Acronis Access

Administratoranleitung

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 Mobiler Zugriff

Dieser Bereich der Weboberfläche enthält alle Einstellungen und Konfigurationen, die Benutzer mobiler Geräte betreffen.

Themen

1.1 Begrifflichkeiten

Access Mobile Clients stellen eine direkte Verbindung mit Ihrem Server her, und verwenden keinen Drittanbieterdienst, sodass Sie die Kontrolle behalten. Acronis Access Server können auf vorhandenen Dateiservern installiert werden, wodurch iPads, iPhones und Android-Geräte Zugriff auf die Dateien auf dem Server haben. Dies sind in der Regel dieselben Dateien, die bereits für PCs zur Verfügung stehen, die die Windows Dateifreigabefunktion nutzen, und für Mac-Computer, die ExtremeZ-IP File Server verwenden.

Clients greifen über ihr Active Directory-Benutzerkonto auf Acronis Access Server zu. In Acronis Access müssen keine zusätzlichen Konten konfiguriert werden. Der Access Mobile Client unterstützt auch den Dateizugriff mithilfe lokaler Computerkonten, die auf dem Windows-Server konfiguriert sind, auf dem Acronis Access ausgeführt wird. Diese Möglichkeit können Sie nutzen, wenn Sie Nicht-AD-Benutzern den Zugriff ermöglichen möchten. Für die im Folgenden beschriebenen Funktionen zur Client-Verwaltung sind AD-Benutzerkonten erforderlich.

Eine minimale Bereitstellung besteht aus einem einzigen Windows-Server, auf dem eine Standardinstallation von Acronis Access ausgeführt wird. Diese Standardinstallation umfasst die Acronis Access Server-Komponente sowie die Installation des lokalen Acronis Access Gateway Servers mit einer Lizenz. In diesem Szenario können Geräte, auf denen die Access Mobile Client-Applikation ausgeführt wird, eine Verbindung mit diesem einzigen Dateiserver herstellen, und es können Clients verwaltet werden. Wenn keine Client-Verwaltung erforderlich ist, können Datenquellen auf dem lokalen Gateway Server eingerichtet werden. Die Access Mobile Clients können auf diese Datenquellen zugreifen, die Benutzer haben jedoch die Kontrolle über ihre App-Einstellungen.

Abb 1. Einzelner Gateway Server, viele Access Mobile Clients

Dem Netzwerk können später beliebig viele Gateway Server hinzugefügt und für den Zugriff über die Client-App konfiguriert werden.

Hinweis: *Einzelheiten zur Installation von Acronis Access finden Sie im Bereich Installation dieser Anleitung. Die Konfiguration von Gateway Servern und Datenquellen wird im Bereich Mobiler Zugriff (S. 6) erläutert.*

Wenn Sie die Access Mobile Clients remote verwalten möchten, können Sie mit dem Acronis Access Client Management Richtlinien jeweils pro Active Directory-Benutzer oder -Gruppe erstellen. Über diese Richtlinien können Sie:

- Allgemeine Einstellungen der Applikation konfigurieren
- Server, Ordner und Basisverzeichnisse zuweisen, die in der Client-App angezeigt werden sollen
- Mit Dateien durchführbare Aktionen einschränken
- Andere Fremdanbieter-Apps einschränken, in denen Access Mobile Client-Dateien geöffnet werden können
- Sicherheitseinstellungen festlegen (Häufigkeit der Anmeldung beim Server, Kennwort zum Sperren der Applikation usw.)
- Die Möglichkeit zum Speichern von Dateien auf dem Gerät deaktivieren
- Die Möglichkeit zum Einbeziehen von Access Mobile Client-Dateien in iTunes-Backups deaktivieren
- Kennwörter von Benutzern zum Sperren der Applikation remote zurücksetzen
- Eine Remote-Löschung der lokalen Daten und Einstellungen der Access Mobile Client-App ausführen
- Und viele weitere Konfigurations- und Sicherheitsoptionen

Nur ein Acronis Access Server ist erforderlich.

Eine typische netzwerkbasierte Client-Verwaltung besteht aus einem Server, auf dem die Komponenten Acronis Access Server und Acronis Access Gateway Server installiert sind, sowie einigen weiteren Gateway Servern, die als Dateiserver fungieren. In diesem Szenario werden alle mobilen Clients für die Verwaltung mit dem Acronis Access Server konfiguriert. Die Clients kontaktieren diesen Server bei jedem Start der Access Mobile Client-Applikation, um festzustellen, ob

Einstellungen geändert wurden, und um Zurücksetzungen des Kennworts zum Sperren der Applikation sowie Befehle für Remote-Löschungen ggf. zu bestätigen.

Access Mobile Client-Clients können in ihrer Verwaltungsrichtlinie eine Liste von Servern, bestimmte Ordner in freigegebenen Volumes und Basisverzeichnisse zugewiesen werden. Diese Ressourcen werden in der Access Mobile Client-App automatisch angezeigt, und diese Server werden von der Client-App je nach Dateizugriff direkt kontaktiert.

Hinweis: *Einzelheiten zum Aktivieren und Konfigurieren der Client-Verwaltung finden Sie in dieser Anleitung in den Bereichen Richtlinien (S. 8) und Mobile Geröte verwalten (S. 35).*

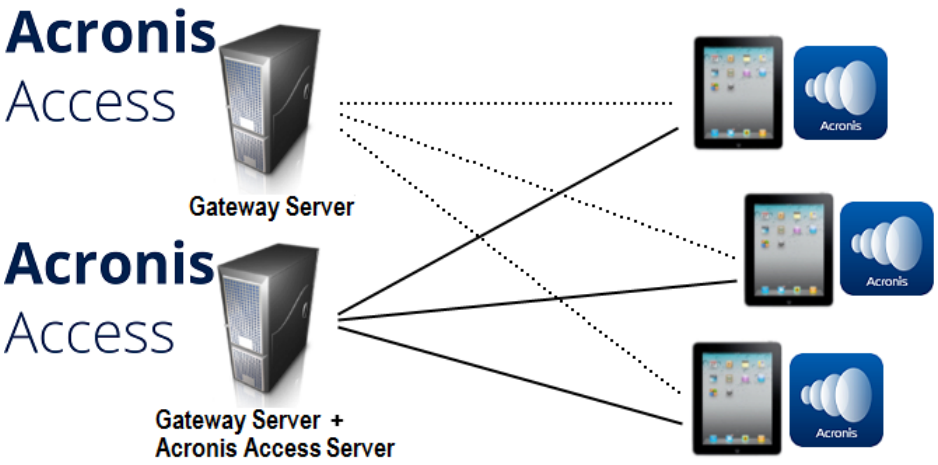


Abb. 2. Ein Gateway Server, ein Gateway Server + Acronis Access Server, viele Clients

1.2 Richtlinien

Themen

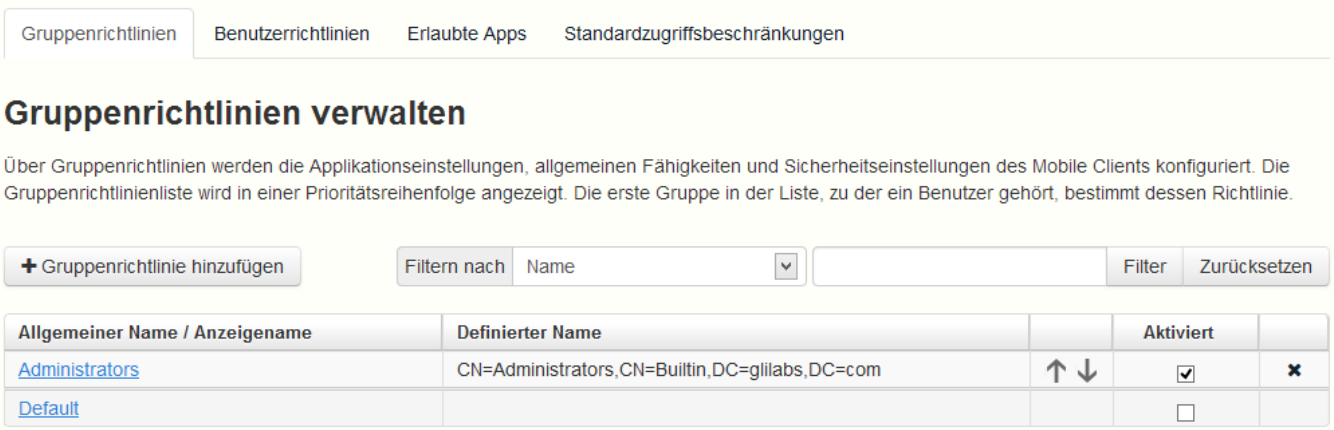
1.2.1 Benutzer- und Gruppenrichtlinien

Acronis Access Client Management ermöglicht die Zuweisung von Profilen zu Active Directory-Gruppen. Gruppenrichtlinien erfüllen normalerweise die meisten oder alle Anforderungen der Client-Verwaltung. Die Gruppenrichtlinienliste wird in der Reihenfolge der Priorität angezeigt, d.h., die erste Gruppe in der Liste besitzt die höchste Priorität. Wenn Benutzer den Acronis Access-Server kontaktieren, werden ihre Einstellungen durch die einzelne Gruppenrichtlinie mit der höchsten Priorität bestimmt, deren Mitglied sie sind.

Benutzerrichtlinien werden verwendet, wenn Sie bestimmte Einstellungen für einen Benutzer erzwingen möchten, egal welcher Gruppe er zugehört, da Benutzerrichtlinien eine höhere Priorität als Gruppenrichtlinien haben. Durch Benutzerrichtlinien werden alle Gruppenrichtlinien überschrieben.

Tipps zur Gruppenverwaltung

*Wenn Sie möchten, dass für alle oder die meisten Ihrer Benutzer die gleichen Richtlinieneinstellungen gelten, können Sie die **Standard**-Gruppenrichtlinie aktivieren. Wenn dies aktiviert ist, werden alle Benutzer, die nicht Mitglieder einer Gruppenrichtlinie sind und für die keine spezifische Gruppenrichtlinie gilt, Mitglieder der **Standard**-Gruppe. Die **Standard**-Gruppe ist standardmäßig deaktiviert. Wenn Sie einer Gruppe von Benutzern den Zugriff auf die Acronis Access-Verwaltung verweigern möchten, stellen Sie sicher, dass sie keine Mitglieder konfigurierter Gruppenrichtlinien sind. Solange ein Benutzerkonto keinen Gruppenrichtlinien entspricht, wird ihm die Möglichkeit der Registrierung bei der Acronis Access-Client-Verwaltung verweigert.*



Themen

1.2.1.1 Eine neue Richtlinie hinzufügen

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 (S. 14), Applikation (S. 16), Synchronisierung (S. 19), Basisordner (S. 20) und Server (S. 21)) 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 (S. 14), Applikation (S. 16), Synchronisierung (S. 19), Basisordner (S. 20) und Server (S. 21)) und drücken Sie **Speichern**.

1.2.1.2 Ausnahmen für Richtlinieneinstellungen

Bei Benutzern, welche die Apps **Access Mobile Client für Android, Access Mobile Client für Good Dynamics** (iOS) und **Access Mobile Client mit Mobile Iron AppConnect** ausführen, gibt es einige Ausnahmen in Bezug auf die Anwendung von Acronis Access-Verwaltungsrichtlinien auf die Access Mobile Client-App. Im Fall von Android werden einige Funktionen des iOS-Clients nicht unterstützt, sodass die entsprechenden Richtlinien nicht angewendet werden. Bei Good Dynamics werden einige der standardmäßigen Access Mobile Client-Richtlinienfunktionen auf das Good Dynamics-System und den Good Dynamics-Richtliniensatz übertragen, den Sie auf dem Good Control-Server konfiguriert haben. Bei MobileIron werden einige der standardmäßigen Acronis Access-Richtlinienfunktionen auf die MobileIron AppConnect-Plattform übertragen. Diese Ausnahmen werden auf den Seiten zur

Acronis Access-Richtlinienkonfiguration vermerkt. Weitere Details zu den einzelnen Richtlinienausnahmen werden angezeigt, wenn Sie den Mauszeiger über das Logo von Good, Android oder Mobilelron führen.

1.2.1.3 Richtlinien ändern

Bestehende Richtlinien können jederzeit geändert werden. Änderungen an Richtlinien werden auf die entsprechenden Access Mobile Client-Benutzer angewendet, sobald sie die mobile App wieder starten.

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.

So ändern Sie eine Gruppenrichtlinie:

1. Klicken Sie in der oberen Menüleiste auf **Gruppenrichtlinien**.
2. Klicken Sie auf die Gruppe, die Sie ändern möchten.
3. Nehmen Sie die erforderlichen Änderungen auf der Seite **Gruppenrichtlinie bearbeiten** vor und drücken Sie **Speichern**.
4. Um eine Richtlinie vorübergehend zu deaktivieren, entfernen Sie das Häkchen im Kontrollkästchen in der Spalte **Aktiviert** für die gewünschte Gruppe. Diese Änderung tritt sofort in Kraft.
5. Zum Ändern der Priorität einer Gruppe klicken Sie in der Liste 'Gruppenprofile verwalten' auf die Pfeiltaste nach oben oder unten. Dadurch wird das Profil um eine Ebene nach oben oder unten verschoben.

So ändern Sie eine Benutzerrichtlinie:

1. Rufen Sie die Registerkarte **Benutzerrichtlinien** auf.
2. Klicken Sie auf den Benutzer, den Sie ändern möchten.
3. Nehmen Sie die erforderlichen Änderungen auf der Seite **Benutzerrichtlinie bearbeiten** vor und drücken Sie **Speichern**.
4. Um eine Richtlinie vorübergehend zu deaktivieren, entfernen Sie das Häkchen im Kontrollkästchen in der Spalte **Aktiviert** für den gewünschten Benutzer. Diese Änderung tritt sofort in Kraft.

1.2.1.4 Erstellen einer Liste mit blockierten Pfaden

Sie können Blacklists für Pfade erstellen, die Benutzer von mobilen Geräten nicht selbst bereitstellen sollen. Diese Listen müssen einer Benutzer- oder Gruppenrichtlinie zugewiesen werden und sind nur für selbst bereitgestellte Pfade gültig. Wenn die Liste erstellt und den entsprechenden Benutzern und/oder Gruppen zugewiesen wurde, müssen Sie **Zugriff auf bestimmte Netzwerkpfade blockieren** für jede Benutzer-/Gruppenrichtlinie aktivieren, für die dies gelten soll.

So erstellen Sie eine Liste:

1. Öffnen Sie die Weboberfläche als Administrator.
2. Öffnen Sie die Seite Richtlinien (S. 8).
3. Klicken Sie auf die gewünschte Benutzer- oder Gruppenrichtlinie.
4. Öffnen Sie die Registerkarte Server-Richtlinie (S. 21).
5. Aktivieren Sie das Kontrollkästchen **Zugriff auf bestimmte Netzwerkpfade blockieren**.

   Hinweis: *Sie müssen diesen Schritt für jede Benutzer-/Gruppenrichtlinie durchführen, die Sie der Blacklist hinzufügen möchten.*

6. Drücken Sie **Listen hinzufügen/bearbeiten**.
7. Drücken Sie **Liste hinzufügen** auf der Seite **Liste mit blockierten Pfaden**.
8. Geben Sie einen Namen für die Liste ein.
9. Geben Sie einen Pfad oder eine Liste von Pfaden ein, die der Blacklist hinzugefügt werden. Jeder Eintrag sollte sich in einer neuen Zeile befinden.
10. Öffnen Sie die Registerkarte **Auf Benutzer oder Gruppen anwenden**.
11. Weisen Sie die Liste den gewünschten Benutzern/Gruppen zu.
12. Drücken Sie **Speichern**.

So aktivieren Sie die Blacklist für eine Benutzer- oder Gruppenrichtlinie:

1. Öffnen Sie die Weboberfläche als Administrator.
2. Öffnen Sie die Seite Richtlinien (S. 8).
3. Klicken Sie auf die gewünschte Benutzer- oder Gruppenrichtlinie.
4. Öffnen Sie die Registerkarte Server-Richtlinie (S. 21).
5. Aktivieren Sie das Kontrollkästchen **Zugriff auf bestimmte Netzwerkpfade blockieren**.

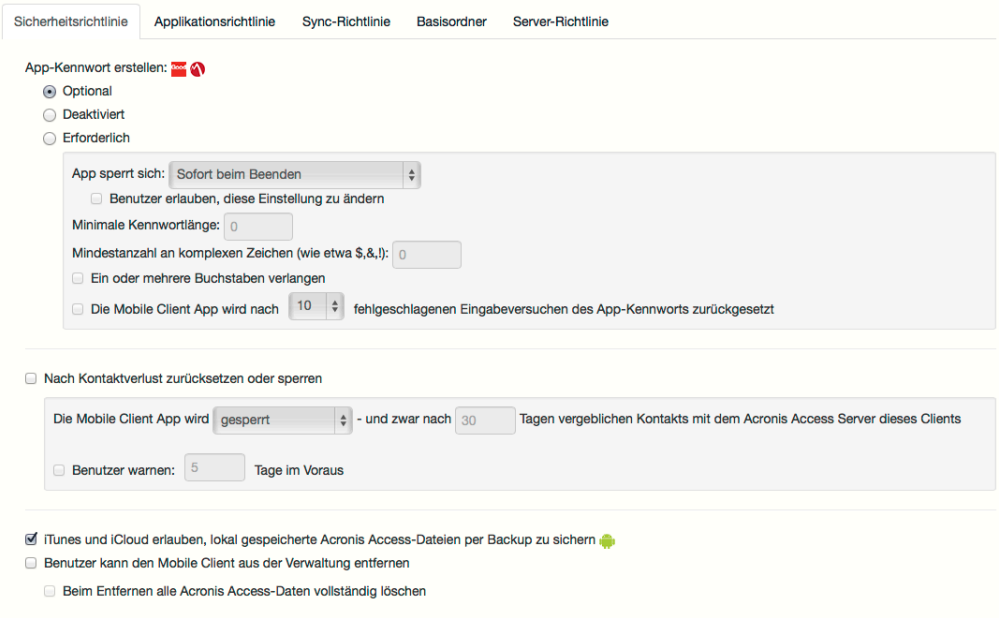
   Hinweis: *Sie müssen diesen Schritt für jede Benutzer-/Gruppenrichtlinie durchführen, die Sie der Blacklist hinzufügen möchten.*

6. Wählen Sie die gewünschte Liste aus dem Drop-down-Menü aus.

   Hinweis: *Wenn Sie **Listen aktualisieren** drücken, werden die Optionen im Drop-down-Menü aktualisiert.*

7. Drücken Sie **Speichern**, um zu speichern und die Richtlinie zu verlassen.

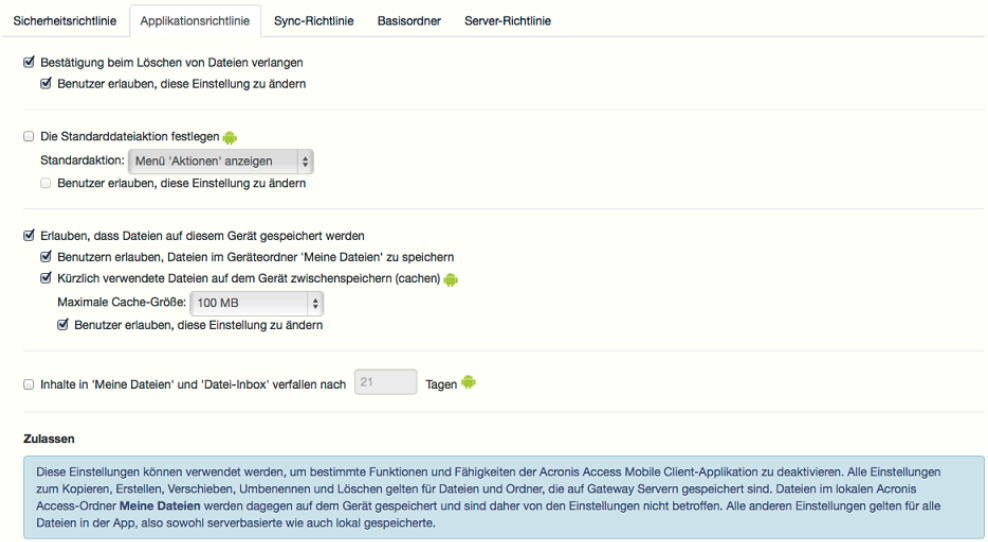
1.2.1.5 Sicherheitsrichtlinie



- **App-Kennwort erstellen** – Für die Access Mobile Client-Applikation kann ein Sperrkennwort festgelegt werden, das beim Starten der Applikation zuvor eingegeben werden muss.
  - **Optional** – Diese Einstellung zwingt die Benutzer nicht zur Konfiguration eines Kennworts zum Sperren der Applikation, sie können jedoch ein Kennwort im Menü **Einstellungen** in der App festlegen, falls sie dies wünschen.
  - **Deaktiviert** – Mit dieser Einstellung wird die Möglichkeit zur Konfiguration eines Kennworts zum Sperren der Applikation im Menü **Einstellungen** in der App deaktiviert. Dies ist eventuell sinnvoll bei gemeinsam genutzten mobilen Geräten, bei denen Sie verhindern möchten, dass ein Benutzer ein Kennwort festlegt und den Access Mobile Client auf diese Weise für andere Benutzer sperrt.
  - **Erforderlich** – Wenn diese Option aktiviert ist, muss der Benutzer ein Sperrkennwort für die Applikation festlegen, wenn er nicht bereits eines besitzt. Die optionalen Komplexitätsanforderungen für das Kennwort sowie die Einstellungen für das Löschen nach falscher Kennworteingabe werden erst aktiviert, wenn für **App-Kennwort erstellen** die Option **Erforderlich** ausgewählt wurde.
    - **App-Sperrung** – Über diese Option kann die Übergangsphase für die Kennworteingabe festgelegt werden. Wenn ein Benutzer vom Access Mobile Client zu einer anderen Applikation auf dem Gerät wechselt und vor dem Verstreichen dieser Übergangsphase zum Access Mobile Client zurückkehrt, muss er das Kennwort zum Sperren der Applikation nicht eingeben. Wenn Sie möchten, dass das Kennwort immer eingegeben werden muss, wählen Sie **Sofort nach Verlassen** aus. Wenn der Benutzer in der Lage sein soll, die Einstellung **App sperrt sich** in den Access Mobile Client-Einstellungen zu ändern, wählen Sie **Benutzer erlauben, diese Einstellung zu ändern**.
    - **Minimale Kennwortlänge** – Die erforderliche Mindestlänge des App-Kennworts.
    - **Mindestanzahl Sonderzeichen** – Die erforderliche Mindestanzahl an Sonderzeichen, d.h. Zeichen, die keine Buchstaben oder Zahlen sind.
    - **Mindestens ein Buchstabe erforderlich** – Stellt sicher, dass das App-Kennwort mindestens einen Buchstaben enthält.

    - **Die Mobile Client App wird nach X fehlgeschlagenen Eingabeversuchen des App-Kennworts zurückgesetzt** – Wenn diese Option aktiviert ist, werden die Einstellungen und Daten in der Access Mobile Client-App nach der festgelegten Anzahl aufeinander folgender Fehlversuche zur Eingabe des App-Kennworts zurückgesetzt.
- **Nach Kontaktverlust zurücksetzen oder sperren** – Aktivieren Sie diese Einstellung, wenn die Access Mobile Client-App automatisch zurückgesetzt oder gesperrt werden soll, falls dieser Acronis Access-Server innerhalb einer bestimmten Anzahl von Tagen nicht kontaktiert wurde. Gesperrte Clients werden automatisch entsperrt, wenn sie den Server später erfolgreich kontaktieren. Bei zurückgesetzten Clients werden sofort alle in der Mobile Client-App gespeicherten lokalen Dateien gelöscht, ihre Client-Verwaltungsrichtlinie wird entfernt, und alle Einstellungen werden auf die Standardwerte zurückgesetzt. Zurückgesetzte Clients müssen erneut bei der Verwaltung registriert werden, um Zugriff auf Gateway Server zu erlangen.
    - **Die Mobile Client App wird gesperrt/zurückgesetzt – und zwar nach X Tagen vergeblichen Kontakts mit dem Acronis Access Server dieses Clients** – Legen Sie die Standardaktion für den Fall fest, dass der Client diesen Acronis Access Server für eine bestimmte Anzahl von Tagen nicht kontaktiert.
    - **Benutzer warnen: [ ] Tage im Voraus** – Die Access Mobile Client-App kann den Benutzer warnen, wenn in Kürze eine Zurücksetzung oder Sperrung aufgrund eines 'Kontaktverlust' bevorsteht. Damit erhalten die Benutzer die Möglichkeit, eine Netzwerkverbindung neu aufzubauen, über welche die Access Mobile Client-App ihren Acronis Access Server kontaktieren und die Sperrung oder Zurücksetzung verhindern kann.
- **Benutzer kann Mobile Client aus der Verwaltung entfernen** – Aktivieren Sie diese Einstellung, wenn die Acronis Access-Benutzer die Möglichkeit haben sollen, ihre Verwaltungsrichtlinie in Acronis Access zu deinstallieren. Hierdurch wird die vollständige Funktionalität der Applikation wiederhergestellt und alle Änderungen an der Konfiguration durch die Richtlinie zurückgesetzt.
    - **Beim Entfernen alle Acronis Access-Daten vollständig löschen** – Wenn das Entfernen von Richtlinien durch den Benutzer aktiviert ist, kann diese Option ausgewählt werden. Bei aktivierter Option werden alle in der Access Mobile Client-Applikation lokal gespeicherten Daten gelöscht, wenn sie aus der Verwaltung entfernt wird. So wird sichergestellt, dass auf einem Client, der keiner Verwaltungskontrolle unterliegt, keine Unternehmensdaten mehr vorhanden sind.
- **iTunes erlauben, lokal gespeicherte Acronis Access-Dateien per Backup zu sichern** – Wenn diese Einstellung deaktiviert ist, erlaubt der Access Mobile Client iTunes nicht, seien Dateien per Backup zu sichern. Damit wird sichergestellt, dass Dateien im geschützten Gerätespeicher von Acronis Access nicht in iTunes-Backups kopiert werden.

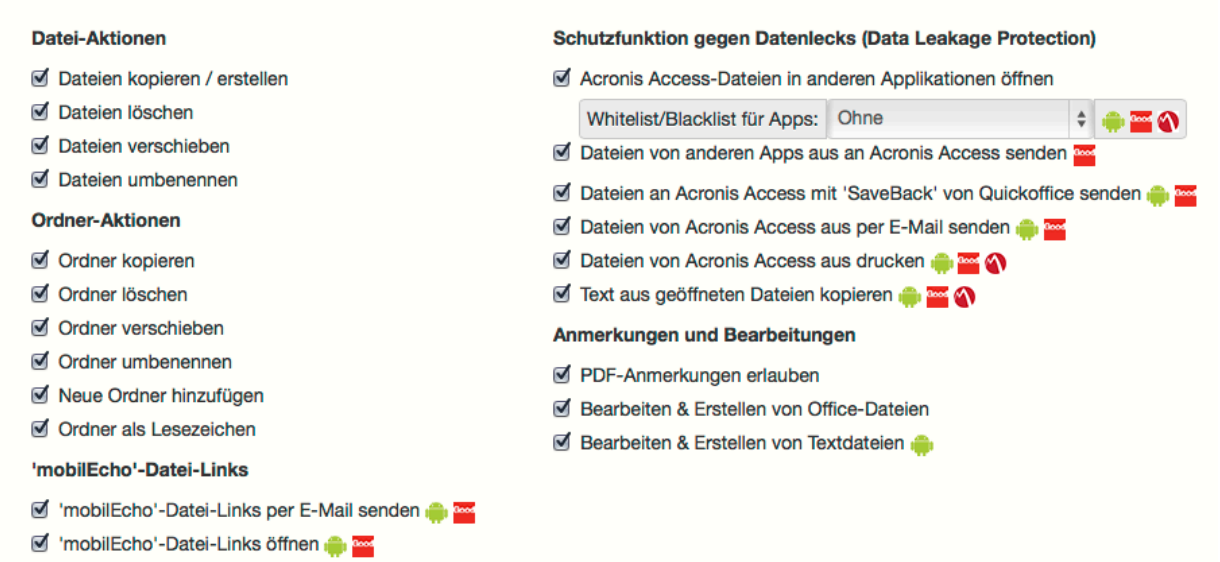
1.2.1.6 Applikationsrichtlinie



- **Bestätigung beim Löschen von Dateien verlangen** – Bei Aktivierung wird der Benutzer bei jedem Löschvorgang für eine Datei um Bestätigung gebeten. Wenn die Benutzer diese Einstellung später ändern können sollen, wählen Sie **Benutzern erlauben, diese Einstellung zu ändern**.
- **Die Standarddateiaktion festlegen** – Diese Option bestimmt, was geschieht, wenn ein Benutzer in der Access Mobile Client-Applikation auf eine Datei tippt. Wenn die Option nicht festgelegt ist, übernimmt die Client-Applikation den Standardwert aus dem Menü **Aktion**. Wenn der Benutzer in der Lage sein soll, diese Einstellung später zu ändern, wählen Sie **Benutzer erlauben, diese Einstellung zu ändern**.
- **Erlauben, dass Dateien auf diesem Gerät gespeichert werden** – Diese Einstellung ist standardmäßig aktiviert. Ist diese Option aktiviert, können Dateien im abgeschirmten Acronis Access-Speicher auf dem Gerät bleiben. Einzelne Funktionen, die Dateien lokal speichern (Ordner 'Meine Dateien', Synchronisierungsordner, Cache für zuletzt verwendete Dateien), können über zusätzliche Richtlinieneinstellungen aktiviert oder deaktiviert werden. Wenn diese Option deaktiviert ist, werden auf dem Gerät keine Dateien gespeichert, um sicherzustellen, dass sich keine Unternehmensdaten auf dem Gerät befinden, falls dieses verloren geht oder gestohlen wird. Ist diese Einstellung deaktiviert, kann der Benutzer Dateien für die Offline-Verwendung nicht speichern oder synchronisieren, Dateien für eine verbesserte Leistung zwischenspeichern oder Dateien aus anderen Applikationen mit der Funktion 'Öffnen in' zum Access Mobile Client senden.
  - **Benutzern erlauben, Dateien im Geräteordner 'Meine Dateien' zu speichern** – Wenn diese Option aktiviert ist, können Dateien für den Offline-Zugriff und zur Bearbeitung in den Ordner 'Meine Dateien' kopiert werden. Dies ist ein Universalspeicherbereich im abgeschirmten Gerätespeicher von Acronis Access.
  - **Kürzlich verwendete Dateien auf dem Gerät zwischenspeichern (cachen)** – Bei Aktivierung werden serverbasierte Dateien, auf die zuletzt zugegriffen wurde, in einem lokalen Cache auf dem Gerät gespeichert, sodass sie, sofern sie nicht geändert wurden, bei Bedarf schnell wieder verfügbar sind. Dies dient der Leistungssteigerung und der Einsparung von Bandbreite. **Maximale Cache-Größe** – Kann angegeben werden; optional können Änderungen durch Benutzer zugelassen werden.

- **Inhalte in 'Meine Dateien' und 'Datei-Inbox' verfallen nach X Tagen** – Bei Aktivierung dieser Option werden Dateien in 'Eingang für Dateien' und 'Meine Dateien' nach der eingestellten Anzahl von Tagen vom Gerät gelöscht.

Zulassen



Mit diesen Einstellungen können bestimmte Funktionen und Fähigkeiten der Access Mobile Client-Applikation deaktiviert werden. Alle Einstellungen zum Kopieren, Erstellen, Verschieben, Umbenennen und Löschen gelten für Dateien und Ordner, die auf Gateway Servern gespeichert sind. Dateien im lokalen Ordner 'Meine Dateien' des mobilen Clients werden dagegen auf dem Gerät gespeichert und sind daher von den Einstellungen nicht betroffen. Alle anderen Einstellungen gelten für alle Dateien in Acronis Access, also sowohl für serverbasierte als auch für auf dem Client lokal gespeicherte.

Dateivorgänge

- **Dateien kopieren/erstellen** – Wenn diese Option deaktiviert ist, können Benutzer keine Dateien aus anderen Applikationen oder aus der iPad-Fotobibliothek auf einem Gateway Server speichern. Sie können außerdem keine neuen Dateien oder Ordner auf dem Gateway Server kopieren oder erstellen. Diese Einstellung überschreibt sämtliche Berechtigungen in NTFS, aufgrund derer der Client möglicherweise Dateien erstellen darf.
- **Dateien löschen** – Wenn diese Option deaktiviert ist, können Benutzer keine Dateien vom Gateway Server löschen. Diese Einstellung überschreibt sämtliche Berechtigungen in NTFS, aufgrund derer der Client möglicherweise Dateien löschen darf.
- **Dateien verschieben** – Wenn diese Option deaktiviert ist, kann der Benutzer Dateien nicht von einem Speicherort in einen anderen auf dem Gateway Server oder vom Server in den lokalen Speicher 'Meine Dateien' der Access Mobile Client-Applikation verschieben. Diese Einstellung überschreibt sämtliche Berechtigungen in NTFS, aufgrund derer der Client möglicherweise Dateien oder Ordner verschieben darf.

- **Dateien umbenennen** – Wenn diese Option deaktiviert ist, können Benutzer keine Dateien auf dem Gateway Server umbenennen. Diese Einstellung überschreibt sämtliche Berechtigungen in NTFS, aufgrund derer der Client möglicherweise Dateien verschieben darf.

Ordnervorgänge

- **Ordner kopieren** – Wenn diese Option deaktiviert ist, können Benutzer keine Ordner auf dem oder auf den Gateway Server kopieren. Diese Einstellung überschreibt sämtliche Berechtigungen in NTFS, aufgrund derer der Client möglicherweise Ordner erstellen darf. **Dateien kopieren / erstellen** muss aktiviert sein, damit diese Einstellung aktiviert werden kann.
- **Ordner löschen** – Wenn diese Option deaktiviert ist, können Benutzer keine Ordner vom Gateway Server löschen. Diese Einstellung überschreibt sämtliche Berechtigungen in NTFS, aufgrund derer der Client möglicherweise Ordner löschen darf.
- **Ordner verschieben** – Wenn diese Option deaktiviert ist, kann der Benutzer Ordner nicht von einem Speicherort in einen anderen auf dem Gateway Server oder vom Server in den lokalen Speicher 'Meine Dateien' der Access Mobile Client-Applikation verschieben. Diese Einstellung überschreibt sämtliche Berechtigungen in NTFS, aufgrund derer der Client möglicherweise Dateien oder Ordner verschieben darf. **Ordner kopieren** muss aktiviert sein, damit diese Einstellung aktiviert werden kann.
- **Ordner umbenennen** – Wenn diese Option deaktiviert ist, können Benutzer keine Ordner auf dem Gateway Server umbenennen. Diese Einstellung überschreibt sämtliche Berechtigungen in NTFS, aufgrund derer der Client möglicherweise Ordner umbenennen darf.
- **Neue Ordner hinzufügen** – Wenn diese Option deaktiviert ist, können Benutzer keine neuen leeren Ordner auf dem Gateway Server erstellen.
- **Ordner als Lesezeichen zulassen** – Wenn diese Option deaktiviert ist, kann der Benutzer Acronis Access-Geräte- oder Server-Ordner nicht für den Schnellzugriff als Lesezeichen setzen.

'mobilEcho'-Datei-Links

- **'mobilEcho'-Datei-Links per E-Mail senden** – Wenn diese Option deaktiviert ist, können die Benutzer keine mobilEcho://-URLs für Acronis Access-Dateien oder -Ordner an andere Acronis Access-Benutzer senden. Diese Links funktionieren nur, wenn sie auf einem Gerät aufgerufen werden, auf dem der Empfänger den Access Mobile Client installiert und mit einem Server oder zugewiesenen Ordner konfiguriert hat, von dem aus ein Zugriff auf die Link-Adresse möglich ist. Der Benutzer muss zudem Berechtigungen auf Datei-/Ordnerebene besitzen, um das betreffende Element lesen zu können.
- **'mobilEcho'-Datei-Links öffnen** – Wenn diese Option deaktiviert ist, können die Benutzer keine mobilEcho://-URLs für Acronis Access-Dateien oder -Ordner öffnen.

Schutz vor Datenverlust

- **Acronis Access-Dateien in anderen Applikationen öffnen** – Wenn diese Option deaktiviert ist, ignoriert die Access Mobile Client-Applikation die Schaltfläche **Öffnen in** und lässt nicht zu, dass Acronis Access-Dateien in anderen Applikationen geöffnet werden. Wird eine Datei in einer anderen Applikation geöffnet, wird die Datei in den Dateispeicherbereich der betreffenden Applikation kopiert, sodass sie nicht mehr der Kontrolle durch Acronis Access unterliegt.

- **Whitelist/Blacklist für Apps** – Wählen Sie eine vordefinierte Whitelist oder Blacklist aus, mit der Drittanbieter-Apps eingeschränkt werden, in denen Acronis Access-Dateien auf dem Gerät geöffnet werden können. Zum Erstellen einer Whitelist oder Blacklist klicken Sie in der oberen Menüleiste auf **Erlaubte Apps**.

- **Dateien von anderen Apps aus an Acronis Access senden** – Wenn diese Option deaktiviert ist, akzeptiert die Access Mobile Client-Applikation keine Dateien, die über die Funktion **Öffnen in** von anderen Applikationen an sie gesendet wurden.
- **Dateien an Acronis Access mit 'Save Back' von Quickoffice senden** – Wenn diese Option deaktiviert ist, akzeptiert die Acronis Access-Applikation keine Dateien, die mit der Funktion **SaveBack** von Quickoffice an sie gesendet wurden.
- **Dateien von Acronis Access aus per E-Mail senden** – Wenn diese Option deaktiviert ist, ignoriert die Access Mobile Client-Applikation die Schaltfläche **Datei per E-Mail senden** und lässt nicht zu, dass Acronis Access-Dateien aus der Applikation per E-Mail gesendet werden.
- **Dateien von Acronis Access aus drucken** – Wenn diese Option deaktiviert ist, ignoriert die Access Mobile Client-Applikation die Schaltfläche **Drucken** und lässt nicht zu, dass Acronis Access-Dateien gedruckt werden.
- **Text aus geöffneten Dateien kopieren** – Wenn diese Option deaktiviert ist, lässt der Access Mobile Client nicht zu, dass der Benutzer Text in geöffneten Dokumenten zum Kopieren/Einfügen auswählen kann. Damit wird verhindert, dass Daten in andere Applikationen kopiert werden.

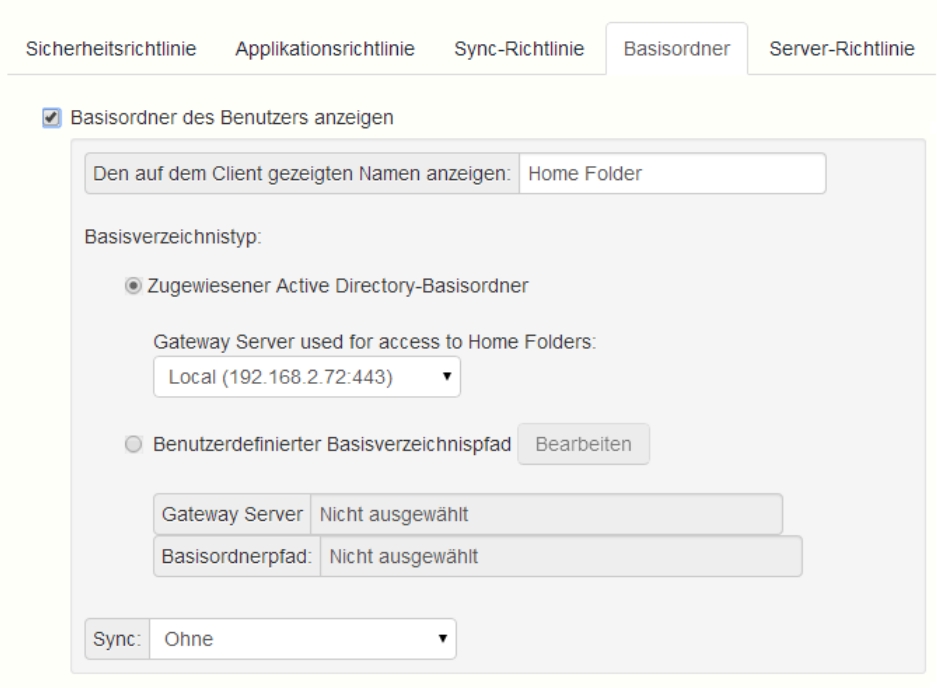
Anmerkungen und Bearbeitung

- **PDF-Anmerkungen erlauben** – Wenn diese Option deaktiviert ist, können Sie mit dem Access Mobile Client keine Anmerkungen in PDF-Dateien erstellen.
- **Bearbeiten & Erstellen von Office-Dateien** – Wenn diese Option deaktiviert ist, können Benutzer keine Dokumente mit dem integrierten SmartOffice-Editor bearbeiten.
- **Bearbeiten & Erstellen von Textdateien** – Wenn diese Option deaktiviert ist, können Benutzer keine .txt-Dateien mit dem integrierten Texteditor bearbeiten.

1.2.1.7 Synchronisierungsordner

- **'Vom Benutzer erstellte Sync-Ordner' erlauben** – Erlaubt dem Benutzer, seine eigenen Synchronisierungsordner zu erstellen.
- **Bestätigungsaufforderung an Client, bevor synchronisierte Dateien heruntergeladen werden** – Wählen Sie die Bedingungen aus, unter denen der Benutzer das Herunterladen von Dateien in synchronisierten Ordnern bestätigen muss. Es gibt folgende Optionen: **Immer**, **Nur in Mobilfunknetzen** und **Nie**. Wenn **Benutzern erlauben, diese Einstellung zu ändern** aktiviert ist, sind Clients in der Lage, die Bestätigungsoptionen zu ändern.
- **Dateisynchronisierung nur erlauben, wenn Gerät per WiFi-Netzwerk verbunden ist** – Wenn diese Option aktiviert ist, lässt Acronis Access eine Synchronisierung von Dateien über Mobilfunkverbindungen nicht zu. Wenn **Benutzern erlauben, diese Einstellung zu ändern** aktiviert ist, sind Clients in der Lage, die automatische Dateisynchronisierung in WiFi-Netzwerken zu aktivieren bzw. zu deaktivieren.
- **Auto-Sync-Intervall** – Wenn diese Option aktiviert ist, führt Acronis Access eine automatische Synchronisierung **nie**, **nur beim App-Start** oder in verschiedenen **Intervallen** aus.
  - **Benutzer erlauben, diese Einstellung zu ändern** – Wenn diese Option aktiviert ist, können die Benutzer das Zeitintervall in der Access Mobile Client-App ändern.
  - **Dateisynchronisierung nur in WiFi-Netzwerken** – Wenn diese Option aktiviert ist, wird die automatische Synchronisierung erst bei einer bestehenden WiFi-Verbindung ausgeführt.

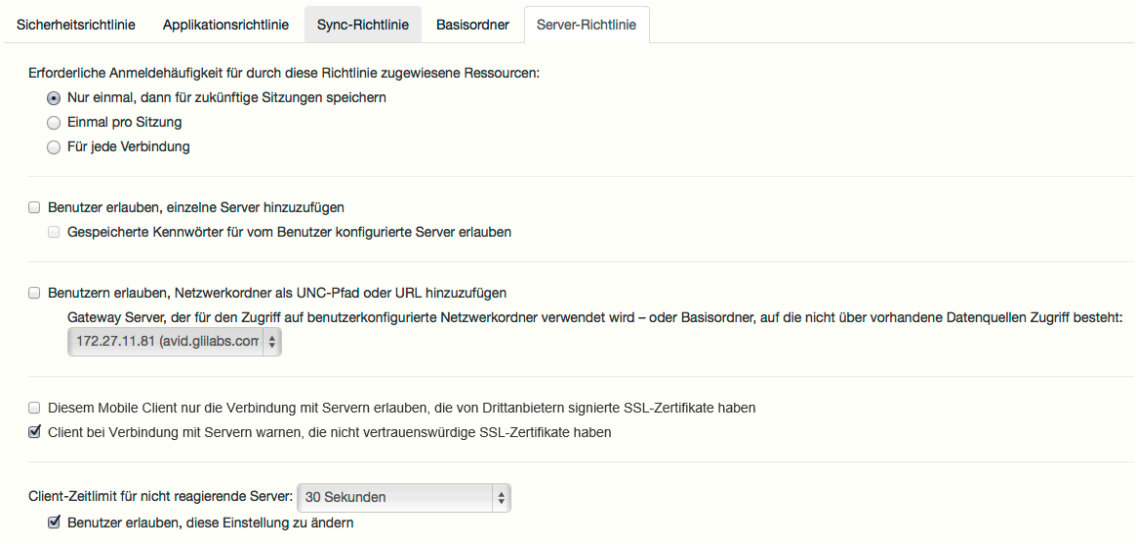
1.2.1.8 Basisordner



- **Basisordner des Benutzers anzeigen** – Diese Option bewirkt, dass das persönliche Basisverzeichnis des Benutzers in der Access Mobile Client-App angezeigt wird.
  - **Den auf dem Client gezeigten Namen anzeigen** – Legt den Anzeigenamen des Basisordners in der Access Mobile Client-App fest.

- **Zugewiesener Active Directory-Basisordner** – Über den in der Access Mobile Client-App angezeigten Basisordner wird der Benutzer mit dem Server/Ordnerpfad verbunden, der in seinem AD-Kontoprofil definiert ist. Der Zugriff auf den Basisordner erfolgt über das ausgewählte Gateway.
- **Benutzerdefinierter Basisverzeichnispfad** – Über den in der Access Mobile Client-App angezeigten Basisordner wird der Benutzer mit dem Server und Pfad verbunden, der in dieser Einstellung definiert ist. Der Platzhalter %USERNAME% kann verwendet werden, um den Benutzernamen des Benutzers in den Pfad für den Basisordner aufzunehmen. %USERNAME% muss in Großbuchstaben eingegeben werden.
- **Sync** – Über diese Option können Sie den Synchronisierungstyp für das Basisverzeichnis festlegen.

1.2.1.9 Serverrichtlinie



- **Erforderliche Anmeldehäufigkeit für durch diese Richtlinie zugewiesene Ressourcen** – Legt die Häufigkeit fest, mit der sich Benutzer bei den Servern anmelden müssen, die ihnen durch ihre Richtlinie zugewiesen sind.
  - **Nur einmal, dann für zukünftige Sitzungen speichern** – Der Benutzer gibt sein Kennwort ein, wenn er in der Verwaltung registriert wird. Das Kennwort wird gespeichert und für alle zukünftigen Verbindungen zum Dateiserver verwendet.
  - **Einmal pro Sitzung** – Nach dem Start des Access Mobile Clients muss der Benutzer sein Kennwort eingeben, sobald er mit dem ersten Server eine Verbindung herstellt. Bis zum Verlassen der Access Mobile Client Anwendung kann er sich anschließend mit weiteren Servern verbinden, ohne das Kennwort erneut eingeben zu müssen. Verlässt er den Access Mobile Client für eine beliebige Zeit und kehrt dann wieder zurück, muss er sein Kennwort erneut eingeben, um eine Verbindung mit dem ersten Server herzustellen.
  - **Für jede Verbindung** – Der Benutzer muss das Kennwort jedes Mal eingeben, wenn er eine Verbindung zu einem Server herstellt.
- **Benutzer erlauben, einzelne Server hinzuzufügen** – Wenn diese Option aktiviert ist, können Benutzer in der Access Mobile Client Anwendung Server manuell hinzufügen, sofern sie den DNS-Namen des Servers oder dessen IP-Adresse kennen. Wenn dem Benutzer nur die Server zur Verfügung stehen sollen, die ihm über seine Richtlinie zugewiesen wurden, lassen Sie diese Option deaktiviert.

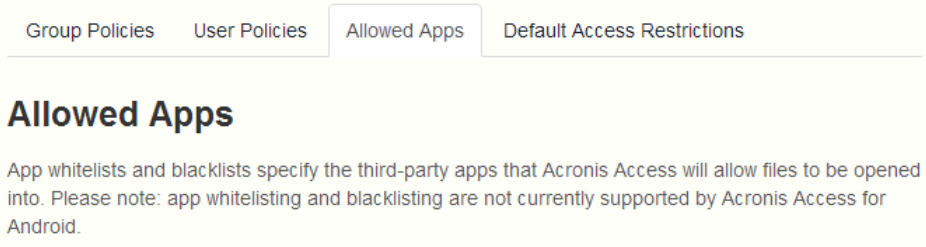
- **Gespeicherte Kennwörter für vom Benutzer konfigurierte Server erlauben** – Wenn dem Benutzer erlaubt ist, Server selbst hinzuzufügen, können Sie über diese Unteroption festlegen, ob er sein Kennwort für diese Server speichern darf.

- **Benutzern erlauben, Netzwerkordner als UNC-Pfad oder URL hinzuzufügen** – Wenn diese Option aktiviert ist, können Benutzer des mobilen Clients Netzwerkordner und SharePoint-Sites hinzufügen und darauf zugreifen, die ihnen nicht zugewiesen sind oder die nicht über die bestehenden Datenquellen zugänglich sind. Der ausgewählte Gateway Server muss Zugriff auf diese SMB-Freigaben oder SharePoint-Sites haben.
  - **Zugriff auf bestimmte Netzwerkpfade blockieren** – Wenn diese Option aktiviert ist, kann der Administrator Blacklists von Netzwerkpfaden erstellen und verwenden, die von den Benutzern nicht selbst bereitgestellt werden dürfen.
- **Diesem Mobile Client nur die Verbindung mit Servern erlauben, die von Drittanbietern signierte SSL-Zertifikate haben** – Wenn diese Option aktiviert ist, kann der Access Mobile Client nur Verbindungen mit Servern herstellen, die über von Drittanbietern signierte SSL-Zertifikate verfügen.

  Hinweis: *Falls der Management-Server nicht über ein Drittanbieter-Zertifikat verfügt, kann der Client nach der Erstkonfiguration keine Verbindung zum Management-Server herstellen. Stellen Sie sicher, dass all Ihre Gateway Server über Drittanbieter-Zertifikate verfügen, bevor Sie diese Option aktivieren.*

- **Client bei Verbindung mit Servern warnen, die nicht vertrauenswürdige SSL-Zertifikate haben** – Wenn Ihre Benutzer regelmäßig Verbindungen zu Servern mit selbstsignierten Zertifikaten herstellen, können Sie den clientseitigen Warnhinweis aktivieren, der beim Herstellen einer solchen Serververbindung angezeigt wird.
- **Client-Zeitlimit für nicht reagierende Server** – Über diese Option kann der Zeitüberschreitungswert für Client-Verbindungen festgelegt werden, wenn der Server nicht reagiert. Wenn die Clients besonders langsame Datenverbindungen nutzen oder die Serververbindung erst durch eine bedarfsabhängige VPN-Lösung hergestellt werden muss, sollte die Zeitüberschreitung standardmäßig auf einen Wert über 30 Sekunden eingestellt werden. Wenn der Client in der Lage sein soll, diese Einstellung über die Access Mobile Client App zu ändern, aktivieren Sie die Option **Benutzer erlauben, diese Einstellung zu ändern**.

1.2.2 Erlaubte Apps



Mit Acronis Access Client Management können Sie Whitelists oder Blacklists erstellen, welche die Möglichkeit des Access Mobile Clients einschränken, Dateien in anderen Applikationen auf einem mobilen Gerät zu öffnen. Mit diesen Listen können Sie sicherstellen, dass Dateien, auf die über den Access Mobile Client zugegriffen werden kann, nur in sicheren, vertrauenswürdigen Apps geöffnet werden können.

Whitelists – Sie können eine Liste von Apps angeben, in denen Acronis Access-Dateien geöffnet werden dürfen. Allen anderen Apps wird der Zugriff verweigert.

Blacklists – Sie können eine Liste von Apps angeben, in denen Acronis Access-Dateien nicht geöffnet werden dürfen. Allen anderen Apps wird der Zugriff gestattet.

Damit Acronis Access eine bestimmte App identifizieren kann, muss es den **Bundle Identifier** der App kennen. Eine Liste häufig verwendeter Apps und ihrer Bundle Identifier ist standardmäßig auf der Acronis Access Weboberfläche enthalten. Wenn eine App, die in einer Whitelist oder Blacklist enthalten sein soll, darin noch nicht enthalten ist, müssen Sie sie der Liste hinzufügen.

Hinweis: *App-Whitelists und -Blacklists werden derzeit vom Access Mobile Client für Android nicht unterstützt.*

Listen

Fügen Sie Whitelists und Blacklists hinzu. Sobald erstellt, können Whitelists und Blacklists jeder Benutzer- oder Gruppenrichtlinie von Acronis Access zugewiesen werden. Sie gelten nur für die von Ihnen spezifizierten Benutzer- oder Gruppenprofile.

- **Name** – Zeigt den vom Administrator festgelegten Namen der Liste an.
- **Typ** – Zeigt den Typ der Liste an (Whitelist/Blacklist).
- **Liste hinzufügen** – Öffnet ein Menü zum Hinzufügen einer neuen Whitelist oder Blacklist.

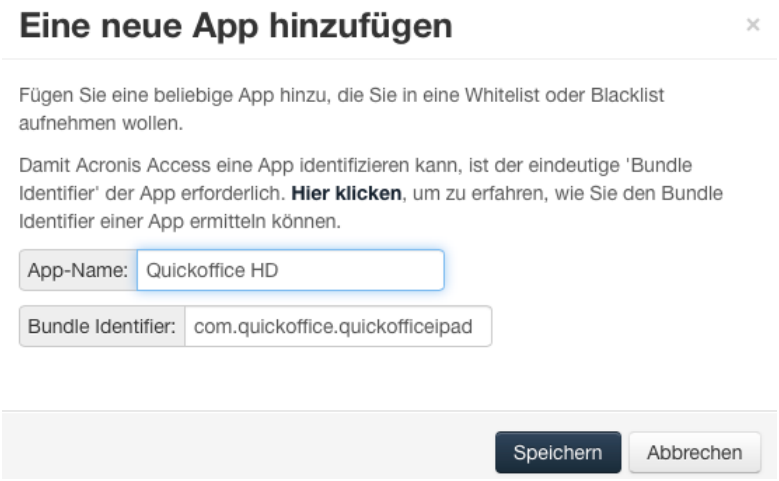
Themen

1.2.2.1 Für die Listen verfügbare Apps hinzufügen

So fügen Sie eine App hinzu, die in eine Whitelist oder Blacklist aufgenommen werden soll:

1. Klicken Sie in der oberen Menüleiste auf **Erlaubte Apps**.
2. Klicken Sie im Abschnitt **Für die Listen verfügbare Apps** auf **App hinzufügen**.
3. Geben Sie den **Namen der App** ein. Dies kann der Name der App wie im App Store sein oder ein alternativer Name Ihrer Wahl.
4. Geben Sie den **Bundle Identifier** der App ein. Dieser muss exakt mit dem Bundle Identifier der gewünschten Apps übereinstimmen, anderenfalls erfolgt keine Aufnahme in eine White- oder Blacklist.
5. Klicken Sie auf **Speichern**.

Sie können den Bundle Identifier suchen, indem Sie entweder die Dateien auf Ihrem Gerät durchsuchen (S. 24) oder diesen in einer iTunes-Bibliothek anzeigen (S. 24).



1.2.2.2 Den Bundle Identifier einer App durch Durchsuchen der Dateien auf Ihrem Gerät ermitteln

Falls Sie Software verwenden, mit der Sie den Inhalt Ihres Gerätespeichers durchsuchen können, können Sie nach einer App auf dem Gerät suchen und ihren **Bundle Identifier** ermitteln. Eine App, die hierfür verwendet werden kann, ist iExplorer.

1. Verbinden Sie Ihr Gerät mit dem Computer über einen USB-Anschluss und öffnen Sie iExplorer oder ein ähnliches Dienstprogramm.
2. Öffnen Sie den Apps-Ordner auf dem Gerät und suchen Sie nach der gewünschten App.
3. Öffnen Sie den Ordner dieser App und suchen Sie nach der Datei **iTunesMetadata.plist**.
4. Öffnen Sie diese PLIST-Datei in einem Texteditor.
5. Suchen Sie nach dem **softwareVersionBundleId**-Schlüssel in der Liste.
6. Die darunter stehende **Zeichenfolge** ist der Wert des Bundle Identifier, den Sie für die App in Acronis Access eingeben müssen. Diese Zeichenfolgen sind gewöhnlich wie folgt formatiert: **com.firmenname.appname**

1.2.2.3 Den Bundle Identifier einer App in einer iTunes Library ermitteln

Wenn Sie Ihr Gerät mit iTunes synchronisieren und sich die gewünschte App entweder auf Ihrem Gerät befindet oder über iTunes heruntergeladen wurde, existiert sie auf der Festplatte Ihres Computers. Sie können auf Ihrer Festplatte danach suchen und dann innerhalb der App den **Bundle Identifier** ermitteln.

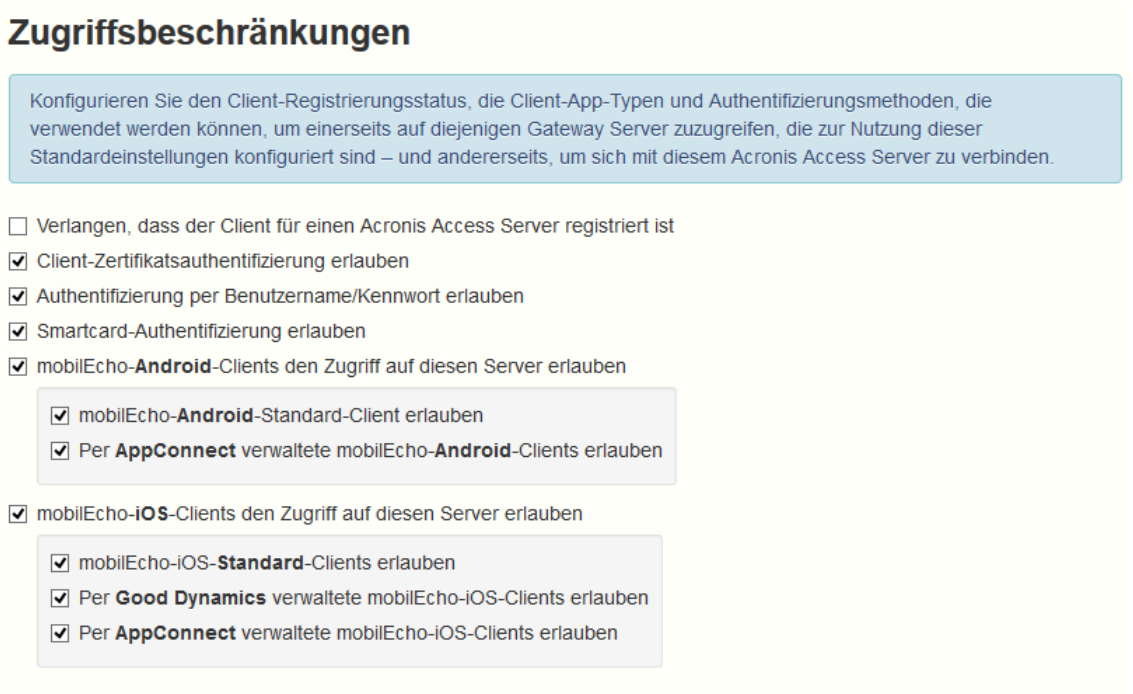
1. Navigieren Sie zur iTunes Library, und öffnen Sie den Ordner **Mobile Applications**.
2. Auf einem Mac befindet sich dieser normalerweise in ~/Music/iTunes/Mobile Applications/
3. Auf einem Windows 7 PC befindet er sich für gewöhnlich in **`C:\Users\username\My Music\iTunes\Mobile Applications/`**
4. Falls Sie die App erst kürzlich auf Ihrem Gerät installiert haben, sollten Sie unbedingt eine iTunes-Synchronisierung durchführen, bevor Sie fortfahren.
5. Suchen Sie nach der benötigten App im Ordner **Mobile Applications**.
6. Duplizieren Sie die Datei und benennen Sie die Erweiterung in .ZIP um.

7. Wenn Sie diese neu erstellte ZIP-Datei dekomprimieren, erhalten Sie einen Ordner mit dem Applikationsnamen.
8. Innerhalb dieses Ordners befindet sich eine Datei namens **iTunesMetadata.plist**.
9. Öffnen Sie diese PLIST-Datei in einem Texteditor.
10. Suchen Sie nach dem **softwareVersionBundleId**-Schlüssel in der Liste.
11. Die darunter stehende **Zeichenfolge** ist der Wert des Bundle Identifier, den Sie für die App in Acronis Access eingeben müssen. Diese Zeichenfolgen sind gewöhnlich wie folgt formatiert: **com.firmenname.appname**

1.2.3 Standardzugriffsbeschränkungen

In diesem Bereich können Sie Beschränkungen für Clients festlegen, die den Management Server kontaktieren. Diese Beschränkungen sind auch die standardmäßigen Beschränkungen für Gateway Server.

Hinweis: *Informationen zum Einstellen von benutzerdefinierten Beschränkungen für Ihre Gateway Server finden Sie im Artikel Gateway Server bearbeiten (S. 43) im Abschnitt 'Gateway Server verwalten'.*



Konfigurieren Sie den Client-Registrierungsstatus, die Client-App-Typen und die Authentifizierungsmethoden, die zur Verbindung mit diesem Acronis Access Server sowie all denjenigen Gateway-Servern verwendet werden können, welche zur Nutzung der Standardzugriffsbeschränkungen konfiguriert sind.

- **Verlangen, dass der Client für einen Acronis Access Server registriert ist** – Wenn Sie diese Option auswählen, müssen alle Access Mobile Clients, die eine Verbindung mit diesem Server herstellen, von einem Acronis Access verwaltet werden, der unter 'Zulässige Acronis Access-Server' aufgeführt wird. Diese Option stellt sicher, dass alle Clients, die auf den Server zugreifen, über die erforderlichen Einstellungen und Sicherheitsoptionen verfügen. Der eingegebene Server-Name muss mit dem Namen des Management Servers übereinstimmen, der in der Access Mobile Client-App konfiguriert ist. Es können auch unvollständige Namen

verwendet werden, um beispielsweise mehrere Client-Management-Server in einer Domain zu erlauben. Bei unvollständigen Namen sind keine Platzhaltersymbole erforderlich.

- **Client-Zertifikatsauthentifizierung erlauben** – Wenn Sie das Kontrollkästchen für diese Option deaktivieren, können Benutzer nicht über ein Zertifikat verbunden werden; sie können aber per Benutzername und Kennwort des Clients oder per Smartcard verbunden werden.
- **Authentifizierung per Benutzername/Kennwort erlauben** – Wenn Sie das Kontrollkästchen für diese Option deaktivieren, können Benutzer nicht per Benutzername und Kennwort verbunden werden; sie können aber per Client-Zertifikat oder Smartcard verbunden werden.
- **Smartcard-Authentifizierung erlauben** – Wenn Sie das Kontrollkästchen für diese Option deaktivieren, können Benutzer nicht per Smartcard verbunden werden; sie können aber per Benutzername und Kennwort des Clients oder per Zertifikat verbunden werden.
- **Acronis Access-Android-Clients den Zugriff auf diesen Server erlauben** – Wenn Sie diese Option deaktivieren, können Android-Geräte keine Verbindung mit dem Acronis Access-Server herstellen, und Sie können zudem nicht auf die Managementfunktion zugreifen. Wenn Sie diese Option auswählen, können Sie des Weiteren einstellen, welche Clients mit den folgenden Optionen verbunden werden können:
  - **Acronis Access-Android-Standard-Clients erlauben** – Wenn Sie diese Option auswählen, lässt dieser Acronis Access-Server Verbindungen mit Benutzern zu, die den Acronis Access-Android-Standard-Client ausführen. Wenn Android-Benutzer nicht auf diesen Acronis Access-Server zugreifen sollen, können Sie diese Einstellung deaktivieren.
  - **Per AppConnect verwaltete Acronis Access-Android-Clients erlauben** – Wenn Sie diese Option auswählen, lässt dieser Acronis Access-Server Android-Benutzer mit Acronis Access-Clients zu, die in MobileIron registriert sind. Wenn Android-Benutzer, die in MobileIron registriert sind, nicht auf diesen Acronis Access-Server zugreifen sollen, können Sie diese Einstellung deaktivieren.
- **Acronis Access-iOS-Clients den Zugriff auf diesen Server erlauben** – Wenn Sie diese Option deaktivieren, können iOS-Geräte keine Verbindung mit dem Acronis Access-Server herstellen, und Sie können zudem nicht auf die Managementfunktion zugreifen. Wenn Sie diese Option auswählen, können Sie mit den unten aufgeführten Optionen weiter festlegen, welche Clients eine Verbindung herstellen können.
  - **Acronis Access-iOS-Standard-Clients erlauben** – Wenn Sie diese Option auswählen, lässt dieser Acronis Access-Server Verbindungen mit Benutzern zu, welche die Standard-iOS-Access Mobile Client-App ausführen. Wenn iOS-Benutzer nicht auf diesen Acronis Access-Server zugreifen sollen, können Sie diese Einstellung deaktivieren.
  - **Per Good Dynamics verwaltete Acronis Access-iOS-Clients erlauben** – Wenn Sie diese Option auswählen, lässt dieser Acronis Access-Server Benutzer zu, die Verbindungen über den per Good Dynamics verwalteten iOS-Client von Access Mobile Client herzustellen. Wenn Benutzer mit dem per Good Dynamics verwalteten iOS-Client von Access Mobile Client nicht auf diesen Acronis Access-Server zugreifen sollen, können Sie diese Einstellung deaktivieren.
  - **Per AppConnect verwaltete Acronis Access-iOS-Clients erlauben** – Wenn Sie diese Option auswählen, lässt dieser Acronis Access-Server iOS-Benutzer mit Access Mobile Client zu, die in MobileIron registriert sind. Wenn iOS-Benutzer, die in MobileIron registriert sind, nicht auf diesen Acronis Access-Server zugreifen sollen, können Sie diese Einstellung deaktivieren.

1.3 Integration mobiler Geräte

Um den mobilen Client von Acronis Access verwenden zu können, müssen die Benutzer die Access Mobile Client-Applikation über den Apple App Store installieren. Wenn Ihr Unternehmen die Client-Verwaltung verwendet, müssen Sie Benutzer außerdem die Access Mobile Client-App auf ihrem Gerät beim Acronis Access-Server registrieren. Nach der Registrierung werden die Konfiguration des mobilen Clients, die Sicherheitseinstellungen und Funktionen von der Acronis Access-Benutzer- oder Gruppenrichtlinie gesteuert.

Von der Verwaltungsrichtlinie werden die folgenden Einstellungen und Funktionen der Access Mobile Client-Applikation gesteuert:

- Kennworts zum Sperren der Access Mobile Client-Applikation verlangen
- Komplexitätsanforderungen für das Kennwort
- Möglichkeit zum Entfernen der Access Mobile Client-App aus der Verwaltung
- Dateien über den Access Mobile Client per E-Mail senden und drucken
- Speichern von Dateien auf dem Gerät erlauben
- Access Mobile Client-Gerätedateien in iTunes-Backups einbeziehen lassen
- Dateien aus anderen Applikationen an den Access Mobile Client senden
- Öffnen von Access Mobile Client-Dateien in anderen Applikationen zulassen
- Andere Applikationen einschränken, in denen Access Mobile Client-Dateien geöffnet werden dürfen
- PDF-Anmerkungen erlauben
- Erstellen, Umbenennen und Löschen von Dateien und Ordnern zulassen
- Verschieben von Dateien zulassen
- Bestätigung beim Löschen von Dateien verlangen
- Server, Ordner und Basisverzeichnisse können zugewiesen werden, sodass sie in der Access Mobile Client-App automatisch angezeigt werden
- Konfiguration von Ordnern für die 1-Weg- oder 2-Wege-Synchronisierung mit dem Server

Themen

1.3.1 Serverseitiger Verwaltungsregistrierungsvorgang

Registrierungsmodus auswählen

1. Rufen Sie die Acronis Access Weboberfläche auf.
2. Melden Sie sich als Administrator an.
3. Öffnen Sie die Registerkarte **Mobiler Zugriff**.
4. Rufen Sie die Registerkarte **Einstellungen** auf.
5. Wählen Sie die Anforderungen für die Registrierung des gewünschten Geräts.

Acronis Access umfasst zwei Modi für die Geräteregistrierung. Dieser Modus wird für alle Clientregistrierungen verwendet. Sie müssen die Option wählen, die Ihren Anforderungen entspricht:

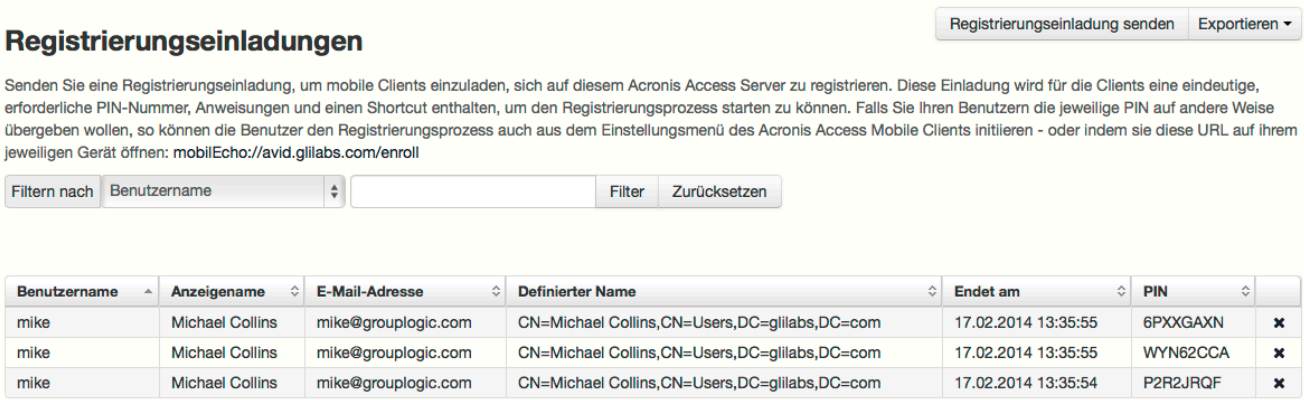
- **PIN-Nummer + Active Directory-Benutzername und Kennwort** – Um die Acronis Access-App zu aktivieren und Zugriff auf Acronis Access-Server zu erhalten, muss der Benutzer eine einmalig verwendbare PIN-Nummer mit Ablaufdatum sowie einen gültigen Active Directory-Benutzernamen und ein gültiges Kennwort eingeben. Mit dieser Option wird sichergestellt, dass Benutzer nur ein Gerät und erst nach Erhalt einer vom IT-Administrator ausgestellten PIN-Nummer registrieren können. Diese Option wird empfohlen, wenn die erhöhte Sicherheit der Zwei-Faktoren-Geräteregistrierung gefordert wird.
- **Nur Active Directory-Benutzername und -Kennwort** – Ein Benutzer kann die Acronis Access-App nur mit dem Active Directory-Benutzernamen und -Kennwort aktivieren. Mit dieser Option können Benutzer jederzeit ein oder mehrere Geräte registrieren. Den Benutzern muss lediglich der Name des Acronis Access Client Management-Server oder eine URL genannt werden, die auf den Acronis Access Client Management-Server verweist. Diese Angaben können auf einer Website bereitgestellt oder per E-Mail gesendet werden. Auf diese Weise wird die Bereitstellung von Acronis Access für eine große Zahl von Benutzern vereinfacht. Diese Option ist in Umgebungen vorzuziehen, in denen keine Zwei-Faktor-Registrierung erforderlich ist und viele Benutzer jederzeit Zugriff auf Acronis Access benötigen, beispielsweise in Deployments für Studierende.

Benutzer zum Registrieren einladen

Benutzer werden normalerweise über eine E-Mail, die vom Acronis Access Administrator gesendet wird, eingeladen, sich beim Acronis Access Server zu registrieren. Falls vom Server verlangt, enthält diese E-Mail eine einmalig zu verwendende PIN-Nummer, die für eine konfigurierbare Anzahl von Tagen gültig ist. Mit der PIN-Nummer kann die Access Mobile Client-App auf nur einem Gerät

registriert werden. Falls ein Benutzer mehrere Geräte verwendet, muss er eine Einladungs-E-Mail für jedes Gerät erhalten, das Zugriff erfordert. Diese E-Mail enthält einen Link zur Access Mobile Client-App im Apple App Store, falls die App zuerst installiert werden muss. Sie enthält darüber hinaus einen zweiten Link. Wenn Sie auf dem Gerät auf diesen Link tippen, wird der Access Mobile Client geöffnet, und in das Formular zum Registrieren des Clients werden automatisch der Name des Acronis Access-Servers, die eindeutige PIN-Nummer für die Registrierung und der Benutzername eingetragen. Bei Verwendung dieses Links muss der Benutzer lediglich sein Kontokennwort eingeben, um die Client-Registrierung abzuschließen.

- Sobald eine Registrierungseinladung generiert wurde, werden eingeladene Benutzer auf der Seite **Registrierungseinladungen** angezeigt. Für den Fall, dass Sie mit einem Benutzer auf einem anderen Weg als über die automatische E-Mail kommunizieren müssen, wird die PIN-Nummer jedes Benutzers aufgeführt.
- Sobald ein Benutzer den Access Mobile Client erfolgreich mit der einmal zu verwendenden PIN-Nummer registriert, wird er nicht mehr in dieser Liste aufgeführt.
- Um die Einladungs-PIN-Nummer eines Benutzers zu widerrufen, drücken Sie 'Löschen', um die Angabe aus der Liste zu entfernen.
- **Filtern nach** – Die Einladungsliste kann nach Benutzernamen, Anzeigenamen oder E-Mail-Adresse gefiltert werden.
- Registrierungseinladungen als CSV herunterladen – Die gesamte oder gefilterte Einladungsliste kann in eine CSV-Datei exportiert und in Excel geöffnet oder in einen benutzerdefinierten Prozess importiert werden.



Einfache URL-Registrierungs-Links verwenden, wenn keine PIN-Nummern benötigt werden:

Wenn Ihr Server so konfiguriert ist, dass für die Client-Registrierung keine PIN-Nummern erforderlich sind, können Sie den Benutzern eine Standard-URL geben, durch die der Registrierungsprozess automatisch gestartet wird, wenn der Benutzer auf seinem Mobilgerät darauf klickt.

Zum Ermitteln der Registrierungs-URL für Ihren Management Server rufen Sie die Registerkarte 'Mobiler Zugriff' und die Registerkarte 'Benutzer registrieren' auf. Die URL wird auf dieser Seite angezeigt.

Hinweis: *Weitere Informationen zu den beiden Modi finden Sie im Bereich Einstellungen (S. 61).*

So erstellen Sie eine Acronis Access-Registrierungseinladung:

1. Rufen Sie die Registerkarte **Mobiler Zugriff** und die Registerkarte **Benutzer registrieren** auf.

2. Drücken Sie die Schaltfläche **Registrierungseinladung senden**.
3. Geben Sie einen Active Directory-Benutzernamen oder -Gruppennamen ein und klicken Sie auf 'Suchen'. Wenn eine Gruppe ausgewählt wird, können Sie 'Hinzufügen' drücken, um die jeweilige E-Mail-Adresse in der Gruppe in der Liste einzuladender Benutzer anzuzeigen. Auf diese Weise können Sie alle Mitglieder in einer Gruppe gleichzeitig einladen. Sie können auf Wunsch auch einzelne Gruppenmitglieder ausschließen, bevor Sie die Einladungen versenden. 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. Sobald Sie den ersten Benutzer oder die erste Gruppe hinzugefügt haben, können Sie eine neue Suche starten und weitere Benutzer oder Gruppen zu der Liste hinzufügen.
5. Überprüfen Sie die Liste der einzuladenden Benutzer. Sie können nicht erwünschte Benutzer aus der Liste löschen.
6. Falls mit dem Konto eines Benutzers keine E-Mail-Adresse verknüpft ist, wird in der Spalte 'E-Mail-Adresse' die Meldung **Keine E-Mail-Adresse zugewiesen – zum Bearbeiten hier klicken** angezeigt. Sie können auf jeden dieser Einträge klicken, um manuell eine alternative E-Mail-Adresse für diesen Benutzer einzugeben. Falls für einen Benutzer **Keine E-Mail-Adresse zugewiesen** angezeigt wird, so wird dennoch eine PIN-Nummer für ihn generiert, die auf der Seite 'Benutzer registrieren' angezeigt wird. Sie müssen diese PIN-Nummer auf andere Weise an den Benutzer übermitteln, erst danach kann er den Access Mobile Client registrieren.

   Hinweis: *Falls Sie die Registrierungs-PIN-Nummern den Benutzern lieber auf manuelle Weise zukommen lassen möchten, deaktivieren Sie die Option* ***Eine Registrierungseinladung per E-Mail an jeden Benutzer mit einer spezifizierten Adresse senden****. Jede PIN-Nummer wird auf der Seite* ***Registrierungseinladungen*** *angezeigt.*

7. Wählen Sie im Feld 'Einladung verfällt in' die Anzahl von Tagen, die die Einladung gültig sein soll.
8. Wählen Sie die Anzahl der PINs, die Sie an die einzelnen Benutzer auf der Einladungsliste senden möchten. Dies kann der Fall sein, wenn der Benutzer 2 oder 3 Geräte besitzt. Der Benutzer erhält einzelne E-Mails, die jeweils eine eindeutige einmalige PIN enthalten.

   Hinweis*: Im Rahmen der Acronis Access-Lizenzierung kann jeder lizenzierte Benutzer bis zu 3 Geräte aktivieren. Jedes weitere Gerät zählt hinsichtlich der Lizenzierung als neues Gerät.*

9. Wählen Sie die Version oder Versionen des Access Mobile Clients, die die Benutzer herunterladen und auf ihrem Gerät installieren sollen. Sie können 'iOS', 'Android' oder 'Beide' wählen. Wenn Sie Acronis Access für Good Dynamics verwenden, können Sie die betreffende Option auswählen. Die Benutzer werden dann nur angewiesen, die Good Dynamics-Version des Access Mobile Clients herunterzuladen.
10. Drücken Sie 'Senden'.

    Hinweis: *Falls Sie beim Senden eine Fehlermeldung erhalten, überprüfen Sie, ob die SMTP-Einstellungen auf der Registerkarte 'SMTP' unter 'Allgemeine Einstellungen' korrekt sind. Wenn Sie* ***Sichere Verbindung*** *verwenden, überprüfen Sie außerdem, ob das von Ihnen verwendete Zertifikat mit dem Hostnamen Ihres SMTP-Servers übereinstimmt.*

Bisher bei mobilEcho 4.5 oder früher registrierte Benutzer einladen

In mobilEcho 2.X musste keine PIN-Nummer eingegeben werden, um einen Client im Client Management-System zu registrieren. Für die Migration von mobilEcho 2.X Clients auf das Acronis Access Management-System sind zwei Optionen verfügbar. Standardmäßig erlauben es von 2.X

aktualisierte mobilEcho Server den zuvor vom Server der Version 2.X verwalteten Clients, sich automatisch zu registrieren sowie in der Liste der Acronis Access **Geräte** angezeigt zu werden, ohne dass eine PIN-Nummer eingegeben werden muss. Wenn Sie sicherstellen möchten, dass alle Geräte, die auf das System zugreifen, mit einer PIN-Nummer registriert wurden, können Sie diese Einstellung deaktivieren. Wenn der Benutzer nicht über die Berechtigung **Benutzer kann Mobile Client aus der Verwaltung entfernen** verfügt, muss er in diesem Fall Acronis Access vom Gerät löschen und eine neue Kopie aus dem App Store neu installieren, bevor die Registrierung mit einer PIN-Nummer möglich ist.

Beachten Sie zudem, dass es bei Aktivierung dieser Einstellung für die automatische Registrierung möglich ist, ein iTunes-Backup eines Geräts mit einer verwalteten Version von mobilEcho 2.X oder 3.0 durchzuführen, dieses Backup auf einem neuen Gerät wiederherzustellen und, solange der betreffende Benutzer den Benutzernamen und das Kennwort für das zugehörige Konto im Active Directory besitzt, das neue Gerät automatisch und ohne PIN-Nummer in Client Management zu registrieren.

Es wird empfohlen, die Einstellung für die automatische Registrierung zu deaktivieren, wenn alle zuvor verwalteten Clients erstmals auf den Management Server zugegriffen haben. Wenn dies der Fall ist, werden sie in der Liste 'Geräte' angezeigt.

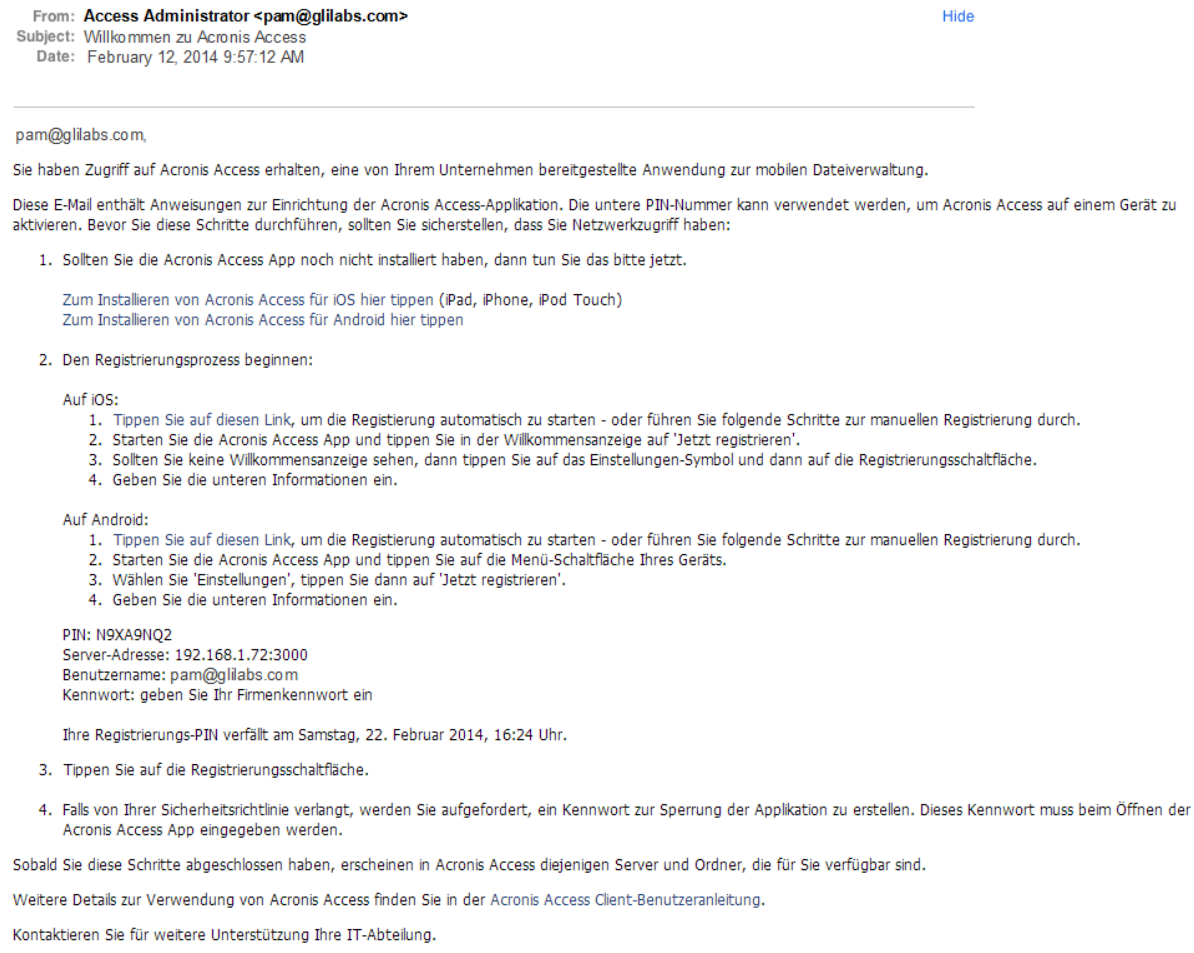
Um es zuvor bei mobilEcho 2.X Client Management registrierten mobilEcho Clients zu erlauben, sich automatisch zu registrieren, nachdem der Server von mobilEcho Client Management auf Acronis Access Server aktualisiert wurde, aktivieren Sie die Einstellung **Zuvor von Servern der Version 2.X verwalteten sowie auf neuen Geräten wiederhergestellten mobilEcho Clients erlauben, sich automatisch ohne PIN zu registrieren**.

1.3.2 Benutzerseitiger Verwaltungsregistrierungsvorgang

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

1.4 Mobile Geräte verwalten

Sobald ein Access Mobile Client beim Acronis Access-Server registriert wurde, wird das mobile Gerät in der Liste **Geräte** angezeigt. Diese Liste gibt detaillierte Statusinformationen zu jedem Gerät an, das mit einer PIN-Nummer aktiviert oder zuvor von einem mobilEcho Server der Version 2.1 oder früher verwaltet wurde, sofern diese Option aktiviert ist.

Zeigt alle verwalteten Geräte mitsamt zugehöriger Informationen an. Sie können Geräte darüber hinaus löschen oder das App-Kennwort ändern.

- **Anzeigename** – der vollständige Name des Benutzers im Active Directory (AD)
- **Benutzername** – der Konto-Benutzername des Benutzers im AD
- **Domain** – die Domäne, in der das AD-Konto des Benutzers Mitglied ist
- **Gerätename** – der vom Benutzer festgelegte Gerätename
- **Modell** – das Modell/der Typ des Geräts
- **Betriebssystem** – Betriebssystemversion des Geräts.
- **Version** – Version der Acronis Access Mobile-App auf dem Gerät.

- **Status** – Status der Acronis Access Mobile-App auf dem Gerät.
- **Letzter Kontakt** – Datum und Uhrzeit des letzten Kontakts zwischen dem Management Server und dem Client.
- **Richtlinie** – Name und Link der Verwaltungsrichtlinie für den Benutzer
- **Aktionen**
  - **Weitere Informationen –** Hiermit zeigen Sie weitere Details zum Gerät an, darunter die eindeutige Geräte-ID und ein bearbeitbares Notizenfeld für das Gerät.
  - **App-Kennwort zurücksetzen –** Das Kennwort zum Sperren der Acronis Access Mobile-Applikation auf dem Gerät remote zurücksetzen. Hier geben Sie den Code ein, den Sie von der Acronis Access Mobile-App erhalten, erzeugen einen Bestätigungscode und geben diesen in der App auf dem Gerät ein.
  - **Remote-Löschung** – Wenn das Gerät das nächste Mal eine Verbindung mit dem Management Server herstellt, werden alle Dateien in der Acronis Access Mobile-App (und deren Einstellungen) gelöscht. Daten anderer Applikationen oder des Betriebssystems sind nicht betroffen.
  - **Aus Liste entfernen** – Hierdurch wird das Gerät aus der **Geräteliste** entfernt. Die Verwaltung für dieses Gerät wird aufgehoben, ohne den gesamten Geräteinhalt zu löschen. Damit werden meist Geräte entfernt, bei denen von keinem weiteren Kontakt mit dem Acronis Access Client Management Server auszugehen ist. Wenn Sie 'Mobilen Clients, die auf neuen Geräten wiederhergestellt wurden, eine automatische Registrierung ohne PIN erlauben' aktiviert haben, wird ein aus der Liste entferntes Gerät automatisch erneut angezeigt und verwaltet, sobald es den Server kontaktiert.

Themen

1.4.1 Kennwort-Resets für die Remote-Applikation durchführen

Der Access Mobile Client kann mit einem Kennwort zum Sperren der Applikation geschützt werden, das beim Start von Acronis Access eingegeben werden muss. Wenn der Benutzer dieses Kennwort vergisst, kann er nicht auf Acronis Access zugreifen. Das Kennwort der Access Mobile Client-App ist unabhängig vom Kennwort für das Active Directory-Konto des Benutzers.

Wenn ein Kennwort verloren geht, hat der Benutzer nur die Möglichkeit, Acronis Access vom Gerät zu deinstallieren und erneut zu installieren. Damit werden vorhandene Daten und Einstellungen gelöscht, sodass die Sicherheit gewahrt bleibt. Die Benutzer haben jedoch wahrscheinlich erst dann wieder Zugriff auf Acronis Access-Server, wenn sie eine neue Verwaltungseinladung erhalten.

Um diese Probleme zu vermeiden, kann der Acronis Access Server das Kennwort für die Remote-Applikation zurücksetzen.

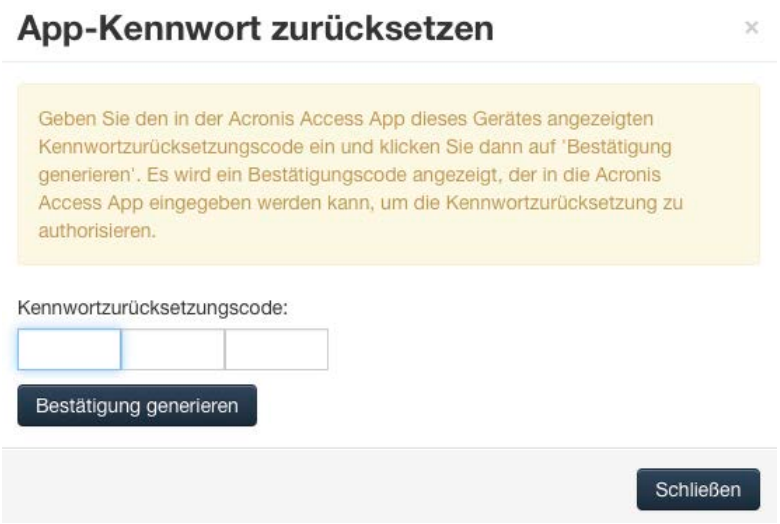
Kennwort für die Applikation zurücksetzen

Acronis Access-Gerätedateien wurden stets mit der Dateiverschlüsselung Apple Data Protection (ADP) geschützt. Um Dateien auf Geräten, für die iTunes- und iCloud-Backups durchgeführt werden, und Geräte ohne aktivierte Sperrcodes auf Geräteebene weiter zu schützen und die Sicherheit generell zu verbessern, wurde eine zweite Ebene einer benutzerdefinierbaren

Vollzeitverschlüsselung eingeführt, die von der Acronis Access-App direkt angewendet wird. Ein Aspekt dieser Verschlüsselung besteht darin, dass es in Acronis Access 5.0 und höher nicht mehr möglich ist, das Kennwort zum Sperren der Anwendung über Datenfunk (Over the Air) zurückzusetzen. Stattdessen müssen zwischen dem Gerätebenutzer und dem Acronis Access-IT-Administrator ein Kennwortzurücksetzungscode und ein Bestätigungscode ausgetauscht werden, damit Acronis Access seine Einstellungsdatenbank entschlüsseln und der Benutzer ein neues App-Kennwort festlegen kann.

So setzen Sie ein Kennwort für die Applikation Acronis Access für iOS oder Android zurück:

1. Ein Endbenutzer verlangt das Zurücksetzen des Kennworts für die Acronis Access-App und übermittelt Ihnen den **Kennwortzurücksetzungscode**.
2. Rufen Sie die Registerkarte **Mobiler Zugriff** auf.
3. Rufen Sie die Registerkarte **Geräte** auf.
4. Suchen Sie auf der Seite **Geräte verwalten** nach dem Gerät, dessen Kennwort zurückgesetzt werden soll, und klicken Sie dann auf **Aktionen**.
5. Drücken Sie **App-Kennwort zurücksetzen...**.
6. Geben Sie den vom Benutzer übermittelten **Kennwortzurücksetzungscode** ein und klicken Sie dann auf **Bestätigung erzeugen**.
7. Geben Sie den angezeigten **Bestätigungscode** mündlich oder per E-Mail an den Benutzer weiter.
8. Der Benutzer gibt diesen Code dann in das entsprechende Dialogfeld für das Zurücksetzen des App-Kennworts ein und wird dann aufgefordert, ein neues Kennwort festzulegen. Wenn er diesen Prozess abbricht, ohne ein geeignetes App-Kennwort festzulegen, wird ihm der Zugriff auf den Access Mobile Client weiterhin verweigert, und er muss den Prozess zum Zurücksetzen des App-Kennworts wiederholen.



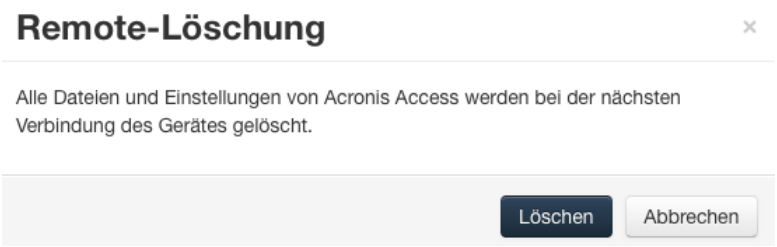
1.4.2 Remote-Löschungen durchführen

Mit Acronis Access Client Management kann eine Remote-Löschung einer Access Mobile Client-Applikation durchgeführt werden. Bei dieser selektiven Remote-Löschung werden alle in der Acronis Access-App lokal gespeicherten oder zwischengespeicherten Dateien entfernt. Alle App-Einstellungen werden auf die vorherigen Standardeinstellungen zurückgesetzt, und alle in der App konfigurierten Server werden entfernt.

Remote-Löschvorgang in Warteschlange stellen

1. Öffnen Sie die Registerkarte **Mobiler Zugriff**.
2. Rufen Sie die Registerkarte **Geräte** auf.
3. Ermitteln Sie auf der Seite **Geräte verwalten** das Gerät, für das Sie einen Remote-Löschvorgang aufrufen möchten, und drücken Sie die Schaltfläche **Aktionen**.
4. Drücken Sie **Remote-Löschung...**
5. Bestätigen Sie die Remote-Löschung durch Drücken von **Remote-Löschung in Warteschlange stellen**.
6. In der **Status**leiste für das Gerät wird der Status **Remote ausstehend** angezeigt. Wenn der Remote-Löschvorgang vom Gerät akzeptiert wurde, ändert sich der **Status** entsprechend.

Hinweis: *Remote-Löschvorgänge können jederzeit abgebrochen werden, bevor der Client das nächste Mal eine Verbindung zum Management-Server herstellt. Diese Option wird im* ***Aktionsmenü*** *angezeigt, nachdem ein Remote-Löschvorgang aufgerufen wurde.*



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.

1.5 Gateway Server verwalten

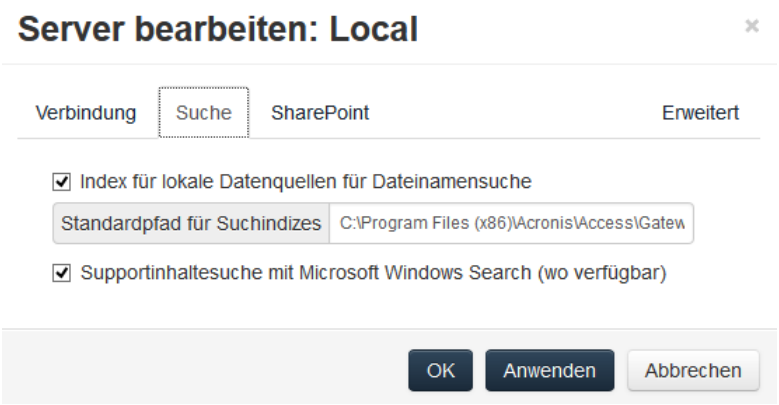
Der Acronis Access Gateway Server wird von den Access Mobile Clients kontaktiert. Dieser Server verwaltet den Zugriff und die Bearbeitung von Dateien und Ordnern auf Dateiservern, in SharePoint-Repositories bzw. Sync & Share-Volumes. Der Gateway Server ist die "Toreinfahrt" für mobile Clients zu ihren Dateien.

Der Acronis Access Server kann einen oder mehrere Gateway Server über dieselbe Managementkonsole verwalten und konfigurieren. Die verwalteten Gateway Server erscheinen im Bereich **Gateway Server** des Menüs **Mobiler Zugriff**.

- **Typ** – Zeigt den Gateway-Typ an; im Moment kann dies nur der Servertyp sein.
- **Name** – Name, den Sie dem Gateway bei dessen Erstellung geben.
- **Adresse** – DNS-Name oder IP-Adresse des Gateways.
- **Version** – Zeigt die Version des Acronis Access Gateway Servers an.
- **Status** – Gibt an, ob der Server online oder offline ist.
- **Aktive Sitzungen** – Anzahl der gegenwärtig aktiven Sitzungen auf diesem Gateway Server.
- **Verwendete Lizenzen** – Anzahl der verwendeten Lizenzen und Anzahl der verfügbaren Lizenzen.
- **Lizenz** – Zeigt die gegenwärtig vom Gateway Server verwendeten Lizenzen an.

Neue Gateway Server können über die Schaltfläche **Neue Gateway Server hinzufügen** registriert werden. Über das Aktionsmenü des jeweiligen Gateway Servers können Sie weitere Einzelheiten zu einem Server und dessen Leistung erfahren, die Konfiguration bearbeiten, Zugriffsbeschränkungen für den Server ändern, Lizenzen für den Server ändern und den Gateway Server entfernen.

Suche



Index für lokale Datenquellen für Dateinamensuche

Standardmäßig ist die indizierte Suche auf allen Gateway-Servern aktiviert. Sie können die indizierte Suche getrennt nach Gateway-Server über das Dialogfeld 'Server bearbeiten' aktivieren oder deaktivieren.

Standardpfad

Auf einem eigenständigen Server speichert Acronis Access Indexdateien standardmäßig im Suchindex-Verzeichnis im Ordner der Acronis Access Gateway Server-Applikation. Wenn die Indexdateien in einem anderen Verzeichnis gespeichert werden soll, geben Sie den gewünschten Ordnerpfad ein.

Supportinhaltssuche mit Microsoft Windows Search (wo verfügbar)

Die Inhaltssuche in freigegebenen Dateien ist standardmäßig aktiviert. Sie kann über diese Option aktiviert bzw. deaktiviert werden. Sie können die Inhaltssuche getrennt nach Gateway-Server über das Dialogfeld 'Server bearbeiten' aktivieren oder deaktivieren.

Für die Inhaltssuche muss nicht nur diese Einstellung aktiviert sein, sondern auf dem Acronis Access Gateway Server muss auch die Applikation Microsoft Windows Search installiert und so konfiguriert sein, dass alle Datenquellen indiziert werden, für welche die Inhaltssuche aktiviert ist. Die Windows-Suche ist in Windows Vista integriert. Eine zusätzliche Installation ist nicht erforderlich. Sie ist ebenfalls in Windows Server 2008 integriert, ist jedoch in der Standardeinstellung nicht aktiviert. Um sie zu aktivieren, fügen Sie die Rolle namens 'Dateidienste' im Server-Manager und lassen Sie den Windows-Suchdienst aktivieren. Die Windows-Suche kann unter Windows 2003 Server und Windows XP durch Ausführen von Windows Update installiert werden. Sie wird als optionale Installationsoption aufgeführt. Nach der Installation kann die Windows-Suche konfiguriert werden, um alle erforderlichen Datenquellen zu indizieren. Klicken Sie hierzu in der Startleiste mit der rechten Maustaste auf das Symbol der Windows-Suche und wählen Sie 'Windows-Suchoptionen' aus. Sie können Windows-Inhaltssuchvorgänge in Windows-Freigabeweiterleitungen ausführen. Dazu müssen sich die Remote-Maschinen allerdings in derselben Domain befinden wie der Gateway Server.

Hinweis: *Der Volume-Pfad der Datenquelle muss ein Host-Name oder vollständig qualifizierter Name sein, damit die Inhaltssuche für Windows-Freigabeweiterleitungen verwendet werden kann. IP-Adressen werden von der Windows-Suche nicht unterstützt.*

SharePoint

Für die allgemeine Unterstützung von SharePoint ist die Eingabe dieser Zugangsdaten optional. Sie ist aber erforderlich, um Websitesammlungen aufzulisten. Beispiel: Sie verfügen über zwei Websitesammlungen: http://sharepoint.beispiel.com und http://sharepoint.beispiel.com/SeparateSammlung. Ohne die Eingabe der Zugangsdaten sehen Sie, wenn Sie ein Volume mit Verweis auf http://sharepoint.beispiel.com erstellen, beim Auflisten des Volumes nicht den Ordner mit dem Namen SeparateSammlung. Das Konto muss vollen Lesezugriff auf die Webanwendung haben.

Themen

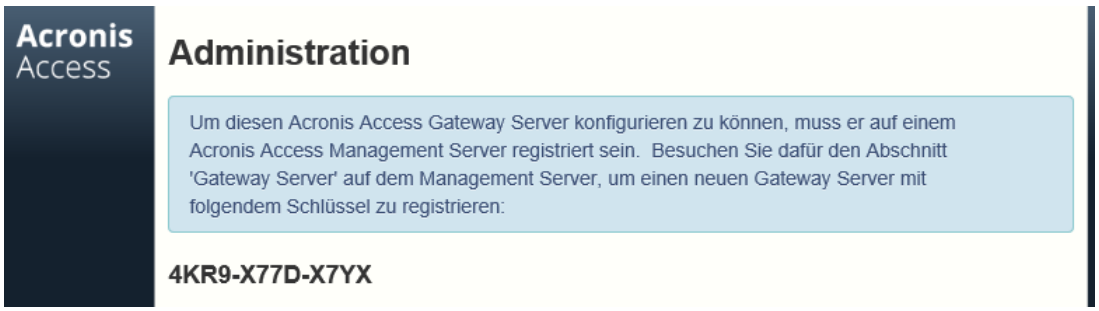
1.5.1 Neue Gateway-Server registrieren

Mit Ausnahme der automatischen Registrierung eines Gateway-Servers, der auf dem gleichen Rechner wie die Management-Webapplikation ausgeführt wird, ist die Registrierung eines Gateway-Servers ein manueller Prozess, der mehrere Schritte einschließt.

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

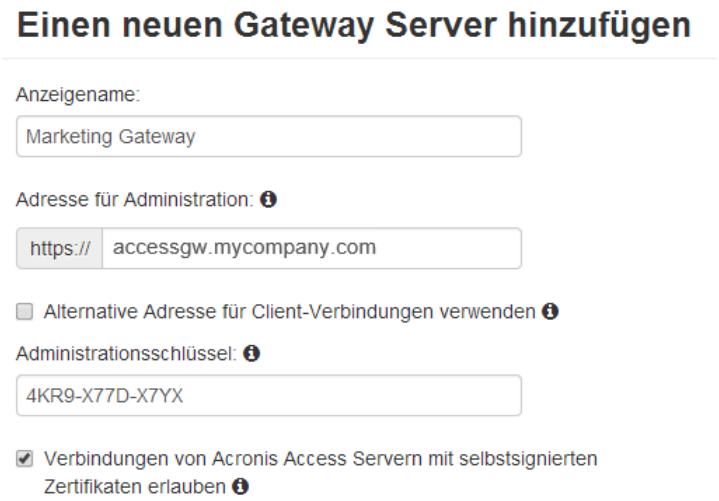
   Hinweis: *Der Port 443 ist der Standard-Port. Falls Sie den Standard-Port geändert haben, geben Sie im Anschluss an localhost Ihre Portnummer ein.*

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.*

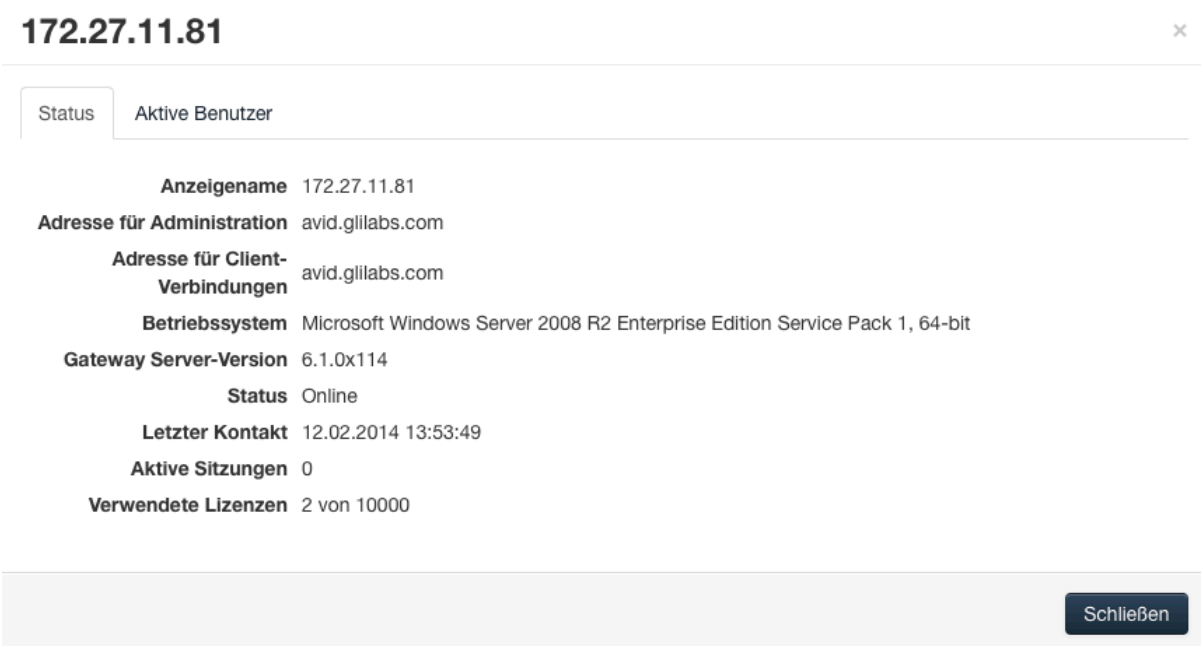
10. Geben Sie den **Administrationsschlüssel** ein.
11. Erlauben Sie bei Bedarf Verbindungen mit selbstsignierten Zertifikaten zu diesem Gateway. Aktivieren Sie dazu die Option **Verbindungen von Acronis Access Servern mit selbstsignierten Zertifikaten erlauben**.
12. Drücken Sie auf **Speichern**.

