



WLAN Benutzerhandbuch

Hochschule Albstadt-Sigmaringen

Inhaltsverzeichnis

Einrichtung des WLAN
Voraussetzungen für Drahtlosnetzwerk (WLAN) an der Hochschule Albstadt-Sigmaringen 4
Einrichtung des WLAN unter Windows 7 4
Einrichtung des WLAN unter Windows 8.1
Netzlaufwerk verbinden
Voraussetzung für den Zugriff auf Netzlaufwerke
Netzlaufwerk verbinden unter Windows 7
Netzlaufwerk verbinden unter Windows 8.114
Pfade16
Drucken im WLAN17
Voraussetzungen für das Drucken im WLAN 18
Drucker verbinden unter Windows 718
Drucker verbinden unter Windows 8.1

Dieses Buch wurde für die Angehörigen der Hochschule Albstadt-Sigmaringen verfasst.

Die IT-Abteilung bietet an beiden Standorten ein Drahtlosnetzwerk (WLAN) an. Sie können damit kabellos auf das Internet und auf das Hochschulnetzwerk und damit auf Ihre persönlichen Daten und E-Mails an der Hochschule zugreifen.

Dieses Buch soll Ihnen bei der Einrichtung des Zugangs helfen. Es wird nach Bedarf aktualisiert. Bitte benutzen Sie stets die aktuelle Version des Buches.

Version 1.1

Kapitel 1

Einrichtung des WLAN

In diesem Kapitel:

- Voraussetzungen f
 ür Drahtlosnetzwerk (WLAN) an der Hochschule Albstadt-Sigmaringen
- Einrichtung des WLAN unter Windows 7
- Einrichtung des WLAN unter Windows 8.1

Voraussetzungen für Drahtlosnetzwerk (WLAN) an der Hochschule Albstadt-Sigmaringen

- ➢ Es gilt die Benutzungsordnung für externen Zugang zum Hochschulnetz. Dieses Dokument finden Sie auf den Webseiten der IT-Abteilung unter <u>www.hs-albsig.de/it</u> → Services → WLAN → "Benutzungsordnung.pdf"
- Eine WLAN-Karte
- Sie müssen sich auf dem Campus der Hochschule befinden

Einrichtung des WLAN unter Windows 7



Einrichtung des WLAN

5. Klicken Sie auf "Verbindungseinstellungen	6. Klicken Sie auf die Registerkartei
ändern".	"Sicherheit".
Construction of the second sec	Verbindung Sicherheit
hs-intern wurde erfolgreich hinzugefügt	Name: hs-intern
→ Verbindungseinstellungen ändern	Solu: ns-mem Netzwerktyp: Zugrifspunkt
Öffnet die Verbindungseigenschaften, um die Einstellungen ändern zu können.	Rezwerkverlugbarkeis Alle behutzer
	ist Mit einem verfügbaren bevorzugten Netzwerk verbinden
	Verbinden, selbst wenn das Netzwerk seinen Namen nicht sendet (SSID)
Schließen	
	OK Abbrechen
7. Klicken Sie auf "Einstellungen".	8. Wählen Sie das Zertifikat "Deutsche
Eigenschaften für Drahtlosnetzwerk hs-intern	I elekom Root CA 2" aus.
	Beim Herstellen der Verbindung:
Sicherheitstyp: WPA2-Enterprise Verschlüssekingstyp: AES	Serverzertifikat überprüfen
	Verbindung mit diesen Servern herstellen:
Wählen Sie eine Methode für die Netzwerkauthentlifzierung aus:	Vertrauenswürdige Stammzertifizierungsstellen:
Für diese Verbindung eigene Anmeldeinformationen für jede Anmeldung seichern	ComSign Secured CA
	Cyberrust Global Root Deutsche Telekom Root CA 2
	Diglect Assured ID Root G2
Erweiterte Einstellungen	
	Keine Benutzeraufforderung zur Autorisierung neuer Server oder vertrauenswürdiger Zertifizierungsstellen
	Authentifizierungsmethode auswählen:
	Gesichertes Kennwort (EAP-MSCHAP v2) Konfigurieren
	Schnelle Wiederherstellung der Verbindung aktivieren Netzwerkzugriffsschutz erzwingen
	Verbindung trennen, wenn Server kein Kryptografiebindungs-TLV vorweist
	aktivieren
	OK Abbrechen

