

# Sun™ Identity Manager Versionshinweise

Version 8.0 Mai 2008

Teilenummer 820-5437-10

---

Diese Versionshinweise enthalten wichtige Informationen, die zum Zeitpunkt der Herausgabe von Sun Identity Manager 8.0 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 8.0 zu arbeiten.

Diese Versionshinweise sind in die folgenden Abschnitte unterteilt:

- [Einführung](#)
- [Identity Manager 8.0-Funktionen](#)
- [Installations- und Aktualisierungshinweise](#)
- [Veraltete APIs \(Unterstützung eingestellt\)](#)
- [Erweiterungen und Korrekturen der Dokumentation](#)

In der vorliegenden Dokumentation wird auf URLs von Drittanbietern verwiesen, über die zusätzliche relevante Informationen zur Verfügung gestellt werden.

---

**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 8.0-Versionshinweise finden Sie folgende Informationen:

- [Unterstützte Software und Umgebungen](#)
- [Aufrüstungsmöglichkeiten und Supportrichtlinien](#)
- [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](#)
- [Java-Unterstützung](#)
- [Anwendungsserver](#)
- [Repository-Datenbankserver](#)
- [Sun Identity Manager Gateway](#)
- [Unterstützte Ressourcen](#)
- [Browser](#)
- [Nicht mehr unterstützte Software](#)

---

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

---

## Betriebssysteme

Diese Version von Identity Manager unterstützt die folgenden Betriebssysteme:

- AIX 5.2, 5L v5.3
- HP-UX 11i v1, 11i v2
- Microsoft Windows 2000 SP3, 2000 SP4
- Microsoft Windows Server 2003
- Solaris 9, 10 Sparc und x86
- Red Hat Linux Advanced Server 2.1
- Red Hat Linux Enterprise Server 3.x, 4.x
- Novell SuSE Linux Enterprise Server 9 SP1

## Java-Unterstützung

Identity Manager benötigt Java Platform, Standard Edition (SE) 5 oder höher.

## Unterstützung für System-Virtualisierung

System-Virtualisierung ist eine Technologie, bei der mehrere Instanzen eines Betriebssystems unabhängig voneinander auf gemeinsam genutzter Hardware ausgeführt werden. Software, die auf einem solchermaßen „virtualisierten“ Betriebssystem ausgeführt wird, merkt in der Regel nicht, dass es sich dabei um eine virtualisierte Plattform handelt. Sun testet seine Sun Java System-Produkte auf ausgewählten Kombinationen aus System-Virtualisierungslösungen und Betriebssystemen. Dies hilft zu gewährleisten, dass diese Produkte in (richtig dimensionierten und konfigurierten) virtualisierten Umgebungen genau so funktionieren wie auf einem nicht-virtualisierten System. Nähere Informationen zur Unterstützung von Sun Java System-Produkten in virtualisierten Umgebungen finden Sie unter <http://docs.sun.com/doc/820-4651>.

## 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. Identity Manager benötigt das Java SE Development Kit (JDK) 5 oder 6 auf einem der folgenden Anwendungsserver (sofern der Anwendungsserver diese Versionen unterstützt).

- Apache® Tomcat 5.5.x, 6.0.x
- BEA WebLogic® Server™ 9.1, 9.2, 10
- IBM WebSphere® 6.1
- JBoss Application Server 4.2
- Oracle Application Server Enterprise Edition 10g Release 3 (10.1.3)
- Oracle Application Server Standard Edition 10g Release 3 (10.1.3)
- Sun Java™ System Application Server 9.1 (GlassFish v2 UR1, 32- und 64-Bit)
- Sun Java™ System Application Server Platform Edition 8.1, 8.2, 9.0
- Sun Java™ System Application Server Enterprise Edition 8.1, 8.2
- Sun Java™ System Application Server Standard Edition 8.2

---

### HINWEIS

- Wenn Ihr derzeitiger Anwendungsserver JDK 5 nicht unterstützt, erkundigen Sie sich beim Hersteller vor der Installation von Identity Manager über die Aufrüstung auf eine geeignete Version.
  - Identity Manager benötigt ein JDK, das korrekt mit der 2007 umgesetzten Sonderregelung für die Sommerzeitumstellung in den USA umgehen kann. Sie müssen alle diesbezüglichen Patches für Ihre JDK-Version installieren. Im Falle des Sun JDK 5 sind die betreffenden Funktionen ab Update 15 integriert. Das Sun JDK 6 enthält die Funktionen bereits von Haus aus.
  - Sie können Identity Manager auf BEA WebLogic-Anwendungsservern mit allen von WebLogic unterstützten JDKs 5 ausführen.
-

# Repository-Datenbankserver

Identity Manager unterstützt die folgenden Repository-Datenbankserver:

- IBM® DB2® Universal Database for Linux, UNIX® und Windows® (Version 8.1, 8.2)
- Microsoft SQL Server™ 2005
- MySQL™ 5.0, 5.1

---

**HINWEIS** Identity Manager unterstützt MySQL als Datenbankressource in Entwicklungs- oder Produktivsystemen. Als Repository-Datenbank wird MySQL nur in Entwicklungssystemen unterstützt.

---

- Oracle 9i® und Oracle Database 10g, 10g Release 1 und 10g Release 2®, 11g

---

**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.

---

---

**ACHTUNG** Falls Sie ein Oracle-Repository verwenden . . .

Die Repository-DDL von Identity Manager 8.0 verwendet Datentypen, mit denen ältere Oracle JDBC-Treiber nicht korrekt umgehen können. Die JDBC-Treiber in `ojdbc14.jar` lesen nicht alle Spalten der Protokolltabelle korrekt.

Damit Identity Manager korrekt funktioniert, müssen Sie auf die Oracle JDBC-Treiber für JDK 1.5 aktualisieren.

---

# Sun Identity Manager Gateway

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

## Unterstützte Ressourcen

Identity Manager unterstützt die folgenden Ressourcen:

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

### CRM (Customer Relationship Management)

- Siebel CRM-Software, Version 7.0.4, 7.7, 7.8, 8.0

### Datenbanken

- Generische Datenbanktabellen
- IBM® DB2® Universal Database für Linux, UNIX® und Windows® 8.1, 8.2
- Microsoft® Identity Integration Server (MIIS) 2003
- Microsoft SQL Server 2000, 2005

- MySQL™ 4.x, 5.0, 5.1

---

**HINWEIS** Identity Manager unterstützt MySQL als Entwicklungs- und Produktivdatenbank.

---

- Oracle Database 9i®, 10g Release 1®, 10g Release 2®
- Sybase Adaptive Server® 12.x
- Skript-JDBC (verwaltet Ressourcen, die JDBC 3.0 -Treiber oder höher verwenden)

## Verzeichnisse

- LDAP v3
- RACF LDAP
- Microsoft® Active Directory® 2000, 2003
- Microsoft® Active Directory® Application Mode (ADAM) Windows 2003 SP1 und höher
- Novell® eDirectory 8.7.1, 8.8
- Novell NetWare® 6.5
- Open LDAP
- Sun™ ONE Directory Server 4.x
- Sun Java™ System Directory Server 5.x, 6.3

---

**HINWEISS**

- Identity Manager wird zwar nur in Verbindung mit Sun Java™ System Directory Server und Open LDAP getestet. Eventuell funktionieren jedoch auch andere LDAP-Server, die v3 unterstützen, ohne weitere Änderungen des Ressourcenadapters.
- Bei Sun Java™ System Directory Server 5 2005Q1 muss ein Patch für das Plugin „retro changelog“ von Directory Server installiert werden, wenn Sie ActiveSync verwenden. Das Patch ist nur für die „regelmäßige“ Replikation erforderlich (nicht für die MMR-Replikation).

---

## Enterprise Resource Planning (ERP)

- MySAP ERP 2005 (ECC 6.0) Kernel, Version 7.00
- Oracle E-Business Suite auf Oracle Applications 11.5.9, 11.5.10, 12
- Peoplesoft® PeopleTools 8.1 bis 8.4.2
- Peoplesoft PeopleTools HRMS 8.0 bis 8.8, 9.0
- SAP® R/3 Enterprise 4.7 (SAP BASIS 6.20)
- SAP® NetWeaver Enterprise Portal 2004 (SAP BASIS 6.40), 2004s (SAP BASIS 7.00)
- SAP® Governance, Risk, and Compliance (GRC) Access Enforcer 5.1, 5.2

## Help Desk

- BMC Remedy Action Request System Server 6.0, 6.3, 7.0
- BMC Remedy Service Desk Application 7.0
- Remedy Help Desk 6.0

---

**HINWEIS** Help Desk 6.0 und Service Desk 7.0 unterscheiden sich erheblich im Hinblick auf Beispieldaten, Standardwerte und Standardkonfiguration. So ist beispielsweise der Name des „Ticket“-Schemas in Version 6.0 *HPD:HelpDesk*. In Version 7.0 wurde er in *HPD:Help Desk* geändert. Entwickler sollten bei einem Upgrade daher die Remedy-Produktdokumentation hinzuziehen.

---

## Messaging-Plattformen

- Sun Java System Messaging und Calender Service Java Enterprise System 2005Q1 und höher
- Lotus Notes® (Domino) 6.5, 7.0
- Microsoft® Exchange 2000, 2003, 2007

---

**HINWEIS**

- Microsoft Exchange 2000, 2003 und 2007 werden über den Active Directory-Ressourcenadapter verwaltet.
- Microsoft Exchange 2007 wird nur unter Windows 2003 unterstützt.

---

- Novell® GroupWise 7.0 (mit dem Novell NDS-Adapter)

## Sonstiges

- Flat Files
- JMS Message Queue Listener (verwaltet alle Warteschlangen, die mit JMS 1.0b oder höher kompatibel sind)
- Generic UNIX Shell Script

---

**HINWEIS** Der Generic UNIX Shell Script-Adapter führt unterstützte Shell-Typen auf unterstützten UNIX-Betriebssystemen aus.

---

- Generic Windows Script Adapter

---

**HINWEIS** Der Generic Windows Script-Adapter führt Skripten in der Befehlszeile (cmd) auf unterstützten Windows-Betriebssystemen aus, auf denen Sun Identity Manager Gateway installiert ist.

---

## Betriebssysteme

- HP OpenVMS 7.2, 8.3
- HP-UX 11.0, 11i v1, 11i v2
- IBM AIX® 4.3.3, 5.2, 5L, 5.3
- IBM OS/400® V4r3, V4r5, V5r1, V5r2, V5r3, V5r4
- Microsoft Windows® 2000, 2003
- Red Hat Linux 9.0
- Red Hat Linux Advanced Server 2.1
- Red Hat Linux Enterprise Server 3.0, 4.0
- Sun Solaris™ 9, 10
- SuSE Enterprise 9

---

**HINWEIS** Wenn Sie NIS-Konten unter Solaris verwalten, müssen Sie auf der Ressource Patch 126632-01 installieren, um die Leistung des Anmeldebefehls und des Solaris-Adapters zu verbessern.

---

## Rollenverwaltungssystem

- BridgeStream SmartRoles 2.7

## Sicherheitsmanager

- eTrust CA-ACF2® Security
- eTrust CA-Top Secret® Security 5.3
- IBM RACF®
- INISafe Nexess 1.1.5
- RSA ClearTrust 5.5.2, 5.5.3
- RSA® SecurID® 5.0, 6.0, 6.1.2
- RSA® SecurID® for UNIX 5.1, 6.0, 6.1.2
- Scripted Host

## Steuerung des Webzugriffs

- IBM Tivoli® Access Manager 4.x, 5.1, 6.0.0 FP09
- Netegrity® Siteminder® 5.5
- RSA® ClearTrust® 5.0.1
- Sun™ ONE Identity Server 6.1, 6.2
- Sun Java™ System Identity Server 2004Q2
- Sun Java™ System Access Manager 6 2005Q1, 7 2005Q4 (Realms wird seit 2005Q4 unterstützt), 7.1

## Browser

Identity Manager unterstützt die folgenden Browser:

- Microsoft Internet Explorer 6.x, 7.x
- Safari 2.0 oder höher für Mac OS X 10.3.3 oder höher, 3.0.x
- Firefox 1.04, 1.05, 1.06, 1.5, 2.0.0.4

## Eingestellte Funktionen von Identity Manager

Die folgenden Funktionen von Identity Manager wurden eingestellt. Die Unterstützung dieser Funktionen wird nur bis zur nächsten Hauptversion von Identity Manager fortgeführt. Bei Fragen wenden Sie sich bitte an Ihren zuständigen Kundendienstmitarbeiter.

### Identity Manager Business Process Editor (BPE)

- Der Business Process Editor (BPE) wird eingestellt und ist in der nächsten Identity Manager-Hauptversion nicht mehr enthalten. Verwenden Sie stattdessen die Identity Manager Integrated Development Environment (Identity Manager-IDE). (ID-17693).

### Metaansicht

- Die Metaansicht (MetaView) wurde aus neuen Identity Manager-Installationen entfernt. Wenn Sie die Metaansicht in einer früheren Version als Identity Manager 8.0 verwenden, können Sie dies jedoch auch weiterhin tun. Bei Fragen wenden Sie sich bitte an Ihren zuständigen Kundendienstmitarbeiter. (ID-17244).

## Nicht mehr unterstützte Software

In Identity Manager wurde oder wird die Unterstützung für die Betriebssysteme, Anwendungsserver, Datenbank-Repositories und verwalteten Ressourcen eingestellt, die in den folgenden Tabellen genannt sind.

### Nächste Hauptversion von Identity Manager

Die Software aus der folgenden Tabelle wird noch bis zur nächsten Hauptversion von Identity Manager unterstützt. 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>• Red Hat Linux Advanced Server 2.1, 3.0</li> <li>• Red Hat Linux Enterprise Server</li> <li>• Solaris 8</li> <li>• Windows 2000 SP3, 2000 SP4</li> </ul>
<b>Anwendungsserver</b>	<ul style="list-style-type: none"> <li>• JBoss Application Server 4.0.x</li> <li>• Sun Java System Application Server Platform Edition 8.0</li> </ul>
<b>Repository-Datenbankserver</b>	<ul style="list-style-type: none"> <li>• Oracle 9i</li> </ul>

Softwarekategorie	Softwarepaket
<b>Ressourcen</b>	<ul style="list-style-type: none"> <li>• BridgeStream SmartRoles</li> <li>• HP OpenVMS 7.2</li> <li>• IBM AIX 4.3.3</li> <li>• IBM Tivoli Access Manager 4.x</li> <li>• INISafe Nexess</li> <li>• Microsoft Active Directory 2000</li> <li>• Microsoft Exchange 2000</li> <li>• Microsoft SQL Server 2000</li> <li>• Microsoft Windows Server 2000</li> <li>• MySQL 4.x</li> <li>• Lotus Notes 6.5</li> <li>• Oracle 9i</li> <li>• Red Hat Linux Enterprise Server</li> <li>• SAP Governance, Risk and Compliance Access Enforcer 5.1</li> <li>• SecurID 5.0, 5.1</li> <li>• Siebel 7.0.4</li> <li>• Solaris 8</li> <li>• Sun Access Manager 6 (2005Q1)</li> <li>• Sun Java System Identity Server 2004Q2</li> <li>• Sun ONE Identity Server 6.1, 6.2</li> <li>• Sun ONE Directory Server 4.x</li> <li>• Windows 2000 SP3, 2000 SP4</li> </ul>
<b>Browser</b>	<ul style="list-style-type: none"> <li>• Firefox 1.0.x</li> <li>• Mozilla</li> </ul>

## Identity Manager 8.0

Die folgende Software wird bereits in Identity Manager 8.0 nicht mehr unterstützt:

Softwarekategorie	Softwarepaket
<b>Betriebssysteme</b>	<ul style="list-style-type: none"> <li>• IBM AIX 4.3.3</li> <li>• Solaris 7</li> </ul>

<b>Softwarekategorie</b>	<b>Softwarepaket</b>
<b>Anwendungsserver</b>	<ul style="list-style-type: none"> <li>• Apache Tomcat 4.1.x, 5.0.x</li> <li>• BEA Weblogic Express 7, 8.1</li> <li>• BEA Weblogic Server 7, 8.1</li> <li>• IBM Websphere Application Server - Express Version 5.1.1</li> <li>• IBM Websphere 4, 4.5, 5, 6.0</li> <li>• iPlanet 6.5</li> <li>• Sun ONE Application Server 7</li> </ul>
<b>Repository-Datenbankserver</b>	<ul style="list-style-type: none"> <li>• IBM DB2 Universal Database für Linux, UNIX und Windows 7.x</li> <li>• Microsoft SQL 2000</li> <li>• MySQL 4.1</li> <li>• Oracle 8i</li> <li>• SQL Server 2000</li> </ul>
<b>Ressourcen</b>	<ul style="list-style-type: none"> <li>• ActivCard 5.0</li> <li>• Blackberry RIM Enterprise Server 4+ (verwendet Generic Windows Script Adapter) und Blackberry Enterprise Server-Skripten</li> <li>• IBM DB2 7.x</li> <li>• Lotus Notes (Domino) 5.0, 6.0.x</li> <li>• Microsoft Exchange 5.5</li> <li>• Microsoft Windows NT 4.0</li> <li>• MySQL 4.1</li> <li>• Natural</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 Identity Manager Gateway auf Microsoft Windows NT 4.0</li> <li>• Sun ONE Identity Server 6.0</li> </ul>
<b>Browser</b>	<ul style="list-style-type: none"> <li>• Internet Explorer 5.x</li> <li>• Safari 1.2.1+</li> </ul>

## API-Unterstützung

Die API (Application Programming Interface, Anwendungsprogrammierschnittstelle) aus Identity Manager 8.0 umfasst alle in der nachstehenden Tabelle aufgeführten öffentlichen Klassen (sowie alle öffentlichen oder geschützten Methoden oder Felder der öffentlichen Klassen).

---

**HINWEIS** `com.waveset.object.RepositoryProxy` ist nur zur internen Verwendung gedacht.

---

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

---

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

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.

### Veraltete APIs (Unterstützung eingestellt)

Der Abschnitt „[Veraltete APIs \(Unterstützung eingestellt\)](#)“ enthält alle Identity Manager-APIs (Application Programming Interfaces), deren Unterstützung in dieser Version eingestellt wurde. Außerdem werden deren Nachfolger aufgelistet, falls verfügbar.

# Aufrüstungsmöglichkeiten und Supportrichtlinien

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.

## Aufrüstungsmöglichkeiten für Identity Manager

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

**HINWEIS** Die Aufrüstung auf Identity Manager 8.0 wird empfohlen. Durch das Aufrüsten auf die neueste Softwareversion profitieren Sie von den neuesten Funktionen und Fehlerkorrekturen sowie von der Unterstützung für aktuelle Ressourcenversionen.

Aktuelle Identity Manager-Version	Zielversion von Identity Manager					
	2005Q3M1	2005Q4M3	7.0	7.1	7.1 Update 1	8.0
Identity Manager 5.0 SPx	2005Q3M1	2005Q4M3	2005Q4M3 > 7.0	2005Q4M3 > 7.1	2005Q4M3 > 7.1 > 7.1 Update 1	2005Q4M3 > 7.1 > 8.0
Identity Manager 2005Q1M3	2005Q3M1	2005Q4M3	2005Q4M3 > 7.0	2005Q4M3 > 7.1	2005Q4M3 > 7.1 > 7.1 Update 1	2005Q4M3 > 7.1 > 8.0
Identity Auditor 1.0						
Identity Manager 2005Q3M1		2005Q4M3	2005Q4M3 > 7.0	2005Q4M3 > 7.1	2005Q4M3 > 7.1 > 7.1 Update 1	2005Q4M3 > 7.1 > 8.0
Identity Manager 2005Q3M3		2005Q4M3	2005Q4M3 > 7.0	2005Q4M3 > 7.1	2005Q4M3 > 7.1 > 7.1 Update 1	2005Q4M3 > 7.1 > 8.0
Identity Manager SPE 1.0						
2005Q4M3 (6.0)			7.0	7.1	7.1 > 7.1 Update 1	7.1 > 8.0
Identity Manager 7.0				7.1	7.1 > 7.1 Update 1	8.0
Identity Manager 7.1					7.1 Update 1	8.0

- 
- HINWEIS**
- Bei der Aufrüstung von Identity Manager ist es nicht erforderlich, innerhalb einer Hauptversion zum Aufrüsten auf die nächste Hauptversion Updates (*früher Service Packs bzw. SP* genannt) zu installieren. Wenn Sie z. B. von Identity Manager 5.0 auf 6.0 aufrüsten, müssen Sie keine der 5.0 Service Packs installieren.
  - Updates sind für eine Hauptversion kumulierend. Nach der Aufrüstung auf die Hauptversion können Sie daher das letzte Update installieren, ohne alle für diese Version herausgegebenen Updates (bzw. Service Packs) installieren zu müssen. Wenn Sie z. B. auf Identity Manager 5.0 aufgerüstet haben, erhalten Sie durch die Installation von SP6 die gesamte Funktionalität, die in den Service Packs SP1 bis SP5 enthalten ist.
  - Das Identity Manager Installation Pack 2005Q4M3 (Version 6.0) war eine Hauptversion. Wenn Sie eine frühere Version von Identity Manager, Identity Auditor oder Identity Manager Service Provider als 6.0 verwenden und aufrüsten möchten, müssen Sie zunächst auf Identity Manager Installation Pack 2005Q4M3 aufrüsten, bevor Sie die aktuelleren Versionen installieren können.
- 

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 Updates**: 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.

---

## Vollständige Support-Phase

In der Phase mit vollem Support gewährt Sun Microsystems, Inc. Softwaresupport gemäß dem Support-Vertrag (einschließlich der jeweiligen 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.

## Beschränkte Support-Phase

In der Phase mit beschränktem Support gewährt Sun Microsystems, Inc. Softwaresupport gemäß dem Support-Vertrag (einschließlich der jeweiligen 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, Fehlerberichte 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 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	25.05.2007	25.05.2008	05/2012	20.11.06
Sun Java System Identity Auditor 1.0 2005Q1	Post-RR	02.02.2007	02/2008	02/2012	01.08.06
Sun Java System Identity Manager Service Provider Edition 1.0 2005Q3	Post-RR	02.02.2007	02/2008	02/2012	01.08.06
Sun Java System Identity Manager 5.0 2004Q3	EOL	11.08.2006	08/2007	08/2011	07.02.06
Sun Java System Identity Manager 5.0 SPx 2004Q3	EOL	11.08.2006	08/2007	08/2011	07.02.06
Sun Java System Identity Manager 5.5	EOL	11.08.2006	08/2007	08/2011	07.02.06
Waveset Lighthouse 4.1			03/2006	03/2010	

## Identity Manager-Richtlinie zur Einstellung der Unterstützung für bestimmte Funktionen

Im Dokument *Identity Manager Upgrade* finden Sie vollständige Informationen darüber, welche Richtlinien in Identity Manager gelten, wenn die Unterstützung für bestimmte Schnittstellen oder Funktionen eingestellt wird.

---

## Weitervertreibbare Dateien

Sun Java System Identity Manager 8.0 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 anderer 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 Bestellnummer 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 Mai 2008 Versionshinweise und die Teilenummer 820-5437-10.

---

## Zusätzliche Sun-Ressourcen

Nützliche Informationen zu Sun Java System finden Sie auf den folgenden Internetadressen:

- Dokumentation für Sun™ Identity Manager  
<http://docs.sun.com/app/docs/prod/ident.mgr#hic>
- 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 © 2008 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, USA. 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.

DIESES PRODUKT ENTHÄLT VERTRAULICHE INFORMATIONEN UND GESCHÄFTSGEHEIMNISSE VON SUN MICROSYSTEMS, INC. VERWENDUNG, OFFENLEGUNG ODER REPRODUKTION IST OHNE VORHERIGE SCHRIFTLICHE GENEHMIGUNG DURCH SUN MICROSYSTEMS, INC., NICHT GESTATTET.

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

Die Nutzung unterliegt Lizenzvereinbarungen.

Diese Ausgabe kann von Drittanbietern entwickelte Bestandteile enthalten.

Sun, Sun Microsystems, das Sun Logo, Java, Solaris, Sun Java System Identity Manager, Sun Java System Identity Manager Service Provider Edition Services, Sun Java System Identity Manager Service Provider Edition Software und Sun Identity Manager 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. Produkte mit SPARC-Marken basieren auf einer Architektur, die von Sun Microsystems, Inc. entwickelt wurde.

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

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

# Identity Manager 8.0-Funktionen

In diesem Abschnitt der Identity Manager 8.0-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 8.0. Die Informationen sind in die folgenden Abschnitte unterteilt:

- [Hauptfunktionen](#)
- [Administrator- und Benutzeroberflächen](#)
- [Überwachung](#)
- [Data Exporter](#)
- [Formulare](#)
- [Identity Manager Business Process Editor \(BPE\)](#)
- [Integrierte Entwicklungsumgebung von Identity Manager \(Identity Manager-IDE\)](#)
- [Installation](#)
- [Passwortsynchronisation](#)
- [Berichte](#)
- [Repository](#)
- [Ressourcen](#)
- [Rollen](#)
- [Szenarien](#)
- [Sicherheit](#)
- [Server](#)
- [SPML](#)
- [Synchronisation](#)
- [Sonstiges](#)

## Suns neuer Patch-Prozess

Ab der Version Identity Manager 7.1 Update 1 werden Updates mit Korrekturen für schwerwiegende und kritische Probleme, die von Kunden gemeldet wurden, über einen neuen *Patch-Prozess* bereitgestellt. Dieser löst den älteren Hotfix-Prozess ab.

Patches werden in einem 6-Wochen-Turnus entwickelt, getestet und veröffentlicht. Die Patches verfügen über ein Installationsprogramm mit grafischer Oberfläche, können aber auch manuell über die Befehlszeile installiert werden. Sie aktualisieren die Dateien in `/WEB-INF/lib`. Installationsanweisungen für einen Patch sind in den dazugehörigen Versionshinweisen (PDF-Datei) enthalten. Falls Korrekturen an den Gateway- oder Password-Sync-Komponenten erforderlich sind, wird dies ebenfalls in den Versionshinweisen beschrieben. In diesem Fall muss die entsprechende Aktualisierung bei der Patch-Installation vorgenommen werden.

Die Identity Manager-Patches sind kumulativ, d. h. es sind weniger Probleme mit einzelnen Fehlerkorrekturen zu erwarten. Wenn Sie eine Haupt- oder Nebenversion installieren oder darauf aufrüsten, sollten Sie gleichzeitig den neuesten Patch einspielen. Wenn Sie z. B. die Version 8.0 installieren (oder darauf aufrüsten) möchten und dafür der Patch 3 zur Verfügung steht, sollten Sie diesen installieren, nachdem Sie die Version 8.0 installiert haben. In diesem Fall müssen Sie die Patches 1 und 2 nicht gesondert installieren, da der Patch 3 alle darin enthaltenen Funktionen und Korrekturen bereits enthält.

Mit dem Patch-Prozess wird es auch einfacher, den Status einer Fehlerkorrektur über die dazugehörige Fehlernummer zu verfolgen. Dennoch kann es vorkommen, dass eine Korrektur aus einer älteren Version in einer neueren Version noch nicht verfügbar ist. Unabhängig von dem Prozess, den Ihre aktuelle Identity Manager-Version verwendet, müssen Sie sich daher immer vergewissern, dass die neue Zielversion von Identity Manager alle Korrekturen enthält, die Sie brauchen.

Bei der Veröffentlichung eines neuen Patches wird der gesamte Kundendienst/Support darüber informiert. Alle Patches stehen über den Kundendienst zur Verfügung. Um den jeweils neuesten Patch zu erhalten, wenden Sie sich bitte an den Sun Kundendienst unter <http://www.sun.com/service/online/us>.

## Hauptfunktionen

Identity Manager 8.0 bietet die folgenden neuen Hauptfunktionen:

- [Verbesserungen an den Rollenfunktionen](#)
- [Verbesserte Berichtsfunktionen \(Data Exporter\)](#)
- [Attributkonfiguration](#)

## Verbesserungen an den Rollenfunktionen

Identity Manager 8.0 bietet jetzt ein Lifecycle-Management für Rollen. Das Erstellen, Bearbeiten und Löschen von Rollen kann damit von einer entsprechenden Änderungsgenehmigung abhängig gemacht werden. Änderungen an Rollen können für alle damit verknüpften Benutzer übernommen werden. Das Lifecycle-Management für die Benutzer-Rollenzuweisung wurde ebenfalls verbessert und unterstützt jetzt auch zukünftige und temporäre Rollenzuweisungen. Neue Rollentypen mit konfigurierbaren Funktionen (standardmäßig Geschäftsrollen, IT-Rollen, Anwendungen und Assets) sollen helfen, Best Practices in der Rollenverwaltung umzusetzen. So können z. B. Geschäftsrollen Rollen enthalten, die für alle Benutzer erforderlich sind, darüber hinaus aber für bestimmte Benutzer nur bedingt gelten sollen und/oder von anderen Benutzern optional (ggf. abhängig von einer Genehmigung) angefordert werden können. So kann der Entwickler der Geschäftsrolle den Zugriff bereits grobkörnig vorgeben, gleichzeitig aber dem Benutzer bzw. dessen Manager die Möglichkeit geben, die endgültige Feinabstimmung der Zugriffsrechte vorzunehmen.

## Verbesserte Berichtsfunktionen (Data Exporter)

Mit der neuen Funktion „Data Exporter“ werden Vorgangsdaten, die von Identity Manager verwendet und produziert werden, auch für andere Prozesse und Anwendungen verfügbar. Mit dieser Funktion können Daten, die in Identity Manager gespeichert sind bzw. diesen durchlaufen, turnusmäßig in ein externes Data-Warehouse-System oder Business-Intelligence- und Reporting-Werkzeuge exportiert werden. Die Data-Exporter-Funktion ist optional. Sofern sie aktiviert ist, kann der Benutzer konfigurieren, welche Daten wann exportiert werden. Mit den Exportdaten lassen sich dann Fragen der Art „Wer hatte Zugriff auf Ressource X, und wer hat diesen Zugriff genehmigt?“ beantworten. Außerdem lassen sich auf dieser Basis Berichte zum Identity Manager-Betrieb erstellen, z. B. „Ressourcenvorgänge nach Ressource“ oder „Reaktionszeiten für manuelle Aktionen im Workflow“. Indem Vorgangsdaten (im Identity Manager-Repository gespeichert) und historische Daten (von der Data-Exporter-Funktion exportiert) voneinander entkoppelt werden, hat der Benutzer volle Kontrolle über die Verwendung dieser Daten. Da die Daten nach einem dokumentierten, schemakonformen Verfahren bereitgestellt werden, kann der Benutzer außerdem Analyseprozesse entwickeln und verwenden, die auch mit zukünftigen Versionen von Identity Manager kompatibel sind.

## Attributkonfiguration

Erweiterte, abfragbare und Übersichtsattribute können jetzt für Rollen und Benutzer konfiguriert werden. Die neue Konfiguration für erweiterte Attribute unterstützt die Angabe einer Wertsyntax (STRING, INT, DATE, oder BOOLEAN) sowie einer Textbeschreibung. Außerdem kann festgelegt werden, ob das Attribut einzelne oder mehrere Werte haben kann.

## Administrator- und Benutzeroberflächen

- Über die Seite „Formular- und Prozesszuordnungen konfigurieren“ können Benutzer jetzt ein benutzerdefiniertes Formular für die fragenbasierte bzw. anonyme Anmeldung festlegen. (ID-4697)
- Die Oberfläche für die Rollenverwaltung wurde um die neuen Rollenfunktionen erweitert. Nähere Informationen finden Sie im Kapitel „Roles and Resources“ im Dokument *Identity Manager Administration 8.0*. (ID-15518)
- Standardmäßig sind Prozessdiagramme in dieser Version von Identity Manager deaktiviert. Sie können sie aktivieren, indem Sie das Systemkonfigurationsobjekt bearbeiten und den bzw. die Anwendungsserver neu starten. Eine Anleitung finden Sie im Abschnitt „Enabling Process Diagrams“ im Dokument *Identity Manager Administration 8.0*. (ID-16337)
- Auf der Seite „Abstimmungsrichtlinie bearbeiten“ wurde eine optionale Sicherung eingebaut. Diese Sicherung ermittelt die Anzahl fehlender Konten auf einer Ressource. Falls ein bestimmter Schwellenwert überschritten wird, hindert sie das Abstimmungsprogramm daran, die Konten zu trennen. Nähere Informationen finden Sie im Kapitel „Data Loading and Synchronization“ im Dokument *Identity Manager Administration 8.0*. (ID-16391)
- Identity Manager verhält sich jetzt anders, wenn Benutzer mit ausstehenden Arbeitselementen gelöscht werden sollen. Nähere Informationen finden Sie im Dokument *Identity Manager Administration 8.0*, Kapitel „Administration“, Abschnitt „Managing Work Items“, Unterabschnitt „Delegations to Deleted Users“. (ID-16417)
- Beim Definieren von AdminRole-Rollen kann jetzt ein Kontrollkästchen namens **Alle gesteuerten untergeordneten Organisationen und enthaltene Objekte ausschließen** aktiviert werden, um alle untergeordneten kontrollierten Organisationen und die darin enthaltenen Objekte aus der Verwaltungsbefugnis auszuschließen. Wenn dieses Kontrollkästchen deaktiviert ist, hat ein Benutzer mit der betreffenden AdminRole-Rolle auch Verwaltungsbefugnis für alle untergeordneten Organisationen und deren Inhalt. (ID-16859)
- Admin-Rollen werden jetzt als Namen in Suchergebnissen angezeigt. (ID-17130)
- In Identity Manager 8.0 wurden die Ergebnisseiten in der Endbenutzeroberfläche dahingehend vereinfacht, dass nur noch eine Statusmeldung angezeigt wird. Beim Aufrüsten von einer Vorgängerversion werden standardmäßig die ursprünglichen Prozessdiagramme beibehalten. Bei neuen Installationen wird hingegen die Statusmeldung angezeigt. Um standardmäßig die Prozessdiagramme anzuzeigen, klicken Sie auf „Konfigurieren“ -> „Benutzeroberfläche“ und aktivieren die Einstellung „Endbenutzer-Prozessdiagramme aktivieren“.

