Acronis Access

Anleitung zu Installation und Upgrade

Urheberrechtserklärung

Von Acronis patentierte Technologien

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

Inhaltsverzeichnis

1 Installation 6

1.1 Voraussetzungen 6

1.1.1 Anforderungen an das Betriebssystem 6

1.1.2 Anforderungen für den mobilen Client 6

1.1.3 Minimale Hardware-Empfehlungen 7

1.1.4 Voraussetzungen für Desktop-Client 7

1.1.5 Netzwerkanforderungen 8

1.2 Acronis Access auf Ihrem Server installieren 9

1.3 Das Konfigurationswerkzeug verwenden 10

1.4 Den Installationsassistenten verwenden 11

2 Wartungsaufgaben 17

2.1 Richtlinien für Desaster-Recovery 17

2.2 Backup und Wiederherstellung von Acronis Access 19

2.3 Tomcat Log-Verwaltung unter Windows 22

2.4 Automatische Datenbanksicherung 27

2.5 Maximalen Speicherpool für Java in Tomcat für Acronis Access erhöhen 29

3 Mobiler Zugriff 31

3.1 Begrifflichkeiten 31

3.2 Richtlinien 33

3.2.1 Gruppenrichtlinie 33

3.2.2 Standardzugriffsbeschränkungen 42

3.3 Integration mobiler Geräte 42

3.3.1 Serverseitiger Verwaltungsregistrierungsvorgang 43

3.3.2 Benutzerseitiger Verwaltungsregistrierungsvorgang 44

3.4 Gateway Server verwalten 47

3.4.1 Server-Details 49

3.4.2 Gateway Server bearbeiten 51

3.5 Datenquellen verwalten 59

3.5.1 Ordner 60

4 Einstellungen 64

5 Schnellstart: Mobile Access 65

5.1 Erste Ausführung 65

6 Einstellen Ihrer Gruppenrichtlinie 70

6.1 Die Access Mobile Client-Applikation installieren 70

6.2 Für das Client Management registrieren 70

7 Schnellstart: Sync & Share 75

7.1 Erster Durchlauf 75

8 Web-Client 80

8.1 Den Desktop-Client verwenden 87

9 Server-Administration 92
9.1 Server verwalten 92
9.2 Administratoren und Berechtigungen 92
9.3 Überwachungsprotokoll 94
9.3.1 Protokoll 94
9.3.2 Einstellungen 96
9.4 Server 96
9.5 SMTP 98
9.6 LDAP 99
9.7 E-Mail-Vorlagen 101
9.8 Lizenzierung 103
9.9 Debug-Protokollierung 104
9.10 Überwachung 105
10 Ergänzendes Material 107
10.1 In Konflikt stehende Software 107
10.2 Vertrauenswürdige Server-Zertifikate mit Acronis Access verwenden 107
10.3 Acronis Access Tomcat SSL-Codierschlüssel ändern 110
10.4 So unterstützen Sie verschiedene Access Desktop Client-Versionen 110
10.5 Weboberfläche anpassen 111
10.6 Ablageordner erstellen 112
10.7 Acronis Access mit New Relic überwachen 113
10.8 Drittanbietersoftware für Acronis Access 114
10.8.1 PostgreSQL 114
10.8.2 Apache Tomcat 115
10.8.3 New Relic 115
11 Sync & Share 116
11.1 Freigabebeschränkungen 116
11.2 LDAP-Bereitstellung 116
11.3 Quotas 117
11.4 Dateibereinigungsrichtlinien 118
11.5 Benutzerablaufrichtlinien 119
11.6 Datei-Repository 120
11.7 Acronis Access-Client 121
12 Upgrades 123
12.1 Upgrade von Acronis Access auf eine neuere Version 123
13 Benutzer und Geräte 125
13.1 Mobile Geräte verwalten 125
13.1.1 Kennwort-Resets für die Remote-Applikation durchführen 126
13.1.2 Remote-Löschungen durchführen 127
13.2 Benutzer verwalten 128

14 Neuerungen 132
14.1 Neuerungen in Acronis Access Server 132
14.2 Neuerungen in der Acronis Access-App 149

1 Installation

Themen

Voraussetzungen 6
Acronis Access auf Ihrem Server installieren 9
Das Konfigurationswerkzeug verwenden 10
Den Installationsassistenten verwenden 11

1.1 Voraussetzungen

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

Themen

Anforderungen an das Betriebssystem 6
Anforderungen für den mobilen Client 6
Minimale Hardware-Empfehlungen 7
Voraussetzungen für Desktop-Client 7
Netzwerkanforderungen 8

1.1.1 Anforderungen an das Betriebssystem

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

Unterstützt:
Windows 2012 R2
Windows 2012, Standard- und Datacenter-Edition
Windows 2008, alle Varianten, 32/64 Bit

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

1.1.2 Anforderungen für den mobilen Client

Die mobile Client-Applikation ist kompatibel mit:

Unterstützte Geräte:

- Apple iPad 2., 3., 4. Generation, Air, Air 2
- Apple iPad Mini 1., 2., 3. Generation
- Apple iPhone 3GS, 4, 4S, 5, 5s, 5c, 6, 6 Plus
- Apple iPod Touch 4., 5. Generation
- Android-Smartphones und -Tablets (Geräte mit x86-Prozessorarchitektur werden nicht unterstützt)

Unterstützte Betriebssysteme:

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

Die Acronis Access App kann heruntergeladen werden von:

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

1.1.3 Minimale Hardware-Empfehlungen

Prozessor: Intel/AMD

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

Arbeitsspeicher:

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

Speicherplatz:

- Die Software-Installation erfordert 300 MB Speicherplatz.

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

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

1.1.4 Voraussetzungen für Desktop-Client

Unterstützte Betriebssysteme:

- Windows XP, Windows Vista, Windows 7, Windows 8 und 8.1

  Hinweis: *Zur Verwendung von Acronis Access Desktop Client unter Windows XP müssen Sie entspannte SSL-Verschlüsselungsregeln verwenden. Weitere Informationen finden Sie unter* *Acronis Access Tomcat SSL-Codierschlüssel ändern (S. 110).*

- Mac OS X 10.6.8 und höher, wenn Mac mit 64-Bit-Software kompatibel ist.

  Hinweis: *Stellen Sie bei der Installation des Acronis Access Desktop Clients sicher, dass der Sync-Ordner, den Sie erstellen, sich nicht in einem Ordner befindet, der von einer anderen Software synchronisiert wird. Eine Liste bekannter Konflikte finden Sie unter* *Konflikte verursachende Software (S. 107).*

Unterstützte Webbrowser:

- Mozilla Firefox 6 und höher
- Internet Explorer 9 und höher

Hinweis: *Bei Bedarf können Sie auch eine* ***unsichere*** *Version von Internet Explorer 8 unterstützen. Befolgen Sie hierfür die Anweisungen aus dem Artikel Acronis Access Tomcat SSL-Codierschlüssel ändern (S. 110). Internet Explorer 8 wird zur Server-Administration nicht unterstützt.*

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

- Google Chrome
- Safari 5.1.10 oder höher

1.1.5 Netzwerkanforderungen

- 1 Statische IP-Adresse.
- Optional, jedoch empfohlen: DNS-Name für die obigen IP-Adresse.
- Netzwerkzugriff auf einen Domain Controller, falls Active Directory verwendet wird.
- Netzwerkzugriff auf den SMTP-Server für E-Mail-Benachrichtigungen und Einladungen.
- Die Adresse **127.0.0.1** wird vom Access Mobile Client intern verwendet und darf nicht durch einen Tunnel (z.B. VPN) geleitet werden.
- Der Computer, auf dem Acronis Access ausgeführt wird, muss mit Windows Active Directory verbunden sein.

Hinweis: *Nach Möglichkeit sollten Sie den Server an die Domäne anbinden. Mobile Clients können nicht auf Datenquellen zugreifen, wenn der Server nicht an die Domäne angebunden ist.*

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

- **Zugriff über Port 443**: Da Acronis Access HTTPS für die verschlüsselte Übertragung verwendet, entspricht es von sich aus den üblichen Firewall-Regeln, die HTTPS-Verkehr über Port 443 zulassen. Wenn Sie den Zugriff über Port 443 auf den Acronis Access-Server zulassen, können autorisierte iPad-Clients innerhalb oder außerhalb der Firewall eine Verbindung aufbauen. Acronis Access kann jedoch auch für die Verwendung eines anderen Ports Ihrer Wahl konfiguriert werden.
- **VPN:** Der Access Mobile Client unterstützt den Zugriff über eine VPN-Verbindung. Sowohl der integrierte iOS VPN-Client als auch VPN-Clients von Drittanbietern werden unterstützt. iOS-Verwaltungsprofile können optional auf Geräte angewendet werden, die das Apple iPhone-Konfigurationswerkzeug verwenden, um die zertifikatsbasierte iOS-Funktion 'VPN auf Anforderung' zu konfigurieren, die nahtlosen Zugriff auf Acronis Access-Server und andere Unternehmensressourcen bietet.
- **Reverse Proxy-Server:** Falls ein Reverse Proxy-Server eingerichtet ist, können Clients für iPad eine Verbindung herstellen, ohne hierfür einen offenen Firewall-Port oder eine VPN-Verbindung zu benötigen. Die Access Mobile Client-App unterstützt die Reverse-Proxy-Pass-Through-Authentifizierung und die Authentifizierung mit Benutzername/Kennwort.

Hinweis: *Wenn Sie Mobilgerätverwaltungen wie GoodDynamics oder MobileIron verwenden möchten, müssen Sie ein Upgrade zu Acronis Access Advanced durchführen.*

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

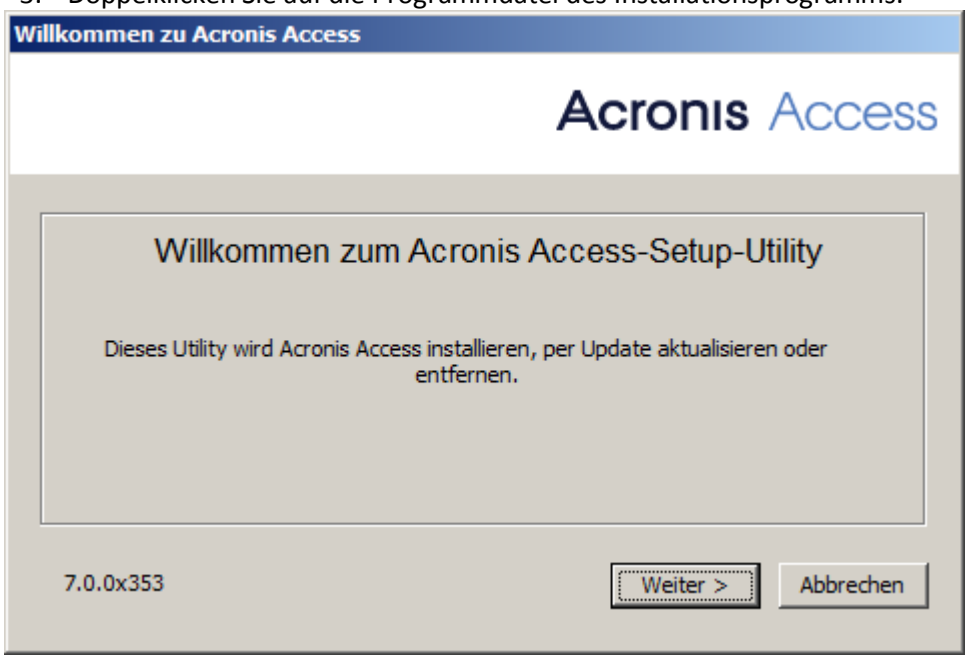
Hinweis: *Einige Webbrowser zeigen bei Verwendung von selbstsignierten Zertifikaten eine Warnmeldung an. Wenn Sie diese Warnmeldungen schließen, können Sie das System problemlos nutzen. Die Verwendung von selbstsignierten Zertifikaten unter Produktionsbedingungen wird nicht empfohlen.*

1.2 Acronis Access auf Ihrem Server installieren

Acronis Access installieren

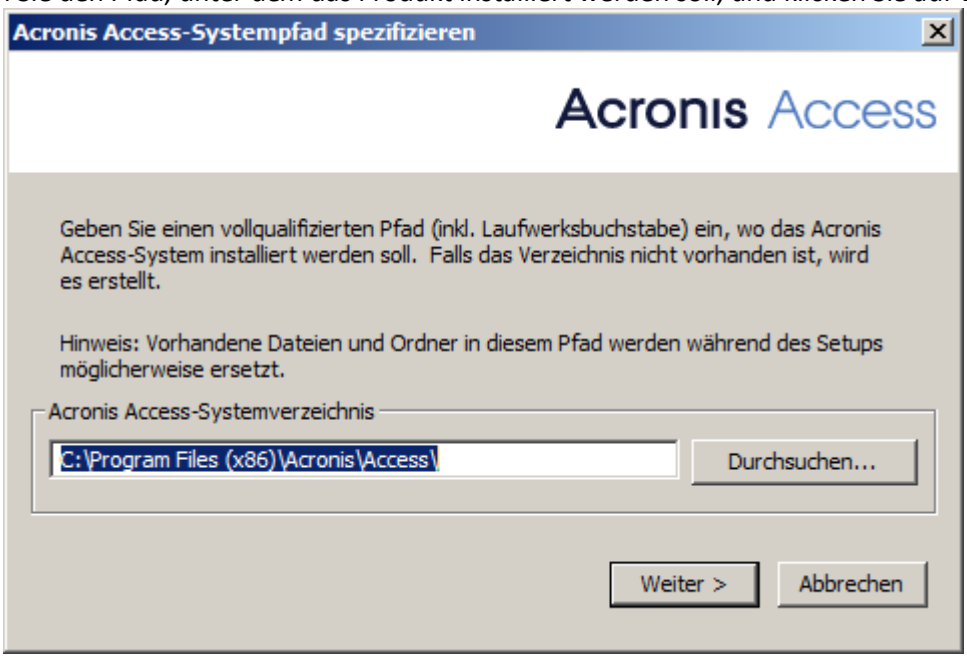
Sie müssen als Administrator angemeldet sein, um Acronis Access installieren zu können.

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.

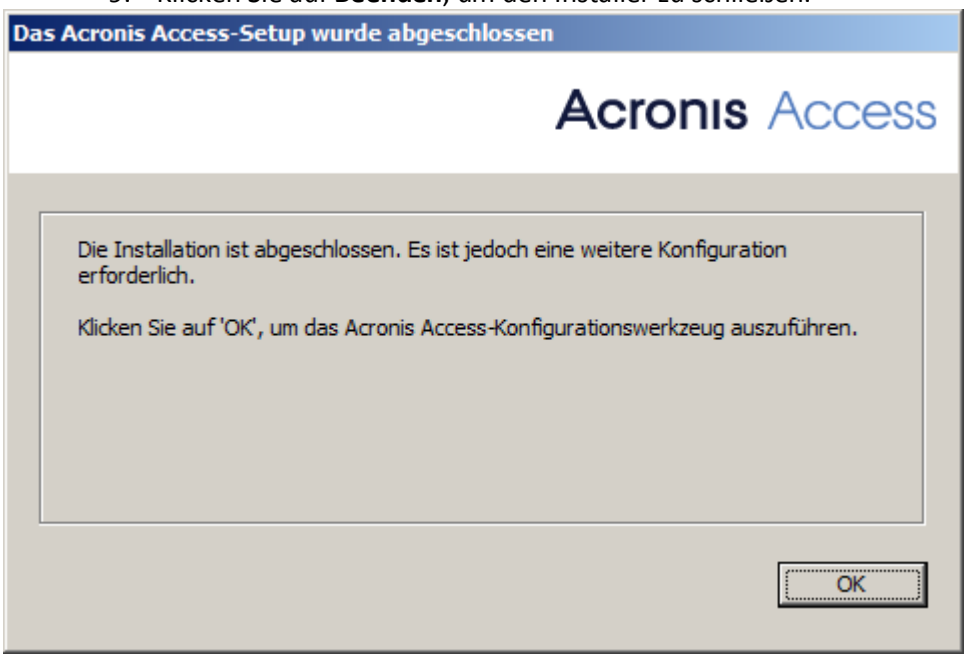


4. Klicken Sie auf **Weiter**, um zu beginnen.
5. Lesen und akzeptieren Sie die Lizenzvereinbarung.
6. Klicken Sie auf **Installieren**.

7. Wählen Sie den Pfad, unter dem das Produkt installiert werden soll, und klicken Sie auf **Weiter**.



8. Überprüfen Sie die zur Installation ausgewählten Komponenten und klicken Sie auf **Installieren**.
9. Klicken Sie auf **Beenden**, um den Installer zu schließen.



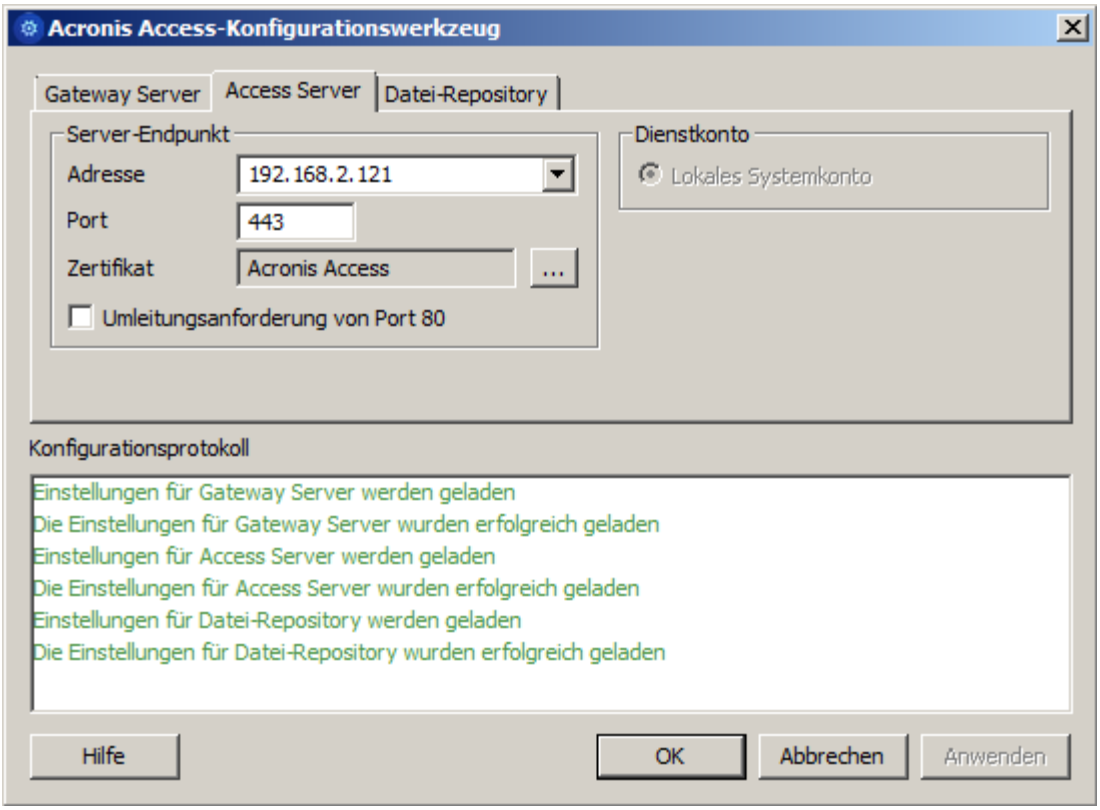
Das Konfigurationswerkzeug wird automatisch gestartet und schließt die Installation ab.

