prozess starten	user/processLaunch.jsp
Antworten auf Authentifizierungsfragen ändern	user/changeAnswers.jsp
Selbsterkennung	user/selfDiscover.jsp
Posteingang	user/workItemList.jsp
Posteingang-Element bearbeiten	user/workItemEdit.jsp

### JSPs für die Administratorbenutzeroberfläche

wieder aktivieren	Zugewiesene JSP
Organisation erstellen und bearbeiten	security/orgedit.jsp
Benutzer erstellen	account/modify.jsp
Benutzer aktualisieren	account/modify.jsp
Ressourcenkonten des Benutzers deaktivieren	account/resourceDisable.jsp
Benutzer umbenennen	account/renameUser.jsp
Ressourcenkonten des Benutzers aktualisieren	account/resourceReprovision.jsp
Sperre der Ressourcenkonten für den Benutzer aufheben	admin/resourceUnlock.jsp
Ressourcenkonten des Benutzers löschen	account/resourceDeprovision.jsp
Benutzer-Passwort ändern	admin/changeUserPassword.jsp

wieder aktivieren	Zugewiesene JSP
Benutzerpasswort zurücksetzen	admin/resetUserPassword.jsp
Mein Passwort ändern	admin/changeself.jsp
Meine Antworten ändern	admin/changeAnswers.jsp
Genehmigungen	approval/approval.jsp
Arbeitselement bearbeiten	approval/itemEdit.jsp
Aufgaben starten	task/taskLaunch.jsp
Geplante Aufgaben erstellen und aktualisieren	task/editSchedule.jsp
Rolle zum Erstellen und Bearbeiten	roles/applicationmodify.jsp
Ressource bearbeiten	resources/modify.jsp
Fähigkeit bearbeiten	account/modifyCapabilities.jsp

## Anhang A, Konfigurationsobjekte bearbeiten

In der Liste der Standardwerte für QueryableAttrNames auf Seite A-4 fehlt `idmManager`.

## Identity Manager 6.0 Resources Reference

---

- Die Liste „Supported Account Attributes“ unter „Resources Reference > Active Directory > Account Attributes > Account Attribute Support“ ist in der PDF-Version des Dokuments aktueller als bei der HTML-Version. Bitte konsultieren Sie die PDF-Version. (ID-12630).
- Der oberste Knoten der Identity Manager 6.0 Resources Reference 2005Q4M3 unter der folgenden URL enthält keinen Verweis auf den Abschnitt „Domino“: (ID-12636).

<http://docs.sun.com/app/docs/doc/819-4520>

Sie finden den Abschnitt „Domino“ durch Öffnen von „Contents“ in diesem Knoten oder unter der folgenden URL:

[http://docs.sun.com/source/819-4520/Domino\\_Exchange.html#wp999317](http://docs.sun.com/source/819-4520/Domino_Exchange.html#wp999317)

### Access Manager Adapter

Schritt 5 in "General Configuration" muss wie folgt lauten:

5. Fügen Sie zur Datei `java.security` die folgenden Zeilen hinzu, falls sie nicht schon vorhanden sind:

```
security.provider.2=com.ibm.crypto.provider.IBMJCE
security.provider.3=com.ibm.net.ssl.internal.ssl.Provider
```

Die Zahl nach „security.provider“ in jeder Zeile gibt die Reihenfolge an, in der Java SecurityProvider-Klassen abfragt und muss eindeutig sein. Die Zahlenfolge kann je nach Umgebung verschieden sein. Wenn in der Datei `java.security` bereits mehrere SecurityProvider vorhanden sind, sollten Sie die neuen SecurityProvider in der oben aufgeführten Reihenfolge einfügen und die bereits vorhandenen SecurityProvider entsprechend umnummerieren. Entfernen Sie keine vorhandenen SecurityProvider und duplizieren Sie diese nicht. (ID-12044).

### Active Directory Adapter

Active Directory unterstützt jetzt die Binärattribute `thumbnailPhoto` (Windows 2000 Server und neuer) und `jpegPhoto` (Windows 2003).

### BridgeStream SmartRoles-Adapter

Identity Manager bietet jetzt einen BridgeStream SmartRoles-Ressourcenadapter, der Benutzer in SmartRoles bereitstellt. Dieser Adapter platziert Benutzer in den passenden Organisationen innerhalb von SmartRoles, sodass SmartRoles ermitteln kann, welche Business-Rollen diese Benutzer haben sollten.

Beim Abrufen von Benutzern aus SmartRoles ruft der Adapter auch die Business-Rollen der Benutzer ab. Diese Business-Rollen dienen in Identity Manager zur Ermittlung der Identity Manager-Rollen, -Ressourcen, -Attribute und -Zugriffe, die einem Benutzer zugewiesen werden sollen.

Darüber hinaus kann SmartRoles mithilfe von Active Sync Benutzerdaten ändern. Sie können SmartRoles-Benutzer in Identity Manager laden und miteinander harmonisieren.

Ausführliche Informationen zu diesem Adapter finden Sie im Kapitel *Sun Java™ System Identity Manager Resources Reference Addendum*. (ID-12714).

### ClearTrust-Adapter

- Der ClearTrust-Ressourcenadapter unterstützt jetzt ClearTrust Version 5.5.2.
  - Die Schritte 2 und 3 im Abschnitt „Identity Manager Installation Notes“ müssen wie folgt lauten (ID-12906):
1. Kopieren Sie die Datei `ct_admin_api.jar` von der Clear Trust-Installations-CD in das Verzeichnis `WEB-INF\lib`.
  2. Bei Verwendung von SSL müssen Sie die folgenden Dateien in das Verzeichnis `WEB-INF\lib` kopieren.

**Hinweis** Wenn Sie eine Bereitstellung für eine RSA Clear Trust 5.5.2-Ressource durchführen, sind zur SSL-Kommunikation keine weiteren Bibliotheken erforderlich.

- `asn1.jar`
- `certj.jar`
- `jce1_2-do.jar`
- `jcet.jar`
- `jnet.jar`
- `jsafe.jar`
- `jsaveJCE.jar`
- `jsse.jar`
- `rsajsse.jar`
- `sslj.jar`

### Datenbanktabellen-Adapter

Dieser Adapter unterstützt binäre Datentypen wie z.B. BLOBs, in Oracle. Die entsprechenden Attribute sind in der Schemazuordnung als binär zu kennzeichnen. Zu den Binärattributen gehören beispielsweise Grafikdateien, Audiodateien und Zertifikate.

## Flat File Active Sync-Adapter

- Administratoren benötigen für das Verzeichnis, in dem sich die Flat File befindet, Lese- und Schreibzugriff. Wenn der Active Sync-Parameter **Nur Unterschiede verarbeiten** aktiviert ist, benötigen diese Benutzer darüber hinaus noch eine Löschberechtigung.

Zusätzlich dazu muss das Administratorkonto für das im Active Sync-Feld **Protokolldateipfad** angegebene Verzeichnis Lese-, Schreib- und Löschberechtigung haben. (ID-12477).

- Bei Flat Files im LDIF-Format können Binärattribute wie Grafikdateien, Audiodateien und Zertifikate angegeben werden. Binärattribute werden für CSV-Dateien und Dateien mit Pipe-Begrenzern nicht unterstützt.

## HP OpenVMS-Adapter

Identity Manager bietet jetzt einen HP OpenVMS-Ressourcenadapter, der VMS Version 7.0 und höher unterstützt. Ausführliche Informationen zu diesem Adapter finden Sie im Kapitel *Sun Java™ System Identity Manager Resources Reference Addendum*. (ID-8556).

## JMS Listener-Adapter

Der JMS Listener-Adapter unterstützt jetzt statt asynchroner die synchrone Meldungsverarbeitung. Infolgedessen muss der zweite Abschnitt im Kapitel „Connections“ der „Usage Notes“ wie folgt lauten:

Der JMS Listener-Adapter arbeitet im Synchronmodus. Er erstellt für die im Feld **JNDI-Name für das Ziel** angegebene Queue bzw. das Themenziel einen synchronen Message Consumer. In jedem Abfrageintervall empfängt und verarbeitet der Adapter alle verfügbaren Meldungen. Meldung können (optional) durch Definition eines gültigen JMS-Meldungsauswahlstrings im Feld **Meldungsauswahl** zusätzlich qualifiziert werden.

Der Abschnitt „Message Mapping“ muss Folgendes enthalten:

Wenn der Adapter eine qualifizierte Meldung verarbeitet, wird die empfangene JMS-Meldung mithilfe des im Feld **Meldungszuordnung** angegebenen Verfahrens zuerst in eine Zuordnung bezeichneter Werte konvertiert. Diese resultierende Zuordnung wird als *Meldungs-Werte-Zuordnung* bezeichnet.

Die Meldungs-Werte-Zuordnung wird dann mithilfe der Schemazuordnung für Kontoattribute in eine Active Sync-Zuordnung umgewandelt. Wenn der Adapter Kontoattribute besitzt, durchsucht er die Meldungs-Werte-Zuordnung nach Schlüsselnamen, die auch in der Schemazuordnung als Benutzerressourcenattribute

vorkommen. Falls vorhanden, werden die entsprechenden Werte in die Active Sync-Zuordnung kopiert. Der Eintragsname in der Active Sync-Zuordnung wird jedoch in den Namen umgewandelt, der in der Spalte „Identity System-Benutzerattribut“ der Schemazuordnung angegeben ist.

Wenn die Meldungs-Werte-Zuordnung einen Eintrag besitzt, der mithilfe der Schemazuordnung für Kontoattribute nicht umgewandelt werden kann, wird der Eintrag aus der Meldungs-Werte-Zuordnung unverändert in die Active Sync-Zuordnung kopiert.

## LDAP-Adapter

### Unterstützung für binäre Kontoattribute

Es werden jetzt die folgenden binären Kontoattribute aus der Objektklasse „inetOrgPerson“ unterstützt:

Ressourcen-Benutzerattribut	LDAP-Syntax	Beschreibung
audio	Audio	Eine Audiodatei.
jpegPhoto	JPEG	Ein Bild im JPEG-Format.
userCertificate	certificate	Ein Zertifikat im Binärformat.

Andere Binärattribute werden möglicherweise unterstützt, sie wurden jedoch nicht getestet.

### Deaktivieren und Aktivieren von Konten

Mit dem LDAP-Adapter können Konten einer LDAP-Ressource mit verschiedenen Methoden deaktiviert werden. Deaktivieren Sie Konten mithilfe eines der folgenden Verfahren.

#### Ändern des Passworts in einen unbekanntes Wert

Wenn Sie Konten durch Ändern des Passworts in einen unbekanntes Wert deaktivieren wollen, lassen Sie die Felder **LDAP Aktivierungsmethode** und **LDAP Aktivierungsparameter** leer. Dies ist das Standardverfahren zum Deaktivieren von Konten. Das betreffende Konto kann durch Zuweisen eines neuen Passworts neu aktiviert werden.

## Identity Manager 6.0 Resources Reference

### Zuweisen der Rolle `nsmanageddisabledrole`

Wenn Sie die LDAP-Rolle `nsmanageddisabledrole` zum Deaktivieren und Aktivieren von Konten nutzen wollen, ist die LDAP-Ressource wie folgt zu konfigurieren:

1. Setzen Sie auf der Seite „Ressourcenparameter“ das Feld **LDAP Aktivierungsmethode** auf `nsmanageddisabledrole`.
2. Setzen Sie das Feld **LDAP Aktivierungsparameter** auf `IDMAttribute=CN=nsmanageddisabledrole,baseContext`. (*IDMAttribute* wird im Schema im nächsten Schritt angegeben.)
3. Fügen Sie auf der Seite „Kontoattribute“ als Identity System-Benutzerattribut den Wert *IDMAttribute* hinzu. Setzen Sie das Ressourcen-Benutzerattribut auf `nsroledn`. Das Attribut muss den Datentyp „String“ besitzen.
4. Erstellen Sie auf der LDAP-Ressource eine Gruppe „nsAccountInactivationTmp“ und weisen Sie als Mitgliedsparameter `CN=nsdisabledrole,baseContext` zu.

LDAP-Konten können jetzt deaktiviert werden. Überprüfen Sie das Attribut `nsaccountlock` mithilfe der LDAP-Konsole. Besitzt dieses Attribut den Wert `true`, ist das betreffende Konto gesperrt.