Kapitel 1 Einrichtung des WLAN	
9a. Wenn Sie Ihren privaten Rechner benutzen, klicken Sie auf "Konfigurieren" und überprüfen Sie, ob diese Option deaktiviert ist. Bestätigen Sie mit "OK". Sestätigen Sie mit "OK". Sestätigen Sie Mit "OK". Sestätigen Sie Mit "OK". Sestätigen Sie Mit "OK". Sestätigen Sie Mit "OK". Sestätigen Sie Mit "OK". Sestätigen Sie Mit Mot Sie Mit Mot Sie Mit Mit Sie Mi	9b. Wenn Ihr Rechner Eigentum der Hochschule und Teil der Hochschuldomäne ist, können Sie auf "Konfigurieren" klicken und die Benutzung des Windows-Accounts für die automatische Anmeldung am WLAN aktivieren. Fgenschaften für geschützte EAP Fur Hentelen der Vetindung: Und Kenwort Ind Doniene, fals vorhenden) Und Kenwort (EAP-MSCHAP v2) und Kenwort (EAP-MSCHAP v2) Und Kenwort (EAP-MSCHAP v2) und Kenweren Understauenswirdiger Zeitfischung attwieren Understauenswirdiger Zeitfischung attwieren
10. Klicken Sie auf "Erweiterte Einstellungen". Figenschaften für Drahtlosnetzwerk hs-intern Verbindung Sicherheit Sicherheitstyp: Verschlüsselungstyp: AES Wahlen Sie eine Methode für die Netzwerkauthentfiberung aus: Microsoft: Geschlütztes EAP (PEAP) Einstellungen Fiele Anmeldung speichern OK	11. Wählen Sie als Authentifizierungsmethode Benutzerauthentifizierung" aus. Bestätigen Sie mit "OK".
12. Geben Sie Ihre Anmeldedaten ein. Windows-Sicherheit Vetzwerkauthentifizierung Geben Sie die Benutzeranmeldeinformationen ein. ad-fhas\IhrBenutzeraccount oK Abbrechen	

Einrichtung des WLAN unter Windows 8.1

Die schnellere Variante...



Kapitel 1	Einrichtu	ng des WLAN		
🕑 Netzwerke				
Flugzeugmodus				
Aus				
Mobiles Breitban Aus	d I			
WiFi				
Ein	_			
ull hs-intern				
🖌 Automatisch verbi	nden			
	Verbinden			
WLAN-FHAS				
Ausgeblendetes I	Netzwerk			

Falls die schnellere Variante nicht funktioniert...

1. Klicken Sie rechts unten auf das WLAN- Symbol. Öffnen Sie das "Netzwerk- und Freigabecenter". Problembehandlung Netzwerk- und Freigabecenter öffnen 14:33 13.06.2014	2. Klicken Sie auf "Neue Verbindung oder neues Netzwerk einrichten".
 3. Klicken Sie auf "Manuell mit einem	 4. Geben Sie als Netzwerkname "hs-intern"
Funknetzwerk verbinden". Erstellen Sie	ein. Wählen Sie als Sicherheitstyp "WPA2-
anschließend ein neues Netzwerkprofil. Image: Sie Sie Sie Sie Sie Sie Sie Sie Sie Sie	baterprise" aus. Klicken Sie auf "Weiter". Image: Manuell mit einem Funknetzwerk verbinden Image: Manuell mit einem Funknetzwerk keine Kennung aussendet Image: Manuell mit einem das Netzwerk keine Kennung aussendet Image: Manuell mit einem Geben Sterner für der Datenschutz dieses Computers gst. gefahrdet. Image: Manuell mit einem Geben Sterner für der Datenschutz dieses Computers gst. gefahrdet. Image: Manuell mit einem Geben Sterner für der Datenschutz dieses Computers gst. gefahrdet. Image: Manuell mit einem Geben Sterner für der Datenschutz dieses Computers gst. gefahrdet. Image: Manuell mit einem Geben Sterner für der Datenschutz dieses Computers gst. gefahrdet. Image: Manuell mit einem Geben Sterner für der Datenschutz dieses Computers gst. gefahrdet. Image: Manuell Mit einem Geben Sterner für der Datenschutz dieses Computers gst. gefahrdet. Image: Manuell Mit einem Geben Sterner für der Datenschutz dieses Computers gst. gefahrdet. Image: Manuell Mit einem Geben Sterner für der Datenschutz dieses Computers gst. gefahrdet. Image: Manuell Mit einem Geben Sterner für der Datenschutz dieses Computers gst. gefahrdet. Image: Manuell Mit einem Geben Sterner für der Datenschutz dieses Computers gst. gefahrdet. Image: Manuell Mit einem Geben Sterner für der Datenschutz dieses Computers gst. gefahrdet.

