



# DFB-MEDIEN

<b>Freigabemitteilung Nr. 5</b>				<b>Version: 3.14</b>
<b>System:</b>		<b>DFBnet</b>		
<b>Speicherpfad/Dokument:</b>		<b>101203_DFBnet-Benutzer_3.14_Freigabemitteilung.doc</b>		
	<b>Erstellt:</b>	<b>Letzte Änderung:</b>	<b>Geprüft:</b>	<b>Freigabe:</b>
<b>Datum:</b>	03.12.2010	06.12.2010	06.12.2010	06.12.2010
<b>Version:</b>	V 1.0	V 1.1	V 1.1	V 1.2
<b>Name:</b>	Gabi Pach	Gabi Pach	Kai Engelke Matthias Knebel etra Smerzinski	Petra Smerzinski

© 2010 DFB-Medien GmbH & Co. KG

Alle Texte und Abbildungen wurden mit größter Sorgfalt erarbeitet, dennoch können etwaige Fehler nicht ausgeschlossen werden. Eine Haftung der DFB-Medien, gleich aus welchem Rechtsgrund, für Schäden oder Folgeschäden, die aus der An- und Verwendung der in diesem Dokument gegebenen Informationen entstehen können, ist ausgeschlossen.

Das Dokument ist urheberrechtlich geschützt. Die Weitergabe sowie die Veröffentlichung dieser Unterlage sind ohne die ausdrückliche und schriftliche Genehmigung der DFB-Medien nicht gestattet. Zuwiderhandlungen verpflichten zu Schadensersatz. Alle Rechte für den Fall der Patenterteilung oder der GM-Eintragung vorbehalten.

Die in diesem Dokument verwendeten Soft- und Hardwarebezeichnungen sind in den meisten Fällen auch eingetragene Warenzeichen und unterliegen als solche den gesetzlichen Bestimmungen.



## Zum Inhalt

<b>1. Ziel des Dokumentes .....</b>	<b>3</b>
<b>2. Funktionale Erweiterungen .....</b>	<b>3</b>
2.1 Benutzer bearbeiten.....	3
2.1.1 Suchstrategien .....	3
2.1.2 Starten einer Suchanfrage .....	5
2.1.3 Aufbau der Trefferliste.....	6
2.2 Passwortänderung nach Anmeldung erforderlich.....	7
2.2.1 Passwort durch den Benutzer erneuern .....	9
2.3 Passwort vergessen.....	10
2.4 Benutzererkennung kopieren .....	10
2.4.1 Regeln und Einschränkungen zum Kopieren von Benutzerkennungen .....	13
2.5 Benutzer suchen .....	15
2.5.1 Auswahl der Strukturelemente .....	16
2.5.2 Suchstrategien .....	19
2.6 Detail einer Benutzererkennung.....	20
2.7 Sicherheitsstufen / Policies .....	23
2.7.1 Beschreibung der Policy .....	23
2.7.2 Konkrete Ausprägung der Policies in Sicherheitsstufen .....	25
2.7.3 Verwaltung und Zuweisung der Sicherheitsstufen.....	25
2.7.4 Sicherheitsstufen ansehen.....	25
2.7.5 Aktivierung der Sicherheitsstufen .....	27
<b>3. Abbildungsverzeichnis .....</b>	<b>28</b>
<b>4. Bearbeitungshistorie .....</b>	<b>28</b>



## 1. Ziel des Dokumentes

Das nachfolgende Dokument beschreibt die funktionalen Erweiterungen der Benutzerverwaltung in der Version 3.14 und gilt in seiner sprachlichen Fassung für Frauen und Männer gleichermaßen.

## 2. Funktionale Erweiterungen

### 2.1 Benutzer bearbeiten

#### 2.1.1 Suchstrategien

Um Benutzerkennungen anlegen oder bearbeiten zu können, muss vorab nach der entsprechenden Benutzerkennung gesucht werden. Die Suchstrategien für Personenkennungen wurden geringfügig überarbeitet und die Suchmaske um das Attribut <Benutzer aktiv> erweitert, das sich als Auswahlliste präsentiert und die Werte <leer> (default), <Ja> und <Nein> beinhaltet.

Unterhalb des Eingabefeldes für die Benutzerkennung wurde eine Checkbox mit der Bezeichnung <bei der Suche mit ODER verknüpfen> positioniert. Hat der Anwender in das Eingabefeld <Benutzerkennung> und in das Eingabefeld <Name> eine Zeichenkette eingegeben und zusätzlich die Checkbox markiert, so werden die Suchattribute <Benutzerkennung> und <Name> mit einem logischen ODER verknüpft. Andernfalls werden die genannten Suchattribute mit einem logischen UND verbunden. Alle zusätzlich eingegebenen Suchkriterien wie beispielsweise das Geburtsdatum oder der Status werden wiederum mit einem UND verkettet.

Bitte beachten Sie bei der Auswahl der Suchstrategie, dass eine UND-Verknüpfung die mögliche Treffermenge immer reduziert, währenddessen eine ODER-Verknüpfung die Anzahl der Treffer erhöht. Die nachfolgenden Beispiele verdeutlichen die alternativen Suchstrategien.

#### **Beispiel 1:**

<b>Benutzerkennung:</b>	9912
<b>Name:</b>	müller
<b>Suchstrategie:</b>	ODER-Verknüpfung
<b>Ergebnis:</b>	Es werden alle Benutzerkennungen gefunden, deren Kennung mit <9912> oder deren Name mit <müller> beginnen.



DFB-MEDIEN

**Beispiel 2:**

**Benutzerkennung:** 9912  
**Name:** meier  
**Suchstrategie:** UND-Verknüpfung  
**Ergebnis:** Es werden alle Benutzerkennungen gefunden, deren Kennung mit <9912> und deren Name mit <meier> beginnen.

**Beispiel 3:**

**Benutzerkennung:** 9912  
**Name:** schulze  
**Suchstrategie:** ODER-Verknüpfung  
**Geburtsdatum:** 01.01.1980  
**Status:** aktiv  
**Ergebnis:** Es werden im ersten Schritt alle Benutzerkennungen gefunden, deren Kennung mit <9912> oder deren Name mit <schulze> beginnen. Ausgehend von dieser Treffermenge werden alle Benutzerkennungen angezeigt, bei denen das Geburtsdatum den Wert <01.01.1980> aufweist und die aktiv sind.



Die nachfolgende Grafik zeigt die überarbeitete Suchmaske.

Abbildung 1 – Benutzer bearbeiten – Suchmaske

## 2.1.2 Starten einer Suchanfrage

Die Pflichteingaben zum Starten einer Suchanfrage bei Personenkennungen wurden verändert. Die Mindestanzahl der einzugebenden Zeichen bei dem Suchattribut <Name> wurde von drei auf zwei reduziert. Darüber hinaus besteht die Möglichkeit, ausschließlich über ein exaktes Geburtsdatum zu suchen.

Zum Starten einer Suchanfrage geben Sie entweder:

- eine Benutzerkennung (min. drei Zeichen) oder
- einen Namen (min. zwei Zeichen) oder
- ein exaktes Geburtsdatum

ein.



### 2.1.3 Aufbau der Trefferliste

Die Bearbeitungsicons in der Trefferliste haben sich in ihrer Symbolik nicht verändert, wurden aber bezüglich ihrer Farbgebung modifiziert, sodass sie sich jetzt besser voneinander unterscheiden.