Die Prozessdiagramme für die Endbenutzeroberfläche können nur aktiviert werden, wenn sie auch für das Produkt insgesamt aktiviert sind. Nähere Informationen hierzu finden Sie unter ID-16337 im Abschnitt [Administrator- und Benutzeroberflächen](#). (ID-17365)

- Das Anmeldeformular für Endbenutzer wurde vereinfacht und umgestaltet, sodass es jetzt einfacher zu bedienen ist.  
Hierzu wurde die JSP-Datei `user/login.jsp` geändert. Wenn diese Datei in der Vorgängerversion angepasst wurde, müssen diese Anpassungen nach dem Upgrade manuell in die neue Version übernommen werden. (ID-17368)
- Auf dem neuen Endbenutzer-Standardformular zur Passwortänderung können Benutzer ihr Passwort ändern. Auf diesem Formular werden die Passwortrichtlinien für alle Ressourcen zusammengefasst, die dem Benutzer zugewiesen sind. Passwortänderungen gelten dann für alle zugewiesenen Ressourcen. Das ursprüngliche, einfache Passwortänderungsformular sollte gewählt werden, wenn der Benutzer auswählen können soll, für welche Ressourcen die Passwortänderung gilt. (ID-17371)
- Die Fehlermeldung, die dem Benutzer bei der Anmeldung angezeigt wird, wenn Authentifizierungsfragen beantwortet werden müssen, wird jetzt als Warnmeldung dargestellt. (ID-17549)
- Wenn die Funktion „Anonyme Anmeldung“ aktiviert ist, erscheint auf der Endbenutzer-Oberfläche keine Schaltfläche „Konto anfordern“ mehr. Stattdessen wird der Text „Neuer Benutzer?“ mit einem Link „Konto anfordern“ angezeigt. Unter dem Link erscheinen weitere Informationen. Der Text auf dieser Seite kann angepasst werden. Nähere Informationen finden Sie im Dokument *Identity Manager Technical Deployment Overview*. (ID-17582)
- Die DatePicker-Anzeigekomponente hat jetzt eine Eigenschaft `disableTextInput`. Wenn diese Eigenschaft aktiviert ist, kann der Benutzer keine Eingaben mehr über ein Textfeld machen, sondern muss ein Datum über den Popup-Kalender auswählen. (ID-17586)

## Überwachung

- Überwachungsprotokolleinträge zu Aktionen im Zusammenhang mit der Bereitstellung von Ressourcenkonten sind jetzt für Überwachungsadministratoren der Objektgruppen sichtbar, die die betreffenden Ressourcen enthalten. Dies gilt unabhängig davon, ob diese Gruppen den Benutzer enthalten, den die Aktion betrifft. (ID-17724)
- E-Mail-Benachrichtigungsereignisse werden jetzt überwacht. In der Administratoroberfläche gibt es auf der Überprüfungs konfigurationsseite (**Konfigurieren** > **Überwachung**) eine neue Überprüfungsgruppe namens *Ereignisverwaltung*. (ID-17734)

## Data Exporter

- Mit der Funktion „Data Exporter“ können Daten aus Identity Manager turnusmäßig zur Weiterverarbeitung in ein externes Data-Warehouse-System exportiert werden.

## Formulare

- Für Felder mit einem Bestätigungseigenschaftswert, der sich auf eine Quellkomponente bezieht (z. B. das Feld „Passwort bestätigen“ auf dem Registerformular für Benutzer), wird der Wert nicht mehr automatisch auf den Wert der Quellkomponente gesetzt, wenn dieser beim Absenden des Formulars an den Server Null ist. Wenn ein Paar aus einem Quell- und einem Bestätigungsfeld einen Standardausdruck hat, sollten Sie daher sicherstellen, dass dieser sowohl auf das Quell- als auch das Bestätigungsfeld angewendet wird. (ID-17838)

## Identity Manager Business Process Editor (BPE)

- Der Business Process Editor (BPE) wird eingestellt und ist in der nächsten Identity Manager-Hauptversion nicht mehr enthalten. Verwenden Sie stattdessen die Identity Manager Integrated Development Environment (Identity Manager-IDE). (ID-17510)

## Integrierte Entwicklungsumgebung von Identity Manager (Identity Manager-IDE)

- Die Identity Manager Integrated Development Environment (Identity Manager-IDE) wird nun unter <https://identitymanageride.dev.java.net> bereitgestellt. Auf derselben Website finden Sie auch Anleitungen zu Installation, Konfiguration und zum Migrieren von Projekten. (ID-17700)

## Installation

- In dieser Identity Manager-Version werden die folgenden Anwendungsserver nicht mehr unterstützt: (ID-16369)
  - Apache Tomcat Version 4.1.x
  - BEA Weblogic Express 8.1
  - BEA Weblogic Server 8.1
  - IBM Websphere Application Server - Express Version 5.1.1
  - IBM Websphere 6.0
  - Sun ONE Application Server 7

## Passwortsynchronisation

- PasswordSync-Versionen vor Version 7.1.1 sollten auf allen Domänen-Controllern zumindest auf Version 7.1.1 aktualisiert werden.

Die Unterstützung für das rpcrouter2-Servlet wird in Version 8.0 eingestellt und in einer zukünftigen Version ganz entfernt. PasswordSync 7.1.1 und höher unterstützen das neue Protokoll.

Informationen zur Installation von PasswordSync finden Sie im Buch *Identity Manager Administration*.

- Es gibt separate Installationsprogramme für die 32- und 64-Bit-Version von PasswordSync. Das 32-Bit-Installationsprogramm kann jetzt nur unter 32-Bit-Versionen von Windows ausgeführt werden, das 64-Bit-Installationsprogramm nur unter 64-Bit-Versionen. Wenn Sie versuchen, das falsche Installationsprogramm zu starten, führt dies zu einem Fehler. (ID-17290)

## Berichte

- Identity Manager-Einsatzberichte und Identity Auditor-Richtlinienverletzungsberichte enthalten beim Download im PDF-Format jetzt Diagramme. (ID-10719)
- Ein neuer Bericht namens „Bericht für einzelnen Benutzerüberprüfungsprotokoll“ steht zur Verfügung. Wie bei den Überprüfungsprotokollberichten beruht auch dieser Bericht auf Ereignissen aus dem System-Überwachungsprotokoll. Er gibt jedoch nur die Aktivitäten zurück, die im Zusammenhang mit einem bestimmten, frei wählbaren Benutzer ausgeführt wurden. Nähere Informationen finden Sie im Kapitel „Reporting“ im Dokument *Identity Manager Administration 8.0*. (ID-16976)
- Bei der Überwachungsberichtsauflage (und anderen Berichten, die die LogRecordFormatter-Komponente verwenden) kann jetzt ausgewählt werden, welche Spalten im Bericht erscheinen. Verwenden Sie hierzu die Attribute `useCustomColumns` und `customColumns` in der Aufgabendefinition und -vorlage. (ID-17712)
- Sie können Berichte jetzt so anpassen, dass auch Administratoren, die lediglich Fähigkeiten zum Ausführen von Berichten haben, vor dem Ausführen des Berichts die Berichtparameter festlegen können. (ID-17733) Hierdurch können solche Administratoren die Berichtparameter festlegen, bevor sie den Bericht ausführen oder als CSV-/PDF-Datei herunterladen. Identity Manager speichert diese Änderungen nicht in der Berichtsdefinition.

Um diese Funktion für vorhandene Berichte zu aktivieren, fügen Sie der Aufgabenvorlage das Feld `alwaysProcessForm` hinzu und setzen es auf den Wert `true`. Um einem neuen Bericht (außer „Bericht für einzelnen Benutzerüberprüfungsprotokoll“) diese Funktion hinzuzufügen, fügen Sie in das Aufgabendefinitions-Startformular ein Feld namens `alwaysProcessForm` mit dem Wert `true` ein.

Der Administrator, der einen Bericht mit `alwaysProcessForm = true` ausführt, muss die nötigen Fähigkeiten haben, um die gewünschten Daten aus dem Repository abzurufen. Bei einem Bericht über Rollen muss der Administrator z. B. die Fähigkeit zum Abrufen einer Liste verfügbarer Rollen haben.

- Sie können auswählen, welche Spalten im Bericht „Individueller Benutzerüberprüfungsbericht“ (und anderen Berichten mit dem Executor `com.waveset.report.AuditReportTask`) angezeigt werden. Verwenden Sie hierzu die Attribute `useCustomColumns` und `customColumns` in der Aufgabendefinition und -vorlage. Bei anderen Berichten als dem individuellen Benutzerüberprüfungsbericht müssen hierzu die `taskDefinition`- und `TaskTemplate`-Objekte aktualisiert werden (durch Hinzufügen der Funktion „`customColumns`“). (ID-17744)
  - `useCustomColumns --` (Boolescher Wert) Legt fest, ob die benutzerdefinierte Spaltenauswahl aktiviert ist.
  - `customColumns --` (Zuordnung) Legt fest, welche Spalten der Bericht enthalten soll. *Schlüssel* und *Wert* sind dabei jeweils ein Schlüssel bzw. Wert im Nachrichten katalog.

Als Beispiel für die Arbeit mit diesen Funktionen können Sie sich den individuellen Benutzerüberprüfungsbericht ansehen.
- Für Identity Manager-Administratoren, die nur über die Fähigkeit „Überwachungsbericht ausführen“ verfügen, stehen die Download-Schaltflächen jetzt auf der Haupt-Berichtsseite zur Verfügung. (ID-17881)

## Repository

- Bei Identity Manager-Installationen, die eine Oracle-Datenbank als Repository verwenden, kann das Feld „`accountAttrChanges`“ in der Überwachungsprotokoll-Tabelle von `VARCHAR(4000)` in `CLOB` umgewandelt werden. Diese Umstellung ist optional und sollte nur vorgenommen werden, wenn Sie im Überwachungsprotokoll „abgeschnittene“ Daten finden. Ein DDL-Beispielskript finden Sie unter `web/sample/convert_log_acctAttrChangesCHAR2CLOB.oracle.sql`. Erstellen Sie eine Sicherungskopie der betroffenen Tabellen, bevor Sie das Skript ausführen. (ID-17343)

## Ressourcen

### Neue Ressourcenadapter

In dieser Version wurden die folgenden neuen Ressourcenversionen hinzugefügt:

- Der Sybase ASE-Ressourcenadapter ersetzt den Sybase-Ressourcenadapter, dessen Unterstützung eingestellt wurde. Der Sybase ASE-Adapter bietet die Möglichkeit, Benutzer in mehreren Datenbanken zu verwalten. (ID-16872)

## Aktualisierungen bei Ressourcenadaptern

- Die Mainframe-Adapter unterstützen IBM Host on Demand V10. (ID-6419)
- Im Ressourcen-Assistent für den Microsoft SQL Server-Adapter wurde die Auswahl der Datenbanken vereinfacht. Die Attribute `userName$(dbName)` und `roles$(dbName)` im Schema werden automatisch entsprechend aktualisiert. (ID-8546)
- Die SAP-Adapter können jetzt internationalisierte Meldungen anzeigen. (ID-9077)
- Die Klasse `com.waveset.adapter.AttrParse` wurde entfernt. Verwenden Sie stattdessen die Klasse `com.waveset.object.AttrParse`. (D-11870)
- Die UNIX-Adapter unterstützen jetzt SSHPubKey-Verbindungen. Mit dieser neuen Funktion können Benutzer von vertrauenswürdigen Rechnern aus Verbindungen zu Remote-Hosts aufbauen, ohne ein Passwort einzugeben. (ID-11959)
- Der SAP-Adapter unterstützt die Bereitstellung in jeder SAP-Tabelle, die von `BAPI_USER_CREATE1` und `BAPI_USER_CHANGE` aufgerufen wird, insbesondere die Tabellen `GROUPS` und `PARAMETER`. (ID-12217)
- In Kontennamen ist jetzt das Sonderzeichen `@` zulässig, sofern die betreffende Ressource dies ebenfalls unterstützt. (ID-12383)

Ressourcennamen und -IDs dürfen das Zeichen `@` *nicht* enthalten. Anderenfalls interpretiert Identity Manager die Ansichts-ID falsch.

- Den Ressourcen „RACF“ und „RACF\_LDAP“ wurde ein neues boolesches Kontenattribut „TSO.Delete Segment“ hinzugefügt. Wenn dieses Attribut auf den Wert „true“ gesetzt ist, wird das TSO-Segment aus dem RACF-Benutzer gelöscht. (ID-13347)

Wenn Sie bei einem Upgrade dieses Attribut einschließen möchten, fügen Sie das folgende Element in den Abschnitt `AccountAttributes` der Ressourcendefinition ein:

```
<AccountAttributeType id='<nächste fortlaufende ID>' name='Delete TSO Segment'  
syntax='boolean' mapName='TSO.Delete Segment' mapType='boolean' writeOnly='true'>
```

- Die Adapter „RACF“ und „RACF\_LDAP“ können so konfiguriert werden, dass sie auch Attribute unterstützen, die sich nicht in den standardmäßig unterstützten Segmenten befinden. (ID-13351)
- Der SAP-Ressourcenadapter gibt jetzt die Liste der verfügbaren Benutzertypen und -gruppen zurück. (ID-16123)
- Dasselbe Gateway kann jetzt für die Bereitstellung und für die Pass-Through-Authentifizierung verwendet werden (NetWare-Konten). Weitere Informationen zum Umsetzen dieser Funktion finden Sie im Dokument *Identity Manager Resources Reference*. (ID-16584)

- Mit dem Ressourcenparameter **Siebel 8.0 nextRecord()-Fehler ignorieren** kann festgelegt werden, dass der Siebel CRM-Adapter den nextRecord()-Fehler ignorieren soll, der unter Siebel 8.0 auftritt. Nähere Informationen zu diesem Fehler finden Sie im Siebel Alert 1315. (ID-16779, 18159)
- Der SAP-Adapter versucht nicht, Konten umzubenennen, wenn das Ressourcenattribut **CUA aktivieren** auf den Wert „true“ gesetzt ist. (SAP unterstützt im CUA-Modus keine Umbenennungen.) (ID-16986)
- Der Datenbanktabellen-Ressourcenadapter unterstützt jetzt das Umbenennen von Konten. (ID-16993)
- Der SAP-Adapter wurde um den Ressourcenparameter **Anzahl der pro Verbindung gelesenen Benutzer** erweitert. Dieser Parameter stellt sicher, dass belegter Speicher zeitnah wieder freigegeben wird. (ID-17017)
- Der Solaris-Ressourcenadapter kann nun erzwingen, dass Benutzer ihre Passwörter bei der nächsten Anmeldung ändern. Um diese Funktion zu aktivieren, fügen Sie `expirePassword` in die Spalte „Identity System-Benutzerattribut“ der Schemazuordnung und `force_change` in die Spalte „Ressourcen-Benutzerattribut“ ein. Dieser Attributtyp muss auf „String“ gesetzt werden. (ID-17032)
- Die Adapter für SAP, SAP HR und AccessEnforcer (zugrunde liegende SAP-Implementierung) unterstützen jetzt Secure Network Communications (SNC). Weitere Informationen zum Umsetzen dieser Funktion finden Sie im Dokument *Identity Manager Resources Reference*. (ID-17059)
- Der integrierte Identity Manager-Pool für JDBC-Verbindungen unterstützt jetzt ein Leerlauf-Timeout. Verbindungen im Pool, die über diese maximale Leerlaufdauer hinaus nicht verwendet werden, werden geschlossen und verworfen. (ID-17107)

Beim Aufrüsten auf die Version 8.0 wird für vorhandene Ressourceninstanzen der folgenden Adapter automatisch eine maximale Leerlaufdauer von 600 Sekunden (10 Minuten) festgelegt:

- Datenbanktabelle
- Microsoft SQL Server
- MIIS
- Oracle ERP
- Oracle
- Skript-JDBC
- Sybase ASE

Benutzerdefinierte Ressourcenadapter, die JdbcResourceAdapter erweitern, können diese neue Funktion ebenfalls nutzen. Hierzu müssen sie um ein neues Ressourcenattribut namens `idleTimeout` erweitert werden.

Auf der Seite `debug/Show_JDBC.jsp` werden jetzt ebenfalls Zusatzinformationen zum Leerlauf-Timeout angezeigt.

- Der SAP-Adapter von Identity Manager unterstützt jetzt die Kontenattribute „`accountLockedNoPwd`“ und „`accountLockedWrngPwd`“. Das Attribut „`accountLockedNoPwd`“ gibt an, ob das Konto gesperrt ist, weil der Benutzer kein Passwort hat. Das Attribut „`accountLockedWrngPwd`“ gibt an, ob das Konto aufgrund von fehlgeschlagenen Anmeldeversuchen gesperrt wurde. (ID-17296)
- Die Klasse „HostAccess“ wurde um die Methode `sendKeys(EncryptedData)` erweitert. Diese kann verwendet werden, um zu vermeiden, dass Passwörter protokolliert werden. (ID-17544)
- Der Datenbanktabellen-Adapter verarbeitet den Oracle-Datentyp „`timestamp`“ korrekt, wenn Sie das Kontrollkästchen **Native Zeitstempel** auf der Seite „Ressourcenparameter“ aktivieren. (ID-17551)
- Für den Adapter „JMS Listener“ steht jetzt der neue Ressourcenparameter **Zeitüberschreitung beim Empfang** zur Verfügung. Hiermit können Sie konfigurieren, wie lang der Adapter auf eine eingehende Meldung wartet, bevor der Abruf abgebrochen wird. Der Standardwert beträgt 10 Sekunden. (ID-17935)
- Der Adapter „JMS Listener“ baut jetzt für jeden Abruf eine neue Verbindung auf. (ID-17941)
- Der Adapter „JMS Listener“ kann jetzt mit Java Management Extensions (JMX) überwacht werden. (ID-17943)
- Bei Passwortänderungen in NDS Groupwise werden verschlüsselte Passwörter jetzt korrekt verarbeitet. (ID-18020)
- Für Sun Access Manager-Ressourcen im Vorgängermodus gibt es jetzt den neuen Ressourcenparameter „Suchumfang“. Dieses Attribut legt den Umfang von Suchen in Access Manager-Objekten fest. Zulässige Werte sind „`oneLevel`“ und „`subTree`“. Der Standardwert ist „`subTree`“. (ID-18079)

# Rollen

- Für jede Rolle können Eigentümer entweder statisch oder dynamisch über eine Regel festgelegt werden. (ID-10602)
- 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.

- Die Rollenverwaltung in Identity Manager wurde stark überarbeitet. Durch neue Funktionen gibt es jetzt viel umfassendere Möglichkeiten für ein Lifecycle-Management sowohl für Rollen als auch für die Benutzer-Rollenzuweisung. Identity Manager unterstützt jetzt vier Rollentypen: Geschäftsrollen, IT-Rollen, Anwendungen und Assets. Beim Aufrüsten von einer früheren Identity Manager-Version auf Identity Manager 8.0 werden die alten Rollen automatisch in IT-Rollen umgewandelt. Ausführliche Informationen zur Funktionsweise von Rollen in Identity Manager 8.0 finden Sie im Kapitel „Roles and Resources“ im Dokument *Identity Manager Administration 8.0*. (ID-17677)
- Die Oberfläche zur Rollenverwaltung bietet jetzt die Möglichkeit, Änderungen an Rollen für die damit verknüpften Benutzer zu übernehmen. (ID-17719)
- Der Benutzerzusammenfassungsbericht und die Rollenberichte enthalten jetzt mehr Informationen zu Rollen und Rollenzuweisungen. (ID-17751)
- Identity Manager unterstützt jetzt erweiterte Attributwerte für Rollen. (ID-17770)

## Szenarien

- Identity Manager 8.0 unterstützt nicht mehr das Szenario „Sun Communications Services“ (bisher in `idm/sample/scenario1`) und das Szenario „HR Database/Active Directory Deployment“ (bisher in `idm/sample/scenario2`). Verweise auf diese Szenarien wurden aus dem Dokument *Identity Manager Technical Deployment Overview* entfernt. (ID-18519)

## Sicherheit

- Die Oberfläche für die Anmeldung über eine Frage funktioniert jetzt intuitiver, wenn sie zur Pass-Through-Authentifizierung für LDAP- und AD-Ressourcen verwendet wird. Benutzer, die ihr Passwort vergessen hatten, mussten bisher ihr Identity Manager-Konto (das sie eventuell gar nicht kannten) anstelle ihres Ressourcenkontos angeben. Auf der interaktiven Seite für geheime Fragen muss der Benutzer jetzt sowohl das Ressourcenkonto als auch das Passwort erneut eingeben, während bisher nur das Passwort erforderlich war. (ID-9616)
- Die SSH-Authentifizierung unterstützt jetzt Paare aus einem privaten und einem öffentlichen Schlüssel. Mit dieser neuen Funktion können Benutzer von vertrauenswürdigen Rechnern aus Verbindungen zu Remote-Hosts aufbauen, ohne ein Passwort einzugeben. (ID-11959)
- Passwörter, die in der Passworthistorie des Benutzerobjekts gespeichert sind, werden jetzt in ihrer ursprünglichen Groß-/Kleinschreibung gespeichert. Der Vergleich im Rahmen der Durchsetzung der Passwortrichtlinie berücksichtigt die Groß-/Kleinschreibung jedoch weiterhin nicht. Die Änderung wirkt sich also nicht auf die Funktionsweise des Produkts aus. (ID-12705)
- Diese Version enthält eine Sicherheitsfunktion zur Verhinderung von CSRF-Angriffen (Cross-Site Request Forgery). Standardmäßig ist diese Funktion nicht aktiviert. Sie erfordert Cookies. Wenn Sie Cookies aus Sicherheitsgründen deaktiviert haben, sollten Sie diese Funktion nicht aktivieren, da Sie ansonsten Identity Manager nicht mehr nutzen können. Das Cookie enthält keine vertraulichen Benutzerdaten und existiert ausschließlich im Arbeitsspeicher während der Benutzersitzung. (ID-16703)

Um die Sicherheitsfunktion zu aktivieren, bearbeiten Sie das Systemkonfigurationsobjekt und ändern Sie die Einstellung `security.csrfGuardToken.enable` auf den Wert `true`. Eine Anleitung zum Bearbeiten des Systemkonfigurationsobjekts finden Sie im Dokument *Identity Manager Administration 8.0*.

- Identity Manager unterstützt jetzt eine neue aufgabenbasierte Fähigkeit namens „Debug“. Es können jetzt nur noch Benutzer mit dieser Fähigkeit auf den Debug-Seiten von Identity Manager auf Vorgänge zugreifen und diese ausführen. Bisher konnten dies unter bestimmten Umständen auch Benutzer ohne die korrekten Berechtigungen, sofern sie über bestimmte andere Fähigkeiten verfügten. Ab sofort werden Benutzer ohne die Fähigkeit „Debug“ jedoch auf eine Fehlerseite weitergeleitet. Standardmäßig erhalten die Administrator- und Configurator-Benutzer diese Fähigkeit. Die neue Fähigkeit „Debug“ ist darüber hinaus auch in den Fähigkeiten „Waveset Administrator“ und „Sicherheits-Administrator“ enthalten. (ID-16999)
- Es gibt jetzt die Möglichkeit, eine Ablaufdauer für Konten festzulegen, die wegen mehreren falschen Antworten auf Anmeldefragen gesperrt wurden. Führen Sie die folgenden Schritte aus, um diese Funktion zu aktivieren:
  - Wählen Sie unter „Sicherheit“ / „Richtlinien“ eine Richtlinie zum Bearbeiten aus.
  - Unter „Benutzerkonto-Richtlinienoptionen“ sehen Sie jetzt die neue Option: „Durch falsche Fragen erzeugte Kontosperrung läuft ab in“. Hier können Sie einen Wert und eine Zeiteinheit festlegen. Der Wert 0 bedeutet, dass die Sperrung nie abläuft. (ID-17139)
- Die Zähler für fehlgeschlagene Passwort- und Frage-Anmeldungen werden beim automatischen Ablauf der Kontosperrung nicht zurückgesetzt. Die Anzahl der fehlgeschlagenen Anmeldeversuche (über Passwort bzw. Fragen) wird in der Endbenutzer- und Administrator-Oberfläche korrekt angezeigt. (ID-17412)
- Waveset.properties enthält jetzt die Eigenschaft ui.web.baseHrefURL zur Konfiguration mit relativen URLs. (ID-17763)
- Identity Manager unterstützt jetzt die Konfiguration von PKCS#11-Schlüsselspeichern. Hierzu musste eine nicht rückwärtskompatible Änderung an der HTML-Komponente „TransactionSigner“ vorgenommen werden. (ID-17769)

Die Anzeigeeigenschaft supportedKeyStoreTypes wird nicht mehr unterstützt. Es gibt nun eine Einzelwert-Eigenschaft namens supportedKeyStoreType. Folgende Werte sind zulässig: JKS, PKCS12, PKCS11. Der Standardwert wird von der Systemkonfigurationseigenschaft security.nonrepudiation.defaultKeystoreType festgelegt. In der Regel sollte es ausreichen, die systemweite Eigenschaft security.nonrepudiation.defaultKeystoreType auf den gewünschten Wert zu setzen.

Aufgrund der neuen Unterstützung für PKCS11-Signaturen muss das Applet TransactionSigner nun Funktionen nutzen, die nur in JRE 1.5 zur Verfügung stehen. Auf Clients, die das Applet TransactionSigner nutzen, muss daher JRE 1.5 installiert und als JRE für den Browser konfiguriert sein.

- Identity Manager unterstützt jetzt relative URLs. (ID-18507)

Um diese Funktion zu aktivieren, setzen Sie die folgenden Werte in der Datei `Waveset.properties`:

- Setzen Sie die Eigenschaft `ui.web.relativeURL` auf den Wert „true“.
- Setzen Sie die Eigenschaft `ui.web.useBaseHref` auf den Wert „false“.
- Setzen Sie die Eigenschaft `ui.web.baseHrefURL` auf den Kontext, in dem Identity Manager bereitgestellt ist (im Format `/IDM/`, z. B. `ui.web.basehrefURL=/idm/`).

## Server

- Die Leistung wird bei steigender Anzahl der dynamischen Mitglieder einer Objektgruppe nun deutlich besser. (ID-17561)
- In Identity Manager 8.0 ist die Definition von erweiterten, abfragbaren und Übersichtsattributen für Benutzerobjekte jetzt im neuen Objekt `IDM Schema Configuration` konsolidiert. (ID-17784) In früheren Versionen von Identity Manager musste der Administrator das Konfigurationsobjekt `User Extended Attributes` bearbeiten, um erweiterte Attribute für Benutzerobjekte hinzuzufügen, bzw. das Konfigurationsobjekt `UserUIConfig`, um weitere abfragbare bzw. Übersichtsattribute festzulegen. Jetzt muss der Administrator für all diese Aufgaben nur noch das Objekt `IDM Schema Configuration` bearbeiten.

Änderungen am Objekt `IDM Schema Configuration` werden erst beim nächsten Start des Identity Manager-Servers wirksam. Aufgrund des neuen Objekts `IDM Schema Configuration` ist beim Aufrüsten keine erneute Rückumwandlung möglich. Weitere Informationen finden Sie im Abschnitt [„Probleme bei der Aufrüstung“](#) in diesen Versionshinweisen.

## SPML

- Die OpenSPML-Implementierung enthält jetzt eine SPML-Timeout-Einstellung für Webdienst-Aufrufe. (ID-17687)
- Falls Sie in einer Vorgängerversion SPMLv2 genutzt und dabei mit dem Wert des Attributs „objectclass“ gearbeitet haben, beachten Sie bitte, dass der Wert dieses Attributs jetzt unter dem Attribut „spml2ObjectClass“ geführt wird. (ID-17757)

## Synchronisation

- Bei der ActiveSync-Formularverarbeitung wurde das `idmManager`-Attribut auf bestimmten Adaptern nicht im ActiveSync-Namespace angezeigt. In dieser Version wurde die Methode `toHashMap` so geändert, dass das `idmManager`-Attribut an die zurückgegebene Zuordnung angehängt wird, sodass auch eine Synchronisation im Rahmen von ActiveSync möglich ist. (ID-16717)

## Sonstiges

- Die Unterstützung für die `com.waveset.server.Server`-Funktionen `public Map getResourceObjectListCache()` und `public Map getResourceObjectGetCache()` wurde eingestellt. Bei diesen Caches handelt es sich um interne Datenstrukturen. Code, der diese Strukturen verwendet, wird daher nicht mehr funktionieren. (ID-14790)
- Identity Manager hat jetzt eine Funktion zur Produktregistrierung. Zur Registrierung benötigen Sie Ihr Sun Online-Konto und Ihr Passwort. Wenn Sie noch kein Sun Online-Konto haben, können Sie sich unter der folgenden Adresse registrieren: (ID-17133)

<https://reg.sun.com/register>

Identity Manager kann über die Konsole oder über die Administratoroberfläche registriert werden. Bei der Registrierung über die Konsole können Sie auch ein lokales Service-Tag erstellen. Dieses können Sie dann in der Sun Service Tag-Software zum Inventarisieren Ihrer Systeme, Software und Dienstleistungen von Sun verwenden. Nähere Informationen finden Sie im Abschnitt „Registering Identity Manager“ im Dokument *Identity Manager Administration 8.0*.

- Bei der Produktregistrierung kann die folgende Fehlermeldung erscheinen, wenn Ihr Anwendungsserver keine abgehenden SSL-Verbindungen zulässt: (ID-18546)

Registrierung auf Sun Connection-Server fehlgeschlagen. Grund: Benutzername/Passwort für Sun-Online-Konto ist ungültig

Um dieses Problem zu beheben, nehmen Sie die nötigen vertrauenswürdigen Root-Zertifikate in den Schlüsselspeicher Ihres Anwendungsservers auf. Nähere Informationen finden Sie in der Dokumentation zu Ihrem Anwendungsserver.

- Bei der Produktregistrierung kann die folgende Fehlermeldung erscheinen, wenn alte Versionen von `xml-apis.jar` und `xercesImpl.jar` im Klassenpfad Ihres Anwendungsservers enthalten sind:

```
java.lang.NoSuchMethodError:org.w3c.dom.Node.getTextContent()Ljava/lang/String;
```

Um dieses Problem zu beheben, ändern Sie den Klassenpfad so, dass er nur die neuesten Versionen von `xml-apis.jar` und `xercesImpl.jar` enthält. (ID-18547)

- Damit Sie die Produktregistrierung nutzen können, muss Java auf Ihrem Identity Manager-Server (bzw. Servern) korrekt für SSL konfiguriert sein. Alle JARs, auf die in Ihrer Datei `java.security` (bzw. der entsprechenden Datei) verwiesen wird, müssen vorhanden sein. (ID-18548)

---

# In dieser Version behobene Fehler

In diesem Abschnitt sind die Fehler beschrieben, die in Identity Manager 8.0 behoben wurden. Die Informationen sind wie folgt unterteilt:

- Administrator- und Benutzeroberfläche
- Überwachung
- Delegationen
- Formulare
- Installation
- lh-Konsole
- Protokollierung
- Organisationen
- Bereitstellung
- Berichte
- Repository
- Ressourcen
- Rollen
- Sicherheit
- Server
- Service Provider
- Synchronisation
- Workflow
- Weitere behobene Probleme

## Administrator- und Benutzeroberfläche

- Über die Seite „Formular- und Prozesszuordnungen konfigurieren“ können Benutzer jetzt ein benutzerdefiniertes Formular für die fragenbasierte bzw. anonyme Anmeldung festlegen. (ID-4697)
- Die DatePicker-Formularkomponente unterstützt jetzt `action=true`. (ID-4930)
- Das NetCharts-Applet wurde durch eine JGraph-Grafik ersetzt. (ID-14736)
- In der Tabelle „Serveraufgaben“ ist jetzt eine korrekte Sortierung nach Typ möglich. (ID-14850)
- Beim Durchsetzen einer Passworrichtlinie nahm Identity Manager das ursprüngliche Benutzerpasswort nicht in die Passworhistorie auf. Es wurden stattdessen nur die geänderten Passwörter protokolliert. Wenn also z. B. laut der Richtlinie die letzten drei Passwörter nicht erneut verwendet werden konnten und der Benutzer sein Passwort erst zweimal geändert hatte, ließ Identity Manager die Wiederverwendung des ersten Passworts zu. Dieser Fehler ist in dieser Version behoben. (ID-15026)
- Beim Aufheben von Zuweisungen von Ressourcenkonten zu Benutzern mithilfe der Oberflächenfunktion „Benutzer bearbeiten“ wird das Feld SITUATION im Kontenindex für alle Klassen jetzt ordnungsgemäß aktualisiert. (ID-15310)
- Das Menü in der Endbenutzeroberfläche, mit dem Genehmigungsarbeits Elemente an andere Genehmiger weitergeleitet werden können, wurde bisher nicht korrekt gefüllt. Dieses Problem wurde behoben. Die Liste wird jetzt mit einer Liste von Genehmigern gefüllt, die in der Verwaltungsbefugnis des Benutzers liegt, der aktuell an der Endbenutzeroberfläche angemeldet ist. (ID-15935)
- Bei einer Zeitüberschreitung für ein Arbeitselement des Typs „ManualAction“ (manuelle Aktion) wurde der betreffende Fehler nicht an den Benutzer zurückgegeben. Stattdessen erhielt der Benutzer ein nicht mehr aktuelles Arbeitsablauf-Prozessdiagramm, das den Eindruck vermittelte, das Formular sei korrekt verarbeitet worden. Dieses Problem wurde behoben. Der Benutzer wird in diesem Fall jetzt auf die Seite `workItemTimeout.jsp` weitergeleitet (es sei denn, die Option `IgnoreTimeout` ist aktiviert). (ID-16467)
- Sie können jetzt aktuelle bzw. frühere Delegierungen von Arbeitselementen bearbeiten und speichern. (ID-16564)
- Wenn ein Administrator Delegierungen im Namen eines Benutzers erstellt, kann er nur Delegierte auswählen, die in der Verwaltungsbefugnis des Benutzers liegen. Die Verwaltungsbefugnis des Administrators entspricht nun also der Verwaltungsbefugnis des Benutzers, in dessen Namen die Delegierung vorgenommen wird. Bisher konnte ein Administrator in solchen Situationen auch Delegierte auswählen, die der Benutzer selbst nicht auswählen konnte. (ID-16561)

- Die Oberfläche zeigt nun die Anzahl der fehlgeschlagenen Anmeldeversuche (über Passwort bzw. Authentifizierungsfrage) an, wenn Sun Identity Manager einen Benutzer nicht authentifizieren kann. (ID-17188)
- Die Sortierung in der Tabelle „Ausstehende Genehmigungen“ der Benutzeroberfläche funktioniert nun korrekt. (ID-17304)
- Die Ergebnisseite nach einem Vorgang enthält jetzt immer eine OK-Schaltfläche. (ID-17482)
- Bei neuen Installationen wird immer eine Ergebnisseite (Erfolg oder Fehler) angezeigt, wenn ein Passwort über die Schaltfläche „Passwort vergessen“ eingerichtet wird. Dasselbe gilt für aufgerüstete Systeme, bei denen System Configuration.forgotPasswordChangeResults.User nicht explizit eingestellt wurde. Wenn System Configuration.forgotPasswordChangeResults.User eingestellt wurde, wird weiter das bisherige Verhalten verwendet. (ID-17619)
- Bei Dropdown-Feldern für die Monatsangabe wird jetzt in allen Browsern eine vollständige Monatsliste angezeigt. (ID-17740)
- Verschiedene Anfälligkeiten für XSS-Angriffe (Cross-Site Scripting) sind jetzt behoben. (ID-17748, 18054).
- Im HTML-Code von Tabellen, die von der SimpleTable-Anzeige Komponente und der Datei gentable.jsp erzeugt wurden, werden die <TH>-Tags jetzt korrekt geschlossen. (ID-17945)
- Wenn ein einziger Browser sowohl mit der Endbenutzer- als auch der Administratoroberfläche verbunden ist, werden Formulare jetzt nur noch in der jeweils richtigen Oberfläche angezeigt. (ID-18039)
- JavaScript ist in der Spalte „Status“ der Ressourcenlisten nicht zulässig. Unbedenklicher HTML-Code im Zeichenfolgeninhalt ist jedoch zulässig und wird jetzt korrekt angezeigt. (ID-18050)
- Ein Fehler im Formular für Massenvorgänge erzeugt jetzt einen InlineAlert ohne sichtbaren HTML-Code. (ID-18338)
- Eine Directory-Traversal-Sicherheitslücke in der Oberfläche, über die Benutzer unbefuggt Zugang zu Dateien auf dem Identity Manager-Server erlangen konnten, wurde behoben. (ID-18653)
- Die Seite „Konten auflisten“ wird jetzt schneller angezeigt. (ID-18751)

## Überwachung

- Im Überwachungsprotokoll werden Aktionen des Typs „Priorisieren“ jetzt korrekt protokolliert. (ID-16924)
- Beim Erstellen einer Überwachungsrichtlinie, die auf eine Ressource mit einem Kontentyp beschränkt ist, trat bisher ein „NullPointerException“-Fehler in der Benutzeroberfläche auf. Dieses Problem wurde behoben. (ID-16977)
- Beim Erstellen einer Überwachungsrichtlinienregel mithilfe von „isTrue“ wurde bisher ein Fehler gemeldet, dass die Regel einen Vergleichswert benötige. Dieses Problem wurde behoben. (ID-17041)
- Kommentartext in Bescheinigungen wird nicht mehr fälschlich gelöscht. (ID-17418)
- E-Mail-Benachrichtigungs-Ereignisse werden jetzt überwacht. (ID-17708)
- Doppelte Datenbankschlüssel wurden aus dem Überwachungsprotokoll entfernt. Es handelt sich dabei um die Schlüssel „Extended Type“ (AV) und „Extended Action“ (PE). (ID-18642)

Mit dem Schlüssel „PE“ wurden die Aktionen „EndProcess“ und „PreOperation“ protokolliert. „PreOperation“ verwendet jetzt den Schlüssel „PP“. Mit dem Schlüssel „AV“ wurden die Aktionen „AccessReview“ und „AccessReviewWorkflow“ protokolliert. „AccessReviewWorkflow“ verwendet jetzt den Schlüssel „AW“.

