

# Sun Java™ System Identity Manager Versionshinweise

Version 7.1 Juni 2007

Teilenummer 820-2282-10

---

Diese Versionshinweise enthalten wichtige Informationen, die zum Zeitpunkt der Herausgabe von Sun Java System Identity Manager 7.1 verfügbar waren. Hier finden Sie u. a. Informationen zu neuen Funktionen, Verbesserungen und bekannten Problemen. Lesen Sie dieses Dokument, bevor Sie beginnen, mit Identity Manager 7.1 zu arbeiten.

Diese Versionshinweise sind in die folgenden Abschnitte unterteilt:

- [Einführung](#)
- [Identity Manager 7.1-Funktionen](#)
- [Bekannte Probleme](#)
- [Installations- und Aktualisierungshinweise](#)
- [Verworfen API](#)
- [Erweiterungen und Korrekturen der Dokumentation](#)

Dieses Dokument enthält URLs von Drittanbietern, die auf zusätzliche Informationen zum Thema verweisen.

---

**HINWEIS** Sun kann für die Verfügbarkeit von Drittanbieter-Websites, die in diesem Dokument angegeben sind, nicht verantwortlich gemacht werden. Sun übernimmt keine Verantwortung oder Haftung für Inhalte, Werbungen, Produkte oder andere Materialien, die auf oder über derartige Websites oder Ressourcen verfügbar sind. Sun übernimmt keine Verantwortung oder Haftung für tatsächliche oder angebliche Schäden oder Verluste, die durch den Gebrauch von oder in Verbindung mit derartigen Inhalten, Gütern oder Diensten entstanden sind, die auf diesen oder durch diese Websites oder Ressourcen verfügbar sind.

---

# Einführung

In diesem Abschnitt der Identity Manager 7.1-Versionshinweise finden Sie folgende Informationen:

- [Unterstützte Software und Umgebungen](#)
- [Aufrüstungsmöglichkeiten und EOSL](#)
- [Weitervertreibbare Dateien](#)
- [Melden von Problemen und Feedback](#)
- [Sun freut sich auf Ihre Kommentare](#)
- [Zusätzliche Sun-Ressourcen](#)

---

## Unterstützte Software und Umgebungen

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

- [Betriebssysteme](#)
- [Anwendungsserver](#)
- [Repository-Datenbankserver](#)
- [Sun Identity Manager Gateway](#)
- [Unterstützte Ressourcen](#)
- [Webserver](#)
- [Browser](#)
- [Nicht mehr unterstützte Software](#)

---

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

---

# Betriebssysteme

Diese Version von Identity Manager unterstützt die folgenden 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 x86
- 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). Für Identity Manager ist JDK 1.4.2 oder höher erforderlich.

- Apache® Tomcat
  - Version 4,1.x (mit JDK 1.4.2)
  - Version 5.0.x (mit JDK 1.4.2)
  - Version 5.5.x (mit JDK 1.5)
- BEA WebLogic® Express 8.1 (mit JDK 1.4.2 oder höher)
- BEA WebLogic® Server™8.1 (mit JDK 1.4.2 oder höher)
- BEA WebLogic® Server™9.1, 9.2
- IBM WebSphere® 6.0, 6.1
- IBM WebSphere® Application Server - Express Version 5.1.1 (mit JDK 1.4.2)
- JBoss Application Server 4.0.x
- 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
- Sun Java™System Application Server Enterprise Edition 8.2

---

**HINWEIS** Wenn Ihr derzeitiger Anwendungsserver JDK 1.4.2 oder höher nicht unterstützt, erkundigen Sie sich beim Hersteller vor der Installation von Identity Manager 7.1 über die Aufrüstung auf eine geeignete Version.

---

## Repository-Datenbankserver

Identity Manager unterstützt die folgenden Repository-Datenbankserver:

- IBM® DB2® Universal Database for Linux, UNIX® und Windows® (Version 7.x, 8.1, 8.2)
- Microsoft SQL Server™2005
- MySQL™5.0

---

**HINWEIS** Identity Manager unterstützt MySQL nur in Entwicklungsumgebungen. In Produktionsumgebungen wird MySQL nicht unterstützt.

---

- Oracle 9i® und Oracle Database 10g, 10g Release 1 und 10g Release 2®

---

**HINWEIS** Oracle RAC (Real Application Cluster) wird in einer Aktiv/Passiv-Konfiguration mit zwei Knoten unterstützt. Bei einer solchen Konfiguration ist der Parameter `active_instance_count` auf 1 gesetzt. Wenn zusätzlich das Failover des JDBC-Treibers bei Ausfall einer Verbindung aktiviert ist, erhält man eine Failover-Konfiguration für das Repository. Wie dies in der jeweiligen Umgebung zu konfigurieren ist, wird in der Oracle-Dokumentation beschrieben.

Oracle RAC wird zurzeit in keiner anderen Konfiguration unterstützt.

---

# Sun Identity Manager Gateway

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

---

**HINWEIS** Der Novell GroupWise-Adapter wurde verworfen und ist in der nächsten Identity Manager-Hauptversion nicht mehr enthalten. Stattdessen können Sie den NetWare NDS-Adapter verwenden, denn dieser unterstützt auch GroupWise-Konten.

---

## Unterstützte Ressourcen

Identity Manager unterstützt die folgenden Ressourcen:

- [CRM \(Customer Relationship Management\)](#)
- [Datenbanken](#)
- [Enterprise Resource Planning \(ERP\)](#)
- [Help Desk](#)
- [Messaging-Plattformen](#)
- [Sonstiges](#)
- [Betriebssysteme](#)
- [Rollenverwaltungssystem](#)
- [Sicherheitsmanager](#)
- [Steuerung des Webzugriffs](#)

### CRM (Customer Relationship Management)

- Siebel CRM-Software, Version 6.2, 7.0.4, 7.7, 7.8

## Datenbanken

- Generische Datenbanktabellen
- 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, 2005
- MySQL™ 4.1.x, 5.x
- Oracle 9i®
- Oracle Database 10g Release 1®
- Sybase Adaptive Server® 12.x
- Skript-JDBC

## Verzeichnisse

- LDAP v3
- RACF LDAP
- Microsoft® Active Directory® 2000, 2003
- Novell® eDirectory on Novell NetWare 5.1, 6.0 und 6.5
- Open LDAP
- Sun™ ONE Directory Server 4.x
- Sun Java™ System Directory Server 5 2004Q2, 2005Q1

- 
- HINWEISS**
- 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 retro changelog-Plug-In 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 E-Business Suite auf Oracle Applications 11.5.9, 11.5.10
- Peoplesoft® PeopleTools 8.1 bis 8.48 mit HRMS 8.0 bis 9.0
- 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)
- SAP® Governance, Risk, and Compliance (GRC) Access Enforcer

## Help Desk

- Remedy Help Desk 4.5, 5.0, 6.0
- BMC Remedy Action Request System Server 6.0, 6.03 und 7.0
- BMC Remedy Service Desk Application 7.0

## Messaging-Plattformen

- Blackberry RIM Enterprise Server 4+ (verwendet Generic Windows Script Adapter)
- Sun Java System Messaging and Calender Service
- Lotus Notes® 5.0 6.5, 6.5.4, 7.0 (Domino)
- Microsoft® Exchange 5.5, 2000, 2003
- Novell® GroupWise 6.0, 6.5 und 7.0 (mit dem Novell NDS-Adapter)

- 
- HINWEISS**
- Microsoft Exchange 2000 und 2003 werden von Microsoft Windows Active Directory 2000 und 2003 verwaltet.
  - Der Blackberry-Ressourcenadapter wird in zukünftigen Versionen nicht mehr unterstützt. Zukünftige Implementierungen, in denen Ressourcenadapter für Blackberry Enterprise Server Version 4+ erforderlich sind, sollten auf dem ScriptedGateway-Ressourcenadapter basieren.
  - Der Novell GroupWise-Adapter wurde verworfen und ist in der nächsten Identity Manager-Hauptversion nicht mehr enthalten. Stattdessen können Sie den NetWare NDS-Adapter verwenden, denn dieser unterstützt auch GroupWise-Konten.
-

## Sonstiges

- Flat Files
- 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 UNIX Shell Script
- 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

## Rollenverwaltungssystem

- BridgeStream SmartRoles

## Sicherheitsmanager

- ActivCard® 5.0
- eTrust CA-ACF2® Security
- Natural
- IBM RACF®
- Skript-Host
- INISafe Nexess 1.1.5
- RSA ClearTrust 5.5.2, 5.5.3

- RSA® SecurID® 5.0, 6.0
- RSA® SecurID® 5.1, 6.0 for 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 (Realms wird seit 2005Q4 unterstützt)

## Webserver

---

**HINWEIS** Die Integration zwischen einem Anwendungsserver und Webserver ist für Identity Manager nicht erforderlich. Die Auswahl eines Webserver bietet einen besseren Lastausgleich 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

## Browser

Identity Manager unterstützt die folgenden Browser:

- Microsoft Internet Explorer 5.x oder höher
- Safari v2.0 oder höher für Mac OS X 10.3.3 oder höher
- Mozilla 1.78 (mit JRE 1.5)
- Firefox 1.0x, 1.5 (mit JRE 1.5), 2.0 und höher

## Nicht mehr unterstützte Software

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

Softwarekategorie	Softwarepaket
<b>Betriebssysteme</b>	<ul style="list-style-type: none"> <li>• IBM AIX 4.3.3</li> </ul>
<b>Anwendungsserver</b>	<ul style="list-style-type: none"> <li>• Apache Tomcat 4.1.x</li> <li>• BEA Weblogic Express 8.1</li> <li>• BEA Weblogic Server 8.1</li> <li>• IBM Websphere Application Server - Express Version 5.1.1</li> <li>• IBM Websphere 6.0</li> <li>• Sun ONE Application Server 7</li> </ul>
<b>Repository-Datenbankserver</b>	<ul style="list-style-type: none"> <li>• MySQL 4.1</li> <li>• Microsoft SQL 2000</li> </ul>
<b>Ressourcen</b>	<ul style="list-style-type: none"> <li>• ActivCard 5.0</li> <li>• Lotus Notes (Domino) 5.0.x, 6.0.x</li> <li>• Microsoft Windows NT 4.0</li> <li>• Sun Identity Manager Gateway ausgeführt auf Microsoft Windows NT 4.0</li> <li>• MySQL 4.1</li> <li>• Novell® GroupWise 5.x, 6.0, 6.5</li> <li>• Novell® eDirectory on Novell NetWare 5.1, 6.0</li> <li>• Oracle 8i (über den Oracle-Ressourcenadapter)</li> <li>• Red Hat Linux 8.0</li> <li>• Remedy® Help Desk 4.5, 5.0</li> <li>• SAP R/3 v4.5, v4.6</li> <li>• Siebel 6.2</li> <li>• Sun ONE Identity Server 6.0</li> </ul>

Die folgenden abhängigen Softwareprodukte werden in Identity Manager 7.1 nicht mehr unterstützt:

Softwarekategorie	Softwarepaket
<b>Repository-Datenbankserver</b>	<ul style="list-style-type: none"> <li>• Oracle 8i</li> <li>• IBM DB2 Universal Database for Linux, UNIX, and Windows 7.0</li> </ul>
<b>Betriebssysteme</b>	<ul style="list-style-type: none"> <li>• Solaris 7, Microsoft Windows NT 4.0</li> </ul>
<b>Ressourcen</b>	<ul style="list-style-type: none"> <li>• Microsoft Exchange 5.5</li> <li>• IBM DB2 7.0</li> <li>• Novell® GroupWise 5.x</li> </ul>

## API-Unterstützung

Die Identity Manager 7.1-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
Bericht	com.waveset.report.BaseReportTask

---

Aufgabe	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

---

Identity Manager SPE enthält außerdem die öffentlichen Klassen, die in der folgenden Tabelle aufgelistet sind.

---

API-Typ	Klassennamen
SPE	com.sun.idm.idmx.api.* 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.

## Verworfenen APIs

Der Abschnitt „[Verworfenen API](#)“ enthält alle Identity Manager-APIs (Application Programming Interfaces), die in dieser Version verworfen wurden. Außerdem werden deren Nachfolger aufgelistet, falls verfügbar.

# Aufrüstungsmöglichkeiten und EOSL

In diesem Abschnitt finden Sie Informationen zu den Aufrüstungsmöglichkeiten, die für Identity Manager existieren und eine Beschreibung der EOSL-Richtlinien (End of Service Life) für Identity Manager-Produkte und -Softwaresupport.

## Identity Manager Aufrüstungsmöglichkeiten

In der folgenden Tabelle sind die Aufrüstungsmöglichkeiten beschrieben, die bei der Aufrüstung auf eine neuere Version von Identity Manager berücksichtigt werden müssen.

Aktuelle Version	Zielversion				
	5.0	2005Q3M1	2005Q4M3	7.0	7.1
Waveset Lighthouse 4.1 SPx	5.0	5.0 > 2005Q3M1	5.0 > 2005Q4M3	5.0 > 2005Q4M3 > 7.0	5.0 > 2005Q4M3 > 7.1
Identity Manager 5.0 SPx		2005Q3M1	2005Q4M3	2005Q4M3 > 7.0	2005Q4M3 > 7.1
Identity Manager 2005Q1M3 Identity Auditor 1.0		2005Q3M1	2005Q4M3	2005Q4M3 > 7.0	2005Q4M3 > 7.1
Identity Manager 2005Q3M1 Identity Manager 5.5			2005Q4M3	2005Q4M3 > 7.0	2005Q4M3 > 7.1
Identity Manager 2005Q3M3 Identity Manager SPE 1.0			2005Q4M3	2005Q4M3 > 7.0	2005Q4M3 > 7.1
Identity Manager 2005Q4M3 Identity Manager 6.0				7.0	7.1
Identity Manager 7.0					7.1

- 
- HINWEIS**
- Bei der Aufrüstung von Identity Manager ist es nicht erforderlich, innerhalb einer Hauptversion zum Aufrüsten auf die nächste Hauptversion Service Packs zu installieren. Wenn Sie z. B. von Identity Manager 5.0 auf 6.0 aufrüsten, müssen Sie keine der 5.0 Service Packs installieren.
  - Service Packs sind für eine Hauptversion kumulierend. Nach der Aufrüstung auf die Hauptversion können Sie daher das letzte Service Pack installieren, ohne alle für diese Version herausgegebenen Service Packs installieren zu müssen. Wenn Sie z. B. auf Identity Manager 5.0 aufrüstet haben, erhalten Sie durch die Installation von SP6 die gesamte Funktionalität, die in den Service Packs SP1 bis SP5 enthalten ist.
- 

Aktualisierungen der Identity Manager-Dokumentation werden wie folgt verfügbar gemacht:

- **Alle Versionen** (einschließlich Service Packs): Es werden Versionshinweise herausgegeben, in denen behobene Fehler, Produktverbesserungen, neue Funktionen und andere wichtige Informationen beschrieben sind.
- **Hauptversionen** (x.0): Es wird die gesamte Identity Manager-Dokumentation aktualisiert und neu herausgegeben.
- **Nebenversionen und Service Packs**: Es werden einzelne Dokumente aktualisiert und neu herausgegeben oder Dokumentationsnachträge verfügbar gemacht.

## Ende (EOSL) des Softwaresupports

Während des EOSL-Zeitraums wird der Identity Manager-Softwaresupport in zwei Phasen angeboten:

- *Phase 1: Voller Support*
- *Phase 2: Beschränkter Support*

---

**HINWEIS** Die Dauer des vollen Produktsupports variiert von Produkt zu Produkt.

---

## Phase mit vollem Support

In der Phase mit vollem Support gewährt Sun Microsystems, Inc. Softwaresupport gemäß dem Support-Vertrag (einschließlich der zutreffenden Serviceliste), den der Kunde mit Sun abgeschlossen hat. Näheres zur Serviceliste finden Sie unter:

<http://www.sun.com/service/servicelist/>

Nach Ablauf des EOSL-Datums haben Sie jedoch keinen Zugriff mehr auf Softwareaktualisierungen und -aufrüstungen für dieses Softwareprodukt.

## Phase mit beschränktem Support

In der Phase mit beschränktem Support gewährt Sun Microsystems, Inc. Softwaresupport gemäß dem Support-Vertrag (einschließlich der zutreffenden Serviceliste), den der Kunde mit Sun abgeschlossen hat. Näheres zur Serviceliste finden Sie unter:

<http://www.sun.com/service/servicelist/>

Der Kunde ist jedoch nicht berechtigt, Fehler einzureichen oder neue Patches von Sun Microsystems, Inc., zu erhalten. Wie bereits in der Phase mit vollem Support haben Sie nach Ablauf des EOSL-Datums jedoch keinen Zugriff mehr auf Softwareaktualisierungen und -aufrüstungen für dieses Softwareprodukt.

Die EOSL- und EOL-Daten für ältere Versionen von Identity Manager sind in der folgenden Tabelle zusammengefasst.

Produktname	Produkt-status	Letzte Auslieferung	Phase 1 Enddatum	Phase 2 Enddatum (EOSL)	EOL-Bekanntgabe
Sun Java System Identity Manager 7.0	Post-RR				
Sun Java System Identity Manager 6.0 2005Q4	Post-RR	05/25/2007	05/25/2008	05/2012	11/20/06
Sun Java System Identity Auditor 1.0 2005Q1	Post-RR	02/02/2007	02/2008	02/2012	08/01/06
Sun Java System Identity Manager Service Provider Edition 1.0 2005Q3	Post-RR	02/02/2007	02/2008	02/2012	08/01/06
Sun Java System Identity Manager 5.0 2004Q3	EOL	08/11/2006	08/2007	08/2011	02/07/06
Sun Java System Identity Manager 5.0 SPx 2004Q3	EOL	08/11/2006	08/2007	08/2011	02/07/06
Sun Java System Identity Manager 5.5	EOL	08/11/2006	08/2007	08/2011	02/07/06
Waveset Lighthouse 4.1			03/2006	03/2010	

## Weitervertreibbare Dateien

Sun Java System Identity Manager 7.1 enthält keine Dateien für den Weitervertrieb.

---

## Melden von Problemen und Feedback

Wenn bei der Arbeit mit Sun Java System Identity Manager Probleme auftreten, wenden Sie sich wie folgt an den Sun-Kundendienst:

- Online-Softwaresupport von Sun unter <http://www.sun.com/service/sunone/software>  
Diese Site bietet neben Links zur Knowledge Base, zum Online Support Center und zum ProductTracker auch Wartungsprogramme und Support-Kontaktnummern.
- Die telefonische Abfertigungsnummer für Ihren Wartungsvertrag

Damit wir Sie optimal unterstützen können, möchten wir Sie bitten, die folgenden Informationen bereitzuhalten, wenn Sie sich an den Support wenden:

- Beschreibung des Problems, einschließlich der Situation, in der das Problem aufgetreten ist und die damit verbundenen Auswirkungen
- Gerätetyp, Version des Betriebssystems und Produktversion, einschließlich Patches und andere Software, die einen Einfluss auf das Problem haben könnte
- Detaillierte Informationen zur Vorgehensweise bei der Wiederholung des Problems
- Fehlerprotokolle oder Speicherabbilder

---

## Sun freut sich auf Ihre Kommentare

Sun ist stets bemüht, die Qualität der Dokumentation zu verbessern und ist dabei auf Ihre Kommentare und Vorschläge angewiesen.

Wenn Sie einen Kommentar einreichen möchten, gehen Sie zu <http://docs.sun.com> und klicken auf Send Comments. Geben Sie auf dem Onlineformular den Namen und die Teilenummer der

Dokumentation an. Die Teilenummer ist eine sieben- bis neunstellige Zahl, die auf der Titelseite der Buches oder oben auf der Dokumentation angegeben ist. Der Titel dieser Dokumentation ist z. B. Sun Java System Identity Manager Juni 2007 Versionshinweise und die Teilenummer 820-2282-10.

---

## Zusätzliche Sun-Ressourcen

Hilfreiche Informationen zum Sun Java System finden Sie im Internet unter:

- Dokumentation für Sun Java™ System Identity Manager  
<http://docs.sun.com/app/docs/coll/1514.1>
- Dokumentation für Sun Java System  
<http://docs.sun.com/prod/java.sys>
- Sun Java System Professional Services  
<http://www.sun.com/service/sunps/sunone>
- Softwareprodukte und -service für Sun Java System  
<http://www.sun.com/software>
- Softwaresupport für Sun Java System  
<http://www.sun.com/service/sunone/software>
- Support und Knowledge Base für Sun Java System  
<http://www.sun.com/service/support/software>
- Sun-Support und -Schulungsangebote  
<http://training.sun.com>
- Sun Java System Consulting und Professional Services  
<http://www.sun.com/service/sunps/sunone>
- Informationen für Sun Java System-Entwickler  
<http://developers.sun.com>
- Sun Developer Support Services  
<http://www.sun.com/developers/support>
- Sun Java System Softwareschulung  
<http://www.sun.com/software/training>
- Datenblätter für Sun-Software  
<http://www.sun.com/software>

Copyright © 2007 Sun Microsystems, Inc. Alle Rechte vorbehalten.

Sun Microsystems, Inc., hat Rechte in Bezug auf geistiges Eigentum an der Technologie, die in dem in diesem Dokument beschriebenen Produkt enthalten ist. Im Besonderen und ohne Einschränkung umfassen diese Ansprüche in Bezug auf geistiges Eigentum eines oder mehrere der unter <http://www.sun.com/patents> aufgelisteten Patente und eines oder mehrere Patente oder Anwendungen mit laufendem Patent in den USA und in anderen Ländern.

SUN URHEBERRECHTLICH/VERTRAULICH.

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

Die Verwendung unterliegt Lizenzbestimmungen.

Diese Ausgabe kann von Drittanbietern entwickelte Bestandteile enthalten.

Bestimmte Teile können von Berkeley BSD Systems stammen (Lizenzierung über U. von CA).

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

# Identity Manager 7.1-Funktionen

In diesem Abschnitt der Identity Manager 7.1-Versionshinweise finden Sie folgende Informationen:

- [Neue Funktionen in dieser Version](#)
- [In dieser Version behobene Fehler](#)

---

## Neue Funktionen in dieser Version

In diesem Abschnitt finden Sie zusätzliche Informationen zu den neuen Funktionen in Identity Manager 7.1, die in die folgenden Abschnitte unterteilt sind:

- [Installation und Aktualisierung](#)
- [Administrator- und Benutzeroberflächen](#)
- [Überwachung](#)
- [Formulare](#)
- [Integrierte Entwicklungsumgebung \(IDE\) von Identity Manager](#)
- [Identity Manager SPE](#)
- [Repository](#)
- [Ressourcen](#)
- [Rollen](#)
- [Sicherheit](#)
- [Server](#)

## Installation und Aktualisierung

- Wenn Ihre Bereitstellungsumgebung aus mehreren Identity Manager-Instanzen besteht, die auf ein Repository auf einem einzelnen physischen Server verweisen, können Sie mit dem Attribut `waveset.serverId` eindeutige Servernamen festlegen. (ID-11578)
- Installation und Aufrüstung können auf einem System ohne Monitor ausgeführt werden. (ID-14258)
- Ein Skript zum Erstellen einer Identity Manager Service Provider-Transaktionsdatenbank für MySQL ist nun unter `sample/create_spe_tables.mysql` verfügbar. (ID-14666)

MySQL wird nicht als Service Provider-Transaktionsdatenbank unterstützt. Das Skript dient lediglich Vorführungszwecken.

- Für die Lokalisierung: Die zuvor für das Verfahren Upgrade Pre-Process benötigte Datei `RAMessage_110n.jar` wurde entfernt und Sie müssen für die Adapter Übersetzungen herunterladen. (ID-16272)

Sprachpakete können vom Sun Download Center heruntergeladen werden, das zum Online Support Center gehört (<http://www.sun.com/download>). Für den Zugriff auf das Download Center ist ein registrierter Kontoname und ein Passwort erforderlich.

Weitere Informationen finden Sie unter Identity Manager 7.1-Installation und in der Identity Manager L10n-Readme-Datei, die in jedem IDM-Sprachpaket enthalten ist.

## Administrator- und Benutzeroberflächen

- Wenn ein Benutzer seine Benutzer-ID vergisst, kann er nun in `login.jsp` oder `user/login.jsp` auf `Forgot My User ID` klicken, um eine neue Seite Lookup User ID zu öffnen. Auf dieser Seite kann der Benutzer eine E-Mail-Adresse für Benachrichtigungen und einige weitere Identity-Attributwerte angeben (z. B. Telefonnummer, Vor- und Nachname, Mitarbeiter-ID usw.). Identity Manager versucht dann, einen Benutzer zu lokalisieren, der mit den angegebenen Identity-Attributwerten übereinstimmt. (ID-4924)
  - Wenn dieser Vorgang erfolgreich durchgeführt werden kann, sendet Identity Manager eine E-Mail mit der Identity Manager-Benutzer-ID an die angegebenen E-Mail-Adresse für Benachrichtigungen. (Für diesen Zweck wurde die neue Vorlage User ID Recovery Email Template erstellt. Die Betreffzeile und der Körper dieser Vorlage bestehen aus Meldungsschlüsseln, damit diese benutzerspezifisch angepasst und internationalisiert werden können.)
  - Wenn der Vorgang nicht erfolgreich ist, wird eine Fehlermeldung ausgegeben, die angibt, dass Identity Manager keinen Benutzer finden konnte, der mit den angegebenen Daten übereinstimmt oder mehrere Benutzer lokalisiert hat, auf die diese Daten zutreffen.

Diese Funktion ist standardmäßig aktiviert, sie kann jedoch deaktiviert werden.

- Wenn Sie im Rahmen einer Anmeldemodulgruppe (von der untergeordneten Registerkarte Sicherheit > Anmelden) ein Ressourcen-Anmeldemodul (Nicht-Identity-System-Benutzer-ID / Password-Anmeldemodul) bearbeiten, können Sie nun eine Anmeldekorrelationsregel auswählen, um die vom Benutzer angegebenen Anmeldeinformationen einem Identity Manager-Benutzer zuzuordnen.

Identity Manager sucht auf der Grundlage der Logik, die in der Anmeldekorrelationsregel angegeben ist, nach einem Identity Manager-Benutzer. Die Regel muss eine Liste mit einem oder mehreren `AttributeConditions`-Elementen zurückgeben und dann nach einem Identity Manager-Benutzer suchen, der diesen Bedingungen entspricht.

Möglicherweise ist eine Übereinstimmung mit der Identity Manager-Benutzer-ID schon ausreichend. Wenn die Identity Manager-Benutzer eine Konto-ID für LDAP-Ressourcen haben, können Sie auch nach der Konto-ID suchen; Identity Manager-Benutzer benötigen dann keine Access Manager-Ressourcenverknüpfung. Das `authType`-Attribut der Anmeldekorrelationsregel muss `LoginCorrelationRule` lauten. (ID-8577)

- Der Synchronisationsstatus wird in der Spalte Beschreibung der Ressourcenbaumstruktur nicht mehr angegeben. Die Spalte Status enthält nun einen für Abstimmung und Synchronisation kombinierten Status. (ID-12465, ID-14005)
- Die Serverkonfigurations- und E-Mail-Vorlagen wurden dahingehend geändert, dass der Administrator nun bestimmen kann, ob auf dem SMTP-Server SSL oder Authentifizierung durchgeführt werden soll. (ID-14899)

Weitere Informationen finden Sie in *Sun Java™ System Identity Manager Administration*.

## Überwachung

- Sie können Richtlinienverletzungen jetzt priorisieren, indem Sie ihnen eine Priorität, einen Schweregrad oder beides zuweisen. Verwenden Sie zum Priorisieren von Richtlinienverletzungen die Seite „Korrekturen“. Weitere Informationen finden Sie unter „Prioritizing Policy Violations“ in *Identity Manager Administration*. (ID-11703)
- Bei der Überwachungsrichtliniensuche werden jetzt auch Mitglieder dynamischer Organisationen einbezogen. (ID-12437)
- Die Überwachungsrichtliniensuche kann jetzt geplant werden. (ID-12474)
- Für die Überwachungsrichtliniensuche gibt es jetzt einen Testmodus, bei dem die Korrektur deaktiviert ist und alle Verletzungen nach Abschluss der Suche gelöscht werden. (ID-12522)

- In der Verletzungszusammenfassung können jetzt Verletzungen anhand des Verletzungsstatus ausgewählt werden. Die Zusammenfassung kann so konfiguriert werden, dass nur Verletzungen mit einem oder mehreren möglichen Statuswerten gemeldet werden. (ID-12612)
- Einträge im Überwachungsprotokoll, die mit Genehmigungen, Ablehnungen und Korrekturen von Zugriffsprüfungen verbunden sind, können nun digital signiert werden. (ID-13264)
- Nach dem Starten einer regelmäßigen Zugriffsprüfung wird Ihre Suche auf der Zugriffsprüfungsseite erst dann in der Liste angezeigt, wenn Sie auf die Schaltfläche Aktualisieren klicken. (D-14169)
- Richtlinienzuweisungen werden nun von Verzeichniszuordnungen und virtuellen Organisationen unterstützt. (ID-14591)
- Der Benutzergültigkeitsbereich von Zugriffsabfragen kann nun auf der Grundlage von zugewiesenen Ressourcen definiert werden. (ID-14654)
- In Identity Manager kann Konformität jetzt durch Installation der Demo-Umgebung schnell nachgewiesen werden. (ID-14970)

Für die Installation der Konformitäts-Demo-Umgebung importieren Sie `sample/auditordemo.xml` oder erstellen eine eigene Demo-Umgebung mit den Tools in `Compliance/RuleBuilder`. Weitere Informationen finden Sie in `Compliance/RuleBuilder/README.txt`.

- Für die Bescheinigungs- und Korrekturfunktionen können jetzt Formulare angegeben werden, die genau die Details enthalten, mit denen sich die Effizienz beim Bescheinigen and Korrigieren erhöhen lässt. Weitere Informationen finden Sie im Abschnitt „Erweiterungen und Korrekturen der Dokumentation“ in diesen Versionshinweisen. (ID-14973)
- Konformitätsverletzungen können nun während der Korrektur neu bewertet werden, um festzustellen, ob sie weiterhin aktiv sind. Ein Benutzer kann so bearbeitet werden, dass die Überwachungsrichtlinie nicht erneut verletzt wird. (ID-15019)
- Noch ausstehende Zugriffsprüfungsberechtigungen können nun mit aktuellen Berechtigungsdaten aktualisiert werden. (ID-15027)
- Mit Hilfe einer neuen Schaltflächen zum Bearbeiten auf dem Korrekturformular kann ein Benutzer direkt durch eine Zugriffsprüfungs-Korrekturfunktion bearbeitet (neu bereitgestellt) werden. (ID-15172)
- Mit Hilfe einer neuen Schaltflächen zum Bearbeiten auf dem Korrekturformular kann ein Benutzer direkt durch eine Konformitätsprüfungs-Korrekturfunktion bearbeitet (neu bereitgestellt) werden. (ID-15173)

- Benutzeransprüche können nun auf einem dieser Wege durch eine Zugriffsprüfung geändert werden: (ID-15180)
  - Der Zugriffsprüfungs-Bescheiniger fordert durch Klicken auf Rescan eine erneute Prüfung an, was dazu führt, dass die Benutzeransprüche aktualisiert und neu bewertet werden.
  - Der Zugriffsprüfungs-Bescheiniger klickt auf Korrigiert, was dazu führt, dass der Benutzeranspruch aktualisiert und neu bewertet wird.
- Durch einen Benutzeranspruch, der im Zustand WIRD KORRIGIERT erstellt wird, wird automatisch ein Korrekturarbeitselement erstellt. (ID-15423)

Weitere Informationen finden Sie in Kapitel 2, „Working with Rules“, in *Identity Manager Deployment Tools*.

**Aufrüstung:** Der Hinweis zur Massenbescheinigung und alle E-Mail-Vorlagen bleiben nach einer Aufrüstung erhalten. Der Hinweis zur Massenbescheinigung in der Datei `auditorwfs.xml` zeigt jedoch, wie die neuen Benachrichtigungsvariablen des Zugriffsprüfungskorrektur-Arbeitselements implementiert werden können.

- Die Zielressourcen können bei Auditorabfragen nun genauer angegeben werden, um Ressourcen mit mehreren Konten zu unterstützen. (ID-15485)
- Die Verwaltungsseite für Überwachungsrichtlinienobjekte ist jetzt Formular-basiert und kann angepasst werden. Sie können die vollständige Ansicht mit detaillierten Informationen oder eine Teilansicht mit weniger Details auswählen. Weitere Informationen finden Sie im Dokumentationsnachtrag in diesen Versionshinweisen. (ID-15486)
- Die Verwaltungsseite für Zugriffsabfragen ist jetzt Formular-basiert und kann angepasst werden. Weitere Informationen finden Sie im Dokumentationsnachtrag in diesen Versionshinweisen. (ID-15515)
- Die Details von Rollenänderungen werden nun in Überwachungsprotokollen festgehalten. (ID-15587)
- Standardmäßig werden nur die folgenden Ereignisse im Zusammenhang mit Benutzeransprüchen protokolliert (ID-15735):
  - Bescheiniger genehmigt
  - Bescheiniger zurückgewiesen
  - Angeforderte Korrektur
  - Erneute Prüfung angefordert
  - Beenden

## Formulare

- Die Anzeigeklasse `TabPanel` unterstützt nun die Ausführung von Validierungsausdrücken Registerkarte für Registerkarte. Wenn Sie die Anzeigeklasse `validatePerTab` auf **true** einstellen, führt Identity Manager Validierungsausdrücke aus, sobald der Benutzer zu einer anderen Registerkarte wechselt. (ID-12442)
- Im Ordner `sample/forms` steht nun ein VMS-Beispielformular zur Verfügung. (ID-12835)

## Integrierte Entwicklungsumgebung (IDE) von Identity Manager

Identity Manager Integrated Development Environment (Identity Manager IDE) ist eine Java-Anwendung, mit der Sie Identity Manager-Objekte in Ihrer Bereitstellung anzeigen, benutzerspezifisch anpassen und auf Fehler durchsuchen können.