Icon	Bedeutung
	Benutzer bearbeiten
	Benutzerdetails anzeigen
	Benutzererkennung umbenennen
	Benutzererkennung anlegen

Der Status einer Benutzererkennung (aktiv oder inaktiv) wird in der ganz rechten Spalte mit der Bezeichnung <AK> (Abkürzung für aktiv) angezeigt. Das grüne Häkchen bedeutet, dass der Benutzer aktiv ist, währenddessen das rote Kreuz besagt, dass der Benutzer inaktiv ist. Wird zu einem Eintrag in der Trefferliste kein Symbol angezeigt, so handelt es sich um eine Person oder um einen Verein, die/der noch keine Benutzererkennung haben.

The screenshot shows the 'Benutzerverwaltung' interface. The search filters are: Kennungstyp: Personenerkennung, Benutzererkennung: micky, and 'bei der Suche mit ODER verknüpfen' is unchecked. The results table is as follows:

Benutzererkennung	Nachname	Vorname	Geburtsdatum	AK
micky	Micky	Mouse	01.01.2000	AK

Page 1/1 (1 Treffer insgesamt)

Abbildung 2 – Benutzer bearbeiten – Trefferliste



DFB-MEDIEN

## 2.2 Passwortänderung nach Anmeldung erforderlich

In der Benutzerverwaltung können die Administratoren die Passwörter der Benutzer ändern. In Abhängigkeit der funktionalen Rechte und der Datenrechte, die der Administrator selbst inne hat, ist die Eingabe des alten Kennwortes erforderlich oder nicht.

Vergibt ein Administrator ein Passwort, so wird dieses zwar verschlüsselt in der Datenbank gespeichert, dennoch kennen die Administratoren die Kennwörter. Zwar hat jeder Anwender die theoretische Möglichkeit sein Kennwort zu ändern, tut dies aber nicht ohne Not.

Aus datenschutzrechtlichen Gründen ist dieses Vorgehen nicht vertretbar, so dass die Benutzerverwaltung dahingehend erweitert wurde, dass die Passwörterneuerung durch den Benutzer selbst quasi „erzungen“ werden kann. Eine Passwörterneuerung ist immer dann erforderlich, wenn ein Kennwort „ungültig“ wird bzw. abgelaufen ist.

Die Box <Kennungsinformationen> im Dialog <UA-AC 010 – Benutzerdaten bearbeiten> wurde um die Check-Box mit dem Titel <Passwortänderung nach Anmeldung erforderlich> erweitert. Per Default ist die Check-Box nicht markiert. Diese Check-Box ist nur aktiv, wenn der Administrator einerseits mindestens über dieselben funktionalen Rechte und Datenrechte verfügt wie die Benutzererkennung, die er bearbeitet und andererseits das Merkmal <Passwortänderung erlaubt> den Wert <Ja> aufweist.

Ändert der Administrator den Wert des Feldes <Passwortänderung erlaubt> von <Ja> auf <Nein>, wird die Check-Box inaktiv. Somit ist gewährleistet, dass eine Passwörterneuerung nur dann eingefordert werden kann, wenn die Passwortänderung grundsätzlich erlaubt ist.

Sind alle Bedingungen erfüllt, kann der Administrator die Check-Box <Passwortänderung nach Anmeldung erforderlich> markieren. Mit Speicherung der Daten wird das Kennwort des Benutzers auf „abgelaufen“ gesetzt werden. An der Benutzeroberfläche sind in den Read-Only Datenfeldern <Passwort abgelaufen/am> die Werte <Ja> und der Zeitpunkt der Speicherung <Datum und Uhrzeit> zu sehen. Die Check-Box <Passwortänderung nach Anmeldung erforderlich> ist nicht mehr markiert.



**Benutzerverwaltung** UA-AC 010

Benutzerkennung: micky

**Kennungsinformationen**

Benutzer aktiv: ja

Passwortänderung erlaubt: ja

Passwort abgelaufen / am: nein

Passwortänderung:  nach Anmeldung erforderlich

**Persönliche Angaben**

Name: Micky, Geschlecht: , Nationalität: Deutschland, Geburtsdatum: 01.01.2000

**Adress- und Kontaktdaten**

Straße: Lister Straße 18, PLZ / Ort: 30163 Hannover, Land: Deutschland

Zurück Übernehmen Speichern & Weiter

Abbildung 3 – Passwortänderung nach Anmeldung erforderlich 1

**Benutzerverwaltung** UA-AC 010

Benutzerkennung: micky

**Kennungsinformationen**

Benutzer aktiv: ja

Passwortänderung erlaubt: ja

Passwort abgelaufen / am: nein

Passwortänderung:  nach Anmeldung erforderlich

**Persönliche Angaben**

Name: Micky, Geschlecht: , Nationalität: Deutschland, Geburtsdatum: 01.01.2000

**Adress- und Kontaktdaten**

Straße: Lister Straße 18, PLZ / Ort: 30163 Hannover, Land: Deutschland

Zurück Übernehmen Speichern & Weiter

Abbildung 4 – Passwortänderung nach Anmeldung erforderlich 2



Ist das Passwort abgelaufen, kann der Wert des Datenfeldes <Passwortänderung erlaubt> nicht verändert werden. Erst wenn der Benutzer sein Passwort erneuert hat oder der Administrator über die Benutzerverwaltung ein neues Passwort vergeben hat, ist die Auswahlliste wieder editierbar und das Kennzeichen <Passwort abgelaufen> wird zurückgesetzt.

The screenshot shows the 'Benutzerverwaltung' (User Management) interface. The user 'micky' is selected. The 'Kennungsinformationen' (Identification Information) section is highlighted with a red circle. It contains the following fields:

Benutzer aktiv	<input type="text" value="ja"/>
Passwortänderung erlaubt	<input type="text" value="ja"/>
Passwort abgelaufen / am	<input type="text" value="ja"/> 30.11.2010 19:27:27
Passwortänderung	<input type="checkbox"/> nach Anmeldung erforderlich

The 'Persönliche Angaben' (Personal Information) section shows:

Name	Micky	Geschlecht	
Vorname	Mouse	Nationalität	Deutschland
Geburtsdatum	01.01.2000		

The 'Adress- und Kontaktdaten' (Address and Contact Data) section shows:

Straße	Lister Straße 18	Telefon privat	
PLZ / Ort	30163 Hannover	Telefon geschäftlich	
Ortsteil		Mobil	
Land	Deutschland	Fax	
Firma		E-Mail	

Buttons at the bottom include 'Zurück', 'Übernehmen', and 'Speichern & Weiter'.

Abbildung 5 – Passwortänderung nach Anmeldung erforderlich 3

## 2.2.1 Passwort durch den Benutzer erneuern

Meldet sich ein Benutzer an DFBnet SpielPLUS an wird überprüft, ob das Kennwort gültig ist oder nicht. Stellt der „Login-Service“ nach der erfolgreichen Anmeldung fest, dass das Kennwort abgelaufen – also nicht mehr gültig – ist, wird der Dialog zum Ändern des Passworts angezeigt werden. Oberhalb des Panels erscheint folgende Hinweisbox:

Ihr Passwort ist entweder nicht mehr gültig oder Sie haben sich ein temporäres Passwort per Mail angefordert. In beiden Fällen müssen Sie Ihr Passwort erneuern. Bitte vergeben Sie ein neues Passwort, das sich von dem alten Passwort unterscheiden muss. Anschließend können Sie die DFBnet Module nutzen.

Ändert der Anwender erfolgreich sein Passwort, so ist dieses wieder gültig. Vergibt der Anwender ein neues Kennwort, so muss sich das neue Kennwort von dem alten Kennwort unterscheiden.