Nachdem Sie Ihren Gateway-Server registriert haben, können Sie individuelle Zugriffsbeschränkungen für diesen Gateway-Server konfigurieren. Weitere Informationen hierzu finden Sie im Abschnitt Gateway-Server bearbeiten (S. 43).

1.5.2 Server-Details

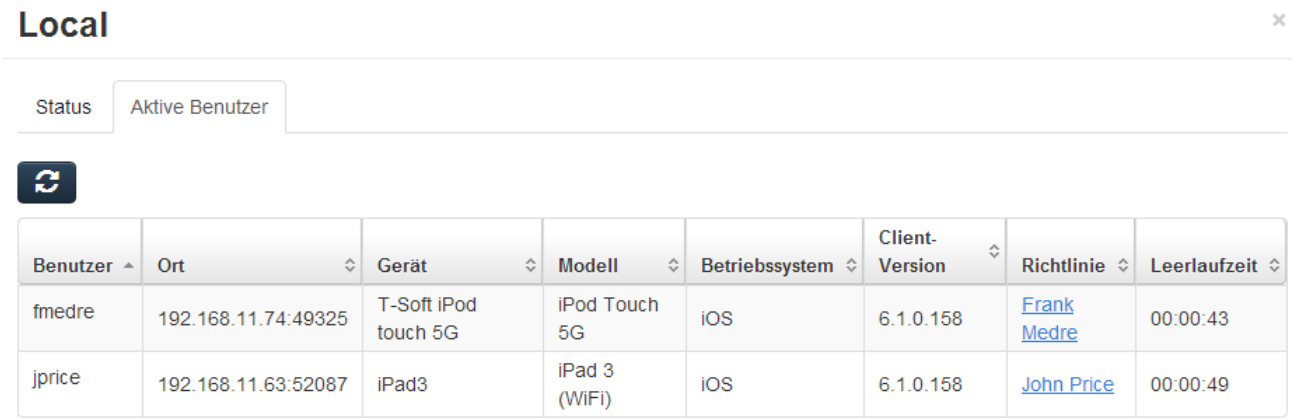
Auf der Seite **Details** eines Gateway Servers erhalten Sie zahlreiche nützliche Informationen zu dem spezifischen Server und seinen Benutzern.

Status



Im Abschnitt 'Status' erhalten Sie Informationen zum Gateway Server selbst. Darunter fallen Informationen wie das Betriebssystem, der Lizenztyp, die Anzahl der verwendeten Lizenzen, die Version des Gateway Servers u. v. m.

Aktive Benutzer



Zeigt eine Tabelle aller Benutzer an, die gegenwärtig auf diesem Gateway Server aktiv sind.

- **Benutzer** – Zeigt den vollständigen Namen des Benutzers im Active Directory (AD) an.
- **Speicherort** – Zeigt die IP-Adresse des Geräts an.
- **Gerät** – Zeigt den Namen an, der diesem Gerät vom Benutzer zugewiesen wurde.
- **Modell** – Zeigt den Typ und das Modell des Geräts an.
- **Betriebssystem** – Zeigt das Betriebssystem des Geräts an.
- **Client-Version** – Zeigt die Version der auf dem Gerät installierten Acronis Access-App.

- **Richtlinie** – Zeigt die Richtlinie für das vom Gerät verwendete Konto an.
- **Leerlaufzeit** – Zeigt an, wie lange der Benutzer mit dem Gateway verbunden ist.

1.5.3 Gateway Server bearbeiten

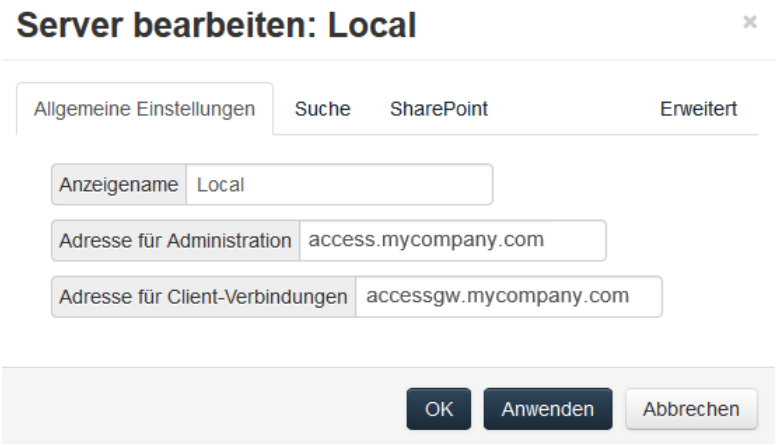
Zugriffsbeschränkungen

Sie können entweder die unter Richtlinien (S. 8) festgelegten Standardzugriffsbeschränkungen verwenden oder eigene Beschränkungen für jeden Gateway Server festlegen.

Benutzerdefinierte Zugriffsbeschränkungen für diesen Gateway Server festlegen

1. Drücken Sie auf den Abwärts-Pfeil neben der Schaltfläche **Details**.
2. Wählen Sie **Zugriffsbeschränkungen** aus.
3. Rufen Sie die Registerkarte **Benutzerdefinierte Einstellungen verwenden** auf.
4. Wählen Sie die gewünschten Zugriffsbeschränkungen für diesen Gateway Server aus.
5. Drücken Sie auf **Anwenden**.

Allgemeine Einstellungen

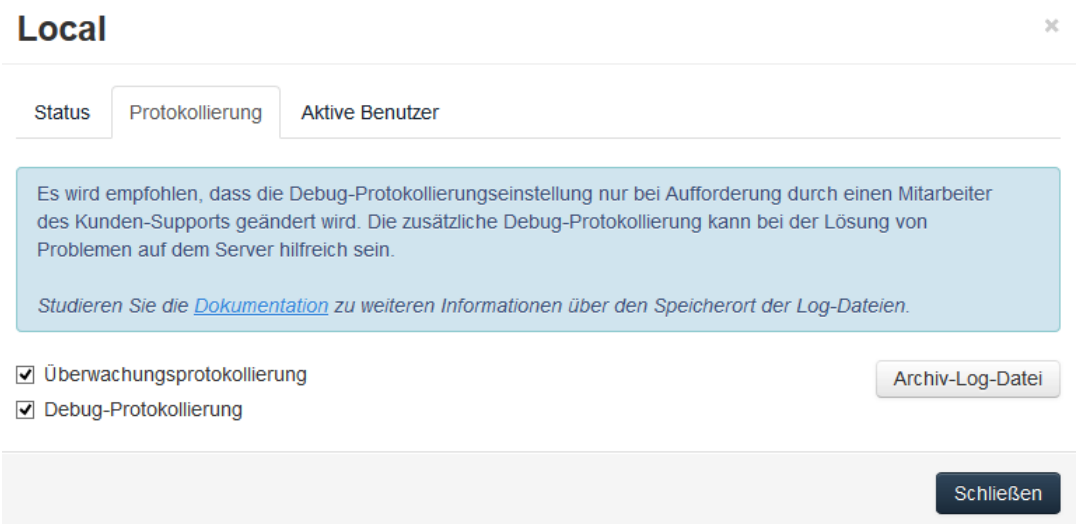


Anzeigename – Legt den Anzeigenamen für den Gateway Server fest.

Adresse für Administration – Legt die Adresse fest, unter der der Gateway Server vom Acronis Access Server erreicht werden kann.

Adresse für Client-Verbindungen – Legt die Adresse fest, unter der mobile Clients eine Verbindung zum Gateway Server herstellen können.

Protokollierung



Im Abschnitt 'Protokollierung' können Sie festlegen, ob die Protokollierungsereignisse von diesem spezifischen Gateway Server im Überwachungsprotokoll angezeigt werden. Außerdem können Sie dort die Debug-Protokollierung für diesen Server aktivieren.

So aktivieren Sie die Überwachungsprotokollierung für einen bestimmten Gateway Server:

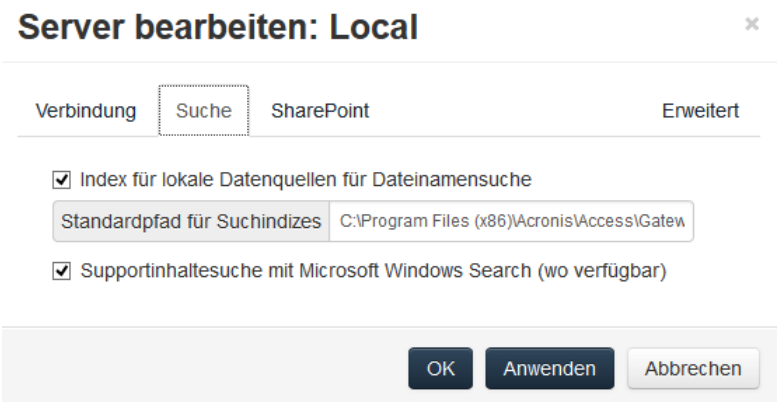
1. Rufen Sie die Weboberfläche auf.
2. Melden Sie sich als Administrator an.
3. Öffnen Sie die Registerkarte **Mobiler Zugriff**.
4. Öffnen Sie die Registerkarte **Gateway Server**.
5. Suchen Sie den Server, für den Sie **Audit Logs aktivieren möchten.**
6. Drücken Sie die Schaltfläche **Details**.
7. Aktivieren Sie im Bereich **Protokollierung** die Option **Überwachungsprotokollierung**.
8. Drücken Sie die Schaltfläche **Speichern**.

So aktivieren Sie die Debug-Protokollierung für einen bestimmten Gateway Server:

Hinweis: *Die Debug-Logs werden standardmäßig in folgendem Ordner gespeichert:* ***`C:\Program Files (x86)\Acronis\Access\Gateway Server\Logs\AcronisAccessGateway`***

1. Rufen Sie die Weboberfläche auf.
2. Melden Sie sich als Administrator an.
3. Öffnen Sie die Registerkarte **Mobiler Zugriff**.
4. Rufen Sie die Registerkarte **Gateway Server** auf.
5. Suchen Sie den Server, für den Sie die **Debug-Protokollierung aktivieren möchten.**
6. Klicken Sie auf die Schaltfläche **Details**.
7. Aktivieren Sie im Bereich **Protokollierung** die Option **Debug-Protokollierung**.
8. Klicken Sie auf die Schaltfläche **Speichern**.

Suche



Index für lokale Datenquellen für Dateinamensuche

Standardmäßig ist die indizierte Suche auf allen Gateway-Servern aktiviert. Sie können die indizierte Suche getrennt nach Gateway-Server über das Dialogfeld 'Server bearbeiten' aktivieren oder deaktivieren.

Standardpfad

Auf einem eigenständigen Server speichert Acronis Access Indexdateien standardmäßig im Suchindex-Verzeichnis im Ordner der Acronis Access Gateway Server-Applikation. Wenn die Indexdateien in einem anderen Verzeichnis gespeichert werden soll, geben Sie den gewünschten Ordnerpfad ein.

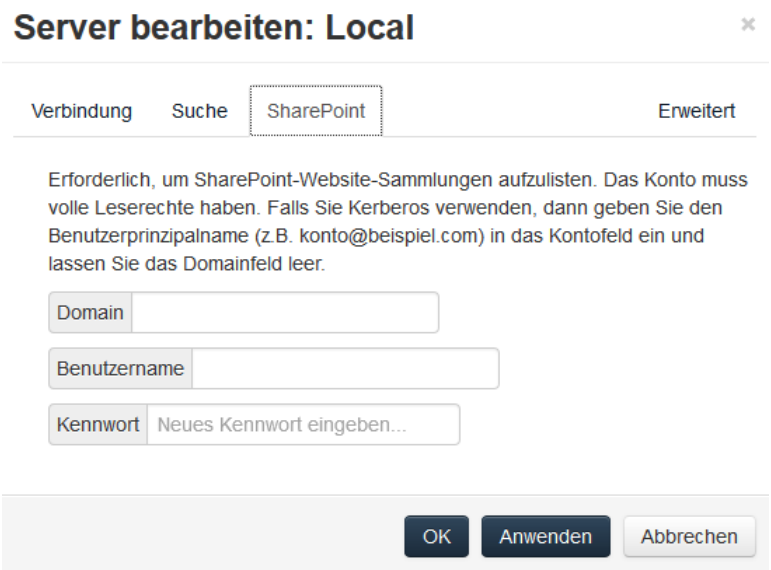
Supportinhaltssuche mit Microsoft Windows Search (wo verfügbar)

Die Inhaltssuche in freigegebenen Dateien ist standardmäßig aktiviert. Sie kann über diese Option aktiviert bzw. deaktiviert werden. Sie können die Inhaltssuche getrennt nach Gateway-Server über das Dialogfeld 'Server bearbeiten' aktivieren oder deaktivieren.

Für die Inhaltssuche muss nicht nur diese Einstellung aktiviert sein, sondern auf dem Acronis Access Gateway Server muss auch die Applikation Microsoft Windows Search installiert und so konfiguriert sein, dass alle Datenquellen indiziert werden, für welche die Inhaltssuche aktiviert ist. Die Windows-Suche ist in Windows Vista integriert. Eine zusätzliche Installation ist nicht erforderlich. Sie ist ebenfalls in Windows Server 2008 integriert, ist jedoch in der Standardeinstellung nicht aktiviert. Um sie zu aktivieren, fügen Sie die Rolle namens 'Dateidienste' im Server-Manager und lassen Sie den Windows-Suchdienst aktivieren. Die Windows-Suche kann unter Windows 2003 Server und Windows XP durch Ausführen von Windows Update installiert werden. Sie wird als optionale Installationsoption aufgeführt. Nach der Installation kann die Windows-Suche konfiguriert werden, um alle erforderlichen Datenquellen zu indizieren. Klicken Sie hierzu in der Startleiste mit der rechten Maustaste auf das Symbol der Windows-Suche und wählen Sie 'Windows-Suchoptionen' aus. Sie können Windows-Inhaltssuchvorgänge in Windows-Freigabeweiterleitungen ausführen. Dazu müssen sich die Remote-Maschinen allerdings in derselben Domain befinden wie der Gateway Server.

Hinweis: *Der Volume-Pfad der Datenquelle muss ein Host-Name oder vollständig qualifizierter Name sein, damit die Inhaltssuche für Windows-Freigabeweiterleitungen verwendet werden kann. IP-Adressen werden von der Windows-Suche nicht unterstützt.*

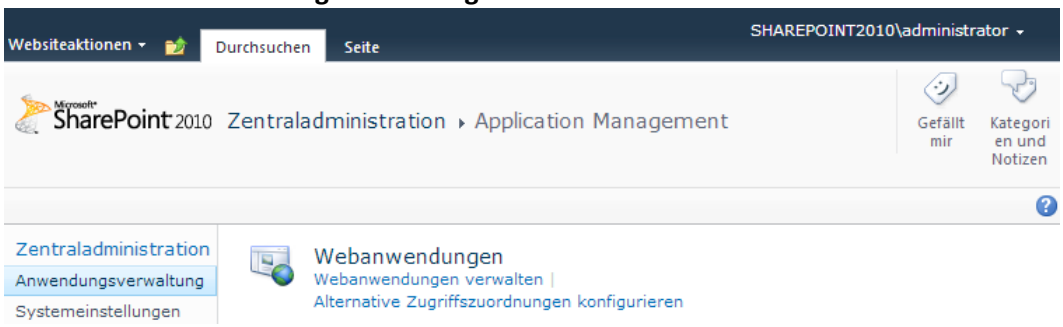
SharePoint



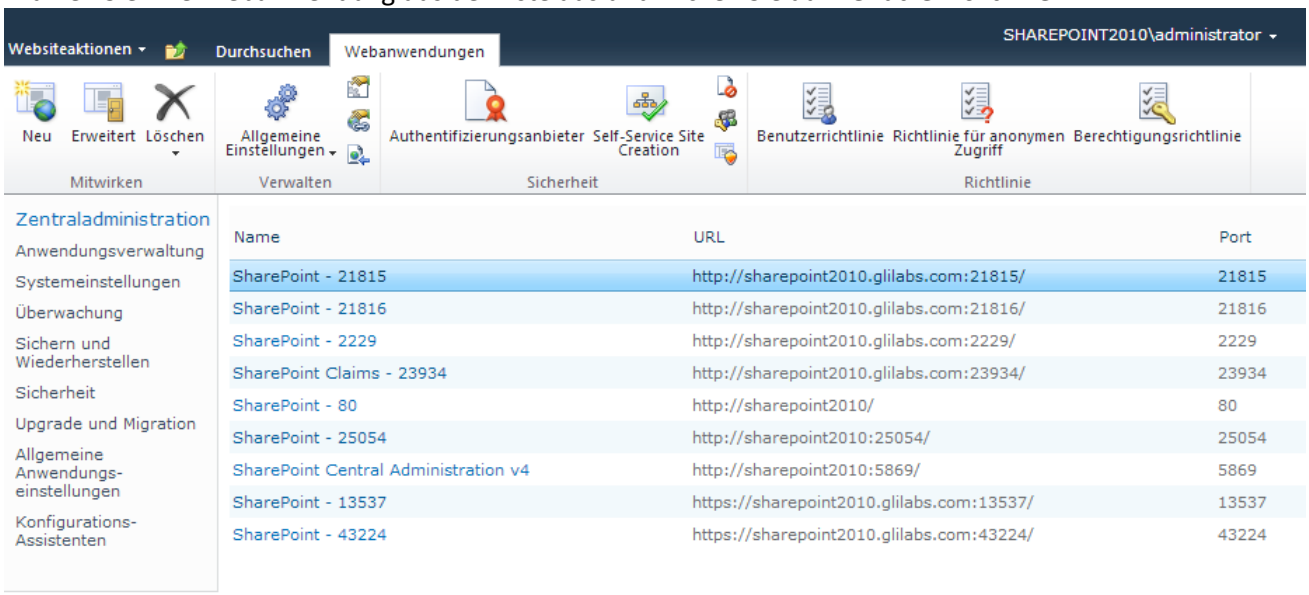
Für die allgemeine Unterstützung von SharePoint ist die Eingabe dieser Zugangsdaten optional. Sie ist aber erforderlich, um Websitesammlungen aufzulisten. Beispiel: Sie verfügen über zwei Websitesammlungen: http://sharepoint.beispiel.com und http://sharepoint.beispiel.com/SeparateSammlung. Ohne die Eingabe der Zugangsdaten sehen Sie, wenn Sie ein Volume mit Verweis auf http://sharepoint.beispiel.com erstellen, beim Auflisten des Volumes nicht den Ordner mit dem Namen SeparateSammlung. Das Konto muss vollen Lesezugriff auf die Webanwendung haben.

Führen Sie die folgenden Schritte (für SharePoint 2010) aus, um für Ihr Konto den vollständigen Lesezugriff zu konfigurieren:

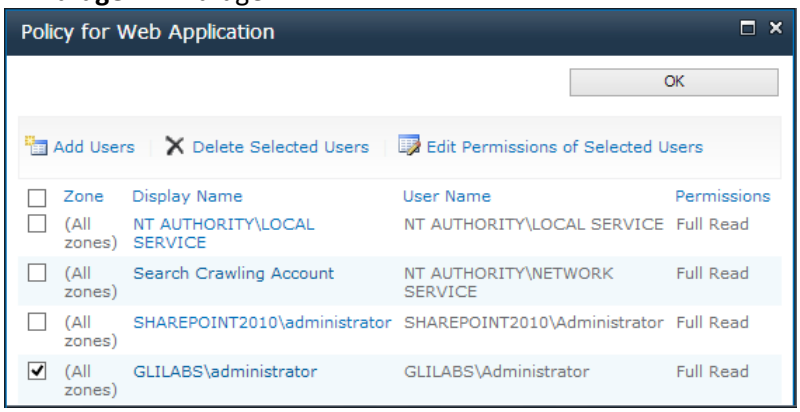
1. Öffnen Sie die **SharePoint-Zentraladministration**.
2. Klicken Sie auf **Anwendungsverwaltung**.



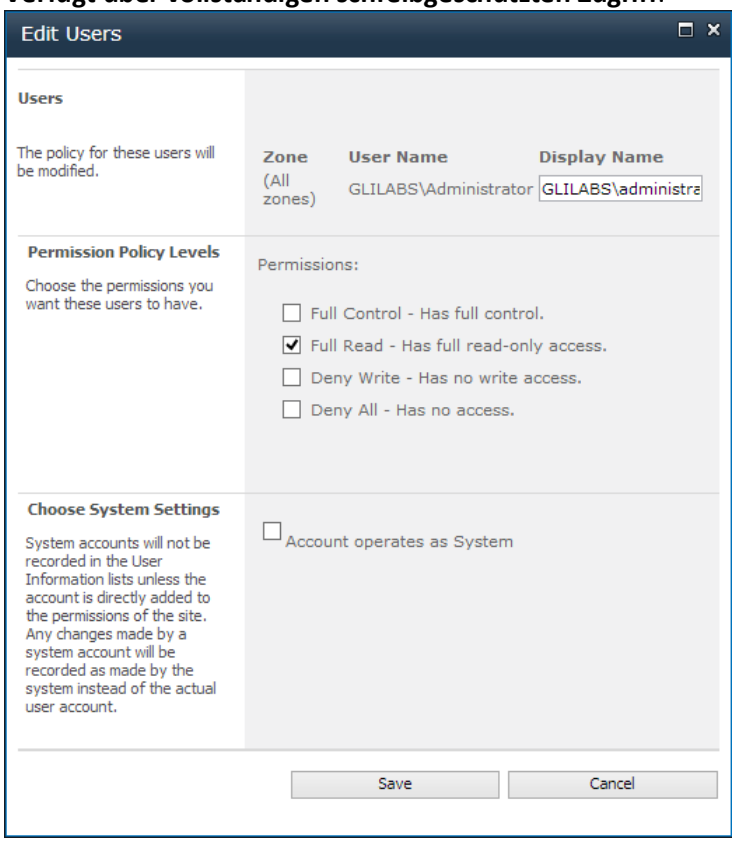
3. Klicken Sie unter **Webanwendungen** auf **Webanwendungen verwalten**.
4. Wählen Sie Ihre Webanwendung aus der Liste aus und klicken Sie auf **Benutzerrichtlinie**.



5. Aktivieren Sie das Kontrollkästchen für den Benutzer, dem Sie Berechtigungen gewähren möchten, und klicken Sie dann auf **Berechtigungen der ausgewählten Benutzer bearbeiten**. Taucht der Benutzer in der Liste nicht auf, können Sie ihn durch Anklicken von **Benutzer hinzufügen** hinzufügen.



6. Aktivieren Sie unter **Richtlinienstufen für Berechtigungen** das Kontrollkästchen **Alles lesen – Verfügt über vollständigen schreibgeschützten Zugriff**.



7. Drücken Sie auf **Speichern**.

Erweitert

***Hinweis**: Es wird empfohlen, dass diese Einstellungen nur bei Aufforderung durch einen Mitarbeiter des Kunden-Supports geändert werden.*

- **Nicht verfügbare Elemente verbergen** – Wenn aktiviert, Dateien und Ordner, für die der Benutzer keine Leseberechtigung besitzt, werden nicht angezeigt.
- **Nicht verfügbare Elemente auf Freigabeweiterleitungen verbergen** - Wenn aktiviert, Dateien und Ordner auf einer Netzwerk-Freigabeweiterleitung, für die der Benutzer keine Leseberechtigung besitzt, werden nicht angezeigt.

  ***Hinweis**: Die Aktivierung dieser Funktion kann die Navigation in den Ordnern erheblich beeinträchtigen.*

- **Nicht verfügbare SharePoint-Websites verbergen** - Wenn aktiviert, SharePoint-Websites, für die der Benutzer nicht über die erforderlichen Berechtigungen verfügt, werden nicht angezeigt.
- **Minimale Android-Client-Version** - Wenn aktiviert, Benutzer, die eine Verbindung mit diesem Gateway herstellen, benötigen diese oder eine spätere Version der Acronis Access-Android-Client-App.
- **Minimale iOS-Client-Version** - Wenn aktiviert, Benutzer, die eine Verbindung mit diesem Gateway herstellen, benötigen diese oder eine spätere Version der Acronis Access-iOS-Client-App.

- **Kerberos für SharePoint-Authentifizierung verwenden** - Wenn der SharePoint-Server eine Kerberos-Authentifizierung verlangt, müssen Sie diese Einstellung aktivieren. Außerdem müssen Sie ein Update des Active Directory-Computerobjekts für den oder die Windows-Server vornehmen, auf dem oder denen die Gateway Server-Software ausgeführt wird. Der Acronis Access Windows-Server muss die Berechtigung erhalten, delegierte Zugangsdaten zu Ihrem SharePoint-Server für Ihre Benutzer anzuzeigen. Kerberos-Delegierung auf Acronis Access-Windows-Server aktivieren:
  1. Suchen Sie in **Active Directory-Benutzer und -Computer** den oder die Windows-Server, auf dem oder denen der Gateway Server installiert ist. Sie befinden sich meist im Ordner **Computer**.
  2. Öffnen Sie das Fenster **Eigenschaften** für den Windows-Server und wählen Sie die Registerkarte **Delegierung**.
  3. Wählen Sie **Computer bei Delegierungen angegebener Dienste vertrauen**.
  4. Wählen Sie **Beliebiges Authentifizierungsprotokoll verwenden**, dies ist für die Aushandlung mit dem SharePoint-Server erforderlich.
  5. Sie müssen jetzt SharePoint-Server hinzufügen, auf die die Benutzer mit Acronis Access zugreifen können sollen. Wenn Ihre SharePoint-Implementierung aus mehreren Knoten mit Lastenausgleich besteht, müssen Sie dieser Liste zugelassener Computer jeden SharePoint-/Windows-Knoten hinzufügen. Klicken Sie auf **Hinzufügen**, um in AD nach diesen Windows-Computern zu suchen und sie hinzuzufügen. Für jeden Computer muss nur der Diensttyp 'http' ausgewählt werden.

  Hinweis: *Warten Sie 15 bis 20 Minuten, bis diese Änderung in AD propagiert und angewendet wurde. Testen Sie erst dann die Client-Verbindung. Die Änderung wird nicht sofort wirksam.*

- **Verbindungen zu SharePoint-Servern mit selbstsignierten Zertifikaten erlauben** - Wenn aktiviert, Ermöglicht Verbindungen von diesem Gateway zu SharePoint-Servern mithilfe selbstsignierter Zertifikate.
- **Verbindungen zu Acronis-Servern mit selbstsignierten Zertifikaten erlauben** - Wenn aktiviert, Ermöglicht Verbindungen von diesem Gateway zu Acronis Access-Servern mithilfe selbstsignierter Zertifikate.
- **Verbindungen von Acronis-Servern mit selbstsignierten Zertifikaten erlauben** - Wenn aktiviert, Ermöglicht Verbindungen zu diesem Gateway von Acronis Access-Servern mithilfe selbstsignierter Zertifikate.
- **Versteckte SMB-Freigaben anzeigen** - Wenn aktiviert, Zeigt den Benutzern versteckte SMB-Systemfreigaben an.
- **Sitzungszeitlimit in Minuten für Client** - Legt die Zeit fest, nach der ein inaktiver Benutzer zwangsweise vom Gateway Server abgemeldet wird.
- **Benutzerprinzipalname (UPN) zur Authentifizierung an SharePoint-Servern verwenden** - Ist diese Option aktiviert, können Benutzer ihren Benutzerprinzipalnamen (z.B. hristo@glilabs.com) für die Authentifizierung an SharePoint-Servern verwenden. Andernfalls verwenden sie für die Authentifizierung die Kombination Domäne/Benutzername (z.B. glilabs/hristo).

1.5.4 Gateway-Server lizenzieren

Informationen zur Lizenzierung Ihrer Gateway-Server finden Sie unter Lizenzierung (S. 86).

1.5.5 Cluster-Gruppen

Ab Acronis Access 5.1 haben Sie die Möglichkeit, eine Cluster-Gruppe von Gateway Servern zu erstellen.

Eine Cluster-Gruppe ist eine Sammlung von Gateway Servern mit derselben Konfiguration. Auf diese Weise können Sie alle Gateways in dieser Gruppe gleichzeitig steuern, ohne dieselben Einstellungen auf jedem Gateway einzeln konfigurieren zu müssen. Diese Server befinden sich normalerweise hinter einem Lastenausgleichsmodul, um mobilen Clients eine hohe Verfügbarkeit und Skalierbarkeit zu bieten.

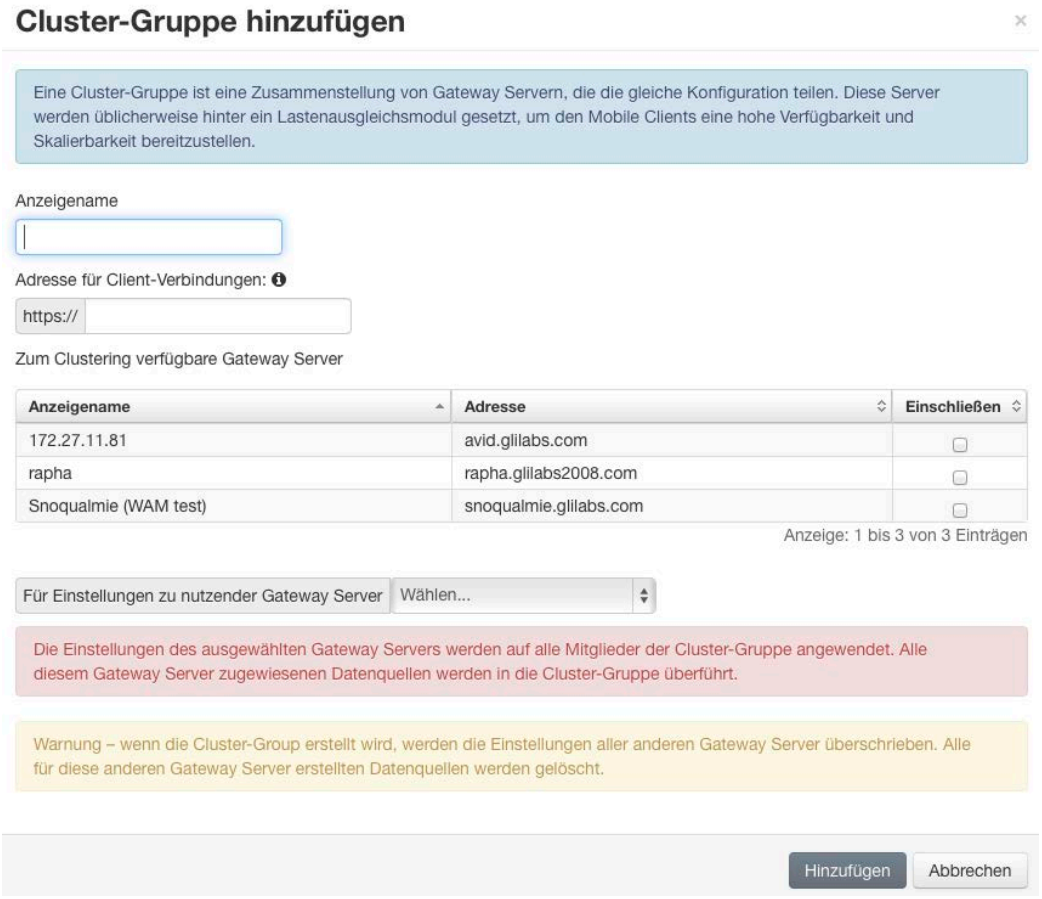
Für eine geclusterte Gateway-Konfiguration benötigen Sie ein Lastenausgleichsmodul, mindestens zwei Gateways und einen Acronis Access Server. Alle Gateway Server sollten in der Weboberfläche von Acronis Access einer Cluster-Gruppe hinzugefügt und hinter dem Lastenausgleichsmodul platziert werden. Der Acronis Access Server fungiert als Management Server und als Server, bei dem sich mobile Clients in der Client-Verwaltung registrieren. Er verwaltet alle Richtlinien, Geräte und Einstellungen, während die Gateways Zugriff auf die Dateifreigaben gewähren.

So erstellen Sie eine Cluster-Gruppe:

Stellen Sie vor dem Fortfahren sicher, dass Sie bereits auf jedem Gateway die richtige **Adresse für Administration** festgelegt haben. This is the DNS or IP address of the Gateway server.

1. Rufen Sie die Acronis Access-Weboberfläche auf.
2. Öffnen Sie die Registerkarte **Mobiler Zugriff**.
3. Öffnen Sie die Seite **Gateway Server**.
4. Drücken Sie die Schaltfläche **Cluster-Gruppe hinzufügen**.
5. Geben Sie einen Anzeigenamen für die Gruppe ein.
6. Geben Sie den DNS-Namen oder die IP-Adresse des Lastenausgleichsmoduls ein.
7. Aktivieren Sie das Kontrollkästchen für jedes Gateway, das in die Gruppe aufgenommen werden soll.

8. Wählen Sie den Gateway, der die Einstellungen der Gruppe steuert. Alle bereits festgelegten Einstellungen dieses Gateways (einschließlich zugewiesener Datenquellen, jedoch nicht die Adresse für Administration) werden auf alle anderen Gateways in der Gruppe kopiert.



9. Drücken Sie **Hinzufügen**.

So bearbeiten Sie eine Cluster-Gruppe:

Das Bearbeiten von Cluster-Gruppen unterscheidet sich nicht vom Bearbeiten herkömmlicher Gateways. Weitere Informationen hierzu finden Sie im Artikel Gateway Server bearbeiten (S. 43).

Mitglieder zu einer bestehenden Cluster-Gruppe hinzufügen:

1. Öffnen Sie die Weboberfläche und navigieren Sie zu **Mobiler Zugriff**-> **Gateway-Server**.
2. Öffnen Sie das Menü 'Aktion' für die gewünschte Cluster-Gruppe und wählen Sie aus den verfügbaren Aktionen **Cluster-Mitglieder hinzufügen** aus.
3. Wählen Sie die gewünschten Gateway-Server aus der Liste und klicken Sie auf **Hinzufügen**.

1.6 Datenquellen verwalten

Sie können NTFS-Verzeichnisse auf dem Windows-Server oder auf einer SMB/CIFS-Remote-Dateifreigabe für den Zugriff durch Access Mobile Client-Benutzer freigeben. Wenn Access Mobile Client-Benutzer eine Verbindung herstellen, sehen sie diese Verzeichnisse als Dateifreigabe-Volumes. Sie können Datenquellen erstellen, die Zugriff auf einen Sync & Share-Server bieten.

Zugriff auf Inhalte in SharePoint 2007, 2010, 2013, 365

Acronis Access kann Zugriff auf Dateien bereitstellen, die sich in Dokumentbibliotheken auf SharePoint 2007-, 2010-, 2013- und 365-Servern befinden. Eine Acronis Access SharePoint-Datenquelle kann auf einen gesamten SharePoint-Server, eine bestimmte SharePoint-Seite oder -Unterseite oder auf eine bestimmte Dokumentbibliothek verweisen. Diese Dateien können geöffnet werden, PDFs können mit Anmerkungen versehen werden, die Dateien können bearbeitet und synchronisiert werden, genau wie Dateien, die auf einem herkömmlichen Dateiserver oder NAS-Storage gespeichert sind. Acronis Access unterstützt auch das Auschecken und Einchecken von SharePoint-Dateien.

Unterstützte Authentifizierungsmethoden für SharePoint

Acronis Access unterstützt SharePoint-Server, die eine Client-Authentifizierung per NTLMv1, NTLMv2 und Kerberos sowie eine anspruchsbasierte Authentifizierung zulassen. Wenn der SharePoint-Server eine Kerberos-Authentifizierung verlangt, müssen Sie das Active Directory-Computerobjekt für den oder die Windows-Server aktualisieren, auf denen die Acronis Access-Server-Software ausgeführt wird. Der Acronis Access Windows-Server muss die Berechtigung erhalten, delegierte Zugangsdaten zu Ihrem SharePoint-Server für Ihre Benutzer anzuzeigen.

Statt einer direkten Authentifizierung beim SharePoint-Server umfasst die anspruchsbasierte Authentifizierung die Authentifizierung bei einem Authentifizierungsserver, den Erhalt eines Authentifizierungstokens und die Bereitstellung dieses Tokens für den SharePoint-Server. Acronis Access unterstützt die anspruchsbasierte Authentifizierung bei Office 365 SharePoint-Websites. Zur Authentifizierung kontaktiert der Gateway-Server zuerst Microsoft Online, um die Adresse des Authentifizierungsservers zu bestimmen. Dieser Server kann von Microsoft Online gehostet werden oder sich im Unternehmensnetzwerk befinden (über Active Directory-Verbunddienste). Nach Abschluss der Authentifizierung und Erhalt eines binären Sicherheitstokens wird dieses Token an den SharePoint-Server gesendet, der ein Authentifizierungscookie zurückgibt. Dieses Cookie wird dann anstelle anderer Benutzeranmeldedaten für SharePoint verwendet.

Berechtigungen für freigegebene Dateien und Ordner ändern

Acronis Access verwendet die vorhandenen Benutzerkonten und Kennwörter von Windows. Da Acronis Access Windows NTFS-Berechtigungen durchsetzt, sollten Sie normalerweise die in Windows integrierten Tools zum Anpassen der Verzeichnis- und Dateiberechtigungen verwenden. Die Standardtools von Windows bieten die größte Flexibilität beim Festlegen Ihrer Sicherheitsrichtlinie.

Der Zugriff auf Acronis Access Datenquellen, die sich auf einem anderen SMB/CIFS-Dateiserver befinden, erfolgt über eine SMB/CIFS-Verbindung vom Gateway Server zum sekundären Server oder NAS. In diesem Fall erfolgt der Zugriff auf den sekundären Server im Kontext des Benutzers, der bei der Access Mobile Client-App angemeldet ist. Damit dieser Benutzer auf Dateien auf dem sekundären Server zugreifen kann, benötigt sein Konto sowohl Windows-Freigabeberechtigungen als auch NTFS-Sicherheitsberechtigungen.

Berechtigungen für Dateien, die sich auf den SharePoint-Servern befinden, werden entsprechend den auf dem SharePoint-Server konfigurierten SharePoint-Berechtigungen gehandhabt. Die Benutzer erhalten über Acronis Access dieselben Berechtigungen wie beim Zugriff auf SharePoint-Dokumentbibliotheken über einen Webbrowser.

Themen

1.6.1 Ordner

Neben Gateway Servern können Ordner auch Acronis Access-Benutzer- und -Gruppenrichtlinien zugewiesen werden, sodass sie in der Acronis Access Mobile Client-Applikation eines Benutzers automatisch angezeigt werden. Ordner können so konfiguriert werden, dass sie auf einen beliebigen Acronis Access Gateway Server oder auf ein Unterverzeichnis in einem freigegebenen Volume verweisen. Dann können Sie Benutzern direkten Zugriff auf beliebige Ordner gewähren, die für sie möglicherweise wichtig sind. Auf diese Weise müssen sie nicht den genauen Namen von Server und freigegebenem Volume sowie den Pfad zum Ordner kennen, um zu dem Ordner zu navigieren.

Ordner können auf beliebige Inhaltstypen zeigen, auf die Acronis Access Zugriff gewährt. Sie verweisen einfach auf Speicherorte auf Gateway Servern, die bereits innerhalb der Verwaltung von Acronis Access konfiguriert wurden. Dies kann ein lokales Volume für Dateifreigaben, ein Volume für 'Netzwerk-Freigabeweiterleitungen' mit Zugriff auf Dateien auf einem anderen Dateiserver oder NAS-Gerät, eine DFS-Freigabe oder aber ein SharePoint-Volume sein.

Hinweis: *Wenn Sie eine DFS-Datenquelle erstellen, müssen Sie den vollständigen Pfad des DFS hinzufügen, z.B.:*

\\company.com\namespace\share

Ordner können so konfiguriert werden, dass sie mit dem Client-Gerät synchronisiert werden. Es gibt folgende Synchronisierungsoptionen für Access Mobile Client-Ordner:

- **Keine** – Der Ordner wird in der Acronis Access-Client-App als Netzwerkressource angezeigt. Der Zugriff darauf und das Arbeiten mit diesem Ordner erfolgt ebenso wie bei einem Gateway Server.
- **1-Weg** – Der Ordner wird in der Acronis Access-Client-App als lokaler Ordner angezeigt. Der gesamte Inhalt wird vom Server auf das Gerät kopiert und auf dem aktuellen Stand gehalten, wenn Dateien auf dem Server hinzugefügt, geändert oder gelöscht werden. Dieser Ordner dient dem lokalen/Offline-Zugriff auf serverbasierte Dateien und wird dem Benutzer als schreibgeschützt angezeigt.

- **2-Wege** – Der Ordner wird in der Acronis Access-Client-App als lokaler Ordner angezeigt. Der komplette Inhalt wird am Anfang vom Server auf das Gerät synchronisiert. Wenn in diesem Ordner auf dem Gerät oder auf dem Server Dateien hinzugefügt, geändert oder gelöscht wurden, werden diese Änderungen auf den Server bzw. das Gerät synchronisiert.

Protokollierung von Salesforce-Aktivität verlangen

Acronis bietet in Partnerschaft mit Salesforce eine Option zum Protokollieren des Zugriffs auf Dateien an, die Kunden mit Acronis Access angezeigt werden. Durch Aktivierung dieser Option wird von jedem Benutzer, der diesen Ordner seiner Verwaltungsrichtlinie zugewiesen hat, verlangt, dass er eine Kundenaktivität in Salesforce protokolliert, bevor er eine Datei oder einen Ordner öffnen kann. Dies geschieht vollständig in der Access Mobile Client-App.

- Es ist für alle Elemente in diesem Ordner untersagt, diese per E-Mail zu versenden, sie zu drucken, sie außerhalb dieses Ordners zu kopieren bzw. zu verschieben, oder sie in anderen Apps auf dem Gerät zu öffnen.
- Diese Funktion verlangt einen Acronis Access-Client und -Server mit Version 5.0 oder höher.
- Diese Salesforce-Integration wird von Acronis Access für Android-Clients nicht unterstützt.

SharePoint-Websites und -Bibliotheken

Durch Erstellen einer Datenquelle können Sie den Access Mobile Client-Benutzern mühelos Zugriff auf SharePoint-Websites und -Bibliotheken erteilen. Es gibt verschiedene Möglichkeiten zum Erstellen von SharePoint-Datenquellen. Diese hängen von der SharePoint-Konfiguration ab:

- Datenquelle erstellen für eine ganze SharePoint-Website oder -Unterwebsite

Beim Erstellen einer Datenquelle für eine SharePoint-Website oder -Unterwebsite müssen Sie nur das Feld **URL** ausfüllen. Hierbei sollte es sich um die Adresse der SharePoint-Website oder -Unterwebsite handeln.

e.g. https://sharepoint.mycompany.com:43222
e.g. https://sharepoint.mycompany.com:43222/subsite name

- Datenquelle erstellen für **eine SharePoint-Bibliothek**

Beim Erstellen einer Datenquelle für eine SharePoint-Bibliothek Library müssen Sie die Felder **URL** und **Dokumentbibliotheksname** ausfüllen. Im Feld 'URL' geben Sie die Adresse der SharePoint-Website oder -Unterwebsite ein. und Im Feld 'Dokumentbibliotheksname' geben Sie den Namen der Bibliothek ein..

e.g. URL: https://sharepoint.mycompany.com:43222
e.g. Document Library Name: My Library

- Datenquelle erstellen für **einen bestimmten Ordner in einer SharePoint-Bibliothek**

Beim Erstellen einer Datenquelle für einen bestimmten Ordner in einer SharePoint-Bibliothek müssen Sie alle Felder ausfüllen. Im Feld 'URL' geben Sie die Adresse der SharePoint-Website oder -Unterwebsite ein., Im Feld 'Dokumentbibliotheksname' geben Sie den Namen der Bibliothek ein. und im Feld 'Unterpfad' geben Sie den Namen des gewünschten Ordners ein.

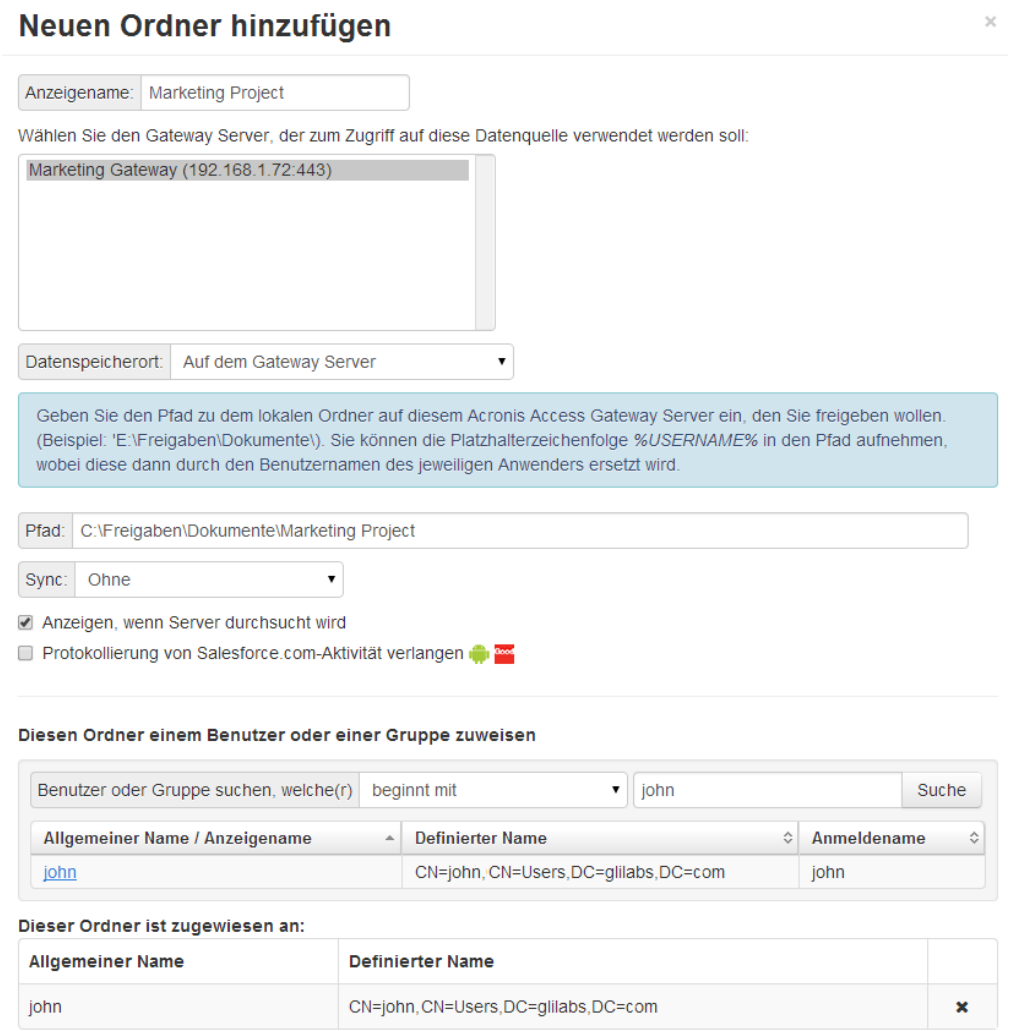
e.g. URL: https://sharepoint.mycompany.com:43222
e.g. Document Library Name: Marketing Library
e.g. Subpath: Sales Report

Hinweis: *Beim Erstellen einer Datenquelle, die mit einem Unterpfad auf eine SharePoint-Ressource verweist, können Sie die Option* ***Anzeigen, wenn Server durchsucht wird*** *nicht aktivieren.*

Der Access Mobile Client unterstützt die NTLM-, die anspruchsbasierte und die SharePoint 365-Authentifizierung sowie die Authentifizierung mit eingeschränkter Kerberos-Delegierung. Je nach SharePoint-Einrichtung müssen Sie unter Umständen den Gateway Server, mit dem die Verbindung zu diesen Datenquellen hergestellt wird, zusätzlich konfigurieren. Weitere Informationen hierzu finden Sie im Artikel Gateway Server bearbeiten (S. 43).

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'.

Hinweis: *Wenn Sie Sync & Share bei einer Neuinstallation von Acronis Access aktivieren und ein Gateway Server vorhanden ist, wird eine Sync & Share-Datenquelle automatisch erstellt. Diese zeigt auf die URL, die Sie im Abschnitt **Server** der Erstkonfiguration festgelegt haben. Dieser Ordner erlaubt den mobilen Benutzern den Zugriff auf Ihre Sync & Share-Dateien und Ordner.*

1.6.2 Zugewiesene Quellen

Auf dieser Seite können Sie nach einem Benutzer oder einer Gruppe suchen, um herauszufinden, welche Ressourcen diesem bzw. dieser zugewiesen sind. Die Ressourcen sind in 2 Tabellen aufgeführt: Server und Ordner.

In der Server-Tabelle sind der Anzeigename, der DNS-Name oder die IP-Adresse des Gateway-Servers sowie die Richtlinien aufgeführt, denen der Server zugewiesen ist.

Server

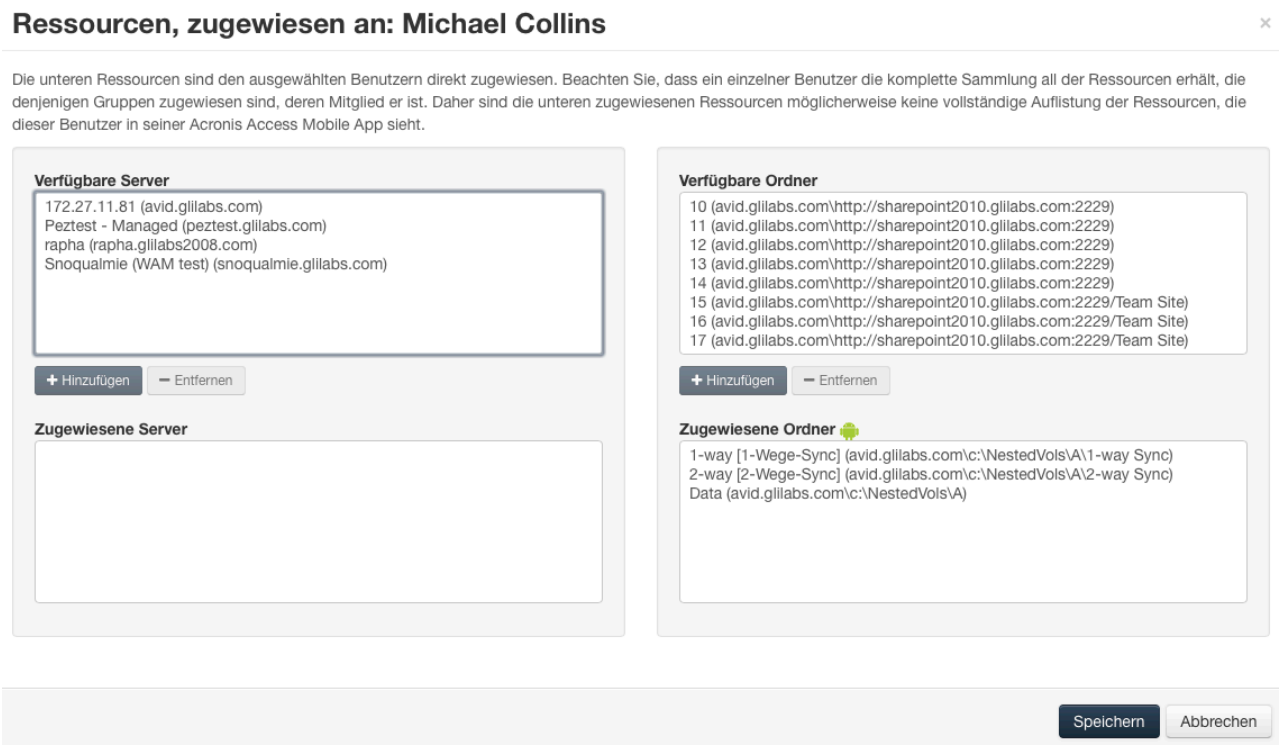
Anzeigename	Adresse	Zugewiesen an
Keine Server zugewiesen.		

In der Ordner-Tabelle sind der Anzeigename der Datenquelle, der Gateway Server, der Synchronisierungstyp, der Pfad und die Richtlinien aufgeführt, auf die diese Datenquelle zugewiesen ist.

Ordner

Anzeigename	Server	Sync	Pfad	Zugewiesen an
Data	172.27.11.81	Ohne	c:\NestedVols\A	Michael Collins
2-way	172.27.11.81	2-Wege	c:\NestedVols\A\2-way Sync	Michael Collins
1-way	172.27.11.81	1-Weg	c:\NestedVols\A\1-way Sync	Michael Collins

Wenn Sie auf die Schaltfläche **An zugewiesene Ressourcen bearbeiten** klicken, kann der Administrator die Zuweisungen für diese Richtlinie schnell bearbeiten.



1.6.3 Auf Clients sichtbare Gateway-Server

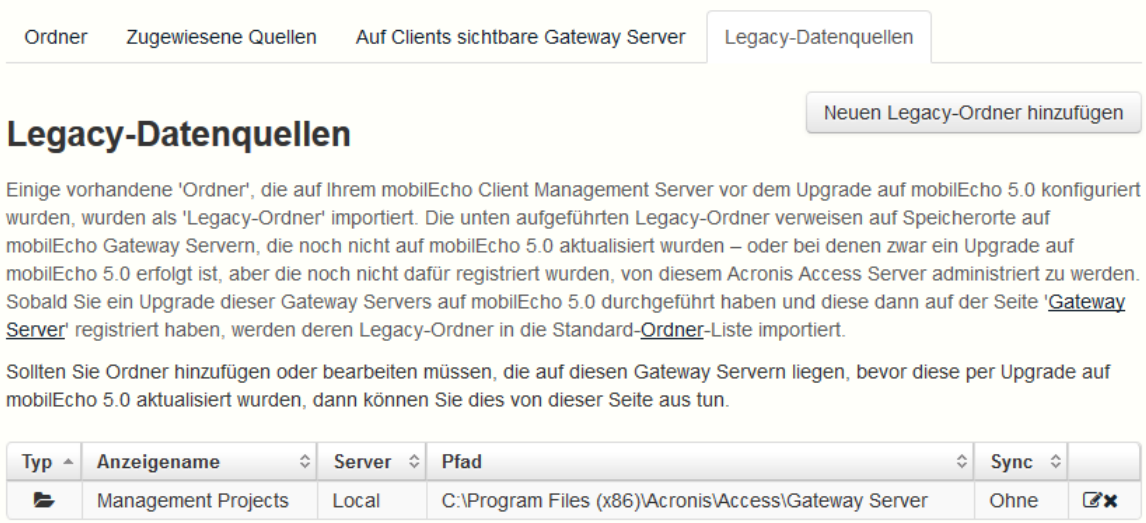
Gateway-Server können Benutzer- oder Gruppenrichtlinien zugewiesen und als Datenquellen eingesetzt werden. Auf dieser Seite werden alle Gateway Server angezeigt, die auf dem Acronis Access Mobile Client des Benutzers angezeigt werden und die einer Benutzer- oder Gruppenrichtlinie zugeordnet sind. Außerdem können Sie diese Zuordnungen hier bearbeiten. Wenn die Access Mobile Client-Benutzer einen Gateway Server durchsuchen, sehen sie die Datenquellen, für welche die Option **Anzeigen, wenn Server durchsucht wird** aktiviert ist.

So ändern Sie die aktuelle Zuordnung eines Servers:

1. Drücken Sie auf dem gewünschten Server auf die Schaltfläche **Bearbeiten**.
   - Wenn Sie die Zuordnung zwischen diesem Server und einem Benutzer aufheben möchten, drücken Sie auf das **X** für den jeweiligen Benutzer.
   - Wenn Sie einen neuen Benutzer oder eine neue Gruppe für diesen Server zuweisen möchten, suchen Sie nach dem Benutzer/der Gruppe und drücken Sie darauf.
2. Drücken Sie auf **Speichern**.

1.6.4 Legacy-Datenquellen

Wenn Sie von einer vorhandenen mobilEcho Installation auf Acronis Access aktualisiert haben, werden alle zugewiesenen Ordner automatisch übernommen und in diesem Abschnitt eingefügt. Wenn Sie noch mit einem Server unter mobilEcho 4.5 oder früher arbeiten, können Sie auch ein Volume im mobilEcho Administrator erstellen und es über diese Seite zu den Legacy-Datenquellen hinzufügen.



Neuen Legacy-Ordner hinzufügen

1. Klicken Sie auf die Schaltfläche **Neuen Legacy-Ordner hinzufügen**.
2. Geben Sie einen **Anzeigenamen** ein. Dieser Name wird in der mobilEcho Client-Applikation angezeigt.
3. Wählen Sie den mobilEcho Server aus, der das mobilEcho-Volume mit dem Ordner enthält.
4. Geben Sie den Pfad des Ordners ein. Der Pfad muss mit dem Namen des freigegebenen mobilEcho-Volumes beginnen. Wenn der Pfad für den Ordner nicht mit dem Namen eines mobilEcho-Volumes beginnt, kann der Ordner beim Zugriff durch Benutzer nicht verwendet werden. Wenn Sie Zugriff auf einen Unterordner in einem freigegebenen Volume gewähren möchten, fügen Sie im Feld 'Pfad' den vollständigen Pfad zu dem betreffenden Unterordner ein.
   - Im Pfad können Sie die Platzhalterzeichenfolge %USERNAME% verwenden. Dieser Platzhalter wird durch den Kontobenutzernamen des Benutzers ersetzt.
   - SharePoint-Websites und Dokumentbibliotheken werden angezeigt, wenn in der mobilEcho-App nach deren 'Titel' gesucht wird. Der Titel einer Website kann sich von deren URL-Namen unterscheiden. Beispielsweise kann 'http://sharepoint.company.com/testsite' den Titel 'Test-Site' haben. Zum Konfigurieren von Ordnern, die auf SharePoint-Speicherorte zeigen, können Sie den URL-Pfad oder den Titel verwenden. Im gesamten angegebenen Pfad müssen die Titel oder URL-Namen aller im Pfad enthaltenen Websites, Unterwebsites und Dokumentbibliotheken enthalten sein.
5. Wählen Sie eine Option für die Synchronisierung: **Keine**, **1-Weg** oder **2-Wege**.
6. Sie können auch **Protokollierung von Salesforce-Aktivität verlangen** aktivieren.
7. Suchen Sie nach einem Benutzer oder einer Gruppe im Active Directory, dem oder der Sie diesem neuen Ordner zuordnen möchten, und klicken Sie dann auf den Namen des Benutzers oder der

Gruppe. Damit wird der Ordner automatisch in der mobilEcho-App für den Benutzer oder die Gruppe angezeigt.

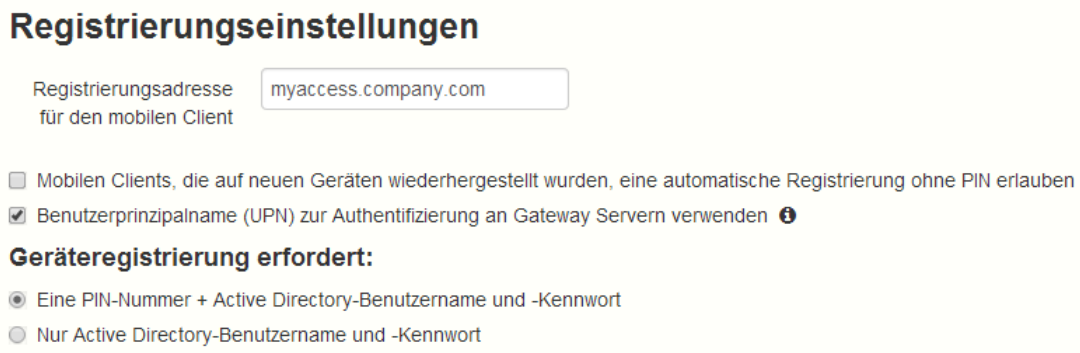
8. Drücken Sie auf **Speichern**.

So übernehmen Sie Ihre Legacy-Datenquellen auf dem neuen System:

1. Machen Sie den mobilEcho Dateiserver ausfindig, auf dem sich die Datenquellen befinden.
2. Führen Sie ein Upgrade des mobilEcho Dateiservers auf den Acronis Access Gateway Server aus.
3. Rufen Sie die Weboberfläche von Acronis Access auf und melden Sie sich als Administrator an.
4. Rufen Sie die Registerkarte **Gateway Server** auf.
5. Fügen Sie den Server zur Liste der Gateway Server hinzu. Weitere Informationen zu diesem Vorgang finden Sie im Abschnitt Gateway Server verwalten (S. 38).
6. Fügen Sie eine Lizenz für den Gateway Server hinzu.
7. Wiederholen Sie diesen Vorgang für jede der Legacy-Datenquellen.

Nach Abschluss des Vorgangs wird die Registerkarte 'Legacy-Datenquellen' nicht mehr angezeigt. Alle Legacy-Datenquellen werden in den Abschnitt 'Ordner' verschoben.

1.7 Einstellungen



Registrierungseinstellungen

- **Adresse für die Registrierung mobiler Clients** – Gibt die Adresse an, die mobile Clients verwenden sollten, wenn sie sich für das Client-Management registrieren.

  Hinweis: *Es wird dringend empfohlen, als Registrierungsadresse für den mobilen Client einen DNS-Namen zu verwenden. Nach der erfolgreichen Registrierung beim Client Management, speichert die Access Mobile Client-App die Adresse des Management Servers. Wenn es sich hierbei um eine IP-Adresse handelt und sich diese ändert, können die Benutzer den Server nicht erreichen, die Verwaltung der App kann nicht aufgehoben werden und die Benutzer müssen die gesamte App löschen und sich erneut zur Verwaltung registrieren.*

- **Mobilen Clients, die auf neuen Geräten wiederhergestellt wurden, eine automatische Registrierung ohne PIN erlauben** – Wenn diese Option aktiviert ist, können sich Benutzer, die von älteren Access Mobile Client-Versionen verwaltet werden, ohne PIN bei dem neuen Server registrieren.
- **Benutzerprinzipalname (UPN) zur Authentifizierung an Gateway Servern verwenden** – Ist diese Option aktiviert, können Benutzer ihren UPN (z.B. user@company.com) für die Authentifizierung an Gateway Servern verwenden. Wenn sie deaktiviert ist, authentifizieren sich Benutzer mit dem Domain-Namen und dem Benutzernamen (z.B. Domain/Benutzer).

Geräteregistrierung erfordert:

- **PIN-Nummer + Active Directory-Benutzername und Kennwort** – Um die Acronis Access-App zu aktivieren und Zugriff auf Acronis Access-Server zu erhalten, muss der Benutzer eine einmalig verwendbare PIN-Nummer mit Ablaufdatum sowie einen gültigen Active Directory-Benutzernamen und ein gültiges Kennwort eingeben. Mit dieser Option wird sichergestellt, dass Benutzer nur ein Gerät und erst nach Erhalt einer vom IT-Administrator ausgestellten PIN-Nummer registrieren können. Diese Option wird empfohlen, wenn die erhöhte Sicherheit der Zwei-Faktoren-Geräteregistrierung gefordert wird.
- **Nur Active Directory-Benutzername und -Kennwort** – Ein Benutzer kann die Acronis Access-App nur mit dem Active Directory-Benutzernamen und -Kennwort aktivieren. Mit dieser Option können Benutzer jederzeit ein oder mehrere Geräte registrieren. Den Benutzern muss lediglich der Name des Acronis Access Client Management-Server oder eine URL genannt werden, die auf den Acronis Access Client Management-Server verweist. Diese Angaben können auf einer Website bereitgestellt oder per E-Mail gesendet werden. Auf diese Weise wird die Bereitstellung von Acronis Access für eine große Zahl von Benutzern vereinfacht. Diese Option ist in Umgebungen vorzuziehen, in denen keine Zwei-Faktor-Registrierung erforderlich ist und viele Benutzer jederzeit Zugriff auf Acronis Access benötigen, beispielsweise in Deployments für Studierende.

2 Sync & Share

Dieser Bereich der Weboberfläche ist nur verfügbar, wenn die Sync & Share-Funktion aktiviert ist. Andernfalls wird die Schaltfläche **Sync & Share-Unterstützung aktivieren** angezeigt.

Themen

2.1 Benutzer verwalten

Aktive Benutzer

Über diesen Bereich können Sie alle Sync & Share-Benutzer verwalten. Sie können über die Schaltfläche 'Benutzer hinzufügen' neue Benutzer einladen oder über die Schaltfläche 'Aktionen' Benutzer bearbeiten bzw. löschen. Wenn Sie einen Benutzer bearbeiten, können Sie ihm administrative Rechte zuweisen (falls Sie dazu berechtigt sind), seine E-Mail-Adresse ändern, sein Kennwort ändern oder sein Konto deaktivieren bzw. aktivieren. Wenn Quotas aktiviert sind, können Sie für den Benutzer einen benutzerdefinierten Quota-Wert festlegen.

Es gibt zwei Arten von Sync & Share-Benutzern – Ad-hoc und **LDAP**

- Ad-hoc-Benutzer können mit verschiedenen Methoden erstellt werden – über eine E-Mail-Einladung oder eine Einladung zu einem freigegebenen Ordner. Diese Benutzer sind standardmäßig nicht lizenziert und der Administrator muss sie manuell in lizenzierte Benutzer umwandeln. Wenn ein Benutzer nicht lizenziert ist, kann er ausschließlich Ordner erstellen, bearbeiten, löschen oder hochladen, die andere Benutzer für ihn freigegeben haben. Nicht lizenzierte Benutzer können keine eigenen Inhalte erstellen oder hochladen und auch nicht den Desktop-Client verwenden.
- LDAP-Benutzer und Benutzer mit administrativen Rechten werden bei der Erstellung automatisch lizenziert. Sie können Dateien und Ordner erstellen und hochladen und diese Dateien und Ordner für andere Benutzer freigeben. Außerdem können sie den Desktop-Client verwenden. Sofern Sie keine bereitgestellte LDAP-Gruppe (S. 67) eingerichtet haben, müssen Sie LDAP-Benutzer auf die gleiche Weise erstellen wie Ad-hoc-Benutzer, Sie müssen sie jedoch nicht manuell lizenzieren. Für Administratoren ohne Sync & Share-Berechtigung muss keine E-Mail-Adresse festgelegt werden. Sie können sich einfach mit ihren LDAP-Anmeldedaten anmelden. Diese Administratoren können hinzugefügt werden, ohne zuvor SMTP für den Acronis Access-Server einzurichten. Weitere Informationen finden Sie im Artikel Administratoren und Berechtigungen (S. 75).

- **Name** – Zeigt den Namen an, mit dem sich der Benutzer beim Server anmeldet.
- **Admin** – Falls der Benutzer über Administrator-Berechtigungen verfügt, wird hier ein Häkchen angezeigt.
- **Lizenziert** – Falls der Benutzer über eine Lizenz verfügt, wird hier ein Häkchen angezeigt.
- **Deaktiviert** – Falls dieses Konto deaktiviert ist, wird hier ein Häkchen angezeigt.
- **Authentifizierung** – Zeigt an, ob sich der Benutzer über seine LDAP-Anmeldedatei oder über Ad-hoc authentifiziert.
- **Letzte Anmeldung** – Datum und Uhrzeit der letzten Anmeldung.
- **Zugehöriger Inhalt** – Zeigt die Anzahl der Ordner, Dateien sowie die Gesamtgröße der Inhalte des Benutzers an.
- **Aktionen**
  - **Bearbeiten** – Mit dieser Option können Sie diesen Benutzer bearbeiten.
  - **Löschen** – Der Benutzer wird gelöscht.

Ad-Hoc-Benutzer hinzufügen

1. Öffnen Sie die Acronis Access Weboberfläche.
2. Melden Sie sich mit einem Administratorkonto an. Stattdessen kann auch ein Konto mit Rechten zur **Verwaltung von Benutzern** verwendet werden.
3. Öffnen Sie die Registerkarte **Sync & Share**.
4. Öffnen Sie die Registerkarte **Benutzer**.
5. Drücken Sie **Benutzer hinzufügen**.
6. Geben Sie die E-Mail-Adresse des Benutzers ein.
7. Geben Sie an, ob der Benutzer administrative Rechte erhalten soll oder nicht.
8. Wählen Sie die Sprache der Einladung.
9. Klicken Sie auf die Schaltfläche **Hinzufügen**.

Der Benutzer erhält eine E-Mail mit einem Link. Sobald er den Link öffnet, wird er gebeten, ein Kennwort festzulegen. Damit ist die Hinzufügung des Kontos abgeschlossen.

LDAP-Benutzer hinzufügen

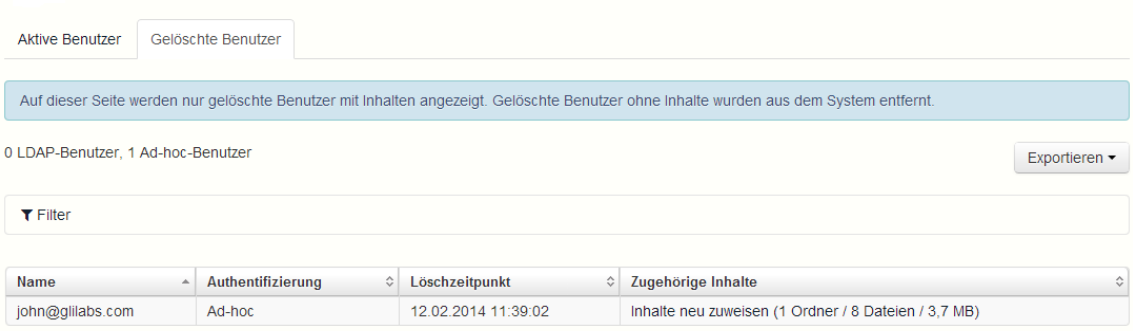
1. Öffnen Sie die Acronis Access Weboberfläche.
2. Melden Sie sich mit einem Administratorkonto an. Stattdessen kann auch ein Konto mit Rechten zur **Verwaltung von Benutzern** verwendet werden.
3. Öffnen Sie die Registerkarte **Sync & Share**.
4. Öffnen Sie die Registerkarte **Benutzer**.
5. Drücken Sie **Benutzer hinzufügen**.
6. Geben Sie die E-Mail-Adresse des Benutzers ein.
7. Geben Sie an, ob der Benutzer administrative Rechte erhalten soll oder nicht.
8. Wählen Sie die Sprache der Einladung.
9. Klicken Sie auf die Schaltfläche **Hinzufügen**.

Der Benutzer kann sich jetzt mit seinen LDAP-Anmeldedaten anmelden. Sobald er sich anmeldet, ist die Hinzufügung seines Kontos abgeschlossen.

Hinweis: *Falls Sie LDAP aktiviert und eine LDAP-Administrator-Gruppe bereitgestellt haben, können sich die Benutzer in dieser LDAP-Gruppe mit ihren LDAP-Anmeldedaten direkt anmelden und erhalten volle administrative Rechte.*

Gelöschte Benutzer

Gelöschte Benutzer ohne Inhalte werden vollständig entfernt. Benutzer, die über Inhalte verfügten (Dateien, Ordner), verbleiben im System und werden in diesen Bereich verschoben. Administratoren haben Zugriff auf die Liste gelöschter Benutzer mit Inhalten, die noch im System gespeichert sind. Diese Inhalte können einem anderen Benutzer zugewiesen oder automatisch vom System bereinigt werden, falls entsprechende Bereinigungsrichtlinien vorliegen.



Beim Löschen eines Benutzers werden Sie gefragt, ob Sie die Inhalte dieses Benutzers einem anderen Benutzer zuweisen möchten. Falls Sie einen anderen Benutzer auswählen, werden die Inhalte des gelöschten Benutzers in den eigenen Bereich der anderen Person verschoben und dieser Benutzer wird nicht auf der Registerkarte **Gelöschte Benutzer** angezeigt.

2.2 Freigabebeschränkungen

Einladen von Teilnehmern zulassen – Wenn diese Einstellung deaktiviert ist, wird das Kontrollkästchen **Teilnehmern erlauben, andere Teilnehmer einzuladen** nicht angezeigt, wenn Benutzer zu Ordnern eingeladen werden. Dadurch wird verhindert, dass Benutzer andere Benutzer einladen können.

Ablauf für einzelne Dateifreigabe

Benutzer daran hindern, Dateien mit unbegrenztem Ablauf freizugeben – Wenn diese Einstellung deaktiviert ist, sind Benutzer in der Lage, einzelne Dateien freizugeben, und dieser Link läuft nie ab. Ist die Einstellung hingegen aktiviert, müssen Benutzer, die einzelne Dateien freigeben, für jeden Link ein Ablaufdatum festlegen.

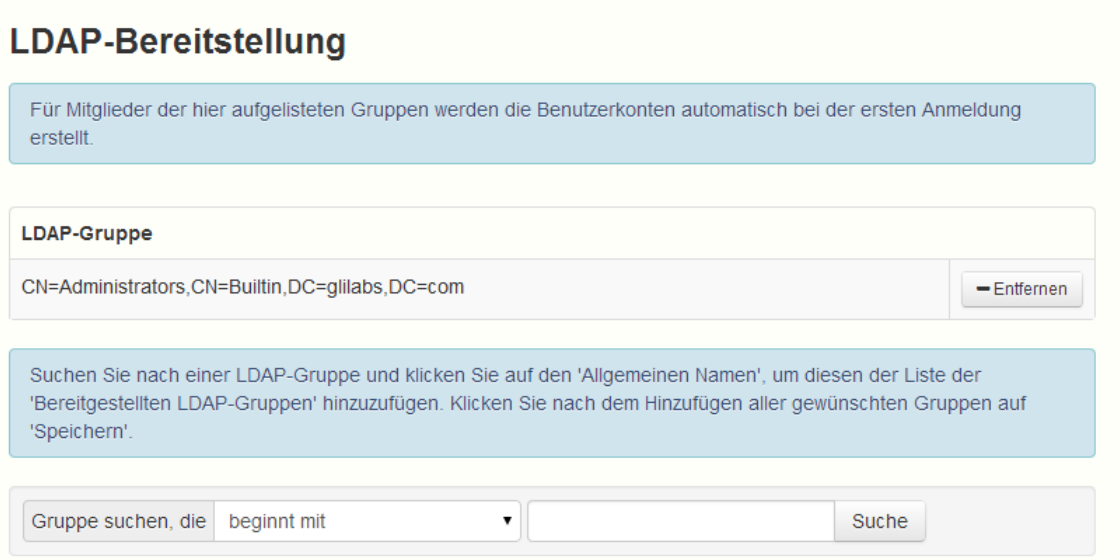
- **Mindest-Ablaufzeit** – Legt die Mindestdauer (in Tagen) fest, die Benutzer festlegen können.
- **Maximale Ablaufzeit** – Legt die maximale Dauer (in Tagen) fest, die Benutzer festlegen können.

Whitelist
– Wenn aktiviert, können sich nur Benutzer in den konfigurierten LDAP-Gruppen oder mit den in der Liste spezifizierten E-Mail-Domains (z.B. beispiel.com) anmelden. Für Domains können Platzhalterzeichen verwendet werden (z.B. *.firma.com). LDAP-Gruppen müssen über ihre definierten Namen (Distinguished Names) spezifiziert werden, beispielsweise CN=meinegruppe,CN=Benutzer,DC=meinefirma,DC=com.

Blacklist
– Benutzer in den LDAP-Gruppen oder mit den in der Blacklist spezifizierten E-Mail-Domains (z.B. beispiel.com) können sich nicht beim System anmelden, selbst wenn sie auf der Whitelist stehen. Für Domains können Platzhalterzeichen verwendet werden (z.B. *.firma.com). LDAP-Gruppen müssen über ihre definierten Namen (Distinguished Names) spezifiziert werden, beispielsweise CN=meinegruppe,CN=Benutzer,DC=meinefirma,DC=com.

Hinweis: *Platzhaltereinträge dürfen nur ein Sternchen enthalten und sollten immer am Anfang einer Zeichenfolge gefolgt von einem Punkt platziert werden (z.B. *.beispiel.com, *.com).*

2.3 LDAP-Bereitstellung



Für die Mitglieder der hier aufgelisteten Gruppen werden die Benutzerkonten automatisch bei der ersten Anmeldung erstellt.

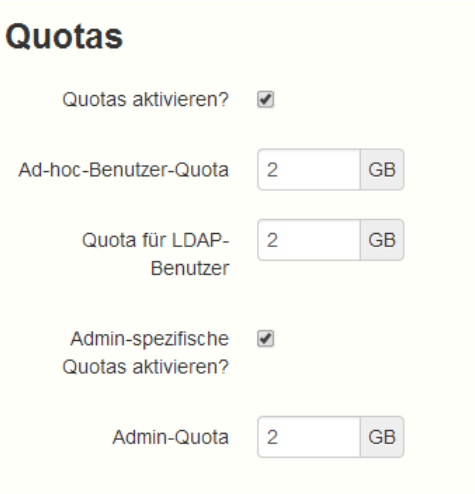
LDAP-Gruppe

Dies ist die Liste der aktuell ausgewählten Gruppen.

- **Allgemeiner Name/Anzeigename** – Der Anzeigename des Benutzers oder der Gruppe.
- **Definierter Name** – Der definierte Name des Benutzers oder der Gruppe. Der definierte Name ist ein eindeutiger Name für einen Eintrag im Directory Service.

2.4 Quotas

Administratoren könne die Menge an Speicherplatz festlegen, der für jeden Benutzer im System reserviert ist.



Es gibt unterschiedliche Standardeinstellungen für externe (Ad-hoc) und interne (Active Directory – LDAP) Benutzer.

Administratoren können darüber hinaus Benutzern Quota-Werte zuweisen, entweder individuell oder auf Grundlage deren Active Directory-Gruppenmitgliedschaft.

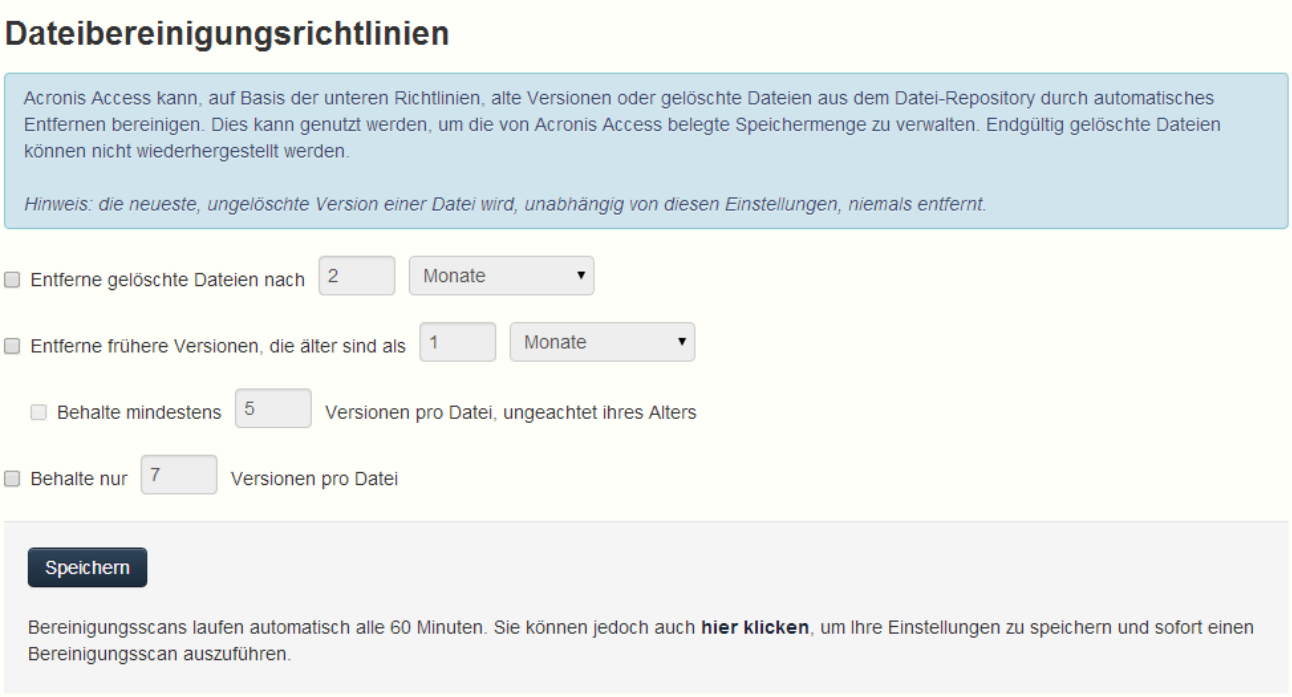
- **Quotas aktivieren?** – Wenn diese Option aktiviert ist, wird der maximale Speicherplatz, der einem Benutzer zur Verfügung steht, durch ein Kontingent beschränkt.
  - **Ad-hoc-Benutzer-Quota** – Legt das Kontingent für Ad-hoc-Benutzer fest.
  - **LDAP-Benutzer-Quota** – Legt das Kontingent für LDAP-Benutzer fest.
  - **Admin-spezifische Quotas aktivieren?** – Wenn diese Option aktiviert ist, wird Administratoren ein separates Kontingent zugewiesen.
    - **Admin-Quota** – Legt das Kontingent für Administratoren fest.

Hinweis: *Wenn ein Benutzer Mitglied mehrerer Gruppen ist, wird nur das größte Kontingent angewendet.*

Hinweis: *Quotas können auch für einzelne Benutzer spezifiziert werden. Die Einstellungen für einzelne Quotas überschreiben alle anderen Quota-Einstellungen. Um Einzelbenutzer-Quotas für andere Benutzer hinzuzufügen, müssen Sie den Benutzer auf der Seite* ***Benutzer*** *bearbeiten.*

2.5 Dateibereinigungsrichtlinien

In Acronis Access bleiben Dokumente, Dateien und Ordner normalerweise solange erhalten, bis sie explizit gelöscht werden. Dies erlaubt dem Benutzer, gelöschte Dateien wiederherzustellen und Vorgängerversionen von Dokumenten beizubehalten. In Acronis Access können Administratoren Richtlinien konfigurieren, die festlegen, wie lange gelöschte Dateien erhalten bleiben und wie viele Versionen einer Datei gespeichert werden bzw. wann ältere Versionen gelöscht werden.



Acronis Access kann anhand der unten genannten Richtlinien alte Versionen und gelöschte Dateien automatisch aus dem Datei-Repository entfernen. Dadurch kann die von Acronis Access verwendete Speichermenge verwaltet werden. Endgültig gelöschte Dateien können nicht wiederhergestellt werden.

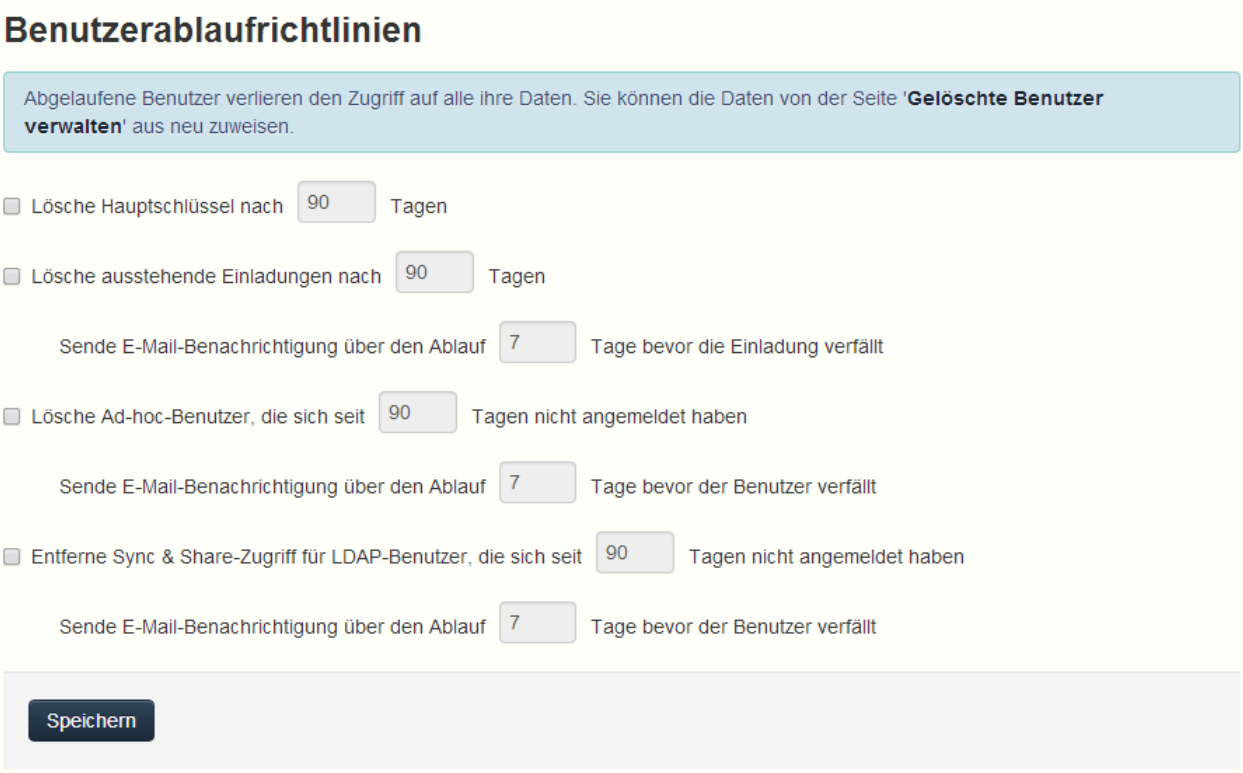
Hinweis: *Die neueste, ungelöschte Version einer Datei wird, unabhängig von diesen Einstellungen, niemals entfernt.*

- **Entferne gelöschte Dateien nach** – Wenn diese Option aktiviert ist, werden Dateien, die älter als diese Einstellung sind, bereinigt.
- **Entferne frühere Versionen, die älter sind als** – Wenn diese Option aktiviert ist, werden Dateiversionen, die älter als diese Einstellung sind, bereinigt.
  - **Behalte mindestens X Versionen pro Datei, ungeachtet ihres Alters** – Wenn diese Option aktiviert ist, wird eine Mindestanzahl von Versionen pro Datei behalten, unabhängig von ihrem Alter.
- **Behalte nur X Versionen pro Datei** – Wenn diese Option aktiviert ist, wird die Anzahl der Versionen pro Datei beschränkt.

Hinweis: *Durch Drücken von 'Speichern' wird die Bereinigung sofort gestartet, anderenfalls findet alle 60 Minuten ein regelmäßiger Scan statt.*

2.6 Benutzerablaufrichtlinien

Benutzer, die ablaufen, verlieren den Zugriff auf alle ihre Daten. Sie können die Daten auf der Seite **Gelöschte Benutzer verwalten** neu zuweisen.



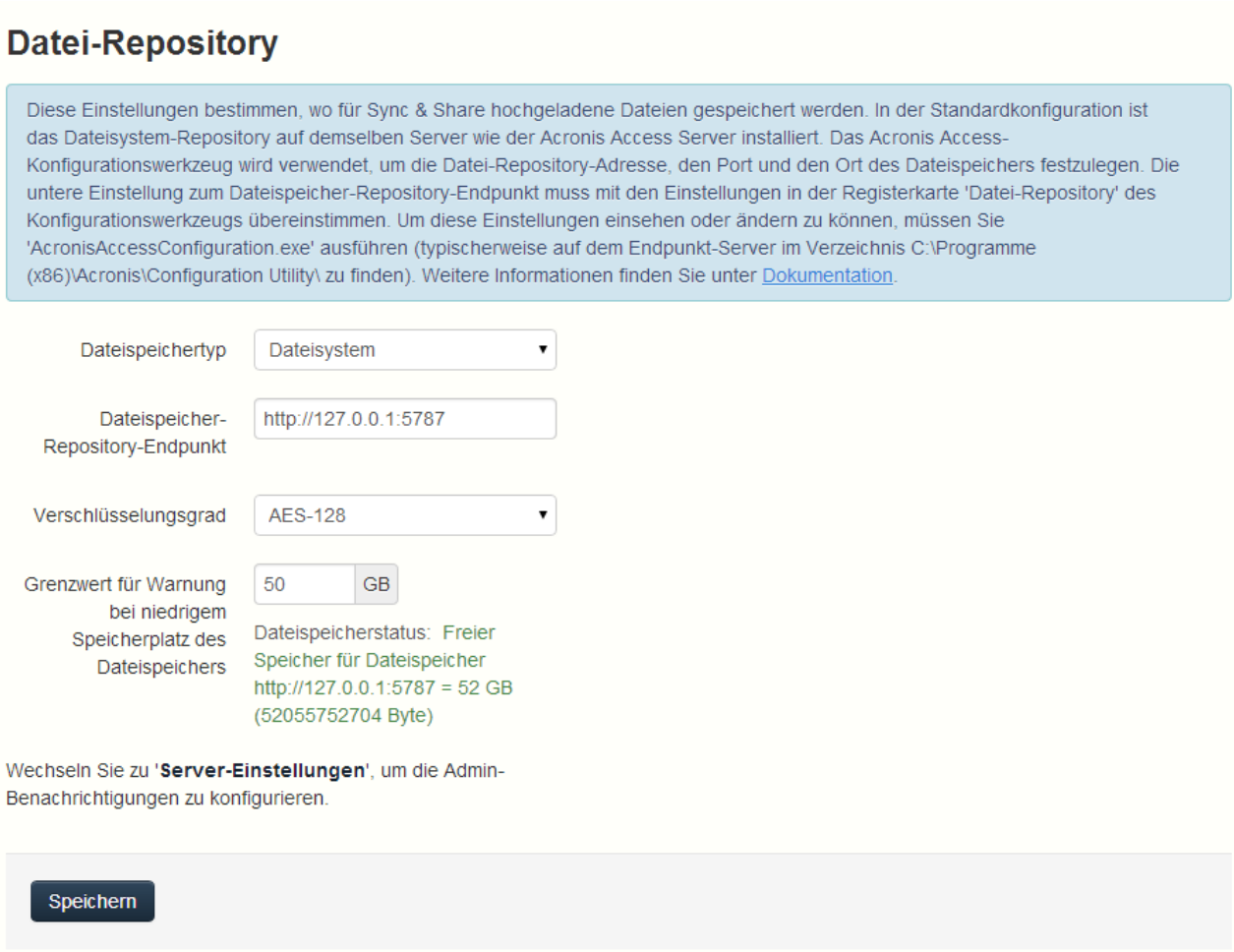
- **Lösche Hauptschlüssel nach** – Wenn diese Option aktiviert ist, werden alle Hauptschlüssel nach der festgelegten Anzahl von Tagen gelöscht.
- **Lösche ausstehende Einladungen nach X Tagen** – Wenn diese Option aktiviert ist, werden alle anstehenden Einladungen nach der festgelegten Anzahl von Tagen gelöscht.

- **Sende E-Mail-Benachrichtigung über den Ablauf X Tage bevor die Einladung verfällt** – Wenn diese Option aktiviert ist, wird bei Erreichen der angegebenen Anzahl von Tagen vor Ablauf der Einladung eine Benachrichtigung gesendet.

- **Lösche Ad-hoc-Benutzer, die sich seit X Tagen nicht angemeldet haben** – Wenn diese Option aktiviert ist, werden Ad-hoc-Benutzer, die sich innerhalb einer festgelegten Anzahl von Tagen nicht angemeldet haben, gelöscht.
  - **Sende E-Mail-Benachrichtigung über den Ablauf X Tage bevor der Benutzer verfällt** – Wenn diese Option aktiviert ist, wird innerhalb der angegebenen Anzahl von Tagen vor Ablauf des Ad-hoc-Benutzers eine Benachrichtigung gesendet.
- **Entferne Sync & Share-Zugriff für LDAP-Benutzer, die sich seit X Tagen nicht angemeldet haben** – Wenn diese Option aktiviert ist, wird der Synchronisierungs- und Freigabezugriff für LDAP-Benutzer, die sich innerhalb einer festgelegten Anzahl von Tagen nicht angemeldet haben, entfernt.
  - **Sende E-Mail-Benachrichtigung über den Ablauf X Tage bevor der Benutzer verfällt** – Wenn diese Option aktiviert ist, wird innerhalb einer festgelegten Anzahl von Tagen vor Ablauf des Benutzers eine Benachrichtigung gesendet.

2.7 Datei-Repository

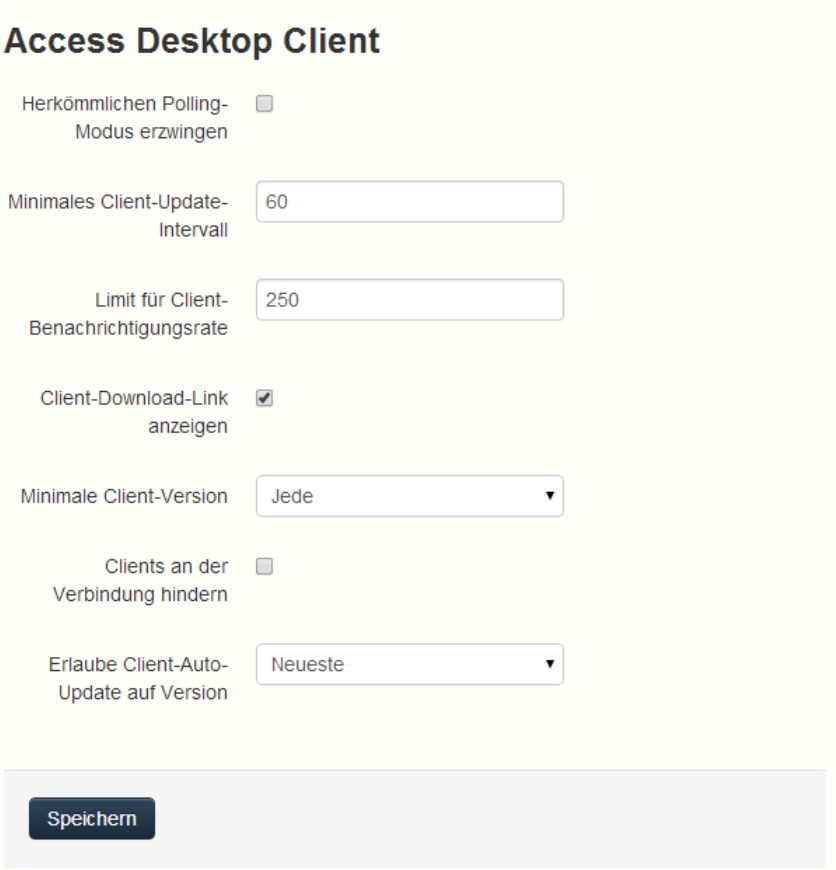
Diese Einstellungen bestimmen, wo für Sync & Share hochgeladene Dateien gespeichert werden. In der Standardkonfiguration ist das Dateisystem-Repository auf demselben Server wie der Acronis Access Server installiert. Im Datei-Repository werden Acronis Access Sync & Share-Dateien und frühere Versionen gespeichert. Mit dem Acronis Access-Konfigurationswerkzeug werden die Adresse des Datei-Repository, der Port und der Speicherort festgelegt. Die Einstellung **Dateispeicher-Repository-Endpunkt** unten muss mit den Einstellungen auf der Registerkarte 'Datei-Repository' des Konfigurationswerkzeugs übereinstimmen. Um diese Einstellungen einsehen oder ändern zu können, müssen Sie 'AcronisAccessConfiguration.exe' ausführen (typischerweise auf dem Endpunkt-Server im Verzeichnis C:\Programme (x86)\Acronis\Configuration Utility\ zu finden).



- **Dateispeichertyp** – Wählen Sie den Speicherort aus, der für das Repository des virtuellen Dateisystems verwendet werden soll. Die Optionen sind 'Dateisystem' und 'Amazon S3'.
- **Dateispeicher-Repository-Endpunkt** – Legen Sie die URL für den Dateisystem-Repository-Endpunkt fest.
- **Verschlüsselungsstufe** – Geben Sie den Verschlüsselungstyp an, der zur Verschlüsselung von Dateien im Repository des virtuellen Dateisystems verwendet werden soll. Die Optionen lauten 'Keine', 'AES-128' und 'AES-256'. Die Standardeinstellung ist 'AES-128'.
- **Grenzwert für Warnung bei niedrigem Speicherplatz des Dateispeichers** – Unterschreitet der freie Speicherplatz diesen Schwellenwert, erhält der Administrator eine entsprechende Warnung.

2.8 Acronis Access-Client

Diese Einstellungen gelten für den Access Desktop Client.



- **Herkömmlichen Polling-Modus erzwingen** – Zwingt die Clients, die Meldungen vom Server abzurufen, anstatt asynchron vom Server benachrichtigt zu werden. Sie sollten diese Option nur aktivieren, falls Sie vom Acronis Support dazu angewiesen werden.
  - **Client-Polling-Dauer** – Stellt die Zeitintervalle ein, in denen der Client vom Server abruft. Diese Option ist nur verfügbar, wenn **Herkömmlichen Polling-Modus erzwingen** aktiviert ist.
- **Minimales Client-Update-Intervall** – Stellt das Mindestintervall (in Sekunden) ein, das der Server abwartet, bevor er den Client erneut darüber benachrichtigt, dass aktualisierte Inhalte vorliegen.
- **Limit für Client-Benachrichtigungsrate** – Stellt die maximale Anzahl von Aktualisierungsbenachrichtigungen für den Client ein, die der Server pro Minute sendet.
- **Client-Download-Link anzeigen** – Wenn diese Option aktiviert ist, wird Webbenutzern ein Link zum Download des Desktop-Clients angezeigt.
- **Minimale Client-Version** – Stellt die niedrigste Client-Version ein, die sich mit diesem Server verbinden kann.
- **Clients an der Verbindung hindern** – Ist diese Option aktiviert, können Access Desktop Clients keine Verbindung mit dem Server herstellen. Dies sollte normalerweise nur zu administrativen Zwecken aktiviert werden. Es verhindert keine Verbindungen zur Weboberfläche.

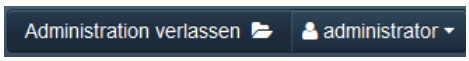
- **Erlaube Client-Auto-Update auf Version** – Legt die Access Desktop Client-Version fest, die per Auto-Update-Prüfung für alle Access Desktop Clients bereitgestellt wird. Wählen Sie **Keine Updates erlauben**, um ein Auto-Update der Clients komplett zu verhindern.

3 Server-Administration

Themen

3.1 Server verwalten

Als Administrator gelangen Sie nach der Anmeldung an der Weboberfläche direkt in den Modus **Administration**. Nach der Anmeldung können Sie zwischen den Modi **Administration** und **Benutzer** wechseln.



Zum Wechseln zwischen den Modi gehen Sie wie folgt vor:

1. Rufen Sie die Weboberfläche auf, und melden Sie sich als Administrator an.

- Um die Administration zu verlassen, klicken Sie oben rechts auf die Schaltfläche **Administration verlassen**. Auf diese Weise gelangen Sie zur Benutzerseite der Weboberfläche.
- Um zur Administration zurückzukehren, klicken Sie oben rechts auf die Schaltfläche **Administration**. Auf diese Weise gelangen Sie zurück in den Administrationsmodus.

Hinweis: *Administratoren haben Zugriff auf die API-Dokumentation. Sie finden den Link im Fußbereich der Access-Weboberfläche.*

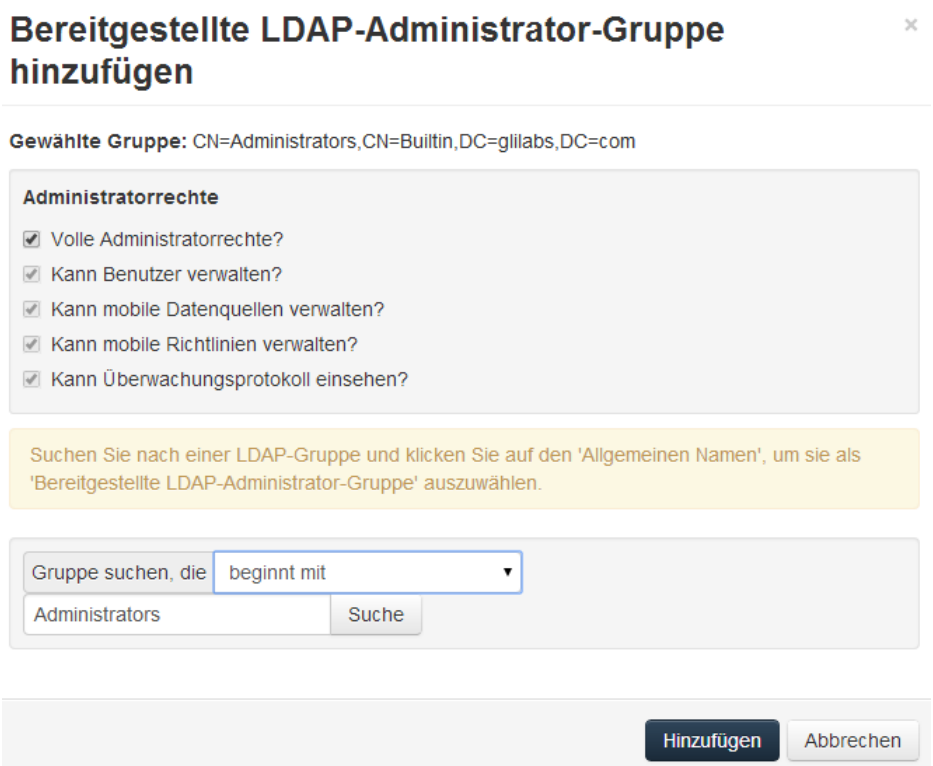
3.2 Administratoren und Berechtigungen

Bereitgestellte LDAP-Administrator-Gruppen

In diesem Abschnitt können Sie die administrativen Gruppen verwalten. Die Benutzer in diesen Gruppen erhalten automatisch die Administratorrechte der Gruppe. Alle Rechte werden in einer Tabelle aufgeführt. Die derzeit aktivierten Rechte haben eine grüne Markierung.

Mit der Schaltfläche **Aktionen** können Sie die Gruppe löschen oder bearbeiten. Sie können die administrativen Rechte der Gruppe bearbeiten.

So fügen Sie eine bereitgestellt LDAP-Administratorgruppe hinzu:



1. Klicken Sie auf die Schaltfläche **Bereitgestellte Gruppe hinzufügen**.
2. Markieren Sie, ob die Gruppe über die Funktion 'Sync & Share' verfügen soll.
3. Markieren Sie alle administrativen Rechte, die die Gruppenbenutzer erhalten sollen.
4. Suchen Sie die Gruppe.
5. Klicken Sie auf den Gruppennamen.
6. Klicken Sie auf **Speichern**.

Administrative Benutzer

In diesem Bereich sind alle Ihre Benutzer mit administrativen Rechten sowie deren Authentifizierungstyp (Ad-Hoc oder LDAP), Sync & Share-Rechte und Status (Deaktiviert oder Aktiviert) aufgeführt.

Mithilfe der Schaltfläche **Administrator hinzufügen** können Sie einen neuen Benutzer mit vollen oder eingeschränkten Administratorrechten einladen. Mit der Schaltfläche **Aktionen** können Sie den Benutzer löschen oder bearbeiten. Sie seine Administratorrechte, seinen Status, seine E-Mail-Adresse und sein Kennwort bearbeiten.