In der Identity Manager IDE wurden in Identity Manager 7.1 die folgenden Funktionen geändert bzw. neu hinzugefügt:

---

**HINWEIS** Weitere Informationen zu diesen Funktionen finden Sie in *Identity Manager Deployment Tools*

---

- Die Identity Manager IDE unterstützt jetzt `GenericObjects`. (ID-12952, 12991)
- Auf der NetBean-Menüleiste der obersten Ebene gibt es nun ein IDM-Menü, in dem Sie Vorgänge auswählen können, die für die ausgewählten Objektknoten geeignet sind. (ID-13158)
- Das Identity Manager IDE 7.0-Projekt wurde durch die beiden folgenden Projekttypen ersetzt. Bei beiden handelt es sich um NetBeans `ant`-Projekte: (ID-14587)
  - **Identity Manager Project:** Primäre Entwicklungsumgebung für Bereitsteller, da dieser Projekttyp den größeren Funktionsumfang bietet, wie z. B.:
    - Java/JSP-Bearbeitung, -Erstellung, -Fehlersuche
    - Starten von Identity Manager in einem in Netbeans eingebetteten Anwendungsserver

- Verwalten eines eingebetteten Repositorys
  - Bei diesem Projekttyp steht ein einfaches Repository zu Testzwecken in der Sandbox-Umgebung zur Verfügung. Beim Erstellen des Projekttyps können Sie ein eingebettetes Repository für das Projekt angeben. Außerdem können Sie eine Option zum Verwalten des eingebetteten Repository aktivieren und das Repository neu initialisieren. Die Identity Manager IDE verfügt über eine Funktion für die automatische Veröffentlichung, mit der das eingebettete Repository beim Ausführen oder Debuggen des Projekts automatisch geladen wird.
- Beispiel-CBE (Configuration Build Environment) und Importdateigenerator. Weitere Informationen über die CBE finden Sie in der Datei `README.txt` zum Identity Manager-Projekt.
- **Identity Manager Project (Remote):** Für kleinere Änderungen und die Fehlersuche in entfernten Projekten auf einem externen Server. Dieser kompakte und leicht einzurichtende Projekttyp bietet sämtliche Bearbeitungsfunktionen von Identity Manager Project, verfügt aber nicht über die Erstellungsumgebung und die Fähigkeit zum Starten von `war`-Dateien.
- Die Identity Manager IDE ist jetzt unabhängig von der Version. (ID-14723)

Version 7.1 der Identity Manager IDE `.nbm` ist nicht mehr an die Identity Manager-Klassen gebunden. In der Version 7.1 unterstützt `.nbm` Identity Manager 7.0 und 7.1 und soll zukünftig auch Identity Manager 6.0 SP3 unterstützen.

Jedes Identity Manager IDE-Projekt ist an eine bestimmte Identity Manager-Version gebunden. Für die Identity Manager IDE ist jetzt ein -Kompatibilitätspaket (`ide-bundle.zip`) erforderlich, das Identity Manager `jar`-Dateien und einige XML-Registries mit versionsspezifischen Informationen für die unterstützten Identity Manager-Versionen zur Verfügung stellt. Das Kompatibilitätspaket wird bei der Projekterstellung angegeben:

- Für **Identity Manager-Projekte**: Das Kompatibilitätspaket ist in der Datei `idm.war` enthalten. Identity Manager IDE greift während der Projekteinrichtung automatisch auf diese Datei zu.
- Für **Identity Manager-Projekte (Remote)**: Da bei entfernten Projekten der Speicherort der Datei `war` nicht angegeben wird, müssen Sie den Speicherort des Kompatibilitätspakets angeben, und zwar:

*Identity Manager-Installations-Root-Verzeichnis/sample/ide-bundle.zip*

---

**HINWEIS** In Identity Manager Version 7.0 ist kein IDE-Kompatibilitätspaket enthalten, Sie können die Datei jedoch von der Identity Manager 7.0-Download-Site herunterladen.

---

- Der Liste der Objekttypen, die im Explorer-Fenster angezeigt wird, wurden Bibliotheksobjekte mit Eigenschaftsfenstern, Palettenfunktionen und Navigationsknoten hinzugefügt. (ID-14817)
- Das Identity Manager IDE-Plug-In benötigt nun JDK 1.5 und Netbeans 5.5. (ID-14950)
- Sie können jetzt ein einzelnes Objekt oder einen Objektordner in einem lokalen Verzeichnis (rekursiv) mit denen im Repository vergleichen (diff). Mit dieser Funktion lassen sich die Unterschiede zwischen den lokalen Kopien und den Kopien auf dem Server anzeigen. Außerdem können Sie mit dieser Funktion modifizierte Objekte hochladen und neu laden. (ID-15151, 15206)
- Wenn Sie für ein Regelobjekt die Designansicht wählen, wird im Editor-Fenster nun ein Ausdrucks-Generator angezeigt, der es ermöglicht, die logische Struktur einer Regel besser zu veranschaulichen und die Eigenschaften der Regel zu ändern. (ID-15104)
- Den Dialogfeldern des Identity Manager IDE-Ausdrucks-Generators wurden neue Merkmale und Funktionen hinzugefügt. Sie haben jetzt folgende Möglichkeiten:
  - Einfache Datentypen (ganze Zahlen und Zeichenfolgen) können direkt in der Tabelle des Ausdrucks-Generators bearbeitet werden. (ID-15528)
  - Beim Definieren von XPRESS-invoke-Anweisungen (statisch oder Instanz) können Sie JavaDoc-Dokumente zu Identity Manager API-Methoden in den Dialogfeldern des Ausdrucks-Generators anzeigen lassen. (ID-12961)  

Wenn Sie Klassen oder Methoden im Menü „Class Name“ bzw. „Method Name“ im Ausdrucks-Generator auswählen, erscheint die entsprechende JavaDoc-Anzeige in einem Pop-up-Fenster neben dem Dialogfeld. (ID-12960)
  - Eigenschaftenwerte, die Ausdrücke und primitive Werte (wie Zeichenfolgen) unterstützen, können direkt in einer Eigenschaftentabelle bearbeitet werden. (ID-13763)
  - Sie können nun direkt einen bestimmten Ausdruck erstellen, anstatt zuerst einen BLOCK zu erstellen und diesen dann in den gewünschten Ausdruck umzuwandeln. (ID-15932)
  - Ein Element in einem Ausdruck kann in einem anderen enthalten sein, so dass sich komplexe Ausdrücke erstellen lassen.
  - Der Ausdruckstyp von Elementen kann mit der neuen Schaltfläche „Change To“ und dem entsprechenden Dialogfeld geändert werden. (ID-15933)
- Die Identity Manager IDE bietet jetzt eigene Knoten für Dateien, persistente Objekte und Erweiterungen, was dem zugrunde liegenden XML-Inhalt besser entspricht. Außerdem können Sie Knoten neu ordnen und Knoten an anderer Stelle einfügen (vor, nach oder in anderen Knoten in der Projektstruktur). (ID-14689)
- Sie können nun Objekte im Identity Manager IDE-Repository löschen. (ID-14081, 15031)

- Sie können nun ein Objekt in die Identity Manager IDE eines Identity Manager 7.0 Servers hochladen und dem Objekt manuell eine ID zuweisen. (ID-15474)
- Um das Verschieben von Objekten zwischen Repositories zu erleichtern, können Sie jetzt die Identity Manager IDE so konfigurieren, dass vor dem Herunterladen aus dem Repository alle automatisch generierten Repository-IDs gelöscht werden. (ID-15307, 15347)  
Die Identity Manager IDE sucht und löscht alle Objekt-IDs und objectRef-IDs, die einem bestimmten Ausdruck entsprechen. Festcodierte, vordefinierte IDs werden dabei nicht gelöscht.
- Beim Bearbeiten von Formularen können Sie jetzt Verweisen auf Formulare und Felder folgen. Beim Bearbeiten von Workflows können Sie zudem externen Prozessen folgen. Die Identity Manager IDE öffnet die entsprechende Datei und sucht die Stelle, auf die verwiesen wird. (ID-14428, 15406)
- Sie können jetzt einen Root-Kontext angeben, indem Sie beim Erstellen des Projekts das Feld „Context“ leer lassen. (ID-15912)

## Identity Manager SPE

- Identity Manager SPE unterstützt jetzt Link-Korrelations- und Link-Bestätigungsregeln. (ID-10500) Weitere Informationen finden Sie in der Beschreibung des Fehlers 15760 im Dokumentationsnachtrag in diesen Versionshinweisen.
- Authentifizierungsantworten für Service Provider-Benutzer können nun auf der Administratorenoberfläche bearbeitet werden. (ID-12781)
- Über LDAP gelöschte Attribute werden jetzt propagiert, sobald eine ausgefallene Ressource wieder zur Verfügung steht. (ID-15471)

## Berichte

- Sie können die beim Generieren von Berichten verwendete Schriftart jetzt global steuern. Bearbeiten Sie dazu die Einstellungen auf der Seite „Konfigurieren > Berichte“. Wenn Sie für einzelne Berichte eine andere Schriftart festlegen wollen, bearbeiten Sie die Konfiguration des jeweiligen Berichts. Standardmäßig werden nur Schriftarten angezeigt, die von allen PDF-Viewern unterstützt werden.

Wenn Sie zusätzliche Schriftarten zum System hinzufügen wollen, kopieren Sie Schriftartdefinitionsdateien in das Unterverzeichnis `WEB-INF/fonts` in dem Verzeichnis, in dem IDM installiert ist (Beispiel: `/var/opt/SUNWappserver/domains/domain1/applications/j2ee-modules/idm/WEBINF/fonts` ).

Danach müssen Sie den Server neu starten. Es werden unter anderem die Schriftartdefinitionsformate .ttf, .ttc, .otf und .afm unterstützt. Wenn eine dieser Schriftarten ausgewählt wird, muss die jeweilige Schriftart auf dem Computer verfügbar sein, auf dem der Bericht angezeigt wird, oder in den Bericht eingebettet sein.

Die Standardschriftarten unterstützen nicht alle Zeichensätze. Zeichen aus asiatischen Sprachen werden z. B. nicht standardmäßig unterstützt. Wenn Sie Berichte generieren wollen, in denen solche Zeichen angezeigt werden können, müssen Sie daher die entsprechende Schriftart im Verzeichnis `fonts/` installieren und in den Konfigurationsseiten auswählen. (ID-10641/14376)

---

**HINWEIS** TrueType-Schriftarten werden mit verschiedenen möglichen Einbettungsstufen lizenziert. Für die zum Generieren der PDF-Datei ausgewählte Schriftart muss eine entsprechende Lizenz vorhanden sein, damit die Schriftart so eingebettet werden kann, dass Sie die PDF-Datei drucken und als Vorschau anzeigen können. Wenn für das Einbetten der Schriftart in die PDF-Datei keine entsprechende Lizenz vorliegt, wird die PDF mit der Standardschriftart generiert. In diesem Fall wird der Inhalt der PDF-Datei beschädigt. In Identity Manager wird zurzeit kein Fehler protokolliert, um Sie auf dieses Problem hinzuweisen.

---

## Repository

- Es sind nun Informationen über die Größe von Repository-Objekten verfügbar. Zugriff auf diese Informationen ist über die Webseiten und die Befehlszeile der Konsole möglich. (ID-9896)

---

**HINWEIS** Bei Aufrüstungen geben vorhandene Objekte eine Größe von 0 an, bis diese aktualisiert oder anderweitig erneuert wurden.

---

## Ressourcen

### Neue Ressourcenadapter

In dieser Version wurden die folgenden Adapter hinzugefügt:

- RACF-LDAP
- SAP Governance, Risk, and Compliance (GRC) Access Enforcer

Weitere Informationen zu diesen Ressourcenadapter finden Sie in *Identity Manager Resources Reference*.

## Aktualisierungen bei Ressourcenadaptern

- Server, die in der Synchronisationsrichtlinie für die Ressource ActiveSync ausführen, sollten nun konfiguriert werden. `waveset.properties` können zwar weiterhin eingesetzt werden, von ihrem Gebrauch ist jedoch abzuraten. Von einer Migration zum Konfigurieren von Synchronisationsrichtlinien ist unbedingt abzuraten. (ID-10167)
- Das Konfigurieren des Flat File ActiveSync-Adapters wurde vereinfacht, insbesondere für Dateien mit Trennzeichen. (ID-11678)
- ActiveSync kann beendet werden, bevor der LDAP-Adapter alle Aktualisierungen verarbeitet hat. (ID-13695)
- Identity Manager unterstützt jetzt PeopleSoft HRMS 9.0. (ID-14195)
- Der Domino-Adapter unterstützt nun die Einstellung des expliziten Richtlinienattributs für Domino 7.0-Ressourcen. (ID-14315)
- Der Oracle ERP-Ressourcenadapter wird nun vor und nach der Ausführung von Aktionen unterstützt. (ID-14659)
- Der standardmäßige RACF-Mechanismus zum Angeben von Benutzern `AttrParse` 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)
- 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)
- Die Unterstützung von GroupWise durch den NDS-Adapter wurde verbessert:
  - Der Adapter ermöglicht jetzt das Verwalten von Post Offices in sekundären Domänen. (ID-15122)
  - GroupWise-Benutzer können jede bekannte Verteilungsliste abonnieren. (ID-15707)
  - Es ist nicht mehr erforderlich, den Parameter **Delete Pattern** des Adapters zu verwenden, wenn festgelegt werden soll, dass ein GroupWise-Benutzer einem Post Office nicht mehr angehören soll. Stattdessen muss jetzt nur noch das Post Office-Feld auf " " (doppelte Anführungszeichen) gesetzt werden. Vorhandene Formulare oder Workflows, bei denen Post Offices programmgesteuert entfernt werden, müssen Sie entsprechend ändern, so dass das Feld auf "" gesetzt wird. (ID-15970)
- Der Domino-Ressourcenadapter unterstützt für Domino 7.0-Server Roaming-Benutzer. (ID-15157)

- 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 ACF2-Adapter unterstützt ACF2 8.0 SP2. (ID-15833)
- Die Beispieldatei `NDSUserForm` enthält praktische Beispiele für alle sieben Verfahren zum Abrufen von Post Offices und Verteilungslisten. (ID-15872)
- Der Adapter für die PeopleSoft-Komponentenschnittstelle unterstützt nun die Angabe separater Schlüssel für die Operationen GET, FIND und CREATE auf einer Komponentenschnittstelle. (ID-16055)
- Der Adapter für die PeopleSoft-Komponentenschnittstelle unterstützt nun PeopleTools 8.1 bis 8.48. (ID-16128)
- 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)

## Rollen

- 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 Aufrüstungsprozesses 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, stellen Sie das `RoleUpdater`-Attribut `nofixsubrolelinks` auf `true` ein. 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](#)“.

- Das Delegierungsmodell wurde wie folgt geändert: (ID-15440)
  - Wenn Sie einen Benutzer bearbeiten, der an einen oder mehrere Benutzer bzw. an eine Regel delegiert wurde, der bzw. die nach der ursprünglichen Festlegung der Delegierung gelöscht wurde, wird der Benutzer oder die Regel, der bzw. die Ziel der Delegierung war, nun in Klammern angezeigt, um deutlich zu machen, dass dieses Element gelöscht wurde. Zum Beispiel: „(auser)“
  - Wenn der aufzulistende Delegierte des Benutzers geändert wird, aber weiterhin den gelöschten Delegierten enthält, wird ein Ausnahmefehler erzeugt und der Speichervorgang schlägt fehl. Wenn der aufzulistende Delegierte des Benutzers nicht geändert wird, jedoch andere Attribute des Benutzers geändert werden, ist eine Speicherung möglich, da es keine Änderungen der Delegierungsinformationen gibt.
  - Wenn Sie einen Benutzer erstellen oder aktualisieren und der Genehmiger an einen Benutzer delegiert wurde, der nicht mehr existiert, kann keine Erstellung oder Aktualisierung durchgeführt werden. Zudem wird eine Meldung angezeigt, die angibt, dass das Genehmigungselement nicht konfigurationsgemäß delegiert werden konnte, da der Delegierte gelöscht wurde.
  - Arbeitselemente, die an einen Benutzer delegiert wurden, der anschließend gelöscht wurde, können vom delegierenden Benutzer wiederhergestellt werden. Der delegierende Benutzer kann die Delegierung an den gelöschten Benutzer dann beenden.

Weitere Informationen finden Sie in *Sun Java™ System Identity Manager Administration*.

## Sicherheit

- Identity Manager ermöglicht nun die Definition unterschiedlicher Delegierungskonfigurationen für verschiedene Arbeitselementtypen (z. B. Bescheinigungen, Korrekturen, Genehmigungen usw.). (ID-14152)
- Identity Manager wurde eine neue integrierte Objektgruppe/Organisation mit der Bezeichnung Endbenutzer hinzugefügt. (ID-14630)

Diese neue Objektgruppe/Organisation ist ein Mitglied des obersten Elements („Top“). Sie hat anfangs keine Mitgliedobjekte. Diese Objektgruppe/Organisation wird auf der Administratoroberfläche nicht in der Baumstruktur der Registerkarte Konten angezeigt und kann keine untergeordneten Organisationen haben. Sie können ein Objekt jedoch beim Bearbeiten von Objekten (z. B. Rollen, AdminRoles, Ressourcen, Richtlinien oder Aufgaben) mit Hilfe der Administratoroberfläche für die Objektgruppe/Organisation des Endbenutzers verfügbar machen.

Zuvor wurden Benutzern beim Anmelden bei der Endbenutzer-Interface automatisch die Rechte für Objekttypen zugeordnet, die in der Endbenutzerfähigkeit angegeben waren (z. B. AdminRole, EndUserConfig oder EndUserTask). Zudem weist Identity Manager diesen nun automatisch die Steuerung der neuen Endbenutzer-Objektgruppe zu und bewertet eine integrierte Endbenutzerregel für kontrollierte Organisationen. Wenn Organisationsnamen zurückgegeben werden, übergibt Identity Manager auch die Steuerung für diese Organisationen an diese Benutzer. Identity Manager verwendet die Ansicht des authentifizierenden Benutzers als Eingabeargument für die Endbenutzerregel für kontrollierte Organisationen. Die Regel kann eine Organisation (in Form einer Zeichenkette) oder mehrere Organisationen (in Form einer Liste) zurückgeben, für die der Benutzer, der sich bei der Endbenutzer-Interface anmeldet, die Endbenutzerrechte hat.

Darüber hinaus wurde für die Verwaltung der neuen Objekte eine neue Administratorfunktion für Endbenutzer hinzugefügt. Benutzer mit dieser Fähigkeit können die Rechte für Objekttypen, die in der Endbenutzerfähigkeit angegeben sind, und für die Inhalte der Endbenutzerregel für kontrollierte Organisationen anzeigen und bearbeiten. Diese Fähigkeit wird standardmäßig dem Konfigurator zugewiesen. Alle Änderungen an der Liste oder den Organisationen, die durch die Evaluierung der Endbenutzerregel für kontrollierte Organisationen zurückgegeben werden, werden für angemeldete Benutzer nicht dynamisch wiedergegeben. Um die Änderungen anzuzeigen, müssen diese Benutzer sich zunächst ab- und dann wieder anmelden.

Sie sollten diese neue Objektgruppe/Organisation als die beste praktische Methode betrachten, um Endbenutzern Zugriff auf Konfigurationselemente von Identity Manager wie z. B. Rollen, Ressourcen, Aufgaben usw., zu gewähren.

Sie sollten diese Methode dann zukünftig anstelle von Endbenutzeraufgaben, Endbenutzerressourcen, System Configuration:EndUserAccess und authTypes für Endbenutzer verwenden, obwohl diese Methoden zur Gewährleistung der Abwärtskompatibilität weiterhin unterstützt werden.

- Sie können einer Passworthistorie eines Benutzers nun beim Erstellen eines Benutzers Passwörter hinzufügen. (ID-15179)
- Wenn Sie Objekte (wie z. B. Rollen oder Ressourcen) auflisten und für jedes der zurückgegebenen Objekte über sechs memberObjectGroups-Elemente vorhanden sind, werden abgeschnittene memberObjectGroups-Elemente nun von Identity Manager nicht mehr aus den Ergebnissen herausgefiltert. (ID-15181)

---

**HINWEIS** Dies gilt jedoch nicht für USER, da diese nur zu einer Objektgruppe gehören können.

---

- 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

- Sie können nun festlegen, dass im Rahmen der Verfolgung eine Methode *und* alle zugehörigen untergeordneten Aufrufe (sowohl direkt als auch indirekt) verfolgt werden sollen. Dies ist insbesondere bei der Fehlersuche hilfreich, wenn Sie wissen, dass die Probleme auf einer Ebene unterhalb einer bestimmten Eingabemethode auftreten. (ID-13436)

Um diese Funktion zu aktivieren, legen Sie wie im folgenden Beispiel veranschaulicht die Verfolgungsebene für einen Bereich mit dem Modifizierer `subcalls` fest.

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

In diesem Beispiel werden die Methode `reconcileAccount()` auf der Ebene 4 und alle untergeordneten Aufrufe auf der Ebene 2 verfolgt.

- WSUser wurden die folgenden Methoden hinzugefügt. Weitere Informationen zu dieser Klasse finden Sie in der JavaDoc des REF-Kits. (ID-15468 / 14152)

### WSUser-Objektmethoden

Methode	Beschreibung
<code>getWorkItemDelegates()</code>	Gibt für den angegebenen Benutzer die aktuellen Delegate-Objekte zurück
<code>getWorkItemDelegate(String workItemType)</code>	Gibt ein Delegate-Objekt des angeforderten <code>workItem</code> -Typs von <code>_delegates</code> zurück
<code>addWorkItemDelegate(Delegate delegate)</code>	Fügt <code>_workItemDelegates</code> ein Delegate-Objekt des angegebenen Arbeitslistentyps hinzu. Wenn einer der angegebenen <code>workItem</code> -Typen bereits existiert, wird dieser ersetzt.
<code>removeWorkItemDelegate(String workItemType)</code>	Entfernt das angegebene <code>workItemType</code> -Element von den Delegate-Objekten des Arbeitselements.

## WSUser-Objektmethoden

<b>Methode</b>	<b>Beschreibung</b>
<code>setWorkItemDelegates (Map workItemDelegates)</code>	Legt für diesen Benutzer die Delegate-Objekte des Arbeitselements fest
<code>getWorkItemDelegateHistory()</code>	Gibt für den angegebenen Benutzer die Liste der historischen Delegate-Objekte zurück
<code>setWorkItemDelegateHistory (Liste workItemDelegateHistory)</code>	Legt für den angegebenen Benutzer die Liste der historischen Delegate-Objekte fest

## Arbeitselemente

- Bei der Weiterleitung eines Bescheinigungs-WorkItem sind alle Kommentare des weiterleitenden Bescheinigers in das WorkItem eingeschlossen, so dass die Kommentare anderer Bescheiniger enthalten sind, wenn das WorkItem schließlich bescheinigt wird. (ID-14643)

---

# In dieser Version behobene Fehler

In diesem Abschnitt sind die Fehler beschrieben, die in Identity Manager 7.1 behoben wurden. Die Informationen sind wie folgt unterteilt:

- [Administrator- und Benutzeroberflächen](#)
- [Überwachung](#)
- [Integrierte Entwicklungsumgebung \(IDE\)](#)
- [MetaView](#)
- [Passwortsynchronisation](#)
- [Abstimmung](#)
- [Berichte](#)
- [Repository](#)
- [Ressourcen](#)
- [Sicherheit](#)
- [Server](#)
- [Arbeitsablauf](#)
- [Weitere behobene Probleme](#)

## Administrator- und Benutzeroberflächen

- Auf den Debug-Seiten erscheinen Objektgruppen nicht mehr in der Dropdown-Liste der Elementtypen, die in einem Massenvorgang gelöscht werden können. (ID-13324)
- Sie können nun die Sperre für ein Organisationsobjekt aufheben, das gesperrt wurde, nachdem ein Benutzer mit unzureichenden Rechten versucht hat, dieses Objekt zu löschen. (ID-14942)
- Benutzerdefinierten Endbenutzeraufgaben, die die Ansicht des angemeldeten Benutzers überprüfen sollen, wird kein Fehler mehr zurückgegeben, wenn das Konto infolge einer Sperrung nicht verfügbar ist. (ID-15040)
- Wenn Sie über die Seite „Rollen finden“ Rollen suchen, die in vielen Organisationen vorkommen, wird jetzt kein Objektgruppenfehler mehr angezeigt. (ID-15303)

- Über Registerkarte „Rollen“ > Rollen finden > Menü „Genehmiger“ können jetzt Benutzer mit der Fähigkeit „Genehmigungsbeauftragter für Regeln“ angezeigt werden. (ID-15373)
- Wenn Sie ein `customEdit.jsp`-Formular für eigene benutzerdefinierte Formulare verwenden, wird keine Seite mehr angezeigt, die keine Navigationsleiste und zwei Exemplare des eigenen benutzerdefinierten Formulars enthält. (ID-15460)
- 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 abbrechen, die für den verarbeiteten Benutzer erkannt wurden, ist die Benutzeransicht nach der Verarbeitung nicht mehr gesperrt. (ID-15912)
- Die Bearbeitung eines Benutzers in der Organisation auf der höchsten Ebene („Top“), die das Resultat einer benutzerdefinierten Listensuche ist, funktioniert nun fehlerfrei. (ID-15977)
- Die Standardregeln für Zugriffsabfragen gehören standardmäßig alle zur Organisation auf der höchsten Ebene („Top“). Wenn Sie in Ihrer Bereitstellung Administratoren ermöglichen möchten, Zugriffsabfragen oder Überwachungsrichtlinien zu bearbeiten, ohne die Organisation auf der obersten Ebene zu kontrollieren, müssen Sie den anderen Organisationen die folgenden Regeln hinzufügen: (ID-15996)
  - Review Everyone
  - Review Changed Users
  - Reject Changed Users
  - Default Remediator
  - Default Attestor
  - Default Escalation
  - AttestorAll
  - Non-Administrators
  - All Administrators
  - Users Without a Manager

# Überwachung

- Mit einer neuen Richtlinie, der IDM Role Comparison-Überwachungsrichtlinie, kann jetzt geprüft werden, ob die Ressourcenattribute des Benutzers den Rollenattributen entsprechen, die in den jeweils zugewiesenen Rollen definiert sind. Wenn mit dieser Richtlinie ein Benutzer überprüft wird, bei dem dies nicht der Fall ist, wird eine Konformitätsverletzung gemeldet. (ID-11225)
- Wenn Sie einen Bericht über Zugriffsprüfungsdetails bearbeiten, in dem das angegebene Ziel der Zugriffsprüfung gelöscht wurde, wird kein Fehler mehr angezeigt. (ID-14805)
- In einer neuen Identity Manager 7.1-Installation wird im Auditor-Bericht über alle Einwilligungsverstöße nun das Attribut `resourceNames` verwendet, damit Konformitätsverletzungen für mehr als eine Ressource erfasst werden können. Zuvor kam in diesem Bericht das Attribut `resourceName` zum Einsatz, wodurch eine Warnmeldung ausgegeben wurde. (ID-15915)

**Aufrüstung:** Dieses Problem wurde ausschließlich für neue Identity Manager 7.1-Installationen behoben. Bei einer Aufrüstung von Identity Manager muss dieses Problem manuell behoben werden, indem in der standardmäßigen Berichtsaufgabe (und in allen anderen Berichten, die für die Verletzungszusammenfassung definiert wurden) `resourceNames` anstelle von `resourceName` angegeben wird.

- Im Überwachungsrichtlinienassistenten können Sie 3 Korrekturfunktionen und einen dazwischen liegenden Eskalationszeitraum festlegen. Bei Angabe des Zeitraums muss auch die Korrekturfunktion angegeben werden, ansonsten wird die Korrektur gelöscht. (ID-14198)
- Es ist jetzt möglich, eine Überprüfungsrichtlinienabfrage oder Zugriffsprüfung durchzuführen, wenn der Benutzergültigkeitsbereich auf eine dynamische Organisation eingestellt ist. (ID-14886)
- Die Details von Rollenänderungen werden in Überwachungsprotokollen festgehalten. (ID-15587)
- Mit den Konformitätsfunktionen in Identity Manager stehen Ihnen Aufgaben, Richtlinien und Regeln zur Verfügung, die Sie unverändert verwenden können. (ID-16127) Anfangs werden diese Objekte von Identity Manager in der Objektgruppe „Top“ oder „All“ erstellt, je nachdem, was angemessen ist. In Bereitstellungen mit delegierter Verwaltung, bei denen die Administratoren keine Kontrolle über die Objektgruppe „Top“ haben, kann es erforderlich sein, einige oder alle Auditor-Objekte zu anderen Objektgruppen hinzuzufügen. Identity Manager enthält ein Skript, mit dem sich Objekte auflisten und Objektgruppen zu den Auditor-Objekten hinzuzufügen bzw. daraus löschen lassen. Eine vollständige Liste der Auditor-Objekte finden Sie in `$WSHOME/sample/scripts/AuditorObjects.txt`.

- So listen Sie Objekte auf:

```
cd $WSHOME/sample/scripts  
beanshell.sh objectGroupUpdate.bsh -action list -data AuditorObjects.txt
```

- So fügen Sie die Objektgruppe 'All' zu allen Objekten hinzu:

```
cd $WSHOME/sample/scripts  
beanshell.sh objectGroupUpdate.bsh -action add -data AuditorObjects.txt  
-groups
```

- So löschen Sie die Objektgruppe 'All' aus allen Objekten:

```
cd $WSHOME/sample/scripts beanshell.sh objectGroupUpdate.bsh -action remove  
-data AuditorObjects.txt -groups All
```

- Die Überwachungskomponente von Identity Manager enthält Workflows, die Sie sofort und wahrscheinlich langfristig verwenden können. (ID-16173) Für die Aufrüstung von 7.0 auf 7.1 müssen Sie alle angehaltenen TaskInstances dieser Workflows umbenennen.

In Identity Manager steht ein Skript zur Verfügung, mit dem Sie die Umbenennung vor der Aufrüstung auf 7.1 automatisch vornehmen können. Diese Skripte befinden sich im Verzeichnis `util_scripts` des Installationabbildes. Zum Ausführen der Skripte müssen Sie in das Verzeichnis mit den Skripten wechseln und der Identity Manager-Server muss ausgeführt werden. Geben Sie die Option `-h IDM-URL` an, auch wenn das Skript lokal auf dem Identity Manager-Server ausgeführt wird. `IDM-URL` muss das erwartete Format aufweisen. Wenn der Identity Manager-Server an den Standard-URL-Pfad gebunden ist, können Sie diese Angabe auslassen. Das Skript ändert das Identity Manager-Repository. Es muss also nur auf einem Identity Manager-Server ausgeführt werden.

- So listen Sie die Aufgaben auf, die umbenannt werden müssen

```
./beanshell.sh taskUpdate.bsh -u Configurator -p configurator -h IDM-URL  
-action list
```

- So führen Sie die Umbenennung durch

```
./beanshell.sh taskUpdate.bsh -u Configurator -p configurator -h IDM-URL  
-action rename
```

Die umbenannten TaskDefinition-Objekte weisen das Format `alter-Name-7.1-update[N]` auf.