The screenshot shows the DFBnet login interface. At the top left is the DFBnet logo. The main header features the 'SpielPLUS' logo and a soccer ball on a green field. Below the header, there is a navigation menu on the left with options like 'Integrations-System', 'Anmelden', 'Service', 'Hilfsangebote', 'Passwort vergessen', and 'Impressum'. The main content area is titled 'Anmeldung' and contains a 'Fehlermeldungen' section with a red error message: 'Ihr Passwort ist entweder nicht mehr gültig oder Sie haben sich ein temporäres Passwort per Mail angefordert. In beiden Fällen müssen Sie ein Ihr Passwort erneuern. Bitte vergeben Sie ein neues Passwort, das sich von dem alten Passwort unterscheiden muss. Anschließend können Sie die DFBnet Module nutzen.' Below this is a form titled 'Bitte geben Sie ihr altes und ihr neues Passwort ein' with three input fields for 'Altes Passwort:', 'Neues Passwort:', and 'Neues Passwort bestätigen:'. A 'Speichern' button is located at the bottom right of the form.

Abbildung 6 – Passwort abgelaufen

**Wichtiger Hinweis:** Die Überprüfung findet bislang nur bei den SpielPLUS Komponenten statt. Für die ORGA-Module, die Schiedsrichteranzetzung, den Vereinsmeldebogen, die Ergebnismeldung (IVR/SMS), die Postfächer, das Forum und Cognos ist die Überprüfung noch nicht aktiviert.

## 2.3 Passwort vergessen

Über die Funktion <Passwort vergessen> kann sich ein Anwender ein neues Passwort anfordern. In diesem Fall wird ein sechsstelliges Passwort generiert und dem Anwender per Mail zugestellt. Mit der Version 3.14 hat dieses Passwort nur noch einen temporären Charakter. Meldet sich der Anwender mit dem generierten Passwort an, wird er aufgefordert, sein Passwort zu erneuern (siehe dazu Abbildung 6 – Passwort abgelaufen).

## 2.4 Benutzerkennung kopieren

Die Administration einer Benutzerkennung kann unter Umständen aufwändig sein, wenn viele Rollen und Datenrechte zugewiesen werden müssen. Aus diesem Grund wird mit der Version 3.14 eine Funktion zum Kopieren von Benutzerkennungen angeboten.

Wie bei jedem Kopiervorgang gibt es eine Quelle und ein Ziel. Voraussetzung für den Kopiervorgang, ist, dass die Benutzerkennung, zu der kopiert werden soll, bereits existiert.



Der eigentliche Kopiervorgang vollzieht sich in mehreren Schritten. Im ersten Schritt sucht der Administrator im Dialog <Benutzer bearbeiten> nach der Benutzerkennung, die er kopieren möchte. Anschließend wählt der Administrator in der Trefferliste das Ansichtssymbol (Benutzerdetails anzeigen) der gewünschten Benutzerkennung (Quelle) aus und verzweigt somit in die Detailansicht. Dieser Navigationsschritt dient als zusätzliche Kontrollfunktion.

The screenshot shows the 'Benutzerverwaltung' (User Management) interface. The user 'pach' is selected. The interface includes a sidebar with navigation options like 'Benutzer bearbeiten', 'Benutzer suchen', and 'Rollen ansehen'. The main content area displays user information, personal data, and contact details. At the bottom, there is a table of roles and permissions. The 'Kopieren' button is circled in red.

Rolle	Datenrecht	Ebene	Recht	Inkl.
<b>Benutzerverwaltung</b>				
Cognos				
DFB-Fußball-Abzeichen				
DFB Medien				
DFBnet Lizenz				
DFBnet Pass				
DFBnet Verband				
Nationalmannschaft				
Pass Online				
Schiriansetzung				
Sicherheitsaufsichten und Ordnungsdienstkontrollen				
Spielbericht				
Spielstättenverwaltung				
Spieltagsreporting Fanbeauftragter				
Talentförderung				
Vereinsmeldebogen				

Abbildung 7 – Benutzerkennung kopieren – Schritt 1

In der Detailansicht ist links neben dem <Bearbeiten>-Button die Schaltfläche <Kopieren> angeordnet, sofern der Benutzer überhaupt Rollen und Rechte innehat. Die Auswahl des Buttons <Kopieren> bewirkt, dass der Administrator jetzt auf einen neuen Dialog navigiert, in dem der Administrator zunächst die Benutzerkennung eingeben muss, zu der kopiert werden soll (Ziel).

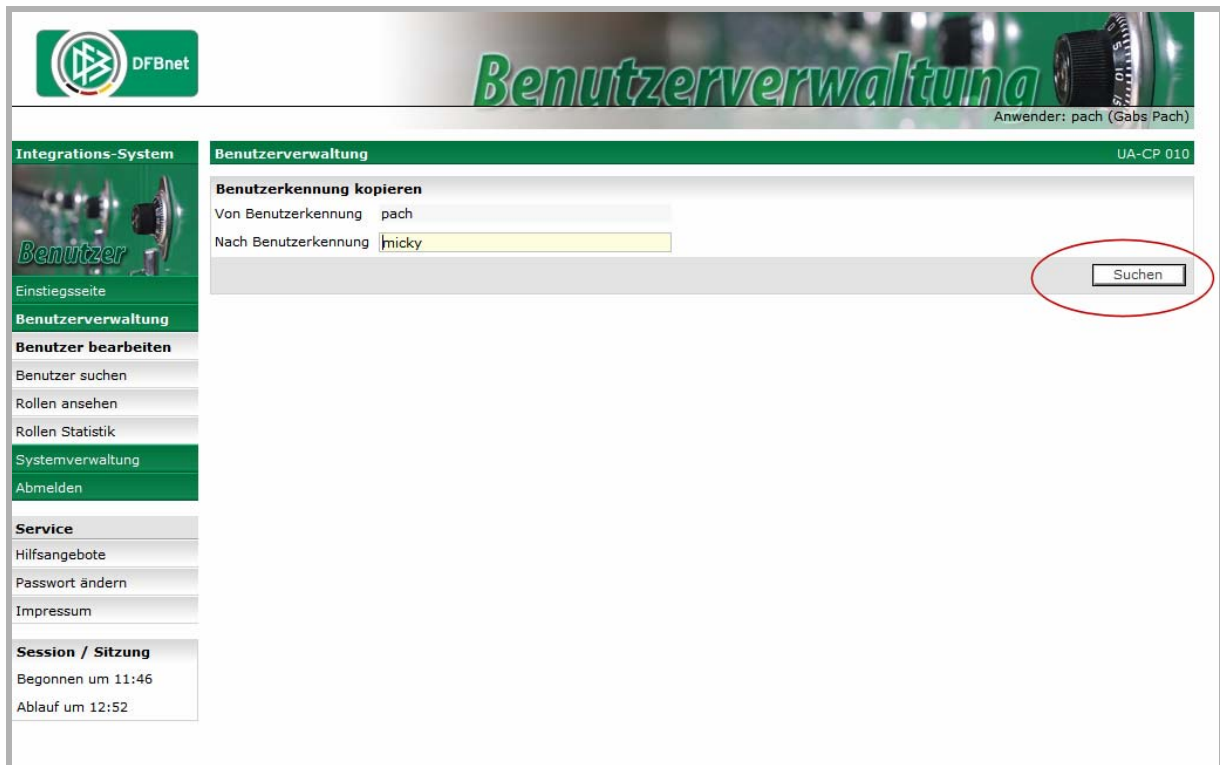


Abbildung 8 – Benutzerkennung kopieren – Schritt 2

Nach der Eingabe der vollständigen und exakten Benutzerkennung, betätigt der Anwender den <Suchen>-Button. Da die Benutzerkennungen eindeutig im System sind, wird entweder ein oder kein Treffer gefunden.

Wenn die Suche keinen Treffer ergibt, erscheint folgende Hinweismeldung:

Die Benutzerkennung <Benutzerkennung> existiert nicht. Bitte überprüfen Sie die Schreibweise oder legen Sie die Benutzerkennung vorher an. Anschließend können Sie den Kopiervorgang wiederholen.