Bei einer späteren Neuaktivierung des Kontos wird es aus dieser Rolle entfernt.

### Setzen des Attributs `nsAccountLock`

Wenn Sie das Attribut `nsAccountLock` zum Deaktivieren und Aktivieren von Konten nutzen wollen, ist die LDAP-Ressource wie folgt zu konfigurieren:

1. Setzen Sie auf der Seite „Ressourcenparameter“ das Feld **LDAP Aktivierungsmethode** auf `nsaccountlock`.
2. Setzen Sie das Feld **LDAP Aktivierungsparameter** auf `IDMAttribute=true`. (*IDMAttribute* wird im Schema im nächsten Schritt angegeben.) z.B. `accountLockAttr=true`.
3. Fügen Sie auf der Seite „Kontoattribute“ den im Feld **LDAPAktivierungsparameter** angegebenen Wert als Identity System-Benutzerattribut hinzu. Setzen Sie das Ressourcen-Benutzerattribut auf `nsaccountlock`. Das Attribut muss den Datentyp „String“ besitzen.
4. Setzen Sie das LDAP-Attribut `nsAccountLock` für die Ressource auf `true`. Identity Manager setzt `nsaccountlock` beim Deaktivieren eines Kontos auf „true“. Außerdem wird davon ausgegangen, dass bereits existierende LDAP-Benutzer, für die `nsaccountlock` auf „true“ gesetzt ist, deaktiviert sind. Wenn `nsaccountlock` einen anderen Wert als „true“ besitzt (einschl. Null), gilt der Benutzer für das System als aktiviert.

### Deaktivierung von Konten ohne die Attribute `nsmanageddisabledrole` und `nsAccountLock`

Falls die Attribute `nsmanageddisabledrole` und `nsAccountLock` auf Ihrem Verzeichnisserver nicht verfügbar sind, dieser aber eine ähnliche Methode zur Deaktivierung von Konten nutzt, geben Sie in das Feld **LDAP Aktivierungsmethode** einen der folgenden Klassennamen ein. Je nach Klasse ist der im Feld **LDAP Aktivierungsparameter** einzugebende Wert unterschiedlich.

Klassenname	Wann sollte er verwendet werden?
<code>com.waveset.adapter.util.ActivationByAttributeEnableFalse</code>	<p>Der Verzeichnisserver aktiviert ein Konto, indem er ein Attribut auf „false“ setzt. Konten werden durch Setzen dieses Attributs auf „true“ deaktiviert.</p> <p>Fügen Sie dieses Attribut zur Schemazuzuordnung hinzu. Geben Sie dann in das Feld Identity ManagerLDAP Aktivierungsparameter den (links in der Schemazuzuordnung definierten) <b>-Namen für das Attribut</b> ein.</p>
<code>com.waveset.adapter.util.ActivationByAttributeEnableTrue</code>	<p>Der Verzeichnisserver aktiviert ein Konto, indem er ein Attribut auf „true“ setzt. Konten werden durch Setzen dieses Attributs auf „false“ deaktiviert.</p> <p>Fügen Sie dieses Attribut zur Schemazuzuordnung hinzu. Geben Sie dann in das Feld <b>LDAP Aktivierungsparameter</b> den (links in der Schemazuzuordnung definierten) Identity Manager-Namen für das Attribut ein.</p>
<code>com.waveset.adapter.util.ActivationByAttributePullDisablePushEnable</code>	<p>Identity Manager aktiviert Konten durch Abrufen eines Attribut-Wert-Paares von LDAP. Konten werden wieder aktiviert, indem das betreffende Attribut-Wert-Paar an LDAP gesendet wird.</p> <p>Fügen Sie dieses Attribut zur Schemazuzuordnung hinzu. Geben Sie das Attribut-Wert-Paar dann in das Feld <b>LDAP Aktivierungsparameter</b> ein. Verwenden Sie den (links in der Schemazuzuordnung definierten) Identity Manager-Namen für das Attribut.</p>

## Identity Manager 6.0 Resources Reference

Klassenname	Wann sollte er verwendet werden?
com.waveset.adapter.util. ActivationByAttributePushDisabl ePullEnable	Identity Manager deaktiviert Konten durch Senden eines Attribut-Wert-Paares an LDAP. Konten werden wieder aktiviert, indem das betreffende Attribut-Wert-Paar von LDAP abgerufen wird.  Fügen Sie dieses Attribut zur Schemazuordnung hinzu. Geben Sie das Attribut-Wert-Paar dann in das Feld <b>LDAP Aktivierungsparameter</b> ein. Verwenden Sie den (links in der Schemazuordnung definierten) Identity Manager-Namen für das Attribut.
com.waveset.adapter.util. ActivationNsManagedDisabledR ole	Das Verzeichnis nutzt zur Ermittlung des Kontostatus eine spezifische Rolle. Wenn diesem Konto diese Rolle zugewiesen ist, wird es deaktiviert.  Fügen Sie diesen Rollennamen zur Schemazuordnung hinzu. Geben Sie den Wert dann in das Feld <b>LDAP Aktivierungsparameter</b> im folgenden Format ein:  <i>IDMAttribut=CN=Rollenname,Basiskontext</i>  <i>IDMAttribut</i> ist der (links in der Schemazuordnung definierte) Identity Manager-Name für die Rolle.

## Mainframe-Adapter (ACF2, Natural, RACF, Top Secret)

Die Emulator-Klassenbibliothek von Attachmate Reflection for the Web (Reflection ECL) ermöglicht die Herstellung einer Verbindung zu einer Mainframe-Ressource. Diese Bibliothek ist mit der IBM Host on Demand-API kompatibel. Befolgen Sie sämtliche Installationsanweisungen des Produktherstellers. Führen Sie dann die unter "Installationshinweise" und "SSL-Konfiguration" beschriebenen Schritte durch.

### Installationshinweise

Gehen Sie wie folgt vor, um mit Attachmate Reflection ECL Verbindungen einzurichten:

1. Fügen Sie die Ressource, wie in *Identity Manager Resources Reference* beschrieben, in die Identity Manager -Ressourcenliste ein.
2. Kopieren Sie die entsprechenden JAR-Dateien in das Verzeichnis `WEB-INF/lib` Ihrer Identity Manager-Installation.
  - `RWebSDK.jar`
  - `wrqtls12.jar`
  - `profile.jar`

3. Fügen Sie folgende Definitionen in die Datei `Waveset.properties` ein, um festzulegen, welcher Dienst die Terminalsitzung verwaltet:

```
serverSettings.serverId.mainframeSessionType=Wert
serverSettings.default.mainframeSessionType=Wert
```

*Wert* kann wie folgt gesetzt werden:

- 1 — IBM Host On-Demand (HOD)
- 3 — Attachmate WRQ

Wenn diese Eigenschaften nicht ausdrücklich gesetzt sind, versucht Identity Manager zuerst WRQ und anschließend HOD zu verwenden.

4. Bei der Installation der Attachmate-Bibliotheken auf einem WebSphere-Anwendungsserver müssen Sie zur Datei `WebSphere/AppServer/configuration/config.ini` die Eigenschaft `com.wrq.profile.dir=Bibliotheksverzeichnis` hinzufügen.

Dadurch findet der Attachmate-Code die Lizenzdatei.

5. Starten Sie den Anwendungsserver neu, damit die Änderungen der Datei `Waveset.properties` wirksam werden können.

Führen Sie die unter *SSL-Konfiguration* beschriebenen Schritte durch.

### SSL-Konfiguration

Die Emulator-Klassenbibliothek von Attachmate Reflection for the Web (Reflection ECL) ist mit der IBM Host on Demand-API kompatibel. Befolgen Sie sämtliche Installationsanweisungen des Produktherstellers. Führen Sie dann in Identity Manager die folgenden Schritte durch.

1. Falls für die Ressource noch kein Ressourcenattribut namens Session Properties vorhanden ist, fügen Sie dem Ressourcenobjekt mithilfe der Identity Manager-IDE oder der Debug-Seiten dieses Attribut hinzu. Fügen Sie folgende Definition in den Abschnitt `<ResourceAttributes>` ein:

```
<ResourceAttribute name="Session Properties" displayName="Session
Properties" description="Session Properties" multi="true">
</ResourceAttribute>
```

2. Fügen Sie dem Ressourcenattribut Session Properties auf der Seite „Ressourcenparameter“ für die Ressource die folgenden Werte hinzu:

```
encryptStream
true
hostURL
tn3270://Host-Name:SSLport
keystoreLocation
Pfad_zur_Trusted_ps.pfx-Datei
```

# Oracle/Oracle ERP-Adapter

Das Kapitel „Oracle/Oracle ERP“ in der *Identity Manager Resources Reference* wurde für diese Version in zwei getrennte Kapitel aufgeteilt. Diese beiden neuen Kapitel finden Sie im *Sun Java™ System Identity Manager Resources Reference Addendum*. (ID-12758).

## Oracle-Adapter

- Die Unterstützung für Oracle 8i wurde irrtümlich aus der Adaptertabelle und aus dem Abschnitt „Oracle Adapter“ in Kapitel 1 der „Identity Manager Resources Reference“ entfernt. Identity Manager unterstützt Oracle 8i als Ressource. (ID-13078).
- Der Abschnittsname `updateableAttributes` wurde in `updatableAttributes` berichtigt (in Schritt 1 des Abschnitts „Cascade Deletes“ dieses Kapitels (ID-13075):
- Das Kontoattribut „noCascade“ legt fest, ob beim Löschen von Benutzern Cascade Drops durchgeführt werden sollen. Standardmäßig werden Cascade Drops ausgeführt. Zum Deaktivieren von Cascade Drops fügen Sie im Abschnitt `updatableAttributes` des Systemkonfigurationsobjekts einen Eintrag hinzu:
- Die Beschreibung des Kontoattributs `oracleTempTSQuota` sollte wie folgt lauten:

Die vom Benutzer einstellbare Maximalkapazität für temporäre Tablespaces. Wenn das Attribut in der Schemazuordnung erscheint, wird das Kontingent stets auf den temporären Tablespace gesetzt. Bei Entfernung des Attributs aus der Schemazuordnung werden die Kontingente nicht auf den temporären Tablespace gesetzt. Dieses Attribut muss bei Adaptern, die mit Oracle 10gR2-Ressourcen kommunizieren, entfernt werden. (ID-12843).

## Oracle ERP-Adapter

- Der Oracle ERP-Adapter bietet jetzt das Kontoattribut `employee_number`. Dieses Attribut repräsentiert eine Mitarbeiternummer (`employee_number`) aus der Tabelle `per_people_f` (ID-12796):
  - Wenn Sie beim Erstellen einen Wert eingeben, versucht der Adapter, aus der Tabelle `per_people_f` einen Benutzerdatensatz abzurufen, `person_id` in die zum Erstellen verwendete API einzulesen und dann `person_id` in die Spalte `employee_id` der Tabelle `fnd_user` einzufügen.
  - Wenn beim Erstellen `employee_number` nicht eingegeben wird, wird diese Verknüpfung nicht durchgeführt.
  - Wenn beim Erstellen `employee_number` eingegeben und dieser Wert nicht gefunden wird, generiert der Adapter eine Ausnahme.

- Der Adapter versucht, `employee_number` in einer `getUser`-Methode zurückzugeben, wenn sich `employee_number` im Adapterschema befindet.
- Das Kontoattribut `npw_number` unterstützt Kontingentausführungen. Es funktioniert genau wie `employee_number`. Die Attribute `employee_number` und `npw_number` schließen sich gegenseitig aus. Wenn beim Erstellen beide Attribute eingegeben werden, hat das Attribut `employee_number` Vorrang. (ID-16507).

### Zuständigkeitsbereiche für die Überwachung

Der Oracle ERP-Adapter wurde zur Unterstützung von Überprüfungsfunktionen um mehrere Attribute erweitert. (ID-11725).