Einzelnen Administrator einladen

1. Rufen Sie die Acronis Access-Weboberfläche auf.
2. Melden Sie sich mit einem Administratorkonto an.
3. Erweitern Sie die Registerkarte **Allgemeine Einstellungen**, und öffnen Sie die Seite **Administratoren**.
4. Klicken Sie auf die Schaltfläche **Administrator hinzufügen** unter **Administrative Benutzer**.
5. Wählen Sie entweder die Registerkarte 'Active Directory/LDAP' oder 'Per E-Mail einladen' aus, je nachdem, welchen Typ von Benutzer Sie einladen und was von diesem Benutzer verwaltet werden soll. LDAP-Benutzern ohne E-Mail-Adresse können die Sync & Share-Funktionen nicht zugewiesen werden.

a) **Gehen Sie für Einladungen über Active Directory/LDAP folgendermaßen vor:**

   1. Suchen Sie nach dem Benutzer, den Sie in Active Directory hinzufügen möchten, und klicken Sie dann auf den 'Allgemeinen Namen', um einen Benutzer auszuwählen.

      Hinweis: *Die Felder 'LDAP-Benutzer' und 'E-Mail' werden automatisch ausgefüllt.*

   2. Aktivieren/deaktivieren Sie die Funktion 'Sync & Share'.
   3. Wählen Sie die Administratorrechte aus, über die der Benutzer verfügen soll.
   4. Klicken Sie auf 'Hinzufügen'

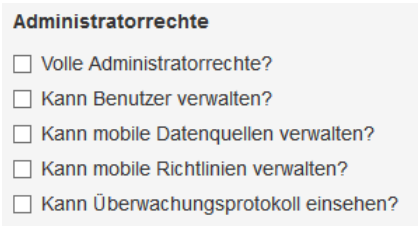
b) **Gehen Sie für Einladungen per E-Mail folgendermaßen vor:**

   1. Geben Sie die E-Mail-Adresse des Benutzers ein, den Sie als Administrator hinzufügen möchten.

      Hinweis: *Per E-Mail eingeladene Ad-hoc-Benutzer verfügen stets über die Funktion 'Sync & Share'.*

   2. Wählen Sie, ob dieser Benutzer lizenziert sein muss.
   3. Wählen Sie die Administratorrechte aus, über die der Benutzer verfügen soll.
   4. Wählen Sie die Sprache der Einladungs-E-Mail aus.
   5. Klicken Sie auf 'Hinzufügen'

Administratorrechte



- **Volle Administratorrechte** – Gewährt dem Benutzer volle Administratorrechte.
- **Kann Benutzer verwalten** – Gewährt dem Benutzer das Recht, Benutzer zu verwalten. Hierzu gehören das Einladen neuer Benutzer, das Bereitstellen von LDAP-Gruppen, das Senden von Acronis Access-Registrierungseinladungen sowie das Verwalten der verbundenen mobilen Geräte.
- **Kann mobile Datenquellen verwalten** – Stattet den Benutzer mit dem Recht aus, mobile Datenquellen zu verwalten. Dazu gehört das Hinzufügen neuer Gateway Server und Datenquellen, das Verwalten der zugewiesenen Quellen, der auf den Clients sichtbaren Gateways und alter Datenquellen.
- **Kann Richtlinien für mobile Geräte verwalten** – Stattet den Benutzer mit dem Recht aus, Richtlinien für mobile Geräte zu verwalten. Dazu gehört das Verwalten von Benutzer- und Gruppenrichtlinien, zulässiger Apps und standardmäßiger Zugriffsbeschränkungen.
- **Kann Überwachungsprotokoll einsehen** – Stattet den Benutzer mit dem Recht aus, das Überwachungsprotokoll einzusehen.

Hinweis: *Neue Benutzer, die sowohl einer bereitgestellten LDAP-Administrator-Gruppe als auch einer bereitgestellten LDAP-Sync & Share-Gruppe angehören, erhalten kombinierte Berechtigungen.*

So geben Sie Benutzern administrative Rechte:

1. Öffnen Sie die Registerkarte **Sync & Share**.
2. Öffnen Sie die Registerkarte **Benutzer**.
3. Klicken Sie dann für den Benutzer, den Sie bearbeiten möchten, auf die Schaltfläche **Aktionen**.
4. Klicken Sie auf **Bearbeiten**.
5. Markieren Sie alle administrativen Rechte, die der Benutzer erhalten soll.
6. Klicken Sie auf **Speichern**.

So geben Sie Benutzern spezifische Rechte:

1. Klicken Sie dann für den Benutzer, den Sie bearbeiten möchten, auf die Schaltfläche **Aktionen**.
2. Klicken Sie auf **Bearbeiten**.
3. Markieren Sie alle administrativen Rechte, die der Benutzer erhalten soll.
4. Klicken Sie auf **Speichern**.

3.3 Überwachungsprotokoll

3.3.1 Protokoll

Hier können Sie die letzten Ereignisse (je nach Bereinigungsrichtlinie kann die Zeitbeschränkung unterschiedlich sein), die Benutzer, von denen das Log stammt, sowie eine erklärende Nachricht zu der Aktion anzeigen lassen.

- **Nach Benutzer filtern** – Filtert die Logs nach Benutzer. Sie können **Alle**, **Kein Benutzer** oder einen der verfügbaren Benutzer auswählen.
- **Nach freigegebenen Projekten filtern** – Filtert die Logs nach freigegebenen Projekten. Sie können **Alle**, **Nicht freigegeben** oder eines der verfügbaren freigegebenen Projekte auswählen.
- **Nach Schweregrad filtern** – Filtert die Logs nach Typ. Verfügbare Typen sind **Alle**, **Info**, **Warnung**, **Fehler** und **Fatal**.
- **Von/Bis** – Filtert nach Datum und Uhrzeit.
- **Nach Text suchen** – Filtert nach dem Inhalt der Lognachrichten.

- **Zeitstempel** – Zeigt Datum und Uhrzeit des Ereignisses an.
- **Typ** – Zeigt den Schweregrad des Ereignisses an.
- **Benutzer** – Zeigt das für das Ereignis verantwortliche Benutzerkonto an.
- **Nachricht** – Zeigt Informationen zum Vorfall an.

Wenn auf dem Gateway Server die Funktion 'Überwachungsprotokolle' aktiviert ist, sehen Sie außerdem die Aktivität Ihrer mobilen Clients.

- **Gerätename** – Der Name des verbundenen Geräts.
- **Geräte-IP** – Die IP-Adresse des verbundenen Geräts.
- **Gateway Server** – Zeigt den Namen des Gateway Servers an, mit dem das Gerät verbunden ist.
- **Gateway Server-Pfad** – Zeigt den Pfad zur Datenquelle auf diesem Gateway Server an.

So aktivieren Sie die Überwachungsprotokollierung für einen bestimmten Gateway Server:

1. Rufen Sie die Weboberfläche auf.
2. Melden Sie sich als Administrator an.
3. Öffnen Sie die Registerkarte **Mobiler Zugriff**.
4. Öffnen Sie die Registerkarte **Gateway Server**.
5. Suchen Sie den Server, für den Sie **Audit Logs aktivieren möchten.**
6. Drücken Sie die Schaltfläche **Details**.
7. Aktivieren Sie im Bereich **Protokollierung** die Option **Überwachungsprotokollierung**.
8. Drücken Sie die Schaltfläche **Speichern**.

So aktivieren Sie die Debug-Protokollierung für einen bestimmten Gateway Server:

Hinweis: *Die Debug-Logs werden standardmäßig in folgendem Ordner gespeichert:* ***C:\Program Files (x86)\Acronis\Access\Gateway Server\Logs\AcronisAccessGateway***

1. Rufen Sie die Weboberfläche auf.
2. Melden Sie sich als Administrator an.
3. Öffnen Sie die Registerkarte **Mobiler Zugriff**.
4. Rufen Sie die Registerkarte **Gateway Server** auf.
5. Suchen Sie den Server, für den Sie die **Debug-Protokollierung aktivieren möchten.**
6. Klicken Sie auf die Schaltfläche **Details**.
7. Aktivieren Sie im Bereich **Protokollierung** die Option **Debug-Protokollierung**.
8. Klicken Sie auf die Schaltfläche **Speichern**.

3.3.2 Einstellungen

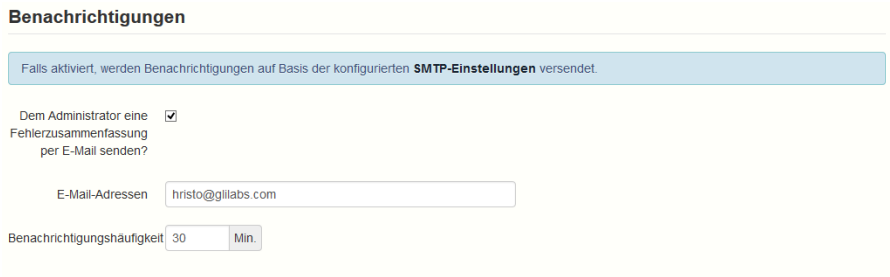
Acronis Access kann auf Basis bestimmter Richtlinien alte Protokolle bereinigen und diese als Dateien exportieren.

- **Protokolleinträge automatisch bereinigen, die älter als X Y sind** – Wenn diese Option aktiviert ist, werden Protokolle, die älter sind als eine bestimmte Anzahl Tage/Wochen/Monate automatisch bereinigt.
  - **Protokolleinträge vor der Bereinigung als Datei im Format X exportieren** – Wenn diese Option aktiviert ist, wird vor der Bereinigung eine Kopie der Protokolle im CSV-, TXT- oder XML-Format exportiert.
    - **Exportdateipfad** – Legt den Ordner fest, in dem exportierte Protokolle gespeichert werden.

3.4 Server

Server-Einstellungen

- **Server-Name** – Kosmetischer Server-Name, der als Titel der Website sowie zur Identifizierung dieses Servers in E-Mails mit Admin-Benachrichtigungen verwendet wird.
- **Webadresse –** Geben Sie hier den DNS-Stammnamen oder die IP-Adresse ein, über die der Benutzer auf die Website zugreift (beginnend mit http:// oder https://). Verwenden Sie hier nicht den 'localhost'. Diese Adresse wird auch für Links in E-Mail-Einladungen verwendet.
- **Farbschema –** Wählen Sie das Farbschema für die Website aus. Die derzeit verfügbaren Optionen sind **Grau, Violett, Cappuccino, Blau, Dunkelblau** und **Orange.** Die Standardeinstellung ist **Dunkelblau**.
- **Sprache für Überwachungsprotokoll** – Wählen Sie die Standardsprache für das Überwachungsprotokoll. Die derzeitig verfügbaren Optionen sind **Englisch, Deutsch, Französisch und Japanisch.** Die Standardeinstellung ist **Englisch**.
- **Sitzungs-Zeitlimit in Minuten** – Geben Sie die maximale Länge der Benutzersitzung an.
- **Sync & Share-Unterstützung aktivieren** – Mit diesem Kontrollkästchen werden die Sync & Share-Funktionen aktiviert/deaktiviert.

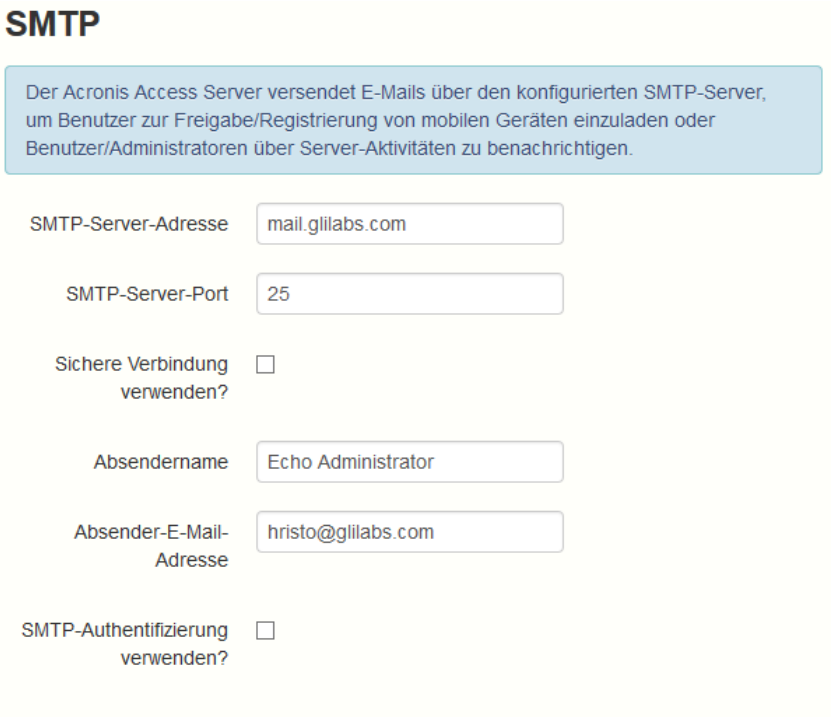


Benachrichtigungseinstellungen

- **Dem Administrator eine Fehlerzusammenfassung per E-Mail senden?** – Wenn diese Option aktiviert ist, wird eine Fehlerzusammenfassung an die angegebenen E-Mail-Adressen gesendet.
  - **E-Mail-Adressen** – Eine oder mehrere E-Mail-Adressen, die eine Fehlerzusammenfassung erhalten.
  - **Benachrichtigungshäufigkeit** – Die Häufigkeit, mit der eine Fehlerzusammenfassung gesendet wird. Sendet E-Mails nur, wenn Fehler vorliegen.

3.5 SMTP

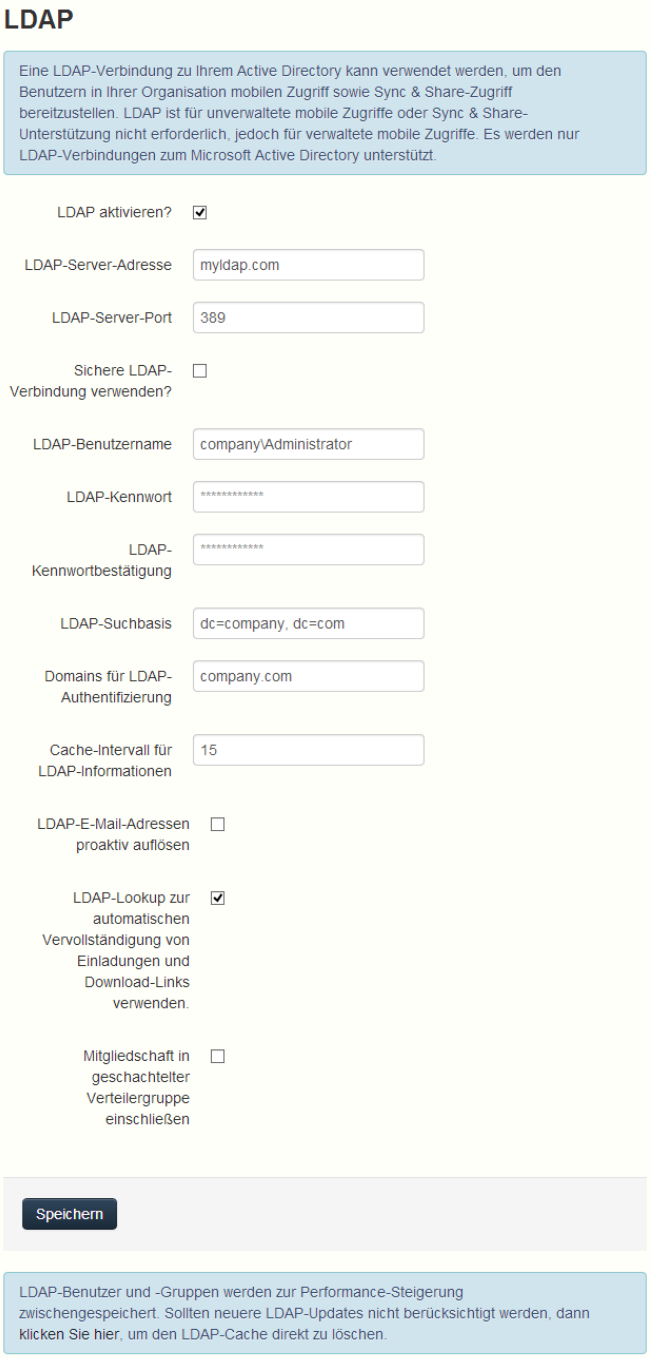
Der Acronis Access Server versendet E-Mails über den konfigurierten SMTP-Server, um Benutzer zur Freigabe/Registrierung von mobilen Geräten einzuladen oder Benutzer/Administratoren über Server-Aktivitäten zu benachrichtigen.



- **SMTP-Serveradresse** – Geben Sie den DNS-Namen des SMTP-Servers ein, über den E-Mail-Einladungen an Benutzer gesendet werden sollen.
- **SMTP-Serverport** – Geben Sie den SMTP-Serverport ein. Die Standardeinstellung ist Port 587.
- **Sichere Verbindung verwenden?** – Über diese Option können Sie festlegen, ob der SMTP-Server eine Secure SSL-Verbindung nutzt. Diese Option ist standardmäßig aktiviert. Deaktivieren Sie das Kontrollkästchen, um sichere SMTP-Verbindungen zu deaktivieren.
- **Absendername** – Dies ist der Benutzername, der in der 'Von'-Zeile von E-Mails angezeigt wird, die vom Server gesendet werden.
- **SMTP-Authentifizierung verwenden?** – Aktivieren Sie diese Option, um eine Verbindung mit einem SMTP-Benutzernamen und -Kennwort herzustellen.
  - **SMTP-Benutzername** – Geben Sie einen Benutzernamen für die SMTP-Authentifizierung ein.
  - **SMTP-Kennwort** – Geben Sie ein Kennwort für die SMTP-Authentifizierung ein.
  - **SMTP-Kennwortbestätigung** – Geben Sie das SMTP-Kennwort zur Bestätigung erneut ein.
- **Test-E-Mail senden** – Sendet eine Test-E-Mail, um sicherzustellen, dass sämtliche Einstellungen erwartungsgemäß funktionieren.

3.6 LDAP

Microsoft Active Directory kann verwendet werden, um Benutzern in Ihrer Organisation mobilen Zugriff sowie Sync & Share-Zugriff bereitzustellen. LDAP ist für nicht verwaltete mobile Zugriffe oder Sync & Share-Unterstützung nicht erforderlich, jedoch eine Voraussetzung für verwaltete mobile Zugriffe. Andere Active Directory-Produkte (z.B. Open Directory) werden derzeit nicht unterstützt.



- **LDAP aktivieren?** – Wenn diese Option aktiviert ist, können Sie LDAP konfigurieren.
  - **LDAP-Server-Adresse** – Geben Sie den DNS-Namen oder die IP-Adresse des Active Directory-Servers an, den Sie zur Zugriffskontrolle verwenden möchten.

- **LDAP-Server-Port** – Der standardmäßige Active Directory-Port ist 389. Dieser muss in den meisten Fällen nicht geändert werden.

  Hinweis: *Wenn Sie mehrere Domains unterstützen, empfiehlt es sich, den Port für den globalen Katalog zu verwenden.*

- **Sichere LDAP-Verbindung verwenden?** – Ist standardmäßig deaktiviert. Aktivieren Sie das Kontrollkästchen, um Verbindungen mit Active Directory über sicheres LDAP herzustellen.
- **LDAP-Benutzername/-Kennwort** – Diese Anmeldedaten werden für alle LDAP-Abfragen verwendet. Fragen Sie Ihren AD-Administrator, ob Ihnen Dienstkonten zugewiesen wurden, die verwendet werden müssen.
- **LDAP-Suchbasis** – Geben Sie die Stammebene ein, auf der Suchvorgänge nach Benutzern und Gruppen beginnen sollen. Wenn Sie die gesamte Domain durchsuchen möchten, geben Sie die Zeichenfolge 'dc=domainname, dc=domainsuffix' ein.
- **Domains für LDAP-Authentifizierung** – Benutzer mit E-Mail-Adressen, deren Domains in dieser per Komma getrennten Liste aufgeführt sind, müssen sich über LDAP authentifizieren. (Für ein Konto mit der E-Mail-Adresse **joe@glilabs.com** würden Sie zur LDAP-Authentifizierung beispielsweise **glilabs.com** eingeben.) Benutzer mit anderen Domains müssen sich über die Acronis Access-Datenbank authentifizieren.
- **Cache-Intervall für LDAP-Informationen** – Legt das Intervall fest, in dem Acronis Access die Active Directory-Struktur im Cache speichert.
- **LDAP-E-Mail-Adressen proaktiv auflösen** – Wenn diese Einstellung aktiviert ist, wird Active Directory von Acronis Access bei Anmeldungen und Einladungen nach dem Benutzer mit der entsprechenden E-Mail-Adresse durchsucht. So können Benutzer sich mit ihren E-Mail-Adressen anmelden und bei Einladungen eine direkte Rückmeldung erhalten. Bei großen LDAP-Katalogen kann die Ausführung jedoch langsam sein. Deaktivieren Sie diese Einstellung, wenn Sie bei Authentifizierungen oder Einladungen Leistungsprobleme oder langsame Antworten beobachten.
- **LDAP-Lookup zur automatischen Vervollständigung von Einladungen und Download-Links verwenden** – Mit LDAP-Suche für Type-ahead wird LDAP nach Benutzern mit übereinstimmenden E-Mail-Adressen durchsucht. Bei großen LDAP-Katalogen kann diese Suche längere Zeit dauern. Falls Sie bei Verwendung der Type-ahead-Funktion auf Leistungsprobleme stoßen, sollten Sie diese Einstellung deaktivieren.
- **Mitgliedschaft in geschachtelter Verteilergruppe einschließen** – Wenn diese Option aktiviert ist, werden beim Einladen einer Verteilergruppe zu einer Freigabe alle Mitglieder der Gruppe sowie alle Mitglieder von Untergruppen eingeladen.

3.7 Email Templates

Acronis Access verwendet häufig E-Mail-Nachrichten, um Benutzern und Administratoren dynamische Informationen bereitzustellen. Für jedes Ereignis gibt es eine zugehörige HTML- und Textvorlage. Sie können auf das Pulldown-Menü 'E-Mail-Vorlage' klicken, um ein Ereignis auszuwählen und um beide Vorlagen zu bearbeiten.

Alle vom Acronis Access Server versendeten E-Mails können an Ihre Bedürfnisse angepasst werden. Sie müssen für jede E-Mail E-Mail-Vorlagen im HTML- und im 'Nur Text'-Format bereitstellen. Die Vorlagen-Textkörper (Bodys) müssen in ERB (Embedded Ruby) geschrieben werden. Prüfen Sie die Standardvorlagen, um zu ermitteln, wie Sie Ihre Vorlagen am besten anpassen.

Nach einem Upgrade von mobilEcho werden die Änderungen an den E-Mail-Vorlagen nicht migriert, sodass Sie die neuen Vorlagen anpassen müssen. 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**.

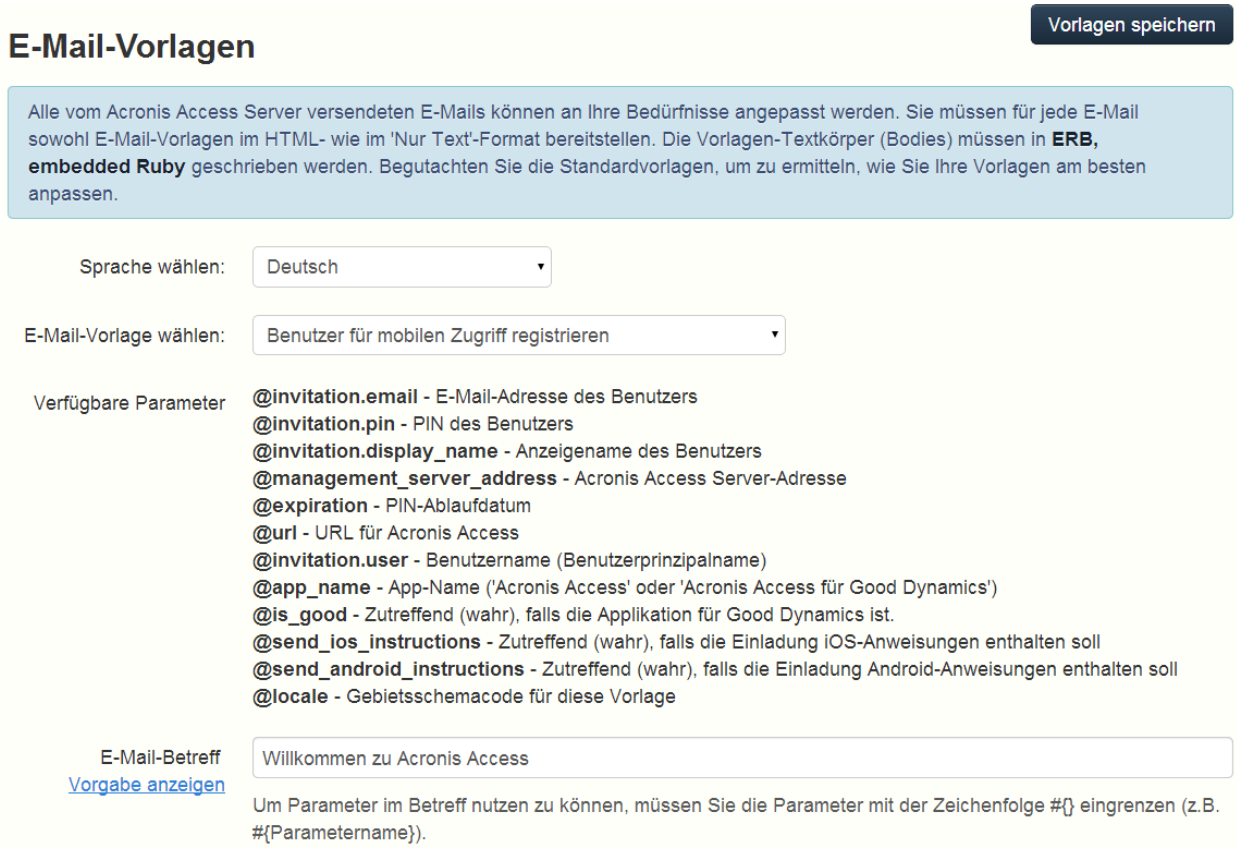
- **Sprache wählen –** Wählen Sie die Standardsprache für Einladungs-E-Mails.

  ***Hinweis**: Wenn Sie eine Registrierungseinladung oder eine Einladung zu einer Freigabe senden bzw. wenn Sie eine einzelne Datei freigeben, können Sie im Dialogfeld für Einladungen eine andere Sprache auswählen.*

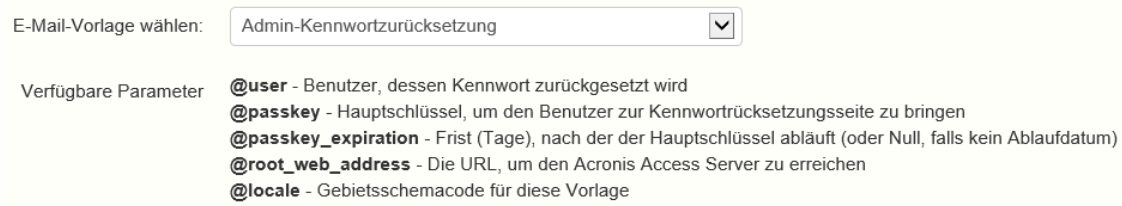
- **E-Mail-Vorlage wählen** – Wählen Sie die Vorlage aus, die Sie anzeigen bzw. bearbeiten möchten. Jede der Vorlagen dient einem bestimmten Zweck (z. B. einen Benutzer für mobilen Zugriff registrieren, das Kennwort eines Benutzers zurücksetzen).
- **Verfügbare Parameter** – Welche Parameter verfügbar sind, hängt davon ab, welche Vorlage Sie ausgewählt haben.
- **E-Mail-Betreff** – Der Betreff der Einladungs-E-Mail. Wenn Sie auf den Link **Vorgabe drücken** klicken, wird der Standardbetreff für diese Sprache und E-Mail-Vorlage angezeigt.
- **HTML-E-Mail-Vorlage** – Zeigt die HTML-codierte E-Mail-Vorlage an. Wenn Sie fehlerfreien HTML-Code eingeben, wird dieser angezeigt. Wenn Sie auf **Vorschau** klicken, sehen Sie eine Vorschau für Ihre aktuelle Vorlage.
- **Text-E-Mail-Vorlage** – Zeigt die textbasierte E-Mail-Vorlage an. Wenn Sie auf **Vorschau** klicken, sehen Sie eine Vorschau für Ihre aktuelle Vorlage.

***Hinweis**: Denken Sie stets daran, auf die Schaltfläche **Vorlagen speichern** zu klicken, nachdem Sie die Bearbeitung der Vorlagen abgeschlossen haben.*

***Hinweis**: Wenn Sie eine englische Vorlage bearbeiten, werden dadurch die anderen Sprachen nicht automatisch geändert. Sie müssen jede Vorlage für jede Sprache einzeln bearbeiten.*



Vorlagen ermöglichen es Ihnen, anhand von Parametern dynamische Informationen einzuschließen. Beim Zustellen einer Nachricht werden diese Parameter durch die entsprechenden Daten ersetzt. Für verschiedene Ereignisse sind unterschiedliche Parameter verfügbar.

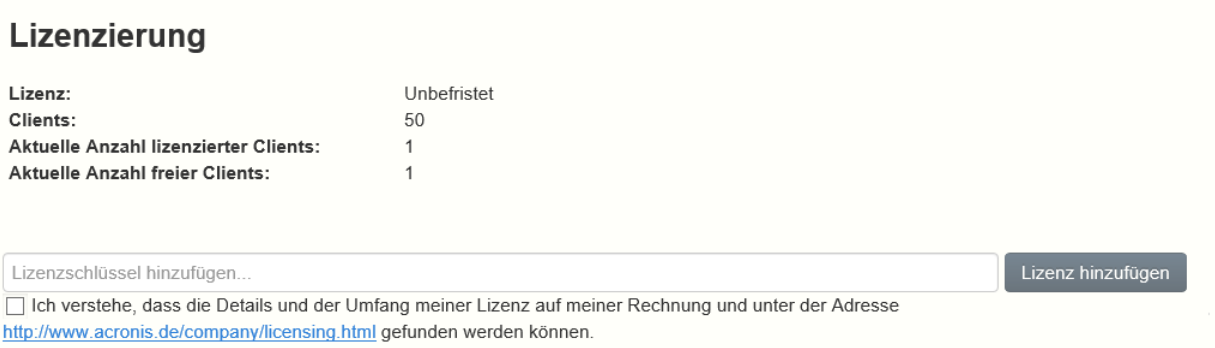


***Dingies**: Wenn Sie auf **Vorgabe anzeigen** klicken, wird die Standardvorlage angezeigt.*

Denken Sie stets daran, auf die Schaltfläche **Vorlagen speichern** zu klicken, nachdem Sie die Bearbeitung der Vorlagen abgeschlossen haben.

3.8 Lizenzierung

Lizenzierung



Eine Liste aller Lizenzen wird angezeigt.

- **Lizenz** – Der Typ der Lizenz (Test, Abonnement etc.).
- **Clients** – Höchstanzahl der zulässigen lizenzierten Benutzer.
- **Aktuelle Anzahl lizenzierter Clients** – Anzahl der aktuell verwendeten Benutzerlizenzen.
- **Aktuelle Anzahl freier Clients** – Anzahl der aktuell ungenutzten Benutzerlizenzen im System.

Eine neue Lizenz hinzufügen

1. Kopieren Sie Ihren Lizenzschlüssel.
2. Fügen Sie ihn im Feld **Lizenzschlüssel hinzufügen** ein.
3. Lesen Sie die Lizenzvereinbarung, und akzeptieren Sie sie durch Aktivieren des Kontrollkästchens.
4. Klicken Sie auf **Lizenz hinzufügen**.

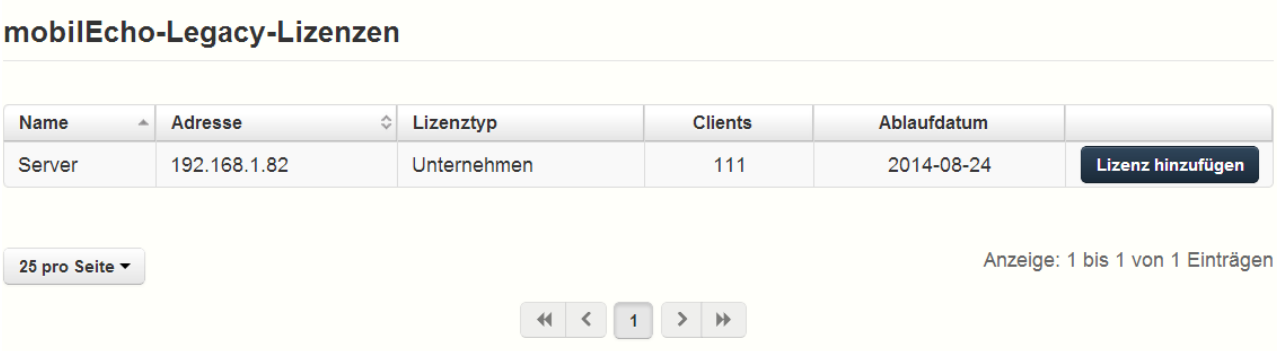
Hinweis: *Wenn Ihre Lizenzen dieselbe eindeutige ID verwenden, wird die Anzahl der zulässigen Benutzer addiert.*

Eine neue Lizenz für einen Gateway Server hinzufügen

In Acronis Access Version 6.0 gilt für den Acronis Access-Server und die Gateway Server die gleiche Lizenz. Sie müssen den Gateway Servern Lizenzen daher nicht manuell hinzufügen.

Wenn Sie weiterhin Gateway Server mit einer älteren Version verwenden, wird auch der Abschnitt mobilEcho-Legacy-Lizenzen angezeigt.

Um diese Versionen zu lizenzieren, benötigen Sie eine mobilEcho-Lizenz. Führen Sie die folgenden Schritte aus:

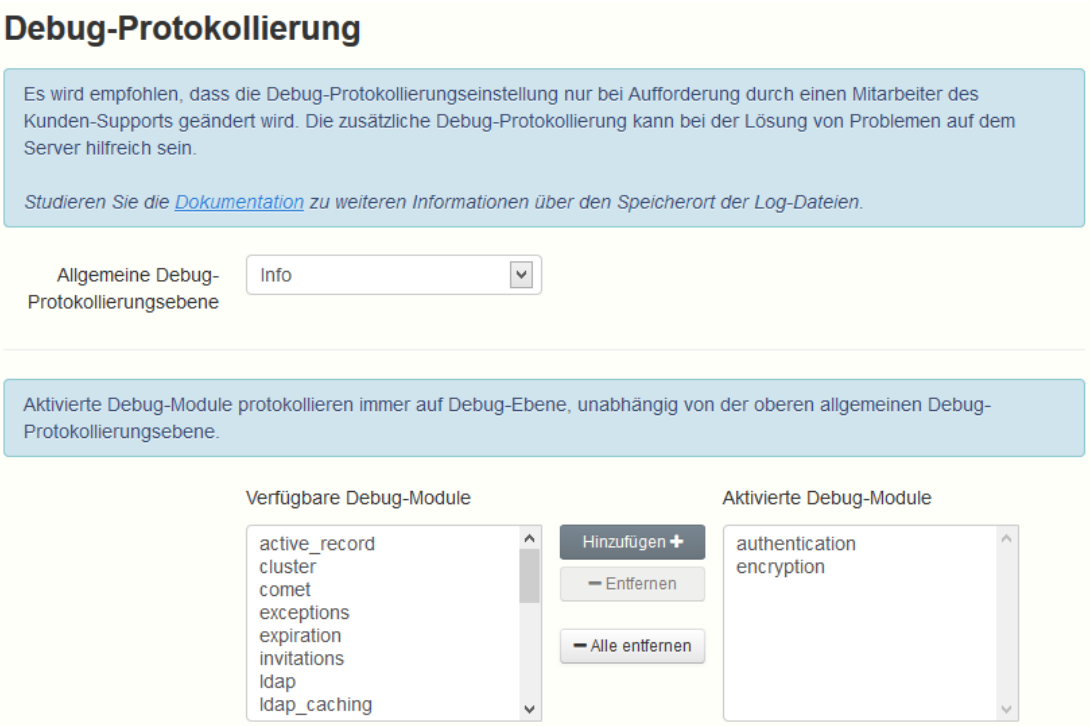


1. Rufen Sie die Weboberfläche auf und melden Sie sich als Administrator an.
2. Rufen Sie die Registerkarte **Allgemeine Einstellungen** auf, und öffnen Sie die Seite **Lizenzierung**.
3. Der Abschnitt **mobilEcho-Legacy-Lizenzen** enthält eine Liste aller Gateway Server, welche die alte Lizenzierung verwenden.
4. Klicken Sie für den gewünschten Gateway auf **Lizenz hinzufügen**, und geben Sie den Lizenzschlüssel ein.
5. Klicken Sie auf **Speichern**.

3.9 Debug-Protokollierung

Über die Einstellungen auf dieser Seite können erweiterte Protokollierungsinformationen aktiviert werden, die bei der Konfiguration und Fehlerbehebung von Acronis Access von Nutzen sind. Es wird empfohlen, diese Einstellungen nur bei Aufforderung durch einen Mitarbeiter des Kunden-Supports zu ändern. Die zusätzliche Debug-Protokollierung kann bei der Lösung von Problemen auf dem Server hilfreich sein.

Hinweis: *Informationen zur Aktivierung bzw. Deaktivierung der Debug-Protokollierung für einen bestimmten Gateway Server finden Sie im Abschnitt Server-Details (S. 41).*



Warnung: *Diese Einstellungen sollten nicht bei normalen Betriebs- und Produktionsbedingungen verwendet werden.*

- **Allgemeine Debug-Protokollierungsebene** – Legt die Hauptebene fest, die protokolliert werden soll (Info, Warnungen, fatale Fehler usw.)

Hinweis: *Aktivierte Debug-Module protokollieren immer auf Debug-Ebene, unabhängig von der oberen allgemeinen Debug-Protokollierungsebene.*

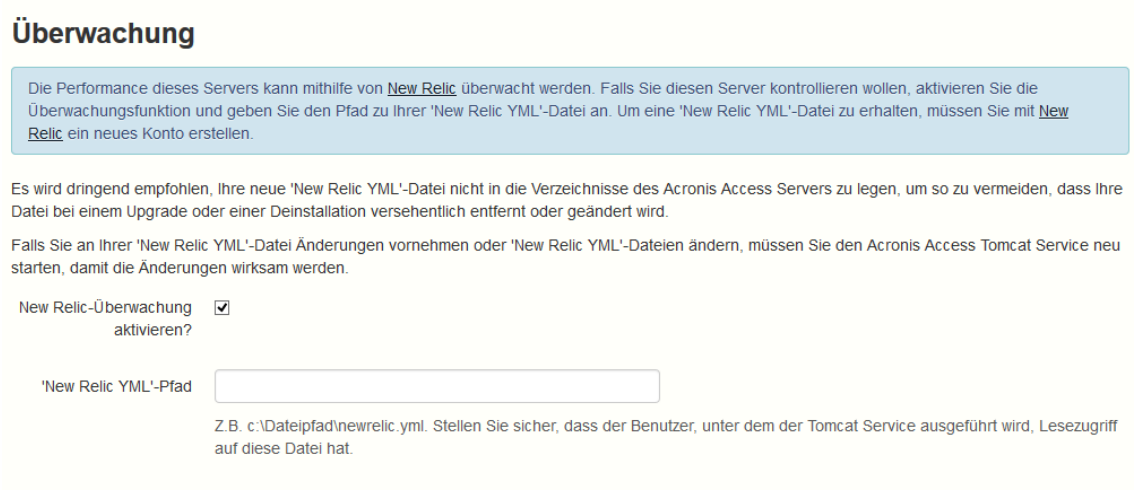
- **Verfügbare Debug-Module** – Zeigt eine Liste der verfügbaren Module an.
- **Aktivierte Debug-Module** – Zeigt die aktiven Module an.

Hinweis: *Falls es sich bei dem Produkt um eine Aktualisierung und nicht um eine Neuinstallation handelt, befinden sich die Log-Dateien im Ordner* ***C:\Programme (x86)\Group Logic\Common\apache-tomcat-7.0.42\logs****.*

Hinweis: *Bei einer Neuinstallation von Acronis Access befinden Sie die Log-Dateien im Ordner* ***C:\Programme (x86)\Acronis\Access\Common\apache-tomcat-7.0.42\logs***

3.10 Überwachung

Die Performance dieses Servers kann mithilfe von New Relic überwacht werden. Falls Sie diesen Server kontrollieren wollen, aktivieren Sie die Überwachungsfunktion, und geben Sie den Pfad zu Ihrer 'New Relic YML'-Datei an. Um eine 'New Relic YML'-Datei zu erhalten, müssen Sie mit New Relic ein neues Konto erstellen.



Hinweis: *Es wird dringend empfohlen, Ihre neue 'New Relic YML'-Datei nicht in den Verzeichnissen des Acronis Access Servers abzulegen, um so zu vermeiden, dass Ihre Datei bei einem Upgrade oder einer Deinstallation versehentlich entfernt oder geändert wird.*

Hinweis: *Falls Sie Änderungen an Ihrer 'New Relic YML'-Datei vornehmen oder 'New Relic YML'-Dateien ändern, müssen Sie den Acronis Access Tomcat-Dienst neu starten, damit die Änderungen wirksam werden.*

New Relic-Überwachung aktivieren? – Wenn diese Option aktiviert ist, müssen Sie den Pfad zur **New Relic**-Konfigurationsdatei (newrelic.yml) angeben.

New Relic installieren

Bei diesem Installationstyp überwachen Sie Ihre Acronis Access Server-Applikation, nicht den eigentlichen Computer, auf dem Sie die Installation vornehmen.

1. Öffnen Sie http://newrelic.com/ http://newrelic.com/ und erstellen Sie ein 'New Relic'-Konto.
2. Wählen Sie unter 'Applikationstyp' die Option 'Mobile App' aus.
3. Markieren Sie unter 'Plattform' den Eintrag 'Ruby'.
4. Schließen Sie die Kontoerstellung ab und melden Sie sich an.
5. Wechseln Sie zu 'Applikationen', übernehmen Sie das **Ruby-Bündel** (Schritt 1) wie vorliegend und gehen Sie zum nächsten Schritt über.
6. Laden Sie das New Relic-Skript, newrelic.yml, herunter.
7. Öffnen Sie die webbasierte Benutzeroberfläche von Acronis Access.
8. Wechseln Sie zu den Einstellungen und klicken Sie auf 'Überwachung'.
9. Geben Sie den Pfad zur Datei newrelic.yml, einschließlich der Erweiterung, ein (z.B. **`C:\software\newrelic.yml`**). Platzieren Sie diese Daten nach Möglichkeit in einem anderen Ordner als dem Ordner für Acronis Access, sodass sie bei einem Upgrade oder einer Deinstallation nicht entfernt oder geändert werden.

10. Klicken Sie auf 'Speichern' und warten Sie einige Minuten oder bis auf der New Relic-Website die Schaltfläche **Aktive Applikation(en)** verfügbar wird.
11. Wenn mehr als 10 Minuten vergehen, starten Sie den Acronis Access Tomcat-Dienst neu, und warten Sie einige Minuten. Die Schaltfläche sollte dann aktiv sein.
12. Sie sollten den Acronis Access Server auf der New Relic-Website überwachen können.

*Alle vom Acronis Access Server protokollierten Informationen zu Verbindungsversuchen mit New Relic und die Einrichtung der Überwachung befinden sich in einer Datei namens **newrelic_agent.log**, die sich an folgendem Speicherort befindet – **C:\Program Files (x86)\Acronis\Common\apache-tomcat-7.0.34\logs**. Wenn Probleme auftreten, finden Sie entsprechende Informationen in der Log-Datei.*

Häufig finden sich Warnungen oder Fehler, die wie folgt beginnen:
WARN : DNS Error caching IP address: Errno::ENOENT: No such file or directory - C:/etc/hosts which

Dies ist eine harmlose Nebenwirkung des Codes, der als Patch für ein anderes Problem mit New Relic verwendet wird.

Wenn Sie auch den eigentlichen Computer überwachen möchten, gehen Sie wie folgt vor:

1. Öffnen Sie http://newrelic.com/ http://newrelic.com/ und melden Sie sich bei Ihrem Konto an.
2. Klicken Sie auf 'Server' und laden Sie das richtige Installationsprogramm von New Relic für Ihr Betriebssystem herunter.
3. Installieren Sie den Monitor von New Relic auf Ihrem Server.
4. Der neue Server-Monitor von New Relic erfordert Microsoft .NET Framework 4. Der vom Installationsprogramm von New Relic verwendete Link gilt nur für das Client-Profil von Microsoft .NET Framework 4. Sie müssen zum Microsoft Download Center wechseln und das gesamte .NET Framework 4 aus dem Internet herunterladen, bevor Sie das Installationsprogramm für den Server-Monitor von New Relic ausführen.

- Warten Sie, bis New Relic Ihren Server erkannt hat.

4 Wartungsaufgaben

Falls Sie ein Backup aller Elemente von Acronis Access erstellen möchten und um die Best Practices und Backup-Verfahren einzuhalten, sollten Sie den Artikel Richtlinien zum Desaster-Recovery (S. 91) lesen.

Themen

4.1 Richtlinien für Desaster-Recovery

Hohe Verfügbarkeit und schnelle Wiederherstellungen sind für geschäftskritische Applikationen wie Acronis Access von höchster Bedeutung. Aufgrund geplanter oder ungeplanter Umstände, die von lokalen Hardwareausfällen bis hin zu Netzwerkstörungen und Wartungsaufgaben reichen, kann es erforderlich werden, in kürzester Zeit die Mittel bereitzustellen, um Acronis Access wieder in einen funktionsfähigen Zustand zu versetzen.

Einführung:

Für geschäftskritische Applikationen wie Acronis Access ist eine hohe Verfügbarkeit von höchster Bedeutung. Aufgrund der verschiedensten Umstände, die von lokalen Hardwareausfällen bis hin zu Netzwerkstörungen und Wartungsaufgaben reichen, kann es erforderlich werden, in kürzester Zeit die Mittel bereitzustellen, um Acronis Access wieder in einen funktionsfähigen Zustand zu versetzen.

Es gibt verschiedene Wege, die Möglichkeit für ein Desaster-Recovery zu implementieren, darunter Backup-Wiederherstellung, Imaging, Virtualisierung und Clustering. In den folgenden Abschnitten gehen wir auf den Ansatz 'Backup/Wiederherstellung' ein.

Beschreibung der Elemente von Acronis Access:

Acronis Access ist eine Lösung, die mehrere separate, jedoch miteinander verbundene Elemente umfasst:

Acronis Access Gateway Server

Hinweis**: Befindet sich normalerweise hier: **`C:\Program Files (x86)\Acronis\Access\Gateway Server`

Acronis Access Server

Hinweis**: Befindet sich normalerweise hier: **`C:\Program Files (x86)\Acronis\Access\Access Server`

Acronis Access Konfigurationswerkzeug

Hinweis**: Befindet sich normalerweise hier: **`C:\Program Files (x86)\Acronis\Access\Configuration Utility`

Dateispeicher

Der Speicherort für den **Dateispeicher** wird während der Installation festgelegt, wenn Sie das **Konfigurationswerkzeug** zum ersten Mal verwenden.

Hinweis: *Die Dateispeicherstruktur enthält die Benutzerdateien und -ordner in verschlüsselter Form. Diese Struktur kann mit einem standardmäßigen Kopiertool für Dateien (robocopy, xtree) kopiert oder gesichert werden. Normalerweise sollte sich diese Struktur in einem hochverfügbaren Netzwerk-Volume oder NAS befinden. Der Speicherort kann also von der Vorgabe abweichen.*

PostGreSQL-Datenbank. Dies ist ein separates Element, das als Windows-Dienst ausgeführt und von Acronis Access installiert und verwendet wird. Die Acronis Access Datenbank ist eines der wichtigsten Elemente, da darin alle Konfigurationen, Beziehungen zwischen Benutzern und Dateien sowie die Datei-Metadaten aufbewahrt werden.

All diese Komponenten werden benötigt, um eine funktionsfähige Instanz von Acronis Access zu bilden.

Zum Implementieren eines schnellen Wiederherstellungsprozesses benötigte Ressourcen

Für einen Desaster-Recovery-Prozess werden die folgenden Ressourcen benötigt:

- Geeignete Hardware zum Hosten des Betriebssystems, der Anwendung und der zugehörigen Daten. Die Hardware muss die System- und Softwareanforderungen für die Anwendung erfüllen.
- Ein Backup- und Wiederherstellungsverfahren, um sicherzustellen, dass zu dem Zeitpunkt, an dem die Umstellung stattfinden soll, alle Software- und Datenelemente vorliegen.
- Netzwerkkonnektivität, einschließlich interner und externer Firewall- und Routing-Regeln, die dem Benutzer ohne oder mit nur minimalen Änderungen der Client-Einstellungen Zugriff auf den neuen Knoten gestatten.
- Netzwerkzugriff für Acronis Access, um einen Active Directory-Domain-Controller und SMTP-Server zu kontaktieren.
- Möglichkeit schneller oder automatischer DNS-Umschaltung, um eingehende Anfragen an den sekundären Knoten weiterzuleiten.

Der Prozess

Backup-Setup

Der empfohlene Ansatz zum Sicherstellen eines sicheren und schnellen Wiederherstellungsszenarios lässt sich folgendermaßen beschreiben:

1. Stellen Sie eine Installation von Acronis Access einschließlich aller Elemente auf dem sekundären Wiederherstellungsknoten bereit. Wenn dies nicht möglich ist, ist eine vollständige Sicherungskopie bzw. ein Image des Quellgeräts eine angemessene Alternative. In virtualisierten Umgebungen sind periodische Snapshots eine wirksame und kostengünstige Alternative.
2. Legen Sie regelmäßig Backups der Acronis Access Server-Software-Suite (alle oben genannten Elemente, einschließlich des gesamten Apache Software-Zweigs) an. Verwenden Sie für diese Aufgabe eine Backup-Lösung des Unternehmens-Standards.
3. Legen Sie so oft wie möglich Backups vom Dateispeicher an. Hierfür kann eine standardmäßige Backup-Lösung verwendet werden, aufgrund der beträchtlichen Datenmenge ist jedoch ein

automatisiertes Tool für differentielle Backups am besten geeignet und vorzuziehen. Differentielle Backups verkürzen die Zeit, die für diesen Vorgang benötigt wird, da nur die Unterschiede zwischen dem Quell- und dem Ziel-Datenspeicher gesichert werden.

4. Legen Sie so oft wie möglich Backups der Acronis Access Datenbank an. Dies erfolgt durch ein automatisiertes Datenbank-Dump-Skript, das vom Windows Task Scheduler ausgelöst wird. Der Datenbank-Dump sollte anschließend mit einem standardmäßigen Backup-Tool gesichert werden.

Wiederherstellung

Wenn die im obigen Abschnitt genannten Bedingungen erfüllt sind, ist der Vorgang zum Online-Schalten der Backup-Ressourcen relativ einfach:

1. Starten Sie den Recovery-Knoten. Passen Sie gegebenenfalls die Netzwerkkonfiguration wie IP-Adresse, Host-Name usw. an. Testen Sie die Active Directory-Verbindung und den SMTP-Zugriff.
2. Führen Sie die Wiederherstellung bei Bedarf aus dem letzten Acronis Access Software-Suite-Backup aus.
3. Vergewissern Sie sich, dass Tomcat nicht ausgeführt wird (Windows Dienststeuerung).
4. Stellen Sie gegebenenfalls den Dateispeicher wieder her. Stellen Sie sicher, dass der relative Speicherort des Dateispeichers der gleiche wie auf dem Quellcomputer ist. Wenn dies nicht der Fall ist, muss der Speicherort anhand des Konfigurationswerkzeugs angepasst werden.
5. Vergewissern Sie sich, dass der PostgreSQL-Dienst ausgeführt wird (Windows Systemsteuerung/Dienstverwaltung).
6. Stellen Sie die Acronis Access Datenbank wieder her.
7. Starten Sie den Acronis Access Tomcat-Dienst.
8. Migrieren Sie das DNS, sodass es auf den neuen Knoten verweist.
9. Vergewissern Sie sich, dass Active Directory und SMTP ordnungsgemäß funktionieren.

4.2 Backup und Wiederherstellung von Acronis Access

Dies ist erforderlich, wenn Sie ein Upgrade, Update oder eine Wartung des Acronis Access Servers durchführen. In diesem Artikel werden Ihnen die Grundlagen vermittelt, um ein Backup und eine Wiederherstellung der Datenbank durchzuführen.

Backup von Datenbanken

Backup der Acronis Access-Datenbank

Mit dem folgenden Verfahren wird eine *.sql-Datei erstellt, die eine Textdarstellung der Quelldatenbank enthält.

1. Öffnen Sie ein Eingabeaufforderungsfenster und navigieren Sie zum Ordner **`9.2\bin`** im PostgreSQL-Installationsverzeichnis.
   z. B. **`cd "C:\PostgreSQL\9.2\bin"`**

2. Sobald Sie als Verzeichnis für die Eingabeaufforderung den Ordner **bin** festgelegt haben, geben Sie die folgende Zeile ein:
   `pg_dump -U postgres -f mybackup.sql acronisaccess_production`
   Dabei ist **`mybackup.sql`** der gewünschte Dateiname für die von Ihnen erstellte Backup-Datei. Dies kann die vollständige Pfadangabe für den Speicherort einschließen, an dem die Backup-Datei erstellt werden soll, zum Beispiel: **`D:\Backups\mybackup.sql`**

   Hinweis: ***`acronisaccess_production`*** *muss genau wie gezeigt eingegeben werden, da dies der Name der Acronis Access-Datenbank ist.*

3. Eine Zeile 'Password:' wird angezeigt. Geben Sie das postgres-Kennwort ein, das Sie während der Installation von Acronis Access festgelegt haben.

   Hinweis: *Die Eingabe des Kennworts bewirkt keine sichtbaren Änderungen im Fenster mit der Eingabeaufforderung.*

4. Die Backup-Datei erscheint standardmäßig im Ordner **bin**, es sei denn, es wurde ein vollständiger Pfad zu einem anderen Verzeichnis für die Ausgabedatei festgelegt.

Hinweis: *Wenn Sie ein Backup der gesamten PostgreSQL-Datenbank erstellen möchten, können Sie auch folgenden Befehl verwenden:*

`pg_dumpall -U postgres > alldbs.sql`

Dabei gibt ***`alldbs.sql`*** *die generierte Backup-Datei an. Sie können auch eine vollständige Pfadspezifikation einschließen, zum Beispiel* ***`D:\Backups\alldbs.sql`***

Die vollständige Syntax für diesen Befehl finden Sie unter:
http://www.postgresql.org/docs/9.2/static/app-pg-dumpall.html
http://www.postgresql.org/docs/9.1/static/app-pg-dumpall.html

Info: *Weitere Informationen zum Backup-Verfahren für PostgreSQL und zur Befehlssyntax finden Sie unter:*
http://www.postgresql.org/docs/9.2/static/backup.html
http://www.postgresql.org/docs/9.1/static/backup.html

Backup der Gateway Server-Datenbank

1. Wechseln Sie zu dem Server, auf dem der Acronis Access Gateway Server installiert ist.
2. Navigieren Sie zum Ordner mit der Datenbank.

   Hinweis: *Der Standardspeicherort ist:* ***`C:\Program Files (x86)\Acronis\Access\Gateway Server\database`***

3. Kopieren Sie die Datei **mobilEcho.sqlite3** an einen sicheren Speicherort.

Acronis Access wiederherstellen

Acronis Access-Datenbank wiederherstellen

Das Verfahren zum Wiederherstellen der Datenbank ähnelt dem Backup-Verfahren.

1. Bevor Sie den Befehl zum Wiederherstellen der Datenbank eingeben, sollten Sie sich vergewissern, dass die Quell-Backupdatei in einem Verzeichnis oder an einem Speicherplatz vorliegt, auf den der angemeldete Benutzer zugreifen kann.

2. Öffnen Sie ein Eingabeaufforderungsfenster und navigieren Sie zum Ordner **9.2\bin** im PostgreSQL-Installationsverzeichnis.
   cd "**C:\PostgreSQL\9.2\bin**"

   Hinweis: *Falls Sie PostgreSQL an einem anderen Speicherort installiert haben, geben Sie das entsprechende Verzeichnis an.*

3. Sie müssen zunächst die alte Datenbank entfernen. Dazu stoppen Sie den Acronis Access Tomcat-Dienst und geben die folgende Zeile ein:

   Warnung! *Fahren Sie erst dann mit diesem Schritt fort, wenn Sie sicher sind, dass Sie ein erfolgreiches Backup durchgeführt haben. Das Entfernen der Datenbank ist ein unumkehrbarer Vorgang, bei dem die gesamte Datenbank gelöscht wird. Sämtliche Information gehen verloren.*

   dropdb -U postgres acronisaccess_production

   Es wird möglicherweise die Meldung '*password for user* **postgres***:*' angezeigt. Geben Sie in diesem Fall das **postgres**-Kennwort ein, das Sie während der Installation von Acronis Access festgelegt haben.
   acronisaccess_production muss genauso eingegeben werden wie angezeigt. Dies ist der Name der **Acronis Access** Datenbank.

4. Nachdem der Vorgang abgeschlossen wurde, geben Sie die folgende Zeile ein:
   createdb -U postgres acronisaccess_production

   Es wird möglicherweise die Meldung '*password for user* **postgres***:*' angezeigt. Geben Sie in diesem Fall das **postgres**-Kennwort ein, das Sie während der Installation von Acronis Access festgelegt haben.
   acronisaccess_production muss genauso eingegeben werden wie angezeigt. Dies ist der Name der **Acronis Access** Datenbank.

5. Um die neu erstellte Datenbank mit Informationen aus Ihrem Backup zu füllen, geben Sie die folgende Zeile ein:
   psql -U postgres -d acronisaccess_production -W -f mybackup.sql

   Ersetzen Sie **mybackup.sql** durch den vollständigen Namen der Backup-Datei, zum Beispiel: **D:\Backups\mybackup.sql**
   Es wird möglicherweise die Meldung '*password for user* **postgres***:*' angezeigt. Geben Sie in diesem Fall das **postgres**-Kennwort ein, das Sie während der Installation von Acronis Access festgelegt haben.
   acronisaccess_production muss genauso eingegeben werden wie angezeigt. Dies ist der Name der **Acronis Access** Datenbank.

6. Nachdem der Vorgang erfolgreich abgeschlossen wurde, starten Sie den postgres-Dienst neu, und starten Sie den Acronis Access Tomcat-Dienst.

Hinweis: *Die Eingabe des Kennworts bewirkt keine sichtbaren Änderungen im Fester mit der Eingabeaufforderung.*

Info: *Informationen zur vollständigen* ***psql*** *-Befehlssyntax finden Sie unter*
http://www.postgresql.org/docs/9.2/static/app-psql.html
http://www.postgresql.org/docs/9.0/static/app-psql.html

Gateway Server-Datenbank wiederherstellen

1. Kopieren Sie die zuvor gesicherte Datei **mobilEcho.sqlite3**.
2. Wechseln Sie zu dem Server, auf dem der Acronis Access Gateway Server installiert ist.
3. Navigieren Sie zum Ordner mit der Datenbank und fügen Sie die Datei **mobilEcho.sqlite3** ein.

   Hinweis: *Der Standardspeicherort ist:* ***C:\Program Files (x86)\Acronis\Access\Gateway Server\database***

4. Starten Sie den Dienst **Acronis Access Gateway Server** neu.

4.3 Tomcat Log-Verwaltung unter Windows

Tomcat erstellt und schreibt im Rahmen des normalen Betriebs Informationen in eine Reihe von Logdateien.

Diese Dateien können sich ansammeln und wertvollen Speicherplatz belegen, sofern sie nicht regelmäßig bereinigt werden. Es wird von der IT-Community allgemein akzeptiert, dass der Informationswert dieser Logs sehr schnell abnimmt. Sofern nicht andere Faktoren wie Vorschriften oder Compliance mit bestimmten Richtlinien eine Rolle spielen, müssen diese Logdateien lediglich eine bestimmte Anzahl von Tagen im System gehalten werden.

Einführung:

Tomcat erstellt und schreibt im Rahmen des normalen Betriebs Informationen in eine Reihe von Logdateien. Unter Windows befinden sich diese Dateien normalerweise in folgendem Verzeichnis:

"**C:\Program Files (x86)\Acronis\Access\Common\apache-tomcat-7.0.34\logs**"
Acronis Access speichert seine eigenen Logs im gleichen Verzeichnis als separate Dateien.

Die Logdateien von Acronis Access haben den Namen ***acronisaccess_date****.*

Es sind zahlreiche Tools verfügbar, die das Löschen unnötiger Logdateien automatisieren. Wir verwenden für unser Beispiel den in Windows verfügbaren Befehl ForFiles.

Info: *Informationen zu ForFiles einschließlich Befehlssyntax und Beispielen finden Sie unter http://technet.microsoft.com/en-us/library/cc753551(v=ws.10).aspx*
http://technet.microsoft.com/en-us/library/cc753551(v=ws.10).aspx

Ein Beispielverfahren:

Das unten beschriebene Beispielverfahren automatisiert den Prozess des Bereinigens von Logdateien, die älter sind als eine bestimmte Anzahl von Tagen. In der Beispiel-Batchdatei ist diese Zahl als Parameter definiert und kann daher für unterschiedliche Aufbewahrungsrichtlinien angepasst werden.

Info: *Das Beispielskript (Batchdatei) funktioniert unter Windows 2003 und Windows 2008. Klicken Sie hier, um dieses Skript herunterzuladen.*
Sie können das Skript auf Wunsch auch kopieren, in ein leeres Textdokument einfügen und unter 'AASTomcatLogPurge.bat' speichern.

Klicken Sie hier für den vollständigen Code das Batch-Skripts...

```
ECHO OFF
 REM Script: aETomcatLogsPurge.bat
 REM 2012-05-12: Version: 1.0: MEA: Created
ECHO This script will delete files older than a number of days from a directory
 ECHO Run it from the command line or from a scheduler
 ECHO Make sure the process has permissions to delete files in the target folder
REM ===== CONFIGURATIONS ==================================================
REM Note: all paths containing spaces must be enclosed in double quotes
 REM Edit this file and set LogPath and NumDays below
REM Path to the folder where all Tomcat logs are
 set LogPath="C:\Program Files (x86)\Group
Logic\Common\apache-tomcat-7.0.34\logs"


REM NumDays - Log files older than NumDays will be processed
 set NumDays=14
REM ===== END OF CONFIGURATIONS ======================
ECHO
ECHO ===== START ============
REM ForFiles options:
 REM "/p": the path where you want to delete files.
 REM "/s": recursively look inside other subfolders present in the folder
mentioned in the batch file path
 REM "/d": days for deleting the files older than the present date. For instance
"/d -7" means older than 7 days
 REM "/c": command to execute to actually delete files: "cmd /c del @file".
forfiles /p %LogPath% /s /d -%NumDays% /c "cmd /c del @FILE"
:End
ECHO ===== BATCH FILE COMPLETED ============================================
```

Warnung: *Dieses Beispiel ist als Richtlinie gedacht, damit Sie Ihren Prozess basierend auf Ihrem spezifischen Deployment planen und implementieren können. Das Beispiel ist nicht für die Verwendung in allen Situationen und Umgebungen gedacht und wurde auch nicht in diesen getestet. Verwenden Sie es als Ausgangsbasis und auf eigene Gefahr.* ***Verwenden Sie das Beispiel nicht in Umgebungen für produktiven Einsatz, ohne zuvor umfassende Offline-Tests durchgeführt zu haben.***

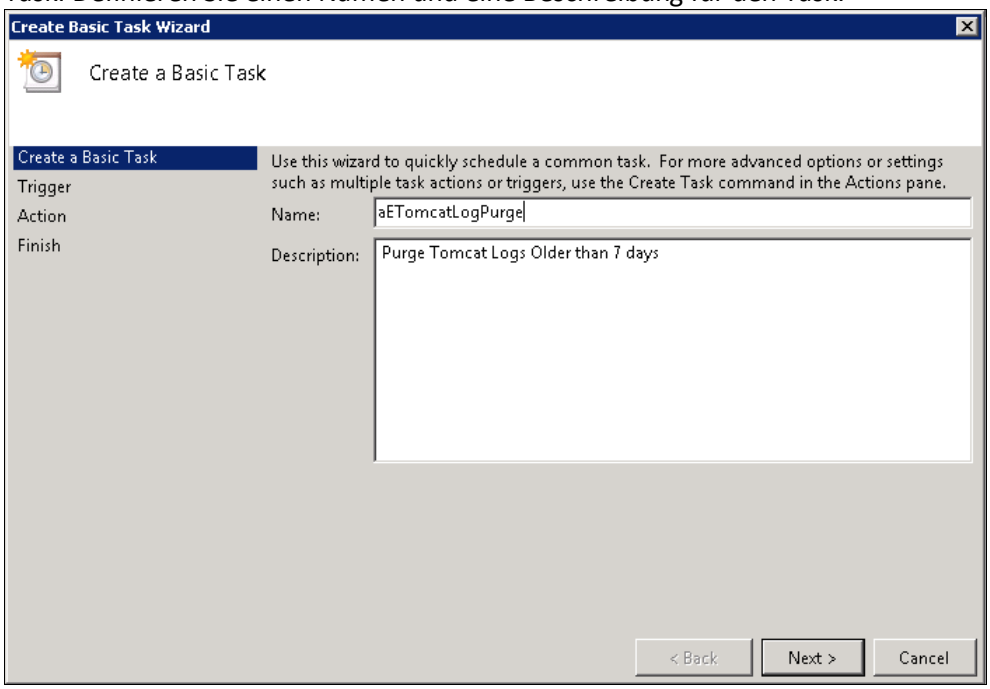
Schritte:

1. Kopieren Sie das Skript auf den Computer, auf dem Acronis Access (Tomcat) ausgeführt wird, und öffnen Sie es mit Notepad oder einem anderen reinen Texteditor.
2. Suchen Sie nach dem im unteren Bild dargestellten Abschnitt und bearbeiten Sie die Variablen LogPath und NumDays. Geben Sie darin Ihre spezifischen Pfade und Aufbewahrungseinstellungen an:

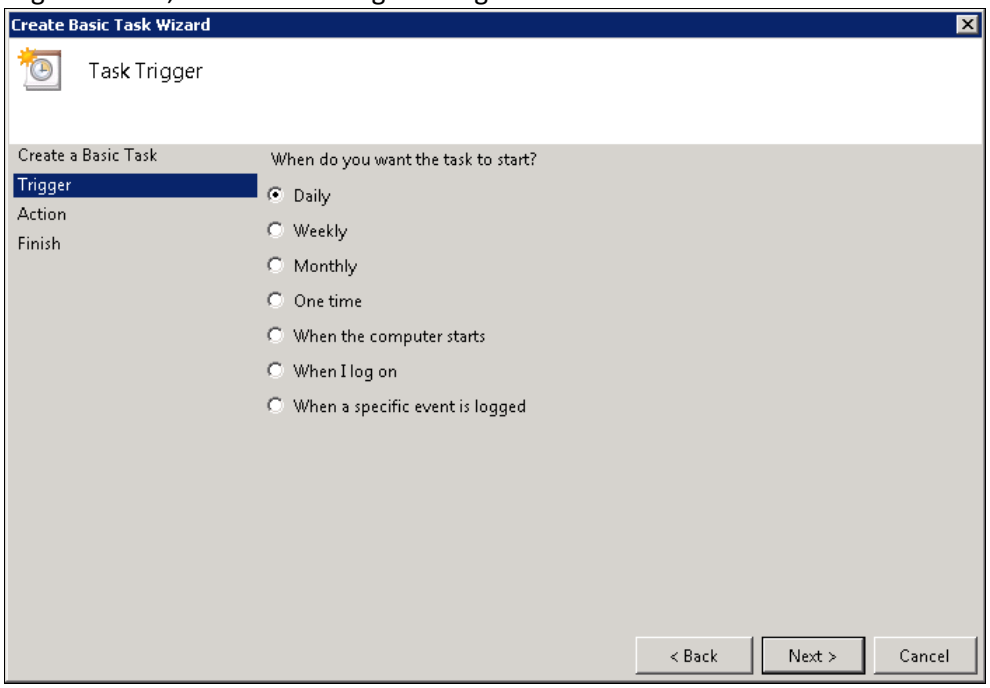
```
REM ===== CONFIGURATIONS ==================================================
REM Note: all paths containing spaces must be enclosed in double quotes
 REM Edit this file and set LogPath and NumDays below
REM Path to the folder where all Tomcat logs are
 set LogPath="C:\Program Files (x86)\Group Logic\Common\apache-tomcat-7.0.34\logs"

REM NumDays - Log files older than NumDays will be processed
 set NumDays=14
REM ===== END OF CONFIGURATIONS ======================
ECHO
ECHO ===== START ============
```

In Acronis Access werden die Logdateien im gleichen Ordner wie diejenigen von Tomcat gespeichert.
*(**C:\Program Files (x86)\Acronis\Access\Common\apache-tomcat-7.0.34\logs**)*

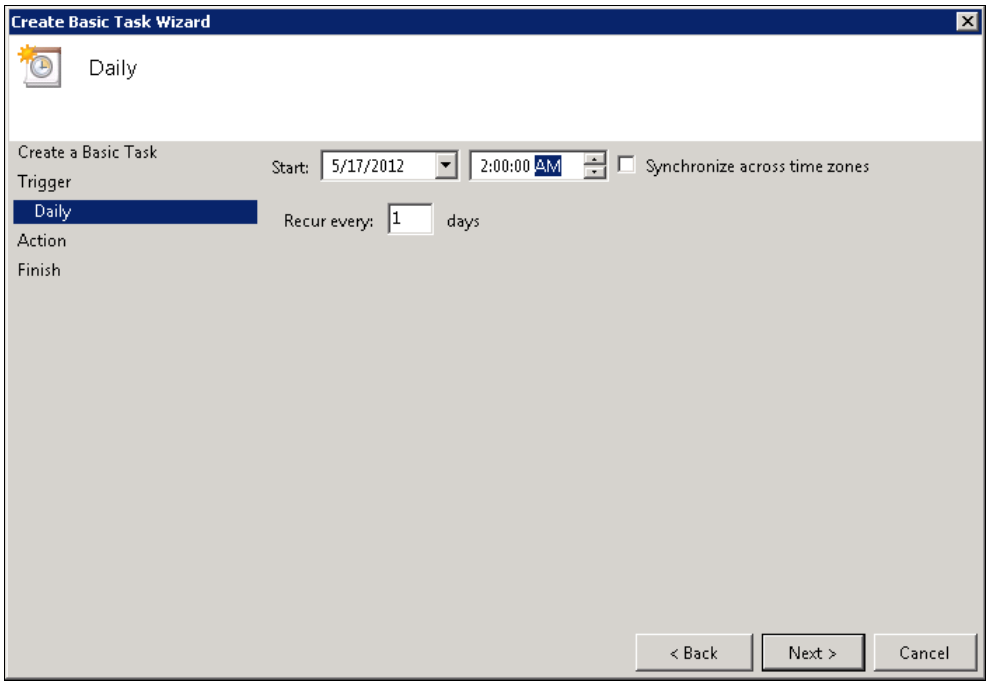
3. Speichern Sie die Datei.
4. Öffnen Sie zum Automatisieren des Prozesses den Task Scheduler, und erstellen Sie eine neue Task. Definieren Sie einen Namen und eine Beschreibung für den Task.



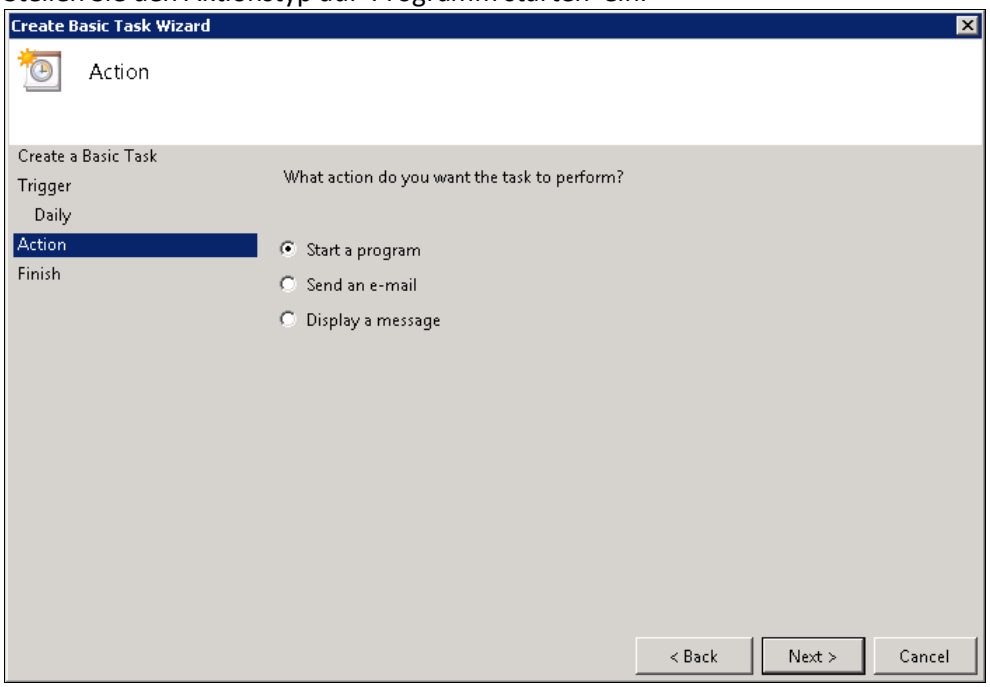
5. Legen Sie fest, dass der Task täglich ausgeführt wird.



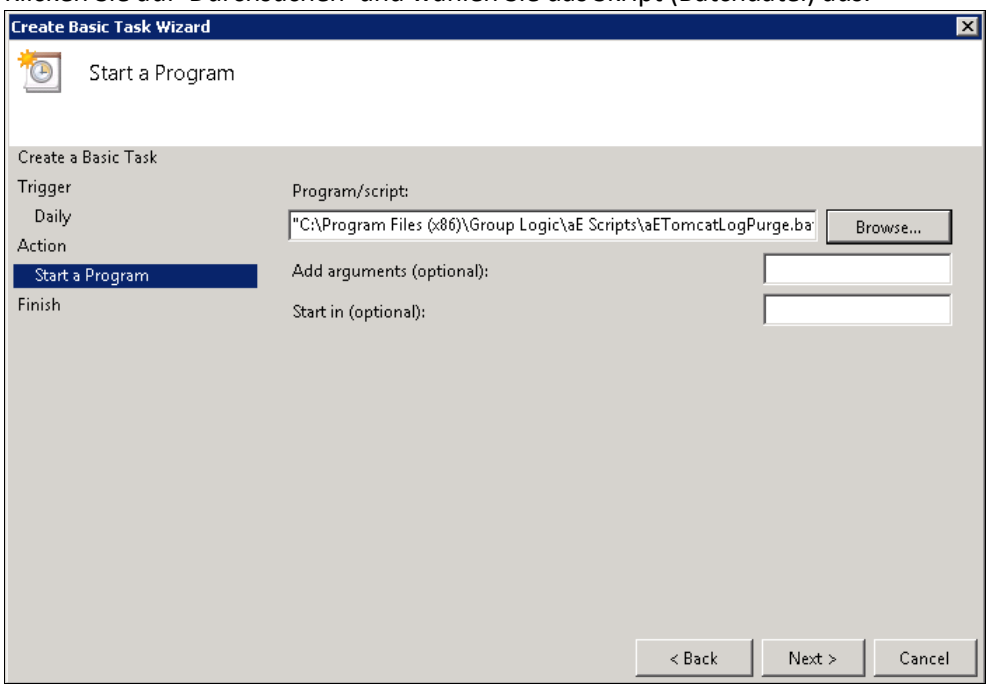
6. Geben Sie an, zu welcher Uhrzeit die Task starten soll. Es wird empfohlen, diesen Prozess nicht auszuführen, wenn das System extrem belastet ist oder andere Wartungsprozesse ausgeführt werden.



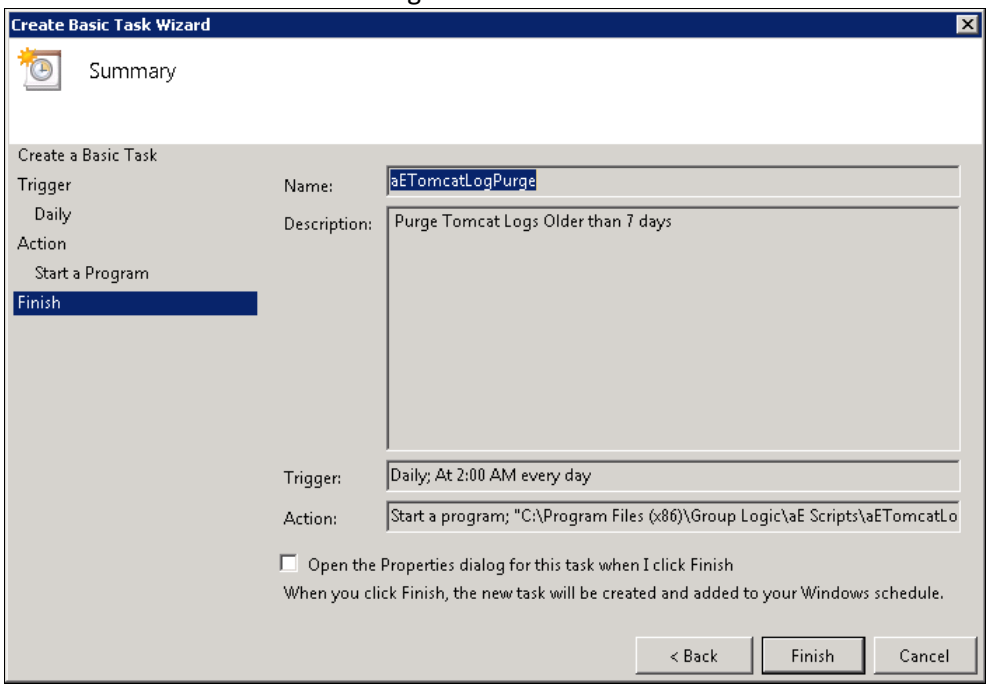
7. Stellen Sie den Aktionstyp auf 'Programm starten' ein.



8. Klicken Sie auf 'Durchsuchen' und wählen Sie das Skript (Batchdatei) aus.



9. Klicken Sie abschließend auf 'Fertig stellen'.



10. Falls dieser Prozess unbeaufsichtigt stattfinden soll, können Sie in der Taskliste mit der rechten Maustaste auf eine Task klicken, 'Eigenschaften' auswählen und sich vergewissern, dass die Task ausgeführt wird, ob der Benutzer angemeldet ist oder nicht.
11. Sie können sich überzeugen, dass die Task korrekt konfiguriert ist und ordnungsgemäß funktioniert, indem Sie die Task auswählen, mit der rechten Maustaste darauf klicken und 'Ausführen' wählen. Im Scheduler-Log sollten Start, Stopp sowie etwaige Fehler aufgezeichnet werden.

5 Ergänzendes Material

Themen

5.1 In Konflikt stehende Software

Einige Software-Produkte können zu Problemen mit Acronis Access führen. Die derzeit bekannten Konflikte sind im Folgenden aufgelistet:

- **VMware View™ Persona Management** – Diese Applikation verursacht Probleme mit dem Synchronisierungsprozess des Acronis Access-Desktop-Clients und Probleme beim Löschen von Dateien. Wenn Sie den Acronis Access-Synchronisierungsordner außerhalb des **Persona Management-Benutzerprofils** platzieren, sollten die bekannten Konflikte sich vermeiden lassen.

5.2 Lastenausgleich für Acronis Access

Es gibt zwei Hauptmöglichkeiten für den Lastenausgleich von Acronis Access:

Lastenausgleich nur für Gateway Server vornehmen

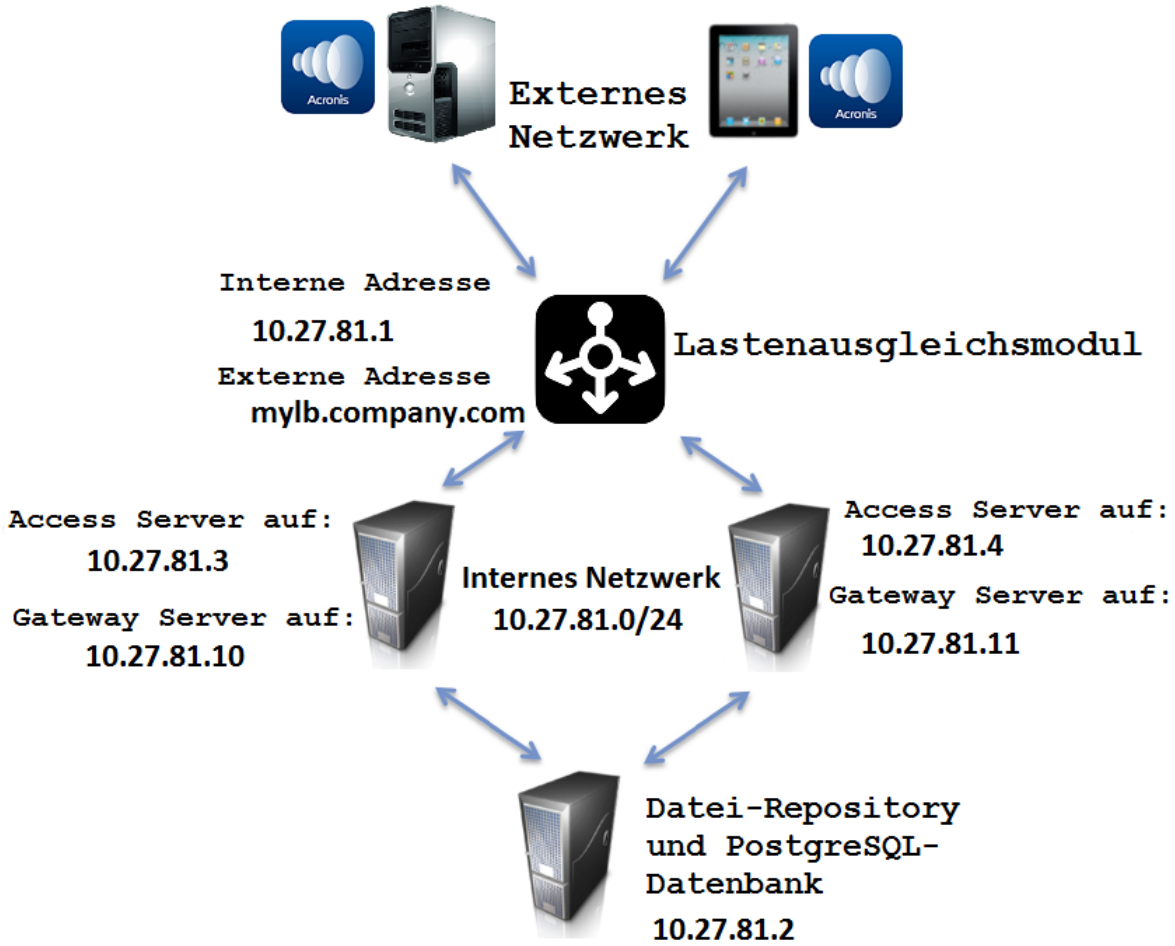
Diese Konfiguration stellt sicher, dass für die Komponenten mit der höchsten Belastung (die Gateway Server) ein Lastenausgleich vorgenommen wird und sie für die mobilen Clients stets verfügbar sind. Der Access Server befindet sich nicht hinter dem Lastenausgleichsmodul, da er nicht benötigt wird, um für nicht verwalteten Zugriff eine Verbindung zu den Gateway Servern herzustellen. Weitere Informationen finden Sie im Artikel Cluster-Gruppen (S. 51).

Lastenausgleich für alle Komponenten von Acronis Access vornehmen

Bei dieser Konfiguration wird ein Lastenausgleich für alle Komponenten von Acronis Access vorgenommen und hohe Verfügbarkeit für alle Benutzer gewährleistet. Um dieses Setup zu testen,

benötigen Sie mindestens zwei getrennte Maschinen. Viele der Einstellungen beim Konfigurieren des Lastenausgleichs unterscheiden sich bei unterschiedlicher Soft- und Hardware. Daher werden sie in dieser Anleitung nicht behandelt.

Im Setup-Beispiel werden drei getrennte Maschinen verwendet. Eine fungiert als Datei-Repository und Datenbank, die anderen beiden jeweils als Access- und Gateway Server. Nachfolgend finden Sie eine Anleitung zur Konfiguration dieses Setups.



Diese Anleitung enthält alle notwendigen Details, um den Lastenausgleich für das Produkt Acronis Access in Ihrer Umgebung ordnungsgemäß vorzunehmen.

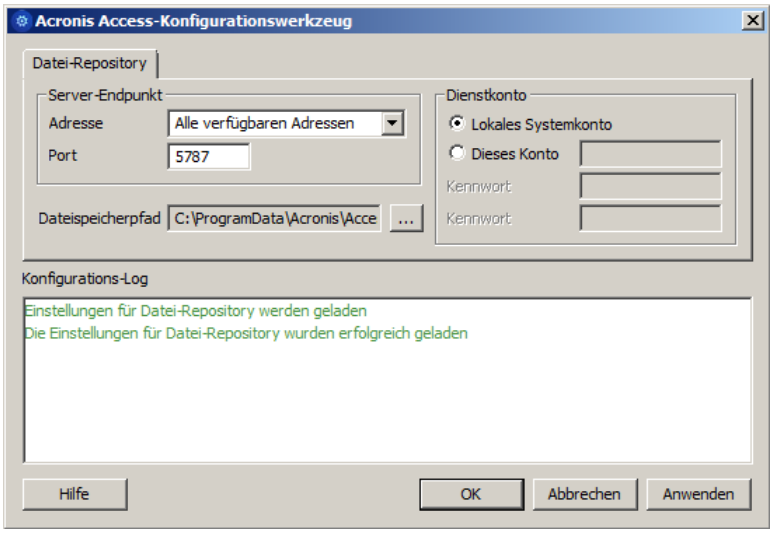
Gehen Sie auf dem Server, der die PostgreSQL-Datenbank und das Datei-Repository hostet, wie folgt vor:

1. Starten Sie das Installationsprogramm von Acronis Access, und klicken Sie auf **Weiter**. Lesen und akzeptieren Sie die Lizenzvereinbarung.
2. Wählen Sie im Access-Installationsprogramm **Benutzerdefiniert**. Wählen Sie **Acronis Access Datei-Repository** und **PostgreSQL Database Server** aus, und klicken Sie auf **Weiter**.
3. Wählen Sie den Speicherort aus, an dem das Datei-Repository und das Konfigurationswerkzeug installiert werden sollen.

4. Wählen Sie den Speicherort aus, an dem PostgreSQL installiert werden soll, und geben Sie ein Kennwort für den Super-User **postgres** ein.
5. Öffnen Sie den TCP-Port 5432. Mit dessen Hilfe greifen Sie von den Remote-Maschinen aus auf die PostgreSQL-Datenbank zu.
6. Fahren Sie nach Abschluss des Installationsvorgangs mit dem Konfigurationswerkzeug fort.
   a. Sie werden aufgefordert, das Konfigurationswerkzeug zu öffnen. Drücken Sie **OK**.
   b. Wählen Sie die Adresse und den Port für den Zugriff auf das Datei-Repository aus.

   Hinweis: *Sie müssen dieselbe Adresse und denselben Port in der Weboberfläche von Acronis Access festlegen. Weitere Informationen finden Sie in den Artikeln Das Konfigurationswerkzeug verwenden und Datei-Repository (S. 71).*

   c. Wählen Sie den Pfad zum Dateispeicher aus. Dort werden die eigentlichen Dateien gespeichert.



   d. Klicken Sie auf **OK**, um die Änderungen zu übernehmen, und schließen Sie das **Konfigurationswerkzeug**.
7. Navigieren Sie zum Installationsverzeichnis von PostgreSQL (z.B. C:\Programme\PostgreSQL\9.2\data\), und bearbeiten Sie **pg_hba.conf** mit einem Texteditor.
8. Beziehen Sie die Host-Einträge für alle Access-Server unter Verwendung ihrer internen Adressen ein, und speichern Sie die Datei. Die Datei **pg_hba.conf** (HBA steht für host-basierte Authentifizierung) steuert die Client-Authentifizierung und wird im Datenverzeichnis des Datenbank-Clusters gespeichert. Darin geben Sie an, welche Server eine Verbindung herstellen dürfen und welche Berechtigungen sie haben sollen, z.B.:

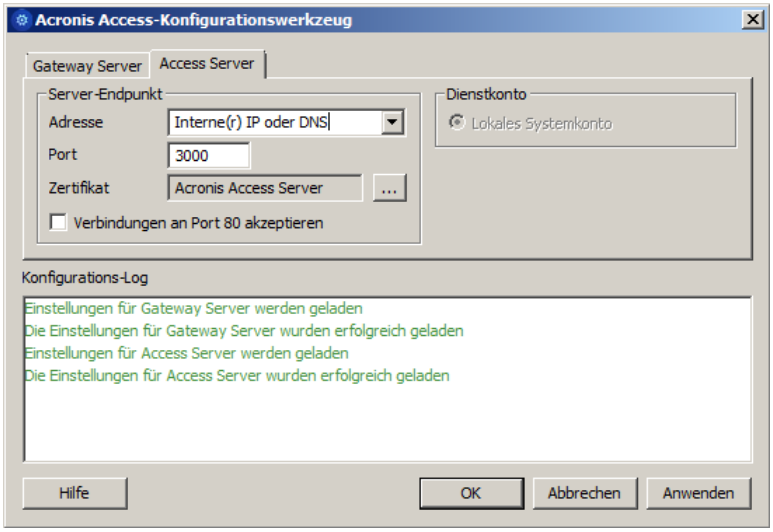
```
# TYPE DATABASE USER ADDRESS       METHOD
# Loadbalancer1 (First Acronis Access & Gateway server)
host     all       all   10.27.81.3/32    md5
# Loadbalancer2 (Second Acronis Access & Gateway server)
host     all       all   10.27.81.4/32    md5
In these examples all users connecting from 10.27.81.3/32 and
10.27.81.4/32 can access the database with full privileges (except
the replication privilege) via a md5 encrypted connection.
```

9. Öffnen Sie das Tool **pgAdmin**, und stellen Sie eine Verbindung zum lokalen Server her. Wählen Sie **Datenbanken** aus, und klicken Sie entweder mit der rechten Maustaste, oder wählen Sie **Neue Datenbank** im Menü **Bearbeiten** -> **Neues Objekt** aus, um eine neue Datenbank zu erstellen. Nennen Sie sie **acronisaccess_production**.

Gehen Sie auf den beiden Servern, die als Access und Gateway Server fungieren, wie folgt vor:

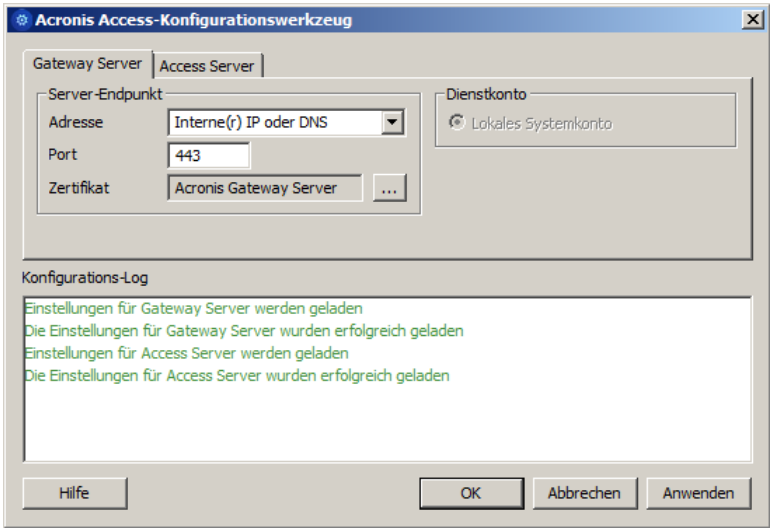
1. Starten Sie das Installationsprogramm von Acronis Access, und klicken Sie auf **Weiter**. Lesen und akzeptieren Sie die Lizenzvereinbarung.
2. Wählen Sie im Access-Installationsprogramm **Benutzerdefiniert**. Wählen Sie nur **Acronis Access Server** und **Acronis Access Gateway Server** aus, und fahren Sie mit dem Installationsvorgang fort.
3. Fahren Sie nach Abschluss des Installationsvorgangs mit dem Konfigurationswerkzeug fort.
   a. Sie werden aufgefordert, das Konfigurationswerkzeug zu öffnen. Drücken Sie **OK**.
   b. **Auf der Registerkarte 'Access Server':**
      - Geben Sie die Adresse und den Port für den Zugriff auf den Acronis Access Management Server ein (z.B. 10.27.81.3 und 10.27.81.4).
      - Wählen Sie das Zertifikat aus. Dabei sollte es sich um dasselbe SSL-Zertifikat handeln, das an die DNS-Adresse des Lastenausgleichsmoduls gebunden ist.
      - Klicken Sie auf **Anwenden**.

      Hinweis: *Wenn Sie über kein Zertifikat verfügen, wird ein selbstsigniertes Zertifikat von Acronis Access erstellt. Dieses Zertifikat sollte NICHT in Produktionsumgebungen verwendet werden.*



   c. **Auf der Registerkarte 'Gateway Server':**
      - Geben Sie die Adresse und den Port für den Zugriff auf den Gateway Server ein (z.B. 10.27.81.10 und 10.27.81.11).
      - Wählen Sie das Zertifikat aus. Dabei sollte es sich um dasselbe SSL-Zertifikat handeln, das an die DNS-Adresse des Lastenausgleichsmoduls gebunden ist.
      - Klicken Sie auf **Anwenden**.

Hinweis: *Wenn Sie über kein Zertifikat verfügen, wird ein selbstsigniertes Zertifikat von Acronis Access erstellt. Dieses Zertifikat sollte NICHT in Produktionsumgebungen verwendet werden.*



4. Navigieren Sie zum Installationsverzeichnis von Acronis Access (z.B. C:\Programme (x86)\Acronis\Access\Access Server\), und bearbeiten Sie **acronisaccess.cfg** mit einem Texteditor.
5. Legen Sie den Benutzernamen, das Kennwort und die interne Adresse des Servers fest, auf dem die PostgreSQL-Datenbank ausgeführt wird, und speichern Sie die Datei. Dadurch wird der Access Server so konfiguriert, dass er eine Verbindung zur PostgreSQL-Remote-Datenbank herstellt, z.B.:

   ```
   DB_DATABASE =acronisaccess_production
   DB_USERNAME =postgres
   DB_PASSWORD =password123
   DB_HOSTNAME =10.27.81.2
   DB_PORT =5432
   ```

6. Öffnen Sie Services.msc, und starten Sie die Acronis Access-Dienste neu.

Gehen Sie auf einem der Access und Gateway Server wie folgt vor:

Hierbei handelt es sich um den Server, den Sie zuerst konfigurieren. Seine Einstellungen werden auf allen anderen Servern repliziert. Nach der Replizierung sind alle Server identisch. Es spielt keine Rolle, welchen Server Sie wählen.

1. Öffnen Sie Services.msc, und starten Sie den **Acronis Access Tomcat**-Dienst neu. Hierdurch wird die erstellte Datenbank gefüllt.
2. Öffnen Sie https://myaccess (d.h. https://10.27.81.3 oder https://10.27.81.4) in Ihrem Webbrowser und führen Sie den Installationsassistenten aus.
   a. **Auf der Registerkarte 'Lizenzierung':**
      - Geben Sie Ihren Lizenzschlüssel ein, aktivieren Sie das Kontrollkästchen, und klicken Sie auf **Fortfahren**.

b. **Auf der Registerkarte 'Allgemeine Einstellungen':**

- Geben Sie einen Servernamen ein.
- Die Webadresse sollte die externe Adresse des Lastenausgleichsmoduls sein (z.B. mylb.company.com). Wenn Sie nicht Port 443 verwenden, müssen Sie auch den Port eintragen.
- Die Adresse für die Registrierung von Clients sollte die externe Adresse des Lastenausgleichsmoduls sein (z.B. mylb.company.com).
- Wählen Sie das Farbschema aus.
- Wählen Sie die Sprache für die Überwachungsprotokollnachrichten aus.

c. **Auf der Registerkarte 'SMTP':**

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

d. **Auf der Registerkarte 'LDAP':**

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

e. **Auf der Registerkarte 'Lokales Gateway':**

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.*

- Legen Sie einen DNS-Namen oder eine IP-Adresse für den lokalen Gateway Server fest. Hierbei handelt es sich um eine interne Adresse hinter dem Lastenausgleichsmodul (z.B. 10.27.81.10).
- Klicken Sie auf **Speichern**.

f. **Auf der Registerkarte 'Datei-Repository':**

- Die Adresse des Datei-Repositorys sollte die interne Adresse des Servers sein, den Sie für die Datei-Repository-Rolle erstellt haben (z.B. 10.27.81.2).

3. Nachdem Sie den Installationsassistenten abgeschlossen haben, klicken Sie auf **Fertig stellen** und navigieren zu **Mobiler Zugriff** -> **Gateway Server**.
4. Nun können Sie den zweiten Gateway Server registrieren:
   a. Geben Sie einen Anzeigenamen für das zweite Gateway ein.
   b. Die **Adresse für Administration** sollte eine interne Adresse hinter dem Lastenausgleichsmodul sein (z.B. 10.27.81.11).
   c. Geben Sie den **Administrationsschlüssel** ein. Diesen können Sie ermitteln, indem Sie auf der Maschine, auf der das hinzuzufügende Gateway installiert ist, zu https://mygateway:443 (d.h. https://10.27.81.10 oder https://10.27.81.11) navigieren. Dort wird der Schlüssel angezeigt. Weitere Informationen hierzu finden Sie im Artikel Neue Gateway-Server registrieren (S. 40).
   d. Klicken Sie auf **Speichern**.
5. Erstellen Sie eine Cluster-Gruppe, und fügen Sie ihr alle Gateway Server hinzu. Der Primärserver sollte der Server sein, für den Sie bereits den Installationsassistenten ausgeführt haben. Weitere Informationen finden Sie im Artikel Cluster-Gruppen (S. 51).

   Hinweis: *Stellen Sie vor dem Fortfahren sicher, dass Sie bereits auf jedem Gateway die richtige Adresse für Administration festgelegt haben. Hierbei handelt es sich um die DNS- oder IP-Adresse des Gateway Servers.*

   a. Erweitern Sie die Registerkarte **Mobiler Zugriff**.
   b. Öffnen Sie die Seite **Gateway Server**.
   c. Drücken Sie die Schaltfläche **Cluster-Gruppe hinzufügen**.
   d. Geben Sie einen Anzeigenamen für die Gruppe ein.
   e. Geben Sie den internen DNS-Namen oder die interne IP-Adresse des Lastenausgleichsmoduls ein (z.B. 10.27.81.1).
   f. Aktivieren Sie das Kontrollkästchen für jedes Gateway, das in die Gruppe aufgenommen werden soll.
   g. Wählen Sie das Gateway, das die Einstellungen der Gruppe steuert. Dies sollte das Gateway sein, das Sie zuerst konfiguriert haben. Alle bereits festgelegten Einstellungen dieses Gateways (einschließlich zugewiesener Datenquellen, jedoch nicht die Adresse für Administration) werden auf alle anderen Gateways in der Gruppe kopiert.

Im Lastenausgleichsmodul:

1. Aktivieren Sie die dauerbasierte Sitzungs-Stickiness (oder die entsprechende Einstellung Ihres Lastenausgleichsmoduls) im Lastenausgleichsmodul, und konfigurieren Sie sie so, dass sie nicht abläuft.
2. Wenn eine Integritätsprüfung erforderlich ist (bei der der HTTP-Status 200 zurückgegeben werden sollte), reicht ein Ping an https://INTERNALSERVERNAME:MANAGEMENTPORT/signin (z.B. https://myaccessserver1.company.com/signin und https://myaccessserver2.company.com/signin).

Öffnen Sie https://mylb.company.com in einem Browser, um sich zu vergewissern, dass die Konfiguration funktioniert.

5.3 Drittanbietersoftware für Acronis Access

Themen

5.3.1 PostgreSQL

Acronis Access Server verwendet PostgreSQL als Datenbankspeicher.

Dokumentation für die aktuelle Version von PostgreSQL http://www.postgresql.org/docs/9.2/interactive/index.html (für andere Versionen besuchen Sie diese Website http://www.postgresql.org/docs/manuals/).
Liste der Fehlercodes http://www.postgresql.org/docs/9.2/interactive/errcodes-appendix.html.
Beim Installieren von Acronis Access Server wird standardmäßig auch pgAdmin installiert. Dieses bietet eine grafische Benutzeroberfläche für PostgreSQL. Dokumentation zu allen Versionen von pgAdmin finden Sie auf dieser Website http://www.pgadmin.org/docs/.
Nützliche Informationen sind im PostgreSQL-Wiki http://wiki.postgresql.org/wiki/Main_Page zu finden, unter anderem auch eine Anleitung zur Fehlerbehebung http://wiki.postgresql.org/wiki/Troubleshooting_Installation.
Bei Problemen im Zusammenhang mit dem Virusschutz lesen Sie diesen Artikel http://wiki.postgresql.org/wiki/Running_&_Installing_PostgreSQL_On_Native_Windows#Antivirus_software.
Informationen für das Backup einer PostgreSQL-Datenbank finden Sie hier: PostgreSQL Backup.

5.3.2 Apache Tomcat

Acronis Access Server verwendet ApacheTomcat als Webserver. Ab Acronis Access 2.7 werden bei der Installation eigene Versionen von Tomcat im Ordner 'Group Logic\Common' oder 'Acronis\Common' installiert.

Fehlerbehebungs-Wiki für Tomcat https://wiki.openmrs.org/display/docs/Troubleshooting+Tomcat.
Fehlerbehebung auf der Apache-Website http://commons.apache.org/logging/troubleshooting.html.

5.3.3 New Relic

New Relic ist eine On-Demand-Überwachungs- und Optimierungslösung für Applikationen, anhand derer Sie Leistungsprobleme bei Ruby-, JRuby-, Java-, PHP- und .NET-Applikationen identifizieren und beheben können. Dies ermöglicht die Überwachung, Fehlerbehebung und Anpassung von Webapplikationen rund um die Uhr. New Relic umfasst Real User Monitoring (RUM) zur Analyse von Webanforderungen in Echtzeit. Dies liefert Einsichten in die Benutzererfahrung, einschließlich der zum Laden von Seiten erforderlichen Zeit, der Zeit in der Anforderungswarteschlange, der für das Rendern benötigten Zeit und des Apdex-Ergebnisses. Außerdem schließt New Relic ein Dashboard ein, um die Leistungsmetriken nach geographischen Daten, nach der längsten Zeit in der Warteschlange, nach dem Durchsatz und vielen weiteren Metriken bildlich darzustellen.

Mit Hilfe von New Relic können Sie die Aktivität Ihres Acronis Access Servers in Echtzeit und auf einfache und benutzerfreundliche Weise überwachen.

Weitere Informationen finden Sie unter http://newrelic.com/ http://newrelic.com/

Informationen zum Installieren von New Relic für Ihren Acronis Access Server finden Sie im Abschnitt Acronis Access mit New Relic überwachen (S. 128).

5.4 Acronis Access mit Microsoft Forefront Threat Management Gateway (TMG) verwenden

Themen

5.4.1 Überblick

Info: *In diesem Dokument wird die Verwendung von TMG als Edge-Firewall behandelt. Wenn Ihre Organisation TMG in einer anderen Netzwerktopologie verwendet,*
wenden Sie sich an Acronis, um spezielle Anweisungen zu erhalten.

Wenn Sie Microsoft Forefront Threat Management Gateway (TMG) verwenden, um Ihr internes Netzwerk vor Bedrohungen und Viren aus dem Internet zu schützen, müssen Sie für den TMG-Server bestimmte Konfigurationseinstellungen festlegen, damit er mit Acronis Access zusammenarbeiten kann. Um TMG als Reverse-Proxy und Firewall für Ihren Acronis Access-Server zu verwenden, müssen Sie auf dem TMG-Computer zwei separate Netzwerke erstellen: ein internes und ein externes. Die zwei TMG-Netzwerkadapter müssen korrekt konfiguriert werden, einer mit einer privaten (interne IP-Adresse) und einer mit einer öffentlichen (externe IP-Adresse) Adresse. Der Acronis Access-Server muss Teil des internen Netzwerks sein.

