

# Novell Identity Manager

3.0

08.12.05

[www.novell.com](http://www.novell.com)

---

IDENTITY MANAGER-  
BENUTZERANWENDUNG:  
ADMINISTRATIONSHANDBUCH



Novell®

## Rechtliche Hinweise

Novell Inc. übernimmt für Inhalt oder Verwendung dieser Dokumentation keine Haftung und schließt insbesondere jegliche ausdrücklichen oder impliziten Gewährleistungsansprüche bezüglich der Marktfähigkeit oder Eignung für einen bestimmten Zweck aus. Novell Inc. behält sich weiterhin das Recht vor, dieses Dokument jederzeit und ohne vorherige Ankündigung teilweise oder vollständig zu überarbeiten.

Novell Inc., gibt ebenfalls keine Erklärungen oder Garantien in Bezug auf Novell-Software und schließt insbesondere jegliche ausdrückliche oder stillschweigende Garantie für handelsübliche Qualität oder Eignung für einen bestimmten Zweck aus. Außerdem behält sich Novell Inc. das Recht vor, Novell-Software jederzeit und ohne vorherige Ankündigung ganz oder teilweise zu ändern.

Gemäß dieser Vereinbarung zur Verfügung gestellte Produkte bzw. technische Informationen unterliegen den Ausfuhrkontrollbestimmungen der USA und den Handelsgesetzen anderer Länder. Sie erkennen alle Ausfuhrkontrollbestimmungen an und erklären sich damit einverstanden, alle für anstehende Exporte, Re-Exporte oder Importe erforderlichen Lizenzen bzw. Klassifizierungen einzuholen. Sie erklären sich ferner damit einverstanden, nicht in Länder zu exportieren oder zu re-exportieren, die sich aktuell auf der Ausschlussliste für US-Exporte befinden, für die ein Embargo verhängt wurde oder die terroristischer Aktivitäten verdächtigt werden. Maßgeblich für diese Kategorisierungen sind die US-Exportgesetze. Sie dürfen die Bestandteile des Produkts nicht zur Herstellung von Raketen bzw. von Waffen nuklearer oder chemisch-biologischer Art einsetzen. Zusätzliche Informationen über den Export von Novell-Software finden Sie unter [www.novell.com/info/exports/](http://www.novell.com/info/exports/). Novell übernimmt keine Verantwortung für Ihr etwaiges Versäumnis in Bezug auf das Einholen der erforderlichen Exportgenehmigungen.

Copyright © 1997, 1998, 1999, 2000, 2001, 2002, 2003, 2004-2005 Novell Inc. Alle Rechte vorbehalten. Ohne die ausdrückliche, schriftliche Genehmigung des Herausgebers darf kein Teil dieser Veröffentlichung reproduziert, fotokopiert, übertragen oder in einem Speichersystem verarbeitet werden.

Novell Inc. besitzt gewerbliche Schutzrechte für die Technologie, die in dem in diesem Dokument beschriebenen Produkt integriert ist. Insbesondere, jedoch nicht beschränkt darauf, können diese gewerblichen Schutzrechte eines oder mehrere der unter <http://www.novell.com/company/legal/patents/> aufgeführten US-Patente und eines oder mehrere Patente oder zum Patent angemeldete Anwendungen in den USA und in anderen Ländern beinhalten.

Das Eigentumsrecht an der Software und deren Dokumentation, Patenten, Urheberrechten und etwaigen anderen darauf anwendbaren gewerblichen Schutzrechten verbleibt zu jeder Zeit exklusiv bei Novell und deren Lizenzgebern und es darf nichts unternommen werden, was im Widerspruch zu diesem Eigentumsrecht steht. Die Software wird durch Urheberrechtsgesetze und internationale Bestimmungen geschützt. Urheberrechtshinweise oder andere Eigentumsvermerke dürfen nicht von der Software oder deren Dokumentation entfernt werden und Sie sind verpflichtet, die entsprechenden Hinweise auf allen Kopien oder Auszügen der Software oder deren Dokumentation anzubringen. Sie erwerben keine Eigentumsrechte an der Software.

Novell Inc.  
404 Wyman Street, Suite 500  
Waltham, MA 02451  
USA.  
[www.novell.com](http://www.novell.com)

*Online-Dokumentation:* Zugriff auf die Online-Dokumentation für dieses und andere Novell-Produkte sowie auf Aktualisierungen erhalten Sie unter [www.novell.com/documentation](http://www.novell.com/documentation).

## **Novell-Marken**

Novell ist eine eingetragene Marke von Novell Inc. in den USA und anderen Ländern.

SUSE ist eine eingetragene Marke von Novell Inc. in den USA und in anderen Ländern.

## Materialien von Drittanbietern

Alle Marken von Drittanbietern sind Eigentum ihrer jeweiligen Inhaber.

## Rechtliche Hinweise von Drittanbietern

*Die Apache Software License, Version 1.1*

Copyright (c) 2000 The Apache Software Foundation. Alle Rechte vorbehalten.

Die Weiterverbreitung und Verwendung in Quell- und Binärformaten, mit oder ohne Änderungen, sind zulässig, sofern die folgenden Bedingungen eingehalten werden:

1. Bei der Weiterverbreitung von Quellcode müssen der oben aufgeführte Copyright-Hinweis, diese Auflistung der Bedingungen sowie der folgende Haftungsausschluss aufgeführt werden.
2. Bei der Weiterverbreitung im Binärformat müssen der oben aufgeführte Copyright-Hinweis, diese Auflistung der Bedingungen sowie der folgende Haftungsausschluss in der Dokumentation und/oder anderen mitgelieferten Materialien aufgeführt werden.
3. Die bei jeglicher Weiterverbreitung enthaltene Endbenutzer-Dokumentation, sofern vorhanden, muss den folgenden Hinweis enthalten: „Dieses Produkt enthält Software, die von der Apache Software Foundation (<http://www.apache.org/>) entwickelt wurde.“

Alternativ kann dieser Hinweis auch in der Software selbst an einer Stelle erscheinen, an der diese Hinweise auf Produkte von Drittanbietern normalerweise erscheinen.

4. Die Namen „Apache“ und „Apache Software Foundation“ dürfen nicht ohne vorherige schriftliche Genehmigung zur Ergänzung oder zu Werbezwecken von Produkten verwendet werden, die auf dieser Software basieren. Eine schriftliche Genehmigung können Sie unter [apache@apache.org](mailto:apache@apache.org) anfordern.
5. Produkte, die auf dieser Software basieren, dürfen nur mit vorheriger schriftlicher Genehmigung von der Apache Software Foundation „Apache“ genannt werden oder „Apache“ in ihrem Produktnamen verwenden.

DIESE SOFTWARE WIRD OHNE MÄNGELGEWÄHR BEREITGESTELLT. ALLE AUSDRÜCKLICHEN ODER STILLSCHWEIGENDEN GEWÄHRLEISTUNGEN, EINSCHLISSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, WERDEN AUSGESCHLOSSEN. DIE APACHE SOFTWARE FOUNDATION ODER AN DIESEM PROJEKT BETEILIGTE SIND IN KEINEM FALL FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, STRAF- ODER FOLGESCHÄDEN (EINSCHLISSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZPRODUKTEN ODER -LEISTUNGEN, NUTZUNGS AUSFALL, DATEN- UND GEWINNVERLUST ODER GESCHÄFTSAUSFALL) HAFTBAR, DIE AUFGRUND DER VERWENDUNG DIESER SOFTWARE ENTSTEHEN KÖNNEN. DIES GILT UNABHÄNGIG DAVON, WIE DIESE SCHÄDEN ENTSTANDEN SIND UND UNABHÄNGIG VON JEGLICHEM HAFTUNGSANSPRUCH, GLEICH OB VERTRAGSGEMÄSSE HAFTUNG, GEFÄHRDUNGSHAFTUNG ODER HAFTUNG AUS UNERLAUBTER HANDLUNG (EINSCHLISSLICH, JEDOCH NICHT BESCHRÄNKT AUF FAHRLÄSSIGKEIT), SOGAR, WENN SIE AUF DIE MÖGLICHKEIT EINES SOLCHEN SCHADENS HINGEWIESEN WORDEN SIND.

*Autonomy*

Copyright © 1996-2000 Autonomy, Inc.

*Bouncy Castle*

Lizenz Copyright (c) 2000 - 2004 The Legion Of The Bouncy Castle (<http://www.bouncycastle.org>)

Hiermit wird allen Personen, die eine Kopie dieser Software und seiner zugehörigen Dokumentationsdateien (die "Software") erhalten, sowie Personen, denen die Software bereitgestellt wird, unter nachfolgenden Bedingungen die kostenfreie Genehmigung erteilt, uneingeschränkt mit der Software zu handeln, darin eingeschlossen das freie Recht auf Verwendung, Vervielfältigung, Veränderung, Zusammenführung, Veröffentlichung, Verteilung, Unterlizenzierung und/oder Verkauf von Kopien der Software:

Der oben aufgeführte urheberrechtliche Hinweis und diese Genehmigung sind in allen Kopien oder erheblichen Teilen der Software ausdrücklich zu erwähnen.

DIE SOFTWARE WIRD OHNE MÄNGELGEWÄHR BEREITGESTELLT. ALLE AUSDRÜCKLICHEN ODER

STILLSCHWEIGENDEN GEWÄHRLEISTUNGEN, EINSCHLISSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT, EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, UND DER NICHTÜBERTRETUNG VON RECHTEN WERDEN AUSGESCHLOSSEN. DIE AUTOREN ODER URHEBERRECHTSINHABER HAFTEN IN KEINEM FALL FÜR EINE FORDERUNG, SCHÄDEN ODER ANDERE HAFTUNGSANSPRÜCHE, GLEICH OB VERTRAGSGEMÄSSE HAFTUNG, HAFTUNG AUS UNERLAUBTER HANDLUNG ODER EINER ANDEREN FORM DER HAFTUNG, DIE DURCH DIE, ALS FOLGE DER ODER IM ZUSAMMENHANG MIT DER SOFTWARE ODER DEREN VERWENDUNG ODER AUF ANDERE ART DURCH DIE SOFTWARE ENTSTANDEN SIND.

#### *Castor Library*

Die Originalversion der Lizenz finden Sie unter <http://www.castor.org/license.html>

Der Code dieses Projekts wird unter einer BSD-ähnlichen Lizenz [license.txt] veröffentlicht:

Copyright 1999-2004 (C) Intalio Inc. und andere. Alle Rechte vorbehalten.

Die Weiterverbreitung und Verwendung dieser Software und der zugehörigen Dokumentation („Software“), mit oder ohne Änderungen, sind unter den folgenden Bedingungen zulässig:

1. Der weiterverbreitete Quellcode muss die oben aufgeführten Urheberrechtserklärungen und Hinweise enthalten. Zudem muss eine Kopie dieses Dokuments beigelegt sein.
2. Bei der Weiterverbreitung im Binärformat müssen der oben aufgeführte Copyright-Hinweis, diese Auflistung der Bedingungen sowie der folgende Haftungsausschluss in der Dokumentation und/oder anderen mitgelieferten Materialien aufgeführt werden.
3. Der Name „ExoLab“ darf nicht ohne vorherige schriftliche Genehmigung von Intalio Inc. zur Ergänzung oder zu Werbezwecken von Produkten verwendet werden, die auf dieser Software basieren. Eine schriftliche Genehmigung können Sie unter [info@exolab.org](mailto:info@exolab.org) anfordern.
4. Produkte, die auf dieser Software basieren, dürfen nur mit vorheriger schriftlicher Genehmigung von Intalio Inc. „Castor“ genannt werden oder „Castor“ in ihrem Produktnamen verwenden. Exolab, Castor und Intalio sind Marken von Intalio Inc.
5. Bei entsprechender Verwendung sollte auch das ExoLab- Projekt (<http://www.exolab.org/>) erwähnt werden.

DIESE SOFTWARE WIRD VON INTALIO UND DEN AN DIESEM PROJEKT BETEILIGTEN OHNE MÄNGELGEWÄHR BEREITGESTELLT. ALLE AUSDRÜCKLICHEN ODER STILLSCHWEIGENDEN GEWÄHRLEISTUNGEN, EINSCHLISSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, WERDEN AUSGESCHLOSSEN. INTALIO ODER AN DIESEM PROJEKT BETEILIGTE SIND IN KEINEM FALL FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, STRAF- ODER FOLGESCHÄDEN (EINSCHLISSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZPRODUKTEN ODER -LEISTUNGEN, NUTZUNGS-AUSFALL, DATEN- UND GEWINNVERLUST ODER GESCHÄFTSAUSFALL) HAFTBAR, DIE AUFGRUND DER VERWENDUNG DIESER SOFTWARE ENTSTEHEN KÖNNEN. DIES GILT UNABHÄNGIG DAVON, WIE DIESE SCHÄDEN ENTSTANDEN SIND UND UNABHÄNGIG VON JEDLICHEM HAFTUNGSANSPRUCH, GLEICH OB VERTRAGSGEMÄSSE HAFTUNG, GEFÄHRDUNGSHAFTUNG ODER HAFTUNG AUS UNERLAUBTER HANDLUNG (EINSCHLISSLICH, JEDOCH NICHT BESCHRÄNKT AUF FAHRLÄSSIGKEIT), SOGAR, WENN SIE AUF DIE MÖGLICHKEIT EINES SOLCHEN SCHADENS HINGEWIESEN WORDEN SIND.

Softwarelizenz von *Indiana University Extreme! Lab*

Version 1.1.1

Copyright (c) 2002 Extreme! Lab, Indiana University. Alle Rechte vorbehalten.

Die Weiterverbreitung und Verwendung in Quell- und Binärformaten, mit oder ohne Änderungen, sind zulässig, sofern die folgenden Bedingungen eingehalten werden:

1. Bei der Weiterverbreitung von Quellcode müssen der oben aufgeführte Copyright-Hinweis, diese Auflistung der Bedingungen sowie der folgende Haftungsausschluss aufgeführt werden.
2. Bei der Weiterverbreitung im Binärformat müssen der oben aufgeführte Copyright-Hinweis, diese Auflistung der Bedingungen sowie der folgende Haftungsausschluss in der Dokumentation und/oder anderen mitgelieferten Materialien aufgeführt werden.

3. Die bei jeglicher Weiterverbreitung enthaltene Endbenutzer-Dokumentation, sofern vorhanden, muss den folgenden Hinweis enthalten: „Dieses Produkt enthält Software, die von Indiana University Extreme! Lab (<http://www.extreme.indiana.edu/>) entwickelt wurde.“

Alternativ kann dieser Hinweis auch in der Software selbst an einer Stelle erscheinen, an der diese Hinweise auf Produkte von Drittanbietern normalerweise erscheinen.

4. Die Namen „Indiana University“ und „Indiana University Extreme! Lab“ dürfen nicht ohne vorherige schriftliche Genehmigung zur Ergänzung oder zu Werbezwecken von Produkten verwendet werden, die auf dieser Software basieren. Eine schriftliche Genehmigung können Sie unter <http://www.extreme.indiana.edu/> anfordern.

5. Produkte, die auf dieser Software basieren, dürfen nur mit vorheriger schriftlicher Genehmigung der Indiana University die Namen „Indiana University“ verwenden oder „Indiana University“ in ihren Produktnamen aufnehmen.

DIESE SOFTWARE WIRD OHNE MÄNGELGEWÄHR BEREITGESTELLT. ALLE AUSDRÜCKLICHEN ODER STILLSCHWEIGENDEN GEWÄHRLEISTUNGEN, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, WERDEN AUSGESCHLOSSEN. DIE AUTOREN, URHEBERRECHTSINHABER ODER AN DIESEM PROJEKT BETEILIGTE SIND IN KEINEM FALL FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, STRAF- ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZPRODUKTEN ODER -LEISTUNGEN, NUTZUNGS AUSFALL, DATEN- UND GEWINNVERLUST ODER GESCHÄFTSAUSFALL) HAFTBAR, DIE AUFGRUND DER VERWENDUNG DIESER SOFTWARE ENTSTEHEN KÖNNEN. DIES GILT UNABHÄNGIG DAVON, WIE DIESE SCHÄDEN ENTSTANDEN SIND UND UNABHÄNGIG VON JEDLICHEM HAFTUNGSANSPRUCH, GLEICH OB VERTRAGSGEMÄSSE HAFTUNG, GEFÄHRDUNGSHAFTUNG ODER HAFTUNG AUS UNERLAUBTER HANDLUNG (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF FAHRLÄSSIGKEIT), SOGAR, WENN SIE AUF DIE MÖGLICHKEIT EINES SOLCHEN SCHADENS HINGEWIESEN WORDEN SIND.

*JDOM.JAR*

Copyright (C) 2000-2002 Brett McLaughlin & Jason Hunter. Alle Rechte vorbehalten.

Die Weiterverbreitung und Verwendung in Quell- und Binärformaten, mit oder ohne Änderungen, sind zulässig, sofern die folgenden Bedingungen eingehalten werden:

1. Bei der Weiterverbreitung von Quellcode müssen der oben aufgeführte Copyright-Hinweis, diese Auflistung der Bedingungen sowie der folgende Haftungsausschluss aufgeführt werden.
2. Bei der Weiterverbreitung im Binärformat müssen der oben aufgeführte Copyright-Hinweis, diese Auflistung der Bedingungen sowie der diesen Bedingungen folgende Haftungsausschluss in der Dokumentation und/oder anderen mitgelieferten Materialien aufgeführt werden.
3. Der Name „JDOM“ darf nicht ohne vorherige schriftliche Genehmigung zu Werbezwecken in Produkten verwendet werden, die auf dieser Software basieren. Eine schriftliche Genehmigung können Sie unter [license@jdom.org](mailto:license@jdom.org) anfordern.
4. Produkte, die auf dieser Software basieren, dürfen nur mit vorheriger schriftlicher Genehmigung von JDOM-Projektmanagement ([pm@jdom.org](mailto:pm@jdom.org)) „JDOM“ genannt werden oder „JDOM“ in ihrem Produktnamen verwenden.

Darüber hinaus empfehlen wir (setzen aber nicht voraus), dass Sie in die bei Weiterverbreitungen enthaltene Endbenutzer-Dokumentation und/oder in die Software einen Hinweis ähnlich dem folgenden aufnehmen: „Dieses Produkt enthält Software, die vom JDOM-Projekt (<http://www.jdom.org/>) entwickelt wurde.“

Alternativ kann auch ein graphischer Hinweis mit einem der unter <http://www.jdom.org/images/logos> zur Verfügung gestellten Logos verwendet werden.

DIESE SOFTWARE WIRD OHNE MÄNGELGEWÄHR BEREITGESTELLT. ALLE AUSDRÜCKLICHEN ODER STILLSCHWEIGENDEN GEWÄHRLEISTUNGEN, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, WERDEN AUSGESCHLOSSEN. DIE JDOM-AUTOREN ODER AN DIESEM PROJEKT BETEILIGTE SIND IN KEINEM FALL FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, STRAF- ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZPRODUKTEN ODER -LEISTUNGEN,

NUTZUNGS AUSFALL, DATEN- UND GEWINNVERLUST ODER GESCHÄFTSAUSFALL) HAFTBAR, DIE AUF DIE VERWENDUNG DIESER SOFTWARE ZURÜCKZUFÜHREN SIND. DIES GILT UNABHÄNGIG DAVON, WIE DIESE SCHÄDEN ENTSTANDEN SIND UND UNABHÄNGIG VON JEGLICHEM HAFTUNGSANSPRUCH, GLEICH OB VERTRAGSGEMÄSSE HAFTUNG, GEFÄHRDUNGSHAFTUNG ODER HAFTUNG AUS UNERLAUBTER HANDLUNG (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF FAHRLÄSSIGKEIT), SOGAR, WENN SIE AUF DIE MÖGLICHKEIT EINES SOLCHEN SCHADENS HINGEWIESEN WORDEN SIND.

#### *Phaos*

Ein Teil dieser Software basiert auf dem SSLava™-Toolkit, Copyright ©1996-1998 Phaos Technology Corporation. Alle Rechte vorbehalten. Der Zugriff des Kunden auf die Funktionalität der Phaos-Software ist verboten.

#### *W3C*

#### W3C® SOFTWARE - HINWEIS UND LIZENZ

Diese Arbeit (sowie darin enthaltene Software und deren Dokumentation wie z. B. READMEs oder ähnliche Elemente) wird von den Urheberrechtsinhabern unter folgender Lizenz bereitgestellt. Durch den Erhalt, die Verwendung und/oder das Kopieren dieser Arbeit erklären Sie (der Lizenznehmer), dass Sie die folgenden Bedingungen gelesen, verstanden und in diese eingewilligt haben.

Die Genehmigung zum Kopieren, Ändern und Verteilen dieser Software und deren Dokumentation, mit oder ohne Änderungen, zu einem beliebigen Zweck, gebühren- und tantiemenfrei, wird hiermit gewährt, vorausgesetzt, dass Sie ALLEN Kopien der Software und Dokumentation oder Teilen davon, einschließlich Änderungen, Folgendes hinzufügen:

1. Den vollständigen Text dieses HINWEISES an für den Benutzer des neu verteilten oder abgeleiteten Produkts sichtbarer Stelle.
2. Alle bereits vorhandenen Haftungsausschlüsse in Bezug auf intellektuelles Eigentum, Hinweise oder Bedingungen. Sind keine vorhanden, muss die Kurzfassung des W3C-Softwarehinweises (W3C Software Short Notice) in den Text des verteilten oder abgeleiteten Codes eingefügt werden (vorzugsweise als Hypertext, eine Textdarstellung ist zulässig).
3. Hinweise über Änderungen an den Dateien, einschließlich Änderungsdatum. (Es wird empfohlen, URIs von dem Speicherort bereitzustellen, von der der Code abgeleitet wird.)

DIESE SOFTWARE UND DEREN DOKUMENTATION WIRD OHNE MÄNGELGEWÄHR GELIEFERT UND DIE URHEBERRECHTSINHABER ÜBERNEHMEN KEINE AUSDRÜCKLICHE ODER STILLSCHWEIGENDE GEWÄHRLEISTUNG ODER HAFTUNG, EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF DIE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT ODER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK ODER DASS DIE VERWENDUNG DER SOFTWARE ODER DEREN DOKUMENTATION NICHT PATENTE VON DRITTANBIETERN, URHEBERRECHTE, MARKEN ODER ANDERE RECHTE VERLETZT.

IN KEINEM FALL SIND DIE URHEBERRECHTSINHABER FÜR DIREKTE, INDIREKTE, BESONDERE ODER FOLGESCHÄDEN HAFTBAR, DIE AUF DIE VERWENDUNG DIESER SOFTWARE ODER DEREN DOKUMENTATION ZURÜCKZUFÜHREN SIND.

Der Name und die Marken von Urheberrechtsinhabern dürfen nur nach vorheriger schriftlicher Genehmigung in Bekanntgaben oder in Werbematerialien für die Software verwendet werden. Das Eigentum des Urheberrechts an dieser Software und der zugehörigen Dokumentation verbleibt zu jeder Zeit bei den Urheberrechtsinhabern.



# Inhalt

<b>Informationen zu diesem Handbuch</b>	<b>9</b>
<b>Teil I Überblick</b>	<b>11</b>
<b>1 Überblick</b>	<b>13</b>
1.1 Unterstützte Funktionstypen	16
1.1.1 LDAP-Administrator	16
1.1.2 Benutzeranwendungsadministrator	17
1.1.3 Endbenutzer	18
1.1.4 Delegierter Benutzer	19
1.1.5 Vertretung	20
1.2 Datenabstraktion: Der Schlüssel zum flexiblen Identitätsmanagement	20
1.3 Allgemeine Übersicht über die Architektur	21
1.3.1 Identitätsdepot	23
1.3.2 JBoss	24
1.3.3 Datenbank	24
1.3.4 Identity Manager-Engine	24
1.3.5 Benutzeranwendungstreiber	25
1.3.6 Verzeichnisabstraktionsschicht	27
1.3.7 Workflow-Engine	27
1.3.8 Benutzeroberfläche	27
1.4 Design- und Konfigurationswerkzeuge	28
1.5 Anwendungsszenarios	29
1.5.1 Szenario A: Der Benutzer sucht Informationen zu anderen Personen der Organisation	30
1.5.2 Szenario B: Der Manager erstellt einen neuen Benutzer	31
1.5.3 Szenario C: Bereitstellungsanforderungen von Benutzern	33
1.6 Weitere Vorgehensweise	35
<b>2 Konfiguration der Produktionsumgebung</b>	<b>37</b>
2.1 Topologie	37
2.1.1 Minimale Konfiguration	37
2.1.2 Hochverfügbarkeitskonfiguration	38
2.1.3 Beschränkungen bei der Konfiguration	39
2.2 Sicherheit	40
2.2.1 Beidseitige Authentifizierung	43
2.3 Leistungsoptimierung	43
2.3.1 Protokollierung	43
2.3.2 Identitätsdepot	44
2.3.3 JVM	45
2.3.4 Sitzungszeitüberschreitung	46
2.4 Cluster-Gruppierung	47
2.4.1 JBoss-Cluster-Gruppierung	47
2.4.2 Installieren der Benutzeranwendung auf einem JBoss-Cluster	50
2.4.3 Konfigurieren des Cluster-Gruppen-Cachings der Benutzeranwendung	52
2.4.4 Konfigurieren der Workflows für die Cluster-Gruppierung	53

<b>Teil II Konfigurieren der Benutzeranwendungsumgebung</b>	<b>55</b>
<b>3 Konfigurieren des Benutzeranwendungstreibers</b>	<b>57</b>
3.1 Allgemeines zum Benutzeranwendungstreiber	57
3.2 Erstellen des Benutzeranwendungstreibers	58
3.3 Starten des Benutzeranwendungstreibers	64
3.4 Einrichten von automatisch startenden Workflows	65
3.4.1 Allgemeines zu Richtlinien	65
3.4.2 Einrichten eines Workflows, der basierend auf einem Ereignis im Identitätsdepot startet	66
<b>4 Konfigurieren der Verzeichnisabstraktionsschicht</b>	<b>75</b>
4.1 Allgemeines zu Verzeichnisabstraktionsschicht-Definitionen	75
4.2 Erste Schritte	76
4.2.1 Konfiguration des Benutzeranwendungstreibers abschließen	78
4.2.2 Zugreifen auf die Bereitstellungsansicht	81
4.2.3 Starten des Verzeichnisabstraktionsschicht-Editors	82
4.3 Arbeiten mit Entitäten und Attributen	87
4.3.1 Vorgehensweise beim Hinzufügen von Entitäten	87
4.3.2 Analysieren der Datenerfordernisse	87
4.3.3 Definieren von Entitäten	88
4.4 Arbeiten mit Listen	104
4.4.1 Allgemeines zur Preferred Locale-Liste	106
4.4.2 Allgemeines zur Bereitstellungskategorieliste	107
4.5 Arbeiten mit Organigramm-Relationen	107
4.5.1 Relationseigenschaften - Referenz	109
4.6 Arbeiten mit Konfigurationseinstellungen	110
4.7 Anzeigetext lokalisieren	111
4.7.1 Unterstützte Sprachen	111
4.7.2 Lokalisieren von Text	111
4.8 Importieren, Validieren und Bereitstellen von Verzeichnisabstraktionsschicht-Definitionen	112
4.8.1 Allgemeines zum Importieren	112
4.8.2 Allgemeines zur Validierung	115
4.8.3 Allgemeines zur Bereitstellung	115
<b>5 Einrichten der Protokollierung</b>	<b>121</b>
5.1 Allgemeines zur Ereignisprotokollierung	121
5.1.1 Allgemeines zu den Einstellungen für den Protokollierumfang	121
5.2 Protokollierung an einen Novell Audit-Server	122
5.2.1 Hinzufügen des Identity Manager-Anwendungsschemas als eine Protokollanwendung zum Novell Audit-Server	122
5.2.2 Aktivieren der Audit-Protokollierung	123
5.2.3 Protokollierte Ereignisse	124
5.2.4 Protokollberichte	125
<b>Teil III Verwalten der Benutzeranwendung</b>	<b>129</b>
<b>6 Verwendung der Registerkarte „Administration“</b>	<b>131</b>
6.1 Allgemeines zur Registerkarte „Administration“	131
6.2 Berechtigte Benutzer	131
6.3 Zugriff auf die Registerkarte „Administration“	132

6.4	Zur Auswahl stehende Verwaltungsaktionen . . . . .	134
<b>7</b>	<b>Seitenadministration</b>	<b>137</b>
7.1	Allgemeines zur Seitenadministration . . . . .	137
7.1.1	Allgemeines zu Containerseiten . . . . .	137
7.1.2	Allgemeines zu freigegebenen Seiten . . . . .	143
7.1.3	Eine Ausnahme bei der Verwendung von Seiten . . . . .	145
7.2	Erstellen und Verwalten von Containerseiten . . . . .	145
7.2.1	Erstellen von Containerseiten . . . . .	145
7.2.2	Hinzufügen von Inhalt zu einer Containerseite . . . . .	148
7.2.3	Inhalt von einer Containerseite löschen . . . . .	149
7.2.4	Ändern des Layouts einer Containerseite . . . . .	150
7.2.5	Inhalt auf einer Containerseite anordnen . . . . .	151
7.2.6	Anzeigen einer Containerseite . . . . .	153
7.3	Erstellen und Verwalten von freigegebenen Seiten . . . . .	154
7.3.1	Erstellen von freigegebenen Seiten . . . . .	154
7.3.2	Inhalt zu einer freigegebenen Seite hinzufügen . . . . .	157
7.3.3	Inhalt von einer freigegebenen Seite löschen . . . . .	159
7.3.4	Ändern des Layouts einer freigegebenen Seite . . . . .	160
7.3.5	Anordnen von Inhalt auf einer freigegebenen Seite . . . . .	161
7.3.6	Anzeigen einer freigegebenen Seite . . . . .	163
7.4	Zuweisen von Seitenberechtigungen . . . . .	164
7.4.1	Zuweisen der Anzeigeberechtigung . . . . .	164
7.4.2	Zuweisen von Eigentumsrechten für freigegebene Seiten . . . . .	167
7.4.3	Zugriffsrechte auf die Seite „Benutzer oder Gruppe erstellen“ . . . . .	168
7.4.4	Zugriffsrechte auf einzelne Administrationsseiten . . . . .	169
7.5	Einrichten von Standardseiten für Gruppen . . . . .	170
7.6	Auswahl einer standardmäßigen freigegebenen Seite für eine Containerseite . . . . .	172
<b>8</b>	<b>Konfiguration von Motiven</b>	<b>175</b>
8.1	Allgemeines zur Motivkonfiguration . . . . .	175
8.2	Vorschau eines Motivs . . . . .	176
8.3	Auswahl eines Motivs . . . . .	177
8.4	Anpassen des Brandings eines Motivs . . . . .	178
<b>9</b>	<b>Portletadministration</b>	<b>181</b>
9.1	Allgemeines zur Portletadministration . . . . .	181
9.2	Verwaltung von Portlet-Anwendungen . . . . .	182
9.2.1	Zugriff auf Portlet-Anwendungen auf dem Server . . . . .	182
9.2.2	Anzeigen von Informationen zu Portlet-Anwendungen . . . . .	183
9.2.3	Aufheben der Registrierung von Portlet-Anwendungen . . . . .	184
9.3	Verwaltung von Portlet-Definitionen . . . . .	185
9.3.1	Zugriff auf Portlet-Definitionen in der bereitgestellten Portlet-Anwendung . . . . .	185
9.3.2	Registrierung von Portlet-Definitionen . . . . .	186
9.3.3	Anzeigen von Informationen zu Portlet-Definitionen . . . . .	187
9.4	Verwaltung registrierter Portlets . . . . .	189
9.4.1	Zugriff auf Portlet-Registrierungen in der installierten Portlet-Anwendung . . . . .	190
9.4.2	Anzeigen von Informationen zu Portlet-Registrierungen . . . . .	191
9.4.3	Zuweisen von Kategorien zu Portlet-Registrierungen . . . . .	191
9.4.4	Ändern von Einstellungen für Portlet-Registrierungen . . . . .	193
9.4.5	Ändern von Standardeinstellungen für Portlet-Registrierungen . . . . .	195
9.4.6	Zuweisen von Sicherheitsberechtigungen zu Portlet-Registrierungen . . . . .	196
9.4.7	Aufheben der Registrierung von Portlets . . . . .	199

<b>10 Portalkonfiguration</b>	<b>201</b>
10.1 Allgemeines zur Portalkonfiguration	201
10.2 Allgemeine Einstellungen	201
10.2.1 Änderbare Einstellungen	202
10.2.2 Schreibgeschützte Einstellungen	204
10.3 LDAP-Verbindungsparameter	204
10.3.1 Änderbare Einstellungen	206
10.3.2 Schreibgeschützte Einstellungen	206
<b>11 Sicherheitskonfiguration</b>	<b>209</b>
11.1 Allgemeines zur Sicherheitskonfiguration	209
11.2 Zuweisen eines Benutzeranwendungsadministrators	210
<b>12 Konfiguration der Protokollierung</b>	<b>213</b>
12.1 Allgemeines zur Konfiguration der Protokollierung	213
12.2 Allgemeines zu den Protokollen	213
12.3 Ändern des Protokollierumfangs	216
12.4 Senden von Protokollmeldungen an Novell Audit	217
12.5 Dauerhafte Übernahme von Protokolleinstellungen	217
<b>13 Cache-Konfiguration</b>	<b>219</b>
13.1 Allgemeines zur Cache-Konfiguration	219
13.2 Leeren von Caches	219
13.2.1 Leeren des Caches der Verzeichnisabstraktionsschicht	221
13.2.2 Leeren von Caches in einem Cluster	222
13.3 Konfiguration von Cache-Einstellungen	222
13.3.1 Wie das Caching implementiert ist	222
13.3.2 Wie Cache-Einstellungen gespeichert werden	222
13.3.3 Wie Cache-Einstellungen angezeigt werden	224
13.3.4 Grundlegende Cache-Einstellungen	224
13.3.5 Cache-Einstellungen für Cluster	226
<b>14 Werkzeuge zum Exportieren und Importieren von Portaldata</b>	<b>229</b>
14.1 Allgemeines zum Exportieren und Importieren von Portaldata	229
14.1.1 Verwendungsmöglichkeiten	229
14.1.2 Anforderungen	230
14.1.3 Einschränkungen	230
14.1.4 Schritte	230
14.2 Exportieren von Portaldata	231
14.3 Importieren von Portaldata	232
<b>Teil IV Portlet-Referenz</b>	<b>237</b>
<b>15 Allgemeines zu Portlets</b>	<b>239</b>
15.1 Zubehör-Portlets	239
15.2 Admin-Portlets	239
15.2.1 Portlet „Navigation für die freigegebene Seite“	240
15.3 Identitäts-Portlets	240
15.4 Passwort-Portlets	241

15.5	System-Portlets .....	241
<b>16</b>	<b>Das Portlet „Erstellen“</b>	<b>243</b>
16.1	Allgemeines zum Portlet „Erstellen“ .....	243
16.2	Konfiguration des Portlets „Erstellen“ .....	244
16.2.1	Einrichtung der Verzeichnisabstraktionsschicht .....	245
16.3	Erstellen von Standardeinstellungen für das Portlet „Erstellen“ .....	246
<b>17</b>	<b>Portlet „Detail“</b>	<b>249</b>
17.1	Allgemeines zum Portlet „Detail“ .....	249
17.1.1	Anzeigen von Entitätsdaten .....	249
17.1.2	Bearbeiten von Entitätsdaten .....	253
17.1.3	Versand von Entitätsdaten per Email .....	256
17.1.4	Verknüpfung mit einem Organigramm .....	256
17.1.5	Verknüpfung mit Details anderer Entitäten .....	257
17.1.6	Drucken von Entitätsdaten .....	257
17.2	Voraussetzungen .....	258
17.2.1	Konfigurieren der Verzeichnisabstraktionsschicht .....	258
17.2.2	Zuweisen von Berechtigungen für Entitäten .....	258
17.3	Starten des Detail-Portlets von anderen Portlets aus .....	258
17.3.1	Vom Portlet „Suchliste“ aus .....	259
17.3.2	Vom Portlet „Organigramm“ aus .....	259
17.4	Verwendung von Details auf einer Seite .....	260
17.5	Festlegen von Standardeinstellungen .....	261
17.5.1	Allgemeines zu Standardeinstellungen .....	261
<b>18</b>	<b>Portlet „Organigramm“</b>	<b>263</b>
18.1	Allgemeines zum Portlet „Organigramm“ .....	263
18.1.1	Allgemeines zu Relationen in Organigrammen .....	264
18.1.2	Allgemeines zur Anzeige von Organigrammen .....	265
18.2	Konfiguration des Portlets „Organigramm“ .....	265
18.2.1	Einrichtung der Verzeichnisabstraktionsschicht .....	266
18.2.2	Festlegen von Standardeinstellungen für Organigramme .....	267
18.2.3	Dynamisches Laden von Bildern .....	276
<b>19</b>	<b>Passwortverwaltungs-Portlet</b>	<b>279</b>
19.1	Vorbereitung für die Passwortverwaltung .....	279
19.1.1	Allgemeines zu den Funktionen der Passwortverwaltung .....	279
19.1.2	Erforderliches Setup in eDirectory .....	279
19.2	Allgemeines zu Passwort-Portlets .....	282
19.2.1	Portlet-Modi bei der Passwortselbstbedienung .....	283
19.3	Portlet für die IDM-Anmeldung .....	284
19.3.1	Anforderungen .....	284
19.3.2	Verwendung .....	284
19.4	Portlet „IDM-Herausforderungsantwort“ .....	285
19.4.1	Anforderungen .....	285
19.4.2	Verwendung .....	286
19.5	Portlet „IDM - Hinweisdefinition“ .....	287
19.5.1	Anforderungen .....	287
19.5.2	Verwendung .....	287
19.6	Portlet „IDM - Passwort ändern“ .....	288

19.6.1	Anforderungen . . . . .	288
19.6.2	Verwendung . . . . .	289
19.7	Portlet „IDM - Passwort vergessen“ . . . . .	290
19.7.1	Anforderungen . . . . .	290
19.7.2	Verwendung . . . . .	290
<b>20</b>	<b>Portlet „Suchliste“</b>	<b>293</b>
20.1	Allgemeines zum Portlet Suchliste . . . . .	293
20.1.1	Allgemeines zu Anzeigeformaten der Ergebnisliste . . . . .	296
20.2	Konfigurieren des Portlets „Suchliste“ . . . . .	298
20.2.1	Einrichtung der Verzeichnisabstraktionsschicht . . . . .	299
20.2.2	Festlegen von Standardeinstellungen für die Suchliste . . . . .	300
<b>Teil V</b>	<b>Entwerfen und Verwalten von Bereitstellungsanforderungen</b>	<b>307</b>
<b>21</b>	<b>Einführung in die Workflow-basierte Bereitstellung</b>	<b>309</b>
21.1	Allgemeines zur Workflow-basierten Bereitstellung . . . . .	309
21.1.1	Übersicht über die Architektur . . . . .	310
21.1.2	Bereitstellung und Workflow - Beispiel . . . . .	313
21.2	Konfiguration und Verwaltung bei der Bereitstellung . . . . .	319
21.3	Sicherheit bei der Bereitstellung . . . . .	319
<b>22</b>	<b>Konfigurieren von Bereitstellungsanforderungsdefinitionen</b>	<b>323</b>
22.1	Allgemeines zum Plugin für die Konfiguration der Bereitstellungsanforderungen . . . . .	323
22.2	Arbeiten mit den installierten Schablonen . . . . .	324
22.3	Konfigurieren einer Bereitstellungsanforderungsdefinition . . . . .	328
22.3.1	Treiberauswahl . . . . .	328
22.3.2	Erstellen oder Bearbeiten einer Bereitstellungsanforderung . . . . .	329
22.3.3	Löschen einer Bereitstellungsanforderung . . . . .	343
22.3.4	Änderung des Status einer vorhandenen Bereitstellungsanforderung . . . . .	344
22.3.5	Definieren von Rechten für eine vorhandene Bereitstellungsanforderung . . . . .	345
<b>23</b>	<b>Verwalten von Bereitstellungs-Workflows</b>	<b>347</b>
23.1	Allgemeines zum Plugin für die Workflow-Administration . . . . .	347
23.2	Verwalten von Workflows . . . . .	348
23.2.1	Verbindungsaufbau mit einem Workflow-Server . . . . .	348
23.2.2	Suchen nach Workflows, die bestimmte Suchkriterien erfüllen . . . . .	351
23.2.3	Steuern der Anzeige der aktiven Workflows . . . . .	353
23.2.4	Beenden von Workflow-Instanzen . . . . .	354
23.2.5	Anzeigen von Details zu einer Workflow-Instanz . . . . .	354
23.2.6	Neuzuordnung von Workflow-Instanzen . . . . .	355
23.3	Konfigurieren des Email-Servers . . . . .	356
23.4	Arbeiten mit den installierten Email-Schablonen . . . . .	357
23.4.1	Standardinhalt und -format . . . . .	358
23.4.2	Bearbeiten der Schablone . . . . .	358
23.4.3	Ändern von Standardwerten der Schablone . . . . .	360

<b>Teil VI Anhänge</b>	<b>363</b>
<b>A Schemaerweiterungen</b>	<b>365</b>
A.1 Attribut-Schemaerweiterungen .....	365
A.2 Objectclass-Schemaerweiterungen .....	367
A.3 LDIF-Darstellung .....	369
<b>B Konfigurieren des Anwendungsarchivs</b>	<b>391</b>
B.1 Allgemeines zur WAR-Datei der Benutzeranwendung .....	391
B.2 Einstellung der Sitzungszeitüberschreitung .....	391



# Informationen zu diesem Handbuch

## Zweck

In diesem Handbuch wird beschrieben, wie Sie die *Benutzeranwendung* Novell Identity Manager verwalten können. Dazu gehören:

- Die im Lieferumfang von Identity Manager enthaltenen Funktionen zur *Identitätsselbstbedienung* (identity self-service)
- Die Funktionen zur *Workflow-basierten Bereitstellung*, wenn Sie das Bereitstellungsmodul mit Identity Manager verwenden

Zum Erlernen der Verwaltung der anderen Funktionen von Identity Manager (in allen Paketen identisch) lesen Sie im *Novell Identity Manager: Administrationshandbuch*.

## Zielgruppe

Dieses Handbuch ist für *Systemadministratoren, -architekten und -berater* gedacht, die für die *Konfiguration, die Implementierung und die Verwaltung* der Funktionen zur Identitätsselbstbedienung und/oder der Workflow-basierten Funktionen zur Bereitstellung der Identity Manager-Benutzeranwendung verantwortlich sind.

Die Endbenutzer-Dokumentation zu diesen Funktionen finden Sie im Handbuch *Identity Manager-Benutzeranwendung: Benutzerhandbuch*.

## Voraussetzungen

In diesem Handbuch wird Folgendes vorausgesetzt:

- Identity Manager und möglicherweise auch das Bereitstellungsmodul für Identity Manager *ist bei Ihnen installiert*

Anweisungen zur Installation dieser Produkte finden Sie im *Novell Identity Manager: Installationshandbuch*.

- Sie haben die anderen Funktionen von Identity Manager Ihren Erfordernissen gemäß *konfiguriert*

Weitere Informationen hierzu finden Sie im *Novell Identity Manager: Administrationshandbuch*.

## Aufbau

Hier eine Zusammenfassung des Inhalts dieses Buchs:

Teil	Beschreibung
Teil I, „Überblick“, auf Seite 11	Bietet eine Einführung in die Identity Manager-Benutzeranwendung und unterstützt Sie bei der Einsatzplanung in Ihrem Unternehmen
Teil II, „Konfigurieren der Benutzeranwendungsumgebung“, auf Seite 55	Anleitung zur Konfiguration verschiedener Module der Umgebung der Identity Manager-Benutzeranwendung (einschließlich Benutzeranwendungstreiber, Verzeichnisabstraktionsschicht und Protokollierung), um diese den Erfordernissen Ihres Unternehmens anzupassen
Teil III, „Verwalten der Benutzeranwendung“, auf Seite 129	Anleitung zur Konfiguration und Verwaltung der Identity Manager-Benutzeranwendung unter Verwendung der Registerkarte „Administration“ (Verwaltung) in der Benutzeroberfläche
Teil IV, „Portlet-Referenz“, auf Seite 237	Anleitung zur Konfiguration der in der Benutzeroberfläche von Identity Manager verwendeten Identitäts- und System-Portlets
Teil V, „Entwerfen und Verwalten von Bereitstellungsanforderungen“, auf Seite 307	Anleitung zur Konfiguration, Implementierung und Verwaltung der Ressourcen, Workflows und Anforderungsdefinitionen für die Bereitstellung mit dem Bereitstellungsmodul für Identity Manager
	<b>Hinweis:</b> Dieser Teil ist nur dann von Interesse, wenn das Bereitstellungsmodul für Identity Manager installiert ist.
Teil VI, „Anhänge“, auf Seite 363	Zusätzliche Referenzangaben (Schemaerweiterungen) und fortgeschrittene Themen (Konfiguration des Anwendungsarchivs) für die Identity Manager-Benutzeranwendung

## Siehe auch

Weitere Informationen finden Sie in Handbüchern und Readme-Dateien auf der [Identity Manager-Seite](http://www.novell.com/idm/) (<http://www.novell.com/idm/>) der Website zur Novell-Dokumentation.

# Überblick

Diese Kapitel bieten eine Einführung in die Identity Manager-Benutzeranwendung und unterstützen Sie bei der Einsatzplanung in ihrem Unternehmen

- [Kapitel 1, „Überblick“, auf Seite 13](#)
- [Kapitel 2, „Konfiguration der Produktionsumgebung“, auf Seite 37](#)



# Überblick

# 1

Die Novell Identity Manager-Benutzeranwendung ist eine leistungsstarke Webanwendung, die dem Benutzer ein umfangreiches, intuitives, flexibel konfigurier- und verwaltbares System auf der Grundlage eines hoch entwickelten Identitätsservices-Framework zur Verfügung stellt. Wenn die Identity Manager-Benutzeranwendung zusammen mit dem Bereitstellungsmodul für Identity Manager und Novell Audit verwendet wird, liefert sie eine umfassende Komplettlösung für die Bereitstellung, die sicher, skalierbar und einfach zu verwalten ist.

Die Benutzeranwendung bietet den Endbenutzern folgende webbasierte Funktionen:

- White Pages
- Organigramme
- Benutzersuche (mit der Möglichkeit, benutzerdefinierte Sucheinstellungen zu speichern)
- Selbstbedienungsfunktion zur Passwortverwaltung
- Werkzeuge mit einer begrenzten Anzahl an Funktionen für die Benutzerverwaltung
- Initiierung und Überwachung von Workflows (bei installiertem Bereitstellungsmodul)
- Verwaltung von persönlichen Aufgaben und/oder Teamaufgaben (bei installiertem Bereitstellungsmodul)
- Funktionen zur Delegation und Vertretung

Die Benutzeranwendung bietet dem Systemadministrator eine große Auswahl an Konfigurations- und Administrationsmöglichkeiten. Dazu gehören:

- Die Einrichtung und Verwaltung von Vertretungs- und Delegiertenrechten über die Benutzeroberfläche
- Zugriff auf Werkzeuge zur Protokollierung und benutzerdefinierte Crystal Reports-Berichte
- Assistentenbasierte Konfiguration von Workflows (bei installiertem Bereitstellungsmodul)
- Workflow-Verwaltung (bei installiertem Bereitstellungsmodul), einschließlich der Möglichkeit zur neuen Zuordnung oder Beendigung von Workflows, die gerade durchgeführt werden
- Eclipse-basierter Designer zum Erstellen von benutzerdefinierten Verzeichnisabstraktionsdefinitionen und -relationen

Eine umfassendere Auflistung der Funktionen finden Sie in der folgenden Tabelle.

<b>Funktion</b>	<b>Beschreibung</b>
Standardbasierte, browseragnostische, erweiterbare Web-Benutzeroberfläche	Der Administrator kann Seitenlayouts und die standardmäßig angezeigte Startseite ändern, neue Seiten hinzufügen und die Gesamtdarstellung ändern (Motive).  Die Benutzeranwendung ist durch die Ergänzung von JSR-168-konformen Portlets erweiterbar.

<b>Funktion</b>	<b>Beschreibung</b>
Bereitstellungs-Workflows (bei installiertem Bereitstellungsmodul)	<p>Der Administrator kann speziell auf die Verarbeitung von Bereitstellungsanforderungen zugeschnittene Workflows einrichten.</p> <p>Diese Workflows können dann von Endbenutzern mit den entsprechenden Rechten initiiert werden.</p>
Ereignisgesteuerte Workflows (bei installiertem Bereitstellungsmodul)	Zusätzlich zu den benutzerinitiierten Workflows kann der Administrator Workflows so konfigurieren, dass diese beim Auftreten von bestimmten Ereignissen im Identitätsdepot automatisch ausgelöst werden.
Verbesserte White Pages	Anzeige von Benutzerinformationen u. a. alphabetisch, geografisch oder nach Kompetenz.
Organigramm	Die Benutzeranwendung umfasst ein erweitertes Portlet für Organigramme, das AJAX nutzt und so vielfältige interaktive Möglichkeiten bietet.
Benutzersuche	Der Benutzer kann nach Identitäten suchen und benutzerdefinierte Suchdefinitionen für eine spätere Wiederverwendung speichern.
Passwort-Selbstbedienung	Die Benutzeranwendung ermöglicht Endbenutzern den Zugriff auf Funktionen zur Passwortverwaltung, sodass Helpdesk-Anrufe nicht mehr erforderlich sind.
Benutzerverwaltung mit begrenzten Funktionen	Die Benutzeranwendung ermöglicht Endbenutzern (die keine IT-Administratoren sind) die Ausführung einer begrenzten Anzahl an Routineaufgaben für das Identitätsmanagement.
Eclipse-basierter Designer	Systemadministratoren, Entwickler und andere IT-Spezialisten können mit der Designer-Anwendung schnell und einfach eine Vielzahl von Konfigurationen vornehmen und andere Aufgaben erledigen. Mit Designer ist es möglich, offline mit Entitätsdefinitionen und Relationen, Treiberrichtlinien und Filtern sowie mit einer Vielzahl von Konfigurationsaufgaben für Treiber und Treibersätze zu arbeiten. Änderungen können in einem Projekt gespeichert und/oder im Identitätsdepot abgelegt werden.
Vertretungsfunktionen (bei installiertem Bereitstellungsmodul)	Die Oberfläche der Benutzeranwendung ermöglicht entsprechend qualifizierten Personen die Definition von Vertretungsfunktionen für bestimmte Benutzer. (Eine Vertretung kann im Namen eines anderen Benutzers Aufgaben ausführen und erhält alle Rechte des anderen Benutzers.)
Aufgabendelegierung (bei installiertem Bereitstellungsmodul)	Die Benutzeroberfläche ermöglicht Managern (und Benutzern mit den entsprechenden Rechten), bei Nichtverfügbarkeit eines Benutzers eine automatische Delegation von Aufgaben an Kollegen einzurichten. Bei der Delegation können bestimmte Aufgabentypen an verschiedene Personen delegiert werden.

Funktion	Beschreibung
Verzeichnisabstraktionsschicht	Das Runtime-Framework isoliert die Webanwendungslogik von den Low-Level-Mechanismen des Identitätsdepot-Zugriffs und -Workflows zur Erzeugung einer sicheren, robusten Verzeichnisabstraktionsarchitektur. Die Isolierung wird durch eine Vermittlungsschicht erzielt, die als Verzeichnisabstraktionsschicht (oder nur als Abstraktionsschicht) bezeichnet wird.
Zugriffssteuerung bei allen benutzerseitigen Daten	Die Abstraktionsschicht (die das hoch entwickelte Modell für effektive Rechte von eDirectory nutzt) beschränkt automatisch die Sichtbarkeit von Identitätsdaten und Workflows sowie das Recht des Benutzers zur Änderung von Daten auf eine für den Benutzer und sogar für die Portlets transparente Weise.
Überprüfung der Identitätsdaten von Endbenutzern	Die Benutzer haben die Möglichkeit, in der Benutzeranwendung ihre persönlichen Identitätsinformationen so anzuzeigen, wie sie im Identitätsdepot dargestellt sind, und können diese bestätigen/aktualisieren.
Flexible Protokollierung	Einfache Protokollierung von vielfältigen Ereignissen in ein Serverprotokoll (über log4j), Novell Audit oder beides.
Berichte von Novell Audit	Das Produkt umfasst vorgegebene Crystal Reports-Berichte für Berichterstellungsaufgaben bei der Bereitstellung.
Hochverfügbarkeit	Die Elemente des Benutzeranwendungs- und Genehmigungsablaufs des Produkts können zur Skalierbarkeit als Cluster gruppiert werden.
<p><b>Wichtig:</b> Bei dieser Version des Bereitstellungsmoduls wird die automatische Ausfallsicherung von in Bearbeitung befindlichen Workflow-Instanzen nicht unterstützt. Wenn ein Ablauf unterbrochen wurde, kann er jedoch nach einem manuellen Bedieneingriff auf Basis der verbleibenden Serverknoten fertig gestellt werden.</p>	
Benutzeroberfläche für die Verwaltung von Email-Schablonen	Mit iManager können Email-Schablonen zu Workflows zugeordnet und für diese angepasst werden.
Zubehör-Portlets	Im Lieferumfang der Benutzeranwendung sind mehrere funktionsbereite Portlets enthalten, einschließlich Portlets für GroupWise, Exchange, Lotus Notes, Web-mail, Netzwerk-Datei, NetStorage, HTML, Shortcut, RSS und Nachrichten-Portlets.

Diese Funktionen sind Zusatzfunktionen zu den Standardfunktionen, die von Identity Manager angeboten werden. Weitere Informationen zur Standardeinstellung der Funktionen des Produkts finden Sie im *Identity Manager-Administratorhandbuch*.

# 1.1 Unterstützte Funktionstypen

Die Identity Manager-Benutzeranwendung umfasst eine breite Palette an Funktionen für das Identitätsmanagement. Nicht jeder Benutzer verwendet alle Merkmale (oder kann diese sehen). Die Möglichkeit hierzu ist abhängig von der Funktion einer Person.

Die Benutzer werden in eine oder mehrere der folgenden Kategorien eingeteilt, für die jeweils unterschiedliche Werkzeuge und Funktionen zur Verfügung stehen. (Die folgende Terminologie wird in dieser Dokumentation verwendet.)

## 1.1.1 LDAP-Administrator

Der LDAP-Administrator ist in Bezug auf das Identitätsdepot (eDirectory 8.7.x oder 8.8) die Person mit den meisten Konfigurations- und Systemadministrationsrechten. Diese logische Funktion kann auch gemeinsam mit dem Benutzeranwendungsadministrator (unten) genutzt werden. Der Benutzeranwendungsadministrator ist die Person oder Entität mit Systemrechten für den Anwendungsserver (JBoss), die Datenbank (z. B. MySQL) und/oder die portalbasierte Web-Benutzeroberfläche.

Dem LDAP-Administrator stehen zur Erfüllung seiner Aufgaben zwei Arten von Werkzeugen zur Verfügung: der Eclipse-basierte Designer für seltene (möglicherweise einmalige) Aufgaben in Identity Manager und iManager-Werkzeuge für die täglichen Administrationsaufgaben.

Zu den seltenen Aufgaben, die in der Regel im Designer für Identity Manager erledigt werden, gehören:

- Definitionen, Attribute und Relationen für Abstraktionsschichten konfigurieren, die in der Identity Manager-Benutzeranwendung verwendet werden können. (Weitere Informationen hierzu finden Sie in [Kapitel 4, „Konfigurieren der Verzeichnisabstraktionsschicht“](#), auf [Seite 75](#).)
- Definitionen für die Verzeichnisabstraktionsschicht validieren (siehe [Kapitel 4, „Konfigurieren der Verzeichnisabstraktionsschicht“](#), auf [Seite 75](#)).
- Änderungen an den Einstellungen des Benutzeranwendungstreibers vornehmen (siehe [Kapitel 3, „Konfigurieren des Benutzeranwendungstreibers“](#), auf [Seite 57](#)).
- Angezeigten Text für Entitäts- und Attributbezeichnungen, Relationsnamen von Organigrammen sowie globale und lokale Listeneinträge lokalisieren (siehe [Kapitel 4, „Konfigurieren der Verzeichnisabstraktionsschicht“](#), auf [Seite 75](#)).
- Benutzeranwendungstreiber und dessen Einstellungen importieren oder exportieren.
- Andere Arten von Offline-Aufgaben.

Alltägliche Aufgaben, die der Administrator (der LDAP-Administrator oder der Benutzeranwendungsadministrator, siehe unten) in der Regel auf einem Live-System erledigt, werden in iManager durchgeführt. Zu solchen Aufgaben gehören:

- Email-Schablonen verwalten.
- Definitionen für bereitstellbare Ressourcen und Bereitstellungsanforderungen definieren oder bestimmen.
- Workflow-Definitionen aktivieren oder deaktivieren.
- Einen aktiven Workflow beenden.
- Berichte basierend auf Protokolldaten von Novell Audit ausführen.

Einige dieser Aufgaben (Workflow-bezogene Aufgaben) sind nur bei installiertem Bereitstellungsmodul möglich. Viele Aufgaben können anstelle des LDAP-Administrators auch vom Benutzeranwendungsadministrator (unten) durchgeführt werden.

## 1.1.2 Benutzeranwendungsadministrator

Der Benutzeranwendungsadministrator ist für Aufgaben im Zusammenhang mit der Verwaltung der Webanwendung (die browserbasierte Anwendung, die auf JBoss läuft) zuständig. Er kann über die Registerkarte „Administration“ auf der Benutzeroberfläche von Identity Manager auf diese Verwaltungswerkzeuge zugreifen.

Zu den Aktionen, die Sie in der Benutzeranwendung ausführen können, gehören:

- Verschiedene Einstellungen der Anwendung konfigurieren, z. B. um festzulegen, wie die Benutzeranwendung eine Verbindung zum Identitätsdepot (LDAP-Anbieter) aufbauen soll. Weitere Informationen finden Sie in [Kapitel 10, „Portalkonfiguration“](#), auf Seite 201.
- Festlegen, welche Seiten auf der Benutzeroberfläche von Identity Manager angezeigt werden und wer eine Zugriffsberechtigung erhalten soll. Weitere Informationen finden Sie in [Kapitel 7, „Seitenadministration“](#), auf Seite 137.
- Festlegen, welche Portlets auf der Benutzeroberfläche von Identity Manager angezeigt werden und wer eine Zugriffsberechtigung erhalten soll. Weitere Informationen finden Sie in [Kapitel 9, „Portletadministration“](#), auf Seite 181.
- Darstellung der Identity Manager-Benutzeroberfläche festlegen. Weitere Informationen finden Sie in [Kapitel 8, „Konfiguration von Motiven“](#), auf Seite 175.
- Umfang der Protokollierungsmeldungen steuern, die von der Identity Manager-Benutzeranwendung erzeugt werden, und festlegen, welche von ihnen (sofern gewünscht) an Novell Audit gesendet werden sollen. Weitere Informationen finden Sie in [Kapitel 12, „Konfiguration der Protokollierung“](#), auf Seite 213.
- Die verschiedenen Cache-Speicher verwalten, die von der Identity Manager-Benutzeranwendung geführt werden. Weitere Informationen finden Sie in [Kapitel 13, „Cache-Konfiguration“](#), auf Seite 219.
- In der Identity Manager-Benutzeranwendung verwendete Webinhalte (Seiten und Portlets) exportieren oder importieren. Weitere Informationen finden Sie in [Kapitel 14, „Werkzeuge zum Exportieren und Importieren von Portaldateien“](#), auf Seite 229.
- Vertretungsrechte für einzelne Personen einrichten.
- Viele andere Aufgaben im Zusammenhang mit der Benutzeroberfläche, die dem Endbenutzer angezeigt wird.

Zu den Aufgaben, die in iManager ausgeführt werden können, gehören:

- Email-Schablonen verwalten.
- Definitionen für bereitstellbare Ressourcen und Bereitstellungsanforderungen definieren oder bestimmen.
- Workflow-Definitionen aktivieren oder deaktivieren.
- Einen aktiven Workflow beenden.
- Berichte basierend auf Protokolldaten von Novell Audit ausführen.

Einige dieser Aufgaben (Workflow-bezogene Aufgaben) sind nur bei installiertem Bereitstellungsmodul möglich.

### 1.1.3 Endbenutzer

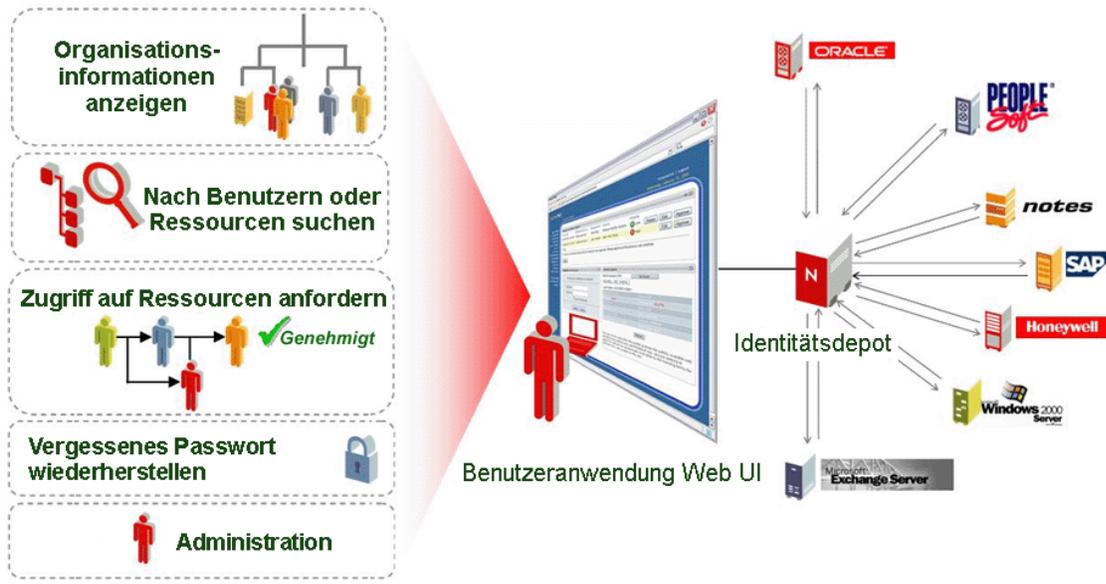
Der Endbenutzer ist die Person, die die verschiedenen Portlets und Webseiten, aus denen die Oberfläche der Benutzeranwendung besteht, anzeigt und mit ihnen interagiert. In diesem Kontext bezeichnet „Endbenutzer“ einen Mitarbeiter, einen Manager bzw. die Vertretung oder den Delegierten eines Mitarbeiters oder Managers.

Der Administrator kann für den Endbenutzer eine große Anzahl an Funktionen aktivieren. In der Mindesteinstellung können Endbenutzer die Identity Manager-Benutzeranwendung für Folgendes verwenden:

- Hierarchische Relationen zwischen Benutzerobjekten über das Organigramm-Portlet anzeigen.
- Benutzerinformationen anzeigen und bearbeiten (mit den entsprechenden Rechten).
- Mithilfe erweiterter Suchkriterien (die zur späteren Wiederverwendung gespeichert werden können) nach Benutzern oder Ressourcen suchen.
- Vergessene Passwörter wiederherstellen.
- Emails an Teammitglieder senden (an einzelne oder mehrere Empfänger).

Bei installiertem Bereitstellungsmodul stehen den Benutzern über die Web-Oberfläche der Benutzeranwendung zusätzlich folgende Möglichkeiten zur Verfügung:

- Eine Ressource anfordern (einen von mehreren möglichen vordefinierten Workflows starten).
- Den Status früherer Anforderungen einsehen.
- Aufgaben beanspruchen und Aufgabenlisten anzeigen (nach Ressource, Empfänger oder anderen Merkmalen).
- Vertretungszuweisungen anzeigen.
- Delegiertenzuweisungen anzeigen.
- Eigenen Status (verfügbar oder nicht verfügbar) angeben.
- Vertretungsmodus starten, um Aufgaben im Namen einer anderen Person zu beanspruchen.
- Teamaufgaben anzeigen, Teamressourcen anfordern (nur Manager) usw.



## 1.1.4 Delegierter Benutzer

Ein delegierter Benutzer bzw. Delegierter ist ein Endbenutzer, an den eine oder mehrere spezifische Aufgaben (entsprechend den Rechten des Benutzers) delegiert werden können, sodass die Delegierten diese Aufgaben im Namen anderer bearbeiten können. Beispiel: John hat Urlaub und möchte, dass Mary sich in seiner Abwesenheit um seine Aufgaben kümmert. Wenn Mary über die entsprechenden Rechte für die von John delegierten Aufgaben verfügt, kann sie die Delegierte von John werden. Wenn John seinen Status in der Benutzeranwendung auf „Nicht verfügbar“ setzt, werden alle Aufgaben, die normalerweise in Johns Aufgabenliste angezeigt werden, in Marys Aufgabenliste angezeigt. Mary agiert also in der Funktion einer delegierten Benutzerin. Sie hat die Möglichkeit, eine Aufgabe von John vollständig für sich zu beanspruchen (d. h., es ist nicht mehr Johns Aufgabe). Lesen Sie in diesem Zusammenhang die Definition eines vertretenden Benutzers (siehe unten).

Beachten Sie, dass eine Delegation aufgabenweise vorgenommen wird. Es ist nicht notwendigerweise ein Verantwortungstransfer nach dem Grundsatz „Alles oder Nichts“ (wenn es auch bei Bedarf möglich ist, über die Benutzeroberfläche alle Aufgaben eines Benutzers global an einen bestimmten Delegierten zu delegieren). Möglicherweise möchte ein Benutzer nicht nur einen einzigen Delegierten bestimmen. Jeder Delegierte kann die Verantwortung nur für die Aufgaben übernehmen, die ihm zugeteilt wurden. (John möchte z. B., dass Mary die eingehenden Anfragen nach Visitenkarten erledigt, während Bill neue Anfragen zum Siebel-Etat bearbeiten soll.) Die Übertragung der Verantwortung - die Neuzuweisung neuer Aufgaben - geschieht automatisch, wenn der ursprüngliche Eigentümer der Aufgabe sich für eine bestimmte Aufgabenart als nicht verfügbar angibt. (Optional kann auch pro Aufgabe eine Zeit angegeben werden, nach der die Delegation abläuft.) Dieser Vorgang wird aus Konformitätsgründen protokolliert.

Eine ausführliche Beschreibung der Funktionen der Benutzeroberfläche für delegierte Benutzer finden Sie in Kapitel 1 des Handbuchs *Identity Manager-Benutzeranwendung: Benutzerhandbuch*. Siehe auch [Abschnitt 21.3, „Sicherheit bei der Bereitstellung“](#), auf Seite 319 in diesem Handbuch.

## 1.1.5 Vertretung

Eine Vertretung ist ein Endbenutzer, der in der Funktion eines anderen Benutzers agiert, indem er zeitweise dessen Identität annimmt. Alle Rechte des ursprünglichen Benutzers gelten auch für die Vertretung. Die Arbeit des ursprünglichen Benutzers geht in das Eigentum des vertretenden Benutzers über. Beispiel: Während John in China ist, möchte er, dass sein Assistent Clive Zugriff auf seine (Johns) Aufgaben hat und diese bearbeiten kann. Wenn John über die entsprechenden Rechte verfügt, kann er Clive zu seiner Vertretung bestimmen. (Wenn er nicht über die entsprechenden Rechte verfügt, kann der Benutzeranwendungsadministrator diese für ihn einrichten.) Sobald die Vertretungsrelation eingerichtet ist, kann Clive in zwei Funktionen agieren: in der Funktion von Clive oder in der Funktion von John. In seiner Funktion als John kann er die gleichen Schritte unternehmen wie John. Wenn Clive Arbeitsschritte erledigt, scheint es, als ob John sie selbst erledigt hätte.

Beachten Sie, dass der vertretende Benutzer im Gegensatz zum zuvor beschriebenen delegierten Benutzer vollständigen Einblick in die Aufgaben und Einstellungen des ursprünglichen Benutzers erhält und diese ändern kann. Alle Attribute, Relationen oder Systemeinstellungen, auf die John zugreifen kann, können für die Dauer der Vertretung von Clive abgerufen werden.

Ein weiterer Unterschied zwischen einem Delegierten und einer Vertretung besteht darin, dass es bei einer Delegation möglich ist, die Aufgaben auf mehrere Delegierte zu verteilen, während einem vertretenden Benutzer immer alle Aufgaben des ursprünglichen Benutzers zugeteilt werden. Anders ausgedrückt, wenn Sie jemanden als Vertretung benennen, können Sie sicher sein, dass nur diese Person alle Ihre Aufgaben einsehen und bearbeiten kann. Das System macht keinen Unterschied zwischen dem ursprünglichen Benutzer und seiner Vertretung.

Beachten Sie, dass Handlungen, die von einer Vertretung im Namen eines anderen Benutzers durchgeführt werden, in Novell Audit (aus Konformitätsgründen) als solche protokolliert werden.

Weitere Informationen zu Vertretungsszenarios finden Sie im Kapitel über die **Konfiguration der Bereitstellungseinstellungen** im *Identity Manager-Benutzeranwendung: Benutzerhandbuch*.

## 1.2 Datenabstraktion: Der Schlüssel zum flexiblen Identitätsmanagement

Das Konzept der Datenabstraktion bzw. die Möglichkeit zur Definition, Anzeige und Verarbeitung der Definitionsinstanzen für Verzeichnisabstraktionsschichten ist entscheidend für das Verständnis der Identity Manager-Benutzeranwendung.

Herkömmliche Speichertechnologien, die auf relationalen Datenbanken, X.500-Verzeichnissen oder anderen Repositories beruhen, verwenden in der Regel Dateneinträge (z. B. Zeilen in einer Datenbank oder Objekte in einem X.500-Verzeichnis), die einem genau definierten Schema entsprechen. Abfragen über die gespeicherten Daten können (theoretisch) beliebig komplex sein und die Daten können Indizes und/oder Backlinks enthalten, die Dateneinträge selbst müssen allerdings einer vorgegebenen Definition entsprechen. Es wird weiterhin angenommen, dass sich die geltenden Schemata im Laufe der Zeit nicht wesentlich ändern (wenn überhaupt).

Dies ist problematisch, wenn Informationen (möglicherweise aus ungleichen zusammengesetzten Datenquellen mit ungleichen Schemata) zusammengeführt werden müssen, um Datenobjekte zu erstellen, die einem beliebigen neuen (und möglicherweise transienten) Schema entsprechen. Identitätsdaten sind hierfür ein klassisches Beispiel, da Identitäten meist aus zusammengesetzten, nicht statischen Daten bestehen. Außerdem können die Daten einer Identität aus unterschiedlichen

Quellen stammen, die möglicherweise von Administratoren verwaltet werden, die die Angaben (verständlicherweise) schützen.

Die verteilte Beschaffenheit von Identitätsdaten stellt das Identitätsmanagement vor Herausforderungen, die angesichts der starren Schemadefinitionen in manchen Situationen nur schwer lösbar sind. Ein möglicher Lösungsansatz besteht darin, die Identitätsdaten in einem logischen Depot (implementiert als Verzeichnis) zusammenzuführen und bei Bedarf logische Identitäten gemäß eines oder mehrerer logischer Schemas aus den Quelldaten zusammenzustellen. Anhand dieser Schemas können herkömmliche LDAP-Objekte und -Attribute beliebigen Definitionen für Abstraktionsschichten und Attributen zugeordnet werden. Auf diese Weise werden Identitätsdaten höchst flexibel und dynamisch. Zur Änderung der Definition einer Identität ist es nicht notwendig, Änderungen an einem LDAP-Schema vorzunehmen. Identitätsobjekte können nach Belieben neu definiert und an spezielle Anwendungen oder sogar an spezielle Benutzer von speziellen Anwendungen angepasst werden.

Dieser Gesamtansatz wird häufig als „Datenabstraktion“ bezeichnet. Dies bedeutet, dass die Identitäten je nach Bedarf und in der gewünschten Form realisiert werden können.

Die Abstraktion von Identitätsdaten hat viele Vorteile:

- Es ist möglich, potentiell riskante Änderungen an den LDAP-Verzeichnisschemas zu vermeiden.
- Abstraktionstechnologie ist unauffällig, verbundene Systeme müssen nicht geändert werden.
- Es sind neue Relationen zwischen den Daten möglich.
- Die Definitionen für die Abstraktionsschichten können jederzeit geändert oder erweitert werden.
- Objekte können so viele oder wenige Attribute haben wie benötigt.
- Attribute von unverbundenen LDAP-Objektclassen können in der Definition einer Abstraktionsschicht zusammengeführt werden.
- Für die Benennung der Attribute können beliebige Namen verwendet werden (es ist nicht erforderlich, LDAP-Namen zu verwenden).
- Eine fein abgestimmte Zugriffssteuerung ist auch weiterhin gewährleistet (Benutzer sehen nur die Daten, für die sie eine entsprechende Berechtigung haben).
- Komplexe Suchvorgänge können über neue Objekttypen (oder Attributkombinationen) durchgeführt werden, die in einer reinen LDAP-Umgebung möglicherweise nicht möglich wären.

Identity Manager nutzt die Abstraktion, um diese Ziele und vieles mehr umzusetzen.

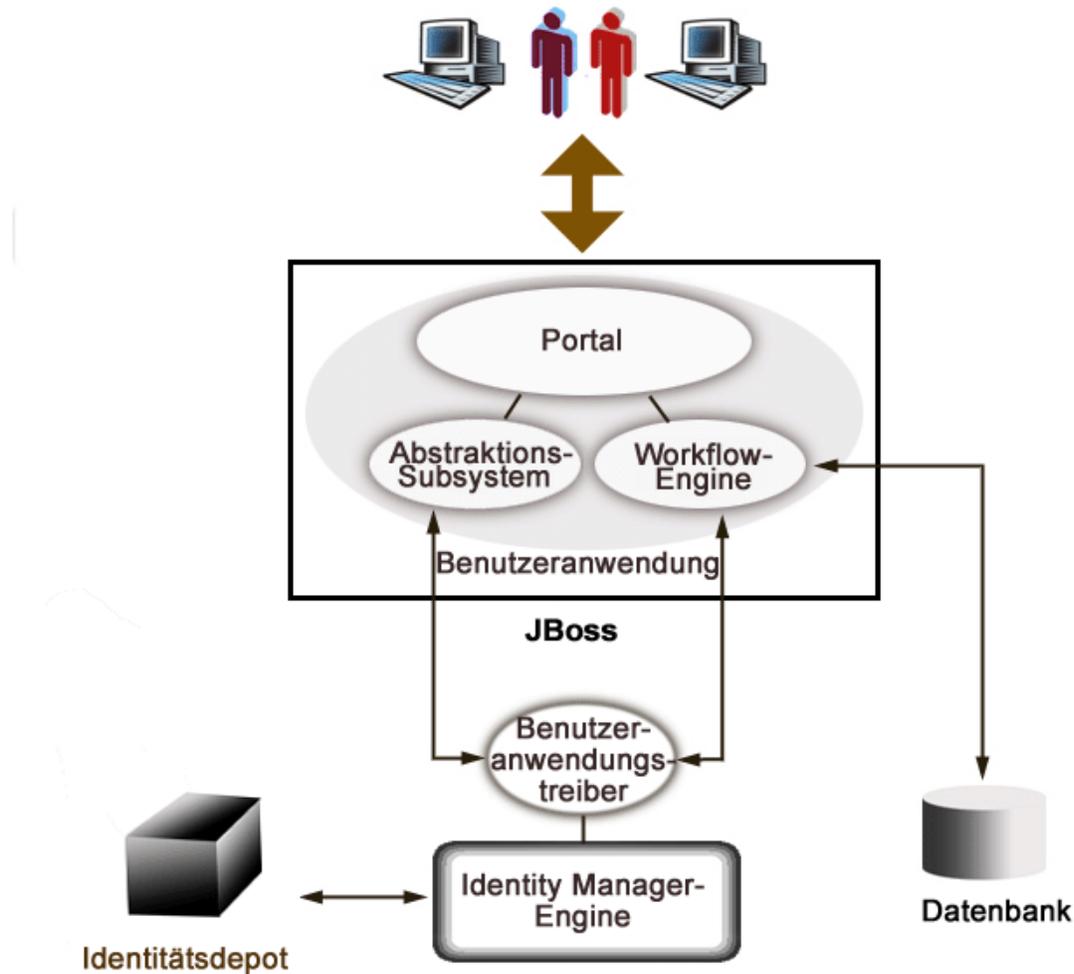
## 1.3 Allgemeine Übersicht über die Architektur

Die Identity Manager-Benutzeranwendung basiert auf mehreren unabhängigen Komponenten, die zusammen agieren. Die Kernkomponenten und deren wesentliche Verantwortlichkeiten werden in der folgenden Tabelle beschrieben.

Komponente	Beschreibung
Identitätsdepot (eDirectory 8.7.3 oder 8.8)	Repository für Benutzerdaten (und andere Identitätsdaten) plus IDM-Treibersatz und Treiber sowie verschiedene Abstraktionsschichten und (bei installiertem Bereitstellungsmodul) Workflow-Artefakte.
Identity Manager-Engine	Dies ist das Runtime-Framework von Identity Manager, das alle Ereignisse in eDirectory (und in verbundenen Systemen) überwacht, Richtlinien auferlegt und Daten an das bzw. aus dem Identitätsdepot weiterleitet.
Benutzeranwendungstreiber	Der Benutzeranwendungstreiber kommuniziert mit der Benutzeranwendung und aktualisiert deren Cache-Speicher mit den geänderten Definitionen für die Abstraktionsschichten. Bei installiertem Bereitstellungsmodul kann der Benutzeranwendungstreiber auch so konfiguriert werden, dass durch Ereignisse im Identitätsdepot Workflows ausgelöst werden. Außerdem leitet er Berechtigungsinformationen zurück an das Identitätsdepot, damit ein Nachweis darüber existiert, der nach Abschluss des Workflows belegt, welche Berechtigung gewährt (bzw. nicht gewährt) wurde.
Benutzeranwendung: Web-Benutzeroberfläche	Die Web-Benutzeroberfläche der Benutzeranwendungen ist eine Browser-basierte Java-Anwendung, mit der die JSR-168-kompatiblen Portlets eine Verbindung herstellen.
Benutzeranwendung: Abstraktionsschicht	Die Abstraktionsschicht isoliert die Datendarstellungslogik aus dem Identitätsdepot, sodass alle Anforderungen nach Identitätsdaten durch die Abstraktionsschicht geleitet werden müssen. Der Direktzugriff von Portlet-Code auf Identitätsinformationen ist nicht möglich. Alle Anforderungen werden durch die Abstraktionsschicht geleitet und unterliegen den entsprechenden Einschränkungen (z. B. der Zugriffssteuerung).
Benutzeranwendung: Workflow-Engine (nur mit dem Bereitstellungsmodul erhältlich)	Die Workflow-Engine besteht aus mehreren Java-Programmdateien, die für die Verwaltung und Ausführung von Schritten in einem vom Administrator definierten Workflow verantwortlich sind.
JBoss Application Server	Der Open-Source-JBoss Application Server stellt das Runtime-Framework bereit, in dem die Benutzeranwendung, die Abstraktionsschicht und die Workflow-Engine ausgeführt werden.
Datenbank (standardmäßig MySQL)	Die Datenbank (eine Liste der unterstützten Datenbanken finden Sie in der Installationsanleitung) speichert bestimmte Arten von Konfigurationsinformationen für die Benutzeranwendung sowie den Workflow-Status (bei installiertem Bereitstellungsmodul).
Composer-Service-Treiber	Der Composer-Service-Treiber ist ein Teil des Benutzeranwendungstreibers, der vom Benutzer so konfiguriert werden kann, dass er auf Identitätsdepot-Ereignisse mit dem Auslösen von Workflows reagiert.
Novell Audit	Novell Audit ist ein eigenständiger Protokollserver, der viele unterschiedliche Daten speichern kann (z. B. Daten, die in Workflow-Schritten generiert werden). Weitere Informationen finden Sie im Kapitel über die Einrichtung der Protokollierung.

Die oben genannten Komponenten sind hinsichtlich des Informationsflusses logisch miteinander verbunden, wie in der Grafik unten veranschaulicht. Es ist möglich (und in den meisten Fällen ist

dies der Fall), dass sich die einzelnen Komponenten physisch auf mehreren Computern befinden. Beispiel: Selbst wenn das Identitätsdepot (und iManager, dessen wichtigstes Administrationswerkzeug) auf derselben Maschine installiert ist wie die Identity Manager-Engine, befindet sich JBoss (sowie die Benutzeranwendung) in der Regel auf einem anderen Computer (oder auf einer Gruppe von Computern, wenn sie als Cluster gruppiert sind). Nicht nur aus Leistungsgründen, sondern auch aus Gründen der Sicherheit und der Datenwiederherstellung befindet sich die Datenbank (MySQL) in der Regel auf einem eigenen Computer.



### 1.3.1 Identitätsdepot

Das Identitätsdepot dient der Speicherung verschiedener Arten von Identitätsdaten und Definitionen für die Abstraktionsschicht. Zu diesem Zweck wird eine Instanz von eDirectory (läuft auf Windows, Solaris oder Linux) verwendet. Mit eDirectory kann Identity Manager ein erprobtes, hochgradig skalierbares unternehmensweites LDAPv3-Verzeichnis mit Funktionen zur Partition und Reproduktion sowie einem flexiblen, webbasierten Management- und Konfigurationswerkzeug (iManager) nutzen, das einen administrativen All-in-one-Integrationspunkt zwischen Identity Manager und eDirectory bietet.

## 1.3.2 JBoss

Die Benutzeranwendung ist als Java-Webanwendungsarchiv oder WAR-Datei komprimiert. Die WAR-Datei wird in JBoss bereitgestellt, dem weit verbreiteten Open-Source-Java-Anwendungsserver (der Tomcat als Servlet-Engine verwendet; nicht in der Grafik dargestellt). Die Verwendung von JBoss als Ausführungsumgebung hat viele Vorteile:

- Der Quellcode ist frei zugänglich.
- JBoss ist ab Version 4.0.3 clusterbar.
- JBoss ist vollständig J2EE-konform, d. h., jede beliebige J2EE-Anwendung kann darauf ausgeführt werden. Sie können zusätzliche Anwendungen (z. B. Web-Services) auf der gleichen JBoss-Instanz hosten, auf der die Benutzeranwendung läuft.
- JBoss unterstützt die standardmäßigen JAAS- und JACC-Java-Sicherheits- und Autorisierungs-Services (die von der Benutzeranwendung für den Zugriff auf das Identitätsdepot verwendet werden).
- JBoss läuft auf vielen verschiedenen Plattformen, einschließlich Windows und Linux.

Die WAR-Datei der Benutzeranwendung enthält ausführbaren Code für die Benutzeranwendung, die wiederum aus Gründen der Übersichtlichkeit mit einer Model-View-Controller-Architektur (MVC) erzeugt wird. Die benutzerseitigen Schnittstellen laufen als modulare Portlets innerhalb der Benutzeranwendung. Zur Anzeige von Organigrammen und Benutzerinformationen, zur Durchführung von Suchvorgängen, zum Zurücksetzen von Passwörtern und vielem mehr stehen separate Portlets zur Verfügung.

Weitere Informationen zu verschiedenen Aspekten der Bereitstellung von Webanwendungen an JBoss finden Sie in der Dokumentation zu JBoss unter <http://www.jboss.org/products/jbossas/docs> (<http://www.jboss.org/products/jbossas/docs>).

## 1.3.3 Datenbank

Die Benutzeranwendung beruht auf einer Datenbank (standardmäßig MySQL; eine Liste der unterstützten Datenbanken finden Sie in der Installationsanleitung) zum Speichern verschiedener Arten von Informationen:

- Konfigurationsdaten der Benutzeranwendung: z. B. Webseitendefinitionen, Portlet-Instanz-Registrierungen und Werte der Standardeinstellungen
- Bei installiertem Bereitstellungsmodul werden die Workflow-Status-Informationen in der Datenbank gespeichert (die eigentlichen Workflow-Definitionen werden im Identitätsdepot gespeichert)
- Novell Audit-Protokolle

## 1.3.4 Identity Manager-Engine

Identity Manager umfasst eine Runtime-Engine, Treiber und Richtlinien. Die Identity Manager-Engine reagiert auf Ereignisse im Identitätsdepot und verwaltet den Datenfluss und die Transformation von Daten, die im Depot eingehen bzw. dieses verlassen. Treiberobjekte verkapseln Programmdatei-Code und Artefakte (z. B. Richtliniendokumente), die einem bestimmten verbundenen System ein spezifisches Verhalten bei der Datenverarbeitung bereitstellen. Die Identity Manager-Benutzeranwendung ist ein verbundenes System. Die Kommunikation zwischen dem

Identitätsdepot, der Abstraktionsschicht der Benutzeranwendung und der Workflow-Engine verläuft über den Benutzeranwendungstreiber (siehe unten).

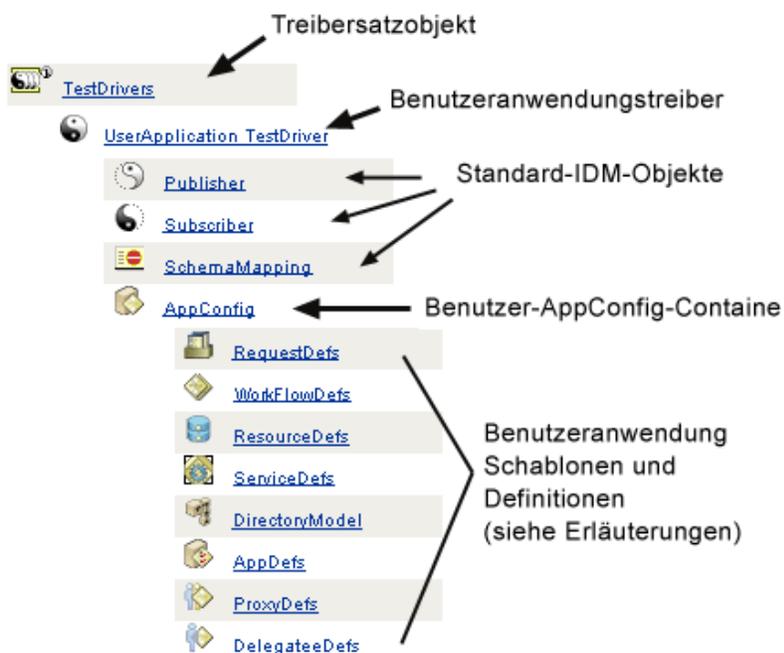
Da die Benutzeranwendung auf verschiedenen Verzeichnisobjekten zur Speicherung von Artefakten der Abstraktionsschicht beruht, muss das eDirectory-Schema erweitert werden, um die von der Benutzeranwendung benötigten benutzerdefinierten LDAP-Objekte und Attribute einzubinden. Die Erweiterung des Schemas wird automatisch als Teil des Identity Manager-Installationsvorgangs durchgeführt. Benutzerdefinierte Objekte und Attribute werden erst dann mit Standardwerten ausgefüllt, wenn der Benutzeranwendungstreiber installiert und aktiviert ist.

### 1.3.5 Benutzeranwendungstreiber

Der Benutzeranwendungstreiber ist eine wichtige Aktivierungskomponente der Benutzeranwendung. Eine der Aufgaben des Benutzeranwendungstreibers ist es, der Abstraktionsschicht eine Änderung wichtiger Datenwerte im Identitätsdepot zu melden, damit die Abstraktionsschicht ihren Cache-Speicher aktualisiert.

Bei installiertem Bereitstellungsmodul kann der Benutzeranwendungstreiber so konfiguriert werden, dass bei Änderungen der Attributwerte im Identitätsdepot automatisch Workflows ausgelöst werden.

Der Benutzeranwendungstreiber ist nicht nur eine Runtime-Komponente, sondern enthält auch Verzeichnisobjekte (einschließlich der Runtime-Artefakte der Benutzeranwendung). Eine typische Darstellung von dem Benutzeranwendungstreiber zugeordneten Verzeichnis-Artefakten wird in der folgenden Abbildung gezeigt.



---

**Hinweis:** Die abgebildeten Namen stellen Common-Name-Werte (cn) von LDAP dar. Auf die tatsächliche Schemabenenennung der verschiedenen Objektklassen wird an anderer Stelle eingegangen.

---

Diese Artefakt-Kategorien werden später ausführlicher beschrieben.

### **Treibersatzobjekt**

Bei jeder Installation von Identity Manager müssen die Treiber in Treibersätzen gruppiert werden. Es kann immer nur ein Treibersatz (auf einem vorhandenen Verzeichnisserver) aktiv sein. Die Treiber dieses Satzes können einzeln aktiviert oder deaktiviert werden, ohne dass dies Auswirkungen auf den Treibersatz im Ganzen hat. Der Benutzeranwendungstreiber muss (wie jeder andere IDM-Treiber) in einem Treibersatz vorhanden sein. Der Treibersatz wird nicht automatisch von der Benutzeranwendung erstellt, sondern Sie müssen zuvor einen Satz erstellen und darin dann den Benutzeranwendungstreiber erstellen.

### **Benutzeranwendungstreiber**

Das Benutzeranwendungstreiber-Objekt (das beliebig benannt werden kann) ist ein Container für eine Vielzahl von Artefakten. Wie bei allen Identity Manager-Treibern implementiert der Benutzeranwendungstreiber Herausgeber- und Abonnentenkanalobjekte und -richtlinien. Der Herausgeberkanal wird nicht von der Benutzeranwendung verwendet, kann aber für benutzerdefinierte Zwecke genutzt werden.

### **AppConfig-Objekt**

Das AppConfig-Objekt ist ein Container für verschiedene Objekte der Benutzeranwendungskonfiguration:

#### **RequestDefs**

Hierbei handelt es sich um einen Container für Bereitstellungsanforderungsdefinitionen, d. h. die vom Administrator konfigurierten Anforderungsdefinitionen, die der Laufzeit der Benutzeranwendung zur Verfügung stehen (bei installiertem Bereitstellungsmodul). Die hier (als XML) gespeicherten Definitionen stellen die Anforderungsklassen dar, die Endbenutzer mit den entsprechenden Rechten über die Benutzeranwendung instanziierten können. RequestDef ordnet einen WorkflowDef (unten) einem ResourceDef zu.

#### **WorkflowDefs**

Ein Container für Workflow-Objekte, einschließlich der Beschreibungen während der Design-Phase plus etwaiger Schablonen bzw. ungenutzter Abläufe.

#### **ResourceDefs**

Ein Container für Definitionen von bereitstellbaren Ressourcen, einschließlich der Beschreibungen während der Design-Phase plus etwaiger Schablonen bzw. ungenutzter Ziele.

#### **ServiceDefs**

Ein Container für Servicedefinitionsobjekte, die die von Workflows aufgerufenen Web-Services enthalten.

#### **DirectoryModel**

Abstraktionsschicht-Objekte auf Metaebene (ChoiceDefs, EntityDefs, RelationshipDefs), die unterschiedliche Inhalte (einige vom Benutzer definierbar, andere vom Administrator eingerichtet) des Verzeichnisses repräsentieren, das von den Identitäts-Portlets freigelegt werden kann.

## AppDefs

Ein Container für Konfigurationsobjekte, die zur Initialisierung der Laufzeitumgebung verwendet werden, z. B. Informationen für die Cache-Konfiguration und Eigenschaften für die Email-Benachrichtigung.

## ProxyDefs

Ein Container für Vertretungsdefinitionen.

## DelegateeDefs

Ein Container für Delegierungsdefinitionen.

## 1.3.6 Verzeichnisabstraktionsschicht

Portlets erhalten ihre Identitätsdaten durch Abfragen in der Verzeichnisabstraktionsschicht. In dieser Code-Schicht werden Angaben über den Zugriff auf Identitätsdaten von Client-Prozessen isoliert. Wenn beispielsweise ein Portlet eine Suche über Identitätsdaten ausführen muss, nimmt anstelle des Portlets die Abstraktionsschicht die entsprechenden Abfragen im Zielcontainer des Identitätsdepots vor. Ein Portlet führt nie direkte Anfragen im Identitätsdepot aus.

Die Abstraktionsschicht ist gleichzeitig die Code-Schicht, über die von Administratoren oder anderen qualifizierten Systembenutzern festgelegte Abstraktionsschichtdefinitionen erstellt oder geändert werden. Zur Durchführung entsprechender Änderungen verwendet der Systemexperte den Verzeichnisabstraktionsschicht-Editor der Designer-Anwendung (siehe [Kapitel 4, „Konfigurieren der Verzeichnisabstraktionsschicht“](#), auf Seite 75).

Die Abstraktionsschicht speichert während der Laufzeit eine große Anzahl der vom Identitätsdepot eingeholten Konfigurations- und Entitätsdefinitionsdaten im Cache. Die verschiedenen Cache-Speicher der Benutzeranwendung können detailliert vom Administrator verwaltet werden. Weitere Informationen zu Cache-Speichern und der Cache-Verwaltung finden Sie in [Kapitel 13, „Cache-Konfiguration“](#), auf Seite 219.

## 1.3.7 Workflow-Engine

Die Workflow-Engine (zusammen mit dem Bereitstellungsmodul erhältlich) ist der Laufzeitklassensatz, der für die Ausführung der Schritte eines Workflows gemäß einer Vorgangsdefinition (ein Laufzeitartefakt, das bei der Instanziierung eines Workflows erstellt wird) zuständig ist und der die Statusinformationen aufzeichnet und in einer Datenbank wie MySQL oder Oracle speichert (siehe oben [Abschnitt 1.3.3, „Datenbank“](#), auf Seite 24).

Weitere Informationen zum Workflow-System sowie zur Erstellung von Workflows finden Sie in diesem Handbuch in [Kapitel 21, „Einführung in die Workflow-basierte Bereitstellung“](#), auf Seite 309.

## 1.3.8 Benutzeroberfläche

Die Identity Manager-Benutzeroberfläche umfasst eine Sammlung von JSR-168-konformen Portlets (sowie Java-Server-Seiten bei installiertem Bereitstellungsmodul), die innerhalb einer Java-Webanwendung auf JBoss laufen. Die Portlet-Architektur gewährleistet ein hohes Maß an Modularität, die Anpassung der Inhalte sowie Benutzerkontrolle über die Seitendarstellung. Die Benutzeranwendung bietet verschiedene Container-Services. Sie verwaltet u. a. den Fensterstatus,

die Portlet-Einstellungen, die permanente Speicherung, das Caching, Themen und die Protokollierung und agiert als Gatekeeper für die Sicherheit. Der Anwendungsserver, auf dem die Benutzeranwendung ausgeführt wird, bietet der Anwendung verschiedene Services, z. B. Skalierung durch Cluster-Gruppierung, Datenbankzugriff über JDBC und Unterstützung von zertifikatbasierter Sicherheit.

Das hohe Maß an Verkapselung, das durch diese Architektur geboten wird, gewährleistet auf Präsentationsebene eine zuverlässige und sichere Umgebung für die Identity Manager-Benutzeranwendung. Sie garantiert außerdem einen hohen Grad an administrativer Steuerung aller Aspekte der Benutzeroberfläche.

Weitere Informationen zur Verwaltung der Komponenten der Benutzeroberfläche finden Sie in den verschiedenen Kapiteln in diesem Handbuch in [Teil III, „Verwalten der Benutzeranwendung“, auf Seite 129](#).

## 1.4 Design- und Konfigurationswerkzeuge

Viele Funktionen der Identity Manager-Benutzeranwendung können benutzerdefiniert oder mithilfe des Designerwerkzeugs von Identity Manager (basierend auf der Eclipse Rich Client-Plattform) oder über iManager-Plugins angepasst werden.

Die verfügbaren Werkzeuge und deren vorgesehener Verwendungszweck werden in der folgenden Tabelle beschrieben.

Werkzeug	Zweck
Designer für Identity Manager	Allgemeines Konfigurationswerkzeug für Identity Manager, das dem Entwickler, Berater oder Systemadministrator detaillierte Konfigurationsänderungen an Treibersätzen, Treibern, Richtliniendefinitionen und anderen Artefakten ermöglicht.
Verzeichnisabstraktionsschicht-Editor-Plugin für Designer	Ermöglicht die Definition von benutzerdefinierten Objekten und Relationen sowie die Durchführung von Änderungen an vielen Konfigurationseinstellungen der Abstraktionsschicht. Siehe <a href="#">Kapitel 4, „Konfigurieren der Verzeichnisabstraktionsschicht“, auf Seite 75</a> in diesem Handbuch.
Plugin für die Konfiguration von Bereitstellungsanforderungen	Ermöglicht die Definition und Konfiguration von verfügbaren Bereitstellungsanforderungstypen (in iManager).
Editor für bereitstellbare Ressourcen (bald erhältlich)	Designer-Plugin für die Erstellung und Konfiguration von Ressourcen (Objekte, die die Ressource darstellen, die als Reaktion auf einen Workflow erteilt wird).
Editor für die Workflow-Definition (bald erhältlich)	Grafisches Plugin zur Workflow-Definition für den Designer.
Editor für Workflow-Email-Schablonen	Ein iManager-Plugin ermöglicht Administratoren, Email-Schablonen hinzuzufügen, zu löschen und zu bearbeiten. Diese Schablonen können vom Workflow-System verwendet werden, um Benutzer über Workflow-Ereignisse in Kenntnis zu setzen.

Werkzeug	Zweck
<b>Ireport.exe</b> (Werkzeug für Protokollberichte) und die Revisions- und Protokollfunktion von iManager.	Einige vordefinierte Protokollberichte (im Lieferumfang von Identity Manager) stehen im Crystal-Reports-Format (.rpt) zum Filtern von Daten zur Verfügung, die in der Novell Audit-Datenbank protokolliert sind. Eine Methode zur Erzeugung von Berichten ist das Protokollbericht-Werkzeug <b>Ireport.exe</b> (nur für Windows). Sie können Berichte auch mithilfe anderer Methoden erstellen. Weitere Informationen hierzu finden Sie in <a href="#">Kapitel 5</a> , „ <a href="#">Einrichten der Protokollierung</a> “, auf Seite 121.

Ein Experte für das Systemdesign richtet in der Regel zunächst mithilfe des Verzeichnisabstraktionsschicht-Editors (in Designer für Identity Manager) benutzerdefinierte Abstraktionsschichtdefinitionen für die Benutzeranwendung ein. Diese Objekte sind dann für die Verwendung durch die Abstraktionsschicht verfügbar (und somit für Benutzer der Benutzeroberfläche). In der Definition und bei der Verwendung dieser Objekte können detaillierte Einstellungen für die Zugriffssteuerung vorgenommen werden, damit der Administrator und die Endbenutzer nur Objekte (und Attribute der Objekte) sehen und bearbeiten können, für die sie über die entsprechenden Rechte verfügen.

Bei installiertem Bereitstellungsmodul definiert der Experte für das Systemdesign oder der Administrator anhand der Assistenten zur Konfiguration von Bereitstellungsanforderungen in iManager üblicherweise die bereitstellbaren Ressourcen und Workflows, die für die Benutzer der Benutzeranwendung verfügbar sind. Gleichzeitig definiert der Administrator über die Editorfunktion für Email-Schablonen (in iManager) die Inhalte von Email-Benachrichtigungen, die von den Workflows gesendet werden. Weitere Informationen hierzu finden Sie in [Kapitel 23](#), „[Verwalten von Bereitstellungs-Workflows](#)“, auf Seite 347.

Nach der Konfiguration der Abstraktionsschicht, Bereitstellungsanforderungsdefinitionen, Revisionsvorgaben und Email-Schablonen führt der Administrator in der Regel verschiedene Konfigurationen bezüglich der Benutzeranwendung (einschließlich Sicherheit, Caching und andere Funktionen) mithilfe der in [Kapitel 10](#), „[Portalkonfiguration](#)“, auf Seite 201 beschriebenen Administrationsfunktionen durch. Abschließend passt der Administrator die einzelnen Portlets mithilfe der in den verschiedenen Kapiteln in Teil IV dieses Handbuchs beschriebenen Schnittstellen nach Bedarf an.

---

**Hinweis:** Es empfiehlt sich, vor der Implementierung einer Produktionsumgebung das folgende Kapitel zu lesen, in dem einige dieser Aufgaben ausführlicher beschrieben werden.

---

## 1.5 Anwendungsszenarios

In der Identity Manager-Benutzeranwendung sind zahlreiche Funktionen verfügbar. Im Folgenden werden einige Beispiele aufgeführt, die veranschaulichen, wie die Benutzeranwendung zur Lösung von Problemen eingesetzt werden kann.

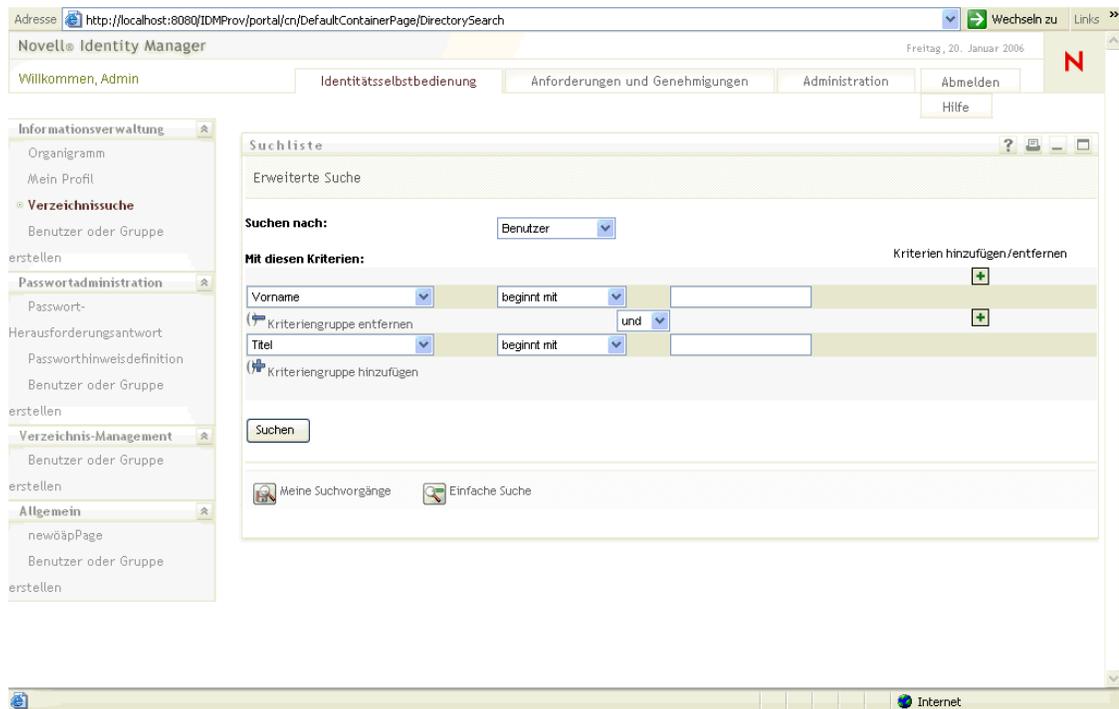
## 1.5.1 Szenario A: Der Benutzer sucht Informationen zu anderen Personen der Organisation

Es kommt häufig vor, dass ein Mitarbeiter Informationen zu einer anderen Person der Organisation benötigt. Zum Beispiel:

- Vollständigen Namen eines Kollegen suchen
- Personen mit einer bestimmten Kompetenz innerhalb eines bestimmten geografischen Bereichs suchen
- Manager einer bestimmten Person ermitteln

Diese Vorgänge (einschließlich erweiterter Suchen basierend auf komplexeren Abfragen) können problemlos über die Verzeichnissuche durchgeführt werden. Der Endbenutzer meldet sich in der Regel bei der Benutzeranwendung an, wählt die Registerkarte „Identitätsselbstbedienung“ aus (wenn sie nicht bereits ausgewählt ist) und klickt in der Spalte mit den Navigations-Links auf der linken Seite des Bildschirms auf den Link „Verzeichnissuche“.

Im Bildschirm unten hat der angemeldete Benutzer eine erweiterte Suche für Benutzer eingerichtet, deren Abteilung mit `Sales` beginnt und deren Titel „Manager“ enthält.



The screenshot displays the Novelle Identity Manager web application interface. The browser address bar shows the URL: `http://localhost:8080/IDMProv/portal/cn/DefaultContainerPage/DirectorySearch`. The page title is "Novelle Identity Manager" and the date is "Freitag, 20. Januar 2006". The user is logged in as "Admin".

The main navigation menu includes: Willkommen, Admin; Identitätsselbstbedienung; Anforderungen und Genehmigungen; Administration; Abmelden; Hilfe.

The left sidebar contains the following sections:

- Informationsverwaltung**
  - Organigramm
  - Mein Profil
  - Verzeichnissuche**
    - Benutzer oder Gruppe erstellen
- Passwortadministration**
  - Passwort-
    - Herausforderungsantwort
    - Passworthinweisdefinition
    - Benutzer oder Gruppe erstellen
- Verzeichnis-Management**
  - Benutzer oder Gruppe erstellen
- Allgemein**
  - newöapPage
  - Benutzer oder Gruppe erstellen

The main content area is titled "Suchliste" and shows an "Erweiterte Suche" (Advanced Search) form. The search criteria are:

- Suchen nach: Benutzer
- Mit diesen Kriterien: Kriterien hinzufügen/entfernen
- Vorname: beginnt mit [ ]
- und
- Titel: beginnt mit [ ]

Buttons for "Suchen", "Kriteriengruppe entfernen", and "Kriteriengruppe hinzufügen" are visible. At the bottom, there are links for "Meine Suchvorgänge" and "Einfache Suche".

Nach der Durchführung der Suche wird ein Ergebnisbildschirm angezeigt, der wie folgt aussieht:

Novell Identity Manager  
Freitag, 20. Januar 2006

Willkommen, Admin | Identitätsselbstbedienung | Anforderungen und Genehmigungen | Administration | Abmelden | Hilfe

Informationsverwaltung  
Organigramm  
Mein Profil  
Verzeichnissuche  
Benutzer oder Gruppe erstellen  
Passwortadministration  
Passwort-  
Herausforderungsantwort  
Passworthinweisdefinition  
Benutzer oder Gruppe erstellen  
Verzeichnis-Management  
Benutzer oder Gruppe erstellen  
Allgemein  
newöapPage  
Benutzer oder Gruppe erstellen

Suchliste

Suchergebnisse

Verwenden Sie die folgenden Registerkarten, um unterschiedliche Ansichten Ihres Ergebnis-Sets anzuzeigen.

Benutzer: (Vorname beginnt mit b)  
Sortiert nach: Nachname  
Gesamtzahl Übereinstimmungen: 2

Identität	Standort	Organisation		
<b>Vorname</b>	<b>Nachname</b>	<b>Titel</b>	<b>Email</b>	<b>Telefonnummer</b>
Bob	Green	CEO	✉	54545-5454
Billy	Murphy	Manager	✉	54454-5456465

1 - 2 von 2

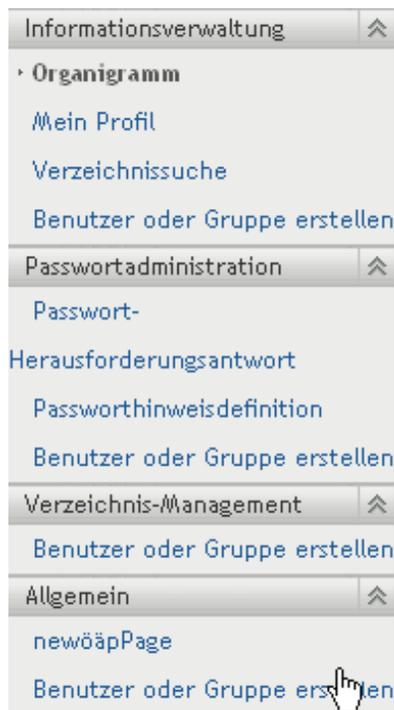
Meine Suchvorgänge | Suche speichern | Ergebnisse exportieren | Suche revidieren | Neue Suche

Beachten Sie die Reihe mit Schaltflächen im unteren Bereich des Bildschirms, über die der Benutzer u. a. diese erweiterte Suche speichern, die Abfrage überarbeiten oder eine neue Suche starten kann. Beachten Sie auch die Registerkarten oberhalb der Liste mit den gefundenen Personen. Die Personen sind nach Identität aufgelistet, können aber auch über die entsprechende Registerkarte nach Standort oder Organisation angezeigt werden.

## 1.5.2 Szenario B: Der Manager erstellt einen neuen Benutzer

Eine Abteilung eines Unternehmens beschäftigt einen neuen Praktikanten oder einen freien Mitarbeiter (der nur für einen begrenzten Zeitraum bei dem Unternehmen arbeitet). Die neue Person muss ins System eingetragen werden, damit ihr die benötigten Ressourcen bereitgestellt werden können (und damit sie bei wie zuvor beschriebenen Suchvorgängen gefunden werden kann). Da die Person nicht fest angestellt ist, wird sie nicht in das reguläre Personalsystem des Unternehmens aufgenommen. Die Identität der Person (und deren Zugriff auf Ressourcen) muss dennoch auf sichere Weise verwaltet werden.

Als Manager der betreffenden Abteilung sind Sie befugt, im System Benutzer zu erstellen. Nach Ihrer Anmeldung wird in der Spalte mit den Navigations-Links auf der linken Seite des Bildschirms der Link „Benutzer oder Gruppe erstellen“ angezeigt (siehe unten):

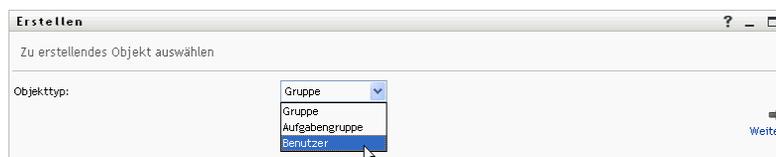


---

**Hinweis:** Dieser Link ist nur sichtbar, wenn der angemeldete Benutzer über die entsprechenden Rechte verfügt.

---

Nach einem Klick auf diesen Link werden Sie gefragt, ob Sie eine neue Gruppe, eine neue Aufgabengruppe oder einen neuen Benutzer erstellen möchten (siehe unten).



Wählen Sie „Benutzer“ aus und klicken Sie auf „Weiter“. Im nächsten Bildschirm des Assistenten können Sie die persönlichen Informationen des Benutzers eingeben:

Im nächsten Bildschirm können Sie dem neuen Benutzer ein Passwort zuweisen:

Im letzten Bildschirm wird das Nettoergebnis des Prozesses angezeigt.

In diesem Beispiel ist die neu eingegebene Person ein Benutzer mit allen Rechten eines normalen Benutzers. Es kann z. B. auch das Objekt „Praktikant“ definiert werden, dem über den Verzeichnisabstraktionsschicht-Editor spezielle Attribute und Rechte zugewiesen werden, die nur für diesen Objekttyp gelten. In diesem Fall hätte in der zuvor angezeigten Auswahlliste neben „Gruppe“, „Aufgabengruppe“ und „Benutzer“ auch das Objekt Praktikant ausgewählt werden können.

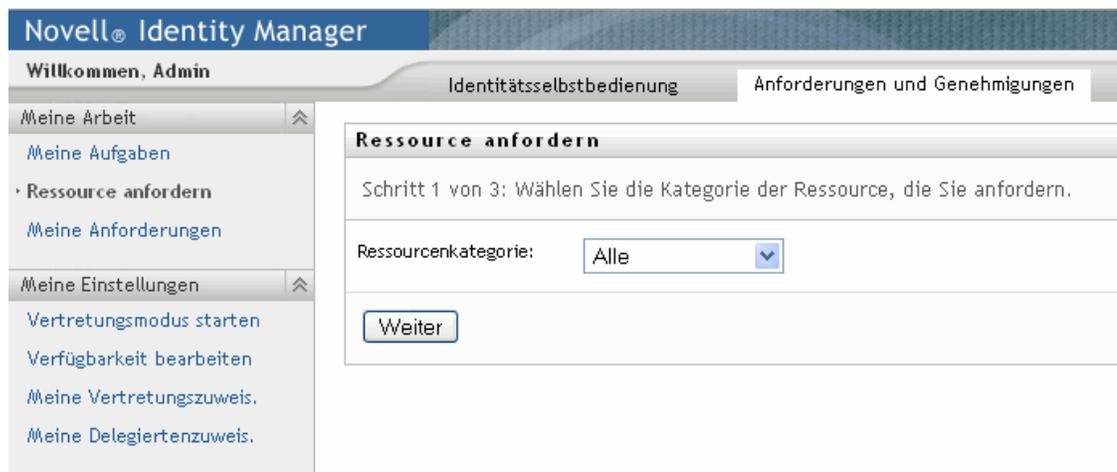
### 1.5.3 Szenario C: Bereitstellungsanforderungen von Benutzern

Es kommt häufig vor, dass ein Angestellter eine bestimmte Ressource benötigt (z. B. Büromaterialien, eine Kreditkarte des Unternehmens oder Zugriff auf eine Datenbank), deren

Freigabe erst von einer anderen Person genehmigt werden muss. Dieser Vorgang wird als Bereitstellungsanforderung bezeichnet. Bei installiertem und konfiguriertem Bereitstellungsmodul können Anforderungen dieser Art in Identity Manager über Workflows bearbeitet werden.

**Hinweis:** Im Gegensatz zu den vorhergehenden Beispielen wird in diesem Beispiel vorausgesetzt, dass das Bereitstellungsmodul installiert und konfiguriert ist.

Nach der Anmeldung des Benutzers wird seine Startseite angezeigt. Der Benutzer klickt dann im oberen Bereich der Seite auf die Registerkarte *Anforderungen und Genehmigungen* und wählt im Navigationsbereich auf der linken Seite den Link *Ressource anfordern* aus. Nach einem Klick auf den Link *Ressource anfordern* wird in der Benutzeranwendung das ursprüngliche Anforderungsformular angezeigt.



Im Dropdown-Menü „Ressourcenkategorie“ werden die Ressourcentypen, einschließlich der Berechtigungen mit beliebigen Namen, aufgeführt. (Weitere Informationen zu Berechtigungen und deren Erstellung finden Sie im Administrationshandbuch von Identity Manager.) Durch die Auswahl von *Alle*, wie in der Abbildung dargestellt, werden alle verfügbaren bereitstellbaren Ressourcen angezeigt (anders ausgedrückt, alle Ressourcen, die der angemeldete Benutzer mit seinen aktuellen Rechten anfordern kann).

Nach einem Klick auf „Weiter“ werden im nächsten Bildschirm alle Bereitstellungsanforderungstypen angezeigt, auf die dieser Benutzer zugreifen kann.



In diesem Beispiel möchte der Benutzer ein Active Directory-Konto anfordern, das vom Manager genehmigt werden muss. Nach einem Klick auf den entsprechenden Link und dem Ausfüllen eines einfachen Formulars wird der verknüpfte Workflow gestartet und der Manager des Benutzers erhält eine Email-Benachrichtigung bezüglich der vom Manager auszuführenden Aufgabe. Der Manager ruft dann seinerseits die Seite mit den *Anforderungen und Genehmigungen* auf und findet die Anforderung des Mitarbeiters in seiner Aufgabenliste, bereit zur Genehmigung oder Ablehnung. (Wenn der Manager Urlaub hat, wird seine ernannte Vertretung benachrichtigt, die sich anmelden und die gleichen Schritte unternehmen kann wie der Manager.) Unterdessen ändert sich der Browserbildschirm und zeigt eine Bestätigung an, dass die Workflow-Anforderung erfolgreich gesendet wurde.

Das Erteilen eines Kontos in einem der Verzeichnisse eines Unternehmens (wie hier beschrieben) ist ein Beispiel für eine Berechtigungsanforderung. In der Identity Manager-Benutzeranwendung können viele Arten von Berechtigungsanforderungen konfiguriert und viele Arten von Workflows (Genehmigung von einem oder mehreren Managern erforderlich, serieller oder paralleler Ablauf, mit oder ohne Zeitüberschreitungen) erstellt werden. In allen Fällen kann die Anzeige von Workflows und anderen Informationen detailliert verwaltet werden.

Weitere Informationen zu diesen Funktionen finden Sie in den letzten Kapiteln dieses Handbuchs. (Die Informationen in diesen Kapiteln sind in erster Linie für Administratoren gedacht. Die Verwendung der Funktionen wird ausführlicher im Benutzerhandbuch der Identity Manager-Benutzeranwendung beschrieben.)

## 1.6 Weitere Vorgehensweise

Wenn Sie mehr über die Planung einer Produktionsumgebung erfahren möchten, lesen Sie das nächste Kapitel ([Kapitel 2, „Konfiguration der Produktionsumgebung“, auf Seite 37](#)). Informationen zu anderen Themen finden Sie in einem der anderen Kapitel dieses Handbuchs:

Weitere Informationen zu den *Protokollier- und Revisionsfunktionen* der Benutzeranwendung finden Sie in [Kapitel 5, „Einrichten der Protokollierung“, auf Seite 121](#).

Weitere Informationen zur Anpassung der *Darstellung der Benutzeroberfläche* finden Sie in [Kapitel 8, „Konfiguration von Motiven“, auf Seite 175](#).

Weitere Informationen zur *Sicherheit* und deren Verwaltung über die Administrationsoberfläche der Benutzeranwendung (im Unterschied zu iManager) finden Sie in [Kapitel 11, „Sicherheitskonfiguration“, auf Seite 209](#).

Weitere Informationen zu den Funktionen der *Cache-Verwaltung* finden Sie in [Kapitel 13, „Cache-Konfiguration“, auf Seite 219](#).

Weitere Informationen zur Funktion der *Passwortverwaltung* finden Sie in [Kapitel 19, „Passwortverwaltungs-Portlet“, auf Seite 279](#).

Weitere Informationen zur *Portletadministration* finden Sie in [Kapitel 9, „Portletadministration“, auf Seite 181](#).

Weitere Informationen zum Import und Export von Portaldateien finden Sie in [Kapitel 14, „Werkzeuge zum Exportieren und Importieren von Portaldateien“, auf Seite 229](#).

Weitere Informationen zu Funktionen für *Organigramme* finden Sie in [Kapitel 18, „Portlet „Organigramm“, auf Seite 263](#).

Weitere Informationen zu Funktionen der *Verzeichnissuche* finden Sie in **Kapitel 20**, „Portlet „Suchliste““, auf Seite 293.

Weitere Informationen über Optionen zum Erstellen von neuen Objekten (Portlet *erstellen*) und zu deren Verwaltung finden Sie in **Kapitel 16**, „Das Portlet „Erstellen““, auf Seite 243.

Weitere Informationen zur Einrichtung und Verwaltung von *Workflows* finden Sie in **Kapitel 21**, „Einführung in die Workflow-basierte Bereitstellung“, auf Seite 309, **Kapitel 22**, „Konfigurieren von Bereitstellungsanforderungsdefinitionen“, auf Seite 323 und **Kapitel 23**, „Verwalten von Bereitstellungs-Workflows“, auf Seite 347.

# Konfiguration der Produktionsumgebung

# 2

In diesem Kapitel werden Aspekte behandelt, die beim Einrichten einer Produktionsumgebung berücksichtigt werden müssen. Es enthält Ratschläge zu mehreren Aspekten, die beim Übergang von einer Sandkasten-/Testumgebung (oder einer anderen Vorproduktionsumgebung) zu einer Produktionsumgebung zu beachten sind.

Dieses Kapitel ist in die folgenden Hauptabschnitte gegliedert:

- [Abschnitt 2.1, „Topologie“, auf Seite 37](#)
- [Abschnitt 2.2, „Sicherheit“, auf Seite 40](#)
- [Abschnitt 2.3, „Leistungsoptimierung“, auf Seite 43](#)
- [Abschnitt 2.4, „Cluster-Gruppierung“, auf Seite 47](#)

## 2.1 Topologie

Die Anzahl von Instanzen in jedem großen Subsystem und die Art und Weise ihrer Verbindung miteinander sind vielfältig. Es wird nicht jedes mögliche Layout unterstützt. Es ist wichtig, nicht nur die Möglichkeiten zu verstehen, sondern auch, warum einige Konfigurationen besser sind als andere.

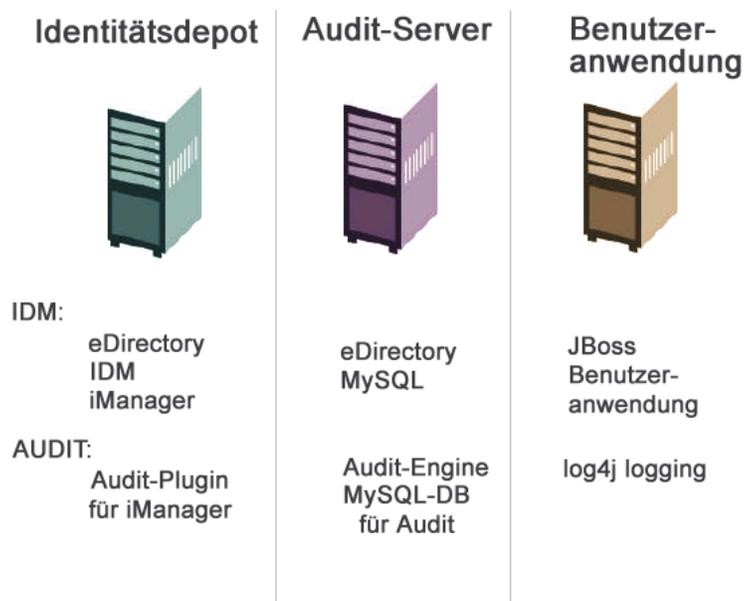
### 2.1.1 Minimale Konfiguration

Die einfachste logische Konfiguration der Benutzeranwendung ist eine Installation, bei der jede Komponente einmal installiert wird, d. h., sie besteht aus einem Identitätsdepot-Baum, einer Instanz der Identity Manager-Engine und deren Treibern sowie einer Instanz von JBoss, auf der eine einzelne Instanz der Benutzeranwendung ausgeführt wird. Hinsichtlich der physischen Implementierung könnten Sie theoretisch all diese Komponenten auf einem Computer ausführen. In der Praxis würde man dies jedoch aus mehreren Gründen vermeiden (hauptsächlich aus Gründen der Sicherheit, der Wartungsfähigkeit und der Performance). Bei der Entscheidung, wie viele Computer in der Praxis für die Installation benötigt werden, sollten Sie (mindestens) Folgendes berücksichtigen:

- *Novell Audit-Server*: Diese Komponente ist zur Laufzeit verantwortlich für die Erfassung von Ereignisinformationen (und möglicherweise vieler anderer Informationen) der Benutzeranwendungsumgebung. Sie erfüllt möglicherweise den weiteren Zweck der persistenten Speicherung für andere Anwendungen in Ihrem Unternehmen. Es gibt mehrere Gründe, aus denen Sie andere Hauptkomponenten des Identity Manager-Systems (z. B. JBoss oder das Identitätsdepot) nicht auf demselben Computer installieren sollten, auf dem der Audit-Server installiert ist.
- *Identitätsdepot*: Bei dieser Komponente tritt ein hoher Datenverkehr auf, daher sind eine gute Leistung und eine gute Skalierbarkeit erforderlich. Sie sollten erwägen, das Identitätsdepot auf einem eigenen Computer zu installieren. Es ist nicht empfehlenswert, auf dem gleichen Computer neben dem Identitätsdepot ein weiteres System mit hohem Datenverkehr auszuführen, z. B. JBoss mit einer Implementierung der Benutzeranwendung.

- *Datenbank*: Wenn diese Instanz von MySQL (oder einer anderen unterstützten Datenbank) gleichzeitig Ihre Novell Audit-Datenbank ist, befindet sie sich vermutlich auf einem eigenen Computer. Beachten Sie, dass diese Komponente folgendermaßen von der Benutzeranwendung verwendet wird:
- Als persistenter Speicher für Portalkonfigurationsdaten
- Als persistenter Speicher für Statusinformationen über aktive Workflows (bei installiertem Bereitstellungsmodul)
- Optional als Protokollspeicher für Novell Audit.
- *JBoss*: Aus Gründen der Leistung und der Kapazität sollte diese Komponente auf einem eigenen Computer ausgeführt werden.

Aus diesen Überlegungen ergibt sich die folgende Mindestkonfiguration auf drei Computern:



## 2.1.2 Hochverfügbarkeitskonfiguration

Die Cluster-Gruppierung zur Erzielung einer hohen Verfügbarkeit/Kapazität wird in einem späteren Abschnitt in diesem Kapitel behandelt. Zunächst einige allgemeine Informationen:

- Identity Manager unterstützt die Hochverfügbarkeit des Identitätsdepots, der Engine und der Treiber über die Multinode-Installation und die Mechanismen der gemeinsamen Speichernutzung, wie im Kapitel über die “Hochverfügbarkeit” im Administrationshandbuch von Identity Manager beschrieben. Eine umfassende Erläuterung zum Einrichten eines solchen Systems mit SUSE Linux finden Sie in einem Artikel unter:

<http://support.novell.com/cgi-bin/search/searchtid.cgi?/10093317.htm> (<http://support.novell.com/cgi-bin/search/searchtid.cgi?/10093317.htm>)

- Eine Hochverfügbarkeit der Benutzeranwendung wird durch das JBoss-Cluster ermöglicht. Sie können ein JBoss-Cluster so einrichten, dass jeder Knoten eine Instanz der Benutzeranwendung ausführt. Alle Instanzen sind gleichrangig (Peers). Es ist jedoch keine Reproduktion von Sitzungen über mehrere Instanzen hinweg möglich. Jede Instanz ist

verantwortlich für ihre entsprechende Arbeitseinheit und beendet keine Sitzung, die auf einem Geschwisterknoten gestartet wurde.

- Ein automatisches Failover wird nicht unterstützt (aus den genannten Gründen). Nach dem Verlust eines Clusterknotens kann ein unterbrochener Workflow wieder aufgenommen werden, wenn ein neuer Knoten mit derselben Workflow-Engine-ID wie der des ausgefallenen Knotens online gestellt wird. (In diesem Fall wird der unterbrochene Workflow nach dem Start der neuen Workflow-Engine automatisch wieder aufgenommen.)

In [Abschnitt 2.4, „Cluster-Gruppierung“](#), auf Seite 47 werden diese Themen ausführlicher behandelt.

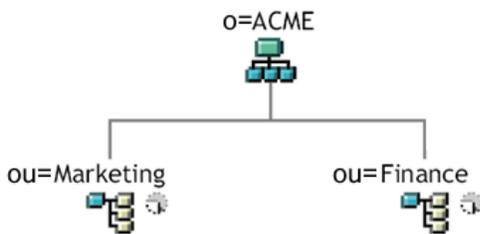
### 2.1.3 Beschränkungen bei der Konfiguration

Insbesondere sollte man die zwei wichtigsten Beschränkungen bei der Architektur beachten:

- Keine Benutzeranwendung kann mehr als einen Benutzercontainer bedienen (z. B. Suche/Abfrage, Hinzufügen von Benutzern). Sobald ein Benutzercontainer mit der Anwendung verknüpft wurde, sollte diese Verknüpfung außerdem dauerhaft sein.
- Es ist nicht möglich, einen Benutzeranwendungstreiber mit mehr als einer Benutzeranwendung zu verknüpfen, es sei denn, die Benutzeranwendungen sind auf gleichgeordneten Knoten desselben JBoss-Clusters installiert. In anderen Worten, die Zuordnung eines Treibers für mehrere Benutzeranwendungen wird nicht unterstützt.

Die erste Beschränkung erzwingt einen hohen Grad an Kapselung bei der Einrichtung von Benutzeranwendungen.

Angenommen, Sie verfügen über die folgende organisatorische Struktur:



Bei der Installation der Benutzeranwendung werden Sie aufgefordert, den Benutzercontainer der obersten Ebene festzulegen, nach dem die Installation im Identitätsdepot sucht. In diesem Fall könnten Sie *ou=Marketing,o=ACME* oder (alternativ) *ou=Finance,o=ACME* festlegen. Sie können nicht beides festlegen. Alle Suchvorgänge und Abfragen (und Anmeldungen des Administrators) der Benutzeranwendung beziehen sich auf den von Ihnen angegebenen Container.

---

**Hinweis:** Theoretisch würde eine Festlegung des Bereichs *o=ACME* auch die Container „Marketing“ und „Finance“ umfassen. In einer großen Organisation mit potentiell vielen *ou*-Containern (anstelle von nur zwei Containern für Marketing und Finance) ist dies allerdings möglicherweise nicht praktikabel.

---

Es ist natürlich möglich, von der Benutzeranwendung zwei unabhängige Installationen zu erstellen (ohne gemeinsame Ressourcen): eine für Marketing und eine andere für Finance. Jede Installation verfügt in diesem Fall über eine eigene Datenbank sowie einen eigenen, entsprechend konfigurierten

Benutzeranwendungstreiber und jede Benutzeranwendung wird, möglicherweise mit eigenen Motiven, separat verwaltet.