Zur Überwachung von Unterelementen (wie z. B. Formularen und Funktionen) von Zuständigkeitsbereichen, die Benutzern zugewiesen sind, müssen Sie zur Schemazuordnung das Attribut `auditorObject` hinzufügen. `auditorObject` ist ein komplexes Attribut, das eine Reihe von Responsibility-Objekten enthält. Die folgende Attribute werden immer in einem Responsibility-Objekt zurückgegeben:

- `responsibility`
- `userMenuNames`
- `menuIds`
- `userFunctionNames`
- `functionIds`
- `formIds`
- `formNames`
- `userFormNames`
- `readOnlyFormIds`
- `readWriteOnlyFormIds`
- `readOnlyFormNames`
- `readOnlyUserFormNames`
- `readWriteOnlyFormNames`
- `readWriteOnlyUserFormNames`
- `functionNames`
- `readOnlyFunctionNames`
- `readWriteOnlyFunctionNames`

**Hinweis** Die Attribute „readOnly“ und „readWrite“ werden durch Abfragen der Spalte „PARAMETERS“ in der Tabelle „fnd\_form\_functions“ nach einem der folgende Werte identifiziert:

## Identity Manager 6.0 Resources Reference

- QUERY\_ONLY= YES
- QUERY\_ONLY= „YES“
- QUERY\_ONLY = YES
- QUERY\_ONLY = „YES“
- QUERY\_ONLY= Y
- QUERY\_ONLY= „Y“
- QUERY\_ONLY = Y
- QUERY\_ONLY = „Y“

Wenn der Ressourcenparameter **Dokumentationssatz und/oder Organisation zurückgeben** auf TRUE gesetzt ist, werden darüber hinaus die folgenden Attribute zurückgegeben:

- setOfBooksName
- setOfBooksId
- organizationalUnitName
- organizationalUnitId

Mit der Ausnahme der Attribute *responsibility*, *setOfBooksName*, *setOfBooksId*, *organizationalUnitId* und *organizationalUnitName* müssen die Attributnamen den Kontoattributnamen entsprechen, die zur Schemazuordnung hinzugefügt werden können. Die Kontoattribute enthalten einen Sammelsatz an Werten, die Benutzern zugewiesen werden. Die in den *responsibility*-Objekten enthaltenen Attribute gelten nur für den jeweiligen Zuständigkeitsbereich.

In der Ansicht „auditorResps[]“ haben Sie Zugriff auf die Attribute des jeweiligen Responsibility-Objekts. Im folgenden Formularausschnitt werden alle aktiven, einem Benutzer zugewiesenen Zuständigkeitsbereiche (und ihre Attribute) zurückgegeben.

```
<defvar name="audObj">
  <invoke name="get">
    <ref>accounts[Oracle ERP 11i VIS].auditorObject</ref>
  </invoke>
</defvar>
<!-- this returns list of responsibility objects -->
<defvar name="audObj">
  <invoke name="get">
    <ref>audObj</ref>
    <s>auditorResps[*]</s>
  </invoke>
</defvar>
```

Beispiel:

- `auditorResps[0].responsibility` gibt den Namen des ersten Responsibility-Objekts zurück.
- `auditorResps[0].formNames` gibt die Formularnamen (formNames) des ersten Responsibility-Objekts zurück.

### Unterstützung für Oracle EBS 12

Der Oracle ERP-Adapter unterstützt Oracle E-Business Suite (EBS) Version 12. Abschnitte in `OracleERPUserForm` müssen, je nach der installierten ERP-Version, nicht mehr geändert oder auskommentiert werden (siehe *Identity Manager Resources Reference*).

Das `FormRef`-Attribut unterstützt jetzt die folgenden Eigenschaften:

- `RESOURCE_NAME` — ERP-Ressourcenname
- `VERSION` - Version der ERP-Ressource. Zulässige Werte: 11.5.9, 11.5.10, 12.
- `RESP_DESCR_COL_EXISTS` — Legt fest, ob die Tabelle „`fnr_user_resp_groups_direct`“ eine Beschreibungsspalte enthält. Diese Eigenschaft ist für Version 11.5.10 oder 12 obligatorisch. Zulässige Werte: `TRUE` und `FALSE`.

Diese Eigenschaften müssen bei jeder Referenzierung des Benutzerformulars eingegeben werden. Es kann beispielsweise sein, dass das Benutzerformular mit Registerkarten wie folgt eingestellt sein muss, damit Version 12 unterstützt wird:

```
<FormRef name="Oracle ERP User Form">
  <Property name="RESOURCE_NAME" value="Oracle ERP R12"/>
  <Property name="VERSION" value="12"/>
  <Property name="RESP_DESCR_COL_EXISTS" value="TRUE"/>
</FormRef>
```

## SAP-Adapter

- Im Abschnitt „Account Attributes“ wurde die Tabelle „Default iDoc infotypes supported by the SAP HR Active Sync adapter“ berichtigt. Die unterstützte Unterart für die Kommunikations-Informationsart 0105 wurde wie folgt von `EMAIL` in `MAIL` geändert (ID-12880):

Standardmäßig werden die folgenden Informationsarten unterstützt:

## Identity Manager 6.0 Resources Reference

Informationsart	Name	Unterstützte Unterarten
0000	Aktionen	nicht zutreffend
0001	Organisationszuweisung	nicht zutreffend
0002	Persönliche Daten	nicht zutreffend
0006	Adressen	01 (ständiger Wohnsitz), 03 (Heimatwohnsitz)
0105	Kommunikation	MAIL (E-Mail-Adresse), 0010 (Internet-Adresse)

Der SAPHRActiveSyncAdapter unterstützt jetzt mySAP ERP ECC 5.0 (SAP 5.0). Infolgedessen wurden im Abschnitt „Resource Configuration Notes“ die folgenden Änderungen vorgenommen: (ID-12769).

### SAP-Ressourcendapter

Die folgenden Hinweise zur Ressourcenkonfiguration gelten nur für den SAP-Ressourcenadapter.

Führen Sie die folgenden Schritte aus, damit Benutzer ihr eigenes SAP-Passwort ändern können:

1. Setzen Sie das Ressourcenattribut auf **Benutzer gibt Passwort bei Änderung an**.
2. Fügen Sie **WS\_USER\_PASSWORD** zu beiden Seiten der Schemazuordnung hinzu. Sie brauchen das Benutzerformular bzw. andere Formulare nicht zu ändern.

### SAP HR Active Sync-Adapter

Die folgenden Hinweise zur Ressourcenkonfiguration gelten nur für den SAP HR Active Sync-Adapter.

Die SAP-Technologie Application Link Enabling (ALE) ermöglicht die Kommunikation zwischen SAP und externen Systemen wie z.B. Identity Manager. Der SAP HR Active Sync-Adapter nutzt eine abgehende ALE-Schnittstelle. In einer abgehenden ALE-Schnittstelle ist das logische Basissystem der Absender abgehender Meldungen und der Empfänger eingehender Meldungen. SAP-Benutzer sind normalerweise am logischen Basissystem/-client angemeldet, wenn sie Änderungen an der Datenbank vornehmen (z.B. Einstellen eines neuen Mitarbeiters, Aktualisieren von Positionsdaten, Entlassen eines Mitarbeiters usw.). Ein logisches System/logischer Client muss auch für den Empfangs-Client definiert sein. Dieses logische System empfängt abgehende Meldungen. Als Meldungstyp zwischen beiden Systemen nutzt der Active Sync-Adapter

den Typ `HRMD_A`. Meldungstypen charakterisieren Daten, die zwischen den Systemen ausgetauscht werden und bezieht sich auf die Struktur dieser Daten. Eine solche Struktur ist auch unter der Bezeichnung „IDoc-Typ“ (z.B. `HRMD_A05`) bekannt.

Mit den folgenden Schritten können Sie die Konfiguration ausführen, die auf SAP für den Active Sync-Adapter zum Empfang autoritativer Feeds von SAP HR erforderlich ist:

**Hinweis** Die SAP-Systemparameter sind so zu konfigurieren, dass die ALE-Verarbeitung von IDocs vom Typ `HRMD_A` möglich ist. Dies ermöglicht den als *Messaging* bezeichneten Datenaustausch zwischen zwei Anwendungssystemen.

### Erstellen eines logischen Systems

Je nach Ihrer aktuellen SAP-Umgebung kann es sein, dass Sie kein logisches System erstellen müssen. Es kann sein, dass Sie ein vorhandenes Datenaustauschmodell nur durch Hinzufügen des Meldungstyps `HRMD_A` zu einer vorher konfigurierten Modellansicht modifizieren müssen. Sie müssen jedoch unbedingt die Empfehlungen von SAP für logische Systeme und die Konfiguration von ALE-Netzwerken einhalten. In den folgenden Anweisungen wird angenommen, dass Sie neue logische Systeme und eine neue Modellansicht erstellen.

1. Geben Sie den Transaktionscode `SPRO` ein und lassen Sie sich dann das Projekt „SAP Reference IMG“ (oder das für Ihre Organisation geltende Projekt) anzeigen.
2. Je nach der eingesetzten SAP-Version müssen Sie einen der folgenden Schritte ausführen:
  - SAP 4.6: Klicken Sie auf **Basis Components > Application Link Enabling (ALE) > Sending and Receiving Systems > Logical Systems > Define Logical System**.
  - SAP 4.7: Klicken Sie auf **SAP Web Application Server > Application Link Enabling (ALE) > Sending and Receiving Systems > Logical Systems > Define Logical System**.
  - SAP 5.0: Klicken Sie auf **SAP Netweaver > SAP Web Application Server > IDOC Interface/Application Link Enabling (ALE) > Basic Settings > Logical Systems > Define Logical System**.
3. Klicken Sie auf **Edit > New Entries**.
4. Geben Sie einen Namen und eine Beschreibung für das neu zu erstellende logische System ein (IDMGR).
5. Speichern Sie Ihren Eintrag.

### Zuweisen eines Clients zum logischen System

1. Geben Sie den Transaktionscode SPRO ein und lassen Sie sich dann das Projekt „SAP Reference IMG“ (oder das für Ihre Organisation geltende Projekt) anzeigen.
2. Je nach der eingesetzten SAP-Version müssen Sie einen der folgenden Schritte ausführen:
  - SAP 4.6: Klicken Sie auf **Basis Components > Application Link Enabling (ALE) > Sending and Receiving Systems > Logical Systems > Assign Client to Logical System**.
  - SAP 4.7: Klicken Sie auf **SAP Web Application Server > Application Link Enabling (ALE) > Sending and Receiving Systems > Logical Systems > Assign Client to Logical System**.
  - SAP 5.0: Klicken Sie auf **SAP Netweaver > SAP Web Application Server > IDOC Interface/Application Link Enabling (ALE) > Basic Settings > Logical Systems > Assign Client to Logical System**.
3. Wählen Sie den Client aus.
4. Klicken Sie auf **GOTO > Details**, um das Dialogfeld „Client Details“ zu öffnen.
5. Geben Sie in das Feld „Logical System“ das logische System ein, das diesem Client zugewiesen werden soll.
6. Klicken Sie im Abschnitt „Changes and Transports for Clients“ auf **Automatic Recording of Changes**.
7. Speichern Sie Ihren Eintrag.

### Erstellen eines Datenaustauschmodells

So erstellen Sie ein neues Datenaustauschmodell:

1. Vergewissern Sie sich, dass Sie am sendenden System/Client angemeldet sind.
2. Geben Sie den Transaktionscode **BD64** ein. Sorgen Sie dafür, dass Sie sich im Änderungsmodus befinden.
3. Klicken Sie auf **Edit > Model View > Create**.
4. Geben Sie den kurzen und den technische Namen der Ansicht ein sowie das Start- und das Enddatum ein, und klicken Sie dann auf **Continue**.
5. Wählen Sie die gerade erstellte Ansicht aus und klicken Sie dann auf **Add Message Type**.
6. Definieren Sie das sendende System (logische System).
7. Definieren Sie das empfangende System (den Server).
8. Klicken Sie im Abschnitt „Protection Client Copier and Comparison Tool“ auf **Protection Level: No Restriction**.

9. Definieren Sie den gewünschten Meldungstyp (HRMD\_A) und klicken Sie dann auf **Continue**.
10. Klicken Sie auf **Speichern**.