Um Acronis Access mit TMG zu verwenden, müssen Sie die in diesem Dokument beschriebenen Schritte ausführen:

- Beziehen Sie ein SSL-Server-Zertifikat, und installieren Sie es auf dem Acronis Access-Server sowie auf dem TMG-Server-Computer.
- Erstellen Sie einen Weblistener in TMG.
- Erstellen Sie eine neue Website-Veröffentlichungsregel für den Acronis Access Gateway Server, damit die Clients außerhalb Ihres Netzwerks eine Verbindung mit Acronis Access herstellen können.
- Erstellen Sie einen externen DNS-Datensatz auf Ihrem DNS-Server.

Die Access Mobile Client-App unterstützt die folgenden Arten der Authentifizierung bei einem Reverse-Proxy-Server:

- Passthrough-Authentifizierung
- HTTP-Authentifizierung (Benutzername/Kennwort)
- Zertifikatsauthentifizierung

5.4.2 Einführung

Acronis Access-Clients stellen über HTTPS sichere Verbindungen zum Acronis Access-Server her, der innerhalb Ihrer Firewall ausgeführt wird, und müssen die Firewall entweder über VPN, HTTP-Reverse-Proxy oder einen offenen HTTPS-Port überwinden. Dieser Artikel enthält Schritt-für-Schritt-Anweisungen, die Benutzern, die den Acronis Access-Desktop- oder mobilen Client außerhalb Ihres Netzwerks ausführen, den Aufbau von Verbindungen mithilfe der 'Reverse-Proxy'-Funktionen der Microsoft Forefront Threat Management Gateway (TMG)-Software ermöglichen, dem Nachfolger von ISA Server 2006.

Forefront Threat Management Gateway (TMG) ist ein sicheres Web-Gateway, das Mitarbeitern die sichere Nutzung des Internets durch umfassenden Schutz vor Malware, Websites mit schädlichen Inhalten und Verwundbarkeiten ermöglicht. TMG beruht auf seinem Vorgänger, ISA Server 2006, und bietet Filterung neuer URLs, Schutz vor Malware sowie Technologien zur Abwehr von Eindringlingen, um Unternehmen vor den neuesten webbasierten Gefahren zu schützen. Diese Technologien sind in Kernfunktionen für den Netzwerkschutz wie Firewall und VPN integriert, sodass ein einheitliches, leicht zu verwaltendes Gateway entsteht.

Die Lösung Forefront TMG umfasst zwei gesondert lizenzierte Komponenten:

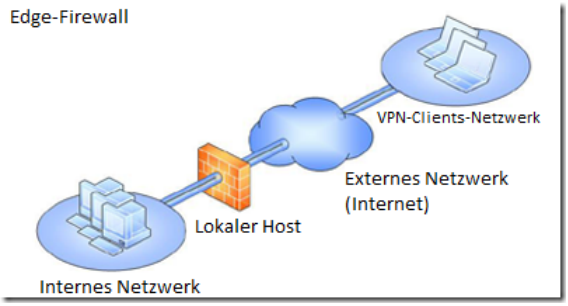
- Forefront TMG-Server mit URL-Filterung, Antimalware-Inspektion, Abwehr von Eindringlingen, Firewall auf Applikations- und Netzwerkebene sowie HTTP-/HTTPS-Inspektion in einer einzigen Lösung.
- Forefront TMG Web Protection Service für kontinuierliche Updates zur Malware-Filterung und für den Zugriff auf cloudbasierte URL-Filtertechnologien, die von mehreren Websicherheits-Anbietern zum Schutz vor den aktuellen webbasierten Gefahren aggregiert werden.

Themen

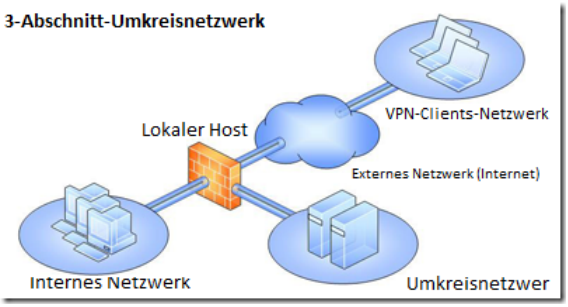
5.4.2.1 Forefront Threat Management Gateway (TMG) Netzwerktopologie verstehen

Forefront TMG umfasst vier verschiedene Netzwerkvorlagen, die in Ihre bestehende Netzwerktopologie eingepasst werden können. Es ist wichtig, diejenige Vorlage zu wählen, die für Ihre Organisation am besten geeignet ist. Nach der Installation von TMG wird der **Assistent 'Erste Schritte'** angezeigt, in dem Sie die ersten Konfigurationseinstellungen in TMG vornehmen müssen. Das erste Menü im **Assistenten 'Erste Schritte'** ist **Netzwerkeinstellungen konfigurieren**. Hier treffen Sie Ihre Wahl bezüglich der zu verwendenden Netzwerkvorlage. Die verfügbaren Optionen sind nachstehend aufgeführt.

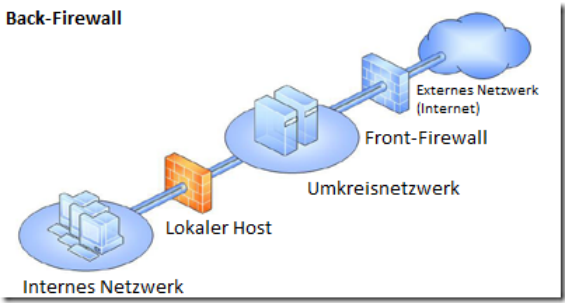
- **Edge Firewall** – In dieser Topologie befindet sich Forefront TMG am Rande des Netzwerks, wo es als Edge Firewall der Organisation fungiert und mit zwei Netzwerken verbunden ist, dem internen und dem externen Netzwerk (für gewöhnlich das Internet).

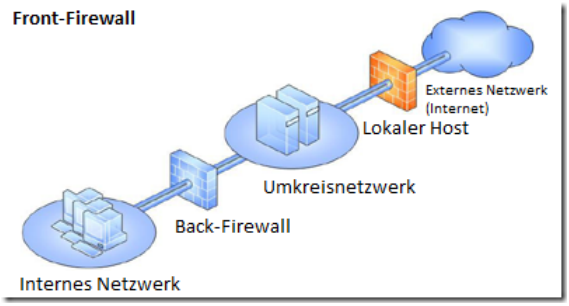


- **3-Leg Perimeter** – Mit dieser Topologie wird ein Perimeternetz (DMZ) implementiert. Forefront TMG ist mit mindestens drei physischen Netzwerken verbunden, dem internen Netzwerk, einem oder zwei Perimeternetzen und dem externen Netzwerk.

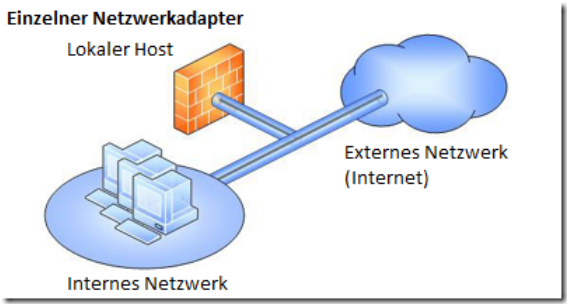


- **Back/Front Firewall** – In dieser Topologie befindet sich Forefront TMG am Backend des Netzwerks. Verwenden Sie diese Topologie, wenn sich ein anderes Netzwerkelement, wie etwa ein Perimeternetz oder eine am Netzwerkrand befindliche Sicherheitsvorrichtung, zwischen Forefront TMG und dem externen Netzwerk befindet. Forefront TMG ist mit dem internen Netzwerk und dem davor befindlichen Netzwerkelement verbunden.





- **Einzelner Netzwerkadapter** – Diese Topologie aktiviert eine limitierte Forefront TMG-Funktionalität. In dieser Topologie ist Forefront TMG nur mit einem Netzwerk verbunden, entweder dem internen Netzwerk oder einem Perimeternetz. Diese Konfiguration wird in der Regel verwendet, wenn sich Forefront TMG im internen Unternehmensnetzwerk oder einem Perimeternetz befindet und eine andere Firewall am Rand des Netzwerks die Unternehmensressourcen vor dem Internet schützt.



Info:

Weitere Informationen zum Installieren und Konfigurieren von TMG finden Sie unter:
http://technet.microsoft.com/en-us/library/cc441445.aspx
http://technet.microsoft.com/en-us/library/cc441445.aspx.

Die Systemanforderungen für TMG sind hier angegeben:
http://www.microsoft.com/forefront/threat-management-gateway/en/us/system-requirements.aspx
http://www.microsoft.com/forefront/threat-management-gateway/en/us/system-requirements.aspx.

Preisangaben erhalten Sie hier:
http://www.microsoft.com/forefront/threat-management-gateway/en/us/pricing-licensing.aspx
http://www.microsoft.com/forefront/threat-management-gateway/en/us/pricing-licensing.aspx.

5.4.2.2 Forefront Threat Management Gateway-Authentifizierung verstehen

TMG bietet drei allgemeine Methoden zur Authentifizierung von Benutzern. Diese sind:

HTTP-Authentifizierung:

- Grundlegende Authentifizierung – Der Benutzer gibt einen Benutzernamen und ein Kennwort ein, die der TMG-Server mit Hilfe des angegebenen Authentifizierungsservers validiert.
- Digest- und WDigest-Authentifizierung – Weist die gleichen Funktionen wie die grundlegende Authentifizierung auf, bietet jedoch verstärkte Sicherheit bei der Übertragung der Authentifizierungsangaben.
- Integrierte Windows-Authentifizierung – Verwendet die NTLM-, Kerberos- und Negotiate-Authentifizierungsmechanismen. Diese bilden sicherere Formen der Authentifizierung, da Benutzername und Kennwort als Hash-Zeichen verschlüsselt werden, bevor sie über das Netzwerk gesendet werden.

Formularbasierte Authentifizierung:

- Kennwortformular – Fordert den Benutzer zur Eingabe eines Benutzernamens und eines Kennworts auf.
- Codeformular – Fordert den Benutzer zur Eingabe eines Benutzernamens und eines Codes auf.
- Code- und Kennwortformular – Fordert den Benutzer zur Eingabe einer Kombination von Benutzername/Kennwort und Benutzername/Code auf.

Clientzertifikat-Authentifizierung

Wenn der Benutzer veröffentlichte Ressourcen anfordert, wird das an Forefront TMG gesendete Clientzertifikat an einen Domain-Controller weitergeleitet, der die Zuordnung zwischen Zertifikaten und Konten bestimmt. Das Zertifikat muss mit einem Benutzerkonto übereinstimmen.

Hinweis: *Clientzertifikat-Authentifizierung wird für die Authentifizierung abgehender Web-Anforderungen nicht unterstützt.*

Info: *Weitere Informationen zur TMG-Authentifizierung finden Sie auf diesen Websites:*
http://technet.microsoft.com/en-us/library/cc441695.aspx
http://technet.microsoft.com/en-us/library/cc441695.aspx

http://technet.microsoft.com/en-us/library/cc441713.aspx
http://technet.microsoft.com/en-us/library/cc441713.aspx

5.4.3 Das SSL-Server-Zertifikat installieren

Fordern Sie für jeden mobilEcho File Server, den Sie per TMG veröffentlichen möchten, ein SSL-Zertifikat mit dem FQDN an, um DNS-Spoofing zu verhindern. Anschließend installieren Sie die Zertifikate. Sie müssen die SSL-Stammzertifikate auf dem TMG-Computer installieren. Diese Zertifikate müssen mit dem FQDN jedes veröffentlichten Servers übereinstimmen.

Führen Sie die im Folgenden angegebenen Schritte aus, um ein Zertifikat auf den TMG-Computer zu importieren:

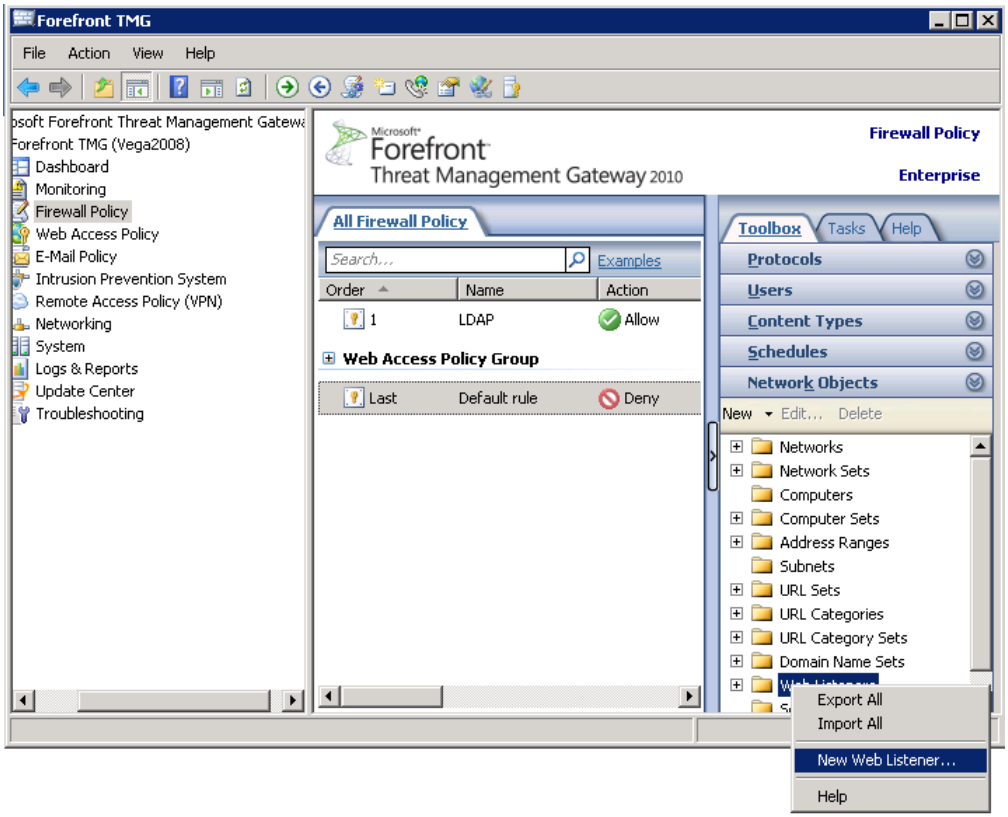
1. Klicken Sie auf dem TMG-Computer auf **Start**, geben Sie **mmc** ein und drücken Sie dann **Enter** oder klicken Sie auf **OK**.
2. 2. Klicken Sie im Menü **Datei** auf **Snap-In hinzufügen/entfernen** oder drücken Sie **Strg+M**. Klicken Sie unter **Verfügbare Snap-Ins** auf **Zertifikate** und dann auf **Hinzufügen**.
3. Wählen Sie 'Computerkonto' und klicken Sie dann auf **Weiter**, anschließend auf **Lokalen Computer** und auf **Fertig stellen**.
4. Klicken Sie im Dialogfeld **Snap-Ins hinzufügen bzw. entfernen** auf **OK**.
5. Erweitern Sie **Zertifikate (Lokaler Computer)**, **Eigene Zertifikate** und dann **Zertifikate**.
6. Klicken Sie mit der rechten Maustaste auf den Knoten **Zertifikate** und wählen Sie **Alle Aufgaben** und dann **Importieren** .
7. Die Seite **Willkommen** des Assistenten für den Zertifikatimport wird angezeigt. Klicken Sie auf **Weiter**.
8. Geben Sie auf der Seite **Zu importierende Datei** den Speicherort des Zertifikats an.
9. Geben Sie auf der Seite **Kennwort** das Kennwort ein, das Ihnen die Stelle, die das Zertifikat ausgestellt hat, bekannt gegeben hat.
10. Überprüfen Sie auf der Seite **Zertifikatspeicher**, ob der Speicherort **Persönlich** ist.
11. Die Seite **Fertigstellen des Assistenten** sollte mit einer Zusammenfassung der von Ihnen ausgewählten Optionen angezeigt werden. Überprüfen Sie die Angaben und klicken Sie auf **Fertig stellen**.

Überzeugen Sie sich, dass Ihre Zertifizierungsstelle (CA) in der Liste der vertrauenswürdigen Stammzertifizierungsstellen aufgeführt wird:

1. Klicken Sie auf jedem Edge-Server auf **Start** und dann auf **Ausführen**. Geben Sie im Feld 'Öffnen' die Zeichenfolge **mmc** ein und klicken Sie dann auf **OK**. Damit öffnen Sie eine **MMC-Konsole**.
2. Klicken Sie im Menü **Datei** auf **Snap-In hinzufügen/entfernen.**
3. Klicken Sie im Feld **Eigenständiges Snap-In hinzufügen** auf **Zertifikate** und dann auf **Hinzufügen**.
4. Klicken Sie im Dialogfeld **Zertifikat-Snap-In** auf **Computerkonto** und dann auf **Weiter**.
5. Stellen Sie im Dialogfeld **Computer auswählen** sicher, dass das Kontrollkästchen **Lokalen Computer (Computer, auf dem diese Konsole ausgeführt wird)** aktiviert ist und klicken Sie dann auf **Fertig stellen**.
6. Klicken Sie auf **OK**. Erweitern Sie in der Konsolenstruktur **Zertifikate (Lokaler Computer)** und dann **Eigene Zertifikate** und **Zertifikate**.
7. Überzeugen Sie sich im Bereich **Details**, dass Ihre Zertifizierungsstelle in der Liste der vertrauenswürdigen Zertifizierungsstellen aufgeführt wird. Wiederholen Sie dieses Verfahren für jeden Server.

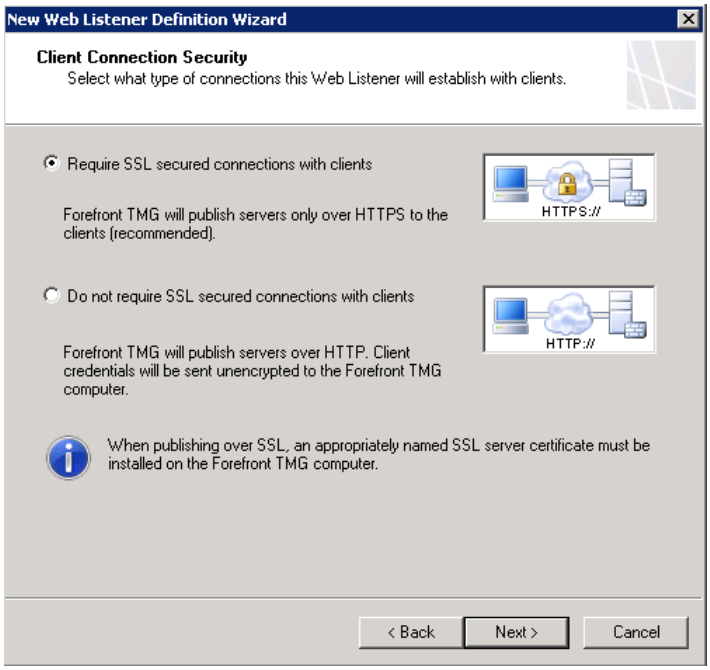
5.4.4 Neuen Web Listener erstellen

1. Öffnen Sie die Verwaltungskonsole von Forefront TMG.
2. Erweitern Sie im linken Bereich 'Forefront TMG' (Array-Name oder Computername) und klicken Sie auf **Firewallrichtlinie**.
3. Klicken Sie im rechten Bereich auf die Registerkarte **Toolbox** und auf **Netzwerkobjekte**, klicken Sie mit der rechten Maustaste auf **Weblistener** und wählen Sie im Menü **Neuer Weblistener** aus.

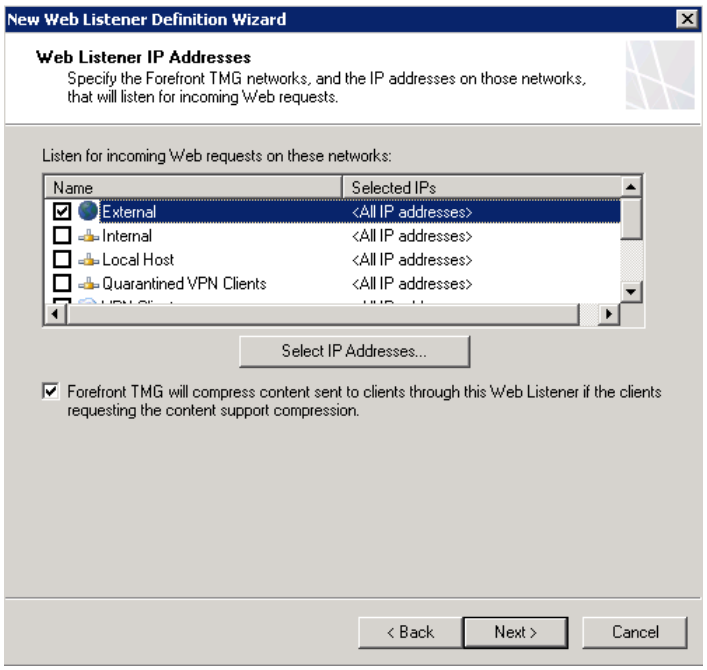


4. Die Seite **Willkommen** des Assistenten für den neuen Weblistener wird angezeigt. Geben Sie dem **Weblistener** einen Namen (z.B. Access WL), und klicken Sie auf **Weiter**.

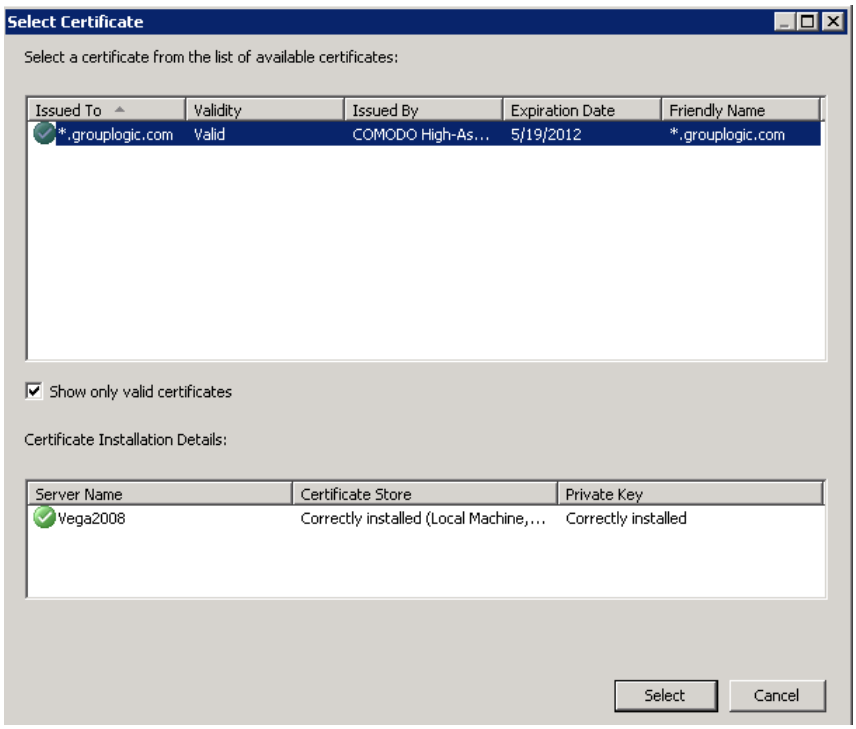
5. Wählen Sie auf der Seite **Clientverbindungssicherheit** die Option **Sichere SSL-Verbindungen mit Clients anfordern** und klicken Sie auf **Weiter**.



6. Wählen Sie auf der Seite **Weblistener-IP-Adressen** die Option **Extern** und klicken Sie auf **Weiter**.



7. Wählen Sie auf der Seite **Listener-SSL-Zertifikate** die Option **Einzelnes Zertifikat für diesen Weblistener verwenden** und klicken Sie auf die Schaltfläche **Zertifikat auswählen**. Wählen Sie das richtige Zertifikat aus und klicken Sie auf die Schaltfläche **Auswählen**, um die Auswahl zu bestätigen.

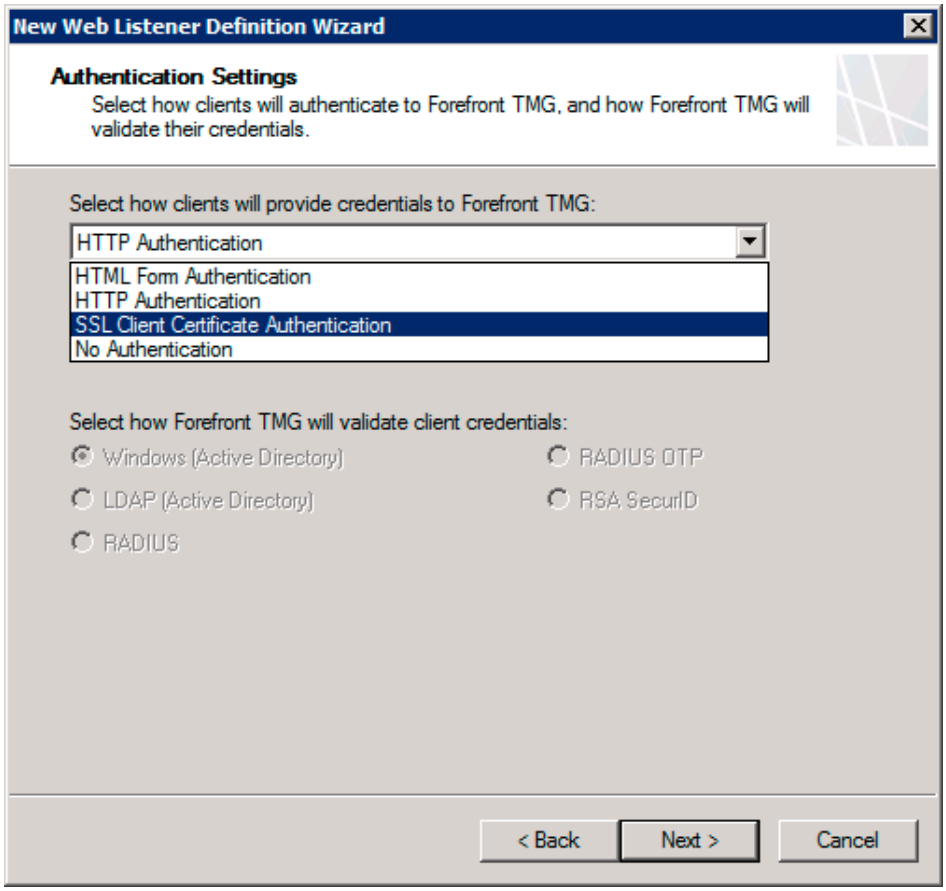


8. Überprüfen Sie, ob auf der Seite **Listener-SSL-Zertifikate** das richtige Zertifikat angezeigt wird, und klicken Sie auf **Weiter**.
9. Wählen Sie auf der Seite **Authentifizierungseinstellungen** den Authentifizierungstyp aus, den Acronis Access beim Kontakt mit dem TMG-Reverse-Proxy-Server verwenden soll, und klicken Sie auf **Weiter**.

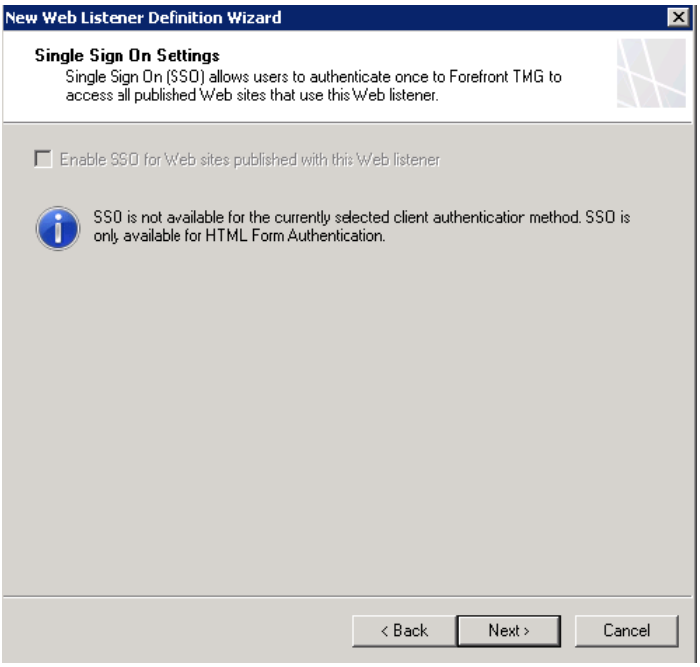
   Acronis Access mobile Client unterstützt:

   - **Keine Authentifizierung** – Verwenden Sie diese Option, wenn die Access Mobile Client-Anforderungen ohne Authentifizierung durch den TMG-Reverse-Proxy-Server geleitet werden sollen.
   - **HTTP-Authentifizierung** – Verwenden Sie diese Option, wenn sich die Access Mobile Client-App beim TMG-Reverse-Proxy mit dem Benutzernamen und dem Kennwort des Benutzers authentifizieren soll. Dies sind normalerweise die Active Directory-Anmeldedaten des Benutzers. Wenn die Access Mobile Client-App die Authentifizierung 'Einmal pro Sitzung' oder 'Einmal pro Server' verlangt, wird der Benutzer zur Eingabe seiner Anmeldedaten aufgefordert, wenn den TMG-Reverse-Proxy-Server erstmals kontaktiert.

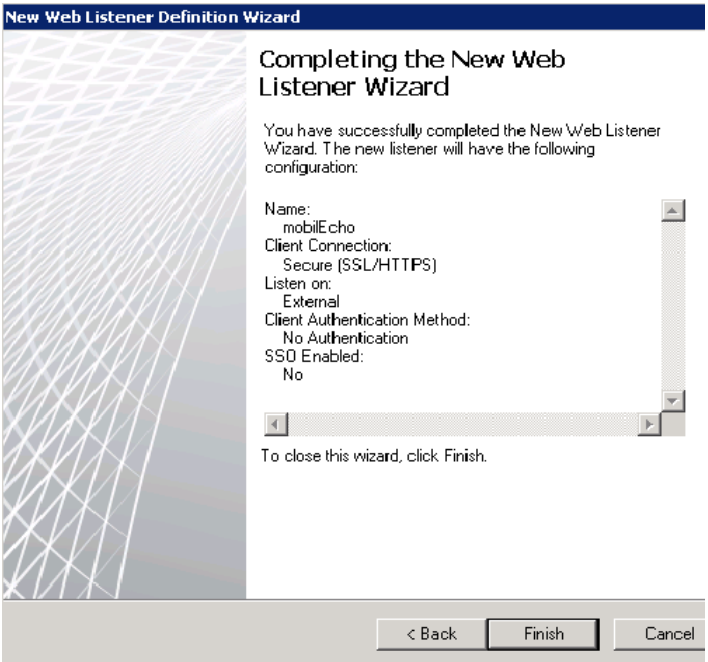
- **Authentifizierung per SSL-Client-Zertifikat** – Verwenden Sie diese Option, wenn sich die Access Mobile Client-App beim TMG-Reverse-Proxy mit einem SSL-Benutzeridentitätszertifikat authentifizieren soll. Dieses Zertifikat muss der Access Mobile Client-App hinzugefügt werden, bevor sich der Benutzer beim TMG-Reverse-Proxy-Server authentifizieren kann. Weitere Anweisungen finden Sie hier. http://support.grouplogic.com/?p=3830



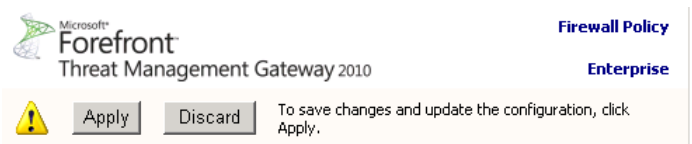
10. Stellen Sie auf der Seite **Einstellungen für Single Sign-On** sicher, dass die Einstellung **SSO** deaktiviert ist, und klicken Sie auf **Weiter**.



11. Überprüfen Sie Ihre Auswahl auf der Seite **Fertigstellen des Assistenten** und klicken Sie auf **Fertig stellen**.



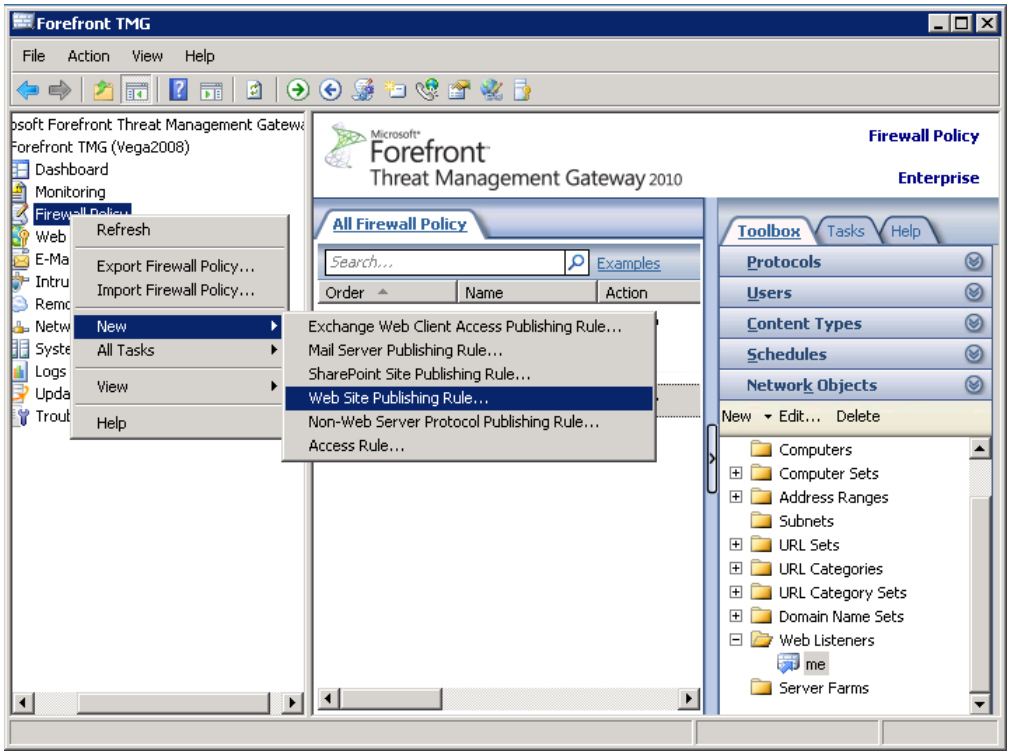
12. Klicken Sie auf die Schaltfläche **Übernehmen**, um die Änderungen zu speichern.



13. Klicken Sie im linken Bereich der Verwaltungskonsole von Forefront TMG auf **Überwachen** und dann im mittleren Bereich auf die Registerkarte **Konfiguration**. Klicken Sie im rechten Bereich (Registerkarte **Aufgaben**) mehrmals auf den Link **Jetzt aktualisieren**, bis vor dem TMG-Computernamen (Array-Namen) ein grünes Symbol mit dem Kontrollkästchen erscheint.

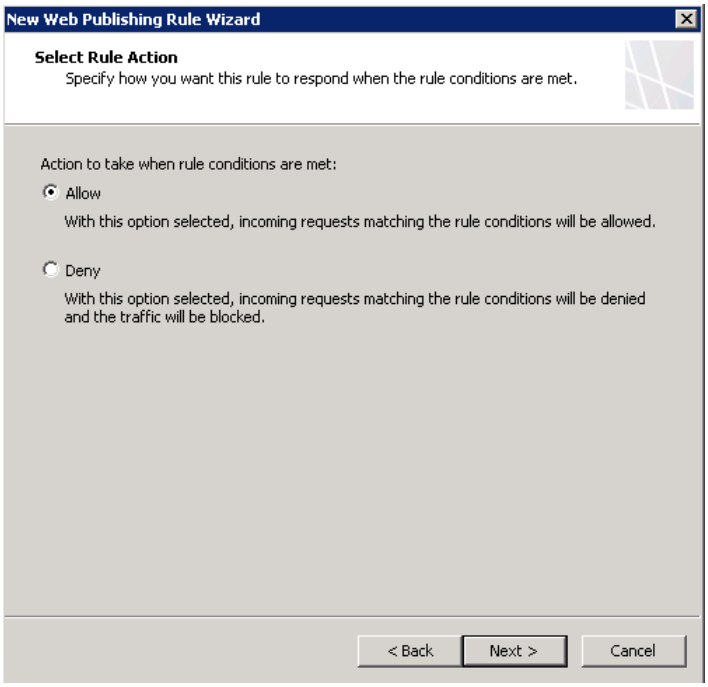
5.4.5 Eine neue Website-Veröffentlichungsregel erstellen

1. Erweitern Sie im linken Bereich der Verwaltungskonsole von Forefront TMG den Eintrag für 'Forefront TMG' (Array-Name oder Computername).
2. Klicken Sie mit der rechten Maustaste auf **Firewallrichtlinie**, wählen Sie **Neu** und klicken Sie auf **Website-Veröffentlichungsregel**.



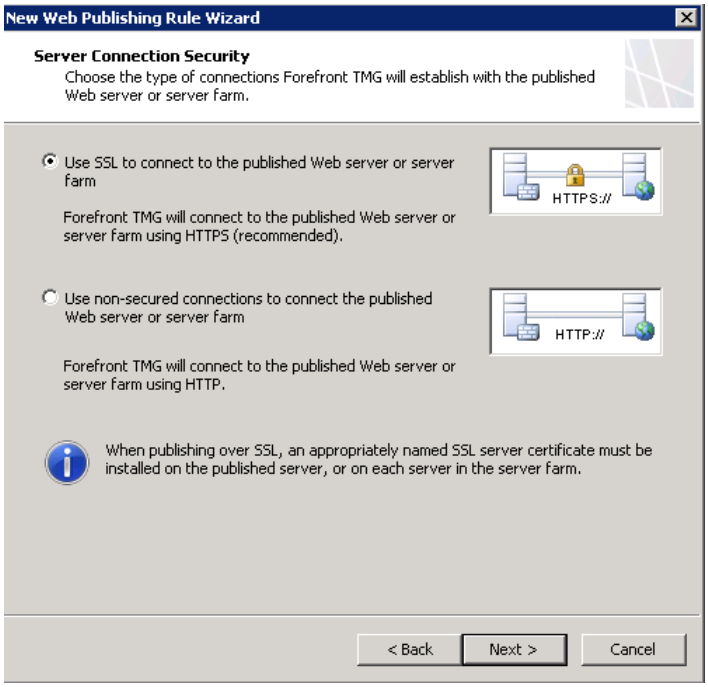
3. Die Seite **Willkommen** des Assistenten für eine neue Website-Veröffentlichungsregel wird angezeigt. Geben Sie einen Namen für die Website-Veröffentlichungsregel (z.B. Access WP) ein, und klicken Sie auf **Weiter**.

4. Stellen Sie auf der Seite **Regelaktion auswählen** sicher, dass die Einstellung **Zulassen** aktiviert ist, und klicken Sie auf **Weiter**.



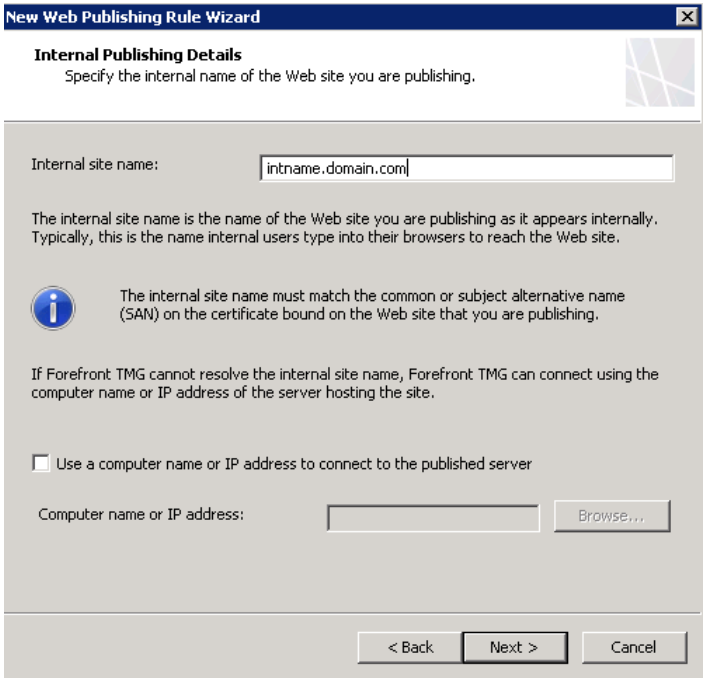
5. Wählen Sie auf der Seite **Veröffentlichungstyp** die richtige Option für Ihren Fall aus und klicken Sie auf **Weiter**.

6. Wählen Sie auf der Seite **Serververbindungssicherheit** die Option **SSL für Verbindungen mit veröffentlichtem Webserver oder veröffentlichter Serverfarm verwenden** und klicken Sie auf **Weiter**.

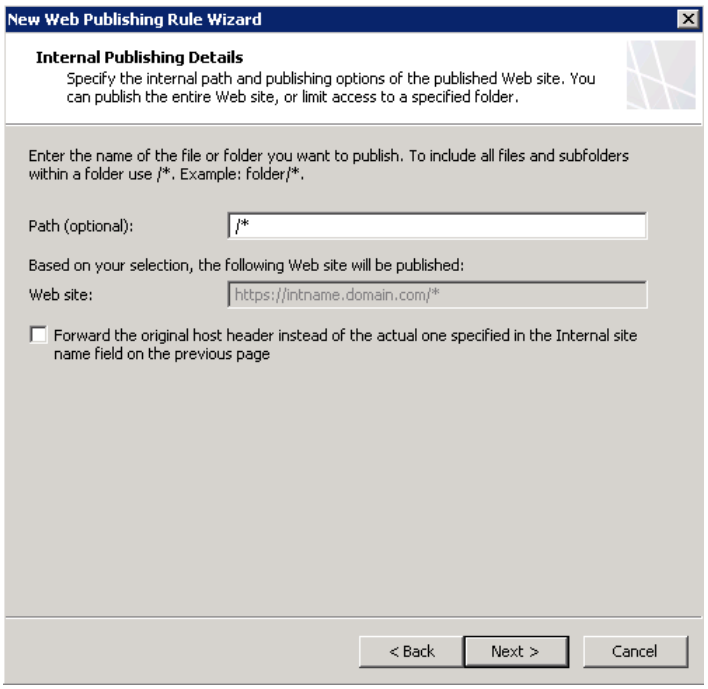


7. Geben Sie auf der Seite **Details für interne Veröffentlichung** im Feld **Name der internen Website** 'intname.domain.com' ein, wobei **domain** ein Platzhalter für den Namen der Domain ist, zu der der zu veröffentlichende Server gehört, und 'intname' der Name, den Sie diesem Server geben, wobei sich dieser vom externen Namen unterscheiden muss, um Routing-Schleifen zu verhindern. Klicken Sie auf **Weiter**, um die Änderungen zu übernehmen.

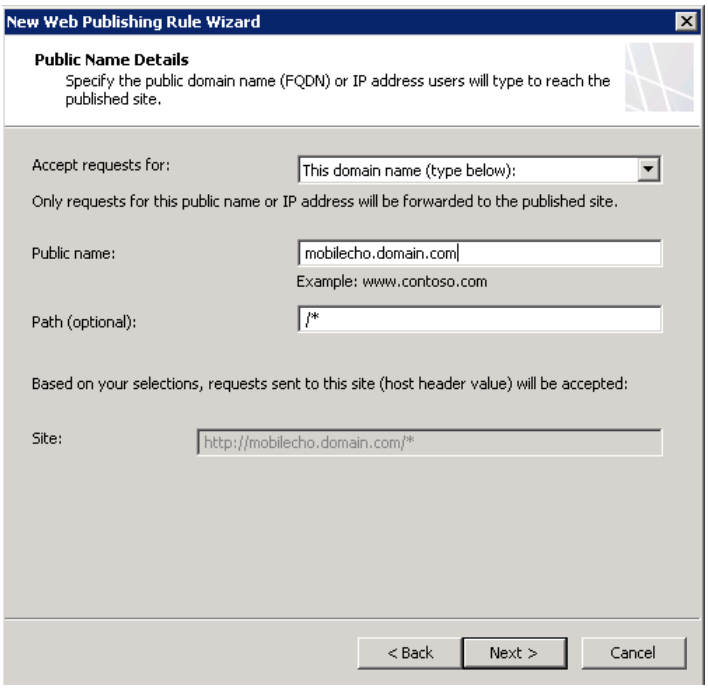
Hinweis: *Erstellen Sie auf dem internen DNS-Server Ihrer Organisation einen DNS-Eintrag für 'intname.domain.com'.*



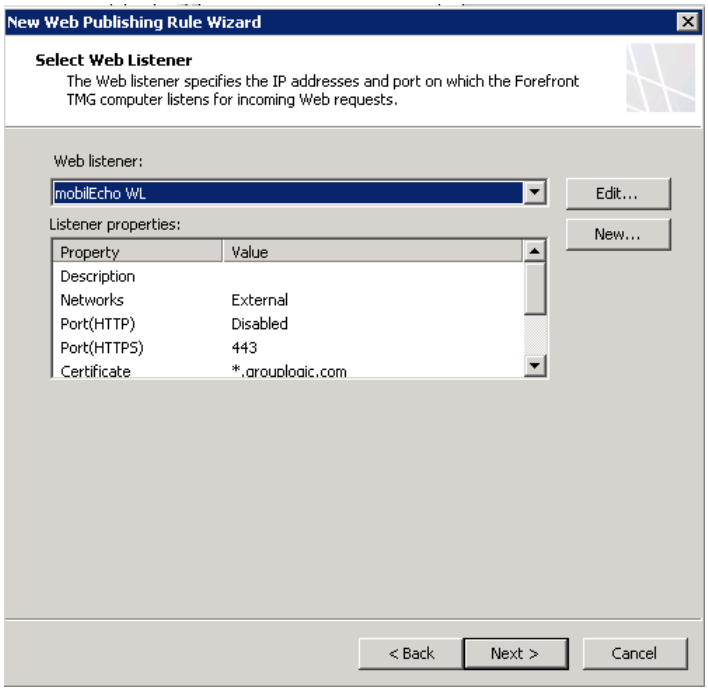
8. Geben Sie auf der Seite **Details für interne Veröffentlichung** '**/***' in das Feld **Pfad (optional)** ein, um Zugriff auf sämtliche Inhalte auf dem Acronis Access Gateway Server zu gestatten. Klicken Sie auf **Weiter**.



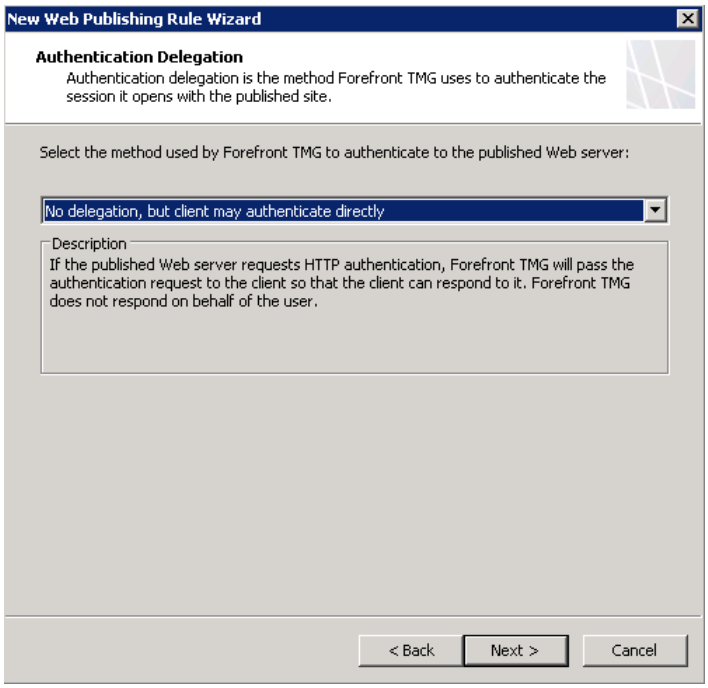
9. Auf der Seite **Details zum öffentlichen Namen** müssen Sie den Namen eingeben, den die Remote-Clients für die Verbindung mit dem veröffentlichten Server verwenden sollen. Geben Sie 'access.domain.com' in das Feld **Öffentlicher Name** ein; dabei ist **domain** ein Platzhalter für den Domain-Namen des Servers, den Sie veröffentlichen möchten. Übernehmen Sie die sonstigen Optionen unverändert und klicken Sie auf **Weiter**.



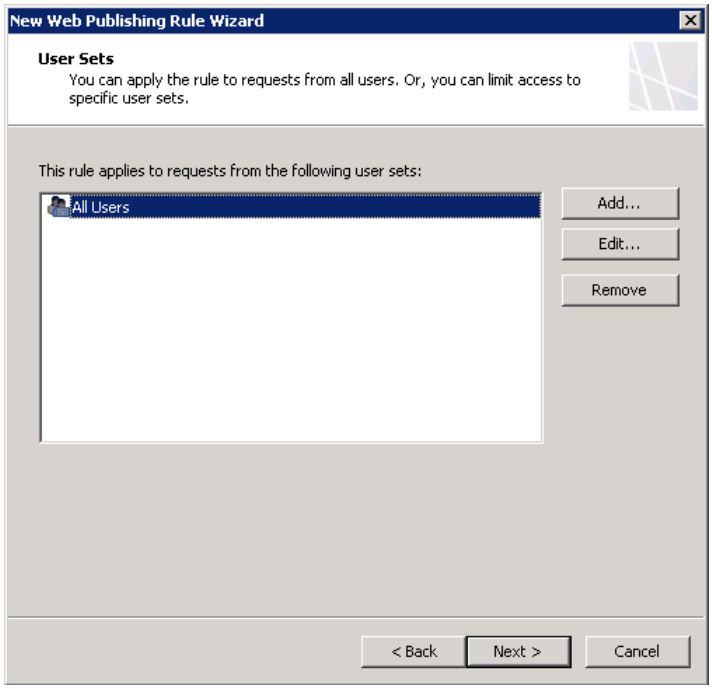
10. Wählen Sie auf der Seite **Weblistener auswählen** im Dropdown-Menü den Weblistener aus, den Sie für Acronis Access erstellt haben, und klicken Sie auf **Weiter**.



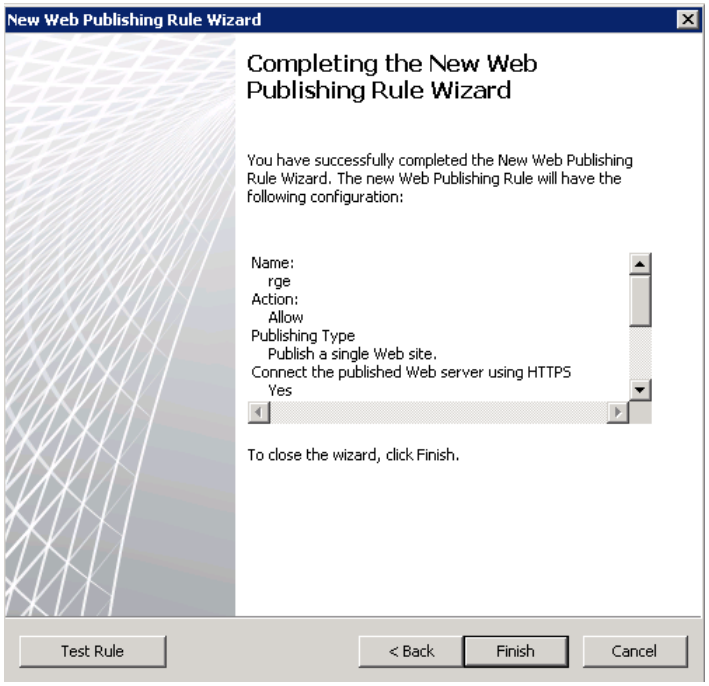
11. Wählen Sie auf der Seite **Authentifizierungsdelegierung** im Dropdown-Menü die Option **Keine Delegierung, Client kann sich direkt authentifizieren** aus und klicken Sie dann auf **Weiter**.



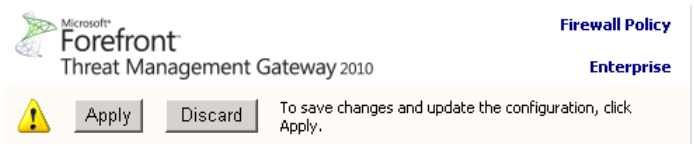
12. Stellen Sie auf der Seite **Benutzergruppen** sicher, dass die Standardoption **Alle Benutzer** vorhanden ist, und klicken Sie zum Fortfahren auf **Weiter**.



13. Überprüfen Sie die Zusammenfassung Ihrer gewählten Optionen auf der Seite **Fertigstellen des Assistenten**. Klicken Sie auf **Regel testen**, um zu überprüfen, ob die Veröffentlichungsregel ordnungsgemäß funktioniert. Klicken Sie auf **Fertig stellen**, um den Vorgang abzuschließen.



14. Klicken Sie auf die Schaltfläche **Übernehmen**, um die Änderungen zu speichern.



15. Klicken Sie im linken Bereich der Verwaltungskonsole von Forefront TMG auf **Überwachen** und dann im mittleren Bereich auf die Registerkarte **Konfiguration**. Klicken Sie im rechten Bereich (Registerkarte **Aufgaben**) mehrmals auf den Link **Jetzt aktualisieren**, bis vor dem TMG-Computernamen (Array-Namen) ein grünes Symbol mit dem Kontrollkästchen erscheint.

5.4.6 Einen externen DNS-Eintrag für den Acronis Access-Gateway Server konfigurieren

Nach dem Abschluss der TMG-Konfiguration müssen Sie auf den externen DNS-Servern einen DNS-Datensatz erstellen, um alle Acronis Access-Desktop- bzw. Mobilgeräteverbindungen zum externen Netzwerkadapter des TMG umzuleiten. Der DNS-Eintrag muss den Namen Ihres Servers (z.B. access.domain.com) in die externe IP-Adresse des TMG-Servers auflösen. Alle Anforderungen werden an das TMG gesendet und von diesem verwaltet. In diesem Konfigurationsszenario erfordert das TMG keine Authentifizierung der Clients, und alle Benutzer greifen auf den Acronis Access Server zu, ohne zu wissen, dass die Antwort stattdessen vom Microsoft Forefront TMG kommt.

5.4.7 Den Access Mobile Client mit einem TMG-Reverse-Proxy-Server verwenden

Diese Funktion ist bereits integriert und erfordert praktisch keine Konfiguration.

In der Access Mobile Client-App fügen Sie den Server manuell folgendermaßen hinzu:

1. Drücken Sie die Schaltfläche **+** in der oberen linken Ecke. Über diese Schaltfläche können Sie einen neuen Server hinzufügen.
2. Geben Sie in das Feld **Servername oder IP-Adresse** den Pfad zu Ihrem Server ein (z.B. yourserver.companyname.com/access http://yourserver.companyname.com/mobilecho).
3. Tragen Sie Ihre **Anmeldedaten** (Benutzername /Kennwort) ein.
4. Tippen Sie auf **Speichern**.

5.4.8 Den Access Desktop Client mit einem TMG-Reverse-Proxy-Server verwenden

Diese Funktion ist bereits integriert und erfordert praktisch keine Konfiguration.

Für den Desktop-Client:

1. Klicken Sie mit der rechten Maustaste in der Taskleiste auf das Acronis Access-Symbol. Wählen Sie **Einstellungen**.
2. Geben Sie in das Feld **Server-URL** den Pfad zu Ihrem Server ein (z.B. access.companyname.com http://yourserver.companyname.com/activecho).
3. Geben Sie Ihre **Anmeldedaten** (Benutzername/Kennwort) ein.
4. Drücken Sie **Übernehmen**.
5. Fertig!

5.5 Unbeaufsichtigte Desktop-Client-Konfiguration

Mit der Gruppenrichtlinienverwaltung von Microsoft können Sie auf einfache Weise eine Remote-Konfiguration des Acronis Access Desktop Clients auf mehreren Maschinen durchführen. Die Endbenutzer müssen lediglich den Client installieren, ihn starten und ihr Kennwort eingeben. Die Gruppenrichtlinienverwaltung stellt außerdem sicher, dass Benutzer die korrekten Einstellungen nicht versehentlich ändern bzw. ersetzen können. In diesem Fall können sie sich einfach abmelden. Wenn sie sich erneut anmelden, werden wieder die richtigen Einstellungen verwendet.

Das Gruppenrichtlinienobjekt erstellen und konfigurieren:

1. Öffnen Sie auf Ihrem Domänencontroller die **Gruppenrichtlinien-Verwaltungskonsole**.
2. Klicken Sie mit der rechten Maustaste auf die gewünschte Domäne und wählen Sie **Gruppenrichtlinienobjekt hier erstellen und verknüpfen ...**.
3. Geben Sie einen Namen ein und klicken Sie auf **OK**.
4. Erweitern Sie den Bereich **Gruppenrichtlinienobjekte** und wählen Sie Ihre neue Richtlinie aus.
5. Wählen Sie auf der Registerkarte **Bereich** die gewünschten Websites, Domänen, Organisationseinheiten, Gruppen, Benutzer und/oder Computer aus.

Ordner und Registrierungseinträge erstellen:

In diesem Beispiel erstellen Sie Einträge für Benutzername, Sync-Ordner, Server-URL sowie das Auto-Update-Kontrollkästchen und legen fest, ob der Client Verbindungen zu Servern mit selbstsignierten Zertifikaten herstellen soll.

1. Erweitern Sie den Bereich **Gruppenrichtlinienobjekte** und klicken Sie mit der rechten Maustaste auf Ihr neues Richtlinienobjekt.
2. Wählen Sie **Bearbeiten** und erweitern Sie **Benutzerkonfiguration** -> **Einstellungen** -> **Windows-Einstellungen**.

Synchronisierungsordner erstellen:

1. Klicken Sie mit der rechten Maustaste auf **Ordner** und wählen Sie **Neu** -> **Ordner**.
2. Setzen Sie die **Aktion** auf **Erstellen**.
3. Geben Sie als Pfad folgendes Token ein: **`%USERPROFILE%\Desktop\AAS Data Folder`**

Registrierung erstellen:

1. Klicken Sie mit der rechten Maustaste auf **Registrierung** und wählen Sie **Neu** -> **Registrierungselement**.
2. Setzen Sie die **Aktion** auf **Erstellen**.
3. Wählen Sie für **Struktur HKEY_CURRENT_USER**.
4. Geben Sie als Pfad Folgendes ein: **`Software\Group Logic, Inc.\activEcho Client\`**
5. Führen Sie jetzt für die gewünschten Einträge Folgendes durch:

6. Für den Benutzernamen:
   a. Für **Wertnamen** "**Username**" eingeben.
   b. Für **Werttyp** REG_SZ eingeben.
   c. Für **Wertdaten** das folgende Token eingeben: **%USERNAME%@%USERDOMAIN%**
7. Für die Server-URL:
   a. Für **Wertnamen** "**Server URL**" eingeben.
   b. Für **Werttyp** REG_SZ eingeben.
   c. Für **Wertdaten** die Adresse Ihres Access Servers eingeben, z. B. **https://myaccess.com**
8. Für den Synchronisierungsordner:
   a. Für **Wertnamen** "**activEcho Folder**" eingeben.
   b. Für **Werttyp** REG_SZ eingeben.
   c. Für **Wertdaten** folgendes Token und folgenden Pfad eingeben: **%USERPROFILE%\Desktop\AAS Data Folder**
9. Für das Auto-Update:
   a. Für **Wertnamen** "**AutoCheckForUpdates**" eingeben.
   b. Für **Werttyp** DWORD eingeben.
   c. Für **Wertdaten** '**00000001**' eingeben. Mit dem Wert "**1**" wird diese Einstellung aktiviert und der Client prüft automatisch auf Updates. Wird der Wert auf "**0**" festgelegt, wird die Einstellung deaktiviert.
10. Für die Zertifikate:
    a. Für **Wertnamen** "**AllowInvalidCertificates**" eingeben.
    b. Für **Werttyp** DWORD eingeben.
    c. Für **Wertdaten** '**00000000**' eingeben. Mit dem Wert '**0**' wird diese Einstellung deaktiviert und der Client kann keine Verbindung mehr zu Acronis Access Servern mit ungültigen Zertifikaten herstellen. Wird der Wert auf '**1**' festgelegt, wird die Einstellung aktiviert.

5.6 Acronis Access mit New Relic überwachen

Bei diesem Installationstyp überwachen Sie Ihre Acronis Access Server-Applikation, nicht den eigentlichen Computer, auf dem Sie die Installation vornehmen.

1. Öffnen Sie http://newrelic.com/ http://newrelic.com/ und erstellen Sie ein 'New Relic'-Konto.
2. Wählen Sie unter 'Applikationstyp' die Option 'Mobile App' aus.
3. Markieren Sie unter 'Plattform' den Eintrag 'Ruby'.
4. Schließen Sie die Kontoerstellung ab und melden Sie sich an.
5. Wechseln Sie zu 'Applikationen', übernehmen Sie das **Ruby-Bündel** (Schritt 1) wie vorliegend und gehen Sie zum nächsten Schritt über.
6. Laden Sie das New Relic-Skript, newrelic.yml, herunter.
7. Öffnen Sie die webbasierte Benutzeroberfläche von Acronis Access.
8. Wechseln Sie zu den Einstellungen und klicken Sie auf 'Überwachung'.
9. Geben Sie den Pfad zur Datei newrelic.yml, einschließlich der Erweiterung, ein (z.B. **C:\software\newrelic.yml**). Platzieren Sie diese Daten nach Möglichkeit in einem anderen Ordner als dem Ordner für Acronis Access, sodass sie bei einem Upgrade oder einer Deinstallation nicht entfernt oder geändert werden.

10. Klicken Sie auf 'Speichern' und warten Sie einige Minuten oder bis auf der New Relic-Website die Schaltfläche **Aktive Applikation(en)** verfügbar wird.
11. Wenn mehr als 10 Minuten vergehen, starten Sie den Acronis Access Tomcat-Dienst neu, und warten Sie einige Minuten. Die Schaltfläche sollte dann aktiv sein.
12. Sie sollten den Acronis Access Server auf der New Relic-Website überwachen können.

*Alle vom Acronis Access Server protokollierten Informationen zu Verbindungsversuchen mit New Relic und die Einrichtung der Überwachung befinden sich in einer Datei namens **newrelic_agent.log**, die sich an folgendem Speicherort befindet – **C:\Program Files (x86)\Acronis\Common\apache-tomcat-7.0.34\logs**. Wenn Probleme auftreten, finden Sie entsprechende Informationen in der Log-Datei.*

Häufig finden sich Warnungen oder Fehler, die wie folgt beginnen:
WARN : DNS Error caching IP address: Errno::ENOENT: No such file or directory - C:/etc/hosts which

Dies ist eine harmlose Nebenwirkung des Codes, der als Patch für ein anderes Problem mit New Relic verwendet wird.

Wenn Sie auch den eigentlichen Computer überwachen möchten, gehen Sie wie folgt vor:

1. Öffnen Sie http://newrelic.com/ http://newrelic.com/ und melden Sie sich bei Ihrem Konto an.
2. Klicken Sie auf 'Server' und laden Sie das richtige Installationsprogramm von New Relic für Ihr Betriebssystem herunter.
3. Installieren Sie den Monitor von New Relic auf Ihrem Server.
4. Der neue Server-Monitor von New Relic erfordert Microsoft .NET Framework 4. Der vom Installationsprogramm von New Relic verwendete Link gilt nur für das Client-Profil von Microsoft .NET Framework 4. Sie müssen zum Microsoft Download Center wechseln und das gesamte .NET Framework 4 aus dem Internet herunterladen, bevor Sie das Installationsprogramm für den Server-Monitor von New Relic ausführen.
5. Warten Sie, bis New Relic Ihren Server erkannt hat.

5.7 Vertrauenswürdige Server-Zertifikate mit Acronis Access verwenden

In diesem Abschnitt wird erläutert, wie Acronis Access mit vertrauenswürdigen Server-Zertifikaten konfiguriert wird. Acronis Access verwendet standardmäßig ein selbst-generiertes SSL-Zertifikat. Bei Verwendung eines von einer vertrauenswürdigen Zertifizierungsstelle signierten Zertifikats wird die Identität des Servers festgestellt und Browser können eine Verbindung herstellen, ohne dass eine Warnmeldung bezüglich eines nicht vertrauenswürdigen Servers angezeigt wird.

***Hinweis:** Acronis Access wird mit selbstsignierten Zertifikaten für Testzwecke ausgegeben 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.*

Voraussetzungen

Das verwendete Zertifikat muss seinen privaten Schlüssel enthalten. Die Verwendung von PFX-Zertifikaten wird dringend empfohlen, es können aber auch andere Arten (CRT, CER) verwendet werden, sofern diese ihren privaten Schlüssel enthalten.

Zertifikat im Windows-Zertifikatspeicher installieren

1. Klicken Sie auf dem Server auf **Start** und dann auf **Ausführen**.
2. Geben Sie im Feld **Öffnen** die Zeichenfolge **mmc** ein und klicken Sie dann auf **OK**.
3. Klicken Sie im Menü **Datei** auf **Snap-In hinzufügen/entfernen**.
4. Klicken Sie im Dialogfeld **Snap-In hinzufügen/entfernen** auf **Hinzufügen**.
5. Klicken Sie im Dialogfeld **Eigenständiges Snap-In hinzufügen** auf **Zertifikate** und dann auf **Hinzufügen**.
6. Klicken Sie im Dialogfeld **Zertifikate-Snap-In** auf **Computerkonto** (standardmäßig nicht aktiviert) und dann auf **Weiter**.
7. Klicken Sie im Dialogfeld **Computer auswählen** auf **Lokalen Computer (Computer, auf dem diese Konsole ausgeführt wird)** und dann auf **Fertig stellen**.
8. Klicken Sie im Dialogfeld **Eigenständiges Snap-In hinzufügen** auf **Schließen**.
9. Klicken Sie im Dialogfeld **Snap-In hinzufügen/entfernen** auf **OK**.
10. Doppelklicken Sie im linken Bereich der Konsole auf **Zertifikate** (**Lokaler Computer**).
11. Klicken Sie mit der rechten Maustaste auf **Persönlich**, zeigen Sie auf **Alle Aufgaben** und klicken Sie dann auf **Importieren**.
12. Klicken Sie auf der Seite **Willkommen** auf **Weiter**.
13. Klicken Sie auf der Seite **Zu importierende Datei** auf **Durchsuchen**, suchen Sie die Zertifikatdatei und klicken Sie dann auf **Weiter**.

    Hinweis: *Wenn Sie eine pfx-Datei importieren, müssen Sie den Dateifilter in '**Personal Information Exchange (*.pfx, *.p12)**' ändern, um ihn anzuzeigen.*

14. Wenn für das Zertifikat ein Kennwort festgelegt ist, geben Sie dieses auf der Seite **Kennwort** ein und klicken Sie dann auf **Weiter**.
15. Aktivieren Sie die folgenden Kontrollkästchen:
    a. **Schlüssel als exportierbar markieren**
    b. **Alle erweiterten Eigenschaften mit einbeziehen**
16. Klicken Sie auf der Seite **Zertifikatspeicher** auf **Alle Zertifikate in folgendem Speicher speichern** und dann auf **Weiter**.
17. Klicken Sie auf **Fertig stellen** und dann auf **OK**, um zu überprüfen, ob der Import erfolgreich war.

Alle Zertifikate, die erfolgreich im Windows Certificate Store installiert wurden, stehen bei Verwendung des Acronis Access-Konfigurationsdienstprogramms zur Verfügung.

Acronis Access **für die Verwendung Ihres Zertifikats konfigurieren**

Nachdem Sie das Zertifikat im Zertifikatspeicher installiert haben, müssen Sie Acronis Access für die Verwendung dieses Zertifikats konfigurieren.

1. Starten Sie das Acronis Access-Konfigurationswerkzeug.

   Hinweis: *Es ist standardmäßig im Verzeichnis* ***C:\Programme (x86)\Acronis\Access\Configuration Utility*** *zu finden.*

2. Wählen Sie Ihr Zertifikat im Auswahlfeld für Zertifikate auf den Registerkarten **Gateway Server** und **Access Server** aus.
3. Klicken Sie auf **Anwenden**.

Die Webdienste werden neu gestartet und sollten nach ungefähr einer Minute mit Ihrem Zertifikat ausgeführt werden.

5.8 Ablageordner erstellen

Diese Anleitung behandelt die Einrichtung eines Ablageordners mithilfe von Acronis Access und Windows Active Directory. Ein Ablageordner ist ein Ordner, in dem bestimmte Benutzer nur neue Dateien und Ordner hinzufügen können (ohne Dateien bearbeiten oder löschen zu können), während andere Benutzer vollständige Rechte besitzen.

Gehen Sie in Active Directory folgendermaßen vor:

1. Wählen Sie entweder zwei bestehende LDAP-Gruppen aus oder erstellen Sie zwei neue Gruppen. Eine davon dient für die Superbenutzer (in Gruppe A befinden sich beispielsweise Administratoren, Lehrer, Ärzte), während sich in der anderen Gruppe Benutzer befinden, die lediglich Ablagerechte besitzen (in Gruppe B befinden sich beispielsweise Kunden, Schüler, Patienten).
2. Fügen Sie jeder Gruppe die gewünschten Mitglieder hinzu.

Führen Sie auf der Maschine, auf der sich der Ablageordner befindet, folgende Schritte durch:

Ablageordner erstellen

1. Erstellen Sie einen neuen Ordner. Dies wird Ihr Ablageordner sein.
2. Klicken Sie mit der rechten Maustaste auf den Ordner und wählen Sie **Eigenschaften**.
3. Klicken Sie auf die Registerkarte 'Sicherheit' und dann auf **Bearbeiten**.
4. Klicken Sie in dem neuen Fenster auf **Hinzufügen**, geben Sie den Namen der Gruppe ein, die Sie hinzufügen möchten, und klicken Sie auf **OK**. Führen Sie dies für beide LDAP-Gruppen und die Gruppe **Ersteller-Besitzer** durch
5. Klicken Sie auf **OK**, um das Fenster zu schließen und zur Registerkarte **Sicherheit** zurückzukehren.

Berechtigungen festlegen

Klicken Sie auf der Registerkarte **Sicherheit** auf **Erweitert**. Klicken Sie dann im Fenster **Erweiterte Sicherheitseinstellungen** auf **Berechtigungen ändern ...**.

Für die Superbenutzer-Gruppe

Klicken Sie auf **Bearbeiten** und markieren Sie unter **Erlauben** die folgenden Berechtigungen:

- **Ordner durchsuchen/Datei ausführen**
- **Ordner auflisten/Daten lesen**
- **Attribute lesen**
- **Erweiterte Attribute lesen**
- **Dateien erstellen/Daten schreiben**
- **Ordner erstellen/Daten anhängen**
- **Attribute schreiben**
- **Erweiterte Attribute schreiben**
- **Löschen**
- **Berechtigungen lesen**

Für die Benutzer mit Ablagerechten

Klicken Sie auf **Bearbeiten** und markieren Sie unter **Erlauben** die folgenden Berechtigungen:

- **Ordner auflisten/Daten lesen**
- **Dateien erstellen/Daten schreiben**
- **Berechtigungen lesen**

Für die Ersteller-Besitzer-Gruppe

Klicken Sie auf **Bearbeiten** und markieren Sie unter **Erlauben** die folgenden Berechtigungen:

- **Löschen**

Führen Sie auf der Weboberfläche von Acronis Access Server folgende Schritte durch:

1. Erweitern Sie die Registerkarte **Mobiler Zugriff** und öffnen Sie die Seite **Richtlinien**.
2. Klicken Sie auf **Gruppenrichtlinie hinzufügen**.
3. Vervollständigen Sie für die Superbenutzer-Gruppe (Gruppe A) alle Richtlinien-Registerkarten entsprechend den Anforderungen Ihres Unternehmens. Weitere Informationen finden Sie im Abschnitt Richtlinien (S. 8).
4. Vervollständigen Sie für die Gruppe mit Ablagerechten (Gruppe B) alle Richtlinien-Registerkarten entsprechend den Anforderungen Ihres Unternehmens. Wählen Sie auf der Registerkarte **Applikationsrichtlinie** die folgenden Aktionen:
   - **Dateien kopieren/erstellen**

- **Dateien löschen**
- **Ordner kopieren**
- **Dateien von anderen Apps aus an Acronis Access senden**
- **Dateien an Acronis Access mit 'SaveBack' von Quickoffice senden**

Fertig! Ihr Ablageordner ist jetzt konfiguriert und einsatzbereit.

5.9 Weboberfläche anpassen

Acronis Access gestattet die Anpassung der webbasierten Benutzeroberfläche, um markenspezifische und Look-and-Feel-Anforderungen zu erfüllen. Farbschemen, Logos und andere Elemente können geändert werden, damit Kunden die Lösung unter Berücksichtigung von Unternehmensstandards integrieren können.

So fügen Sie ein benutzerdefiniertes Logo hinzu:

1. Öffnen Sie die Weboberfläche und navigieren Sie zu **Allgemeine Einstellungen** -> **Server**.
2. Wählen Sie **Benutzerdefiniertes Logo verwenden** und wählen Sie dann das gewünschte Bild aus. Es muss sich um eine JPEG- oder PNG-Datei mit einer Mindestbreite von 160 Pixeln handeln. Um ein anderes Bild auszuwählen, klicken Sie auf 'Benutzerdefiniertes Logo', wählen **Neu...** aus dem Dropdown-Menü und wählen dann eine neue Bilddatei aus.
3. Klicken Sie auf **Speichern**.

Hinweis: *Bilddateien für benutzerdefinierte Logos werden im Ordner 'Web Application\customizations' gespeichert. Dieser befindet sich gewöhnlich unter:* ***C:\Programme (x86)\Acronis\Access\Access Server\Web Application\customizations****. Diese Dateien werden bei der Aktualisierung von Acronis Access beibehalten.*

Hinweis: *Copyright-Hinweise, Logos und die Elemente am unteren Rand jeder Webseite (in der Fußzeile) dürfen ohne ausdrückliche Genehmigung von Acronis weder geändert noch entfernt werden.*

So fügen Sie benutzerdefinierte Stilvorlagen hinzu:

1. Erstellen Sie eine Kopie einer der Standardstilvorlagen im Verzeichnis **\stylesheets**. Diese sind normalerweise unter folgendem Pfad gespeichert: **`C:\Program Files (x86)\Acronis\Access\Access Server\Web Application\stylesheets`**.
2. Fügen Sie diese im Ordner **customizations** ein. Dieser ist normalerweise unter folgendem Pfad gespeichert: **`C:\Program Files (x86)\Acronis\Access\Access Server\Web Application\customizations`**.
3. Bearbeiten Sie die Stilvorlage und ändern Sie die Farben und Einstellungen entsprechend Ihren Vorstellungen. Speichern Sie dann die Änderungen.
4. Geben Sie der Datei einen neuen Namen, der mit **`color_scheme_*.css`** beginnt. (z.B. **`color_scheme_My_Color.css`**). Diese Datei erscheint in der Dropdown-Liste **Farbschema** auf der Seite Server-Einstellungen (S. 79).
5. Öffnen Sie die Weboberfläche und navigieren Sie zu **Allgemeine Einstellungen** -> **Server**.
6. Klicken Sie auf **Farbschema** und wählen Sie Ihr benutzerdefiniertes Schema (**My Color**) aus dem Dropdown-Menü aus.
7. Klicken Sie auf **Speichern**.

5.10 So unterstützen Sie verschiedene Access Desktop Client-Versionen

Wenn Sie eine ältere Access Desktop Client-Version verwenden möchten, gehen Sie folgendermaßen vor:

1. Laden Sie die Access Desktop Client-Version herunter, die Sie verwenden möchten. Achten Sie darauf, dass die folgenden vier Dateien vorhanden sind:
   - AcronisAccessMac.zip
   - AAClientInstaller.msi
   - AcronisAccessInstaller.dmg
   - AcronisAccessClientInstaller.exe
2. Kopieren Sie die Dateien.
3. Öffnen Sie auf dem Server den Access Desktop Clients-Ordner (**`C:\Program Files (x86)\Acronis\Access Server\Web Application\clients`**).
4. Erstellen Sie einen Unterordner für diese Version des Clients. Dieser sollte mit der **Versionsnummer des Clients** (z.B. **2.7.0x167**, **2.6.0.x140**, **2.7.1x145**) benannt sein.
5. Fügen Sie die vier Dateien in den eben erstellten Unterordner ein.
6. Öffnen Sie anschließend die **webbasierte Benutzeroberfläche** des Acronis Access Servers.
7. Melden Sie sich als **Administrator** an, gehen Sie zur Registerkarte **Sync & Share**, und öffnen Sie die Seite **Acronis Access Client**.
8. Suchen Sie die folgende Einstellung: **Erlaube Client-Auto-Update auf Version**.
9. Wählen Sie Ihre gewünschte Version im Dropdown-Menü aus.

Hinweis: *Über den Download-Link im **Menü 'Action'** für Ihr Konto können Sie weiterhin die neueste verfügbare Acronis Access Desktop Client-Version herunterladen. Wenn die Benutzer nicht die aktuelle Version herunterladen sollen, gehen Sie zum Ordner **\Access Server\Web Application\clients** und geben Sie dem Ordnernamen der aktuellen Clientversion (z.B. **3.0.3x102**) den Namen '**Versionsnummer nicht verwenden**' (z.B. '**3.0.3x102 nicht verwenden**').*

5.11 So verschieben Sie den FileStore an einen anderen als den Standardspeicherort.

Hinweis: *Bevor Sie fortfahren, melden Sie sich als Administrator an, rufen die Seite **Server-Einstellungen** auf und notieren im Feld **File Store Repository Service** den verwendeten Port. Dieser Port ist normalerweise 5787, kann aber bei Ihrem Setup abweichen. Sie benötigen diesen Port für die folgende Vorgehensweise.*

1. Wechseln Sie zu dem Computer, auf dem Acronis Access installiert ist.
2. Halten Sie den **Acronis Access Datei-Repository-Server**dienst an.
3. Stoppen Sie den **Acronis Access Tomcat**-Dienst.
4. Sie finden den aktuellen FileStore-Ordner in dem Verzeichnis, das Sie im **Konfigurationswerkzeug** ausgewählt haben.
5. Sie können den gesamten FileStore-Ordner einschließlich aller Inhalte an einen gewünschten Zielspeicherort kopieren oder verschieben, z.B.:
   `D:\MyCustom Folder\FileStore`
6. Öffnen Sie das **Konfigurationswerkzeug**.

7. Ersetzen Sie auf der Registerkarte **Datei-Repository** den Pfad des **FileStore**-Ordners durch den Speicherort, an den Sie den **FileStore**-Ordner verschoben haben.
8. Ändern Sie ggf. den FileStore-Port. Wenn Sie den FileStore-Port ändern, müssen Sie in den Einstellungen für Sync & Share-Datei-Repository (S. 71) auch den Dateispeicher-Repository-Endpunkt ändern.
9. Wenn sich der Dateispeicher für das Datei-Repository auf einer entfernten Netzwerkfreigabe befindet, konfigurieren Sie für das Dienstkonto Berechtigungen für den Zugriff auf diese Netzwerkfreigabe. 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.
10. Starten Sie den **Acronis Access Datei-Repository-Server**dienst.
11. Starten Sie den **Acronis Access Tomcat**-Dienst.
12. Fertig.

5.12 Acronis Access für Good Dynamics

Themen

5.12.1 Einführung

Acronis und Good Technology sind eine Partnerschaft eingegangen, um die mobile Dateiverwaltung von Acronis Access auf die Good Dynamics-Plattform zu übertragen. Dank dieser optionalen Acronis Access-Funktion kann die Access Mobile Client-App zusammen mit anderen Good-fähigen Apps mit einem einheitlichen Satz von Good Dynamics-Richtlinien und -Diensten verwaltet werden.

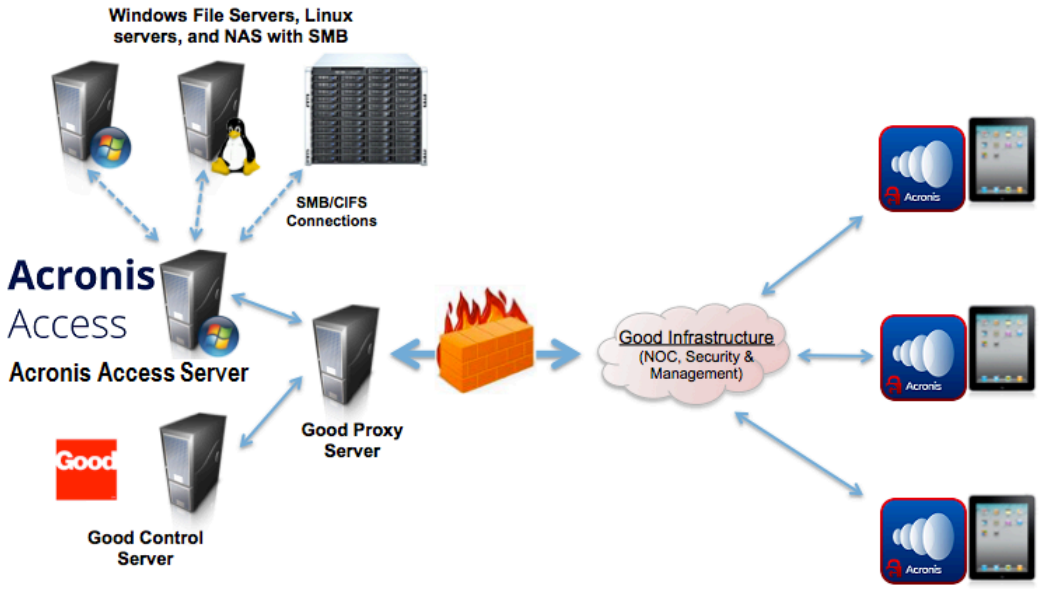
Die Plattform von Good Dynamics umfasst folgende Komponenten:

- **Server von Good Control** – Eine serverbasierte Konsole, mit der das Unternehmen den Client-Zugriff auf für Good Dynamics aktivierte Apps ermöglichen, Richtliniensätze für Applikationsberechtigungen und die erlaubten Gerätetypen erstellen sowie den Zugriff auf Apps von Good Dynamics auf bestimmten Geräten widerrufen und die Apps auf diesen löschen kann.
- **Good Proxy-Server** – Dieser Dienst wird auf einem Server vor Ort installiert und bietet Netzwerkzugriff für Good Dynamics-Apps, die mit Servern vor Ort kommunizieren müssen, z.B. mit einem Acronis Access Gateway Server.
- **Acronis Access für Good Dynamics-App** – Good Dynamics-fähige Apps wie Acronis Access für Good Dynamics enthalten integrierte Good Dynamics-Dienste, die eine Remote-Verwaltung der App über die Good Dynamics-Plattform zulassen und der App außerdem einen sicheren verschlüsselten nach FIPS 140-2 zertifizierten Gerätespeicher und eine sichere Good-Kommunikation zur Verfügung stellen.

Acronis Access für Good Dynamics erfordert:

- **Acronis Access für Good Dynamics-Client-App** – Die im Apple App Store erhдltliche Acronis Access fьr Good Dynamics-Client-App http://www.grouplogic.com/web/megoodappstore ist speziell als integrierte Good Dynamics-Applikation konzipiert. Wenn die Acronis Access für Good Dynamics-App erstmals auf einem Gerät installiert und ausgeführt wurde, wird der Benutzer aufgefordert, die App in Good Dynamics zu aktivieren. Diese Aktivierung ist erforderlich, bevor der Benutzer mit der Registrierung der App auf dem Acronis Access-Server und dem Zugriff auf Dateien fortfahren kann.
- **Acronis Access-Server** – Acronis Access für Good Dynamics verwendet die gleiche serverseitige Software wie die Standardversion von Acronis Access. Es sind keine serverseitigen Änderungen erforderlich, damit Acronis Access-Server mit Good Dynamics-fähigen Acronis Access-Clients arbeiten können. So wird sichergestellt, dass alle Access Mobile Clients Zugriff auf Acronis Access-Dateien haben, die von Good Dynamics verwaltet werden.

Sobald ein Acronis Access für Good Dynamics-Client in Good Dynamics registriert ist, wird die gesamte Kommunikation mit den Gateway Servern über den sicheren Good Dynamics-Kommunikationskanal geleitet.



5.12.2 Eine Testversion von Acronis Access für Good Dynamics testen

Das Testen von Acronis Access für Good Dynamics entspricht weitgehend dem Test einer normalen Acronis Access-Testversion.

1. Eine Testversion der Serversoftware kann auf der Seite Testversion angefordert werden. Sobald das Anforderungsformular gesendet wurde, erhalten Sie eine E-Mail mit Links zum Herunterladen des Installers für die Acronis Access-Server-Testversion und zur Schnellstart-Anleitung, die Sie bei der erstmaligen Einrichtung unterstützt.
2. Die Acronis Access für Good Dynamics-Client-App kann kostenlos aus dem Apple App Store http://www.grouplogic.com/web/megoodappstore heruntergeladen werden.

Acronis Access für Good Dynamics-Client-Apps müssen im Good Dynamics-System aktiviert werden, bevor sie für den Zugriff auf Gateway Server konfiguriert werden können. Wenn Sie bereit sind, Acronis Accesss in Good Dynamics zu registrieren, lesen Sie die folgenden Abschnitte in diesem Dokument.

5.12.3 Acronis Access in Good Control anfordern und konfigurieren

Bevor eine Acronis Access für Good Dynamics-Client-App in Good Dynamics registriert werden kann, muss Acronis Access der Liste **Verwaltete Anwendungen** auf dem Good Control-Server hinzugefügt werden. Damit dies geschieht, müssen Sie über die Good Dynamics **beGood Communities**-Website den Zugriff auf die **Acronis Access für Good Dynamics**-App anfordern. Wenn Sie derzeit nicht als Mitglied der beGood-Website registriert sind, ist möglicherweise ein anderer Mitarbeiter für die Verwaltung der Anbieterbeziehungen auf dieser Website verantwortlich oder Sie müssen sich einfach bei beGood registrieren.

Themen

5.12.3.1 Zugriff auf Acronis Access für Good Dynamics anfordern

Um den Zugriff auf **Acronis Access für Good Dynamics** anzufordern, besuchen Sie die folgende URL:
https://begood.good.com/gd-app-details.jspa?ID=248978
https://begood.good.com/gd-app-details.jspa?ID=248978

Über diesen Link gelangen Sie direkt zur App. Falls dies nicht funktioniert, besuchen Sie https://begood.good.com/marketplace.jspa https://begood.good.com/marketplace.jspa, und suchen Sie **Acronis Access für Good Dynamics** in der Liste verfügbarer **Good Dynamics**-Apps.

Klicken Sie auf der Seite der Acronis Access für Good Dynamics-App auf die Schaltfläche 'Get Application', um eine Demoversion oder eine lizenzierte Version der App zu erhalten.
https://begood.good.com/gd-app-details.jspa?ID=248978

Good Dynamics Marketplace > Acronis Access For Good (formerly mobilEcho)

Acronis Access For Good (formerly mobilEcho)

by GroupLogic
v. 6.0.3.0
Registered on Apr 8, 2014

Get Application

OR Request Call Back

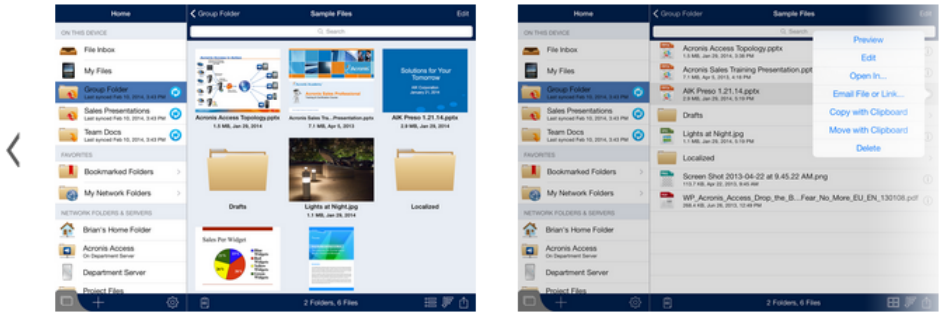
Category:
Document Editing / Annotation
SharePoint / File Access / Sync

Developer Website
Data Sheet

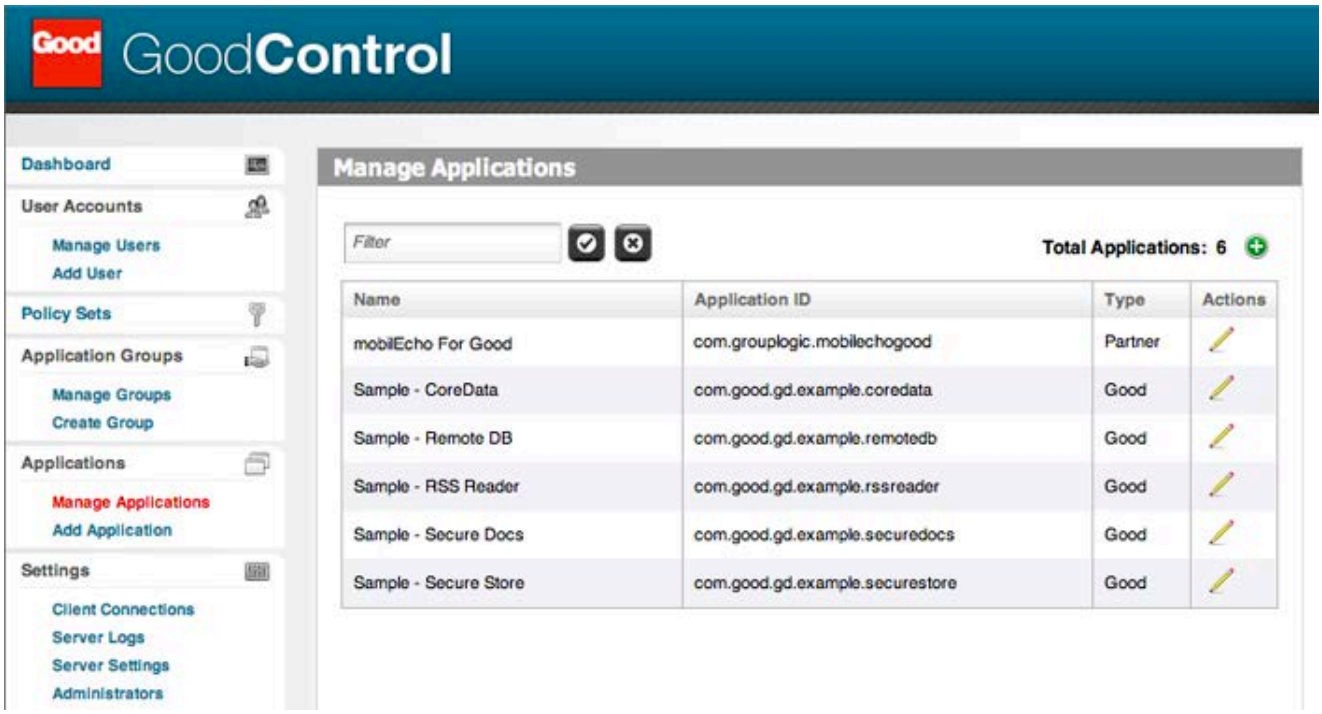
Description

Acronis Access (formerly mobilEcho) enables enterprise employees using any device - desktop, laptop, tablet or smartphone - to securely access, sync and share corporate content while IT maintains control over security and compliance. Content can be accessed from file servers, NAS, SharePoint, and personal devices, and shared with internal and external constituents. Acronis Access empowers IT to control the level of security needed and promote end user productivity anywhere, Read More...

Screenshots



Wenn Sie eine Demoversion der App anfordern, sollten Sie innerhalb weniger Minuten Zugriff darauf haben. Wenn Ihre Anforderung akzeptiert wurde, erhalten Sie von der beGood-Website eine Benachrichtigung, in der Sie darüber informiert werden, dass die **Acronis Access für Good Dynamics**-App auf Ihrem Good Control-Server veröffentlicht wurde. Melden Sie sich danach auf dem Good Control-Server an, und klicken Sie im Menü auf der linken Seite auf 'Applikationen verwalten (Manage Applications)'. Acronis Access sollte jetzt als Partner-App in der Liste verwalteter Applikationen aufgeführt werden. Ist dies nicht der Fall, warten Sie ca. eine Viertelstunde ab und überprüfen Sie die Liste dann noch einmal. Diese Zeit sollte ausreichen, um die Änderung auf dem Server umzusetzen.

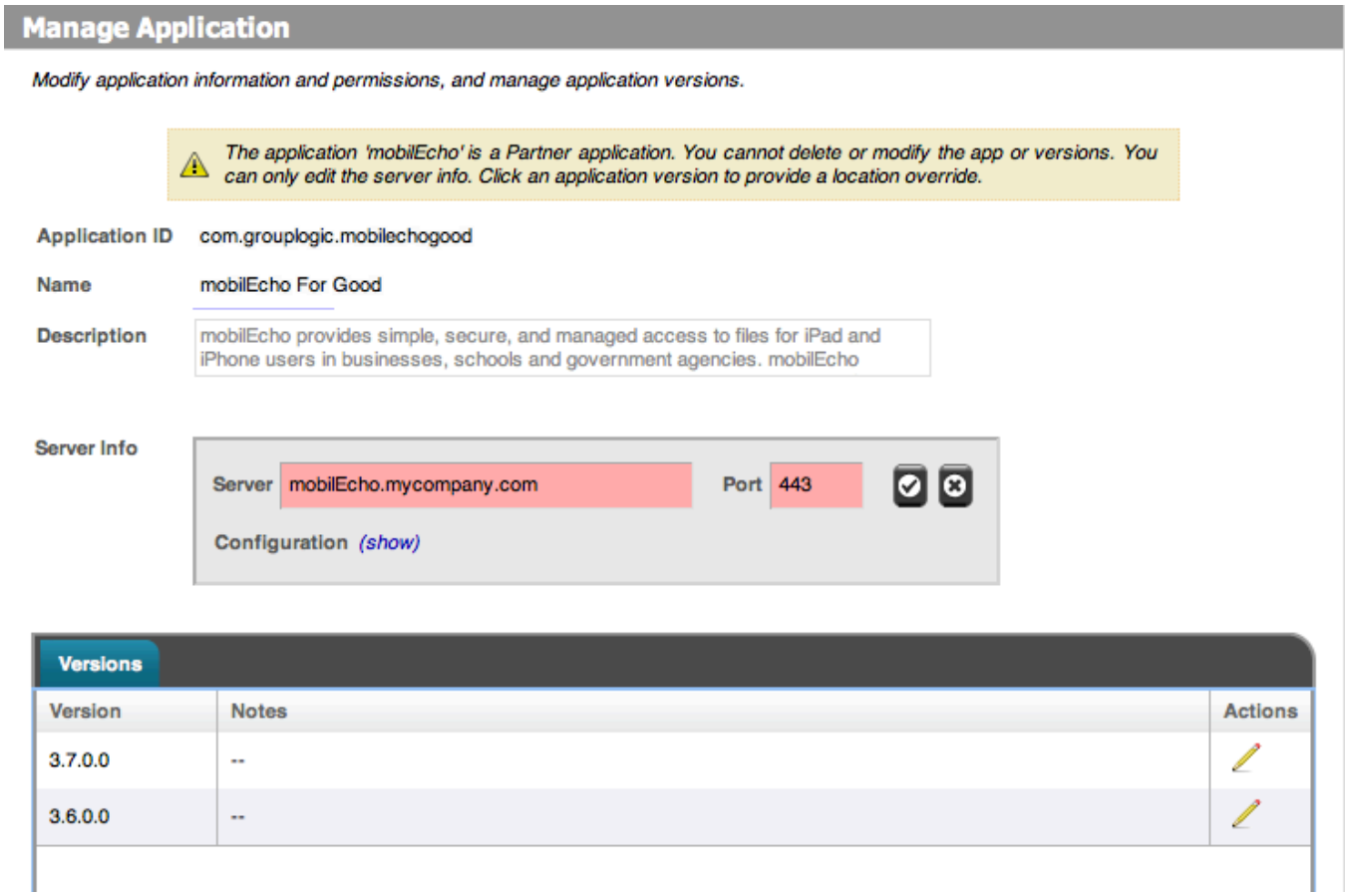


5.12.3.2 Good Proxy-Zugriff auf den/die Acronis Access Gateway Server konfigurieren

Damit die Access Mobile Clients über den Good Proxy-Server auf den Acronis Access Gateway Server zugreifen können, müssen Sie die Adresse des Acronis Access Gateway Servers in der Konfiguration der Applikation eingeben. Wenn Sie mehrere Acronis Access Gateway Server haben, konfigurieren Sie hier den Zugriff auf einen Acronis Access Gateway Server. Weitere Server können auf der Seite 'Client-Verbindungen (Client Connections)' in der Good Control-Konsole hinzugefügt werden. Einzelheiten dazu finden Sie weiter unten.

Klicken Sie auf die **Acronis Access**-App in der Liste **Applikationen verwalten (Manage Applications)**, um deren Einstellungen zu öffnen.

Geben Sie in das Feld **Server-Info (Server Info)** den DNS-Namen oder die IP-Adresse des Acronis Access Gateway Servers ein. Die **Port**-Nummer lautet in der Regel **443**, es sei denn, Sie haben für Acronis Access einen nicht standardmäßigen Port konfiguriert. Die gesamte Kommunikation zwischen Acronis Access-Clients und den Gateway Servern findet standardmäßig über Port 443 statt. Klicken Sie auf die Schaltfläche 'Überprüfen', um diese Änderung zu speichern.

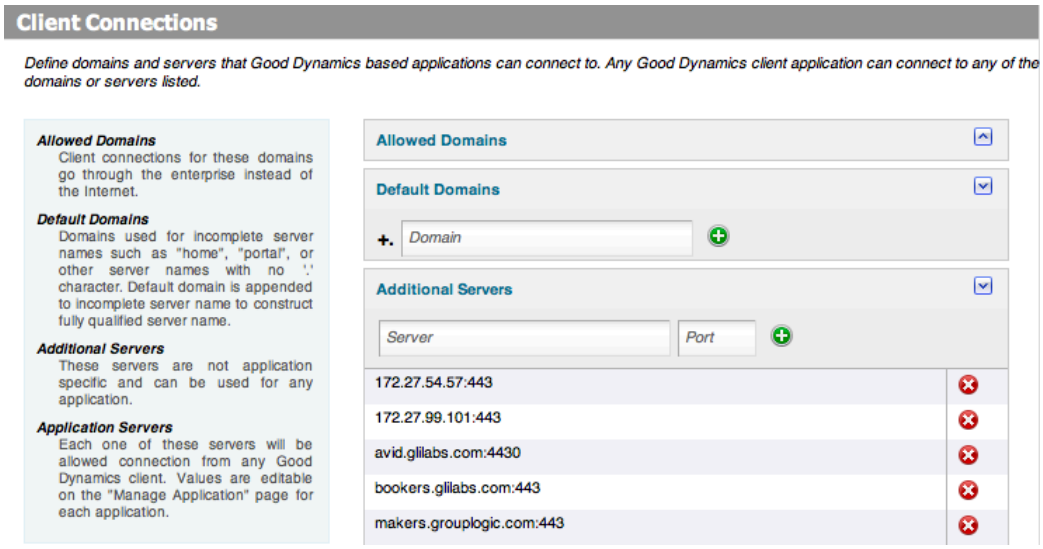


5.12.3.3 Zugriff auf mehrere Acronis Access Gateway Server erlauben

Wenn das Netzwerk mehrere Acronis Access Gateway Server enthält, müssen Sie in der Good Control-Konsole zusätzliche Server-Adressen zulassen. Wenn Sie dies nicht tun, kann der Access Mobile Client nur eine Verbindung mit dem einen Server herstellen, den Sie im vorherigen Schritt konfiguriert haben.

Um den Zugriff auf weitere Gateway Server zu gestatten, wählen Sie in der Good Control-Konsole im Menü auf der linken Seite das Element **Client-Verbindungen (Client Connections)** aus.

Geben Sie in das Feld **Zusätzliche Server (Additional Servers)** den DNS-Namen oder die IP-Adresse des Gateway Servers und seinen Port ein, und klicken Sie auf das '+'-Symbol, um ihn der Liste hinzuzufügen. Der Standardport des Gateway Servers lautet 443.



5.12.4 Good Dynamics-Richtliniensätze und Acronis Access

Die Acronis Access für Good Dynamics-App berücksichtigt die Richtlinieneinstellungen, die in dem einem Benutzer zugewiesenen **Richtliniensatz** enthalten sind. Richtliniensätze werden auf dem Good Control-Server konfiguriert.

Dazu gehören diese Einstellungen:

- Kennwortanforderungen zum Sperren der Applikation
- Richtlinien zum Sperren des Bildschirms
- Schutzfunktion gegen Datenlecks
- Zulässige iOS-Versionen und Hardwaremodelle
- Überprüfung der Verbindung
- Jailbreak/Root-Erkennung

Auswirkungen und Beschränkungen der Schutzfunktion gegen Datenlecks

Wenn die **Schutzfunktion gegen Datenlecks (Data Leakage Protection)** in einem Richtliniensatz aktiviert ist, ist dem Access Mobile Client Folgendes nicht gestattet:

- Öffnen von standardmäßigen Dateien in Drittanbieterapplikationen auf dem Gerät
- Empfangen von standardmäßigen Dateien von anderen Drittanbieterapplikationen auf dem Gerät
- Senden von Dateien per E-Mail mit dem iOS-E-Mail-Client
- Drucken von Dateien
- Kopieren und Einfügen von Text innerhalb von geöffneten Dateien

*Falls Sie diese Funktionen benötigen, müssen Sie das Kontrollkästchen **Schutz vor Datenverlusten deaktivieren** im betreffenden Good-Richtliniensatz aktivieren.*

Acronis Access für Good Dynamics umfasst eine Good Dynamics-Funktion mit dem Namen 'Secure Docs'. Diese Funktion ermöglicht die Übertragung von Dateien zwischen der Acronis Access für Good Dynamics-App und der Good for Enterprise-App. Sobald eine Datei in der Good für Enterprise-App geöffnet wurde, kann sie in anderen aktivierten Good Dynamic-Apps von Drittanbietern geöffnet werden, die diese Funktion beinhalten. Diese Funktion ist auch dann verfügbar, wenn die Good Control-Richtlinieneinstellung ***Schutzfunktion gegen Datenlecks*** *aktiviert ist.*

In einer kommenden Version von Acronis Access für Good Dynamics wird es möglich sein, Dateien zwischen der Acronis Access für Good Dynamics-App und anderen Good Dynamics-Drittanbieter-Apps direkt zu übertragen. Diese Funktion erfordert Änderungen an Acronis Access für Good Dynamics und den betroffenen Drittanbieter-Apps, sodass alle Apps, die Sie für die Überragung von Dateien benötigen, auch von ihren Anbietern aktualisiert werden müssen.

5.12.5 Acronis Access Zugriff auf Good Dynamics-Benutzer oder -Gruppen gewähren

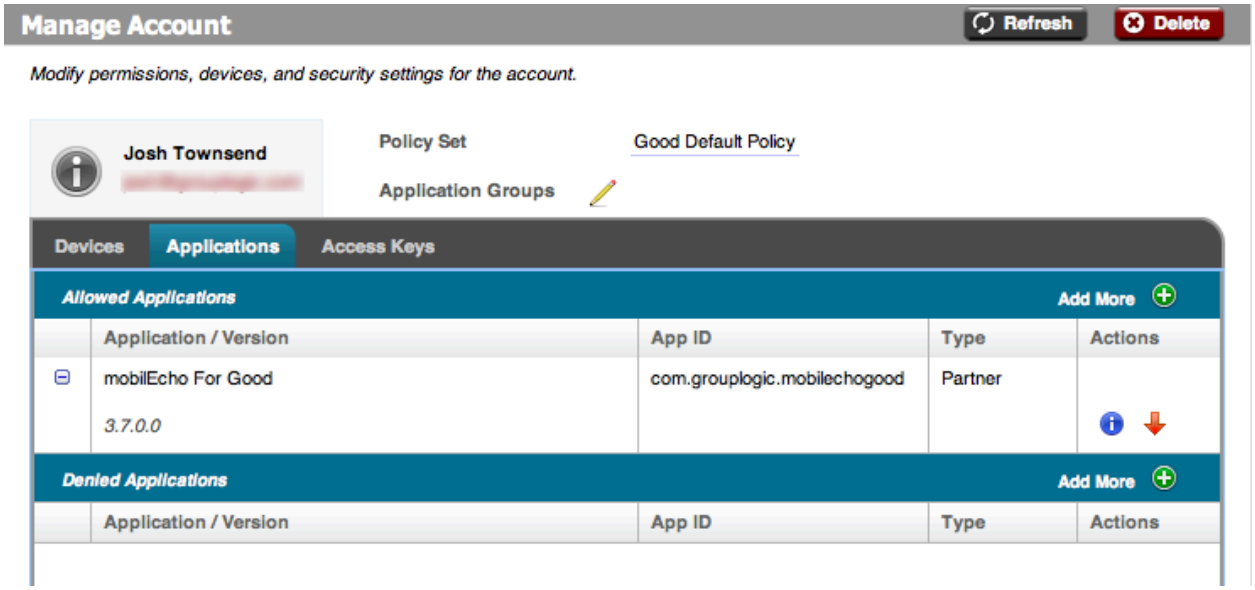
Bevor ein Benutzer die Access Mobile Client-App in Good Dynamics registrieren kann, muss die Acronis Access-Applikation der Liste **Erlaubte Apps** seines Benutzerkontos oder einer zugelassenen **Applikationsgruppe** hinzugefügt werden, der er angehört. Darüber hinaus muss dem Benutzer ein eindeutiger **Zugriffsschlüssel** gesendet werden, der während des Registrierungsprozesses in die Acronis Access-App eingegeben werden muss.