- Beim Beenden oder Löschen einer Zugriffsprüfung können bei den entsprechenden Aufgaben Fehler auftreten, so dass die Aufgaben nicht ordnungsgemäß abgeschlossen werden. In diesem Fall erhält die Zugriffsprüfung den Status `TERMINATE ERROR` oder `DELETE ERROR`. Nähere Fehlerinformationen finden Sie in den Aufgabenergebnissen unter „System Tasks“ -> „Aufgaben verwalten“. (ID-16211)

## Integrierte Entwicklungsumgebung (IDE)

- Für die meisten Knoten sind die zugeordneten Eigenschaften in Eigenschaftsfenstern aufgeführt und die meisten dieser Knoten haben eine Eigenschaft Name für die Verwaltung von Namenswerten. Wenn Sie ein bestimmtes Objekt über den zugehörigen Knoten umbenennen, indem Sie entweder mit der rechten Maustaste darauf klicken und Umbenennen wählen oder auf den Knoten klicken und den Text in das Beschriftungsfeld eingeben, wird die Beschriftung des Knotens aktualisiert und der XML-Code geändert. Die Eigenschaftsfenster wird jedoch nicht aktualisiert. Um den neuen Namen zu implementieren, gehen Sie wie folgt vor: Klicken Sie auf einen anderen Knoten und klicken Sie erneut auf den umbenannten Knoten. Das Eigenschaftsfenster wird dann aktualisiert. Sie können auch auf den Titel des Eigenschaftsfensters klicken, um eine Aktualisierung auf den richtigen Wert zu erreichen. (ID-13696)
- Regelbibliotheken werden zur Zeit nur für die allgemeine XML-Bearbeitung und -Prüfung im Regeltester unterstützt. Navigations- und Eigenschaftsunterstützung ist derzeit nicht implementiert. (ID-14093)
- Für ganzzahlige und Boolesche Werte können die Werte von Formulareigenschaften nicht im Eigenschaften-Editor festgelegt werden. (ID-14128)

**Zwischenlösung:** Bearbeiten Sie den Wert der Eigenschaft direkt in XML.

- Das Herunterladen, Hochladen oder erneute Laden eines Objekts führt dazu, dass das Objekt im Repository gesperrt wird. Versuche eines anderen Benutzers, der die Projekteinstellungen nicht festgelegt hat, innerhalb der Sperrdauer auf das Objekt zuzugreifen, schlagen dann folglich fehl. (ID-14132)
- Umbenennungen eines Objekts über das Kontextmenü von NetBeans müssen gespeichert werden. Nach der Durchführung einer Änderung kann diese über Datei ->Speichern gespeichert werden, ohne dafür die Datei öffnen zu müssen. Ist die Datei bereits geöffnet, wählen Sie Datei ->Speichern oder schließen die Datei und wählen bei Aufforderung aus, dass die Änderungen gespeichert werden sollen. (ID-14420)
- Bei der Einstellung der displayClass eines Feldes auf InlineAlert wird die Werteigenschaft von InlineAlert nicht angezeigt, wenn das Feld einen Namen hat. (ID-14456)
- Durch das Auschecken einer Benutzeransicht in Identity Manager IDE wird das Objekt gesperrt. Die Sperre kann durch Einchecken oder Schließen der Ansicht nicht aufgehoben werden. Die Sperre wird nach 5 Minuten automatisch aufgehoben. Sie können die Sperre auch dadurch aufheben, dass Sie sich bei Identity Manager als derjenige Administrator anmelden, der die Ansicht in IDM IDE ausgecheckt hat, und den Benutzer anzeigen. (ID-14797)
- Sie können jetzt einen Root-Kontext angeben, indem Sie beim Erstellen des Projekts das Feld **Context** leer lassen. (ID-15925)

## Identity Manager SPE

- Sie können nun vor der Verarbeitung aller Aktualisierungen die SPE-Synchronisation beenden. (ID-15077)
- Sie können SPE nun für Endbenutzerverzeichnisse mit aktiviertem SSL konfigurieren. (ID-15773)
- Auf der Konfigurationsseite von Identity Manager SPE können nur noch Richtlinien für SPE-Konten festgelegt werden. (ID-14833)

## MetaView

- Das Attribut `idmManager` wird nun beim Arbeiten mit MetaView richtig gespeichert. (ID-14445)

## Passwortsynchronisation

- Die Anwendung zum Konfigurieren der Passwortsynchronisation (`Configure.exe`) kürzt JMS-Eigenschaften beim Lesen vom Repository nicht mehr am Gleichheitszeichen (=). (ID-12658)
- 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)
- Die Option `checkDynamicallyAssignedAdminRolesAtLoginTo` verursacht beim Aktualisieren des Abstimmungsplans keine Fehler mehr im Abstimmungsrichtlinien-Editor. (ID-15338)

## Berichte

- Bei der Erstellung, Änderung und Löschung von Admin-Rollen wird nun Überwachungsprotokollierung unterstützt. (ID-12514)
- Die Ressourcenkonto-ID wird für alle Konten der Ressource in einer durch Semikolon getrennten Liste in Benutzerberichten angezeigt. Konten und Ressourcen, die indirekt durch eine Rolle oder Ressourcengruppe zugewiesen wurden, werden ebenfalls aufgeführt. Gibt es nur ein Ressourcenkonto, wird die Konto-ID nur dann angezeigt, wenn sie sich von der Identity Manager-Konto-ID unterscheidet. (ID-12820)
- Änderungen der Authentifizierungsfragen eines Benutzers werden nun in den Überwachungsprotokollen erfasst. (ID-13082)
- Das **Protokoll der Konformitätsverletzungen durch Benutzer** sollte im Menü Berichte unter dem Selektor Audio-Berichte nicht angezeigt werden. Dies die Aufgabe **Default Compliance Audit Report** und sie sollte nicht sichtbar sein. (ID-14721)
- Wenn Sie das Formular Conflict Violation Details Form in einer früheren Version benutzerspezifisch angepasst haben, sollten Sie es vor der Aufrüstung auf 7.0 exportieren. Sie können es dann nach der Aufrüstung wieder importieren. (ID-14772)
- 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)

## Repository

- Die Option `ObjectSource.OP_ALLOW_NOT_FOUND` (`allowNotFound`) wird nun in Aufrufen von `getView` und `checkoutView` für eine `IDMXUserView` und in Aufrufen von `getObject` über ein `LighthouseContext` in Identity Manager richtig beachtet. (ID-11900)
- Eine aktive Datenbankverbindung wird vom Identity Manager-Repository nun geschlossen (d.h. zurückgesetzt), sobald das Repository einen Java-Fehler (also eine Instanz von `java.lang.Error`) erkennt. Zuvor wurde eine aktive Datenverbindung immer dann geschlossen, wenn das Repository eine deklarierte Ausnahme oder eine Laufzeitausnahme (nicht aber einen Fehler) erkannte. Mit dieser Änderung wird verhindert, dass eine geöffnete (nicht zugesagte) Transaktion zurückbleibt, wenn die virtuelle Java-Maschine einen Fehler erzeugt (z. B. `OutOfMemoryError`). (ID-14411)

- Mit der Option `-n` des Befehls `setRepo` wird jetzt verhindert, dass der aktuelle Repositoryspeicherort überprüft wird. Mit der Option `-n` kann der Befehl `setRepo` auch dann erfolgreich ausgeführt werden, wenn der aktuelle Repositoryspeicherort ungültig ist bzw. die Datenbankinstanz am aktuellen Speicherort nicht verfügbar ist. Damit wird eine Rückentwicklung behoben, die seit Identity Manager 2005Q4M3 (Identity Manager 6.0) bestand. (ID-14809)
- Das Identity Manager-Repository wird nun schneller initialisiert, da `RelationalDataStore` nun eine SQL-Anweisung ausgibt, die gegenüber größeren Datenbanktabellen schneller ausgeführt wird. (ID-14937)
- 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 Benutzer werden die Repository-Einträge anderer Benutzer nicht mehr beeinträchtigt und es verhindert auch nicht mehr, diese Benutzer beim Suchen nach einer Rolle zu lokalisieren. (ID-15584)

## Ressourcen

- Für den LDAP-Ressourcenadapter wurde das Ressourcenparameterfeld **Failover-Server** hinzugefügt. In diesem Feld können mehrere Server für das Failover aufgelistet werden, für den Fall, dass der eigentliche Failover-Server ausfällt. Der LDAP-Ressourcenadapter erhält die Verbindung zum LDAP-Verzeichnis mithilfe von JNDI aufrecht. JNDI probiert bei der Verbindungsherstellung automatisch einen Server nach dem anderen aus, bis eine Verbindung gefunden wird. Sobald dies der Fall ist, verwendet JNDI den entsprechenden Server, bis dieser ausfällt, woraufhin der oben beschriebene Vorgang erneut abläuft. Für die Replikation über alle Failover-Server hinweg ist der Kunde zuständig. (ID-10889)
- 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:

```
<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.

---

- Der NDS-Ressourcenadapter ermöglicht es nun, in der NDS-Vorlage enthaltene Gruppen mit solchen Gruppen zusammenzuführen, die in der NDS-Vorlage nicht definiert sind. Diese Aktion wird von der Benutzeroberfläche aus durch benutzerdefinierte Formularänderungen durchgeführt. Weitere Informationen hierzu finden Sie in `NDSUserForm.xml`. (ID-12083)
- Linux-Adapter geben jetzt zur letzten Anmeldung eine Jahresangabe zurück. (ID-12182)
- Wenn Sie eine Ansicht eines anderen Oracle-Benutzers verwenden wollen, müssen Sie einen Alias definieren, so dass auf die Ansicht verwiesen werden kann, ohne sie mit einem Benutzernamen zu qualifizieren. In Identity Manager wurde dies bislang nicht erkannt und Sie konnten eine solche Ansicht im Ressourcenadapter angeben. Jetzt wird dieser Fehler in Identity Manager erkannt und eine entsprechende Meldung wird ausgegeben. (ID-12643)
- Beim Anzeigen von Benutzern auf einer Solaris NIS-Ressource wird die Einstellung für die primäre Gruppe jetzt als Gruppenname angezeigt. (ID-12667)
- Beim Arbeiten im CUA-Modus auf der SAP-Ressource können Sie nun Passwörter auf Nicht abgelaufen einstellen. (ID-13355)
- Der VMS-Ressourcenadapter bietet jetzt Abstimmungsfunktionen. (ID-13425)
- Die Bereitstellung kann nun erkennen, wenn beim Erstellen oder Aktualisieren von Benutzern ein Fehler vom `ResourceAction`-Skript erfasst wird. (ID-13465)
- Identity Manager bietet nun den Parameter zum Konfigurieren von Ressourcen `enableEmptyString`. Sie können diesen Parameter verwenden, um (anstelle eines `NULL`-Wertes) eine leere Zeichenkette in zeichenbasierte Spalten zu schreiben, die im Tabellenschema als nicht null definiert sind. Der Parameter `enableEmptyString` wirkt sich nicht darauf aus, wie Zeichenketten für Oracle-basierte Tabellen geschrieben werden. (ID-13737)

Der Standardwert für diesen Parameter ist `OFF` oder `FALSE` (aktuelles Verhalten). Um eine leere Zeichenkette zu schreiben, ändern Sie den Parameter auf `ON` oder `TRUE`.

- Durch die Aktualisierung der Zuständigkeit eines Oracle ERP-Kontos mit Hilfe eines Oracle ERP-Ressourcenadapters werden die anderen Zuständigkeiten des Kontos nicht mehr aktualisiert. (ID-13889)

Der Oracle ERP-Prüfungs-Zeitstempel wird nur für die geänderte Zuständigkeit aktualisiert. Die Oracle ERP-Prüfungs-Zeitstempel für alle anderen Kontozuständigkeiten bleiben unverändert.

- Active Sync des NDS-Adapters ruft keine Änderungen mehr ab, die auf `lastModifiedTimeStamp` des Benutzerobjekts basieren. Zuvor wurde dieses Attribut bei jeder An- und Abmeldung eines Benutzers aktualisiert. Der zuletzt geänderte Wert wird nun auf der Grundlage von `lastModifiedTimeStamp` der Attribute eines Benutzers berechnet, die im Identity Manager-Schema definiert sind. Wenn `lastModifiedTimeStamp` eines Attributs den oberen Grenzwert des Adapters überschreitet, wird dieser Benutzer vom Gateway als geändert zum Server zurückgesendet. (ID-13896)
- Der Shell-Skript-Adapter bietet jetzt Funktionen zum Umbenennen, Deaktivieren und Aktivieren. (ID-14472)
- Active Directory Active Sync hängt sich jetzt nicht mehr auf, wenn Verbindungen zum Gateway nicht geschlossen werden. In der Vergangenheit wuchs die Anzahl der Verbindungen auf den Höchstwert an und offene Verbindung verblieben im Status `CLOSED_WAIT`. Sobald die Höchstanzahl der Verbindungen erreicht ist und alle Verbindungen sich im Status `CLOSED_WAIT` befinden, wird Active Sync pausiert, bis diese Verbindungen bereinigt werden. (ID-14597)
- Die Attributzuordnung, die der Adapter zum Aktualisierungsskript des Kunden sendet, enthält nun einen Eintrag für das genullte Attribut und der Wert des Zuordnungseintrags beträgt null. Diese Bedingung (ein leerer Wert in der Attributzuordnung) bedeutet ausdrücklich, dass ein Attribut gelöscht wird. (ID-14655)
- 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)
- 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)
- Der LDAP-Ressourcenadapter verwendet zum Auflisten und Suchen von Benutzerkonten wieder das VLV-Steuerelement, sofern dieses vom LDAP-Server unterstützt wird und der Server richtig konfiguriert ist. (ID-14526)
- Das Oracle ERP-Benutzerformular verfügt nun über das Feld Person Name. Dieses schreibgeschützte Feld zeigt den vollen Namen der Oracle HR-Person an, wenn ein Oracle ERP-Konto anhand der Mitarbeiternummer mit dem Oracle HR-System verknüpft ist. (ID-14675)
- Der SAP-Adapter gibt nun den Status Deaktiviert richtig an. (ID-14834)
- Die Aktivierungsverknüpfung `nsaccountlock` kann bei der Bestimmung, ob ein LDAP-Benutzer deaktiviert ist, nun auf der Basis der Anwesenheit/ Abwesenheit eines Wertes Logik einsetzen. (ID-14925)

- Identity Manager beachtet nun für eine Ressource die Kombinationseinstellung *deny, ignore* von unterstützten Funktionen. Bei der 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)
- Der Oracle ERP-Ressourcenadapter verhindert nun die Aufhebung von Verknüpfungen zwischen Ressourcenkonten, wenn die Oracle ERP-Ressource während der vollständigen Abstimmung nicht verfügbar ist. (ID-14960)
- 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)
- 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)
- 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)
- Verbindungen werden beim Abfragen von Ressourcenobjekten nun vom ADSIResourceAdapter geschlossen. (ID-15098)
- ACF2-Verbindungseigenschaften (wie Breite und Höhe des virtuellen Bildschirms) können jetzt angegeben werden. (ID-15158) Zum Implementieren dieser Funktion müssen Sie ein eigenes `update.xml`-Skript mit folgenden Angaben importieren:

```
<?xml version='1.0' encoding='UTF-8'?>
<!DOCTYPE Waveset PUBLIC 'waveset.dtd' 'waveset.dtd'>
<Waveset>
  <ImportCommand class='com.waveset.session.ResourceUpdater' >
    <Map>
      <MapEntry key='updateAttributes' value='true' />
    </Map>
  </ImportCommand>
</Waveset>
```

Nachdem die Aktualisierung ausgeführt wurde, muss der Anwendungsserver gestoppt und neu gestartet werden.

Um die Bildschirmgröße auf einen Modell-5-Terminaltyp zu erhöhen, müssen Sie die folgenden Eigenschaften hinzufügen:

```
Enable TN3270E: 1  
Session Properties: SESSION_PS_SIZE <newline> 5
```

<newline> bedeutet dabei, dass SESSION\_PS\_SIZE und 5 auf zwei Zeilen erscheinen müssen.

- Es gibt ein neues Ressourcenattribut für das Oracle ERP-Schema: `person_fullname`. Das Beispielskript `$WSHOME/sample/other/CreateLHERPAdminUser.oracle` wurde aktualisiert. Es enthält nun eine ICX\*-Tabelle und Ansichten für Synonyme, die für Nicht-APPS-Benutzer erstellt werden. (ID-15188)
- Bei den JDBC-Beispielskripten wurden ResultSets und Statements nicht geschlossen, wenn sie nicht länger benötigt wurden. In großen Anwendungen konnte es dabei zu gewissen Ressourcenverlusten kommen. Die Beispielskripte wurden so modifiziert, dass solche Objekte jetzt geschlossen werden, sobald sie nicht mehr benötigt werden. (ID-15254)
- Die Ausgabe von Lösch-Skripten, die mit einem Fehler zurückgegeben werden, werden in Identity Manager jetzt abgefangen und gemeldet. (ID-15340)
- Ein Speicherzuordnungsproblem bei der Zeichenübersetzung wurde gelöst. (ID-15341)

Am Gateway ist einheitlich UTF-8 zu verwenden und das Windows-Gateway ist mit einer standardmäßigen ANSI-Codeseite zu konfigurieren, die mit Ihren Anwendungsdaten kompatibel ist. Sie sollten also eine Windows-Zeichenkodierung verwenden, mit der alle Unicode-Zeichen dargestellt werden können, die in den mit Identity Manager verwalteten Daten vorkommen.

- Die temporären Dateinamen, die beim Ausführen von Shell-Skripten für Ressourcenaktionen verwendet werden, wurden mit dem Ziel geändert, mehr Eindeutigkeit zu erzielen. (ID-15348)
- 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)
- Für Solaris NIS wird nun anstelle von `defgroup defgname` in der Datei `/usr/sadm/defadduser` dafür verwendet, die primäre Standardgruppe als eine optionale Standardwertquelle für neu erstellte Konten festzulegen. (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)
- Active Sync wird nicht mehr weiter ausgeführt, wenn „Konten ohne Übereinstimmung erstellen“ auf „true“ eingestellt ist und die zulässige Fehleranzahl überschritten wird. (ID-15662)
- Der Adapter der PeopleSoft-Komponentenschnittstelle kann nun den Status Deaktiviert angeben. (ID-15674)
- Identity Manager liest keine Kontoattribute mehr, die ausschließlich für den Schreibzugriff vorgesehen sind, von einem LDAP-Verzeichnis oder Active Directory (ID-15838)
- Mit dem Skriptgateway-Ressourcenadapter können jetzt Rückgabecodes aus Skripten, die einen anderen Wert als Null aufweisen, richtig erfasst werden, so dass ein Fehler gemeldet wird. (ID-15860)
- 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)
- Das Ressourcenattribut der NDS-Vorlage zeigt anstelle des Meldungsschlüssels `NDS_TEMPLATE_HELP` nun die Popup-Hilfe (i-Help) an. (ID-15986)
- Die Ressourcenaktionen „Enable“ und „Disable“ werden jetzt für den Skriptgateway-Ressourcenadapter unterstützt. (ID-16066)
- Der Skriptgateway-Ressourcenadapter übergibt jetzt Ressourcenattribute an die Skripte, mit denen die `getInfo`- und `listAllObjects`-Aktionen implementiert sind. (ID-16149)
- Der GroupWise-Ressourcenadapter wurde verworfen. Verwenden Sie zum Verwalten von GroupWise-Benutzern stattdessen den NDS-Adapter. (ID-16308)

## Scheduler

- Die Ausgabe des Syslog-Eintrags, 'EVNT00', LockedByAnother-Fehler, wurde unterdrückt. Dies führte in Cluster-Umgebungen zu übermäßiger Ausgabe in das Syslog. (ID-15714)

## Sicherheit

- Änderungen von Endbenutzerpasswörtern, die von Administratoren (über SPML oder anderweitig) vorgenommen werden, werden nun zur Passworthistorie hinzugefügt, sofern diese aktiviert ist. Dadurch wurden sowohl eine Systemkonfigurations- als auch eine Anzeigeoption (für Formulare) hinzugefügt, die es dem Administrator ermöglichen, das gewünschte Verhalten auszuwählen. (ID-13029)
  - Administratoren können je nach Anmeldeanwendung die Option Systemkonfiguration ein- oder ausschalten, was mehr Flexibilität bietet, denn Administratoren möchten u. U. kein Verhalten, das sich auf alle Anwendungen erstreckt.
  - Einstellungen der Systemkonfiguration werden durch die Anzeigeoption stets außer Kraft gesetzt.
- Ein delegierter Administrator, der ausschließlich über Berechtigungen zum Berichtsadministrator verfügt, ist nicht mehr in der Lage, Organisationen (für die ein Bericht erstellt wird) von einem Bericht zu entfernen, die außerhalb des Geltungsbereichs liegen. (ID-14765)
- Ein Überwachungsprotokoll für eine Organisation enthält nun die Organisationsgenehmiger, die von der Organisation gelöscht oder dieser hinzugefügt wurden. (ID-15232)
- Ein Admin-Rollen-Administrator verfügt nun über die erforderlichen Rechte zum Erstellen einer Admin-Rolle. Der Ersteller muss bei der Erstellung einer neuen Admin-Rolle oder -Fähigkeit u. U. einen oder mehrere Benutzer auswählen, die die Admin-Rolle oder -Fähigkeit anderen Benutzern zuweisen können. Dieser Fall tritt ein, wenn ein Ersteller nicht dazu autorisiert ist, Admin-Rollen oder -Fähigkeiten zuzuweisen. Die Gruppe der Benutzer, von der der Ersteller einen zuweisenden Benutzer auswählen kann, unterliegt nicht dem Geltungsbereich der Identity Manager-Autorisierung, da der Ersteller möglicherweise einen oder mehrere Benutzer auswählen muss, die außerhalb ihres Kontrollgeltungsbereichs liegen. Der Gruppe der verfügbaren Benutzer wurde nun das Recht Benutzerfunktion zuweisen erteilt. (ID-15980)

## Server

- Der SPML-Server gibt nun Fehler zurück, wenn Anforderungen Filter mit Operatoren enthalten, die noch nicht implementiert sind. (ID-11343)
- Beim Entfernen von Attributen aus dem Konfigurationsobjekt „User Extended Attributes“ wurden diese nicht aus den WSUser-Attributen entfernt. Stattdessen blieben die alten Werte in der XML-Datei erhalten. Dieser Fehler wurde behoben und die Werte werden jetzt aus der XML-Datei entfernt. (ID-11721)
- Wenn Sie über den Eingabebereich der GUI Befehle oder Benutzer für Massenvorgänge angeben, schlägt der Vorgang nicht mehr mit Anzeige der Meldung „Es muss ein Objektname angegeben werden“ fehl. Dies gilt auch für den Fall, dass Sie tatsächlich einen Benutzernamen angegeben haben. (ID-15112)
- Die Probleme, die beim intensiven Zugriff auf eine Ressource OutOfMemory-Fehler verursachten, (wie z. B. bei der Abstimmung) wurden behoben. (ID-16222)
- Für die Rückgabe einer workItem-spezifischen Delegiertenliste stehen in Identity Manager jetzt die folgenden neuen öffentlichen Methoden zur Verfügung. Verwenden Sie diese Methoden mit dem Argument *workItemType*. (ID-15787 / 14152)

```
DelegateUtil#checkWorkItemDelegates()
```

```
DelegateUtil#getWorkItemDelegates()
```

## Aufgaben

Wenn Sie eine geplante Aufgabe bearbeiten, muss das Startdatum im Format MM/DD/YYYY erneut angegeben werden (ID-5675).

## Arbeitsablauf

- Die Definition der Identity Manager-Beispielaufgabe Notify Reconcile Finish erstellt und versendet bei Abschluss nun E-Mail-Benachrichtigungen. (ID-9259)

## Weitere behobene Probleme

8691, 8961, 9913, 10100, 10802, 11538, 12509, 12571, 12585, 12872, 13223, 13251, 13258, 13701, 13741, 13965, 14282, 14334, 14459, 14564, 14663, 14748, 14893, 15036, 15098, 15234, 15345, 15424, 15746, 15798, 15851, 15864, 16041, 16087, 16121, 16171, 16177, 16215, 16288,

In dieser Version behobene Fehler

# Bekannte Probleme

In diesem Abschnitt der Identity Manager 7.1-Versionshinweise finden Sie bekannte Probleme und Zwischenlösungen für die folgenden Themen:

- [Identity Manager](#)
- [Service Provider Edition](#)

---

## Identity Manager

In diesem Abschnitt sind bekannte Probleme und Zwischenlösungen für Identity Manager beschrieben. Die Informationen sind wie folgt unterteilt:

- [Allgemein](#)
- [Installieren und Aktualisieren](#)
- [Kontoverwaltung](#)
- [Genehmigungen](#)
- [Überwachung](#)
- [Integrierte Entwicklungsumgebung \(IDE\)](#)
- [Anmeldekonfiguration](#)
- [Organisationen](#)
- [Richtlinien und Fähigkeiten](#)
- [Abstimmen und Importieren von Benutzern](#)
- [Berichte](#)
- [Ressourcen](#)
- [Ressourcenobjektverwaltung](#)
- [Ressourcengruppen](#)
- [Sicherheit](#)
- [Server](#)
- [Sun Identity Manager Gateway](#)
- [Aufgaben](#)
- [Workflow, Formulare, Regeln und XPRESS](#)

## Allgemein

- Erforderliche Felder, die in der Ressourcenschemazuordnung festgelegt wurden, werden nur beim Erstellen von Benutzerkonten geprüft (ID-220). Wenn ein Feld bei Benutzeraktualisierungen benötigt wird, muss das Benutzerformular entsprechend konfiguriert werden.
- Der Organisationsname, Administratortname, Kontoname, Name des Benutzerattributs (links in der Schemazuordnung) und die Aufgabennamen werden nicht auf ungültige Zeichen geprüft (ID-1145, 1206, 1679, 1734, 1767, 2413, 3331). In den Namen für diese Objekttypen sind folgende Zeichen nicht zulässig: (\$), Komma ( , ), Punkt ( . ), Apostroph ( ' ), Ampersand ( & ), linke eckige Klammer ( [ ), rechte eckige Klammer ( ] ) und Doppelpunkt ( : ).
- Wenn Sie versuchen, eine Aktion nach einem Sitzungstimeout auszuführen, wird eine irreführende Fehlermeldung auf der Kontoseite angezeigt (ID-1223).
- Das Kalenderobjekt wird nicht vollständig angezeigt, wenn der Browser große Schriftarten verwendet. (ID-2120)
- Das Kontrollkästchen Alle auswählen auf der Seite für die Suchergebnisse und die Listenaufgabe wird nicht deaktiviert, wenn eines der Listenelemente deaktiviert ist (ID-5090). Das Kontrollkästchen Alle auswählen wird während der sich ergebenden Aktion ignoriert, wenn nicht die Kontrollkästchen aller Listenelemente aktiviert sind.
- Um die Änderungen bei einem angepassten Meldungskatalog zu übernehmen, muss der Server neu gestartet werden. (ID-6792)
- Der derzeitige Mechanismus zum Ermitteln eines fehlgeschlagenen Servers geht davon aus, dass alle Systeme eines Identity Manager-Clusters in Bezug auf die Zeit synchronisiert sind (ID-7064). Wenn bei dem Standardausfallintervall von fünf Minuten ein Server fünf Minuten lang nicht mit einem anderen Server synchron ist, deklariert der Server, der zeitlich voraus ist, den zeitlich nachstehenden Server für inaktiv, was unvorhersehbare Ergebnisse zur Folge haben kann.

**Zwischenlösung:** Einrichtung einer besseren Zeitsynchronisation oder Erhöhung des Failoverintervalls.

- Wenn Sie sich unter Windows mit einem Benutzernamen mit Doppelbytezeichen anmelden und die Standardcodierung für den Computer nur Einzelbytezeichen unterstützt, müssen Sie die USER\_JPI\_PROFILE-Umgebungsvariable auf ein vorhandenes Verzeichnis setzen, dessen Name nur Einzelbytezeichen enthält. (ID-8540)
- Wenn ein erweiterter Knoten weniger als eine Datensatz enthält und Sie *vor* dem ersten Datensatz auf der Seite für diesen Knoten ein neues untergeordnetes Element erstellen (z. B. einen Benutzer in der Organisation), fügt Identity Manager bei der nächsten Aktualisierung vor der aktuellen Seite eine Seite mit einem Element ein. (ID-12151)

**Zwischenlösung:** Um die Seiten *erneut auszurichten*, klicken Sie auf die Schaltfläche Erste Seite.

- 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“ auf Seite 30.

- Sie müssen das JDK, auf dem Sie den Anwendungsserver ausführen, auf JDK 1.4.2\_13 aktualisieren, damit die im Jahr 2007 in Kraft tretende neue Sommerzeit (DST, Daylight Savings Time) unterstützt wird. (ID-15475)

So aktualisieren Sie:

- a. Aktualisieren Sie die Zeitfunktionen für das Gateway-Hosting von

<http://www.microsoft.com/windows/timezone/dst2007.msp>

(Identity Manager ruft vom Windows-Betriebssystem die Zeitfunktionen für das Gateway-Hosting ab.)

- b. Führen Sie auf dem Anwendungsserver eine Aufrüstung auf eine Java-konforme Version durch. Anweisungen zum Herunterfahren, Aufrüsten und Neustarten des Anwendungsservers finden Sie in *Identity Manager Installation*.
- c. Prüfen Sie die Liste der Aufgaben, die über die verlängerten Zeiträume der DST gestartet werden sollen (Weitere Informationen zu diesen Zeiträumen finden Sie im Folgenden).

Nach der Implementierung der DST-Patches müssen alle Elemente, deren Start innerhalb dieses Zeitraum festgelegt ist, neu geplant werden. Sich wiederholende Elemente, die mindestens einmal nach der Implementierung des DST-Patches und vor Beginn dieser Zeiträume ausgeführt werden, werden zeitgerecht abgearbeitet.

Zur Behebung von DST-Problemen verweisen wir Sie auf Java-Aufrüstungen oder das Tool *tzupdater* (<http://java.sun.com/developer/technicalArticles/Intl/USDST/>).  
Siehe auch Sun Alert for Java.

Die Sommerzeit (DST, Daylight Savings Time) fängt in den USA und Kanada früher an und endet später als in vorausgehenden Jahren. Die Verlängerungszeiträume erstrecken sich vom zweiten Sonntag im März bis zum ersten Sonntag im April und vom letzten Sonntag im Oktober bis zum ersten Sonntag im November. Im Jahr 2007 entspricht dies den Daten 11.03 bis 01.04 und 28.10 bis 04.11. Durch nicht konforme Software verursachte Probleme bleiben so lange bestehen, bis Konformität der Software hergestellt wurde.

---

**HINWEIS** Werden die oben beschriebenen Schritte nicht durchgeführt, dann dies folgende Konsequenzen haben:

- Einige geplante Aufgaben (z. B. Abstimmung und Active Sync) werden je nach den jeweiligen Planungsparametern mit einer Abweichung von einer Stunde ausgeführt.
  - Ereignisse, die im angegebenen Zeitraum von bis zu einer Stunde stattfinden, sind in den Berichten eingeschlossen oder ausgeschlossen.
  - Benutzerdefinierte Änderungen mit Zeitabhängigkeit führen u. U. zu fehlerhaften Ergebnissen.
- 

- Das Menü der Endbenutzeroberfläche, über das Genehmigungsarbeitselemente aus der Arbeitselementliste an einen anderen Genehmiger weitergeleitet werden können, wird nicht richtig gefüllt. (ID-15935)

**Zwischenlösung:** Fügen Sie hinter dem Feld `userIds` das folgende Feld in das Formular ein und ersetzen Sie die „`user*`“-Zeichenfolgen durch die gewünschte Liste der Konten-IDs:

```
<Field name='forwardingUsers'>
  <Derivation>
    <list>
      <s>user1</s>
      <s>user2</s>
    </list>
  </Derivation>
</Field>
```

- Wenn Sie Einstellungen in einem vorhandenen Änderungsprotokoll ändern, also z. B. weitere Spaltenattribute hinzufügen, erscheinen diese Änderungen in einer bereits vorhandenen CSV-Änderungsprotokolldatei möglicherweise nicht. (ID-15973)

- Auf den Registerkarten der TabPanel-Anzeigekomponenten angezeigte Zeichenfolgen werden umbrochen, wenn sie Leerzeichen enthalten. Diese Zeichenfolgen werden z. B. im Benutzerformular mit Registerkarten verwendet. Damit die Zeichenfolgen nicht mehr umbrochen werden, fügen Sie die folgenden beiden Zeilen in `$/SHOME/styles/customStyle.css` ein:

```
table.Tab2TblNew td
{background-image:url(../images/tabs/level2_deselect.jpg);background-repeat:repeat-x;back
ground-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);backgroun
d-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}
```

- Prozessdiagramm-Applets sind auch in einer lokalisierten Identity Manager-Sitzung u. U. nicht vollständig lokalisiert (d.h. sie enthalten eine Mischung aus Englisch und Deutsch). (ID-16139)
- Wenn beim Bearbeiten einer Rolle eine zweite Rolle als übergeordnete und als untergeordnete Rolle angegeben wird, entsteht ein Zirkelbezug, was zu einem `StackOverflowError` führen kann. (ID-16326)
- Für die Passwortsynchronisation im Direktmodus muss `SimpleRpcHandler` in der Datei `web.xml` konfiguriert sein. Standardmäßig steht diese Behandlungsroutine nicht als Behandlungsroutine für das `rpcrouter2`-Servlet zur Verfügung. (ID-16469) Wenn Sie die Passwortsynchronisation im Direktmodus verwenden wollen, stellen Sie die Initialisierungsparameter für die Behandlungsroutine folgendermaßen ein:

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

Beachten Sie, dass `SimpleRpcHandler` bestimmte `RemoteSession`-Aufrufe stört. Konfigurieren Sie ein eigenes Servlet für die Abarbeitung von `RemoteSession`-Aufrufen, wenn Sie `RemoteSession` und die Passwortsynchronisation im Direktmodus verwenden wollen.

# Installieren und Aktualisieren

---

**HINWEIS** Informationen zu Problemen, die nur in dieser Version auftreten, finden Sie in „Installations- und Aktualisierungshinweise“ auf Seite 77.

---

- Wenn Sie von einer 6.x-Installation aufrüsten, aber die neuen Endbenutzerseiten verwenden möchten, müssen Sie die Systemkonfiguration `ui.web.user.showMenu` auf **true** einstellen, damit die horizontale Navigationsleiste angezeigt wird. (ID-14900, 16401)

Außerdem müssen Sie die Endbenutzer-Formularzuordnung in der Systemkonfiguration folgendermaßen ändern:

```
<Attribute name='endUserMenu' value='End User Dashboard' />
```

- Infolge eines Compiler-Fehlers, der mehrere Seiten betrifft, wird WebLogic 9.0 nicht unterstützt.

**Zwischenlösung:** Verwenden Sie stattdessen WebLogic 9.1 oder 9.2. (ID-16002)

- Es gibt kein Datenbankaufrüstungsskript für den Service Provider-Transaktionsspeicher. Beim Aufrüsten von Identity Manager 5.6 (Service Provider Edition 1.0) oder Identity Manager 6.0 auf 7.0 oder 7.1 muss eine neue Spalte ('userId') zur vorhandenen Tabelle hinzugefügt werden. Die Beispieldatenbankskripte (`create_spe_tables.*`) in dieser Version zeigen den erwarteten Typ und die standardmäßige maximale Wertelänge für diese Spalte. (ID-16423)
- Beim Aufrüsten wird in seltenen Fällen der folgende Fehler angezeigt, wenn `update.xml` ausgeführt wird:

```
com.waveset.util.InternalError: Reserved item  
'ComplianceViolation:LastModified' name is already in use by existing item  
'ComplianceViolation:LastModified'.
```

Löschen Sie in diesem Fall das entsprechende Element mit der folgenden SQL-Anweisung aus dem Repository:

```
delete from object where type='ComplianceViolation' and name='LASTMODIFIED'
```

Danach können Sie die Aufrüstung an der Stelle fortsetzen, an der sie fehlgeschlagen ist, indem Sie `update.xml` erneut importieren. (ID-16437)

## Kontoverwaltung

- Es können jetzt NT-Konten erstellt werden, die mehr als 20 Zeichen lang sind und von den nativen NT-Tools nicht unterstützt werden. (ID-710)
- Ein Administrator kann nur Ressourcen oder Rollen speichern, deren Organisationen von ihm verwaltet werden. (ID-839)
- Beim Sortieren der Spalten auf der Seite für die Bereitstellungsergebnisse werden zusätzliche leere Zeilen zu den Ergebnissen hinzugefügt. (ID-1105)
- Genehmigungen für mehrere hundert Benutzerkonten dauern sehr lange. (ID-1149)

**Zwischenlösung:** Genehmigen Sie Datensätze von Benutzerkonten in kleineren Gruppen.

- Die Genehmigungsdatensätze eines Administrators, der nicht mehr über Genehmigungsberechtigung verfügt, können nicht genehmigt werden. (ID-1150)
- Zwischenlösung:** Entfernen Sie den Administrator aus den Ressourcen, Rollen und Organisationen, für die Genehmigungsrechte bestehen, und genehmigen Sie anschließend alle ausstehenden Genehmigungsdatensätze, bevor Sie den Administrator oder die Genehmigungsberechtigung für den Administrator entfernen.

- Wenn ein Benutzer ohne Änderungen aktualisiert wird, wird die detaillierte Ergebnisseite nicht angezeigt (ID-2327).
- Wenn Sie einen neuen Benutzer erstellen oder eine Ressource zu einem vorhandenen Benutzer hinzufügen, wobei der DN für den Benutzer falsch ist, wird der falsche Wert zwischengespeichert, bis sich der Administrator abmeldet (ID-2508). Wenn der DN korrigiert wurde, kann der Benutzer erst neu erstellt werden, nachdem sich der Administrator abgemeldet hat.
- In Windows Active Directory muss das Gateway als Administrator ausgeführt werden, der Verzeichnisse erstellen kann (ID-2919). Identity Manager kann Ausgangsverzeichnisse unter Windows 2000 erstellen. Der Kontoerstellungsvorgang für ein Ausgangsverzeichnis wird nicht vom in der Ressourcendefinition angegebenen Administrator, sondern vom Benutzer, unter dem der Gateway-Prozess läuft, ausgeführt.

**Zwischenlösung:** Geben Sie statt des Benutzers, unter dem das Gateway auf dem lokalen System läuft, ein Konto an, das über Berechtigungen zum Erstellen von entfernten Freigaben verfügt, und legen Sie die Berechtigungen für diese Freigaben fest. Dieses Konto muss außerdem die durchsuchende Überprüfung umgehen und als Betriebssystemberechtigung fungieren.

- Die Windows NT-Ressource erzeugt eine Warnmeldung anstelle einer Fehlermeldung, wenn beim Deaktivieren eines Benutzerkontos ein Fehler auftritt. (ID-3222)

- Es wird manchmal eine `java.lang.NullPointerException` angezeigt, wenn auf der Seite zum Bearbeiten von Benutzern alle Ressourcen aus einem Benutzer entfernt werden. (ID-4811)  
**Zwischenlösung:** Trennen oder löschen Sie diese Ressourcenkonten auf der Seite zum Löschen von Benutzern aus dem Benutzer.
- Wenn ein Identity Manager-Benutzer erstellt und einer Windows Active Directory-Ressource zugewiesen wird, in der das Benutzerkonto bereits vorhanden ist, wird der Benutzer ohne GUID-Attribut in den Ressourceninformationen erstellt (ID-5114). Diese GUID ermittelt Änderungen bei der Organisation oder dem Namen des Benutzers in Active Directory. Sie können dieses Problem beheben, indem Sie in der Ressource eine Abstimmung ausführen.
- Beim Erstellen eines Benutzers wird eine Warnung ausgegeben, falls Sie dem Benutzer eine Rolle hinzufügen, die eine direkt zugewiesene Ressource enthält. (ID-5385)
- Ein „Weiterleiten an“-Administrator kann nicht angegeben werden, wenn ein Benutzer erstellt wird. Diese Option kann nur festgelegt werden, wenn der Benutzer bearbeitet wird. (ID-5695)

## Genehmigungen

- Wenn Sie einen Benutzer im Hintergrund aktualisieren, wird auf der Seite für die Aufgabenergebnisse eine Genehmigungsaktivität angezeigt (ID-3301). Diese Genehmigung kann ignoriert werden.
- Die Genehmigungsdatensätze für einen Administrator werden erst angezeigt, nachdem der Benutzer umbenannt wurde. (ID-3386)  
**Zwischenlösung:** Bearbeiten Sie alle ausstehenden Genehmigungen, bevor Sie den Benutzer umbenennen.
- Zuvor genehmigte oder abgelehnte Genehmigungsdatensätze können von einem Administrator nicht angezeigt werden, wenn der zu genehmigende Benutzer einer Organisation angehört, die der Genehmiger nicht steuert. (ID-3494)
- Ressourcenwiederholungsaufgaben werden in der ausstehenden Genehmigungsliste für den Configurator angezeigt. (ID-3508)

# Überwachung

- Während einer Prüfung wird der erneute Abruf von Benutzerkonten, die von den Ressourcen nicht abgerufen werden konnten oder bei denen andere Ausfälle aufgetreten sind, nicht unterstützt. Diese Ausfälle werden nach der Prüfung gemeldet. Es gibt jedoch keine automatisierte Möglichkeit zur erneuten Prüfung der Konten. (ID-9112)
- Identity Auditor versucht, die Benutzer zwischen Richtlinienprüfungen konform zu halten, indem die Richtlinie immer dann durchgesetzt wird, wenn der Benutzer bearbeitet wird. Wenn Sie einen Benutzer bearbeiten, dem Überwachungsrichtlinien zugewiesen sind und der außerdem eine Richtlinie verletzt, können Sie die Änderungen beim Benutzer nicht speichern, und zwar auch dann nicht, wenn der Benutzer lediglich zu einer anderen Organisation verschoben werden soll. (ID-9504)

**Zwischenlösung:** Über das Kontextmenü (oder die Suchfunktion) im Benutzerapplet können Sie Benutzer verschieben oder die Prüfungen der Überwachungsrichtlinie vorübergehend deaktivieren.

Um die Prüfungen der Auditorrichtlinie zu deaktivieren, entfernen Sie die `userViewValidators`-Eigenschaft aus der Systemkonfiguration. Diese Eigenschaft hat den Wert einer Liste von Zeichenfolgen und wird während des Imports von `init.xml` oder `upgrade.xml` hinzugefügt.

- Im Verstoßverlauf für die AuditPolicy, Ressource und Organisation kann die Implementierung der logarithmischen Skalierung für den STACK-Diagrammtyp zu einer ungewöhnlichen Anzeige führen. (ID-9522)
- Der Administrator für Auditor-Zugriffsabfragenberichte ist derzeit nicht in der Lage, eine Überwachungsrichtliniensuche zu planen. Es wird eine Fehlermeldung angezeigt: `Error message: Create access denied to Subject auditadmin on type TaskSchedule`. Für die Planung von Aufgaben benötigen Administratoren Erstellungsrechte für `TaskSchedule` `authType`. (ID-14713)

**Zwischenlösung:** Bearbeiten Sie den Administrator und erteilen Sie ihm Erstellungsrechte für `TaskSchedule` oder geben Sie einen Benutzer an, der mindestens über die Fähigkeiten `Auditor Administrator` oder `Waveset Administrator` verfügt.

- Wenn Sie in älteren Versionen von Identity Auditor Berichte für Überwachungsrichtliniensuchen erstellt haben, sind diese Berichte nach einer Aufrüstung auf Identity Manager 7.0 nicht mehr sichtbar. Um diesen Mangel zu beheben, kann ein Administrator mit (mindestens) der Fähigkeit `Auditor-Bericht-Administrator` diese Berichte bearbeiten und die Sichtbarkeit auf `run` ändern. (ID-14881)

- Bei der Ausführung von Überprüfungsrichtlinienabfragen, die mehrere Verletzungen zurückgeben, erstellt Auditor u. U. einen Korrekturarbeitsablauf für die Verarbeitung der Verletzungen. Die MySQL-StandardEinstellung für `max_allowed_packet` (1M) ist für einen Arbeitsablauf mit Dutzenden von Verletzungen zu niedrig. Bei Erreichen dieses Grenzwerts wird der Korrekturarbeitsablauf von Auditor nicht gestartet.

**Zwischenlösung:** Bei einer hohen Auslastung von Auditor muss dieser Wert deutlich größer sein. Um dieses Problem zu beheben, fügen Sie der MySQL-Konfigurationsdatei (`my.cnf`) `max_allowed_packet = 32M` hinzu und starten den Anwendungsserver erneut. (ID-15830)

- Die Namen von Überwachungsrichtlinien dürfen die folgenden Zeichen NICHT enthalten: ' (Apostroph), . (Punkt), | (Linie), [ (Klammer links), ] (Klammer rechts), , (Komma), : (Doppelpunkt), \$ (Dollarzeichen), " (doppeltes Anführungszeichen), = (Gleichheitszeichen). (ID-16078)
- Beim Ändern der Schweregrads- und Prioritätswerte für die Korrektur von Konformitätsverletzungen kann es zu Missverständnissen kommen. Die Anfangswerte im Formular entsprechen *nicht* den aktuellen Werten der Konformitätsverletzungen. Es handelt sich vielmehr um die beim Vornehmen von Änderungen zuletzt eingestellten Werte. Sie müssen sich in der Listenansicht darüber im Klaren sein, welche Schweregrads- / Prioritätswerte Sie einstellen wollen, denn die aktuellen Werte lassen sich auf der Seite, auf der Sie die Werte ändern können, nicht ermitteln. (ID-16040)
- Bei Konformitätsverletzungen, die vor der Aufrüstung auf IdM 7.1 erstellt wurden, können der Schweregrad und die Priorität nicht eingestellt werden. Es wird eine Fehlermeldung zurückgegeben, dass die Konformitätsverletzung nicht mehr vorhanden ist, dies stimmt jedoch nicht. Die Konformitätsverletzung ist vorhanden, aber in IdM kann der Schweregrad und die Priorität nicht eingestellt werden. (ID-16420)

## Integrierte Entwicklungsumgebung (IDE)

- Die Umbenennung von Objekten im Identity Manager IDE sollte anstelle der Bearbeitung von XML im Editor mit Hilfe des Kontextmenüs (Klicken mit der rechten Maustaste) im Projektmenü durchgeführt werden. (ID-13828)
- Der XML-Navigator wurde im IDM IDE deaktiviert. Durch Windows ->Navigator wird das Navigatorfenster geöffnet und es wird `<No view available>` angezeigt. (ID-13390)
- Funktionen zum Löschen von Projekten sind nicht verfügbar. (ID-14013)
- Die Option Discard All funktioniert beim Schließen eines Projekts nicht einwandfrei. Wenn Sie die an einem Objekt vorgenommenen Änderungen verwerfen möchten, müssen Sie das Editorfenster schließen und Discard wählen. Dies ist ein bekanntes Problem, das im Zusammenhang mit NetBeans auftritt (Fehler 84236). (ID-14164)

- Beim Arbeiten mit dem Identity Manager IDE-Standardprojekt starten Sie die gebündelte Tomcat-Instanz; es wird das Dialogfeld Tomcat Manager angezeigt, das normalerweise eine der folgenden Bedingungen angibt: (ID-15546)
  - Es werden mehrere Tomcat-Instanzen ausgeführt.
  - Die Berechtigungsnachweise stimmen nicht überein.

Dies ist ein bekanntes Problem, das im Zusammenhang mit NetBeans auftritt.

**Zwischenlösung:** Stellen Sie sicher, dass nur eine Tomcat-Instanz auf dem Host-System ausgeführt wird und zum Überwachen des gleichen Anschlusses konfiguriert ist wie beim gebündelten Tomcat.

Die Berechtigungsnachweise, die als Teil des gebündelten Tomcat-Servers gespeichert werden, müssen mit denen übereinstimmen, die in den Server Manager-Feldern Benutzername und Passwort gespeichert sind. Weitere Informationen zu den Werten dieser Felder finden Sie auf folgender Website:

<http://wiki.netbeans.org/wiki/view/FaqInstallationDefaultTomcatPassword>

So prüfen Sie die Anschlussnummer des gebündelten Tomcat und die gespeicherten Berechtigungsnachweise:

- a. Wählen Sie in Identity Manager IDE die Registerkarte Laufzeit und erweitern Sie die Knoten Server und Bundled Tomcat.
  - b. Klicken Sie mit der rechten Maustaste auf den Knoten Bundled Tomcat und wählen Sie im Popup-Menü Eigenschaften.
  - c. Wenn das Dialogfeld Server Manager angezeigt wird, prüfen Sie die Felder Server-Port, Benutzername und Passwort.
- Das Klonen von Dokumenten funktioniert nicht. (ID-15725)
  - Wenn Sie ein Dokument vergleichen (diff) und die Änderungen nicht speichern, werden keine Ergebnisse angezeigt. Zurzeit weist keine Warnmeldung darauf hin. In Identity Manager IDE kann nur ein Vergleich des Dateiinhalts, nicht jedoch der Anzeige im Editorfenster vorgenommen werden. (ID-15952)
  - Wenn Sie einen Vergleich für ein Verzeichnis mit nicht gespeicherten Dateien ausführen, werden im Diff-Ausgabefenster keine Ergebnisse angezeigt. (ID-15955)
  - Wenn Sie mit dem Ausdrucks-Generator eine invoke-Anweisung erstellen, wird ein Fenster mit dem Javadoc-Dokument zur ausgewählten Methode angezeigt. Zurzeit können Sie nicht mit den Bildlaufleisten in dem Dokument blättern. Bei manchen Methoden wird das Javadoc-Dokument daher nicht vollständig angezeigt. (ID-16093)

### Zwischenlösungen:

- Nachdem Sie die Methode ausgewählt haben, wird das Javadoc-Dokument zeitweilig unten an den Rand des Ausdrucksfensters gestellt. Hier können Sie im gesamten Javadoc-Dokument blättern, doch da es sich um eine temporäre Kopie handelt, wird die Anzeige ausgeblendet, sobald Sie auf ein anderes Ausdruckselement oder einen anderen Ausdruck klicken.
- Verwenden Sie das Javadoc-Dokument, das im Verzeichnis *Image/REF/javadoc* auf dem Installationsmedium gespeichert ist.
- Eine NULL-Zeiger-Ausnahme tritt auf, wenn Sie die Validierung in der Designansicht aktivieren. (ID-16168)

**Zwischenlösung:** Führen Sie die Validierung in der XML-Datei durch (Quellenansicht).

## Anmeldekonfiguration

- Das Modul für die Pass-Through-Authentifizierung funktioniert bei der Domino-Ressource nicht (ID-1646).
- Änderungen bei den Seiten für das Administratoranmeldungssetup und Benutzeranmeldungssetup werden anderen angemeldeten Administratoren nicht angezeigt (ID-3487). Um die Änderungen anzuzeigen, müssen sich die anderen Administratoren bei der Administratorbenutzeroberfläche abmelden und anschließend wieder anmelden.
- Wenn sich ein Administrator anmeldet und erst Mein Passwort ändern und anschließend eine andere Registerkarte auswählt, wird das Konto gesperrt, bis die Sperre abgelaufen ist. (ID-3705)

Wenn ein anderer Administrator versucht, den gesperrten Administrator zu bearbeiten, wird folgende Meldung angezeigt:

```
com.waveset.util.WavesetException: Auf Konto #ID#Configurator kann zur Zeit nicht  
zugegriffen werden. Führen Sie den Vorgang später erneut aus.
```

Wenn dieser Administrator auf OK klickt, wird das Workflow-Prozessdiagramm der letzten Aktion angezeigt.

## Organisationen

- Wenn beim Löschen von mehreren Organisationen der Löschvorgang für eine Organisation fehlschlägt, werden die verbleibenden Organisationen auch nicht gelöscht (ID-517).
- Wenn bei einer Organisation, die zugewiesene Benutzer und ausstehende Bereitstellungsanforderungen aufweist, umbenannt wird, schlägt die Bereitstellungsanforderung fehl (ID-564).

**Zwischenlösung:** Stellen Sie sicher, dass keine ausstehenden Anforderungen vorhanden sind, bevor Sie eine Organisation umbenennen.

- Wenn beim Erstellen einer neuen Organisation die Option für die Benutzermitgliedsregel vor der Angabe eines Organisationsnamens ausgewählt wird und anschließend die Seite aktualisiert wird, erscheint eine Organisations-ID im Feld für den Organisationsnamen (ID-6302). Der Name kann weiterhin vor dem Speichern der neuen Organisation festgelegt werden.

( ) - Achtung: In Klammer stehende Werte im Feld Genehmiger entsprechen keinem der zulässigen Werte.

## Richtlinien und Fähigkeiten

- Das Identity Manager-Kontorichtlinienattribut Rücksetzungs-Benachrichtigungsoption hat die Wertoption „administrator“, welche keine Auswirkung hat (ID-944). Die einzig gültigen Optionen sind sofort und Benutzer.
- Wenn beim Löschen von mehreren Rollen ein Fehler auftritt, wird nicht mit den anderen Rollen fortgefahren, sondern der gesamte Vorgang angehalten (ID-1168).
- Die Mindestanzahl der Fragen, die ein Benutzer beantworten muss, kann auf einen Wert gesetzt werden, der größer als die Anzahl der definierten Fragen ist (ID-1834). In diesem Fall kann sich der Benutzer nicht über die Option Passwort vergessen anmelden.
- Die Lighthouse-Standardkontorichtlinie kann nicht durch Bearbeiten der Richtlinie, Ändern des Namens oder Erstellen eines neuen Objekts geklont werden (ID-5147).

**Zwischenlösung:** Erstellen Sie eine neue Kontorichtlinie.

## Abstimmen und Importieren von Benutzern

- Das Importieren von Benutzern aus einer CSV-Datei aktualisiert nicht die Ressourcenattribute, wenn der Benutzer bereits in Identity Manager vorhanden ist (ID-2041).
- Wenn bei einer CSV-Datei (bei der die Felder durch Kommas getrennt werden) die Konto-IDs in einfache Anführungszeichen (') gesetzt sind, werden die Anführungszeichen als Fragezeichen (?) geladen (ID-2100).
- Geplante Aufgaben werden auf der Seite Aufgaben suchen nicht als Ergebnis angezeigt, wenn die Option „ist geplant“ verwendet wird (ID-5001).
- Die Abstimmung schlägt fehl, wenn sie bei einer Ressource von Red Hat Version 8 ausgeführt wird (ID-6087).
- Die Abstimmung einer Oracle ERP-Ressource wird mit Fehlern abgeschlossen, wenn bei der Ressource das Verbindungspooling aktiviert ist (ID-6386). Zwischenlösung: Deaktivieren Sie das Verbindungspooling während der Abstimmung.

## Berichte

- Sicherheitsadministratoren können keine Berichte ausführen oder erstellen (ID-1217).

**Zwischenlösung:** Erteilen Sie den Administratoren die Berechtigungen zum Berichtsadministrator.

- Risikoanalyseberichte können auch von Administratoren angezeigt werden, die keine Berichtsadministratoren sind (ID-1224).
- Berichtsergebnisse, die mit der Option für das Nur-Text-Format per E-Mail gesendet werden, sind nicht formatiert (ID-2191).

**Zwischenlösung:** Verwenden Sie die HTML-Option für die E-Mail.

- Überwachungsprotokolleinträge werden möglicherweise bei umfangreichen Ergebnissen nicht erfasst (ID-5050).
- Die aktivierte Laufschrift wird nicht angezeigt, wenn in den Namen von Organisationen Apostrophe (') vorkommen (ID-5653).
- Wenn Sie versuchen, einen Administratorbericht auszuführen, und festlegen, dass nur Administratoren gemeldet werden, die einer bestimmten Organisation angehören, welche keine Administratoren hat, wird ein java.lang.NullPointerException-Fehler zurückgegeben (ID-5722).

## Ressourcen

- Über die Schaltfläche für den Ressourcentest werden nicht alle Felder getestet (ID-51).
- Zuweisungen für den Ressourcenport können auf Werte größer als 65535 gesetzt werden (ID-59).
- Wenn Sie einen falschen Active Directory-Gruppennamen festlegen, wird eine ungültige Fehlermeldung angezeigt (ID-393). Wenn Sie versuchen, einen Active Directory-Gruppennamen auf „groupname“ statt auf „cn=groupname,cn=builtin,dc=waveset,dc=com“ zu setzen, wird eine Fehlermeldung angezeigt, die besagt, dass sich der Arrayindex außerhalb der Grenzen befindet.
- Erforderliche Kontoattribute werden manchmal ignoriert, wenn eine andere Ressource mit demselben Kontoattributnamen vorhanden ist, bei der das erforderliche Flag nicht gesetzt ist (ID-1161).
- Wenn ein Administrator versucht, eine Organisation zu einer Ressource hinzuzufügen, ohne mit den zugehörigen Rechten ausgestattet zu sein, wird ein Fehler erzeugt. Die Bearbeitung der Ressource muss dann abgebrochen und anschließend wieder aufgenommen werden, um weitere Änderungen bei der Ressource vorzunehmen (ID-1274).
- Die Fehlermeldung, die bei einem falschen Ressourcenkontokennwort oder Benutzernamen erzeugt wird, ist bei einer nicht klaren PeopleSoft-Ressource falsch (ID-2235). Die Fehlermeldung lautet:

`bea.jolt.ApplicationException: TPESVCFAIL - Dienstausfall auf Anwendungsebene`

- Bei Windows Active Directory-Ressourcenaktionen, die den Beendigungsstatus `%DISPLAY_INFO_CODE%` verwenden, schlägt die Aktion mit Fehlern fehl (ID-2827).
- Bei Windows NT-Ressourcenaktionen, die einen Beendigungscode ungleich null zurückgeben, schlägt die Aktion fehl (ID-2828).
- Beim Erstellen eines Benutzers kann die primäre Gruppen-ID des Benutzers in Active Directory nicht festgelegt werden (ID-3221).

**Zwischenlösung:** Erstellen Sie den Benutzer, ohne die primäre Gruppen-ID festzulegen. Bearbeiten Sie anschließend den Benutzer, und legen Sie den Wert fest. Die primäre Gruppen-ID wird außerdem nach Nummer und nicht nach DN der Gruppe festgelegt.

- Ressourcen-IP-Adressen werden in der JVM zwischengespeichert, nachdem der Hostname in eine IP-Adresse aufgelöst wurde. Wenn eine Ressourcen-IP-Adresse geändert wurde, ist ein Neustart des Anwendungsservers erforderlich, damit Identity Manager die Änderung erkennt (ID-3635). Dies ist eine Einstellung in Sun JDK (ab Version 1.3), die über die Eigenschaft `sun.net.inetaddr.ttl` gesteuert wird, die in der Regel in `jre/lib/security/java.security` festgelegt wird.

- Sie können nicht mehrere Konten für einen einzelnen Benutzer bei Oracle-Ressourcen erstellen (ID-3832).
- Endbenutzer können die Selbsterkennungsfunktion nicht für Domino-Ressourcenkonten verwenden (ID-4775).
- Wenn ein Benutzer aus einem oder in einen Untercontainer innerhalb der Active Directory-Organisation verschoben wird, erkennt der ActiveSync-Adapter diese Änderung. Wenn Sie jedoch den Benutzer auf der Bearbeitungsseite anzeigen (oder eine Änderung vornehmen und die Bestätigungsseite aufrufen) wird die Konto-ID des Benutzers weiterhin als ursprünglicher DN (Distinguished Name, eindeutiger Name) angezeigt (ID-4950). Da der Benutzer über die GUID geändert wird, entstehen keine Probleme beim Betrieb. Sie können dieses Problem beheben, indem Sie für die Ressource eine Abstimmung ausführen.
- Wenn ein Benutzer aus einer Organisation (OU) in eine Unterorganisation verschoben wird, erkennt der LDAP ChangeLog-Adapter die Änderung nicht und geht davon aus, dass der Benutzer gelöscht wurde. Das Benutzerobjekt wird anschließend in Identity Manager gesperrt (wenn dies der aktuellen Einstellung entspricht), und es wird kein neues Konto für das verschobene Konto erstellt (ID-4953).
- Die im Pool abgelegten Verbindungen für die UNIX-Ressourcenadapter können in einem nicht festgelegten Status belassen werden, wenn bei der Ausführung von Befehlen oder Skripten Fehler auftreten (ID-5406).
- NDS-Organisationen können nur dann auf der obersten Ebene der Struktur erstellt werden, wenn Sie den Basiskontext für die Ressource auf „[ROOT]“ setzen (ID-5509).
- Wenn Sie in NDS ein Feld (beispielsweise die Verlängerungsfrist für die Anmeldung) während der ersten Bereitstellung bearbeiten und keine Werte für die booleschen Felder angeben, werden alle booleschen Felder auf FALSE gesetzt (ID-6770). Dadurch wird verhindert, dass die anderen Felder der Registerkarte für die Einschränkung bearbeitet werden können, weil bei denen für bestimmte Kontrollkästchenwerte TRUE gelten muss. Um dies zu vermeiden, stellen Sie immer sicher, dass alle gewünschten booleschen Felder auf TRUE gesetzt sind, damit sie beim Bearbeiten anderer Felder korrekt aktiviert werden.
- Wenn Sie das Passwort für einen UNIX-Computer über die Funktion Verbindung verwalten --> Ressourcenpasswortänderungs-Administrator ändern, wird der Aufgabenname folgendermaßen angezeigt:  

```
_FM_PASSWORD_CHANGING_TASK null:null
```

Es soll ein benutzerfreundlicher Name angezeigt werden. (ID-6947)
- Sie können die Funktion zum Verwalten von Verbindungen nicht für UNIX-Ressourcen einsetzen, die NIS verwenden (ID-6948). Es wird ein Fehler erzeugt, weil das Passwort, das Sie ändern möchten, für das Root-Konto bestimmt ist, das von NIS nicht verwaltet wird.

- Wenn Sie Benutzer aktualisieren, indem Sie eine Aktualisierung aus einer Identity Manager-Organisation auswählen, erhalten Benutzer mit einem Sun One ID Server-Konto einen Fehler, falls diese nativ erstellt und in Identity Manager geladen wurden (ID-7094).  
Zwischenlösung: Aktualisieren Sie diese Benutzer individuell.
- Identity Manager enthält weiterhin folgende verworfenen Klassen:
  - com.waveset.object.IAPI
  - com.waveset.object.IAPIProcess
  - com.waveset.object.IAPIUser

Angepasste Adapterklassen sollten nicht mehr auf diese Klassen, sondern auf die entsprechenden Klassen in package com.waveset.adapter.iapi verweisen (ID-8246).

- Beim Löschen eines Benutzers, der ein Konto bei der Ressource für die PeopleSoft Komponentenschnittstelle hat, tritt ein Fehler auf. Diese Ressource unterstützt derzeit nicht das Löschen von Konten. (ID-9000)
- Wenn Sie den Assistenten „Neues Ressourcenobjekt“ beenden, ohne auf die Schaltfläche **Speichern** oder **Abbrechen** zu klicken, wird das verworfene Formular möglicherweise nicht vollständig gelöscht. Dies kann später beim Erstellen neuer Ressourcenobjekte zu Problemen führen. (ID-11033) In diesem Fall wird folgender Fehler angezeigt:

No resource form id found in options or view.

**Zwischenlösung:** Klicken Sie immer auf „Abbrechen“, wenn Sie den Assistenten „Neues Ressourcenobjekt“ beenden wollen, ohne die Änderungen zu speichern.

- Kontingenteinstellungen sind für temporäre Tablespaces 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 Tablespaces ein Kontingent fest, auch wenn das Attribut 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 Tablespaces dagegen kein Kontingent festgelegt.

**Zwischenlösung:** Löschen Sie für Oracle 10gR2-Installationen das Attribut oracleTempTSQuota aus dem Ressourcenadapter.

- Beim Remedy-Integrations-Vorlageneditor sind zwei Probleme bekannt. (ID-14729)
  - Der standardmäßige Remedy-Schemawert „HPD:HelpDesk“ ist für spätere Versionen von BMC Remedy nicht geeignet. Spätere Versionen enthalten das Schema „HPE:Help Desk“.
  - Die Optionen-Spalten werden nicht für alle Felder angezeigt. Die Verwendung von Remedy-Vorlagen wird dadurch nicht eingeschränkt.

- Es kann vorkommen, dass bei in Identity Manager erstellten NDS/Groupwise-Benutzern mit Access- und AccountID-Feldern die entsprechenden Werte scheinbar nicht gespeichert sind, wenn für die Anzeige bestimmte Viewer innerhalb der NDS ConsoleOne-Anwendung verwendet werden. Dies ist z. B. der Fall, wenn Benutzereigenschaften und dann die Registerkarte „Groupwise“ ausgewählt werden.

Wenn dagegen die Anzeige über „Groupwise Diagnostisc“ -> „Objekt anzeigen“ erfolgt, sind die Felder zu sehen. In Identity Manager an den oben genannten Feldern vorgenommene Aktualisierungen scheinen von diesem Viewer-Fehler nicht betroffen zu sein. (ID-16330)

- Die Regel IS\_DELETE (zum Konfigurieren des PeopleSoft Active Sync-Adapters) wird im Pulldown-Menü der bekannten Regeln nicht angezeigt. (ID-16398)

Zwischenlösung: Bearbeiten Sie die Datei \$WSHOME/sample/rules/PeopleSoftRules.xml und geben Sie den unten angegebenen Text ein. Importieren Sie die Datei über „Konfiguration“ -> „Exchange-Datei importieren“ dann erneut.

```
<?xml version='1.0' encoding='UTF-8'?>
<!DOCTYPE Waveset PUBLIC 'waveset.dtd' 'waveset.dtd'>
<Waveset>
  <Rule name='IS_DELETE'>
    <Description>Should the active sync event delete the user?</Description>
    <oder>
      <eq><ref>activeSync.Status</ref><s>T</s></eq>
      <eq><ref>activeSync.Status</ref><s>L</s></eq>
    </or>
  </Rule>
</Waveset>
```

- Beim Laden eines Benutzers löscht der Oracle ERP-Adapter die vorherigen Zuständigkeitswerte. Die aktuellen Werte für description, start\_date und end\_date der Zuständigkeiten des Benutzers werden beim Ausführen von getUser() nicht richtig formatiert in das Formular übernommen. Dadurch können Zuständigkeitsdaten beschädigt werden. (ID-16414)

**Zwischenlösung:** Bearbeiten Sie das Feld `includeResponsibilities` im Beispielbenutzerformular `OracleERPUserForm.xml` und fügen Sie einen Standardwert ein. Importieren Sie die Datei über „Konfiguration“ -> „Exchange-Datei importieren“ dann erneut.

```
<Field name='includeResponsibilities'>
  <Display class='Checkbox' action='true'>
    <Property name='title' value='Add Direct Responsibilities' />
  </Display>
  <Standard>
    <cond>
      <gt>
        <length>
          <ref>global.responsibilities</ref>
        </length>
        <i>0</i>
      </gt>
      <s>true</s>
    </cond>
  </Default>
  <Disable>
    <not>
      <ref>global.showOracleERPFields</ref>
    </not>
  </Disable>
</Field>
```

—ODER—

Wählen Sie auf der Seite „Attribute“ die Schaltfläche **Laden**, um den Benutzer ein zweites Mal zu laden.

## Ressourcenobjektverwaltung

- Ein Windows Active Directory-Objekt (Gruppe, Organisationseinheit oder Container) kann auf der Seite Ressourcen auflisten nicht umbenannt werden (ID-3329).
- Es können keine neuen LDAP-Gruppen erstellt werden, wenn Benutzer mit CNs mit mehreren Werten vorhanden sind (ID-3848).

**Zwischenlösung:** Verwalten Sie die Mitglieder der Gruppe nicht nach dem im LDAP-Formular zum Erstellen von Gruppen konfiguriertem CN, sondern nach dem DN.

## Ressourcengruppen

- Wenn Sie auf der Seite zum Erstellen oder Bearbeiten von Ressourcengruppen die EINGABETASTE drücken, werden die auf der Seite vorgenommenen Änderungen gelöscht (ID-3430).
- Berichte über Ressourcengruppen können nicht als CSV-Datei gespeichert werden. (ID-8001)

## Sicherheit

- Identity Manager gibt keine `java.lang.StackOverflowError`-Ausnahme mehr aus, wenn folgende Bedingungen eintreten: (ID-15035)
  - a. Mindestens eine dynamische Organisation (regelgesteuerte Benutzermitglieder) ist unter Identity Manager definiert.
  - b. Das Benutzerformular enthält ein `<Field>`, das bei `Type.USER` die Funktion `getObject` aufruft.

Die `StackOverflowError`-Ausnahme wurde durch eine Endlosschleife verursacht, die bei der Auswertung der Erweiterungsberechtigung entstanden ist.

Zur Behebung dieses Problems wurden zwei neue Boolesche Optionen für die Benutzeransicht hinzugefügt:

- `NoFormDerviation` (Standardwert „true“)
- `NoFormExpansion` (Standardwert „true“)

Diese Optionen werden immer übergeben, wenn die Übergabe einer Benutzeransicht an eine Regel angefordert wird. Indem Sie diese Optionen auf **true** setzen, können Sie Formularableitungen und -erweiterungen verhindern.

---

**HINWEIS** Wenn die Optionen auf **true** gesetzt sind und innerhalb einer Regel das Formularfeld „Derivation“ oder „Expansion“ benötigt wird, muss dieses Bestandteil der Regellogik sein.

Weitere Informationen zum Einstellen von Ansichtsoptionen finden Sie unter „Setting View Options in Forms“ im Dokument *Identity Manager Workflows, Forms, and Views*.

---

## Server

- Benutzer von Identity Manager 4.x sollten sicherstellen, dass ihr Hostserver in einer eindeutigen Zeitzone operiert. So kann beispielsweise die Zeitzone EST entweder in Australien oder den USA verwendet werden, GMT+10 oder GMT-6 ist dagegen eindeutig. (ID-8297)
  - Die Klasse `com.waveset.rpm.SimpleRpcHandler` wurde ab Version 7.1 verworfen. (ID-14756)
1. Fügen Sie der Bereitstellungsbeschreibung die folgende Servlet-Definition hinzu:

```
<servlet>
  <servlet-name>rpcrouter3</servlet-name>
  <display-name>OpenSPML SOAP Router</display-name>
  <description>no description</description>
  <servlet-class>
    org.openspml.server.SOAPRouter
  </servlet-class>

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

  <init-param>
    <param-name>spmlHandler</param-name>
    <param-value>com.waveset.rpc.SpmlHandler</param-value>
  </init-param>

  <init-param>
    <param-name>rpcHandler</param-name>
    <param-value>com.waveset.rpc.RemoteSessionHandler</param-value>
  </init-param>
</servlet>
```

2. Fügen Sie der Bereitstellungsbeschreibung die folgende Servlet-Zuordnung hinzu:

```
<servlet-mapping>
  <servlet-name>rpcrouter3</servlet-name>
  <url-pattern>/servlet/rpcrouter3</url-pattern>
</servlet-mapping>
```

Zur Verwendung von `createView` mit `RemoteSession` ist das Servlet `rpcrouter3` erforderlich. Für den Zugriff auf das Servlet `rpcrouter3` ist der Konstruktor `RemoteSession(URL, String, EncryptedData)` erforderlich.

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

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

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

- Wenn Sie Identity Manager auf dem Sun Application Server bereitstellen und die Option `--precompile` übergeben, schlägt die JSP-Vorkompilierung fehl, weil Identity Manager zwar mit JSP-Fragmenten arbeitet, diese jedoch nicht die Erweiterung `.jspx` aufweisen. (ID-16373)

**Zwischenlösung:** Benennen Sie diese Dateien um, so dass sie die Erweiterung `.jspx` aufweisen.

In Sun Application Server 8.2 und 9.0 gibt es jetzt eine Option, mit der Sie festlegen können, dass Vorkompilierungsfehler aufgrund von `.jsp`-Fragmenten ignoriert werden. Weitere Informationen finden Sie hier:

[http://bugs.sun.com/bugdatabase/view\\_bug.do?bug\\_id=6393940](http://bugs.sun.com/bugdatabase/view_bug.do?bug_id=6393940)

## Sun Identity Manager Gateway

- Sun Identity Manager Gateway wird nicht angehalten, wenn im Fenster für die NT-Dienste die Schaltfläche zum Stoppen aktiviert wird. (ID-590)

**Zwischenlösung:** Brechen Sie die Ausführung des Stoppbefehls ab (wenn dieser immer noch inaktiv ist), und stoppen Sie den Dienst erneut; oder beenden Sie das Dialogfeld für die NT-Dienste, und führen Sie den Stoppvorgang erneut aus.

- Die Benutzer können in einer NT-Domäne nicht zu Gruppen hinzugefügt werden, wenn sich das Gateway in einer entfernten vertrauenswürdigen Domäne befindet. (ID-711)
- Das Gateway wird gelegentlich nicht angehalten, wenn der Befehl `'net stop "Sun Identity Manager Gateway"'` verwendet wird. (ID-2337)

## Aufgaben

- Administratoren mit Identity Manager-Administratorrechten können die Seite zum Verwalten von Aufgaben nicht anzeigen, wenn sich in der Aufgabenliste eine Risikoanalyse befindet. (ID-1225)
- Administratoren, die das oberste Element („Top“) nicht steuern, können keine geplanten Aufgaben für Discovery oder ResourceScanner erstellen. (ID-1414)
- Auf der Seite zum Ermitteln von Aufgaben wird die Anzahl der Aufgaben, die den Suchkriterien entsprechen (ID-5152), nicht angezeigt.
- Delegierte Administratoren, die das oberste Element („Top“) nicht steuern, können Aufgaben planen und die Aufgabenergebnisse anzeigen. Diese Administratoren können die Aufgabe jedoch nicht anzeigen, nachdem sie erstellt wurde (ID-6659). Die geplante Aufgabe wurde an oberster Stelle platziert, und der delegierte Administrator ist nicht berechtigt, das Objekt anzuzeigen.
- In der Bibliothek wurde ein Feld für verschobene Aufgaben hinzugefügt. Hierbei werden die verschobenen Aufgaben für einen Benutzer aufgelistet. Um dieses Feld zu implementieren, müssen Sie dem in Registerkarten unterteilen Benutzerformular und dem in Registerkarten unterteilten Benutzeranzeigeformular folgende Zeile hinzufügen. (ID-7660)

```
<FieldRef name='Deferred Tasks' />
```

## Workflow, Formulare, Regeln und XPRESS

- Zum Vergleichen von Booleschen Werten mit den Zeichenketten TRUE oder FALSE oder den ganzen Zahlen 1 oder 2 kann die XPRESS-Funktion <eq> nicht verwendet werden. (ID-3904)

**Zwischenlösung:** Verwenden Sie Folgendes:

```
<cond>
  <isTrue><ref>Boolean_variable</ref></isTrue>
  <s>True action</s>
  <s>False action</s>
</cond>
```

- Die Pfadausdrücke funktionieren nicht bei der Iteration einer Liste mit generischen Objekten über eine Dolist (ID-4920).