### Registrierung des RFC-Servermoduls beim SAP-Gateway

Während der Initialisierung wird der Active Sync-Adapter beim SAP-Gateway registriert. Als ID dient „IDMRFC“. Dieser Wert muss mit dem in der SAP-Anwendung eingestellten Wert übereinstimmen. Sie müssen die SAP-Anwendung so konfigurieren, dass das RFC-Servermodul dafür einen Handle erstellen kann. So registrieren Sie das RFC-Servermodul als RFC-Ziel:

1. Gehen Sie in der SAP-Anwendung zu Transaktion SM59.
2. Klappen Sie das Verzeichnis für TCP/IP-Verbindungen auf.
3. Klicken Sie auf **Create (F8)**.
4. Geben Sie im Feld „RFC Destination“ den Namen des RFC-Zielsystems ein. (IDMRFC).
5. Setzen Sie den Verbindungstyp auf  $\pi$  (Starten eines externen Programms über TCP/IP).
6. Geben Sie für das neue RFC-Ziel eine Beschreibung ein und klicken Sie dann auf **Speichern**.
7. Klicken Sie auf die Schaltfläche „Registration“ des jeweiligen Aktivierungstyps.
8. Setzen Sie die Programm-ID. Wir empfehlen, dafür den gleichen Wert wie den für das RFC-Ziel (IDMRFC) zu verwenden. Klicken Sie dann auf „Enter“.
9. Wenn es sich bei dem betreffenden SAP-System um ein Unicode-System handelt, muss der Port für Unicode konfiguriert sein. Klicken Sie auf die Registerkarte **Special Options** und suchen Sie den Abschnitt „Character Width In Target System“. Dort gibt es eine Einstellung für Unicode.
10. Testen Sie mithilfe der oberen Schaltflächen (**Test Connection** und **Unicode Test**) die Verbindung zur Identity Manager-Ressource. Damit der Test erfolgreich verläuft, muss der Adapter bereits laufen.

### Erstellen einer Port-Definition

Der Port ist der Kommunikationskanal, an den IDocs gesendet werden. Ein Port beschreibt die technische Verbindung zwischen dem sendenden und dem empfangenden System. Für diesen Anwendungsfall sollten Sie ein RFC-Port konfigurieren. So erstellen Sie eine Port-Definition.

1. Geben Sie den Transaktionscode **WE21** ein.
2. Wählen Sie „Transactional RFC“ und klicken Sie dann auf das Symbol **Erstellen**. Geben Sie als RFC-Ziel **IDMRFC** ein.
3. Speichern Sie die Änderungen.

### Ändern der Port-Definition

Wenn Sie ein Partnerprofil erstellt haben, kann es sein, dass die Port-Definition nicht ordnungsgemäß eingegeben wurde. Damit Ihr System ordnungsgemäß funktioniert, müssen Sie die Port-Definition ändern.

1. Geben Sie den Transaktionscode **WE20** ein.
2. Wählen Sie **Partner Type LS**.
3. Wählen Sie das Empfangspartnerprofil aus.
4. Wählen Sie **Outbound Parameters** und klicken Sie dann auf **Display**.
5. Wählen Sie den Meldungstyp **HRMD\_A**.
6. Klicken Sie auf **Outbound Options** und ändern Sie dann das Empfänger-Port so, dass es den Namen des von Ihnen erstellten RFC-Ports enthält (IDMGR).
7. Wählen Sie im Ausgabemodus **Transfer IDoc Immediately**, wenn IDocs unmittelbar nach dem Erstellen gesendet werden sollen.
8. Wählen Sie im Abschnitt „IDoc Type“ einen Basistyp aus:
  - SAP 4.6 - **HRMD\_A05**
  - SAP 4.7 oder 5.0 - **HRMD\_A06**
9. Klicken Sie auf **Continue/Save**.

### Skript-JDBC-Adapter

Identity Manager bietet jetzt einen Skript-JDBC-Ressourcenadapter zur Unterstützung der Verwaltung von Benutzerkonten in Datenbankschemen und in Datenbanken, auf die mit JDBC zugegriffen werden kann. Dieser Adapter unterstützt auch Active Sync, um Kontenänderungen in der Datenbank abzufragen. Ausführliche Informationen zu diesem Adapter finden Sie im Kapitel Sun Java™ System *Identity Manager Resources Reference Addendum*. (ID-12506).

### Shell-Skript-Adapter

Identity Manager bietet jetzt einen Shell-Skript-Ressourcenadapter zur Unterstützung der Verwaltung von Ressourcen, die durch Shell-Skripte gesteuert werden. Solche Shell-Skripte laufen auf dem System, auf dem die betreffende Ressource installiert ist. Diese Adapter ist zur allgemeinen Verwendung bestimmt und aus diesem Grund hochgradig anpassbar.

### Siebel CRM-Adapter

Es können jetzt Siebel-Objekte, die eine hierarchische Navigation von Business-Komponenten erfordern, erstellt und aktualisiert werden. Hierbei handelt es sich um eine erweiterte Funktion, die normalerweise nicht in Identity Manager implementiert ist.

Mit der erweiterten Navigationsfunktion können Sie wahlweise die folgenden Informationen angeben, die zum Erstellen und Aktualisieren untergeordneter Business-Komponenten erforderlich sind:

- Name des Business-Objekts
- Name der übergeordneten Business-Komponente
- übergeordnetes Suchattribut
- Business-Zielkomponente
- Zielsuchattribut
- Attribute im Gültigkeitsbereich (d.h. welche Attribute der Business-Komponente sollten gesetzt/aktualisiert werden)
- optionale Zusatzaktion

Während Erstellungs- und Aktualisierungsaktionen können erweiterte Navigationsregeln verwendet werden. Diese sind jedoch nicht für andere Aktionsarten einsetzbar.

Führen Sie die folgenden Aufgaben durch, um die erweiterte Navigationsfunktion für den Siebel CRM-Adapter zu implementieren:

- Fügen Sie zu der Schema-Zuordnung, in der das Ressourcen-Benutzerattribut (rechte Seite) PARENT\_COMP\_ID heißt, ein Attribut zu.
- Fügen Sie zum XML-Code der betreffenden Ressource mithilfe der Debug-Seite manuell das folgende ResourceAttribute hinzu:

```
<ResourceAttribute name="AdvancedNavRule"
  displayName="Advanced Nav Rule"
  value="MY_SIEBEL_NAV_RULE">
</ResourceAttribute>
```

Ersetzen Sie *MY\_SIEBEL\_NAV\_RULE* durch einen gültigen Regelnamen.

## Identity Manager 6.0 Resources Reference

- Schreiben Sie die erweiterte Navigationsregel. Diese regel muss die folgenden beiden Variablen enthalten:

`resource.action` — Dieser Variable muss auf `create` oder `update` gesetzt sein.

`resource.objectType` — Für die normale Kontoverwaltung muss diese Variable auf `account` gesetzt sein.

Die Regel muss eine Zuordnung mit mindestens einem der folgenden Namen-Wert-Paare zurückgeben:

Attribut	Definition
<code>busObj</code>	Der Name des Business-Objekts.
<code>parentBusComp</code>	Der Name der übergeordneten Business-Komponente für <code>busObj</code> . Der Kontext dieses Business-Objekts wird durch Springen zum ersten qualifizierten (siehe <code>parentSearchAttr</code> ) Datensatz dieser Business-Komponente aktualisiert
<code>parentSearchAttr</code>	Das in <code>parentBusComp</code> als Suchfeld zu verwendende Attribut. Es wird vorausgesetzt, dass der Wert, nach dem gesucht werden soll, als Wert des Attributs, dessen Ressource-Benutzerattributname <code>PARENT_COMP_ID</code> ist, vorhanden ist.
<code>busComp</code>	Der Name der finalen Business-Komponente, die erstellt oder aktualisiert werden soll. Beim Erstellen wird im Business-Objekt ein neuer Datensatz dieser Business-Komponente erstellt. Beim Aktualisieren wird zu aktualisierende Datensatz der Business-Komponente durch Springen zum ersten qualifizierten (siehe <code>SearchAttr</code> ) Datensatz dieser Business-Komponente ausgewählt
<code>searchAttr</code>	Das in <code>busComp</code> als Suchfeld zu verwendende Attribut. Der Wert, nach dem gesucht wird, ist die Konto-ID des jeweiligen Benutzers.
<code>attributes</code>	Eine Stringliste, die die Felder in <code>busComp</code> festlegt, die gesetzt oder aktualisiert werden sollen. Diese Liste hat Vorrang vor den Attributen, die in der Ressourcen-Schemazuordnung der ausführenden Aktion definiert sind.
<code>coAction</code>	Wenn die angeforderte Aktion ( <code>resource.action</code> ) auf <code>create</code> gesetzt ist, müssen Sie <code>coAction</code> auf <code>update</code> setzen. Dies weist den Adapter an, unmittelbar nach dem Erstellen eine Aktualisierung durchzuführen. Das kann erforderlich sein, wenn die Erstellungsaktion nicht alle erforderlichen Felder setzen kann. Aus diesem Grund muss zum logischen Abschluss der Erstellungsaktion noch eine Aktualisierung durchgeführt werden. Dieses Attribut wird ignoriert, wenn <code>resource.action</code> nicht auf <code>create</code> und <code>coAction</code> nicht auf <code>update</code> gesetzt ist.

Ein Beispiel für eine Navigationsregel finden Sie in  
`$WSHOME/sample/rules/SiebelNavigationRule.xml`.

## Sun Java System Access Manager-Adapter

- Dieser Adapter unterstützt den Legacy-Modus nur für Access Manager 7 und neuere Versionen. Es werden keine Realms unterstützt.

### Installation und Konfiguration von Sun Java System Access Manager (Versionen vor Access Manager 7.0)

Die Schritte 4 und 8 in "Installing and Configuring Sun Java System Access Manager" müssen wie folgt lauten (ID-13087):

1. Erstellen Sie ein Verzeichnis, in das Dateien vom Sun Java System Access Manager-Server kopiert werden können. Hier wird dieses Verzeichnis *CfgDir* genannt. Die Installationsverzeichnis von Sun Java System Access Manager wird *AccessMgrHome* genannt.
2. Kopieren Sie die folgenden von *AccessMgrHome* nach *CfgDir*. Die Verzeichnisstruktur darf nicht kopiert werden.
  - lib/\*.\*
  - locale/\*.properties
  - config/serverconfig.xml
  - config/SSOConfig.properties (Identity Server 2004Q2 und neuer)
  - config/ums/ums.xml
3. In UNIX kann es erforderlich sein, dass die Zugriffsrechte der JAR-Dateien im Verzeichnis *CfgDir* geändert werden müssen, um universellen Lesezugriff zu ermöglichen. Führen Sie den folgenden Befehl aus, um Zugriffsrechte zu ändern:  

```
chmod a+r CfgDir/*.jar
```
4. Stellen Sie dem JAVA-Classpath Folgendes voran:
  - **Windows:** *CfgDir*; *CfgDir/am\_sdk.jar*; *CfgDir/am\_services.jar*; *CfgDir/am\_logging.jar*
  - **UNIX:** *CfgDir:CfgDir/am\_sdk.jar:CfgDir/am\_services.jar:CfgDir/am\_logging.jar*
5. Wenn Sie Version 6.0 verwenden, muss die Java-Systemeigenschaft auf das Verzeichnis *CfgDir* zeigen. Verwenden Sie einen Befehl, der dem folgenden ähnelt:  

```
java -Dcom.ipplanet.coreservices.configpath=CfgDir
```

## Identity Manager 6.0 Resources Reference

6. Wenn Sie Version 6.1 oder neuer verwenden, müssen Sie zur Datei `CfgDir/AMConfig.properties` folgende Zeilen einfügen bzw. diese entsprechend abändern:  

```
com.ipplanet.services.configpath=CfgDircom.ipplanet.security.  
SecureRandomFactoryImpl=com.ipplanet.am.util.SecureRandomFact  
oryImpl  
  
com.ipplanet.security.SSLSocketFactoryImpl=netscape.ldap.  
factory.JSSESocketFactory  
  
com.ipplanet.security.encryptor=com.ipplanet.services.util.  
JCEEncryption
```

Mit der ersten Zeile wird der `configpath` gesetzt. Die letzten drei Zeilen ändern Sicherheitseinstellungen.
7. Kopieren Sie die Dateien `CfgDir/am_*.jar` nach `$WSHOME/WEB-INF/lib`. Wenn Sie Version 6.0 verwenden, müssen Sie auch die Datei `jss311.jar` in das Verzeichnis `$WSHOME/WEB-INF/lib` kopieren.
8. Wenn Identity Manager unter Windows läuft und Sie Identity Server 6.0 verwenden, müssen Sie `IdServer\lib\jss\*.dll` nach `CfgDir` kopieren und `CfgDir` zu Ihrem Systempfad hinzufügen.

