



**Ihr Provider**

## Handbuch virtuelle Server Stand September 2007 Version 5.15

---

Herzlich willkommen und vielen Dank, dass Sie sich für einen Webserver von EDIS.AT entschieden haben. Sie haben die richtige Wahl getroffen, denn die 4 Buchstaben von EDIS sind ein Synonym für Qualität in Dienstleistung und Service.

Ihr Linux-Webserver wurde mit viel Sorgfalt für Sie installiert und getestet und wird bereits mit den gängigsten Features, die Sie für einen erfolgreichen Start ins Web benötigen, ausgeliefert.

Dazu zählen die neuesten Programmiersprachen wie z.B. PHP4 / PHP5, zusätzliche Bibliotheken wie GD-LIB 2.x für .gif, .bmp und JPEG Support, ZLIB für Datenkomprimierung, XML/XSLT (Sablotron), DOM-XML, imap- und gettext-Support, MING für die coolsten Flash-Grafiken direkt aus PHP, PDF Support und die PHP-Beschleunigungs-Engine von ZEND Labs (ZEND Optimizer), Datenbanken wie MySQL 4.1.x und Interbase, Zugriffs-Statistiken (Webalizer), CGI uns noch vieles mehr ...

Bei den Servern ab ADVANCED Hosting steht auf Wunsch der Applikation-Server ZOPE mit eigener IP-Adresse für Sie bereit. Jetzt aber genug der Worte, denn Sie wollen doch so schnell wie möglich online sein.

Na dann nichts wie los!

Viel Freude mit Ihrem Server wünschen

Gerhard Kleewein  
Daniel Ruschka  
Gerhard Luisser  
Egon Lauppert  
Christa Markgraf

## Inhaltsverzeichnis

---

<b>Handbuch virtuelle Server Stand Juni 2006 Version 5.13 .....</b>	<b>2</b>
<b>Inhaltsverzeichnis.....</b>	<b>3</b>
<b>Management Oberfläche - <a href="https://manage.edis.at/">https://manage.edis.at/</a>.....</b>	<b>5</b>
<b>Teil 1. Kunden Bereich .....</b>	<b>6</b>
1. Passwort ändern .....	7
2. Einstellungen.....	7
3. Bestellen.....	7
4. vHost .....	8
5. Domain .....	8
5.1 Auflisten .....	8
5.2 Datenänderung.....	9
5.3 Status.....	10
5.4 Domaininhaber .....	10
6. Redirect .....	10
7. Links .....	10
8. Support.....	11
8.1 FAQ .....	11
8.2 Handbuch .....	11
<b>Teil 2. vHost-Bereich .....</b>	<b>12</b>
Einstellungen – Übersicht.....	13
1. Passwort ändern .....	14
2. Email-Adressen verwalten.....	14
2.1 Neue Email anlegen .....	15
2.2 Übersicht der Email-Einstellungen .....	18
2.3 Spam- und Virenschutzeinstellungen.....	20
2.4 Abfragen und Senden von Emails mit Webmail .....	27
3. Apache .....	29
3.1 Zugriffsschutz: .....	29
3.2 Errorsites – Definition von individuellen Fehlerseiten.....	30
3.3 Subdomain:.....	32
3.4 PHP Version .....	33
4. FTP.....	34
4.1 FTP Verwaltung.....	35
4.2 Dateirechte .....	36
4.3 Web-FTP .....	36
5. Scripts.....	39
5.1 Gästebuch .....	39
5.2 Forum .....	39

5.3 Formmail.....	39
6. Statistiken .....	40
6.1 Verwaltung.....	40
6.2 Speichernutzung.....	41
6.3 Homepage .....	41
7.Datenbank .....	42
7.1 Verwaltung.....	42
7.2 phpMyAdmin 2.6.1.....	42
8. Links .....	44
9. Support.....	44
9.1 FAQ .....	44
9.2 Handbuch .....	44
<b>Teil 3. Email-Bereich.....</b>	<b>45</b>
1. Email Adresse .....	45
1.1 Lokale Email .....	45
1.2 White/Blacklist .....	45
2. Support.....	45
2.1 FAQ .....	45
2.2 Handbuch .....	45
<b>Teil 4. FTP-Bereich.....</b>	<b>46</b>
1. Passwort ändern .....	46
2. phpWebFTP .....	46
<b>Teil 5. Passwort-zusenden.....</b>	<b>47</b>

## Management Oberfläche - <https://manage.edis.at/>

Die Administration Ihres Webservers erfolgt über das Webserver-Administrations-Interface erreichbar unter der Adresse <https://manage.edis.at>



The screenshot displays the EDIS.at management interface. At the top left is the EDIS.at logo and 'Ihr Provider'. The main header contains the text 'Hier können Sie in Ruhe alles richtig gut managen!' and ':: ISP-Server Admin'. Below this, there are five distinct login options, each with an icon and a list of services:

- Kundenbereich:** Login mit Kunden Nr und Kunden Passwort. Services: Bestellbereich, Domainportfolio, Webhostportfolio, Weiterleitungen verw., Pers. Daten ändern.
- vHost Bereich:** Login mit FTP User und FTP Passwort. Services: Email Adressen verw., Geschützte Bereiche, Errorpages definieren, Server Statistiken, MYSQL Datenbanken, Subdomains verw., Formmailer, Scripts.
- Email Konfiguration:** Login mit Kontoname und Passwort des Email Postfaches. Services: Alias Verwaltung, eMail Passwort ändern, Webmail.
- FTP Bereich:** Login mit FTP User und FTP Passwort. Services: Kennwort ändern, Web FTP.
- Passwort anfordern:** mittels Eingabe von Kundennummer oder Email.

Das Administrations-Interface ist wahlweise über <http://manage.edis.at> oder mit 128 Bit verschlüsselt über <https://manage.edis.at> erreichbar.



## Teil 1. Kunden Bereich

---

Der **Kundenbereich** dient vorwiegend dazu, Ihre bei EDIS.AT registrierten **Domains zu verwalten** (Domain Portfolio) und eine Übersicht über gebuchte Dienstleistungen und Services zu erhalten.

Dazu zählen die

- Einrichtung und Änderung von URL- und Email-Weiterleitungen (Redirects)
- der Zonefile-Editor für Echtzeit-Änderungen von Nameserver-Einträgen in den EDIS.AT Nameservern
  - die Änderung Ihrer persönlichen Daten, die Änderung der Zahlungsart (Kreditkarte, Lastschrift von Ihrem Konto)
- Inhaberwechsel und Datenänderungen (WHOIS) Ihrer Domains

Um sich anzumelden klicken Sie unter <https://manage.edis.at> auf „Kunden Bereich“ und geben Sie Ihre **Kundennummer** und Ihr **Kundenkennwort** an. Diese Daten haben Sie bei Ihrer Anmeldung im Shop erhalten. Das Passwort haben Sie selbst vergeben. Anbei ein kurzes Beispiel-Email:

### EDIS.AT: Ihre Kundendaten

---

```
[...]  
Ihre Logindaten, mit denen Sie ab sofort einfach und komfortabel  
Bestellungen tätigen können, lauten:  
  
Kundennummer: 16867  
Passwort: amdev2  
[...]
```



## 1. Passwort ändern

---

Hier können Sie das Passwort für den Kundenbereich selbst ändern. Der Benutzername (Kunden-Nr.) bleibt dabei unverändert.

## 2. Einstellungen

---

Die Einstellungen im Kundenbereich betreffen Ihre persönlichen Daten wie Post-Adresse, Zahlungsweise und Kontostand. Sie haben hier die Möglichkeit alle Daten z.B. auch Ihre Bankverbindung auf aktuellem Stand zu halten.

Unter dem Punkt Kontostand finden sie eine tabellarische Übersicht sämtlicher Zahlungen:

- Beleg Nr (Belegnummer )
- vom (Datum der Rechnung )
- ZA (Zahlungsart: ELV Lastschrift, 10T: Zahlungsziel 10 Tage)
- Fällig am (Fälligkeit)
- Beahlt am (Bezahlungsdatum)
- Belegbetrag
- Bisher bezahlt
- Restbetrag

Durch Klick auf die Belegnummer können Sie die Rechnung online als .pdf downloaden.

## 3. Bestellen

---

Hier haben Sie Zugang zum EDIS.at Shopsystem mit folgenden Optionen:

- Eine neue Domain registrieren (parken, weiterleiten, Webpace)
- Providerwechsel einer bestehenden Domain
- Webpace zu einer bestehenden Domain
- Webpace für ein bestehendes Paket erweitern
  
- Virtuellen RootServer bestellen
- RootServer Zusatzleistung bestellen
  
- Dedicated Server
- Serverhousing
- SMS Produkte

Sie brauchen sich nicht gesondert zu registrieren, da Sie sich ja bereits eingeloggt haben.

**Achtung:** Bestellungen über den Kundenbereich werden nicht mehr geprüft und Domain-Aufträge direkt an die Vergabestelle weitergeleitet.



## 4. vHost

---

In der vHost-Übersicht sehen Sie alle Ihre vHosts mit den zugehörigen Domains aufgelistet.

- Domain
- Alias Domains (konfigurierte Zusatzdomains)
- User
- Max PopAccounts (max. Anzahl zulässiger Email-Adressen)
- Speicherplatzart (vCard, STARTER, BASIC Hosting ...)
- Abgerechnet bis (Datum bis wann Ihr Produkt bezahlt ist)
- Kündigung bis
- Preis/ Monat
- Zahlungsintervall

## 5. Domain

---

### 5.1 Auflisten

---

Sie sehen eine Auflistung Ihrer Domains mit folgenden Informationen:

- Domain
- Domain Typ
- abgerechnet bis
- Kündigung bis
- Preis/ Jahr
- Verr. ja/nein
- Gekündigt

Für Experten: Über **modify zone** gelangen Sie in den Zonefile-Editor. Hier haben Sie die Möglichkeit DNS-Einträge jeder Ihrer Domains selbst zu verwalten.