Vorhandene Überwachungseinträge mit dem Schlüssel „PE“ werden in den Überwachungsprotokoll-Berichten als „EndProcess“ interpretiert. Vorhandene Überwachungseinträge mit dem Schlüssel „AV“ werden als „AccessReview“ interpretiert.

Das Aktualisieren von Überwachungseinträgen in der Datenbank mithilfe eines SQL-Skripts ist aus Sicherheitsgründen problematisch, da es anschließend so aussieht, als ob diese Einträge manipuliert wurden. Es wird daher empfohlen, Einträge der betroffenen Typen (d. h. logDb-Schlüssel PE oder AV), die vor der Version 8.0 erstellt wurden, zu ignorieren.

## Delegierungen

- Delegierungszyklen werden nun bei der Ausführung und bei der Erstellung überprüft. (ID-17387)
- Bei einer zweistufigen Delegierung werden vorhandene Korrektur-Arbeitselemente jetzt wieder dem ersten Delegierenden zugeordnet, wenn dieser die Delegierung für Korrektur-Arbeitselemente beendet. (ID-18435)

- Bei der Konfiguration der Delegierung erscheinen jetzt alle Arten von Arbeitselementen, die delegiert werden können, in der Dropdown-Liste. In der Administratoroberfläche wird die Liste nicht mehr gefiltert, sodass jetzt alle möglichen Arten von Arbeitselementen erscheinen. In der Endbenutzeroberfläche erscheinen nur die fünf grundlegenden Arten von Arbeitselementen in der Liste. (ID-18496)
- In Identity Manager 8.0 gibt es jetzt Genehmigungen im Zusammenhang mit Rollentypen und Rollenänderungen, darunter auch Rollentyp-spezifische Änderungsgenehmigungen. Diese Arbeitselemente können auch delegiert werden. Außerdem können beim Delegieren dieser neuen Arbeitselemente (Rollentyp/Rollenänderung) spezifische Rollen festgelegt werden. (ID-18558)

## Formulare

- MultiSelect unterstützt jetzt die neue Eigenschaft `displayCase`, die auf „upper“ oder „lower“ gesetzt werden kann. Dies ist eine praktische Alternative zu einer `valueMap`-Zuordnung, die für jeden zulässigen Wert die Entsprechung in Groß- bzw. Kleinbuchstaben definiert. (ID-8356)

## Installation

- Wenn Sie von 6.0 oder 7.0 auf Version 7.1 oder 8.0 aufrüsten und LocalFiles verwenden, müssen Sie vor der Aufrüstung alle Ihre Daten exportieren und dann nach der Neuinstallation von 7.1 bzw. 8.0 wieder importieren. (ID-15366)

## lh-Konsole

- Der Befehl „`lh syslog`“ gibt jetzt korrekt die passenden Einträge zurück, wenn eine sehr große Anzahl von Tagen angegeben wird. (ID-17844)

## Protokollierung

- Die Klasse `com.waveset.ui.FormUtil` gibt jetzt bei `ClassNotFoundException`-Fehlern (und anderen Fehlern, soweit sie in dieser Klasse auftreten) eine kurze Meldung im Anwendungsserver-Protokoll aus, die auf das Systemprotokoll verweist. Die Detailangaben zum Fehler sind jetzt im Systemprotokoll zu finden. Bisher wurden die Stack-Protokolle dieser Ausnahmefehler direkt im Anwendungsserver-Protokoll ausgegeben. (ID-18473)

## Organisationen

- Die Objekte „User“ und „ObjectGroup“ wurden verbessert (vgl. Fehlernr. 14973) und unterstützen jetzt jeweils mehrere benutzerdefinierte Formulare (als Erweiterung der zwei bisher unterstützten Formulare „Benutzer anzeigen“ und „Benutzer bearbeiten“). Diese neuen Formulare werden in einem <CustomForms>-Element im XML-Code des User- bzw. ObjectGroup-Objekts gespeichert. In der waveset.dtd war <CustomForms> jedoch nicht als Element von <ObjectGroup> deklariert. Der XML-Code eines ObjectGroup-Objekts mit benutzerdefinierten Formularen konnte daher nicht validiert werden. Im Rahmen dieser Fehlerkorrektur wurde <CustomForms> als Element in die waveset.dtd aufgenommen. (ID-17812)

## Bereitstellung

- Wenn die Bereitstellung bei mehreren Ressourcen beim ersten Versuch fehlschlägt und die Ressourcen unterschiedliche Intervalle für Wiederholungsversuche haben, finden die Wiederholungsversuche jetzt bei all diesen Ressourcen korrekt statt (mit der eingestellten Anzahl und dem eingestellten Intervall). Bisher fand ein Wiederholungsversuch nur bei den Ressourcen mit dem kürzesten Intervall statt. (ID-18190)

## Berichte

- Die Objekte „ReportsConfig“ und „TrackedEvents“ bleiben beim Aufrüsten von einer Vorgängerversion jetzt erhalten. (ID-17363).

Um die vorhandenen Berichtskonfigurationsobjekte (ReportsConfig und TrackedEvents) nach Abschluss der Aufrüstung zu überschreiben, entfernen Sie den folgenden Text vom Anfang der Datei reportConfig.xml und importieren Sie die Datei dann in das Identity Manager-Repository.

```
<ImportCommand type='preserve'>  
  <ObjectRef type='Configuration' id='#ID#Configuration:ReportsConfig' />  
  <ObjectRef type='Configuration' id='#ID#Configuration:TrackedEvents' />  
</ImportCommand>
```

- Sie können Berichte, die denselben Aufgabennamen haben, jetzt gleichzeitig ausführen. Aktivieren Sie hierzu das Kontrollkästchen **Gleichzeitige Ausführung von Berichten zulassen?** auf der Berichtsseite. (ID-14631)
- Beim Bearbeiten eines Berichts kann dieser jetzt über die Schaltfläche „Ausführen“ ausgeführt werden, ohne dass dadurch die Änderungen am Bericht automatisch gespeichert werden. Verwenden Sie die Schaltfläche „Speichern“, um die Änderungen am Bericht zu speichern. (ID-17212)

- Bestimmte HTML-E-Mail-Berichte enthalten jetzt korrekte, nicht-leere Spaltenüberschriften (die leeren Links in diesen Spalten wurden entfernt). (ID-17369)
- Überwachungsprotokoll-Berichte zeigen jetzt alle relevanten Einträge, wenn ein Datumszeitraum als Berichtszeitraum ausgewählt wird. (ID-17621)
- Gruppenberichte für Active Directory-Server mit Sicherheitsgruppen, deren Name ein &-Zeichen enthält, werden jetzt korrekt dargestellt (ohne XMLParserException-Fehler). (ID-17942)
- Im Ressourcenbenutzerbericht, Ressourcengruppenbericht und Benutzerzugriffsbericht (sowie allen benutzerdefinierten Berichten, die `com.waveset.report.IndividualUserReport` oder `com.waveset.report.GroupMemberReport` verwenden) wird jetzt nicht mehr die Meldung „Keine Datensätze gefunden“ zwischen den Berichtseinträgen ausgegeben. (ID-18049)
- Die Berichtsanzeige verarbeitet jetzt die Formulareigenschaft „`refType`“ korrekt, wenn ein Bericht bearbeitet und dann mit der Schaltfläche „Ausführen“ ausgeführt wird. Die Eigenschaft „`refType`“ in einem Formular weist die Berichtsanzeige an, einen `ObjectRef`-Verweis mit dem in `refType` angegebenen Typ zu erstellen. Dieser Verweis wird anstelle des Objektnamens als Attributwert für die Abfrage verwendet. (ID-18107)
- Berichte, die `IndividualUserReport.java` verwenden (Ressourcenbenutzerbericht und Benutzerdetailbericht), werden jetzt korrekt abgerufen, wenn das Benutzername-Feld auf einen korrekten Wert gesetzt wird. (ID-18260)
- Der „Bericht über Zusammenfassung der Zugriffsprüfung“ verwendet in den Bedingungen zum Abrufen der Zugriffsprüfungs-Liste jetzt das Attribut „`parInstanceName`“ anstelle von „`parTaskInstanceName`“. Wenn keine Zugriffsprüfungs-Objekte ausgewählt sind, meldet der Bericht jetzt außerdem korrekt, dass keine Datensätze gefunden wurden. (ID-18282)
- Der Bericht „Bericht für einzelnen Benutzerüberprüfungsprotokoll“ hat jetzt eine Hilfeseite. (ID-18539)
- Berichte mit langen Nicht-ASCII-Aufgabennamen werden jetzt mit dem korrekten Dateinamen heruntergeladen. (ID-18550)
- Im Bericht über die letzten Systemmeldungen werden die Daten in der Haupttabelle des Berichts jetzt zur Anzeige auf 128 Zeichen abgeschnitten. Der Bericht wird dadurch besser lesbar, wenn der Inhalt der Meldungsspalte sehr lang ist. In den Details des Berichtseintrags sind weiterhin alle Daten enthalten. Diese Änderung gilt auch für alle Berichte, die `com.waveset.report.SyslogReportTask` als Executor in der Aufgabendefinition verwenden. (ID-18657)

## Repository

- Wenn `role` als Übersichtsattribut im Objekt `UserUIConfig` konfiguriert wird, enthält die Zusammenfassungs-Zeichenfolge standardmäßig nur drei Rollen. Verwenden Sie das Attribut `SummaryAttrResourceCountLimit` in `UserUIConfig`, um den Standardwert zu ändern. (ID-13291)
- Es kommt jetzt nicht mehr vor, dass Identity Manager gültige Verbindungen schließt und aus dem Verbindungspool entfernt. Bisher konnte es bei einem nicht-schwerwiegenden Ausnahmefehler vorkommen, dass Identity Manager eine funktionierende Verbindung schloss. (ID-13719)
- Der `NullPointerException`-Fehler im Überwachungsbericht „Heutige/Wöchentliche Aktivität“ für das CLOB `log.acctAttrChanges` wurde behoben. (ID-17346)
- Bei einem Überwachungsprotokoll mit einer großen Tabelle treten beim Schreiben von Überwachungsereignissen keine deutlichen Leistungseinbußen mehr auf. (ID-18053)

## Ressourcen

- Die Methode `getResourceObjects()` aus `com.waveset.ui.FormUtil` gibt beim Aufruf aus XPRESS jetzt mehrwertige Attribute für Active Directory-Ressourcen korrekt zurück. (ID-11965)
- Der Skeleton-Test aus dem REF-Kit (Resource Extension Facility) benötigt keine Klassen mehr, die nicht im Produkt enthalten sind. Bisher war dieser Test auf die Klassen `com.waveset.junit.WavesetRunner` und `com.waveset.junit.WavesetSuite` angewiesen, die jedoch nicht mit dem Produkt ausgeliefert wurden. Der Test wurde umgeschrieben und ist jetzt nicht mehr von diesen Klassen abhängig. (ID-12370)
- Die Methode `Resource.getAccountAttributeType(name, mapName)` funktioniert jetzt korrekt, wenn das Attribut `name` oder `mapName` den Wert `null` hat. (ID-13598)
- Wenn Sie den Vorgang „Synchronisationsrichtlinie bearbeiten“ für eine Ressource abbuchen, hinterlässt Identity Manager keine Überbleibsel mehr im Repository, und bei Remedy-Ressourcen tritt kein Fehler mehr auf. (ID-14356)
- Identity Manager zeigt eine Fehlermeldung an, wenn beim Aktualisieren von Solaris NIS-Konten ein ungültiger Gruppenname angegeben wird. (ID-15841)
- Benutzer des Adapters `ExampleSPML2ResourceAdapter` haben gemeldet, dass Änderungsanforderungen nicht ausgeführt wurden. Die SPML-v2-Änderungsanforderung wird nun verarbeitet, wenn die Änderungselemente in Datenelementen verschachtelt sind. (ID-16646)

- Bei der Fehlerbehandlung für LDAP-Ressourcenadapter wurden bisher verschiedene festkodierte Zeichenfolgen und Meldungsformate verwendet. In dieser Version sind Fehlermeldungen für Ausnahmefehler in LDAP-basierten Ressourcenadaptern nun lokalisiert. (ID-16721)
- Eine Buffer-Overrun-Sicherheitslücke im Gateway-Verfolgungsmodul wurde behoben. (ID-17093)
- Wenn die Option „Realm-Konfiguration kopieren“ (Copy Realm Configuration) im Sun Access Manager-Datenspeicher gesetzt ist, findet die Bereitstellung in einem Sub-Realm durch dessen Administratorbenutzer (anstelle von amAdmin) statt. Der Grund dafür ist, dass bei dieser Option die Identitäten technisch gesehen nur in dem Realm bzw. Sub-Realm existieren, in dem sie erstellt wurden. (ID-17101)
- Es gibt keinen Singlethreading-Modus für die Version 8.0 des Identity Manager-NDS-Gateway. Der Registrierungsschlüssel ExclusiveNDSContext wird daher nicht mehr verwendet. Der Fehler, der bisher beim Bereitstellen von GroupWise-Benutzern über ein NDS-Gateway im Singlethreading-Modus auftrat, tritt dadurch nicht mehr auf. (ID-17144)
- Der LDAP-Ressourcenadapter verursacht bei der Abstimmung keinen IndexOutOfBoundsException-Ausnahmefehler mehr. (ID-17454)
- Der Adapter „Skriptgateway“ unterstützt keine Passwortänderungen. Der Adapter verhindert nun Versuche, diese Einschränkung zu umgehen, wenn Sie der Schemazuordnung ein Passwortknotenattribut hinzufügen. (ID-17533)
- Bei aktivierter Verfolgung für die Klasse „LDAPResourceAdapterBase“ trat ein „Null pointer“-Ausnahmefehler auf. Dieses Problem wurde behoben. (ID-17588)
- Der Verweis auf `accounts[os400].accountId` gibt nicht mehr `waveset.accountId` zurück. Stattdessen wird der korrekte `accountId`-Wert des OS400-Kontos zurückgegeben. (ID-17632)
- Der SAP-Ressourcenadapter meldet keinen „JCO\_ERROR\_FUNCTION\_NOT\_FOUND“-Fehler mehr, wenn das SAP-System, zu dem eine Verbindung hergestellt wird, das Funktionsmodul „PASSWORD\_FORMAL\_CHECK“ nicht enthält. (ID-17665)

Bei der Passwortsynchronisation mit SAP R/3-Systemen der Version 4.6C verwendet Identity Manager außerdem jetzt `BAPI_USER_EXISTENCE_CHECK` (anstatt `BAPI_USER_GET_DETAIL`).

- Verbindungen zu VMS-Ressourcen über SSH können jetzt erfolgreich hergestellt werden. Beim Aufrüsten müssen Sie entweder `update.xml` ausführen oder die Datei `resourceWizardForms.xml` erneut importieren, damit die entsprechenden Änderungen am VMS-Ressourcenassistenten übernommen werden. (ID-17695)

- Der Ressourcenadapter „Shell-Skript“ berücksichtigt jetzt die Rückgabecodes der Vorgänge „Deaktivieren“, „Aktivieren“ und „Umbenennen“. (ID-17749)
- Wenn Identity Manager Gateway korrekt heruntergefahren wird, tritt im Domino 7.x Server-Konsolenprotokoll keine Meldung über ein unerwartetes Programmende mehr auf. (ID-17782)
- Die UNIX-Ressourcenadapter erstellen Temporärdateien jetzt nur noch mit Lese-/Schreibrechten für den Benutzer. (ID-17835)
- Verschlüsselte Passwörter für Netware NDS GroupWise-Konten werden jetzt korrekt aktualisiert. (ID-18020)

## Rollen

- Regeln zur Berechnung von Ressourcenattributen aus Rollen werden nicht mehr angewendet, wenn sich ein Benutzer bei der Endbenutzerseite anmeldet. (ID-13338)
- Bei der Konfiguration der Delegation erscheinen jetzt alle Arten von Arbeitselementen, die über die jeweilige Benutzeroberfläche delegiert werden können, in der Dropdown-Liste. In der Administratoroberfläche wird die Liste nicht mehr gefiltert, sodass jetzt alle möglichen Arten von Arbeitselementen erscheinen. In der Endbenutzeroberfläche erscheinen nur die fünf grundlegenden Arten von Arbeitselementen in der Liste. (ID-18496)

## Sicherheit

- Benutzer müssen jetzt über die erforderlichen Rechte verfügen, um das Konto eines anderen Benutzers zu löschen. Anderenfalls wird ein Ausnahmefehler gemeldet, und die Löschung wird verhindert. Darüber hinaus wird ein Überwachungseintrag mit näheren Angaben zum Löschversuch protokolliert. (ID-15552)
- Das Einrichten einer Korrelationsregel mit dem X509-Anmeldemodul verursacht keine Fehler bei der Anmeldung mehr. (ID-17128)
- Verschiedene Anfälligkeiten für XSS-Angriffe (Cross-Site Scripting) wurden in dieser Version behoben. (ID-17830, 18015).

## Server

- Zeitstempel sind jetzt eindeutig und enthalten eine Zeitzoneangabe im Format GMT +/- <Zahl>. (ID-8297)
- Das Standard-Repository LocalFiles funktioniert jetzt unter GlassFish. (ID-15589)
- Ein Problem wurde behoben, das zu einem Repository-Stillstand (Deadlock) bei Genehmigungsvorgängen (Endbenutzer) und Bearbeitungsvorgängen (Administrator) führen konnte. (ID-16926)
- Anwendungsserver protokollieren keine Warnmeldung mehr, wenn die Zeichenkodierung nach dem Aufruf von `getReader()` gesetzt wird. (ID-17900)
- Eine Benutzeransicht enthält keine Arbeitselemente für das abrufende Subjekt mehr, wenn es sich bei diesem nicht um den Benutzer in der Ansicht handelt. (ID-18430)

## Service Provider

- Die Service Provider-Standardbenutzersuchseite (ID-11245) meldet jetzt den Fehler  
 Ein Suchwert muss eingegeben werden.  
 wenn kein Suchwert angegeben wird. Es erscheint dann nicht mehr die Meldung  
`javax.naming.CommunicationException: [LDAP: error code 2 - Bad search filter]`  
 oder  
`java.lang.IndexOutOfBoundsException: Posn: -1, Size: 0`
- Wenn sich ein Benutzer an einem SSO-Realm (Single Sign-On) authentifiziert, der zur Verwendung mit einer Service Provider Edition-Instanz konfiguriert ist, und der Benutzer in dieser Instanz aber nicht existiert, so erhält er eine entsprechende Fehlermeldung. Bisher gelangte der Benutzer dann zwar zur Service Provider Edition-Homepage, konnte dort aber keine der angezeigten Aktionen ausführen. (ID-13194)
- Bei der Konfiguration von Service Provider schlägt der Befehl „export all“ von „lh console“ nicht mehr mit der Meldung `java.lang.UnsupportedOperationException` fehl. Auf der Debuggingseite wird IDMXUser nicht mehr als Option unter „Listenobjekte“ angezeigt. (ID-16141)
- Wenn sich ein Service Provider-Benutzer bei der Service Provider-Benutzeroberfläche anmeldete, wurden bisher zwei Überwachungsereignisse für die Anmeldung erzeugt. Dieses Verhalten wurde korrigiert, und es wird nur noch ein einziges Ereignis erzeugt. (ID-16742)

- Bis zu dieser Version wurden Änderungen auf Attributebene für Service Provider-Benutzer nicht in den Überwachungseinträgen verfolgt. Identity Manager überwacht jetzt hingegen auch Änderungen an Service Provider-Attributen, den Namen des Servers, auf dem die Transaktion ausgeführt wurde, sowie den Anmeldeoberflächennamen. (ID-16837)  
Anders als in Identity Manager werden bei Attributänderungen in Service Provider nicht die alten Werte, sondern lediglich die angeforderten und neuen Werte aufgezeichnet. Änderungen an Ressourcenzuweisungen und Authentifizierungsantworten werden in Service Provider ebenfalls nicht aufgezeichnet.
- Bei aktivierter Ereignisverfolgung wurde die Aufgabentabelle im Repository bisher sehr groß. Dieses Problem wurde behoben. (ID-16923)
- SPML-Änderungsanforderungen (Service Provisioning Markup Language) in Service Provider löschen jetzt nicht mehr erweiterte Attribute, die in der Anforderung nicht angegeben sind. (ID-17145)
- Transaktionsdaten im Speicher und im persistenten Datenspeicher werden jetzt korrekt synchronisiert. (ID-17384)

## Synchronisation

- Identity Manager protokolliert einen Fehler, wenn Sie einen nicht vorhandenen Benutzer löschen, erstellt jedoch kein Überprüfungsereignis für Berichte. Identity Manager protokolliert Löschvorgänge für nicht existierende Benutzer jetzt entsprechend. Dieses Protokoll ist in den Systemprotokollen und den Überwachungsprotokoll-Berichten ab Version 6.0 SP4 enthalten. (ID-13284)
- Die Aufgabe „AD Sync Recovery Collector“ funktioniert korrekt mit Servern für den globalen Katalog (ID-17851)
- Wenn ein globaler Katalog zur Active Sync-Synchronisation mit einer Active Directory-Ressource verwendet wird, zählt jetzt jeder Hostname in der Aufgabe „AD Sync Recovery Collector“ für die betreffende Ressource als globaler Katalog. (ID-18597)

## Workflow

- Das Sunrise-Datum berechnet jetzt korrekt die vergangene Zeit. (ID-11247)
- Ein `java.lang.NullPointerException`-Fehler im Nachabstimmungs-Arbeitsablauf wurde behoben. (ID-16893)
- Der Beispiel-Nachabstimmungs-Arbeitsablauf „Benachrichtigung über das Abstimmungsende“ wurde geändert. Die Option `waitForCompletion` wurde aus dem Aufruf von `getView` für die Ansicht `ReconcileStatus` entfernt. (ID-17151) Kunden sollten die Option `waitForCompletion` auch aus allen anderen Nachabstimmungs-Arbeitsabläufen entfernen. Diese Option wird innerhalb der Arbeitsabläufe nie benötigt, da das Abstimmungsprogramm die Ergebnisse vor dem Start des Arbeitsablaufs löscht. Wenn ein Nachabstimmungs-Arbeitsablauf trotzdem die Option `waitForCompletion=true` setzt, führt dies dazu, dass er nicht mehr reagiert.

## Weitere behobene Probleme

17111, 17242, 17269, 17414, 17668, 18555

In dieser Version behobene Fehler

# Identity Manager 8.0 – Bekannte Probleme

In diesem Abschnitt der Identity Manager 8.0-Versionshinweise finden Sie bekannte Probleme und Zwischenlösungen.

---

## Bekannte Probleme

In diesem Abschnitt der Identity Manager 8.0-Versionshinweise finden Sie bekannte Probleme und Zwischenlösungen für die folgenden Themen:

- [Allgemein](#)
- [Installieren und Aktualisieren](#)
- [Überwachung](#)
- [Data Exporter](#)
- [Identity Manager Service Provider](#)
- [Anmeldekonfiguration](#)
- [Organisationen](#)
- [Richtlinien und Fähigkeiten](#)
- [Abstimmen und Importieren von Benutzern](#)
- [Berichte](#)
- [Ressourcen](#)
- [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, Administratorname, 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: Dollar (\$), Komma (,), Punkt (.), Apostroph ('), kaufmännisches Und (&), 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 ist nicht vollständig sichtbar, wenn große Schriftarten im Browser verwendet werden (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 Sie über das XML-Dateiformat eine Ressource in eine XML-Datei extrahieren und dann das CSV-Dateiformat aus der Dropdown-Liste wählen, wird die folgende Meldung angezeigt:

Das Formular wurde bereits übermittelt.

**Zwischenlösung:** Um diese Meldung zu vermeiden, klicken Sie auf „Konten“ > „In Datei extrahieren“ > Ressource wählen > CSV-Dateiformat wählen. Klicken Sie auf „Herunterladen“, um die Kontendetails der Ressource im Format .csv herunterzuladen. (ID-10847)

- Wenn ein erweiterter Knoten weniger als eine Datenseite 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](#).

- Beim Bearbeiten des AdminRole-Objekts kann bei bestimmten Nicht-ASCII-Zeichen ein ItemNotFound-Ausnahmefehler auftreten. (ID-15782)

### Zwischenlösungen:

- Ändern Sie die Datei `adminrolemodify.jsp` so, dass die ID nicht mehr als Abfragezeichenfolge übergeben wird.

```
<%
String bodyAttributes = "onload=\"selectFirstEditField();\"";
try {
    String id = requestState.getParameter("id");
    if (id == null) {
        :
    }
} else {
    form.setTitle(Messages.UI_ADMIN_ROLES_JSP_EDIT_ROLE_TITLE);
    form.setSubTitle(Messages.UI_ADMIN_ROLES_JSP_EDIT_ROLE_SUBTITLE);
    // ID nicht mehr als Abfragezeichenfolge übergeben

    //form.setPostURL(response.encodeURL("security/adminrolemodify.jsp?id="+id));
    form.setPostURL(response.encodeURL("security/adminrolemodify.jsp"));
}
}
```

- Ändern Sie die Datei `adminrolemodify.jsp` so, dass der ID-Abfrageparameter korrekt kodiert wird.

```
<%
String bodyAttributes = "onload=\"selectFirstEditField();\"";
try {
    String id = requestState.getParameter("id");
    if (id == null) {
        :
    }
} else {
    form.setTitle(Messages.UI_ADMIN_ROLES_JSP_EDIT_ROLE_TITLE);
    form.setSubTitle(Messages.UI_ADMIN_ROLES_JSP_EDIT_ROLE_SUBTITLE);
    // Wert des ID-Abfrageparameters kodieren

    //form.setPostURL(response.encodeURL("security/adminrolemodify.jsp?id="+id
));
    form.setPostURL(response.encodeURL("security/adminrolemodify.jsp?id="
+ com.waveset.util.URLUTF8Encoder.encode(id)));
}
}
```

- 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)

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

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

```
table.Tab2TblNew td
{background-image:url(../images/tabs/level2_deselect.jpg);background-repeat:repeat-x;backgroun
d-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)
- Das Repositorykonfigurationsobjekt hat ein Attribut namens `maxAttrValLength`. Dieses Attribut hat immer den Wert 255 und wird ignoriert. (ID-16261)
- 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.

- Wenn Sie beim Bearbeiten bzw. Erstellen von Benutzern einen `idmManager` zuweisen, einem weiteren `idmManager` zugewiesen ist, der nicht existiert (wenn z.B. der `idmManager` fehlt), wird die folgende Fehlermeldung angezeigt und die Änderung wird nicht gespeichert. (ID-17339)

```
'Eintrag [nicht vorhandener „idmManager“] wurde im Repository nicht gefunden;
möglicherweise wurde er in einer anderen Sitzung gelöscht.'
```

Beim Erstellen neuer Benutzer tritt dieses Problem nicht auf.

- Der Befehl „Konten“ > „In Datei extrahieren“ speichert XML- und CSV-Dateien mit der Endung `.dat` (statt mit den korrekten Endungen `.xml` bzw. `.csv`). (ID-17521)

**Zwischenlösung:** Sie können die gespeicherten Dateien manuell umbenennen und ihnen die passende Endung geben.

- Auf der Seite „Qualitätsrichtlinie für die Zeichenfolge“ wird Text in vertikalen Linien angezeigt. (ID-18551)
- Rollentyp-Delegierungen haben Vorrang vor Rollengenehmigungs-Delegierungen für eine bestimmte Rolle. (ID-18559) Wenn Sie z. B. Rollen-Arbeits Elemente für bestimmte Rollen an Benutzer 1 delegieren, alle Geschäftsrollen-Arbeits Elemente aber an Benutzer 2, so werden auch Genehmigungen für die Rollen aus der ersten Delegierung an Benutzer 2 (und nicht an Benutzer 1) delegiert. Das Szenario ist also wie folgt:
  - Sie delegieren die Rollengenehmigung für die Geschäftsrolle 1 an Benutzer 1.
  - Sie delegieren die Rollengenehmigung für Geschäftsrollen allgemein an Benutzer 2.

Alle Anforderungen bezüglich der Genehmigung einer Geschäftsrolle für einen Benutzer werden in diesem Fall an Benutzer 2 delegiert.

- Beim Aktivieren einer Rolle hat der Benutzer keine Möglichkeit, die zugewiesenen Rollen zu aktualisieren. (ID-18647)

**Zwischenlösungen:** Aktualisieren Sie die zugewiesenen Benutzer von Hand oder über die Seiten „Rollen auflisten“ bzw. „Rollen finden“.

- Rollen, die in anderen Rollen enthalten sind, können Benutzern nun bedingt zugewiesen werden, wenn die übergeordnete Rolle zugewiesen wird. Beim Bearbeiten der übergeordneten Rolle kann eine Bedingung für die Verknüpfung zwischen der übergeordneten und der enthaltenen Rolle festgelegt werden. Diese Bedingung kann auch auf eine Regel verweisen. Wenn eine Regel verwendet wird, müssen alle für ihre Auswertung erforderlichen Benutzeransicht-Attribute als Argumente übergeben werden. (ID-18734)
- Der verwendete Data-Warehouse-Meldungskatalog (`WICMessages.properties`) richtet sich nach dem Gebietsschema des Servers, nicht dem des Benutzers. (ID-18898) Wenn ein Anwendungsserver z. B. unter dem Gebietsschema „Japanisch“ läuft, werden die Abfrageattribute auf Japanisch angezeigt, auch wenn die Benutzeroberfläche normalerweise auf Englisch oder einer anderen Sprache angezeigt wird.

**Zwischenlösung:** Starten Sie den Anwendungsserver in einem Gebietsschema mit einer UTF-8-Variante neu, die der Spracheinstellung des Browsers entspricht.

- In Identity Manager 8.0 gibt es ein neues abfragbares Attribut namens „assignedRoles“, das auf alle direkten und indirekten Rollen verweist, die einem Benutzer zugewiesen sind. (ID-18921) In Vorgängerversionen gab es das (weiterhin verfügbare) Attribut „role“, das lediglich die Rollen enthält, die einem Benutzer direkt zugewiesen sind. Beim Aufrüsten werden nur Benutzer mit indirekten Rollen automatisch aktualisiert, um das Attribut „assignedRoles“ mit den korrekten Daten zu füllen. Berichte über die Benutzer, die einer Regel zugewiesen sind, zeigen in einer aufgerüsteten Umgebung erst dann alle Benutzer korrekt an, nachdem alle Benutzer aktualisiert wurden.

#### Zwischenlösungen:

- Aktualisieren Sie alle Benutzer.
- Erstellen Sie einen Bericht für Benutzer mit direkt zugewiesenen Rollen.
- In der Version 8.0 können drei Referenzattribute der Objektklasse „Principal“ nicht auf „User“ für den Datenexport offengelegt werden: MemberAdminGroups, adminRoles und adminGroupsRule.

Die Attribute „MemberAdminGroups“ und „adminRoles“ sind abfragbare Attribute von „User“, werden aber im Objektklassenschema nicht als solche angezeigt. (ID-18536)

## Installieren und Aktualisieren

- Das Installationsprogramm von Identity Manager funktioniert unter Umständen nicht mit der 64-Bit-Version des JDK. (ID-18534)

#### Zwischenlösungen:

- Führen Sie eine manuelle Installation durch.
- Verwenden Sie zur Ausführung des Installationsprogramms die 32-Bit-Version des JDK.
- Setzen Sie `os.arch=ppc` durch Setzen von `JAVA_OPTS` (vom Installationskript verwendet), um eine Installation durchführen zu können. Zum Beispiel:

```
export JAVA_OPTS="-Dos.arch=ppc"
```

```
install
```

- Oder falls `JAVA_OPTS` bereits die erforderlichen Optionen enthält:

```
export JAVA_OPTS="$JAVA_OPTS -Dos.arch=ppc"
```

```
install
```

- Wenn sich der Aufrüstungsprozess nicht mit dem Standardkonto und -passwort „configurator“ anmelden kann, wird dieser Fehler in der Protokolldatei protokolliert, anschließend jedoch nichts mehr. (ID-18929)

Beim Aufrüsten wird die Datei `update.xml` importiert. Dabei versucht die Importroutine, sich als „configurator“ mit dem Standardpasswort anzumelden. Falls die Anmeldung fehlschlägt, wird ein Fehler angezeigt, und das Aufrüstungsprogramm bittet Sie um Eingabe der korrekten Anmeldedaten. Wenn Sie die korrekten Daten eingeben, wird die Aufrüstung fortgesetzt. Wenn Sie sich anschließend die Protokolldatei für die Aufrüstung ansehen, finden Sie dort zwar noch die Fehlermeldung über die fehlgeschlagene Anmeldung, danach aber keine weiteren Protokollinformationen über die Aufrüstung. Dieses Problem betrifft aber lediglich die Protokolldatei, nicht die Aufrüstung an sich.

- Das Skript `upgradeto80from71.mysql` enthält einen Fehler, der dazu führt, dass das Skript in der Mitte abgebrochen wird. (ID-18874, 18977)

Um diesen Fehler zu vermeiden, müssen Sie die folgende Zeile im Skript ändern:

```
INSERT INTO waveset.roleobj SELECT * from waveset.object where type = 'Role';
```

Ändern Sie diese Zeile wie folgt:

```
INSERT INTO waveset.roleobj (SELECT id, type, name, lockinfo, modified,
repomod, summary, attr1, attr2, attr3, attr4, attr5, counter, xmlSize, xml FROM
waveset.object WHERE type='Role');
```

Die Spaltennamen müssen explizit angegeben werden, da die Spalten in einer aufrüsteten 7.1-Datenbank in einer anderen Reihenfolge vorliegen.

## 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.

- Die logarithmische Skalierung für Überwachungsrichtlinien-Berichte ist nicht implementiert. (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 Adminsistrator` verfügt.

- Bei der Ausführung von Überwachungsrichtlinienabfragen, die mehrere Verletzungen zurückgeben, erstellt Auditor u. U. einen Korrekturarbeitsablauf für die Verarbeitung der Verletzungen. (ID-15830) 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.

- 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)
- 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)
- Bei Konformitätsverletzungen, die vor der Aufrüstung auf Identity Manager 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 Identity Manager kann der Schweregrad und die Priorität nicht eingestellt werden. (ID-16420)

## Data Exporter

- Als Ausführungskonto für die Funktion „Data Exporter“ kann ein beliebiger Identity Manager-Administrator mit den erforderlichen Fähigkeiten konfiguriert werden. Die Export-Aufgabe wird als Dämon ausgeführt und vom Identity Manager-Planer (Scheduler) gestartet und überwacht. Von der Data-Exporter-Funktion erstellte Überwachungseinträge zeigen daher das Subjekt des Identity Manager-Planers (Scheduler:*IDMServer*) und nicht das Subjekt, das für die Aufgabe konfiguriert wurde. (ID-18055)
- Die forensische Abfrage unterstützt keine Bearbeiten-/Ändern-Aktionen an Rollentypen. (ID-18769)

## Identity Manager Service Provider

- Identity Manager Service Provider 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
```

- Einige Konfigurationsoptionen in der Identity Manager-Administratorbenutzeroberfläche werden in Identity Manager Service Provider 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)

- 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 Ressourcenname 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.