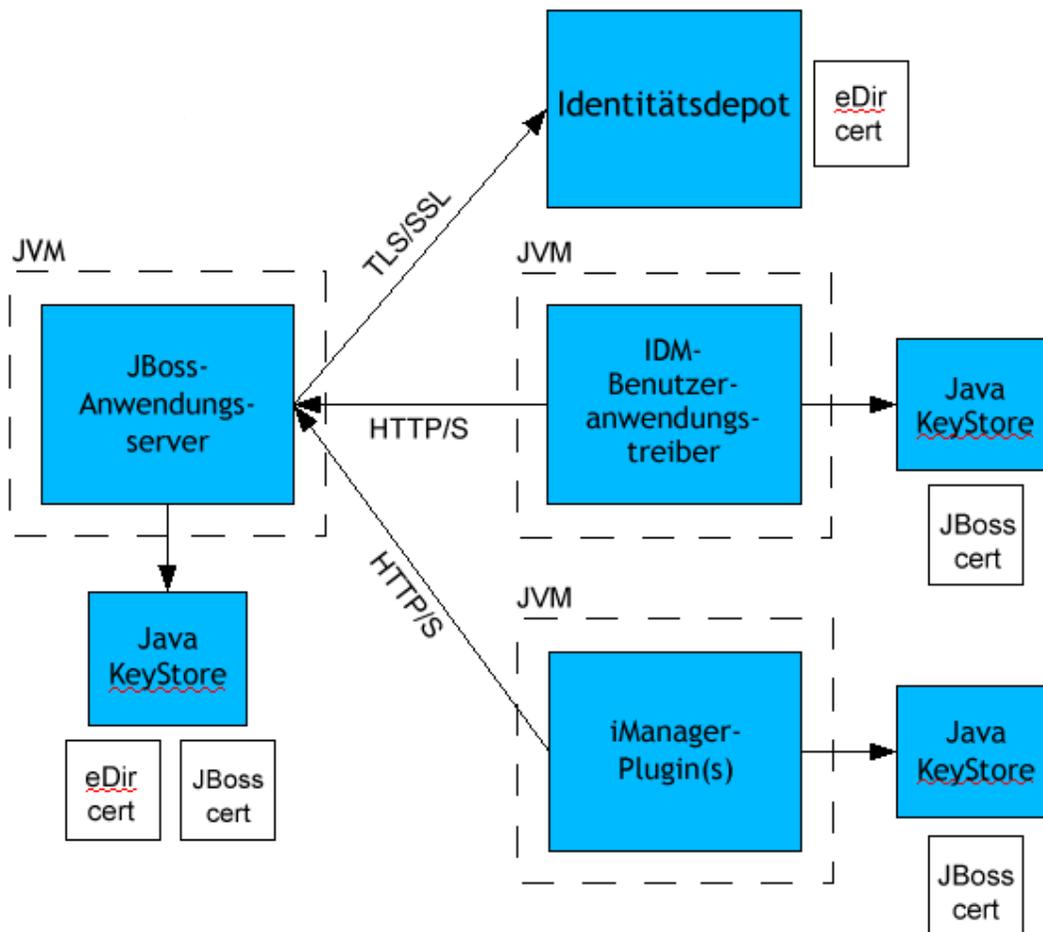
Wenn es erforderlich ist, „Marketing“ und „Finance“ im Rahmen einer Installation einer Benutzeranwendung in denselben Bereich zu stellen, kann dies auf zwei Arten geschehen. Eine Möglichkeit besteht darin, in der Hierarchie oberhalb der beiden gleichgeordneten Knoten ein neues Containerobjekt (z. B. *ou=MarketingAndFinance*) einzufügen und dann auf den neuen Container als übergeordneten Bereich zu verweisen. Eine andere Möglichkeit besteht darin, eine gefilterte Reproduktion (eine spezielle Art der eDirectory-Baumstruktur) zu erstellen, die die benötigten Teile der Original-ACME-Baumstruktur zusammensetzt, und die Benutzeranwendung auf den übergeordneten Container der Reproduktion zu verweisen. (Weitere Informationen zu gefilterten Reproduktionen finden Sie im Novell eDirectory-Administrationshandbuch.)

Wenden Sie sich an Ihre Novell-Vertretung, wenn Sie Fragen zu einem bestimmten Systemlayout haben.

## 2.2 Sicherheit

Der Übergang von der Vorproduktion zur Produktion ist in der Regel mit einer Verstärkung der Sicherheit des Systems verbunden. In der Sandkastenumgebung haben Sie möglicherweise ein reguläres HTTP für die Verbindung von Benutzeranwendungstreiber und JBoss verwendet oder (als vorübergehende Maßnahme) ein selbstsigniertes Zertifikat für die Kommunikation zwischen Treiber und Anwendungsserver. Bei der Produktion sollten Sie sichere Verbindungen mit Serverauthentifizierung verwenden, die auf dem Verisign-Zertifikat (oder dem Zertifikat eines anderen vertrauenswürdigen Anbieters) basiert.

Es ist typisch, dass X.509-Zertifikate an mehreren Stellen in der Identity Manager-Benutzeranwendungsumgebung verwendet werden (siehe nachfolgendes Schema).



Die Kommunikation zwischen der Benutzeranwendung und dem Identitätsdepot ist sicher und verwendet standardmäßig Transport Layer Security (Transportschichtssicherheit). Bei der Installation wird das Identitätsdepot-Zertifikat (eDirectory) automatisch im JBoss-Keystore installiert. Sofern nicht anders angegeben, platziert das Benutzeranwendungs-Installationsprogramm eine Kopie des eDirectory-Zertifikats im Standardspeicher *cacerts* der JRE.

Wie im Schema dargestellt, muss sich das Serverzertifikat an verschiedenen Stellen befinden, damit eine sichere Kommunikation gewährleistet wird. Abhängig davon, ob Sie ein selbstsigniertes Zertifikat an den verschiedenen Positionen des Diagramms, an denen das Kästchen *JBoss cert* angezeigt wird, verwenden oder ob Sie stattdessen ein von einer vertrauenswürdigen Zertifizierungsstelle (CA, certificate authority) wie Verisign ausgestelltes Zertifikat verwenden möchten, können bei der Einrichtung mehrere Schritte erforderlich sein.

### Selbstsignierte Zertifikate

Bei der Verwendung eines Zertifikats von einem bekannten, vertrauenswürdigen Herausgeber (z. B. Verisign) sind in der Regel keine besonderen Konfigurationsschritte erforderlich. Wenn Sie

allerdings beabsichtigen, ein selbstsigniertes Zertifikat zu erstellen und zu verwenden, müssen folgende Schritte ausgeführt werden:

- 1 Erstellen Sie einen Keystore mit einem selbstsignierten Zertifikat. Verwenden Sie hierzu eine Befehlszeilsyntax ähnlich wie im folgenden Beispiel:

```
keytool -genkey -alias tomcat -keyalg RSA -storepass changeit -
keystore jboss.jks -dname
"cn=JBoss,ou=exteNd,o=Novell,l=Waltham,s=MA,c=US" -keypass
changeit
```

Beachten Sie, dass Sie zusammen mit dem Zertifikat auch die Datei „jboss.jks“ erstellen.

- 2 Kopieren Sie die Keystore-Datei (jboss.jks) in das Verzeichnis der JBoss-Benutzeranwendung, z. B.:

```
cp jboss.jks ~/jboss-4.0.2/server/spitfire/conf
```

### Aktivierung von SSL in JBoss

Zur Aktivierung von SSL in JBoss, suchen Sie die Datei *jbossweb-tomcat55.sar* unter *[IDM]/jboss/server/IDM/deploy/*. Öffnen Sie dort die Datei *server.xml* in einem Texteditor. Aktivieren Sie SSL, indem Sie die Kommentarzeichen entfernen oder einen Abschnitt wie diesen hinzufügen:

```
<Connector port="8443" address="{jboss.bind.address}"
  maxThreads="100" strategy="ms" maxHttpHeaderSize="8192"
  emptySessionPath="true"
  scheme="https" secure="true" clientAuth="false"
  keystoreFile="{jboss.server.home.dir}/spitfire/conf/jboss.jks"
  keystorePass="changeit" sslProtocol = "TLS" />
```

### Aktivierung der SOAP-Sicherheit

Öffnen Sie die Datei *web.xml* aus der Web-Archivdatei *IDM.war* in einem Texteditor. Entfernen Sie am Ende der Datei die Kommentarzeichen des folgenden Abschnitts:

```
<security-constraint>
  <web-resource-collection>
    <web-resource-name>IDMProv</web-resource-name>
    <url-pattern>/*</url-pattern>
    <http-method>POST</http-method>
    <http-method>GET</http-method>
    <description>IDM Provisioning Edition</description>
  </web-resource-collection>
  <user-data-constraint>
    <transport-guarantee>CONFIDENTIAL</transport guarantee>
  </user-data-constraint>
</security-constraint>
```

Speichern Sie die Datei und das Archiv. Starten Sie JBoss neu.

## 2.2.1 Beiderseitige Authentifizierung

Die Identity Manager-Benutzeranwendung unterstützt herkömmliche Szenarios für die *Serverauthentifizierung* (wie allgemein in https-Sitzungen mit *sicheren Websites* im Internet verwendet), umfasst allerdings zunächst keine bidirektionale zertifikatbasierte Authentifizierung. Diese Funktionalität kann jedoch mit Novell iChain hinzugefügt werden. Wenn es beispielsweise in Ihrer Organisation erforderlich ist, dass die Anmeldung von Benutzern über ein Benutzerzertifikat erfolgen kann, könnten Sie dies umsetzen, indem Sie iChain in Ihrer Umgebung hinzufügen.

Weitere Informationen können Sie bei Ihrer Novell-Vertretung erfragen.

## 2.3 Leistungsoptimierung

Die Leistungsoptimierung ist ein komplexes Thema. Die Identity Manager-Benutzeranwendung beruht auf verschiedenen Technologien mit vielen Interaktionen. Es ist daher nicht möglich, jedes einzelne Konfigurationsszenario oder Benutzerinteraktionsszenario vorherzusehen, das zu einer unzulänglichen Funktionsweise führen könnte. Die Leistung einiger Subsysteme kann jedoch durch Best Practices verbessert werden. Diese werden im Folgenden aufgeführt.

### 2.3.1 Protokollierung

Die Benutzeranwendung ermöglicht eine Protokollierung sowohl über Novell Audit als auch über das Open-Source-Framework Apache *log4j*. Die Protokollierung über Novell Audit ist in der Standardeinstellung deaktiviert. Die Datei- und Konsolenprotokollierung über *log4j* ist jedoch standardmäßig aktiviert.

---

**Hinweis:** In [Kapitel 5](#), „Einrichten der Protokollierung“, auf Seite 121 und [Kapitel 12](#), „Konfiguration der Protokollierung“, auf Seite 213 dieses Handbuchs wird beschrieben, welche Ereignistypen protokolliert werden und wie Sie die Protokollierung aktivieren und deaktivieren können.

---

Die *log4j*-Konfigurationseinstellungen sind in einer Datei namens *log4j.xml* unter `$IDMINSTALL/jboss/server/IDMProv/conf/` enthalten. Gegen Ende der Datei finden Sie den folgenden Eintrag:

```
<root>
  <priority value="INFO" />
  <appender-ref ref="CONSOLE" />
  <appender-ref ref="FILE" />
</root>
```

Wenn Sie `root` einen Wert zuweisen, wird sichergestellt, dass alle Appender-Einträge, denen kein Protokollierungsumfang speziell zugewiesen wurde, den Wert von `root` (in diesem Fall INFO) übernehmen. Wenn dem FILE-Appender z. B. standardmäßig kein Wert für den Protokollierungsumfang zugewiesen ist, übernimmt er die Einstellung von „root“.

Die von *log4j* verwendeten möglichen Protokollierungsumfänge sind DEBUG, INFO, WARN, ERROR und FATAL gemäß der Definition in der Klasse `org.apache.log4j.Level`. Die Nichtbeachtung der korrekten Verwendung dieser Einstellungen kann zu Leistungseinbußen führen.

Es wird empfohlen, INFO oder DEBUG nur bei der Behebung eines bestimmten Problems zu verwenden.

Bei jedem „root“-Appender mit einem zugewiesenen Protokollierungsumfang sollte dieser ERROR, WARN oder FATAL sein, es sei denn (wie soeben ausgeführt), es wird eine Fehlersuche durchgeführt.

Die Leistungseinbußen bei hohem Protokollierungsumfang hängen weniger mit der Ausführlichkeit der Meldungen als vielmehr mit der einfachen Tatsache zusammen, dass bei der Konsolen- und Dateiprotokollierung in *log4j* synchrone Schreibvorgänge stattfinden. Es ist die Klasse *AsyncAppender* verfügbar, allerdings wird durch ihre Verwendung keine bessere Leistung gewährleistet. Die Probleme (die bekannt sind und durch Apache *log4j*, nicht aber durch Identity Manager hervorgerufen werden) sind unter <http://logging.apache.org/log4j/docs/api-1.2.8/org/apache/log4j/performance/Logging.html> dargelegt.

Die Standardeinstellung INFO in der Protokoll-Konfigurationsdatei (oben) reicht für die meisten Umgebungen aus. Wenn die Leistungsfähigkeit allerdings von besonderer Wichtigkeit ist, empfiehlt es sich, den oben stehenden Eintrag in *log4j.xml* wie folgt zu ändern:

```
<root>
  <priority value="ERROR"/>
  <appender-ref ref="FILE"/>
</root>
```

Anders ausgedrückt, entfernen Sie CONSOLE und setzen Sie den Protokollierungsumfang auf ERROR. Für eine vollständig getestete/von Fehlern befreite Produktionseinrichtung ist es nicht notwendig, mit dem INFO-Umfang zu protokollieren oder die CONSOLE-Protokollierung zu aktivieren. Diese Deaktivierung wirkt sich meist erheblich auf die Leistung aus.

Weitere Informationen zu *log4j* finden Sie in der Dokumentation, die unter <http://logging.apache.org/log4j/docs> zur Verfügung steht.

Weitere Informationen zur Verwendung von Novell Audit mit Identity Manager finden Sie im Novell Identity Manager-Administrationshandbuch.

## 2.3.2 Identitätsdepot

LDAP-Abfragen können zu einem Engpass in einer stark ausgelasteten Verzeichnisserver-Umgebung führen. Damit auch bei einer großen Anzahl von Objekten ein hoher Leistungsgrad aufrechterhalten werden kann, zeichnet Novell eDirectory (die Basis des Identitätsdepots in Identity Manager) fortlaufend angeforderte Informationen auf und speichert diese in Indizes. Dadurch werden bei einer komplexen Abfrage über Objekte mit indizierten Attributen die Abfrageergebnisse viel schneller ausgegeben.

Im Lieferzustand sind folgende Attribute von eDirectory bereits indiziert:

```
Aliased Object Name
cn
dc
Equivalent to Me
extensionInfo
Given Name
GUID
ldapAttributeList
ldapClassList
```

Member  
NLS: Common Certificate  
Obituary  
Reference  
Revision  
Surname  
uniqueID  
uniqueID\_SS

Wenn Sie Identity Manager installieren, wird das Standardverzeichnisschema mit neuen Objektklassentypen und neuen Attributen, die die Benutzeranwendung betreffen, erweitert. Spezifische Attribute der Benutzeranwendung werden (standardmäßig) nicht indiziert. Zur Erzielung einer besseren Leistung ist es nützlich, einige dieser Attribute (und eventuell auch einige der herkömmlichen LDAP-Attribute) zu indizieren. Dies empfiehlt sich besonders dann, wenn Ihr Benutzercontainer mehr als 5.000 Objekte enthält.

Man sollte nur die Attribute indizieren, die regelmäßig abgefragt werden. (Diese Attribute können je nach Produktionsumgebung sehr unterschiedlich sein.) Die einzige Möglichkeit, herauszufinden, welche Attribute häufig abgefragt werden, besteht darin, während der Laufzeit Prädikatstatistiken zu sammeln. (Dieser Erfassungsvorgang führt jedoch zu Leistungseinbußen.)

Das Verfahren zum Erfassen von Prädikatstatistiken wird im eDirectory-Administrationshandbuch ausführlicher beschrieben. Die Indizierung wird ebenfalls dort ausführlicher behandelt. In der Regel müssen Sie folgende Schritte ausführen:

- Verwenden Sie Console One zur Aktivierung der Erfassung von Prädikatstatistiken für die gewünschten Attribute.
- Setzen Sie das System unter Last.
- Deaktivieren Sie die Statistikerfassung und analysieren Sie die Ergebnisse.
- Erstellen Sie für jeden Attributtyp, für den es sinnvoll sein könnte, einen Index.

Wenn Sie bereits wissen, welche Attribute Sie indizieren möchten, ist die Verwendung von Console One nicht erforderlich. In iManager können Sie Indizes über „eDirectory-Wartung > Indizes“ erstellen und verwalten. Wenn Sie z. B. wissen, dass die Benutzer Ihres Organigramms sehr wahrscheinlich Suchvorgänge basierend auf dem Attribut *isManager* ausführen, können Sie versuchen, dieses Attribut zu indizieren und überprüfen, ob die Leistung dadurch positiv beeinflusst wird.

---

**Hinweis:** Als Best Practice wird empfohlen, zumindest die Attribute *manager* und *isManager* zu indizieren.

---

Das Indizieren von Attributen und die Auswirkungen auf die Leistung werden im Kapitel „Tuning eDirectory“ (Optimierung von eDirectory) in *Novell's Guide to Troubleshooting eDirectory* von Peter Kuo und Jim Henderson (QUE Books, ISBN 0-7897-3146-0) eingehender behandelt.

Weitere Informationen finden Sie außerdem im Kapitel über die Wartung von Novell eDirectory (das Ratschläge zur Leistungsoptimierung umfasst) im eDirectory-Administrationshandbuch.

### 2.3.3 JVM

Die Größe des Heap-Speichers, der der Java Virtual Machine zugeordnet ist, kann die Leistung beeinflussen. Wenn Sie zu niedrige oder zu hohe Mindest- oder Maximalwerte für den Speicher

festlegen („zu hoch“ im Sinne von höher als der physische Arbeitsspeicher des Computers) besteht die Möglichkeit, dass übermäßig viele Daten in die Auslagerungsdatei verschoben werden.

Sie können die maximale JVM-Größe für den JBoss-Server festlegen, indem Sie die Datei `run.conf` oder `run.bat` (die erstere für Linux, die letztere für Windows) unter `[IDM] / jboss/bin/` in einem Texteditor bearbeiten. Erhöhen Sie „-Xmx“ von `128m` auf `512m` oder möglicherweise höher. Experimentieren Sie ein wenig, um die optimale Einstellung für Ihre spezielle Umgebung zu ermitteln.

---

**Hinweis:** Tipps für die Leistungsoptimierung von JBoss und Tomcat finden Sie unter <http://wiki.jboss.org/wiki/Wiki.jsp?page=JBossASTuningSliming> (<http://wiki.jboss.org/wiki/Wiki.jsp?page=JBossASTuningSliming>).

---

## 2.3.4 Sitzungszeitüberschreitung

Der Wert für die Sitzungszeitüberschreitung (der Zeitraum, in dem ein Benutzer eine Seite in seinem Webbrowser unbeaufsichtigt lassen kann, bevor der Server eine Warnmeldung für die Sitzungszeitüberschreitung erzeugt) kann in der Datei `web.xml` im Archiv `IDM.war` geändert werden. Dieser Wert sollte so angepasst werden, dass er optimal auf die Serverumgebung und die bestehende Auslastung abgestimmt ist. In der Regel empfiehlt es sich, den Wert für die Sitzungszeitüberschreitung so niedrig wie möglich zu wählen. Wenn es die geschäftlichen Erfordernisse erlauben, sollte der Wert auf 5 Minuten eingestellt werden, denn dies würde dem Server ermöglichen, ungenutzte Ressourcen doppelt so schnell freizugeben als bei einem Wert von 10 Minuten. Dadurch wird die Webanwendung schneller und skalierbarer.

Folgende Aspekte sollten Sie bei der Anpassung des Werts für die Sitzungszeitüberschreitung beachten:

- Ein höherer Wert für die Sitzungszeitüberschreitung kann unter Umständen dazu führen, dass der JBoss-Server über unzureichenden Arbeitsspeicher verfügt, wenn sich mehrere Benutzer innerhalb eines kurzen Zeitraums anmelden. Dies gilt für alle Anwendungsserver mit zu vielen geöffneten Sitzungen.
- Wenn sich ein Benutzer bei der Benutzeranwendung anmeldet, wird für den Benutzer eine LDAP-Verbindung erstellt und an die entsprechende Sitzung gebunden. Das bedeutet, je mehr Sitzungen offen sind, desto höher ist die Anzahl der bestehenden LDAP-Verbindungen. Je höher der Wert für die Sitzungszeitüberschreitung gewählt wird, desto länger werden diese Verbindungen aufrechterhalten. Zu viele offene Verbindungen zum LDAP-Server (selbst wenn diese ungenutzt sind) können eine Verminderung der Systemleistung mit sich bringen.
- Wenn auf dem Server `OutOfMemoryErrors` auftreten und die Tuning-Parameter für den JVM-Heap und die Speicherbereinigung bereits optimal an die Serverumgebung und die bestehende Auslastung angepasst wurden, sollte das Herabsetzen des Werts für die Sitzungszeitüberschreitung in Erwägung gezogen werden.

Um den Wert für die Sitzungszeitüberschreitung anzupassen, öffnen Sie das Archiv `IDM.war` und bearbeiten Sie in der Datei `web.xml` den folgenden Abschnitt (insbesondere den numerischen Wert, hier 20 für 20 Minuten, den Standardwert):

```
<session-config>
  <session-timeout>20</session-timeout>
</session-config>
```

Speichern Sie anschließend die Datei und das Archiv und starten Sie den Server neu.

---

**Hinweis:** Die manuelle Bearbeitung von Webarchivdateien sollte nur von einer Person vorgenommen werden, die über Erfahrung bei der Entwicklung und Implementierung der Java-Webanwendung verfügt.

---

## 2.4 Cluster-Gruppierung

Wenn Sie die Benutzeranwendung in einer Cluster-Umgebung verwenden, müssen Sie drei Dinge beachten:

- Die JBoss-Clusterkonfiguration (siehe [Abschnitt 2.4.1, „JBoss-Cluster-Gruppierung“](#), auf [Seite 47](#))
- Die Caching-Konfiguration der Benutzeranwendung (siehe [Abschnitt 2.4.3, „Konfigurieren des Cluster-Gruppen-Cachings der Benutzeranwendung“](#), auf [Seite 52](#))
- Die Konfiguration der Workflow-Engine (siehe [Abschnitt 2.4.4, „Konfigurieren der Workflows für die Cluster-Gruppierung“](#), auf [Seite 53](#))

### 2.4.1 JBoss-Cluster-Gruppierung

Ein Cluster ist eine Sammlung von Anwendungsserverknoten, die mehrere Services bereitstellen. Ein Cluster hat den Zweck, die Leistung und die Zuverlässigkeit von Anwendungen zu steigern. In der Regel bietet ein Cluster Unternehmensanwendungen drei wesentliche Vorteile:

- Hochverfügbarkeit
- Skalierbarkeit (mehr Kapazität)
- Lastausgleich

Hochverfügbarkeit bedeutet, dass eine Anwendung in der eingesetzten Zeit zu einem hohen Prozentsatz zuverlässig und verfügbar ist. Cluster liefern eine hohe Verfügbarkeit, weil auf allen Knoten dieselbe Anwendung ausgeführt wird. Wenn bei einem Knoten eine Fehlfunktion auftritt, wird die Anwendung weiterhin auf den anderen Knoten ausgeführt. Die Identity Manager-Benutzeranwendung profitiert von einer höheren Verfügbarkeit, wenn sie in einem Cluster ausgeführt wird. Die Identity Manager-Benutzeranwendung unterstützt jedoch keine Reproduktion von HTTP-Sitzungen. Dies bedeutet, dass die Sitzungsinformationen verloren gehen, wenn bei einem Knoten, auf dem eine Sitzung läuft, eine Fehlfunktion auftritt.

Der Lastausgleich ist der Vorgang der Verteilung der Arbeitslast auf die Mitglieder eines Clusters. Das Ziel des Lastausgleichs ist eine Steigerung der Leistung. Ein Lastausgleich kann auf unterschiedliche Weise erzielt werden (z. B. DNS-Round-Robin, Hardware-Lastausgleich). Unter <http://www.onjava.com/pub/a/onjava/2001/09/26/load.html> (<http://www.onjava.com/pub/a/onjava/2001/09/26/load.html>) werden verschiedene Methoden für den Lastausgleich erörtert. Unabhängig von der gewählten Methode sollten Sie den Lastausgleich in Ihre Clusterkonfiguration einbinden.

#### JBoss-Cluster-Gruppen

JBoss-Cluster basieren auf dem Kommunikationsmodul JGroups. JGroups wird zusammen mit JBoss installiert (das Modul kann auch ohne JBoss verwendet werden). JGroups bietet Kommunikation innerhalb von Gruppen, die einen Eigennamen, eine Multicast-Adresse und einen Multicast-Port gemeinsam nutzen.

Bei der Installation eines geclusterten JBoss-Servers definiert JBoss zwei verschiedene JGroups-Gruppen, die zur Verwaltung des Clusters verwendet werden können. Eine Gruppe heißt *DefaultPartition* und ist in `/deploy/cluster-service.xml` definiert. Diese Cluster-Gruppe wird von JBoss zum Bereitstellen von Core-Services im Zusammenhang mit der Cluster-Gruppierung verwendet. JBoss definiert außerdem eine zweite Cluster-Gruppe namens *Tomcat-Cluster*. Diese Cluster-Gruppe ist in `/deploy/tc-cluster-service.xml` definiert und ermöglicht dem Tomcat-Server, der in JBoss ausgeführt wird, die Sitzungsreproduktion.

Die Identity Manager-Benutzeranwendung verwendet eine dritte Cluster-Gruppe. Diese Cluster-Gruppe nutzt einen UUID-Namen, um das Risiko von Konflikten mit anderen Cluster-Gruppen, die Benutzer möglicherweise zu ihren Servern hinzufügen, zu minimieren. Die Cluster-Gruppe heißt standardmäßig `c373e901aba5e8ee9966444553544200`. Dieses Cluster wird nicht durch eine JBoss-Service-datei konfiguriert. Stattdessen befinden sich die Konfigurationseinstellungen in dem Verzeichnis und können anhand der Administrationsfunktionen der Benutzeranwendung konfiguriert werden. Wenn Sie mit dem JGroups- und JBoss-Clustering vertraut sind, können Sie die Clusterkonfiguration der Benutzeranwendung anhand dieser Schnittstelle anpassen. Änderungen der Clusterkonfiguration werden erst nach einem Neustart des entsprechenden Serverknotens wirksam.

Die Benutzeranwendungs-Cluster-Gruppe wird ausschließlich für die Koordination der Benutzeranwendungs-Cache-Speicher in einer geclusterten Umgebung verwendet. Sie ist unabhängig von den beiden JBoss-Cluster-Gruppen und es findet keinerlei Interaktion statt. Die Benutzeranwendungs-Cluster-Gruppe und die beiden JBoss-Gruppen verwenden standardmäßig unterschiedliche Gruppennamen, Multicast-Adressen und Multicast-Ports, sodass keine Neukonfiguration erforderlich ist.

Die Cluster-Gruppen-Einstellungen der Benutzeranwendung werden von jeder Identity Manager 3-Anwendung mit derselben Verzeichniskonfiguration gemeinsam genutzt. Die Option der lokalen Einstellung in der Administrationsoberfläche der Benutzeranwendung ermöglicht dem Administrator, einen Knoten aus einem Cluster zu entfernen oder die Zugehörigkeit der Server zu einem Cluster zu ändern. Sie können die Cluster-Gruppierung z. B. zunächst global deaktivieren und dann lokal für einen Teil der Server mit derselben Verzeichniskonfiguration aktivieren.

## Application Farming

JBoss ermöglicht Ihnen die clusterübergreifende Implementierung im laufenden Betrieb („hot-deploy“), indem ein Anwendungs-EAR, -WAR oder -JAR in das Farm-Verzeichnis einer geclusterten JBoss-Instanz kopiert wird. Die Implementierung im laufenden Betrieb auf einem Computer führt dazu, dass diese Komponente automatisch auf allen Instanzen innerhalb des Clusters verteilt wird, während das Cluster ausgeführt wird.

Diese Form der Anwendungsimplementierung wird für die Version von JBoss Application Server (4.0.2), die zu dem Zeitpunkt, als dieses Dokument geschrieben wurde, im Benutzeranwendungsinstallationsprogramm enthalten war, nicht empfohlen, da noch ungelöste Probleme bestehen. Es werden jedoch die grundlegenden Schritte aufgeführt (siehe [„Implementieren der Benutzeranwendung mittels JBoss-Farming“ auf Seite 51](#)), die für eine erfolgreiche Implementierung der Benutzeranwendung unter Verwendung der JBoss-Farming-Technologie auszuführen sind, da nach der Veröffentlichung dieses Dokuments mit einer Verbesserung der Technologie gerechnet werden kann.

## MySQL-Datenbank

Das Installationsprogramm der Benutzeranwendung installiert entweder den MySQL-Datenbankmanager und erstellt eine Datenbank, die mit der Benutzeranwendung verwendet werden kann, oder es verwendet eine vorhandene Oracle-, Microsoft SQL Server- oder MySQL-Datenbank. Die Datenbank ist für die Datenpersistenz verantwortlich. Alle Knoten im JBoss-Cluster müssen auf dieselbe Datenbankinstanz zugreifen. Die Benutzeranwendung verwendet Standard-JDBC-Aufrufe für den Zugriff auf und die Aktualisierung der Datenbank. Die Benutzeranwendung verwendet eine an den JNDI-Baum gebundene JDBC-Datenquelle zum Herstellen einer Verbindung mit der Datenbank. Wenn Sie mit dem Installationsprogramm der Benutzeranwendung ein JBoss-Cluster erstellen, wird die Datenquelle für Sie installiert. Wenn Sie das JBoss-Cluster manuell einrichten möchten, müssen Sie die Datenquellendatei (IDM-ds.xml) auf allen Knoten in Ihrem Cluster in das Implementierungsverzeichnis kopieren. Wenn Sie MySQL verwenden, müssen Sie auch den MySQL-JDBC-Treiber (*mysql-connector-java-3.1.10-utf8-clob-fix-bin.jar*), der sich im JBoss-Verzeichnis `/server/IDM/lib` befindet, in das JBoss-Verzeichnis `server/IDM/lib` kopieren.

## Protokollierung

Um die Protokollierung für Cluster zu aktivieren, müssen Sie die Konfigurationsdatei „log4j.xml“ im Verzeichnis `\conf` für die JBoss-Serverkonfiguration (z. B. `\server\IDM\conf`) bearbeiten, indem Sie am Ende der Datei bei einem ähnlichen Abschnitt wie diesem die Kommentarzeichen entfernen:

```
<!-- Clustering logging
-->
- <!--
  Uncomment the following to redirect the org.jgroups and
  org.jboss.ha categories to a cluster.log file.
  <appender name="CLUSTER"
class="org.jboss.logging.appender.RollingFileAppender">
  <errorHandler
class="org.jboss.logging.util.OnlyOnceErrorHandler"/>
  <param name="File" value="{jboss.server.home.dir}/log
cluster.log"/>
  <param name="Append" value="false"/>
  <param name="MaxFileSize" value="500KB"/>
  <param name="MaxBackupIndex" value="1"/>
  <layout class="org.apache.log4j.PatternLayout">
    <param name="ConversionPattern" value="%d %-5p [%c] %m%n"/>
  </layout>
</appender>
<category name="org.jgroups">
  <priority value="DEBUG" />
  <appender-ref ref="CLUSTER"/>
</category>
<category name="org.jboss.ha">
  <priority value="DEBUG" />
  <appender-ref ref="CLUSTER"/>
</category>
-->
```

Die Datei *cluster.log* wird im *log*-Verzeichnis für die JBoss-Serverkonfiguration gespeichert (z. B. `\server\IDM\log`).

## 2.4.2 Installieren der Benutzeranwendung auf einem JBoss-Cluster

Es wird empfohlen, die Benutzeranwendung mithilfe ihres Installationsprogramms auf jedem Knoten in einem Cluster zu installieren. Obwohl es nicht empfohlen wird, die Benutzeranwendung in einem Cluster mittels JBoss-Farming zu implementieren, beinhaltet dieser Abschnitt alternativ eine entsprechende Anleitung.

### Verwendung des Installationsprogramms der Benutzeranwendung auf jedem Knoten im Cluster

Im Lieferumfang von JBoss sind drei einsatzbereite Serverkonfigurationen enthalten: *minimal*, *default* und *all*. Die Cluster-Gruppierung ist nur in der Konfiguration *all* aktiviert. In der Datei `cluster-service.xml` im Ordner `/deploy` wird die Konfiguration der standardmäßigen Cluster-Partition beschrieben. Wenn Sie bei der Installation der Benutzeranwendung angeben, dass die Anwendung in ein Cluster installiert werden soll, kopiert das Installationsprogramm die Konfiguration *all*, benennt die Kopie *IDM* (Standard - eine Änderung des Namens ist möglich) und installiert die Benutzeranwendung in dieser Konfiguration.

So installieren Sie die Benutzeranwendung mit dem Installationsprogramm der Benutzeranwendung auf jedem Knoten in einem Cluster:

- 1 Installieren Sie die Benutzeranwendung vollständig (MySQL, JBoss und die Benutzeranwendung) auf dem ersten JBoss-Knoten. Informationen zur Verwendung des Installationsprogramms der Benutzeranwendung finden Sie in der *Identity Manager 3-Installationsanleitung*.
  - Wenn Sie MySQL als Datenbank für die Benutzeranwendung verwenden, erstellt das Installationsprogramm der Benutzeranwendung eine neue Installation von MySQL. Notieren Sie sich das von Ihnen festgelegte Kennwort für den „root“-Benutzer von MySQL. Sie benötigen diese Informationen bei der Installation der Benutzeranwendung auf den anderen Knoten im Cluster.
  - Wählen Sie im Installationsprogramm für die IDM-Konfiguration die Option für das vollständige Clustering („clustering (all)“).
  - Wählen Sie entsprechend Ihrer Umgebung weitere Installationsoptionen aus.
- 2 Wenn MySQL noch nicht läuft, starten Sie MySQL über die Datei `start-mysql.bat` im Verzeichnis `/IDM/mysql`.

---

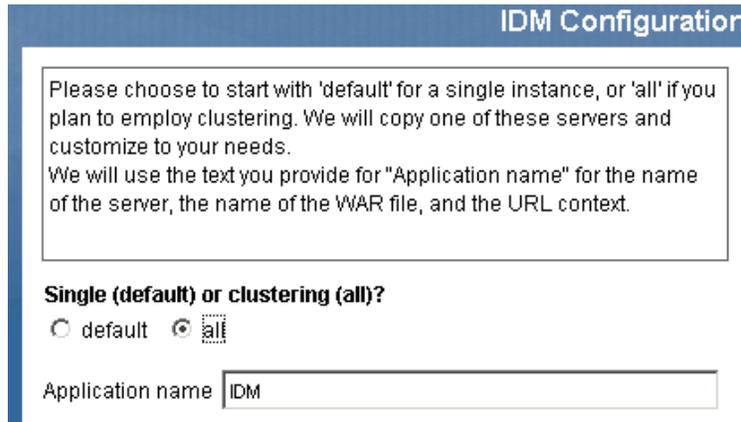
**Hinweis:** Unter Linux können Sie mithilfe des folgenden Shell-Befehls ermitteln, ob der MySQL-Daemon ausgeführt wird:

---

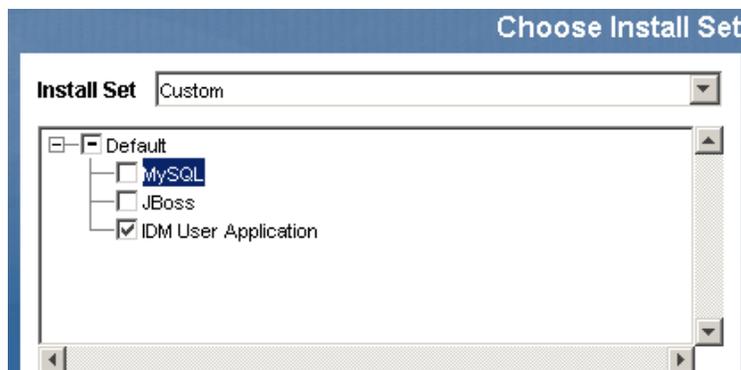
```
ps -A | grep mysqld
```

Wenn dieser Befehl mehrere Zeilen zurückgibt, die auf `mysqld` enden, ist der Daemon aktiv.

- 3 Starten Sie JBoss und die Benutzeranwendung über die Datei *start-jboss.bat* (Windows) oder *start-jboss.sh* (Linux) im Verzeichnis *IDM*.



- 4 Führen Sie auf jedem Knoten des JBoss-Clusters eine benutzerdefinierte Installation der Benutzeranwendung durch.
- Wählen Sie aus, dass nur die Benutzeranwendung installiert werden soll:



- Geben Sie die IP-Adresse oder den Hostnamen des Servers an, auf dem die Datenbank für die Benutzeranwendung installiert ist.
  - Geben Sie den Benutzernamen und das Passwort für die Datenbank der Benutzeranwendung an. Bei MySQL lautet der Benutzername `root` und das Passwort ist das von Ihnen in **Schritt 1** festgelegte Passwort.
  - Wählen Sie im Installationsprogramm für die IDM-Konfiguration die Option für das vollständige Clustering („clustering (all)“).
  - Wählen Sie entsprechend Ihrer Umgebung weitere Installationsoptionen aus.
- 5 Starten Sie jeden Knoten im JBoss-Cluster über die Datei *start-jboss.bat* (Windows) oder *start-jboss.sh* (Linux) im Verzeichnis *IDM*.

### Implementieren der Benutzeranwendung mittels JBoss-Farming

Verwenden Sie JBoss-Farming nicht mit der JBoss-Version 4.0.2 oder früher, da andernfalls Probleme auftreten könnten (siehe <http://jira.jboss.com/jira/browse/JBAS-1899> (<http://jira.jboss.com/jira/browse/JBAS-1899>)). Es wird empfohlen, dass Sie die Benutzeranwendung

mithilfe des Installationsprogramms der Benutzeranwendung auf jedem Knoten im Cluster installieren (siehe „[Verwendung des Installationsprogramms der Benutzeranwendung auf jedem Knoten im Cluster](#)“ auf Seite 50 in diesem Kapitel). Wenn Sie die Benutzeranwendung trotzdem mittels Farming in einem JBoss-Cluster mit JBoss 4.0.3 oder höher implementieren möchten, führen Sie die folgenden Schritte aus.

---

**Hinweis:** Diese Schritte sind nur für Kunden gedacht, die JBoss 4.0.3 auf eigene Gefahr und experimentell verwenden möchten. Die offiziell unterstützte Version ist 4.0.2.

---

So implementieren Sie die Benutzeranwendung mittels JBoss-Farming

- 1** Führen Sie eine benutzerdefinierte Installation der Benutzeranwendung auf einem der JBoss-Clusterknoten aus und wählen Sie die Benutzeranwendung und MySQL (falls Sie MySQL verwenden, andernfalls installieren Sie nur die Benutzeranwendung) für die Installation aus. Während der Installation können alle Cluster im Knoten ausgeführt werden. Der Knoten, auf dem Sie die Benutzeranwendung installieren, sollte jedoch der erste im Cluster gestartete Knoten sein.
- 2** Kopieren Sie die JDBC-Treiberdatei (bei der Verwendung von MySQL ist der JDBC-Treiber beispielsweise *mysql-connector-java-3.1.10-utf8-clob-fix-bin.jar*) im Verzeichnis `/server/IDM/lib` in das entsprechende Verzeichnis auf jedem Knoten im Cluster.
- 3** Kopieren Sie die Datei *cacerts* aus dem Verzeichnis `/lib/security` der JRE, die gemeinsam mit der Benutzeranwendung installiert wurde, in das JRE-Verzeichnis `/lib/security` jedes Knotens im Cluster.
- 4** Verschieben Sie die Datei *IDM.war* und die Datenursprungsdatei *IDM-ds.xml* aus dem `/deploy`-Verzeichnis im Serverkonfigurationsverzeichnis in das `/farm`-Verzeichnis im Serverkonfigurationsverzeichnis. Beachten Sie, dass Sie die Dateien verschieben und nicht kopieren müssen. Belassen Sie die Originale nicht im `/deploy`-Verzeichnis.
- 5** Starten Sie die Datenbank für die Benutzeranwendung (wenn Sie die mitgelieferte MySQL-Datenbank verwenden, starten Sie MySQL über die Datei *start-mysql.bat* im Verzeichnis `/IDM/mysql`).
- 6** Starten Sie JBoss und die Benutzeranwendung über die Datei *start-jboss.bat* (Windows) oder *start-jboss.sh* (Linux) im Verzeichnis *IDM* des Knotens, in dem Sie die Benutzeranwendung und die Datenbank der Benutzeranwendung installiert haben.
- 7** Starten Sie die anderen Knoten im Cluster.

### 2.4.3 Konfigurieren des Cluster-Gruppen-Cachings der Benutzeranwendung

Benutzer, die mit der JGroups- und der JBoss-Cluster-Gruppierung vertraut sind, können die Konfiguration des Cluster-Gruppen-Cachings über die Administrationsschnittstelle der Benutzeranwendung ändern (siehe [Abschnitt 13.3.5, „Cache-Einstellungen für Cluster“](#), auf Seite 226). Änderungen der Clusterkonfiguration werden erst nach einem Neustart des entsprechenden Serverknotens wirksam.

## 2.4.4 Konfigurieren der Workflows für die Cluster-Gruppierung

Die Cluster-Gruppierung der Workflow-Engine arbeitet unabhängig vom Cache-Framework der Benutzeranwendung. Sie müssen mehrere Schritte ausführen, um sicherzustellen, dass die Workflow-Engine in einer Cluster-Umgebung ordnungsgemäß funktioniert.

- Alle Server im Cluster müssen auf dieselbe Datenbank verweisen. Wenn Sie die Benutzeranwendung wie empfohlen (siehe „[Verwendung des Installationsprogramms der Benutzeranwendung auf jedem Knoten im Cluster](#)“ auf Seite 50) auf dem Cluster installieren, geschieht dies während des Installationsvorgangs durch die Angabe der IP-Adresse bzw. des Hostnamens des Servers, auf dem die Datenbank für die Benutzeranwendung installiert ist. Wenn Sie die Benutzeranwendung mittels Farming auf den Cluster-Knoten implementieren (siehe „[Implementieren der Benutzeranwendung mittels JBoss-Farming](#)“ auf Seite 51), geschieht dies durch das Verschieben der Datenquellendatei (IDM-ds.xml) vom /deploy-Verzeichnis in das /farm-Verzeichnis auf dem Knoten, auf dem die Benutzeranwendung als erstes installiert wurde. Dadurch wird die Datenquelle auf allen Knoten im Cluster implementiert.
- Jeder Server im Cluster muss mit einer eindeutigen Engine-ID gestartet werden. Dies erfolgt durch die Anpassung der Systemeigenschaft `com.novell.afw.wf.engine-id` beim Start des Servers. Wenn Sie z. B. JBoss starten und der Workflow-Engine für diesen Server die Engine-ID ENGINE1 zuweisen möchten, verwenden Sie folgenden Befehl:  

```
run.sh -Dcom.novell.afw.wf.engine-id=ENGINE1 (Linux)
```

```
run.bat -Dcom.novell.afw.wf.engine-id=ENGINE1 (Windows)
```

Sobald eine Instanz eines Workflow-Prozesses von einer auf einem bestimmten Server ausgeführten Workflow-Engine gestartet wird, kann sie nur auf diesem Server ausgeführt und beendet werden. Dadurch wird sichergestellt, dass der Workflow-Prozess sicher ausgeführt wird. Es wird jedoch kein Failover einer Prozessinstanz unterstützt. Wenn ein Server in einem Cluster abstürzt, wird die Prozessinstanz erst dann neu gestartet, wenn eine Engine mit derselben ID neu gestartet wird.

Wenn ein Servercomputer aufgrund von schwerwiegenden Hardware- oder Softwarefehlfunktionen nicht neu gestartet werden kann, können Sie den Anwendungsserver auf einem neuen Computer starten, indem Sie dieselbe Workflow-Engine-ID wie für den Computer mit dem nicht behebbaren Fehler verwenden. Da die Engine-ID ein logischer Name ist und nicht direkt dem physischen Computer zugeordnet ist, auf dem die Engine ausgeführt wurde, wird die unterbrochene Prozessinstanz auf dem neuen Computer erfolgreich abgeschlossen.

Prozessinstanzen gehören zu der Engine, die den Prozess gestartet hat. Ein Benutzer kann sich jedoch auf jeder Benutzeranwendung in einem Cluster anmelden und sich Prozessdetails anzeigen lassen, Prozesse zurückziehen oder ihm zugewiesene Aufgaben erledigen. Zurückgezogene Prozesse oder abgeschlossene Aufgaben auf einer Engine, zu der der entsprechende Prozess nicht gehört, erhalten den Status „Ausstehend“ und werden wieder ausgeführt, wenn sie von der zugehörigen Engine gefunden werden.



# Konfigurieren der Benutzeranwendungsumgebung



In diesen Kapiteln wird die Konfigurierung der verschiedenen Aspekte der Identity Manager-Benutzeranwendungsumgebung beschrieben, damit Sie diese auf Ihre Erfordernisse anpassen können.

- [Kapitel 3, „Konfigurieren des Benutzeranwendungstreibers“](#), auf Seite 57
- [Kapitel 4, „Konfigurieren der Verzeichnisabstraktionsschicht“](#), auf Seite 75
- [Kapitel 5, „Einrichten der Protokollierung“](#), auf Seite 121



# Konfigurieren des Benutzeranwendungstreibers

# 3

## 3.1 Allgemeines zum Benutzeranwendungstreiber

Der Benutzeranwendungstreiber startet Bereitstellungs-Workflows und meldet Änderungen im Identitätsdepot an die Benutzeranwendung (z. B. bei Änderungen an der Verzeichnisabstraktionsschicht über den Designer für Identity Manager). In diesem Treiber wird nur der Abonnementkanal verwendet. Der Treiber verarbeitet Meldungen vom Identitätsdepot an die Benutzeranwendung, die auf einem Anwendungsserver ausgeführt wird. Das Identitätsdepot wird über Ereignisse, die in der Benutzeranwendung auftreten, informiert, diese Ereignisse werden jedoch nicht durch den Herausgeberkanal des Benutzeranwendungstreibers geleitet.

Wenn der Anwendungsserver gestartet wird, baut der Treiber eine Sitzung mit dem Anwendungsserver auf. Der Treiber sendet eine Nachricht an die auf dem Anwendungsserver ausgeführte Benutzeranwendung (z. B. zum Abrufen eines neuen Satzes virtueller Verzeichnisdefinitionen).

Zu den Quellkomponenten des Treibers gehören:

- `ComposerDriverShim.jar` – Das Treiberschnittstellenmodul des Composer. Es ist unter Windows im *lib*-Verzeichnis `\Novell\NDS\lib` bzw. unter Linux im *classes*-Verzeichnis `/usr/lib/dirxml/classes` installiert.
- `srvprvUAD.jar` – Das Treiberschnittstellenmodul der Anwendung. Es ist unter Windows im *lib*-Verzeichnis `\Novell\NDS\lib` bzw. unter Linux im *classes*-Verzeichnis `/usr/lib/dirxml/classes` installiert.
- `UserApplicationDriver.xml` – Eine Datei, die die vorkonfigurierten Daten zum Einrichten des neuen Treibers enthält. Sie ist unter Windows im *DirXML.Drivers* Verzeichnis `\Tomcat\webapps\nps\DirXML.Drivers` bzw. unter Linux im Verzeichnis `/usr/lib/dirxml/rules/DirXML.Drivers` installiert.

Die Komponenten des Benutzeranwendungstreibers werden bei der Installation von Identity Manager 3 installiert. Bevor Sie die Identity Manager 3-Benutzeranwendung ausführen können, müssen Sie den Benutzeranwendungstreiber zu einem neuen oder vorhandenen Treibersatz hinzufügen und den Treiber aktivieren.

Je nach Arbeitsumgebung ist eine geringfügige Konfiguration des Benutzeranwendungstreibers erforderlich. Es besteht aber auch die Möglichkeit, dass Sie z. B. einen komplexen Satz an Geschäftsregeln in den Treiberrichtlinien implementieren. Der Benutzeranwendungstreiber verfügt über dieselben flexiblen Mechanismen für die Datensynchronisierung wie andere Identity Manager-Treiber.

In diesem Kapitel wird beschrieben, wie ein Benutzeranwendungstreiber erstellt, konfiguriert und gestartet werden kann. Außerdem erfahren Sie, wie Sie einen Treiber konfigurieren können, damit

bei einem bestimmten Ereignis im Identitätsdepot automatisch ein Workflow ausgelöst wird. Das Kapitel ist in drei Abschnitte unterteilt:

- [Abschnitt 3.2, „Erstellen des Benutzeranwendungstreibers“](#), auf Seite 58
- [Abschnitt 3.3, „Starten des Benutzeranwendungstreibers“](#), auf Seite 64
- [Abschnitt 3.4, „Einrichten von automatisch startenden Workflows“](#), auf Seite 65

## 3.2 Erstellen des Benutzeranwendungstreibers

So erstellen Sie den Treiber:

- 1 Melden Sie sich bei der Instanz von iManager an, die Ihr Identitätsdepot verwaltet.
- 2 Öffnen Sie im Navigationsrahmen von iManager den Knoten *Identity Manager-Dienstprogramme*.



3 Klicken Sie auf *Neuer Treiber*. Der Assistent zur Treibererstellung wird angezeigt:

**Treiber importieren**

**Willkommen beim Assistenten zum Importieren von Treibern**

Der Identity Manager enthält alle Produktkomponenten. Es hängt von den erworbenen Komponenten ab, welche Treiber Sie implementieren dürfen.

Anwendungstreiber sind im Treibersatz enthalten. Stellen Sie beim Erstellen eines Treibers sicher, dass der dem Treibersatz zugeordnete Server eine nicht gefilterte, beschreibbare Reproduktion der Partition enthält, auf der sich der Treibersatz befindet. Ist dies nicht der Fall, wird eine Lese-/Schreibreproduktion hinzugefügt oder die vorhandene Reproduktion wird in eine Lese-/Schreibreproduktion konvertiert.

Wo wollen Sie die neuen Treiber platzieren?

In einem vorhandenen Treibersatz

In einem neuen Treibersatz

<< Zurück   Weiter >>   Abbrechen   Fertig stellen

Im nächsten Schritt wählen Sie aus, wo Sie den neuen Treiber erstellen möchten. Sie können den Treiber in einem vorhandenen oder in einem neuen Treibersatz erstellen.

4 Wenn Sie *In einem vorhandenen Treibersatz* auswählen, wird ein Assistent angezeigt, mit dessen Hilfe Sie das Identitätsdepot nach dem Treibersatz durchsuchen können. Wählen Sie den vorhandenen Treibersatz aus und klicken Sie auf *Weiter*.

Wenn Sie *In einem neuen Treibersatz* auswählen, wird ein Bildschirm angezeigt, in dem Sie Eigenschaften für den neuen Treibersatz definieren können. Geben Sie einen Namen, einen Baumkontext und einen Server an und klicken Sie auf *Weiter*.

Der nächste Bildschirm des *Assistenten zur Treibererstellung* wird angezeigt:

Neuen Anwendungstreiber für diesen Treibersatz importieren oder erstellen.

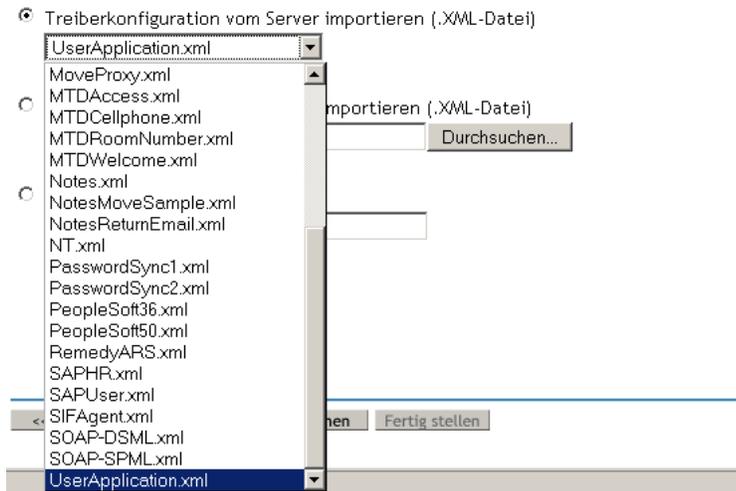
Treiberkonfiguration vom Server importieren (.XML-Datei)

Treiberkonfiguration vom Client importieren (.XML-Datei)  
Datei:

Neuen Treiber erstellen  
Name:

- 5 Klicken Sie auf die Option *Treiberkonfiguration vom Server importieren* und wählen Sie in der Liste der XML-Dateien die Datei *UserApplication.xml* aus:

Neuen Anwendungstreiber für diesen Treibersatz importieren oder erstellen.



- 6 Klicken Sie auf *Weiter*. Der *Assistent zur Treibererstellung* zeigt eine Seite an, auf der Sie den Treiber benennen und konfigurieren können:

### **UserApplication** (Treiber)

Der Treiberhersteller hat zum Import dieser Treiberkonfigurationsdatei die Angabe der folgenden Informationen angefordert. Ein \* zeigt erforderliche Informationen an.

Der Name des Treibers in der Treiberkonfigurationsdatei ist 'UserApplication'. Geben Sie den Namen ein, den Sie für diesen Treiber benutzen wollen.

Treibername: \*  Vorhandene Treiber:

Der Standardname des Treibers ist „UserApplication“. Sie können den Standardnamen verwenden oder einen eigenen Namen eingeben.

- 7 Geben Sie bei Bedarf im Feld *Treibername* einen neuen Namen für den Treiber ein.
- 8 Geben Sie im Feld *Authentifizierungs-ID* den DN des Benutzeranwendungsadministrators (eine Beschreibung des Benutzeranwendungsadministrators finden Sie in [Abschnitt 1.1.2](#),

„Benutzeranwendungsadministrator“, auf Seite 17) im Punktformat (z. B. admin.orgunit.novell) ein.

- 9 Geben Sie in den Feldern *Anwendungspasswort* und *Passwort erneut eingeben* das von Ihnen im Feld *Authentifizierungs-ID* festgelegte Passwort für den Benutzeranwendungsadministrator ein.
- 10 Geben Sie im Feld *Anwendungskontext* den Anwendungsnamen ein, der bei der Installation der Benutzeranwendung angegeben wurde. Der Standardname ist IDM.
- 11 Geben Sie im Feld *Host* den Hostnamen oder die IP-Adresse des Anwendungsservers ein, auf dem die Benutzeranwendung ausgeführt wird.
- 12 Geben Sie im Feld *Port* den Port (z. B. 8080) ein, den der Treiber für die Kommunikation mit der Benutzeranwendung verwendet, die auf dem Anwendungsserver ausgeführt wird.
- 13 Klicken Sie auf *Weiter*. Zunächst wird eine Meldung zum Import der Treiberkonfiguration angezeigt. Anschließend wird die nächste Seite des *Assistenten zur Treibererstellung* angezeigt:

#### **UserApplication2** (Treiber)

Novell empfiehlt, in Bezug auf den neu erstellten Treiber wie folgt vorzugehen:

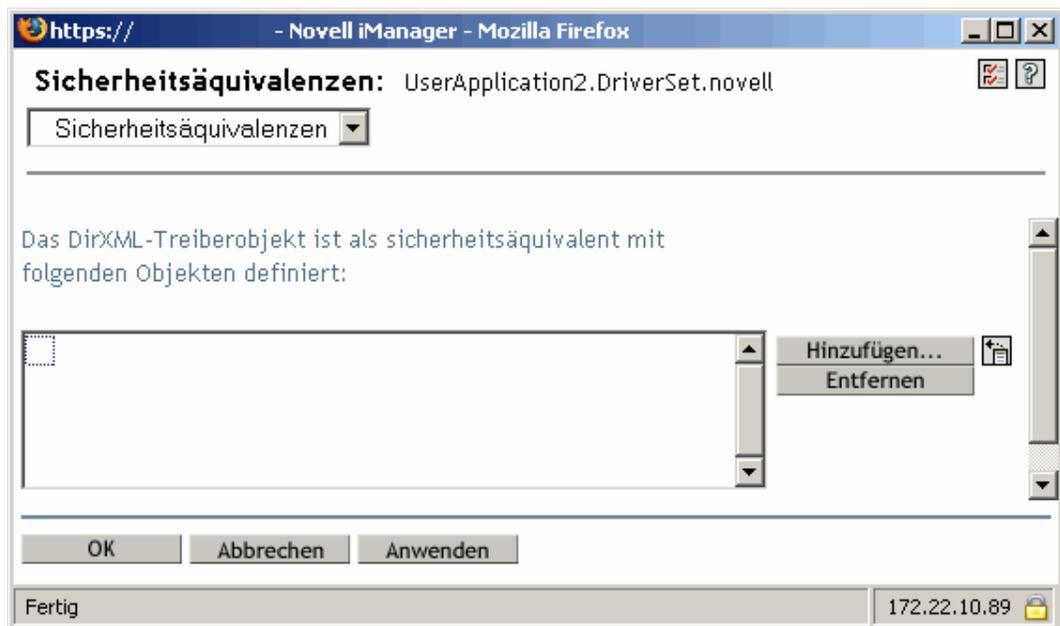
- 'Sicherheitsäquivalenzen' für den Treiber definieren.
- Alle Objekte identifizieren, die 'Verwaltungsfunktionen' darstellen. Diese von der Reproduktion ausschließen.

**Sicherheitsäquivalenzen' definieren**

**Verwaltungsfunktionen' ausschließen**

Das Treiberobjekt muss ausreichende Identitätsdepot-Rechte für alle Objekte besitzen, die es liest bzw. schreibt. Sie können diese Rechte gewähren, indem Sie dem Treiberobjekt *Sicherheitsäquivalenzen* gewähren. Der Treiber muss über einen Lese-/Schreibzugriff auf Benutzer, Post-Offices, Ressourcen und Verteilerlisten sowie über Erstellungs-, Lese- und Schreibrechte für den Post-Office-Container verfügen. Üblicherweise sollten die Sicherheitsäquivalenzen des Treibers den Administratorrechten entsprechen.

- 14 Klicken Sie auf *'Sicherheitsäquivalenzen' definieren*. Es wird ein neues Fenster angezeigt:



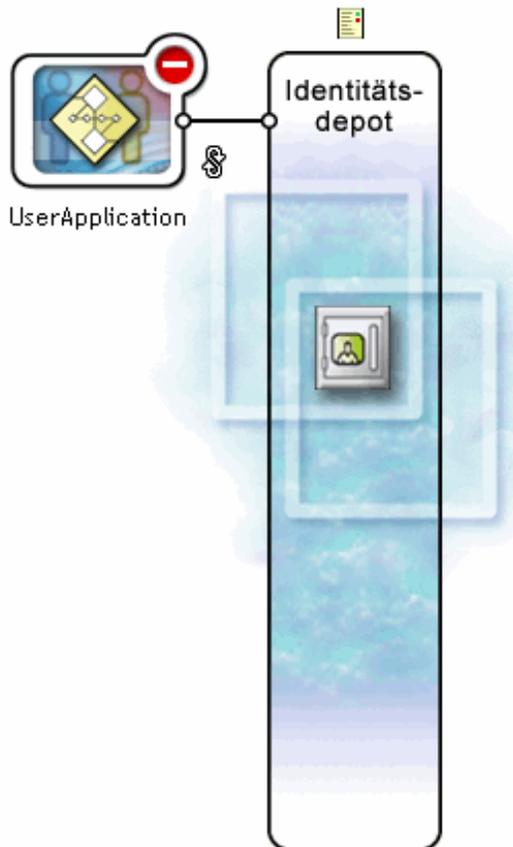
- 15 Klicken Sie auf *Hinzufügen*. Es wird ein Fenster angezeigt, in dem Sie im Baum ein Objekt auswählen können, das über die entsprechenden Rechte verfügt, die Sie dem Treiber zuweisen möchten (z. B. Admin):



- 16 Wählen Sie ein Objekt mit den gewünschten Identitätsdepot-Rechten im Baum aus und klicken Sie auf *OK*. Sie gelangen zurück zum vorherigen Fenster.
- 17 Klicken Sie auf *OK*. Der *Assistent zur Treibererstellung* wird wieder angezeigt.
- 18 Klicken Sie auf *'Verwaltungsfunktionen' ausschließen*. Das Fenster *Ausgeschlossene Benutzer* wird angezeigt. Mit dieser Funktion können Sie verhindern, dass ein Administrator nicht mehr auf den Benutzeranwendungstreiber zugreifen kann, wenn sich in einem anderen

Identitätsdepot das Administratorpasswort ändert und auf den Baum reproduziert wird, zu dem dieser Treiber gehört.

- 19 Klicken Sie auf *Hinzufügen*. Ein Fenster wird angezeigt, in dem Sie den Verzeichnisbaum nach Benutzern durchsuchen und diese von der Datenweitergabe an den Treiber ausschließen können. Üblicherweise werden Admin-Objekte ausgeschlossen, da die Reproduktion ihrer Daten über eine Treiberverbindung in den meisten Fällen kein besonders sinnvolles Verfahren ist.
- 20 Wählen Sie die auszuschließenden Verwaltungsfunktionen aus und klicken Sie anschließend auf *OK*. Sie gelangen zurück zum vorherigen Fenster.
- 21 Klicken Sie auf *OK*. Der *Assistent zur Treibererstellung* wird wieder angezeigt.
- 22 Klicken Sie auf *Weiter*. Es wird eine Zusammenfassung der Treiberkonfiguration angezeigt.
- 23 Klicken Sie auf *Fertig stellen & Überblick*. Im Identitätsdepot wird eine grafische Darstellung des Treibers angezeigt:



---

**Hinweis:** Sie können diesen Bildschirm jederzeit im iManager-Navigationsbaum über den Link *Identity Manager-Überblick* unter *Identity Manager* aufrufen.

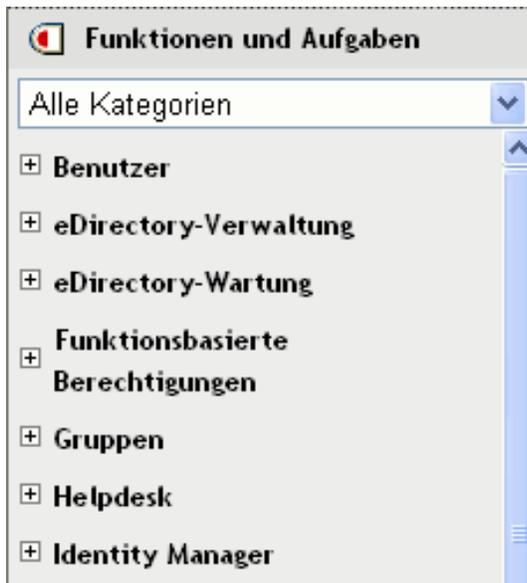
---

Der neue Treiber wird als großes Symbol dargestellt, das mit dem Identitätsdepot-Stamm verbunden ist.

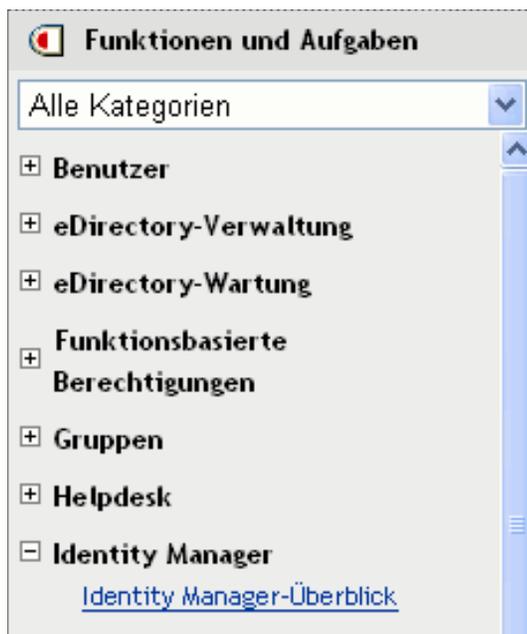
### 3.3 Starten des Benutzeranwendungstreibers

So starten Sie den Benutzeranwendungstreiber:

- 1 Klicken Sie im iManager-Navigationsbaum auf den Link *Identity Manager*, um die verfügbaren Befehle in der Kategorie „Identity Manager“ anzuzeigen:



- 2 Klicken Sie im iManager-Navigationsbaum auf den Link *Identity Manager-Überblick* unterhalb des Links *Identity Manager*:



Es wird ein Assistent angezeigt, mit dessen Hilfe Sie das System nach dem Treibersatz durchsuchen können, der den zu aktivierenden Treiber enthält.

- 3 Wählen Sie den Treibersatz aus und klicken Sie auf *Weiter*. Die Seite *Identity Manager-Überblick* wird angezeigt.
- 4 Klicken Sie auf den runden Statusindikator in der rechten oberen Ecke des Treibersymbols:



Es wird ein Menü mit Befehlen zum Starten und Stoppen des Treibers und zum Bearbeiten der Treibereigenschaften angezeigt:



- 5 Klicken Sie auf *Treiber starten*.

## 3.4 Einrichten von automatisch startenden Workflows

Bei installiertem Bereitstellungsmodul werden Workflows automatisch gestartet, wenn ein Benutzer durch die Anforderung einer Ressource eine Bereitstellungsanforderung startet. Zudem überwacht die Identity Manager-Benutzeranwendung Ereignisse im Identitätsdepot und reagiert, wenn entsprechend konfiguriert, auf die Ereignisse mit dem Auslösen der zugehörigen Bereitstellungs-Workflows. Sie können den Benutzeranwendungstreiber z. B. so konfigurieren, dass er automatisch einen Bereitstellungs-Workflow startet, sobald ein neuer Benutzer zum Identitätsdepot hinzugefügt wird. Verwenden Sie die Richtlinien und Regeln von Identity Manager, um den Benutzeranwendungstreiber für das automatische Starten von Workflows zu konfigurieren.

### 3.4.1 Allgemeines zu Richtlinien

Sie können Filter und Richtlinien für den Benutzeranwendungstreiber auf die gleiche Weise verwenden wie für andere Identity Manager-Treiber. Wenn ein Ereignis im Identitätsdepot auftritt, generiert Identity Manager ein XML-Dokument mit einer Beschreibung dieses Ereignisses. Das XML-Dokument wird über den Kanal an das verbundene System weitergegeben (in diesem Fall ist das verbundene System die Benutzeranwendung). Über Filter und Richtlinien, die einem Treiber zugeordnet sind, können Sie die Art der Reaktion auf ein Ereignis festlegen und das XML-Dokument in das von dem verbundenen System erwartete Format transformieren. Identity Manager stellt verschiedene Kategorien von Richtlinien zur Verfügung (z. B. Ereignistransformation, Befehlstransformation, Schemazuordnung, Ausgabetransformation), die Sie in einer vorgegebenen Reihenfolge zur Transformation des XML-Dokuments anwenden können. Dieser Abschnitt enthält ein Beispiel für das Starten eines Workflows basierend auf Ereignissen im Identitätsdepot. Es

können zwar alle Richtlinien verwendet werden, um einen Workflow auszulösen, aber die im Beispiel veranschaulichte Methode ist am einfachsten und effektivsten.

Bei der Erstellung eines Benutzeranwendungstreibers wird eine Ereignistransformationsrichtlinie erstellt, die vom Treiber verwendet wird. Die Ereignistransformationsrichtlinie ist verantwortlich für das Erstellen des XML-Dokuments, das von den verbleibenden Abonnentenkanalrichtlinien verarbeitet wird.

---

**Hinweis:** Nehmen Sie keine Änderungen an der Ereignistransformationsrichtlinie vor, die bei der Erstellung des Benutzeranwendungstreibers erzeugt wurde. Der DN dieser Richtlinie beginnt mit `Manage.Modify.Subscriber`. Bei einer Änderung dieser Richtlinie wird der Workflow möglicherweise fehlerhaft ausgeführt.

---

Es wird außerdem eine leere Schemazuordnungsrichtlinie erstellt. Sie können diese Richtlinie als Ausgangspunkt für das Auslösen eines Workflows verwenden, der auf Ereignissen im Identitätsdepot basiert.

### 3.4.2 Einrichten eines Workflows, der basierend auf einem Ereignis im Identitätsdepot startet

Die einfachste Methode für das automatische Starten eines Workflows besteht in der Verwendung des Schemazuordnungsrichtlinien-Editors. Im Benutzeranwendungstreiber ist eine leere Richtlinie verfügbar, die Sie zu diesem Zweck bearbeiten können.

Der Schemazuordnungsrichtlinien-Editor wird zum Zuordnen der Identitätsdepot-Attribute (einschließlich des eDirectory-Attributs *trigger*, das bei einer Änderung den Workflow startet) zu den Laufzeitdaten eines Ziel-Workflows verwendet. Die Laufzeitdaten werden von der Workflow-Definitionsschablone festgelegt (weitere Informationen zu Workflow-Definitionsschablonen finden Sie in [Kapitel 22, „Konfigurieren von Bereitstellungsanforderungsdefinitionen“](#), auf Seite 323). Die Laufzeitdaten werden benötigt, damit ein Workflow erfolgreich abgeschlossen werden kann. Wenn ein Workflow erstellt wird, werden mehrere *globale Attribute* im Identitätsdepot erstellt, mit deren Hilfe das Verhalten des Benutzeranwendungstreibers angepasst werden kann. Ein globales Attribut ist ein Attribut, das keiner Identitätsdepot-Objektklasse angehört. Diese Attribute heißen „`<workflowName>_StartWorkflow`“, „`<workflowName>_recipient`“ und „`<workflowName>_reason`“. Zwei weitere immer vorhandene Attribute sind „`AllWorkflows:reason`“ und „`AllWorkflows:recipient`“. Das Attribut `_StartWorkflow` wird zum Starten eines Workflows verwendet. Die `_recipient`- und `_reason`-Attribute werden zum Entgegennehmen von Laufzeitdaten verwendet, die der Workflow vom Identitätsdepot benötigt.

Bevor Sie diesen Vorgang ausführen, sollten Sie den Namen des Identitätsdepot-Attributs kennen, das Sie als Auslöser für den Workflow verwenden möchten. Außerdem müssen Sie den Namen des zu startenden Workflows kennen. Alle Workflows beinhalten ein spezielles Attribut namens `<workflowName>_StartApprovalFlow`. Sie können festlegen, dass ein Workflow basierend

auf einem Ereignis im Identitätsdepot automatisch startet, indem Sie das gewünschte eDirectory-Attribut dem Attribut „<workflowName>\_StartApprovalFlow“ des Workflows zuordnen.

So richten Sie einen Workflow ein, der basierend auf einem Ereignis im Identitätsdepot startet:

- 1 Klicken Sie im iManager-Navigationsbaum unter „Identity Manager“ auf den Link *Identity Manager-Überblick*.

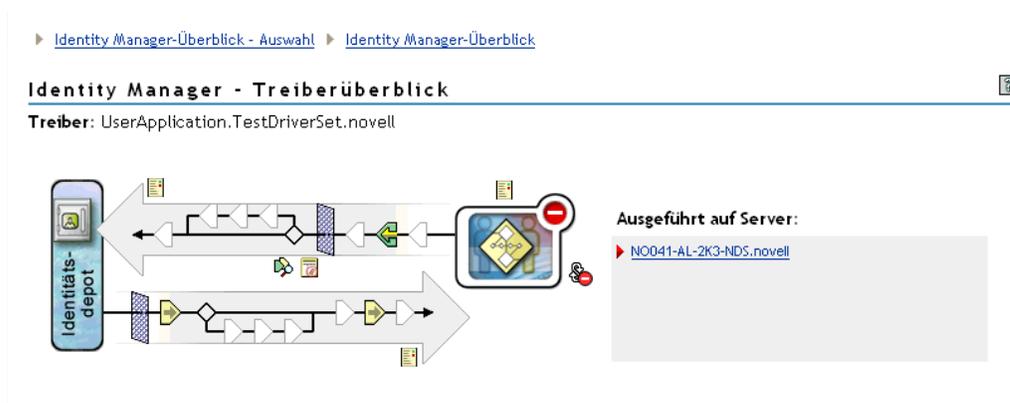


Die Seite *Identity Manager-Überblick* wird angezeigt. Sie werden aufgefordert, einen Treibersatz auszuwählen.

- 2 Klicken Sie auf *Gesamten Baum durchsuchen* und anschließend auf *Suchen*. Die Seite *Identity Manager-Überblick* wird zusammen mit einer Grafik angezeigt, die die Treiber des aktuell ausgewählten Treibersatzes darstellt.
- 3 Klicken Sie auf das große Treibersymbol für den Benutzeranwendungstreiber:

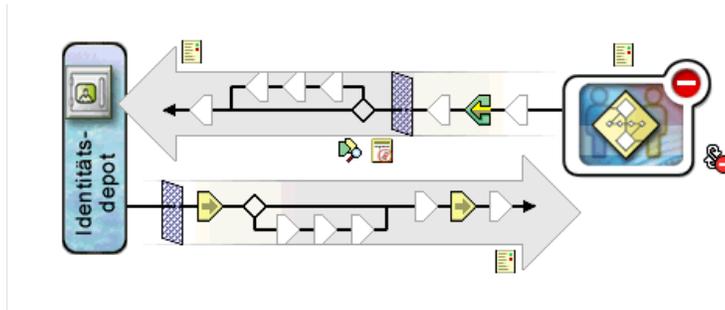


Der *Identity Manager - Treiberüberblick* wird angezeigt:

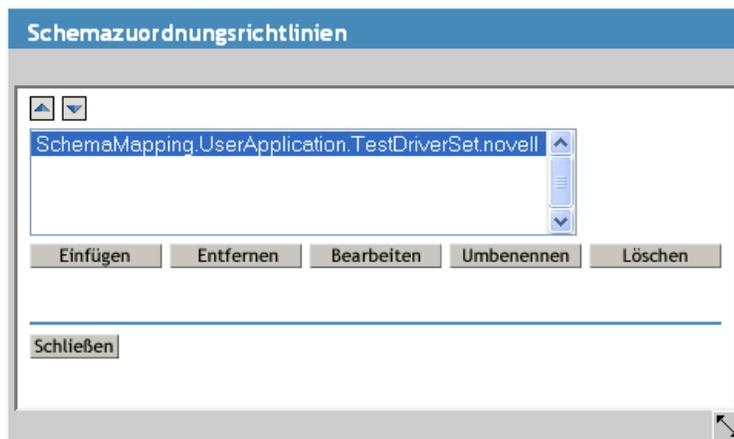
A screenshot of the 'Identity Manager - Treiberüberblick' page. At the top, there are navigation links: 'Identity Manager-Überblick - Auswahl' and 'Identity Manager-Überblick'. Below this is the title 'Identity Manager - Treiberüberblick' and a help icon. The main content area shows 'Treiber: UserApplication.TestDriverSet.novell'. A diagram illustrates the driver set with a central 'identitäts-depot' box on the left and a 'UserApplication' icon on the right. Two large horizontal arrows connect them: the top one points left (Herausgeberkanal) and the bottom one points right (Abonnentenkanal). To the right of the diagram, a box labeled 'Ausgeführt auf Server:' contains the text 'NO041-AL-2K3-NDS.novell'.

Der obere waagrechte Pfeil stellt den Herausgeberkanal dar (der im Benutzeranwendungstreiber nicht verwendet wird), der untere Pfeil den Abonnentenkanal.

Wenn Sie den Mauszeiger über ein Objekt in der Grafik bewegen, wird eine Beschreibung des Objekts angezeigt:

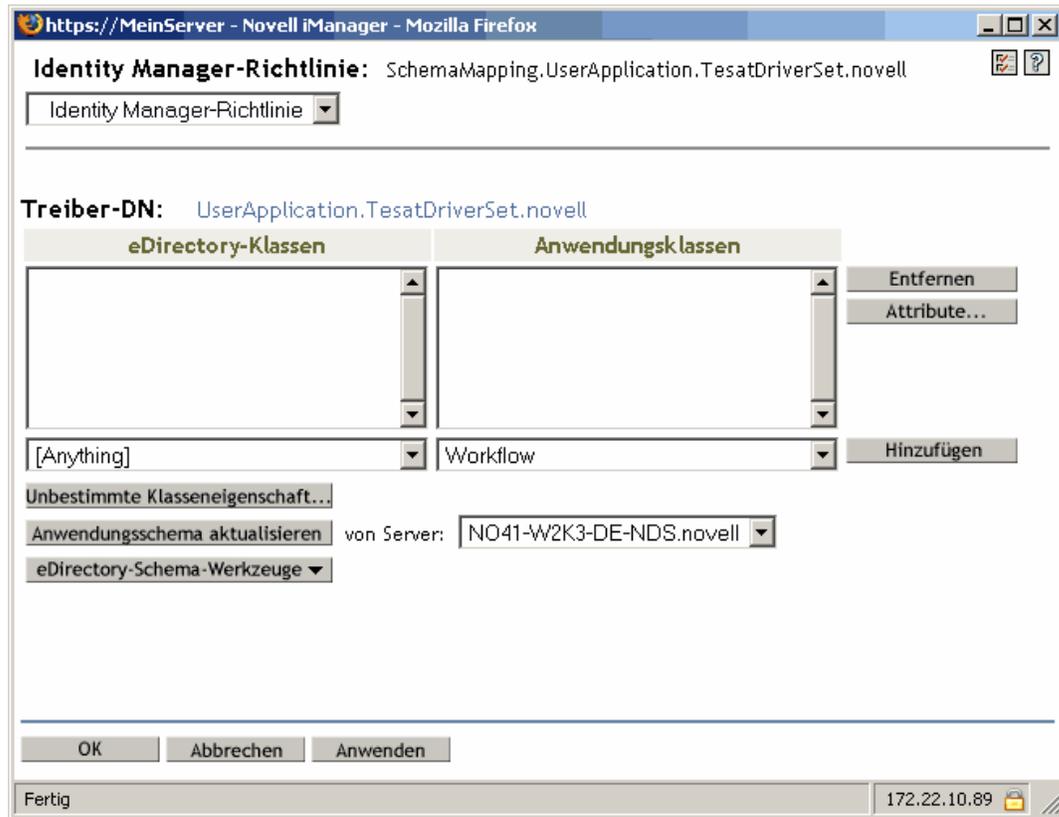


- 4 Klicken Sie auf das Symbol *Schemazuordnungsrichtlinien* für den Abonnementkanal. Das Dialogfeld *Schemazuordnungsrichtlinien* wird angezeigt und der Name der standardmäßigen Schemazuordnungsrichtlinie ist hervorgehoben:



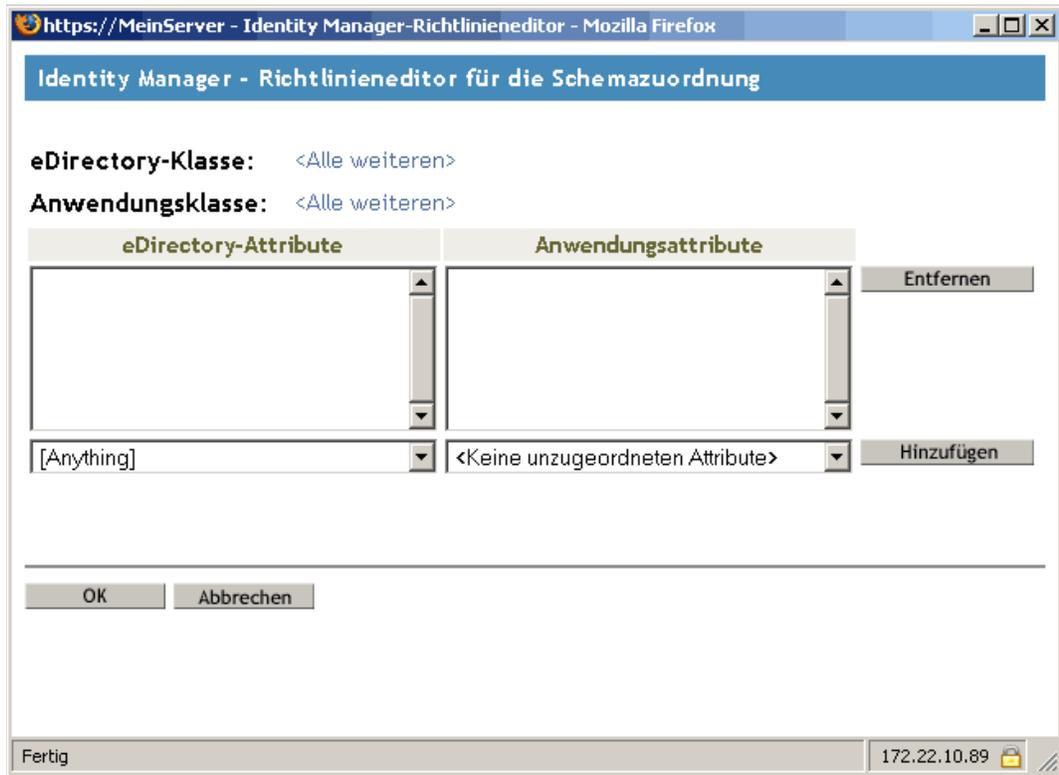
- 5 Klicken Sie auf *Bearbeiten*. Das Dialogfeld *Identity Manager-Richtlinie* wird angezeigt. Über dieses Dialogfeld werden die Identitätsdepot-Klassen den Anwendungsklassen zugeordnet. Bei

diesem Vorgang wird diese Funktion nicht verwendet. Stattdessen werden die eDirectory-Attribute den globalen Benutzeranwendungsattributen zugeordnet.



- 6 Klicken Sie auf *Anwendungsschema aktualisieren*. Eine Meldung informiert Sie darüber, dass der Treiber zum Lesen des Schemas gestoppt und anschließend neu gestartet werden muss. Es werden etwa 60 Sekunden für die Aktualisierung des Schemas benötigt. In diesem Schritt wird zur Vorbereitung auf den folgenden Schritt der neueste Workflow-Informationssatz gelesen, in dem angegeben ist, welche Informationen vom Identitätsdepot an den zu startenden Workflow weitergeleitet werden sollen.
- 7 Klicken Sie auf *OK*, um das Schema zu aktualisieren. Wenn die Aktualisierung des Schemas abgeschlossen ist, wird eine entsprechende Meldung angezeigt.
- 8 Klicken Sie auf *OK*, um die Meldung zu schließen. Das Dialogfeld *Identity Manager-Richtlinie* wird wieder angezeigt.

- 9 Klicken Sie auf *Nicht-klassenspezifische Attribute*. Das Dialogfeld *Identity Manager - Richtlinieneditor für die Schemazuordnung* wird angezeigt.



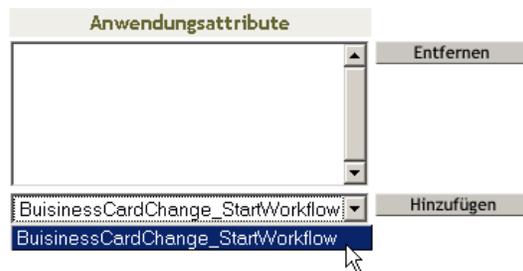
Die Dropdown-Liste *eDirectory-Attribute* enthält alle eDirectory-Attribute.

Die Dropdown-Liste *Anwendungsattribute* enthält die Attribute aller aktiven Workflows. Die Attribute in der Liste werden entweder mit `AllWorkflows` (das bedeutet, dass die Attribute für alle Workflows gelten) oder mit dem Namen eines spezifischen Workflows eingeleitet. Wenn ein eDirectory-Attribut (z. B. `manager`) dem `manager`-Attribut für alle Workflows zugeordnet werden soll, muss `manager` zu `Allworkflows:manager` zugeordnet werden. Wenn für einen bestimmten Workflow ein anderes eDirectory-Attribut verwendet werden soll (z. B. `HRmanager`), muss das eDirectory-Attribut dem spezifischen Workflow-Attribut (z. B. `BusinessCardChange:manager`) zugeordnet werden.

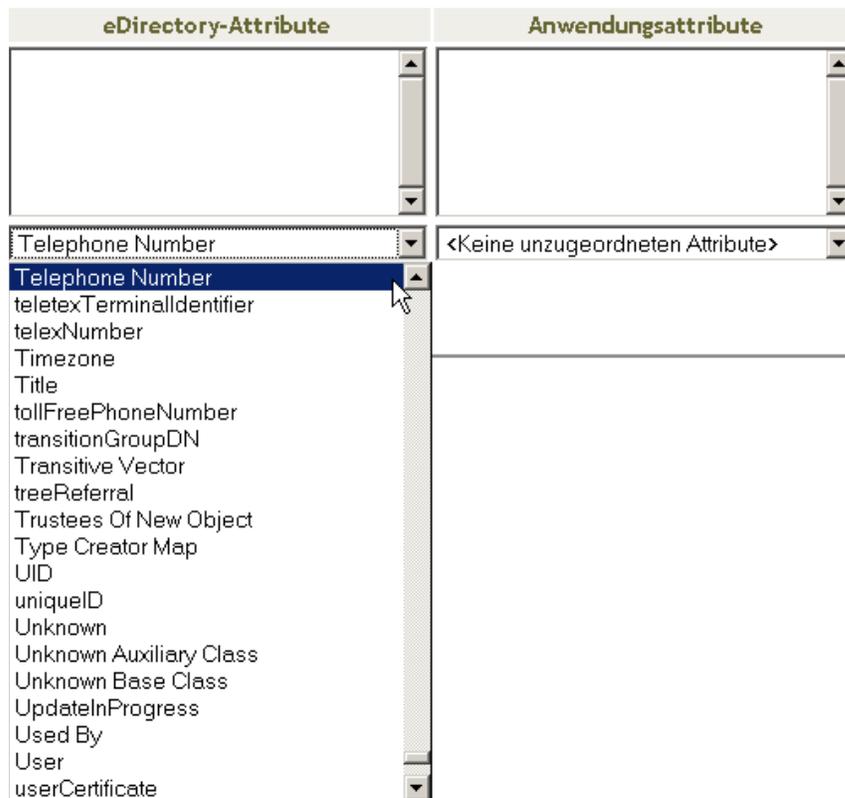
Einander zugeordnete Attribute werden nebeneinander in den Spalten *eDirectory-Attribute* und *Anwendungsattribute* angezeigt.

In den folgenden Schritten wird das eDirectory-Attribut, das den Workflow starten soll, dem `_StartWorkflow`-Attribut für diesen Workflow zugeordnet. Wenn zusätzliche eDirectory-Attribute vom Workflow erwartet werden, müssen auch diese Attribute entsprechend zugeordnet werden. Wenn z. B. das eDirectory-Attribut `Address` der Auslöser für einen Workflow ist, benötigt der Workflow möglicherweise auch Attribute wie `City` und `State`. Diese Attribute können alternativ über Richtlinien zugeordnet werden.

- 10 Wählen Sie in der Liste *Anwendungsattribute* das *\_StartWorkflow*-Attribut für den Workflow, den Sie konfigurieren möchten. Das folgende Beispiel zeigt das *\_StartWorkflow*-Attribut für einen *BusinessCardChange*-Workflow (*BusinessCardChange\_StartWorkflow*).



- 11 Wählen Sie in der Liste *eDirectory-Attribute* das *eDirectory*-Attribut aus, das bei einer Änderung des Attributs den Workflow starten soll. Im folgenden Beispiel wurde das *Telefonattribut* ausgewählt. Dies bedeutet, dass der *BusinessCardChange*-Workflow immer dann startet, wenn sich die Telefonnummer eines Mitarbeiters ändert.



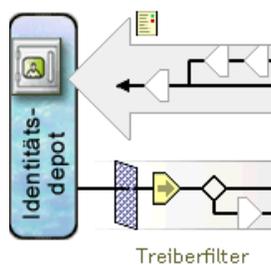
- 12** Klicken Sie auf *Hinzufügen*. Das eDirectory-Attribut wird dem Anwendungsattribut zugeordnet.

eDirectory-Klassen	Anwendungsklassen
[Anything]	Workflow

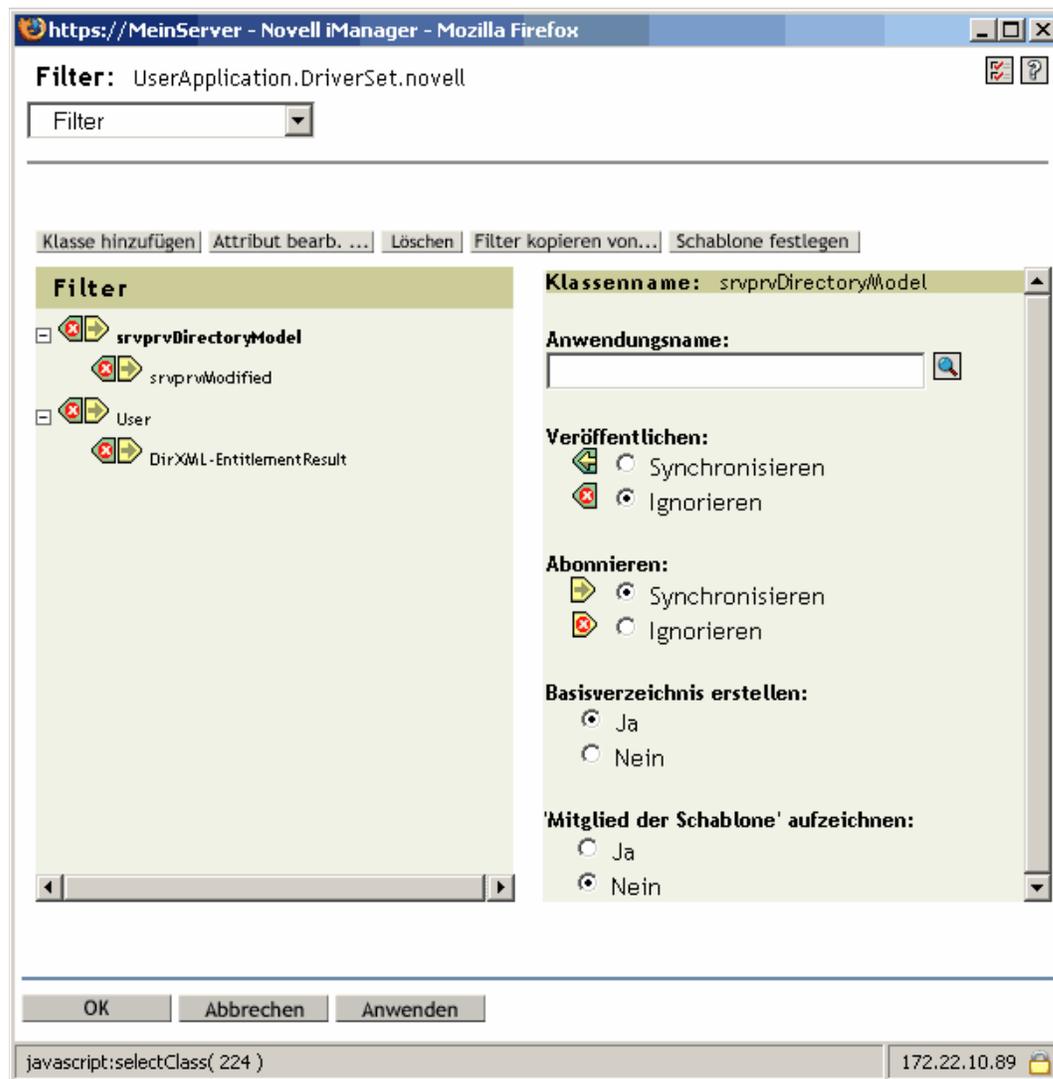
- 13** Wenn zusätzliche eDirectory-Attribute vom Workflow benötigt werden, wiederholen Sie **Schritt 10** bis **Schritt 12**, bis alle erforderlichen Attribute zugeordnet sind.

Der Workflow startet automatisch, wenn eine Änderung in dem eDirectory-Attribut vorgenommen wird, das einem `_StartApprovalFlow`-Anwendungsattribut zugeordnet ist. Das eDirectory-Attribut erreicht die Schemazuordnungsrichtlinie nur, wenn es in den Abonnentenkanal-Treiberfilter einbezogen wird. In den folgenden Schritten wird das eDirectory-Attribut zum Abonnentenkanal-Treiberfilter hinzugefügt.

- 14** Klicken Sie auf *OK*, um den *Identity Manager - Richtlinieneditor für die Schemazuordnung* zu schließen.
- 15** Klicken Sie auf *OK*, um das Dialogfeld *Identity Manager-Richtlinie* zu schließen.
- 16** Klicken Sie auf *Schließen*, um das Dialogfeld „Schemazuordnungsrichtlinien“ zu schließen.
- 17** Klicken Sie auf das Symbol *Treiberfilter* für den Abonnentenkanal.



Das Fenster mit den Filtern wird angezeigt:



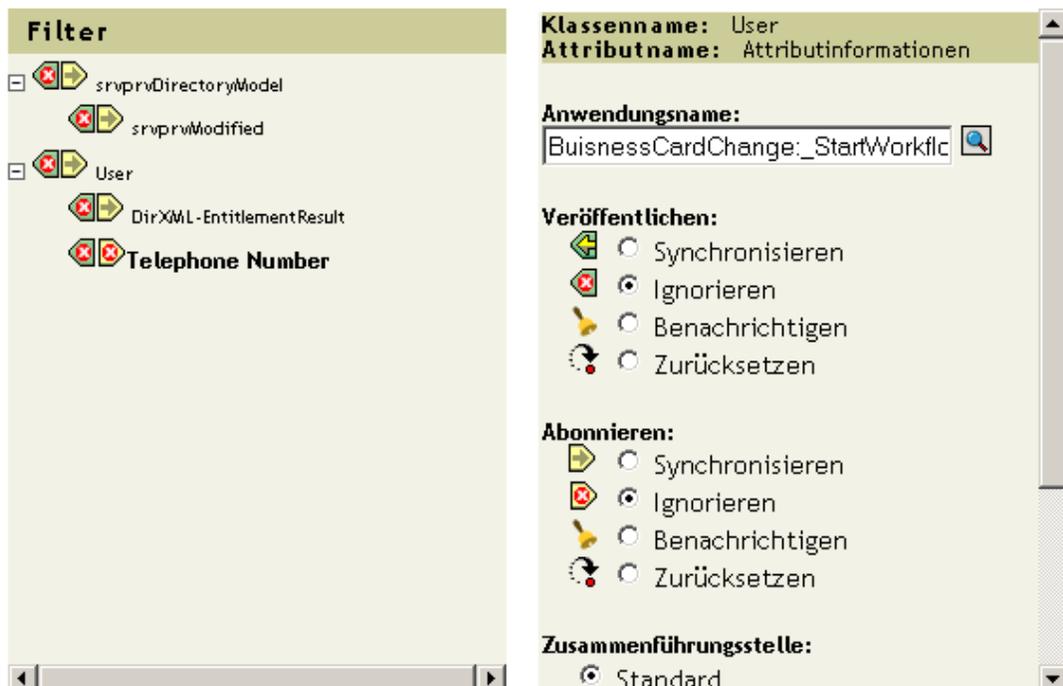
Ereignisfilter geben die Objektklassen und die Attribute an, für die die Identity Manager-Engine Ereignisse verarbeitet. In der schreibgeschützten Liste *Filter* auf der linken Seite werden die Attribute der Klasse aufgeführt. Die Liste *Klassenname* auf der rechten Seite zeigt die Optionen an, die zu dem Zielobjekt gehören.

- 18 Klicken Sie auf den Namen der Klasse (z. B. „User“), zu der das Attribut gehört, das Sie zum Filter hinzufügen möchten.
- 19 Klicken Sie auf *Attribut hinzufügen*. Es wird eine Liste mit Attributen angezeigt.

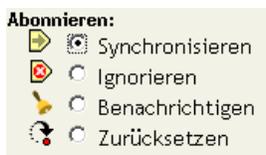
- 20 Wählen Sie ein Attribut aus und klicken Sie anschließend auf *OK*. Das Attribut wird zur Liste *Filter* hinzugefügt.



- 21 Klicken Sie auf den Attributnamen. Die Synchronisierungsoptionen für das Attribut werden im rechten Teilfenster angezeigt.



- 22 Klicken Sie unter *Abonnieren* auf *Synchronisieren*.



- 23 Geben Sie beliebige weitere Attribute für den Filter an. Wählen Sie für ein Attribut *Synchronisieren* aus, wenn Änderungen an Attributwerten berichtet und synchronisiert werden sollen. Wählen Sie *Ignorieren* aus, wenn Änderungen an Attributwerten nicht berichtet und synchronisiert werden sollen.
- 24 Klicken Sie auf *OK*. Es wird eine Meldung angezeigt, in der Sie gefragt werden, ob der Treiber neu gestartet werden soll, damit die Änderungen wirksam werden.
- 25 Klicken Sie auf *OK*. Sie kehren zur Seite *Identity Manager - Treiberüberblick* zurück.

# Konfigurieren der Verzeichnisabstraktionsschicht

# 4

In diesem Kapitel wird die Verwendung des Verzeichnisabstraktionsschicht-Editors beschrieben, mit dem die Datendefinitionen der Verzeichnisabstraktionsschicht für die Identity Manager-Benutzeranwendung definiert werden. Es werden folgende Themen erläutert:

- [Abschnitt 4.1, „Allgemeines zu Verzeichnisabstraktionsschicht-Definitionen“](#), auf Seite 75
- [Abschnitt 4.2, „Erste Schritte“](#), auf Seite 76
- [Abschnitt 4.3, „Arbeiten mit Entitäten und Attributen“](#), auf Seite 87
- [Abschnitt 4.4, „Arbeiten mit Listen“](#), auf Seite 104
- [Abschnitt 4.5, „Arbeiten mit Organigramm-Relationen“](#), auf Seite 107
- [Abschnitt 4.6, „Arbeiten mit Konfigurationseinstellungen“](#), auf Seite 110
- [Abschnitt 4.7, „Anzeigetext lokalisieren“](#), auf Seite 111

## 4.1 Allgemeines zu Verzeichnisabstraktionsschicht-Definitionen

Unter der *Verzeichnisabstraktionsschicht* versteht man eine Reihe von Datendefinitionen, die für die logische Ansicht eines Identitätsdepots erforderlich sind. Die Verzeichnisabstraktionsschicht definiert Folgendes:

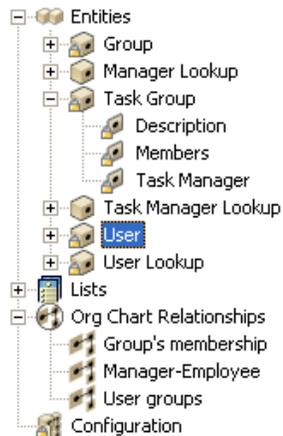
- Die Objekte und Attribute des Identitätsdepots, die in der Identity Manager-Benutzeranwendung verwendet werden können.
- Die Art, wie die Daten des Identitätsdepots in der Benutzeroberfläche angezeigt werden.
- Die für das Organigramm-Portlet zur Verfügung stehenden Relationen.

Mit dem *Verzeichnisabstraktionsschicht-Editor* können Sie diese Datendefinitionen bearbeiten, wenn Sie die Darstellung oder Funktionsweise der Benutzeranwendung ändern möchten. Sie können die Definitionen wie folgt ändern:

- Durch Hinzufügen weiterer Identitätsdepot-Objekte
- Durch Ändern der Attribute, die für ein Identitätsdepot-Objekt zur Verfügung stehen
- Durch Ändern von Listeninhalten
- Durch Anzeigen unterschiedlicher Relationen zwischen den Identitätsdepot-Objekten

Die Installationsprozedur der Identity Manager-Benutzeranwendung installiert und implementiert den für die ordnungsgemäße Funktionsweise der Benutzeranwendung erforderlichen Standardsatz an Abstraktionsschichtdefinitionen. Bei der Installation werden auch eDirectory-Schemaerweiterungen erstellt, die vom Benutzeranwendungstreiber und von der Benutzeranwendung verwendet werden. Sie erfahren mehr über diese Schemaerweiterungen in [Anhang A, „Schemaerweiterungen“](#), auf Seite 365. Der gleiche Standardsatz von Dateien wird auf dem lokalen Dateisystem erstellt, wenn Sie mit dem Identity Manager-Designer eine neue Instanz des Benutzeranwendungstreibers erstellen.

**Erforderliche Datendefinitionen für die Abstraktionsschicht** Beim Anpassen Ihrer Identity Manager-Benutzeranwendung möchten Sie möglicherweise Änderungen an den Verzeichnisabstraktionsschicht-Objekten vornehmen. Bestimmte Identitätsdepot-Objekte („Entitäten“), Attribute, Relationen und Listen können aber weder entfernt noch geändert werden, da die Benutzeranwendung ansonsten nicht mehr ordnungsgemäß funktionieren würde. Die Definitionen, die nicht entfernt werden können, sind mit einem Vorhängeschloss gekennzeichnet. Im nachfolgend dargestellten Beispiel sind die Aufgabengruppe und alle ihre Attribute gesperrt.



**Speicherort der Verzeichnisabstraktionsschicht-Definitionen** *Verzeichnisabstraktionsschicht*-Definitionen sind XML-Dateien, für die Folgendes gilt:

- Sie werden lokal im Dateisystem des Designer-Computers im Unterverzeichnis „Provisioning\AppConfig\DirectoryModel“ des Bereitstellungsprojekts *gespeichert*. Enthält Ihr Projekt mehr als eine Benutzeranwendung, werden die Verzeichnisnamen nummeriert. Beispielsweise AppConfig1, AppConfig2 usw.
- Sie werden im Container „AppConfig.DirectoryModel“ des Benutzeranwendungstreibers *bereitgestellt*. Die XML-Dateien werden im XMLData-Attribut des entsprechenden Objekts der Verzeichnisabstraktionsschicht-Definition gespeichert. Jede Entität, Relation und Liste ist eine eindeutige Objektinstanz, die im Container „AppConfig.DirectoryModel“ des Benutzeranwendungstreibers abgelegt wird.
- Sie werden im *Cache* des Anwendungsservers abgelegt, auf dem die Benutzeranwendung bereitgestellt ist.

## 4.2 Erste Schritte

Sie benötigen die Funktionen des Designers für die Identity Manager-Bereitstellungsansicht sowie den Verzeichnisabstraktionsschicht-Editor zum Definieren des Inhalts der Verzeichnisabstraktionsschicht. Führen Sie die folgenden ersten Schritte durch:

Schritt	Aufgabe	Beschreibung
1	Identity Manager-Projekt erstellen	<p>Dies beinhaltet:</p> <ul style="list-style-type: none"> <li>• Das Konfigurieren des Identitätsdepots</li> <li>• Die Angabe der Treibersatzeigenschaften</li> </ul> <p>Anweisungen finden Sie in der Identity Manager-Dokumentation.</p>
2	Benutzeranwendungstreiber zum Modeler hinzufügen	<p>Der Identity Manager-Benutzeranwendungstreiber befindet sich im Bereitstellungsordner der Modeler-Palette.</p> 
3	Konfiguration des Benutzeranwendungstreibers abschließen	<p>Siehe die Prozedur in <a href="#">Abschnitt 4.2.1, „Konfiguration des Benutzeranwendungstreibers abschließen“</a>, auf Seite 78.</p>
4	Auf die Bereitstellungsansicht zugreifen	<p>Weitere Informationen hierzu finden Sie in <a href="#">Abschnitt 4.2.2, „Zugreifen auf die Bereitstellungsansicht“</a>, auf Seite 81.</p>
5	Den Verzeichnisabstraktionsschicht-Editor starten	<p>Weitere Informationen hierzu finden Sie unter <a href="#">„So öffnen Sie den Verzeichnisabstraktionsschicht-Editor:“</a> auf Seite 82.</p>

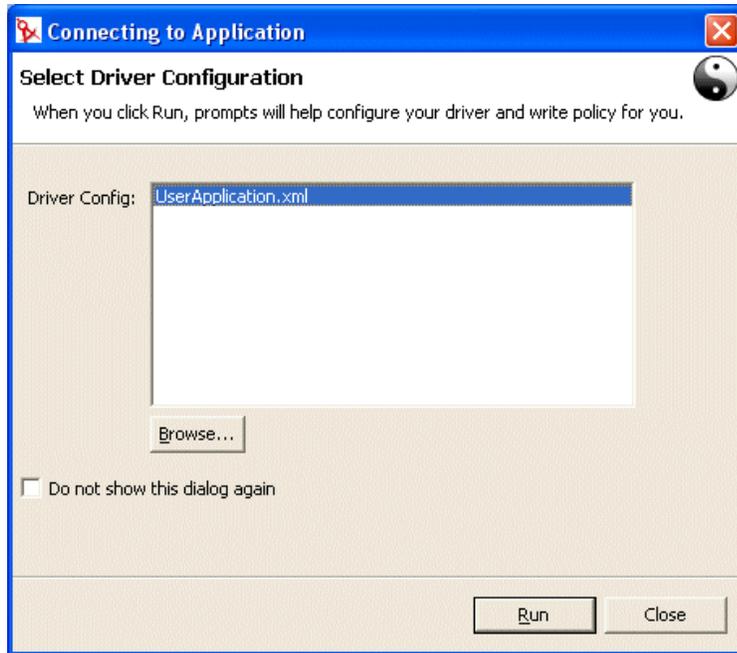
## 4.2.1 Konfiguration des Benutzeranwendungstreibers abschließen

Führen Sie folgende Schritte aus, nachdem Sie ein Identity Manager-Projekt erstellt haben.

So schließen Sie die Konfiguration des Benutzeranwendungstreibers ab:

- 1 Legen Sie ein *Benutzeranwendungs*-Treibersymbol im dafür vorgesehenen Bereich ab.

Sie müssen dann eine Treiberkonfiguration angeben.



- 2 Wählen Sie *UserApplication.xml* (die Standardeinstellung) und klicken Sie anschließend auf *Ausführen*.

- 3 Geben Sie an, wie der Assistent die Validierung Ihrer Einträge handhaben soll, indem Sie auf „Ja“ oder „Nein“ klicken.

**Import Information Requested**

The driver writer requested that the following information be supplied in order to import this driver configuration file.

Information requested: \* Required

Enter the driver name. Entering the name of or selecting an existing driver will overwrite its configuration. The Driver name 'UserApplication' was provided as a default value by the Configuration File.

Driver name: \*

Enter the DN of the User Application Administrator. This value should match the user entered during the User Application installation. Use the DOT format i.e., admin.orgunit.novell or use browse. This is a required field.

Authentication ID: \*

Enter the password of the User Application Administrator specified above.

Application Password :

Reenter the password:

Enter the User Application Context. This is the context portion of the URL for the User Application WAR file. The default is: IDM.

Application Context:

OK Cancel

Enter the Host Name or IP address of the application server where the User Application is running. For example, 'http://ServerName' or 'https://123.456.78.99'. This is a required field.

Host: \*

Enter the host port on the application server specified above. This is the port where the User Application is accessible e.g. 80, 8080, 8090.

Port:

OK Cancel

#### 4 Machen Sie folgende Angaben:

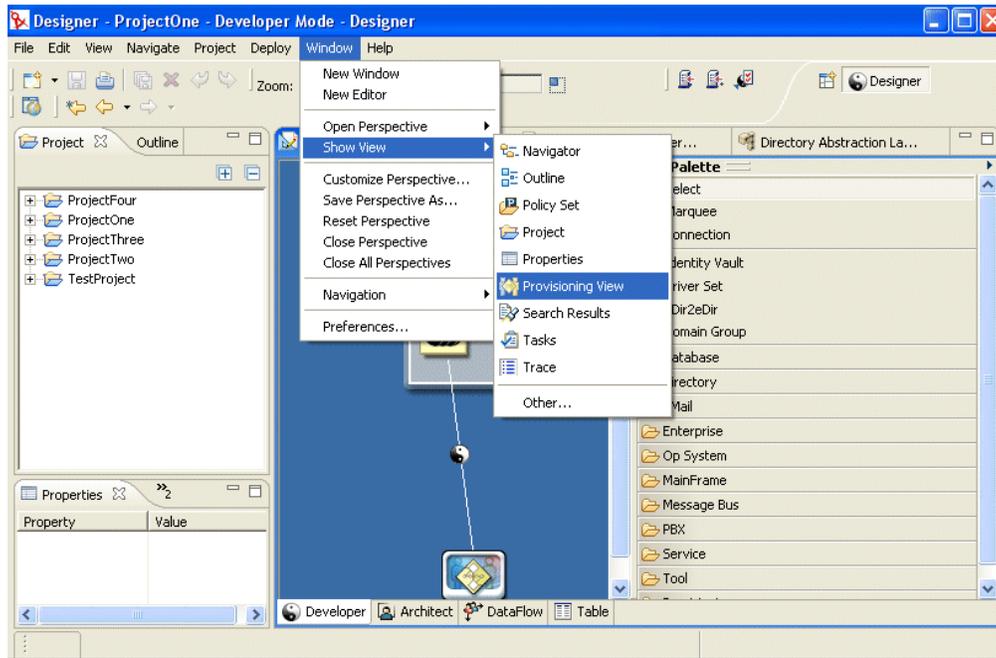
Eigenschaft	Erforderliche Angaben
Driver Name	<ul style="list-style-type: none"> <li>• Der Name eines vorhandenen Treibers (der Treiber im Treibersatz, der bei der Installation der Benutzeranwendung angegeben wurde).</li> <li>• Der Name eines neuen Treibers.</li> </ul>
Authentication ID	Der DN des Benutzeranwendungsadministrators.
Application password/Reenter the password	Das Passwort des Benutzeranwendungsadministrators.
Application context	Der Name des Benutzeranwendungskontexts (wird bei der Installation angegeben, beispielsweise IDM).
Host	<p>Der Hostname oder die IP-Adresse des Anwendungsservers, auf dem die Identity Manager-Benutzeranwendung bereitgestellt ist. Diese Angaben werden wie folgt verwendet:</p> <ul style="list-style-type: none"> <li>• Als Auslöser, damit Workflows auf dem Anwendungsserver eine Verbindung für den Zugriff auf Workflows (Beenden, Zurückziehen usw.) herstellen.</li> <li>• Zum Aktualisieren von Datendefinitionen, die im Cache abgelegt sind.</li> </ul>
Port	Der Port für obigen Host.

#### 5 Klicken Sie auf *OK*.

## 4.2.2 Zugreifen auf die Bereitstellungsansicht

So greifen Sie auf die Bereitstellungsansicht zu:

- 1 Sie haben folgende Möglichkeiten:
  - Wählen Sie *Window>Show View>Provisioning View*.



- Öffnen Sie den Ordner *Provisioning* und wählen Sie *Provisioning View*.
- Klicken Sie auf *OK*.

ODER:

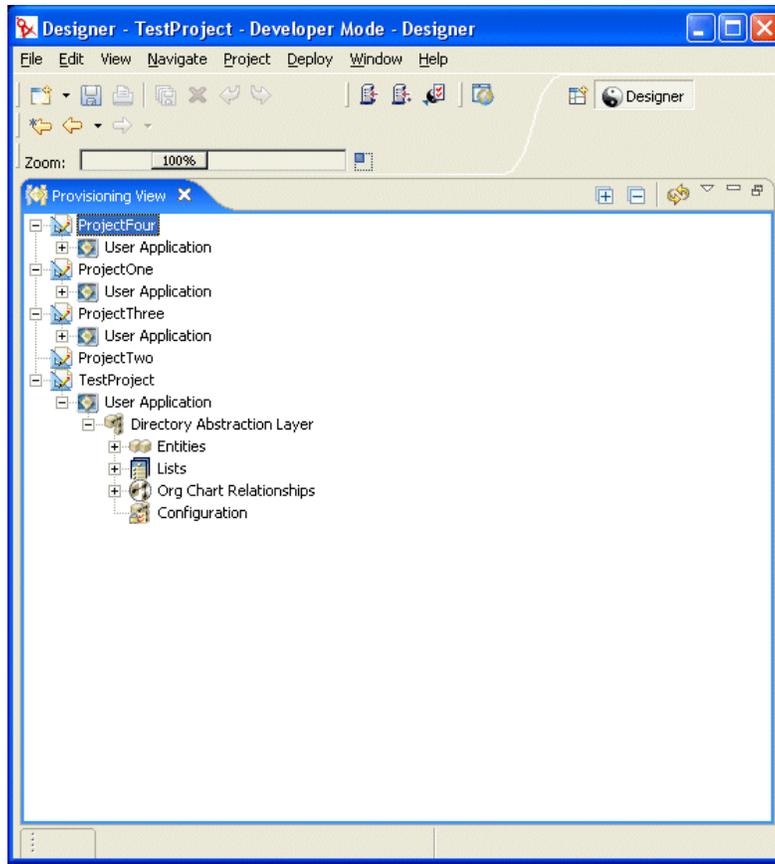
- Wählen Sie das Benutzeranwendungssymbol, klicken Sie mit der rechten Maustaste und wählen Sie *Application>Show Provisioning View*.

In der Bereitstellungsansicht finden Sie das Projekt, das Sie gerade zusammen mit anderen Bereitstellungsprojekten erstellt haben, die sich im selben Arbeitsbereich befinden.

---

**Tipp:** Wenn Sie die Anwendungen wider Erwarten nicht in der Ansicht finden, *kann* dies daran liegen, dass das Projekt beschädigt ist. In diesem Fall müssen Sie es neu erstellen.

---



### Allgemeines zur Bereitstellungsansicht

Die Bereitstellungsansicht bietet dauerhaften Zugriff auf die Bereitstellungsfunktionen. Wenn Sie auf ein Element in der Bereitstellungsansicht doppelklicken, wird der Editor für dieses Element geöffnet. Die Bereitstellungsansicht dient dazu, folgende Aktionen mit den Verzeichnisabstraktionsschicht-Definitionen durchzuführen:

- *Importieren* einer oder mehrerer Objektdefinitionen aus dem Identitätsdepot.
- *Validieren* der Struktur der Datendefinitionen.
- *Bereitstellen* Ihrer Definitionen in dem Identitätsdepot, das im Projekt festgelegt wurde.
- *Erstellen und Löschen* der Verzeichnisabstraktionsschicht-Definitionen.

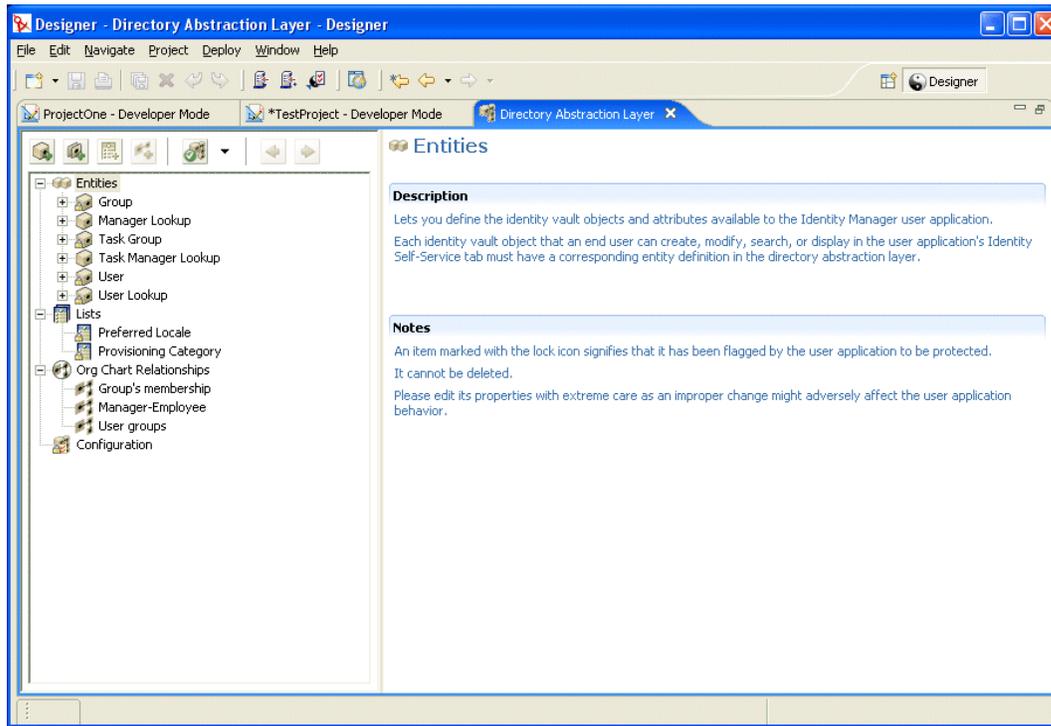
Weitere Informationen finden Sie in [Abschnitt 4.8, „Importieren, Validieren und Bereitstellen von Verzeichnisabstraktionsschicht-Definitionen“](#), auf Seite 112.

### 4.2.3 Starten des Verzeichnisabstraktionsschicht-Editors

So öffnen Sie den Verzeichnisabstraktionsschicht-Editor:

- 1 Navigieren Sie bei geöffneter *Bereitstellungsansicht* zum Verzeichnisabstraktionsschicht-Knoten.
- 2 Doppelklicken Sie auf den Verzeichnisabstraktionsschicht-Knoten.

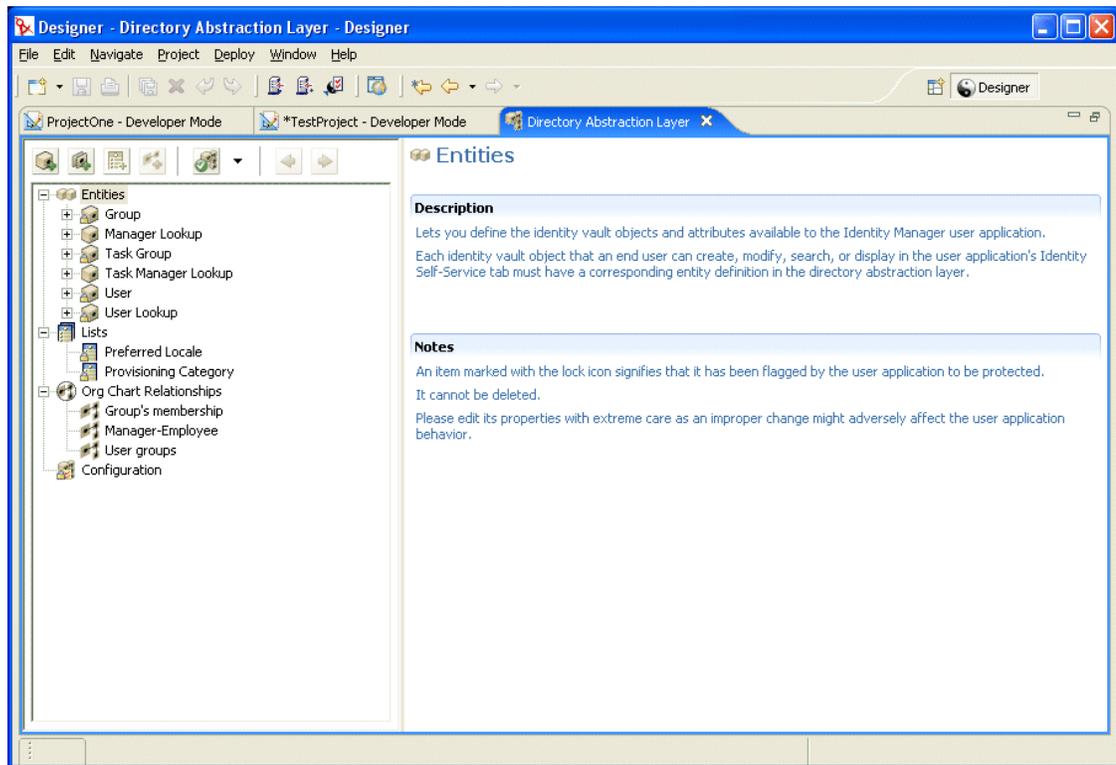
Sie sehen einen Baum, der aus Entitäten, Listen, Organigramm-Relationen und der Konfiguration besteht.



### Allgemeines zum Verzeichnisabstraktionsschicht-Editor

Der Verzeichnisabstraktionsschicht-Editor bietet eine grafische Oberfläche zum Definieren der XML-Dateien, aus denen sich die Verzeichnisabstraktionsschicht zusammensetzt. Der Verzeichnisabstraktionsschicht-Editor ist ein Eclipse-basiertes Werkzeug, auf das Sie von einer *Bereitstellungsansicht* eines Identity Manager-Projekts aus zugreifen können.

Wenn Sie den Verzeichnisabstraktionsschicht-Editor das erste Mal öffnen, finden Sie einen Standardsatz von Abstraktionsschichtobjekten vor, die immer dann automatisch erstellt werden, wenn Sie ein neues Bereitstellungsprojekt erstellen:



Es gibt folgende Knoten für den Verzeichnisabstraktionsschicht-Editor:

Element	Beschreibung
Entities	<p>Entitäten repräsentieren die Identitätsdepot-Objekte, die für dieses Projekt konfiguriert wurden und der Benutzeranwendung zur Verfügung stehen. Es gibt zwei Entitätstypen:</p> <ul style="list-style-type: none"> <li>• <b>Entitäten, die von einem Schema zugeordnet sind.</b> Diese Entitäten stellen Objekte dar, die sich im Identitätsdepot befinden und die den Benutzern über die Benutzeranwendung direkt zugänglich sind. Die Benutzer können die Attribute dieser Objekttypen für gewöhnlich erstellen, suchen und bearbeiten.</li> <li>• <b>Entitäten, die LDAP-Relationen repräsentieren.</b> Sie werden auch DNLookups genannt. Diese Entitäten stellen indizierte Suchen dar und dienen der Unterstützung bestimmter Attributtypen, die Sie freilegen möchten. DNLookup-Entitäten enthalten Informationen über Relationen zwischen LDAP-Objekten. DNLookup-Entitäten werden verwendet von: <ul style="list-style-type: none"> <li>• Dem Organigramm-Portlet zum Ermitteln von Relationen.</li> <li>• Den Suchlisten-, Erstellungs- und Detail-Portlets für Popup-Auswahllisten und DN-Kontexte.</li> </ul> </li> </ul> <p>Weitere Informationen finden Sie in <a href="#">Abschnitt 4.3.3, „Definieren von Entitäten“</a>, auf Seite 88.</p>
Lists	<p>Hier können Sie den Inhalt der globalen Listen definieren. Globale Listen:</p> <ul style="list-style-type: none"> <li>• Sind einem Attribut zugeordnet. Das Attribut ist, wenn es dort angezeigt wird, in der Benutzeranwendung als Drop-down-Liste sichtbar.</li> <li>• Dienen dem Anzeigen von Kategorien, die vom iManager-Plugin für die Konfiguration der Bereitstellungsanforderungen verwendet werden.</li> </ul> <p>Weitere Informationen finden Sie in <a href="#">Abschnitt 4.4, „Arbeiten mit Listen“</a>, auf Seite 104.</p>
Org Chart Relationships	<p>Diese werden von der Organigrammaktion der Identitätsselbstbedienungs-Registerkarte der Benutzeranwendung verwendet. Mithilfe dieser Relationen können Sie hierarchische Relationen zwischen schemabasierten Entitäten definieren.</p> <p>Weitere Informationen finden Sie in <a href="#">Abschnitt 4.5, „Arbeiten mit Organigramm-Relationen“</a>, auf Seite 107.</p>
Configuration	<p>Allgemeine Konfigurationsparameter.</p> <p>Weitere Informationen finden Sie in <a href="#">Abschnitt 4.6, „Arbeiten mit Konfigurationseinstellungen“</a>, auf Seite 110.</p>

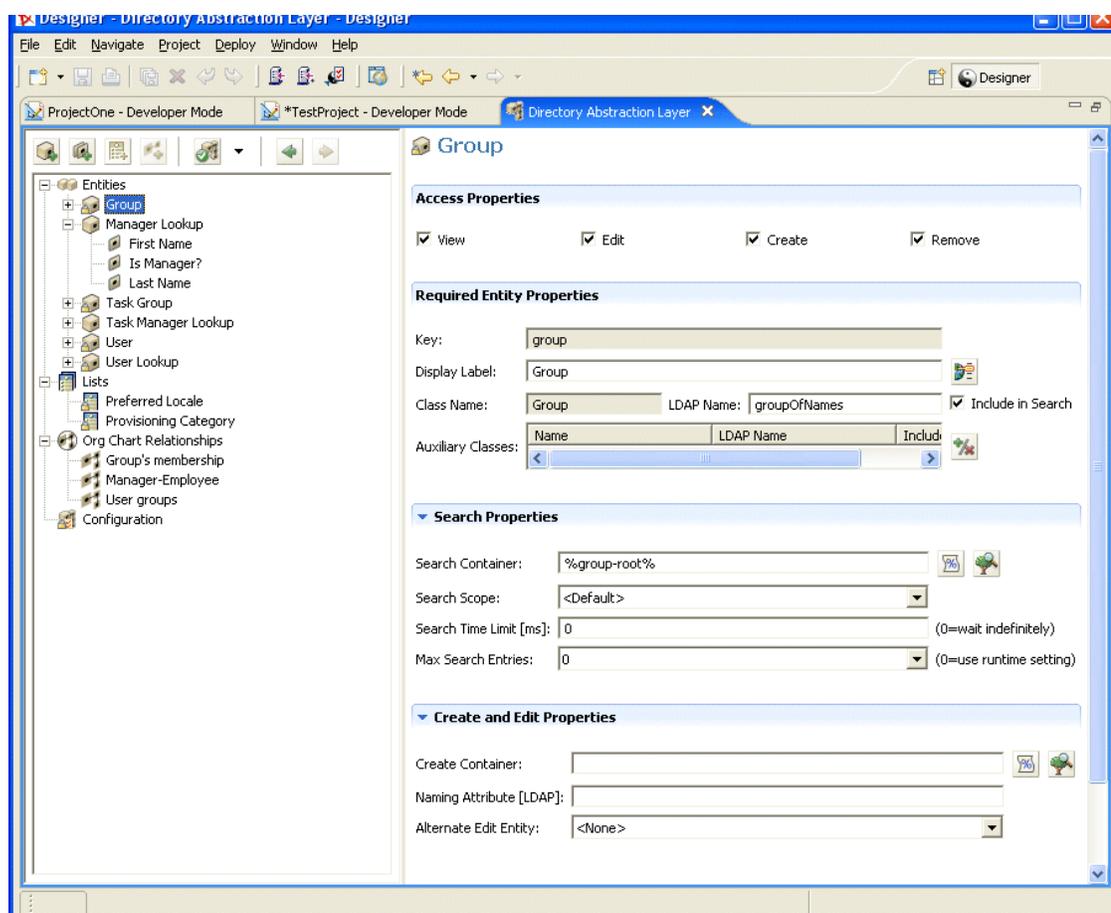
**Lokaler Speicherort der XML-Dateien** Der Verzeichnisabstraktionsschicht-Editor generiert eine einzelne XML-Datei für jede Entität, Liste oder Relation. Die Dateien werden im Projektordner „Provisioning\AppConfig\DirectoryModel“ gespeichert. Der Dateiname basiert auf dem Schlüssel des Objekts. Dazu gehören:

Verzeichnis	Beschreibung
ChoiceDefs	Enthält die Dateien, die globale Listen definieren. Diese Dateien haben die Erweiterung „.choice“.
EntityDefs	Enthält die Dateien, die die Entitäten und Attribute definieren. Diese Dateien haben die Erweiterung „.entity“.
RelationshipDefs	Enthält die Dateien, die die dem Organigramm-Portlet verfügbaren Relationen definieren. Diese Dateien haben die Erweiterung „.relation“.

Sie benötigen die Funktionen des Verzeichnisabstraktionsschicht-Editors, um neue Definitionen zu erstellen, mit denen Sie Ihr eigenes Identitätsdepot-Schema modellieren können. Sie benötigen die Funktionen der *Bereitstellungsansicht*, um neue Definitionen im Identitätsdepot bereitzustellen.

### Verwenden des Verzeichnisabstraktionsschicht-Editors

Der Verzeichnisabstraktionsschicht-Editor setzt sich aus zwei Teilfenstern zusammen. Das linke Teilfenster besteht aus einer Ansicht des Inhalts der Verzeichnisabstraktionsschicht. Wenn Sie ein Element im linken Teilfenster auswählen, werden im rechten Teilfenster die Attribute und Einstellungen des ausgewählten Elements angezeigt.