Wenn die Suche genau einen Treffer ergibt, dann wird diese Benutzerkennung wiederum in der Detailansicht (als Kontrollfunktion) präsentiert. Der Button <Bearbeiten> ist in dieser Ansicht nicht verfügbar, stattdessen erscheint ein Button mit der Bezeichnung <Kopiervorgang abschließen>. Die Auswahl des Buttons bewirkt, dass alle Rollen und Rechte kopiert werden.



Abbildung 9 – Benutzererkennung kopieren – Schritt 3

Nach dem Kopiervorgang ist der Button <Kopiervorgang abschließen> nicht mehr verfügbar, stattdessen erscheint jetzt wieder der Button <Bearbeiten>. Im Such-Panel ist das Eingabefeld für die Benutzererkennung geleert, sodass der Kopiervorgang für eine weitere Benutzererkennung wiederholt werden könnte.

### 2.4.1 Regeln und Einschränkungen zum Kopieren von Benutzerkennungen

- Ein Administrator darf nur die Anwendungen, Rollen und Datenrechte kopieren, die er selbst innehat. Bezüglich der Datenrechte gilt, dass der Administrator mindestens dieselben oder mehr Datenrechte für eine Rolle haben muss als die Quelle. Es werden keine Ausschnitte kopiert. Hat beispielsweise die Quelle ein Datenrecht auf die Spielgebiete Bezirk Hannover und Bezirk Braunschweig und der Administrator nur ein Datenrecht auf das Spielgebiet Bezirk Hannover, wird die Rolle nicht kopiert.
- Es werden nur die Rollen kopiert, die vollständig administriert wurden. Benötigt beispielsweise eine Rolle grundsätzlich die Datenrechte Mannschaftsart, Spielklasse und Gebiet und fehlt mindestens eins der aufgeführten Rechte, so wird die Rolle nicht kopiert.
- Grundsätzlich werden die Anwendungen Cognos, E-Postfach und A-Nationalmannschaft nicht kopiert.



- Wenn eine Rolle nicht kopiert werden konnte, erhält der Administrator eine entsprechende Hinweismeldung.

Integrations-System
Benutzerverwaltung
UA-CP 010

Benutzer

**Benutzerverwaltung**

**Benutzer bearbeiten**

Benutzer suchen

Rollen ansehen

Rollen Statistik

Systemverwaltung

Abmelden

**Service**

Hilfsangebote

Passwort ändern

Impressum

**Session / Sitzung**

Begonnen um 11:46

Ablauf um 13:05

**Fehlermeldungen / Hinweise**

Der Kopiervorgang wurde erfolgreich abgeschlossen.

Rollen und Rechte der Anwendung <Nationalmannschaft> können nicht kopiert werden.  
 Rollen und Rechte der Anwendung <Cognos> können nicht kopiert werden.  
 Folgende Rollen konnten nicht kopiert werden, da diesen Rolle unvollständig sind bzw. Datenrechte fehlen:

- <Spieldagsreporting Fanbeauftragter : Fanbeauftragter>
- <Schiriansetzung : Beobachteransetzer>
- <Schiriansetzung : Administrator (Benutzer)>
- <Schiriansetzung : Schiriverwalter>
- <Schiriansetzung : Schiriansetzer>
- <Spielbericht : Mannschaftenverantwortlicher>
- <DFB-Fußball-Abzeichen : Klub2006>

**Benutzerkennung kopieren**

Von Benutzerkennung

Nach Benutzerkennung

**Information**

Benutzerkennung

**Persönliche Angaben**

Name	<input type="text" value="Micky"/>	Geschlecht	<input type="text"/>
Vorname	<input type="text" value="Mouse"/>	Nationalität	<input type="text" value="Deutschland"/>
Geburtsdatum	<input type="text" value="01.01.2000"/>		

**Adress- und Kontaktdaten**

Straße	<input type="text" value="Lister Straße 18"/>	Telefon privat	<input type="text"/>
PLZ / Ort	<input type="text" value="30163 Hannover"/>	Telefon geschäftlich	<input type="text"/>
Ortsteil	<input type="text"/>	Mobil	<input type="text"/>
Land	<input type="text" value="Deutschland"/>	Fax	<input type="text"/>
Firma	<input type="text"/>	E-Mail	<input type="text"/>

Rolle	Datenrecht	Ebene	Recht	Inkl.
<b>Benutzerverwaltung</b>				↕
<b>DFB-Fußball-Abzeichen</b>				↕
<b>DFB Medien</b>				↕
<b>DFBnet Lizenz</b>				↕
<b>DFBnet Pass</b>				↕
<b>DFBnet Verband</b>				↕
<b>Pass Online</b>				↕
<b>Sicherheitsaufsichten und Ordnungsdienstkontrollen</b>				↕
<b>Spielbericht</b>				↕
<b>Spielstättenverwaltung</b>				↕
<b>Spieldagsreporting Fanbeauftragter</b>				↕
<b>Talentförderung</b>				↕
<b>Vereinsmeldebogen</b>				↕

Abbildung 10 – Benutzerkennung kopiert



## 2.5 Benutzer suchen

Die Funktion <Benutzer suchen> wurde komplett überarbeitet. Bislang konnten Benutzerkennungen nur in Verbindung mit einer Anwendung, einer Rolle und einem Verband gesucht werden. Eine Einschränkung auf ein bestimmtes Verwaltungs- oder Spielgebiet war allerdings nicht möglich. Die nachfolgende Tabelle zeigt die neuen Suchkriterien, deren Verhalten in den nachfolgenden Kapiteln genauer beschrieben wird.

Suchkriterien	Pflicht	Typ und Defaults
Kennungstyp	Nein	Auswahlliste mit den zulässigen Kennungstypen erweitert um einen Leereintrag: <ul style="list-style-type: none"><li>• &lt;Leer&gt; (Default)</li><li>• &lt;Personenkennung&gt;</li><li>• &lt;Vereinskennung&gt;</li></ul>
Anwendung	Bedingt	Auswahlliste der Anwendungen, für die der Administrator berechtigt ist.
Rolle	Nein	Auswahlliste der Rollen, wenn zuvor eine Anwendung ausgewählt wurde. Andernfalls ist die Liste leer.
Strukturelemente	Nein	Liste ausgewählter Strukturelemente (hier können auch Vereine ausgewählt werden, wenn auf Vereine abgefragt werden soll)
Suchstrategien	Bedingt	Wenn ein oder mehrere Strukturelemente ausgewählt wurden, muss eine Suchstrategie festgelegt werden. Mögliche Suchstrategien: <ul style="list-style-type: none"><li>• Das Datenrecht des Benutzers ist im Strukturelement enthalten (Default)</li><li>• Mindestens ein Datenrecht des Benutzers stimmt exakt überein</li></ul>
Benutzerkennung	Bedingt	Textfeld, Eingabe einer Benutzerkennung (min. 3 Zeichen)
Benutzer aktiv	Nein	Auswahlliste mit den Werten: <ul style="list-style-type: none"><li>• &lt;Leer&gt; (Default)</li><li>• &lt;Ja&gt; (Benutzer ist aktiv)</li><li>• &lt;Nein&gt; (Benutzer ist nicht aktiv)</li></ul>

Zum Starten einer Suchanfrage müssen entweder eine Anwendung ausgewählt oder eine Benutzerkennung mit mindestens drei Zeichen eingegeben werden. Alle ausgewählten bzw. eingegebenen Suchkriterien werden mit einem logischen UND verknüpft. Eine Ausnahme bilden die Strukturelemen-



te. Werden mehrere Strukturelemente selektiert (z.B. Bezirk Hannover und Bezirk Braunschweig), so werden diese Elemente mit einem ODER verbunden.

