# Acronis Access

## Anleitung zu Installation und Upgrade

## Urheberrechtserklärung



## Von Acronis patentierte Technologien

Die in diesem Produkt verwendeten Technologien werden durch einzelne oder mehrere U.S.-Patentnummern abgedeckt und geschützt: 7,047,380; 7,275,139; 7,281,104; 7,318,135; 7,353,355; 7,366,859; 7,475,282; 7,603,533; 7,636,824; 7,650,473; 7,721,138; 7,779,221; 7,831,789; 7,886,120; 7,895,403; 7,934,064; 7,937,612; 7,949,635; 7,953,948; 7,979,690; 8,005,797; 8,051,044; 8,069,320; 8,073,815; 8,074,035; 8,145,607; 8,180,984; 8,225,133; 8,261,035; 8,296,264; 8,312,259; 8,347,137; 8,484,427; 8,645,748; 8,732,121 sowie schwebende Patentanmeldungen.

# Inhaltsverzeichnis

# 1 Installation

**Themen**



## 1.1 Voraussetzungen

Zum Installieren von Acronis Access müssen Sie als Administrator angemeldet sein. Überzeugen Sie sich, dass Sie folgende Anforderungen erfüllen:

**Themen**



### 1.1.1 Anforderungen an das Betriebssystem

**Empfohlen:**
Windows 2012, alle Varianten
Windows 2008 R2 64 Bit

**Unterstützt:**
Windows 2012 R2
Windows 2012, Standard und Datacenter Edition
Windows 2008, alle Varianten, 32/64 Bit
Windows 2003 SP2 oder höher

***Hinweis:*** *Bei Installation auf einer Maschine mit einem Windows Server 2003-Betriebssystem muss* ***Microsoft Core XML Services (MSXML) 6.0*** *installiert sein, damit das Konfigurationswerkzeug funktioniert.*

***Hinweis:*** *Das System kann zu Testzwecken unter Windows 7 oder höher installiert und ausgeführt werden. Diese Desktop-Konfigurationen werden jedoch nicht für Produktionsumgebungen unterstützt.*

### 1.1.2 Anforderungen für den mobilen Client

Die mobile Client-Applikation ist kompatibel mit:

**Von der Access Mobile Client-Applikation unterstützte Geräte:**

- Apple iPad 2., 3., 4. Generation
- Apple iPad Mini 1., 2. Generation
- Apple iPhone 3GS, 4, 4S, 5, 5s, 5c

- Apple iPod Touch 4., 5. Generation
- Android-Smartphones und -Tablets (Geräte mit x86-Prozessorarchitektur werden nicht unterstützt)

**Von der Access Mobile Client-Applikation unterstützte Betriebssysteme:**

- iOS 6 oder höher
- Android 2.2 oder höher (Geräte mit x86-Prozessorarchitektur werden nicht unterstützt)

**Die Access Mobile Client-Applikation kann heruntergeladen werden von:**

- Für iOS http://www.grouplogic.com/web/meappstore
- Für Android https://play.google.com/store/apps/details?id=com.grouplogic.mobilecho

### 1.1.3 Minimale Hardware-Empfehlungen

**Prozessor:** Intel/AMD

***Hinweis:*** *Acronis Access Server können auf virtuellen Maschinen installiert werden.*

**Arbeitsspeicher:**

- Umgebungen für produktiven Einsatz: mindestens 8 GB. Mehr wird empfohlen.
- Testumgebungen: mindestens 4 GB. Mindestens 8 GB werden empfohlen.

**Speicherplatz:**

- Die Software-Installation erfordert 300 MB Speicherplatz.

  ***Hinweis:*** *Stellen Sie sicher, dass genügend Speicherplatz zum Ausführen des Installationsprogramms von Acronis Access vorhanden ist. Für die Ausführung des Installationsprogramms wird 1 GB Speicherplatz benötigt.*

- Das von den Sync & Share-Funktionen verwendete Datei-Repository wird standardmäßig auf dem lokalen Computer installiert.
- Sorgen Sie für ausreichend freien Speicherplatz, um die Testparameter zu erfüllen. Mindestens 50 GB werden empfohlen.

### 1.1.4 Netzwerkanforderungen

- 1 Statische IP-Adresse. Für bestimmte Konfigurationen werden 2 IP-Adressen benötigt.
- Optional, jedoch empfohlen: DNS-Namen für die obigen IP-Adressen.
- Netzwerkzugriff auf einen Domain Controller, falls Active Directory verwendet wird.
- Netzwerkzugriff auf den SMTP-Server für E-Mail-Benachrichtigungen und Einladungen.
- Die Adresse **127.0.0.1** wird vom Access Mobile Client intern verwendet und darf nicht durch einen Tunnel wie VPN, MobileIron, Good Dynamics usw. geleitet werden.
- Alle Computer, auf denen der Access Server oder der Gateway Server ausgeführt werden, müssen an Windows Active Directory gebunden sein.

Es gibt zwei Komponenten, die HTTPS-Verkehr verarbeiten: der Gateway Server und der Acronis Access-Server. Der Gateway Server wird von mobilen Clients für den Zugriff auf Dateien und Freigaben aus den Datenquellen verwendet. Der Access Server stellt die Webbenutzeroberfläche für Sync & Share-Clients bereit und fungiert zudem als Verwaltungskonsole sowohl für Mobile Access als auch Sync & Share. Es wird empfohlen, dem Server zwei IP-Adressen und zwei separate DNS-Einträge für diese Adressen zuzuweisen. Der Server kann aber auch so konfiguriert werden, dass nur eine IP-Adresse verwendet wird, aber mit verschiedenen Ports für die jeweilige Komponente. Diese Konfiguration mit nur einer IP-Adresse reicht für die meisten auf Mobile Access beschränkten Installationen aus. Zwei IP-Adressen werden jedoch empfohlen, wenn auch Sync & Share verwendet wird.

**Falls Sie zulassen wollen, dass mobile Geräte auch von außerhalb Ihrer Firewall zugreifen dürfen, haben Sie mehrere Optionen:**

- **Zugriff über Port 443**: Da Acronis Access HTTPS für die verschlüsselte Übertragung verwendet, entspricht es von sich aus den üblichen Firewall-Regeln, die HTTPS-Verkehr über Port 443 zulassen. Wenn Sie den Zugriff über Port 443 auf den Acronis Access-Server zulassen, können autorisierte iPad-Clients innerhalb oder außerhalb der Firewall eine Verbindung aufbauen. Acronis Access kann jedoch auch für die Verwendung eines anderen Ports Ihrer Wahl konfiguriert werden.
- **VPN:** Der Access Mobile Client unterstützt den Zugriff über eine VPN-Verbindung. Sowohl der integrierte iOS VPN-Client als auch VPN-Clients von Drittanbietern werden unterstützt. iOS-Verwaltungsprofile können optional auf Geräte angewendet werden, die MDM-Systeme (Mobile Device Management) oder das Apple iPhone-Konfigurationswerkzeug verwenden, um die zertifikatsbasierte iOS-Funktion 'VPN auf Anforderung' zu konfigurieren, die nahtlosen Zugriff auf Acronis Access-Server und andere Unternehmensressourcen bietet.
- **Reverse Proxy-Server:** Falls ein Reverse Proxy-Server eingerichtet ist, können Clients für iPad eine Verbindung herstellen, ohne hierfür einen offenen Firewall-Port oder eine VPN-Verbindung zu benötigen. Die Access Mobile Client-App unterstützt die Reverse-Proxy-Pass-Through-Authentifizierung, die Authentifizierung mit Benutzername/Kennwort, die Authentifizierung per eingeschränkter Kerberos-Delegierung und die Zertifikatsauthentifizierung. Detaillierte Informationen zum Hinzufügen von Zertifikaten zur Access Mobile Client-App finden Sie im Artikel Client-Zertifikate verwenden.
- **Good Dynamics-fähige** Access Mobile Client**-App:** Die Access Mobile Client-App kann sowohl für die Good Dynamics-Plattform registriert als auch von dieser Plattform verwaltet werden. In dieser Konfiguration wird die gesamte Netzwerkkommunikation zwischen Access Mobile Clients und Gateway Servern über den geschützten Good Dynamics-Kommunikationskanal und den Good Proxy-Server geleitet. Weitere Einzelheiten hierzu finden Sie im Handbuch zu Access Mobile Client für Good Dynamics.
- **Für MobileIron AppConnect registrierte Access Mobile Client-App**: Wenn die Access Mobile Client-Applikation bei der MobileIron's AppConnect-Plattform registriert ist, kann die gesamte Netzwerkkommunikation zwischen Access Mobile Client-Clients und Gateway Servern über MobileIron Sentry geleitet werden. Weitere Informationen finden Sie in der Anleitung zu MobileIron AppConnect.

**Zertifikate:**
Acronis Access wird zu Testzwecken mit selbstsignierten Zertifikaten ausgeliefert und installiert. Für Produktionsumgebungen sollten geeignete CA-Zertifikate verwendet werden.

- **Hinweis:** Einige Webbrowser zeigen bei Verwendung von selbstsignierten Zertifikaten eine Warnmeldung an. Wenn Sie diese Warnmeldungen schließen, können Sie das System problemlos nutzen. Die Verwendung von selbstsignierten Zertifikaten unter Produktionsbedingungen wird nicht empfohlen.

### 1.1.5 Voraussetzungen für Desktop-Client

**Unterstützte Betriebssysteme:**

- Windows XP, Windows Vista, Windows 7, Windows 8 und 8.1
- Mac OS X 10.6.8 und höher, wenn Mac mit 64-Bit-Software kompatibel ist.

***Hinweis:*** *Stellen Sie bei der Installation des Acronis Access Desktop Clients sicher, dass der Sync-Ordner, den Sie erstellen, sich nicht in einem Ordner befindet, der von einer anderen Software synchronisiert wird. Eine Liste bekannter Konflikte finden Sie unter Konflikte verursachende Software.*

**Unterstützte Webbrowser:**

- Mozilla Firefox 6 und höher
- Internet Explorer 8 und höher (Internet Explorer 8 wird nicht für Server-Administration unterstützt)

***Hinweis:*** *Stellen Sie bei Nutzung von Internet Explorer sicher, dass die Option* ***Verschlüsselte Seiten nicht auf dem Datenträger speichern*** *deaktiviert ist, damit Sie Dateien herunterladen können. Öffnen Sie dazu* ***Internetoptionen*** *>* ***Erweitert*** *>* ***Sicherheit****.*

- Google Chrome
- Safari 5.1.10 oder höher

## 1.2 Acronis Access auf Ihrem Server installieren

Mit den folgenden Schritten können Sie eine Erstinstallation durchführen und Acronis Access mit HTTPS und dem bereitgestellten selbstsignierten Zertifikat testen.

***Hinweis:*** *Anweisungen zu Upgrades finden Sie im Abschnitt zu Upgrades (S. 19).*

***Hinweis:*** *Anweisungen zum Installieren in einem Cluster finden Sie im Abschnitt Acronis Access in einem Cluster installieren.*

Die Installation von Acronis Access besteht aus drei Schritten:

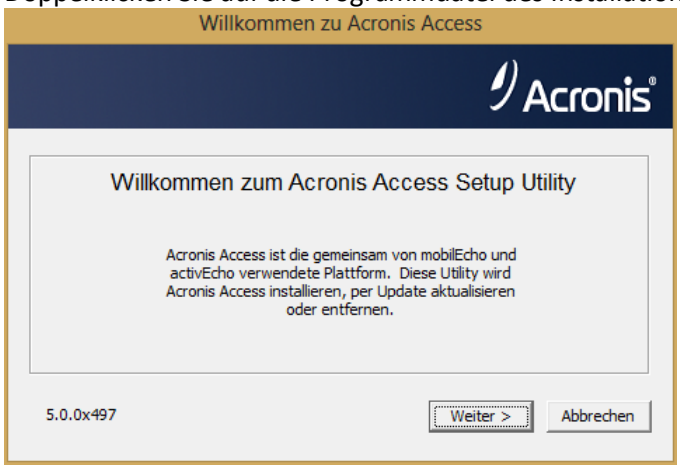
1. Installation des Installers für Acronis Access Server.
2. Konfiguration der von Acronis Access Server genutzten Netzwerk-Ports und SSL-Zertifikate.
3. Nutzung des webbasierten Installationsassistenten zur Konfiguration des Servers.

### Acronis Access installieren

Sie müssen als Administrator angemeldet sein, um Acronis Access installieren zu können.

1. Laden Sie das Installationsprogramm für Acronis Access herunter.

2. Deaktivieren Sie alle vorhandenen Virenschutzprogramme, da sie unter Umständen den Installationsvorgang unterbrechen und somit eine fehlerhafte Installation verursachen können.
3. Doppelklicken Sie auf die Programmdatei des Installationsprogramms.

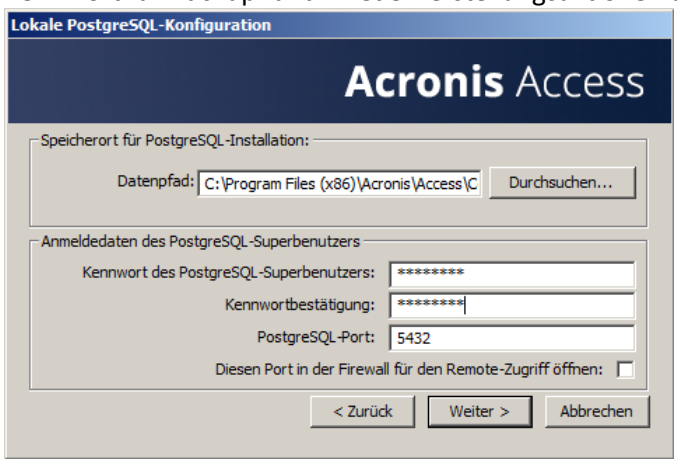



4. Klicken Sie auf **Weiter**, um zu beginnen.
5. Lesen und akzeptieren Sie die Lizenzvereinbarung.
6. Drücken Sie **Installieren**.

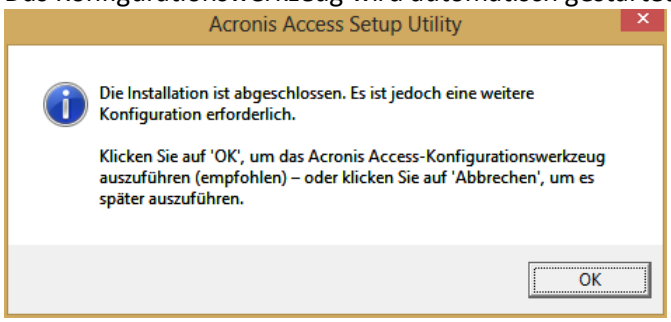
***Hinweis:*** *Wenn Sie mehrere Acronis Access Server einsetzen oder eine nicht standardmäßige Konfiguration installieren möchten, können Sie über die Schaltfläche* ***Benutzerdefinierte Installation*** *festlegen, welche Komponenten installiert werden sollen.*

7. Verwenden Sie entweder die Standardpfade, oder wählen Sie für jede Komponente die gewünschten Pfade aus – und drücken Sie dann auf 'OK'.


8. Legen Sie ein Kennwort für den Benutzer 'Postgres' fest, und notieren Sie es. Sie benötigen dieses Kennwort für Backup- und Wiederherstellungsaktionen der Datenbank.




9. Es wird ein Fenster angezeigt, in dem alle zu installierenden Komponenten aufgelistet sind. Drücken Sie **OK**, um fortzufahren.
10. Wenn der Installationsvorgang für Acronis Access abgeschlossen ist, drücken Sie **Beenden**.
11. Das Konfigurationswerkzeug wird automatisch gestartet und schließt die Installation ab.




Informationen zur Verwendung des Konfigurationswerkzeugs finden Sie unter Das Konfigurationswerkzeug verwenden (S. 10).

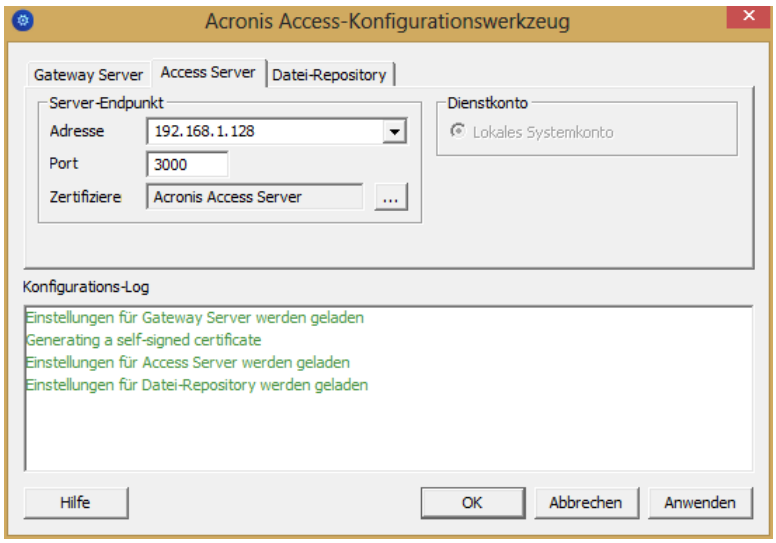
## 1.3 Das Konfigurationswerkzeug verwenden

Der Installer für Acronis Access beinhaltet ein Konfigurationswerkzeug, mit dem Sie den Acronis Access Gateway Server, das Datei-Repository und den Acronis Access Server schnell und einfach einrichten können. Der Gateway Server wird von mobilen Clients für den Zugriff auf Dateien und Freigaben verwendet. Der Access Server stellt die Webbenutzeroberfläche für Acronis Access-Clients bereit und fungiert zudem als Verwaltungskonsole sowohl für Mobile Access als auch Sync & Share.

***Hinweis:*** *Im Abschnitt Netzwerkanforderungen (S. 5) finden Sie weitere Informationen zu optimalen Vorgehensweisen für die IP-Adressenkonfigurationen von Acronis Access.*

***Hinweis:*** *Weitere Informationen zum Hinzufügen Ihres Zertifikats zum Microsoft Windows-Zertifikatspeicher finden Sie im Artikel Zertifikate verwenden.*

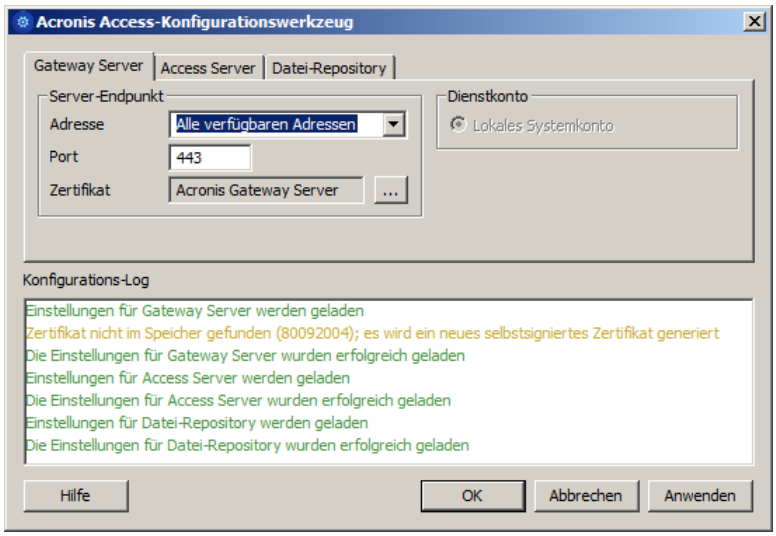
**Überblick über den Access Server**




Der Access Server stellt die Webbenutzeroberfläche für Acronis Access-Clients bereit und fungiert zudem als Verwaltungskonsole sowohl für Mobile Access als auch Sync & Share.

- **Adresse** – Der DNS-Name oder die IP-Adresse der Weboberfläche; wählen Sie alternativ **Alle Adressen**, um an allen Schnittstellen abzuhören.
- **Port –** Der Port Ihrer Weboberfläche.
- **Zertifikat –** Pfad zum Zertifikat der Weboberfläche. Sie können ein Zertifikat aus dem Microsoft Windows-Zertifikatspeicher wählen.
- **Verbindungen an Port 80 akzeptieren** – Wenn diese Option ausgewählt ist, Tomcat den unsicheren Port 80 auf eingehenden Datenverkehr hin ab und leitet ihn zum HTTPS-Port um, den Sie zuvor festgelegt haben.
- **Dienst-Konto –** Dies ermöglicht Ihnen, den Acronis Access Server-Dienst im Kontext eines anderen Kontos auszuführen. In typischen Installationen ist dies normalerweise nicht erforderlich.

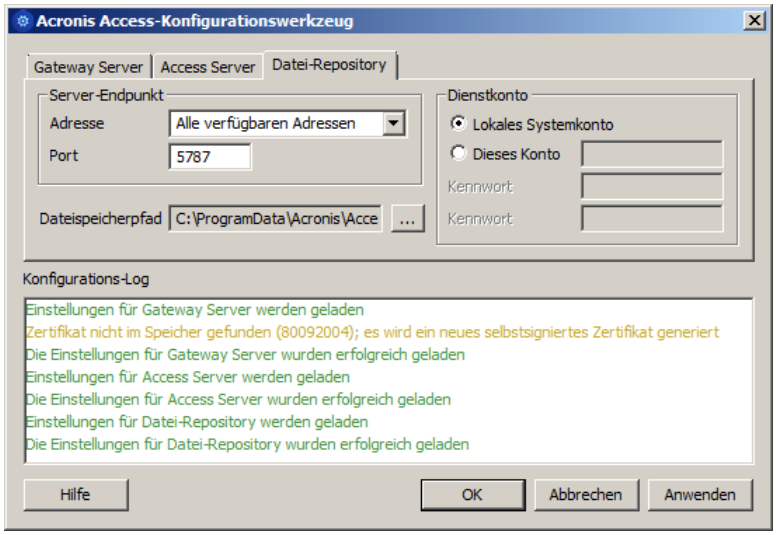
### Überblick über den Gateway Server




Der Gateway Server wird von mobilen Clients für den Zugriff auf Dateien und Freigaben verwendet.

- **Adresse –** Der DNS-Name oder die IP-Adresse des Gateway Servers; wählen Sie alternativ **Alle Adressen**, um an allen Schnittstellen abzuhören.
- **Port –** Der Port des Gateway Servers.
- **Zertifikat –** Pfad zum Zertifikat des Gateway Servers. Sie können ein Zertifikat aus dem Microsoft Windows Zertifikatspeicher wählen.
- **Dienst-Konto –** Dies ermöglicht Ihnen, den Gateway Server-Dienst im Kontext eines anderen Kontos auszuführen. Bei einer typischen Installation ist dies in der Regel nicht erforderlich.

### Überblick über das Datei-Repository



Das Datei-Repository wird von den Sync & Share-Funktionen verwendet. Wenn Sie Sync & Share nicht aktiviert haben, können Sie die Standardwerte akzeptieren. Wenn Sie Sync & Share verwenden, muss der Dateispeicherpfad den für die Speicherung zu verwendenden Laufwerkspeicherort angeben. Wenn Sie vorhaben, Amazon S3 für die Speicherung zu verwenden, können Sie die Standardwerte übernehmen.

- **Adresse –** Der DNS-Name oder die IP-Adresse des Datei-Repository; wählen Sie alternativ **Alle Adressen**, um an allen Schnittstellen abzuhören. Wenn Sie eine IP- oder DNS-Adresse angeben, dann wird die gleiche Adresse auch im Abschnitt **Datei-Repository** der Weboberfläche festgelegt. Weitere Informationen darüber finden Sie im Artikel Datei-Repository.
- **Port –** Der Port des Datei-Repository. Der gleiche Port wird auch im Abschnitt **Datei-Repository** der Weboberfläche festgelegt. Weitere Informationen darüber finden Sie im Artikel Datei-Repository.
- **Dateispeicherpfad –** UNC-Pfad des Dateispeichers. Wenn Sie den Dateispeicherpfad ändern, müssen Sie manuell alle Dateien, die sich bereits am ursprünglichen Dateispeicherort befinden, an den neuen Speicherort kopieren.

  ***Hinweis:*** *Wenn Sie den Dateispeicher an einen anderen Speicherort verschieben, dann laden Sie eine neue Datei hoch, um sicherzustellen, dass der richtige neue Speicherort übernommen wurde. Laden Sie darüber hinaus eine Datei herunter, die sich bereits im Dateispeicher befand, um sicherzustellen, dass Sie auch vom neuen Speicherort aus auf alle Dateien des ursprünglichen Speicherorts zugreifen können.*

- **Dienst-Konto –** Wenn sich der Dateispeicher für das Repository auf einer Remote-Netzwerkfreigabe befindet, sollte als Dienst-Konto ein Konto konfiguriert werden, das Zugriff auf diese Netzwerkfreigabe hat. Dieses Konto benötigt außerdem Lese- und Schreibzugriff auf den Repository-Ordner (z.B. C:\Programme (x86)\Acronis\Access\File Repository\Repository), um die Log-Datei zu schreiben.

Nachdem Sie alle erforderlichen Felder ausgefüllt haben, werden durch Klicken auf 'Anwenden' oder 'OK' die Dienste neu gestartet, an denen Sie Änderungen vorgenommen haben. Nach dem Starten der Dienste dauert es 30 bis 45 Sekunden, bevor der Acronis Access Server verfügbar ist. Dann wird automatisch ein Webbrowser geöffnet, in dem eine Verbindung zur IP-Adresse und zum Port von Acronis Access hergestellt wird. Legen Sie auf der Anmeldeseite das Administratorkennwort fest, woraufhin der Installationsassistent (S. 12) Sie durch den Einrichtungsvorgang führt.

***Hinweis:*** *Notieren Sie sich das Administratorkennwort, da Sie es nicht wiederherstellen können, wenn Sie es vergessen.*

***Hinweis:*** *Falls Sie irgendwelche der von den Acronis Access-Komponenten verwendeten IP-Adressen/Ports des Netzwerks oder Zertifikate ändern müssen, können Sie das Konfigurationswerkzeug jederzeit erneut ausführen, um diese Änderungen vorzunehmen. Das Werkzeug passt die relevanten Konfigurationsdateien automatisch an und startet die Dienste neu.*

## 1.4 Den Installationsassistenten verwenden

Nach der Installation der Software und dem Ausführen des Konfigurationsdienstprogramms zum Einrichten der Netzwerk-Ports und der SSL-Zertifikate muss der Administrator als Nächstes den Acronis Access-Server konfigurieren. Der Installationsassistent leitet den Administrator durch eine Reihe von Schritten, um die grundlegenden Funktionen des Servers einzurichten.

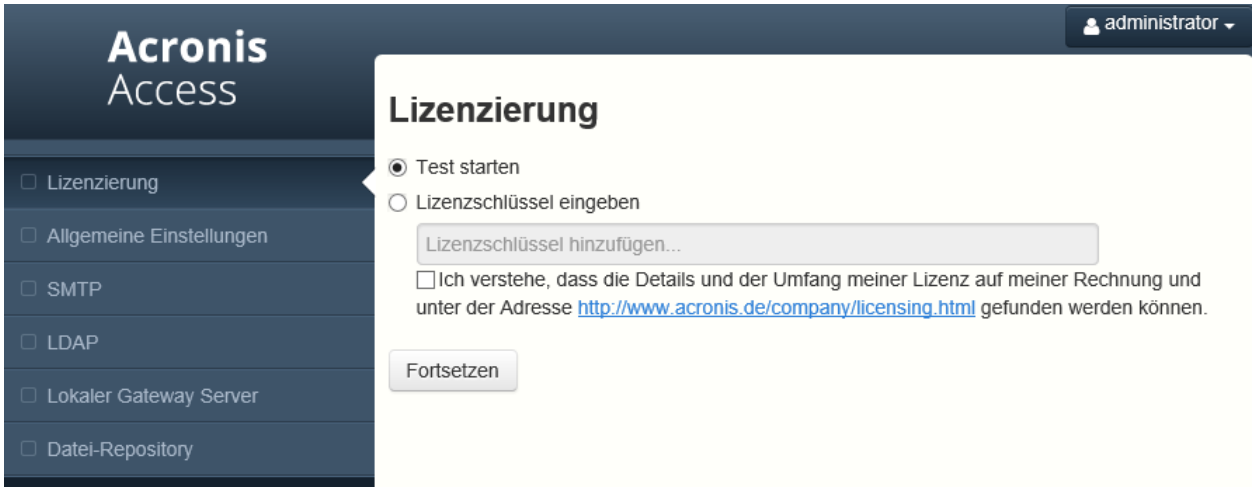
***Hinweis:*** *Wenn Sie ein Upgrade von activEcho oder mobilEcho vornehmen, lesen Sie die Anweisungen im Abschnitt zu Upgrades (S. 19).*

***Hinweis:*** *Nach dem Ausführen des Konfigurationsdienstprogramms dauert es ca. 30-45 Sekunden, bis der Server zum ersten Mal hochfährt.*

Navigieren Sie zur Weboberfläche von Acronis Access unter Verwendung der im Konfigurationsdienstprogramm angegebenen IP-Adresse und des Ports. Sie werden zum Einrichten des Kennworts für das Standard-Administratorkonto aufgefordert.

***Hinweis:*** *Administratoren können später konfiguriert werden. Weitere Informationen hierzu finden Sie im Abschnitt Server-Administration.*

Der Assistent hilft Ihnen, die grundlegenden Einstellungen für die Funktionalität Ihres Produkts vorzunehmen.

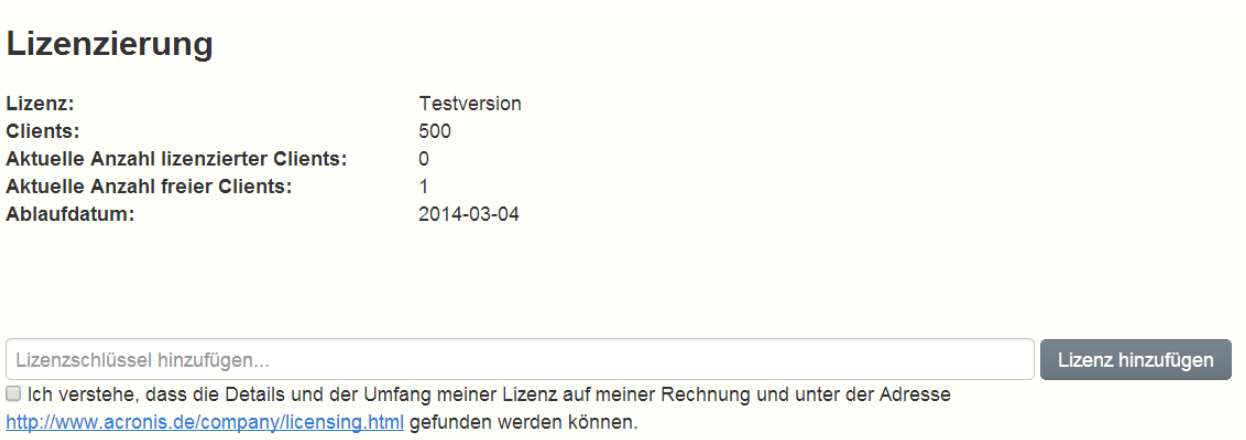



- 'Allgemeine Einstellungen' betreffen die Einstellungen der Weboberfläche selbst, z.B. Sprache, Farbschema, den in Admin-Benachrichtigungen verwendeten Server-Namen, Lizenzierung und Administratoren.
- Über die LDAP-Einstellungen können Sie die Anmeldedaten, Regeln und Richtlinien für Active Directory mit unserem Produkt verwenden.
- Die SMTP-Einstellungen betreffen sowohl Mobile Access- als auch Sync & Share-Funktionen. Für Mobile Access wird der SMTP-Server beim Senden von Registrierungseinladungen verwendet. Die Sync & Share-Funktionen verwenden den SMTP-Server zum Senden von Ordnereinladungen, Warnungen und Fehlerzusammenfassungen.

Alle auf der Seite 'Erstkonfiguration' angezeigten Einstellungen sind auch nach Abschluss der Erstkonfiguration verfügbar. Weitere Informationen über diese Einstellungen finden Sie in den Artikeln zum Thema Server-Administration.

## Den Prozess der Erstkonfiguration durchlaufen

### Lizenzierung




**So starten Sie eine Testversion:**

1. Wählen Sie **Test starten** und dann **Fortsetzen**.

**So lizenzieren Sie Ihren Access Server:**

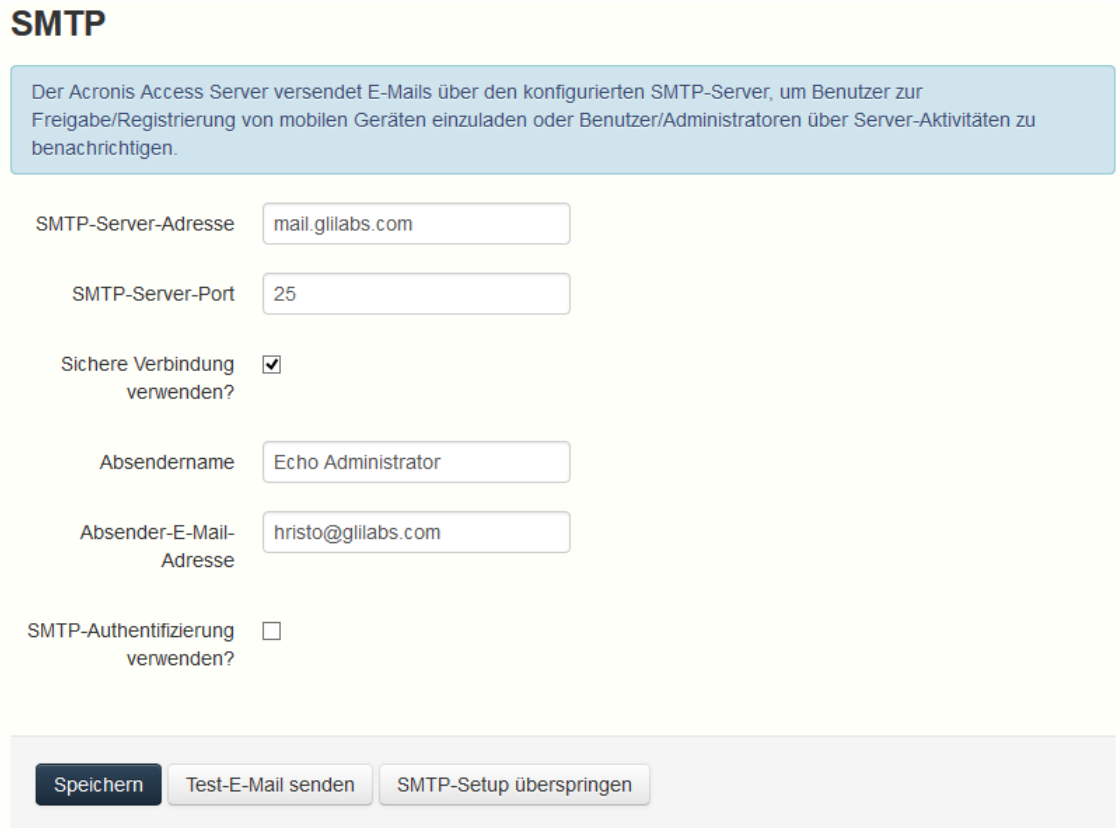
1. Wählen Sie **Lizenzschlüssel eingeben**.
2. Geben Sie Ihren Lizenzschlüssel ein, und aktivieren Sie das Kontrollkästchen.
3. Drücken Sie **Speichern**.

### Allgemeine Einstellungen


1. Geben Sie einen Servernamen ein.
2. Geben Sie den DNS-Stammnamen oder die IP-Adresse ein, über den bzw. die Benutzer auf die Website zugreifen (beginnend mit http:// oder https://).
3. Geben Sie den DNS-Namen oder die IP-Adresse an, über den bzw. die sich mobile Benutzer registrieren.
4. Wählen Sie ein Farbschema aus. Die derzeit verfügbaren Optionen sind Grau, Violett, Cappuccino, Blau, Dunkelblau und Orange.

5. Wählen Sie die Standardsprache für das **Überwachungsprotokoll** aus. Die derzeit verfügbaren Optionen sind Englisch, Deutsch, Französisch und Japanisch.
6. Klicken Sie auf **Speichern**.

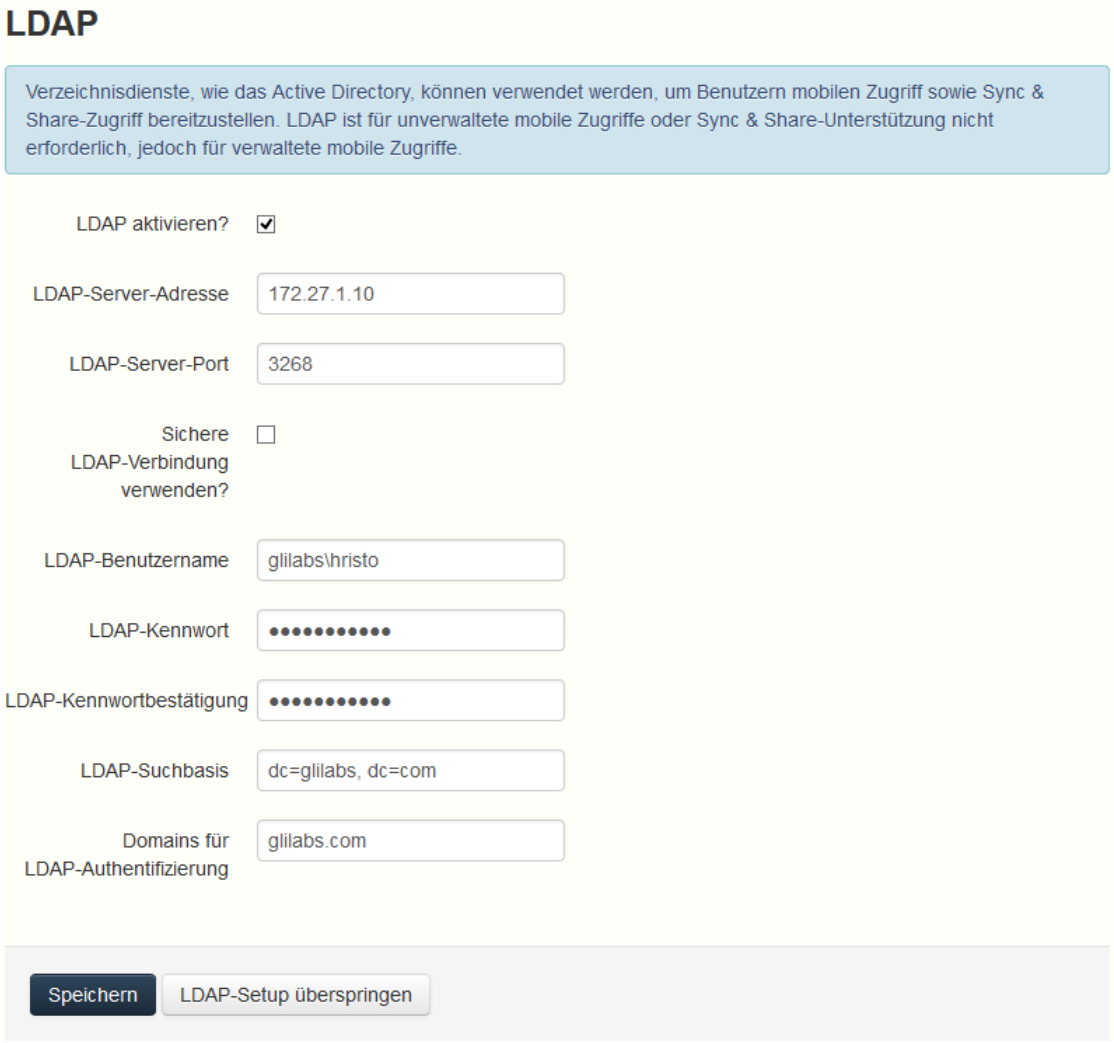
### SMTP




***Hinweis:*** *Sie können diesen Abschnitt überspringen und SMTP später konfigurieren.*

1. Geben Sie den DNS-Namen oder die IP-Adresse des SMTP-Servers ein.
2. Geben Sie den SMTP-Port des Servers ein.
3. Wenn Sie keine Zertifikate für den SMTP-Server verwenden, deaktivieren Sie **Sichere Verbindung verwenden?**.
4. Geben Sie den Namen ein, der in der 'Von'-Zeile von E-Mails angezeigt wird, die vom Server gesendet werden.
5. Geben Sie die Adresse ein, die als Absender der vom Server gesendeten E-Mails verwendet wird.
6. Falls Sie für den SMTP-Server eine Authentifizierung per Benutzername/Kennwort verwenden, aktivieren Sie **SMTP-Authentifizierung verwenden?**, und geben Sie Ihre Anmeldedaten ein.
7. Klicken Sie auf **Test-E-Mail senden**, um eine Test-E-Mail an die in Schritt 5 festgelegte Adresse zu senden.
8. Klicken Sie auf **Speichern**.

**LDAP**




***Hinweis:*** *Sie können diesen Abschnitt überspringen und LDAP später konfigurieren.*

1. Markieren Sie **LDAP aktivieren**.
2. Geben Sie den DNS-Namen oder die IP-Adresse des LDAP-Servers ein.
3. Geben Sie den Port des LDAP-Servers ein.
4. Falls Sie ein Zertifikat für Verbindungen mit dem LDAP-Server verwenden, markieren Sie **Sichere LDAP-Verbindung verwenden**.
5. Geben Sie Ihre LDAP-Anmeldedaten einschließlich der Domain ein (z.B. acronis\hristo).
6. Geben Sie die LDAP-Suchbasis ein.
7. Geben Sie die gewünschte(n) Domain(s) für die LDAP-Authentifizierung ein. (Für ein Konto mit der E-Mail-Adresse **joe@glilabs.com** würden Sie zur LDAP-Authentifizierung beispielsweise **glilabs.com** eingeben.)
8. Klicken Sie auf **Speichern**.

**Lokaler Gateway Server**


***Hinweis:*** *Wenn Sie einen Gateway Server und den Acronis Access Server auf derselben Maschine installieren, wird der Gateway Server automatisch erkannt und vom Acronis Access Server verwaltet. Sie werden aufgefordert, den DNS-Namen oder die IP-Adresse festzulegen, unter dem bzw. der der lokale Gateway Server für die Clients erreichbar ist. Diese Adresse können Sie später ändern.*

1. Legen Sie einen DNS-Namen oder eine IP-Adresse für den lokalen Gateway Server fest.
2. Klicken Sie auf **Speichern**.

**Datei-Repository**

1. Wählen Sie einen Dateispeichertyp aus. Verwenden Sie **Dateisystem** für einen Dateispeicher auf Ihren Computern oder **Amazon S3** für einen Dateispeicher in der Cloud.
2. Geben Sie den DNS-Namen oder die IP-Adresse des Datei-Repository-Dienstes ein.

   ***Hinweis:*** *Das Konfigurationswerkzeug für Acronis Access wird zum Festlegen der Adresse des Datei-Repository, des Ports und des Dateispeicherorts verwendet. Die Einstellung 'Dateispeicher-Repository-Endpunkt' muss den Einstellungen auf der Registerkarte 'Datei-Repository' des Konfigurationswerkzeugs entsprechen. Führen Sie die Datei 'AcronisAccessConfiguration.exe' aus, die sicher in der Regel im Verzeichnis* ***`C:\Program Files (x86)\Acronis\Configuration Utility\`*** *auf dem Endpunktserver befindet, um diese Einstellungen anzuzeigen oder zu ändern.*

3. Wählen Sie einen Verschlüsselungsgrad. Wählen Sie zwischen **Ohne**, **AES-128** und **AES-256**.
4. Legen Sie den minimalen verfügbaren Speicherplatz fest, bevor der Server Ihnen eine Warnung sendet.
5. Drücken Sie **Speichern**.

## 1.5 Clustering von Acronis Access

Acronis Access ermöglicht die Konfiguration hochverfügbarer Setups ohne Clustering-Software von Drittanbietern. Die Konfiguration erfolgt mithilfe der neuen Cluster-Gruppen-Funktion, die in Acronis Access 5.1 eingeführt wurde. Das Einrichtungsverfahren ist einfach, bietet jedoch hohe Verfügbarkeit für die Acronis Access Gateway Server, da es sich bei ihnen um die Komponenten mit der höchsten Last handelt. All diese Konfigurationen werden durch den Acronis Access Server verwaltet.

Weitere Informationen und Anweisungen zum Einrichten einer Cluster-Gruppe finden Sie im Artikel Cluster-Gruppen.

Zwar empfiehlt sich der Einsatz der integrierten Cluster-Gruppen-Funktion, doch unterstützt Acronis Access auch das Microsoft Failover-Clustering. Weitere Informationen finden Sie im Artikel Ergänzendes Material.

## 1.6 Lastenausgleich für Acronis Access

Acronis Access unterstützt den Lastenausgleich. Weitere Informationen finden Sie in den Artikeln Lastenausgleich für Acronis Access und Cluster-Gruppen.

# 2 Upgrades

**Themen**



## 2.1 Upgrade von Acronis Access auf eine neuere Version

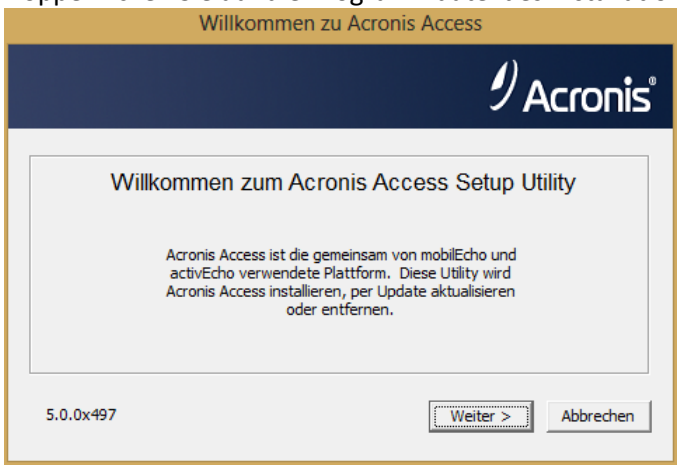
Das Verfahren für das Upgrade von einer vorherigen Version von Acronis Access ist ein vereinfachter Prozess und erfordert nahezu keine Konfiguration.