	Sicharbait#
X	Eigenschaften für Drahtlosnetzwerk hs-intern
📀 🔮 Manuell mit einem Funknetzwerk verbinden	Verhindung
hs-intern wurde erfolgreich hinzugefügt	Schemer
	Name: hs-intern
Verbindungseinstellungen ändern Offnet die Verbindungseinenschaften um die Einstellungen ändern	SSID: hs-intern
zu können.	Netzwerktyp: Zugriffspunkt
	Netzwerkverfügbarkeit: Alle Benutzer
	Automatisch verbinden, wenn dieses Netzwerk in Reichweite ist
	Bei hergestellter Verbindung mit diesem Netzwerk andere
	Funknetzwerke suchen
	Verbinden, selbst wenn das Netzwerk seinen Namen nicht sendet (SSID)
Schließen	
	OK Abbrechen
	OK Abreaten
7. Klicken Sie auf "Einstellungen".	8. Wählen Sie das Zertifikat "Deutsche
Eigenschaften für Drahtlosnetzwerk hs-intern	Telekom Root CA 2" aus.
	Eigenschaften für geschütztes EAP
Verbindung Sicherneit	Beim Herstellen der Verbindung:
Sicherheitstyp: WPA2-Enterprise V	
	✓ Identität des Servers mittels Zertifikatprüfung überprüfen
Verschlüsselungstyp: AES	✓ Identität des Servers mittels Zertifikatprüfung überprüfen Verbindung mit folgenden Servern herstellen (Beispiele: "srv1", "srv2", ".*\.srv3\.com"):
Verschlüsselungstyp: AES 🗸	✓ Identität des Servers mittels Zertifikatprüfung überprüfen Verbindung mit folgenden Servern herstellen (Beispiele: "srv1", "srv2", ".*\.srv3\.com"):
Verschlüsselungstyp: AES 🗸	✓ Identität des Servers mittels Zertifikatprüfung überprüfen Verbindung mit folgenden Servern herstellen (Beispiele: "srv1", "srv2", ".*\.srv3\.com"):
Verschlüsselungstyp: AES v	Identität des Servers mittels Zertifikatprüfung überprüfen Verbindung mit folgenden Servern herstellen (Beispiele: "srv1", "srv2", ".*\.srv3\.com"): Vertrauenswürdige Stammzertifizierungsstellen: AddTrust External CA Root
Verschlüsselungstyp: AES Wählen Sie eine Methode für die Netzwerkauthentifizierung aus: Microsoft: Geschütztes EAP (PEAP) Einstellungen	Identität des Servers mittels Zertifikatprüfung überprüfen Verbindung mit folgenden Servern herstellen (Beispiele: "srv1", "srv2", ".*\.srv3\.com"): Vertrauenswürdige Stammzertifizierungsstellen: AddTrust External CA Root Baltimore CyberTrust Root Cherg 2 Della Deren Service in the interval of the service in th
Verschlüsselungstyp: AES Wählen Sie eine Methode für die Netzwerkauthentifizierung aus: Microsoft: Geschütztes EAP (PEAP) Einstellungen	 ✓ Identität des Servers mittels Zertifikatprüfung überprüfen Verbindung mit folgenden Servern herstellen (Beispiele: "srv1", "srv2", ".*\.srv3\.com"): Vertrauenswürdige Stammzertifizierungsstellen: AddTrust External CA Root AddTrust External CA Root Class 3 Public Primary Certification Authority ✓ Deutsche Telekom Root CA 2
Verschlüsselungstyp: AES Wählen Sie eine Methode für die Netzwerkauthentifizierung aus: Microsoft: Geschütztes EAP (PEAP) Einstellungen Für diese Verbindung eigene Anmeldeinformationen für jede Anmeldung speichern	 ✓ Identität des Servers mittels Zertifikatprüfung überprüfen Verbindung mit folgenden Servern herstellen (Beispiele: "srv1", "srv2", ".*\.srv3\.com"): Vertrauenswürdige Stammzertifizierungsstellen: AddTrust External CA Root Baltimore CyberTrust Root Class 3 Public Primary Certification Authority ✓ Deutsche Telekom Root CA 2 DiglCert Assured ID Root CA
Verschlüsselungstyp: AES Wählen Sie eine Methode für die Netzwerkauthentifizierung aus: Microsoft: Geschütztes EAP (PEAP) Einstellungen Für diese Verbindung eigene Anmeldeinformationen für jede Anmeldung speichern	Identität des Servers mittels Zertifikatprüfung überprüfen Verbindung mit folgenden Servern herstellen (Beispiele: "srv1", "srv2", ".*\.srv3\.com"): Vertrauenswürdige Stammzertifizierungsstellen: AddTrust External CA Root Baltimore CyberTrust Root Class 3 Public Primary Certification Authority Deutsche Telekom Root CA 2 DiglCert Assured ID Root CA Equifax Secure Certificate Authority Ceatrust Clabal CA