WICHTIGER HINWEIS ZUR BEREITSTELLUNG: *Wenn Sie einzelnen Benutzern Zugriff auf Good Dynamics-Applikationen zuweisen, müssen Sie die bestimmten Versionsnummern der App auswählen, auf die Zugriff gewährt werden soll. Wenn Sie den Zugriff auf der Benutzerebene verwalten, müssen Sie bei der Veröffentlichung neuer Versionen von Acronis Access für Good Dynamics die Good Control-Konfiguration des Benutzers aufrufen und die neue Version hinzufügen. Erst danach kann diese Version verwendet werden. Es wird* ***dringend geraten****, den Zugriff auf Good Dynamics-Apps über die Funktion* ***Gruppen verwalten*** *in der Konsole von Good Control zu gestatten. Mit Good Control sind Sie in der Lage, einer Gruppe Zugriff auf ALLE Versionen einer App zu gewähren, damit auch zukünftige Versionen ohne Eingriff durch den IT-Administrator erlaubt werden.*

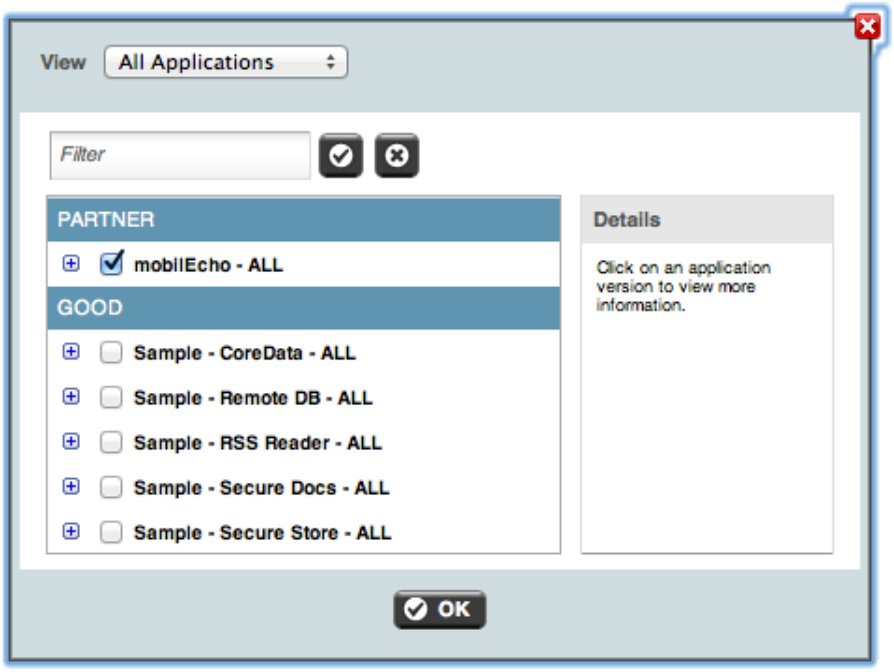
So fügen Sie die Acronis Access-App der Liste Erlaubte Apps in einem Benutzerkonto oder einer Applikationsgruppe hinzu:

1. Wählen Sie im Menü auf der linken Seite der Konsole von Good Control **Gruppen verwalten** oder **Benutzer verwalten**.
2. Wählen Sie die Gruppe oder den Benutzer aus, der bzw. dem Sie Zugriff auf Acronis Access für Good Dynamics gestatten möchten.

3. Klicken Sie auf der Registerkarte **Applikationen** auf **Erlaubte Apps** und '**Weitere hinzufügen**'.



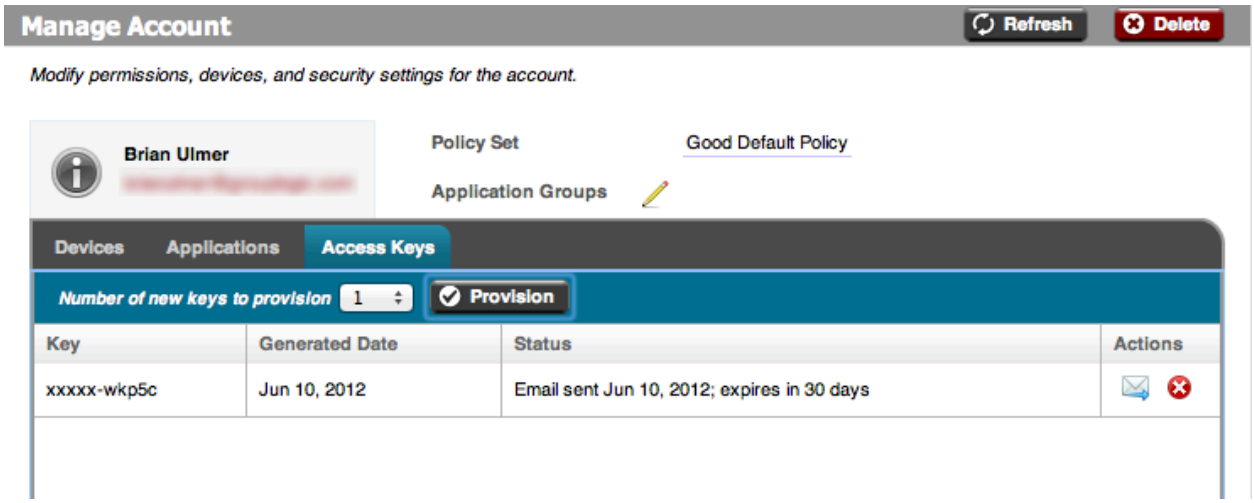
4. Wählen Sie **Acronis Access für Good Dynamics** in der Liste verfügbarer Applikationen aus, und klicken Sie auf **OK**.



So erstellen Sie einen Zugriffsschlüssel, mit dem ein Benutzer seine Acronis Access für Good Dynamics-App bei Good Dynamics registrieren kann:

1. Wählen Sie im Menü auf der linken Seite der Konsole von Good Control **Benutzer verwalten**.
2. Wählen Sie den Benutzer aus, für den Sie einen **Zugriffsschlüssel** erstellen möchten.

3. Wählen Sie auf der Registerkarte **Zugriffsschlüssel** die Anzahl der zu sendenden Schlüssel aus und klicken Sie auf **Bereitstellen**.



Der Benutzer erhält eine E-Mail mit dem **Zugriffsschlüssel** und einige grundlegende Anweisungen zu Good Dynamics.

5.12.6 Die Acronis Access-Client-App in Good Dynamics registrieren

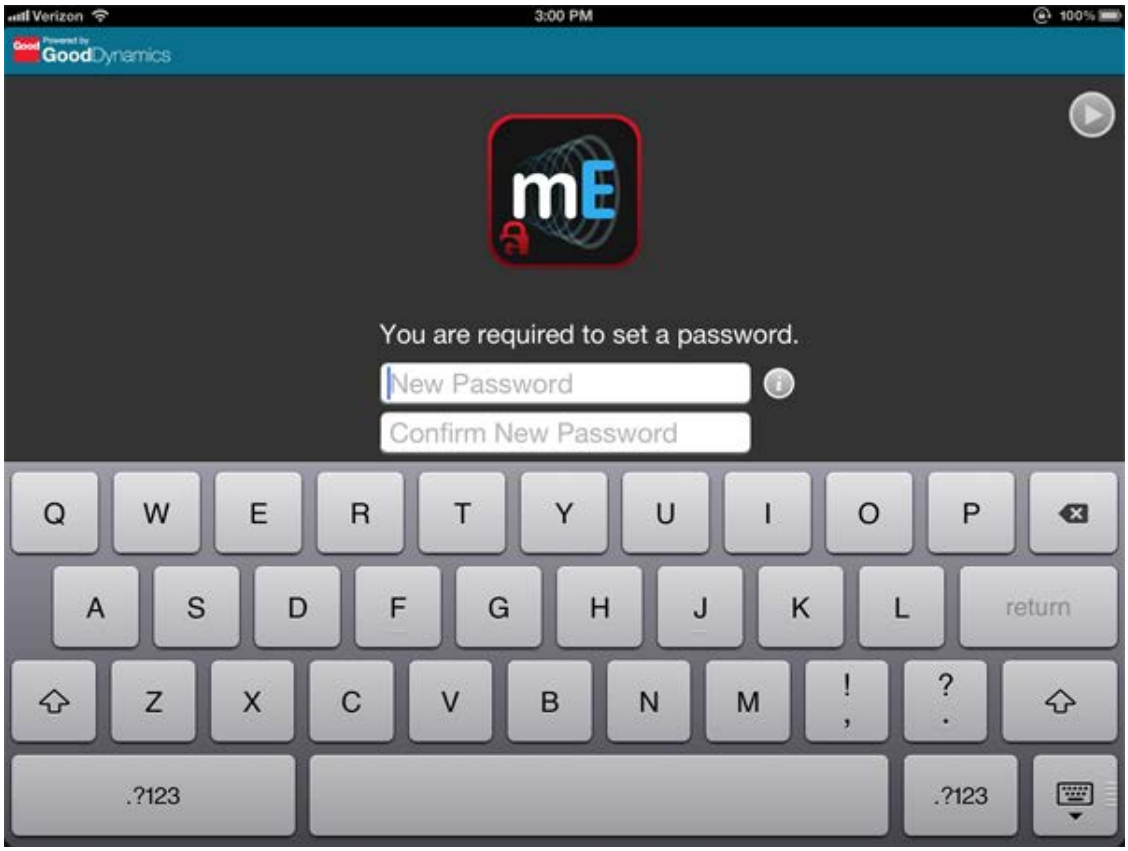
Die im Apple App Store erhältliche Acronis Access für Good Dynamics-Client-App http://www.grouplogic.com/web/megoodappstore ist speziell als Good Dynamics-integrierte Applikation konzipiert. Bei der Erstinstallation auf einem Gerät wird die Acronis Access-App gestartet, und der Benutzer wird aufgefordert, sie in Ihrem Good Dynamics-System zu aktivieren.

So registrieren Sie eine Acronis Access-**Client-App in Good Dynamics:**

1. Starten Sie **Acronis Access für Good Dynamics** auf Ihrem Gerät.
2. Geben Sie Ihre **E-Mail-Adresse** und den **Zugangsschlüssel** ein, der Ihnen vom IT-Administrator zugeschickt wurde.

3. Während der Registrierung Ihrer App bei Good Dynamics sehen Sie eine Statusanzeige.

4. Falls von Ihrer Good Dynamics-Richtlinie verlangt, werden Sie aufgefordert, ein Kennwort zum Sperren der Applikation zu erstellen. Wenn Sie auch Good for Enterprise verwenden, verlangt Acronis Access u.U. die Anmeldung bei Good for Enterprise, damit Sie Zugriff auf die Acronis Access-App erhalten.



5. Sobald dieser Prozess abgeschlossen ist, gelangen Sie zum Startbildschirm der Acronis Access-App.

Ab diesem Punkt müssen Sie beim Starten der Access Mobile Client-App eventuell das Kennwort für die Acronis Access für Good Dynamics-App eingeben, das Sie zuvor konfiguriert haben, oder Sie müssen sich bei Ihrer Good for Enterprise-App authentifizieren, bevor Acronis Access geöffnet wird.

Abgesehen von dieser Anforderung funktioniert Acronis Access für Good Dynamics auf die gleiche Weise wie der standardmäßige Access Mobile Client. Manche Funktionen sind aufgrund der festgelegten Good Dynamics-Richtlinien möglicherweise eingeschränkt. Dies betrifft Funktionen wie das Öffnen von Acronis Access-Dateien in anderen Drittanbieter-Applikationen, das Senden von Dateien per E-Mail, das Drucken von Dateien, das Kopieren und Einfügen von Text aus Acronis Access-Dateien usw.

Sobald die Acronis Access für Good Dynamics-App in Good Dynamics aktiviert wurde, kann sie nicht mehr deaktiviert werden. Wenn Sie zu einer Standardversion von Acronis Access wechseln möchten, müssen Sie die Acronis Access für Good Dynamics-App löschen und die standardmäßige Access Mobile Client-App über den Apple App Store http://www.grouplogic.com/web/meappstore neu installieren.

5.13 MobileIron AppConnect-Support

Themen

5.13.1 Einführung

Acronis und MobileIron sind eine Partnerschaft eingegangen, um die mobile Dateiverwaltung von Acronis Access auf die MobileIron AppConnect-Plattform zu übertragen. Dank dieser Acronis Access-Funktion kann die standardmäßige Access Mobile Client-App zusammen mit anderen AppConnect-fähigen Apps optional automatisch von in AppConnect definierten Richtlinien konfiguriert und verwaltet werden. Der Acronis Access unterstützt außerdem MobileIron AppTunnel für den Remote-Zugriff auf Acronis Access Gateway Server, die innerhalb des unternehmenseigenen Datencenters angesiedelt sind.

Zu den Komponenten von Acronis Access mit MobileIron AppConnect gehören:

- **MobileIron Virtual Smartphone-Plattform (VSP)** – Eine serverbasierte Konsole, mit der das Unternehmen den Client-Zugriff auf für AppConnect aktivierte Apps ermöglichen, diese Apps automatisch konfigurieren, Richtlinien für die App-Funktionen erstellen sowie den Zugriff auf für AppConnect aktivierte Apps auf bestimmten Geräten widerrufen und die Apps auf diesen löschen kann.
- **MobileIron Sentry** – Dieser Dienst ermöglicht den Netzwerkzugriff von AppConnect-fähigen Apps, die mit Applikations-Servern vor Ort kommunizieren müssen, z.B. einem Acronis Access Gateway Server.
- **MobileIron Mobile@Work App** – Diese App handelt die Authentifizierung und Konfiguration für AppConnect aktivierter Apps aus. Sie muss auf dem mobilen Gerät installiert werden, um für AppConnect aktivierte Apps konfigurieren und verwalten zu können.
- **Acronis Access-iOS-App** – Die Standardversion von Acronis Access für iOS (Version 5.0 oder höher), die im Apple App Store erhältlich ist, kann von AppConnect konfiguriert und verwaltet werden und über AppTunnel mit Acronis Access Gateway Servern kommunizieren.
- **Acronis Access Server** – Die Standardversion von Acronis Access Server (Version 5.0 oder höher) ist vollständig kompatibel mit Access Mobile Clients, die von AppConnect verwaltet werden.

5.13.2 Eine Testversion von Acronis Access für AppConnect testen

Das Testen von Acronis Access mit AppConnect entspricht weitgehend dem Test einer normalen Acronis Access-Testversion.

1. Eine Testversion der serverseitigen Software können Sie über die Seite 'Testversion' anfordern. Sobald die Anfrage eingesendet wurde, erhalten Sie eine E-Mail mit Links zum Herunterladen des Installationsprogramms für die Testversion von Acronis Access Server sowie der Schnellstartanleitung, die Sie bei der Ersteinrichtung unterstützt.

2. Die Acronis Access-iOS-Client-App kann kostenlos aus dem Apple App Store http://www.grouplogic.com/web/meappstore heruntergeladen werden.

Für die Acronis Access-iOS-App muss eine AppConnect-Konfiguration und -Richtlinie auf der MobileIron Virtual Smartphone-Plattform (VSP) erstellt werden, bevor sie automatisch für den Zugriff auf Ihre(n) Acronis Access Gateway Server konfiguriert werden kann.

Außerdem muss auf dem iOS-Gerät die MobileIron Mobile@Work-App https://itunes.apple.com/app/mobilecho/id320659794 installiert sein, bevor irgendwelche AppConnect-fähigen Apps aktiviert werden können.

Wenn Sie bereit sind, Access Mobile Clients mit AppConnect zu aktivieren, lesen Sie die folgenden Abschnitte dieses Dokuments.

5.13.3 Eine AppConnect-Konfiguration und -Richtlinie für Acronis Access auf der MobileIron-VSP erstellen

Sie können erst dann mit dem Einbinden von Acronis Access-Benutzern (S. 27) beginnen, wenn Sie in MobileIron VSP zwei Elemente erstellt haben:

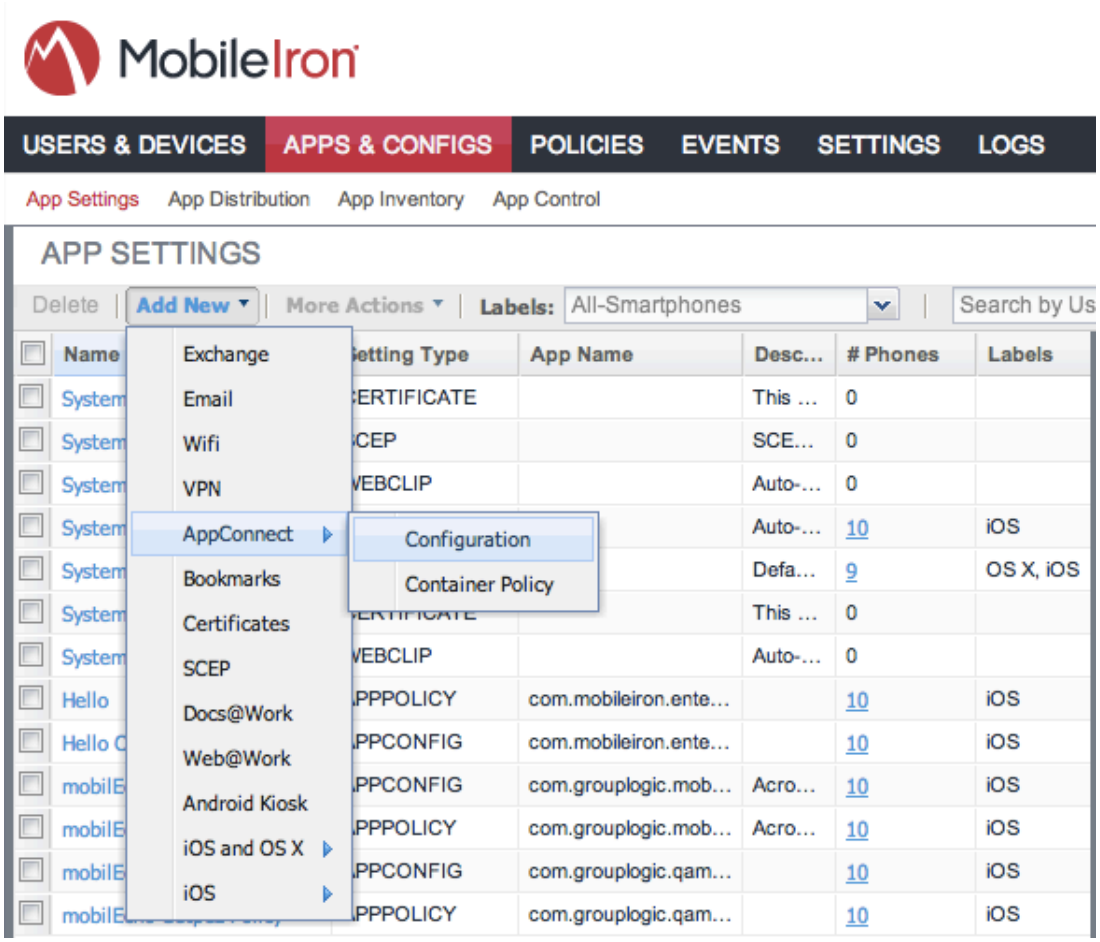
1. Access Mobile Client-App-**Konfiguration** – Damit kann AppConnect die Access Mobile Client-App automatisch konfigurieren und das Acronis Access-'Registrierungsformular' ganz oder teilweise ausfüllen und die Stelle des Acronis Access-Benutzereinladungsprozesses einnehmen.
2. Access Mobile Client-App-**Container-Richtlinie** – Diese Richtlinie ermöglicht die Einschränkung einer Funktionen von Acronis Access.

Themen

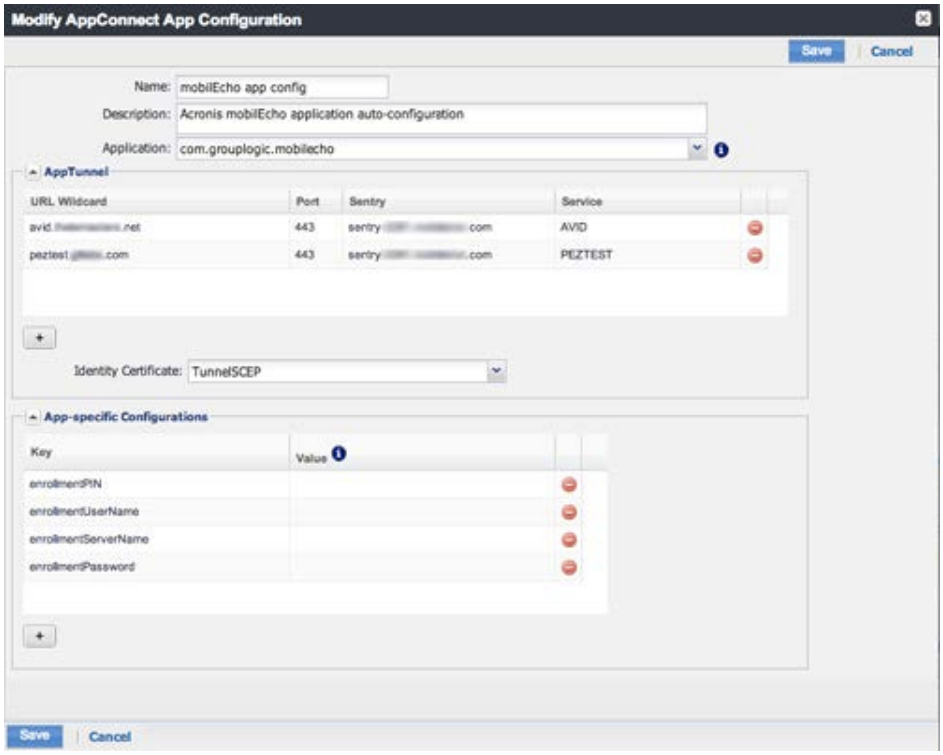
5.13.3.1 Eine Access Mobile Client-App-Konfiguration erstellen

Melden Sie sich bei der Web-Konsole von MobileIron VSP an und wählen Sie die Registerkarte **APPS UND KONFIGURATIONEN**.

Klicken Sie in den **App-Einstellungen** auf **Neu hinzufügen** und wählen Sie unter dem Menüelement **AppConnect** den Eintrag '**Konfiguration**' aus.



Geben Sie in dieser neuen App-Konfiguration von AppConnect folgende Informationen ein:



Name – Dieser Konfiguration können Sie einen beliebigen Namen zuweisen. Sie können mehrere Konfigurationen erstellen und diese unterschiedlichen MobileIron-Labels zuweisen.

Beschreibung – Diese Beschreibung können Sie beliebig wählen.

Applikation – Diese muss auf den *Bundle Identifier* der Access Mobile Client-App festgelegt werden, der folgendermaßen lautet: **com.grouplogic.mobilecho**

AppTunnel – Die AppTunnel-Einstellungen sind optional und werden nur benötigt, wenn Sie über AppTunnel den Zugriff auf Ihre(n) Acronis Access Gateway Server bereitstellen.
URL-Platzhalterzeichen = Die DNS-Adresse des/der Gateway Server(s) oder Ihrer Domain insgesamt. Acronis Accesss verwenden standardmäßig Port 443. **Sentry** – Die DNS-Adresse des Servers für MobileIron Sentry.

App-spezifische Konfigurationen – In diesem Abschnitt können Sie basierend auf der MobileIron-Bezeichnung Werte festlegen, die beim automatischen Ausfüllen des Acronis Access-Registrierungsformulars für diejenigen Benutzer verwendet werden, für die diese Konfiguration gilt. Die folgenden **Schlüssel** können hinzugefügt werden:

- **enrollmentServerName** – Dieses Schlüsselfeld muss angegeben werden. Der Wert dieses Schlüssels muss auf die DNS-Adresse des Acronis Access Servers eingestellt werden, bei dem sich der Benutzer registrieren muss.
- **enrollmentPIN** – Dieser Schlüssel ist optional. Wenn der Acronis Access Server für die Client-Registrierung eine PIN-Nummer verlangt, können Sie mit diesem Wert das Feld für die PIN-Nummer auf dem Acronis Access-Registrierungsformular automatisch ausfüllen lassen. Normalerweise ist die PIN-Anforderung für den Acronis Access Server deaktiviert, da statt der einmalig zu verwendenden PIN-Nummer AppConnect als zweiter Faktor für die Authentifizierung

verwendet werden kann, bevor ein Benutzer Zugriff erhält. Diese PIN-Anforderung wird auf der Seite **Einstellungen** (S. 61) der **Acronis Access**-Webkonsole konfiguriert.

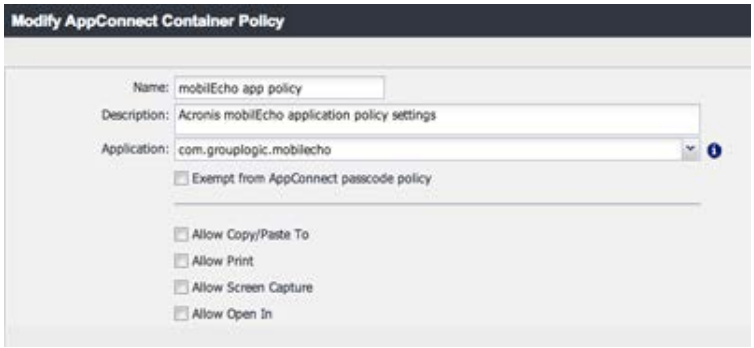
- **enrollmentAutoSubmit** – Dieser Schlüssel ist optional. Dieser Schlüssel bewirkt, dass das Registrierungsformular automatisch gesendet wird, sodass der Benutzer nicht auf die Schaltfläche 'Jetzt registrieren' tippen muss, um fortzufahren. Wenn Sie diesen Schlüssel aktivieren möchten, legen Sie folgenden Wert fest: **Ja**
- **requirePIN** – Dieser Schlüssel ist optional. Wenn Sie eine PIN an mobile Acronis Access-Benutzer verteilen, die diese manuell in das Acronis Access-Registrierungsformular eingeben müssen, können Sie festlegen, dass das PIN-Feld sofort im Formular angezeigt wird. Dazu müssen Sie den Wert dieses Schlüssels auf **Ja** festlegen.
- **enrollmentUserName** – Dieser Schlüssel ist optional. Der Wert dieses Schlüssels wird in das Feld 'Benutzername' im Acronis Access-Registrierungsformular eingefügt. Sie können eine MobileIron-Variable zum automatischen Vervollständigen dieses Werts mit dem Benutzernamen des betreffenden Benutzers verwenden.
- **enrollmentPassword** – Dieser Schlüssel ist optional. Der Wert dieses Schlüssels wird in das Feld 'Kennwort' im Acronis Access-Registrierungsformular eingefügt. Sie können eine MobileIron-Variable zum automatischen Vervollständigen dieses Werts mit dem Kennwort des betreffenden Benutzers verwenden.

5.13.3.2 Eine Container-Richtlinie für die Acronis Access-App erstellen

Melden Sie sich bei der Web-Konsole von MobileIron VSP an oder kehren Sie zu dieser zurück und rufen Sie die Registerkarte **APPS UND KONFIGURATIONEN** auf.

Klicken Sie in den **App-Einstellungen** auf **Neu hinzufügen** und wählen Sie unter dem Menüelement **AppConnect** den Eintrag '**Container-Richtlinie**' aus.

Geben Sie in dieser neuen Container-Richtlinie folgende Informationen ein:



Name – Dieser Konfiguration können Sie einen beliebigen Namen zuweisen. Sie können mehrere Konfigurationen erstellen und diese unterschiedlichen MobileIron-Labels zuweisen.

Beschreibung – Diese Beschreibung können Sie beliebig wählen.

Applikation – Diese muss auf den *Bundle Identifier* der Access Mobile Client-App festgelegt werden, der folgendermaßen lautet: **com.grouplogic.mobilecho**

Von AppConnect-Passcode-Richtlinie ausnehmen – Wählen Sie diese Option, wenn Benutzer in der Lage sein sollen, Acronis Access zu öffnen, ohne sich zuerst mit ihrem AppConnect-Passcode zu authentifizieren.

Kopieren/einfügen in zulassen – Wählen Sie diese Option, wenn es Benutzern gestattet sein soll, Text aus Dokumenten, die im Access Mobile Client angezeigt werden, in andere Apps auf dem Gerät zu kopieren und einzufügen, die nicht von AppConnect verwaltet werden.

Drucken erlauben – Wählen Sie diese Option, wenn es Acronis Access-Benutzern gestattet sein soll, Dokumente auf verfügbaren AirPrint-fähigen Druckern auszugeben.

Screenshots erlauben – Diese Option wird im AppConnect-SDK noch nicht unterstützt. Im Access Mobile Client ist Benutzern stets gestattet, Screenshots zu erstellen, sofern sie nicht durch ihre MDM-Konfiguration auf Geräteebene daran gehindert sind.

Öffnen in erlauben – Wählen Sie diese Option, wenn es Acronis Access-Benutzern gestattet sein soll, Dateien in anderen Applikationen auf dem Gerät zu öffnen. Wenn diese Option aktiviert ist, können Sie eine Liste zulässiger Apps angeben.

5.13.3.3 Zuordnen von Labels zur neuen Konfigurations- und Container-Richtlinie

Diese neuen Richtlinien können nur auf Mobilgeräte angewendet werden, wenn Sie die MobileIron-Labels für alle erforderlichen Benutzer der **Konfigurations-** und der **Container-Richtlinie** zuweisen.

5.13.4 Den Acronis Access-iOS-Client mit AppConnect aktivieren

Sobald auf der MobileIron-VSP die benötigte Konfiguration und Container-Richtlinie erstellt wurden, können Sie Acronis Access auf Client-Geräten installieren und konfigurieren.

Sicherstellen, das Mobile@Work installiert und konfiguriert wurde

Stellen Sie vor der Installation oder Aktivierung des Access Mobile Clients sicher, dass die MobileIron Mobile@Work-iOS-App https://itunes.apple.com/app/mobileiron-mobile-work-client/id320659794 auf dem Gerät installiert ist. Diese App fungiert als Kanal, über den Acronis Access mit der MobileIron-VSP kommuniziert und über den AppConnect-Konfiguration und -Befehle empfangen werden.

Nach der Installation von Mobile@Work müssen Sie die App mit Ihren Benutzerkontoinformationen und der Adresse Ihres VSP-Servers konfigurieren.

Sobald Mobile@Work installiert und konfiguriert ist, können Sie mit Acronis Access fortfahren. Es gibt drei mögliche Szenarien zum Einrichten von Acronis Access mit AppConnect:

Themen

5.13.4.1 Acronis Access wurde bereits auf dem Gerät installiert und bereits bei einem Acronis Access-Server registriert

Dieses Szenario ähnelt dem vorherigen; der einzige Unterschied besteht darin, dass die AppConnect Acronis Access-Konfiguration nicht zur automatischen Registrierung der Access Mobile Client-App verwendet wird. Wenn die Access Mobile Client-App bereits bei einem Acronis Access-Server registriert ist, wird die ursprüngliche Konfiguration beibehalten. Acronis Access wird mit AppConnect verwaltet und verwendet die Container-Richtlinie für den AppConnect-Passcode und die AppConnect-Berechtigungen. Wenn sich ein Benutzer bei einem anderen Acronis Access-Server registrieren soll, muss er Acronis Access deinstallieren und die App neu installieren. Erst danach ist eine Konfiguration über AppConnect möglich.

5.13.4.2 Acronis Access wurde bereits auf dem Gerät installiert, wurde jedoch noch nicht bei einem Acronis Access-Server registriert

In diesem Szenario wurde die Acronis Access-iOS-App möglicherweise auf einem Gerät installiert und geöffnet, bevor die Mobile@Work- und die AppConnect-VSP-Konfiguration eingerichtet wurden. Lediglich durch Starten des Access Mobile Client wird die AppConnect-Einrichtung eventuell nicht ausgelöst. In diesem Fall ist es möglich, den AppConnect-Einrichtungsprozess manuell zu starten, indem Sie das Menü 'Einstellungen'  in der Acronis Access-App öffnen, auf die MobileIron AppConnect-Option am Ende der Einstellungsliste tippen und die Schaltfläche 'Aktivieren' auswählen. Wenn die AppConnect-Einrichtung nicht sofort beginnt, lassen Sie die Acronis Access-App für einige Minuten geöffnet, damit die Einrichtung beginnen kann. Sobald der Einrichtungsvorgang beginnt, fährt er gemäß der Beschreibung des vorherigen Szenarios fort.

Wenn die Mobile@Work-App auf dem Gerät nicht vorhanden ist, zeigt Acronis Access in diesem Menü **Einstellungen** statt der Schaltfläche **Aktivieren** eine Warnung an.

5.13.4.3 Acronis Access wurde noch nicht auf dem Gerät installiert

In diesem Szenario müssen Sie Acronis Access erstmalig ьber den Apple App Store http://www.grouplogic.com/web/meappstore installieren.

Starten Sie Acronis Access nach der Installation.

Acronis Access prüft, ob eine konfigurierte Mobile@Work-App vorhanden ist, wechselt vorübergehend zur Mobile@Work-App und anschließend wieder zu Acronis Access zurück. Wenn eine gültige Acronis Access-AppConnect-Konfiguration gefunden wird, ruft Acronis Access automatisch den Registrierungsmodus auf und zeigt dem Benutzer das Access Mobile Client-Registrierungsformular an. Alle in der AppConnect-Konfiguration enthaltenen Felder werden automatisch ausgefüllt. Der Benutzer muss für gewöhnlich nur sein AD-Kennwort in das Formular eingeben und dieses einsenden. Sobald das Formular ausgefüllt ist, wird die entsprechende Acronis Access Client Management-Richtlinie auf Acronis Access angewendet, und der Benutzer kann die App verwenden.

Gibt es auf der VSP keine gültige Konfiguration für Acronis Access oder wurde die Mobile@Work-App nicht installiert oder konfiguriert, erhält der Benutzer eine Fehlermeldung, oder wenn Mobile@Work nicht installiert ist, startet Acronis Access einfach im Standardmodus ohne aktiviertes AppConnect.

5.13.5 Laufende AppConnect-Verwaltung von Access Mobile Clients

Sobald Acronis Access von AppConnect aktiv verwaltet wird, empfängt der Access Mobile Client Änderungen an der jeweiligen Container-Richtlinie, sobald er sich bei der Mobile@Work-App auf dem Gerät eincheckt. Das Intervall, mit dem dieses Einchecken erfolgt, wird auf der MobileIron-VSP festgelegt und bewirkt, dass die Acronis Access-App vorübergehend zur Mobile@Work-App wechselt, um die Prüfung durchzuführen. Der Benutzer wird hierdurch gestört. Es wird daher empfohlen, die Eincheck-Intervalle auf einen langfristigen Zeitraum einzustellen, damit diese die Verwendung der App nicht allzu häufig stören.

Änderungen an der Container-Richtlinie, die Entziehung des Zugriffs auf Acronis Access usw. werden beim nächsten Einchecken der App auf diese angewendet.

5.13.6 Verwenden von AppConnect mit der eingeschränkten Kerberos-Delegierung

Dieser Artikel erläutert die Vorgehensweise bei der Konfiguration der erforderlichen Systemkomponenten, um den mobilen Client von Acronis Access mit dem Acronis Access Server zu verbinden, der für den MobileIron AppTunnel als Proxy fungiert, mit einer Authentifizierung durch die eingeschränkte Kerberos-Delegierung.

Hinweis: *Die Dokumentation der Vorgehensweise bei der Konfiguration von MobileIron für die eingeschränkte Kerberos-Delegierung wird freundlicherweise als Unterstützung beim Einrichten der Konfiguration bereitgestellt. Alle Schritte bis hin zu der Überprüfung, ob Sentry das Kerberos-Ticket von KDC erhält, betreffen jedoch ausschließlich die MobileIron-Software. Wenn Sie bei der Befolgung dieser Schritte und dem Empfang eines Kerberos-Tickets auf Probleme stoßen, wenden Sie sich bitte an den Support von* ***MobileIron****.*

Da dies ein komplexes Setup ist, wird es zum Verringern von Fehlern und zum Vereinfachen der Fehlerbehebung in zwei Phasen unterteilt. Bei der ersten Phase wird per Benutzername/Kennwort zur Authentifizierung am Acronis Access Server ein AppTunnel eingerichtet. Auf diese Infrastruktur wird in der zweiten Phase aufgebaut, um eine eingeschränkte Kerberos-Delegierung hinzuzufügen. Es wird unbedingt empfohlen, die Funktion des Tunnels per Benutzername/Kennwort zur Authentifizierung zu testen, bevor Sie mit Kerberos fortfahren, um die Schritte bei der Problembehandlung zu reduzieren.

Vor Beginn

- Mit der eingeschränkten Kerberos-Delegierung (Kerberos Constrained Delegation, KCD) können sich Benutzer mit Kerberos bei Netzwerkressourcen authentifizieren, nachdem ihre Identität mit einer anderen Authentifizierungsmethode als der von Kerberos bestimmt worden ist. Bei Acronis Access können Benutzer damit die Authentifizierung unter Verwendung von Identitätszertifikaten, die von MobilIron vergeben werden, auf iOS Geräteebene durchführen. Ohne KCD könnte die Access-App nur ein direkt in der App installiertes Zertifikat verwenden.

  Hinweis: *Die gesamte Konfiguration bezüglich der KCD erfolgt über MobileIron und Windows. In Acronis Access selbst sind keine speziellen Änderungen vorzunehmen.*

- Key Distribution Center (KDC) ist ein Netzwerkdienst, der Benutzern und Computern innerhalb einer Active Directory-Domäne Sitzungstickets und temporäre Sitzungsschlüssel zur Verfügung stellt.
- Nur der Gateway Server akzeptiert eine Kerberos-Authentifizierung. Der Access Server jedoch nicht.
  - Die Access Client-Applikation muss im Client Management mit einem Gateway Server registriert sein. Wenn der Client beim Access Server registriert ist, schlägt die Anmeldung fehl.
  - Mobile Clients, die eine Kerberos-Authentifizierung verwenden, können sich nur bei Netzwerkfreigaben und SharePoint-Sites authentifizieren. Sie können KCD nicht für den Zugriff auf die Ordner von Acronis Access Sync & Share verwenden, da der Access-Dienst keine Kerberos-Authentifizierung zulässt.

Voraussetzungen

Die folgende Software muss installiert und konfiguriert sein:

- MobileIron VSP (in diesem Dokument wird auf Version 5.9 Bezug genommen)
- Für eine ordnungsgemäße Funktion von Kerberos müssen die Benutzerkonten auf dem VSP aus dem Active Directory stammen, das zur Unterstützung von Kerberos konfiguriert wird.
- MobileIron Sentry (in diesem Dokument wird auf Version 4.8 Bezug genommen)
- Installierter Access Server (in diesem Dokument wird auf Version 6.0.2 Bezug genommen)
- Serverinteroperabilität
  - Die Uhrzeit auf den VSP-, Sentry-, Domain Controller- und Access-Servern muss synchronisiert sein (NTP empfohlen).
  - Domänennamenauflösung (DNS). Sentry fordert ein Ticket vom KDC mithilfe des DNS-Namen an, der für den Kontakt konfiguriert ist. Dieser Name muss mit dem Computernamen übereinstimmen, der für die Kerberos-Delegierung eingerichtet wurde; ansonsten lehnt KDC die Ausgabe eines Tickets ab.
  - Der VSP muss in der Lage sein, auf Sentry zuzugreifen (standardmäßig über die Ports 9090 und 443 – weitere je nach Ihrer Konfiguration).
  - Sentry muss in der Lage sein, auf das Active Directory und den Access Server zuzugreifen (über die Ports 88, 389, 636).
  - Die Ports 88 (UDP und TCP) und 389 (TCP) zwischen Active Directory und Sentry (oder Port 636 (TCP), wenn Sie ein SSL-aktiviertes Active Directory verwenden) müssen für den Datenverkehr geöffnet sein. Port 88 wird zur Kommunikation mit dem Kerberos-Protokoll verwendet. Port 389 (oder 636) wird für das LDAP-Ping zwischen Sentry und KDC verwendet, um zu überprüfen, ob die KDC-IP mit der Active Directory-IP identisch ist.
  - Bei Verwendung von Windows Server 2003 kann der KDC auf Anforderungen am Port 88 unter Verwendung von UDP anstatt von TCP warten. Sie können erzwingen, dass Kerberos TCP statt UDP verwendet, indem Sie im Registry-Editor die MaxPacketSize von 0 in 1 ändern. Weitere Informationen zur korrekten Vorgehensweise finden Sie im folgenden Microsoft KB-Artikel: http://support.microsoft.com/kb/244474 http://support.microsoft.com/kb/244474.
- Das iOS-Gerät muss in der Lage sein, eine Verbindung mit VSP und Sentry herzustellen.
- Auf VSP registriertes iOS -Gerät.

- Mobile@Work ist auf dem Gerät installiert und auf VSP registriert. Die MDM-Profile wurden während der Registrierung ordnungsgemäß installiert.

Themen

6 Konfigurieren eines AppConnect-Tunnels zwischen dem Access Mobile Client und dem Access Server durch Authentifizierung per Benutzername/Kennwort

Der erste Schritt beim Konfigurieren eines AppConnect-Tunnels zwischen dem Access Mobile Client und dem Acronis Access Server ist das Hinzufügen und Konfigurieren einer Sentry zum VSP. Dies ist ein mehrere Schritte umfassender Prozess. Diese einzelnen Phasen sind nachstehend aufgeführt.

- Eine neue lokale Zertifizierungsstelle (CA) erstellen
- Ein neues SCEP erstellen
- Sentry hinzufügen und konfigurieren
- Konfigurieren von Acronis Access auf dem VSP

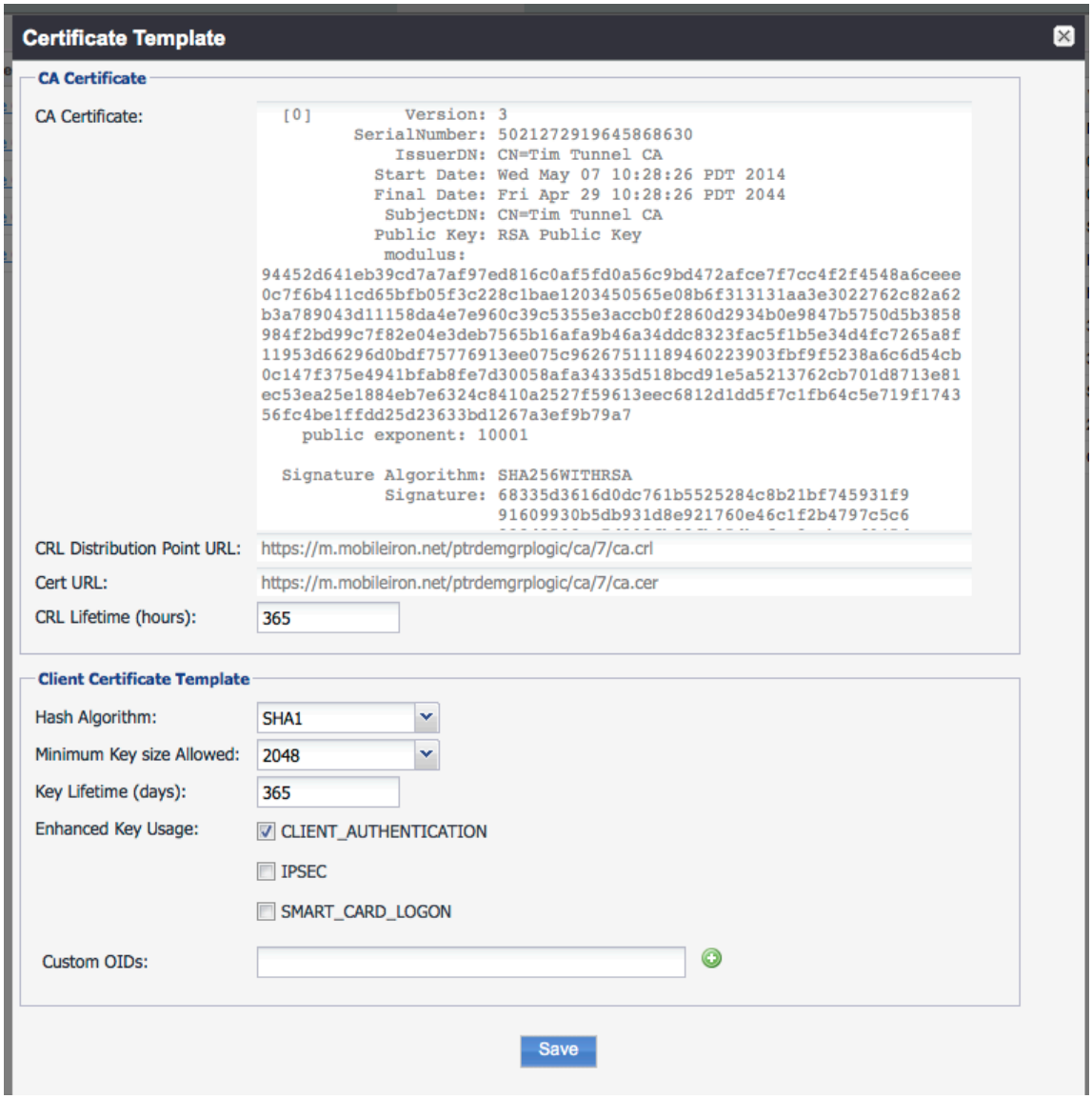
Sie können eine anderen Zertifizierungsstelle (CA) und einen anderen Anbieter des einfachen Zertifizierungsprotokolls (SCEP) haben, aber diese Anleitung geht zur Vollständigkeit davon aus, dass dies nicht der Fall ist. Zu Fragen bezüglich der Konfigurierung einer CA und eines SCEP von Drittanbietern lesen Sie die MobileIron-Dokumentation.

Themen

1. Öffnen Sie das Admin-Portal von MobileIron VSP.
2. Wählen Sie **Einstellungen**, und öffnen Sie **Lokale CA**.
3. Klicken Sie auf **Neue hinzufügen**, und wählen Sie **Selbstsigniertes Zertifikat erstellen**.

- **Name der lokalen CA:** Geben Sie den gewünschten Namen ein.
- **Schlüssellänge**: Wählen Sie **2048**.
- **Ausstellername:** Geben Sie den gewünschten Namen ein; er muss jedoch mit **CN=** beginnen.

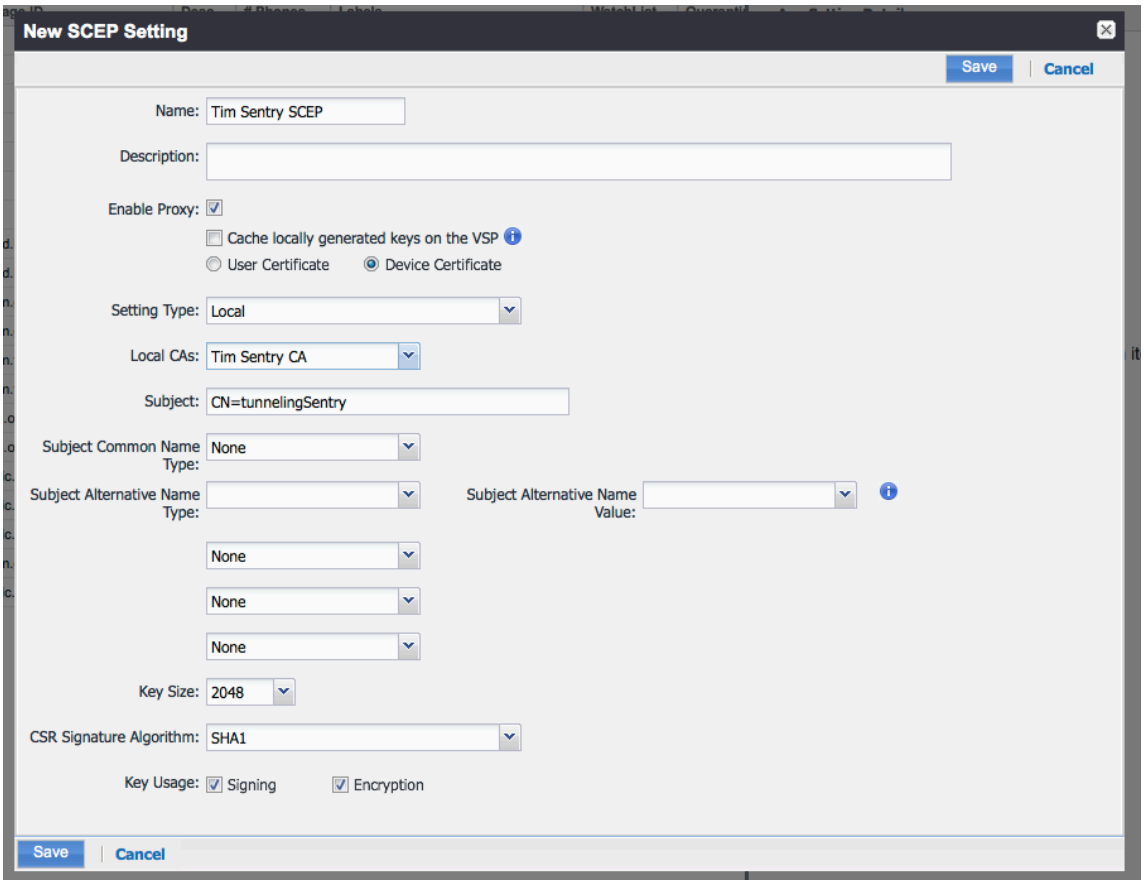
4. Klicken Sie auf **Erstellen**.



5. Klicken Sie dann auf **Speichern**.
6. Klicken Sie auf der neuen CA auf **Zertifikat anzeigen**.
7. Kopieren Sie das Zertifikat in eine neue Textdatei, und speichern Sie diese auf dem Desktop.

1. Öffnen Sie das Admin-Portal von MobileIron VSP.
2. Wählen Sie **Richtlinien und Konfigurationen**, und öffnen Sie **Konfigurationen**.

3. Drücken Sie auf **Neue hinzufügen**, und wählen Sie **SCEP**.

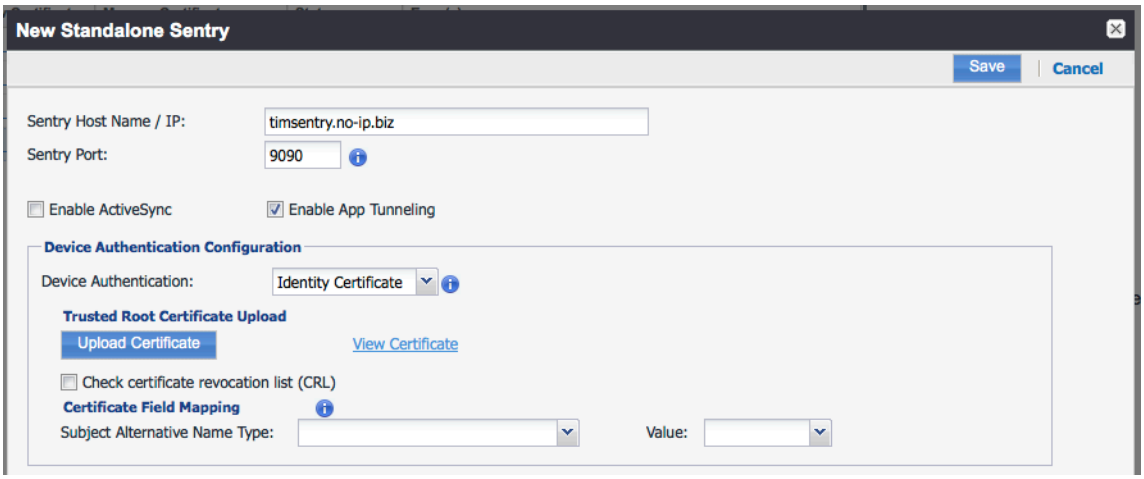


- **Name**: Geben Sie den gewünschten Namen ein.
- **Einstellungstyp**: Wählen Sie **Lokal**.
- **Lokale CA**: Name der unter 'Eine neue lokale Zertifizierungsstelle (CA) erstellen' erstellte CA.
- **Betreff**: Geben Sie den gewünschten Namen ein (z. B. CN=tunneling); er muss jedoch mit **CN=** beginnen.
- **Schlüsselgröße**: Wählen Sie den gleichen Wert, den Sie bei der Erstellung der CA ausgewählt haben. Wählen Sie in diesem Fall **2048**.

4. Klicken Sie auf **Speichern**.

1. Während Sie sich noch im Admin-Portal von MobileIron VSP befinden, wählen Sie **Einstellungen** und öffnen Sie **Sentry**.

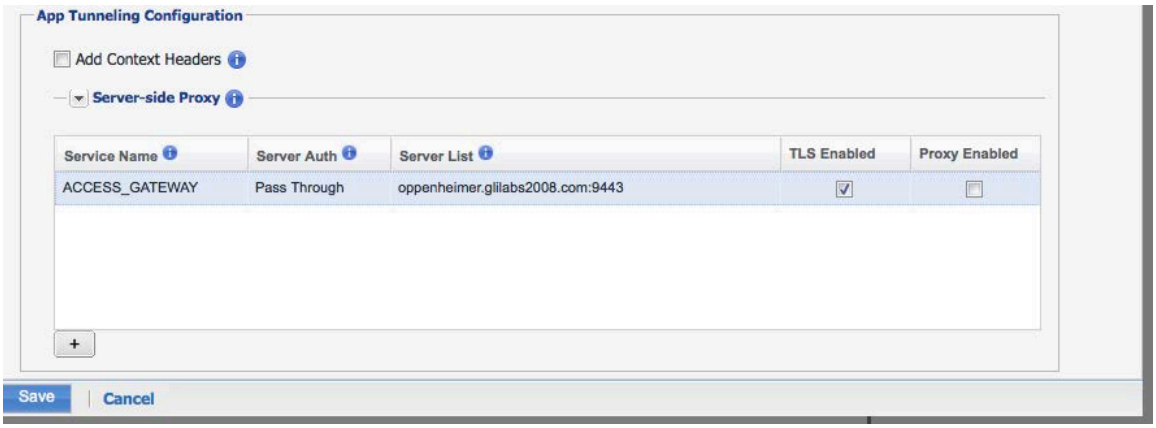
2. Drücken Sie auf **Neue hinzufügen**, und wählen Sie **Standalone-Sentry**.



- **Hostname/IP der Sentry**: Der DNS-Name Ihrer Sentry wurde installiert. Auf ihn muss über den MobileIron VSP zugegriffen werden können.
- **Sentry-Port**: Der Port, der für eine Verbindung per MobileIron VSP geöffnet ist (Standardeinstellung ist 9090).
- **AppTunneling aktivieren**: Aktivieren Sie das Kontrollkästchen.
- **Geräte-Authentifizierung**: Wählen Sie **Identitätszertifikat**.

3. Klicken Sie auf **Zertifikat hochladen**.
4. Suchen und wählen Sie die Textdatei, die Sie unter 'Eine neue lokale Zertifizierungsstelle (CA) erstellen' auf dem Desktop gespeichert haben.
5. Klicken Sie auf **Zertifikat hochladen**.

In diesem Abschnitt richten Sie die Dienste ein, die den Acronis Access Gateway Servern zugeordnet werden. Der Management-Server unterstützt nicht die eingeschränkte Kerberos-Delegierung, aber Sie können sich mithilfe des Gateway registrieren, das auf der gleichen Maschine installiert ist wie der Management-Server. Das heißt, die Konfiguration, die zur Unterstützung der Registrierung per eingeschränkter Kerberos-Delegierung verwendet werden sollte.



- **Dienst-Name**: Geben Sie den gewünschten Namen ein.

- **Server-Auth.**: Wählen Sie **Passthrough**. Dies wird zu einem späteren Zeitpunkt in dieser Anleitung geändert.
- **Serverliste**: Durch Semikolon getrennte Liste der Server. Für dieses Dokument verwenden wir einen einzelnen Server. Dies ist die DNS-Adresse des Access Gateway Servers und der Port, den er abhört.
- **TLS aktiviert**: Aktivieren Sie das Kontrollkästchen.

Klicken Sie auf **Speichern**.

Klicken Sie auf dem neuen Sentry-Eintrag auf '**Zertifikat anzeigen**'. Damit wird die Verbindung zwischen VSP und Sentry getestet. Wenn Sie das Zertifikat nicht erhalten, prüfen Sie die Verbindungen und Ports zwischen VSP und Sentry. Fahren Sie erst fort, wenn dies einwandfrei funktioniert.

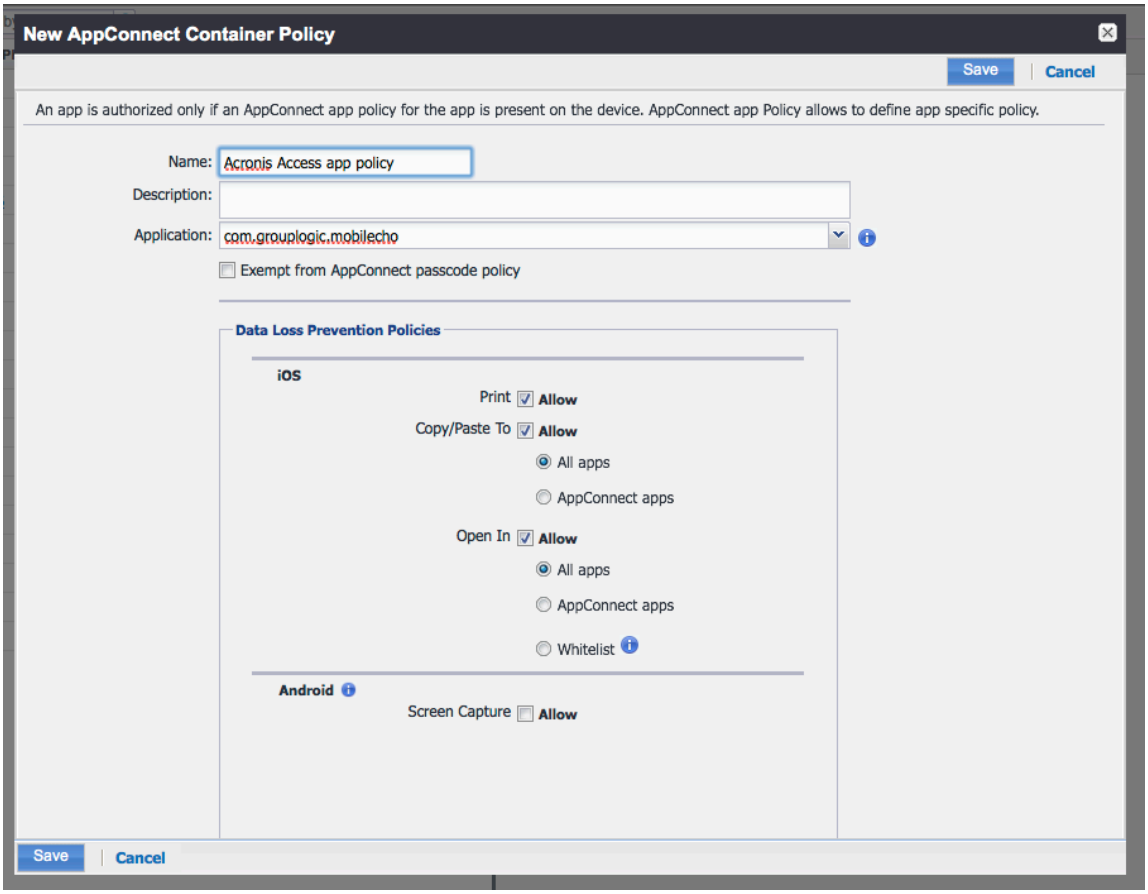
Konfigurieren von Acronis Access auf dem VSP

Sobald Sentry eingerichtet ist, müssen die App-Richtlinie und die App-Konfiguration für Acronis Access erstellt werden. Dies ist ein mehrere Schritte umfassender Prozess. Diese Schritte sind nachstehend aufgeführt.

Themen

1. Wählen Sie noch innerhalb des Admin-Portals von MobileIron VSP **Richtlinien und Konfigurationen**, und öffnen Sie **Konfigurationen**.

2. Klicken Sie auf **Neue hinzufügen**, wählen Sie **AppConnect** und **Container-Richtlinie**.

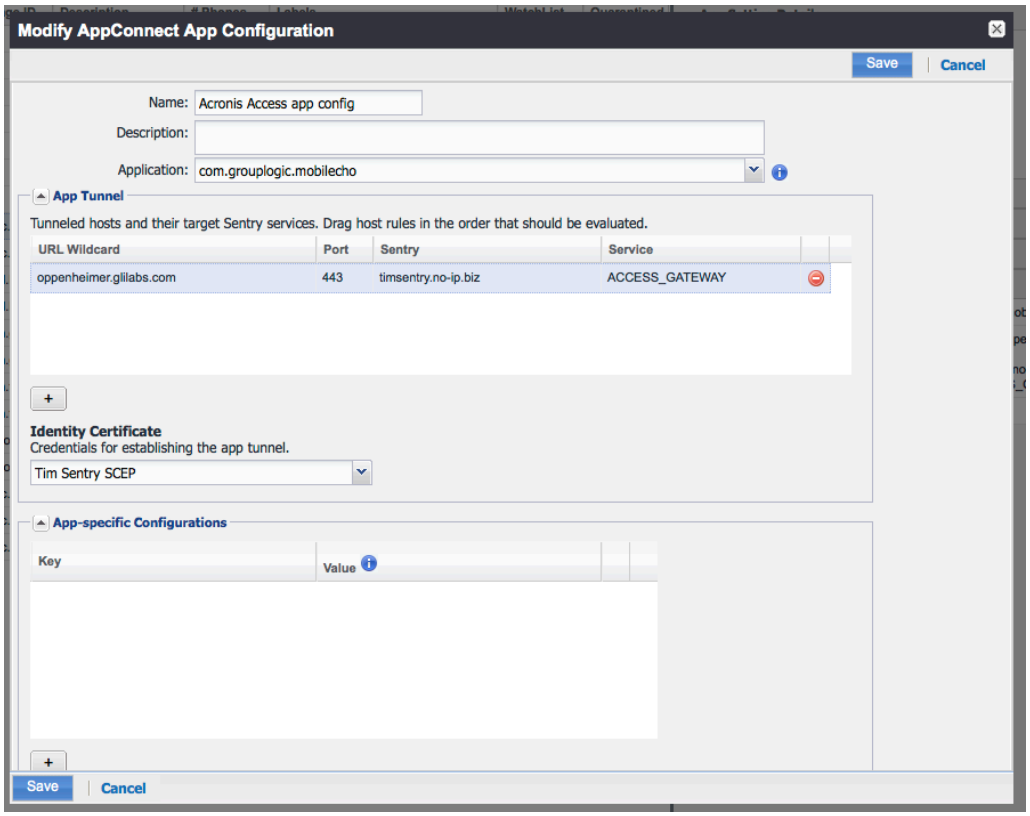


- **Name**: Geben Sie den gewünschten Namen ein.
- **Anwendung**: Geben Sie **com.grouplogic.mobilecho** ein. Dies ist eine Bundle-ID vom iOS App Store.
- **Richtlinien**: Legen Sie die Richtlinien von MobileIron, die zur Verwaltung von Acronis Access verwendet werden sollen, nach eigener Wahl fest.

3. Klicken Sie auf **Speichern**.

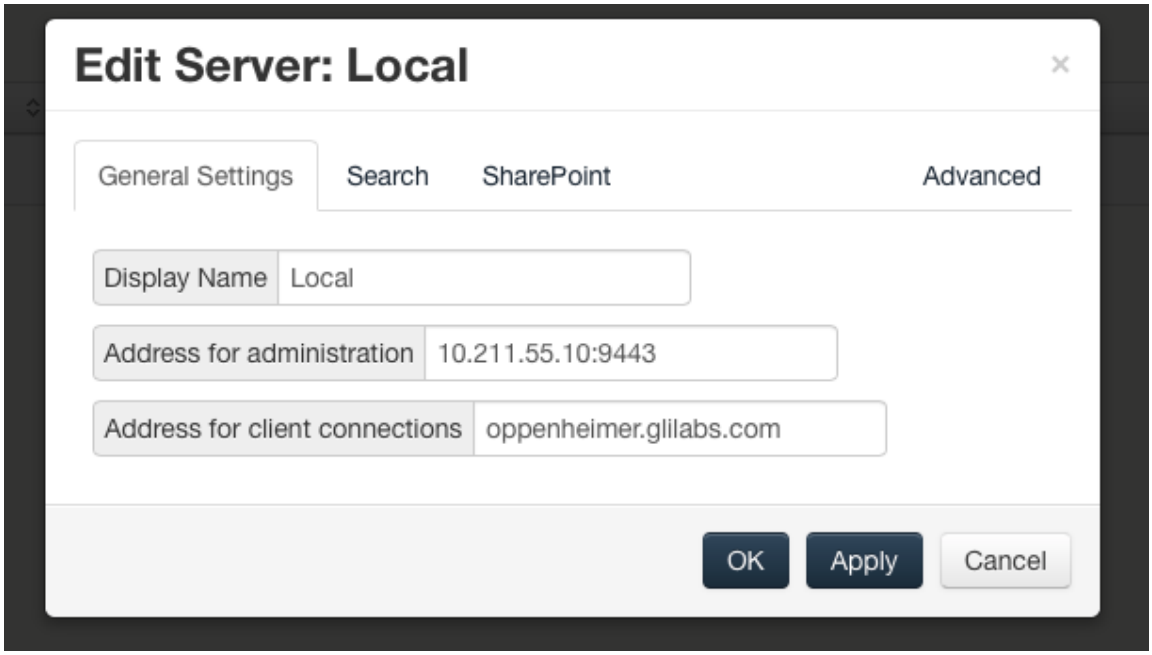
1. Wählen Sie noch innerhalb des Admin-Portals von MobileIron VSP **Richtlinien und Konfigurationen**, und öffnen Sie **Konfigurationen**.

2. Drücken Sie auf **Neue hinzufügen**, wählen Sie **AppConnect** und **Konfiguration**.

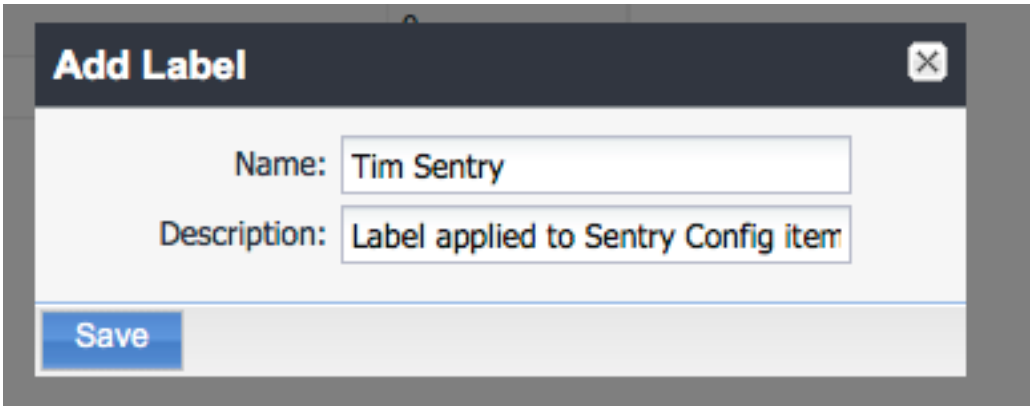


- **Name**: Geben Sie den gewünschten Namen ein.
- **Applikation**: Geben Sie com.grouplogic.mobilecho ein. Dies ist die Bundle-ID aus dem Apple Store.
- **AppTunnel**
  - **URL-Platzhalter**: Die URL, die der Client für den Verbindungsaufbau mit dem Acronis Access Gateway Server verwendet. Die für den Gateway Server in der Acronis Access-Administratoroberfläche konfigurierte 'Adresse für Client-Verbindungen' muss übereinstimmen. Dies kann ein gewöhnlicher Ausdruck sein, um mehrere Gateways abzugleichen. Für dieses Dokument geben wir jedoch den genauen Hostnamen ein.*
  - **Port**: Der Port, den der Client für den Verbindungsaufbau verwendet (Standardeinstellung: 443).
  - **Sentry**: Die unter 'Sentry hinzufügen und konfigurieren' erstellte Sentry.
  - **Dienst**: Der unter 'Sentry hinzufügen und konfigurieren' für das Gateway konfigurierte Dienst.
  - **Identitätszertifikat**: Das in 'Ein neues SCEP erstellen' erstellte SCEP.
3. Klicken Sie auf **Speichern**.

*Adresse für die Client-Verbindungen von der Acronis Access-Weboberfläche. Die Adresse wird in den Profilen verwendet, die an den mobilen Client gesandt werden, um Verbindungen mit dem Dateisystem herzustellen. Der **URL-Platzhalter** der Sentry muss mit dieser Adresse und dem Port übereinstimmen, um diese Verbindungen bis zur Sentry weiterzuleiten.



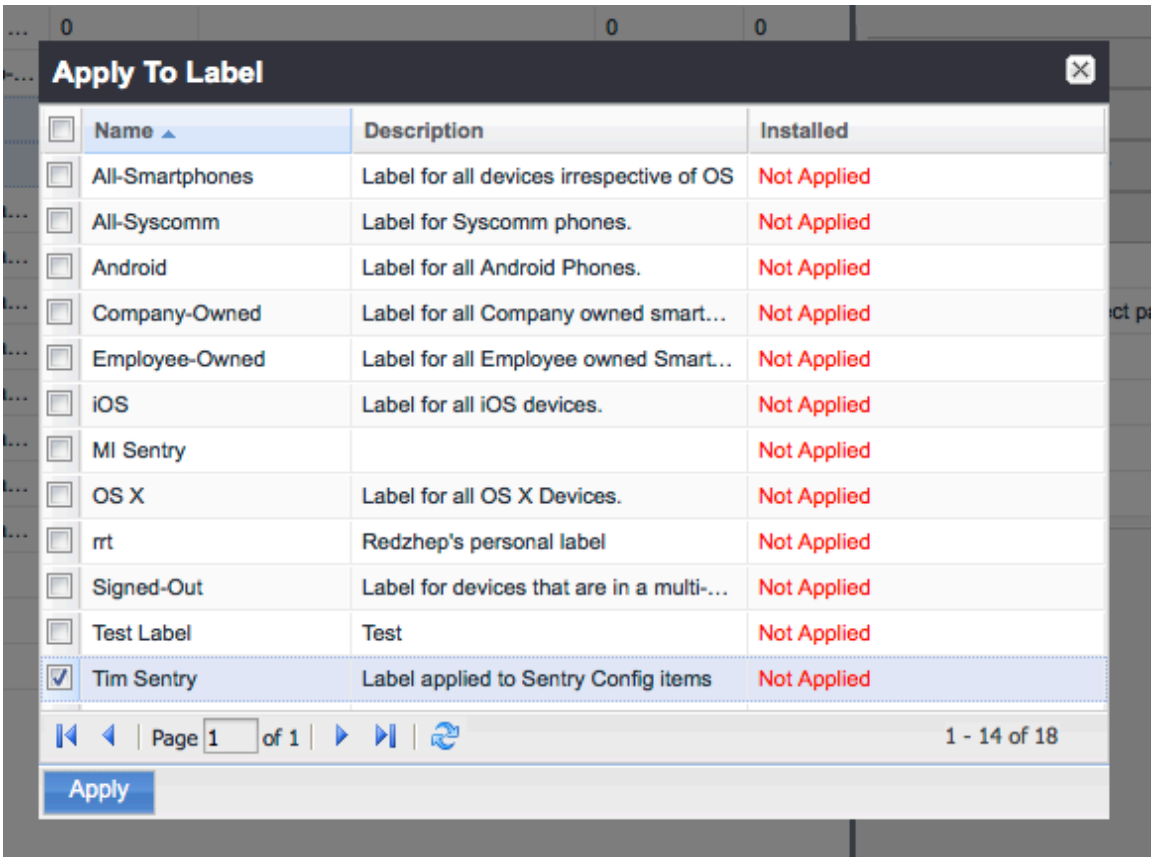
1. Wählen Sie noch innerhalb des Admin-Portals von MobileIron VSP **Benutzer und Geräte** und öffnen Sie **Label**.
2. Drücken Sie auf **Neues hinzufügen**.



   - **Name**: Geben Sie den gewünschten Namen ein.
   - **Beschreibung**: Geben Sie eine Beschreibung nach eigener Wahl ein.
3. Klicken Sie auf **Speichern**.

1. Während Sie sich noch im Admin-Portal von MobileIron VSP befinden, wählen Sie die Option **Richtlinien und Konfigurationen**.

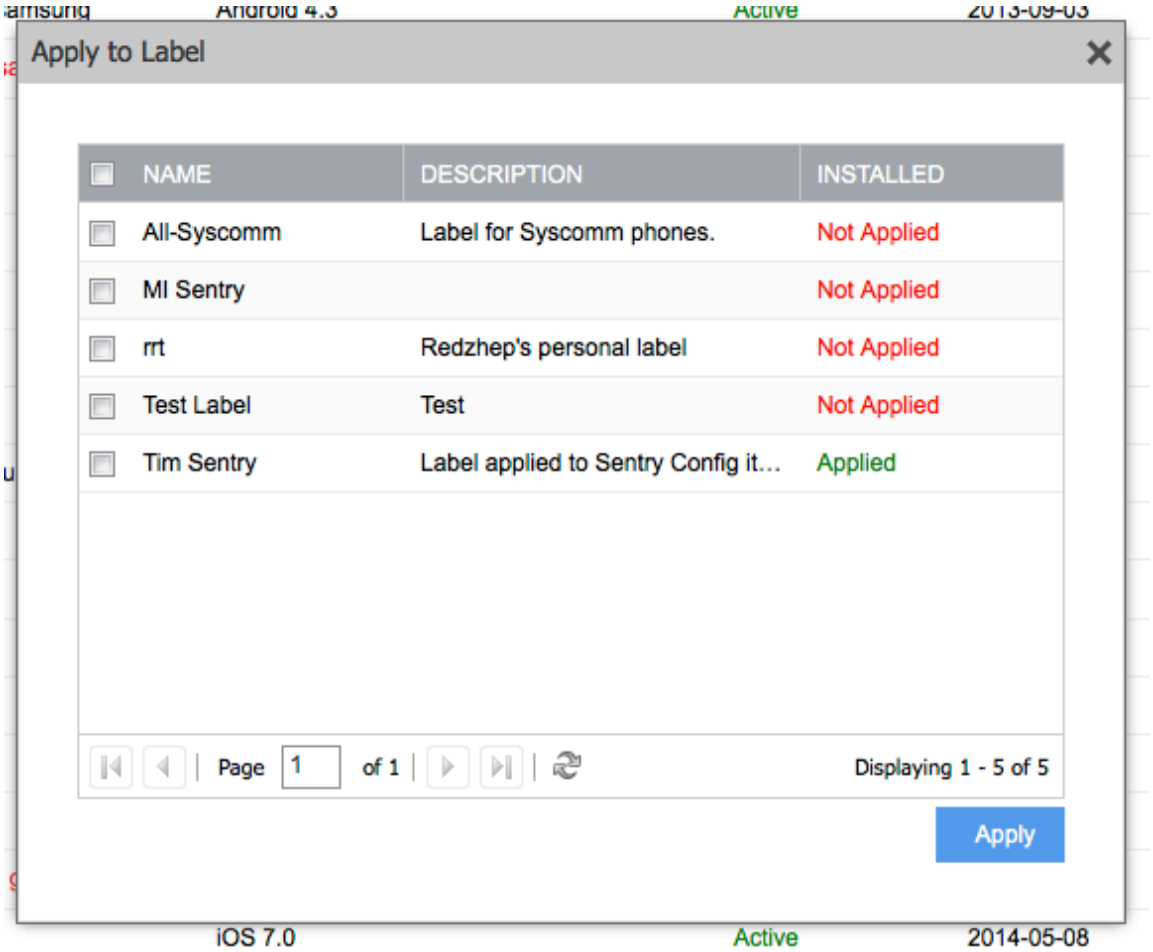
2. Markieren Sie die von Ihnen gemäß diesem Dokument erstellten SCEP, AppConnect-Richtlinien und AppConnection-Konfigurationen. Öffnen Sie **Konfigurationen,** um diese anzuzeigen.



3. Drücken Sie auf **Weitere Aktionen**, und wählen Sie **Für Label übernehmen**.
4. Markieren Sie das in 'Ein neues Label erstellen' erstellte Label.
5. Klicken Sie auf **Übernehmen**.

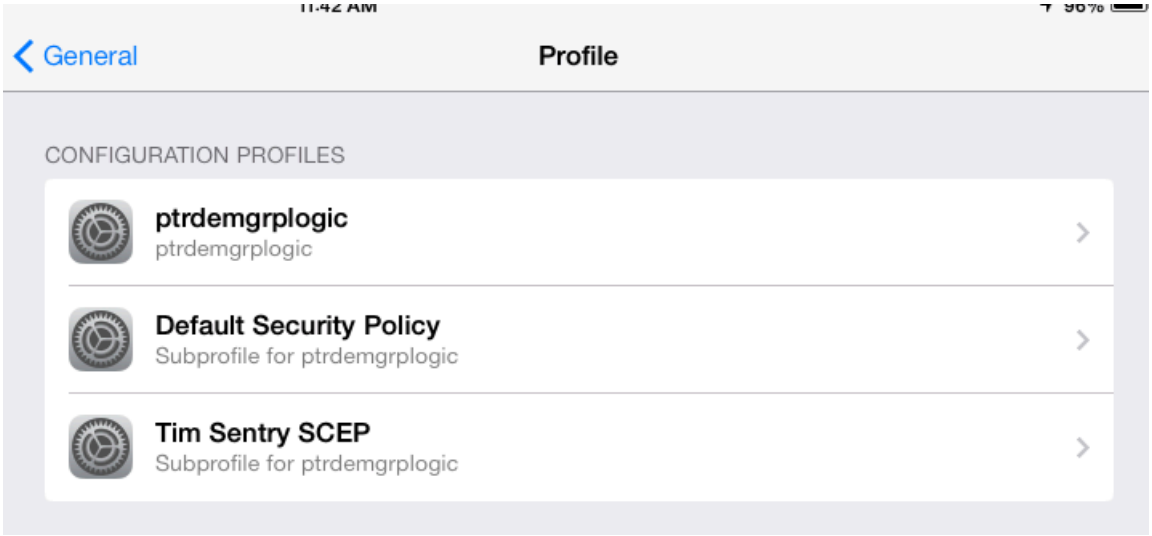
1. Während Sie sich noch im Admin-Portal von MobileIron VSP befinden, wählen Sie **Benutzer und Geräte**, und öffnen Sie **Geräte**.

2. Markieren Sie das für den Sentry-Test zu verwendende iOS-Gerät.

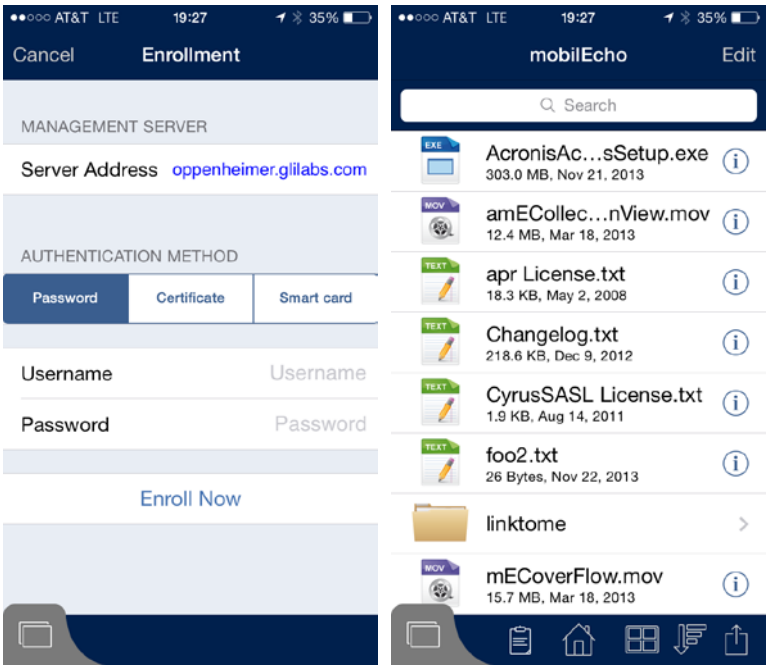


3. Wählen Sie **Aktionen** -> **Für Label übernehmen**.
4. Markieren Sie das in 'Ein neues Label erstellen' erstellte Label.
5. Klicken Sie auf **Übernehmen**.
1. Öffnen Sie die App Mobile@Work, und rufen Sie die **Einstellungen** auf.
2. Tippen Sie auf 'Automatisch auf Updates prüfen'.

3. Tippen Sie auf **Einchecken des Geräts erzwingen**. Wenn dies erfolgreich ist, sollte das in diesem Dokument konfigurierte SCEP in den Geräteeinstellungen unter **Einstellungen** -> **Allgemein** -> **Profile** angezeigt werden.



4. Installieren Sie Acronis Access vom App Store, und starten Sie es.
5. Wählen Sie in der Ansicht 'Willkommen' die Option **Jetzt registrieren**, oder gehen Sie zu **Einstellungen**, und blättern Sie nach unten zu **Registrierung**.



6. Geben Sie die für die Client-Verbindungen mit dem Acronis Access Gateway verwendete und in der **AppConnection-Konfiguration** konfigurierte Adresse ein. Für einen echten Test sollte der mobile Client mit dieser URL keine Verbindung aufbauen können (Mobilfunk oder ein externes Netz verwenden).
7. Tippen Sie auf **Weiter**.
8. Geben Sie **Benutzername** und **Kennwort** ein, und tippen Sie auf **Jetzt registrieren**.

Sie sollten nun die Meldung 'Sie sind jetzt für das Acronis Access Client Management registriert.' sehen.

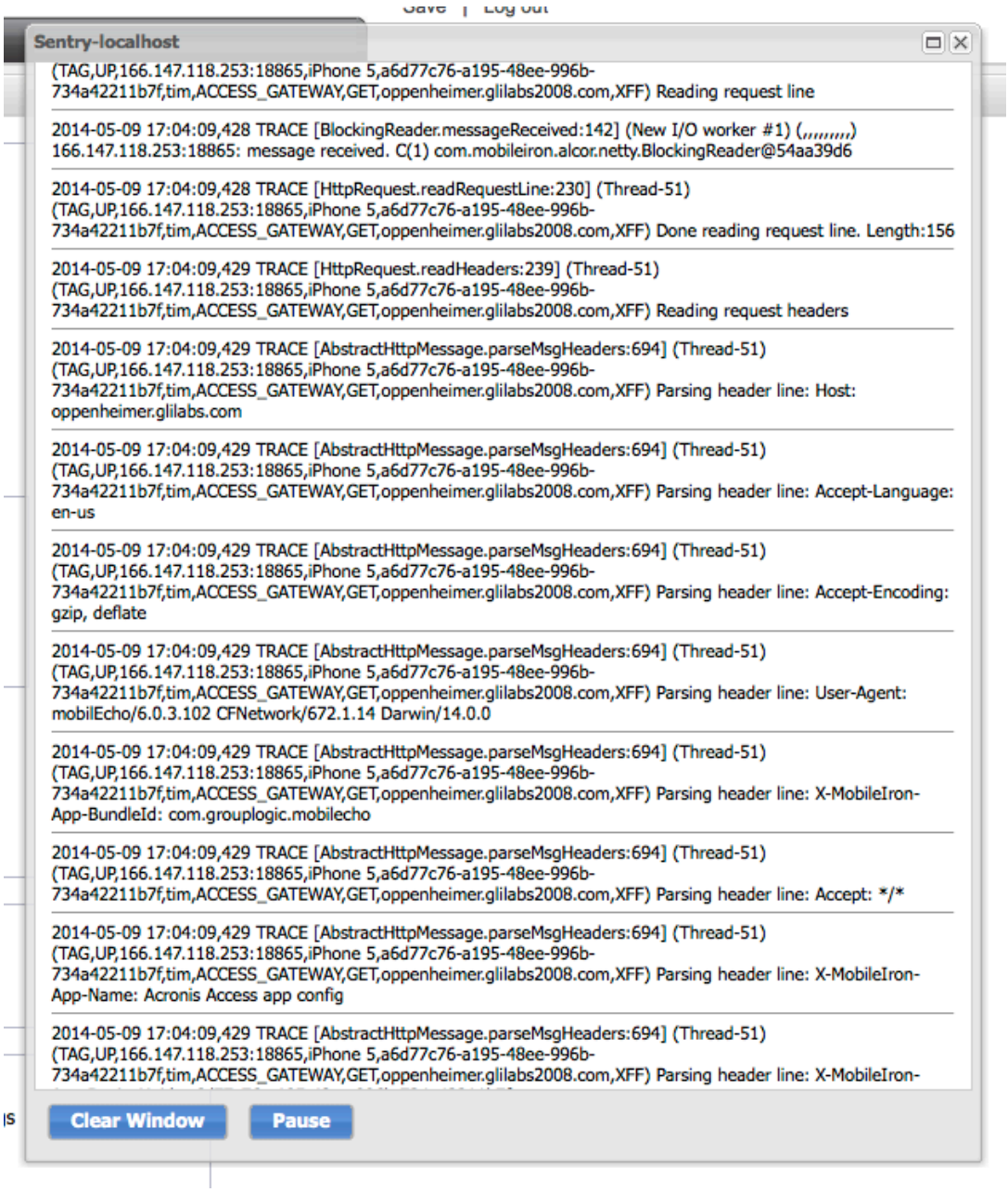
Wenn die Datenquellen in Ihrem Profil alle Bestandteil des Acronis Access Gateway sind, das für eine Weiterleitung durch Sentry konfiguriert wurde, sollten Sie in der Lage sein, diese Quellen an diesem Punkt mithilfe des AppTunnel zu durchsuchen.

Nutzung des AppTunnel überprüfen

Sie können überprüfen, ob dieser Datenverkehr durch AppTunnel erfolgt, indem Sie sich beim Sentry-Dienst-Manager von MobileIron anmelden.

1. Wählen Sie 'Fehlerbehebung', und öffnen Sie **Protokolle**.
2. Prüfen Sie **Sentry**, **An/Vom Gerät**, **An/Vom Dienst** und **Stufe 4**.
3. Wählen Sie **Übernehmen**.
4. Wählen Sie unter "**Modulprotokolle anzeigen**" die Option **Sentry**.

5. Wenn vom Mobilgerät Datenverkehr ankommt, sollten beim Scrollen des Sentry-Protokolls Einträge bezüglich des Hostnamens konfiguriert sein.



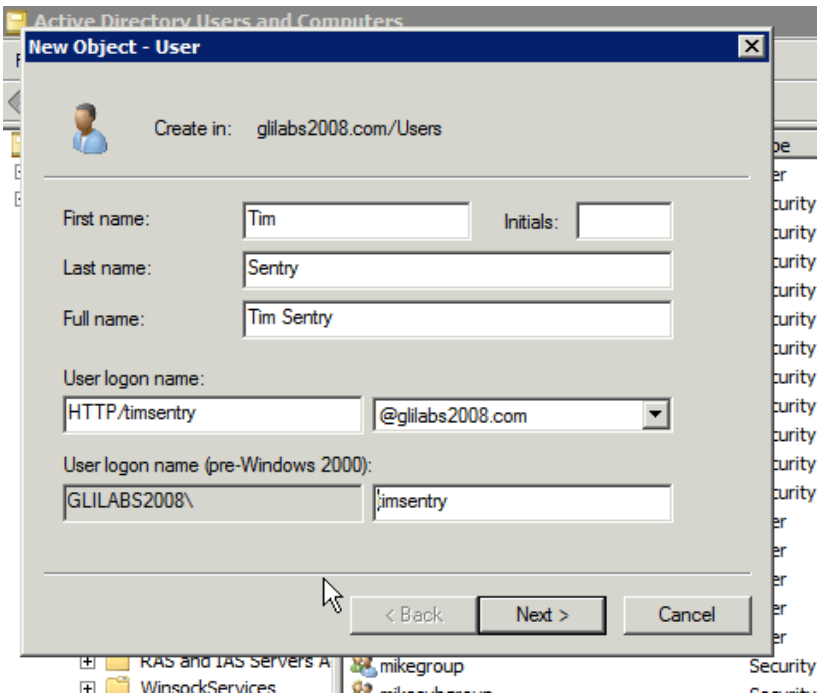
7 Hinzufügen der Authentifizierung per eingeschränkter Kerberos-Delegierung

Sobald Sie AppTunnel eingerichtet und überprüft haben, dass die Authentifizierung per Benutzername/Kennwort für Acronis Access funktioniert, können Sie die erstellten Konfigurationen so ändern, dass die Authentifizierung per eingeschränkter Kerberos-Delegierung beim Acronis Access Gateway zulässig ist. Sobald dies ordnungsgemäß konfiguriert worden ist, muss der Benutzer bei der Registrierung in der Verwaltung oder beim Durchsuchen von Daten nicht mehr Benutzername oder Kennwort angeben.

Dieses Dokument richtet die grundlegende Konfiguration ein und wird an einen Acronis Access Gateway Server delegiert, der auf dem gleichen Server wie der Management-Server ausgeführt wird, um eine Registrierung bei diesem lokalen Management-Server zuzulassen und die auf diesem Gateway konfigurierten Datenquellen zu durchsuchen. Für zusätzliche Gateways, SharePoint-Server und erneute Freigaben ist eine zusätzliche Delegierung erforderlich.

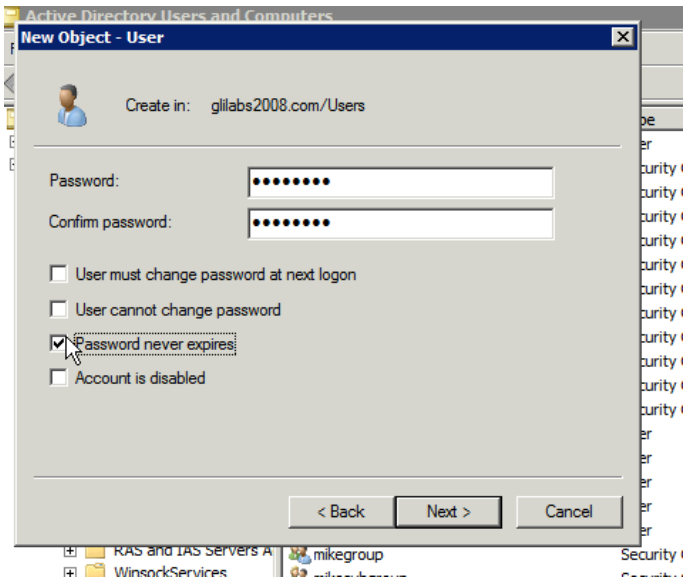
Wenn Sie das gleiche iOS-Gerät zum Testen der eingeschränkten Kerberos-Delegierung verwenden, wird empfohlen, dass Sie diese Mal den Acronis Access Mobile Client deinstallieren.

1. Melden Sie sich an Ihrem KDC-Server als Administrator an.
2. Wählen Sie im Windows-Startmenü **Alle Programme**, und wählen Sie **Verwaltung** > **Active Directory-Benutzer und -Computer**.
3. Erweitern Sie in der neu geöffneten Konsole den Bereich (in Kerberos die Bezeichnung für Domäne).
4. Klicken Sie mit der rechten Maustaste auf **Benutzer**, und wählen Sie **Neu** > **Benutzer**.



- Geben Sie einen **Namen** und einen **Benutzeranmeldenamen** für das Kerberos-Dienstkonto an. Der Name muss mit **HTTP/** beginnen. Verwenden Sie standardmäßige alphanumerische Zeichen ohne Leerzeichen für den **Benutzeranmeldenamen**, da er später in der Anleitung in eine Eingabeaufforderung eingegeben wird. Wenn **HTTP/** automatisch neben dem Feld **Benutzeranmeldename (älter als Windows 2000)** angezeigt wird, löschen Sie es aus diesem Feld.
- Vergewissern Sie sich, dass der korrekte Domänen-Name im Feld neben dem Feld **Benutzeranmeldename** ausgewählt wurde. Wenn nicht der korrekte Domänen-Name ausgewählt ist, wählen Sie den korrekten Domänen-Namen aus der Dropdown-Liste neben dem Feld **Benutzeranmeldename** aus.

5. Klicken Sie auf **Weiter**.



- **Kennwort**: Geben Sie das Kennwort ein.
- **Kennwort läuft nie ab**: Stellen Sie sicher, dass 'Benutzer muss Kennwort bei der nächsten Anmeldung ändern.' nicht ausgewählt ist. Bei der Enterprise-Bereitstellung dürfen die Felder **Benutzer kann Kennwort nicht ändern** und **Kennwort läuft nie ab** nicht ausgewählt sein.

6. Klicken Sie auf **Weiter**.
7. Klicken Sie auf **Fertig stellen**.

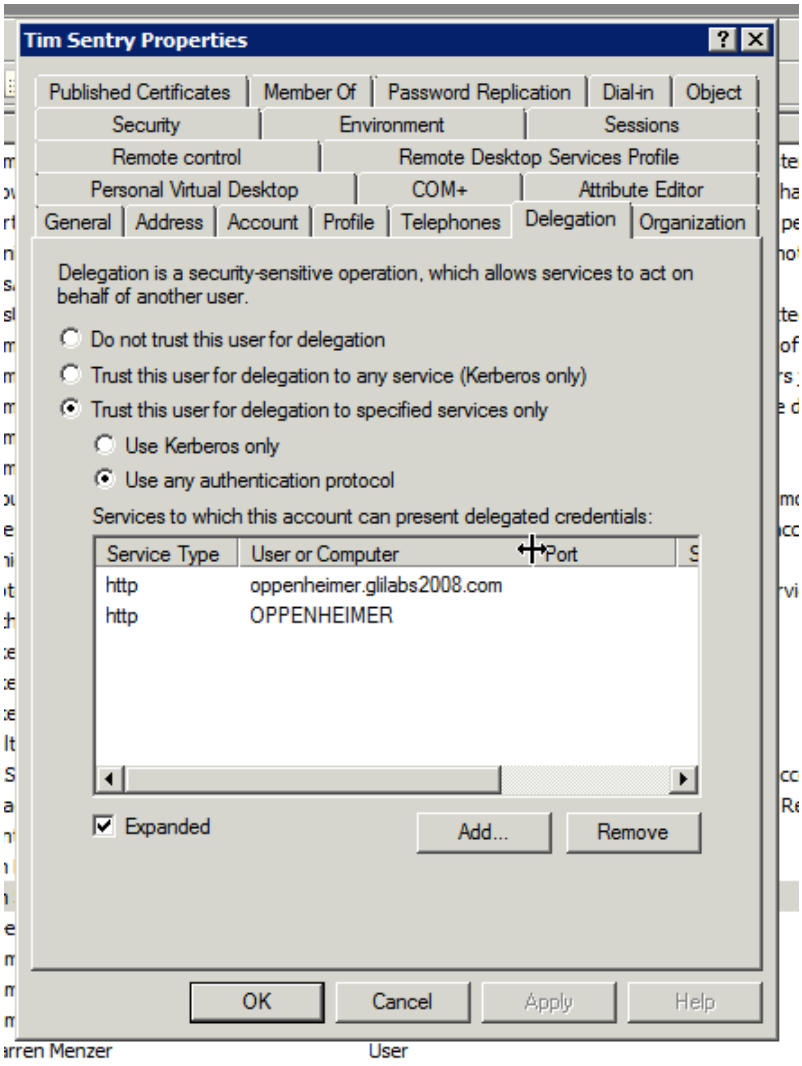
Wenn Sie eine Keytab erstellen, wird das Sentry-Dienstkonto gleichzeitig zum **DienstPrinzipalnamen** zugeordnet.

1. Öffnen Sie auf dem KDC-Server ein Fenster mit einer Eingabeaufforderung.
2. Geben Sie bei der Eingabeaufforderung den folgenden Befehl ein: **ktpass /out nameofsentry.keytab /mapuser nameofuser@domain /princ HTTP/nameofuser /pass password**

```
E.g. ktpass /out timsentry.keytab /mapuser timsentry@glilabs2008.com /princ
HTTP/timsentry@glilabs2008.com /pass 123456
```

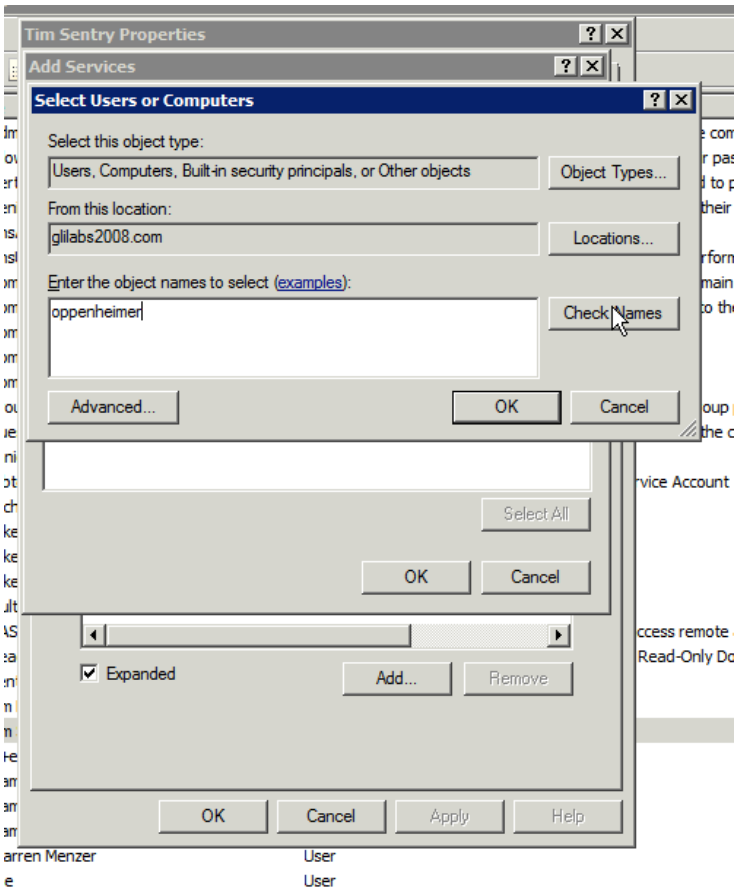
Diese Warnung kann ignoriert werden.

1. Wählen Sie im Windows-Startmenü **Alle Programme**, und öffnen Sie **Verwaltung** > **Active Directory-Benutzer und -Computer**.
2. Erweitern Sie in der neu geöffneten Konsole den Bereich (Domäne).
3. Klicken Sie auf **Benutzer**.
4. Suchen und wählen Sie das Kerberos-Benutzerkonto, das Sie unter "Ein Kerberos-Dienstkonto erstellen" erstellt haben.
5. Klicken Sie mit der rechten Maustaste auf das Konto, und wählen Sie **Eigenschaften**.
   - Klicken Sie auf die Registerkarte **Delegierung**.
   - Wählen Sie **Benutzer bei Delegierungen angegebener Dienste vertrauen**.
   - Wählen Sie **Beliebiges Authentifizierungsprotokoll verwenden**.



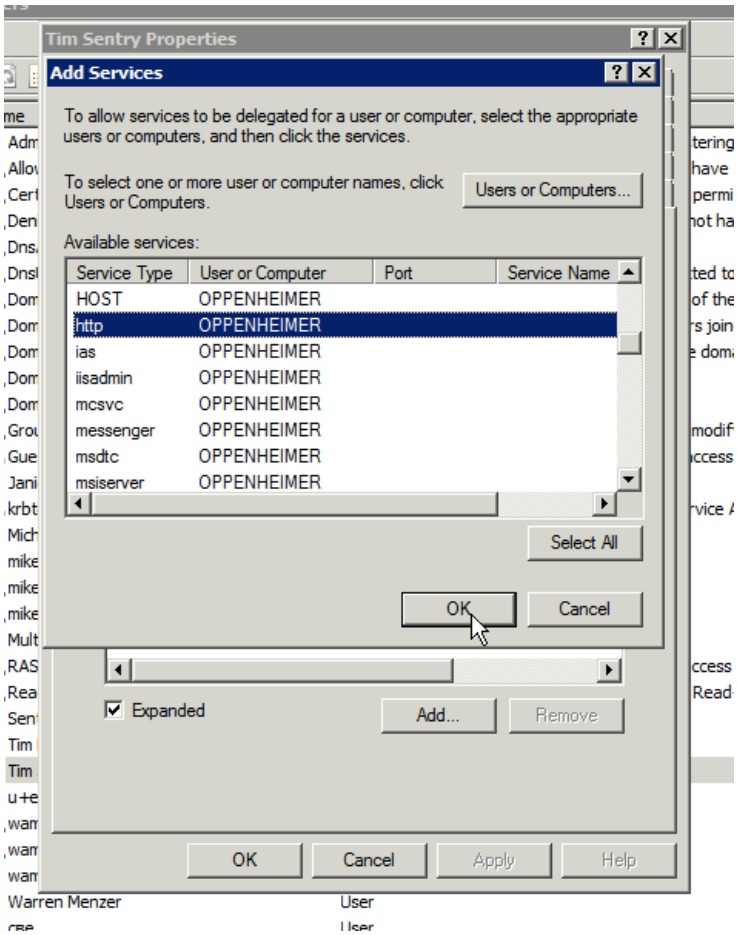
6. Klicken Sie auf **Hinzufügen**.
7. Klicken Sie auf **Benutzer oder Computer**.
   - Geben Sie den Computernamen des Acronis Access Gateway Server ein.
   - Klicken Sie auf **Namen überprüfen**.

- Der richtige Computername sollte im Kästchen 'Objektname' angezeigt werden.



8. Klicken Sie auf **OK**.

9. Suchen und wählen Sie den "**http**"-Dienst im Fenster **Dienste hinzufügen** aus.

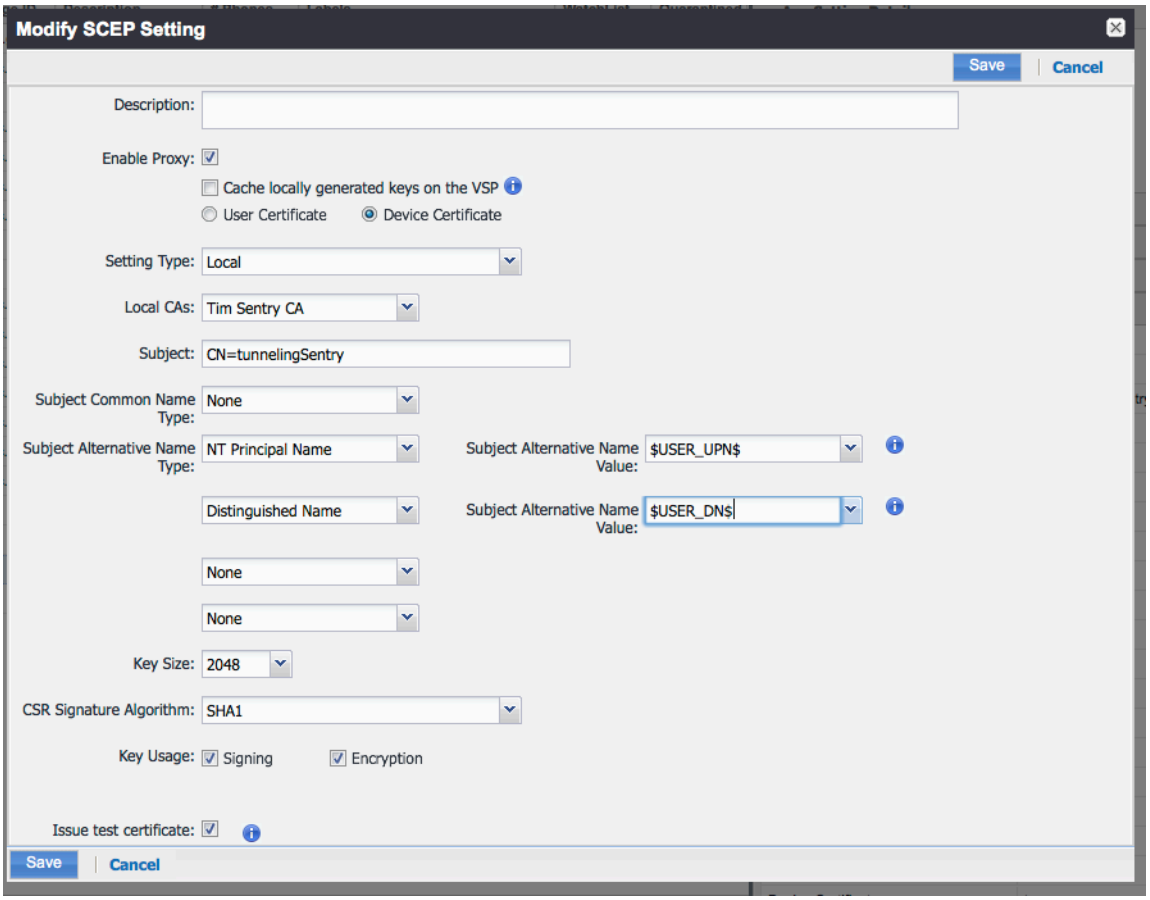


10. Klicken Sie auf **OK**.

Hinweis: *Für ein großangelegtes Deployment mit mehreren Gateway Servern wiederholen Sie bei für jeden einzelnen Gateway Server die Schritte 6 bis 10. Bei der ersten Inbetriebnahme empfiehlt es sich jedoch, mit einem einzelnen Gateway Server zu beginnen, der einige lokale Testordner hostet. Sobald Sie überprüft haben, dass Sie darauf zugreifen können, können Sie weitere Gateway Server und nicht-lokale Ordner hinzufügen.*

1. Öffnen Sie das Admin-Portal von MobileIron VSP.
2. Wählen Sie **Richtlinien und Konfigurationen**, und öffnen Sie **Konfigurationen**.
3. Suchen Sie das in "Ein neues SCEP erstellen" erstellte SCEP.