**Apache Tomcat-Ordner per Backup sichern**

Beim Upgrade wird möglicherweise ein Upgrade für Apache Tomcat und für alle aktuellen Tomcat-Konfigurationsdateien durchgeführt und die Protokolldateien werden entfernt. Es empfiehlt sich, eine Kopie des Apache Tomcat-Ordners anzulegen. Dieser befindet sich standardmäßig hier: **C:\Programme (x86)\Acronis\Access\Common**.

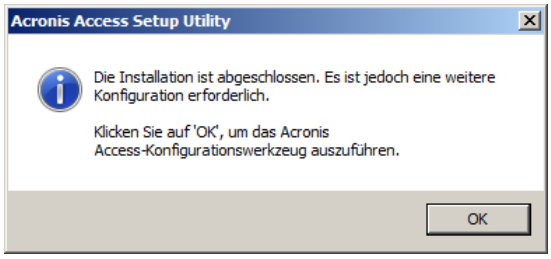
**Upgrade**

1. Deaktivieren Sie alle vorhandenen Virenschutzprogramme, da sie unter Umständen den Installationsvorgang unterbrechen und somit eine fehlerhafte Installation verursachen können.
2. Doppelklicken Sie auf die Programmdatei des Installationsprogramms.




3. Klicken Sie auf **Weiter**, um zu beginnen.
4. Lesen und akzeptieren Sie die Lizenzvereinbarung.
5. Drücken Sie **Upgrade**.
6. Überprüfen Sie die zur Installation ausgewählten Komponenten und klicken Sie auf **Installieren**.
7. Prüfen Sie die installierten Komponenten, und schließen Sie den Installer.

8. Wenn Sie aufgefordert werden, das Konfigurationswerkzeug zu öffnen, drücken Sie **OK**.




9. Stellen Sie sicher, dass sich keine der Einstellungen im Konfigurationswerkzeug geändert hat. Nachdem Sie überprüft haben, dass alle Einstellungen den Erwartungen entsprechen, drücken Sie **OK**, um das Konfigurationswerkzeug zu schließen und die Acronis Access-Dienste zu starten.

## 2.2 Upgrade von mobilEcho 4.5 oder früheren Versionen

**Themen**



### 2.2.1 Vor Beginn

**mobilEcho vor dem Upgrade per Backup sichern**

Sichern Sie die Datendateien, die vom vorhandenen mobilEcho Server verwendet werden. Das Acronis Access Installationsprogramm sichert diese Dateien zwar, aus Sicherheitsgründen wird jedoch empfohlen, vor Beginn des Upgrades eine eigene Backup-Kopie anzufertigen.

Das Backup- und Wiederherstellungsverfahren für einen mobilEcho Server bis Version 4.5 wird hier erläutert:
http://docs.grouplogic.com/display/MobilEcho/mobilEcho+Server+Backup+and+Restoration

**Führen Sie ein Upgrade Ihrer Version von mobilEcho auf Version 4.5 aus, bevor Sie mit dem Upgrade auf Acronis Access fortfahren.**

**Eigene Konfiguration kennen**

Stellen Sie sicher, dass Sie die folgenden Fragen beantworten können, bevor Sie mit dem Upgrade fortfahren:

- Ist sowohl mobilEcho als auch activEcho installiert?
- Befinden sie sich auf demselben Computer oder auf unterschiedlichen Maschinen?
- Welche Ports verwendet mobilEcho? An welchem Port befindet sich der File Server und an welchem der Management Server?
- Welchen Port verwendet activEcho? Befindet sich das Datei-Repository auf derselben Maschine?

**Verbesserungen**

Acronis Access umfasst eine Reihe von Verbesserungen, die die Konfiguration und Verwaltung von mobilEcho Servern optimieren. Weiterhin wurde die Verwaltung von mobilEcho und activEcho in einer gemeinsamen Konsole konsolidiert. Diese Anleitung beschreibt die Architektur- und Funktionsänderungen, die Sie bei einem Upgrade auf Acronis Access berücksichtigen müssen.

In Acronis Access ist keine Einrichtung einer Pfadzuordnung für eine Netzwerk-Freigabeweiterleitung erforderlich, weil diese automatisch erfolgt. Sie müssen jedoch eine 'Ordner'-Datenquelle erstellen, die auf jeden Server verweist, der Basisverzeichnisse hostet.

**Upgrades müssen sorgfältig geplant werden**

Acronis Access enthält umfassende Architektur- und Funktionsänderungen an den Software-Diensten, den Speicherorten von Datenbanken und Einstellungen sowie der Administration von mobilEcho. Zwar werden durch diese Änderungen leistungsfähige neue Funktionen und Integrationsmöglichkeiten zur Verfügung gestellt, jedoch muss das Upgrade auf Acronis Access sorgfältig überlegt und geplant werden.

Bei mobilEcho Deployments mit nur einem Server ist das Verfahren relativ unkompliziert. Falls Sie jedoch einen Reverse-Proxy-Server oder ein Lastenausgleichsmodul verwenden, über mehrere mobilEcho Server verfügen oder Microsoft Failover Clustering verwenden, müssen Sie sich unbedingt mit den in diesem Dokument aufgeführten Upgrade-Überlegungen für das jeweilige Szenario vertraut machen.

Dieses Dokument enthält alle Informationen, die Sie zum Planen und sicheren Durchführen eines Upgrades auf Acronis Access benötigen. Es wird dringend empfohlen, dieses Upgrade in einer Testumgebung durchzuführen, die das jeweilige mobilEcho Deployment simuliert, bevor Sie das Upgrade für die mobilEcho Produktionsserver durchführen.

**mobilEcho Server mit Lastenausgleichsmodul und Microsoft Failover Cluster**

Wenn Sie mehrere mobilEcho Server mit einem Front-End-Lastenausgleichsmodul bereitgestellt haben oder mobilEcho auf einem Microsoft Failover Cluster ausführen, müssen Sie ein Upgrade auf Acronis Access 5.1 oder höher ausführen. Ab Version 5.1 ist eine neue Funktion verfügbar, mit der Servergruppen mit Lastenausgleichsmodul automatisch über die Acronis Access Server-Konsole verwaltet werden können. Mit dieser Funktion erübrigt sich die Replizierung von Registry-Einstellungen und Skript-Updates auf die Server. Zum Hinzufügen einer neuen Datenquelle (Volume) zu den Servern ist nur noch ein einziger Schritt erforderlich, der automatisch von der Management Konsole ausgeführt wird. Weitere Informationen finden Sie im Artikel Cluster-Gruppen.

*Die Installation und das Upgrade von mobilEcho in einem Windows Failover Cluster ist ein kompliziertes Verfahren. Aufgrund der in mobilEcho 5.0 eingeführten Architekturänderungen funktioniert mobilEcho auf Windows Failover Clustern jetzt anders als zuvor.*

*Anweisungen zum Installieren von Acronis Access in einem Cluster finden Sie im Artikel Acronis Access in einem Cluster installieren.*

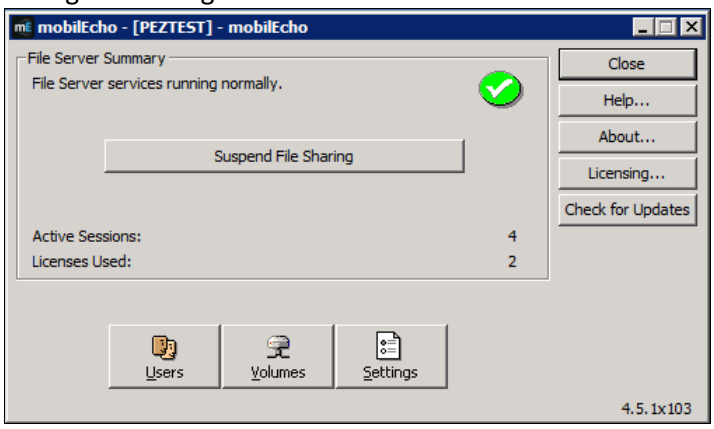
*Anweisungen für das Upgrade eines mobilEcho-Clusters auf ein Acronis Access Cluster finden Sie im Artikel Upgrade von Acronis Access in einem Cluster.*

**Änderungen bei Architektur und Terminologie**

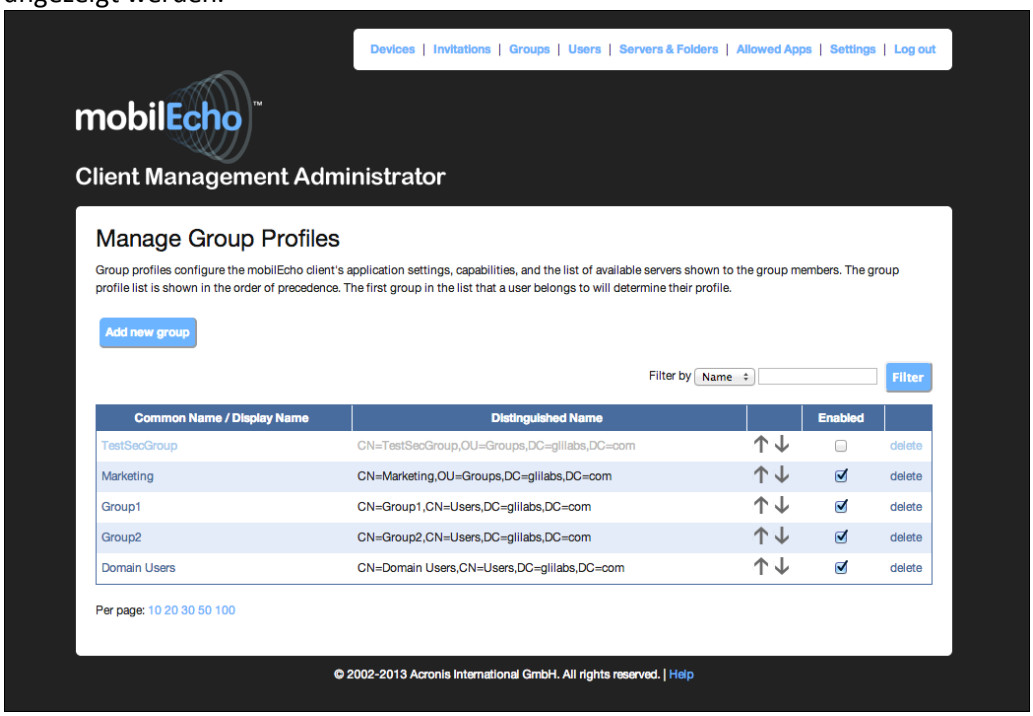
Acronis hat die Produkte mobilEcho und activEcho in einer gemeinsamen Software-Plattform konsolidiert. Die beiden Produkte werden nach wie vor getrennt lizenziert und können einzeln oder zusammen verwendet werden, sie haben jetzt jedoch ein gemeinsames Installationsprogramm und werden über dieselbe Konsole verwaltet. Diese gemeinsame webbasierte Konsole wird als Acronis Access Server bezeichnet.

**mobilEcho 4.5 und frühere Versionen enthielten zwei Management Konsolen:**

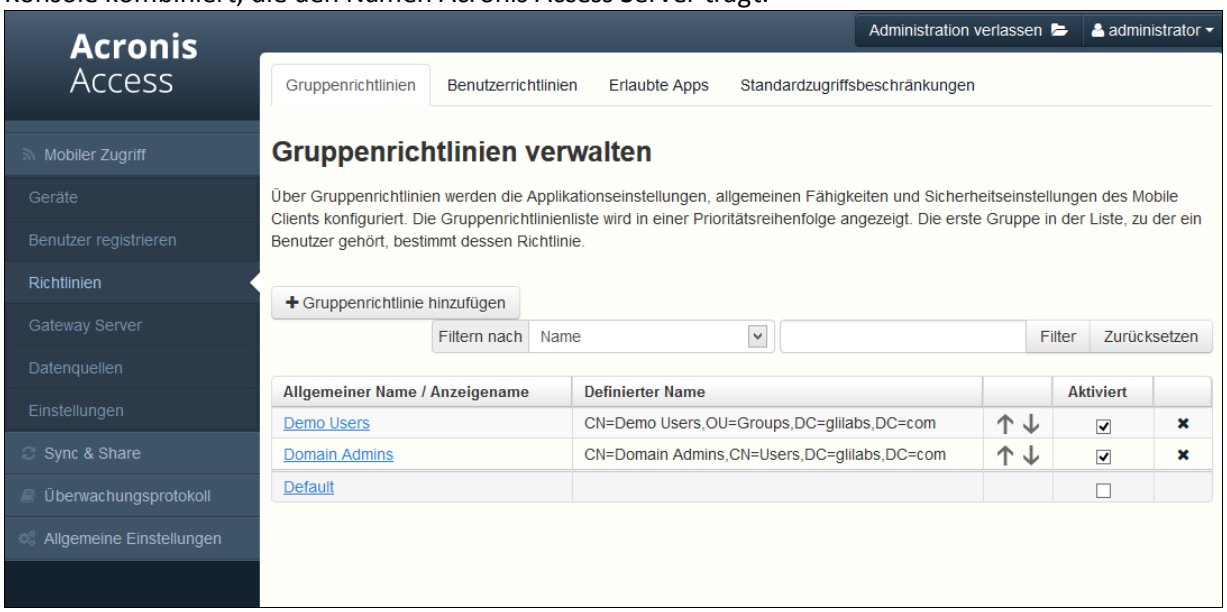
**mobilEcho-Administrator** – Dieses Windows-Programm diente zur Definition der Dateifreigabe-'Volumes' für mobilEcho Clients, zur Überwachung der aktiven Benutzer und zur Konfiguration allgemeiner mobilEcho File Access Server-Einstellungen.




**mobilEcho Client Management Administrator** – Diese webbasierte Konsole diente zum Onboarding, zur Überwachung und Remote-Löschung von mobilEcho Client-Benutzern, zur Definition von Richtlinien für Client-Sicherheit und -Konfiguration sowie zur Zuweisung der mobilEcho Server, Netzwerkordner-Verknüpfungen und synchronisierten Ordner, die automatisch in der mobilEcho App angezeigt werden.



In Acronis Access wurden diese beiden Management Konsolen in einer einzigen webbasierten Konsole kombiniert, die den Namen Acronis Access Server trägt.




Der Acronis Access Server ist eine Webanwendung, die folgende Rollen übernimmt:

- Verwaltungskonsole für mobilEcho
- Verwaltungskonsole für activEcho
- Weboberfläche des activEcho Clients

Falls Sie nur mobilEcho verwenden, wird die vorhandene mobilEcho Client Management Administrator-Webkonsole (die in der Regel auf Port 3000 des mobilEcho Servers ausgeführt wird) auf eine Acronis Access Server Webkonsole aktualisiert, wenn Sie das Upgrade auf Acronis Access durchführen.

Die Funktionen des Windows-Programms mobilEcho-Administrator werden jetzt von der Acronis Access Server Webkonsole übernommen. Nach dem Upgrade auf Acronis Access wird der mobilEcho-Administrator nicht mehr zur Konfiguration des mobilEcho File Access Server-Diensts verwendet und vom mobilEcho Server entfernt.

**Einstellungen werden nicht mehr in der Windows-Registry gespeichert**

In früheren Versionen von mobilEcho wurden mobilEcho File Access Server Einstellungen und konfigurierte Volumes in der Windows-Registry gespeichert. Beim Upgrade auf Acronis Access werden diese Einstellungen in eine interne SQL-Datenbank verschoben. Falls automatisierte Prozesse vorliegen, die mobilEcho Volumes direkt der Windows-Registry hinzufügen oder die die Registry-Einstellungen von mobilEcho sichern, müssen diese Prozesse so abgeändert werden, dass sie stattdessen für die SQL-Datenbank ausgeführt werden.

Auf einem Server, für den ein Upgrade durchgeführt wurde, ist diese SQL-Datenbank standardmäßig in diesem Ordner gespeichert:

```
C:\Program Files (x86)\Group Logic\mobilEcho Server\database\mobilEcho.sqlite3
```

Falls Sie Volumes für eine Gruppe von mobilEcho Servern mit Lastenausgleichsmodul durch direkte Bearbeitung der Registry verwalten, steht demnächst eine neue Funktion zur Verwaltung von mobilEcho Server-Clustern zur Verfügung, die Volume-Änderungen in der Registry überflüssig macht.

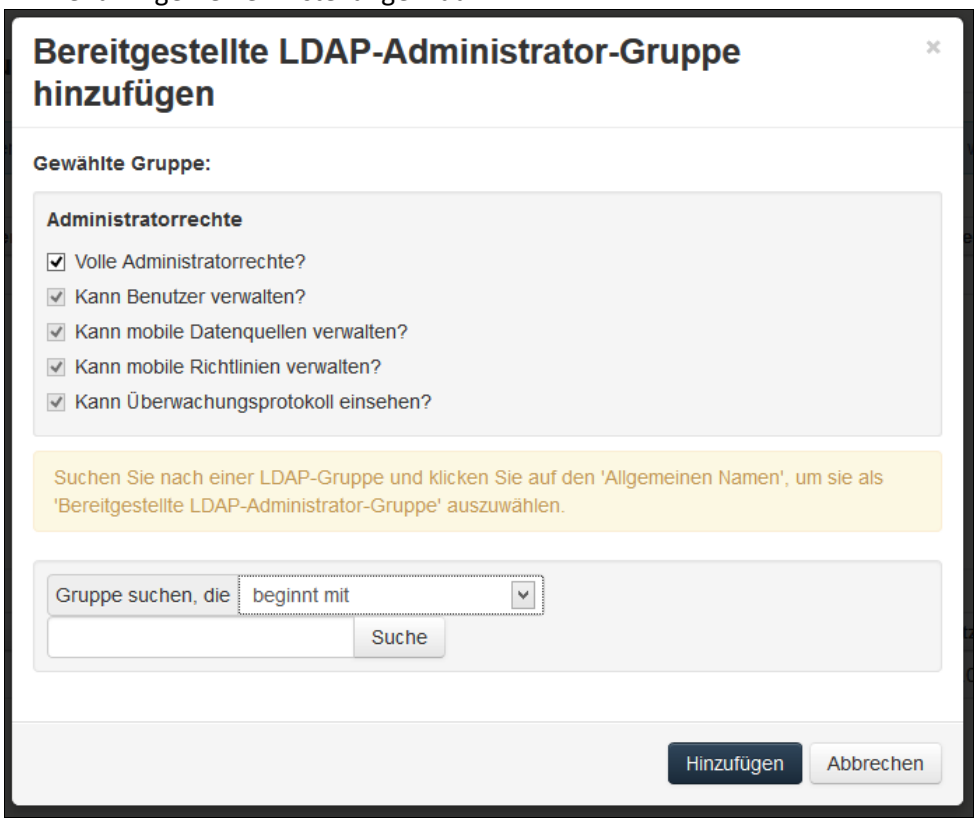
**Den Acronis Access Server verwalten**

**Vorhandene Einstellungen**

Alle vorhandenen Volumes, registrierten Benutzer, Richtlinien, zugewiesenen Server und Ordner sowie zulässigen Apps der Version mobilEcho 4.5 oder früher werden während des Upgrades auf den Acronis Access Server migriert. Bestehende mobilEcho Client-Benutzer können die Verbindung zum Server weiterhin wie gewohnt herstellen (keine clientseitigen Änderungen erforderlich) und haben Zugriff auf die gleichen Richtlinien und Datenquellen. Zwar wird empfohlen, dass die Benutzer ein Upgrade auf die Acronis Access iOS-Client-App oder die Acronis Access Android-Client-App durchführen, jedoch sind auch ältere Versionen der Client-App mit dem Acronis Access Server kompatibel.

### Server-Administratoren konfigurieren

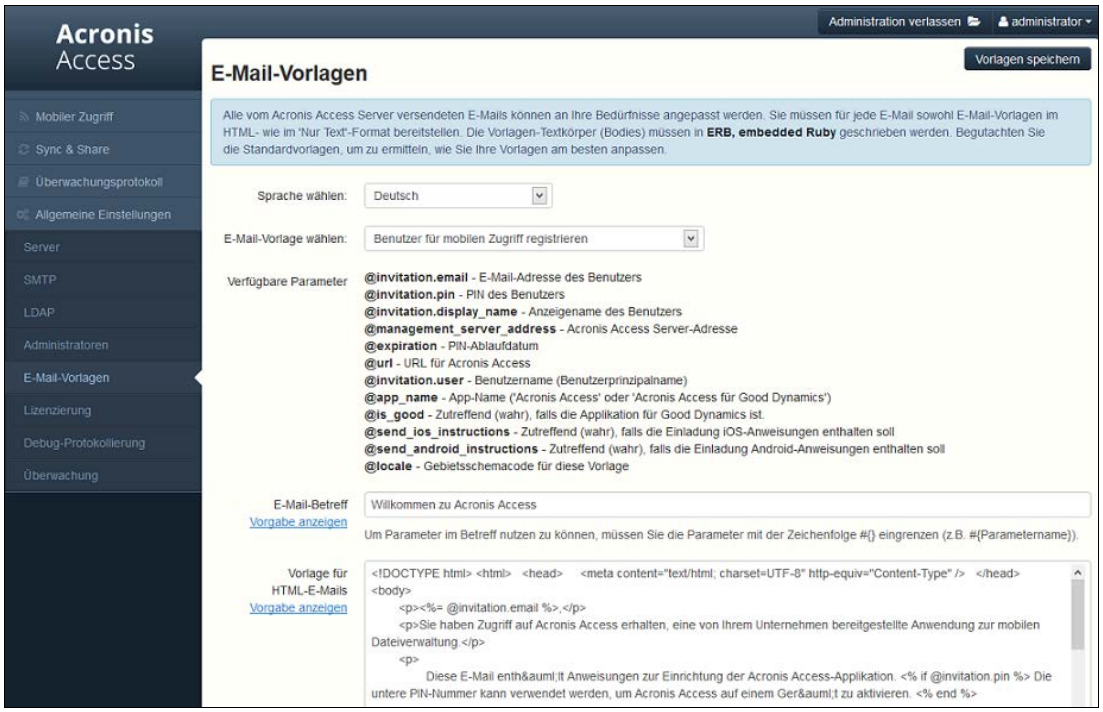
Alle vorhandenen Benutzer oder Gruppen, die vor dem Upgrade auf Acronis Access als mobilEcho Administratoren konfiguriert waren, haben weiterhin volle Admin-Rechte für die Acronis Access Server Webkonsole. In Acronis Access stehen neue rollenbasierte Admin-Rechte zur Verfügung, mit denen die Admin-Berechtigungen für bestimmte Benutzer oder Gruppen eingeschränkt werden können. Um Administratoren hinzuzufügen oder zu bearbeiten, rufen Sie die Seite 'Administratoren' im Menü 'Allgemeine Einstellungen' auf.




### E-Mail-Vorlagen

Falls Sie die Vorlage für die E-Mails mit mobilEcho Registrierungseinladungen angepasst haben, die an Benutzer gesendet werden, wird diese E-Mail-Vorlage bei einem Upgrade auf Acronis Access nicht migriert. Für die Bearbeitung von E-Mail-Vorlagen ist eine neue Oberfläche verfügbar. Öffnen Sie in der Acronis Access Konsole die Seite 'E-Mail-Vorlagen' im Menü 'Allgemeine Einstellungen' und ändern Sie die E-Mail-Vorlage nach Bedarf. Weitere Informationen finden Sie im Artikel Einstellungen fьr E-Mail-Vorlagen.

***Hinweis:*** *Eine Kopie der vorherigen mobilEcho Vorlagen finden Sie im Ordner* ***Legacy mobilEcho files****, der sich standardmäßig hier befindet:* ***`C:\Program Files (x86)\Group Logic\Access Server\Legacy mobilEcho files`****. Die Dateien haben die folgenden Namen:* ***invitation.html.erb*** *und* ***invitation.txt.erb****. Diese Dateien können bei der Anpassung neuer Vorlagen als Referenz verwendet werden.*



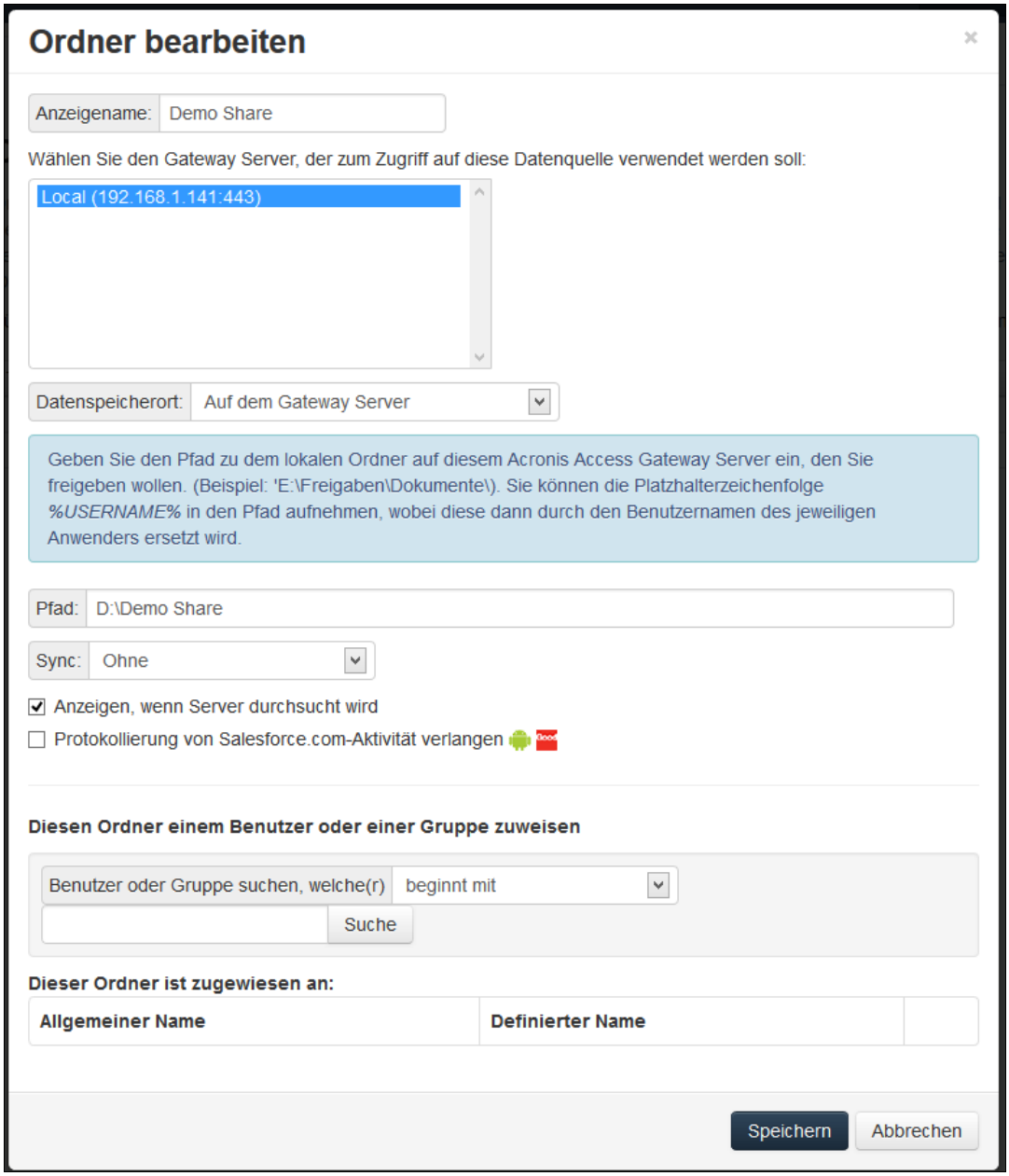

**Datenquellen-/Volume-Management**

Acronis Access konsolidiert die Server-Verwaltungsfunktionen des Windows-Programms mobilEcho-Administrator und der mobilEcho Client Management Administrator-Webkonsole in einer gemeinsamen Weboberfläche. Hierdurch wird das Volume-Konzept überflüssig.

Benutzern kann nun in einem einzigen Schritt Zugriff auf eine neue Dateifreigabe oder einen neuen SharePoint-Speicherort gewährt werden. Klicken Sie hierzu auf der Seite 'Datenquellen' auf die Registerkarte 'Ordner' und dann auf 'Neuen Ordner hinzufügen'. Dieser eine Schritt umfasst folgende Aktionen:

1. Zuweisen eines Anzeigenamens zum Ordner, der den Benutzern angezeigt wird
2. Auswählen des Gateway Servers, über den der Zugriff auf diese Datenquelle erfolgen soll
3. Auswählen des Datenquellentyps: lokaler Ordner auf dem Gateway Server, SMB/CIFS-Freigabe, SharePoint-Website oder Dokumentbibliothek oder activEcho Server.
4. Auswählen, ob dieser Ordner automatisch für die Benutzer synchronisiert wird, denen er zugewiesen wird
5. Festlegen, ob dieser Ordner im Stamm des mobilEcho Servers angezeigt wird, ausgehend von der Annahme, dass den Benutzern das Durchsuchen des Server-Stamms gestattet ist

6. Zuweisen dieses Ordners zu einer Sammlung von AD-Benutzern oder -Gruppen (Active Directory), sodass er automatisch in deren mobilEcho App angezeigt wird



Um festzulegen, dass ein Gateway Server automatisch in der mobilEcho Client-App angezeigt wird, verwenden Sie die Registerkarte 'Auf Clients sichtbare Gateway Server'. Auf dieser Seite können Sie den Gateway Servern AD-Benutzer oder -Gruppen zuweisen; diesen Benutzern werden die Server in ihrer mobilEcho App angezeigt. Sie können alle Ordner anzeigen und durchsuchen, für die die Eigenschaft 'Anzeigen, wenn Server durchsucht wird' aktiviert ist UND für die sie über Dateizugriffsberechtigungen verfügen.


**Erweiterte mobilEcho Client Management-Funktionen verwenden**

Falls für den vorhandenen mobilEcho Server keine mobilEcho Client Management-Funktionen konfiguriert waren, führt Sie der Acronis Access Installationsprozess durch die Basiskonfiguration, sodass Sie diese erweiterten Funktionen nutzen können.

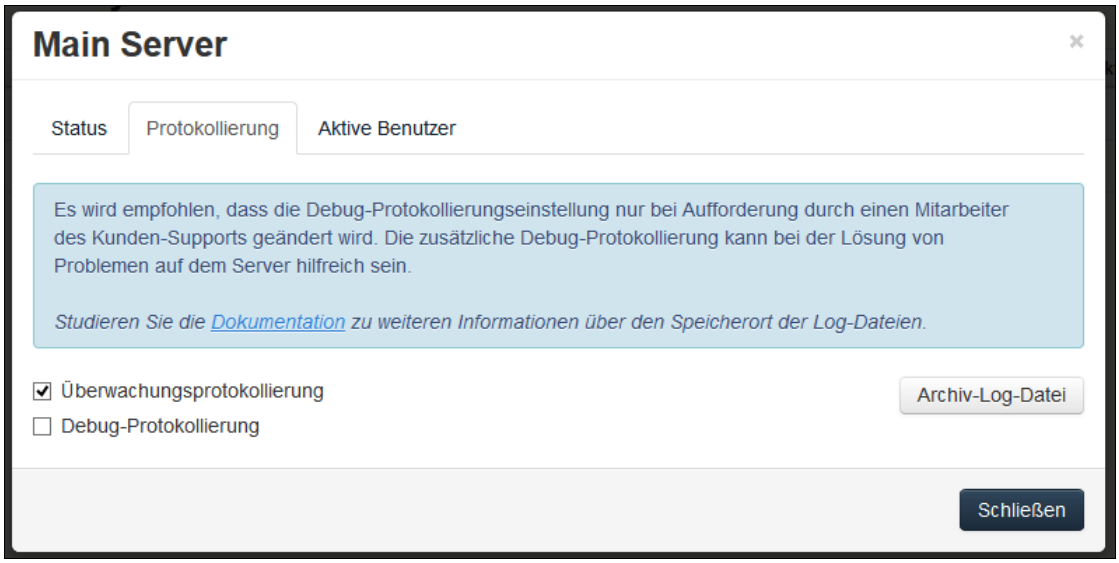
Zunächst werden Sie zur Eingabe von LDAP-Einstellungen aufgefordert, damit Acronis Access Server die Active Directory-Benutzer und -Gruppen auflisten kann, und von SMTP-Einstellungen, damit E-Mails mit Registrierungseinladungen an die Benutzer gesendet werden können.

Nach Abschluss dieser Konfiguration können Sie die Vorteile von Benutzer- und Gruppenrichtlinien, Statusüberwachung pro Gerät und vieler weiterer Funktionen nutzen.

**Neue Option 'Audit-Logs'**

Acronis Access enthält die neue Funktion 'Audit-Logs', mit der Acronis Access Gateway Server alle Dateiaktivitäten an die Acronis Access Webkonsole melden können. Diese Aktivitäten werden in einem konsolidierten Audit-Log gespeichert, mit dessen Hilfe alle von den Benutzern durchgeführten Dateivorgänge überwacht werden können.

Die Option 'Audit-Logs' ist auf Gateway Servern standardmäßig deaktiviert. Um die Überwachungsfunktion auf einem Gateway Server zu aktivieren, rufen Sie die Seite 'Gateway Server' auf, klicken auf die Schaltfläche 'Details' für den gewünschten Server und aktivieren auf der Registerkarte für die Protokollierung die Option 'Audit-Logs'.




Jetzt werden Ereignisse im Audit-Log protokolliert, auf das über das Hauptmenü des Acronis Access Servers zugegriffen werden kann.

## 2.2.2 Der Upgrade-Prozess

**Acronis Access Upgrade-Prozess**

Geben Sie zunächst die Art des mobilEcho-Deployments an, für das ein Upgrade durchgeführt werden soll. Ausführliche Anweisungen für diese Szenarien finden Sie im nächsten Abschnitt dieses Dokuments. Die gängigsten Szenarien sind folgende:

1. **Einzelner mobilEcho Server ohne Client Management**
   - Ein einzelner Windows Server, auf dem ausschließlich der mobilEcho File Access Server-Dienst ausgeführt wird
2. **Einzelner mobilEcho Server mit Client Management**
   - Ein einzelner Windows Server, auf dem der mobilEcho File Access Server-Dienst und der mobilEcho Client Management-Dienst ausgeführt werden
3. **Mehrere mobilEcho Server mit Client Management**
   - Mehrere Windows Server, auf denen der mobilEcho File Access Server-Dienst ausgeführt wird, wobei auf einem der Windows Server außerdem der mobilEcho Client Management-Dienst ausgeführt wird
4. **Mehrere mobilEcho Server mit einem Lastenausgleichsmodul am Front-End**
   - Ein autonomer Windows Server, auf dem der mobilEcho Client Management-Dienst ausgeführt wird, sowie zwei oder mehr Windows Server, auf denen nur der mobilEcho File Access Server-Dienst mit einem Lastenausgleichsmodul am Front-End ausgeführt wird.
5. **Windows Failover Cluster**
   - Unterstützung ab Version 5.0.3.

- Ein Windows Failover Cluster mit mehreren Knoten, auf dem mobilEcho auf mindestens einem virtuellen Server im Aktiv/Aktiv- oder Aktiv/Passiv-Modus ausgeführt wird.

**Wichtige Hinweise zu Szenario 4 – mobilEcho File Access Server mit Lastenausgleichsmodul**

*Falls Sie mehrere mobilEcho File Access Server mit einem Lastenausgleichsmodul am Front-End ausführen, müssen diese mobilEcho Server immer mit identischen mobilEcho-Volumes konfiguriert sein, damit die Benutzer über jeden Knoten Zugriff auf ihre Dateien erhalten. Das gängigste Verfahren zur Aufrechterhaltung identischer Volumes in diesen Servergruppen mit Lastenausgleichsmodul besteht darin, die Einstellungen der mobilEcho-Volumes zu replizieren; in mobilEcho 4.5 oder früher sind diese Einstellungen in der Registry gespeichert.*

*In Acronis Access wurden die Volume-Einstellungen in eine SQL-Datenbank ausgelagert. Nach einem Upgrade auf Acronis Access können die vorhandenen Skript-Registry-Updates, die beim Hinzufügen neuer Volumes zu mobilEcho Servern genutzt wurden, nicht mehr verwendet werden. Ab Version 5.1 ist eine neue Funktion verfügbar, mit der Servergruppen mit Lastenausgleichsmodul automatisch über die Acronis Access Server-Konsole verwaltet werden können. Mit dieser Funktion erübrigt sich die Replizierung von Registry-Einstellungen und Skript-Updates auf die Server. Zum Hinzufügen einer neuen Datenquelle (Volume) zu den Servern ist nur noch ein einziger Schritt erforderlich, der automatisch von der Management Konsole ausgeführt wird. Weitere Informationen finden Sie im Artikel Cluster-Gruppen.*

**Wichtige Hinweise zu Szenario 5 – Windows Failover Cluster**

*Die Installation und das Upgrade von mobilEcho in einem Windows Failover Cluster ist ein kompliziertes Verfahren. Aufgrund der in mobilEcho 5.0 eingeführten Architekturänderungen funktioniert mobilEcho auf Windows Failover Clustern jetzt anders als zuvor.*

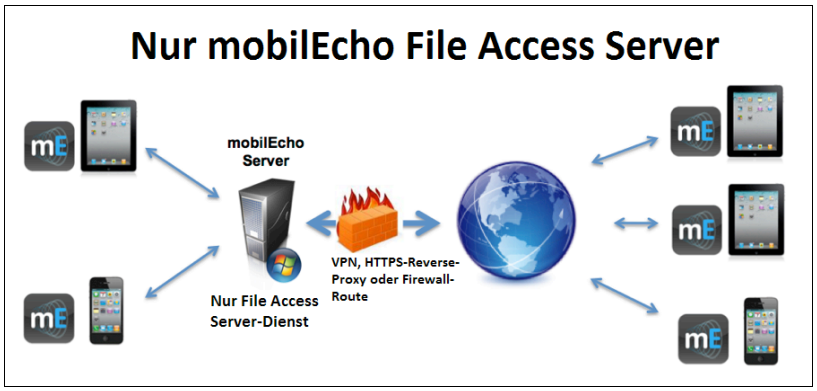
*Anweisungen zum Installieren von Acronis Access in einem Cluster finden Sie im Artikel Acronis Access in einem Cluster installieren.*

*Anweisungen für das Upgrade eines mobilEcho-Clusters auf ein Acronis Access Cluster finden Sie im Artikel Upgrade von Acronis Access in einem Cluster.*

## Themen

### 2.2.2.1 Upgrade eines einzelnen mobilEcho Servers ohne Client Management

**Szenario 1 – Upgrade eines einzelnen mobilEcho Servers ohne Client Management**




In diesem Szenario wird auf einem einzelnen Windows Server nur der mobilEcho File Access Server Dienst ausgeführt. In dieser Architektur ist die optionale mobilEcho Client Management Administrator-Webkonsole nicht aktiviert und die Richtlinien- und Remote-Verwaltungsfunktionen von mobilEcho werden nicht verwendet. Bei der Einrichtung von mobilEcho geben die Benutzer den Servernamen, ihren Benutzernamen und ihr Kennwort manuell in die mobilEcho App ein.

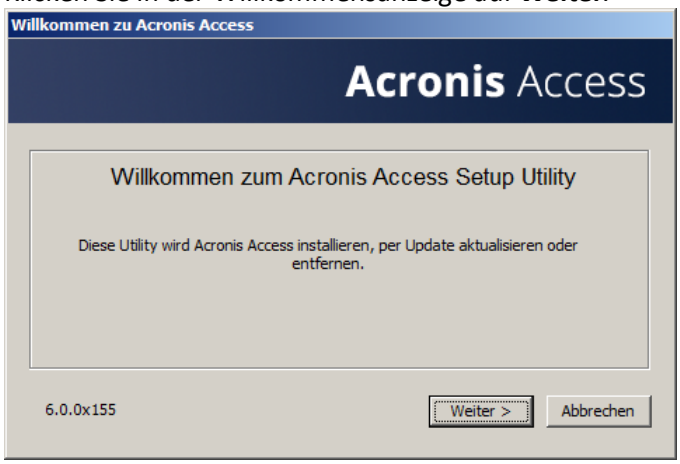
Bei einem Upgrade auf Acronis Access wird ein Upgrade des mobilEcho File Access Servers auf einen Acronis Access Gateway Server durchgeführt. mobilEcho Clients können weiterhin eine Verbindung zu diesem Dienst herstellen und der Dienst fungiert weiterhin als Gateway zu allen Dateiserver-, NAS- oder SharePoint-Datenquellen, auf die die Benutzer zugreifen.

Bei dem Upgrade wird auch die Acronis Access Server Webkonsole installiert. Diese neue Konsole ersetzt das Windows-Programm mobilEcho-Administrator, das bisher zur Verwaltung von mobilEcho Servern verwendet wurde. Mit der Acronis Access Server Webkonsole können Sie mobilEcho Server über eine einheitliche Weboberfläche verwalten und bei Bedarf die Vorteile weiterer Funktionen zur Verwaltung von Clients nutzen.

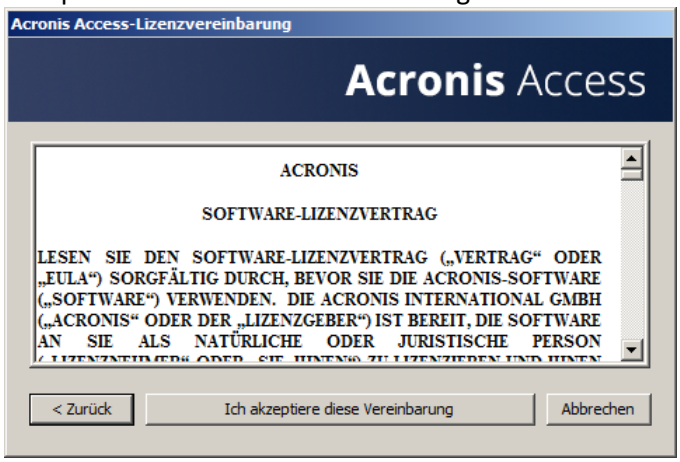
**So führen Sie ein Upgrade auf Acronis Access aus:**

1. Sichern Sie alle erforderlichen Dateien wie in den folgenden Anleitungen beschrieben: mobilEcho 4.5 Backup bzw. activEcho 2.7 Backup.
2. Deaktivieren Sie alle vorhandenen Virenschutzprogramme, da sie unter Umständen den Installationsvorgang unterbrechen und somit eine fehlerhafte Installation verursachen können.
3. Laden Sie den Acronis Access Server Installer auf den mobilEcho Server herunter und führen Sie ihn aus.
   a. Um auf den neuesten Installer zuzugreifen, besuchen Sie die folgende Website: http://support.grouplogic.com/?page_id=3598
   b. Sie müssen die Seriennummer des Produkts zur Überprüfung eingeben, bevor Sie den Installer herunterladen.
   c. Die Installer-Datei hat folgenden Namen: AcronisAccessSetup.exe

4. Klicken Sie in der Willkommensanzeige auf **Weiter**.

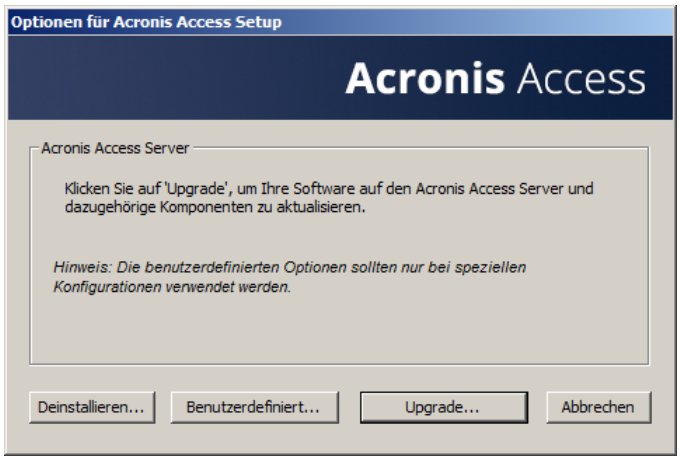



5. Akzeptieren Sie die Lizenzvereinbarung.

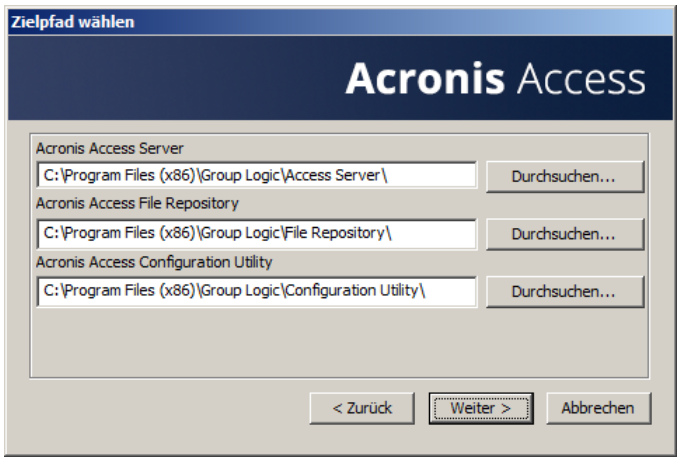



6. Klicken Sie auf **Upgrade**, um den mobilEcho File Access Server-Dienst automatisch auf einen Acronis Access Gateway Server zu aktualisieren. Im Rahmen des Upgrade-Prozesses werden der Acronis Access Server und die erforderlichen Dienste installiert.

> ***Hinweis**: Wählen Sie nicht **Benutzerdefiniert** und installieren Sie nur den Acronis Access Gateway Server. Der Acronis Access Server ist die neue Webkonsole, die das Windows-Programm mobilEcho-Administrator ersetzt. Er ist für die Verwaltung des mobilEcho Servers erforderlich. Wenn Sie ihn nicht installieren, haben Sie keine Möglichkeit, die mobilEcho-Einstellungen zu ändern oder Zugriff auf neue Dateifreigaben zu gewähren.*



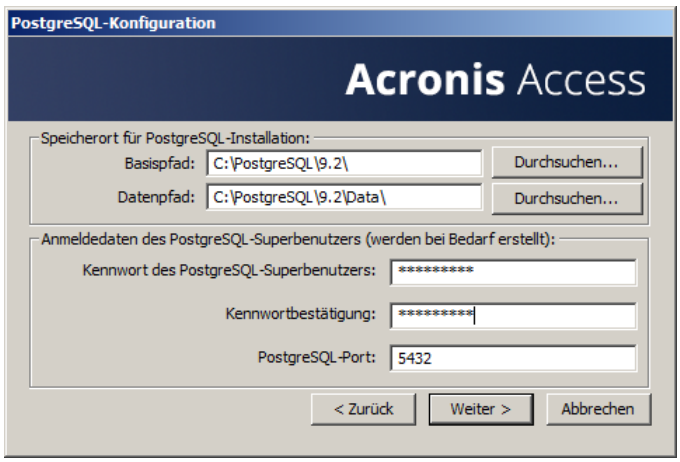
7. Wählen Sie einen Installationsspeicherort für die zu installierenden Acronis Access-Komponenten aus. Falls Sie ein Upgrade eines vorhandenen mobilEcho Servers durchführen, wird für diese Pfade standardmäßig der vorhandene Installationsspeicherort verwendet. Wir empfehlen, diese Installationspfade nicht zu ändern.