1.3 Das Konfigurationswerkzeug verwenden

Der Installer für Acronis Access beinhaltet ein Konfigurationswerkzeug, mit dem Sie den Zugriff auf den Acronis Access Gateway Server, das Datei-Repository und den Acronis Access Server schnell und einfach einrichten können.

Hinweis: *Im Abschnitt Netzwerkanforderungen (S. 8) finden Sie weitere Informationen zu optimalen Vorgehensweisen für die IP-Adressenkonfigurationen von Acronis Access.*

Hinweis: *Weitere Informationen zum Hinzufügen Ihres Zertifikats zum Microsoft Windows-Zertifikatspeicher finden Sie im Artikel Zertifikate verwenden (S. 107).*



- **Port** – der Port Ihrer Weboberfläche und Ihres Gateway Servers.
- **Zertifikat** – SSL-Zertifikat der Weboberfläche und des Gateway Servers. Sie können ein Zertifikat aus dem Microsoft Windows Zertifikatspeicher wählen.
- Wenn **Umleitungsanforderung von Port 80** ausgewählt ist, Tomcat den unsicheren Port 80 auf eingehenden Datenverkehr hin ab und leitet ihn zum HTTPS-Port um, den Sie zuvor festgelegt haben.
- **Dateispeicherpfad –** Lokaler Pfad des Dateispeichers. Wenn Sie den Dateispeicherpfad ändern, müssen Sie alle Dateien, die sich bereits am ursprünglichen Dateispeicherort befinden, manuell an den neuen Speicherort kopieren.

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

1.4 Den Installationsassistenten verwenden

Nach der Installation der Software und dem Ausführen des Konfigurationsdienstprogramms zum Einrichten des Netzwerk-Ports muss der Administrator als Nächstes den Acronis Access Server konfigurieren. Der Installationsassistent ermittelt automatisch die meisten notwendigen Einstellungen (LDAP, Server und SMTP), um Ihnen beim Einrichten der grundlegenden Funktionen des Servers zu helfen. Sie können alle diese Einstellungen manuell ändern, bevor Sie fortfahren.

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

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

Hinweis: *Administratoren können später konfiguriert werden. Weitere Informationen hierzu finden Sie im Abschnitt Server-Administration (S. 91).*

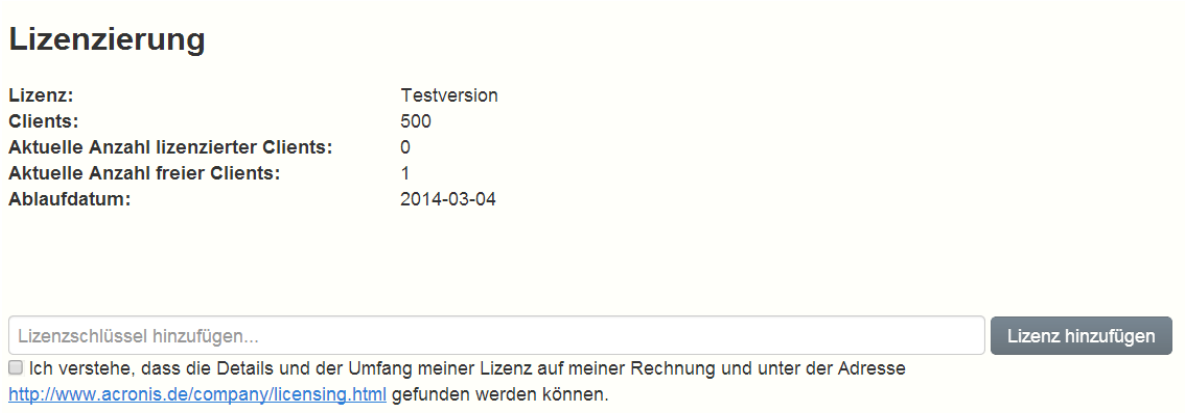
Der Assistent hilft Ihnen, die grundlegenden Einstellungen für die Funktionalität Ihres Produkts vorzunehmen.

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

Alle auf der Seite 'Erstkonfiguration' angezeigten Einstellungen sind auch nach Abschluss der Erstkonfiguration verfügbar. Weitere Informationen über diese Einstellungen finden Sie in den Artikeln zum Thema Server-Administration (S. 91).

Den Prozess der Erstkonfiguration durchlaufen

Lizenzierung



So starten Sie eine Testversion:

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

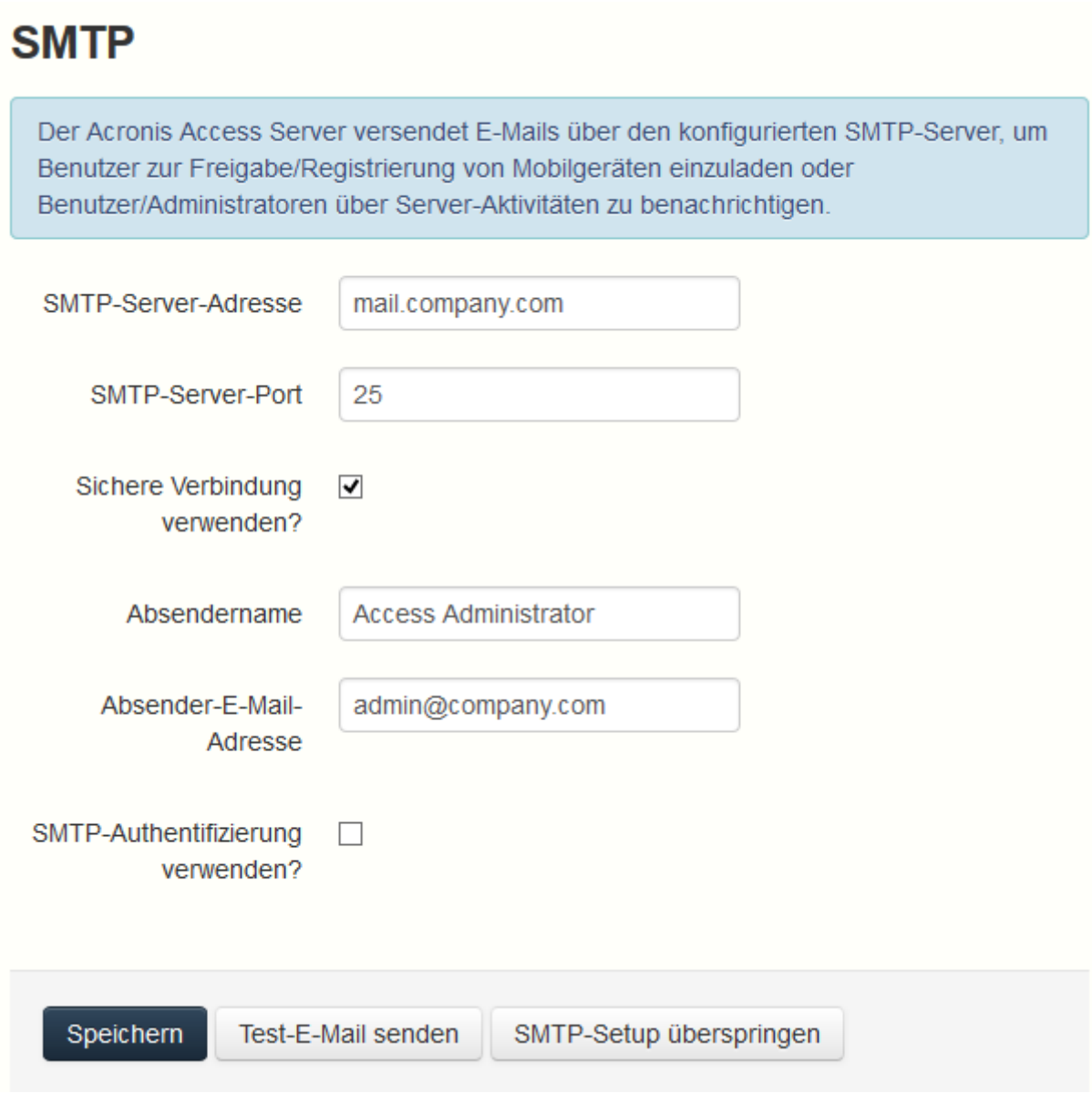
So lizenzieren Sie Ihren Access Server:

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

Allgemeine Einstellungen

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

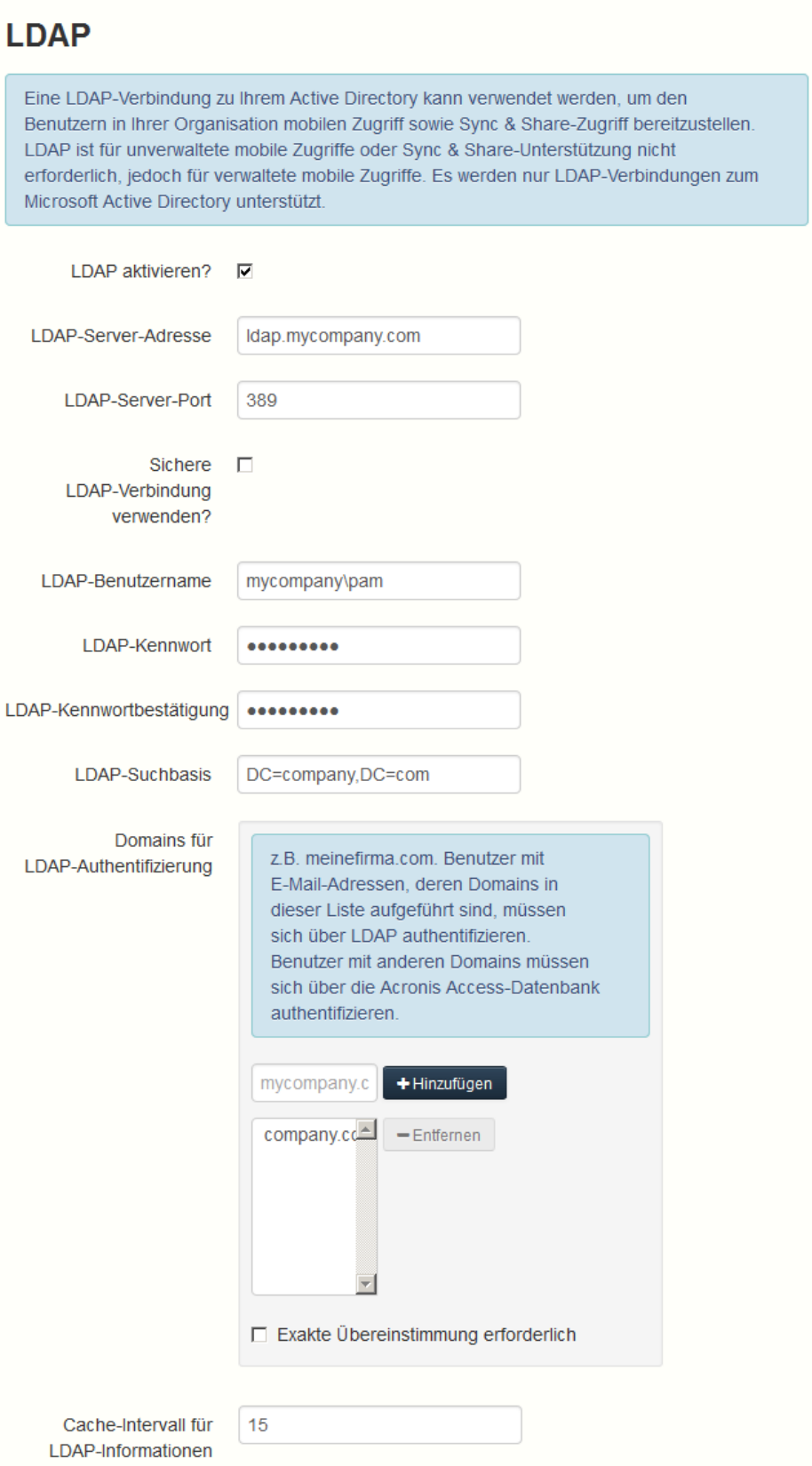
SMTP



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

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

LDAP



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

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

2 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. 17) lesen.

Themen

Richtlinien für Desaster-Recovery 17
Backup und Wiederherstellung von Acronis Access 19
Tomcat Log-Verwaltung unter Windows 22
Automatische Datenbanksicherung 27
Maximalen Speicherpool für Java in Tomcat für Acronis Access erhöhen 29

2.1 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.

2.2 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 **`PostgreSQL\bin`** im PostgreSQL-Installationsverzeichnis.
   z. B. **`cd "C:\Program Files (x86)\Acronis\Access\Common\PostgreSQL\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 Fester 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 Acronis Access 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 **`PostgreSQL\bin`** im PostgreSQL-Installationsverzeichnis.
   `cd "C:\Program Files (x86)\Acronis\Access\Common\PostgreSQL\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 Acronis Access 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.

Acronis Access auf einer neuen Instanz wiederherstellen

1. Führen Sie das oben beschriebene Backup-Verfahren aus und verschieben Sie die Dateien **alldbs.sql** und **mobilEcho.sqlite3** auf den neuen Server.

2. Führen Sie auf dem neuen Server das oben beschriebene Verfahren zum Wiederherstellen der Datenbank aus.
3. Starten Sie die Acronis Access-Dienste.
4. Führen Sie das folgende Verfahren aus:

Konfigurationen auf der neuen Instanz

Hinweis: *Es wird empfohlen, die von Acronis Access vewendeten DNS-Namen* ***nicht*** *zu ändern, sondern lediglich die IP-Adressen, auf die gezeigt wird. In den folgenden Anweisungen wird davon ausgegangen, dass Sie die DNS-Namen der früheren Instanz von Acronis Access wiederverwenden.*

1. Rufen Sie die Acronis Access Weboberfläche auf und melden Sie sich an.
2. Navigieren Sie zu **Mobile Access** -> **Gateway Server**.
3. Drücken Sie auf den Abwärts-Pfeil neben der Schaltfläche **Details** und wählen Sie **Bearbeiten** aus.
4. Klicken Sie auf die Registerkarte **SharePoint** und geben Sie die Administrator-Anmeldedaten für SharePoint ein.
5. Wenn für die **Adresse für Administration** eine IP-Adresse festgelegt ist, ändern Sie diese in die neue IP-Adresse, die Sie für den Acronis Access Server festgelegt haben.
6. Klicken Sie auf **Anwenden**.

Wenn Sie nicht dieselbe IP-Adresse wie die frühere Instanz verwenden möchten, ändern Sie die IP-Einträge für die von dem Acronis Access und Gateway Server verwendeten DNS-Namen.

2.3 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/de-de/library/cc753551(v=ws.10).aspx*
http://technet.microsoft.com/de-de/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: *Die Beispielskriptdatei (Batchdatei) ist für Windows 2008 konzipiert. Klicken Sie hier, um das 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.***

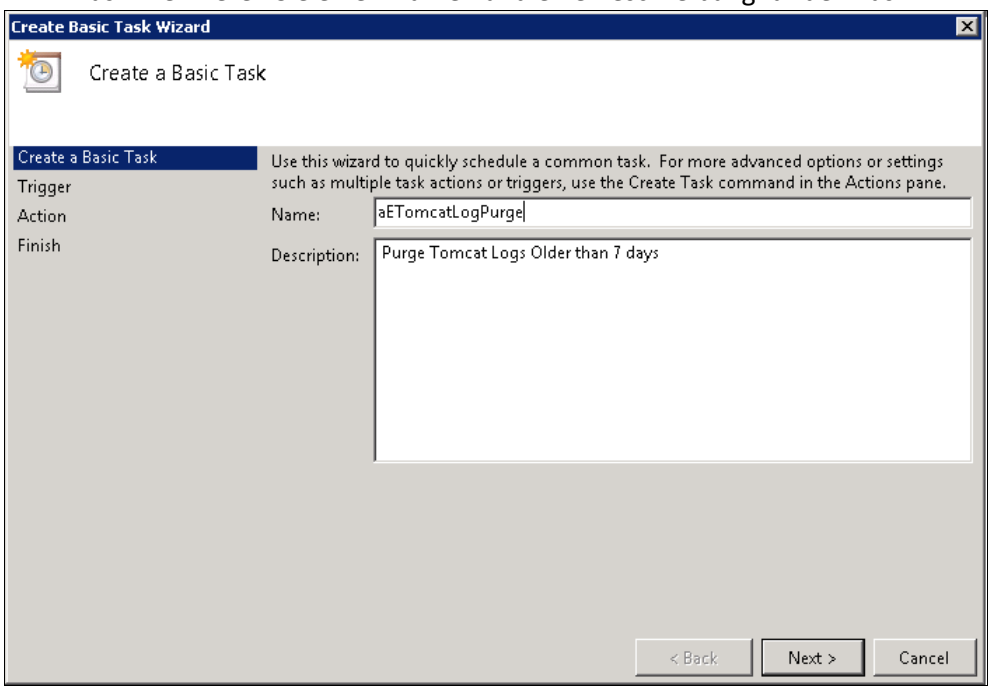
Schritte:

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:

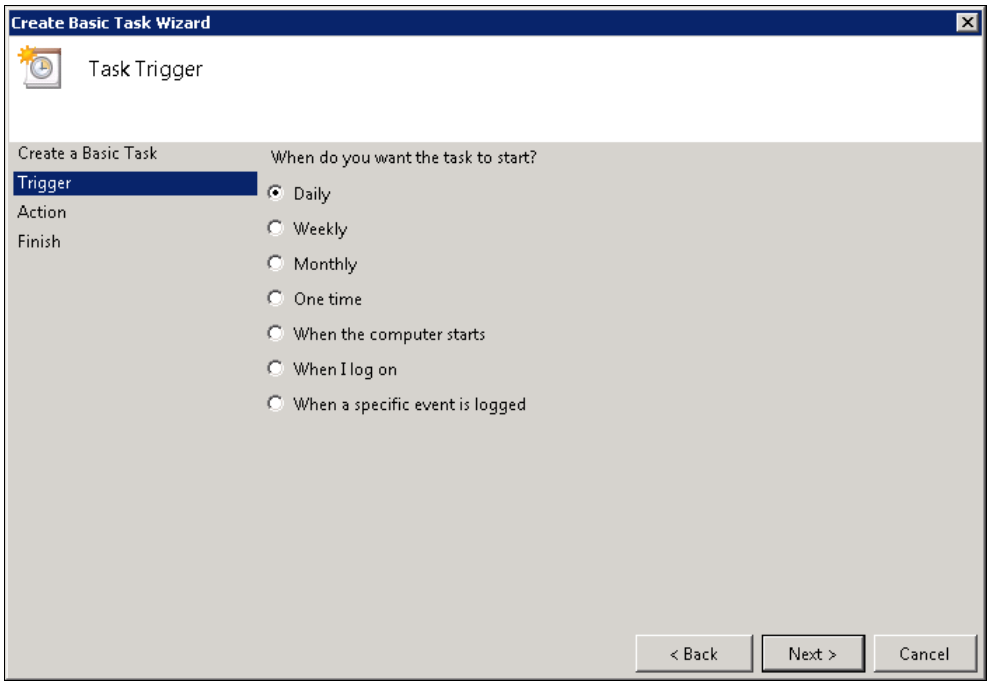
```
REM ===== CONFIGURATIONS ================================================
REM Note: all paths containing spaces must be enclosed in double quotes
 REM Edit this file and set LogPath and NumDays below
REM Path to the folder where all Tomcat logs are
 set LogPath="C:\Program Files (x86)\Group Logic\Common\apache-tomcat-7.0.34\logs"

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)***

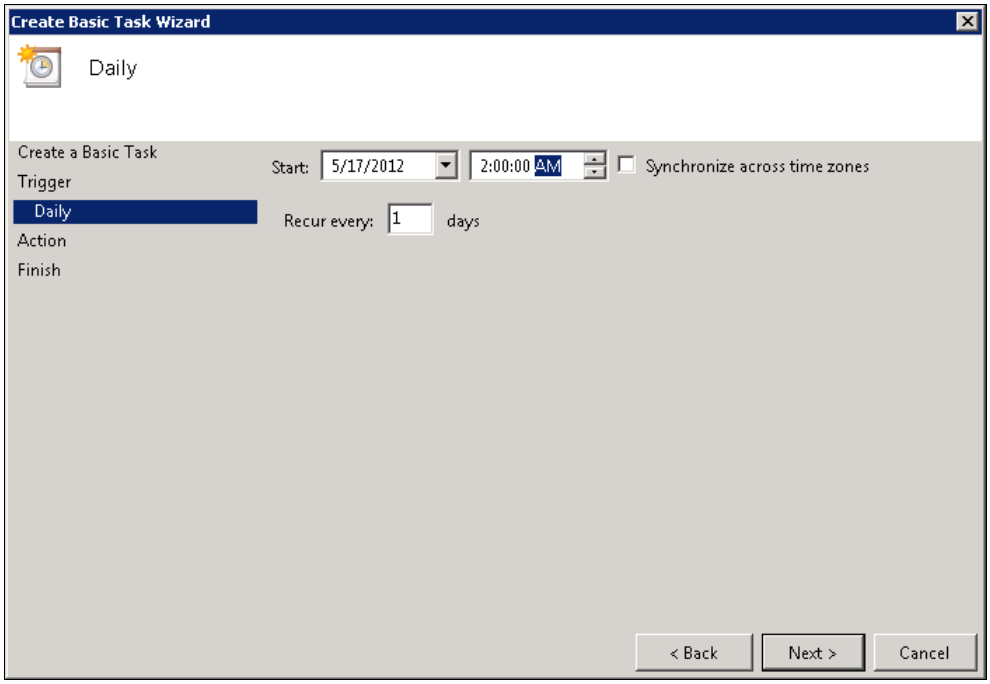
3. Speichern Sie die Datei.
4. Öffnen Sie zum Automatisieren des Prozesses den Task Scheduler, und erstellen Sie eine neue Task. Definieren Sie einen Namen und eine Beschreibung für den Task.



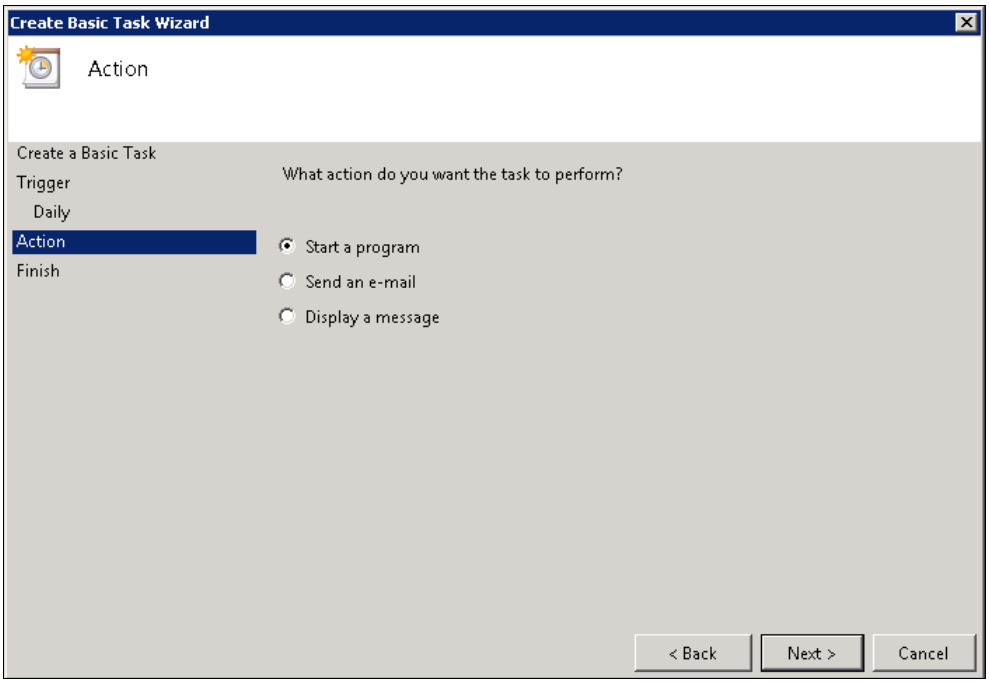
5. Legen Sie fest, dass der Task täglich ausgeführt wird.



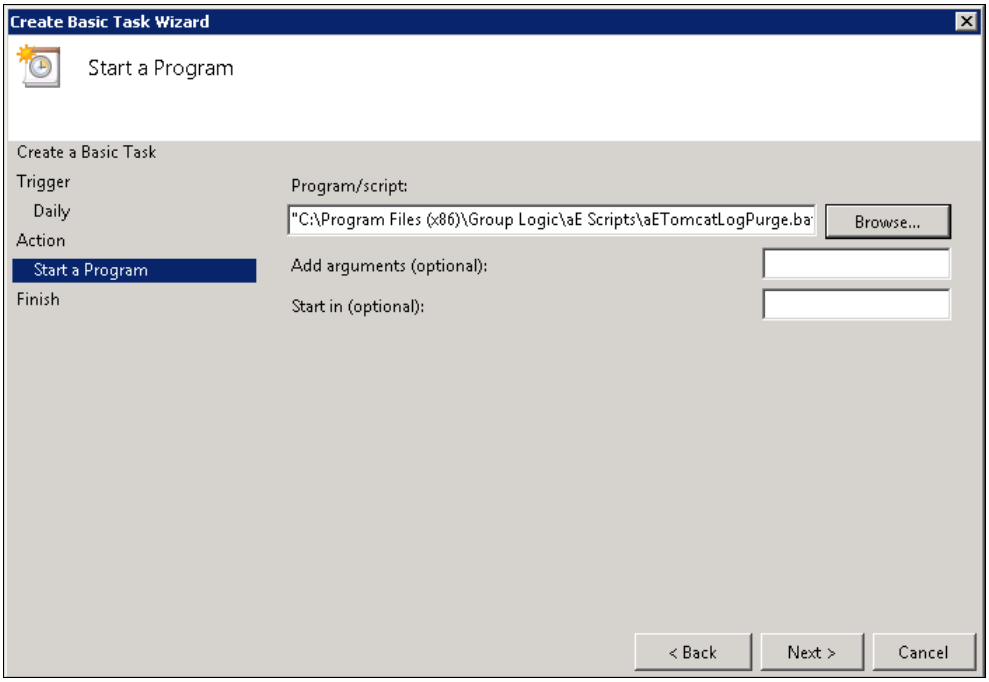
6. Geben Sie an, zu welcher Uhrzeit die Task starten soll. Es wird empfohlen, diesen Prozess nicht auszuführen, wenn das System extrem belastet ist oder andere Wartungsprozesse ausgeführt werden.



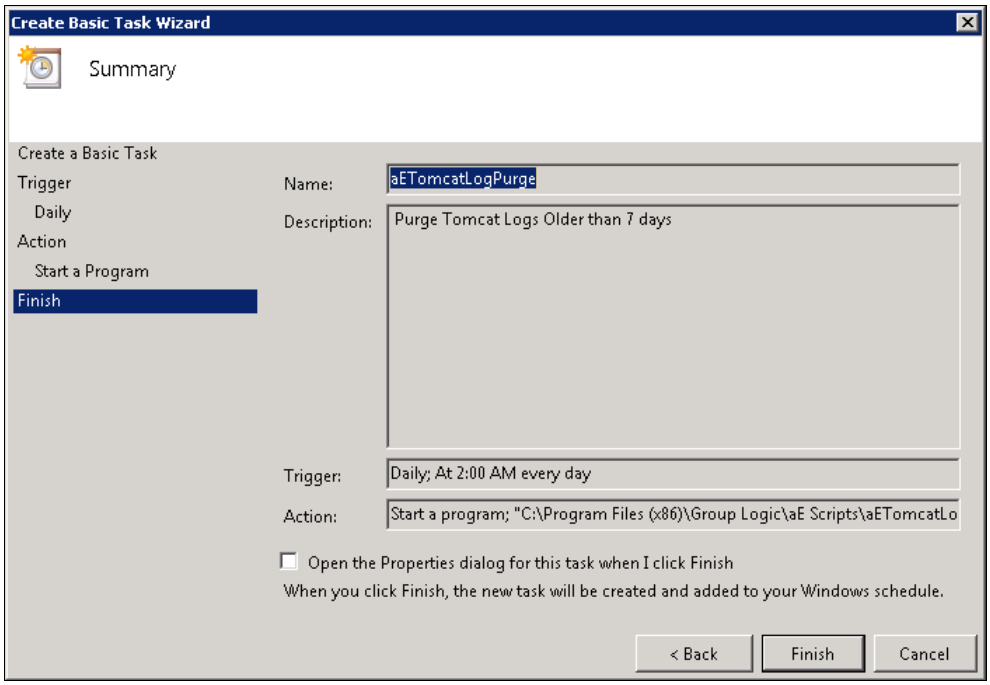
7. Stellen Sie den Aktionstyp auf 'Programm starten' ein.



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.

2.4 Automatische Datenbanksicherung

Mithilfe des Windows Task Scheduler können Sie auf einfache Weise einen automatischen Sicherungszeitplan für Ihre PRODUCT_NAME>-Datenbank einrichten.

Datenbanksicherungsskript erstellen

1. Öffnen Sie **Notepad** (oder einen anderen Texteditor) und geben Sie Folgendes ein:

```
@echo off

for /f "tokens=1-4 delims=/ " %%i in ("%date%") do (

set dow=%%i

set month=%%j

set day=%%k

set year=%%l

)