## 4.3 Arbeiten mit Entitäten und Attributen

Ein Identitätsdepot-Objekt, das Benutzer in der Identity Manager-Benutzeranwendung suchen, anzeigen oder bearbeiten sollen, muss in der Verzeichnisabstraktionsschicht als eine *Entität* definiert werden. Um beispielsweise das inetOrgPerson-Identitätsdepot-Objekt in der Benutzeranwendung zu verwenden, müssen Sie dafür eine Entitätsdefinition erstellen.

### 4.3.1 Vorgehensweise beim Hinzufügen von Entitäten

Führen Sie folgende Schritte aus, um Entitäten zur Verzeichnisabstraktionsschicht hinzuzufügen:

Schritt	Aufgabe	Weitere Informationen
1	Legen Sie fest, welche Identitätsdepot-Objekte in der Benutzeranwendung verwendet werden sollen	<a href="#">Abschnitt 4.3.2, „Analysieren der Datenerfordernisse“, auf Seite 87</a>
2	Definieren Sie mit dem Verzeichnisabstraktionsschicht-Editor die Identitätsdepot-Objekte in der Verzeichnisabstraktionsschicht	<a href="#">Abschnitt 4.3.3, „Definieren von Entitäten“, auf Seite 88</a>
3	Verwenden Sie die Bereitstellungsansicht zum Validieren der Datendefinitionen	<a href="#">Abschnitt 4.8, „Importieren, Validieren und Bereitstellen von Verzeichnisabstraktionsschicht-Definitionen“, auf Seite 112</a>
4	Stellen Sie die Definitionen im Identitätsdepot bereit	<a href="#">Abschnitt 4.8.3, „Allgemeines zur Bereitstellung“, auf Seite 115</a>
5	Aktualisieren Sie den Cache des Anwendungsservers, damit die neuen Abstraktionsschicht-Definitionen berücksichtigt werden	<a href="#">Kapitel 13, „Cache-Konfiguration“, auf Seite 219</a>
6	Testen Sie die Identity Manager-Benutzeranwendung und stellen Sie dabei sicher, dass Ihre Änderungen korrekt angezeigt werden	

### 4.3.2 Analysieren der Datenerfordernisse

Sie benötigen folgende Informationen, wenn Sie die Identitätsdepotdaten in der Verzeichnisabstraktionsschicht modellieren möchten:

- Die *Teile der Verzeichnisstruktur*, die Sie für die Identity Manager-Benutzeranwendung bereitstellen möchten.

Dies kann beispielsweise die Liste der Objekte sein, die der Benutzer suchen und anzeigen kann. Vergleichen Sie die Liste mit dem Standardsatz der Abstraktionsschicht-Definitionen. So finden Sie heraus, was Sie noch hinzufügen müssen.

- Die *Struktur des Schemas* einschließlich benutzerdefinierter Erweiterungen und Hilfsklassen
- Die *Struktur der Daten*. Dazu gehören auch folgende Informationen:
  - Was erforderlich und was optional ist
  - Validierungsregeln
  - Relationen zwischen Objekten (DN-Referenzen)

- Wie Attribute definiert werden (z. B. sollte ein Attribut, das eine Telefonnummer repräsentiert, mehrere Nummern aufnehmen können: jeweils eine Nummer für den Privatanschluss, den Büroanschluss und das Handy)
- Wer die Daten sehen darf  
Ist dies eine öffentliche oder eine private Site?

Stehen alle Informationen zur Verfügung, können Sie Ihre Identitätsdepot-Objekte den Abstraktionsschicht-Entitäten zuordnen.

---

**Hinweis:** Die eDirectory-ACLs können für alle Abstraktionsschicht-Objekte verwendet werden. Effektive Rechte an Objekten und Attributen basieren auf dem authentifizierten Benutzer, der sich bei der Anwendung angemeldet hat.

---

### 4.3.3 Definieren von Entitäten

Abhängig davon, was in der Benutzeranwendung sichtbar gemacht werden soll, müssen Sie zwei Entitätstypen definieren:

- *Entitäten, die von einem Schema zugeordnet sind.* Diese Entitäten stellen Objekte dar, die sich im Identitätsdepot befinden und die den Benutzern in der Benutzeranwendung direkt zugänglich sind. Wenn Sie eine solche Entität definieren, legen Sie alle Attribute frei, die die Benutzer bearbeiten sollen. Zu diesem Entitätstyp gehören: Benutzer, Gruppe und Aufgabengruppe. Sie können auch mehrere Entitätsdefinitionen für dasselbe Objekt erstellen, wenn Sie für verschiedene Benutzer auch jeweils verschiedene Attributsätze freigeben möchten. Weitere Informationen finden Sie unter „[Erstellen mehrerer Entitätsdefinitionen für ein einzelnes Objekt](#)“ auf Seite 88.
- *Entitäten, die LDAP-Relationen repräsentieren.* Dieser Entitätstyp ist als DNLookup bekannt und wird von der Benutzeranwendung zu folgenden Zwecken verwendet:
  - Wenn Sie mit den Ergebnissen einer DN-Suche über verwandte Entitäten eine Liste füllen möchten
  - Wenn Sie bei Änderungs- und Löschvorgängen die referentielle Integrität für DN-referenzierte Attribute sicherstellen möchten

Entitäten, die DNLookups unterstützen, werden vom Organigramm-Portlet zum Ermitteln der Relationen verwendet. Zudem werden sie von Suchlisten-, Erstellungs- und Detail-Portlets für Popup-Auswahllisten und DN-Kontexte verwendet. Beispiele für diesen Entitätstyp: Manager Lookup, Task Manager Lookup und User Lookup. Weitere Informationen finden Sie unter „[Verwenden von DNLookup-Steuerungstypen](#)“ auf Seite 101.

#### Erstellen mehrerer Entitätsdefinitionen für ein einzelnes Objekt

Sie können mehrere Entitätsdefinitionen erstellen, die ein und dasselbe Identitätsdepot-Objekt repräsentieren, aber unterschiedliche Ansichten der Daten liefern. Mit den Entitätsdefinitionen können Sie:

- *Unterschiedliche Attribute* für jede einzelne Entitätsdefinition definieren

oder

- *Dieselben Attribute definieren*, aber verschiedene Zugriffseigenschaften angeben, die steuern, wie die Attribute gesucht, angezeigt, bearbeitet oder verborgen werden

---

**Hinweis:** Die Entitätsdefinitionen können optional einen Filter enthalten, um bestimmte Entitäten aus dem Ergebnis-Set herauszufiltern.

---

Sie können diese Entitätsdefinitionen dann in den verschiedenen Teilen der Benutzeroberfläche verwenden. Angenommen, Sie möchten ein Verzeichnis der Mitarbeiter erstellen; eines für eine öffentliche Site und eines für eine interne Site. Auf der öffentlichen Site möchten Sie den Vor- und Nachnamen sowie die Telefonnummer angeben. Auf der internen Site möchten Sie darüber hinaus Informationen wie Titel, Manager usw. auflisten. Sie können diese Aufgabe wie folgt lösen:

- 1 Erstellen Sie zwei Entitätsdefinitionen (mit unterschiedlichen Schlüsseln).

Mit beiden Entitätsdefinitionen wird dasselbe Identitätsdepot-Objekt freigelegt, aber der eine Schlüssel dient öffentlich zugänglichen, der andere nur intern zugänglichen Mitarbeiterdaten.

- 2 Definieren Sie in jeder Entitätsdefinition einen unterschiedlichen Attributsatz: einen für öffentlich zugängliche und einen für nur intern zugängliche Mitarbeiterdaten.
- 3 Erstellen Sie auf der Registerkarte „Portaladministration“ der Identity Manager-Benutzeranwendung eine Portlet-Instanz für die öffentliche und eine für die interne Seite.

Weitere Informationen zum Erstellen von Portlet-Instanzen finden Sie in [Kapitel 9](#), „[Portletadministration](#)“, auf Seite 181.

## Prozeduren für das Erstellen von Entitätsdefinitionen

Wenn Sie wissen, welche Entitäten und Attribute Sie freigeben möchten, können Sie sie mit dem Editor zur Verzeichnisabstraktionsschicht hinzufügen. Folgende Schritte sind dazu erforderlich:

---

Schritt	Vorgehensweise	Siehe Prozedur
1.	Wählen Sie die Dateien aus, mit denen Sie beginnen möchten. <ul style="list-style-type: none"><li>• Sie möchten den Standardsatz der Definitionen ergänzen</li><li>• Sie möchten mit bereits implementierten Definitionen beginnen</li></ul>	<a href="#">Abschnitt 4.3.1, „Vorgehensweise beim Hinzufügen von Entitäten“, auf Seite 87</a> <a href="#">Abschnitt 4.8.1, „Allgemeines zum Importieren“, auf Seite 112</a>
1a.	Einige der Entitäten, die Sie verwenden möchten, sind nicht Teil des eDirectory-Basisschemas. Erweiterungen des eDirectory-Schemas werden in der Editorliste der auswählbaren Objekte und Attribute nicht automatisch angezeigt. Dies bedeutet, dass Sie die lokale Schemadatei des Designers aktualisieren müssen, damit diese benutzerdefinierten Objekte und Attribute berücksichtigt werden.	<a href="#">„So aktualisieren Sie die Liste der verfügbaren Schemaelemente:“ auf Seite 90</a>
2.	Fügen Sie der Verzeichnisabstraktionsschicht mindestens eine Entität hinzu	<a href="#">„Entitäten hinzufügen“ auf Seite 90</a>
3.	Versehen Sie die Entitäten mit Attributen	<a href="#">„Attribute hinzufügen“ auf Seite 93</a>

---

## Die Liste der verfügbaren Schemaelemente aktualisieren

So aktualisieren Sie die Liste der verfügbaren Schemaelemente:

- 1 Wählen Sie bei geöffnetem Identity Manager-Projekt das Identitätsdepot, klicken Sie mit der rechten Maustaste und wählen Sie *Live Operations>Import Schema*.
- 2 Wählen Sie *Import from eDirectory* und stellen Sie die Spezifikationen für den eDirectory-Host zur Verfügung.
- 3 Klicken Sie auf *Next*.
- 4 Wählen Sie die Klassen und Attribute aus, die Sie importieren möchten, und klicken Sie auf *Finish*.

## Entitäten hinzufügen

Sie können eine Entität mit dem gleichnamigen Assistenten (nachfolgend beschrieben) hinzufügen oder indem Sie in der Symbolleiste des Editors auf die Schaltfläche *Add Entity* klicken.

---

**Hinweis:** Wenn Sie die Schaltfläche „Add Entity“ verwenden, werden Sie dazu aufgefordert, die Objektklasse der Entität auszuwählen, die Sie erstellen möchten. Der Editor fügt die obligatorischen Attribute automatisch zur Entität hinzu. Sie können dann mithilfe des Dialogfelds „Add Attribute“ die Entitätsdefinition abschließen.

---

So fügen Sie eine Entität mit dem Assistenten zum Hinzufügen von Entitäten hinzu:

- 1 Sie haben folgende Möglichkeiten, den Assistenten zum Hinzufügen von Entitäten zu starten:

In der *Bereitstellungsansicht*:

- Wählen Sie den Knoten *Entities*, klicken Sie mit der rechten Maustaste und wählen Sie *New*.
- Wählen Sie *File>New>Provisioning*. Wählen Sie *Directory Abstraction Layer Entity* (Verzeichnisabstraktionsschicht-Entität). Klicken Sie auf *Next*.

Im Verzeichnisabstraktionsschicht-Editor:

- Wählen Sie den Knoten *Entities*, klicken Sie mit der rechten Maustaste und wählen Sie *New Entity-Attributes Wizard*.

Das Dialogfeld „New Entity“ wird angezeigt.

---

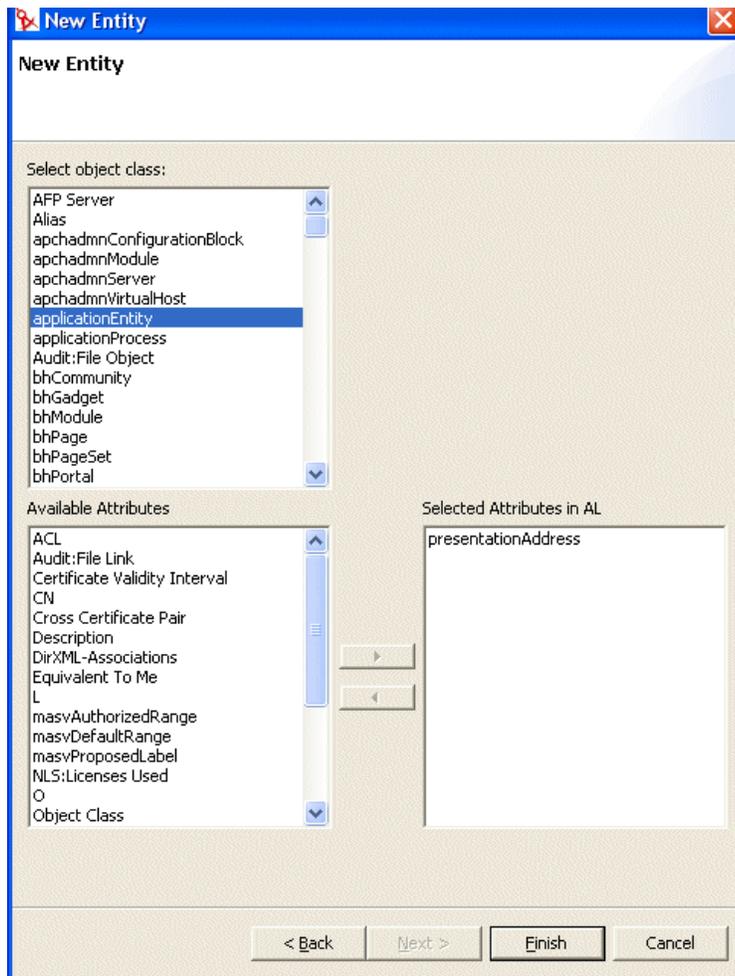
**Hinweis:** Wenn das Dialogfeld über das Dateimenü aufgerufen wird, enthält es Felder, die nicht angezeigt werden, wenn es auf eine der anderen Arten aufgerufen wird. Die folgende Abbildung zeigt das Dialogfeld.

---

**2** Machen Sie folgende Angaben:

Feld	Beschreibung
„Identity Manager Project“ und „Provisioning Application“	Wählen Sie das Identity Manager-Projekt und die Bereitstellungsanwendung aus, zu der Sie die Entität und die Attribute hinzufügen möchten.  <b>Hinweis:</b> Diese Felder werden angezeigt, wenn Sie den Assistenten über das Dateimenü aufrufen.
Entity Key	Die eindeutige ID der Entität.
Display Label	Die Zeichenkette, die angezeigt wird, wenn diese Entität über die Benutzerschnittstelle referenziert wird.

3 Klicken Sie auf *Next*. Das Dialogfeld „New Entity“ wird angezeigt:



4 Wählen Sie die Objektklasse der zu erstellenden Entität und anschließend die gewünschten Attribute aus der Liste der verfügbaren Attribute aus.

---

**Tipp:** Wenn die Objektklasse der zu erstellenden Entität in der Liste der verfügbaren Objektklassen nicht angezeigt wird, müssen Sie möglicherweise die lokale Schemadatei des Designers aktualisieren. Befolgen Sie die Anweisungen in „[So aktualisieren Sie die Liste der verfügbaren Schemaelemente:](#)“ auf Seite 90.

---

5 Klicken Sie auf *Finish*.

Das Eigenschaftsblatt wird zur Bearbeitung angezeigt.

Weitere Informationen finden Sie unter „[Entitätseigenschaften - Referenz](#)“ auf Seite 94.

---

**Hinweis:** Damit das Attribut der Benutzeranwendung zur Verfügung steht, müssen Sie die Entität bereitstellen, die das Attribut enthält.

---

## Attribute hinzufügen

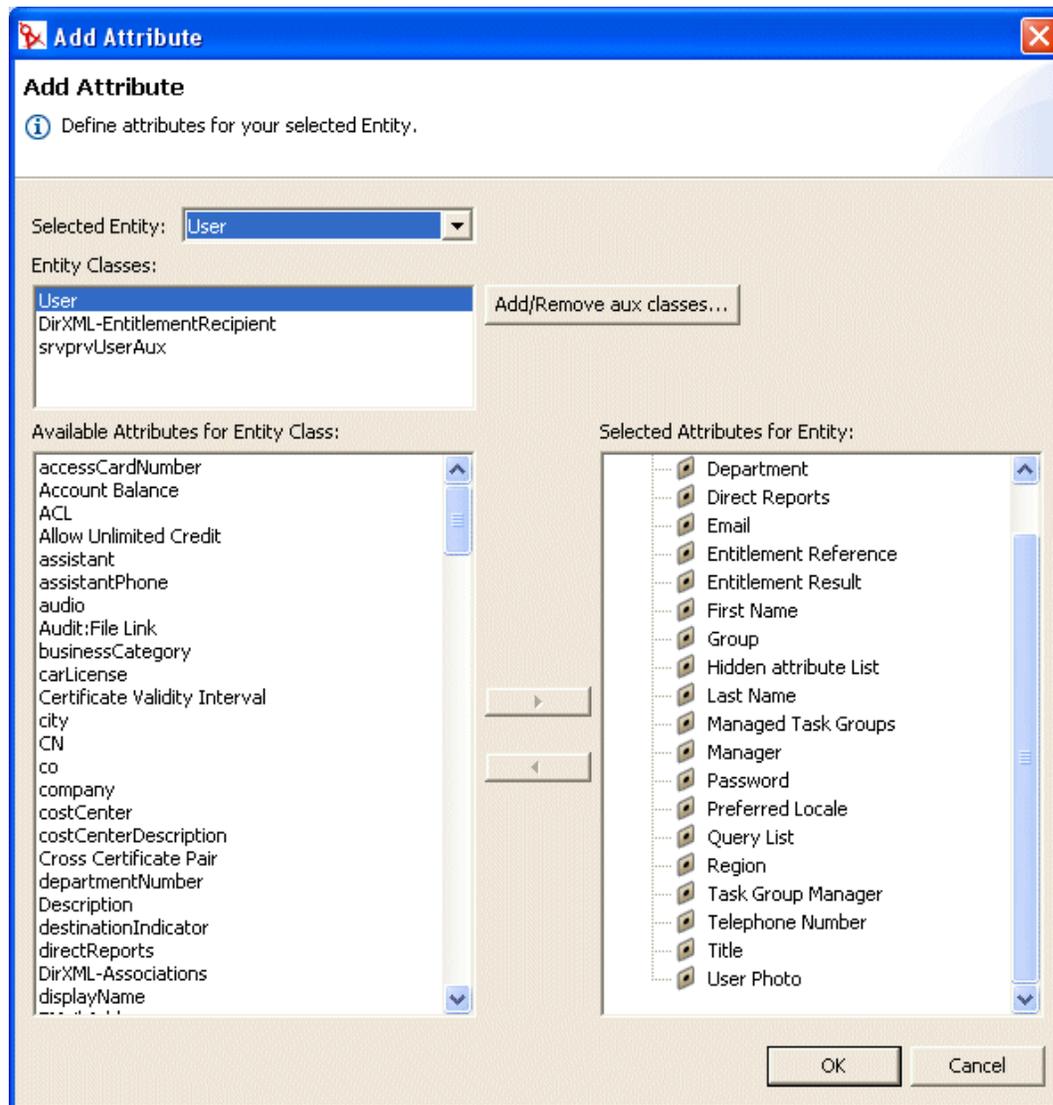
So fügen Sie ein Attribut hinzu:

- 1 Wählen Sie eine Entität aus.
- 2 Fügen Sie wie folgt ein Attribut hinzu:
  - Klicken Sie mit der rechten Maustaste und wählen Sie *Add Attribute*.

ODER:

- Klicken Sie auf das Symbol *Add Attribute*.

Folgendes Dialogfeld wird angezeigt:



- 3 Wählen Sie das gewünschte Attribut aus der Liste *Available Attributes for Entity Class* aus und fügen Sie es zur Liste *Selected Attributes for Entity* hinzu.

---

**Tipp:** Wenn das zu erstellende Attribut in der Liste der verfügbaren Attribute der Entitätsklasse nicht angezeigt wird, müssen Sie möglicherweise die lokale Schemadatei des Designers aktualisieren. Befolgen Sie die Anweisungen in [„So aktualisieren Sie die Liste der verfügbaren Schemaelemente:“](#) auf Seite 90.

---

**4** Klicken Sie auf *OK*.

Das Eigenschaftsblatt wird zur Bearbeitung angezeigt.

Weitere Informationen finden Sie unter [„Attributeigenschaften - Referenz“](#) auf Seite 97.

---

**Hinweis:** Damit das Attribut der Benutzeranwendung zur Verfügung steht, müssen Sie es bereitstellen.

---

## Entitätseigenschaften - Referenz

Sie können die folgenden Eigenschaften für Entitäten festlegen:

- [„Zugriffseigenschaften für Entitäten“](#) auf Seite 94
- [„Entitätseigenschaften für „Required“ \(Erforderlich\)“](#) auf Seite 94
- [„Entitätseigenschaften für die Suche“](#) auf Seite 95
- [„Entitätseigenschaften für das Erstellen und Bearbeiten“](#) auf Seite 96
- [„Eigenschaften für die Passwortverwaltung“](#) auf Seite 96

### Zugriffseigenschaften für Entitäten

Mit den *Zugriffseigenschaften* können Sie steuern, wie die Benutzeranwendung mit der Entität interagiert. Dazu gehören:

---

Eigenschaft	Beschreibung
Create	<b>Aktiviert</b> - Dieses Objekt kann von der Benutzeranwendung erstellt werden.
Edit	<b>Deaktiviert</b> - Dieses Objekt kann unabhängig von den zu Grunde liegenden ACLs nicht von der Benutzeranwendung geändert werden. <b>Aktiviert</b> - Dieses Objekt kann geändert werden. Dies wird aber durch die ACLs des Identitätsdepots festgelegt.
View	<b>Aktiviert</b> - Dieses Objekt kann in der Benutzeranwendung angezeigt werden.
Remove	<b>Aktiviert</b> - Dieses Objekt kann in der Benutzeranwendung gelöscht werden.

---

### Entitätseigenschaften für „Required“ (Erforderlich)

Die Entitätseigenschaften für *Required* lauten:

---

Eigenschaftsname	Beschreibung
Key	Die eindeutige ID der Entität. Der Schlüssel („key“) definiert die Art und Weise, mit der die Benutzeranwendung dieses Objekt referenziert.
Display Label	Definiert, wie das Objekt in der Benutzeroberfläche angezeigt wird.

---

Eigenschaftsname	Beschreibung
Class name	Der Klassenname des Novell Directory Service (NDS).
LDAP name	Der Klassenname des LDAP-Objekts.
Search	<b>Aktiviert</b> - Diese Entität wird bei der Suche berücksichtigt. Entitäten, die von Identitäts-Portlets (wie z. B. Entitäts-Suchliste oder Entitäts-Organigramm) in Abfragen verwendet werden, müssen ausgewählt sein.
Auxiliary Classes	Eine Liste mit null oder mehreren Hilfsklassen für diese Entität.  Wenn Sie eine Hilfsklasse hinzufügen, müssen Sie deren LDAP- und NDS-Namen angeben und festlegen, ob diese Klasse zur Suche verwendet werden kann.

## Entitätseigenschaften für die Suche

Die Entitätseigenschaften für die *Suche* lauten:

Eigenschaftsname	Beschreibung
Search Container	Der eindeutige Name des LDAP-Knotens oder Containers, bei dem die Suche starten soll (der Suchstamm). Zum Beispiel:  <code>ou=Beispiel,o=UnsereOrganisation</code>  Zum Auswählen des Containers können Sie das Identitätsdepot durchsuchen oder einen der vordefinierten Parameter verwenden, die in „ <a href="#">Vordefinierte Parameter verwenden</a> “ auf Seite 97 beschrieben werden.
Search Scope	Gibt in Relation zum Suchstamm an, wo die Suche stattfindet.  Gültige Werte:  <b>&lt;Default&gt;</b> - Dieser Suchbereich ist identisch mit der Suche nach Containern und Untercontainern.  <b>Container</b> - Die Suche wird in der Suchstamm-DN und allen Einträgen auf Suchstammebene durchgeführt.  <b>Container and subcontainers</b> - Die Suche wird in der Suchstamm-DN und in allen Untercontainern durchgeführt. Dies entspricht der Auswahl von <b>&lt;Default&gt;</b> .  <b>Object</b> - Beschränkt die Suche auf das angegebene Objekt. Mit dieser Suche kann die Existenz eines angegebenen Objekts überprüft werden.
Search Time Limit [ms]	Geben Sie einen Wert in Millisekunden für die Suchdauer an oder 0 für kein Zeitlimit.

Eigenschaftsname	Beschreibung
Max Search Entries	<p>Geben Sie die maximale Anzahl an Suchergebnissen für eine Suche an.</p> <p>Geben Sie 0 an, wenn Sie die Laufzeiteinstellung verwenden möchten.</p> <p>Empfehlungen:</p> <p>Legen Sie <b>100 bis 200</b> Ergebnisse fest. Diese Einstellungen sorgen für die beste Effizienz.</p> <p>Legen Sie <b>keinen Wert über 1000</b> fest.</p>

## Entitätseigenschaften für das Erstellen und Bearbeiten

Die *Entitätseigenschaften für das Erstellen und Bearbeiten* lauten:

Eigenschaftsname	Definition
Create Container	<p>Der Name des Containers, in dem eine neue Entität dieses Typs erstellt wird.</p> <p>Zum Auswählen des Containers können Sie das Identitätsdepot durchsuchen oder einen der vordefinierten Parameter verwenden, die in „<b>Vordefinierte Parameter verwenden</b>“ auf Seite 97 beschrieben werden.</p> <p>Ist kein Wert angegeben, fordert das Erstellungs-Portlet den Benutzer auf, einen Container für das neue Objekt zu benennen. Das Portlet verwendet den angegebenen Suchstamm in der Entitätsdefinition als Basis und ermöglicht dem Benutzer die Suche ab dieser Ebene. Wurde in der Entitätsdefinition kein Suchstamm angegeben, wird der Stamm-DN verwendet, der bei der Installation der Benutzeranwendung angegeben wurde.</p>
Naming Attribute	<p>Das Benennungsattribut der Entität (Relative Distinguished Name [RDN]). Dieser Wert ist nur für Entitäten erforderlich, wenn der Zugriffsparameter „Erstellen“ ausgewählt wurde.</p>
Alternate Edit Entity	<p>Die Attribute der Bearbeitungsentität werden im Bearbeitungsmodus des Detail-Portlets angezeigt.</p> <p>Wählen Sie eine Entität aus der Dropdown-Liste aus oder &lt;None&gt;, wenn diese Entität nicht im Detail-Portlet angezeigt wird.</p>

## Eigenschaften für die Passwortverwaltung

Die *Eigenschaften für die Passwortverwaltung* lauten:

Eigenschaftsname	Definition
Password Attribute	<p>Wählen Sie das Attribut für das Passwort dieser Entität.</p>
Password required when attribute is created	<p><b>Aktiviert</b> - Bedeutet, dass ein Passwort erforderlich ist, wenn diese Entität erstellt wird.</p>

## Vordefinierte Parameter verwenden

Der Verzeichnisabstraktionsschicht-Editor ermöglicht die Verwendung vordefinierter Parameter für bestimmte Werte. Die Parameter lauten:

Vordefinierter Parameter	Beschreibung
%driver-root%	Der Bereitstellungstreiber-DN. Dieser Wert wird beim Konfigurieren der Benutzeranwendung während der Installation oder bei einer später durchgeführten Konfiguration angegeben. Er wird in der Konfiguration des Benutzeranwendungsbereichs („realm“) gespeichert.
%user-root%	Der Benutzercontainer-DN. Dieser Wert wird beim Konfigurieren der Benutzeranwendung während der Installation oder bei einer später durchgeführten Konfiguration angegeben. Er wird in der Konfiguration des Benutzeranwendungsbereichs („realm“) gespeichert.
%group-root%	Der Gruppencontainer-DN. Dieser Wert wird beim Konfigurieren der Benutzeranwendung während der Installation oder bei einer später durchgeführten Konfiguration angegeben. Er wird in der Konfiguration des Benutzeranwendungsbereichs („realm“) gespeichert.

## Attributeigenschaften - Referenz

Sie können die folgenden Eigenschaften für Attribute festlegen:

- [„Zugriffseigenschaften für Attribute“ auf Seite 97](#)
- [„Attributeigenschaften für „Erforderlich““ auf Seite 98](#)
- [„Attributeigenschaften zum Filtern und Formatieren“ auf Seite 99](#)
- [„Attributeigenschaften für UI-Steuerelemente“ auf Seite 99](#)

## Zugriffseigenschaften für Attribute

Die *Zugriffseigenschaften für Attribute* lauten:

Name	Beschreibung
Edit	<b>Aktiviert</b> - Dieses Attribut kann in der Benutzeranwendung bearbeitet/geändert werden. Selbst wenn es ausgewählt („Wahr“) ist, kann das Attribut möglicherweise nicht bearbeitet werden, falls die zu Grunde liegenden Identitätsdepot-ACLs/effektiven Rechte dies verhindern.
Enable	<b>Deaktiviert</b> - Dieses Attribut kann von der Benutzeranwendung nicht verwendet werden. Die Einstellung entspricht dem Entfernen des Eintrags aus der Datei.

Name	Beschreibung
Hide	<p>Legt fest, ob das Auswahlfeld „Hide“ in der Benutzeranwendung aktiviert oder deaktiviert ist. Das Auswahlfeld „Hide“ ermöglicht es dem Benutzer festzulegen, ob ein Attribut (wie z. B. sein Foto) in der Anwendung angezeigt wird oder nicht.</p> <p><b>Deaktiviert</b> - Das Auswahlfeld „Hide“ ist für dieses Attribut deaktiviert, d. h. der Benutzer kann dieses Attribut nicht verstecken.</p> <p><b>Aktiviert</b> - Das Auswahlfeld „Hide“ kann in der Benutzeranwendung aktiviert werden. Zudem muss Folgendes für den angemeldeten Benutzer zutreffen. <b>***DELETE***</b></p> <ul style="list-style-type: none"> <li>• Er ist entweder der Eigentümer des Attributs oder ein Benutzeranwendungsadministrator.</li> <li>• Er hat Trustee-Rechte zum Aktualisieren des srvprvHideAttributes-Attributs im Identitätsdepot.</li> </ul> <p>Sind diese Bedingungen nicht erfüllt, ist das Auswahlfeld „Hide“ in der Benutzeroberfläche deaktiviert, selbst wenn die Einstellung aktiviert wurde („Wahr“).</p> <hr/> <p><b>Tipp:</b> Wenn ein Benutzer ein Attribut versteckt, das ein Bild enthält, können Benutzer, die das Bild bereits angesehen haben, es möglicherweise weiter sehen, bis ihr Browser-Cache aktualisiert wird.</p>
Multivalue	<p>Gibt an, ob das Attribut mehrere Werte haben kann, zum Beispiel mehrere Telefonnummern.</p> <p><b>Aktiviert</b> - Das Attribut kann mehrere Werte haben.</p>
Read	<p><b>Aktiviert</b> - Die Benutzeranwendung kann dieses Attribut abfragen. Bei den meisten Attributen sollte diese Eigenschaft aktiviert sein. Bei einigen Attributen, wie beispielsweise dem Passwort, sollte es allerdings deaktiviert sein.</p>
Require	<p><b>Aktiviert</b> - Das Attribut muss angegeben werden.</p>
Search	<p><b>Aktiviert</b> - Die Benutzeranwendung kann dieses Attribut in Suchvorgängen verwenden. Attribute, die von Identitäts-Portlets (wie z. B. Entitäts-Suchliste oder Entitäts-Organigramm) in Abfragen verwendet werden, müssen aktiviert sein.</p> <hr/> <p><b>Tipp:</b> Wenn ein in einer Suche verwendetes Attribut zudem in eDirectory indiziert ist, funktioniert die Suche schneller.</p>
View	<p><b>Aktiviert</b> - Die Benutzeranwendung kann dieses Attribut anzeigen. In den meisten Fällen trifft dies zu, aber bei einigen Attributen, wie beispielsweise Passwörtern, ist diese Eigenschaft wahrscheinlich deaktiviert.</p>

#### Attributeigenschaften für „Erforderlich“

Name	Beschreibung
Key	Die eindeutige ID des Attributs.
Display Label	Die Bezeichnung, die in der Benutzeranwendung angezeigt wird.
Attribute Name	Der NDS-Name dieses Attributs.
LDAP Name	Der LDAP-Name dieses Attributs.

## Attributeigenschaften zum Filtern und Formatieren

Name	Beschreibung
Filter: WHERE Attribut	Sie können hier einen LDAP-Filter für die Suche im Identitätsdepot angeben.
Enable	<b>Aktiviert</b> - Aktiviert den Filter.

## Attributeigenschaften für UI-Steuererelemente

Name	Beschreibung
Data Type	<p>Wählen Sie aus der folgenden Liste einen Datentyp:</p> <ul style="list-style-type: none"><li>• Binary</li><li>• Boolean</li><li>• DN</li><li>• Integer</li><li>• LocalizedString</li><li>• String</li><li>• Time</li></ul>
Format Type	<p>Wird von der Benutzeranwendung zum Formatieren der Daten verwendet. Zu den Formattypen gehören:</p> <ul style="list-style-type: none"><li>• Kein</li><li>• AOL IM</li><li>• Email</li><li>• Groupwise IM</li><li>• Image</li><li>• Phone Number</li><li>• Yahoo IM</li><li>• Image URL</li><li>• Date</li><li>• DateTime</li></ul>

Die Formattypen hängen vom Datentyp ab. Dem Zeit-Datentyp können beispielsweise nur die Formate „Date“ und „DateTime“ zugeordnet werden.

Name	Beschreibung
Control Type	<p>Zu den Typen gehören:</p> <p><b>DNLookup</b> - Definiert, dass dieses Attribut eine DN-Referenz enthält. Verwenden Sie die Eigenschaft in folgenden Fällen:</p> <ul style="list-style-type: none"> <li>• Wenn Sie mit den Ergebnissen einer DN-Suche über verwandte Entitäten eine Liste füllen möchten</li> <li>• Wenn Sie bei Änderungs- und Löschvorgängen die referentielle Integrität für DN-referenzierte Attribute sicherstellen möchten</li> </ul> <p>Die Benutzeranwendung verwendet diese Informationen zum Generieren bestimmter Elemente der Benutzerschnittstelle und für optimierte Suchvorgänge, die auf der DNLookup-Definition basieren.</p> <p>Weitere Informationen finden Sie unter <a href="#">„Verwenden von DNLookup-Steuerungstypen“ auf Seite 101</a>.</p> <p><b>Global List</b> - Zeigt dieses Attribut als eine Dropdown-Liste an, deren Inhalt in einer Datei außerhalb dieser Attributdefinition definiert wird.</p> <p>Weitere Informationen finden Sie in <a href="#">Abschnitt 4.4, „Arbeiten mit Listen“, auf Seite 104</a>.</p> <p><b>Local List</b> - Zeigt dieses Attribut als eine Dropdown-Liste an, deren Inhalt mit diesem Attribut definiert wird. So definieren Sie eine lokale Liste:</p> <ol style="list-style-type: none"> <li>1. Stellen Sie bei ausgewähltem Attribut den Steuerungstyp („Control Type“) auf „Local List“ ein.</li> </ol>  <ol style="list-style-type: none"> <li>2. Klicken Sie auf „Add“, um mehr Werte hinzuzufügen. Mit den Pfeiltasten können Sie die Position des Elements in der Liste ändern.</li> </ol> <p>Geben Sie in der Wertspalte den Wert ein, der im Identitätsdepot gespeichert werden soll. Es sind nur Kleinbuchstaben, Zahlen und der Unterstrich ( _ ) zulässig.</p> <ol style="list-style-type: none"> <li>3. Geben Sie in der Bezeichnungsspalte den Text ein, der in der Benutzeroberfläche angezeigt werden soll.</li> </ol> <p><b>Range</b> - Verwenden Sie den „Control Type“ „Range“ mit Integer-Datentypen, um die Benutzereingabe auf einen zusammenhängenden Wertebereich zu beschränken. Sie müssen den Anfangs- und Endwert des Zahlenbereichs angeben.</p>

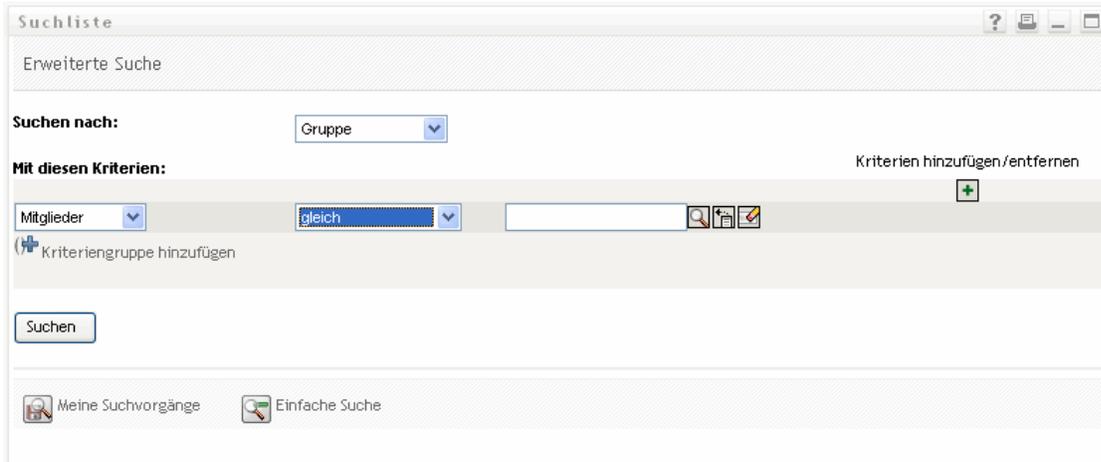
## Verwenden von DNLookup-Steuerungstypen

Wenn Sie einen Steuerungstyp („control type“) als DNLookup definieren, bedeutet dies Folgendes:

- Benutzer können einen Wert aus einer Liste möglicher Werte auswählen, wenn sie in diesem Attribut suchen.
- Wenn dieses Attribut erstellt, gefüllt oder gelöscht wird, werden Attribute verwandter Entitäten je nach Benutzeraktion (Erstellen, Löschen, Aktualisieren) entsprechend aktualisiert, damit die referentielle Integrität erhalten bleibt.

### DNLookups für Auswahllisten

Die installierte Benutzeranwendung enthält Entitätsdefinitionen für Benutzer und Gruppen. Die Entitätsdefinition des Benutzers enthält ein Gruppenattribut, das als DNLookup-Steuerungstyp definiert ist. Dadurch kann jedes Identitäts-Portlet einem bestimmten Benutzer eine Auswahlliste mit Gruppen zur Verfügung stellen. Beispielsweise möchte ein Benutzer eine Verzeichnissuche durchführen. Er möchte einen Benutzer in einer bestimmten Gruppe suchen, aber er kennt den Namen der Gruppe nicht. Der Benutzer würde in diesem Fall „User“ als zu suchendes Objekt und „Group“ als ein Suchkriterium angeben:



The screenshot shows a search interface titled "Suchliste" with a window title bar containing a question mark, a print icon, and a close icon. The main content area is titled "Erweiterte Suche". Below this, there is a section "Suchen nach:" with a dropdown menu set to "Gruppe". Underneath, the section "Mit diesen Kriterien:" is displayed, with a link "Kriterien hinzufügen/entfernen" and a green plus icon. The criteria list includes "Mitglieder" (dropdown), "gleich" (dropdown), and an empty text input field. Below the criteria list is a link "Kriteriengruppe hinzufügen" with a plus icon. A "Suchen" button is located below the criteria list. At the bottom of the interface, there are two icons: "Meine Suchvorgänge" and "Einfache Suche".

Da „Group“ als DNLookup-Steuerungstyp für die Benutzerentität definiert ist, wird das Lookup-Symbol angezeigt. Wenn der Benutzer es auswählt, wird eine Gruppenliste angezeigt:

Vorname	Nachname
Abby	Spencer
Admin	idmsample
Alison	Blake
Angie	Chung
Anthony	Palini
April	Smith

Der Benutzer kann eine Gruppe aus der Liste auswählen.

#### DNLookups für referentielle Integrität

DNLookups für Aktualisierungen und zur Synchronisierung sind wichtig, weil LDAP die Zuordnung von Gruppenrelationen in beide Richtungen ermöglicht. So können Ihre Daten beispielsweise wie folgt eingerichtet sein:

- Das Benutzerobjekt enthält ein Gruppenattribut. Das Gruppenattribut:
  - Besteht aus mehreren Werten
  - Listet alle Gruppen auf, zu denen ein Benutzer gehört
- Das Gruppenobjekt enthält ein Benutzerattribut. Das Benutzerattribut:
  - Besteht aus mehreren Werten
  - Listet alle Benutzer auf, die zu dieser Gruppe gehören

Sie können also ein Attribut für ein Benutzerobjekt haben, das alle Gruppen auflistet, zu denen ein Benutzer gehört. Außerdem hat das Gruppenobjekt ein DN-Attribut, das alle Mitglieder dieser Gruppe enthält.

Wenn der Benutzer eine Aktualisierung anfordert, muss die Benutzeranwendung die Relationen berücksichtigen und sicherstellen, dass die Ziel- und Ursprungsattribute synchronisiert werden. In DNLookup geben Sie beide Attribute an, die synchronisiert werden müssen. Mit diesem Verfahren können Sie nicht nur Objekte in einer Gruppenstruktur, sondern alle Objekte, die Relationen aufweisen, synchronisieren. Sie erstellen diese Art des DNLookup-Steuerungstyps mithilfe der

erweiterten DNLookup-Eigenschaften, die in der Referenz für die *Eigenschaften zur Bewahrung der relationalen Integrität bei DNLookup* beschrieben werden.

## DNLookup-Eigenschaften - Referenz

Die DNLookup-Anzeigeeigenschaften lauten:

Feld	Definition
Lookup Entity	Der Name der Suchentität. Die Aufgabengruppen-Entität („Task Group Entity“) enthält beispielsweise ein Attribut für den Aufgabenmanager. Um dieses Feld zu bestücken, müssen Sie wissen, welche Benutzer Aufgabenmanager sind.
Detail entity	Der Schlüssel der Entität, deren Details angezeigt werden sollen, wenn der Benutzer durch Klicken auf eine Hypertext-Verbindung in der Benutzeranwendung mehr Informationen anfordert. Wenn Sie ein DNLookup definieren, können die Identitäts-Portlets eine Hypertext-Verbindung bereitstellen, mit denen Benutzer die Details des verbundenen Objekts anzeigen können.
Attributes to display	Wählen Sie mindestens ein Attribut, das angezeigt werden soll, wenn der Suchvorgang abgeschlossen wurde.
Perform Automatic Query	Definiert, wie die <b>anzuzeigenden Attribute</b> (siehe oben) angezeigt werden. <ul style="list-style-type: none"> <li>• <b>Aktiviert</b> - Führt eine automatische Abfrage über die Entität aus und zeigt die Ergebnisse in einer Liste an, aus der eine Auswahl getroffen werden kann. Sie sollten diese Option nicht verwenden, wenn davon auszugehen ist, dass das Ergebnis-Set sehr umfangreich ausfallen wird, da der Benutzer dann sehr viel blättern muss.</li> <li>• <b>Deaktiviert</b> - Ermöglicht dem Benutzer die Angabe der Suchkriterien für die Entitätsabfrage und präsentiert die Ergebnisse in einer Liste, aus der eine Auswahl getroffen werden kann.</li> </ul>

*Eigenschaften zur Bewahrung der relationalen Integrität bei DNLookup* - Diese Eigenschaften dienen der Synchronisierung der Daten zwischen zwei Objekten wie z. B. Gruppen und Gruppenmitgliedern.

Eigenschaft	Definition
Source attributes to update	Name des zu aktualisierenden Attributs. Das Attribut muss eine DN-Referenz zu den zu aktualisierenden Zielattributen („ <b>Target attributes to update</b> “) enthalten. Dies ist zur Synchronisierung der Attribute zweier verschiedener Objekte erforderlich.
Target attributes to update	Der Name des Attributs, das aktualisiert werden muss, sowie die zu aktualisierenden Ursprungsattribute („ <b>Source attributes to update</b> “). Der Name ist ein LDAP-Attributname. Dies ist zur Synchronisierung der Attribute zweier verschiedener Objekte erforderlich. Das Attribut muss eine DN-Referenz enthalten.

---

Eigenschaft	Definition
Target auxiliary classes, if any	Der Name der Hilfsklasse, die die aktualisierenden Zielattribute („Target attributes to update“) enthält.

---

## 4.4 Arbeiten mit Listen

Mit dem Listenknoten können Sie den Inhalt globaler Listen definieren. Die Identity Manager-Benutzeranwendung verwendet globale Listen für Folgendes:

- Zum Bereitstellen einer Werteliste für ein Attribut. Wenn das Attribut zur Bearbeitung in der Benutzeroberfläche angezeigt wird, werden die möglichen Werte in einer Dropdown-Liste zur Auswahl bereitgestellt.
- Zum Definieren von Kategorien, die dem iManager-Plugin für die Konfiguration der Bereitstellungsanforderungen zur Verfügung stehen. Dies ist eine besondere Liste. Weitere Informationen finden Sie in [Abschnitt 4.4.2, „Allgemeines zur Bereitstellungskategorieliste“, auf Seite 107](#).

So erstellen Sie eine neue globale Liste:

- 1 Sie haben folgende Möglichkeiten, den Assistenten für neue Listen zu starten:

In der *Bereitstellungsansicht*:

- Wählen Sie *File>New>Provisioning*. Wählen Sie *Directory Abstraction Layer List*. Klicken Sie auf *Next*.
- Wählen Sie den Knoten *Lists*, klicken Sie mit der rechten Maustaste und wählen Sie *New*.

Im *Verzeichnisabstraktionsschicht-Editor*:

- Klicken Sie auf die Schaltfläche *New List*.
- Wählen Sie den Listenknoten, klicken Sie mit der rechten Maustaste und wählen Sie *Add List*.

Das Dialogfeld „New List“ wird angezeigt.

---

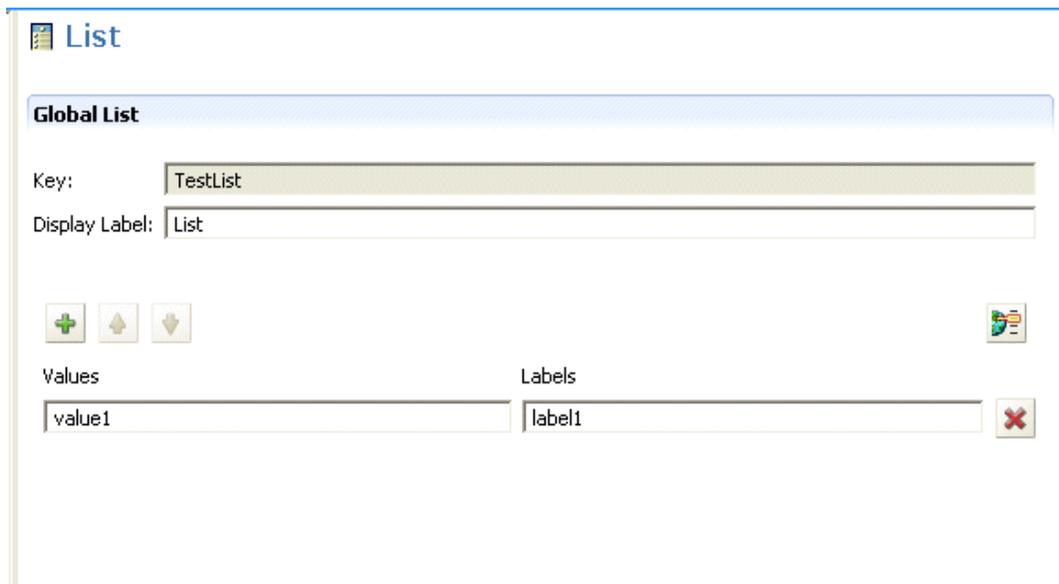
**Hinweis:** Wenn das Dialogfeld über das Dateimenü aufgerufen wird, enthält es Felder, die nicht angezeigt werden, wenn es auf eine der anderen Arten aufgerufen wird.

---

## 2 Machen Sie folgende Angaben:

Feld	Beschreibung
„Identity Manager Project“ und „Provisioning Application“	Wählen Sie das Identity Manager-Projekt und die Bereitstellungsanwendung aus, zu der Sie die Entität und die Attribute hinzufügen möchten.  <b>Hinweis:</b> Diese Felder werden angezeigt, wenn Sie den Assistenten über das Dateimenü aufrufen.
List Key	Die eindeutige ID der Liste.
Display Label	Die Zeichenkette, die verwendet wird, wenn diese Liste über die Benutzerschnittstelle referenziert wird.

3 Klicken Sie auf *Finish*. Das Eigenschaftsblatt für globale Listen wird angezeigt.



4 Vervollständigen Sie folgende Felder:

Feld	Beschreibung
Display Label	Der Name dieser Liste, wie er im Designer angegeben ist.
Labels	Der Text des Listenelements, das in der Benutzeroberfläche angezeigt werden soll.
Values	Der Wert des Listenelements, der im Identitätsdepot gespeichert werden soll. Es sind nur Kleinbuchstaben, Zahlen und der Unterstrich ( _ ) zulässig.

Die Liste ist nun in der Design-Umgebung verfügbar.

5 Speichern Sie das Projekt.

**Hinweis:** Damit die Liste der Laufzeitumgebung zur Verfügung steht, müssen Sie sie bereitstellen.

#### 4.4.1 Allgemeines zur Preferred Locale-Liste

Die Preferred Locale-Liste enthält die Standardsprache, die verwendet wird, wenn die Browsersprache nicht zu den unterstützten Sprachen gehört. Der Inhalt dieser Liste wird von der Standardkonfiguration der Aktion „Benutzer bearbeiten“ in der Benutzeranwendung angezeigt.

## 4.4.2 Allgemeines zur Bereitstellungskategorieliste

Die Bereitstellungskategorieliste definiert die Kategorien, die Sie zur Verwaltung der bereitstellbaren Ressourcen (Berechtigungen) und der Bereitstellungsanforderungen einsetzen können. Die Kategorien in dieser Liste werden angezeigt in:

- *iManager* - Plugin für die Konfiguration der Bereitstellungsanforderungen
- *Benutzeranwendung* - Registerkarte „Anforderungen und Genehmigungen“

Sie können den Bereitstellungsanforderungs-Listenschlüssel nicht ändern, aber Sie können mehr Elemente zur Liste hinzufügen oder die vorhandenen Kategoriewerte und -bezeichnungen ändern.

So ändern Sie den Inhalt der Bereitstellungskategorieliste:

- 1 Stellen Sie sicher, dass das gewünschte Projekt im Editor geöffnet ist.
- 2 Klicken Sie auf den Listenknoten.
- 3 Wählen Sie *Provisioning Category*.
- 4 Nehmen Sie die Änderungen im Eigenschaftsfenster für globale Listen vor.

---

**Hinweis:** Der Categorieschlüssel wird mit den Werten des Wertefelds bestückt. Im Wertefeld sind nur Kleinbuchstaben, Zahlen und der Unterstrich (\_) zulässig, da dies die einzig gültigen Zeichen für den Categorieschlüssel sind. Der Categorieschlüssel wird intern als Bezeichner (ID) der Kategorie verwendet.

---

- 5 Speichern und verteilen Sie dann die Änderungen. Vergessen Sie nicht, den Cache des Anwendungsservers zu aktualisieren.  
Sobald die Änderungen verteilt wurden, stehen sie in der Benutzeranwendung und im iManager-Plugin zur Verfügung.

## 4.5 Arbeiten mit Organigramm-Relationen

Der Knoten für die Organigramm-Relationen dient dazu, hierarchische Relationen zwischen Entitäten, die in der Verzeichnisabstraktionsschicht definiert sind, herzustellen. Es können Relationen zwischen Entitäten gleichen Typs (wie z. B. Benutzer/Benutzer) oder zwischen Entitäten unterschiedlicher Typen (wie z. B. Benutzer/Gerät) hergestellt werden.

Folgende Relationen sind für die Benutzeranwendung definiert:

- Gruppenmitgliedschaft
- Manager-Mitarbeiter
- Benutzergruppen

Damit eine Relation erfolgreich implementiert werden kann, müssen alle Komponenten (Entitäten und Attribute) der Relation bereits implementiert sein.

So erstellen Sie eine neue Relation:

- 1 Sie haben folgende Möglichkeiten, eine neue Relation zu erstellen:

In der *Bereitstellungsansicht*:

- Wählen Sie *File>New>Provisioning*. Wählen Sie *Directory Abstraction Layer Relationship* und klicken Sie auf *Next*.

- Wählen Sie den Knoten *Org Chart Relationships*, klicken Sie mit der rechten Maustaste und wählen Sie *Add*.

Im *Verzeichnisabstraktionsschicht-Editor*:

- Klicken Sie auf die Schaltfläche *Add Relationship*.
- Wählen Sie den Knoten *Org Chart Relationships*, klicken Sie mit der rechten Maustaste und wählen Sie *Add Relationship*.

Das Dialogfeld „New Relationship“ wird angezeigt.

---

**Hinweis:** Wenn das Dialogfeld über das Dateimenü aufgerufen wird, enthält es Felder, die nicht angezeigt werden, wenn es auf eine der anderen Arten aufgerufen wird.

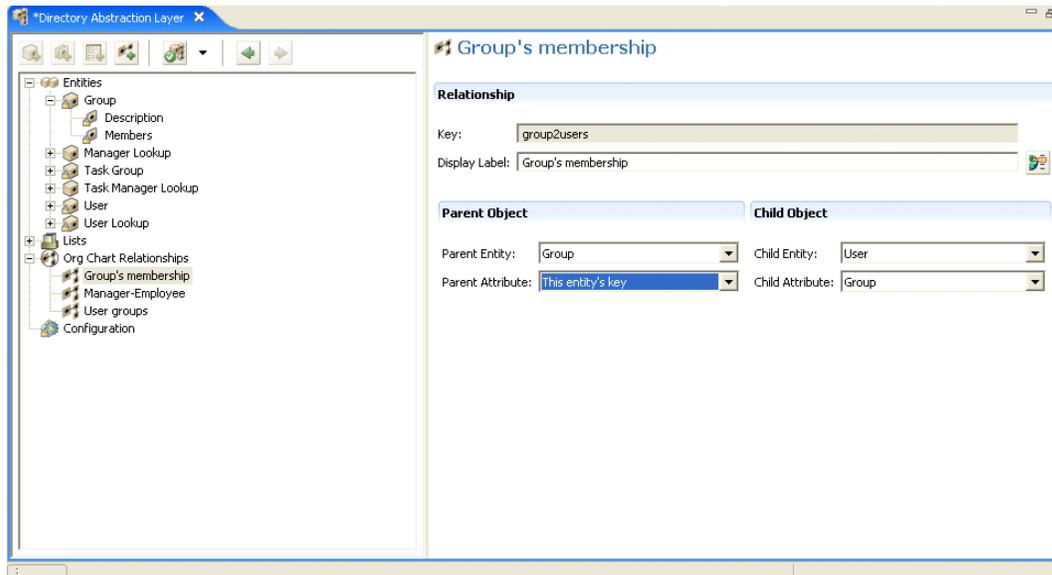
---

## 2 Machen Sie folgende Angaben:

Feld	Vorgehensweise
„Identity Manager Project“ und „Provisioning Application“	Stellen Sie sicher, dass das richtige Identity Manager-Projekt und die richtigen Bereitstellungsanwendungen („Provisioning Applications“) ausgewählt sind.  <b>Hinweis:</b> Dieses Feld wird angezeigt, wenn Sie Relationen über das Dateimenü erstellen.
Relationship Key	Geben Sie für den Relationsschlüssel einen eindeutigen Wert ein.
Display Label	Geben Sie die Zeichenkette ein, die immer dann angezeigt wird, wenn die Relation in der Identity Manager-Benutzeroberfläche sichtbar ist.

## 3 Klicken Sie auf *Finish*.

Die Relation wird erstellt und das zugehörige Eigenschaftsblatt wird zum Bearbeiten geöffnet.



## 4.5.1 Relationseigenschaften - Referenz

Feld	Beschreibung
Key	<p>Die schreibgeschützte, eindeutige ID für die Relation.</p> <p><b>Tipp:</b> Sie geben diesen Wert in den Einstellungen des Organigramm-Portlets an.</p>
Display Label	<p>Geben Sie einen Namen an, der angezeigt wird, wenn diese Relation von anderen Identitäts-Portlets referenziert wird. Dieser Wert wird beispielsweise angezeigt, wenn Benutzer im Detail-Portlet auf das Symbol zum Wählen des Organigramms klicken.</p> <p>Klicken Sie auf <b>Localize</b>, um die Übersetzung des Texts anzugeben.</p>
Parent entity	<p>Wählen Sie eine Entität aus der Dropdown-Liste aus.</p> <p>Die ausgewählte Entität wird zum übergeordneten Objekt in der Hierarchie des Organigramms. Zum Beispiel wäre in einer Manager-Mitarbeiter-Relation die übergeordnete Entität „User“. In einer Gruppe-Mitglied-Relation wäre beispielsweise die übergeordnete Entität „Group“.</p> <p><b>Verzeichnisabstraktionsschicht-Anforderungen</b> - Die Entitäten in dieser Liste sind eine Teilmenge der Entitäten, die in der Verzeichnisabstraktionsschicht definiert sind. Bei übergeordneten Entitäten muss die Zugriffseigenschaft aktiviert sein.</p>

Feld	Beschreibung
Parent attribute	<p>Wählen Sie ein Attribut aus der Dropdown-Liste aus.</p> <p>Dieses Attribut dient dazu, übereinstimmende untergeordnete Entitäten zu finden. Wenn der Wert dieses Attributs mit dem entsprechenden Wert eines Attributs einer untergeordneten Entität (siehe „Untergeordnetes Attribut“ unten) übereinstimmt, kann eine Relation hergestellt werden.</p> <p><b>Verzeichnisabstraktionsschicht-Anforderungen</b> - Diese Attributliste wird mit den ausgewählten Attributen der übergeordneten Entität bestückt. Sie enthält nur die Attribute, die als DNLookup-Steuerungstyp definiert sind.</p>
Child entity	<p>Wählen Sie die Entität, die das untergeordnete Objekt in der Hierarchie darstellt. In einer Manager-Mitarbeiter-Relation wäre dies beispielsweise „User“. In einer Mitarbeiter-Ressourcen-Relation wäre dies beispielsweise „Devices“</p> <p>Diese Entität muss das Attribut enthalten, das mit dem übergeordneten Attribut verwandt ist.</p>
Child attribute	<p>Wählen Sie das Attribut, das zum übergeordneten Attribut passt.</p> <p>Damit wird das zu verwendende Attribut der untergeordneten Entität spezifiziert, mit dem die übereinstimmenden übergeordneten Entitäten gesucht werden. Wenn der Wert dieses Attributs mit dem entsprechenden Wert eines Attributs einer übergeordneten Entität (siehe „Parent Attribute“ oben) übereinstimmt, kann eine Relation hergestellt werden.</p>

**Hinweis:** Dynamische Gruppen werden vom Organigramm-Portlet nicht vollständig unterstützt. Sie können eine dynamische Gruppe nicht als übergeordnete, aber als untergeordnete Entität in einer Relation definieren.

So löschen Sie eine Relation:

- 1 Wählen Sie die zu löschende Relation aus.
- 2 Klicken Sie mit der rechten Maustaste und wählen Sie *Delete*.

## 4.6 Arbeiten mit Konfigurationseinstellungen

Der Konfigurationsknoten ermöglicht das Festlegen allgemeiner Konfigurationseigenschaften für die Benutzeranwendung. Dazu gehören:

Eigenschaft	Beschreibung
Default 'My Profile' Entity	<p>Definiert die Entität, die angezeigt wird, wenn der Benutzer in der Benutzeroberfläche auf <b>My Profile</b> klickt.</p> <p>Dieses Feld enthält nur Entitäten, deren Objektklasse „User“ (oder „LDAP inetOrgPerson“) ist.</p>

Eigenschaft	Beschreibung
Default Locale	Definiert die Standardsprache für die Anzeigebezeichnungen in der Benutzeranwendung. Wenn für den Browser eine nicht unterstützte Sprache eingestellt ist, wird stattdessen diese Ländereinstellung verwendet.  <b>Hinweis:</b> Die Ländereinstellung des Browsers hat Vorrang vor der Standard-Ländereinstellung für die unterstützten Sprachen.
Container Classes	Enthält die Aktion zum Erstellen von Benutzern oder Gruppen („Create User or Group“) mit einer Auswahlliste für Containerklassen. Der Benutzer wählt aus der Auswahlliste einen Container als Speicherort für die neu erstellten Objekte aus.

## 4.7 Anzeigetext lokalisieren

Der Verzeichnisabstraktionsschicht-Editor ermöglicht das Lokalisieren des Anzeigetexts für:

- Anzeigebezeichnungen für Entitäten und Attribute
- Organigramm-Relationsnamen
- Elemente von globalen und lokalen Listen

### 4.7.1 Unterstützte Sprachen

Sie können den Anzeigetext in einer oder mehreren dieser Sprachen lokalisieren:

- Englisch
- Französisch
- Deutsch
- Italienisch
- Japanisch
- Koreanisch
- Portugiesisch
- Russisch
- Chinesisch (Vereinfacht)
- Spanisch
- Chinesisch (Traditionell)

### 4.7.2 Lokalisieren von Text

Der Verzeichnisabstraktionsschicht-Editor bietet mehrere Methoden zum Lokalisieren der Abstraktionsschicht-Definitionen. Sie haben folgende Möglichkeiten, auf die Lokalisierungs-Dialogfelder zuzugreifen:

Lokalisieren des Texts für	Aktion
Jedes lokalisierbare Element in der Verzeichnisabstraktionsschicht	<ul style="list-style-type: none"> <li>Klicken Sie auf <b>Set Global Localization</b> (in der Symbolleiste des Verzeichnisabstraktionsschicht-Editors).</li> </ul> <p>Wählen Sie zuerst die Zielsprache, bevor Sie den lokalisierten Text in das Zielfeld eingeben.</p>
Eine bestimmte Entität, Relation oder Liste	<ul style="list-style-type: none"> <li>Wählen Sie in der Baumansicht des Verzeichnisabstraktionsschicht-Editors das zu lokalisierende Objekt aus.</li> <li>Klicken Sie mit der rechten Maustaste und wählen Sie <b>Localize</b>.</li> </ul> <p>Wählen Sie zuerst die Zielsprache, bevor Sie den lokalisierten Text in das Zielfeld eingeben.</p>
Eine einzelne Anzeigebezeichnung	<ul style="list-style-type: none"> <li>Wählen Sie eine bestimmte Entität oder ein bestimmtes Attribut aus.</li> <li>Klicken Sie auf <b>Localize Display Label</b> (neben dem Feld „Display Label“ im Eigenschaftsfenster).</li> </ul>

Die Dialogfelder können sich geringfügig unterscheiden, enthalten aber alle die folgenden Felder:

- *Origin* - Dies ist in der Regel der Objekttyp (wie z. B. eine Entität, Liste oder Relation) und der Schlüssel
- *Source* - Der zu übersetzende Text (Anzeigebezeichnung)
- *Target Language* - Eine der unterstützten Sprachen
- *Target* - Die Übersetzung

## 4.8 Importieren, Validieren und Bereitstellen von Verzeichnisabstraktionsschicht-Definitionen

Das Importieren, Validieren und Bereitstellen von Verzeichnisabstraktionsschicht-Definitionen sind Aktionen, die in der Bereitstellungsansicht des Designers ausgeführt werden.

- [Abschnitt 4.8.1, „Allgemeines zum Importieren“, auf Seite 112](#)
- [Abschnitt 4.8.2, „Allgemeines zur Validierung“, auf Seite 115](#)
- [Abschnitt 4.8.3, „Allgemeines zur Bereitstellung“, auf Seite 115](#)

### 4.8.1 Allgemeines zum Importieren

Mit der Importfunktion können Sie vorhandene Definitionen importieren. Importieren Sie in folgenden Fällen:

- Wenn Sie auf Basis eines bereitgestellten Projekts ein neues Projekt beginnen möchten.
- Wenn Sie gemeinsam mit anderen Entwicklern, die an demselben Projekt arbeiten, Definitionen nutzen möchten. Beispielsweise kann ein anderer Entwickler ein Attribut zur Benutzerentität hinzufügen oder eine neue globale Liste für alle Entwickler bereitstellen. Wenn

der Entwickler die neue Definition im Identitätsdepot bereitstellt, können Sie sie importieren und damit sicherstellen, dass sie beide identische Definitionen verwenden.

So importieren Sie vorhandene Definitionen:

- 1 Öffnen Sie die *Bereitstellungsansicht*.
- 2 Entscheiden Sie, was Sie importieren möchten:
  - Einen vollständigen Definitionssatz
  - Einen Satz einer Definitionsart, wie z. B. alle Entitäten oder alle Relationen.
  - Ein bestimmtes Objekt (wie z. B. die Benutzerentität)
- 3 Zum Importieren:
  - Eines bestimmten Objekts wählen Sie es aus der Liste aus, klicken Sie mit der rechten Maustaste und wählen Sie *Import Object*.
  - Eines kompletten Definitionssatzes wählen Sie den Verzeichnisabstraktionsschicht-Knoten, klicken Sie mit der rechten Maustaste und wählen Sie *Import All* oder *Import Object*.
- 4 Klicken Sie auf das eDirectory-Symbol zum Durchsuchen, navigieren Sie zum DirectoryModel-Knoten und wählen Sie die zu importierenden Objekte aus. Klicken Sie anschließend auf *OK*.
  - Stimmen die Objekte überein, werden Sie darüber benachrichtigt, dass es keine Unterschiede gibt, und der Importvorgang wird nicht fortgesetzt.
  - Stimmen die Objekte nicht überein, können Sie bestätigen, welche Objekte importiert werden sollen. Überprüfen Sie die Elemente, die zum Import ausgewählt wurden, nehmen Sie bei Bedarf Änderungen vor und klicken Sie anschließend auf *OK*.

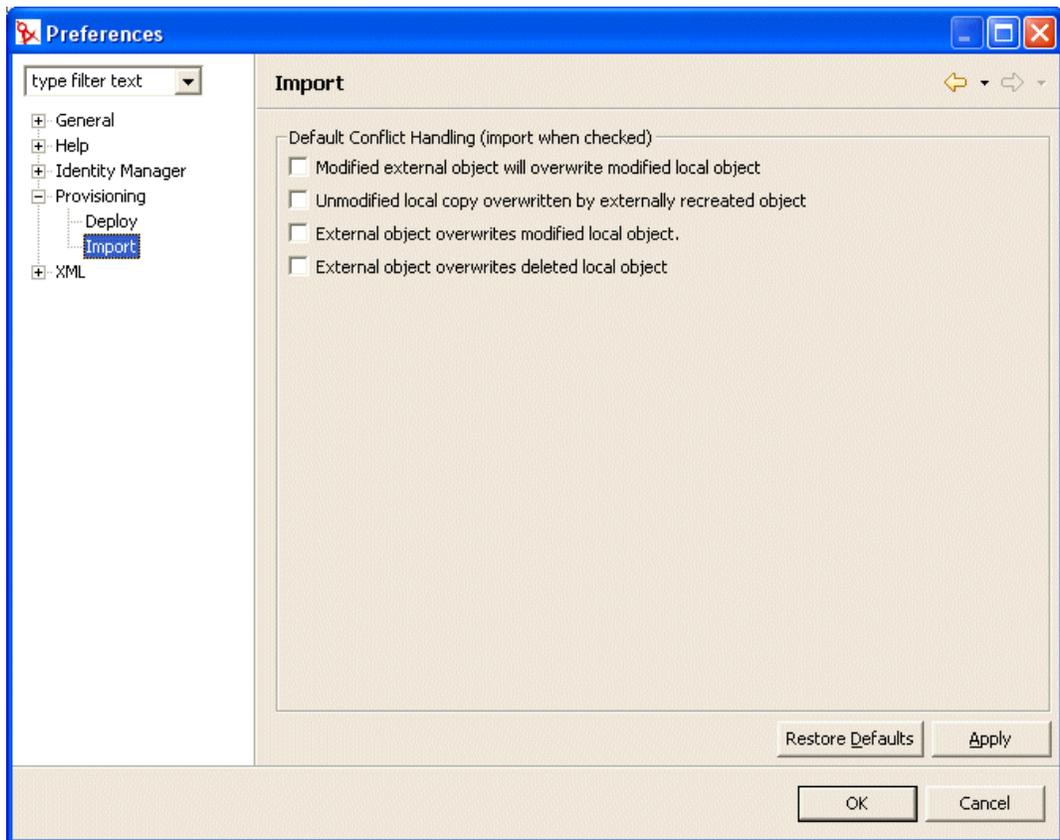
## Festlegen von Importeinstellungen

Mit den Importeinstellungen können Sie angeben, wie der Designer Konflikte zwischen den Daten im Identitätsdepot und den Dateien in der lokalen Verzeichnisabstraktionsschicht lösen soll. Diese Konflikte entstehen dann, wenn verschiedene Benutzer und Werkzeuge Zugriff auf die Verzeichnisabstraktionsschicht-Definitionen des Identitätsdepots haben. Die Definitionen können von anderen Administratoren oder Entwicklern mit den iManager-Werkzeugen oder ihrem eigenen lokalen Designer-basierten Projekt geändert werden. Wenn Konflikte zwischen den Definitionen in Ihrem lokalen Dateisystem und denen im Identitätsdepot auftreten, können Sie anhand dieser Einstellungen angeben, wie diese Konflikte gehandhabt werden sollen.

So legen Sie Importeinstellungen fest:

- 1 Wählen Sie *Window>Preferences*.

2 Öffnen Sie den Bereitstellungsknoten des Baums und klicken sie auf *Import*.



3 Nehmen Sie die gewünschten Einstellungen vor:

Standardeinstellung	Beschreibung
Modified external object will overwrite modified local object	<p>Sowohl die lokale Datei als auch die Definitionen im Identitätsdepot enthalten Änderungen. Die lokalen Änderungen wurden noch nicht bereitgestellt.</p> <p>Wählen Sie diese Option, wenn das Objekt im Identitätsdepot die Änderungen in der lokalen Datei überschreiben soll.</p>
Unmodified local copy overwritten by externally recreated object	<p>Das Identitätsdepot-Objekt wurde gelöscht und anschließend neu erstellt. Der lokale Dateisatz enthält die Originaldefinition ohne Änderungen.</p> <p>Wählen Sie diese Option, wenn durch den Import die lokale Kopie überschrieben werden soll.</p>
External object overwrites modified local object	<p>Die lokale Datei enthält Änderungen, die noch nicht an das Identitätsdepot verteilt wurden. Wählen Sie diese Option, wenn die lokalen Dateien beim Import überschrieben werden sollen.</p>

Standardeinstellung	Beschreibung
External object overwrites deleted local object	<p>Sie haben eine Definition lokal gelöscht, aber die Änderungen noch nicht verteilt. Dies bedeutet, dass das Objekt noch im Identitätsdepot vorhanden ist.</p> <p>Wählen Sie diese Option, wenn die Objekte im Identitätsdepot in das lokale Dateisystem kopiert werden sollen. Wenn Sie diese Option wählen, gehen die nicht verteilten Änderungen verloren.</p>

## 4.8.2 Allgemeines zur Validierung

Sie können die Datendefinitionen der Verzeichnisabstraktionsschicht im lokalen Dateisystem validieren, bevor Sie sie zu verteilen versuchen. Die Validierung hat folgende Funktionen:

- Sie überprüft, ob der verwendete XML-Code ordnungsgemäß ist und dem Schema entspricht, das die für Entitäten, Attribute, Listen, Relationen usw. erforderlichen Elemente definiert.
- Sie überprüft zudem alle Entitäten, um sicherzustellen, dass Referenzen auf andere Entitäten und globale Listen gültig sind.

So überprüft die Validierung beispielsweise bei Entitäten und ihren Attributen, dass alle Referenzen auf andere Entitäten über die Felder *Edit Entity*, *DN Lookup* und *Detail Entity* Entitäten referenzieren, die es auch wirklich gibt.

- Sie stellt sicher, dass für jede Entität mindestens ein Attribut definiert wurde.
- Sie stellt sicher, dass jede lokale und globale Liste mindestens ein Element enthält.

Sie können Definitionen selektiv in der *Bereitstellungsansicht* validieren. Zum Validieren:

- Aller Elemente eines Knotens wählen Sie den Knoten aus, klicken Sie mit der rechten Maustaste und wählen Sie *Validate*.
- Eines einzelnen Objekts in einem Knoten wählen Sie das Objekt aus, klicken Sie mit der rechten Maustaste und wählen Sie *Validate*.

Wenn Sie alle Definitionen validieren möchten, klicken Sie in der Symbolleiste der Verzeichnisabstraktionsschicht auf die Schaltfläche *Validate Abstraction Layer*.

---

**Hinweis:** Die Validierung überprüft das Identitätsdepot nicht auf das Vorhandensein von Objekten.

---

## 4.8.3 Allgemeines zur Bereitstellung

Sie müssen Ihre Definitionen in einem Identitätsdepot bereitstellen, bevor Sie die Änderungen in der Identity Manager-Benutzeranwendung sehen können.

So stellen Sie einen Definitionssatz in einem Identitätsdepot bereit:

- 1 Speichern Sie alle Änderungen, die Sie mit dem Verzeichnisabstraktionsschicht-Editor vorgenommen haben.

Wenn Sie die Änderungen nicht vor der Bereitstellung speichern, wird im Editor ein Dialogfeld angezeigt, in dem die Definitionen aufgelistet sind, die nicht gespeichert wurden. Sie werden dann dazu aufgefordert, die letzten Änderungen zu speichern. Wenn Sie die Änderungen nicht

speichern, wird das Objekt zwar auf dem Server bereitgestellt, es enthält aber nicht die ungespeicherten Änderungen. Wenn Sie die Änderungen nicht speichern, wird die Bereitstellung nicht abgebrochen.

**2** Öffnen Sie die *Bereitstellungsansicht*.

**3** Sie müssen entscheiden, ob Sie alle oder nur einen Teil der Objekte, die Sie mit dem Verzeichnisabstraktionsschicht-Editor definiert haben, bereitstellen möchten.

- Wenn Sie alle Objekte bereitstellen möchten:

Wählen Sie den Stammknoten aus, klicken Sie mit der rechten Maustaste und wählen Sie *Deploy all*.

- Wenn Sie eine bestimmte Entität, Relation, Liste oder Konfigurationseinstellung bereitstellen möchten:

Wählen Sie das Objekt aus, klicken Sie mit der rechten Maustaste und wählen Sie *Deploy object*.

Möglicherweise müssen Sie Identifikationsdaten für das Identitätsdepot angeben. Der Editor führt eine Validierung durch und zeigt alle Validierungsmeldungen in einem Dialogfeld an. Wählen Sie anhand der Validierungsmeldungen die bereitzustellenden Elemente aus bzw. heben Sie die Auswahl auf. Nachdem Sie die Auswahl für die Bereitstellung getroffen und verteilt haben, werden Sie über den Erfolg oder Misserfolg des Bereitstellvorgangs informiert.

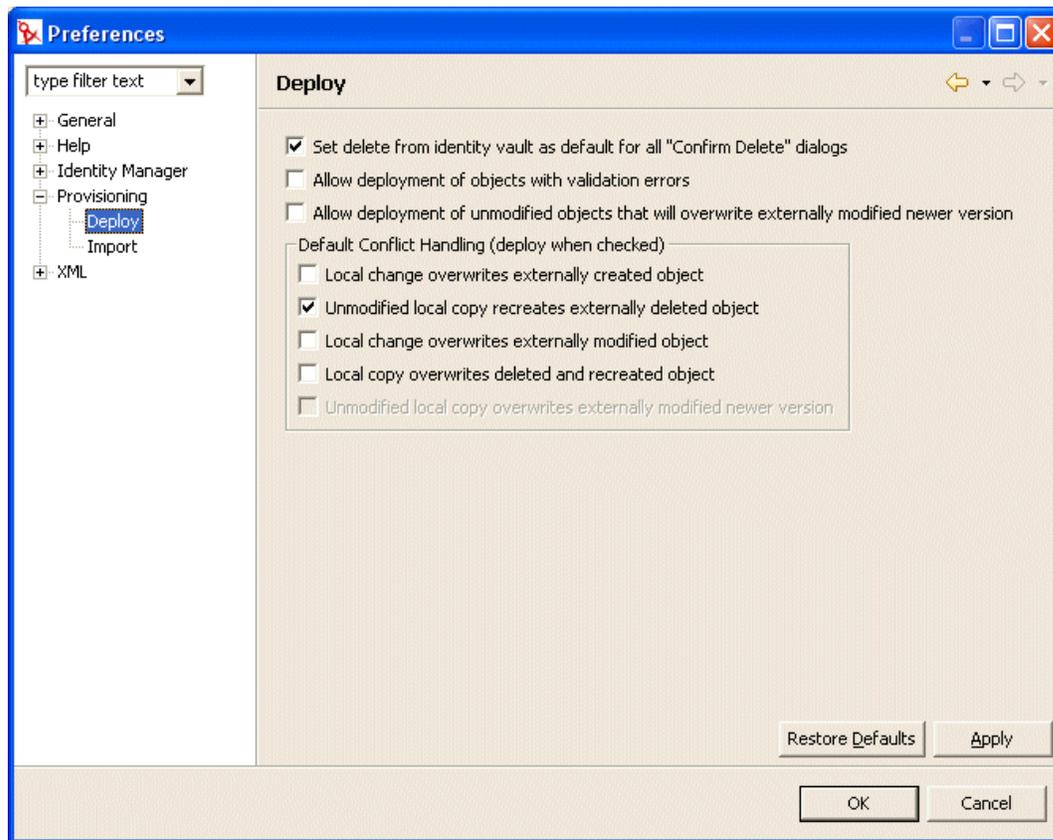
## **Einstellen von Bereitstellungsoptionen**

Mit den Einstellungen für die Bereitstellung können Sie angeben, wie der Designer Konflikte zwischen den Daten im Identitätsdepot und den Dateien in der lokalen Verzeichnisabstraktionsschicht lösen soll. Konflikte können entstehen, wenn andere Benutzer Änderungen im Identitätsdepot bereitgestellt haben und diese Änderungen nicht in den Definitionen im lokalen Dateisystem reflektiert sind. Wenn Sie sicherstellen möchten, dass Konflikte so gehandhabt werden, wie Sie es wünschen, sollten Sie die Einstellungen für die Konfliktlösung entsprechend festlegen.

So legen Sie Einstellungen für die Bereitstellung fest:

- 1** Wählen Sie *Window > Preferences*.

2 Öffnen Sie den Bereitstellungsknoten des Baums und klicken sie auf *Deploy*.



3 Geben Sie allgemeine Standardeinstellungen für die Bereitstellung an:

Standardeinstellung	Beschreibung
Set delete from identity vault as default for all "Confirm Delete" dialogs	<p>Wenn Sie in der Bereitstellungsansicht oder im Verzeichnis-abstraktionsschicht-Editor ein Objekt zu löschen versuchen, werden Sie in einem Dialogfeld wie dem folgenden zur Bestätigung des Löschvorgangs aufgefordert:</p> <div data-bbox="787 430 1344 741" data-label="Image"> </div>
Allow deployment of objects with validation errors	<p>Diese Einstellung legt fest, ob das Auswahlfeld <b>Delete object in identity vault on deploy</b> standardmäßig aktiviert ist. Ist diese Einstellung aktiviert, werden die Objekte im Identitätsdepot immer gelöscht.</p> <p>Das lokale Objekt wird immer gelöscht.</p> <p><b>Aktivieren</b> - Wählen Sie diese Option, wenn Sie Objekte bereitstellen möchten, bei denen die Validierung fehlschlägt. Beim Bereitstellungsprozess validiert der Designer die bereitzustellenden Definitionen anhand der Validierungsregeln, die in <a href="#">Abschnitt 4.8, „Importieren, Validieren und Bereitstellen von Verzeichnisabstraktionsschicht-Definitionen“</a>, auf Seite 112 dargestellt sind.</p> <p><b>Deaktivieren</b> - Dies verhindert die Bereitstellung der Definitionen, bei denen die Validierung fehlschlägt.</p>
Allow deployment of unmodified objects that will overwrite externally modified newer version	<p><b>Aktivieren</b> - Wenn Ihre lokalen Dateien nicht geändert wurden, aber die Objekte im Identitätsdepot. Möchten Sie, dass die lokalen Dateien die Dateien im Identitätsdepot überschreiben? Falls ja, wählen Sie diese Einstellung.</p> <p><b>Deaktivieren</b> - Wenn Sie die neueren Versionen im Identitätsdepot beibehalten möchten.</p> <p>Ist diese Option aktiviert, können Sie dies als Standardverhalten festlegen, indem Sie zusätzlich die Konfliktlösungseinstellung <b>Unmodified local copy overwrites externally modified newer version</b> aktivieren.</p>

**4** Nehmen Sie Konfliktlösungseinstellungen vor:

Standardeinstellung	Beschreibung
Local change overwrites externally created object	<p><b>Aktivieren</b> - Wenn Sie möchten, dass das bereitzustellende Objekt das Objekt überschreiben soll, das sich im Identitätsdepot befindet.</p> <p><b>Deaktivieren</b> - Tritt dieser Konflikt auf, wird keine Bereitstellung durchgeführt.</p>
Unmodified local copy recreates externally deleted object	<p><b>Aktivieren</b> - Wenn Sie möchten, dass das bereitzustellende lokale Objekt ein Objekt erstellen soll, das bereits im Identitätsdepot gelöscht wurde.</p> <p><b>Deaktivieren</b> - Tritt dieser Konflikt auf, wird keine Bereitstellung durchgeführt.</p>
Local change overwrites externally modified object	<p><b>Aktivieren</b> - Wenn Sie möchten, dass die lokale Definition immer bereitgestellt wird, selbst wenn das Identitätsdepot von einem anderen Benutzer geändert wurde.</p> <p><b>Deaktivieren</b> - Tritt dieser Konflikt auf, wird keine Bereitstellung durchgeführt.</p>
Local copy overwrites deleted and recreated object	<p><b>Aktivieren</b> - Wenn Sie möchten, dass das lokale Objekt immer bereitgestellt wird, selbst wenn das Objekt im Identitätsdepot gelöscht bzw. gelöscht und wieder neu erstellt wurde.</p> <p><b>Deaktivieren</b> - Tritt dieser Konflikt auf, wird keine Bereitstellung durchgeführt.</p>
Unmodified local copy overwrites externally modified newer version	<p>Diese Einstellung kann nur aktiviert werden, wenn auch die allgemeine Bereitstellungseinstellung <b>&gt;Allow deployment of unmodified objects that will overwrite externally modified newer version</b> aktiviert ist.</p> <p><b>Aktivieren</b> - Wenn Ihre lokalen Dateien nicht geändert wurden, aber die Objekte im Identitätsdepot, und die lokalen Dateien standardmäßig <b>immer</b> die Dateien im Identitätsdepot überschreiben sollen.</p> <p><b>Deaktivieren</b> - Wenn Sie die neueren Versionen im Identitätsdepot beibehalten möchten.</p>



Dieses Kapitel enthält Folgendes:

- [Abschnitt 5.1, „Allgemeines zur Ereignisprotokollierung“](#), auf Seite 121
- [Abschnitt 5.2, „Protokollierung an einen Novell Audit-Server“](#), auf Seite 122

## 5.1 Allgemeines zur Ereignisprotokollierung

Die Identity Manager-Benutzeranwendung implementiert die Protokollierung unter Verwendung von *log4j*, einem Open-Source-Protokollierungspaket der Apache Software Foundation. Standardmäßig werden Ereignisnachrichten in der *Systemkonsole* und in der Protokolldatei des Anwendungsservers mit dem Protokollierumfang INFO und höher protokolliert. Sie können die Benutzeranwendung so konfigurieren, dass sie auch an Novell Audit protokolliert. Ereignisse werden für *alle* aktivierten Logger protokolliert.

---

**Wichtig:** Wenn Sie sich bei Novell Audit anmelden, wird empfohlen, dass Sie zuvor die [Novell Audit-Dokumentation \(http://www.novell.com/documentation/nsureaudit\)](http://www.novell.com/documentation/nsureaudit) lesen.

---

### 5.1.1 Allgemeines zu den Einstellungen für den Protokollierumfang

Bei der Protokollierung der Konsole werden synchronisierte Schreibvorgänge ausgeführt. Dies bedeutet, dass die Protokollierung zu einer starken Beanspruchung des Prozessors sowie zu Problemen bei gleichzeitigen Zugriffen („concurrency impedance“) führen kann. Sie können die Standardeinstellung für den Wert in ERROR ändern, indem Sie die Einstellung in der Datei `<installdir>/jboss/server/IDMProv/conf/log4j.xml` ändern. Suchen Sie den root-Knoten. Er sieht etwa folgendermaßen aus:

```
<root>
  <appender-ref ref="CONSOLE"/>
  <appender-ref ref="FILE"/>
</root>
```

Ändern Sie den priority-Wert in:

```
<root>
  <priority value="ERROR"/>
  <appender-ref ref="FILE"/>
</root>
```

Wenn Sie „root“ einen Wert zuweisen, wird sichergestellt, dass alle Appender-Einträge, denen explizit kein Protokollierumfang zugewiesen wurde, den Wert von „root“ übernehmen. Dem FILE-Appender ist standardmäßig kein Protokollierumfang zugewiesen. Deshalb übernimmt er den Wert von „root“. Bei jedem „root“-Appender mit einem zugewiesenen Protokollierumfang sollte dieser ERROR oder WARN sein. Ist der Protokollierumfang größer als WARN, wird die Leistung beeinträchtigt.

## 5.2 Protokollierung an einen Novell Audit-Server

Wenn sie auf einen Novell Audit-Server protokollieren möchten, führen Sie folgende Schritte aus:

Schritt	Vorgehensweise	Weitere Informationen
1	Verwenden Sie das Identity Manager-Anwendungsschema als eine Protokollanwendung für den Novell Audit-Server	<b>Abschnitt 5.2.1, „Hinzufügen des Identity Manager-Anwendungsschemas als eine Protokollanwendung zum Novell Audit-Server“, auf Seite 122</b>
2	Konfigurieren Sie den Novell Audit- <b>Plattformagenten</b> auf Ihrem Anwendungsserver	<p>Der Plattformagent ist auf jedem Client erforderlich, der Ereignisse an Novell Audit protokolliert. Der Plattformagent wird mit der <b>logevent-Konfigurationsdatei</b> konfiguriert. Diese Datei enthält die Angaben zur Konfiguration, die der Plattformagent für die Kommunikation mit dem Novell Audit-Server benötigt. Der standardmäßige Speicherort dieser Datei auf dem Anwendungsserver ist:</p> <ul style="list-style-type: none"><li>• Linux - /etc/logevent.conf</li><li>• Windows - /&lt;Windows-Verzeichnis&gt;/logevent.cfg (Normalerweise c:\windows)</li></ul> <p>Geben Sie auf jeden Fall die <b>IP-Adresse oder den DNS-Namen Ihres Novell Audit-Servers</b> mit der <b>LogHost</b>-Einstellung an. Zum Beispiel:</p> <pre>LogHost=xxx.xxx.xxx.xxx</pre> <p>Nehmen Sie weitere, für Ihre Umgebung erforderliche Einstellungen vor.</p> <hr/> <p><b>Wichtig:</b> Nachdem Sie die logevent-Konfigurationsdatei erstellt oder geändert haben, müssen Sie JBoss Application Server neu starten, damit die Änderungen wirksam werden.</p> <hr/> <p>Weitere Informationen zur Struktur der logevent-Konfigurationsdatei finden Sie im Abschnitt zum Konfigurieren der <b>Plattformagenten</b> (<a href="http://www.novell.com/documentation/nsureaudit">http://www.novell.com/documentation/nsureaudit</a>) im Kapitel über die Protokollierung im Novell Audit Administration Guide.</p>
3	Aktivieren Sie die Novell Audit-Protokollierung	<b>Abschnitt 5.2.2, „Aktivieren der Audit-Protokollierung“, auf Seite 123</b>

### 5.2.1 Hinzufügen des Identity Manager-Anwendungsschemas als eine Protokollanwendung zum Novell Audit-Server

So konfigurieren Sie Audit, damit die Identity Manager-Benutzeranwendung als Protokollanwendung verwendet wird:

- 1 Suchen Sie folgende Datei:

DirXML.lsc

Plattform	Speicherort
Linux	Nach der Installation:  /opt/novell/naudit/logschema/dirxml.lsc
Windows	Auf dem Installationsmedium:  /nt/dirxml/nsure_audit/nauditextensions/lsc/ dirxml.lsc

- 2 Verwenden Sie für den Zugriff auf *iManager* einen Webbrowser und melden Sie sich als *Administrator* an.
- 3 Wechseln Sie zu *Roles and Tasks > Auditing and Logging* und wählen Sie *Logging Server Options*.
- 4 Navigieren Sie zum *Logging Services-Container* in Ihrem Baum und wählen Sie den entsprechenden *Audit Secure Logging Server*. Klicken Sie anschließend auf *OK*.
- 5 Wechseln Sie zur Registerkarte *Log Applications*, wählen Sie den *Containernamen* aus und klicken Sie auf den Link *New Log Application*.
- 6 Wenn das Dialogfeld „New Log Application“ angezeigt wird, geben Sie Folgendes an:

Für diese Einstellung	Führen Sie diese Schritte aus
Log Application Name	Geben Sie einen Namen mit einer sinnvollen Bedeutung ein
Import LSC File	Wählen Sie die Datei <b>DirXML.lsc</b> aus

Klicken Sie anschließend auf *OK*. Auf der Registerkarte „Log Applications“ wird der hinzugefügte Anwendungsname angezeigt.

- 7 Klicken Sie zum Abschließen der Novell Audit-Serverkonfiguration auf *OK*.
- 8 Stellen Sie sicher, dass der Status der Protokollanwendung aktiviert ist (ON). (Der Kreis unter dem Status sollte grün sein. Ist er rot, klicken Sie darauf, um ihn zu aktivieren (ON).)
- 9 *Starten* Sie den Novell Audit-Server, damit die neuen Protokollanwendungseinstellungen wirksam werden.

## 5.2.2 Aktivieren der Audit-Protokollierung

So aktivieren Sie die Novell Audit-Protokollierung in Ihrer Identity Manager-Benutzeranwendung:

- 1 Melden Sie sich als Admin-Benutzer bei der Benutzeranwendung an.
- 2 Wählen Sie die Registerkarte *Administration*.
- 3 Wählen Sie die Registerkarte *Protokollierung*.
- 4 Markieren Sie das Kontrollkästchen *Auch Protokollierungsmeldungen an Audit senden* (am unteren Ende der Registerkarte).

- 5 Damit die Änderungen für alle zukünftigen Neustarts des Anwendungsservers zur Verfügung stehen, stellen Sie sicher, dass *Protokollierungsänderungen permanent speichern* ausgewählt ist.

### 5.2.3 Protokollierte Ereignisse

Die Identity Manager-Benutzeranwendung protokolliert automatisch Ereignisse von Workflow-, Such-, Detail- und Passwortanforderungen. Standardmäßig protokolliert die Identity Manager-Benutzeranwendung automatisch folgende Ereignisse in alle aktiven Protokollierungskanäle:

Ereignis-ID	Vorgang	Ereignis	Protokollierumfang
31400	Detail-Portlet	Delete_Entity	Info
31401		Update_Entity	Info
31410	Portlet „Passwort ändern“	Change_Password_Failure	Error
31411		Change_Password_Success	Info
31420	Portlet „Passwort vergessen“	Forgot_Password_Change_Failure	Error
31421		Forgot_Password_Change_Success	Info
31430	Such-Portlet	Search_Request	Info
31431		Search_Saved	Info
31440	Portlet „Erstellen“	Create_Entity	Info
31520	Workflow	Workflow_Error	Error
31521		Workflow_Started	Info
31522		Workflow_Forwarded	Info
31523		Workflow_Reassigned	Info
31524		Workflow_Approved	Info
31525		Workflow_Refused	Info
31526		Workflow_Ended	Info
31527		Workflow_Claimed	Info
31528		Workflow_Unclaimed	Info
31529		Workflow_Denied	Info
3152A		Workflow_Completed	Info
3152B		Workflow_Timedout	Info
3152C		User_Message	Info
31533		Workflow_Retracted	Info

Ereignis-ID	Vorgang	Ereignis	Protokollierumfang
3152D	Bereitstellung	Provision_Error	Error
3152E		Provision_Submitted	Info
3152F		Provision_Success	Info
31530		Provision_Failure	Error
31531		Provision_Granted	Info
31532		Provision_Revoked	Info
31450	Sicherheitskontext	Create_Proxy_Definition_Success	Info
31451		Create_Proxy_Definition_Failure	Error
31452		Update_Proxy_Definition_Success	Info
31453		Update_Proxy_Definition_Failure	Error
31454		Delete_Proxy_Definition_Success	Info
31455		Delete_Proxy_Definition_Failure	Error
31456		Create_Delegatee_Definition_Success	Info
31457		Create_Delegatee_Definition_Failure	Error
31458		Update_Delegatee_Definition_Success	Info
31459		Update_Delegatee_Definition_Failure	Error
3145A		Delete_Delegatee_Definition_Success	Info
3145B		Delete_Delegatee_Definition_Failure	Error
3145C		Create_Availability_Success	Info
3145D		Create_Availability_Failure	Error
3145E		Delete_Availability_Success	Info
3145F		Delete_Availability_Failure	Error

## 5.2.4 Protokollberichte

Wenn Sie Ereignisse an den Novell Audit-Datenbankkanal protokollieren, können Sie Berichte zu den erfassten Daten erstellen. Es gibt verschiedene Möglichkeiten, Berichte anhand der Daten zu generieren, die in einer Novell Audit-Datenbank protokolliert wurden:

- Mit der Novell Audit-Berichts-anwendung können Sie Ihre eigenen oder vordefinierte Berichte ausführen. Dies wird nachfolgend in „[Vordefinierte Protokollberichte](#)“ auf Seite 126 beschrieben.
- Erstellen Sie mit iManager Abfragen auf die protokollierten Daten. Wählen Sie dazu *Auditing and Logging > Queries*.
- Schreiben Sie Ihre eigenen SQL-Abfragen für die protokollierten Daten.

Die Novell Audit-Standardtabelle heißt NAUDITLOG.

## Vordefinierte Protokollberichte

Folgende vordefinierten Protokollberichte können im Crystal Reports-Format (.rpt) zum Filtern von Daten erstellt werden, die in der Novell Audit-Datenbank protokolliert werden:

Berichtsname	Beschreibung
Administrative Action Report	Enthält alle administrativen Aktionen, die von der Identity Manager-Benutzeranwendung initiiert wurden. Dieser Bericht führt jeweils auch den Administrator auf, der die Aktion initiiert hat.  Er enthält keine administrativen Änderungen, die von iManager oder dem IDM-Designer vorgenommen wurden.
Historical Approval Flow Report	Er enthält alle Aktivitäten eines Genehmigungsablaufs für einen bestimmten Zeitraum.
Resource Provisioning report	Er enthält alle Bereitstellungsaktivitäten, sortiert nach Ressource.
Specific User Audit Trail	Er enthält alle Aktivitäten eines Benutzers. Bei den Aktivitäten handelt es sich sowohl um Bereitstellungs- als auch um Selbstbedienungsaktivitäten.
Specific User Provisioning report	Er enthält alle Bereitstellungsaktivitäten eines bestimmten Benutzers.
User Provisioning report	Er enthält alle Bereitstellungsaktivitäten, sortiert nach Benutzer.

**Beispielbericht** Dies ist ein Beispiel des Berichts „Specific User Audit Trail“:

# Novell® Audit Report for Identity Manager

## Specific User Audit Trail

Report Period: - 10/13/2005 8:51:32AM

User ID: ablake

Report Last Modified: 10/13/2005

Report Generated On: 10/13/2005

Total pages: 8

### Approval Flow

#### Workflow Event: fecedbe80a3d4abd83c9476a1b576ea2

Date / Time	Action	Initiator ID
9/12/2005 3:20:42PM	Workflow Started	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell
9/12/2005 3:20:43PM	Workflow Forwarded	Workflow Administrator
9/12/2005 3:25:43PM	Workflow Reassigned	Unclaimed
9/12/2005 3:30:44PM	Workflow Forwarded	Workflow Administrator
9/12/2005 3:30:44PM	Workflow Ended	Workflow Administrator
9/12/2005 3:30:44PM	Workflow Denied	System

#### Workflow Event: fc6d74b1268243b3beac52261439dea0

Date / Time	Action	Initiator ID
9/28/2005 1:12:19PM	Workflow Started	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell
9/28/2005 1:12:22PM	Workflow Forwarded	Workflow Administrator
9/28/2005 2:12:23PM	Workflow Forwarded	Workflow Administrator
9/28/2005 2:12:23PM	Workflow Forwarded	Workflow Administrator
9/28/2005 2:12:23PM	Workflow Forwarded	Workflow Administrator
9/28/2005 2:12:23PM	Workflow Forwarded	Workflow Administrator
9/28/2005 2:12:23PM	Workflow Approved	System
9/28/2005 2:12:23PM	Workflow Approved	System
9/28/2005 2:12:23PM	Workflow Completed	Workflow Administrator
9/28/2005 2:12:27PM	Workflow Forwarded	Workflow Administrator
9/28/2005 2:12:27PM	Workflow Ended	Workflow Administrator
9/28/2005 2:12:27PM	Provision Submitted	Workflow Administrator
9/28/2005 2:12:27PM	Provision Granted	Workflow Administrator

#### Workflow Event: efaa8304e07641edb9e6375a1a36e396

Date / Time	Action	Initiator ID
10/12/2005 11:58:13AM	Workflow Started	cn=ablake,ou=users,ou=idm sample-qatest,o=novell
10/12/2005 11:58:13AM	Workflow Forwarded	Workflow Administrator

#### Workflow Event: ea341eb11a824e669e356837745fe264

Date / Time	Action	Initiator ID
9/27/2005 4:24:44PM	Workflow Started	cn=m m ackenzie,ou=users,ou=idm sample-Jeff,o=novell
9/27/2005 4:24:44PM	Workflow Forwarded	Workflow Administrator

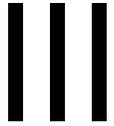
Speicherort der Berichtsdateien Die Berichtsdateien befinden sich in:

Plattform	Standort
Windows	/nt/dirxml/reports

Sie können diese Berichte als Schablonen zum Erstellen eigener Berichte im Crystal Reports Designer verwenden oder sie mit *Audit Report* (lreport.exe) ausführen, einem Windows-Programm, das mit Novell Audit ausgeliefert wird. Die vordefinierten Berichte führen Abfragen über die Daten der standardmäßigem Novell Audit-Protokolldatenbank *naudit* und der Datenbanktabelle *nauditlog* aus. Wenn Ihre Novell Audit-Protokolldatenbank einen anderen Namen hat, können Sie über die Menüoption *Set Datasource Location* in Crystal Reports Designer den Datenbanknamen *naudit* durch den Namen Ihrer Datenbank ersetzen.

Weitere Informationen finden Sie im Abschnitt zu den Berichten in der Novell [Audit-Dokumentation](http://www.novell.com/documentation/nsureaudit) (<http://www.novell.com/documentation/nsureaudit>).

# Verwalten der Benutzeranwendung



In diesen Kapiteln wird die Konfigurierung und Verwaltung der Identity Manager-Benutzeranwendung unter Verwendung der Registerkarte „Administration“ beschrieben.

- Kapitel 6, „Verwendung der Registerkarte „Administration““, auf Seite 131
- Kapitel 7, „Seitenadministration“, auf Seite 137
- Kapitel 8, „Konfiguration von Motiven“, auf Seite 175
- Kapitel 9, „Portletadministration“, auf Seite 181
- Kapitel 10, „Portalkonfiguration“, auf Seite 201
- Kapitel 11, „Sicherheitskonfiguration“, auf Seite 209
- Kapitel 12, „Konfiguration der Protokollierung“, auf Seite 213
- Kapitel 13, „Cache-Konfiguration“, auf Seite 219
- Kapitel 14, „Werkzeuge zum Exportieren und Importieren von Portaldaten“, auf Seite 229



# Verwendung der Registerkarte „Administration“

# 6

Dieses Kapitel bietet eine Einführung in die Registerkarte „Administration“ der Benutzeroberfläche von Identity Manager. Sie erfahren, wie Sie mithilfe der Registerkarte „Administration“ die Identity Manager-Benutzeranwendung konfigurieren und verwalten können. Es werden folgende Themen erläutert:

- [Abschnitt 6.1, „Allgemeines zur Registerkarte „Administration““, auf Seite 131](#)
- [Abschnitt 6.2, „Berechtigte Benutzer“, auf Seite 131](#)
- [Abschnitt 6.3, „Zugriff auf die Registerkarte „Administration““, auf Seite 132](#)
- [Abschnitt 6.4, „Zur Auswahl stehende Verwaltungsaktionen“, auf Seite 134](#)

## 6.1 Allgemeines zur Registerkarte „Administration“

Auf die *Benutzeroberfläche* von Identity Manager greifen hauptsächlich Endbenutzer zu, die mit den Registerkarten arbeiten, die für die Identitätsselbstbedienung und die Workflow-basierte Bereitstellung (über das Bereitstellungsmodul Identität Manager) zur Verfügung stehen. Diese browserbasierte Benutzeroberfläche enthält auch eine Registerkarte *Administration*, auf die Administratoren zugreifen können, um die verschiedenen Eigenschaften der zu Grunde liegenden Identity Manager-Benutzeranwendung zu konfigurieren.

Über die Registerkarte „Administration“ können folgende Funktionen ausgeführt werden:

- Sie können *das Motiv ändern*, das für die Darstellung der Benutzeroberfläche verwendet wird.
- Sie können die für Endbenutzer verfügbaren *Funktionen der Identitätsselbstbedienung anpassen*.
- Sie können *festlegen, wer Administrationsaktionen ausführen darf*.
- Sie können *weitere Details hinsichtlich der Benutzeranwendung verwalten* und festlegen, wie diese ausgeführt wird.

## 6.2 Berechtigte Benutzer

Die Registerkarte „Administration“ ist für typische Endbenutzer der Identity Manager-Benutzeroberfläche nicht sichtbar. Es gibt zwei Arten von Benutzern, die diese Registerkarte anzeigen und auf diese zugreifen können:

- *Benutzeranwendungsadministratoren*

Ein Benutzeranwendungsadministrator ist berechtigt, alle Verwaltungsfunktionen in Verbindung mit der Identity Manager-Benutzeranwendung auszuführen. Dies umfasst den Zugriff auf die Registerkarte „Administration“ der Benutzeroberfläche von Identity Manager, um die dort verfügbaren Verwaltungsaktionen auszuführen.

Bei der Installation wird ein Benutzer als Benutzeranwendungsadministrator festgelegt. Nach der Installation kann dieser Benutzer auf der Seite *Sicherheit* der Registerkarte „Administration“ bei Bedarf weitere Benutzeranwendungsadministratoren angeben.

Weitere Informationen finden Sie in [Kapitel 11, „Sicherheitskonfiguration“](#), auf Seite 209.

- *Von Benutzeranwendungsadministratoren berechtigte Benutzer*

Bei Bedarf kann ein Benutzeranwendungsadministrator einem oder mehreren Endbenutzern die Anzeige- und Zugriffsberechtigungen für bestimmte Seiten der Registerkarte „Administration“ erteilen. Diese Berechtigungen werden über die Seite *Seitenadministration* der Registerkarte „Administration“ erteilt.

Weitere Informationen finden Sie in [Kapitel 7, „Seitenadministration“](#), auf Seite 137.

## 6.3 Zugriff auf die Registerkarte „Administration“

Wenn Sie ein Benutzeranwendungsadministrator (oder ein berechtigter Benutzer) sind, können Sie auf die Registerkarte „Administration“ der Identity Manager-Benutzeroberfläche zugreifen, wenn eine Verwaltung der Identity Manager-Benutzeranwendung erforderlich ist. Sie benötigen lediglich einen unterstützten Webbrowser.

Eine Liste der unterstützten Webbrowser finden Sie im *Novell Identity Manager-Installationshandbuch*.

---

**Hinweis:** Vergewissern Sie sich, dass in Ihrem Webbrowser *JavaScript aktiviert* ist, damit Sie die Identity Manager-Benutzeranwendung verwenden können.

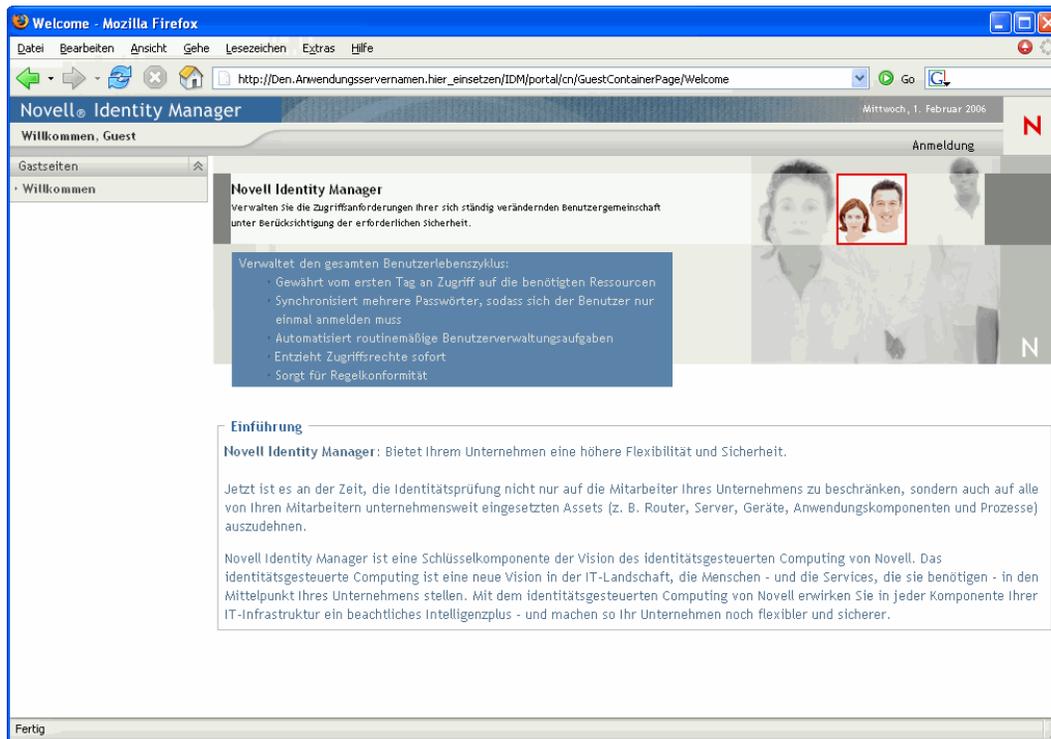
---

So greifen Sie auf die Registerkarte „Administration“ zu:

- 1 Rufen Sie in Ihrem *Webbrowser* die URL der Identity Manager-Benutzeroberfläche auf (wie an Ihrem Standort definiert). Zum Beispiel:

```
http://meinanwendungsserver:8080/IDM
```

Die Benutzeranwendung zeigt die *Begrüßungsseite für Gäste* an:

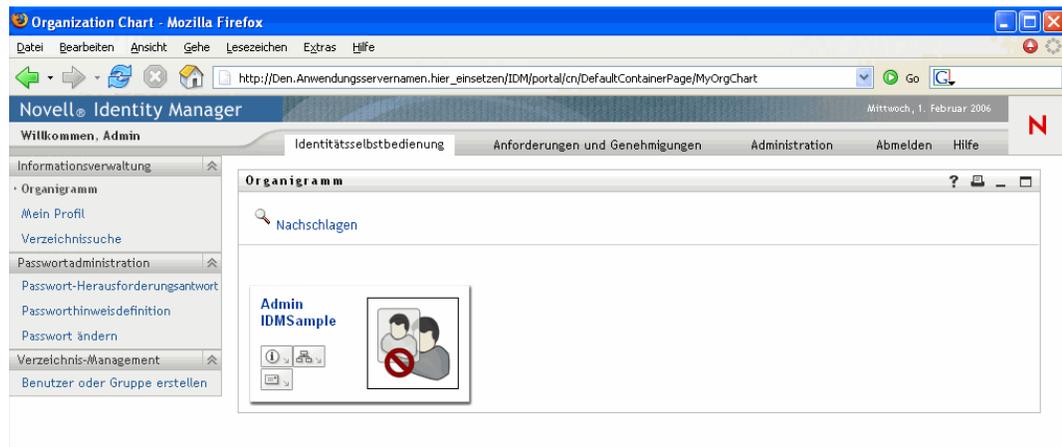


2 Klicken Sie im Titel der Seite auf den Anmeldungs-Link.

Sie werden zur Eingabe von Benutzername und Passwort aufgefordert.

3 Geben Sie den Benutzernamen und das Passwort eines *Benutzeranwendungsadministrators* (oder eines Benutzers mit Berechtigungen für die Registerkarte „Administration“) ein und klicken Sie anschließend auf *Anmeldung*.

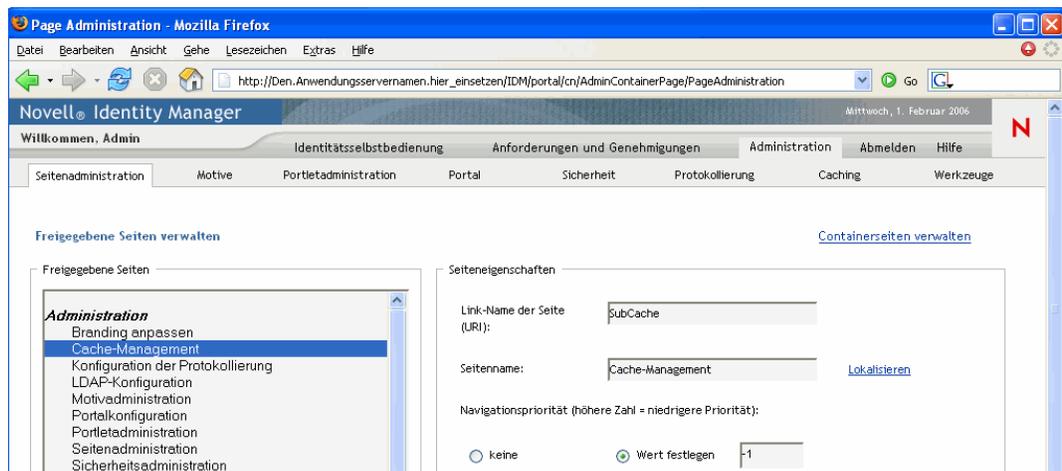
Sobald Sie sich angemeldet haben, wird die Benutzeroberfläche mit dem entsprechenden Inhalt für diesen Benutzer angezeigt. Zum Beispiel:



Standardmäßig wird die Registerkarte *Identitätsselbstbedienung* geöffnet.

**4** Klicken Sie auf die Registerkarte *Administration*.

Die Registerkarte „Administration“ zeigt ein Menü mit *Verwaltungsaktionen* an, die Sie ausführen können. Nach Auswahl einer Aktion wird eine zugehörige Seite mit Einstellungen und Bedienelementen angezeigt. Standardmäßig wird die Seite *Seitenadministration* angezeigt:



Weitere allgemeine Informationen zum Zugriff auf die Identity Manager-Benutzeroberfläche und dazu, wie Sie mit dieser arbeiten können, finden Sie im *Identity Manager-Benutzeranwendung- Benutzerhandbuch*.

## 6.4 Zur Auswahl stehende Verwaltungsaktionen

Wenn Sie sich in der Registerkarte „Administration“ befinden, können Sie alle verfügbaren Aktionen zur Konfiguration und Verwaltung der Identity Manager-Benutzeranwendung verwenden. Im Folgenden finden Sie eine Zusammenfassung:

<b>Aktion</b>	<b>Beschreibung</b>
Seitenadministration	<p>Steuert, welche Seiten auf der Benutzeroberfläche von Identity Manager angezeigt werden und wer eine Zugriffsberechtigung erhalten soll.</p> <p>Weitere Informationen finden Sie in <a href="#">Kapitel 7, „Seitenadministration“</a>, auf <a href="#">Seite 137</a>.</p>
Motive	<p>Steuert das Erscheinungsbild der Identity Manager-Benutzeroberfläche.</p> <p>Weitere Informationen finden Sie in <a href="#">Kapitel 8, „Konfiguration von Motiven“</a>, auf <a href="#">Seite 175</a>.</p>
Portletadministration	<p>Steuert, welche Portlets über die Benutzeroberfläche von Identity Manager verfügbar sind und wer eine Zugriffsberechtigung erhalten soll.</p> <p>Weitere Informationen finden Sie in <a href="#">Kapitel 9, „Portletadministration“</a>, auf <a href="#">Seite 181</a>.</p>
Portal	<p>Steuert die Portaleigenschaften der Identity Manager-Benutzeranwendung und legt fest, auf welche Weise die Benutzeranwendung eine Verbindung mit dem Identitätsdepot (LDAP-Anbieter) aufbaut.</p> <p>Weitere Informationen finden Sie in <a href="#">Kapitel 10, „Portalkonfiguration“</a>, auf <a href="#">Seite 201</a>.</p>
Sicherheit	<p>Legt den Benutzeranwendungsadministrator für die Identity Manager-Benutzeranwendung fest.</p> <p>Weitere Informationen finden Sie in <a href="#">Kapitel 11, „Sicherheitskonfiguration“</a>, auf <a href="#">Seite 209</a>.</p>
Protokollierung	<p>Steuert den Umfang der Protokollierungsmeldungen, die von der Identity Manager-Benutzeranwendung generiert werden, und legt fest, ob diese Meldungen an Novell Audit gesendet werden.</p> <p>Weitere Informationen finden Sie in <a href="#">Kapitel 12, „Konfiguration der Protokollierung“</a>, auf <a href="#">Seite 213</a>.</p>
Caching	<p>Verwaltet verschiedene Cache-Speicher, die von der Identity Manager-Benutzeranwendung geführt werden.</p> <p>Weitere Informationen finden Sie in <a href="#">Kapitel 13, „Cache-Konfiguration“</a>, auf <a href="#">Seite 219</a>.</p>
Werkzeuge	<p>Ermöglicht Ihnen den Export oder Import der in der Identity Manager-Benutzeranwendung verwendeten Portalinhalte (Seiten und Portlets).</p> <p>Weitere Informationen finden Sie in <a href="#">Kapitel 14, „Werkzeuge zum Exportieren und Importieren von Portaldaten“</a>, auf <a href="#">Seite 229</a>.</p>



In diesem Kapitel erfahren Sie, wie Sie die Seite *Seitenadministration* auf der Registerkarte *Administration* der Benutzeroberfläche von Identity Manager verwenden. Es werden folgende Themen erläutert:

- [Abschnitt 7.1, „Allgemeines zur Seitenadministration“](#), auf Seite 137
- [Abschnitt 7.2, „Erstellen und Verwalten von Containerseiten“](#), auf Seite 145
- [Abschnitt 7.3, „Erstellen und Verwalten von freigegebenen Seiten“](#), auf Seite 154
- [Abschnitt 7.4, „Zuweisen von Seitenberechtigungen“](#), auf Seite 164
- [Abschnitt 7.5, „Einrichten von Standardseiten für Gruppen“](#), auf Seite 170
- [Abschnitt 7.6, „Auswahl einer standardmäßigen freigegebenen Seite für eine Containerseite“](#), auf Seite 172

Allgemeine Informationen zum Zugriff auf die und zum Arbeiten mit der Registerkarte „Administration“ finden Sie in [Kapitel 6, „Verwendung der Registerkarte „Administration““](#), auf Seite 131.

## 7.1 Allgemeines zur Seitenadministration

Die Seite „Seitenadministration“ dient der Steuerung der in der Benutzeroberfläche von Identity Manager angezeigten *Seiten* und der zugehörigen *Berechtigungen*. Die Benutzeroberfläche enthält *zwei Arten von Seiten*:

Art der Seite	Beschreibung
Container	Containerseiten enthalten freigegebene Seiten und sorgen dafür, dass diese über ein einheitliches Erscheinungsbild, Corporate Branding und einheitliche Navigationsfunktionen verfügen.
Freigegeben	Freigegebene Seiten bieten einen zusammenhängenden Inhalt, der für bestimmte Zwecke (z. B. für die Aktualisierung eines Benutzerprofils) verwendet wird. Sie werden als „freigegebene Seiten“ bezeichnet, weil sie Services anbieten, die von mehreren Personen verwendet werden.

Beide Arten von Seiten enthalten Inhalt in Form von *Portlets* (ein Java-Standard für Plugin-Elemente der Benutzeroberfläche).

Weitere Informationen zu Portlets finden Sie in [Kapitel 9, „Portletadministration“](#), auf Seite 181 und [Teil IV, „Portlet-Referenz“](#), auf Seite 237.

### 7.1.1 Allgemeines zu Containerseiten

Dieser Abschnitt bietet eine Einführung in einige Containerseiten, die in der Benutzeroberfläche von Identity Manager eine wichtige Funktion haben:

- [„GuestContainerPage“](#) auf Seite 138
- [„DefaultContainerPage“](#) auf Seite 140

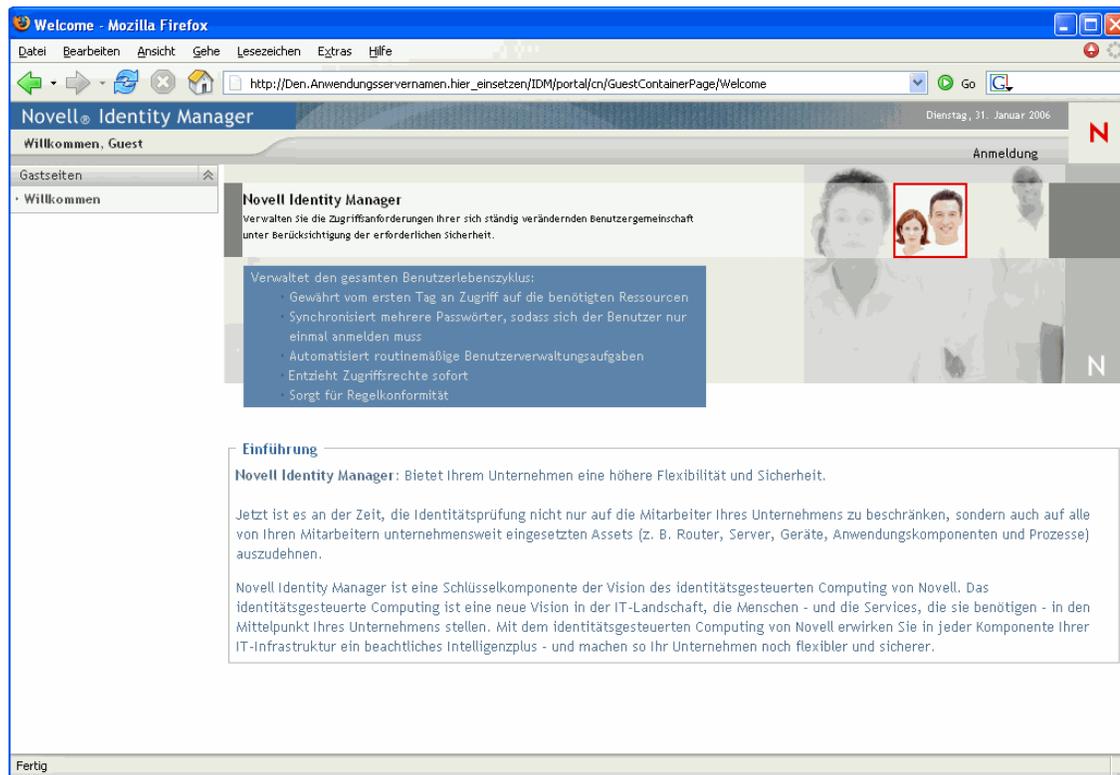
- „Admin-Containerseite“ auf Seite 142

Sie können diese Containerseiten bei Bedarf ändern. Es besteht außerdem die Möglichkeit, eigene Containerseiten hinzuzufügen.

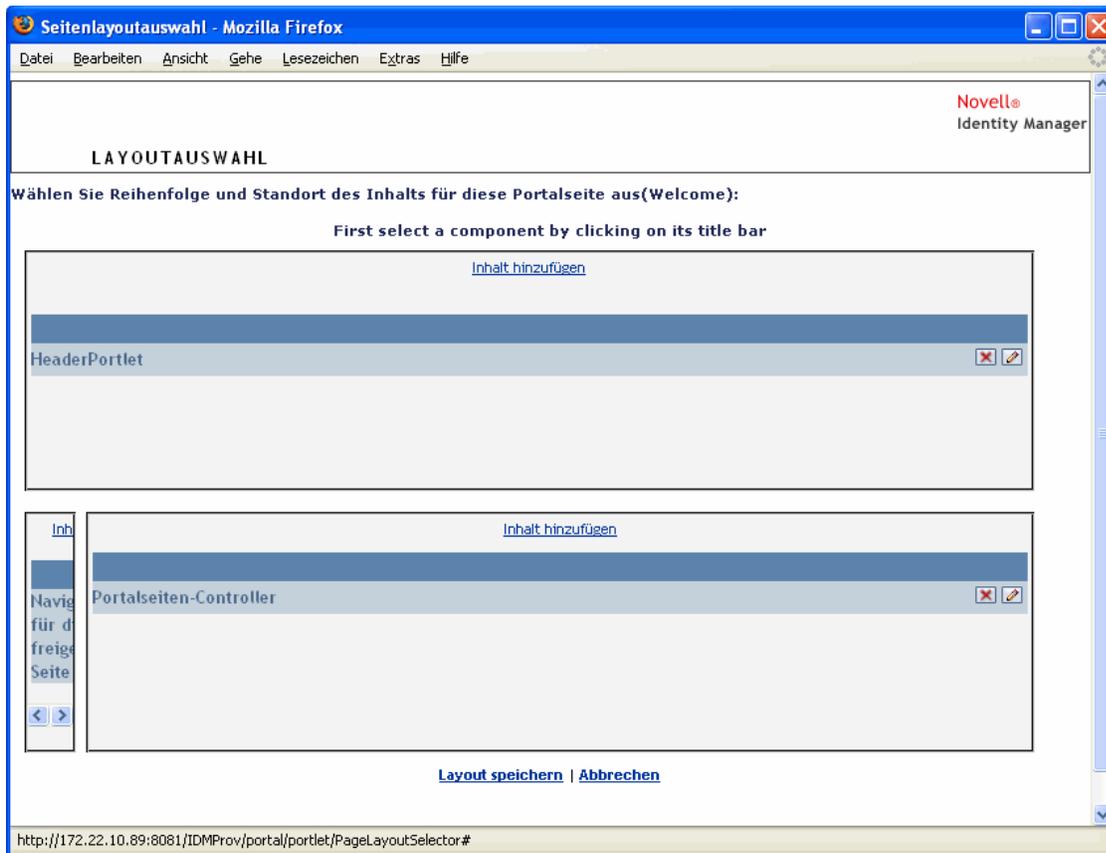
Weitere Informationen zum Arbeiten mit Containerseiten finden Sie in [Abschnitt 7.2, „Erstellen und Verwalten von Containerseiten“](#), auf Seite 145.

## GuestContainerPage

Wenn Benutzer die Identity Manager-Benutzeroberfläche aufrufen, wird *vor der Anmeldung* die Containerseite namens *GuestContainerPage* angezeigt. Die angezeigte Containerseite sieht wie folgt aus:



Intern hat die Seite „GuestContainerPage“ folgendes *Layout*:



Das Layout der Seite „GuestContainerPage“ ist in *drei Bereiche* unterteilt, in denen die folgenden Portlets angezeigt werden:

Portlet	Beschreibung
HeaderPortlet	Zeigt die Header-Informationen und die Registerkarten der obersten Ebene für die Benutzeroberfläche an.
Navigation für die freigegebene Seite	Zeigt ein vertikales Menü an, in dem der Benutzer eine freigegebene Seite zum Anzeigen auswählen kann.
Portalseiten-Controller	Zeigt die freigegebene Seite an, die der Benutzer mithilfe des Portlets „Navigation für die freigegebene Seite“ aktuell ausgewählt hat.

Beachten Sie, dass die Benutzer vor der Anmeldung in diesen Portlets standardmäßig nur die folgenden Inhalte sehen:

- Ein Link im Header: *Anmeldung*
- Eine freigegebene Seite: *Willkommen*

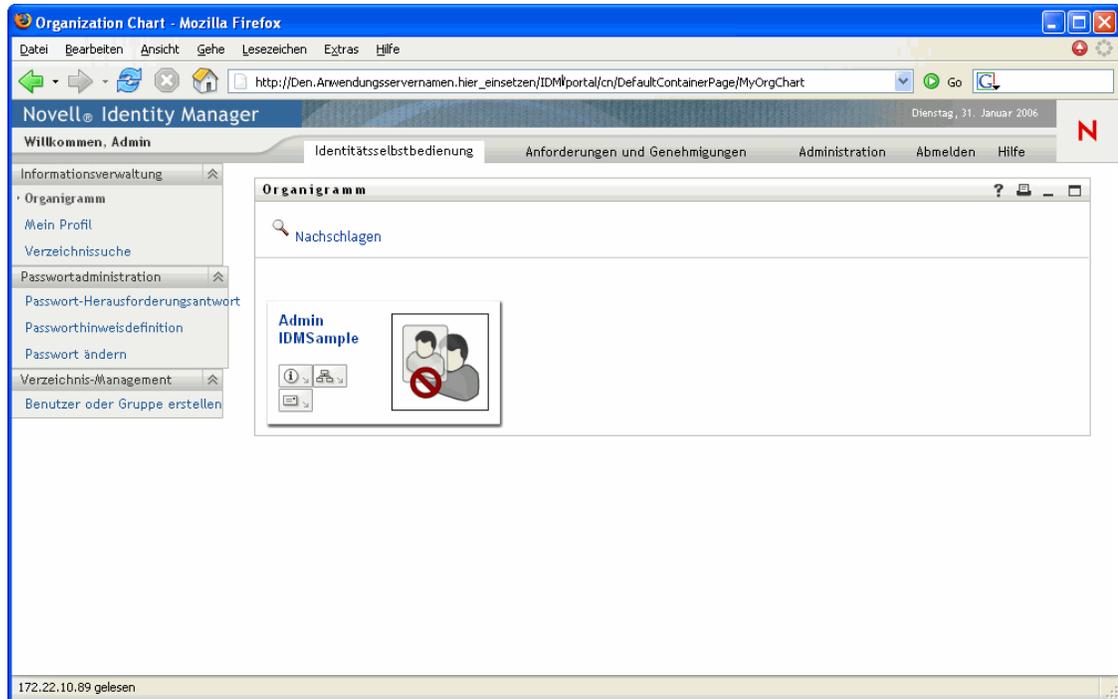
Da der Benutzer noch nicht angemeldet ist, zeigt das Portlet „Navigation für die freigegebene Seite“ nur die freigegebenen Seiten der Kategorie *Gastseiten* an. Alle anderen Kategorien werden herausgefiltert. Standardmäßig gehört nur die Begrüßungsseite zur Kategorie „Gastseiten“.

Nach der Anmeldung filtert das Portlet „Navigation für die freigegebene Seite“ die Kategorie der Gastseiten heraus. Stattdessen werden die anderen Kategorien der freigegebenen Seiten angezeigt (wie in den Standardeinstellungen angegeben).