## 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. Versuchen Sie es später erneut.`

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

## Organisationen

- 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 „immediate“ und „user“.
- 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.

- Auf dem Formular zum Starten einer Überwachungsrichtlinien-Überprüfungsaufgabe gibt es eine Option, nach Abschluss der Prüfung eine E-Mail mit einem Verletzungsbericht an eine bestimmte Adresse zu schicken. Wenn keine Verletzungen gefunden werden, wird diese E-Mail auch nicht verschickt. (ID-18773)

## Abstimmen und Importieren von Benutzern

- Beim Abbrechen einer Vollabstimmung wird die folgende Fehlermeldung angezeigt:  
Abbruch der schrittweisen Abstimmung von [Ressource], ausgeführt auf [Server].  
Die Meldung sollte wie folgt lauten:  
Abbruch der vollen Abstimmung von [Ressource], ausgeführt auf [Server].  
(ID-14554)
- Der Wert des Attributs „waitForCompletion“ im Arbeitsablauf „Benachrichtigung über das Abstimmungsende“ muss auf „false“ geändert werden, um zu verhindern, dass der Ablauf bei der Abstimmung nicht mehr reagiert. Das Attribut „waitForCompletion“ wird in der nächsten Identity Manager-Hauptversion entfernt. (ID-16888)

**Zwischenlösungen:**

- Importieren Sie die Datei `<idm_root>/sample/wfrecon.xml` mithilfe von `lh console`.
- Ändern Sie den Arbeitsablauf „Benachrichtigung über das Abstimmungsende“ manuell mithilfe von `lh config`.

- Wenn Objekte aus einer Ressource geladen werden und die betreffende Ressource das Attribut `ACCOUNT_CASE_INSENSITIVE_IDS` unterstützt, wird zum Benutzerobjekt ein zweites `ResourceInfo`-Feld hinzugefügt, das die gleiche Konto-ID wie die der Ressource besitzt, wenn sich die Benutzerkonto-ID in Groß- und Kleinschreibung von der ID unterscheidet, die im `ResourceInfo`-Benutzerobjekt von Identity Manager gespeichert ist.

**Zwischenlösung:** Stellen Sie sicher, dass die Groß- und Kleinschreibung der Konto-ID im `ResourceInfo`-Objekt von Identity Manager die gleiche ist wie die in der Ressource. (ID-17377)

- Wenn Sie das Anzeigekomponenten-Applet „MultiSelect“ deaktiviert haben (und stattdessen die HTML-Version verwenden) und die Abstimmungsrichtlinie einer Ressourceninstanz bearbeiten, kann ein Fehler auftreten, wenn Sie das Kontrollkästchen „Ressourcentyp-Richtlinie übernehmen“ deaktivieren. (ID-18964)

**Zwischenlösung:** Aktivieren Sie die MultiSelect-Applets wieder.

## Berichte

- 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.

- In den Spalten „Priorität“ und „Schweregrad“ der Verletzungszusammenfassung werden Zahlen anstatt Text angezeigt. (ID-16932)
- Der Bericht „Verletzungszusammenfassung“ enthält keine korrigierten Verletzungen. Er umfasst nur Verletzungen, die momentan aktiv (neu oder wiederholt aufgetreten) sind bzw. gemindert wurden. (ID-16933)
- Die Spalte „Verletzungsstatus“ in der Verletzungszusammenfassung muss lokalisiert sein. (ID-17011)
- Fügen Sie zum Dropdown-Menü „Mögliche Zustände“ in der Verletzungszusammenfassung die Option EXEMPTED hinzu. (ID-17042)
- Wenn mehrere Bedingungen zum Erzeugen eines Nutzungsberichts festgelegt werden, wird das Diagramm zwar korrekt auf der Berichtsergebnisseite angezeigt, aufgrund der festen Zeilenbreite wird der Bedingungstext jedoch abgeschnitten. (ID-17224)
- Bei Berichten für die Suche nach inaktiven Konten werden die Ergebnisse nicht auf der Seite „Risikoanalyseberichte anzeigen“ angezeigt. Gehen Sie zur Seite „Serveraufgaben“, wenn Sie sich die Ergebnisse dieser Berichte anzeigen lassen wollen. (ID-17255)

- Im Bericht zu Benutzerfragen wird kein Berichtstitel angezeigt, wenn die Fragenrichtlinie nicht konfiguriert ist. (ID-17415)
- Im Ressourcenbenutzerbericht wird der Rücksetzungs-Administrator als Benutzer aufgeführt. Hierbei handelt es sich jedoch um einen verborgenen Benutzer, der nicht angezeigt werden sollte. (ID-17650)

## 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)
- 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 --> Ressourcenpasswort ändern, wird der Aufgabenname folgendermaßen angezeigt:

```
_FM_PASSWORD_CHANGING_TASK null:null
```

Es soll ein benutzerfreundlicher Name angezeigt werden. (ID-6947)

- 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 die folgenden Klassen, deren Unterstützung eingestellt wurde:
  - `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 im Paket `com.waveset.adapter.iapi` verweisen. (ID-8246)

- 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.

- Wenn Sie bei der Ausführung von ActiveSync einen Benutzer unter einem anderen Administratortypen bearbeiten, wird ein ActiveSync-Ausnahmefehler ausgelöst. Da der betreffende Benutzer vom anderen Administrator gesperrt wurde, kann ActiveSync den betreffenden Prozess nicht ausführen. (ID-11255)

**Zwischenlösung:** Zum Aktivieren wiederholter ActiveSync-Zugriffe auf eine Ressource müssen Sie den XML-Code der Ressource mit den folgenden beiden Ressourcenattributen im folgenden Format ergänzen:

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

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

Wobei:

- **syncRetryCountLimit** gibt an, wie oft die Aktualisierung versucht werden soll.
- **syncRetryInterval** ist die Zeit (in ms), die zwischen den Aktualisierungsversuchen gewartet werden soll.

Diese Werte erscheinen danach bei der ActiveSync-Konfiguration als benutzerspezifische Ressourceneinstellungen. Sie sollten einen Anzeigenamen (`displayName`) angeben. Verwenden Sie dafür einen benutzerspezifischen Katalogschlüssel, wenn dieser Name lokalisiert angezeigt werden soll.

- 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.
- Die Identity Manager-Passwortsynchronisation schlägt aufgrund einer Regression fehl, wenn sie mit Sun Java™ System Directory Server Enterprise Edition 6.0, 6.1 oder 6.2 verwendet wird. Dieser Fehler wird in Directory Server 6.3 behoben. Wenn Identity Manager mit den Versionen 6.0, 6.1 oder 6.2 zusammenarbeiten soll, müssen Sie vom Technischen Support ein Directory Server-Hotfix anfordern. Geben Sie bei der Anforderung Directory Server-Bug 6604342 an. (ID-14895)
- Wenn Sie Ressourcenobjekte einer Sun Java™ System Access Manager 7.0-Ressource von der Registerkarte „Ressourcen“ aus erweitern, kann es sein, dass die folgende Fehlermeldung angezeigt wird: (ID-15525)

```
Fehler beim Auflisten der Objekte. ==> com.waveset.util.WavesetException: Fehler beim Abrufen des Attributwerts für das Attribut 'guid'. ==> java.lang.IllegalAccessError: tried to access method com.sun.identity.idm.AMIdentity.getUniversalId()Ljava/lang/String; from class com.waveset.adapter.SunAccessManagerRealmResourceAdapter
```

Dieser Fehler tritt auf Access Manager 7.0-Ressourcen auf, für die noch keine Patches installiert wurden. Zur Behebung dieses Problems müssen Sie mindestens Patch 1 von Access Manager installieren und dann das Access Manager Client-SDK neu erstellen und bereitstellen.

- Wegen Interoperabilitätsproblemen zwischen WebSphere-Datenquellen und Oracle JDBC-Treibern müssen Oracle-Kunden, die WebSphere-Datenquellen mit Identity Manager verwenden wollen, Oracle 10g R2 und den entsprechenden JDBC-Treiber verwenden. (Der Oracle 9 JDBC-Treiber funktioniert nicht mit WebSphere-Datenquellen und Identity Manager.) (ID-16167)

Wenn Sie eine Oracle-Version vor 10g R2 haben und nicht auf Oracle 10g R2 aktualisieren können, müssen Sie das Identity Manager-Repository so konfigurieren, dass Verbindungen zur Oracle-Datenbank mithilfe des JDBC-Treibermanagers von Oracle (und nicht mit WebSphere-Datenquellen) hergestellt werden.

Weitere Informationen finden Sie unter der folgenden URL:

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

- 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 Console 1-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)

- WRQ sucht die im CLASSPATH aufgeführten Verzeichnisse ab, um seinen eigenen Eintrag zu finden. Aus diesem Eintrag ermittelt WRQ das Verzeichnis, in dem die JAR-Datei gespeichert ist, und liest dann mithilfe dieses Verzeichnisses die JAW-Datei (Lizenzierungsdatei) ein. BEA und WebSphere nutzen jedoch beide statt des Standardformats JAR, dass vom WRQ-Code als vorhanden vorausgesetzt wird, keine Standardprotokollnamen (BEA verwendet zip und WebSphere wsjar). (ID-16709, 17319)

### Zwischenlösungen:

- Für BEA fügen Sie zum Befehl java in der der Datei startWeblogic.sh die folgende Zeile hinzu:

```
-Dcom.wrq.profile.dir="VerzeichnisMitBibliotheken"
```

- Für WebSphere fügen Sie die Eigenschaft com.wrq.profile.dir=VerzeichnisMitBibliotheken in die Datei WebSphere/AppServer/configuration/config.ini ein.

- Bei der Verwendung von Identity Manager 7.1 bzw. 8.0 mit Oracle 10g auf Sun Java™ System Application Server Enterprise Edition 8.2 kann der Ausnahmefehler „Sealing Violation“ ausgelöst werden. Dieses Problem kann verursacht werden, wenn sich in den in CLASSPATH angegebenen Verzeichnissen mehrere Oracle JDBC JAR-Dateien befinden oder im CLASSPATH eine nicht kompatible Version einer JDBC JAR-Datei gespeichert ist. (ID-17311)  
  
Sie sollten sicherstellen, dass sich in den in CLASSPATH angegebenen Verzeichnissen nur eine Oracle JDBC JAR-Datei (z. B. die während der Oracle-Installation bereitgestellte JAR-Datei) befindet.
- Vor dem Erstellen einer neuen Ressource müssen Sie in der Liste konfigurierter Typen den entsprechenden Ressourcentyp aktivieren. Andernfalls kann es sein, dass das neu erstellte Ressourcenobjekt nicht alle erforderlichen Felder besitzt. (ID-17324)
- Der Standardwert des Attributs `verzeichnis_erstellen` ist bei den Unix-Ressourcen nicht konsistent. (ID-18301)
- Wenn Identity Manager unter einem Gebietsschema mit einem Multibyte-Zeichensatz verwendet wird, ist der Name der CSV-Datei mit den Ergebnissen einer Massenaktion nicht korrekt. (ID-18661)

## Rollen

- Das Datumsauswahlfenster (zum Festlegen von Aktivierungs-/Deaktivierungsterminen für Rollen, die einem Benutzer zugewiesen wurden) funktioniert nicht, wenn ein Rollennamen einen Apostrophen enthält. (ID-18941)  
  
**Zwischenlösung:** Geben Sie das betreffende Datum in das Textfeld neben dem Datumsauswahl-Symbol ein.
- Bei der manuellen Eingabe von Aktivierungs-/Deaktivierungsterminen für die Rollen eines Benutzers werden die Felder automatisch abgeschickt, sobald man sie verlässt (durch Klicken/Tabulatortaste). Dies führt dazu, dass die Meldung „Formular bereits übermittelt“ angezeigt wird, wenn Sie nach einer solchen manuellen Änderung auf „Speichern“ klicken. (ID-18927)

- Beim Löschen einer Rolle sollte geprüft werden, ob Verweise darauf vorhanden sind (als enthaltene Rolle bzw. durch Benutzer). Wenn solche Verweise vorhanden sind, wird ein Fehler gemeldet, und die Rolle wird nicht gelöscht. (ID-18981)

Diese Prüfung funktioniert jedoch nicht korrekt, wenn Verweise durch andere Rollen vorhanden sind. Die Rolle wird aus ihren übergeordneten Rollen entfernt, obwohl dies nicht geschehen sollte. Die Rolle wird nicht gelöscht, da Benutzer noch auf sie verweisen. Die Verweise auf die enthaltene Rolle bleiben im Benutzerobjekt erhalten, obwohl die übergeordnete Rolle diese Rolle nicht mehr enthält.

Prüfen Sie vor dem Löschen einer Rolle daher, dass die Rolle nicht in anderen Rollen enthalten oder (direkt oder indirekt) noch Benutzern zugewiesen ist.

## Server

- Die aktivierte Laufschrift wird nicht angezeigt, wenn in den Namen von Organisationen Apostrophe (') vorkommen. (ID-5653)

## Sun Identity Manager Gateway

- Das Sun Identity Manager Gateway wird unter Umständen nicht angehalten, wenn im Fenster für die Windows-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 Windows-Dienste, und führen Sie den Stoppvorgang erneut aus.

- Das Gateway wird gelegentlich nicht angehalten, wenn der Befehl 'net stop „Sun Identity Manager Gateway“' verwendet wird (ID-2337).
- Im Sun Identity Manager Gateway tritt ein Speicherleck auf, wenn die Exchange 2007-Unterstützung im Active Directory-Ressourcenadapter aktiviert ist. Dadurch wächst die Speicherbelegung des Prozesses mit der Zeit. (ID-18854)

**Zwischenlösung:** Überwachen Sie den Prozess des Gateway-Dienstes und starten Sie den Dienst neu, bevor er zu viel Speicher belegt.

## Aufgaben

- 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 ist eine Folge der neuen Unterstützung von Sonderzeichen (&\<>) in Auswahllisten. (ID-5548)
- Die Formular-, Workflow- und Regelkommentare in <Comment>-Tags 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 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)
- Wenn Identity Manager durch einen Sun Access Manager Policy Agent geschützt wird, werden die Arbeitsablauf-Prozessdiagramme unter Umständen nicht vollständig angezeigt. (ID-18304)

## Bekannte Probleme

# Installations- und Aktualisierungshinweise

In diesem Abschnitt finden Sie Informationen zur Installation und Aktualisierung von Identity Manager. Die Informationen sind wie folgt unterteilt:

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

---

**HINWEIS** Bekannte Probleme im Zusammenhang mit der Installation oder Aufrüstung finden Sie im Abschnitt [Installieren und Aktualisieren](#) dieses Dokuments.

---

---

## Installationshinweise

Die folgenden Informationen beziehen sich auf die Installation des Produktes:

- Bei der Installation von PasswordSync müssen Sie die passende Binärdatei für das Betriebssystem verwenden, auf dem Sie die Installation durchführen. Die Binärdatei für die 32-Bit-Version von Windows heißt `IdmPwSync_x86.msi`, die für die 64-Bit-Version von Windows `IdmPwSync_x64.msi`.

Sie müssen PasswordSync mithilfe der Funktion „Software“ in der Windows-Systemsteuerung deinstallieren, damit alle Dateien ordnungsgemäß entfernt werden. Wenn Sie die Installation mit der falschen Binärdatei durchführen, scheint sie erfolgreich abgeschlossen zu werden, PasswordSync funktioniert dann aber nicht ordnungsgemäß. (ID-17290)

- Sie müssen Identity Manager unter HP-UX manuell installieren.
- Das Installationsprogramm von Identity Manager kann jetzt Installationen und Aktualisierungen in beliebigen Installationsverzeichnissen vornehmen. Sie müssen dieses Verzeichnis vor dem Installationsvorgang erstellen oder ein Verzeichnis aus dem Setup-Fenster auswählen.
- Zur Ausführung von Sun Identity Manager Gateway unter Windows muss das Zusatzmodul Microsoft Active Directory Client installiert sein. 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 im Dokument *Sun Identity Manager-Installation*.

---

---

# Aufrüstungshinweise

Dieser Abschnitt enthält Informationen und bekannte Probleme im Hinblick auf die Aufrüstung von Identity Manager von Version 6.0 auf die Version 7.0 oder 8.0.

Die Informationen in diesem Abschnitt sind wie folgt unterteilt:

- [Vorbereitung](#)
- [Probleme bei der Aufrüstung](#)
- [Aktualisieren von Benutzerobjekten](#)

- 
- HINWEISS**
- Eine Anleitung und Informationen zum Aufrüsten finden Sie im Dokument *Identity Manager Upgrade*.
  - Sehen Sie vor der Aufrüstung von Identity Manager in *Sun Identity Manager-Installation* die für Ihren Anwendungsserver spezifischen Installationsanweisungen ein.
  - Wenn Ihre aktuelle Identity Manager-Installation viele benutzerdefinierte Anpassungen enthält, sollten Sie sich für Unterstützung bei der Planung und Ausführung der Aufrüstung an Sun Professional Services wenden.
- 

## Vorbereitung

Beachten Sie die folgenden Informationen, bevor Sie mit der Aufrüstung beginnen:

---

**ACHTUNG** Falls Sie ein Oracle-Repository verwenden: Die Repository-DDL von Identity Manager 8.0 verwendet Datentypen, mit denen ältere Oracle JDBC-Treiber nicht korrekt umgehen können. Die JDBC-Treiber in `ojdbc14.jar` lesen nicht alle Spalten der Protokolltabelle korrekt.

Sie müssen auf die Treiberversion aus der Datei `oracle11g_jdbc.jar` aufrüsten, damit Identity Manager korrekt funktioniert.

---

- In Identity Manager 8.0 gibt es einige neue Tabellen für Rollenobjekte. Sie müssen die Beispielskripten im Verzeichnis `db_scripts` verwenden, um die Schemaänderungen vorzunehmen, die neuen Tabellenstrukturen zu erstellen und Ihre vorhandenen Daten zu verschieben.

- 
- HINWEIS**
- Vor dem Aufrüsten der Tabellendefinitionen in der Repository-Datenbank sollten Sie von allen Repository-Tabellen Sicherungskopien erstellen.
  - Weitere Informationen hierzu finden Sie im Skript `db_scripts/upgradeto8.0from71.DBMSName`.
- 

- Wenn Sie auf Identity Manager 8.0 aufrüsten und bisher eigenen Code verwendet haben, der `UserUIConfig#getRepoIndexAttributes()` aufruft, müssen Sie diese Aufrufe entfernen oder so ändern, dass stattdessen `Type.USER#getInlineAttributeNamees()` aufgerufen wird.

Beim Importieren von `update.xml` werden die Werte aus `UserUIConfig RepoIndexAttrs` in XML-Attributwerte des `TypeDataStore`-Elements für `Type.USER` im `RepositoryConfiguration`-Objekt konvertiert. Die Datei `update.xml` schließt die Datei `UserUIConfigUpdater.xml` ein. In dieser ruft ein `Import-Befehl` `UserUIConfigUpdater` auf, um `RepoIndexAttrs` zu konvertieren. Die Konvertierung setzt außerdem eine Markierung im `SystemConfiguration`-Objekt, die eine erneute Konvertierung (bzw. Rückkonvertierung) verhindert.

Wenn Sie in Zukunft Änderungen an den `Inline`-Attributen für `Type.USER` vornehmen möchten, sollten Sie hierzu das `RepositoryConfiguration`-Objekt bearbeiten. Wenn Sie die `Inline`-Attribute für `Type.USER` ändern, müssen Sie im Regelfall alle `Type.USER`-Objekte aktualisieren.

---

**HINWEIS** Änderungen am `RepositoryConfiguration`-Objekt werden erst nach einem Neustart des betreffenden Identity Manager-Servers wirksam.

---

- Stellen Sie sicher, dass Sie die Datei `update.xml` nur über einen einzigen Identity Manager-Server importieren und dass während der Aufrüstung nur ein einziger Identity Manager-Server läuft. Wenn Sie andere Identity Manager-Server während der Aufrüstung starten, müssen Sie diese anhalten und neu starten, bevor Sie sie verfügbar machen.
- Gehen Sie beim Bearbeiten des Felds „`SuperRoles`“ im Rollenformular mit Bedacht vor, da die `SuperRole` selbst eine verschachtelte Rolle sein kann. Die Felder „`SuperRoles`“ und „`SubRoles`“ weisen Verschachtelungen von Rollen und deren zugehörigen Ressourcen bzw. Ressourcengruppen auf. Wenn sie auf einen Benutzer angewendet wird, enthält die betreffende `SuperRole` die zugehörigen Ressourcen mit den dafür vorgesehenen `SubRoles` (Unterrollen). Das Feld „`SuperRole`“ wird angezeigt, um auf die Rollen hinzuweisen, die die angezeigte Rolle enthalten.

- Während der Aufrüstung analysiert Identity Manager alle Rollen im System und aktualisiert alle fehlenden Verknüpfungen zwischen untergeordneten und übergeordneten Rollen mithilfe der Klasse `RoleUpdater`.

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`.

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='nouupdate' value='false' />
      <MapEntry key='nofixsubrolelinks' value='false' />
    </Map>
  </ImportCommand>
</Waveset>
```

Wobei:

- **verbose:** Beim Aktualisieren von Rollen erfolgt eine ausführliche Ausgabe. Geben Sie **false** an, wenn die Aktualisierung von Rollen ohne Ausgabe erfolgen soll.
- **nouupdate:** 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.
- Administratoren müssen zum Anzeigen oder Bearbeiten des Identity Manager-Schemas für Benutzer oder Rollen Mitglied der Admin-Gruppe `IDM Schema Configuration` sein und die Fähigkeit `IDM Schema Configuration` besitzen.

- Die SPML 2.0-Implementierung in Identity Manager wurde in Identity Manager 8.0 geändert. In früheren Versionen war das in SPML-Nachrichten verwendete SPML-Attribut `objectclass` direkt dem Attribut `objectclass` von User-Objekten in Identity Manager zugeordnet. Das Attribut `objectclass` ist jetzt intern dem Attribut `spm12objectClass` zugeordnet und wird für andere Zwecke verwendet.

Bei der Aufrüstung wird der `objectclass`-Attributwert für vorhandene Benutzer automatisch umbenannt. Wenn Ihre SPML 2.0-Konfiguration Formulare mit Verweisen auf das Attribut `objectclass` enthält, müssen Sie diese manuell auf das Attribut `spm12objectClass` abändern.

Identity Manager ersetzt die Beispiel-Konfigurationsdatei `spm12.xml` während einer Aufrüstung nicht. Wenn Sie die Datei `spm12.xml` als Ausgangspunkt für eine eigene Konfiguration verwendet haben, so beachten Sie bitte, dass diese Datei ebenfalls ein Formular mit Verweisen auf `objectclass` enthält, die Sie in `spm12objectClass` ändern müssen. Ändern Sie das Attribut `objectclass` außerdem nur in Formularen (wo es intern verwendet wird), *nicht* aber im Zielschema (wo es nach außen hin offengelegt wird).

- 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`
- Alle zuvor installierten Hotfixes werden im folgenden Verzeichnis archiviert:

`$WSHOME/patches/HotfixName`

## 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. (ID-9228)

```
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/lhpwic.dll
bin/winnt/msems.inf
bin/winnt/pwicsvc.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
```

- Vom Benutzer erweiterte Attribute in Identity Manager können jetzt mehrere Attributwerte enthalten. (ID-14863)

---

**HINWEIS** Sie können vom Benutzer erweiterte Attribute mit mehreren Werten zur Kontolistentabelle hinzufügen. Die Liste wird jetzt fehlerlos ausgegeben. Wenn Sie jedoch versuchen, für diese Spalte eine Sortierung durchzuführen, wird die folgende Fehlermeldung angezeigt:

```
java.lang.ClassCastException: java.util.ArrayList
```

---

Eine Attributbedingung, die sich auf ein erweitertes Attribut mit mehreren Attributwerten bezieht, wird *erst dann* für ein Benutzerobjekt korrekt evaluiert, wenn dieses Objekt neu serialisiert wurde. Wenn eine solche Attributbedingung für alle Benutzerobjekte korrekt evaluiert werden soll, müssen Sie alle Benutzerobjekte neu serialisieren. Anweisungen dazu finden Sie unter [„Aktualisieren von Benutzerobjekten“](#) auf Seite 87.

- Wenn Sie von Identity Manager 6.x auf Version 7.x oder 8.0 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 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“.

---

**HINWEIS** Wenn Sie direkt von Identity Manager 7.x auf Version 8.0 aufrüsten, sind diese Änderungen nicht erforderlich.

---

- Wenn Sie von Version 6.0 oder 7.0 auf Version 7.1 oder 8.0 aufrüsten und LocalFiles verwenden, müssen Sie vor der Aufrüstung alle Ihre Daten exportieren und dann nach der Neuinstallation von 7.1 bzw. 8.0 wieder importieren. (ID-15366)
- Wenn Ihre Installation eine Remedy-Ressource enthält, müssen Sie die Remedy API-Bibliotheken in das Verzeichnis kopieren, in dem das Gateway installiert ist. Sie finden diese Bibliotheken auf dem Remedy-Server.

**Tabelle 1** Remedy API-Bibliotheken

Remedy 4.x und 5.x	Remedy 6.3	Remedy 7.0
• arapiXX.dll	• arapi63.dll	• arapi70.dll
• arrpcXX.dll	• arrpc63.dll	• arrpc70.dll
• arutlXX.dll	• arutl63.dll	• arutl70.dll
Hierbei entspricht XX der Remedy-Version. Beispiel: arapi45.dll für Remedy 4.5.	• icudt20.dll	• icudt32.dll
	• icuin20.dll	• icuin32.dll
	• icuuc20.dll	• icuuc32.dll

- Bei der Aufrüstung auf Identity Manager 8.0 werden das Objekt `User Extended Attributes` sowie die Elemente `QueryableAttrNames` und `SummaryAttrNames` des Objekts `UserUIConfig` automatisch in das Objekt `IDM Schema Configuration` konvertiert. (ID-17784) Das Beispielskript `update.xml` ruft über einen `Import`-Befehl `IDMSchemaConfigurationUpdater` auf, um die alten Benutzerschema-Konfigurationsobjekte zu konvertieren. Bei einer erfolgreichen Konvertierung dieser alten Objekte geschieht Folgendes:
  - In `IDM Schema Configuration` wird ein `IDMObjectClassAttribute`-Element für jedes erweiterte Attribut aus `User Extended Attributes` erstellt.
  - Jedes `IDMObjectClassAttribute`, das einem Wert im Element `SummaryAttrNames` in `UserUIConfig` entspricht, wird als „summary“ (Übersichtsattribut) markiert.
  - Jedes `IDMObjectClassAttribute`, das einem Wert im Element `QueryableAttrNames` in `UserUIConfig` entspricht, wird als „queryable“ (abfragbares Attribut) markiert.
  - Das Element `SummaryAttrNames` in `UserUIConfig` wird geleert.
  - Das Element `QueryableAttrNames` in `UserUIConfig` wird geleert.
  - Erweiterte Attribute mit dem Namen `objectClass` werden in `spml2ObjectClass` umbenannt. (Altattribute mit dem Namen `objectClass` führen zu einem Namenskonflikt mit einem Kernattribut des Identity Manager 8.0-Schemas.)
- Wenn Sie auf Identity Manager 8.0 aufrüsten und bisher eigenen Code verwendet haben, der `UserUIConfig#getRepoIndexAttributes()` aufruft, müssen Sie diese Aufrufe entfernen oder so ändern, dass stattdessen `Type.USER#getInlineAttributeNames()` aufgerufen wird. (ID-18051)

Beim Importieren von `update.xml` werden die Werte aus `UserUIConfig RepoIndexAttrs` in XML-Attributwerte des `TypeDataStore`-Elements für `Type.USER` im `RepositoryConfiguration`-Objekt konvertiert. Die Datei `update.xml` schließt die Datei `UserUIConfigUpdater.xml` ein. In dieser ruft ein `Import`-Befehl `UserUIConfigUpdater` auf, um `RepoIndexAttrs` zu konvertieren. Die Konvertierung setzt außerdem eine Markierung im `SystemConfiguration`-Objekt, die eine erneute Konvertierung (bzw. Rückkonvertierung) verhindert.

Wenn Sie in Zukunft Änderungen an den `Inline`-Attributen für `Type.USER` vornehmen möchten, sollten Sie hierzu das `RepositoryConfiguration`-Objekt bearbeiten. Wenn Sie die `Inline`-Attribute für `Type.USER` ändern, müssen Sie im Regelfall alle `Type.USER`-Objekte aktualisieren.

---

**HINWEIS** Änderungen am `RepositoryConfiguration`-Objekt werden erst nach einem Neustart des betreffenden Identity Manager-Servers wirksam.

---

- Stellen Sie sicher, dass Sie die Datei `update.xml` nur über einen einzigen Identity Manager-Server importieren und dass während der Aufrüstung nur ein einziger Identity Manager-Server läuft. (ID-18051)

Wenn Sie andere Identity Manager-Server während der Aufrüstung starten, müssen Sie diese anhalten und neu starten, bevor Sie sie verfügbar machen.

- Beim Aufrüsten auf Identity Manager 8.0 von einer Identity Manager-Version vor Identity Manager 7.1 können „ItemNotFound“-Ausnahmefehler im Aufrüstungsprotokoll auftreten. Dies liegt daran, dass „Identity Manager Service Provider Edition“ (SPE)-Objekte in Identity Manager 8.0 in „Identity Manager Service Provider“ umbenannt werden. (ID-18860)

## Eingestellte Funktionen

- In Identity Manager 8.0 wurde die Anzeigemethode für Diagramme in Berichten geändert. Berichte, die in einer Vorgängerversion erstellt wurden, werden in Identity Manager 8.0 wie erwartet angezeigt, in den nachfolgenden Hauptversionen und Patches aber nicht mehr. Ein Bericht, der in Identity Manager 7.1 erstellt wurde, wird beispielsweise in Identity Manager 8.0 und Identity Manager 8.0 Patch 1 wie erwartet angezeigt, in Identity Manager 9.0 jedoch nicht mehr. (ID-17636)

## Aktualisieren von Benutzerobjekten

Bei bestimmten Änderungen muss ein Administrator alle `User`-Objekte aktualisieren. Dies ist beispielsweise dann der Fall, wenn Sie die Inline-Attribute für `Type.USER` im `RepositoryConfiguration`-Objekt ändern. Wenn Sie ein Attribut im `IDMSchemaConfiguration`-Objekt als abfragbar oder als Übersichtsattribut markieren, müssen Sie alle `User`-Objekte aktualisieren, damit die Änderung auch für ältere, nicht geänderte Objekte wirksam wird. Entsprechendes gilt, wenn in einer neuen Identity Manager-Version ein neues Attribut hinzugefügt wird oder wenn die Werte eines vorhandenen Attributs geändert werden. In diesem Fall muss der Aufrüstungsvorgang oder ein Administrator alle `User`-Objekte aktualisieren, damit die Änderung auch für ältere, nicht geänderte Objekte wirksam wird.

Sie können vorhandene Benutzerobjekte auf dreierlei Art neu serialisieren:

- Ändern eines einzelnen Benutzerobjekts im Normalbetrieb

Sie können beispielsweise ein Benutzerkonto über die Benutzeroberfläche öffnen und dieses mit oder ohne Änderungen speichern.

**Nachteil:** Diese Methode ist zeitaufwändig, und der Administrator muss besonders sorgfältig darauf achten, dass auch alle vorhandenen Benutzerobjekte neu serialisiert wurden.

- Neuserialisierung aller Benutzerobjekte mithilfe des Dienstprogramms `lh refreshType`. Die Ausgabe des Dienstprogramms `refreshType` ist die aktualisierte Benutzerliste.