8. Die Einstellungen des Acronis Access Servers werden in einer PostgreSQL-Datenbank gespeichert. Diese Datenbank ist erforderlich und wird automatisch installiert.

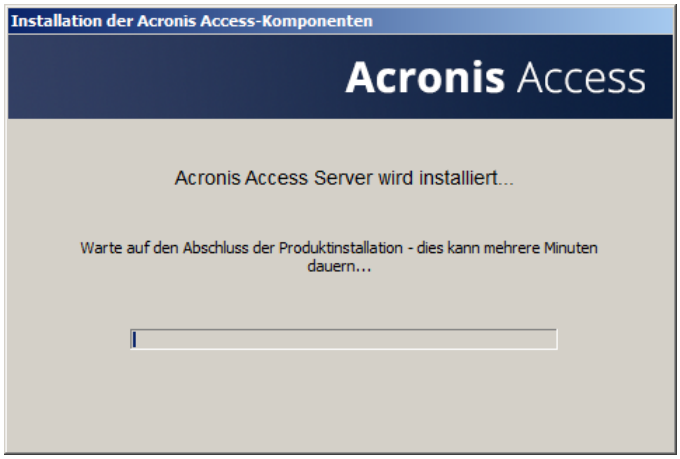
   ***Hinweis:*** *Geben Sie ein Super-User-Kennwort für das Administratorkonto 'postgres' ein und bestätigen Sie es. Bewahren Sie dieses Kennwort an einem sicheren Platz auf.*

   ***Hinweis:*** *Eine Änderung des PostgresSQL-Installationsspeicherorts und -Ports wird nicht empfohlen.*

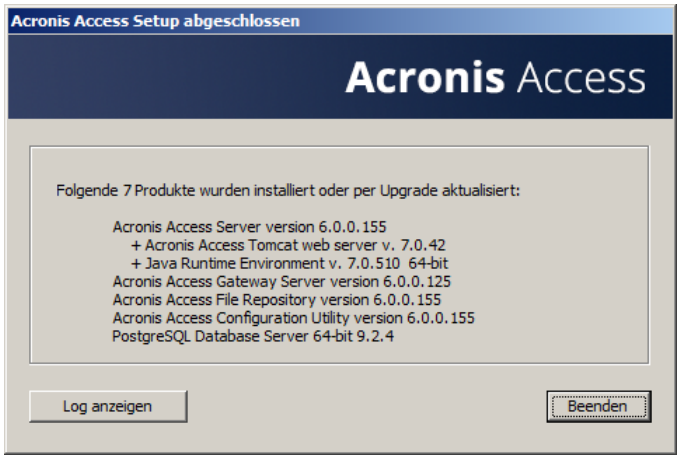


9. Überprüfen Sie die für Installation und Upgrade aufgeführten Dienste. Klicken Sie dann auf **Installieren**, um mit dem Upgrade zu beginnen.


**Hinweis:** Alle erforderlichen Komponenten werden automatisch nacheinander installiert. Dieser Vorgang kann je nach Server 5 bis 15 Minuten dauern. Zukünftige Upgrades werden schneller installiert.



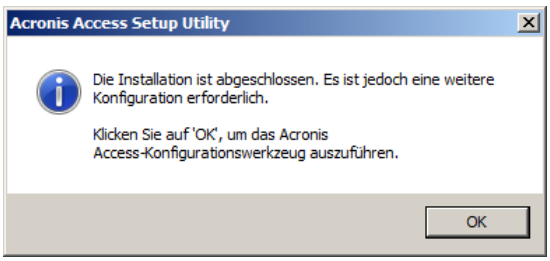

10. Nach Abschluss der Installation wird eine Zusammenfassung der installierten Komponenten angezeigt. Klicken Sie auf **Beenden**, um fortzufahren.



11. An diesem Punkt des Upgrade-Prozesses sind alle erforderlichen Software-Komponenten installiert. Jetzt müssen Sie jedoch die Netzwerkschnittstellen, Ports und Zertifikate konfigurieren, die verwendet werden sollen.

    ***WICHTIGER HINWEIS:*** *Wenn Sie diesen Konfigurationsschritt nicht ausführen, ist der mobilEcho Server nicht funktionsfähig. Dieser Schritt ist obligatorisch.*

    *Beim Beenden des Installationsprogramms werden Sie zur Ausführung des Acronis Access-Konfigurationswerkzeugs aufgefordert. Klicken Sie auf* ***OK****, um fortzufahren.*

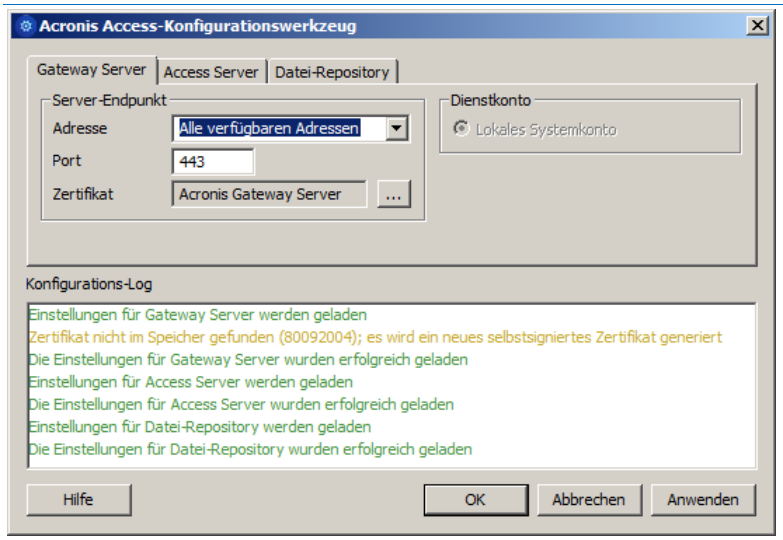
    *Falls Sie diesen Schritt versehentlich überspringen oder die Netzwerkschnittstellen, Ports oder Zertifikate zu einem späteren Zeitpunkt ändern müssen, können Sie das Konfigurationswerkzeug jederzeit manuell ausführen.*

    *Auf mobilEcho Servern, für die ein Upgrade durchgeführt wurde, ist das Werkzeug standardmäßig in folgendem Ordner gespeichert:*

    ***C:\Programme (x86)\Group Logic\Configuration Utility\AcronisAccessConfiguration.exe***

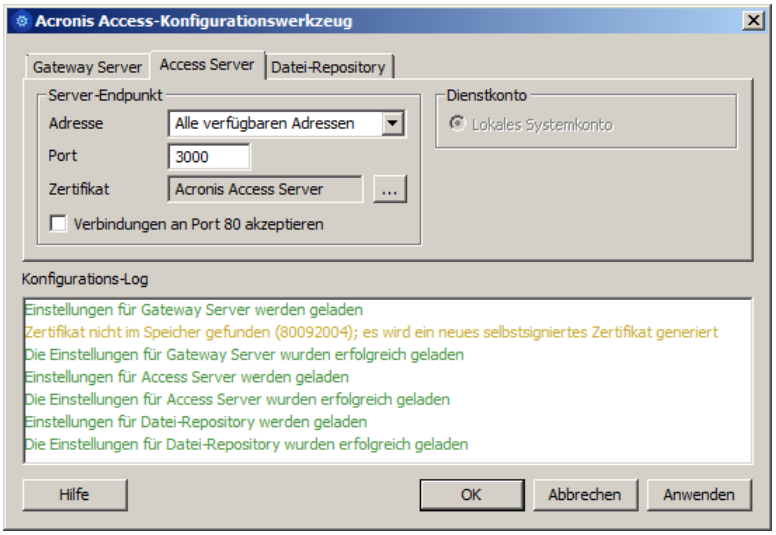
12. Im Konfigurationswerkzeug können Sie auf der Registerkarte 'Gateway Server' die Netzwerkadresse, den Port und das Zertifikat des Acronis Access Gateway Servers konfigurieren. Der Acronis Access Gateway Server ist der mobilEcho-Kerndienst, zu dem die mobilEcho Clients eine Verbindung herstellen und der Zugriff auf Dateiserver, NAS und SharePoint-Server bietet. Dieser Dienst trug in Versionen vor Acronis Access die Bezeichnung mobilEcho File Access Server.

    ***Hinweis:*** *Die vorhandenen Einstellungen bleiben erhalten. Überprüfen Sie, ob diese Einstellungen mit den vorhandenen mobilEcho File Access Server-Einstellungen übereinstimmen. Dieser Dienst kann in der Regel auf allen verfügbaren Netzwerkadressen an Port 443 ausgeführt werden. Falls Sie über ein SSL-Serveridentitätszertifikat verfügen, wird dieses automatisch ausgewählt. Andernfalls wird ein selbstsigniertes Zertifikat generiert.*

13. Auf der Registerkarte 'Access Server' werden die Netzwerkadresse, der Port und das Zertifikat des Acronis Access Servers konfiguriert. Der Acronis Access Server ist die Webkonsole, über die alle Aufgaben im Zusammenhang mit Serveradministration und Remote-Client-Management durchgeführt werden. Diese Konsole ersetzt das Windows-Programm mobilEcho-Administrator und ist eine erforderliche Komponente.

    ***Hinweis:*** *Überprüfen Sie die Einstellungen für den Access Server. Die Standardeinstellungen werden empfohlen. Diese Webkonsole kann in der Regel auf allen verfügbaren Netzwerkadressen an Port 3000 ausgeführt werden. Falls Sie über ein SSL-Serveridentitätszertifikat verfügen, wird dieses automatisch ausgewählt. Andernfalls wird ein selbstsigniertes Zertifikat generiert.*



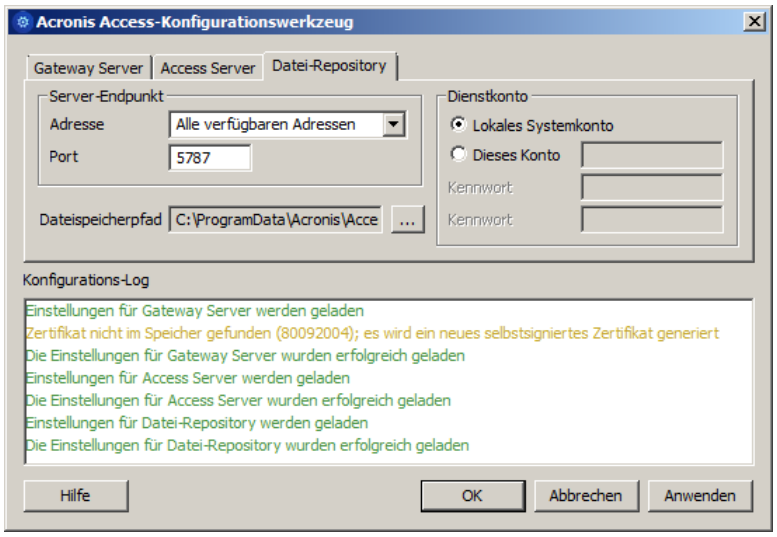

14. Acronis Access Server erfordert die Auswahl eines Speicherorts für das Datei-Repository. Falls Sie nur mobilEcho verwenden, wird in diesem Datei-Repository zwar nichts gespeichert, die Angabe eines Speicherorts ist aber dennoch erforderlich.

    *Dieses Repository wird von den Dateisynchronisierungs- und Freigabefunktionen (Sync & Share) von Acronis activEcho verwendet. Beim Upgrade eines Servers, auf dem diese Funktionen noch nicht installiert sind, werden sie nicht aktiviert, Sie können sie jedoch bei Bedarf zu einem späteren Zeitpunkt aktivieren.*

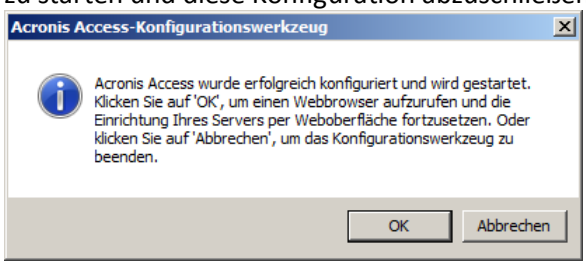
    *Das Datei-Repository wird standardmäßig in folgendem Ordner gespeichert:*

    ***C:\ProgramData\Acronis\Access\FileStore***

    *Falls Sie activEcho später testen möchten, wählen Sie einen Speicherort auf einem Datenlaufwerk anstatt auf Laufwerk C: Auch dieser Speicherort kann nach der Installation geändert werden.*




15. Klicken Sie auf **OK**, um das Konfigurationswerkzeug zu beenden und diese Einstellungen anzuwenden.
16. Jetzt melden Sie sich zum ersten Mal bei der Acronis Access Server-Webkonsole an, um die Konfiguration abzuschließen. Sie werden aufgefordert, auf 'OK' zu klicken, um einen Webbrowser zu starten und diese Konfiguration abzuschließen.

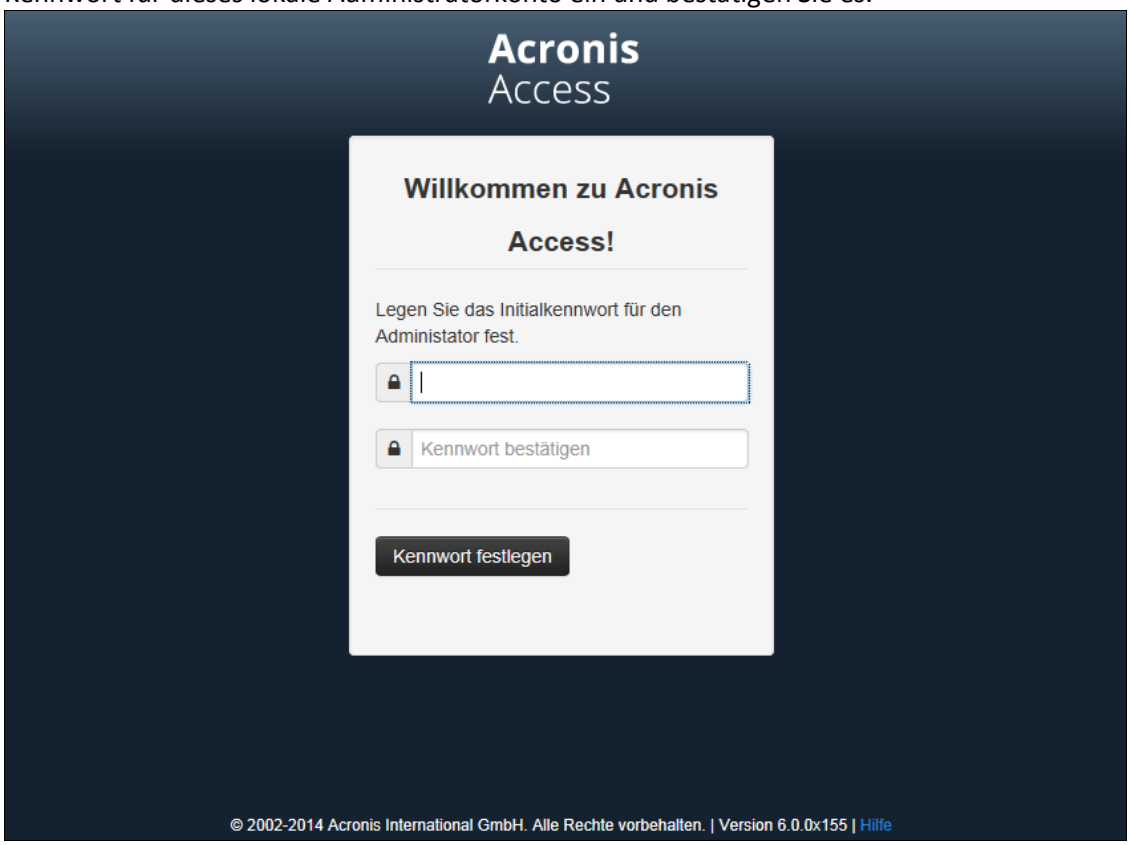



**Erforderliche Erstkonfiguration von Acronis Access:**

1. Nach Durchführung der oben genannten Schritte sollte die Acronis Access Server-Webkonsole automatisch geöffnet werden. Beim ersten Mal können das Starten der Dienste und das Laden der Webseite bis zu 30 Sekunden dauern.
2. Falls die Webseite nicht automatisch geladen wird, öffnen Sie einen Webbrowser und navigieren Sie zur HTTPS-Adresse und zum Port des Access Servers, die bzw. den Sie im Konfigurationswerkzeug ausgewählt haben.
   a. Zum Beispiel: https://mobilecho.mycompany.com:3000 oder https://localhost:3000

***Hinweis**: Die meisten Einstellungen auf den Seiten 'SMTP', 'Allgemeine Einstellungen' und 'LDAP' sind bereits aufgrund der mobilEcho-Installation vorhanden.*

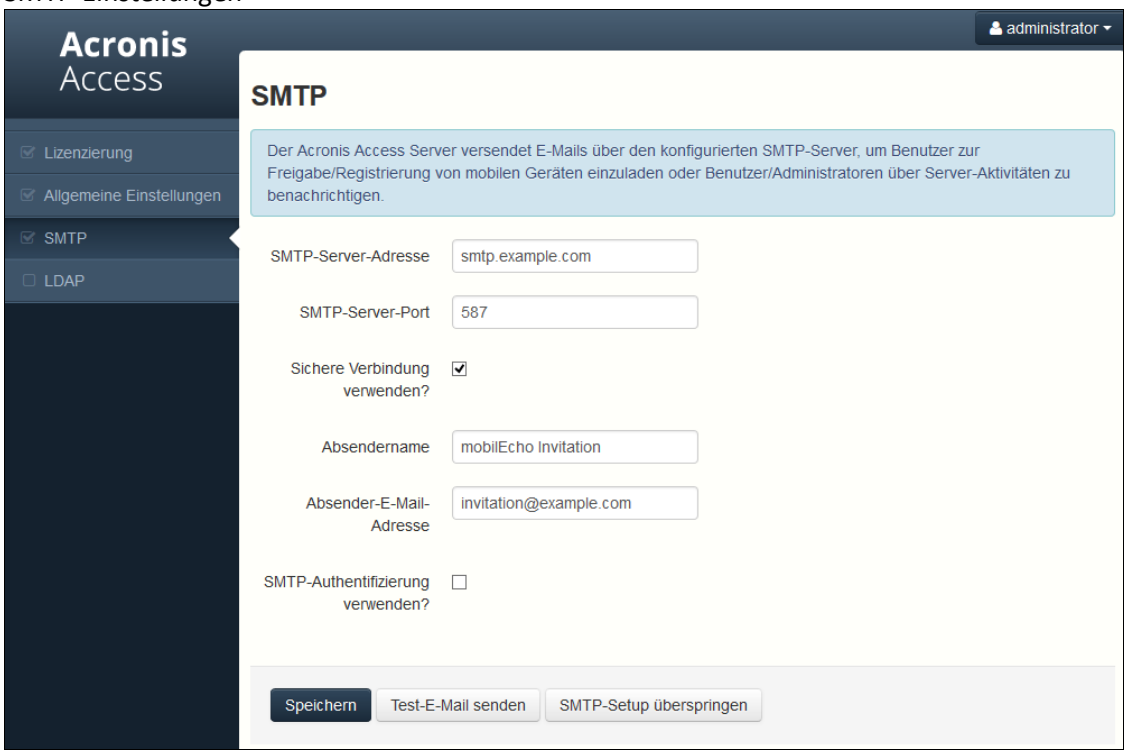
3. Acronis Access Server erfordert die Erstellung eines lokalen Administratorkontos. Geben Sie ein Kennwort für dieses lokale Administratorkonto ein und bestätigen Sie es.




   a. Der Benutzername für dieses lokale Administratorkonto lautet: administrator
   b. Bewahren Sie das Kennwort für das lokale Administratorkonto an einem sicheren Platz auf. Sie benötigen es zur Anmeldung als Administrator, bis Sie zusätzliche Benutzer als Administratoren konfigurieren.
   c. Nach der Konfiguration des Servers können Sie weitere Active Directory-Benutzer oder -Gruppen als Administratoren des Servers festlegen.
4. Jetzt wird ein Setup-Assistent angezeigt, der Sie durch den verbleibenden Konfigurationsprozess führt.
5. Lizenzierung

a) Sie werden aufgefordert, den neuen Lizenztyp einzugeben oder die alte mobilEcho-Lizenz weiter zu verwenden.

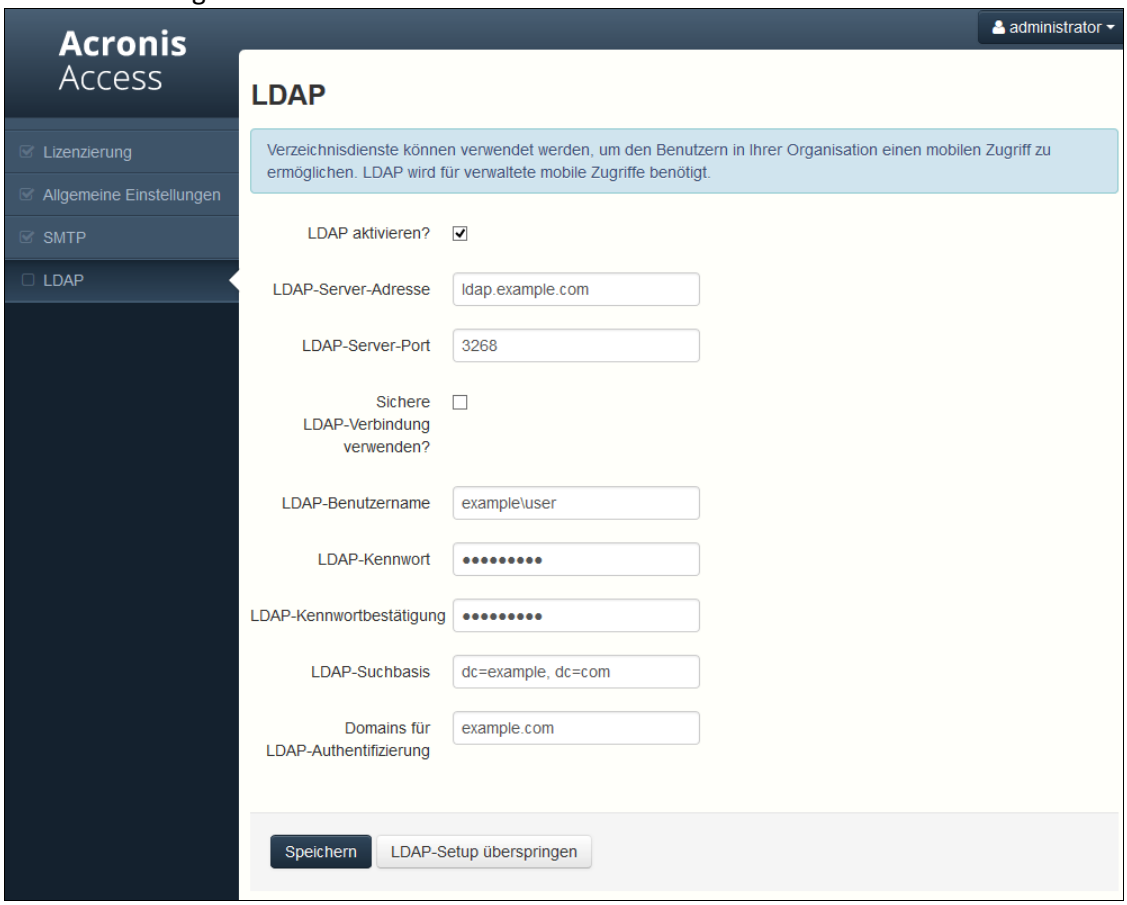
6. SMTP-Einstellungen




a. Sie werden aufgefordert, die SMTP-Einstellungen zu konfigurieren, die der Access Server zum Senden von E-Mail-Warnungen und Einladungen zur Client-Registrierung verwendet.

b. Es steht eine Option zum Senden einer Test-E-Mail zur Verfügung, um diese Einstellungen zu bestätigen.

7. LDAP-Einstellungen




   a. Der Acronis Access Server benötigt eine LDAP-Verbindung, um das Active Directory nach den Benutzern und Gruppen zu durchsuchen, denen Sie Richtlinien und Datenquellen zuweisen möchten.
   b. Geben Sie die LDAP-Informationen für einen Active Directory-Server im Netzwerk ein. Im Fall eines Netzwerks mit mehreren Domains muss es sich hierbei um einen globalen Katalog-Server an Port 3268 oder 3269 handeln (für SSL-Verbindungen). Für jedes Feld steht eine QuickInfo mit weiteren Details zur Verfügung.
   c. Sie müssen einen LDAP-Benutzernamen und ein Kennwort konfigurieren; diese Angaben werden verwendet, wenn der Server LDAP-Anforderungen stellt.
   d. Die eingegebenen LDAP-Einstellungen werden beim Speichern getestet.

8. Lokaler Gateway Server – Adresse für Client-Verbindungen


   a. Der mobilEcho Gateway Server wurde automatisch für die Verwaltung durch die Acronis Access Server Webkonsole gekoppelt. Diese Verbindung wird standardmäßig anhand der IP-Adresse hergestellt und kann später geändert werden.

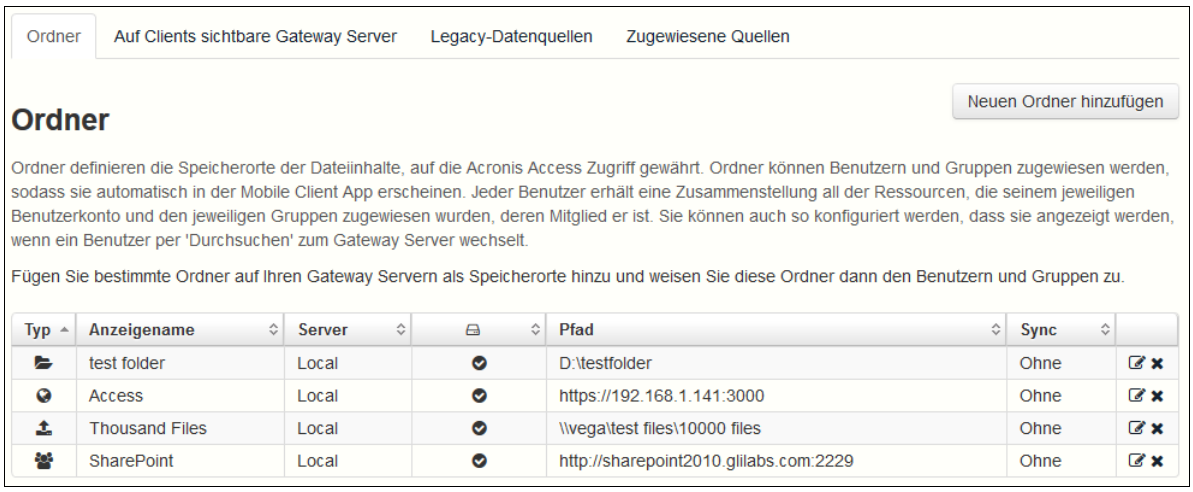
b. In diesem Schritt müssen Sie die Netzwerkadresse eingeben, über die die mobilEcho Clients eine Verbindung zu diesem mobilEcho Server herstellen. In der Regel ist dies eine DNS-Adresse, möglicherweise die DNS-Adresse dieses Servers. Es kann aber auch die Adresse eines Proxy-Servers sein, über den der Zugriff auf diesen Server erfolgt.

9. Die Erstkonfiguration ist jetzt abgeschlossen.
   a. Klicken Sie auf **Konfiguration beenden**, um fortzufahren.

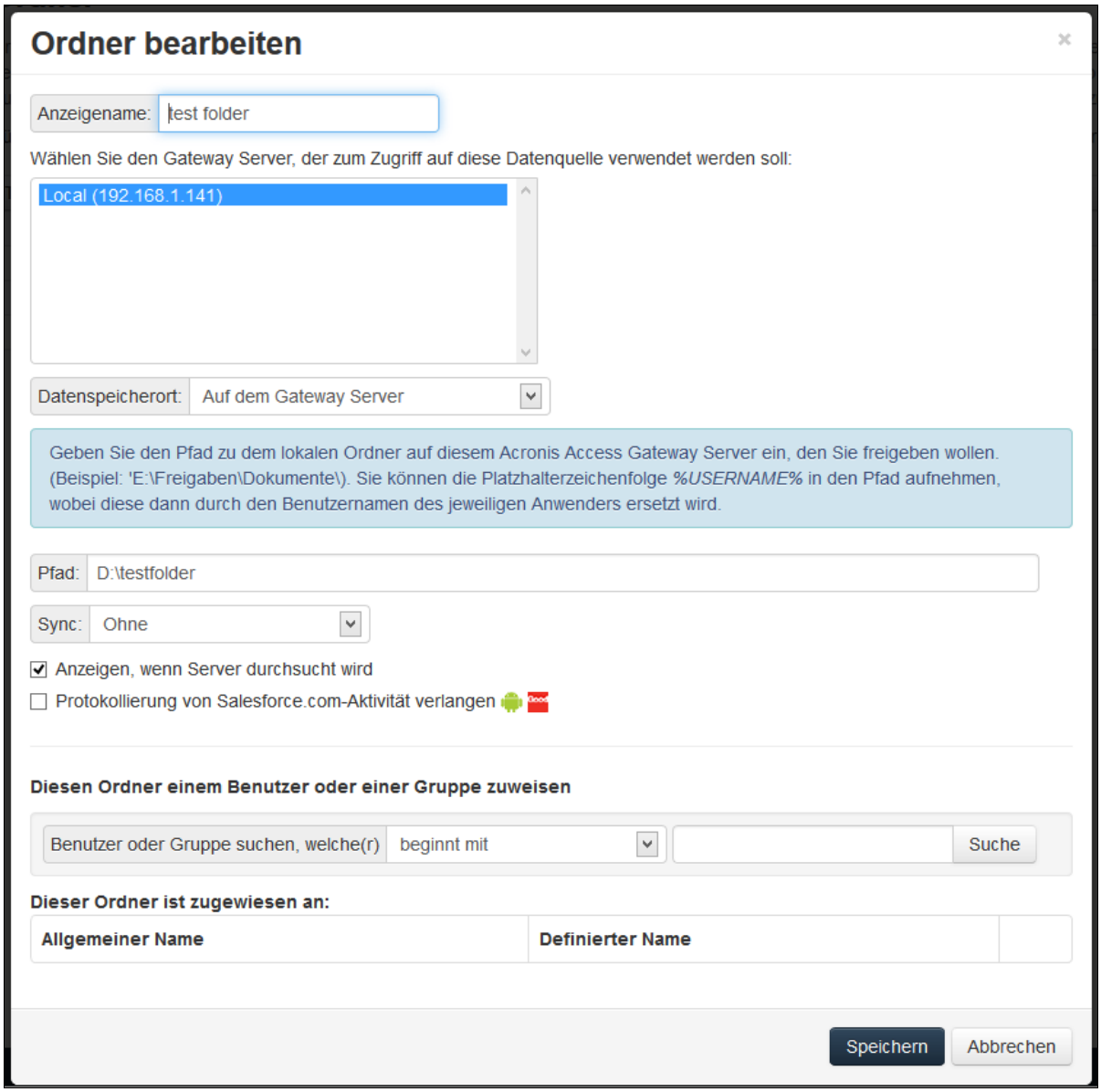
### Mit dem mobilEcho Gateway Server arbeiten

Der Gateway Server wird während des Setup-Vorgangs automatisch registriert und anschließend in der Liste der Gateway Server angezeigt. Hier können Sie die Einstellungen des Servers ändern sowie Details und Status anzeigen.


Bei der Registrierung wurden die Volumes, die vor dem Upgrade auf Acronis Access auf dem mobilEcho Gateway Server vorhanden waren, in die Ordnerliste auf der Seite 'Datenquellen' importiert.



In mobilEcho 5.0 gibt es keine „Volumes“ mehr. Anstatt Volumes für die Freigabe von Datenquellen zu verwenden, erstellen Sie jetzt Ordner. Diese Ordner verfügen über die optionale Eigenschaft 'Anzeigen, wenn Server durchsucht wird'. Bei aktivierter Option wird der Ordner angezeigt, wenn ein Benutzer den Stamm des Gateway Servers in seiner mobilEcho-App durchsucht, ebenso wie in mobilEcho 4.5 oder früher Volumes angezeigt wurden.




Alle Volumes aus dem mobilEcho Server der Version 4.5 oder früher wurden als Ordner mit aktivierter Eigenschaft 'Anzeigen, wenn Server durchsucht wird' in die Acronis Access-Konsole importiert. Daher werden sie weiterhin angezeigt, wenn die Benutzer den Stamm eines mobilEcho Gateway Servers durchsuchen. Alle später hinzugefügten Ordner können durch Aktivierung dieser Einstellung so konfiguriert werden, dass sie sich wie Volumes verhalten. Sie können nun auch erweiterte Funktionen zur Client-Verwaltung nutzen, z.B. die Funktion, Ordner hinzuzufügen, die automatisch in der mobilEcho Client-App der Active Directory-Benutzer oder -Gruppen angezeigt werden, denen Sie sie zuweisen.

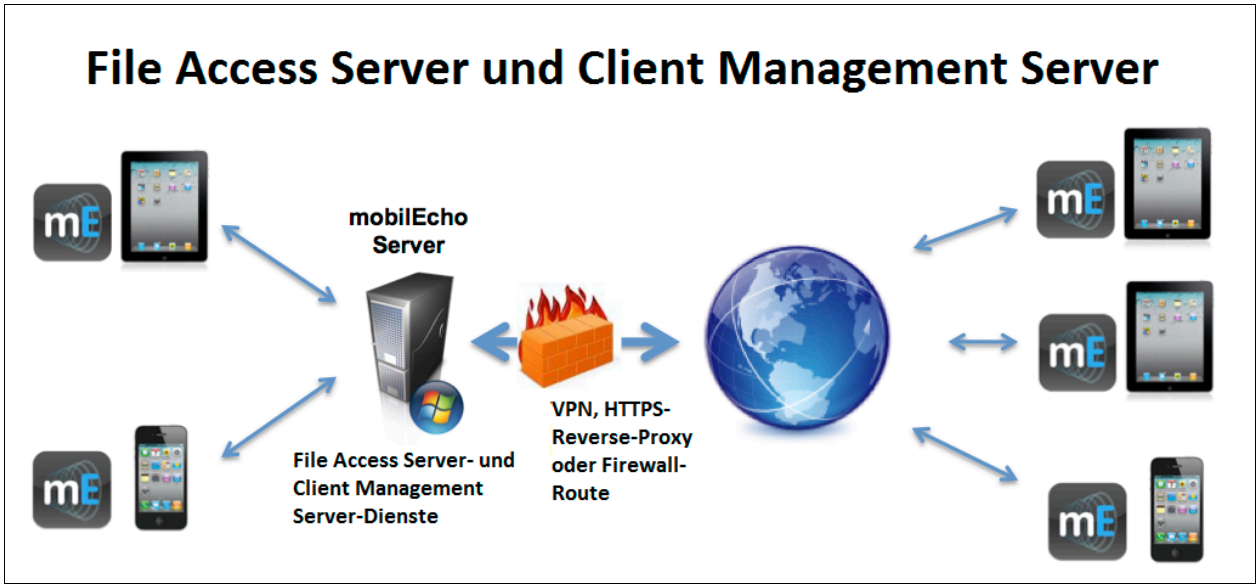
Wie unten dargestellt wurden die vier vorhandenen Volumes dieses mobilEcho 4.5 Servers nach der Gateway Server-Registrierung in die Ordnerliste importiert und werden beim Durchsuchen des Servers mit der mobilEcho-App weiterhin angezeigt.


Sie können jetzt außerdem Client-Richtlinien erstellen und verwenden und offiziell Benutzer beim Server registrieren, damit diese von den Richtlinien verwaltet werden. Sie können eine für alle Benutzer geltende Standardrichtlinie aktivieren und konfigurieren oder aber benutzerdefinierte Richtlinien auf Basis von Active Directory-Benutzern und -Gruppen hinzufügen.

Nachdem Sie Richtlinien konfiguriert haben, können Sie auf der Seite 'Benutzer registrieren' E-Mails mit Registrierungseinladungen an die Benutzer senden, sodass sich diese als verwaltete Benutzer registrieren können.

### 2.2.2.2 Upgrade eines einzelnen mobilEcho Servers mit aktiviertem Client Management-Dienst

**Szenario 2 – Upgrade eines einzelnen mobilEcho Servers mit aktiviertem Client Management-Dienst**



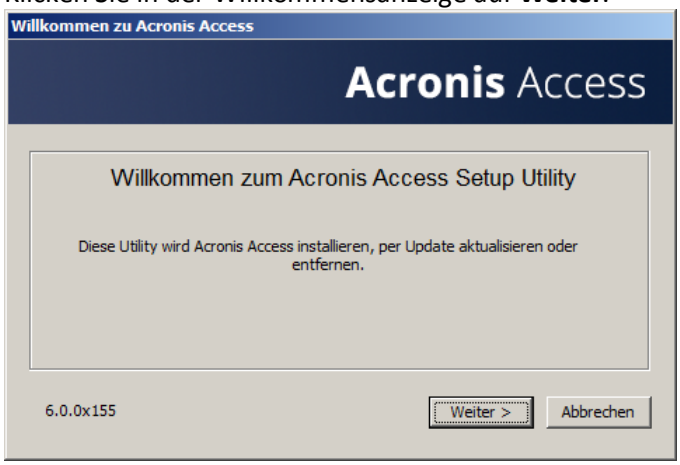
In diesem Szenario wird auf einem einzelnen Windows Server mobilEcho 4.5 oder früher ausgeführt. Auf diesem Server wird zum einen der erforderliche mobilEcho File Access Server-Dienst ausgeführt, zum anderen ist der optionale mobilEcho Client Management Server-Dienst aktiviert.

Bei einem Upgrade auf Acronis Access wird ein Upgrade des mobilEcho File Access Servers auf einen Acronis Access Gateway Server durchgeführt. mobilEcho Clients können weiterhin eine Verbindung zu diesem Dienst herstellen und der Dienst fungiert weiterhin als Gateway zu allen Dateiserver-, NAS- oder SharePoint-Datenquellen, auf die die Benutzer zugreifen.

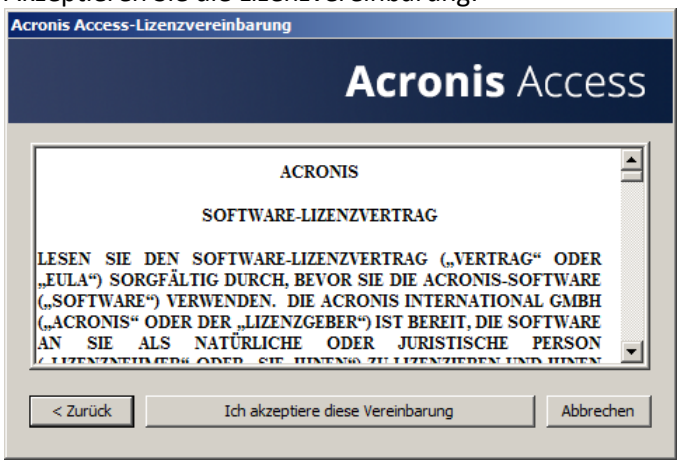
Für die mobilEcho Client Management Administrator-Webkonsole erfolgt ein Upgrade auf die Acronis Access Server-Webkonsole. Mit dieser neuen Webkonsole können Sie mobilEcho Server und Clients über eine einheitliche Weboberfläche verwalten.

**So führen Sie ein Upgrade von Acronis Access aus:**

1. Sichern Sie alle erforderlichen Dateien wie in den folgenden Anleitungen beschrieben: mobilEcho 4.5 Backup bzw. activEcho 2.7 Backup.
2. Deaktivieren Sie alle vorhandenen Virenschutzprogramme, da sie unter Umständen den Installationsvorgang unterbrechen und somit eine fehlerhafte Installation verursachen können.
3. Laden Sie den Acronis Access Server Installer auf den mobilEcho Server herunter und führen Sie ihn aus.
   a. Um auf den neuesten Installer zuzugreifen, besuchen Sie die folgende Website: http://support.grouplogic.com/?page_id=3598
   b. Sie müssen die Seriennummer des Produkts zur Überprüfung eingeben, bevor Sie den Installer herunterladen.
   c. Die Installer-Datei hat folgenden Namen: AcronisAccessSetup.exe
4. Klicken Sie in der Willkommensanzeige auf **Weiter**.

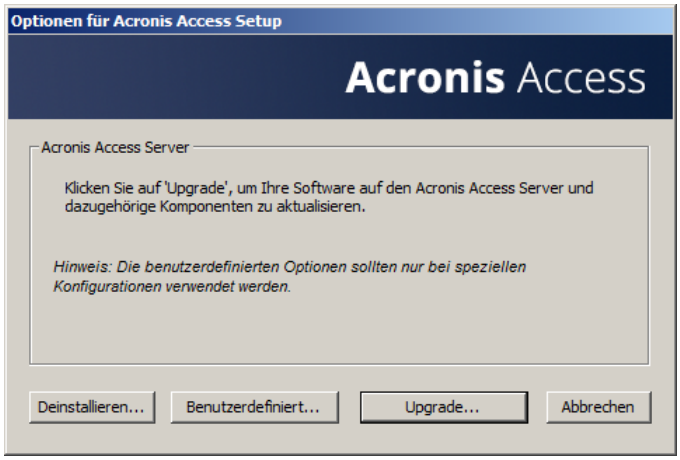


5. Akzeptieren Sie die Lizenzvereinbarung.

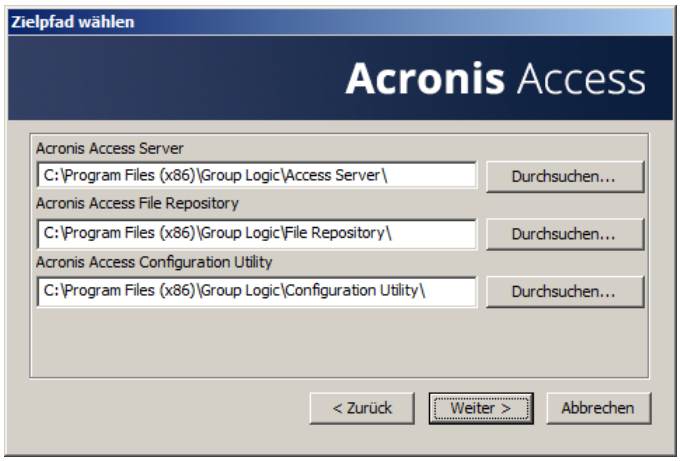



6. Klicken Sie auf **Upgrade**, um den mobilEcho File Access Server-Dienst automatisch auf einen Acronis Access Gateway Server zu aktualisieren. Im Rahmen des Upgrade-Prozesses werden der Acronis Access Server und die erforderlichen Dienste installiert.

> ***Hinweis**: Wählen Sie nicht **Benutzerdefiniert** und installieren Sie nur den Acronis Access Gateway Server. Der Acronis Access Server ist die neue Webkonsole, die das Windows-Programm mobilEcho-Administrator ersetzt. Er ist für die Verwaltung des mobilEcho Servers erforderlich. Wenn Sie ihn nicht installieren, haben Sie keine Möglichkeit, die mobilEcho-Einstellungen zu ändern oder Zugriff auf neue Dateifreigaben zu gewähren.*



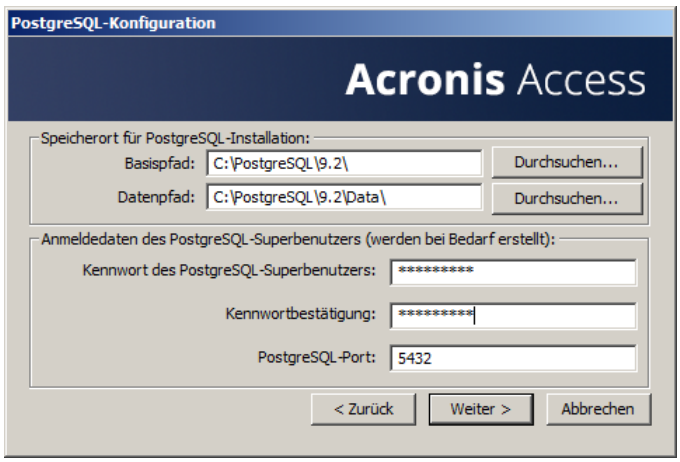
7. Wählen Sie einen Installationsspeicherort für die zu installierenden Acronis Access-Komponenten aus. Falls Sie ein Upgrade eines vorhandenen mobilEcho Servers durchführen, wird für diese Pfade standardmäßig der vorhandene Installationsspeicherort verwendet. Wir empfehlen, diese Installationspfade nicht zu ändern.




8. Die Einstellungen des Acronis Access Servers werden in einer PostgreSQL-Datenbank gespeichert. Diese Datenbank ist erforderlich und wird automatisch installiert.