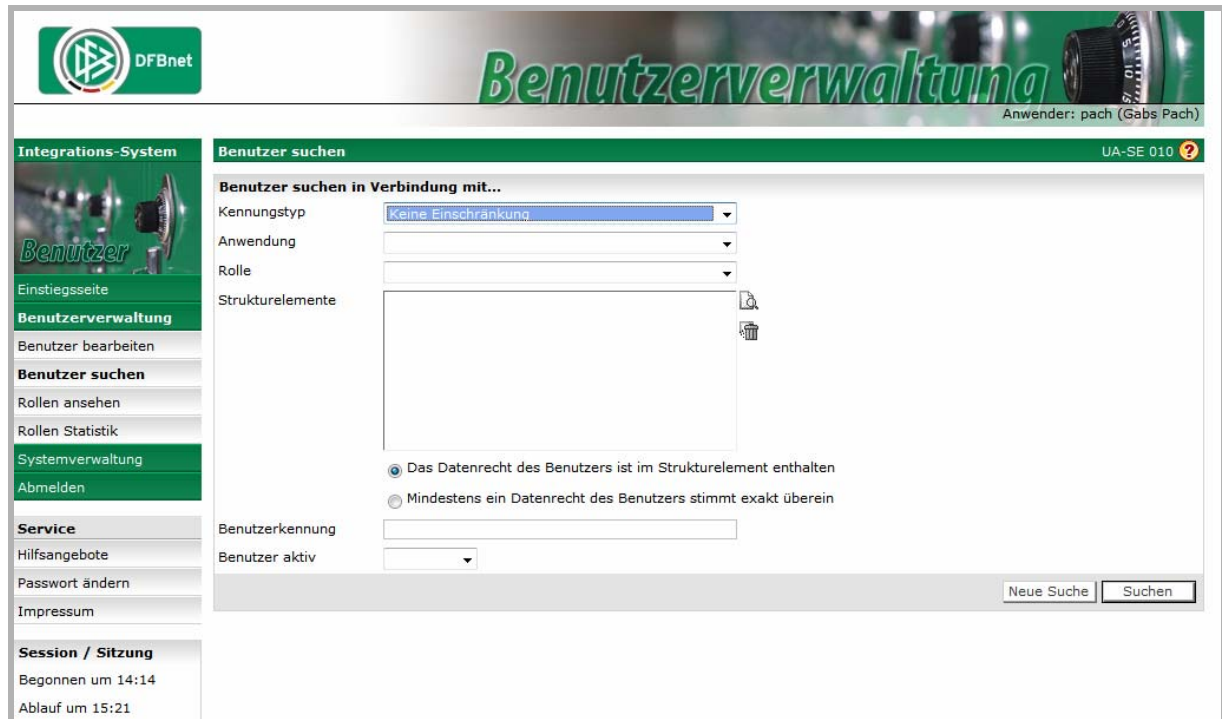


Abbildung 11 – Benutzer suchen

## 2.5.1 Auswahl der Strukturelemente

Das DFBnet kennt unterschiedliche Strukturen, die entweder die organisatorische Struktur oder die Spielgebietsstruktur inkl. Schiedsrichtergebiete eines Verbandes reflektieren. Im Rahmen des Talentförderprogramms wurden zusätzlich Koordinatorengbiete und Stützpunkte abgebildet. Konkret sind im DFBnet folgende Strukturen implementiert:

- Verwaltungsgebiete [V]
- Spielgebiete [G]
- Schiedsrichtergebiete [S]
- Stützpunkte [T]

Bis auf wenige Ausnahmen ist eine DFB-Anwendung immer nur auf eine Struktur berechtigt. Um Elemente aus einem Strukturbaum auswählen zu können, muss vorab eine Anwendung selektiert werden, damit der richtige Strukturbaum angezeigt wird.

Rechts neben der Multiselektionsliste befinden sich die Symbole zum Hinzufügen und Entfernen von Strukturelementen. Das Icon zum Hinzufügen von Strukturelementen ist nur aktiv, wenn vorab eine



Anwendung ausgewählt wurde. Durch die Auswahl des Icons zum Hinzufügen von Strukturelementen navigiert der Administrator auf eine neue Seite, die den entsprechenden Strukturbaum präsentiert. Im Strukturbaum werden immer nur Elemente zur Auswahl angeboten, für die der Administrator selbst berechtigt ist. Die Funktionsweise des Strukturbaumes entspricht der Vorgehensweise zum Zuordnen von Datenrechten.

Hinter jedem Strukturelement wird in eckigen Klammern der Strukturtyp angezeigt (siehe dazu die obige Liste). Ist eine Anwendung auf mehrere Strukturen berechtigt (z.B. Freundschaftsspiele) werden die Strukturtypen durch Kommata getrennt aufgelistet (z.B. [V, G]).

The screenshot shows the 'Benutzerverwaltung' (User Management) interface. The main area displays a tree structure of 'Verbands- und Gebietsstrukturen' (Association and Regional Structures). The tree includes 'Deutschland mit Regionen [G]', 'DFB (Verein für Wechsel ins Ausland) [G]', 'Fédération Internationale de Football Association [G]', 'Norddeutschland [G]', 'Bremen [G]', 'Hamburg [G]', 'Niedersachsen [G]', 'Bezirk Braunschweig [G]', 'Bezirk Hannover [G]', 'Bezirk Lüneburg [G]', 'Bezirk Weser-Ems [G]', 'Schleswig-Holstein [G]', 'Nordostdeutschland [G]', 'Region Südwestdeutschland [G]', 'Süddeutschland [G]', and 'Westdeutschland [G]'. Each item has checkboxes for 'inkl.' (inclusive) and 'exkl.' (exclusive) selection. A table above shows selected elements: 'Bezirk Braunschweig' and 'Bezirk Hannover' are both marked as inclusive. The interface also includes a sidebar with navigation options like 'Benutzer suchen', 'Rollen ansehen', and 'Systemverwaltung', and a top navigation bar with 'Benutzer suchen / Filterkriterien in Verbands- und Gebietsstrukturen'.

Abbildung 12 – Strukturbaum

Die Auswahl eines oder mehrerer Strukturelemente erfolgt, indem der Administrator die entsprechenden Check-Boxen markiert und zuordnet. Betätigt der Anwender anschließend den <Zurück> Button, so werden die ausgewählten Elemente in der Multiselektionsliste angezeigt. In runden Klammern wird angezeigt, ob die Strukturelemente exklusiv oder inklusiv ausgewählt wurden.



DFB-MEDIEN

Zum Entfernen eines oder mehrerer Strukturelemente müssen diese in der Liste markiert und anschließend das <Entfernen> Symbol betätigt werden.

The screenshot shows the 'Benutzerverwaltung' (User Management) interface. The main heading is 'Benutzer suchen' (Search Users). The search criteria are as follows:

- Benutzer suchen in Verbindung mit...**
- Kennungstyp:** Personenkennung
- Anwendung:** Meisterschaftsbetrieb
- Rolle:** Staffelleiter
- Strukturelemente:** Bezirk Braunschweig (inkl.), Bezirk Hannover (inkl.)

Below the search criteria, there are two radio buttons for data rights:

- Das Datenrecht des Benutzers ist im Strukturelement enthalten
- Mindestens ein Datenrecht des Benutzers stimmt exakt überein

At the bottom, there are input fields for 'Benutzerkennung' and 'Benutzer aktiv', and buttons for 'Neue Suche' and 'Suchen'.