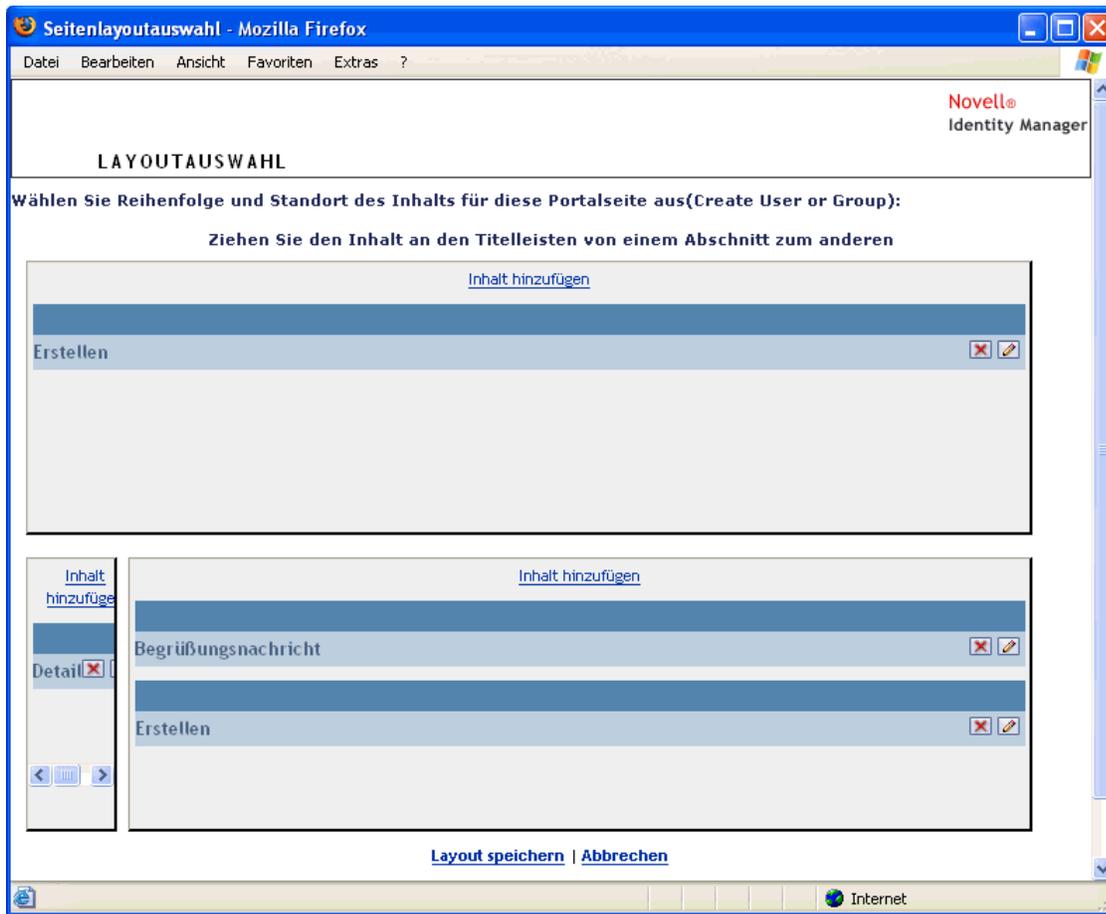
Weitere Informationen zum Portlet „Navigation für die freigegebene Seite“ finden Sie in [Kapitel 15](#), „Allgemeines zu Portlets“, auf Seite 239.

## DefaultContainerPage

Standardmäßig wird *nach der Anmeldung* bei der Identity Manager-Benutzeroberfläche der Container *DefaultContainerPage* angezeigt. Die angezeigte Containerseite sieht wie folgt aus:



Intern hat die Seite „DefaultContainerPage“ folgendes *Layout*:



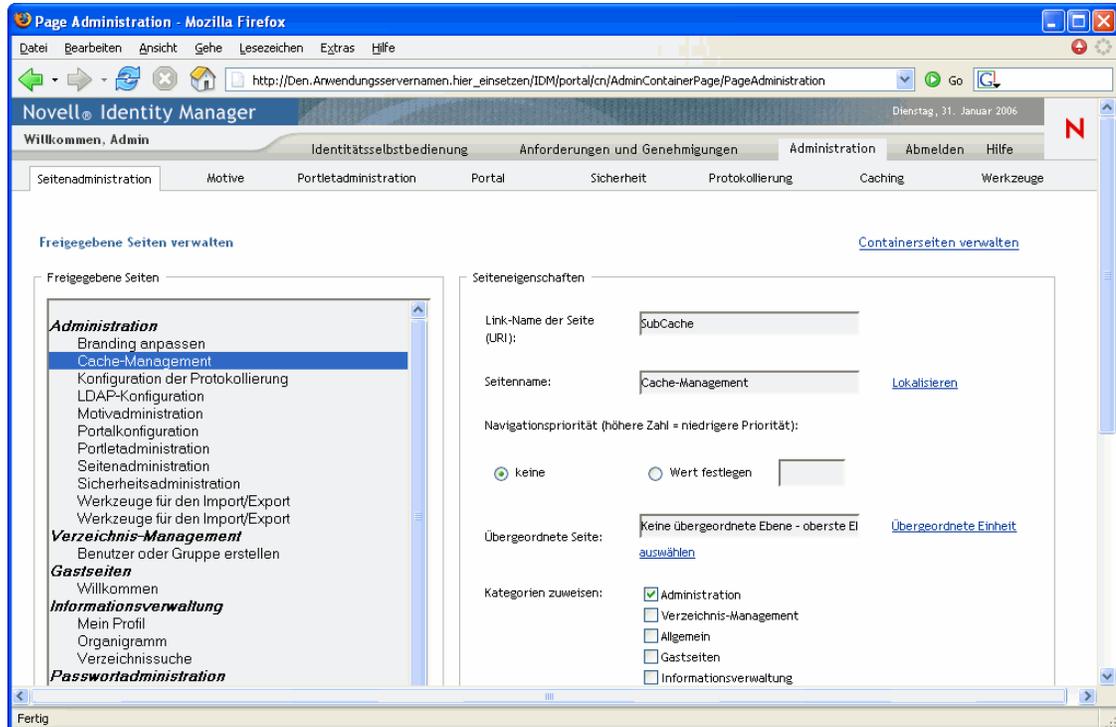
Das Layout der Seite „DefaultContainerPage“ ist in *drei Bereiche* unterteilt, in denen die folgenden Portlets angezeigt werden:

Portlet	Beschreibung
HeaderPortlet	Zeigt die Header-Informationen und die Registerkarten der obersten Ebene für die Benutzeroberfläche an.
Navigation für die freigegebene Seite	Zeigt ein vertikales Menü an, in dem der Benutzer eine freigegebene Seite zum Anzeigen auswählen kann.
Portalseiten-Controller	Zeigt die freigegebene Seite an, die der Benutzer mithilfe des Portlets „Navigation für die freigegebene Seite“ aktuell ausgewählt hat.
Warnmeldung für die Sitzungszeitüberschreitung	Zeigt kurz vor der Zeitüberschreitung einer Benutzersitzung eine Warnmeldung an.

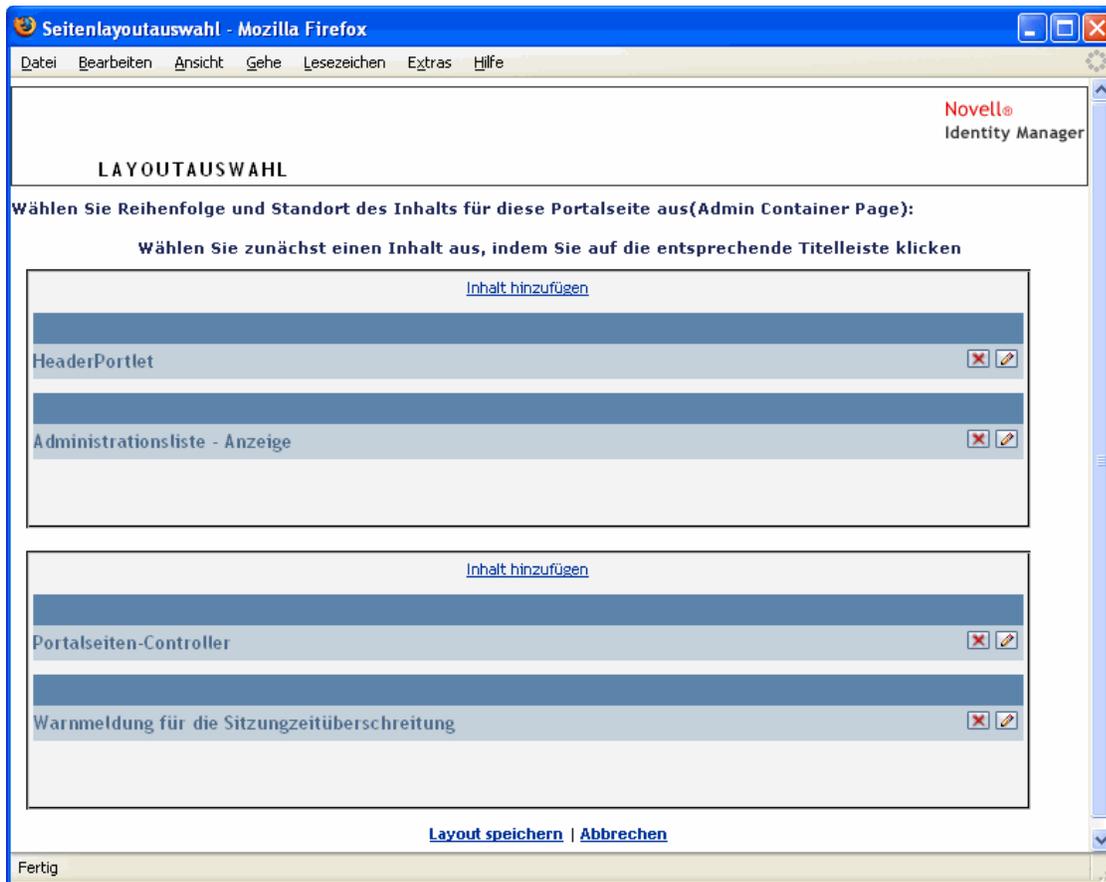
Beachten Sie, dass nach der Anmeldung eines Benutzers *DefaultContainerPage* automatisch die Registerkarte „Identitätsselbstbedienung“ im HeaderPortlet öffnet.

## Admin-Containerseite

Wenn Benutzeranwendungsadministratoren (und andere autorisierte Benutzer) in der Identity Manager-Benutzeroberfläche auf die Registerkarte „Administration“ klicken, wird die Admin-Containerseite angezeigt. Die angezeigte Containerseite sieht wie folgt aus:



Intern hat die Admin-Containerseite folgendes *Layout*:



Das Layout der Admin-Containerseite ist in *zwei Bereiche* unterteilt, in denen die folgenden Portlets angezeigt werden:

Portlet	Beschreibung
HeaderPortlet	Zeigt die Header-Informationen und die Registerkarten der obersten Ebene für die Benutzeroberfläche an.
Administrationsliste - Anzeige	Zeigt eine zweite Ebene mit Registerkarten an, aus denen der Benutzer eine Verwaltungsaktion wählen kann.
Portalseiten-Controller	Zeigt eine freigegebene Seite an, die der vom Benutzer über das Portlet „Administrationsliste - Anzeige“ aktuell ausgewählten Registerkarte entspricht.
Warnmeldung für die Sitzungszeitüberschreitung	Zeigt kurz vor der Zeitüberschreitung einer Benutzersitzung eine Warnmeldung an.

## 7.1.2 Allgemeines zu freigegebenen Seiten

Die Identity Manager-Benutzeroberfläche enthält viele freigegebene Seiten, die den größten Teil des Inhalts der Containerseiten enthalten. Sie können diese freigegebenen Seiten bei Bedarf ändern. Es besteht außerdem die Möglichkeit, eigene freigegebene Seiten hinzuzufügen.

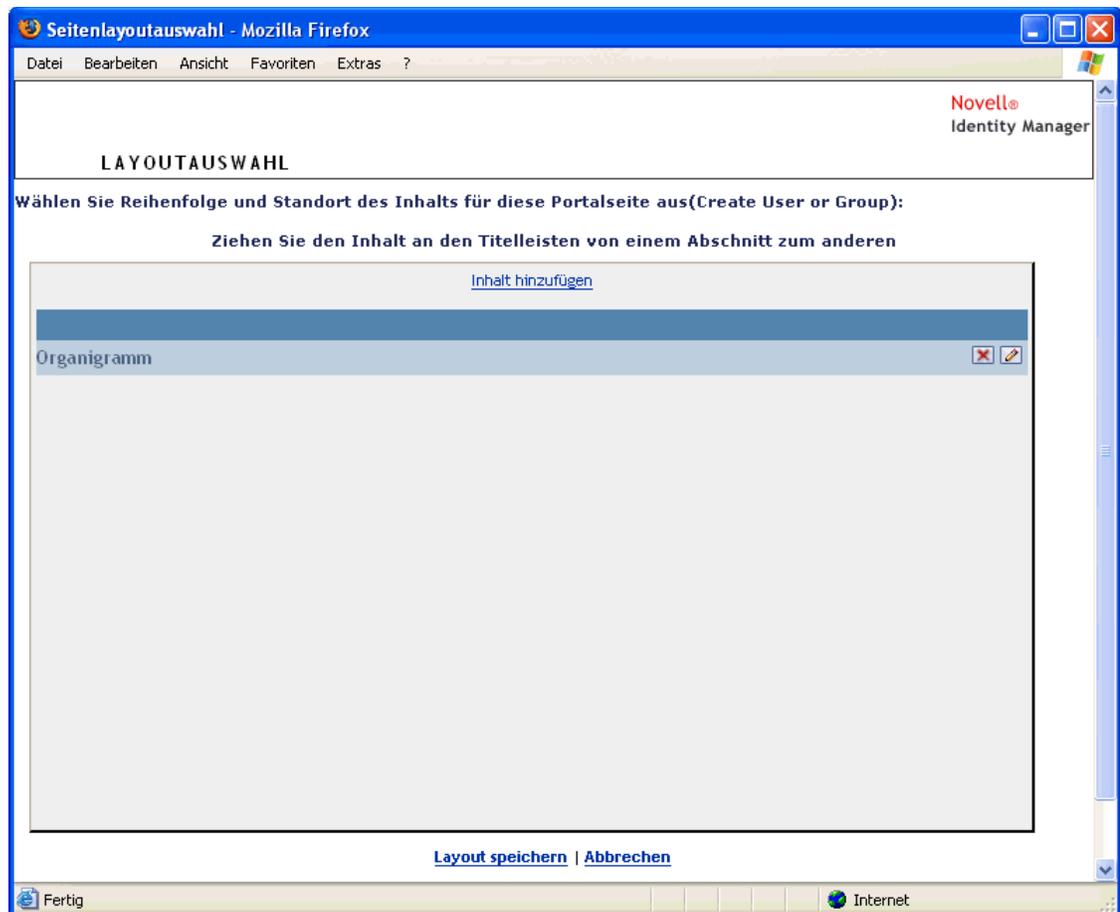
Weitere Informationen zum Arbeiten mit freigegebenen Seiten finden Sie in [Abschnitt 7.3](#), „Erstellen und Verwalten von freigegebenen Seiten“, auf Seite 154.

### Eine typische freigegebene Seite

Im Folgenden ist eine dieser freigegebenen Seiten abgebildet. Die *standardmäßige freigegebene Seite* ist *Organigramm*. Sie wird von der DefaultContainerPage angezeigt, nachdem sich ein Benutzer bei der Identity Manager-Benutzeroberfläche angemeldet hat:



Intern hat die Seite „Organigramm“ folgendes *Layout*:



Das Layout der Seite „Organigramm“ besteht nur aus *einem Bereich*, in dem nur ein Portlet (das Portlet *Organigramm*) angezeigt wird.

### 7.1.3 Eine Ausnahme bei der Verwendung von Seiten

In diesem Kapitel haben Sie erfahren, dass die Registerkarten der oberen Ebene der Identity Manager-Benutzeroberfläche auf Seiten basieren:

- Die Registerkarte *Identitätsselbstbedienung* verwendet die *DefaultContainerPage*
- Die Registerkarte *Administration* verwendet die *Admin-Containerseite*

Beachten Sie, dass die Registerkarte *Anforderungen und Genehmigungen* auf einer anderen Architektur basiert und *nicht über die Seitenadministration bearbeitet werden kann*.

## 7.2 Erstellen und Verwalten von Containerseiten

Der Vorgang zum Erstellen und Verwalten von Containerseiten besteht aus den folgenden Schritten:

- 1 *Erstellen* einer neuen Containerseite oder *Auswählen* einer vorhandenen Containerseite, wie in [Abschnitt 7.2.1, „Erstellen von Containerseiten“](#), auf Seite 145 beschrieben.
- 2 *Hinzufügen von Inhalt* (in Form von Portlets) zur Seite, wie in [Abschnitt 7.2.2, „Hinzufügen von Inhalt zu einer Containerseite“](#), auf Seite 148 beschrieben.  
Es können auch *Inhalte von der Seite gelöscht* werden, wie in [Abschnitt 7.2.3, „Inhalt von einer Containerseite löschen“](#), auf Seite 149 beschrieben.
- 3 *Auswählen eines Portallayouts*, wie in [Abschnitt 7.2.4, „Ändern des Layouts einer Containerseite“](#), auf Seite 150 beschrieben.
- 4 *Anordnen der Reihenfolge und Position* des Inhalts im ausgewählten Layout, wie in [Abschnitt 7.2.5, „Inhalt auf einer Containerseite anordnen“](#), auf Seite 151 beschrieben.
- 5 *Direkte Anzeige der neuen Seite* durch Eingabe der URL der Containerseite in Ihrem Browser, wie in [Abschnitt 7.2.6, „Anzeigen einer Containerseite“](#), auf Seite 153 beschrieben.

**Containerseiten und -layouts** Containerseiten sind nicht an Portallayouts gebunden. Dies bedeutet, dass Sie das Layout von Containerseiten ändern können, ohne dabei Seiteninhalte zu verlieren. Wenn Sie ein neues Layout auf eine Containerseite anwenden, werden alle zur Seite hinzugefügten Portlets automatisch im neuen Layout angezeigt. Möglicherweise muss die Anordnung des Inhalts im neuen Layout korrigiert werden.

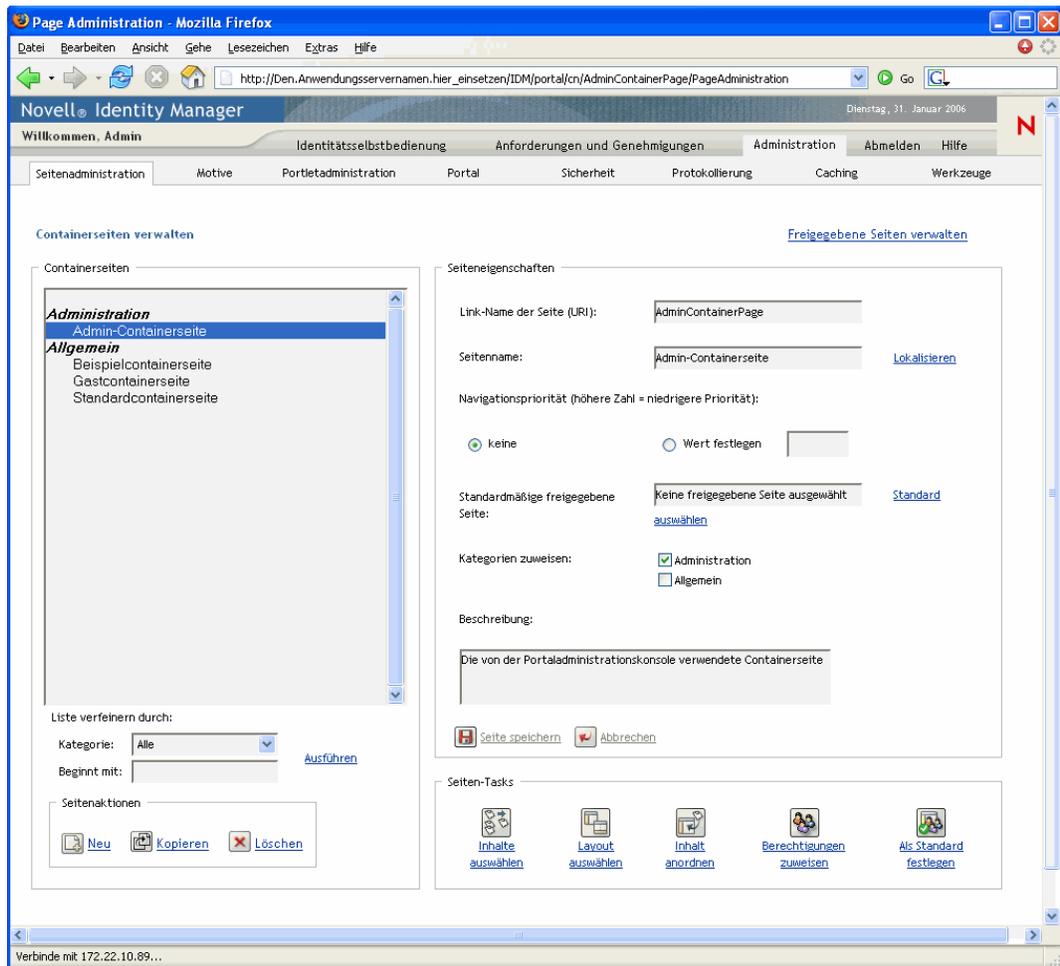
### 7.2.1 Erstellen von Containerseiten

Sie können Containerseiten ganz neu erstellen oder vorhandene Seiten kopieren. In diesem Abschnitt werden beide Vorgehensweisen beschrieben.

So erstellen Sie eine Containerseite neu:

- 1 Wählen Sie auf der Seite „Seitenadministration“ *Containerseiten verwalten* aus.

Das Teilfenster „Containerseiten verwalten“ wird angezeigt:



2 Wählen Sie die Seitenaktion *Neu* aus (unten links im Teilfenster).

Es wird eine unbenannte, nicht kategorisierte Containerseite erstellt.

3 Legen Sie die *Seiteneigenschaften* der Containerseite fest:

Eigenschaft	Vorgehensweise
Link-Name der Seite (URI)	Geben Sie den URI-Namen für die Seite an (wie er in der URL der Benutzeroberfläche angezeigt werden soll). Wenn Sie beispielsweise den folgenden URI-Namen festlegen:  <div style="text-align: center;"> <pre>MeineContainerseite</pre> </div> wird dieser wie folgt in der URL angezeigt:  <div style="text-align: center;"> <pre>http://myappserver:8080/IDM/portal/cn/<b>MeineContainerseite</b></pre> </div>

Eigenschaft	Vorgehensweise
Seitenname	Legen Sie einen Anzeigenamen für die Seite fest. Zum Beispiel:  Meine Containerseite  Wenn Sie auf <b>Lokalisieren</b> klicken, wird der Name in andere Sprachen übersetzt.
Navigationspriorität	Wählen Sie eine der folgenden Optionen aus: <ul style="list-style-type: none"> <li>• <b>Keine</b>, falls der Containerseite keine Priorität zugewiesen werden soll.</li> <li>• <b>Wert festlegen</b>, um der Containerseite bezüglich anderer Containerseiten eine Priorität zuzuweisen. Die Priorität kann eine Ganzzahl zwischen -1 und 9999 annehmen, wobei -1 die höchste und 9999 die niedrigste Priorität ist.  Das Festlegen von Prioritätswerten ist nützlich, um bei einer Auflistung nach Priorität eine bestimmte Reihenfolge zu gewährleisten oder um sicherzustellen, dass bei mehreren vorhandenen Standardseiten (wenn ein Benutzer mehreren Gruppen angehört) eine bestimmte Auswahl vorgenommen wird.</li> </ul>
Standardmäßige freigegebene Seite	Weitere Informationen hierzu finden Sie in <a href="#">Abschnitt 7.6</a> , „Auswahl einer standardmäßigen freigegebenen Seite für eine Containerseite“, auf Seite 172.
Kategorien zuweisen	Wählen Sie keine oder mehrere der folgenden Kategorien für die Seite aus: <ul style="list-style-type: none"> <li>• Administration</li> <li>• Allgemein</li> </ul> <p>Das Zuweisen von Kategorien ist nützlich, um eine geeignete Organisation zu gewährleisten, wenn die Seiten nach Kategorien aufgelistet werden, oder um bei einer Filterung nach Kategorien die Anzeige einer bestimmten Teilmenge zu gewährleisten.</p>
Beschreibung	Geben Sie einen beschreibenden Text für die Seite ein.

**4** Klicken Sie auf *Seite speichern* (im unteren Bereich des Abschnitts „Seiteneigenschaften“).

So erstellen Sie eine Containerseite, indem Sie eine vorhandene Seite kopieren:

**1** Wählen Sie auf der Seite „Seitenadministration“ *Containerseiten verwalten* aus.

Das Teilfenster „Containerseiten verwalten“ wird angezeigt (siehe vorherige Vorgehensweise).

**2** Wählen Sie in der Liste der Containerseiten die zu kopierende Seite aus.

---

**Tipp:** Eine lange Liste können Sie *strukturieren* (nach Kategorie oder Textanfang), damit Sie die gewünschte Seite leichter finden.

---

**3** Wählen Sie die Seitenaktion *Kopieren* aus (unten links im Teilfenster).

Es wird eine neue Containerseite mit dem Namen *Kopie von <Name der Originalseite>* erstellt.

**4** Legen Sie die *Seiteneigenschaften* der Containerseite (wie zuvor beschrieben) fest.

5 Klicken Sie auf *Seite speichern* (im unteren Bereich des Abschnitts „Seiteneigenschaften“).

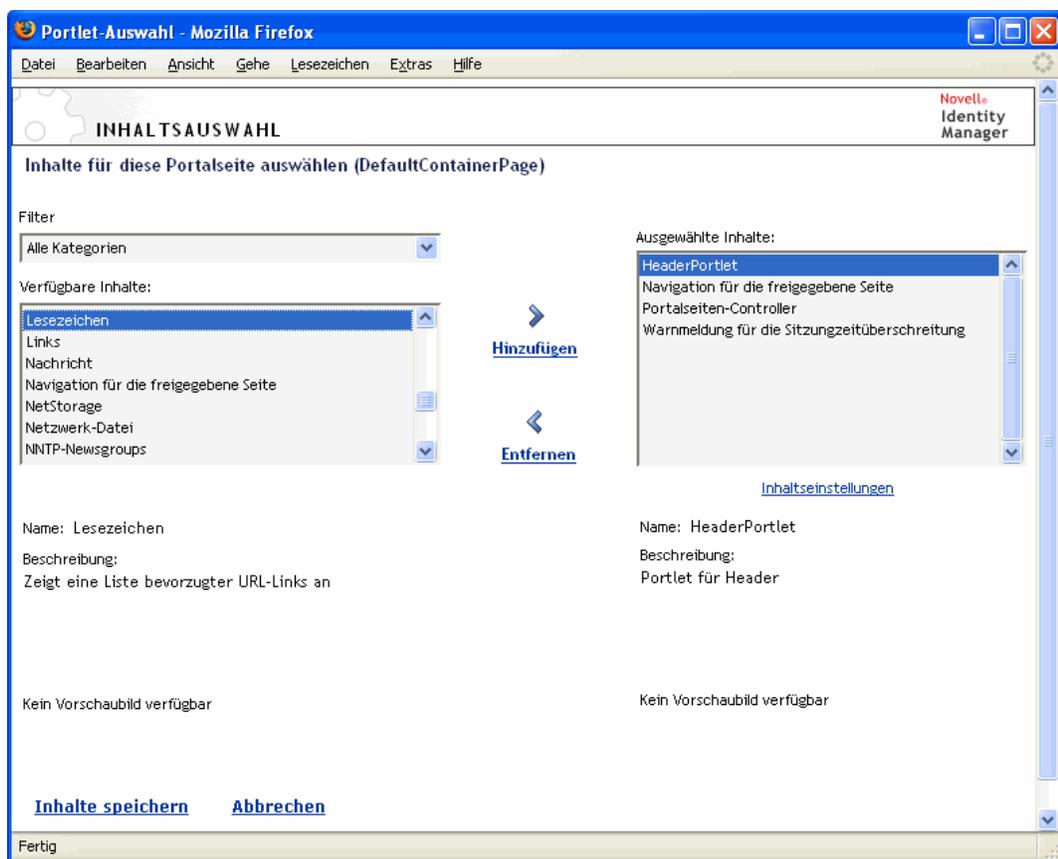
## 7.2.2 Hinzufügen von Inhalt zu einer Containerseite

Nach dem Erstellen einer Containerseite können Sie im nächsten Schritt Inhalt hinzufügen, indem Sie Portlets auswählen und diese auf der Seite platzieren. Sie können vordefinierte Portlets, die im Lieferumfang der Identity Manager-Benutzeranwendung enthalten sind, oder andere von Ihnen registrierte Portlets verwenden.

So fügen Sie Inhalt zu einer Containerseite hinzu:

- 1 Öffnen Sie im Teilfenster „Containerseiten verwalten“ eine neue oder vorhandene Seite und klicken Sie auf die Seitenaufgabe *Inhalt auswählen* (im unteren Bereich des Teilfensters).

Die Seite *Inhaltsauswahl* wird in einem neuen Browserfenster angezeigt:



- 2 Wenn Sie eine bestimmte Kategorie des verfügbaren Inhalts anzeigen möchten, wählen Sie eine Kategorie aus dem Dropdown-Menü *Filter* aus.
- 3 Wählen Sie in der Liste *Verfügbare Inhalte* ein oder mehrere Portlets aus.

---

**Tipp:** Halten Sie die *Strg*-Taste gedrückt, um mehrere nicht direkt untereinander stehende Portlets auszuwählen. Mit der *Umschalttaste* können Sie mehrere direkt untereinander stehende Portlets auswählen.

---

- 4 Wenn Sie auf *Hinzufügen* klicken, werden die ausgewählten Elemente in die Liste *Ausgewählte Inhalte* verschoben.
- 5 Klicken Sie zum Bearbeiten der Einstellungen eines beliebigen Portlets, das Sie für Ihre Containerseite ausgewählt haben, auf *Inhaltseinstellungen*. Die von Ihnen angegebenen Werte der Standardeinstellungen gelten für die Instanz des Portlets, das auf Ihrer Seite angezeigt wird.
- 6 Klicken Sie auf *Inhalte speichern*.

Nachdem Sie den Inhalt für Ihre Containerseite festgelegt haben, können Sie (wie in [Abschnitt 7.2.4, „Ändern des Layouts einer Containerseite“](#), auf Seite 150 beschrieben) ein neues Layout auswählen oder den Inhalt im aktuellen Layout anordnen (wie in [Abschnitt 7.2.5, „Inhalt auf einer Containerseite anordnen“](#), auf Seite 151 beschrieben).

### 7.2.3 Inhalt von einer Containerseite löschen

Beim Erstellen von Containerseiten können Inhalte gelöscht werden, indem Sie Portlets von einer Seite entfernen. Sie können hierzu die Inhaltsauswahl oder die Layoutauswahl verwenden, wie im Folgenden beschrieben.

So löschen Sie mithilfe der Inhaltsauswahl Inhalte von einer Containerseite:

- 1 Öffnen Sie eine Seite im Teilfenster „Containerseiten verwalten“ und klicken Sie auf die Seitenaufgabe *Inhalt auswählen* (im unteren Bereich des Teilfensters).

Die Seite *Inhaltsauswahl* wird in einem neuen Browserfenster angezeigt (wie zuvor dargestellt).

- 2 Wählen Sie ein zu löschendes Portlet in der Liste „Ausgewählte Inhalte“ aus und klicken Sie auf *Entfernen*.

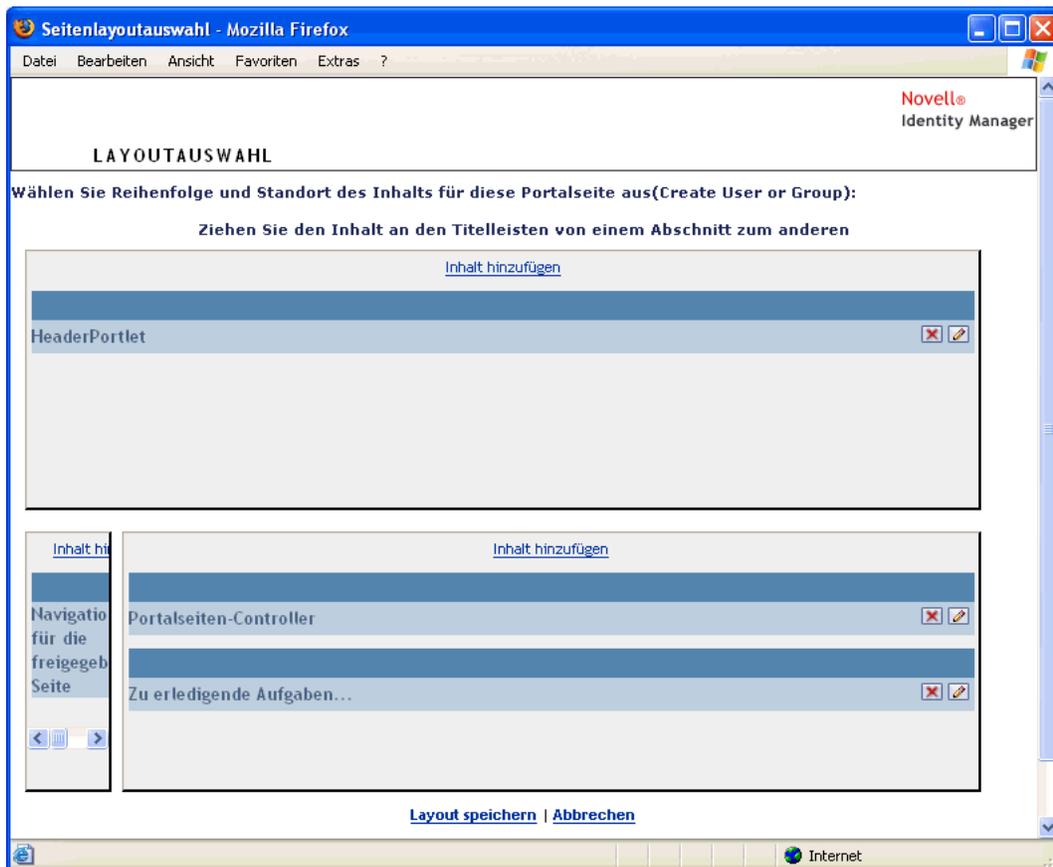
Das Portlet wird von der Seite entfernt.

- 3 Klicken Sie auf *Inhalte speichern*.

So löschen Sie mithilfe der Layoutauswahl Inhalte von einer Containerseite:

- 1 Öffnen Sie eine Seite im Teilfenster „Containerseiten verwalten“ und klicken Sie auf die Seitenaufgabe *Inhalt anordnen* (im unteren Bereich des Teilfensters).

Die *Layoutauswahl* wird in einem neuen Browserfenster aufgerufen. Die Seite enthält die folgenden Portlets:



- 2 Wählen Sie ein Portlet aus und klicken Sie zum Entfernen auf *X*.
- 3 Klicken Sie zum Bestätigen des Löschvorgangs auf *OK*.  
Das Portlet wird von der Seite entfernt.
- 4 Klicken Sie auf *Layout speichern*.

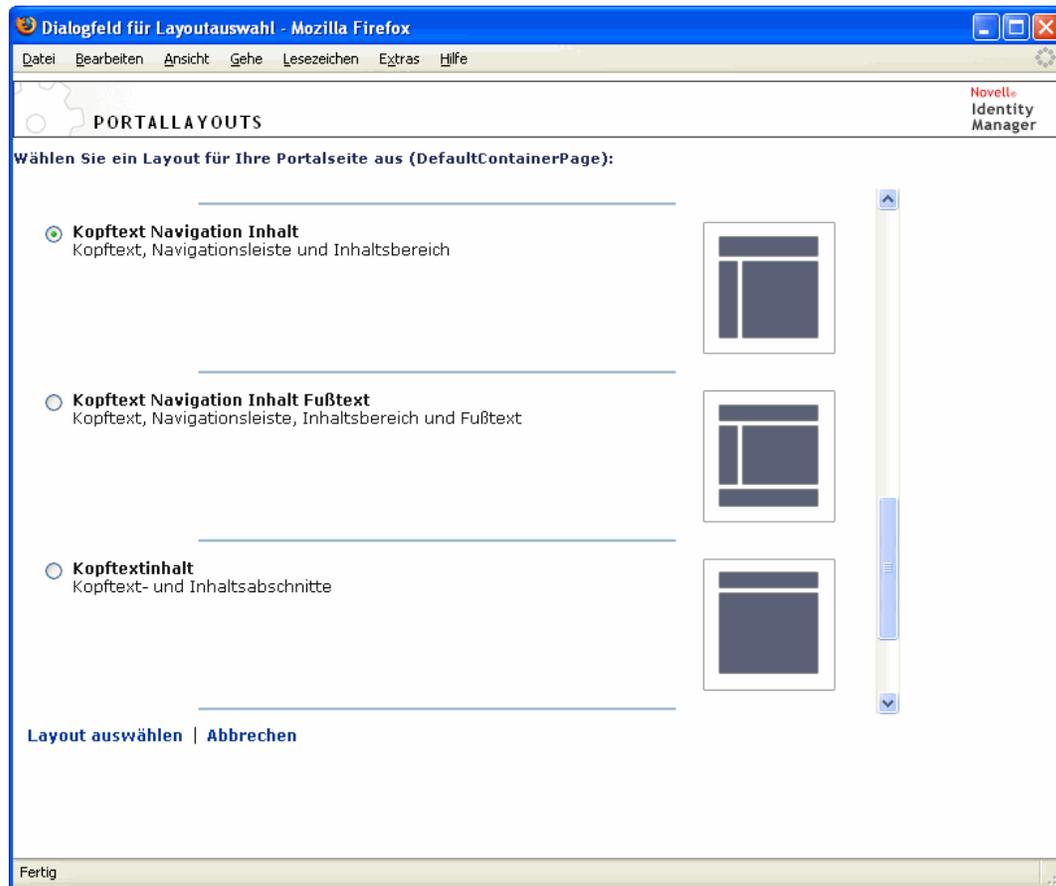
## 7.2.4 Ändern des Layouts einer Containerseite

Wenn Sie das Layout einer Containerseite ändern, wird der vorhandene Inhalt in das neue Layout eingefügt. In einigen Fällen muss gegebenenfalls die Anordnung des Inhalts korrigiert werden.

So ändern Sie das Layout einer Containerseite:

- 1 Öffnen Sie eine Seite im Teilfenster „Containerseiten verwalten“ und klicken Sie auf die Seitenaufgabe *Layout auswählen* (im unteren Bereich des Teilfensters).

Die Liste *Portallayouts* wird in einem neuen Browserfenster angezeigt:



**2** *Blättern* Sie durch die Auswahlmöglichkeiten und *wählen* Sie das gewünschte Layout aus.

**3** Klicken Sie auf *Layout auswählen*.

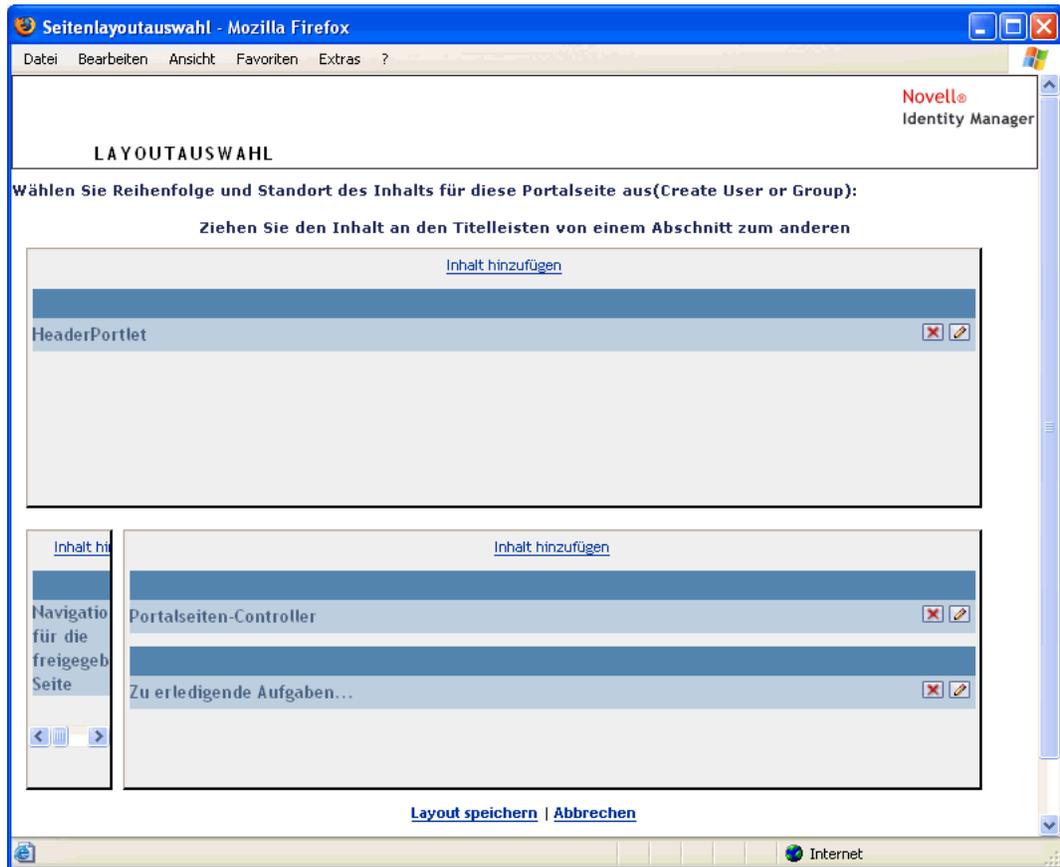
## 7.2.5 Inhalt auf einer Containerseite anordnen

Nachdem Sie den Inhalt und das Layout Ihrer Containerseite bestimmt haben, können Sie den Inhalt im ausgewählten Layout anordnen, an ausgewählten Stellen andere Portlets hinzufügen oder Portlets löschen.

So ordnen Sie Inhalt auf einer Containerseite an:

**1** Öffnen Sie eine Seite im Teilfenster „Containerseiten verwalten“ und klicken Sie auf die Seitenaufgabe *Inhalt anordnen* (im unteren Bereich des Teilfensters).

Die *Layoutauswahl* wird in einem neuen Browserfenster aufgerufen. Die Seite enthält die folgenden Portlets:



- 2 Führen Sie folgende Schritte aus, um einer Seite *ein Portlet hinzuzufügen*:
  - 2a Klicken Sie im gewünschten Layoutrahmen auf *Inhalt hinzufügen*.

Die Seite *Portlet-Auswahl* wird in einem neuen Browserfenster angezeigt.
  - 2b Wenn Sie eine bestimmte Kategorie des verfügbaren Inhalts anzeigen möchten, wählen Sie eine Kategorie aus dem Dropdown-Menü *Filter* aus.
  - 2c Wählen Sie das gewünschte Portlet in der Liste *Verfügbare Inhalte* aus.
  - 2d Klicken Sie auf *Inhalt auswählen*.

Die Portlet-Auswahl wird geschlossen und das ausgewählte Portlet wird im angegebenen Layoutrahmen in der Layoutauswahl angezeigt.
- 3 Wenn Sie ein Portlet an eine andere Position im Layout *verschieben* möchten, führen Sie diese browserspezifischen Schritte aus:

Browser	Vorgehensweise
Internet Explorer	<ol style="list-style-type: none"> <li>1. Bewegen Sie den Mauszeiger über die Titelleiste des Portlets, bis er die Form einer Hand annimmt.</li> <li>2. Halten Sie die linke Maustaste gedrückt und ziehen Sie das Portlet an die gewünschte Position im Layout.</li> </ol>
Mozilla	<ol style="list-style-type: none"> <li>1. Klicken Sie auf das Portlet, das Sie verschieben möchten.</li> <li>2. Klicken Sie in den Layoutrahmen, in dem es angezeigt werden soll.</li> </ol> <p>Das Portlet wird an das ausgewählte Ziel verschoben.</p>

**4** Führen Sie folgende Schritte aus, um *ein Portlet aus dem Layout zu entfernen*:

**4a** Wählen Sie ein Portlet aus und klicken Sie zum Entfernen auf *X*.

**4b** Klicken Sie zum Bestätigen des Löschvorgangs auf *OK*.

Das Portlet wird aus dem Layout entfernt.

**5** Führen Sie folgende Schritte aus, um die *Einstellungen eines Portlets zu bearbeiten*:

**5a** Wählen Sie ein Portlet aus und klicken Sie zum Bearbeiten auf die *Bleistift*-Schaltfläche.

Die *Inhaltseinstellungen* des Portlets werden in Ihrem Browser angezeigt.

**5b** *Ändern* Sie die Werte der Standardeinstellung nach Bedarf.

Die von Ihnen angegebenen Werte der Standardeinstellungen gelten für die Instanz des Portlets, das auf Ihrer Seite angezeigt wird.

**5c** Klicken Sie auf *Standardeinstellungen speichern*.

**6** Klicken Sie zum Speichern Ihrer Änderungen auf *Layout speichern* und schließen Sie das Fenster „Layoutauswahl“.

## 7.2.6 Anzeigen einer Containerseite

Sie können Ihre Seite anzeigen, indem Sie in Ihrem Browser zur URL der Containerseite wechseln.

### So zeigen Sie eine Containerseite an:

- Rufen Sie in Ihrem *Webbrowser* folgende URL auf:

`http://server:port/IDM-war-context/portal/cn/container-page-name`

Z. B. zum Anzeigen der Containerseite *MeineContainerseite*:

`http://myappserver:8080/IDM/portal/cn/MeineContainerseite`

## 7.3 Erstellen und Verwalten von freigegebenen Seiten

Der Vorgang des Erstellens und Verwaltens von freigegebenen Seiten besteht aus den folgenden Schritten:

- 1 *Erstellen* einer neuen freigegebenen Seite oder *Auswählen* einer vorhandenen freigegebenen Seite, wie in [Abschnitt 7.3.1, „Erstellen von freigegebenen Seiten“](#), auf Seite 154 beschrieben.
- 2 *Hinzufügen von Inhalt* (in Form von Portlets) zur Seite, wie in [Abschnitt 7.3.2, „Inhalt zu einer freigegebenen Seite hinzufügen“](#), auf Seite 157 beschrieben.  
Es können auch *Inhalte von der Seite gelöscht* werden, wie in [Abschnitt 7.3.3, „Inhalt von einer freigegebenen Seite löschen“](#), auf Seite 159 beschrieben.
- 3 *Auswählen eines Portallayouts*, wie in [Abschnitt 7.3.4, „Ändern des Layouts einer freigegebenen Seite“](#), auf Seite 160 beschrieben.
- 4 *Anordnen der Reihenfolge und Position* des Inhalts im ausgewählten Layout, wie in [Abschnitt 7.3.5, „Anordnen von Inhalt auf einer freigegebenen Seite“](#), auf Seite 161 beschrieben.
- 5 *Direkte Anzeige der neuen Seite* durch Eingabe der URL der freigegebenen Seite in Ihrem Browser, wie in [Abschnitt 7.3.6, „Anzeigen einer freigegebenen Seite“](#), auf Seite 163 beschrieben.

**Freigegebene Seiten und Layouts** Freigegebene Seiten sind nicht an Portallayouts gebunden. Dies bedeutet, dass Sie das Layout von freigegebenen Seiten ändern können, ohne dabei Seiteninhalte zu verlieren. Wenn ein neues Layout angewendet wird, werden alle zur Seite hinzugefügten Portlets automatisch im neuen Layout angezeigt. Möglicherweise muss die Anordnung des Inhalts im neuen Layout korrigiert werden.

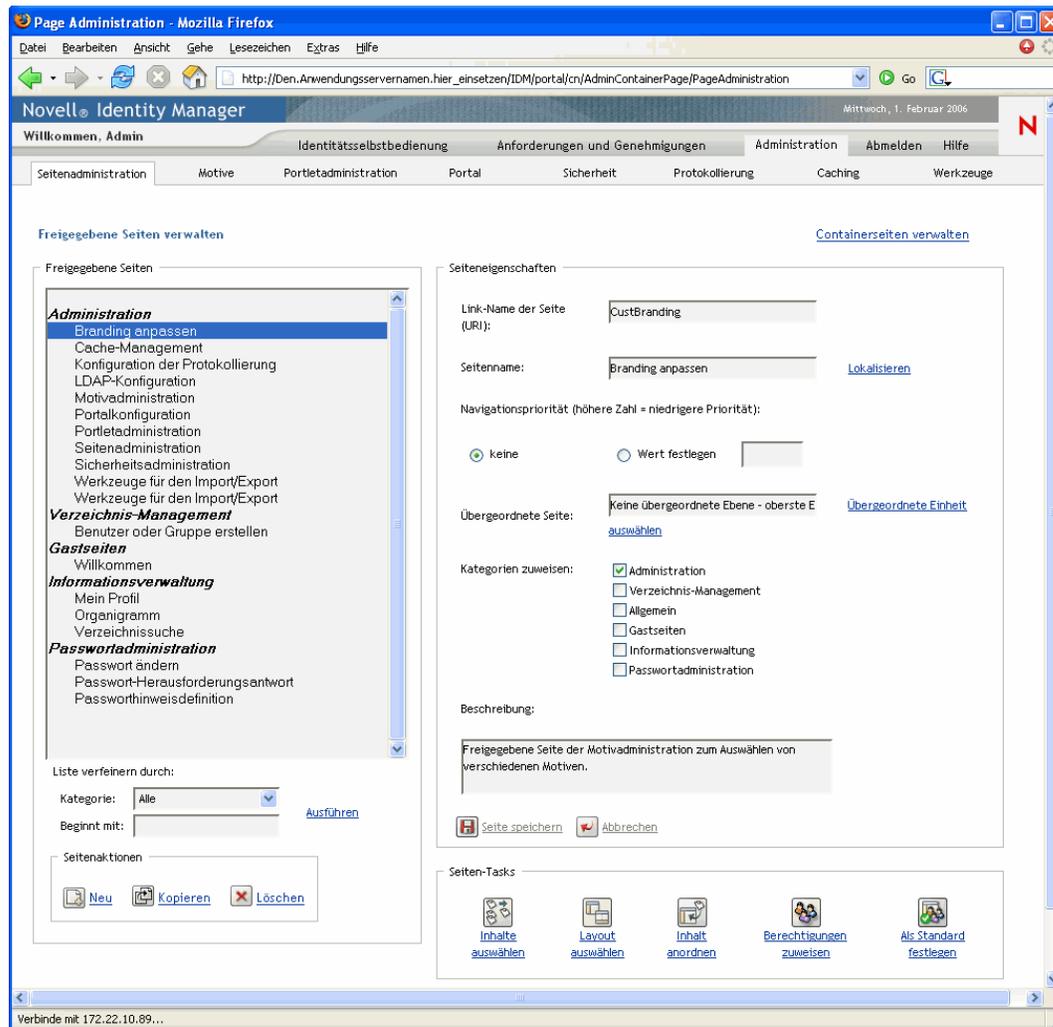
### 7.3.1 Erstellen von freigegebenen Seiten

Sie können freigegebene Seiten ganz neu erstellen oder vorhandene Seiten kopieren. In diesem Abschnitt werden beide Vorgehensweisen beschrieben.

So erstellen Sie eine freigegebene Seite neu:

- 1 Wählen Sie auf der Seite „Seitenadministration“ *Freigegebene Seiten verwalten* aus.

Das Teilfenster „Freigegebene Seiten verwalten“ wird angezeigt:



2 Wählen Sie die Seitenaktion *Neu* aus (unten links im Teilfenster).

Es wird eine unbenannte, nicht kategorisierte freigegebene Seite erstellt.

3 Legen Sie die *Seiteneigenschaften* der freigegebenen Seite fest:

Eigenschaft	Vorgehensweise
Link-Name der Seite (URI)	<p>Geben Sie den URI-Namen für die Seite an (wie er in der URL der Benutzeroberfläche angezeigt werden soll). Wenn Sie beispielsweise den folgenden URI-Namen festlegen:</p> <p><code>MeineFreigegebeneSeite</code></p> <p>wird dieser wie folgt in der URL angezeigt:</p> <p><code>http://myappserver:8080/IDM/portal/cn/MeineContainerseite/MeineFreigegebeneSeite</code></p>
Seitenname	<p>Legen Sie einen Anzeigenamen für die Seite fest. Zum Beispiel:</p> <p><code>Meine freigegebene Seite</code></p> <p>Wenn Sie auf <b>Lokalisieren</b> klicken, wird der Name in andere Sprachen übersetzt.</p>
Navigationspriorität	<p>Wählen Sie eine der folgenden Optionen aus:</p> <ul style="list-style-type: none"> <li>• <b>Keine</b>, falls der freigegebenen Seite keine Priorität zugewiesen werden soll.</li> <li>• <b>Wert festlegen</b>, um der freigegebenen Seite bezüglich anderer freigegebenen Seiten eine Priorität zuzuweisen. Die Priorität kann eine Ganzzahl zwischen -1 und 9999 annehmen, wobei -1 die höchste und 9999 die niedrigste Priorität ist.</li> </ul> <p>Das Festlegen von Prioritätswerten ist nützlich, um bei einer Auflistung nach Priorität eine bestimmte Reihenfolge zu gewährleisten oder um sicherzustellen, dass bei mehreren vorhandenen Standardseiten (wenn ein Benutzer mehreren Gruppen angehört) eine bestimmte Auswahl vorgenommen wird.</p>
Übergeordnete Seite	<p>Wenn diese freigegebene Seite einer anderen freigegebenen Seite untergeordnet sein soll, klicken Sie auf <b>Übergeordnete Einheit auswählen</b>. Stellen Sie sicher, dass die über- und die untergeordneten Seiten <b>denselben Kategorien</b> angehören (um Probleme bei der Anzeige zu vermeiden).</p> <p>Während der Laufzeit wird dem Endbenutzer diese Verbindung angezeigt, wenn er das Portlet „Navigation für die freigegebene Seite“ verwendet. Wenn die Liste mit den freigegebenen Seiten angezeigt wird, werden die übergeordneten Seiten mit ihren jeweiligen untergeordneten Seiten angezeigt.</p> <p>(Beachten Sie, dass untergeordnete Seiten keine Inhalte, Standardeinstellungen oder Einstellungen von den entsprechenden übergeordneten Seiten übernehmen. Umgekehrt zeigen die übergeordneten Seiten neben ihrem eigenen Inhalt nicht automatisch den Inhalt der untergeordneten Seiten an.)</p>

Eigenschaft	Vorgehensweise
Kategorien zuweisen	<p>Wählen Sie keine oder mehrere der folgenden Kategorien für die Seite aus:</p> <ul style="list-style-type: none"> <li>• Administration</li> <li>• Verzeichnis-Management</li> <li>• Allgemein</li> <li>• Gastseiten</li> <li>• Informationsverwaltung</li> <li>• Passwortverwaltung</li> </ul> <p>Das Zuweisen von Kategorien ist nützlich, um eine geeignete Organisation zu gewährleisten, wenn die Seiten nach Kategorien aufgelistet werden, oder um bei einer Filterung nach Kategorien die Anzeige einer bestimmten Teilmenge zu gewährleisten.</p> <hr/> <p><b>Hinweis:</b> <b>Gastseiten</b> sind eine spezielle Kategorie zum Identifizieren von freigegebenen Seiten, die vor der Anmeldung eines Benutzers (nicht danach) angezeigt werden können. Weitere Informationen finden Sie im Abschnitt zum Portlet „Navigation für die freigegebene Seite“ in <b>Kapitel 15, „Allgemeines zu Portlets“</b>, auf Seite 239.</p> <hr/>
Beschreibung	Geben Sie einen beschreibenden Text für die Seite ein.

**4** Klicken Sie auf *Seite speichern* (im unteren Bereich des Abschnitts „Seiteneigenschaften“).

So erstellen Sie eine freigegebene Seite, indem Sie eine vorhandene Seite kopieren:

**1** Wählen Sie auf der Seite „Seitenadministration“ *Freigegebene Seiten verwalten* aus.

Das Teilfenster „Freigegebene Seiten verwalten“ wird angezeigt (siehe vorherige Vorgehensweise).

**2** Wählen Sie in der Liste der freigegebenen Seiten die zu kopierende Seite aus.

---

**Tipp:** Eine lange Liste können Sie *strukturieren* (nach Kategorie oder Textanfang), damit Sie die gewünschte Seite leichter finden.

---

**3** Wählen Sie die Seitenaktion *Kopieren* aus (unten links im Teilfenster).

Es wird eine neue freigegebene Seite mit dem Namen *Kopie von <Name der Originalseite>* erstellt.

**4** Legen Sie die *Seiteneigenschaften* der freigegebenen Seite (wie zuvor beschrieben) fest.

**5** Klicken Sie auf *Seite speichern* (im unteren Bereich des Abschnitts „Seiteneigenschaften“).

### 7.3.2 Inhalt zu einer freigegebenen Seite hinzufügen

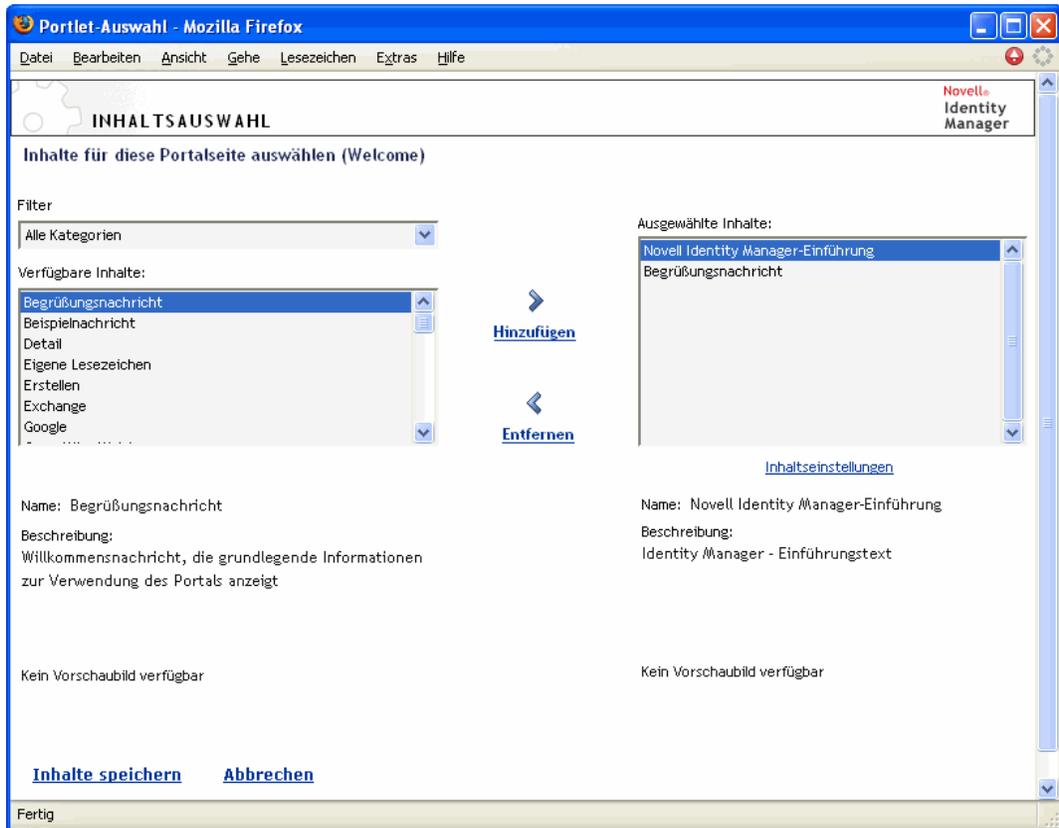
Nach dem Erstellen einer freigegebenen Seite können Sie im nächsten Schritt Inhalt hinzufügen, indem Sie Portlets auswählen und diese auf der Seite platzieren. Sie können vordefinierte Portlets,

die im Lieferumfang der Identity Manager-Benutzeranwendung enthalten sind, oder andere von Ihnen registrierte Portlets verwenden.

So fügen Sie Inhalt zu einer freigegebenen Seite hinzu:

- 1 Öffnen Sie im Teilfenster „Freigegebene Seiten verwalten“ eine neue oder vorhandene Seite und klicken Sie auf die Seitenaufgabe *Inhalt auswählen* (im unteren Bereich des Teilfensters).

Die Seite *Inhaltsauswahl* wird in einem neuen Browserfenster angezeigt:



- 2 Wenn Sie eine bestimmte Kategorie des verfügbaren Inhalts anzeigen möchten, wählen Sie eine Kategorie aus dem Dropdown-Menü *Filter* aus.
- 3 Wählen Sie in der Liste *Verfügbare Inhalte* ein oder mehrere Portlets aus.

---

**Tipp:** Halten Sie die *Strg*-Taste gedrückt, um mehrere nicht direkt untereinander stehende Portlets auszuwählen. Mit der *Umschalttaste* können Sie mehrere direkt untereinander stehende Portlets auswählen.

---

- 4 Wenn Sie auf *Hinzufügen* klicken, werden die ausgewählten Elemente in die Liste *Ausgewählte Inhalte* verschoben.
- 5 Klicken Sie zum Bearbeiten der Einstellungen eines beliebigen Portlets, das Sie für Ihre freigegebene Seite ausgewählt haben, auf *Inhaltseinstellungen*. Die von Ihnen angegebenen Werte der Standardeinstellungen gelten für die Instanz des Portlets, das auf Ihrer Seite angezeigt wird.

**6** Klicken Sie auf *Inhalte speichern*.

Nachdem Sie den Inhalt für Ihre freigegebene Seite festgelegt haben, können Sie (wie in [Abschnitt 7.3.4, „Ändern des Layouts einer freigegebenen Seite“](#), auf Seite 160 beschrieben) ein neues Layout auswählen oder den Inhalt im aktuellen Layout anordnen (wie in [Abschnitt 7.3.5, „Anordnen von Inhalt auf einer freigegebenen Seite“](#), auf Seite 161 beschrieben).

### 7.3.3 Inhalt von einer freigegebenen Seite löschen

Beim Erstellen von freigegebenen Seiten können Sie Inhalte löschen, indem Sie Portlets von einer Seite entfernen. Sie können hierzu die Inhaltsauswahl oder die Layoutauswahl verwenden, wie im Folgenden beschrieben.

So löschen Sie mithilfe der Inhaltsauswahl Inhalte von einer freigegebenen Seite:

- 1** Öffnen Sie eine Seite im Teilfenster „Freigegebene Seiten verwalten“ und klicken Sie auf die Seitenaufgabe *Inhalt auswählen* (im unteren Bereich des Teilfensters).

Die Seite *Inhaltsauswahl* wird in einem neuen Browserfenster angezeigt (wie zuvor dargestellt).

- 2** Wählen Sie ein zu löschendes Portlet in der Liste „Ausgewählte Inhalte“ aus und klicken Sie auf *Entfernen*.

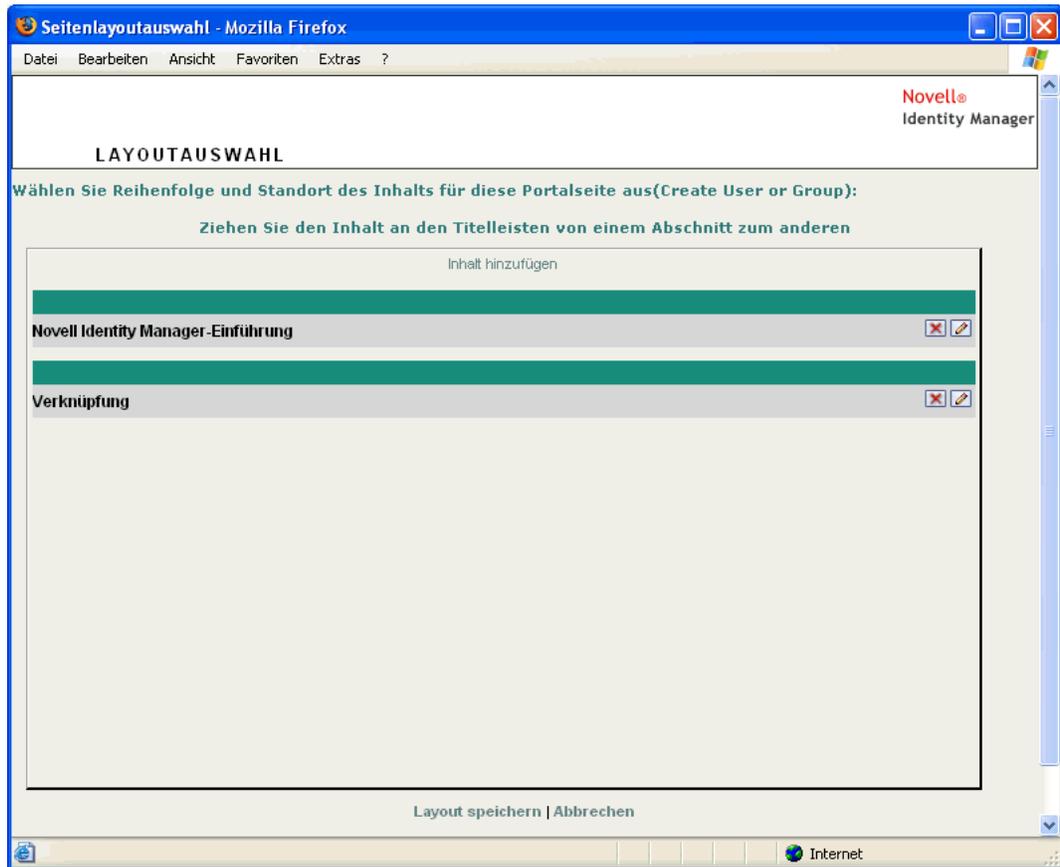
Das Portlet wird von der Seite entfernt.

- 3** Klicken Sie auf *Inhalte speichern*.

So löschen Sie mithilfe der Layoutauswahl Inhalte von einer freigegebenen Seite:

- 1** Öffnen Sie eine Seite im Teilfenster „Freigegebene Seiten verwalten“ und klicken Sie auf die Seitenaufgabe *Inhalt anordnen* (im unteren Bereich des Teilfensters).

Die *Layoutauswahl* wird in einem neuen Browserfenster aufgerufen. Die Seite enthält die folgenden Portlets:



- 2 Wählen Sie ein Portlet aus und klicken Sie zum Entfernen auf *X*.
- 3 Klicken Sie zum Bestätigen des Löschvorgangs auf *OK*.  
Das Portlet wird von der Seite entfernt.
- 4 Klicken Sie auf *Layout speichern*.

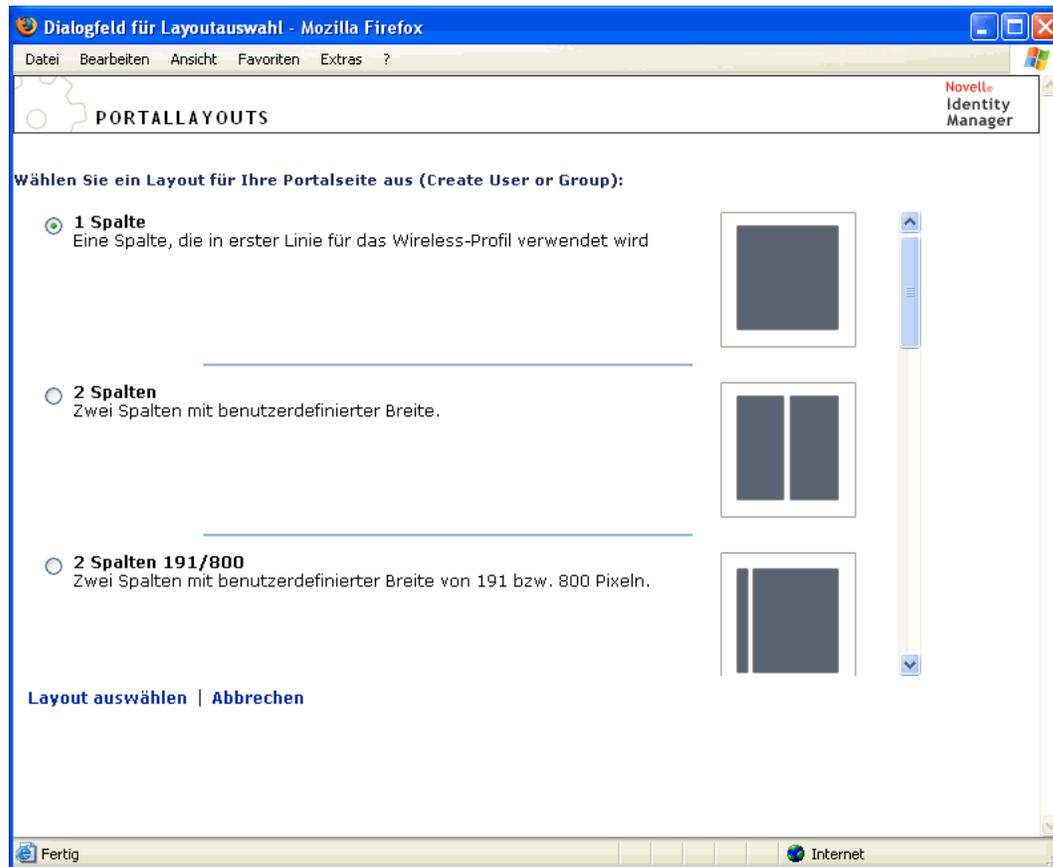
### 7.3.4 Ändern des Layouts einer freigegebenen Seite

Wenn Sie das Layout einer freigegebenen Seite ändern, wird der vorhandene Inhalt in das neue Layout eingefügt. In einigen Fällen muss gegebenenfalls die Anordnung des Inhalts korrigiert werden.

So ändern Sie das Layout einer freigegebenen Seite:

- 1 Öffnen Sie eine Seite im Teilfenster „Freigegebene Seiten verwalten“ und klicken Sie auf die Seitenaufgabe *Layout auswählen* (im unteren Bereich des Teilfensters).

Die Liste *Portallayouts* wird in einem neuen Browserfenster angezeigt:



- 2 Blättern Sie durch die Auswahlmöglichkeiten und wählen Sie das gewünschte Layout aus.
- 3 Klicken Sie auf *Layout auswählen*.

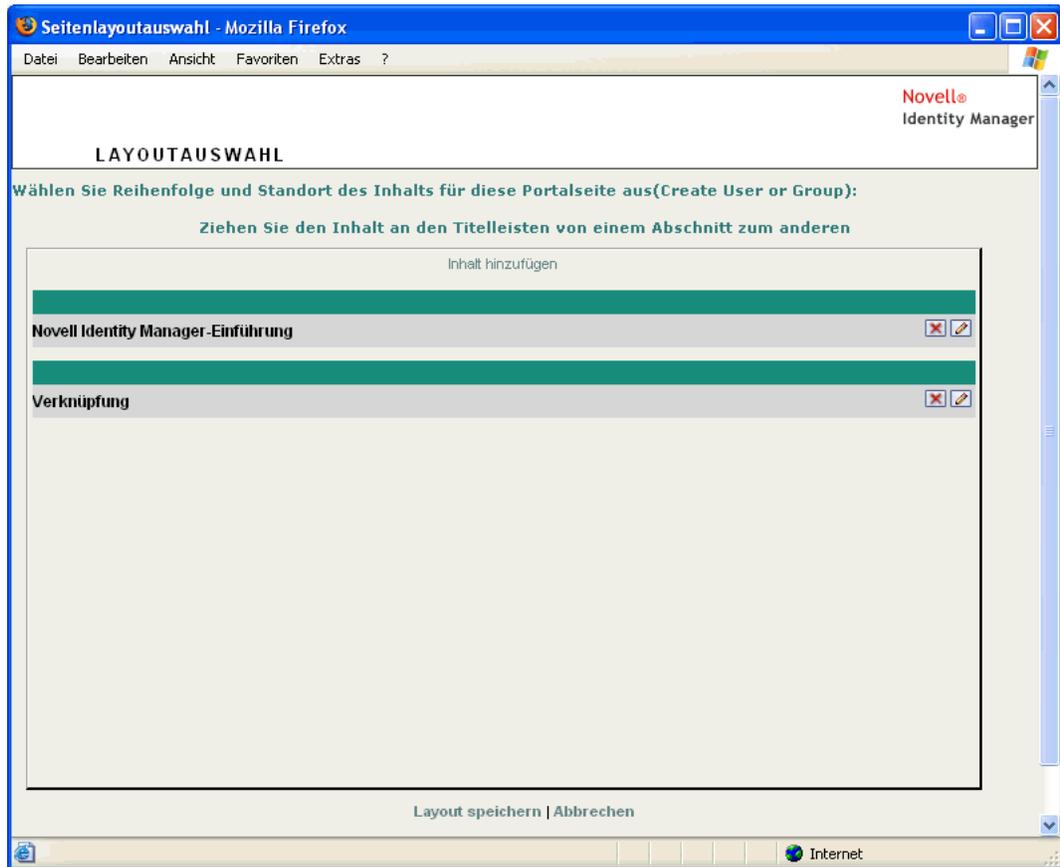
### 7.3.5 Anordnen von Inhalt auf einer freigegebenen Seite

Nachdem Sie den Inhalt und das Layout Ihrer freigegebenen Seite festgelegt haben, können Sie den Inhalt im ausgewählten Layout anordnen, andere Portlets an ausgewählten Stellen hinzufügen oder Portlets löschen.

So ordnen Sie Inhalt auf einer freigegebenen Seite an:

- 1 Öffnen Sie eine Seite im Teilfenster „Freigegebene Seiten verwalten“ und klicken Sie auf die Seitenaufgabe *Inhalt anordnen* (im unteren Bereich des Teilfensters).

Die *Layoutauswahl* wird in einem neuen Browserfenster aufgerufen. Die Seite enthält die folgenden Portlets:



- 2 Führen Sie folgende Schritte aus, um einer Seite *ein Portlet hinzuzufügen*:
  - 2a Klicken Sie im gewünschten Layoutrahmen auf *Inhalt hinzufügen*.

Die Seite *Portlet-Auswahl* wird in einem neuen Browserfenster angezeigt.
  - 2b Wenn Sie eine bestimmte Kategorie des verfügbaren Inhalts anzeigen möchten, wählen Sie eine Kategorie aus dem Dropdown-Menü *Filter* aus.
  - 2c Wählen Sie das gewünschte Portlet in der Liste *Verfügbare Inhalte* aus.
  - 2d Klicken Sie auf *Inhalt auswählen*.

Die Portlet-Auswahl wird geschlossen und das ausgewählte Portlet wird im angegebenen Layoutrahmen in der Layoutauswahl angezeigt.
- 3 Wenn Sie ein Portlet an eine andere Position im Layout *verschieben* möchten, führen Sie diese browserspezifischen Schritte aus:

Browser	Vorgehensweise
Internet Explorer	<ol style="list-style-type: none"> <li>1. Bewegen Sie den Mauszeiger über die Titelleiste des Portlets, bis er die Form einer Hand annimmt.</li> <li>2. Halten Sie die linke Maustaste gedrückt und ziehen Sie das Portlet an die gewünschte Position im Layout.</li> </ol>
Mozilla	<ol style="list-style-type: none"> <li>1. Klicken Sie auf das Portlet, das Sie verschieben möchten.</li> <li>2. Klicken Sie in den Layoutrahmen, in dem es angezeigt werden soll.</li> </ol> <p>Das Portlet wird an das ausgewählte Ziel verschoben.</p>

**4** Führen Sie folgende Schritte aus, um *ein Portlet aus dem Layout zu entfernen*:

**4a** Wählen Sie ein Portlet aus und klicken Sie zum Entfernen auf *X*.

**4b** Klicken Sie zum Bestätigen des Löschvorgangs auf *OK*.

Das Portlet wird aus dem Layout entfernt.

**5** Führen Sie folgende Schritte aus, um die *Einstellungen eines Portlets zu bearbeiten*:

**5a** Wählen Sie ein Portlet aus und klicken Sie zum Bearbeiten auf die *Bleistift*-Schaltfläche.

Die *Inhaltseinstellungen* des Portlets werden in Ihrem Browser angezeigt.

**5b** *Ändern* Sie die Werte der Standardeinstellung nach Bedarf.

Die von Ihnen angegebenen Werte der Standardeinstellungen gelten für die Instanz des Portlets, das auf Ihrer Seite angezeigt wird.

**5c** Klicken Sie auf *Standardeinstellungen speichern*.

**6** Klicken Sie zum Speichern Ihrer Änderungen auf *Layout speichern* und schließen Sie das Fenster „Layoutauswahl“.

### 7.3.6 Anzeigen einer freigegebenen Seite

Sie können Ihre Seite anzeigen, indem Sie in Ihrem Browser zur URL der freigegebenen Seite wechseln.

**So zeigen Sie eine freigegebene Seite an:**

- Rufen Sie in Ihrem *Webbrowser* folgende URL auf:

```
http://server:port/IDM-war-context/portal/pg/name-der-
freigegebenen-Seite
```

Z. B. zum Anzeigen der freigegebenen Seite *MeineFreigegebeneSeite*:

```
http://myappserver:8080/IDM/portal/pg/MeineFreigegebeneSeite
```

## 7.4 Zuweisen von Seitenberechtigungen

Sie können anderen Benutzern, Gruppen und Containern Berechtigungen für das Arbeiten mit bestimmten Containerseiten und freigegebenen Seiten zuweisen. Für Berechtigungen stehen zwei Sicherheitsebenen zur Verfügung:

Berechtigung	Beschreibung	Zuweisung möglich für
<b>Anzeigen</b>	Ermöglicht einem Benutzer, einer Gruppe oder einem Container den Zugriff auf eine Seite. Zusätzlich erscheint die Seite in der Liste mit verfügbaren Seiten.	<b>Containerseiten und freigegebene Seiten</b>
<b>Eigentümerschaft</b>	Ermöglicht einem Benutzer, einer Gruppe oder einem Container, den Inhalt und das Layout einer Seite zu ändern und anderen Benutzern, Gruppen und Containern Anzeige- und Eigentumsberechtigungen zuzuweisen.	<b>Freigegebene Seiten</b>

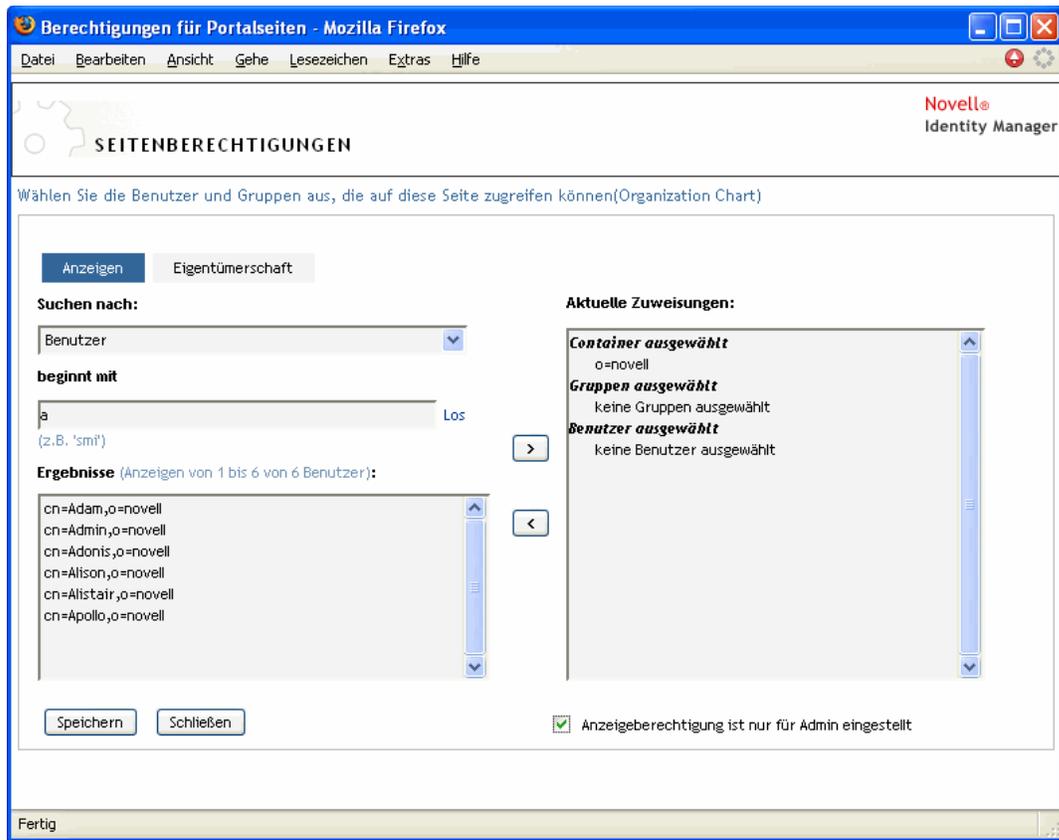
### 7.4.1 Zuweisen der Anzeigeberechtigung

Wenn Sie Benutzern eine Anzeigeberechtigung für eine Containerseite oder eine freigegebene Seite zuweisen, haben diese Zugriff auf die Seite und können sie in einer Liste der verfügbaren Seiten anzeigen.

So weisen Sie Anzeigeberechtigungen für Containerseiten oder freigegebene Seiten zu:

- 1 Öffnen Sie eine Seite im Teilfenster „Containerseiten verwalten“ oder „Freigegebene Seiten verwalten“ und klicken Sie auf die Seitenaufgabe *Berechtigungen zuweisen* (im unteren Bereich des Teilfensters).

Das Dialogfeld *Seitenberechtigungen* wird in einem neuen Browserfenster angezeigt:



2 Wählen Sie die Registerkarte *Anzeigen*.

3 Geben Sie Werte für die folgenden *Sucheinstellungen* an:

Einstellung	Vorgehensweise
Suchen nach	Wählen Sie eine der folgenden Optionen im Dropdown-Menü aus: <ul style="list-style-type: none"> <li>• Benutzer</li> <li>• Gruppen</li> <li>• Container</li> </ul>

Einstellung	Vorgehensweise
Beginnt mit	<p>Um Folgendes zu erzielen:</p> <ul style="list-style-type: none"> <li>• Wenn Sie nach <b>allen</b> verfügbaren Objekten des von Ihnen angegebenen Typs (Benutzer, Gruppe oder Container) suchen möchten, geben Sie in diesem Feld nichts ein.</li> <li>• Wenn Sie nach einer <b>bestimmten Teilmenge</b> dieser Objekte suchen möchten, geben Sie hier den bzw. die Anfangsbuchstaben der gewünschten CN-Werte ein. (Die Groß-/Kleinschreibung wird dabei nicht berücksichtigt. Es werden keine Platzhalter unterstützt.)</li> </ul> <p>Wenn Sie beispielsweise nach Gruppen suchen, die mit <b>s</b> beginnen, erhalten Sie folgendes Ergebnis:</p> <pre>cn=Schulung,ou=Gruppen,o=MeineFirma</pre> <pre>cn=Service,ou=Gruppen,o=MeineFirma</pre> <pre>cn=Sicherheit,ou=Gruppen,o=MeineFirma</pre> <p>Wenn Sie nach Gruppen suchen, die mit <b>se</b> beginnen, erhalten Sie in diesem Fall folgendes Ergebnis:</p> <pre>cn=Service,ou=Gruppen,o=MeineFirma</pre>

**4** Klicken Sie auf *Ausführen*.

Die Ergebnisse Ihrer Suche werden in der Liste *Ergebnisse* angezeigt.

**5** Wählen Sie die Benutzer, Gruppen oder Container aus, die Sie der Seite zuweisen möchten, und klicken Sie anschließend auf die Schaltfläche *Hinzufügen (>)*.

**Tipp:** Halten Sie die *Strg*-Taste gedrückt, wenn Sie mehrere Elemente auswählen möchten.

**6** Aktivieren bzw. deaktivieren Sie die *Sperre* für die Seite wie folgt:

Um Folgendes zu erzielen	Führen Sie diese Schritte aus
Die Seite sperren, damit nur Benutzeranwendungsadministratoren sie anzeigen können	Aktivieren Sie die Option <b>Anzeigeberechtigung ist nur für Admin eingestellt</b> .
Allen zugewiesenen Benutzern, Gruppen und Containern ermöglichen, die Seite anzuzeigen	Deaktivieren Sie die Option <b>Anzeigeberechtigung ist nur für Admin eingestellt</b> .
	<b>Hinweis:</b> Wenn Sie diese Einstellung deaktivieren, jedoch keine Benutzer, Gruppen oder Container ausdrücklich der Seite zugewiesen sind, <b>erhalten alle eine Anzeigeberechtigung</b> für die entsprechende Seite.

**7** Klicken Sie auf *Speichern* und anschließend auf *Schließen*.

## 7.4.2 Zuweisen von Eigentumsrechten für freigegebene Seiten

Benutzer, die über Eigentumsrechte an freigegebenen Seiten verfügen, können den Inhalt sowie die Standardeinstellungen der Portlets auf den betreffenden Seiten ändern.

So weisen Sie die Eigentumsberechtigung für freigegebene Seiten zu:

- 1 Öffnen Sie eine Seite im Teilfenster „Freigegebene Seiten verwalten“ und klicken Sie auf die Seitenaufgabe *Berechtigungen zuweisen* (im unteren Bereich des Teilfensters).

Das Dialogfeld *Seitenberechtigungen* wird in einem neuen Browserfenster angezeigt (wie zuvor dargestellt).

- 2 Wählen Sie die Registerkarte *Eigentümerschaft*.
- 3 Geben Sie Werte für die folgenden *Sucheinstellungen* an:

Einstellung	Vorgehensweise
Suchen nach	Wählen Sie eine der folgenden Optionen im Dropdown-Menü aus: <ul style="list-style-type: none"><li>• Benutzer</li><li>• Gruppen</li><li>• Container</li></ul>
Beginnt mit	Um Folgendes zu erzielen: <ul style="list-style-type: none"><li>• Wenn Sie nach <b>allen</b> verfügbaren Objekten des von Ihnen angegebenen Typs (Benutzer, Gruppe oder Container) suchen möchten, geben Sie in diesem Feld nichts ein.</li><li>• Wenn Sie nach einer <b>bestimmten Teilmenge</b> dieser Objekte suchen möchten, geben Sie hier den bzw. die Anfangsbuchstaben der gewünschten CN-Werte ein. (Die Groß-/Kleinschreibung wird dabei nicht berücksichtigt. Es werden keine Platzhalter unterstützt.)</li></ul> Wenn Sie beispielsweise nach Gruppen suchen, die mit <i>s</i> beginnen, erhalten Sie folgendes Ergebnis:  <pre>cn=Schulung,ou=Gruppen,o=MeineFirma</pre> <pre>cn=Service,ou=Gruppen,o=MeineFirma</pre> <pre>cn=Sicherheit,ou=Gruppen,o=MeineFirma</pre> Wenn Sie nach Gruppen suchen, die mit <i>se</i> beginnen, erhalten Sie in diesem Fall folgendes Ergebnis:  <pre>cn=Service,ou=Gruppen,o=MeineFirma</pre>

- 4 Klicken Sie auf *Ausführen*.

Die Ergebnisse Ihrer Suche werden in der Liste *Ergebnisse* angezeigt.

- 5 Wählen Sie die Benutzer, Gruppen oder Container aus, die Sie der Seite zuweisen möchten, und klicken Sie anschließend auf die Schaltfläche *Hinzufügen* (>).

---

**Tipp:** Halten Sie die *Strg*-Taste gedrückt, wenn Sie mehrere Elemente auswählen möchten.

---

- 6 Aktivieren bzw. deaktivieren Sie die *Sperre* für die Seite wie folgt:

---

Um Folgendes zu erzielen	Führen Sie diese Schritte aus
Die Seite sperren, damit nur Benutzeranwendungsadministratoren mit ihr arbeiten können	Aktivieren Sie die Option <b>Eigentumsberechtigung ist nur für Admin eingestellt</b> .
Allen zugewiesenen Benutzern, Gruppen und Containern ermöglichen, mit der Seite zu arbeiten	Deaktivieren Sie die Option <b>Eigentumsberechtigung ist nur für Admin eingestellt</b> .

---

**Hinweis:** Wenn Sie diese Einstellung deaktivieren, jedoch keine Benutzer, Gruppen oder Container ausdrücklich der Seite zugewiesen sind, **erhalten alle eine Eigentumsberechtigung** für die entsprechende Seite.

---

- 7 Klicken Sie auf *Speichern* und anschließend auf *Schließen*.

### 7.4.3 Zugriffsrechte auf die Seite „Benutzer oder Gruppe erstellen“

Standardmäßig können nur Benutzeranwendungsadministratoren die Seite *Benutzer oder Gruppe erstellen* anzeigen lassen und verwenden. Die Seite ist eine freigegebene Seite der Registerkarte *Identitätsselbstbedienung* der Identity Manager-Benutzeroberfläche. Es ist jedoch möglich, dass ein Benutzeranwendungsadministrator *einem oder mehreren Endbenutzern die Berechtigung* zum Zugriff auf die entsprechende Seite zuweist. Ausgewählte Personen in Administrations- oder Managementpositionen benötigen ggf. selbst die Möglichkeit zum Erstellen von Benutzern, Gruppen oder Aufgabengruppen.

So gewähren Sie Benutzern den Zugriff auf die Seite „Benutzer oder Gruppe erstellen“

- 1 Öffnen Sie im Teilfenster *Freigegebene Seiten verwalten* die Seite *Benutzer oder Gruppe erstellen*.
- 2 Erteilen Sie Benutzern, Gruppen oder Containern über die Seitenaufgabe *Berechtigungen zuweisen* eine *Anzeigeberechtigung* für die freigegebene Seite „Benutzer oder Gruppe erstellen“.
- 3 Wechseln Sie von „Seitenadministration“ zu *Portletadministration* und öffnen Sie die Portlet-Registrierung mit dem Namen *CreatePortlet* (die auf der Seite „Benutzer oder Gruppe erstellen“ verwendet wird).
- 4 Erteilen Sie Benutzern, Gruppen oder Containern über das Teilfenster *Sicherheit Ausführungsberechtigungen und Berechtigungen für Listen* für die Portlet-Registrierung „CreatePortlet“.  
Weitere Informationen zur Erteilung von Berechtigungen für Portlets finden Sie in **Kapitel 9, „Portletadministration“**, auf Seite 181.
- 5 Rufen Sie *iManager* auf und melden Sie sich über ein Administratorkonto *im Baum* Ihres Identitätsdepots an.

- 6** Stellen Sie sicher, dass die Personen, die die Seite „Benutzer oder Gruppe erstellen“ verwenden, über *Erstellungsrechte für die Eigenschaft [Eintragsrechte]* für die Container verfügen, in denen Objekte (Benutzer, Gruppen oder Aufgabengruppe) erstellt werden.

Sie können z. B. die *Trustees eines ausgewählten Containers bearbeiten* und Benutzer, Gruppen oder Container als Trustees hinzufügen. Anschließend können Sie jedem Trustee folgende Rechte zuweisen:

Eigenschaftsname	Zugewiesene Rechte	Vererben
[Alle Attributrechte]	<ul style="list-style-type: none"> <li>• Vergleichen</li> <li>• Lesen</li> <li>• Schreiben</li> </ul>	Ja (aktivieren Sie dieses Kontrollkästchen)
[Eintragsrechte]	<ul style="list-style-type: none"> <li>• Durchsuchen</li> <li>• Erstellen</li> </ul>	Ja (aktivieren Sie dieses Kontrollkästchen)

Wenn Sie im Identitätsdepot nicht die erforderlichen Rechte zuweisen (oder wenn eine Ableitung dieser Rechte nicht möglich ist), erhält ein Endbenutzer bei Verwendung der Seite „Benutzer oder Gruppe erstellen“ möglicherweise eine *Fehlermeldung*. Diese kann wie folgt aussehen:

```
Benutzer 'cn=mmangold,ou=benutzer,ou=idmtest,o=novell' hat keine Berechtigung, 'cn=MeineNeueGruppe,ou=groups,ou=idmsample,o=novell' zu erstellen oder verwandte Objekte zu ändern.
```

Weitere Informationen zur Verwendung der Seite „Benutzer oder Gruppe erstellen“ (von Personen, die auf sie zugreifen können) finden Sie im *Identity Manager-Benutzeranwendung: Benutzerhandbuch*.

## 7.4.4 Zugriffsrechte auf einzelne Administrationsseiten

Standardmäßig haben nur Benutzeranwendungsadministratoren Zugriff auf die Registerkarte *Administration* der Identity Manager-Benutzeroberfläche und die in dieser Registerkarte enthaltenen *Seiten* („Seitenadministration“, „Motive“, „Portletadministration“, „Portal“, „Sicherheit“, „Protokollierung“, „Caching“, „Werkzeuge“). Bei Bedarf kann ein Benutzeranwendungsadministrator aber auch *einem oder mehreren Endbenutzern die Berechtigung zur Anzeige und zur Verwendung von bestimmten Seiten der Registerkarte „Administration“ erteilen*. Ein Beispiel hierfür ist eine Gruppe von Benutzern, die regelmäßig die Motive ändern müssen, obwohl sie keine Benutzeranwendungsadministratoren sind.

So erteilen Sie Benutzern Zugriff auf einzelne Administrationsseiten:

- 1** Öffnen Sie im Teilfenster *Containerseiten verwalten* die *Admin-Containerseite*.  
Diese Containerseite wird angezeigt, wenn Sie die Registerkarte „Administration“ der Identity Manager-Benutzeroberfläche aufrufen.
- 2** Erteilen Sie Benutzern, Gruppen oder Containern über die Seitenaufgabe *Berechtigungen zuweisen* eine *Anzeigeberechtigung* für die Admin-Containerseite.
- 3** Öffnen Sie im Teilfenster *Freigegebene Seiten verwalten* die entsprechende Administrationsseite (eine der freigegebenen Seiten unterhalb der Kategorie *Administration*).

- 4 Erteilen Sie Benutzern, Gruppen oder Containern über die Seitenaufgabe *Berechtigungen zuweisen Anzeige- und Eigentumsberechtigungen* für die freigegebene Seite.
- 5 Stellen Sie sicher, dass die festgelegten Benutzer, Gruppen oder Container über eine *Ausführungsberechtigung für jedes Portlet* verfügen, das auf der angegebenen Seite verwendet wird (sofern es für diese Portlets eingeschränkte Zugriffsrechte gibt).

Weitere Informationen zur Erteilung von Berechtigungen für Portlets finden Sie in **Kapitel 9**, „Portletadministration“, auf Seite 181.

## 7.5 Einrichten von Standardseiten für Gruppen

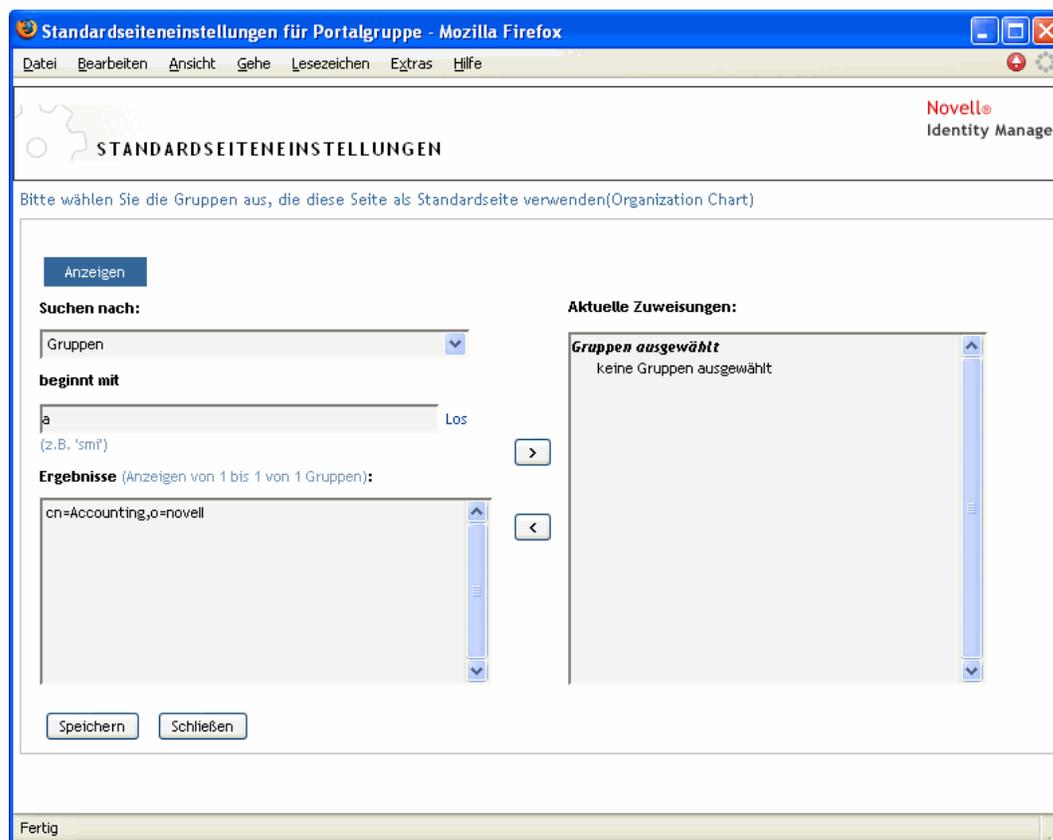
Sie können jeder autorisierten Benutzergruppe eine *Standardcontainerseite* und eine *standardmäßige freigegebene Seite* zuweisen. Diese Einstellungen beeinflussen die Containerseite, die diesen Benutzern bei der Anmeldung angezeigt wird, und die freigegebene Seite, die auf der Containerseite angezeigt wird.

Wenn Benutzer zu mehreren Gruppen mit eigenen Standardseiten gehören, wird anhand der Navigationspriorität bestimmt, welche Containerseite und welche freigegebene Seite angezeigt wird.

So weisen Sie einer Gruppe eine Standardcontainerseite oder eine standardmäßige freigegebene Seite zu:

- 1 Öffnen Sie eine Seite im Teilfenster „Containerseiten verwalten“ oder „Freigegebene Seiten verwalten“ und klicken Sie auf die Seitenaufgabe *Als Standard festlegen* (im unteren Bereich des Teilfensters).

Das Dialogfeld *Standardeinstellungen* wird in einem neuen Browserfenster angezeigt:



2 Geben Sie Werte für die folgenden *Sucheinstellungen* an:

Einstellung	Vorgehensweise
Suchen nach	(Es wird automatisch <b>Gruppen</b> ausgewählt.)

Einstellung	Vorgehensweise
Beginnt mit	<p>Um Folgendes zu erzielen:</p> <ul style="list-style-type: none"> <li>• Wenn Sie <b>alle</b> verfügbaren Gruppen suchen möchten, geben Sie in diesem Feld nichts ein.</li> <li>• Wenn Sie nach einer <b>bestimmten Teilmenge</b> dieser Gruppen suchen möchten, geben Sie hier den bzw. die Anfangsbuchstaben der gewünschten CN-Werte ein. (Die Groß-/Kleinschreibung wird dabei nicht berücksichtigt. Es werden keine Platzhalter unterstützt.)</li> </ul> <p>Wenn Sie beispielsweise nach Gruppen suchen, die mit <code>s</code> beginnen, erhalten Sie folgendes Ergebnis:</p> <pre>cn=Schulung,ou=Gruppen,o=MeineFirma</pre> <pre>cn=Service,ou=Gruppen,o=MeineFirma</pre> <pre>cn=Sicherheit,ou=Gruppen,o=MeineFirma</pre> <p>Wenn Sie nach Gruppen suchen, die mit <code>se</code> beginnen, erhalten Sie in diesem Fall folgendes Ergebnis:</p> <pre>cn=Service,ou=Gruppen,o=MeineFirma</pre>

**3** Klicken Sie auf *Ausführen*.

Die Ergebnisse Ihrer Suche werden in der Liste *Ergebnisse* angezeigt.

**4** Wählen Sie die Gruppen aus, für die diese Seite standardmäßig angezeigt werden soll, und klicken Sie anschließend auf *Hinzufügen* (>).

**Tip:** Halten Sie die *Strg*-Taste gedrückt, wenn Sie mehrere Elemente auswählen möchten.

**5** Klicken Sie auf *Speichern* und anschließend auf *Schließen*.

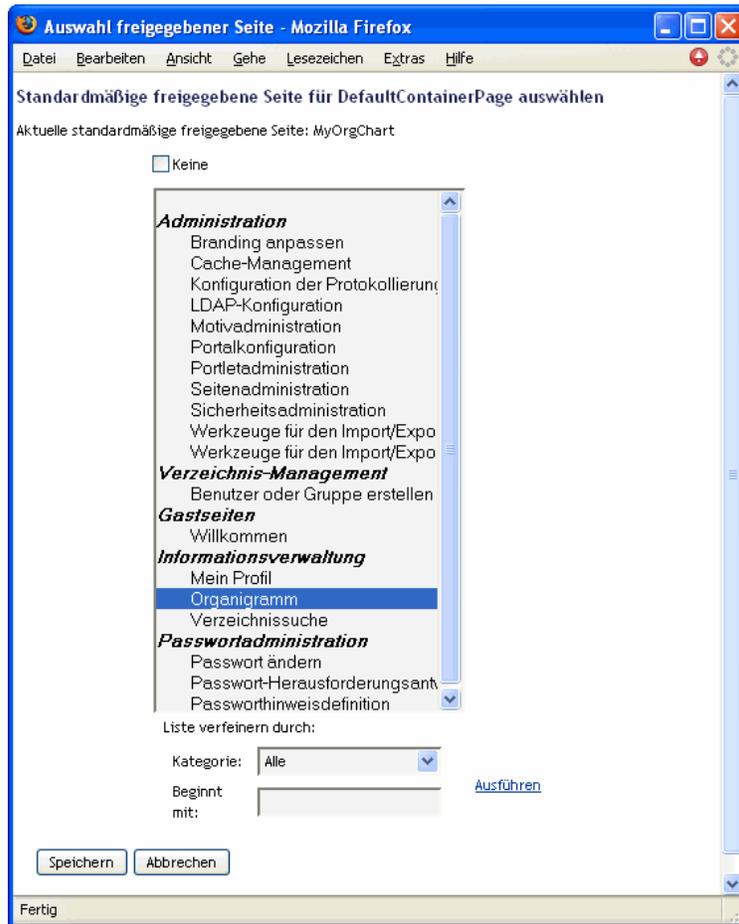
## 7.6 Auswahl einer standardmäßigen freigegebenen Seite für eine Containerseite

Sie können jeder Containerseite eine standardmäßige freigegebene Seite zuweisen. Die Benutzeroberfläche berücksichtigt diese Seitenzuweisung bei der Festlegung, welche Elemente angezeigt werden sollen.

So weisen Sie einer Containerseite eine standardmäßige freigegebene Seite zu:

- 1** Öffnen Sie im Teilfenster *Containerseiten verwalten* eine Containerseite.
- 2** Wählen Sie im Abschnitt „Seiteneigenschaften“ *Standardmäßige freigegebene Seite* aus und klicken Sie auf *Standard auswählen*.

Das Dialogfeld für die Auswahl einer standardmäßigen freigegebenen Seite wird in einem neuen Browserfenster angezeigt:



- 3 Eine lange Liste mit freigegebenen Seiten können Sie *strukturieren* (nach Kategorie oder Textanfang), damit Sie die gewünschte Seite leichter finden.
- 4 *Wählen Sie* eine freigegebene Seite aus, die standardmäßig für die Containerseite angezeigt werden soll (oder aktivieren Sie *Keine*, wenn keine Standardseite ausgewählt werden soll).
- 5 Bestätigen Sie Ihre Auswahl mit *Speichern* und schließen Sie das Dialogfeld.
- 6 Klicken Sie auf *Seite speichern* (im unteren Bereich des Abschnitts „Seiteneigenschaften“).



# Konfiguration von Motiven

# 8

In diesem Kapitel erfahren Sie, wie Sie die Seite *Motive* der Registerkarte *Administration* der Benutzeroberfläche von Identity Manager verwenden. Es werden folgende Themen erläutert:

- [Abschnitt 8.1, „Allgemeines zur Motivkonfiguration“](#), auf Seite 175
- [Abschnitt 8.2, „Vorschau eines Motivs“](#), auf Seite 176
- [Abschnitt 8.3, „Auswahl eines Motivs“](#), auf Seite 177
- [Abschnitt 8.4, „Anpassen des Brandings eines Motivs“](#), auf Seite 178

Allgemeine Informationen zum Zugriff auf die und zum Arbeiten mit der Registerkarte „Administration“ finden Sie in [Kapitel 6, „Verwendung der Registerkarte „Administration““](#), auf Seite 131.

## 8.1 Allgemeines zur Motivkonfiguration

Über die Seite „Motive“ können Sie das Erscheinungsbild der Identity Manager-Benutzeroberfläche steuern.

Ein *Motiv* ist ein Satz visueller Charakteristiken, die für die gesamte Benutzeroberfläche gelten (einschließlich der Gast- und Anmeldungsseiten sowie der Registerkarten „Identitätsselbstbedienung“, „Anforderungen und Genehmigungen“ und „Administration“). Für die Benutzeroberfläche ist jeweils genau ein Motiv gültig. Auf der Seite „Motive“ stehen verschiedene Motive zur Auswahl, falls Sie ein anderes Motiv auswählen möchten.

Die Seite „Motive“ bietet Ihnen außerdem folgende Funktionen:

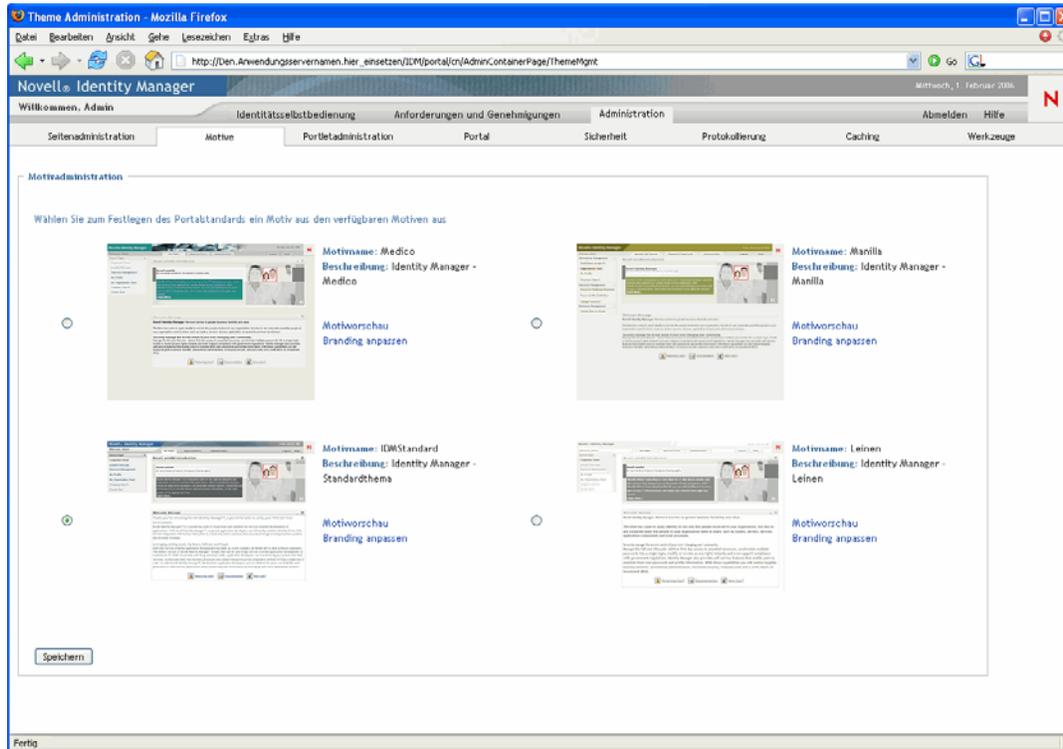
- Sie können sich eine *Vorschau* des ausgewählten Motivs ansehen
- Sie können jedes Motiv an Ihr persönliches Branding (z. B. Logo) *anpassen*.

## 8.2 Vorschau eines Motivs

Vor der Auswahl eines Motivs können Sie in einer Vorschau anzeigen, wie die Darstellung der Identity Manager-Benutzeroberfläche geändert wird.

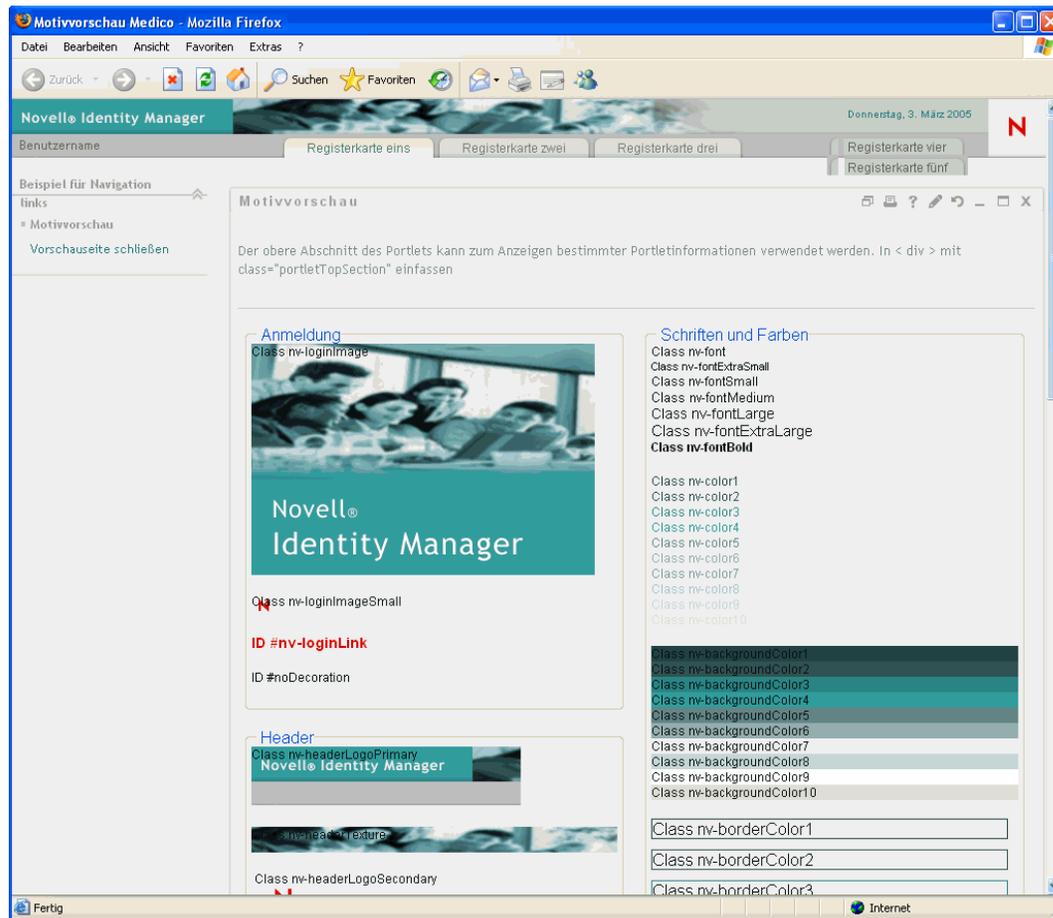
So zeigen Sie die Vorschau eines Motivs an:

- 1 Rufen Sie die Seite *Motive* auf:



- 2 Wählen Sie das gewünschte Motiv aus und klicken Sie dann auf den zugehörigen Link *Motivvorschau*.

Die Vorschau des Motivs wird in einem neuen Browserfenster angezeigt:



- 3 *Blättern* Sie durch die Vorschau und sehen Sie sich die Charakteristika des Motivs an.
- 4 Klicken Sie anschließend auf *Vorschauseite schließen* (in der linken oberen Ecke) oder schließen Sie das Fenster manuell.

## 8.3 Auswahl eines Motivs

Wenn Sie ein Motiv gefunden haben, das Ihren Wünschen entspricht, können Sie es als *aktuelles Motiv* für die Identity Manager-Benutzeroberfläche festlegen.

Sie wählen Sie ein Motiv aus:

- 1 Rufen Sie die Seite *Motive* auf.
- 2 Wählen Sie ein Motiv aus und klicken Sie auf das zugehörige *Optionsfeld*.
- 3 Klicken Sie auf *Speichern*.

Die Benutzeroberfläche übernimmt die Darstellung des ausgewählten Motivs.

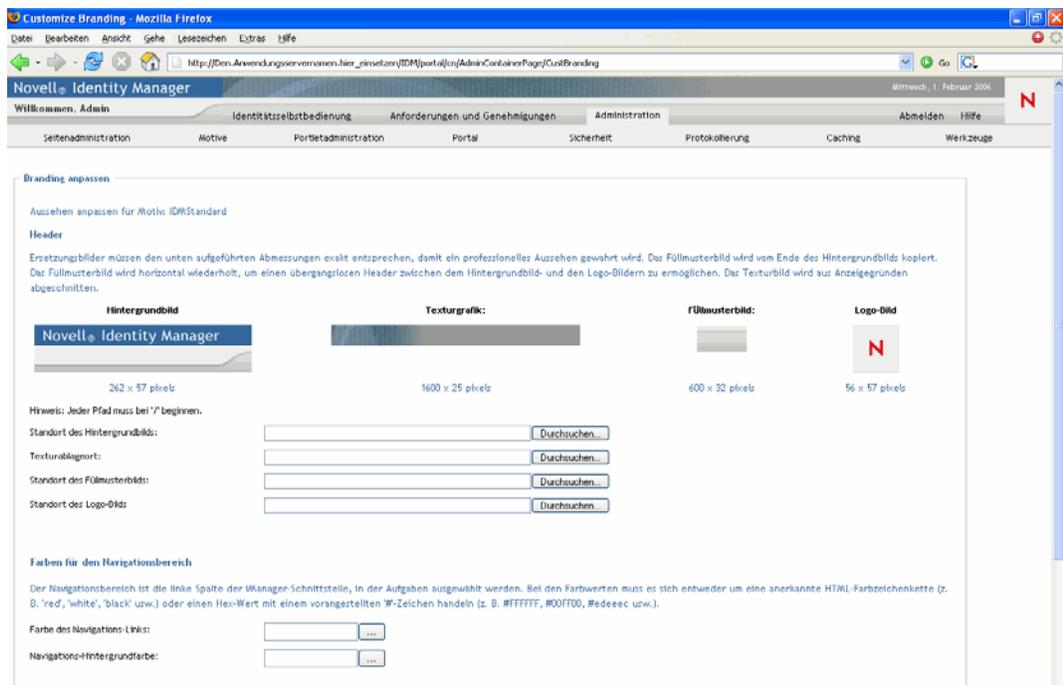
## 8.4 Anpassen des Brandings eines Motivs

Sie können jedes Motiv anpassen, indem Sie Ihre eigenen *Bilder* verwenden und einige *Farbeinstellungen* verändern. Dadurch verleihen Sie der Identity Manager-Benutzeroberfläche ein eigenes Erscheinungsbild, das den Anforderungen Ihres Unternehmens oder Ihrer Organisation hinsichtlich des Brandings entspricht.

So passen Sie das Branding für ein Motiv an:

- 1 Rufen Sie die Seite *Motive* auf.
- 2 Wählen Sie das gewünschte Motiv aus und klicken Sie dann auf den zugehörigen Link *Branding anpassen*.

Es wird die Seite „Motive“ mit den Einstellungen zum Anpassen des Brandings für dieses Motiv angezeigt:





**3** Legen Sie *Ihre Anpassungen* (nach Bedarf) in diesen Einstellungen fest. Dazu gehören:

- Bilder für Kopfzeilen
- Farben für die Navigationsbereiche
- Anmeldebilder

*Befolgen Sie die Bildschirmanweisungen zum Festlegen der einzelnen Einstellungen.*

**4** Klicken Sie auf *Speichern*.

Wenn Sie das aktuelle Motiv bearbeiten, ändert sich das Erscheinungsbild der Benutzeroberfläche entsprechend Ihren Änderungen. (Wenn Sie alle vorgenommenen Änderungen an dem Motiv rückgängig machen möchten, klicken Sie auf die Schaltfläche *Zurücksetzen*.)

---

**Hinweis:** Die Schaltfläche *Motivvorschau* ist verfügbar, während Sie Anpassungen vornehmen, beachten Sie aber, dass über diese Schaltfläche nur die *ursprünglichen Charakteristika* des Motivs angezeigt werden. Ihre Änderungen werden nicht angezeigt.

---

**5** Wenn Sie die Bearbeitung des Motivs beendet haben, klicken Sie auf die Schaltfläche *Zur Motivauswahl zurück*.



In diesem Kapitel erfahren Sie, wie Sie die Seite *Portletadministration* der Registerkarte *Administration* der Benutzeroberfläche von Identity Manager verwenden. Es werden folgende Themen erläutert:

- [Abschnitt 9.1](#), „Allgemeines zur Portletadministration“, auf Seite 181
- [Abschnitt 9.2](#), „Verwaltung von Portlet-Anwendungen“, auf Seite 182
- [Abschnitt 9.3](#), „Verwaltung von Portlet-Definitionen“, auf Seite 185
- [Abschnitt 9.4](#), „Verwaltung registrierter Portlets“, auf Seite 189

Allgemeine Informationen zum Zugriff auf die und zum Arbeiten mit der Registerkarte „Administration“ finden Sie in [Kapitel 6](#), „Verwendung der Registerkarte „Administration““, auf Seite 131.

## 9.1 Allgemeines zur Portletadministration

Sie können die Seite „Portletadministration“ zur Steuerung der über die Benutzeroberfläche von Identity Manager verfügbaren *Portlets* und der zugehörigen Zugriffsrechte verwenden. Portlets sind (auf einem *Java-Standard* basierende) Plugin-Elemente der Benutzeroberfläche, die Inhalte für Seiten der Benutzeroberfläche bieten (einschließlich Containerseiten und freigegebene Seiten).

Beim Verwalten von Portlets stehen folgende Elemente zur Verfügung:

Elemente	Beschreibung
Portlet-Anwendungen	<p>Java Portlet 1.0-konforme WAR-Dateien, die den Portlet-Implementationsdeskriptor „portlet.xml“ und (optional) weitere Portlet-Laufzeitkomponenten enthalten.</p> <p>Weitere Informationen hierzu finden Sie in <a href="#">Abschnitt 9.2</a>, „Verwaltung von Portlet-Anwendungen“, auf Seite 182.</p>
Portlet-Definitionen	<p>Deskriptoren (werden aus portlet.xml ausgelesen), die die Portlet-Konfigurationsparameter festlegen. Für jedes Portlet einer Anwendung gibt es genau eine Definition.</p> <p>Weitere Informationen hierzu finden Sie in <a href="#">Abschnitt 9.3</a>, „Verwaltung von Portlet-Definitionen“, auf Seite 185.</p>
Portlet-Registrierungen	<p>Registrierungen von Portlets, basierend auf deren Definitionen. Eine Portlet-Anwendung kann mehrere Registrierungen für dasselbe Portlet enthalten.</p> <p>Weitere Informationen hierzu finden Sie in <a href="#">Abschnitt 9.4</a>, „Verwaltung registrierter Portlets“, auf Seite 189.</p>

Details zu den mit der Identity Manager-Benutzeroberfläche ausgelieferten Portlets finden Sie in [Teil IV](#), „Portlet-Referenz“, auf Seite 237. Informationen zur Verwendung von Portlets auf Containerseiten und freigegebenen Seiten finden Sie in [Kapitel 7](#), „Seitenadministration“, auf Seite 137.

## 9.2 Verwaltung von Portlet-Anwendungen

Bei der Installation der Identity Manager-Benutzeranwendung wird die Datei *IDM.war* auf Ihrem Anwendungsserver installiert und automatisch als Portlet-Anwendung registriert. Die Datei „IDM.war“ (die ggf. bei der Installation umbenannt werden kann) enthält alle Portlets, die bei der Standardkonfiguration der Identity Manager-Benutzeroberfläche verwendet werden. Darüber hinaus enthält sie einige zusätzliche Portlets, die nicht im Rahmen der Standardkonfiguration verwendet werden. (Die Portlets in der Datei „IDM.war“ werden in [Teil IV, „Portlet-Referenz“, auf Seite 237](#) beschrieben.)

Sie müssen sich allerdings nicht auf die Verwendung von Portlets aus der Datei „IDM.war“ beschränken. Sie können beliebige weitere *Standard-Portlet-Anwendungen* (Java Portlet 1.0-konforme WAR-Dateien) auf Ihrem Anwendungsserver installieren und mit diesen Portlet-Anwendungen und deren Portlets über die Identity Manager-Benutzeroberfläche arbeiten. So werden diese Portlet-Anwendungen beispielsweise zusammen mit der Datei „IDM.war“ auf der Seite „Portletadministration“ angezeigt.

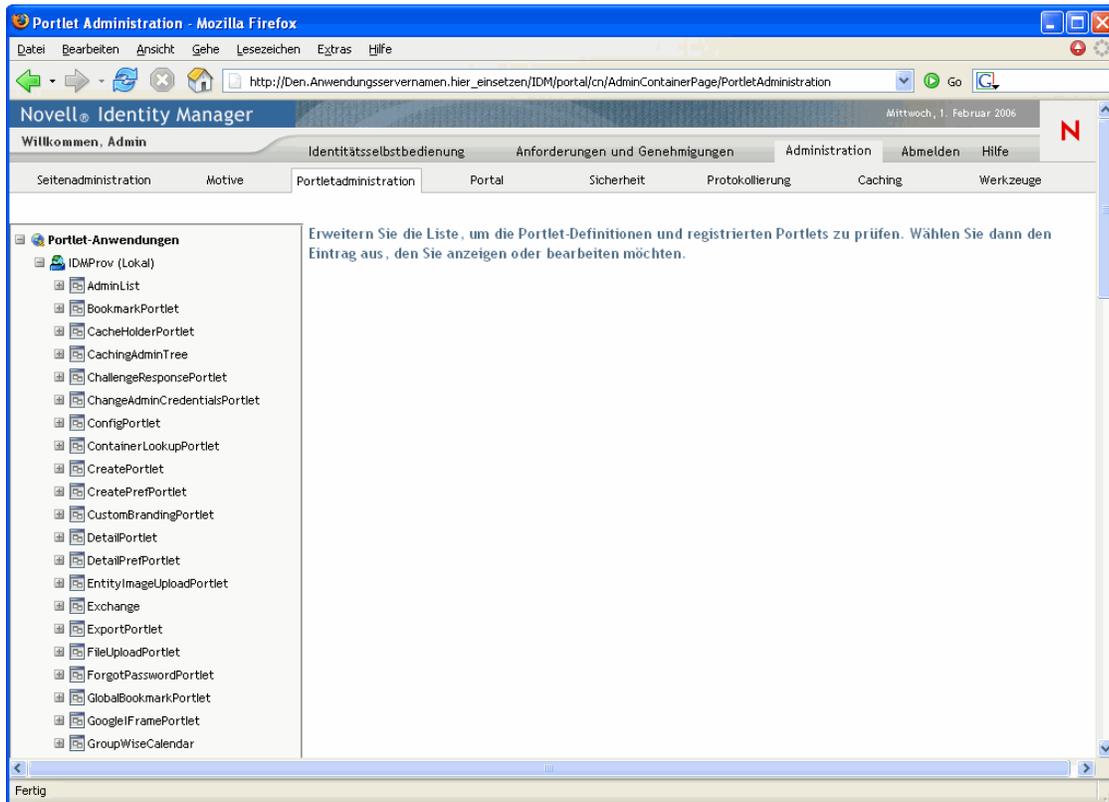
Auf der Seite „Portletadministration“ können Sie *die Datei „IDM.war“ und andere Portlet-Anwendungen verwalten*. Hierbei haben Sie folgende Möglichkeiten:

- [Abschnitt 9.2.1, „Zugriff auf Portlet-Anwendungen auf dem Server“, auf Seite 182](#)
- [Abschnitt 9.2.2, „Anzeigen von Informationen zu Portlet-Anwendungen“, auf Seite 183](#)
- [Abschnitt 9.2.3, „Aufheben der Registrierung von Portlet-Anwendungen“, auf Seite 184](#)

### 9.2.1 Zugriff auf Portlet-Anwendungen auf dem Server

Wenn Sie zur Seite „Portletadministration“ wechseln, wird automatisch *eine Liste der Portlet-Anwendungen angezeigt* („IDM.war“ und ggf. weitere Portlet-Anwendungen), die auf Ihrem Anwendungsserver installiert sind. Diese Liste wird auf der linken Seite als Baumstruktur angezeigt,

die Sie erweitern und in der Sie navigieren können, um ein ausgewähltes Portlet und dessen Inhalt zu verwalten:



## 9.2.2 Anzeigen von Informationen zu Portlet-Anwendungen

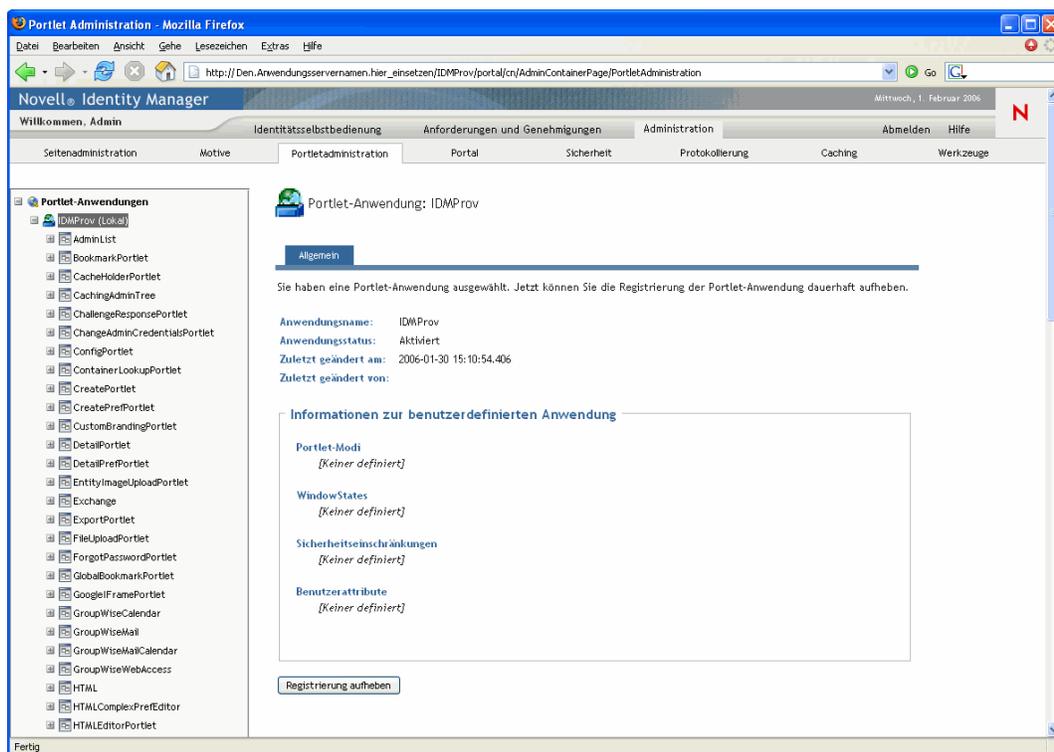
Sie können die folgenden schreibgeschützten Informationen zu einer aufgeführten Portlet-Anwendung anzeigen:

- Name
- Status (aktiviert oder deaktiviert)
- Datum der letzten Änderung
- Benutzer, der die letzte Änderung vorgenommen hat
- Informationen zur benutzerdefinierten Anwendung (soweit vorhanden): Portlet-Modi, Fensterzustände, Sicherheitseinschränkungen und Benutzerattribute

**So zeigen Sie Informationen zu einer Portlet-Anwendung an:**

- *Wählen Sie* in der Liste „Portlet-Anwendungen“ die Portlet-Anwendung aus, über die Sie mehr erfahren möchten.

Auf der rechten Seite wird das Teilfenster *Allgemein* mit Informationen zur ausgewählten Portlet-Anwendung angezeigt:



### 9.2.3 Aufheben der Registrierung von Portlet-Anwendungen

Wenn Sie eine Portlet-Anwendung von Ihrem Anwendungsserver entfernen möchten, müssen Sie vor der Deinstallation deren *Registrierung aufheben*. Anderenfalls wird die Portlet-Anwendung beim Neustart des Servers automatisch erneut installiert.

Wenn Sie die Registrierung einer Portlet-Anwendung aufheben, werden alle zugehörigen Standardeinstellungen und Einstellungen aus der Datenbank mit Ihren Anwendungsdaten entfernt.

---

**Hinweis:** Es ist nicht möglich, die Registrierung für den *lokalen* Portlet-Container aufzuheben, bei dem es sich um eine lokale Portlet-Anwendung des Portals handelt. Der lokale Portlet-Container verwaltet Portlets, die im Portal enthalten sind (Identity Manager-Benutzeranwendung).

---

So heben Sie die Registrierung einer Portlet-Anwendung auf:

- 1 Wählen Sie in der Liste „Portlet-Anwendungen“ die Portlet-Anwendung aus, deren Registrierung Sie aufheben möchten.

Auf der rechten Seite wird das Teilfenster *Allgemein* angezeigt (siehe vorherige Vorgehensweise).

- 2 Klicken Sie auf *Registrierung aufheben*.

Es wird ein Bestätigungsfenster angezeigt.

- 3 Bestätigen Sie die Aktion, indem Sie auf *OK* klicken.

Nach Beendigung des Vorgangs ist die Portlet-Anwendung, deren Registrierung aufgehoben wurde, nicht mehr in der Liste „Portlet-Anwendungen“ vorhanden.

- 4 Um die Portlet-Anwendung vom Anwendungsserver zu entfernen, verwenden Sie die Werkzeuge Ihres Servers zur *Deinstallation des Archivs*, das die Portlet-Anwendung enthält.