Verschlüsselungstyp: AES Wählen Sie eine Methode für die Netzwerkauthentifizierung aus: Microsoft: Geschütztes EAP (PEAP) Einstellungen Für diese Verbindung eigene Anmeldeinformationen für jede Anmeldung speichern	 ✓ Identität des Servers mittels Zertifikatprüfung überprüfen Verbindung mit folgenden Servern herstellen (Beispiele: "srv1",
Verschlüsselungstyp: AES Wählen Sie eine Methode für die Netzwerkauthentifizierung aus: Microsoft: Geschütztes EAP (PEAP) Einstellungen Für diese Verbindung eigene Anmeldeinformationen für jede Anmeldung speichern	Identität des Servers mittels Zertifikatprüfung überprüfen Verbindung mit folgenden Servern herstellen (Beispiele: "srv1", "srv2", ".*\.srv3\.com"): Vertrauenswürdige Stammzertifizierungsstellen: AddTrust External CA Root Baltimore CyberTrust Root Class 3 Public Primary Certification Authority Deutsche Telekom Root CA 2 DigiCert Assured ID Root CA Equifax Secure Certificate Authority GeoTrust Global CA Class 1 Public Primary Lettority
Verschlüsselungstyp: AES Wählen Sie eine Methode für die Netzwerkauthentifizierung aus: Microsoft: Geschütztes EAP (PEAP) Einstellungen Image: Für diese Verbindung eigene Anmeldeinformationen für jede Anmeldung speichern	Identität des Servers mittels Zertifikatprüfung überprüfen Verbindung mit folgenden Servern herstellen (Beispiele: "srv1", "srv2", ".*\.srv3\.com"): Vertrauenswürdige Stammzertifizierungsstellen: AddTrust External CA Root Baltimore CyberTrust Root Class 3 Public Primary Certification Authority Øeutsche Telekom Root CA 2 DigiCert Assured ID Root CA Equifax Secure Certificate Authority GeoTrust Global CA ClabelCize Deut CA Benachrichtigungen vor der Verbindungsherstellung:
Verschlüsselungstyp: AES Wählen Sie eine Methode für die Netzwerkauthentifizierung aus: Microsoft: Geschütztes EAP (PEAP) Für diese Verbindung eigene Anmeldeinformationen für jede Anmeldung speichern Erweiterte Einstellungen	 ✓ Identität des Servers mittels Zertifikatprüfung überprüfen Verbindung mit folgenden Servern herstellen (Beispiele: "srv1",
Verschlüsselungstyp: AES Wählen Sie eine Methode für die Netzwerkauthentifizierung aus: Microsoft: Geschütztes EAP (PEAP) Einstellungen Image: State of the s	 ✓ Identität des Servers mittels Zertifikatprüfung überprüfen Verbindung mit folgenden Servern herstellen (Beispiele: "srv1",
Verschlüsselungstyp: AES Wählen Sie eine Methode für die Netzwerkauthentifizierung aus: Microsoft: Geschütztes EAP (PEAP) Für diese Verbindung eigene Anmeldeinformationen für jede Anmeldung speichern Erweiterte Einstellungen	Identität des Servers mittels Zertifikatprüfung überprüfen Verbindung mit folgenden Servern herstellen (Beispiele: "srv1", "srv2", ".*\.srv3\.com"): Vertrauenswürdige Stammzertifizierungsstellen: AddTrust External CA Root Baltimore CyberTrust Root Class 3 Public Primary Certification Authority Deutsche Telekom Root CA 2 DigiCert Assured ID Root CA Equifax Secure Certificate Authority GeoTrust Global CA Class 3 Public Primary Certification Authority Benachrichtigungen vor der Verbindungsherstellung: Benutzer benachrichtigen, wenn die Serveridentität nicht überpi v Authentifizierungsmethode auswählen: Gesichertes Kennwort (EAP-MSCHAP v2) Konfigurieren
Verschlüsselungstyp: AES Wählen Sie eine Methode für die Netzwerkauthentifizierung aus: Microsoft: Geschütztes EAP (PEAP) Für diese Verbindung eigene Anmeldeinformationen für jede Anmeldung speichern Erweiterte Einstellungen	✓ Identität des Servers mittels Zertifikatprüfung überprüfen Verbindung mit folgenden Servern herstellen (Beispiele: "srv1", "srv2", ".*"\.srv3\.com"): Vertrauenswürdige Stammzertifizierungsstellen: AddTrust External CA Root Baltimore CyberTrust Root Class 3 Public Primary Certification Authority ✓ Deutsche Telekom Root CA 2 DigiCert Assured ID Root CA Equifax Secure Certificate Authority GeoTrust Global CA Class 10 Dut CA Benutzer benachrichtigen, wenn die Serveridentität nicht überpi ∨ Authentifizierungsmethode auswählen: Gesichertes Kennwort (EAP-MSCHAP v2) ✓ Konfigurieren