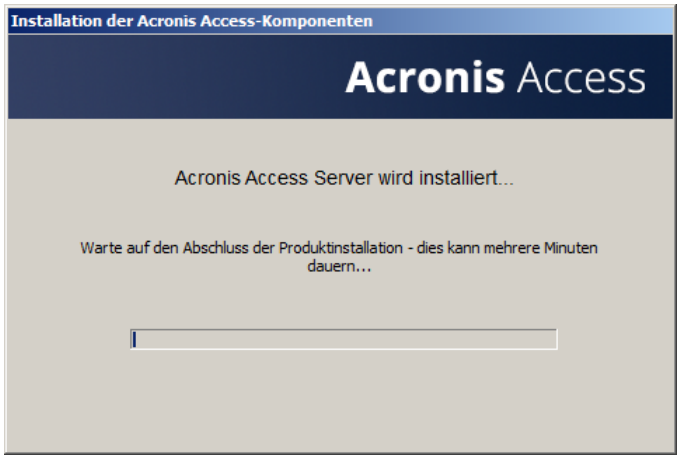
   ***Hinweis:*** *Geben Sie ein Super-User-Kennwort für das Administratorkonto 'postgres' ein und bestätigen Sie es. Bewahren Sie dieses Kennwort an einem sicheren Platz auf.*

   ***Hinweis:*** *Eine Änderung des PostgresSQL-Installationsspeicherorts und -Ports wird nicht empfohlen.*

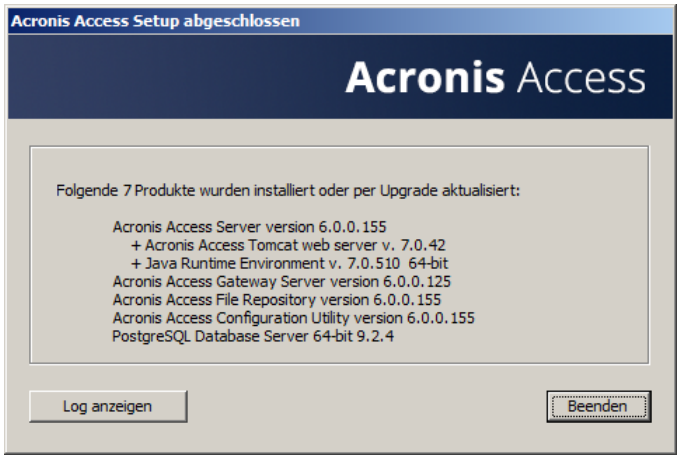


9. Überprüfen Sie die für Installation und Upgrade aufgeführten Dienste. Klicken Sie dann auf **Installieren**, um mit dem Upgrade zu beginnen.


**Hinweis:** Alle erforderlichen Komponenten werden automatisch nacheinander installiert. Dieser Vorgang kann je nach Server 5 bis 15 Minuten dauern. Zukünftige Upgrades werden schneller installiert.



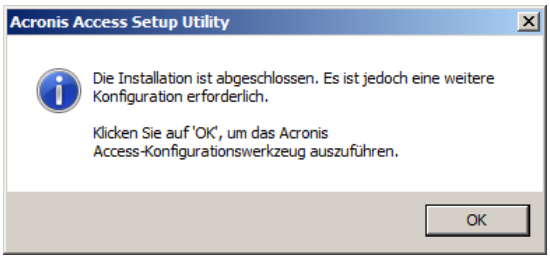

10. Nach Abschluss der Installation wird eine Zusammenfassung der installierten Komponenten angezeigt. Klicken Sie auf **Beenden**, um fortzufahren.




11. An diesem Punkt des Upgrade-Prozesses sind alle erforderlichen Software-Komponenten installiert. Jetzt müssen Sie jedoch die Netzwerkschnittstellen, Ports und Zertifikate konfigurieren, die verwendet werden sollen.

***WICHTIGER HINWEIS:*** *Wenn Sie diesen Konfigurationsschritt nicht ausführen, ist der mobilEcho Server nicht funktionsfähig. Dieser Schritt ist obligatorisch.*

*Beim Beenden des Installationsprogramms werden Sie zur Ausführung des Acronis Access-Konfigurationswerkzeugs aufgefordert. Klicken Sie auf* ***OK****, um fortzufahren.*



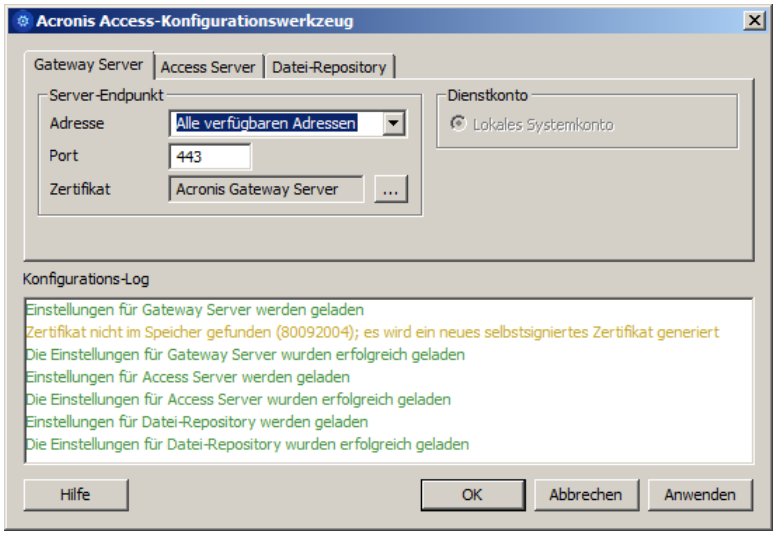

*Falls Sie diesen Schritt versehentlich überspringen oder die Netzwerkschnittstellen, Ports oder Zertifikate zu einem späteren Zeitpunkt ändern müssen, können Sie das Konfigurationswerkzeug jederzeit manuell ausführen.*

*Auf mobilEcho Servern, für die ein Upgrade durchgeführt wurde, ist das Werkzeug standardmäßig in folgendem Ordner gespeichert:*

***C:\Programme (x86)\Group Logic\Configuration Utility\AcronisAccessConfiguration.exe***

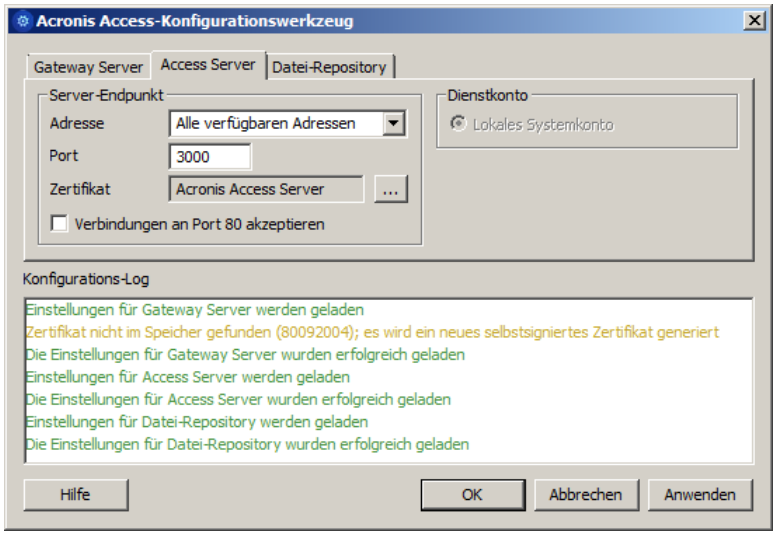
12. Im Konfigurationswerkzeug können Sie auf der Registerkarte 'Gateway Server' die Netzwerkadresse, den Port und das Zertifikat des Acronis Access Gateway Servers konfigurieren. Der Acronis Access Gateway Server ist der mobilEcho-Kerndienst, zu dem die mobilEcho Clients eine Verbindung herstellen und der Zugriff auf Dateiserver, NAS und SharePoint-Server bietet. Dieser Dienst trug in Versionen vor Acronis Access die Bezeichnung mobilEcho File Access Server.

***Hinweis:*** *Die vorhandenen Einstellungen bleiben erhalten. Überprüfen Sie, ob diese Einstellungen mit den vorhandenen mobilEcho File Access Server-Einstellungen übereinstimmen. Dieser Dienst kann in der Regel auf allen verfügbaren Netzwerkadressen an Port 443 ausgeführt werden. Falls Sie über ein SSL-Serveridentitätszertifikat verfügen, wird dieses automatisch ausgewählt. Andernfalls wird ein selbstsigniertes Zertifikat generiert.*




13. Auf der Registerkarte 'Access Server' werden die Netzwerkadresse, der Port und das Zertifikat des Acronis Access Servers konfiguriert. Der Acronis Access Server ist die Webkonsole, die die mobilEcho Client Management Server-Webkonsole ersetzt.

***Hinweis:*** *Überprüfen Sie, ob die Einstellungen mit den vorhandenen mobilEcho Client Management Server-Einstellungen übereinstimmen. Diese Webkonsole kann in der Regel auf allen verfügbaren Netzwerkadressen an Port 3000 ausgeführt werden. Falls Sie über ein SSL-Serveridentitätszertifikat verfügen, wird dieses automatisch ausgewählt. Andernfalls wird ein selbstsigniertes Zertifikat generiert.*



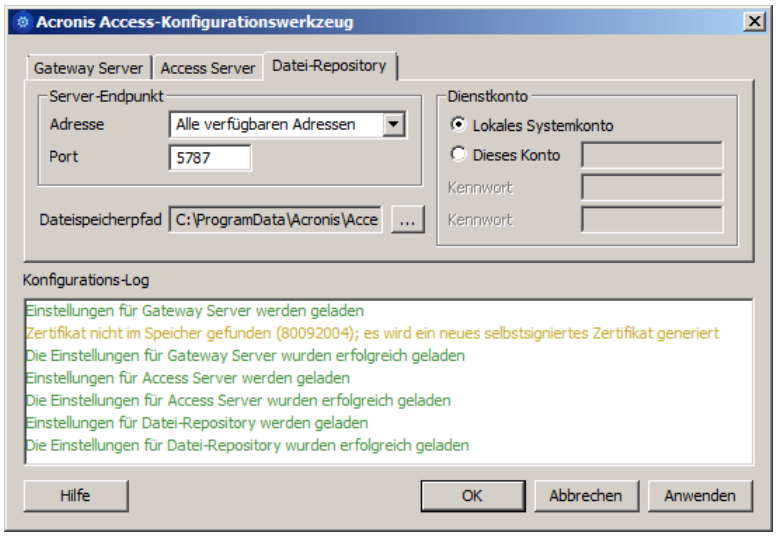

14. Acronis Access Server erfordert die Auswahl eines Speicherorts für das Datei-Repository. Falls Sie nur mobilEcho verwenden, wird in diesem Datei-Repository zwar nichts gespeichert, die Angabe eines Speicherorts ist aber dennoch erforderlich.

    *Dieses Repository wird von den Dateisynchronisierungs- und Freigabefunktionen (Sync & Share) von Acronis activEcho verwendet. Beim Upgrade eines Servers, auf dem diese Funktionen noch nicht installiert sind, werden sie nicht aktiviert, Sie können sie jedoch bei Bedarf zu einem späteren Zeitpunkt aktivieren.*

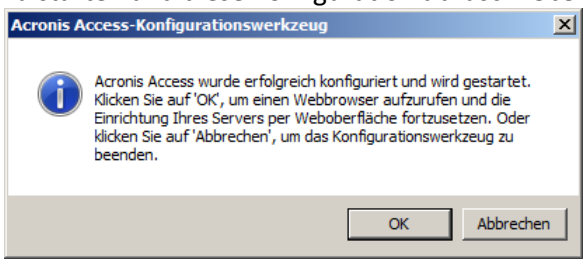
    *Das Datei-Repository wird standardmäßig in folgendem Ordner gespeichert:*

    ***C:\ProgramData\Acronis\Access\FileStore***

    *Falls Sie activEcho später testen möchten, wählen Sie einen Speicherort auf einem Datenlaufwerk anstatt auf Laufwerk C: Auch dieser Speicherort kann nach der Installation geändert werden.*



15. Klicken Sie auf **OK**, um das Konfigurationswerkzeug zu beenden und diese Einstellungen anzuwenden.
16. Jetzt melden Sie sich zum ersten Mal bei der Acronis Access Server-Webkonsole an, um die Konfiguration abzuschließen. Sie werden aufgefordert, auf 'OK' zu klicken, um einen Webbrowser zu starten und diese Konfiguration abzuschließen.

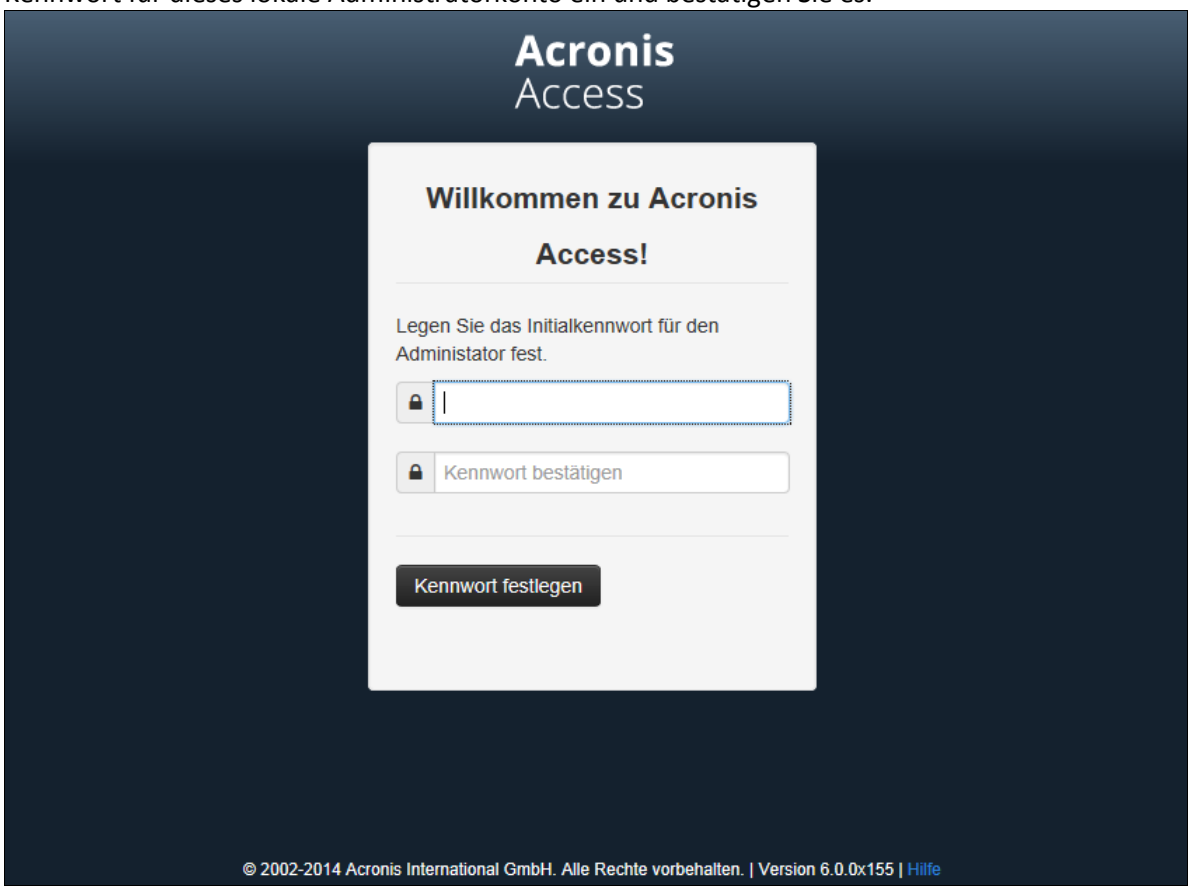



**Erforderliche Erstkonfiguration von Acronis Access:**

1. Nach Durchführung der oben genannten Schritte sollte die Acronis Access Server-Webkonsole automatisch geöffnet werden. Beim ersten Mal können das Starten der Dienste und das Laden der Webseite bis zu 30 Sekunden dauern.
2. Falls die Webseite nicht automatisch geladen wird, öffnen Sie einen Webbrowser und navigieren Sie zur HTTPS-Adresse und zum Port des Access Servers, die bzw. den Sie im Konfigurationswerkzeug ausgewählt haben.
   a. Zum Beispiel: https://mobilecho.mycompany.com:3000 oder https://localhost:3000

***Hinweis**: Die meisten Einstellungen auf den Seiten 'SMTP', 'Allgemeine Einstellungen' und 'LDAP' sind bereits aufgrund der mobilEcho-Installation vorhanden.*

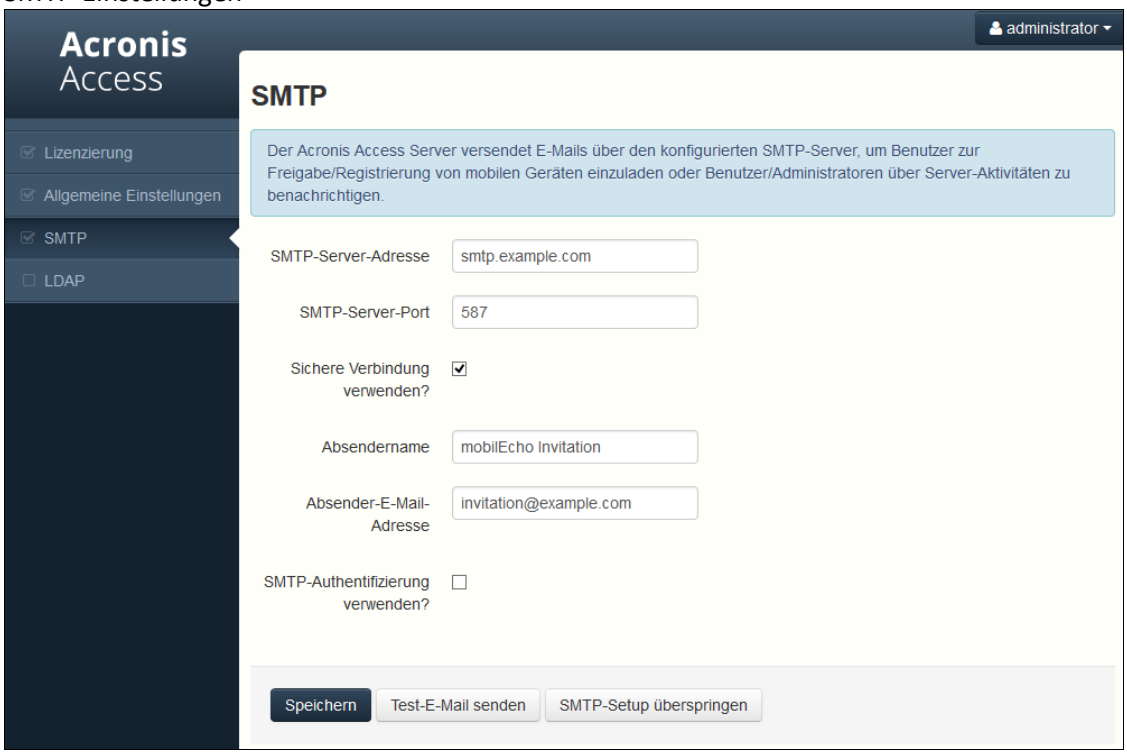
3. Acronis Access Server erfordert die Erstellung eines lokalen Administratorkontos. Geben Sie ein Kennwort für dieses lokale Administratorkonto ein und bestätigen Sie es.




   a. Der Benutzername für dieses lokale Administratorkonto lautet: administrator
   b. Bewahren Sie das Kennwort für das lokale Administratorkonto an einem sicheren Platz auf. Sie benötigen es zur Anmeldung als Administrator, bis Sie zusätzliche Benutzer als Administratoren konfigurieren.
   c. Nach der Konfiguration des Servers können Sie weitere Active Directory-Benutzer oder -Gruppen als Administratoren des Servers festlegen.
4. Jetzt wird ein Setup-Assistent angezeigt, der Sie durch den verbleibenden Konfigurationsprozess führt.
5. Lizenzierung

a) Sie werden aufgefordert, den neuen Lizenztyp einzugeben oder die alte mobilEcho-Lizenz weiter zu verwenden.

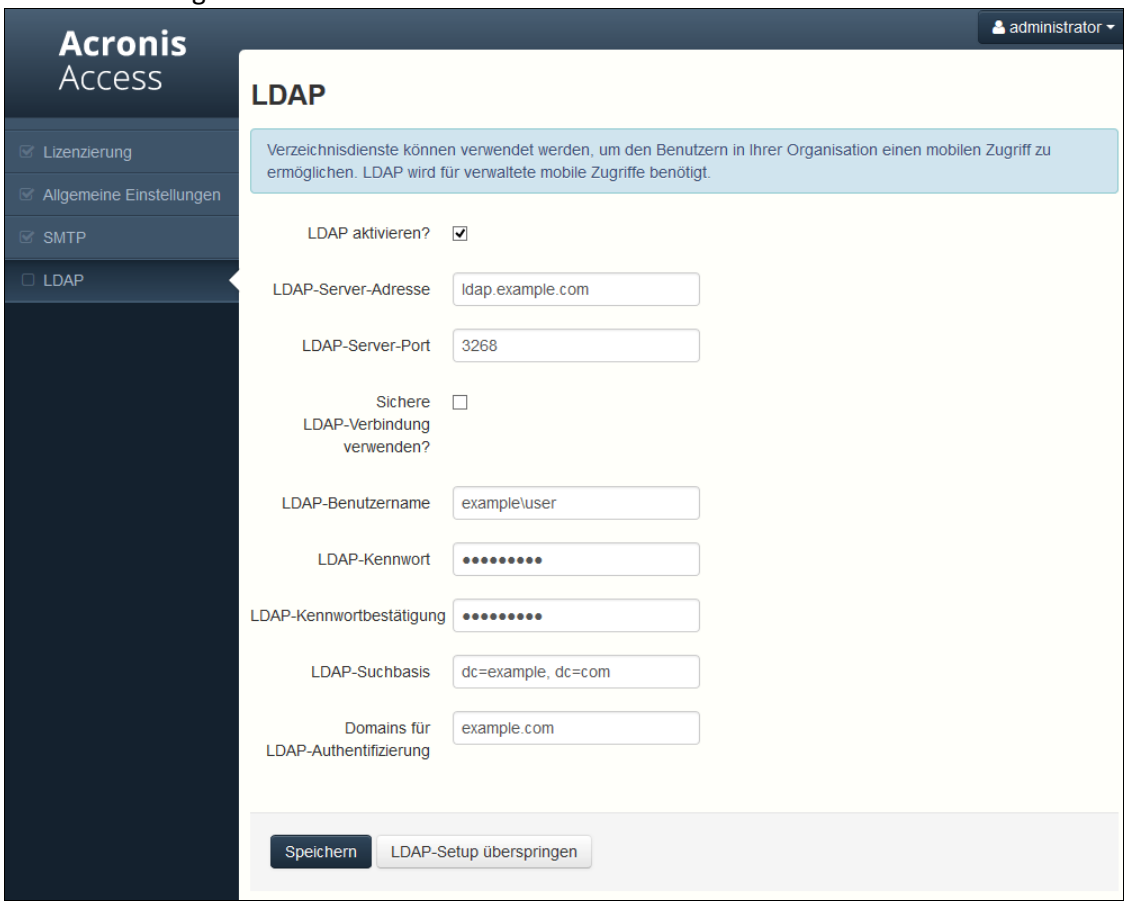
6. SMTP-Einstellungen




a. Sie werden aufgefordert, die SMTP-Einstellungen zu konfigurieren, die der Access Server zum Senden von E-Mail-Warnungen und Einladungen zur Client-Registrierung verwendet.

b. Es steht eine Option zum Senden einer Test-E-Mail zur Verfügung, um diese Einstellungen zu bestätigen.

7. LDAP-Einstellungen




   a. Der Acronis Access Server benötigt eine LDAP-Verbindung, um das Active Directory nach den Benutzern und Gruppen zu durchsuchen, denen Sie Richtlinien und Datenquellen zuweisen möchten.
   b. Geben Sie die LDAP-Informationen für einen Active Directory-Server im Netzwerk ein. Im Fall eines Netzwerks mit mehreren Domains muss es sich hierbei um einen globalen Katalog-Server an Port 3268 oder 3269 handeln (für SSL-Verbindungen). Für jedes Feld steht eine QuickInfo mit weiteren Details zur Verfügung.
   c. Sie müssen einen LDAP-Benutzernamen und ein Kennwort konfigurieren; diese Angaben werden verwendet, wenn der Server LDAP-Anforderungen stellt.
   d. Die eingegebenen LDAP-Einstellungen werden beim Speichern getestet.
8. Die Erstkonfiguration ist jetzt abgeschlossen.
   a. Klicken Sie auf **Konfiguration beenden**, um fortzufahren.

### mobilEcho Gateway Server registrieren

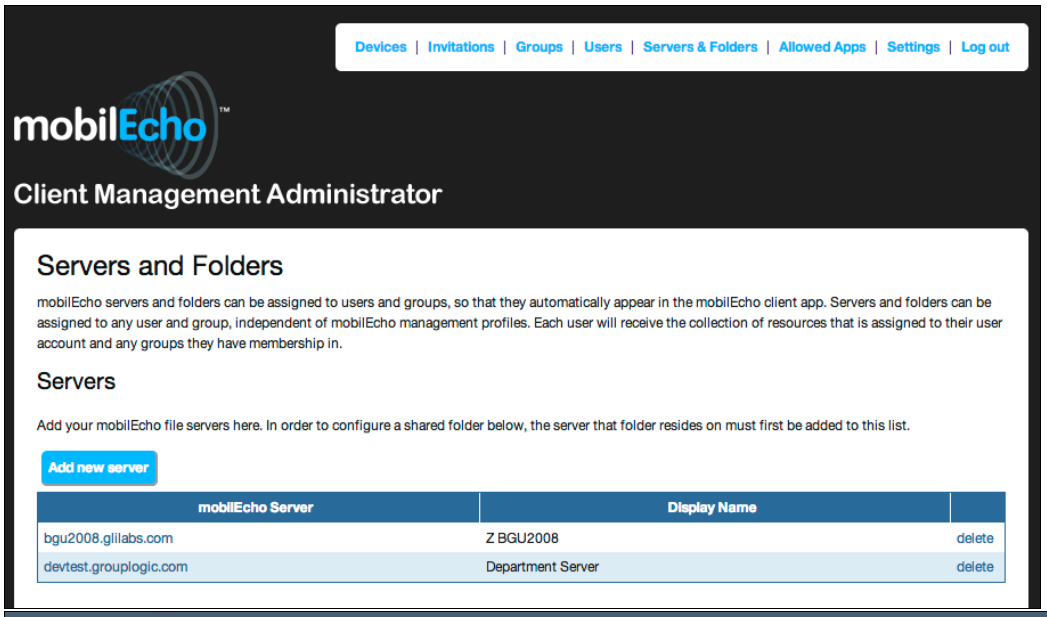
Bei einem Upgrade eines vorhandenen mobilEcho Servers der Version 4.5 oder früher, auf dem der mobilEcho Client Management-Dienst konfiguriert ist, werden alle auf der Seite 'Server und Ordner' konfigurierten Server in die Liste der Acronis Access Gateway Server importiert.

Diese Gateway Server werden zunächst als Legacy-Gateway Server importiert. Dies bedeutet, dass sie noch nicht registriert wurden und daher noch nicht von der Acronis Access Webkonsole gesteuert

und verwaltet werden können. Diese Registrierung ist erforderlich, um diese Gateway Server verwalten zu können, nachdem ein Upgrade auf Acronis Access durchgeführt wurde.

Diese Server können erst dann für die Verwaltung registriert werden, wenn das Upgrade auf Acronis Access für sie durchgeführt wurde. Bis zum Abschluss des Upgrades erfolgt die Verwaltung dieser Server weiterhin mit dem Windows-Programm mobilEcho-Administrator.

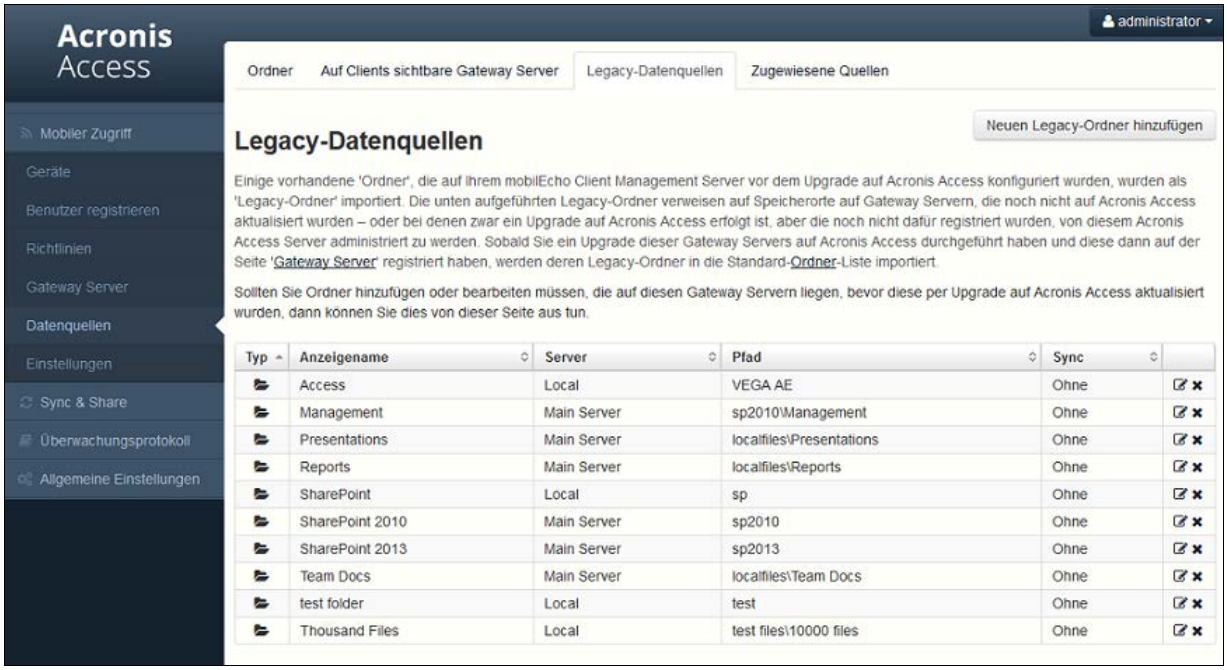
Wie im folgenden Beispiel dargestellt, werden die beiden Server auf der Seite 'Server und Ordner' von mobilEcho 4.5 jetzt auf der Seite 'Gateway Server' angezeigt.





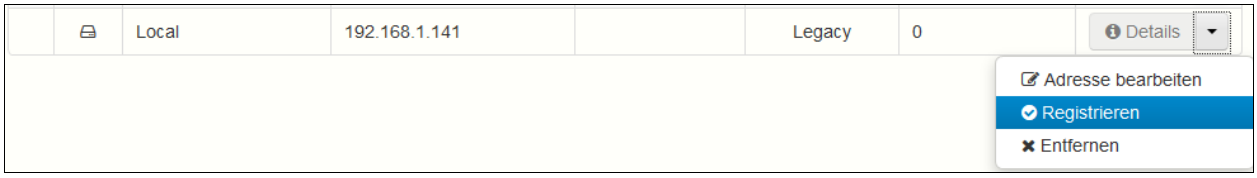
Alle vorhandenen Ordner, die im mobilEcho 4.5 Client Management Administrator konfiguriert sind, werden zunächst auf die Registerkarte 'Legacy-Datenquellen' der Seite 'Datenquellen' migriert. Sie können weiterhin Ordner auf dieser Seite hinzufügen und die Ordner ändern, bis Sie ein Upgrade des zugehörigen Gateway Servers auf Acronis Access durchführen. Sobald für einen Gateway Server ein Upgrade auf Acronis Access durchgeführt und der Gateway Server für die Verwaltung mit diesem Acronis Access Server registriert wird, werden die mit diesem Gateway Server verknüpften Ordner auf die Hauptregisterseite 'Ordner' auf der Seite 'Datenquellen' verschoben.

***Hinweis:*** *Jeder mobilEcho Gateway Server kann nur über eine Acronis Access-Konsole verwaltet werden. Falls in der Organisation mehrere mobilEcho Client Management Server (jetzt als Acronis Access Server bezeichnet) im Einsatz sind, müssen Sie für jeden Acronis Access Server einen eigenen Gateway Server bereitstellen.*




In diesem Szenario darf nur ein einziger Windows Server vorhanden sein, auf dem die Acronis Access-Konsole und der Gateway Server ausgeführt werden, daher wird auf der Seite 'Gateway Server' nur ein Server aufgeführt. Dieser Server muss registriert werden, damit Sie ihn verwalten können.

1. Klicken Sie auf dem Acronis Access Server auf die Menüschaltfläche für den Gateway Server und wählen Sie **Registrieren**.



2. Sie werden gefragt, ob die vorhandene Netzwerkadresse für den zu registrierenden Server den direkten Zugriff auf den Server ermöglicht. Die vorhandene Adresse ist in der Regel die Netzwerkadresse, über die die Benutzer mobiler Geräte auf den Gateway Server zugreifen, daher kann es sein, dass diese Adresse auf einen Proxy-Server oder ein Lastenausgleichsmodul verweist.

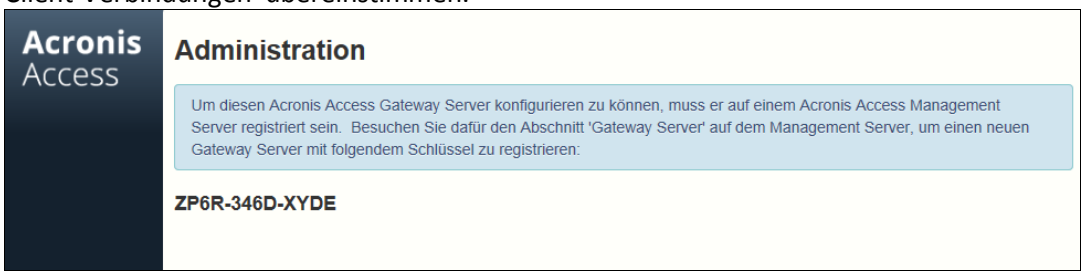
   ***Hinweis:*** *In diesem Fall müssen Sie in diesem Dialogfeld* ***'Nein'*** *wählen und eine alternative Netzwerkadresse eingeben, mit der der Acronis Access Server direkten Netzwerkzugriff auf den betreffenden Gateway Server erhält.*


3. Anschließend wird das Registrierungsdialogfeld angezeigt.


   ***Hinweis:*** *Falls der Gateway Server ein selbstsigniertes SSL-Zertifikat verwendet, müssen Sie die Option 'Verbindungen von Acronis Access Servern mit selbstsignierten Zertifikaten erlauben' aktivieren.*

   ***Hinweis:*** *Sie müssen außerdem einen Administrationsschlüssel eingeben, um die Kopplung mit diesem Remote-Server zu aktivieren. Dieser Schlüssel dient zur Validierung und Sicherung der administrativen Beziehung.*

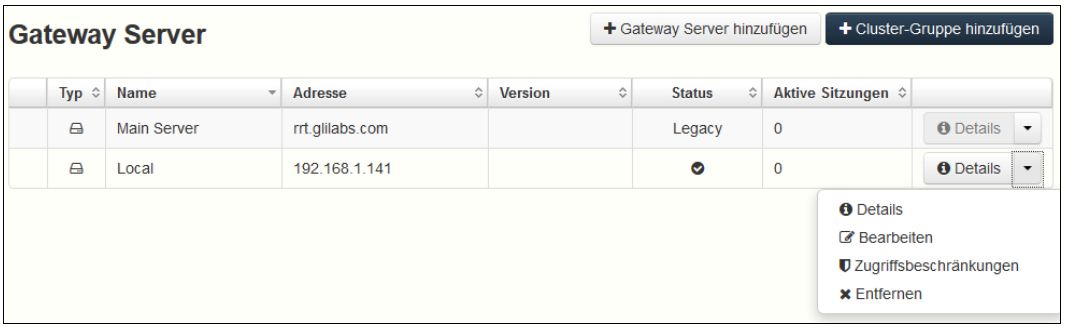
4. Um einen Administrationsschlüssel vom Gateway Server zu erhalten, öffnen Sie ein neues Fenster oder eine neue Registerkarte im Browser und navigieren Sie zur HTTPS-Adresse des Gateway Servers. Diese muss mit der Adresse im Feld 'Adresse für Administration und Client-Verbindungen' übereinstimmen.



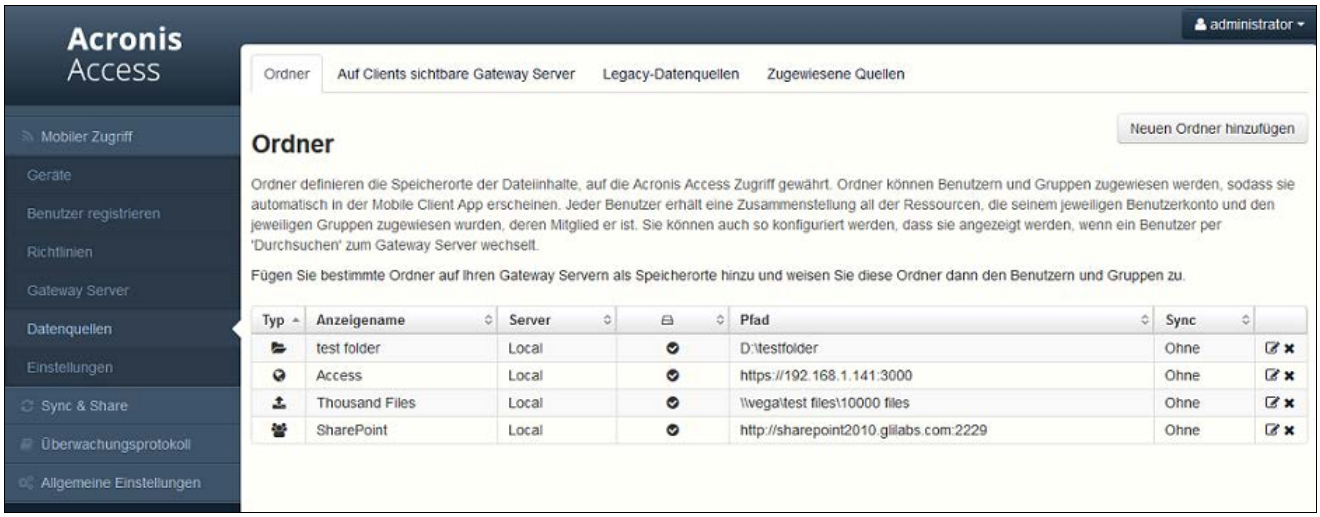

***Hinweis:*** *Aus Sicherheitsgründen muss dieser Schritt in einem Webbrowser auf dem Windows Server durchgeführt werden, auf dem der Gateway Server ausgeführt wird. In einem Remote-Webbrowser kann der Administrationsschlüssel nicht angezeigt werden.*

5. Geben Sie den 12-stelligen Administrationsschlüssel (einschließlich Bindestrichen) in das Registrierungsformular ein und klicken Sie auf **Speichern**.

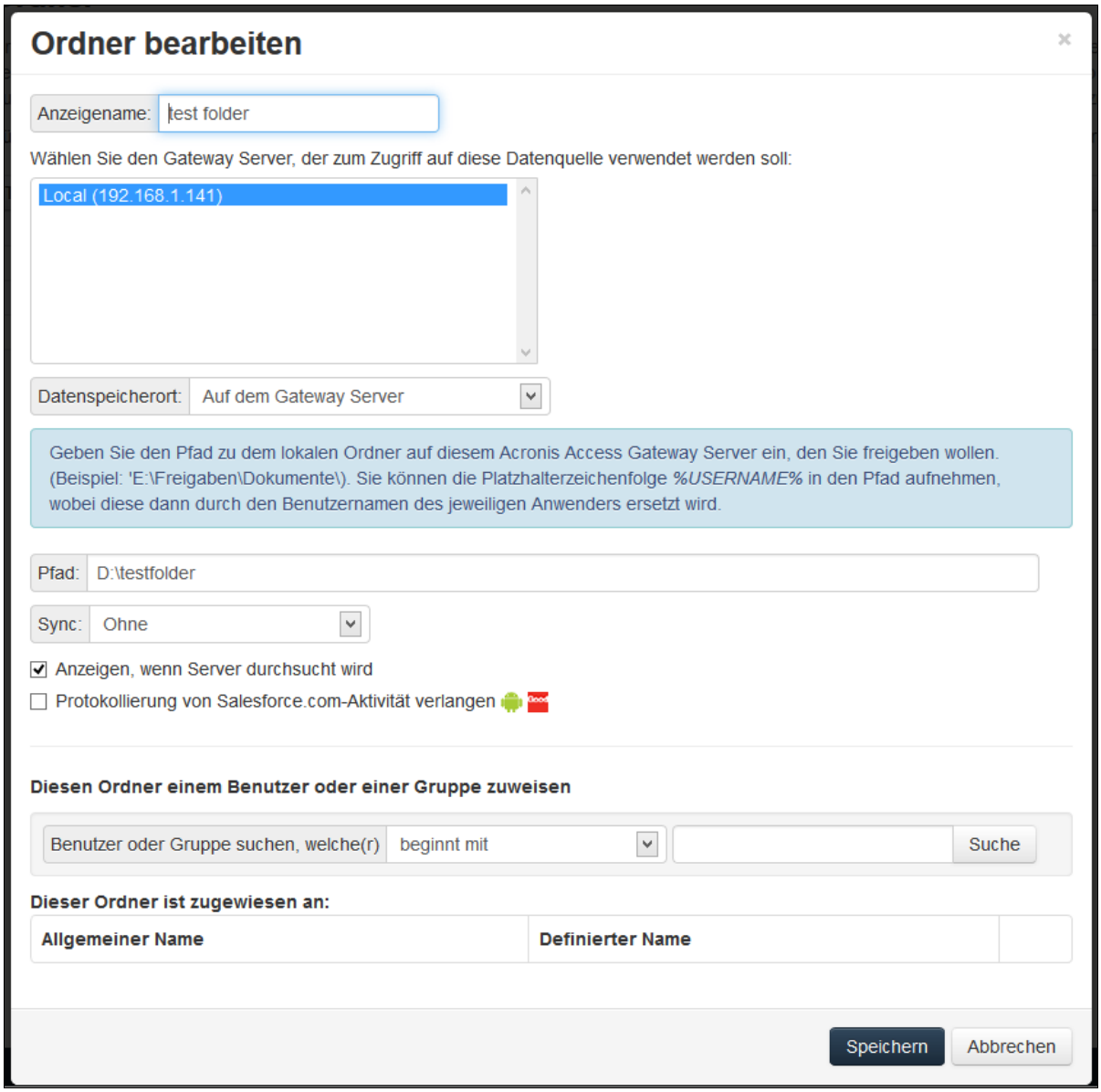
***Hinweis:*** *Nachdem der Server registriert wurde, wird er in der Liste der Gateway Server als registriert angezeigt, sodass Sie jetzt die Einstellungen anpassen sowie die Details und den Status anzeigen können.*




Bei der Registrierung werden die Volumes, die vor dem Upgrade auf Acronis Access auf dem mobilEcho Gateway Server vorhanden waren, in die Ordnerliste auf der Seite 'Datenquellen' importiert.

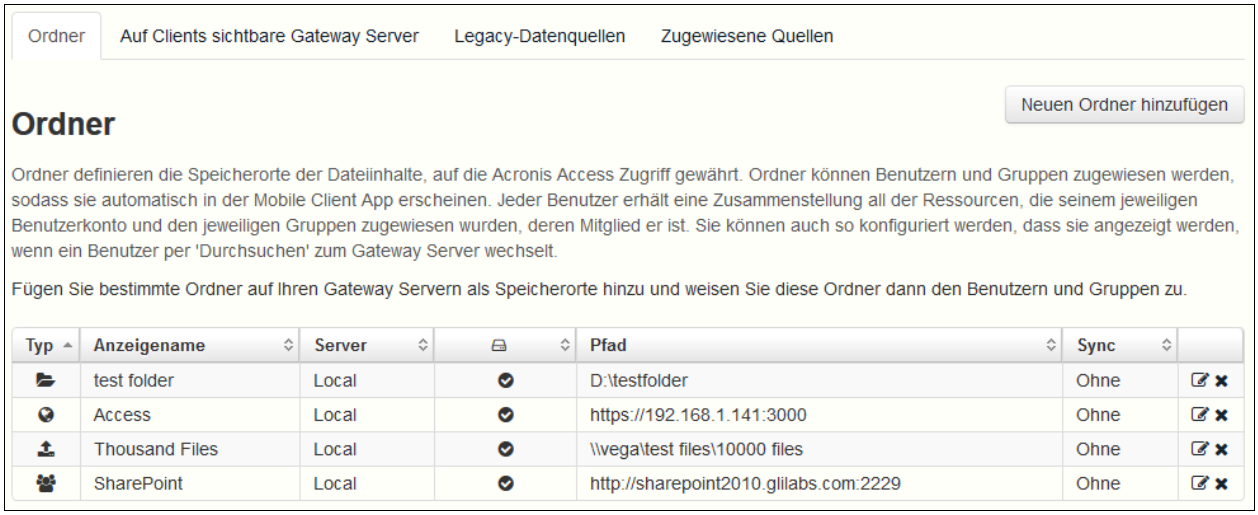


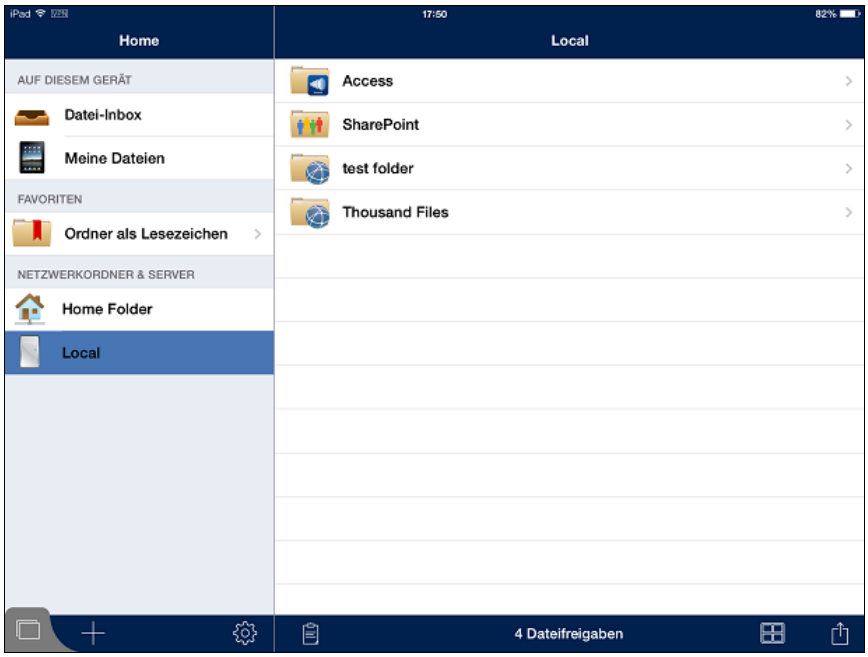
In mobilEcho 5.0 gibt es keine „Volumes“ mehr. Anstatt Volumes für die Freigabe von Datenquellen zu verwenden, erstellen Sie jetzt Ordner. Diese Ordner verfügen über die optionale Eigenschaft 'Anzeigen, wenn Server durchsucht wird'. Bei aktivierter Option wird der Ordner angezeigt, wenn ein Benutzer den Stamm des Gateway Servers in seiner mobilEcho-App durchsucht, ebenso wie in mobilEcho 4.5 oder früher Volumes angezeigt wurden.