---

**Hinweis:** Zur erneuten Registrierung einer Portlet-Anwendung, deren Registrierung aufgehoben wurde, müssen Sie sie *erneut bereitstellen*.

---

## 9.3 Verwaltung von Portlet-Definitionen

Die Seite „Portletadministration“ ermöglicht es Ihnen, die folgenden Aktionen im Zusammenhang mit *Portlet-Definitionen* in einer Portlet-Anwendung auszuführen:

- [Abschnitt 9.3.1, „Zugriff auf Portlet-Definitionen in der bereitgestellten Portlet-Anwendung“, auf Seite 185](#)
- [Abschnitt 9.3.2, „Registrierung von Portlet-Definitionen“, auf Seite 186](#)
- [Abschnitt 9.3.3, „Anzeigen von Informationen zu Portlet-Definitionen“, auf Seite 187](#)

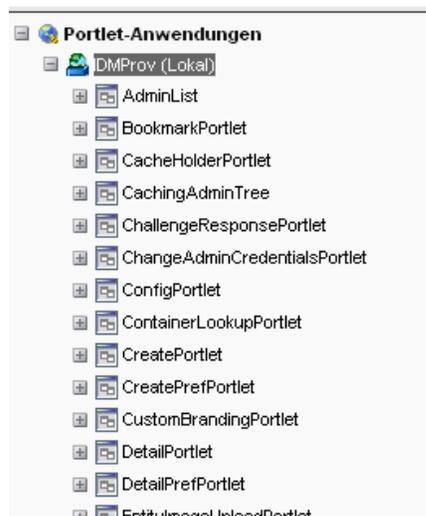
### 9.3.1 Zugriff auf Portlet-Definitionen in der bereitgestellten Portlet-Anwendung

In der Liste „Portlet-Anwendungen“ werden die Portlet-Definitionen in einer ausgewählten Portlet-Anwendung angezeigt.

**So greifen Sie auf die Portlet-Definitionen in der bereitgestellten Portlet-Anwendung zu:**

- *Erweitern Sie* in der Liste „Portlet-Anwendungen“ die Portlet-Anwendung, auf deren Portlet-Definitionen Sie zugreifen möchten.

In der Baumstruktur werden alle Portlet-Definitionen unterhalb dieser Portlet-Anwendung angezeigt:



## 9.3.2 Registrierung von Portlet-Definitionen

Bevor Sie ein Portlet verwenden können, müssen Sie die zugehörige Portlet-Definition beim Portal (Identity Manager-Benutzeranwendung) registrieren. Eine registrierte Portlet-Definition wird als *Portlet-Registrierung* bezeichnet. Sie können pro Portlet mehrere Registrierungen erstellen, wodurch Sie mehrere Instanzen desselben Portlets auf derselben Seite einsetzen können.

Die Portlet-Registrierung übernimmt alle *Standardeinstellungen und Einstellungen* der Portlet-Klasse. Sie können die entsprechenden Werte jedoch wie folgt ändern:

- *Beim Registrieren* der Portlet-Definition - siehe [Abschnitt 9.4, „Verwaltung registrierter Portlets“](#), auf Seite 189
- *Beim Hinzufügen einer Instanz* des Portlets zu einer Seite - siehe [Kapitel 7, „Seitenadministration“](#), auf Seite 137

Alle mit der Identity Manager-Benutzeranwendung ausgelieferten Portlets *werden automatisch registriert*.

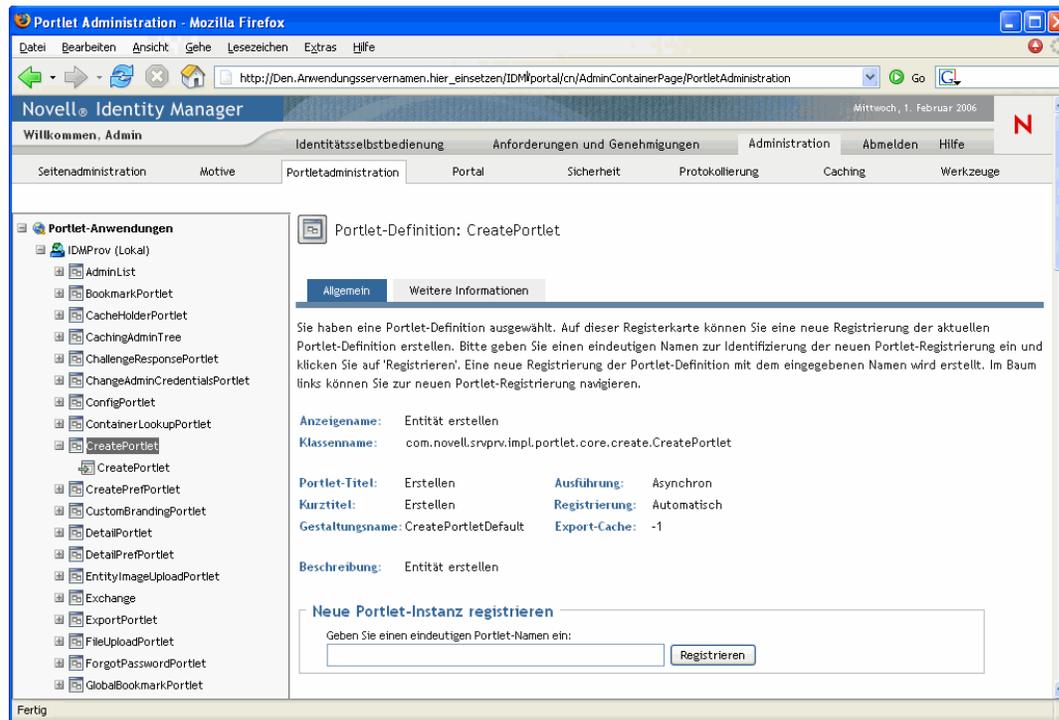
**Bearbeitungsmodus** Wenn die Portlet-Definition über einen Bearbeitungsmodus verfügt, kann der Endbenutzer zur Laufzeit gemäß der Logik der Methode „doEdit()“ des Portlets spezifische Standardeinstellungen der Portlet-Registrierung ändern.

Die Identity Manager-Benutzeranwendung bietet zudem eine Standardimplementierung für den Bearbeitungsmodus. Wenn die Methode „doEdit()“ nicht ausdrücklich implementiert ist, wird ein vorgegebenes Standardeinstellungsblatt angezeigt.

So registrieren Sie eine Portlet-Definition:

- 1 *Wählen Sie* in der Liste „Portlet-Anwendungen“ die Portlet-Definition aus, für die Sie eine Portlet-Registrierung erstellen möchten.

Auf der rechten Seite wird das Teilfenster *Allgemein* angezeigt:



Alle *vorhandenen Registrierungen* des ausgewählten Portlets sind in der Baumstruktur unter „Portlet-Anwendungen“ (links) unterhalb des Namens der jeweiligen Portlet-Definition aufgeführt.

- 2 Geben Sie im Textfeld *Neue Portlet-Instanz registrieren* einen eindeutigen Namen für die Portlet-Registrierung ein und klicken Sie anschließend auf *Registrieren*.

Die neue Portlet-Registrierung wird erstellt und in der Baumstruktur unter „Portlet-Anwendungen“ aufgeführt.

- 3 Informationen zum Ändern der Standardeinstellungen und Einstellungen der neuen Portlet-Registrierung finden Sie in [Abschnitt 9.4, „Verwaltung registrierter Portlets“](#), auf Seite 189.

### 9.3.3 Anzeigen von Informationen zu Portlet-Definitionen

Sie können die folgenden schreibgeschützten Informationen zu einer aufgeführten Portlet-Definition anzeigen:

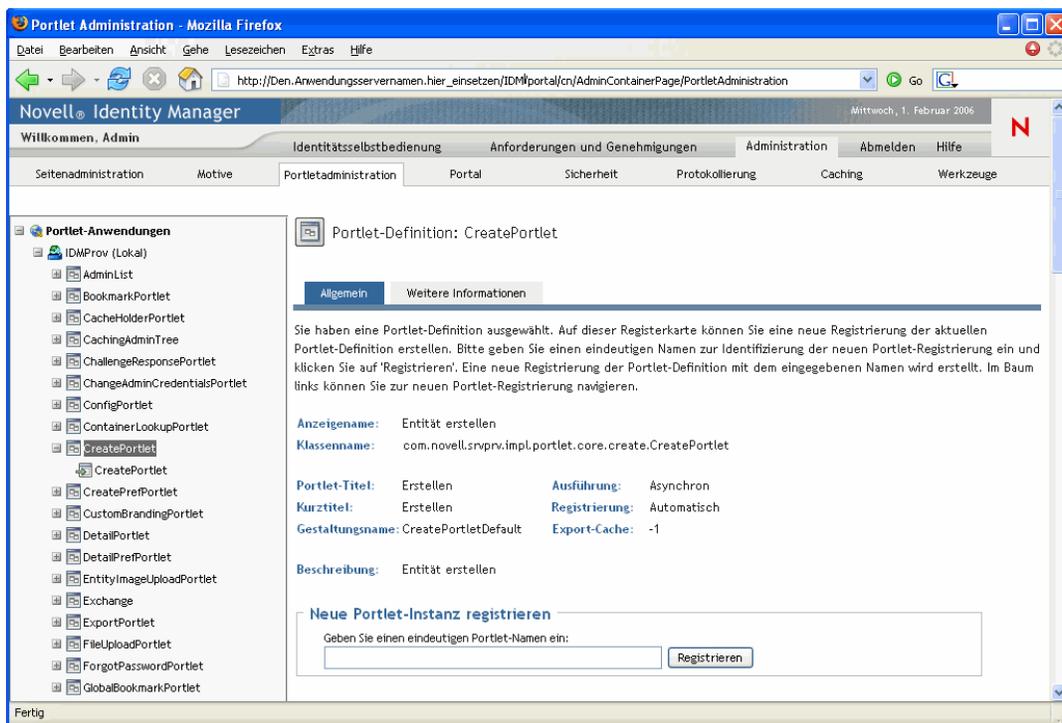
- Anzeigename
- Klassenname
- Portlet-Titel
- Art der Ausführung (synchron oder asynchron)
- Kurztitel
- Art der Registrierung
- Gestaltungsname

- Cache-Ablaufzeit
- Beschreibung
- Initialisierungsparameter
- Schlüsselwörter
- Unterstützte Mime-Typen
- Vom Portlet unterstützte Modi
- Unterstützte Gebietsschemata
- Unterstützte Geräte
- Sicherheitsfunktionen

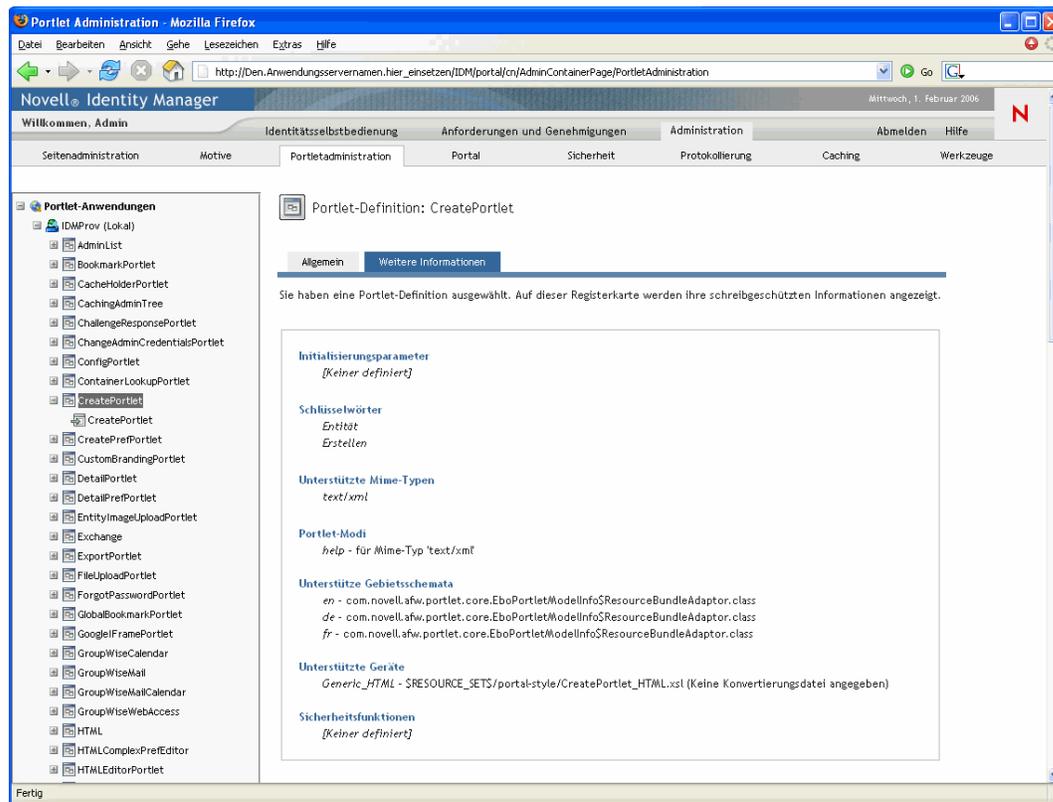
So zeigen Sie Informationen zu Portlet-Definitionen an:

- 1 Wählen Sie in der Liste „Portlet-Anwendungen“ die Portlet-Definition aus, über die Sie mehr erfahren möchten.

Auf der rechten Seite wird das Teilfenster *Allgemein* mit Informationen zur ausgewählten Portlet-Definition angezeigt:



- 2 Wechseln Sie zum Teilfenster *Weitere Informationen*, um weitere Details zur ausgewählten Portlet-Definition zu erhalten:



## 9.4 Verwaltung registrierter Portlets

Die Seite „Portletadministration“ ermöglicht es Ihnen, die folgenden Aufgaben im Zusammenhang mit *Portlet-Registrierungen* in einer Portlet-Anwendung auszuführen:

- Abschnitt 9.4.1, „Zugriff auf Portlet-Registrierungen in der installierten Portlet-Anwendung“, auf Seite 190
- Abschnitt 9.4.2, „Anzeigen von Informationen zu Portlet-Registrierungen“, auf Seite 191
- Abschnitt 9.4.3, „Zuweisen von Kategorien zu Portlet-Registrierungen“, auf Seite 191
- Abschnitt 9.4.4, „Ändern von Einstellungen für Portlet-Registrierungen“, auf Seite 193
- Abschnitt 9.4.5, „Ändern von Standardeinstellungen für Portlet-Registrierungen“, auf Seite 195
- Abschnitt 9.4.6, „Zuweisen von Sicherheitsberechtigungen zu Portlet-Registrierungen“, auf Seite 196
- Abschnitt 9.4.7, „Aufheben der Registrierung von Portlets“, auf Seite 199

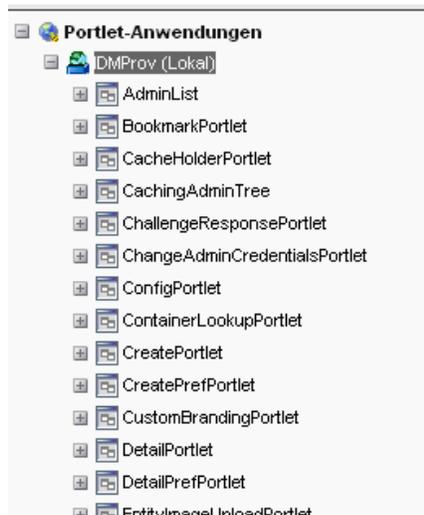
## 9.4.1 Zugriff auf Portlet-Registrierungen in der installierten Portlet-Anwendung

In der Liste „Portlet-Anwendungen“ werden die Portlet-Registrierungen für jede Portlet-Definition in einer ausgewählten Portlet-Anwendung angezeigt.

So greifen Sie auf die Portlet-Registrierungen in der installierten Portlet-Anwendung zu:

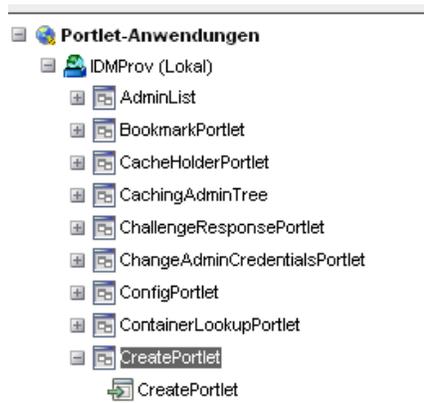
- 1 *Erweitern Sie in der Liste „Portlet-Anwendungen“ die Portlet-Anwendung, auf deren Portlet-Definitionen und -Registrierungen Sie zugreifen möchten.*

In der Baumstruktur werden alle Portlet-Definitionen unterhalb dieser Portlet-Anwendung angezeigt:



- 2 *Erweitern Sie die Portlet-Definition, auf deren Portlet-Registrierungen Sie zugreifen möchten.*

In der Baumstruktur werden alle Portlet-Registrierungen unterhalb dieser Portlet-Definition angezeigt:



## 9.4.2 Anzeigen von Informationen zu Portlet-Registrierungen

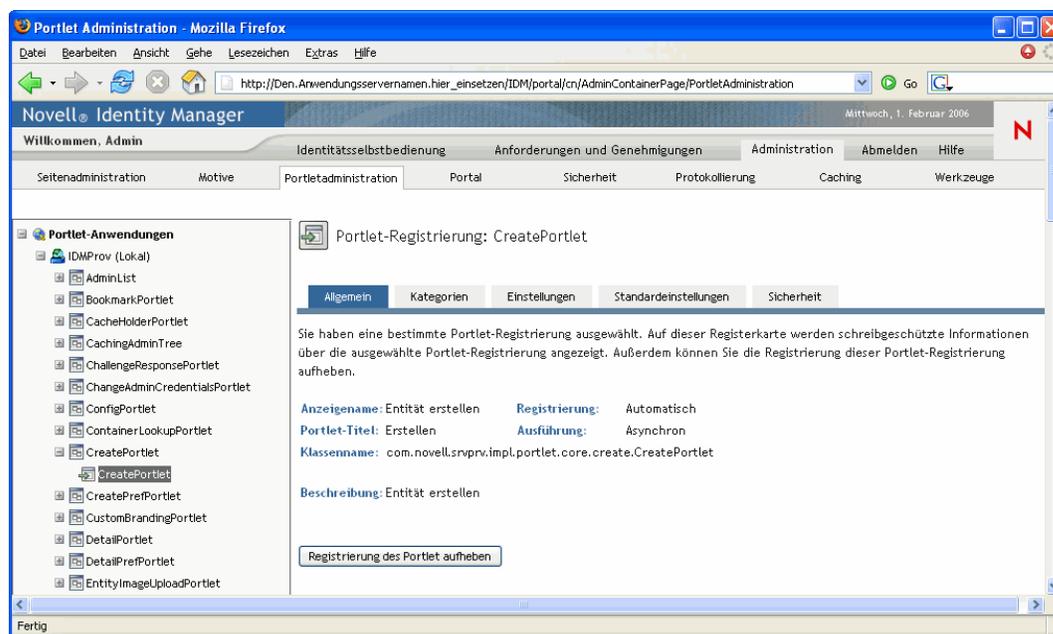
Sie können die folgenden schreibgeschützten Informationen zu einer aufgeführten Portlet-Registrierung anzeigen:

- Anzeigename
- Art der Registrierung
- Portlet-Titel
- Art der Ausführung (synchron oder asynchron)
- Klassenname
- Beschreibung

**So zeigen Sie Informationen einer Portlet-Registrierung an:**

- *Wählen Sie* in der Liste „Portlet-Anwendungen“ die Portlet-Registrierung aus, über die Sie mehr erfahren möchten.

Auf der rechten Seite wird das Teilfenster *Allgemein* mit Informationen zur ausgewählten Portlet-Registrierung angezeigt:



## 9.4.3 Zuweisen von Kategorien zu Portlet-Registrierungen

Um die Suche nach bestimmten Portlets in einer Portlet-Anwendung zu erleichtern, können Sie Portlet-Registrierungen in Kategorien organisieren.

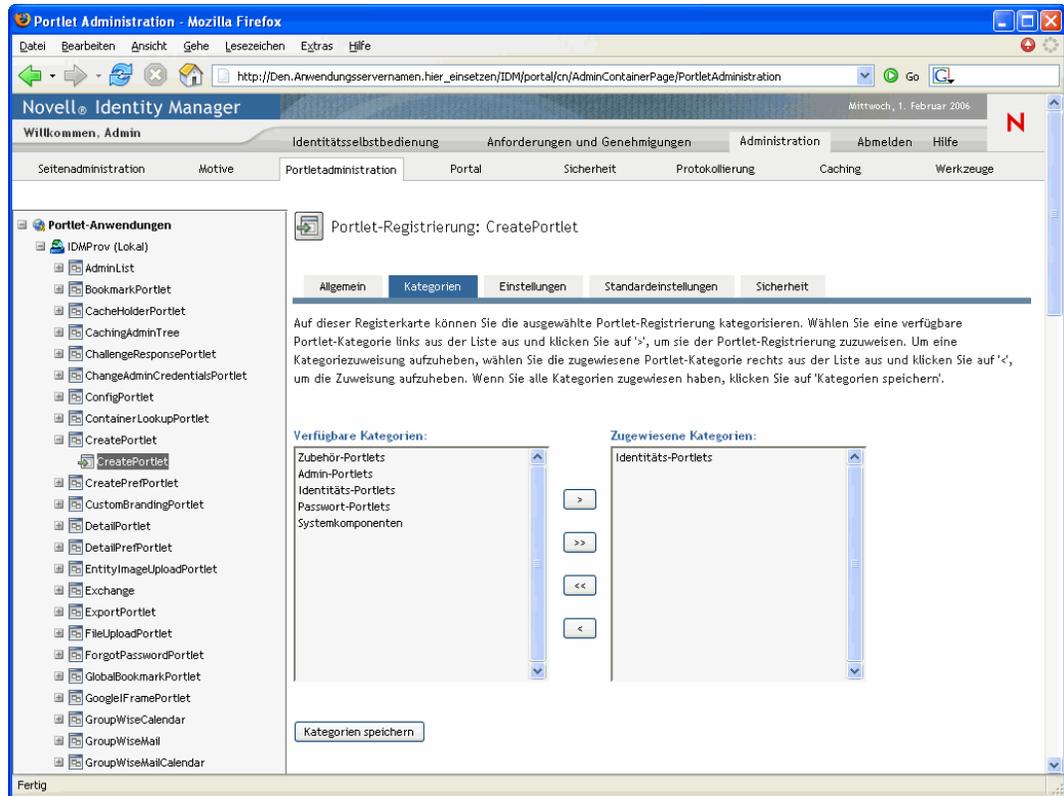
So weisen Sie Portlet-Registrierungen Kategorien zu:

- 1 *Wählen Sie* in der Liste „Portlet-Anwendungen“ die Portlet-Registrierung aus, der Sie eine Kategorie zuweisen möchten.

Auf der rechten Seite wird das Teilfenster *Allgemein* angezeigt.

**2** Wechseln Sie zum Teilfenster *Kategorien*.

In diesem Teilfenster werden die verfügbaren und zugewiesenen Kategorien für die ausgewählte Portlet-Registrierung angezeigt:



**3** Aktualisieren Sie bei Bedarf die Liste *Zugewiesene Kategorien*:

Um Folgendes zu erzielen	Führen Sie diese Schritte aus
Der Portlet-Registrierung eine oder mehrere Kategorien zuweisen	Wählen Sie jede zuzuweisende Kategorie aus und klicken Sie auf >
Der Portlet-Registrierung alle Kategorien zuweisen	Klicken Sie auf >>
Zuweisung einer oder mehrerer Kategorien aufheben	Wählen Sie jede zu entfernende Kategorie aus und klicken Sie auf <
Zuweisung aller Kategorien aufheben	Klicken Sie auf <<

**4** Klicken Sie auf *Kategorien speichern*.

## 9.4.4 Ändern von Einstellungen für Portlet-Registrierungen

Portlet-Einstellungen legen fest, wie das Portal (Identity Manager-Benutzeranwendung) mit den einzelnen Portlets interagiert. Jedes einzelne Portlet wird mit den folgenden Einstellungen konfiguriert:

- Titel
- Maximale Zeitüberschreitung
- Authentifizierung erforderlich
- Titelleiste anzeigen
- Für den Benutzer nicht sichtbar
- In der Portlet-Anwendung definierte Optionen

Die standardmäßigen Java Portlet 1.0-Einstellungen sind im Portlet-Implementierungsdeskriptor (portlet.xml) der WAR-Datei der Portlet-Anwendung definiert. Sie können die Werte dieser Einstellungen über die Seite „Portletadministration“ für jede einzelne Registrierung ändern. In diesem Fall werden die neuen Werte nur für die ausgewählte Portlet-Registrierung wirksam.

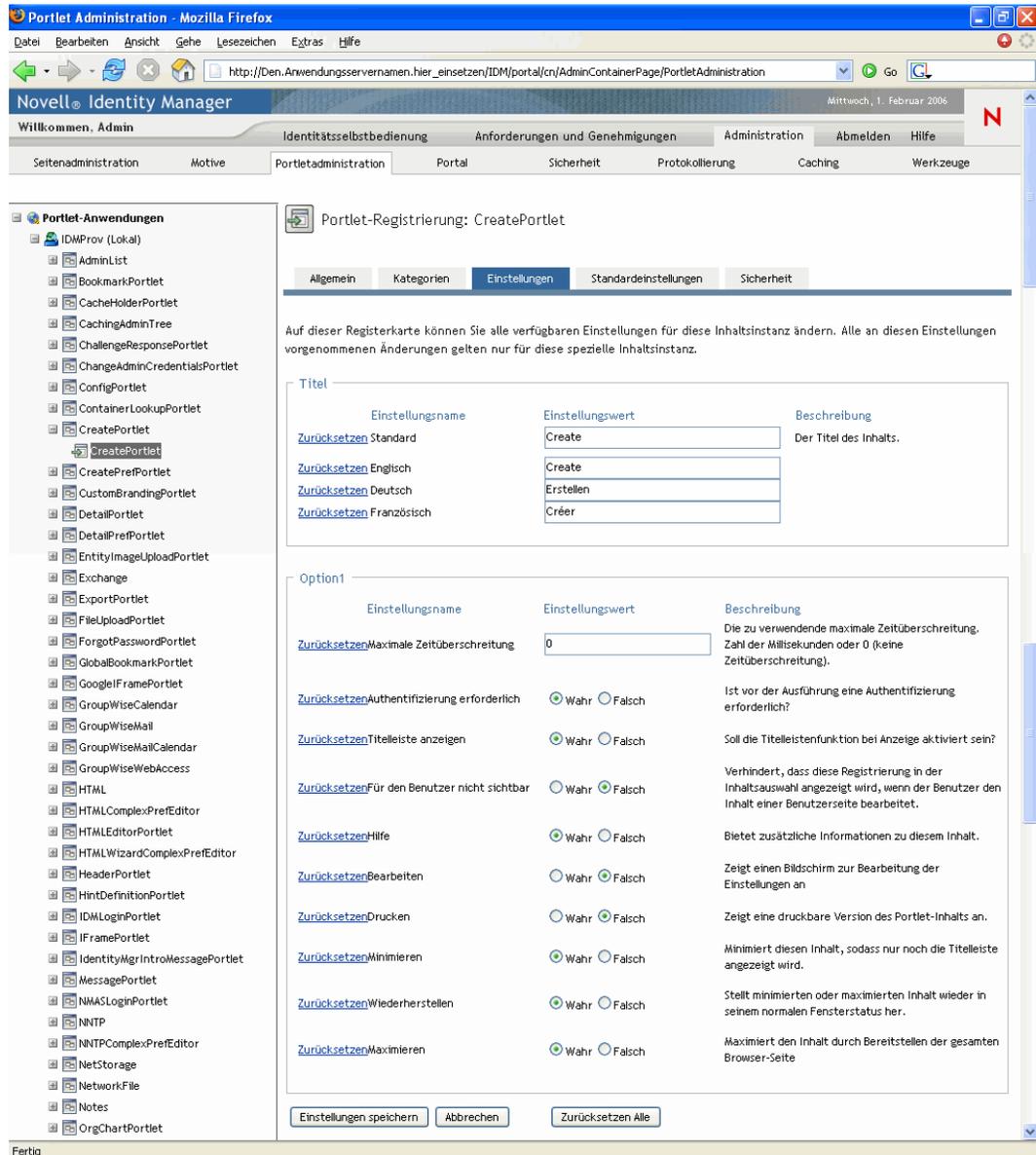
So ändern Sie Portlet-Registrierungseinstellungen:

- 1** Wählen Sie in der Liste „Portlet-Anwendungen“ die Portlet-Registrierung aus, deren Einstellungen Sie ändern möchten.

Auf der rechten Seite wird das Teilfenster *Allgemein* angezeigt.

- 2** Wechseln Sie zum Teilfenster *Einstellungen*.

In diesem Teilfenster werden die aktuellen Einstellungen für die ausgewählte Portlet-Registrierung angezeigt:



### 3 Nehmen Sie die gewünschten *Änderungen* an den Einstellungen vor.

Beim Arbeiten mit diesem Teilfenster können Sie zudem die folgenden Aktionen ausführen:

#### Um Folgendes zu erzielen

#### Führen Sie diese Schritte aus

Ungespeicherte Änderungen verwerfen

Klicken Sie auf **Abbrechen**

Alle Einstellungen für die ausgewählte Portlet-Registrierung auf ihre Standardwerte zurücksetzen (wie in der zugehörigen Portlet-Definition festgelegt)

Klicken Sie auf **Alle zurücksetzen**

---

Um Folgendes zu erzielen

Führen Sie diese Schritte aus

---

Einzelne Einstellung auf ihren Standardwert zurücksetzen

Klicken Sie neben der entsprechenden Einstellung auf den Link **Zurücksetzen**

---

4 Klicken Sie auf *Einstellungen speichern*.

## 9.4.5 Ändern von Standardeinstellungen für Portlet-Registrierungen

Portlet-Standardeinstellungen werden durch den Portlet-Entwickler während der Entwicklungsphase im Portlet-Implementierungsdeskriptor festgelegt. Die Standardeinstellungen sind von Portlet zu Portlet verschieden und sind von der Implementierung durch den Portlet-Entwickler abhängig.

Sie können die Werte dieser Standardeinstellungen für jede einzelnen Registrierung über die Seite „Portletadministration“ ändern. In diesem Fall werden die neuen Werte nur für die ausgewählte Portlet-Registrierung wirksam.

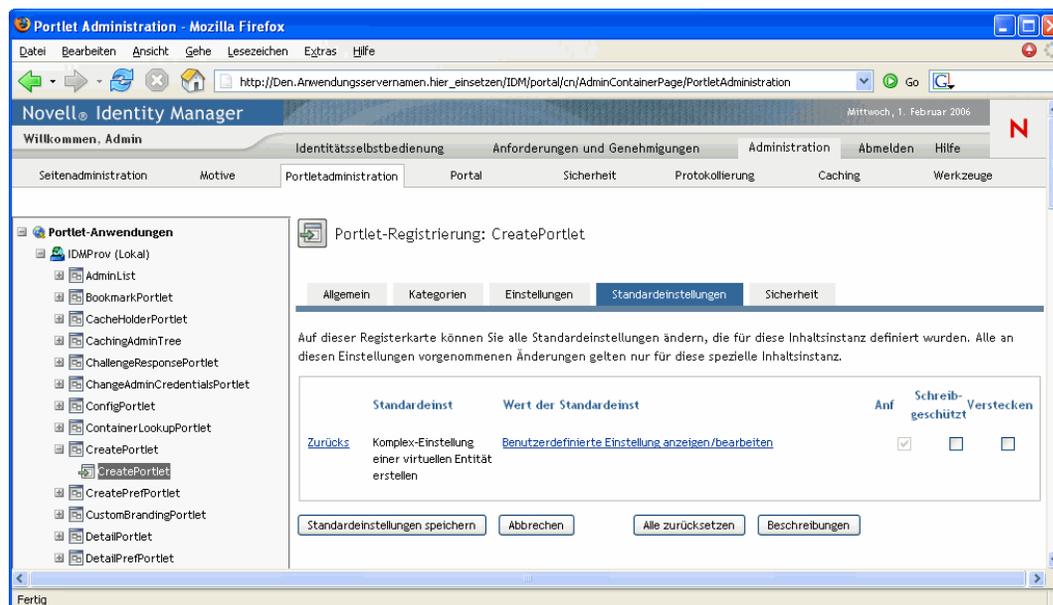
So ändern Sie Standardeinstellungen für die Portlet-Registrierung:

- 1 Wählen Sie in der Liste „Portlet-Anwendungen“ die Portlet-Registrierung aus, deren Standardeinstellungen Sie ändern möchten.

Auf der rechten Seite wird das Teilfenster *Allgemein* angezeigt.

- 2 Wechseln Sie zum Teilfenster *Standardeinstellungen*.

In diesem Teilfenster werden die aktuellen Standardeinstellungen für die ausgewählte Portlet-Registrierung angezeigt:



- 3 Nehmen Sie die gewünschten *Änderungen* an den Standardeinstellungen vor.

Beim Arbeiten mit diesem Teilfenster können Sie zudem die folgenden Aktionen ausführen:

Um Folgendes zu erzielen	Führen Sie diese Schritte aus
Weitere Informationen zu den Standardeinstellungen anzeigen	Klicken Sie auf <b>Beschreibungen</b>
Ungespeicherte Änderungen verwerfen	Klicken Sie auf <b>Abbrechen</b>
Alle Standardeinstellungen für die ausgewählte Portlet-Registrierung auf ihre Standardwerte zurücksetzen (wie in der zugehörigen Portlet-Definition festgelegt)	Klicken Sie auf <b>Alle zurücksetzen</b>
Einzelne Standardeinstellung auf ihren Standardwert zurücksetzen	Klicken Sie neben der entsprechenden Standardeinstellung auf den Link <b>Zurücksetzen</b>

- 4 Um die *lokalisierte Version* einer Standardeinstellung für jede in der Portlet-Definition angegebene Ländereinstellung zu ändern, gehen Sie wie folgt vor:
  - 4a Klicken Sie neben der entsprechenden Standardeinstellung auf den Link *Detail* (falls vorhanden).  
Im Teilfenster werden die Standardeinstellungswerte für die einzelnen Ländereinstellungen angezeigt.
  - 4b Nehmen Sie die gewünschten *Änderungen* an den Werten vor.
  - 4c Klicken Sie auf *OK*, um Ihre Änderungen zu übernehmen und zur Hauptliste der Standardeinstellungen zurückzukehren.
- 5 Klicken Sie auf *Standardeinstellungen speichern*.

## 9.4.6 Zuweisen von Sicherheitsberechtigungen zu Portlet-Registrierungen

Sie können Benutzern, Gruppen und Containern für Portlet-Registrierungen die folgenden Sicherheitsberechtigungen zuweisen:

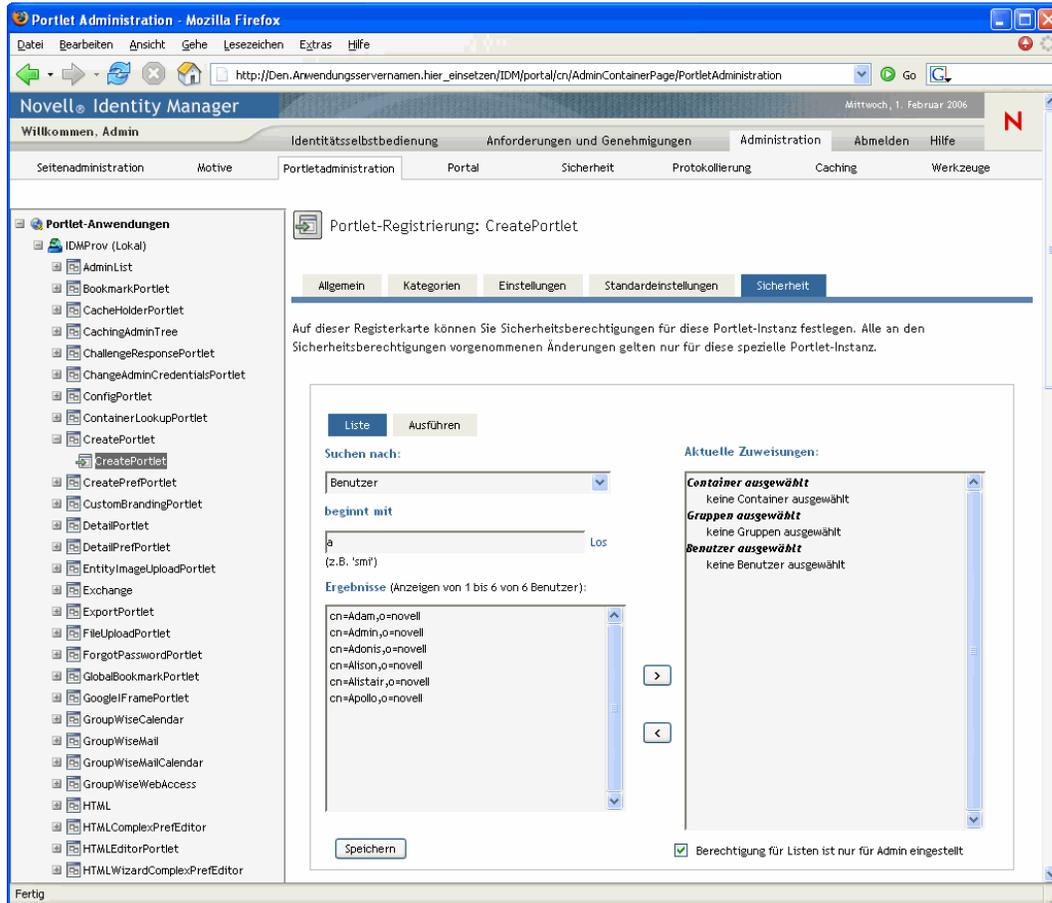
Berechtigung	Beschreibung
Liste	Benutzer können die Portlet-Registrierung in einer Auswahlliste <b>anzeigen</b>
Ausführen	Benutzer können die Portlet-Registrierung auf einer Portalseite <b>ausführen</b>

Beim Ändern von Sicherheitsberechtigungen werden die neuen Werte nur für die ausgewählte Portlet-Registrierung wirksam.

So weisen Sie Portlet-Registrierungen Sicherheitsberechtigungen zu:

- 1 Wählen Sie in der Liste „Portlet-Anwendungen“ die Portlet-Registrierung aus, deren Sicherheitsberechtigungen Sie ändern möchten.  
Auf der rechten Seite wird das Teilfenster *Allgemein* angezeigt.
- 2 Wechseln Sie zum Teilfenster *Sicherheit*.

In diesem Teilfenster werden die aktuellen Sicherheitsberechtigungen für die ausgewählte Portlet-Registrierung angezeigt:



- 3 Wechseln Sie zum Register *Liste* oder *Ausführen*, je nachdem, welche Art der Berechtigung Sie erteilen möchten.
- 4 Geben Sie Werte für die folgenden *Sucheinstellungen* an:

Einstellung	Vorgehensweise
Suchen nach	Wählen Sie eine der folgenden Optionen im Dropdown-Menü aus: <ul style="list-style-type: none"> <li>• Benutzer</li> <li>• Gruppen</li> <li>• Container</li> </ul>

Einstellung	Vorgehensweise
Beginnt mit	<p>Um Folgendes zu erzielen:</p> <ul style="list-style-type: none"> <li>• Wenn Sie nach <b>allen</b> verfügbaren Objekten des von Ihnen angegebenen Typs (Benutzer, Gruppe oder Container) suchen möchten, geben Sie in diesem Feld nichts ein.</li> <li>• Wenn Sie nach einer <b>bestimmten Teilmenge</b> dieser Objekte suchen möchten, geben Sie hier den bzw. die Anfangsbuchstaben der gewünschten CN-Werte ein. (Die Groß-/Kleinschreibung wird dabei nicht berücksichtigt. Es werden keine Platzhalter unterstützt.)</li> </ul> <p>Wenn Sie beispielsweise nach Gruppen suchen, die mit <b>s</b> beginnen, erhalten Sie folgendes Ergebnis:</p> <pre>cn=Schulung,ou=Gruppen,o=MeineFirma</pre> <pre>cn=Service,ou=Gruppen,o=MeineFirma</pre> <pre>cn=Sicherheit,ou=Gruppen,o=MeineFirma</pre> <p>Wenn Sie nach Gruppen suchen, die mit <b>se</b> beginnen, erhalten Sie in diesem Fall folgendes Ergebnis:</p> <pre>cn=Service,ou=Gruppen,o=MeineFirma</pre>

**5** Klicken Sie auf *Ausführen*.

Die Ergebnisse Ihrer Suche werden in der Liste *Ergebnisse* angezeigt.

**6** Wählen Sie die Benutzer, Gruppen oder Container aus, die Sie der Portlet-Registrierung zuweisen möchten, und klicken Sie anschließend auf die Schaltfläche *Hinzufügen (>)*.

**Tipp:** Halten Sie die *Strg*-Taste gedrückt, wenn Sie mehrere Elemente auswählen möchten.

**7** Aktivieren bzw. deaktivieren Sie die *Sperre* für die Portlet-Registrierung wie folgt:

Um Folgendes zu erzielen	Führen Sie diese Schritte aus
Die Portlet-Registrierung sperren, damit nur Benutzeranwendungsadministratoren sie in der Liste anzeigen/ausführen können	Aktivieren Sie die Option <b>Berechtigung für Listen/Ausführungsberechtigung ist nur für Admin eingestellt</b>
Allen zugewiesenen Benutzern, Gruppen und Containern ermöglichen, die Portlet-Registrierung in einer Liste anzuzeigen/auszuführen	Deaktivieren Sie die Option <b>Berechtigung für Listen/Ausführungsberechtigung ist nur für Admin eingestellt</b>
	<p><b>Hinweis:</b> Wenn Sie diese Einstellung deaktivieren, jedoch keine Benutzer, Gruppen oder Container ausdrücklich der Portlet-Registrierung zugewiesen sind, erhalten alle die <b>Berechtigung für Listen/Ausführungsberechtigung</b> für die entsprechende Portlet-Registrierung.</p>

8 Klicken Sie auf *Speichern*.

## 9.4.7 Aufheben der Registrierung von Portlets

Über die Seite „Portletadministration“ können Sie bei Bedarf die Registrierung eines Portlets aufheben.

---

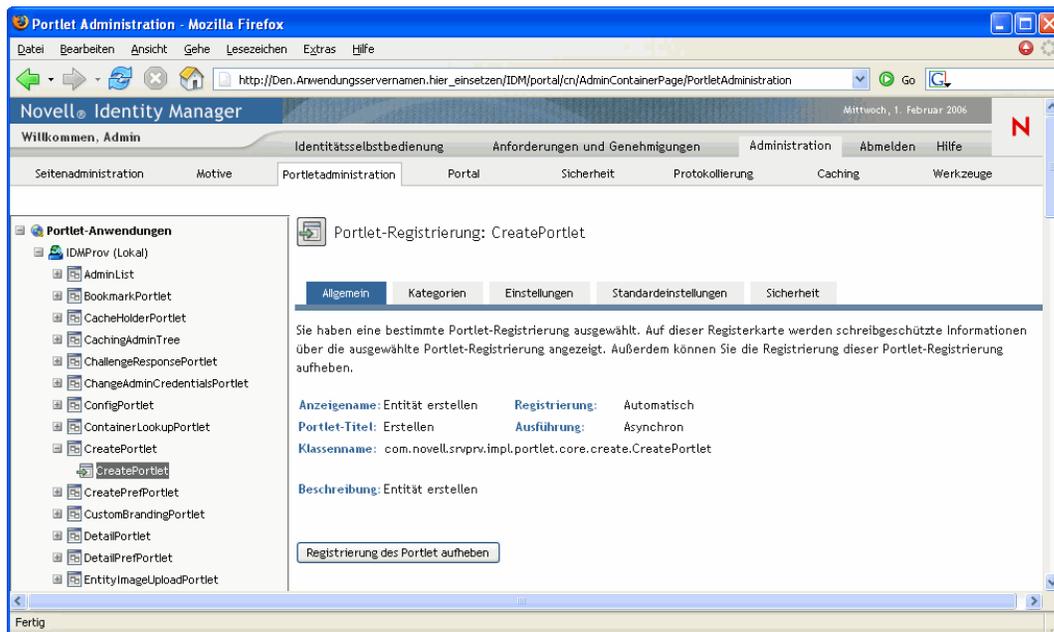
**Hinweis:** Wenn Sie die Registrierung eines Portlets aufheben, das als *automatisch registriert* definiert ist, wird dieses Portlet bei einem Neustart des Anwendungsservers automatisch erneut registriert.

---

So heben Sie die Registrierung eines Portlets auf:

- 1 Wählen Sie in der Liste „Portlet-Anwendungen“ die Portlet-Registrierung aus, deren Registrierung Sie aufheben möchten.

Auf der rechten Seite wird das Teilfenster *Allgemein* mit Informationen zur ausgewählten Portlet-Registrierung angezeigt:



- 2 Klicken Sie auf *Registrierung des Portlet aufheben*.
- 3 Wenn Sie dazu aufgefordert werden, die Aufhebung der Registrierung zu bestätigen, klicken Sie auf *OK*.



In diesem Kapitel erfahren Sie, wie Sie die Seite *Portal* der Registerkarte *Administration* der Benutzeroberfläche von Identity Manager verwenden. Es werden folgende Themen erläutert:

- **Abschnitt 10.1**, „Allgemeines zur Portalkonfiguration“, auf Seite 201
- **Abschnitt 10.2**, „Allgemeine Einstellungen“, auf Seite 201
- **Abschnitt 10.3**, „LDAP-Verbindungsparameter“, auf Seite 204

Allgemeine Informationen zum Zugriff auf die und zum Arbeiten mit der Registerkarte „Administration“ finden Sie in **Kapitel 6**, „Verwendung der Registerkarte „Administration““, auf Seite 131.

## 10.1 Allgemeines zur Portalkonfiguration

Über die Seite „Portal“ können Sie die *Portaleigenschaften* der Identity Manager-Benutzeranwendung steuern und angeben, wie die Verbindung der Benutzeranwendung mit dem *Identitätsdepot* (LDAP-Anbieter) hergestellt werden soll.

## 10.2 Allgemeine Einstellungen

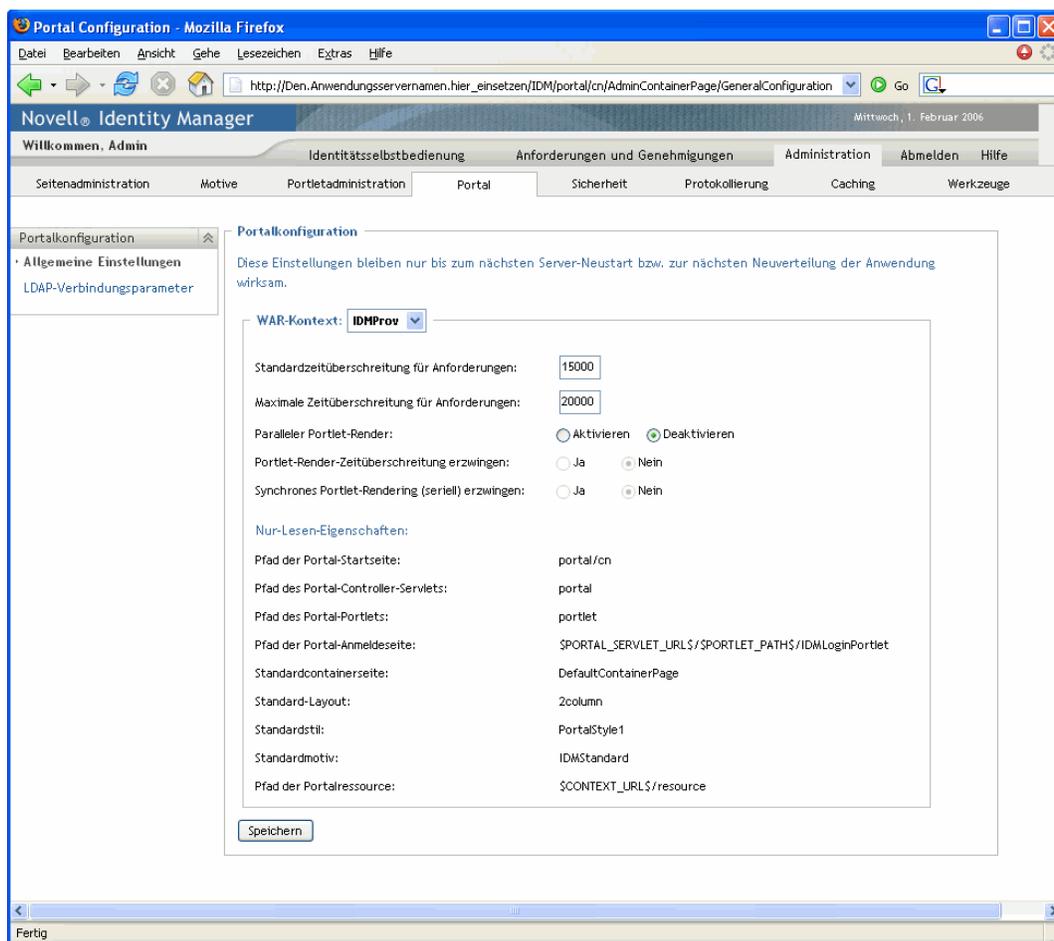
Eines der Elemente der Portal-Seite ist das Teilfenster „Allgemeine Einstellungen“, das Ihnen folgende Möglichkeiten bietet:

- Vorübergehendes *Ändern einiger Portaleigenschaften* der Identity Manager-Benutzeranwendung (bis zum nächsten Neustart des Anwendungsservers bzw. bis zur erneuten Implementierung der Benutzeranwendung)
- *Anzeigen weiterer Portaleigenschaften* der Identity Manager-Benutzeranwendung

So verwalten Sie allgemeine Einstellungen:

- 1 Wählen Sie im Navigationsmenü links auf der Seite „Portal“ die Option *Allgemeine Einstellungen*.

Das gleichnamige Teilfenster wird angezeigt:



- 2 Wenn Ihnen mehr als ein *WAR-Kontext* zur Verfügung steht, wählen Sie den Kontext aus, auf dessen Einstellungen Sie zugreifen möchten.

Das Teilfenster wird aktualisiert und zeigt die aktuellen Einstellungen für den ausgewählten Kontext an.

- 3 *Überprüfen* Sie die Einstellungen und nehmen Sie die gewünschten *Änderungen* daran vor. Weitere Informationen finden Sie in:
  - [Abschnitt 10.2.1, „Änderbare Einstellungen“, auf Seite 202](#)
  - [Abschnitt 10.2.2, „Schreibgeschützte Einstellungen“, auf Seite 204](#)
- 4 Wenn Sie die vorgenommenen Änderungen übernehmen möchten, klicken Sie auf *Speichern*.

## 10.2.1 Änderbare Einstellungen

Sie können mehrere Portaleinstellungen im Teilfenster „Allgemeine Einstellungen“ ändern. Die von Ihnen eingegebenen Werte bleiben bis zum nächsten Anwendungsserver-Neustart bzw. bis zur erneuten Implementierung der Benutzeranwendung gültig. Bei einem Neustart oder einer erneuten

Implementierung werden diese Einstellungen auf die Standardwerte für die WAR-Datei der Benutzeranwendung zurückgesetzt.

Einstellung	Vorgehensweise
Standardzeitüberschreitung für Anforderungen	<p>Geben Sie die Standardzeit (in Millisekunden) an, die eine Anforderung wartet, bevor eine Zeitüberschreitung eintritt.</p> <p>Wenn keines der asynchronen Portlets eine Zeitüberschreitung definiert oder keines der Portlets eine Zeitüberschreitung mit einem höheren Wert definiert, wird dieser Standardwert verwendet. Wenn eines oder mehrere der zu rendernden Portlets eine Zeitüberschreitung definiert, die größer als dieser Standardwert ist, wird dieser höhere Wert anstelle des Standardwerts verwendet.</p> <p>Diese Einstellung kann zum Schutz der Anwendung vor zu vielen Portlet-Zeitüberschreitungsmeldungen verwendet werden (ein Problem, das auftreten kann, wenn die durch die Portlets definierten Werte zu niedrig sind).</p> <hr/> <p><b>Hinweis:</b> Falls alle Portlets gerendert werden können, bevor die Zeitüberschreitung eintritt, wird die Anforderung umgehend an den Client zurückgegeben.</p>
Maximale Zeitüberschreitung für Anforderungen	<p>Geben Sie die maximale Zeit (in Millisekunden) an, die das Abschließen einer Anforderung hinausgezögert werden kann. Hierbei handelt es sich um den Zeitraum, nach dem alle Anforderungen an den Client zurückgegeben werden, auch wenn ein oder mehrere Portlets einen höheren Zeitüberschreitungswert definieren.</p> <p>Diese Einstellung kann verwendet werden, um sicherzustellen, dass das Portal auch dann zeitnah Daten zurückgibt, wenn ein oder mehrere Portlets einen hohen Zeitüberschreitungswert definieren.</p>
Paralleler Portlet-Render	<p>Hiermit lässt sich das asynchrone Portlet-Rendering durch das Portal aktivieren bzw. deaktivieren.</p> <p>Diese erweiterte Funktion ist standardmäßig deaktiviert. Wenn Sie diese Funktion aktivieren, weist das Portal individuellen Threads asynchrone Rendering-Anforderungen zu (wodurch Portlets Inhalte parallel rendern können).</p> <p>Wenn diese Funktion deaktiviert ist, rendern alle Portlets Inhalte synchron im Hauptanforderungs-Thread.</p>
Portlet-Render-Zeitüberschreitung erzwingen	<p>Diese Einstellung legt fest, ob asynchrone Portlets zum Inhalts-Rendering an den Hauptanforderungs-Thread delegiert werden sollen, wenn im Thread-Pool nicht genügend individuelle Threads vorhanden sind.</p> <p>Wenn Sie <b>Nein</b> wählen, können asynchrone Portlets im Hauptanforderungs-Thread ausgeführt werden, wenn keine individuellen Threads zur Verfügung stehen.</p> <p>Wenn Sie <b>Ja</b> wählen, müssen asynchrone Portlets warten, bis individuelle Threads zum Inhalts-Rendering zur Verfügung stehen. Wenn bei Portlets eine Zeitüberschreitung auftritt, bevor sie die Rendering-Anforderung ausführen können, wird im Portlet-Fenster eine portletspezifische Fehlermeldung generiert.</p>

Einstellung	Vorgehensweise
Synchrones Portlet-Rendering (seriell) erzwingen	<p>Diese Einstellung legt fest, wie synchrone Portlets ausgeführt werden.</p> <p>Wenn Sie <b>Ja</b> wählen, werden alle synchronen Portlets im Hauptanforderungs-Thread ausgeführt.</p> <p>Wählen Sie <b>Nein</b>, kann das Portal der Verarbeitung von synchronen Rendering-Anforderungen einen eigenen Thread zuordnen (wodurch Engpässe beim Hauptanforderungs-Thread vermieden werden).</p>

## 10.2.2 Schreibgeschützte Einstellungen

Die folgenden Einstellungen werden nur zu Informationszwecken angezeigt und können nicht im Teilfenster „Allgemeine Einstellungen“ geändert werden:

Pfad der Portal-Startseite	Standard-Layout
Pfad des Portal-Controller-Servlets	Standardstil
Pfad des Portal-Portlets	Standardmotiv
Pfad der Portal-Anmeldeseite	Pfad der Portalressource
Standardcontainerseite	

Die Werte dieser Einstellungen werden in der WAR-Datei der Benutzeranwendung festgelegt. (Beachten Sie, dass als „Standardmotiv“ das Motiv angegeben wird, das Sie auf der Seite „Motive“ ausgewählt haben.)

## 10.3 LDAP-Verbindungsparameter

Ein Element der Seite „Portal“ ist das Teilfenster „LDAP-Verbindungsparameter“, das Ihnen folgende Möglichkeiten bietet:

- *Ändern der Berechtigungsnachweise*, die die Identity Manager-Benutzeranwendung beim Verbindungsaufbau mit dem Identitätsdepot (LDAP-Anbieter) verwendet
- *Anzeigen weiterer LDAP-Eigenschaften* der Identity Manager-Benutzeranwendung

So verwalten Sie LDAP-Verbindungsparameter:

- 1 Wählen Sie im Navigationsmenü links auf der Seite „Portal“ die Option *LDAP-Verbindungsparameter*.

Das Teilfenster „LDAP-Verbindungsparameter“ wird angezeigt:

LDAP-Verbindungsparameter

LDAP-Verbindungsberechtigungs-nachweis ändern

Sie können den Berechtigungsnachweis ändern, der verwendet wird, um eine Verbindung von der Identity Manager-Benutzeranwendung zum LDAP-Provider (Identitätsdepot) herzustellen. Geben Sie einen Benutzer auf Administrationsebene an (möglichst nicht den Benutzer, der als Benutzeranwendungsadministrator angegeben ist).

Benutzername:

Passwort:

Passwort bestätigen:

LDAP-Eigenschaften (Nur Lesen)

ALIAS_HANDLING	never
ANONYMOUS_USER	ANONYMOUS
AUTHORITY	172.22.10.89
CONNECTION_TIMEOUT	300000
CONTAINER_OBJECT	locality
CONTAINER_OBJECT_ATTRIB	l
CONTAINER_OBJECT2	country
CONTAINER_OBJECT2_ATTRIB	c
CONTAINER_OBJECT3	organizationalUnit
CONTAINER_OBJECT3_ATTRIB	ou
CONTAINER_OBJECT4	organization
CONTAINER_OBJECT4_ATTRIB	o
CONTEXT_FACTORY	com.sun.jndi.ldap.LdapCtxFactory
DYNAMIC_GROUP_OBJECT	dynamicGroup
GROUP_OBJECT	groupOfNames
GROUP_ROOT_CONTAINER	o=novell
GROUP_SEARCH_SCOPE	subtree
GROUP_USER_MEMBER_ATTRIB	member
KEYSTORE_PATH	c:\Novell\IDM\jre\lib\security\cacerts
LOGIN_ATTRIBUTE	cn
NAME	LDAPRealm
OBJECT_ATTRIB	objectClass
PROVISION_ROOT	cn=UserApplication,cn=TestatDriverSet,o=novell
REFERRAL	ignore
ROOT_NAME	o=novell
USE_DYNAMIC_GROUPS	false
USE_REGISTERED_DYNAMIC_GROUPS	false
USE_SSL	true
USER_GROUP_MEMBER_ATTRIB	groupMembership
USER_OBJECT	inetOrgPerson
USER_ROOT_CONTAINER	o=novell
USER_SEARCH_SCOPE	subtree
UUID_ATTRIB	srvpriUUID
UUID_AUX_CLASS	srvpriEntityAux

2 Überprüfen Sie die Einstellungen und nehmen Sie die gewünschten Änderungen daran vor. Weitere Informationen finden Sie in:

- [Abschnitt 10.2.1, „Änderbare Einstellungen“, auf Seite 202](#)
- [Abschnitt 10.3.2, „Schreibgeschützte Einstellungen“, auf Seite 206](#)

3 Wenn Sie die vorgenommenen Änderungen übernehmen möchten, klicken Sie auf *Senden*.

## 10.3.1 Änderbare Einstellungen

Im Teilfenster „LDAP-Verbindungsparameter“ können Sie die Einstellungen für die Berechtigungsnachweise ändern, die die Identity Manager-Benutzeranwendung bei jedem Verbindungsaufbau mit dem Identitätsdepot (LDAP-Anbieter) verwenden soll. Ihre Änderungen in diesem Teilfenster werden in der Datenbank der Benutzeranwendung gespeichert und zur Laufzeit verwendet und mit den Vorgaben des Identitätsdepots abgeglichen. (Beachten Sie, dass die Werte für die Berechtigungsnachweise, die von der WAR-Datei der Benutzeranwendung bei der Installation vorgegeben wurden, nicht über dieses Fenster aktualisiert werden.)

Einstellung	Vorgehensweise
Benutzername	<p>Geben Sie den Namen eines Benutzers mit uneingeschränkten <b>Administrator</b>-Rechten für das Identitätsdepot ein. Die Identity Manager-Benutzeranwendung muss auf das Identitätsdepot als Administrator zugreifen, damit sie ordnungsgemäß arbeiten kann.</p> <p>Üblicherweise wird als Benutzername für die LDAP-Verbindung der <b>root-Administrator</b> des Identitätsdepots angegeben. Der root-Administrator hat uneingeschränkten Zugriff auf die Verzeichnisstruktur, daher ist es nicht erforderlich, spezielle Trustee-Rechte zuzuweisen.</p> <p>Zum Beispiel:</p> <pre>cn=admin,o=meinefirma</pre> <p>Wenn Sie einen anderen Benutzer angeben, müssen Sie den Eigenschaften [All Attributes Rights] und [Entry Rights] Ihres Benutzeranwendungsstreibers vererbbsame Trustee-Rechte zuweisen.</p> <hr/> <p><b>Hinweis:</b> Um Verwechslungen zu vermeiden, wird empfohlen, <b>nicht</b> den Benutzeranwendungsadministrator der Benutzeranwendung als Benutzername für die LDAP-Verbindung zu verwenden. Am besten verwendet man für diese beiden Zwecke getrennte Konten.</p>
Passwort und Passwort bestätigen	<p>Geben Sie das Passwort ein, das aktuell für diesen Benutzernamen im Identitätsdepot festgelegt ist.</p>

## 10.3.2 Schreibgeschützte Einstellungen

Die folgenden Einstellungen werden nur zu Informationszwecken angezeigt und können nicht im Teilfenster „LDAP-Verbindungsparameter“ geändert werden:

ALIAS_HANDLING	GROUP_USER_MEMBER_ATTRIB
ANONYMOUS_USER	KEYSTORE_PATH
AUTHORITY	LOGIN_ATTRIBUTE
CONNECTION_TIMEOUT	NAME
CONTAINER_OBJECT	OBJECT_ATTRIB

---

CONTAINER_OBJECT_ATTRIB	PROVISION_ROOT
CONTAINER_OBJECT2	REFERRAL
CONTAINER_OBJECT2_ATTRIB	ROOT_NAME
CONTAINER_OBJECT3	USE_DYNAMIC_GROUPS
CONTAINER_OBJECT3_ATTRIB	USE_REGISTERED_DYNAMIC_GROUPS
CONTAINER_OBJECT4	USE_SSL
CONTAINER_OBJECT4_ATTRIB	USER_GROUP_MEMBER_ATTRIB
CONTEXT_FACTORY	USER_OBJECT
DYNAMIC_GROUP_OBJECT	USER_ROOT_CONTAINER
GROUP_OBJECT	USER_SEARCH_SCOPE
GROUP_ROOT_CONTAINER	UUID_ATTRIB
GROUP_SEARCH_SCOPE	UUID_AUX_CLASS

---

Die Werte dieser Einstellungen werden beim Installieren der Benutzeranwendung festgelegt.



In diesem Kapitel erfahren Sie, wie Sie die Seite *Sicherheit* der Registerkarte *Administration* der Benutzeroberfläche von Identity Manager verwenden. Es werden folgende Themen erläutert:

- [Abschnitt 11.1, „Allgemeines zur Sicherheitskonfiguration“](#), auf Seite 209
- [Abschnitt 11.2, „Zuweisen eines Benutzeranwendungsadministrators“](#), auf Seite 210

Allgemeine Informationen zum Zugriff auf die und zum Arbeiten mit der Registerkarte „Administration“ finden Sie in [Kapitel 6, „Verwendung der Registerkarte „Administration““](#), auf Seite 131.

## 11.1 Allgemeines zur Sicherheitskonfiguration

Auf der Seite „Sicherheit“ können Sie den *Benutzeranwendungsadministrator* für die Identity Manager-Benutzeranwendung festlegen.

Ein Benutzeranwendungsadministrator ist berechtigt, alle Verwaltungsfunktionen in Verbindung mit der Identity Manager-Benutzeranwendung auszuführen. Dies umfasst den Zugriff auf die Registerkarte „Administration“ der Benutzeroberfläche von Identity Manager, um die dort verfügbaren Verwaltungsaktionen auszuführen.

Bei der Installation wird ein Benutzer als Benutzeranwendungsadministrator festgelegt. Nach der Installation kann dieser Benutzer auf der Seite „Sicherheit“ bei Bedarf weitere Benutzeranwendungsadministratoren angeben.

Ein Benutzer, der als Benutzeranwendungsadministrator konfiguriert werden soll, sollte sich üblicherweise *im Benutzerstammcontainer befinden*, der in der LDAP-Konfiguration der Benutzeranwendung festgelegt ist. Hierdurch kann sich der Benutzer einfach mit seinem Benutzernamen anmelden (und muss nicht jedes Mal seinen eindeutigen Namen [Distinguished Name, DN] eingeben). Üblicherweise hat dieser Benutzer außerdem *Rechte zum Verwalten und Erstellen von Objekten* in der Baumstruktur. Diese sind jedoch nicht zwingend erforderlich.

---

**Hinweis:** Bei Bedarf kann ein Benutzeranwendungsadministrator einem oder mehreren Endbenutzern die Anzeige- und Zugriffsberechtigungen für bestimmte Seiten der Registerkarte „Administration“ erteilen. Diese Berechtigungen werden über die Seite *Seitenadministration* der Registerkarte „Administration“ erteilt. (Weitere Informationen hierzu finden Sie in [Kapitel 7, „Seitenadministration“](#), auf Seite 137.)

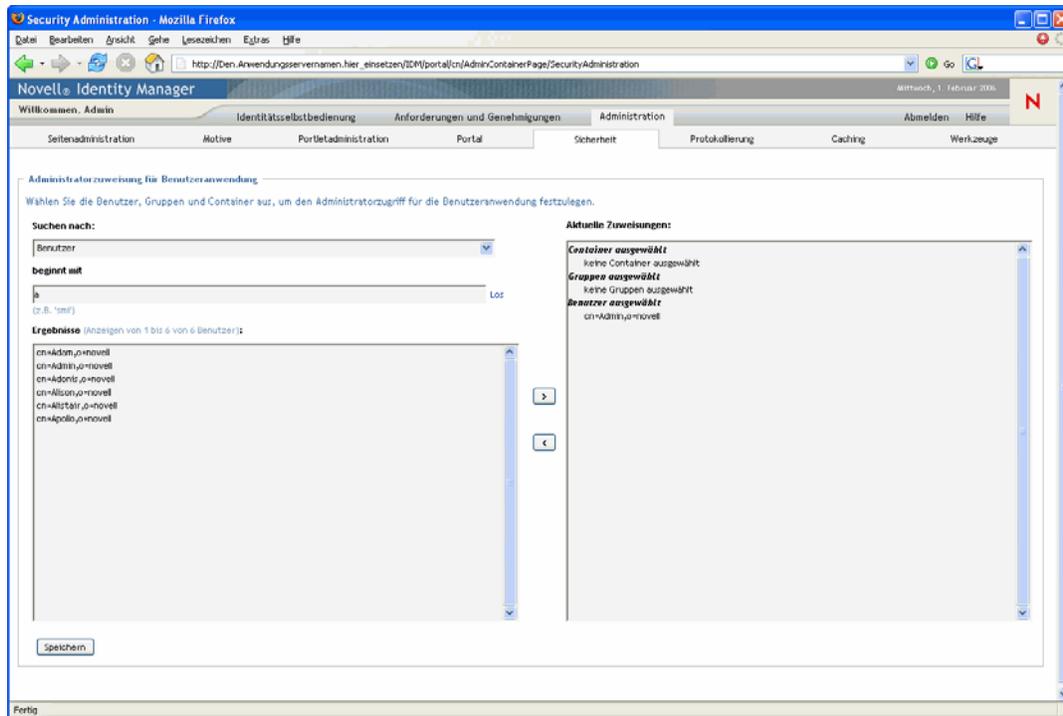
---

## 11.2 Zuweisen eines Benutzeranwendungsadministrators

Beim Zuweisen von Benutzeranwendungsadministratoren können Sie Benutzer, Gruppen oder Container angeben.

So weisen Sie Benutzeranwendungsadministratoren zu:

- 1 Wechseln Sie zur Seite *Sicherheit*:



- 2 Geben Sie Werte für die folgenden *Sucheinstellungen* an:

Einstellung	Vorgehensweise
Suchen nach	Wählen Sie eine der folgenden <i>Sucheinstellungen</i> an: <ul style="list-style-type: none"><li>• Benutzer</li><li>• Gruppen</li><li>• Container</li></ul>

Einstellung	Vorgehensweise
Beginnt mit	<p>Um Folgendes zu erzielen:</p> <ul style="list-style-type: none"> <li>• Wenn Sie nach <b>allen</b> verfügbaren Objekten des von Ihnen angegebenen Typs (Benutzer, Gruppe oder Container) suchen möchten, geben Sie in diesem Feld nichts ein.</li> <li>• Wenn Sie nach einer <b>bestimmten Teilmenge</b> dieser Objekte suchen möchten, geben Sie hier den bzw. die Anfangsbuchstaben der gewünschten CN-Werte ein. (Die Groß-/Kleinschreibung wird dabei nicht berücksichtigt. Es werden keine Platzhalter unterstützt.)</li> </ul> <p>Wenn Sie beispielsweise nach Gruppen suchen, die mit <i>s</i> beginnen, erhalten Sie folgendes Ergebnis:</p> <pre>cn=Schulung,ou=Gruppen,o=MeineFirma</pre> <pre>cn=Service,ou=Gruppen,o=MeineFirma</pre> <pre>cn=Sicherheit,ou=Gruppen,o=MeineFirma</pre> <p>Wenn Sie nach Gruppen suchen, die mit <i>se</i> beginnen, erhalten Sie in diesem Fall folgendes Ergebnis:</p> <pre>cn=Service,ou=Gruppen,o=MeineFirma</pre>

**3** Klicken Sie auf *Ausführen*.

Die Ergebnisse Ihrer Suche werden in der Liste *Ergebnisse* angezeigt.

**4** Wählen Sie die Benutzer, Gruppen oder Container aus, die Sie als Benutzeranwendungsadministratoren benennen möchten, und klicken Sie anschließend auf die Schaltfläche *Hinzufügen* (>).

**Tipp:** Halten Sie die *Strg*-Taste gedrückt, wenn Sie mehrere Elemente auswählen möchten.

**5** Klicken Sie auf *Speichern*.

So heben Sie die Zuweisung von Benutzeranwendungsadministratoren auf:

**1** Wählen Sie in der Liste *Aktuelle Zuweisungen* die Benutzer, Gruppen oder Container aus, deren Zuweisung als Benutzeranwendungsadministratoren Sie aufheben möchten, und klicken Sie anschließend auf die Schaltfläche *Entfernen* (<).

**Tipp:** Halten Sie die *Strg*-Taste gedrückt, wenn Sie mehrere Elemente auswählen möchten.

**2** Klicken Sie auf *Speichern*.



In diesem Kapitel erfahren Sie, wie Sie die Seite *Protokollierung* der Registerkarte *Administration* der Benutzeroberfläche von Identity Manager verwenden. Es werden folgende Themen erläutert:

- [Abschnitt 12.1, „Allgemeines zur Konfiguration der Protokollierung“](#), auf Seite 213
- [Abschnitt 12.2, „Allgemeines zu den Protokollen“](#), auf Seite 213
- [Abschnitt 12.3, „Ändern des Protokollierungsumfangs“](#), auf Seite 216
- [Abschnitt 12.4, „Senden von Protokollmeldungen an Novell Audit“](#), auf Seite 217
- [Abschnitt 12.5, „Dauerhafte Übernahme von Protokolleinstellungen“](#), auf Seite 217

Allgemeine Informationen zum Zugriff auf die und zum Arbeiten mit der Registerkarte „Administration“ finden Sie in [Kapitel 6, „Verwendung der Registerkarte „Administration““](#), auf Seite 131.

## 12.1 Allgemeines zur Konfiguration der Protokollierung

Über die Seite „Protokollierung“ können Sie den *Umfang der Protokollierungsmeldungen* festlegen, die die Identity Manager-Benutzeranwendung generieren soll, und angeben, ob diese Meldungen an *Novell Audit* gesendet werden sollen.

Die Identity Manager-Benutzeranwendung implementiert die Protokollierung unter Verwendung von *log4j*, einem Open-Source-Protokollierungspaket der Apache Software Foundation. Standardmäßig werden Ereignismeldungen an zwei Orten gleichzeitig protokolliert:

- *Auf der Systemkonsole* des Anwendungsservers, auf dem die Identity Manager-Benutzeranwendung implementiert ist
- *In einer Protokolldatei* auf diesem Anwendungsserver, beispielsweise:

```
jboss/server/IDM/log/server.log
```

Hierbei handelt es sich um eine rollierende Protokolldatei, d. h. wenn sie eine bestimmte Größe erreicht hat, wird die Protokollierung in einer neuen Protokolldatei fortgeführt (und so weiter).

Wenn Sie Ihre Umgebung für die Verwendung von Novell Audit konfiguriert haben, können Sie optional auch dort Ereignismeldungen protokollieren.

Details zur Konfiguration Ihrer Protokollierungsumgebung und von Novell Audit finden Sie in [Kapitel 5, „Einrichten der Protokollierung“](#), auf Seite 121.

## 12.2 Allgemeines zu den Protokollen

Auf der Seite „Protokollierung“ sind zahlreiche Protokolle aufgeführt, die jeweils Ereignismeldungen von einem unterschiedlichen Teil der Identity Manager-Benutzeranwendung ausgeben. Jede Protokolldatei verfügt über ihre eigene, unabhängige Ausgabeebene.

Die Protokollnamen basieren auf log4j-Konventionen. Diese Protokollnamen werden in den generierten Ereignismeldungen angezeigt, wodurch sich der Kontext der Meldungsausgabe erkennen lässt.

Protokollname	Beschreibung
com.novell	Übergeordnetes Protokoll zu anderen Protokollen der Identity Manager-Benutzeranwendung
com.novell.afw.portal.aggregation	Meldungen im Zusammenhang mit der Portalseitenverarbeitung
com.novell.afw.portal.persist	Meldungen im Zusammenhang mit der Persistenz von Portal-daten (einschließlich Portalseiten und Portlet-Registrierungen)
com.novell.afw.portal.portlet	Meldungen von den Haupt- und Zubehör-Portlets des Portals
com.novell.afw.portal.util	Meldungen von den Import-/Export- und Navigations-Portlets des Portals
com.novell.afw.portlet.consumer	Meldungen im Zusammenhang mit dem Portlet-Rendering
com.novell.afw.portlet.core	Meldungen im Zusammenhang mit der Haupt-Portlet-API
com.novell.afw.portlet.persist	Meldungen im Zusammenhang mit der Persistenz von Portlet-Daten (einschließlich Portlet-StandardEinstellungen und Einstellungswerten)
com.novell.afw.portlet.producer	Meldungen im Zusammenhang mit der Registrierung und Konfiguration von Portlets innerhalb des Portals
com.novell.afw.portlet.util	Meldungen im Zusammenhang mit von Portlets verwendetem Dienstprogrammcode
com.novell.afw.theme	Meldungen vom Motiv-Subsystem
com.novell.afw.util	Meldungen im Zusammenhang mit Portaldienstprogramm-klassen
com.novell.soa.af.impl	Meldungen vom Genehmigungsablauf (Bereitstellungs-Workflow)-Subsystem
com.novell.srvprv.apwa	Meldungen von der Webanwendung für Anforderungen und Genehmigungen (Aktionen und Tags)
com.novell.srvprv.impl.portlet.core	Meldungen von den Haupt-Identitäts-Portlets und Passwort-Portlets
com.novell.srvprv.impl.portlet.util	Meldungen von den identitätsbezogenen Dienstprogramm-Portlets
com.novell.srvprv.impl.servlet	Meldungen von dem ajax-Servlet und den ajax-Diensten des UI-Steuerungs-Frameworks
com.novell.srvprv.impl.uictrl	Meldungen von der UI-Steuerungs-Registrierungs-API und dem Rendern von Genehmigungsformularen
com.novell.srvprv.impl.vdata	Meldungen von der Verzeichnisabstraktionsschicht
com.novell.srvprv.spi	Meldungen von der UI-Steuerungs-Registrierungs-API

<b>Protokollname</b>	<b>Beschreibung</b>
com.sssw.fw.cachemgr	Meldungen im Zusammenhang mit dem Framework-Cache-Subsystem
com.sssw.fw.core	Meldungen im Zusammenhang mit dem Framework-Core-Subsystem
com.sssw.fw.directory	Meldungen im Zusammenhang mit dem Framework-Verzeichnis-Subsystem
com.sssw.fw.event	Meldungen im Zusammenhang mit dem Framework-Ereignis-Subsystem
com.sssw.fw.factory	Meldungen im Zusammenhang mit dem Framework-Factory-Subsystem
com.sssw.fw.persist	Meldungen im Zusammenhang mit dem Framework-Persistenz-Subsystem
com.sssw.fw.resource	Meldungen im Zusammenhang mit dem Framework-Ressourcen-Subsystem
com.sssw.fw.security	Meldungen im Zusammenhang mit dem Framework-Sicherheits-Subsystem
com.sssw.fw.server	Meldungen im Zusammenhang mit dem Framework-Server-Subsystem
com.sssw.fw.servlet	Meldungen im Zusammenhang mit dem Framework-Servlet-Subsystem
com.sssw.fw.session	Meldungen im Zusammenhang mit dem Framework-Sitzungs-Subsystem
com.sssw.fw.usermgr	Meldungen im Zusammenhang mit dem Framework-Benutzer-Subsystem
com.sssw.fw.util	Meldungen im Zusammenhang mit dem Framework-Dienstprogramm-Subsystem
com.sssw.portal.manager	Meldungen im Zusammenhang mit dem Portal Manager
com.sssw.portal.persist	Meldungen im Zusammenhang mit der Portal-Persistenz

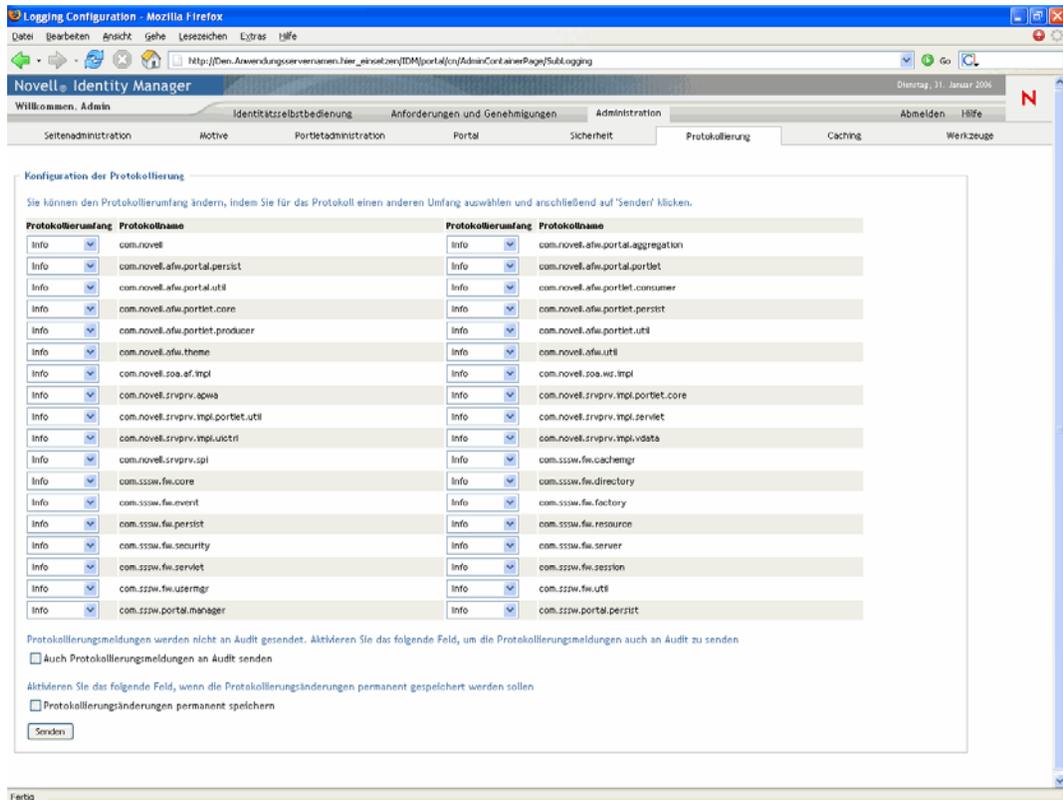
Beachten Sie, dass die Protokolle der Benutzeranwendung eine hierarchische Struktur aufweisen. So ist beispielsweise „com.novell“ den darunter befindlichen Protokollen übergeordnet. Jedes neue Protokoll erbt seine Eigenschaften.

## 12.3 Ändern des Protokollierumfangs

Sie können die Menge der Informationen, die in ein Protokoll geschrieben wird, mithilfe des zugehörigen Protokollierumfangs anpassen. Standardmäßig sind alle Protokolle auf *Info* eingestellt, wobei es sich um einen mittleren Umfang handelt.

So ändern Sie den Protokollierumfang:

- 1 Wechseln Sie zur Seite *Protokollierung*:



- 2 Wählen Sie im oberen Teil der Seite *ein Protokoll aus*, dessen Umfang Sie ändern möchten.
- 3 Wählen Sie in der Dropdown-Liste eine der folgenden Umfänge *auszuwählen*:

Umfang	Beschreibung
Gravierend	<b>Wenig Details:</b> Im Protokoll werden gravierende Fehler vermerkt.
Fehler	Zusätzlich zu den oben genannten Daten werden Fehler in das Protokoll aufgenommen.
Warnen	Zusätzlich zu den oben genannten Daten werden Warnungen in das Protokoll aufgenommen.
Info	Zusätzlich zu den oben genannten Daten werden Informationsmeldungen in das Protokoll aufgenommen.

Umfang	Beschreibung
Debug	Zusätzlich zu den oben genannten Daten werden Informationen zur Fehlersuche in das Protokoll aufgenommen.
Trace	<b>Viele Details:</b> Zusätzlich zu den oben genannten Daten werden Tracing-Informationen in das Protokoll aufgenommen

4 Wiederholen Sie bei Bedarf **Schritt 2** und **Schritt 3** für weitere Protokolle.

5 Klicken Sie auf *Senden*.

## 12.4 Senden von Protokollmeldungen an Novell Audit

Auf der Seite „Protokollierung“ können Sie festlegen, ob die Identity Manager-Benutzeranwendung Ereignismeldungen an Novell Audit sendet. Die Option für die Novell Audit-Protokollierung ist standardmäßig deaktiviert, wenn Sie sie nicht bei der Installation der Benutzeranwendung aktivieren.

So aktivieren bzw. deaktivieren Sie die Novell Audit-Protokollierung:

1 Wechseln Sie zur Seite *Protokollierung*.

2 *Aktivieren bzw. deaktivieren* Sie entsprechend Ihren Anforderungen die folgende Einstellung:

`Auch Protokollierungsmeldungen an Audit senden`

3 Klicken Sie auf *Senden*.

## 12.5 Dauerhafte Übernahme von Protokolleinstellungen

Standardmäßig bleiben die von Ihnen auf der Seite „Protokollierung“ vorgenommenen Änderungen bis zum nächsten Anwendungsserver-Neustart bzw. bis zur erneuten Implementierung der Benutzeranwendung gültig. Anschließend werden die Protokolleinstellungen auf ihre Standardwerte zurückgesetzt.

Auf der Seite „Protokollierung“ haben Sie jedoch die Möglichkeit, Ihre Änderungen dauerhaft zu speichern. Wenn Sie diese Funktion aktivieren, werden die Werte für die Protokolleinstellungen in einer *Konfigurationsdatei für die Protokollierung* auf dem Anwendungsserver gespeichert, auf dem die Identity Manager-Benutzeranwendung implementiert ist. Zum Beispiel:

`jboss/server/IDM/conf/extendlogging.xml`

So aktivieren bzw. deaktivieren Sie die Persistenz von Einstellungen:

1 Wechseln Sie zur Seite *Protokollierung*.

2 *Aktivieren bzw. deaktivieren* Sie entsprechend Ihren Anforderungen die folgende Einstellung:

`Protokollierungsänderungen permanent speichern`

**3** Klicken Sie auf *Senden*.

In diesem Kapitel erfahren Sie, wie Sie die Seite *Caching* der Registerkarte *Administration* der Benutzeroberfläche von Identity Manager verwenden. Es werden folgende Themen erläutert:

- [Abschnitt 13.1, „Allgemeines zur Cache-Konfiguration“](#), auf Seite 219
- [Abschnitt 13.2, „Leeren von Caches“](#), auf Seite 219
- [Abschnitt 13.3, „Konfiguration von Cache-Einstellungen“](#), auf Seite 222

Allgemeine Informationen zum Zugriff auf die und zum Arbeiten mit der Registerkarte „Administration“ finden Sie in [Kapitel 6, „Verwendung der Registerkarte „Administration““](#), auf Seite 131.

## 13.1 Allgemeines zur Cache-Konfiguration

Auf der Seite „Caching“ können Sie verschiedene *Cache-Speicher* verwalten, die von der Identity Manager-Benutzeranwendung verwendet werden. Die Benutzeranwendung nutzt diese Caches zum Speichern wieder verwendbarer, temporärer Daten auf dem Anwendungsserver, wodurch sich die Leistung optimieren lässt.

Sie haben die Möglichkeit, die Cache-Speicher bei Bedarf zu beeinflussen, indem Sie sie *leeren* und *deren Konfigurationseinstellungen ändern*.

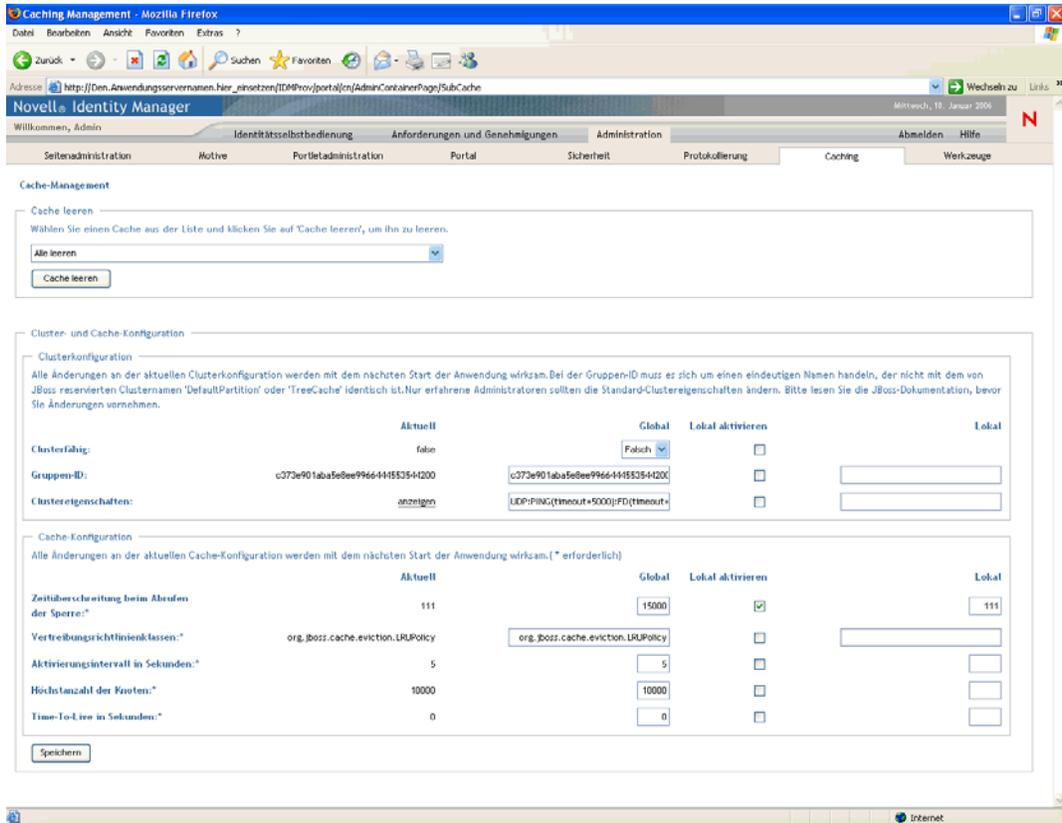
## 13.2 Leeren von Caches

Die Cache-Speicher sind entsprechend den *Subsystemen* benannt, von denen sie in der Identity Manager-Benutzeranwendung genutzt werden. Normalerweise ist es nicht erforderlich, sie manuell zu leeren, weil dies automatisch von der Benutzeranwendung auf der Grundlage der Nutzungshäufigkeit der enthaltenen Daten bzw. bei der Änderung von Quelldaten vorgenommen

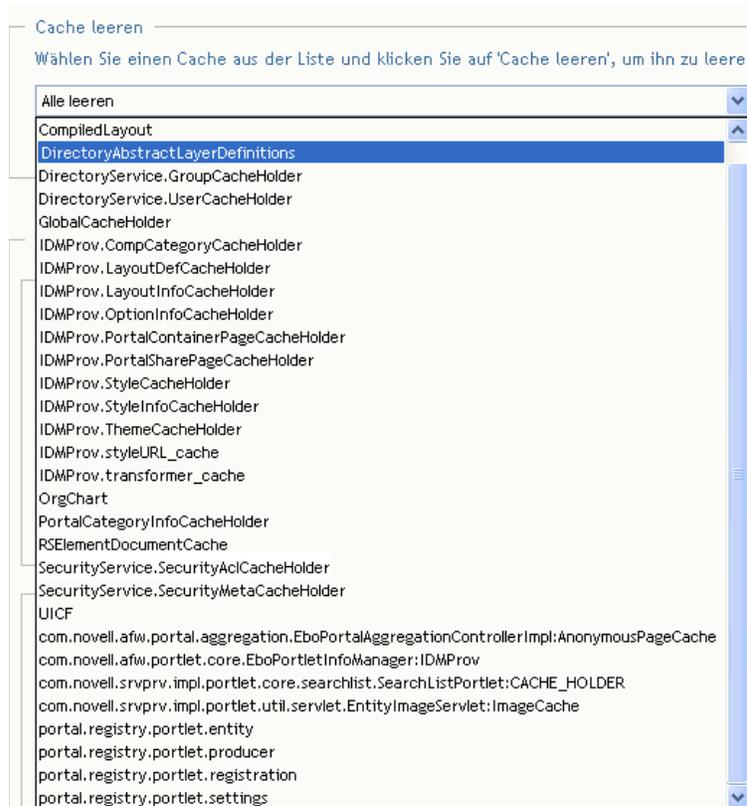
wird. Wenn es aus besonderen Gründen erforderlich ist, können Sie jedoch ausgewählte oder alle Caches *manuell leeren*.

So leeren Sie Caches:

### 1 Wechseln Sie zur Seite *Caching*:



- 2 Wählen Sie im Abschnitt *Cache leeren* auf dieser Seite in der Dropdown-Liste einen zu leerenden Cache-Speicher aus (oder wählen Sie *Alle leeren*):



Beachten Sie, dass die Liste der verfügbaren Cache-Speicher *dynamisch* ist. Sie ändert sich also abhängig von den gerade zwischengespeicherten Daten.

- 3 Klicken Sie auf die Schaltfläche *Cache leeren*.

## 13.2.1 Leeren des Caches der Verzeichnisabstraktionsschicht

Auch die *Verzeichnisabstraktionsschicht* der Benutzeranwendung verfügt über einen Cache-Speicher. Der Cache *DirectoryAbstractLayerDefinitions* speichert die Definitionen der Abstraktionsschicht auf dem Anwendungsserver, um die Leistung für alle Datenmodelloperationen zu optimieren.

In der Regel sorgt die Benutzeranwendung automatisch für die Synchronisierung des Caches *DirectoryAbstractLayerDefinitions* mit den im Identitätsdepot gespeicherten Abstraktionsschichtdefinitionen. Bei Bedarf können Sie den Cache *DirectoryAbstractLayerDefinitions* jedoch auch manuell leeren (wie oben beschrieben), um zu erzwingen, dass die neuesten Definitionen aus dem Identitätsdepot geladen werden.

Weitere Informationen zur Verzeichnisabstraktionsschicht der Benutzeranwendung finden Sie in [Kapitel 4, „Konfigurieren der Verzeichnisabstraktionsschicht“](#), auf Seite 75.

## 13.2.2 Leeren von Caches in einem Cluster

Das Leeren von Caches wird sowohl in geclusterten als auch in nicht geclusterten Anwendungsserver-Umgebungen unterstützt. Wenn Ihr Anwendungsserver Teil eines Clusters ist und Sie einen Cache-Speicher manuell leeren, wird dieser Cache automatisch *auf allen Servern* im Cluster geleert.

## 13.3 Konfiguration von Cache-Einstellungen

Auf der Seite „Caching“ können Sie Cache-Konfigurationseinstellungen für *geclusterte oder nicht geclusterte* Anwendungsserver-Umgebungen anzeigen und ändern. Ihre Änderungen werden unmittelbar gespeichert, werden jedoch erst beim nächsten *Neustart der Benutzeranwendung* wirksam.

---

**Tipp:** Führen Sie zum Neustarten der Benutzeranwendung einen der folgenden Schritte aus: Starten Sie den Anwendungsserver neu, implementieren Sie die Anwendung erneut (falls die WAR-Datei geändert wurde) oder erzwingen Sie einen Neustart der Anwendung (wie in der Dokumentation zu Ihrem Anwendungsserver beschrieben).

---

Zum Konfigurieren der Cache-Einstellungen müssen Sie sich mit Folgendem auskennen:

- [Abschnitt 13.3.1, „Wie das Caching implementiert ist“](#), auf Seite 222
- [Abschnitt 13.3.2, „Wie Cache-Einstellungen gespeichert werden“](#), auf Seite 222
- [Abschnitt 13.3.3, „Wie Cache-Einstellungen angezeigt werden“](#), auf Seite 224
- [Abschnitt 13.3.4, „Grundlegende Cache-Einstellungen“](#), auf Seite 224
- [Abschnitt 13.3.5, „Cache-Einstellungen für Cluster“](#), auf Seite 226

### 13.3.1 Wie das Caching implementiert ist

In der Identity Manager-Benutzeranwendung ist das Caching per *JBoss Cache* implementiert. JBoss Cache ist eine Open-Source-Caching-Architektur, die mit JBoss Application Server ausgeliefert wird, jedoch auch auf anderen Anwendungsservern ausgeführt werden kann.

Weitere Informationen zu JBoss Cache finden Sie unter [www.jboss.org/products/jboss-cache](http://www.jboss.org/products/jboss-cache) (<http://www.jboss.org/products/jboss-cache>).

### 13.3.2 Wie Cache-Einstellungen gespeichert werden

Zum Konfigurieren des Cache-Speichers stehen Ihnen *zwei Ebenen von Einstellungen* zur Verfügung. Diese können Sie beliebig kombinieren, um das Caching-Verhalten der Identity Manager-Benutzeranwendung genau festzulegen.

Ebene	Beschreibung
Globale Einstellungen	<p>Globale Einstellungen werden <b>an einem zentralen Ort</b> (dem Identitätsdepot) gespeichert, damit mehrere Anwendungsserver mit denselben Einstellungswerten arbeiten können. Bei geclusterten Anwendungsservern werden beispielsweise in der Regel globale Einstellungen für die Werte der Cluster-Konfiguration verwendet.</p> <p>Um die <b>globalen Einstellungen</b> in Ihrem Identitätsdepot zu finden, suchen Sie das folgende Objekt unterhalb des Treibers der Identity Manager-Benutzeranwendung:</p> <pre data-bbox="516 600 1008 621">configuration.AppDefs.AppConfig</pre> <p>Zum Beispiel:</p> <pre data-bbox="516 737 1281 789">configuration.AppDefs.AppConfig.MeinBenutzeranwendungstreiber.MeinTreiberSatz.MeineOrg</pre> <p>Das Attribut <b>XmlData</b> des Konfigurationsobjekts enthält die globalen Einstellungsdaten.</p>
Lokale Einstellungen	<p>Lokale Einstellungen werden <b>separat auf jedem einzelnen Anwendungsserver gespeichert</b>, sodass ein einzelner Server den Wert einer oder mehrerer globaler Einstellungen <b>außer Kraft setzen</b> kann. Beispielsweise kann es sinnvoll sein, eine lokale Einstellung festzulegen, um einen Anwendungsserver aus dem in den globalen Einstellungen angegebenen Cluster zu entfernen oder um einen Server einem anderen Cluster zuzuweisen.</p> <p>Um die <b>lokalen Einstellungen</b> auf Ihrem Anwendungsserver zu finden, Suchen Sie nach der folgenden Datei im conf-Verzeichnis Ihrer JBoss-Serverkonfiguration:</p> <pre data-bbox="516 1266 976 1287">sys-configuration-xmldata.xml</pre> <p>Zum Beispiel:</p> <pre data-bbox="516 1402 1149 1455">jboss/server/IDM/conf/sys-configuration-xmldata.xml</pre> <p>Wenn für Ihren Server lokale Einstellungen vorhanden sind, befinden sich die entsprechenden Daten in dieser Datei. (Wurden keine lokalen Einstellungen festgelegt, ist die Datei nicht vorhanden.)</p>

Sie können sich globale Einstellungen als *Standardwerte* für jeden Anwendungsserver vorstellen, der eine bestimmte Instanz des Benutzeranwendungstreibers nutzt. Wenn Sie eine globale Einstellung ändern, *betrifft dies alle Server* (beim nächsten Neustart der Benutzeranwendung) mit Ausnahme der Server, für die eine lokale Einstellung festgelegt ist, die Vorrang vor der globalen hat.

### 13.3.3 Wie Cache-Einstellungen angezeigt werden

Auf der Seite „Caching“ werden die *aktuellen Cache-Einstellungen* (Einstellungen beim letzten Neustart der Benutzeranwendung) angezeigt. Außerdem werden die zugehörigen *globalen und lokalen Werte* dieser Einstellungen angezeigt, und Sie haben die Möglichkeit, diese zu *ändern* (zur Verwendung beim nächsten Neustart der Benutzeranwendung).

Cluster- und Cache-Konfiguration

Clusterkonfiguration

Alle Änderungen an der aktuellen Clusterkonfiguration werden mit dem nächsten Start der Anwendung wirksam. Bei der Gruppen-ID muss es sich um einen eindeutigen Namen handeln, der nicht mit dem von JBoss reservierten Clusternamen 'DefaultPartition' oder 'TreeCache' identisch ist. Nur erfahrene Administratoren sollten die Standard-Clustereigenschaften ändern. Bitte lesen Sie die JBoss-Dokumentation, bevor Sie Änderungen vornehmen.

	Aktuell	Global	Lokal aktivieren	Lokal
Clusterfähig:	false	Falsch	<input type="checkbox"/>	
Gruppen-ID:	c373e901aba5e8ee9966444553544200	c373e901aba5e8ee9966444553544200	<input type="checkbox"/>	<input type="text"/>
Clustereigenschaften:	anzeigen	UDP:PING(timeout=5000);FD(timeout=	<input type="checkbox"/>	<input type="text"/>

Cache-Konfiguration

Alle Änderungen an der aktuellen Cache-Konfiguration werden mit dem nächsten Start der Anwendung wirksam. (\* erforderlich)

	Aktuell	Global	Lokal aktivieren	Lokal
Zeitüberschreitung beim Abrufen der Sperre:*	111	15000	<input checked="" type="checkbox"/>	111
Verteilungsrichtlinienklassen:*	org.jboss.cache.eviction.LRUPolicy	org.jboss.cache.eviction.LRUPolicy	<input type="checkbox"/>	<input type="text"/>
Aktivierungsintervall in Sekunden:*	5	5	<input type="checkbox"/>	<input type="text"/>
Höchstanzahl der Knoten:*	10000	10000	<input type="checkbox"/>	<input type="text"/>
Time-To-Live in Sekunden:*	0	0	<input type="checkbox"/>	<input type="text"/>

Beachten Sie, dass für die globalen Einstellungen immer Werte vorhanden sind. Die lokalen Einstellungen sind optional.

### 13.3.4 Grundlegende Cache-Einstellungen

Diese Cache-Einstellungen betreffen sowohl geclusterte als auch nicht geclusterte Anwendungsserver.

So konfigurieren Sie grundlegende Cache-Einstellungen:

- 1 Wechseln Sie zur Seite *Caching*.
- 2 Geben Sie im Abschnitt *Cache-Konfiguration* dieser Seite die gewünschten *globalen oder lokalen Werte* ein:

Einstellung	Vorgehensweise
Zeitüberschreitung beim Abrufen der Sperre	Geben Sie das <b>Zeitintervall (in Millisekunden)</b> an, das der Cache-Speicher abwarten soll, bis er eine Sperre für ein Objekt erhält. Es kann sinnvoll sein, diesen Wert zu erhöhen, wenn das Anwendungsprotokoll der Benutzeranwendung zahlreiche Ausnahmen wegen Sperren-Zeitüberschreitungen aufweist. Der Standardwert ist 15000 ms.

Einstellung	Vorgehensweise
Vertreibungsrichtlinienklassen	<p>Geben Sie den <b>Klassennamen</b> für die Cache-Vertreibungsrichtlinie an, die Sie verwenden möchten. Standardmäßig wird die LRU-Vertreibungsrichtlinie von JBoss Cache verwendet:</p> <pre>org.jboss.cache.eviction.LRUPolicy</pre> <p>Bei Bedarf können Sie diese in eine andere von JBoss Cache unterstützte Vertreibungsrichtlinie ändern.</p> <p>Weitere Informationen zu unterstützten Vertreibungsrichtlinien erhalten Sie unter <a href="http://www.jboss.org/products/jboss-cache">www.jboss.org/products/jboss-cache</a> (<a href="http://www.jboss.org/products/jboss-cache">http://www.jboss.org/products/jboss-cache</a>).</p>
Aktivierungsintervall in Sekunden	<p>Geben Sie das <b>Zeitintervall (in Sekunden)</b> an, nach der die Vertreibungsrichtlinie aktiv wird und Folgendes ausführt:</p> <ul style="list-style-type: none"> <li>• Die Ereignisse der vertriebenen Knoten verarbeiten</li> <li>• Die Größenbeschränkungs- und abgelaufenen Knoten bereinigen</li> </ul>
Höchstanzahl der Knoten	<p>Geben Sie die <b>maximal Knotenanzahl</b> an, die im Cache zugelassen ist. Bei keiner Beschränkung geben Sie Folgendes ein:</p> <p>0</p>
Time-To-Live in Sekunden	<p>Geben Sie die <b>Leerlaufzeit (in Sekunden)</b> an, nach der der Knoten entfernt wird. Bei keiner Beschränkung geben Sie Folgendes ein:</p> <p>0</p>

Diese Einstellungen sind *erforderlich*, es muss also für jede einzelne Einstellung ein globaler Wert und optional zusätzlich ein lokaler Wert vorhanden sein.

Wenn Sie den globalen Wert einer Einstellung durch einen lokalen Wert *außer Kraft setzen* möchten, aktivieren Sie für die entsprechende Einstellung das Kontrollkästchen *Lokal aktivieren*. Geben Sie anschließend den lokalen Wert an. (Stellen Sie sicher, dass alle lokalen Werte *gültig* sind. Anderenfalls können Sie Ihre Änderungen nicht speichern.)

**Hinweis:** Bei den Einstellungen, bei denen die Option „Lokal aktivieren“ nicht ausgewählt ist, werden ggf. beim Speichern vorhandene lokale Werte gelöscht.

- 3 Klicken Sie auf *Speichern*.
- 4 Wenn Sie die gewünschten Werte gespeichert haben und diese wirksam werden sollen, *starten Sie die Benutzeranwendung* auf den entsprechenden Anwendungsservern neu.

## 13.3.5 Cache-Einstellungen für Cluster

In diesem Abschnitt wird erläutert, wie Sie die Caching-Funktion konfigurieren, wenn Sie die Identity Manager-Benutzeranwendung über ein Anwendungsserver-Cluster verteilt ausführen. Sie sollten sich mit Folgendem auskennen:

- [Abschnitt „Wie das Clustering implementiert ist“](#), auf Seite 226
- [„Wie das Caching mit einem Cluster funktioniert“](#) auf Seite 226
- [„Vorbereitungen für die Verwendung eines Clusters“](#) auf Seite 226
- [„Konfiguration von Cache-Einstellungen für Cluster“](#) auf Seite 227

### Wie das Clustering implementiert ist

In der Identity Manager-Benutzeranwendung ist die Cluster-Unterstützung für das Caching per *JGroups* implementiert. *JGroups* ist eine Open-Source-Clustering-Architektur, die mit JBoss Application Server ausgeliefert wird, jedoch auch auf anderen Anwendungsservern ausgeführt werden kann.

Das *Cluster der Benutzeranwendung* besteht aus Knoten in einem Netzwerk, die *JGroups* ausführen und die eine gemeinsame *Gruppen-ID* haben. Standardmäßig ist die für das Cluster der Benutzeranwendung bereitgestellte Gruppen-ID eine UUID, die wie folgt aussieht:

```
c373e901aba5e8ee9966444553544200
```

Die UUID gewährleistet die Eindeutigkeit, damit kein Konflikt zwischen der Gruppen-ID des Clusters der Benutzeranwendung und den Gruppen-IDs anderer Cluster in Ihrer Umgebung auftritt. Beispielsweise nutzt der JBoss Application Server selbst zwei *JGroups*-Cluster, für die er die Gruppen-IDs *DefaultPartition* und *TreeCache* reserviert.

Weitere Informationen zu *JGroups* finden Sie in [www.jboss.org/products/jgroups](http://www.jboss.org/products/jgroups) (<http://www.jboss.org/products/jgroups>).

### Wie das Caching mit einem Cluster funktioniert

Wenn Sie die Benutzeranwendung starten, legen die Cache-Konfigurationseinstellungen der Anwendung fest, ob diese an einem Cluster teilnehmen und Cache-Änderungen auf den anderen Knoten in diesem Cluster replizieren soll. Wenn Clustering aktiviert ist, nimmt die Benutzeranwendung diese Replizierung vor, indem sie bei Änderungen *Cache-Eintrag-Invalidierungsmeldungen* an jeden Knoten sendet.

### Vorbereitungen für die Verwendung eines Clusters

Für die Verwendung von Caching in einem Cluster sind zwei vorbereitende Schritte erforderlich:

#### 1 *Einrichtung des JGroups-Clusters*

Dies umfasst die Installation des JBoss Application Server mit der Vorgabe, dass die Konfiguration *all* verwendet werden soll, und die anschließende Verteilung der Identity Manager-Benutzeranwendung (*IDM.war*) an jeden Server im Cluster. Üblicherweise wird sie im Verzeichnis *farm* abgelegt.

#### 2 *Aktivierung der Verwendung dieses Clusters* in den Cache-Konfigurationseinstellungen der Benutzeranwendung.

Weitere Informationen hierzu finden Sie in „[Konfiguration von Cache-Einstellungen für Cluster](#)“ auf Seite 227 (unten).

## Konfiguration von Cache-Einstellungen für Cluster

Sobald Ihr Cluster einsatzbereit ist, können Sie Einstellungen für die Unterstützung von Caching in diesem Cluster festlegen.

So konfigurieren Sie Cache-Einstellungen für Cluster:

- 1 Wechseln Sie zur Seite *Caching*.
- 2 Geben Sie im Abschnitt *Clusterkonfiguration* dieser Seite die gewünschten *globalen oder lokalen Werte* für die folgenden Einstellungen ein:

Einstellung	Vorgehensweise
Clusterfähig	Wählen Sie <b>Wahr</b> , um Cache-Änderungen auf den anderen Knoten des Clusters mit derselben Gruppen-ID zu replizieren. Wenn Sie die Cluster-Funktionalität nicht nutzen möchten, wählen Sie <b>Falsch</b> .
Gruppen-ID	<p>Geben Sie die Gruppen-ID des JGroups-Clusters an, das verwendet werden soll. Es ist <b>nur dann erforderlich, die standardmäßige Gruppen-ID zu ändern</b>, die für das Cluster der Benutzeranwendung vorgegeben ist, <b>wenn Sie mit einem anderen Cluster arbeiten möchten</b>.</p> <p>Denken Sie daran, dass die folgenden Gruppen-IDs für die Verwendung durch den JBoss Application Server reserviert sind: „DefaultPartition“ und „TreeCache“.</p> <hr/> <p><b>Tipp:</b> Damit die Gruppen-ID in Protokollierungsmeldungen angegeben wird, müssen Sie sicherstellen, dass der Umfang für das Caching-Protokoll (com.sssw.fw.cachemgr) auf „Info“ oder höher eingestellt ist.</p>
Clustereigenschaften	<p>Geben Sie den JGroups-<b>Protokoll-Stack</b> für das durch die Gruppen-ID festgelegte Cluster an. Beachten Sie, dass diese Einstellung nur für <b>erfahrene Administratoren</b> gedacht ist, die ggf. die Cluster-Eigenschaften anpassen müssen. Anderenfalls sollten Sie den standardmäßigen Protokoll-Stack nicht ändern.</p> <p>Klicken Sie zum Anzeigen der aktuellen Cluster-Eigenschaften auf <b>Anzeigen</b>.</p> <p>Details zum JGroups-Protokoll-Stack finden Sie unter <a href="http://www.jboss.org/wiki/Wiki.jsp?page=JGroups">www.jboss.org/wiki/Wiki.jsp?page=JGroups</a> (<a href="http://www.jboss.org/wiki/Wiki.jsp?page=JGroups">http://www.jboss.org/wiki/Wiki.jsp?page=JGroups</a>).</p>

Wenn Sie den globalen Wert einer Einstellung durch einen lokalen Wert *außer Kraft setzen* möchten, aktivieren Sie für die entsprechende Einstellung das Kontrollkästchen *Lokal aktivieren*. Geben Sie anschließend den lokalen Wert an.

**Hinweis:** Bei den Einstellungen, bei denen die Option „Lokal aktivieren“ nicht ausgewählt ist, werden ggf. beim Speichern vorhandene lokale Werte gelöscht.

Stellen Sie sicher, dass *alle Knoten* in Ihrem Cluster *dieselbe* Gruppen-ID und dieselben Clustereigenschaften aufweisen. (Sie können diese Einstellungen für einen bestimmten Knoten

anzeigen, indem Sie auf diesem Knoten auf die Benutzeroberfläche von Identity Manager zugreifen - wechseln Sie hierzu zur URL der Benutzeroberfläche auf diesem Server und dort die Seite „Caching“ anzeigen.)

- 3** Klicken Sie auf *Speichern*.
- 4** Wenn Sie die gewünschten Werte gespeichert haben und diese wirksam werden sollen, *starten Sie die Benutzeranwendung* auf den entsprechenden Anwendungsservern neu.

# Werkzeuge zum Exportieren und Importieren von Portaldaten

# 14

In diesem Kapitel erfahren Sie, wie Sie die Seite *Werkzeuge* der Registerkarte *Administration* der Benutzeroberfläche von Identity Manager verwenden. Es werden folgende Themen erläutert:

- [Abschnitt 14.1, „Allgemeines zum Exportieren und Importieren von Portaldaten“](#), auf Seite 229
- [Abschnitt 14.2, „Exportieren von Portaldaten“](#), auf Seite 231
- [Abschnitt 14.3, „Importieren von Portaldaten“](#), auf Seite 232

Allgemeine Informationen zum Zugriff auf die und zum Arbeiten mit der Registerkarte „Administration“ finden Sie in [Kapitel 6, „Verwendung der Registerkarte „Administration““](#), auf Seite 131.

## 14.1 Allgemeines zum Exportieren und Importieren von Portaldaten

Auf der Seite „Werkzeuge“ können Sie in der Identity Manager-Benutzeranwendung verwendete Portalinhalte (Seiten und Portlets) *exportieren oder importieren*. Diese Inhalte werden auch als *Stand der Portalkonfiguration* bezeichnet und umfassen Folgendes:

- Container und freigegebene Seiten (einschließlich den jeder Seite zugeordneten Portlets und den Standardeinstellungen und Einstellungen der einzelnen Portlets)
- Portlet-Registrierungen

Mit den Werkzeugen zum Exportieren und Importieren können Sie den Stand der Portalkonfiguration bei Bedarf von einem Portal (Benutzeranwendung) zu einem anderen verschieben. So funktionieren diese Werkzeuge:

Werkzeug	Funktionsweise
Portaldatenexport	Es werden XML-Beschreibungen eines Satzes ausgewählter Container und freigegebener Seiten sowie Portlets erstellt. Die XML-Dateien werden in einer <b>Portaldatenexport-ZIP-Datei</b> gespeichert, die vom Portaldatenimport-Werkzeug eingelesen werden kann.
Portaldatenimport	Diese Funktion kann Portaldatenexport-ZIP-Dateien einlesen. Sie verwendet die Portaldatenexport-ZIP-Datei zum Generieren von Container- und freigegebenen Seiten sowie Portlets in einem Portal (Benutzeranwendung).

### 14.1.1 Verwendungsmöglichkeiten

Mithilfe der Werkzeuge zum Portaldatenexport bzw. -import können Sie folgende Aktionen durchführen:

- Portalkonfiguration aus einer Testumgebung (Quellumgebung) in eine Produktionsumgebung (Zielumgebung) *verschieben*

- Stand der Konfiguration eines Portals inkrementell *aktualisieren*
- Portal *klonen*
- Optional den Stand der Konfiguration des Zielportals *überschreiben*

## 14.1.2 Anforderungen

Damit Sie die Export- und Importwerkzeuge für Portaldata verwenden können, stellen Sie sicher, dass die Identity Manager-Benutzeranwendung (Portal) auf Ihren Quell- und Ziel-Anwendungsservern *implementiert wurde und ausgeführt wird*.

Es ist *nicht erforderlich*, dass Ihre Quell- und Zielservers auf dasselbe *Identitätsdepot* zugreifen. Bei Bedarf können sie unterschiedliche nutzen. Die *Benutzer, Gruppen und Container* in diesen Identitätsdepots *müssen nicht* dieselben sein.

## 14.1.3 Einschränkungen

Zu folgenden Zwecken können Sie die Export- und Importwerkzeuge für Portaldata *nicht* verwenden:

- Den Stand der Portalkonfiguration eines Servers exportieren oder importieren, der gerade Benutzeranforderungen verarbeitet
- Portalklassen und -ressourcen exportieren oder importieren
- Portletklassen und -ressourcen exportieren oder importieren
- Identitäts- und Bereitstellungsdaten eines Portals exportieren oder importieren
- Verwaltungseinstellungen (außer für Seiten und Portlets) exportieren oder importieren
- Migration des Stands der Konfiguration einer älteren Portalversion auf eine neuere Version durchführen (die Portale müssen dieselbe Version aufweisen)

## 14.1.4 Schritte

So exportieren und importieren Sie Portaldata:

- 1** Wenn Sie eine inkrementelle Aktualisierung durchführen, *sichern* Sie das Zielportal.
- 2** *Exportieren* Sie die Portaldata mithilfe des Werkzeugs für den Portaldataexport vom Quellportal.  
Weitere Informationen hierzu finden Sie in [Abschnitt 14.2, „Exportieren von Portaldata“](#), auf [Seite 231](#).
- 3** *Importieren* Sie die Portaldata mithilfe des Werkzeugs für den Portaldataimport vom Zielportal.  
Weitere Informationen hierzu finden Sie in [Abschnitt 14.3, „Importieren von Portaldata“](#), auf [Seite 232](#).
- 4** *Testen* Sie das Zielportal, um sicherzustellen, dass Sie die gewünschten Daten importiert haben.

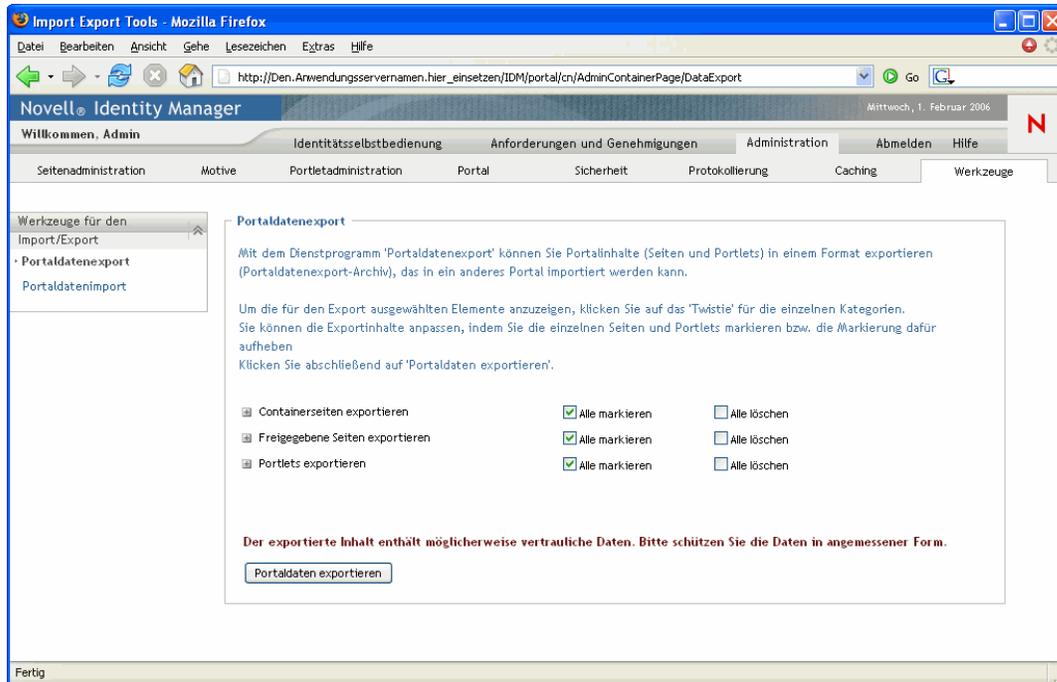
## 14.2 Exportieren von Portaldata

In diesem Abschnitt wird beschrieben, wie der Stand der Konfiguration eines Portals in eine Portaldataexport-ZIP-Datei exportiert wird.

So exportieren Sie Portaldata:

- 1 Wählen Sie im Navigationsmenü links auf der Seite „Werkzeuge“ die Option *Portaldataexport*.

Das Teilfenster „Portaldataexport“ wird eingeblendet:



- 2 Befolgen Sie die Anweisungen auf dem Bildschirm, um die zu exportierenden *Portalseiten und Portlets auszuwählen*.

---

**Hinweis:** Möglicherweise werden auch einige Portlets exportiert, die Sie nicht für den Export ausgewählt haben. Wenn Sie eine Seite exportieren, die ein Portlet enthält, das Portlet jedoch nicht für den Export ausgewählt ist, wird es trotzdem exportiert (um sicherzustellen, dass bei der exportierten Seite kein Laufzeitfehler auftritt).

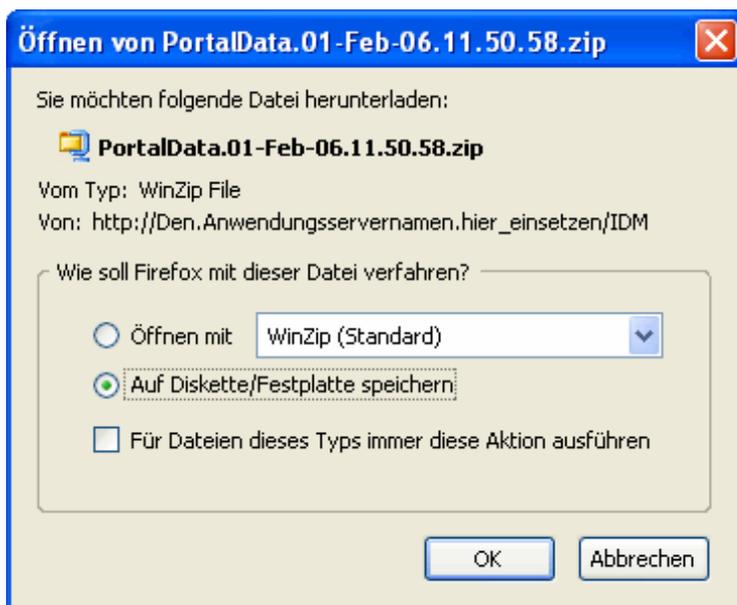
---

- 3 Wenn Sie Ihre Auswahl vorgenommen haben, klicken Sie auf die Schaltfläche *Portaldata exportieren*.

Es wird eine neue *Portaldataexport-ZIP-Datei* generiert. Diese hat einen vorgegebenen Namen, der das aktuelle Datum und die aktuelle Uhrzeit umfasst. Zum Beispiel:

PortalData.21-Oct-05.09.12.16.zip

Anschließend werden Sie dazu aufgefordert, diese ZIP-Datei lokal zu speichern (oder sie mit einem geeigneten Archivierungsprogramm zu öffnen). Zum Beispiel:



4 *Speichern* Sie die Portaldatenexport-ZIP-Datei am gewünschten Ort.

## 14.3 Importieren von Portaldaten

In diesem Abschnitt wird beschrieben, wie Sie eine Portaldatenexport-ZIP-Datei in ein Portal importieren.

---

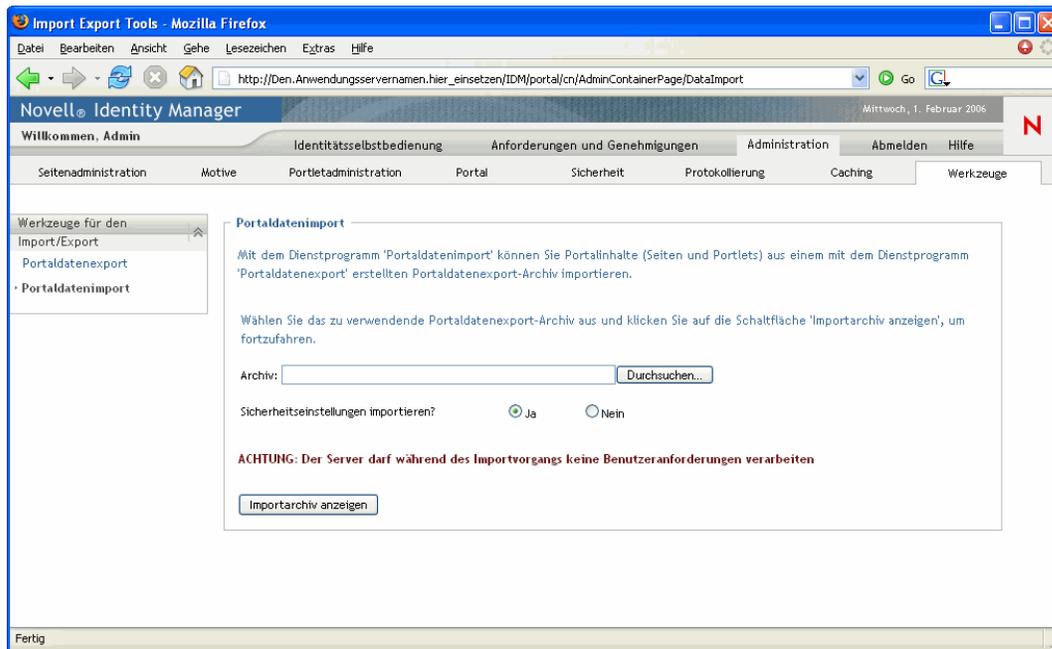
**Hinweis:** Denken Sie daran, dass der Ziel-Anwendungsserver während des Imports laufen muss, jedoch *keine Benutzeranforderungen verarbeiten darf*.

---

So importieren Sie Portaldaten:

- 1 Wählen Sie im Navigationsmenü links auf der Seite „Werkzeuge“ die Option *Portaldatenimport*.