Verschlüsselungstyp: AES Wählen Sie eine Methode für die Netzwerkauthentifizierung aus: Microsoft: Geschütztes EAP (PEAP) Einstellungen Image: State of the state o	Verbindung mit folgenden Servern herstellen (Beispiele: "srv1",
Verschlüsselungstyp: AES Wählen Sie eine Methode für die Netzwerkauthentifizierung aus: Microsoft: Geschütztes EAP (PEAP) Einstellungen Image: State of the s	Identität des Servers mittels Zertifikatprüfung überprüfen Verbindung mit folgenden Servern herstellen (Beispiele: "srv1", "srv2", ".*\.srv3\.com"): Vertrauenswürdige Stammzertifizierungsstellen: AddTrust External CA Root Baltimore CyberTrust Root Class 3 Public Primary Certification Authority Deutsche Telekom Root CA 2 DigiCert Assured ID Root CA Equifax Secure Certificate Authority GeoTrust Global CA clutteries Port 64 Benachrichtigungen vor der Verbindungsherstellung: Benachrichtigen, wenn die Serveridentität nicht überpi Authentifizierungsmethode auswählen: Gesichertes Kennwort (EAP-MSCHAP v2) Konfigurieren Schnelle Wiederherstellung der Verbindung aktivieren Netzwerkzugriffsschutz erzwingen Verbindung trennen, wenn Server kein
Verschlüsselungstyp: AES Wählen Sie eine Methode für die Netzwerkauthentifizierung aus: Microsoft: Geschütztes EAP (PEAP) Für diese Verbindung eigene Anmeldeinformationen für jede Anmeldung speichern Erweiterte Einstellungen OK Abbrechen	Identität des Servers mittels Zertifikatprüfung überprüfen Verbindung mit folgenden Servern herstellen (Beispiele: "srv1", "srv2", ".*\.srv3\.com"): Vertrauenswürdige Stammzertifizierungsstellen: AddTrust External CA Root Baltimore CyberTrust Root Class 3 Public Primary Certification Authority Vertrauenswürdige Stammzertifizierungsstellen: Class 3 Public Primary Certification Authority Vertrauenswürdige Stammer Certification Authority Vertrauenswürdige Stammary Certification Authority Vertrauenswürdige Telekom Root CA 2 DigiCert Assured ID Root CA Equifax Secure Certificate Authority GeoTrust Global CA Classification Context Carteria Context Ca
Verschlüsselungstyp: AES Wählen Sie eine Methode für die Netzwerkauthentifizierung aus: Microsoft: Geschütztes EAP (PEAP) Einstellungen Image: State in the image of the i	Verbindung mit folgenden Servern herstellen (Beispiele: "srv1", "srv2", ".*\.srv3\.com"): Vertrauenswürdige Stammzertifizierungsstellen: AddTrust External CA Root Baltimore CyberTrust Root Class 3 Public Primary Certification Authority Deutsche Telekom Root CA 2 DiglCert Assured ID Root CA Equifax Secure Certificate Authority GeoTrust Global CA Clisterie Deut Ca Senachrichtigungen vor der Verbindungsherstellung: Benutzer benachrichtigen, wenn die Serveridentität nicht überpi v Authentifizierungsmethode auswählen: Gesichertes Kennwort (EAP-MSCHAP v2) Schnelle Wiederherstellung der Verbindung aktivieren Netzwerkzugriffsschutz erzwingen Verbindung trennen, wenn Server kein Kryptografiebindungs-TLV vorweist
Verschlüsselungstyp: AES Wählen Sie eine Methode für die Netzwerkauthentifizierung aus: Microsoft: Geschütztes EAP (PEAP) Für diese Verbindung eigene Anmeldeinformationen für jede Anmeldung speichern Erweiterte Einstellungen OK Abbrechen	Verbindung mit folgenden Servern herstellen (Beispiele: "srv1", "srv2", ".*\.srv3\.com"): Vertrauenswürdige Stammzertifizierungsstellen: AddTrust External CA Root Baltimore CyberTrust Root Class 3 Public Primary Certification Authority Deutsche Telekom Root CA 2 DigiCert Assured ID Root CA Equifax Secure Certificate Authority GeoTrust Global CA clubelcie Deut Ct Authentifizierungsmethode auswählen: Gesichertes Kennwort (EAP-MSCHAP v2) Schnelle Wiederherstellung der Verbindung aktivieren Netzwerkzugriffsschutz erzwingen Verbindung trennen, wenn Server kein Kryptografiebindungs-TLV vorweist Identitätsschutz aktivieren