Abbildung 13 – Benutzer suchen – Strukturelemente

Wählt der Administrator aus der Auswahlliste eine andere Anwendung aus, so leert sich die Liste mit den Rollen. Wurden bei der vorherigen Suchabfrage Strukturelemente ausgewählt, bleiben diese erhalten, sofern der Strukturtyp des jeweiligen Strukturelementes für die ausgewählte Anwendung bzw. Rolle zulässig ist. Gleiches gilt, wenn der Administrator innerhalb einer Anwendung die Rolle wechselt. Passt der Strukturtyp nicht zu der ausgewählten Rolle bzw. Anwendung wird dieser implizit gelöscht.

#### Beispiel:

Der Administrator sucht in der Anwendung Meisterschaft nach allen Staffelleitern im Bezirk Braunschweig und Hannover. Bei diesen Gebieten handelt sich um den Strukturtyp Spielgebiet [G]. Wählt der Anwender jetzt die Applikation Schiedsrichter und die Rolle Schiriansetzer aus, so werden die Spielgebiete aus der Multiselektionsliste gelöscht, da der Schiriansetzer auf Schiedsrichtergebiete [S] zu berechnen ist. Würde der Admin stattdessen die Rolle Staffelleiter im Spielbericht selektieren, blieben die Spielgebiete in der Multiselektionsliste erhalten, da auch der Staffelleiter im Spielbericht Datenrechte auf Spielgebiete benötigt.

## 2.5.2 Suchstrategien

Die Auswahl eines Strukturelementes kann „exklusiv“ oder „inklusive“ aller darunter liegenden Strukturen erfolgen. Wird ein Element „exklusiv“ zugeordnet, so werden alle Benutzerkennungen gefunden, die exakt dasselbe exklusive Datenrecht besitzen. Bei der Auswahl eines „inklusive“ Strukturelementes kann der Anwender eine der folgenden Suchstrategien auswählen:

- Strategie 1: das Datenrecht des Benutzers ist im Strukturelement enthalten (default)
- Strategie 2: mindestens ein Datenrecht des Benutzers stimmt exakt überein

Suchstrategie 1 besagt, dass alle Benutzerkennungen gefunden werden, die über mindestens ein Datenrecht verfügen, das mit dem ausgewählten Strukturelement übereinstimmt oder im ausgewählten Strukturelement enthalten ist.

Suchstrategie 2 besagt, dass alle Benutzerkennungen gefunden werden, die mindestens über ein Datenrecht verfügen, das mit dem Strukturelement exakt identisch ist.

Wählt der Administrator kein Strukturelement aus, so wird implizit das Datenrecht des Administrators bei der Suche verwendet.

### Beispiel 1:

<b>Kennungstyp:</b>	Personenkennung
<b>Anwendung:</b>	Meisterschaft
<b>Rolle:</b>	Staffelleiter
<b>Strukturelemente:</b>	Bezirk Braunschweig (inkl.) Bezirk Hannover (inkl.)

### Ergebnis: Suchstrategie 1

Es werden alle Personenkennungen gefunden, die in der Anwendung <Meisterschaft> die Rolle <Staffelleiter> innehaben und die entweder auf den Bezirk Braunschweig oder auf den Bezirk Hannover oder auf untergeordnete Gliederungsebenen (z.B. Kreis Wolfenbüttel oder Kreis Hannover Stadt) berechtigt sind.

### Ergebnis: Suchstrategie 2

Es werden alle Personenkennungen gefunden, die in der Anwendung <Meisterschaft> die Rolle <Staffelleiter> innehaben und die entweder auf den Bezirk Braunschweig (inkl.) oder auf den Bezirk Hannover (inkl.) berechtigt sind.



## 2.6 Detail einer Benutzererkennung

Im Detail einer Benutzererkennung sind die persönlichen Daten und die Adress- und Kontaktinformationen sowie die Anwendungen, Rollen und Datenrechte sichtbar, die einer Benutzererkennung zugeordnet wurden.

Per se sieht der Administrator nur die Anwendungen, für die er selbst die Administrationsrechte hat. Gleiches gilt für die Datenrechte. Wurden einer Benutzererkennung Datenrechte zugewiesen, die außerhalb des Zuständigkeitsbereiches des Administrators liegen, werden diese nicht angezeigt. Stattdessen erscheint eine entsprechende Hinweismeldung.

Um dem Administrator einen schnellen Überblick über den Zustand einer Benutzererkennung zu geben, werden jetzt in der Liste der Anwendungen Symbole präsentiert, die entweder besagen, dass eine Rolle unzureichend administriert wurde oder dass einer Rolle Datenrechte zugewordnet wurden, die außerhalb des Zuständigkeitsbereiches des Administrators liegen.

Die nachfolgende Grafik vermittelt einen visuellen Eindruck.

The screenshot shows the 'Benutzerverwaltung' (User Management) interface. The user 'micky' is selected. The interface is divided into several sections:

- Information:** Benutzererkennung: micky
- Fehlermeldungen / Hinweise:** Sie besitzen nicht zu allen Anwendungen des Benutzers Administratorrechte (highlighted with a red oval).
- Kennungsinformationen:**
  - Altes Passwort: [input field]
  - Neues Passwort: [input field]
  - Passwortbestätigung: [input field]
  - Benutzer aktiv: ja
  - Passwortänderung erlaubt: ja
  - Passwort abgelaufen / am: ja 30.11.2010 19:27:27
  - Passwortänderung:  nach Anmeldung erforderlich
- Persönliche Angaben:**
  - Name: Micky
  - Vorname: Mouse
  - Geburtsdatum: 01.01.2000
  - Geschlecht: [input field]
  - Nationalität: Deutschland
- Adress- und Kontaktdaten:**
  - Straße: Lister Straße 18
  - PLZ / Ort: 30163 Hannover
  - Ortsteil: [input field]
  - Land: Deutschland
  - Firma: [input field]
  - Telefon privat: [input field]
  - Telefon geschäftlich: [input field]
  - Mobil: [input field]
  - Fax: [input field]
  - E-Mail: [input field]
- Buttons:** Zurück, Kopieren, Bearbeiten
- Table of Roles and Rights:**




Rolle	Datenrecht	Ebene	Recht	Inkl.
<b>Benutzerverwaltung</b>				
DFBnet Lizenz				
DFBnet Pass				
DFBnet Verband				
Ergebnisdienst				
Pass Online				
Schiriansetzung				
Spielstättenverwaltung				

Abbildung 14 – Benutzerdetail – Anwendungen



DFB-MEDIEN

Wie der Grafik zu entnehmen ist, werden vor den Anwendungen verschieden farbige Symbole angezeigt, deren Bedeutung im Tool-Tipp des jeweiligen Icons angezeigt und durch die nachfolgende Tabelle beschrieben werden.

Icon	Bedeutung
	Mindestens eine Rolle der Anwendung wurde unzureichend administriert
	Zu mindestens einer Rolle der Anwendung besitzt der Anwender nicht die notwendigen Datenrechte
	Mindestens eine Rolle der Anwendung wurde unzureichend administriert und zu mindestens einer Rolle derselben Anwendung besitzt der Anwender nicht die notwendigen Datenrechte oder für eine Rolle treffen beide Bedingungen zu

Durch das Aufklappen einer oder mehrerer Anwendungen werden die zugeordneten Rollen und Datenrechte sichtbar. In diesem Zustand ist ersichtlich, welche Rollen unzureichend administriert wurden oder für welche Rollen dem Administrator Datenrechte fehlen bzw. außerhalb seines Zuständigkeitsbereiches liegen.