```
lh console
```

```
refreshType User
```

**Nachteil:** Da das Dienstprogramm `refreshType` im Vordergrund und nicht im Hintergrund läuft, kann dieser Prozess zeitaufwändig sein. Bei einer großen Benutzeranzahl kann die Neuserialisierung lange dauern.

- Verwendung der Abfragefunktion für verschobene Aufgaben

---

**HINWEIS** Vor dem Ausführen der Abfragefunktion für verschobene Aufgaben müssen Sie das System Configuration-Objekt in der Identity Manager Integrated Development Environment (Identity Manager-IDE) oder mithilfe einer anderen Methode bearbeiten.

Suchen Sie nach `'refreshOfType'` und entfernen Sie die Attribute für `'2005Q4M3refreshOfTypeUserIsComplete'` und `'2005Q4M3refreshOfTypeUserUpperBound'`.

Nach dem Bearbeiten des System Configuration-Objekts muss dieses wieder in das Repository importiert werden, damit die Änderungen wirksam werden.

---

**Nachteil:** Durch dieses Verfahren dauert die Abfragefunktion für verschobene Aufgaben relativ lange, da die Funktion jedes einzelne Benutzerobjekt untersucht und neu schreibt. Nachfolgende Ausführungen der Abfragefunktion für verschobene Aufgaben sollten jedoch mit regulärer Geschwindigkeit und Zeitdauer ausgeführt werden.

# Veraltete APIs (Unterstützung eingestellt)

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

- [Veraltete Java-Klassen, -Methoden und -Felder](#)
- [Veraltete JSP-Dateien und URLs](#)
- [Veraltete Konfigurationsobjekte](#)
- [Veraltete Ansichten und Pfadausdrücke](#)

---

**HINWEIS** Die Unterstützung für die Applets MultiSelect und TreeTable wird in der nächsten Hauptversion von Identity Manager eingestellt. Es werden jedoch weiterhin ähnliche Funktionen bereitgestellt. (ID-18785)

---

---

## Veraltete Java-Klassen, -Methoden und -Felder

Die folgende Tabelle enthält die Klassen, Methoden und Felder, deren Unterstützung eingestellt wurde. Soweit verfügbar, ist auch der jeweilige Nachfolger angegeben. Die Tabelle ist nach dem Klassennamen sortiert. Alle Klassen, Methoden und Felder sind in JavaDoc-Syntax aufgeführt.

---

<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.sun.idm.idmx.sync.util.CaseInsensitiveString Comparator</code>	<code>java.lang.String.CASE_INSENSITIVE_ORDER</code>
<code>com.waveset.adapter.AccessManagerResourceAdapter# handlePDEException(Exception)</code>	<code>com.waveset.adapter. AccessManagerResourceAdapter# handlePDEException(PDEException)</code>
<code>com.waveset.adapter.ACF2ResourceAdapter# getAccountAttributes(String)</code>	
<code>com.waveset.adapter.ActivCardResourceAdapter</code>	
<code>com.waveset.adapter.ActiveDirectoryActiveSyncAdapter</code>	<code>com.waveset.adapter.ADSIResourceAdapter</code>
<code>com.waveset.adapter.ActiveSync# RA_PARAMETERIZED_INPUT_FORM</code>	

---

Verworfen	Nachfolger
com.waveset.adapter.ActiveSync# RA_SYNC_CONFIG_MODE	
com.waveset.adapter.ActiveSync# RA_SYNC_POST_PROCESS_FORM	
com.waveset.adapter.ActiveSync# RA_UPDATE_IF_DELETE	
com.waveset.adapter.ActiveSync#RA_USE_INPUT_FORM	
com.waveset.adapter.ActiveSyncUtil#getLogFileFullPath()	
com.waveset.adapter.AD_LDAPResourceAdapter	com.waveset.adapter.LDAPResourceAdapter
com.waveset.adapter.ADSIResourceAdapter# buildEvent(UpdateRow)	com.waveset.adapter.iapi.IAPIFactory# getAPI(Map,Map,ResourceAdapterBase)
com.waveset.adapter.ADSIResourceAdapter# getBaseContextAttrName()	com.waveset.adapter.ResourceAdapter# getBaseContexts()
com.waveset.adapter.ADSIResourceAdapter# RA_UPDATE_IF_DELETE	com.waveset.adapter.ActiveSync# RA_DELETE_RULE
com.waveset.adapter.AgentResourceAdapter# getAccountAttributes(String)	
com.waveset.adapter.AIXResourceAdapter.BlockAcctlter	Verweise auf diese Klasse sollten durch einen AccountIterator auf Grundlage des Lieferantenmodells ersetzt werden. Beispiel: BufferedAccountQueue(new AIXAccountSupplier).
com.waveset.adapter.AuthSSOResourceAdapter# getAccountAttributes(String)	
com.waveset.adapter.BlackberryResourceAdapter	com.waveset.adapter.ScriptedGatewayResource Adapter
com.waveset.adapter.ClearTrustResourceAdapter# getAccountAttributes(String)	
com.waveset.adapter.ConfirmedSync	Verweise auf diese Klasse sollten durch einen AccountIterator auf Grundlage des Lieferantenmodells ersetzt werden. Beispiel: BufferedAccountQueue(new LinuxAccountSupplier).
com.waveset.adapter.DatabaseTableResourceAdapter# RA_PROCESS_NAME	com.waveset.adapter.ActiveSync# RA_PROCESS_RULE
com.waveset.adapter.DbIBufIterator	com.waveset.util.BufferedIterator com.waveset.util.BlockIterator com.waveset.adapter.AccountIteratorWrapper

Verworfen	Nachfolger
com.waveset.adapter.DB2ResourceAdapter# getAccountAttributes(String)	
com.waveset.adapter.DominoActiveSyncAdapter	com.waveset.adapter.DominoResourceAdapter
com.waveset.adapter.DominoResourceAdapter# buildEvent(UpdateRow)	com.waveset.adapter.iapi.IAPIFactory# getAPI(Map,Map,ResourceAdapterBase)
com.waveset.adapter.DominoResourceAdapter# RA_UPDATE_IF_DELETE	com.waveset.adapter.ActiveSync# RA_DELETE_RULE
com.waveset.adapter.DominoResourceAdapterBase# getAccountAttributes(String)	
com.waveset.adapter.Exchange55ResourceAdapter	
com.waveset.adapter.ExampleTableResourceAdapter# getAccountAttributes(String)	
com.waveset.adapter.GenericScriptResourceAdapter# getAccountAttributes(String)	
com.waveset.adapter.GetAccessResourceAdapter# getAccountAttributes(String)	
com.waveset.adapter.HostConnectionPool# getConnectionHostAccessLogin)	com.waveset.adapter.HostConnPool# getAffinityConnection(HostAccessLogin)
com.waveset.adapter.HostConnectionPool# releaseConnection(HostAccess)	com.waveset.adapter.HostConnPool# releaseConnection(HostAccess)
com.waveset.adapter.HostConnectionPool# releaseConnection(IHostAccess)	com.waveset.adapter.HostConnPool# releaseConnection(IHostAccess)
com.waveset.adapter.HostConnPool# getConnection(HostAccessLogin)	com.waveset.adapter.HostConnPool# getAffinityConnection(HostAccessLogin)
com.waveset.adapter.HostConnPool#putFree()	
com.waveset.adapter.HostConnPool#putFree(IHostAccess)	com.waveset.adapter.HostConnPool#putAffinityFree
com.waveset.adapter.iapi.IAPIFactory# getAPIProcess(Map,Map,String,Resource)	com.waveset.adapter.iapi.IAPIFactory# getAPI(Map,Map,String,ResourceAdapterBase)
com.waveset.adapter.iapi.IAPIFactory# getAPIProcess(Element)	
com.waveset.adapter.iapi.IAPIFactory# getAPIUser(Element)	
com.waveset.adapter.iapi.IAPIFactory# getAPIUser(Map,Map,String,Map)	com.waveset.adapter.iapi.IAPIFactory# getAPI(Map, Map, String, ResourceAdapterBase)
com.waveset.adapter.iapi.IAPIFactory# getAPIUser(Map,Map,String,Resource)	com.waveset.adapter.iapi.IAPIFactory# getAPI(Map,Map,String,ResourceAdapterBase)

Verworfen	Nachfolger
com.waveset.adapter.IDMResourceAdapter# getAccountAttributes(String)	
com.waveset.adapter.INISafeNexessResourceAdapter# getAccountAttributes(String)	
com.waveset.adapter.LDAPChangeLogActiveSyncAdapter	com.waveset.adapter.LDAPResourceAdapter
com.waveset.adapter.LDAPListenerActiveSyncAdapter	com.waveset.adapter.LDAPChangeLogActiveSyncAdapter
com.waveset.adapter.LDAPResourceAdapterBase# addUserToGroup(LDAPObject,String,String)	com.waveset.adapter.LDAPResourceAdapterBase# addUserToGroup(String,String,String)
com.waveset.adapter.LDAPResourceAdapterBase# buildBaseUrl()	
com.waveset.adapter.LDAPResourceAdapterBase# buildBaseUrl(String)	
com.waveset.adapter.LDAPResourceAdapterBase# buildEvent(UpdateRow)	
com.waveset.adapter.LDAPResourceAdapterBase# getAccountAttributes(String)	
com.waveset.adapter.LDAPResourceAdapterBase# getBaseContextAttrName()	com.waveset.adapter.ResourceAdapter# getBaseContexts()
com.waveset.adapter.LDAPResourceAdapterBase# getGroups(Name,String,Vector,Vector)	com.waveset.adapter.LDAPResourceAdapterBase# getGroups(String,String,Vector,Vector)
com.waveset.adapter.LDAPResourceAdapterBase# getLDAPAttributes(String,DirContext[],String)	com.waveset.adapter.LDAPResourceAdapterBase# getLDAPAttributes(String,DirContext,String,String[])
com.waveset.adapter.LDAPResourceAdapterBase# getLDAPAttributes(String,DirContext[])	com.waveset.adapter.LDAPResourceAdapterBase# getLDAPAttributes(String,DirContext,String,String[])
com.waveset.adapter.LDAPResourceAdapterBase# RA_PROCESS_NAME	com.waveset.adapter.ActiveSync# RA_PROCESS_RULE
com.waveset.adapter.LDAPResourceAdapterBase# removeNameFromAttribute(DirContext,Name,Attribute)	com.waveset.adapter.LDAPResourceAdapterBase# removeNameFromAttribute(DirContext,String, boolean,Attribute)
com.waveset.adapter.LDAPResourceAdapterBase# removeUserFromAllGroups(Name,String,WavesetResult)	com.waveset.adapter.LDAPResourceAdapterBase# removeUserFromAllGroups(String,boolean,String, WavesetResult)
com.waveset.adapter.LDAPResourceAdapterBase# removeUserFromGroup(DirContext,Name,String,String, Attributes)	com.waveset.adapter.LDAPResourceAdapterBase# removeUserFromGroup(DirContext,String,boolean, String,String,Attributes)

Verworfen	Nachfolger
com.waveset.adapter.LDAPResourceAdapterBase# removeUserFromGroups(Name,Vector,String, WavesetResult)	com.waveset.adapter.LDAPResourceAdapterBase# removeUserFromGroups(String, boolean,Vector,String,WavesetResult)
com.waveset.adapter.LinuxResourceAdapter.BlockAcctIter	
com.waveset.adapter.MySQLResourceAdapter# getAccountAttributes(String)	
com.waveset.adapter.NaturalResourceAdapter# getAccountAttributes(String)	
com.waveset.adapter.NaturalResourceAdapter.getUser()	com.waveset.adapter.NaturalResourceAdapter# affinity
com.waveset.adapter.NaturalResourceAdapter.login (IHostAccess)	com.waveset.adapter.NaturalResourceAdapter# login(IHostAccess,ServerAffinity)
com.waveset.adapter.NDSActiveSyncAdapter	com.waveset.adapter.NDSResourceAdapter
com.waveset.adapter.NDSResourceAdapter# buildEvent(UpdateRow)	
com.waveset.adapter.NDSResourceAdapter# getBaseContextAttrName()	com.waveset.adapter.ResourceAdapter# getBaseContexts()
com.waveset.adapter.NISResourceAdapter	
com.waveset.adapter.NTResourceAdapter	
com.waveset.adapter.ONTDirectorySmartResourceAdapter# getAccountAttributes(String)	
com.waveset.adapter.OS400ResourceAdapter# getAccountAttributes(String)	
com.waveset.adapter.PeopleSoftComponentActiveSync Adapter#DEFAULT_AUDIT_STAMP_FORMAT	
com.waveset.adapter.PeopleSoftComponentActiveSync Adapter#DEFAULT_AUDIT_STAMP_START_DATE	
com.waveset.adapter.PeopleSoftComponentActiveSync Adapter#getAccountAttributes(String)	
com.waveset.adapter.PeopleSoftComponentActiveSync Adapter#getUpdateRows(UpdateRow)	com.waveset.adapter.PeopleSoftComponentActive SyncAdapter#getUpdateRows(UpdateRow)
com.waveset.adapter.PeopleSoftComponentActiveSync Adapter#RA_AUDIT_STAMP_FORMAT	
com.waveset.adapter.PeopleSoftResourceAdapter	
com.waveset.adapter.RACFResourceAdapter# getAccountAttributes(String)	

Verworfen	Nachfolger
com.waveset.adapter.RASecureConnection# ExchangeAuth(boolean)	com.waveset.adapter.RASecureConnection# ExchangeAuth(boolean,byte[])
com.waveset.adapter.RemedyActiveSyncResourceAdapter	com.waveset.adapter.RemedyResourceAdapter
com.waveset.adapter.RequestResourceAdapter# getAccountAttributes(String)	
com.waveset.adapter.ResourceAdapter# getAccountAttributes(String)	
com.waveset.adapter.ResourceAdapter# getBaseContextAttrName()	com.waveset.adapter.ResourceAdapter# getBaseContexts()
com.waveset.adapter.ResourceAdapterBase# getAccountAttributes(String)	
com.waveset.adapter.ResourceAdapterBase# getAdapter(Resource,LighthouseContext)	com.waveset.adapter.ResourceAdapterBase# getAdapterProxy(Resource,LighthouseContext)
com.waveset.adapter.ResourceAdapterBase# getAdapter(Resource,ObjectCache,WSUser)	com.waveset.adapter.ResourceAdapterBase# getAdapterProxy(Resource,ObjectCache)
com.waveset.adapter.ResourceAdapterBase# getAdapter(Resource,ObjectCache)	
com.waveset.adapter.ResourceAdapterBase# getBaseContextAttrName()	com.waveset.adapter.ResourceAdapterBase# getBaseContexts()
com.waveset.adapter.ResourceAdapterBase# isExcludedAccount(String,Rule)	com.waveset.adapter.ResourceAdapterProxy# isExcludedAccount(String,Map,ResourceOperation, Rule)
com.waveset.adapter.ResourceAdapterBase# isExcludedAccount(String)	com.waveset.adapter.ResourceAdapterProxy# isExcludedAccount(String,Map,ResourceOperation, Rule)
com.waveset.adapter.ResourceAdapterBase.SimpleAccount Iterator	Anstelle dieser Klasse sollte das Lieferantenmodell für die Konteniteration verwendet werden. Die Klasse ließe sich z. B. durch Folgendes direkt ersetzen: new BufferedAccountQueue(new SimpleAccountSupplier(Konten));
com.waveset.adapter.ResourceAdapterProxy# getAccountAttributes(String)	
com.waveset.adapter.ResourceAdapterProxy# getBaseContextAttrName()	com.waveset.adapter.ResourceAdapterProxy# getBaseContexts()
com.waveset.adapter.ResourceManager# getResourceTypes()	com.waveset.adapter.ResourceManager# getResourcePrototypes()  com.waveset.adapter.ResourceManager# getResourcePrototypes(ObjectCache,boolean)

Verworfen	Nachfolger
com.waveset.adapter.ResourceManager#getResourceTypeStrings()	com.waveset.adapter.ResourceManager#getResourcePrototypeNames(ObjectCache)
com.waveset.adapter.SAPHRActiveSyncAdapter#RA_PROCESS_NAME	com.waveset.adapter.ActiveSync#RA_PROCESS_RULE
com.waveset.adapter.SAPResourceAdapter#reverseMapMultiAttr(String, Object, WSUser)	
com.waveset.adapter.SAPResourceAdapter#setUserField(JCO.Function, String)	Function#setUserField(String)
com.waveset.adapter.SAPResourceAdapter#unexpirePassword(String,WavesetResult)	com.waveset.adapter.SAPResourceAdapter#unexpirePassword(String,String,String,WavesetResult)
com.waveset.adapter.SAPResourceAdapter#unexpirePassword(WSUser,WavesetResult)	com.waveset.adapter.SAPResourceAdapter#unexpirePassword(String,String,String,WavesetResult)
com.waveset.adapter.ScriptedConnection.Script#hasNextToken()	
com.waveset.adapter.ScriptedConnection.Script#nextToken()	
com.waveset.adapter.ScriptedConnection.ScriptedConnection#disconnect()	com.waveset.adapter.ResourceConnection#disconnect()
com.waveset.adapter.ScriptedConnection.ScriptedConnectionFactory#getScriptedConnection(String,HashMap)	com.waveset.adapter.ScriptedConnectionPool#getConnection(HashMap,String,long,boolean)
com.waveset.adapter.ScriptedConnection.SSHConnection#disconnect()	com.waveset.adapter.ScriptedConnection.SSHConnection#disconnect()
com.waveset.adapter.ScriptedConnection.TelnetConnection#disconnect()	com.waveset.adapter.ScriptedConnection.TelnetConnection#disconnect()
com.waveset.adapter.ScriptedHostResourceAdapter#getAccountAttributes(String)	
com.waveset.adapter.SkeletonActiveSyncAdapter	
com.waveset.adapter.SkeletonResourceAdapter	
com.waveset.adapter.SkeletonResourceAdapter#getAccountAttributes(String)	
com.waveset.adapter.SMEResourceAdapter#getAccountAttributes(String)	
com.waveset.adapter.SQLServerResourceAdapter	com.waveset.adapter.MSSQLServerResourceAdapter
com.waveset.adapter.SunAccessManagerResourceAdapter#getAccountAttributes(String)	

Verworfen	Nachfolger
com.waveset.adapter.SunAccessManagerResourceAdapter#getBaseContextAttrName()	com.waveset.adapter.ResourceAdapter#getBaseContexts()
com.waveset.adapter.SVIDResourceAdapter.BlockAcctIter	Verweise auf diese Klasse sollten durch einen AccountIterator auf Grundlage des Lieferantenmodells ersetzt werden. Beispiel: BufferedAccountQueue(new SVIDAccountSupplier).
com.waveset.adapter.SybaseResourceAdapter	com.waveset.adapter.SybaseASEResourceAdapter
com.waveset.adapter.TestResourceAdapter#getAccountAttributes(String)	
com.waveset.adapter.TopSecretActiveSyncAdapter	com.waveset.adapter.TopSecretResourceAdapter
com.waveset.adapter.TopSecretResourceAdapter#hasError(String,String)	com.waveset.adapter.TopSecretResourceAdapter#hasError(String,String,String)
com.waveset.adapter.TopSecretResourceAdapter#login(HostAccess hostAccess)	com.waveset.adapter.TopSecretResourceAdapter#login(HostAccess,ServerAffinity)
com.waveset.adapter.TopSecretResourceAdapter#login(IHostAccess hostAccess)	com.waveset.adapter.TopSecretResourceAdapter#login(IHostAccess hostAccess,ServerAffinity affinity)
com.waveset.adapter.VerityResourceAdapter#getAccountAttributes(String)	
com.waveset.adapter.XMLResourceAdapter#getAccountAttributes(String)	
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.extractor.CSVFormatter	com.sun.idm.changelog.CSVFormatter
com.waveset.msgcat.Catalog#getMessage(String,Object[],Locale)	com.waveset.msgcat.Catalog#format(Locale,String,Object[])
com.waveset.msgcat.Catalog#getMessage(Locale,String,Object[])	com.waveset.msgcat.Catalog#format(Locale,String,Object[])
com.waveset.msgcat.Catalog#getMessage(Locale,String)	com.waveset.msgcat.Catalog#format(Locale,String)
com.waveset.msgcat.Catalog#getMessage(String,Locale)	com.waveset.msgcat.Catalog#format(Locale,String)
com.waveset.msgcat.Catalog#getMessage(String,Object[])	com.waveset.msgcat.Catalog#format(Locale,String,Object[])
com.waveset.object.Account#getUnowned()	com.waveset.object.Account#hasOwner()
com.waveset.object.Account#setUnowned(boolean)	com.waveset.object.Account#setOwner(WSUser)
com.waveset.object.AccountAttributeType#getAttrType()	com.waveset.object.AccountAttributeType#getSyntax()

<b>Verworfen</b>	<b>Nachfolger</b>
com.waveset.object.AccountAttributeType# setAttrType(String)	com.waveset.object.AccountAttributeType# setSyntax(String)
	com.waveset.object.AccountAttributeType# setSyntax(Syntax)
com.waveset.object.Attribute#BLOCK_SIZE	com.waveset.object.Attribute#BLOCK_ROWS_GET
	com.waveset.object.Attribute#BLOCK_ROWS_LIST
com.waveset.object.Attribute#EVENTDATE	com.waveset.object.Attribute#EVENT_DATETIME
com.waveset.object.Attribute#EVENTTIME	com.waveset.object.Attribute#EVENT_DATETIME
com.waveset.object.Attribute#getDbColumnLength()	
com.waveset.object.Attribute#getDbColumnName()	
com.waveset.object.Attribute#STARTUP_TYPE_AUTO	com.waveset.object.Resource# STARTUP_TYPE_AUTO
com.waveset.object.Attribute# STARTUP_TYPE_AUTO_FAILOVER	com.waveset.object.Resource# STARTUP_TYPE_AUTO_FAILOVER
com.waveset.object.Attribute#STARTUP_TYPE_DISABLED	com.waveset.object.Resource# STARTUP_TYPE_DISABLED
com.waveset.object.Attribute#STARTUP_TYPE_MANUAL	com.waveset.object.Resource# STARTUP_TYPE_MANUAL
com.waveset.object.Attribute#STARTUP_TYPES	com.waveset.object.Resource#STARTUP_TYPES
com.waveset.object.Attribute# STARTUP_TYPES_DISPLAY_NAMES	com.waveset.object.Resource# STARTUP_TYPES_DISPLAY_NAMES
com.waveset.object.AttributeDefinition# AttributeDefinition(String,String)	com.waveset.object.AttributeDefinition# AttributeDefinition(String,Syntax)
com.waveset.object.AttributeDefinition# setAttrType(String)	com.waveset.object.AttributeDefinition# setSyntax(Syntax)
com.waveset.object.AuditEvent#setAttributeMap(Map)	com.waveset.object.AuditEvent# setAuditableAttributes(Map)
com.waveset.object.AuditEvent# addAuditableAttributes(AccountAttributeType[], WSAttributes)	com.waveset.object.AuditEvent# setAuditableAttributes(Map)
com.waveset.object.AuditEvent#getAttributeMap()	com.waveset.object.AuditEvent# getAuditableAttributes()
com.waveset.object.AuditEvent#getAttributeValue(String)	com.waveset.object.AuditEvent# getAuditableAttributes()
com.waveset.object.AuditEvent# setAccountAttributesBlob(Map)	com.waveset.object.AuditEvent# setAccountAttributesBlob(Map,Map)

Verworfen	Nachfolger
com.waveset.object.AuditEvent# setAccountAttributesBlob(WSAttributes,List)	com.waveset.object.AuditEvent# setAccountAttributesBlob(WSAttributes, WSAttributes, List)
com.waveset.object.AuditEvent.setAccountAttributesBlob (List)	Verwenden Sie eine der anderen Formen von setAccountAttributesBlob (um neue, versuchte oder alte Werte zu ermöglichen).
com.waveset.object.AuditEvent.setAccountAttributesBlob (Map, Map)	Attributliste im Format Name=Wert;; speichern, dies wird wiederum in einem Blob gespeichert. Das Begrenzungszeichen ;; wird gefiltert.
com.waveset.object.AuditEvent.setAccountAttributesBlob (Map,Map,Set)	Verwenden Sie eine der anderen Formen von setAccountAttributesBlob (um neue, versuchte oder alte Werte zu ermöglichen).
com.waveset.object.CacheManager# getAllObjects(Type,AttributeCondition[])	com.waveset.object.CacheManager# listObjects(Type,AttributeCondition[])
com.waveset.object.CacheManager# getAllObjects(Type,WSAttributes)	com.waveset.object.CacheManager# listObjects(Type,WSAttributes)
com.waveset.object.CacheManager# getAllObjects(Type)	com.waveset.object.CacheManager# listObjects(Type)
com.waveset.object.Constants# MAX_SUMMARY_STRING_LENGTH	
com.waveset.object.EmailTemplate#setToAddress(String)	com.waveset.object.EmailTemplate#setTo(String)
com.waveset.object.EmailTemplate#getFromAddress()	com.waveset.object.EmailTemplate#getFrom()
com.waveset.object.EmailTemplate#getToAddress()	com.waveset.object.EmailTemplate#getTo()
com.waveset.object.EmailTemplate#setFromAddress(String)	com.waveset.object.EmailTemplate#setFrom(String)
com.waveset.object.EmailTemplate#VAR_FROM_ADDRES S	com.waveset.object.EmailTemplate#VAR_FROM
com.waveset.object.EmailTemplate#VAR_TO_ADDRESS	com.waveset.object.EmailTemplate#VAR_TO
com.waveset.object.Form#EL_HELP	com.waveset.object.GenericObject#toMap(int)
com.waveset.object.Form#getDefaultDataType()	com.waveset.object.Form#getDefaultSyntax()
com.waveset.object.Form#getType()	com.waveset.object.Form#getSyntax()
com.waveset.object.Form#setType(String)	com.waveset.object.Form#setSyntax(Syntax)
com.waveset.object.GenericObject.addAlias(String,String)	
com.waveset.object.GenericObject#toMap(boolean)	com.waveset.object.GenericObject#toMap(String,int)
com.waveset.object.GenericObject#toMap(String,boolean)	
com.waveset.object.IAPI	com.waveset.adapter.iapi.IAPI

<b>Verworfen</b>	<b>Nachfolger</b>
com.waveset.object.IAPIProcess	com.waveset.adapter.iapi.IAPIFactory
com.waveset.object.IAPIUser	com.waveset.adapter.iapi.IAPIUser
com.waveset.object.LighthouseContext#OP_NO_RESULT	
com.waveset.object.LoginConfig#getApp(String)	com.waveset.object.LoginConfig# getLoginApp(String)
com.waveset.object.MessageUtil# getActionDisplayKey(String)	
com.waveset.object.MessageUtil# getEventParmDisplayKey(String)	
com.waveset.object.MessageUtil# getResultDisplayKey(String)	
com.waveset.object.MessageUtil# getTypeDisplayKey(String)	com.waveset.ui.FormUtil# getTypeDisplayName(LighthouseContext,String)
com.waveset.object.PersistentObject()	com.waveset.object.PersistentObject(ObjectClass)
com.waveset.object.PersistentObject.fakeId(Type,String)	com.waveset.object.IDFactory.fakeID(type,name).to String()
com.waveset.object.PersistentObject.isId(String)	com.waveset.object.IDFactory.isValidID(id)
com.waveset.object.Principal()	com.waveset.object.Principal(ObjectClass)
com.waveset.object.Principal(String)	com.waveset.object.Principal(ObjectClass,String)
com.waveset.object.RemedyTemplate	
com.waveset.object.ReportCounter	
com.waveset.object.RepositoryProxy.sort(RepositoryResult)	
com.waveset.object.RepositoryResult#get(int)	
com.waveset.object.RepositoryResult#getId(int)	
com.waveset.object.RepositoryResult#getName(int)	
com.waveset.object.RepositoryResult#getObject(int)	
com.waveset.object.RepositoryResult#getRowCount()	
com.waveset.object.RepositoryResult#getRows()	
com.waveset.object.RepositoryResult#seek(int)	com.waveset.object.RepositoryResult#hasNext() com.waveset.object.RepositoryResult#next()
com.waveset.object.RepositoryResult#sort()	
com.waveset.object.RepositoryResult.Row# getSummaryAttributes()	com.waveset.object.RepositoryResult.Row# getAttributes()

<b>Verworfen</b>	<b>Nachfolger</b>
com.waveset.object.ResourceAttribute#setType(String)	com.waveset.object.ResourceAttribute#setSyntax(Syntax)
com.waveset.object.Role()	com.waveset.object.Role(ObjectClass)
com.waveset.object.Service()	com.waveset.object.Service(ObjectClass)
com.waveset.object.SourceManager	com.waveset.view.SourceAdapterManagerView
com.waveset.object.Syntax.getDescription()	
com.waveset.object.TaskInstance#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)
com.waveset.object.TaskInstance#VAR_RESULT_LIMIT	com.waveset.object.TaskInstance#setResultLimit(int) com.waveset.object.TaskInstance#getResultLimit()
com.waveset.object.TaskInstance#VAR_TASK_STATUS	
com.waveset.object.TaskTemplate#setMode(String)	com.waveset.object.TaskTemplate#setExecMode(String)
com.waveset.object.TaskTemplate#setMode(TaskDefinition.ExecMode)	com.waveset.object.TaskTemplate#setExecMode(TaskDefinition,ExecMode)
com.waveset.object.Type#AUDIT_CONFIG	
com.waveset.object.Type#AUDIT_PRUNER_TASK	
com.waveset.object.Type#AUDIT_QUERY	
com.waveset.object.Type#DISCOVERY	
com.waveset.object.Type#getSubtypes()	com.waveset.object.Type#getLegacyTypes()
com.waveset.object.Type#NOTIFY_CONFIG	
com.waveset.object.Type#REPORT_COUNTER	
com.waveset.object.Type#SUMMARY_REPORT_TASK	
com.waveset.object.Type#USAGE_REPORT	
com.waveset.object.Type#USAGE_REPORT_TASK	
com.waveset.object.UserUIConfig.emptyQueryableAttributeNames()	
com.waveset.object.UserUIConfig.emptyRepolIndexAttributes()	

<b>Verworfen</b>	<b>Nachfolger</b>
com.waveset.object.UserUIConfig.emptySummary AttributeNames()	
com.waveset.object.UserUIConfig#getAppletColumns()	com.waveset.object.UserUIConfig# getAppletColumnDefs()
com.waveset.object.UserUIConfig# getFindMatchOperatorDisplayNameKeys()	
com.waveset.object.UserUIConfig#getFindMatchOperators()	
com.waveset.object.UserUIConfig#getFindResultsColumns()	
com.waveset.object.UserUIConfig# getFindResultsSortColumn()	
com.waveset.object.UserUIConfig# getFindUserDefaultSearchAttribute()	
com.waveset.object.UserUIConfig# getFindUserSearchAttributes()	
com.waveset.object.UserUIConfig# getFindUserShowAttribute(int)	
com.waveset.object.UserUIConfig# getFindUserShowCapabilitiesSearch(int)	
com.waveset.object.UserUIConfig# getFindUserShowDisabled(int)	
com.waveset.object.UserUIConfig# getFindUserShowOrganizationSearch(int)	
com.waveset.object.UserUIConfig# getFindUserShowProvisioningSearch(int)	
com.waveset.object.UserUIConfig# getFindUserShowResourcesSearch(int)	
com.waveset.object.UserUIConfig# getFindUserShowRoleSearch(int)	
com.waveset.object.UserUIConfig# getQueryableAttributeNames	com.waveset.object.IDMSchema.get QueryableAttributeNames(String ocName)
com.waveset.object.UserUIConfig.getRepoIndexAttributes()	
com.waveset.object.UserUIConfig.getSummary AttributeNames()	com.waveset.object.IDMSchema#getSummary AttributeNames(String name)
com.waveset.object.UserUIConfig.getSummary AttributeTypes()	com.waveset.object.WSUser#getSummary AttributeTypes()
com.waveset.object.UserUIConfig# SUMMARY_ATTTR_TYPES_WRAPPER	

<b>Verworfen</b>	<b>Nachfolger</b>
com.waveset.object.ViewMaster()	
com.waveset.object.ViewMaster.ViewMaster(String,String)	
com.waveset.object.ViewMaster.ViewMaster(Subject,String)	
com.waveset.object.WorkItem.getDelegator()	
com.waveset.object.WorkItem.setDelegator(String)	
com.waveset.object.WSUser.clearExtendedAttributes()	
com.waveset.object.WSUser#getApproverDelegate()	com.waveset.object.WSUser# getWorkItemDelegate(String workItemType)
com.waveset.object.WSUser.getCurrentServiceRefs()	
com.waveset.object.WSUser#getDelegateHistory()	com.waveset.object.WSUser# getWorkItemDelegateHistory()
com.waveset.object.WSUser.getRoleAttributeRefs()	
com.waveset.object.WSUser# setApproverDelegate(WsUser.Delegate)	com.waveset.object.WSUser# addWorkItemDelegate(Delegate workItemDelegate)
com.waveset.object.WSUser#setDelegateHistory(List)	com.waveset.object.WSUser# setWorkItemDelegateHistory (ListworkItemDelegateHistory)
com.waveset.rpc.SimpleRpcHandler	
com.waveset.security.authn.EncryptedData	
com.waveset.security.authn.Encryptor	
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.server.Server#getResourceObjectGetCache()	
com.waveset.server.Server#getResourceObjectListCache()	
com.waveset.session.LocalSession# deleteAccountImmediate()	
com.waveset.session.LocalSession#getAdministrators(Map)	com.waveset.view.WorkItemUtil#getAdministrators
com.waveset.session.Session#listApprovers()	com.waveset.session.Session# getAdministrators(Map)
com.waveset.session#listControlledApprovers()	com.waveset.session#getAdministrators(Map)

Verworfen	Nachfolger
com.waveset.session#listSimilarApprovers(String adminName)	com.waveset.session#getAdministrators(Map)
com.waveset.session.SessionFactory#getApp(String)	com.waveset.session.SessionFactory#getLoginApp(String)
com.waveset.session#getApps()	com.waveset.session#getLoginApps()
com.waveset.session.WorkflowServices#ARG_TASK_DATE	com.waveset.object.Attribute#DATE
com.waveset.task.TaskContext#getAccessPolicy()	
com.waveset.task.TaskContext#getRepository()	
com.waveset.ui.SearchTableBase	
com.waveset.ui.util.FormUtil#getAdministrators(Session,List)	com.waveset.ui.util.FormUtil#getUser(LighthouseContext,Map)
com.waveset.ui.util.FormUtil#getAdministrators(Session,Map)	com.waveset.ui.util.FormUtil#getUser(LighthouseContext,Map)
com.waveset.ui.util.FormUtil#getApplications(LighthouseContext,List)	com.waveset.ui.util.FormUtil#getApplications(LighthouseContext,Map)
com.waveset.ui.util.FormUtil#getApplications(LighthouseContext)	com.waveset.ui.util.FormUtil#getApplications(LighthouseContext,Map)
com.waveset.ui.util.FormUtil#getApproverNames(Session,List)	com.waveset.ui.util.FormUtil#getUser(LighthouseContext,Map)
com.waveset.ui.util.FormUtil#getApproverNames(Session)	com.waveset.ui.util.FormUtil#getUser(LighthouseContext,Map)
com.waveset.ui.util.FormUtil#getApprovers(Session, List)	com.waveset.ui.util.FormUtil#getUser(LighthouseContext,Map)
com.waveset.ui.util.FormUtil#getApprovers(Session)	com.waveset.ui.util.FormUtil#getUser(LighthouseContext,Map)
com.waveset.ui.util.FormUtil#getCapabilities(LighthouseContext,List,Map)	com.waveset.ui.util.FormUtil#getCapabilities(LighthouseContext,Map)
com.waveset.ui.util.FormUtil#getCapabilities(LighthouseContext,List)	com.waveset.ui.util.FormUtil#getCapabilities(LighthouseContext,Map)
com.waveset.ui.util.FormUtil#getCapabilities(LighthouseContext,String,String)	com.waveset.ui.util.FormUtil#getCapabilities(LighthouseContext,Map)
com.waveset.ui.util.FormUtil#getCapabilities(LighthouseContext)	com.waveset.ui.util.FormUtil#getCapabilities(LighthouseContext,Map)
com.waveset.ui.util.FormUtil#getObjectNames(LighthouseContext,String,List,Map)	com.waveset.ui.util.FormUtil#getObjectNames(LighthouseContext,String,Map)
com.waveset.ui.util.FormUtil#getObjectNames(LighthouseContext,String,List)	com.waveset.ui.util.FormUtil#getObjectNames(LighthouseContext,String,Map)

<b>Verworfen</b>	<b>Nachfolger</b>
com.waveset.ui.util.FormUtil# getObjectNames (LighthouseContext,String,String,String,List,Map)	com.waveset.ui.util.FormUtil# getObjectNames(LighthouseContext,String,Map)
com.waveset.ui.util.FormUtil# getObjectNames (LighthouseContext,String,String,String,List)	com.waveset.ui.util.FormUtil# getObjectNames(LighthouseContext,String,Map)
com.waveset.ui.util.FormUtil# getObjectNames (LighthouseContext,Type,String,String,List,Map)	com.waveset.ui.util.FormUtil# getObjectNames(LighthouseContext,String,Map)
com.waveset.ui.util.FormUtil# getObjectNames(LighthouseContext,Type,String,String,List)	com.waveset.ui.util.FormUtil# getObjectNames(LighthouseContext,String,Map)
com.waveset.ui.util.FormUtil# getOrganizations(LighthouseContext,boolean,List)	com.waveset.ui.util.FormUtil# getOrganizationsDisplayNames (LighthouseContext,Map)
com.waveset.ui.util.FormUtil# getOrganizations(LighthouseContext,boolean)	com.waveset.ui.util.FormUtil# getOrganizationsDisplayNames (LighthouseContext,Map)
com.waveset.ui.util.FormUtil# getOrganizations(LighthouseContext,List)	com.waveset.ui.util.FormUtil# getOrganizationsDisplayNames (LighthouseContext,Map)
com.waveset.ui.util.FormUtil# getOrganizations(LighthouseContext)	com.waveset.ui.util.FormUtil# getOrganizationsDisplayNames (LighthouseContext,Map)
com.waveset.ui.util.FormUtil# getOrganizationsDisplayNames(LighthouseContext,boolean, List)	com.waveset.ui.util.FormUtil# getOrganizationsDisplayNames (LighthouseContext,Map)
com.waveset.ui.util.FormUtil# getOrganizationsDisplayNames(LighthouseContext,boolean)	com.waveset.ui.util.FormUtil# getOrganizationsDisplayNames (LighthouseContext,Map)
com.waveset.ui.util.FormUtil# getOrganizationsDisplayNames(LighthouseContext)	com.waveset.ui.util.FormUtil# getOrganizationsDisplayNames (LighthouseContext,Map)
com.waveset.ui.util.FormUtil# getOrganizationsDisplayNamesWithPrefixes (LighthouseContext,List)	com.waveset.ui.util.FormUtil# getOrganizationsDisplayNames (LighthouseContext,Map)
com.waveset.ui.util.FormUtil# getOrganizationsDisplayNamesWithPrefixes (LighthouseContext)	com.waveset.ui.util.FormUtil# getOrganizationsDisplayNames (LighthouseContext,Map)
com.waveset.ui.util.FormUtil# getOrganizationsWithPrefixes(LighthouseContext,List)	com.waveset.ui.util.FormUtil# getOrganizationsDisplayNames (LighthouseContext,Map)

<b>Verworfen</b>	<b>Nachfolger</b>
com.waveset.ui.util.FormUtil# getOrganizationsWithPrefixes(LighthouseContext)	com.waveset.ui.util.FormUtil# getOrganizationsDisplayNames (LighthouseContext,Map)
com.waveset.ui.util.FormUtil# getSimilarApproverNames(Session,String)	com.waveset.ui.util.FormUtil# getUsers(LighthouseContext,Map)
com.waveset.ui.util.FormUtil# getSimilarApproverNames(Session)	com.waveset.ui.util.FormUtil# getUsers(LighthouseContext,Map)
com.waveset.ui.util.FormUtil# getUnassignedOrganizations(LighthouseContext,List)	com.waveset.ui.util.FormUtil# getOrganizationsDisplayNames (LighthouseContext,Map)
com.waveset.ui.util.FormUtil# getUnassignedOrganizations(LighthouseContext)	com.waveset.ui.util.FormUtil# getOrganizationsDisplayNames (LighthouseContext,Map)
com.waveset.ui.util.FormUtil# getUnassignedOrganizationsDisplayNames (LighthouseContext,List)	com.waveset.ui.util.FormUtil# getOrganizationsDisplayNames (LighthouseContext,Map)
com.waveset.ui.util.FormUtil# getUnassignedOrganizationsDisplayNames (LighthouseContext,Map)	com.waveset.ui.util.FormUtil# getOrganizationsDisplayNames (LighthouseContext,Map)
com.waveset.ui.util.FormUtil# getUnassignedOrganizationsDisplayNames (LighthouseContext)	com.waveset.ui.util.FormUtil# getOrganizationsDisplayNames (LighthouseContext,Map)
com.waveset.ui.util.FormUtil# getUnassignedOrganizationsDisplayNamesWithPrefixes (LighthouseContext,List)	com.waveset.ui.util.FormUtil# getOrganizationsDisplayNames (LighthouseContext,Map)
com.waveset.ui.util.FormUtil# getUnassignedOrganizationsDisplayNamesWithPrefixes (LighthouseContext)	com.waveset.ui.util.FormUtil# getOrganizationsDisplayNames (LighthouseContext,Map)
com.waveset.ui.util.FormUtil# getUnassignedOrganizationsWithPrefixes (LighthouseContext,List)	com.waveset.ui.util.FormUtil# getOrganizationsDisplayNames (LighthouseContext,Map)
com.waveset.ui.util.FormUtil# getUnassignedOrganizationsWithPrefixes (LighthouseContext)	com.waveset.ui.util.FormUtil# getOrganizationsDisplayNames (LighthouseContext,Map)
com.waveset.ui.util.FormUtil# getUnassignedResources(LighthouseContext,List,List)	com.waveset.ui.util.FormUtil# getUnassignedResources(LighthouseContext,Map)
com.waveset.ui.util.FormUtil# getUnassignedResources(LighthouseContext,String)	com.waveset.ui.util.FormUtil# getUnassignedResources(LighthouseContext,Map)
com.waveset.ui.util.FormUtil# getUnassignedResources(LighthouseContext,String,List)	com.waveset.ui.util.FormUtil# getUnassignedResources(LighthouseContext,Map)

<b>Verworfen</b>	<b>Nachfolger</b>
com.waveset.ui.util.html.Component#isNoWrap()	
com.waveset.ui.util.html.HtmlHeader#NORMAL_BODY	
com.waveset.ui.util.html.MultiSelect#isLockhart()	
com.waveset.ui.util.html#setHelpKey(String)	
com.waveset.ui.util.html#setLockhart(boolean)	
com.waveset.ui.util.html#setNoWrap(boolean)	
com.waveset.ui.util.html.TransactionSigner.getSupportedKeyStoreTypes()	com.waveset.ui.util.html.TransactionSigner.getSupportedKeyStoreType
com.waveset.ui.util.html.TransactionSigner.setSupportedKeyStoreTypes(String)	com.waveset.ui.util.html.TransactionSigner.setSupportedKeyStoreType
com.waveset.ui.util.html.WizardPanel#setPreviousLabel(String)	com.waveset.ui.util.html.WizardPanel#setPrevLabel(String)
com.waveset.ui.web.account.SearchForm	
com.waveset.ui.web.account.SearchTable	
com.waveset.ui.web.account.UserAppletTable	
com.waveset.ui.web.resources.ResourceAppletTable	
com.waveset.ui.web.roles.SearchRoleForm	
com.waveset.ui.web.roles.SearchRoleTable	
com.waveset.util.ArgumentsParser.parse(String[])	com.waveset.util.ArgumentsParser.parse(String[] args,List additionalArguments,boolean ignoreIncorrectUsage)
com.waveset.util.CaseInsensitiveStringComparator	java.lang.String.CASE_INSENSITIVE_ORDER
com.waveset.util.ConnectionPool.getConnection(String,String,String,boolean,String)	com.waveset.util.ConnectionPool#getConnection(String,String,String,boolean,String)
com.waveset.util.ConnectionPool.getConnection(String,String,String)	com.waveset.util.ConnectionPool#getConnection(String,String,String,String)
com.waveset.util.ConnectionPool.getConnection(String,String,String,String,String,String,boolean)	com.waveset.util.ConnectionPool#getConnection(String driverClass,String driverPrefix,String url,String user,String password,boolean checkConnection,String validationSql)
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.JSSE#installIfAvailable()	

<b>Verworfen</b>	<b>Nachfolger</b>
com.waveset.util.ITrace	com.sun.idm.logging.Trace
com.waveset.util.PipeDelimitedParser	com.waveset.util.ConfigurableDelimitedFileParser
com.waveset.util.PdfReportRenderer# render(Element,boolean,String,OutputStream)	com.waveset.util.PdfReportRenderer# render(Element,boolean,String,OutputStream, String,boolean)
com.waveset.util.PdfReportRenderer# render(Element,boolean,String)	com.waveset.util.PdfReportRenderer# render(Element,boolean,String,String,boolean)
com.waveset.util.PdfReportRenderer# render(Report,boolean,String,OutputStream)	com.waveset.util.PdfReportRenderer# render(Report,boolean,String,OutputStream, String,boolean)
com.waveset.util.PdfReportRenderer# render(Report,boolean,String)	com.waveset.util.PdfReportRenderer# render(String,boolean,String,String,boolean)
com.waveset.util.PooledConnection.isValid()	isValid(String SQL)
com.waveset.util.Quota#getQuota()	
com.waveset.util.ReportRenderer# renderToPdf(Report,boolean,String,OutputStream)	com.waveset.util.ReportRenderer# renderToPdf(Report,boolean,String,OutputStream, String,boolean)
com.waveset.util.ReportRenderer# renderToPdf(Report,boolean,String)	com.waveset.util.ReportRenderer# renderToPdf(Report,boolean,String,String,boolean)
com.waveset.util.Trace#data(long,Object,String,byte[])	com.sun.idm.logging.trace.Trace# data(long,String,byte[])
com.waveset.util.Trace#entry(long,Object,String,Object[])	com.sun.idm.logging.trace.Trace# entry(long,String,Object[])
com.waveset.util.Trace#entry(long,Object,String,String)	com.sun.idm.logging.trace.Trace#entry(long,String)
com.waveset.util.Trace#entry(long,Object,String)	com.sun.idm.logging.trace.Trace#entry(long,String)
com.waveset.util.Trace#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)
com.waveset.util.Trace#exit(long,Object,String,boolean)	com.sun.idm.logging.trace.Trace# exit(long,String,boolean)
com.waveset.util.Trace#exit(long,Object,String,int)	com.sun.idm.logging.trace.Trace#exit(long,String,int)
com.waveset.util.Trace#exit(long,Object,String,long)	com.sun.idm.logging.trace.Trace# exit(long,String,long)
com.waveset.util.Trace#exit(long,Object,String,Object)	com.sun.idm.logging.trace.Trace# exit(long,String,Object)
com.waveset.util.Trace#exit(long,Object,String)	com.sun.idm.logging.trace.Trace#exit(long,String)

<b>Verworfen</b>	<b>Nachfolger</b>
com.waveset.util.Trace#getTrace()	com.sun.idm.logging.trace.TraceManager# getTrace(String)
com.waveset.util.Trace#getTrace(Class)	com.sun.idm.logging.trace.TraceManager# getTrace(String)
com.waveset.util.Trace#getTrace(String)	com.sun.idm.logging.trace.TraceManager# getTrace(String)
com.waveset.util.Trace#level1(Class,String)	com.sun.idm.logging.trace.Trace#level1(String)
com.waveset.util.Trace#level1(Object,String)	com.sun.idm.logging.trace.Trace#level1(String)
com.waveset.util.Trace#level2(Class,String)	com.sun.idm.logging.trace.Trace#level2(String)
com.waveset.util.Trace#level2(Object,String)	com.sun.idm.logging.trace.Trace#level2(String)
com.waveset.util.Trace#level3(Class,String)	com.sun.idm.logging.trace.Trace#level3(String)
com.waveset.util.Trace#level3(Object,String)	com.sun.idm.logging.trace.Trace#level3(String)
com.waveset.util.Trace#level4(Class,String)	com.sun.idm.logging.trace.Trace#level4(String)
com.waveset.util.Trace#level4(Object,String)	com.sun.idm.logging.trace.Trace#level4(String)
com.waveset.util.Trace# variable(long,Object,String,String,boolean)	com.sun.idm.logging.trace.Trace# variable(long,String,String,boolean)
com.waveset.util.Trace# variable(long,Object,String,String,int)	com.sun.idm.logging.trace.Trace# variable(long,String,String,int)
com.waveset.util.Trace# variable(long,Object,String,String,long)	com.sun.idm.logging.trace.Trace# variable(long,String,String,long)
com.waveset.util.Trace# variable(long,Object,String,String,Object)	com.sun.idm.logging.trace.Trace# variable(long,String,String,Object)
com.waveset.util.Trace#void info(long,Object,String,String)	com.sun.idm.logging.trace.Trace# info(long,String,String)
com.waveset.util.Util#DATE_FORMAT_CANONICAL	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)
com.waveset.util.Util#debug(Object)	
com.waveset.util.Util#getCanonicalDateFormat()	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)

Verworfen	Nachfolger
com.waveset.util.Util#getLocalHostName()	#getServerId() (Abrufen einer eindeutigen Server-ID)
com.waveset.util.Util# getOldCanonicalDateString(Date,boolean)	com.waveset.util.Util#getCanonicalDateString(Date)
com.waveset.util.Util.getUniqueld()	com.waveset.util.Util.generateGUID()
com.waveset.util.Util#rfc2396URLPieceEncode(String)	com.waveset.util.RFC2396URLPieceEncode# encode(String)
com.waveset.util.Util# rfc2396URLPieceEncode(String,String)	com.waveset.util.RFC2396URLPieceEncode# encode(String,String)
com.waveset.view.ViewUtil.getExtendedAttributes (LighthouseContext)	com.sun.idm.util.ObjectClasses.getExtended Attributes(ObjectClass)
com.waveset.view.ViewUtil.isExtendedAttribute (ViewMaster vm, String name)	ObjectClasses.getExtendedAttributes(ObjectClass)
com.waveset.view.ViewUtil.reloadExtendedAttributes()	
com.waveset.view.ViewUtil.setExtendedAttributes (LighthouseContext, List attributes)	IDMSchemaConfiguration
com.waveset.workflow.WorkflowContext# VAR_CASE_TERMINATED	com.waveset.object.WFProcess# VAR_CASE_TERMINATED

## Veraltete JSP-Dateien und URLs

Die folgende Tabelle enthält die JSP-Dateien und URLs, deren Unterstützung eingestellt wurde. Soweit verfügbar, ist auch der jeweilige Nachfolger angegeben.

Verworfen	Nachfolger
account/listapplet.jsp	
resources/listapplet.jsp	
resources/reconLinkAccountFilter.jsp	

---

## Veraltete Konfigurationsobjekte

Die folgende Tabelle enthält die Konfigurationsobjekte, deren Unterstützung eingestellt wurde. Soweit verfügbar, ist auch der jeweilige Nachfolger angegeben.

<b>Verworfen</b>	<b>Nachfolger</b>
UserExtendedAttributes	IDMSchemaConfiguration
UserUIConfig	IDMSchemaConfiguration

---

## Veraltete Ansichten und Pfadausdrücke

Die folgende Tabelle enthält die Ansichten und Pfadausdrücke, deren Unterstützung eingestellt wurde. Soweit verfügbar, ist auch der jeweilige Nachfolger angegeben.

<b>Verworfen</b>	<b>Nachfolger</b>
DelegateApproversViewer	DelegateWorkItemsViewer

# Erweiterungen und Korrekturen der Dokumentation

Dieser Abschnitt enthält neue Informationen und Korrekturen, die nach der Herausgabe der Identity Manager 8.0-Dokumentation bekannt wurden. Die Informationen sind wie folgt unterteilt:

- [Identity Manager 8.0 Administration](#)
- [Identity Manager Technical Deployment Overview](#)
- [Identity Manager Workflows, Forms, and Views](#)
- [Identity Manager Deployment Tools](#)
- [Umfang der Lokalisierung](#)
- [Onlinehilfe](#)

---

## *Identity Manager 8.0 Administration*

Dieser Abschnitt enthält eine Korrektur für das Dokument *Sun Identity Manager Administration*:

- Auf Seite 340 enthält das Handbuch „Administration“ den folgenden Hinweis:

Identity Manager uses email templates to deliver information and requests for action to administrators, approvers, and users. For more information about Identity Manager email templates, see the section titled Understanding Email Templates in this guide.
- Der Querverweis sollte stattdessen auf den Abschnitt „Customizing Email Templates“ (S. 196) gehen.

---

# Identity Manager Technical Deployment Overview

Dieser Abschnitt enthält neue Informationen und Dokumentationskorrekturen für das Dokument *Sun Identity Manager Technical Deployment Overview*:

Die folgenden Informationen werden dem Kapitel „Private Labeling of Identity Manager“ im Dokument *Identity Manager Technical Deployment Overview* hinzugefügt bzw. dort korrigiert:

- Das Lighthouse-Konto wird nun als *Identity Manager*-Konto bezeichnet. Sie können diese Namensänderung mit Hilfe eines benutzerdefinierten Katalogs aussetzen. 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
```