17 -		1 4	
ка	hITe		
nа	ρπυ		

Einrichtung des WLAN

9a. Wenn Sie Ihren privaten Rechner benutzen, klicken Sie auf "Konfigurieren" und überprüfen Sie, ob diese Option deaktiviert ist. Bestätigen Sie mit "OK".	9b. Wenn Ihr Rechner Eigentum der Hochschule und Teil der Hochschuldomäne ist, können Sie auf "Konfigurieren" klicken und die Benutzung des Windows-Accounts für die eutomatische Anmeldung om WLAN
Eigenschaften für geschütztes EAP	aktivieren.
EAP-IVISCHAPV2-Eigenschalten	Eigenschaften für geschütztes EAP
Beim Herstellen der Verbindung:	EAP-MSCHAPv2-Eigenschaften
Utomatisch eigenen Windows-Anmeldenamen und ennwort (und Domäne, falls vorhanden) verwenden	Beim Herstellen der Verbindung:
OK Abbrechen	utomatisch eigenen Windows-Anmeldenamen und ennwort (und Domäne, falls vorhanden) verwenden
Class 3 Public Primary Certification Authority	OK Abbrechen
Deutsche Telekom Root CA 2	Clase 3 Public Primary Cartification Authority
Equifax Secure Certificate Authority	Class S Public Printary Certification Automy Deutsche Telekom Root CA 2
GeoTrust Global CA	DigiCert Assured ID Root CA
	Equifax Secure Certificate Authority
	GeoTrust Global CA
Benachrichtigungen vor der Verbindungsherstellung:	< >
Benutzer benachrichtigen, wenn die Serveridentität nicht überp ı \checkmark	Benachrichtigungen vor der Verbindungsherstellung:
Authentifizierungsmethode auswählen:	Benutzer benachrichtigen, wenn die Serveridentität nicht überpi $ \checkmark $
Gesichertes Kennwort (EAP-MSCHAP v2)	
	Authentifizierungsmethode auswahlen:
	Gesichertes Kennwort (EAP-MSCHAP v2) Konfigurieren
Netzwerkzugrinsschutz erzwingen	Schnelle Wiederherstellung der Verbindung aktivieren
Kryptografiebindungs-TLV vorweist	Netzwerkzugriffsschutz erzwingen
	Verbindung trennen, wenn Server kein
	Kryptografiebindungs-TLV vorweist
OK Abbrechen	Identitätsschutz aktivieren
	OK Abbrechen
10 Klicken Sie auf Erweiterte Einstellungen"	11 Wählen Sie als Authentifizierungsmethode
Figure a la figure file Desktlage strengt ha intern	Reputzerauthentifizierung" aus Bestätigen
Elgenschaften für Drantiosnetzwerk ns-Inter	Sie mit OK''
Verbindung Sicherheit	
	Erweiterte Einstellungen
	802.1X-Einstellungen 802.11-Einstellungen
Sicherheitstyp: WPA2-Enterprise V	Authentifizierungsmodus angeben:
Verschlüsselungstyp: AES	
	Anmeldeinformationen speichern
	Anmeldeinformationen für alle Benutzer löschen
Wählen Sie eine Methode für die Netzwerkauthentifizierung aus:	
Microsoft: Geschütztes EAP (PEAP) V Einstellungen	LINMaliges Anmelden für dieses Netzwerk aktivieren
Für diese Verbindung eigene Anmeldeinformationen für	Onmittelbar vor der Benutzeranmeldung ausführen
jede Anmeldung speichern	Unmittelbar nach der Benutzeranmeldung ausführen
	Maximale verzogerung (Sekunden); 10
	Anzeige zusätzlicher Dialoge während des einmaligen Anmeldens zulassen
	In diesem Netzwerk werden für die Computer- und
	die Benutzerauthentifizierung separate virtuelle LANs
Erweiterte Einstellungen	verwender.
L	
OK Abbrechen	OK Abbrechen