**Hinweis** In einer Umgebung, in der Identity Manager auf einem anderen System als Sun Java System Access Manager installiert ist, müssen Sie die folgenden Fehlerbedingungen überprüfen. Wenn beim Herstellen einer Verbindung zur Sun Java System Access Manager-Ressource nach mehreren Versuchen `java.lang.ExceptionInInitializerError` und danach `java.lang.NoClassDefFoundError` zurückgegeben wird, sollten Sie nach falschen oder fehlenden Konfigurationsdaten suchen.

Darüber hinaus sollten Sie die JAR-Datei auf die Klasse, die von `java.lang.NoClassDefFoundError` ausgegeben wird, überprüfen. Stellen Sie dem Classpath der JAR-Datei, die die Klasse enthält, dem JAVA-Classpath auf dem Anwendungsserver voran.

## Installation und Konfiguration von Sun Java System Access Manager (Versionen 7.0 und höher im Legacy-Modus)

Mit den folgenden Schritten installieren und konfigurieren Sie den Ressourcenadapter für den Legacy-Modus.

1. Folgen Sie den Anweisungen im *Sun Java™ System Access Manager 7 2005Q4 Developer's Guide*, um das Client-SDK aus der Sun Access Manager-Installation heraus zu erstellen.
2. Extrahieren Sie aus der generierten `war`-Datei `AMConfig.properties` und die in `amclientsdk.jar` enthaltenen Dateien.

3. Legen Sie ein Kopie von `AMConfig.properties` im folgenden Verzeichnis ab:  
`InstallDir/WEB-INF/classes`
4. Legen Sie ein Kopie von `amclientsdk.jar` im folgenden Verzeichnis ab:  
`InstallDir/WEB-INF/lib`

## Sun Java System Communications Services-Adapter

- Das Beispiel-Skript, das auf einer Proxy-Ressource nach dem Erstellen eines Benutzers ausgeführt werden kann, ist falsch. Verwenden Sie stattdessen das folgende Skript: (ID-12536).

```
SET PATH=c:\Sun\Server-Root\lib
SET SYSTEMROOT=c:\winnt
SET CONFIGROOT=C:/Sun/Server-Root/Config
mboxutil -c -P user/%WSUSER_accountId%.*
```

- Es werden jetzt die folgenden binären Kontoattribute aus der Objektklasse „inetOrgPerson“ unterstützt:

Ressourcen-Benutzerattribut	LDAP-Syntax	Beschreibung
audio	Audio	Eine Audiodatei.
jpegPhoto	JPEG	Ein Bild im JPEG-Format.
userCertificate	certificate	Ein Zertifikat im Binärformat.

Andere Binärattribute werden möglicherweise unterstützt, sie wurden jedoch nicht getestet.

## Top Secret-Adapter

In *Identity Manager Resources Reference* ist fälschlicherweise angegeben, dass der Top Secret-Adapter das Umbenennen von Konten unterstützt. Der Adapter unterstützt das Umbenennen von Top Secret-Konten nicht.

## Kapitel 3: Aktionen zu Ressourcen hinzufügen

Im Abschnitt "Windows NT Examples" sind die `Field`-Namen für alle drei Beispiele falsch definiert. Ersetzen Sie Instanzen von `accounts[NT].attributes.` durch `resourceAccounts.currentResourceAccounts[NT].attributes.` Beispielsweise sollte in Abschnitt „Example 3: Action that Follows the Deletion of a User“, Schritt 4, der `Field`-Name wie folgt definiert sein:

```
<Field name=
"resourceAccounts.currentResourceAccounts[NT].attributes.delete after
action">
```

# Identity Manager Tuning, Troubleshooting, and Error Messages

---

## Zusätzliche Informationen

- Sie können jetzt mit dem Standardtool für die Ablaufverfolgung von `com.waveset.task.Scheduler` den Ablauf des Aufgabenplaners verfolgen, wenn bei einer Aufgabe Probleme auftreten.

Weitere Informationen hierzu finden Sie unter *Tracing the Identity Manager Server* in *Sun Java™ System Identity Manager Tuning, Troubleshooting, and Error Messages*.

- Zur Fehlersuche bei Problemen, die auf einer Ebene unter einer bestimmten Eintrittsmethode auftreten, sollten Sie den Fehler auf der Methodenebene verfolgen. Identity Manager bietet jetzt die Möglichkeit, nur eine Methode und ihre direkten und indirekten Unteraufrufe zu verfolgen. (ID-14967).

Zum Aktivieren dieser Funktion müssen Sie die Verfolgungsebene für einen Gültigkeitsbereich mithilfe des `subcalls`-Bezeichners setzen (siehe folgendes Beispiel):

```
trace 4,subcalls=2
com.waveset.recon.ReconTask$WorkerThread#reconcileAccount
```

Dies verfolgt die Methode `reconcileAccount()` auf Ebene 4 und alle Unteraufrufe auf Ebene 2.

Weitere Informationen hierzu finden Sie unter *Defining a Trace Configuration* in *Sun Java™ System Identity Manager Tuning, Troubleshooting, and Error Messages*.

## Korrekturen

Da Sie JDK 1.4.2 für diese Version installieren müssen, gilt die Anweisung zum Entfernen der Cryptix-JAR-Dateien (`cryptix-jceapi.jar` und `cryptix-jce-provider.jar`) im Verzeichnis `idm\WEB-INF\lib` in Kapitel 1: *Performance Tuning, Optimizing the J2EE Environment* nicht mehr (es sei denn, Sie rüsten eine frühere Version von Identity Manager auf).

# Identity Manager Deployment Tools

---

## Korrekturen

### Kapitel 7: Using Identity Manager Web Services

Das launchProcess-Beispiel im Abschnitt „ExtendedRequest Examples“ wurde wie folgt berichtigt (ID-13044):

#### launchProcess

Das folgende Beispiel zeigt ein typisches Format für eine launchProcess-Anforderung. (Ansicht — Prozessansicht).

```
ExtendedRequest req = new ExtendedRequest();
req.setOperationIdentifier("launchProcess");
req.setAsynchronous(false);
req.setAttribute("process", "Custom Process Name");
req.setAttribute("taskName", "Custom Process Display Name");
SpmlResponse res = client.request(req);
```

## Arbeiten mit HelpTool

---

Identity Manager 6.0 enthält eine neue Funktion zum Durchsuchen der Onlinehilfe und der Hilfedateien im HTML-Format. Das Suchmodul basiert auf der SunLabs Nova-Technologie.

Die Verwendung des Nova-Suchmoduls verläuft in zwei Phasen: *Indizierung* und *Abruf*. Während der Indizierung werden die Eingabedokumente analysiert und ein Index für die Abrufphase erstellt. Während des Abrufs können „Passagen“ abgerufen werden, die aus dem Kontext bestehen, in dem die Abfragebegriffe gefunden wurden. Der Abrufprozess für die Passagen benötigt die ursprünglichen HTML-Dateien. Diese Dateien müssen sich deshalb in einem Speicherort des Dateisystems befinden, auf den das Suchmodul Zugriff hat.

helpTool ist ein Java-Programm, das zwei grundlegende Funktionen ausführt:

- Kopiert die HTML-Quelldateien in einen Speicherort, auf den das Suchmodul Zugriff hat
- Erstellt den Index für die Abrufphase

## Arbeiten mit HelpTool

Sie führen helpTool folgendermaßen über die Befehlszeile aus:

```
$ java -jar helpTool.jar
Syntax: HelpTool
-d    Zielverzeichnis
-h    Diese Hilfeinformationen
-i    Verzeichnis oder JAR-Datei mit Eingabedateien, keine Platzhalter
-n    Verzeichnis für den Nova-Index
-o    Name der Ausgabedatei
-p    Eigenschaftendatei für die Indizierung
```

## Index der Onlinehilfe neu erstellen

Die HTML-Dateien für die Onlinehilfe sind in einer JAR-Datei als Paket enthalten. Sie müssen diese Dateien in ein Verzeichnis für das Suchmodul extrahieren. Gehen Sie folgendermaßen vor:

1. Entpacken Sie das helpTool-Paket in ein temporäres Verzeichnis. (Details werden später angegeben)  
In diesem Beispiel werden die Dateien in das Verzeichnis `/tmp/helpTool` extrahiert.
2. Geben Sie in einer UNIX-Shell oder in einem Windows-Befehlsfenster das Verzeichnis an, in dem die Identity Manager-Anwendung Ihrem Webcontainer bereitgestellt wurde.

Es kann beispielsweise folgendes Verzeichnis für Sun Java System Application Server verwendet werden:

```
/opt/SUNWappserver/domains/domain1/applications/j2ee-modules/idm
```

3. Verwenden Sie `help/` als aktuelles Arbeitsverzeichnis.

**Hinweis** Führen Sie helpTool unbedingt von diesem Verzeichnis aus, weil andernfalls der Index nicht korrekt erstellt wird. Entfernen Sie außerdem die alten Indexdateien, indem Sie den Inhalt des Verzeichnisses `index/help/` löschen.

4. Erfassen Sie folgende Informationen für Ihre Befehlszeilenargumente:

• <b>Zielverzeichnis:</b>	html/help/en_US <b>Hinweis:</b> Verwenden Sie die für Ihre Installation geeignete Gebietsschemazeichenfolge.
• <b>Eingabedateien:</b>	../WEB-INF/lib/idm.jar
• <b>Nova-Indexverzeichnis:</b>	index/help
• <b>Name der Ausgabedatei:</b>	index_files_help.txt <b>Hinweis:</b> Dieser Dateiname ist nicht wichtig, das Tool wird jedoch beendet, falls diese Datei bereits vorhanden ist.
• <b>Eigenschaftendatei für die Indizierung:</b>	index/index.properties

5. Führen Sie folgenden Befehl aus:

```
$ java -jar /tmp/helpTool/helpTool.jar -d html/help/en_US -i ../
WEB-INF/lib/idm.jar -n index/help -o help_files_help.txt -p
index/index.properties
Extracted 475 files.
[15/Dec/2005:13:11:38] PM Init index/help AWord 1085803878
[15/Dec/2005:13:11:38] PM Making meta file: index/help/MF: 0
[15/Dec/2005:13:11:38] PM Created active file: index/help/AL
[15/Dec/2005:13:11:40] MP Partition: 1, 475 documents, 5496 terms.
[15/Dec/2005:13:11:40] MP Finished dumping: 1 index/help 0.266
[15/Dec/2005:13:11:40] IS 475 documents, 6,56 MB, 2,11 s, 11166,66 MB/h
[15/Dec/2005:13:11:40] PM Waiting for housekeeper to finish
[15/Dec/2005:13:11:41] PM Shutdown index/help AWord 1085803878
```

## Dokumentationsindex neu erstellen

Gehen Sie folgendermaßen vor, um den Dokumentationsindex neu zu erstellen:

1. Entpacken Sie das helpTool-Paket in ein temporäres Verzeichnis. (Details werden später angegeben)  
In diesem Beispiel werden die Dateien in das Verzeichnis `/tmp/helpTool` extrahiert.
2. Geben Sie in einer UNIX-Shell oder in einem Windows-Befehlsfenster das Verzeichnis an, in dem die Identity Manager-Anwendung Ihrem Webcontainer bereitgestellt wurde.  
Es kann beispielsweise folgendes Verzeichnis für Sun Java System Application Server verwendet werden:

```
/opt/SUNWappserver/domains/domain1/applications/j2ee-modules/idm
```

3. Verwenden Sie `help/` als aktuelles Arbeitsverzeichnis.

**Hinweis** Führen Sie helpTool unbedingt von diesem Verzeichnis aus, weil andernfalls der Index nicht korrekt erstellt wird. Entfernen Sie außerdem die alten Indexdateien, indem Sie den Inhalt des Verzeichnisses `index/docs/` löschen.