Alle Volumes aus dem mobilEcho Server der Version 4.5 oder früher wurden als Ordner mit aktivierter Eigenschaft 'Anzeigen, wenn Server durchsucht wird' in die Acronis Access-Konsole importiert. Daher werden sie weiterhin angezeigt, wenn die Benutzer den Stamm eines mobilEcho Gateway Servers durchsuchen. Alle später hinzugefügten Ordner können durch Aktivierung dieser Einstellung so konfiguriert werden, dass sie sich wie Volumes verhalten. Sie können nun auch erweiterte Funktionen zur Client-Verwaltung nutzen, z.B. die Funktion, Ordner hinzuzufügen, die automatisch in der mobilEcho Client-App der Active Directory-Benutzer oder -Gruppen angezeigt werden, denen Sie sie zuweisen.

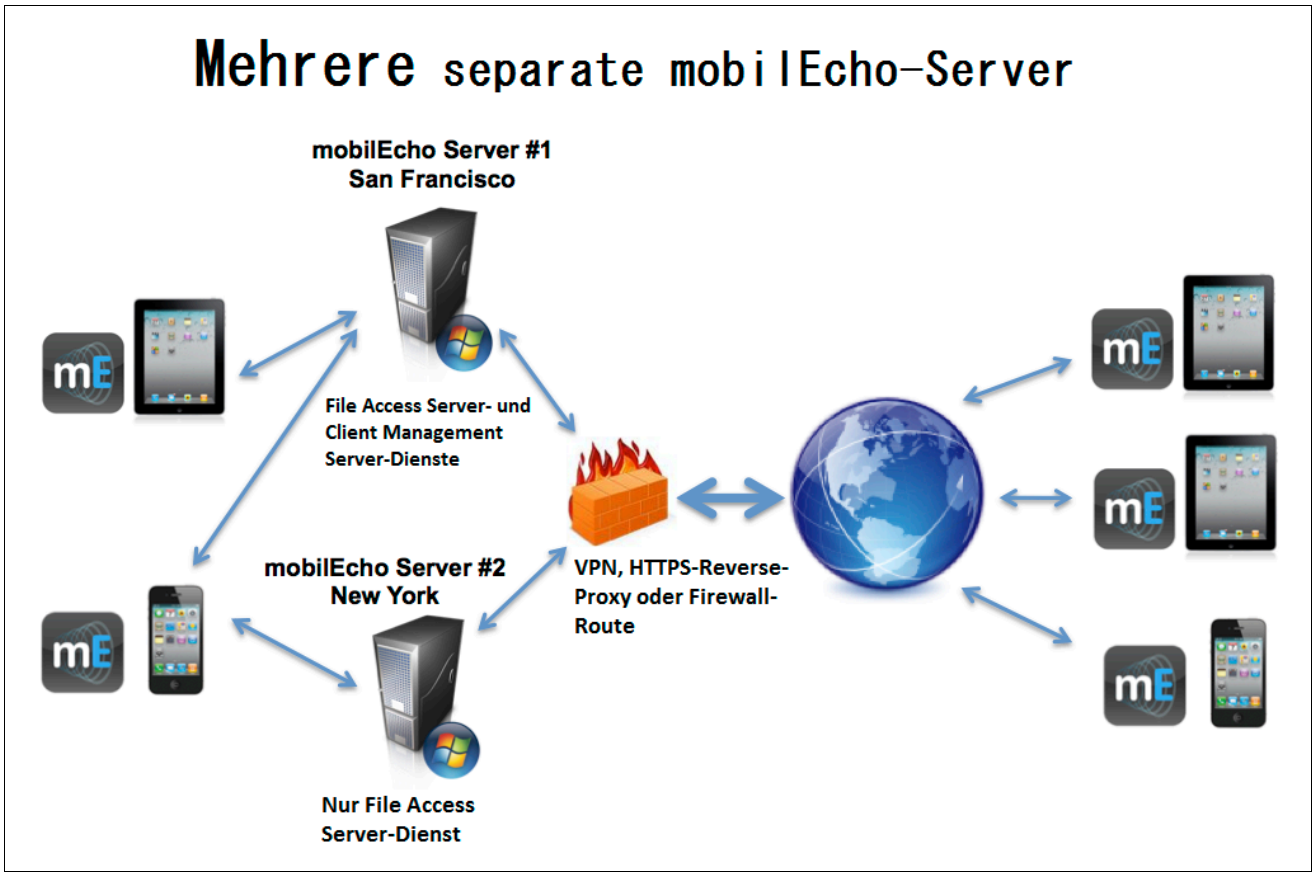
Wie unten dargestellt wurden die vier vorhandenen Volumes dieses mobilEcho 4.5 Servers nach der Gateway Server-Registrierung in die Ordnerliste importiert und werden beim Durchsuchen des Servers mit der mobilEcho-App weiterhin angezeigt.



### 2.2.2.3 Upgrade mehrerer mobilEcho Server mit Client Management

**Szenario 3 – Upgrade mehrerer mobilEcho Server mit Client Management**




In diesem Szenario wird auf mehreren Windows-Servern mobilEcho 4.5 oder früher ausgeführt. Auf einem Server wird zum einen der erforderliche mobilEcho File Access Server Dienst ausgeführt, zum anderen ist der optionale mobilEcho Client Management Server-Dienst aktiviert. Die anderen Server fungieren lediglich als mobilEcho File Access Server.

Bei einem Upgrade auf Acronis Access wird ein Upgrade der mobilEcho File Access Server auf Acronis Access Gateway Server durchgeführt. mobilEcho Clients können weiterhin eine Verbindung zu diesem Dienst herstellen und der Dienst fungiert weiterhin als Gateway zu allen Dateiserver-, NAS- oder SharePoint-Datenquellen, auf die die Benutzer zugreifen.

Für die mobilEcho Client Management Administrator-Webkonsole auf dem Server, der als mobilEcho Client Management Server fungiert, wird ein Upgrade auf die Acronis Access Server Webkonsole durchgeführt. Nach dem Upgrade werden die mobilEcho File Access Server nicht mehr mit dem Windows-Programm mobilEcho-Administrator auf den einzelnen Servern verwaltet. Mit dieser neuen Webkonsole werden alle mobilEcho Server und Clients über eine einheitliche Weboberfläche verwaltet.

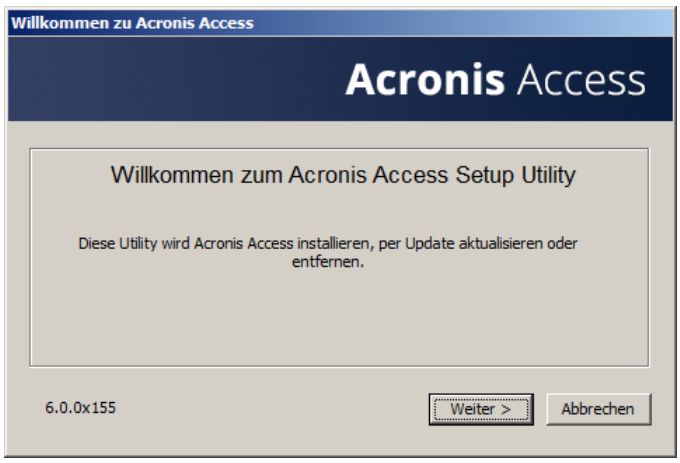
**So führen Sie ein Upgrade von Acronis Access aus:**

**Gehen Sie auf dem Windows Server, der als mobilEcho Client Management Server fungiert, folgendermaßen vor:**

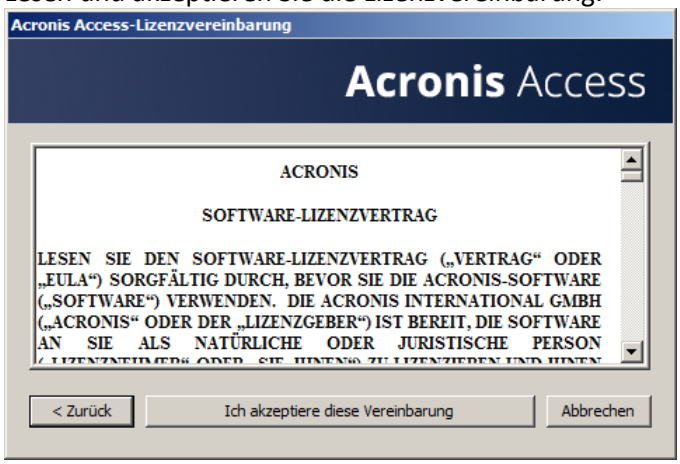
1. Führen Sie die Anweisungen in Szenario 2 aus, um ein Upgrade des Windows Servers durchzuführen, der als mobilEcho Client Management Server fungiert. Zu diesem Server stellen Sie eine Verbindung her, wenn Sie sich bei der mobilEcho Client Management Administrator-Webkonsole anmelden.
2. Nach Abschluss des Upgrades verfügen Sie über eine funktionsfähige Acronis Access Server-Webkonsole. Der mobilEcho File Access Server (jetzt als Acronis Access Gateway Server bezeichnet) befindet sich auf dem für die Verwaltung registrierten Windows Server. Zudem werden die zusätzlichen Server auf der Seite der Acronis Access Gateway Server als „Legacy“-Server aufgeführt. Im folgenden Beispiel ist der Upgrade-Server 'BGU2008' registriert und der Server 'Department Server', dessen Upgrade noch aussteht, wurde noch nicht registriert.
3. Als Nächstes führen Sie ein Upgrade aller zusätzlichen Server durch, die nur als mobilEcho File Access Server fungieren. Führen Sie die nachfolgenden Schritte aus.

**Auf jedem Windows Server, der nur als mobilEcho File Access Server fungiert:**

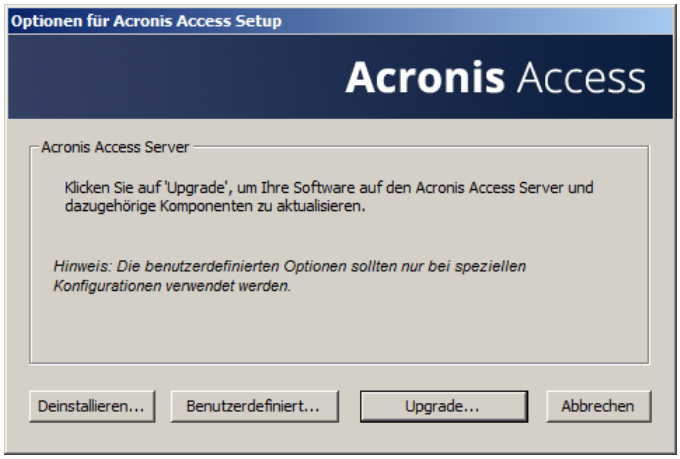
1. Sichern Sie alle erforderlichen Dateien wie in den folgenden Anleitungen beschrieben: mobilEcho 4.5 Backup bzw. activEcho 2.7 Backup.
2. Führen Sie das Acronis Access-Installationsprogramm auf dem gewünschten Server aus.
3. Klicken Sie auf der Willkommensseite auf **Weiter**.



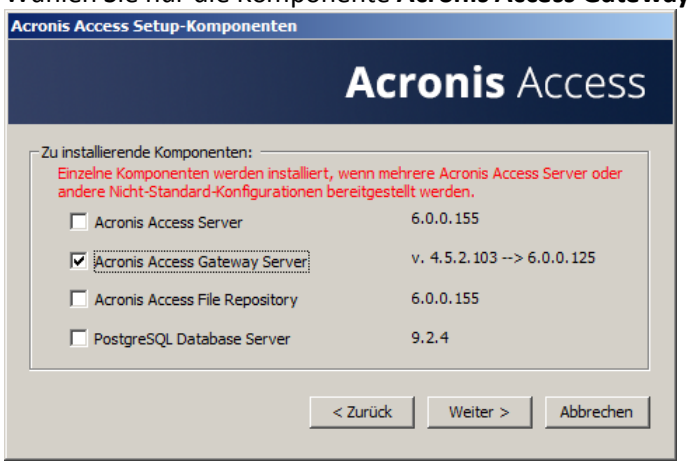
4. Lesen und akzeptieren Sie die Lizenzvereinbarung.




5. Klicken Sie auf **Benutzerdefiniert**.




6. Wählen Sie nur die Komponente **Acronis Access Gateway Server** aus, und klicken Sie auf **Weiter**.




7. Die restlichen Schritte der Installation und des Konfigurationswerkzeugs entsprechen den in früheren Szenarien erläuterten, mit der Ausnahme, dass Sie den Access Server und das Datei-Repository im Konfigurationswerkzeug nicht konfigurieren müssen.
8. Nach Abschluss des Konfigurationswerkzeugs ist keine weitere Webkonsolen-Konfiguration erforderlich, da die Acronis Access Server-Konsole nicht installiert wurde.
9. Kehren Sie zur Acronis Access Server-Konsole auf dem ersten Server zurück, auf dem Sie die Vollinstallation durchgeführt haben. Öffnen Sie die Seite 'Gateway Server', klicken Sie auf die

Menüschaltfläche für den zusätzlichen Gateway Server, für den Sie soeben ein Upgrade auf Acronis Access durchgeführt haben, und wählen Sie **Registrieren**.

10. Sie werden gefragt, ob die vorhandene Netzwerkadresse für den zu registrierenden Server den direkten Zugriff auf den Server ermöglicht. Die vorhandene Adresse ist in der Regel die Netzwerkadresse, über die die Benutzer mobiler Geräte auf den Gateway Server zugreifen, daher kann es sein, dass diese Adresse auf einen Proxy-Server oder ein Lastenausgleichsmodul verweist.

    ***Hinweis:*** *In diesem Fall müssen Sie in diesem Dialogfeld 'Nein' wählen und eine alternative Netzwerkadresse eingeben, mit der der Acronis Access Server direkten Netzwerkzugriff auf den betreffenden Gateway Server erhält.*

11. Anschließend wird das Registrierungsdialogfeld angezeigt.

    ***Hinweis:*** *Falls der Gateway Server ein selbstsigniertes SSL-Zertifikat verwendet, müssen Sie die Option 'Verbindungen von Acronis Access Servern mit selbstsignierten Zertifikaten erlauben' aktivieren.*

    ***Hinweis:*** *Sie müssen außerdem einen Administrationsschlüssel eingeben, um die Kopplung mit diesem Remote-Server zu aktivieren. Dieser Schlüssel dient zur Validierung und Sicherung der administrativen Beziehung.*

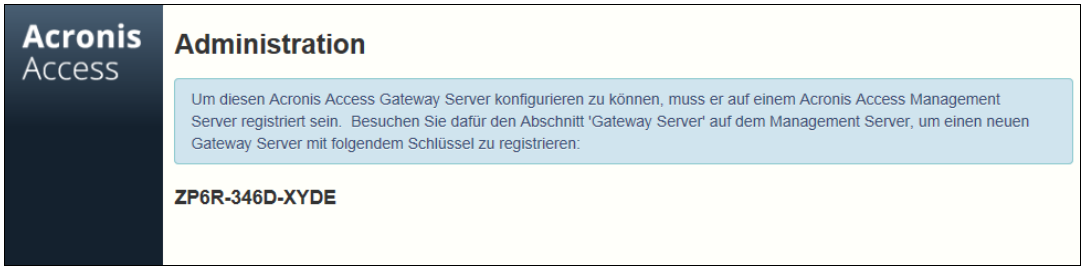
12. Um einen Administrationsschlüssel von diesem Gateway Server zu erhalten, öffnen Sie ein neues Fenster oder eine neue Registerkarte im Browser des Windows Servers, den Sie registrieren, und navigieren Sie zur HTTPS-Adresse des Gateway Servers. Diese muss mit der Adresse im Feld 'Adresse für Administration und Client-Verbindungen' übereinstimmen.

    ***Hinweis:*** *Aus Sicherheitsgründen muss dieser Schritt in einem Webbrowser auf dem Windows Server durchgeführt werden, auf dem der Gateway Server ausgeführt wird. In einem Remote-Webbrowser kann der Administrationsschlüssel nicht angezeigt werden.*

13. Geben Sie den 12-stelligen Administrationsschlüssel (einschließlich Bindestrichen) in das Registrierungsformular ein und klicken Sie auf **Speichern**.

    ***Hinweis:*** *Nachdem der Server registriert wurde, wird er in der Liste der Gateway Server als registriert angezeigt; Sie können jetzt die Einstellungen anpassen sowie die Details und den Status anzeigen.*

    ***Hinweis:*** *Bei der Registrierung werden die Volumes, die vor dem Upgrade auf Acronis Access auf diesem mobilEcho Gateway Server vorhanden waren, in die Ordnerliste auf der Seite 'Datenquellen' importiert. Sie verhalten sich wie in den vorherigen Upgrade-Szenarien erläutert.*

14. Die gesamte Verwaltung dieses Gateway Servers erfolgt nun in der Acronis Access Server Webkonsole. Wenn Sie auf der Seite 'Datenquellen' neue Ordner erstellen, wird dieser Gateway Server jetzt in der Liste der Gateway Server angezeigt, die für den Zugriff auf den neuen Ordner verfügbar sind.
15. Falls Sie Upgrades und Registrierungen für weitere Gateway Server durchführen möchten, führen Sie die Schritte des oben beschriebenen Verfahrens aus.

#### 2.2.2.4 Upgrade eines einzelnen mobilEcho Servers mit aktiviertem Client Management-Dienst und eines activEcho Servers

Informationen zu diesem Verfahren finden Sie im Abschnitt Upgrade eines activEcho Servers mit mobilEcho Client Management Server (S. 73).

### 2.2.3 Downgrade auf mobilEcho 4.5

Ein Downgrade von Acronis Access auf mobilEcho 4.5 ist kompliziert und sollte nur im absoluten Notfall durchgeführt werden. Erstellen Sie unbedingt einwandfreie Backups und bewahren Sie sie an sicheren Orten auf.

**So führen Sie ein Downgrade von Acronis Access auf mobilEcho 4.5 durch:**

***Warnung: Fügen Sie dem mobilEcho-Administrator keine Lizenzen hinzu, bis das Verfahren vollständig abgeschlossen ist. Nehmen Sie während der Durchführung des Verfahrens keine Änderungen an der Registry vor.***

Damit dieses Verfahren ausgeführt werden kann, müssen Sie zuvor ein Upgrade auf Acronis Access erfolgreich durchgeführt haben.

1. Erstellen Sie vor Beginn ein Backup der Datei **settings_backup** und des Ordners **Legacy mobilEcho files**.

   ***Hinweis:*** *Die Datei befindet sich im folgenden Verzeichnis:* ***C:\Programme (x86)\Group Logic\mobilEcho Server***

   *und der Ordner befindet sich hier:* ***C:\Programme (x86)\Group Logic\Access Server\Legacy mobilEcho files***

2. Laden Sie die Installer für mobilEcho 4.5 und Acronis Access herunter.
3. Führen Sie den Acronis Access Installer aus.
4. Klicken Sie auf der Willkommensseite auf **Weiter**.
5. Akzeptieren Sie die Lizenzvereinbarung.
6. Klicken Sie auf **Deinstallieren**, um das Downgrade-Verfahren zu starten.
7. Klicken Sie im Pop-up-Fenster mit der Warnmeldung auf **OK**.
8. Wählen Sie die Option zum Deinstallieren aller Acronis Access-Komponenten.
9. Überprüfen Sie die ausgewählten Komponenten, und klicken Sie auf **Deinstallieren**.
10. Klicken Sie im Pop-up-Fenster zur PostgreSQL-Deinstallation auf **Ja**. Einige Dateien und Einstellungen werden nicht deinstalliert.
11. Überprüfen Sie alle deinstallierten Komponenten und klicken Sie auf **Beenden**.
12. Führen Sie den mobilEcho 4.5 Installer aus.
13. Lesen und akzeptieren Sie die Lizenzvereinbarung und klicken Sie auf **Weiter**.
14. Wählen Sie die Ordner aus, in denen mobilEcho zuvor installiert war. Falls die Standardordner verwendet wurden, können Sie diese übernehmen.
15. Klicken Sie auf **Installieren**, um mit der Installation von mobilEcho 4.5 zu beginnen. Nach Abschluss der Installation deaktivieren Sie die Option zum Starten von File Server Administrator und klicken Sie auf **Abschluss**.
16. Führen Sie die zuvor gesicherte Datei **settings_backup** aus.
17. Öffnen Sie den zuvor gesicherten Ordner **Legacy mobilEcho files**.
    a. Kopieren Sie die Dateien **invitation.html.erb** und **invitation.txt.erb** in das Verzeichnis **C:\Programme (x86)\Group Logic\mobilEcho Server\ManagementUI\app\views\user_mailer**.
    b. Kopieren Sie die Datei **mobilEcho_manager** in das Verzeichnis **C:\Programme (x86)\Group Logic\mobilEcho Server\ManagementUI**.
    c. Kopieren Sie die Datei **production.sqlite3** in das Verzeichnis **C:\Programme (x86)\Group Logic\mobilEcho Server\ManagementUI\db**.
    d. Möglicherweise gibt es noch eine vierte Datei mit dem Namen 'priority.txt'; kopieren Sie sie ggf. in das Verzeichnis **C:\Programme (x86)\Group Logic\mobilEcho Server\Management**. Den Ordner **Management** müssen Sie manuell erstellen.

       ***Hinweis:*** *Es wird dringend empfohlen, die alte Datei zu löschen, bevor die neue Datei abgelegt wird.*

18. Starten Sie die Dienste **mobilEcho File Access** und **mobilEcho Management**.

    ***Hinweis:*** *Alle Benutzer- und Gruppenprofile müssen manuell neu aktiviert werden.*

# 2.3 Upgrade von activEcho 2.7 oder früheren Versionen

**Themen**



## 2.3.1 Vor Beginn

**activEcho vor dem Upgrade per Backup sichern**

Sichern Sie die Datendateien, die vom vorhandenen activEcho Server verwendet werden.

Das Backup- und Wiederherstellungsverfahren für einen activeEcho Server bis Version 2.7 wird hier erläutert: http://docs.grouplogic.com/display/ActivEcho/Maintenance+Tasks

***Hinweis:*** *Beim Upgrade gehen alle Anpassungen der activEcho-Weboberfläche verloren.*

**Aktualisieren Sie Ihre Version von activEcho auf Version 2.7, bevor Sie ein Upgrade auf Acronis Access durchführen.**

**Tomcat vor dem Upgrade per Backup sichern**

Beim Upgrade wird möglicherweise ein Upgrade für Apache Tomcat und für alle aktuellen Tomcat-Konfigurationsdateien durchgeführt, Zertifikate und die Protokolldateien werden entfernt. Es empfiehlt sich, eine Kopie des Apache Tomcat-Ordners anzulegen. Dieser befindet sich standardmäßig hier: **C:\Programme (x86)\Group Logic\Common**.

**Eigene Konfiguration kennen**

Stellen Sie sicher, dass Sie die folgenden Fragen beantworten können, bevor Sie mit dem Upgrade fortfahren:

- Ist sowohl mobilEcho als auch activEcho installiert?
- Befinden sie sich auf demselben Computer oder auf unterschiedlichen Maschinen?
- Welche Ports verwendet mobilEcho? An welchem Port befindet sich der File Server und an welchem der Management Server?
- Welchen Port verwendet activEcho? Befindet sich das Datei-Repository auf derselben Maschine?

## 2.3.2 Der Upgrade-Prozess

**activEcho 5.0 Upgrade-Prozess**

Geben Sie zunächst die Art des activEcho-Deployments an, für das ein Upgrade durchgeführt werden soll. Ausführliche Anweisungen für diese Szenarien finden Sie im nächsten Abschnitt dieses Dokuments. Die gängigsten Szenarien sind folgende:

1. **Einzelner activEcho Server ohne mobilEcho Client Management Server**
   - Ein einzelner Windows Server, auf dem ausschließlich der activEcho Server ausgeführt wird.
2. **Einzelner activEcho Server mit mobilEcho Client Management Server**
   - Ein einzelner Windows Server, auf dem der activEcho Server und der mobilEcho Client Management- und der File Server-Dienst ausgeführt werden.
3. **Ein activEcho Server und ein mobilEcho Client Management Server auf einem anderen Server**
   - Ein Windows Server, auf dem der activEcho Server ausgeführt wird, und ein anderer Server, auf dem der mobilEcho Client Management-Dienst ausgeführt wird.

### Themen



### 2.3.2.1 Upgrade eines einzelnen activEcho Servers ohne mobilEcho Client Management Server

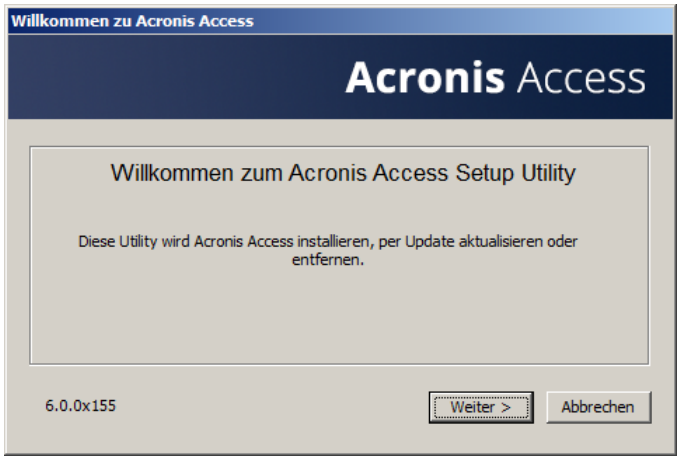
**Szenario 1 – Upgrade eines einzelnen activEcho Servers ohne mobilEcho Client Management Server**

In diesem Szenario wird auf einem einzelnen Windows Server nur der activEcho Server ausgeführt. Dieses Verfahren führt ein Upgrade des activEcho Servers auf die Acronis Access Server-Webkonsole durch. Diese neue Konsole behält alle activEcho-Funktionen bei und verfügt darüber hinaus über einige weitere Funktionen. Mit der Acronis Access Server-Webkonsole können Sie activEcho und mobilEcho über eine einheitliche Weboberfläche verwalten.

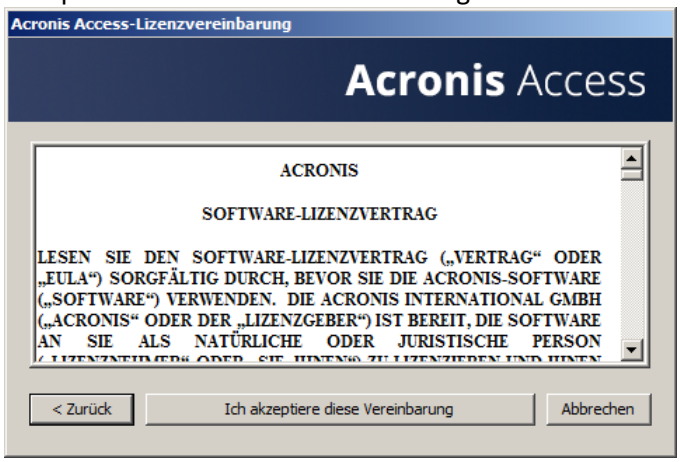
**So führen Sie ein Upgrade von activEcho durch:**

1. Sichern Sie alle erforderlichen Dateien wie in den folgenden Anleitungen beschrieben: mobilEcho 4.5 Backup bzw. activEcho 2.7 Backup.
2. Deaktivieren Sie alle vorhandenen Virenschutzprogramme, da sie unter Umständen den Installationsvorgang unterbrechen und somit eine fehlerhafte Installation verursachen können.
3. Laden Sie den Acronis Access Server Installer auf den activEcho Server herunter und führen Sie ihn aus.
   a. Um auf den neuesten Installer zuzugreifen, besuchen Sie die folgende Website: http://support.grouplogic.com/?page_id=3598
   b. Sie müssen die Produkt-Seriennummer zur Überprüfung eingeben, bevor Sie das Installationsprogramm herunterladen können.
   c. Die Installer-Datei hat folgenden Namen: AcronisAccessSetup.exe

4. Klicken Sie auf der Willkommensseite auf **Weiter**.

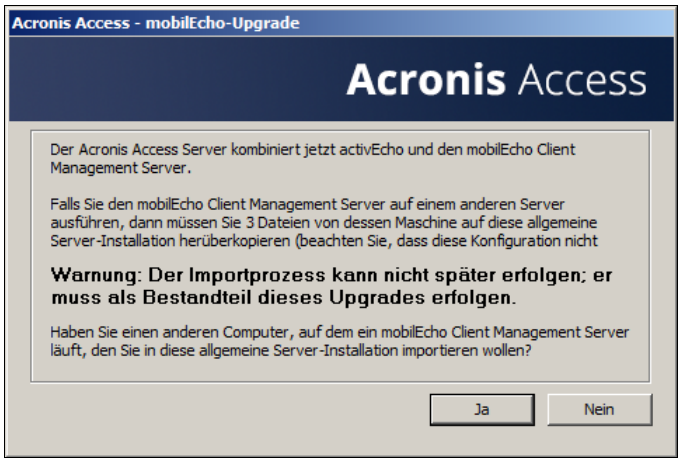



5. Akzeptieren Sie die Lizenzvereinbarung.

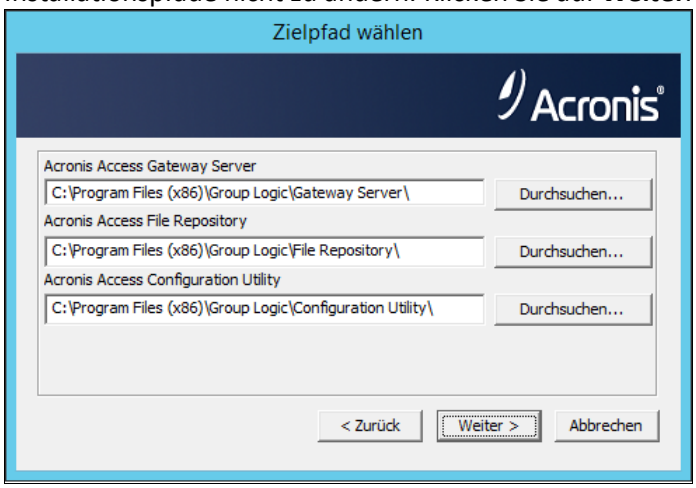



6. Klicken Sie auf **Upgrade**, um den activEcho Server automatisch auf den neuen Acronis Access Server zu aktualisieren. Im Rahmen des Upgrade-Prozesses werden auch ein Gateway Server und die erforderlichen Dienste installiert.

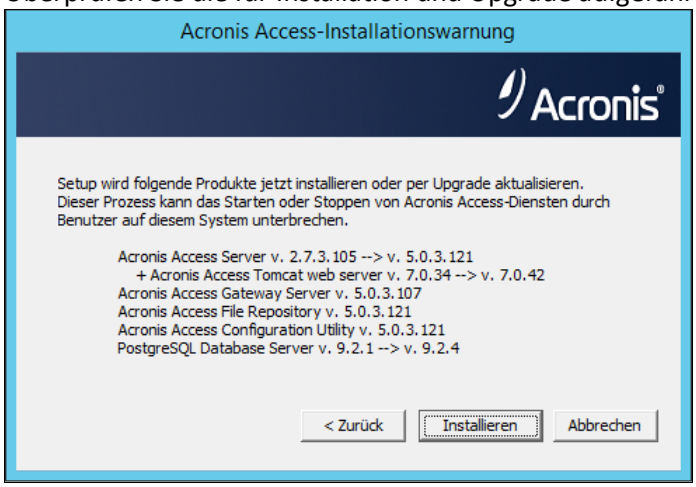
7. Eine Aufforderung zur Eingabe von Remote-mobilEcho Servern wird angezeigt. Falls Sie nicht über einen mobilEcho Client Management Server verfügen, wählen Sie **Nein**. Lesen Sie für einen mobilEcho Client Management Server die Artikel Upgrade eines activEcho Servers mit mobilEcho Client Management Server (S. 73) oder Upgrade eines activEcho Servers mit einem mobilEcho Client Management Server auf einem anderen Server (S. 80) durch, in denen das Upgrade mit einer mobilEcho Installation beschrieben wird.



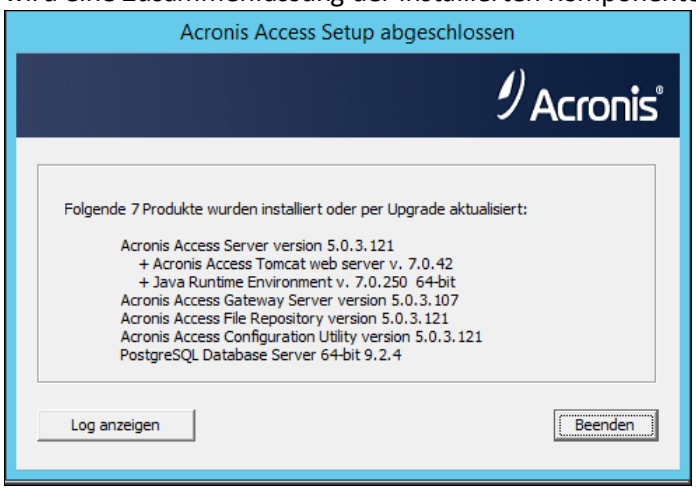

8. Wählen Sie einen Installationsspeicherort für die zu installierenden Acronis Access-Komponenten aus. Falls Sie ein Upgrade eines vorhandenen activEcho Servers durchführen, wird für diese Pfade standardmäßig der vorhandene Installationsspeicherort verwendet. Wir empfehlen, diese Installationspfade nicht zu ändern. Klicken Sie auf **Weiter**.



9. Überprüfen Sie die für Installation und Upgrade aufgeführten Dienste.

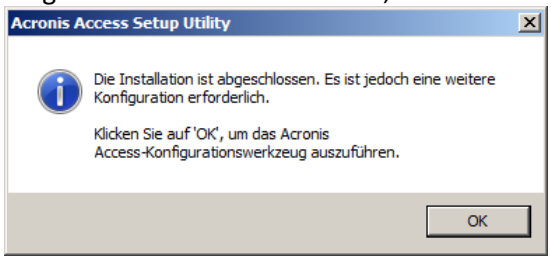



10. Klicken Sie auf **Installieren**, um mit der Installation zu beginnen. Nach Abschluss der Installation wird eine Zusammenfassung der installierten Komponenten angezeigt. Klicken Sie auf **Beenden**.




***Hinweis:*** *Alle erforderlichen Komponenten werden automatisch nacheinander installiert. Dieser Vorgang kann je nach Server 5 bis 15 Minuten dauern. Zukünftige Upgrades werden schneller installiert.*

11. An diesem Punkt des Upgrade-Prozesses wurden alle erforderlichen Software-Komponenten installiert. Jetzt müssen Sie jedoch die Netzwerkschnittstellen, Ports und Zertifikate konfigurieren, die verwendet werden sollen. Dieser Schritt ist obligatorisch. Beim Beenden des Installationsprogramms werden Sie zur Ausführung des Acronis Access-Konfigurationswerkzeugs aufgefordert. Klicken Sie auf **OK**, um fortzufahren.

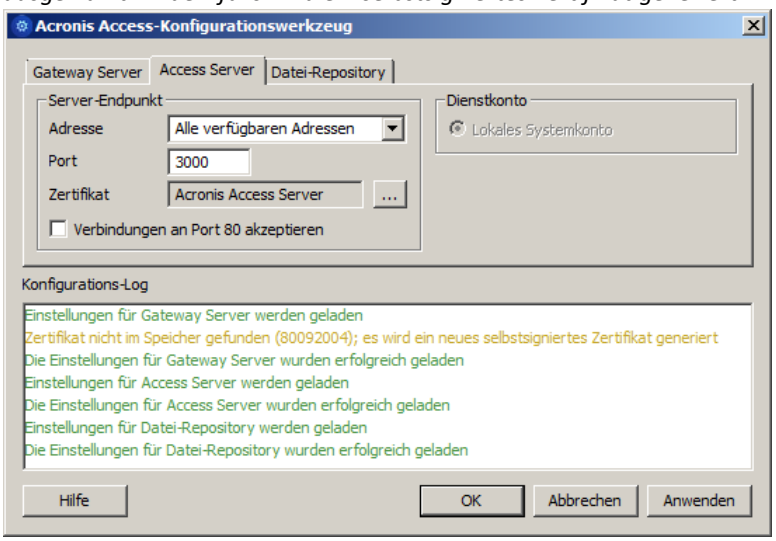



12. Im Konfigurationswerkzeug können Sie auf der Registerkarte 'Gateway Server' die Netzwerkadresse, den Port und das Zertifikat des Acronis Access Gateway Servers konfigurieren. Der Acronis Access Gateway Server ist der Acronis Access Kerndienst, zu dem die mobilEcho Clients eine Verbindung herstellen und der Zugriff auf Dateiserver, NAS und SharePoint-Server bietet.

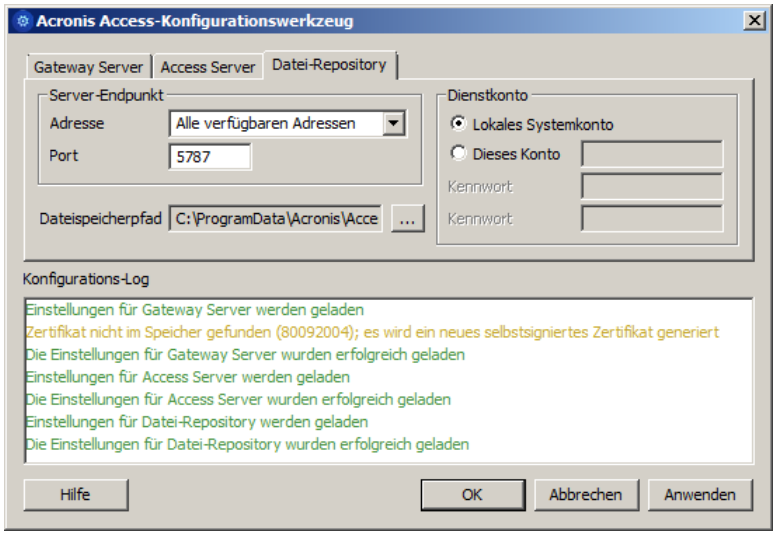
***Hinweis:*** *Die vorhandenen Einstellungen bleiben erhalten. Überprüfen Sie, ob diese Einstellungen mit den vorhandenen mobilEcho File Access Server-Einstellungen übereinstimmen. Dieser Dienst kann in der Regel auf allen verfügbaren Netzwerkadressen an Port 443 ausgeführt werden. Falls Sie über ein SSL-Serveridentitätszertifikat verfügen, wird dieses automatisch ausgewählt. Andernfalls wird ein selbstsigniertes Zertifikat generiert.*

13. Auf der Registerkarte 'Access Server' werden die Netzwerkadresse, der Port und das Zertifikat des Acronis Access Servers konfiguriert. Der Acronis Access Server ist die Webkonsole, über die alle Sync & Share-Funktionen und die activEcho-Benutzer konfiguriert und alle Aufgaben im Zusammenhang mit Serveradministration und Remote-Client-Management durchgeführt werden. Dies ist auch die Konsole, mit der Benutzer auf den Web-Client zugreifen.

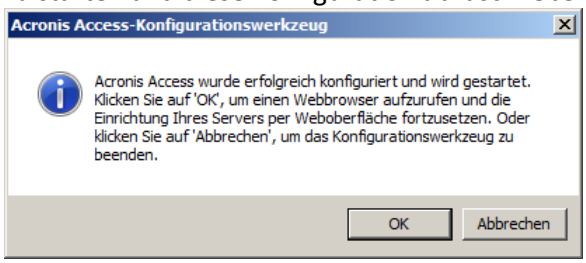
    ***Hinweis:*** *Überprüfen Sie die Einstellungen für den Access Server. Die Standardeinstellungen werden empfohlen. Diese Webkonsole kann in der Regel auf allen verfügbaren Netzwerkadressen an Port 3000 ausgeführt werden. Falls Sie über ein SSL-Serveridentitätszertifikat verfügen, wird dieses automatisch ausgewählt. Andernfalls wird ein selbstsigniertes Zertifikat generiert.*




***Hinweis:*** *Acronis Access Server erfordert die Auswahl eines Speicherorts für das Datei-Repository. Dieses Repository wird von den Dateisynchronisierungs- und Freigabefunktionen (Sync & Share) von Acronis activEcho verwendet.*



14. Klicken Sie auf **OK**, um das Konfigurationswerkzeug zu beenden und diese Einstellungen anzuwenden.
15. Jetzt melden Sie sich zum ersten Mal bei der Acronis Access Server-Webkonsole an, um die Konfiguration abzuschließen. Sie werden aufgefordert, auf 'OK' zu klicken, um einen Webbrowser zu starten und diese Konfiguration abzuschließen.




### 2.3.2.2 Upgrade eines activEcho Servers mit mobilEcho Client Management Server

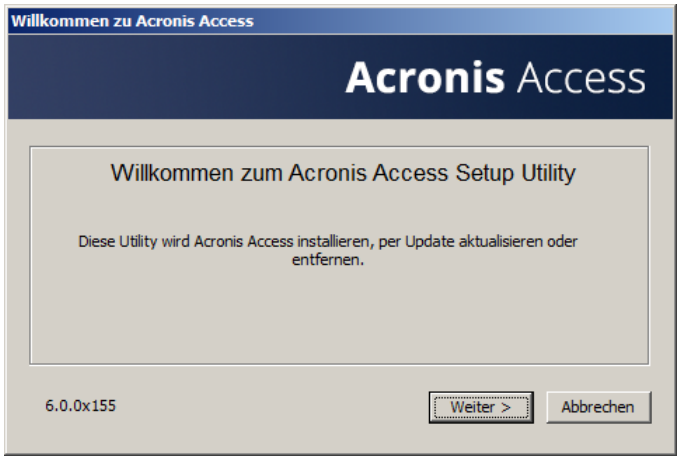
**Szenario 2 – Upgrade eines activEcho Servers mit mobilEcho Client Management Server**

In diesem Szenario werden auf einem Windows Server der activEcho Server sowie der mobilEcho File Server und Management Server ausgeführt. Bei diesem Vorgang erfolgt ein Upgrade des activEcho Servers und des mobilEcho Client Management Servers auf die einheitliche Acronis Access Server-Webkonsole. Die neue Konsole ersetzt außerdem das Windows-Programm mobilEcho-Administrator, das bisher zur Verwaltung von mobilEcho Servern verwendet wurde. Mit der Acronis Access Server-Webkonsole können Sie activEcho und mobilEcho über eine einheitliche Weboberfläche verwalten.

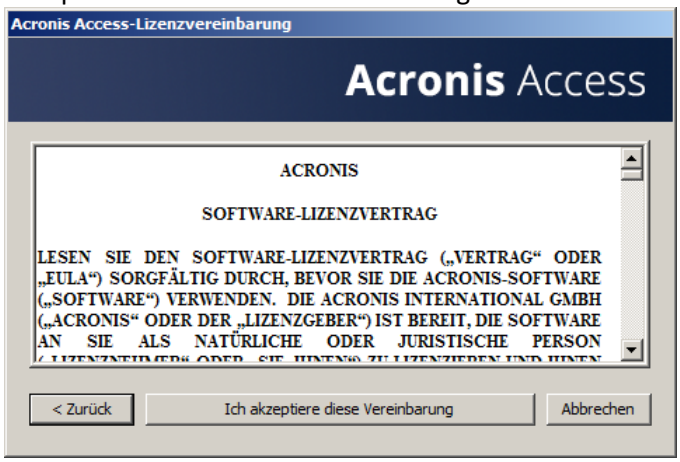
**So führen Sie ein Upgrade von activEcho durch:**

1. Sichern Sie alle erforderlichen Dateien wie in den folgenden Anleitungen beschrieben: mobilEcho 4.5 Backup bzw. activEcho 2.7 Backup.
2. Deaktivieren Sie alle vorhandenen Virenschutzprogramme, da sie unter Umständen den Installationsvorgang unterbrechen und somit eine fehlerhafte Installation verursachen können.
3. Laden Sie den Acronis Access Server Installer auf den activEcho Server herunter und führen Sie ihn aus.
   a. Um auf den neuesten Installer zuzugreifen, besuchen Sie die folgende Website: http://support.grouplogic.com/?page_id=3598
   b. Sie müssen die Produkt-Seriennummer zur Überprüfung eingeben, bevor Sie das Installationsprogramm herunterladen können.
   c. Die Installer-Datei hat folgenden Namen: AcronisAccessSetup.exe

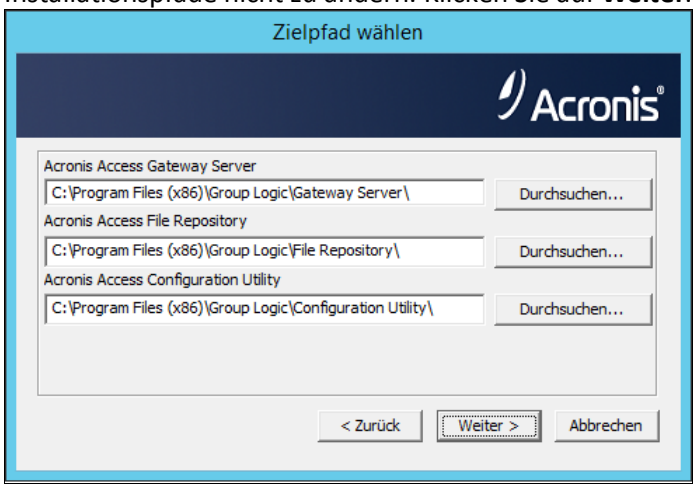
4. Klicken Sie auf der Willkommensseite auf **Weiter**.