17.			4
Ka	116	21	
1000			

12 Geben Sie Ihre Anmeldedaten ein	
Netzwerke	
Netzwerkanforderungen werden	
Anmelden	
ad-fhas\IhrBenutzeraccount	
••••••	
Domäne: ad-fhas	
OK Abbrechen	

Kapitel 2

Netzlaufwerk verbinden

In diesem Kapitel:

- Voraussetzung für den Zugriff auf Netzlaufwerke
- Netzlaufwerk verbinden unter Windows 7
- Netzlaufwerk verbinden unter Windows 8.1
- Pfade

Voraussetzung für den Zugriff auf Netzlaufwerke

> WLAN-Verbindung zum Hochschulnetz

Netzlaufwerk verbinden unter Windows 7

1. Starten Sie den Windows Explorer. Klicken Sie "Netzlaufwerk verbinden" an.



 Geben Sie den Pfad ein. Im Bild wird gezeigt wie der Pfad zum Info-Laufwerk aussieht¹. Deaktivieren Sie die Option "Verbindung bei Anmeldung wiederherstellen" und aktivieren Sie die Option "Verbindung mit anderen Anmeldeinformationen herstellen"². Bestätigen Sie anschließend mit "Fertig stellen".

🕞 😪 Netzlauf	werk verbinden		
Welcher Bestimme hergestell	Netzwerkordner soll zugeordne n Sie den Laufwerkbuchstaben für die Ver twerden soll:	t werden? bindung und de	n Ordner, mit dem die Verbindung
Laufwerk:	[l: 👻		
Ordner:	\\ad.fh-albsig.de\info Beispiel: \\Server\Freigabe ☐ Verbindung bei Anmeldung wiederh ☑ Verbindung mit anderen Anmeldeinf <u>Verbindung mit einer Website hersteller</u> <u>können</u>	← erstellen formationen her: <u>auf der Sie Do</u> ł	Durchsuchen stellen sumente und Bilder speichern
		ĺ	Fertig stellen Abbrechen

 Sie werden nach Ihren Anmeldedaten gefragt. Vergessen Sie nicht die Domäne der Hochschule anzugeben ad.fh-albsig.de\IhrBenutzername, sonst bekommen Sie später beim Zugriff auf Verzeichnisse eine Fehlermeldung! Der Benutzername und das Passwort sind dieselben, die Sie zum Anmelden an einem Hochschulrechner angeben.

Vindows-Sicherh Netzwerkke Geben Sie das ad.fh-albsig.de	eit ennwort eingeben Kennwort ein, um eine Verbindung herzustellen mit:
	ad.fh-albsig.de\IhrBenutzername Kennwort Domäne: ad.fh-albsig.de
	Smartcard einlegen
	OK Abbrechen

Netzlaufwerk verbinden unter Windows 8.1

1. Starten Sie den Windows Explorer, klicken Sie auf "Computer" und auf "Netzlaufwerk verbinden".



 Geben Sie den Pfad ein. Im Bild wird gezeigt wie der Pfad zum Info-Laufwerk aussieht. Deaktivieren Sie die Option "Verbindung bei Anmeldung wiederherstellen" und aktivieren Sie die Option "Verbindung mit anderen Anmeldeinformationen herstellen". Bestätigen Sie

Netzlaufwerk verbinden

anschließend mit "Fertig stellen".