Bitte beachten Sie, dass MX-Records nur auf Hostnamen und nicht auf IP-Adressen verweisen dürfen und dass bei Änderung von MX-Records (zuerst bei EDIS, dann extern) Unbedingt Rücksprache mit unserem Support-Team zu halten ist, damit es zu keinen ungewünschten mail-loops kommt.





Domain bearbeiten

Domain

Eintrag hinzufügen  .flashspiele.at

Bestehende Einträge:

	Host	Type	Data
	flashspiele.at	<b>MX10</b>	mail.flashspiele.at
	*.flashspiele.at	<b>A</b>	213.229.30.35
	flashspiele.at	<b>A</b>	213.229.30.35
	mail.flashspiele.at	<b>A</b>	62.99.242.131

Standard-Konfiguration für vHost oder Domain-/Emailweiterleitung wiederherstellen

## 5.2 Datenänderung

Hier haben Sie die Möglichkeit einen Inhaberwechsel zu veranlassen, die eingetragenen Nameserver oder Zone-C und Tech-C Ihrer Domains zu ändern.

(Funktioniert für: .at,.co.at,.or.at,.com,.net,.org,.info,.biz,.cc)

Bitte wählen Sie eine Option:

### Zone-C, Tech-C Update

Domain Update einleiten

Domain

Zone-C  Nur bei .at, .co.at und .or.at Domains relevant

Tech-C

### Inhaberwechsel

Domain Update einleiten

Domain

Inhaber/Admin-C



## Nameserver Update

---

Domain Update einleiten	
Domain	<input type="text"/>
NS1 (Domain, IP)	<input type="text"/> , <input type="text"/>
NS2 (Domain, IP)	<input type="text"/> , <input type="text"/>
<input type="button" value="Zurücksetzen"/> <input type="button" value="Erstellen"/>	

## 5.3 Status

---

Folgende Informationen über laufende bzw. abgeschlossene Transaktionen können hier eingesehen werden: TID (ID), Action (zB register), Domain (Domainname), Datum (Datum und Uhrzeit der Änderung), von (Provider), Status (zB: erfolgreich, abgelehnt), Kommentar

## 5.4 Domaininhaber

---

Zeigt eine Liste der von Ihnen angelegten Inhaber-Handles zum komfortablen Registrieren von Domains.

## 6. Redirect

---

Hier können Sie vorhandene Redirects [Auflisten](#) oder neue [Anlegen](#) .

**Um einen neuen Redirect anzulegen benötigen Sie eine freie Domain, die noch keinem vHost zugeordnet ist!**

## 7. Links

---

Hier finden Sie nützliche Links für die Erstellung von Websites mittels HTML und PHP

- selfHTML (<http://selfhtml.org/>)
- selfPHP (<http://www.selfphp.info/>)
- PHP Archiv (<http://www.php-archiv.de/>)
- Webmail (<http://manage.edis.at/horde/>)



## 8. Support

---

### 8.1 FAQ

---

Die FAQ (Frequently Asked Questions = Häufig gestellte Fragen) sind nach folgenden Kategorien strukturiert:

- Domains, Weiterleitungen (22)
- Webhosts, virtual Hosting (20)
- CMS Systeme, Applikation Server (6)
- eMail, Webmail (12)
- Rack Services, Server housing (3)
- SMS Versand (0)
- Glossar (5)

Sie können sie aber auch mittels Volltextsuche nach Stichwörtern durchsuchen.

### 8.2 Handbuch

---

Der Link zum Handbuch für die Managementoberfläche im PDF-Format.





## Teil 2. vHost-Bereich

---

Der vHost-Bereich ist die Verwaltungs-Oberfläche für Ihren Webserver.

Im **vHost Bereich** melden Sie sich mit Benutzername und Passwort Ihres Webserver an. Die Zugangsdaten für Ihren Webserver entnehmen Sie bitte aus der Email mit dem Betreff

### EDIS.AT: Ihre Zugangsdaten für edis.at (Achtung, nur Beispieldaten!)

---

*Sehr geehrte Damen und Herren,*

*vielen Dank für Ihre Bestellung. Wir freuen uns, dass Sie sich für Produkte von EDIS.AT entschieden haben. Ihr Webserver wurde soeben für Sie eingerichtet. Die Zugangsdaten hierfür lauten wie folgt:*

*Domain: edis.at*

*Username: ed001ped*

*Passwort: AcK2j27c*



## Einstellungen – Übersicht

---


Folgende Bereiche können Sie im vHost bearbeiten:

- Einstellungen > Serveradminpasswort ändern
- Email Adressen
  - Verwaltung > Postfächer und Adressen anlegen, bearbeiten und verwalten.
  - Webmail > Webbasierter Emailclient
- Apache
  - Zugriffsschutz > Schutz für bestehende Ordner vor unbefugten Zugriffen
  - Fehlerseiten > Individualisierung von Fehlermeldungen Ihres Servers
  - SubDomains > Anlegen echter Subdomains (echter vHost!)
  - PHP Version > Zeigt an, welche PHP-Versionen vorhanden sind
- FTP
  - FTP-User > Verwaltung der FTP-User
  - Dateirechte > Zurücksetzen Datei-, Gruppenrechte und Berechtigungen
  - Web-FTP > Managen Sie Dateien auf Ihrem Server einfach über den Browser
- Scripte > einfach zu installieren und gleich verwendbar
  - Gästebuch > Einträge von Gästen
  - Forum > Frage und Antwort, Diskussion
  - Formmail > Um Formulare über das Internet zu verschicken benötigt man einen Formmailer – (dieser ist spamsicher)
- Statistiken
  - Verwaltung > Globale und Domainuser erstellen/bearbeiten
  - Speichernutzung
  - Homepage > Statistik Homepage
- Datenbank
  - Verwaltung > Passwort ändern
  - phpMyAdmin 2.6.1 > Anlegen und Verwalten von Datenbanken
- Links > Nützliche Informationen zum Thema HTML und PHP-Programmierung
  - selfHTML
  - selfPHP
  - PHP Archiv
- Support
  - FAQ
  - Handbuch



## 1. Passwort ändern

Unter **Verwaltung** können Sie das Administrations-Passwort Ihres Webservers (vHost-Bereich) ändern. Geben Sie das neue Passwort ein, bestätigen Sie es und klicken anschließend auf **speichern**.




The screenshot shows a form for changing the administrative password. It includes a blue square icon on the left. The form fields are:

- Benutzername:** f1003ned
- Passwort:** [input field]
- bestätigen:** [input field]
- Emailadresse:** office@flashspiele.at

At the bottom, there is a blue square icon and a **Speichern** button.

## 2. Email-Adressen verwalten

Klicken Sie in der Navigationsleiste links auf **Email Adressen** und anschließend auf **Verwaltung** um zu folgender Auswahl zu gelangen: (Achtung Beispielansicht!) An erster Stelle sehen Sie die den derzeitigen Speicherplatzverbrauch der gesamten Emails, die in diesem vHost angelegt sind.



The screenshot shows the email address management interface. It includes a blue square icon on the left. The interface is divided into three sections:

- aktuelle Mail-Speicherplatznutzung:** Shows a blue square icon, **verbraucht:** 0.00 MB, and **Stand:** 2006-06-07 15:00:14.
- Email Adresse anlegen:** Shows a blue square icon, **Neue Adresse:** [input field] @ ad-games.at [dropdown], and an **anlegen** button.
- Anzeige Einstellungen:** Shows a blue square icon, **Nur Adressen mit der Domain:** -- Zeige Keine -- [dropdown], **Nur diese Adresse:** -- Zeige Keine -- [dropdown], **Expertenansicht:** , and an **anwenden** button.



## 2.1 Neue Email anlegen

Um eine neue Email-Adresse anzulegen, geben Sie den Namen der gewünschten Email-Adresse im Feld neben „Neue Adresse:“ ein und klicken abschließend auf

**anlegen**.

✉ **Email Adresse anlegen:**

Neue Adresse:  @

Sie können nun auswählen ob Sie ein Postfach anlegen wollen Punkt b) (siehe FAQ — Postfach) oder Mails an diese Email-Adresse an ein Ziel (eine oder mehrere beliebige Emailadressen) weiterleiten möchten a).

✉ **Lokale Email-Einstellungen der Adresse test@flashspiele.at**

✉ **Verwendungszweck festlegen:**

**Email - Weiterleitung**  
 **Email - Postfach (Mailbox)**

### a) Email-Weiterleitung

Wählen Sie den Radiobutton  **Email – Weiterleitung**

Tragen Sie in das Feld mit der Überschrift „Ziel“ die gewünschten Empfänger ein. Sie können auch mehrere Empfänger eingeben, in diesem Fall schreiben Sie die Emailadressen ohne Komma untereinander.

✉ **Weiterleitungen einrichten**

**Ziel:** (Weiterleitung nach:)

pro Zeile nur eine Emailadresse!



**Wenn Sie kein Postfach anlegen muss mindestens eine Email-Adresse als Ziel angegeben werden!**

Für Weiterleitungen können Sie auch Spam- und Antivirus-Einstellungen treffen. Da diese Einstellungen sehr vielfältig sind, wird im Kapitel 2.3 genauer darauf eingegangen:-

Zum Abschließen klicken Sie auf **Speichern**.

## b) Postfach (Mailbox) anlegen

Wählen Sie zunächst den Radiobutton  **Email – Postfach (Mailbox)**

**Weiterleitungen einrichten**

**Ziel:** (Weiterleitung nach:)


beispiel@edis.at

pro Zeile nur eine Emailadresse!

vorhandene Weiterleitungen nach office@flashspiele.at anzeigen!