Das Teilfenster „Portaldatenimport“ wird eingeblendet:

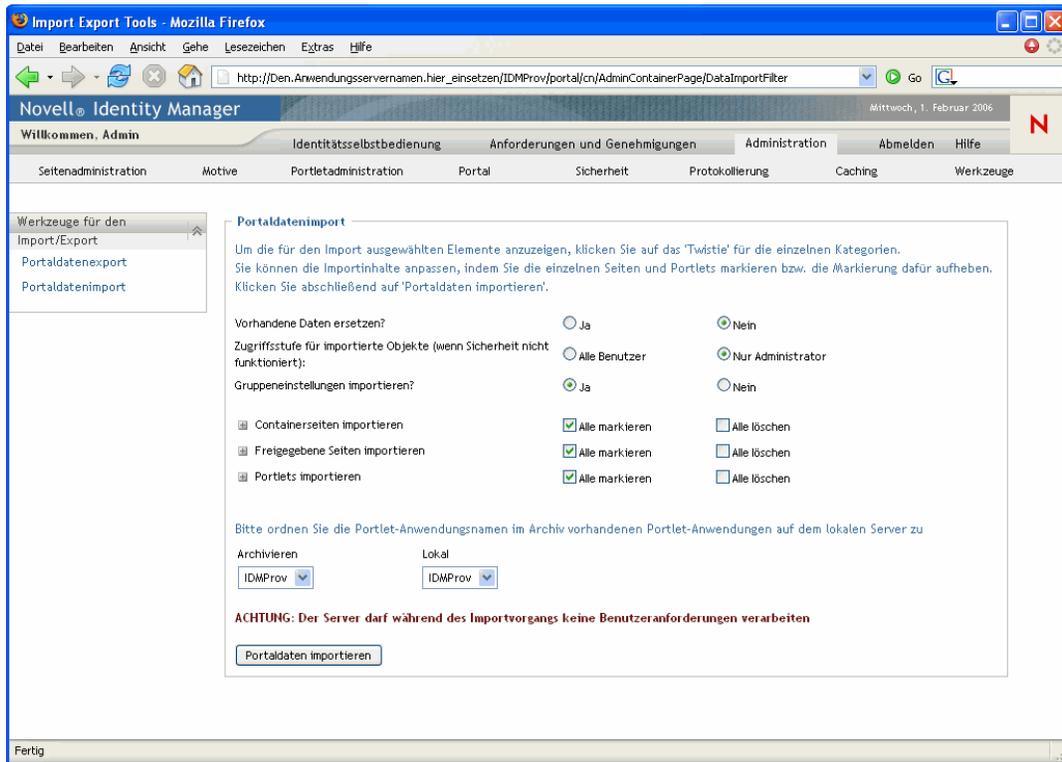


2 Geben Sie die folgenden *allgemeinen Importeinstellungen* an:

Einstellung	Vorgehensweise
Archiv	<p>Klicken Sie auf die Schaltfläche <b>Durchsuchen</b>, um die zu importierende <b>Portaldatenexport-ZIP-Datei</b> auszuwählen. Zum Beispiel:</p> <p style="text-align: center;">PortalData.21-Oct-05.09.12.16.zip</p>
Sicherheitseinstellungen importieren?	<p>Wählen Sie eine der folgenden Optionen aus:</p> <ul style="list-style-type: none"> <li>• <b>Ja</b>, wenn Sie die Berechtigungen importieren möchten, die in der Portaldatenexport-ZIP-Datei für den Zugriff auf Seiten und Portlets durch Benutzer, Gruppen und Container angegeben sind. Stellen Sie sicher, dass die entsprechenden Benutzer, Gruppen und Container im Identitätsdepot des Zielportals vorhanden sind. Berechtigungen für nicht vorhandene Elemente werden nicht importiert.</li> <li>• <b>Nein</b>, wenn Sie die Berechtigungen in der Portaldatenexport-ZIP-Datei nicht berücksichtigen möchten.</li> </ul>

3 Klicken Sie auf die Schaltfläche *Importarchiv anzeigen*.

Im Teilfenster werden daraufhin detailliertere Daten zur ausgewählten Portaldatenexport-ZIP-Datei sowie weitere Importoptionen angezeigt:



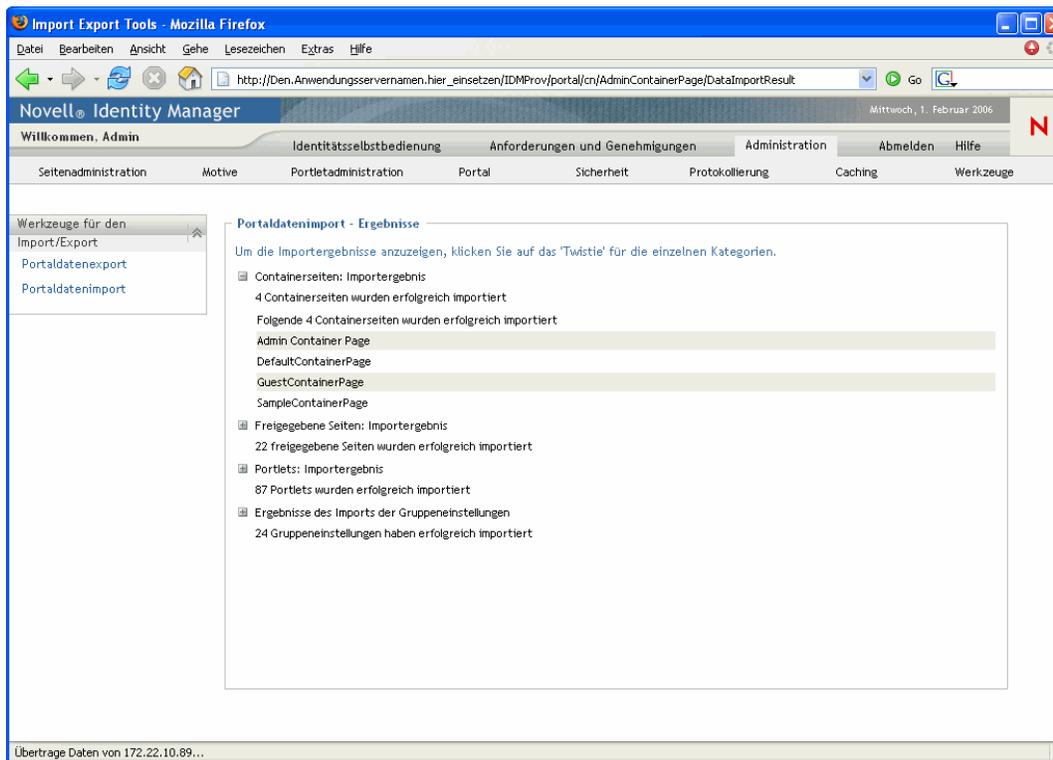
#### 4 Geben Sie die folgenden *detaillierten Importeinstellungen* an:

Einstellung	Vorgehensweise
Vorhandene Daten ersetzen?	<p>Wählen Sie eine der folgenden Optionen aus:</p> <ul style="list-style-type: none"> <li>• <b>Ja</b>, wenn Sie möchten, dass bereits im Zielportal vorhandene Seiten und Portlets mit entsprechenden Inhalten der Portaldatenexport-ZIP-Datei überschrieben werden. Enthält die Portaldatenexport-ZIP-Datei beispielsweise eine freigegebene Seite mit dem Namen „MeineSeite“ und enthält das Zielportal eine freigegebene Seite desselben Namens, wird die im Zielportal vorhandene Seite überschrieben.</li> <li>• <b>Nein</b>, wenn Sie nicht möchten, dass bereits vorhandene Seiten und Portlets importiert werden.</li> </ul>

Einstellung	Vorgehensweise
Zugriffsstufe für importierte Objekte	<p>Wählen Sie eine der folgenden Optionen aus:</p> <ul style="list-style-type: none"> <li>• <b>Alle Benutzer</b> für uneingeschränkten Zugriff auf importierte Seiten und Portlets.</li> <li>• <b>Nur Administrator</b> für eingeschränkten Zugriff auf importierte Seiten und Portlets.</li> </ul> <p><b>Wenn Sie sich für den Import von Sicherheitseinstellungen entscheiden</b>, wird diese Zugriffsebene nur auf die importierten Seiten und Portlets angewendet, bei denen keine Sicherheitseinstellung importiert werden konnte (in der Regel, weil angegebene Benutzer, Gruppen oder Container nicht im Identitätsdepot des Zielportals vorhanden sind).</p> <p><b>Wenn Sie sich dafür entscheiden, keine Sicherheitseinstellungen zu importieren</b>, wird diese Zugriffsebene auf alle importierten Seiten und Portlets angewendet.</p>
Gruppeneinstellungen importieren?	<p>(Wenn Sie sich dafür entscheiden, Sicherheitseinstellungen zu importieren) Wählen Sie eine der folgenden Optionen aus:</p> <ul style="list-style-type: none"> <li>• <b>Ja</b>, wenn Sie die Zuweisungen für Standardcontainerseiten und standardmäßig freigegebene Seiten der Portaldatenexport-ZIP-Datei für Gruppen importieren möchten. Stellen Sie sicher, dass die entsprechenden Gruppen im Identitätsdepot des Zielportals vorhanden sind. Zuweisungen für fehlende Gruppen werden nicht importiert.</li> <li>• <b>Nein</b>, wenn Sie die Standard-Seitenzuweisungen der Portaldatenexport-ZIP-Datei für Gruppen nicht berücksichtigen möchten.</li> </ul>
Containerseiten importieren Freigegebene Seiten importieren Portlets importieren	<p>Befolgen Sie die Anweisungen auf dem Bildschirm, um <b>die Seiten und Portlets auszuwählen</b>, die Sie aus der Portaldatenexport-ZIP-Datei in das Zielportal importieren möchten.</p> <hr/> <p><b>Hinweis:</b> Möglicherweise werden auch einige Portlets importiert, die Sie nicht für den Import ausgewählt haben. Wenn Sie eine Seite importieren, die ein Portlet enthält, das Portlet jedoch nicht für den Import ausgewählt ist, wird es trotzdem importiert (um sicherzustellen, dass bei der importierten Seite kein Laufzeitfehler auftritt).</p> <hr/>
Bitte ordnen Sie die Portlet-Anwendungsnamen... Archiv/ Lokal	<p>Ordnen Sie über die Dropdown-Menüs <b>Archiv</b> und <b>Lokal</b> die Portlet-Anwendungsnamen im Archiv (Portaldatenexport-ZIP-Datei) vorhandenen Portlet-Anwendungen auf dem lokalen Anwendungsserver (Zielserver) zu.</p>

- 5** Wenn Sie alle Vorbereitungen für den Import abgeschlossen haben, klicken Sie auf die Schaltfläche *Portaldaten importieren*.

Sobald der Import abgeschlossen ist, wird das Teilfenster *Portaldatenimport - Ergebnisse* angezeigt:



Nicht erfolgreich importierte Daten werden rot dargestellt. Um *Import- oder Exportprobleme zu beheben*, überprüfen Sie die Systemkonsole oder die Protokolldatei Ihres Anwendungsservers (z. B. `jboss/server/IDM/log/server.log`) auf Meldungen des folgenden Benutzeranwendungs-Protokolls:

```
com.novell.afw.portal.util
```

# Portlet-Referenz

# IV

In diesen Kapiteln wird die Konfigurierung der Identitäts- und System-Portlets beschrieben, die in der Identity Manager-Benutzeroberfläche verwendet werden.

- [Kapitel 15, „Allgemeines zu Portlets“](#), auf Seite 239
- [Kapitel 16, „Das Portlet „Erstellen““](#), auf Seite 243
- [Kapitel 17, „Portlet „Detail““](#), auf Seite 249
- [Kapitel 18, „Portlet „Organigramm““](#), auf Seite 263
- [Kapitel 19, „Passwortverwaltungs-Portlet“](#), auf Seite 279
- [Kapitel 20, „Portlet „Suchliste““](#), auf Seite 293



In diesem Kapitel erhalten Sie Informationen zu den Portlets, die in der Identity Manager-Benutzeranwendung verwendet werden. Es werden folgende Themen erläutert:

- [Abschnitt 15.1, „Zubehör-Portlets“](#), auf Seite 239
- [Abschnitt 15.2, „Admin-Portlets“](#), auf Seite 239
- [Abschnitt 15.3, „Identitäts-Portlets“](#), auf Seite 240
- [Abschnitt 15.4, „Passwort-Portlets“](#), auf Seite 241
- [Abschnitt 15.5, „System-Portlets“](#), auf Seite 241

Weitere Informationen zur Verwaltung von Portlets finden Sie in [Kapitel 9, „Portletadministration“](#), auf Seite 181.

## 15.1 Zubehör-Portlets

Zubehör-Portlets bieten verschiedene Funktionen, um die Sie die Identity Manager-Benutzeranwendung erweitern können. Zubehör-Portlets stellen Email-, Dateisystem- und weitere Funktionen zur Verfügung. Weitere Informationen:

Portlet-Kategorie	Weitere Informationen
Email	Siehe Identity Manager Accessory Portlet Administration Guide (Identity Manager-Administrationshandbuch für Zubehör-Portlets)
Dateisystem	
Sonstige	

## 15.2 Admin-Portlets

Die Portlets der Administrator-Kategorie werden zur Steuerung des Layouts und des Inhalts der Benutzeroberfläche verwendet.

**Hinweis:** Es wird empfohlen, diese Portlets weder zu verwenden noch zu ändern. Sie bieten Framework-Services für die Benutzeranwendung.

Zu den Admin-Portlets zählen:

Portlet-Name	Beschreibung
Header-Portlet	Zeigt die Header-Informationen und die Registerkarten der obersten Ebene für die Benutzeroberfläche an.  Für dieses Portlet gibt es keine Standardeinstellungen.

Portlet-Name	Beschreibung
Navigation für die freigegebene Seite	<p>Zeigt ein Menü mit den freigegebenen Seiten der Identity Manager-Benutzeranwendung an.</p> <p>In den Standardeinstellungen ist definiert, welche Elemente angezeigt und wie diese dargestellt werden.</p> <p>Weitere Informationen hierzu finden Sie in <a href="#">Abschnitt 15.2.1, „Portlet „Navigation für die freigegebene Seite““</a>, auf Seite 240.</p>

## 15.2.1 Portlet „Navigation für die freigegebene Seite“

Das Portlet „Navigation für die freigegebene Seite“ generiert Links zu den freigegebenen Seiten der Identity Manager-Benutzeranwendung. Die Standardeinstellungen legen fest, welche Links zu freigegebenen Seiten angezeigt werden. Zu diesen Standardeinstellungen zählen:

Standardeinstellung	Erforderliche Angaben
sharedpages-sorting	Die Reihenfolge, in der freigegebene Seiten innerhalb einer Kategorie angezeigt werden: Aufsteigend/Absteigend.
sharedpages-sortmode	Wie die freigegebenen Seiten sortiert werden sollen: Alphabetisch oder nach Priorität.
sharedpages-category	<p>Geben Sie eine oder mehrere Kategorien der freigegebenen Seiten an.</p> <p>Der Name der Kategorie wird als Kopfzeile angezeigt und darunter befinden sich alle freigegebenen Seiten der entsprechenden Kategorie in Form von Links. Weist eine Kategorie keine freigegebenen Seiten auf, wird sie nicht angezeigt. Wenn die freigegebene Seite keiner Kategorie angehört, wird sie als nicht kategorisiert angezeigt.</p>
guest-category	Geben Sie eine Kategorie an, deren Portlets Sie auf der Portal-seite anzeigen möchten. Dabei muss es sich um eine bereits vorhandene Kategorie handeln und die Seiten dieser Kategorie dürfen in der ACL keine Leseinschränkung aufweisen.

## 15.3 Identitäts-Portlets

Die Identitäts-Portlets werden von der Registerkarte „Identitätsselbstbedienung“ der Identity Manager-Benutzeranwendung genutzt. Dazu gehören:

Portlet-Name	Beschreibung
Erstellen	<p>Bietet eine assistentengeführte Benutzeroberfläche, die es dem Benutzer ermöglicht, Objekte im Identitätsdepot zu erstellen.</p> <p>Weitere Informationen hierzu finden Sie in <a href="#">Kapitel 16, „Das Portlet „Erstellen““</a>, auf Seite 243.</p>

Portlet-Name	Beschreibung
Detail	Ermöglicht es Benutzern, die Attributdaten einer Entität anzuzeigen und zu bearbeiten.  Weitere Informationen hierzu finden Sie in <a href="#">Kapitel 17, „Portlet „Detail““</a> , auf <a href="#">Seite 249</a> .
Organigramm	Ermöglicht es Benutzern, hierarchische Beziehungen zwischen Objekten im Identitätsdepot anzuzeigen und zu durchsuchen.  Weitere Informationen hierzu finden Sie in <a href="#">Kapitel 18, „Portlet „Organigramm““</a> , auf <a href="#">Seite 263</a> .
Suchliste	Ermöglicht es Benutzern, Objekte im Identitätsdepot zu suchen.  Weitere Informationen hierzu finden Sie in <a href="#">Kapitel 20, „Portlet „Suchliste““</a> , auf <a href="#">Seite 293</a> .

## 15.4 Passwort-Portlets

Die Passwort-Portlets erweitern die Identity Manager-Benutzeranwendung um Funktionen zur Passwortselbstbedienung. Dazu gehören:

Portlet-Name	Weitere Informationen
IDM-Herausforderungsantwort	Siehe <a href="#">Kapitel 19, „Passwortverwaltungs-Portlet“</a> , auf <a href="#">Seite 279</a>
IDM - Passwort ändern	
IDM - Passwort vergessen	
IDM - Hinweisdefinition	
IDM-Anmeldung	

## 15.5 System-Portlets

Die System-Portlets bieten Services für die Identity Manager-Benutzeranwendung.

**Hinweis:** Es wird empfohlen, Portlets dieser Kategorie weder zu verwenden noch zu ändern.

Die System-Portlets umfassen:

Portlet-Name	Beschreibung
Portalseiten-Controller	Zeigt die freigegebene Seite an, die der Benutzer mithilfe des Portlets „Navigation für die freigegebene Seite“ aktuell ausgewählt hat.  Für dieses Portlet gibt es keine Standardeinstellungen.



In diesem Kapitel wird beschrieben, wie Sie das *Portlet* „Erstellen“ der Identity Manager-Benutzeranwendung verwenden. Es werden folgende Themen erläutert:

- [Abschnitt 16.1, „Allgemeines zum Portlet „Erstellen““](#), auf Seite 243
- [Abschnitt 16.2, „Konfiguration des Portlets „Erstellen““](#), auf Seite 244
- [Abschnitt 16.3, „Erstellen von Standardeinstellungen für das Portlet „Erstellen““](#), auf Seite 246

## 16.1 Allgemeines zum Portlet „Erstellen“

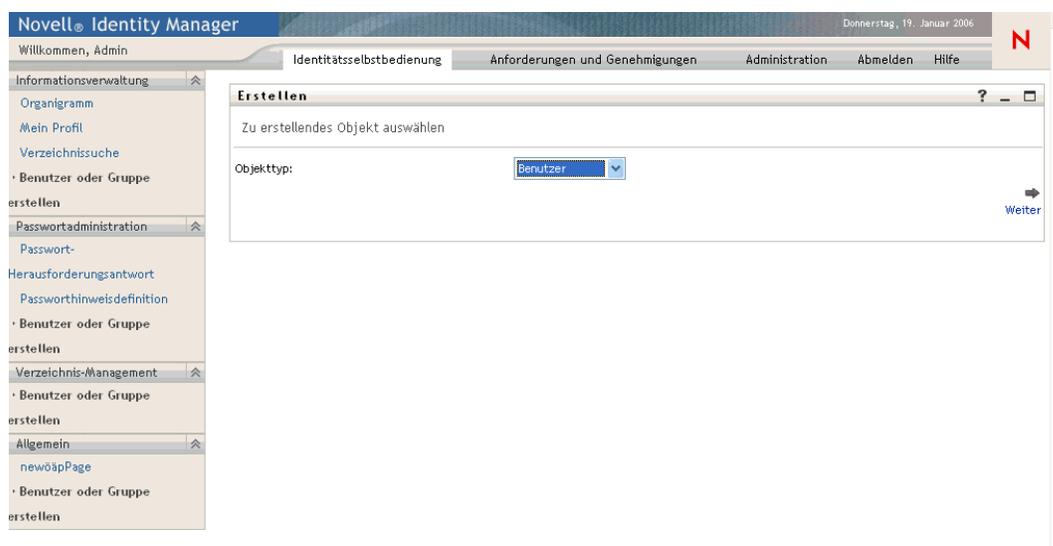
Das Portlet „Erstellen“ bietet einen benutzerfreundlichen Assistenten, der es Benutzern ermöglicht, unterschiedliche Identitätsdepot-Objekte zu erstellen. Die Portlet-Standardinstellungen steuern Folgendes:

- Die Objekttypen, die der Benutzer erstellen kann.
- Die Attribute, die der Benutzer festlegen kann.

Weitere Informationen finden Sie in [Abschnitt 16.3, „Erstellen von Standardeinstellungen für das Portlet „Erstellen““](#), auf Seite 246.

In der Standardkonfiguration des Portlets „Erstellen“ (auf die über die Aktion *Benutzer oder Gruppe erstellen* der Identity Manager-Benutzeranwendung zugegriffen werden kann) können Benutzer, Gruppen oder Aufgabengruppen erstellt werden. Dieses Portlet kann standardmäßig nur vom Benutzeranwendungsadministrator verwendet werden. Im folgenden Beispiel wird gezeigt, wie der standardmäßige Assistent für das Portlet „Erstellen“ den Benutzer zu Folgendem auffordert:

- *Typ des zu erstellenden Objekts auswählen:*



- *Attribute des Objekts festlegen:*

The screenshot shows the 'Erstellen' (Create) page in Novell Identity Manager. The main heading is 'Attribute festlegen für Benutzer' (Set attributes for user). Below this, there are two sections: 'Basisparameter' (Basic parameters) and 'Objektribute' (Object attributes). The 'Basisparameter' section includes fields for 'Objekt-ID\*' and 'Container\*'. The 'Objektribute' section includes fields for 'Vorname\*', 'Nachname\*', 'Titel', 'Abteilung', and 'Region', each with a 'Verstecken' (Hide) checkbox to its left. A left-hand navigation menu is visible, listing various administrative tasks like 'Organigramm', 'Mein Profil', and 'Verzeichnissuche'.

- *Zur Passworтеingabe auffordern, falls dies für den entsprechenden Objekttyp erforderlich ist:*

The screenshot shows the 'Erstellen' (Create) page in Novell Identity Manager, specifically the 'Passwort erstellen' (Create password) step. The main heading is 'Passwort erstellen'. Below this, there are two input fields: 'Passwort:' and 'Passwort bestätigen:'. Below the input fields, there are 'Zurück' (Back) and 'Weiter' (Next) buttons. A left-hand navigation menu is visible, listing various administrative tasks like 'Organigramm', 'Mein Profil', and 'Verzeichnissuche'.

Ist eine Passwortrichtlinie zugewiesen, werden alle benutzerdefinierten Richtlinienmeldungen von diesem Portlet angezeigt.

- *Bereitstellen einer Info-Meldung* nach erfolgreicher Installation des Objekts, das einen Link zum Portlet „Detail“ für das entsprechende Objekt enthält (sofern das Portlet „Detail“ entsprechend konfiguriert ist), um eine weitere Bearbeitung zu ermöglichen.

## 16.2 Konfiguration des Portlets „Erstellen“

Gehen Sie zum Konfigurieren des Portlets „Erstellen“ wie folgt vor:

Schritt	Aufgabe	Beschreibung
1	Entscheiden Sie, ob die Standardfunktion „Benutzer oder Gruppe erstellen“ Ihren Anforderungen entspricht	<p>Ist dies der Fall, müssen Sie keine weiteren Schritte unternehmen.</p> <p>Ist dies nicht der Fall, müssen Sie die verbleibenden Schritte ausführen.</p>
2	Definieren Sie die Objekttypen, deren Erstellung Sie Benutzern ermöglichen möchten	<p>Fügen Sie die Objekte und Attribute zur Verzeichnisabstraktionsschicht hinzu.</p> <p>Weitere Informationen finden Sie in <a href="#">Kapitel 4, „Konfigurieren der Verzeichnisabstraktionsschicht“</a>, auf <a href="#">Seite 75</a></p>
3	Legen Sie fest, auf welche Weise Sie Benutzern den Zugriff auf dieses neue Portlet ermöglichen möchten	<p>Möchten Sie es den Benutzern ermöglichen, dieses Portlet von einer vorhandenen oder von einer neuen Seite aus zu starten? Welche Benutzer sollen Zugriff auf das Portlet und die Seite haben?</p> <p>Weitere Informationen zu Seiten finden Sie in <a href="#">Kapitel 7, „Seitenadministration“</a>, auf <a href="#">Seite 137</a>.</p>
4	Geben Sie die Benutzer an, die Zugriff auf die Seite und die Portlet-Instanz haben sollen	<p>Bearbeiten Sie die Sicherheitseinstellungen und nehmen Sie Benutzer in die Liste auf. Weitere Informationen zur Beschränkung des Benutzerzugriffs auf Seiten finden Sie in <a href="#">Kapitel 7, „Seitenadministration“</a>, auf <a href="#">Seite 137</a>.</p> <p>Bearbeiten Sie die Portlet-Instanz, um die Sicherheitseinstellungen zu ändern. Weitere Informationen zur Beschränkung des Benutzerzugriffs auf Portlets finden Sie in <a href="#">Kapitel 9, „Portletadministration“</a>, auf <a href="#">Seite 181</a>.</p>
5	Legen Sie Standardeinstellungen für das Portlet fest	<p>Mit Standardeinstellungen können Sie Folgendes definieren:</p> <ul style="list-style-type: none"> <li>• Welche Objekte Benutzer erstellen können.</li> <li>• Welche Attribute beim Erstellen bereitzustellen sind.</li> </ul> <p>Weitere Informationen finden Sie in <a href="#">Abschnitt 16.3, „Erstellen von Standardeinstellungen für das Portlet „Erstellen““</a>, auf <a href="#">Seite 246</a>.</p>
6	Testen Sie Ihre Einstellungen	Überprüfen Sie, ob die Objekte korrekt erstellt werden und ob die Attribute ordnungsgemäß angegeben werden.
7	Legen Sie die gewünschten effektiven Rechte für die Endbenutzer in eDirectory fest	Um ein Objekt zu erstellen, muss der Benutzer <b>Trustee</b> der Organisationseinheit und der Organisation sein, in der das Objekt erstellt wird.

## 16.2.1 Einrichtung der Verzeichnisabstraktionsschicht

Von Benutzern des Portlets „Erstellen“ erstellbare Objekte und festlegbare Attribute müssen in der Verzeichnisabstraktionsschicht wie folgt definiert werden:

Definitionsart	Eigenschaft	Wert
Entität	create	Ausgewählt
	view	Ausgewählt
	Container for Create	Geben Sie einen gültigen Identitätsdepot-Container an.  Wird kein gültiger Container angegeben, wird der bei der Installation der Benutzeranwendung festgelegte Stammcontainer verwendet.
	Password	Ausgewählt, wenn für die Erstellung des Entitätstyps ein Passwort erforderlich ist.  Jeder Benutzer mit Zugriff auf das Portlet „Erstellen“ und Trustee-Rechten für die Organisationseinheit kann Benutzer erstellen und ein <b>Ausgangspasswort</b> festlegen. Sobald sich der neue Benutzer zum ersten Mal anmeldet, wird er an das Portlet „IDM - Passwort ändern“ weitergeleitet, damit er das Ausgangspasswort ändern kann.  Weitere Informationen zum Portlet „IDM - Passwort ändern“ finden Sie in <a href="#">Kapitel 19, „Passwortverwaltungs-Portlet“</a> , auf Seite 279.
Attribut	enabled	Ausgewählt
	viewable	Falls weder „enabled“ noch „viewable“ ausgewählt ist („false“), kann das Attribut nicht vom Portlet verwendet werden.

Weitere Informationen zum Einrichten der Abstraktionsschicht finden Sie in [Kapitel 4, „Konfigurieren der Verzeichnisabstraktionsschicht“](#), auf Seite 75.

## 16.3 Erstellen von Standardeinstellungen für das Portlet „Erstellen“

Mithilfe von Standardeinstellungen können Sie konfigurieren, welche Objekttypen Benutzer erstellen dürfen und welche Attribute sie angeben dürfen bzw. müssen.

Die Standardeinstellungen für das Portlet „Erstellen“ sind auf einer einzigen Seite für benutzerdefinierte Standardeinstellungen zusammengefasst. Beim Öffnen dieser Seite werden die individuellen Standardeinstellungen für das Portlet „Erstellen“ angezeigt:

Inhaltseinstellungen für diese Registrierungsinstanz ändern (Erstellen)

Entität erstellen

Create VirtualEntity complex preference

**Create**

**Zusammenfassung**

Entitätsdefinition	Benutzer	[X]
Attribute		[Pencil]
	Vorname	
	Nachname	
	Titel	
	Abteilung	
	Region	
	Email	
	Manager	
	Telefonnummer	
Entitätsdefinition	Gruppe	[X]
Attribute		[Pencil]
	Beschreibung	
Entitätsdefinition	Aufgabengruppe	[X]
Attribute		[Pencil]

[Zurück zu Listenansicht](#)

Die Standardeinstellungen werden im Folgenden beschrieben (alternativ können Sie auch auf die Schaltfläche „Beschreibungen“ klicken, um eine Online-Hilfe zu diesem Portlet anzuzeigen).

#### Standardeinstellung

#### Beschreibung

##### Entitätsdefinition

Der Name des zu erstellenden Objekttyps.

Dieser Name stellt den Anfang eines Entitätsdefinitionsblocks dar, in dem Sie definieren, wie das Portlet den Erstellungsvorgang handhaben soll.

##### So legen Sie Beschränkungen für Objekte fest:

Objekte, die in den komplexen Standardeinstellungen aufgelistet sind, werden dem Benutzer in einem Dropdown-Menü angezeigt. Wenn Sie die Objekte, die Benutzer erstellen können, einschränken möchten, entfernen Sie diese mithilfe der Löschschriftfläche aus dem Standardeinstellungsblatt.

##### So fügen Sie weitere Entitäten hinzu:

Klicken Sie auf **Entitätsdefinition hinzufügen** und befolgen Sie die Anweisungen des Assistenten.

Standardeinstellung	Beschreibung
Attribute	<p>Steuert die Attribute, für die der Benutzer aufgefordert wird, Werte anzugeben. Sie müssen alle erforderlichen Attribute des Objekts angeben, weil anderenfalls der Erstellungsvorgang für das Objekt fehlschlägt. Darüber hinaus werden die Standardeinstellungen nicht ordnungsgemäß gespeichert, wenn ein erforderliches Attribut fehlt.</p> <p><b>So fügen Sie ein Attribut hinzu bzw. entfernen es:</b></p> <ul style="list-style-type: none"> <li>• Klicken Sie auf die Schaltfläche zum Ändern von Attributen.</li> </ul> <div data-bbox="664 535 724 594" style="text-align: center;">  </div> <ul style="list-style-type: none"> <li>• Wählen Sie in der Liste der verfügbaren Attribute ein Attribut aus, das Sie hinzufügen möchten. Sie können mehrere Attribute auswählen, indem Sie die Strg- bzw. Umschalttaste gedrückt halten.</li> <li>• Klicken Sie auf den Pfeil, um das Attribut in die Liste der ausgewählten Elemente zu verschieben. Wenn Sie ein Attribut entfernen möchten, verfahren Sie umgekehrt.</li> <li>• Klicken Sie zum Umsortieren der Attributliste auf den Aufwärts- bzw. Abwärtspfeil rechts neben der Liste der ausgewählten Elemente. Klicken Sie auf <b>Senden</b>.</li> </ul> <p><b>Attribute und Datentypen:</b></p> <p>Der Datentyp des Attributs legt fest, wie das Attribut angezeigt wird. Wenn ein Attribut beispielsweise als Untertyp der Liste „Lokal“ oder „Global“ definiert ist, wird es in einem Listenfeld angezeigt.</p> <p>Weitere Informationen finden Sie in <a href="#">Abschnitt 4.3, „Arbeiten mit Entitäten und Attributen“</a>, auf Seite 87.</p>

**Fertigstellen der Standardeinstellungsseite** Klicken Sie auf *Senden*, wenn Sie überprüfen möchten, ob alle von Ihnen eingegebenen Daten gültig sind. Ist ein Eintrag ungültig, wird im oberen Teil der Standardeinstellungsseite eine Fehlermeldung angezeigt. Klicken Sie auf *Zurück zu Listenansicht*, wenn nach dem Klicken auf *Senden* keine Fehler mehr auftreten. Nachdem Sie zur Listenansicht zurückgekehrt sind, müssen Sie auf *Standardeinstellungen speichern* klicken.

In diesem Kapitel wird das *Portlet* „Detail“ beschrieben, mit dessen Hilfe Benutzer die Attributdaten einer Entität anzeigen und bearbeiten können. Es stellt die Grundlage für die Aktion „Mein Profil“ im Register „Identitätsselbstbedienung“ der Identity Manager-Benutzeranwendung dar. Es werden folgende Themen erläutert:

- [Abschnitt 17.1, „Allgemeines zum Portlet „Detail““, auf Seite 249](#)
- [Abschnitt 17.2, „Voraussetzungen“, auf Seite 258](#)
- [Abschnitt 17.5, „Festlegen von Standardeinstellungen“, auf Seite 261](#)

## 17.1 Allgemeines zum Portlet „Detail“

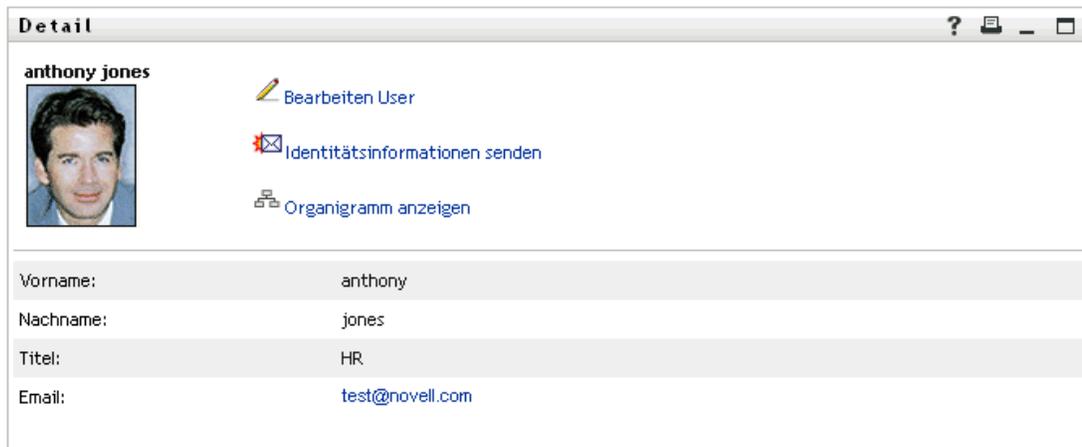
Das Detail-Portlet bietet Benutzern eine detaillierte Ansicht der Attribute einer Entität und deren Werte. Das Portlet verfügt über zwei Modi: „Anzeigen“ und „Bearbeiten“. Beim Zugriff auf das Detail-Portlet können Benutzer dessen integrierte Funktionen zum Bearbeiten dieser Daten nutzen:

- [Abschnitt 17.1.1, „Anzeigen von Entitätsdaten“, auf Seite 249](#)
- [Abschnitt 17.1.2, „Bearbeiten von Entitätsdaten“, auf Seite 253](#)
- [Abschnitt 17.1.3, „Versand von Entitätsdaten per Email“, auf Seite 256](#) (nur Anzeigemodus)
- [Abschnitt 17.1.4, „Verknüpfung mit einem Organigramm“, auf Seite 256](#)
- [Abschnitt 17.1.5, „Verknüpfung mit Details anderer Entitäten“, auf Seite 257](#) (nur Anzeigemodus)
- [Abschnitt 17.1.6, „Drucken von Entitätsdaten“, auf Seite 257](#) (nur Anzeigemodus)

### 17.1.1 Anzeigen von Entitätsdaten

Wenn auf das Detail-Portlet zugegriffen wird, zeigt es *Attributdaten zu einer ausgewählten Entität an*, beispielsweise zu einem Benutzer oder zu einer Gruppe. Im Folgenden sehen Sie, was das

Detail-Portlet beispielsweise anzeigen könnte, wenn der Benutzer Bill Brown seine persönlichen Daten aufruft:



**Bilder von Benutzern** Standardmäßig ist das Detail-Portlet so konfiguriert, dass es das Attribut „User Photo“ (Benutzerfoto) anzeigt. Wenn Ihr Identitätsdepot dieses Attribut jedoch nicht umfasst oder kein Bild vorhanden ist, wird zur Laufzeit ein Standardbild angezeigt. Wenn Sie Ihre Benutzerbilder an einem anderen Ort speichern, können Sie das Portlet entsprechend konfigurieren.

Weitere Informationen finden Sie in [„Dynamisches Laden von Bildern“ auf Seite 253](#).

### Festlegen der anzuzeigenden Attribute

Das Detail-Portlet zeigt nur die folgenden Attribute an:

- Attribute, die gemäß den Datendefinitionen der *Verzeichnisabstraktionsschicht* zur Anzeige verfügbar sind

Weitere Informationen zur VDD-Konfiguration finden Sie in [Kapitel 4, „Konfigurieren der Verzeichnisabstraktionsschicht“](#), auf Seite 75.

- Attribute, die in den *Detail-StandardEinstellungen* angegeben sind

Weitere Informationen dazu, wie Sie die im Detail-Portlet anzuzeigenden Attribute festlegen, finden Sie in [Abschnitt 17.5, „Festlegen von Standardeinstellungen“](#), auf Seite 261.

- Attribute, für die der aktuelle Benutzer eine *Anzeigeberechtigung* hat

So werden beispielsweise Managern mit der Berechtigung zum Anzeigen von Gehältern die entsprechenden Daten angezeigt. Andere Benutzer haben darauf keinen Zugriff.

Weitere Informationen finden Sie in [Abschnitt 17.2.2, „Zuweisen von Berechtigungen für Entitäten“](#), auf Seite 258.

- Attribute, die einen *Wert* aufweisen

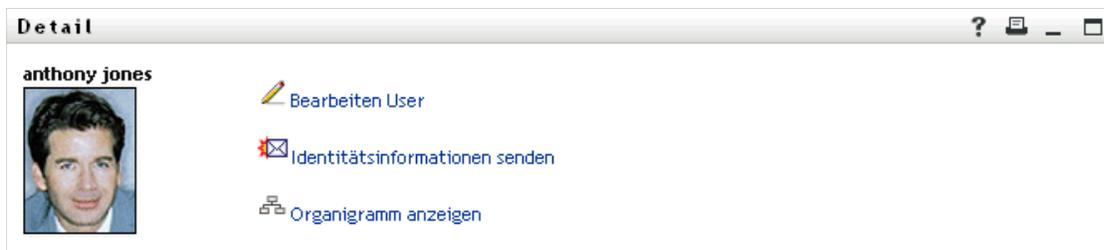
### Festlegen der Anzeigeeigenschaften für Attribute

Beim Anzeigen von Attributen werden im Detail-Portlet *alle Daten als Text formatiert*. Dabei gelten folgende Ausnahmen:

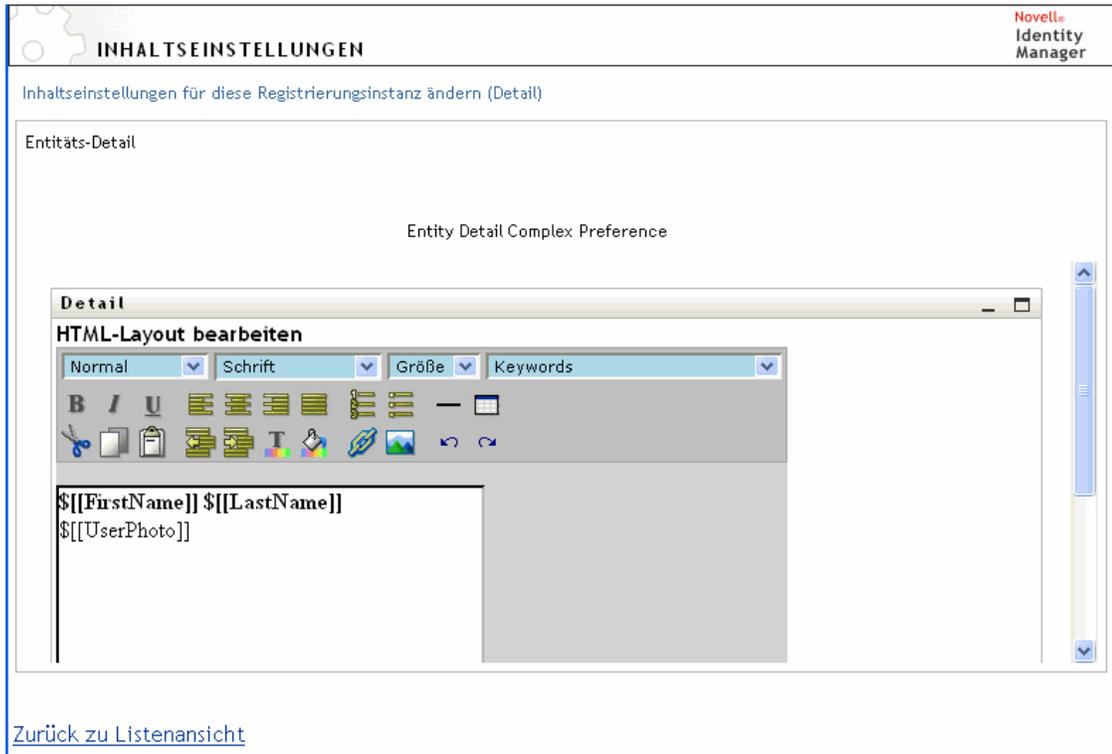
Formatangabe in der Definition der Abstraktionsschicht	Art der Anzeige
<b>Format:</b> email	Als mailto-Link
<b>Format:</b> <ul style="list-style-type: none"> <li>• groupwise-im</li> <li>• aol-im</li> <li>• yahoo-im</li> </ul>	Als Symbol, über das eine Chat-Session initiiert und der Benutzer hinzugefügt wird
<b>Datentyp:</b> Binär	Als Schaltfläche und Link zum Anzeigen des Bilds
<b>Format:</b> image	
<b>Datentyp:</b> Boolesch	Als deaktivierte Optionsfelder für „Wahr“ oder „Falsch“  Die Felder werden ohne einen Standardwert angezeigt, weil das Attribut erst für den Benutzer erstellt wird, wenn ein Wert angegeben wird.
<b>Multivalue:</b> Ausgewählt	Als sich wiederholende Steuerelemente zum Bearbeiten, Hinzufügen und Entfernen einzelner Attributwerte (in Form einer durch Kommas getrennten Liste)
<b>Control type:</b> DNLookup	Als Link  Im oben abgebildeten Beispiel wird ein Link (Terry Mellon) angezeigt, über den der Zugriff auf die Detail-Daten von Bill Browns Chef möglich ist.
<b>Control type:</b> <ul style="list-style-type: none"> <li>• Local List</li> <li>• Global List</li> </ul>	Als Anzeigebezeichnung und nicht als eigentlicher (Schlüssel-)Wert  Beispielsweise zeigt das Attribut „EmployeeType“ den String <code>Full Time</code> und nicht den eigentlichen Wert <code>ft an</code> .

## Festlegen der Anzeigeelemente im Kopfbereich

Sie können das Layout des Kopfbereichs des Detail-Portlets unter Verwendung von standardmäßigen HTML-Funktionen anpassen:



In den Detail-Standard-Einstellungen finden Sie einen *HTML-Layout-Editor*, mit dessen Hilfe Sie Aussehen und Inhalt des Portlets nach Wunsch anpassen können:



### Verwendung des HTML-Layout-Editors

Der HTML-Layout-Editor bietet die üblichen Funktionen eines HTML-Editors zum Formatieren von Text und Listen, zum Einfügen von Anker und Bildern usw.

**Schlüsselwörter** Beim Erstellen Ihres Layouts können Sie die Dropdown-Liste „Schlüsselwörter“ nutzen, um Variablen in den Kopfbereich des Detail-Portlets einzusetzen, die zur Laufzeit durch bestimmte Attributwerte ersetzt werden. Alternativ können Sie diese Variablen auch mithilfe der folgenden Syntax eingeben:

```
$[[Schlüsselwort]]
```

Dabei steht *Schlüsselwort* für den Wert eines Attributs wie „LastName“.

Es ist möglich, Attribute mithilfe der folgenden Syntax zu verketteten:

```
$[[Schlüsselwort+Schlüsselwort]]
```

Zum Beispiel:

```
$[[FirstName+LastName]]
```

Dabei können Sie beliebig viele Attribute miteinander verketteten und darüber hinaus in Anführungszeichen eingeschlossenen Textstrings eingeben:

```
${[Schlüsselwort+"Beispieltext"+Schlüsselwort]}
```

Hierdurch werden die Werte der Schlüsselwörter und der in Anführungszeichen stehende Text angezeigt.

---

**Hinweis:** Wenn ein Schlüsselwort in einem Layout falsch geschrieben ist, wird es zur Laufzeit als Textstring angezeigt (einschließlich \${[]}).

---

**Dynamisches Laden von Bildern** Um im Identitätsdepot gespeicherte Bilder, beispielsweise Fotos, anzuzeigen, können Sie den Attributnamen mithilfe des HTML-Layout-Editors einfügen. Wenn Sie beispielsweise das Attribut „User Photo“ einfügen, wird das Foto des Benutzers angezeigt. Wenn Sie Bilder außerhalb des Identitätsdepots speichern, müssen Sie das Tag „IMG:“ (im *Modus* „*Quelltext anzeigen*“ des HTML-Editors) wie folgt verwenden:

- 1 Wechseln Sie zu den Standardeinstellungen des Portlets und öffnen Sie den HTML-Editor.
- 2 Klicken Sie auf *Quelltext anzeigen*.
- 3 Geben Sie unter Verwendung des Tags „IMG:“ eine Kombination aus Speicherort, Attributschlüssel und Dateierweiterung ein. Verwenden Sie dabei folgende Syntax:

```
${[IMG:"URL" + Attributschlüssel + "Dateierweiterung"]}
```

Im folgenden Beispiel sehen Sie die Syntax, die Sie verwenden müssen, wenn Sie die Fotos Ihrer Mitarbeiter als JPG-Dateien nach Nachnamen geordnet im Unterverzeichnis „/images“ Ihres Anwendungsservers gespeichert haben:

```
${[IMG:"http://meinhost:8080/images/"+LastName+".jpg"]}
```

Zur Laufzeit verkettet das Portlet die URL mit dem Attribut „LastName“ und der Dateierweiterung „.jpg“.

Der HTML-Editor unterstützt eine flexible Syntax. Er unterstützt eine beliebige Kombination aus Text und Attributen, beispielsweise:

```
${[IMG:"beliebiger Text" + Attributschlüssel + ...]}
```

## 17.1.2 Bearbeiten von Entitätsdaten

Das Detail-Portlet stellt automatisch einen Link zum *Bearbeiten* (z. B. *Ihre Informationen bearbeiten*, *Benutzer bearbeiten* oder *Gerät bearbeiten*) bereit, über den Sie vom Anzeige- in den Bearbeitungsmodus wechseln können. Hierdurch können Benutzer mit den entsprechenden Berechtigungen für die aktuelle Entität deren Attributwerte ändern und diese Änderungen speichern.

Für den Benutzer Bill Brown (der über die erforderlichen Berechtigungen verfügt) könnten im Bearbeitungsmodus des Detail-Portlets seine eigenen Daten beispielsweise folgendermaßen aussehen:

**Detail**
? [Icon] [Icon]

### Bearbeiten Benutzer

\* - erforderlich.

Verstecken	Attribut	Wert
<input type="checkbox"/>	Vorname:*	<input type="text" value="Billy"/>
<input type="checkbox"/>	Nachname:*	<input type="text" value="Murphy"/>
<input type="checkbox"/>	Titel:	<input type="text" value="Manager"/>
<input type="checkbox"/>	Abteilung:	
<input type="checkbox"/>	Region:	Irland
<input type="checkbox"/>	Email:	<input type="text" value="test@novell.com"/>
<input type="checkbox"/>	Manager:	<input type="text"/>
<input type="checkbox"/>	Gruppe:	<input type="text"/>
<input type="checkbox"/>	Telefonnummer:	<input type="text" value="(555) 555-1225"/>
<input type="checkbox"/>	Bevorzugtes Gebietsschema:	<input type="text" value="(nichts ausgewählt)"/> ▼
<input checked="" type="checkbox"/>	Benutzerfoto:	<a href="#">Grafik hinzufügen</a>
<input type="checkbox"/>	Admin-Manager:	<input type="radio"/> Wahr <input type="radio"/> Falsch
<input type="checkbox"/>	Aufgabengruppenmanager:	<input type="radio"/> Wahr <input type="radio"/> Falsch
<input type="checkbox"/>	Verwaltete Aufgabengruppen:	<input type="text"/>

**Hinweis:** Wenn bei booleschen Attributen beide Optionsfelder deaktiviert sind, bedeutet dies, dass das entsprechende Attribut für den Benutzer nicht verfügbar ist. Wenn Sie das Optionsfeld *Wahr* oder *Falsch* auswählen, wird das Attribut für den Benutzer erstellt und der ausgewählte Wert übernommen.

## Festlegen der anzuzeigenden Attribute

Im Bearbeitungsmodus des Detail-Portlets werden nur die folgenden Attribute angezeigt:

- Attribute, die gemäß den Datendefinitionen der *Verzeichnisabstraktionsschicht* zur Anzeige bereitgestellt werden

Weitere Informationen zu Datendefinitionen finden Sie in [Kapitel 4, „Konfigurieren der Verzeichnisabstraktionsschicht“](#), auf Seite 75.

- Attribute, für die der aktuelle Benutzer eine *Anzeigeberechtigung* hat

So werden beispielsweise Managern mit der Berechtigung zum Anzeigen von Gehältern die entsprechenden Daten angezeigt. Andere Benutzer haben darauf keinen Zugriff.

Weitere Informationen finden Sie in [Abschnitt 17.2.2, „Zuweisen von Berechtigungen für Entitäten“](#), auf Seite 258.

Ein Attribut wird nur im Bearbeitungsmodus angezeigt, wenn es allen oben genannten Kriterien entspricht.

## Festlegen der Anzeigeeigenschaften für Attribute

Im Bearbeitungsmodus des Detail-Portlets wird jedes bearbeitbare Attribut als *Textfeld* formatiert. Dabei gelten folgende Ausnahmen:

Attributtyp-Spezifikation (in VDD-Dateien)	Art der Anzeige
Data type: Binary Format: Image	Als Schaltfläche und Link zum Portlet „Entity Image Upload“, mit dem das Bild angezeigt, aktualisiert oder hinzugefügt werden kann
Data type: Boolesch hide:Ausgewählt	Als Optionsfelder für „Wahr“ oder „Falsch“ Als Kontrollkästchen mit der Beschriftung „hide“
multivalue=Ausgewählt	Als Steuerelemente zum Bearbeiten, Hinzufügen und Entfernen von Attributwerten
Control type: DNLookup	Als Schaltfläche zum Starten des Portlets „Param List“, mit dem Sie einen DN suchen und auswählen können
Control type: <ul style="list-style-type: none"><li>• Local list</li><li>• Global list</li></ul>	Als Dropdown-Liste (ggf. können mehrere Elemente ausgewählt werden)

Attribute, die nicht bearbeitet werden können (entweder aufgrund ihrer Definition oder wegen unzureichender Benutzerrechte) werden *deaktiviert* oder als *schreibgeschützt* angezeigt.

## Überprüfen von Änderungen

Während der Bearbeitung werden automatisch die Daten der folgenden Attributtyp-Spezifikationen überprüft:

- Format: email
- Data type: Integer

- Control type: Range

Wenn Sie mit einem Steuerelementtyp einer lokalen oder globalen Liste arbeiten, enthält die angezeigte Liste unter Umständen Werte, die außerhalb des festgelegten Attributbereichs liegen. Solche Werte werden als außerhalb des zulässigen Bereichs markiert und können aufgrund der Überprüfung nicht gesendet werden.

### Definieren einer Standardentität für „Mein Profil“

Wenn Sie eine Entität in der Verzeichnisabstraktionsschicht definieren, können Sie einen Wert für *Default MyProfile Entity* angeben (im Element „Konfiguration“ des Verzeichnisabstraktionsschicht-Editors), um festzulegen, dass eine andere Entitätsdefinition zur Bearbeitung verwendet werden soll. Beim Wechseln vom Anzeige- in den Bearbeitungsmodus überprüft das Detail-Portlet immer, ob dieses Element angegeben ist, und verwendet die passende Entitätsdefinition zum Anzeigen der Attribute.

Angenommen, die Entitätsdefinition für „Student“ umfasst *user* als Wert für *Default My Profile Entity*. In diesem Fall wird im Anzeigemodus die Entitätsdefinition „Student“, im Bearbeitungsmodus jedoch die Entitätsdefinition „user“ verwendet.

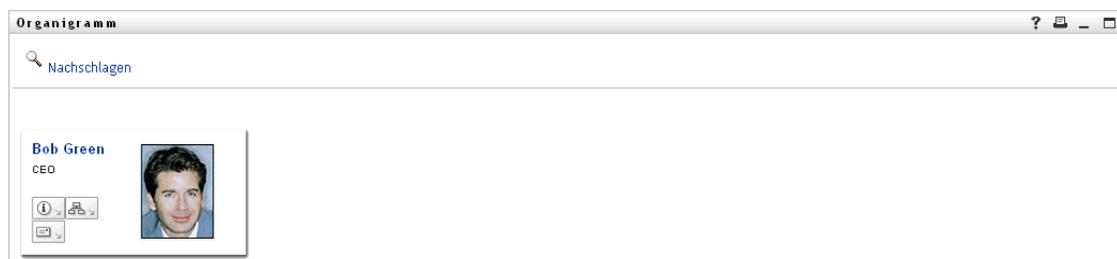
## 17.1.3 Versand von Entitätsdaten per Email

Das Detail-Portlet bietet automatisch einen Link mit der Bezeichnung *Identitätsinformationen senden*. Benutzer können darauf klicken, um die URL der Details zur aktuellen Entität per Email an einen oder mehrere Benutzer zu senden. Durch das Versenden der Detail-URL anstelle der eigentlichen Daten wird die Sicherheit gewährleistet (weil jeder, Empfänger der URL die entsprechenden Berechtigungen zu ihrer Nutzung benötigt).

## 17.1.4 Verknüpfung mit einem Organigramm

Das Detail-Portlet bietet automatisch einen Link mit der Bezeichnung *Organigramm anzeigen*. Benutzer können darauf klicken, um das Portlet „Organigramm“ für den aktuellen Eintrag anzuzeigen.

Wenn Sie beispielsweise das Detail-Portlet für den Benutzer Bill Brown anzeigen und auf diesen Link klicken, wird Folgendes angezeigt:

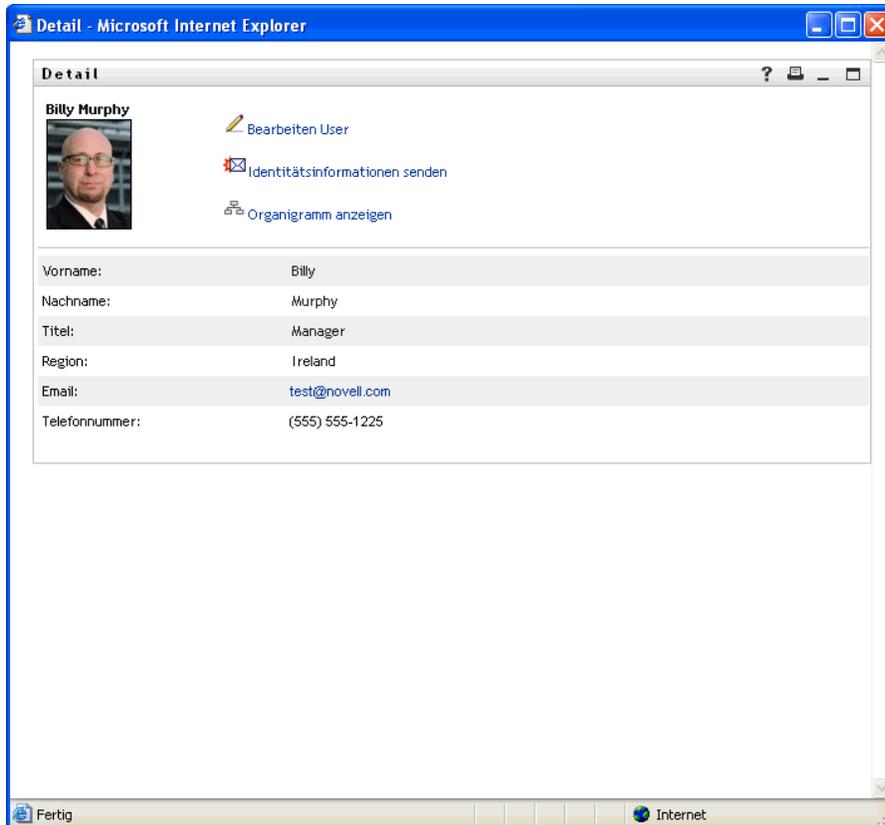


Weitere Informationen zum Portlet „Organigramm“ finden Sie in [Kapitel 18, „Portlet „Organigramm““](#), auf Seite 263.

## 17.1.5 Verknüpfung mit Details anderer Entitäten

Beim Konfigurieren des Detail-Portlets kann es sinnvoll sein, für Benutzer Links von der aktuellen Entität zu anderen, verwandten Entitäten bereitzustellen. Sie können diese Links erstellen, indem Sie Attribute einfügen, die (in Ihrer Verzeichnisabstraktionsschicht) mit dem *Steuerungstyp* „*DNLookup*“ definiert sind.

Umfasst das Detail-Portlet für einen Benutzer das Attribut „Manager“, wird dieses als *Link* angezeigt. Wenn ein Benutzer auf diesen Link klickt, wird das Detail-Portlet für den Manager angezeigt.



Weitere Informationen zur Verzeichnisabstraktionsschicht finden Sie in [Kapitel 4, „Konfigurieren der Verzeichnisabstraktionsschicht“](#), auf Seite 75.

Weitere Informationen dazu, wie Sie die im Detail-Portlet anzuzeigenden Attribute festlegen, finden Sie in [Abschnitt 17.5, „Festlegen von Standardeinstellungen“](#), auf Seite 261.

## 17.1.6 Drucken von Entitätsdaten

Standardmäßig ist in den Anzeigeeinstellungen für das Detail-Portlet die Option *Drucken* in der Titelleiste des Portlets aktiviert. Wenn Sie diese Option aktiviert lassen, können Benutzer darauf klicken, um eine druckerfreundliche Version des Inhalts des Detail-Portlets anzuzeigen.

Um diese oder andere Einstellungen für das Detail-Portlet zu ändern, aktualisieren Sie über die Registerkarte „Administration“ die Portlet-Registrierung für *DetailPortlet* (auf der Seite „Portletadministration“).

Weitere Informationen finden Sie in [Kapitel 9, „Portletadministration“](#), auf Seite 181.

## 17.2 Voraussetzungen

Bevor Sie das Detail-Portlet verwenden, sollten Sie sich mit Folgendem auskennen:

- [Abschnitt 17.2.1, „Konfigurieren der Verzeichnisabstraktionsschicht“](#), auf Seite 258
- [Abschnitt 17.2.2, „Zuweisen von Berechtigungen für Entitäten“](#), auf Seite 258

### 17.2.1 Konfigurieren der Verzeichnisabstraktionsschicht

Das Detail-Portlet ist in mehrfacher Hinsicht von den Definitionen der *Verzeichnisabstraktionsschicht* abhängig. Anweisungen dazu, wie Sie die Definitionen der Abstraktionsschichtdaten so konfigurieren, dass sie bestimmte Funktionen des Detail-Portlets unterstützen, finden Sie in den folgenden Abschnitten dieses Kapitels:

- [Abschnitt 17.1.1, „Anzeigen von Entitätsdaten“](#), auf Seite 249
- [Abschnitt 17.1.2, „Bearbeiten von Entitätsdaten“](#), auf Seite 253
- [Abschnitt 17.4, „Verwendung von Details auf einer Seite“](#), auf Seite 260

Weitere Informationen zur Konfiguration finden Sie in [Kapitel 4, „Konfigurieren der Verzeichnisabstraktionsschicht“](#), auf Seite 75.

### 17.2.2 Zuweisen von Berechtigungen für Entitäten

Um auf eine Entität und deren Attribute im Detail-Portlet zuzugreifen, müssen Benutzern *in eDirectory die entsprechenden Berechtigungen* zugewiesen sein:

Für diese Aktion	Benötigt ein Benutzer diese Berechtigung
Attribut anzeigen	Lesen
Attribut bearbeiten	Schreiben

Sie können Rechte zuweisen, indem Sie festlegen, dass es sich bei einem Benutzer um einen *Trustee* eines Objekts (einer Entität) handelt. Anschließend können Sie festlegen, welche Rechte für welche Attribute gelten sollen.

## 17.3 Starten des Detail-Portlets von anderen Portlets aus

Eine typische Verwendung des Detail-Portlets besteht darin, es zu starten, nachdem man in einem anderen Identitäts-Portlet eine Entität ausgewählt hat. Sie können das Detail-Portlet folgendermaßen starten:

- [Abschnitt 17.3.1, „Vom Portlet „Suchliste“ aus“](#), auf Seite 259
- [Abschnitt 17.3.2, „Vom Portlet „Organigramm“ aus“](#), auf Seite 259

## 17.3.1 Vom Portlet „Suchliste“ aus

Benutzer können in den Suchergebnissen des Suchlisten-Portlets *auf die Zeile einer Entität klicken*, um das Detail-Portlet für die entsprechende Entität anzuzeigen. Wenn Sie beispielsweise in der folgenden Liste auf die Zeile „Bill Brown“ klicken, wird das Detail-Portlet mit seinen Attributdaten angezeigt:

Novell Identity Manager Donnerstag, 19. Januar 2006

Willkommen, Admin Identitätsselbstbedienung Anforderungen und Genehmigungen Administration Abmelden N

Hilfe

Informationsverwaltung

- Organigramm
- Mein Profil
- ▣ **Verzeichnissuche**
- Benutzer oder Gruppe erstellen

Passwortadministration

- Passwort-

Herausforderungsantwort

- Passwortschwächen
- Benutzer oder Gruppe erstellen

Verzeichnis-Management

- Benutzer oder Gruppe erstellen

Allgemein

- newöapPage
- Benutzer oder Gruppe erstellen

Suchliste

Suchergebnisse

Verwenden Sie die folgenden Registerkarten, um unterschiedliche Ansichten Ihres Ergebnis-Sets anzuzeigen.

**Benutzer:** (Vorname beginnt mit \*)  
**Sortiert nach:** Nachname  
**Gesamtzahl Übereinstimmungen:** 5

Identität	Standort	Organisation		
Vorname	Nachname	Titel	Email	Telefonnummer
admin				
john	frank	Supervisor	✉	
anthony	jones	HR	✉	
Billy	Murphy	Manager		
Tim	Smith	QA	✉	

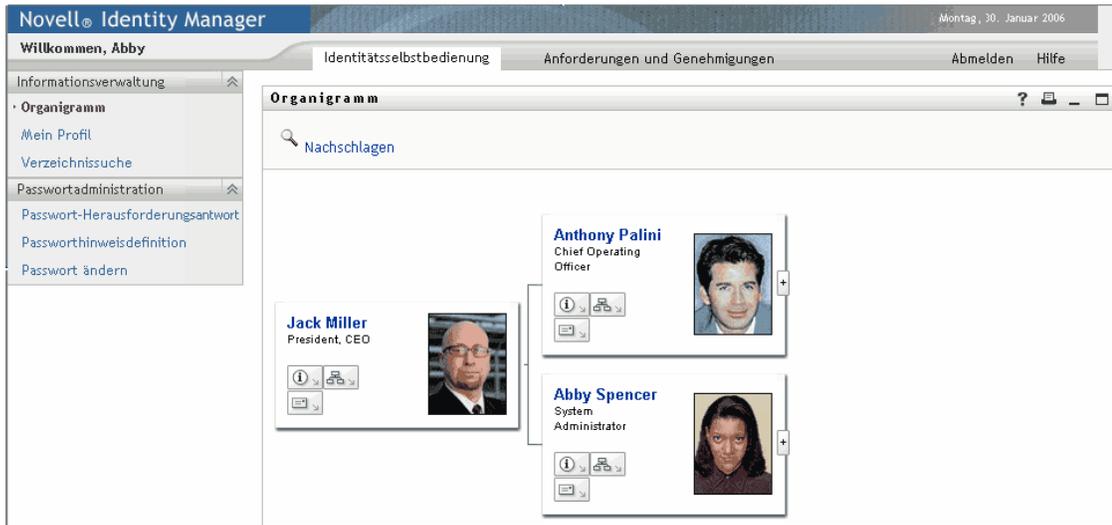
1 - 5 von 5

Weitere Informationen zum Portlet „Suchliste“ finden Sie in [Kapitel 20, „Portlet „Suchliste““](#), auf [Seite 293](#).

## 17.3.2 Vom Portlet „Organigramm“ aus

Im Organigramm-Portlet können Benutzer auf das *Symbol „Identitätsaktionen“* für eine Entität klicken und anschließend *Info anzeigen* wählen, um die Details zur entsprechenden Entität

anzuzeigen. Wenn Sie beispielsweise im folgenden Organigramm bei Bill Brown auf „Info anzeigen“ klicken, wird das Detail-Portlet mit seinen Attributdaten angezeigt:

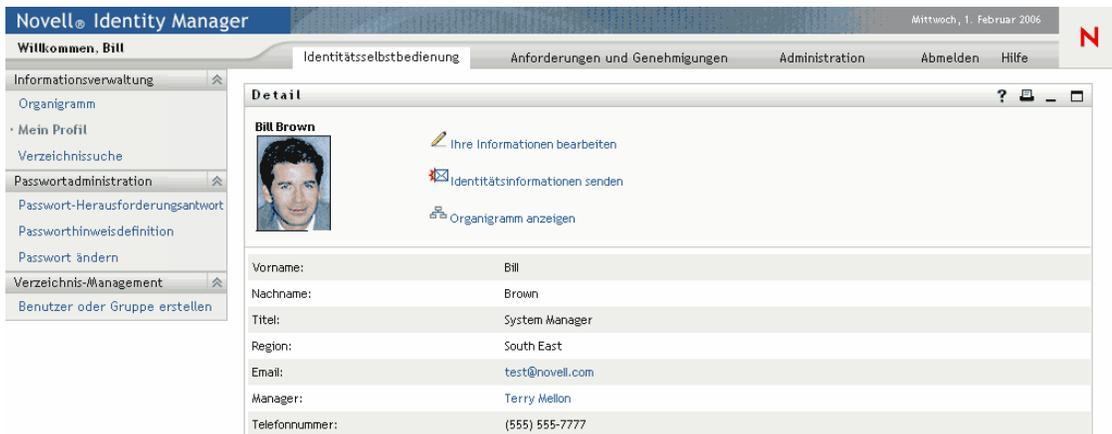


Weitere Informationen zum Portlet „Organigramm“ finden Sie in [Kapitel 18](#), „Portlet „Organigramm““, auf Seite 263.

## 17.4 Verwendung von Details auf einer Seite

Wenn Sie möchten, dass Benutzer eigenständig ihre eigenen Attributdaten anzeigen und ggf. bearbeiten können, können Sie das Detail-Portlet in eine *freigegebene Seite* aufnehmen. Wird das Detail-Portlet auf einer freigegebenen Seite verwendet, greift es automatisch auf die Daten des aktuellen Benutzers (oder einer anderen Standardentität) zu.

So kann sich beispielsweise der Benutzer Bill Brown anmelden und zur folgenden persönlichen Seite wechseln, um seine eigenen Informationen über das Detail-Portlet zu verwalten:



Um festzulegen, welche Entitätsdefinition das Detail-Portlet bei diesem Szenario verwenden soll (also, wenn es über eine Seite und nicht von einem anderen Portlet aufgerufen wird), passen Sie die

Einstellung *Default 'My Profile' Entity* im Element „Konfiguration“ der Verzeichnisabstraktionsschicht an.

## 17.5 Festlegen von Standardeinstellungen

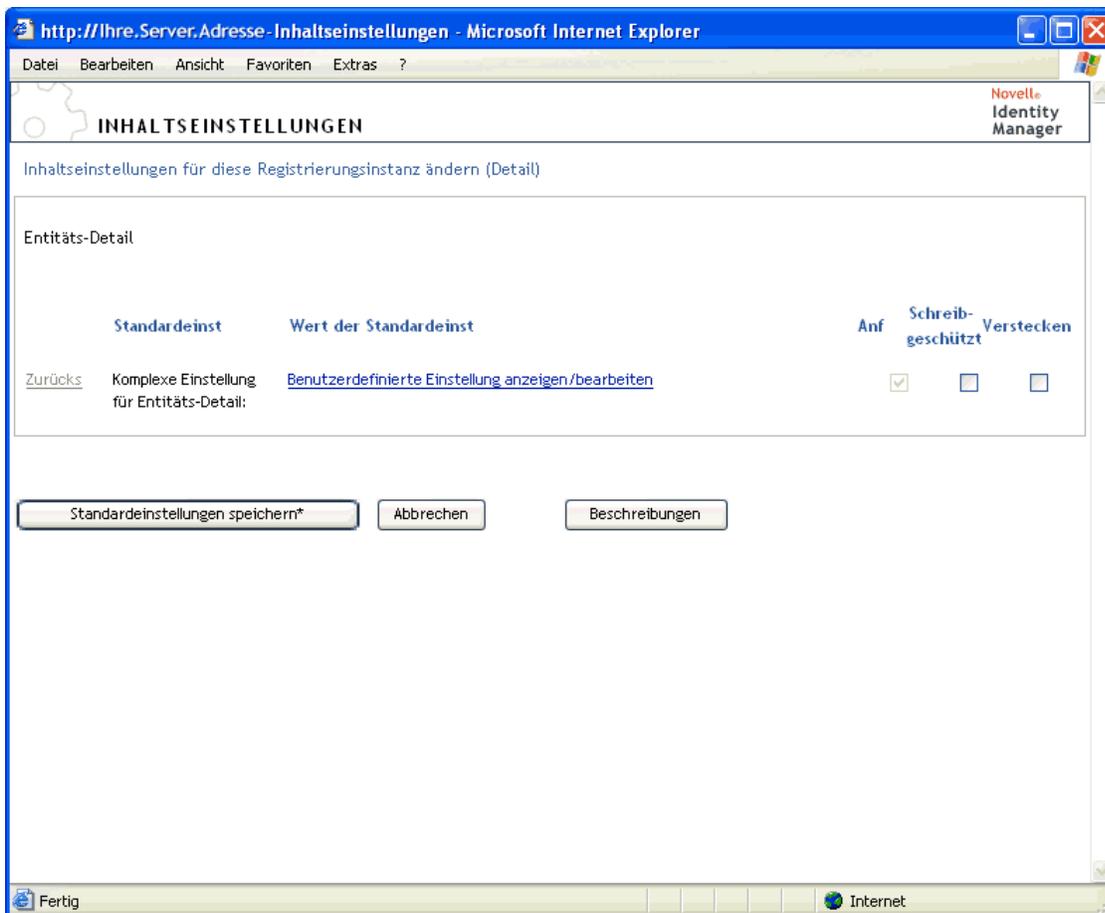
Mithilfe der Standardeinstellungen können Sie den Inhalt und das Aussehen des Detail-Portlets festlegen. An welcher Stelle Sie die Standardeinstellungen festlegen müssen, ist davon abhängig, wie Sie das Detail-Portlet verwenden:

Weitere Informationen dazu, wie Sie auf die Standardeinstellungen für ein Portlet zugreifen, auf das über eine freigegebene Seite oder eine Containerseite zugegriffen wird, finden Sie in **Kapitel 7**, „**Seitenadministration**“, auf Seite 137.

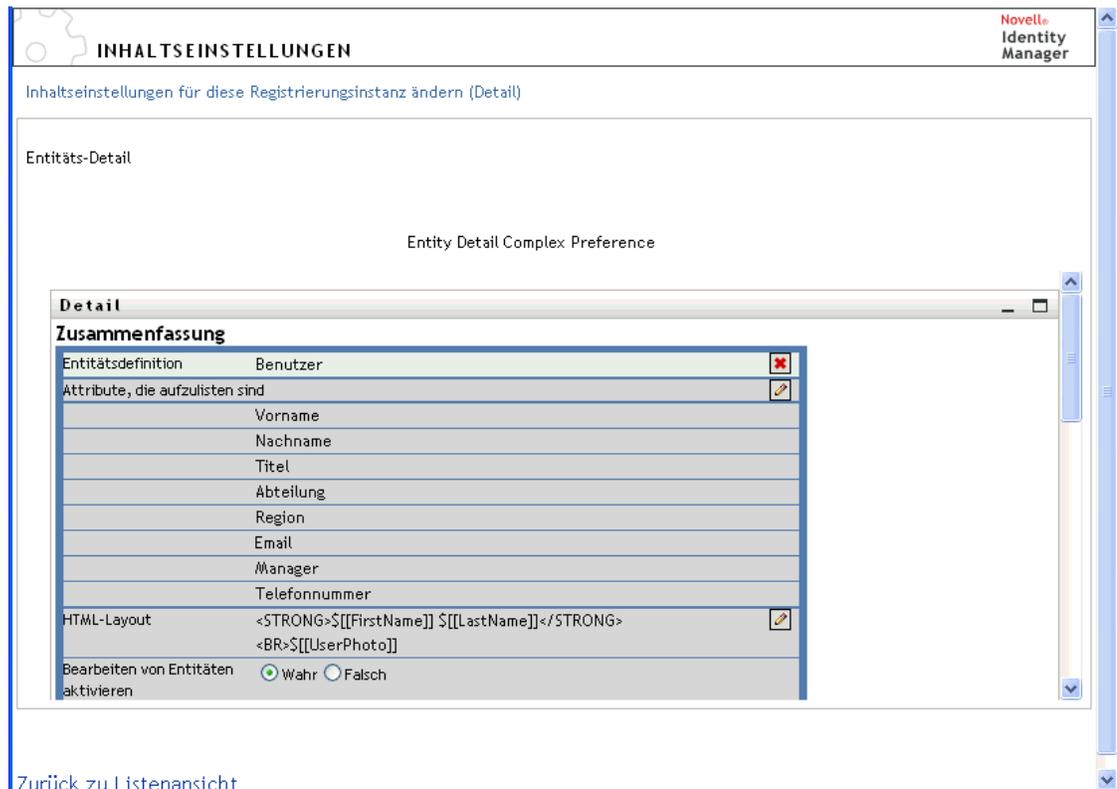
Weitere Informationen dazu, wie Sie auf die Standardeinstellungen für eine Portlet-Registrierung zugreifen, finden Sie in **Kapitel 9**, „**Portletadministration**“, auf Seite 181.

### 17.5.1 Allgemeines zu Standardeinstellungen

Die Standardeinstellungen für das Detail-Portlet befinden sich alle unter einer einzigen *komplexen Einstellung für Details*:



Wenn Sie diese komplexe Einstellung öffnen, erhalten Sie Zugriff auf die einzelnen Detail-Standard Einstellungen:



Diese Standardeinstellungen *gelten nur für den Anzeigemodus* (nicht für den Bearbeitungsmodus). Sie umfassen Folgendes:

Standardeinstellung	Details
Entitätsdefinition	<p>Gibt die Attributliste und das HTML-Layout an, die angezeigt werden sollen, wenn das Detail-Portlet für einen bestimmten Entitätstyp (z. B. Benutzer, Gerät oder Gruppe) verwendet wird.</p> <p>Sie können auf <b>Entitätsdefinition hinzufügen</b> klicken, um die Unterstützung weiterer Entitätstypen durch das Detail-Portlet festzulegen.</p>
Attribute, die aufzulisten sind	<p>Gibt an, welche Attribute der ausgewählten Entität das Portlet anzeigen soll. Diese Attribute werden in der von Ihnen gewählten Reihenfolge aufgeführt.</p> <p>Zum Hinzufügen bzw. Entfernen von Attributen steht eine Schaltfläche zur Verfügung.</p>
HTML-Layout	<p>Bietet eine Schaltfläche zum Öffnen des <b>HTML-Layout-Editors</b>, mit dem Sie den Kopfbereich gestalten können, der im Detail-Portlet für die ausgewählte Entität angezeigt werden soll.</p> <p>Weitere Informationen finden Sie in „<b>Festlegen der Anzeigeelemente im Kopfbereich</b>“ auf Seite 251.</p>

In diesem Kapitel erfahren Sie, wie Sie vorhandene Organigramm-Funktionen in Ihrer Identity Manager-Benutzeranwendung bearbeiten bzw. neue hinzufügen. Es werden folgende Themen erläutert:

- [Abschnitt 18.1, „Allgemeines zum Portlet „Organigramm““](#), auf Seite 263
- [Abschnitt 18.2, „Konfiguration des Portlets „Organigramm““](#), auf Seite 265
- [Abschnitt 18.2.2, „Festlegen von Standardeinstellungen für Organigramme“](#), auf Seite 267

## 18.1 Allgemeines zum Portlet „Organigramm“

Mithilfe des Organigramm-Portlets können Endbenutzer eine grafische Darstellung der hierarchischen Relationen zwischen Objekten im Identitätsdepot anzeigen und durchsuchen. So können Sie beispielsweise Organigramm-Portlets definieren, um die Hierarchie folgender Objekte darzustellen:

- Unternehmen (z. B. Mitarbeiter und Manager)
- Gruppenmitgliedschaft (z. B. alle Mitarbeiter in einer Gruppe)
- Geräte, die einem Benutzer zugeordnet sind (z. B. Mobiltelefone und Notebooks)

In der Standardkonfiguration umfasst die Registerkarte „Identitätsselbstbedienung“ der Identity Manager-Benutzeranwendung die Aktion „Organigramm“. Bei dieser Aktion handelt es sich um ein Organigramm-Portlet, das so konfiguriert ist, dass es die Relationen zwischen den Benutzerobjekten im Identitätsdepot anzeigt. Im folgenden Beispiel wird (unter Verwendung von Beispieldaten) veranschaulicht, wie das standardmäßige Organigramm-Portlet diese Relation darstellt.

The screenshot displays the Novell Identity Manager web interface. The top navigation bar includes the Novell logo, the text "Novell Identity Manager", and the date "Montag, 30. Januar 2006". Below this, a secondary navigation bar shows "Willkommen, Admin" and several menu items: "Identitätsselbstbedienung", "Anforderungen und Genehmigungen", "Administration", "Abmelden", and "Hilfe". A sidebar on the left contains a tree view with categories like "Informationsverwaltung", "Organigramm", "Mein Profil", "Verzeichnissuche", "Passwortadministration", "Herausforderungsantwort", "Verzeichnis-Management", and "Nicht kategorisiert". The main content area is titled "Organigramm" and features a search bar with the placeholder text "Nachschlagen". The organizational chart shows a hierarchy starting with "Jack Miller, President, CEO" at the top. Below him are three direct reports: "Anthony Palini, Chief Operating Officer", "Alison Blake, Creative Assistant", and "Abby Spencer, System Administrator". Each person's card includes a profile picture, name, title, and several small icons representing different attributes or roles.

**Integrierte Links** Das Organigramm-Portlet umfasst die im Folgenden beschriebenen integrierten Links.

Link	Beschreibung
	Ermöglicht es dem Benutzer, zur übergeordneten Ebene zu wechseln. Dieser Link ist nur verfügbar, wenn eine Relation angezeigt wird, bei der die übergeordnete und die untergeordnete Entität übereinstimmen.
	Startet das Detail-Portlet.  Dieser integrierte Link ist über die Standardeinstellungen für das Organigramm-Layout konfigurierbar. Weitere Informationen hierzu finden Sie in <a href="#">„Standardeinstellungen für das Organigramm-Layout“ auf Seite 270</a>
	Zeigt eine Liste mit Organigrammen an. Die Benutzer können ein Organigramm für die Anzeige auswählen.  Diese Organigramm-Liste ist dynamisch. Sie zeigt andere Organigramme mit demselben übergeordneten Entitätstyp an. Wenn Sie beispielsweise ein Manager-Mitarbeiter-Organigramm anzeigen (die übergeordnete Entität ist hier „user“) und auf dieses Symbol klicken, enthält die Liste der anzeigbaren Organigramme nur Relationen, deren übergeordnete Entität ebenfalls „user“ ist.  Dieser integrierte Link ist über die Standardeinstellungen für das Organigramm-Layout konfigurierbar. Weitere Informationen hierzu finden Sie in <a href="#">„Standardeinstellungen für das Organigramm-Layout“ auf Seite 270</a>
	Startet ein Email-Programm, damit Sie folgende Aktionen ausführen können: <ul style="list-style-type: none"> <li>• Die Identitätsdetails des aktuell ausgewählten Benutzers versenden</li> <li>• Eine Email schreiben</li> </ul> Dieser integrierte Link ist über die Standardeinstellungen für das Organigramm-Layout konfigurierbar. Weitere Informationen hierzu finden Sie in <a href="#">„Standardeinstellungen für das Organigramm-Layout“ auf Seite 270</a>
 Nachschlagen	Mithilfe des Links „Nachschlagen“ können Benutzer nach Entitäten suchen. Nach erfolgreichen Suchvorgängen wird die gefundene Entität als oberster Knoten des Organigramms dargestellt.
	Ermöglicht es dem Benutzer, die nächste Unterebene anzuzeigen.

Weitere Informationen zum Hinzufügen von integrierten Links und zum Beschränken des Zugriffs darauf in Ihren Organigrammen finden Sie in [„Standardeinstellungen für das Organigramm-Layout“ auf Seite 270](#).

### 18.1.1 Allgemeines zu Relationen in Organigrammen

Das Organigramm-Portlet zeigt Relationen an, die in der Verzeichnisabstraktionsschicht definiert sind. Nach der Installation der Identity Manager-Benutzeranwendung sind die im Folgenden aufgeführten Relationen verfügbar.

- Gruppenmitgliedschaft

- Manager-Mitarbeiter
- Benutzergruppen

Weitere Informationen zum Erstellen und Bearbeiten von Relationen in Organigrammen finden Sie in [Kapitel 4, „Konfigurieren der Verzeichnisabstraktionsschicht“](#), auf Seite 75.

---

**Hinweis:** Dynamische Gruppen werden nicht vollständig vom Organigramm-Portlet unterstützt. Sie können eine dynamische Gruppe nicht als übergeordnete, aber als untergeordnete Entität in einer Relation definieren.

---

## 18.1.2 Allgemeines zur Anzeige von Organigrammen

Standardmäßig wird das Organigramm innerhalb des Portlet-Rahmens in einem Bereich angezeigt, der durch die Standardeinstellungen für die Portlet-Breite und die Portlet-Höhe festgelegt ist. Benötigt der Inhalt mehr Platz als den festgelegten Bereich, werden die Begrenzungen des Portlets erweitert und somit auch die Seitenhöhe und -breite. Benutzer können ein Organigramm in voller Größe anzeigen, indem sie auf das Symbol zum Maximieren in der Titelleiste des Portlets klicken. (Das Organigramm wird standardmäßig im maximierten Format angezeigt, wenn es vom Detail-Portlet aus aufgerufen wird.)

**Bilder von Benutzern** Das Organigramm-Layout für das Benutzerobjekt umfasst standardmäßig das Attribut „User Photo“. Wenn Ihr Identitätsdepot dieses Attribut jedoch nicht umfasst oder kein Bild vorhanden ist, ignoriert das Organigramm dieses Attribut zur Laufzeit. Wenn Sie Ihre Fotos an einem anderen Ort speichern, können Sie das Organigramm entsprechend konfigurieren.

Weitere Informationen finden Sie in [Abschnitt 18.2.3, „Dynamisches Laden von Bildern“](#), auf Seite 276.

## 18.2 Konfiguration des Portlets „Organigramm“

Gehen Sie zum Konfigurieren des Portlets „Organigramm“ wie folgt vor:

Schritt	Aufgabe	Beschreibung
1	Definieren Sie die anzuzeigende Relation	Sie können eine der vordefinierten Relationen verwenden, die mit der Identity Manager-Benutzeranwendung installiert wurden, oder Sie können Ihre eigene erstellen.  Weitere Informationen zum Definieren einer Relation finden Sie in <a href="#">Kapitel 4, „Konfigurieren der Verzeichnisabstraktionsschicht“</a> , auf Seite 75.
2	Stellen Sie sicher, dass die Entitäten und Attribute, die für die Relation verwendet werden sollen, in der Verzeichnisabstraktionsschicht vorhanden sind	Weitere Informationen zum Definieren einer Relation finden Sie in <a href="#">Abschnitt 18.2.1, „Einrichtung der Verzeichnisabstraktionsschicht“</a> , auf Seite 266.

Schritt	Aufgabe	Beschreibung
3	Legen Sie fest, wo Sie diese Relation anzeigen möchten	<p>Möchten Sie eine neue Seite zum Aufrufen des Organigramms erstellen? Oder möchten Sie das Organigramm vom Detail-Portlet oder von einem anderen Organigramm aus starten?</p> <p>Weitere Informationen zum Erstellen von Seiten und zum Hinzufügen von Portlets zu diesen Seiten finden Sie in <a href="#">Kapitel 7, „Seitenadministration“, auf Seite 137</a>.</p>
4	Legen Sie Standardeinstellungen für das Portlet fest	<p>Mit Standardeinstellungen können Sie Folgendes definieren:</p> <ul style="list-style-type: none"> <li>• Welche Attribute angezeigt werden</li> <li>• Wie diese Attribute angezeigt werden (ihr HTML-Layout)</li> </ul> <p>Weitere Informationen finden Sie in <a href="#">Abschnitt 18.2.2, „Festlegen von Standardeinstellungen für Organigramme“, auf Seite 267</a>.</p>
5	Testen Sie Ihre Einstellungen	Testen Sie die Relationsdefinitionen und das Layout.
6	Richten Sie eDirectory-Rechte ein und erstellen Sie Indizes, die zur Verbesserung der Leistung benötigt werden	<p><b>Effektive Rechte</b> - Benutzer benötigen zum Anzeigen der durch das Portlet definierten Attribute <b>Leserechte</b>.</p> <p><b>Verbesserung der Leistung</b> - Die Leistung der Organigramm-Anzeige kann verbessert werden, indem zum „Child“-Attribut der Relation ein eDirectory-Werteindex hinzugefügt wird, weil das „Child“-Attribut für die LDAP-Suche verwendet wird.</p>

## 18.2.1 Einrichtung der Verzeichnisabstraktionsschicht

Die in einem Organigramm angezeigten Entitäten und Attribute müssen in der Verzeichnisabstraktionsschicht definiert sein. In der folgenden Tabelle sind die Attribute und Eigenschaften aufgeführt, die Sie für die Entitäten und Attribute, die in einem Organigramm angezeigt werden sollen, festlegen müssen.

Definitionsart	Einstellung	Wert
entity	view	Ausgewählt (Wahr)
attribute	read	Ausgewählt (Wahr)
	search	Ausgewählt (Wahr)

**Anforderungen für den Link „Nachschlagen“** Der Link „Nachschlagen“ ermöglicht es Benutzern, im Organigramm zu navigieren, indem sie nach anderen Objekten suchen, die denselben Typ wie der Schlüssel für die übergeordnete Entität aufweisen. Hierfür ist es erforderlich, dass der Schlüssel für die übergeordnete Entität mindestens ein Attribut hat, dessen Zugriffseigenschaften *require* und *search* auf „Wahr“ gesetzt (im Verzeichnisabstraktionsschicht-Editor ausgewählt) sind.

Anderenfalls kann das Dialogfeld „Objektsuche“ des Links „Nachschlagen“ nicht mit Daten ausgefüllt werden und es wird ein leeres Dialogfeld angezeigt.

Weitere Informationen zur Konfiguration von Entitäten und Attributen finden Sie in [Kapitel 4](#), „Konfigurieren der Verzeichnisabstraktionsschicht“, auf Seite 75.

## 18.2.2 Festlegen von Standardeinstellungen für Organigramme

Sie können zwei Typen von Standardeinstellungen festlegen:

- „Standardeinstellungen für Relationen in Organigrammen“ auf Seite 267
- „Standardeinstellungen für das Organigramm-Layout“ auf Seite 270

### Standardeinstellungen für Relationen in Organigrammen

Die Standardeinstellungen für Relationen in Organigrammen sind auf einer einzigen Standardeinstellungsseite zusammengefasst.

**INHALTSEINSTELLUNGEN** Novell Identity Manager

Inhaltseinstellungen für diese Registrierungsinstanz ändern (Organigramm)

Entitäts-Organigramm

	Standardeinst	Wert der Standardeinst		Anf	Schreib-geschützt	Verstecken
<a href="#">Zurücks</a>	Präsentations-Layouts:	<a href="#">Benutzerdefinierte Einstellung anzeigen/bearbeiten</a>		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<a href="#">Zurücks</a>	Relationsschlüssel:	<input type="text" value="user2users"/>	<a href="#">Detail</a>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<a href="#">Zurücks</a>	Schlüssel für übergeordnete Entität:	<input type="text" value="{User/id}"/>	<a href="#">Detail</a>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<a href="#">Zurücks</a>	Standardtiefe:	<input type="text" value="1"/>	<a href="#">Detail</a>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<a href="#">Zurücks</a>	Max. Tiefe:	<input type="text" value="10"/>	<a href="#">Detail</a>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<a href="#">Zurücks</a>	Portlet-Breite:	<input type="text" value="700"/>	<a href="#">Detail</a>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<a href="#">Zurücks</a>	Portlet-Höhe:	<input type="text" value="400"/>	<a href="#">Detail</a>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<a href="#">Zurücks</a>	Bildlaufleisten anzeigen:	<input type="radio"/> Wahr <input checked="" type="radio"/> Falsch	<a href="#">Detail</a>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<a href="#">Zurücks</a>	Organigramm-Skin:	<input type="text" value="Business Card"/>	<a href="#">Detail</a>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Auswahl

Wert	Anzeigen
Card	<input type="checkbox"/>
Business Ca	<input checked="" type="checkbox"/>
<a href="#">Einfüg</a>	<a href="#">Entf</a>

---

Zurücks
Linien mit Elementen verbinden:  Wahr  Falsch
[Detail](#)

---

Zurücks
Zeitüberschreitung bei Menü: 
[Detail](#)

---

Zurücks
Baumpräsentation:   
[Detail](#)

---

Zurücks
Blattpräsentation: 
[Detail](#)

Auswahl	
Wert	Anzeigen
<input type="text" value="0"/>	Vertical List <input type="button" value="Einfg Entf"/>
<input type="text" value="1"/>	Vertical List <input type="button" value="Einfg Entf"/>
<input type="text" value="2"/>	Horizontal L <input type="button" value="Einfg Entf"/>
<input type="text" value="3"/>	Horizontal L <input type="button" value="Einfg Entf"/>

---

Zurücks
Mindestbreite für Elemente: 
[Detail](#)

---

Zurücks
Mindesthöhe für Elemente: 
[Detail](#)

---

Zurücks
Trennzeichen bei mehreren Werten: 
[Detail](#)

### Standardeinstellung

### Vorgehensweise

Präsentations-Layouts

Klicken Sie auf „Benutzerdefinierte Einstellung anzeigen/bearbeiten“, um auf die Layout-Standardinstellungen zuzugreifen. Diese werden unter „**Standardeinstellungen für das Organigramm-Layout**“ auf Seite 270 beschrieben.

Relationsschlüssel

Geben Sie den Relationsschlüssel ein. Dieser Wert muss mit einem der in der Verzeichnisabstraktionsschicht angegebenen Relationsschlüssel übereinstimmen.

Standardeinstellung	Vorgehensweise
Schlüssel für übergeordnete Entität	<p>Geben Sie den DN der Entität ein, die den Stammknoten des anzuzeigenden Organigramms darstellt, oder geben Sie <code>#{User/id}</code> ein, um das Organigramm des aktuellen Benutzers anzuzeigen. (Der Parameter <code>#{User/id}</code> wird als DN des aktuellen Benutzers aufgelöst.)</p> <p>Wenn dieser Wert nicht innerhalb der durch die Suchstamm-Eigenschaft in der Verzeichnisabstraktionsschicht festgelegten Knoten liegt, tritt bei der LDAP-Suche ein Fehler auf.</p> <p>Beispiele für gültige DNs (unter Verwendung von Beispieldaten):</p> <ul style="list-style-type: none"> <li>• Wenn Sie den <code>user2users</code>-Relationsschlüssel mit dem Mitarbeiter „Jack Miller“ als Stammknoten des Organigramms anzeigen möchten, müssen Sie Folgendes eingeben:</li> </ul> <pre>cn=jmiller,ou=users,ou=sample,o=novell</pre> <ul style="list-style-type: none"> <li>• Wenn Sie den <code>group2users</code>-Relationsschlüssel mit der Gruppe „Buchhaltung“ als Stammknoten anzeigen möchten, müssen Sie Folgendes angeben:</li> </ul> <pre>cn=Buchhaltung,ou=groups,ou=sample,o=novell</pre>
Standardtiefe	<p>Gibt die Tiefe des Organigramms bei der ersten Anzeige an.</p> <ul style="list-style-type: none"> <li>• 0 - Nur Stammknoten anzeigen</li> <li>• 1 - Stammknoten und direkt untergeordnete Knoten anzeigen</li> <li>• 2 - Stammknoten und untergeordnete Knoten erster und zweiter Ebene anzeigen</li> </ul> <p>Dasselbe Prinzip gilt für weitere Ebenen. Wenn dieser Wert den Wert der maximalen Tiefe (siehe unten) übersteigt, hat der Wert für die maximalen Tiefe Vorrang.</p>
Max. Tiefe	<p>Gibt die maximale Tiefe der Unterebenen an, die ein Benutzer in einem Organigramm anzeigen kann. Hierbei handelt es sich nicht um die Möglichkeit, ein Organigramm navigieren zu können, einen Vorgang, der durch effektive Rechte beschränkt wird.</p>
Organigramm-Skin	<p>Visitenkarte</p> <p>eGuide</p> <p>Novell.com</p> <p>Wired</p> <p>True Blue</p>

Standardeinstellung	Vorgehensweise
Linien mit Elementen verbinden	Legt fest, ob die Karten des Organigramms durch Linien verbunden sind. Die Option „Falsch“ bedeutet, dass keine Linien eingefügt werden.
Zeitüberschreitung bei Menü	Anzahl der Millisekunden, bis das aktuell angezeigte Menü für integrierte Links ausgeblendet wird.
Baumpräsentation	<p>Definiert die Ausrichtung, Verteilung und Darstellung des Organigramms pro Tiefenbereich.</p> <p>Die ersten <math>n</math> Werte definieren die Ausrichtung, Verteilung und Darstellung für die Ebenen von 0 bis <math>n-1</math>. Der letzte Wert wird fortlaufend für die Ebenen ab <math>n</math> verwendet. Die Werte müssen zwischen 0 und 5 liegen.</p> <p>Gültige Werte:</p> <ul style="list-style-type: none"> <li>0: Positionskarte über einer vertikalen Elementliste</li> <li>1: Linie über einer vertikalen Elementliste</li> <li>2: Positionskarte über einer horizontalen Elementliste</li> <li>3: Linie über einer horizontalen Elementliste</li> <li>4: Positionskarte vor einer vertikalen Elementliste</li> <li>5: Linie vor einer vertikalen Elementliste</li> </ul>
Blattpräsentation	Gibt die Ausrichtung, Verteilung und Darstellung für die maximale Unterebenenanzahl einer Organigramm-Verzweigung an.
Mindestbreite für Elemente	Dieser Wert sollte $\text{round}(\text{'Mindesthöhe des Elements'} * 1,618)$ entsprechen.
Mindesthöhe für Elemente	Dieser Wert sollte $\text{round}(\text{'Mindestbreite des Elements'} / 1,618)$ entsprechen.
Trennzeichen bei Attributen mit mehreren Werten	Das Zeichen, das als Trennzeichen für Attribute mit mehreren Werten verwendet wird.

### Standardeinstellungen für das Organigramm-Layout

Über die Standardeinstellungen für das Organigramm-Layout können Sie das HTML-Layout für die Anzeige von Organigramm-Einträgen festlegen. Für präzisere Bearbeitungen können Sie einen

HTML-Editor Ihrer Wahl verwenden. Weitere Informationen hierzu finden Sie unter „So verwenden Sie einen externen Editor“ auf Seite 276.

INHALTSEINSTELLUNGEN

Novell Identity Manager

Inhaltseinstellungen für diese Registrierungsinstanz ändern (Organigramm)

Entitäts-Organigramm

Presentation Layouts

Org Chart

Zusammenfassung

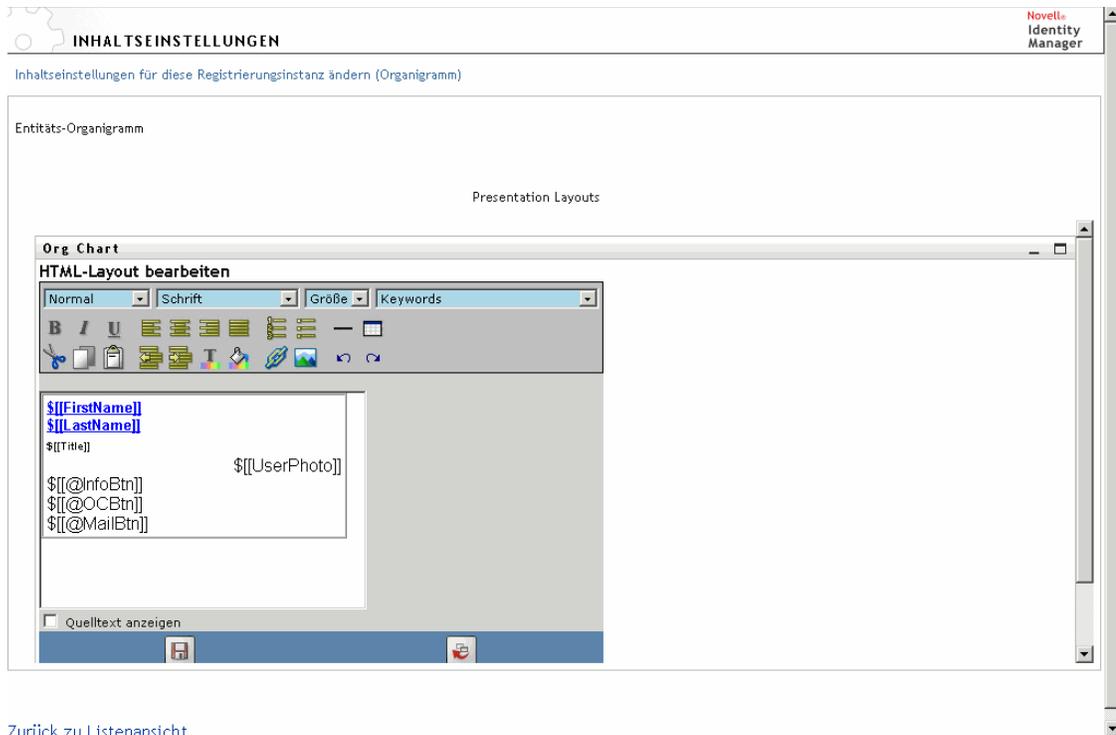
Entitätsdefinition	Benutzer
HTML-Layout für Visitenkarten	<code>[[FirstName]]</code> <code>[[LastName]]</code> <code>[[Title]]</code> <code>[[UserPhoto]]</code> <code>[[@InfoBtn]]</code> <code>[[@OCBtn]]</code> <code>[[@MailBtn]]</code>
HTML-Layout für einfache Anzeige	<code>[[FirstName]] [[LastName]] - [[Title]]</code>

[Zurück zu Listenansicht](#)

*HTML-Layout für Visitenkarten* - das Standard-Layout.

*HTML-Layout für einfache Anzeige* - das Layout, das angezeigt wird, wenn die Standardeinstellung für die Baumpräsentation auf 1 gesetzt ist.

**HTML-Editor** Sie können den HTML-Editor öffnen, indem Sie auf die Schaltfläche zum Bearbeiten klicken. Der HTML-Editor sieht wie folgt aus:



## Verwendung des HTML-Editors

Der HTML-Editor bietet eine WYSIWYG-Oberfläche, mit der Sie das Layout der Blätter des Organigramms festlegen können. Er bietet die üblichen Funktionen eines HTML-Editors zum Festlegen der Formatierung von Text und Listen, zum Einfügen von Anker und Bildern usw. Mithilfe der Dropdown-Liste *Schlüsselwörter* können Sie Attribute, Befehle und Navigations-URLs im Layoutbereich einfügen. Wenn Sie ein Schlüsselwort aus der Dropdown-Liste auswählen, wird es mit der passenden Syntax eingefügt. Sie können jedoch auch HTML-Code im Layoutbereich eingeben.

**Schlüsselwörter** Beim Erstellen Ihres Layouts können Sie die Dropdown-Liste mit den Schlüsselwörtern verwenden, um Variablen einzusetzen, die zur Laufzeit durch spezifische Attributwerte ersetzt werden. Alternativ können Sie unter Verwendung der folgenden Syntax auf sie verweisen:

```
${[Schlüsselwort]}
```

Dabei steht *Schlüsselwort* für den Wert einer Entität wie „LastName“.

Es ist möglich, Attribute mithilfe der folgenden Syntax zu verketteten:

```
${[Schlüsselwort+Schlüsselwort]}
```

Zum Beispiel:

```
${[FirstName+LastName]}
```

Dabei können Sie beliebig viele Attribute miteinander verketteten und darüber hinaus in Anführungszeichen eingeschlossenen Textstrings eingeben:

```
$[[Schlüsselwort+"Beispieltext"+Schlüsselwort]]
```

Hierdurch werden die Werte der Schlüsselwörter und der in Anführungszeichen stehende Text angezeigt.

---

**Hinweis:** Wenn ein Schlüsselwort in einem Layout falsch geschrieben ist, wird es im Organigramm als Textstring angezeigt (einschließlich \$[[ ]]).

---

**Verwendung der Funktionen des HTML-Editors und der Schlüsselwörter** So verwenden Sie die Funktionen des HTML-Editors und die Dropdown-Liste mit den Schlüsselwörtern:

---

<b>Funktion</b>	<b>Tipp</b>
Schaltfläche zum Einfügen von Links	<p>So fügen Sie einen Link ein:</p> <p><b>In Mozilla:</b></p> <ol style="list-style-type: none"><li>1. Markieren Sie den Text, den Sie in einen Hyperlink umwandeln möchten, und klicken Sie auf die Schaltfläche zum <b>Einfügen von Links</b>.</li><li>2. Geben Sie die URL ein und klicken Sie auf <b>Link erstellen</b>.</li><li>3. Speichern Sie die Standardeinstellungen.</li></ol> <p><b>In Internet Explorer:</b></p> <ol style="list-style-type: none"><li>1. Klicken Sie auf die Schaltfläche zum Einfügen von Links.</li><li>2. Geben Sie die URL im Popup-Fenster ein.</li><li>3. Markieren Sie den Text, den Sie in einen Hyperlink umwandeln möchten, und klicken Sie auf <b>Link erstellen</b> (im Popup-Fenster).</li><li>4. Speichern Sie die Standardeinstellungen.</li></ol> <hr/> <p><b>Hinweis:</b> Wenn sich das Bild oder die URL im linken oberen Quadranten des HTML-Editors befindet, führt dies zu einer Überlappung durch das Popup-Fenster. Da das Popup-Fenster nicht verschoben werden kann, müssen Sie den gewünschten Text an einer anderen Stelle im Editor erstellen, anschließend ausschneiden und am richtigen Ort einfügen.</p> <hr/>

Funktion	Tipp
Schaltfläche „Grafik hinzufügen“	<p><b>In Mozilla:</b></p> <ol style="list-style-type: none"> <li>1. Platzieren Sie den Mauszeiger an der Stelle, an der Sie ein Bild einfügen möchten, und klicken Sie auf <b>Grafik hinzufügen</b>.</li> <li>2. Geben Sie die URL und den Text ein und klicken Sie anschließend auf <b>Bild erstellen</b> im Popup-Fenster.</li> <li>3. Speichern Sie die Standardeinstellungen.</li> </ol> <p><b>In Internet Explorer:</b></p> <ol style="list-style-type: none"> <li>1. Klicken Sie auf <b>Grafik hinzufügen</b>.</li> <li>2. Geben Sie die URL und den Text im Popup-Fenster ein und platzieren Sie anschließend den Mauszeiger an der Stelle, an der Sie das Bild einfügen möchten. Klicken Sie dann auf <b>Bild erstellen</b> im Popup-Fenster.</li> <li>3. Speichern Sie die Standardeinstellungen.</li> </ol> <hr/> <p><b>Hinweis:</b> Wenn sich das Bild oder die URL im linken oberen Quadranten des HTML-Editors befindet, führt dies zu einer Überlappung durch das Popup-Fenster. Da das Popup-Fenster nicht verschoben werden kann, müssen Sie den gewünschten Text an einer anderen Stelle im Editor erstellen, anschließend ausschneiden und am richtigen Ort einfügen.</p>
Schlüsselwort-Dropdown-Liste: Attribute	Eine Liste der Attribute, die für diese Entität zur Verfügung stehen.
Schlüsselwort-Dropdown-Liste: Befehle	<p>Mithilfe dieser Befehle kann das Organigramm-Portlet weitere Identitäts-Portlets oder integrierte Funktionen wie IM- oder Email-Werkzeuge starten.</p> <ul style="list-style-type: none"> <li>• <b>IM-Aktionsschaltfläche</b> - Erstellt eine Schaltfläche zum Senden von IMs</li> <li>• <b>Mail-Aktionsschaltfläche</b> - Erstellt eine Schaltfläche zum Senden von Emails</li> <li>• <b>Organigramm-Aktionsschaltfläche</b> - Erstellt eine Schaltfläche zum Wechseln zu einer anderen Relation, die der ausgewählten Entitätsinstanz unmittelbar untergeordnet ist</li> <li>• <b>Info-Aktionsschaltfläche</b> - Startet das Detail-Portlet</li> </ul> <p>Beispiele der Schaltflächen, die generiert werden, finden Sie in <a href="#">„Integrierte Links“ auf Seite 264</a>.</p>

Funktion	Tipp
URLs	<p data-bbox="479 262 1299 409"><b>Link „Organigramm-Navigations-URL“</b> - Ermöglicht es Ihnen, eine URL oder ein Entitätsattribut anzugeben, die bzw. das als Link angezeigt wird. Wenn ein Benutzer auf den Link klickt, wird die Anzeige des Organigramm-Portlets aktualisiert und die Entität, auf die geklickt wurde, wird als Stammknoten angezeigt.</p> <p data-bbox="479 430 1299 451"><b>Einschränkung:</b></p> <p data-bbox="479 472 1299 556">Dies gilt nur, wenn der Objekttyp der übergeordneten und untergeordneten Entität einer Relation identisch ist. In einer Manager-Mitarbeiter-Relation lauten beispielsweise beide „user“.</p> <p data-bbox="479 577 1299 598"><b>Tipps zur Verwendung:</b></p> <p data-bbox="479 619 1299 661">Dieses Schlüsselwort verwenden Sie wie folgt:</p> <ol data-bbox="503 682 1299 787" style="list-style-type: none"> <li>1. Klicken Sie auf „Quelltext anzeigen“.</li> <li>2. Geben Sie das Schlüsselwort „@NavUrl“ unter Verwendung der folgenden Syntax ein:</li> </ol> <pre data-bbox="479 829 1299 892">&lt;a href="javascript:\$ [[@NavUrl]] "&gt;beliebigerText&lt;/a&gt;</pre> <p data-bbox="479 913 1299 1018">Dabei steht <i>beliebigerText</i> für den Link, der zur Laufzeit angezeigt werden soll, oder für ein Entitätsattribut. Im folgenden Beispiel wird <b>Hier klicken</b> zu einem Link, auf den geklickt werden kann.</p> <pre data-bbox="479 1060 1299 1102">&lt;a href="javascript:\$ [[@NavUrl]] "&gt;Hier klicken&lt;/a&gt;</pre> <p data-bbox="479 1123 1299 1186">Im folgenden Beispiel wird das Attribut „FirstName“ zu einem Link, auf den geklickt werden kann:</p> <pre data-bbox="479 1228 1299 1291">&lt;a href="javascript:\$ [[@NavUrl]] "&gt;\$ [[FirstName]]&lt;/a&gt;</pre> <p data-bbox="479 1312 1299 1333"><b>Einschränkungen:</b></p> <p data-bbox="479 1354 1299 1396">Mit Internet Explorer können Sie die folgende Syntax <b>nicht</b> verwenden:</p> <pre data-bbox="479 1438 1299 1480">&lt;a href="\$ [[@NavUrl]] "&gt;beliebigerText&lt;/a&gt;</pre> <p data-bbox="479 1501 1299 1522">Während des Speicherns fügt Internet Explorer Folgendes hinzu:</p> <pre data-bbox="479 1575 1299 1617">http://Kontext vor \$ [[@NavUrl]]</pre> <p data-bbox="479 1638 1299 1659">Das bedeutet, dass</p> <pre data-bbox="479 1711 1299 1753">&lt;a href="\$ [[@NavUrl]] "&gt;beliebigerText&lt;/a&gt;</pre> <p data-bbox="479 1774 1299 1795">zu</p> <pre data-bbox="479 1848 1299 1911">&lt;a href="http://localhost/.../ \$ [[@NavUrl]] "&gt;beliebigerText&lt;/a&gt;</pre> <p data-bbox="479 1932 1299 1963">wird und zur Laufzeit <b>nicht</b> korrekt angezeigt wird.</p>

Funktion	Tipp
	<p><b>Org Chart Navigation Click Link</b> - Zum Einfügen eines Ereignisses vom Typ „onClick“. (Ermöglicht es, dass nur der Bereich des Organigramm-Portlets und nicht die gesamte Seite aktualisiert wird.)</p> <p><b>Tipps zur Verwendung:</b></p> <p>Dieses Schlüsselwort verwenden Sie wie folgt:</p> <ol style="list-style-type: none"> <li>1. Klicken Sie auf „Quelltext anzeigen“.</li> <li>2. Geben Sie das Schlüsselwort „@NavClick“ unter Verwendung der folgenden Syntax ein:</li> </ol> <pre>&lt;A href="javascript:return false;" onClick="§ [[@NavClick]] "&gt;§ [[BeliebigesAttribut]] &lt;/ A&gt;</pre> <p>Dabei steht <i>BeliebigesAttribut</i> für ein Entitätsattribut, das zu einem Link wird, auf den geklickt werden kann.</p> <p>Der String "javascript:return false;" ist erforderlich. Ist er nicht vorhanden, tritt ein Fehler auf.</p>

Klicken Sie zum Speichern der definierten Layouts auf *Senden*.

**So verwenden Sie einen externen Editor** Wenn Sie einen externen HTML-Editor verwenden möchten, haben Sie folgende Möglichkeiten:

- 1 Erstellen Sie den HTML-Quelltext für die Entitätsattribute, Befehle und Schlüsselwörter mithilfe des in den Standardeinstellungen verfügbaren HTML-Layout-Editors.
- 2 Kopieren Sie den HTML-Quelltext in einen Editor Ihrer Wahl.
- 3 Nehmen Sie die gewünschten Änderungen vor.
- 4 Kopieren Sie den HTML-Quelltext nach dem Bearbeiten zurück in den HTML-Layout-Editor.

### 18.2.3 Dynamisches Laden von Bildern

Um im Identitätsdepot gespeicherte Bilder, beispielsweise Benutzerfotos, anzuzeigen, können Sie den Attributnamen in die Visitenkarte einfügen. Wenn Sie beispielsweise das Attribut „User Photo“ in das Visitenkarten-Layout einfügen, wird das Foto des Benutzers angezeigt.

Wenn Sie Bilder außerhalb des Identitätsdepots speichern, müssen Sie das Tag „IMG:“ im *Modus „Quelltext anzeigen“* des HTML-Editors wie folgt verwenden:

- 1 Wechseln Sie zu den Standardeinstellungen des Organigramm-Portlets und öffnen Sie den HTML-Editor.
- 2 Klicken Sie auf *Quelltext anzeigen*.
- 3 Geben Sie unter Verwendung des Tags „IMG:“ eine Kombination aus Speicherort, Attributsschlüssel und Dateierweiterung ein. Verwenden Sie dabei folgende Syntax:

```
§ [[IMG:"URL" + Attributsschlüssel + "Dateierweiterung"]]
```

Im folgenden Beispiel sehen Sie die Syntax, die Sie verwenden müssen, wenn Sie die Fotos Ihrer Mitarbeiter als JPG-Dateien nach Nachnamen geordnet im Unterverzeichnis „/images“ Ihres Anwendungsservers gespeichert haben:

```
[[IMG:"http://meinhost:8080/images/"+LastName+".jpg"]]
```

Zur Laufzeit verkettet das Organigramm-Portlet die URL mit dem Attribut „LastName“ und der Dateierweiterung „.jpg“.

Der HTML-Editor unterstützt eine flexible Syntax. Er unterstützt eine beliebige Kombination aus Text und Attributen, beispielsweise:

```
[[IMG:"beliebiger Text" + Attributschlüssel + ...]]
```



In diesem Kapitel erfahren Sie, wie Sie die Funktionen zur Passwortselbstbedienung und zur Benutzerauthentifizierung in Ihre Identity Manager-Benutzeranwendung integrieren. Es werden folgende Themen erläutert:

- [Abschnitt 19.1, „Vorbereitung für die Passwortverwaltung“, auf Seite 279](#)
- [Abschnitt 19.2, „Allgemeines zu Passwort-Portlets“, auf Seite 282](#)
- [Abschnitt 19.3, „Portlet für die IDM-Anmeldung“, auf Seite 284](#)
- [Abschnitt 19.4, „Portlet „IDM-Herausforderungsantwort“, auf Seite 285](#)
- [Abschnitt 19.5, „Portlet „IDM - Hinweisdefinition“, auf Seite 287](#)
- [Abschnitt 19.6, „Portlet „IDM - Passwort ändern“, auf Seite 288](#)
- [Abschnitt 19.7, „Portlet „IDM - Passwort vergessen“, auf Seite 290](#)

## 19.1 Vorbereitung für die Passwortverwaltung

Vor dem Hinzufügen der Integration der Passwortselbstbedienung und der Benutzerauthentifizierung zu einer Identity Manager-Benutzeranwendung müssen Sie über folgende Kenntnisse verfügen:

- [Abschnitt 19.1.1, „Allgemeines zu den Funktionen der Passwortverwaltung“, auf Seite 279](#)
- [Abschnitt 19.1.2, „Erforderliches Setup in eDirectory“, auf Seite 279](#)

### 19.1.1 Allgemeines zu den Funktionen der Passwortverwaltung

Die von einer Identity Manager-Benutzeranwendung unterstützten Funktionen zur Passwortverwaltung umfassen die *Benutzerauthentifizierung* und die *Passwortselbstbedienung*. Wenn Sie diese Funktionen einsetzen, verfügt Ihre Anwendung über folgende Möglichkeiten:

- Eingabeaufforderung für *Anmeldeinformationen* (Benutzername und Passwort) zur Authentifizierung bei Novell eDirectory
- Selbstbedienung für Benutzer bei der *Passwortänderung*
- Selbstbedienung für Benutzer bei *vergessenen Passwörtern* (einschließlich Eingabeaufforderung für Herausforderungsantworten, Anzeigen eines Passworthinweises oder bei Bedarf Zulassen einer Passwortänderung)
- Selbstbedienung für Benutzer bei der *Herausforderungsfrage*
- Selbstbedienung für Benutzer beim *Passworthinweis*

### 19.1.2 Erforderliches Setup in eDirectory

Bevor Sie die meisten Funktionen zur Passwortselbstbedienung und zur Benutzerauthentifizierung verwenden können, müssen Sie in eDirectory folgende Einstellungen vornehmen:

- *Universelles Passwort* aktivieren
- Eine oder mehrere *Passwortrichtlinien* erstellen

- *Benutzern* die entsprechenden Passwortrichtlinien zuweisen

Eine Passwortrichtlinie ist eine Sammlung von vom Administrator festgelegten Regeln, die die Kriterien für das Erstellen und Ersetzen von Benutzerpasswörtern festlegen. Novell Identity Manager nutzt *NMAS* (Novell Modular Authentication Service) zum Durchsetzen von Passwortrichtlinien, die Sie Benutzern in eDirectory zuweisen.

Für die Ausführung der erforderlichen Setup-Schritte können Sie *Novell iManager* verwenden. Im Folgenden finden Sie ein Beispiel für die Definition der DocumentationPassword-Richtlinie in iManager.

The screenshot shows the Novell iManager administration interface. The left sidebar contains a tree view of system components, with 'Passwörter' (Passwords) selected. The main window displays the configuration for a password policy named 'Sample Password Policy'. The 'Universelles Passwort' (Universal Password) section is active, showing various options and rules with their respective status (True/False).

**Passwortrichtlinie:** Sample Password Policy, Password Policies, Security

Die Richtlinie hat die folgenden Einstellungen:

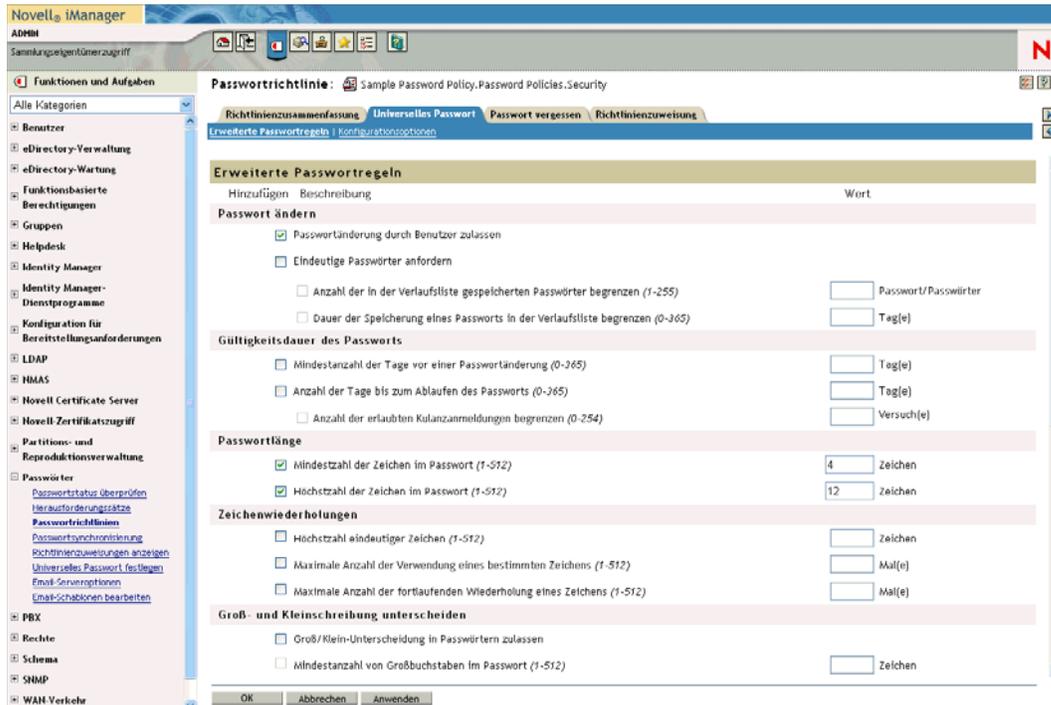
Zuletzt geändert: 05.01.06

Zusammenfassung der Passwortrichtlinien		
Name	Sample	
Beschreibung		
<b>Universelles Passwort</b>		
Optionen	<ul style="list-style-type: none"> <li>Universelles Passwort aktivieren: Wahr</li> <li>Erweiterte Passwortregeln aktivieren: Wahr</li> <li>NDS-Passwort bei Auswahl des universellen Passworts entfernen: Falsch</li> <li>NDS-Passwort bei Auswahl des universellen Passworts synchronisieren: Wahr</li> <li>Einfaches Passwort bei Auswahl des universellen Passworts synchronisieren: Falsch</li> <li>Benutzer darf Passwort abrufen: Falsch</li> <li>Administrator darf Passwörter abrufen: Falsch</li> <li>Verteilungspasswort bei Auswahl des universellen Passworts synchronisieren: Falsch</li> <li>Überprüfen, ob vorhandene Passwörter der Passwortrichtlinie entsprechen (erfolgt bei der Anmeldung): Falsch</li> </ul>	
Regeln	<ul style="list-style-type: none"> <li>Passwortänderung durch Benutzer zulassen: Wahr</li> <li>Eindeutige Passwörter anfordern: Falsch</li> <li>Mindestzahl der Zeichen im Passwort: 4</li> <li>Höchstzahl der Zeichen im Passwort: 12</li> <li>Numerische Zeichen in Passwörtern zulassen: Wahr</li> <li>Erstes Zeichen darf nicht numerisch sein: Falsch</li> <li>Letztes Zeichen darf nicht numerisch sein: Falsch</li> <li>Sonderzeichen im Passwort zulassen: Wahr</li> <li>Erstes Zeichen darf kein Sonderzeichen sein: Falsch</li> <li>Letztes Zeichen darf kein Sonderzeichen sein: Falsch</li> </ul>	
<b>Passwort vergessen</b>	Aktiviert:	Falsch
<b>Richtlinienzweisungen</b>		

Buttons: OK, Abbrechen, Anwenden

Diese Passwortrichtlinie legt Folgendes fest:

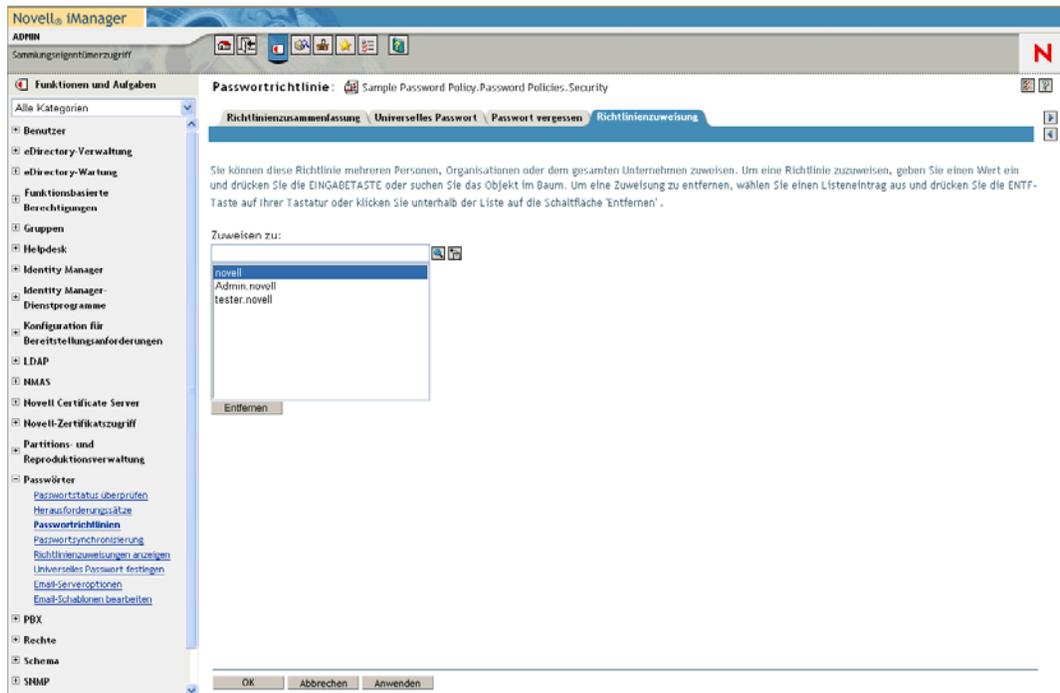
- Einstellungen für das *universelle Passwort*



- Einstellungen für die Vorgehensweise bei einem *vergessenen Passwort*



- *Zuweisungen*, die die Richtlinie für bestimmte Benutzer in Kraft setzt



Weitere Informationen zum Einrichten eines universellen Passworts und von Passwortrichtlinien in eDirectory finden Sie im [Novell Identity Manager-Administrationshandbuch](http://www.novell.com/documentation/dirxml20/index.html) (<http://www.novell.com/documentation/dirxml20/index.html>).

## 19.2 Allgemeines zu Passwort-Portlets

Verwenden Sie folgende Portlets, um die Funktionen zur Passwortselbstbedienung und zur Benutzerauthentifizierung in Ihrer Identity Manager-Benutzeranwendung zu implementieren:

Portlet	Beschreibung
<a href="#">Abschnitt 19.3, „Portlet für die IDM-Anmeldung“, auf Seite 284</a>	Die IDM-Anmeldung bietet eine zuverlässige Benutzerauthentifizierung, die von Identity Manager unterstützt wird (durch das universelle Passwort, Passwortrichtlinien und NMAS). Das Portlet für die IDM-Anmeldung leitet während des Anmeldevorgangs bei Bedarf an andere Passwort-Portlets um.
<a href="#">Abschnitt 19.4, „Portlet „IDM-Herausforderungsantwort“, auf Seite 285</a>	Mit diesem Selbstbedienungs-Portlet können Benutzer: <ul style="list-style-type: none"> <li>• Gültige Antworten auf vom Administrator definierte Herausforderungsfragen sowie benutzerdefinierte Herausforderungsfragen und -antworten einrichten</li> <li>• Gültige Antworten auf vom Administrator definierte Herausforderungsfragen sowie benutzerdefinierte Herausforderungsfragen und -antworten ändern</li> </ul>

Portlet	Beschreibung
Abschnitt 19.5, „Portlet „IDM - Hinweisdefinition“, auf Seite 287	Über dieses Selbstbedienungs-Portlet können Benutzer ihren Passworthinweis ändern (der bei vergessenem Passwort als Hinweis angezeigt oder per Email zugesendet werden kann).
Abschnitt 19.6, „Portlet „IDM - Passwort ändern“, auf Seite 288	Über dieses Selbstbedienungs-Portlet können Benutzer ihr universelles Passwort gemäß der zugewiesenen Passwortrichtlinie ändern (zurücksetzen). Es verwendet diese Richtlinie für die Anzeige der Regeln, die das neue Passwort einhalten muss.  Wenn die Funktion „Universelles Passwort“ nicht aktiviert ist, ändert dieses Portlet entsprechend den Passwortbeschränkungen des Benutzers das (einfache) eDirectory-Passwort des Benutzers.
Abschnitt 19.7, „Portlet „IDM - Passwort vergessen“, auf Seite 290	Der Benutzer erhält über dieses Selbstbedienungs-Portlet mittels Herausforderungs-/Antwortauthentifizierung Informationen zu seinem Passwort (von NMAS). Das Ergebnis ist abhängig von der zugewiesenen Passwortrichtlinie und kann Folgendes enthalten: <ul style="list-style-type: none"> <li>• Anzeige des Passworthinweises des Benutzers auf dem Bildschirm</li> <li>• Versenden des Hinweises per Email an den Benutzer</li> <li>• Versenden des Passworts an den Benutzer</li> <li>• Eingabeaufforderung zum Zurücksetzen (Ändern) des Passworts</li> </ul>

## 19.2.1 Portlet-Modi bei der Passwortselbstbedienung

Die Portlets für die Passwortselbstbedienung („IDM-Herausforderungsantwort“, „IDM - Hinweisdefinition“ und „IDM - Passwort ändern“) können in einem der beiden folgenden Modi ausgeführt werden:

Modus	Beschreibung	Laufzeitverhalten
Eigenständiger Modus	Portlets werden auf freigegebenen Seiten eigenständig ausgeführt.	<ul style="list-style-type: none"> <li>• Wenn das Portlet <b>erfolgreich</b> ausgeführt wird, zeigt es eine Erfolgsmeldung mit einem Link an, über den die Operation erneut ausgeführt werden kann.</li> <li>• Wenn ein Portlet <b>nicht erfolgreich</b> ist, zeigt es im vorhandenen Formular eine Fehlermeldung an.</li> </ul>
Delegierungsmodus	Portlets werden als Ergebnis einer Validierungsprüfung bei der Anmeldung auf der Seite angezeigt.	<ul style="list-style-type: none"> <li>• Wenn ein Portlet <b>erfolgreich</b> ausgeführt wird, wird der Benutzer an ein anderes Portlet oder zur Hauptseite der Benutzeranwendung umgeleitet. Es wird keine Erfolgsmeldung angezeigt.</li> <li>• Wenn ein Portlet <b>nicht erfolgreich</b> ist, zeigt es im vorhandenen Formular eine Fehlermeldung an.</li> </ul>

## 19.3 Portlet für die IDM-Anmeldung

Das Portlet für die IDM-Anmeldung führt eine zuverlässige Benutzerauthentifizierung aus, die von Identity Manager unterstützt wird (durch das universelle Passwort, Passwortrichtlinien und NMAS). Das Portlet für die IDM-Anmeldung leitet während des Anmeldevorgangs bei Bedarf an andere Passwort-Portlets um.



### 19.3.1 Anforderungen

Für das Portlet zur IDM-Anmeldung gelten folgende Anforderungen:

Thema	Anforderungen
Passwortrichtlinie	Für dieses Portlet ist keine Passwortrichtlinie erforderlich, es sein denn, Sie möchten erweiterte Passwortregeln verwenden oder lassen zu, dass Benutzer auf den Link <b>Passwort vergessen</b> klicken können.
Universelles Passwort	Für dieses Portlet muss die Funktion „Universelles Passwort“ nicht aktiviert sein, es sein denn, Sie möchten eine Passwortrichtlinie mit erweiterten Passwortregeln verwenden.
SSL	Dieses Portlet verwendet SSL, daher sollten Sie sich vergewissern, dass Ihr Anwendungsserver ordnungsgemäß konfiguriert ist und die SSL-Verbindungen zu Ihrem LDAP-Realm unterstützt.

### 19.3.2 Verwendung

Wenn Sie das Portlet für die IDM-Anmeldung verwenden möchten, sollten Sie sich mit Folgendem auskennen:

- „So leitet das Portlet für die IDM-Anmeldung an andere Portlets weiter“ auf Seite 284
- „Verwendung von Kulanzanmeldungen“ auf Seite 285

#### So leitet das Portlet für die IDM-Anmeldung an andere Portlets weiter

Während der Laufzeit leitet das Portlet für die IDM-Anmeldung entsprechend den Anforderungen für die Beendigung des Anmeldevorgangs an andere Passwort-Portlets um. Zum Beispiel:

Wenn der Benutzer	leitet die IDM-Anmeldung um zu
Auf den Link <b>Passwort vergessen</b> klickt	Abschnitt 19.7, „Portlet „IDM - Passwort vergessen““, auf Seite 290
Herausforderungsfragen und -antworten einrichten möchte	Abschnitt 19.4, „Portlet „IDM-Herausforderungsantwort““, auf Seite 285
Seinen Passworthinweis einrichten möchte	Abschnitt 19.5, „Portlet „IDM - Hinweisdefinition““, auf Seite 287
Ein ungültiges Passwort zurücksetzen möchte	Abschnitt 19.6, „Portlet „IDM - Passwort ändern““, auf Seite 288

## Verwendung von Kulanzanmeldungen

Wenn Sie eine Kulanzanmeldung verwenden, zeigt das Portlet für die IDM-Anmeldung eine Warnmeldung an, die Sie zur Änderung Ihres Passworts auffordert und die Anzahl der verbleibenden Kulanzanmeldungen anzeigt. Bei Ihrem letzten Anmeldeversuch leitet Sie das Portlet für die IDM-Anmeldung zum Portlet „IDM - Passwort ändern“ um.

## 19.4 Portlet „IDM-Herausforderungsantwort“

Mit diesem Selbstbedienungs-Portlet können Benutzer:

- Gültige Antworten auf vom Administrator definierte Herausforderungsfragen sowie benutzerdefinierte Herausforderungsfragen und -antworten einrichten
- Gültige Antworten auf vom Administrator definierte Herausforderungsfragen sowie benutzerdefinierte Herausforderungsfragen und -antworten ändern

**IDM-Herausforderungsantwort** ? \_ □

Herausforderungsantwort

Diese Fragen sind Ihrer Passwortrichtlinie zugewiesen. Geben Sie für alle administratordefinierten Fragen eine Antwort an. Erstellen Sie für alle benutzerdefinierten Fragen eine eigene Frage und geben Sie eine Antwort an.