Weitere Informationen über benutzerdefinierte Kataloge finden Sie in [Appendix B, „Enabling Internationalization“](#).

- Der Abschnitt „Changing the Appearance of the User Interface Navigation Menus“ sollte die folgenden Informationen enthalten:

Für die Endbenutzerseiten von Identity Manager legt das Benutzerformular für die Endbenutzer-Navigation in `enduser.xml` fest, wie die horizontale Navigationsleiste angezeigt wird. Die Endbenutzerseiten enthalten eine Datei `userHeader.jsp`, die wiederum eine weitere JSP-Datei namens `menuStart.jsp` enthält. Die Datei `menuStart.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 (`horizontal`) oder als vertikales Strukturmenü (`vertical`) dargestellt werden soll.  
(Standardwert: `horizontal`)

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

---

**HINWEIS** Wenn Sie eigene JavaScript-Funktionen in der Endbenutzer-Navigationsleiste (Registerkarten) implementieren, müssen Sie zum Verweis auf dieses Formular `endUserNavigation` verwenden. Beispiel:

```
document.forms['endUserNavigation'].elements
```

---

- Mit Hilfe von CSS-Stildefinitionen 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 auskommentiert) hinzu. Die Werte können dann an die Anforderungen des Benutzers angepasst werden.

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

th#UserListTreeContent_Col1 {
    width: 1px;
}

th#UserListTreeContent_Col2 {
    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 Mauszeiger in einen horizontalen Pfeil für Größenänderungen. Durch Klicken mit der linken Maustaste und Ziehen des Mauszeigers wird die Größe der Spalte geändert. (Die Größenänderung wird beim Loslassen der Maustaste beendet.)

- Kunden, die benutzerdefinierte JavaScript-Funktionen in der Endbenutzer-Navigationleiste (Registerkarten) verwenden wollen, müssen dieses Formular mithilfe von `endUserNavigation` referenzieren, z. B. `document.forms['endUserNavigation'].elements.(ID-13769)`
- 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:

- Öffnen Sie entweder in der Identity Manager-IDE oder einem Editor Ihrer Wahl die Datei `compliance/dashboard.jsp`:
- 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 gezeigt, um die Prüfungen auf die letzten sechs Monate einzuschränken. Es werden die oben beschriebenen Kennzeichner verwendet:

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

bis

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

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 */
.TabLvl1Div {
    background-image:url(../images/other/dot.gif);
    background-repeat:repeat-x;
    background-position:left bottom;
    background-color:#333366;
    padding:6px 10px 0px;
}
a.TabLvl1Lnk:link, a.TabLvl1Lnk:visited {
    display:block;
    padding:4px 10px 3px;
    font: bold 0.95em sans-serif;
```

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

```

        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 #aba1b5;
}
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 #aba1b5;
}
table.TabLvl2Tbl td.TabLvl2TblSelTd {
    border-bottom:none;
    background-image:url(../images/other/dot.gif);
    background-repeat:repeat-x;
    background-position:left bottom;
}

```

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

```
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 in der Endbenutzeroberfläche von Identity Manager 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`.

- Im Codebeispiel in Abschnitt „Changing Masthead Appearance“ ist irrtümlich „MstDiv“ als erste Zeile aufgeführt. Diese Zeile muss „MstDiv“ lauten. (ID-16072)

- Der Abschnitt „Customizing the Browser Bar“ wurde wie folgt überarbeitet: (ID-16073)

Der Produktname in der Titelleiste des Browsers kann jetzt durch einen lokalisierbaren Text Ihrer Wahl ersetzt werden.

1. Importieren Sie die folgende XML-Datei:

#### Codebeispiel 1      Zu importierende XML-Datei

```
<?xml version='1.0' encoding='UTF-8'?>
<!DOCTYPE Configuration PUBLIC 'waveset.dtd' 'waveset.dtd'>
<Configuration name='AltMsgCatalog'>
  <Extension>
    <CustomCatalog id='AltMsgCatalog' enabled='true'>
      <MessageSet language='en' country='US'>
        <Msg id='UI_BROWSER_TITLE_PROD_NAME_OVERRIDE'>Neuer Name</Msg>
      </MessageSet>
    </CustomCatalog>
  </Configuration>
</Extension>
```

2. Laden Sie mithilfe der Identity Manager-IDE das SystemConfiguration-Objekt zum Bearbeiten. Fügen Sie auf der obersten Hierarchieebene ein neues Attribut hinzu:

Name = customMessageCatalog

Type = string

Value = AltMsgCatalog

3. Öffnen Sie das generische Objekt „ui.web“ und suchen Sie das Attribut browserTitleProdNameOverride. Setzen Sie diesen Wert auf „true“.
4. Speichern Sie diese Änderung im SystemConfiguration-Objekt, und starten Sie den Anwendungsserver neu.

- Die Anleitung zum Anpassen von Anmeldeseiten im Abschnitt „Customizing Identity Manager End User Pages“ sollte die folgenden Informationen über Meldungsschlüssel enthalten. (ID-16072)

JSP- bzw. Identity Manager-Komponente	Betroffene Oberfläche	Meldungsschlüssel
Anmeldeseite - TITEL	Administrator/Endbenutzer	UI_LOGIN_TITLE_TO_RESOURCE UI_LOGIN_CHALLENGE
Anmeldeseite - UNTERTITEL	Administrator/Endbenutzer	Wählen Sie je nach Anmeldemodus einen Schlüssel aus: Passwort vergessen, Benutzer-ID vergessen, Authentifizierung mittels geheimer Fragen. UI_LOGIN_WELCOME3 UI_LOGIN_WELCOME4 UI_LOGIN_WELCOME5 UI_LOGIN_WELCOME6 UI_LOGIN_CHALLENGE_INFO
staticLogout.jsp und user/staticUserLogout.jsp	Administrator/Endbenutzer	UI_LOGIN_TITLE
continueLogin.jsp	Administrator	UI_LOGIN_IN_PROGRESS_TITLE UI_LOGIN_WELCOME

Die folgenden Schlüssel werden nicht mehr verwendet:

- UI\_LOGIN\_TITLE\_LONG
- UI\_LOGIN\_WELCOME2
- Die Anleitung „Changing the Default “Logged in as ...” Text“ sollte wie folgt korrigiert werden: (ID-18545)
- Nach der Aufzählung zu deactivateDate im Abschnitt „features“ von Anhang A, „Editing Configuration Objects“, sollte der folgende Hinweis eingefügt werden.

---

**HINWEIS** Sie können sowohl activateDate als auch deactivateDate auf true setzen, selbst wenn userAssignment.manual nicht diesen Wert hat. Wenn Sie beide Attribute für einen Rollentyp auf true setzen und wenn die Rolle optional in einer anderen Rolle enthalten ist, können Sie einen Aktivierungs- und Deaktivierungstermin festlegen, wenn Sie die optionale Rolle einem Benutzer zuweisen.

---

## Den Standardtext „Angemeldet als“ ändern

1. Importieren Sie die folgende XML-Datei:

```
<?xml version='1.0' encoding='UTF-8'?>
<!DOCTYPE Configuration PUBLIC 'waveset.dtd' 'waveset.dtd'>
<Configuration name='AltMsgCatalog'>
  <Extension>
    <CustomCatalog id='AltMsgCatalog' enabled='true'>
      <MessageSet language='en' country='US'>
        <Msg id='UI_NAV_FOOT_LOG_AS'>Eigener Text {0}!</Msg>
      </MessageSet>
    </CustomCatalog>
  </Extension>
</Configuration>
```

2. Fügen Sie dem SystemConfiguration-Objekt die folgende Zeile innerhalb des <Configuration><Extension><Object>-Elements hinzu:  
  
<Attribute name='customMessageCatalog' value='AltMsgCatalog' />
3. Speichern Sie die Änderung und starten Sie Ihren Anwendungsserver neu.

# Identity Manager Workflows, Forms, and Views

Dieser Abschnitt enthält neue Informationen und Dokumentationskorrekturen für das Dokument *Sun Identity Manager Workflows, Forms, and Views*.

- Sie können die Richtlinienprüfung in Ihrem Benutzerformular deaktivieren, indem Sie dem Formular das folgende Feld hinzufügen: (ID-13346)

```
<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 1, „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 Benutzeranspruchsobjekte 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)

Name des Arbeitsablaufs	Zweck
Korrektur	Korrektur für eine einzelne Korrekturfunktion, die mit einer einzelnen Konformitätsverletzung arbeitet
Korrektur der Zugriffsprüfung	Korrektur für eine einzelne Korrekturfunktion, die mit einer einzelnen UserEntitlement arbeitet
Bescheinigung	Bescheinigung für einen einzelnen Bescheiniger, der mit einem 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 „Scripted Task Executor“ eingebettet ist, ist eine erneute Kompilierung und Bereitstellung nicht erforderlich.)

## Kapitel 2, „Workflow Services“

- Die Argumenttabelle für die Workflow-Dienstszugung `createView` ist falsch. In der folgenden Tabelle werden die für diesen Dienst verfügbaren Argumente beschrieben. (ID-14201)

**Tabelle 1**

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

- In der Beschreibung zum Workflow-Dienst `disableUser` muss klargestellt werden, dass dieser Dienst das Identity Manager-Konto sowie das Ressourcenkonto standardmäßig deaktiviert. (ID-14572) Übergeben Sie das folgende Argument, wenn das Identity Manager-Konto nicht deaktiviert werden soll:

```
<Argument name='doWaveset' value='false' />
```

Die Diskussion der Argumente dieser Methode muss wie folgt lauten:

Name	Erforderlich	Gültige Werte	Beschreibung
<code>op</code>	ja	<code>disableUser</code>	
<code>accountId</code>	ja		Legt den Identity Manager-Benutzer fest, für den Konten deaktiviert werden sollen.
<code>doWaveset</code>	nein	<code>true/false</code>	<code>true</code> : Das Identity Manager-Konto ist deaktiviert. Wenn kein Wert angegeben ist, wird er standardmäßig auf <code>true</code> gesetzt, und das Konto wird deaktiviert.
<code>services</code>	nein		Eine Liste mit Ressourcen, die deaktiviert werden sollen. Wenn dieses Argument nicht angegeben wird, werden alle Ressourcenkonten des Benutzers deaktiviert.

- In diesem Dokument ist das Attribut `viewId` der Methoden `checkoutView` und `createView` irrtümlich als „`viewid`“ angegeben. Bitte beachten Sie, dass dieser Parameter richtig `viewId` heißt. (ID-15411)
- Das Kapitel enthält jetzt die folgende Beschreibung der Workflow-Dienste zum Sperren und Entsperren.(ID-17070)

## Workflow-Bereitstellungsdienst „lock“

Sperren eines Objekts.

Argument	Erforderlich	Beschreibung
<i>subject</i>	nein	Effektiver Betreff für den Aufruf. Wenn nichts angegeben ist, verwendet Identity Manager das Attribut <i>subject</i> der Aufgabe. Wenn der Wert dieses Arguments leer ist, führt Identity Manager keine Autorisierung aus.
<i>options</i>	nein	(Map) Eine Wertematrix mit Optionsname/Optionswert-Paaren. Wenn nichts angegeben ist, werden die untenstehenden spezifischen Argumente verwendet. Wenn hier etwas angegeben ist, haben die untenstehenden spezifischen Argumente Vorrang vor den Argumenten in dieser Optionsmatrix.
<i>accountId</i>	nein	(Zeichenkette) Der Name des Identity Manager-Benutzers, der gesperrt werden soll.
<i>adminName</i>	nein	(Zeichenkette) Der Name des Administrators, der die Operation ausführt.
<i>loginAppName</i>	nein	(Zeichenkette) Der Anmeldename für die Anwendung.
<i>op</i>	ja	Gültiger Wert: <i>unlock</i>

Diese Methode gibt einen Nullwert zurück.

## Workflow-Bereitstellungsdienst „unlock“

Entsperren eines gesperrten Objekts.

**Tabelle 1**

Argument	Erforderlich	Beschreibung
<i>subject</i>	nein	(Zeichenkette) Effektiver Betreff für den Aufruf. Wenn nichts angegeben ist, wird das Attribut „subject“ der Aufgabe verwendet. Wenn der Wert dieses Arguments leer ist, wird keine Autorisierung ausgeführt.
<i>options</i>	nein	(Map) Eine Wertematrix mit Optionsname/Optionswert-Paaren. Wenn nichts angegeben ist, verwendet Identity Manager die untenstehenden spezifischen Argumente. Wenn hier etwas angegeben ist, haben die untenstehenden spezifischen Argumente Vorrang vor den Argumenten in dieser Optionsmatrix.
<i>accountId</i>	nein	(Zeichenkette) Der Name des Identity Manager-Benutzers, der entsperrt werden soll.
<i>adminName</i>	nein	(Zeichenkette) Der Name des Administrators, der die Operation ausführt.
<i>loginAppName</i>	nein	(Zeichenkette) Der Anmeldename für die Anwendung.
<i>doLighthouse</i>	nein	(Boolean) Legt fest, ob das Identity Manager-Konto entsperrt werden soll oder nicht.
<i>doResources</i>	nein	(Boolean) Legt fest, ob die Benutzerressourcen entsperrt werden sollen oder nicht.

**Tabelle 1**

<b>Argument</b>	<b>Erforderlich</b>	<b>Beschreibung</b>
<i>doAuthenticators</i>	nein	(Boolean) Ist dieser Wert auf „true“ gesetzt, wird die gesamte Pass-Through-Authentifizierung entsperrt.
<i>op</i>	ja	Gültiger Wert: <i>unlock</i>

Diese Methode gibt ein WavesetResult-Objekt mit dem Ergebnis der Operation zurück.

- Die Beschreibung des Sitzungs-Workflowdienstes „removeDeferredTask“ wurde wie folgt überarbeitet: (ID-17302)

Dient zum Entfernen einer verschobenen Aufgabe aus einem Identity Manager-Objekt. Identity Manager stellt sicher, dass der Administrator, der den Workflow aufgerufen hat, auch zum Entfernen des Objekts autorisiert ist.

**Tabelle 2** Methodenargumente für „removeDeferredTask“

<b>Name</b>	<b>Erforderlich</b>	<b>Gültige Werte</b>	<b>Beschreibung</b>
<i>Typ</i>	nein	Typenliste	Der Typ des Objekts, aus dem die verschobene Aufgabe entfernt werden soll. Wenn nichts angegeben ist, wird „type“ standardmäßig auf <i>user</i> gesetzt.
<i>name</i>	ja		Der Name des Objekts, aus dem die verschobene Aufgabe entfernt werden soll.
<i>task</i>			Der Name der TaskDefinition, die entfernt werden soll.

## 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 grundlegender 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: Jeder Benutzer kann ein Formular festlegen. Welches Formular ein Benutzer verwenden sollte, hängt von der Organisation des Benutzers ab.

## 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.

**Tabelle 2**

Formularname	Zugeordneter Name	Zuweisung auf Benutzerebene	Zweck
Access Approval List	accessApprovalList		Zeigt eine Liste mit Bescheinigungs-Arbeits-elementen an
Access Review Delete Confirmation	accessReviewDeleteConfirmation		Bestätigt das Löschen einer Zugriffsprüfung
Access Review Delete Confirmation	accessReviewAbortConfirmation		Bestätigt die Beendigung einer Zugriffsprüfung
Access Review Dashboard	accessReviewDashboard		Zeigt eine Liste mit allen Zugriffsprüfungen an
Access Review Remediation Form	accessReviewRemediationWorkItem	Ja	Zeigt alle UE-basierten Korrekturarbeitselemente an
Access Review Summary	accessReviewSummary		Zeigt die Details einer bestimmten Zugriffsprüfung an
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-Arbeits-elemente an
UserEntitlementForm	userEntitlementForm		Zeigt den Inhalt eines UserEntitlement an

**Tabelle 2**

<b>Formularname</b>	<b>Zugeordneter Name</b>	<b>Zuweisung auf Benutzerebene</b>	<b>Zweck</b>
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
maxThreads	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.
userLock	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.
scanDelay	0	Gibt die Zeit (in ms) an, die bis zur Ausgabe eines neuen Threads 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 (WARNING), 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, in der 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 im Beispielcode den Meldungsschlüssel, der den Meldungstext kennzeichnet, der im Meldungsfeld 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>
      <notnull>
        <ref>username</ref>
      </notnull>
      <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.

- Dieses Kapitel enthält jetzt die folgende Beschreibung der Anzeigekomponente „Hidden“:

Die Anzeigeklasse „Hidden“ entspricht der HTML-Komponente `<input type=hidden' />`. Diese Komponente unterstützt nur Datentypen mit einem Datenwert, da es keine Möglichkeit zum zuverlässigen Serialisieren und Deserialisieren von Datentypen mit mehreren Datenwerten gibt. (ID-16904)

Wenn Sie eine Liste als Zeichenkette ausgeben möchten, muss diese Liste explizit in eine Zeichenkette konvertiert werden. Beispiel:

**Codebeispiel 0-1**      Ausgabe von Datentypen mit mehreren Datenwerten mit der Anzeigekomponente „Hidden“

```
<Field name='testHiddenFieldList' >
  <Display class='Hidden' / >
  <Derivation>
    <invoke name='toString'> <List> <String>aaaa</String> <String>bbbb</String>
  </List> </invoke>
  </Derivation>
</Field>
```

- Sie können jetzt die Eigenschaft `RequiresChallenge` im Formular „Passwort ändern“ der Endbenutzeroberfläche setzen, damit Benutzer zunächst für ihr Konto ihr altes Passwort eingeben müssen, bevor sie es ändern können. Ein Beispiel zum Setzen dieser Eigenschaft finden Sie im Basisformular „Change Password“ in `enduser.xml`. (ID-17309)

## 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	String	Vom System generiert
orgDisplayName	Lesen/Schreiben	String	Ja
orgType	Lesen/Schreiben	String	Nein
orgId	Lesen	String	Vom System generiert
orgAction	Schreiben	String	Nein
orgNewDisplayName	Schreiben	String	Nein
orgParentName	Lesen/Schreiben	String	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	String	Nein
orgViewUserForm	Lesen/Schreiben	String	Nein
orgPolicies	Lesen/Schreiben	Liste	Nein
orgAuditPolicies	Lesen/Schreiben	Liste	Nein
renameCreate	Lesen/Schreiben	String	Nein
renameSaveAs	Lesen/Schreiben	String	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?
<code>orgContainerId</code>	Lesen	String	Vom System generiert
<code>orgContainerTypes</code>	Lesen	Liste	Vom System generiert
<code>orgContainers</code>	Lesen	Liste	Vom System generiert
<code>orgParentContainerId</code>	Lesen	String	Vom System generiert
<code>orgResource</code>	Lesen/Schreiben	String	Ja, für Verzeichniszuordnung bzw. virtuelle Organisation

<b>Name</b>	<b>Bearbeitbar?</b>	<b>Datentyp</b>	<b>Obligatorisch?</b>
orgResourceType	Lesen	String	Vom System generiert
orgResourceId	Lesen	String	Vom System generiert
orgRefreshAllOrgsUserMembers	Schreiben	String	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?
orgUserMembersRule	Lesen/Schreiben	String	Nein
orgUserMembersRuleCacheTimeout	Lesen/Schreiben	String	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 Arbeitselementtyp enthält.

- Wenn `delegatedApproversRule` den Wert `delegateApproversTo` hat, ist hier die ausgewählte Regel angegeben.
- Wenn `manager` den Wert `delegateApproversTo` hat, besitzt dieses Attribut keinen Wert.

### *accounts[Lighthouse].delegatesHistory*

Führt Delegate-Objekte 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 Delegation 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 Delegation gestartet werden soll.
<code>endDate</code>	Gibt das Datum an, an dem die Delegation 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 Indexwerte (\*) 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		String	Ja
Status		String	Ja
Benutzer		String	Ja
userId		String	Ja
attestorHint		String	Nein
userView		GenericObject	Ja
reviewInstanceId		String	Ja
reviewStartDate		String	Ja
scanId		String	Ja
scanInstanceId		String	Ja
approvalWorkflowName		String	Ja
organizationId		String	Ja
attestorComments.name		String	Nein
attestorComments.attestor		String	Nein
attestorComments.time		String	Nein
attestorComments.timestamp		String	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.

***Benutzer***

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.

***reviewInstanceId***

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.

***scanInstanceId***

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.
- Die Beschreibung der isTrue-Funktion wurde wie folgt überarbeitet: (ID-17078)

Diese Funktion wird verwendet, wenn in Zeichenketten enthaltene Boolesche Werte statt 0 und 1 die Werte „true“ und „false“ enthalten. 1 Argument wird übergeben.

Die folgenden Werte entsprechen dem Wert „true“. Alle anderen Werte werden als „false“ interpretiert.

- die Zeichenfolge true
- der boolesche Wert „true“
- ein Ganzzahlwert ungleich 0

Der Rückgabewert ist:

- 0 – Das Argument ist logisch unwahr.
- 1 – Das Argument ist logisch wahr.

Beispiel

Der folgende Ausdruck gibt 0 zurück.