Es ist auch möglich vorhandene Weiterleitungen die im selben vHost eingerichtet wurden und die auf dieses Email-Postfach weiterleiten anzuzeigen. Klicken Sie dazu auf die entsprechende Checkbox.

**Sie können natürlich auch ein Postfach anlegen und zusätzlich Weiterleitungen im Feld „Ziel“ angeben.**

 **Passwort ändern**

**Benutzername:** test@flashspiele.at

**Passwort:**

**bestätigen:**

Neue Zugangsdaten senden an

Hier wird das neue Passwort, die Bestätigung des Passwortes und die Emailadresse, an die die Zugangsdaten gesendet werden sollen eingegeben. Vergeben Sie selbst kein Passwort wird eines von unserem System vorgegeben. Zugangsdaten werden an den zuständigen





Server-Admin gesendet, die Emailadresse kann jedoch jederzeit geändert (übertippt) werden.

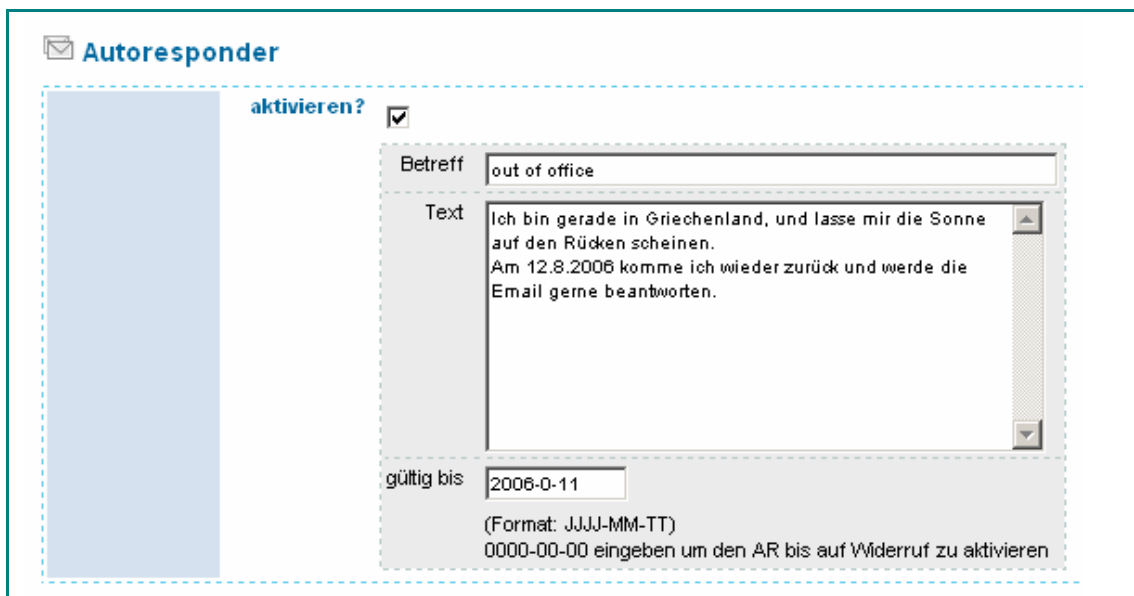
Weiters erscheint ein Fenster mit der Überschrift „Autoresponder“



The screenshot shows a window titled "Autoresponder" with a dashed border. On the left is a large blue rectangular area. To its right, the text "aktivieren?" is followed by an unchecked checkbox.

Die **Urlaubsschaltung** oder **Autoresponder** ist eine Mailserver-Funktion zum automatischen Beantworten von Emails bei Eingang in Ihrem Postfach. Sie haben damit die Möglichkeit in Zeiten längerer Absenz den Absendern von Emails die Information zukommen zulassen, dass Sie länger Ihre Mails nicht lesen können, aber dass deren Email bei Ihnen erfolgreich eingegangen ist.

Wird hier die Checkbox aktiviert, so erscheinen 3 weitere Felder in denen der Emailbetreff, der Emailtext des Autoresponders und der Zeitpunkt bis wann er aktiv sein soll eingegeben werden können. Bitte beachten Sie das Datumsformat: JJJJ-MM-TT also z.B. 2006-12-24 um den Autoresponder bis 24 Dezember 2006 eingeschaltet zu lassen.



The screenshot shows the "Autoresponder" window with the "aktivieren?" checkbox checked. The "Betreff" field contains "out of office". The "Text" field contains the message: "Ich bin gerade in Griechenland, und lasse mir die Sonne auf den Rücken scheinen. Am 12.8.2006 komme ich wieder zurück und werde die Email gerne beantworten." The "gültig bis" field contains "2006-0-11". Below the date field, it says "(Format: JJJJ-MM-TT)" and "0000-00-00 eingeben um den AR bis auf Widerruf zu aktivieren".

Alle Änderungen werden per Email an Ihre office@ Email-Adresse bestätigt



## 2.2 Übersicht der Email-Einstellungen

Wählen Sie zunächst anhand der Dropdowns die Domain und/oder die Emailadresse aus die Sie bearbeiten möchten und klicken Sie anschließend auf **anwenden**.

Es erscheint eine Übersicht mit folgenden Informationen:

**✉ Anzeige Einstellungen:**

Nur Adressen mit der Domain:

Nur diese Adresse:

Expertenansicht:

**anwenden**

Domain / E-Mail	Typ	Aktionen	Quelle	Ziel	Spam	Virus	Greylist	RBL	AutoResp.
<b>FLASHSPIELE.AT</b>	Domain								
@flashspiele.at	Catchall			office@flashspiele.at					
beispiel@flashspiele.at	Email			max.mustermann@gmx.at irgendwer@irgendwo.com		G	G	G	

Wird die Checkbox „Expertenansicht“ aktiviert, so erscheinen zusätzlich die Spalten: Quelle, Ziel und Greylist. in der Standardansicht sind diese Spalten nicht sichtbar.

### Domain/ E-Mail

Die erste Zeile (Domainname in Großbuchstaben, Typ: Domain) betrifft die globalen Spam- und Virenschutzeinstellungen der Domain. Werden in weiterer Folge bei den einzelnen Emailadressen keine lokalen (individuellen) Einstellungen getätigt, gelten die globalen Einstellungen der Domain. Über das Icon können nun diese Spam- und Virenschutzeinstellungen gesetzt werden. Wurden hier der **Spamfilter** **aktiv** gesetzt, erscheint in der Übersicht zusätzlich das Icon über welches die Black/Whitelist-Einträge gewartet werden können.

Die folgenden Zeilen zeigen die vorhandenen Emailadressen an, wobei die erste immer die Catchall-Adresse ist. Diese verwaltet alle Emails die an die gewählte Domain einlangen und nicht eigens eingerichtet sind. Standardmäßig werden diese Emails an die [office@ihredomain.com](mailto:office@ihredomain.com) Adresse weitergeleitet.

**Achtung:** Catchall-Einträge begünstigen die Zustellung von SPAM-Mails! Bitte überdenken, ob diese Funktion wirklich benötigt wird, sonst unbedingt auf inaktiv setzen. Sie können den Catchalleintrag mit dem Icon löschen oder über das Symbol auf inaktiv setzen.



## Typ

---

Mögliche Varianten sind: **Domain**, **Catchall**, **Email** (Weiterleitung) oder **Postfach**

- **Domain** zeigt die globalen Einstellungen für die Email-Adresse innerhalb der gewählten Domain an (siehe oben)
- **Catchall** ist eine Weiterleitung aller Emails die mit @ihredomain.com enden und nicht gesondert eingerichtet sind. Über das Symbol können Sie die gewünschte Weiterleitung einrichten.
- **Email**: diese Email-Adresse wird an eine definierte Zieladresse (siehe Spalte „Weiterleitung nach“) weitergeleitet
- **Postfach**: diese Email-Adresse hat ein eigenes lokales Postfach (POP3/IMAP4 Mailbox) und ist über Webmail oder Mailclient abfragbar.

## Aktionen

---

Je nach Typ gibt es unterschiedliche Funktionen um die Email zu konfigurieren.

**Bearbeiten**: es erscheinen die je nach Typ die Email-Einstellungen

	Weiterleitung	Spam	Autoresponder	Passwort
<b>Domain:</b>	-	ja	-	-
<b>Catchall:</b>	ja	-	-	-
<b>Email:</b>	ja	ja	-	-
<b>Postfach:</b>	ja	ja	ja	ja

**Löschen**: klicken Sie auf den Löschen-Button neben der zu löschenden Email-Adresse. Die Löschung wird per Email an Ihre office@ Email-Adresse bestätigt. **Achtung**: Ab sofort werden Emails an die gelöschte Adresse an jene Adresse zugestellt, die bei der Catchall-Adresse als Ziel eingestellt ist.

**B/W**: Hier warten Sie die Black- und Whitelist-Einträge des Spamfilters. Von Email-Adressen in der Blacklist erhalten Sie nie wieder Emails. Von Adressen in der Whitelist erhalten Sie auch dann Mails, wenn diese vom Spamfilter als Spam identifiziert worden wären. Der Button  erscheint erst, wenn der Spam-Filter aktiv gesetzt ist (Virus- oder Spamprüfung muss nicht aktiviert sein)

### Beispiele für Einträge in Black- oder Whitelists:

@domain.tld -> Catchall Eintrag für eine komplette Domain hinzufügen

name@domain.tld -> Email-Adresse hinzufügen

**Passwort**: Damit können Sie sich die Zugangsdaten des jeweiligen Postfaches zuschicken lassen.



## Quelle

---

Anzeige aller Weiterleitungen am kompletten Mailserver auf die entsprechende eMail-Adresse. Ebenso werden alle Catchall-Adressen (@ihreDomain.com) angezeigt. Achtung: Diese Anzeige ist nur sichtbar wenn die Expertenansicht in den Anzeige Einstellungen aktiviert wurde.