DFB-MEDIEN

Rolle	Datenrecht	Ebene	Recht	Inkl.
<b>Benutzerverwaltung</b>				↻
<b>DFBnet Lizenz</b>				↻
<b>DFBnet Pass</b>				↻
Adressbeauftragter	Verwaltungsgebiete	Landesverband	Niedersächsischer Fußballverband	✓
Artikelbearbeiter	Verwaltungsgebiete	Landesverband	Niedersächsischer Fußballverband	✓
Beauftragter Bußgeld	Verwaltungsgebiete	Landesverband	Niedersächsischer Fußballverband	✓
Beauftragter Stornierung/Korrektur	Verwaltungsgebiete	Landesverband	Niedersächsischer Fußballverband	✓
Druckbeauftragter	Verwaltungsgebiete	Landesverband	Niedersächsischer Fußballverband	✓
FIBU-Beauftragter	Verwaltungsgebiete	Landesverband	Niedersächsischer Fußballverband	✓
<b>Passstellenleiter</b>	keine Datenrechte			
<b>VIP-Adressbeauftragter</b>	Verwaltungsgebiete	Landesverband	Niedersächsischer Fußballverband	✓
			Datenrechte ausserhalb Ihrer Zuständigkeit	
Verbandskoordinator	Verwaltungsgebiete	Landesverband	Niedersächsischer Fußballverband	✓
Verbandsmitarbeiter	Verwaltungsgebiete	Landesverband	Niedersächsischer Fußballverband	✓
Wechselrechtbeauftragter	Verwaltungsgebiete	Landesverband	Niedersächsischer Fußballverband	✓
<b>DFBnet Verband</b>				↻
<b>Ergebnisdienst</b>				↻
<b>Administrator</b>	Spielgebiete	Landesgebiet	Niedersachsen	✓
	Spielklassen	NFV 01	Alle Spielklassen	
Administrator (Benutzer)	Spielgebiete	Landesgebiet	Niedersachsen	✓
	Spielklassen	NFV 01	Alle Spielklassen	
	Mannschaftsarten	NFV 01	Alle Mannschaftsarten	
<b>Pass Online</b>				↻
<b>Schiriansetzung</b>				↻
<b>Beobachteransetzer</b>	Schirigebiete		Datenrechte ausserhalb Ihrer Zuständigkeit	
	Spielklassen		Datenrechte ausserhalb Ihrer Zuständigkeit	
	Mannschaftsarten		Datenrechte ausserhalb Ihrer Zuständigkeit	
<b>Schiriansetzer</b>	Schirigebiete		Datenrechte ausserhalb Ihrer Zuständigkeit	
	Spielklassen		Datenrechte ausserhalb Ihrer Zuständigkeit	
	Mannschaftsarten		Datenrechte ausserhalb Ihrer Zuständigkeit	
<b>Schiriverwalter</b>	Schirigebiete		Datenrechte ausserhalb Ihrer Zuständigkeit	
<b>Staffelschiriansetzer</b>	Schirigebiete		Datenrechte ausserhalb Ihrer Zuständigkeit	
<b>Spielstättenverwaltung</b>				↻

Abbildung 15 – Benutzerdetail – Rollen

**Hinweis:** Rollen, die durch ein rotes, oranges oder rot-oranges Icon gekennzeichnet sind, können durch den Administrator nicht kopiert werden (siehe dazu Kapitel 2.4.1 – Regeln und Einschränkungen zum Kopieren von Benutzerkennungen).



## 2.7 Sicherheitsstufen / Policies

Um den Anforderungen des Datenschutzes gerecht zu werden, sollen anwendungsspezifische Policies eingeführt werden. Dabei handelt es sich um Richtlinien, die den Zugang zu den DFBnet Anwendungen regeln. Beispielsweise wird in einer Policy hinterlegt, welche Mindestanforderungen für die Vergabe eines Kennwortes zu erfüllen sind und in welchen zeitlichen Abständen der Benutzer sein Kennwort ändern muss. Die Einführung der Policies erfolgt in mehreren Schritten. Im ersten Schritt ist festzulegen, welche Regeln grundsätzlich etabliert werden sollen. Dabei geht es um eine abstrakte Definition wie beispielsweise die Mindestlänge eines Passwortes. Je nach Sicherheitsstufe werden die einzelnen Merkmale, die für alle Applikationen gleichermaßen gelten, in einem zweiten Schritt konkret ausgeprägt und den Anwendungen zugewiesen. Die Überprüfung und Einhaltung der Policies soll in einem dritten Schritt gewährleistet werden.

**Hinweis:** Die Policies gelten für alle Mitgliedsorganisationen gleichermaßen. Das Konzept sieht keine mandantenspezifische Implementierung vor.

### 2.7.1 Beschreibung der Policy

Die nachfolgende Tabelle beschreibt, welche Merkmale für die Kennwort-Policy etabliert werden sollen.

Nr.	Regel
1	<b>Minimale Länge des Kennwortes</b> Über diese Regel wird festgelegt, aus wie viel Zeichen ein Kennwort mindestens bestehen muss (z.B. 8 Zeichen)
2	<b>Davon Mindestanzahl Kleinbuchstaben</b> Ausgehend von der Mindestlänge wird festgelegt, wie viele Kleinbuchstaben das Kennwort enthalten muss (z.B. 1 Zeichen)
3	<b>Davon Mindestanzahl Großbuchstaben</b> Ausgehend von der Mindestlänge wird festgelegt, wie viele Großbuchstaben das Kennwort enthalten muss (z.B. 1 Zeichen)
4	<b>Davon Mindestanzahl Ziffern</b> Ausgehend von der Mindestlänge wird festgelegt, wie viele Ziffern das Kennwort enthalten muss (z.B. 2 Ziffern)
5	<b>Davon Mindestanzahl Sonderzeichen (ohne Whitespace)</b> Ausgehend von der Mindestlänge wird festgelegt, wie viele Sonderzeichen das Kennwort enthalten muss (z.B. 1 Sonderzeichen)
6	<b>Davon erlaubte Mehrfachnennung eines Zeichens</b> Dieses Kriterium legt fest, wie häufig ein Zeichen im Kennwort vorkommen darf (z.B. zweimal)



Nr.	Regel
7	<p><b>Anzahl der unterschiedlichen Zeichen bei Kennwortänderung</b></p> <p>Ausgehend von der Mindestlänge wird festgelegt, in wie vielen Zeichen sich das neue Kennwort von dem alten Kennwort unterscheiden muss (z.B. 5 Zeichen)</p> <p><b>Beispiel:</b></p> <p>Altes Kennwort = fussball</p> <p>Neues Kennwort = handball (nicht zulässig)</p>
8	<p><b>Kennwort darf den Namen nicht enthalten</b></p> <p>Für eine Personenkennung gilt, dass der Name des Benutzers nicht im Kennwort enthalten sein darf</p> <p><b>Beispiel:</b></p> <p>Name des Benutzers = pach</p> <p>Kennwort = pach12 (nicht zulässig)</p>
9	<p><b>Kennwort darf den Vornamen nicht enthalten</b></p> <p>Für eine Personenkennung gilt, dass der Vorname des Benutzers nicht im Kennwort enthalten sein darf</p> <p><b>Beispiel:</b></p> <p>Vorname des Benutzers = gabi</p> <p>Kennwort = gabi99 (nicht zulässig)</p>
10	<p><b>Kennwort darf das Geburtsdatum nicht enthalten</b></p> <p>Für eine Personenkennung gilt, dass das Geburtsdatum des Benutzers – sofern vorhanden – nicht im Kennwort enthalten sein darf</p>
11	<p><b>Kennwort muss sich von der Kennung unterscheiden</b></p> <p>Für eine beliebige Kennung gilt, dass die Kennung nicht im Kennwort enthalten sein darf</p>
12	<p><b>Kennwort-Historie, Anzahl der zuvor verwendeten Passwörter, die nicht erneut vergeben werden dürfen</b></p>
13	<p><b>Kennwort läuft ab</b></p> <p>Das Flag kennzeichnet, ob ein Kennwort zeitlich abläuft oder nicht. Wenn ein Kennwort abläuft, sind zusätzlich die Zeitdauer und das Ereignis anzugeben.</p>
14	<p><b>Kennwort läuft bei Anforderung per E-Mail ab</b></p> <p>Dieses Kriterium besagt, dass ein per E-Mail angefordertes Kennwort abläuft, wenn sich der Anwender über einen festgelegten Zeitraum nicht mehr angemeldet hat.</p>
15	<p><b>Kennwort läuft ab nach der letzten Aktualisierung</b></p> <p>Dieses Kriterium besagt, dass ein Kennwort abläuft, wenn der Anwender sein Kennwort über einen festgelegten Zeitraum nicht mehr aktualisiert hat.</p>