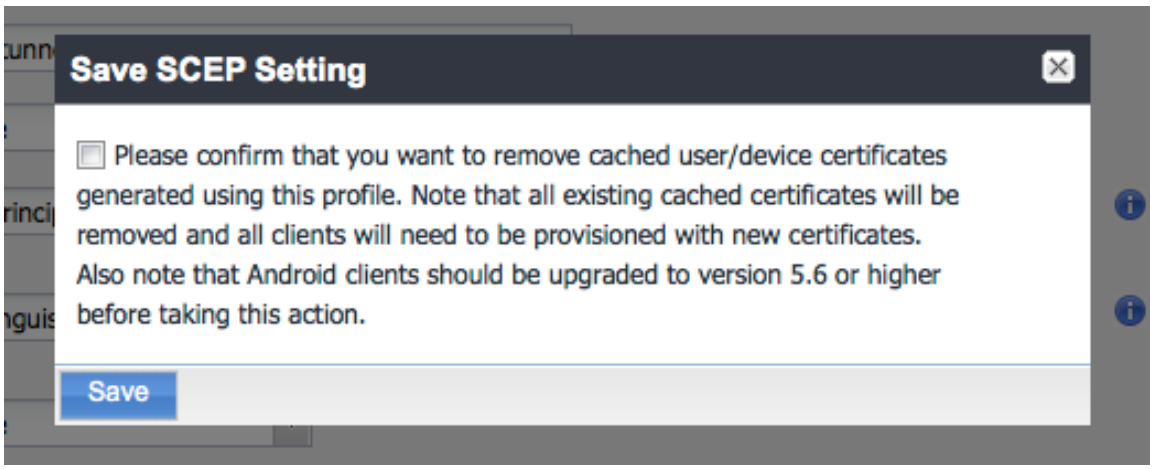
4. Klicken Sie auf dessen Namen und dann im Feld auf der rechten Seite auf **Bearbeiten**.



- Geben Sie zwei **Typen für alternative Betreffnamen ein**
  - **NT Prinzipalname**: **$USER_UPN$**
  - **Definierter Name**: **$USER_DN$**

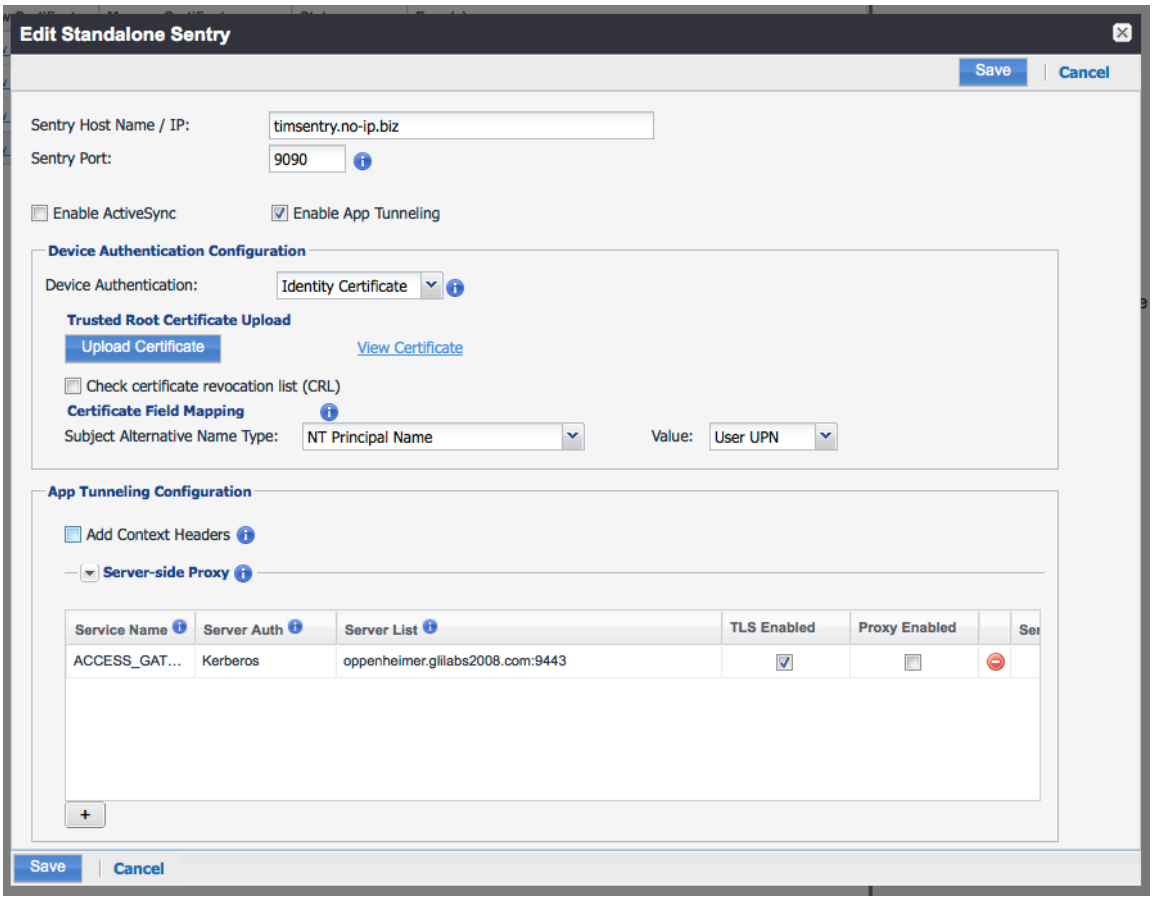
Hinweis: *Diese Einträge erfordern, dass Benutzerkonten auf dem VSP von Active Directory stammen und diese Variablen von ihm bereitgestellt werden. Diese Konfiguration sprengt den Rahmen dieses Dokuments.*

5. Klicken Sie auf **Speichern**.

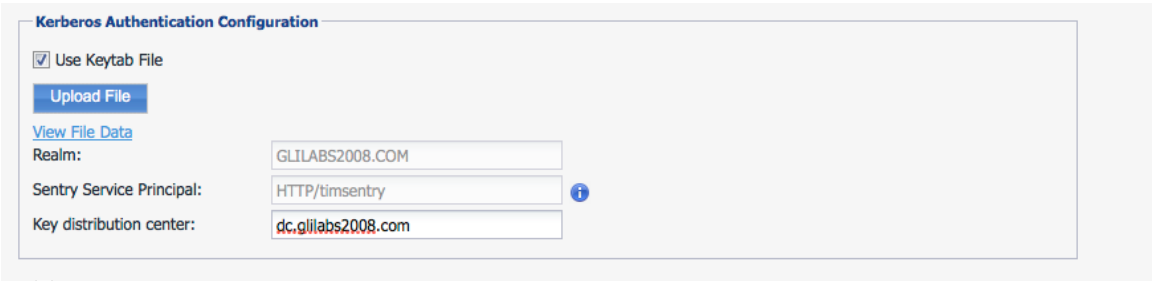


6. Da Sie das SCEP geändert haben, müssen Sie das Gerät in Mobile@Work erneut bereitstellen, bevor Sie den iOS-Client testen.

1. Während Sie sich noch im Admin-Portal von MobileIron VSP befinden, wählen Sie **Einstellungen** und öffnen Sie **Sentry**.
2. Suchen Sie die unter "Sentry hinzufügen und konfigurieren" erstellte **Sentry**.
3. Klicken Sie auf das Symbol für **Bearbeiten**.



- Wählen Sie unter **Konfiguration der Geräte-Authentifizierung** Folgendes für **Zuordnung der Zertifikatfelder**:
  - **Typ für alternative Betreffnamen**: **NT Prinzipalname**
  - **Wert**: **Benutzer-UPN**
- Ändern Sie unter **AppTunneling-Konfiguration** die **Server-Authentifizierung** auf Kerberos.

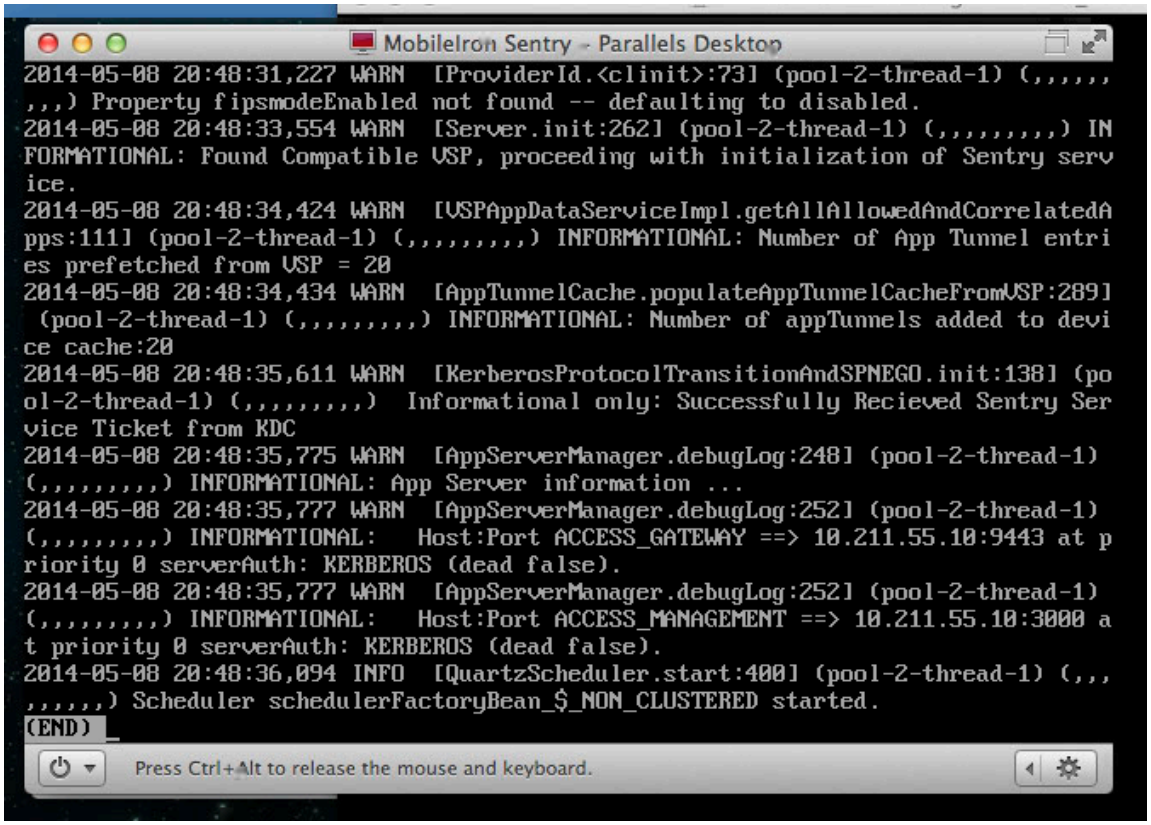


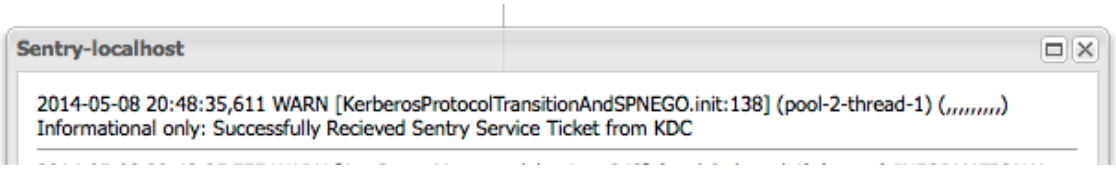
- Im Abschnitt **Konfiguration der Kerberos-Authentifizierung**.
  - Markieren Sie **Keytab-Datei verwenden**.
  - Klicken Sie auf **Datei hochladen**.
  - Laden Sie die unter "Eine Keytab für das Kerberos-Dienstkonto erstellen" erstellte Keytab-Datei hoch.
  - Verschieben Sie den Domain-Controller in den KDC.

4. Klicken Sie auf **Speichern**.

Überprüfen Sie entweder mit **Sentry EXEC** oder den Sentry-Protokollen im **System-Manager**, ob Sentry in der Lage ist, auf ein Kerberos-Ticket von KDC zuzugreifen und eines zu erhalten.

Suchen Sie die Zeile "**Nur für Informationszwecke: Erfolgreich Sentry-Dienst-Ticket von KDC erhalten**". Damit stellen Sie sicher, dass Sentry in der Lage ist, auf KDC zuzugreifen und damit zu kommunizieren.

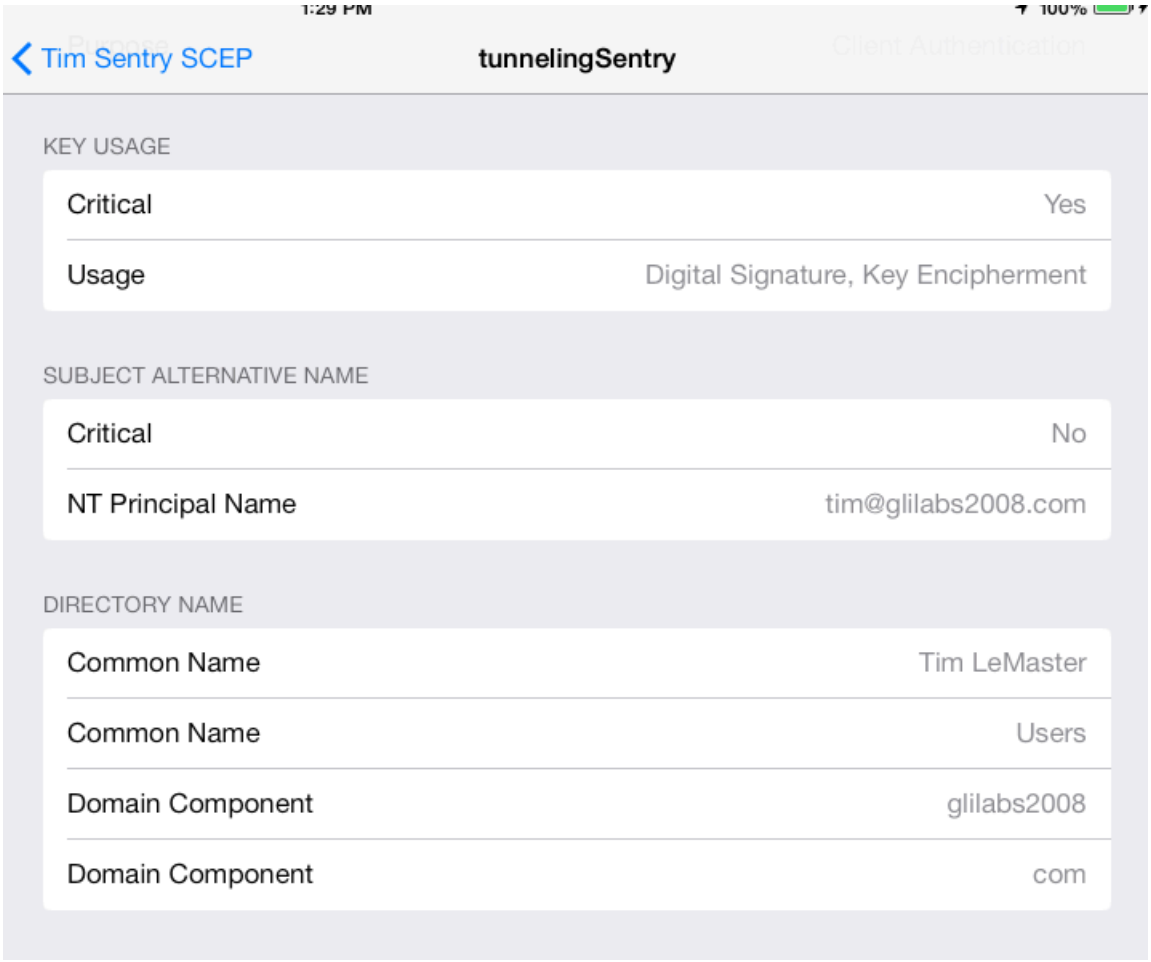




Die von uns durchgeführten Änderungen des SCEP müssen an das iOS-Gerät übertragen werden. Es kann einige Minuten dauern, bis die an Sentry durchgeführten Änderungen vollständig übertragen worden sind.

Rufen Sie auf dem Gerät "AppConnect" -> "Einstellungen" -> "Auf Updates prüfen" auf, tippen Sie auf "Gerät erneut registrieren" und befolgen Sie die Aufforderungen.

Mit der iOS Settings-App können Sie überprüfen, ob das SCEP ordnungsgemäß aktualisiert wurde. Unter "Einstellungen" -> "Allgemein" -> "Profile" -> "Der von Ihnen erstellte SCEP-Name" -> "Weitere Details" -> "Zertifikat" -> "Der Teil nach CN=, den Sie in den Betreffnamen des SCEP eingeben" sollten Sie die Einträge für "Alternativer Betreffname" und "Directory-Name" sehen. Wenn dies korrekt aus Active Directory abgerufen wurde, sollte dies mit dem Benutzer übereinstimmen, den Sie zur Aktivierung von Mobile@Work verwendet haben.



Wenn dies richtig ist, installieren Sie den Acronis Access Mobile Client erneut. Wiederholen Sie die oben aufgeführten Registrierungsschritte, aber lassen Sie dieses Mal die Felder für Benutzername und Kennwort leer. Wenn dies erfolgreich durchgeführt wurde, sollten Sie mit dem Konto, das mit dem NT-Prinzipalname im gerade überprüften Profil übereinstimmt, registriert sein.

7.1.1 Erweiterte Delegierungskonfigurationen

Dieser Artikel unterstützt Sie bei der Konfiguration der Delegierungsmethoden zur MobileIron-Anmeldung mit Netzwerkfreigaben und SharePoint-Sites. Diese Anleitung erfordert, dass Sie bereits sowohl MobileIron als auch Acronis Access, deren Interoperabilität und entsprechenden Active Directory-Konten, die die Authentifizierung delegieren, konfiguriert haben.

Bei Netzwerkfreigaben und SharePoint-Servern gehen Sie wie folgt vor:

Wenn Sie diese Schritte befolgen, aktivieren Sie die Delegierung vom Gateway-Server zu den Zielservern.

1. Öffnen Sie **Active Directory-Benutzer und -Computer**.
2. Suchen Sie das Computerobjekt, das dem Gateway-Server entspricht.
3. Klicken Sie mit der rechten Maustaste auf den Benutzer und wählen Sie "Eigenschaften".
4. Rufen Sie die Registerkarte **Delegierung** auf.
5. Wählen Sie **Computer bei Delegierungen angegebener Dienste vertrauen**.
6. Wählen Sie darunter die Option **Beliebiges Authentifizierungsprotokoll verwenden**.
7. Klicken Sie auf **Hinzufügen**.
8. Klicken Sie auf **Benutzer oder Computer**.
9. Suchen Sie nach dem Serverobjekt für die SMB-Freigabe oder den SharePoint-Server und klicken Sie auf **OK**.
   - Wählen Sie für SMB-Freigaben den Dienst **cifs**.
   - Wählen Sie für SharePoint den Dienst **http**.
10. Wiederholen Sie diese Schritte für jeden Server, auf den der Gateway-Server von Acronis Access zugreifen muss.
11. Wiederholen Sie dieses Verfahren für jeden Gateway-Server.

Es kann, je nach Größe der Domänen-Gesamtstruktur, einige Minuten dauern, bis diese Delegierungsänderungen übernommen werden. Sie müssen eventuell bis zu 15 Minuten (oder länger) warten, bis die Änderungen wirksam werden. Wenn es nach 15 Minuten immer noch nicht funktioniert, starten Sie den Acronis Access-Gateway-Dienst erneut.

7.2 Acronis Access auf einem Microsoft Failover Cluster installieren

Warnung! *Acronis Access Failover Clustering wird von Versionen vor 5.0.3 nicht unterstützt. Wenn Sie eine ältere Version verwenden, müssen Sie ein Upgrade auf Version 5.0.3 oder höher durchführen, bevor Sie Cluster-Konfigurationen vornehmen können.*

Die nachfolgend aufgeführten Anleitungen helfen Ihnen beim Installieren von Acronis Access in einem Cluster.

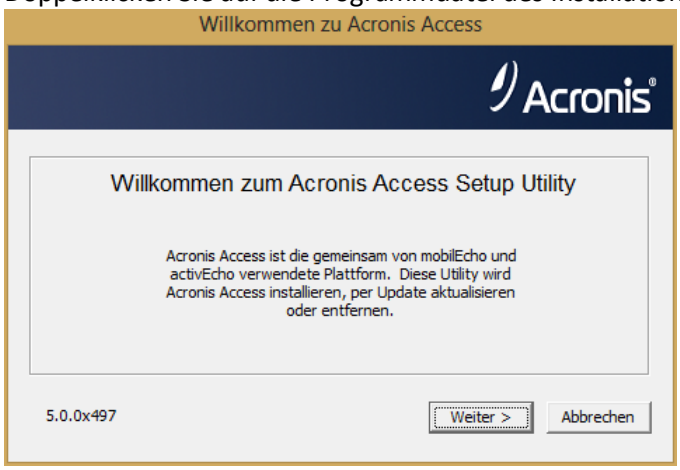
Themen

7.2.1 Acronis Access auf einem Microsoft Windows 2003 Failover Cluster installieren

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.



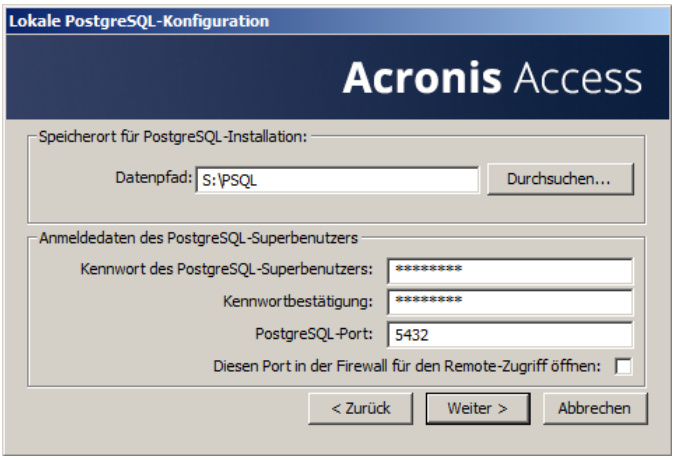
4. Klicken Sie auf **Weiter**, um zu beginnen.
5. Lesen und akzeptieren Sie die Lizenzvereinbarung.
6. Drücken Sie **Installieren**.

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. Wählen Sie auf einem freigegebenen Laufwerk einen Speicherort für den Ordner **Postgres Data** und drücken Sie **Weiter**.

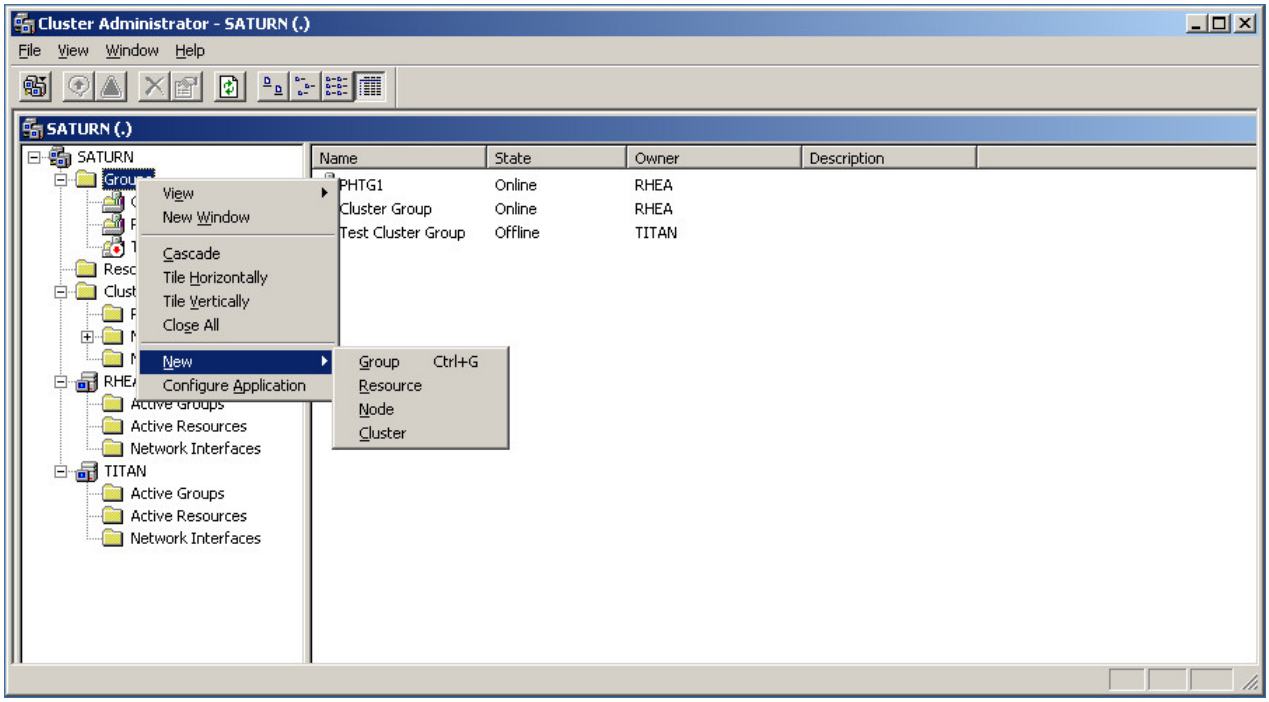


10. Es wird ein Fenster angezeigt, in dem alle zu installierenden Komponenten aufgelistet sind. Drücken Sie **OK**, um fortzufahren.

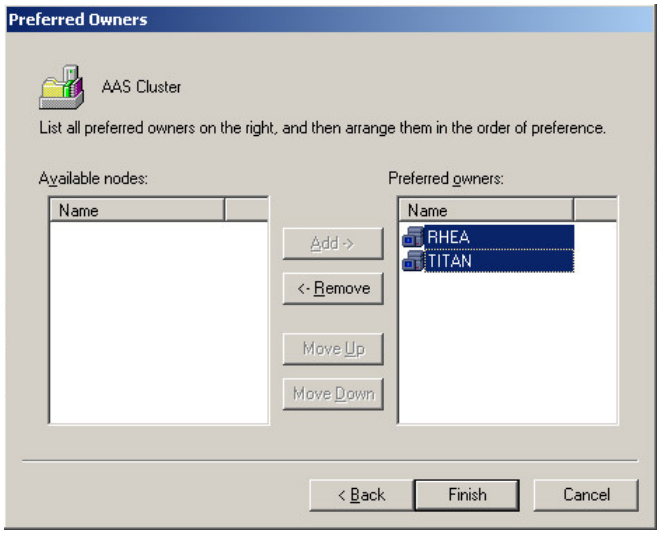
Wenn der Installationsvorgang für Acronis Access abgeschlossen ist, drücken Sie Beenden**.**

Die Cluster-Gruppe erstellen

1. Öffnen Sie die **Clusterverwaltung** und dann **Gruppen**.
2. Klicken Sie mit der rechten Maustaste auf **Gruppen** und wählen Sie **Neu** und dann **Gruppe**. Geben Sie der Cluster-Gruppe einen angemessenen Namen (z.B. Acronis Access, AAS Cluster).



3. Wählen Sie die Maschinen aus, die Teil dieser Cluster-Gruppe sein sollen, und drücken Sie **Fertig stellen**.



Konfigurationen auf dem aktiven Knoten

1. Konfigurieren Sie die Gateway Server-Datenbank, sodass sie sich auf einem freigegebenen Laufwerk befindet.
   a. Navigieren Sie zu **`C:\Program Files (x86)\Acronis\Access\Gateway Server\`**
      - Bei einem Upgrade lautet der Pfad: **`C:\Program Files (x86)\GroupLogic\mobilEcho Server\`**
   b. Suchen Sie die Datei **database.yml** und öffnen Sie sie mit einem Texteditor.
   c. Gehen Sie zu dieser Zeile: **`database_path: './database/'`** und ersetzen Sie **./database/** durch den gewünschten Pfad (z.B. **`database_path: 'S:/mobilEcho_cluster/database/'`**).

   Hinweis: *Verwenden Sie als Pfadtrennzeichen Schrägstriche (/).*

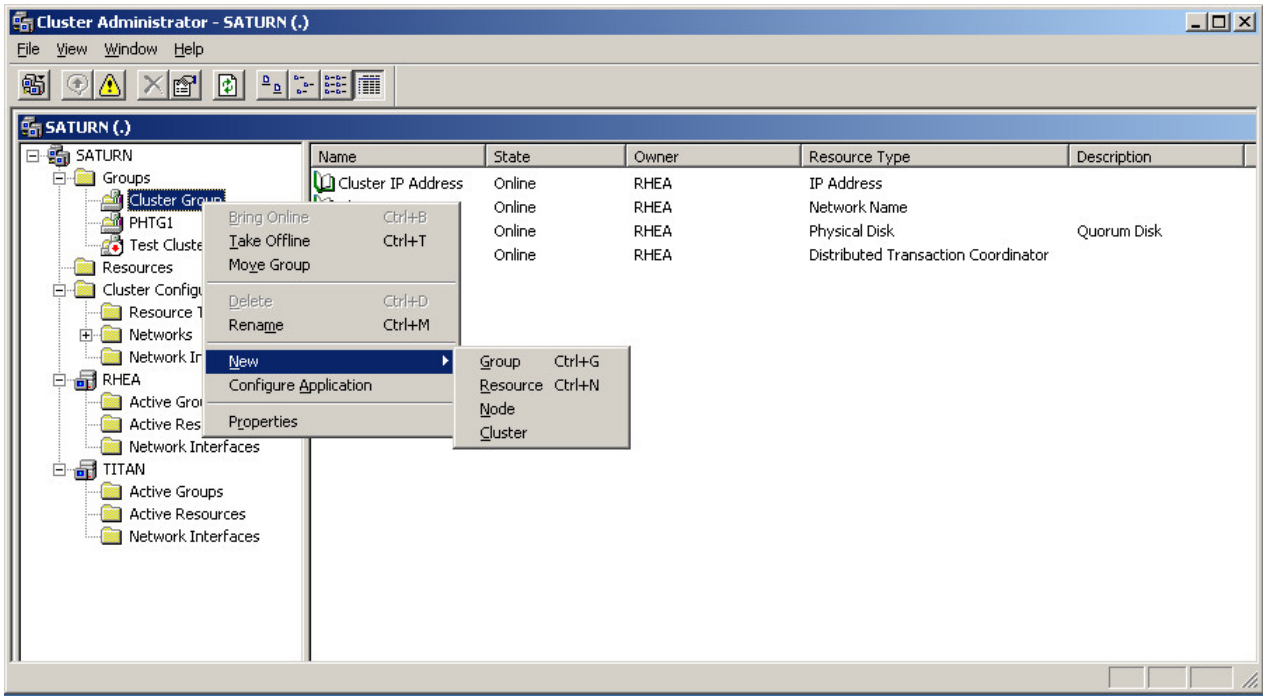
   Hinweis: *Sie können die konfigurierte Datei 'database.yml' aus dem ersten Knoten kopieren und im zweiten Knoten einfügen.*

Alle erforderlichen Dienste der Acronis Access Cluster-Gruppe hinzufügen

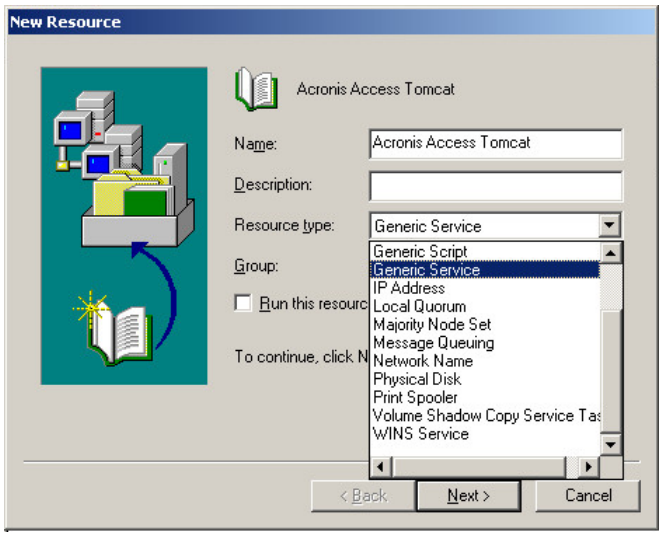
Führen Sie das folgende Verfahren für die einzelnen Dienste aus: AcronisAccessGateway, AcronisAccessPostgreSQL (abhängig von der Acronis Access-Version), AcronisAccessRepository und AcronisAccessTomcat.

1. Klicken Sie mit der rechten Maustaste auf die Acronis Access Cluster-Gruppe.

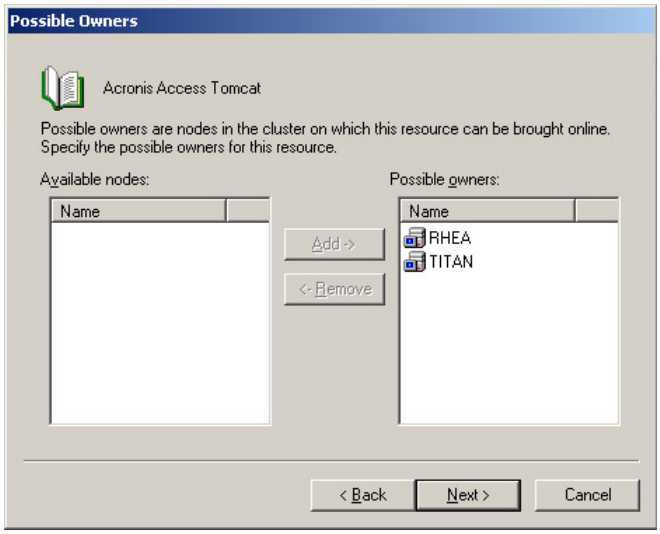
2. Öffnen Sie **Neu** und wählen Sie **Ressource**.



3. Geben Sie einen Namen für den Dienst ein und wählen Sie die richtige Cluster-Gruppe aus.
4. Wählen Sie aus dem Dropdown-Menü **Ressourcentyp** die Option **Allgemeiner Dienst** aus und drücken Sie **Weiter**.



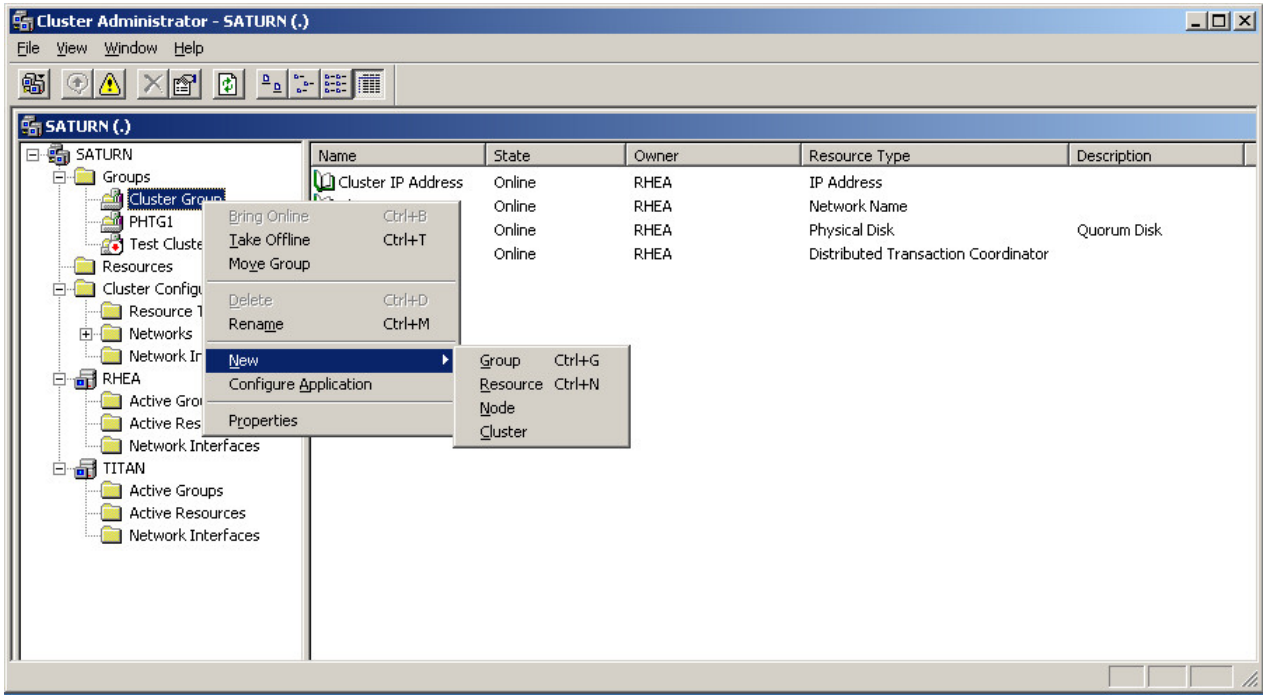
5. Stellen Sie sicher, dass beide Knoten als **Mögliche Besitzer** aufgeführt sind und drücken Sie **Weiter**.



6. Überspringen Sie zunächst die Abhängigkeiten, indem Sie **Weiter** drücken.
7. Geben Sie den richtigen Namen des Dienstes ein, den Sie hinzufügen, (z.B. postgresql-x64-9.2) und drücken Sie **Weiter**.
8. Überspringen Sie zunächst das Fenster **Registrierungsreplikation**, indem Sie auf **Weiter** drücken.
9. Drücken Sie **Fertig stellen**, um den Vorgang abzuschließen.

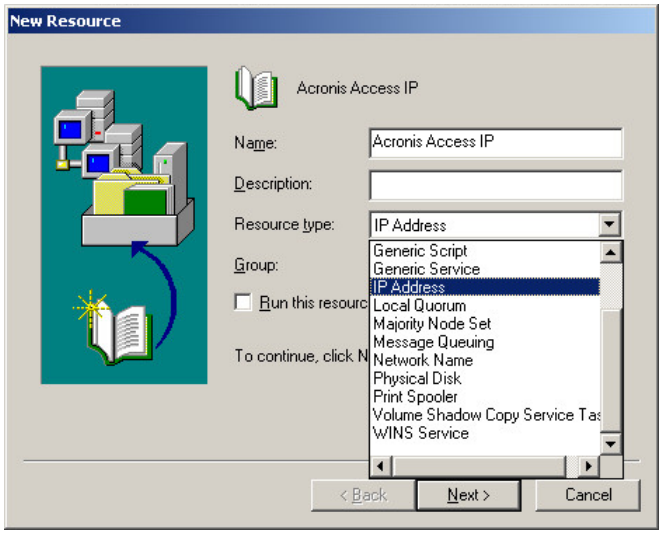
IP-Adresse für die Cluster-Gruppe festlegen

1. Klicken Sie mit der rechten Maustaste auf die Acronis Access Cluster-Gruppe.
2. Öffnen Sie **Neu** und wählen Sie **Ressource**.

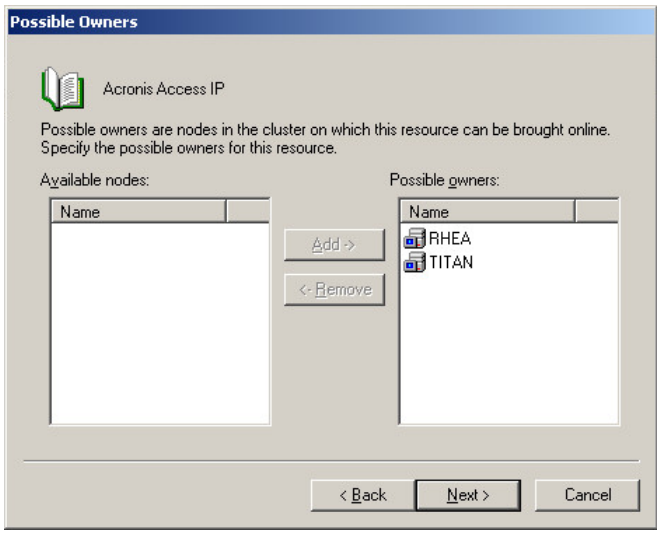


3. Geben Sie einen Namen für die Ressource ein und wählen Sie die richtige Cluster-Gruppe aus.

4. Wählen Sie aus dem Dropdown-Menü **Ressourcentyp** die Option **IP-Adresse** aus und drücken Sie **Weiter**.



5. Stellen Sie sicher, dass beide Knoten als **Mögliche Besitzer** aufgeführt sind und drücken Sie **Weiter**.

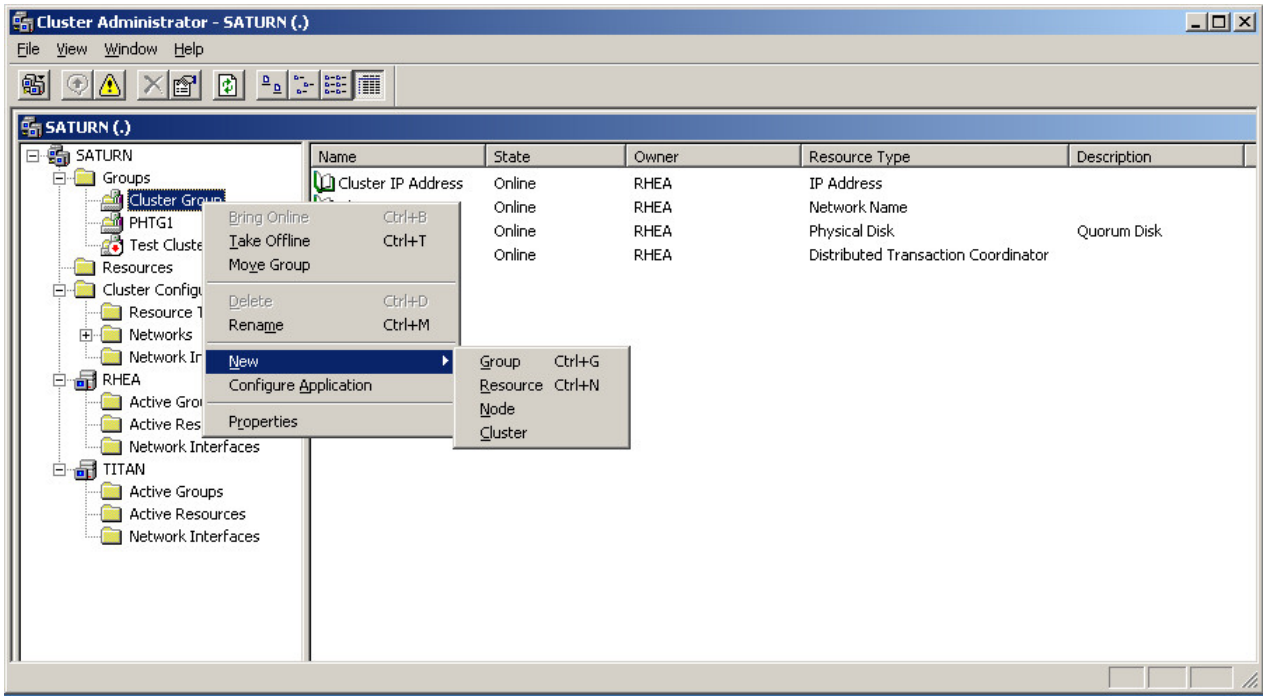


6. Überspringen Sie zunächst die Abhängigkeiten, indem Sie **Weiter** drücken.
7. Geben Sie die IP-Adresse ein, die Sie für diese Cluster-Gruppe verwenden möchten.
8. Geben Sie die Subnetzmaske ein und drücken Sie **Fertig stellen**.

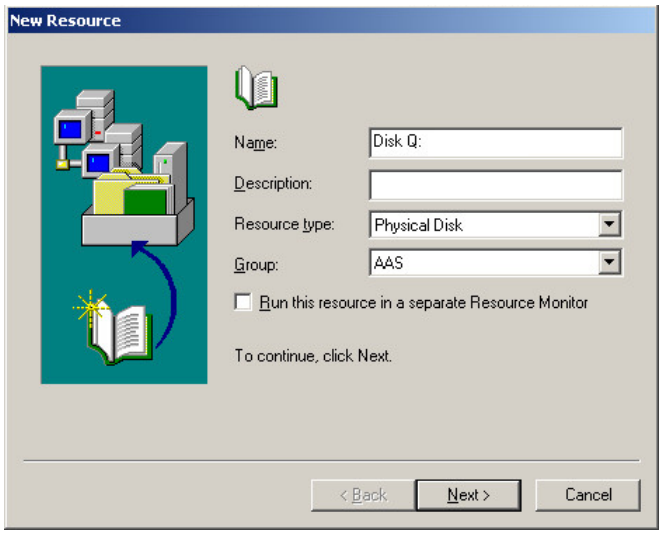
Freigegebenes Laufwerk hinzufügen

1. Klicken Sie mit der rechten Maustaste auf die Acronis Access Cluster-Gruppe.

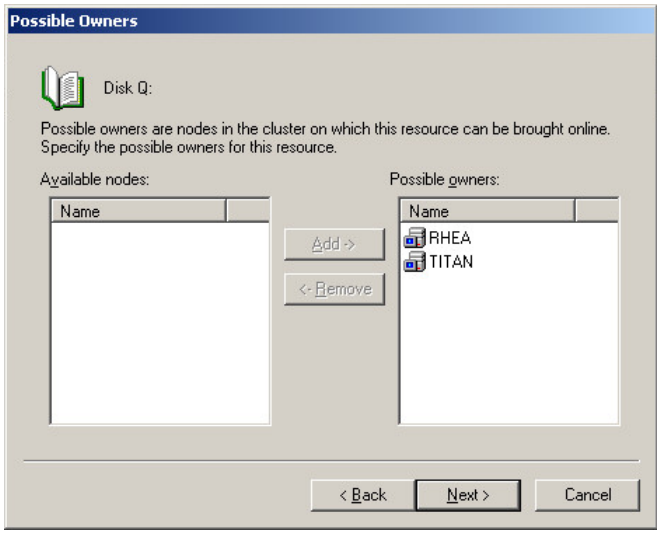
2. Öffnen Sie **Neu** und wählen Sie **Ressource**.



3. Geben Sie einen Namen für die Ressource ein und wählen Sie die richtige Cluster-Gruppe aus.
4. Wählen Sie aus dem Dropdown-Menü **Ressourcentyp** die Option **Physisches Laufwerk** aus und drücken Sie **Weiter**.



5. Stellen Sie sicher, dass beide Knoten als **Mögliche Besitzer** aufgeführt sind und drücken Sie **Weiter**.



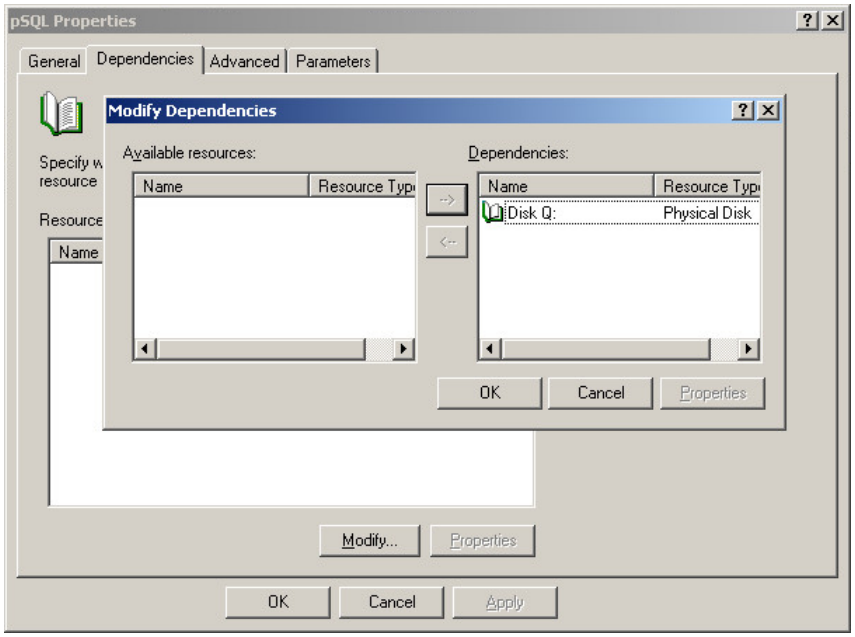
6. Überspringen Sie zunächst die Abhängigkeiten, indem Sie **Weiter** drücken.
7. Wählen Sie ein verfügbares Laufwerk aus dem Dropdown-Menü aus und drücken Sie **Fertig stellen**.

Abhängigkeiten konfigurieren

Führen Sie für PostgreSQL und das Acronis Access Datei-Repository Folgendes durch:

1. Klicken Sie mit der rechten Maustaste auf den entsprechenden Dienst und wählen Sie **Eigenschaften**.
2. Klicken Sie auf die Registerkarte **Abhängigkeiten**.
3. Klicken Sie auf **Ändern**.

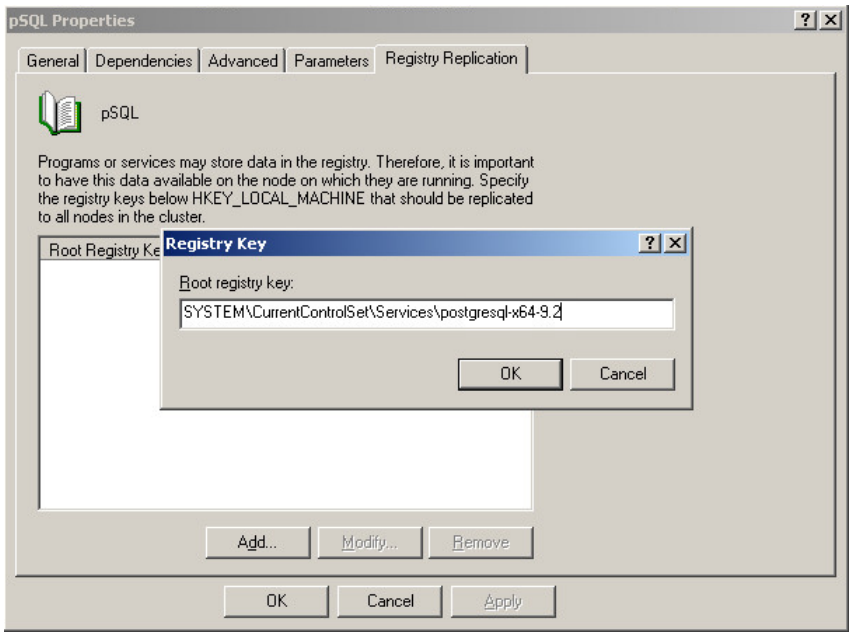
4. Wählen Sie das freigegebene Laufwerk aus, das Sie hinzugefügt haben, und verschieben Sie es nach rechts.



5. Drücken Sie **OK**.

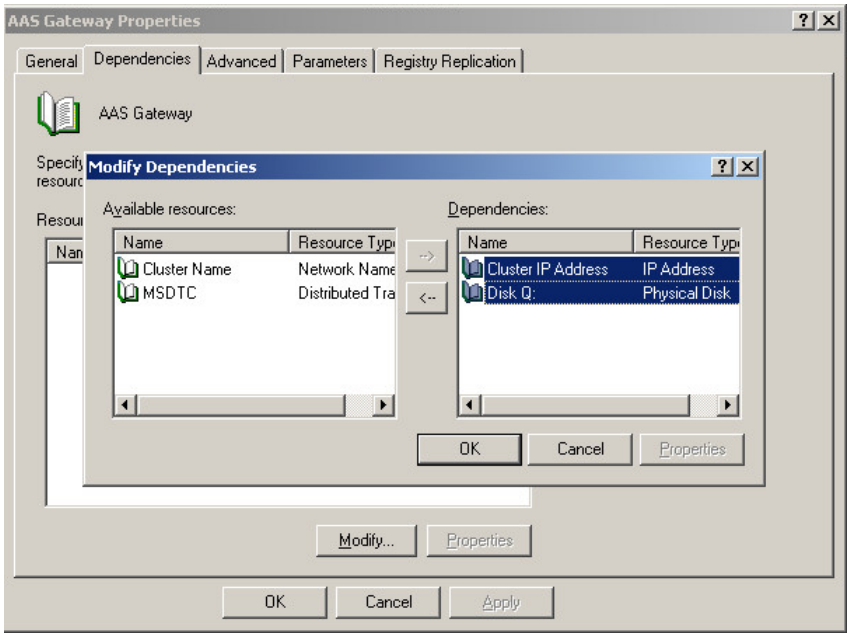
Führen Sie für PostgreSQL zudem Folgendes durch:

1. Klicken Sie auf die Registerkarte **Registrierungsreplikation**.
2. Drücken Sie **Hinzufügen** und geben Sie Folgendes ein: **`SYSTEM\CurrentControlSet\Services\AcronisAccessPostgreSQL\`**(Für ältere Versionen von Acronis Access kann der Service unterschiedlich sein, z. B. **postgresql-x64-9.2**)



Führen Sie für den Acronis Access Gateway Server-Dienst Folgendes durch:

1. Klicken Sie mit der rechten Maustaste auf den entsprechenden Dienst und wählen Sie **Eigenschaften**.
2. Klicken Sie auf die Registerkarte **Abhängigkeiten**.
3. Klicken Sie auf **Ändern**.
4. Wählen Sie die **IP-Adresse** und das **physische Laufwerk** aus und verschieben Sie sie nach rechts.

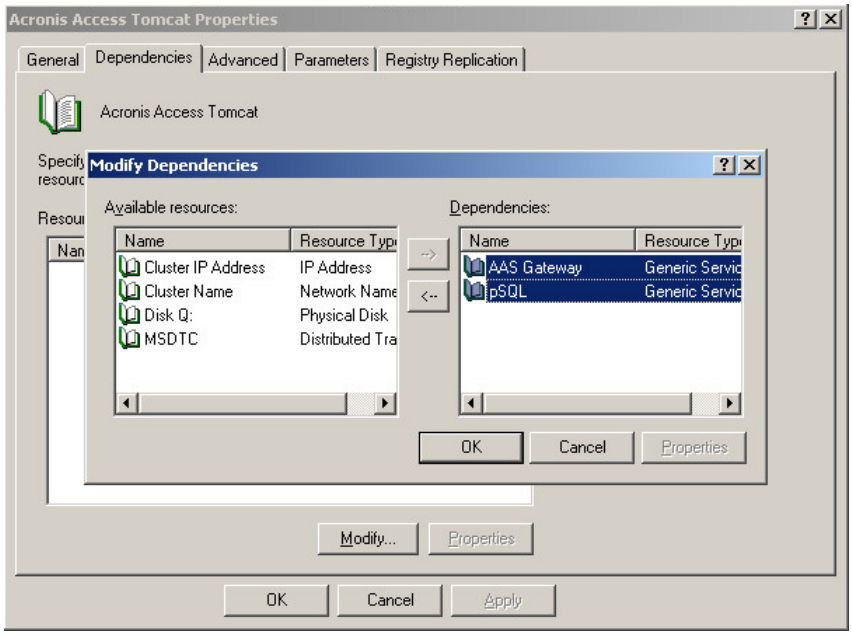


5. Drücken Sie **OK**.

Führen Sie für den Acronis Access Tomcat-Dienst Folgendes durch:

1. Klicken Sie mit der rechten Maustaste auf den entsprechenden Dienst und wählen Sie **Eigenschaften**.
2. Klicken Sie auf die Registerkarte **Abhängigkeiten**.
3. Klicken Sie auf **Ändern**.

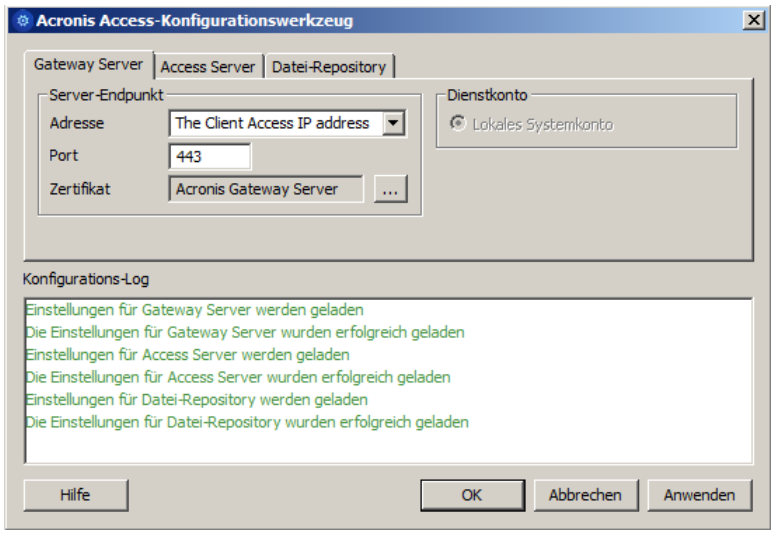
4. Wählen Sie die PostgreSQL- und Acronis Access Gateway Server-Dienste aus und verschieben Sie sie nach rechts.



5. Drücken Sie **OK**.

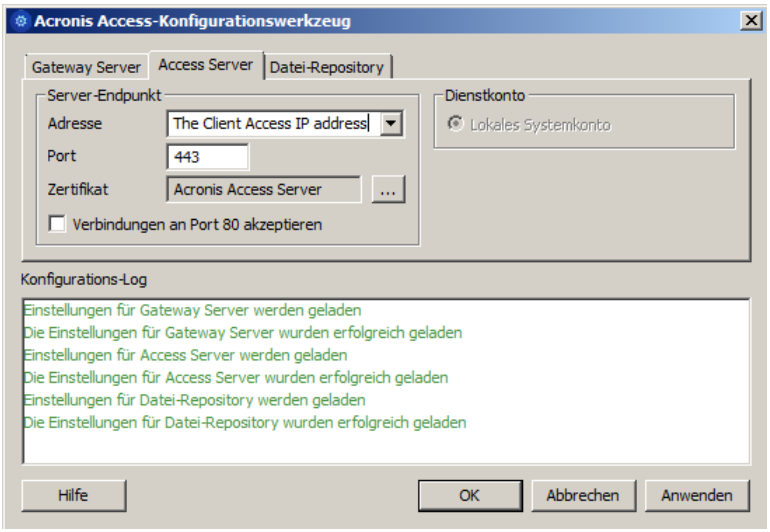
Die Cluster-Gruppe online schalten und das Konfigurationswerkzeug verwenden

1. Klicken Sie mit der rechten Maustaste auf die Cluster-Gruppe und drücken Sie **Online schalten**.
2. Starten Sie das Konfigurationswerkzeug.
   - Bei einer Neuinstallation befindet sich dies normalerweise unter **`C:\Program Files (x86)\Acronis\Access\Configuration Utility`**
   - Bei einem Upgrade von mobilEcho befindet es sich normalerweise unter **`C:\Program Files (x86)\GroupLogic\Configuration Utility`**
3. Konfigurieren Sie den Acronis Access Gateway Server-Dienst, um die IP-Adresse(n) für die Acronis Access Dienstgruppe abzuhören.

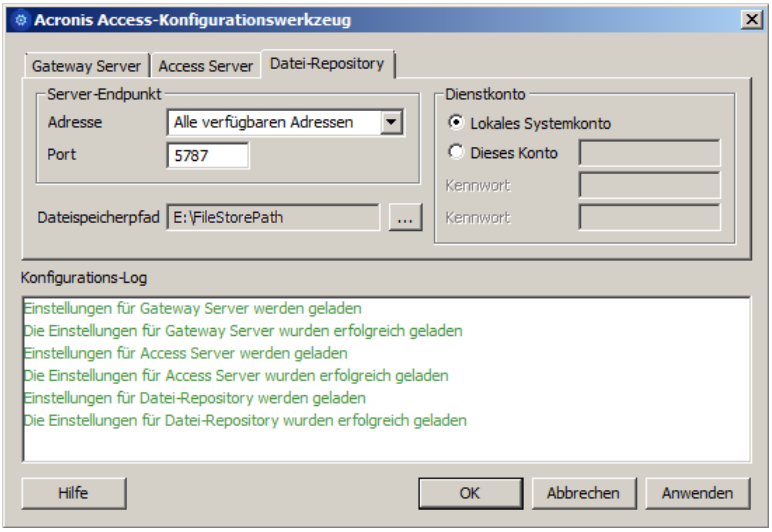


4. Konfigurieren Sie den Acronis Access Server-Dienst, um die IP-Adresse(n) für die Acronis Access Dienstgruppe abzuhören.

   Hinweis: *Wenn* ***Verbindungen an Port 80 akzeptieren*** *ausgewählt ist, hört Tomcat den unsicheren Port 80 auf eingehenden Datenverkehr hin ab und leitet ihn zum HTTPS-Port um, den Sie zuvor festgelegt haben.*



5. Konfigurieren Sie das Acronis Access Datei-Repository, um 'localhost' abzuhören, und ändern Sie den Dateispeicherpfad in ein Verzeichnis auf dem freigegebenen Laufwerk. Dieser Pfad sollte für beide Knoten gleich sein.



6. Klicken Sie auf **OK**, um die Konfiguration abzuschließen, und starten Sie die Dienste neu.

Installation und Konfiguration auf dem zweiten Knoten

1. Deaktivieren Sie alle vorhandenen Virenschutzprogramme, da sie unter Umständen den Installationsvorgang unterbrechen und somit eine fehlerhafte Installation verursachen können.
2. Installieren Sie Acronis Access auf dem zweiten Knoten, verwenden Sie jedoch diesmal den Standardspeicherort für **Postgres Data** sowie dasselbe postgres-Benutzerkennwort wie für den ersten Knoten.
3. Schließen Sie die Installation ab.

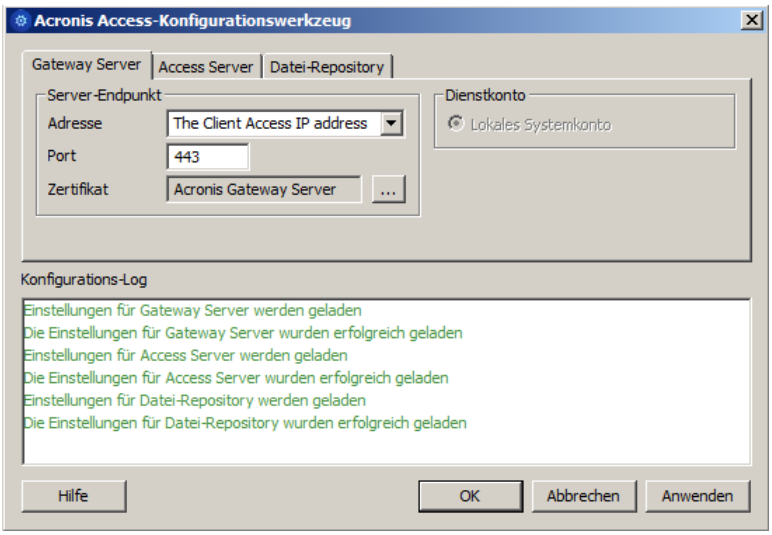
4. Konfigurieren Sie die Gateway Server-Datenbank, sodass sie sich auf einem freigegebenen Laufwerk befindet.
   a. Navigieren Sie zu **`C:\Program Files (x86)\Acronis\Access\Gateway Server\`**
      - Bei einem Upgrade lautet der Pfad: **`C:\Program Files (x86)\GroupLogic\mobilEcho Server\`**
   b. Suchen Sie die Datei **database.yml** und öffnen Sie sie mit einem Texteditor.
   c. Gehen Sie zu dieser Zeile: **`database_path: './database/'`** und ersetzen Sie **./database/** durch den gewünschten Pfad (z.B. **`database_path: 'S:/mobilEcho_cluster/database/'`**).

   Hinweis: *Verwenden Sie als Pfadtrennzeichen Schrägstriche (/).*

   Hinweis: *Sie können die konfigurierte Datei 'database.yml' aus dem ersten Knoten kopieren und im zweiten Knoten einfügen.*

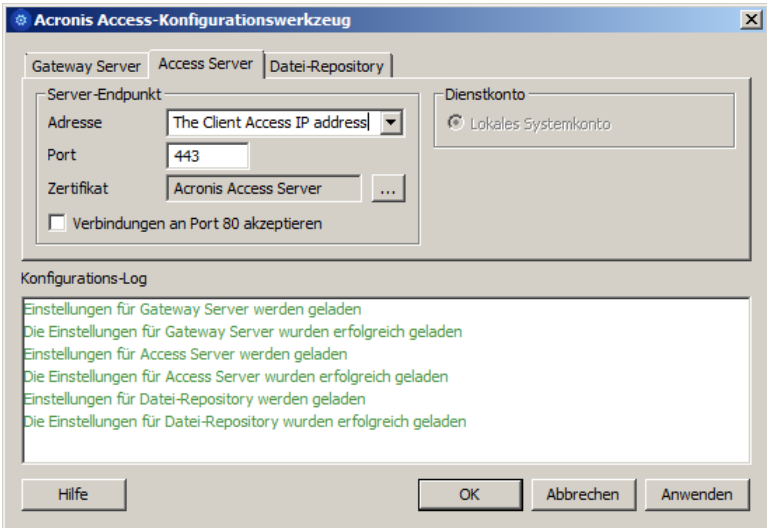
   Hinweis: *Der Pfad sollte mit dem Pfad auf dem ersten Knoten übereinstimmen.*

5. Verschieben Sie die Cluster-Gruppe in den zweiten Knoten. Klicken Sie dazu mit der rechten Maustaste auf die Cluster-Gruppe und klicken Sie auf **Gruppe verschieben**.
6. Starten Sie das Konfigurationswerkzeug.
   - Bei einer Neuinstallation befindet sich dies normalerweise unter **`C:\Program Files (x86)\Acronis\Access\Configuration Utility`**
   - Bei einem Upgrade von mobilEcho befindet es sich normalerweise unter **`C:\Program Files (x86)\GroupLogic\Configuration Utility`**
7. Konfigurieren Sie den Acronis Access Gateway Server-Dienst, um die IP-Adresse(n) für die Acronis Access Dienstgruppe abzuhören.

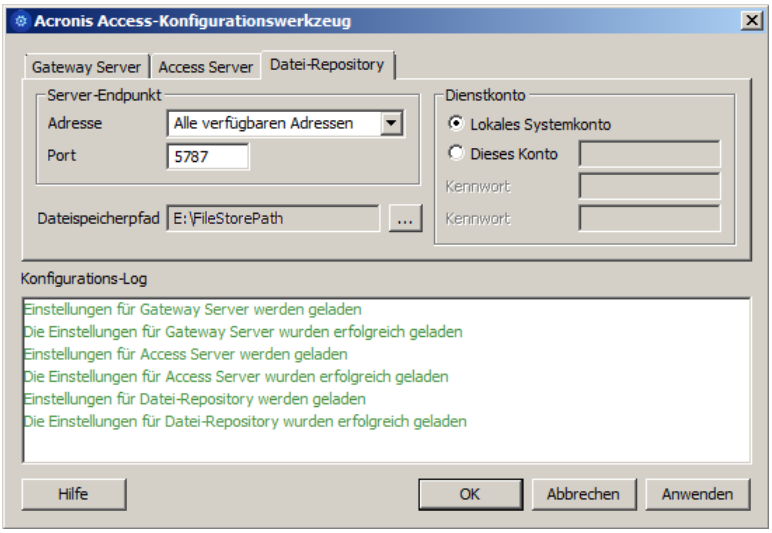


8. Konfigurieren Sie den Acronis Access Server-Dienst, um die IP-Adresse(n) für die Acronis Access Dienstgruppe abzuhören.

Hinweis: *Wenn* ***Verbindungen an Port 80 akzeptieren*** *ausgewählt ist, hört Tomcat den unsicheren Port 80 auf eingehenden Datenverkehr hin ab und leitet ihn zum HTTPS-Port um, den Sie zuvor festgelegt haben.*



9. Konfigurieren Sie das Acronis Access Datei-Repository, um 'localhost' abzuhören, und ändern Sie den Dateispeicherpfad in ein Verzeichnis auf dem freigegebenen Laufwerk. Dieser Pfad sollte für beide Knoten gleich sein.



10. Klicken Sie auf **OK**, um die Konfiguration abzuschließen, und starten Sie die Dienste neu.

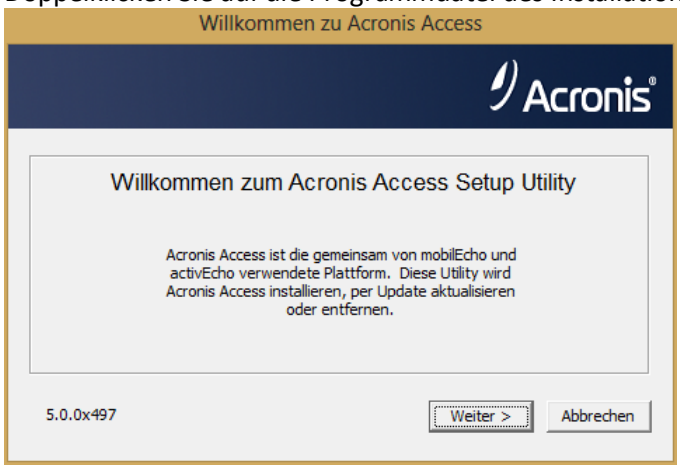
7.2.2 Acronis Access auf einem Microsoft Windows 2008 Failover Cluster installieren

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.



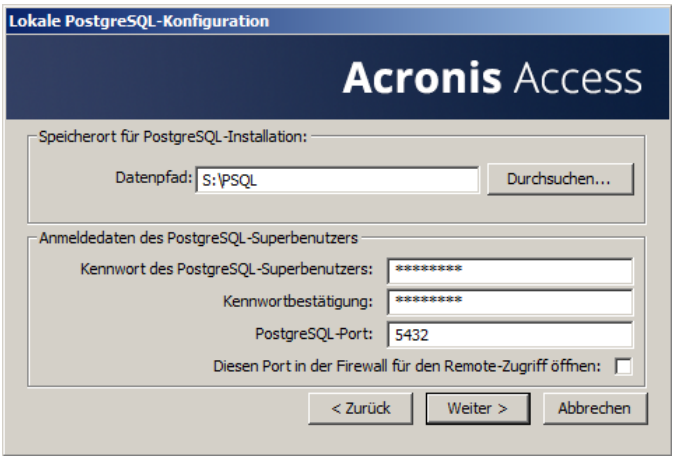
4. Klicken Sie auf **Weiter**, um zu beginnen.
5. Lesen und akzeptieren Sie die Lizenzvereinbarung.
6. Drücken Sie **Installieren**.

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. Wählen Sie auf einem freigegebenen Laufwerk einen Speicherort für den Ordner **Postgres Data** und drücken Sie **Weiter**.



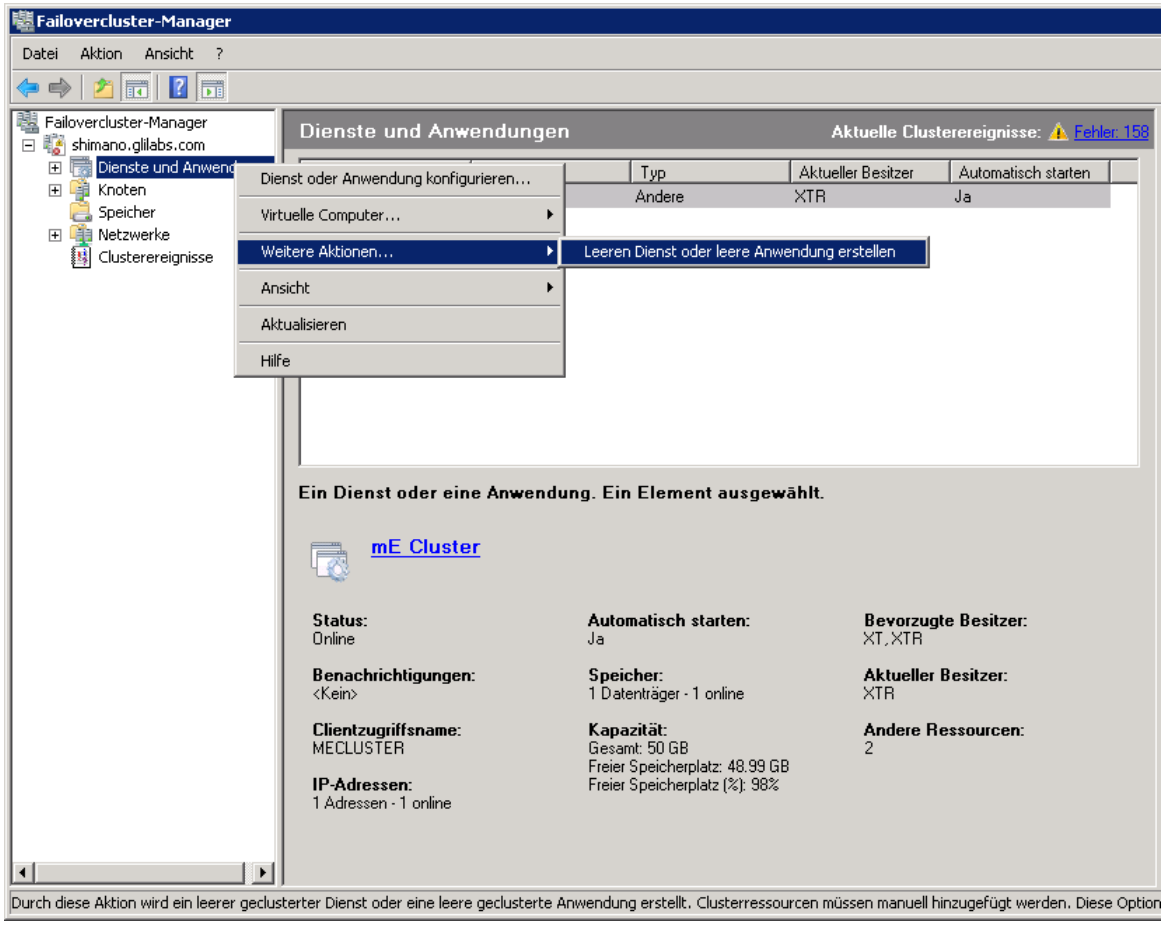
10. Es wird ein Fenster angezeigt, in dem alle zu installierenden Komponenten aufgelistet sind. Drücken Sie **OK**, um fortzufahren.

Wenn der Installationsvorgang für Acronis Access abgeschlossen ist, drücken Sie Beenden**.**

Die Dienstgruppe erstellen

1. Öffnen Sie die **Failover-Clusterverwaltung** und erweitern Sie Ihr Cluster.
2. Klicken Sie mit der rechten Maustaste auf **Dienste und Anwendungen** und wählen Sie **Weitere Aktionen**.

3. Wählen Sie die Option **Leeren Dienst oder leere Anwendung erstellen** und drücken Sie **Weiter**. Geben Sie der Dienstgruppe einen geeigneten Namen (z.B. Acronis Access, AAS Cluster).



Konfigurationen auf dem aktiven Knoten

1. Konfigurieren Sie die Gateway Server-Datenbank, sodass sie sich auf einem freigegebenen Laufwerk befindet.
   a. Navigieren Sie zu **`C:\Program Files (x86)\Acronis\Access\Gateway Server\`**
      - Bei einem Upgrade lautet der Pfad: **`C:\Program Files (x86)\GroupLogic\mobilEcho Server\`**
   b. Suchen Sie die Datei **database.yml** und öffnen Sie sie mit einem Texteditor.
   c. Gehen Sie zu dieser Zeile: **`database_path: './database/'`** und ersetzen Sie **./database/** durch den gewünschten Pfad (z.B. **`database_path: 'S:/mobilEcho_cluster/database/'`**).

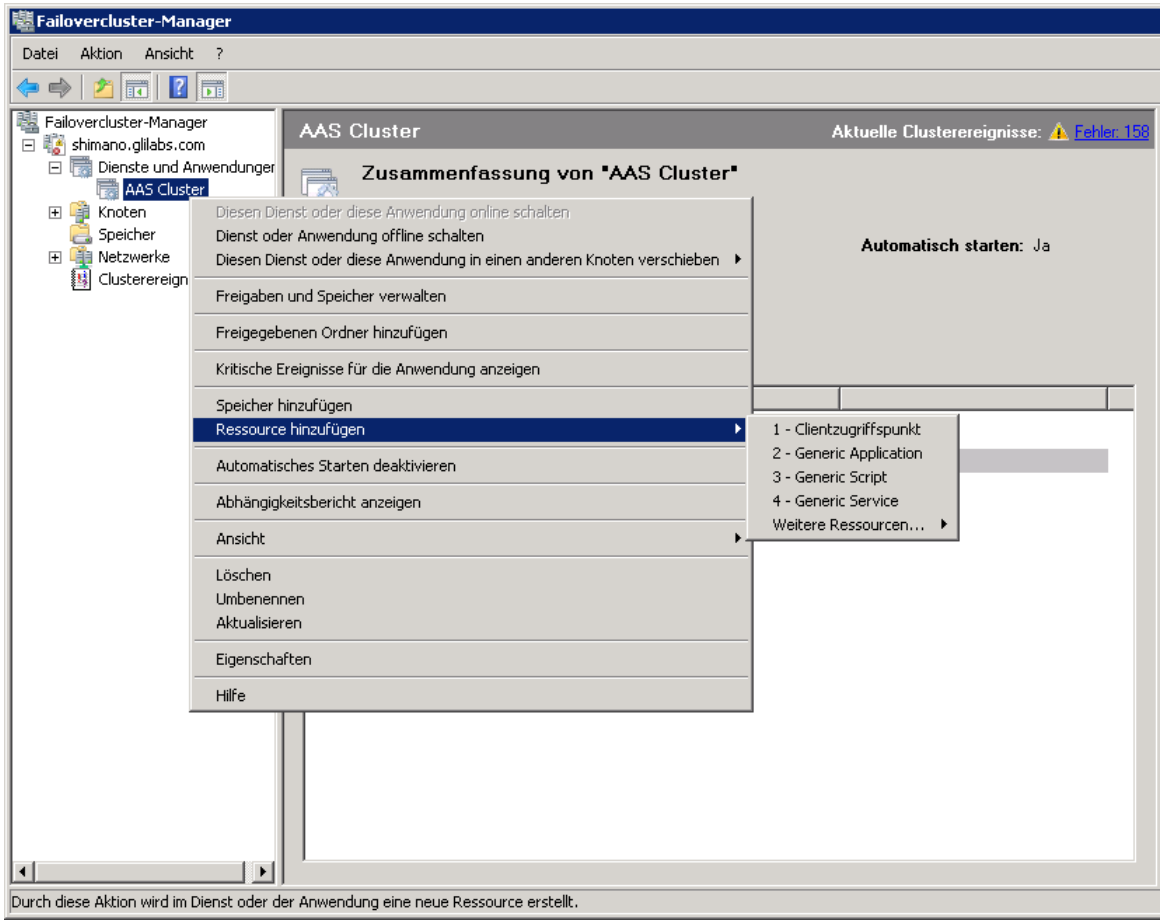
   Hinweis: *Verwenden Sie als Pfadtrennzeichen Schrägstriche (/).*

   Hinweis: *Sie können die konfigurierte Datei 'database.yml' aus dem ersten Knoten kopieren und im zweiten Knoten einfügen.*

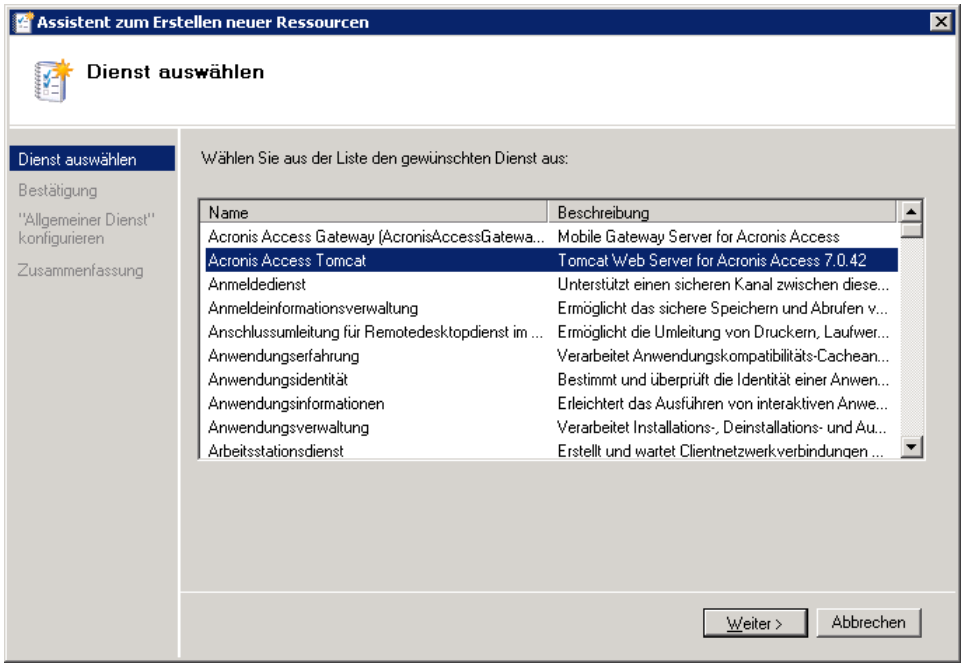
Alle erforderlichen Dienste der Acronis Access Dienstgruppe hinzufügen

Führen Sie das folgende Verfahren für die einzelnen Dienste aus: AcronisAccessGateway, AcronisAccessPostgreSQL (abhängig von der Acronis Access-Version), AcronisAccessRepository und AcronisAccessTomcat.

1. Klicken Sie mit der rechten Maustaste auf die Acronis Access Dienstgruppe und wählen Sie **Ressource hinzufügen**.
2. Wählen Sie **Allgemeiner Dienst** aus.



3. Wählen Sie den geeigneten Dienst aus und drücken Sie **Weiter**.

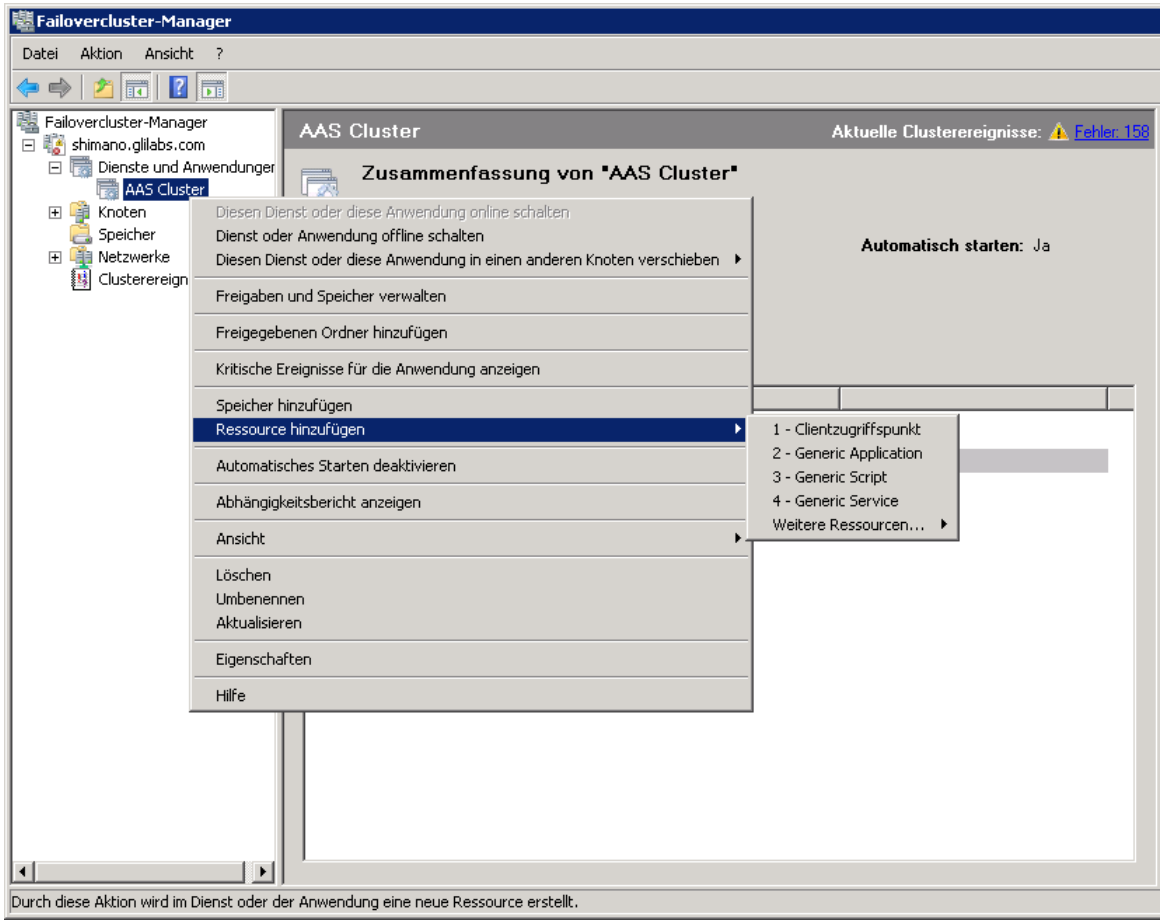


4. Drücken Sie im Bestätigungsfenster **Weiter**.
5. Drücken Sie im Fenster **Registrierungseinstellungen replizieren Weiter**.
6. Drücken Sie im Zusammenfassungsfenster **Fertig stellen**.

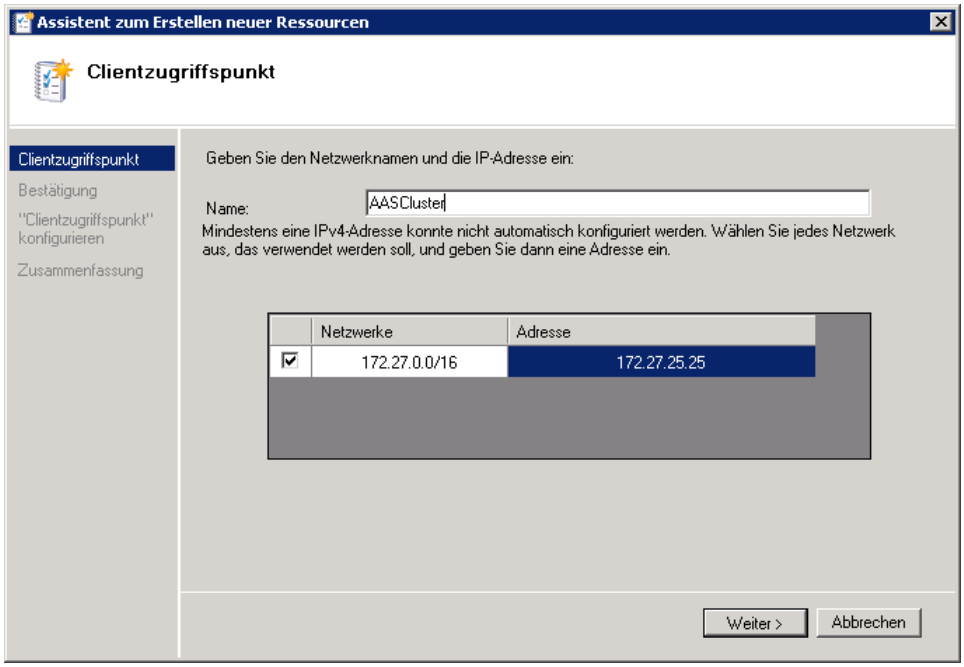
Clientzugriffspunkt festlegen

1. Klicken Sie mit der rechten Maustaste auf die Acronis Access Dienstgruppe und wählen Sie **Ressource hinzufügen**.

2. Wählen Sie **Clientzugriffspunkt** aus.



3. Geben Sie einen Namen für diesen Zugriffspunkt ein.
4. Wählen Sie ein Netzwerk.

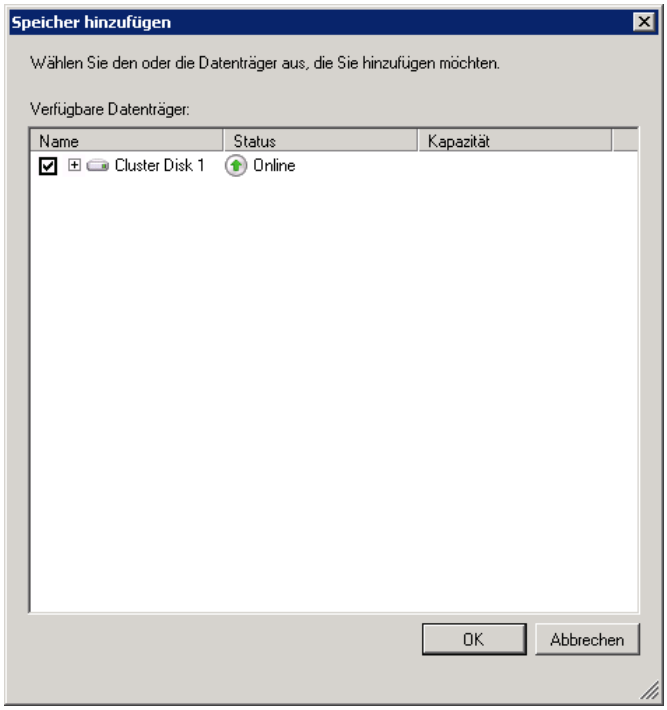


5. Geben Sie die IP-Adresse ein und drücken Sie **Weiter**.

6. Drücken Sie im Bestätigungsfenster **Weiter**.
7. Drücken Sie im Zusammenfassungsfenster **Fertig stellen**.

Freigegebenes Laufwerk hinzufügen

1. Klicken Sie mit der rechten Maustaste auf die Acronis Access Dienstgruppe und wählen Sie **Ressource hinzufügen**.
2. Wählen Sie das gewünschte freigegebene Laufwerk aus.



3. Drücken Sie im Bestätigungsfenster **Weiter**.
4. Drücken Sie im Zusammenfassungsfenster **Fertig stellen**.

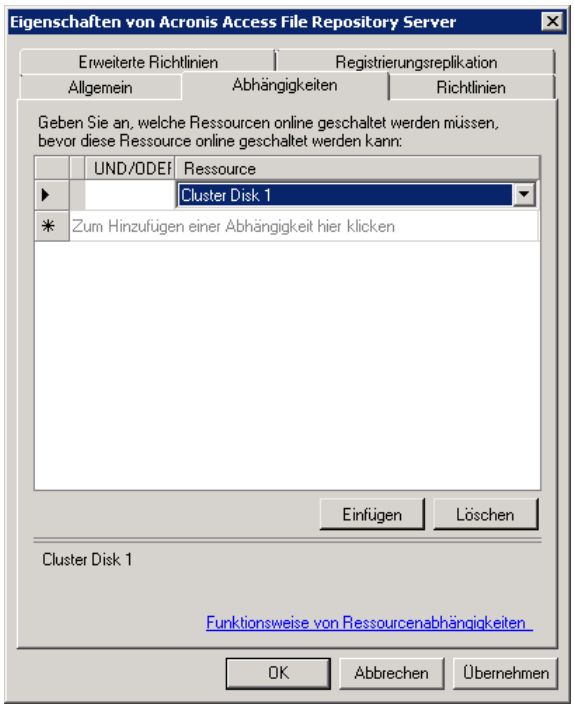
Abhängigkeiten konfigurieren

1. Doppelklicken Sie auf die Acronis Access Dienstgruppe.

Führen Sie für PostgreSQL und das Acronis Access Datei-Repository-Dienste Folgendes durch:

1. Klicken Sie mit der rechten Maustaste auf den entsprechenden Dienst und wählen Sie **Eigenschaften**.
2. Klicken Sie auf die Registerkarte **Abhängigkeiten**.

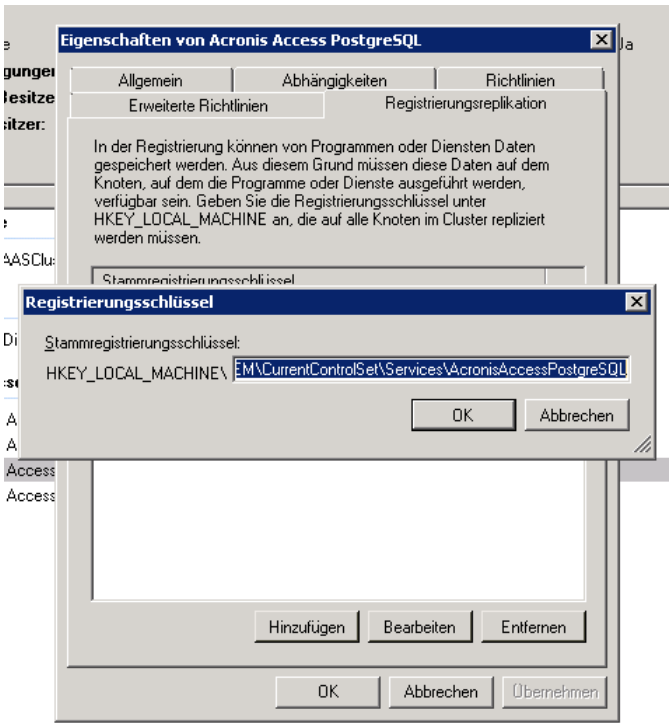
3. Klicken Sie auf **Ressource** und wählen Sie das freigegebene Laufwerk aus, das Sie hinzugefügt haben.



4. Drücken Sie **Anwenden** und schließen Sie das Fenster.

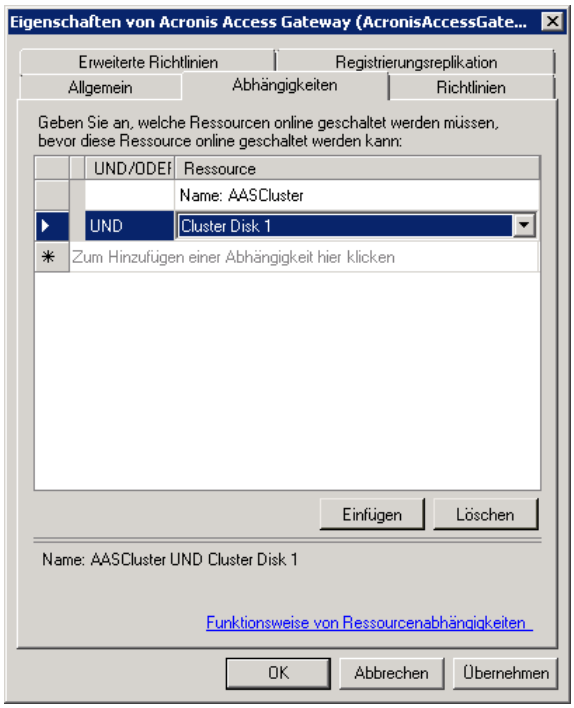
Führen Sie für PostgreSQL außerdem Folgendes aus:

1. Klicken Sie auf die Registerkarte **Registrierungsreplikation**.
2. Drücken Sie **Hinzufügen** und geben Sie Folgendes ein: **`SYSTEM\CurrentControlSet\Services\AcronisAccessPostgreSQL\`**(Für ältere Versionen von Acronis Access kann der Service unterschiedlich sein, z. B. **postgresql-x64-9.2**)



Führen Sie für den Acronis Access Gateway Server-Dienst Folgendes aus:

1. Klicken Sie mit der rechten Maustaste auf den entsprechenden Dienst und wählen Sie **Eigenschaften**.
2. Klicken Sie auf die Registerkarte **Abhängigkeiten**.
3. Klicken Sie auf **Ressource** und wählen Sie das freigegebene Laufwerk aus, das Sie hinzugefügt haben, sowie den **Netzwerknamen** (der zugleich der Name des Clientzugriffspunkts ist).

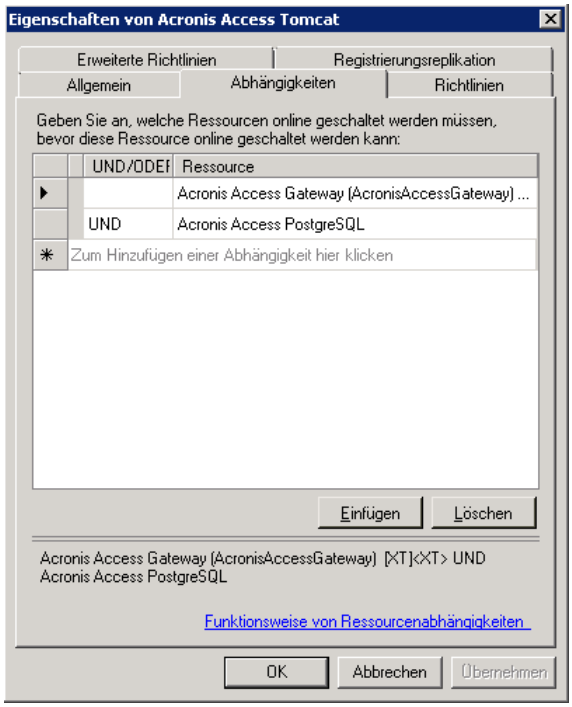


4. Drücken Sie **Anwenden** und schließen Sie das Fenster.

Führen Sie für den Acronis Access Tomcat-Dienst Folgendes aus:

1. Klicken Sie mit der rechten Maustaste auf den entsprechenden Dienst und wählen Sie **Eigenschaften**.
2. Klicken Sie auf die Registerkarte **Abhängigkeiten**.

3. Klicken Sie auf **Ressource** und wählen Sie die PostgreSQL und Acronis Access Gateway Server-Dienste als Abhängigkeiten aus. Drücken Sie **Anwenden** und schließen Sie das Fenster.

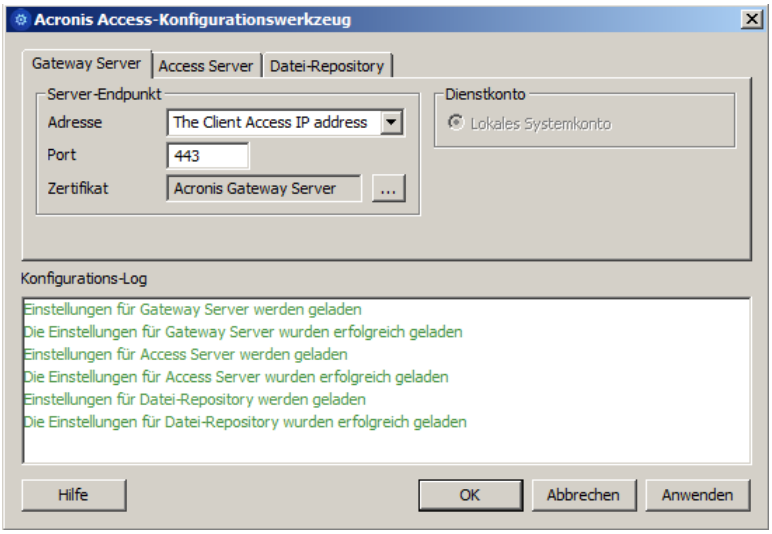


Hinweis: *Wenn die Gateway und Access Server auf verschiedenen IP-Adressen ausgeführt werden sollen, fügen Sie die zweite IP-Adresse der Acronis Access Dienstgruppe als Ressource hinzu und legen Sie sie als Abhängigkeit für den Netzwerknamen fest.*

Dienstgruppe online schalten und Konfigurationswerkzeug verwenden

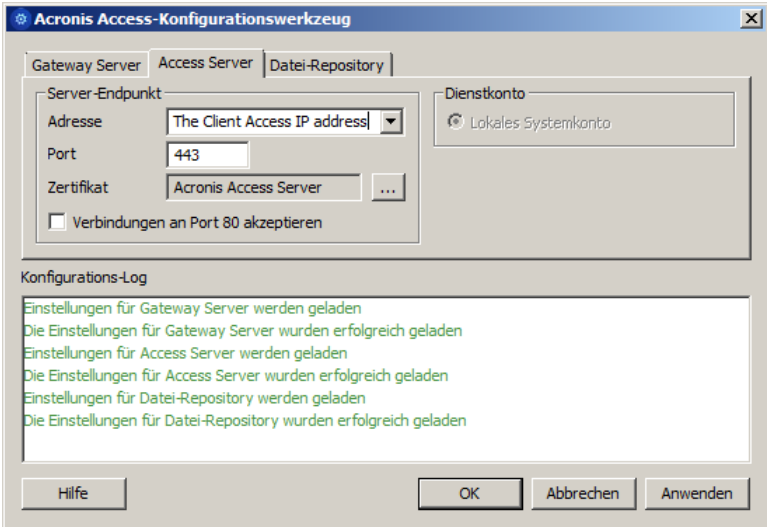
1. Klicken Sie mit der rechten Maustaste auf die Acronis Access Dienstgruppe und wählen Sie **Diese Anwendung oder Dienstgruppe online schalten**.
2. Starten Sie das Konfigurationswerkzeug.
   - Bei einer Neuinstallation befindet sich dies normalerweise unter **`C:\Program Files (x86)\Acronis\Access\Configuration Utility`**
   - Bei einem Upgrade von mobilEcho befindet es sich normalerweise unter **`C:\Program Files (x86)\GroupLogic\Configuration Utility`**

3. Konfigurieren Sie den Acronis Access Gateway Server-Dienst, um die IP-Adresse(n) für die Acronis Access Dienstgruppe abzuhören.

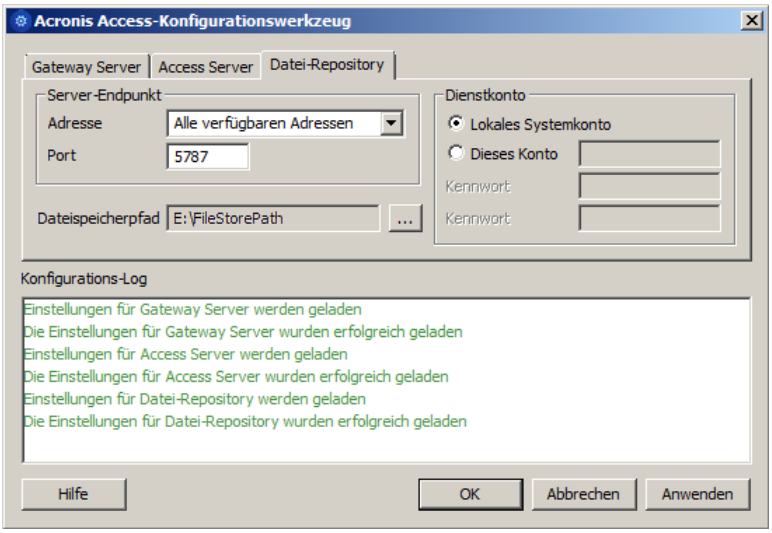


4. Konfigurieren Sie den Acronis Access Server-Dienst, um die IP-Adresse(n) für die Acronis Access Dienstgruppe abzuhören.