```
<dolist name='genericObj'>
  <ref>listOfGenericObjects</ref>
  <ref>genericObj.name</ref>
</dolist>
```

**Zwischenlösung:** Verwenden Sie <get> / <set> wie folgt:

```
<dolist name='genericObj'>
  <ref>listOfGenericObjects</ref>
  <get><ref>genericObject</ref><s>name</s>
</dolist>
```

- Wenn Sie global.attrname-Variablen für die Felder Ihres Benutzerformulars verwenden und das Attribut für mehrere Ressourcen freigegeben ist, müssen Sie außerdem eine Ableitungsregel definieren (ID-5074). Wenn andernfalls das Attribut nativ auf einer der Ressourcen geändert wird, kann das Attribut ausgewählt und auf die anderen Ressourcen propagiert werden.
- Es können in den HTML-Komponenten der Formulare keine Sonderzeichen verwendet werden, die mit & beginnen. So wird beispielsweise &nbsp; nicht als Leerzeichen dargestellt. Dieses Problem wurde wegen der neuen Unterstützung von Sonderzeichen (&\<>) in Auswahllisten nicht angegeben. (ID-5548)
- Die Formular-, Workflow- und Regelkommentare in <Comment>-Marken haben &#xA;-Zeichenfolgen für das Zeilenvorschubzeichen (ID-6243). Diese Zeichen werden nur im XML-Format für diese Objekte angezeigt. Der Identity Manager-Server und Business Process Editor verarbeiten diese Zeichen korrekt.
- Wenn Sie die Löschvorlagen mit Massenaktionen verwenden, wird das Verhalten der Massenaktion durch die Löschvorlagen außer Kraft gesetzt, ohne dass es Anzeichen für diese Aktion gibt. (ID-10320)
- Wenn Sie das Ressourcentabellenbenutzer-Formular zum Bearbeiten von Benutzern verwenden, während Sie die Ressource eines Benutzers bearbeiten, werden die Ressourcenattribute bei der ersten Anzeige des Formulars nicht abgerufen.

**Zwischenlösung:** Klicken Sie auf die Schaltfläche Aktualisieren, um die Attributdaten abzurufen. (ID-10551)

---

# Service Provider Edition

In diesem Abschnitt sind bekannte Probleme und Zwischenlösungen für Identity Manager SPE beschrieben.

- Identity Manager SPE und Sun Java System Portal Server sind nicht immer kompatibel, weil ein Problem bei den verschlüsselten Bibliotheken vorliegt. (ID-10744)

Sie können dieses Problem beheben, indem Sie folgende Werte in der Datei `/etc/opt/SUNWam/config/AMConfig.properties` für den Portalserver festlegen und anschließend den Webcontainer neu starten:

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

- Beim Arbeiten mit SPE-Bedienfeldern: Wenn das erstmalige Laden der Diagramme mehrere Minuten dauert, stellen Sie sicher, dass der Browser nicht für MSJVM (Microsoft Java Virtual Machine) konfiguriert ist. Identity Manager SPE unterstützt MSJVM nicht für die Ausführung von Browserapplets. (ID-10837)
- Einige Konfigurationsoptionen in der Identity Manager-Administratorbenutzeroberfläche werden in Identity Manager SPE nicht verwendet (ID-10843). Hierzu gehören:
  - Ressourcenoptionen: Kontenausschlussregel, Genehmiger und die Organisation, der die Ressource zugeordnet ist.
  - Rollenattribute
- Standardmäßig wird die Überwachung bei `checkinObject-` und `deleteObject-IDMXContext-API-`Aufrufen nicht ausgeführt. Die Überwachung muss ausdrücklich angefordert werden, indem der `IDMXContext.OP_AUDIT`-Schlüssel in der Optionszuordnung, die diesen Methoden übergeben wird, auf `TRUE` gesetzt wird. Die `createAndLinkUser()`-Methode der `ApiUsage`-Klasse veranschaulicht, wie die Überwachung angefordert wird. (ID-11261)
- Das Ändern von Bedienfelddiagrammnamen funktioniert nicht richtig. Der neue Name wird beim Bearbeiten des Diagramms zwar angezeigt, auf allen anderen Seiten wird der neue Name dagegen nicht für das Diagramm verwendet. (ID-11690)

- Die Standardgruppe des Service Provider-Anmeldmoduls geht davon aus, dass die Service Provider-Ressource den Namen „SPE End-User Directory“ hat. Hat die Ressource jedoch einen anderen Namen, funktioniert die Anmeldeseite für Service Provider-Endbenutzer nicht einwandfrei. Auf der Seite werden dann keine Anmeldefelder angezeigt. (ID-14891)

**Zwischenlösung:** Aktualisieren Sie den Ressourcennamen im Objekt

`UI_LOGIN_MOD_GRP_DEFAULT_SPE_PWD LoginModGroup`, damit der richtige Ressourcename referenziert wird.

- Da es sich bei SPE Sync um eine geplante Aufgabe handelt, lässt sich die Synchronisation nicht stoppen, indem Sie die Aufgabe auf der Aufgabenseite stoppen. Sie können dazu den Zeitplan selbst deaktivieren. (ID-16000)

**Zwischenlösung:** Vorzugsweise sollten Sie die Aufgabe über die Benutzeroberfläche auf der Ressourcenseite starten und stoppen oder SPE Sync programmgesteuert (z. B. aus einem Workflow heraus) über die `SessionUtil`-Methoden starten und stoppen. Damit SPE Sync beim Starten einer Identity Manager-Serverinstanz nicht automatisch gestartet wird, müssen Sie sie in der Synchronisationsrichtlinie für die Ressource deaktivieren. Durch das Stoppen von SPE Sync über die Benutzeroberfläche oder `SessionUtil`-Methoden wird die Synchronisation nur beendet, bis eine weitere Identity Manager-Serverinstanz gestartet wird.

- Wenn Sie die Anmeldeseite für Identity Manager SPE-Endbenutzer in WebSphere verwenden, tritt die Ausnahme `javax.servlet.UnavailableException` auf und es wird ein 404-Fehler im Browser angezeigt. (ID-16001)

**Zwischenlösung:** Sie müssen im IBM 1.5 JDK die folgenden Eigenschaften festlegen:

- a. Benennen Sie im Verzeichnis `was-install/java/jre/lib` `jaxb.properties.sample` in `jax.properties` um und entfernen Sie den Kommentar in diesen beiden Zeilen:

```
javax.xml.parsers.SAXParserFactory=  
    org.apache.xerces.jaxp.SAXParserFactoryImpl  
javax.xml.parsers.DocumentBuilderFactory=  
    org.apache.xerces.jaxp.DocumentBuilderFactoryImpl
```

- b. Speichern Sie die Datei und starten Sie den Anwendungsserver neu.

# Installations- und Aktualisierungshinweise

In diesem Abschnitt finden Sie Informationen zur Installation und Aktualisierung; die Informationen sind wie folgt unterteilt:

- [Installationshinweise](#)
- [Aufrüstungshinweise](#)

Eine Schemaänderung findet bei den meisten Identity Manager-Hauptversionen statt. Vor der Aufrüstung auf eine neue Identity Manager-Version müssen Sie das Schema aktualisieren. Je nach der Version, von der aus Sie aufrüsten, führen Sie zur Aufrüstung auf Identity Manager 7.1 eines der folgenden Aufrüstungsskripte für Schemata aus: (ID-15392 und ID-15722)

- Ausgehend von Identity Manager 6.0: Führen Sie das Skript `upgradeto71from60` aus.
- Ausgehend von Identity Manager 7.0: Führen Sie das Skript `upgradeto71from70` aus.

- 
- HINWEISS**
- Sehen Sie vor der Aufrüstung von Identity Manager in *Sun Java™System Identity Manager Installation* die für Ihren Anwendungsserver spezifischen Installationsanweisungen ein.
  - Detaillierte Informationen und Anweisungen für Aufrüstungen finden Sie in *Sun Java™System Identity Manager Upgrade*.
  - Wenn Ihre aktuelle Identity Manager-Installation ein großes Volumen von benutzerdefinierten Arbeiten enthält, sollten Sie sich für Unterstützung bei der Planung und Ausführung der Aufrüstung an den Sun Professional Services wenden.
- 

## Installationshinweise

Die folgenden Informationen beziehen sich auf die Installation des Produktes:

- Identity Manager muss unter HP-UX manuell installiert werden.
- Das Identity Manager-Installationsdienstprogramm unterstützt bei der Installation nun ein beliebiges Installationsverzeichnis. Sie müssen dieses Verzeichnis jedoch vor der Installation selbst erstellen oder im Setup-Fenster festlegen, dass das Verzeichnis erstellt werden soll.
- Für die Ausführung von Sun Identity Manager Gateway unter Windows NT ist die Active Directory Clienterweiterung von Microsoft erforderlich. Der DSClient ist unter folgender Adresse verfügbar:

<http://support.microsoft.com/default.aspx?scid=kb;en-us;Q288358>

---

**HINWEIS** Detaillierte Anweisungen zur Produktinstallation finden Sie in *Sun Java™ System Identity Manager Installation*.

---

- Für Unix/Linux gibt es zwei zusätzliche Installationsvoraussetzungen (ID-8403):
  - Für 5.0 - 5.0 SP1:
    - muss `/var/tmp` vorhanden sein.
    - muss `/var/tmp` vom Benutzer, der die Installation ausführt, beschreibbar sein.
  - Für 5.0 SP2 oder höher:
    - muss `/var/opt/sun/install` vorhanden sein.
    - muss `/var/opt/sun/install` vom Benutzer, der die Installation ausführt, beschreibbar sein.

---

## Aufrüstungshinweise

In diesem Abschnitt sind die Aufgaben zusammengefasst, die zum Aufrüsten von Identity Manager von Version 6.0 oder 7.0 auf Version 7.1 ausgeführt werden müssen. (Weitere Informationen zu den Versionen, die auf Identity Manager 7.1 aufgerüstet werden können, finden Sie in „[Identity Manager Aufrüstungsmöglichkeiten](#)“ auf Seite 13.)

Die Informationen in diesem Abschnitt sind wie folgt unterteilt:

- [Probleme bei der Aufrüstung](#)
- [Arbeiten mit dem Identity Manager-Aufrüstungsprogramm](#)
- [Manuelle Aufrüstung](#)

## Probleme bei der Aufrüstung

- Die Dateilisten `changedFileList` und `notRestoredFileLists` enthalten nach der Aufrüstung die folgenden Dateien. Diese Dateien sollten nicht angezeigt werden und es sind keine Aktionen erforderlich. (ID9228)

```
bin/winnt/nspr4.dll
bin/winnt/jdic.dll
bin/winnt/MozEmbed.exe
bin/winnt/IeEmbed.exe
bin/winnt/AceApi.dll
bin/winnt/DominoAPIWrapper.dll
bin/winnt/DotNetWrapper.dll
bin/winnt/gateway.exe
bin/winnt/lhpic.dll
bin/winnt/msems.inf
bin/winnt/pwicvc.exe
bin/winnt/remedy.dll
bin/solaris/libjdic.so
bin/solaris/mozembed-solaris-gtk2
bin/linux/librfccm.so
bin/linux/libsapjcorfc.so
bin/linux/libjdic.so
bin/linux/mozembed-linux-gtk2
```

- Wenn Sie von einer 6.x-Installation auf Version 7.0 oder 7.1 aufrüsten und die neuen Identity Manager-Endbenutzerseiten verwenden möchten, müssen Sie die Systemkonfiguration `ui.web.user.showMenu` manuell auf „true“ einstellen, damit die horizontale Navigationsleiste angezeigt wird. (ID-14901)

Wenn das neue Endbenutzer-Dashboard auf der Endbenutzer-Homepage angezeigt werden soll, müssen Sie außerdem die Endbenutzer-Formularzuordnung für den Formulartyp 'endUserMenu' manuell ändern. Rufen Sie „Konfigurieren“ -> „Formular- und Prozesszuordnungen“ auf. Ändern Sie für den Formulartyp 'endUserMenu' die Angabe unter „Formularname, zugeordnet zu“ in 'End User Dashboard'.

Aktualisieren Sie außerdem die Zuordnung für den Formulartyp 'endUserWorkItemListExt'. Ändern Sie die Angabe unter „Formularname, zugeordnet zu“ in 'End User Approvals List'.

- Wenn Sie von 6.0 oder 7.0 auf Version 7.1 aufrüsten und LocalFiles verwenden, müssen Sie vor der Aufrüstung alle Ihre Daten exportieren und dann nach der Neuinstallation von 7.1 wieder importieren. (ID-15366)
- Wenn Sie von einer älteren Version auf Identity Manager 7.1 aufrüsten, wird die Datei `WEB-INF/speConfiguration.xml` bei der Aufrüstung nicht entfernt. Diese Datei wird jedoch von der Service Provider-Funktion nicht mehr benötigt und kann daher problemlos entfernt werden. Auch die Eigenschaft `spe.enableServer` kann in der Datei `Waveset.properties` noch enthalten sein. Diese Eigenschaft wird in Identity Manager 7.0 oder 7.1 ebenfalls nicht mehr benötigt. (ID-15765)

# Arbeiten mit dem Identity Manager-Aufrüstungsprogramm

In diesem Abschnitt sind die Schritte beschrieben, die zum Aufrüsten von Identity Manager mit dem Identity Manager-Installations- und Aufrüstungsprogramm erforderlich sind.

---

**HINWEISS** • Eine Schemaänderung findet bei den meisten Identity Manager-Hauptversionen statt. Vor der Aufrüstung auf eine neue Identity Manager-Version müssen Sie das Schema aktualisieren. Je nach der Version, von der aus Sie aufrüsten, führen Sie zur Aufrüstung auf Identity Manager 7.1 eines der folgenden Aufrüstungsskripte für Schemata aus: (ID-15722)

- Ausgehend von Identity Manager 6.0: Führen Sie das Skript `upgradeto71from60` aus.
- Ausgehend von Identity Manager 7.0: Führen Sie das Skript `upgradeto71from70` aus.

Weitere Informationen finden Sie in *Sun Java™ System Identity Manager Upgrade*.

- In einigen Umgebungen wie z. B. HP-UX müssen oder möchten Sie u. U. eine manuelle Aktualisierung durchführen. In diesem Fall gehen Sie direkt zu [„Manuelle Aufrüstung“ auf Seite 84](#).
  - Stellen Sie in UNIX-Umgebungen sicher, dass an einem der folgenden Speicherorte ein Verzeichnis mit der Bezeichnung `install` vorhanden ist und dass dieses beschreibbar ist:
    - **Linux/HP-UX:** `/var/opt/sun/install`
    - **Solaris:** `/var/sadm/install`
  - Während der Aktualisierung müssen Sie den Pfad angeben, auf dem der Anwendungsserver installiert ist.
  - Alle zuvor installierten Hotfixes werden im folgenden Verzeichnis archiviert:
 

```
$WSHOME/patches/HotfixName
```
  - Alle in den folgenden Schritten angegebenen Befehle setzen eine Windows-Installation und einen Tomcat-Anwendungsserver voraus. Die von Ihnen verwendeten Befehle können sich daher je nach Umgebung unterscheiden.
-

So rüsten Sie Identity Manager auf:

1. Schließen Sie den Anwendungsserver.
2. Wenn Sie auf Identity Manager 6.0 oder Identity Manager 7.0 aufrüsten, müssen Sie das Repository-Datenbankschema wie folgt aktualisieren:
  - **Identity Manager 6.0** umfasst eine Schemaänderung, die neue Tabellen für Aufgaben, Gruppen, Organisationen und das Syslog beinhaltet. Sie müssen diese neuen Tabellenstrukturen erstellen und die vorhandenen Daten verschieben.
  - In Identity Manager 6.0 werden Benutzerobjekte in zwei Tabellen gespeichert. Sie können für die Schemaänderungen die Beispielskripte verwenden, die sich im Verzeichnis `db_scripts` befinden. Verwenden Sie das Skript `db_scripts/upgradeto2005Q4M3.DatabaseName`, um die Repository-Tabellen zu aktualisieren.

---

**HINWEIS**

- Vor der Aktualisierung des Repository-Schemas erstellen Sie eine vollständige Datensicherung der Repository-Tabellen.
- Die Aufrüstung der MySQL-Datenbanken ist höchstkomplex. Weitere Informationen hierzu finden Sie in `db_scripts/upgradeto2005Q4M3.mysql`.

---

- **Identity Manager 7.0** umfasst neue Tabellen für Benutzeransprüche. Sie müssen diese neuen Tabellenstrukturen erstellen und die vorhandenen Daten verschieben. Sie können für die Schemaänderungen die Beispielskripte verwenden, die sich im Verzeichnis `db_scripts` befinden.

---

**HINWEIS**

- Vor der Aktualisierung des Repository-Schemas erstellen Sie eine vollständige Datensicherung der Repository-Tabellen.
- Weitere Informationen hierzu finden Sie im Skript `db_scripts/upgrade7.0.DBMSName`.

---

3. Wenn Sie Sun Identity Manager Gateway auf dem Identity Manager-Server ausführen, unterbrechen Sie den Gateway-Dienst mit dem folgenden Befehl:

```
net stop "Sun Identity Manager Gateway"
```

4. Wählen Sie eine der folgenden beiden Möglichkeiten zum Starten des Installationsprogramms:

- Um das GUI-Installationsprogramm zu verwenden, führen Sie `install.bat` (für Windows) oder `install` (für UNIX) aus.

Das Installationsprogramm zeigt das Fenster Willkommen an.

- Um das Installationsprogramm im Modus `nodisplay` zu aktivieren, wechseln Sie in das Verzeichnis, in dem sich die Software befindet, und geben den folgenden Befehl ein:

```
install -nodisplay
```

Das Installationsprogramm zeigt eine Begrüßung an und fährt dann mit einer Liste von Fragen fort, mit der in der gleichen Reihenfolge wie beim GUI-Installationsprogramm Installationsinformationen erfasst werden sollen:

- 
- HINWEIS**
- Wenn nichts angezeigt wird, arbeitet das Installationsprogramm im Modus `nodisplay`.
  - Das Installationsprogramm installiert keine ältere Version der Software über eine neuere Version. Sollte diese Situation eintreten, wird eine Fehlermeldung angezeigt und das Installationsprogramm wird geschlossen.
- 

5. Klicken Sie im Fenster Willkommen auf Weiter.

6. Wählen Sie im Fenster Install or Upgrade? die Option Upgrade und klicken Sie dann auf Weiter.

7. Wählen Sie im Fenster Select Installation Directory das Verzeichnis aus, in dem sich die vorherige Identity Manager-Version befindet und klicken Sie auf Weiter.

Das Installationsprogramm zeigt Fortschrittsbalken für die Prozesse vor und nach der Aufrüstung an; danach wird das Fenster Installation Summary angezeigt.

8. Um detaillierte Installationsinformationen anzuzeigen, klicken Sie auf Details und zeigen die Protokolldatei an. Klicken Sie dann auf Schließen, um das Installationsprogramm zu beenden.

9. Entfernen Sie alle kompilierten Identity Manager-Dateien aus dem Arbeitsverzeichnis des Anwendungsservers.

10. Wenn Sie ein Gateway auf einem Remotesystem betreiben, rüsten Sie dieses wie folgt auf.

a. Melden Sie sich beim Windows-System an und wechseln Sie in das Verzeichnis, in dem das Gateway installiert ist.

b. Stoppen Sie den Gateway-Dienst durch die Ausführung des folgenden Befehls:

```
gateway -k
```

c. Wenn Sie unter Windows 2000 oder höher arbeiten, beenden Sie alle Instanzen des Services MMC-Plugins.

d. Entfernen Sie den Gateway-Dienst durch die Ausführung des folgenden Befehls:

```
gateway -r
```

e. Sichern und löschen Sie die vorhandenen Gateway-Dateien.

f. Extrahieren Sie die neuen Gateway-Dateien.

Wenn Sie das neu aufgerüstete Gateway auf einem System installieren, bei dem es sich nicht um den Identity Manager-Server handelt, kopieren Sie die Datei `gateway.zip` von der Identity Manager Installations-CD .

g. Entpacken Sie die Datei `gateway.zip` in das Verzeichnis, in dem das Gateway installiert war.

h. Installieren Sie den Gateway-Dienst durch die Ausführung des folgenden Befehls:

```
gateway -i
```

i. Starten Sie den Gateway-Dienst durch die Ausführung des folgenden Befehls:

```
gateway -s
```

## Manuelle Aufrüstung

In einigen Umgebungen möchten Sie die Aufrüstung u. U. nicht mit Identity Manager-Installations- und Aufrüstungsprogramm, sondern manuell durchführen.

- 
- HINWEIS**
- Achten Sie darauf, dass Sie die Umgebungsvariable `JAVA_HOME` einstellen.
  - Vergewissern Sie sich, dass sich das Verzeichnis `bin` im Verzeichnis `JAVA_HOME` in Ihrem Pfad befindet.
  - Alle zuvor installierten Hotfixes werden im Verzeichnis `$(WSHOME)/patches/HotfixName` archiviert.
-

## Auf einer Windows-Plattform

So rüsten Sie Identity Manager auf einer unterstützten Windows-Plattform auf:

1. Beenden Sie den Applikationsserver und Sun Identity Manager Gateway.
2. Aktualisieren Sie die Identity Manager-Datenbank (detaillierte Anweisungen unter [Schritt 2 auf Seite 82](#)).
3. Führen Sie zur Einstellung der Umgebung die folgenden Befehle aus:

```
set ISPATH=Pfad zur Installationssoftware
set WSHOME=Pfad zum Identity Manager Installations- oder Stagingverzeichnis
set TEMP=Pfad zum temporären Verzeichnis
```

4. Führen Sie den Prozess vor der Aufrüstung aus:

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

5. Installieren Sie die Software:

```
cd %WSHOME%
jar -xvf %ISPATH%\IDM.WAR
```

6. Führen Sie den Prozess nach der Aufrüstung aus:

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

---

**HINWEIS** Das Installationsprogramm unterstützt die Aufrüstung von Installationen, in denen das standardmäßige Konfigurator-Konto umbenannt, gelöscht oder deaktiviert wurde.

Das Installationsprogramm fordert Sie zur Eingabe des Benutzernamens und Passwortes auf, um im Rahmen des Prozesses nach der Aufrüstung die Datei `update.xml` zu importieren. Wenn Sie den falschen Benutzernamen oder das falsche Passwort eingeben, werden Sie (maximal dreimal) aufgefordert, die richtigen Daten einzugeben. Der Fehler wird im Textfeld im Hintergrund angezeigt.

Für eine manuelle Installation müssen Sie die Flags `-U username -P password` angeben, um die Anmeldedaten an die Prozedur `UpgradePostProcess` zu übergeben.

---

7. Bei Installation in einem Stagingverzeichnis erstellen Sie zur Bereitstellung für Ihren Anwendungsserver die Datei `.war`.
8. Entfernen Sie die Identity Manager-Dateien aus dem Arbeitsverzeichnis des Anwendungsservers.
9. Wenn nicht bereits während der Aufrüstung geschehen, verschieben Sie alle Hotfix-Klassendateien vom Verzeichnis `WEB-INF\classes` in das Verzeichnis `$_WSHOME\patches\HotfixName`.
10. Starten Sie den Anwendungsserver.
11. Rüsten Sie Sun Identity Manager Gateway auf und starten Sie die Anwendung dann (detaillierte Anweisungen unter [Schritt 10 auf Seite 84](#)).

## Auf einer UNIX-Plattform

So rüsten Sie Identity Manager auf einer unterstützten UNIX-Plattform auf:

1. Beenden Sie den Applikationsserver und Sun Identity Manager Gateway.
2. Aktualisieren Sie die Identity Manager-Datenbank (Anweisungen unter [Schritt 2 auf Seite 82](#)).
3. Führen Sie zur Einstellung der Umgebung die folgenden Befehle aus:

```
export ISPATH=Pfad zur Installationssoftware
export WSHOME=Pfad zum Identity Manager-Installations- oder Stagingverzeichnis
export TEMP=Pfad zum temporären Verzeichnis
```

4. Führen Sie den Prozess vor der Aufrüstung aus:

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

5. Installieren Sie die Software:

```
cd $WSHOME
jar -xvf $ISPATH/idm.war
```

6. Führen Sie den Prozess nach der Aufrüstung aus:

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

---

**HINWEIS** Das Installationsprogramm unterstützt die Aufrüstung von Installationen, in denen das standardmäßige Konfiguratorkonto umbenannt, gelöscht oder deaktiviert wurde.

Das Installationsprogramm fordert Sie zur Eingabe des Benutzernamens und Passwortes auf, um im Rahmen des Prozesses nach der Aufrüstung die Datei `update.xml` zu importieren. Wenn Sie den falschen Benutzernamen oder das falsche Passwort eingeben, werden Sie (maximal dreimal) aufgefordert, die richtigen Daten einzugeben. Der Fehler wird im Textfeld im Hintergrund angezeigt.

Für eine manuelle Installation müssen Sie die Flags `-U username -P password` angeben, um die Anmeldedaten an die Prozedur `UpgradePostProcess` zu übergeben.

---

7. Ändern Sie das Verzeichnis auf `$WSHOME/bin/solaris` oder `$WSHOME/bin/linux` und legen Sie dann für die Dateien im Verzeichnis Berechtigungen fest, damit diese ausführbar sind.
8. Bei Installation in einem Stagingverzeichnis erstellen Sie zur Bereitstellung für Ihren Anwendungsserver die Datei `.war`.
9. Entfernen Sie die Identity Manager-Dateien aus dem Arbeitsverzeichnis des Anwendungsservers.

10. Wenn nicht bereits während der Aufrüstung geschehen, verschieben Sie alle Hotfix-Klassendateien vom Verzeichnis `WEB-INF/classes` in das Verzeichnis `$WSHOME/patches/HotfixName`.
11. Starten Sie den Anwendungsserver.
12. Rüsten Sie Sun Identity Manager Gateway auf und starten Sie die Anwendung dann (Anweisungen unter [Schritt 10 auf Seite 84](#)).

# Verworfen API

Dieser Abschnitt enthält alle Identity Manager-APIs (Application Programming Interfaces), die seit Identity Manager 6.0 2005Q4M3 verworfen wurden. Außerdem werden, falls verfügbar, deren Nachfolger aufgelistet. Die hier gegebenen Informationen sind wie folgt unterteilt:

- [Verworfen Konstruktoren und Klassen](#)
- [Verworfen Methoden und Felder](#)

---

## Verworfen Konstruktoren und Klassen

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

<b>Verworfen</b>	<b>Nachfolger</b>
<code>com.sun.idm.idmx.IDMXContext</code>	<code>com.waveset.object.LighthouseContext</code>
<code>com.sun.idm.idmx.IDMXContextFactory</code>	<code>com.waveset.session.SessionFactory</code>
<code>com.waveset.adapter.ActiveDirectoryActiveSyncAdapter</code>	<code>com.waveset.adapter.ADSIResourceAdapter</code>
<code>com.waveset.adapter.AIXResourceAdapter.BlockAcctIter</code>	Verweise auf diese Klasse sollten durch einen AccountIterator auf Grundlage des Lieferantenmodells ersetzt werden. Beispiel: <code>BufferedAccountQueue(neuer AIXAccountSupplier)</code> .
<code>com.waveset.adapter.AD_LDAPResourceAdapter</code>	<code>com.waveset.adapter.LDAPResourceAdapter</code>
<code>com.waveset.adapter.AttrParse</code>	<code>com.waveset.object.AttrParse</code>
<code>com.waveset.adapter.ConfirmedSync</code>	Verweise auf diese Klasse sollten durch einen AccountIterator auf Grundlage des Lieferantenmodells ersetzt werden. Beispiel: <code>BufferedAccountQueue(neuer LinuxAccountSupplier)</code> .
<code>com.waveset.adapter.DbiBufIterator</code>	<code>com.waveset.util.BufferedIterator</code> <code>com.waveset.util.BlockIterator</code> <code>com.waveset.adapter.AccountIteratorWrapper</code>
<code>com.waveset.adapter.DominoActiveSyncAdapter</code>	<code>com.waveset.adapter.DominoResourceAdapter</code>
<code>com.waveset.adapter.LDAPChangeLogActiveSyncAdapter</code>	<code>com.waveset.adapter.LDAPResourceAdapter</code>
<code>com.waveset.adapter.LinuxResourceAdapter.BlockAcctIter</code>	
<code>com.waveset.adapter.NDSActiveSyncAdapter</code>	<code>com.waveset.adapter.NDSResourceAdapter</code>
<code>com.waveset.adapter.PeopleSoftResourceAdapter</code>	

---

<b>Verworfen</b>	<b>Nachfolger</b>
com.waveset.adapter.RemedyActiveSyncResourceAdapter	com.waveset.adapter.RemedyResourceAdapter
com.waveset.adapter.ResourceAdapterBase.SimpleAccountIterator	Anstelle dieser Klasse sollte das Lieferantenmodell für die Konteniteration verwendet werden. Die Klasse ließe sich z. B. durch Folgendes direkt ersetzen: neue BufferedAccountQueue(neuer SimpleAccountSupplier(Konten));
com.waveset.adapter.SVIDResourceAdapter.BlockAccountIterator	Verweise auf diese Klasse sollten durch einen AccountIterator auf Grundlage des Lieferantenmodells ersetzt werden. Beispiel: BufferedAccountQueue(neuer SVIDAccountSupplier).
com.waveset.adapter.TopSecretActiveSyncAdapter	com.waveset.adapter.TopSecretResourceAdapter
com.waveset.exception.ConfigurationError	com.waveset.util.ConfigurationError
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.object.ViewMaster()	
com.waveset.object.ViewMaster.ViewMaster(String,String)	
com.waveset.object.ViewMaster.ViewMaster(Subject,String)	
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.CSVParser	com.waveset.util.ConfigurableDelimitedFileParser
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
com.waveset.util.PipeDelimitedParser	com.waveset.util.ConfigurableDelimitedFileParser

---

# Verworfenene Methoden und Felder

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

Die Daten in der Spalte **Nachfolger** können folgende Informationstypen 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()` aufgelistet.

wobei gilt:

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

## `com.waveset.adapter.AccessManagerResourceAdapter`

Verworfenene Methoden oder Felder	Nachfolger
<code>handlePDEException(Exception)</code>	<code>handlePDEException(PDEException)</code>

## `com.waveset.adapter.ACF2ResourceAdapter`

Verworfenene Methoden oder Felder	Nachfolger
<code>getAccountAttributes(String)</code>	

## com.waveset.adapter.ActiveSync

Verworfenne Methoden oder Felder	Nachfolger
RA_UPDATE_IF_DELETE	

## com.waveset.adapter.ActiveSyncUtil

Verworfenne Methoden oder Felder	Nachfolger
getLogFileFullPath()	

## 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 Methoden oder Felder	Nachfolger
getAccountAttributes(String)	

## com.waveset.adapter.AuthSSOResourceAdapter

Verworfenne Methoden oder Felder	Nachfolger
getAccountAttributes(String)	

## com.waveset.adapter.ClearTrustResourceAdapter

Verworfenne Methoden oder Felder	Nachfolger
getAccountAttributes(String)	

## com.waveset.adapter.DatabaseTableResourceAdapter

Verworfenne Methoden oder Felder	Nachfolger
RA_PROCESS_NAME	com.waveset.adapter.ActiveSync#RA_PROCESS_RULE

## com.waveset.adapter.DB2ResourceAdapter

Verworfenne Methoden oder Felder	Nachfolger
getAccountAttributes(String)	

## com.waveset.adapter.DominoResourceAdapter

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

## com.waveset.adapter.DominoResourceAdapterBase

Verworfenne Methoden oder Felder	Nachfolger
getAccountAttributes(String)	

## com.waveset.adapter.ExampleTableResourceAdapter

Verworfenne Methoden oder Felder	Nachfolger
getAccountAttributes(String)	

## com.waveset.adapter.GenericScriptResourceAdapter

Verworfenne Methoden oder Felder	Nachfolger
getAccountAttributes(String)	

## com.waveset.adapter.GetAccessResourceAdapter

Verworfenne Methoden oder Felder	Nachfolger
getAccountAttributes(String)	

## com.waveset.adapter.HostConnectionPool

Verworfenne Methoden oder Felder	Nachfolger
getConnection(HostAccessLogin)	com.waveset.adapter.HostConnPool#getAffinityConnection(HostAccessLogin)
releaseConnection(HostAccess)	com.waveset.adapter.HostConnPool#releaseConnection(HostAccess)
releaseConnection(IHostAccess)	com.waveset.adapter.HostConnPool#releaseConnection(IHostAccess)

## com.waveset.adapter.HostConnPool

Verworfenne Methoden oder Felder	Nachfolger
getConnection(HostAccessLogin)	getAffinityConnection(HostAccessLogin)
putFree()	
putFree(IHostAccess)	putAffinityFree

## com.waveset.adapter.iapi.IAPIFactory

Verworfenne Methoden oder Felder	Nachfolger
getAPIProcess(Map,Map,String,Resource)	getAPI(Map,Map,String,ResourceAdapterBase)
getAPIProcess(Element)	
getAPIUser(Element)	
getAPIUser(Map,Map,String,Map)	getAPI(Map,Map,String,ResourceAdapterBase)
getAPIUser(Map,Map,String,Resource)	getAPI(Map,Map,String,ResourceAdapterBase)

## com.waveset.adapter.IDMResourceAdapter

Verworfenne Methoden oder Felder	Nachfolger
getAccountAttributes(String)	

## com.waveset.adapter.INISafeNexessResourceAdapter

Verworfenne Methoden oder Felder	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)	
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 Methoden oder Felder	Nachfolger
getAccountAttributes(String)	

## com.waveset.adapter.NaturalResourceAdapter

Verworfenne Methoden oder Felder	Nachfolger
getAccountAttributes(String)	

## com.waveset.adapter.NDSResourceAdapter

Verworfenne Methoden oder Felder	Nachfolger
buildEvent(UpdateRow)	
getBaseContextAttrName()	com.waveset.adapter.ResourceAdapter#getBaseContexts()

## com.waveset.adapter.ONTDirectorySmartResourceAdapter

Verworfenne Methoden oder Felder	Nachfolger
getAccountAttributes(String)	

## com.waveset.adapter.OS400ResourceAdapter

Verworfenne Methoden oder Felder	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	

## com.waveset.adapter.RACFResourceAdapter

Verworfenne Methoden oder Felder	Nachfolger
getAccountAttributes(String)	

## com.waveset.adapter.RASecureConnection

Verworfenne Methoden oder Felder	Nachfolger
ExchangeAuth(boolean)	ExchangeAuth(boolean,byte[])

## com.waveset.adapter.RequestResourceAdapter

Verworfenne Methoden oder Felder	Nachfolger
getAccountAttributes(String)	

## com.waveset.adapter.ResourceAdapter

Verworfenne Methoden oder Felder	Nachfolger
getAccountAttributes(String)	
getBaseContextAttrName()	getBaseContexts()

## com.waveset.adapter.ResourceAdapterBase

Verworfenne Methoden oder Felder	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 Methoden oder Felder	Nachfolger
getAccountAttributes(String)	
getBaseContextAttrName()	getBaseContexts()

## com.waveset.adapter.ResourceManager

Verworfenne Methoden oder Felder	Nachfolger
getResourceTypes()	getResourcePrototypes() getResourcePrototypes(ObjectCache,boolean)
getResourceTypeStrings()	getResourcePrototypeNames(ObjectCache)

## com.waveset.adapter.SAPHRActiveSyncAdapter

Verworfenne Methoden oder Felder	Nachfolger
RA_PROCESS_NAME	com.waveset.adapter.ActiveSync#RA_PROCESS_RULE

## com.waveset.adapter.SAPResourceAdapter

Verworfenne Methoden oder Felder	Nachfolger
reverseMapMultiAttr(String, Object, WSUser)	
setUserField(JCO.Function, String)	Function#setUserField(String)
unexpirePassword(String, WavesetResult)	unexpirePassword(String, String,String,WavesetResult)
unexpirePassword(WSUser,WavesetResult)	unexpirePassword(String, String,String,WavesetResult)

## com.waveset.adapter.ScriptedConnection

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

## com.waveset.adapter.ScriptedHostResourceAdapter

Verworfenne Methoden oder Felder	Nachfolger
getAccountAttributes(String)	

## com.waveset.adapter.SkeletonResourceAdapter

Verworfenne Methoden oder Felder	Nachfolger
getAccountAttributes(String)	

## com.waveset.adapter.SMEResourceAdapter

Verworfenne Methoden oder Felder	Nachfolger
getAccountAttributes(String)	

## com.waveset.adapter.SQLServerResourceAdapter

Verworfenne Methoden oder Felder	Nachfolger
getAccountAttributes(String)	

## com.waveset.adapter.SunAccessManagerResourceAdapter

Verworfenne Methoden oder Felder	Nachfolger
getAccountAttributes(String)	
getBaseContextAttrName()	com.waveset.adapter.ResourceAdapter#getBaseContexts()

## com.waveset.adapter.SybaseResourceAdapter

Verworfenne Methoden oder Felder	Nachfolger
getAccountAttributes(String)	

## com.waveset.adapter.TestResourceAdapter

Verworfenne Methoden oder Felder	Nachfolger
getAccountAttributes(String)	

## com.waveset.adapter.TopSecretResourceAdapter

Verworfenne Methoden oder Felder	Nachfolger
hasError(String,String)	hasError(String,String,String)
login(HostAccess hostAccess)	login(HostAccess,ServerAffinity)
login(IHostAccess hostAccess)	#login(IHostAccess hostAccess, ServerAffinity affinity)

## com.waveset.adapter.VerityResourceAdapter

Verworfenne Methoden oder Felder	Nachfolger
getAccountAttributes(String)	

## com.waveset.adapter.XMLResourceAdapter

Verworfenne Methoden oder Felder	Nachfolger
getAccountAttributes(String)	

## com.waveset.msgcat.Catalog

Verworfenne Methoden oder Felder	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 Methoden oder Felder	Nachfolger
getUnowned()	hasOwner()
setUnowned(boolean)	setOwner(WSUser)

## com.waveset.object.AccountAttributeType

Verworfenne Methoden oder Felder	Nachfolger
getAttrType()	getSyntax()
setAttrType(String)	setSyntax(String)
	setSyntax(Syntax)

## 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 Methoden oder Felder	Nachfolger
AttributeDefinition(String,String)	AttributeDefinition(String,Syntax)
setAttrType(String)	setSyntax(Syntax)

## com.waveset.object.AuditEvent

Verworfenne Methoden oder Felder	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 Methoden oder Felder	Nachfolger
getAllObjects(Type,AttributeCondition[])	listObjects(Type,AttributeCondition[])
getAllObjects(Type,WSAttributes)	listObjects(Type,WSAttributes)
getAllObjects(Type)	listObjects(Type)

## com.waveset.object.Constants

Verworfenne Methoden oder Felder	Nachfolger
MAX_SUMMARY_STRING_LENGTH	

## 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 Methoden oder Felder	Nachfolger
toMap(boolean)	toMap(String,int)
toMap(String,boolean)	

## com.waveset.object.LoginConfig

Verworfenne Methoden oder Felder	Nachfolger
getApp(String)	getLoginApp(String)

## com.waveset.object.MessageUtil

---

Verworfenne Methoden oder Felder	Nachfolger
getActionDisplayKey(String)	
getEventParmDisplayKey(String)	
getResultDisplayKey(String)	
getTypeDisplayKey(String)	com.waveset.ui.FormUtil#getTypeDisplayName(LighthouseContext,String)

---

## com.waveset.object.RepositoryResult

---

Verworfenne Methoden oder Felder	Nachfolger
get(int)	
getId(int)	
getName(int)	
getObject(int)	
getRowCount()	
getRows()	
seek(int)	hasNext() next()
sort()	

---

## com.waveset.object.RepositoryResult.Row

---

Verworfenne Methoden oder Felder	Nachfolger
getSummaryAttributes()	getAttributes()

---

## com.waveset.object.ResourceAttribute

Verworfenne Methoden oder Felder	Nachfolger
setType(String)	setSyntax(Syntax)

## com.waveset.object.TaskInstance

Verworfenne Methoden oder Felder	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 Methoden oder Felder	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	
getSubtypes()	getLegacyTypes()
NOTIFY_CONFIG	

Verworfenne Methoden oder Felder	Nachfolger
REPORT_COUNTER	
SUMMARY_REPORT_TASK	
USAGE_REPORT	
USAGE_REPORT_TASK	

## com.waveset.object.UserUIConfig

Verworfenne Methoden oder Felder	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)	

## com.waveset.object.WSUser

Verworfenne Methoden oder Felder	Nachfolger
getApproverDelegate()	getWorkItemDelegate(String workItemTyp)
getDelegateHistory()	getWorkItemDelegateHistory()
setApproverDelegate(WsUser.Delegate)	addWorkItemDelegate(Delegate workItemDelegate)
setDelegateHistory(List)	etWorkItemDelegateHistory(List workItemDelegateHistory)

## com.waveset.session

Unterklasse	Verworfenne Methoden oder Felder	Nachfolger
LocalSession	getAdministrators(Map)	com.waveset.view.WorkItemUtil#getAdministrators
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 Methoden oder Felder	Nachfolger
getAccessPolicy()	
getRepository()	

## com.waveset.ui.util.FormUtil

Verworfenne Methoden oder Felder	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,String,List)	getObjectNames(LighthouseContext,String,Map)
getObjectNames(LighthouseContext,String,String,String,String,List,Map)	getObjectNames(LighthouseContext,String,Map)
getObjectNames(LighthouseContext,String,String,String,String,List)	getObjectNames(LighthouseContext,String,Map)
getObjectNames(LighthouseContext,String,String,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)
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)

<b>Verworfenne Methoden oder Felder</b>	<b>Nachfolger</b>
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)
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)
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 Methoden oder Felder	Nachfolger
installIfAvailable()	

## com.waveset.util.PdfReportRenderer

Verworfenne Methoden oder Felder	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 Methoden oder Felder	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 Methoden oder Felder	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)

Verworfenne Methoden oder Felder	Nachfolger
variable(long, Object, String, String, boolean)	com.sun.idm.logging.trace.Trace#variable(long, String, String, boolean)
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

Verworfenne 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)
getLocalHostName()	#getServerId() (Abrufen einer eindeutigen Server-ID)

## com.waveset.workflow.WorkflowContext

---

<b>Verworfenne Methoden oder Felder</b>	<b>Nachfolger</b>
VAR_CASE_TERMINATED	com.waveset.object.WFProcess#VAR_CASE_TERMINATED

---

---

<b>Verworfenne Methoden oder Felder</b>	<b>Nachfolger</b>
---	-------------------

---

getApproverDelegate()

setApproverDelegate()

getDelegateHistory()

setDelegateHistory()

---



# Erweiterungen und Korrekturen der Dokumentation

Dieser Abschnitt enthält neue Informationen und Korrekturen, die nach der Herausgabe der Identity Manager 7.1-Dokumentation bekannt wurden. Die Informationen sind wie folgt unterteilt:

- [Identity Manager Installation](#)
- [Identity Manager Upgrade](#)
- [Identity Manager Administration](#)
- [Identity Manager Resources Reference](#)
- [Identity Manager Technical Deployment Overview](#)
- [Identity Manager Workflows, Forms, and Views](#)
- [Identity Manager Deployment Tools](#)
- [Identity Manager Tuning, Troubleshooting, and Error Messages](#)
- [Identity Manager Service Provider Edition Deployment](#)
- [helpTool verwenden](#)

---

## *Identity Manager Installation*

Dieser Abschnitt enthält neue Informationen und Dokumentationskorrekturen in Bezug auf *Sun Java™ System Identity Manager Installation*.

- Der Exchange 5.5-Ressourcenadapter wird nicht unterstützt. Ignorieren Sie bitte alle Verweise auf diesen Adapter.

---

# Identity Manager Upgrade

Dieser Abschnitt enthält neue Informationen und Dokumentationskorrekturen für *Sun Java™ System Identity Manager Upgrade*.

- Vor der Aufrüstung müssen das Verzeichnis, in dem Identity Manager installiert ist, und die Datenbank, die von Identity Manager verwendet wird, gesichert werden. Zum Sichern des Identity Manager-Dateisystems können Sie Sicherungssoftware eines Drittanbieters oder ein mit Ihrem System geliefertes Sicherungsdienstprogramm verwenden. Die empfohlenen Sicherungsmethoden für die Datenbank schlagen Sie bitte in der Dokumentation zur Datenbank nach. (ID-2810)

Zum Erstellen von Sicherungskopien müssen Sie zunächst Identity Manager herunterfahren (in den Leerlauf schalten). Sichern Sie dann die Datenbank und das Dateisystem, in dem Identity Manager installiert ist, mit den jeweiligen Sicherungsdienstprogrammen.

- Die AD ActiveSync-Ressource wurde verworfen und durch die AD-Ressource ersetzt. Führen Sie folgende Schritte aus, um zu AD ActiveSync für neuere Versionen zu migrieren: (ID-11363)
  - Exportieren Sie das vorhandene AD ActiveSync-Ressourcenobjekt in eine XML-Datei (über die Befehlszeile oder auf den Debug-Seiten).
  - Löschen Sie die vorhandene Ressource. (Von diesem Vorgang sind keine Benutzer von Identity Manager oder des Ressourcenkontos betroffen.)
  - Erstellen Sie eine neue AD-Ressource als ActiveSync-Ressource.
  - Exportieren Sie dieses neue Ressourcenobjekt in eine XML-Datei.
  - Setzen Sie in dieser Datei die Werte für das id-Attribut und das name-Attribut auf die Werte des ALTEN Ressourcenobjekts, das in Schritt 1 gespeichert wurde. Diese Attribute befinden sich im Tag `<Resource id='ID-Nummer' name='AD' ...>`.
  - Speichern Sie die Änderungen in der Datei.
  - Importieren Sie das geänderte Objekt zurück in Identity Manager. Verwenden Sie hierzu die Seite Konfigurieren->Exchange-Datei importieren oder die Befehlszeile.
- Der Abschnitt „Other Custom Repository Objects“ enthält jetzt Anweisungen zur SnapShot-Funktion von Identity Manager, mit der sich ein Snapshot (eine Momentaufnahme) der benutzerdefinierten Repository-Objekte in einer Bereitstellungsumgebung erstellen lässt. (ID-14840)

### *Weitere benutzerdefinierte Repository-Objekte*

Notieren Sie die Namen aller weiteren benutzerdefinierten Repository-Objekte, die Sie erstellt oder aktualisiert haben. Sie können diese Objekte aus der aktuellen Installation exportieren und nach der Aufrüstung in der neuen Identity Manager-Version importieren.

- Admin-Gruppe
- Admin-Rolle
- Konfiguration
- Richtlinie
- Bereitstellungsaufgabe
- Remedy-Konfiguration
- Ressourcenformular
- Ressourcenformular
- Rolle
- Regel
- Aufgabendefinition
- Aufgabenvorlage
- Benutzerformular

Mit der SnapShot-Funktion von Identity Manager können Sie einen Snapshot (eine Momentaufnahme) der benutzerdefinierten Repository-Objekte in Ihrer Bereitstellungsumgebung erstellen. Dies kann beim Planen einer Aufrüstung sehr nützlich sein.

SnapShot kopiert zum Vergleich die folgenden Objekttypen des jeweiligen Systems:

- AdminGroup
- AdminRole
- Configuration
- EmailTemplate
- Policy
- ProvisionTask
- RemedyConfig
- ResourceAction

- Resourceform
- Role
- Rule
- TaskDefinition
- TaskTemplate
- UserForm

Danach können Sie durch einen Vergleich von zwei Snapshots vor und nach einer Aufrüstung ermitteln, welche Änderungen an bestimmten Systemobjekten vorgenommen wurden.

---

**HINWEIS** Diese Funktion gibt keinen detaillierten Aufschluss über fortlaufende XML-Unterschiede, sondern liefert einen Kurzbericht für einen ersten Vergleich.

---

So erstellen Sie einen Snapshot:

1. Klicken Sie auf der Debug-Seite in Identity Manager ([Abbildung 1](#)) auf die Schaltfläche „SnapShot“, um die SnapShot-Verwaltungsseite aufzurufen.

**Abbildung 1** SnapShot-Verwaltungsseite

### SnapShot-Verwaltung

Auf dieser Seite können Sie Momentaufnahmen der Systemkonfiguration (Snapshots) verwalten. Dabei werden bestimmte Objekttypen des Systems zu Vergleichszwecken kopiert. Anhand eines Vergleichs lässt sich dann ermitteln, welche Änderungen zwischen den Snapshots vorgenommen wurden. So erhalten Sie einen Überblick über Änderungen an Objekten, was die Planung einer Aufrüstung erleichtert.

The screenshot shows a control panel for snapshot management. It includes a text input field next to an 'Erstellen' button. Below this are 'Löschen' and 'Vergleich' buttons, each with a dropdown arrow. Underneath the 'Vergleich' button is an 'Exportieren' label. At the bottom is an 'Abbrechen' button.

2. Geben Sie in das Textfeld „Erstellen“ einen Namen für den Snapshot ein und klicken Sie auf die Schaltfläche „Erstellen“.

Identity Manager fügt den Snapshot hinzu. Der Name wird in der Menüliste „Vergleich“ und rechts neben „Exportieren“ angezeigt.

So vergleichen Sie zwei Snapshots:

1. Wählen Sie in jedem Menü „Vergleich“ einen Snapshot aus ([Abbildung 2](#)).

**Abbildung 2** SnapShot-Verwaltungsseite



2. Klicken Sie auf die Schaltfläche „Vergleich“.
  - Liegen keine Objektänderungen vor, zeigt die Seite an, dass keine Unterschiede gefunden wurden.
  - Wurden Objektänderungen erkannt, zeigt die Seite den Objekttyp und -namen an und ob ein Objekt anders, vorhanden oder nicht vorhanden ist.

Wenn ein Objekt z. B. in Momentaufnahme\_1, nicht aber in Momentaufnahme\_2 enthalten ist, wird in der Spalte „Momentaufnahme\_1“ Present und in der Spalte „Momentaufnahme\_2“ Absent angezeigt.

Ein Snapshot kann im XML-Format exportiert werden. Klicken Sie auf den Namen des Snapshots, um ihn in eine Datei zu exportieren.

Um einen Snapshot zu löschen, wählen Sie ihn im Menü „Löschen“ aus und klicken auf die Schaltfläche „Löschen“.

- Der folgende Absatz ergänzt den Abschnitt „Modified JSPs“ mit Informationen zum Befehl `inventory -m`. Mit diesem Befehl lassen sich modifizierte JSPs in einer Bereitstellungsumgebung identifizieren: (ID-14840)

Mit dem Befehl `inventory -m` (siehe Erläuterungen weiter oben) können Sie alle in der jeweiligen Bereitstellungsumgebung vorgenommenen JSP-Modifikationen identifizieren.

- Wenn Sie von einer 6.x-Installation auf Version 7.0 oder 7.1 aufrüsten und die neuen Identity Manager-Endbenutzerseiten verwenden möchten, müssen Sie in der Systemkonfiguration `ui.web.user.showMenu` manuell auf **true** einstellen, damit die horizontale Navigationsleiste angezeigt wird. (ID-14901)
- Wenn Sie von 6.0 oder 7.0 auf Version 7.1 aufrüsten und `LocalFiles` verwenden, müssen Sie vor der Aufrüstung alle Ihre Daten exportieren und dann nach der Neuinstallation von 7.1 wieder importieren. (ID-15366)

- Bei der Aufrüstung von Version 6.0 oder 7.0 auf Version 7.1 muss das Datenbankschema aufgerüstet werden. (ID-15392)
  - Bei der Aufrüstung von 6.0 auf 7.1 müssen Sie das `upgradeto71.*`-Skript für den jeweils verwendeten RDBMS-Typ ausführen.
  - Bei der Aufrüstung von 7.0 auf 7.1 müssen Sie das `upgradeto71from70.*`-Skript für den jeweils verwendeten RDBMS-Typ ausführen.
- Während der Aufrüstung analysiert Identity Manager alle Rollen im System und aktualisiert alle fehlenden Verknüpfungen zwischen untergeordneten und übergeordneten Rollen mithilfe der Klasse `RoleUpdater`. (ID-15734)

Rollen können auch unabhängig von der Aufrüstung überprüft und aktualisiert werden. Importieren Sie dazu das neue Konfigurationsobjekt `RoleUpdater`. Es befindet sich in `sample/forms/RoleUpdater.xml`. Zum Beispiel:

```
<?xml version='1.0' encoding='UTF-8'?>
<!DOCTYPE Waveset PUBLIC 'waveset.dtd' 'waveset.dtd'>
<Waveset>
  <ImportCommand class='com.waveset.session.RoleUpdater' >
    <Map>
      <MapEntry key='verbose' value='true' />
      <MapEntry key='noupdate' value='false' />
      <MapEntry key='nofixsubrolelinks' value='false' />
    </Map>
  </ImportCommand>
</Waveset>
```

Hierbei gilt Folgendes:

- **verbose**: Beim Aktualisieren von Rollen erfolgt eine ausführliche Ausgabe. Geben Sie **false** an, wenn die Aktualisierung von Rollen ohne Ausgabe erfolgen soll.
- **noupdate**: Hiermit legen Sie fest, ob die Rollen aktualisiert werden. Geben Sie **false** an, um eine reine Auflistung der Rollen zu erzeugen, die gegebenenfalls aktualisiert werden.
- **nofixsubrolelinks**: Hiermit legen Sie fest, ob bei übergeordneten Rollen fehlende Verknüpfungen mit untergeordneten Rollen wiederhergestellt werden. Standardmäßig ist hier „false“ eingestellt und die Verknüpfungen werden repariert.

- Wenn der Pfad zum Identity Manager-Installationsverzeichnis ein Leerzeichen enthält, müssen Sie die Umgebungsvariable `WSHOME` ohne Anführungszeichen angeben ("), wie im folgenden Beispiel gezeigt (ID-15470):

---

**HINWEIS** Nachstehende Schrägstriche (\) dürfen bei der Pfadangabe auch dann nicht verwendet werden, wenn der Pfad keine Leerzeichen enthält.

---

```
set WSHOME=c:\Program Files\Apache Group\Tomcat 4.1\idm
```

oder

```
set WSHOME=c:\Progra~1\Apache~1\Tomcat~1\idm
```

Die folgende Pfadangabe ist ungültig:

```
set WSHOME="c:\Program Files\Apache Group\Tomcat 4.1\idm"
```

---

# Identity Manager Administration

Dieser Abschnitt enthält neue Informationen und Dokumentationskorrekturen für *Sun Java™ System Identity Manager Administration*.

## Kapitel 3, „User and Account Management“

- Die folgende Korrektur bezieht sich auf den Hinweis im Abschnitt „Disable Users (User Actions, Organization Actions)“:

---

**HINWEIS** Wenn bei einer zugewiesenen Ressource das Deaktivieren von Konten nicht, das Ändern von Passwörtern dagegen unterstützt wird, können Sie Identity Manager so konfigurieren, dass sich Benutzerkonten auf dieser Ressource durch das Zuweisen neuer, willkürlich generierter Passwörter deaktivieren lassen. Dazu müssen Sie auf der Seite „Identity System-Parameter“ im Ressourcen-Assistenten die Kontofunktionen „Deaktivieren“ und „Passwort“ für die Ressource aktivieren. Weitere Informationen finden Sie in Kapitel 4, „Configuration“.

---

- Die folgende Ergänzung bezieht sich auf den Hinweis im Abschnitt „Enable Users (User Actions, Organization Actions)“:

---

**HINWEIS** Wenn bei einer zugewiesenen Ressource das Aktivieren von Konten nicht, das Ändern von Passwörtern dagegen unterstützt wird, können Sie Identity Manager so konfigurieren, dass sich Benutzerkonten auf dieser Ressource durch das Zurücksetzen von Passwörtern aktivieren lassen. Dazu müssen Sie auf der Seite „Identity System-Parameter“ im Ressourcen-Assistenten die Kontofunktionen „Aktivieren“ und „Passwort“ für die Ressource aktivieren. Weitere Informationen finden Sie in Kapitel 4, „Configuration“.

---

## Kapitel 5, „Administration“

- Der folgende Hinweis ergänzt den Abschnitt „Delegating Work Items“.

---

**HINWEIS** Wenn Sie Delegierungen eingerichtet haben, werden alle Arbeitselemente, die während des geltenden Delegierungszeitraums erstellt wurden, Ihrer Liste und der Liste des Delegierten hinzugefügt. Beim Beenden der Delegierung werden die delegierten Arbeitselemente wiederhergestellt. Dies kann dazu führen, dass einige Arbeitselemente doppelt vorhanden sind. Wenn Sie ein Arbeitselement genehmigen oder zurückweisen, wird das doppelt vorhandene Element automatisch aus Ihrer Liste entfernt.

---

- Die folgenden Informationen ergänzen den Abschnitt „Managing Work Items“.

### *Delegierungen an gelöschte Benutzer*

Wenn Sie ein Arbeitselement an einen Benutzer delegieren, der zu einem späteren Zeitpunkt aus Identity Manager gelöscht wird, so wird der gelöschte Benutzer in der Liste „Aktuelle Delegierungen“ in Klammern angezeigt. Wenn Sie anschließend eine Delegierung erstellen oder bearbeiten, die den gelöschten Benutzer umfasst, so schlägt diese Aktion fehl. Darüber hinaus führt jedes von einem Benutzer erstellte oder aktualisierte Arbeitselement, das an einen gelöschten Benutzer delegiert wird, zu einem Fehler.

Arbeitselemente, die an einen gelöschten Benutzer delegiert wurden, können Sie durch Beenden der Delegierung wiederherstellen.

- Die Tabelle „Identity Manager Capabilities Descriptions“ ist um die Fähigkeit „Endbenutzer-Administrator“ zu ergänzen. Benutzer, denen diese Fähigkeit zugewiesen wurde, können die Rechte an Objekttypen, die in der Endbenutzerfähigkeit angegeben sind, und die Inhalte der Endbenutzerregel für kontrollierte Organisationen anzeigen und bearbeiten. Diese Fähigkeit wird standardmäßig dem Konfigurator zugewiesen.

## Kapitel 11, „Identity Auditing“

Dieses Kapitel wurde um die folgenden neuen Informationen ergänzt:

### *Umgehen der Einschränkungen von Auditor-Fähigkeiten*

Standardmäßig sind die für Überwachungsaufgaben erforderlichen Fähigkeiten in der Organisation auf der höchsten Ebene („Top“) (Objektgruppe) enthalten. Daher können nur Administratoren, die das oberste Element („Top“) steuern, diese Fähigkeiten anderen Administratoren zuweisen.

Diese Einschränkung können Sie umgehen, indem Sie die Fähigkeiten zu einer anderen Organisation hinzufügen. In Identity Manager stehen im Verzeichnis `sample/scripts` zwei Dienstprogramme für diese Aufgabe zur Verfügung.

1. Führen Sie den folgenden Befehl aus, um alle Fähigkeiten (Admin-Gruppen) und die zugehörigen Organisationen (Objektgruppen) aufzulisten:

```
beanshell objectGroupUpdate.bsh -type AdminGroup -action list -csv
```

Die Ausgabe wird in eine CSV-Datei (durch Kommas getrennte Werte) geschrieben.

2. Bearbeiten Sie die CSV-Datei und verschieben Sie die Fähigkeiten nach Bedarf zwischen den Organisationen.
3. Aktualisieren Sie Identity Manager mit dem folgenden Befehl.

```
beanshell objectGroupUpdate.bsh -data CSVFileName -action add -groups NewObjectGroup
```

## Kapitel 13, „Service Provider Administrator“

Im Abschnitt „Configure Synchronization“ sollte als Standardsynchronisationsintervall für Service Provider Edition-Synchronisationsaufgaben 1 Minute angegeben sein.

# Identity Manager Resources Reference

Dieser Abschnitt enthält neue Informationen und Dokumentationskorrekturen für *Sun Java™ System Identity Manager Resources Reference*:

- Der Exchange 5.5-Ressourcenadapter wird nicht unterstützt. Ignorieren Sie bitte alle Verweise auf diesen Adapter.
- In der Dokumentation zum Datenbanktabellen-Adapter ist das Beispiel für „Last Fetched Predicate“ ungültig. Die Definition muss folgendermaßen lauten:  

```
lastMod > '$(lastmod)'
```
- Beim Flat File ActiveSync-Adapter wird das Einstellen der Eigenschaft „sources.hosts“ in der Datei „Waveset.properties“ erläutert. Für diese Konfiguration sollte jetzt die Synchronisationsrichtlinie verwendet werden.
- Die Unterstützung von GroupWise durch den NDS-Adapter wurde verbessert:
  - Der Adapter ermöglicht jetzt das Verwalten von Post Offices in sekundären Domänen.
  - GroupWise-Benutzer können jede bekannte Verteilungsliste abonnieren.
  - Beim Löschen eines Post Office ist es nicht mehr erforderlich, ein „Löschmuster“ (Delete Pattern) anzugeben.
- Unter „Managing ACL List“ ist der folgende Schritt aufgeführt: (ID-16476)  
3. Edit the user in Identity Manager and on the Edit User form.  
Richtig lautet die Anweisung folgendermaßen:  
3. Edit the user in Identity Manager on the Edit User form.

---

# Identity Manager Technical Deployment Overview

Dieser Abschnitt enthält neue Informationen und Dokumentationskorrekturen für *Sun Java™ System Identity Manager Technical Deployment Overview*:

- Mit Hilfe der zentralen Struktureinheit (CSS) können Sie die Spaltenbreite in der Benutzer- und Ressourcenliste auf einen festen Pixelwert oder einen Prozentsatz einstellen. Fügen Sie `customStyle.css` dazu die folgenden Stilklassen (standardmäßig ausgewiesen) hinzu. Die Werte können dann an die Anforderungen des Benutzers angepasst werden.