set datestr=%month%_%day%_%year%

echo datestr is %datestr%
```

```
set BACKUP_FILE=AAS_%datestr%_DB_Backup.sql

echo backup file name is %BACKUP_FILE%

SET PGPASSWORD=password

echo on

bin\pg_dumpall -U postgres -f %BACKUP_FILE%


move "%BACKUP_FILE%" "C:\destination folder"
```

2. Ersetzen Sie "**password**" durch das Kennwort für den Benutzer **postgres** , das Sie bei der Installation von Acronis Access eingegeben haben.
3. Ersetzen Sie **C:\destination folder** durch den Pfad zu dem Ordner, in dem Ihre Backups gespeichert werden sollen.
4. Speichern Sie die Datei unter dem Namen **DatabaseBackup.bat** (achten Sie auf die Dateierweiterung!) und wählen Sie als Dateityp **Alle Dateien**.
5. Verschieben Sie die Datei in den PostgreSQL-Installationsordner im Verzeichnis mit der entsprechenden Versionsnummer (z.B. \9.3\).

Geplante Task erstellen

1. Öffnen Sie die **Dienstesteuerung** und öffnen Sie anschließend **Verwaltung**.
2. Öffnen Sie den **Task Scheduler**.
3. Klicken Sie auf **Aktion** und wählen Sie **Task erstellen**.

Gehen Sie auf der Registerkarte Allgemein wie folgt vor:

1. Geben Sie einen Namen und eine Beschreibung für den Task ein (z.B. AAS-Datenbanksicherung).
2. Wählen Sie **Unabhängig von Anmeldung des Benutzers ausführen**.

Gehen Sie auf der Registerkarte Auslöser wie folgt vor:

1. Klicken Sie auf **Neu**.
2. Wählen Sie **Planmäßiger Start des Task**.
3. Wählen Sie eine tägliche Ausführung. Wählen Sie außerdem die Uhrzeit, zu der das Skript ausgeführt werden soll und wie oft die Ausführung des Skripts wiederholt werden soll (d.h. wie oft Sie Ihre Datenbank sichern möchten).
4. Wählen Sie in **Erweiterte Einstellungen** die Option **Aktiviert** und wählen Sie **OK**.

Gehen Sie auf der Registerkarte Aktionen wie folgt vor:

1. Klicken Sie auf **Neu**.
2. Wählen Sie für **Aktion Programm starten** aus.
3. Klicken Sie für **Programm/Skript** auf **Durchsuchen**, navigieren Sie zur Datei **DatabaseBackup.bat** und wählen Sie diese aus.

4. Geben Sie für **Starten in (optional)** den Pfad zu dem Ordner ein, in dem das Skript gespeichert ist. Lautet der Pfad zum Skript beispielsweise **C:\Programme (x86)\Acronis\Access\Common\PostgreSQL\9.3\PSQL.bat**, geben Sie **C:\Programme (x86)\Acronis\Access\Common\PostgreSQL\9.3\ ein**
5. Wählen Sie **OK**.

Konfigurieren Sie auf den übrigen Registerkarten beliebige zusätzliche Einstellungen und wählen Sie OK**.**

Sie werden aufgefordert, die Anmeldedaten für das aktuelle Konto einzugeben.

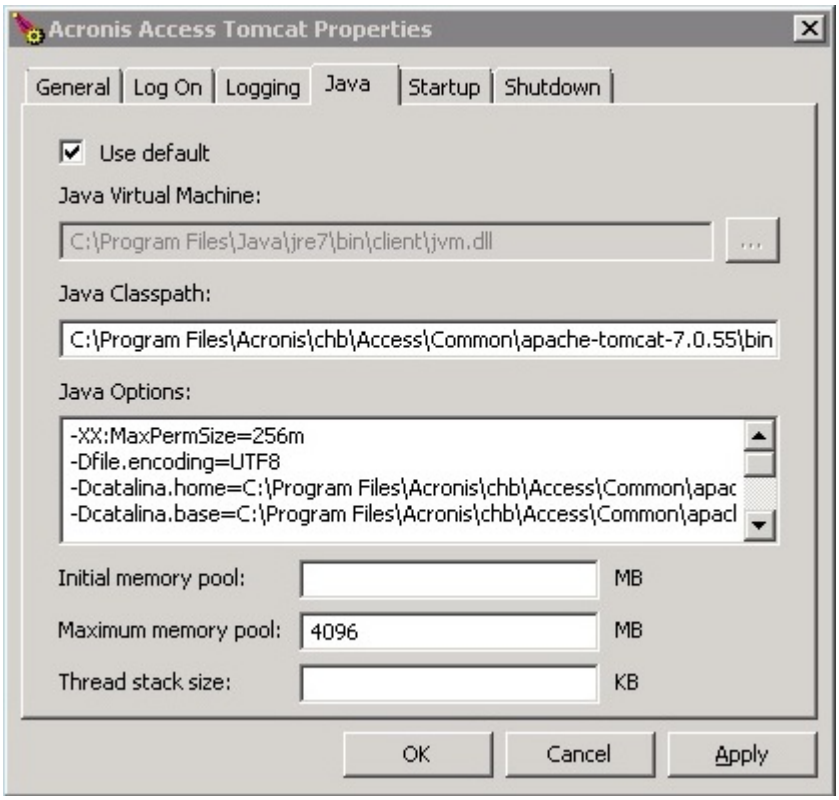
2.5 Maximalen Speicherpool für Java in Tomcat für Acronis Access erhöhen

Der Standardwert für den maximalen Speicherpool für Java in Acronis Access Tomcat beträgt bei einem 64-Bit-Betriebssystem 4 GB. Je nach Bereitstellung benötigen Sie einen größeren Pool.

***Hinweis**: Bei einem 32-Bit-Betriebssystem beträgt die maximale Größe des Speicherpools 1 GB.*

So vergrößern Sie den maximalen Speicherpool:

1. Klicken Sie auf "Start" -> **Alle Programme** -> Acronis Access.
2. Klicken Sie auf die Option **Acronis Access Tomcat Configuration**.



3. Öffnen Sie die Registerkarte **Java**.

4. Ändern Sie den Wert unter **Maximaler Speicherpool** in die gewünschte Größe. Klicken Sie anschließend auf **OK**.
5. Starten Sie den Acronis Access Tomcat-Dienst neu.

3 Mobiler Zugriff

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

Themen

Begrifflichkeiten 31
Richtlinien 33
Integration mobiler Geräte 42
Gateway Server verwalten 47
Datenquellen verwalten 59
Einstellungen 64

3.1 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.

Die Bereitstellung besteht aus einem einzigen Windows-Server, auf dem eine Installation von Acronis Access ausgeführt wird. Diese beinhaltet, dass die Acronis Access Server-Komponente und der Acronis Access Gateway Server installiert sind. 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 und die Access Mobile Clients können auf diese Datenquellen zugreifen. Jeder Benutzer wird die Kontrolle über seiner eigenen App-Einstellungen haben.

Abb 1. Einzelner Gateway Server, viele Access Mobile Clients

Hinweis: *Einzelheiten zur Installation von Acronis Access finden Sie im Bereich Installation (S. 1) dieser Anleitung. Die Konfiguration von Datenquellen wird im Bereich Mobiler Zugriff (S. 31) erläutert.*

Wenn Sie die Access Mobile Clients per Fernzugriff verwalten möchten, können Sie mit Acronis Access eine Gruppenrichtlinie verwenden. Über diese Richtlinie 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 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 erlaubt.

Eine typische netzwerkbasierte Client-Verwaltung besteht aus einem Server, auf dem die Komponenten Acronis Access Server und Acronis Access Gateway Server installiert sind. In diesem Szenario werden alle mobilen Clients vom Acronis Access Server verwaltet und kontaktieren diesen Server bei jedem Start der Acronis Access-Applikation, um gegebenenfalls nach Änderungen in den Einstellungen zu suchen, zurückgesetzte Kennwörter zum Sperren der Applikation zu akzeptieren und Befehle zum standortfernen Löschen auszuführen.

Acronis Access Clients können in ihrer Verwaltungsrichtlinie eine Liste von Servern, bestimmte Ordner in freigegebenen Volumes und Basisverzeichnisse zugewiesen werden. Diese Ressourcen erscheinen automatisch in der Acronis Access App, und die Client-App kontaktiert diese Server direkt, wenn dies zum Zugriff auf Dateien erforderlich ist.

Hinweis: *Einzelheiten zum Aktivieren und Konfigurieren der Client-Verwaltung finden Sie in dieser Anleitung in den Bereichen Richtlinien (S. 33) und Mobile Geräte verwalten (S. 125).*

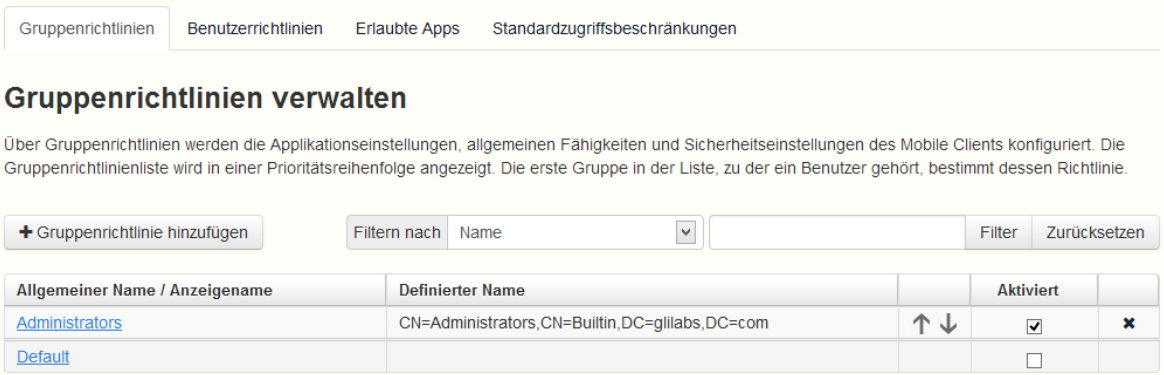
3.2 Richtlinien

Themen

Gruppenrichtlinie 33
Standardzugriffsbeschränkungen.....42

3.2.1 Gruppenrichtlinie

Das Acronis Access verwendet eine einzige Gruppenrichtlinie zur Verwaltung aller mobilen Benutzer.



3.2.1.1 Ausnahmen für Richtlinieneinstellungen

Die Apps **Acronis Access für Good Dynamics** und **Acronis Access mit Mobile Iron AppConnect** werden von Acronis Access nicht unterstützt.

3.2.1.2 Richtlinie ändern

Änderungen an der Richtlinie werden auf die entsprechenden Acronis Access Client-Benutzer angewendet, sobald sie die App wieder starten.

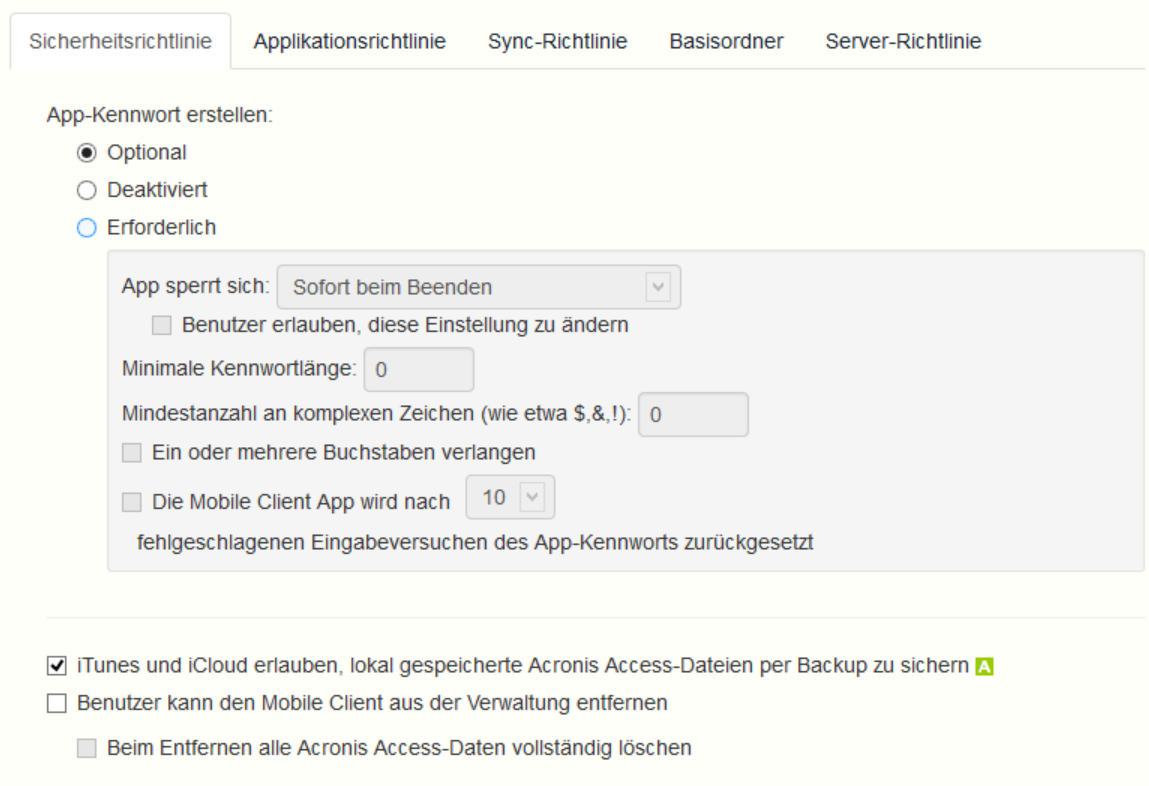