Hinweis: *Wenn* ***Verbindungen an Port 80 akzeptieren*** *ausgewählt ist, hört Tomcat den unsicheren Port 80 auf eingehenden Datenverkehr hin ab und leitet ihn zum HTTPS-Port um, den Sie zuvor festgelegt haben.*



5. Konfigurieren Sie das Acronis Access Datei-Repository, um 'localhost' abzuhören, und ändern Sie den Dateispeicherpfad in ein Verzeichnis auf dem freigegebenen Laufwerk. Dieser Pfad sollte für beide Knoten gleich sein.



6. Klicken Sie auf **OK**, um die Konfiguration abzuschließen, und starten Sie die Dienste neu.

Installation und Konfiguration auf dem zweiten Knoten

1. Deaktivieren Sie alle vorhandenen Virenschutzprogramme, da sie unter Umständen den Installationsvorgang unterbrechen und somit eine fehlerhafte Installation verursachen können.
2. Installieren Sie Acronis Access auf dem zweiten Knoten, verwenden Sie jedoch diesmal den Standardspeicherort für **Postgres Data** sowie dasselbe postgres-Benutzerkennwort wie für den ersten Knoten.
3. Schließen Sie die Installation ab.
4. Konfigurieren Sie die Gateway Server-Datenbank, sodass sie sich auf einem freigegebenen Laufwerk befindet.
   a. Navigieren Sie zu **`C:\Program Files (x86)\Acronis\Access\Gateway Server\`**
      - Bei einem Upgrade lautet der Pfad: **`C:\Program Files (x86)\GroupLogic\mobilEcho Server\`**
   b. Suchen Sie die Datei **database.yml** und öffnen Sie sie mit einem Texteditor.
   c. Gehen Sie zu dieser Zeile: **`database_path: './database/'`** und ersetzen Sie **./database/** durch den gewünschten Pfad (z.B. **`database_path: 'S:/mobilEcho_cluster/database/'`**).

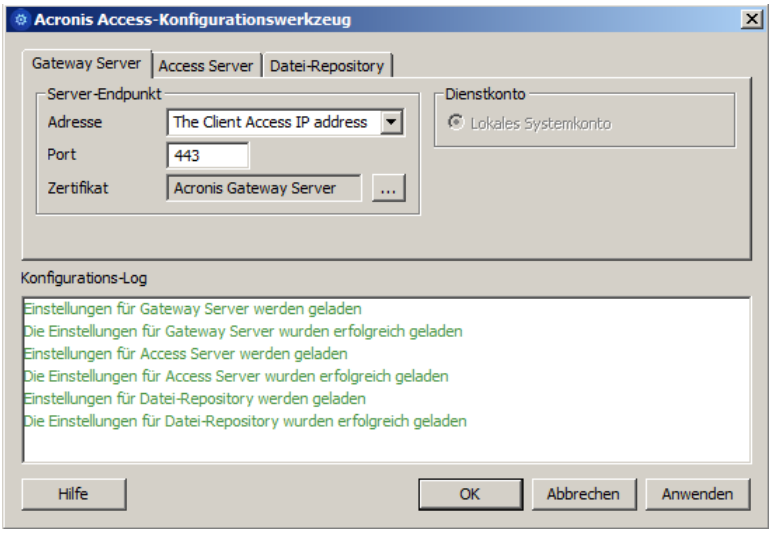
   Hinweis: *Verwenden Sie als Pfadtrennzeichen Schrägstriche (/).*

   Hinweis: *Sie können die konfigurierte Datei 'database.yml' aus dem ersten Knoten kopieren und im zweiten Knoten einfügen.*

   Hinweis: *Der Pfad sollte mit dem Pfad auf dem ersten Knoten übereinstimmen.*
5. Verschieben Sie die Acronis Access Dienstgruppe in den zweiten Knoten. Klicken Sie dazu mit der rechten Maustaste auf die Dienstgruppe und klicken Sie auf **In den zweiten Knoten verschieben**.
6. Starten Sie das Konfigurationswerkzeug.

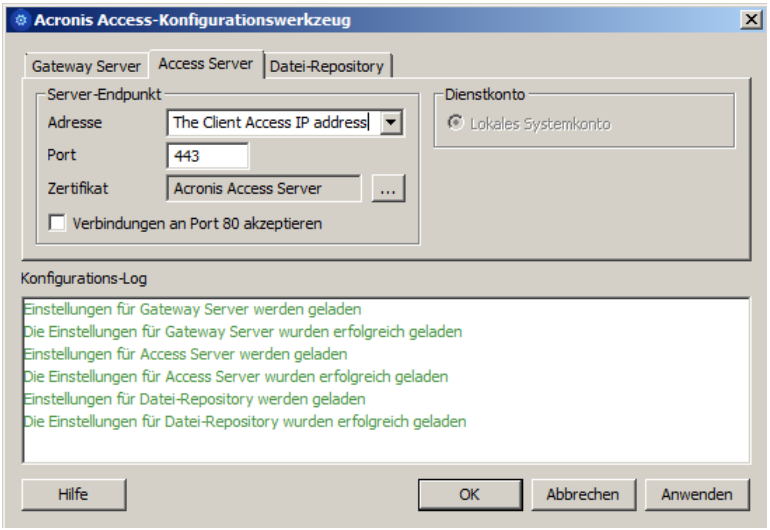
- Bei einer Neuinstallation befindet sich dies normalerweise unter **`C:\Program Files (x86)\Acronis\Access\Configuration Utility`**
- Bei einem Upgrade von mobilEcho befindet es sich normalerweise unter **`C:\Program Files (x86)\GroupLogic\Configuration Utility`**

7. Konfigurieren Sie den Acronis Access Gateway Server-Dienst, um die IP-Adresse(n) für die Acronis Access Dienstgruppe abzuhören.

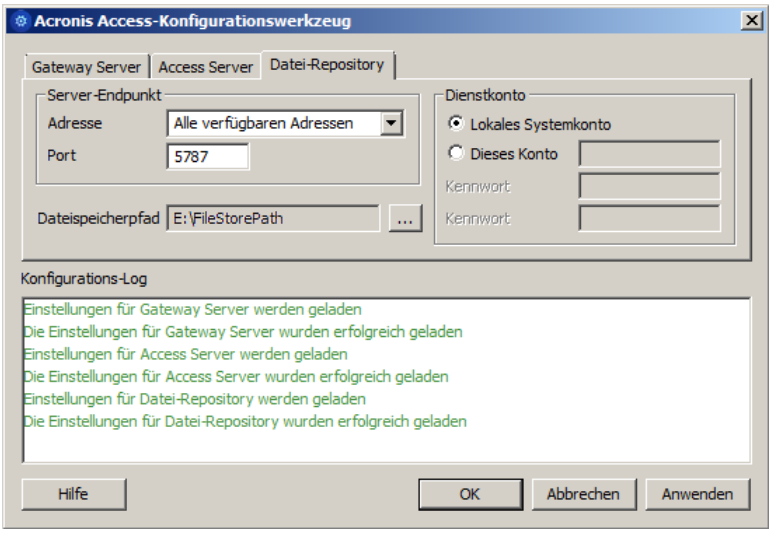


8. Konfigurieren Sie den Acronis Access Server-Dienst, um die IP-Adresse(n) für die Acronis Access Dienstgruppe abzuhören.

Hinweis: *Wenn* ***Verbindungen an Port 80 akzeptieren*** *ausgewählt ist, hört Tomcat den unsicheren Port 80 auf eingehenden Datenverkehr hin ab und leitet ihn zum HTTPS-Port um, den Sie zuvor festgelegt haben.*



9. Konfigurieren Sie das Acronis Access Datei-Repository, um 'localhost' abzuhören, und ändern Sie den Dateispeicherpfad in ein Verzeichnis auf dem freigegebenen Laufwerk. Dieser Pfad sollte für beide Knoten gleich sein.



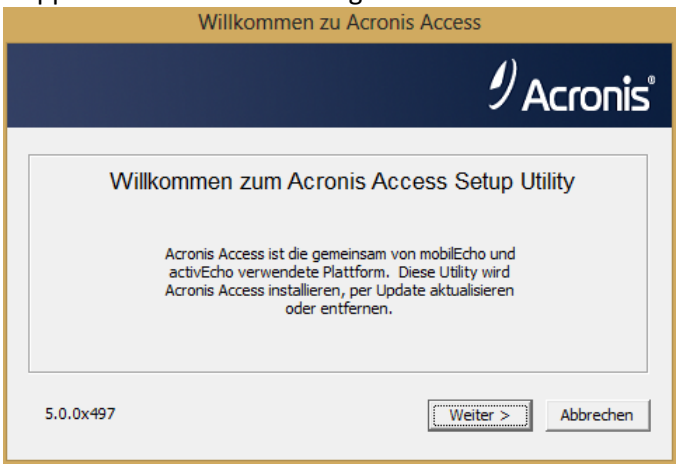
10. Klicken Sie auf **OK**, um die Konfiguration abzuschließen, und starten Sie die Dienste neu.

7.2.3 Acronis Access auf einem Microsoft Windows 2012 Failover Cluster installieren

Acronis Access installieren

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

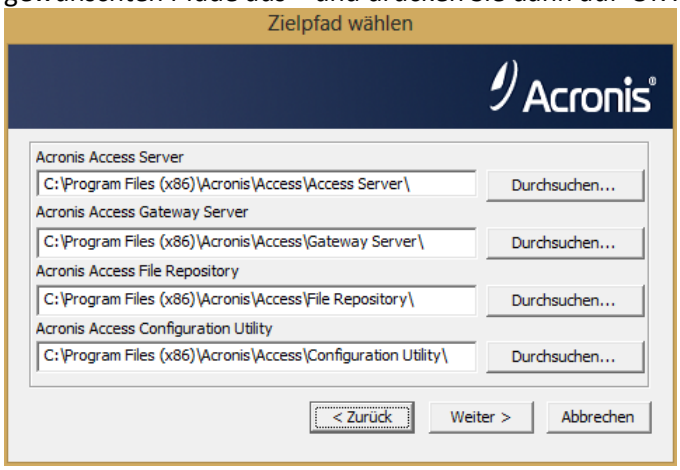
1. Laden Sie das Installationsprogramm für Acronis Access herunter.
2. Deaktivieren Sie alle vorhandenen Virenschutzprogramme, da sie unter Umständen den Installationsvorgang unterbrechen und somit eine fehlerhafte Installation verursachen können.
3. Doppelklicken Sie auf die Programmdatei des Installationsprogramms.



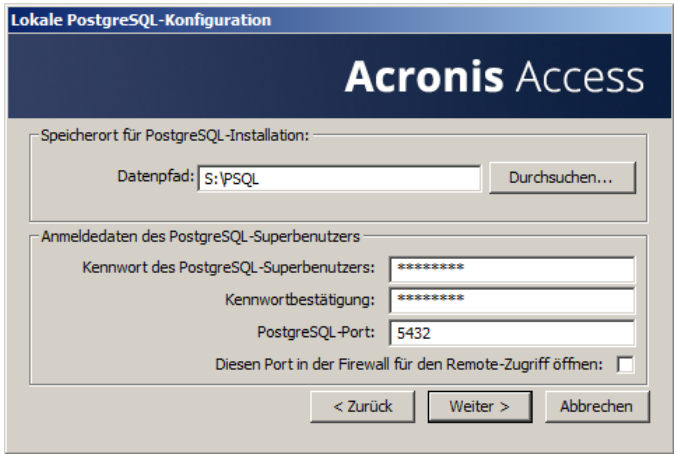
4. Klicken Sie auf **Weiter**, um zu beginnen.
5. Lesen und akzeptieren Sie die Lizenzvereinbarung.
6. Drücken Sie **Installieren**.

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. Wählen Sie auf einem freigegebenen Laufwerk einen Speicherort für den Ordner **Postgres Data** und drücken Sie **Weiter**.



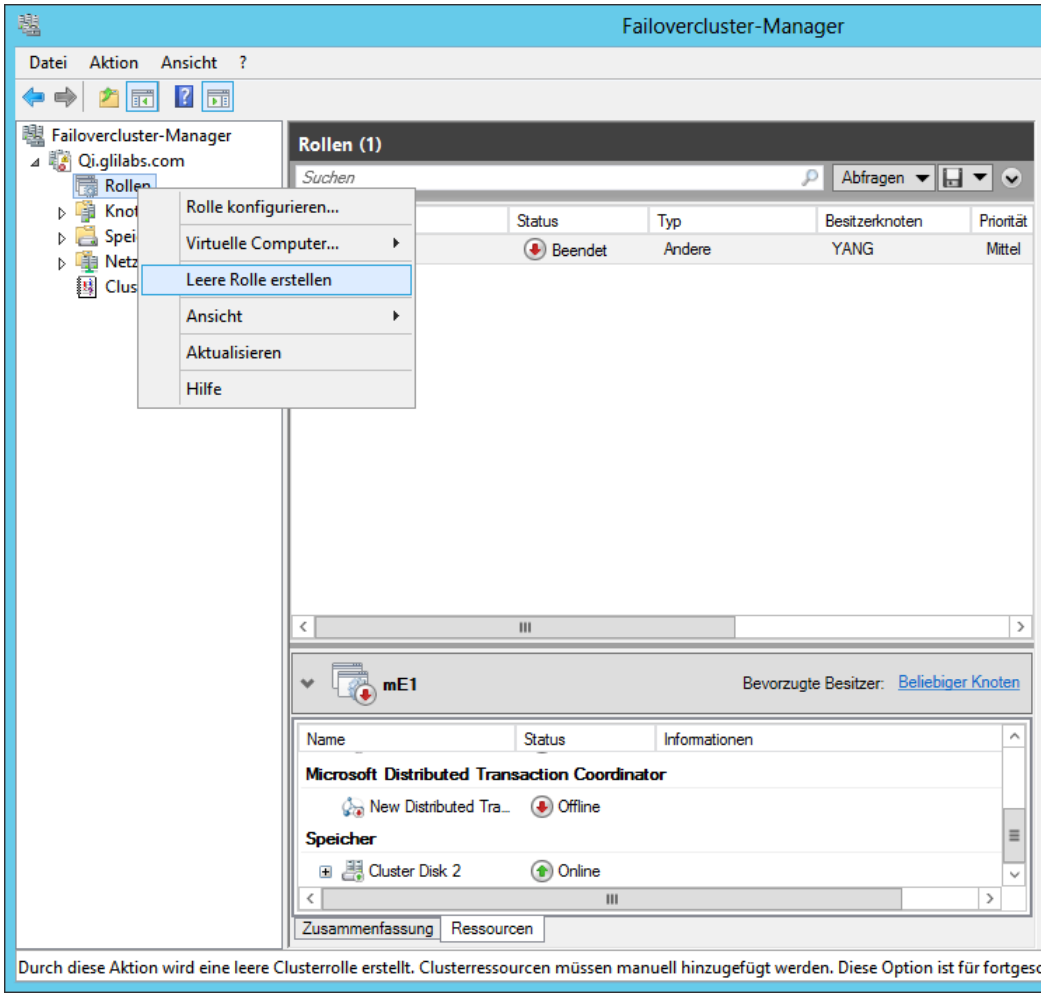
10. Es wird ein Fenster angezeigt, in dem alle zu installierenden Komponenten aufgelistet sind. Drücken Sie **OK**, um fortzufahren.

Wenn der Installationsvorgang für Acronis Access abgeschlossen ist, drücken Sie **Beenden**.

Rolle erstellen

1. Öffnen Sie die **Failover-Clusterverwaltung** und klicken Sie mit der rechten Maustaste auf **Rollen**.

2. Wählen Sie **Leere Rolle erstellen**. Geben Sie der Rolle einen geeigneten Namen (z.B. Acronis Access, AAS Cluster).



Konfigurationen auf dem aktiven Knoten

1. Konfigurieren Sie die Gateway Server-Datenbank, sodass sie sich auf einem freigegebenen Laufwerk befindet.
   a. Navigieren Sie zu **`C:\Program Files (x86)\Acronis\Access\Gateway Server\`**
      - Bei einem Upgrade lautet der Pfad: **`C:\Program Files (x86)\GroupLogic\mobilEcho Server\`**
   b. Suchen Sie die Datei **database.yml** und öffnen Sie sie mit einem Texteditor.
   c. Gehen Sie zu dieser Zeile: **`database_path: './database/'`** und ersetzen Sie **./database/** durch den gewünschten Pfad (z.B. **`database_path: 'S:/mobilEcho_cluster/database/'`**).

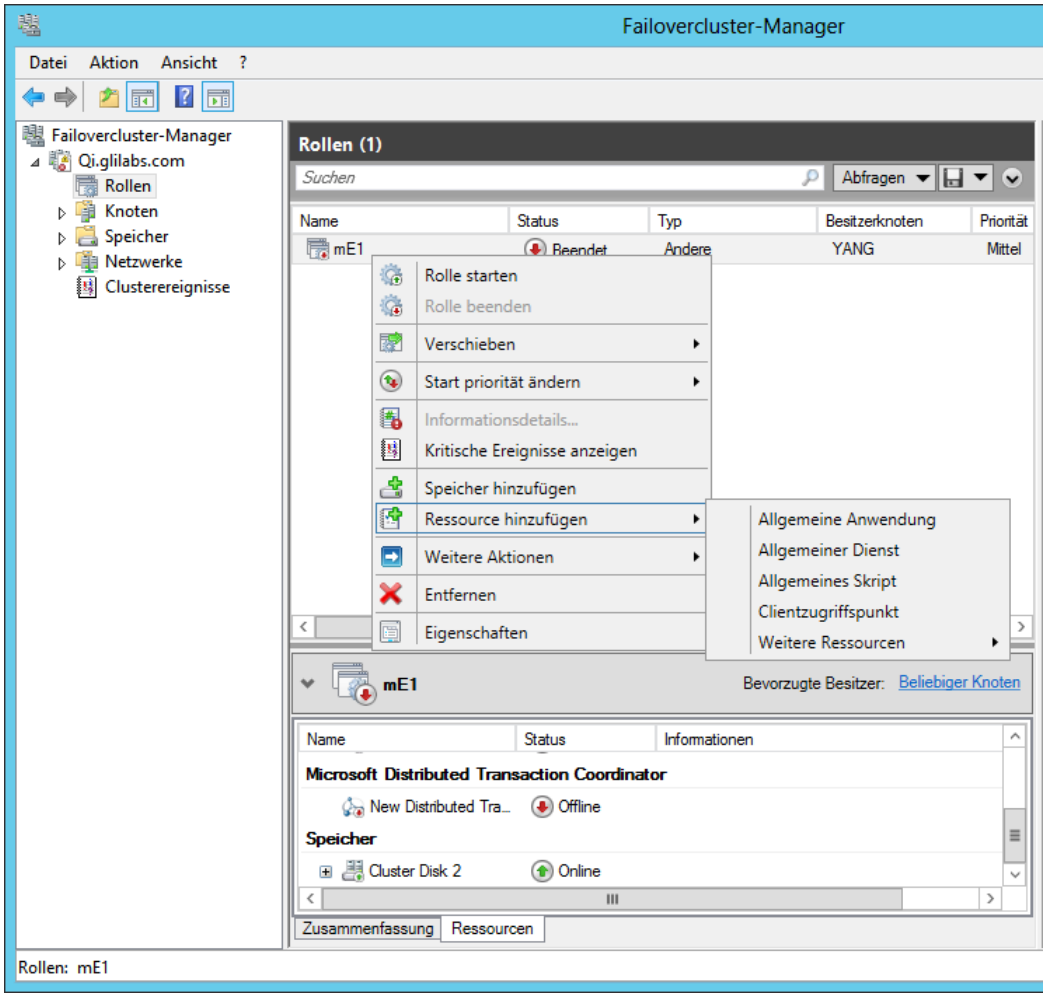
Hinweis: *Verwenden Sie als Pfadtrennzeichen Schrägstriche (/).*

Hinweis: *Sie können die konfigurierte Datei 'database.yml' aus dem ersten Knoten kopieren und im zweiten Knoten einfügen.*

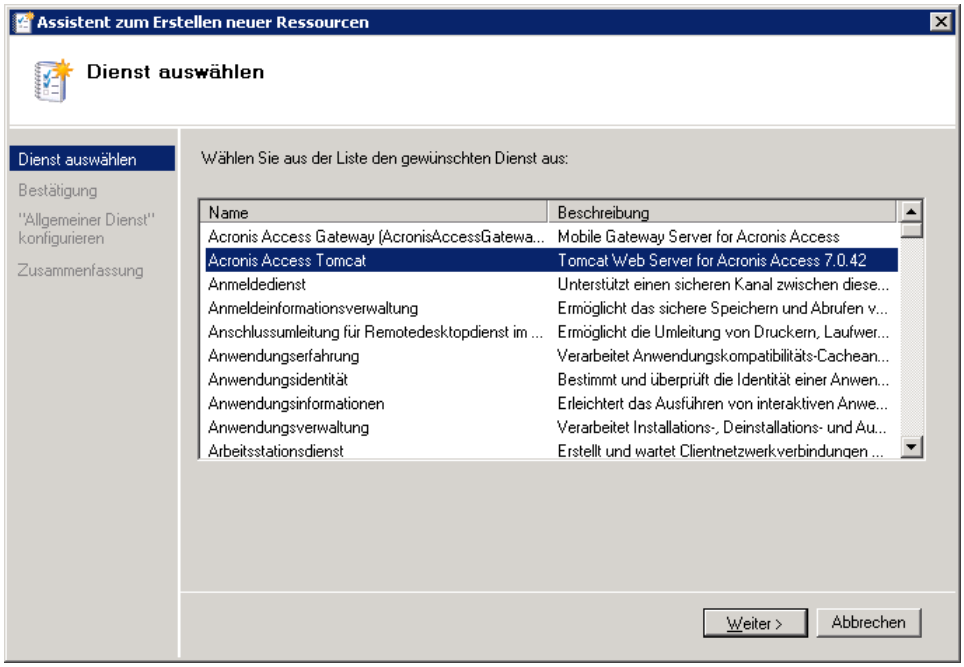
Alle erforderlichen Dienste der Acronis Access Rolle hinzufügen

Führen Sie das folgende Verfahren für die einzelnen Dienste aus: AcronisAccessGateway, AcronisAccessPostgreSQL (abhängig von der Acronis Access-Version), AcronisAccessRepository und AcronisAccessTomcat.

1. Klicken Sie mit der rechten Maustaste auf die Acronis Access Rolle und wählen Sie **Ressource hinzufügen**.
2. Wählen Sie **Allgemeiner Dienst** aus.



3. Wählen Sie den geeigneten Dienst aus und drücken Sie **Weiter**.

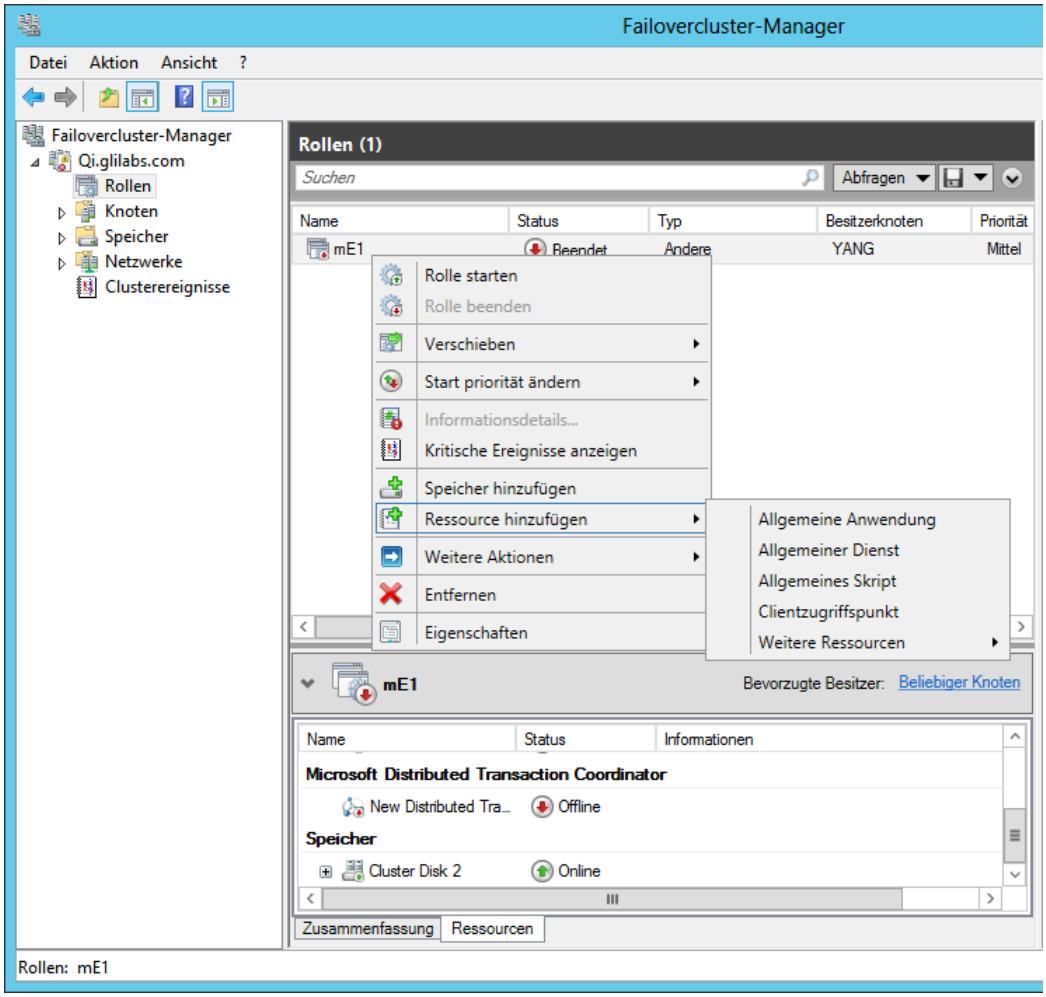


4. Drücken Sie im Bestätigungsfenster **Weiter**.
5. Drücken Sie im Zusammenfassungsfenster **Fertig stellen**.

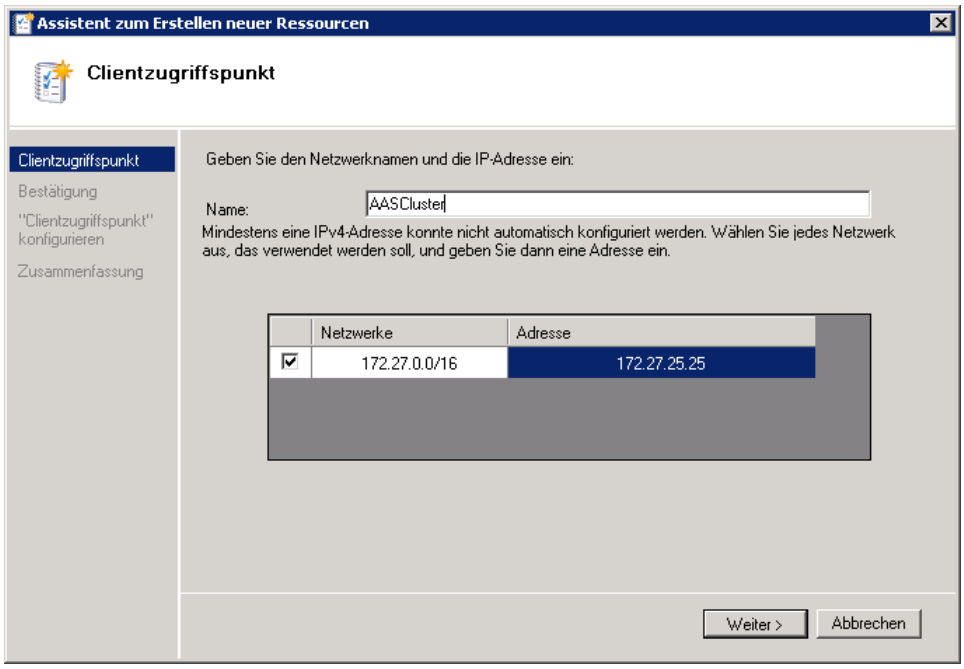
Zugriffspunkt festlegen

1. Klicken Sie mit der rechten Maustaste auf die Acronis Access Rolle und wählen Sie **Ressource hinzufügen**.

2. Wählen Sie **Clientzugriffspunkt** aus.



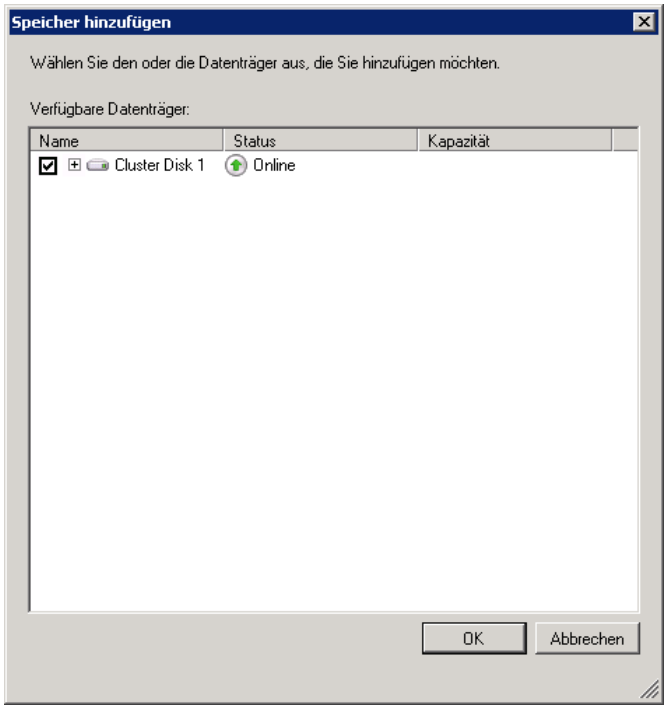
3. Geben Sie einen Namen für diesen Zugriffspunkt ein.
4. Wählen Sie ein Netzwerk.



5. Geben Sie die IP-Adresse ein und drücken Sie **Weiter**.
6. Drücken Sie im Bestätigungsfenster **Weiter**.
7. Drücken Sie im Zusammenfassungsfenster **Fertig stellen**.

Freigegebenes Laufwerk hinzufügen

1. Klicken Sie mit der rechten Maustaste auf die Acronis Access Rolle und wählen Sie **Speicher hinzufügen**.
2. Wählen Sie das gewünschte freigegebene Laufwerk aus.



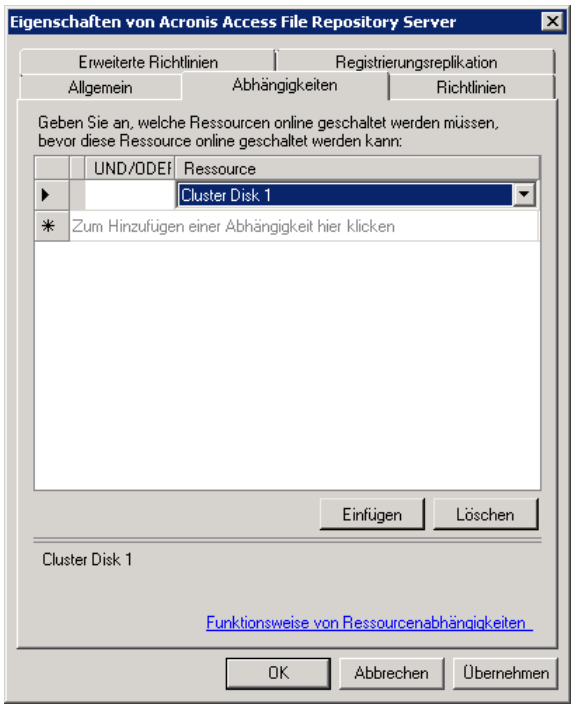
Abhängigkeiten konfigurieren

1. Wählen Sie die Acronis Access Rolle aus und klicken Sie auf die Registerkarte **Ressourcen**.

Führen Sie für PostgreSQL und das Acronis Access Datei-Repository-Dienste Folgendes durch:

1. Klicken Sie mit der rechten Maustaste auf den entsprechenden Dienst und wählen Sie **Eigenschaften**.
2. Klicken Sie auf die Registerkarte **Abhängigkeiten**.

3. Klicken Sie auf **Ressource** und wählen Sie das freigegebene Laufwerk aus, das Sie hinzugefügt haben.

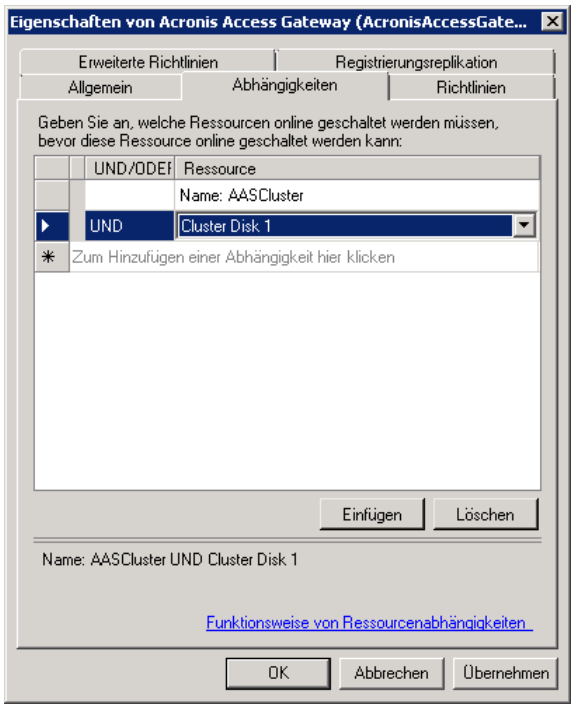


4. Drücken Sie **Anwenden** und schließen Sie das Fenster.

Führen Sie für den Acronis Access Gateway Server-Dienst Folgendes durch:

1. Klicken Sie mit der rechten Maustaste auf den entsprechenden Dienst und wählen Sie **Eigenschaften**.
2. Klicken Sie auf die Registerkarte **Abhängigkeiten**.

3. Klicken Sie auf **Ressource** und wählen Sie das freigegebene Laufwerk aus, das Sie hinzugefügt haben, sowie den **Netzwerknamen** (der zugleich der Name des Clientzugriffspunkts ist).

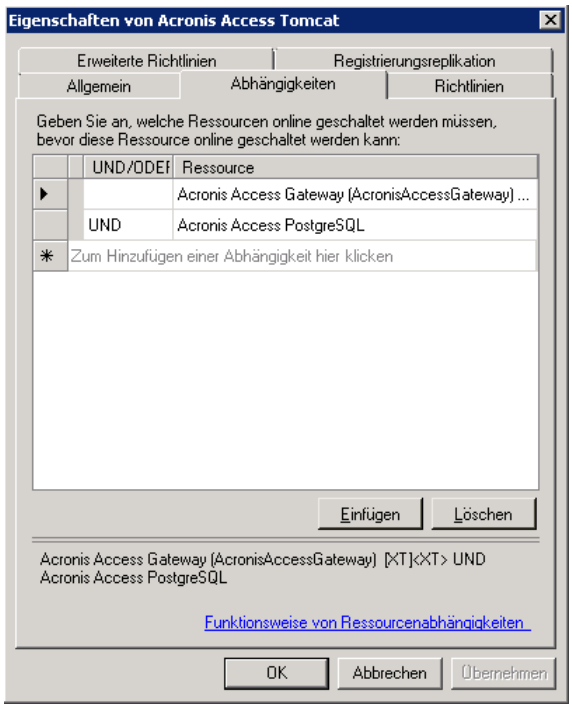


4. Drücken Sie **Anwenden** und schließen Sie das Fenster.

Führen Sie für den Acronis Access Tomcat-Dienst Folgendes durch:

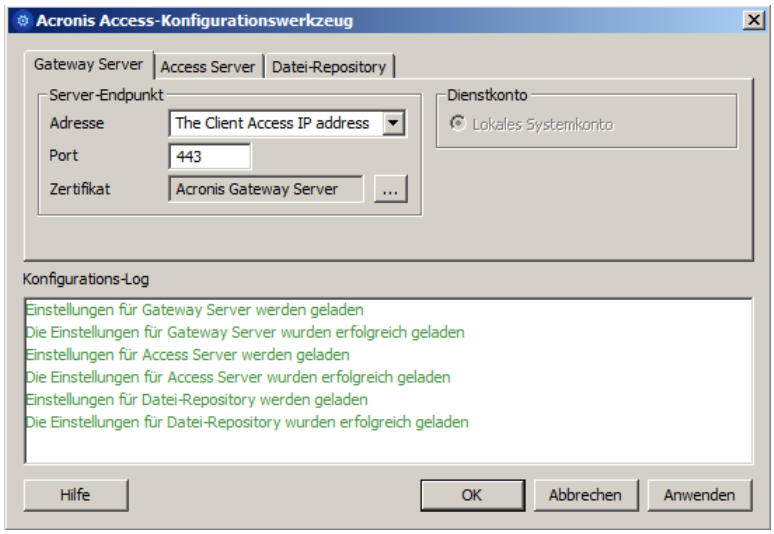
1. Klicken Sie mit der rechten Maustaste auf den entsprechenden Dienst und wählen Sie **Eigenschaften**.
2. Klicken Sie auf die Registerkarte **Abhängigkeiten**.
3. Klicken Sie auf **Ressource** und wählen Sie die PostgreSQL und Acronis Access Gateway Server-Dienste als Abhängigkeiten aus. Drücken Sie **Anwenden** und schließen Sie das Fenster.

Hinweis: *Wenn die Gateway und Access Server unter verschiedenen IP-Adressen ausgeführt werden sollen, fügen Sie die zweite IP-Adresse der Acronis Access Rolle als Ressource hinzu und legen Sie sie als Abhängigkeit für den Netzwerknamen fest.*



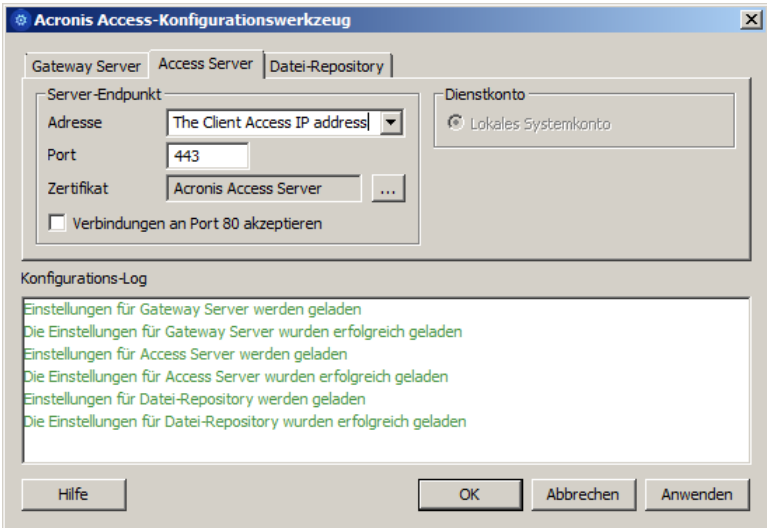
Rolle starten und Konfigurationswerkzeug verwenden

1. Klicken Sie mit der rechten Maustaste auf die Acronis Access Rolle und drücken Sie **Rolle starten**.
2. Starten Sie das Konfigurationswerkzeug.
   - Bei einer Neuinstallation befindet sich dies normalerweise unter **`C:\Program Files (x86)\Acronis\Access\Configuration Utility`**
   - Bei einem Upgrade von mobilEcho befindet es sich normalerweise unter **`C:\Program Files (x86)\GroupLogic\Configuration Utility`**
3. Konfigurieren Sie den Acronis Access Gateway Server-Dienst, um die IP-Adresse(n) für die Acronis Access Dienstgruppe abzuhören.

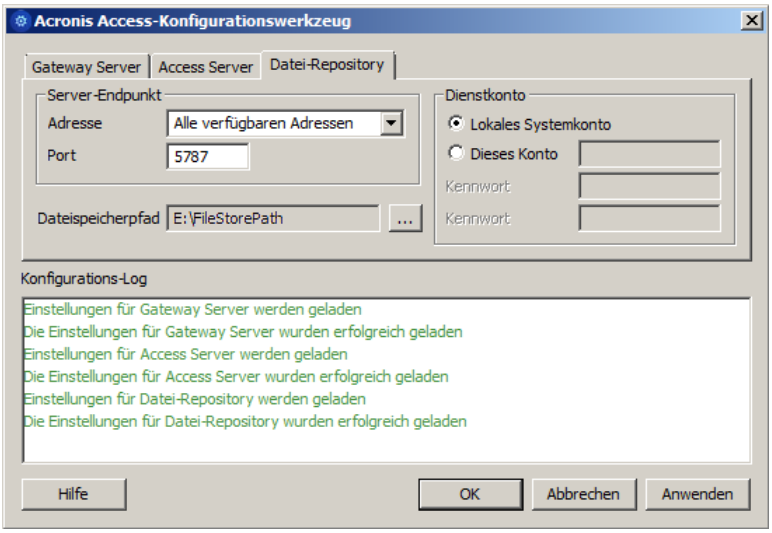


4. Konfigurieren Sie den Acronis Access Server-Dienst, um die IP-Adresse(n) für die Acronis Access Dienstgruppe abzuhören.

Hinweis: *Wenn* ***Verbindungen an Port 80 akzeptieren*** *ausgewählt ist, hört Tomcat den unsicheren Port 80 auf eingehenden Datenverkehr hin ab und leitet ihn zum HTTPS-Port um, den Sie zuvor festgelegt haben.*



5. Konfigurieren Sie das Acronis Access Datei-Repository, um 'localhost' abzuhören, und ändern Sie den Dateispeicherpfad in ein Verzeichnis auf dem freigegebenen Laufwerk. Dieser Pfad sollte für beide Knoten gleich sein.



6. Klicken Sie auf **OK**, um die Konfiguration abzuschließen, und starten Sie die Dienste neu.

Installation und Konfiguration auf dem zweiten Knoten

1. Deaktivieren Sie alle vorhandenen Virenschutzprogramme, da sie unter Umständen den Installationsvorgang unterbrechen und somit eine fehlerhafte Installation verursachen können.
2. Installieren Sie Acronis Access auf dem zweiten Knoten, verwenden Sie jedoch diesmal den Standardspeicherort für **Postgres Data** sowie dasselbe postgres-Benutzerkennwort wie für den ersten Knoten.
3. Schließen Sie die Installation ab.
4. Konfigurieren Sie die Gateway Server-Datenbank, sodass sie sich auf einem freigegebenen Laufwerk befindet.

a. Navigieren Sie zu **`C:\Program Files (x86)\Acronis\Access\Gateway Server\`**
   - Bei einem Upgrade lautet der Pfad: **`C:\Program Files (x86)\GroupLogic\mobilEcho Server\`**

b. Suchen Sie die Datei **database.yml** und öffnen Sie sie mit einem Texteditor.

c. Gehen Sie zu dieser Zeile: **`database_path: './database/'`** und ersetzen Sie **./database/** durch den gewünschten Pfad (z.B. **`database_path: 'S:/mobilEcho_cluster/database/'`**).

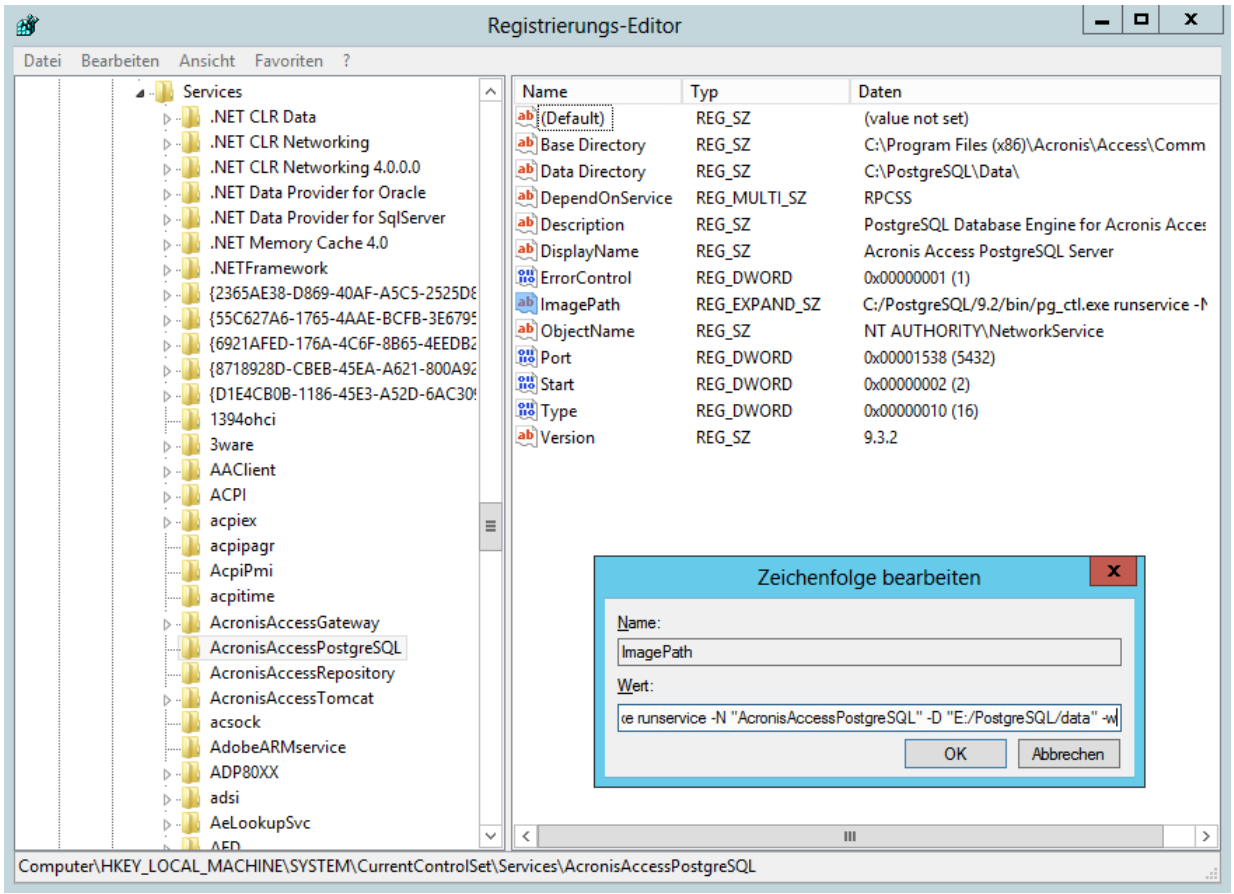
Hinweis: *Verwenden Sie als Pfadtrennzeichen Schrägstriche (/).*

Hinweis: *Sie können die konfigurierte Datei 'database.yml' aus dem ersten Knoten kopieren und im zweiten Knoten einfügen.*

Hinweis: *Der Pfad sollte mit dem Pfad auf dem ersten Knoten übereinstimmen.*

Für PostgreSQL müssen Sie die Registry manuell replizieren:

1. Öffnen Sie **Regedit**.
2. Navigieren Sie zum Eintrag **`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\postgresql-some version\`** und öffnen Sie den folgenden Schlüssel: **ImagePath**
3. Ändern Sie den Wert dieses Schlüssel in: **`-D "The path you selected for the PostgreSQL data location" -w`** (z.B. **`-D "E:/PostgreSQL/data" -w`**)

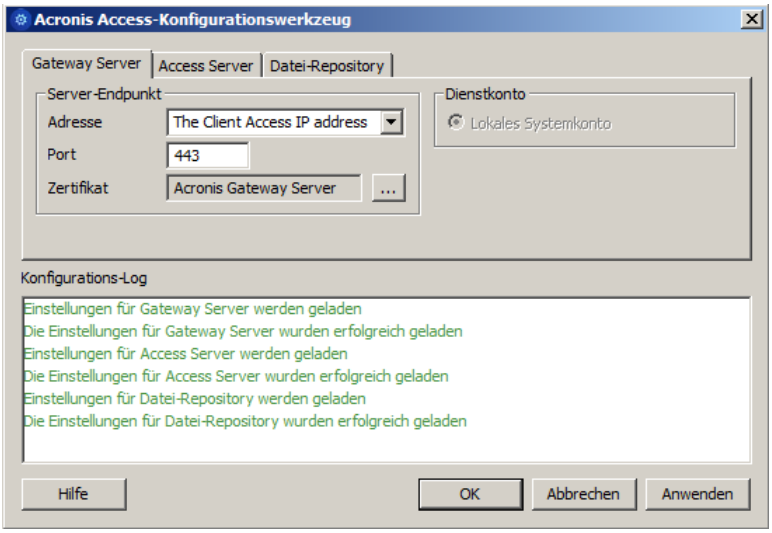


4. Schließen Sie **Regedit** und fahren Sie mit den unten stehenden Schritten fort.

5. Verschieben Sie die Acronis Access Rolle in den zweiten Knoten.

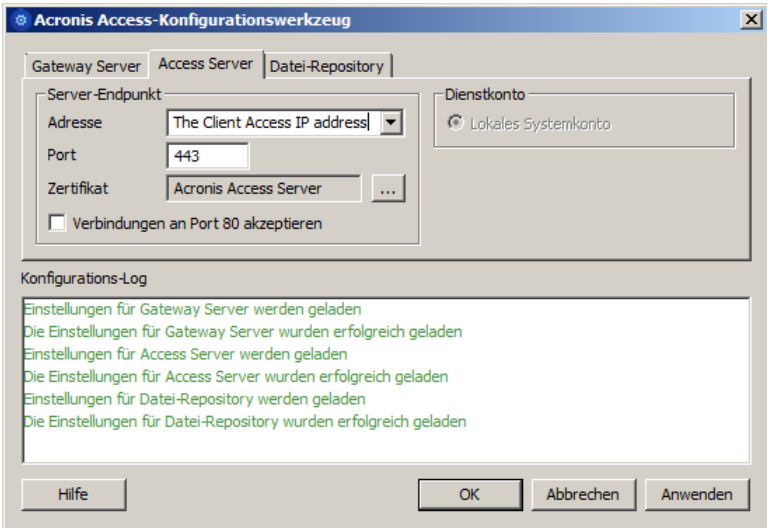
Verwenden des Konfigurationswerkzeugs auf dem zweiten Knoten

1. Starten Sie das Konfigurationswerkzeug.
   - Bei einer Neuinstallation befindet sich dies normalerweise unter **`C:\Program Files (x86)\Acronis\Access\Configuration Utility`**
   - Bei einem Upgrade von mobilEcho befindet es sich normalerweise unter **`C:\Program Files (x86)\GroupLogic\Configuration Utility`**
2. Konfigurieren Sie den Acronis Access Gateway Server-Dienst, um die IP-Adresse(n) für die Acronis Access Dienstgruppe abzuhören.

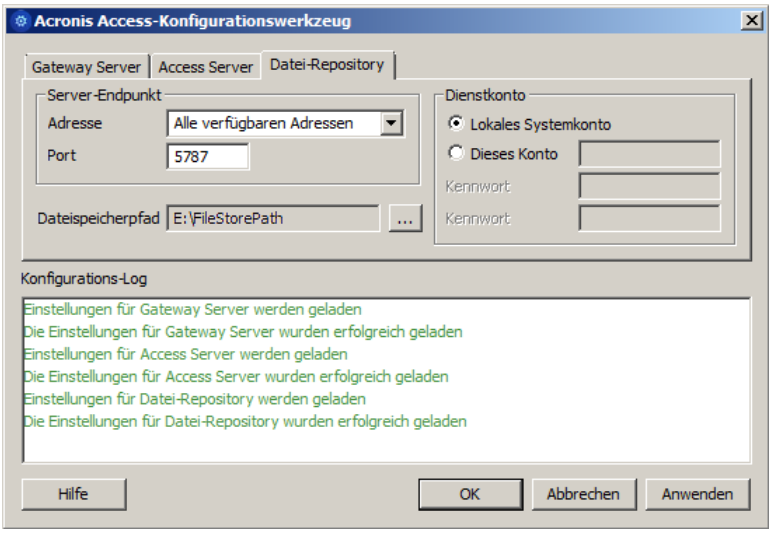


3. Konfigurieren Sie den Acronis Access Server-Dienst, um die IP-Adresse(n) für die Acronis Access Dienstgruppe abzuhören.

Hinweis: *Wenn* ***Verbindungen an Port 80 akzeptieren*** *ausgewählt ist, hört Tomcat den unsicheren Port 80 auf eingehenden Datenverkehr hin ab und leitet ihn zum HTTPS-Port um, den Sie zuvor festgelegt haben.*



4. Konfigurieren Sie das Acronis Access Datei-Repository, um 'localhost' abzuhören, und ändern Sie den Dateispeicherpfad in ein Verzeichnis auf dem freigegebenen Laufwerk. Dieser Pfad sollte für beide Knoten gleich sein.



5. Klicken Sie auf **OK**, um die Konfiguration abzuschließen, und starten Sie die Dienste neu.

7.3 Upgrade von mobilEcho 4.5 in einem Microsoft Failover Cluster

Warnung! *Acronis Access Failover Clustering wird von Versionen vor 5.0.3 nicht unterstützt. Wenn Sie eine ältere Version verwenden, müssen Sie ein Upgrade auf Version 5.0.3 oder höher durchführen, bevor Sie Cluster-Konfigurationen vornehmen können.*

Die unten stehenden Anleitungen enthalten Informationen für das Upgrade Ihres Clusters von mobilEcho auf Acronis Access.

Themen

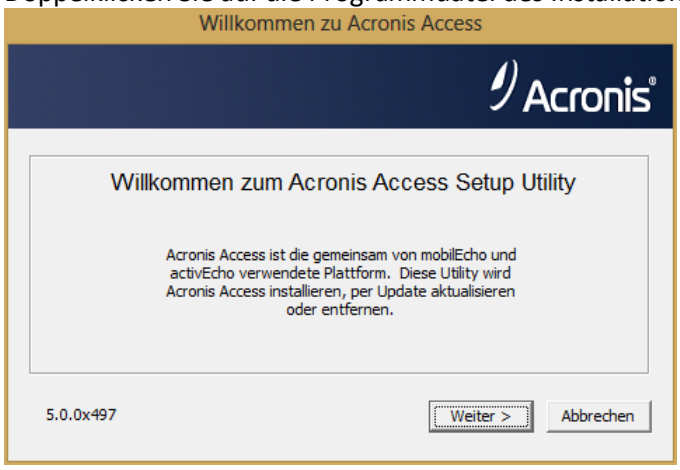
7.3.1 Upgrade eines mobilEcho-Servers auf einem Windows 2003 Failover Cluster auf Acronis Access durchführen

1. Öffnen Sie die **Clusterverwaltung** und doppelklicken Sie auf die Dienstgruppe.
2. Löschen Sie die mobilEcho Dienstressourcen.

   Hinweis: *Schalten Sie nicht die gesamte Cluster-Gruppe offline, sondern löschen Sie nur die mobilEcho Dienstressourcen.*

3. Starten Sie den Installer auf dem aktiven Knoten.

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



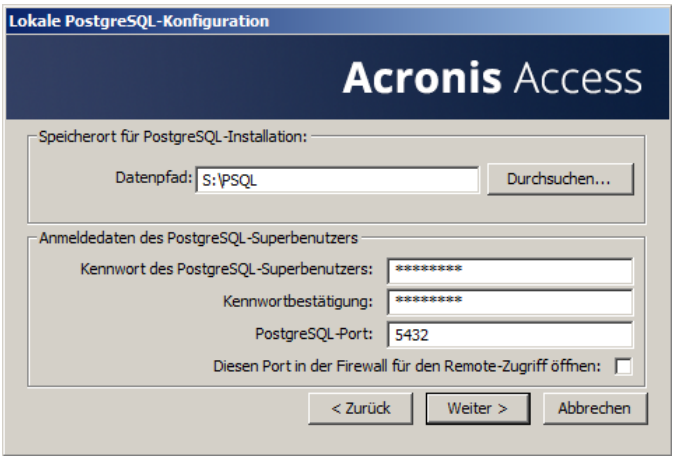
6. Klicken Sie auf **Weiter**, um zu beginnen.
7. Lesen und akzeptieren Sie die Lizenzvereinbarung.
8. Drücken Sie **Installieren**.

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.*

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

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

11. Wählen Sie auf einem freigegebenen Laufwerk einen Speicherort für den Ordner **Postgres Data** und drücken Sie **Weiter**.



12. Es wird ein Fenster angezeigt, in dem alle zu installierenden Komponenten aufgelistet sind. Drücken Sie **OK**, um fortzufahren.
13. Wenn der Installationsvorgang für Acronis Access abgeschlossen ist, drücken Sie **Beenden**.Navigieren Sie zum freigegebenen Laufwerk, und suchen und kopieren Sie die drei folgenden Dateien: **production.sqlite3**, **mobilEcho_manager.cfg** und **priority.txt** (diese ist eventuell nicht vorhanden). Fügen Sie die Dateien in das Acronis Access-Installationsverzeichnis ein, und ersetzen Sie die vorhandenen Dateien.

Hinweis: *Die Dateien, die Sie ersetzen sollen, befinden sich normalerweise im folgenden Verzeichnis:*

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

Konfigurationen auf dem aktiven Knoten

1. Konfigurieren Sie die Gateway Server-Datenbank, sodass sie sich auf einem freigegebenen Laufwerk befindet.
   a. Navigieren Sie zu **`C:\Program Files (x86)\Acronis\Access\Gateway Server\`**
      - Bei einem Upgrade lautet der Pfad: **`C:\Program Files (x86)\GroupLogic\mobilEcho Server\`**
   b. Suchen Sie die Datei **database.yml** und öffnen Sie sie mit einem Texteditor.
   c. Gehen Sie zu dieser Zeile: **`database_path: './database/'`** und ersetzen Sie **./database/** durch den gewünschten Pfad (z.B. **`database_path: 'S:/mobilEcho_cluster/database/'`**).

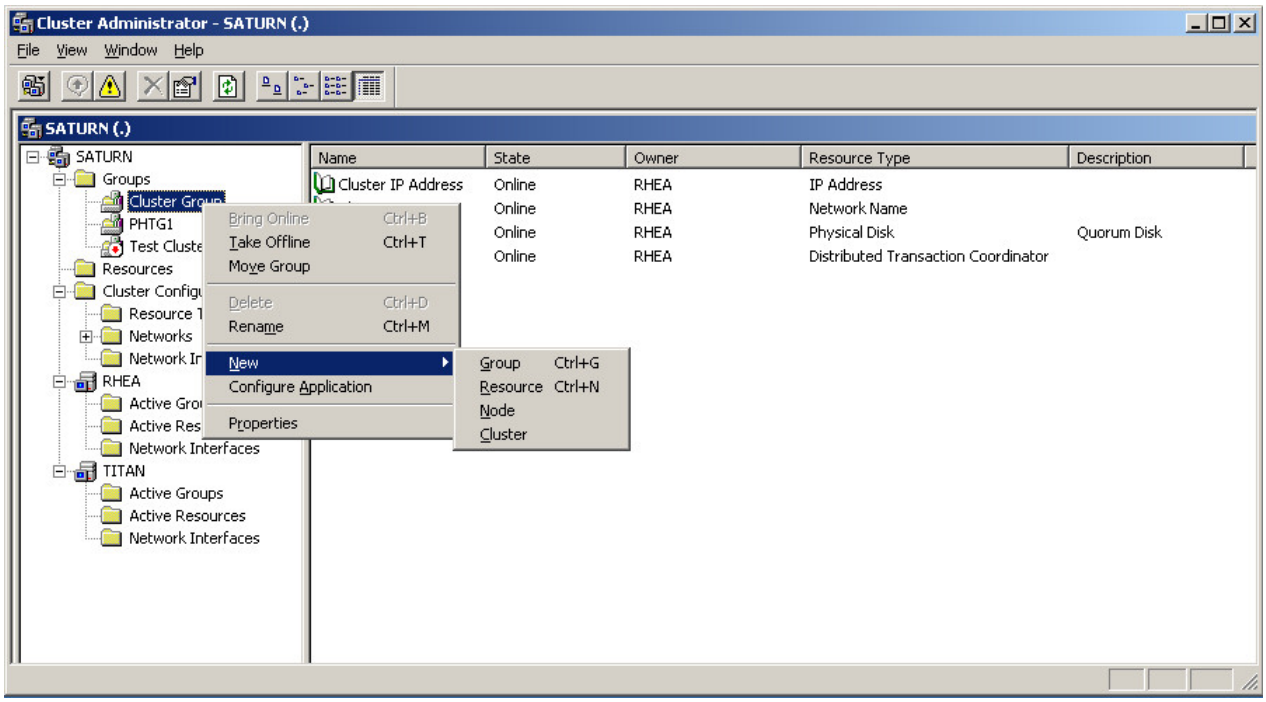
Hinweis: *Verwenden Sie als Pfadtrennzeichen Schrägstriche (/).*

Hinweis: *Sie können die konfigurierte Datei 'database.yml' aus dem ersten Knoten kopieren und im zweiten Knoten einfügen.*

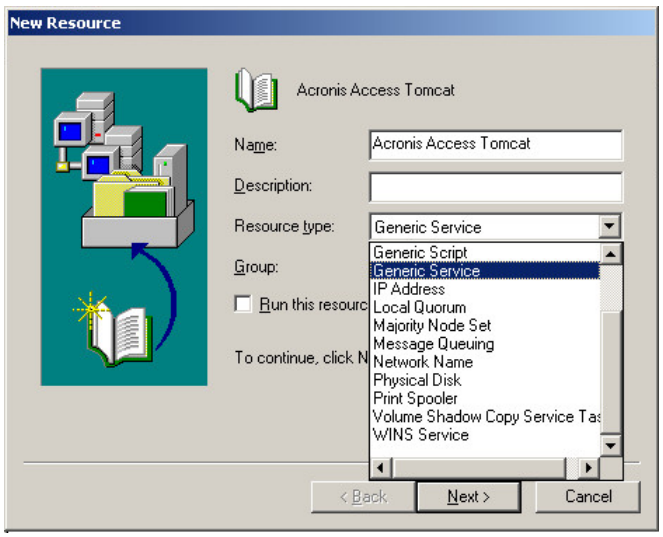
Alle erforderlichen Dienste der Acronis Access Cluster-Gruppe hinzufügen

Führen Sie das folgende Verfahren für die einzelnen Dienste aus: AcronisAccessGateway, AcronisAccessPostgreSQL (abhängig von der Acronis Access-Version), AcronisAccessRepository und AcronisAccessTomcat.

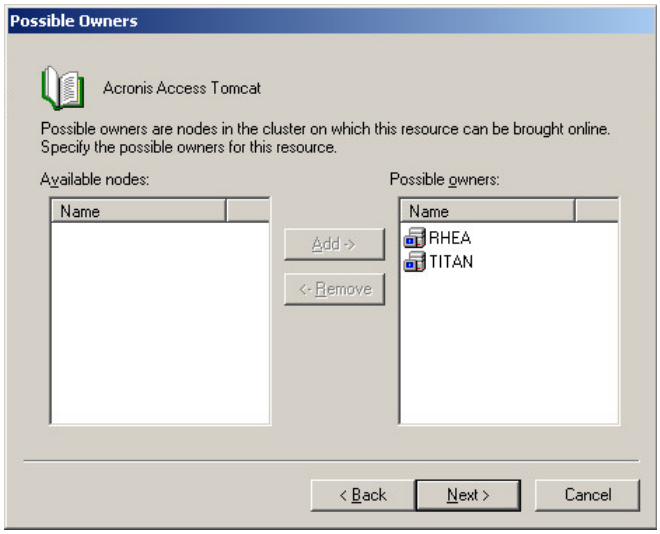
1. Klicken Sie mit der rechten Maustaste auf die Acronis Access Cluster-Gruppe.
2. Öffnen Sie **Neu** und wählen Sie **Ressource**.



3. Geben Sie einen Namen für den Dienst ein und wählen Sie die richtige Cluster-Gruppe aus.
4. Wählen Sie aus dem Dropdown-Menü **Ressourcentyp** die Option **Allgemeiner Dienst** aus und drücken Sie **Weiter**.



5. Stellen Sie sicher, dass beide Knoten als **Mögliche Besitzer** aufgeführt sind und drücken Sie **Weiter**.



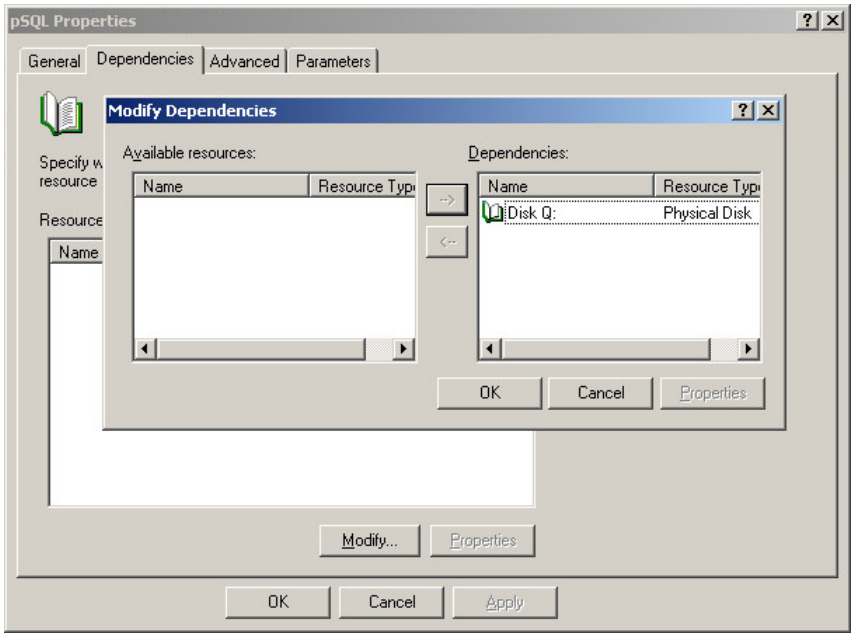
6. Überspringen Sie zunächst die Abhängigkeiten, indem Sie **Weiter** drücken.
7. Geben Sie den richtigen Namen des Dienstes ein, den Sie hinzufügen, (z.B. postgresql-x64-9.2) und drücken Sie **Weiter**.
8. Überspringen Sie zunächst das Fenster **Registrierungsreplikation**, indem Sie auf **Weiter** drücken.
9. Drücken Sie **Fertig stellen**, um den Vorgang abzuschließen.

Abhängigkeiten konfigurieren

Führen Sie für PostgreSQL und das Acronis Access Datei-Repository Folgendes durch:

1. Klicken Sie mit der rechten Maustaste auf den entsprechenden Dienst und wählen Sie **Eigenschaften**.
2. Klicken Sie auf die Registerkarte **Abhängigkeiten**.
3. Klicken Sie auf **Ändern**.

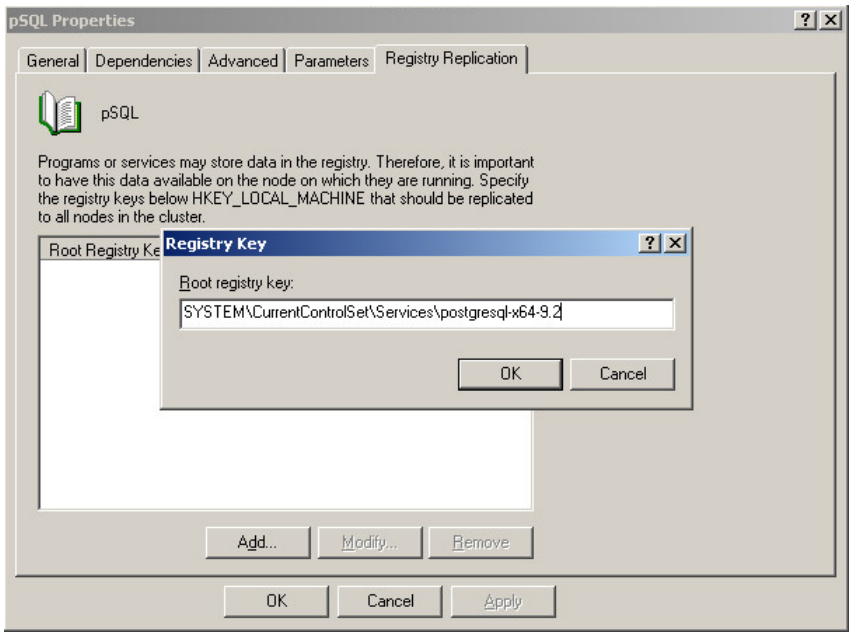
4. Wählen Sie das freigegebene Laufwerk aus, das Sie hinzugefügt haben, und verschieben Sie es nach rechts.



5. Drücken Sie **OK**.

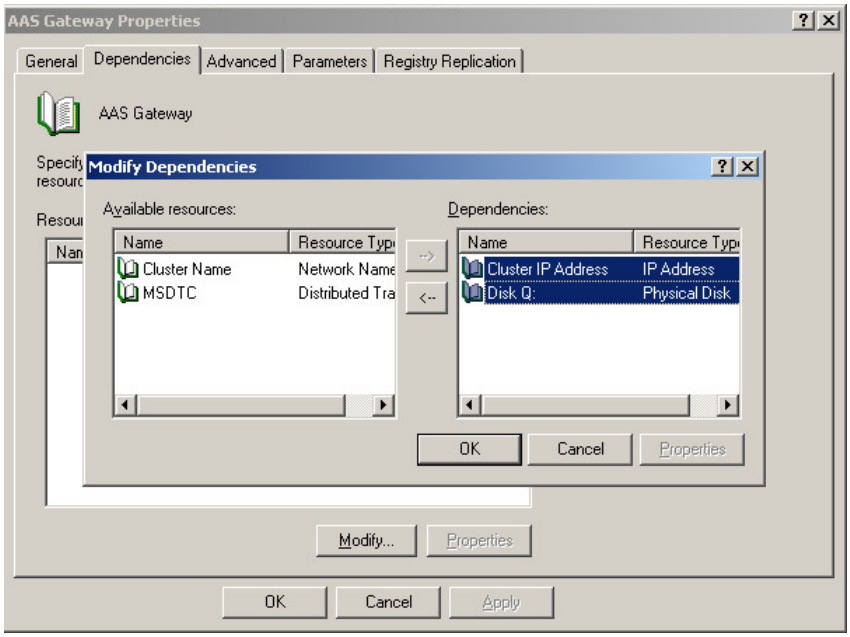
Führen Sie für PostgreSQL zudem Folgendes durch:

1. Klicken Sie auf die Registerkarte **Registrierungsreplikation**.
2. Drücken Sie **Hinzufügen** und geben Sie Folgendes ein: **`SYSTEM\CurrentControlSet\Services\AcronisAccessPostgreSQL\`**(Für ältere Versionen von Acronis Access kann der Service unterschiedlich sein, z. B. **postgresql-x64-9.2**)



Führen Sie für den Acronis Access Gateway Server-Dienst Folgendes durch:

1. Klicken Sie mit der rechten Maustaste auf den entsprechenden Dienst und wählen Sie **Eigenschaften**.
2. Klicken Sie auf die Registerkarte **Abhängigkeiten**.
3. Klicken Sie auf **Ändern**.
4. Wählen Sie die **IP-Adresse** und das **physische Laufwerk** aus und verschieben Sie sie nach rechts.

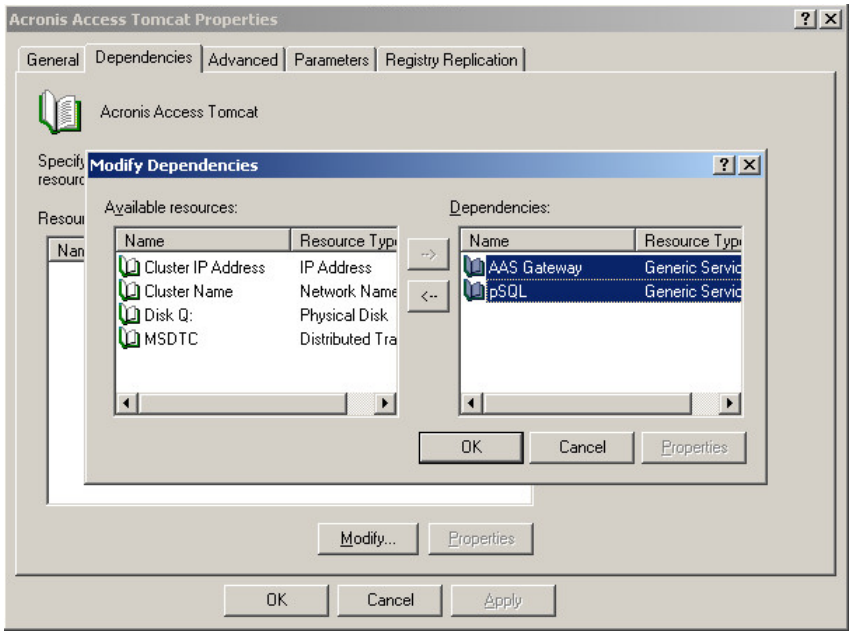


5. Drücken Sie **OK**.

Führen Sie für den Acronis Access Tomcat-Dienst Folgendes durch:

1. Klicken Sie mit der rechten Maustaste auf den entsprechenden Dienst und wählen Sie **Eigenschaften**.
2. Klicken Sie auf die Registerkarte **Abhängigkeiten**.
3. Klicken Sie auf **Ändern**.

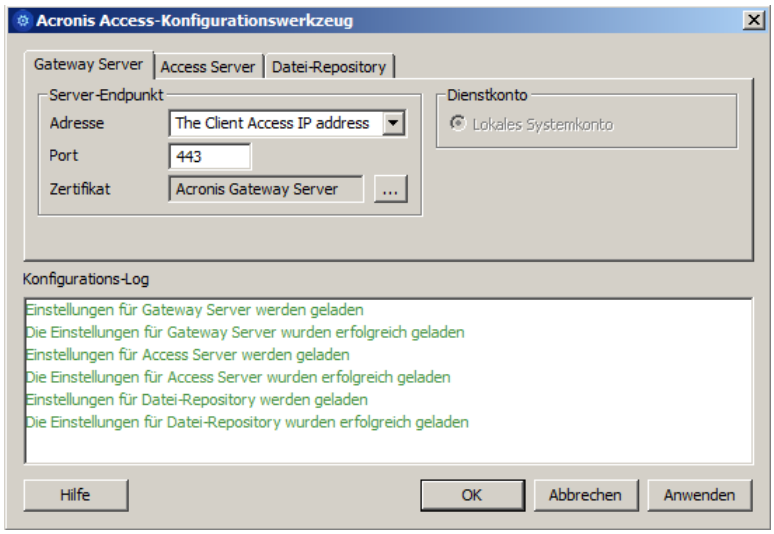
4. Wählen Sie die PostgreSQL- und Acronis Access Gateway Server-Dienste aus und verschieben Sie sie nach rechts.



5. Drücken Sie **OK**.

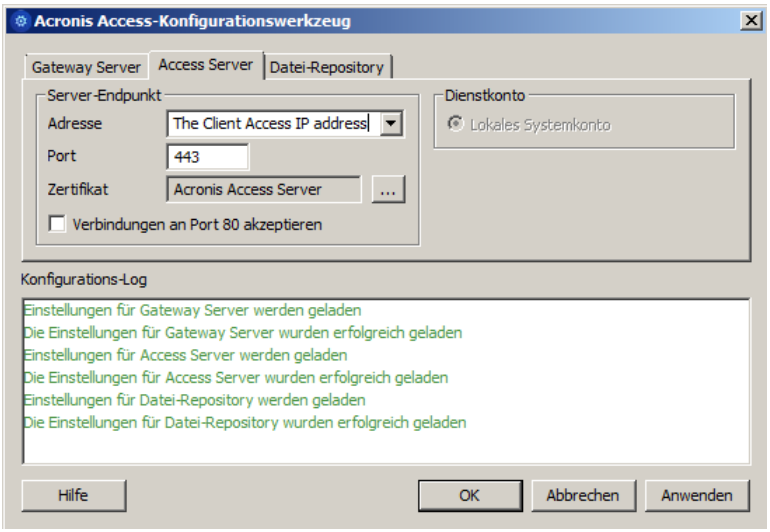
Die Cluster-Gruppe online schalten und das Konfigurationswerkzeug verwenden

1. Klicken Sie mit der rechten Maustaste auf die Cluster-Gruppe und drücken Sie **Online schalten**.
2. Starten Sie das Konfigurationswerkzeug.
   - Bei einer Neuinstallation befindet sich dies normalerweise unter **`C:\Program Files (x86)\Acronis\Access\Configuration Utility`**
   - Bei einem Upgrade von mobilEcho befindet es sich normalerweise unter **`C:\Program Files (x86)\GroupLogic\Configuration Utility`**
3. Konfigurieren Sie den Acronis Access Gateway Server-Dienst, um die IP-Adresse(n) für die Acronis Access Dienstgruppe abzuhören.

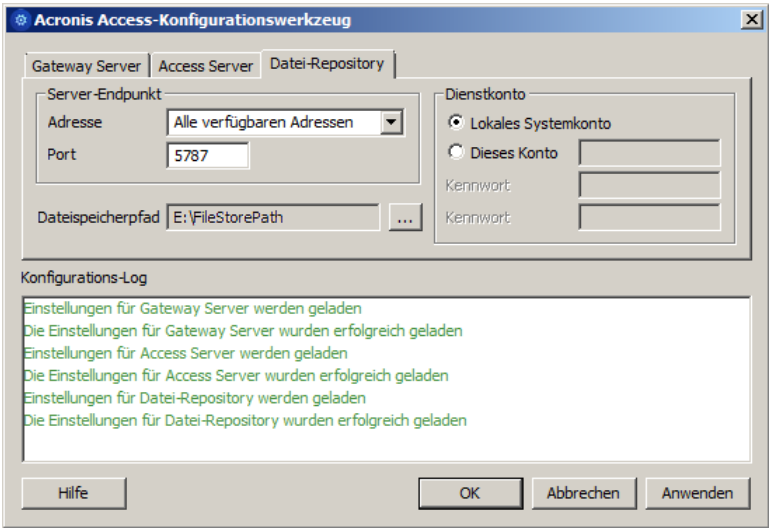


4. Konfigurieren Sie den Acronis Access Server-Dienst, um die IP-Adresse(n) für die Acronis Access Dienstgruppe abzuhören.

   Hinweis: *Wenn* ***Verbindungen an Port 80 akzeptieren*** *ausgewählt ist, hört Tomcat den unsicheren Port 80 auf eingehenden Datenverkehr hin ab und leitet ihn zum HTTPS-Port um, den Sie zuvor festgelegt haben.*



5. Konfigurieren Sie das Acronis Access Datei-Repository, um 'localhost' abzuhören, und ändern Sie den Dateispeicherpfad in ein Verzeichnis auf dem freigegebenen Laufwerk. Dieser Pfad sollte für beide Knoten gleich sein.



6. Klicken Sie auf **OK**, um die Konfiguration abzuschließen, und starten Sie die Dienste neu.

Installation und Konfiguration auf dem zweiten Knoten

1. Deaktivieren Sie alle vorhandenen Virenschutzprogramme, da sie unter Umständen den Installationsvorgang unterbrechen und somit eine fehlerhafte Installation verursachen können.
2. Installieren Sie Acronis Access auf dem zweiten Knoten, verwenden Sie jedoch diesmal den Standardspeicherort für **Postgres Data** sowie dasselbe postgres-Benutzerkennwort wie für den ersten Knoten.
3. Schließen Sie die Installation ab.

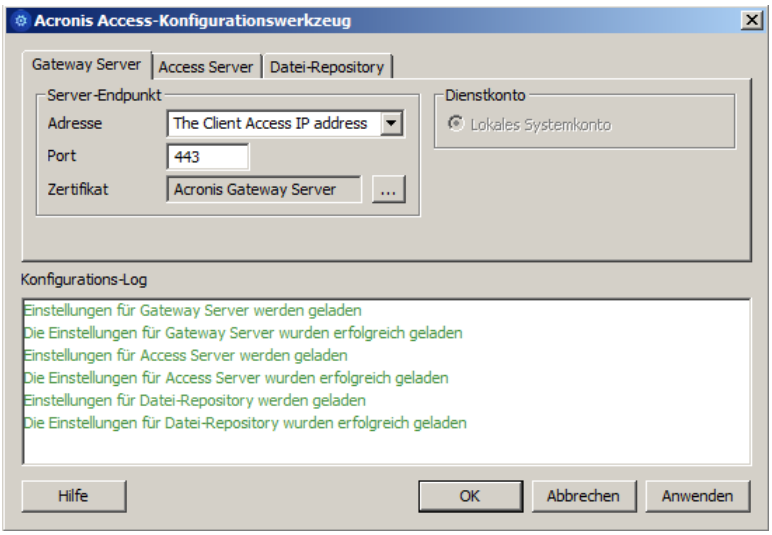
4. Konfigurieren Sie die Gateway Server-Datenbank, sodass sie sich auf einem freigegebenen Laufwerk befindet.
   a. Navigieren Sie zu **`C:\Program Files (x86)\Acronis\Access\Gateway Server\`**
      - Bei einem Upgrade lautet der Pfad: **`C:\Program Files (x86)\GroupLogic\mobilEcho Server\`**
   b. Suchen Sie die Datei **database.yml** und öffnen Sie sie mit einem Texteditor.
   c. Gehen Sie zu dieser Zeile: **`database_path: './database/'`** und ersetzen Sie **./database/** durch den gewünschten Pfad (z.B. **`database_path: 'S:/mobilEcho_cluster/database/'`**).

   Hinweis: *Verwenden Sie als Pfadtrennzeichen Schrägstriche (/).*

   Hinweis: *Sie können die konfigurierte Datei 'database.yml' aus dem ersten Knoten kopieren und im zweiten Knoten einfügen.*

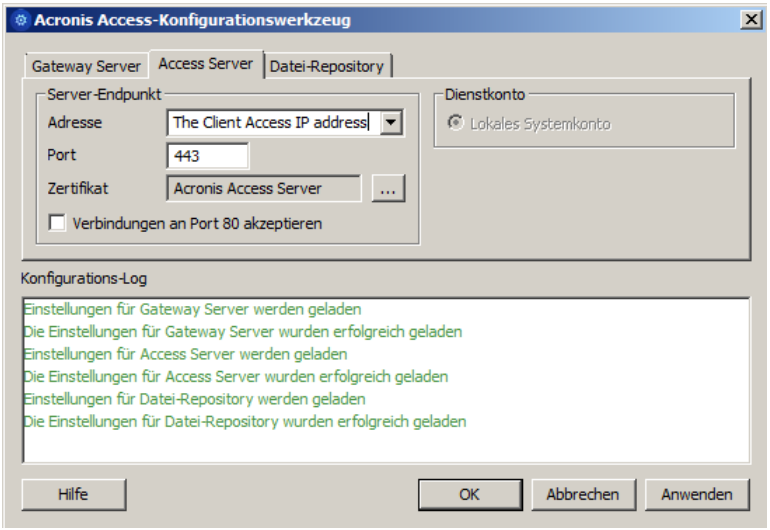
   Hinweis: *Der Pfad sollte mit dem Pfad auf dem ersten Knoten übereinstimmen.*

5. Verschieben Sie die Cluster-Gruppe in den zweiten Knoten. Klicken Sie dazu mit der rechten Maustaste auf die Cluster-Gruppe und klicken Sie auf **Gruppe verschieben**.
6. Starten Sie das Konfigurationswerkzeug.
   - Bei einer Neuinstallation befindet sich dies normalerweise unter **`C:\Program Files (x86)\Acronis\Access\Configuration Utility`**
   - Bei einem Upgrade von mobilEcho befindet es sich normalerweise unter **`C:\Program Files (x86)\GroupLogic\Configuration Utility`**
7. Konfigurieren Sie den Acronis Access Gateway Server-Dienst, um die IP-Adresse(n) für die Acronis Access Dienstgruppe abzuhören.

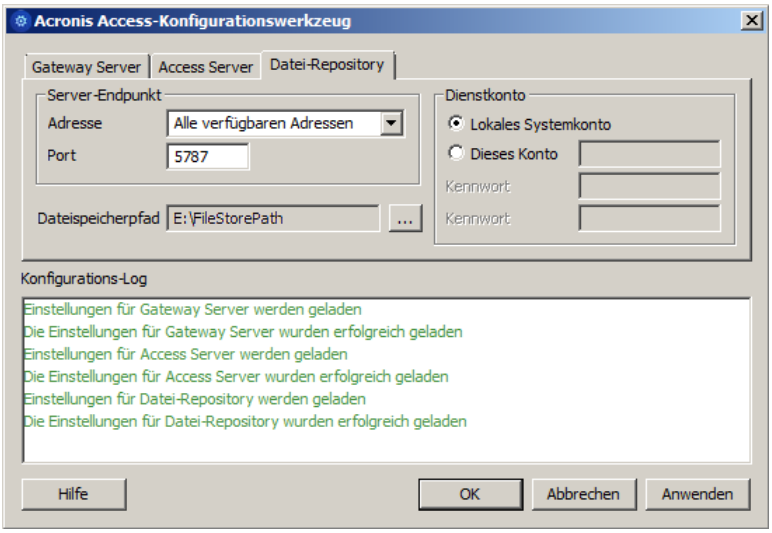


8. Konfigurieren Sie den Acronis Access Server-Dienst, um die IP-Adresse(n) für die Acronis Access Dienstgruppe abzuhören.

Hinweis: *Wenn* ***Verbindungen an Port 80 akzeptieren*** *ausgewählt ist, hört Tomcat den unsicheren Port 80 auf eingehenden Datenverkehr hin ab und leitet ihn zum HTTPS-Port um, den Sie zuvor festgelegt haben.*



9. Konfigurieren Sie das Acronis Access Datei-Repository, um 'localhost' abzuhören, und ändern Sie den Dateispeicherpfad in ein Verzeichnis auf dem freigegebenen Laufwerk. Dieser Pfad sollte für beide Knoten gleich sein.



10. Klicken Sie auf **OK**, um die Konfiguration abzuschließen, und starten Sie die Dienste neu.

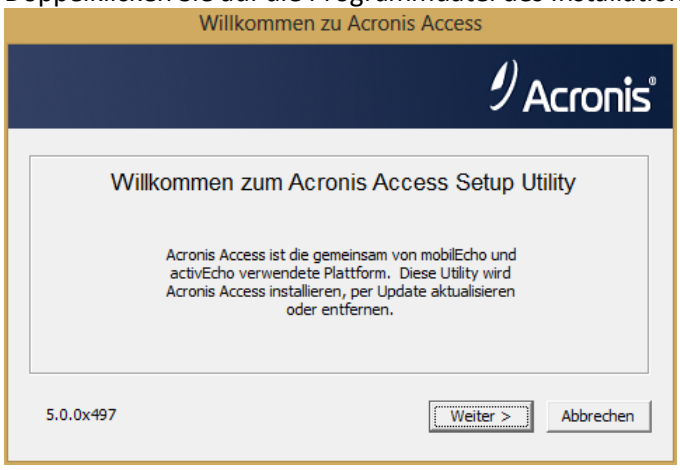
7.3.2 Upgrade eines mobilEcho-Servers auf einem Windows 2008 Failover Cluster auf Acronis Access durchführen

1. Öffnen Sie die **Failover-Clusterverwaltung** und doppelklicken Sie auf die Dienstgruppe.
2. Löschen Sie die mobilEcho Dienstressourcen.

   Hinweis: *Schalten Sie nicht die gesamte Cluster-Gruppe offline, sondern löschen Sie nur die mobilEcho Dienstressourcen.*

3. Starten Sie den Installer auf dem aktiven Knoten.

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



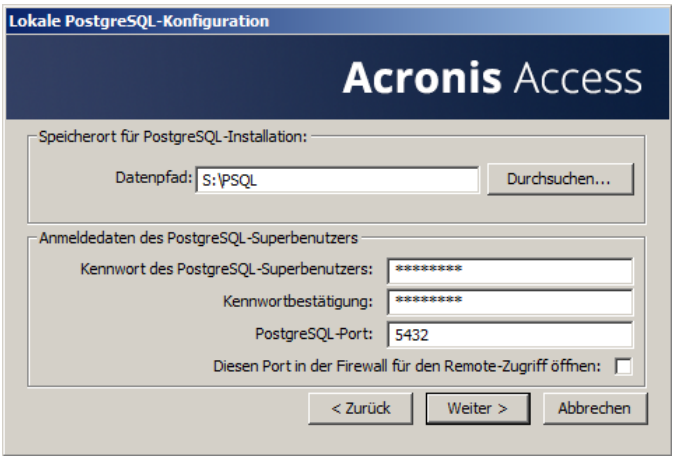
6. Klicken Sie auf **Weiter**, um zu beginnen.
7. Lesen und akzeptieren Sie die Lizenzvereinbarung.
8. Drücken Sie **Installieren**.

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.*

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

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

11. Wählen Sie auf einem freigegebenen Laufwerk einen Speicherort für den Ordner **Postgres Data** und drücken Sie **Weiter**.



12. Es wird ein Fenster angezeigt, in dem alle zu installierenden Komponenten aufgelistet sind. Drücken Sie **OK**, um fortzufahren.
13. Wenn der Installationsvorgang für Acronis Access abgeschlossen ist, drücken Sie **Beenden**.Navigieren Sie zum freigegebenen Laufwerk, und suchen und kopieren Sie die drei folgenden Dateien: **production.sqlite3**, **mobilEcho_manager.cfg** und **priority.txt** (diese ist eventuell nicht vorhanden). Fügen Sie die Dateien in das Acronis Access-Installationsverzeichnis ein, und ersetzen Sie die vorhandenen Dateien.

Hinweis: *Die Dateien, die Sie ersetzen sollen, befinden sich normalerweise im folgenden Verzeichnis:*

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

Konfigurationen auf dem aktiven Knoten

1. Konfigurieren Sie die Gateway Server-Datenbank, sodass sie sich auf einem freigegebenen Laufwerk befindet.
   a. Navigieren Sie zu **`C:\Program Files (x86)\Acronis\Access\Gateway Server\`**
      - Bei einem Upgrade lautet der Pfad: **`C:\Program Files (x86)\GroupLogic\mobilEcho Server\`**
   b. Suchen Sie die Datei **database.yml** und öffnen Sie sie mit einem Texteditor.
   c. Gehen Sie zu dieser Zeile: **`database_path: './database/'`** und ersetzen Sie **./database/** durch den gewünschten Pfad (z.B. **`database_path: 'S:/mobilEcho_cluster/database/'`**).

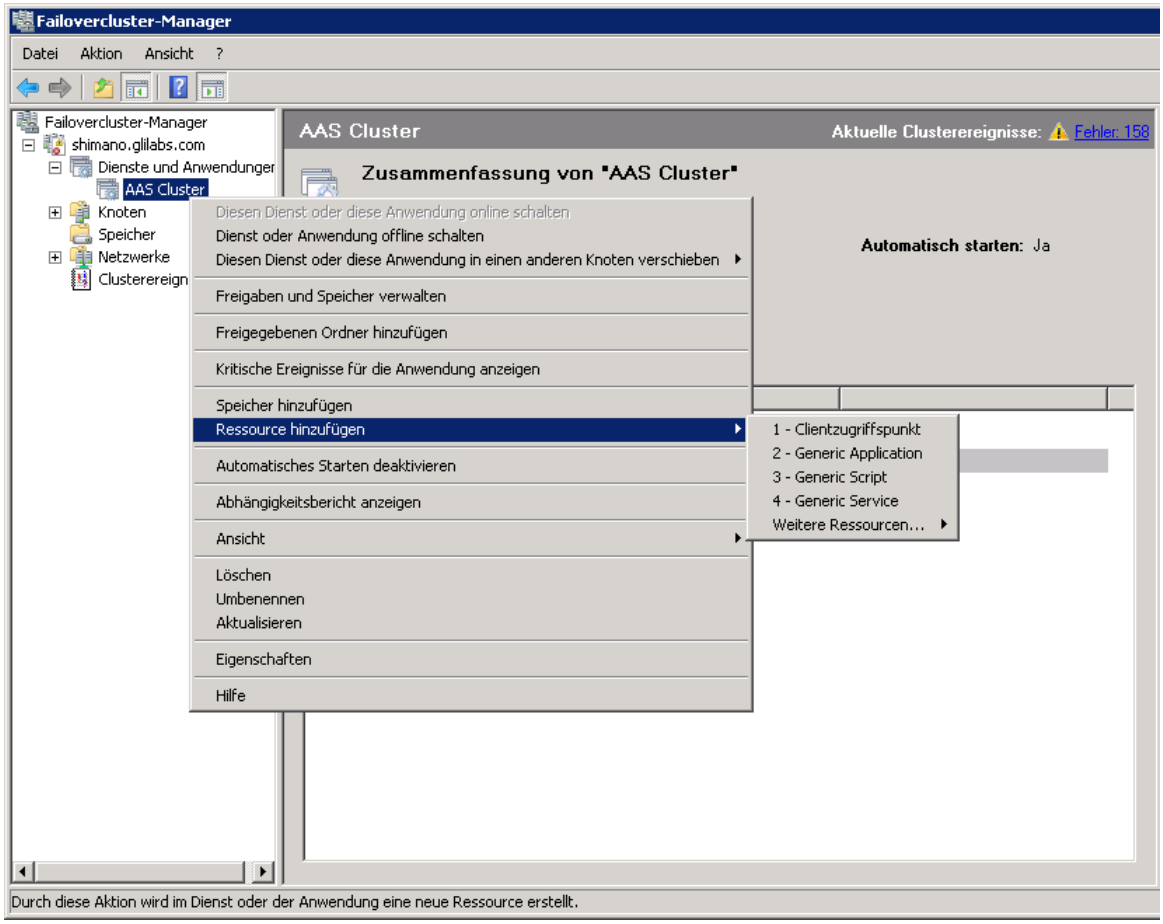
Hinweis: *Verwenden Sie als Pfadtrennzeichen Schrägstriche (/).*

Hinweis: *Sie können die konfigurierte Datei 'database.yml' aus dem ersten Knoten kopieren und im zweiten Knoten einfügen.*

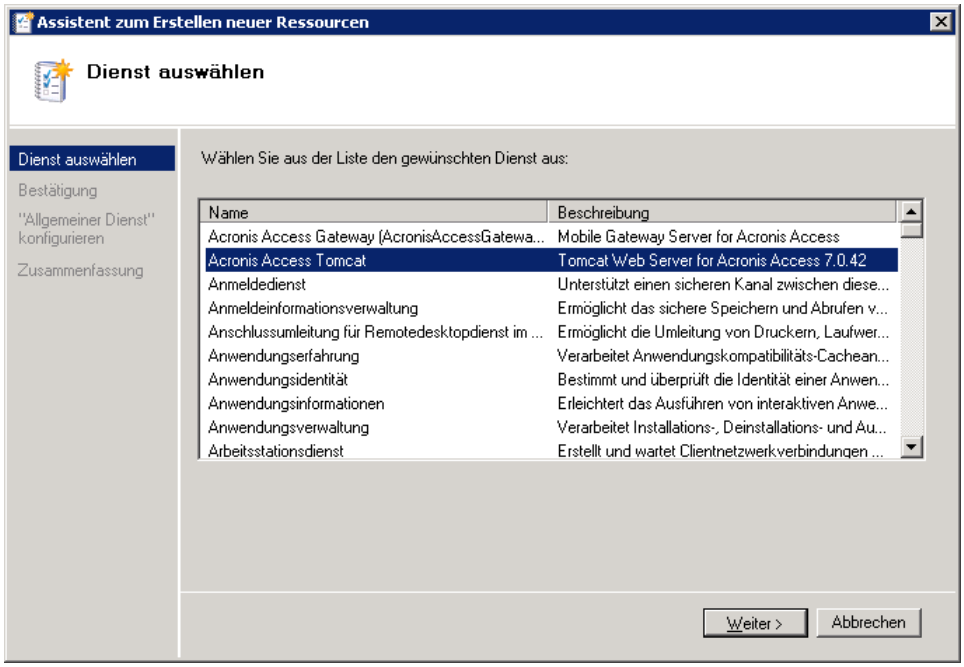
Alle erforderlichen Dienste der Acronis Access Dienstgruppe hinzufügen

Führen Sie das folgende Verfahren für die einzelnen Dienste aus: AcronisAccessGateway, AcronisAccessPostgreSQL (abhängig von der Acronis Access-Version), AcronisAccessRepository und AcronisAccessTomcat.

1. Klicken Sie mit der rechten Maustaste auf die Acronis Access Dienstgruppe und wählen Sie **Ressource hinzufügen**.
2. Wählen Sie **Allgemeiner Dienst** aus.



3. Wählen Sie den geeigneten Dienst aus und drücken Sie **Weiter**.



4. Drücken Sie im Bestätigungsfenster **Weiter**.
5. Drücken Sie im Fenster **Registrierungseinstellungen replizieren Weiter**.
6. Drücken Sie im Zusammenfassungsfenster **Fertig stellen**.

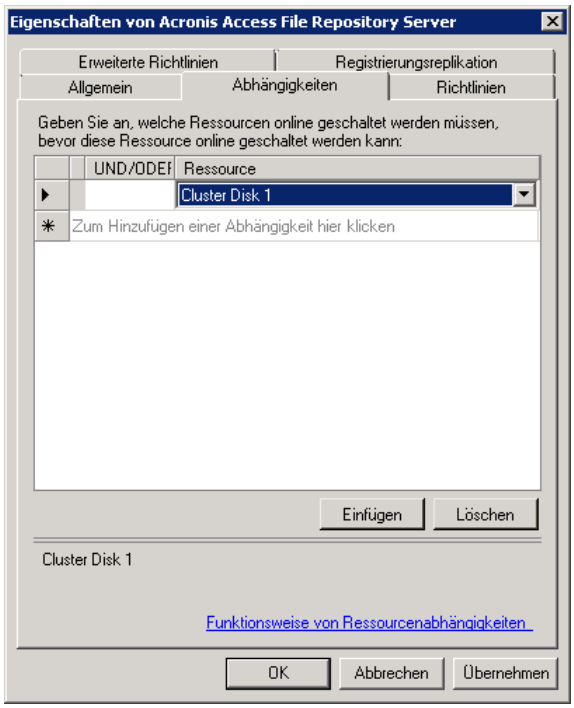
Abhängigkeiten konfigurieren

1. Doppelklicken Sie auf die Acronis Access Dienstgruppe.

Führen Sie für PostgreSQL und das Acronis Access Datei-Repository-Dienste Folgendes durch:

1. Klicken Sie mit der rechten Maustaste auf den entsprechenden Dienst und wählen Sie **Eigenschaften**.
2. Klicken Sie auf die Registerkarte **Abhängigkeiten**.

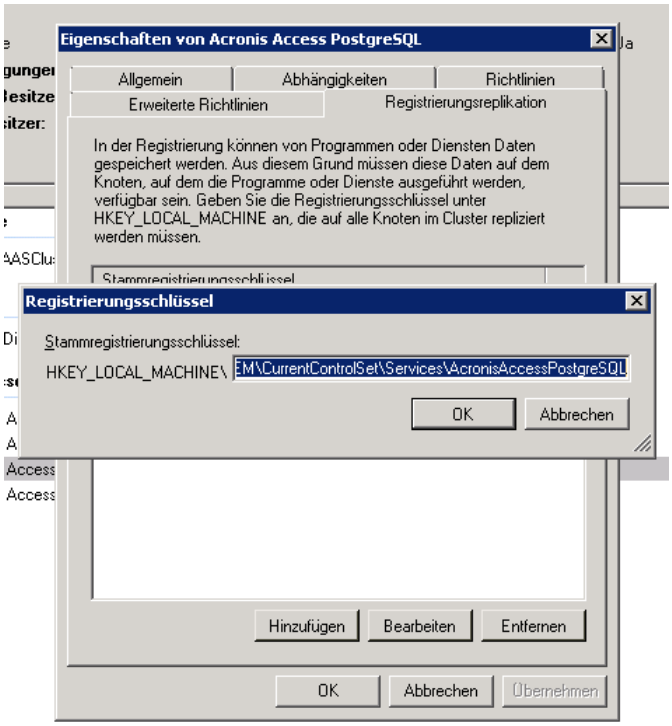
3. Klicken Sie auf **Ressource** und wählen Sie das freigegebene Laufwerk aus, das Sie hinzugefügt haben.



4. Drücken Sie **Anwenden** und schließen Sie das Fenster.

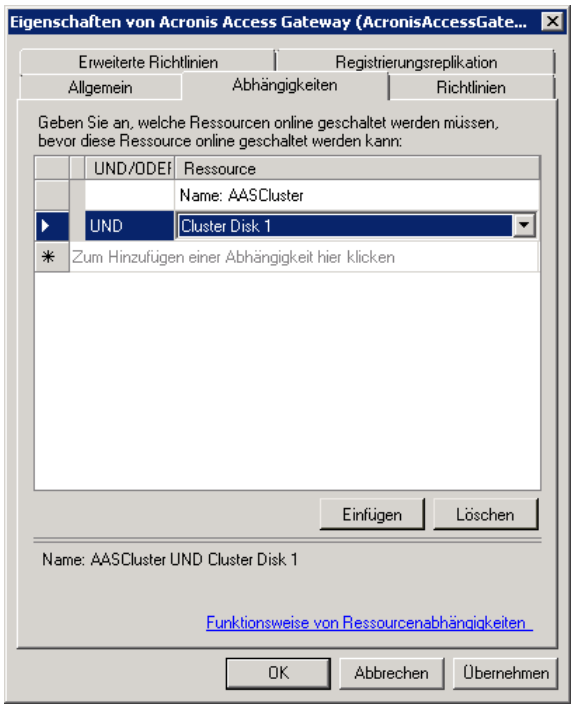
Führen Sie für PostgreSQL außerdem Folgendes aus:

1. Klicken Sie auf die Registerkarte **Registrierungsreplikation**.
2. Drücken Sie **Hinzufügen** und geben Sie Folgendes ein: **`SYSTEM\CurrentControlSet\Services\AcronisAccessPostgreSQL\`**(Für ältere Versionen von Acronis Access kann der Service unterschiedlich sein, z. B. **postgresql-x64-9.2**)



Führen Sie für den Acronis Access Gateway Server-Dienst Folgendes aus:

1. Klicken Sie mit der rechten Maustaste auf den entsprechenden Dienst und wählen Sie **Eigenschaften**.
2. Klicken Sie auf die Registerkarte **Abhängigkeiten**.
3. Klicken Sie auf **Ressource** und wählen Sie das freigegebene Laufwerk aus, das Sie hinzugefügt haben, sowie den **Netzwerknamen** (der zugleich der Name des Clientzugriffspunkts ist).

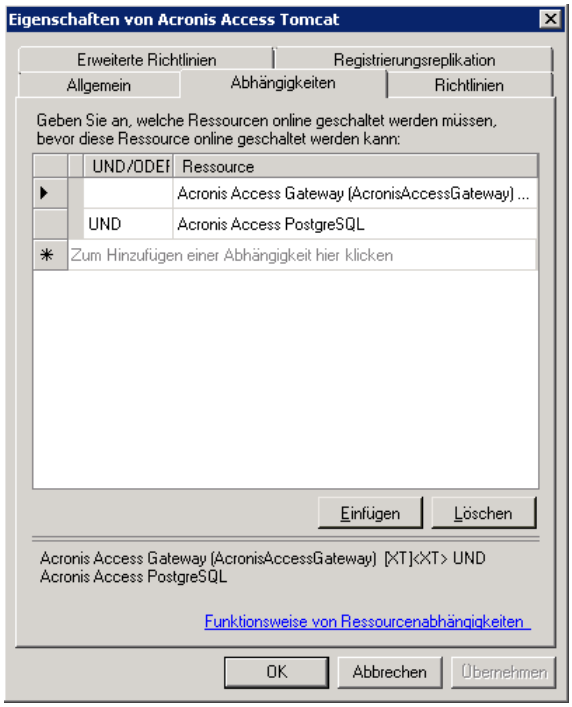


4. Drücken Sie **Anwenden** und schließen Sie das Fenster.

Führen Sie für den Acronis Access Tomcat-Dienst Folgendes aus:

1. Klicken Sie mit der rechten Maustaste auf den entsprechenden Dienst und wählen Sie **Eigenschaften**.
2. Klicken Sie auf die Registerkarte **Abhängigkeiten**.

3. Klicken Sie auf **Ressource** und wählen Sie die PostgreSQL und Acronis Access Gateway Server-Dienste als Abhängigkeiten aus. Drücken Sie **Anwenden** und schließen Sie das Fenster.