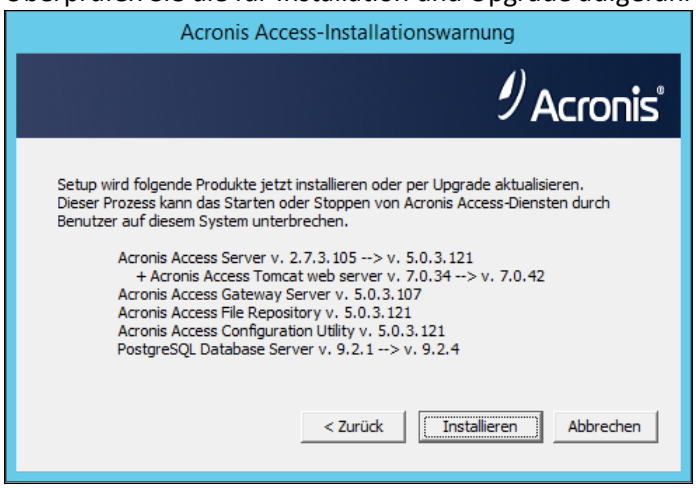

5. Akzeptieren Sie die Lizenzvereinbarung.



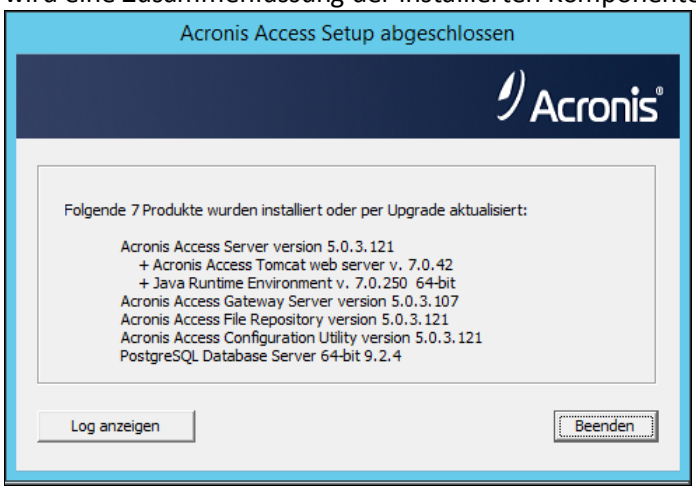
6. Klicken Sie auf **Upgrade**, um den activEcho Server und den mobilEcho Client Management Server automatisch auf den neuen Acronis Access Server zu aktualisieren. Im Rahmen des Upgrade-Prozesses werden auch ein Gateway Server und die erforderlichen Dienste installiert. Falls ein File Server vorhanden ist, führt das Installationsprogramm ein Upgrade des File Servers auf den neuen Gateway Server durch, anstatt einen neuen File Server zu installieren.
7. Wählen Sie einen Installationsspeicherort für die zu installierenden Acronis Access-Komponenten aus. Falls Sie ein Upgrade eines vorhandenen activEcho Servers durchführen, wird für diese Pfade standardmäßig der vorhandene Installationsspeicherort verwendet. Wir empfehlen, diese Installationspfade nicht zu ändern. Klicken Sie auf **Weiter**.




8. Überprüfen Sie die für Installation und Upgrade aufgeführten Dienste.

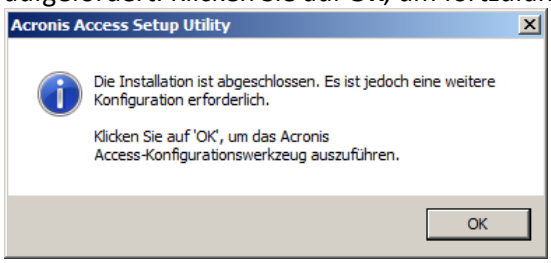


9. Klicken Sie auf **Installieren**, um mit der Installation zu beginnen. Nach Abschluss der Installation wird eine Zusammenfassung der installierten Komponenten angezeigt. Klicken Sie auf **Beenden**.




***Hinweis:*** *Alle erforderlichen Komponenten werden automatisch nacheinander installiert. Dieser Vorgang kann je nach Server 5 bis 15 Minuten dauern. Zukünftige Upgrades werden schneller installiert.*

10. An diesem Punkt des Upgrade-Prozesses wurden alle erforderlichen Software-Komponenten installiert. Jetzt müssen Sie jedoch die Netzwerkschnittstellen, Ports und Zertifikate konfigurieren, die verwendet werden sollen. Dieser Schritt ist obligatorisch. Beim Beenden des Installationsprogramms werden Sie zur Ausführung des Acronis Access-Konfigurationswerkzeugs aufgefordert. Klicken Sie auf **OK**, um fortzufahren.

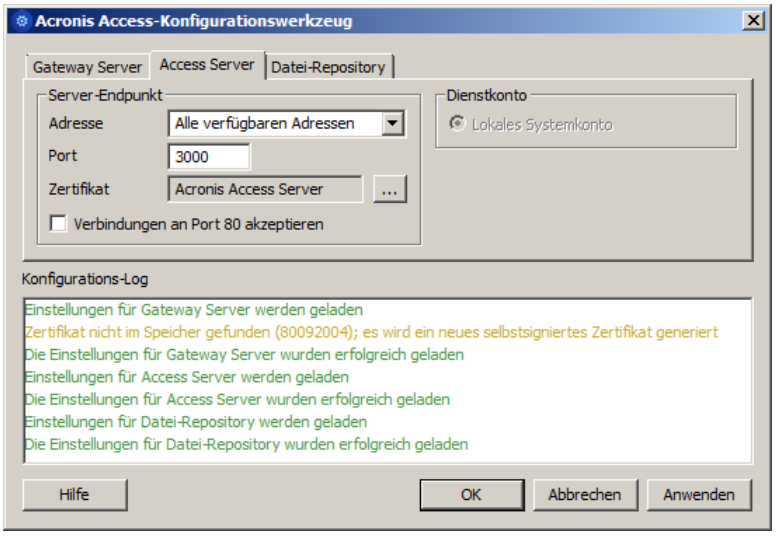



11. Im Konfigurationswerkzeug können Sie auf der Registerkarte 'Gateway Server' die Netzwerkadresse, den Port und das Zertifikat des Acronis Access Gateway Servers konfigurieren. Der Acronis Access Gateway Server ist der Acronis Access Kerndienst, zu dem die mobilEcho Clients eine Verbindung herstellen und der Zugriff auf Dateiserver, NAS und SharePoint-Server bietet.

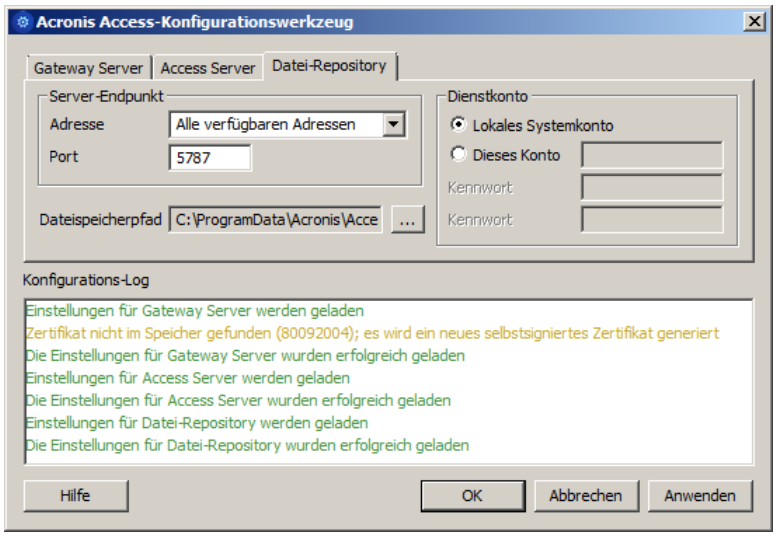
***Hinweis:*** *Die vorhandenen Einstellungen bleiben erhalten. Überprüfen Sie, ob diese Einstellungen mit den vorhandenen mobilEcho File Access Server-Einstellungen übereinstimmen. Dieser Dienst kann in der Regel auf allen verfügbaren Netzwerkadressen an Port 443 ausgeführt werden. Falls Sie über ein SSL-Serveridentitätszertifikat verfügen, wird dieses automatisch ausgewählt. Andernfalls wird ein selbstsigniertes Zertifikat generiert.*

12. Auf der Registerkarte 'Access Server' werden die Netzwerkadresse, der Port und das Zertifikat des Acronis Access Servers konfiguriert. Der Acronis Access Server ist die Webkonsole, über die alle Sync & Share-Funktionen und die activEcho-Benutzer konfiguriert und alle Aufgaben im Zusammenhang mit Serveradministration und Remote-Client-Management durchgeführt werden. Dies ist auch die Konsole, mit der Benutzer auf den Web-Client zugreifen.

***Hinweis:*** *Überprüfen Sie die Einstellungen für den Access Server. Die Standardeinstellungen werden empfohlen. Diese Webkonsole kann in der Regel auf allen verfügbaren Netzwerkadressen an Port 3000 ausgeführt werden. Falls Sie über ein SSL-Serveridentitätszertifikat verfügen, wird dieses automatisch ausgewählt. Andernfalls wird ein selbstsigniertes Zertifikat generiert.*

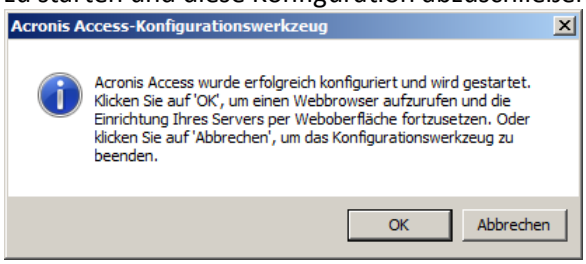



***Hinweis:*** *Acronis Access Server erfordert die Auswahl eines Speicherorts für das Datei-Repository. Dieses Repository wird von den Dateisynchronisierungs- und Freigabefunktionen (Sync & Share) von Acronis activEcho verwendet.*




13. Klicken Sie auf **OK**, um das Konfigurationswerkzeug zu beenden und diese Einstellungen anzuwenden.

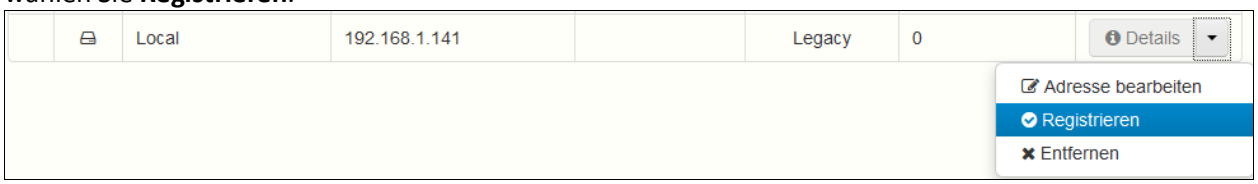
14. Jetzt melden Sie sich zum ersten Mal bei der Acronis Access Server-Webkonsole an, um die Konfiguration abzuschließen. Sie werden aufgefordert, auf 'OK' zu klicken, um einen Webbrowser zu starten und diese Konfiguration abzuschließen.




## Den Gateway registrieren

In diesem Szenario darf nur ein einziger Windows Server vorhanden sein, auf dem die Acronis Access-Konsole und der Gateway Server ausgeführt werden, daher wird auf der Seite 'Gateway Server' nur ein Server aufgeführt. Dieser Server muss registriert werden, damit Sie ihn verwalten können.

1. Klicken Sie auf dem Acronis Access Server auf die Menüschaltfläche für den Gateway Server und wählen Sie **Registrieren**.




2. Sie werden gefragt, ob die vorhandene Netzwerkadresse für den zu registrierenden Server den direkten Zugriff auf den Server ermöglicht. Die vorhandene Adresse ist in der Regel die Netzwerkadresse, über die die Benutzer mobiler Geräte auf den Gateway Server zugreifen, daher kann es sein, dass diese Adresse auf einen Proxy-Server oder ein Lastenausgleichsmodul verweist.

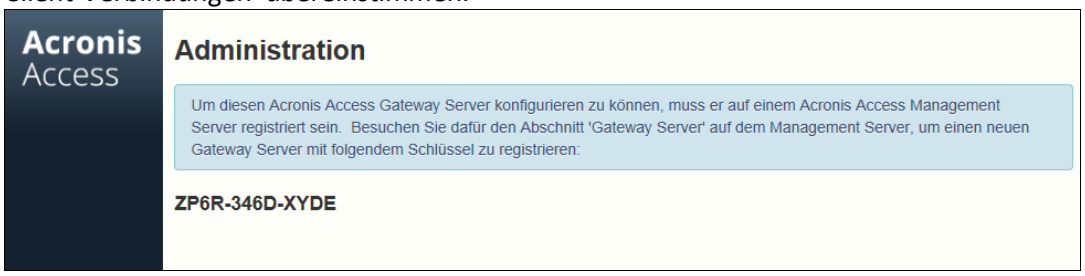
***Hinweis:*** *In diesem Fall müssen Sie in diesem Dialogfeld* ***'Nein'*** *wählen und eine alternative Netzwerkadresse eingeben, mit der der Acronis Access Server direkten Netzwerkzugriff auf den betreffenden Gateway Server erhält.*

3. Anschließend wird das Registrierungsdialogfeld angezeigt.


***Hinweis:*** *Falls der Gateway Server ein selbstsigniertes SSL-Zertifikat verwendet, müssen Sie die Option 'Verbindungen von Acronis Access Servern mit selbstsignierten Zertifikaten erlauben' aktivieren.*

***Hinweis:*** *Sie müssen außerdem einen Administrationsschlüssel eingeben, um die Kopplung mit diesem Remote-Server zu aktivieren. Dieser Schlüssel dient zur Validierung und Sicherung der administrativen Beziehung.*

4. Um einen Administrationsschlüssel vom Gateway Server zu erhalten, öffnen Sie ein neues Fenster oder eine neue Registerkarte im Browser und navigieren Sie zur HTTPS-Adresse des Gateway Servers. Diese muss mit der Adresse im Feld 'Adresse für Administration und Client-Verbindungen' übereinstimmen.




***Hinweis:*** *Aus Sicherheitsgründen muss dieser Schritt in einem Webbrowser auf dem Windows Server durchgeführt werden, auf dem der Gateway Server ausgeführt wird. In einem Remote-Webbrowser kann der Administrationsschlüssel nicht angezeigt werden.*

5. Geben Sie den 12-stelligen Administrationsschlüssel (einschließlich Bindestrichen) in das Registrierungsformular ein und klicken Sie auf **Speichern**.

> ***Hinweis:*** *Nachdem der Server registriert wurde, wird er in der Liste der Gateway Server als registriert angezeigt, sodass Sie jetzt die Einstellungen anpassen sowie die Details und den Status anzeigen können.*


### 2.3.2.3 Upgrade eines activEcho Servers mit einem mobilEcho Client Management Server auf einem anderen Server

**Szenario 3 – Upgrade eines activEcho Servers mit einem mobilEcho Client Management Server auf einem anderen Server**

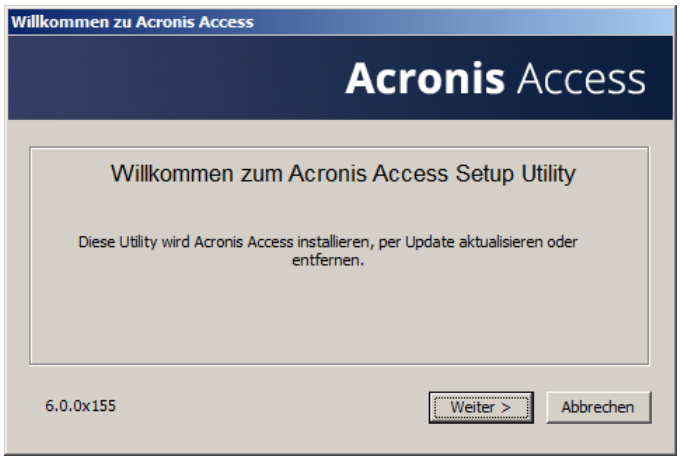
> ***Warnung!*** *Für dieses Szenario wird empfohlen, den activEcho Server und den mobilEcho Server getrennt zu verwalten und das Upgrade für jeden Server einzeln durchzuführen. Anweisungen zum Upgrade des activEcho Servers finden Sie unter Upgrade eines einzelnen activEcho Servers ohne mobilEcho Client Management Server (S. 68) und Anweisungen zum Upgrade des mobilEcho Servers unter Upgrade eines einzelnen mobilEcho Servers mit aktiviertem Client Management-Dienst (S. 44).*

In diesem Szenario besteht die Umgebung aus zwei (oder mehr) Windows Servern, wobei auf einem nur der activEcho Server ausgeführt wird und auf dem anderen der mobilEcho File Server und Management Server ausgeführt werden. Bei diesem Vorgang erfolgt ein Upgrade des activEcho Servers und des mobilEcho Client Management Servers auf die einheitliche Acronis Access Server-Webkonsole. Die neue Konsole ersetzt außerdem das Windows-Programm mobilEcho-Administrator, das bisher zur Verwaltung von mobilEcho Servern verwendet wurde. Mit der Acronis Access Server-Webkonsole können Sie activEcho und mobilEcho über eine einheitliche Weboberfläche verwalten.

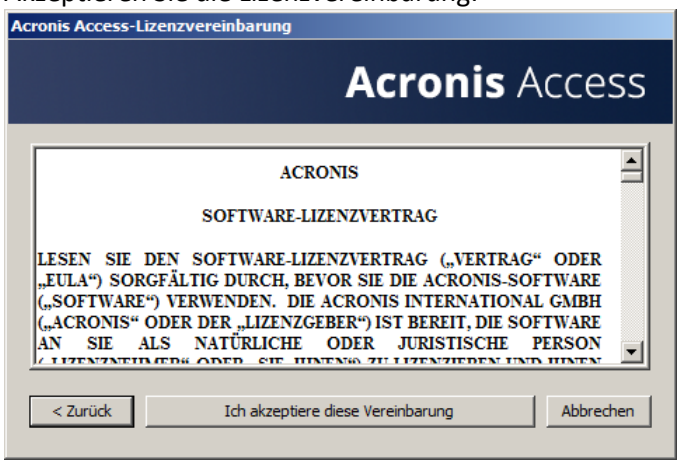
So führen Sie ein Upgrade auf Acronis Access Server durch:

1. Sichern Sie alle erforderlichen Dateien wie in den folgenden Anleitungen beschrieben: mobilEcho 4.5 Backup bzw. activEcho 2.7 Backup.
2. Notieren Sie die aktuelle IP-Adresse des Servers, auf dem mobilEcho ausgeführt wird, und weisen Sie dem Computer eine andere IP-Adresse zu (die neue Adresse wird ebenfalls benötigt).
3. Wechseln Sie zum Server mit activEcho und fügen Sie die IP-Adresse des Servers, auf dem mobilEcho ausgeführt wird, einem separaten Netzwerkadapter hinzu.
4. Deaktivieren Sie alle vorhandenen Virenschutzprogramme, da sie unter Umständen den Installationsvorgang unterbrechen und somit eine fehlerhafte Installation verursachen können.

5. Laden Sie den Acronis Access Server Installer auf den activEcho Server herunter und führen Sie ihn aus.
   a. Um auf den neuesten Installer zuzugreifen, besuchen Sie die folgende Website: http://support.grouplogic.com/?page_id=3598
   b. Sie müssen die Produkt-Seriennummer zur Überprüfung eingeben, bevor Sie das Installationsprogramm herunterladen können.
   c. Die Installer-Datei hat folgenden Namen: AcronisAccessSetup.exe
6. Klicken Sie auf der Willkommensseite auf **Weiter**.

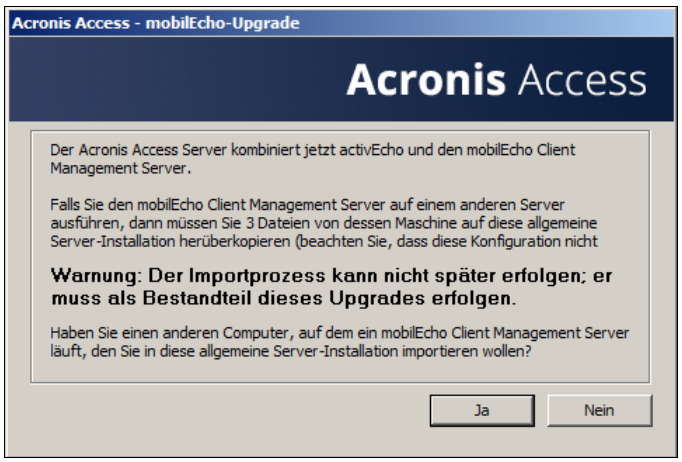



7. Akzeptieren Sie die Lizenzvereinbarung.

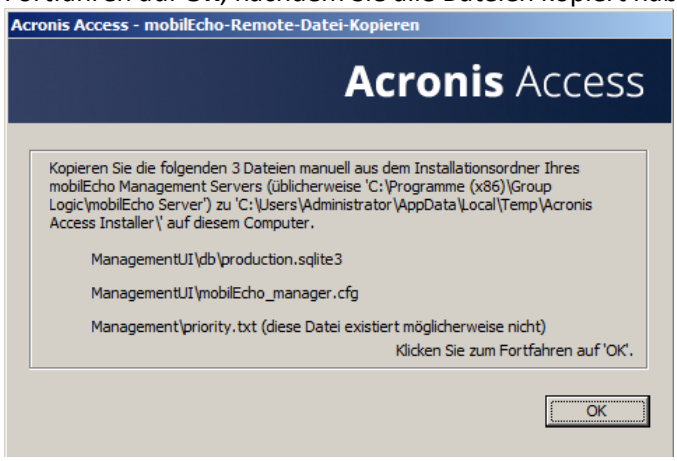



8. Klicken Sie auf **Upgrade**, um den activEcho Server automatisch auf den neuen Acronis Access Server zu aktualisieren. Im Rahmen des Upgrade-Prozesses werden auch ein Gateway Server und die erforderlichen Dienste installiert.

9. Falls Sie über einen mobilEcho Client Management Server verfügen, wählen Sie **Ja**. Andernfalls fahren Sie mit dem ersten Abschnitt fort, in dem das Upgrade ohne vorhandene mobilEcho-Installation beschrieben wird.




10. Wechseln Sie zu dem Server, auf dem der mobilEcho Client Management Server ausgeführt wird, und suchen Sie die folgenden drei Dateien: **production.sqlite3**, **mobilEcho_manager.cfg**, **priority.txt** (diese Datei ist möglicherweise nicht vorhanden). Kopieren Sie die Dateien auf der Maschine, auf der Sie das Upgrade initiiert haben, in den im Dialogfeld angegebenen Ordner. Der Pfad ist bei jeder Installation anders. (Beispiel: C:\Benutzer\Administrator\AppData\Local\Temp\Acronis Access Installer\). Klicken Sie zum Fortfahren auf **OK**, nachdem Sie alle Dateien kopiert haben.



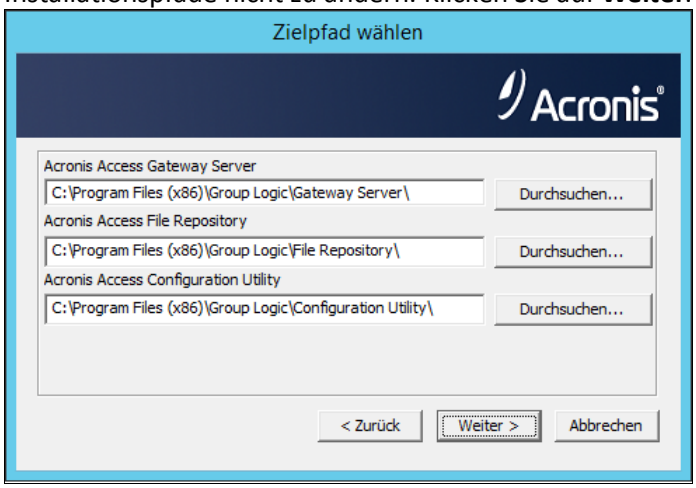

***Hinweis:*** *Diese Dateien werden normalerweise im folgenden Verzeichnis gespeichert:*

***C:\Program Files (x86)\Group Logic\mobilEcho Server\ManagementUI\db\production.sqlite3***

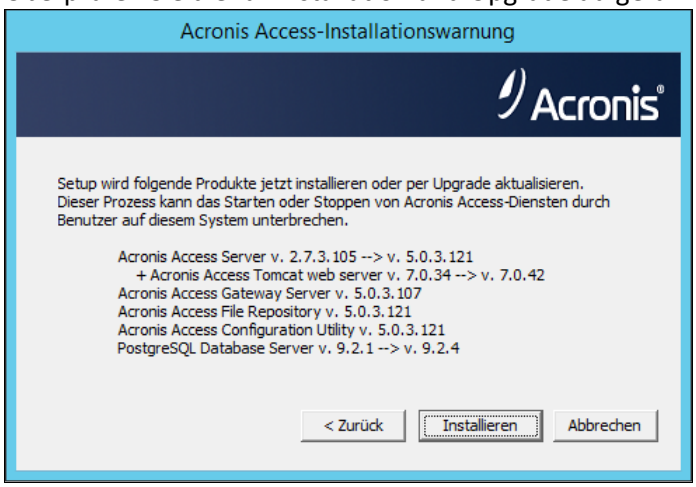
***C:\Program Files (x86)\Group Logic\mobilEcho Server\ManagementUI\mobilEcho_manager.cfg***

***C:\Program Files (x86)\Group Logic\mobilEcho Server\Management\priority.txt***

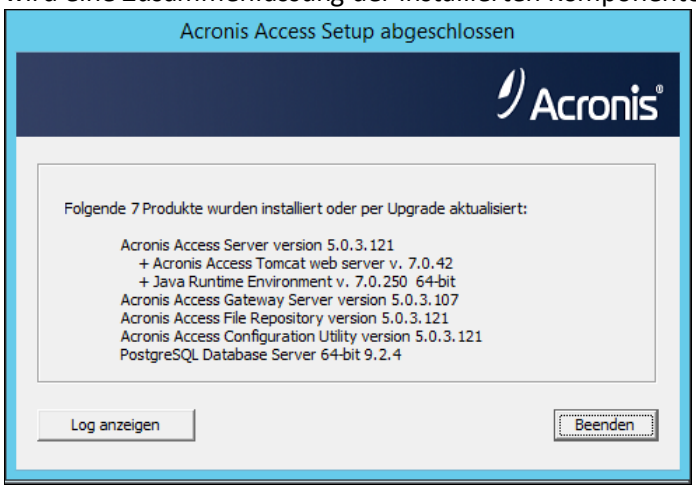
11. Wählen Sie einen Installationsspeicherort für die zu installierenden Acronis Access-Komponenten aus. Falls Sie ein Upgrade eines vorhandenen activEcho Servers durchführen, wird für diese Pfade standardmäßig der vorhandene Installationsspeicherort verwendet. Wir empfehlen, diese Installationspfade nicht zu ändern. Klicken Sie auf **Weiter**.




12. Überprüfen Sie die für Installation und Upgrade aufgeführten Dienste.

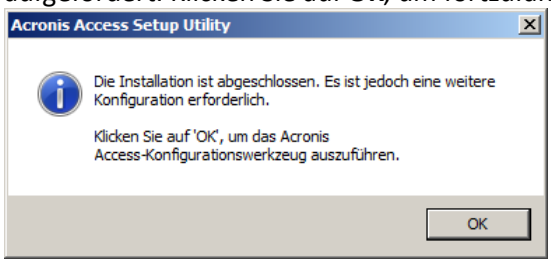



13. Klicken Sie auf **Installieren**, um mit der Installation zu beginnen. Nach Abschluss der Installation wird eine Zusammenfassung der installierten Komponenten angezeigt. Klicken Sie auf **Beenden**.




***Hinweis:*** *Alle erforderlichen Komponenten werden automatisch nacheinander installiert. Dieser Vorgang kann je nach Server 5 bis 15 Minuten dauern. Zukünftige Upgrades werden schneller installiert.*

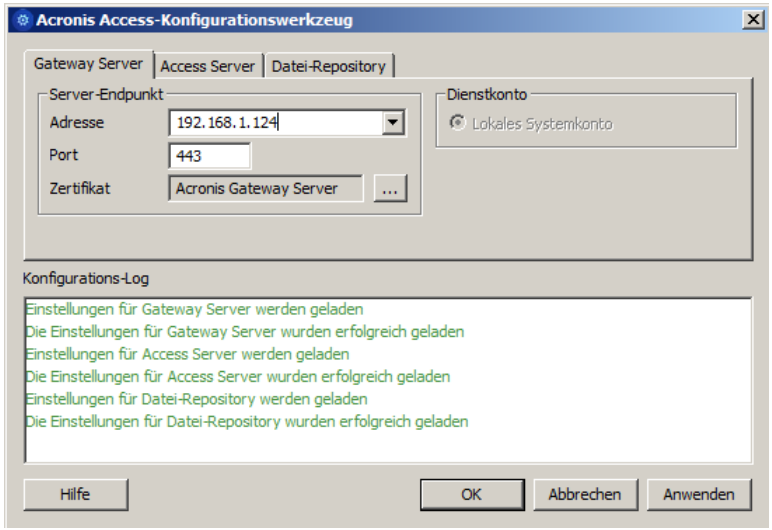
14. An diesem Punkt des Upgrade-Prozesses wurden alle erforderlichen Software-Komponenten installiert. Jetzt müssen Sie jedoch die Netzwerkschnittstellen, Ports und Zertifikate konfigurieren, die verwendet werden sollen. Dieser Schritt ist obligatorisch. Beim Beenden des Installationsprogramms werden Sie zur Ausführung des Acronis Access-Konfigurationswerkzeugs aufgefordert. Klicken Sie auf **OK**, um fortzufahren.




## Das Konfigurationswerkzeug verwenden

### Auf der Registerkarte „Gateway Server“

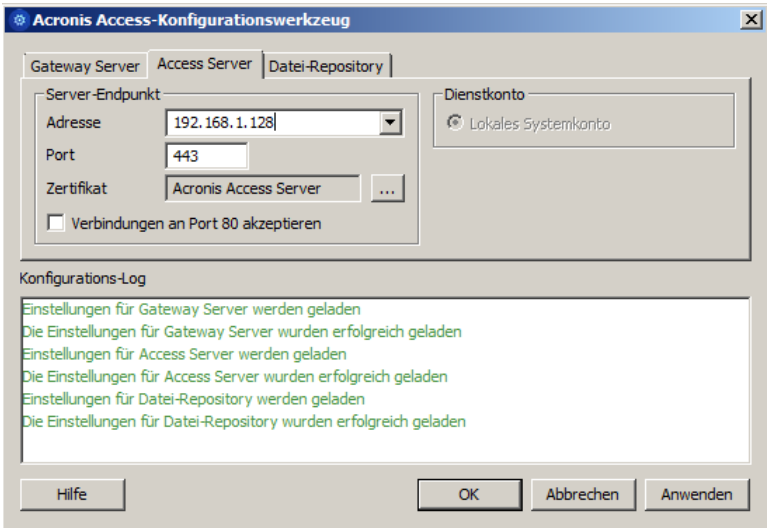
1. Geben Sie im Feld **Adresse** die IP-Adresse des Servers ein, auf dem mobilEcho ausgeführt wurde. Dies ist die Adresse, die Sie zu Beginn des Verfahrens notiert haben.
2. Geben Sie in das Feld **Port** die Port-Nummer ein, die vom mobilEcho File Server verwendet wurde.
3. Fügen Sie das Zertifikat hinzu, das Sie für den mobilEcho File Server verwendet haben.




### Auf dem Access Server

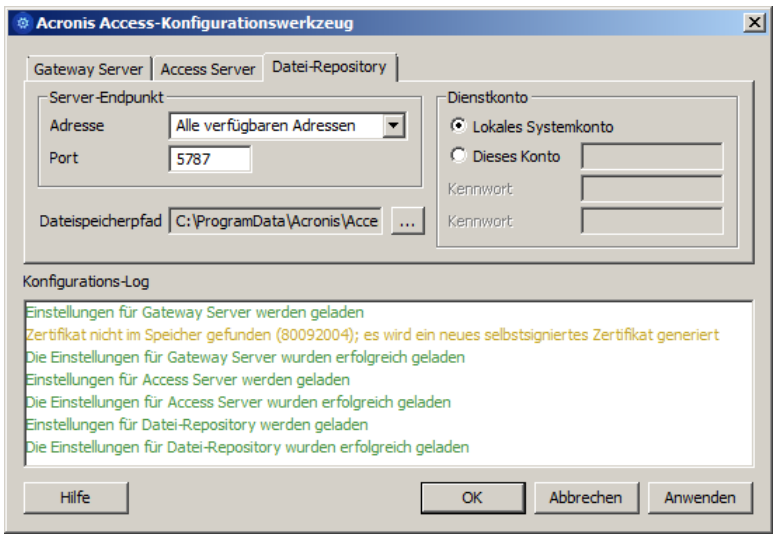
1. Geben Sie im Feld **Adresse** die IP-Adresse ein, die Sie bisher für den activEcho Server verwendet haben. Dies ist in der Regel der Standardwert.
2. Geben Sie im Feld **Port** die Port-Nummer ein, die Sie bisher für den activEcho Server verwendet haben. Dies sollte der Standardwert sein.

3. Fügen Sie das Zertifikat hinzu, das Sie für den activEcho Server verwendet haben.




**Auf der Registerkarte „Datei-Repository“**

1. Geben Sie im Feld **Adresse** die IP-Adresse oder den DNS-Namen des Repository-Diensts ein. Dies sollte der Standardwert sein.
2. Geben Sie im Feld **Port** die Port-Nummer für den Repository-Dienst ein. Dies sollte der Standardwert sein.
3. Wählen Sie den Pfad zum FileStore-Ordner aus. Dies sollte der Standardwert sein.

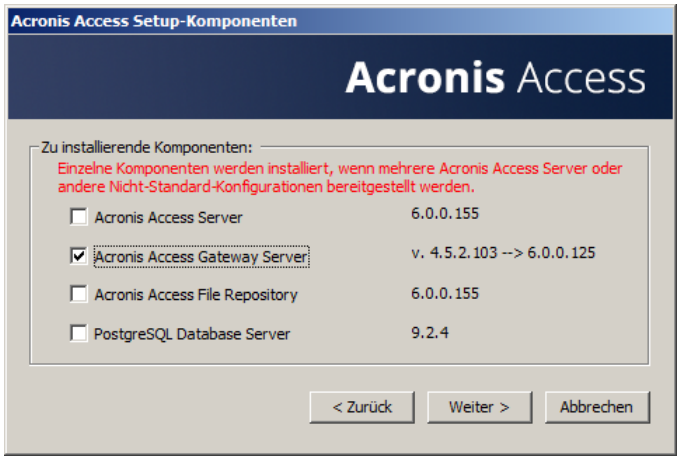



Nachdem Sie alle erforderlichen Konfigurationen vorgenommen haben, klicken Sie auf „OK“, um das Konfigurationswerkzeug zu beenden.

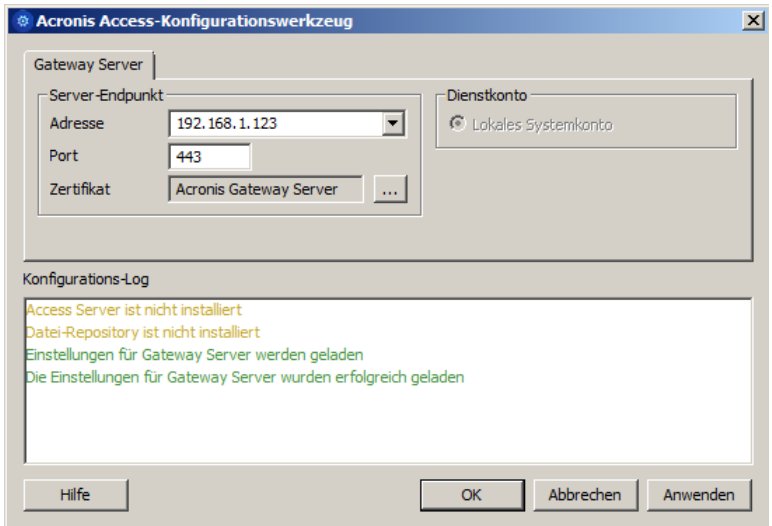
## Den lokalen Gateway Server konfigurieren

1. Kopieren Sie das Installationsprogramm von Acronis Access und legen Sie es auf dem Server mit mobilEcho ab.
2. Stoppen Sie den Dienst mobilEcho Management Server.

3. Führen Sie das Installationsprogramm aus und klicken Sie auf der Willkommensseite auf **Weiter**.
4. Lesen und akzeptieren Sie die Lizenzvereinbarung.
5. Klicken Sie auf **Benutzerdefiniert**.
6. Wählen Sie nur die Komponente **Gateway Server** aus und klicken Sie auf **Weiter**.

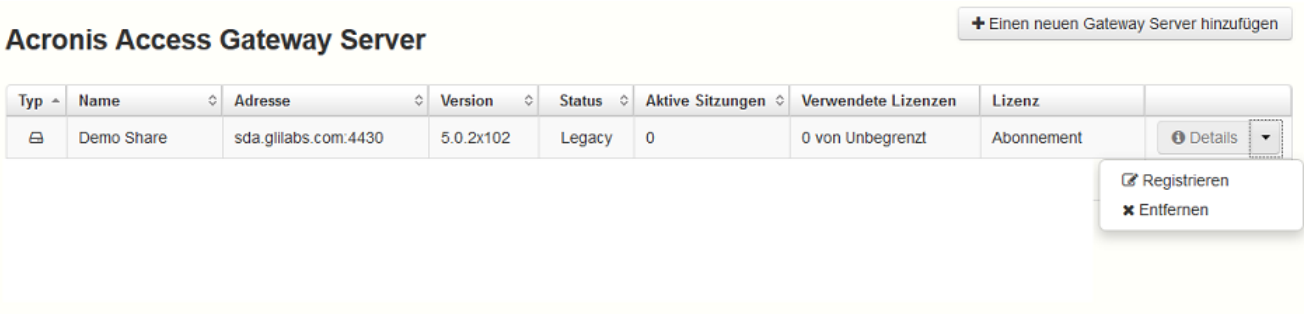



7. Überprüfen Sie den Installationspfad und klicken Sie auf **Weiter**. Dies ist in der Regel der Standardwert.
8. Überprüfen Sie die zur Installation ausgewählten Komponenten und klicken Sie auf **Installieren**.
9. Schließen Sie den Installer nach Abschluss der Installation, und starten Sie das Konfigurationswerkzeug (wenn es nicht automatisch startet, finden Sie es im Allgemeinen unter: **`C:\Program Files (x86)\Group Logic\Configuration Utility`**).
10. Geben Sie im Feld **Adresse** die neue IP-Adresse ein, die Sie dem Computer zugewiesen haben, der mobilEcho hostet.
11. Geben Sie in das Feld **Port** die Port-Nummer ein, die vom mobilEcho File Server zuvor verwendet wurde (dies sollte der Standardwert sein).



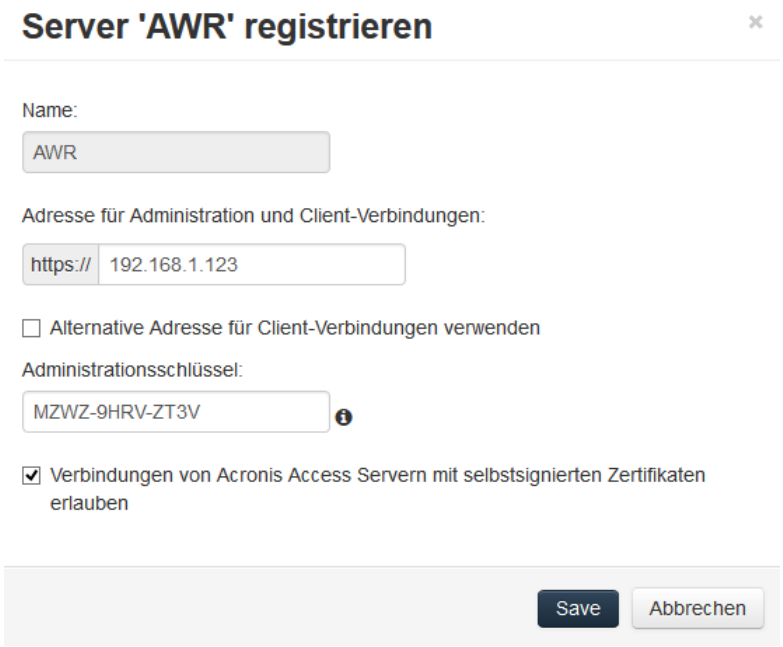

12. Drücken Sie **OK**, um die Konfiguration abzuschließen und das Werkzeug zu schließen.
13. Rufen Sie die Acronis Access Weboberfläche auf und melden Sie sich an.
14. Erweitern Sie die Registerkarte **Mobiler Zugriff** und öffnen Sie die Seite **Gateway Server**.

15. Suchen Sie den Gateway Server mit einem **Legacy**-Status, öffnen Sie das Dropdown-Menü für dieses Gateway und wählen Sie **Registrieren**.




16. Klicken Sie im angezeigten Dialogfeld auf **Ja**.


17. Geben Sie in das Feld **Adresse für Administration und Client-Verbindungen** die IP-Adresse des aktualisierten Gateway Servers ein. Dies ist die neue IP-Adresse, die Sie dem Computer zugewiesen haben, von dem mobilEcho zuvor gehostet wurde.

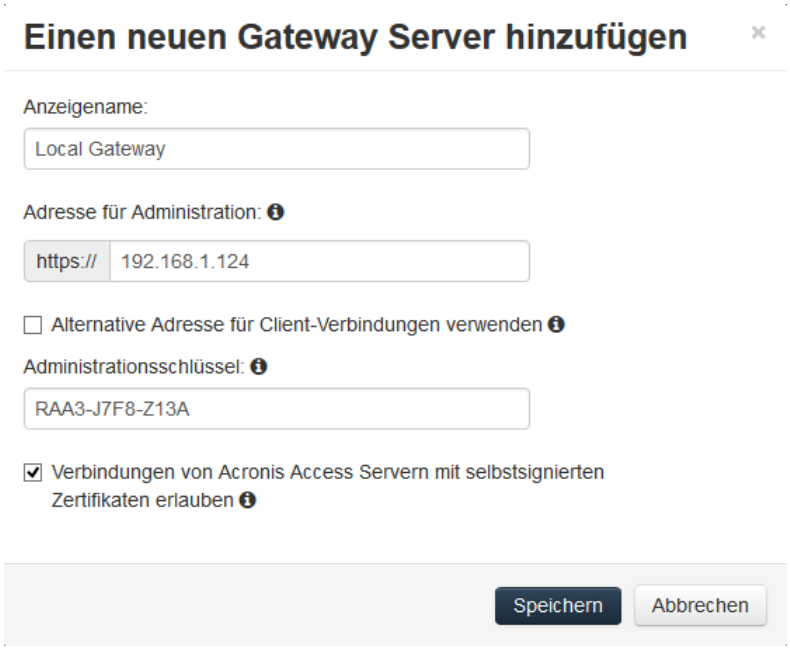



18. Geben Sie im Feld **Administrationsschlüssel** den Schlüssel des Gateway Servers ein. Um den Schlüssel zu erhalten, öffnen Sie die IP-Adresse des Gateways in einem Browser (z.B. https://192.168.1.1). Dies muss auf dem Computer geschehen, auf dem mobilEcho zuvor installiert war.
19. Registrieren Sie das Gateway, indem Sie auf **Speichern** klicken.

### Den lokalen Gateway Server registrieren

Gehen Sie auf der Seite 'Gateway Server' folgendermaßen vor:

1. Klicken Sie auf die Schaltfläche **Gateway Server hinzufügen**.
2. Geben Sie einen Anzeigenamen für den neuen Gateway Server ein.
3. Geben Sie die IP-Adresse des Gateway Servers ein. Dies ist die IP-Adresse, die zuvor vom mobilEcho-Server verwendet wurde (diese IP-Adresse haben Sie zu Anfang notiert).
4. Geben Sie den Administrationsschlüssel für den Gateway ein. Um den Schlüssel zu erhalten, öffnen Sie die IP-Adresse des Gateways in einem Browser (z.B. https://192.168.1.1). Die muss auf dem Computer geschehen, auf dem jetzt der Acronis Access-Server gehostet wird.




5. Registrieren Sie den Gateway, indem Sie auf **Speichern** klicken.

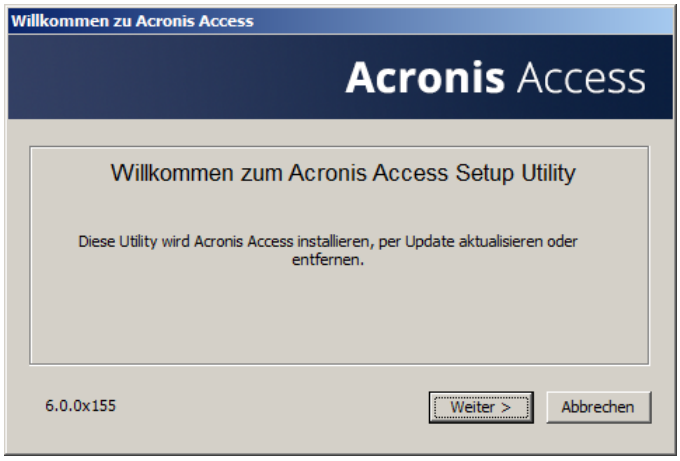
## 2.4 Upgrade – Geclusterte Konfigurationen

Um das Upgrade einer geclusterten Konfiguration von Acronis Access durchzuführen, müssen Sie sowohl für den Acronis Access Server als auch für die Gateway Server in der Cluster-Gruppe ein Upgrade durchführen. Anweisungen zum Upgrade von Access Server finden Sie im Artikel Upgrade von Acronis Access auf eine neuere Version (S. 19). Für jedes Gateway müssen Sie das folgende Verfahren durchführen.