Anforderungen bezüglich der Verbindung

Acronis Access Clients benötigen Netzwerkzugriff auf den Acronis Access 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 erhält, so wird diese Verbindung zum VPN auch benötigt, bevor Verwaltungsbefehle akzeptiert werden.

So ändern Sie die Gruppenrichtlinie:

1. Klicken Sie auf die Standardgruppe.
2. Nehmen Sie die erforderlichen Änderungen auf der Seite **Gruppenrichtlinie bearbeiten** vor und drücken Sie **Speichern**.

3.2.1.3 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, ein Sperrkennwort für die Applikation zu konfigurieren. Sie können ein solches Kennwort jedoch 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 Mobilgeräten, 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 sperrt sich** – über diese Option kann die Übergangsfrist 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 Übergangsfrist 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 Kennworts zum Sperren der Applikation.
- **Mindestanzahl an komplexen Zeichen (wie etwa $,&,!)** – die erforderliche Mindestanzahl an Sonderzeichen, d. h. Zeichen, die keine Buchstaben oder Zahlen sind.
- **Ein oder mehrere Buchstaben verlangen** – 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 aufeinanderfolgender Fehlversuche zur Eingabe des App-Kennworts zurückgesetzt.

- **Benutzer kann den 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 werden 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 und iCloud erlauben, lokal gespeicherte Acronis Access-Dateien per Backup zu sichern** – wenn diese Einstellung deaktiviert ist, erlaubt der Access Mobile Client iTunes nicht, seine Dateien per Backup zu sichern. Damit wird sichergestellt, dass Dateien im geschützten Gerätespeicher von Acronis Access nicht in iTunes-Backups kopiert werden.

3.2.1.4 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**.
- **Miniaturbildervorschauen für serverseitige Dateien anzeigen** – Wenn aktiviert, werden beim Durchsuchen von Datenquellen und Gateway Servern Miniaturbildervorschauen anstelle von Dateitypsymbolen angezeigt.
  - **Cache-Größe von Miniaturbildern:** – Legt fest, wie viel Platz für Miniaturbilder reserviert wird.
  - **Miniaturbildvorschauen nur in WiFi-Netzwerken herunterladen** – Wenn aktiviert, sind Miniaturbilder nur dann verfügbar, wenn der Benutzer mit einem WiFi-Netzwerk verbunden ist.

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.

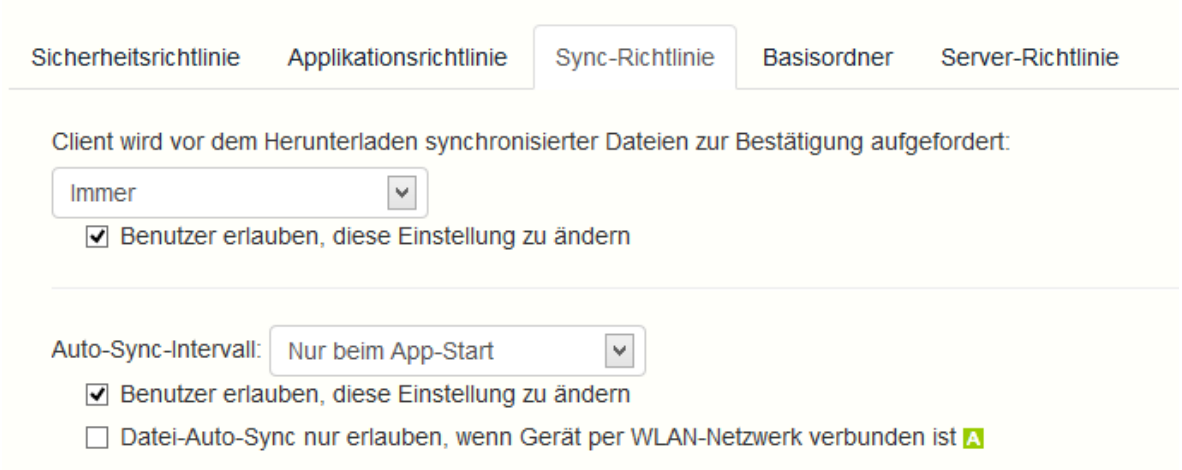
Ordnervorgänge

- **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.
- **Lesezeichen für Ordner erstellen** – Wenn diese Option deaktiviert ist, kann der Benutzer keine Lesezeichen für den Schnellzugriff auf Acronis Access-Geräte- oder -Server-Ordner setzen.

Schutz vor Datenverlust

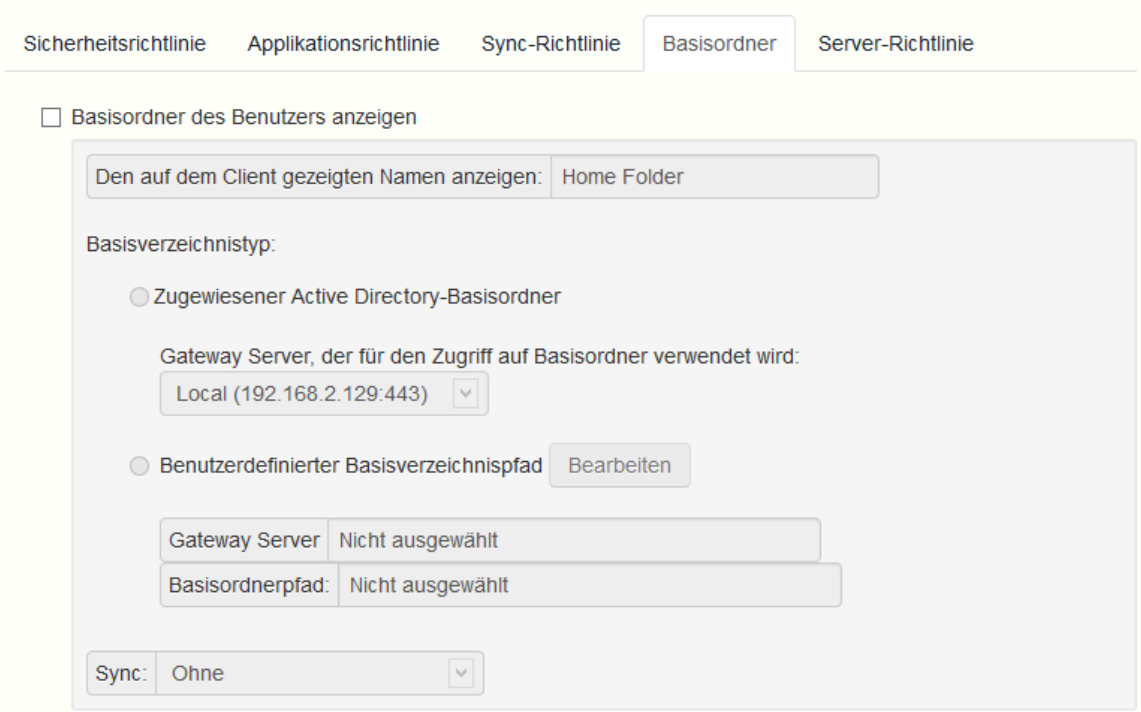
- **Acronis Access Dateien in anderen Applikationen öffnen** – Wenn diese Option deaktiviert ist, ignoriert die Access Mobile Client-Applikation die Schaltfläche **Öffnen in** und lässt nicht zu, dass Acronis Access Dateien in anderen Applikationen geöffnet werden. Wird eine Datei in einer anderen Applikation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

3.2.1.5 Synchronisierungsrichtlinie



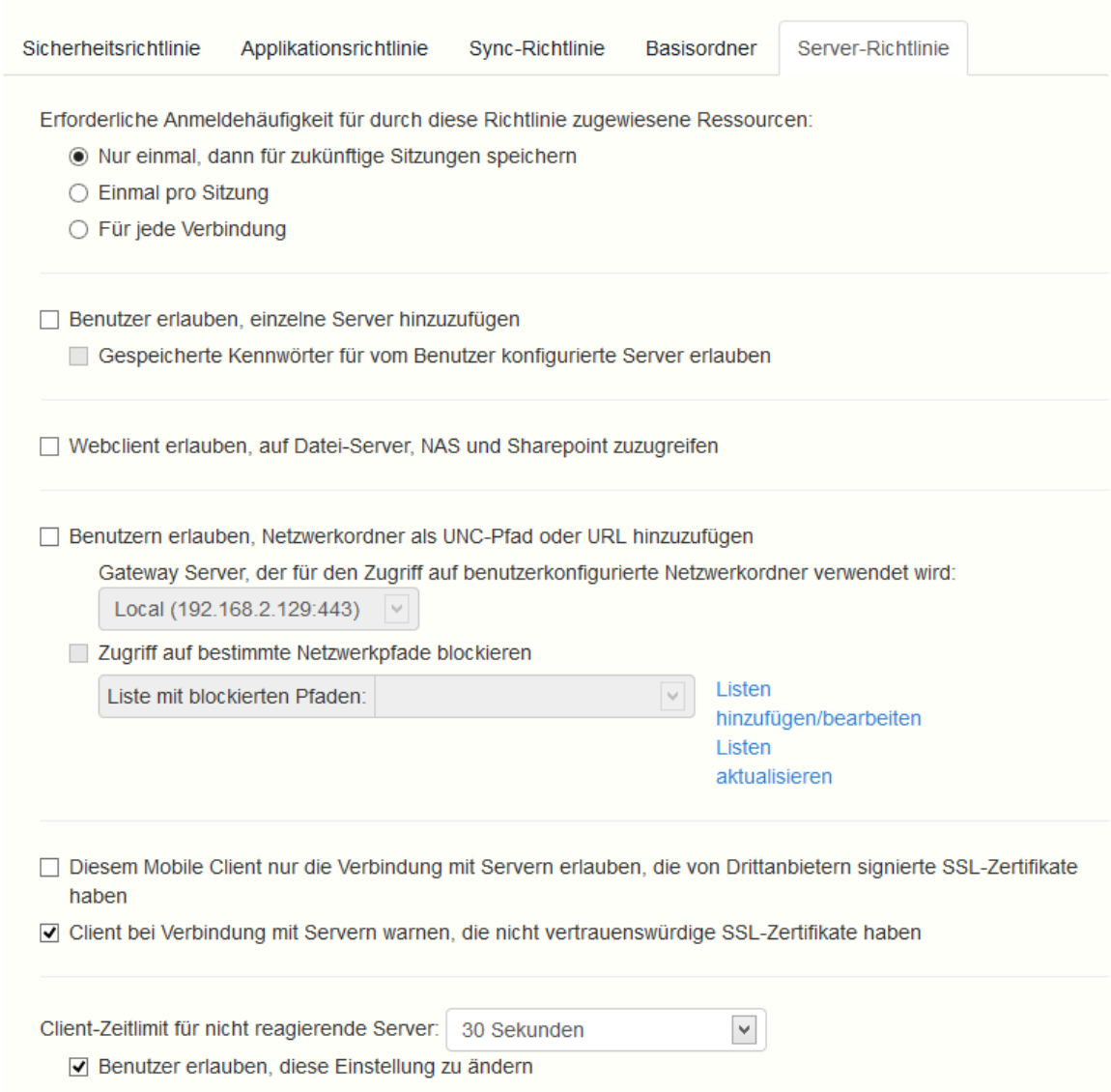
- **Client wird vor dem Herunterladen synchronisierter Dateien zur Bestätigung aufgefordert** – Wählen Sie die Bedingungen aus, unter denen der Benutzer das Herunterladen von Dateien in synchronisierten Ordnern bestätigen muss. Es gibt folgende Optionen: **Immer**, **Nur in Mobilfunknetzen** und **Nie**. Wenn **Benutzern erlauben, diese Einstellung zu ändern** aktiviert ist, sind Clients in der Lage, die Bestätigungsoptionen zu ändern.
- **Auto-Sync-Intervall** – Wenn diese Option aktiviert ist, führt Acronis Access eine automatische Synchronisierung **nie**, **nur beim App-Start** oder in verschiedenen **Zeitintervallen** 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 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 **Benutzer erlauben, diese Einstellung zu ändern** aktiviert ist, sind Clients in der Lage, die automatische Dateisynchronisierung in WiFi-Netzwerken zu aktivieren bzw. zu deaktivieren.

3.2.1.6 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.

3.2.1.7 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-Applikation 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.

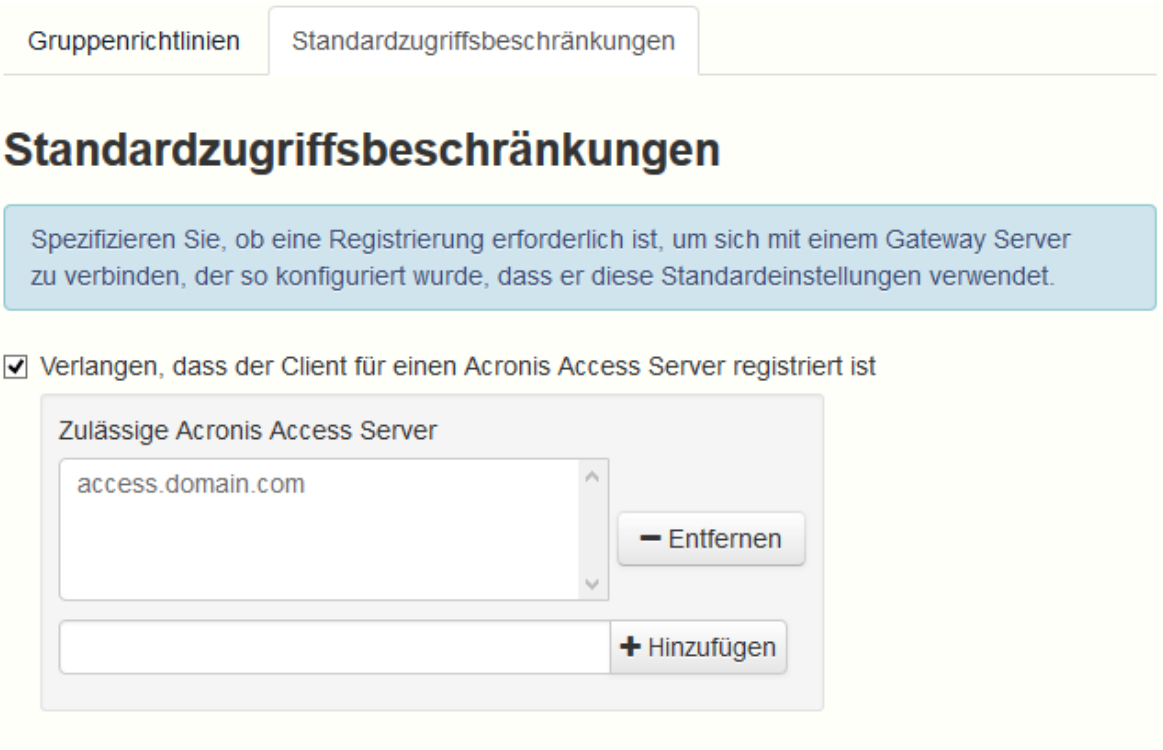
- **Benutzer erlauben, einzelne Server hinzuzufügen** – Wenn diese Option aktiviert ist, können Benutzer in der Access Mobile Client-Applikation Server manuell hinzufügen, sofern sie den DNS-Namen des Servers oder dessen IP-Adresse kennen. Wenn dem Benutzer nur die **Server zur Verfügung stehen sollen, 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.
- **Zugriff auf File Server, NAS und Sharepoint über Web Client zulassen** – Wenn aktiviert, können Web Client-Benutzer auch mobile Datenquellen sehen und darauf zugreifen.
- **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**.

3.2.2 Standardzugriffsbeschränkungen

In diesem Bereich können Sie festlegen, ob Mobile Clients für den Management Server registriert sein müssen.



3.3 Integration mobiler Geräte

Um die Acronis Access-App verwenden zu können, müssen die Benutzer sie über den Apple App Store (iOS) oder den Google Play Store (Android) installieren. Je nach der Bereitstellung von Acronis Access durch Ihr Unternehmen, müssen die Benutzer außerdem die Access Mobile-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 Verwaltungsrichtlinie gesteuert.

Zu den Einstellungen und Funktionen in der Acronis Access App, die durch die Verwaltungsrichtlinie vorgegeben werden, gehören:

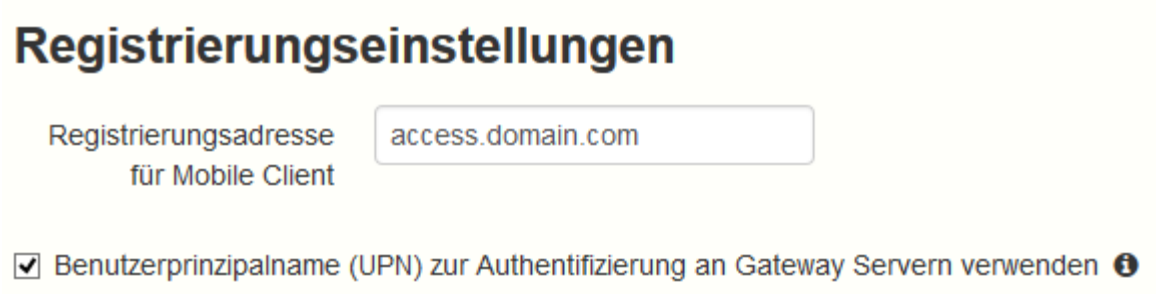
- Kennwort zum Sperren der Applikation verlangen
- Komplexitätsanforderungen für das Kennwort
- Möglichkeit, die Acronis Access App aus der Verwaltung zu entfernen
- iTunes erlauben, lokale Acronis Access Dateien zu sichern
- Das Öffnen von Acronis Access App-Dateien in anderen Applikationen erlauben
- 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

Serverseitiger Verwaltungsregistrierungsvorgang 43
Benutzerseitiger Verwaltungsregistrierungsvorgang 44

3.3.1 Serverseitiger Verwaltungsregistrierungsvorgang