```
<isTrue>  
  <s>>false</s>  
</isTrue>
```

## 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 `MenuBar`s oder `MenuItem`s 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>
```

- Diesem Kapitel wurden die folgenden Erläuterungen zur ListEditor-Komponente hinzugefügt: (ID-16518)

## ListEditor

Gibt eine bearbeitbare Zeichenkettenliste aus.

**Tabelle 3** Eigenschaften der ListEditor-Komponente

Eigenschaft	Beschreibung
listTitle	(String) Die Beschriftung, die Identity Manager neben der grafischen Darstellung des ListEditor-Objekts anzeigt.
pickListTitle	(String) Die Beschriftung für die pickList-Komponente.
valueMap	(Map) Eine Matrix mit Beschriftungen für die Werte der Liste.
allowDuplicates	(Boolean) Der Wert true gibt an, dass Identity Manager in der Liste Duplikate zulässt.
allowTextEntry	(Boolean) Der Wert true gibt an, dass Identity Manager ein Texteingabefeld und eine Schaltfläche zum Hinzufügen anzeigt.
fixedWidth	(Boolean) Der Wert true gibt an, dass die Komponente eine feste Breite haben soll (das gleiche Verhalten wie bei der Multiselect-Komponente).
ordered	(Boolean) Der Wert true gibt an, dass die Reihenfolge der Werte wichtig ist.
sorted	(Boolean) Der Wert true gibt an, dass die Werte der Auswahlliste sortiert werden sollen. Wenn Datenwerte mehrere Werte enthalten und nicht sortiert sind, sortiert Identity Manager die Werteliste ebenfalls.
pickValueMap	(List oder Map) Eine Matrix mit Beschriftungen für die Werte der Auswahlliste.
pickValues	(List) Verfügbare Werte in der pickList-Komponente. Ist dieser Wert null, wird die picklist nicht angezeigt.
height	(Integer) Die bevorzugte Höhe.
width	(Integer) Die bevorzugte Breite. Kann von Containern als Eigenschaft der Tabellenzelle, in der das Objekt ausgegeben werden soll, verwendet werden.

## Beispiel

Das folgende Beispiel eines Formulars mit Registerkarten zeigt ein Formularfeld an, das die ListEditor-Anzeigeklasse verwendet:

```
<Field name='accounts[Sim1].Group'>
  <Display class='ListEditor' action='true'>
    <Property name='listTitle' value='stuff' />
    <Property name='allowTextEntry'>
      <Boolean>true</Boolean>
    </Property>
    <Property name='ordered'>
      <Boolean>true</Boolean>
    </Property>
  </Display>
  <Expansion>
    <ref>accounts[Sim1].Group</ref>
  </Expansion>
</Field>
```

Dieser Codeausschnitt erstellt ein Feld, in dem der Kunde einem Benutzer Gruppen hinzufügen bzw. diese vom Benutzer wieder entfernen kann.

---

**HINWEIS** Für diese Anzeigeklasse ist normalerweise eine Zeichenkettenliste als Eingabeparameter erforderlich. So erstellen Sie aus einzelnen Zeichenketten eine Zeichenkettenliste:

```
<Expansion>
  <appendAll><ref>accounts[Sim1].Group</ref></appendAll>
</Expansion>
```

---

- Die Anzeigekomponente Text enthält die neue Eigenschaft `autocomplete`. (ID-17310) Durch Setzen der Eigenschaft `autocomplete` auf `off` wird verhindert, dass Browser Berechtigungsdaten von Benutzern auf deren Computern speichern.

Sie können diese Funktion in XPRESS-Eingabefeldern durch Hinzufügen dieser Anzeigeeigenschaft implementieren. Alle anderen Werte außer `off` verhindern, dass Identity Manager das Attribut `autocomplete` im erzeugten HTML-Formular ausgibt. Dies entspricht dem Verhalten beim Nichtsetzen dieser Eigenschaft.

## Aktivieren von „autocomplete“ für Identity Manager-Anmeldeseiten

Zum Aktivieren dieser Funktion für die Anmeldeseiten von Identity Manager setzen Sie das Systemkonfigurationsobjekt `ui.web.disableAutocomplete` auf `true`.

Die Anmeldeseiten von Identity Manager sind `login.jsp`, `continueLogin.jsp`, `user/login.jsp` und `user/continueLogin.jsp`.

Alle anderen Identity Manager-Anmeldeseiten werden von XPRESS generiert, und Sie müssen diese Formulare entsprechend bearbeiten, wenn Sie die neue Anzeigeeigenschaft dort nutzen wollen. In diesen Formularen, die sich im Beispielverzeichnis befinden, ist diese Eigenschaft standardmäßig auskommentiert.

- Anonyme Benutzeranmeldung
- Formular mit Anmeldefragen
- Formular für Validierung der anonymen Endbenutzereinschreibung
- Formular für Abschluss der anonymen Endbenutzereinschreibung
- Benutzer-ID finden

## 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
Zugriffsprüfung	<code>accessReview</code>	Ausführung einer Zugriffsprüfung
Zugriffsabfrage	<code>accessReviewScan</code>	Ausführung einer Zugriffsabfrage
Erneute Suche nach Zugriffsprüfung	<code>accessReviewRescan</code>	Ausführung einer erneuten Zugriffsabfrage
Erneute Prüfung der Überwachungsrichtlinien	<code>auditPolicyRescan</code>	Ausführung einer erneuten Überwachungsrichtliniensuche
Zugriffsprüfung abbrechen	<code>abortAccessReview</code>	Beendigung einer Zugriffsprüfung
Zugriffsprüfung löschen	<code>deleteAccessReview</code>	Löschen einer Zugriffsprüfung
Zugriffsprüfung auf Statusobjekte wiederherstellen	<code>recoverAccessReview</code>	Wiederherstellung fehlender Zugriffsprüfungs-Statusobjekte von Überwachungsprotokollen

---

# Identity Manager Deployment Tools

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

- Das Kapitel „Using the Identity Manager-IDE“ aus früheren Versionen wurde in dieser Version entfernt. Informationen zur Installation und Konfiguration der Identity Manager Integrated Development Environment (Identity Manager-IDE) finden Sie jetzt unter <https://identitymanageride.dev.java.net>. (ID-17700)

Auf den folgenden Seiten finden Sie zur einfacheren Referenz die Anleitung für den Identity Manager-Profiler sowie die häufig gestellten Fragen (FAQ) zu Identity Manager.

---

**HINWEIS** Der Identity Manager-Profiler wird erst ab Version 7.1 Update 1 unterstützt.

---

## Arbeiten mit dem Identity Manager-Profiler

Identity Manager besitzt jetzt ein Profilerdienstprogramm, das Ihnen in Ihrer Bereitstellung beim Auffinden von Leistungsproblemen bei Formularen, Java, Regeln, Workflows und XPRESS hilft.

Formulare, Java, Regeln, Workflows und XPRESS können Leistungs- und Skalierungsprobleme verursachen. Der Profiler analysiert, wieviel Zeit diese verschiedenen Bereiche zur Ausführung benötigen. Somit können Sie feststellen, ob sie zu Leistungs- und Skalierungsproblemen beitragen und – wenn dies der Fall ist – welche Teile dieser Objekte diese Probleme verursachen.

In diesem Abschnitt wird die Arbeit mit dem Identity Manager-Profiler beschrieben. Darüber hinaus finden Sie hier eine Anleitung für das Finden und Eliminieren von Leistungsproblemen in Ihrer Bereitstellung. Die Informationen sind wie folgt unterteilt:

- [Übersicht](#)
- [Erste Schritte](#)
- [Arbeiten mit dem Profiler](#)
- [Tutorium: Beheben von Leistungsproblemen](#)

---

**HINWEIS** Der Identity Manager-Profiler wird erst ab Version 7.1 Update 1 unterstützt.

---

## Übersicht

Dieser Abschnitt enthält einen Überblick über Leistungsmerkmale und Funktionen des Identity Manager-Profilers. Die Informationen sind wie folgt unterteilt:

- [Hauptfunktionen](#)
- [Wie findet und verwaltet der Profiler Quellcode?](#)
- [Interpretationshinweise zu den Statistiken](#)

### *Hauptfunktionen*

Mit dem Profiler können Sie folgende Funktionen ausführen:

- Erstellen von „Snapshots“ für Profiling-Daten
 

Unter einem *Snapshot* versteht man die kumulative Gesamtheit der Profilingdaten seit dem letzten Löschen aller gesammelten Profilermessergebnisse.
- Snapshotergebnisse können in vier verschiedenen Datenansichten dargestellt werden:
  - **Ansicht der Aufrufhierarchie** - zeigt eine Hierarchieansicht mit den Aufrufzeiten und -dauern im gesamten System an.
  - **Hotspot-Ansicht** - zeigt eine flache Knotenliste mit den aufsummierten Aufrufzeiten unabhängig von der aufrufenden Routine an.
  - **Rückverfolgungsansicht** - zeigt einen invertierten Aufrufstack mit allen Aufrufketten, von denen ein bestimmter Knoten (der sog. *Root-Knoten*) aufgerufen wurde, an.
  - **Ansicht der aufgerufenen Routinen** - zeigt eine Gesamtaufrufhierarchie für den Root-Knoten (unabhängig von dessen aufrufender Kette) an.
- Sie müssen angeben, welche Informationen im Snapshot enthalten sein sollen.
  - Sie können alle Elemente von Formularen, Workflows und XPRESS-Objekten angeben oder den Inhalt auf eine bestimmte Menge spezifischer Elemente beschränken.
  - Sie können festlegen, welche Java-Methoden und -Konstruktoren mit dem Profiling analysiert werden sollen. Die Instrumentierung von Identity Manager- und benutzerspezifischen Klassen wird unterstützt.
- Sie sollten Ihre Projekt-Snapshots wie folgt verwalten:
  - Speichern Sie den Snapshot im Verzeichnis `nbproject/private/idm-profiler` Ihres Projekts oder in einem beliebigen anderen Verzeichnis außerhalb Ihres Projekts.

---

**HINWEIS** Im Abschnitt „Saved Snapshots“ der IDM-Profilersicht können Sie sich eine Liste aller gespeicherten Snapshots anzeigen lassen.

---

- Sie können Snapshots innerhalb Ihres Projekts oder aus einem anderen Verzeichnis außerhalb Ihres Projekts heraus öffnen.
- Sie können Snapshots löschen.
- Sie können bestimmte Knoten nach Namen suchen.

### *Wie findet und verwaltet der Profiler Quellcode?*

In diesem Abschnitt wird beschrieben, wie der Profiler Quellcode für die folgenden Identity Manager-Objekte findet und verwaltet:

- [Für Formulare, Workflows, Regeln und XPRESS-Objekte](#)
- [Für Java-Quellen](#)

---

**TIPP** In der Aufrufhierarchie- bzw. Hotspot-Ansicht können Sie auf einen Knoten, der einer Java-Methode, einem Workflow, Formular, einer Regel oder einem XPRESS-Objekt entspricht, doppelklicken.

---

**Für Formulare, Workflows, Regeln und XPRESS-Objekte** Wenn Sie mit dem Profiler einen Snapshot erstellen, evaluiert der Server alle Profilingdaten und findet heraus, von welchem Quellcode die betreffenden Daten abhängen. Der Server ruft dann diesen Quellcode aus dem Repository ab und fügt ihn in den Snapshot ein. Deswegen können Sie sicher sein, dass die in einem Snapshot angezeigten Identity Manager-Objekte auch wirklich den Zustand besitzen, den sie während der Erstellung des Snapshot einnahmen.

Dieser Prozess erhöht zwar die Snapshotgröße, die Quellcodegröße beträgt aber nur einen Bruchteil der Gesamtobjektgröße. So können Sie Snapshots an den Technischen Support von Sun senden, ohne einzelne Dateien schicken zu müssen.

**Für Java-Quellen** Wenn Sie einen Snapshot von Java-Quellcode erstellen, lädt der Client den Snapshot herunter und sucht dann in diesem Snapshot alle referenzierten Java-Quellen aus dem Projekt heraus. Beim Speichern des Snapshots komprimiert und archiviert der Client den Quellcode und hängt ihn an das Ende des Snapshots an.

Wenn Sie dann den Snapshot anzeigen und zum Java-Quellcode gehen, überprüft der Client zunächst den Inhalt des Snapshots. Wenn der Client den Inhalt dort nicht finden kann, überprüft er den Projektinhalt. Dieser Vorgang ermöglicht das Senden eines Snapshots mit Profiling-Daten aus benutzerspezifischem Java-Code und Identity Manager-Code.

---

**HINWEIS** Bei Snapshots aus Java-Quellcode kann nicht vorausgesetzt werden, dass der Code auf dem aktuellsten Stand (d. h. identisch mit dem Code auf dem Server) bzw. stets verfügbar ist.

---

## *Interpretationshinweise zu den Statistiken*

Die folgenden Abschnitte enthalten Informationen, die bei der Auswertung der vom Profiler ermittelten Ergebnisse zu berücksichtigen sind.

- [Berechnung der Eigenausführungszeit](#)
- [Konstruktoraufrufe](#)
- [Dämon-Threads](#)

**Berechnung der Eigenausführungszeit** Zur Berechnungen der Eigenausführungszeit eines Root-Knotens subtrahiert der Profiler die Ausführungszeiten aller vom Root-Knoten aufgerufenen Routinen von der Gesamtausführungszeit des Knotens.

Deswegen fließt die Ausführungszeit eines uninstrumentierten, vom Root-Knoten aufgerufenen Knotens in die Eigenausführungszeit des Root-Knotens ein. Wenn die Eigenausführungszeit eines Root-Knotens relativ groß ist, sollten sie der Ursache unbedingt nachgehen. Es könnte beispielsweise sein, dass Sie nicht die passenden Methoden analysieren und deswegen an der falschen Stelle suchen.

Nehmen wir z. B. an, dass Methode A Methode B aufruft.

Die Ausführungszeit von Methode A beträgt isg. 10 s (dies schließt den Aufruf von B ein) und der Aufruf von B dauert isg. 10 s.

Wenn sowohl Methode A als auch Methode B instrumentiert sind, wird dies im Aufrufstack festgehalten. Sie sehen, dass Methode A eine Eigenausführungszeit von 0 s und B von 10 s besitzt. Das heißt, die gesamten 10 Sekunden wurden in Methode B verbracht. Wenn B jedoch nicht instrumentiert ist, sehen Sie nur, dass der Aufruf von Methode A 10 s dauert und die Eigenausführungszeit von Methode A 10 s beträgt. So kann es sein, dass Sie annehmen, dass das Problem statt in Methode B in Methode A liegt.

Ihnen fällt vielleicht auf, dass die Eigenausführungszeiten von JSPs während der Erstcompilierung sehr hoch sind. Wenn Sie die erfassten Ergebnisse löschen und die Seite dann erneut anzeigen, ist der Wert für die Eigenausführungszeit bedeutend niedriger.

**Konstruktoraufrufe** Wegen vorhandener Einschränkungen bei der Java-Instrumentierungsstrategie erscheinen Erstaufrufe zu `this()` oder `super()` auf der gleichen Aufrufebene wie der Konstruktor statt darunter. Hierzu ein Beispiel:

```

class A
{
    public A()
    {
        this(0);
    }
    public A(int i)
    {
    }
}

```

und:

```

class B
{
    public static void test()
    {
        new A();
    }
}

```

Die Aufrufhierarchie sieht wie folgt aus:

```

B.test()
  -A.<init>(int)
  -A.<init>()
... und nicht etwa so:
B.test()
  -A.<init>()
    -A.<init>(int)

```

**Dämon-Threads** Lassen Sie sich nicht von einer scheinbar langen Zeit verwirren, die in Dämon-Threads von Identity Manager (z. B. `ReconTask.WorkerThread.run()` oder `TaskThread.WorkerThread.run()`) verbraucht wurde. Die meiste Zeit hier wird im Leerlauf, d. h. mit dem Warten auf Ereignisse verbraucht. Sie müssen diese Aufrufe näher untersuchen, um zu sehen, wieviel Zeit in solchen Threads beim eigentlichen Auftreten eines Ereignisses verbraucht wird.

## Erste Schritte

In diesem Abschnitt wird beschrieben, wie Sie den Profiler starten und wie Sie mit den einzelnen Funktionen der grafischen Benutzeroberfläche des Profilers arbeiten. Die Informationen sind wie folgt unterteilt:

- [Vorbereitung](#)
- [Starten des Profilers](#)
- [Festlegen von Optionen für das Profiling](#)

### Vorbereitung

Da der Profiler sehr speicherintensiv ist, sollten Sie die Speicherressourcen für den Server und die Netbeans Java Virtual Machine (JVM) erhöhen.

- So erhöhen Sie Speicherressourcen für den Server:
  - a. Öffnen Sie das Netbeans-Fenster und klicken Sie auf die Registerkarte „Laufzeit“.
  - b. Klappen Sie den Serverknoten auf, klicken Sie mit der rechten Maustaste auf „Bundled Tomcat“ und wählen Sie aus dem Menü „Eigenschaften“.
  - c. Demarkieren Sie in der Registerkarte „Verbindung“ das Kontrollkästchen „HTTP-Monitor aktivieren“, wenn das Dialogfeld „Server Manager“ angezeigt wird.
  - d. Klicken Sie auf die Registerkarte „Plattform“ und setzen Sie die VM-Optionen auf **-Xmx1024M**.
- So erhöhen Sie Speicherressourcen für die Netbeans JVM:
  - a. Öffnen Sie die Datei *Netbeans-InstallationsVerz\etc\netbeans.conf* und suchen Sie die folgende Zeile:

```
netbeans_default_options="-J-Xms32m -J-Xmx ...
```
  - b. Setzen Sie den Wert `-J-Xmx` auf **-J-Xmx1024M**.
  - c. Speichern und schließen Sie die Datei.

Nach Abschluss dieses Vorgangs können Sie den Profiler wie im nächsten Abschnitt beschrieben starten.

## Starten des Profilers

Der Profiler kann aus dem Identity Manager-IDE-Fenster mit einer der folgenden Methoden gestartet werden:

- Klicken Sie auf das Symbol „Start Identity Manager Profiler on Main Project“  in der Menüleiste.

---

**HINWEIS** Das Symbol „Start Identity Manager Profiler on Main Project“ ist aktiviert, wenn das Identity Manager-Projekt die Version 7.1 Update 1 oder höher hat.

---

- Wählen Sie in der Menüleiste „Window > IDM Profiler“.
- Im Explorer-Fenster wird das Fenster „Identity Manager Profiler“ angezeigt. Wählen Sie in diesem Fenster aus dem Dropdown-Menü „Current Project“ ein Identity Manager-Projekt aus und klicken Sie dann auf das Symbol „Start Identity Manager Profiler“  im Abschnitt „Controls“.
- Klicken Sie mit der rechten Maustaste auf ein Projekt im Projektfenster und wählen Sie anschließend im Popup-Menü „Start Identity Manager Profiler“.
- Wählen Sie ein Projekt im Projektfenster aus und wählen Sie anschließend in der Menüleiste „IdM > Start Identity Manager Profiler“.

Nach dem Start des Profilers wird das Dialogfeld „Profiler Options“ angezeigt, sodass Sie die von Ihnen gewünschten Optionen für das Profiling einstellen können. Eine Anleitung zum Einstellen dieser Optionen finden Sie im Abschnitt [„Festlegen von Optionen für das Profiling“](#) auf Seite 158.

## Arbeiten mit dem Profiler

In diesem Abschnitt werden die Funktionen der grafischen Benutzeroberfläche des Profilers beschrieben und wie Sie mit diesen arbeiten können. Die Informationen sind wie folgt unterteilt:

- [Festlegen von Optionen für das Profiling](#)
- [Arbeiten mit der IDM-Profilersicht](#)
- [Arbeiten mit der Snapshot-Ansicht](#)
- [Arbeiten mit Kontextmenüoptionen](#)
- [Suchen eines Snapshots](#)
- [Speichern eines Snapshots](#)

## Festlegen von Optionen für das Profiling

Das Dialogfeld „Profiler Options“ enthält folgende Registerkarten:

- [Modus](#)
- [IDM Object Filters](#)
- [Java Filters](#)
- [Sonstiges](#)

Mit den Optionen in diesen Registerkarten legen Sie fest, für welche Objekte das Profiling ausgeführt werden soll und welche Elemente im Profil anzuzeigen sind.

Klicken Sie auf „OK“, um den Profiler zu starten, wenn Sie die Optionen für das Profiling festgelegt haben. Je nach Projektkonfiguration führt der Profiler einen der folgenden beiden Vorgänge aus:

- Bei regulären Identity Manager-Projekten mit einer *eingebetteten* Identity Manager-Instanz führt der Profiler ein vollständiges Build durch, stellt das Projekt auf dem NetBean-Anwendungsserver bereit und startet den Profiler.
- Bei regulären Identity Manager-Projekten mit einer *externen* Identity Manager-Instanz oder Identity Manager-Fernprojekten verbindet sich der Profiler mit der für das Projekt konfigurierten Identity Manager-Instanz.

---

**HINWEIS** Sie können „IdM > Set Identity Manager Instance“ auswählen, um die Aktion der Identity Manager-Instanz für das Projekt festzulegen.

---

**Modus** Die Registerkarte „Mode“ enthält folgende Optionen:

- **IDM Objects Only:** Wählen Sie diese Option, um das Profiling für Formulare, Regeln, Workflows und XPRESS-Objekte durchzuführen. Es wird kein Profiling für Java-Objekte ausgeführt.
- **Java and IDM Objects:** Wählen Sie diese Option, um das Profiling für Regeln, Workflows, Java- und XPRESS-Objekte durchzuführen.

---

**HINWEIS**

- Die Option „Java and IDM Objects“ ist für reguläre Identity Manager-Projekte mit *externer* Identity Manager-Instanz bzw. Identity Manager-Fernprojekte nicht verfügbar.
- Sie können den Modus nicht ändern, während das Profiling läuft. Wenn Sie den Modus ändern möchten, muss der Profiler angehalten werden.

---

**IDM Object Filters** Die Registerkarte „IDM Object Filters“ enthält folgende Optionen:

- **Show IDM Object details:**
  - Markieren Sie dieses Kontrollkästchen, um alle Formulare, Workflows und XPRESS-Elemente, die ausgeführt werden, in den Snapshot einzubeziehen.
  - Demarkieren Sie dieses Kontrollkästchen, wenn nur die folgende Elemente im Snapshot enthalten sein sollen:
    - <invoke>
    - <new>
    - <Regel>
    - <Formular>
    - <WFProcess>
    - <ExScript>
    - <ExDefun>
    - <FieldRef>
    - <Action> (für Zusatzaktionen von Workflow-Anwendungen)
- **Einbeziehen von anonymem Quellcode:**

---

**HINWEIS** Unter *anonymen Quellcode* versteht man Formulare (oder Teile davon), die dynamisch generiert werden (z. B. Anmeldeformulare oder Formulare, die auf fehlende Felder hinweisen) und keinem der persistenten Formulare im Identity Manager-Repository entsprechen.

---

- Markieren Sie dieses Kontrollkästchen, wenn anonymes Quellcode in den Snapshot einbezogen werden soll.
- Demarkieren Sie dieses Kontrollkästchen, wenn kein anonymes Quellcode im Snapshot enthalten sein soll.

**Java Filters** In der Registerkarte „Java Filters“ können Sie:

- Java-Filter einbeziehen bzw. ausschließen
- neue Filter erstellen
- vorhandene Filter löschen
- Standardfilter wiederherstellen

Java-Filter sind in Bezug auf Methodenmuster gegeben und werden in ein- bzw. ausschließenden, auf dem *kanonischen Methodennamen* basierenden Mustern angegeben. Kanonische Methodennamen sehen wie folgt aus:

*Klassenname\_mit\_vollständigem\_Pfad.Methodenname (Parametertyp-1, Parametertyp-2, ...)*

---

**HINWEIS** Für Konstruktoren lautet der *Methodenname* <init>.

---

Hier sind einige Beispiele:

- Zum Ausschließen von Konstruktoren markieren Sie das Kontrollkästchen „Exclude“ und fügen den folgenden Filter hinzu:

```
*.<init>(*)
```

- Zum Ausschließen aller Konstruktoren mit einem einzigen Parameter `org.w3c.dom.Element` markieren Sie das Kontrollkästchen „Exclude“ und fügen den folgenden Filter hinzu:

```
*.<init>(org.w3c.dom.Element)
```

- Zum Ausschließen aller Identity Manager-Klassen markieren Sie das Kontrollkästchen „Exclude“ und fügen die folgenden Filter hinzu:

```
"com.waveset.*"
```

```
"com.sun.idm.*"
```

- Wenn Sie nur benutzerspezifischen Code instrumentieren wollen, markieren Sie das Kontrollkästchen „Exclude“, entfernen den Filter `* include` zu Beginn und fügen dann den folgenden Filter hinzu:

```
"com.yourcompany.*"
```

---

**HINWEIS** Die letzten beiden Beispiele haben gegenwärtig den gleichen Effekt, da Filter nur auf benutzerspezifische Klassen und Identity Manager-Klassen angewendet werden.

---

Falls erforderlich, können Sie durch entsprechendes Ändern der folgenden Zeilen in der Datei `build.xml` noch andere JAR-Dateien instrumentieren. Zum Beispiel:

```
<instrument todir="${lighthouse-dir-profiler}/WEB-INF" verbose="${instrumentor.verbose}"
includeMethods="${profiler.includes}" excludeMethods="${profiler.excludes}">
  <fileset dir="${lighthouse-dir}/WEB-INF">
    <include name="lib/idm*.jar"/>
    <include name="classes/**/*.class"/>
  </fileset>
</instrument>
```

Standardmäßig sind in der Konfiguration alle benutzerspezifischen und die meisten Identity Manager-Klassen enthalten. Eine Reihe von Identity Manager-Klassen sind zwangsläufig nicht enthalten, da deren Einbeziehung den Profiler funktionsunfähig machen würde.

So sind z. B. Klassen aus den Workflow-, Formular- und XPRESS-Programmen nicht enthalten, da der Profiler beim Profiling von Java- und Identity Manager-Objekten unverständliche Ausgaben generieren würde.

Bitte beachten Sie, dass Java-Filter eine erheblich feinere Filtergranularität als IDM-Objektfilter bieten. Java-Instrumentierungen verlangsamen die Ausführungszeit *erheblich*, was bei den Profiling-Ergebnissen zu drastischen Abweichungen führen kann. Da Identity Manager-Objekte interpretiert und nicht compiliert werden, ist der Einfluss der Instrumentierung auf die Ausführungszeit vernachlässigbar. So gibt es beispielsweise keinen Grund, Workflow A auszuschließen und Workflow B einzubeziehen usw.

---

**HINWEIS** Sie können Java-Filter nicht ändern, während das Profiling läuft. Wenn Sie die Java-Filter ändern möchten, muss der Profiler angehalten werden.

---

**Sonstiges** Die Registerkarte „Miscellaneous“ enthält folgende Optionen:

- **Prune snapshot nodes where execution time is 0:**

- Deaktivieren Sie die Option (standardmäßig deaktiviert), wenn der Snapshot Aufrufdaten für alle ausgeführten Entitäten (auch für die, deren Ausführungszeit 0 ist) enthalten soll.

Unter Umständen ist die Verfolgung der Aufrufanzahl bei Knoten nützlich, deren Ausführungszeit gleich null ist.

- Aktivieren Sie diese Option, um diese Knoten auszuschließen. Damit können Sie sich auf die relevantesten Profiling-Daten konzentrieren. Darüber hinaus kann durch Aktivieren dieser Option die Größe eines Profiler-Snapshots erheblich reduziert werden.

- **Automatically Open Browser Upon Profiler Start:**

- Aktivieren Sie diese Option (standardmäßig aktiviert), wenn beim Start des Profilers automatisch ein Browser geöffnet werden soll, in dem die Identity Manager-Instanz angezeigt wird, für die das Profiling ausgeführt wird.
- Deaktivieren Sie diese Option, wenn kein Browser geöffnet werden soll.

- **Include Java Sources in Snapshot:**

- Aktivieren Sie diese Option (standardmäßig aktiviert), wenn Java-Quellcode für alle Java-Methoden enthalten sein soll, die im Snapshot der Profiling-Daten referenziert werden sollen. Diese Einstellung sollte stets für Snapshots unter Produktionsbedingungen verwendet werden. Benutzerspezifischer Java-Code beansprucht wenig Ressourcen, und es wichtig, diesen für die Fehlersuche zur Verfügung zu haben.
- Deaktivieren Sie diese Option, wenn Sie das Profiling für Identity Manager durchführen und der vollständige Identity Manager-Quellcode verfügbar ist.

In solchen Fällen sollte der Identity Manager-Quellcode nicht in den Snapshots enthalten sein, da dadurch die Snapshot-Größe extrem erhöht wird. Weitere Informationen finden Sie unter [„Wie findet und verwaltet der Profiler Quellcode?“](#) auf [Seite 153](#).

## Arbeiten mit der IDM-Profilersicht

Die IDM-Profilersicht enthält die folgenden Bereiche:

- Bereich „Current Project“
- Bereich „Controls“
- Bereich „Status“
- Bereich „Saved Snapshots“

**Bereich „Current Project“** Der Bereich „Current Project“ besteht aus einem Dropdown-Menü, in dem alle aktuellen Projekte aufgeführt sind. In diesem Menü wählen Sie das Projekt aus, für das ein Profiling durchgeführt werden soll.

**Bereich „Controls“** Der Bereich „Controls“ enthält vier Symbole. Diese sind in der folgenden Tabelle beschrieben:

Symbol	Zweck	
	Start Identity Manager Profiler	Startet den Profiler und öffnet das Dialogfeld „Profiler Options“.
	Stop Identity Manager Profiler	Stoppt den Profiler.
	Reset Collected Results	Löscht alle bis hierhin erfassten Profiling-Ergebnisse.
	Modify Profiling	Öffnet das Dialogfeld „Profiler Options“ erneut, sodass Sie an den Einstellungen Änderungen vornehmen können.

**Bereich „Status“** Im Bereich „Status“ wird gemeldet, ob der Profiler mit dem Host eine Verbindung herstellen konnte, und es werden Informationen zum Starten, Laufen und Stoppen des Profilers angezeigt.

**Bereich „Profiling Results“** Der Bereich „Profiling Results“ enthält zwei Symbole. Diese sind in der folgenden Tabelle beschrieben:

Symbol	Zweck	
	Start Identity Manager Profiler	Startet den Profiler und öffnet das Dialogfeld „Profiler Options“.
	Reset Collected Results	Löscht alle bis hierhin erfassten Profiling-Ergebnisse.

**Bereich „Saved Snapshots“** Der Bereich „Saved Snapshots“ enthält eine Liste aller gespeicherten Snapshots.

---

**HINWEIS** Eine Anleitung zum Speichern von Snapshots finden Sie im Abschnitt [„Speichern eines Snapshots“](#) auf Seite 168.

---

Darüber hinaus dienen die folgenden Schaltflächen zum Verwalten dieser Snapshots:

- **Open:** Klicken Sie auf diese Schaltfläche, um einen gespeicherten Snapshot im Fenster „Snapshot View“ zu öffnen.

---

**TIPP** Sie können auch auf einen Snapshot in dieser Liste doppelklicken, um ihn zu öffnen.

---

- **Delete:** Wählen Sie einen Snapshot in der Liste „Saved Snapshots“ aus und klicken Sie auf diese Schaltfläche, um den Snapshot zu löschen.
- **Save As:** Wählen Sie einen Snapshot in der Liste aus und klicken Sie auf diese Schaltfläche, um den Snapshot in einem beliebigen externen Verzeichnis zu speichern.
- **Load:** Klicken Sie auf diese Schaltfläche, um einen in einem beliebigen externen Verzeichnis gespeicherten Snapshot im Fenster „Snapshot View“ zu öffnen.

### *Arbeiten mit der Snapshot-Ansicht*

Beim Öffnen eines Snapshots werden die Ergebnisse in der Snapshot-Ansicht angezeigt. Diese befindet sich rechts oben in der Identity Manager-IDE.

Ein Snapshot bietet verschiedene Anzeigemöglichkeiten für Profiling-Daten. Diese werden in den folgenden Abschnitten beschrieben:

- [Ansicht der Aufrufhierarchie](#)
- [Hotspot-Ansicht](#)
- [Rückverfolgungsansicht](#)
- [Ansicht der aufgerufenen Routinen](#)

**Ansicht der Aufrufhierarchie** Die Ansicht der Aufrufhierarchie zeigt eine Hierarchieansicht mit den Aufrufzeiten und -dauern im gesamten System an.