Bestimmer	n Sie den Laufwerkbuchstaben für die Verbindung und den Ordner, mit dem die
Verbindun	g hergestellt werden soll:
Laufwerk:	l: ~
Ordner:	\\ad.fh-albsig.de\info
	Beispiel: \\Server\Freigabe
	Verbindung bei Anmeldung wiederherstellen
	/erbindung mit anderen Anmeldeinformationen herstellen
	Verbindung mit einer Website herstellen, auf der Sie Dokumente und Bilder speichern können

 Sie werden nach Ihren Anmeldedaten gefragt. Vergessen Sie nicht die Domäne der Hochschule anzugeben ad.fh-albsig.de\IhrBenutzername, sonst bekommen Sie später beim Zugriff auf Verzeichnisse eine Fehlermeldung! Der Benutzername und das Passwort sind dieselben, die Sie zum Anmelden an einem Hochschulrechner angeben.



Netzlaufwerk verbinden

Pfade

Info-Laufwerk:

\\ad.fh-albsig.de\info

Home-Laufwerk für Studenten:

\\ad.fh-albsig.de\stud\IhrStudiengang\IhrBenutzername

Home-Laufwerk für Professoren und Mitarbeiter:

\\ad.fh-albsig.de\ma\IhrStudiengang\IhrBenutzername

Bei einigen Professoren und Mitarbeitern der Fakultät 3 kann sich der Pfad unterscheiden:

\\ad.fh-albsig.de\ma\f3\IhrBenutzername

Kapit	el 3		
Drucken im WLAN			
In diesem Kapitel:	 Voraussetzungen für das Drucken im WLAN Drucker verbinden unter Windows 7 Drucker verbinden unter Windows 8.1 		

Voraussetzungen für das Drucken im WLAN

> WLAN-Verbindung zum Hochschulnetz

Drucker verbinden unter Windows 7

Um einen Drucker zu verbinden, gehen sie wie folgt vor:

- 1. Wählen Sie Menü "Start" ⇒ "Ausführen…" aus.
- 2. Geben Sie im Eingabefeld "Öffnen" den Druckerserver ein: \\izcpm1.ad.fh-albsig.de
- 3. Geben Sie Ihren Benutzernamen und Ihr Passwort ein. Vor Ihrem Benutzernamen müssen Sie zusätzlich **ad.fh-albsig.de**\ eingeben, z.B. so: **ad.fh-albsig.de**\IhrBenutzername.
- 4. Eine Liste mit verfügbaren Druckern wird angezeigt. Suchen Sie den Drucker "Follow Me", klicken Sie ihn mit der rechten Maustaste an und wählen Sie "Verbinden…" aus. Ein Treiber wird installiert, der Drucker wird verbunden und Sie können Ihr Dokument ausdrucken.

Drucker verbinden unter Windows 8.1

Um einen Drucker zu verbinden, gehen sie wie folgt vor:

 Starten Sie den Windows Explorer und geben Sie den Namen des Druckservers ein: <u>\izcpm1.ad.fh-albsig.de.</u>



2. Geben Sie Ihren Benutzernamen und Ihr Passwort ein. Vor Ihrem Benutzernamen müssen Sie zusätzlich **ad.fh-albsig.de**\ eingeben, z.B. so: **ad.fh-albsig.de**\IhrBenutzername.

Windows-Sicherheit	×
Netzwerkanmeldeinformationen eingeben Geben Sie Ihre Anmeldeinformationen ein, um eine Verbindung mit folgendem Netzwerk herzustellen: izcpm1.ad.fh-albsig.de	
ad.fh-albsig.de\lhrBenutzername	
Domäne: ad.fh-albsig.de	
😵 Der Benutzername bzw. das Kennwort ist falsch.	
OK Abbreck	nen

3. Eine Liste mit verfügbaren Druckern wird angezeigt. Suchen Sie den Drucker "Follow Me", klicken Sie ihn mit der rechten Maustaste an und wählen Sie "Verbinden…" aus. Ein Treiber wird installiert, der Drucker wird verbunden und Sie können Ihr Dokument ausdrucken.