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 ein Benutzer mehrere Geräte verwendet, muss er eine Einladungs-E-Mail für jedes Gerät erhalten, das Zugriff erfordert.

Diese E-Mail schließt einen Link zur Acronis Access App im Apple App Store oder Google Play Store ein, falls die App zunächst installiert werden muss. Sie schließt auch einen zweiten Link ein. Wenn Sie auf dem Gerät darauf tippen, wird Acronis Access geöffnet und das Client-Registrierungsformular automatisch mit dem Namen des Acronis Access Servers und dem Benutzernamen des Benutzers ausgefüllt. Bei Verwendung dieses Links muss der Benutzer lediglich sein Kontokennwort eingeben, um die Client-Registrierung abzuschließen.

Einfache URL-Registrierungs-Links verwenden:

Sie können Ihren 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.

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.
7. Wählen Sie im Feld 'Einladung verfällt in' die Anzahl von Tagen, die die Einladung gültig sein soll.

   ***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.*

8. 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.
9. Drücken Sie 'Senden'.

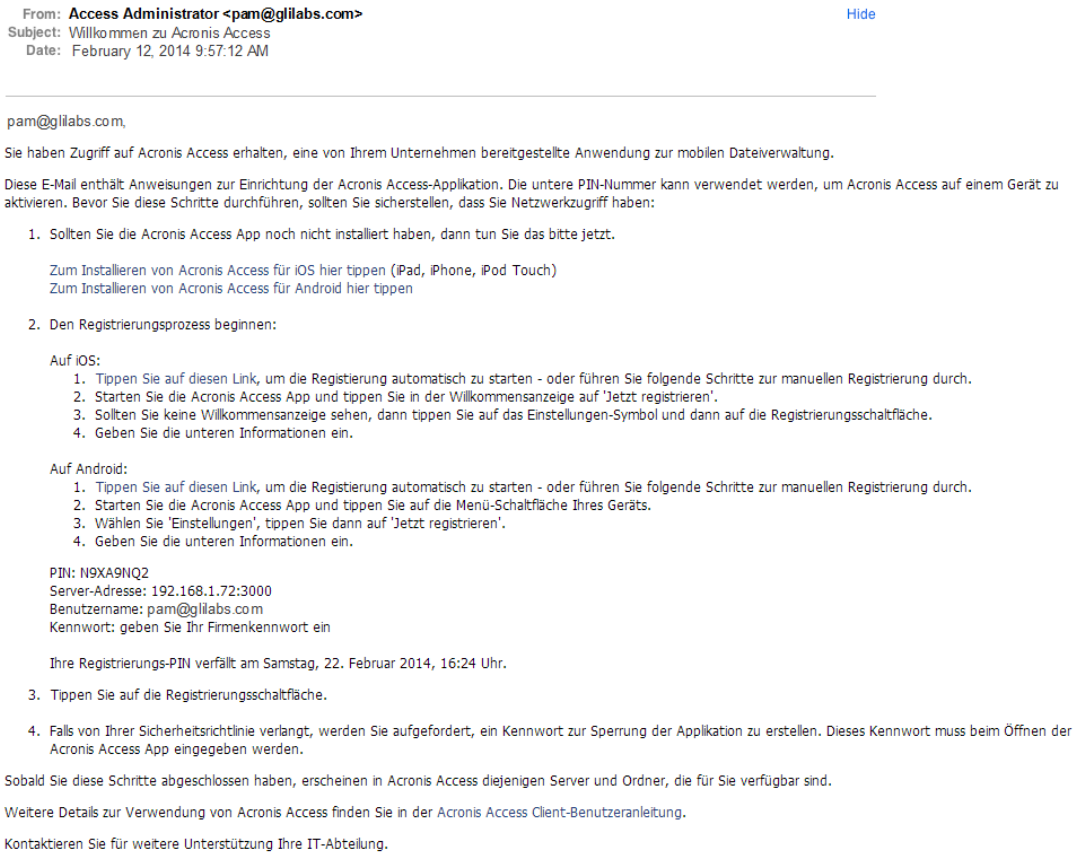
   ***Hinweis:** Falls Sie beim Senden eine Fehlermeldung erhalten, überprüfen Sie, ob die SMTP-Einstellungen auf der Registerkarte 'SMTP' unter 'Allgemeine Einstellungen' korrekt sind. Wenn Sie **Sichere Verbindung** verwenden, überprüfen Sie außerdem, ob das von Ihnen verwendete Zertifikat mit dem Hostnamen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

3.3.2 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
- 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 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 eingeben, 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 Gruppenrichtlinie zuzuordnen, auf den Gateway-Server zuzugreifen und die Anmeldedaten für Acronis Access Server-Anmeldungen zu speichern, falls die Richtlinie 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.

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 und Benutzername automatisch ausgefüllt.
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.

Manuelle Registrierung

1. Öffnen Sie die Acronis Access-App.
2. Öffnen Sie **Einstellungen**.
3. Tippen Sie auf **Registrieren**.
4. Geben Sie Ihre Serveradresse, Ihren Benutzernamen und Ihr 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.

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.

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

Acronis Access Clients benötigen Netzwerkzugriff auf den Acronis Access 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 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

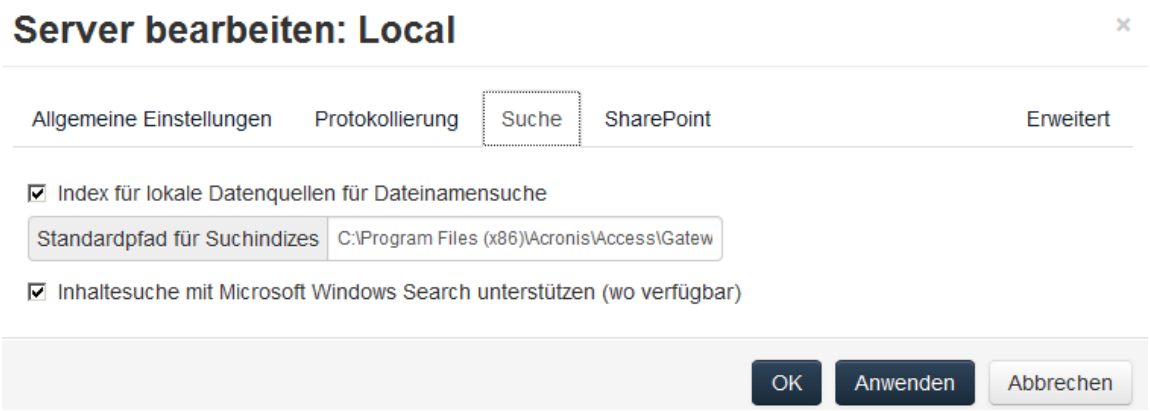
3.4 Gateway Server verwalten

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 verwaltet den Gateway Server über dieselbe Managementkonsole. 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.

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 sollen, geben Sie den gewünschten Ordnerpfad ein.

Inhaltssuche mit Microsoft Windows Search unterstützen (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-Suche 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 die Windows-Suche zu aktivieren, fügen Sie die Rolle namens **Dateidienste** im Server-Manager hinzu und lassen Sie den Windows-Suchdienst aktivieren. Die Windows-Suche kann

konfiguriert werden, um die 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 (Reshares) 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.

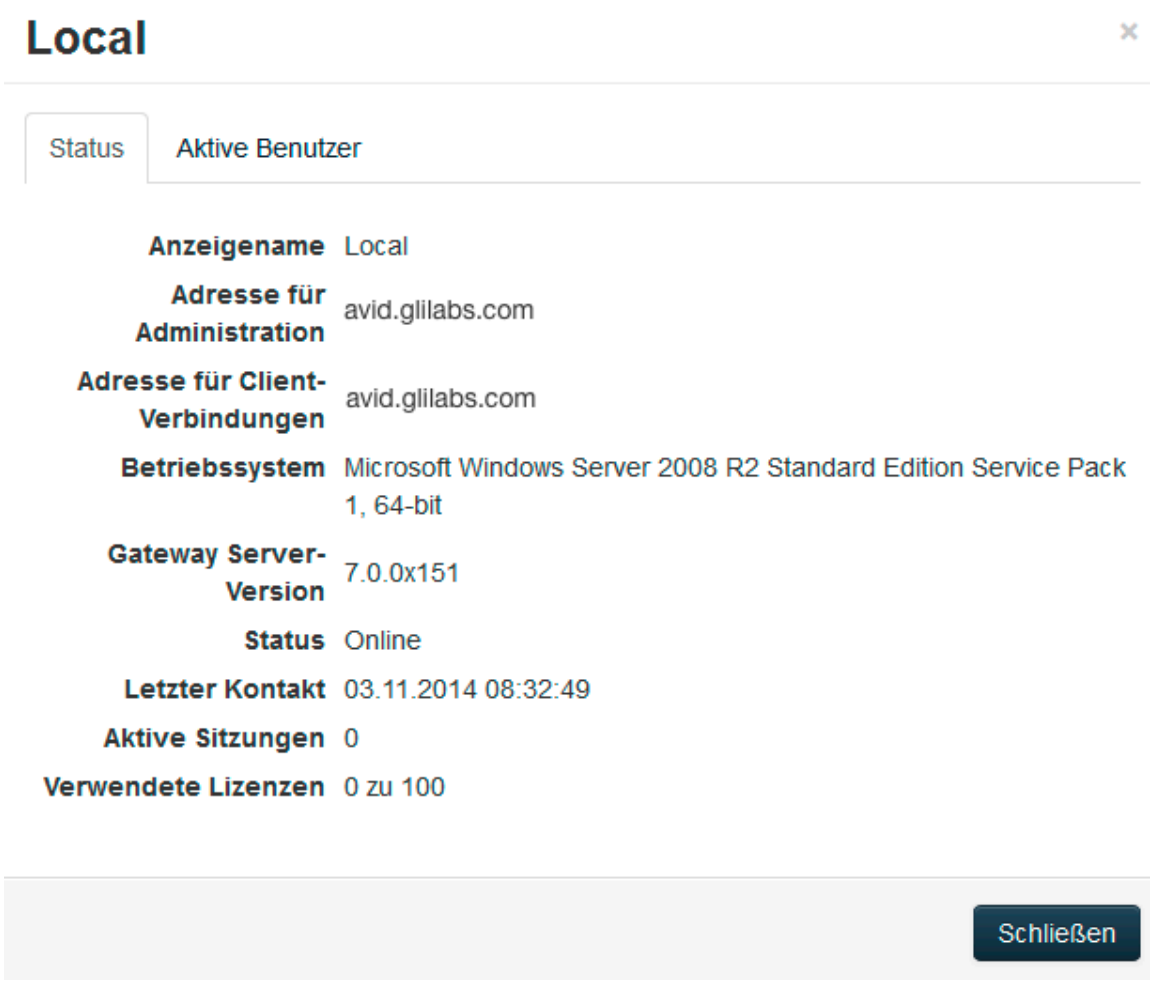
Themen

Server-Details 49
Gateway Server bearbeiten 51

3.4.1 Server-Details

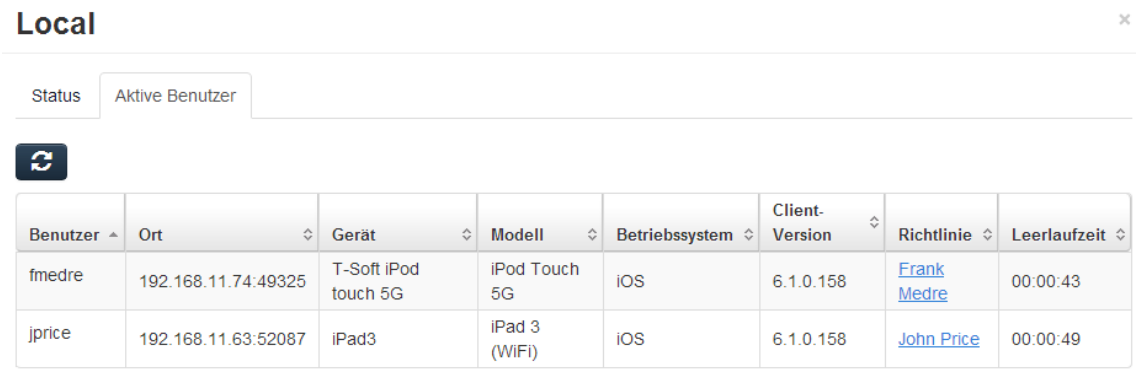
Auf der Seite **Details** eines Gateway Servers erhalten Sie zahlreiche nützliche Informationen zu dem spezifischen Server und seinen Benutzern.

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



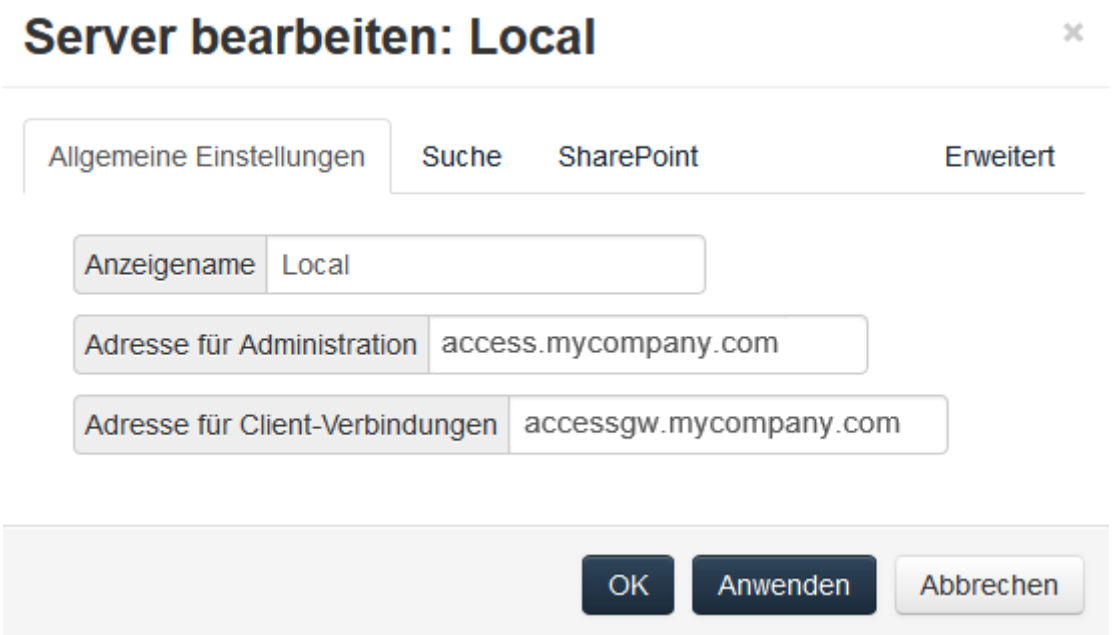
Zeigt eine Tabelle aller Benutzer an, die gegenwärtig auf diesem Gateway Server aktiv sind.

- **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.

3.4.2 Gateway Server bearbeiten

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:

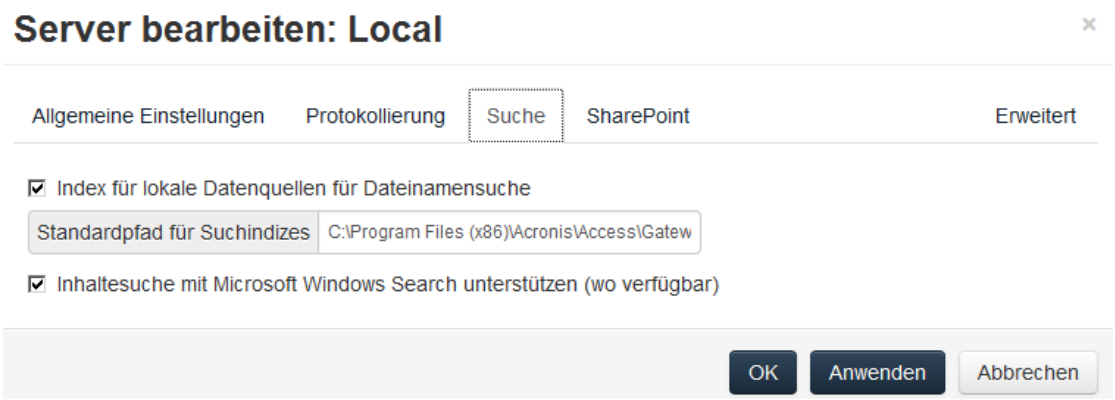
1. Rufen Sie die Weboberfläche auf.
2. Melden Sie sich als Administrator an.
3. Öffnen Sie die Registerkarte **Mobiler Zugriff**.
4. Öffnen Sie die Registerkarte **Gateway Server**.
5. Suchen Sie den Server, für den Sie **Audit Logs aktivieren möchten.**
6. Drücken Sie die Schaltfläche **Details**.
7. 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 sollen, geben Sie den gewünschten Ordnerpfad ein.

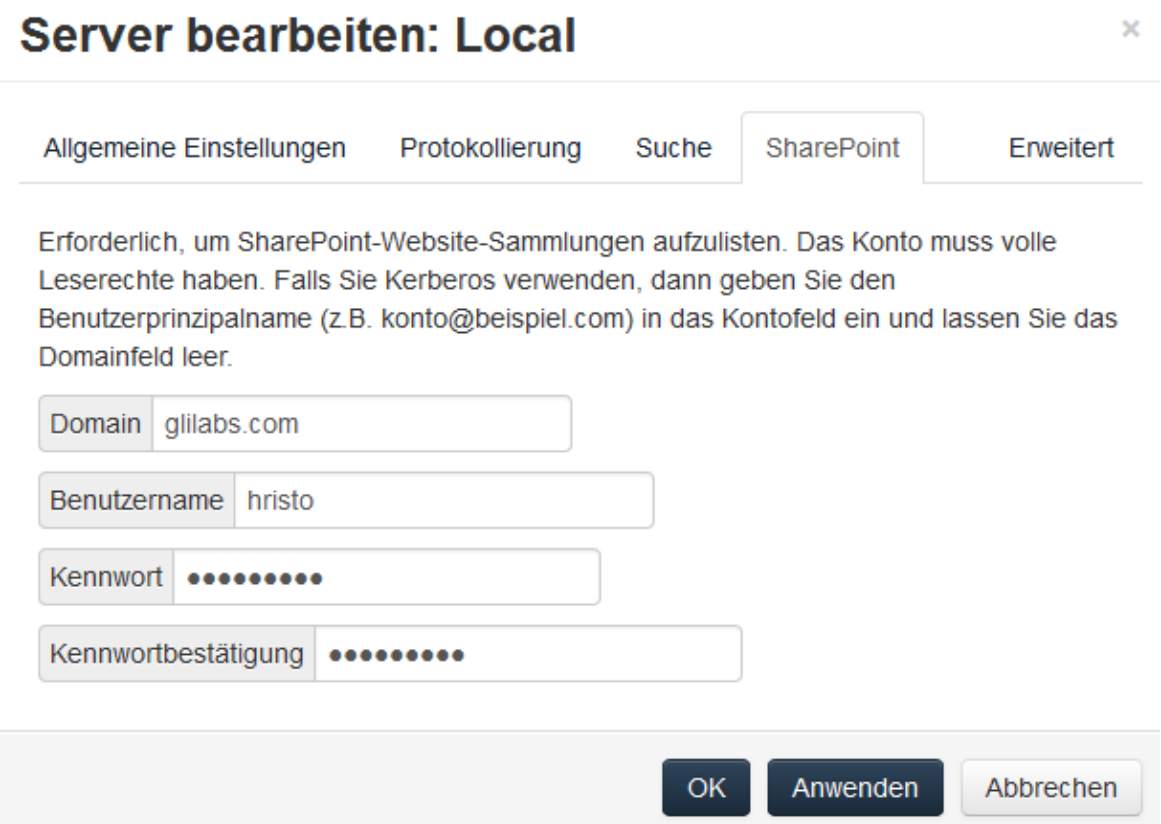
Inhaltssuche mit Microsoft Windows Search unterstützen (wo verfügbar)

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-Suche 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 die Windows-Suche zu aktivieren, fügen Sie die Rolle namens **Dateidienste** im Server-Manager hinzu und lassen Sie den Windows-Suchdienst aktivieren. Die Windows-Suche kann konfiguriert werden, um die 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 (Reshares) 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.*

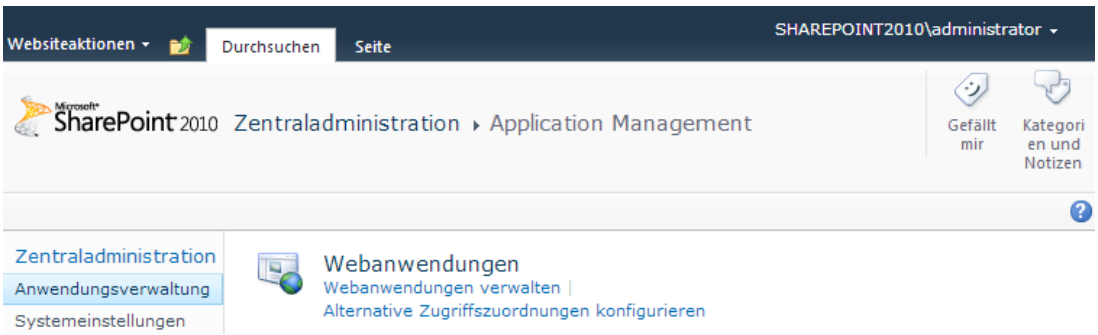
SharePoint



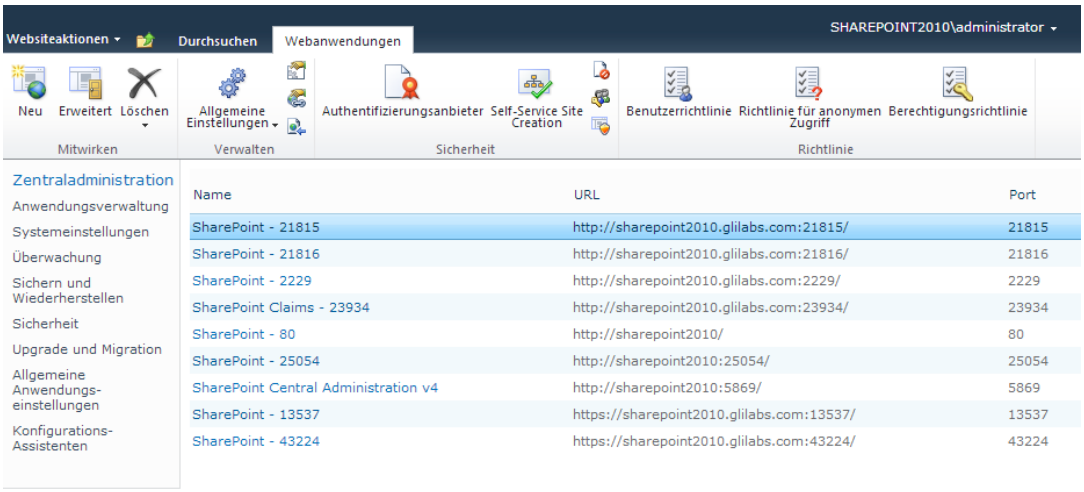
Für die allgemeine Unterstützung von SharePoint ist die Eingabe dieser Zugangsdaten optional. Sie ist aber erforderlich, um Websitesammlungen aufzulisten. Beispiel: Sie verfügen über zwei Websitesammlungen: http://sharepoint.beispiel.com und http://sharepoint.beispiel.com/SeparateSammlung. Ohne die Eingabe 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:

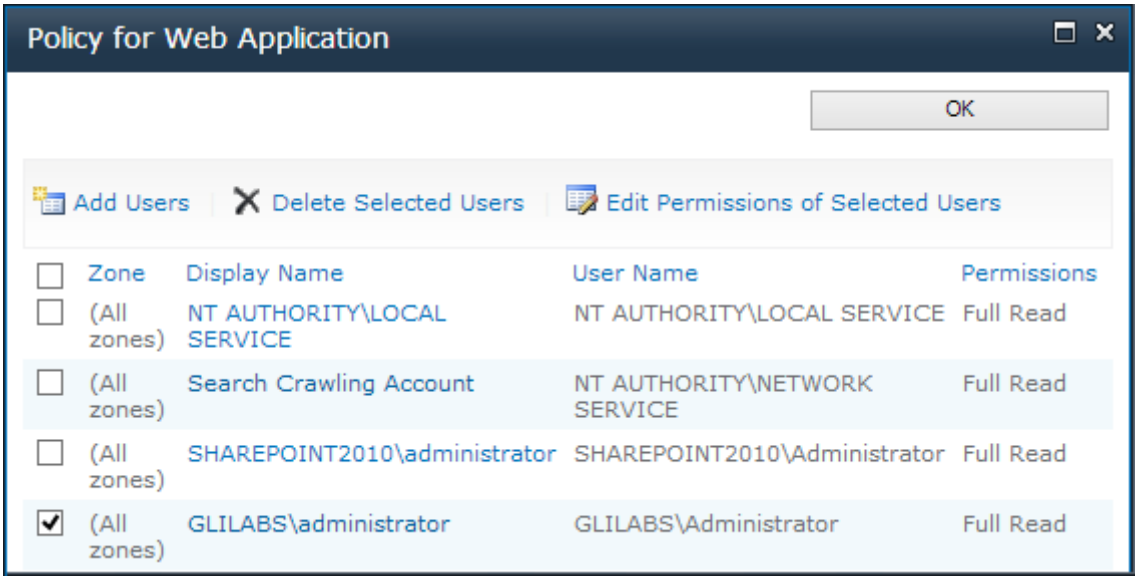
1. Öffnen Sie die **SharePoint-Zentraladministration**.
2. Klicken Sie auf **Anwendungsverwaltung**.



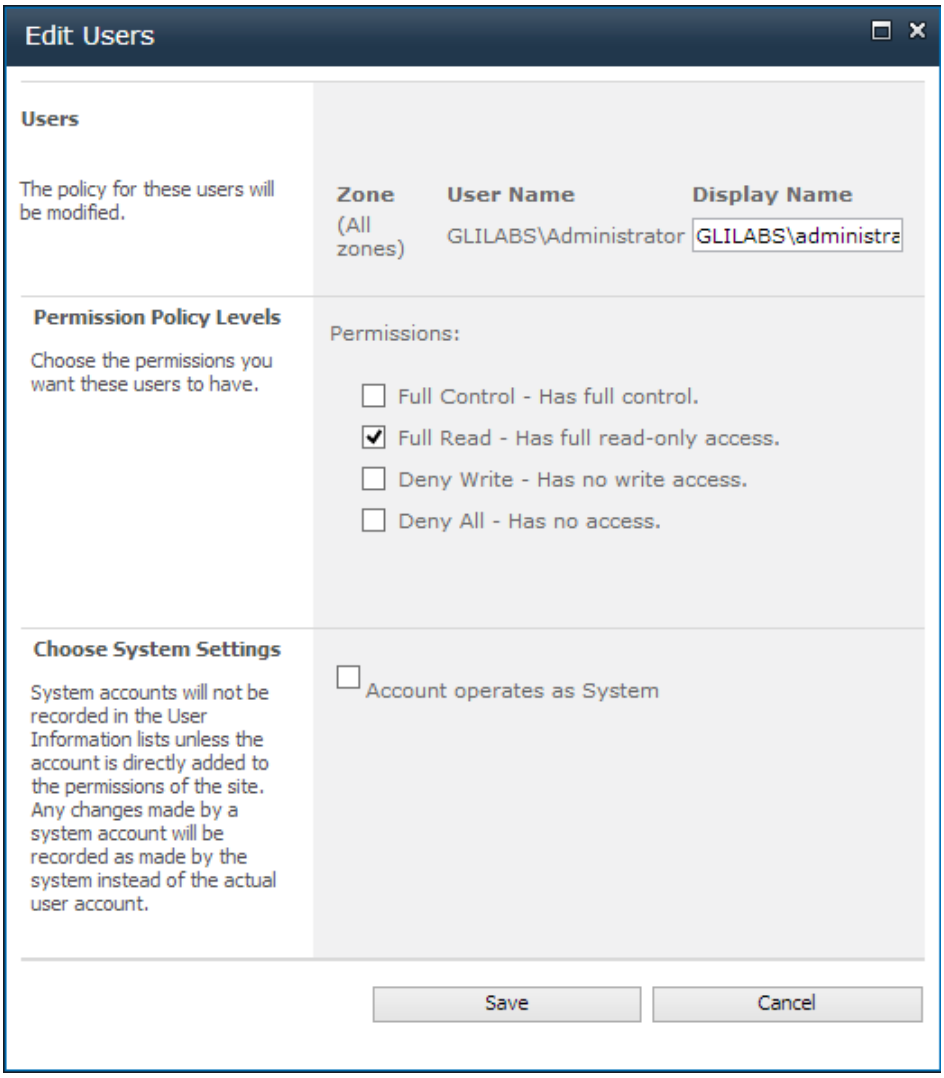
3. Klicken Sie unter **Webanwendungen** auf **Webanwendungen verwalten**.
4. Wählen Sie Ihre Webanwendung aus der Liste aus und klicken Sie auf **Benutzerrichtlinie**.



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.

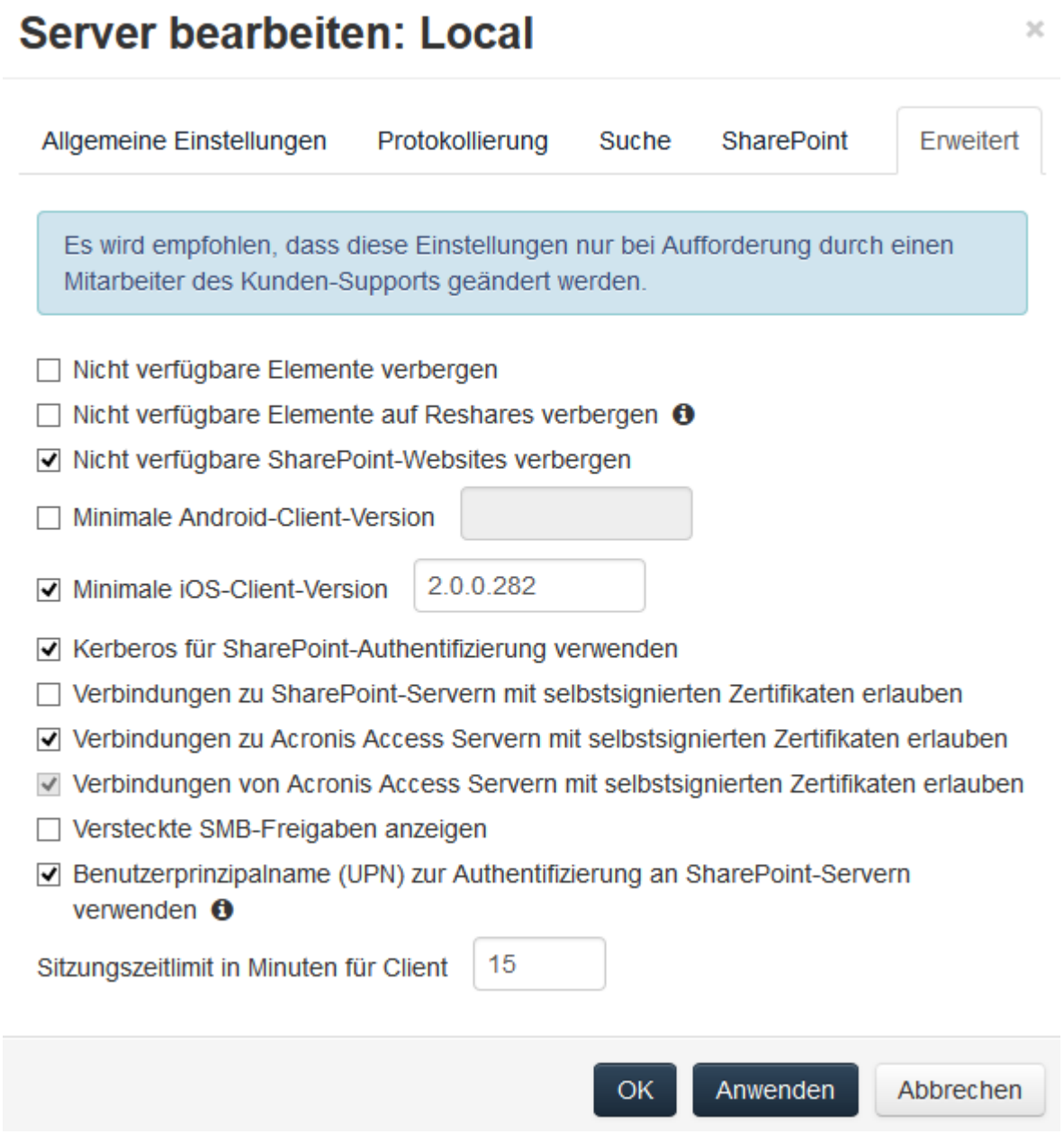


6. Aktivieren Sie unter **Richtlinienstufen für Berechtigungen** das Kontrollkästchen **Alles lesen – Verfügt über vollständigen schreibgeschützten Zugriff**.



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 dürfen Sie nur den Diensttyp 'http' auswählen.