## Ziel

---

Ziele von Weiterleitungen, oder Kopien-Empfänger der jeweiligen eMail-Adresse.

## SPAM, Antivirus, Greylisting, RBL (Realtime Blacklist)

---

Die folgenden 4 Spalten (**Spam**, **Virus**, **Greylist**, **RBL**) zeigen eine Übersicht, welche Spam-Einstellungen gesetzt wurden. Die Häkchen ✓ in der Zeile der Domain zeigen an, dass diese Funktion aktiv ist. **G** und **L** in den Emailzeilen bedeuten, dass diese Bereiche entweder mit globalen (**G**) oder lokalen (**L**) Einstellungen aktiv sind.

## Autoresponder

---




Das Häkchensymbol ✓ zeigt an, dass der Autoresponder eingeschaltet und gültig ist (Datum ist noch nicht abgelaufen).

## 2.3 Spam- und Virenschutzeinstellungen

---

Es sind vielfältige Optionen eingerichtet, die unabhängig voneinander aktiviert werden können. So ist es möglich Ihre eingehenden Emails individuell nach Spam zu selektieren und damit das Spam-Aufkommen auf ein Minimum zu reduzieren ohne gültige Emails zu verlieren. Die Spam-Einstellungen können global für die Domain, oder lokal für jedes Email-Postfach und Weiterleitungen angegeben werden: Die Optionen im Überblick:

- Spamfilter mit Virus- und Spam-Prüfung
- Greylisting
- Realtime Blacklist (DNS basierte Blacklists siehe FAQ -> RBL)
- Black/Whitelist (persönliche Negativ/Positivliste)

Die ersten drei Punkte werden über das Bearbeiten-Symbol  eingerichtet, die Black/Whitelist über das Symbol . (Bitte beachten Sie, dass das  Symbol erst erscheint, wenn der Spamfilter aktiv ist).

Beim Einrichten einer neuen Emailadresse bzw. beim Bearbeiten der EmailEinstellungen lassen sich zunächst folgende Punkte einstellen:



✉ **Spam und Virenschutz**

**Spamfilter:**  verwende globale Spamfilter der Domain  
 setze eigene lokale Spamfilter

**Greylisting:**  verwende globale Einstellungen der Domain **flashspiele.at**  
 **inaktiv** (office@flashspiele.at)  
 **aktiv** (office@flashspiele.at)

**Realtime Blacklist:**  verwende globale Einstellungen der Domain **flashspiele.at**  
 **inaktiv** (office@flashspiele.at)  
 **aktiv** (office@flashspiele.at)

Für Greylisting (siehe 2.3.3) und Realtime Blacklist (RBL siehe 2.3.4) gibt es nur die Einstellung Global, **inaktiv** oder **aktiv**. Wie schon zuvor erwähnt wird die persönliche Black/White-Liste über das  Symbol in der Emailübersicht verwaltet.

„**Verwende globale Einstellungen der Domain**“ bedeutet, dass für diese Emailadresse die in der Email-Übersicht festgelegten Einstellungen für die Domain (siehe Punkt 2.2) verwendet werden. **aktiv** bedeutet Greylisting oder RBL eingeschaltet - **inaktiv** heißt dass die entsprechende Funktion nicht aktiv ist.

Die Einstellungen für den Spamfilter sind komplexer und können für jede Emailadresse ebenfalls individuell (lokal) eingestellt werden. Ansonsten gelten die globalen Einstellungen der Domain.

**Spamfilter:**  verwende globale Spamfilter der Domain  
 setze eigene lokale Spamfilter

Black/White-Liste ist nun **aktiv**

**Virus-Prüfung aktivieren? (Mails werden gelöscht)**

**Spam-Prüfung aktivieren?**

### 2.3.1 Virus-Prüfung

Um die Effizienz der Antivirus-Software zu erhöhen werden zwei unabhängige Viren-Scanner eingesetzt. Findet der erste kein Virus, wird das Email zusätzlich noch vom zweiten Scanner überprüft und erst dann weitergeleitet wenn in beiden Fällen kein Virus entdeckt wurde. Emails in denen Viren entdeckt wurden, werden sofort gelöscht sofern die Checkbox aktiviert wurde, andernfalls werden diese Emails regulär zugestellt.



### 2.3.2 Spamfilter

Mittels des Spam-Reglers kann die Empfindlichkeit des Spam-Filters (vordefinierte presets) eingestellt werden.

In folgendem Beispiel ist der Spam-Regler auf **schwach** gesetzt, d.h es werden nur sehr wenige Emails als Spam erkannt. Es kann also leicht sein, dass eine Email die tatsächlich Spam ist unerkannt bleibt (False-Negative).



Wird der Spam-Regler im Gegenzug **stark** eingestellt, so werden viele Emails als Spam erkannt, und auch die Wahrscheinlichkeit, dass seriöse Emails fälschlicherweise als Spam erkannt werden ist größer (False-Positive)



Wir empfehlen mit einer niedrigen Stufe zu beginnen und die Empfindlichkeit erst Schrittweise zu erhöhen um Fehlresultate zu vermeiden.

Was geschieht nun mit Emails, die als Spam erkannt werden? Hier gibt es 2 Möglichkeiten der Auszeichnung bzw. Verarbeitung der Emails die voneinander unabhängig eingestellt werden können:

- **Auszeichnung X-Spam-Flag im Mailheader**  
Das Email kommt regulär in Ihrem Postfach an, wird aber im Header mit dem X-SPAM-Flag \*\*\* SPAM \*\*\* ausgezeichnet. Wählen sie zusätzlich die Option „zusätzlich Auszeichnung im Betreff“, wird zusätzlich zur Header-Markierung im Betreff der Email der Marker \*\*\* SPAM \*\*\* vorangesetzt. Damit wird der wahrscheinliche Spam-Status der Email noch deutlicher gemacht. So können Sie in Ihrem Mailprogramm beispielsweise eine Regel erstellen, Emails mit dieser Markierung in einen speziellen Ordner zu verschieben oder löschen zu lassen.

- **Quarantäne-action**  
Einstellungen dieses Parameters bewirken Aktionen ab Erreichen des definierten Spam-Scores.

Mögliche Aktionen:



- (1) **Löschen** von Quarantäne-Mails (Standard)
- (2) Weiterleitung in ein **Quarantäne-Postfach** [quarantine@lhredomain.com](mailto:quarantine@lhredomain.com)

**Achtung:**

**Das Quarantäne-Postfach muss zuvor manuell eingerichtet werden!**

**Voreinstellung Empfindlichkeit**

**X-Spam-Flag** Auszeichnung im Mailheader ab score

zusätzlich Auszeichnung \*\*\* SPAM \*\*\* im Betreff

---

**Quarantäne-action** ab score

action: Quarantäne-Mails löschen

action: Quarantäne-Mails an [quarantine@terrassenhaus.at](mailto:quarantine@terrassenhaus.at) weiterleiten

**Wir empfehlen die Option „action: Quarantäne-Mails löschen“ auf keinen Fall zu aktivieren, bevor Sie nicht 100% sicher sind, den optimalen Wert für sich gefunden zu haben!**

**Expertentipp / Benutzerdefinierte Einstellungen:**

Sie können die Spam-Scores für Auszeichnung bzw. Quarantäne-actions auch benutzerdefiniert setzen. So ist z.B. auch die Spam-Markierung in der Betreffzeile ausschaltbar. Sobald Sie einen eigenen Wert in eines der 2 Felder setzen wird die Voreinstellung ausgeblendet und „Benutzerdefinierte Einstellung“ angezeigt.



Der Spam-Score ist ein von SpamAssassin aufgrund von Mail-Analyse errechneter Wert (siehe unten Funktionsweise des Spamfilters).

Grundsätzlich gilt:

- Je höher der Spam-Score eines Emails, desto wahrscheinlicher ist es SPAM.
- Je niedriger der Spam-Score eines Emails, desto wahrscheinlicher ist es ein gültiges Email.



Je höher der Spam-Score im Spamfilter gesetzt wird, desto mehr Emails werden als „gute“ Emails erkannt. Es werden allerdings auch mehr SPAM-Emails, die niedrige Spam-Scores haben „durchrutschen“ (False Positive). Wird zum Beispiel die Quarantäne-action auf 8 gesetzt, so werden alle Emails mit Spam-Scores von -999 bis +7 als positive Email gewertet und die Quarantäne-action erst auf Emails mit Spam-Scores von +8 bis +999 angewandt.

Je niedriger der Spam-Score im Spamfilter gesetzt wird, desto kritischer arbeitet der Filter, es werden viele Emails als SPAM-Mails gewertet, die Wahrscheinlichkeit dass reguläre Mails als SPAM erkannt werden ist aber auch größer (False Negative).

Die Werte der Voreinstellungen dienen als Richtwerte und können je nach Spamaufkommen unterschiedliche Auswirkungen haben.

#### Funktionsweise des Spamfilters (SpamAssassin):

Der Spamfilter prüft (sofern eingeschaltet) alle eingehenden Mails nach diversen Kriterien auf SPAM. Es handelt sich dabei um ein additives Verfahren, d.h. es werden die Emails nach Spam-Merkmalen durchsucht, und je nach gefundenem Spam-Hinweis wird ein entsprechender Wert hinzuaddiert. Dieser Wert kann positiv sein (d.h. höhere Spamwahrscheinlichkeit) oder negativ (d.h. geringere Spamwahrscheinlichkeit). In Summe ergibt sich dann ein Spam-Score.

Normale Emails bewegen sich in den Spam-Scorebereichen von -1 bis +3. Oberhalb von +3 sind die Emails mit großer Wahrscheinlichkeit SPAM.