4. Erfassen Sie folgende Informationen für Ihre Befehlszeilenargumente:

• <b>Zielverzeichnis:</b>	html/docs
• <b>Eingabedateien:</b>	../doc/HTML/en_US <b>Hinweis:</b> Das Tool kopiert das Verzeichnis en_US/ und dessen Unterverzeichnisse in dieses Ziel.
• <b>Nova-Indexverzeichnis:</b>	index/docs
• <b>Name der Ausgabedatei:</b>	index_files_docs.txt <b>Hinweis:</b> Dieser Dateiname ist nicht wichtig, das Tool wird jedoch beendet, falls diese Datei bereits vorhanden ist.
• <b>Eigenschaftendatei für die Indizierung:</b>	index/index.properties

## Arbeiten mit HelpTool

### 5. Führen Sie folgenden Befehl aus:

```
$ java -jar /tmp/helpTool/helpTool.jar -d html/docs -i
../doc/HTML/en_US -n index/docs -o help_files_docs.txt -p
index/index.properties
Copied 84 files.
Copied 105 files.
Copied 1 files.
Copied 15 files.
Copied 1 files.
Copied 58 files.
Copied 134 files.
Copied 156 files.
Copied 116 files.
Copied 136 files.
Copied 21 files.
Copied 37 files.
Copied 1 files.
Copied 13 files.
Copied 2 files.
Copied 19 files.
Copied 20 files.
Copied 52 files.
Copied 3 files.
Copied 14 files.
Copied 3 files.
Copied 3 files.
Copied 608 files.
[15/Dec/2005:13:24:25] PM Init index/docs AWord 1252155067
[15/Dec/2005:13:24:25] PM Making meta file: index/docs/MF: 0
[15/Dec/2005:13:24:25] PM Created active file: index/docs/AL
[15/Dec/2005:13:24:28] MP Partition: 1, 192 documents, 38488 terms.
[15/Dec/2005:13:24:29] MP Finished dumping: 1 index/docs 0.617
[15/Dec/2005:13:24:29] IS 192 documents, 14.70 MB, 3.81 s, 13900.78 MB/h
[15/Dec/2005:13:24:29] PM Waiting for housekeeper to finish
[15/Dec/2005:13:24:30] PM Shutdown index/docs AWord 1252155067
```

# Verworfenne APIs

---

Dieses Kapitel enthält alle Identity Manager-APIs (Application Programming Interfaces), die in Identity Manager 6.0 2005Q4M3 SP1 verworfen wurden. Außerdem werden, falls verfügbar, deren Nachfolger aufgelistet. Dieses Kapitel ist in folgende Abschnitte unterteilt:

- Verworfenne Konstruktoren
- Verworfenne Methoden und Felder

## Verworfenne Konstruktoren

---

Die folgende Tabelle enthält die verworfenen Konstruktoren und, falls verfügbar, deren Nachfolger.

Verworfenner Konstruktor	Nachfolger
com.waveset.adapter.ActiveDirectoryActiveSyncAdapter	com.waveset.adapter.ADSIResourceAdapter
com.waveset.adapter.AD_LDAPResourceAdapter	com.waveset.adapter.LDAPResourceAdapter
com.waveset.adapter.AttrParse	com.waveset.object.AttrParse
com.waveset.adapter.ConfirmedSync	
com.waveset.adapter.DblBuflterator	com.waveset.util.BufferedIterator com.waveset.util.BlockIterator com.waveset.adapter.AccountIteratorWrapper
com.waveset.adapter.DominoActiveSyncAdapter	com.waveset.adapter.DominoResourceAdapter
com.waveset.adapter.LDAPChangeLogActiveSyncAdapter	com.waveset.adapter.LDAPResourceAdapter
com.waveset.adapter.NDSActiveSyncAdapter	com.waveset.adapter.NDSResourceAdapter
com.waveset.adapter.PeopleSoftResourceAdapter	
com.waveset.adapter.RemedyActiveSyncResourceAdapter	com.waveset.adapter.RemedyResourceAdapter
com.waveset.adapter.TopSecretActiveSyncAdapter	com.waveset.adapter.TopSecretResourceAdapter
com.waveset.exception.ConfigurationError	com.waveset.util.ConfigurationError

## Verworfenne Methoden und Felder

Verworfenner Konstruktor	Nachfolger
com.waveset.exception.IOException	com.waveset.util.IOException
com.waveset.exception.XmlParseException	com.waveset.util.XmlParseException
com.waveset.object.IAPI	com.waveset.adapter.iapi.IAPI
com.waveset.object.IAPIProcess	com.waveset.adapter.iapi.IAPIFactory
com.waveset.object.IAPIUser	com.waveset.adapter.iapi.IAPIUser
com.waveset.object.RemedyTemplate	
com.waveset.object.ReportCounter	
com.waveset.object.SourceManager	com.waveset.view.SourceAdapterManagerView
com.waveset.security.authn.LoginInfo	com.waveset.object.LoginInfo
com.waveset.security.authn.SignedString	com.waveset.util.SignedString
com.waveset.security.authn.Subject	com.waveset.object.Subject
com.waveset.security.authz.Permission	com.waveset.object.Permission
com.waveset.security.authz.Right	com.waveset.object.Right
com.waveset.util.Debug	com.sun.idm.logging.Trace
com.waveset.util.HtmlUtil	com.waveset.ui.util.html.HtmlUtil
com.waveset.util.ITrace	com.sun.idm.logging.Trace

## Verworfenne Methoden und Felder

---

Die Tabellen in diesem Abschnitt enthalten alle Methoden und Felder, die in dieser Version verworfen wurden. Die Methoden und Felder sind nach Klassennamen sortiert.

Die Daten in der Spalte **Nachfolger** können folgende Informationsarten enthalten:

- Wenn die Spalte leer ist, gibt es keinen Nachfolger für die Methode oder das Feld.
- Wenn kein Klassenname angegeben ist, wird der Nachfolger für die Methode oder das Feld in derselben Klasse wie das verworfene Element definiert.
- Wenn der Nachfolger für die Methode oder das Feld in einer anderen Klasse als das verworfene Element definiert ist, wird der Nachfolger in der Javadoc-Syntax aufgelistet. Beispiel: Die `getBaseContextAttrName()`-Methode der Klasse `com.waveset.adapter.ADSIResourceAdapter` wurde verworfen.

Der Nachfolger wird als

`com.waveset.adapter.ResourceAdapter#ResourceAdapter()`  
aufgeführt.

wobei gilt:

- `com.waveset.adapter` ist der Package-Name.
- `ResourceAdapter` ist der Klassenname.
- `ResourceAdapter()` ist die Methode und Argumentliste.

### **com.waveset.adapter.AccessManagerResourceAdapter**

Verworfenne Methode	Nachfolger
<code>handlePDEException(Exception)</code>	<code>handlePDEException(PDEException)</code>

### **com.waveset.adapter.ACF2ResourceAdapter**

Verworfenne Methode	Nachfolger
<code>getAccountAttributes(String)</code>	

### **com.waveset.adapter.ActiveSync**

Verworfenes Feld	Nachfolger
<code>RA_UPDATE_IF_DELETE</code>	

### **com.waveset.adapter.ActiveSyncUtil**

Verworfenne Methode	Nachfolger
<code>getLogFileFullPath()</code>	

## Verworfenne Methoden und Felder

### **com.waveset.adapter.ADSIResourceAdapter**

Verworfenne Methoden oder Felder	Nachfolger
buildEvent(UpdateRow)	com.waveset.adapter.iapi.IAPIFactory#getIAPI(Map,Map,ResourceAdapterBase)
getBaseContextAttrName()	com.waveset.adapter.ResourceAdapter#getBaseContexts()
RA_UPDATE_IF_DELETE	com.waveset.adapter.ActiveSync#RA_DELETE_RULE

### **com.waveset.adapter.AgentResourceAdapter**

Verworfenne Methode	Nachfolger
getAccountAttributes(String)	

### **com.waveset.adapter.AIXResourceAdapter.BlockAcctItr**

Verworfenne Methode	Nachfolger
BlockAcctItr(AIXResourceAdapter,CaptureList)	BlockAcctItr(CaptureList)
BlockAcctItr(int,CaptureList)	BlockAcctItr(CaptureList)

### **com.waveset.adapter.AuthSSOResourceAdapter**

Verworfenne Methode	Nachfolger
getAccountAttributes(String)	

### **com.waveset.adapter.ClearTrustResourceAdapter**

Verworfenne Methode	Nachfolger
getAccountAttributes(String)	

### **com.waveset.adapter.DatabaseTableResourceAdapter**

Verworfenes Feld	Nachfolger
RA_PROCESS_NAME	com.waveset.adapter.ActiveSync#RA_PROCESS_RULE

### **com.waveset.adapter.DB2ResourceAdapter**

Verworfenne Methode	Nachfolger
getAccountAttributes(String)	

### **com.waveset.adapter.DominoResourceAdapter**

Verworfenne Methoden oder Felder	Nachfolger
buildEvent(UpdateRow)	com.waveset.adapter.iapi.IAPIFactory#getIAPI(Map,Map,ResourceAdapterBase)
RA_UPDATE_IF_DELETE	com.waveset.adapter.ActiveSync#RA_DELETE_RULE

### **com.waveset.adapter.DominoResourceAdapterBase**

Verworfenne Methode	Nachfolger
getAccountAttributes(String)	

## Verworfenne Methoden und Felder

### **com.waveset.adapter.ExampleTableResourceAdapter**

Verworfenne Methode	Nachfolger
getAccountAttributes(String)	

### **com.waveset.adapter.GenericScriptResourceAdapter**

Verworfenne Methode	Nachfolger
getAccountAttributes(String)	

### **com.waveset.adapter.GetAccessResourceAdapter**

Verworfenne Methode	Nachfolger
getAccountAttributes(String)	

### **com.waveset.adapter.HostConnectionPool**

Verworfenne Methode	Nachfolger
getConnection(HostAccessLogin)	com.waveset.adapter.HostConnPool#getAffinityConnection(HostAccessLogin)
releaseConnection(HostAccess)	com.waveset.adapter.HostConnPool#releaseConnection(HostAccess)

### **com.waveset.adapter.HostConnPool**

Verworfenne Methode	Nachfolger
getConnection(HostAccessLogin)	getAffinityConnection(HostAccessLogin)
putFree()	

### com.waveset.adapter.iapi.IAPIFactory

Verworfenne Methode	Nachfolger
getIAPIDProcess(Map,Map,String,Resource)	getIAPID(Map,Map,String,ResourceAdapterBase)
getIAPIDProcess(Element)	
getIAPIDUser(Element)	
getIAPIDUser(Map,Map,String,Map)	getIAPID(Map,Map,String,ResourceAdapterBase)
getIAPIDUser(Map,Map,String,Resource)	getIAPID(Map,Map,String,ResourceAdapterBase)

### com.waveset.adapter.IDMResourceAdapter

Verworfenne Methode	Nachfolger
getAccountAttributes(String)	

### com.waveset.adapter.INISafeNexessResourceAdapter

Verworfenne Methode	Nachfolger
getAccountAttributes(String)	

### com.waveset.adapter.LDAPResourceAdapterBase

Verworfenne Methoden oder Felder	Nachfolger
addUserToGroup(LDAPObject,String,String)	addUserToGroup(String,String,String)
buildBaseUrl()	
buildBaseUrl(String)	
buildEvent(UpdateRow)	
getAccountAttributes(String)	

## Verworfenne Methoden und Felder

Verworfenne Methoden oder Felder	Nachfolger
getBaseContextAttrName()	com.waveset.adapter.ResourceAdapter#getBaseContexts()
getGroups(Name,String,Vector,Vector)	getGroups(String,String,Vector,Vector)
getLDAPAttributes(String,DirContext[],String)	getLDAPAttributes(String,DirContext,String,String[])
getLDAPAttributes(String,DirContext[])	getLDAPAttributes(String,DirContext,String,String[])
RA_PROCESS_NAME	com.waveset.adapter.ActiveSync#RA_PROCESS_RULE
removeNameFromAttribute(DirContext,Name,Attribute)	removeNameFromAttribute(DirContext,String,boolean,Attribute)
removeUserFromAllGroups(Name,String,WavesetResult)	removeUserFromAllGroups(String,boolean,String,WavesetResult)
removeUserFromGroup(DirContext,Name,String,String,Attributes)	removeUserFromGroup(DirContext,String,boolean,String,String,Attributes)
removeUserFromGroups(Name,Vector,String,WavesetResult)	removeUserFromGroups(String,boolean,Vector,String,WavesetResult)