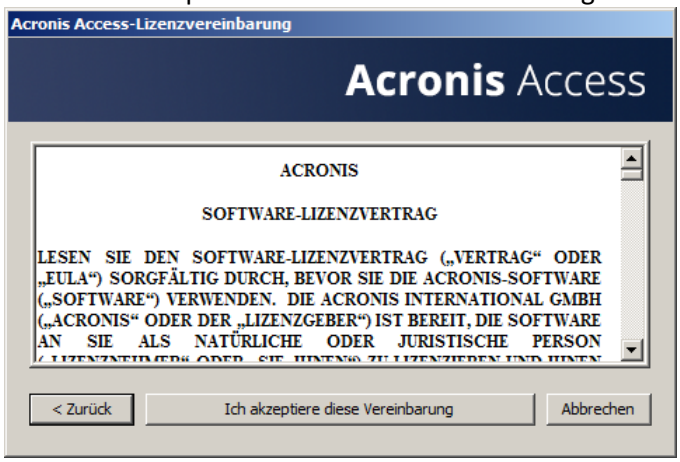
Informationen zum Upgrade einer Microsoft Failover-Clustering-Konfiguration finden Sie im Abschnitt Ergänzendes Material.

## Upgrade eines Gateway Servers

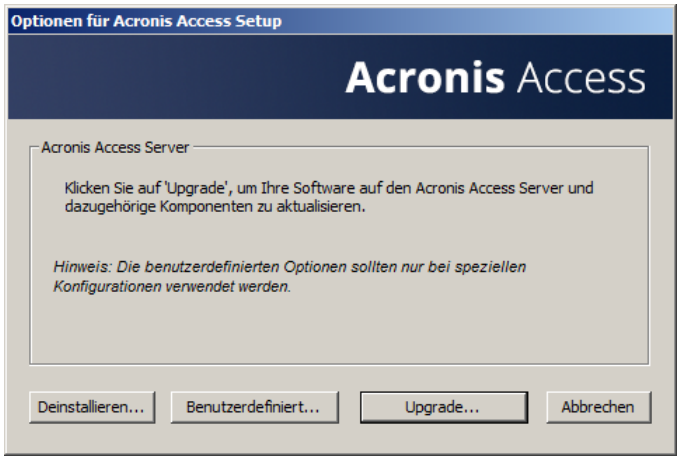
1. Führen Sie das Acronis Access-Installationsprogramm auf dem gewünschten Server aus.
2. Klicken Sie auf der Willkommensseite auf **Weiter**.




3. Lesen und akzeptieren Sie die Lizenzvereinbarung.




4. Klicken Sie auf **Benutzerdefiniert**.




5. Wählen Sie nur die Komponente **Acronis Access Gateway Server** aus, und klicken Sie auf **Weiter**.
6. Überprüfen Sie die Komponenten, und klicken Sie auf **Installieren**.
7. Überprüfen Sie nach Abschluss der Installation die Zusammenfassung, und schließen Sie das Installationsprogramm. Sie werden aufgefordert, das Konfigurationswerkzeug zu öffnen. Öffnen Sie es, um zu überprüfen, ob alle vorherigen Gateway Server-Einstellungen vorhanden sind. Nehmen Sie bei Bedarf Änderungen vor, und klicken Sie auf 'OK'.

# 3 Schnellstart: Mobile Access

Diese Anleitung enthält die wesentlichen Schritte zum Einrichten eines Gateway Servers, zum Hinzufügen einer Datenquelle und zur Installation der Access Mobile Client-App. Ausführlichere Informationen über die Konfiguration des Acronis Access Gateway Servers und der Client Management-Komponenten finden Sie in den Abschnitten Gateway-Server verwalten und Mobiler Zugriff.

**Themen**



## 3.1 Erste Ausführung

Wenn Sie es nicht bereits erledigt haben, installieren und konfigurieren Sie Acronis Access. Weitere Informationen hierzu finden Sie in den Abschnitten zur Installation (S. 4) und zum Konfigurationswerkzeug (S. 10).

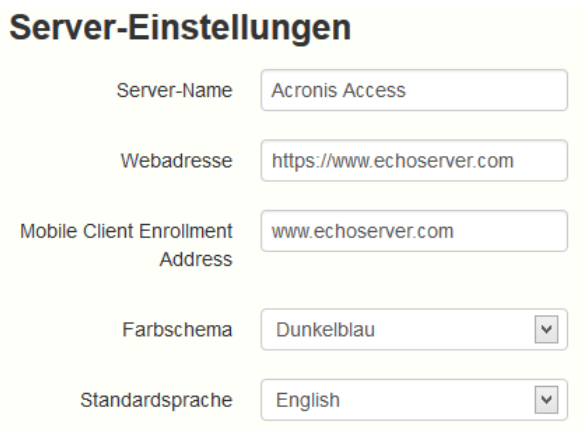
Wenn Sie die Weboberfläche erstmals verwenden, müssen Sie ein Kennwort für das Standardadministratorkonto eingeben. Nach der Anmeldung wird dann der **Installationsassistent** aufgerufen.

***Warnung!*** *Merken Sie sich das Administratorkennwort gut, denn der Support kann dieses Kennwort nicht wiederherstellen.*

***Hinweis:*** *Es kann 30 - 45 Sekunden dauern, bis die Applikation zur Verfügung steht, nachdem Sie sie über das Konfigurationswerkzeug gestartet haben.*

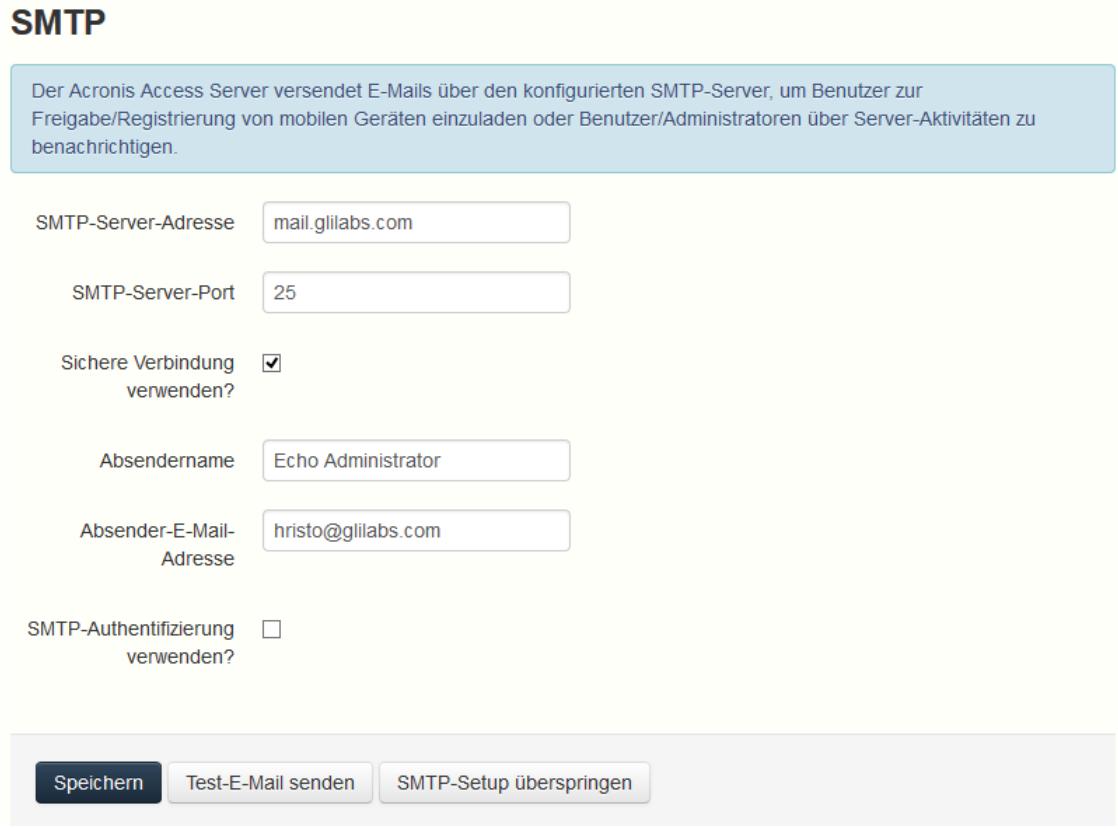
Sobald Sie die oben genannten Schritte abgeschlossen haben, können Sie die unten beschriebene Erstkonfiguration ausführen.

**Allgemeine Einstellungen**



1. Geben Sie einen Servernamen ein.
2. Geben Sie den DNS-Stammnamen oder die IP-Adresse ein, über den bzw. die Benutzer auf die Website zugreifen (beginnend mit http:// oder https://).
3. Geben Sie den DNS-Namen oder die IP-Adresse an, über den bzw. die sich mobile Benutzer registrieren.
4. Wählen Sie ein Farbschema aus. Die derzeit verfügbaren Optionen sind Grau, Violett, Cappuccino, Blau, Dunkelblau und Orange.
5. Wählen Sie die Standardsprache für das **Überwachungsprotokoll** aus. Die derzeit verfügbaren Optionen sind Englisch, Deutsch, Französisch und Japanisch.
6. Klicken Sie auf **Speichern**.

**SMTP**

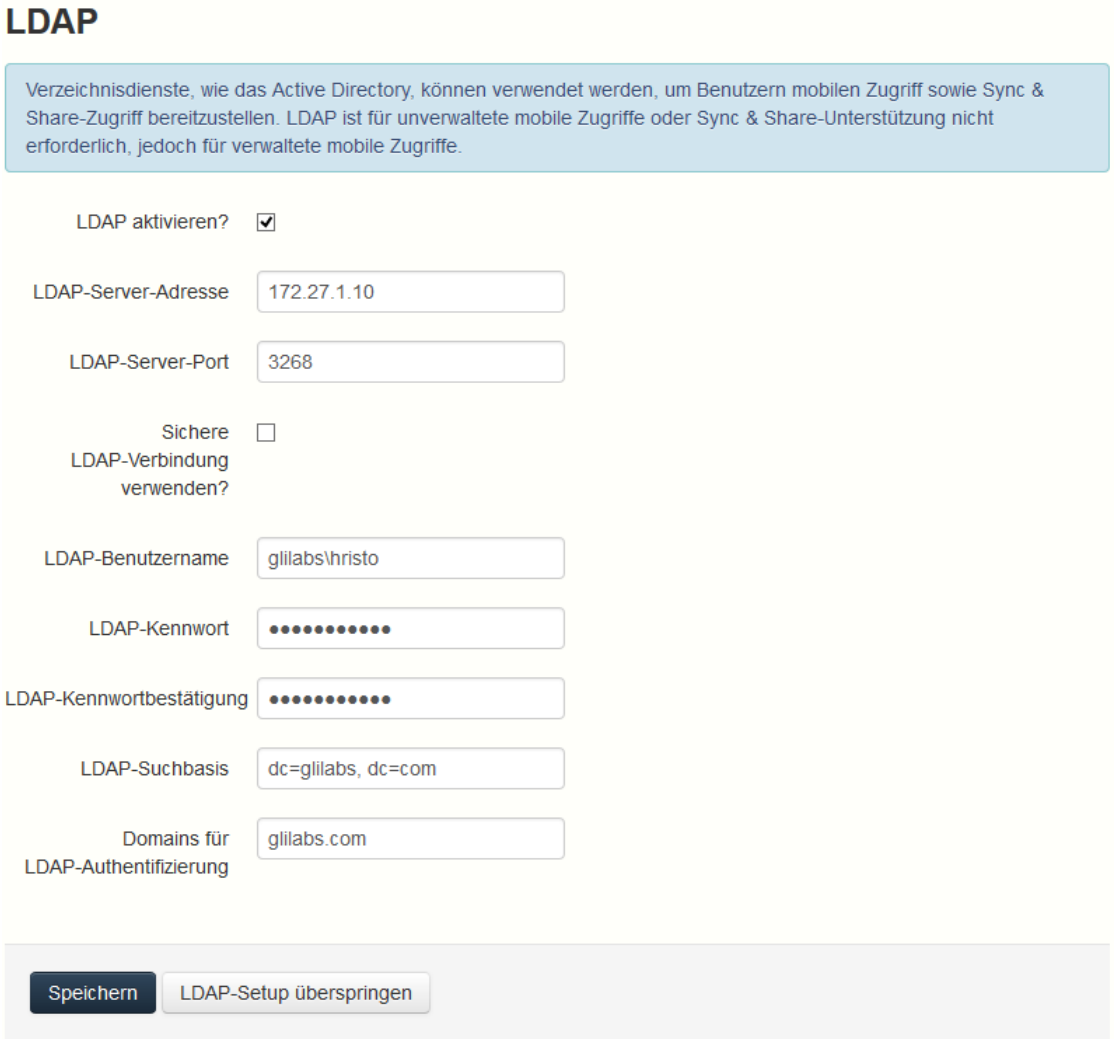



***Hinweis:*** *Sie können diesen Abschnitt überspringen und SMTP später konfigurieren.*

1. Geben Sie den DNS-Namen oder die IP-Adresse des SMTP-Servers ein.
2. Geben Sie den SMTP-Port des Servers ein.
3. Wenn Sie keine Zertifikate für den SMTP-Server verwenden, deaktivieren Sie **Sichere Verbindung verwenden?**.
4. Geben Sie den Namen ein, der in der 'Von'-Zeile von E-Mails angezeigt wird, die vom Server gesendet werden.
5. Geben Sie die Adresse ein, die als Absender der vom Server gesendeten E-Mails verwendet wird.

6. Falls Sie für den SMTP-Server eine Authentifizierung per Benutzername/Kennwort verwenden, aktivieren Sie **SMTP-Authentifizierung verwenden?**, und geben Sie Ihre Anmeldedaten ein.
7. Klicken Sie auf **Test-E-Mail senden**, um eine Test-E-Mail an die in Schritt 5 festgelegte Adresse zu senden.
8. Klicken Sie auf **Speichern**.

**LDAP**




***Hinweis:*** *Sie können diesen Abschnitt überspringen und LDAP später konfigurieren.*

1. Markieren Sie **LDAP aktivieren**.
2. Geben Sie den DNS-Namen oder die IP-Adresse des LDAP-Servers ein.
3. Geben Sie den Port des LDAP-Servers ein.
4. Falls Sie ein Zertifikat für Verbindungen mit dem LDAP-Server verwenden, markieren Sie **Sichere LDAP-Verbindung verwenden**.
5. Geben Sie Ihre LDAP-Anmeldedaten einschließlich der Domain ein (z.B. acronis\hristo).
6. Geben Sie die LDAP-Suchbasis ein.

7. Geben Sie die gewünschte(n) Domain(s) für die LDAP-Authentifizierung ein. (Für ein Konto mit der E-Mail-Adresse **joe@glilabs.com** würden Sie zur LDAP-Authentifizierung beispielsweise **glilabs.com** eingeben.)
8. Klicken Sie auf **Speichern**.

**Lokaler Gateway Server**


***Hinweis:*** *Wenn Sie einen Gateway Server und den Acronis Access Server auf derselben Maschine installieren, wird der Gateway Server automatisch erkannt und vom Acronis Access Server verwaltet. Sie werden aufgefordert, den DNS-Namen oder die IP-Adresse festzulegen, unter dem bzw. der der lokale Gateway Server für die Clients erreichbar ist. Diese Adresse können Sie später ändern.*

1. Legen Sie einen DNS-Namen oder eine IP-Adresse für den lokalen Gateway Server fest.
2. Klicken Sie auf **Speichern**.

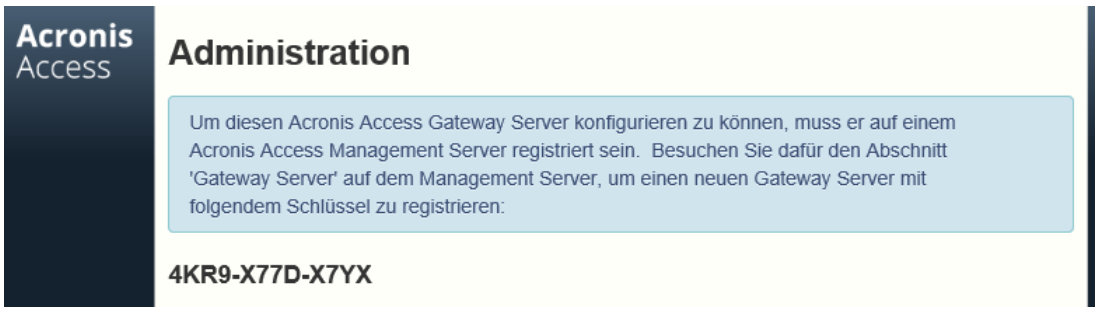
## 3.2 Den ersten Gateway Server und die erste Datenquelle konfigurieren

**Einen neuen Gateway Server registrieren:**

1. Greifen Sie auf den Computer zu, auf dem der Gateway Server installiert ist.
2. Öffnen Sie **https://localhost/**.

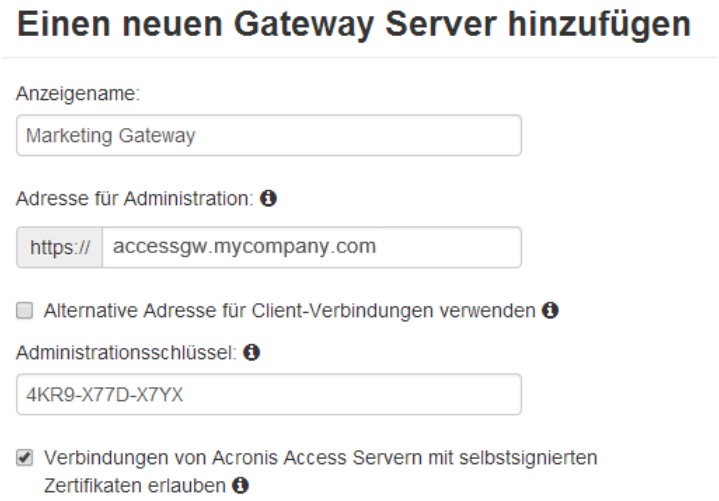
   ***Hinweis:*** *Der Port 443 ist der Standard-Port. Falls Sie den Standard-Port geändert haben, geben Sie im Anschluss an localhost Ihre Portnummer ein.*

3. Notieren Sie den **Administrationsschlüssel**.




4. Rufen Sie die Acronis Access-Weboberfläche auf.
5. Öffnen Sie die Registerkarte **Mobiler Zugriff**.
6. Öffnen Sie die Seite **Gateway Server**.

7. Drücken Sie die Schaltfläche **Einen neuen Gateway Server hinzufügen**.



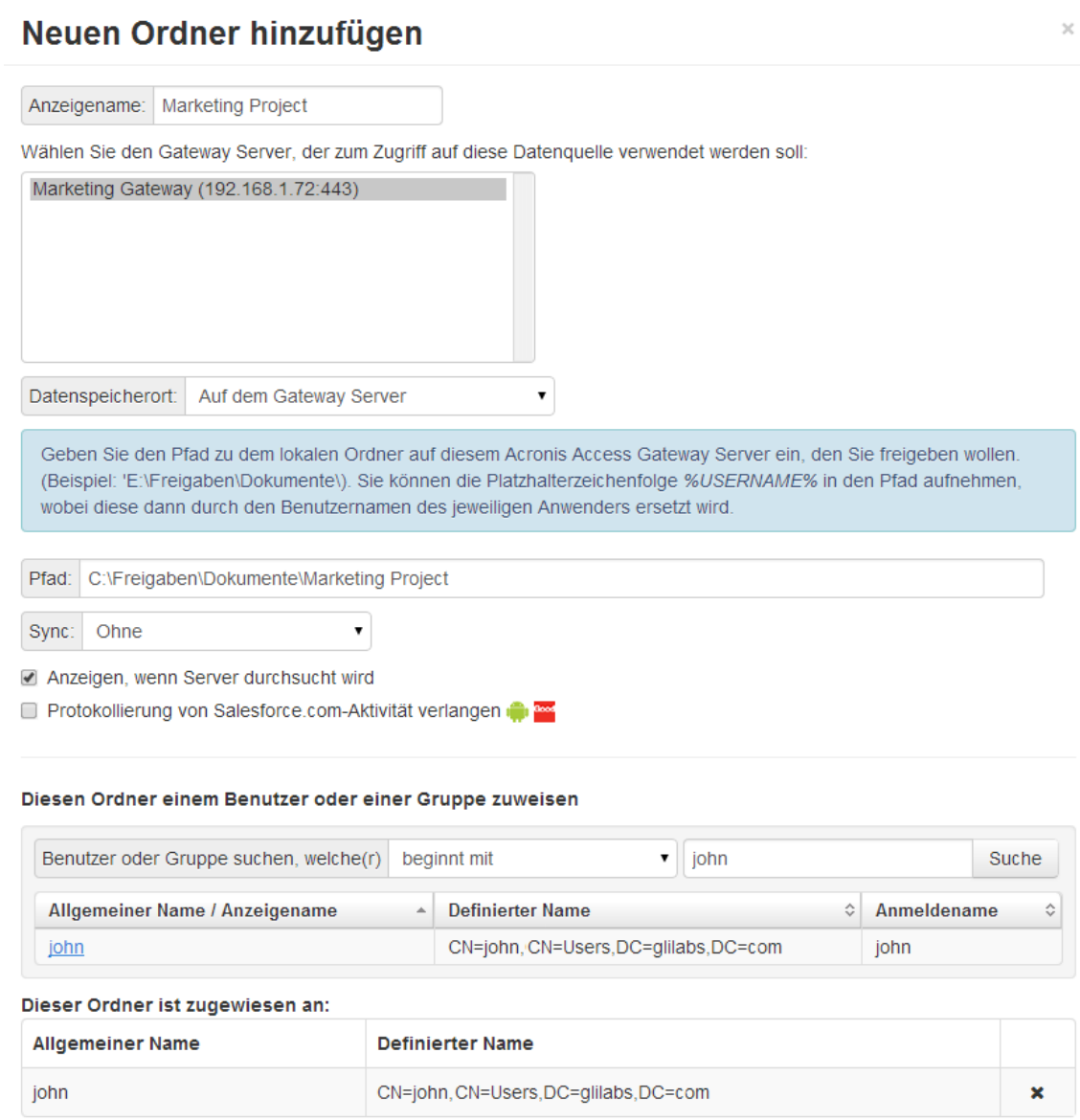

8. Geben Sie einen Anzeigenamen für den Gateway Server ein.
9. Geben Sie den DNS-Namen oder die IP-Adresse des Gateway Servers ein.

   ***Hinweis:*** *Wenn Ihre mobilen Clients über einen Reverse-Proxy-Server oder Loadbalancer mit dem Gateway verbunden werden, aktivieren Sie* ***Alternative Adresse für Client-Verbindungen verwenden*** *und geben Sie den DNS-Namen oder die IP-Adresse des Reverse-Proxy-Servers bzw. Loadbalancers ein.*

10. Geben Sie den **Administrationsschlüssel** ein.
11. Erlauben Sie bei Bedarf Verbindungen mit selbstsignierten Zertifikaten zu diesem Gateway. Aktivieren Sie dazu die Option **Verbindungen von Acronis Access Servern mit selbstsignierten Zertifikaten erlauben**.
12. Drücken Sie auf **Speichern**.

***Hinweis:*** *Stellen Sie sicher, dass mindestens ein Gateway Server verfügbar ist.*

**Datenquellen erstellen**




**So erstellen Sie eine Datenquelle:**

1. Öffnen Sie die Acronis Access Weboberfläche.
2. Öffnen Sie die Registerkarte **Mobiler Zugriff**.
3. Öffnen Sie die Registerkarte **Datenquellen**.
4. Wechseln Sie zu **Ordner**.
5. Klicken Sie auf die Schaltfläche **Neuen Ordner hinzufügen**.
6. Geben Sie einen Anzeigenamen für den Ordner ein.
7. Wählen Sie den Gateway-Server aus, über den der Zugriff auf diesen Ordner erfolgt.
8. Wählen Sie den Speicherort für die Daten. Dieser kann sich auf dem eigentlichen Gateway Server, auf einem anderen SMB-Server, auf einer SharePoint-Website oder -Bibliothek oder auf einem Sync & Share-Server befinden.

   ***Hinweis:*** *Wenn Sie Sync & Share auswählen, geben Sie den vollständigen Pfad zum Server mit der Port-Nummer ein, z. B.: https://mycompany.com:3000*

9. Geben Sie basierend auf dem gewählten Speicherort den Pfad zu diesem Ordner oder Server bzw. zu dieser Site oder Bibliothek ein.
10. Wählen Sie den **Synchronisierungstyp** dieses Ordners.
11. Aktivieren Sie **Anzeigen, wenn Server durchsucht wird**, wenn diese Datenquelle sichtbar sein soll, wenn mobile Acronis Access-Clients den Gateway Server durchsuchen.
12. Wählen Sie, ob der Ordner Protokollierung von Salesforce-Aktivität erfordert.
13. Wählen Sie den Benutzer oder die Gruppe aus, dem bzw. der Sie den Ordner zuweisen möchten.
14. Drücken Sie 'Speichern'.

## 3.3 Richtlinie einrichten

Um Benutzer im Client Management zu registrieren, müssen Sie eine Benutzer- oder Gruppenrichtlinie konfigurieren. Weitere Informationen finden Sie im Artikel Benutzer- und Gruppenrichtlinien.

**So fügen Sie eine neue Gruppenrichtlinie hinzu:**

1. Öffnen Sie die Registerkarte **Gruppenrichtlinien**.
2. Klicken Sie auf die Schaltfläche **Neue Richtlinie hinzufügen**, um eine neue Gruppenrichtlinie hinzuzufügen. Damit öffnen Sie die Seite **Eine neue Gruppenrichtlinie hinzufügen**.


3. Geben Sie im Feld **Gruppe suchen** den Active Directory-Gruppennamen, für den Sie eine Richtlinie erstellen möchten, ganz oder teilweise ein. Die Suche nach Active Directory-Gruppen können Sie mit den Einschränkungen '**beginnt mit**' oder '**enthält**' ausführen. Suchvorgänge mit der Einschränkung 'beginnt mit' sind viel schneller als solche mit 'enthält'.
4. Klicken Sie auf **Suchen** und klicken Sie in den aufgeführten Ergebnissen auf den gewünschten Gruppennamen.
5. Nehmen Sie die erforderlichen Konfigurationen auf den jeweiligen Registerkarten vor (Sicherheit, Applikation, Synchronisierung, Basisordner und Server) und drücken Sie **Speichern**.

**So fügen Sie eine neue Benutzerrichtlinie hinzu:**

1. Öffnen Sie die Registerkarte **Benutzerrichtlinien**.
2. Klicken Sie auf die Schaltfläche **Neue Richtlinie hinzufügen**, um eine neue Benutzerrichtlinie hinzuzufügen. Damit öffnen Sie die Seite **Eine neue Benutzerrichtlinie hinzufügen**.


3. Geben Sie im Feld **Benutzer suchen** den Active Directory-Benutzernamen, für den Sie eine Richtlinie erstellen möchten, ganz oder teilweise ein. Die Suche nach Active Directory-Benutzern können Sie mit den Einschränkungen '**beginnt mit**' oder '**enthält**' ausführen. Suchvorgänge mit der Einschränkung 'beginnt mit' sind viel schneller als solche mit 'enthält'.
4. Klicken Sie auf **Suche** und klicken Sie in den aufgeführten Ergebnissen auf den gewünschten Benutzernamen.
5. Nehmen Sie die erforderlichen Konfigurationen auf den jeweiligen Registerkarten vor (Sicherheit, Applikation, Synchronisierung, Basisordner und Server) und drücken Sie **Speichern**.

## 3.4 Die Access Mobile Client-Applikation installieren

1. Navigieren Sie im Apple oder Android App Store zu Acronis Access.
   - Besuchen Sie mit Ihrem iOS-Gerät den Apple App Store, und suchen Sie nach Acronis Access, oder folgen Sie diesem Link: http://www.grouplogic.com/web/meappstore
   - Besuchen Sie mit Ihrem Android-Gerät den Google Play Store, und suchen Sie nach Acronis Access, oder folgen Sie diesem Link: https://play.google.com/store/apps/details?id=com.grouplogic.mobilecho
2. Installieren Sie die Access Mobile Client-App, und klicken Sie darauf, um sie zu starten.

3. Tippen Sie im Begrüßungsbildschirm auf 'Weiter'.
   - Tippen Sie unter iOS auf das Symbol '+', um einen Server hinzuzufügen.
   - Öffnen Sie unter Android das Menü **Einstellungen** und tippen Sie auf **Server hinzufügen**.
4. Geben Sie den Servernamen oder die IP-Adresse des Servers ein, auf dem Sie den Acronis Access-Server oder den Gateway Server installiert haben. Sie können einen Anzeigenamen für diesen Server angeben, der in der Serverliste angezeigt wird.
5. Geben Sie den Namen eines Benutzers ein, der Zugriff auf den Gateway Server hat. <RPODUCT_NAME> regelt den Zugriff mithilfe von Standard-NTFS-Berechtigungen.
6. Schalten Sie **Kennwort speichern** auf EIN um, wenn Ihr Kennwort gespeichert werden soll. Geben Sie dann Ihr Kennwort ein und bestätigen Sie es.
7. Tippen Sie auf **Speichern**, um die Servereinstellungen zu übernehmen.
8. Tippen Sie auf den im linken Fensterbereich angezeigten Server, um eine Verbindung herzustellen und die verfügbaren Volumes zu durchsuchen.
9. Sämtliche Details zu den Einstellungen und Funktionen der Access Mobile Client-Applikation finden Sie auf der Seite Mobile Client.

## 3.5 Für das Client Management registrieren

Nach der Installation von Acronis Access mit aktiviertem Mobile Access haben Sie zwei Möglichkeiten den Access Mobile Client zu verwenden:

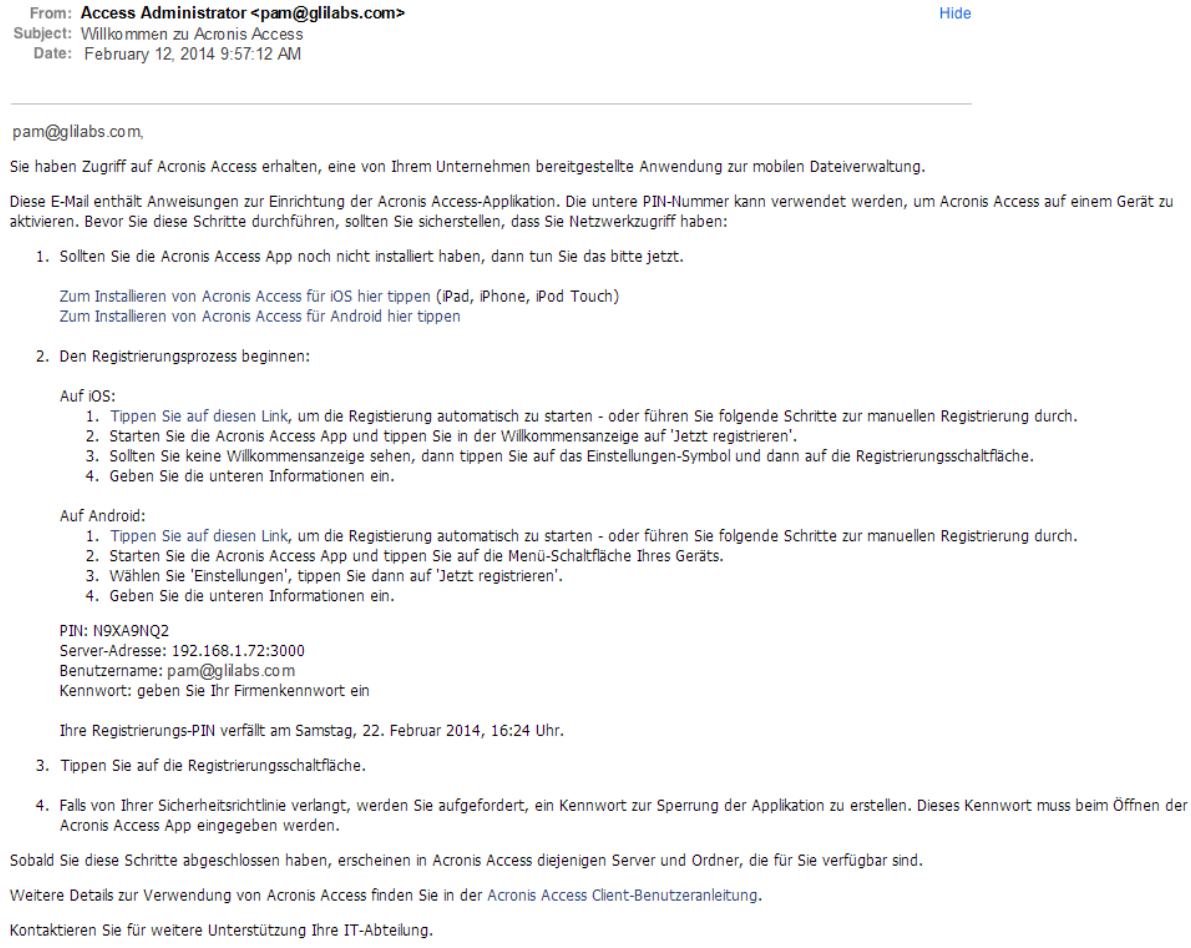
Wenn Ihre Organisation den Zugriff auf den Access Mobile Client und dessen Einstellungen zentral verwaltet, müssen Sie von der IT-Abteilung den Zugriff auf Acronis Access anfordern. Sobald Ihnen der Zugriff gewährt wurde, erhalten Sie eine Registrierungs-E-Mail. Diese E-Mail enthält Informationen und Anweisungen, die Sie für die Verwendung des Access Mobile Clients benötigen.

Wenn der Acronis Access-Server den Zugriff zulässt, ohne dass der Access Mobile Client zentral verwaltet wird, müssen Sie lediglich den Namen des Acronis Access-Servers sowie Ihren Benutzernamen und Ihr Kennwort eingeben, um zu beginnen.

Jeder Benutzer, dem eine Registrierungseinladung zur Verwaltung gesendet wurde, erhält eine E-Mail mit folgendem Inhalt:

- Link zur Installation des Access Mobile Clients über den Apple App Store
- Link zum Starten der Access Mobile Client-App und zum Automatisieren des Registrierungsprozesses
- Eine einmalige PIN-Nummer
- Die Adresse des Management-Servers

- Die E-Mail begleitet die Benutzer bei der Installation des Access Mobile Clients und der Eingabe der Registrierungsinformationen.



From: **Access Administrator <pam@glilabs.com>** Hide
Subject: Willkommen zu Acronis Access
Date: February 12, 2014 9:57:12 AM

pam@glilabs.com,

Sie haben Zugriff auf Acronis Access erhalten, eine von Ihrem Unternehmen bereitgestellte Anwendung zur mobilen Dateiverwaltung.

Diese E-Mail enthält Anweisungen zur Einrichtung der Acronis Access-Applikation. Die untere PIN-Nummer kann verwendet werden, um Acronis Access auf einem Gerät zu aktivieren. Bevor Sie diese Schritte durchführen, sollten Sie sicherstellen, dass Sie Netzwerkzugriff haben:

1. Sollten Sie die Acronis Access App noch nicht installiert haben, dann tun Sie das bitte jetzt.

   Zum Installieren von Acronis Access für iOS hier tippen (iPad, iPhone, iPod Touch)
   Zum Installieren von Acronis Access für Android hier tippen

2. Den Registrierungsprozess beginnen:

   Auf iOS:
   1. Tippen Sie auf diesen Link, um die Registierung automatisch zu starten - oder führen Sie folgende Schritte zur manuellen Registrierung durch.
   2. Starten Sie die Acronis Access App und tippen Sie in der Willkommensanzeige auf 'Jetzt registrieren'.
   3. Sollten Sie keine Willkommensanzeige sehen, dann tippen Sie auf das Einstellungen-Symbol und dann auf die Registrierungsschaltfläche.
   4. Geben Sie die unteren Informationen ein.

   Auf Android:
   1. Tippen Sie auf diesen Link, um die Registierung automatisch zu starten - oder führen Sie folgende Schritte zur manuellen Registrierung durch.
   2. Starten Sie die Acronis Access App und tippen Sie auf die Menü-Schaltfläche Ihres Geräts.
   3. Wählen Sie 'Einstellungen', tippen Sie dann auf 'Jetzt registrieren'.
   4. Geben Sie die unteren Informationen ein.

   PIN: N9XA9NQ2
   Server-Adresse: 192.168.1.72:3000
   Benutzername: pam@glilabs.com
   Kennwort: geben Sie Ihr Firmenkennwort ein

   Ihre Registrierungs-PIN verfällt am Samstag, 22. Februar 2014, 16:24 Uhr.

3. Tippen Sie auf die Registrierungsschaltfläche.

4. Falls von Ihrer Sicherheitsrichtlinie verlangt, werden Sie aufgefordert, ein Kennwort zur Sperrung der Applikation zu erstellen. Dieses Kennwort muss beim Öffnen der Acronis Access App eingegeben werden.

Sobald Sie diese Schritte abgeschlossen haben, erscheinen in Acronis Access diejenigen Server und Ordner, die für Sie verfügbar sind.

Weitere Details zur Verwendung von Acronis Access finden Sie in der Acronis Access Client-Benutzeranleitung.

Kontaktieren Sie für weitere Unterstützung Ihre IT-Abteilung.

Wenn die Access Mobile Client-App bereits installiert wurde und der Benutzer auf die Option 'Tippen Sie auf diesen Link, um die Registrierung automatisch zu starten...' klickt, während er diese E-Mail auf seinem Gerät sieht, wird Acronis Access automatisch gestartet, und das Registrierungsformular wird angezeigt. Die Server-Adresse, PIN-Nummer und der Benutzername des Benutzers sind ebenfalls in dieser URL kodiert, daher werden diese Felder im Registrierungsformular automatisch ausgefüllt. Zu diesem Zeitpunkt muss der Benutzer lediglich sein Kennwort eingaben, um den Registrierungsvorgang abzuschließen.

Der erforderliche Benutzername und das Kennwort sind der Active Directory-Benutzername und das Active Directory-Kennwort des Benutzers. Diese Anmeldedaten dienen dazu, die Benutzer der richtigen Benutzer- oder Gruppenverwaltungsrichtlinie zuzuordnen, den Zugriff auf Gateway-Server zu ermöglichen und die Anmeldedaten für Acronis Access-Server-Anmeldungen zu speichern, falls die Verwaltungsrichtlinie der Benutzer dies zulässt.

Wenn die Verwaltungsrichtlinie ein Kennwort zur Sperrung der Applikation verlangt, werden die Benutzer aufgefordert, das Kennwort einzugeben. Alle Anforderungen bezüglich der Komplexität von Kennwörtern in der Richtlinie des Benutzers werden für dieses erstmalige Kennwort sowie für jede zukünftige Änderung des Kennworts zur Sperrung der Applikation erzwungen.

Wenn die Richtlinie die lokale Speicherung von Dateien auf dem Gerät des Benutzers einschränkt, wird dieser gewarnt, dass bestehende Dateien gelöscht werden. Er erhält die Möglichkeit, den Management-Einrichtungsvorgang abzubrechen, um diese Dateien anderweitig zu speichern, bevor sie entfernt werden.

### So erfolgt die Registrierung für die Verwaltung

#### Automatisch per Registrierungs-E-Mail registrieren

1. Öffnen Sie die Ihnen vom IT-Administrator gesendete E-Mail, und tippen Sie auf den Link **Zum Installieren von Acronis Access hier tippen**, wenn Sie Acronis Access noch nicht installiert haben.
2. Sobald Acronis Access installiert ist, kehren Sie zur Einladungs-E-Mail auf Ihrem Gerät zurück, und tippen Sie auf **Tippen Sie auf diesen Link, um die Registrierung automatisch zu starten** in Schritt 2 der E-Mail.
3. Ein Registrierungsformular wird angezeigt. Falls Sie den Registrierungsvorgang über den Link in der Einladungs-E-Mail gestartet haben, werden die Felder für Serveradresse, PIN und Benutzername automatisch ausgefüllt.

   ***Hinweis:*** *Falls Ihr Server keine PIN erfordert, wird dieses Feld im Registrierungsformular nicht angezeigt.*

4. Geben Sie Ihr Kennwort ein, und tippen Sie auf **Jetzt registrieren**, um fortzufahren.

   ***Hinweis:*** *Benutzername und Kennwort entsprechen Ihrem standardmäßigen Unternehmens-Benutzernamen und -Kennwort. Dies sind wahrscheinlich die gleichen Angaben, die Sie auch zum Anmelden bei Ihrem Computer oder E-Mail-Konto verwenden.*

5. Tippen Sie nach dem Ausfüllen des gesamten Formulars auf die Schaltfläche **Registrieren**.
6. Abhängig von der Konfiguration Ihres Unternehmensservers werden Sie unter Umständen gewarnt, dass das Sicherheitszertifikat des Management Servers nicht vertrauenswürdig ist. Um diese Warnung zu akzeptieren und fortzufahren, können Sie auf **Immer fortsetzen** klicken.
7. Wenn für die Access Mobile Client-App ein Kennwort zum Sperren der Applikation erforderlich ist, werden Sie aufgefordert, eines festzulegen. Möglicherweise gelten auch Anforderungen bezüglich der Komplexität des Kennworts. Diese werden gegebenenfalls angezeigt.
8. Wenn Ihre Verwaltungsrichtlinie das Speichern von Dateien in Acronis Access einschränkt oder Sie daran hindert, einzelne Server über die Access Mobile Client-App hinzuzufügen, wird möglicherweise ein Bestätigungsfenster angezeigt. Wenn Sie in der Access Mobile Client-App Dateien lokal gespeichert haben, werden Sie aufgefordert zu bestätigen, dass Dateien im lokalen Dateispeicher **Meine Dateien** gelöscht werden. Wenn Sie hier 'Nein' wählen, wird der Verwaltungsregistrierungsvorgang abgebrochen und Ihre Dateien bleiben unverändert.

#### Manuelle Registrierung

1. Öffnen Sie die Acronis Access-App.
2. Öffnen Sie **Einstellungen**.
3. Tippen Sie auf **Registrieren**.

4. Geben Sie Ihre Serveradresse, Ihre PIN (falls erforderlich), Benutzernamen und Kennwort ein.
5. Tippen Sie nach dem Ausfüllen des gesamten Formulars auf die Schaltfläche **Registrieren**.
6. Abhängig von der Konfiguration Ihres Unternehmensservers werden Sie unter Umständen gewarnt, dass das Sicherheitszertifikat des Management Servers nicht vertrauenswürdig ist. Um diese Warnung zu akzeptieren und fortzufahren, können Sie auf **Immer fortsetzen** klicken.
7. Wenn für die Access Mobile Client-App ein Kennwort zum Sperren der Applikation erforderlich ist, werden Sie aufgefordert, eines festzulegen. Möglicherweise gelten auch Anforderungen bezüglich der Komplexität des Kennworts. Diese werden gegebenenfalls angezeigt.

Wenn Ihre Verwaltungsrichtlinie das Speichern von Dateien in Acronis Access einschränkt oder Sie daran hindert, einzelne Server über die Access Mobile Client-App hinzuzufügen, wird möglicherweise ein Bestätigungsfenster angezeigt. Wenn Sie in der Access Mobile Client-App Dateien lokal gespeichert haben, werden Sie aufgefordert zu bestätigen, dass Dateien im lokalen Dateispeicher **Meine Dateien** gelöscht werden. Wenn Sie hier 'Nein' wählen, wird der Verwaltungsregistrierungsvorgang abgebrochen und Ihre Dateien bleiben unverändert.

### Fortlaufende Management-Updates

Nach der Ersteinrichtung der Verwaltung versuchen Access Mobile Clients bei jedem Start der Client-App, eine Verbindung zum Management Server herzustellen. Jegliche Änderungen der Einstellungen, von Server- oder Ordnerzuordnungen, Resets des Kennworts zur Sperrung der Applikation oder Remote-Löschungen werden zu diesem Zeitpunkt von der Client-App akzeptiert.

***Anforderungen bezüglich der Verbindung zum Client Management***

*Access Mobile Clients benötigen Netzwerkzugriff auf den Management Server, um Profilaktualisierungen, Remote-Kennwortzurücksetzungen und Remote-Löschungen zu empfangen. Falls Ihr Client eine Verbindung zu einem VPN herstellen muss, bevor er Zugriff auf Acronis Access Gateway Server erhält, so wird diese Verbindung zum VPN auch benötigt, bevor Verwaltungsbefehle akzeptiert werden.*

### Verwaltung entfernen

Es gibt zwei Optionen zum Entfernen des Access Mobile Clients aus der Verwaltung:

- Deaktivieren der Option 'Verwaltung verwenden' (falls Ihre Richtlinie dies zulässt)
- Entfernen der Access Mobile Client-Applikation

Je nach Ihren Richtlinien für die Acronis Access-Verwaltung haben Sie eventuell das Recht, den Access Mobile Client aus der Verwaltung zu entfernen. Dies hat zur Folge, dass Sie nicht mehr auf die Dateiserver des Unternehmens zugreifen können. Wenn Ihr Verwaltungsprofil es zulässt, befolgen Sie diese Schritte, um die Verwaltung Ihres Geräts aufzuheben:

**Zum Aufheben der Verwaltung für das Gerät führen Sie die nachstehenden Schritte aus:**

1. Tippen Sie auf das Menü **Einstellungen**.
2. Deaktivieren Sie die Option **Verwaltung verwenden**.

3. Ihr Profil verlangt möglicherweise, Ihre Access Mobile Client-Daten zu löschen, wenn Sie das Gerät aus der Verwaltung entfernen. Sie können den Vorgang hier abbrechen, wenn Sie das Löschen der Daten verhindern möchten.
4. Bestätigen Sie das Entfernen von Acronis Access aus der Verwaltung, indem Sie im Bestätigungsfenster auf **JA** tippen.