Beispiel-Analyse mit fiktiven Zahlen:

Mail enthält einen verschlüsselten Abmeldelink: +0.6 Punkte

Mail enthält Begriffe wie „million dollars“: +2 Punkte

Mail enthält eine Zeile  $\geq$  199 Zeichen lang: +1.5 Punkte

ergibt eine Spam-Score von  $0.6 + 2 + 1.5 = 4.1$  Punkte

Sie können den Spam-Score jederzeit im Mailheader eingehender Mails überprüfen (In MS Outlook im geöffneten Mail auf „Ansicht“ + „Optionen“)

```

Internetkopfeilen:  References: <001e01c41b1c$13d86700$1d30df51@power>
                   Content-Type: multipart/alternative;
                   boundary="-----65CB1BEAB4D61406B49F0DD6"
                   X-Virus-Scanned: by EDIS.AT Virus Scanner
                   X-Spam-Status: No, hits=0.0 required=5.0 tests= version=2.20
                   X-Spam-Level:
  
```

Das obige Beispiel würde folgendes aussagen:

X-Virus-Scanned: by EDIS.AT Virus Scanner → Mail wurde vom EDIS.AT Antivirus gescannt

X-Spam-Status: No, hits=0.0 required=5.0 → Mail hat einen Spam-Score von 0.0, der eingestellte → Spam-Score von 5.0 wurde nicht erreicht und somit → email nicht als SPAM klassifiziert.





### 2.3.3 Greylisting

---

Greylisting ist ein effektives Hilfsmittel im Kampf gegen SPAM und funktioniert folgendermaßen:

Wird ein Mail an einen Mailserver der Greylisting unterstützt gesendet, werden folgende Daten aufgezeichnet:

- IP-Adresse des Absender-Mailserver
- Absender-Emailadresse und
- Empfänger-Emailadresse

Ist dieses Dreierpaar noch nicht in der Greylisting-Datenbank verzeichnet, wird es aufgenommen und der Mailserver gibt an den senden Mailserver einen temporären Fehler zurück - das Mail wird vorerst nicht angenommen (soft-error)

Daraufhin versucht der Absender-Mailserver die Email innerhalb weniger Minuten erneut zu senden. Bei diesem Sendeversuch ist das o.g. Dreierpaar bereits vorhanden und der Ziel-Mailserver nimmt das Mail ohne Verzögerung entgegen.

Spam-Versender (meist gehackte Windows-Computer im Internet) kümmern sich im Gegensatz dazu nicht mehr um den Verbleib der abgelehnten Emails und senden diese nicht erneut, womit das Ziel einer effektiven Spam-Bekämpfung erreicht wird.

### 2.3.4 Realtime Blacklists (RBL)

---

RBL bzw. Realtime Blacklists sind DNS-basierte Listen zur Abwehr von unerwünschten Emails.

Die Listen beinhalten offenen Relays, IP-Adressen von gehackten Servern oder DSL-Anschlüssel und Email-Adressen von denen Spam ausgeht. Diese Listen werden von meist non-profit Organisationen gewartet und im 15-Minuten Intervall aktualisiert.

EDIS.AT prüft eintreffende Mails bei Aktivierung von RBL gegen folgende Listen in Echtzeit:

- sbl-xbl.spamhaus.org
- cbl.abuseat.org
- relays.ordb.org
- dul.dnsbl.sorbs.net
- list.dsbl.org
- opm.blitzed.org

Tipp: Die Verwendung von Greylisting und RBL wird dringend empfohlen!

### 2.3.5 White- und Blacklists

---

White- und Blacklists sind Hilfsmittel im Kampf gegen Spam und können über die Emailverwaltung mit dem Symbol  angesprochen werden.



Das Symbol zum bearbeiten der White- und Blacklists erscheint erst wenn der Radiobutton **Spamfilter** in den Email-Einstellungen gesetzt wurde (die **Spam-Prüfung braucht** dazu **nicht** aktiviert zu werden!).

Whitelists enthalten Email-Adressen oder -domänen von denen Mails immer angenommen werden, auch wenn Emails dieser Absender als Spam klassifiziert worden wären.

Beispiel-Einträge in Whitelists:  
support@edis.at @oe.gkk.at (= Catchall)

Blacklists enthalten Email-Adressen oder -domänen von denen Mails generell abgelehnt werden, auch wenn Emails dieser Absender nicht als Spam klassifiziert werden würden.

Beispiel-Einträge in Blacklists:  
hacker@spam.org @microsoft.com (= Catchall)

**White- und Blacklists stehen in der Hierarchie über dem Spamfilter!**

### Hinzufügen einer Email-Adresse bzw. einer -domäne

Geben Sie im Feld Email / Catchall eine Emailadresse oder -domäne (= Catchall) ein und aktivieren entweder den Radiobutton „W“ = Whitelist oder „B“ = Blacklist.

### Löschen einer Email-Adresse bzw. einer -domäne

Sobald Sie einen Eintrag in die White/Blacklist gemacht haben erscheint daneben der Bereich **löschen**. Klicken Sie nun einfach auf Löschen um den Eintrag wieder zu entfernen.

### Importieren von mehreren Email-Adressen bzw. -domänen

Wenn Sie gleich mehrere Email-Adressen einfügen wollen, empfiehlt es sich, diese in Form einer CSV Datei zu importieren. Das ist eine einfache Textdatei mit der Endung .csv oder .txt

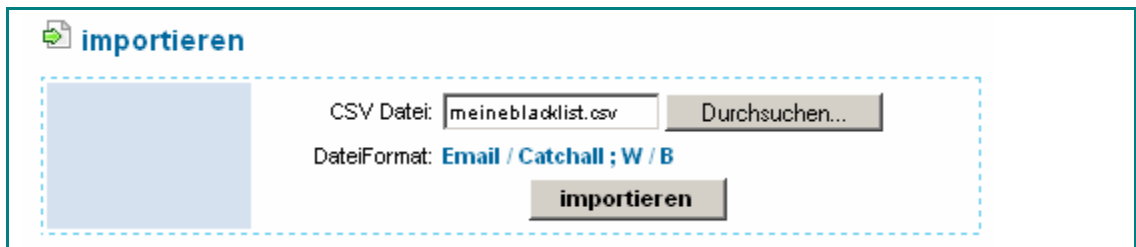


Format: in einer Zeile die Email-Adresse oder Domain und durch Strichpunkt getrennt W oder B.

meineblacklist.txt

```
support@edis.at;W
@oe.gkk.at;W
hacker@spam.org;B
@microsoft.com;B
```

Zum Importieren klicken Sie auf **Durchsuchen** und wählen die Datei im Dialogfenster aus, bestätigen die Auswahl und klicken anschließend auf **Importieren**. Sie können auch hier jederzeit im Bereich **löschen** einzelne Emails löschen.



**importieren**

CSV Datei:

DateiFormat: **Email / Catchall ; W / B**

## 2.4 Abfragen und Senden von Emails mit Webmail



Zum Abfragen Ihrer Emails von Unterwegs nutzen Sie bequem unser Webmailsystem unter <http://webmail.edis.at> bzw. 128bit verschlüsselt unter <https://manage.edis.at/horde>

Einfach einloggen mit Benutzername und Passwort Ihres Email-Kontos.



**Achtung, wenn der Benutzername ungleich Email-Adresse ist (alte Logins)**

**Bevor Sie Emails verschicken können, müssen Sie unbedingt sicherstellen, dass eine gültige Email-Adresse als Absender-Adresse definiert ist.**

**Klicken Sie auf**

**Webmail >> Inbox >> Einstellungen >> Persönliche Angaben >> Identität bearbeiten um eine gültige Email-Adresse zu erfassen (einmalige Handlung)**



### 3. Apache

Apache ist der am häufigsten eingesetzte Webserver im Internet. Der Name wurde aus Respekt vor dem nordamerikanischen Indianerstamm der Apachen gewählt ;-)

Im Bereich Apache können Sie über das Web zugängliche Verzeichnisse schützen, individuelle Fehlerseiten definieren und echte Apache-Subdomains anlegen, ...


#### 3.1 Zugriffsschutz:


Mit der Funktion **Geschützter Bereich** können bereits bestehende Ordner auf Ihrem Webserver vor unbefugten Zugriffen geschützt werden. Es werden sog. `.htaccess` und `.htpasswd` Dateien im jeweiligen Ordner angelegt welche die Schutzinformationen enthalten.

**Achtung! Die Datei „.htaccess“ bzw. „.htpasswd“ darf nicht über FTP gelöscht werden, wenn der Schutz bestehen bleiben soll!**

#### Verzeichnisschutz erstellen

Um ein neues Verzeichnis (Ordner) zu schützen, klicken Sie auf **Apache** und dann auf **Zugriffsschutz** in der linken Navigation, womit Sie zu folgender Eingabemaske gelangen:

 **Verwaltung Apache Zugriffsschutz**

 **Apache Verzeichnisschutz erstellen**

**Verzeichnis:** `/www/home/`

**Bezeichnung Bereich:**

Geben Sie hier **den Namen des zu schützenden Verzeichnisses** sowie eine **Bezeichnung für diesen geschützten Bereich** ein, und klicken Sie auf

#### Verzeichnisschutz Übersicht





Im Bereich **Apache Verzeichnisschutz** sehen Sie eine Übersicht über die vorhandenen geschützten Verzeichnisse und deren zugeordnete User.

 **Apache Verzeichnisschutz**

	Verzeichnis:	Bereich:	
	+ /www/home/private	Geschuetzter Bereich	   

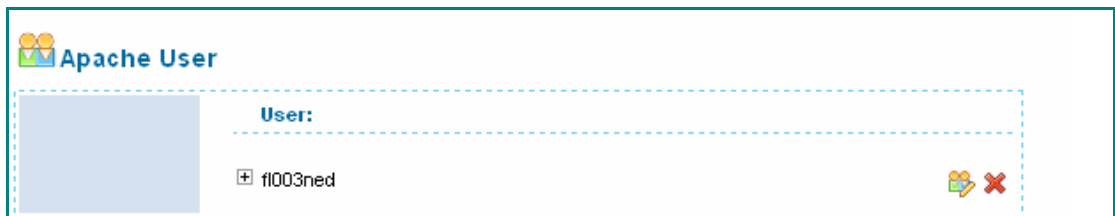





Erklärung zu den Symbolen:

-  Hier kann man die Bezeichnung des Bereichs ändern
-  Dem Verzeichnis einen bestehenden Benutzer zuordnen
-  Dem Verzeichnis einen neuen berechtigten User hinzufügen
-  Den Verzeichnisschutz löschen

## Benutzer bearbeiten

Im Bereich **Apache User** sind die vorhandenen Benutzer aufgelistet.