## com.waveset.adapter.MySQLResourceAdapter

Verworfenne Methode	Nachfolger
getAccountAttributes(String)	

## com.waveset.adapter.NaturalResourceAdapter

Verworfenne Methode	Nachfolger
getAccountAttributes(String)	

**com.waveset.adapter.NDSResourceAdapter**

Verworfenne Methode	Nachfolger
buildEvent(UpdateRow)	
getBaseContextAttrName()	com.waveset.adapter.ResourceAdapter#getBaseContexts()

**com.waveset.adapter.ONTDirectorySmartResourceAdapter**

Verworfenne Methode	Nachfolger
getAccountAttributes(String)	

**com.waveset.adapter.OS400ResourceAdapter**

Verworfenne Methode	Nachfolger
getAccountAttributes(String)	

**com.waveset.adapter.PeopleSoftComponentActiveSyncAdapter**

Verworfenne Methoden oder Felder	Nachfolger
DEFAULT_AUDIT_STAMP_FORMAT	
DEFAULT_AUDIT_STAMP_START_DATE	
getAccountAttributes(String)	
getUpdateRows(UpdateRow)	getUpdateRows(UpdateRow)
RA_AUDIT_STAMP_FORMAT	

## Verworfenen Methoden und Felder

### **com.waveset.adapter.RACFResourceAdapter**

Verworfenen Methode	Nachfolger
getAccountAttributes(String)	

### **com.waveset.adapter.RASecureConnection**

Verworfenen Methode	Nachfolger
ExchangeAuth(boolean)	ExchangeAuth(boolean,byte[])

### **com.waveset.adapter.RedHatLinuxResourceAdapter. BlockAcctlter**

Verworfenen Methode	Nachfolger
BlockAcctlter(int,CaptureList)	BlockAcctlter(SVIDResourceAdapter,Capture List)

### **com.waveset.adapter.RequestResourceAdapter**

Verworfenen Methode	Nachfolger
getAccountAttributes(String)	

### **com.waveset.adapter.ResourceAdapter**

Verworfenen Methode	Nachfolger
getAccountAttributes(String)	
getBaseContextAttrName()	getBaseContexts()

### com.waveset.adapter.ResourceAdapterBase

Verworfenne Methode	Nachfolger
getAccountAttributes(String)	
getAdapter(Resource,LighthouseContext)	getAdapterProxy(Resource,LighthouseContext)
getAdapter(Resource,ObjectCache,WSUser)	getAdapterProxy(Resource,ObjectCache)
getAdapter(Resource,ObjectCache)	getAdapterProxy(Resource,LighthouseContext)
getBaseContextAttrName()	getBaseContexts()
isExcludedAccount(String,Rule)	com.waveset.adapter.ResourceAdapterProxy #isExcludedAccount(String, Map,ResourceOperation,Rule)
isExcludedAccount(String)	com.waveset.adapter.ResourceAdapterProxy #isExcludedAccount(String, Map,ResourceOperation,Rule)

### com.waveset.adapter.ResourceAdapterProxy

Verworfenne Methode	Nachfolger
getAccountAttributes(String)	
getBaseContextAttrName()	getBaseContexts()

### com.waveset.adapter.ResourceManager

Verworfenne Methode	Nachfolger
getResourceTypes()	getResourcePrototypes() getResourcePrototypes(ObjectCache,boolean)
getResourceTypeStrings()	getResourcePrototypeNames(ObjectCache)

## Verworfenne Methoden und Felder

### **com.waveset.adapter.SAPHRActiveSyncAdapter**

Verworfenes Feld	Nachfolger
RA_PROCESS_NAME	com.waveset.adapter.ActiveSync#RA_PROCESS_RULE

### **com.waveset.adapter.SAPResourceAdapter**

Verworfenne Methode	Nachfolger
unexpirePassword(String,WavesetResult)	unexpirePassword(String,String,WavesetResult)
unexpirePassword(WSUser,WavesetResult)	unexpirePassword(String,String,WavesetResult)

### **com.waveset.adapter.ScriptedConnection**

Unterklasse	Verworfenne Methode	Nachfolger
Skript	hasNextToken()	
Skript	nextToken()	
ScriptedConnection	disconnect()	com.waveset.adapter.ResourceConnection#disconnect()
ScriptedConnection Factory	getScriptedConnection(String,HashMap)	com.waveset.adapter.ScriptedConnectionPool#getConnection(HashMap,String,long,boolean)
SSHConnection	disconnect()	disconnect()
TelnetConnection	disconnect()	disconnect()

### **com.waveset.adapter.ScriptedHostResourceAdapter**

Verworfenne Methode	Nachfolger
getAccountAttributes(String)	

### **com.waveset.adapter.SkeletonResourceAdapter**

Verworfenne Methode	Nachfolger
getAccountAttributes(String)	

### **com.waveset.adapter.SMEResourceAdapter**

Verworfenne Methode	Nachfolger
getAccountAttributes(String)	

### **com.waveset.adapter.SQLServerResourceAdapter**

Verworfenne Methode	Nachfolger
getAccountAttributes(String)	

### **com.waveset.adapter.SunAccessManagerResourceAdapter**

Verworfenne Methode	Nachfolger
getAccountAttributes(String)	
getBaseContextAttrName()	com.waveset.adapter.ResourceAdapter#getBaseContexts()

## Verworfenne Methoden und Felder

### **com.waveset.adapter.SVIDResourceAdapter.BlockAcctlter**

Verworfenne Methoden oder Felder	Nachfolger
BlockAcctlter(int,CaptureList)	BlockAcctlter(CaptureList)
BlockAcctlter(SVIDResourceAdapter,CaptureList)	BlockAcctlter(CaptureList)

### **com.waveset.adapter.SybaseResourceAdapter**

Verworfenne Methode	Nachfolger
getAccountAttributes(String)	

### **com.waveset.adapter.TestResourceAdapter**

Verworfenne Methode	Nachfolger
getAccountAttributes(String)	

### **com.waveset.adapter.TopSecretResourceAdapter**

Verworfenne Methode	Nachfolger
hasError(String,String)	hasError(String,String,String)
login(HostAccess hostAccess)	login(HostAccess,ServerAffinity)

### **com.waveset.adapter.VerityResourceAdapter**

Verworfenne Methode	Nachfolger
getAccountAttributes(String)	

**com.waveset.adapter.XMLResourceAdapter**

Verworfenne Methode	Nachfolger
getAccountAttributes(String)	

**com.waveset.msgcat.Catalog**

Verworfenne Methode	Nachfolger
getMessage(String, Object[], Locale)	format (Locale, String, Object[])
getMessage(Locale, String, Object[])	format (Locale, String, Object[])
getMessage(Locale, String)	format (Locale, String)
getMessage(String, Locale)	format (Locale, String)
getMessage(String, Object[])	format (Locale, String, Object[])

**com.waveset.object.Account**

Verworfenne Methode	Nachfolger
getUnowned()	hasOwner()
setUnowned(boolean)	setOwner(WSUser)

**com.waveset.object.AccountAttributeType**

Verworfenne Methode	Nachfolger
getAttrType()	getSyntax()
setAttrType(String)	setSyntax(String) setSyntax(Syntax)

## Verworfenne Methoden und Felder

### com.waveset.object.Attribute

Verworfenne Methoden oder Felder	Nachfolger
BLOCK_SIZE	BLOCK_ROWS_GET BLOCK_ROWS_LIST
EVENTDATE	EVENT_DATETIME
EVENTTIME	EVENT_DATETIME
getDbColumnLength()	
getDbColumnName()	
STARTUP_TYPE_AUTO	com.waveset.object.Resource#STARTUP_TYPE_AUTO
STARTUP_TYPE_AUTO_FAILOVER	com.waveset.object.Resource#STARTUP_TYPE_AUTO_FAILOVER
STARTUP_TYPE_DISABLED	com.waveset.object.Resource#STARTUP_TYPE_DISABLED
STARTUP_TYPE_MANUAL	com.waveset.object.Resource#STARTUP_TYPE_MANUAL
STARTUP_TYPES	com.waveset.object.Resource#STARTUP_TYPES
STARTUP_TYPES_DISPLAY_NAMES	com.waveset.object.Resource#STARTUP_TYPES_DISPLAY_NAMES

### com.waveset.object.AttributeDefinition

Verworfenne Methode	Nachfolger
AttributeDefinition(String,String)	AttributeDefinition(String,Syntax)
setAttrType(String)	setSyntax(Syntax)

### com.waveset.object.AuditEvent

Verworfenne Methode	Nachfolger
setAttributeMap(Map)	setAuditableAttributes(Map)
addAuditableAttributes(AccountAttributeType[], WSAttributes)	setAuditableAttributes(Map)
getAttributeMap()	getAuditableAttributes()
getAttributeValue(String)	getAuditableAttributes()
setAccountAttributesBlob(Map)	setAccountAttributesBlob(Map,Map)
setAccountAttributesBlob(WSAttributes,List)	setAccountAttributesBlob(WSAttributes,WSAttributes,List)

### com.waveset.object.CacheManager

Verworfenne Methode	Nachfolger
getAllObjects(Type,AttributeCondition[])	listObjects(Type,AttributeCondition[])
getAllObjects(Type,WSAttributes)	listObjects(Type,WSAttributes)
getAllObjects(Type)	listObjects(Type)

### com.waveset.object.Constants

Verworfenes Feld	Nachfolger
MAX_SUMMARY_STRING_LENGTH	

## Verworfenne Methoden und Felder

### com.waveset.object.EmailTemplate

Verworfenne Methoden oder Felder	Nachfolger
setToAddress(String)	setTo(String)
getFromAddress()	getFrom()
getToAddress()	getTo()
setFromAddress(String)	setFrom(String)
VAR_FROM_ADDRESS	VAR_FROM
VAR_TO_ADDRESS	VAR_TO

### com.waveset.object.Form

Verworfenne Methoden oder Felder	Nachfolger
EL_HELP	com.waveset.object.GenericObject#toMap(int)
getDefaultDataType()	getDefaultSyntax()
getType()	getSyntax()
setType(String)	setSyntax(Syntax)

### com.waveset.object.GenericObject

Verworfenne Methode	Nachfolger
toMap(boolean)	toMap(String,int)
toMap(String,boolean)	

### com.waveset.object.LoginConfig

Verworfenne Methode	Nachfolger
getApp(String)	getLoginApp(String)

**com.waveset.object.MessageUtil**

Verworfenne Methode	Nachfolger
getActionDisplayKey(String)	
getEventParmDisplayKey(String)	
getResultDisplayKey(String)	
getTypeDisplayKey(String)	com.waveset.ui.FormUtil#getTypeDisplayNa me(LighthouseContext,String)

**com.waveset.object.RepositoryResult**

Verworfenne Methode	Nachfolger
get(int)	next()
getId(int)	
getName(int)	
getObject(int)	
getRowCount()	
getRows()	
seek(int)	hasNext() next()
sort()	

**com.waveset.object.RepositoryResult.Row**

Verworfenne Methode	Nachfolger
getSummaryAttributes()	getAttributes()

## Verworfenne Methoden und Felder

### com.waveset.object.ResourceAttribute

Verworfenne Methode	Nachfolger
setType(String)	setSyntax(Syntax)

### com.waveset.object.TaskInstance

Verworfenes Feld	Nachfolger
DATE_FORMAT	com.waveset.util.Util#stringToDate(String,String) com.waveset.util.Util#getCanonicalDate(Date) com.waveset.util.Util#getCanonicalDate(Date,TimeZone) com.waveset.util.Util#getCanonicalDate(long)
VAR_RESULT_LIMIT	setResultLimit(int) getResultLimit()
VAR_TASK_STATUS	

### com.waveset.object.TaskTemplate

Verworfenne Methode	Nachfolger
setMode(String)	setExecMode(String)
setMode(TaskDefinition.ExecMode)	setExecMode(TaskDefinition,ExecMode)

### com.waveset.object.Type

Verworfenne Methoden oder Felder	Nachfolger
AUDIT_CONFIG	
AUDIT_PRUNER_TASK	
AUDIT_QUERY	
DISCOVERY	