```
th#UserListTreeContent_Col0 {
    width: 1px;
}

th#UserListTreeContent_Col0 {
    width: 1px;
}

th#UserListTreeContent_Col0 {
    width: 50%;
}

th#UserListTreeContent_Col3 {
    width: 50%;
}

th#ResourceListTreeContent_Col0 {
    width: 1px;
}

th#ResourceListTreeContent_Col1 {
    width: 1px;
}

th#ResourceListTreeContent_Col2 {
    width: 33%;
}

th#ResourceListTreeContent_Col3 {
    width: 33%;
}

th#ResourceListTreeContent_Col4 {
    width: 33%;
}
```

Sie können auch die Größe der Spalten ändern, indem Sie den rechten Rand der Spaltenüberschrift mit der Maus ziehen. Wenn Sie die Maus über den rechten Rand der Spaltenüberschrift ziehen, ändert sich der Cursor in einen horizontalen Pfeil für Größenänderungen. Durch Klicken mit der linken Maustaste und Ziehen des Cursors wird die Größe der Spalte geändert. (Die Größenänderung wird beim Loslassen der Maustaste beendet.)

- Das SystemConfiguration-Objekt enthält dann das Attribut `security.delegation.historyLength`, mit dem die Anzahl der zuvor gespeicherten Delegierungen gesteuert wird.
- Die Instanzen der Prüfungen, die in den Überwachungsprotokollen aufgezeichnet wurden, sind sowohl im Bedienfeld „Zugriffsprüfung“ als auch im Bericht über Zugriffsprüfungsdetails aufgeführt. Ohne Datenbankwartung werden die Überwachungsprotokolle nicht gekürzt und die Liste der Prüfungen wird immer größer. Identity Manager bietet die Möglichkeit, nur Prüfungen aus einem bestimmten Zeitraum anzeigen zu lassen. Um diese Grenze zu ändern, müssen Sie `compliance/dashboard.jsp` (für das Bedienfeld) und `sample/auditortasks.xml` (für den Detailbericht) entsprechend anpassen. (Standardmäßig werden nur Prüfungen angezeigt, die weniger als 2 Jahre alt sind.)

Um die Prüfungen zu beschränken, die im Bedienfeld Zugriffsprüfung enthalten sind, passen Sie `compliance/dashboard.jsp` wie folgt an:

- a. Öffnen Sie entweder in der Identity Manager IDE oder einem Editor Ihrer Wahl die Datei `compliance/dashboard.jsp`:
- b. Ändern Sie die Zeile `form.setOption("maxAge", "2y");` auf `form.setOption("maxAge", "6M");`, um die Liste auf Prüfungen zu beschränken, die in den letzten 6 Monaten durchgeführt wurden. Folgende Kennzeichner werden verwendet:
  - m - Minute
  - h - Stunde
  - d - Tag
  - w - Woche
  - M - Monat
  - y - Jahr

Um alle Prüfungen anzuzeigen, die noch in den Überwachungsprotokollen enthalten sind, kommentieren Sie diese Zeile aus:

Um die Prüfungen im Bericht über Zugriffsprüfungsdetails zu beschränken, gehen Sie wie folgt vor:

- a. Öffnen Sie entweder in der integrierten Entwicklungsumgebung (IDE) oder einem Editor Ihrer Wahl `sample/auditortasks.xml`.
- b. Ändern Sie die folgende Zeile wie angegeben:

```
<s>maxAge</s>
<s>2y</s>
```

nach

```
<s>maxAge</s>
<s>6M</s>
```

Dadurch werden die Prüfungen auf die letzten 6 Monate beschränkt. Es werden die oben beschriebenen Kennzeichner verwendet.

Jede regelmäßige Zugriffsprüfung enthält eine Reihe von UserEntitlement-Datensätzen, die bei der Ausführung der Prüfung erstellt wurden. Diese Datensätze, die über die Zeit angesammelt wurden, enthalten wertvolle historische Informationen über die Konten. Um den verfügbaren Datenbankspeicherplatz möglichst effizient zu verwalten, sollten einige Datensätze u. U. gelöscht werden. Sie können einen Datensatz löschen, indem Sie **Serveraufgaben > Aufgaben ausführen > Zugriffsprüfung löschen** ausführen. Durch das Löschen einer Prüfung werden dem Überwachungsprotokoll neue Einträge hinzugefügt, die angeben, dass die Prüfung gelöscht wurde. Zudem werden alle mit der Prüfung verbundenen UserEntitlement-Datensätze gelöscht, wodurch Datenbankspeicherplatz freigegeben wird.

- Im Abschnitt „Changing Background Image on the Login Page“ muss die dritte Codezeile wie folgt lauten:

```
url(../images/other/login-backimage2.jpg)
```

- Codebeispiel 5-5 enthält Informationen, die in Codebeispiel 5-4 enthalten sein sollten: Codebeispiel 5-4 sollte wie folgt aussehen:

#### Codebeispiel 5-4 Registerkarten zum Anpassen der Navigation

```
/* LEVEL 1 TABS */
.TabLv11Div {
    background-image:url(../images/other/dot.gif);
    background-repeat:repeat-x;
    background-position:left bottom;
    background-color:#333366;
    padding:6px 10px 0px;
}
a.TabLv11Lnk:link, a.TabLv11Lnk:visited {
    display:block;
```

**Codebeispiel 5-4** Registerkarten zum Anpassen der Navigation (*Fortsetzung*)

```

padding:4px 10px 3px;
font: bold 0.95em sans-serif;
color:#FFF;
text-decoration:none;
text-align:center;
}
table.TabLvl1Tbl td {
background-image:url(..images/other/dot.gif);
background-repeat:repeat-x;
background-position:left top;
background-color:#666699;
border:solid 1px #abab5;
}
table.TabLvl1Tbl td.TabLvl1TblSelTd {
background-color:#9999CC;
background-image:url(..images/other/dot.gif);
background-repeat:repeat-x;
background-position:left bottom;
border-bottom:none;
}

/* LEVEL 2 TABS */
.TabLvl2Div {
background-image:url(..images/other/dot.gif);
background-repeat:repeat-x;
background-position:left bottom;
background-color:#9999CC;
padding:6px 0px 0px 10px
}
a.TabLvl2Lnk:link, a.TabLvl2Lnk:visited{
display:block;
padding:3px 6px 2px;
font: 0.8em sans-serif;
color:#333;
text-decoration:none;
text-align:center;
}
table.TabLvl2Tbl div.TabLvl2SelTxt {
display:block;
padding:3px 6px 2px;
font: 0.8em sans-serif;
color:#333;
font-weight:normal;
text-align:center;
}
table.TabLvl2Tbl td {
background-image:url(..images/other/dot.gif);
background-repeat:repeat-x;
background-position:left top;
background-color:#CCCCFF;
border:solid 1px #abab5;
}
table.TabLvl2Tbl td.TabLvl2TblSelTd {
border-bottom:none;
background-image:url(..images/other/dot.gif);

```

**Codebeispiel 5-4** Registerkarten zum Anpassen der Navigation (*Fortsetzung*)

```
background-repeat:repeat-x;
background-position:left bottom;
background-color:#FFF;
border-left:solid 1px #aba1b5;
border-right:solid 1px #aba1b5;
border-top:solid 1px #aba1b5;
```

Codebeispiel 5.5 sollte wie folgt aussehen:

**Codebeispiel 5-5** Ändern von Registerkarten

```
table.Tab2TblNew td
{background-image:url(..images/other/dot.gif);background-repeat:repeat-x;background-positi
on:left top;background-color:#CCCCFF;border:solid 1px #8f989f}
table.Tab2TblNew td.Tab2TblSelTd
{border-bottom:none;background-image:url(..images/other/dot.gif);background-repeat:repeat-
x;background-position:left bottom;background-color:#FFF;border-left:solid 1px
#8f989f;border-right:solid 1px #8f989f;border-top:solid 1px #8f989f}
```

- Die horizontale Navigationsleiste im Identity Manager-Endbenutzer-Interface wird vom Benutzerformular für die Endbenutzer-Navigation in `enduser.xml` gesteuert. (ID-12415) `userHeader.jsp`, das in allen Endbenutzerseiten enthalten ist, beinhaltet ein anderes JSP mit der Bezeichnung `menuStart.jsp`. Dieses JSP greift auf zwei Systemkonfigurationsobjekte zu:
  - `ui.web.user.showMenu`: Blendet das Navigationsmenü ein oder aus (Standard: `true`)
  - `ui.web.user.menuLayout`: Legt fest, ob das Menü als horizontale Navigationsleiste mit Registerkarten (Standard: `horizontal`) oder als vertikales Strukturmenü (`vertical`) dargestellt wird.

Die CSS-Stilklassen, die bestimmen, wie das Menü dargestellt werden soll, befinden sich in `style.css`.

- In Identity Manager wird das **Lighthouse**-Konto nun als **Identity Manager**-Konto bezeichnet. Sie können diese Namensänderung mit Hilfe eines benutzerdefinierten Katalogs aussetzen. (ID-14918) Weitere Informationen zu benutzerdefinierten Katalogen finden Sie unter *Aktivieren der Lokalisierung in Identity Manager Technical Deployment Overview*.

Die Anzeige des Produktnamens wird durch die folgenden Katalogeinträge gesteuert:

PRODUCT\_NAME=Identity Manager

LIGHTHOUSE\_DISPLAY\_NAME=[PRODUCT\_NAME]

LIGHTHOUSE\_TYPE\_DISPLAY\_NAME=[PRODUCT\_NAME]

LIGHTHOUSE\_DEFAULT\_POLICY=Default [PRODUCT\_NAME] Account Policy

- Identity Manager umfasst nun ein neues Konfigurationsobjekt (Konfigurationsobjekt `workItemTypes`), das alle Namen, Erweiterungen und Anzeigenamen von unterstützten Arbeitselementtypen angibt. (ID-15468) Dieses Konfigurationselement ist in `sample/workItemTypes.xml` definiert, die von `init.xml` und `update.xml` importiert wird.

Das Attribut `extends` ermöglicht eine Hierarchie von Arbeitselementtypen (`workItem`-Typen). Bei der Erstellung eines Arbeitselements delegiert Identity Manager das Arbeitselement an den angegebenen Benutzer, wenn der zugehörige `workItem`-Typ:

- der delegierte Typ ist
- einer der untergeordneten `workItem`-Typen des delegierten Typs ist

<b>workItem-Typ</b>	<b>Beschreibung</b>	<b>Anzeigename</b>
Approval	erweitert WorkItem	Approval
OrganizationApproval	erweitert Approval	Organisationsgenehmigung
ResourceApproval	erweitert Approval	Ressourcengenehmigungen
RoleApproval	erweitert Approval	Rollengenehmigungen
Attestation	WorkItem	Bescheinigung der Zugriffsprüfung
Prüfung	WorkItem	Remediation
accessReviewRemediation	WorkItem	Zugriff

- Im Rahmen der anonymen Registrierung von Identity Manager werden für `accountId` und `emailAddress` generiert. Dies geschieht auf der Grundlage von Vor- (`firstName`) und Nachname (`lastName`) sowie `employeeId`, die allesamt vom Benutzer angegeben wurden. (ID-16131)

Da bei der anonymen Registrierung Nicht-ASCII-Zeichen in E-Mail-Adressen und Konto-IDs vorkommen können, sollten internationale Benutzer `EndUserRuleLibrary`-Regeln dahingehend ändern, dass Identity Manager Konto-IDs und E-Mail-Adressen bei der anonymen Registrierung im ASCII-Format hält.

Um die Werte für Konto-ID und E-Mail-Adresse bei der anonymen Registrierung im ASCII-Format zu halten, führen Sie die folgenden beiden Schritte durch:

1. Bearbeiten Sie die folgenden drei Regeln in `EndUserRuleLibrary` wie unten angegeben:

Bearbeiten	um diese Änderung zu erreichen...
<code>getAccountId</code>	Es wird nur <code>employeeId</code> verwendet ( <code>firstName</code> und <code>lastName</code> werden entfernt).
<code>getEmailAddress</code>	Es wird nur <code>employeeId</code> verwendet ( <code>firstName</code> , <code>lastName</code> und "." werden entfernt).
<code>verifyFirstname</code>	Die Längenprüfung wird von 2 auf 1 geändert, um Kompatibilität mit asiatischen Vornamen aus nur einem Zeichen zu erhalten.

2. Bearbeiten Sie das Formular `End User Anon Enrollment Completion`, um die Argumente `firstName` und `lastName` von Aufrufen der Regeln `getAccountId` und `getEmailAddress` zu entfernen.

---

# Identity Manager Workflows, Forms, and Views

Dieser Abschnitt enthält neue Informationen und Dokumentationskorrekturen für *Sun Java™ System Identity Manager Workflows, Forms, and Views*.

- Sie können die Richtlinienprüfung in Ihrem Benutzerformular deaktivieren, indem Sie dem Formular das folgende Feld hinzufügen:

```
<Field name='viewOptions.CallViewValidators'>
  <Display class='Hidden' />
  <Expansion>
    <s>false</s>
  </Expansion>
</Field>
```

Dieses Feld überschreibt den Wert im Feld `OP_CALL_VIEW_VALIDATORS` von `modify.jsp`.

- Die Seiten der Identity Manager-Benutzeroberfläche umfassen ein zweites XPRESS-Formular zur Implementierung der Navigationsleiste. Die dargestellte Seite enthält daher zwei `<FORM>`-Tags mit jeweils unterschiedlichen Namensattributen:

```
<form name="endUserNavigation"> und <form name="mainform">
```

Um mögliche Verwechslungen dieser beiden `<FORM>`-Elemente zu vermeiden, verwenden Sie das Attribut `name` wie folgt, damit deutlich wird, auf welches `<FORM>`-Element Bezug genommen wird: `document.mainform` oder `document.endUserNavigation`.

## Kapitel 2, „Identity Manager Workflow“

- Identity Manager bietet unter `/sample/workflows` den folgenden neuen Beispielarbeitsablauf für die Zugriffsprüfung. (ID-15393)

### Testen der automatischen Bescheinigung

Ermöglicht das Testen neuer Regeln für die Prüfungsbestimmung, ohne dafür Bescheinigungs-Arbeitselemente erstellen zu müssen. Dieser Arbeitsablauf erstellt keine Arbeitselemente und wird kurz nach dem Start beendet. Alle Benutzeranspruchs-Objekte werden in dem Zustand belassen, den sie bei der Erstellung durch die Zugriffsabfrage hatten. Verwenden Sie die Optionen Beenden und Löschen, um die in diesem Arbeitsablauf erhaltenen Ergebnisse der Zugriffsabfragen zu entfernen.

Sie können diesen Dummyarbeitsablauf nach Bedarf importieren. (Er wird nicht automatisch von Identity Manager importiert.)

- Identity Manager-Konformität setzt Arbeitsabläufe als Integrations- und Anpassungspunkte für die Anwendung ein. Die standardmäßigen konformitätsspezifischen Arbeitsabläufe sind im Folgenden beschrieben. (ID-15447)

<b>Arbeitsablauf-Name</b>	<b>Zweck</b>
Remediation	Korrektur für eine einzelne Korrekturfunktion, die mit einer einzelnen Konformitätsverletzung arbeitet
Access Review Remediation	Korrektur für eine einzelne Korrekturfunktion, die mit einer einzelnen UserEntitlement arbeitet
Attestation	Korrektur für eine einzelne Korrekturfunktion, die mit einer einzelnen UserEntitlement arbeitet
Multi Remediation	Korrektur für eine einzelne Konformitätsverletzung und mehrere Korrekturfunktionen
Update Compliance Violation	Mindert eine Konformitätsverletzung
Launch Access Scan	Startet eine Zugriffsabfrageaufgabe von einer Zugriffsprüfungsaufgabe
Launch Entitlement Rescan	Startet eine erneute Zugriffsabfrage für einen einzelnen Benutzer
Launch Violation Rescan	Startet eine erneute Überwachungsrichtliniensuche für einen einzelnen Benutzer

- Die Beschreibung der maxSteps-Eigenschaft wurde wie folgt überarbeitet: (ID-15618)

Gibt die maximale Anzahl der Schritte an, die in einem Arbeitsablaufvorgang oder untergeordneten Arbeitsablaufvorgang zulässig sind. Bei Überschreitung dieses Wertes wird der Arbeitsablauf von Identity Manager beendet. Diese Einstellung dient als Sicherheitsmaßnahme bei der Erkennung, ob sich ein Arbeitsablauf in einer Endlosschleife befindet. Der im Arbeitsablauf selbst festgelegte Standardwert beträgt 0 und gibt an, dass Identity Manager den tatsächlichen Wert von der globalen Einstellung abrufen muss, die im Attribut `workflow.maxSteps` des SystemConfiguration-Objekts gespeichert ist. Der Wert dieser globalen Einstellung beträgt 5000.

- Dieses Kapitel enthält nun die folgende Beschreibung der Aufgabe Scripted Task Executor. (ID-15258)

Führt auf der Grundlage des zur Verfügung gestellten Skripts Beanshell oder JavaScript aus. Dies kann als Aufgabe regelmäßig ausgeführt werden. Sie können diese Aufgabe z. B. im Rahmen der Berichterstellung und Analyse zum Exportieren von Daten vom Repository zu einer Datenbank verwenden. Zu den Vorteilen gehört die Möglichkeit, eine benutzerdefinierte Aufgabe zu schreiben, ohne dafür benutzerdefinierten Java-Code erzeugen zu müssen. (Benutzerdefinierter Java-Code muss bei jeder Aufrüstung neu kompiliert und auf jedem Server bereitgestellt werden und da das Skript in die Aufgabe eingebettet ist, ist eine erneute Kompilierung und Bereitstellung nicht erforderlich.)

### Kapitel 3, „Identity Manager Forms“

- Das Kapitel wird durch die folgende Beschreibung der in Überwachungs- und Konformitätsverfahren verwendeten Formulare ergänzt. (ID-15447, 16240)

Überwachungs- und Konformitätsformulare in Identity Manager zeichnen sich durch ein Merkmal aus, das andere Identity Manager-Formulare nicht aufweisen: Sie können solche Formulare auf Benutzer- und auf Organisationsebene zuweisen. Auf Benutzerebene zugewiesene Formulare können die Effizienz beim Verarbeiten von Bescheinigungen und Korrekturen steigern.

Sie können z. B. das Benutzerformular festlegen, das in Identity Manager zum Bearbeiten eines Benutzers im Zusammenhang mit einer Zugriffsprüfung, einer Korrektur oder einer Korrektur von Konformitätsverletzungen angezeigt wird. Das Benutzerformular kann auf Benutzer- oder Organisationsebene festgelegt werden. Wenn in Identity Manager ein Benutzer im Zusammenhang mit einer erneuten Zugriffsprüfungssuche oder Zugriffsprüfungskorrektur erneut geprüft wird, werden dabei die in der Zugriffsabfrage definierten Überwachungsrichtlinien berücksichtigt. Die Überwachungsrichtlinien zur Sicherstellung dauerhafter Konformität können in die Definition einbezogen werden.

---

**HINWEIS** Nur Identity Manager-Administratoren mit den Fähigkeiten „Überwachung konfigurieren“ und „Auditor-Administrator“ können Überwachungskomponenten konfigurieren.

---

### Zusätzliche Informationen

- Eine Erläuterung der grundlegenden Überwachungs- und Konformitätskonzepte in Identity Manager sowie Anweisungen zum Implementieren von grundlegenden Überwachungs- und Konformitätsfunktionen finden Sie in *Identity Manager Administration*.
- Unter „Identity Manager Rules“ in *Identity Manager Deployment Tools* finden Sie allgemeine Erklärungen zu Regeln sowie nähere Informationen zu Korrekturregeln.

## Formularverarbeitung zu Überwachungszwecken

Wie bei `userForm` und `viewUserForm` können Sie Formulare für einen Benutzer oder eine Organisation festlegen. Der Benutzer oder alle Benutzer in der Organisation arbeiten dann mit diesem Formular. Wenn Sie ein Formular für einen Benutzer und eine Organisation festlegen, hat das für den Benutzer eingestellte Formular Vorrang. Bei der Suche nach dem Formular durchsucht Identity Manager die Organisationen von unten nach oben.

Formulare für die Überwachung verhalten sich genauso wie Benutzer- und Benutzeranzeigeformulare: Wenn einem Benutzer ein Formular zugewiesen wurde, verwendet der Benutzer dieses Formular, andernfalls verwendet er das seiner Organisation zugewiesene Formular.

## Festlegen von Benutzerformularen

Die Formulare „Audit Policy List“ und „Access Scan List“ unterstützen die Eigenschaft `fullView`. Diese bewirkt, dass in den Formularen detaillierte Informationen zu den Listenelementen angezeigt werden. Setzen Sie diese Eigenschaft auf `false`, damit der Benutzer, der die Liste anzeigen lässt, effizienter arbeiten kann.

Das Formular „Access Approval List“ verfügt über eine ähnliche Eigenschaft, `includeUE`, und das Formular „Remediation List“ über die Eigenschaft `includeCV`.

## Standardformulare für die Überwachung

In der folgenden Tabelle sind die Standardformulare für die Überwachung aufgeführt, die in Identity Manager enthalten sind.

Formularname	Zugeordneter Name	Zuweisung auf Benutzerebene	Zweck
Access Approval List	<code>accessApprovalList</code>		Zeigt eine Liste mit Bescheinigungs-Arbeitselementen an
Access Review Delete Confirmation	<code>accessReviewDeleteConfirmation</code>		Bestätigt das Löschen einer Zugriffsprüfung
Access Review Delete Confirmation	<code>accessReviewAbortConfirmation</code>		Bestätigt die Beendigung einer Zugriffsprüfung
Access Review Dashboard	<code>accessReviewDashboard</code>		Zeigt eine Liste mit allen Zugriffsprüfungen an
Access Review Remediation Form	<code>accessReviewRemediationWorkItem</code>	Ja	Zeigt alle UE-basierten Korrekturarbeits Elemente an
Access Review Summary	<code>accessReviewSummary</code>		Zeigt die Details einer bestimmten Zugriffsprüfung an

<b>Formularname</b>	<b>Zugeordneter Name</b>	<b>Zuweisung auf Benutzerebene</b>	<b>Zweck</b>
Access Scan Form	accessScanForm		Zeigt eine Zugriffsprüfung an oder ermöglicht deren Bearbeitung
Access Scan List	accessScanList		Zeigt eine Liste mit allen Zugriffsabfragen an
Access Scan Delete Confirmation	accessScanDeleteConfirmation		Bestätigt das Löschen einer Zugriffsabfrage
Access Approval List	attestationList	Ja	Zeigt eine Liste aller anstehenden Bescheinigungen an
Attestation Form	attestationWorkItem	Ja	Zeigt alle Bescheinigungs-Arbeitselemente an
UserEntitlementForm	userEntitlementForm		Zeigt den Inhalt einer UserEntitlement an
UserEntitlement Summary Form	userEntitlementSummaryForm		
Violation Detail Form	violationDetailForm		Zeigt die Details einer Konformitätsverletzung an
Remediation List	remediationList	Ja	Zeigt eine Liste mit Korrekturarbeitselementen an
Audit Policy List	auditPolicyList		Zeigt eine Liste mit Überwachungsrichtlinien an
Audit Policy Delete Confirmation Form	auditPolicyDeleteConfirmation		Bestätigt das Löschen einer Überwachungsrichtlinie
Conflict Violation Details Form	conflictViolationDetailsForm		Zeigt die SOD-Verletzungsmatrix an
Compliance Violation Summary Form	complianceViolationSummaryForm		
Remediation Form	reviewWorkItem	Ja	Zeigt eine Konformitätsverletzung an

## Warum sollten die Formulare angepasst werden?

Für die Bescheinigungs- und Korrekturfunktionen können Formulare angegeben werden, die genau die Details enthalten, mit denen sich die Effizienz beim Bescheinigen und Korrigieren erhöhen lässt. Der Bescheiniger für eine Ressource möchte sich z. B. bestimmte ressourcenspezifische Attribute im Listenformular anzeigen lassen und müsste beim Bescheinigen dann nicht mehr jedes Arbeitselement anzeigen lassen. Ein solches Formular würde je nach Ressourcentyp (und den entsprechenden Attributen) variieren. Es wäre daher sinnvoll, das Formular für einzelne Bescheiniger anzupassen.

Beim Bescheinigen hängt es von der Aufgabe des Bescheinigers ab, welche Ansprüche jeweils von Interesse sind. Der `idmManager`-Bescheiniger interessiert sich z. B. ganz allgemein für die Benutzeransprüche, ein Bescheiniger für eine Ressource dagegen nur für ressourcenspezifische Daten. Wenn Bescheiniger die Formulare „`attestationList`“ und „`AttestationWorkItem`“ so anpassen können, dass nur die benötigten Informationen abgerufen und angezeigt werden, lässt sich die Effizienz erheblich steigern.

## Variablen für Abfrageaufgaben

In den Definitionen der Aufgaben Überwachungsrichtliniensuche und Zugriffsabfrage sind die Formulare angegeben, die beim Starten einer Aufgabe verwendet werden müssen. Diese Formulare enthalten Felder, mit deren Hilfe die meisten, jedoch nicht alle Variablen für Abfrageaufgaben gesteuert werden können.

Variablenname	Standardwert	Zweck
<code>maxThreads</code>	5	Gibt die Anzahl gleichzeitig angemeldeter Benutzer an, die für eine einzelne Abfragefunktion gleichzeitig arbeiten können. Erhöhen Sie diesen Wert, wenn Sie beim Prüfen von Benutzern, die Konten auf sehr langsamen Ressourcen haben, die Leistungsfähigkeit erhöhen möchten.
<code>userLock</code>	5000	Gibt die Zeit (in ms) an, die benötigt wird, um für einen Benutzer, der geprüft werden soll, eine Sperre zu erhalten. Wenn mehrere gleichzeitig arbeitende Abfragefunktionen einen Benutzer bearbeiten und dieser über sehr langsame Ressourcen verfügt, führt eine Erhöhung dieses Werts u. U. zu weniger Sperrfehlern, aber zu einer insgesamt langsameren Abfrage.
<code>scanDelay</code>	0	Gibt die Zeit (in ms) an, die bis zur Ausgabe eines neuen Thread vergehen soll. Kann auf einen positiven Wert eingestellt werden, damit die Abfragefunktion weniger CPU-intensiv ist.

- Die Beschreibung des Disable-Elements wurde wie folgt überarbeitet: (ID-14920)  
Berechnet einen Booleschen Wert. Wenn der Wert „True“ lautet, werden das Feld und alle verschachtelten Felder während der Verarbeitung des aktuellen Formulars ignoriert.  
Erstellen Sie keine potenziell langen Aktivitäten in Disable-Elementen. Diese Ausdrücke werden bei jeder erneuten Berechnung des Formulars ausgeführt. Verwenden Sie stattdessen ein anderes Formularelement, das im Rahmen dieser Berechnung nicht so häufig ausgeführt wird.
- Im Abschnitt „Inserting Javascript into a Form“ ist fälschlicherweise angegeben, dass Sie mit einem <JavaScript>-Tag JavaScript in ein Formular einfügen können (ID-15741). JavaScript kann auch wie folgt eingefügt werden:

```
<Field>
  <Expansion>
    <script>
    .....
```

---

**HINWEIS** Die Variablen `display.session` und `display.subject` sind für Disable-Formularelemente nicht verfügbar.

---

- Sie können nun Warnmeldungen vom Typ WARNUNG, Fehler (ERROR) oder Information (OK) in ein XPRESS-Formular einfügen. (ID-14540, ID-14953)

---

**HINWEIS** In diesem Beispiel wird zwar ein `ErrorMessage`-Objekt vom Typ Warnung in ein Formular eingefügt, Sie können jedoch auch einen anderen Schweregrad zuweisen.

---

1. Öffnen Sie das Formular, dem Sie die Warnung hinzufügen möchten im Identity Manager IDE.
2. Fügen Sie der Hauptanzeigeklasse `EditForm` oder `HtmlPage` `<Property name='messages'>` hinzu.
3. Fügen Sie den Codeblock `<defvar name='msgList'>` vom folgenden Beispielcode hinzu.
4. Ersetzen Sie den Meldungsschlüssel, der den Meldungstext kennzeichnet, der im Feld Alert der Beispielcode-Zeichenkette angezeigt werden soll:  
`<message name='UI_USER_REQUESTS_ACCOUNTID_NOT_FOUND_ALERT_VALUE >`
5. Speichern und schließen Sie die Datei.

## Codebeispiel

```

<Display class='EditForm'>
  <Property name='componentTableWidth' value='100%' />
  <Property name='rowPolarity' value='false' />
  <Property name='requiredMarkerLocation' value='left' />
  <Property name='messages'>
    <ref>msgList</ref>
  </Property>
</Display>
<defvar name='msgList'>
  <cond>
    <and>
      <nonnull>
        <ref>username</ref>
      </nonnull>
      <isnull>
        <ref>userview</ref>
      </isnull>
    </and>
    <list>
      <new class='com.waveset.msgcat.ErrorMessage'>
        <invoke class='com.waveset.msgcat.Severity' name='fromString'>
          <s>warning</s>
        </invoke>
        <message name='UI_USER_REQUESTS_ACCOUNTID_NOT_FOUND_ALERT_VALUE'>
          <ref>username</ref>
        </message>
      </new>
    </list>
  </cond>
</defvar>

```

Um einen anderen Schweregrad als Warnung anzuzeigen, ersetzen Sie `<s>warning</s>` im obigen Beispiel durch einen der folgenden beiden Werte:

- `error` -- Führt dazu, dass Identity Manager ein InlineAlert mit einem roten Fehlersymbol („error“) darstellt.
- `ok` -- Führt dazu, dass für Meldungen, die entweder Erfolg oder nicht kritische Vorgänge anzeigen, ein InlineAlert mit einem blauen Informationssymbol angezeigt wird.

Identity Manager stellt dies als ein InlineAlert mit einem Warnsymbol dar.

```

<invoke class='com.waveset.msgcat.Severity' name='fromString'>
  <s>warning</s>
</invoke>

```

wobei `warning` auch `error` oder `ok` sein kann.

## Kapitel 4, „Identity Manager Views“

- Die folgende Aktualisierung bezieht sich auf die Beschreibung der Organisationsansicht: (ID-13584)

Wird zum Festlegen des erstellten Organisationstyps und der Verarbeitungsoptionen verwendet.

### *Allgemeine Attribute*

Die Organisationsansichtsattribute höherer Ebene sind im Folgenden aufgelistet.

<b>Name</b>	<b>Bearbeitbar?</b>	<b>Datentyp</b>	<b>Obligatorisch?</b>
orgName	Lesen	Zeichenfolge	Vom System generiert
orgDisplayName	Lesen/Schreiben	Zeichenfolge	Ja
orgType	Lesen/Schreiben	Zeichenfolge	Nein
orgId	Lesen	Zeichenfolge	Vom System generiert
orgAction	Schreiben	Zeichenfolge	Nein
orgNewDisplayName	Schreiben	Zeichenfolge	Nein
orgParentName	Lesen/Schreiben	Zeichenfolge	Nein
orgChildOrgNames	Lesen	Liste	Vom System generiert
orgApprovers	Lesen/Schreiben	Liste	Nein
allowsOrgApprovers	Lesen	Liste	Vom System generiert
allowedOrgApproverIds	Lesen	Liste	Vom System generiert
orgUserForm	Lesen/Schreiben	Zeichenfolge	Nein
orgViewUserForm	Lesen/Schreiben	Zeichenfolge	Nein
orgPolicies	Lesen/Schreiben	Liste	Nein
orgAuditPolicies	Lesen/Schreiben	Liste	Nein
renameCreate	Lesen/Schreiben	Zeichenfolge	Nein
renameSaveAs	Lesen/Schreiben	Zeichenfolge	Nein

### *orgName*

Gibt die UID für die Organisation an. Dieser Wert unterscheidet sich von den meisten Ansichtobjektnamen, da Organisationen denselben Kurznamen aufweisen und doch zu verschiedenen übergeordneten Organisationen gehören können.

### *orgDisplayName*

Gibt den Kurznamen der Organisation an. Dieser Wert dient nur der Anzeige und muss nicht eindeutig sein.

### *orgType*

Definiert den Organisationstyp. Zulässige Werte sind `junction` oder `virtual`. Organisationen, die nicht zum Typ `junction` oder `virtual` gehören, weisen keinen Wert auf.

### *orgId*

Gibt die ID an, mit der die Organisation in Identity Manager eindeutig identifiziert wird.

### *orgAction*

Wird nur für Verzeichniszuordnungen, virtuelle Organisationen und dynamische Organisationen unterstützt. Zulässiger Wert ist `refresh`. Wenn es sich bei der Organisation um eine Verzeichniszuordnung oder eine virtuelle Organisation handelt, hängt das Verhalten bei der Aktualisierung vom Wert von `orgRefreshAllOrgsUserMembers` ab.

### *orgNewDisplayName*

Legt beim Umbenennen einer Organisation den neuen Kurznamen fest.

### *orgParentName*

Gibt den vollständigen Pfadnamen der übergeordneten Organisation an.

### *orgChildOrgNames*

Listet die Identity Manager-Schnittstellennamen aller direkten und indirekten untergeordneten Organisationen auf.

### *orgApprovers*

Listet die Identity Manager-Administratoren auf, die das Hinzufügen bzw. Modifizieren von Benutzern in der jeweiligen Organisation genehmigen müssen.

### *allowedOrgApprovers*

Listet die Namen von Benutzern auf, die ebenfalls das Hinzufügen und Modifizieren von Benutzern in der jeweiligen Organisation genehmigen könnten.

### *allowedOrgApproverIds*

Listet die IDs von Benutzern auf, die ebenfalls das Hinzufügen und Modifizieren von Benutzern in der jeweiligen Organisation genehmigen könnten.

### *orgUserForm*

Legt das `userForm` fest, das Benutzer, die Mitglied der jeweiligen Organisation sind, beim Erstellen oder Bearbeiten von Benutzern verwenden.

### *orgViewUserForm*

Legt das Benutzeranzeigeformular fest, das Benutzer, die Mitglied der jeweiligen Organisation sind, beim Anzeigen von Benutzern verwenden.

### *orgPolicies*

Gibt Richtlinien an, die für alle Benutzer gelten, die Mitglied der jeweiligen Organisation sind. Hierbei handelt es sich um eine Liste von Objekten, geordnet nach Typzeichenfolge: Alle Richtlinienobjekte enthalten die folgenden Ansichtsattribute, denen `orgPolicies[<type>]` vorangestellt ist. `<type>` steht für den Richtlinientyp (Beispiel: Lighthouse-Konto).

- `policyName` -- Gibt den Namen an.
- `id` -- Gibt die ID an.
- `implementation` -- Gibt die Klasse zur Implementierung der Richtlinie an.

### *orgAuditPolicies*

Gibt die Überwachungsrichtlinien an, die für alle Benutzer gelten, die Mitglied der jeweiligen Organisation sind.

### *renameCreate*

Wenn dieses Attribut auf „true“ gesetzt ist, wird die jeweilige Organisation geklont. Für die neu erstellte Organisation gilt der Wert von `orgNewDisplayName`.

### *renameSaveAs*

Wenn dieses Attribut auf „true“ gesetzt ist, wird die jeweilige Organisation in den Wert von `orgNewDisplayName` umbenannt.

## Attribute für Verzeichniszuordnung und virtuelle Organisationen

Name	Bearbeitbar?	Datentyp	Obligatorisch?
orgContainerId	Lesen	Zeichenfolge	Vom System generiert
orgContainerTypes	Lesen	Liste	Vom System generiert
orgContainers	Lesen	Liste	Vom System generiert
orgParentContainerId	Lesen	Zeichenfolge	Vom System generiert
orgResource	Lesen/Schreiben	Zeichenfolge	Ja, für Verzeichniszuordnung bzw. virtuelle Organisation
orgResourceType	Lesen	Zeichenfolge	Vom System generiert
orgResourceId	Lesen	Zeichenfolge	Vom System generiert
orgRefreshAllOrgsUserMembers	Schreiben	Zeichenfolge	Nein

### *orgContainerId*

Gibt den DN des zugehörigen LDAP-Verzeichniscontainers an (Beispiel: cn=foo,ou=bar,o=foobar.com).

### *orgContainerTypes*

Listet die zulässigen Ressourcenobjekttypen auf, die andere Ressourcenobjekte enthalten können.

### *orgContainers*

Listet die Basiscontainer für die Ressource auf, die von der Identity Manager-Schnittstelle zum Anzeigen einer Auswahlliste verwendet werden.

### *orgParentContainerId*

Gibt den DN des zugehörigen übergeordneten LDAP-Verzeichniscontainers an (Beispiel: ou=bar,o=foobar.com).

### *orgResource*

Gibt den Namen der Identity Manager-Ressource zum Synchronisieren der Verzeichniszuordnung und der virtuellen Organisationen an (Beispiel: West Directory Server).

### *orgResourceType*

Gibt den Typ der Identity Manager-Ressource an, von der aus die Verzeichniszuordnung und die virtuellen Organisationen synchronisiert werden (Beispiel: LDAP).

### *orgResourceId*

Gibt die ID der Identity Manager-Ressource an, die zum Synchronisieren von Verzeichniszuordnungen und virtuellen Organisationen verwendet wird.

### *orgRefreshAllOrgsUserMembers*

Wenn dieses Attribut auf `true` und `orgAction` auf `refresh` gesetzt ist, werden für die ausgewählte Organisation und alle untergeordneten Organisationen die Benutzer, die Mitglied in der Identity Manager-Organisation sind, mit den Benutzern im Ressourcencontainer synchronisiert. Wenn dieses Attribut auf `false` gesetzt ist, erfolgt keine Synchronisation mit den Benutzern im Ressourcencontainer. Für die ausgewählte Organisation und alle untergeordneten Organisationen werden nur die Ressourcencontainer mit den Identity-Manager-Organisationen synchronisiert.

### *Attribute für dynamische Organisationen*

Name	Bearbeitbar?	Datentyp	Obligatorisch?
<code>orgUserMembersRule</code>	Lesen/Schreiben	Zeichenfolge	Nein
<code>orgUserMembersRuleCacheTimeout</code>	Lesen/Schreiben	Zeichenfolge	Nein

### *orgUserMembersRule*

Gibt (anhand des Namens oder der UID) die Regel an, deren `authType` „UserMembersRule“ lautet. Diese wird zur Laufzeit ausgewertet, um die Mitgliedschaft zu ermitteln.

### *orgUserMembersCacheTimeout*

Gibt an, nach wie viel Millisekunden es zu einer Cache-Zeitüberschreitung kommt, wenn von „orgUserMembersRule“ zurückgegebene Benutzer in den Cache geschrieben werden sollen. Der Wert 0 gibt an, dass keine Zwischenspeicherung erfolgt.

Die Erläuterungen zur Benutzeransicht umfassen nun auch Informationen zu `accounts[Lighthouse].delegates`-Attributen: (ID-15468)

### *accounts[Lighthouse].delegates*

Führt Delegate-Objekte auf, die über `workItemType` indiziert werden, wobei jedes Objekt Delegate-Informationen für einen bestimmten Typ von Arbeitselement enthält.

- Wenn `delegateApproversTo` den Wert `delegatedApproversRule` hat, wird die ausgewählte Regel angegeben.
- Ist jedoch `manager` der Wert von `delegateApproversTo`, hat dieses Attribut keinen Wert.

***accounts[Lighthouse].delegatesHistory***

Führt Delegate-Objekt auf, die von 0 bis  $n$  indiziert sind, wobei  $n$  die aktuelle Anzahl der historischen Delegate-Objekte bis zur historischen Delegate-Tiefe angibt.

Dieses Attribut hat ein eindeutiges Attribut, `selected`, das ein Boolescher Wert ist, der das gerade ausgewählte historische Delegate-Objekt angibt.

***accounts[Lighthouse].delegatesOriginal***

Originalliste von Delegate-Objekten, die nach einem Abrufvorgang oder dem Auschecken einer Ansicht über `workItemType` indiziert werden.

Alle `accounts[Lighthouse].delegates*`-Attribute nehmen die folgenden Attribute an:

Attribute von <code>accounts[Lighthouse].delegate*</code> -Attributen	Beschreibung
<code>workItemType</code>	Identifiziert den Typ von <code>workItem</code> , das gerade delegiert wird. Eine Liste mit zulässigen <code>workItem</code> -Typen finden Sie in der Beschreibung des Modells für Delegate-Objekte unter <i>Identity Manager Technical Deployment Overview</i> dieses Dokumentationsnachtrags.
<code>workItemTypeObjects</code>	Führt die Namen spezifischer Rollen, Ressourcen oder Organisationen auf, in denen der Benutzer zukünftige <code>workItem</code> -Genehmigungsanforderungen delegiert. Dieses Attribut ist zulässig, wenn <code>workItemType</code> den Wert <code>roleApproval</code> , <code>resourceApproval</code> oder <code>organizationApproval</code> hat.  Wenn nicht angegeben, gibt dieses Attribut standardmäßig die Delegierung zukünftiger <code>workItem</code> -Anforderungen von allen Rollen, Ressourcen oder Organisationen an, in denen der Benutzer als Genehmiger fungiert.
<code>toType</code>	Typ, an den delegiert wird. Gültige Werte sind:  <code>manager</code>  <code>delegateWorkItemsRule</code>  <code>selectedUsers</code>
<code>toUsers</code>	Führt die Namen der Benutzer auf, an die delegiert werden soll (wenn <code>toType</code> den Wert <code>selectedUsers</code> hat).
<code>toRule</code>	Gibt den Namen der Regel an, die bei der Bestimmung der Benutzer angewendet wird, an die delegiert werden soll (wenn <code>toType</code> den Wert <code>delegateWorkItemsRule</code> hat).
<code>startDate</code>	Gibt das Datum an, an dem die Delegierung gestartet werden soll.
<code>endDate</code>	Gibt das Datum an, an dem die Delegierung beendet werden soll.

### Verweisen auf ein *DelegateWorkItems*-Ansichtsobjekt von einem Formular aus

Das folgende Codebeispiel veranschaulicht, wie Sie von einem Formular aus auf ein *DelegateWorkItems*-Delegate-Objekt verweisen können:

```
<Field name='delegates[*].workItemType'>
<Field name='delegates[*].workItemTypeObjects'>
<Field name='delegates[*].toType'>
<Field name='delegates[*].toUsers'>
<Field name='delegates[*].toRule'>
<Field name='delegates[*].startDate'>
<Field name='delegates[*].endDate'>
```

wobei unterstützte Indexwert (\*) *workItemType*-Werte sind.

- Das Kapitel wird durch die folgende Beschreibung der Benutzeranspruchsansicht ergänzt:  
Dient zum Erstellen und Modifizieren von *UserEntitlement*-Objekten.  
Diese Ansicht weist auf höchster Ebene die folgenden Attribute auf:

Name	Bearbeitbar?	Typ	Obligatorisch?
name		Zeichenfolge	Ja
Status		Zeichenfolge	Ja
Benutzer		Zeichenfolge	Ja
userId		Zeichenfolge	Ja
attestorHint		Zeichenfolge	Nein
userView		Generisches Objekt	Ja
reviewInstanceId		Zeichenfolge	Ja
reviewStartDate		Zeichenfolge	Ja
scanId		Zeichenfolge	Ja
scanInstanceId		Zeichenfolge	Ja
approvalWorkflowName		Zeichenfolge	Ja
organizationId		Zeichenfolge	Ja
attestorComments.name		Zeichenfolge	Nein
attestorComments.attestor		Zeichenfolge	Nein
attestorComments.time		Zeichenfolge	Nein

<b>Name</b>	<b>Bearbeitbar?</b>	<b>Typ</b>	<b>Obligatorisch?</b>
attestorComments.timestamp		Zeichenfolge	Nein
attestorComments.status			Nein

***name***

Gibt den Benutzeranspruch an (anhand einer eindeutigen ID).

***Status***

Gibt den Status des UserEntitlement-Objekts an. Zulässige Statuswerte sind u. a. PENDING, ACCEPTED, REJECTED, REMEDIATING und CANCELLED.

***user***

Gibt den Namen des zugehörigen WSUser für diesen Anspruch an.

***userId***

Gibt die ID des zugehörigen WSUser an.

***attestorHint***

Zeigt den Tipp (Zeichenfolge) für den Bescheiniger an, der in der Regel für Prüfungsbestimmung festgelegt ist. Dieser Tipp enthält für den Bescheiniger nützliche Informationen über die Regel.

***userView***

Enthält die von der Benutzeranspruchs-Prüffunktion erfasste Benutzeransicht. Wie viele Ressourcenkonten diese Ansicht enthält, hängt von der Konfiguration des AccessScan-Objekts ab.

***reviewInstanceld***

Gibt die ID der PAR-Aufgabeninstanz an.

***reviewStartDate***

Gibt das Startdatum (Zeichenfolge) der PAR-Aufgabe an (im Standardformat).

***scanId***

Gibt die ID der AccessScan-Aufgabendefinition an.

***scanInstanceld***

Gibt die ID der AccessScan-Aufgabeninstanz an.

***approvalWorkflowName***

Gibt den Namen des für die Genehmigung auszuführenden Workflows an. Dieser Wert stammt aus der AccessScan-Aufgabendefinition.

### *organizationId*

Gibt die ID der Organisation des WSUser zur Zeit der Prüfung an.

### *attestorComments*

Listet Bescheinigungsdatensätze für den Anspruch auf. Jeder Bescheinigungsdatensatz gibt eine Aktion oder eine Anweisung in Bezug auf den Anspruch an, u. a. Genehmigung, Ablehnung und erneute Prüfung.

### *attestorComments[timestamp].name*

Zeitstempel zum Identifizieren des Elements in der Liste.

### *attestorComments[timestamp].attestor*

Gibt den WSUser-Namen des Bescheinigers an, von dem der Kommentar zum Anspruch stammt.

### *attestorComments[timestamp].time*

Gibt die Uhrzeit an, zu der dieser Datensatz vom Bescheiniger bescheinigt wurde. Kann vom Zeitstempel abweichen.

### *attestorComments[timestamp].status*

Gibt den vom Bescheiniger zugewiesenen Status an. Hierbei kann es sich um eine beliebige Zeichenfolge handeln. Normalerweise wird jedoch die vom Bescheiniger ausgeführte Aktion angegeben, also z. B. Genehmigung, Ablehnung, erneute Prüfung, Korrektur.

### *attestorComments[name].comment*

Enthält vom Bescheiniger hinzugefügte Kommentare.

- Die folgenden Benutzeransichtsattribute wurden verworfen. (ID-15468)
  - `accounts[Lighthouse].delegateApproversTo`
  - `accounts[Lighthouse].delegateApproversSelected`
  - `accounts[Lighthouse].delegateApproversStartDate`
  - `accounts[Lighthouse].delegateApproversEndDate`
- Die Ansicht für delegierte Genehmiger wurde verworfen, kann jedoch weiterhin für die Bearbeitung von Delegate-Objekten verwendet werden, bei denen `workItemType` auf `approval` gesetzt ist.

Die bisherigen `accounts[Lighthouse].delegate*`-Attribute für die Benutzeransicht wurden verworfen und stehen über die Benutzeransicht nicht mehr zur Verfügung. Verwenden Sie die neue `accounts[Lighthouse].delegates`-Ansicht.

## Kapitel 6, „XPRESS Language“

Dieses Kapitel wurde erheblich aktualisiert. Näheres finden Sie in der .pdf-Datei „XPRESS“. Sie befindet sich im gleichen Verzeichnis wie diese Versionshinweise.

## Kapitel 8, „HTML Display Components“

- Die folgenden Erläuterungen über eine Alternative zur MultiSelect-Komponente wurde diesem Kapitel hinzugefügt:

Die Anzeige vieler Admin-Rollen über die MultiSelect-Komponente (entweder die Applet- oder HTML-Version) ist u. U. recht umständlich. Identity Manager bietet eine besser skalierbare Möglichkeit zum Anzeigen und Verwalten von Admin-Rollen: die objectSelector-Feldvorlage. (ID-15433)

Die Scalable Selection Library (in sample/formlib.xml) enthält ein Beispiel, das beschreibt, wie Sie mit Hilfe einer objectSelector-Feldvorlage nach Admin-Rollen suchen können, die vom Benutzer ausgewählt werden können.

### Codebeispiel

Beispiel einer objectSelector-Feldvorlage

```
<Field name='scalableWaveset.adminRoles'>
  <FieldRef name='objectSelector'>
    <Property name='selectorTitle' value='_FM_ADMIN_ROLES' />
    <Property name='selectorFieldName' value='waveset.adminRoles' />
    <Property name='selectorObjectType' value='AdminRole' />
    <Property name='selectorMultiValued' value='true' />
    <Property name='selectorAllowManualEntry' value='true' />
    <Property name='selectorFixedConditions'>
      <appendAll>
        <new class='com.waveset.object.AttributeCondition'>
          <s>hidden</s>
          <s>notEquals</s>
          <s>true</s>
        </new>
        <map>
          <s>onlyAssignedToCurrentSubject</s>
          <Boolean>true</Boolean>
        </map>
      </appendAll>
    </Property>
    <Property name='selectorFixedInclusions'>
      <appendAll>
        <ref>waveset.original.adminRoles</ref>
      </appendAll>
    </Property>
  </FieldRef>
</Field>
```

## Verwenden des objectSelector-Beispielcodes

1. Öffnen Sie in der Identity Manager IDE das UserForm-Objekt der Administratorenbibliothek.
2. Fügen Sie diesem Formular den folgenden Code hinzu:

```
<Include>
    <ObjectRef type='UserForm' name='Scalable Selection Library' />
</Include>
```

3. Wählen Sie im Feld AdministratorFields das Feld accounts[Lighthouse].adminRoles .
4. Ersetzen Sie die gesamte Referenz accounts[Lighthouse].adminRoles durch folgende Referenz:

```
<FieldRef name='scalableWaveset.adminRoles' />
```

5. Speichern Sie das Objekt.

Wenn Sie das nächste Mal einen Benutzer bearbeiten und die Registerkarte Sicherheit auswählen, zeigt Identity Manager das angepasste Formular an. Durch Klicken auf ... wird die Selektorkomponente geöffnet und ein Suchfeld angezeigt. Suchen Sie mit Hilfe dieses Felds nach Admin-Rollen, die mit einer Zeichenfolge beginnen und stellen Sie das Feld auf einen oder mehrere Werte ein.

Um das Formular wiederherzustellen, importieren Sie `$WSHOME/sample/formlib.xml` über **Konfigurieren > Exchange-Datei importieren**.

Weitere Beispiele zum Verwalten von Ressourcen und Rollen in objektreichen Umgebungen mit der objectSelector-Vorlage finden Sie in der Scalable Selection Library in `sample/formlib.xml`.

- Die Erläuterungen zur TabPanel-Komponente enthalten nun die folgende Beschreibung der validatePerTab-Eigenschaft: (ID-15501)

validatePerTab: Bei Einstellung auf „true“ führt Identity Manager Validierungsausdrücke aus, sobald der Benutzer zu einer anderen Registerkarte wechselt.

- Die Erläuterungen zur MultiSelect-Komponente enthalten nun die folgende Beschreibung der displayCase-Eigenschaft: (ID-14854)

displayCase: Weist jedem zulässigen Wert die zugehörige Groß- oder Kleinbuchstabenentsprechung zu. Zulässig sind die beiden Werte upper und lower.

- Diesem Kapitel wurden die folgenden Erläuterungen zur Menu-Komponente hinzugefügt: (ID-13043)

Besteht aus drei Klassen: `Menu`, `MenuBar` und `MenuItem`.

- `Menu` bezieht sich auf die gesamte Komponente.
- `MenuItem` ist ein Blatt oder Knoten, das bzw. der einer Registerkarte auf der ersten oder zweiten Ebene entspricht.
- `MenuBar` entspricht einer Registerkarte, die `MenuBars` oder `MenuItems` enthält.

`Menu` enthält die folgenden Eigenschaften:

- `layout`: Eine Zeichenfolge mit dem Wert `horizontal` oder `vertical`. Mit dem Wert `horizontal` wird eine horizontale Navigationsleiste mit Registerkarten erzeugt. `vertical` führt dazu, dass das Menü in Form eines vertikalen Strukturmenüs mit einem typischen Knotenlayout dargestellt wird.
- `stylePrefix`: Präfix für den CSS-Klassenname. Für Identity Manager-Endbenutzerseiten lautet dieser Wert `User`.

`MenuBar` enthält die folgenden Eigenschaften:

- `default`: Ein URL-Pfad, der einer der `MenuItem`-Eigenschaften von `MenuBar` entspricht. Dadurch wird gesteuert, welche untergeordnete Registerkarte standardmäßig als `selected` angezeigt werden soll, wenn auf die Registerkarte `MenuBar` geklickt wird.

`MenuItem` enthält die folgenden Eigenschaften:

- `containedUrls`: Eine Liste mit URL-Pfaden zu JSPs, die mit `MenuItem` „verwandt“ sind. Das aktuelle `MenuItem` wird bei der Anzeige von `containedUrls`-JSPs als „selected“ dargestellt. Ein Beispiel hierfür ist die Ergebnisseite eines Anforderungsstarts, die nach dem Start eines Arbeitsablaufs von der Anforderungsstartseite aus angezeigt wird.

Sie können diese Eigenschaften entweder für `MenuBar` oder `MenuItem` festlegen:

- `title`: Legt die Textzeichenfolge fest, die auf der Registerkarte oder dem Strukturblatt als Hyperlink angezeigt werden soll.
- `URL`: Legt den URL-Pfad für den Titel-Hyperlink fest.

Mit dem folgenden XPRESS-Beispiel wird ein Menü mit zwei Registerkarten erzeugt. Die zweite Registerkarte enthält zwei untergeordnete Registerkarten:

## Codebeispiel Implementierung von Menu-, MenuItem- und MenuBar-Komponenten

```

<Display class='Menu' />
<Field>
  <Display class='MenuItem'>
    <Property name='URL' value='user/main.jsp' />
    <Property name='title' value='Home' />
  </Display>
</Field>
<Field>
  <Display class='MenuBar' >
    <Property name='title' value='Work Items' />
    <Property name='URL' value='user/workItemListExt.jsp' />
  </Display>
  <Field>
    <Display class='MenuItem'>
      <Property name='URL' value='user/workItemListExt.jsp' />
      <Property name='title' value='Approvals' />
    </Display>
  </Field>
  <Field>
    <Display class='MenuItem'>
      <Property name='URL' value='user/otherWorkItems/listOtherWorkItems.jsp' />
      <Property name='title' value='Other' />
    </Display>
  </Field>
</Field>
</Field>

```

## Anhang A, „Form and Process Mappings“

- Eine aktualisierte Version des Anhangs „Form and Process Mappings“ finden Sie im selben Verzeichnis wie diese Versionshinweise.
- Es ist möglich, über zugeordnete Namen auf konformitätsspezifische Aufgaben zuzugreifen. (ID-15447)

Prozessname	Zugeordneter Name	Beschreibung
Access Review	accessReview	Ausführung einer Zugriffsprüfung
Access Scan	accessReviewScan	Ausführung einer Zugriffsabfrage
Access Review Rescan	accessReviewRescan	Ausführung einer erneuten Zugriffsabfrage
Audit Policy Rescan	auditPolicyRescan	Ausführung einer erneuten Überwachungsrichtliniensuche
Abort Access Review	abortAccessReview	Beendigung einer Zugriffsprüfung
Delete Access Review	deleteAccessReview	Löschen einer Zugriffsprüfung
Recover Access Review	recoverAccessReview	Wiederherstellung fehlender Zugriffsprüfungs-Statusobjekte von Überwachungsprotokollen

---

# Identity Manager Deployment Tools

Dieser Abschnitt enthält neue Informationen und Dokumentationskorrekturen für *Sun Java™ System Identity Manager Deployment Tools*:

## Neuigkeiten

Den folgenden Kapiteln der *Identity Manager Deployment Tools*-Dokumentation wurden wichtige Informationen hinzugefügt:

- Kapitel 1, „*Using the Identity Manager IDE*“ wurde ergänzt und enthält nun Informationen zu den folgenden neuen Merkmalen und Funktionen:
  - Der Prozess zum Erstellen und Verwenden von Identity Manager IDE-Projekten wurde um zwei Projekttypen erweitert (ID-14587):
    - Identity Manager Project ist eine voll funktionsfähige, primäre Entwicklungsumgebung für Entwickler.
    - Identity Manager Project (Remote) ist für kleine Änderungen und Fehlersuchen auf einem externen Server vorgesehen.
  - Identity Manager IDE-Projekte verfügen nun über eine CBE (Configuration Build Environment) (ID-14980).
  - Auf der NetBean-Menüleiste der obersten Ebene gibt es nun ein IDM-Menü, in dem Sie Vorgänge auswählen können, die für die ausgewählten Objektknoten geeignet sind. (ID-14787)
  - Der Liste der Objekttypen, die im Explorer-Fenster angezeigt wird, wurden Bibliotheksobjekte mit Eigenschaftsfenstern, Palettenfunktionen und Navigationsknoten hinzugefügt. (ID-14817)
  - Wenn Sie für ein Regelobjekt die Designansicht wählen, wird im Editor-Fenster nun ein Ausdrucks-Generator angezeigt, der es ermöglicht, die logische Struktur einer Regel besser zu veranschaulichen und die Eigenschaften der Regel zu ändern. (ID-15104)
  - Sie können nun (diff-) Objekte in einem lokalen Verzeichnis mit denen im Repository vergleichen. (ID-15206)
  - Der Prozess zum Testen von Formularen und Regeln wurde geändert. Die Option *Formularvorschau* wurde in *Formulartester* umbenannt. (ID-15325)

- Den Dialogfeldern des Identity Manager IDEAusdrucks-Generators wurden neue Merkmale und Funktionen hingefügt:
  - Sie können nun einfache Datentypen (ganze Zahlen und Zeichenfolgen) direkt in der Tabelle des Ausdrucks-Generators bearbeiten. (ID-15528)
  - Anstatt zuerst einen BLOCK erstellen und diesen dann in den gewünschten Ausdruck umwandeln zu müssen, können Sie nun direkt einen bestimmten Ausdruck erstellen. (ID-15932)
  - Es wurden eine neue Schaltfläche und ein neues Dialogfeld hinzugefügt, mit der bzw. mit dem Sie den Ausdruckstyp eines Elements ändern können. (ID-15933)
  - Sie können Eigenschaftswerte, die einen Ausdruck und primitive Werte (wie Zeichenfolgen) unterstützen, jetzt direkt in einer Eigenschaftentabelle bearbeiten. (ID-15528)
  - Beim Definieren von XPRESS-invoke-Anweisungen (statisch oder Instanz) im Ausdrucks-Generator können Sie die zugehörigen JavaDoc-Informationen zu den Methoden der Identity Manager-API anzeigen lassen. Zum Aufrufen der JavaDoc-Dokumentation stellen Sie den Cursor über die Methoden, die im Menü „Method Name“ aufgelistet sind. Die Informationen werden in einem Popup-Fenster angezeigt.
- Das Identity Manager IDE-Plug-In benötigt nun JDK 1.5 und Netbeans 5.5. (ID-14950)
- Sie können nun Objekt im Identity Manager IDE-Repository löschen. (ID-15031)
- Sie können nun ein Objekt in die IDE eines Identity Manager 7.0 Servers hochladen und dem Objekt manuell eine ID zuweisen. (ID-15474)
- Sie können nun in der Projektstruktur mit der rechten Maustaste auf Knoten klicken und Objekte öffnen, auf die bestimmte Referenzen verweisen (z. B. ObjectRefs, FormRefs, FieldRefs und untergeordnete Arbeitsablaufprozesse). (ID-15406)
- Andere, geringfügige Benutzeroberflächen- und Prozessänderungen
- Der Abschnitt „*Auditor Rules*“ in Kapitel 2, „*Working with Rules*“, wurde aktualisiert und enthält nun mehr detaillierte Informationen über Identity Auditor-Regeln. (ID-15367, 15496, 15609, 15934, 16166, 16263 und 16292)
- Kapitel 7, „*Using SPML 1.0 with Identity Manager Web Services*“, wurde aktualisiert und enthält nun Informationen über die SPE-SPML-Schnittstelle. (ID-14458)
- Der Abschnitt „*Using Trace in SPML*“ in Kapitel 7, „*Using SPML 1.0 with Identity Manager Web Services*“, wurde aktualisiert und enthält nun zusätzliche Informationen über die Aktivierung des Ablaufprotokolls, damit Sie den SPML-Datenverkehr in Identity Manager protokollieren und Probleme diagnostizieren können. (ID-15346)

- Der Abschnitt „*Using Trace in SPML*“ in Kapitel 8, „*Using SPML 2.0 with Identity Manager Web Services*“, wurde aktualisiert und enthält nun zusätzliche Informationen über die Aktivierung des Ablaufprotokolls, damit Sie den SPML-Datenverkehr in Identity Manager protokollieren und Probleme diagnostizieren können. (ID-15346)

## Aktualisierungen

Dieser Abschnitt enthält Korrekturen und Ergänzungen für die Dokumentation *Identity Manager Deployment Tools*:

- Die Abschnitte „*Palette Window*“ und „*Properties Window*“ in Kapitel 1, „*Using the Identity Manager IDE*“, sollten in der Liste der Elemente im ersten Absatz jeweils die Angabe „*GenericObjects*“ enthalten: (ID-14817)
  - Im Palettenfenster (siehe z. B. Abbildung 1-11) können Sie Elemente per Ziehen und Ablegen in die E-Mail-Vorlagen-, Formular-, *GenericObjects*-, Bibliotheks-, Arbeitsablaufprozess- oder untergeordneten Arbeitsablaufprozessobjekte einfügen, die in den Editorfenstern angezeigt werden. Die Eingabe von XML-Code ist nicht erforderlich.
  - Das Identity Manager IDE-Eigenschaftsfenster besteht aus einem Eigenschaftsfenster für XML-Elemente, die zu den E-Mail-Vorlagen-, Formular-, *GenericObjects*-, Bibliotheks-, Regel-, Arbeitsablaufprozess- und untergeordneten Arbeitsablaufprozessobjekten gehören. In diesem Eigenschaftsfenster können Sie die Eigenschaften eines ausgewählten Objekts anzeigen und bearbeiten, so auch den Objektamen, Dateigrößen, Modifikationszeiten, Ergebnisse usw.

---

# Identity Manager Tuning, Troubleshooting, and Error Messages

Dieser Abschnitt enthält neue Informationen und Dokumentationskorrekturen für *Sun Java™ System Identity Manager Tuning, Troubleshooting, and Error Messages*.

- Es sind nun Informationen über die Größe von Repository-Objekten (in Zeichen) verfügbar. Mit Hilfe dieser Informationen können Sie sehr große Objekte identifizieren, die ein Proben für das System darstellen könnten. (ID-9896, ID-15239)

Der Zugriff auf diese Informationen ist über die Webseite `debug/Show_Sizes.jsp` oder über die Befehlszeile der Konsole möglich. Geben Sie dazu Folgendes ein:

```
showSizes [<type> [<limit>]]
```

---

**HINWEIS** Bei Aufrüstungen geben vorhandene Objekte eine Größe von 0 an, bis diese aktualisiert oder anderweitig erneuert wurden.

---

- Einige Aufgaben wurden vom Adapter- zum Aufgabenpaket verschoben. Wenn Sie für die folgenden Aufgaben die Verfolgung aktiviert haben oder mit benutzerdefinierten Aufgabendefinitionen arbeiten, die auf diese Paket verweisen, müssen diese Pfade aktualisiert werden.

---

Alter Paketname	Neuer Paketname
com.waveset.adapter.ADSyncFailoverTask	com.waveset.task.ADSyncFailoverTask
com.waveset.adapter.ADSyncRecoveryCollectorTask	com.waveset.task.ADSyncRecoveryCollectorTask
com.waveset.adapter.SARunner	com.waveset.task.SARunner
com.waveset.adapter.SourceAdapterTask	com.waveset.task.SourceAdapterTask

---

---

# Identity Manager Service Provider Edition Deployment

Dieser Abschnitt enthält neue Informationen und Dokumentationskorrekturen für *Sun Java™ System Identity Manager SPE Deployment*.

## Kapitel 5, „Other Objects in Identity Manager SPE“

Identity Manager SPE unterstützt nun Link-Korrelationsregeln und Link-Bestätigungsregeln.

### Link-Korrelationsregeln

Die Option `linkTargets` der `IDMXUser`-Ansicht ermöglicht dem Aufrufer, die Liste der Ressourcen anzugeben, die zum Verknüpfen herangezogen werden sollen. Beim Arbeiten mit Formularen kann die Liste als eine Formulareigenschaft mit dem gleichen Namen bereitgestellt werden. Formeigenschaften werden beim Einchecken der `IDMXUser`-Ansicht in die Ansichtsoptionen aufgenommen.

Die Ressourcenkonten, über die der Benutzer u. U. verfügt, werden durch eine Link-Korrelationsregel ausgewählt. Ausgehend von der Ansicht des Benutzers gibt eine Link-Korrelationsregel eine Identität, eine Liste mit Identitäten oder eine Optionszuordnung zurück.

Wird eine Optionszuordnung zurückgegeben, sucht die Ansichtsbehandlungsroutine mit Hilfe der Zuordnung nach Ressourcenkonten und erhält eine Liste mit Identitäten, die diesen Optionen entsprechen. So kann z. B. die `searchFilter`-Option der `FormUtil`-Methode `getResourceObjects` dazu verwendet werden, einen Suchfilter an einen LDAP-Ressourcenadapter zu übergeben.

In einer Link-Korrelationsregel muss das Attribut `authType` auf `SPERule` und `subtype` auf `SUBTYPE_SPE_LINK_CORRELATION_RULE` eingestellt sein.

### Link-Bestätigungsregel

Durch eine Link-Bestätigungsregel werden alle Ressourcenkonten von der Liste der potenziellen Konten entfernt, die durch die Link-Korrelationsregel ausgewählt sind. Ausgehend von der Ansicht des Benutzers und der Liste der Kandidaten-Ressourcenkonten, wählt eine Link-Bestätigungsregel höchstens ein Ressourcenkonto von der Kandidatenliste aus. Die Ansicht des Benutzer wird unter dem Pfad 'view' angezeigt, während die Liste der Kandidaten unter dem Pfad 'candidates' verfügbar ist.

Wenn durch die Link-Korrelationsregel höchstens ein Ressourcenkonto ausgewählt wird, ist die Link-Bestätigungsregel optional.

---

**HINWEIS** Im Gegensatz zu Identity Manager-Bestätigungsregeln wird eine Link-Bestätigungsregel nur während des Verknüpfungsprozesses aufgerufen.

---

In einer Link-Bestätigungsregel muss das Attribut `authType` auf `SPERule` und `subtype` auf `SUBTYPE_SPE_LINK_CONFIRMATION_RULE` eingestellt sein.

## LighthouseContext-API

Der `SessionFactory`-Klasse wurden mehrere erweiterte Methoden hinzugefügt. Die Tabelle auf Seite 16 ist wie folgt zu aktualisieren.

Verbindungstyp	Methode	Beschreibung
Local anonymous	<code>getServerInternalContext()</code>	Gibt einen vollständig autorisieren Kontext ohne jegliche Authentifizierung zurück
Local authenticated	<code>getSPESession(String user, EncryptedData password)</code>	Erstellt eine Sitzung für die Service Provider-Benutzeroberfläche.
Local authenticated	<code>getSPESession(Map credentials)</code>	Erstellt eine Sitzung für die Service Provider-Benutzeroberfläche. In der Zuordnungstabelle sind alle Berechtigungsnachweise des Benutzers aufgeführt, einschließlich der Werte für Benutzer- und Passwortschlüssel.
Local pre-authenticated	<code>getSPEPreAuthenticatedSession(String user)</code>	Erstellt eine vorauthentifizierte Sitzung für die Service Provider-Benutzeroberfläche
Remote anonymous	Nicht zutreffend	Dieser Verbindungstyp ist nur über SPML verfügbar.
Remote authenticated	<code>getSession(URL url, String user, EncryptedData pass)</code>	Gibt eine authentifizierte Sitzung zurück

---

# Umfang der Lokalisierung

In Identity Manager wurden und werden Ressourcenobjekte und Funktionen nicht lokalisiert, denn es handelt sich in erster Linie um Beispiele, die während der Initialisierung von Identity Manager geladen werden (über `init.xml`), und zudem können die Attribute von Objekttypen in verschiedenen Bereitstellungsumgebungen beim Kunden variieren, je nachdem, wie stark die Bereitstellung angepasst wurde. Im Folgenden sind die Bereiche aufgeführt, in denen die Benutzer auf englische Ausdrücke stoßen können: (ID-16349)

- Standardbenutzerformulare und Prozesszuordnungen
  - **Beispiel:** Benutzer bearbeiten > Sicherheit > Pulldown-Menüs „Benutzerformular“
  - **Beispiel:** Konfigurieren > Formular- und Prozesszuordnungen
- Attributnamen von Konfigurationsobjekten

**Beispiel:** Konfigurieren > Benutzeroberfläche, zusammengesetzte Namen wie `displayPasswordExpirationWarning`
- Standardaufgaben
  - Aufgabenvorlagen

**Beispiel:** Serveraufgaben > Aufgaben konfigurieren > Namen in der Tabelle „Verfügbare Aufgaben“
  - Aufgabentypbezeichnungen

**Beispiel:** Serveraufgaben > Aufgaben ausführen > Elemente in der zweiten Spalte der Tabelle „Verfügbare Aufgaben“
  - Aufgabendefinitionen

**Beispiel:** Serveraufgaben > Aufgaben suchen > zweites Pulldown-Menü zum Auswählen der Aufgabendefinition
- Standardberichtsamen

**Beispiel:** Berichtsamen unter Berichte > Berichte ausführen > Berichtstabelle
- Standardrichtliniennamen

**Beispiel:** Konformität > Richtlinien verwalten > Namen und Beschreibungen von Überwachungsrichtlinien

- Standardfähigkeiten  
**Beispiel:** Benutzer bearbeiten > Sicherheit > Verfügbare Fähigkeiten
- Standardberichts- und -diagrammnamen
- Prozess-/Workflow-Diagramm-Applets

---

## helpTool verwenden

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

Sie führen helpTool folgendermaßen über die Befehlszeile aus:

```
$ java -jar helpTool.jar
Verwendung: 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:

- **Zielverzeichnis:** `html/help/en_US`

---

**HINWEIS** Verwenden Sie die für Ihre Installation geeignete Gebietsschemazeichenfolge.

---

- **Eingabedatei:** `../WEB-INF/lib/idm.jar`
- **Nova-Indexverzeichnis:** `index/help`
- **Name der Ausgabedatei:** `index_files_help.txt`

---

**HINWEIS** Dieser Dateiname ist nicht wichtig; das Tool wird jedoch beendet, falls diese Datei bereits vorhanden ist.

---

- **Eigenschaftendatei für die Indizierung:** `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:

- **Zielverzeichnis:** `html/docs`
- **Eingabedateien:** `../doc/HTML/en_US`

---

**HINWEIS** Das Tool kopiert das Verzeichnis `en_US/` und dessen Unterverzeichnisse in dieses Ziel.

---

- **Nova-Indexverzeichnis:** `index/docs`
- **Name der Ausgabedatei:** `index_files_docs.txt`

---

**HINWEIS** Dieser Dateiname ist nicht wichtig, das Tool wird jedoch beendet, falls diese Datei bereits vorhanden ist.

---

- **Eigenschaftendatei für die Indizierung:** `index/index.properties`

## 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
```