Sie haben die Möglichkeit einen Benutzer zu löschen () oder das Passwort dieses Benutzers zu ändern (). Hinzufügen eines neuen Benutzers benutzen Sie das Symbol  im Bereich **Apache Verzeichnisschutz**.


## 3.2 Errorsites – Definition von individuellen Fehlerseiten

Um Fehlermeldungen Ihres Webservers zu individualisieren, haben Sie die Möglichkeit für Standard-Fehlercodes z.B. 404 – „Datei nicht gefunden“ eigene Fehlermeldungen auszugeben.

Klicken Sie auf **Apache** und dann auf **Fehlerseiten** in der linken Navigation.

Es erscheint eine Auflistung all Ihrer Domains und Subdomains Ihres Webservers. Über das  Symbol lassen sich die Fehlerseiten je Domain/Subdomain anzeigen.



Über das Bearbeiten-Symbol  können Sie nun folgenden Fehlern individuelle HTML-Seiten zuordnen:



bearbeiten

flashspiele.at

Fehler:	Fehlerseite:	
401	/home/fl003ned/www/home/	<input type="text"/>
402	/home/fl003ned/www/home/	<input type="text"/>
403	/home/fl003ned/www/home/	<input type="text"/>
404	/home/fl003ned/www/home/	<input type="text"/>

Speichern

Error 401: Unauthorized: Zugriff nicht erlaubt

Error 402: Payment required

Error 403: Forbidden

Error 404: Not found

Error 405: Method not allowed

### Error 401: Unauthorized (Nicht autorisiert)

Der Webserver konnte die Datei ohne erfolgreiche Authentifizierung nicht ausliefern. Die aufgerufene Datei liegt in einem kennwortgeschützten Bereich (Siehe 3.1 Verzeichnisschutz). Werden Username oder Passwort falsch eingegeben so erscheint diese Fehlermeldung. Wenn man die Zugangsberechtigung hierfür hat, liegt es oft nur an Tippfehlern (Groß- und Kleinschreibung).

### Error 403: Forbidden (Verboten)

Webserver konnte die Datei nicht ausliefern, da z.B. von einem unbekanntem System zugegriffen wird, die Seiten oder Dokumente generell nicht verfügbar sind oder der Zugriff z.B. auf Verzeichnis-Listings generell nicht erlaubt ist.

### Error 404: Not Found (Nicht gefunden)

Der Webserver konnte die Datei nicht finden, die aufgerufen wurde. Die Ursachen für diese Fehlermeldung können folgende sein: Eingabefehler in der URL (Adresse), das Dokument existiert unter dieser URL nicht mehr oder der Name des Dokuments oder der Dateipfad wurde geändert.

Dies ist der häufigste Fehlercode. Es empfiehlt sich insbesondere für diesen eine freundliche Seite zu gestalten. Es kann leicht passieren, dass ein Link auf Ihrer Seite nicht mehr aktuell ist und schon ist es passiert ...



## Error 405: Method not allowed

---

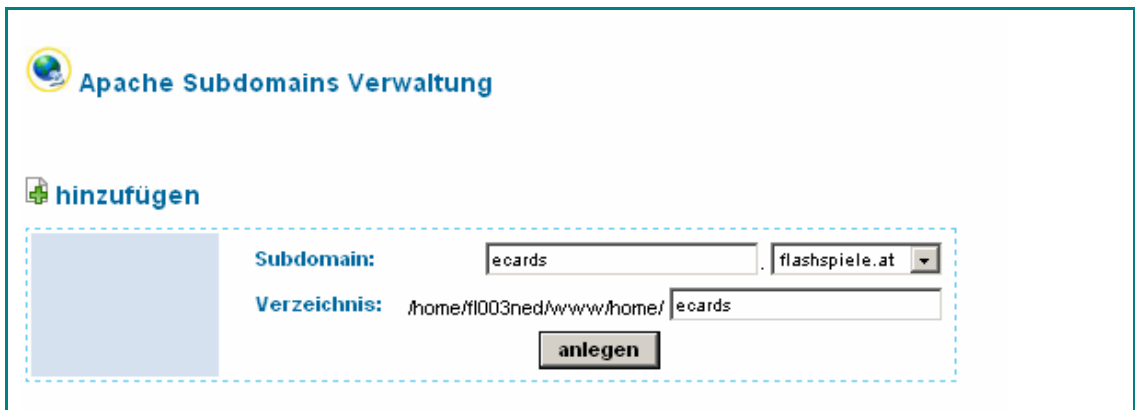
*Was es bedeutet:* Die versuchte Zugriffsmethode ist nicht erlaubt.

*Was Sie tun können:* Vergewissern Sie sich, dass Sie den richtigen MIME-Typ für die angefragte Ressource verwendet haben. Der Server schickt zur "Hilfe" gleich die erlaubten Methoden zurück.

## 3.3 Subdomain:

---

In diesem Bereich können Sie eigene echte\*) Subdomains anlegen, welche in zuvor angelegte Verzeichnisse gemappt werden (echter vHost!).



The screenshot shows a web interface for managing Apache subdomains. At the top left is a globe icon and the text 'Apache Subdomains Verwaltung'. Below this is a green plus icon and the text 'hinzufügen'. The main form area is enclosed in a dashed blue border and contains two rows of input fields. The first row is labeled 'Subdomain:' and has a text input field containing 'ecards' followed by a dropdown menu currently showing 'flashspiele.at'. The second row is labeled 'Verzeichnis:' and has a text input field containing the path '/home/f1003ned/www/home/ecards'. Below these fields is a grey button labeled 'anlegen'.

Im obigen Beispiel würde die Subdomain <http://ecards.flashspiele.at> angelegt werden. Bei Aufruf der Subdomain würde die Homepage aus dem Ordner /www/home/ecards angezeigt werden.

\*) Anmerkung: eine „echte“ Subdomain wird direkt im Webserver konfiguriert und ist mit einem zusätzlichen eigenen Webserver vergleichbar. „unechte“ Subdomains werden über Weiterleitungen sog. Redirects realisiert und haben gegenüber Suchmaschinen enorme Nachteile.

Aber Achtung! Die relativen Verlinkungen in übergeordnete Ordner („../“) gelten nicht mehr, da die Subdomain nicht mehr als Unterordner angesehen wird, sondern wie eine eigenständige Domain behandelt wird!

**Tipp:** Verwalten Sie mit Ihrem virtuellen Server doch mehrere Domains gleichzeitig. Mit dem Subdomain-Tool können Sie auch Subdomains wie z.B. WWW. Anlegen und auf Ihren Zusatzdomains eigene Homepages anzeigen lassen – und das ganz ohne Mehrkosten!







### 3.4 PHP Version

---

Hier können Sie einer .PHP Endung eine PHP-Version zuordnen.  
zZ ist die Auswahl von PHP 4.3.11 oder 5.1.10 gegeben.

 **PHP Version bearbeiten**

 **Domain flashspiele.at**

PHP Endung	Version
.php	4.3.11
.phtml	4.3.11
.php3	4.3.11
.php4	4.3.11
.php5	5.1.10



## 4. FTP

---

FTP (File Transfer Protocol) dient der Übertragung von Dateien (Webseiten) von Ihrem Computer auf den Webserver = **Upload** sowie umgekehrt = **Download**. Dies kann mit Hilfe von so genannten FTP-Programmen vollzogen werden, oder mittels Web-FTP, siehe 4.3.

Um einen Ordner auf dem Webserver ansprechen zu können benötigen Sie einen gültigen Usernamen und ein Passwort (= Zugangsdaten). Die **Zugangsdaten** für Ihren eigenen Webserver entnehmen Sie bitte aus der Email mit dem Betreff

### EDIS.AT: Ihre Zugangsdaten für beispiel.at

---

*Sehr geehrte Damen und Herren,*

*vielen Dank für Ihre Bestellung. Wir freuen uns, dass Sie sich für Produkte von EDIS.AT entschieden haben. Ihr Webserver wurde soeben für Sie eingerichtet. Die Zugangsdaten hierfür lauten wie folgt:*

*Domain: beispiel.at*

*Username: be021ged*

*Passwort: AcK2j27c*

*[...]*

**Achten Sie unbedingt auf „GROSS- und klein“-Schreibung bei Benutzernamen und Passwörtern!**

**FTP ist nicht mit Zugriffsschutz (siehe 3.1) zu verwechseln!**

**Im einen Fall dient der Benutzername und das Passwort zum Anzeigen der Inhalte eines geschützten Verzeichnisses aus dem Browser heraus (http-Protokoll) und ist meist mehreren Usern zugänglich im anderen Fall dient es zum Verändern von Inhalten eines Verzeichnisses über Browser oder FTP-Programm und ist meist nur Administratoren zugänglich (FTP-Protokoll)**



## 4.1 FTP Verwaltung

Sie haben die Möglichkeit für jeden Ordner innerhalb von /www/home auf Ihrem Webserver einen eigenen FTP-Zugang anzulegen. Klicken Sie dazu auf **FTP** und dann auf

**Verwaltung** in der linken Navigation.

**FTP User erstellen**

<b>Verzeichnis:</b>	/home/f1003ned/www/home/	<input type="text"/>
<b>Username:</b>	f1003ned_	<input type="text"/>
<b>Passwort:</b>		<input type="password"/>
<b>bestätigen:</b>		<input type="password"/>

Geben Sie zunächst das Verzeichnis ein, für das Sie einen neuen Benutzer anlegen wollen. Achtung! Das Verzeichnis muss bereits existieren!