***Hinweis**: Wenn Ihr Acronis Access-Verwaltungsprofil das Entfernen Ihres Clients aus der Verwaltung nicht zulässt, wird die Option **Verwaltung verwenden** im Menü **Einstellungen** nicht angezeigt. In diesem Fall können Sie das Gerät nur aus der Verwaltung entfernen, indem Sie die Access Mobile Client-Applikation deinstallieren. Durch Deinstallieren der Applikation werden alle Access Mobile Client-Daten und -Einstellungen gelöscht, und der Benutzer verfügt nach der erneuten Installation wieder über die Standardeinstellungen für die Applikation.*

**Führen Sie die folgenden Schritte aus, um die Access Mobile Client-App zu deinstallieren:**

1. Setzen Sie einen Finger auf das Symbol der Access Mobile Client-App, bis es sich zu bewegen beginnt.
2. Tippen Sie auf die Schaltfläche '**X**' in der Access Mobile Client-Applikation, und bestätigen Sie den Deinstallationsvorgang.

Um die Access Mobile Client-App neu zu installieren, besuchen Sie http://www.grouplogic.com/web/meappstore

# 4 Schnellstart: Sync & Share

Diese Anleitung enthält die wesentlichen Schritte zum Einrichten von Sync & Share, zum Verwenden der Weboberfläche für den Zugriff auf Dateien und zum Verwenden des Acronis Access-Desktop-Clients. Ausführlichere Informationen über die Konfiguration dieser Komponenten erhalten Sie in den Abschnitten Sync & Share und Desktop-Client.

**Themen**



## 4.1 Erster Durchlauf

Wenn Sie es nicht bereits erledigt haben, installieren und konfigurieren Sie Acronis Access. Weitere Informationen hierzu finden Sie in den Abschnitten zur Installation (S. 4) und zum Konfigurationswerkzeug (S. 10).

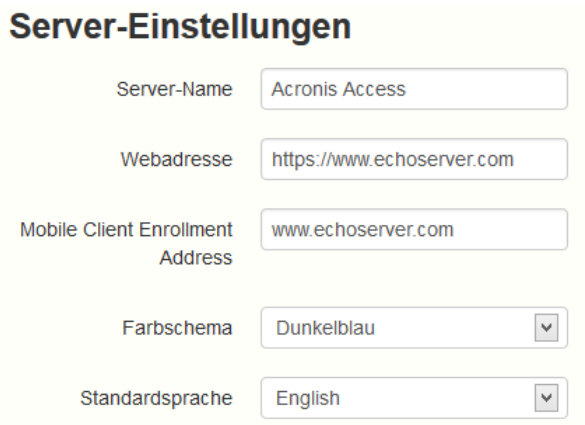
Wenn Sie die Weboberfläche erstmals verwenden, müssen Sie ein Kennwort für das Standardadministratorkonto eingeben. Nach der Anmeldung wird dann der **Installationsassistent** aufgerufen.

***Warnung!*** *Merken Sie sich das Administratorkennwort gut, denn der Support kann dieses Kennwort nicht wiederherstellen.*

***Hinweis:*** *Es kann 30 - 45 Sekunden dauern, bis die Applikation zur Verfügung steht, nachdem Sie sie über das Konfigurationswerkzeug gestartet haben.*

Sobald Sie die oben genannten Schritte abgeschlossen haben, können Sie die unten beschriebene Erstkonfiguration ausführen.

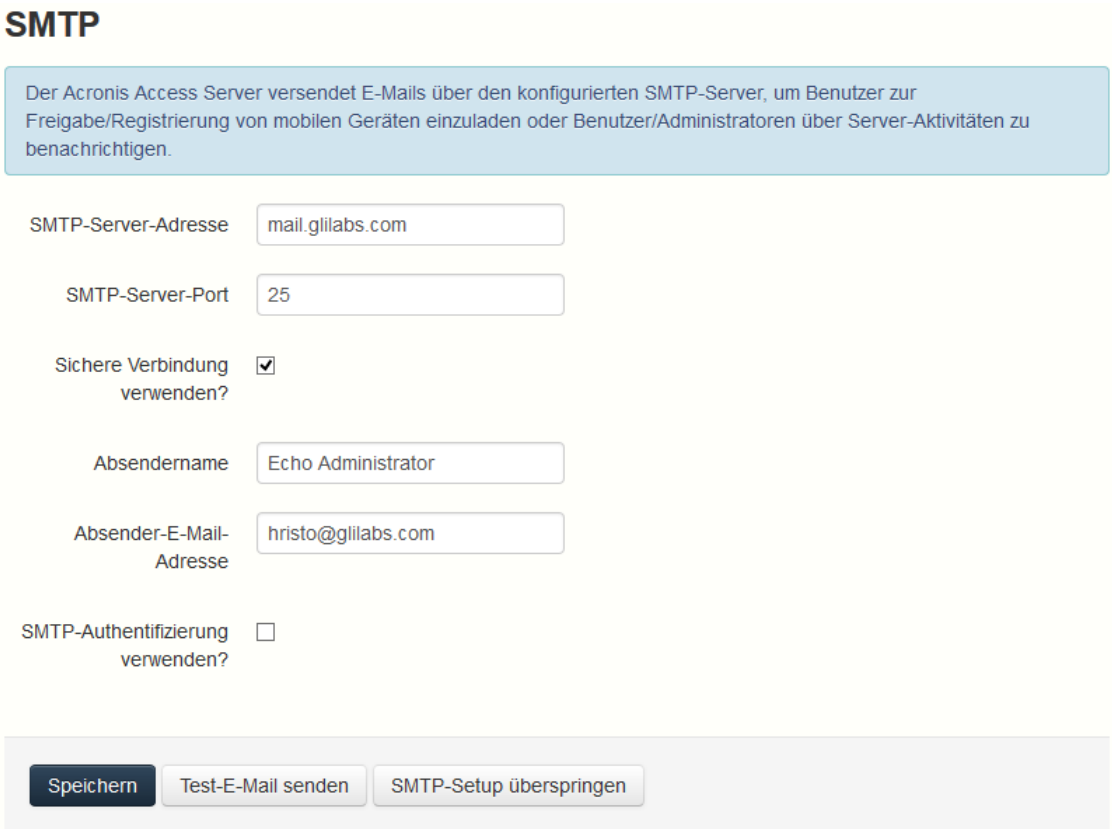
**Allgemeine Einstellungen**




1. Geben Sie einen Servernamen ein.
2. Geben Sie den DNS-Stammnamen oder die IP-Adresse ein, über den bzw. die Benutzer auf die Website zugreifen (beginnend mit http:// oder https://).

3. Geben Sie den DNS-Namen oder die IP-Adresse an, über den bzw. die sich mobile Benutzer registrieren.
4. Wählen Sie ein Farbschema aus. Die derzeit verfügbaren Optionen sind Grau, Violett, Cappuccino, Blau, Dunkelblau und Orange.
5. Wählen Sie die Standardsprache für das **Überwachungsprotokoll** aus. Die derzeit verfügbaren Optionen sind Englisch, Deutsch, Französisch und Japanisch.
6. Klicken Sie auf **Speichern**.

**SMTP**

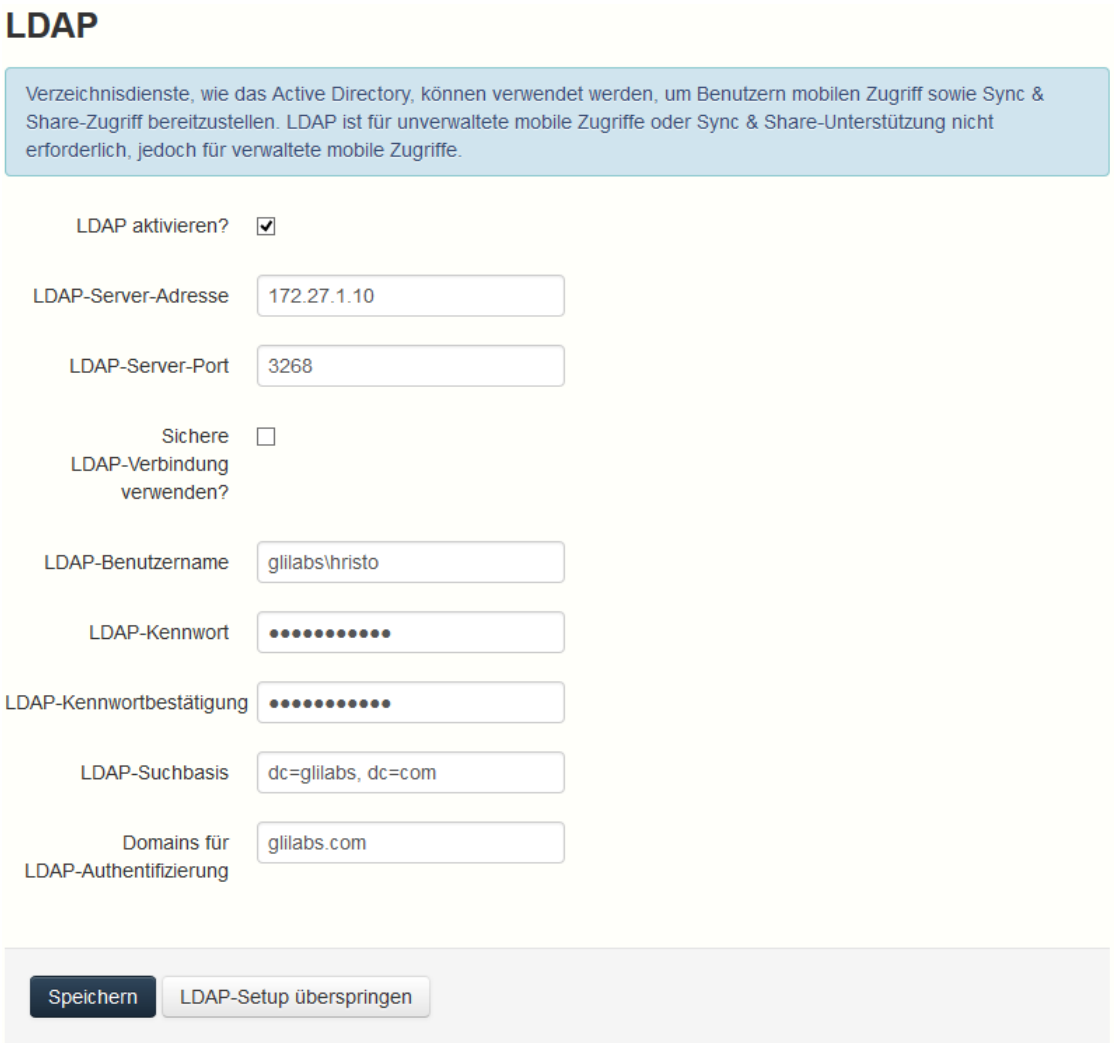



***Hinweis:*** *Sie können diesen Abschnitt überspringen und SMTP später konfigurieren.*

1. Geben Sie den DNS-Namen oder die IP-Adresse des SMTP-Servers ein.
2. Geben Sie den SMTP-Port des Servers ein.
3. Wenn Sie keine Zertifikate für den SMTP-Server verwenden, deaktivieren Sie **Sichere Verbindung verwenden?**.
4. Geben Sie den Namen ein, der in der 'Von'-Zeile von E-Mails angezeigt wird, die vom Server gesendet werden.
5. Geben Sie die Adresse ein, die als Absender der vom Server gesendeten E-Mails verwendet wird.
6. Falls Sie für den SMTP-Server eine Authentifizierung per Benutzername/Kennwort verwenden, aktivieren Sie **SMTP-Authentifizierung verwenden?**, und geben Sie Ihre Anmeldedaten ein.

7. Klicken Sie auf **Test-E-Mail senden**, um eine Test-E-Mail an die in Schritt 5 festgelegte Adresse zu senden.
8. Klicken Sie auf **Speichern**.

**LDAP**




***Hinweis:*** *Sie können diesen Abschnitt überspringen und LDAP später konfigurieren.*

1. Markieren Sie **LDAP aktivieren**.
2. Geben Sie den DNS-Namen oder die IP-Adresse des LDAP-Servers ein.
3. Geben Sie den Port des LDAP-Servers ein.
4. Falls Sie ein Zertifikat für Verbindungen mit dem LDAP-Server verwenden, markieren Sie **Sichere LDAP-Verbindung verwenden**.
5. Geben Sie Ihre LDAP-Anmeldedaten einschließlich der Domain ein (z.B. acronis\hristo).
6. Geben Sie die LDAP-Suchbasis ein.
7. Geben Sie die gewünschte(n) Domain(s) für die LDAP-Authentifizierung ein. (Für ein Konto mit der E-Mail-Adresse **joe@glilabs.com** würden Sie zur LDAP-Authentifizierung beispielsweise **glilabs.com** eingeben.)
8. Klicken Sie auf **Speichern**.

**Lokaler Gateway Server**


***Hinweis:*** *Wenn Sie einen Gateway Server und den Acronis Access Server auf derselben Maschine installieren, wird der Gateway Server automatisch erkannt und vom Acronis Access Server verwaltet. Sie werden aufgefordert, den DNS-Namen oder die IP-Adresse festzulegen, unter dem bzw. der der lokale Gateway Server für die Clients erreichbar ist. Diese Adresse können Sie später ändern.*

1. Legen Sie einen DNS-Namen oder eine IP-Adresse für den lokalen Gateway Server fest.
2. Klicken Sie auf **Speichern**.

## 4.2 Weboberfläche zum Zugriff auf Dateien verwenden

### Öffnen Sie den Acronis Access Web-Client.

1. Starten Sie den Webbrowser und navigieren Sie zu: https://meinserver https://myserver, wobei **meinserver** die URL oder IP-Adresse des Computers ist, auf dem der Acronis Access Server ausgeführt wird.


2. Melden Sie sich mit Ihren Anmeldedaten an.
   a. Falls nur der Acronis Access Server installiert ist, melden Sie sich als **administrator** mit dem Kennwort an, das Sie nach der Installation festgelegt haben. Wenn Sie die Weboberfläche zum ersten Mal öffnen, werden Sie aufgefordert, das Kennwort jetzt festzulegen.

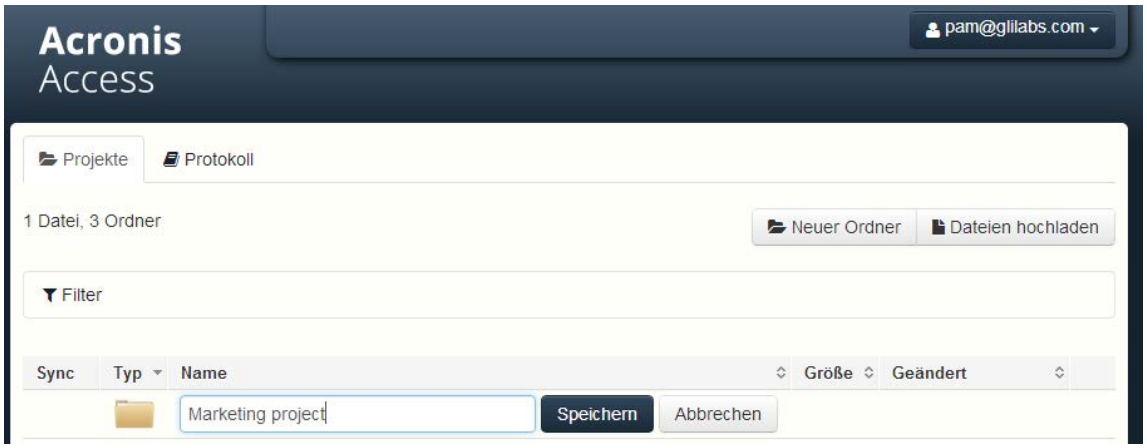
b. Falls Sie eine E-Mail-Einladung für Acronis Access erhalten haben, müssen Sie zu diesem Zeitpunkt möglicherweise **Ihr persönliches Kennwort** festlegen oder sich mit Ihren Active Directory-Anmeldedaten anmelden.

c. Falls Ihr Acronis Access Server zur Verwendung von Active Directory für die Authentifizierung und Bereitstellung von Benutzerkonten konfiguriert wurde, sollten Sie in der Lage sein, sich mit gültigen Netzwerkangaben für das Netzwerk anzumelden.

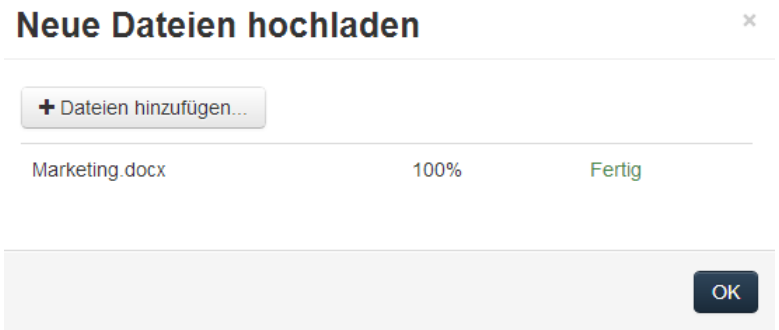
3. Wenn Sie als Administrator angemeldet sind, müssen Sie den Administrationsmodus verlassen, um den Web-Client zu verwenden.
   - Klicken Sie hierzu einfach auf die Schaltfläche **Administration verlassen** oben rechts.

## Ordner erstellen und Dateien hochladen

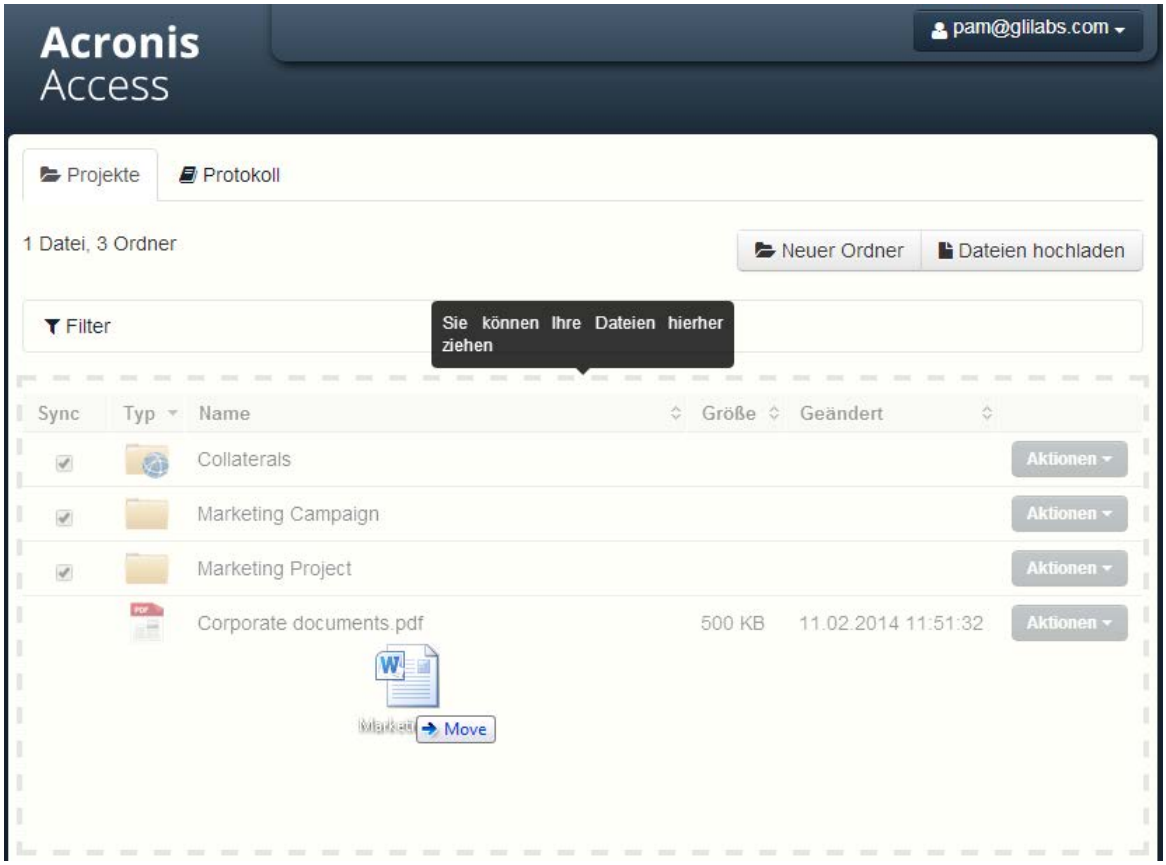
1. Klicken Sie auf die Schaltfläche **Ordner erstellen** und geben Sie einen Namen für den neuen Ordner ein. In diesem Beispiel verwenden wir **Marketing-Projekt**. Drücken Sie **Speichern**.




2. Navigieren Sie zu dem neuen Ordner durch Klicken auf seinen Namen.
3. Klicken Sie auf **Dateien hochladen**, dann auf **Dateien hinzufügen...** und wählen Sie mindestens eine Datei auf dem Computer aus.

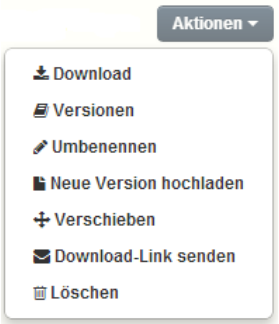


4. Die Dateien werden in den Ordner hochgeladen, in dem Sie sich befinden. Drücken Sie **OK**.
5. Alternativ können Dateien auch durch Ziehen und Ablegen auf der Webseite hochgeladen werden.




## Datei- und Ordneraktionen

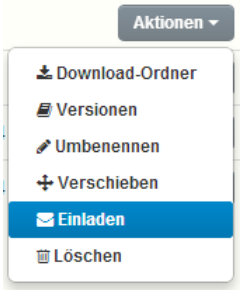
1. Beachten Sie die Schaltfläche **Aktionen**, die neben jeder Datei und jedem Ordner angezeigt wird. Durch Klicken darauf zeigen Sie die möglichen Aktionen und Informationen zu dem Element an, einschließlich des Zugriffs auf frühere Versionen derselben Datei.



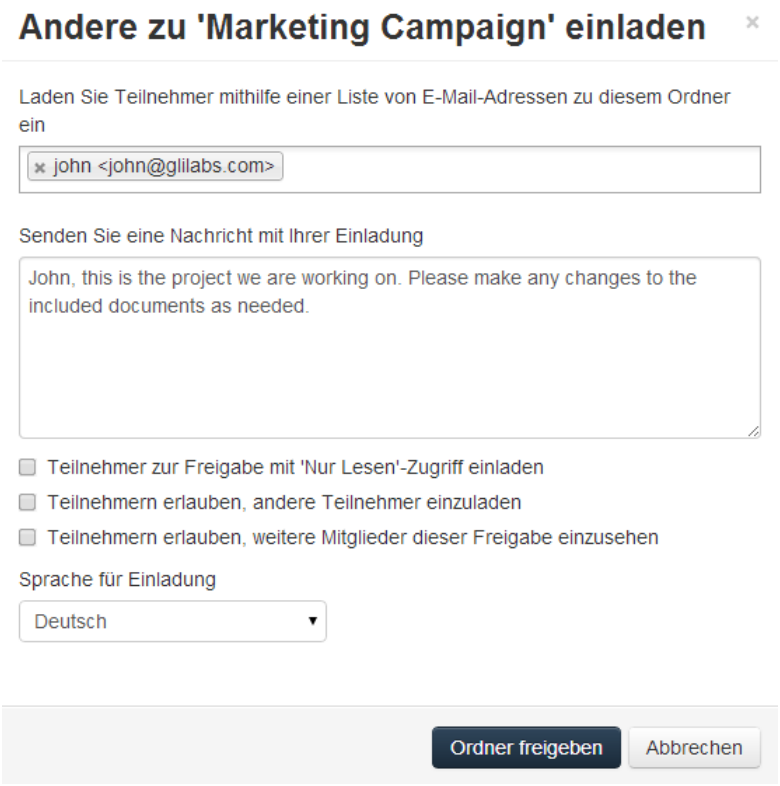

2. Wenn Sie diese oder eine andere Datei herunterladen möchten, klicken Sie einfach auf ihren Namen. Alternativ können Sie auf die Schaltfläche **Aktionen** und dann auf **Download** klicken.

***Hinweis:*** *Stellen Sie bei Nutzung von Internet Explorer sicher, dass die Option* ***Verschlüsselte Seiten nicht auf dem Datenträger speichern*** *deaktiviert ist, damit Sie Dateien herunterladen können. Öffnen Sie dazu* ***Internetoptionen*** *>* ***Erweitert*** *>* ***Sicherheit****.*

3. Nun können Sie einen Ordner für einen Kollegen oder Geschäftspartner freigeben. Klicken Sie auf **Projekte**, dann auf die Schaltfläche **Aktionen** für den freizugebenden Ordner und anschließend auf **Einladen**.

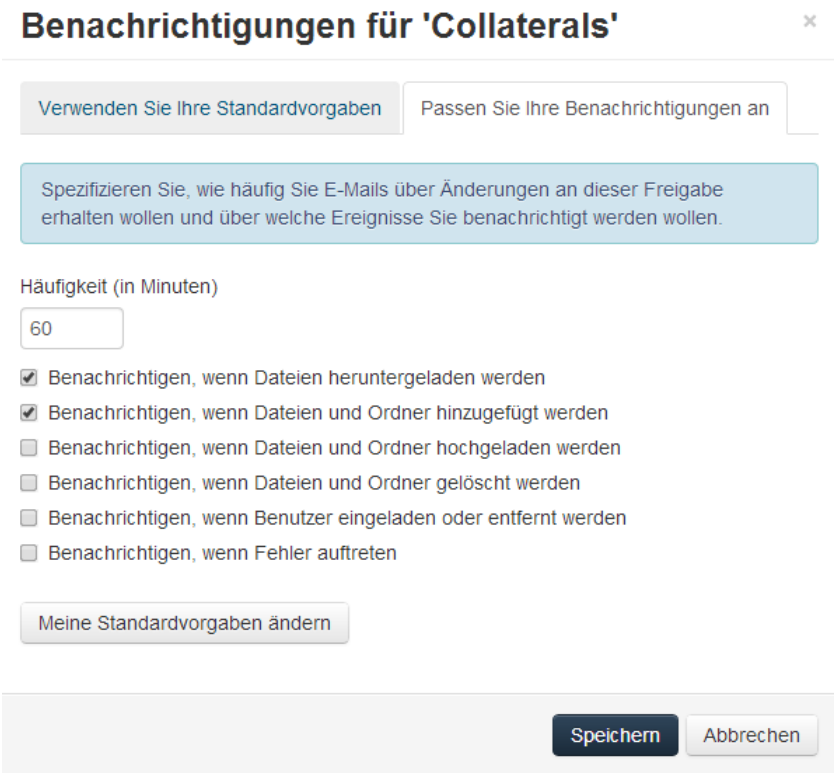



4. Geben Sie im Dialogfeld **Andere einladen** eine E-Mail-Adresse und eine entsprechende Textnachricht ein. Eine E-Mail mit Ihren Informationen und Zugriffsanweisungen wird generiert und an den Empfänger gesendet.



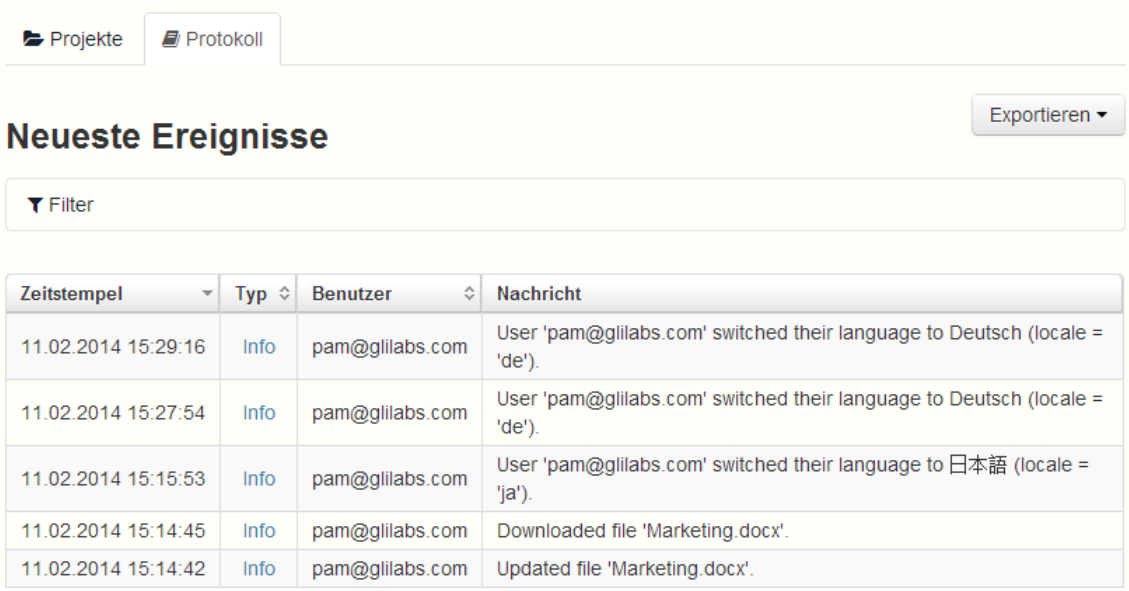

***Hinweis:*** *Falls das Kontrollkästchen* ***Teilnehmer zum Freigeben mit Nur-Lesen-Zugriff einladen*** *aktiviert ist, können eingeladene Benutzer die im freigegebenen Ordner enthaltenen Dokumente nur mit Lesezugriff herunterladen.*

5. Sie können E-Mail-Benachrichtigungen für Ordner abonnieren, die für Sie freigegeben wurden. Dazu klicken Sie einfach auf die Schaltfläche **Aktionen** für den betreffenden freigegebenen Ordner und dann auf **Benachrichtigungen**.

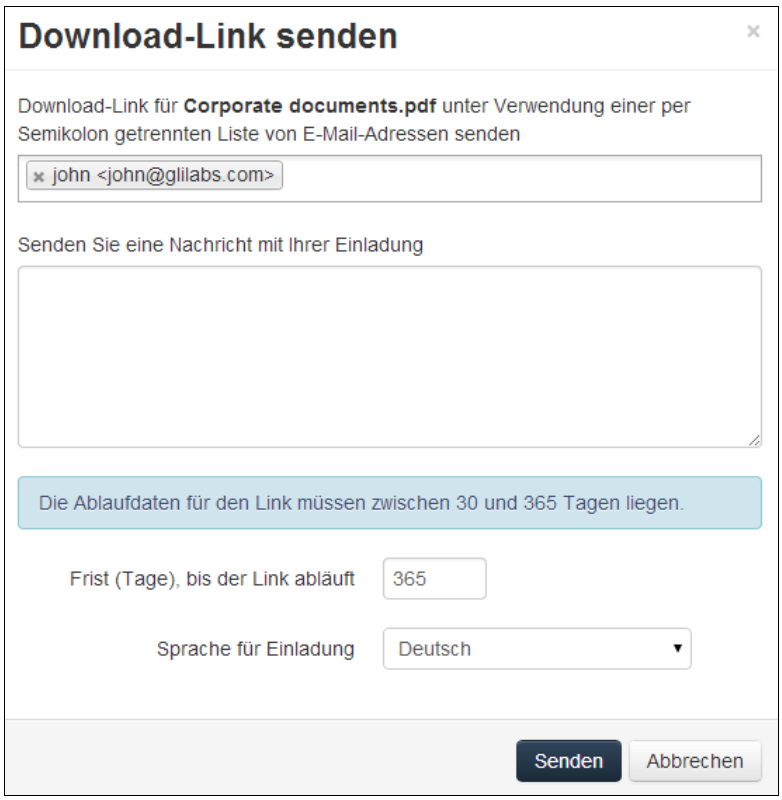



## Überwachungsprotokollierung

Sie können auch den Verlauf der Ereignisse nachverfolgen, indem Sie auf die Registerkarte **Log** klicken. Es sind Such- und Filteroptionen verfügbar. Sie können die Ergebnisse als XML-, CSV- oder Textdateien exportieren.



## Eine einzelne Datei freigeben




***Hinweis:*** *Falls Sie eine Datei oder einen Ordner freigeben möchten, die bzw. den ein anderer Benutzer für Sie freigegeben hat, benötigen Sie die Berechtigungen, andere Benutzer zu dieser Freigabe einzuladen. Falls Sie nicht zum Einladen anderer Benutzer berechtigt sind, können Sie die Dateien und Ordner nicht für einen anderen Benutzer freigeben. Die Option* ***Download-Link senden*** *im Menü „Aktionen“ ist dann ebenfalls nicht sichtbar.*

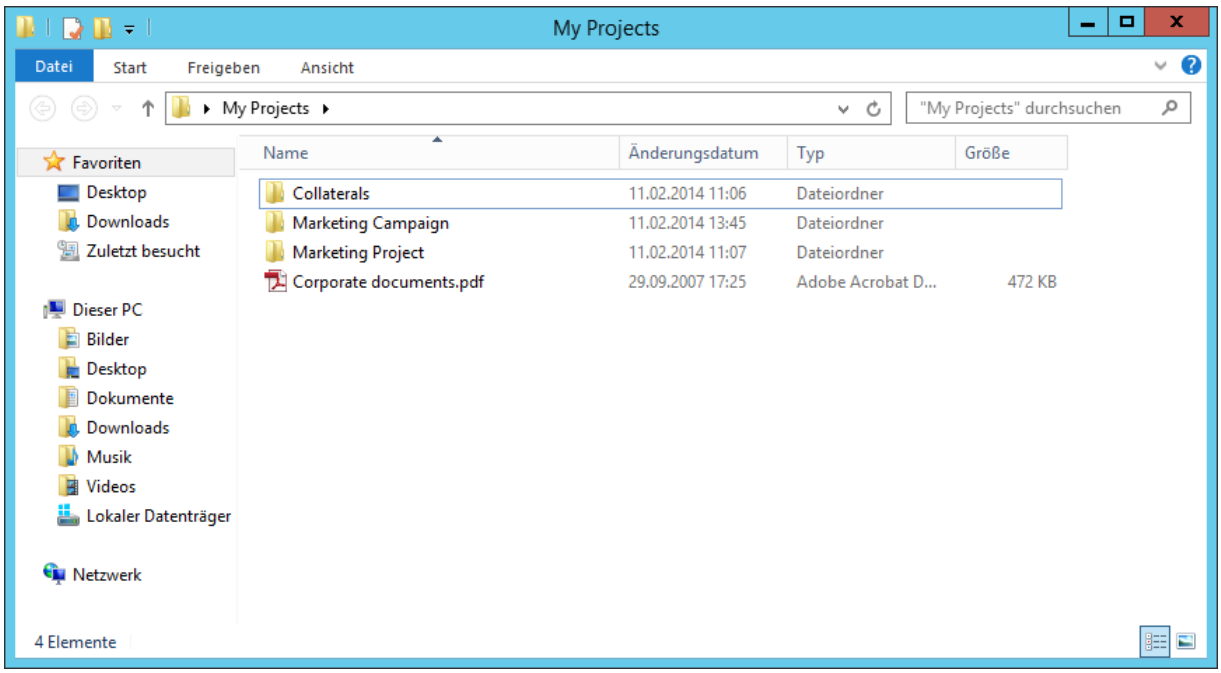
1. Rufen Sie die Acronis Access Weboberfläche auf.
2. Wenn Sie sich mit einem Administratorkonto angemeldet haben, drücken Sie in der oberen rechten Ecke **Administration verlassen**.
3. Drücken Sie dann für die Datei, die Sie freigeben möchten, die Schaltfläche **Aktionen**.
4. Drücken Sie **Download-Link senden**.
5. Geben Sie die E-Mail-Adressen der Benutzer ein, an die Sie den Download-Link senden möchten.
6. Geben Sie die Ablauffrist des Links an.
7. Wählen Sie die Sprache der E-Mail.
8. Drücken Sie **Senden**.

## 4.3 Den Desktop-Client verwenden

**Erste Schritte**

***Hinweis:*** *Wenn Sie den Acronis Access-Desktop-Client noch nicht installiert haben, folgen Sie der Anleitung Client-Installation und -Konfiguration.*

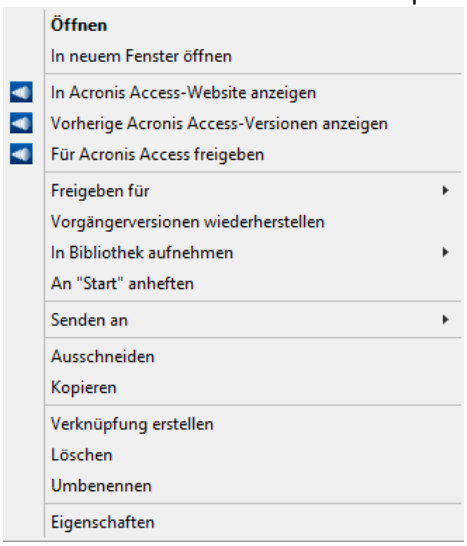
1. Öffnen Sie den Ordner, den Sie während des Konfigurationsvorgangs für die Synchronisierung ausgewählt hatten. Dies ist ein ganz normaler Ordner; weisen Sie ihm also einen ganz normalen Namen und nicht 'Sync-Ordner' zu. In diesem Beispiel hat er den Namen **Meine Projekte**.
2. Erstellen Sie in **Meine Projekte** einen Ordner mit dem Namen **Marketing-Kampagne**.
3. Erstellen Sie in **Meine Projekte** ein Textdokument, geben Sie Text darin ein und speichern und schließen Sie das Dokument.
4. Erstellen Sie einen weiteren Ordner in **Meine Projekte** mit dem Namen **Werbematerialien**.



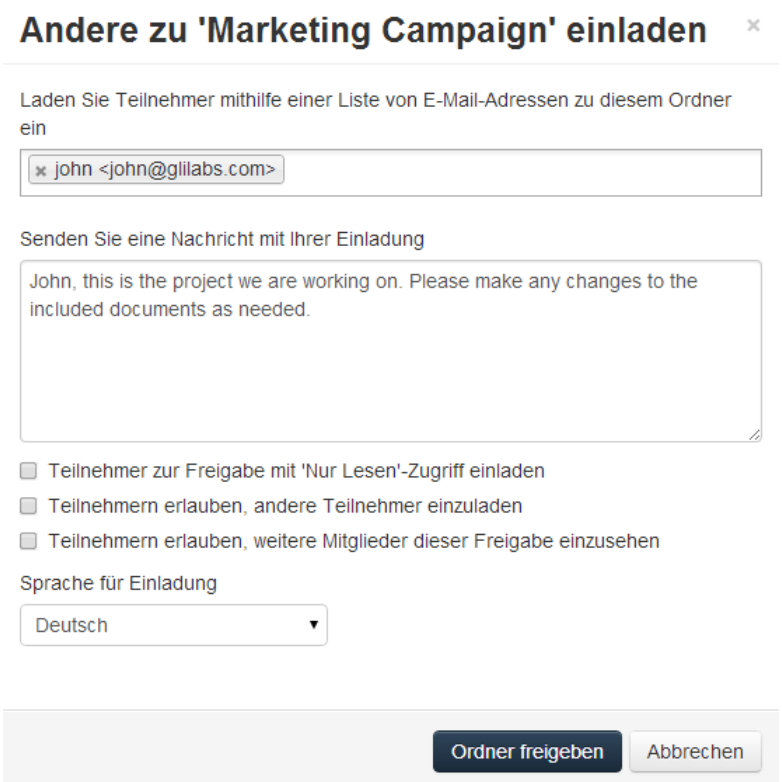

5. Legen Sie einige Dateien darin ab, indem Sie sie von Ihrem Computer kopieren.
6. Nun können Sie einen Ordner für einen Kollegen freigeben. Hierbei sind zwei unterschiedliche Methoden möglich: direkt über Windows Explorer oder mithilfe Ihres Webbrowsers. Führen Sie Schritt 7 aus, um Inhalte von Ihrem Desktop über Windows Explorer freizugeben, oder befolgen Sie Schritt 8, um Inhalte über Ihren bevorzugten Webbrowser freizugeben.

   ***Hinweis:*** *Sie können auch eine einzelne Datei freigeben. Dies wird am Ende dieses Artikels beschrieben.*

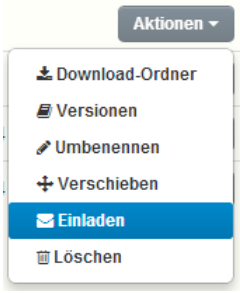
7. Wenn Sie dies direkt vom Desktop aus erledigen möchten, wählen Sie den Ordner **Marketing-Kampagne** aus.
   a. Klicken Sie mit der rechten Maustaste darauf.
   b. Wählen Sie im Kontextmenü die Option **Für Acronis Access freigeben**



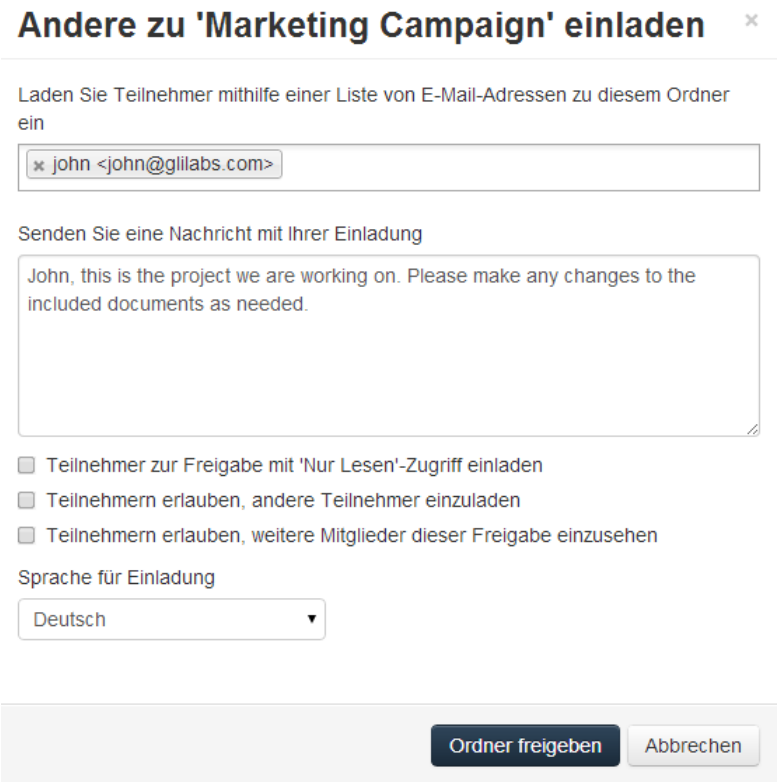

   c. Dadurch wird ein Webbrowser gestartet und das Dialogfeld 'Einladen' angezeigt.
   d. Geben Sie im Dialogfeld **Andere einladen** eine E-Mail-Adresse und eine entsprechende Textnachricht ein.



8. Wenn Sie lieber Ihren Webbrowser verwenden, öffnen Sie https://server.com/ https://server.com/, wobei **server.com** die Adresse des Acronis Access Servers ist, und melden Sie sich mit Ihrem Benutzernamen und Kennwort an.
   a. Wechseln Sie zur Seite **Projekte**, und suchen Sie nach dem Ordner **Marketing-Kampagne**.
   b. Klicken Sie auf die Schaltfläche **Aktionen** neben dem Ordner **Marketing-Kampagne**, und klicken Sie dann auf **Einladen**.




   c. Geben Sie im Dialogfeld **Andere einladen** eine E-Mail-Adresse und eine entsprechende Textnachricht ein.




9. Unabhängig von der zum Einladen einer Person verwendeten Methode, erhält der Empfänger eine oder zwei E-Mails. Dies hängt davon ab, ob es sich um einen internen (Active Directory) oder externen Benutzer handelt.
   1. Für einen externen Benutzer enthält die erste E-Mail mit dem Betreff **Sie wurden zu Acronis Access eingeladen** einen Link zum Festlegen eines persönlichen Kennworts.
   2. Die zweite E-Mail mit dem Betreff **Sie haben Zugriff auf die Marketing-Kampagne erhalten** enthält Ihre Nachricht und einen Link zum Zugriff auf die freigegebenen Dateien.

10. Sobald der eingeladene Benutzer auf den Link zum Zugriff auf das System (und gegebenenfalls zum Festlegen seines Kennworts) klickt, erhalten Sie und Ihr Kollege gemeinsamen Zugriff auf die Dateien im Ordner **Marketing-Kampagne**.

Informieren Sie Ihren Kollegen über den Desktop-Client, damit Sie Dateien auf Ihren Computern automatisch synchronisieren können.

***Hinweis:*** *Die maximale Pfadlänge ist bei Mac OS X und Windows unterschiedlich, was bei plattformübergreifenden Bereitstellungen zu Synchronisierungsfehlern führen kann. Bei Windows gilt eine vom Betriebssystem auferlegte Beschränkung von 260 Zeichen (MAX_PATH) für den gesamten Pfad, einschließlich des Teils '**`C:\myshare folder\`**'. Bei Windows ist also die maximale Länge des Dateinamens 260 - [Pfadlänge des freigegebenen Ordners] - 1 (für NULL-Abschlusszeichen).*

*Beispiel: Der Benutzer gibt den Ordner C:\meine_freigegebenen_dokumente frei und versucht, eine Datei in C:\meine_freigegebenen_dokumente\dies_ist_ein_ordner\ herunterzuladen. Die maximale Länge des Dateinamens für dieses Unterverzeichnis wäre 260 - 53 - 1 = 206 Zeichen. Unter Mac OS X ist die Länge auf maximal 1024 Zeichen beschränkt.*

## Eine einzelne Datei freigeben


***Hinweis:*** *Falls Sie eine Datei oder einen Ordner freigeben möchten, die bzw. den ein anderer Benutzer für Sie freigegeben hat, benötigen Sie die Berechtigungen, andere Benutzer zu dieser Freigabe einzuladen. Falls Sie nicht zum Einladen anderer Benutzer berechtigt sind, können Sie die Dateien und Ordner nicht für einen anderen Benutzer freigeben. Die Option **Download-Link senden** im Menü „Aktionen“ ist dann ebenfalls nicht sichtbar.*

1. Rufen Sie die Acronis Access Weboberfläche auf.
2. Wenn Sie sich mit einem Administratorkonto angemeldet haben, drücken Sie in der oberen rechten Ecke **Administration verlassen**.

3. Drücken Sie dann für die Datei, die Sie freigeben möchten, die Schaltfläche **Aktionen**.
4. Drücken Sie **Download-Link senden**.
5. Geben Sie die E-Mail-Adressen der Benutzer ein, an die Sie den Download-Link senden möchten.
6. Geben Sie die Ablauffrist des Links an.
7. Wählen Sie die Sprache der E-Mail.
8. Drücken Sie **Senden**.