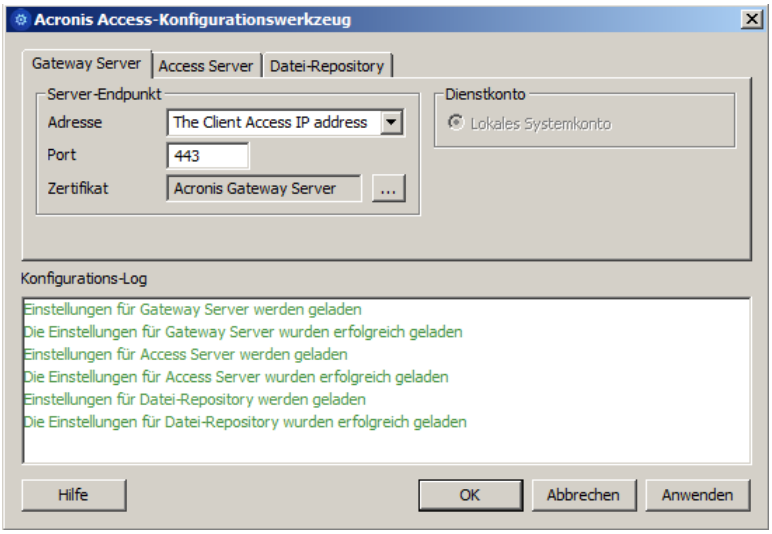


Hinweis: *Wenn die Gateway und Access Server auf verschiedenen IP-Adressen ausgeführt werden sollen, fügen Sie die zweite IP-Adresse der Acronis Access Dienstgruppe als Ressource hinzu und legen Sie sie als Abhängigkeit für den Netzwerknamen fest.*

Dienstgruppe online schalten und Konfigurationswerkzeug verwenden

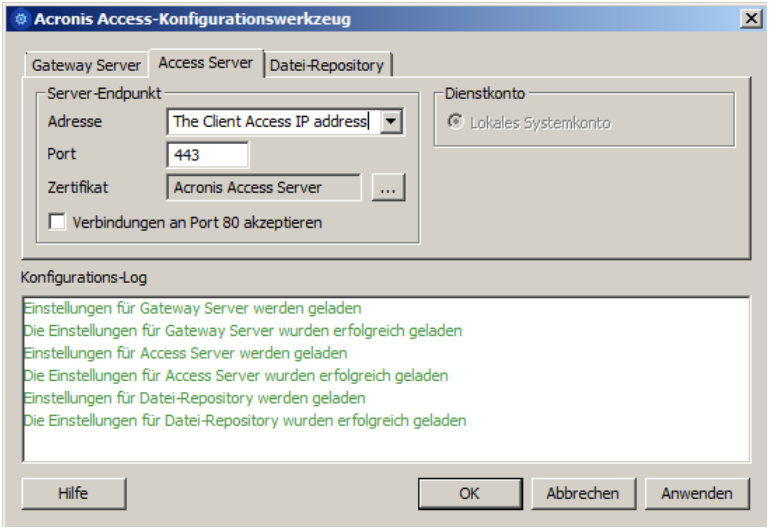
1. Klicken Sie mit der rechten Maustaste auf die Acronis Access Dienstgruppe und wählen Sie **Diese Anwendung oder Dienstgruppe online schalten**.
2. Starten Sie das Konfigurationswerkzeug.
   - Bei einer Neuinstallation befindet sich dies normalerweise unter **`C:\Program Files (x86)\Acronis\Access\Configuration Utility`**
   - Bei einem Upgrade von mobilEcho befindet es sich normalerweise unter **`C:\Program Files (x86)\GroupLogic\Configuration Utility`**

3. Konfigurieren Sie den Acronis Access Gateway Server-Dienst, um die IP-Adresse(n) für die Acronis Access Dienstgruppe abzuhören.

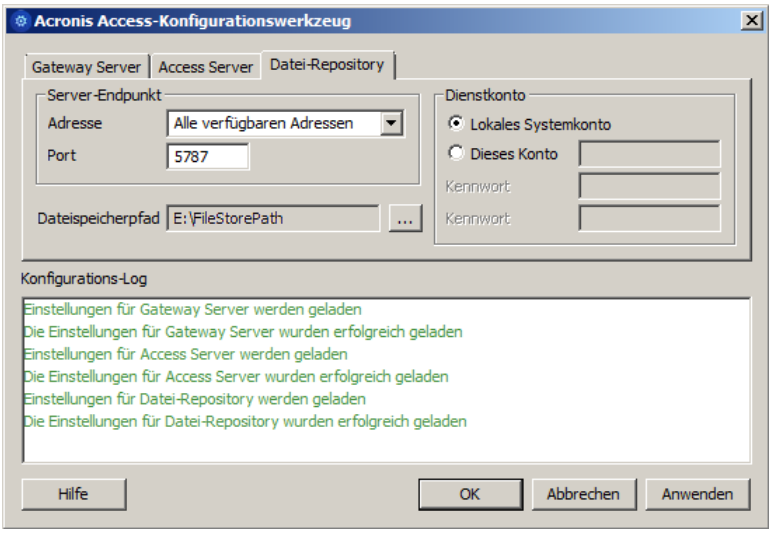


4. Konfigurieren Sie den Acronis Access Server-Dienst, um die IP-Adresse(n) für die Acronis Access Dienstgruppe abzuhören.

Hinweis: *Wenn* ***Verbindungen an Port 80 akzeptieren*** *ausgewählt ist, hört Tomcat den unsicheren Port 80 auf eingehenden Datenverkehr hin ab und leitet ihn zum HTTPS-Port um, den Sie zuvor festgelegt haben.*



5. Konfigurieren Sie das Acronis Access Datei-Repository, um 'localhost' abzuhören, und ändern Sie den Dateispeicherpfad in ein Verzeichnis auf dem freigegebenen Laufwerk. Dieser Pfad sollte für beide Knoten gleich sein.



6. Klicken Sie auf **OK**, um die Konfiguration abzuschließen, und starten Sie die Dienste neu.

Installation und Konfiguration auf dem zweiten Knoten

1. Deaktivieren Sie alle vorhandenen Virenschutzprogramme, da sie unter Umständen den Installationsvorgang unterbrechen und somit eine fehlerhafte Installation verursachen können.
2. Installieren Sie Acronis Access auf dem zweiten Knoten, verwenden Sie jedoch diesmal den Standardspeicherort für **Postgres Data** sowie dasselbe postgres-Benutzerkennwort wie für den ersten Knoten.
3. Schließen Sie die Installation ab.
4. Konfigurieren Sie die Gateway Server-Datenbank, sodass sie sich auf einem freigegebenen Laufwerk befindet.
   a. Navigieren Sie zu **`C:\Program Files (x86)\Acronis\Access\Gateway Server\`**
      - Bei einem Upgrade lautet der Pfad: **`C:\Program Files (x86)\GroupLogic\mobilEcho Server\`**
   b. Suchen Sie die Datei **database.yml** und öffnen Sie sie mit einem Texteditor.
   c. Gehen Sie zu dieser Zeile: **`database_path: './database/'`** und ersetzen Sie **./database/** durch den gewünschten Pfad (z.B. **`database_path: 'S:/mobilEcho_cluster/database/'`**).

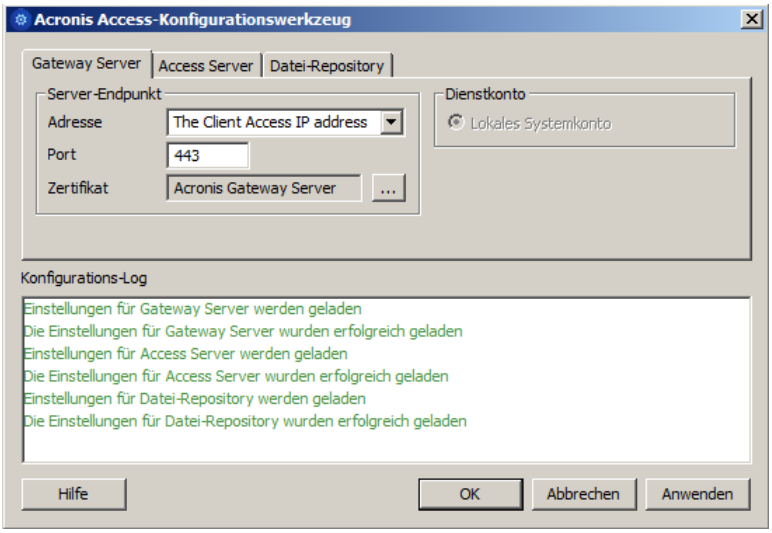
   Hinweis: *Verwenden Sie als Pfadtrennzeichen Schrägstriche (/).*

   Hinweis: *Sie können die konfigurierte Datei 'database.yml' aus dem ersten Knoten kopieren und im zweiten Knoten einfügen.*

   Hinweis: *Der Pfad sollte mit dem Pfad auf dem ersten Knoten übereinstimmen.*
5. Verschieben Sie die Acronis Access Dienstgruppe in den zweiten Knoten. Klicken Sie dazu mit der rechten Maustaste auf die Dienstgruppe und klicken Sie auf **In den zweiten Knoten verschieben**.
6. Starten Sie das Konfigurationswerkzeug.

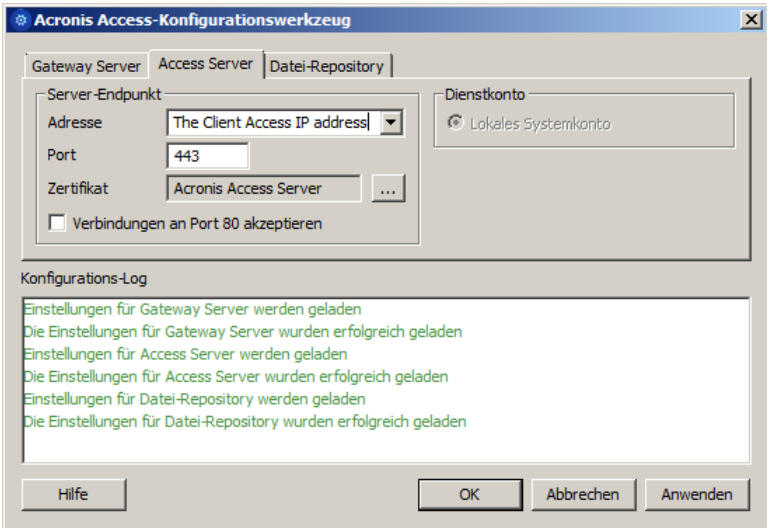
- Bei einer Neuinstallation befindet sich dies normalerweise unter **`C:\Program Files (x86)\Acronis\Access\Configuration Utility`**
- Bei einem Upgrade von mobilEcho befindet es sich normalerweise unter **`C:\Program Files (x86)\GroupLogic\Configuration Utility`**

7. Konfigurieren Sie den Acronis Access Gateway Server-Dienst, um die IP-Adresse(n) für die Acronis Access Dienstgruppe abzuhören.

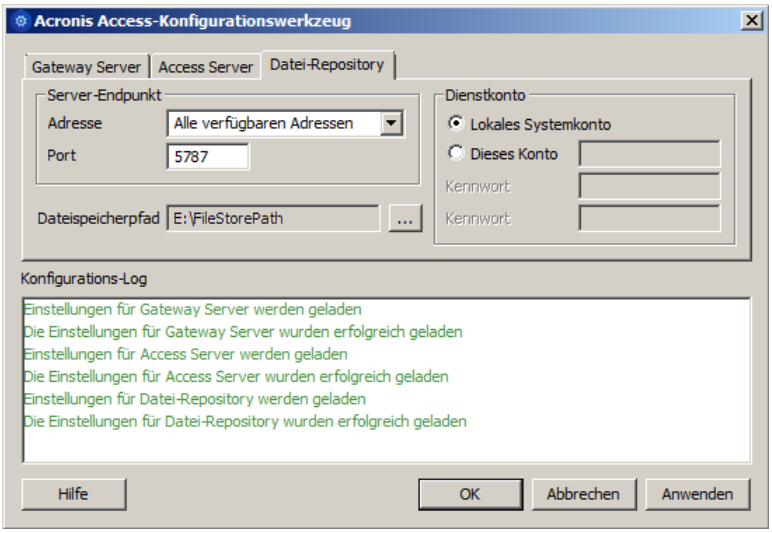


8. Konfigurieren Sie den Acronis Access Server-Dienst, um die IP-Adresse(n) für die Acronis Access Dienstgruppe abzuhören.

Hinweis: *Wenn* ***Verbindungen an Port 80 akzeptieren*** *ausgewählt ist, hört Tomcat den unsicheren Port 80 auf eingehenden Datenverkehr hin ab und leitet ihn zum HTTPS-Port um, den Sie zuvor festgelegt haben.*



9. Konfigurieren Sie das Acronis Access Datei-Repository, um 'localhost' abzuhören, und ändern Sie den Dateispeicherpfad in ein Verzeichnis auf dem freigegebenen Laufwerk. Dieser Pfad sollte für beide Knoten gleich sein.



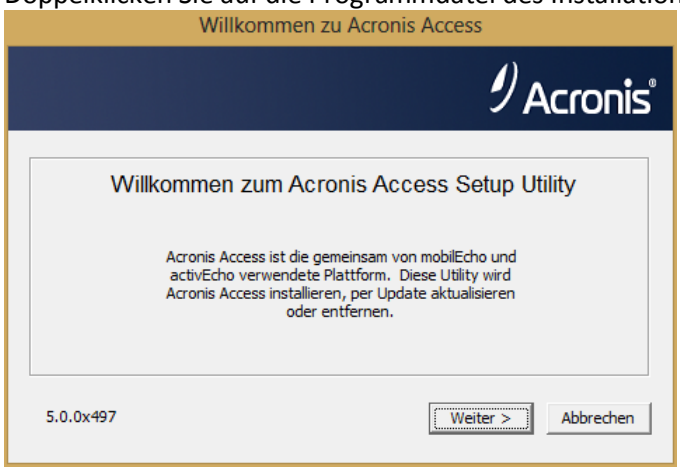
10. Klicken Sie auf **OK**, um die Konfiguration abzuschließen, und starten Sie die Dienste neu.

7.3.3 Upgrade eines mobilEcho-Servers auf einem Windows 2012 Failover Cluster auf Acronis Access durchführen

1. Öffnen Sie die **Failover-Clusterverwaltung** und doppelklicken Sie auf die Dienstgruppe.
2. Löschen Sie die mobilEcho Dienstressourcen.

   Hinweis: *Schalten Sie nicht die gesamte Cluster-Gruppe offline, sondern löschen Sie nur die mobilEcho Dienstressourcen.*

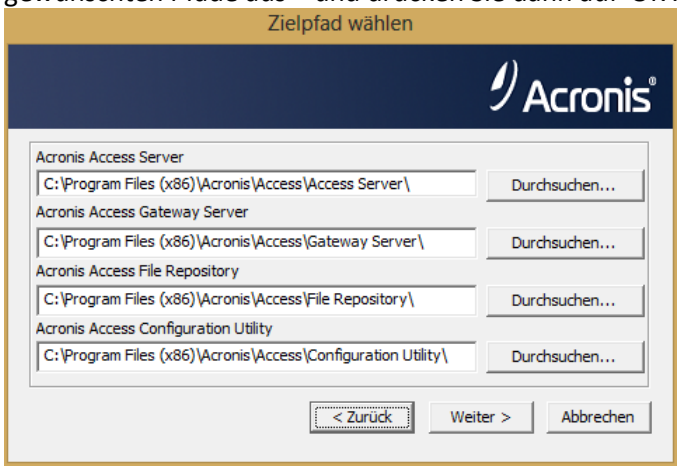
3. Starten Sie den Installer auf dem aktiven Knoten.
4. Deaktivieren Sie alle vorhandenen Virenschutzprogramme, da sie unter Umständen den Installationsvorgang unterbrechen und somit eine fehlerhafte Installation verursachen können.
5. Doppelklicken Sie auf die Programmdatei des Installationsprogramms.



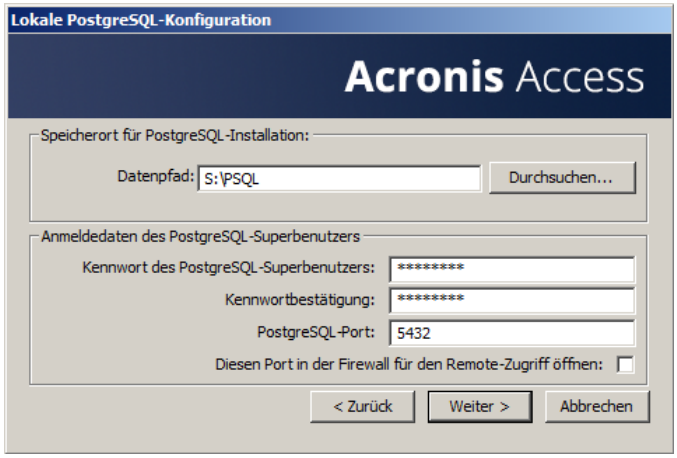
6. Klicken Sie auf **Weiter**, um zu beginnen.
7. Lesen und akzeptieren Sie die Lizenzvereinbarung.
8. Drücken Sie **Installieren**.

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.*

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



10. Legen Sie ein Kennwort für den Benutzer 'Postgres' fest, und notieren Sie es. Sie benötigen dieses Kennwort für Backup- und Wiederherstellungsaktionen der Datenbank.
11. Wählen Sie auf einem freigegebenen Laufwerk einen Speicherort für den Ordner **Postgres Data** und drücken Sie **Weiter**.



12. Es wird ein Fenster angezeigt, in dem alle zu installierenden Komponenten aufgelistet sind. Drücken Sie **OK**, um fortzufahren.
13. Wenn der Installationsvorgang für Acronis Access abgeschlossen ist, drücken Sie **Beenden**.Navigieren Sie zum freigegebenen Laufwerk, und suchen und kopieren Sie die drei folgenden Dateien: **production.sqlite3**, **mobilEcho_manager.cfg** und **priority.txt** (diese ist eventuell nicht vorhanden). Fügen Sie die Dateien in das Acronis Access-Installationsverzeichnis ein, und ersetzen Sie die vorhandenen Dateien.

Hinweis: *Die Dateien, die Sie ersetzen sollen, befinden sich normalerweise im folgenden Verzeichnis:*

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

Konfigurationen auf dem aktiven Knoten

1. Konfigurieren Sie die Gateway Server-Datenbank, sodass sie sich auf einem freigegebenen Laufwerk befindet.
   a. Navigieren Sie zu **`C:\Program Files (x86)\Acronis\Access\Gateway Server\`**
      - Bei einem Upgrade lautet der Pfad: **`C:\Program Files (x86)\GroupLogic\mobilEcho Server\`**
   b. Suchen Sie die Datei **database.yml** und öffnen Sie sie mit einem Texteditor.
   c. Gehen Sie zu dieser Zeile: **`database_path: './database/'`** und ersetzen Sie **./database/** durch den gewünschten Pfad (z.B. **`database_path: 'S:/mobilEcho_cluster/database/'`**).

Hinweis: *Verwenden Sie als Pfadtrennzeichen Schrägstriche (/).*

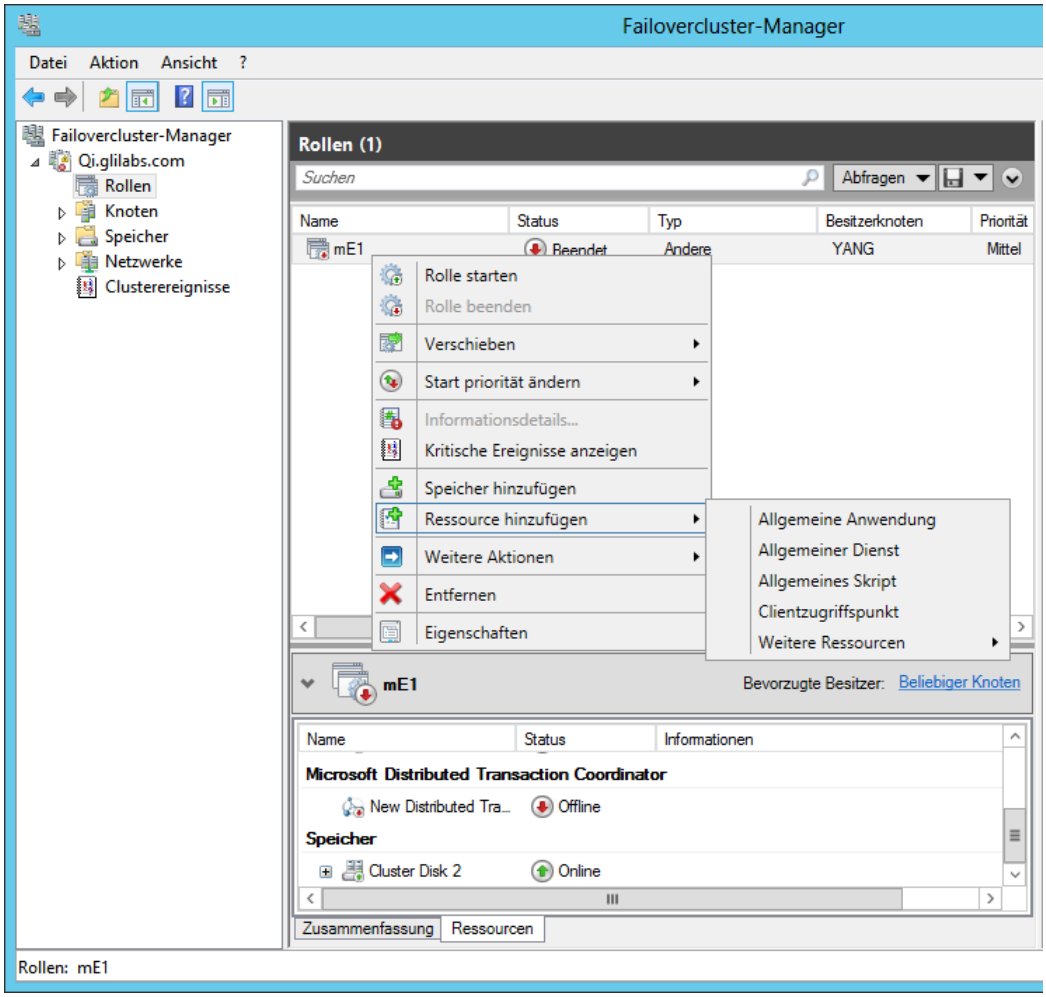
Hinweis: *Sie können die konfigurierte Datei 'database.yml' aus dem ersten Knoten kopieren und im zweiten Knoten einfügen.*

Alle erforderlichen Dienste der Acronis Access Rolle hinzufügen

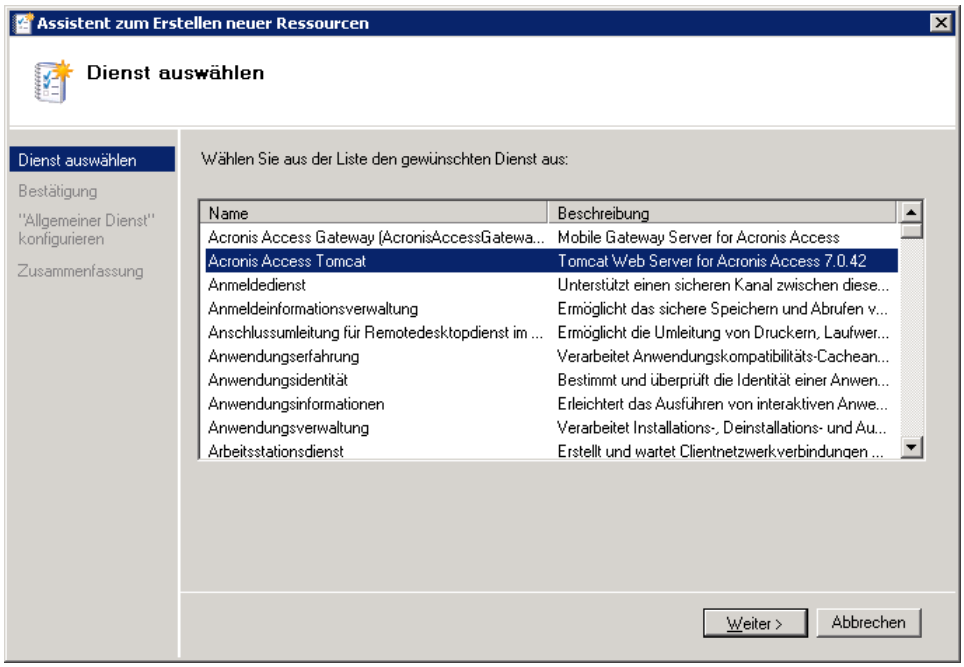
Führen Sie das folgende Verfahren für die einzelnen Dienste aus: AcronisAccessGateway, AcronisAccessPostgreSQL (abhängig von der Acronis Access-Version), AcronisAccessRepository und AcronisAccessTomcat.

1. Klicken Sie mit der rechten Maustaste auf die Acronis Access Rolle und wählen Sie **Ressource hinzufügen**.

2. Wählen Sie **Allgemeiner Dienst** aus.



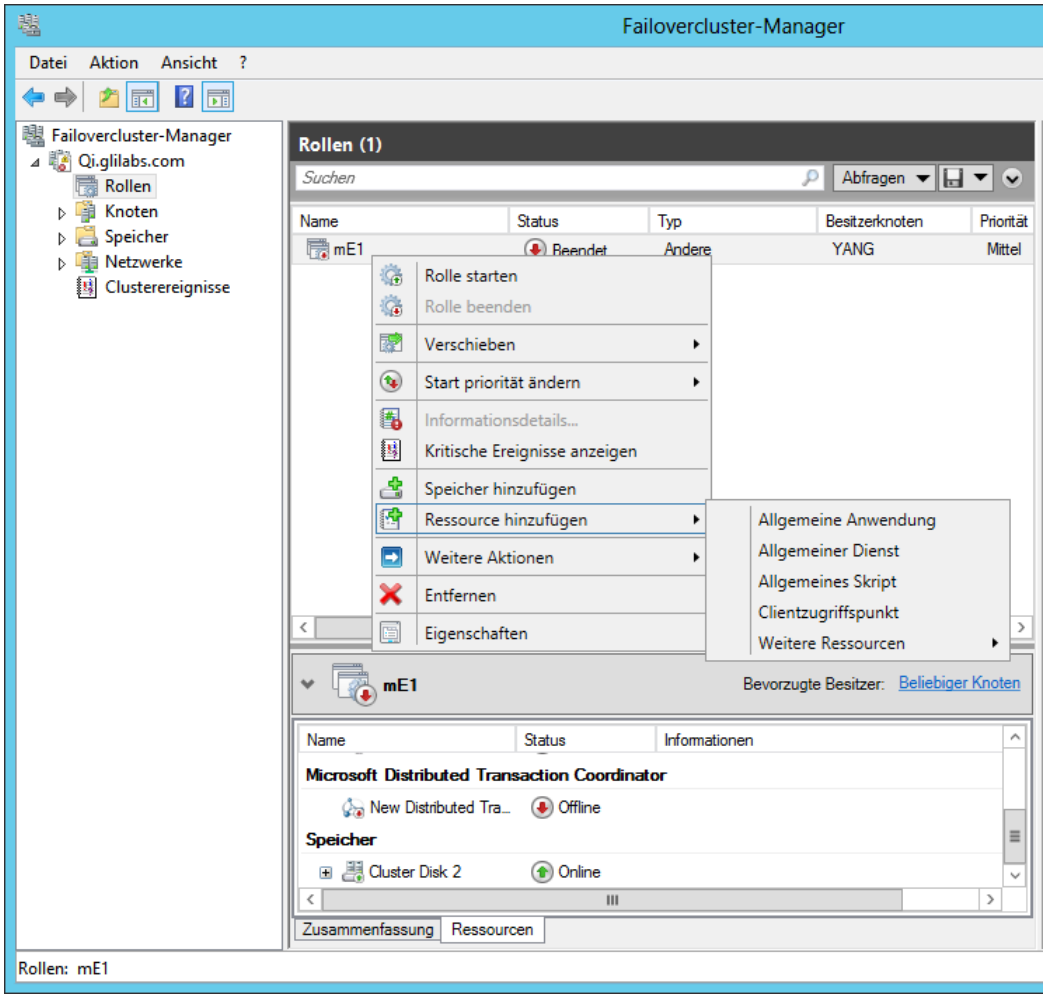
3. Wählen Sie den geeigneten Dienst aus und drücken Sie **Weiter**.



4. Drücken Sie im Bestätigungsfenster **Weiter**.
5. Drücken Sie im Zusammenfassungsfenster **Fertig stellen**.

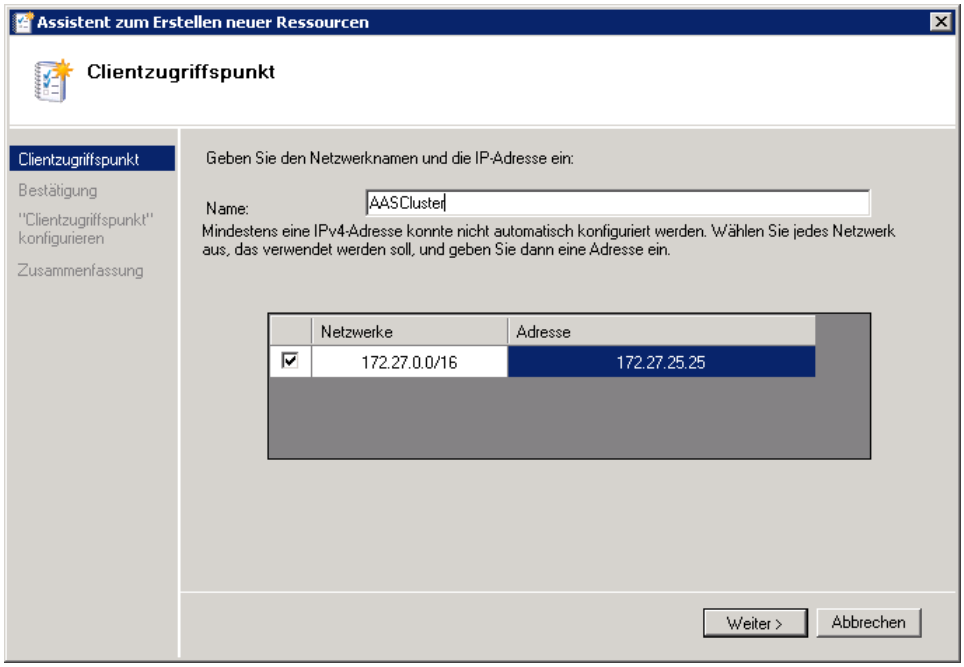
Zugriffspunkt festlegen

1. Klicken Sie mit der rechten Maustaste auf die Acronis Access Rolle und wählen Sie **Ressource hinzufügen**.
2. Wählen Sie **Clientzugriffspunkt** aus.



3. Geben Sie einen Namen für diesen Zugriffspunkt ein.

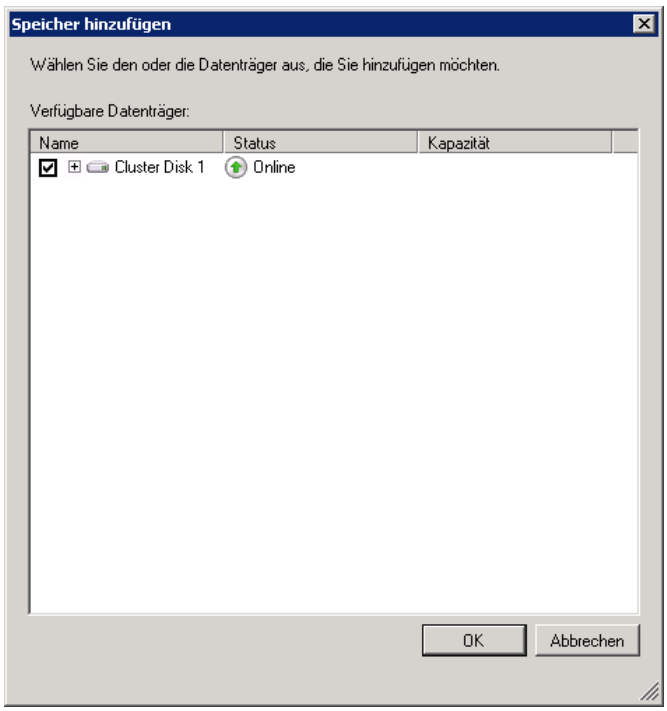
4. Wählen Sie ein Netzwerk.



5. Geben Sie die IP-Adresse ein und drücken Sie **Weiter**.
6. Drücken Sie im Bestätigungsfenster **Weiter**.
7. Drücken Sie im Zusammenfassungsfenster **Fertig stellen**.

Freigegebenes Laufwerk hinzufügen

1. Klicken Sie mit der rechten Maustaste auf die Acronis Access Rolle und wählen Sie **Speicher hinzufügen**.
2. Wählen Sie das gewünschte freigegebene Laufwerk aus.

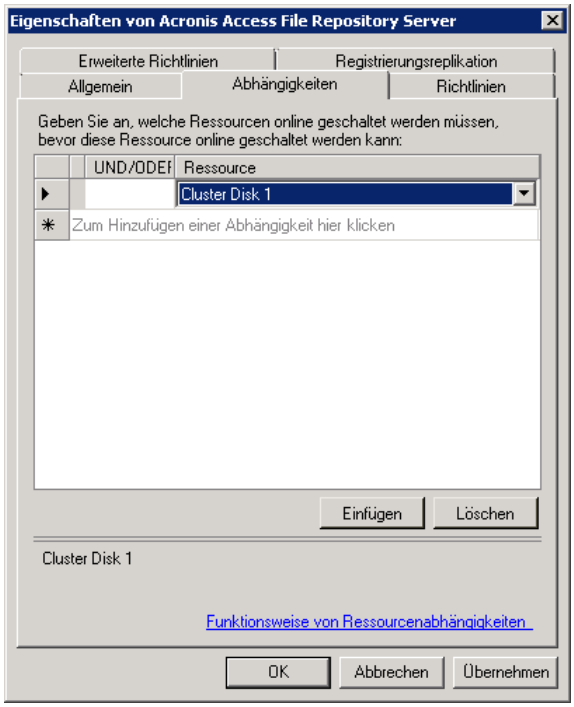


Abhängigkeiten konfigurieren

1. Wählen Sie die Acronis Access Rolle aus und klicken Sie auf die Registerkarte **Ressourcen**.

Führen Sie für PostgreSQL und das Acronis Access Datei-Repository-Dienste Folgendes durch:

1. Klicken Sie mit der rechten Maustaste auf den entsprechenden Dienst und wählen Sie **Eigenschaften**.
2. Klicken Sie auf die Registerkarte **Abhängigkeiten**.
3. Klicken Sie auf **Ressource** und wählen Sie das freigegebene Laufwerk aus, das Sie hinzugefügt haben.

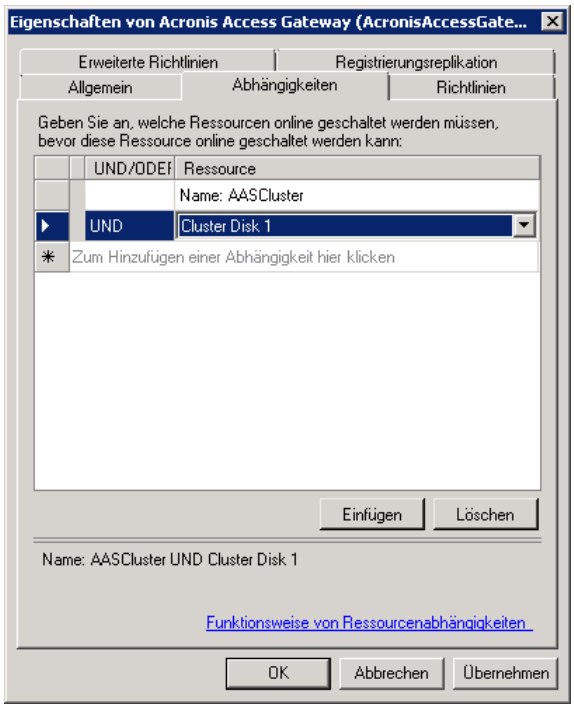


4. Drücken Sie **Anwenden** und schließen Sie das Fenster.

Führen Sie für den Acronis Access Gateway Server-Dienst Folgendes durch:

1. Klicken Sie mit der rechten Maustaste auf den entsprechenden Dienst und wählen Sie **Eigenschaften**.
2. Klicken Sie auf die Registerkarte **Abhängigkeiten**.

3. Klicken Sie auf **Ressource** und wählen Sie das freigegebene Laufwerk aus, das Sie hinzugefügt haben, sowie den **Netzwerknamen** (der zugleich der Name des Clientzugriffspunkts ist).

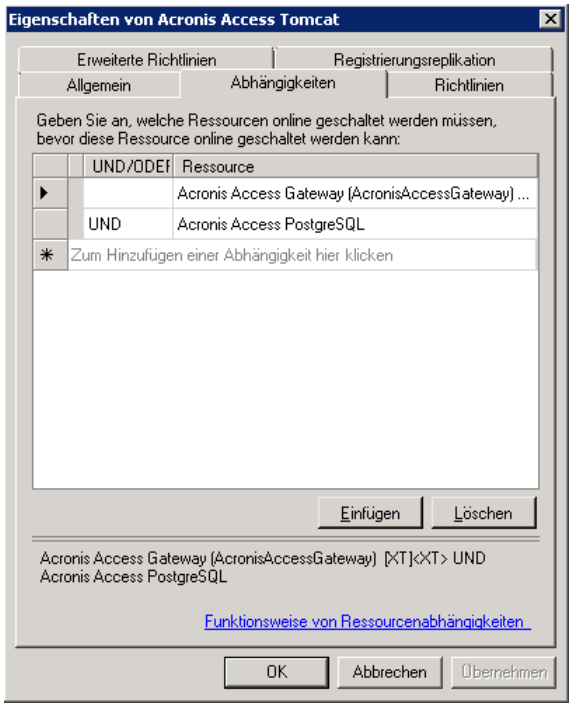


4. Drücken Sie **Anwenden** und schließen Sie das Fenster.

Führen Sie für den Acronis Access Tomcat-Dienst Folgendes durch:

1. Klicken Sie mit der rechten Maustaste auf den entsprechenden Dienst und wählen Sie **Eigenschaften**.
2. Klicken Sie auf die Registerkarte **Abhängigkeiten**.
3. Klicken Sie auf **Ressource** und wählen Sie die PostgreSQL und Acronis Access Gateway Server-Dienste als Abhängigkeiten aus. Drücken Sie **Anwenden** und schließen Sie das Fenster.

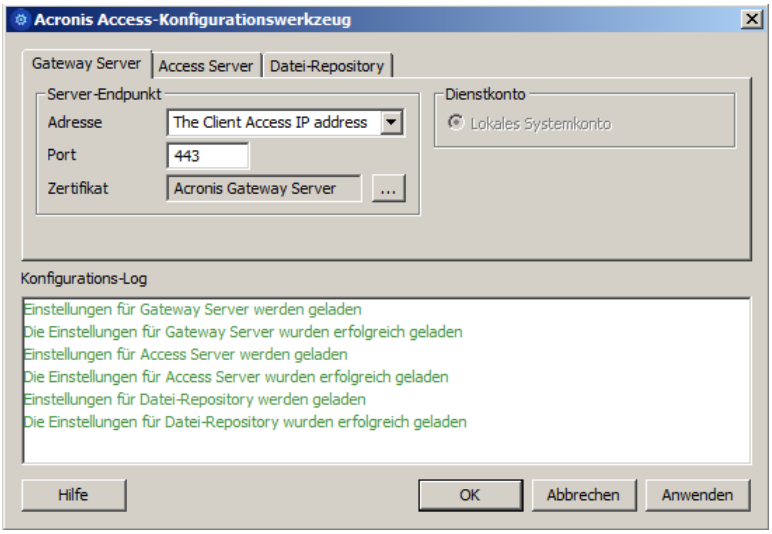
Hinweis: *Wenn die Gateway und Access Server unter verschiedenen IP-Adressen ausgeführt werden sollen, fügen Sie die zweite IP-Adresse der Acronis Access Rolle als Ressource hinzu und legen Sie sie als Abhängigkeit für den Netzwerknamen fest.*



Rolle starten und Konfigurationswerkzeug verwenden

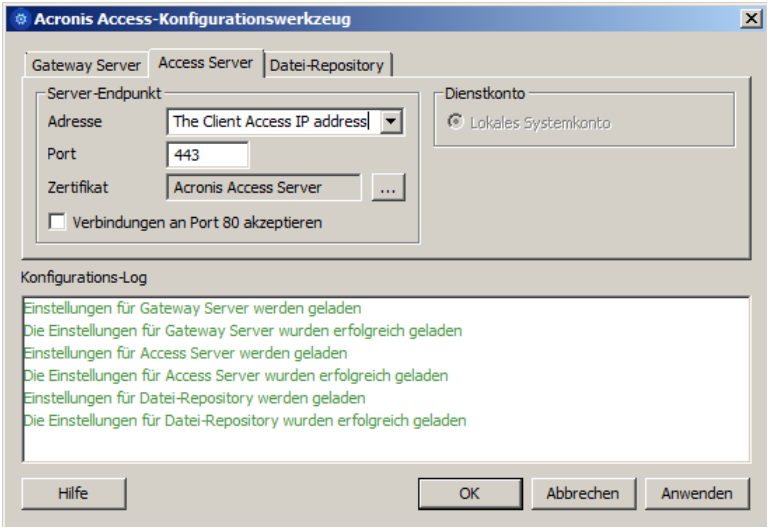
1. Klicken Sie mit der rechten Maustaste auf die Acronis Access Rolle und drücken Sie **Rolle starten**.
2. Starten Sie das Konfigurationswerkzeug.
   - Bei einer Neuinstallation befindet sich dies normalerweise unter **`C:\Program Files (x86)\Acronis\Access\Configuration Utility`**
   - Bei einem Upgrade von mobilEcho befindet es sich normalerweise unter **`C:\Program Files (x86)\GroupLogic\Configuration Utility`**

3. Konfigurieren Sie den Acronis Access Gateway Server-Dienst, um die IP-Adresse(n) für die Acronis Access Dienstgruppe abzuhören.

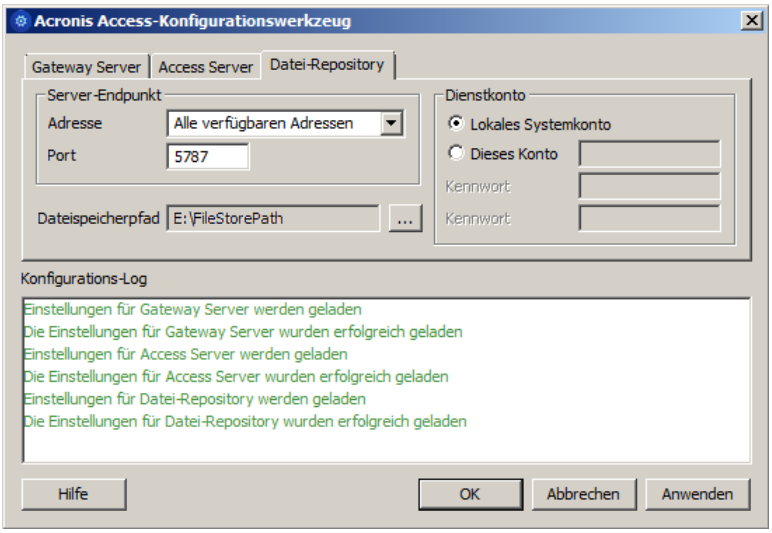


4. Konfigurieren Sie den Acronis Access Server-Dienst, um die IP-Adresse(n) für die Acronis Access Dienstgruppe abzuhören.

Hinweis: *Wenn* ***Verbindungen an Port 80 akzeptieren*** *ausgewählt ist, hört Tomcat den unsicheren Port 80 auf eingehenden Datenverkehr hin ab und leitet ihn zum HTTPS-Port um, den Sie zuvor festgelegt haben.*



5. Konfigurieren Sie das Acronis Access Datei-Repository, um 'localhost' abzuhören, und ändern Sie den Dateispeicherpfad in ein Verzeichnis auf dem freigegebenen Laufwerk. Dieser Pfad sollte für beide Knoten gleich sein.



6. Klicken Sie auf **OK**, um die Konfiguration abzuschließen, und starten Sie die Dienste neu.

Installation und Konfiguration auf dem zweiten Knoten

1. Deaktivieren Sie alle vorhandenen Virenschutzprogramme, da sie unter Umständen den Installationsvorgang unterbrechen und somit eine fehlerhafte Installation verursachen können.
2. Installieren Sie Acronis Access auf dem zweiten Knoten, verwenden Sie jedoch diesmal den Standardspeicherort für **Postgres Data** sowie dasselbe postgres-Benutzerkennwort wie für den ersten Knoten.
3. Schließen Sie die Installation ab.
4. Konfigurieren Sie die Gateway Server-Datenbank, sodass sie sich auf einem freigegebenen Laufwerk befindet.
   a. Navigieren Sie zu **`C:\Program Files (x86)\Acronis\Access\Gateway Server\`**
      - Bei einem Upgrade lautet der Pfad: **`C:\Program Files (x86)\GroupLogic\mobilEcho Server\`**
   b. Suchen Sie die Datei **database.yml** und öffnen Sie sie mit einem Texteditor.
   c. Gehen Sie zu dieser Zeile: **`database_path: './database/'`** und ersetzen Sie **./database/** durch den gewünschten Pfad (z.B. **`database_path: 'S:/mobilEcho_cluster/database/'`**).

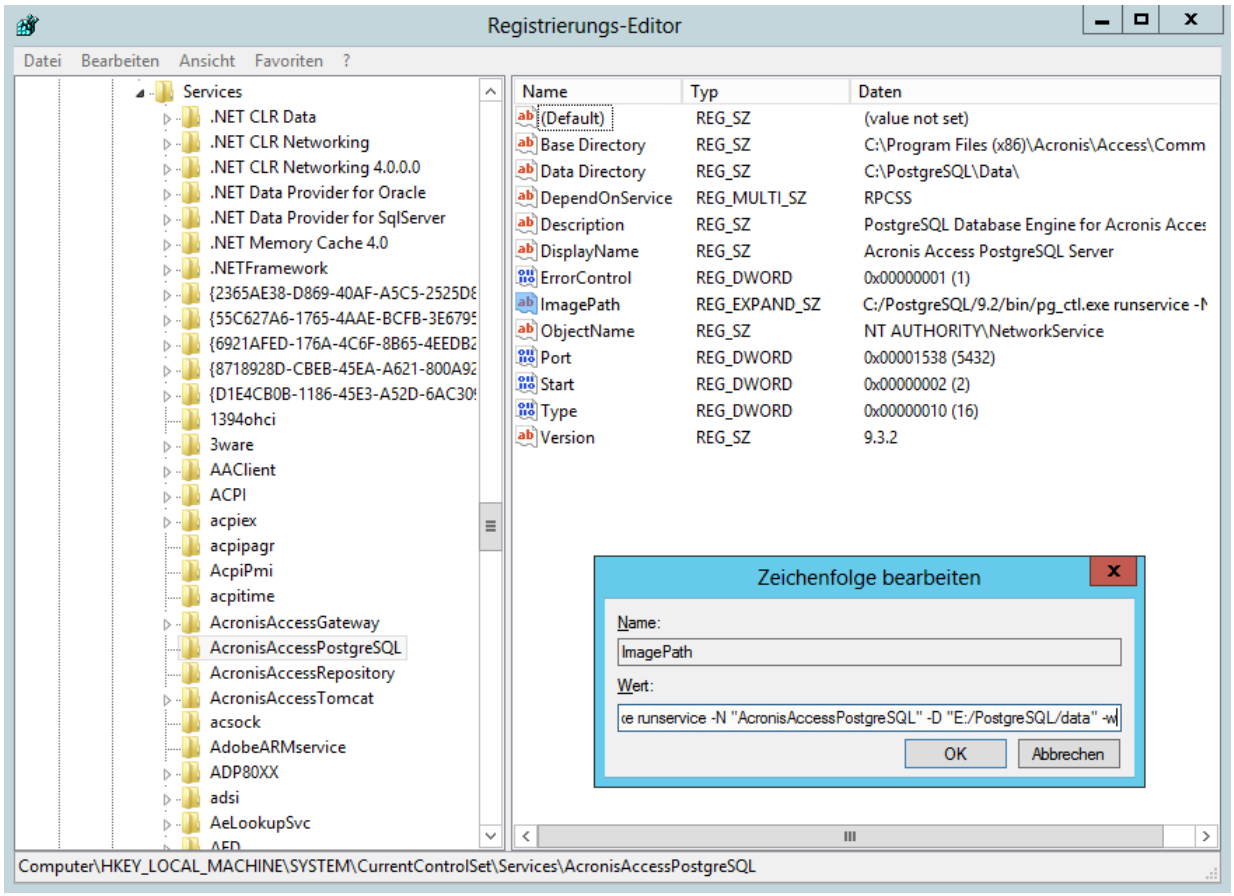
   Hinweis: *Verwenden Sie als Pfadtrennzeichen Schrägstriche (/).*

   Hinweis: *Sie können die konfigurierte Datei 'database.yml' aus dem ersten Knoten kopieren und im zweiten Knoten einfügen.*

   Hinweis: *Der Pfad sollte mit dem Pfad auf dem ersten Knoten übereinstimmen.*

Für PostgreSQL müssen Sie die Registry manuell replizieren:

1. Öffnen Sie **Regedit**.
2. Navigieren Sie zum Eintrag **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\postgresql-some version** und öffnen Sie den folgenden Schlüssel: **ImagePath**
3. Ändern Sie den Wert dieses Schlüssel in: **-D "The path you selected for the PostgreSQL data location" -w** (z.B. **-D "E:/PostgreSQL/data" -w**)

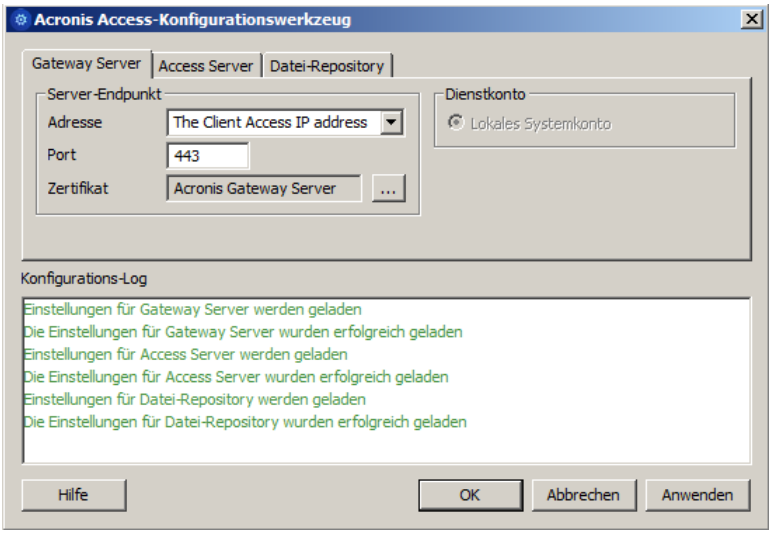


4. Schließen Sie **Regedit** und fahren Sie mit den unten stehenden Schritten fort.
5. Verschieben Sie die Acronis Access Rolle in den zweiten Knoten.

Verwenden des Konfigurationswerkzeugs auf dem zweiten Knoten

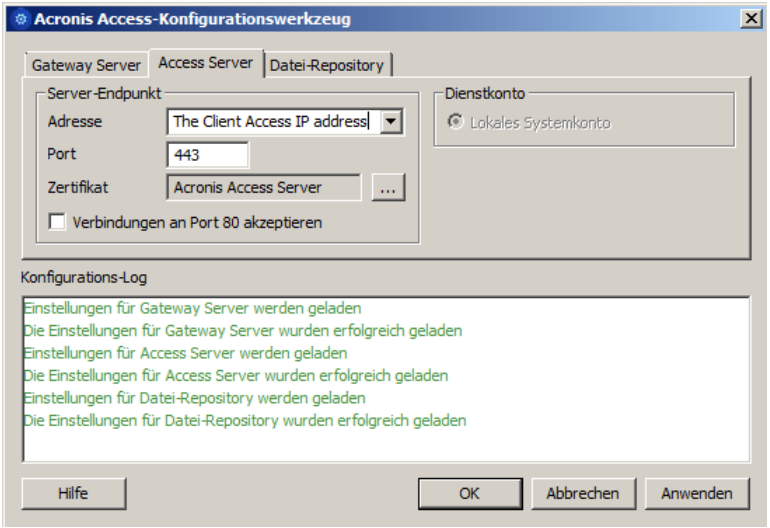
1. Starten Sie das Konfigurationswerkzeug.
   - Bei einer Neuinstallation befindet sich dies normalerweise unter **C:\Program Files (x86)\Acronis\Access\Configuration Utility**
   - Bei einem Upgrade von mobilEcho befindet es sich normalerweise unter **C:\Program Files (x86)\GroupLogic\Configuration Utility**

2. Konfigurieren Sie den Acronis Access Gateway Server-Dienst, um die IP-Adresse(n) für die Acronis Access Dienstgruppe abzuhören.

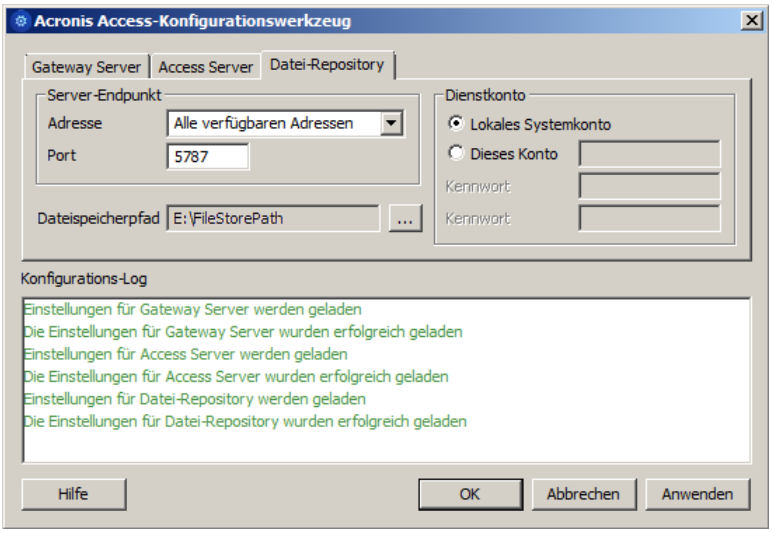


3. Konfigurieren Sie den Acronis Access Server-Dienst, um die IP-Adresse(n) für die Acronis Access Dienstgruppe abzuhören.

Hinweis: *Wenn* ***Verbindungen an Port 80 akzeptieren*** *ausgewählt ist, hört Tomcat den unsicheren Port 80 auf eingehenden Datenverkehr hin ab und leitet ihn zum HTTPS-Port um, den Sie zuvor festgelegt haben.*



4. Konfigurieren Sie das Acronis Access Datei-Repository, um 'localhost' abzuhören, und ändern Sie den Dateispeicherpfad in ein Verzeichnis auf dem freigegebenen Laufwerk. Dieser Pfad sollte für beide Knoten gleich sein.

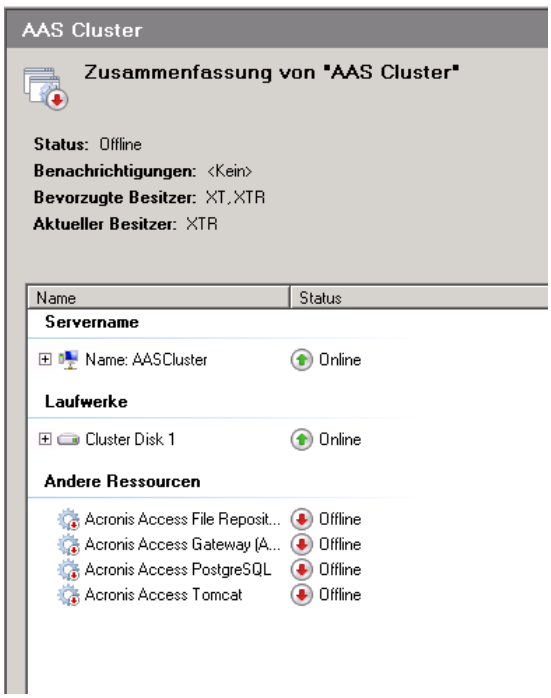


5. Klicken Sie auf **OK**, um die Konfiguration abzuschließen, und starten Sie die Dienste neu.

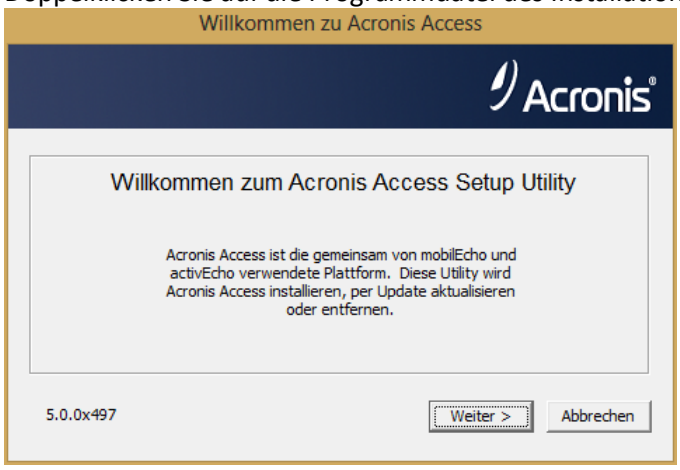
7.4 Upgrade von Acronis Access auf einem Microsoft Failover Cluster durchführen

Die folgenden Schritte helfen Ihnen dabei, ein Upgrade Ihres Acronis Access Server-Clusters auf eine neue Version von Acronis Access durchzuführen.

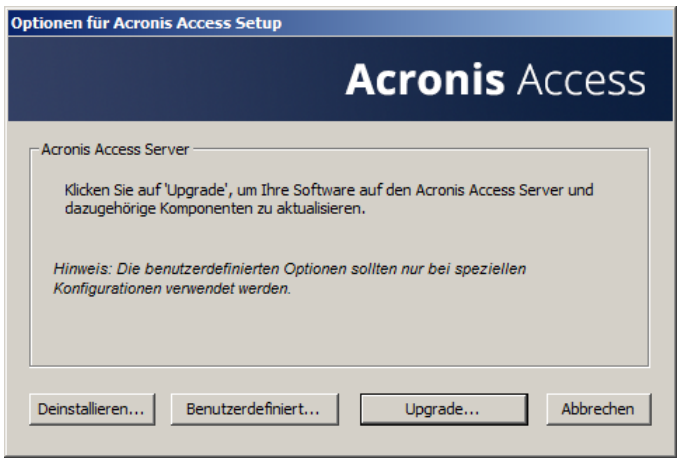
1. Gehen Sie zum aktiven Knoten.
2. Öffnen Sie die **Clusterverwaltung**/den **Failovercluster-Manager**.
3. Halten Sie alle Acronis Access Dienste an (darunter auch **postgres-beliebige-version**). Das freigegebene Laufwerk muss online geschaltet sein.



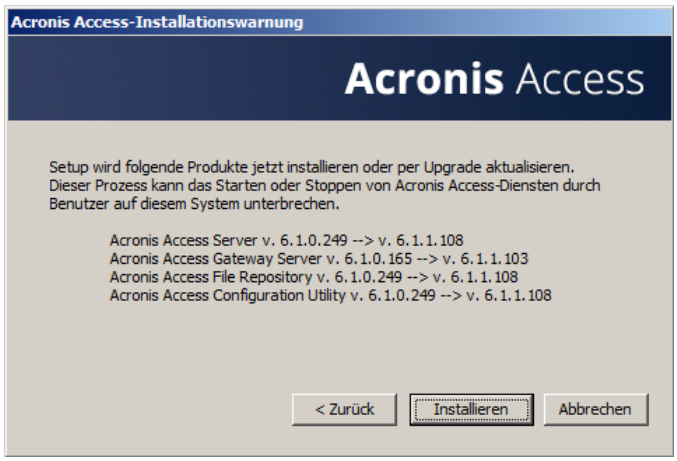
4. Deaktivieren Sie alle vorhandenen Virenschutzprogramme, da sie unter Umständen den Installationsvorgang unterbrechen und somit eine fehlerhafte Installation verursachen können.
5. Doppelklicken Sie auf die Programmdatei des Installationsprogramms.



6. Klicken Sie auf **Weiter**, um zu beginnen.
7. Lesen und akzeptieren Sie die Lizenzvereinbarung.
8. Drücken Sie **Upgrade**.



9. Überprüfen Sie die zur Installation ausgewählten Komponenten und klicken Sie auf **Installieren**.



10. Geben Sie das Kennwort des **postgres**-Super-Users ein und drücken Sie **Weiter**.

11. Drücken Sie nach Abschluss der Installation **Beenden**, um den Installer zu schließen.

Warnung! *Schalten Sie die Cluster-Gruppe nicht online!*

12. Verschieben Sie die Cluster-Gruppe zum zweiten Knoten.
13. Schließen Sie denselben Installationsvorgang auf dem zweiten Knoten ab.
14. Schalten Sie alle Acronis Access Dienste online.

8 Neuerungen

Themen

8.1 Neuerungen in Acronis Access Server

Acronis Access 6.1.1

VERBESSERUNGEN

- Verbesserte Authentifizierungsgeschwindigkeit für Benutzer in großen Active Directory-Katalogen, die sich auf der Acronis Access-Weboberfläche anmelden.
- Das Konfigurieren der Benutzer-Sychronisierungs- und Freigabe-Kontingente über die Access-API erfolgt nun in Gigabyte (GB).
- Verbesserte Fehlerbehandlungen von Gateway Server-Interaktionen mit Microsoft SharePoint.
- Organisatorische Einheiten und Domänen werden beim Erstellen von mobilen Zugriffsgruppenrichtlinien nicht mehr angezeigt, da sie nicht unterstützt werden.

BUG-FIXES

- Benutzer mit der reservierten Zeichenkette „data“ im Benutzernamen können nun die mobile App-Anmeldung abschließen.
- Folgendes Problem wurde behoben: der Acronis Access Gateway Server konnte mehrmals in der Access Mobile-App aufgelistet werden, wenn der Gateway Server so konfiguriert war, dass er sichtbar ist und ihm mehrere Datenquellenordner zugewiesen waren.
- Aktivieren/Deaktivieren der Protokollierung für eine Acess Server Cluster-Gruppe wurde behoben.
- Behandelt ein Abhängigkeitsproblem, das möglicherweise verhindert, das der Access Gateway Service nach einem Neustart von Windows Server 2008R2 automatisch startet.

Acronis Access 6.1

VERBESSERUNGEN

- Webdienste-API für die Verwaltung von Acronis Access Server. Die API-Dokumentation ist innerhalb des Access Servers verpackt und Administratoren können darauf zugreifen. Der Link befindet sich in der Fußzeile.
- Das Acronis Access Überwachungsprotokoll kann jetzt so konfiguriert werden, dass alte Protokolleinträge automatisch exportiert und bereinigt werden. Die Einstellungen für Exportieren und Bereinigen können auf der Seite 'Überwachungsprotokoll => Einstellungen' festgelegt werden.
- Neues Acronis Access Konfigurationsübersichtswerkzeug sammelt relevante Serverkonfigurationsdetails, die an den Acronis Support gesendet werden.

- Verbesserte Anmeldeleistung durch allgemeine Leistungsverbesserungen und durch Zwischenspeichern der Informationen zur Active Directory-Gruppenmitgliedschaft.
- Administratoren können jetzt eine Vorschau benutzerdefinierter E-Mail-Vorlagen anzeigen, bevor diese gespeichert werden.
- Das Logo und das Farbschema des Acronis Access Servers können jetzt ohne weiteres angepasst werden. Informationen zum Anpassen des Servers finden Sie in der folgenden Dokumentation: Weboberfläche anpassen (S. 133).
- Mit einer neuen E-Mail-Vorlage kann nun die E-Mail angepasst werden, die an neu eingeladene Administratoren gesendet wird, die keinen Sync & Share-Zugriff haben.
- Die Registerkarte für die Gateway Server-Protokollierung wird jetzt über die Menüoption 'Bearbeiten' und nicht mehr über 'Details' aufgerufen.
- Wenn Registrierungseinladungen hinzugefügt werden, geht nun aus den Suchergebnissen hervor, ob für den betreffenden Benutzer bereits registrierte Geräte vorhanden sind.
- Acronis Access sendet jetzt eine E-Mail an den ursprünglichen Absender, wenn in dessen Auftrag gesendete E-Mails wegen einer ungültigen E-Mail-Adresse des Empfängers nicht zugestellt werden können.
- Whitelists und Blacklists können dem Standardprofil jetzt über die Seite 'Erlaubte Apps' zugewiesen werden.
- Administratoren können auf der Seite 'LDAP-Einstellungen' auf einen Link klicken, um die Aktualisierung aller zwischengespeicherten LDAP-Informationen zu erzwingen.
- Bereitgestellte LDAP-Administratorgruppen können jetzt für den Sync & Share-Zugriff konfiguriert werden.
- Cluster-Gruppenmitglieder können nun über das Menü der Cluster-Gruppe hinzugefügt werden.
- Unterstützung für Windows 8.1.
- Unterstützung des Installationsprogramms für Installationen, bei denen sich PostgreSQL auf einem anderen Server befindet.
- Verbesserter PostgreSQL-Installationsprozess.
- Verbesserter Deinstallationsprozess.
- Verbesserte Fehlerberichterstattung in der Weboberfläche.

BUG-FIXES

- Die Anzahl aktiver Sitzungen wird aktualisiert, wenn die Seite 'Gateway Server' neu geladen wird.
- Type-ahead-Suche zur Auswahl von Benutzern, die zu freigegebenen Dateien und Ordnern eingeladen werden sollen, wird jetzt in Internet Explorer 8 unterstützt.
- Der Dienst Acronis Gateway Server hängt jetzt von anderen wichtigen Diensten ab, damit sichergestellt ist, dass er beim Start des Servers ordnungsgemäß gestartet wird.
- Wenn eine Cluster-Gruppe aufgelöst wird, werden alle Richtlinien, die diese Gruppe als Gateway Server für den Zugriff auf 'Meine Netzwerkordner' (vom Benutzer hinzugefügte Speicherorte) nutzen, so aktualisiert, dass sie stattdessen den letzten Gateway Server verwenden, der Mitglied der Cluster-Gruppe war.
- Ein Problem bei der Filterung von E-Mail-Adressen für registrierte Benutzer wurde behoben.
- Administratoren wird kein kritischer Fehler mehr angezeigt, wenn sie die Spracheinstellung nach Erhalt einer Fehlermeldung ändern.

- Administratoren können nach der Aktualisierung eines abgelaufenen Servers nun problemlos Testerweiterungen anwenden.
- Sobald sie sich erfolgreich authentifiziert haben, werden LDAP-Benutzer mit Sync & Share-Zugriff jetzt stets als LDAP-Benutzer aufgelistet, auch wenn ihre E-Mail-Domäne nicht mit den Domänen für die LDAP-Authentifizierung übereinstimmt. Administratoren können aus LDAP hinzugefügt werden, auch wenn die E-Mail-Domäne nicht in den Domänen für die LDAP-Authentifizierung enthalten ist.
- Wenn Administratoren neue Benutzer oder Administratoren hinzufügen, erhalten sie sofort eine Fehlermeldung, wenn sie einen Benutzer mit einer ungültigen E-Mail-Adresse hinzufügen.
- Ausstehende Einladungen werden jetzt einwandfrei gelöst, um vorhandenen Administratoren Sync & Share-Zugriff zu gewähren.
- Im Export der Benutzertabelle ist jetzt das Feld 'Lizenziert' enthalten.
- Beim Senden eines Download-Links werden nun die Blacklist- und die Whitelist-Beschränkungen berücksichtigt.
- Die Suche nach neuen zu registrierenden LDAP-Benutzern erfolgt jetzt wesentlich schneller.
- Neue Benutzer, die sowohl einer bereitgestellten LDAP-Administratorgruppe als auch einer bereitgestellten LDAP-Sync & Share-Gruppe angehören, erhalten kombinierte Berechtigungen.
- Die Zuordnung eines Basisverzeichnisses zu einer vorhandenen Datenquelle funktioniert jetzt einwandfrei, wenn die verfügbare Datenquelle den Platzhalter %USERNAME% verwendet.
- Bei LDAP-Suchvorgängen werden keine integrierten Gruppen mehr angezeigt, die für Gruppenmitgliedschaften nicht zulässig sind.
- Langsame Basisverzeichnis-Lookups führen nicht mehr dazu, dass sich mobile Benutzer nicht registrieren können.
- Es wurde ein Problem behoben, das dazu führen konnte, dass unter Windows 2003 R2 die Authentifizierung von zugewiesenen Quellen und der Zugriff auf zugewiesene Quellen mit Zertifikaten fehlschlugen.
- Nicht lizenzierte Ad-hoc-Benutzer werden jetzt ordnungsgemäß daran gehindert, mit dem Client eine Verbindung zum Server herzustellen.
- Die Informationen in der Tabelle der Gateway Server werden nun sofort aktualisiert, nicht erst beim Öffnen der Detailregisterkarte des Servers.
- Die kosmetische 'Von'-Adresse in von Acronis Access gesendeten E-Mails wird jetzt als tatsächliche E-Mail-Adresse des Absenders angezeigt.
- Alte Acronis Access Seriennummern werden nun entfernt, wenn eine neue Basisseriennummer angewendet wird.
- Das Installationsprogramm erstellt beim Upgrade nicht mehr mehrere Gateway Server-Einträge in 'Programme und Funktionen'.
- Behobenes Arbeitsspeicherleck in Gateway-Server.

Acronis Access 6.0.2

BUG-FIXES

- Umfasst eine aktualisierte OpenSSL-DLL zur Behebung der Anfälligkeit gegenüber **HeartBleed**.

Acronis Access 6.0.1

VERBESSERUNGEN

- Es wurde eine neue Richtlinie hinzugefügt, mit der festgelegt wird, mit welchem Gateway oder welcher Cluster-Gruppe die zugewiesenen Active Directory-Basisverzeichnisse von Benutzern freigegeben werden. Zugewiesene Active Directory-Basisverzeichnisse werden jetzt automatisch von einem Gateway freigegeben, ohne dass eine Datenquelle manuell erstellt oder die Richtlinieneinstellung 'Benutzern erlauben, Netzwerkordner anhand von UNC-Pfad oder URL hinzuzufügen' aktiviert werden muss.
- Auf der Seite 'LDAP-Einstellungen' steht nun die neue Einstellung 'Cache-Intervall für LDAP-Informationen' zur Verfügung. Damit können Administratoren angeben, wie oft der Acronis Access Server zwischengespeicherte Informationen über LDAP-Benutzer und -Gruppen aktualisiert.
- Auf der Seite 'Einstellungen für mobilen Zugriff' gibt es die neue Einstellung 'Benutzerprinzipalname (UPN) zur Authentifizierung an Gateway Servern verwenden'. Wenn sie aktiviert ist, authentifizieren sich Benutzer unabhängig vom Format des Benutzernamens, mit dem sie sich registriert haben, mit ihrem UPN an Gateway Servern. Ist diese Option deaktiviert, werden Benutzer mit dem Benutzernamen in dem Format authentifiziert, mit dem sie sich registriert haben.
- Es wurden Leistungsverbesserungen bei der Festlegung von LDAP-Gruppenmitgliedschaften erzielt. Diese beschleunigen die Registrierung und Authentifizierung. Zur Leistungssteigerung werden geschachtelte LDAP-Verteilergruppen beim Festlegen der Gruppenmitgliedschaft nicht mehr automatisch einbezogen. Wenn in Ihrer Konfiguration Mitglieder von geschachtelten Verteilergruppen einbezogen werden müssen, aktivieren Sie auf der Seite 'LDAP-Einstellungen' die neue Einstellung 'Mitgliedschaft in geschachtelter Verteilergruppe einschließen'.

FEHLERBEHEBUNGEN

- Der Access Desktop Client stürzt unter Windows nicht mehr ab, wenn der Client eine große Anzahl von Dateien herunter- oder hochlädt.
- Gateway Server werden nun automatisch kontaktiert, nachdem sie in neuen Installationen hinzugefügt wurden, damit sie umgehend einer Cluster-Gruppe hinzugefügt werden können oder Self-Provisioning für sie aktiviert werden kann.
- Die Sync & Share-Funktionalität und Datenquellen funktionieren nun in der Übergangsphase nach Ablauf der Lizenz weiterhin.
- Warnmeldungen zur Lizenzierung von Überwachungsprotokollen sind nun in allen Fällen richtig lokalisiert.
- Volumes bleiben weiterhin verfügbar, wenn deren Parameter den senkrechten Strich (‘|’) enthalten.
- Das Senden von Links oder Einladungen in der mobilen Acronis Access-Applikation schlägt nicht mehr fehl, wenn das Gerät für andere Sprachen als Englisch, Französisch, Deutsch oder Japanisch konfiguriert ist.
- Das Installationsprogramm erstellt beim Upgrade für nicht-englische Installationen nicht mehr mehrere Gateway-Servereinträge in 'Programme und Funktionen'.
- Es wurde ein Fehler behoben, der dazu führte, dass der Acronis Access Tomcat-Dienst zeitweise nicht richtig gestartet wurde und neu gestartet werden musste, damit Clients eine Verbindung herstellen konnten.

- Es wurde ein Fehler behoben, der dazu führte, dass Clients, die gemäß Konfiguration Anmeldedaten 'einmal pro Sitzung' verlangen sollten, den Benutzer bei der Herstellung einer Verbindung zum Management Server zur Eingabe eines Kennworts aufforderten, nachdem für den Server ein Upgrade von 4.x durchgeführt wurde.
- Selbst bereitgestellte Ordner können nun erfolgreich hinzugefügt und entfernt werden, wenn das Profil zur Verwendung eines Gateway Servers oder einer Cluster-Gruppe konfiguriert ist, unabhängig davon, ob der Server oder die Cluster-Gruppe online ist.
- Die Priorisierung der Richtlinien wird respektiert, sodass Benutzer die Gruppenrichtlinie mit der höchsten Priorität erhalten, zu der sie berechtigt sind.
- Clients, bei denen die Sync & Share-Funktion nicht aktiviert ist, werden im Überwachungsprotokoll nicht mehr fälschlicherweise als 'nicht verwaltet' aufgeführt.
- Bei Dateien mit japanischen oder ähnlichen Zeichen im Dateinamen wird der Dateiname nicht mehr geändert, wenn sie mit Internet Explorer heruntergeladen werden.
- Beim Ablauf von Abonnementlizenzen werden Administratoren keine unlösbaren Fehler mehr angezeigt.
- Die Liste der Access Desktop Client-Mindestversionen enthält nun richtigerweise 3.0-Client-Versionen und wird sowohl für alte als auch für neue Desktop-Clients eingehalten.
- Basisverzeichnisse sollten nach Upgrades von mobilEcho-Versionen vor 5.0 weiterhin verfügbar sein.
- Verschiedene Fehlerbehebungen bei der Lokalisierung.

Acronis Access 6.0.0

VERBESSERUNGEN

- Die Produkte mobilEcho und activEcho wurde zu einem neuen Produkt mit der Bezeichnung Acronis Access Server kombiniert. Dadurch ändern sich die Marken- und Produktbezeichnungen im mobilen und im Desktop-Client sowie in der Web-Applikation. Acronis Access Server 6.0 kann als Upgrade zu mobilEcho bzw. activEcho installiert werden. Die vorhandenen Lizenzen funktionieren weiterhin. Die Kunden haben das Recht, ihre vorhandenen mobilEcho- bzw. activEcho-Lizenz(en) gegen eine neue Acronis Access-Lizenz umzutauschen, mit der der volle Funktionsumfang des kombinierten Produkts aktiviert wird. Um dieses Upgrade anzufordern, **schicken Sie dieses Webformular ab**.
- Active Directory-basierten Administratorbenutzern muss keine E-Mail-Adresse mehr zugewiesen werden. Administratorbenutzer können zudem hinzugefügt werden, ohne den Acronis Access Server für SMTP zu konfigurieren.
- Unter 'Server-Einstellungen' findet sich ein neues Kontrollkästchen, mit dem die Sync & Share-Funktion ein- oder ausgeschaltet werden kann. Bei einem Upgrade von mobilEcho zu Acronis Access Server wird Sync & Share (früher activEcho) standardmäßig deaktiviert.
- Active Directory-Verteilungsgruppen können jetzt zu Sync & Share-Ordnern eingeladen werden.
- Zahlreicher Benutzer werden jetzt wesentlich schneller zu Sync & Share-Ordner eingeladen.
- Das Konfigurationswerkzeug zeigt jetzt mehr Status-/Fortschrittsmeldungen beim Einrichten des Servers an.

- Das Konfigurationswerkzeug erzeugt jetzt einen Fehler, wenn sich das Repository auf einem Remote-Netzwerk-Volume befindet, der Repository-Dienst jedoch für die Ausführung unter dem lokalen Systemkonto konfiguriert ist. Der Repository-Dienst muss unter einem Konto mit Berechtigungen für das Remote-Netzwerk-Volume ausgeführt werden.
- Das Konfigurationswerkzeug zeigt jetzt einen Fehler an, wenn ein SSL-Zertifikat ausgewählt wird, das keinen eingebetteten privaten Schlüssel enthält.
- Java wurde auf Version 7 Update 51 aktualisiert.
- Der unter 'Server-Einstellungen' festgelegte Server-Name wird jetzt als Titel der Website verwendet, die den Endbenutzern angezeigt wird.
- Das Aktualisierungsintervall für den LDAP-Cache wurde von 60 auf 15 Minuten geändert.
- Eine neue erweiterte Einstellung für Gateway Server wurde hinzugefügt, die bei Aktivierung die Authentifizierung von Benutzern mit ihrem UPN (Beispiel: benutzername@domain.com) zulässt. Andernfalls authentifizieren sich die Benutzer per Domain und Benutzername (Beispiel: domain\benutzername). Dies ist gelegentlich bei der Authentifizierung in einigen Verbundszenarien erforderlich, z.B. SharePoint 365.

BUG-FIXES

- Die Einstellung 'Standardsprache' in den 'Server-Einstellungen' wurde umbenannt, um zu verdeutlichen, dass es sich um die Überwachungsprotokoll-Standardsprache handelt.
- Wenn eine Datenquelle für einen Active Directory-Basisordner nicht aufgelöst werden kann, können die mobilen Clients den Basisordner nicht mehr sehen. Beim Zugriff auf !HOME_DIR_SERVER wird jetzt kein Fehler mehr angezeigt.
- Verschiedene Fehlerbehebungen im Acronis Access Desktop Client.
- Verschiedene Verbesserungen der Lokalisierung.

Acronis Access 5.1.0

VERBESSERUNGEN

- Das Konfigurationswerkzeug bietet jetzt die Möglichkeit zu steuern, ob der Access Server an HTTP-Port 80 gebunden werden und automatisch zum konfigurierten HTTPS-Port umgeleitet werden soll. Dies war zuvor standardmäßig aktiviert, jetzt muss der Administrator diese Einstellung bei Neuinstallationen aktivieren.
- Beim Bearbeiten von E-Mail-Vorlagen erlaubt eine neue Option dem Administrator, den Standardwert für den E-Mail-Betreff anzuzeigen.
- Benutzer mit mobilEcho 5.1 oder später unter iOS können Datenquellen jetzt direkt aus der Anwendung erstellen, um auf eine beliebige Dateifreigabe oder einen SharePoint-Speicherort zuzugreifen. Benutzer geben UNC-Pfade oder SharePoint-URLS über den Client ein. Es wurden neue Richtlinieneinstellungen auf dem Management-Server eingeführt, um zu steuern, ob Clients berechtigt sind, diese Datenquellen zu erstellen, und um zu steuern, welche Gateway Server für diese Anforderungen verwendet werden.

- Mehrere Gateway Server können jetzt im Rahmen einer Cluster-Gruppe eine gemeinsame Konfiguration nutzen. Änderungen an den Einstellungen und Richtlinien, die der Cluster-Gruppe zugewiesen sind, werden automatisch an alle Mitglieder der Gruppe übertragen. Dies wird in der Regel dann eingesetzt, wenn mehrere Gateway Server für eine hohe Verfügbarkeit hinter einem Lastenausgleichsmoduls platziert werden.
- Gateway Server unterstützen nun die Authentifizierung mit Kerberos. Dies kann in Szenarien eingesetzt werden, in denen die eingeschränkte Kerberos-Delegierung verwendet wird, um mobilEcho iOS-Clients über einen Reverse-Proxy mit Client-Zertifikaten zu authentifizieren. Es kann auch für die Authentifizierung von mobilen Geräten mit Client-Zertifikaten mithilfe von MobileIron AppTunnel verwendet werden. Beachten Sie, dass bei dieser Authentifizierungsform mobile Clients nicht auf activEcho-Freigaben zugreifen können.
- Die erforderlichen Datenquellen werden jetzt automatisch erstellt, wenn Basisordner einer Benutzer- oder Gruppenrichtlinie zugewiesen werden. Zuvor mussten Administratoren manuell eine Datenquelle für den Server erstellen, auf dem das Basisverzeichnis gehostet wird.
- Die Adresse eines alten Gateway Servers kann jetzt geändert werden.
- Die Richtlinienausnahmen für Android wurden um die Funktionen des mobilEcho Android 3.1 Clients erweitert.

BUG-FIXES

- Das Exportieren einer großen Menge Datensätze aus dem Überwachungsprotokoll wurde erheblich beschleunigt.
- Fehlermeldungen aus einigen Dialogfeldern werden jetzt einwandfrei gelöscht, wenn die Fehlerbedingung aufgelöst ist.
- Jetzt kann immer nur eine Instanz des Konfigurationswerkzeugs ausgeführt werden.
- Unter Windows Server 2003 wird bei der Deinstallation nicht mehr gemeldet, dass PostgreSQL vom Acronis Access Server-Installer nicht installiert wurde.
- Das Konfigurationswerkzeug erzeugt jetzt einen Fehler, wenn der Gateway-Dienst so konfiguriert ist, dass alle Adressen an einen Port und der Access Server an eine bestimmte Adresse bei demselben Port gebunden werden.
- Bei Neuinstallationen wird Tomcat standardmäßig jetzt so konfiguriert, auf Port 8005 nicht auf Anforderungen zum Herunterfahren zu warten. Dies verhindert Konflikte mit anderen Instanzen von Tomcat auf einem Server. Da die Access Server Tomcat-Instanz als Dienst ausgeführt wird, werden über Netzwerkports gesendete Anforderungen zum Herunterfahren nicht benötigt.
- Verschiedene Verbesserungen der Lokalisierung.
- Verbesserte Protokollanzeigeleistung für Nicht-Administratoren.
- Benachrichtigungen über abgelaufene Lizenzen werden nicht mehr angezeigt, wenn activEcho über den Access Server Administrator deaktiviert wurde.
- Neue Benutzer, die eine Einladungs-E-Mail erhalten, werden in einer Nachricht aufgefordert, ein Kennwort festzulegen, anstatt das Kennwort zu ändern.
- Das Dialogfeld 'Neue Dateien hochladen' enthält kein zusätzliches Feld, wenn Internet Explorer 8 oder 9 verwendet wird.
- Der Windows Desktop Client lädt in bestimmten Situationen, in denen das Kennwort des Benutzers abläuft und erneut eingegeben wird, Inhalte nicht mehr erneut hoch.
- Sonstige Fixes an der Dateisynchronisierungslogik für Desktop Client

- Durch Entfernen einer Benutzer- oder Gruppenrichtlinie mit einem benutzerdefinierten Basisordner wird jetzt das Volume auf dem Gateway Server ordnungsgemäß entfernt.
- Bei der Anzeige von 'Zugewiesene Quellen' für einen Benutzer werden jetzt Quellen angezeigt, die diesem Benutzer über die Gruppenmitgliedschaften zugewiesen wurden.
- Die Reihenfolge der Registerkarten auf der Verwaltungsseite 'Datenquellen' wurde verbessert.
- Beim Ändern der Gateway Server-Verwaltungsadresse wird das Bearbeitungsdialogfeld durch Klicken auf 'Anwenden' nicht mehr geschlossen.
- mobilEcho Clients, die mit Client-Zertifikaten für das Management registriert werden, schlagen nicht mehr regelmäßig fehl, wenn der Benutzer sich noch nicht im LDAP-Cache des Servers befand.
- Durch Einfügen von Leerstellen in Gateway Server-Adressen wird eine ordnungsgemäße Verwaltung des Gateway Servers nicht mehr behindert.
- Hinweise im Dialogfeld 'Geräteinformationen' werden jetzt ordnungsgemäß gespeichert.
- Wenn Richtlinien deaktiviert wurden, werden sie jetzt in der Richtlinienliste ausgegraut angezeigt.
- Bei einem Upgrade von mobilEcho Server 4.5 werden die mobilEcho-Benutzer jetzt ordnungsgemäß importiert, auch dann, wenn die falsche LDAP-Suchbasis im Konfigurationsassistenten eingegeben wurde.
- Lizenzschlüssel, die mit 'YD1' beginnen, werden jetzt auf der Lizenzierungsseite ordnungsgemäß als Testschlüssel mit einem Ablaufdatum angezeigt, und nicht mehr als unbefristete Lizenzen.
- Einladungs-E-Mails für die Registrierung enthalten jetzt die richtigen Links für Android-Clients.
- Die Bearbeitung von SharePoint-Anmeldeinformationen für einen Gateway Server ist jetzt deaktiviert, wenn der Gateway Server nicht über eine Lizenz verfügt, die die SharePoint-Verbindung unterstützt.

Acronis Access 5.0.3

VERBESSERUNGEN

- Acronis Access Server kann jetzt unter Windows Server 2003 SP2, 2008/2008R2 und 2012/2012R2 auf einem Windows-Failovercluster installiert werden. Informationen zur Installation oder zum Upgrade mit dieser Konfiguration finden Sie unter Acronis Access in einem Cluster installieren (S. 180) und Upgrade von Acronis Access in einem Cluster (S. 221).

BUG-FIXES

- E-Mail-Benachrichtigungen werden jetzt nach einem Upgrade ordnungsgemäß versandt, wenn benutzerdefinierte Vorlagen verwendet wurden.
- Beim Konfigurieren von Datenquellen kann jetzt das Token '%USERNAME%' als Teil des Ordnernamens anstelle des ganzen Namens verwendet werden.
- Neu erstellte Datenquellen werden jetzt geprüft, um zu ermitteln, ob sie unmittelbar durchsucht werden können. Zuvor wurde nur alle 15 Minuten eine Prüfung durchgeführt.
- Die Suche ist jetzt für Datenquellen verfügbar, die nach dem Start des Gateway Servers einen Suchindex hinzufügen.

Acronis Access 5.0.2

VERBESSERUNGEN

- Acronis Access Server wurde für Windows Server 2012 R2 zertifiziert.
- LDAP-Administratoren können jetzt auch dann hinzugefügt werden, wenn SMTP nicht konfiguriert ist.
- Das Konfigurationswerkzeug erstellt beim Anwenden von Änderungen keine doppelten Firewall-Regeln mehr.
- Die Authentifizierung für umfangreiche LDAP-Strukturen mit mehreren Domains erfolgt jetzt erheblich schneller als zuvor.
- Die Leistung des activEcho Clients bei einer großen Anzahl Updates wurde verbessert.
- Die Ordnerliste auf der Seite 'Datenquellen' zeigt den zugewiesenen Gateway Server jetzt mit seinem Anzeigenamen anstatt mit der IP-Adresse an.

BUG-FIXES

- Lokalisierungsverbesserungen.
- Die Deinstallation kann jetzt auch unter Windows Server 2003 über das Installationsprogramm gestartet werden.
- Das Installationsprogramm erzwingt vor der Installation mindestens 1 GB freien Festplattenspeicher.
- Upgrades von activEcho 2.7 funktionieren auf nicht englischen PostgreSQL-Installationen jetzt fehlerfrei.
- Clients können jetzt auf Datenquellen mit einem Doppelpunkt im Namen zugreifen.
- Bei Upgrades von mobilEcho 4.5 wird die Migration von SharePoint-Datenquellen jetzt ordnungsgemäß durchgeführt.
- Nach einem Upgrade werden die einem Benutzer zugewiesenen Ressourcen jetzt ordnungsgemäß auf der Registerkarte 'Zugewiesene Quellen' der Seite 'Datenquellen' angezeigt.
- Beim Sortieren der Tabelle 'Aktive Benutzer' nach Richtlinie oder Leerlaufzeit wird kein Fehler mehr generiert.
- Clients können jetzt auf Gateway Server zugreifen, die als auf Clients sichtbar bereitgestellt werden und unterschiedliche Adressen für Client-Verbindungen aufweisen.
- Folgendes Problem wurde behoben: Basisordner wurden manchmal nicht im mobilEcho Client geöffnet, wenn der Access Server Datenquellen mit ähnlichen Pfaden enthielt (z.B. „\\homes“ und „\\homes2“)

Acronis Access 5.0.1

BUG-FIXES

- Folgendes Problem wurde behoben: Die Datenbankmigration von mobilEcho 4.5 auf 5.0 schlug fehl, wenn Gerätekennwörter in einer früheren Version von mobilEcho zurückgesetzt wurden, dieser Vorgang aber noch ausstehend war. In diesem Fall wurde beim Start des Servers ein Fehler ähnlich dem Folgenden im Webbrowser angezeigt:

ActiveRecord::JDBCError: ERROR: value too long for type character varying(255): INSERT INTO "password_resets" ....
Customers that have this condition can upgrade to this new version of the server and the problem will be resolved automatically.

- Die Ursache für folgendes Problem wurde behoben: Nach dem Upgrade auf mobilEcho 5.0 wechselten einige Clients in den eingeschränkten Modus.
- In den Datenquellentabellen des Management Servers wird jetzt der Anzeigename des Gateway Servers anstelle der IP-Adresse angezeigt.

Acronis Access 5.0.0

VERBESSERUNGEN

- Acronis Access Server ist eine neue gemeinsam genutzte Plattform für mobilEcho und activEcho. Beide Produkte verwenden nun die gleiche Backend-Infrastruktur. Die Funktionen jedes Produkts werden durch die Lizenzierung bestimmt und entsprechend aktiviert.
- Neues integriertes Installationsprogramm für die Plattform. Acronis Access Server, mobilEcho und activEcho sind im Installationsprogramm enthalten. Die Laufzeit-Installationsoptionen für das Installationsprogramm erlauben es dem Administrator zu bestimmen, welche Elemente installiert werden.
- Mit Acronis Access Server werden automatisch die Java JRE und die benötigten Richtliniendateien der Java Cryptographic Engine installiert.
- Mit dem neuen Serverkonfigurationsprogramm können Administratoren grundlegende Konfigurationsoptionen wie die Bindung an bestimmte IP-Adressen und Ports, die Verarbeitung von Firewall-Regeln auf der lokalen Maschine und die Installation von SSL-Zertifikaten festlegen.
- Acronis Access Server ist in englischer, deutscher, japanischer und französischer Sprache verfügbar.
- Neuer Startassistent vereinfacht die Erstkonfiguration des Servers.
- Neu gestaltete, aktualisierte Benutzer- und Verwaltungs-Weboberflächen, inklusive eines benutzerfreundlichen Designs mit Unterstützung für mobile Geräte.
- Neue Paging-Tabellen unterstützen Anzeige, Sortierung und Filterung wesentlich größerer Datenmengen. Die Protokollfilterung wurde verbessert, einschließlich der Filterung durch Eingabe von Teilen von Benutzernamen, nach Nachrichtentyp usw.
- Neu gestaltete, benutzerfreundliche Projektanzeige für Endbenutzer.
- activEcho Clients (Mac/Windows) sind auch in deutscher, japanischer und französischer Sprache verfügbar.
- HTML5-Unterstützung für direktes Hochladen von Dateien per Drag & Drop in die Weboberfläche. Per Drag & Drop können in einem Vorgang eine oder auch viele Dateien hochgeladen werden.
- Verbesserte Verarbeitung von Datei-Uploads, inklusive Fortschrittsanzeigen in der Weboberfläche und Funktion zum Abbrechen von Uploads.
- Ordner können als zip-Datei aus der Projektansicht der Web-UI heruntergeladen werden.
- Einzelne Dateien können für andere Benutzer freigegeben werden. Diese Benutzer erhalten einen Link zum Herunterladen der Dateien, deren Ablauf konfiguriert werden kann.
- Die Dialogfelder für Freigabeeinladungen unterstützen nun Type-ahead für lokale Benutzer und Benutzer in Active Directory/LDAP.

- Die Funktionen zum Suchen/Herunterladen/Wiederherstellen früherer Dateiversionen wurden umgestaltet und sind nun flexibler. Frühere Versionen können nun als aktuelle Version festgelegt werden.
- activEcho Desktop-Clients (Mac/Windows) zeigen nun Fortschrittsanzeigen für derzeit synchronisierte Dateien an.
- In von Ihnen freigegebenen Ordnern ist eine neue Schaltfläche zum Beenden des Abonnements verfügbar.
- Die vom Endbenutzer gewählten Sortierkriterien werden nun beim Navigieren in Projektordnern gespeichert.
- Benachrichtigungen über Ereignisse können nun global als Standardeinstellungen für alle Freigaben konfiguriert werden. Benutzer können die Standards für einzelne Freigaben überschreiben.
- Es können Benachrichtigungen konfiguriert werden, die beim Herunterladen/Synchronisieren von Dateien gesendet werden.
- activEcho Clients führen unter Windows nun eine Validierung von SSL-Zertifikaten mit dem integrierten Zertifikatsspeicher von Windows aus. Damit verbessert sich die Kompatibilität mit Zertifizierungsstellen von Drittanbietern.
- Verbesserte Reaktionsfähigkeit der Benutzeroberfläche beim Neuzuweisen von Inhalten, wenn Tausende Benutzer im System aktiv sind.
- Der Amazon S3-Zugriffsschlüssel wird auf den Verwaltungsseiten nicht mehr als Klartext angezeigt.
- Verbesserte Seitenladezeiten bei vielen Benutzern und/oder Dateien, insbesondere, wenn Kontingente verwendet werden.
- Verbesserte Unterstützung für E-Mail-Einladungen mit unterschiedlichen Formaten der E-Mail-Adressen.
- In Domains können nun Platzhalterzeichen für die freizugebenden Black- und Whitelists verwendet werden.
- Administratoren können nun global das Kontrollkästchen 'Teilnehmern erlauben, andere Teilnehmer einzuladen' ausblenden.
- Im neuen Administrationsmodus kann zwischen den einzelnen Projekt-/Protokollansichten eines Benutzers und der Verwaltungskonsole gewechselt werden.
- mobilEcho Client Management wurde vollständig in eine gemeinsame Webverwaltungsoberfläche integriert. In dieser können mobile Clients für activEcho oder, wenn eine Lizenz für mobilEcho vorhanden ist, an einer einzigen Konsole alle Funktionen von mobilEcho und activEcho verwaltet werden.
- Benutzerlisten können nun exportiert werden.
- Der mobilEcho Client Management Server ist in Acronis Access Server integriert und beruht auf Apache Tomcat und PostgreSQL Datenbanken, um eine verbesserte Skalierbarkeit und Ausfallsicherheit zu gewährleisten.
- Der bisher zum Verwalten einzelner mobilEcho Server genutzte mobilEcho Administrator wurde entfernt. Access Gateway Server (früher mobilEcho File Access Server) werden nun direkt in der Benutzer-Weboberfläche für die Verwaltung von Acronis Access Server verwaltet.
- Die Konfigurationsdatei für mobilEcho Client Management Server wurde entfernt. Die bisher in der Konfigurationsdatei gespeicherten Konfigurationseinstellungen werden automatisch migriert und nun über die Benutzer-Weboberfläche für die Verwaltung von Acronis Access Server verwaltet.

- Die Konfiguration von Datenquellen (früher zugewiesene 'Ordner'), die für mobile Geräten freigegeben werden sollen, wurde umgestaltet.
- Neue Funktion 'Zugewiesene Quellen' ermöglicht es Administratoren, einen Bericht zu allen zugewiesenen Ressourcen abzurufen, die ein bestimmter Active Directory-Benutzer oder eine solche Gruppe erhält.
- Die Überwachungsprotokollierung kann für Berichte zu Aktivitäten mobiler Benutzer auf mehreren Acronis Access Gateway Servern aktiviert werden.
- Administratoren können nun unterschiedliche Berechtigungen für Verwaltungsaufgaben erhalten, darunter Benutzerverwaltung, Datenquellen, Richtlinien für mobile Geräte und Anzeige des Überwachungsprotokolls. Diese können für einzelne Benutzer und/oder Mitgliedschaften in Active Directory-Gruppen festgelegt werden.
- Gerätevorgänge wie Remote-Löschung oder Entfernen von Geräten aus der Geräteliste können nun batchweise ausgeführt werden.
- Es kann eine übergreifende 'Standardrichtlinie' konfiguriert werden, die für alle Benutzer gilt, die nicht den konfigurierten Richtlinien für Active Directory-Benutzer oder -Gruppen unterliegen.
- Neue Richtlinienoptionen ermöglichen die Festlegung, dass Inhalte in den Ordnern 'Meine Dateien' und 'Datei-Inbox' des Geräts ablaufen und nach einer bestimmten Zeitdauer entfernt werden.
- Beim Senden einer Registrierungseinladung an eine Active Directory-Gruppe können Benutzer, die bereits über eine andere Gruppe registriert sind, herausgefiltert werden.
- Es wird eine Warnung angezeigt, wenn ein Benutzer zur Registrierung eingeladen wurde, aber keiner bestehenden Benutzer-/Gruppenrichtlinie unterliegt.
- Die Gerätetabelle listet nun die für die einzelnen Geräte verwendeten Benutzer- oder Gruppenrichtlinien auf.
- Zwischengespeicherte Active Directory-/LDAP-Informationen zu Benutzern werden nun regelmäßig im Hintergrund aktualisiert.
- Die Inhaltssuche ist nun mit der Windows-Suche für Windows-Remote-Dateifreigaben verfügbar.
- Richtlinien können nicht gelöscht werden, wenn diese gerade zur Verwaltung eines Geräts verwendet werden.
- Vorlagen für Registrierungseinladungen für mobilEcho können direkt an der Webverwaltungskonsole geändert werden. Für jede Vorlage werden mehrere Sprachen unterstützt.
- In den Vorlagen für Registrierungseinladungen ist ein neues Token verfügbar, das den Anzeigenamen des Active Directory-Benutzers enthält.
- Die Bildschirme für Geräteliste und Gerätedetails geben nun an, ob die Geräte von Good Dynamics oder MobileIron AppConnect verwaltet werden.
- Die Unterstützung für die Authentifizierung an der Webverwaltungskonsole mit SSLv2 ist durch den Wechsel zum Apache Tomcat-Webserver nun veraltet.
- Unterstützung für Trace-Logging und Leistungsüberwachung mit New Relic.

BUG-FIXES

- Verbesserte Unterstützung für den Export von Unicode-Zeichen in txt- oder csv-Dateien.
- Für Ordner, die nicht freigegeben werden können, ist keine Einladungsfunktion mehr verfügbar.

- Benutzer können sich nun selbst auch dann aus der Freigabe entfernen, wenn sie keine Berechtigung zum Einladen anderer Benutzer zur Freigabe besitzen.
- Wenn eine Datei oder ein Ordner nicht auf einen Windows-Client heruntergeladen werden kann, weil der Name zu lang ist, wird der Fehler auf dem Client durch Deaktivieren der Option zum Synchronisieren auf Geräte in der Weboberfläche behoben, da der gesamte freigegebene Ordner entfernt wird.
- Wenn der Benutzer beim Hochladen von Dateien den kontingentierten Speicherplatz überschritten hat, behandeln activEcho Clients den Fehler ordnungsgemäß.
- Benutzer können nun auch dann gelöscht werden, wenn sie auf der Blacklist angegeben sind.
- Dateien können in das Repository hochgeladen werden, wenn die Verschlüsselung deaktiviert ist.
- Die Konfiguration des Basisverzeichnisses wird nun ordnungsgemäß abgerufen, wenn LDAP für die Verwendung des globalen Katalogs konfiguriert ist.
- Verbesserte Verarbeitung von Active Directory-Lookups bei Verwendung nachgestellter Leerzeichen.
- Das Registrierungsdatum wird beim Export in eine csv-Datei nun richtig formatiert.
- Verbesserte Unterstützung für die Unicode-Anzeige in der Benutzer-Weboberfläche für die Verwaltung.
- SharePoint-Ordner, die mit einem Leerzeichen enden, können von den Clients nun aufgelistet werden.
- SharePoint-Bibliotheken mit zusätzlichen Schrägstrichen unterstützen nun ordnungsgemäß das Löschen und Kopieren von Dateien.

8.2 Neuerungen in der Acronis Access-App

Access Mobile Client 6.1

VERBESSERUNGEN

- Unterstützung der Konfigurationsfunktionen für verwaltete Apps von iOS 7.
- Aktualisierung der Integration von MobileIron AppConnect in die Version 1.7.
- Behebung eines Problems, bei dem iWork-Dateien als ZIP-Dateien angezeigt werden können.
- Hinzufügung neuer mobilecho:// Linkvariablen (Aktion=bearbeiten & Aktion=Vorschau), die zum automatischen Öffnen einer verknüpften Datei verwendet werden können.
- Verschiedene Fehlerbehebungen und Verbesserungen.

Access Mobile Client 6.0.1

BUG-FIXES

- Absturz behoben, der auftreten kann, wenn PDF-Dokumente mithilfe des Stempelwerkzeugs mit Anmerkungen versehen werden.

Access Mobile Client 6.0

VERBESSERUNGEN

- Die mobile App mobilEcho heißt nun 'Acronis Access'.
- Verschiedene Fehlerbehebungen und Verbesserungen.

mobilEcho 5.1

VERBESSERUNGEN

- Neue Oberfläche im iOS 7-Stil implementiert.
- Netzwerkfreigaben und SharePoint-Speicherorte können nun in der App hinzugefügt werden, sofern Ihr mobilEcho-Profil dies zulässt.
- Unterstützung für die Authentifizierung per eingeschränkter Kerberos-Delegierung gegenüber mobilEcho Servern.
- Verschiedene Fehlerbehebungen und Verbesserungen.

mobilEcho 5.0

VERBESSERUNGEN

- Optionaler richtlinienbasierter Ablauf von geräteresidenten Dateien in 'Meine Dateien' und 'Datei-Inbox'.
- Optionen für die Schriftgröße bei der Vorschau oder Bearbeitung von Textdateien.
- In eine E-Mail können nun mehrere Dateianhänge eingefügt werden.
- Unterstützung für das Senden von Einladungen an freigegebene Dateien und Ordner von activEcho.
- Verschiedene Fehlerbehebungen und Verbesserungen.

mobilEcho 4.5.2

VERBESSERUNGEN

- Unterstützung für den Einsatz von Smartcards zum Entsperren der mobilEcho-App und zum Authentifizieren von mobilEcho Servern. Diese Funktion nutzt die Thursby PKard Reader-App sowie die Smartcards (CAC, PIV usw.) und Kartenleser, die die Thursby-App unterstützt.
- Verschiedene Fehlerbehebungen und Verbesserungen.

mobilEcho 4.5.1

- mobilEcho unterstützt nun iOS 7, sowohl als eigenständige App als auch als MobileIron AppConnect-fähige App.
- Verschiedene Fehlerbehebungen und Verbesserungen.

mobilEcho 4.5

VERBESSERUNGEN

- Bearbeitung von Office-Dokumenten in der App (Unterstützung für: DOC, DOCX, XLS, XLSX, PPT, PPTX).
- Bearbeitung von Textdateien in der App.
- Unterstützung für SharePoint 365.
- Das Verschlüsselungsmodul von mobilEcho ist jetzt nach FIPS 140-2 zertifiziert.
- Alternative Rasteransicht beim Durchsuchen von Dateien, mit Thumbnail-Vorschau von Dateien auf dem Gerät.
- Es können jetzt mehrere Dateien gleichzeitig geöffnet werden.
- Falls beim Beenden der mobilEcho-App noch eine Dateisynchronisierung läuft, wird diese im Hintergrund fortgesetzt, bis der Prozess abgeschlossen ist oder von iOS beendet wird.
- Das Intervall zur Synchronisierung von Dateien bei geöffneter App kann jetzt eingestellt werden.
- Die Synchronisierung kann in der App so konfiguriert werden, dass sie nur bei bestehender WiFi-Verbindung erfolgt.
- Verbesserungen beim Synchronisierungsvorgang und bei der Fehleranzeige.
- mobilEcho-Verknüpfungen zu SharePoint-Speicherorten in Website-Sammlungen können nun geöffnet werden, solange der Benutzer Zugriff auf einen Speicherort höherer Ebene auf dem SharePoint-Server hat, auf dem die Website-Sammlung liegt.
- Bei der PDF-Dateianzeige ist jetzt, trotz deaktivierter PDF-Anmerkungsfunktion durch den IT-Administrator, die Textsuche und das Inhaltsverzeichnis verfügbar.
- Unterstützung für Benutzerzertifikatsauthentifizierung bei mobilEcho Servern.
- Verschiedene Fehlerbehebungen und Verbesserungen.