**Administratordefinierte Herausforderungsfragen**

Frage: Geburtsname der Mutter?  
Antwort:

Frage: Name Ihres Haustiers in der Kindheit?  
Antwort:

**Benutzerdefinierte Herausforderungsfragen**

Frage:   
Antwort:

### 19.4.1 Anforderungen

Das Portlet „IDM-Herausforderungsantwort“ hat folgende Anforderungen:

Thema	Anforderungen
Passwortrichtlinie	Für dieses Portlet ist eine Passwortrichtlinie mit aktivierter Funktion „Passwort vergessen“ und einem Herausforderungssatz erforderlich.
Universelles Passwort	Bei diesem Portlet muss das universelle Passwort nicht aktiviert sein.
eDirectory-Konfiguration	<p>Für dieses Portlet ist es erforderlich, dass Sie dem Benutzeranwendungsadministrator Supervisor-Rechte für den Container erteilen, dem der angemeldete Benutzer angehört. Wenn diese Rechte erteilt sind, kann der Benutzer eine Herausforderungsantwort an den Secret Store schreiben.</p> <p>Beispiel: Angenommen, der Administrator für den LDAP-Realm ist cn=admin, ou=sample, n=novell, und Sie melden sich als cn=user1, ou=testou, o=novell an. Sie müssen in diesem Fall cn=admin, ou=sample, n=novell als Trustee von <b>testou</b> zuweisen und Supervisor-Rechte auf <b>[Alle Attributrechte]</b> gewähren.</p>

## 19.4.2 Verwendung

Wenn Sie das Portlet „IDM-Herausforderungsantwort“ verwenden möchten, sollten Sie sich mit Folgendem auskennen:

- [„Verwendung der IDM-Herausforderungsantwort während der Anmeldung“ auf Seite 286](#)
- [„Verwendung von „IDM-Herausforderungsantwort“ in der Benutzeranwendung“ auf Seite 286](#)

### Verwendung der IDM-Herausforderungsantwort während der Anmeldung

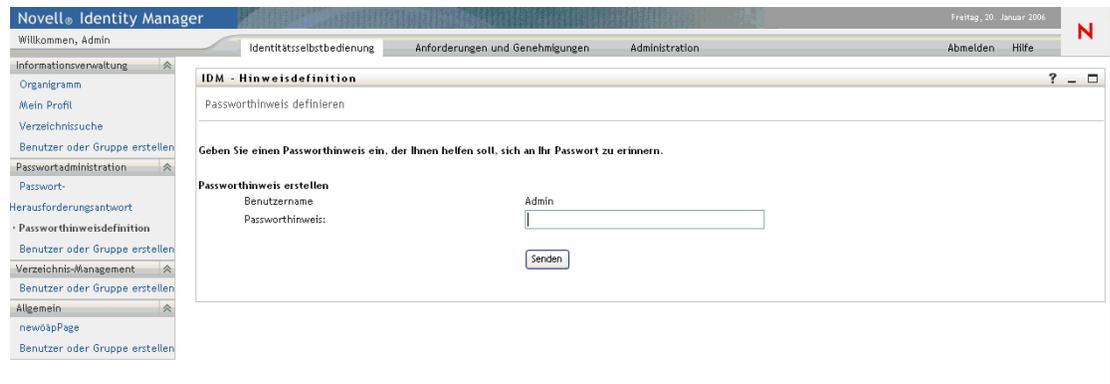
Bei der Anmeldung leitet das [Portlet für die IDM-Anmeldung \(Seite 284\)](#) automatisch zum Portlet „IDM-Herausforderungsantwort“ um, sofern der Benutzer Herausforderungsfragen und -antworten einrichten muss (z. B. beim ersten Anmeldeversuch eines Benutzers, nachdem ein Administrator den Benutzer in iManager einer Passwortrichtlinie zugewiesen hat). Bei der Passwortrichtlinie muss die Funktion „Passwort vergessen“ aktiviert sein und sie muss einen Herausforderungssatz enthalten.

### Verwendung von „IDM-Herausforderungsantwort“ in der Benutzeranwendung

Die Benutzeranwendung stellt Benutzern standardmäßig die Selbstbedienung bei der Änderung von Herausforderungsfragen und -antworten zur Verfügung.

## 19.5 Portlet „IDM - Hinweisdefinition“

Über dieses Selbstbedienungs-Portlet können Benutzer ihren Passworthinweis ändern (der bei vergessenem Passwort als Hinweis angezeigt oder per Email zugesendet werden kann).



### 19.5.1 Anforderungen

Für das Portlet „IDM - Hinweisdefinition“ gelten folgende Anforderungen:

Thema	Anforderungen
Passwortrichtlinie	Für dieses Portlet ist eine Passwortrichtlinie mit aktivierter Funktion „Passwort vergessen“ und einem Herausforderungssatz erforderlich.
Universelles Passwort	Bei diesem Portlet muss das universelle Passwort nicht aktiviert sein.

### 19.5.2 Verwendung

Wenn Sie das Portlet „IDM - Hinweisdefinition“ verwenden möchten, sollten Sie sich mit Folgendem auskennen:

- [„Verwendung der IDM - Hinweisdefinition während der Anmeldung“ auf Seite 287](#)
- [„Verwendung der „IDM - Hinweisdefinition“ auf der Benutzeranwendungsseite“ auf Seite 287](#)

#### Verwendung der IDM - Hinweisdefinition während der Anmeldung

Bei der Anmeldung leitet das [Portlet für die IDM-Anmeldung \(Seite 284\)](#) automatisch zum Portlet „IDM - Hinweisdefinition“ um, sofern der Benutzer seinen Passworthinweis einrichten muss (z. B. beim ersten Anmeldeversuch eines Benutzers, nachdem ein Administrator den Benutzer in iManager einer Passwortrichtlinie zugewiesen hat). In der Passwortrichtlinie muss die Funktion „Passwort vergessen“ aktiviert und die Aktion auf *Hinweis per Email an den Benutzer senden* oder *Hinweis auf Seite anzeigen* gesetzt sein).

#### Verwendung der „IDM - Hinweisdefinition“ auf der Benutzeranwendungsseite

Die Benutzeranwendung stellt Benutzern standardmäßig die Selbstbedienung bei der Änderung ihres Passworthinweises zur Verfügung.

## 19.6 Portlet „IDM - Passwort ändern“

Über dieses Selbstbedienungs-Portlet können Benutzer ihr universelles Passwort gemäß der zugewiesenen Passwortrichtlinie ändern (zurücksetzen). Es verwendet diese Richtlinie für die Anzeige der Regeln, die das neue Passwort einhalten muss.

Wenn die Funktion „Universelles Passwort“ nicht aktiviert ist, ändert dieses Portlet entsprechend den Passwortbeschränkungen des Benutzers das (einfache) eDirectory-Passwort des Benutzers.

Identitätsselbstbedienung    Anforderungen und Genehmigungen    Administration    Abmelden    Hilfe

### IDM - Passwort ändern

Passwort ändern

Quel est votre film de favori?

Ihr Passwort muss folgende Eigenschaften aufweisen:

- Mindestzahl der Zeichen im Passwort: 4
- Höchstzahl der Zeichen im Passwort: 12

Das Passwort darf Zahlen enthalten.

Für das Passwort wird die Groß-/Kleinschreibung berücksichtigt.

Sie dürfen Sonderzeichen im Passwort verwenden.

Altes Passwort:

Neues Passwort:

Passwort wiederholen:

### 19.6.1 Anforderungen

Für das Portlet „IDM - Passwort ändern“ gelten folgende Anforderungen:

Thema	Anforderungen
Konfiguration der Verzeichnisabstraktionsschicht	Für dieses Portlet ist keine Konfiguration der Verzeichnisabstraktionsschicht erforderlich.
Passwortrichtlinie	Für dieses Portlet ist keine Passwortrichtlinie erforderlich, es sein denn, Sie möchten erweiterte Passwortregeln verwenden (mit aktivierter Funktion „Universelles Passwort“).

Thema	Anforderungen
Universelles Passwort	<p>Wenn Sie dieses Portlet für ein universelles Passwort verwenden möchten, muss in den erweiterten Passwortregeln der dem Benutzer zugewiesenen Passwortrichtlinie die Einstellung <b>Passwortänderung durch Benutzer zulassen</b> aktiviert sein.</p> <p>Wenn Sie dieses Portlet für ein (einfaches) eDirectory-Passwort verwenden möchten, muss in den Passwortbeschränkungen des Benutzers die Einstellung <b>Passwortänderung durch Benutzer zulassen</b> aktiviert sein.</p>

## 19.6.2 Verwendung

Wenn Sie das Portlet „IDM - Passwort ändern“ verwenden möchten, sollten Sie sich mit Folgendem auskennen:

- „Verwendung von „IDM - Passwort ändern“ während der Anmeldung“ auf Seite 289
- „Verwendung von „IDM - Passwort ändern“ in der Benutzeranwendung“ auf Seite 289

### Verwendung von „IDM - Passwort ändern“ während der Anmeldung

Bei der Anmeldung leitet das [Portlet für die IDM-Anmeldung \(Seite 284\)](#) automatisch zum Portlet „IDM - Passwort ändern“ um, sofern der Benutzer ein ungültiges Passwort zurücksetzen muss (z. B. beim ersten Anmeldeversuch eines Benutzers, nachdem ein Administrator eine Passwortrichtlinie implementiert hat, durch die ein Benutzer sein Passwort zurücksetzen muss).

Das [Portlet „IDM - Passwort vergessen“ \(Seite 290\)](#) leitet auch dann automatisch zu „IDM - Passwort ändern“ um, wenn in der dem Benutzer zugewiesenen Passwortrichtlinie festgelegt ist, dass bei einem vergessenen Passwort das Passwort zurückgesetzt werden muss.

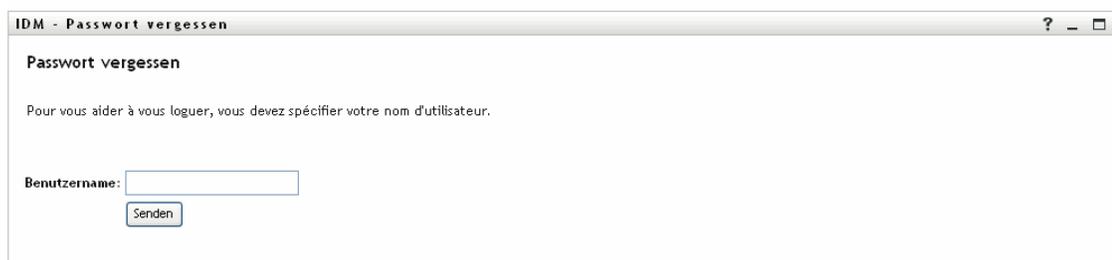
### Verwendung von „IDM - Passwort ändern“ in der Benutzeranwendung

Die Benutzeranwendung ermöglicht Benutzern standardmäßig über das Portlet „IDM - Passwort ändern“ die Selbstbedienung bei der Passwortänderung. Zum Beispiel:

## 19.7 Portlet „IDM - Passwort vergessen“

Der Benutzer erhält über dieses Selbstbedienungs-Portlet mittels Herausforderungs-/ Antwortauthentifizierung Informationen über sein Passwort. Das Ergebnis ist abhängig von der zugewiesenen Passwortrichtlinie und kann Folgendes enthalten:

- Anzeige des Passworthinweises des Benutzers auf dem Bildschirm
- Versenden des Hinweises per Email an den Benutzer
- Versenden des Passworts an den Benutzer
- Eingabeaufforderung zum Zurücksetzen (Ändern) des Passworts



### 19.7.1 Anforderungen

Das Portlet „IDM - Passwort vergessen“ hat folgende Anforderungen:

Thema	Anforderungen
Passwortrichtlinie	Für dieses Portlet ist eine Passwortrichtlinie mit aktivierter Funktion „Passwort vergessen“ und einem Herausforderungssatz erforderlich.
Universelles Passwort	Für dieses Portlet muss die Funktion „Universelles Passwort“ nicht aktiviert sein (es sein denn, Sie möchten bei vergessenem Passwort folgende Aktionen unterstützen: Passwort zurücksetzen oder Passwort per Email an den Benutzer senden).

### 19.7.2 Verwendung

Wenn Sie das Portlet „IDM - Passwort vergessen“ verwenden möchten, sollten Sie sich mit Folgendem auskennen:

- [„Verwendung von „IDM - Passwort vergessen“ während der Anmeldung“ auf Seite 290](#)
- [„Konfigurieren Ihrer Umgebung für Email-Aktionen“ auf Seite 291](#)
- [„Standardeinstellungen für „IDM - Passwort vergessen““ auf Seite 291](#)

#### Verwendung von „IDM - Passwort vergessen“ während der Anmeldung

Während der Anmeldung leitet das [Portlet für die IDM-Anmeldung \(Seite 284\)](#) zum Portlet „IDM - Passwort vergessen“ um, wenn der Benutzer auf den Link *Passwort vergessen* klickt. Bei der Anzeige von „IDM - Passwort vergessen“ wird Folgendes ausgeführt:

- 1 Aufforderung zur Eingabe des *Benutzernamens*.

- 2 Umleitung zum **Portlet für die IDM-Anmeldung (Seite 284)**, wo für diesen Benutzer die *Herausforderungs-/antwortauthentifizierung* durchgeführt wird.
- 3 Ausführung der *Aktion bei vergessenem Passwort*, die in der dem Benutzer zugewiesenen Passwortrichtlinie festgelegt ist. Eine der folgenden Aktionen wird ausgeführt:
  - Umleitung an das **Portlet „IDM - Passwort ändern“ (Seite 288)**, damit der Benutzer sein Passwort zurücksetzen kann
  - Versenden des Passworts oder des Hinweises *per Email* an den Benutzer
  - *Anzeige* des Hinweises

---

**Hinweis:** Das Portlet „IDM - Passwort vergessen“ ist nicht für die eigenständige Verwendung gedacht. Dies bedeutet, Sie sollten es nicht zu einer freigegebenen Seite in der Benutzeranwendung hinzufügen. Wenn Sie das Portlet auf einer Seite platzieren, entsteht ein potenzielles Sicherheitsrisiko, da Personen auf einem unbeaufsichtigten Computer ohne Wissen oder Genehmigung des Benutzers ein Passwort ändern können.

---

## Konfigurieren Ihrer Umgebung für Email-Aktionen

Wenn Sie die Email-Aktionen bei vergessenem Passwort unterstützen möchten, stellen Sie sicher, dass Ihr *Email-Benachrichtigungsserver* ordnungsgemäß konfiguriert ist:

- 1 Verwenden Sie zum Zugriff auf *iManager* auf Ihrem eDirectory-Server einen Webbrowser und melden Sie sich als *Administrator* an.
- 2 Wechseln Sie zu *Funktionen und Aufgaben > Passwörter* und wählen Sie *Email-Serveroptionen*.
- 3 Nehmen Sie die entsprechenden Einstellungen vor und klicken Sie anschließend auf *OK*.

Das Portlet „IDM - Passwort vergessen“ verwendet zwei *Email-Schablonen*. In *iManager* finden Sie sie unter *Funktionen und Aufgaben > Passwörter > Email-Schablonen bearbeiten*. Sie heißen:

- Password hint request (Anforderung für Passworthinweis)
- Your password request (Anforderung für Ihr Passwort)

Sie können den Inhalt dieser Schablonen bei Bedarf an Ihre Anwendung anpassen (ändern Sie aber nicht die Struktur).

## Standardeinstellungen für „IDM - Passwort vergessen“

Für das Portlet „IDM - Passwort vergessen“ gelten folgende Standardeinstellungen:

Standardeinstellung	Details
login-sequence	Die zu verwendende NMAS-Anmeldesequenz. In dieser Version unterstützt das Portlet nur <b>Herausforderungsantwort</b> .
ldap-sslport	Der sichere LDAP-Port, der zu verwenden ist. Der Standardport ist <b>636</b> .
allow-wildcard	Legt fest, ob der Benutzer bei der Eingabe des Benutzernamens Platzhalter verwenden kann. Die Standardeinstellung ist <b>false</b> .
encoding	Die zu verwendende Zeichenkodierung. Die Standardeinstellung ist <b>utf-8</b> .



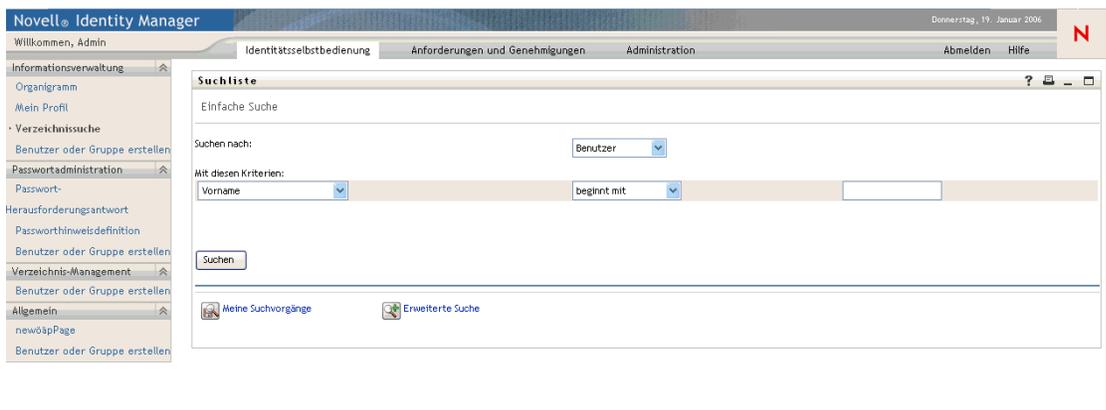
In diesem Kapitel wird beschrieben, wie Sie das Portlet *Suchliste* für die Verwendung mit der Identity Manager-Benutzeranwendung einrichten und anpassen können. Es werden folgende Themen erläutert:

- [Abschnitt 20.1, „Allgemeines zum Portlet Suchliste“](#), auf Seite 293
- [Abschnitt 20.2, „Konfigurieren des Portlets „Suchliste““](#), auf Seite 298

## 20.1 Allgemeines zum Portlet Suchliste

Das Portlet *Suchliste* ermöglicht Benutzern, das Identitätsdepot zu durchsuchen und dessen Inhalte anzuzeigen. Es stellt die Grundlage für die Aktion *Verzeichnissuche* in der Registerkarte „Identitätsselbstbedienung“ der Identity Manager-Benutzeranwendung dar. Die Aktion „Verzeichnissuche“ ist so konfiguriert, dass Benutzer nach Benutzern, Gruppen und Aufgabengruppen suchen können. Es ist jedoch möglich, Änderungen vorzunehmen und den Bereich der durchsuchbaren Objekte und Attribute zu ändern.

Im folgenden Beispiel wird veranschaulicht, auf welche Weise Benutzer die Suchkriterien definieren können.



### Element der Benutzeroberfläche

### Beschreibung

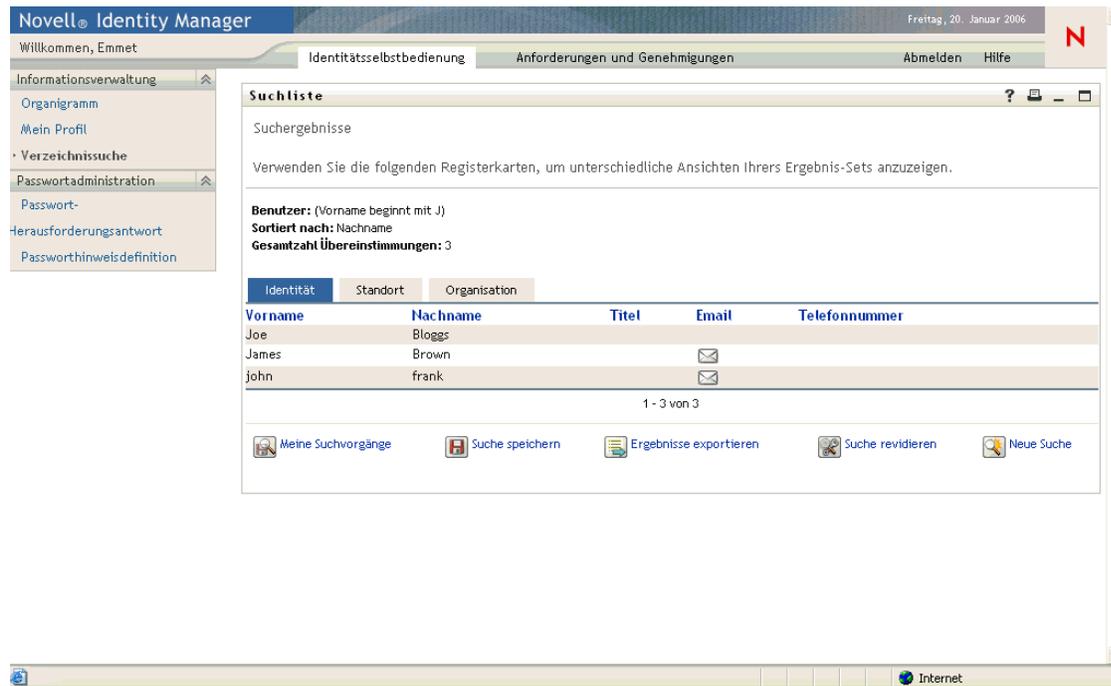
Suchen nach

Benutzer wählen den Objekttyp aus, nach dem gesucht werden soll.

Weitere Informationen zur Definition der Inhalte dieser Liste finden Sie in [Abschnitt 20.2.2, „Festlegen von Standardeinstellungen für die Suchliste“](#), auf Seite 300.

Element der Benutzeroberfläche	Beschreibung
Mit diesen Kriterien	<p>Benutzer definieren die Suchkriterien durch Auswahl von Attributen und Suchoperatoren in der Dropdown-Liste.</p> <p>Wenn der Benutzer die Option „Erweiterte Suche“ auswählt, können mehrere Reihen und Blöcke von Suchkriterien-Gruppierungen festgelegt werden, die bei einer Suche mit UND oder ODER verwendet werden können.</p> <p>Weitere Informationen zur Definition von durchsuchbaren Attributen finden Sie in <a href="#">Abschnitt 20.2.2, „Festlegen von Standardeinstellungen für die Suchliste“</a>, auf Seite 300.</p>
Suchen	<p>Führt die angegebenen Suchkriterien aus.</p> <p>Weitere Informationen zur Definition der Standardsuche finden Sie in <a href="#">Abschnitt 20.2.2, „Festlegen von Standardeinstellungen für die Suchliste“</a>, auf Seite 300.</p>
Meine gespeicherten Suchvorgänge	<p>Mithilfe dieser Schaltfläche kann ein Benutzer eine zuvor gespeicherte Suche auswählen, ausführen, bearbeiten oder löschen.</p>
	
Erweiterte Suche	<p>Wie bei der Suche über die Schaltfläche kann der Benutzer Zeilen oder Blöcke von Suchkriterien hinzufügen. Bei einer erweiterten Suche können jedoch mehrere Reihen und Blöcke von Suchkriterien-Gruppierungen festgelegt werden, die bei einer Suche mit UND oder ODER verwendet werden können.</p> <p>Weitere Informationen zur Definition von durchsuchbaren Attributen finden Sie in <a href="#">Abschnitt 20.2.2, „Festlegen von Standardeinstellungen für die Suchliste“</a>, auf Seite 300.</p>
	

In diesem Beispiel wird (anhand von Beispieldaten) veranschaulicht, wie das Portlet nach Eingabe des Suchkriteriums *Vorname beginnt mit A* die Ergebnisse anzeigt:



Sie können das Portlet „Suchliste“ so konfigurieren, dass es beliebige der folgenden Funktionen verwendet:

Element der Benutzeroberfläche	Beschreibung
Registerkarten „Identität“, „Standort“, „Organisation“	Wenn Benutzer auf eine dieser Registerkarten klicken, wird die Ergebnisliste auf unterschiedliche Weise angezeigt.  Weitere Informationen zu Formaten finden Sie in <a href="#">Abschnitt 20.1.1, „Allgemeines zu Anzeigeformaten der Ergebnisliste“</a> , auf Seite 296.
Meine gespeicherten Suchvorgänge 	Ermöglicht den Benutzern die Auswahl einer zuvor gespeicherten Suche.
Suche speichern 	Ermöglicht Benutzern, die Suchkriterien zu speichern und die gespeicherten Suchvorgänge bei Bedarf erneut auszuführen. Die Suchvorgänge werden im Attribut „srvprvQueryList“ des aktuell ausgewählten Benutzers gespeichert.
Ergebnisse exportieren 	Mit dieser Schaltfläche können Benutzer die Suchergebnisse in ein anderes Format exportieren.

Element der Benutzeroberfläche	Beschreibung
	Ermöglicht den Benutzern die Änderung von Suchkriterien.
	Ermöglicht dem Benutzer die Definition einer neuen Suche.

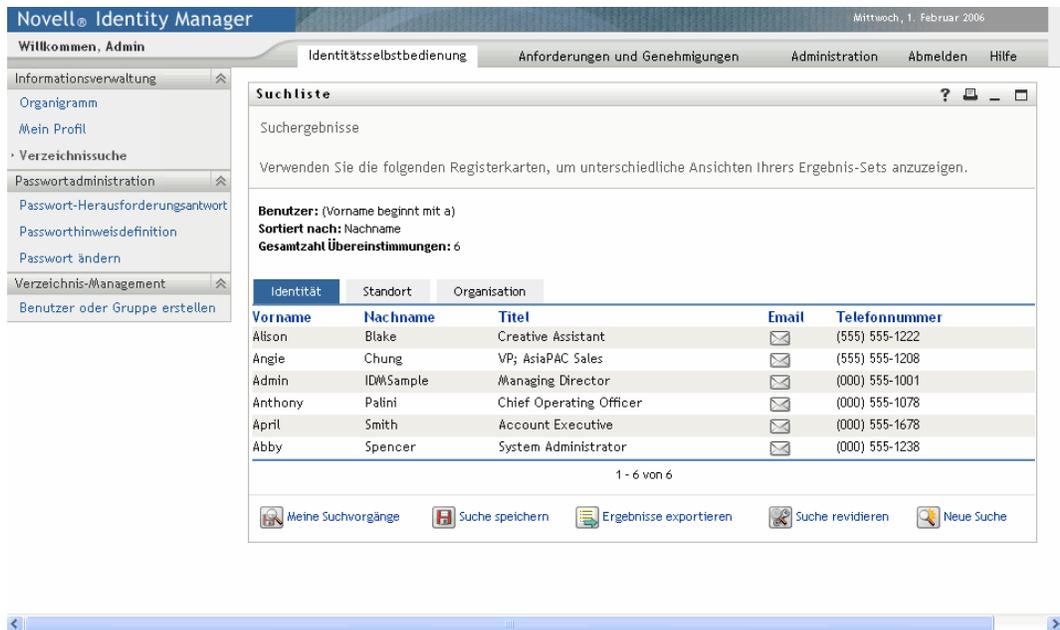
Das Portlet „Suchliste“ bietet den Endbenutzern standardmäßig auch folgende Möglichkeiten:

- Drucken der Suchergebnisse
- Email-Start von der Ergebnisliste aus
- Starten des Detail-Portlets von der Ergebnisliste aus

## 20.1.1 Allgemeines zu Anzeigeformaten der Ergebnisliste

Sie können definieren, auf welche Weise Daten, die von der Suche im Identitätsdepot zurückgegeben werden, den Endbenutzern angezeigt werden. Die Daten können in einem oder mehreren der folgenden Seitentypen organisiert werden:

- *Identitätsseiten* - Diese Seiten enthalten üblicherweise Kontaktinformationen:



**Novell Identity Manager** Mittwoch, 1. Februar 2006

Willkommen, Admin Identitätsselbstbedienung Anforderungen und Genehmigungen Administration Abmelden Hilfe

Informationsverwaltung ? - □

Organigramm

Mein Profil

Verzeichnissuche

Passwortadministration

Passwort-Herausforderungsantwort

Passworthinweisdefinition

Passwort ändern

Verzeichnis-Management

Benutzer oder Gruppe erstellen

---

**Suchliste**

Suchergebnisse

Verwenden Sie die folgenden Registerkarten, um unterschiedliche Ansichten Ihres Ergebnis-Sets anzuzeigen.

**Benutzer:** (Vorname beginnt mit a)  
**Sortiert nach:** Nachname  
**Gesamtzahl Übereinstimmungen:** 6

Identität	Standort	Organisation		
Vorname	Nachname	Titel	Email	Telefonnummer
Alison	Blake	Creative Assistant	✉	(555) 555-1222
Angie	Chung	VP; AsiaPAC Sales	✉	(555) 555-1208
Admin	IDM.Sample	Managing Director	✉	(000) 555-1001
Anthony	Palini	Chief Operating Officer	✉	(000) 555-1078
April	Smith	Account Executive	✉	(000) 555-1678
Abby	Spencer	System Administrator	✉	(000) 555-1238

1 - 6 von 6







- *Standortseiten* - Diese Seiten enthalten üblicherweise Standortinformationen:

The screenshot shows the Novell Identity Manager interface. The left sidebar contains navigation options like 'Organigramm', 'Mein Profil', and 'Verzeichnissuche'. The main content area is titled 'Suchliste' and displays search results for 'Standort'. The search criteria are: Benutzer: (Vorname beginnt mit B), Sortiert nach: Region, Gesamtzahl Übereinstimmungen: 2. The results table has columns for Identity, Location, and Organization. Two results are shown: Billy Murphy (Ireland) and Bob Green (US). Below the table are navigation buttons: 'Meine Suchvorgänge', 'Suche speichern', 'Ergebnisse exportieren', 'Suche revidieren', and 'Neue Suche'.

Identität	Standort	Organisation
<b>Vorname</b>	<b>Nachname</b>	<b>Region</b>
Billy	Murphy	Ireland
Bob	Green	US

- *Organisationsseiten* - Diese Seiten enthalten üblicherweise Informationen zur Organisationshierarchie:

The screenshot shows the Novell Identity Manager interface. The left sidebar is the same as in the previous screenshot. The main content area is titled 'Suchliste' and displays search results for 'Organisation'. The search criteria are: Benutzer: (Vorname beginnt mit B), Sortiert nach: Abteilung, Gesamtzahl Übereinstimmungen: 2. The results table has columns for Identity, Location, and Organization. Two results are shown: Billy Murphy (Manager) and Bob Green (CEO). Below the table are navigation buttons: 'Meine Suchvorgänge', 'Suche speichern', 'Ergebnisse exportieren', 'Suche revidieren', and 'Neue Suche'.

Identität	Standort	Organisation
<b>Vorname</b>	<b>Nachname</b>	<b>Titel</b>
Billy	Murphy	Manager
Bob	Green	CEO

Mithilfe der komplexen Standardeinstellungen des Portlets haben Sie die Möglichkeit, weitere Formate für die Ergebnisliste zu definieren. Wenn Ihr Identitätsdepot-Schema z. B. Informationen

zur Qualifikation oder zu Urkunden enthält, können Sie eine Ergebnisliste einrichten, die diese Informationen anzeigt.

Je nach Konfiguration des Portlets können Endbenutzer:

- Die zu suchenden Objekttypen des Identitätsdepots anzeigen (z. B. Benutzer und Gruppen).
- *Suchkriterien* festlegen (z. B. „Vorname beginnt mit“ oder „Nachname enthält“).
- Das *Anzeigeformat* auswählen, in dem die Suchergebnisse angezeigt werden sollen.
- Die *Sortierreihenfolge* ändern.

## 20.2 Konfigurieren des Portlets „Suchliste“

Im Folgenden finden Sie ein Beispiel für die Vorgehensweise zur Konfiguration des Portlets „Suchliste“:

Schritt	Aufgabe	Beschreibung
1	Definieren Sie: <ul style="list-style-type: none"><li>• die Entitäten und Attribute, nach denen Benutzer suchen können.</li><li>• das Anzeigeformat der Ergebnisliste.</li></ul>	<p>Sie können die vordefinierte Aktion „Verzeichnissuche“ verwenden, die zusammen mit der Identity Manager-Benutzeranwendung installiert wird. Sie können diese Aktion ändern oder eine eigene erstellen.</p> <p>Weitere Informationen finden Sie in <a href="#">Abschnitt 20.2.2, „Festlegen von Standardeinstellungen für die Suchliste“, auf Seite 300.</a></p>
2	Überprüfen Sie, ob die Entitäten und Attribute für die Suche in der Verzeichnisabstraktionsschicht definiert sind.	<p>Weitere Informationen finden Sie in <a href="#">Kapitel 4, „Konfigurieren der Verzeichnisabstraktionsschicht“, auf Seite 75.</a></p>
3	Legen Sie fest, auf welche Weise Sie Benutzern den Zugriff auf das Portlet ermöglichen möchten.	<p>Möchten Sie es den Benutzern ermöglichen, dieses Portlet von einer vorhandenen oder von einer neuen Seite aus zu starten?</p> <p>Weitere Informationen zu Seiten finden Sie in <a href="#">Kapitel 7, „Seitenadministration“, auf Seite 137.</a></p>
4	Legen Sie Standardeinstellungen für das Portlet fest	<p>Standardeinstellungen für das Portlet „Suchliste“, das Sie definieren:</p> <ul style="list-style-type: none"><li>• Die Attribute, die in den einzelnen Formaten der Ergebnisliste angezeigt werden.</li><li>• Welches Anzeigeformat für die Ergebnisliste nach einer Suche gewählt wird.</li><li>• Die Standard-Sortierreihenfolge für die Formate der Ergebnisliste.</li></ul> <p>Weitere Informationen finden Sie in <a href="#">Abschnitt 20.2.2, „Festlegen von Standardeinstellungen für die Suchliste“, auf Seite 300.</a></p>
5	Testen Sie Ihre Einstellungen	<p>Vergewissern Sie sich, dass die Ergebnislisten die gewünschten Attribute anzeigen.</p>

Schritt	Aufgabe	Beschreibung
6	Richten Sie eDirectory-Rechte ein und erstellen Sie Indizes, die zur Verbesserung der Leistung benötigt werden	<p>eDirectory-Rechte:</p> <p>Zum Ausführen einer Suche:</p> <ul style="list-style-type: none"> <li>• Der Benutzer, der die Suche ausführt, benötigt die Zugriffsberechtigung <b>Durchsuchen</b> für alle Benutzer oder Objekte, nach denen gesucht wird.</li> </ul> <p>Zum Speichern einer Suche (für Benutzer ohne Administratorrechte):</p> <ul style="list-style-type: none"> <li>• <b>Trustee</b> der organisatorischen Einheit und der Organisation, in denen sie die Suche ausführen.</li> <li>• Für <b>User</b> mit den Rechten „Schreiben“, „Eigene Namen hinzufügen“, „Eigene Namen löschen“ und „Supervisor“.</li> </ul> <p><b>Verbesserung der Leistung</b> - Die Leistung der Suche kann verbessert werden, indem zum Attribut, auf dem die Suche basiert, ein eDirectory-Werteindex hinzugefügt wird.</p>

Weitere Informationen zur Definition der unterschiedlichen Anzeigeformate für die Liste finden Sie in [Abschnitt 20.2.2, „Festlegen von Standardeinstellungen für die Suchliste“](#), auf Seite 300.

## 20.2.1 Einrichtung der Verzeichnisabstraktionsschicht

Die Identitäten und Attribute, die aus der Dropdown-Liste der Suchkriterien ausgewählt werden können, und die Daten, die von Suchvorgängen im Identitätsdepot zurückgegeben werden, müssen in der Verzeichnisabstraktionsschicht definiert sein. In der folgenden Tabelle werden die Eigenschaften angezeigt, die Sie für die von der Suchliste verwendeten Entitäten und Attribute festlegen sollten.

Definitionsart	Einstellung	Wert der Verzeichnisabstraktionsschicht
Entität	view	Ausgewählt (Wahr)

Definitionsart	Einstellung	Wert der Verzeichnisabstraktionsschicht
Attribut	enable	Ausgewählt (Wahr)
	search	Ausgewählt (Wahr)
	hide	Nicht ausgewählt

Wenn die Option nicht ausgewählt ist, kann für das entsprechende Attribut keine Suche ausgeführt und es kann auch nicht in ein Ergebnislistenformat einbezogen werden.

Bei jedem Attribut, das für die Suche ausgewählt ist, darf die Einstellung „hide“ nicht ausgewählt werden. Dies liegt daran, dass das Portlet „Suchliste“ während der Suche nicht den Wert der hide-Eigenschaft untersucht (weil dadurch die Leistung beeinträchtigt würde).

Angenommen, Benutzer 1 setzt das „HomePhone“-Attribut auf hide=true (in eDirectory). HomePhone kann durchsucht werden und das Portlet „Suchliste“ kann den Datensatz abrufen. „Suchliste“ überprüft allerdings nicht die Werte der anderen Attribute (weil dies eine Beeinträchtigung der Leistung zur Folge hätte). Wenn ein anderer Benutzer nach einer genauen Entsprechung für das „HomePhone“-Attribut suchen würde, würde der versteckte Datensatz in der Ergebnisliste angezeigt werden.

**Weitere Einstellungen für die Verzeichnisabstraktionsschicht** Datentyp, Formattyp, Filter und Suchbereich der Verzeichnisabstraktionsschicht beeinflussen auch das Portlet „Suchliste“. Der Datentyp und der Formattyp beeinflussen die Darstellung, der Filter und der Suchbereich beeinflussen die Menge der zurückgegebenen Daten.

Weitere Informationen finden Sie in [Abschnitt 4.3, „Arbeiten mit Entitäten und Attributen“](#), auf [Seite 87](#).

## 20.2.2 Festlegen von Standardeinstellungen für die Suchliste

Sie können zwei Typen von Standardeinstellungen festlegen:

- „[Standardeinstellungen für die Suche](#)“ auf [Seite 301](#)
- „[Standardeinstellungen für das Format der Ergebnisliste](#)“ auf [Seite 303](#)

## Standardeinstellungen für die Suche

Die Standardeinstellungen für die Suche können über eine einzige Seite vorgenommen werden:

Inhaltseinstellungen für diese Registrierungsinstanz ändern (Suchliste)

Suchliste

	Standardeinst	Wert der Standardeinst	Anf	Schreib- geschützt	Verstecken												
<a href="#">Zurücks</a>	Standardmodus:	<input type="text" value="My Saved Searches"/>	<a href="#">Detail</a>	<input checked="" type="checkbox"/>	<input type="checkbox"/>												
<table border="1"><thead><tr><th colspan="2">Auswahl</th></tr><tr><th>Wert</th><th>Anzeigen</th></tr></thead><tbody><tr><td>MODE_SIMP</td><td>Basic Search <a href="#">Einfüg</a> <a href="#">Entf</a></td></tr><tr><td>MODE_ADV</td><td>Advanced Search <a href="#">Einfüg</a> <a href="#">Entf</a></td></tr><tr><td>MODE_SAVE</td><td>My Saved Searches <a href="#">Einfüg</a> <a href="#">Entf</a></td></tr><tr><td colspan="2"><a href="#">Hinzufügen</a></td></tr></tbody></table>						Auswahl		Wert	Anzeigen	MODE_SIMP	Basic Search <a href="#">Einfüg</a> <a href="#">Entf</a>	MODE_ADV	Advanced Search <a href="#">Einfüg</a> <a href="#">Entf</a>	MODE_SAVE	My Saved Searches <a href="#">Einfüg</a> <a href="#">Entf</a>	<a href="#">Hinzufügen</a>	
Auswahl																	
Wert	Anzeigen																
MODE_SIMP	Basic Search <a href="#">Einfüg</a> <a href="#">Entf</a>																
MODE_ADV	Advanced Search <a href="#">Einfüg</a> <a href="#">Entf</a>																
MODE_SAVE	My Saved Searches <a href="#">Einfüg</a> <a href="#">Entf</a>																
<a href="#">Hinzufügen</a>																	
<a href="#">Zurücks</a>	Seitennummerierung:	<input type="text" value="10"/>	<a href="#">Detail</a>	<input checked="" type="checkbox"/>	<input type="checkbox"/>												
<table border="1"><thead><tr><th colspan="2">Bereich</th></tr><tr><th>Min</th><th>Max</th></tr></thead><tbody><tr><td><input type="text"/></td><td><input type="text"/></td></tr></tbody></table>						Bereich		Min	Max	<input type="text"/>	<input type="text"/>						
Bereich																	
Min	Max																
<input type="text"/>	<input type="text"/>																
<a href="#">Zurücks</a>	Ergebnisgrenze:	<input type="text" value="0"/>	<a href="#">Detail</a>	<input checked="" type="checkbox"/>	<input type="checkbox"/>												
<table border="1"><thead><tr><th colspan="2">Bereich</th></tr><tr><th>Min</th><th>Max</th></tr></thead><tbody><tr><td><input type="text"/></td><td><input type="text"/></td></tr></tbody></table>						Bereich		Min	Max	<input type="text"/>	<input type="text"/>						
Bereich																	
Min	Max																
<input type="text"/>	<input type="text"/>																
<a href="#">Zurücks</a>	Komplexe Einstellung für Suche und Listen:	<a href="#">Benutzerdefinierte Einstellung anzeigen/bearbeiten</a>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>												

Im Folgenden finden Sie eine Liste der Standardeinstellungen für die Suche:

Standardeinstellung	Vorgehensweise
Standardmodus	<p>Legen Sie fest, wie das Portlet angezeigt werden soll, wenn ein Benutzer zum ersten Mal darauf zugreift. Gültige Werte:</p> <p><b>Einfache Suche</b> - Die Benutzer können ein einzelnes Suchkriterium eingeben. Zum Beispiel:</p> <p>Vorname beginnt mit A</p> <p><b>Erweiterte Suche</b> - Benutzer können in einem oder mehreren Suchblöcken mehrere Suchkriterien definieren. Benutzer können die logischen Operatoren „und“/„oder“ innerhalb der Suchkriterien oder der Suchblöcke verwenden. Benutzer haben z. B. die Möglichkeit, eine Suche wie diese zu erstellen:</p> <p>(Vorname beginnt mitA oder Vorname beginnt mit B) und (Region = Northeast oder Region = Southeast)</p> <p>oder</p> <p>(Vorname beginnt mit A und Nachname beginnt mit B) oder (Vorname beginnt mit B und Nachname beginnt mit A)</p> <p><b>Meine gespeicherten Suchvorgänge</b> - Zeigt eine Liste der gespeicherten Suchvorgänge des zurzeit angemeldeten Benutzers an. Die Suchvorgänge werden im Attribut „srvprvQueryList“ des Benutzers gespeichert.</p> <hr/> <p><b>Hinweis:</b> Benutzer können zur Laufzeit auf diese Modi zugreifen, indem sie auf eine Suche ausführen oder bearbeiten oder indem sie eine Schaltfläche im unteren Bereich des Portlets klicken.</p>
Seitennummerierung	Die maximale Zeilenzahl pro Seite.
Ergebnisgrenze	Die Höchstanzahl der Entsprechungen, die von der Suche zurückgegeben werden. Wenn die Anzahl auf 0 gesetzt ist, wird für die Höchstanzahl die Einstellung der Verzeichnisabstraktionsschicht übernommen.
Komplexe Standardeinstellung für Suche und Listen	<p>Klicken Sie, um:</p> <ul style="list-style-type: none"> <li>• die Suche nach Entitäten zu verfeinern</li> <li>• den Typ des Ergebnis-Sets zu verfeinern</li> <li>• die Attribute, die auf der Seite angezeigt werden sollen, und deren Reihenfolge zu verfeinern</li> </ul> <p>Standardmäßig werden alle Objekte in der Verzeichnisabstraktionsschicht mit dem Attribut view=true in die Suche einbezogen. Die Attributliste der Entität wird aus den in der Verzeichnisabstraktionsschicht aufgeführten Attributen abgeleitet, die mit enable=true definiert sind.</p>

## Standardeinstellungen für das Format der Ergebnisliste

Auf der Seite mit den komplexen Standardeinstellungen können Sie definieren, welche Entitäten in die Suche aufgenommen werden, und wie die Ergebnisliste formatiert werden soll. Im Folgenden wird die Seite mit den vorgegebenen Standardeinstellungen angezeigt:

Suchliste

Search and List complex preference

**Search List**

**Zusammenfassung**

Entitätsdefinition	Benutzer	<input type="checkbox"/>
Email als Symbol anzeigen	<input checked="" type="radio"/> Wahr <input type="radio"/> Falsch	
Ergebnislistentypen	Standard	<input checked="" type="checkbox"/>
Sortieren		<input checked="" type="checkbox"/>
Attribute	Vorname	<input type="radio"/>
	Nachname	<input checked="" type="radio"/>
	Titel	<input type="radio"/>
	Email	<input type="radio"/>
	Telefonnummer	<input type="radio"/>
Sortieren		<input type="checkbox"/>
Attribute	Vorname	<input type="radio"/>
	Nachname	<input type="radio"/>
	Region	<input checked="" type="radio"/>
	Email	<input type="radio"/>
	Telefonnummer	<input type="radio"/>
Sortieren		<input type="checkbox"/>
Organisation		<input type="checkbox"/>

[Zurück zu Listenansicht](#)

Folgende Standardeinstellungen gehören zu den komplexen Standardeinstellungen:

Standardeinstellung	Vorgehensweise
Entitätsdefinition	<p>Jedes für die Suche geeignete Objekt (view=true) hat auf dieser Seite einen zugehörigen Entitätsdefinitionsblock. Anhand dieser Standardeinstellungen können Sie folgende Vorgänge ausführen:</p> <ul style="list-style-type: none"> <li>• Die Objekte definieren, die in die Suche einbezogen werden.</li> <li>• Die Formatdefinitionen der Ergebnisliste ändern (z. B. Attribute zur Anzeige hinzufügen oder aus ihr entfernen und deren Standard-Sortierreihenfolge ändern).</li> <li>• Alle Objekte entfernen, die nicht in die Suche einbezogen werden sollen, indem Sie auf die Schaltfläche „Löschen“ klicken, die in der Entitätsdefinitionszeile angezeigt wird. Dadurch wird der gesamte Block mit Definitionen gelöscht.</li> </ul> <p>Sie können ein Objekt zu einem späteren Zeitpunkt wieder zur Suche hinzufügen, indem Sie (im unteren Bereich der Seite) auf <b>Entitätsdefinition hinzufügen</b> klicken und in den Teilfenstern des Assistenten die entsprechende Auswahl treffen.</p> <hr/> <p><b>Tipp:</b> Wenn ein Objekt nicht in dieser Liste angezeigt, aber in der Verzeichnisabstraktionsschicht aufgeführt ist, überprüfen Sie den <b>view</b>-Modifikator (des Entitätobjekts). Wenn der Wert auf „false“ gesetzt ist, kann diese Entität nicht von den Identitäts-Portlets verwendet werden.</p>
Email als Symbol anzeigen	<p>Wenn dieser Wert auf „true“ gesetzt ist und ein Email-Attribut in der Ergebnisliste festgelegt ist, wird es als Symbol angezeigt. Wenn der Wert auf „false“ gesetzt ist, zeigt das Email-Attribut die vollständige Email-Adresse an. Das Email-Attribut (Text oder Symbol) ist ein Link vom Typ mailto: Link.</p>
Ergebnislistentypen (Standard)	<p>Legt für die aktuelle Entität das Standardformat der Ergebnisliste fest. Die Standardeinstellung wird nur verwendet, wenn der aktuelle Benutzer kein anderes Format ausgewählt hat.</p>
Anzeigeformatbereich für Ergebnisliste	<p>Legt das Anzeigeformat fest (z. B. Identitäts-, Standort- oder Organisationsseiten) und bezieht den entsprechenden Attributsatz des Typs ein.</p> <p><b>So entfernen Sie einen Ergebnislistentyp:</b></p> <ul style="list-style-type: none"> <li>• Klicken Sie neben dem Ergebnislistentyp auf die Schaltfläche „Löschen“.</li> </ul> <p>Dadurch werden der Seitentyp und die ihm zugeordneten Attribute aus der Suche gelöscht.</p> <p><b>So fügen Sie eine Ergebnis-Set-Seite hinzu:</b></p> <ul style="list-style-type: none"> <li>• Klicken Sie auf die Schaltfläche „Erweitern“ und wählen Sie in der Auswahlliste das Ergebnis-Set-Format aus.</li> </ul>

Standardeinstellung	Vorgehensweise
Attribute	<p>Legt den Attributsatz fest, der im betreffenden Anzeigeformat angezeigt wird.</p> <p><b>So fügen Sie ein Attribut hinzu bzw. entfernen es:</b></p> <ul style="list-style-type: none"> <li>• Klicken Sie auf die Schaltfläche zum Ändern von Attributen.</li> <li>• Wählen Sie in der Liste der verfügbaren Attribute ein Attribut aus, das Sie hinzufügen möchten.</li> <li>• Klicken Sie auf den Pfeil, um das Attribut in die Liste der ausgewählten Elemente zu verschieben. Führen Sie zum Entfernen eines Attributs aus der Ergebnisliste den umgekehrten Vorgang aus.</li> <li>• Klicken Sie auf der rechten Seite der ausgewählten Liste auf den Auf- und Abwärtspfeil, um die Attribute in der Liste neu anzuordnen.</li> <li>• Klicken Sie auf <b>Senden</b>.</li> </ul> <p><b>Attribute und Datentypen</b> - Der Datentyp eines Attributs wirkt sich auf dessen Anzeige aus. Wenn ein Attribut z. B. als untergeordneter Typ einer lokalen oder globalen Liste definiert ist, werden in einem Dropdown-Listefeld in den Bildschirmen zu einfachen oder erweiterten Suchkriterien die möglichen Werte angezeigt. Bei Auswahl des Typs „DN“ werden Schaltflächen für die Suche und den Verlauf angezeigt, über die die Benutzer in den Bildschirmen einen Wert zu einfachen oder erweiterten Suchkriterien auswählen können, und der DN wird in der Ergebnisliste in benutzerfreundlicher Form angezeigt. Der Datentyp und der untergeordnete Typ schränken auch den Vergleichsoperator ein, der dem Benutzer angezeigt wird, um sicherzustellen, dass nur gültige Vergleiche erzeugt werden.</p> <p>Weitere Informationen finden Sie in <a href="#">Kapitel 4, „Konfigurieren der Verzeichnisabstraktionsschicht“</a>, auf Seite 75.</p>
Anzeigeformatbereich für Ergebnisliste - Sortieren	<p>Auf diesem Attribut basiert die Sortierreihenfolge der Ergebnisliste. Die standardmäßige Sortierreihenfolge wird nur wirksam, wenn der Ergebnis-Set-Typ nicht das Anzeigeformat der aktuellen Benutzersitzung ist.</p> <p><b>Mehrwertige Attribute und einwertige Attribute</b> - Die in einer Ergebnisliste angezeigte Anzahl der Datensätze ist unterschiedlich und hängt davon ab, ob das Sortierattribut ein- oder mehrwertig ist. Bei der Sortierung mit mehrwertigen Attributen wird im Allgemeinen der Anschein erweckt, als ob eine höhere Anzahl an Ergebnissen angezeigt wird, obwohl die Gesamtzahl der Entsprechungen unverändert bleibt. Dies liegt daran, dass jeder Wert eines mehrwertigen Attributs in einer separaten Zeile angezeigt wird.</p>

### Fertigstellen der Standardeinstellungsseite

Klicken Sie auf *Senden*, wenn Sie überprüfen möchten, ob alle von Ihnen eingegebenen Daten gültig sind. Ist ein Eintrag ungültig, wird im oberen Teil der Standardeinstellungsseite eine Fehlermeldung angezeigt. Klicken Sie auf *Zurück zu Listenansicht* und anschließend auf *Standardeinstellungen speichern*, wenn Sie alle Fehler beheben konnten.



# Entwerfen und Verwalten von Bereitstellungsanforderungen



In diesen Kapiteln wird die Funktionsweise des Bereitstellungsmoduls von Identity Manager beschrieben.

- [Kapitel 21, „Einführung in die Workflow-basierte Bereitstellung“, auf Seite 309](#)
- [Kapitel 22, „Konfigurieren von Bereitstellungsanforderungsdefinitionen“, auf Seite 323](#)
- [Kapitel 23, „Verwalten von Bereitstellungs-Workflows“, auf Seite 347](#)



# Einführung in die Workflow-basierte Bereitstellung

# 21

Dieses Kapitel enthält einen Überblick über die Workflow-basierte Bereitstellung. Es werden folgende Themen erläutert:

- [Abschnitt 21.1, „Allgemeines zur Workflow-basierten Bereitstellung“, auf Seite 309](#)
- [Abschnitt 21.2, „Konfiguration und Verwaltung bei der Bereitstellung“, auf Seite 319](#)
- [Abschnitt 21.3, „Sicherheit bei der Bereitstellung“, auf Seite 319](#)

## 21.1 Allgemeines zur Workflow-basierten Bereitstellung

Eine wichtige Funktion von Identity Manager ist die *Workflow-basierte Bereitstellung*. Darunter versteht man den Vorgang der Verwaltung des Benutzerzugriffs auf die sicheren Ressourcen in einer Organisation. Diese Ressourcen können auch digitale Entitäten wie z. B. Benutzerkonten, Computer und Datenbanken umfassen. In dieser Version werden die bereitstellbaren Ressourcen Identity Manager-Berechtigungen zugeordnet.

Identity Manager kann einen großen Bereich an *Bereitstellungsanforderungen* bedienen. Bereitstellungsanforderungen sind Benutzer- oder Systemaktionen, durch die ein Zugriff auf die Ressourcen der Organisation gewährt oder verweigert wird. Sie können vom Endbenutzer direkt über die Identity Manager-Benutzeranwendung oder indirekt als Reaktion auf Ereignisse initiiert werden, die im Identitätsdepot (eDirectory) auftreten.

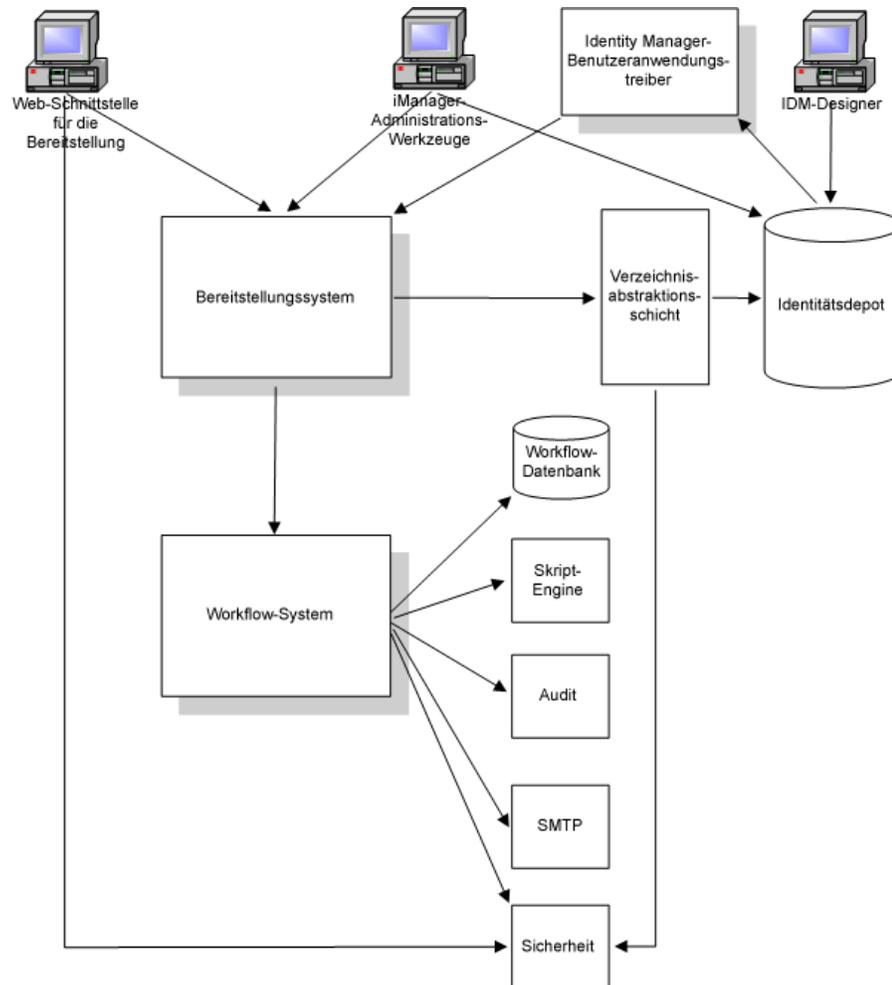
Wenn eine Bereitstellungsanforderung die Berechtigung von einer oder mehreren Personen in einer Organisation erfordert, wird durch die Anforderung ein Workflow gestartet. Der Workflow koordiniert die *Genehmigungen*, die zur Erfüllung der Anforderung benötigt werden. Einige Bereitstellungsanforderungen müssen von einer einzelnen Person genehmigt werden, andere müssen von mehreren Personen genehmigt werden. In manchen Fällen kann eine Anforderung auch ohne Genehmigung erfüllt werden.

Bei einigen Workflows muss die Verarbeitung *sequenziell* erfolgen, d. h., die Genehmigungsstufen müssen der Reihe nach erfolgen. Andere Workflows unterstützen die *parallele* Verarbeitung. Bei der Definition einer Bereitstellungsanforderung legen Sie fest, ob der Workflow die sequenzielle oder die parallele Verarbeitung unterstützen soll.

Identity Manager stellt mehrere webbasierte Werkzeuge zur Verfügung, mit denen der Administrator Bereitstellungsfunktionen in die Benutzeranwendung integrieren kann. Mit diesen Werkzeugen haben Sie die Möglichkeit, Bereitstellungsanforderungen zu konfigurieren und aktive Workflows zu verwalten. Der Administrator erstellt zum Konfigurieren einer Bereitstellungsanforderung eine *Bereitstellungsanforderungsdefinition*, durch die die Ressource an einen Workflow gebunden wird.

## 21.1.1 Übersicht über die Architektur

Im folgenden Schema ist eine Übersicht über die Architektur des Workflow-basierten Bereitstellungssystems abgebildet, das in Identity Manager enthalten ist:



In den folgenden Abschnitten werden die einzelnen Komponenten dieser Architektur beschrieben.

### Web-Schnittstelle für die Bereitstellung

Die Identity Manager-Benutzeranwendung verfügt über eine Web-Schnittstelle, über die Endbenutzer Bereitstellungsanforderungen senden und diese nach der Übermittlung verwalten können. Außerdem bietet die Benutzeranwendung dem Benutzeranwendungsadministrator oder einem Vorgesetzten die Möglichkeit, Bereitstellungs-Workflows delegierten und vertretenden Benutzern zuzuweisen.

---

**Tipp:** Die Bereitstellungs- und Workflow-Aktionen stehen über die Registerkarte *Anforderungen und Genehmigungen* der Identity Manager-Benutzeranwendung zur Verfügung.

---

Weitere Informationen zu delegierten und vertretenden Benutzern finden Sie in [Abschnitt 21.3](#), „Sicherheit bei der Bereitstellung“, auf Seite 319. Ausführliche Informationen zum Arbeiten mit der Benutzeranwendung finden Sie im *Identity Manager-Benutzeranwendung: Benutzerhandbuch*.

## Verwaltungswerkzeuge von iManager

iManager bietet Plugins, mit deren Hilfe Sie Bereitstellungsanforderungen und deren zugeordnete Workflows konfigurieren und verwalten können.

Zum Konfigurieren einer Bereitstellungsanforderung binden Sie sie an eine bereitstellbare Ressource, legen Sie die Laufzeit-Charakteristika des zugeordneten Workflows fest und aktivieren Sie sie. Sobald eine Bereitstellungsanforderung initiiert wurde, können Sie über iManager den Status des Workflow-Prozesses anzeigen, Aktivitäten innerhalb der Workflows neu zuweisen oder einen Workflow beenden, falls er „hängt“.

## Identity Manager-Benutzeranwendungstreiber

Identity Manager unterstützt nicht nur Anforderungen von Endbenutzern zur Bereitstellung von Ressourcen, sondern ermöglicht außerdem die Initiierung von Bereitstellungsanforderungen als Reaktion auf Ereignisse, die in eDirectory auftreten. Der Identity Manager-*Benutzeranwendungstreiber* überwacht Ereignisse und reagiert mit der Initiierung der entsprechenden Bereitstellungsanforderungen. Diese Anforderungen können wiederum Workflows zur Verarbeitung des Genehmigungsverfahrens initiieren. Wenn entsprechend konfiguriert, unterstützt Identity Manager ein Szenario, in dem durch das Hinzufügen eines neuen Benutzers in eDirectory automatisch eine zuvor festgelegte Bereitstellungsanforderung und der entsprechende Workflow gestartet wird.

## Bereitstellungssystem

Das Bereitstellungssystem führt alle erforderlichen Prozesse zur Initiierung und Erfüllung der Bereitstellungsanforderungen aus. Wenn eine Anforderung eine oder mehrere Genehmigungen erfordert, ruft das Bereitstellungssystem das Workflow-System zum Starten eines Workflow-Prozesses auf. Sobald die erforderlichen Genehmigungen erteilt wurden, stellt das Bereitstellungssystem die angeforderte Ressource bereit.

Das Bereitstellungssystem speichert Informationen über verfügbare und ausstehende Bereitstellungsanforderungen im Identitätsdepot (eDirectory).

Zum Initiieren einer Anforderung oder zum Ausführen der Verarbeitung zur Erfüllung einer Anforderung greift das System über die Verzeichnisabstraktionsschicht auf das Identitätsdepot zu.

Weitere Informationen zur Verzeichnisabstraktionsschicht finden Sie in [Kapitel 4, „Konfigurieren der Verzeichnisabstraktionsschicht“](#), auf Seite 75.

## Workflow-System

Wenn für eine Bereitstellungsanforderung eine oder mehrere Genehmigungen erforderlich sind, koordiniert das Workflow-System den Genehmigungsverfahren. Während der Verarbeitung interagiert es mit folgenden Komponenten:

- Workflow-Datenbank
- Skript-Engine
- Audit
- SMTP
- Sicherheitssystem

## **Workflow-Datenbank**

Zum Protokollieren des Status der aktiven Workflows speichert das Workflow-System Informationen in einer Datenbank. Diese Datenbank enthält Informationen zu den Workflow-Prozessinstanzen, Arbeitslisten (Warteschlangen) und Adressaten der Workflows. Zudem werden alle Kommentare gespeichert, die während der Verarbeitung eines Workflow-Prozesses hinzugefügt werden.

## **Skript-Engine**

Das Workflow-System ruft die Skript-Engine auf, wenn ein Workflow einen auszuwertenden dynamischen Ausdruck enthält. Dynamische Ausdrücke können Variablen, Funktionen und Operatoren sowie Referenzen zu Entitäten in der Verzeichnisabstraktionsschicht enthalten.

## **Novell Audit**

Zum Protokollieren von Informationen zum Status eines Workflow-Prozesses interagiert das Workflow-System mit Novell Audit. Während seiner Verarbeitung protokolliert ein Workflow möglicherweise Informationen zu verschiedenen aufgetretenen Ereignissen. Benutzer können die Protokolldaten anschließend über die Berichterstellungswerkzeuge von Novell einsehen.

Weitere Informationen zum Einrichten der Protokollierung finden Sie in [Kapitel 5, „Einrichten der Protokollierung“](#), auf Seite 121. Informationen zur Steuerung des Umfangs der Protokollierungsmeldungen, die von der Identity Manager-Benutzeranwendung erzeugt werden, finden Sie in [Kapitel 12, „Konfiguration der Protokollierung“](#), auf Seite 213.

## **SMTP**

Während der Verarbeitung eines Workflow-Prozesses werden häufig Email-Benachrichtigungen versendet. Eine Email kann beispielsweise versendet werden, wenn eine Workflow-Aktivität einem neuen Adressaten zugewiesen wird.

Ein Administrator kann eine Email-Schablone in iManager bearbeiten und diese dann in einem Workflow-Prozess verwenden. Zur Laufzeit lädt das Workflow-System sie von eDirectory und ersetzt alle Tags mit geeignetem dynamischem Text für die Benachrichtigung.

E-Mail-Benachrichtigungen werden mit SMTP (Simple Mail Transfer Protocol) verarbeitet.

Grundlegende Schritte für das Einrichten von Email-Benachrichtigungen finden Sie in [Abschnitt 23.3, „Konfigurieren des Email-Servers“](#), auf Seite 356 und [Abschnitt 23.4, „Arbeiten mit den installierten Email-Schablonen“](#), auf Seite 357. Weitere Informationen zum Konfigurieren von Email-Benachrichtigungen für einen Workflow finden Sie in [„Konfigurieren der Workflow-Aktivitäten“](#) auf Seite 337.

## **Sicherheit**

Das Sicherheitssystem verarbeitet alle Sicherheitsaspekte einer Workflow-basierten Bereitstellungsanwendung.

Weitere Informationen zur Sicherheit von Workflows finden Sie in [Abschnitt 21.3, „Sicherheit bei der Bereitstellung“](#), auf Seite 319.

## 21.1.2 Bereitstellung und Workflow - Beispiel

Angenommen, ein Benutzer benötigt in einem IT-System ein Konto. Zum Einrichten des Kontos initiiert der Benutzer über die Identity Manager-Benutzeranwendung eine Anforderung. Durch diese Anforderung wird ein Workflow gestartet, der einen Genehmigungsvorgang koordiniert. Sobald die erforderlichen Genehmigungen erteilt wurden, ist die Anforderung erfüllt. Dieser Vorgang besteht aus drei grundlegenden Schritten, die im Folgenden kurz dargestellt werden.

### 1. Schritt: Initiierung der Anforderung

Der Benutzer durchsucht in der Identity Manager-Benutzeranwendung eine Liste mit Ressourcen nach *Kategorien* und wählt die bereitstellbare Ressource aus. Im Identitätsdepot wird die *bereitstellbare Ressource* ausgewählt und einer *Bereitstellungsanforderungsdefinition* zugeordnet. Die Bereitstellungsanforderungsdefinition ist das bedeutendste Objekt in einem Bereitstellungssystem. Es bindet eine bereitstellbare Ressource an einen *Workflow* und agiert als das Mittel, durch das der Workflow-Prozess dem Endbenutzer bereitgestellt wird. Die Bereitstellungsanforderungsdefinition enthält alle Informationen, die erforderlich sind, um dem Benutzer das *Formular für die anfängliche Anforderung* anzuzeigen und den Ablauf zu starten, der durch die ursprüngliche Anforderung ausgelöst wird.

In diesem Beispiel wählt der Benutzer die Ressource „Neues Konto“. Wenn der Benutzer die Anforderung initiiert, ruft die Webanwendung das Formular für die anfängliche Anforderung und die Beschreibung der zugeordneten *anfänglichen Anforderungsdaten* vom Bereitstellungssystem ab, das diese Objekte von der Bereitstellungsanforderungsdefinition erhält.

Wenn eine Bereitstellungsanforderung initiiert wird, protokolliert das Bereitstellungssystem den Initiator und den Empfänger. Der *Initiator* ist die Person, die die Anforderung gestellt hat. Der *Empfänger* ist die Person, an den die Anforderung gerichtet ist. In einigen Fällen sind Initiator und Empfänger dieselbe Person.

Jeder Bereitstellungsanforderung ist ein *Vorgang* zugeordnet. Der Vorgang legt fest, ob der Benutzer die Ressource *zuweisen* oder *entziehen* möchte.

### 2. Schritt: Genehmigung der Anforderung

Sobald der Benutzer eine Anforderung initiiert hat, startet das Bereitstellungssystem den Workflow-Prozess. Der *Workflow-Prozess* koordiniert die Genehmigungen. In diesem Beispiel muss die Anforderung von zwei Personen genehmigt werden, vom Manager und vom Supervisor des Benutzers. Wenn ein Benutzer in einem Workflow eine Genehmigung nicht erteilt, wird der Workflow beendet und die Anforderung zurückgewiesen.

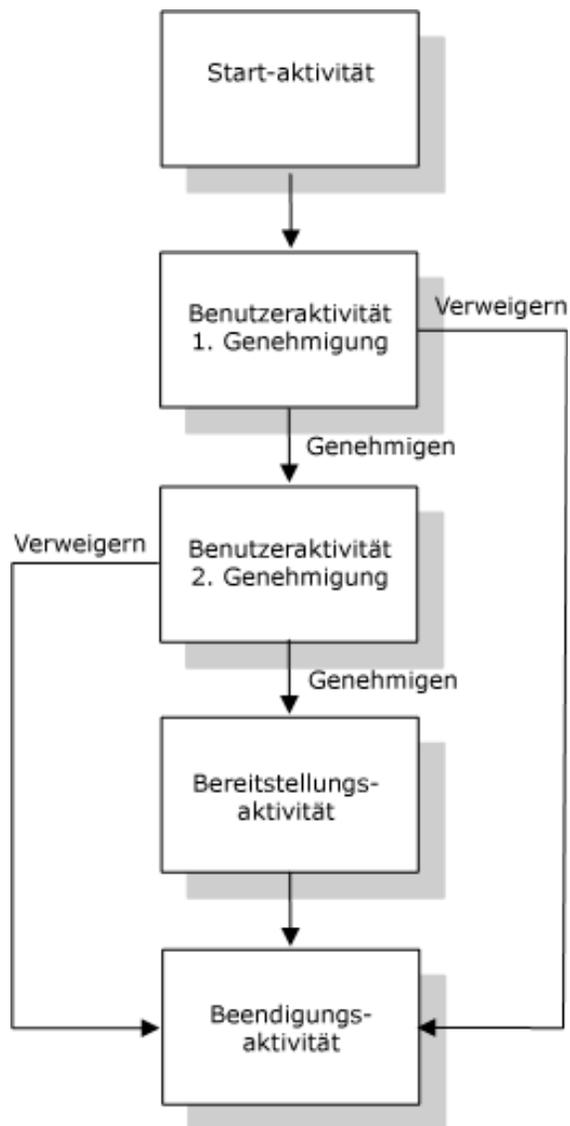
---

**Hinweis:** Im Lieferumfang von Identity Manager sind mehrere Schablonen für Bereitstellungsanforderungen enthalten, die bis zu fünf Genehmigungsstufen für einen Workflow unterstützen. In einer Folgeversion von Identity Manager werden in der Eclipse-basierten Design-Umgebung Werkzeuge zur Verfügung stehen, mit denen Sie benutzerdefinierte Workflow-Prozesse erstellen können. Weitere Informationen zu den Schablonen, die im Lieferumfang dieser Version enthalten sind, finden Sie in [Abschnitt 22.2, „Arbeiten mit den installierten Schablonen“](#), auf [Seite 324](#).

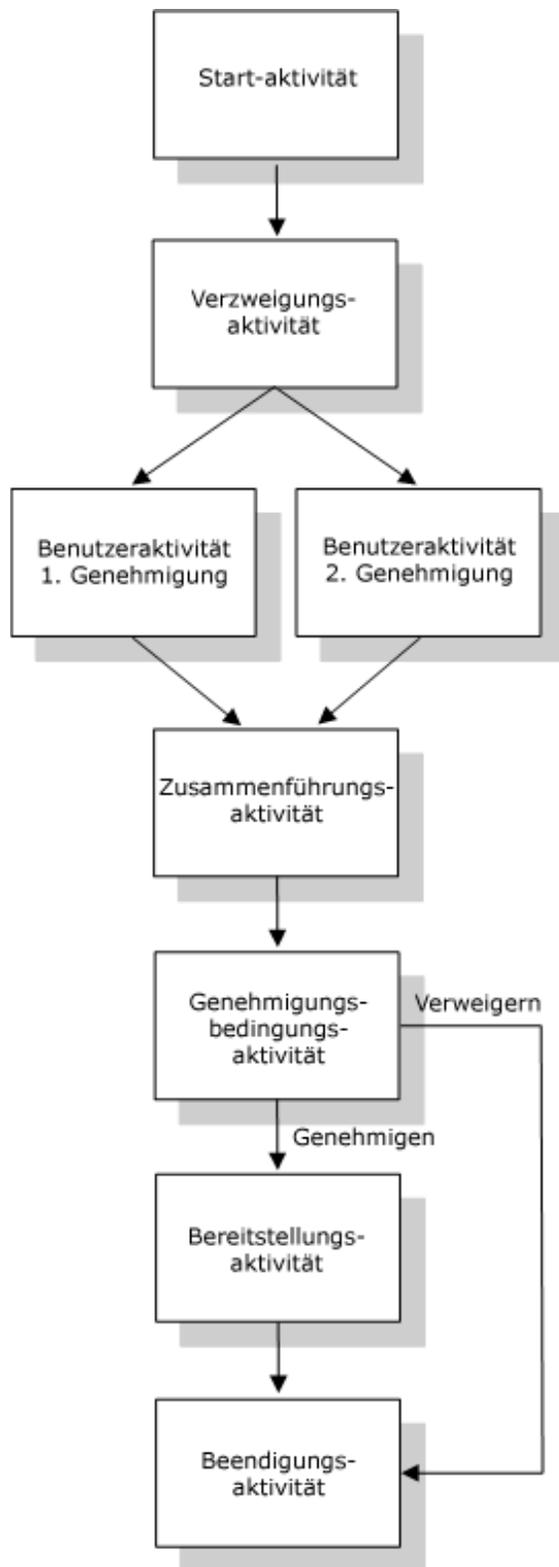
---

Workflows können Genehmigungen sequenziell oder parallel verarbeiten. Bei einem *sequenziellen Workflow* muss jede Genehmigungsaufgabe vor dem Beginn der nächsten verarbeitet werden. Bei einem *parallelen Workflow* können Benutzer die Genehmigungsaufgaben gleichzeitig bearbeiten.

**Sequenzieller Ablauf** Nachstehend finden Sie die grundlegende Struktur eines sequenziellen Workflows, für den zwei Genehmigungen erforderlich sind:



**Paralleler Ablauf** Nachstehend finden Sie die grundlegende Struktur eines parallelen Workflows, für den zwei Genehmigungen erforderlich sind:



**Hinweis:** Die Anzeigebezeichnungen („1. Genehmigung“, „2. Genehmigung“ usw.) können auf einfache Weise an Ihre Anforderungen angepasst werden. Für parallele Abläufe empfiehlt es sich,

Bezeichnungen anzugeben, die keine sequenzielle Verarbeitung implizieren. Sie könnten z. B. Bezeichnungen zuweisen wie „Eine von drei parallelen Genehmigungen“, „Zwei von drei parallelen Genehmigungen“ usw.

Die Workflowdefinition besteht aus folgenden Komponenten:

Prozesskomponenten	Beschreibung
Aktivitäten	<p>Eine Aktivität ist ein Objekt, das eine Aufgabe darstellt. Eine Aktivität kann dem Benutzer Informationen anzeigen und auf Interaktionen des Benutzers reagieren oder im Hintergrund für den Benutzer nicht sichtbare Funktionen ausführen.</p> <p>In den oben angeführten Beispielen für Workflows werden die Aktivitäten durch Felder dargestellt.</p> <p>In der Identity Manager-Benutzeranwendung werden Benutzeraktivitäten, die den Genehmigungsprozess abwickeln, als <b>Aufgaben</b> bezeichnet. Ein Endbenutzer kann die Liste mit den Aufgaben, die sich in der Warteschlange befinden, abrufen, indem er auf <b>Meine Aufgaben</b> unter <b>Meine Arbeit</b> klickt. Wenn ein Benutzer sehen möchte, welche Workflow-Aktivitäten für eine bestimmte Aufgabe ausgeführt wurden, kann er die entsprechende Aufgabe auswählen und auf die Schaltfläche <b>Kommentarverlauf anzeigen</b> im Formular „Aufgabendetail“ klicken.</p> <p>Wenn der Benutzer sehen möchte, welche Workflow-Aktivitäten für eine bestimmte Bereitstellungsanforderung ausgeführt wurden, kann er auf <b>Meine Anforderungen</b> klicken, die Anforderung auswählen und auf die Schaltfläche <b>Kommentar und Ablaufverlauf anzeigen</b> im Formular „Anforderungsdetail“ klicken.</p> <p>Weitere Informationen zu den Aktionen <b>Meine Aufgaben</b> und <b>Meine Anforderungen</b> finden Sie im <i>Identity Manager Benutzeranwendung-Benutzerhandbuch</i>.</p>
Links	<p>Aktivitäten werden durch Links in einem Workflow zusammengehalten. Ein Link verkörpert einen Pfad, der zwischen zwei Aktivitäten eingehalten werden muss.</p> <p>Eine Aktivität kann mehrere ein- und ausgehende Links haben. Wenn eine Aktivität mehr als einen ausgehenden Link hat, hängt der ausgewählte Link vom <b>Resultat</b> der Aktivität ab. Das Resultat ist das Endergebnis der von der Aktivität ausgeführten Verarbeitung. Eine Benutzeraktivität kann z. B. in Abhängigkeit von der vom Benutzer unternommenen <b>Aktion</b> das Resultat „Genehmigt“ oder „Verweigert“ haben.</p> <p>In den oben angeführten Beispielen für Workflows werden die Links durch Pfeile dargestellt.</p>

**Startaktivität** Der Workflow-Prozess beginnt mit der Ausführung der *Startaktivität*. Diese Aktivität initialisiert ein Arbeitsdokument, das die anfänglichen Anforderungsdaten verwendet. Es bindet außerdem mehrere Systemwerte wie z. B. Initiator und Empfänger, sodass diese in Skript-Ausdrücken verwendet werden können.

**Benutzeraktivitäten** Wenn die Ausführung der Startaktivität beendet ist, leitet das Workflow-System die Verarbeitung an die erste *Benutzeraktivität* im Ablauf weiter. Eine Benutzeraktivität ist eine Aktivität, die Benutzerinteraktionen unterstützt. Die Aktivität zeigt zum Verarbeiten dieser Interaktionen ein Formular an, wodurch der Benutzer die Möglichkeit hat, auf die Anforderung zu

reagieren. In den oben angeführten Beispielen für Workflows sind 1. Genehmigung und 2. Genehmigung Beispiele für Benutzeraktivitäten. Die Anzeigebezeichnungen für Benutzeraktivitäten können übersetzt werden, um internationalen Anforderungen zu genügen.

Eine Benutzeraktivität unterstützt möglicherweise eine oder mehrere der folgenden *Aktionen*:

- Beanspruchen
- Genehmigen
- Verweigern
- Ablehnen
- Neu zuweisen (nur für Manager der Organisation und Benutzeranwendungsadministratoren verfügbar)

---

**Hinweis:** Die Felder und Schaltflächen auf dem Formular sind je nach angeforderter Ressource und nach Konfiguration des Workflows unterschiedlich. Die Aktion *Ablehnen* wird z. B. von vielen der im Lieferumfang enthaltenen Schablonen nicht unterstützt.

---

Bei einer Benutzeraktivität gibt es fünf mögliche *Resultate*:

- Genehmigt
- Verweigert
- Abgelehnt
- Fehler
- Zeitüberschreitung

---

**Hinweis:** Die Resultate „Fehler“ und „Zeitüberschreitung“ können auftreten, ohne dass der Benutzer eine Aktion unternommen hat.

---

Wenn der Benutzer die Anforderung genehmigt, übergibt der Workflow die Kontrolle an die nächste Aktivität im Ablauf. Wenn keine weitere Genehmigungen erforderlich sind, wird die Ressource bereitgestellt. Wenn der Benutzer die Anforderung ablehnt, wird der Arbeitsschritt an die nächste Aktivität im Workflow weitergeleitet und die Anforderung wird abgelehnt. Wahlweise kann der Benutzer die Aufgabe neu zuordnen (sofern er ein Vorgesetzter oder ein Benutzeranwendungsadministrator ist), wodurch der Arbeitsschritt in die Warteschlange eines anderen Benutzers gestellt wird.

---

**Hinweis:** Bei den im Lieferumfang enthaltenen Bereitstellungsanforderungsschablonen wird ein Workflow beendet, wenn eine Anforderung abgelehnt wird. Wenn eine Anforderung abgelehnt wird, wird der Arbeitsschritt an die Beendigungsaktivität weitergeleitet, die den Ablauf beendet.

---

Der Benutzer, dem eine Benutzeraktivität zugewiesen wurde, wird als *Adressat* bezeichnet. Der Adressat einer Aktivität kann per Email über die ihm zugewiesene Aufgabe benachrichtigt werden. Wenn der Adressat die der Aktivität zugeordneten Arbeit erledigen möchte, kann er auf die URL in der Email klicken, die Aufgabe in der Arbeitsliste (Warteschlange) suchen und die Aufgabe beanspruchen.

Der Adressat muss innerhalb der festgelegten Zeit auf eine Benutzeraktivität reagieren, andernfalls tritt bei der Aktivität eine Zeitüberschreitung auf. Üblicherweise wird das

*Zeitüberschreitungsintervall* in Stunden oder Tagen festgelegt, um dem Benutzer genügend Zeit für eine Reaktion zur Verfügung zu stellen.

Wenn es bei einer Aktivität zu einer Zeitüberschreitung kommt, versucht der Workflow-Prozess möglicherweise in Abhängigkeit von den für die Aktivität festgelegten *Wiederholungsversuchen* erneut, die Aktivität zu erledigen. In einigen Fällen ist der Workflow-Prozess möglicherweise so konfiguriert, dass eine Aktivität, bei der es zu einer Zeitüberschreitung kam, an einen anderen Benutzer eskaliert wird. In diesem Fall wird die Aktivität einem neuen Adressaten zugewiesen (z. B. dem Manager des Benutzers), damit dieser die Möglichkeit hat, die Arbeit der Aktivität zu erledigen. Falls beim letzten Wiederholversuch eine Zeitüberschreitung auftritt, wird die Aktivität entsprechend der Konfiguration des Workflows als genehmigt oder abgelehnt markiert.

**Bedingte Aktivitäten** Während der Verarbeitung ist es möglich, dass ein Workflow-Prozess einen Test ausführt und das Resultat überprüft, um zu sehen, was als Nächstes zu tun ist. Die *bedingte Aktivität* bietet diese Funktion. Bedingte Aktivitäten verwenden für die Definition einer auszuwertenden Bedingung einen Skript-Ausdruck. In den oben dargestellten Beispielen ist die Genehmigungsaktivität ein Beispiel für eine bedingte Aktivität.

Bedingte Aktivitäten unterstützen drei mögliche *Resultate*:

- Wahr
- Falsch
- Fehler

**Zusammenführungs- und Verzweigungsaktivitäten** In einem Workflow, der die parallele Verarbeitung unterstützt, ermöglicht die *Verzweigungsaktivität*, dass zwei Benutzer parallel auf verschiedene Bereiche des Arbeitsschritts zugreifen können. Sobald die Benutzer ihre Arbeit abgeschlossen haben, synchronisiert die *Zusammenführungsaktivität* die eingehenden Verzweigungen des Ablaufs.

**Bereitstellungsaktivität** Die *Bereitstellungsaktivität* erfüllt die Bereitstellungsanforderung. Diese Aktivität wird nur ausgeführt, wenn alle erforderlichen Genehmigungen erteilt wurden.

Weitere Informationen zum Arbeitsschritt der Bereitstellung finden Sie in [„3. Schritt: Erfüllen der Anforderung“ auf Seite 318](#).

**Beendigungsaktivität** Die *Beendigungsaktivität* ist die letzte Aktivität eines Workflows. Wenn alle Aktivitäten innerhalb eines Ablaufs erledigt sind und das Endergebnis des Ablaufs verfügbar ist, kann die Beendigungsaktivität ausgeführt werden. Das Workflow-System kann den Endstatus des Prozesses ermitteln, indem es die Links zur Beendigungsaktivität überprüft. Der Gesamtstatus eines Ablaufs wird auf *Genehmigt* gesetzt, wenn ein Genehmigungs-Link die Beendigungsaktivität erreicht. Falls ein anderes Resultat („Verweigern“, „Zeitüberschreitung“ oder „Fehler“) zur Beendigungsaktivität führt, lautet der Gesamtstatus des Ablaufs *Verweigert*.

Wenn ein Workflow-Prozess die Beendigungsaktivität mit dem Status „Genehmigt“ erreicht, ist der Genehmigungsvorgang vollständig und die Bereitstellungsanforderung kann erfüllt werden.

### 3. Schritt: Erfüllen der Anforderung

Wenn eine Bereitstellungsanforderung genehmigt wurde, kann das Workflow-System mit der *Bereitstellung* beginnen. An diesem Punkt wird die Kontrolle wieder an das Bereitstellungssystem übergeben.

Das Bereitstellungssystem kann zum Erfüllen der Bereitstellungsanforderung eine Identity Manager-Berechtigung ausführen oder direkt ein eDirectory-Objekt und dessen Attribute bearbeiten. Während der Bereitstellungsstufe erstellt es etwaige verwandte Objekte und zeichnet die Ergebnisse der Bereitstellungsaktion auf dem Empfänger, wie in der Bereitstellungsdatendefinition beschrieben, auf. Abhängig davon, ob es sich bei der Anforderung des Benutzers um einen Erteilungs- oder einen Entziehungsvorgang handelt, wird möglicherweise der Wert eines Attributs auf dem Empfänger gesetzt oder entfernt oder ein Eintrag aus einem mehrwertigen Attribut auf dem Empfänger entfernt bzw. zu diesem hinzugefügt. Die involvierten Attribute sind eDirectory-Attribute (möglicherweise bereitgestellt, indem eine Hilfsklasse zum Empfänger hinzugefügt wurde). Die Attributwerte können einfach sein oder es kann sich um komplexere Werte handeln, die es dem Bereitstellungssystem ermöglichen, den Wert interner untergeordneter Attribute festzulegen.

## 21.2 Konfiguration und Verwaltung bei der Bereitstellung

Zum Konfigurieren einer Bereitstellungsanforderungsdefinition binden Sie sie mit iManager an eine bereitstellbare Ressource, legen Sie die Laufzeit-Charakteristika des zugeordneten Workflows fest und aktivieren Sie sie. Identity Manager wird mit mehreren vorimplementierten Bereitstellungsanforderungsdefinitionen und Workflows geliefert. Sie können diese als *Schablonen* für den Aufbau Ihres eigenen Bereitstellungssystems verwenden. Die installierten Schablonen sind leicht zu verwenden und dennoch flexibel genug, um den Anforderungen vieler Geschäftsumgebungen zu entsprechen. Definieren Sie zum Einrichten Ihres Systems basierend auf den installierten Schablonen neue Objekte und passen Sie sie an die Erfordernisse Ihres Unternehmens an.

Sobald eine Bereitstellungsanforderungsdefinition konfiguriert wurde, können Sie über iManager den Status von aktiven Workflow-Prozessen anzeigen, Aktivitäten innerhalb der Workflows neu zuweisen oder einen Workflow beenden, falls er „hängt“.

Weitere Informationen zur Verwendung von iManager zur Konfiguration und zur Verwaltung bei der Bereitstellung finden Sie in [Kapitel 22, „Konfigurieren von Bereitstellungsanforderungsdefinitionen“](#), auf Seite 323 und [Kapitel 23, „Verwalten von Bereitstellungs-Workflows“](#), auf Seite 347.

## 21.3 Sicherheit bei der Bereitstellung

Wenn sich ein Benutzer bei der Identity Manager-Benutzeranwendung anmeldet, authentifiziert das Sicherheitssystem diesen Benutzer und setzt Zugriffssteuerungen, um Bereitstellungs- und Workflow-Objekte vor unbefugtem Gebrauch zu schützen. Dadurch wird sichergestellt, dass der Benutzer nur die Bereitstellungsanforderungsdefinitionen sehen kann, auf die er Zugriff hat. Neben der Ausführung von Authentifizierungs- und Autorisierungsservices für die Benutzeranwendung verwaltet das Sicherheitssystem Vertretungs- und Delegiertenzuweisungen.

- Ein *Delegierter* ist ein Benutzer, der zur Ausführung von Arbeiten eines anderen Benutzers autorisiert ist. Eine Delegiertenzuweisung gilt für eine bestimmte Bereitstellungsanforderungsdefinition.
- Eine *Vertretung* ist ein Benutzer, der autorisiert ist, die gesamte Arbeit von einem oder mehreren Benutzern, Gruppen oder Containern auszuführen. Im Gegensatz zu Delegiertenzuweisungen sind Vertretungszuweisungen unabhängig von Bereitstellungsanforderungsdefinitionen und gelten daher für alle Arbeiten und Einstellungen.

Bei aktivierter Protokollierung werden alle Aktionen, die von einer Vertretung oder von einem Delegierten ausgeführt werden, gemeinsam mit den Aktionen anderer Benutzer protokolliert. Wenn eine Aktion von einer Vertretung oder einem Delegierten eines Benutzers ausgeführt wird, zeigt dies die Protokollmeldung eindeutig an. Außerdem wird auch jede neue Vertretungs- oder Delegiertenzuweisung protokolliert.

Wenn eine Bereitstellungsanforderungsdefinition so konfiguriert ist, dass Email-Benachrichtigungen generiert werden, werden neben den Adressaten auch die Vertretungen per Email benachrichtigt. Delegierte erhalten keine E-Mail-Benachrichtigungen.

**Sicherheitsfunktionen des Workflows** Das Sicherheitssystem erkennt folgende Sicherheitsfunktionen:

Funktion	Beschreibung	Rechte
Benutzeranwendungsadministrator	Locksmith-Benutzer mit vollständigen Verwaltungsrechten.	<p>Der Benutzeranwendungsadministrator kann folgende Aufgaben in <b>iManager</b> ausführen:</p> <ul style="list-style-type: none"> <li>• Konfigurieren von Bereitstellungsanforderungen</li> <li>• Verwaltung von bereits aktiven Workflows</li> </ul> <p>Der Benutzeranwendungsadministrator kann folgende Aufgaben in der <b>Benutzeranwendung</b> ausführen:</p> <ul style="list-style-type: none"> <li>• Anzeigen und Bearbeiten aller in der Warteschlange befindlichen Workflow-Aufgaben.</li> <li>• Definieren von Vertretungs- und Delegiertenzuweisungen für alle Benutzer des Systems.</li> <li>• Anzeigen von versteckten Informationen (versteckte Attribute) für alle Benutzer des Systems.</li> <li>• Erstellen von Aufgabengruppenmanagern und deren Zuweisung zu Gruppen. Der Benutzeranwendungsadministrator ist der einzige Benutzer, der Aufgabengruppenmanager erstellen und zuweisen kann.</li> </ul>

---

**Hinweis:** Die Registerkarte **Administration** der Identity Manager-Benutzeranwendung bietet Werkzeuge zum Zuweisen von Rechten für die Verwaltung der Benutzeranwendung. Wenn Sie diese Registerkarte verwenden möchten, müssen Sie sich zunächst als der Benutzer anmelden, der bei der Installation als Benutzeranwendungsadministrator festgelegt wurde.

---

Weitere Informationen zur Verwendung der Sicherheitsfunktionen der Benutzeranwendung finden Sie in [Kapitel 11, „Sicherheitskonfiguration“](#), auf Seite 209.

Funktion	Beschreibung	Rechte
Vorgesetzter	<p>Supervisor, dem ein Mitarbeiter direkt unterstellt ist. Jeder Benutzer hat nur einen Vorgesetzten.</p> <hr/> <p><b>Tipp:</b> Der Vorgesetzte kann auch als ein administrativer Manager verstanden werden.</p> <hr/>	<p>Der Vorgesetzte verfügt über folgende Rechte:</p> <ul style="list-style-type: none"> <li>• Anzeigen aller Aufgaben, die sich in den Workflow-Warteschlangen seines Teams befinden. Diese Funktion gilt für eine einzelne Ebene in der Verwaltungshierarchie, daher kann eine übergeordnete Person eines Vorgesetzten nicht die Aufgaben von Mitarbeitern sehen, die dem Vorgesetzten direkt unterstellt sind.</li> <li>• Bearbeiten von Aufgaben für direkt unterstellte Mitarbeiter, es sei denn, ein direkt Unterstellter hat eine Aufgabe, die einer Gruppe zugeordnet ist, deren Aufgabengruppenmanager nicht der Vorgesetzte ist. In diesem Fall kann der Vorgesetzte die Aufgabe zwar anzeigen, diese aber nicht bearbeiten. Bei der Eskalation wird die Aufgabe nicht zum Vorgesetzten, sondern zum Aufgabengruppenmanager verschoben.</li> <li>• Beanspruchung und Rückgabe von Aufgaben sowie Neuzuweisung von Aufgaben an die Teammitglieder.</li> <li>• Definition von Vertretungs- und Delegiertenbeziehungen für ihn selbst und seine Teammitglieder.</li> <li>• Anzeigen von versteckten Attributen für seine Teammitglieder.</li> </ul>

Funktion	Beschreibung	Rechte
Aufgabengruppenmanager	<p>Benutzer, der für den Aufgabensatz zuständig ist, der einer Aufgabengruppe zugeordnet ist. Eine Aufgabengruppe ist eine Erweiterung des Objekts „LDAP-Gruppe“. Jede Aufgabengruppe kann nur einen Aufgabengruppenmanager haben.</p> <p>Aufgabengruppenmanager werden vom Benutzeranwendungsadministrator zugewiesen.</p> <p>Wenn eine Aufgabe einer Gruppe zugewiesen ist, enthält das <code>srvprvTaskManager</code>-Attribut für die Gruppe den DN des zum Aufgabengruppenmanager bestimmten Benutzers. Um eine bessere Leistung zu erzielen, werden Aufgabengruppenmanager auch durch ein Attribut auf dem Benutzerobjekt identifiziert. Das <code>srvprvsTaskManager</code>-Attribut wird für den Benutzer, der zum Aufgabengruppenmanager bestimmt wurde, auf „Wahr“ gesetzt.</p>	<p>Der Aufgabengruppenmanager verfügt über folgende Rechte:</p> <ul style="list-style-type: none"> <li>Anzeigen und Bearbeiten aller Aufgaben, die einer unter seiner Leitung stehenden Gruppe zugewiesen sind.</li> </ul> <p>Der Aufgabengruppenmanager verfügt <b>nicht</b> über folgende Rechte:</p> <ul style="list-style-type: none"> <li>Erstellen von Ressourcen oder Zurückziehen von Anforderungen.</li> <li>Definieren von Vertretungs- oder Delegiertenbeziehungen.</li> <li>Anzeigen von versteckten Attributen für seine Teammitglieder.</li> </ul>

**Hinweis:** Jeder Benutzer kann versteckte Attribute anzeigen, die seiner eigenen Identität zugeordnet sind.

**Definieren von Vertretungs- und Delegiertenbeziehungen** Verwenden Sie zum Definieren einer Vertretungszuweisung für einen Benutzer die Seite *Team-Vertretungszuweisungen* der Registerkarte *Anforderungen und Genehmigungen* auf der Identity Manager-Schnittstelle. Verwenden Sie zum Definieren einer Delegiertenzuweisung für einen Benutzer die Seite *Team-Delegiertenzuweisungen*, die auch auf der Registerkarte *Anforderungen und Genehmigungen* verfügbar ist.

**Erstellen von Aufgabengruppenmanagern** Verwenden Sie zum Definieren eines Aufgabengruppenmanagers für eine Aufgabengruppe die Seite *Benutzer oder Gruppe erstellen* der Registerkarte *Identitätsselbstbedienung* auf der Identity Manager-Schnittstelle.

Ausführliche Informationen zum Definieren von Aufgabengruppenmanagern, Vertretungen und Delegierten finden Sie im *Identity Manager-Benutzeranwendung- Benutzerhandbuch*.

# Konfigurieren von Bereitstellungsanforderungsdefini- tionen

# 22

Dieses Kapitel enthält Anweisungen für die Konfiguration von Bereitstellungsanforderungsdefinitionen. Es werden folgende Themen erläutert:

- [Abschnitt 22.1, „Allgemeines zum Plugin für die Konfiguration der Bereitstellungsanforderungen“, auf Seite 323](#)
- [Abschnitt 22.2, „Arbeiten mit den installierten Schablonen“, auf Seite 324](#)
- [Abschnitt 22.3, „Konfigurieren einer Bereitstellungsanforderungsdefinition“, auf Seite 328](#)

## 22.1 Allgemeines zum Plugin für die Konfiguration der Bereitstellungsanforderungen

Für die Konfiguration einer Bereitstellungsanforderungsdefinition muss das Plugin für die Konfiguration der Bereitstellungsanforderungen von iManager verwendet werden. Über dieses Plugin können Sie die Bereitstellungsanforderungsdefinition an eine bereitstellbare Ressource binden, die Laufzeit-Charakteristika des zugeordneten Workflows festlegen und ihn für die Verwendung aktivieren. In dieser Version werden die bereitstellbaren Ressourcen Identity Manager-Berechtigungen zugeordnet.

---

**Hinweis:** Sie können auch Bereitstellungsanforderungsdefinitionen ausführen, die Attributen im Identitätsdepot direkt zugeordnet sind. Die installierten Schablonen unterstützen diese Art Ressource jedoch nicht, da sie auf Berechtigungen basieren.

---

Das Plugin für die Konfiguration der Bereitstellungsanforderungen befindet sich in der Kategorie *Identity Manager* in iManager. Es enthält die Aufgabe *Bereitstellungsanforderungen*, die Teil der Funktion *Konfiguration für Bereitstellungsanforderungen* ist. Die Aufgabe „Bereitstellungsanforderungen“ besteht aus den folgenden Teilfenstern:

---

Teilfenster	Beschreibung
Bereitstellungsanforderungen - Treiber-auswahl	Ermöglicht Ihnen die Auswahl eines Treibers für die Identity Manager-Benutzeranwendung. Der Treiber enthält mehrere vorimplementierte Bereitstellungsdefinitionen, sodass Sie einen Treiber auswählen müssen, bevor Sie mit der Konfiguration der Bereitstellungsanforderungen beginnen können.

---

Teilfenster	Beschreibung
Konfiguration für Bereitstellungsanforderungen	<p>Stellt Werkzeuge für folgende Funktionen zur Verfügung:</p> <ul style="list-style-type: none"> <li>• Durchsuchen der verfügbaren Bereitstellungsanforderungsdefinitionen und Auswahl der zu konfigurierenden Definition</li> <li>• Erstellen einer neuen Bereitstellungsanforderungsdefinition, die auf einer vorhandenen Definition basiert</li> <li>• Einrichten der Eigenschaften einer Bereitstellungsanforderungsdefinition</li> <li>• Zuweisen der Bereitstellungsanforderungsdefinition zu einer bereitstellbaren Ressource</li> <li>• Bearbeiten des Adressaten und der Einstellungen für die Zeitüberschreitung für jede Aktivität im zugeordneten Workflow</li> </ul> <p>Wenn Sie eine neue Bereitstellungsanforderung erstellen oder eine vorhandene Anforderung bearbeiten möchten und eine entsprechende Auswahl vornehmen, führt das Plugin den <b>Konfigurationsassistenten für Bereitstellungsanforderungen</b> aus.</p>

## 22.2 Arbeiten mit den installierten Schablonen

Identity Manager wird mit mehreren vorimplementierten Bereitstellungsanforderungsdefinitionen und Workflows geliefert. Sie können diese als *Schablonen* zum Erstellen Ihres eigenen Bereitstellungssystems verwenden. Richten Sie Ihr System ein, indem Sie basierend auf den installierten Schablonen neue Objekte definieren und diese anschließend an die Anforderungen in Ihrer Organisation anpassen.

Anhand der installierten Schablonen können Sie die Anzahl der Genehmigungsstufen ermitteln, die für die Erfüllung der Anforderung erforderlich sind. Sie können folgende Genehmigungsstufen für eine Bereitstellungsanforderung festlegen:

- Keine Genehmigungen
- Eine Genehmigungsstufe
- Zwei Genehmigungsstufen
- Drei Genehmigungsstufen
- Vier Genehmigungsstufen
- Fünf Genehmigungsstufen

Sie können außerdem festlegen, ob die sequenzielle oder die parallele Verarbeitung unterstützt wird und ob Sie die Anforderung im Falle einer Zeitüberschreitung bei der Verarbeitung genehmigen oder verweigern möchten.

Weitere Informationen zu Mustern für das Workflow-Design finden Sie in [Abschnitt 21.1.2](#), „Bereitstellung und Workflow - Beispiel“, auf Seite 313.

Im Lieferumfang von Identity Manager sind folgende Schablonen enthalten:

Schablone	Beschreibung
Selbstbereitstellungsgenehmigung	Eine Bereitstellungsanforderung kann ohne Genehmigungen erfüllt werden.
Genehmigung in einer Stufe (Genehmigung bei Zeitüberschreitung)	Zur Erfüllung einer Bereitstellungsanforderung ist eine einzelne Genehmigung erforderlich. Wenn bei einer Aktivität eine Zeitüberschreitung auftritt, genehmigt die Aktivität die Anforderung und der Arbeitsschritt fährt mit der nächsten Aktivität fort.
Sequenzielle Genehmigung in zwei Stufen (Genehmigung bei Zeitüberschreitung)	Zur Erfüllung einer Bereitstellungsanforderung sind zwei Genehmigungen erforderlich. Wenn bei einer Aktivität eine Zeitüberschreitung auftritt, genehmigt die Aktivität die Anforderung und der Arbeitsschritt fährt mit der nächsten Aktivität fort.  Diese Schablone unterstützt die sequenzielle Verarbeitung.
Sequenzielle Genehmigung in drei Stufen (Genehmigung bei Zeitüberschreitung)	Zur Erfüllung einer Bereitstellungsanforderung sind drei Genehmigungen erforderlich. Wenn bei einer Aktivität eine Zeitüberschreitung auftritt, genehmigt die Aktivität die Anforderung und der Arbeitsschritt fährt mit der nächsten Aktivität fort.  Diese Schablone unterstützt die sequenzielle Verarbeitung.
Sequenzielle Genehmigung in vier Stufen (Genehmigung bei Zeitüberschreitung)	Zur Erfüllung einer Bereitstellungsanforderung sind vier Genehmigungen erforderlich. Wenn bei einer Aktivität eine Zeitüberschreitung auftritt, genehmigt die Aktivität die Anforderung und der Arbeitsschritt fährt mit der nächsten Aktivität fort.  Diese Schablone unterstützt die sequenzielle Verarbeitung.
Sequenzielle Genehmigung in fünf Stufen (Genehmigung bei Zeitüberschreitung)	Zur Erfüllung einer Bereitstellungsanforderung sind fünf Genehmigungen erforderlich. Wenn bei einer Aktivität eine Zeitüberschreitung auftritt, genehmigt die Aktivität die Anforderung und der Arbeitsschritt fährt mit der nächsten Aktivität fort.  Diese Schablone unterstützt die sequenzielle Verarbeitung.
Genehmigung in einer Stufe (Ablehnung bei Zeitüberschreitung)	Zur Erfüllung einer Bereitstellungsanforderung ist eine einzelne Genehmigung erforderlich. Wenn bei einer Aktivität eine Zeitüberschreitung auftritt, wird die Anforderung vom Workflow abgelehnt.  Diese Schablone unterstützt die sequenzielle Verarbeitung.

Schablone	Beschreibung
Sequenzielle Genehmigung in zwei Stufen (Ablehnung bei Zeitüberschreitung)	<p>Zur Erfüllung einer Bereitstellungsanforderung sind zwei Genehmigungen erforderlich. Wenn bei einer Aktivität eine Zeitüberschreitung auftritt, wird die Anforderung vom Workflow abgelehnt.</p> <p>Diese Schablone unterstützt die sequenzielle Verarbeitung.</p>
Sequenzielle Genehmigung in drei Stufen (Ablehnung bei Zeitüberschreitung)	<p>Zur Erfüllung einer Bereitstellungsanforderung sind drei Genehmigungen erforderlich. Wenn bei einer Aktivität eine Zeitüberschreitung auftritt, wird die Anforderung vom Workflow abgelehnt.</p> <p>Diese Schablone unterstützt die sequenzielle Verarbeitung.</p>
Sequenzielle Genehmigung in vier Stufen (Ablehnung bei Zeitüberschreitung)	<p>Zur Erfüllung einer Bereitstellungsanforderung sind vier Genehmigungen erforderlich. Wenn bei einer Aktivität eine Zeitüberschreitung auftritt, wird die Anforderung vom Workflow abgelehnt.</p> <p>Diese Schablone unterstützt die sequenzielle Verarbeitung.</p>
Sequenzielle Genehmigung in fünf Stufen (Ablehnung bei Zeitüberschreitung)	<p>Zur Erfüllung einer Bereitstellungsanforderung sind fünf Genehmigungen erforderlich. Wenn bei einer Aktivität eine Zeitüberschreitung auftritt, wird die Anforderung vom Workflow abgelehnt.</p> <p>Diese Schablone unterstützt die sequenzielle Verarbeitung.</p>
Parallele Genehmigung in zwei Stufen (Genehmigung bei Zeitüberschreitung)	<p>Zur Erfüllung einer Bereitstellungsanforderung sind zwei Genehmigungen erforderlich. Wenn bei einer Aktivität eine Zeitüberschreitung auftritt, genehmigt die Aktivität die Anforderung und der Arbeitsschritt fährt mit der nächsten Aktivität fort.</p> <p>Diese Schablone unterstützt die parallele Verarbeitung.</p>
Parallele Genehmigung in drei Stufen (Genehmigung bei Zeitüberschreitung)	<p>Zur Erfüllung einer Bereitstellungsanforderung sind drei Genehmigungen erforderlich. Wenn bei einer Aktivität eine Zeitüberschreitung auftritt, genehmigt die Aktivität die Anforderung und der Arbeitsschritt fährt mit der nächsten Aktivität fort.</p> <p>Diese Schablone unterstützt die parallele Verarbeitung.</p>
Parallele Genehmigung in vier Stufen (Genehmigung bei Zeitüberschreitung)	<p>Zur Erfüllung einer Bereitstellungsanforderung sind vier Genehmigungen erforderlich. Wenn bei einer Aktivität eine Zeitüberschreitung auftritt, genehmigt die Aktivität die Anforderung und der Arbeitsschritt fährt mit der nächsten Aktivität fort.</p> <p>Diese Schablone unterstützt die parallele Verarbeitung.</p>

Schablone	Beschreibung
Parallele Genehmigung in fünf Stufen (Genehmigung bei Zeitüberschreitung)	<p>Zur Erfüllung einer Bereitstellungsanforderung sind fünf Genehmigungen erforderlich. Wenn bei einer Aktivität eine Zeitüberschreitung auftritt, genehmigt die Aktivität die Anforderung und der Arbeitsschritt fährt mit der nächsten Aktivität fort.</p> <p>Diese Schablone unterstützt die parallele Verarbeitung.</p>
Parallele Genehmigung in zwei Stufen (Ablehnung bei Zeitüberschreitung)	<p>Zur Erfüllung einer Bereitstellungsanforderung sind zwei Genehmigungen erforderlich. Wenn bei einer Aktivität eine Zeitüberschreitung auftritt, wird die Anforderung vom Workflow abgelehnt.</p> <p>Diese Schablone unterstützt die parallele Verarbeitung.</p>
Parallele Genehmigung in drei Stufen (Ablehnung bei Zeitüberschreitung)	<p>Zur Erfüllung einer Bereitstellungsanforderung sind drei Genehmigungen erforderlich. Wenn bei einer Aktivität eine Zeitüberschreitung auftritt, wird die Anforderung vom Workflow abgelehnt.</p> <p>Diese Schablone unterstützt die parallele Verarbeitung.</p>
Parallele Genehmigung in vier Stufen (Ablehnung bei Zeitüberschreitung)	<p>Zur Erfüllung einer Bereitstellungsanforderung sind vier Genehmigungen erforderlich. Wenn bei einer Aktivität eine Zeitüberschreitung auftritt, wird die Anforderung vom Workflow abgelehnt.</p> <p>Diese Schablone unterstützt die parallele Verarbeitung.</p>
Parallele Genehmigung in fünf Stufen (Ablehnung bei Zeitüberschreitung)	<p>Zur Erfüllung einer Bereitstellungsanforderung sind fünf Genehmigungen erforderlich. Wenn bei einer Aktivität eine Zeitüberschreitung auftritt, wird die Anforderung vom Workflow abgelehnt.</p> <p>Diese Schablone unterstützt die parallele Verarbeitung.</p>

**Workflows und bereitstellbare Ressourcen** Jede dieser Bereitstellungsanforderungsdefinitionen verfügt über eine vorkonfigurierte Bindung an einen Workflow und an eine bereitstellbare Ressource. Sie können die der Anforderungsdefinition zugewiesene bereitstellbare Ressource ändern, nicht aber den Workflow oder dessen Topologie.

**Kategorien für Bereitstellungsanforderungen** Jede Bereitstellungsanforderungsschablone ist zugleich an eine *Kategorie* gebunden. Kategorien sind praktisch für die Organisation von Bereitstellungsanforderungen für den Endbenutzer. Die Standardkategorie für alle Bereitstellungsanforderungsschablonen ist *Berechtigungen*. Der Categorieschlüssel, d. h. der Wert des `srvprvCategoryKey`-Attributs, ist *entitlements* (Kleinschreibung).

Sie können zur Erstellung von eigenen Kategorien den Verzeichnisabstraktionsschicht-Editor verwenden. Achten Sie bei der Erstellung einer neuen Kategorie darauf, für den Categorieschlüssel (der Wert von `srvprvCategoryKey`) Kleinschreibung zu verwenden. Dies ist erforderlich, um sicherzustellen, dass die Kategorien in der Identity Manager-Benutzeranwendung ordnungsgemäß funktionieren.

Weitere Informationen zum Erstellen von Bereitstellungskategorien finden Sie in [Abschnitt 4.4](#), „Arbeiten mit Listen“, auf Seite 104.

## 22.3 Konfigurieren einer Bereitstellungsanforderungsdefinition

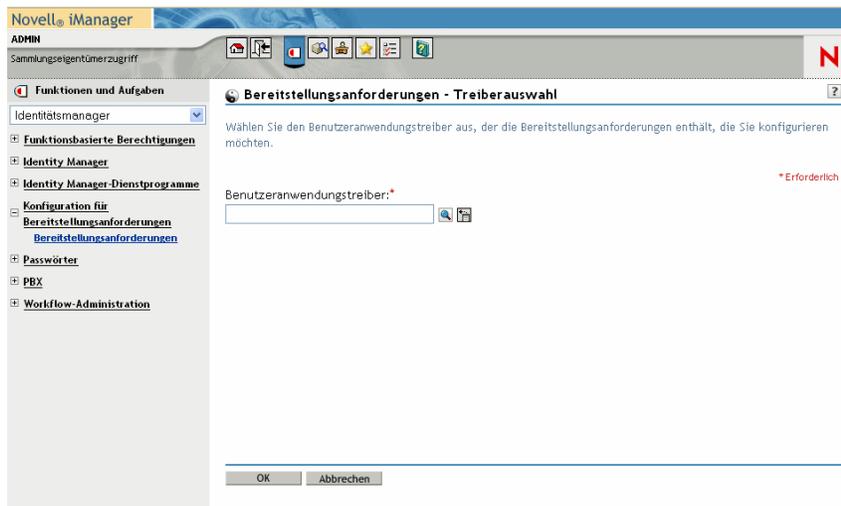
Vor der Konfiguration einer Bereitstellungsanforderungsdefinition müssen Sie den Treiber der Identity Manager-Benutzeranwendung auswählen, der die entsprechende Definition enthält. Nach Auswahl des Treibers können Sie eine neue Bereitstellungsanforderungsdefinition erstellen oder eine vorhandene Definition bearbeiten. Sie können außerdem Bereitstellungsanforderungsdefinitionen löschen, den Status einer Anforderungsdefinition ändern oder Rechte für eine Anforderungsdefinition festlegen.

### 22.3.1 Treiberauswahl

So wählen Sie einen Treiber für die Identity Manager-Benutzeranwendung aus:

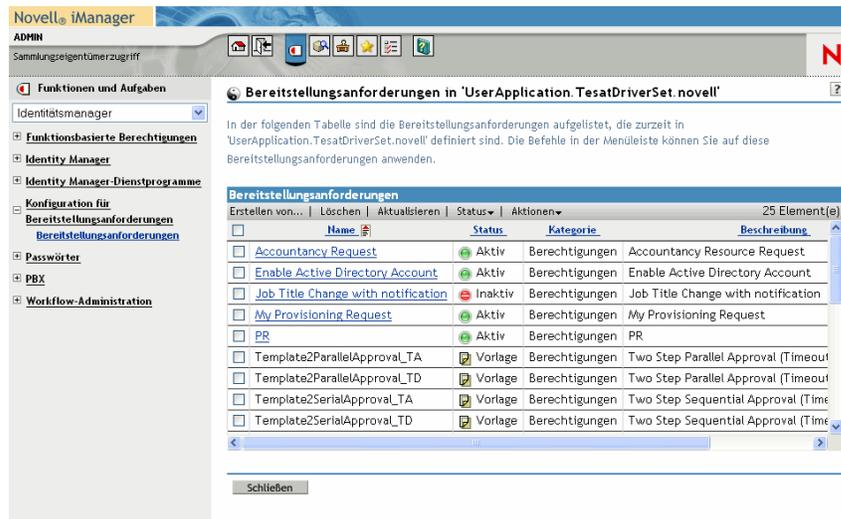
- 1 Wählen Sie in iManager die Kategorie *Identity Manager*.
- 2 Öffnen Sie die Funktion *Konfiguration für Bereitstellungsanforderungen*.
- 3 Klicken Sie auf die Aufgabe *Bereitstellungsanforderungen*.

In iManager wird der Bildschirm „Benutzeranwendungstreiber“ angezeigt.



- 4 Geben Sie im Feld *Benutzeranwendungstreiber* den Treibernamen an und klicken Sie auf *OK*.

In iManager wird das Teilfenster „Konfiguration für Bereitstellungsanforderungen“ angezeigt. Das Teilfenster „Konfiguration für Bereitstellungsanforderungen“ enthält eine Liste der verfügbaren Bereitstellungsanforderungsdefinitionen.



Die installierten Schablonen werden in dunkler Schrift und mit dem Status *Schablone* angezeigt. Anforderungsdefinitionen, die als Schablonen dienen, zeigen keine Links an, da sie schreibgeschützt sind.

**Hinweis:** Wenn in der Konfiguration festgelegt ist, dass die Anforderungsdefinitionen lokalisiert werden sollen, werden die Namen und Beschreibungen dieser Definitionen in der der Ländereinstellung entsprechenden Sprache angezeigt.

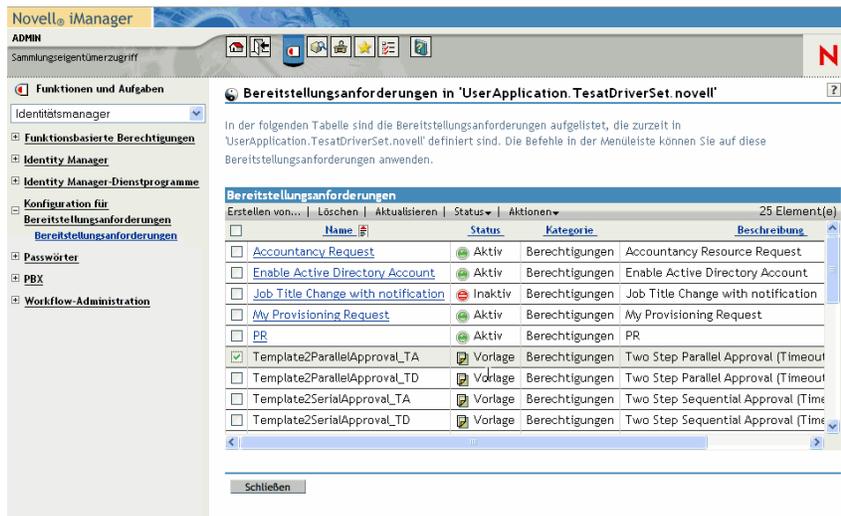
**Wechsel des Treibers** Wenn Sie einen Treiber ausgewählt haben, gilt diese Auswahl für die Dauer Ihrer iManager-Sitzung, es sein denn, Sie wählen einen neuen Treiber. Klicken Sie zum Auswählen eines neuen Treibers auf den Befehl *Aktionen* und wählen Sie im Menü *Aktionen* die Option *Benutzeranwendungstreiber auswählen*.

## 22.3.2 Erstellen oder Bearbeiten einer Bereitstellungsanforderung

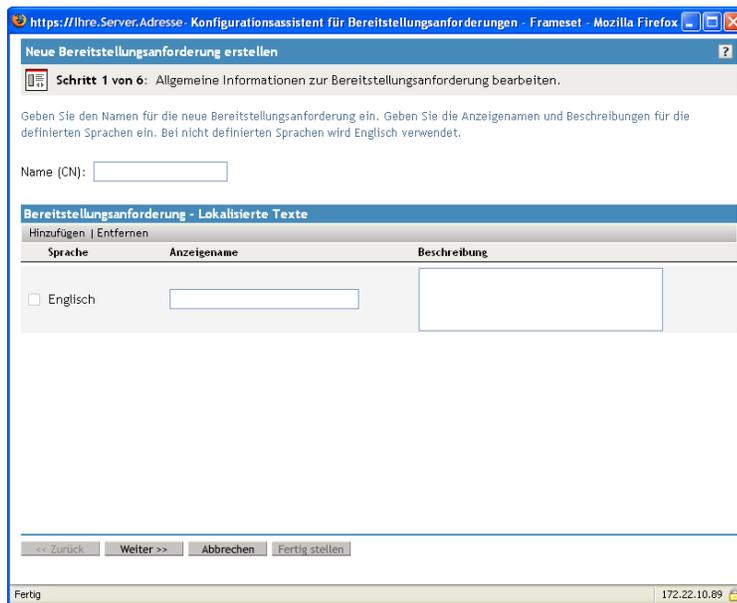
So erstellen Sie eine neue Bereitstellungsanforderung:

- 1 Klicken Sie auf den Namen der Bereitstellungsanforderung, die als Schablone im Teilfenster „Konfiguration für Bereitstellungsanforderungen“ verwendet werden soll.

- 2 Klicken Sie im Teilfenster „Konfiguration für Bereitstellungsanforderungen“ auf den Befehl *Erstellen von*.



Die erste Seite des Assistenten für die Erstellung einer neuen Bereitstellungsanforderung wird angezeigt.



- 3 Geben Sie im Feld *Name* einen Namen für das neue Objekt ein.
- 4 Geben Sie für jede Sprache, die von der Anwendung unterstützt werden soll, in die Felder *Anzeigename* und *Beschreibung* unter *Bereitstellungsanforderung - Lokalisierte Texte* den lokalisierten Text ein. Dieser Text wird verwendet, um die Bereitstellungsanforderung innerhalb der Benutzeranwendung zu identifizieren.
- 5 Wenn Sie der Liste eine neue Sprache hinzufügen möchten, klicken Sie auf *Hinzufügen* und wählen Sie die gewünschte Sprache aus.

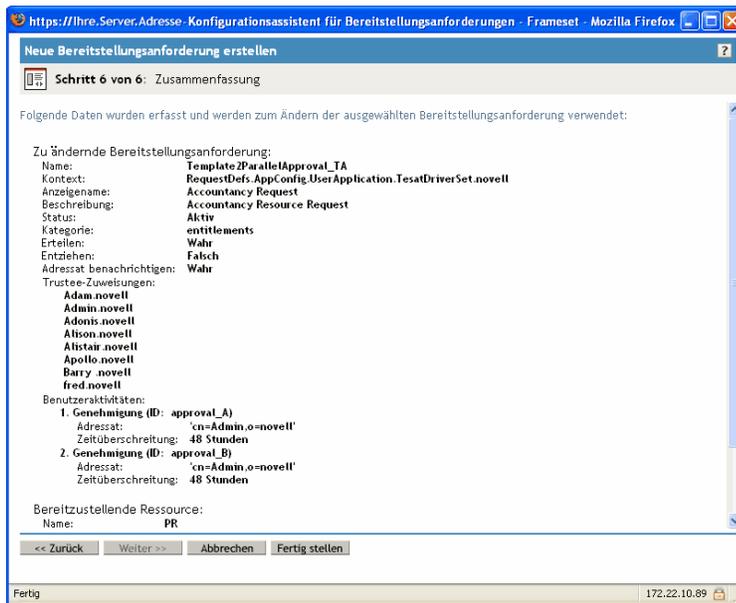
---

**Hinweis:** Standardmäßig unterstützt eine neu erstellte Bereitstellungsanforderung nur Englisch.

---

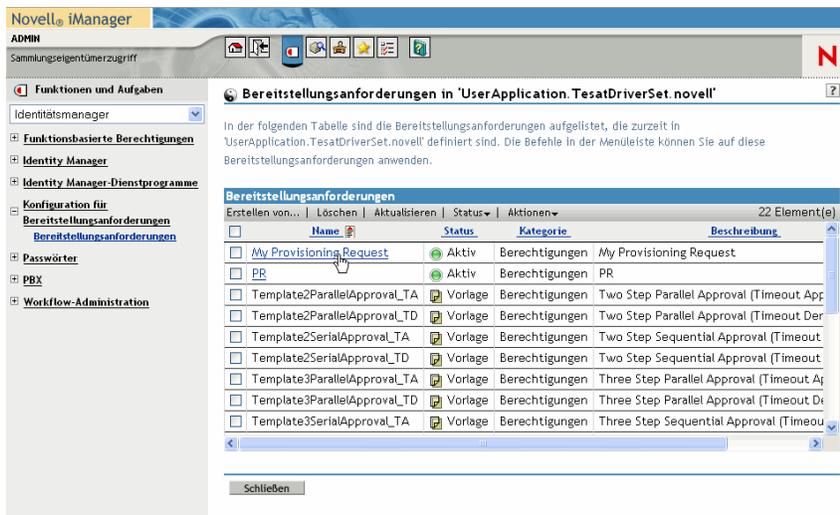
- 6 Klicken Sie auf *Weiter*.
- 7 Legen Sie die bereitstellbare Ressource für die Anforderungsdefinition fest (wie in „**Festlegung der bereitstellbaren Ressource**“ auf Seite 333 beschrieben).
- 8 Konfigurieren Sie die Aktivitäten für den der Anforderungsdefinition zugeordneten Workflow (wie in „**Konfigurieren der Workflow-Aktivitäten**“ auf Seite 337 beschrieben).
- 9 Legen Sie die Zugriffsrechte für die Anforderungsdefinition fest (wie in „**Festlegen der Zugriffsrechte für die Bereitstellungsanforderung**“ auf Seite 342 beschrieben).
- 10 Legen Sie den Anfangsstatus für die Anforderungsdefinition fest (wie in „**Festlegen des Anfangsstatus einer Bereitstellungsanforderung**“ auf Seite 342 beschrieben).

## 11 Überprüfen Sie Ihre Einstellungen und klicken Sie auf *Fertig stellen*.



So bearbeiten Sie eine vorhandene Bereitstellungsanforderung:

- 1 Klicken Sie im Teilfenster „Konfiguration für Bereitstellungsanforderungen“ auf den Namen der Bereitstellungsanforderung.



Die Bearbeitung einer Bereitstellungsanforderung, die als Schablone dient, ist nicht möglich. Anforderungsdefinitionen mit dem Status „Schablone“ zeigen keine Links an, da sie schreibgeschützt sind.

**Hinweis:** Wenn eine große Anzahl an Anforderungsdefinitionen vorhanden ist, ist es hilfreich, die Liste nach einer bestimmten Spalte zu sortieren, z. B. nach Name oder Beschreibung.

Klicken Sie einfach auf den Spaltennamen, um die Liste nach einer bestimmten Spalte zu sortieren.

---

- 2 Klicken Sie für jede Sprache, die von der Anwendung unterstützt werden soll, auf das entsprechende Kontrollkästchen neben der Sprache in der Liste unter *Bereitstellungsanforderung - Lokalisierte Texte* und geben Sie in die Felder *Anzeigename* und *Beschreibung* den lokalisierten Text ein. Dieser Text wird verwendet, um die Bereitstellungsanforderung innerhalb der Benutzeranwendung zu identifizieren.
  - 3 Wenn Sie der Liste eine neue Sprache hinzufügen möchten, klicken Sie auf *Hinzufügen* und wählen Sie die gewünschte Sprache aus.
- 

**Hinweis:** Standardmäßig unterstützt eine neu erstellte Bereitstellungsanforderung nur Englisch.

---

- 4 Klicken Sie auf *Weiter*.
- 5 Legen Sie die bereitstellbare Ressource für die Anforderungsdefinition fest (wie in „**Festlegung der bereitstellbaren Ressource**“ auf Seite 333 beschrieben).
- 6 Konfigurieren Sie die Aktivitäten für den der Anforderungsdefinition zugeordneten Workflow (wie in „**Konfigurieren der Workflow-Aktivitäten**“ auf Seite 337 beschrieben).
- 7 Legen Sie die Zugriffsrechte für die Anforderungsdefinition fest (wie in „**Festlegen der Zugriffsrechte für die Bereitstellungsanforderung**“ auf Seite 342 beschrieben).
- 8 Legen Sie den Anfangsstatus für die Anforderungsdefinition fest (wie in „**Festlegen des Anfangsstatus einer Bereitstellungsanforderung**“ auf Seite 342 beschrieben).
- 9 Überprüfen Sie Ihre Einstellungen und klicken Sie auf *Fertig stellen*.

## **Festlegung der bereitstellbaren Ressource**

Dieser Abschnitt enthält Anweisungen für die Festlegung einer bereitstellbaren Ressource basierend auf einer Berechtigung. Dieses Kapitel enthält keine konzeptionellen Informationen zu Berechtigungen oder Anweisungen für die Erstellung und Verwendung von Berechtigungen.

Ausführliche Informationen zu Berechtigungen finden Sie im *<z-DocTitleInVariable>Novell Identity Manager: Administrationshandbuch*.

So legen Sie die bereitstellbare Ressource fest:

- 1 Wenn Sie das aktuell der Anforderungsdefinition zugeordnete Ziel verwenden möchten, wählen Sie das Optionsfeld *Bereitstellbare Ressource*.

Das Optionsfeld „Bereitstellbare Ressource“ wird standardmäßig ausgewählt, wenn Sie eine Anforderungsdefinition bearbeiten, die auf eine gültige Ressource verweist. Bei der Definition einer neuen Bereitstellungsanforderung ist dieses Optionsfeld nicht ausgewählt.

- 2 Wenn Sie die Anforderungsdefinition an eine andere Ressource binden möchten, die zuvor innerhalb des aktuell ausgewählten Treibers definiert war, aktivieren Sie das Optionsfeld *Verfügbare bereitstellbare Ressourcen* aus und wählen Sie ein Ziel in der Dropdown-Liste aus.

---

**Hinweis:** Wenn die Anforderungsdefinition an eine Ressource gebunden war, die keine Berechtigung ist, ist eine Änderung der Ressource nicht möglich.

---

- 3 Wählen Sie in der Dropdown-Liste *Kategorie* eine Kategorie für die Definition der bereitstellbaren Ressource aus.

Die Kategorie wechselt standardmäßig zur Kategorie der aktuell ausgewählten bereitstellbaren Ressource. Wenn Sie die bereitstellbare Ressource ändern, wird stets auch die Kategorie für die Anforderungsdefinition geändert und an die Kategorie der Ressource angepasst. Wenn Sie der Anforderungsdefinition eine andere Kategorie zuweisen möchten, wählen Sie die entsprechende Kategorie in der Dropdown-Liste „Kategorie“ aus.

- 4 Wenn Sie basierend auf einer Identity Manager-Berechtigung eine neue Ressource erstellen möchten, klicken Sie auf die Schaltfläche +.



Klicken Sie zum Bearbeiten einer vorhandenen Ressource auf das Stift-Symbol.



Führen Sie folgende Schritte aus, um die Charakteristika der Ressource zu definieren:

- 4a Legen Sie im Feld *Name (CN)* den Namen für die Ressource fest.
- 4b Wählen Sie in der Dropdown-Liste *Kategorie* eine Kategorie für die Ressource aus.
- 4c Legen Sie im Feld *Berechtigung* die Berechtigung fest.

- 4d** Klicken Sie für jede Sprache, die von der Anwendung unterstützt werden soll, auf das entsprechende Kontrollkästchen neben der Sprache in der Liste unter *Bereitstellbare Ressource - Lokalisierte Texte* und geben Sie in die Felder *Anzeigename* und *Beschreibung* den lokalisierten Text ein. Dieser Text wird verwendet, um die Bereitstellungsressource innerhalb der Benutzeranwendung zu identifizieren.
- 4e** Wenn Sie der Liste eine neue Sprache hinzufügen möchten, klicken Sie auf *Hinzufügen* und wählen Sie die gewünschte Sprache aus.

---

**Hinweis:** Standardmäßig unterstützt eine neu erstellte Bereitstellungsressource nur Englisch.

---

https://Ihre.Server.Adresse - Assistent für bereitstellbare Ressourcen - Frameset - Mozilla Firefox

**Neue bereitstellbare Ressource erstellen**

**Schritt 1 von 6:** Allgemeine Informationen zur bereitstellbaren Ressource bearbeiten.

Geben Sie den Namen für die neue bereitstellbare Ressource ein und wählen Sie die dazugehörige Kategorie und zuzuordnende Identity Manager-Berechtigung aus. Geben Sie die Anzeigenamen und Beschreibungen für die definierten Sprachen ein. Bei nicht definierten Sprachen wird Englisch verwendet.