## Verworfenne Methoden und Felder

Verworfenne Methoden oder Felder	Nachfolger
getSubtypes()	getLegacyTypes()
NOTIFY_CONFIG	
REPORT_COUNTER	
SUMMARY_REPORT_TASK	
USAGE_REPORT	
USAGE_REPORT_TASK	

### **com.waveset.object.UserUIConfig**

Verworfenne Methode	Nachfolger
getCapabilityGroups()	
getAppletColumns()	getAppletColumnDefs()
getCapabilityGroup(String)	
getCapabilityGroupNames()	
getFindMatchOperatorDisplayNameKeys()	
getFindMatchOperators()	
getFindResultsColumns()	
getFindResultsSortColumn()	
getFindUserDefaultSearchAttribute()	
getFindUserSearchAttributes()	
getFindUserShowAttribute(int)	
getFindUserShowCapabilitiesSearch(int)	
getFindUserShowDisabled(int)	
getFindUserShowOrganizationSearch(int)	
getFindUserShowProvisioningSearch(int)	
getFindUserShowResourcesSearch(int)	
getFindUserShowRoleSearch(int)	

## Verworfenne Methoden und Felder

### com.waveset.object.ViewMaster

Verworfenne Methode	Nachfolger
ViewMaster()	ViewMaster(LighthouseContext)
ViewMaster(String,String)	ViewMaster(LighthouseContext)
ViewMaster(Subject,String)	ViewMaster(LighthouseContext)

### com.waveset.session

Unterklasse	Verworfenne Methoden oder Felder	Nachfolger
Sitzung	listApprovers()	getAdministrators(Map)
	listControlledApprovers()	getAdministrators(Map)
	listSimilarApprovers(String adminName)	getAdministrators(Map)
SessionFactory	getApp(String)	getLoginApp(String)
	getApps()	getLoginApps()
WorkflowServices	ARG_TASK_DATE	com.waveset.object.Attribute#DATE

### com.waveset.task.TaskContext

Verworfenne Methode	Nachfolger
getAccessPolicy()	
getRepository()	

**com.waveset.ui.util.FormUtil**

Verworfenne Methode	Nachfolger
getAdministrators(Session,List)	getUsers(LighthouseContext,Map)
getAdministrators(Session,Map)	getUsers(LighthouseContext,Map)
getApplications(LighthouseContext,List)	getApplications(LighthouseContext,Map)
getApplications(LighthouseContext)	getApplications(LighthouseContext,Map)
getApproverNames(Session,List)	getUsers(LighthouseContext,Map)
getApproverNames(Session)	getUsers(LighthouseContext,Map)
getApprovers(Session,List)	getUsers(LighthouseContext,Map)
getApprovers(Session)	getUsers(LighthouseContext,Map)
getCapabilities(LighthouseContext,List,Map)	getCapabilities(LighthouseContext,Map)
getCapabilities(LighthouseContext,List)	getCapabilities(LighthouseContext,Map)
getCapabilities(LighthouseContext,String,String)	getCapabilities(LighthouseContext,Map)
getCapabilities(LighthouseContext)	getCapabilities(LighthouseContext,Map)
getObjectNames(LighthouseContext,String,List,Map)	getObjectNames(LighthouseContext,String,Map)
getObjectNames(LighthouseContext,String,List)	getObjectNames(LighthouseContext,String,Map)
getObjectNames(LighthouseContext,String,String,String,List,Map)	getObjectNames(LighthouseContext,String,Map)
getObjectNames(LighthouseContext,String,String,String,List)	getObjectNames(LighthouseContext,String,Map)
getObjectNames(LighthouseContext,Type,String,String,List,Map)	getObjectNames(LighthouseContext,String,Map)
getObjectNames(LighthouseContext,Type,String,String,List)	getObjectNames(LighthouseContext,String,Map)
getOrganizations(LighthouseContext,boolean,List)	getOrganizationsDisplayNames(LighthouseContext,Map)
getOrganizations(LighthouseContext,boolean)	getOrganizationsDisplayNames(LighthouseContext,Map)
getOrganizations(LighthouseContext,List)	getOrganizationsDisplayNames(LighthouseContext,Map)

## Verworfenne Methoden und Felder

Verworfenne Methode	Nachfolger
getOrganizations(LighthouseContext)	getOrganizationsDisplayNames(LighthouseContext,Map)
getOrganizationsDisplayNames(LighthouseContext,boolean,List)	getOrganizationsDisplayNames(LighthouseContext,Map)
getOrganizationsDisplayNames(LighthouseContext,boolean)	getOrganizationsDisplayNames(LighthouseContext,Map)
getOrganizationsDisplayNames(LighthouseContext)	getOrganizationsDisplayNames(LighthouseContext,Map)
getOrganizationsDisplayNamesWithPrefixes(LighthouseContext,List)	getOrganizationsDisplayNames(LighthouseContext,Map)
getOrganizationsDisplayNamesWithPrefixes(LighthouseContext)	getOrganizationsDisplayNames(LighthouseContext,Map)
getOrganizationsWithPrefixes(LighthouseContext,List)	getOrganizationsDisplayNames(LighthouseContext,Map)
getOrganizationsWithPrefixes(LighthouseContext)	getOrganizationsDisplayNames(LighthouseContext,Map)
getSimilarApproverNames(Session,String)	getUsers(LighthouseContext,Map)
getSimilarApproverNames(Session)	getUsers(LighthouseContext,Map)
getSimilarApprovers(Session,String)	getUsers(LighthouseContext,Map)
getSimilarApprovers(Session)	getUsers(LighthouseContext,Map)
getUnassignedOrganizations(LighthouseContext,List)	getOrganizationsDisplayNames(LighthouseContext,Map)
getUnassignedOrganizations(LighthouseContext)	getOrganizationsDisplayNames(LighthouseContext,Map)
getUnassignedOrganizationsDisplayNames(LighthouseContext,List)	getOrganizationsDisplayNames(LighthouseContext,Map)
getUnassignedOrganizationsDisplayNames(LighthouseContext,Map)	getOrganizationsDisplayNames(LighthouseContext,Map)
getUnassignedOrganizationsDisplayNames(LighthouseContext)	getOrganizationsDisplayNames(LighthouseContext,Map)
getUnassignedOrganizationsDisplayNamesWithPrefixes(LighthouseContext,List)	getOrganizationsDisplayNames(LighthouseContext,Map)
getUnassignedOrganizationsDisplayNamesWithPrefixes(LighthouseContext)	getOrganizationsDisplayNames(LighthouseContext,Map)

## Verworfenne Methoden und Felder

Verworfenne Methode	Nachfolger
getUnassignedOrganizationsWithPrefixes(LighthouseContext,List)	getOrganizationsDisplayNames(LighthouseContext,Map)
getUnassignedOrganizationsWithPrefixes(LighthouseContext)	getOrganizationsDisplayNames(LighthouseContext,Map)
getUnassignedResources(LighthouseContext,List,List)	getUnassignedResources(LighthouseContext,Map)
getUnassignedResources(LighthouseContext,String,List)	getUnassignedResources(LighthouseContext,Map)
getUnassignedResources(LighthouseContext,String)	getUnassignedResources(LighthouseContext,Map)

## com.waveset.ui.util.html

Unterklasse	Verworfenne Methoden oder Felder	Nachfolger
Komponente	isNoWrap()	
	setHelpKey(String)	
	setNoWrap(boolean)	
HtmlHeader	NORMAL_BODY	
MultiSelect	isLockhart()	
	setLockhart(boolean)	
WizardPanel	setPreviousLabel(String)	setPrevLabel(String)

## com.waveset.util.JSSE

Verworfenne Methode	Nachfolger
installIfAvailable()	

## Verworfenne Methoden und Felder

### **com.waveset.util.PdfReportRenderer**

Verworfenne Methode	Nachfolger
render(Element,boolean,String,OutputStream)	render(Element,boolean,String,OutputStream,String,boolean)
render(Element,boolean,String)	render(Element,boolean,String,String,boolean)
render(Report,boolean,String,OutputStream)	render(Report,boolean,String,OutputStream,String,boolean)
render(Report,boolean,String)	render(String,boolean,String,String,boolean)

### **com.waveset.util.Quota**

Verworfenne Methode	Nachfolger
getQuota()	

### **com.waveset.util.ReportRenderer**

Verworfenne Methoden oder Felder	Nachfolger
renderToPdf(Report,boolean,String,OutputStream)	renderToPdf(Report,boolean,String,OutputStream,String,boolean)
renderToPdf(Report,boolean,String)	renderToPdf(Report,boolean,String,String,boolean)

**com.waveset.util.Trace**

Verworfenne Methode	Nachfolger
data(long, Object, String, byte[])	com.sun.idm.logging.trace.Trace#data(long, String, byte[])
entry(long, Object, String, Object[])	com.sun.idm.logging.trace.Trace#entry(long, String, Object[])
entry(long, Object, String, String)	com.sun.idm.logging.trace.Trace#entry(long, String)
entry(long, Object, String)	com.sun.idm.logging.trace.Trace#entry(long, String)
exception(long, Object, String, t)	com.sun.idm.logging.trace.Trace#throwing(long, String, Throwable) com.sun.idm.logging.trace.Trace#caught(long, String, Throwable)
exit(long, Object, String, boolean)	com.sun.idm.logging.trace.Trace#exit(long, String, boolean)
exit(long, Object, String, int)	com.sun.idm.logging.trace.Trace#exit(long, String, int)
exit(long, Object, String, long)	com.sun.idm.logging.trace.Trace#exit(long, String, long)
exit(long, Object, String, Object)	com.sun.idm.logging.trace.Trace#exit(long, String, Object)
exit(long, Object, String)	com.sun.idm.logging.trace.Trace#exit(long, String)
getTrace()	com.sun.idm.logging.trace.TraceManager#getTrace(String)
getTrace(Class)	com.sun.idm.logging.trace.TraceManager#getTrace(String)
getTrace(String)	com.sun.idm.logging.trace.TraceManager#getTrace(String)
level1(Class, String)	com.sun.idm.logging.trace.Trace#level1(String)
level1(Object, String)	com.sun.idm.logging.trace.Trace#level1(String)
level2(Class, String)	com.sun.idm.logging.trace.Trace#level2(String)
level2(Object, String)	com.sun.idm.logging.trace.Trace#level2(String)
level3(Class, String)	com.sun.idm.logging.trace.Trace#level3(String)
level3(Object, String)	com.sun.idm.logging.trace.Trace#level3(String)
level4(Class, String)	com.sun.idm.logging.trace.Trace#level4(String)
level4(Object, String)	com.sun.idm.logging.trace.Trace#level4(String)
variable(long, Object, String, String, boolean)	com.sun.idm.logging.trace.Trace#variable(long, String, String, boolean)

## Verworfenen Methoden und Felder

Verworfenen Methode	Nachfolger
variable(long, Object, String, String, int)	com.sun.idm.logging.trace.Trace#variable(long, String, String, int)
variable(long, Object, String, String, long)	com.sun.idm.logging.trace.Trace#variable(long, String, String, long)
variable(long, Object, String, String, Object)	com.sun.idm.logging.trace.Trace#variable(long, String, String, Object)
void info(long, Object, String, String)	com.sun.idm.logging.trace.Trace#info(long, String, String)

## com.waveset.util.Util

Verworfenen Methoden oder Felder	Nachfolger
DATE_FORMAT_CANONICAL	stringToDate(String, String) getCanonicalDate(Date) getCanonicalDate(Date, TimeZone) getCanonicalDate(long)
debug(Object)	
getCanonicalDateFormat()	stringToDate(String, String) getCanonicalDate(Date) getCanonicalDate(Date, TimeZone) getCanonicalDate(long)
getOldCanonicalDateString(Date, boolean)	getCanonicalDateString(Date)
rfc2396URLPieceEncode(String, String)	com.waveset.util.RFC2396URLPieceEncode#encode(String, String)
rfc2396URLPieceEncode(String)	com.waveset.util.RFC2396URLPieceEncode#encode(String)

## com.waveset.workflow.WorkflowContext

Verworfenen Feld	Nachfolger
VAR_CASE_TERMINATED	com.waveset.object.WFProcess#VAR_CASE_TERMINATED