Diese Tabelle enthält drei Spalten:

- **Spalte „Call Tree“:** Hier werden alle Knoten aufgeführt.

Knoten der obersten Ebene können folgende Entitäten sein:

- `Thread.run()`-Methoden für verschiedene Hintergrund-Threads im System

Wenn Sie beispielsweise Java-Profiling aktiviert haben, sehen Sie hier die Methode `ReconTask.WorkerThread.run()`.

- Zeitdauern für Anforderungen

Wenn Sie beispielsweise die URL `idm/login.jsp` angezeigt haben, sehen Sie in der obersten Ebene einen Eintrag für `idm/login.jsp`. Die Spalte „Time“ zeigt die Gesamtzeit, die für diese Anforderung (bzw. Anforderungen) benötigt wurde. Die Spalte „Invocations“ zeigt, wie oft diese Seite insgesamt aufgerufen wurde. Sie können diese Daten näher untersuchen, um festzustellen, welche Aufrufe zur Gesamtzeit beigetragen haben.

---

**HINWEIS** Die Ansicht der Aufrufhierarchie enthält darüber hinaus Knoten mit Eigenausführungszeiten. Unter Eigenausführungszeit versteht man die Zeit, die ein Knoten für seine eigene Ausführung benötigt. (Weitere Informationen dazu finden Sie unter „[Berechnung der Eigenausführungszeit](#)“ auf Seite 154.)

---

- **Spalte Time:** Die Zeit, die in jedem Knoten verbracht wurde, als dieser Knoten von seiner übergeordneten Routine aufgerufen wurde. Die Werte sind Prozentsätze relativ zur Ausführungszeit der aufrufenden Routine.
- **Spalte Invocations:** Hält fest, wie oft jeder Knoten von seiner übergeordneten Routine aufgerufen wurde.

**Hotspot-Ansicht** Die Hotspot-Ansicht zeigt eine flache Knotenliste mit den aufsummierten Aufrufzeiten unabhängig von der aufrufenden Routine an.

Diese Ansicht enthält die folgenden Spalten:

- **Self Time:** Die Gesamtzeit, die in jedem Knoten verbracht wurde.
- **Invocations:** Hält fest, wie oft jeder Knoten insgesamt von seiner übergeordneten Routine aufgerufen wurde.
- **Time:** Die Gesamtzeit, die in jedem Knoten und in allen von diesem Knoten aufgerufenen Unterroutrinen verbracht wurde.

**Rückverfolgungsansicht** Die Rückverfolgungsansicht zeigt einen invertierten Aufrufstack mit allen Aufrufketten, von denen jeder Knoten aufgerufen wurde, an.

Mit diesen Statistikdaten können Sie nachvollziehen, wieviel Zeit Sie durch Eliminierung einer bestimmten Aufrufkette aus dem betreffenden Knoten einsparen würden.

Sie können die Rückverfolgungsansicht von allen anderen Snapshot-Ansichten aufrufen, indem Sie mit der rechten Maustaste auf einen Knoten klicken (der dann in der Rückverfolgungsansicht zum sog. *Root-Knoten* wird) und aus dem Kontextmenü die Option „Show Back Traces“ auswählen.

---

**HINWEIS** In der Rückverfolgungsansicht haben die Werte in den Spalten „Time“ und „Invocations“ eine andere Bedeutung:

- **Time:** Die Werte in dieser Spalte geben die Zeit an, die im Root-Knoten verbracht wurde, wenn dieser von einer bestimmten Aufrufkette aufgerufen wird.
  - **Invocations:** Die Werte in dieser Spalte geben an, wieviel mal der Root-Knoten von einer bestimmten Aufrufkette aus aufgerufen wurde.
- 

**Ansicht der aufgerufenen Routinen** Die Ansicht der aufgerufenen Routinen zeigt eine Gesamtaufruflhierarchie für einen Knoten (den sog. *Root-Knoten*) unabhängig von dessen aufrufender Kette an.

Diese Statistikdaten sind bei Problembereichen nützlich, die innerhalb der Masterhierarchie von vielen Routinen aufgerufen werden, und wo Sie sich das Gesamtprofil des betreffenden Knotens ansehen möchten.

Sie können die Ansicht der aufgerufenen Routinen von allen anderen Snapshot-Ansichten aufrufen, indem Sie mit der rechten Maustaste auf einen Knoten klicken (der dann in der Rückverfolgungsansicht zum sog. *Root-Knoten* wird) und aus dem Kontextmenü die Option „Show Calles“ auswählen.

---

**HINWEIS** In der Ansicht der aufgerufenen Routinen haben die Werte in den Spalten „Time“ und „Invocations“ die gleiche Bedeutung wie bei der Ansicht der Aufrufhierarchie.

---

## Arbeiten mit Kontextmenüoptionen

Klicken Sie in der Ansicht der Aufrufhierarchie bzw. in der Hotspot-Ansicht mit der rechten Maustaste auf einen beliebigen Knoten. Es wird ein Kontextmenü mit den in der folgenden Tabelle beschriebenen Optionen angezeigt:

Menüoption	Beschreibung
GoTo Source	Wählen Sie diese Option zur Anzeige des XML-Quellcodes für einen Knoten, der einer Java-Methode, einem Workflow, Formular, einer Regel oder einem XPRESS-Objekt entspricht. Ausführliche Informationen zu dieser Ansicht finden Sie unter „ <a href="#">Wie findet und verwaltet der Profiler Quellcode?</a> “ auf Seite 153.
Show Back Traces	Wählen Sie diese Option, um zur Rückverfolgungsansicht zu schalten. Ausführliche Informationen zu dieser Ansicht finden Sie unter „ <a href="#">Rückverfolgungsansicht</a> “ auf Seite 166.
Show Callees	Wählen Sie diese Option, um zur Ansicht der aufgerufenen Routinen zu schalten. Ausführliche Informationen zu dieser Ansicht finden Sie unter „ <a href="#">Ansicht der aufgerufenen Routinen</a> “ auf Seite 166.
Find In Hotspots	Wählen Sie diese Option, um in der Hotspot-Ansicht einen Knoten zu suchen. Ausführliche Informationen zu dieser Ansicht finden Sie unter „ <a href="#">Hotspot-Ansicht</a> “ auf Seite 165.
List Options > Sort >	Wählen Sie diese Option, um den Sortiermodus festzulegen. Sortierung nach: <ul style="list-style-type: none"> <li>• Keine</li> <li>• Aufrufhierarchie</li> <li>• Zeit</li> <li>• Aufrufen</li> <li>• aufsteigend</li> <li>• Absteigend</li> </ul>
List Options > Change Visible Columns	Wählen Sie diese Option, um die angezeigten Tabellenspalten in der Ansicht der Aufrufhierarchie bzw. Hotspot-Ansicht zu ändern.  Im Dialogfeld „Change Visible Columns“ können Sie eine oder mehrere der folgenden Optionen festlegen: <ul style="list-style-type: none"> <li>• Call Tree: Aufrufhierarchie</li> <li>• Invocations: Aufrufe</li> <li>• Time: Zeit</li> </ul>

## Suchen eines Snapshots

Mit dem Suchsymbol  am oberen Rand der Snapshot-Ansicht können Sie in der Ansicht der Aufrufhierarchie bzw. der Hotspot-Ansicht Knoten nach Namen suchen.

Alternativ dazu können Sie in der Ansicht der Aufrufhierarchie bzw. in der Hotspot-Ansicht mit der rechten Maustaste auf einen beliebigen Knoten klicken und aus dem angezeigten Kontextmenü die Option „Find in Call Tree“ bzw. „Find in Hotspots“ auswählen.

## Speichern eines Snapshots

Der Profiler bietet mehrere Möglichkeiten zum Speichern eines Snapshots. Die folgende Tabelle enthält eine Beschreibung dieser Optionen:

Symbol	Zweck	
	Symbol „Save the Snapshot in the Project“ (am oberen Rand der Snapshot-Ansicht)	Speichert den Snapshot im Verzeichnis <code>nbproject/private/idm-profiler</code> Ihres Projekts. Die im Projekt gespeicherten Snapshots werden im Bereich „Saved Snapshots“ der Profiler-Ansicht angezeigt.
	Symbol „Save the Snapshot Externally“ (am oberen Rand der Snapshot-Ansicht)	Speichert den Snapshot in einem beliebigen externen Verzeichnis.
	Schaltfläche „Save As“ (im Bereich „Saved Snapshots“)	Speichert den Snapshot in einem beliebigen externen Verzeichnis.

## Tutorium: Beheben von Leistungsproblemen

Identity Manager enthält ein Tutorium (`profiler-tutorial.zip`), mit dem Sie lernen können, wie Sie den Profiler zur Problembeseitigung bei Formularen, Java-Objekten, Regeln, Workflows und XPRESS-Objekten nutzen.

### Schritt 1: Erstellen eines Identity Manager-Projekts

Führen Sie die folgenden Schritte aus, um ein Identity Manager-Projekt zu erstellen:

1. Wählen Sie „File > New Project“.
2. Geben Sie Folgendes an, wenn der Assistent zum Erstellen neuer Projekte angezeigt wird, und klicken Sie dann auf „Weiter“:
  - a. Wählen Sie aus der Liste „Categories“ den Eintrag „Web“, um festzulegen, welchen Projekttyp Sie erstellen wollen.
  - b. Wählen Sie aus der Projektliste den Eintrag „Identity Manager Project“.

---

**HINWEIS** Wenn Sie eine Entwicklungsumgebung mit vollem Leistungsumfang erhalten möchten, müssen Sie ein reguläres Identity Manager-Projekt erstellen. Wählen Sie nicht die Option „Identity Manager Project (Remote)“ aus.

---

3. Füllen Sie im Fenster „Name and Location“ die folgenden Felder aus und klicken Sie dann auf „Weiter“.
  - **Project Name:** Geben Sie als Projektnamen **Idm80** ein.
  - **Project Location:** Übernehmen Sie das Standardverzeichnis oder geben Sie ein anderes Verzeichnis an.
  - **Project Folder:** Übernehmen Sie den Standardordner oder geben Sie einen anderen Ordner an.
4. Geben Sie den Ort der war-Datei von Identity Manager 8.0 ein, wenn das Dialogfeld „Identity Manager WAR File Location“ angezeigt wird. Beim Entpacken dieser Datei wird in der Regel eine idm.war-Datei im gleichen Verzeichnis erzeugt.
5. Klicken Sie auf „Weiter“. Das Fenster „Repository Setup“ wird angezeigt.

Sie brauchen die Standardeinstellungen in diesem Fenster nicht zu ändern. Klicken Sie auf „Fertigstellen“. Wenn im Ausgabefenster von von Identity Manager-IDE die Meldung BUILD SUCCESSFUL angezeigt wird, können Sie die Dateien des Profiler-Tutoriums extrahieren. Anweisungen dazu finden Sie unter [“Schritt 2: Entpacken des Profiler-Tutoriums”](#).

### *Schritt 2: Entpacken des Profiler-Tutoriums*

Entpacken Sie die Datei `profiler-tutorial.zip` in das Projekt-Wurzelverzeichnis. Es werden folgende Dateien extrahiert:

```
<Projekt-Wurzelverzeichnis>/custom/WEB-INF/config/ProfilerTutorial1.xml
<Projekt-Wurzelverzeichnis>/custom/WEB-INF/config/ProfilerTutorial2.xml
<Projekt-Wurzelverzeichnis>/src/org/example/ProfilerTutorialExample.java
<Projekt-Wurzelverzeichnis>/PROFILER_TUTORIAL_README.txt
```

Sie können jetzt den Profiler starten.

### *Schritt 3: Starten des Profilers*

So starten Sie den Profiler:

1. Erhöhen Sie mithilfe der Anleitung unter „[Vorbereitung](#)“ auf Seite 156 die Speicherressourcen für den Server und die Netbeans-JVM.
2. Starten Sie den Profiler mit einer der beiden unter „[Übersicht](#)“ auf Seite 152 beschriebenen Möglichkeiten.
3. Wenn das Dialogfeld „Profiler Options“ angezeigt wird, können Sie Optionen für das Profiling eingeben.
4. Gehen Sie zu [“Schritt 4: Festlegen von Optionen für das Profiling.”](#)

### *Schritt 4: Festlegen von Optionen für das Profiling*

---

**HINWEIS** Weitere Informationen zu den verschiedenen Profiler-Optionen finden Sie unter [„Festlegen von Optionen für das Profiling“](#) auf Seite 158.

---

Für dieses Tutorium sollten Sie die folgenden Profiler-Optionen eingeben:

1. Wählen Sie in der Registerkarte „Mode“ die Option „Java and IDM Objects“, um das Profiling für Formulare, Regeln, Workflows, Java- und XPRESS-Objekte durchzuführen.
2. Klicken Sie auf die Registerkarte „Java Filters“.

Gehen Sie wie folgt vor, um alle Java-Klassen von Identity Manager *aufßer* Ihre benutzerspezifischen Java-Klassen (in diesem Fall `org.example.ProfilerTutorialExample`) zu deaktivieren:

- a. Klicken Sie auf „New“. Ein neues leeres Feld erscheint am Ende der Filterspalte.
  - b. Geben Sie in das neue Feld `com.waveset.*` ein und markieren Sie dann das Kontrollkästchen „Exclude“.
  - c. Klicken Sie erneut auf „New“.
  - d. Geben Sie in das neue Feld `com.sun.idm.*` ein und markieren Sie dann das Kontrollkästchen „Exclude“.
3. Klicken Sie auf „OK“, um den Profiler auszuführen.

---

**HINWEIS** Der Profiler benötigt einige Minuten zur Abarbeitung, wenn er zum ersten Mal nach einer Clean Project-Aktion an einem Projekt ausgeführt wird.

---

Nach Abschluss des Profiling werden Sie aufgefordert, sich anzumelden.

4. Geben Sie das Passwort **configurator** ein, markieren Sie das Kontrollkästchen „Passwort speichern“ und klicken Sie anschließend auf „OK“, um fortzufahren.
5. Melden Sie sich an, wenn das Identity Manager-Fenster angezeigt wird.

---

**HINWEIS** Normalerweise sollten Sie sich in Identity Manager als ein anderer Benutzer statt nochmals als `configurator` anmelden. Sie sind im Profiler bereits als „configurator“ angemeldet, und der Sitzungspool von Identity Manager erlaubt nur einen Eintrag pro Benutzer. Mehrere Benutzereinträge können die Funktion des Sitzungspools beeinträchtigen und die feiner abgestimmte Suche nach Leistungsproblemen erschweren.

In diesem einfachen Beispiel hat dies jedoch keine Auswirkungen, sodass Sie sich als `configurator/configurator` anmelden können.

---

6. Wählen Sie in Identity Manager „Serveraufgaben > Aufgaben ausführen“, und klicken Sie dann auf „ProfilerTutorialWorkflow1“.

Es kann sein, dass es einige Augenblicke dauert, bis das Tutorium reagiert.

7. Obwohl Sie jetzt schon einen Snapshot erstellen können, sollten Sie zunächst die Profiling-Ergebnisse löschen, den Profiler starten, ihn nochmals ausführen und dann erst einen Snapshot erstellen.

---

**HINWEIS** Am Besten ist es, den Profiler vor dem Erstellen eines Snapshots einige Male auszuführen, damit Sie sicherstellen können, dass alle Cache-Speicher vorbereitet und alle JSPs kompiliert sind usw.

Durch mehrmalige Ausführung des Profilers können Sie sich auf die eigentlichen Leistungsprobleme konzentrieren. Die einzige Ausnahme von dieser Regel besteht dann, wenn beim Füllen des Cache-Speichers selbst Probleme auftreten.

---

- a. Gehen Sie zur IDM-Profileransicht in der Identity Manager-IDE zurück. Klicken Sie auf das Symbol „Reset Collected Results“  im Abschnitt „Profiling Results“ (oder „Controls“), um alle bisher erfassten Profiling-Ergebnisse zu löschen.
- b. Wählen Sie in Identity Manager erneut „Serveraufgaben > Aufgaben ausführen“, und klicken Sie dann auf „ProfilerTutorialWorkflow1“.
- c. Wenn das Prozessdiagramm angezeigt wird, sollten Sie zur Identity Manager-IDE zurückgehen und im Abschnitt „Profiling Results“ auf „Take Snapshot“ klicken.

8. Die Identity Manager-IDE lädt die Snapshots und zeigt die Ergebnisse in der rechten Fensterhälfte an.

Dieser Bereich wird als *Ansicht der Aufrufhierarchie* bezeichnet. In der obersten Ebene der Aufrufhierarchie sollte `/idm/task/taskLaunch.jsp` zusammen mit einer Zeitdauer in der Spalte „Time“ erscheinen. Die Zeit sollte zeigen, dass der gesamte Vorgang sechs oder mehr Sekunden dauerte.

9. Klappen Sie den Knoten `/idm/task/taskLaunch.jsp` auf, und jetzt sehen Sie, dass `ProfilerTutorialWorkflow1` sechs Sekunden dauerte.
10. Klappen Sie den Knoten `ProfilerTutorialWorkflow1` auf. Beachten Sie, dass `activity2` vier Sekunden und `activity1` zwei Sekunden dauerte.

11. Klappen Sie `activity2` auf.

Beachten Sie, dass `action1` zwei Sekunden und `action2` zwei Sekunden dauerte.

12. Klappen Sie `action1` auf. Sie sehen, dass der Aufruf (`<invoke>`) ebenfalls zwei Sekunden dauerte.

13. Doppelklicken Sie auf `<invoke>`, um `ProfilerTutorialWorkflow1.xml` zu öffnen, und markieren Sie die folgende Zeile:

```
<invoke name='example' class='org.example.ProfilerTutorialExample' />
```

Sie sollten sehen, dass der Aufruf der Methode `ProfilerTutorialExample` zwei Sekunden dauerte.

---

**HINWEIS** Statt des Quellcodes im Projekt schauen Sie sich durch den Snapshot erfassten XML-Code an. Snapshots sind vollkommen unabhängig (Weitere Informationen dazu finden Sie unter [„Wie findet und verwaltet der Profiler Quellcode?“](#) auf Seite 153.)

---

14. Klicken Sie auf die Registerkarte „CPU:<Datum><Zeit>“, um zum Snapshot zurückzukehren.
15. Klappen Sie den `<invoke>`-Knoten auf. Sie sehen, dass der Profiler zwei Sekunden in der Java-Methode `ProfilerTutorialExample.example()` verbraucht hat.
16. Doppelklicken Sie auf den Methodennamen, um den Quellcode (`ProfilerTutorialExample.java`) zu öffnen, und markieren Sie die folgende Zeile:

```
Thread.sleep(2000);
```

Das ist das Problem! Diese Methode enthält einen 2 Sekunden dauernden Sleep-Thread.

17. Wenn Sie zur Ansicht der Aufrufhierarchie zurückkehren, sehen Sie, dass alle 2 s-Pfade zu dieser Methode führen. Es sollten isg. drei Pfade mit einer Gesamtdauer von sechs Sekunden zu sehen sein.
18. Klicken Sie auf die Registerkarte „Hotspots“ am unteren Rand der Aufrufhierarchie, um die Hotspot-Ansicht zu öffnen. Sie sehen, dass die Methode `ProfilerTutorialExample.example()` insgesamt sechs Sekunden zur Ausführung benötigte.

Weitere Informationen zu Hotspots finden Sie unter [„Hotspot-Ansicht“ auf Seite 165](#).

19. Klicken Sie mit der rechten Maustaste auf `ProfilerTutorialExample.example()` und wählen Sie aus dem Kontextmenü die Option „Show Back Traces“.

Im unteren Bereich wird eine neue Registerkarte namens „Back Traces“ angezeigt.

20. Klappen Sie den Knoten `ProfilerTutorialExample.example()` in der Registerkarte „Back Traces“ auf. Sie sehen, dass diese Methode an drei verschiedenen Stellen aufgerufen wurde und jede Ausführung zwei Sekunden dauerte.

Weitere Informationen zu Rückverfolgungen finden Sie unter [„Rückverfolgungsansicht“ auf Seite 166](#).

21. Klicken Sie auf das Symbol „Save the snapshot in the project“  um den Snapshot zu speichern, und schließen Sie ihn.

Im Abschnitt „Saved Snapshots“ der Registerkarte „IDM Profiler“ sollte der gespeicherte Snapshot jetzt aufgeführt sein. Es kann sein, dass Sie bei längeren Listen einen Bildlauf nach unten durchführen müssen, um ihn zu sehen.

22. Markieren Sie den gespeicherten Snapshot und klicken Sie dann auf „Open“, um ihn wieder zu öffnen.

---

**HINWEIS** Mithilfe der Schaltfläche „Save As“ können Sie Snapshots extern speichern. Mithilfe der Schaltfläche „Load“ laden Sie einen Snapshot von außerhalb eines Projekts.

---

23. Schließen Sie den Snapshot wieder.

## *Verwenden des Profilers für die Workflow-Aktion „ManualAction“*

Der nächste Abschnitt dieses Tutoriums befasst sich mit dem Profiling einer „ManualAction“ eines Workflows.

1. Wählen Sie in Identity Manager „Serveraufgaben > Aufgaben ausführen“, und klicken Sie dann auf „ProfilerTutorialWorkflow2“.

Nach einigen Sekunden wird ein leeres Formular angezeigt.

2. Klicken Sie auf „Speichern“. Das Prozessdiagramm wird angezeigt.
3. Klicken Sie erneut auf „Serveraufgaben > Aufgaben ausführen“.
4. Gehen Sie zur IDM-Profilerview der Identity Manager-IDE zurück und klicken Sie im Abschnitt „Profiling Results“ auf „Reset Collected Results“.
5. Klicken Sie jetzt in Identity Manager auf ProfilerTutorialWorkflow2.
6. Klicken Sie auf „Speichern“, wenn das leere Formular erneut angezeigt wird.
7. Klicken Sie in der IDM-Profilerview auf „Take Snapshot“.

Nach einigen Sekunden wird in der Aufrufhierarchie ein Snapshot angezeigt. Sie sehen, dass `/idm/task/workItemEdit.jsp` zur Ausführung ca. sechs Sekunden benötigte. Dieses Ergebnis entspricht dem der manuellen Aktion im Workflow.

8. Klappen Sie den Knoten `/idm/task/workItemEdit.jsp` auf. Sie sehen, dass die Ausführung aller Ableitungen im Formular ManualAction sechs Sekunden dauerte.
9. Klappen Sie die Knoten `Derivation`, `displayNameForm`, `variables.dummy` und `<block>` auf.

Sie sehen, dass der `<block>`-Knoten zur Ausführung sechs Sekunden benötigte und der Profiler in jedem Aufruf der Methode `ProfilerTutorialExample.example()` zwei Sekunden verbraucht hat.

10. Sie können auf `<block>` doppelklicken, um den Quellcode zu sehen.

# Identity Manager-IDE Häufig gestellte Fragen

Hier werden einige häufig gestellte Fragen in Bezug zur Identity Manager Integrated Development Environment (Identity Manager-IDE) beantwortet. Diese Informationen sind in die folgenden Kategorien unterteilt:

- [Arbeiten mit NetBeans](#)
- [Arbeiten mit Projekten](#)
- [Arbeiten mit dem Repository](#)
- [Arbeiten mit dem Debugger der Identity Manager-IDE](#)

## Arbeiten mit NetBeans

### **F: Welche Netbeans-Version sollte ich verwenden?**

**A:** Verwenden Sie die Netbeans-Version, die in der Identity Manager-Produktdokumentation für die Version des von Ihnen verwendeten Netbeans-Plugins angegeben ist.

---

**HINWEIS** Sie sollten stets *genau* die gleiche Version verwenden, die in der Dokumentation angegeben ist, da auch Patch-Releases die Funktionalität beeinträchtigen können.

---

### **F: Das Netbeans-Plugin funktionierte, ich habe Änderungen vorgenommen, und jetzt funktioniert es nicht mehr. Was könnte die Ursache sein?**

**A:** Solche Probleme werden im Allgemeinen von beschädigten Dateien im Verzeichnis `.netbeans` verursacht. Durch Löschen des Verzeichnisses `.netbeans` und Neuinstallation des NetBeans-Plugins wird dieses Problem normalerweise beseitigt. (Durch Löschen des Verzeichnisses `.netbeans` wird das NetBeans-Plugin praktisch deinstalliert. Sie verlieren zwar alle Ihre benutzerspezifischen Einstellungen, Projekte sind jedoch sicher und werden nicht gelöscht.)

Gehen Sie dazu wie folgt vor:

1. Beenden Sie NetBeans.
2. Löschen Sie das Verzeichnis „.netbeans“.
3. Starten Sie NetBeans.
4. Installieren Sie das NetBeans-Plugin.
5. Starten Sie NetBeans neu.

## Arbeiten mit Projekten

**F: Das Erstellen und Ausführen eines Projekts dauert sehr lange, und die Identity Manager-IDE scheint viele Dateien zu kopieren. Was könnte die Ursache sein?**

A: Dieses Problem kann unter folgenden Bedingungen auftreten:

- Sie verwenden die Version 7.0 bzw. 7.1 des Identity Manager-IDE-Plugins.

Verwenden Sie das Identity Manager-IDE 8.0-Plugin.

Zur Leistungsverbesserung wurden am Configuration Build Environment (CBE) der Identity Manager-IDE 8.0 einige Änderungen vorgenommen.

- Es kann sein, dass Clean-Befehle unnötigerweise ausgeführt werden.

Bei Verwendung von `Clean Project` bzw. `Clean And Build Project` löscht die Identity Manager-IDE das gesamte `image`-Verzeichnis, das mehrere Tausend Dateien enthält. Beim nächsten Build muss die Identity Manager-IDE alle diese Dateien von `idm-staging` kopieren.

Zur effektiven Verwendung der Identity Manager-IDE muss Ihnen klar sein, wann die Clean-Befehle eingesetzt werden sollten. Weitere Informationen dazu finden Sie im Abschnitt „When to Use Clean“ in der Datei `README.txt` der Identity Manager-IDE.

**F: Welche Dateien sollten nach der Erstellung eines Identity Manager-Projekts in ein Quellcodeverwaltungssystem eingecheckt werden?**

A: Weitere Informationen dazu finden Sie im Abschnitt „CVS Best Practices“ in der Datei `README.txt` der Identity Manager-IDE.

**F: Wie verwende ich die CVS-Funktionen zur Projektverwaltung optimal?**

A: Weitere Informationen dazu finden Sie im Abschnitt „CVS Best Practices“ in der Datei `README.txt` der Identity Manager-IDE.

**F: Wann werden Objekte in das Repository importiert?**

A: Informationen dazu finden Sie unter [„Arbeiten mit dem Repository“](#) auf Seite 177.

**F: Wie füge ich zu einem Projekt eine neue JAR-Datei hinzu?**

A: Weitere Informationen dazu finden Sie im Abschnitt „How to add a new JAR dependency“ in der Datei `README.txt` der Identity Manager-IDE.

## Arbeiten mit dem Repository

### F: Welches Repository sollte ich für ein Sandbox-Repository verwenden?

**A:** Verwenden Sie für eine Sandbox ein eingebettetes Repository. Dies gilt insbesondere dann, wenn Sie Identity Manager 7.1 (oder höher) verwenden, da diese Version ein HsSQL-Repository besitzt. Wenn Sie kein eingebettetes Repository verwenden, verlieren Sie Funktionalität.

Weitere Informationen dazu finden Sie im Abschnitt „Working with the Repository“ in der Datei `README.txt` der Identity Manager-IDE.

### F: Wann werden Objekte automatisch importiert?

**A:** Die Identity Manager-IDE muss zum automatischen Import von Objekten speziell konfiguriert werden.

Gehen Sie dazu wie folgt vor:

1. Wählen Sie aus dem IDM-Menü die Option „Repository > Manage Embedded Repository“.
2. Aktivieren Sie im Dialogfeld „Manage Embedded Repository“ die Option „Automatically Publish Identity Manager Objects“.

---

**HINWEIS** Diese Option ist nicht bei Identity Manager-Fernprojekten und bei der Nutzung eines eigenen Repositories verfügbar.

---

3. Wählen Sie „Projekt > Projekt ausführen“ bzw. „Projekt > Debug Project“.

Die Identity Manager-IDE importiert automatisch alle Objekte, die seit der letzten Projektausführung geändert wurden.

---

**HINWEIS** Das automatische Herausgeben von Identity Manager-Objekten verlängert die Zeit, die zum Hochfahren des Servers benötigt wird. Zur Minimierung der Serverstartzeit sollten Sie diese Option deaktivieren und Objekte explizit (manuell) in das Repository laden.

---

## F: Wie können Objekte am effektivsten geladen werden?

A: Wählen Sie eine der folgenden Vorgehensweisen, um geänderte Objekte neu zu laden:

- Klicken Sie mit der rechten Maustaste auf die geänderten Objekte in der Projekthierarchie und wählen Sie anschließend im angezeigten Kontextmenü die Option „Objekt hochladen“.

---

**TIPP** Zum Laden mehrerer Objekte müssen Sie beim Markieren der Objekte in der Liste die STRG-Taste gedrückt halten.

---

- Markieren Sie alle geänderten Objekte und wählen Sie anschließend im IDM-Menü die Option „Repository > Objekte hochladen“. Es wird ein Dialogfeld angezeigt, sodass Sie die hochzuladenden Objekte auswählen können.

Alle diese Methoden laden die betreffenden Objekte direkt auf den Server, sodass es keine Probleme mit Antwortzeiten des Cache-Speichers gibt und diese somit sehr viel schneller als die Optionen „Projekt ausführen“ bzw. „Debug Project“ ausgeführt werden. Die Hochladefunktion für Objekte ist bei allen Repositories verfügbar.

## Arbeiten mit dem Debugger der Identity Manager-IDE

### F: Der Debugger der Identity Manager-IDE ist sehr langsam. Was könnte die Ursache sein?

A: Zur Leistungsverbesserung des Debuggers sollten Sie stets Folgendes sicherstellen:

- Der Tomcat HTTP-Monitor sollte stets deaktiviert sein. Gehen Sie dazu wie folgt vor:
  - a. Klicken Sie in der Identity Manager-IDE auf die Registerkarte „Laufzeit“.
  - b. Klappen Sie den Serverknoten auf und klicken Sie mit der rechten Maustaste auf „Bundled Tomcat“. Wählen Sie dann aus dem Kontextmenü die Option „Eigenschaften“.
  - c. Deaktivieren Sie das Kontrollkästchen „HTTP-Monitor aktivieren“ und schließen Sie das Dialogfeld.

Beim nächsten Start von Tomcat wird der HTTP-Monitor deaktiviert.

- Wenn Sie keine Fehlersuche an Java-Quellcode durchführen, sollten Sie „Projekt > Projekt ausführen“ wählen und dann auf „Attach Debugger > Identity Manager XML Object Debugger“ klicken, um nur den XPRESS-Debugger zu verwenden.

Durch Auswahl von „Projekt > Debug Project“ für Fernprojekte der Identity Manager-IDE werden der XPRESS-Debugger *und* der Java-Debugger gestartet, und der Java-Debugger verlangsamt das System erheblich.

**F: Ich sehe keine Haltepunkte im Debugger. Was könnte die Ursache sein?**

A: Das Setzen von Haltepunkten kann in den folgenden Situationen verhindert werden:

- Sie haben NBM gerade installiert, Netbeans jedoch noch nicht gestartet.
- Ihr XML-Code enthält das Wrapper-Element `<Waveset>`.

Die Identity Manager-IDE ignoriert praktisch alle Dateien, die mit dem Wrapper-Element `<Waveset>` beginnen, da die Identity Manager-IDE dieses Element als Datei mit mehreren Objekten interpretiert.

Folgende Module funktionieren nicht mit Dateien, die mehrere Objekten enthalten:

- Debugger
- Regeltester
- Formularvorschau
- Alle Editoren
- Dateiimportmodul
- Dateihochlademodul
- Diff-Objektmodul

Dateien, die mehrere Objekten enthalten, können praktisch nur importiert werden. Die einzigen Dateien, die ein Wrapper-Element `<Waveset>` enthalten, sollten die Dateien auf der obersten Ebene einer Projekthierarchie sein.

**F: Ich habe im Debugger einen Haltepunkt gesetzt, und dieser Haltepunkt kann nicht temporär deaktiviert werden. Was könnte die Ursache sein?**

A: Sie sollten zwei Dinge überprüfen:

- Der Objektname darf keinen CBE-Platzhalter (%%) enthalten. CBE-Platzhalter sind in Objektnamen nicht zugelassen.
- Überprüfen Sie, dass der von Ihnen gewünschte Code auch tatsächlich ausgeführt wird. Fügen Sie eine Verfolgung (Trace) ein und sehen Sie, ob etwas ausgegeben wird

## Arbeiten mit Regeln

### **F: Warum steht der Designmodus bei der Entwicklung von Netbeans-Regeln nicht für Regelbibliotheken zur Verfügung?**

A: Der Designmodus ist in der Explorerhierarchie der Projektansicht verfügbar. Führen Sie dazu die folgenden Schritte aus:

1. Klappen Sie den Bibliotheksknoten auf und klicken Sie mit der rechten Maustaste auf eine Regel.
2. Wählen Sie aus dem angezeigten Kontextmenü die Option „Eigenschaften“ aus und klicken Sie dann auf „Body“.

---

# Identity Manager Tuning, Troubleshooting, and Error Messages

Dieser Abschnitt enthält neue Informationen und Dokumentationskorrekturen für das Dokument *Sun Identity Manager Tuning, Troubleshooting, and Error Messages*.

- 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

- Die Fehlerbehebungs-Informationen zum Thema „Unable to Delete Errors“, die bisher im Abschnitt „Troubleshooting Identity Manager IDE“ enthalten waren, sind nicht mehr relevant und wurden entfernt. Der integrierte Netbeans-Anwendungsserver wird jetzt automatisch heruntergefahren, wenn Sie eine der folgenden Projektoperationen ausführen: (ID-16851)
  - Bereinigung eines Projekts
  - Erstellen einer Delta-Distribution
  - Erstellen einer JAR-Datei
  - Fehlersuche im Projekt
  - Verwalten eines eingebetteten Repositorys
  - Projektprofilierung
  - Ausführen eines Projekts
- Der Abschnitt „Debugging PasswordSync“ wurde aus dem Kapitel „PasswordSync“ im Dokument *Identity Manager Administration* in das Kapitel „Tracing and Troubleshooting Identity Manager“ im Dokument *Identity Manager Tuning, Troubleshooting, and Error Messages* verschoben. (ID-17340)

# 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`). 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
- Standardberichtsnamen

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

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

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

---

## Onlinehilfe

Dieser Abschnitt enthält Korrekturen an der Onlinehilfe.

- Ignorieren Sie auf der Hilfeseite „Berichte konfigurieren“ den folgenden Satz:

*Schriftarten sollten auch der JVM hinzugefügt werden, damit Diagramme korrekt angezeigt werden.*

Dieser Satz ist falsch. Der Text im PDF-Bericht wird auch dann korrekt angezeigt, wenn Sie die Schriftarten nicht der JVM hinzufügen.