  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).

3.5 Datenquellen verwalten

Sie können NTFS-Verzeichnisse freigeben, die sich auf Ihrem Windows-Server oder in einer Remote-SMB/CIFS-Dateifreigabe befinden, damit Acronis Access Benutzer darauf zugreifen können. Wenn die mobilen Acronis Access Benutzer die Verbindung herstellen, sehen sie diese Datenquellen als Ordner. Sie können Datenquellen erstellen, die Zugriff auf einen Sync & Share-Server bieten.

***Hinweis**: Mit Acronis Access können Sie insgesamt **3** Datenquellen an Remote-Speicherorten haben. Diese Speicherorte umfassen SharePoint-Websites, SharePoint-Bibliotheken und SMB/CIFS-Freigaben.*

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

Ordner.....60

3.5.1 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-Wege** – 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.

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**

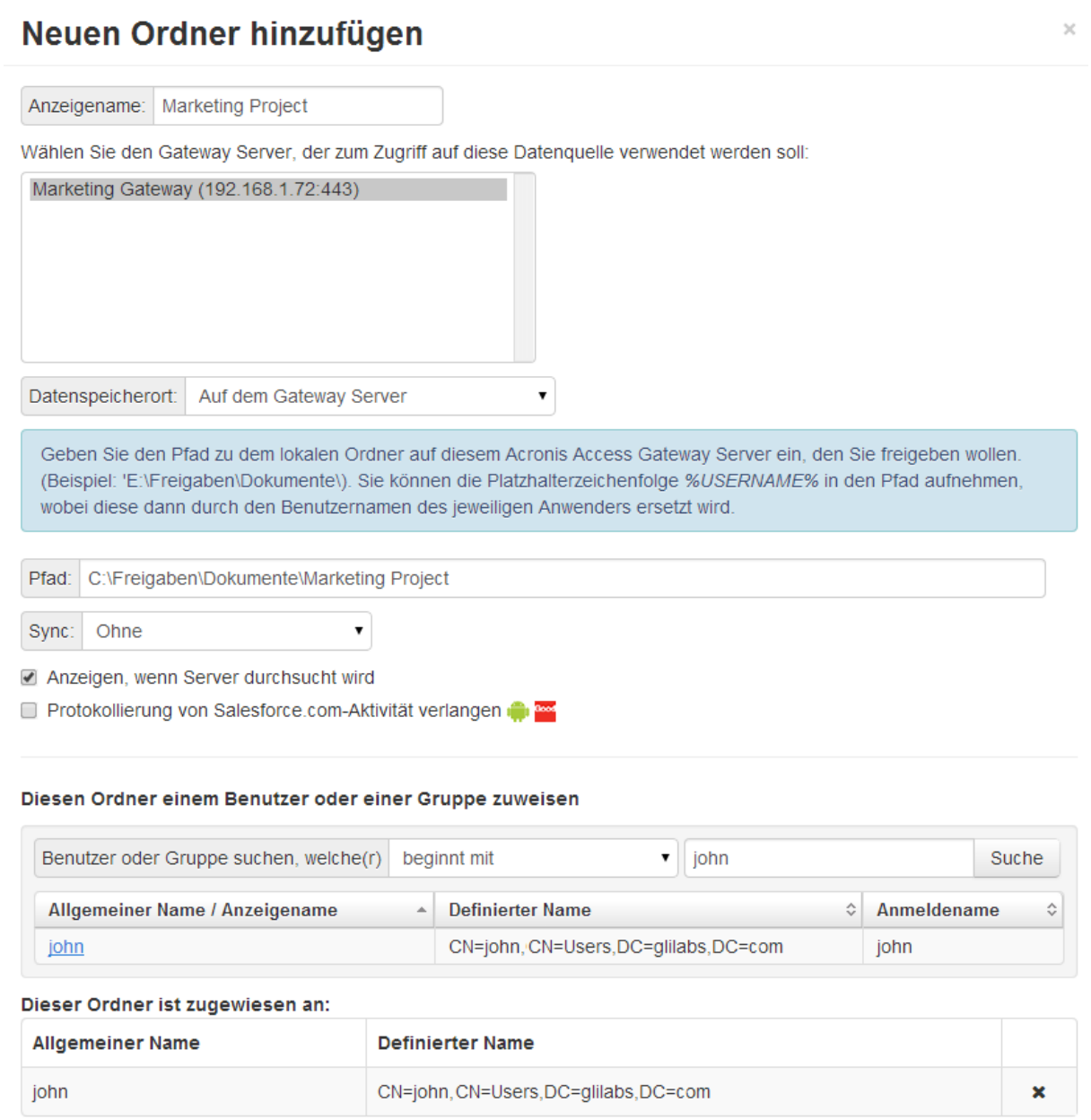
Beim Erstellen einer Datenquelle für einen bestimmten Ordner in einer SharePoint-Bibliothek müssen Sie alle Felder ausfüllen. Im Feld 'URL' geben Sie die Adresse der SharePoint-Website oder -Unterwebsite ein., Im Feld 'Dokumentbibliotheksname' geben Sie den Namen der Bibliothek ein. und im Feld 'Unterpfad' 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. 51).

Datenquellen erstellen



So erstellen Sie eine Datenquelle:

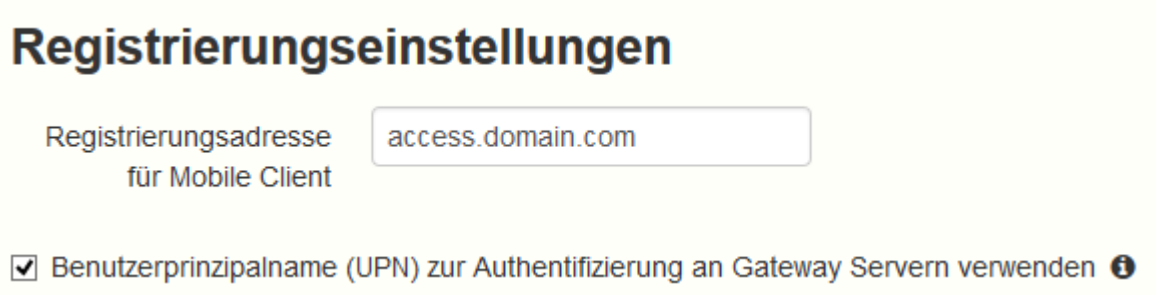
1. Öffnen Sie die Acronis Access Weboberfläche.
2. Öffnen Sie die Registerkarte **Mobiler Zugriff**.
3. Öffnen Sie die Registerkarte **Datenquellen**.
4. Wechseln Sie zu **Ordner**.
5. Klicken Sie auf die Schaltfläche **Neuen Ordner hinzufügen**.
6. Geben Sie einen Anzeigenamen für den Ordner ein.
7. 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. 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.*

4 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 erfolgreicher Registrierung im Management speichert die Acronis Access-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.*

5 Schnellstart: Mobile Access

Diese Anleitung enthält die wesentlichen Schritte zum Einstellen Ihrer Gruppenrichtlinie, zum Hinzufügen einer Datenquelle und zur Installation der Access Mobile Client-App. Ausführlichere Informationen über die Konfiguration des Acronis Access Gateway Servers und der Management-Komponenten finden Sie im Abschnitt Mobiler Zugriff (S. 31).

Themen

Erste Ausführung 65
Einstellen Ihrer Gruppenrichtlinie 70
Die Access Mobile Client-Applikation installieren 70
Für das Client Management registrieren 70

5.1 Erste Ausführung

Wenn Sie es nicht bereits erledigt haben, installieren und konfigurieren Sie Acronis Access. Weitere Informationen hierzu finden Sie in den Abschnitten zur Installation (S. 1) und zum Konfigurationswerkzeug.

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

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

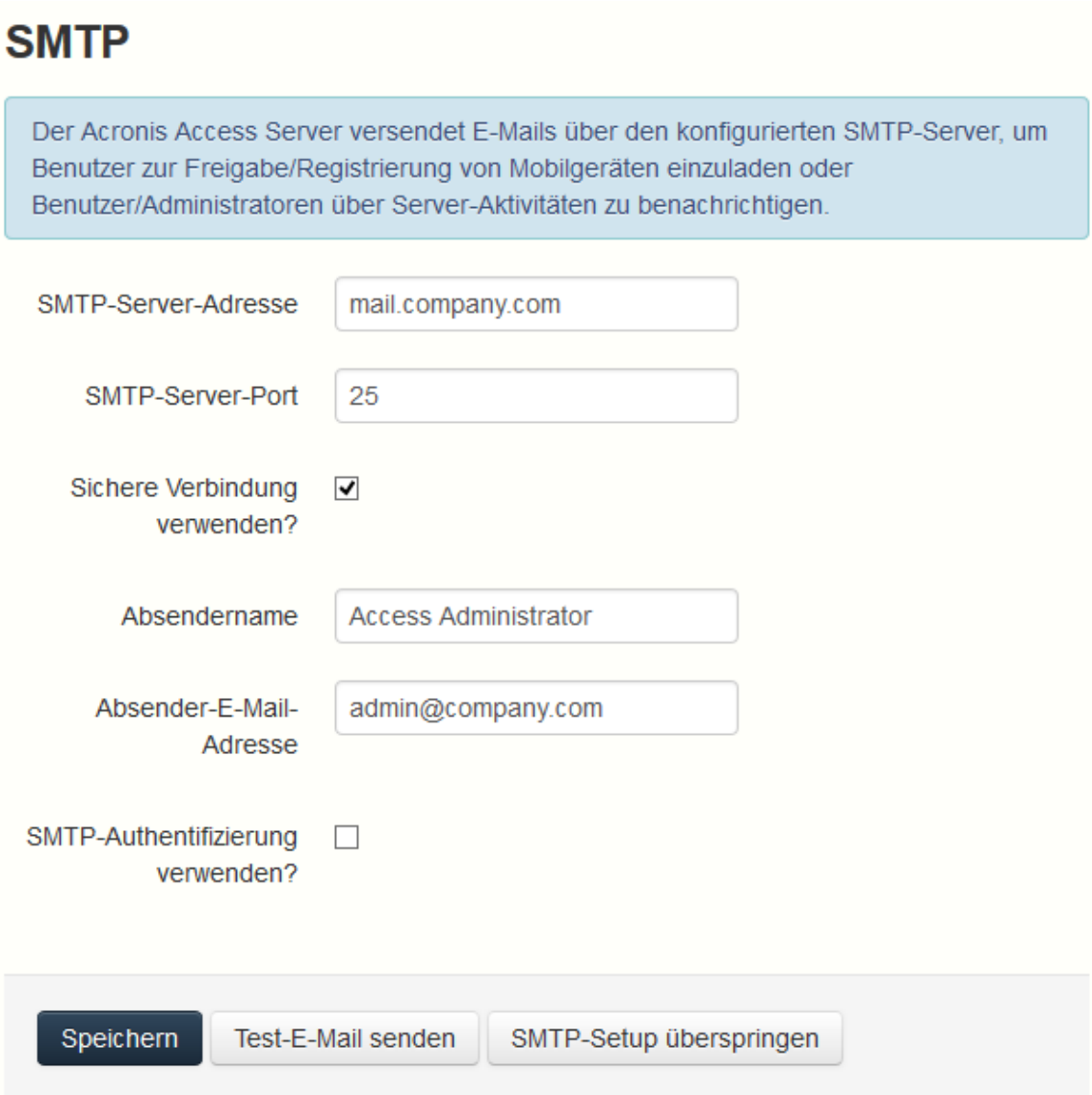
Hinweis: *Es kann 30 bis 45 Sekunden dauern, bis die Applikation zur Verfügung steht, nachdem Sie sie über das Konfigurationswerkzeug gestartet haben.*

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

Allgemeine Einstellungen

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

SMTP

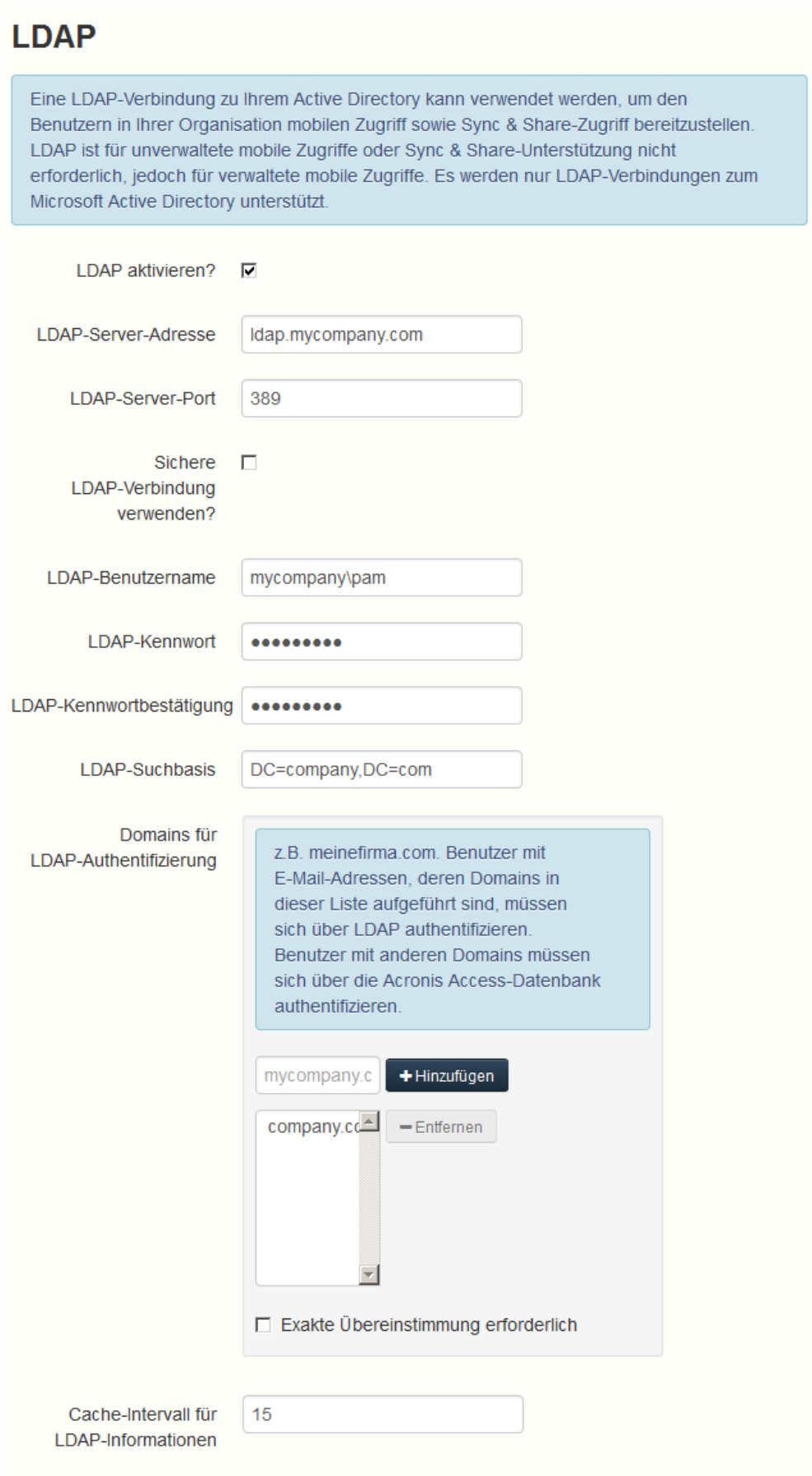


Hinweis: *Sie können diesen Abschnitt überspringen und SMTP später konfigurieren.*

1. Geben Sie den DNS-Namen oder die IP-Adresse Ihres SMTP-Servers ein.
2. Geben Sie den SMTP-Port Ihres Servers ein.

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

LDAP



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

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

6 Einstellen Ihrer Gruppenrichtlinie

Innerhalb Ihrer Gruppenrichtlinie können Sie festlegen, was Ihre Benutzer mit Dateien tun können und worauf sie Zugriff haben.

Einstellen Ihrer Gruppenrichtlinie:

1. Öffnen Sie die Registerkarte **Richtlinien**.
2. Klicken Sie auf die **Standard**richtlinie.
3. Nehmen Sie die erforderlichen Konfigurationen auf den jeweiligen Registerkarten vor (Sicherheit (S. 34), Applikation (S. 35), Synchronisierung (S. 38), Basisordner (S. 39) und Server (S. 40)) und drücken Sie **Speichern**.

6.1 Die Access Mobile Client-Applikation installieren

1. Navigieren Sie im Apple App Store oder im Google Play Store zu Acronis Access.
   - Rufen Sie mit Ihrem iOS-Gerät den Apple App Store auf, und suchen Sie nach Acronis Access, oder folgen Sie diesem Link: http://www.grouplogic.com/web/meappstore.
   - Rufen Sie mit Ihrem Android-Gerät den Google Play Store auf, und suchen Sie nach Acronis Access, oder folgen Sie diesem Link: https://play.google.com/store/apps/details?id=com.grouplogic.mobilecho.
2. Installieren Sie die Acronis Access App und tippen Sie darauf, um sie zu starten.
3. Tippen Sie im Begrüßungsbildschirm auf 'Weiter'.
   - Tippen Sie unter iOS auf das Symbol '+', um einen Server hinzuzufügen.
   - Öffnen Sie unter Android das Menü **Einstellungen** und tippen Sie auf **Server hinzufügen**.
4. Geben Sie den Server-Namen oder die IP-Adresse des Servers ein, auf dem Sie Acronis Access installiert haben. Sie können einen Anzeigenamen für diesen Server angeben, der in der Serverliste angezeigt wird.
5. Geben Sie den Namen eines Benutzers ein, der Zugriff auf den Gateway Server hat. <RPODUCT_NAME> regelt den Zugriff mithilfe von Standard-NTFS-Berechtigungen.
6. Schalten Sie **Kennwort speichern** auf EIN um, wenn Ihr Kennwort gespeichert werden soll. Geben Sie dann Ihr Kennwort ein und bestätigen Sie es.
7. Tippen Sie auf **Speichern**, um die Servereinstellungen zu übernehmen.
8. Tippen Sie auf den im linken Fensterbereich angezeigten Server, um eine Verbindung herzustellen und die verfügbaren Volumes zu durchsuchen.
9. Sämtliche Details zu den Einstellungen und Funktionen der Access Mobile Client-Applikation finden Sie auf der Seite Mobile Client.

6.2 Für das Client Management registrieren

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

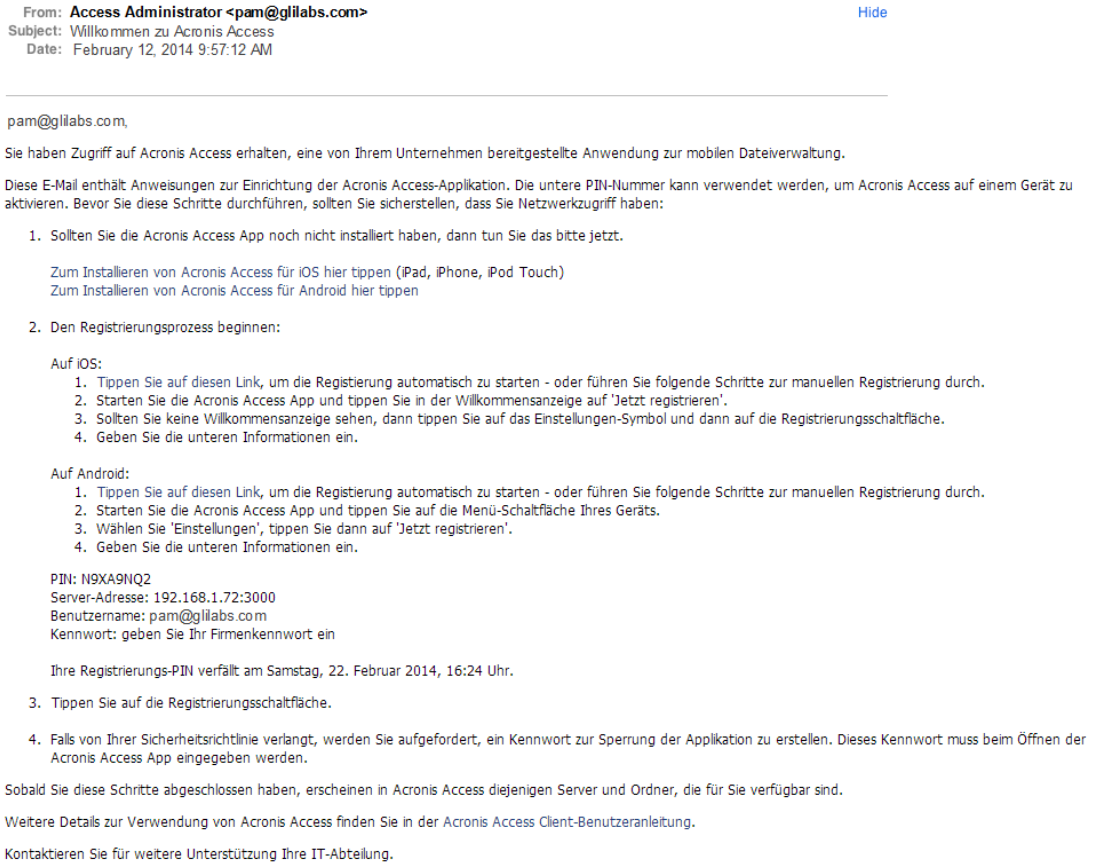
Wenn Ihre Organisation den Zugriff auf den Access Mobile Client und dessen Einstellungen zentral verwaltet, müssen Sie von der IT-Abteilung den Zugriff auf Acronis Access anfordern. Sobald Ihnen