Anschließend den Usernamen – dieser beginnt **immer** mit dem Usernamen der vHost-Bereiches – und dann das gewünschte Passwort.

Jetzt können Sie vorhande User auch bearbeiten () , d.h. das Passwort ändern oder den User löschen ().


**FTP User**

	<b>User:</b>	<b>Verzeichnis:</b>	
	f1003ned	/home/f1003ned	
	f1003ned_ecards	/home/f1003ned/www/home/ecards_test	



## 4.2 Dateirechte

Die Funktion Dateirechte ermöglicht es Ihnen die chmod-Einstellungen auf Ihrem gesamten Webserver auf einmal in den Auslieferungszustand zurückzusetzen.

 **Rücksetzen Datei-, Gruppenrechte und Berechtigungen**

**Standardrechte:**

Verzeichnis:

```
drwxr-xr-x f1003ned f1003ned
```

Datei:

```
-rw-r--r-- f1003ned f1003ned
```

**Verzeichnis:** /home/f1003ned/

**Standardrechte neu setzen**


Achten Sie bitte darauf, dass sog. 777er Rechte (r-w-x für user / group und others) bei EDIS nicht notwendig sind und ALLE Scripts mit Standard-Rechten lauffähig sind.

## 4.3 Web-FTP

Web-Ftp ermöglicht es Ihnen, ohne einen eigenständigen FTP-Client (FTP-Programm) Dateien auf Ihren Webserver hinauf- oder herunterzuladen.

Wenn Sie auf **Web-FTP** klicken, kommen Sie auf einen neuen Bereich (FTP –Bereich)..

**Einloggen**



Verbinde zu FTP Server

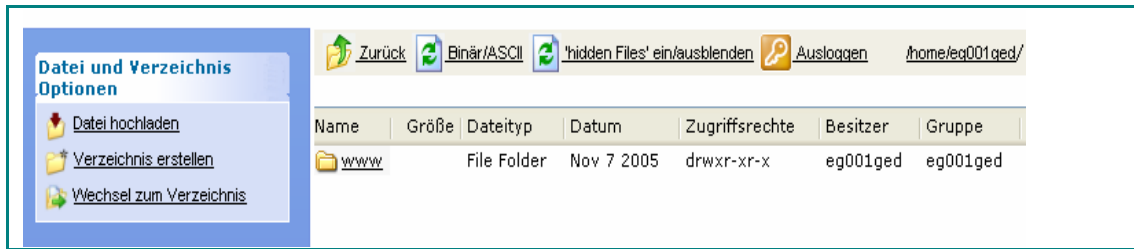
Server **manage.edis.at**

User

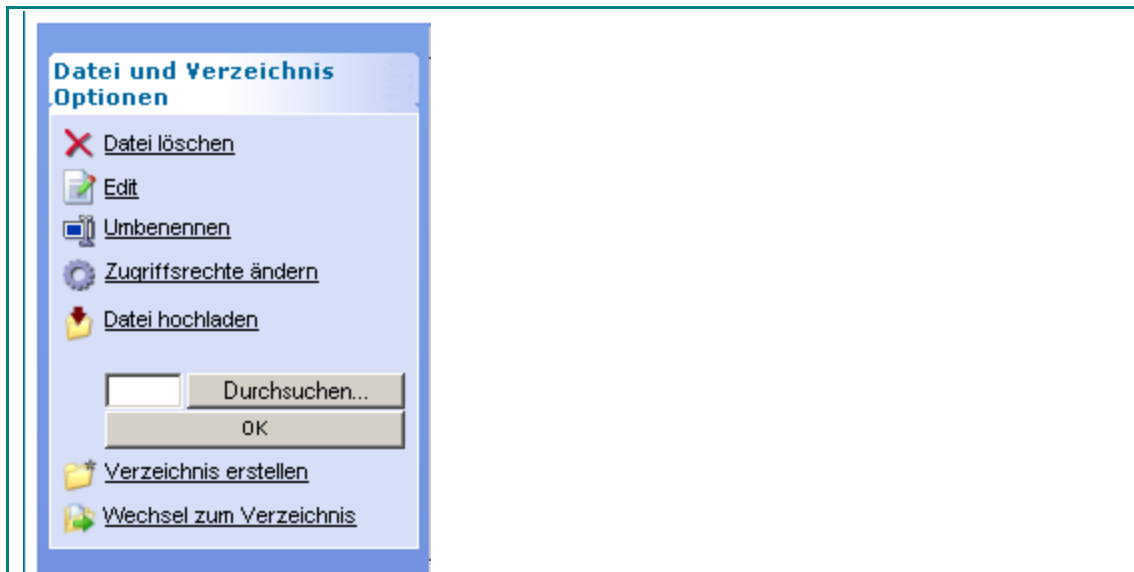
Passwort

Sie werden nun nochmals aufgefordert Ihren Usernamen und Passwort einzugeben. Klicken Sie anschließend auf **Log on**.





Sie haben nun die Möglichkeit, Dateien zu löschen, bearbeiten, umbenennen, die Zugriffsrechte (chmod) zu ändern und schließlich eine Datei hochzuladen.



## Priorität und Name auszuführender Dateien

Um Ihre Homepage automatisch beim Aufruf Ihrer Domain zu starten, muss die Homepage im Ordner **/www/home** abgelegt werden und die auszuführende Datei einen der folgenden Namen haben.

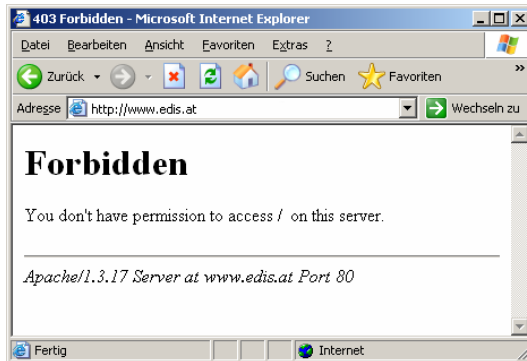
Der Server überprüft auf Existenz folgender Dateien und führt je nach Vorhandensein die Dateien in **folgender Reihenfolge** aus:

- (1) **default.php**
- (2) **index.wml**
- (3) **default.html**
- (4) **index.php**
- (5) **index.php4**
- (6) **index.php3**
- (7) **index.htm**
- (8) **index.html**
- (9) **index.shtml**

Bitte achten Sie auf die Schreibung - alle Dateien **müssen „klein“** (lower-case) geschrieben werden! Linux unterscheidet im Gegensatz zu Windows-Systemen zwischen UPPER- und lowercase Dateinamen. Somit können Dateien wie z.B. default.htm und Default.htm in einem Ordner nebeneinander existieren und zu ungewünschten Verwirrungen führen.



Sie haben Ihre Homepage bereits hochgeladen und sehen noch immer diese „Fehlermeldung“?



Die Meldung „**Forbiddien**“ heißt NICHT, dass Ihr Server nicht funktioniert oder gar dass Sie keine Berechtigungen haben. Die Meldung besagt lediglich, dass im Ordner **/www/home** **keine der oben genannten auszuführenden Dateien gefunden werden konnten!**



## 5. Scripts

### 5.1 Gästebuch

Mit einigen wenigen Angaben können Sie in kürze Ihr eigenes Gästebuch für Ihre Homepage installieren.

#### Gästebuch installieren

Dieses Script installiert und konfiguriert ein Gästebuch-Script für Ihre Homepage. Bitte füllen Sie die folgenden Felder aus.

Verzeichnis:	http://www.flashspiele.at/	<input type="text"/>
Datenbank Name:	f1003ned_	<input type="text"/>
Admin Name:		<input type="text" value="f1003ned"/>
Admin Passwort:		<input type="password" value="*****"/>
Admin Passwort bestätigen :		<input type="password" value="*****"/>
Admin Email:		<input type="text" value="office@flashspiele.at"/>
Tabellenname Einträge:		<input type="text" value="inno_gb_eintraege"/>
Tabellenname Adminlog:		<input type="text" value="inno_gb_admin"/>

Bitte beachten Sie, dass Sie noch nicht vorhandene Verzeichnis- und Datenbanknamen wählen

### 5.2 Forum

Das Script installiert das bekannte phpBB Forum, wahlweise in Version 2.0.5 oder 2.0.18

#### Forum installieren

Dieses Script installiert das von Ihnen gewählte Forum Script. Klicken Sie auf den Versionsnamen um zu einer Demo zu gelangen.

Ziel Verzeichnis:	http://www.flashspiele.at/	<input type="text"/>
Datenbank Name:	f1003ned_	<input type="text"/>
Version:		<input type="radio"/> phpBB 2.0.5 <input checked="" type="radio"/> phpBB 2.0.18

### 5.3 Formmail

Um Emails über den Server verschicken zu können, benötigt man einen Formmailer. Dieser wird hier beispielhaft beschrieben und eine Vorlage als Download bereitgestellt.






## 6. Statistiken


### 6.1 Verwaltung

Sie haben die Möglichkeit mehrere User anzulegen, welche die Rechte haben Zugriffs-Statistiken anzusehen. Einerseits können Sie mehrere globale User anlegen die die gesamten Statistiken des vHosts einsehen können. Zusätzlich ist es aber auch noch möglich für jede Ihrer Domänen weitere berechnigte User anzulegen. Damit wird es ermöglicht, Ihren Kunden von der Hauptseite getrennte Statistiken anzubieten.

Die ersten beiden Bereiche dienen dem Anzeigen und Erstellen/Bearbeiten der **globalen User**. Geben Sie hier einfach einen neuen Benutzernamen und das Passwort ein.