Name (CN):

Kategorie:

Berechtigung:

**Bereitstellbare Ressource - Lokalisierte Texte**

Hinzufügen | Entfernen

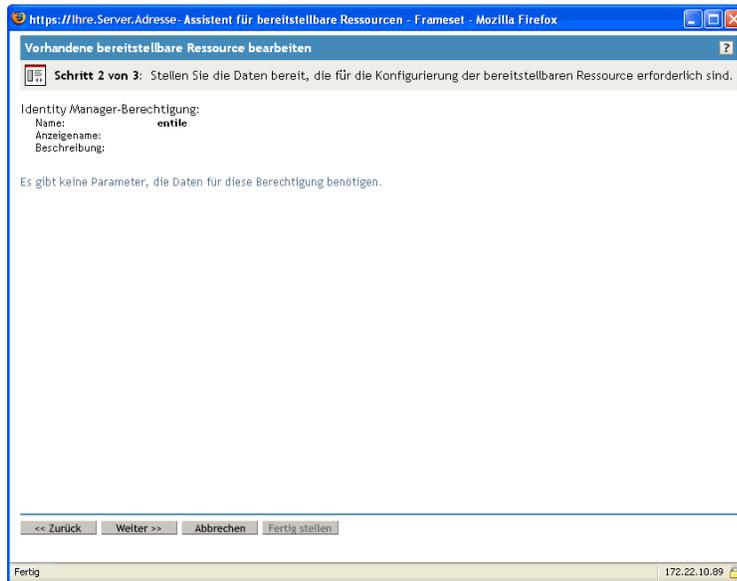
Sprache	Anzeigename	Beschreibung
<input type="checkbox"/> Englisch	<input type="text" value="Resource"/>	<input type="text"/>

<< Zurück   Weiter >>   Abbrechen   Fertig stellen

https://172.22.10.89/nps/servlet/frameservice?Autoparse=true&taskId=ApprovalFlow.AFTarget~26&error=dev.genErr&merge=Approval... 172.22.10.89

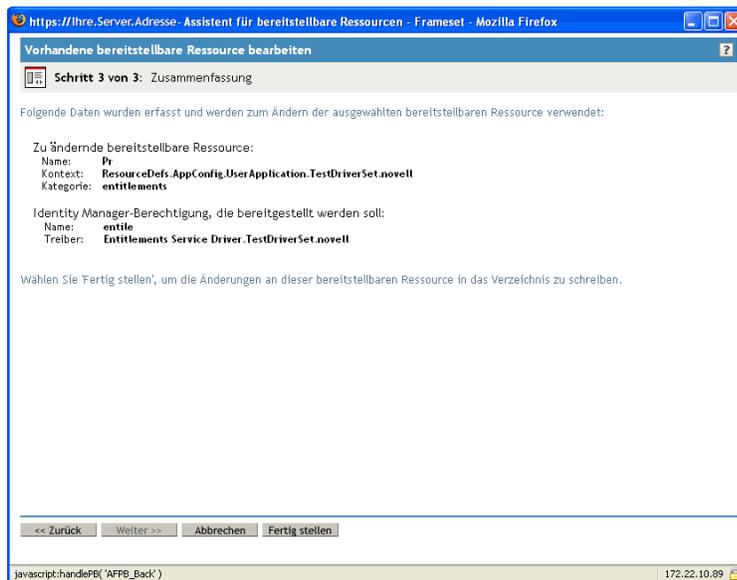
- 5** Klicken Sie auf *Weiter*.

Der Assistent für bereitstellbare Ressourcen zeigt einen Bildschirm an, in dem Sie Parameterdaten angeben können, die für die Berechtigung erforderlich sind.



- 6 Wenn für die Berechtigung keine Berechtigungsparameter erforderlich sind, klicken Sie auf *Weiter*.

Der Assistent für die Erstellung neuer bereitstellbarer Ressourcen zeigt eine Seite mit einer Zusammenfassung an, in der Informationen zu der von Ihnen definierten Ressource angezeigt werden.



- 7 Klicken Sie auf *Fertig stellen*.

## Konfigurieren der Workflow-Aktivitäten

So konfigurieren Sie die Aktivitäten für den zugeordneten Workflow:

- 1 Geben Sie an, ob der Adressat einer Aktivität per E-Mail benachrichtigt werden soll, indem Sie das Kontrollkästchen *Teilnehmer per Email benachrichtigen* aktivieren oder deaktivieren.

https://Ihre.Server.Adresse - Konfigurationsassistent für Bereitstellungsanforderungen - Frameset - Mozilla Firefox

### Neue Bereitstellungsanforderung erstellen

Schritt 3 von 6: Geben Sie die Daten an, die für die Konfigurierung der Bereitstellungsanforderung erforderlich sind.

Email-Benachrichtigungen aktivieren bzw. deaktivieren und Adressaten, Zeitlimit und Wiederholintervall für jede Aktivität der Bereitstellungsanforderung definieren. Zeitlimit ist der Zeitraum, der dem Adressat für die Durchführung der Aktivität zur Verfügung steht.

Teilnehmer per Email benachrichtigen

#### 1. Genehmigung

Adressat:

Ausdruck: Empfänger Manager

DN: (z. B.: CN=Admin,O=Novell)

Zeitüberschreitung: 48 Stunden (Kein Wert: Systemvorgaben verwenden)

Wiederholen:

Versuche: 3 (Kein Wert: keine Wiederholungsversuche)

Adressat:

Ausdruck: Adressat von '1. Genehmigung' Manager

DN: (z. B.: CN=Admin,O=Novell)

<< Zurück Weiter >> Abbrechen Fertig stellen

Übertrage Daten von 172.22.10.89... 172.22.10.89

---

**Hinweis:** Wenn Sie das Kontrollkästchen *Teilnehmer per Email benachrichtigen* auswählen und der Adressat eine Vertretung bestimmt hat, erhält seine Vertretung die Email-Benachrichtigung. Delegierte erhalten keine E-Mail-Benachrichtigungen.

---

- 2 Für jede Workflow-Aktivität besteht die Möglichkeit, die Anzeigebezeichnung zu ändern, indem Sie auf das Symbol neben dem Namen der Aktivität (in diesem Fall „1. Genehmigung“) klicken.

The screenshot shows a web browser window titled "https://Ihre.Server.Adresse - Konfigurationsassistent für Bereitstellungsanforderungen - Frameset - Mozilla Firefox". The page content is titled "Neue Bereitstellungsanforderung erstellen" and indicates "Schritt 3 von 6".

Text: "Email-Benachrichtigungen aktivieren bzw. deaktivieren und Adressaten, Zeitlimit und Wiederholintervall für jede Aktivität der Bereitstellungsanforderung definieren. Zeitlimit ist der Zeitraum, der dem Adressat für die Durchführung der Aktivität zur Verfügung steht."

Teilnehmer per Email benachrichtigen

**1. Genehmigung**  Lokalisierte Anzeigebezeichnungen dieser Aktivität bearbeiten...

Adressat:

Ausdruck: Initiator <Kein Attribut>

DN: cn=Admin,o=novell (z. B.: CN=Admin,O=Novell)

Zeitüberschreitung: 48 Stunden (Kein Wert: Systemvorgaben verwenden)

Wiederholen:

Versuche: 3 (Kein Wert: keine Wiederholungsversuche)

Adressat:

Ausdruck: Initiator <Kein Attribut>

DN: cn=Admin,o=novell (z. B.: CN=Admin,O=Novell)

Navigation: << Zurück, Weiter >>, Abbrechen, Fertig stellen

Footer: javascript:editDisplayLabels('0');

Geben Sie die Anzeigebezeichnung in das Feld *Anzeigebezeichnung* ein und klicken Sie auf *OK*.

https://Ihre.Server.Adresse - Editor für Anzeigebezeichnungen der Bereitstellungsanforderungen - Frameset

**Benutzeraktivität - Editor für Anzeigebezeichnungen**

Geben Sie die Anzeigebezeichnungen der Benutzeraktivität für die definierten Sprachen ein. Bei nicht definierten Sprachen wird Englisch verwendet.

**Benutzeraktivität - Lokalisierte Anzeigebezeichnungen**

Hinzufügen | Entfernen

Sprache	Anzeigebezeichnung
<input type="checkbox"/> Englisch	First approval
<input type="checkbox"/> Deutsch	1. Genehmigung
<input type="checkbox"/> Französisch	Première approbation

OK Abbrechen

Fertig 172.22.10.89

---

**Hinweis:** Bei den standardmäßigen Anzeigebezeichnungen („1. Genehmigung“, „2. Genehmigung“ usw.) wird davon ausgegangen, dass Bestätigungen sequenziell verarbeitet werden. Für parallele Abläufe empfiehlt es sich, Bezeichnungen anzugeben, die keine sequenzielle Verarbeitung implizieren. Sie könnten z. B. Bezeichnungen zuweisen wie „Eine von drei parallelen Genehmigungen“, „Zwei von drei parallelen Genehmigungen“ usw.

---

- 3 Geben Sie für jede Workflow-Aktivität auch die folgenden Informationen an:

Feld	Beschreibung
Adressat > Ausdruck	<p>Legt einen dynamischen Ausdruck fest, der den Adressaten der Aktivität identifiziert. Der Adressat wird zur Laufzeit basierend auf der Auswertung des Ausdrucks ermittelt.</p> <p>Der <b>erste Begriff</b> eines Adressaten-Ausdrucks kann einer der folgenden Werte sein:</p> <ul style="list-style-type: none"> <li>• Initiator</li> <li>• Empfänger</li> <li>• Adressat von <i>Aktivitätsname</i></li> </ul> <p>Ein separater Begriff für Adressat von <i>Aktivitätsname</i> ist in der Dropdown-Liste „Ausdruck“ für jede Aktivität im Workflow aufgelistet (mit Ausnahme der Aktivität, die Sie gerade konfigurieren). Der <i>Aktivitätsname</i> ist entweder die von Ihnen für die Aktivität festgelegte Anzeigebezeichnung oder der Standardname, wenn Sie keine Anzeigebezeichnung angegeben haben.</p> <p>Der <b>zweite Begriff</b> eines Adressaten-Ausdrucks kann einer der folgenden beiden Werte sein:</p> <ul style="list-style-type: none"> <li>• Manager</li> <li>• &lt;Kein Attribut&gt;</li> </ul> <hr/> <p><b>Hinweis:</b> Das Attribut <code>Manager</code> ist automatisch verfügbar, weil es zuvor bei der Benutzerentität in der Abstraktionsschicht definiert wurde. Möglicherweise stehen neben „Manager“ auch andere Attribute zur Auswahl, sofern sie folgende Bedingungen erfüllen:</p> <hr/> <ul style="list-style-type: none"> <li>• Sie müssen bei der Benutzerentität in der Abstraktionsschicht definiert sein.</li> <li>• Sie müssen einwertig sein.</li> <li>• Sie müssen über einen DN-Datentyp verfügen.</li> </ul>
Adressat > DN	<p>Legt den eindeutigen Namen eines Benutzers, einer Gruppe oder einer Aufgabengruppe fest.</p> <hr/> <p><b>Hinweis:</b> Wenn Sie Aufgabengruppenmanagern ermöglichen möchten, Aufgaben nach Aufgabengruppen zu suchen (über die Aktion „Teamaufgaben des Benutzers“ in der Benutzeranwendung), müssen Sie die Aufgabengruppe als Adressaten festlegen.</p>
Zeitüberschreitung	<p>Legt den Zeitraum fest, der dem Adressaten für die Erledigung der Aufgabe zur Verfügung steht. Das Zeitüberschreitungsintervall wird jedes Mal angewendet, wenn die entsprechende Aktivität vom Adressaten ausgeführt wird.</p> <p>Geben Sie einen Wert in Sekunden, Minuten, Stunden oder Tagen an.</p>

Feld	Beschreibung
Wiederholversuche	<p>Legt für den Fall einer Zeitüberschreitung die Anzahl der Wiederholversuche für die Aktivität fest.</p> <p>Wenn es bei einer Aktivität zu einer Zeitüberschreitung kommt, versucht der Workflow-Prozess möglicherweise in Abhängigkeit von den für die Aktivität festgelegten Wiederholversuchen erneut, die Aktivität zu erledigen. Bei jedem erneuten Versuch eskaliert der Workflow-Prozess die Aktivität möglicherweise an einen anderen Benutzer. In diesem Fall wird die Aktivität einem anderen Adressaten zugewiesen (z. B. dem Manager des Benutzers), damit dieser die Möglichkeit hat, die Arbeit der Aktivität zu erledigen. Falls beim letzten Wiederholversuch eine Zeitüberschreitung auftritt, wird die Aktivität entsprechend der Konfiguration des Workflows als genehmigt oder abgelehnt markiert.</p>
Wiederholen > Adressat > Ausdruck	<p>Legt einen dynamischen Ausdruck fest, anhand dessen der Benutzer identifiziert wird, an den die Aufgabe weitergeleitet wird, wenn die maximale Anzahl der Wiederholversuche erreicht wurde.</p> <p>Der Adressat für die erneute Sendung wird während der Laufzeit basierend auf der Auswertung des Ausdrucks ermittelt.</p> <p>Der <b>erste Begriff</b> eines Adressaten-Ausdrucks kann einer der folgenden Werte sein:</p> <ul style="list-style-type: none"> <li>• <code>approval.getAddressee()</code></li> <li>• <code>Initiator</code></li> <li>• <code>Empfänger</code></li> <li>• <code>Adressat von <i>Aktivitätsname</i></code></li> </ul> <p>Anhand der Option <code>approval.getAddressee()</code> wird der aktuelle Adressat ausgewählt.</p> <p>Ein separater Begriff für <code>Adressat von <i>Aktivitätsname</i></code> ist in der Dropdown-Liste „Ausdruck“ für jede Aktivität im Workflow aufgelistet (einschließlich der Aktivität, die Sie gerade konfigurieren). Der <i>Aktivitätsname</i> ist entweder die von Ihnen für die Aktivität festgelegte Anzeigebezeichnung oder der Standardname, wenn Sie keine Anzeigebezeichnung angegeben haben.</p> <p>Der <b>zweite Begriff</b> eines Adressaten-Ausdrucks kann einer der folgenden beiden Werte sein:</p> <ul style="list-style-type: none"> <li>• <code>Manager</code></li> <li>• <code>&lt;Kein Attribut&gt;</code></li> </ul> <p>Wenn Sie die Option <code>approval.getAddressee()</code> und anschließend <code>Manager</code> auswählen, wird jeder erneute Versuch an einen anderen Manager auf einer höheren Ebene innerhalb der Organisation eskaliert. Daher müssen Sie sicherstellen, dass die Anzahl der Wiederholversuche auf einen Wert gesetzt wird, der für Ihre Organisation geeignet ist. Die Anzahl der Wiederholversuche darf die Anzahl der Management-Ebenen nicht übersteigen, die oberhalb des aktuellen Adressaten vorhanden sind.</p>
Wiederholen > Adressat > DN	<p>Legt den eindeutigen Namen eines Benutzers oder einer Gruppe fest, an den bzw. die die Aufgabe weitergeleitet wird, wenn die maximale Anzahl der Wiederholversuche erreicht wurde.</p>

- 4 Wenn Sie die Konfiguration einer Aktivität beenden, müssen Sie möglicherweise nach unten blättern, um die anderen Aktivitäten des Ablaufs einzusehen.
- 5 Klicken Sie auf *Weiter*.

---

**Hinweis:** Die mögliche Anzahl der Aktivitäten, die Sie konfigurieren können, hängt davon ab, welche Workflow-Schablone an die Anforderungsdefinition gebunden wurde. Die Anzahl und der Typ der Berechtigungsparameter sind unterschiedlich und hängen von der bereitstellbaren Ressource ab, die der Anforderung zugeordnet ist.

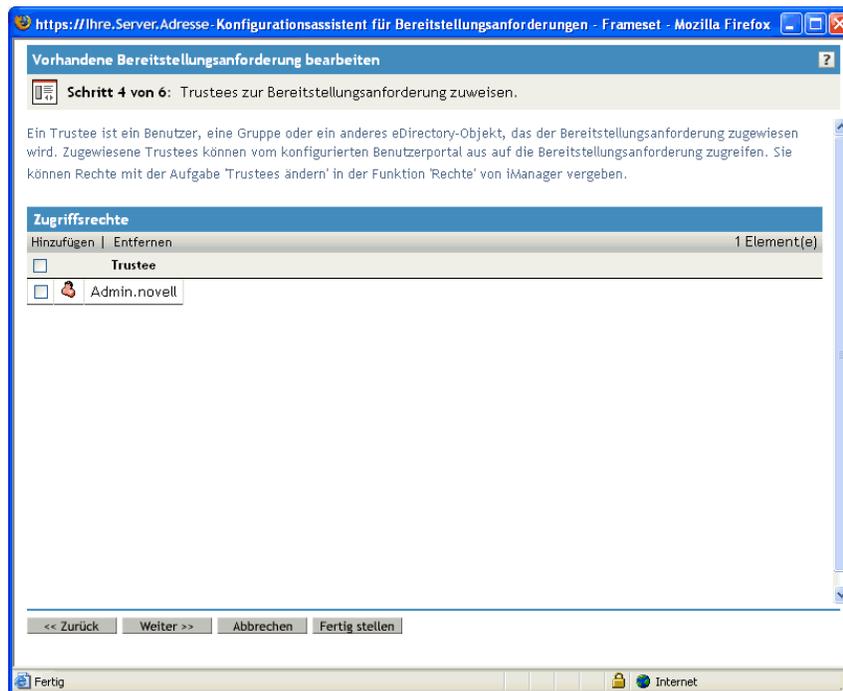
---

## Festlegen der Zugriffsrechte für die Bereitstellungsanforderung

So legen Sie die Zugriffsrechte für eine Bereitstellungsanforderung fest:

- 1 Klicken Sie zum Hinzufügen eines Benutzers, einer Gruppe oder eines anderen eDirectory-Objekts zur Liste der Trustees für die Anforderungsdefinition auf *Hinzufügen* und wählen Sie das entsprechende Objekt aus.

Sobald Sie ein Objekt hinzugefügt haben, wird es in der Liste der Trustees aufgeführt.



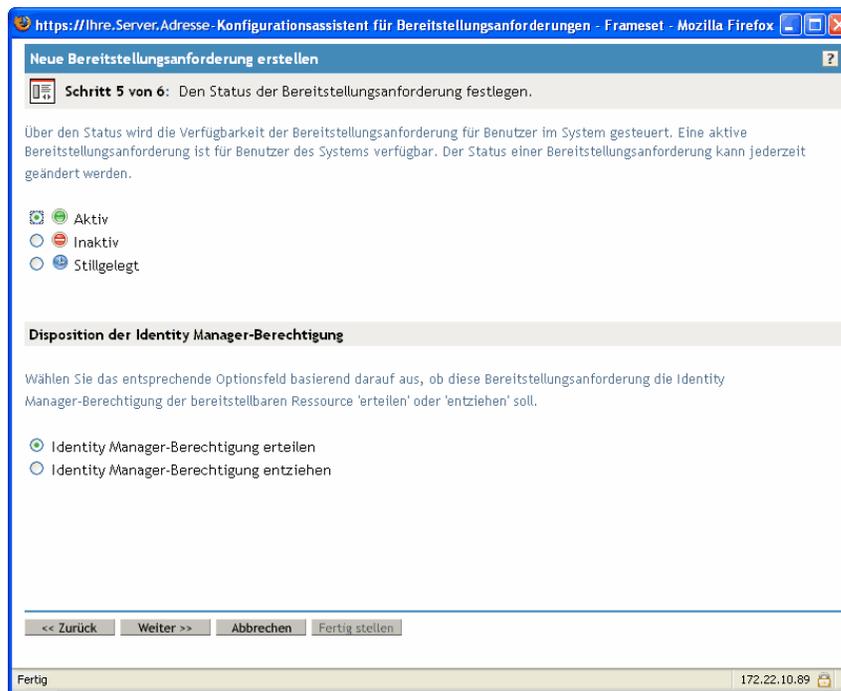
- 2 Wählen Sie zum Entfernen eines Benutzers, einer Gruppe oder eines anderen Objekts einen Eintrag in der Liste *Trustee* aus und klicken Sie anschließend auf *Entfernen*.
- 3 Klicken Sie auf *Weiter*.

## Festlegen des Anfangsstatus einer Bereitstellungsanforderung

So legen Sie den Anfangsstatus einer Bereitstellungsanforderung fest:

- 1 Klicken Sie auf das Optionsfeld des gewünschten Status:

Status	Beschreibung
Aktiv	Kann verwendet werden.
Inaktiv	Kann vorübergehend nicht verwendet werden. Dies ist die Standardeinstellung.
Stillgelegt	Dauerhaft deaktiviert.



- 2 Klicken Sie auf das Optionsfeld neben der gewünschten Aktion („Erteilen“ oder „Entziehen“).
- 3 Klicken Sie auf *Weiter*.

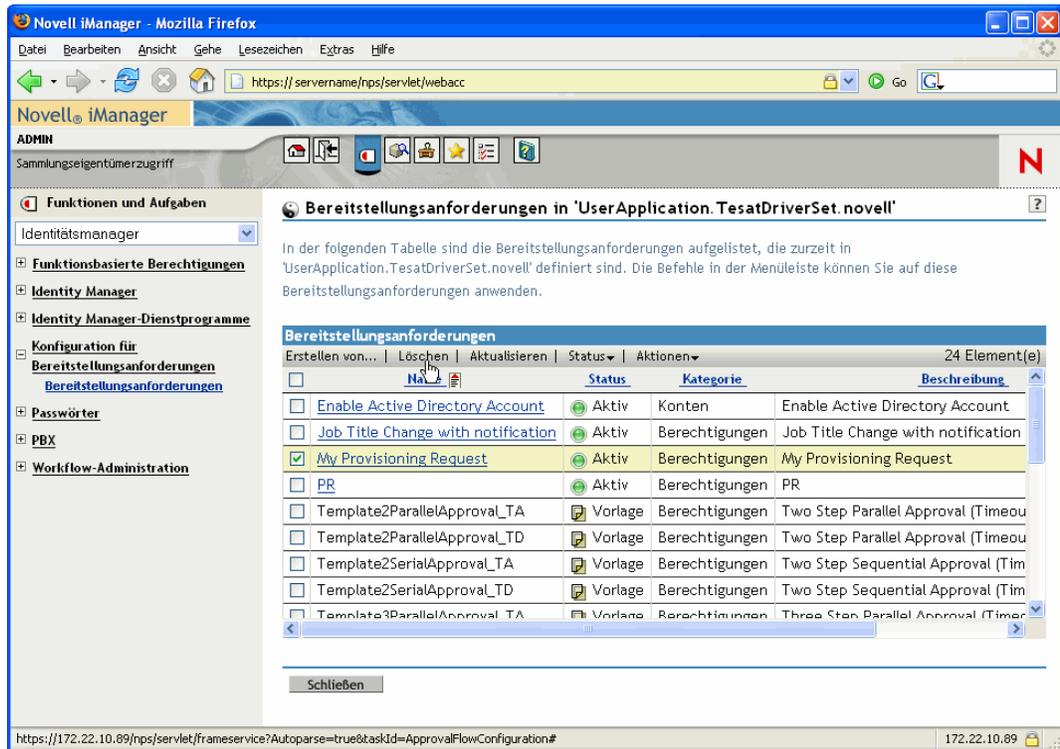
### 22.3.3 Löschen einer Bereitstellungsanforderung

So löschen Sie eine Bereitstellungsanforderung:

- 1 Wählen Sie die zu löschende Bereitstellungsanforderung aus, indem Sie auf das Kontrollkästchen neben dem Namen klicken.

Sie dürfen eine Bereitstellungsanforderung nicht löschen, die als Schablone dient.

- 2 Klicken Sie im Teilfenster „Konfiguration für Bereitstellungsanforderungen“ auf den Befehl *Löschen*.

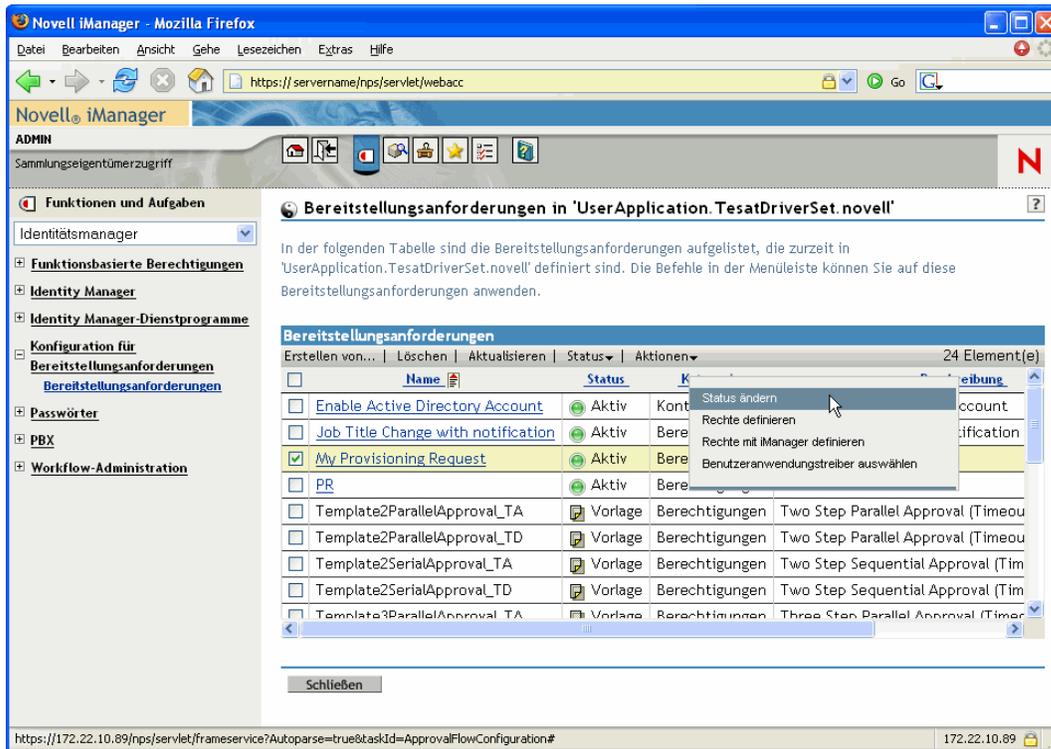


### 22.3.4 Änderung des Status einer vorhandenen Bereitstellungsanforderung

So ändern Sie den Status einer vorhandenen Bereitstellungsanforderung:

- 1 Wählen Sie die Bereitstellungsanforderung aus, deren Status Sie ändern möchten, indem Sie auf das Kontrollkästchen neben dem Namen klicken.

- 2 Klicken Sie im Teilfenster „Konfiguration für Bereitstellungsanforderungen“ auf den Befehl *Status ändern*.



- 3 Klicken Sie im Menü „Status“ auf die gewünschte Option:

Status	Beschreibung
Aktiv	Kann verwendet werden.
Inaktiv	Kann vorübergehend nicht verwendet werden.
Stillgelegt	Dauerhaft deaktiviert.

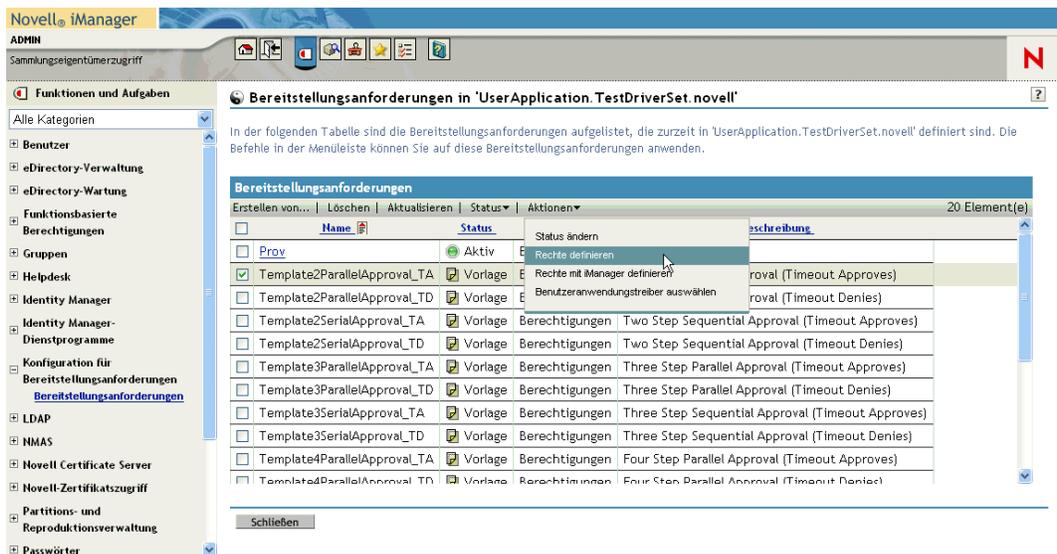
- 4 Klicken Sie auf das Optionsfeld neben der gewünschten Aktion („Erteilen“ oder „Entziehen“).
- 5 Klicken Sie auf *Fertig stellen*.

### 22.3.5 Definieren von Rechten für eine vorhandene Bereitstellungsanforderung

So definieren Sie Rechte für eine vorhandene Bereitstellungsanforderung:

- 1 Wählen Sie die Bereitstellungsanforderung aus, deren Rechte Sie definieren möchten, indem Sie auf das Kontrollkästchen neben dem Namen klicken.
- 2 Klicken Sie im Teilfenster „Konfiguration für Bereitstellungsanforderungen“ auf den Befehl *Aktionen*.

**3** Klicken Sie im Menü „Aktionen“ auf den Befehl *Rechte definieren*.



**4** Befolgen Sie die Anweisungen unter „Festlegen der Zugriffsrechte für die Bereitstellungsanforderung“ auf Seite 342.

So definieren Sie mit iManager Rechte für eine Bereitstellungsanforderung:

- 1 Wählen Sie die Bereitstellungsanforderung aus, deren Rechte Sie definieren möchten, indem Sie auf das Kontrollkästchen neben dem Namen klicken.
- 2 Klicken Sie im Teilfenster „Konfiguration für Bereitstellungsanforderungen“ auf den Befehl *Aktionen*.
- 3 Klicken Sie im Menü „Aktionen“ auf den Befehl *Rechte mit iManager definieren*.

# Verwalten von Bereitstellungs-Workflows

# 23

Dieses Kapitel enthält Anweisungen für die Verwaltung von Bereitstellungs-Workflows während der Laufzeit. Zudem erfahren Sie, wie Email-Benachrichtigungen für Bereitstellungs-Workflows konfiguriert werden.

Es werden folgende Themen erläutert:

- [Abschnitt 23.1, „Allgemeines zum Plugin für die Workflow-Administration“, auf Seite 347](#)
- [Abschnitt 23.2, „Verwalten von Workflows“, auf Seite 348](#)
- [Abschnitt 23.3, „Konfigurieren des Email-Servers“, auf Seite 356](#)
- [Abschnitt 23.4, „Arbeiten mit den installierten Email-Schablonen“, auf Seite 357](#)

## 23.1 Allgemeines zum Plugin für die Workflow-Administration

Das iManager-Plugin für die Workflow-Administration bietet eine browserbasierte Benutzerschnittstelle, mit der Sie den Status von Workflow-Prozessen anzeigen, Aktivitäten eines Workflows neu zuweisen oder einen Workflow beenden können.

Das Plugin für die Workflow-Administration befindet sich in der Kategorie *Identity Manager* in iManager. Es enthält die Aufgabe *Workflows*, die Teil der Funktion *Workflow-Administration* ist.

Zudem umfasst die Funktion „Workflow-Administration“ die Aufgaben *Email-Schablonen* und *Email-Serveroptionen*. Diese Aufgaben sind Verknüpfungen zu anderen Aufgaben, die unter der Funktion *Passwörter* aufgeführt sind.

**Allgemeines zur Aufgabe „Workflows“** Die Aufgabe „Workflows“ besteht aus den folgenden Teilfenstern:

Teilfenster	Beschreibung
Workflows	<p>Dies ist die primäre Benutzerschnittstelle für die Administration von Bereitstellungs-Workflows. In dieser Schnittstelle werden die aktuell verarbeiteten Workflows aufgelistet, für die Sie unterschiedliche Aktionen ausführen können.</p> <p>Wenn Sie die Aufgabe „Workflows“ des erste Mal starten, müssen Sie einen Identity Manager-Benutzeranwendungstreiber auswählen. Der Treiber verweist auf einen Workflow-Server. Sie müssen einen Treiber auswählen, bevor Sie sich beim Server anmelden und mit der Workflow-Administration beginnen können.</p> <p>Nachdem Sie einen Treiber ausgewählt haben, können Sie Suchkriterien für die Auswahl der zu verwaltenden Workflows angeben.</p>
Workflow-Details	<p>Dies ist eine schreibgeschützte Benutzerschnittstelle zum Anzeigen von Details zu einem bestimmten Workflow.</p>

## 23.2 Verwalten von Workflows

In diesem Abschnitt wird beschrieben, wie Sie Bereitstellungs-Workflows mithilfe des Plugins für die Workflow-Administration verwalten können.

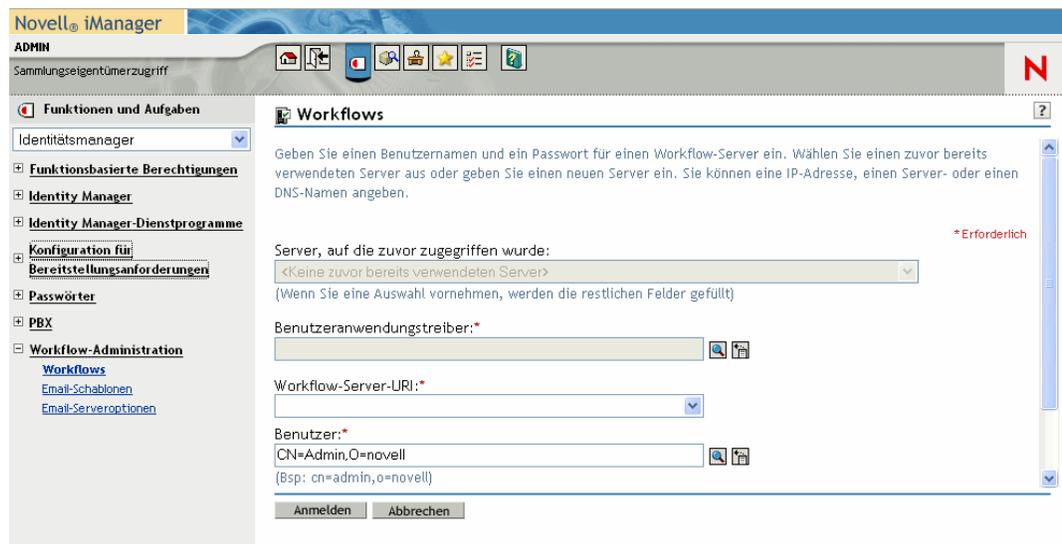
### 23.2.1 Verbindungsaufbau mit einem Workflow-Server

Bevor Sie mit der Workflow-Administration beginnen können, müssen Sie mit einem Workflow-Server verbunden sein. Wenn der Benutzeranwendungstreiber einem einzelnen Workflow-Server zugeordnet ist, genügt es, den Namen des Treibers anzugeben. Wenn der Treiber mehreren Workflow-Servern zugeordnet ist, müssen Sie den Ziel-Workflow-Server auswählen.

So stellen Sie eine Verbindung mit dem Workflow-Server her:

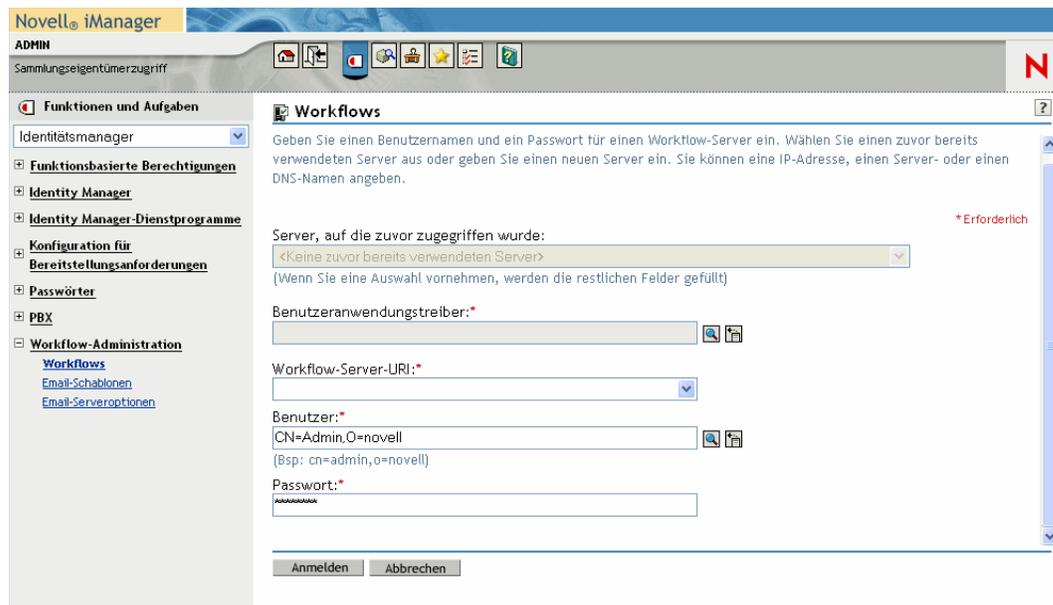
- 1 Wählen Sie in iManager die Kategorie „Identity Manager“.
- 2 Öffnen Sie die Funktion *Workflow-Administration*.
- 3 Klicken Sie auf die Aufgabe *Workflows*.

Der Bildschirm „Workflows“ wird angezeigt.



- 4 Wenn Sie zuvor auf den Ziel-Workflow-Server zugegriffen haben, können Sie ihn in der Dropdown-Liste *Server, auf die zuvor zugegriffen wurde* auswählen.  
Die anderen Felder auf dem Bildschirm werden automatisch von iManager ausgefüllt.
- 5 Wenn Sie das erste Mal eine Verbindung zu einem Workflow-Server herstellen, geben Sie im Feld *Benutzeranwendungstreiber* den Namen des Treibers ein und klicken Sie auf *OK*.

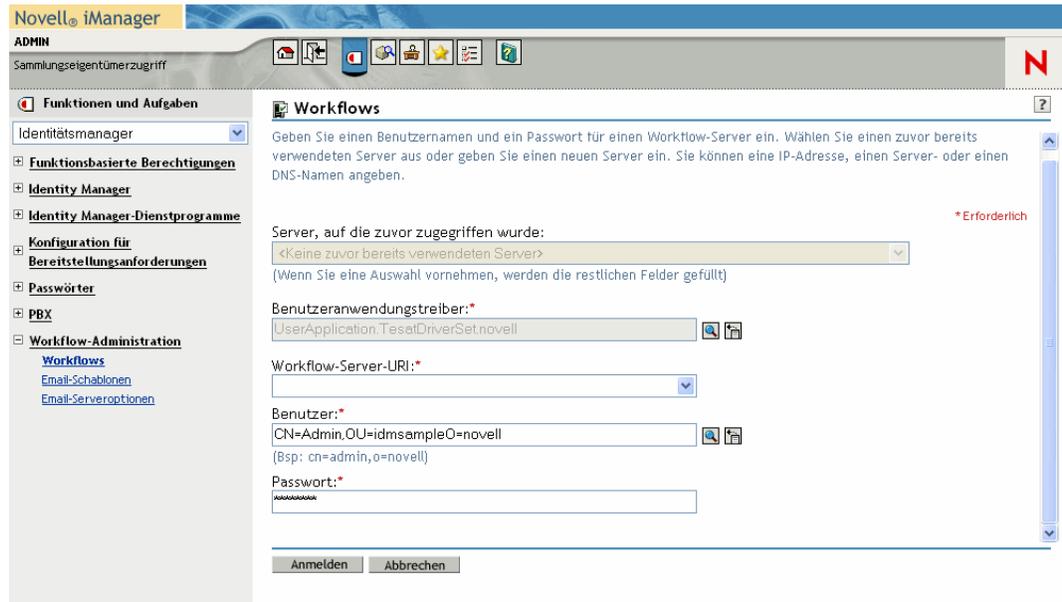
Die anderen Felder auf dem Bildschirm werden automatisch von iManager ausgefüllt.



- 6 Wenn der Treiber mehreren Workflow-Servern zugeordnet ist, wählen Sie im Feld *Workflow-Server-URI* den Zielservers aus.
- 7 Falls nötig, können Sie den Benutzernamen und das Passwort in den Feldern *Benutzer* und *Passwort* ändern.

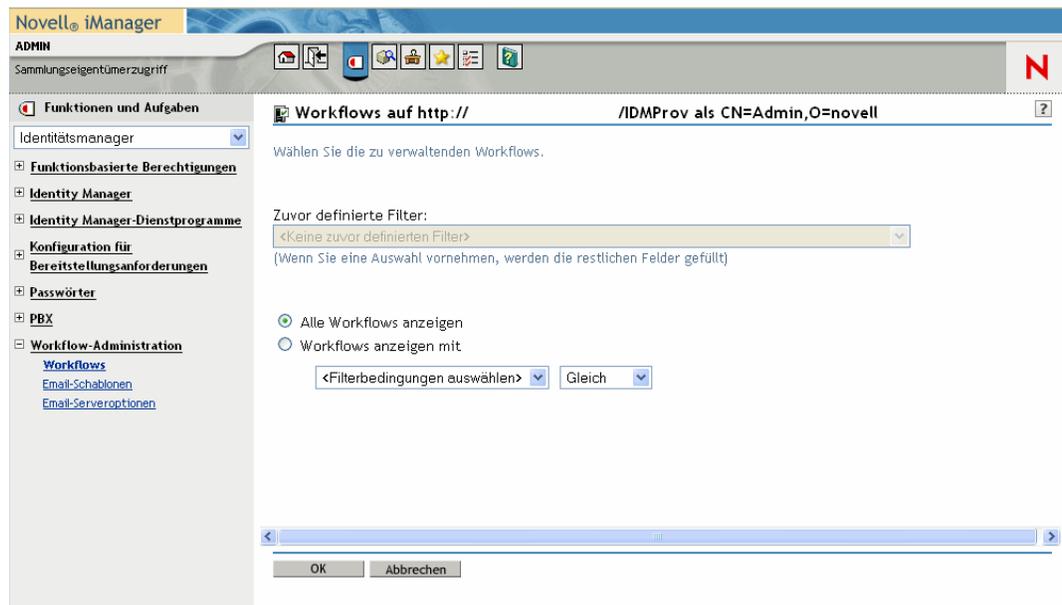
Der Benutzer muss der Benutzeranwendungsadministrator sein. Standardmäßig wird der Benutzername des Benutzers verwendet, der zurzeit bei iManager angemeldet ist. Ist dieser kein Administrator, müssen Sie den Benutzernamen ändern. Sie können beispielsweise den

Benutzernamen des Benutzeranwendungsadministrators der Test-OU „idmsample“ (siehe unten) verwenden:



8 Klicken Sie auf *Anmelden*.

Das Plugin „Workflow-Administration“ öffnet eine Seite, auf der Sie einen Filter für die Workflow-Suche erstellen können:

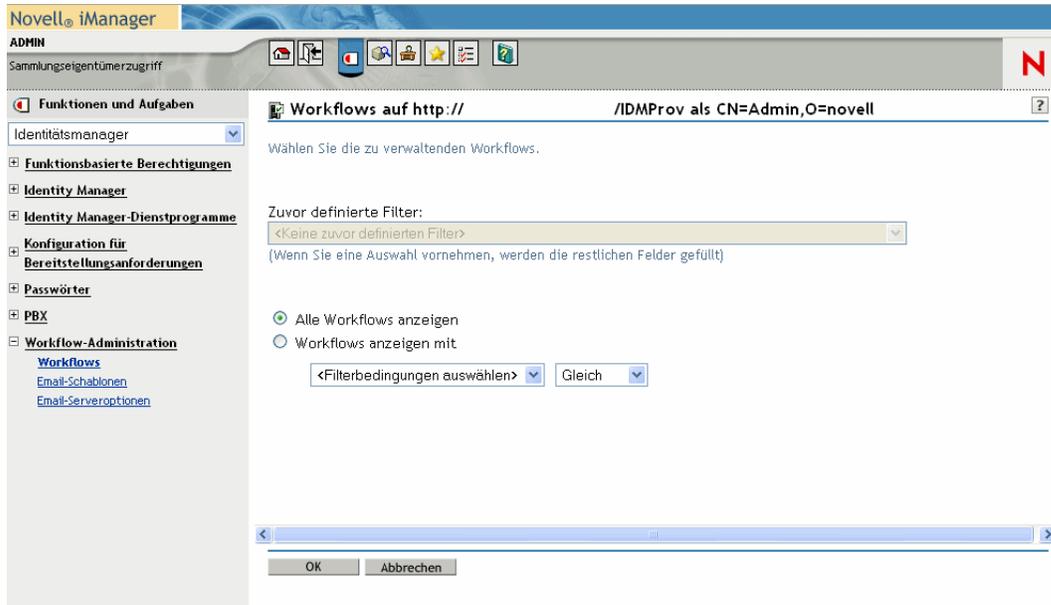


## 23.2.2 Suchen nach Workflows, die bestimmte Suchkriterien erfüllen

Wenn auf dem Ziel-Workflow-Server eine große Anzahl von Workflow-Prozessen läuft, ist es hilfreich, die in iManager angezeigte Liste von Workflows zu filtern. Hierzu müssen Sie Suchkriterien angeben.

So geben Sie Suchkriterien zum Filtern der Workflow-Liste an:

- 1 Klicken Sie auf das Optionsfeld *Workflows anzeigen mit*.



**Hinweis:** Standardmäßig ist das Optionsfeld *Alle Workflows anzeigen* ausgewählt. Ändern Sie die Vorgabe nicht, wenn die vollständige Liste der Workflows angezeigt werden soll.

- 2 Wählen Sie das Attribut aus, das Sie als Suchkriterium definieren möchten.

Attribut	Beschreibung
Erstellungsuhrzeit	Startzeit des Workflows.
Initiator	Benutzername des Erstellers.
Empfänger	Benutzername des Empfängers.
Prozessstatus	Allgemeiner Status des Workflow-Prozesses („Abgeschlossen“, „Läuft“ oder „Abgebrochen“).
Genehmigungsstatus	Status des Genehmigungsverfahrens („Genehmigt“, „Verweigert“ oder „Zurückgezogen“).
Berechtigungsstatus	Status der von der Bereitstellungsanforderung initiierten Berechtigung („Fehler“, „Gravierend“, „Erfolg“, „Unbekannt“ oder „Warnmeldung“).

3 Wählen Sie einen Operator aus:

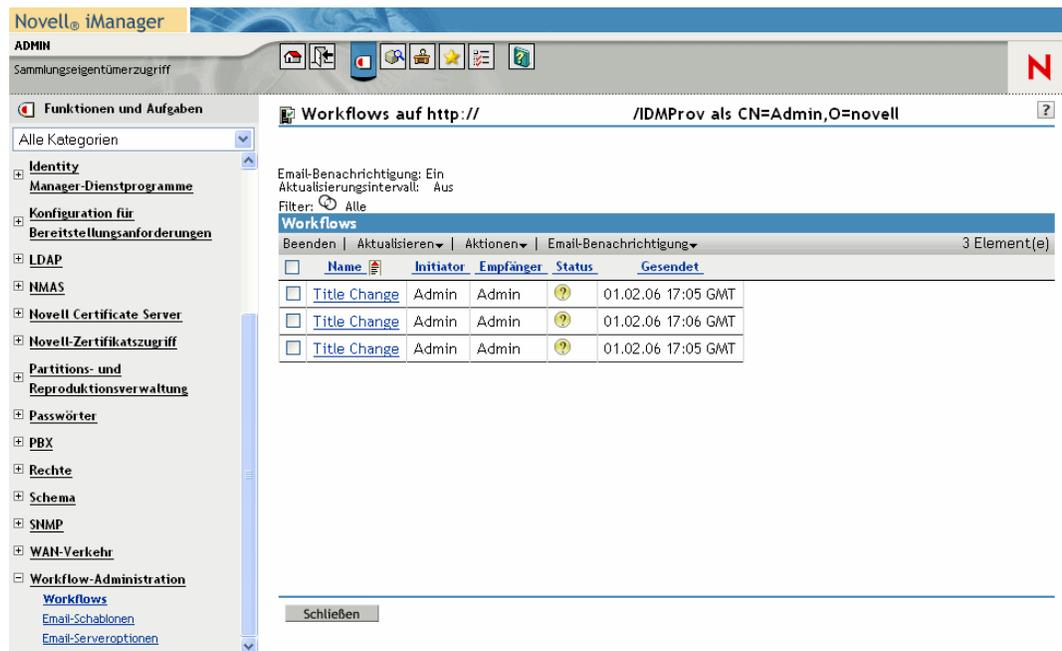
Operator	Kommentar
Gleich	Wird von allen Attributen unterstützt.
Vor	Gilt nur für das Attribut „Erstellungsuhrzeit“.
Nach	Gilt nur für das Attribut „Erstellungsuhrzeit“.
Zwischen	Gilt nur für das Attribut „Erstellungsuhrzeit“.

4 Geben Sie einen Wert im Feld unter dem Attribut und dem Operator ein.

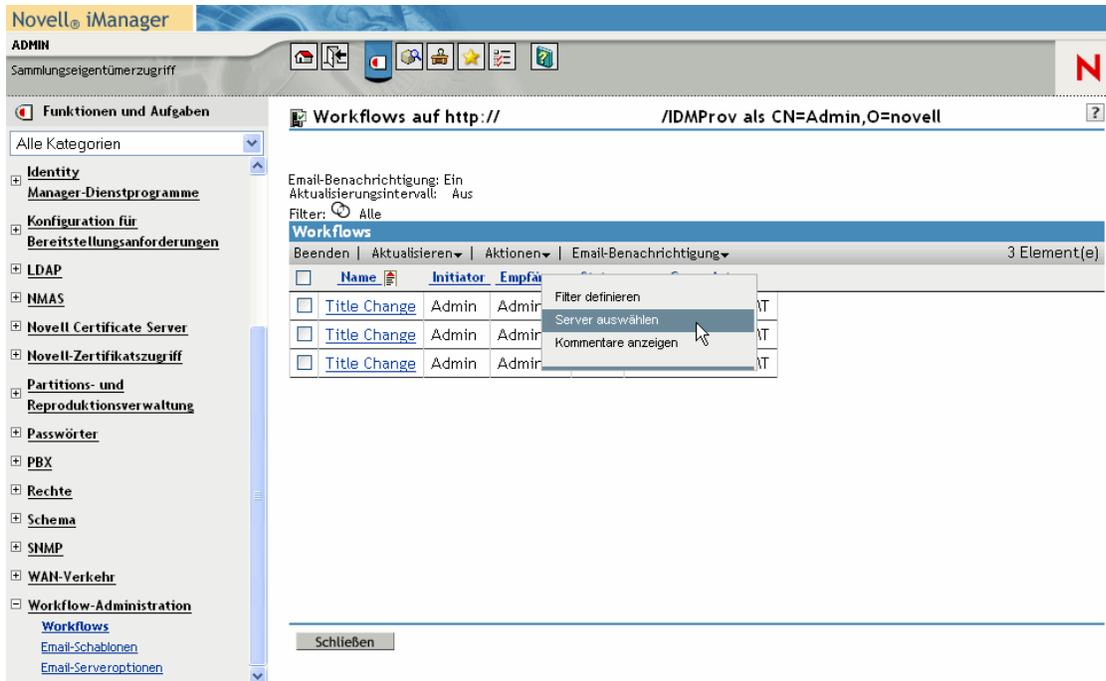
Sie können die Werte für die Erstellungsuhrzeit mit dem Steuerelement für Datum und Uhrzeit auswählen. Legen Sie die Werte für Initiator und Empfänger mithilfe des Objektverlaufs bzw. der Objektauswahl fest. Wählen Sie alle anderen Attributwerte in der Dropdown-Liste aus.

5 Klicken Sie auf *OK*.

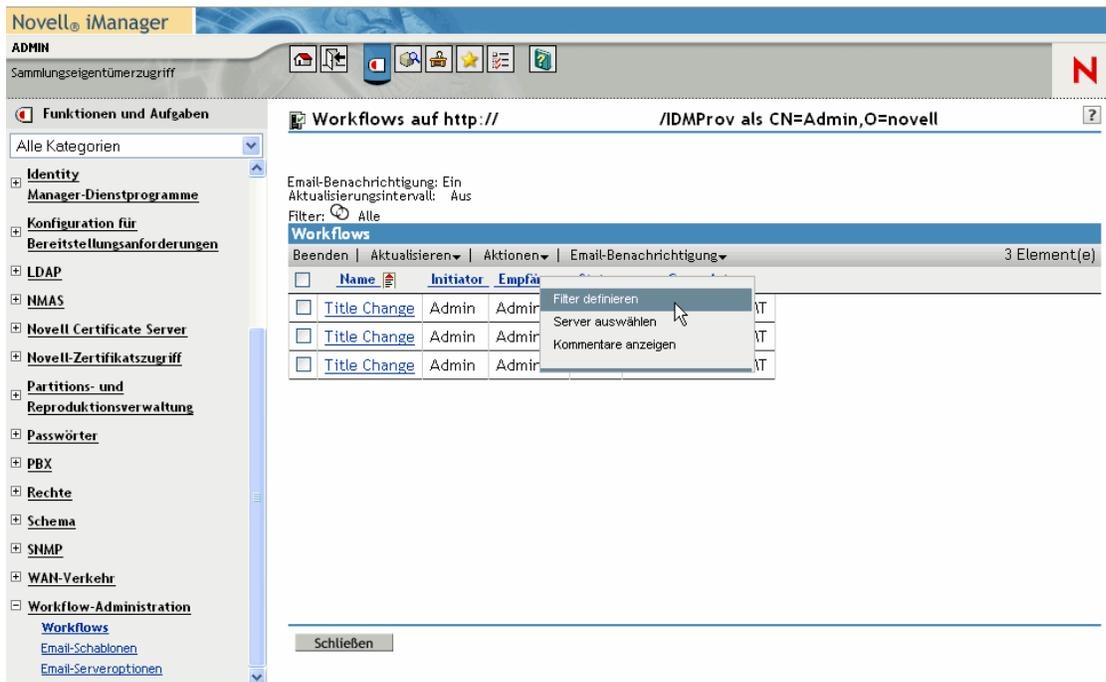
In iManager werden die ausgewählten Workflows im Teilfenster „Workflows“ angezeigt.



**Ändern des Zielservers und des Filters** Wenn Sie einen Workflow-Server ausgewählt haben, gilt diese Auswahl für die Dauer Ihrer iManager-Sitzung, es sein denn, Sie wählen einen neuen Server. Klicken Sie zum Auswählen eines neuen Servers auf den Befehl *Aktionen* und wählen Sie ihn im Menü *Server auswählen* aus.



Wenn Sie andere Suchkriterien erstellen möchten, wählen Sie *Filter definieren* im Menü *Aktionen*.



### 23.2.3 Steuern der Anzeige der aktiven Workflows

Das Teilfenster „Workflows“ enthält die Workflows, die die angegebenen Suchkriterien erfüllen. Neben dem Filtern der Liste können Sie auch die Anzeige steuern. Legen Sie beispielsweise fest, wie oft die Liste aktualisiert werden soll, oder sortieren Sie sie nach einer bestimmten Spalte.

## Aktualisieren der Workflow-Liste

Wenn auf dem Workflow-Server sehr viele Prozesse verarbeitet werden, ändert sich die Liste der aktiven Workflows sehr häufig. In diesem Fall ist es sinnvoll, die Liste der auf dem Server laufenden aktiven Workflows zu aktualisieren.

So aktualisieren Sie die Workflow-Liste:

- 1 Klicken Sie im Teilfenster „Workflows“ auf den Befehl *Aktualisieren*.
- 2 Wählen Sie eine der folgenden Optionen für das Aktualisierungsintervall im Menü „Aktualisieren“ aus:
  - 2a Aktualisieren Aus
  - 2b Jetzt aktualisieren
  - 2c 10 Sekunden
  - 2d 30 Sekunden
  - 2e 60 Sekunden
  - 2f 5 Minuten

## Sortieren der Workflow-Liste

Wenn eine große Anzahl an Anforderungsdefinitionen vorhanden ist, ist es hilfreich, die Liste nach einer bestimmten Spalte zu sortieren, z. B. nach Name oder Beschreibung.

So sortieren Sie die Workflow-Liste:

- 1 Klicken Sie auf die Überschrift der Spalte, nach der sortiert werden soll.

## 23.2.4 Beenden von Workflow-Instanzen

Falls eine Workflow-Instanz nicht weiter verarbeitet werden soll, können Sie den Workflow beenden.

So beenden Sie die Verarbeitung einer Workflow-Instanz:

- 1 Wählen Sie im Teilfenster „Workflows“ den Workflow aus, indem Sie auf das Kontrollkästchen neben dem Namen klicken.
- 2 Klicken Sie im Teilfenster „Workflows“ auf den Befehl *Beenden*.

## 23.2.5 Anzeigen von Details zu einer Workflow-Instanz

Während der Anzeige mehrerer auf einem bestimmten Server aktiven Workflows können Sie eine Workflow-Instanz auswählen, um weitere Details zu einem laufenden Prozess zu sehen.

---

**Hinweis:** Wenn die Workflow-Instanz seriell verarbeitet wird, sehen Sie nur eine aktuelle Aktivität, da nicht mehrere Benutzer gleichzeitig auf den Arbeitsschritt zugreifen dürfen. Bei einer parallelen

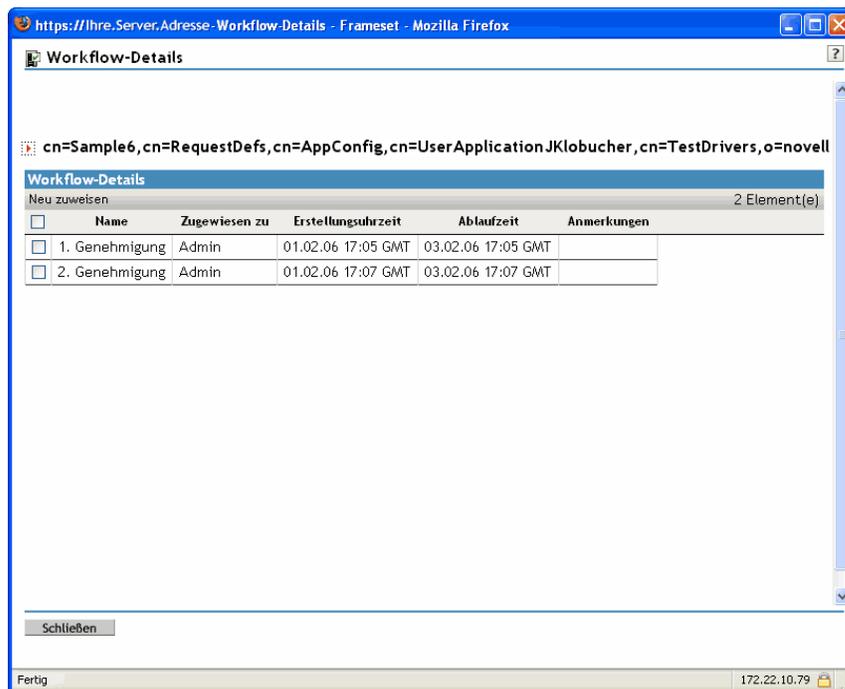
Verarbeitung und Verzweigung können mehrere aktuelle Aktivitäten für eine Workflow-Instanz angezeigt werden.

---

So zeigen Sie Details zu einer bestimmten Workflow-Instanz an:

- 1 Klicken Sie im Teilfenster „Workflows“ auf den Namen der Workflow-Instanz.

In iManager wird das Teilfenster „Workflow-Details“ angezeigt.



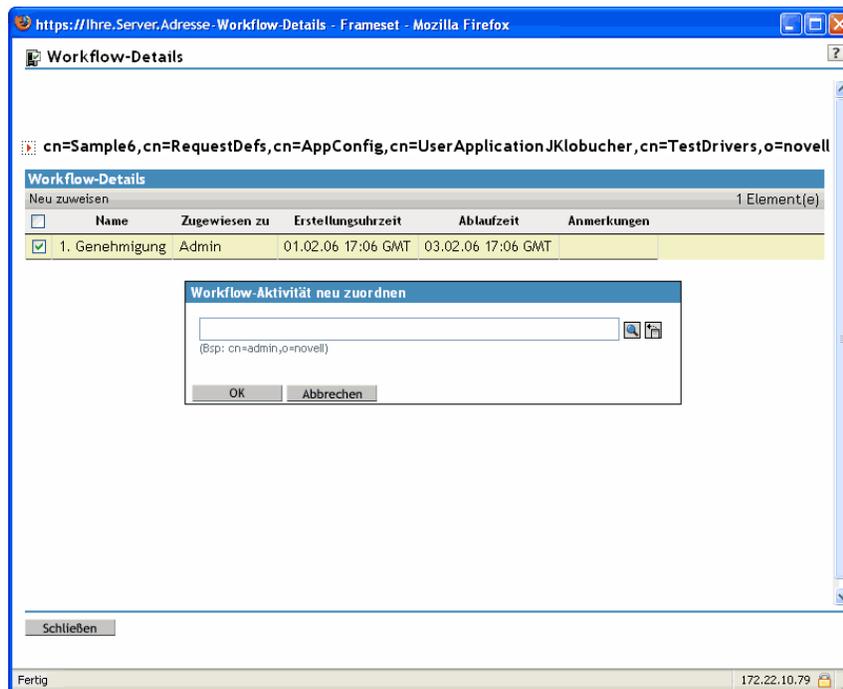
## 23.2.6 Neuordnung von Workflow-Instanzen

Falls eine Workflow-Instanz „hängt“, können Sie den Arbeitsschritt einem anderen Benutzer oder einer anderen Gruppe zuordnen.

So ordnen Sie eine Workflow-Instanz neu zu:

- 1 Wählen Sie im Teilfenster „Workflows“ die dem Workflow zugeordnete Aktivität aus, indem Sie auf das Kontrollkästchen neben ihrem Namen klicken.

2 Klicken Sie im Teilfenster „Workflows“ auf den Befehl *Neu zuordnen*.



3 Wählen Sie einen Benutzer oder eine Gruppe für die Neuordnung des Arbeitsschritts aus.

## 23.3 Konfigurieren des Email-Servers

Während der Verarbeitung eines Workflow-Prozesses werden häufig Email-Benachrichtigungen versendet. Beispielsweise kann es sinnvoll sein, eine Email zu versenden, wenn eine Workflow-Aktivität einem neuen Adressaten zugewiesen wird.

Bevor Sie die Email-Benachrichtigungsfunktionen von Identity Manager nutzen können, müssen Sie den SMTP-Email-Server konfigurieren. Verwenden Sie hierzu die Aufgabe *Email-Serveroptionen* der Funktion *Workflow-Administration* in iManager.

---

**Hinweis:** Diese Aufgabe ist eine Verknüpfung zur Aufgabe *Email-Serveroptionen* der Funktion *Passwörter*.

---

So konfigurieren Sie den Email-Server:

- 1 Wählen Sie in iManager die Kategorie „Identity Manager“.
- 2 Öffnen Sie die Funktion *Workflow-Administration*.
- 3 Klicken Sie auf die Aufgabe *Email-Serveroptionen*.

Der Bildschirm „Email-Serveroptionen“ wird angezeigt.

The screenshot shows the Novell iManager interface. The main window title is 'Novell iManager' and the user is logged in as 'ADMIN'. The left sidebar shows a navigation tree with 'Email-Serveroptionen' selected. The main content area is titled 'Email-Serveroptionen' and contains the following form:

Geben Sie die Einstellungen für Ihren Email-Benachrichtigungsserver ein.

Hostname:   
(zum Beispiel: mail.novell.com oder 137.89.119.5)

Von:   
(zum Beispiel: admin@novell.com)

Mit Berechtigungsnachweis beim Server authentifizieren:

Benutzername:

Passwort:

Passwort wiederholen:

Buttons: OK, Abbrechen

4 Geben Sie den Namen (oder die IP-Adresse) des Hostservers im Feld *Hostname* ein.

5 Geben Sie die Email-Adresse des Absenders im Feld *Von* ein.

Wenn die Email vom Empfänger geöffnet wird, wird dieser Text im Feld „Von“ des Email-Headers angezeigt. Je nach den Einstellungen des Mailservers muss der Text in diesem Feld unter Umständen mit einem gültigen Absender im System übereinstimmen, damit auf dem Mailserver Reverse-Lookups durchgeführt werden oder eine Authentifizierung stattfinden kann. Ein Beispiel ist helpdesk@firma.com anstelle eines beschreibenden Texts wie „Der Passwortadministrator“.

6 Wenn vor dem Senden von Emails Ihr Server eine Authentifizierung verlangt, wählen Sie das Kontrollkästchen *Mit Berechtigungsnachweis beim Server authentifizieren* aus und geben Sie den Benutzernamen und das Passwort ein.

7 Klicken Sie zum Abschluss auf *OK*.

## 23.4 Arbeiten mit den installierten Email-Schablonen

Im Lieferumfang von Identity Manager ist eine Email-Schablone enthalten, die speziell für die Workflow-basierte Bereitstellung erstellt wurde. Diese Email-Schablone heißt *Neue Bereitstellungsanforderung*. Alle im Produkt enthaltenen Bereitstellungsanforderungsschablonen sind mit dieser Email-Schablone verknüpft. Von Ihnen neu erstellte Anforderungsdefinitionen verwenden daher ebenfalls diese Email-Schablone.

Sie können die Schablone „Neue Bereitstellungsanforderung“ bearbeiten, um den Inhalt und das Format von Emails zu ändern. Das Erstellen neuer Email-Schablonen ist jedoch nicht möglich.

Bearbeiten Sie die Schablone „Neue Bereitstellungsanforderung“ in iManager mithilfe der Aufgabe *Email-Schablonen* der Funktion *Workflow-Administration*.

---

**Hinweis:** Diese Aufgabe ist eine Verknüpfung zur Aufgabe *Email-Schablonen bearbeiten* der Funktion *Passwörter*.

---

### 23.4.1 Standardinhalt und -format

Nach der Installation des Produkts sieht die Schablone „Neue Bereitstellungsanforderung“ wie folgt aus:

```
Dear $userFirstName$,
A new provisioning request has been submitted that requires your
approval.
Request name: $requestTitle$
Submitted by: $initiatorFullName$
Recipient: $recipientFullName$
Please review the details of this request at $PROTOCOL$://
$HOST$: $PORT$/$TASK_DETAILS$ to take the appropriate action.
You can review a list of all requests pending your approval at
$PROTOCOL$://$HOST$: $PORT$/$TASKLIST_CONTEXT$.
```

Die Schablone gibt die Bereitstellungsanforderungsdefinition an, die die Email ausgelöst hat. Zudem enthält sie eine URL-Adresse, die den Adressaten zu der Aufgabe umleitet, die genehmigt werden muss, und eine URL-Adresse, die eine vollständige Liste der ausstehenden Aufgaben des Benutzers anzeigt.

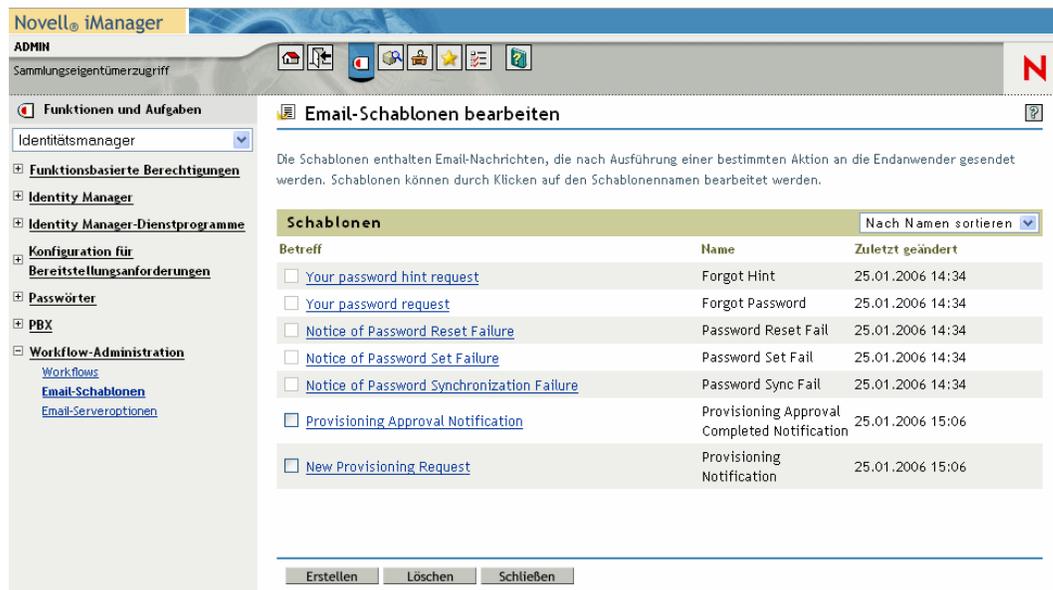
### 23.4.2 Bearbeiten der Schablone

Sie können den Inhalt oder das Format der Schablone „Neue Bereitstellungsanforderung“ ändern. Beachten Sie, dass die Schablone für alle Bereitstellungsanforderungen in der Identity Manager-Benutzeranwendung gilt. Stellen Sie daher sicher, dass die Änderungen für alle Benutzer und Workflow-Aufgaben geeignet sind.

So bearbeiten Sie die Schablone:

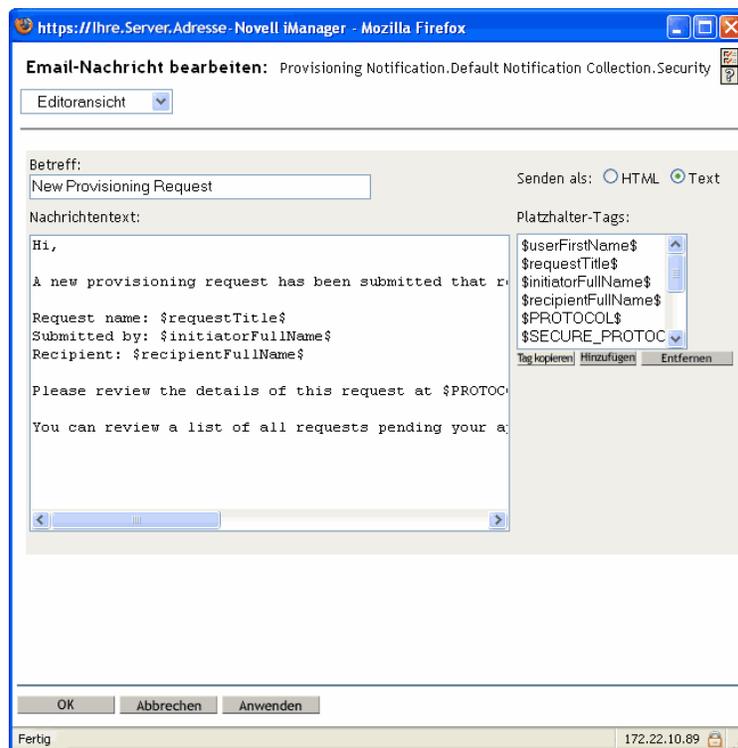
- 1 Wählen Sie in iManager die Kategorie „Identity Manager“.
- 2 Öffnen Sie die Funktion *Workflow-Administration*.
- 3 Klicken Sie auf die Aufgabe *Email-Schablonen*.

Der Bildschirm „Email-Schablonen bearbeiten“ wird angezeigt.



4 Klicken Sie in der Liste der Schablonen auf *Neue Bereitstellungsanforderung*.

Der Bildschirm „Email-Nachricht bearbeiten“ wird angezeigt.



5 Geben Sie die Änderungen im Feld *Nachrichtentext* ein.

- 6 Falls nötig, kopieren Sie ein oder mehrere der mitgelieferten Tags aus dem Listenfeld „Platzhalter-Tags“, wenn Sie dynamischen Text in den Nachrichtentext einfügen möchten. Im Folgenden werden die Platzhalter-Tags kurz beschrieben:

Tag	Beschreibung
<code>\$userFirstName\$</code>	Der Vorname des Adressaten.
<code>\$requestTitle\$</code>	Der Anzeigename der Bereitstellungsanforderungsdefinition.
<code>\$initiatorFullName\$</code>	Der vollständige Name des Initiators.
<code>\$recipientFullName\$</code>	Der vollständige Name des Empfängers.
PROTOCOL	Das Protokoll für in Emails enthaltene URL-Adressen.
<code>\$SECURE_PROTOCOL\$</code>	Das sichere Protokoll für in Emails enthaltene URL-Adressen.
<code>\$HOST\$</code>	Der Host des JBoss Application Server, auf dem die Identity Manager-Benutzeranwendung läuft.
<code>\$PORT\$</code>	Der Port der Identity Manager-Benutzeranwendung.
<code>\$SECURE_PORT\$</code>	Der sichere Port der Identity Manager-Benutzeranwendung.
<code>\$TASKLIST_CONTEXT\$</code>	Die Seite, die eine Liste aller ausstehenden Anforderungen des Adressaten anzeigt.
<code>\$TASK_DETAILS\$</code>	Die Seite, die Details zu der Anforderung anzeigt, für die diese Email erstellt wurde.

- 7 Klicken Sie zum Abschluss auf *OK*.

### 23.4.3 Ändern von Standardwerten der Schablone

Bei der Installation können Sie Standardwerte für einige der in Email-Schablonen verwendeten Platzhalter-Tags festlegen. Nach der Installation können Sie diese Werte mithilfe des Werkzeugs zur Konfiguration der Benutzeranwendung ändern.

So ändern Sie die Installationseinstellungen:

- 1 Führen Sie das Skript „`ldapconfig.sh`“ aus, das sich im Ordner „`idm`“ befindet.

```
./configupdate.sh
```

---

**Hinweis:** Unter Windows müssen Sie die Datei `configupdate.bat` ausführen.

---

2 Ändern Sie, falls notwendig, die Einträge der folgenden Felder:

Feld	Beschreibung
Email Notify Host	Ersetzt das Token \$HOST\$ in Email-Schablonen, die in Genehmigungsabläufen verwendet werden. Ist das Feld leer, wird es vom Server ausgefüllt. (Dies ist der JBoss-Host.)
Email Notify Port	Ersetzt das Token \$PORT\$ in Email-Schablonen, die in Genehmigungsabläufen verwendet werden.
Email Notify Secure Port	Ersetzt das Token \$SECURE_PORT\$ in Email-Schablonen, die in Genehmigungsabläufen verwendet werden.

3 Klicken Sie auf *OK*, um die Änderungen zu bestätigen.



# Anhänge

# VI

Die folgenden Anhänge bieten zusätzliche Referenzinformationen und erweiterte Aspekte der Identity Manager-Benutzeranwendung.

- [Anhang A, „Schemaerweiterungen“, auf Seite 365](#)
- [Anhang B, „Konfigurieren des Anwendungsarchivs“, auf Seite 391](#)



# Schemaerweiterungen

# A

## A.1 Attribut-Schemaerweiterungen

ATTRIBUTNAME	BESCHREIBUNG
<b>srvprvAOLIMAddress</b>	<b>AOL IM-Adresse</b>
srvprvActiveDelegateds	Die aktiven Delegierten eines Benutzers
srvprvActiveDelegators	Die aktiven Delegierenden eines Benutzers
srvprvAssetRef	Darstellung der Aggregat-Asset-Eigenschaften für ein benanntes Asset, das einem Benutzer über die <code>srvprvAssetRecipientAux</code> -Klasse zugeordnet ist
srvprvAssignExpiration	Zeitpunkt, zu dem eine Vertretungs- oder Delegiertenzuweisung abläuft
srvprvAssignFromContainer	Container-Subjekte einer Vertretungs- oder Delegiertenzuweisung
srvprvAssignFromGroup	Gruppensubjekte einer Vertretungs- oder Delegiertenzuweisung
srvprvAssignFromUser	Benutzersubjekte einer Vertretungs- oder Delegiertenzuweisung
srvprvAssignToRelationship	Zielrelation einer Delegiertenzuweisung
srvprvAssignToUser	Benutzerziele einer Vertretungs- oder Delegiertenzuweisung
srvprvCategoryKey	Weist eine bestimmte Bereitstellungsanforderungsdefinition einem Satz von Bereitstellungskategorien zu. Die Werte sind Schlüssel für eine <code>srvprvChoice</code> -Instanz
srvprvDefaultTheme	Das Standardmotiv
srvprvEntitlementRef	Referenz auf eine DirXML-Berechtigung
srvprvEntityType	Gibt den Entitätsdefinitionstyp der Verzeichnisabstraktionsschicht an
srvprvFlowStrategy	Gibt die Ablaufstrategie für die Bereitstellungsanforderungsdefinition an
srvprvGrant	Falls „Wahr“ bedeutet dies, dass die Bereitstellungsanforderungsdefinition die Grant-Operation unterstützt
srvprvGroupwiseIMAddress	Groupwise IM-Adresse
srvprvHeaderFillerFile	Dateiname des Header-Füllers
srvprvHeaderFillerImage	Header-Füllbild
srvprvHeaderFillerLastMod	Header-Füllbild zuletzt geändert
srvprvHeaderLogo2File	Dateiname des sekundären Bilds des Header-Logos

<b>ATTRIBUTNAME</b>	<b>BESCHREIBUNG</b>
<b>srvprvAOLIMAddress</b>	<b>AOL IM-Adresse</b>
srvprvHeaderLogo2Image	Sekundäres Bild des Header-Logos
srvprvHeaderLogo2LastMod	Sekundäres Header-Logo zuletzt geändert
srvprvHeaderLogoFile	Dateiname des primären Bilds des Header-Logos
srvprvHeaderLogoImage	Primäres Bild des Header-Logos
srvprvHeaderLogoLastMod	Primäres Header-Logo zuletzt geändert
srvprvHeaderTextureFile	Dateiname der Header-Textur
srvprvHeaderTextureImage	Header-Texturgrafik
srvprvHeaderTextureLastMod	Header-Textur zuletzt geändert
srvprvIsTaskManager	Gibt an, ob der Benutzer ein Aufgabengruppenmanager ist
srvprvLocalizedDescrs	Bietet lokalisierte Beschreibungen für Webanwendungen, Designer und iManager zur Bereitstellung
srvprvLocalizedNames	Bietet lokalisierte Anzeigenamen für Webanwendungen, Designer und iManager zur Bereitstellung
srvprvLoginFile	Dateiname des Anmeldebilds
srvprvLoginImage	Anmeldebild
srvprvLoginLastMod	Anmeldebild zuletzt geändert
srvprvLoginSmallFile	Dateiname des kleinen Anmeldebilds
srvprvLoginSmallImage	Kleines Anmeldebild
srvprvLoginSmallLastMod	Kleines Anmeldebild zuletzt geändert
srvprvModified	Gibt Änderungen an Definitionsobjektinstanzen im Verzeichnismodellcontainer an
srvprvNavBckgrColor	Navigations-Hintergrundfarbe
srvprvNavBckgrColorLastMod	Navigations-Hintergrundfarbe zuletzt geändert
srvprvNavColor	Navigationsfarbe
srvprvNavColorLastMod	Navigationsfarbe zuletzt geändert
srvprvPreferredLocale	Liste gespeicherter Abfrage-/Suchkriterien
srvprvProcessXML	XML-Dokument, das eine Bereitstellungsprozessdefinition enthält, einschließlich Workflow- und Bereitstellungsaktionen
srvprvRequestDefName	Der Name der Bereitstellungsanforderungsdefinition, die einer Delegiertendefinition zugeordnet ist.
srvprvRequestXML	XML-Dokument, das das ursprüngliche Anforderungsformular und seine Datenbindungen enthält
srvprvRevoke	Falls „Wahr“ bedeutet dies, dass die Bereitstellungsanforderungsdefinition die Revoke-Operation unterstützt

ATTRIBUTNAME	BESCHREIBUNG
srvprvAOLIMAddress	AOL IM-Adresse
srvprvStatus	Status des Bereitstellungsobjekts
srvprvTaskGroups	Gruppen, für die der Benutzer ein Aufgabenmanager ist
srvprvUUID	Eindeutige ID des Portlets
srvprvTaskManager	Aufgabenmanager der Aufgabengruppe
srvprvYahooIMAddress	Yahoo IM-Adresse

## A.2 Objectclass-Schemaerweiterungen

OBJECTCLASS-NAME	BESCHREIBUNG
srvprvAppConfig	<b>Container für Anwen­dungskonfigurationsobjekte des Bereitstellungs­systems, zu denen der übergeordnete DirXML-Treiber eine Verbindung herstellt</b>
srvprvAppDefs	Container für Konfigurationsobjekte, die zur Initialisierung der Bereitstellungs-Laufzeitumgebung verwendet werden, z. B. Motive für das Identitäts-Portlet
srvprvAssetRecipientAux	Zeichnet die Bereitstellung von Nicht-IT-Assets für den Benutzer auf
srvprvChoice	Auflistung von Werten, die einem bestimmten Attribut zugewiesen werden können, das in einer Abfrage o. ä. für Identitäts-Portlets und andere Webanwendungskomponenten verwendet werden kann
srvprvChoiceDefs	Container für Verzeichnisabstraktionsschicht-Auswahldefini­tionen, die von den Identitäts-Portlets und Webanwendungen freigelegt werden
srvprvDelegateeAssignment	Delegiertenzuweisungsdefinition
srvprvDelegateeDefs	Container für Delegiertendefinitionen
srvprvDirectoryModel	Container für Verzeichnisabstraktionsschicht-Objekte auf Metaebene, ausgewählte Inhalte des Verzeichnisses, das von den Identitäts-Portlets und Webanwendungen freigelegt wird
srvprvDirectoryModelConfig	Konfigurationsparameter der Laufzeit-Verzeichnisabstrak­tionsschicht
srvprvEntity	Definiert eine Ansicht ausgewählter Attribute für definierte Klas­sen in dem Verzeichnis, das von Identitäts-Portlets und anderen Webanwendungskomponenten verwendet wird
srvprvEntityAux	Standard-ObjectClass
srvprvEntityDefs	Container für Verzeichnisabstraktionsschicht-Entitätsdefini­tionen, die von den Identitäts-Portlets und Webanwendungen freigelegt werden
srvprvProxyAssignment	Vertretungszuweisungsdefinition

OBJECTCLASS-NAME	BESCHREIBUNG
srvprvAppConfig	<b>Container für Anwendungskonfigurationsobjekte des Bereitstellungssystems, zu denen der übergeordnete DirXML-Treiber eine Verbindung herstellt</b>
srvprvProxyDefs	Container für Vertretungsdefinitionen
srvprvRelationship	Definiert Relationen zwischen Objekten im Verzeichnis zur Verwendung in Identitäts-Portlets und anderen Webanwendungskomponenten
srvprvRelationshipDefs	Container für Verzeichnisabstraktionsschicht-Relationsdefinitionen, die von den Identitäts-Portlets und Webanwendungen freigelegt werden
srvprvRequest	Legt ein bereitstellbares Element zum Erteilen oder Entziehen frei, einschließlich des Workflow-Prozesses, der die Laufzeitaspekte des Workflow- und Bereitstellungsziels definiert
srvprvRequestDefs	Container für Bereitstellungsanforderungsdefinitionen, einen Satz bereitstellbarer Elemente für die Webanwendungs-Laufzeit
srvprvResource	Definiert die Verzeichniszuweisungen, die für eine Bereitstellungs-Fulfillment-Operation (entweder Grant oder Revoke) ausgeführt werden müssen
srvprvResourceDefs	Ein Container für Definitionen von Bereitstellungszielen, einschließlich Beschreibungen während der Design-Phase sowie beliebiger Schablonen oder ungenutzter Ziele
srvprvService	Beschreibt den Aufruf eines bestimmten Web-Service aus einem Workflow, dazu gehört die Angabe von Input- und Rückgabewerten
srvprvServiceDefs	Container für Servicedefinitionsobjekte, die die von Workflows aufgerufenen Web-Services enthalten.
srvprvTaskGroupAux	Aufgabengruppe für die Bereitstellung von Services
srvprvTheme	Motivobjekt
srvprvUserAux	Benutzerentität für die Bereitstellung von Services
srvprvWebAppConfig	Webanwendungs-Konfigurationsobjekt
srvprvWorkflow	Definiert das Netzwerk der Aktivitäten einschließlich traversaler Bedingungen, die zur Genehmigung einer Bereitstellungsaktion ausgeführt werden müssen
srvprvWorkflowDefs	Container für Workflow-Objekte, einschließlich der Beschreibungen während des Designs plus etwaiger Schablonen-abläufe bzw. unbenutzter Abläufe
srvprvServiceDefs	Container für Servicedefinitionsobjekte, die die von Workflows aufgerufenen Web-Services enthalten.
srvprvStatus	Status des Bereitstellungsobjekts
srvprvTaskGroupAux	Aufgabengruppe für die Bereitstellung von Services
srvprvTaskGroups	Gruppen, für die der Benutzer ein Aufgabenmanager ist

OBJECTCLASS-NAME	BESCHREIBUNG
srvprvAppConfig	Container für Anwen­dungskonfigurationsobjekte des Bereitstellungs­systems, zu denen der übergeordnete DirXML-Treiber eine Verbindung herstellt
srvprvTaskManager	Aufgabenmanager der Aufgabengruppe
srvprvTheme	Motivobjekt
srvprvUserAux	Benutzerentität für die Bereitstellung von Services
srvprvWebAppConfig	Webanwendungs-Konfigurationsobjekt
srvprvWorkflow	Definiert das Netzwerk der Aktivitäten einschließlich traversaler Bedingungen, die zur Genehmigung einer Bereitstellungsaktion ausgeführt werden müssen
srvprvWorkflowDefs	Container für Workflow-Objekte, einschließlich der Beschreibungen während des Designs plus etwaiger Schablonen-abläufe bzw. unbenutzter Abläufe
srvprvYahooIMAddress	Yahoo IM-Adresse

## A.3 LDIF-Darstellung

Die vollständigen Schemainformationen einschließlich Syntax, Containment-Regeln und weiteren Informationen, die in der obigen Zusammenfassung nicht enthalten sind, werden nachfolgend (in LDIF-Format) dargestellt. Diese Informationen unterliegen Änderungen.

```

version: 1
# Copyright (c) 2004-2005 Unpublished Work of Novell, Inc. All Rights
# Reserved.
#
# THIS WORK IS AN UNPUBLISHED WORK AND CONTAINS CONFIDENTIAL,
# PROPRIETARY AND TRADE SECRET INFORMATION OF NOVELL, INC. ACCESS TO
# THIS WORK IS RESTRICTED TO (I) NOVELL, INC. EMPLOYEES WHO HAVE A NEED
# TO KNOW HOW TO PERFORM TASKS WITHIN THE SCOPE OF THEIR ASSIGNMENTS
AND
# (II) ENTITIES OTHER THAN NOVELL, INC. WHO HAVE ENTERED INTO
# APPROPRIATE LICENSE AGREEMENTS. NO PART OF THIS WORK MAY BE USED,
# PRACTICED, PERFORMED, COPIED, DISTRIBUTED, REVISED, MODIFIED,
# TRANSLATED, ABRIDGED, CONDENSED, EXPANDED, COLLECTED, COMPILED,
# LINKED, RECAST, TRANSFORMED OR ADAPTED WITHOUT THE PRIOR WRITTEN
# CONSENT OF NOVELL, INC. ANY USE OR EXPLOITATION OF THIS WORK WITHOUT
# AUTHORIZATION COULD SUBJECT THE PERPETRATOR TO CRIMINAL AND CIVIL
# LIABILITY.
#
# Base schema extensions for SpitFire
#
# Last Modified: 6/27/05 (ek)
#
# See rfc2252 for information on attribute syntax definitions
#   String = 1.3.6.1.4.1.1466.115.121.1.15
#   Boolean = 1.3.6.1.4.1.1466.115.121.1.7

```

```

#   Octet String = 1.3.6.1.4.1.1466.115.121.1.40
#   DN = 1.3.6.1.4.1.1466.115.121.1.12
#   Case Exact String = 1.3.6.1.4.1.1466.115.121.1.26
#   Case Ignore List = 2.16.840.1.113719.1.1.5.1.6
#   Case Ignore String = 1.3.6.1.4.1.1466.115.121.1.15
#   Stream = 1.3.6.1.4.1.1466.115.121.1.5
#   Time = 1.3.6.1.4.1.1466.115.121.1.24
#
# OID registered for EPM:
#   subarc "450" registered at: https://wiki.innerweb.novell.com/
wiki.phtml?title=OID_Registration
#   attribute prefix: 2.16.840.1.113719.1.450.4.{3 digit unique per
attribute}
#   object class prefix: 2.16.840.1.113719.1.450.6.{3 digit unique
number per class}
#-----
#-----
#-- Framework Attributes
#-----
#-----
dn: cn=schema
changetype: modify
add: attributeTypes
attributeTypes: (
  2.16.840.1.113719.1.450.4.127
  NAME 'srvprvUUID'
  DESC 'Standard Attribute'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26{64512}
  SINGLE-VALUE
  X-NDS_PUBLIC_READ '1'
  X-NDS_NOT_SCHED_SYNC_IMMEDIATE '1'
)
dn: cn=schema
changetype: modify
add: objectClasses
objectClasses: (
  2.16.840.1.113719.1.450.6.127
  NAME 'srvprvEntityAux'
  DESC 'Standard ObjectClass'
  AUXILIARY MAY srvprvUUID
  X-NDS_NOT_CONTAINER '1'
)
#-----
#-----
#-- User Attributes
#-----
#-----
dn: cn=schema
changetype: modify
add: attributeTypes
attributeTypes: (
  2.16.840.1.113719.1.450.4.60
  NAME 'srvprvHideUser'
  DESC 'Indicates if a user is hidden during searches'
)

```

```

    SYNTAX 1.3.6.1.4.1.1466.115.121.1.7
    SINGLE-VALUE
)
dn: cn=schema
changetype: modify
add: attributeTypes
attributeTypes: (
    2.16.840.1.113719.1.450.4.61
    NAME 'srvprvHideAttributes'
    DESC 'List of attributes a user is hiding from other users'
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
)
dn: cn=schema
changetype: modify
add: attributeTypes
attributeTypes: (
    2.16.840.1.113719.1.450.4.62
    NAME 'srvprvQueryList'
    DESC 'List of saved query/search criteria'
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
    SINGLE-VALUE
)
dn: cn=schema
changetype: modify
add: attributeTypes
attributeTypes: (
    2.16.840.1.113719.1.450.4.63
    NAME 'srvprvCapabilities1'
    DESC 'Place holder for classifying skills, knowledge, references,
etc. Classifications are defined in the application.'
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
)
dn: cn=schema
changetype: modify
add: attributeTypes
attributeTypes: (
    2.16.840.1.113719.1.450.4.64
    NAME 'srvprvCapabilities2'
    DESC 'Place holder for classifying skills, knowledge, references,
etc. Classifications are defined in the application.'
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
)
dn: cn=schema
changetype: modify
add: attributeTypes
attributeTypes: (
    2.16.840.1.113719.1.450.4.65
    NAME 'srvprvCapabilities3'
    DESC 'Place holder for classifying skills, knowledge, references,
etc. Classifications are defined in the application.'
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
)
dn: cn=schema
changetype: modify

```

```

add: attributeTypes
attributeTypes: (
  2.16.840.1.113719.1.450.4.66
  NAME 'srvprvCapabilities4'
  DESC 'Place holder for classifying skills, knowledge, references,
etc. Classifications are defined in the application.'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
)
dn: cn=schema
changetype: modify
add: attributeTypes
attributeTypes: (
  2.16.840.1.113719.1.450.4.67
  NAME 'srvprvCapabilities5'
  DESC 'Place holder for classifying skills, knowledge, references,
etc. Classifications are defined in the application.'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
)
dn: cn=schema
changetype: modify
add: attributeTypes
attributeTypes: (
  2.16.840.1.113719.1.450.4.68
  NAME 'srvprvIMAddress'
  DESC 'Key-value pair of Instant messenger Addresses i.e.
groupwise~jsmith'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
)
# This is temporary until we convert the application to use the multi-
value IM address (srvprvIMAddress) above
dn: cn=schema
changetype: modify
add: attributeTypes
attributeTypes: (
  2.16.840.1.113719.1.450.4.69
  NAME 'srvprvGroupwiseIMAddress'
  DESC 'Groupwise IM address'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
  SINGLE-VALUE
)
# This is temporary until we convert the application to use the multi-
value IM address (srvprvIMAddress) above
dn: cn=schema
changetype: modify
add: attributeTypes
attributeTypes: (
  2.16.840.1.113719.1.450.4.70
  NAME 'srvprvYahooIMAddress'
  DESC 'Yahoo IM address'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
  SINGLE-VALUE
)
# This is temporary until we convert the application to use the multi-
value IM address (srvprvIMAddress) above

```

```

dn: cn=schema
changetype: modify
add: attributeTypes
attributeTypes: (
  2.16.840.1.113719.1.450.4.71
  NAME 'srvprvAOLIMAddress'
  DESC 'AOL IM address'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
  SINGLE-VALUE
)
dn: cn=schema
changetype: modify
add: attributeTypes
attributeTypes: (
  2.16.840.1.113719.1.450.4.72
  NAME 'srvprvActiveDelegates'
  DESC 'The active delegates of a user'
  SYNTAX 2.16.840.1.113719.1.1.5.1.6
)
dn: cn=schema
changetype: modify
add: attributeTypes
attributeTypes: (
  2.16.840.1.113719.1.450.4.73
  NAME 'srvprvActiveDelegators'
  DESC 'The active delegators of a user'
  SYNTAX 2.16.840.1.113719.1.1.5.1.6
)
dn: cn=schema
changetype: modify
add: attributeTypes
attributeTypes: (
  2.16.840.1.113719.1.450.4.74
  NAME 'srvprvIsTaskManager'
  DESC 'Indicates if user is a task group manager'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.7
  SINGLE-VALUE
)
dn: cn=schema
changetype: modify
add: attributeTypes
attributeTypes: (
  2.16.840.1.113719.1.450.4.75
  NAME 'srvprvTaskGroups'
  DESC 'Groups for which the user is a task manager'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
)
dn: cn=schema
changetype: modify
add: attributeTypes
attributeTypes: (
  2.16.840.1.113719.1.450.4.77
  NAME 'srvprvPreferredLocale'
  DESC 'List of saved query/search criteria'
)

```

```

SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE
)
dn: cn=schema
changetype: modify
add: objectclasses
objectClasses: (
  2.16.840.1.113719.1.450.6.128
  NAME 'srvprvUserAux'
  DESC 'Service provisioning user entity'
  AUXILIARY MAY ( srvprvHideUser $ srvprvHideAttributes $
srvprvQueryList $
                srvprvCapabilities1 $ srvprvCapabilities2 $
srvprvCapabilities3 $ srvprvCapabilities4 $ srvprvCapabilities5 $
                srvprvIMAddress $ srvprvGroupwiseIMAddress $
srvprvYahooIMAddress $ srvprvAOLIMAddress $ srvprvIsTaskManager $
                srvprvTaskGroups $ srvprvActiveDelegates $
srvprvActiveDelegators $ srvprvPreferredLocale)
  X-NDS_NOT_CONTAINER '1'
)
dn: cn=schema
changetype: modify
add: attributeTypes
attributeTypes: (
  2.16.840.1.113719.1.450.4.129
  NAME 'srvprvTaskManager'
  DESC 'Task manager of the task group'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
)
dn: cn=schema
changetype: modify
add: objectclasses
objectClasses: (
  2.16.840.1.113719.1.450.6.130
  NAME 'srvprvTaskGroupAux'
  DESC 'Service provisioning task group'
  AUXILIARY MAY ( srvprvTaskManager )
  X-NDS_NOT_CONTAINER '1'
)
#-----
#-----
#-- Provisioning Attributes
#-----
#-----
dn: cn=schema
changetype: modify
add: attributeTypes
attributeTypes: (
  2.16.840.1.113719.1.450.4.100
  NAME 'srvprvCategoryKey'
  DESC 'Associates a given Provisioning Request Definition to a set of
provisioning categories. Values are keys to a srvprvChoice instance.'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
)

```

```

dn: cn=schema
changetype: modify
add: attributeTypes
attributeTypes: (
  2.16.840.1.113719.1.450.4.101
  NAME 'srvprvGrant'
  DESC 'Flag which if true specifies that the Provisioning Request
Definition supports a Grant operation.'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.7
  SINGLE-VALUE
)
dn: cn=schema
changetype: modify
add: attributeTypes
attributeTypes: (
  2.16.840.1.113719.1.450.4.102
  NAME 'srvprvRevoke'
  DESC 'Flag which if true specifies that the Provisioning Request
Definition supports a Revoke operation.'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.7
  SINGLE-VALUE
)
dn: cn=schema
changetype: modify
add: attributeTypes
attributeTypes: (
  2.16.840.1.113719.1.450.4.103
  NAME 'srvprvFlowStrategy'
  DESC 'Specifies the flow invocation strategy to be used for the
Provisioning Request Definition.'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
  SINGLE-VALUE
)
dn: cn=schema
changetype: modify
add: attributeTypes
attributeTypes: (
  2.16.840.1.113719.1.450.4.104
  NAME 'srvprvLocalizedNames'
  DESC 'Provides set of localized display name strings for the
provisioning web applications, Designers and iManager.'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26
)
dn: cn=schema
changetype: modify
add: attributeTypes
attributeTypes: (
  2.16.840.1.113719.1.450.4.105
  NAME 'srvprvLocalizedDescrs'
  DESC 'Provides set of localized description strings for the
provisioning web applications, Designers and iManager.'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26
)
dn: cn=schema

```

```

changetype: modify
add: attributeTypes
attributeTypes: (
  2.16.840.1.113719.1.450.4.106
  NAME 'srvprvStatus'
  DESC 'Specifies the status of the Provisioning Object. Supported
values will include: Inactive, Active, Template, and Retired.'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26
  SINGLE-VALUE
)
dn: cn=schema
changetype: modify
add: attributeTypes
attributeTypes: (
  2.16.840.1.113719.1.450.4.107
  NAME 'srvprvProcessXML'
  DESC 'XML document representing a Provisioning process definition
including Workflow and Provisioning Action.'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.5
  SINGLE-VALUE
)
dn: cn=schema
changetype: modify
add: attributeTypes
attributeTypes: (
  2.16.840.1.113719.1.450.4.108
  NAME 'srvprvEntityType'
  DESC 'Specifies Directory Abstraction Layer Entity definition type:
P-Public definitions or S-System definitions.'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
  SINGLE-VALUE
)
dn: cn=schema
changetype: modify
add: attributeTypes
attributeTypes: (
  2.16.840.1.113719.1.450.4.109
  NAME 'srvprvRequestXML'
  DESC 'XML document representing the initial request form and its data
bindings'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.5
  SINGLE-VALUE
)
dn: cn=schema
changetype: modify
add: attributeTypes
attributeTypes: (
  2.16.840.1.113719.1.450.4.110
  NAME 'srvprvModified'
  DESC 'Flag to indicate changes to definitions object instances in the
directory model container'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
  SINGLE-VALUE
)

```

```

dn: cn=schema
changetype: modify
add: attributeTypes
attributeTypes: (
  2.16.840.1.113719.1.450.4.111
  NAME 'srvprvEntitlementRef'
  DESC 'Reference to a DirXML-Entitlement'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
  SINGLE-VALUE
)
#-----
#-- Provisioning Configuration Containers
#-----

dn: cn=schema
changetype: modify
add: objectclasses
objectClasses: (
  2.16.840.1.113719.1.450.6.100
  NAME 'srvprvAppConfig'
  DESC 'Container for application configuration objects of the
Provisioning System to which its DirXML-Driver parent connects.'
  SUP top
  STRUCTURAL
  MUST ( cn $ version )
  MAY ( description )
  X-NDS_NAMING ( 'cn' )
  X-NDS_CONTAINMENT ( 'DirXML-Driver' )
)
dn: cn=schema
changetype: modify
add: objectclasses
objectClasses: (
  2.16.840.1.113719.1.450.6.101
  NAME 'srvprvRequestDefs'
  DESC 'Container for Provisioning Request Definitions, the set of
provisionable items to the Web Application run-time.'
  SUP top
  STRUCTURAL
  MUST ( cn )
  MAY ( description )
  X-NDS_NAMING ( 'cn' )
  X-NDS_CONTAINMENT ( 'srvprvAppConfig' )
)
dn: cn=schema
changetype: modify
add: objectclasses
objectClasses: (
  2.16.840.1.113719.1.450.6.102
  NAME 'srvprvWorkflowDefs'
  DESC 'Container for Workflow objects, including design-time
descriptions plus any template or unused flows.'
  SUP top

```

```

    STRUCTURAL
    MUST ( cn )
    MAY ( description )
    X-NDS_NAMING ( 'cn' )
    X-NDS_CONTAINMENT ( 'srvprvAppConfig' )
)
dn: cn=schema
changetype: modify
add: objectclasses
objectClasses: (
    2.16.840.1.113719.1.450.6.103
    NAME 'srvprvResourceDefs'
    DESC 'Container for Provisioning Target definitions, including
design-time descriptions plus any template or unused targets.'
    SUP top
    STRUCTURAL
    MUST ( cn )
    MAY ( description )
    X-NDS_NAMING ( 'cn' )
    X-NDS_CONTAINMENT ( 'srvprvAppConfig' )
)
dn: cn=schema
changetype: modify
add: objectclasses
objectClasses: (
    2.16.840.1.113719.1.450.6.104
    NAME 'srvprvServiceDefs'
    DESC 'Container for Service Definition objects, which wrap Web
Services called by Workflows.'
    SUP top
    STRUCTURAL
    MUST ( cn )
    MAY ( description )
    X-NDS_NAMING ( 'cn' )
    X-NDS_CONTAINMENT ( 'srvprvAppConfig' )
)
dn: cn=schema
changetype: modify
add: objectclasses
objectClasses: (
    2.16.840.1.113719.1.450.6.105
    NAME 'srvprvDirectoryModel'
    DESC 'Container for Directory Abstraction Layer meta-level objects,
selected contents of the directory to be exposed by the Identity
Portlets and Web Applications.'
    SUP top
    STRUCTURAL
    MUST ( cn )
    MAY ( description $ srvprvModified )
    X-NDS_NAMING ( 'cn' )
    X-NDS_CONTAINMENT ( 'srvprvAppConfig' )
)
dn: cn=schema
changetype: modify

```

```

add: objectclasses
objectClasses: (
  2.16.840.1.113719.1.450.6.106
  NAME 'srvprvAppDefs'
  DESC 'Container for configuration objects used to initialise the
Provisioning run-time environment, such as themes for the Identity
Portal.'
  SUP top
  STRUCTURAL
  MUST ( cn )
  MAY ( description )
  X-NDS_NAMING ( 'cn' )
  X-NDS_CONTAINMENT ( 'srvprvAppConfig' )
)
dn: cn=schema
changetype: modify
add: objectclasses
objectClasses: (
  2.16.840.1.113719.1.450.6.111
  NAME 'srvprvEntityDefs'
  DESC 'Container for Directory Abstraction Layer Entity defintions, to
be exposed by the Identity Portlets and Web Applications.'
  SUP top
  STRUCTURAL
  MUST ( cn )
  MAY ( description )
  X-NDS_NAMING ( 'cn' )
  X-NDS_CONTAINMENT ( 'srvprvDirectoryModel' )
)
dn: cn=schema
changetype: modify
add: objectclasses
objectClasses: (
  2.16.840.1.113719.1.450.6.112
  NAME 'srvprvRelationshipDefs'
  DESC 'Container for Directory Abstraction Layer Relationship
definitions, to be exposed by the Identity Portlets and Web
Applications.'
  SUP top
  STRUCTURAL
  MUST ( cn )
  MAY ( description )
  X-NDS_NAMING ( 'cn' )
  X-NDS_CONTAINMENT ( 'srvprvDirectoryModel' )
)
dn: cn=schema
changetype: modify
add: objectclasses
objectClasses: (
  2.16.840.1.113719.1.450.6.113
  NAME 'srvprvChoiceDefs'
  DESC 'Container for Directory Abstraction Layer Choice definitions,
to be exposed by the Identity Portlets and Web Applications.'
  SUP top

```

```

    STRUCTURAL
    MUST ( cn )
    MAY ( description )
    X-NDS_NAMING ( 'cn' )
    X-NDS_CONTAINMENT ( 'srvprvDirectoryModel' )
)
#### Provisioning Configuration Object Classes
dn: cn=schema
changetype: modify
add: objectclasses
objectClasses: (
    2.16.840.1.113719.1.450.6.107
    NAME 'srvprvRequest'
    DESC 'Exposes one provisionable item to be granted or revoked,
including the workflow process which defines the run-time aspects of
the Workflow and Provisioning Target.'
    SUP top
    STRUCTURAL
    MUST ( cn $ srvprvStatus $ srvprvFlowStrategy $ srvprvGrant $
srvprvRevoke $ srvprvCategoryKey $ srvprvLocalizedNames $
srvprvLocalizedDescrs )
    MAY ( description $ srvprvEntitlementRef $ XmlData $ srvprvRequestXML
$ srvprvProcessXML )
    X-NDS_NOT_CONTAINER '1'
    X-NDS_NAMING ( 'cn' )
    X-NDS_CONTAINMENT ( 'srvprvRequestDefs' )
)
dn: cn=schema
changetype: modify
add: objectclasses
objectClasses: (
    2.16.840.1.113719.1.450.6.108
    NAME 'srvprvWorkflow'
    DESC 'Defines the network of activites including traversal conditions
to be executed in order to obtain approval for a provisioning action.'
    SUP top
    STRUCTURAL
    MUST ( cn $ srvprvLocalizedNames $ srvprvLocalizedDescrs )
    MAY ( description $ XmlData )
    X-NDS_NOT_CONTAINER '1'
    X-NDS_NAMING ( 'cn' )
    X-NDS_CONTAINMENT ( 'srvprvWorkflowDefs' )
)
dn: cn=schema
changetype: modify
add: objectclasses
objectClasses: (
    2.16.840.1.113719.1.450.6.109
    NAME 'srvprvResource'
    DESC 'Defines the set of directory assignments to execute for a
provisioning fulfillment operation (either Grant or Revoke).'
    SUP top
    STRUCTURAL
    MUST ( cn $ srvprvLocalizedNames $ srvprvLocalizedDescrs )
)

```

```

    MAY ( description $ srvprvEntitlementRef $ XmlData )
    X-NDS_NOT_CONTAINER '1'
    X-NDS_NAMING ( 'cn' )
    X-NDS_CONTAINMENT ( 'srvprvResourceDefs' )
)
dn: cn=schema
changetype: modify
add: objectclasses
objectClasses: (
    2.16.840.1.113719.1.450.6.110
    NAME 'srvprvService'
    DESC 'Describes how to invoke a specific Web Service from an
Workflow. This includes specification of input and return values.'
    SUP top
    STRUCTURAL
    MUST ( cn )
    MAY ( description $ XmlData )
    X-NDS_NOT_CONTAINER '1'
    X-NDS_NAMING ( 'cn' )
    X-NDS_CONTAINMENT ( 'srvprvServiceDefs' )
)
dn: cn=schema
changetype: modify
add: objectclasses
objectClasses: (
    2.16.840.1.113719.1.450.6.114
    NAME 'srvprvEntity'
    DESC 'Defines a view of selected attributes for defined classes in
the directory, used by the Identity Portlets and other Web Application
components.'
    SUP top
    STRUCTURAL
    MUST ( cn $ srvprvEntityType )
    MAY ( description $ XmlData )
    X-NDS_NOT_CONTAINER '1'
    X-NDS_NAMING ( 'cn' )
    X-NDS_CONTAINMENT ( 'srvprvEntityDefs' )
)
dn: cn=schema
changetype: modify
add: objectclasses
objectClasses: (
    2.16.840.1.113719.1.450.6.115
    NAME 'srvprvRelationship'
    DESC 'Defines relationships between objects in the directory, for use
in the Identity Portlets and other Web Application components.'
    SUP top
    STRUCTURAL
    MUST ( cn )
    MAY ( description $ XmlData )
    X-NDS_NOT_CONTAINER '1'
    X-NDS_NAMING ( 'cn' )
    X-NDS_CONTAINMENT ( 'srvprvRelationshipDefs' )
)

```

```

dn: cn=schema
changetype: modify
add: objectclasses
objectClasses: (
  2.16.840.1.113719.1.450.6.116
  NAME 'srvprvChoice'
  DESC 'Enumeration of values which can be assigned to a particular
attribute, used in a query, etc. for use in the Identity Portlets and
other Web Application components.'
  SUP top
  STRUCTURAL
  MUST ( cn )
  MAY ( description $ XmlData )
  X-NDS_NOT_CONTAINER '1'
  X-NDS_NAMING ( 'cn' )
  X-NDS_CONTAINMENT ( 'srvprvChoiceDefs' )
)
dn: cn=schema
changetype: modify
add: objectclasses
objectClasses: (
  2.16.840.113719.1.450.6.117
  NAME 'srvprvDirectoryModelConfig'
  DESC 'Runtime Directory Abstraction Layer configurarion parameters'
  SUP top
  STRUCTURAL
  MUST ( cn )
  MAY ( description $ XmlData )
  X-NDS_NOT_CONTAINER '1'
  X-NDS_NAMING ( 'cn' )
  X-NDS_CONTAINMENT ( 'srvprvDirectoryModel' )
)
#### User Aux Classes and Attributes
dn: cn=schema
changetype: modify
add: attributeTypes
attributeTypes: (
  2.16.840.1.113719.1.450.4.80
  NAME 'srvprvAssetRef'
  DESC 'Representation of the aggregate asset properties for a named
asset associated to a user via the srvprvAssetRecipientAux class.'
  SYNTAX 2.16.840.1.113719.1.1.5.1.6
)
dn: cn=schema
changetype: modify
add: objectclasses
objectClasses: (
  2.16.840.1.113719.1.450.6.80
  NAME 'srvprvAssetRecipientAux'
  DESC 'Records the provisioning of non-IT assets on a user'
  AUXILIARY
  MAY ( srvprvAssetRef )
)
#-----

```

```
-----  
#-- Web Application Config Class  
#-----  
-----
```

```
dn: cn=schema  
changetype: modify  
add: attributeTypes  
attributeTypes: (2.16.840.1.113719.1.450.4.20 NAME  
'srvprvDefaultTheme' DESC 'The default theme'  
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )  
dn: cn=schema  
changetype: modify  
add: objectclasses  
objectClasses: ( 2.16.840.1.113719.1.450.6.21 NAME  
'srvprvWebAppConfig'  
DESC 'Web Application Config Object'  
SUP top STRUCTURAL MUST (cn) MAY (description $ srvprvDefaultTheme $  
XmlData )  
X-NDS_NOT_CONTAINER '1'  
X-NDS_NAMING 'cn'  
X-NDS_CONTAINMENT ( 'srvprvAppDefs' )  
)
```

```
#-----  
-----
```

```
#-- Theme Branding Structural Class  
#-----  
-----
```

```
dn: cn=schema  
changetype: modify  
add: attributeTypes  
attributeTypes: (  
2.16.840.1.113719.1.450.4.21  
NAME 'srvprvHeaderLogoImage'  
DESC 'Header Logo Primary Image'  
SYNTAX 1.3.6.1.4.1.1466.115.121.1.5  
SINGLE-VALUE  
)  
dn: cn=schema  
changetype: modify  
add: attributeTypes  
attributeTypes: (  
2.16.840.1.113719.1.450.4.22  
NAME 'srvprvHeaderLogoFile'  
DESC 'Header Logo Primary Image File Name'  
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15  
SINGLE-VALUE  
)  
dn: cn=schema  
changetype: modify  
add: attributeTypes  
attributeTypes: (  
2.16.840.1.113719.1.450.4.23  
NAME 'srvprvHeaderLogoLastMod'  
DESC 'Header Logo Primary Last Modified'
```

```

    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
    SINGLE-VALUE
  )
dn: cn=schema
changetype: modify
add: attributeTypes
attributeTypes: (
  2.16.840.1.113719.1.450.4.24
  NAME 'srvprvHeaderLogo2Image'
  DESC 'Header Logo Secondary Image'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.5
  SINGLE-VALUE
)
dn: cn=schema
changetype: modify
add: attributeTypes
attributeTypes: (
  2.16.840.1.113719.1.450.4.25
  NAME 'srvprvHeaderLogo2File'
  DESC 'Header Logo Secondary Image File Name'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 |
  SINGLE-VALUE
)
dn: cn=schema
changetype: modify
add: attributeTypes
attributeTypes: (
  2.16.840.1.113719.1.450.4.26
  NAME 'srvprvHeaderLogo2LastMod'
  DESC 'Header Logo Secondary Last Modified'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
  SINGLE-VALUE
)
dn: cn=schema
changetype: modify
add: attributeTypes
attributeTypes: (
  2.16.840.1.113719.1.450.4.27
  NAME 'srvprvHeaderTextureImage'
  DESC 'Header Texture Image'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.5
  SINGLE-VALUE
)
dn: cn=schema
changetype: modify
add: attributeTypes
attributeTypes: (
  2.16.840.1.113719.1.450.4.28
  NAME 'srvprvHeaderTextureFile'
  DESC 'Header Texture File Name'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
  SINGLE-VALUE
)
dn: cn=schema

```

```

changetype: modify
add: attributeTypes
attributeTypes: (
  2.16.840.1.113719.1.450.4.29
  NAME 'srvprvHeaderTextureLastMod'
  DESC 'Header Texture Last Modified'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
  SINGLE-VALUE
)
dn: cn=schema
changetype: modify
add: attributeTypes
attributeTypes: (
  2.16.840.1.113719.1.450.4.30
  NAME 'srvprvHeaderFillerImage'
  DESC 'Header Filler Image'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.5
  SINGLE-VALUE
)
dn: cn=schema
changetype: modify
add: attributeTypes
attributeTypes: (
  2.16.840.1.113719.1.450.4.31
  NAME 'srvprvHeaderFillerFile'
  DESC 'Header Filler File Name'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
  SINGLE-VALUE
)
dn: cn=schema
changetype: modify
add: attributeTypes
attributeTypes: (
  2.16.840.1.113719.1.450.4.32
  NAME 'srvprvHeaderFillerLastMod'
  DESC 'Header Filler Last Modified'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
  SINGLE-VALUE
)
dn: cn=schema
changetype: modify
add: attributeTypes
attributeTypes: (
  2.16.840.1.113719.1.450.4.33
  NAME 'srvprvLoginImage'
  DESC 'Login Image'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.5
  SINGLE-VALUE
)
dn: cn=schema
changetype: modify
add: attributeTypes
attributeTypes: (
  2.16.840.1.113719.1.450.4.34

```

```

    NAME 'srvprvLoginFile'
    DESC 'Login File Name'
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
    SINGLE-VALUE
  )
dn: cn=schema
changetype: modify
add: attributeTypes
attributeTypes: (
  2.16.840.1.113719.1.450.4.35
  NAME 'srvprvLoginLastMod'
  DESC 'Login Last Modified'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
  SINGLE-VALUE
)
dn: cn=schema
changetype: modify
add: attributeTypes
attributeTypes: (
  2.16.840.1.113719.1.450.4.36
  NAME 'srvprvLoginSmallImage'
  DESC 'Login Small Image'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.5
  SINGLE-VALUE
)
dn: cn=schema
changetype: modify
add: attributeTypes
attributeTypes: (
  2.16.840.1.113719.1.450.4.37
  NAME 'srvprvLoginSmallFile'
  DESC 'Login Small File Name'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
  SINGLE-VALUE
)
dn: cn=schema
changetype: modify
add: attributeTypes
attributeTypes: (
  2.16.840.1.113719.1.450.4.38
  NAME 'srvprvLoginSmallLastMod'
  DESC 'Login Small Last Modified'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
  SINGLE-VALUE
)
dn: cn=schema
changetype: modify
add: attributeTypes
attributeTypes: (
  2.16.840.1.113719.1.450.4.39
  NAME 'srvprvNavColor'
  DESC 'Navigation Color'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
  SINGLE-VALUE
)

```

```

)
dn: cn=schema
changetype: modify
add: attributeTypes
attributeTypes: (
  2.16.840.1.113719.1.450.4.40
  NAME 'srvprvNavColorLastMod'
  DESC 'Navigation Color Last Modified'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
  SINGLE-VALUE
)
dn: cn=schema
changetype: modify
add: attributeTypes
attributeTypes: (
  2.16.840.1.113719.1.450.4.41
  NAME 'srvprvNavBckgrColor'
  DESC 'Navigation Background Color'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
  SINGLE-VALUE
)
dn: cn=schema
changetype: modify
add: attributeTypes
attributeTypes: (
  2.16.840.1.113719.1.450.4.42
  NAME 'srvprvNavBckgrColorLastMod'
  DESC 'Navigation Background Color Last Modified'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
  SINGLE-VALUE
)
dn: cn=schema
changetype: modify
add: objectclasses
objectClasses: (
  2.16.840.1.113719.1.450.6.20
  NAME 'srvprvTheme'
  DESC 'Theme Object'
  SUP top STRUCTURAL MUST (cn) MAY (description $
    srvprvHeaderLogoImage $
  srvprvHeaderLogoFile $ srvprvHeaderLogoLastMod $
    srvprvHeaderLogo2Image $
  srvprvHeaderLogo2File $ srvprvHeaderLogo2LastMod $
    srvprvHeaderTextureImage $
  srvprvHeaderTextureFile $ srvprvHeaderTextureLastMod $
    srvprvHeaderFillerImage $
  srvprvHeaderFillerFile $ srvprvHeaderFillerLastMod $
    srvprvLoginImage $ srvprvLoginFile $
  srvprvLoginLastMod $
    srvprvLoginSmallImage $
  srvprvLoginSmallFile $ srvprvLoginSmallLastMod $
    srvprvNavColor $ srvprvNavColorLastMod
  $
    srvprvNavBckgrColor $

```

```

srvprvNavBckgrColorLastMod )
  X-NDS_NOT_CONTAINER '1'
  X-NDS_CONTAINMENT ( 'srvprvAppDefs' )
  X-NDS_NAMING 'cn'
)
#-----
#-----
#-- Attributes, objects, and containers for Proxy, Delegatee and User
availability,
#-----
#-----
dn: cn=schema
changetype: modify
add: attributeTypes
attributeTypes: (
  2.16.840.1.113719.1.450.4.120
  NAME 'srvprvAssignFromUser'
  DESC 'User subjects of a proxy or delegatee assignment'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
)
dn: cn=schema
changetype: modify
add: attributeTypes
attributeTypes: (
  2.16.840.1.113719.1.450.4.121
  NAME 'srvprvAssignFromGroup'
  DESC 'Group subjects of a proxy or delegatee assignment'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
)
dn: cn=schema
changetype: modify
add: attributeTypes
attributeTypes: (
  2.16.840.1.113719.1.450.4.122
  NAME 'srvprvAssignFromContainer'
  DESC 'Container subjects of a proxy or delegatee assignment'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
)
dn: cn=schema
changetype: modify
add: attributeTypes
attributeTypes: (
  2.16.840.1.113719.1.450.4.123
  NAME 'srvprvAssignToUser'
  DESC 'The User targets of a proxy or delegatee assignment'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
)
dn: cn=schema
changetype: modify
add: attributeTypes
attributeTypes: (
  2.16.840.1.113719.1.450.4.124
  NAME 'srvprvAssignToRelationship'
  DESC 'A target relationship of a delegatee assignment'
)

```

```

    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
    SINGLE-VALUE
  )
dn: cn=schema
changetype: modify
add: attributeTypes
attributeTypes: (
  2.16.840.1.113719.1.450.4.125
  NAME 'srvprvAssignExpiration'
  DESC 'Time at which a proxy or delegatee assignment expires'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.24
  SINGLE-VALUE
)
dn: cn=schema
changetype: modify
add: attributeTypes
attributeTypes: (
  2.16.840.1.113719.1.450.4.126
  NAME 'srvprvRequestDefName'
  DESC 'The provisioning request definition name associated with a
delegatee definition.'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
)
dn: cn=schema
changetype: modify
add: objectclasses
objectClasses: (
  2.16.840.1.113719.1.450.6.120
  NAME 'srvprvProxyDefs'
  DESC 'Container for proxy definitions.'
  SUP top
  STRUCTURAL
  MUST ( cn )
  MAY ( description )
  X-NDS_NAMING ( 'cn' )
  X-NDS_CONTAINMENT ( 'srvprvAppConfig' )
)
dn: cn=schema
changetype: modify
add: objectclasses
objectClasses: (
  2.16.840.1.113719.1.450.6.121
  NAME 'srvprvDelegateeDefs'
  DESC 'Container for delegatee definitions.'
  SUP top
  STRUCTURAL
  MUST ( cn )
  MAY ( description )
  X-NDS_NAMING ( 'cn' )
  X-NDS_CONTAINMENT ( 'srvprvAppConfig' )
)
dn: cn=schema
changetype: modify
add: objectclasses

```

```

objectClasses: (
  2.16.840.1.113719.1.450.6.122
  NAME 'srvprvProxyAssignment'
  DESC 'Proxy assignment definition'
  SUP top
  STRUCTURAL
  MUST ( cn $ srvprvAssignToUser )
  MAY ( description $ srvprvAssignFromUser $ srvprvAssignFromGroup $
srvprvAssignFromContainer $ srvprvAssignExpiration )
  X-NDS_NAMING ( 'cn' )
  X-NDS_CONTAINMENT ( 'srvprvProxyDefs' )
)
dn: cn=schema
changetype: modify
add: objectclasses
objectClasses: (
  2.16.840.1.113719.1.450.6.123
  NAME 'srvprvDelegateeAssignment'
  DESC 'Delegatee assignment definition'
  SUP top
  STRUCTURAL
  MUST cn
  MAY ( srvprvRequestDefName $ description $ srvprvAssignFromUser $
srvprvAssignFromGroup $ srvprvAssignFromContainer $ srvprvAssignToUser
$ srvprvAssignToRelationship $ srvprvAssignExpiration )
  X-NDS_NAMING ( 'cn' )
  X-NDS_CONTAINMENT ( 'srvprvDelegateeDefs' )
)
##### DO NOT DELETE THIS LINE #####
#####

```

# Konfigurieren des Anwendungsarchivs

# B

In diesem Anhang werden die erweiterten Einstellungen beschrieben, die nur durch Bearbeiten der WAR-Datei für die Benutzeranwendung konfiguriert werden können. Es werden folgende Themen erläutert:

- [Abschnitt B.1, „Allgemeines zur WAR-Datei der Benutzeranwendung“](#), auf Seite 391
- [Abschnitt B.2, „Einstellung der Sitzungszeitüberschreitung“](#), auf Seite 391

## B.1 Allgemeines zur WAR-Datei der Benutzeranwendung

Die Identity Manager-Benutzeranwendung ist in einer J2EE-konformen WAR-Datei komprimiert (WAR = Web Application Archive). Die WAR-Datei der Benutzeranwendung enthält Java-Klassen und XML-Dateien, die das Laufzeitverhalten der Anwendung steuern. Generell sollte die WAR-Datei nicht geändert werden. In seltenen Fällen müssen Sie die WAR-Datei möglicherweise doch öffnen und Änderungen darin vornehmen, um das Verhalten der Anwendung Ihren Erfordernissen gemäß anzupassen.

---

**Hinweis:** Für die Ausführungen in diesem Anhang wird vorausgesetzt, dass Sie mit J2EE-Konzepten und -Verfahrensweisen vertraut sind. Wenn Sie nicht sicher sind, wie Sie Änderungen in der WAR-Datei vornehmen sollen, lesen Sie die relevanten Abschnitte in der J2EE-Dokumentation.

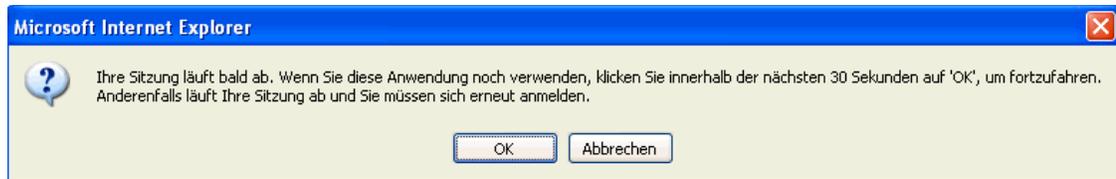
---

## B.2 Einstellung der Sitzungszeitüberschreitung

Damit der Server nicht mit inaktiven Sitzungen überladen wird, kann man in der Identity Manager-Benutzeranwendung ein Zeitlimit für Benutzersitzungen definieren, die über einen bestimmten Zeitraum hinweg inaktiv bleiben. Das Standard-Zeitüberschreitungsintervall beträgt 10 Minuten. Sie können den Standardwert in der Datei *web.xml* ändern. Die Datei befindet sich im Ordner WEB-INF in der WAR-Datei der Benutzeranwendung.

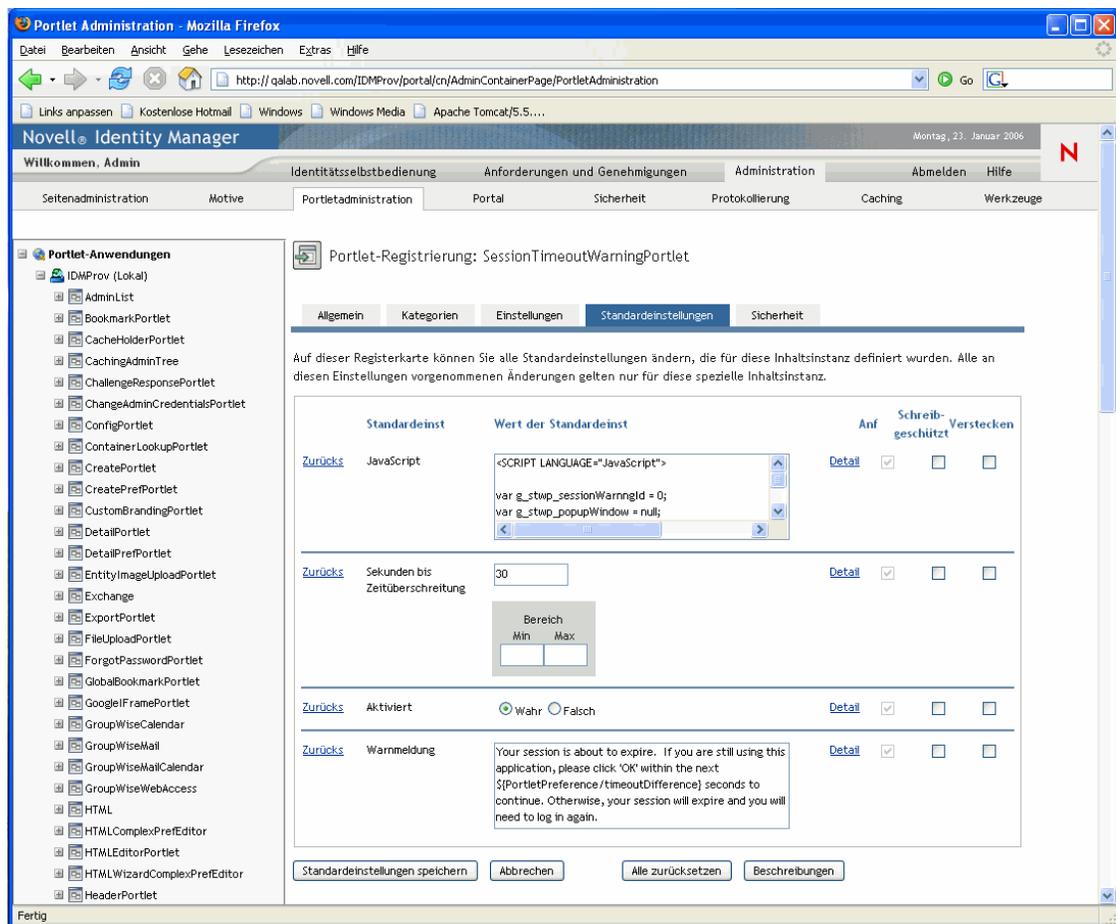
**Bearbeiten des Werts für die Sitzungszeitüberschreitung** Die Datei „web.xml“ im WAR-Archiv enthält ein Element mit Namen `<session-timeout>` (befindet sich unter dem `<session-config>`-Element), das angibt, wie lange eine Sitzung inaktiv sein kann, bevor sie das Zeitlimit überschreitet. Wenn Sie den Wert für die Sitzungszeitüberschreitung ändern möchten, müssen Sie dieses Element bearbeiten. Der Wert wird in Minuten angegeben.

**Steuerung des Verhaltens der Warnmeldung** Standardmäßig zeigt die Identity Manager-Benutzeranwendung immer dann eine Warnmeldung an, wenn bei einer Benutzersitzung eine Zeitüberschreitung bevorsteht.



Reagiert der Benutzer durch Klicken auf „OK“ nicht auf die Meldung, wird die Sitzung wegen Zeitüberschreitung abgebrochen. Die Warnmeldung wird standardmäßig aktiviert. Sie können sie bei Bedarf deaktivieren. Zusätzlich können Sie angeben, wie viel Zeit der Benutzer hat, um auf die Warnmeldung zu reagieren.

Wenn Sie das Verhalten der Warnmeldung ändern möchten, müssen Sie das *SessionTimeoutWarningPortlet* konfigurieren. Dazu ist eine Bearbeitung der Portlet-Einstellungen bei der Portlet-Registrierung erforderlich, wie nachfolgend dargestellt:



Wenn Sie angeben möchten, wie viel Zeit der Benutzer hat, um auf die Warnmeldung zu reagieren, ändern Sie den Wert *Sekunden bis Zeitüberschreitung*. Wenn Sie die Warnmeldung deaktivieren möchten, klicken Sie neben *Aktiviert* auf *Falsch*. Wenn Sie die Änderungen vorgenommen haben, klicken Sie auf *Standard-einstellungen speichern*.