## 2.7.2 Konkrete Ausprägung der Policies in Sicherheitsstufen

Die Ausprägung der in Kapitel 2.7.1 aufgeführten Merkmale wird nicht pro Anwendung sondern pro Sicherheitsstufe vorgenommen. Zunächst werden die Sicherheitsstufen:

- Hoch,
- Mittel,
- Niedrig und
- (Keine Sicherheitsstufe)

eingeführt. Einer Anwendung wird dann eine Sicherheitsstufe zugeordnet.

Neben den drei aufgeführten Sicherheitsstufen wurde eine Default-Sicherheitsstufe (Keine Sicherheitsstufe) implementiert. Diese Sicherheitsstufe wird immer dann angewendet, wenn einer Applikation nicht explizit eine Sicherheitsstufe zugeordnet wurde.

## 2.7.3 Verwaltung und Zuweisung der Sicherheitsstufen

Für die Verwaltung der Policies und für das Zuweisen der Sicherheitsstufen wurde eine neue Anwendung mit dem Namen „System Administration“ etabliert. Diese Anwendung stellt die Rollen <Systemadministrator> und <Infoanwender> bereit. Der Systemadministrator darf Sicherheitsstufen anlegen, verändern und diese einer oder mehreren Anwendungen zuweisen. Der Infoanwender hat lediglich ein Leserecht, d.h. er sieht welcher Applikation welche Sicherheitsstufe zugeordnet wurde und wie sich die Sicherheitsstufe konkret ausprägt.

Der Systemadministrator ordnet jeder DFBnet Applikation genau eine Sicherheitsstufe zu. Darüber hinaus legt er fest, welche(r) Kennungstyp (Personenkennung oder Vereinskennung oder beides) der Applikation zuzuordnen ist. Über die Sicherheitsstufen hinaus kann also auch gesteuert werden, welche Kennungstypen bei einer Applikation zulässig sind. Für das Anlegen und Bearbeiten von Sicherheitsstufen wird in der ersten Version keine Benutzerschnittstelle zur Verfügung gestellt.

**Hinweis:** Die Bearbeitung und Zuweisung einer Sicherheitsstufe und des Kennungstyps erfolgt ausschließlich durch die DFB-Medien. Die Zuweisung der Sicherheitsstufen zu den Applikationen erfolgt als nächster Schritt in enger Abstimmung mit den Verbänden

## 2.7.4 Sicherheitsstufen ansehen

Bem.: Diese Möglichkeit, sich zu informieren, wird ebenfalls erst später angeboten, da zum Release 3.14 noch keine Sicherheitsstufen implementiert sind.



Wählt der Anwender den Menüpunkt <Sicherheitsstufen> aus, navigiert er auf eine Seite, die die vorhandenen Sicherheitsstufen in Form einer Liste mit folgendem Aufbau präsentiert:

- Ansichtssymbol
- Name der Sicherheitsstufe
- Anzahl der Applikationen, denen die Sicherheitsstufe zugeordnet wurde

Die Auswahl des Ansichtssymbols bewirkt, dass die konkret ausgeprägte Sicherheitsstufe im Detail angezeigt wird. Im Kopfbereich der Seite ist das Info-Panel mit dem Name der Sicherheitsstufe zu sehen. Darunter befindet sich die Box mit dem Titel „Sicherheitsstufe“. In dieser Box sind alle Kriterien mit ihren konkreten Ausprägungen „read only“ dargestellt.

Sicherheitsstufe	Anzahl der zugeordneten Anwendungen
hoch	0
mittel	0
niedrig	2
keine Sicherheitsstufe	46

Abbildung 16 – Sicherheitsstufen – Übersicht



Sicherheitsstufen		SA-PD 010
Information		
Sicherheitsstufe	keine Sicherheitsstufe	
<b>Sicherheitsstufe: keine Sicherheitsstufe</b>		
Minimale Länge des Kennwortes	3	
Davon mindestens Kleinbuchstaben		
Davon mindestens Großbuchstaben		
Davon Mindestanzahl Ziffern		
Davon Mindestanzahl Sonderzeichen (ohne Whitespace)		
Davon erlaubte Mehrfachnennung eines Zeichens		
Anzahl der unterschiedlichen Zeichen bei Kennwortänderung		
Kennwort darf die Kennung enthalten	nein	
Kennwort darf den Namen enthalten	nein	
Kennwort darf den Vornamen enthalten	nein	
Kennwort darf das Geburtsdatum enthalten	nein	
Kennwort muß sich von der Kennung unterscheiden	ja	
Anzahl der zuvor verwendeten Passwörter, die nicht vergeben werden dürfen		
Kennwort läuft nie ab	nein	
Kennwort läuft bei Anforderung per Email ab nach		
Kennwort läuft nach der letzten Aktualisierung ab nach		

Abbildung 17 – Sicherheitsstufen – Detail

### 2.7.5 Aktivierung der Sicherheitsstufen

Mit dem Release 3.14 werden alle Funktionen bereitgestellt, um Sicherheitsstufen verwalten und zuordnen zu können. Die Überprüfung der Policy im Anmeldevorgang ist ebenfalls realisiert. Allerdings sind alle Mechanismen deaktiviert und werden erst in Abstimmung mit den Verbänden freigeschaltet.



### 3. Abbildungsverzeichnis

Abbildung 1 – Benutzer bearbeiten – Suchmaske .....	5
Abbildung 2 – Benutzer bearbeiten – Trefferliste .....	6
Abbildung 3 – Passwortänderung nach Anmeldung erforderlich 1 .....	8
Abbildung 4 – Passwortänderung nach Anmeldung erforderlich 2 .....	8
Abbildung 5 – Passwortänderung nach Anmeldung erforderlich 3 .....	9
Abbildung 6 – Passwort abgelaufen .....	10
Abbildung 7 – Benutzererkennung kopieren – Schritt 1 .....	11
Abbildung 8 – Benutzererkennung kopieren – Schritt 2 .....	12
Abbildung 9 – Benutzererkennung kopieren – Schritt 3 .....	13
Abbildung 10 – Benutzererkennung kopiert .....	14
Abbildung 11 – Benutzer suchen .....	16
Abbildung 12 – Strukturbaum .....	17
Abbildung 13 – Benutzer suchen – Strukturelemente .....	18
Abbildung 14 – Benutzerdetail – Anwendungen .....	20
Abbildung 15 – Benutzerdetail – Rollen .....	22
Abbildung 18 – Sicherheitsstufen – Übersicht .....	26
Abbildung 19 – Sicherheitsstufen – Detail .....	27

### 4. Bearbeitungshistorie

Version	Wer	Wann	Was
V 1.0	Gabi Pach	03.12.2010	Dokument erstellt
V 1.1	Gabi Pach	06.12.2010	Nach Review aktualisiert
V 1.2	P. Smerzinski	08.12.2010	Änderung auf Seite 25 Kennungstyp