**Global-User anzeigen (<http://statistics.at/f1003ned>)**

	User:	Link:	
	f1003ned	<a href="http://statistics.at/f1003ned">http://statistics.at/f1003ned</a>	 



**Global-User erstellen/bearbeiten (<http://statistics.at/f1003ned>)**

	Username: <input type="text" value="f1003ned"/>		
	Password: <input type="password"/>		
	bestätigen: <input type="password"/>		
<input type="button" value="speichern"/>			

Um Domain-User anzulegen, wählen Sie in dem letzten Bereich zunächst eine Domain und geben dann Username und Passwort ein. Im oberen Bereich werden alle Domainuser angezeigt, und über den **Link** können gleich die Statistiken angesehen werden.


**Domain-User anzeigen (<http://statistics.at/DomainName>)**

	Domain:	User:	Link:


**Domain-User erstellen/bearbeiten (<http://statistics.at/DomainName>)**

	Domain: <input type="text"/>		
	Username: <input type="text"/>		
	Password: <input type="password"/>		
	bestätigen: <input type="password"/>		
<input type="button" value="speichern"/>			





Beim ersten Login sind die Usernamen und Passwort für FTP, vHost und globale Statistiken identisch. Sie können aber für alle Bereiche individuelle Passwörter erstellen.

## 6.2 Speichernutzung

Sie sehen eine Auflistung der Speicherplatznutzung für die Bereiche Web (FTP), Datenbank und Mail. Über die Symbole [+] bekommen Sie eine detaillierte Aufgliederung des Speicherplatzverbrauches für Datenbanken und Postfächer.

**i Web - Speicherplatznutzung**

	<b>Verzeichnis:</b> /home/f1003ned/
	<b>bezahlt:</b> 100.00 MB
	<b>verbraucht:</b> 101.68 MB
	<b>Stand:</b> 2006-06-07 11:52:18

**i Datenbank - Speicherplatznutzung**

	<b>Datenbank:</b> mysql01:f1003ned*
	<b>verbraucht:</b> 6.89 MB
	<b>Stand:</b> 2006-06-08 11:28:39
	<b>Detailinfo:</b> 

**i Mail - Speicherplatznutzung**

	<b>Mailserver:</b> mail.flashspiele.at
	<b>verbraucht:</b> 0.00 MB
	<b>Stand:</b> 2006-06-08 11:28:39
	<b>Detailinfo:</b> 

## 6.3 Homepage

Hier öffnet sich ein neues Fenster und Sie haben nun die Möglichkeit, mit ihrem Usernamen und Passwort die Statistiken Ihrer Domain oder die globalen Statistiken anzusehen.



## 7. Datenbank

### 7.1 Verwaltung

In diesem Unterpunkt können Sie aktuell den Speicherplatzverbrauch Ihrer Datenbanken ablesen. Zukünftig wird hier das Anlegen von MySQL-Benutzern und deren Verwaltung möglich sein.

**i** **aktuelle Datenbank-Speicherplatznutzung:**

	<b>Datenbank:</b>	mysql01:fl003ned*
	<b>verbraucht:</b>	<b>6.89 MB</b>
	<b>Stand:</b>	2006-06-08 11:28:39

### 7.2 phpMyAdmin 2.6.1

Über den Link auf [phpMyAdmin](#) gelangen Sie zur Administration Ihrer MySQL-Datenbanken.

Der erste Schritt, ist das **Anlegen einer eigenen Datenbank**. Die **Syntax zur Namensvergabe** ist **strikt einzuhalten**, da sonst keine Datenbank angelegt werden kann.

Syntax: **Benutzername\_Datenbankname** (z.B. fa004ned\_topshop)

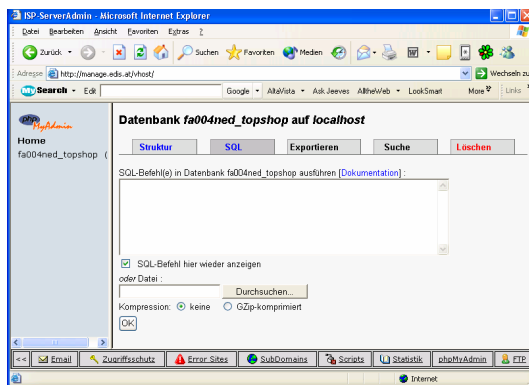


Sie können beliebig viele Datenbanken anlegen. Wenn Sie sich nicht an die Namens-Syntax (siehe oben) halten, kann keine Datenbank angelegt werden und es wird folgende Fehlermeldung ausgegeben:

`CREATE DATABASE `test``  
MySQL meldet:

**Access denied for user: 'fa004ned@10.1.1.11' to database 'test'**

Richtig wäre `CREATE DATABASE `fa004ned_test``



Danach können nach Ihren Wünschen Tabellen innerhalb ihrer Datenbanken angelegt werden

An dieser Stelle können Sie bereits mit **Standard SQL Befehlen** Ihre **Tabellen** in der Datenbank **anlegen** bzw. **Abfragen ausführen**.

## PHP und MySQL



Um mit Ihrem PHP-Script eine Verbindung auf den Datenbank-Server herzustellen verwenden Sie Benutzernamen und Passwort Ihres Webservers.

Als Datenbank-Host geben Sie „mysql01“ oder 10.1.1.21 an.

„localhost“ sollte aus Performance- und Sicherheitsgründen NICHT verwendet werden.

Ein einfacher Connect könnte z.B. so aussehen:

```
mysql_connect("mysql01", "Username", "Passwort");
```

```
mysql_select_db("Datenbankname z.B. fa004ned_hotspot");
```

```
$result=mysql_query("SELECT feld1, feld2 FROM tabelle1");
```



Tipp: Als Nachschlagewerke empfehlen wir das Buch „php – dynamische Webauftritte professionell realisieren“ vom Verlag Markt & Technik ISBN 3-8272-5524-4

Der Schwerpunkt dieses Buches liegt dabei auf der am häufigsten anzutreffenden Kombination: einem Linuxsystem mit Apache-Webserver, MySQL-Datenbank und PHP.

#### Ressourcen im Internet:

- <http://at.php.net/manual/de/>
- <http://www.php-archiv.de/>

## 8. Links

---

Hier finden Sie nützliche Links für die Erstellung von Websites mittels HTML und PHP

- selfHTML
- selfPHP
- PHP Archiv

## 9. Support

---

### 9.1 FAQ

---

Die FAQ (Frequently Asked Questions = Häufig gestellte Fragen) sind nach folgenden Kategorien strukturiert:

- Domains, Weiterleitungen (22)
- Webhosts, virtual Hosting (20)
- CMS Systeme, Applikation Server (6)
- eMail, Webmail (12)
- Rack Services, Server housing (3)
- SMS Versand (0)
- Glossar (5)

Sie können sie aber auch mittels Volltextsuche nach Stichwörtern durchsuchen.

### 9.2 Handbuch

---

Der Link zum Handbuch für die Managementoberfläche im PDF-Format.





## Teil 3. Email-Bereich

---

### 1. Email Adresse

#### 1.1 Lokale Email

---

Hier gelten die gleichen Einstellungen wie bei **Teil 2 (vHost) Punkt 2.1.b.**

#### 1.2 White/Blacklist

---

Diese ist nur aktiv, wenn der Spamfilter für diese Email (bzw. Domain) aktiviert wurde. Ansonsten kommt die Fehlermeldung:

**Für die Emailadresse 'office@domainname.at' wurde kein SpamAssassin aktiviert!**  
Bitte gehen Sie [zurück](#) und berichtigen Sie Ihre Angaben.

Die Beschreibung der White/Blacklist finden Sie im **Teil 2 (vHost) Punkt 2.3.5.**

### 2. Support

---

#### 2.1 FAQ

---

Die FAQ (Frequently Asked Questions = Häufig gestellte Fragen) sind nach folgenden Kategorien strukturiert:

- Domains, Weiterleitungen (22)
- Webhosts, virtual Hosting (20)
- CMS Systeme, Applikation Server (6)
- eMail, Webmail (12)
- Rack Services, Server housing (3)
- SMS Versand (0)
- Glossar (5)

Sie können sie aber auch mittels Volltextsuche nach Stichwörtern durchsuchen.

#### 2.2 Handbuch

---

Der Link zum Handbuch für die Managementoberfläche im PDF-Format.





## Teil 4. FTP-Bereich

---

Loggen Sie sich in den FTP-Bereich mit Ihrem FTP-Usernamen und Passwort ein.

### 1. Passwort ändern

---

Hier können Sie Ihr FTP-Passwort ändern

### 2. phpWebFTP

---

Beschreibung siehe [Teil 2 \(vHost\) Punkt 4.3](#)





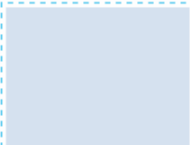
## Teil 5. Passwort-zusenden

Falls Sie Ihr Kunden-Passwort vergessen haben sollten, können Sie es sich hier an Ihre eingetragene Email (Kunden oder Rechnungsadresse) zukommen lassen. Zur Verifizierung haben Sie die Möglichkeit Ihre Kundennummer (oben) anzugeben oder die bei uns eingetragene Emailadresse (unten). Sie bekommen anschließend sofort Ihre Kundennummer und Ihr Passwort zugeschickt.

### ... über KundenNr.

	<b>KundenNr.:</b> <input type="text"/>
	<b>Übermittlung der Zugangsdaten an:</b> <input type="text" value="Kunden Emailadresse"/>
	<input type="button" value="anfordern"/>

### ... über Empfänger-Email

	<b>Email-Adresse.:</b> <input type="text"/>
	<b>Übermittlung der Zugangsdaten an:</b> <input type="text" value="Kunden Emailadresse"/>
	<input type="button" value="anfordern"/>