der Zugriff gewährt wurde, erhalten Sie eine Registrierungs-E-Mail. Diese E-Mail enthält Informationen und Anweisungen, die Sie für die Verwendung des Access Mobile Clients benötigen.

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

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

- Link zur Installation des Access Mobile Clients über den Apple App Store
- Link zum Starten der Access Mobile Client-App und zum Automatisieren des Registrierungsprozesses
- 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 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 eingeben, 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 Gruppenrichtlinie zuzuordnen, auf den Gateway-Server zuzugreifen und die Anmeldedaten für Acronis Access Server-Anmeldungen zu speichern, falls die Richtlinie 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.

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 und Benutzername automatisch ausgefüllt.
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.

Manuelle Registrierung

1. Öffnen Sie die Acronis Access-App.
2. Öffnen Sie **Einstellungen**.
3. Tippen Sie auf **Registrieren**.
4. Geben Sie Ihre Serveradresse, Ihren Benutzernamen und Ihr 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.

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.

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

Acronis Access Clients benötigen Netzwerkzugriff auf den Acronis Access 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 erhält, so wird diese Verbindung zum VPN auch benötigt, bevor Verwaltungsbefehle akzeptiert werden.

Verwaltung entfernen

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

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

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

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

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

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

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

1. Setzen Sie einen Finger auf das Symbol der Access Mobile Client-App, bis es sich zu bewegen beginnt.

2. Tippen Sie auf die Schaltfläche '**X**' in der Access Mobile Client-Applikation, und bestätigen Sie den Deinstallationsvorgang.

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

7 Schnellstart: Sync & Share

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

Themen

Erster Durchlauf 75
Web-Client 80
Den Desktop-Client verwenden 87

7.1 Erster Durchlauf

Wenn Sie es nicht bereits erledigt haben, installieren und konfigurieren Sie Acronis Access. Weitere Informationen hierzu finden Sie in den Abschnitten zur Installation (S. 1) und zum Konfigurationswerkzeug.

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

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

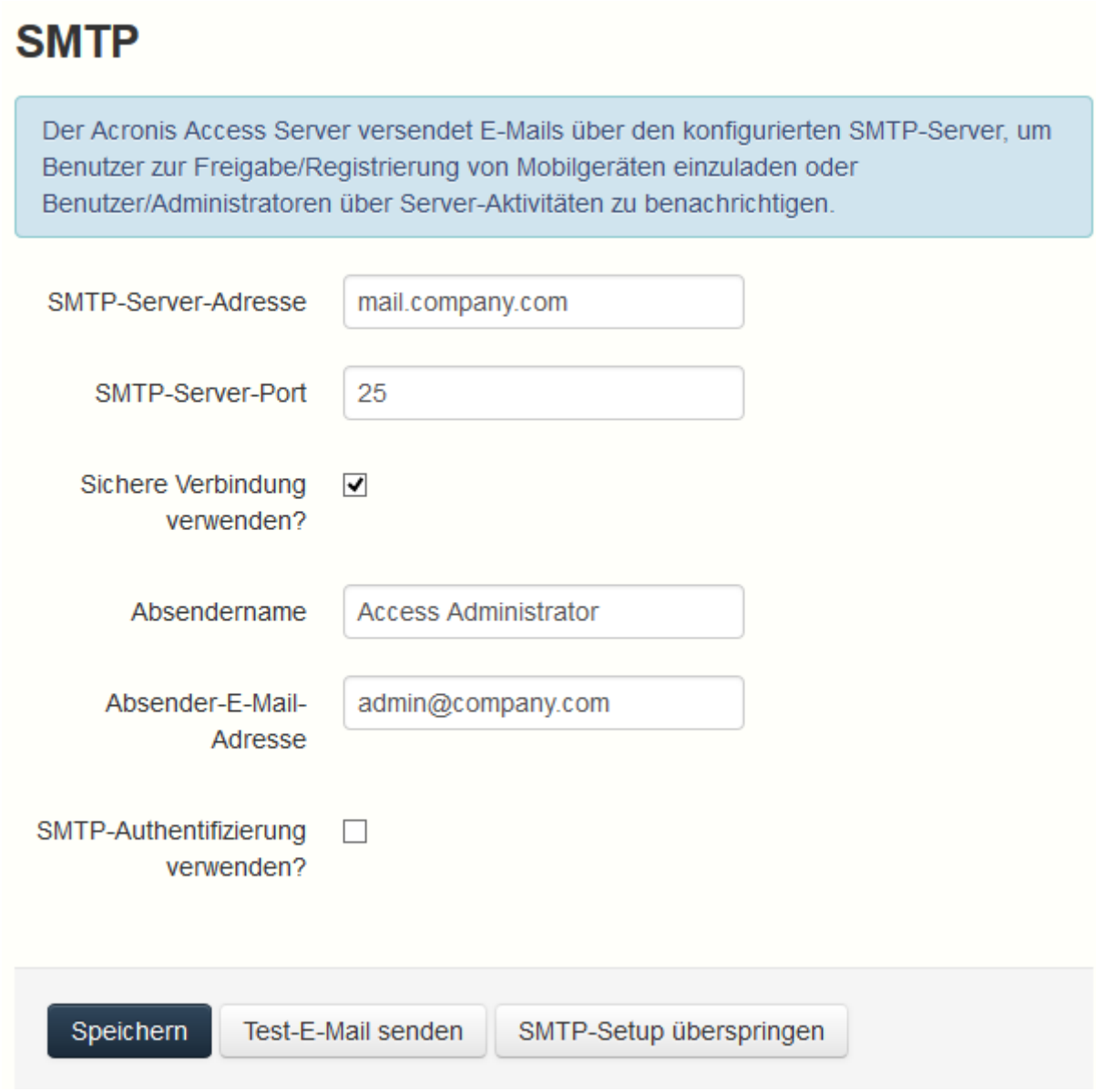
Hinweis: *Es kann 30 bis 45 Sekunden dauern, bis die Applikation zur Verfügung steht, nachdem Sie sie über das Konfigurationswerkzeug gestartet haben.*

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

Allgemeine Einstellungen

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

SMTP

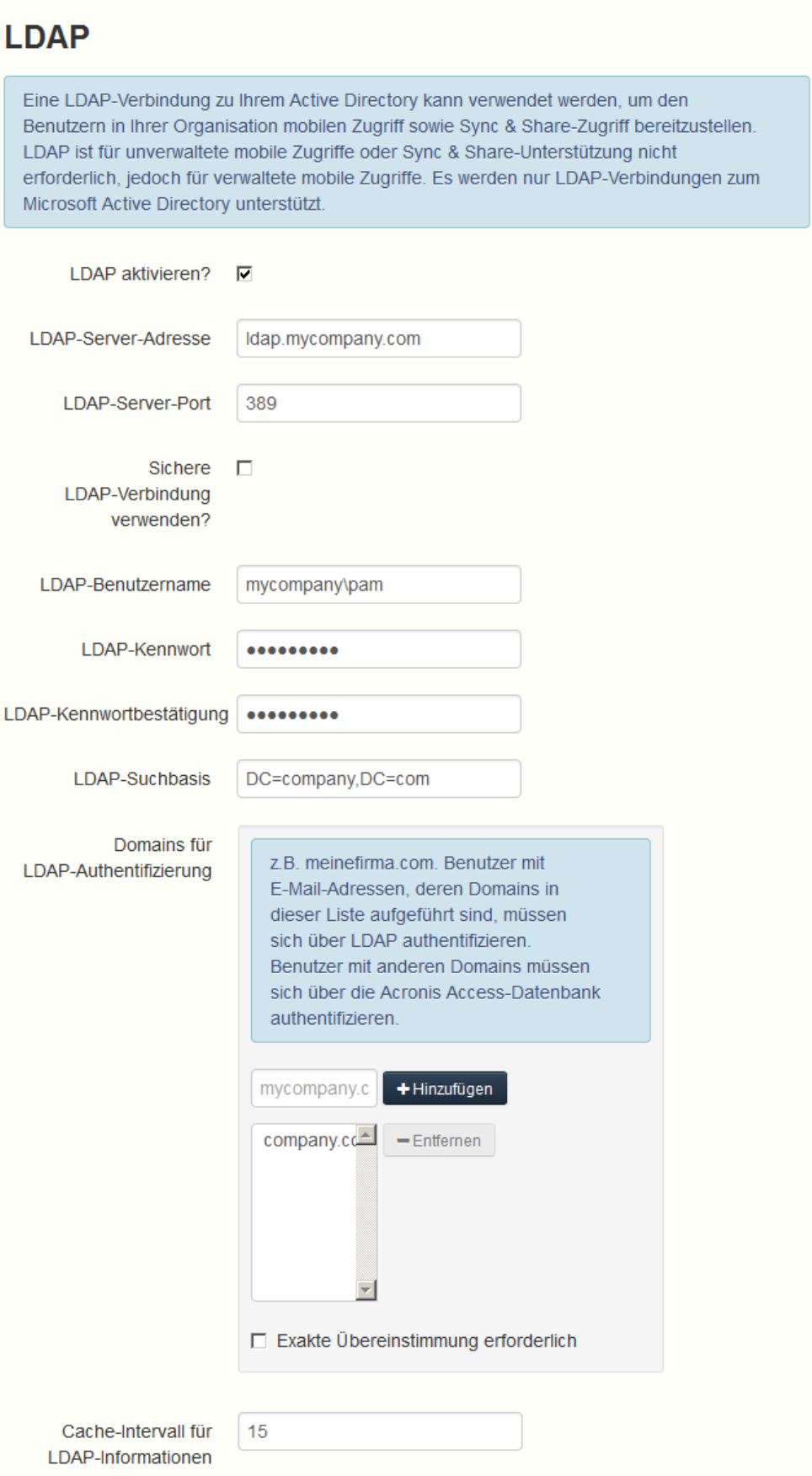


Hinweis: *Sie können diesen Abschnitt überspringen und SMTP später konfigurieren.*

1. Geben Sie den DNS-Namen oder die IP-Adresse Ihres SMTP-Servers ein.

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

LDAP



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

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

8 Web-Client

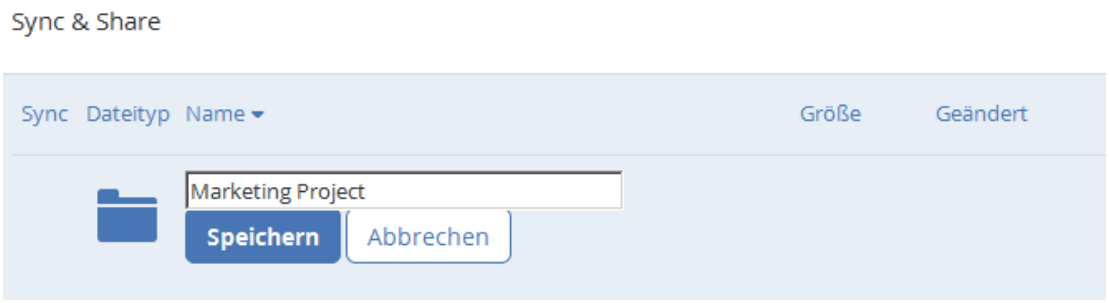
1. Starten Sie den Webbrowser und navigieren Sie zu: https://meinserver https://myserver, wobei **meinserver** die URL oder IP-Adresse des Computers ist, auf dem der Acronis Access Server ausgeführt wird.

2. Melden Sie sich mit Ihren Anmeldedaten an.
   a. Falls nur der Acronis Access Server installiert ist, melden Sie sich als **administrator** mit dem Kennwort an, das Sie nach der Installation festgelegt haben. Wenn Sie die Weboberfläche zum ersten Mal öffnen, werden Sie aufgefordert, das Kennwort jetzt festzulegen.
   b. Falls Sie eine E-Mail-Einladung für Acronis Access erhalten haben, müssen Sie zu diesem Zeitpunkt möglicherweise **Ihr persönliches Kennwort** festlegen oder sich mit Ihren Active Directory-Anmeldedaten anmelden.
   c. Falls Ihr Acronis Access Server zur Verwendung von Active Directory für die Authentifizierung und Bereitstellung von Benutzerkonten konfiguriert wurde, sollten Sie in der Lage sein, sich mit gültigen Netzwerkangaben für das Netzwerk anzumelden.

Hinweis: *Wenn Sie als Administrator angemeldet sind, haben Sie keinen Zugriff auf den Web-Client. Sie müssen ein vom Standard-Administratorkonto abweichendes Konto verwenden.*

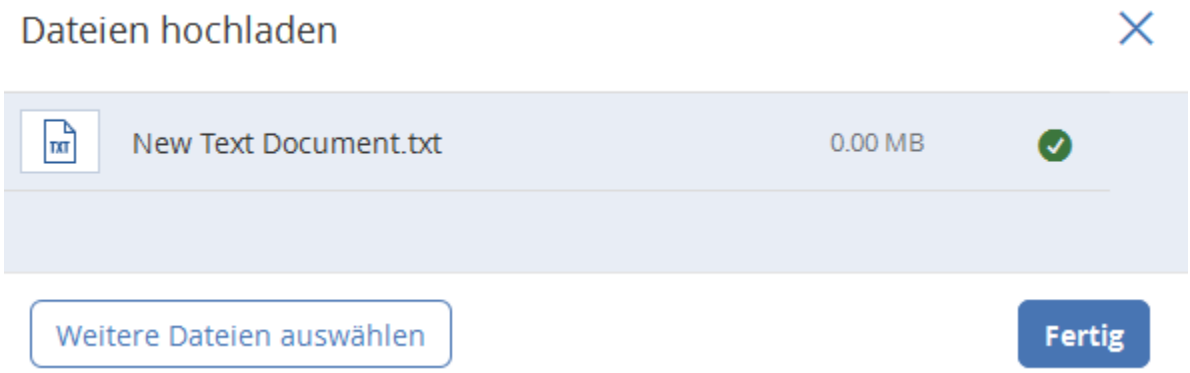
Neuer Ordner

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



Dateien hochladen

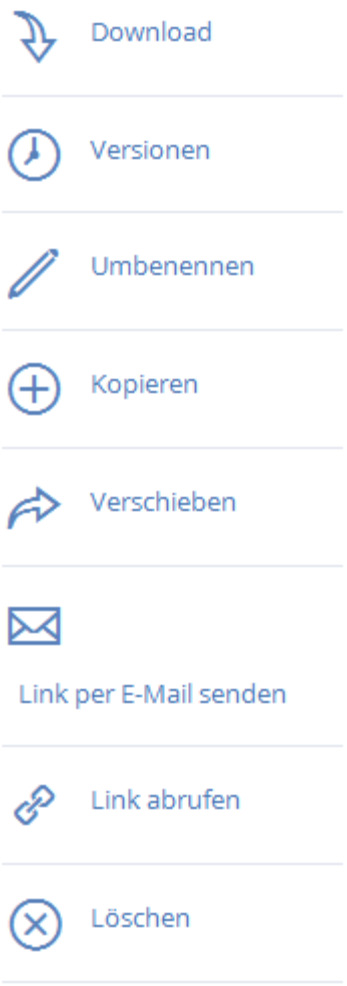
1. Navigieren Sie zu dem neuen Ordner durch Klicken auf seinen Namen.
2. Klicken Sie auf **Dateien hochladen**, dann auf **Dateien hinzufügen...** und wählen Sie mindestens eine Datei auf dem Computer aus.



3. Die Dateien werden in den Ordner hochgeladen, in dem Sie sich befinden. Drücken Sie auf **Fertig**.

Alternativ können Dateien auch durch Ziehen und Ablegen auf der Webseite hochgeladen werden:

Durch Klicken auf eine Datei oder einen Ordner werden die verfügbaren Aktionen in der rechten Seitenleiste angezeigt.



Download von Datei

Für den Download einer Datei müssen Sie nur auf deren Namen klicken. Sie könne auch auf die Zeile rechts neben Datei- oder Ordnernamen klicken, und in der Seitenleiste auf **Download** drücken.

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

Eine Datei oder einen Ordner kopieren

Gehen Sie wie folgt vor, um eine Datei oder einen Ordner zu kopieren:

1. Klicken Sie in der Zeile rechts neben Datei- oder Ordnernamen, und wählen Sie **Kopieren**.
2. Navigieren Sie in der neuen Lightbox zu dem Ordner, in den Sie die Datei einfügen möchten, und klicken Sie auf **Kopieren**.

Eine Datei oder einen Ordner verschieben

1. Klicken Sie in der Zeile rechts neben Datei- oder Ordnernamen, und wählen Sie **Verschieben**.
2. Navigieren Sie in der neuen Lightbox zu dem Ordner, in den Sie die Datei verschieben möchten, und klicken Sie auf **Verschieben**.

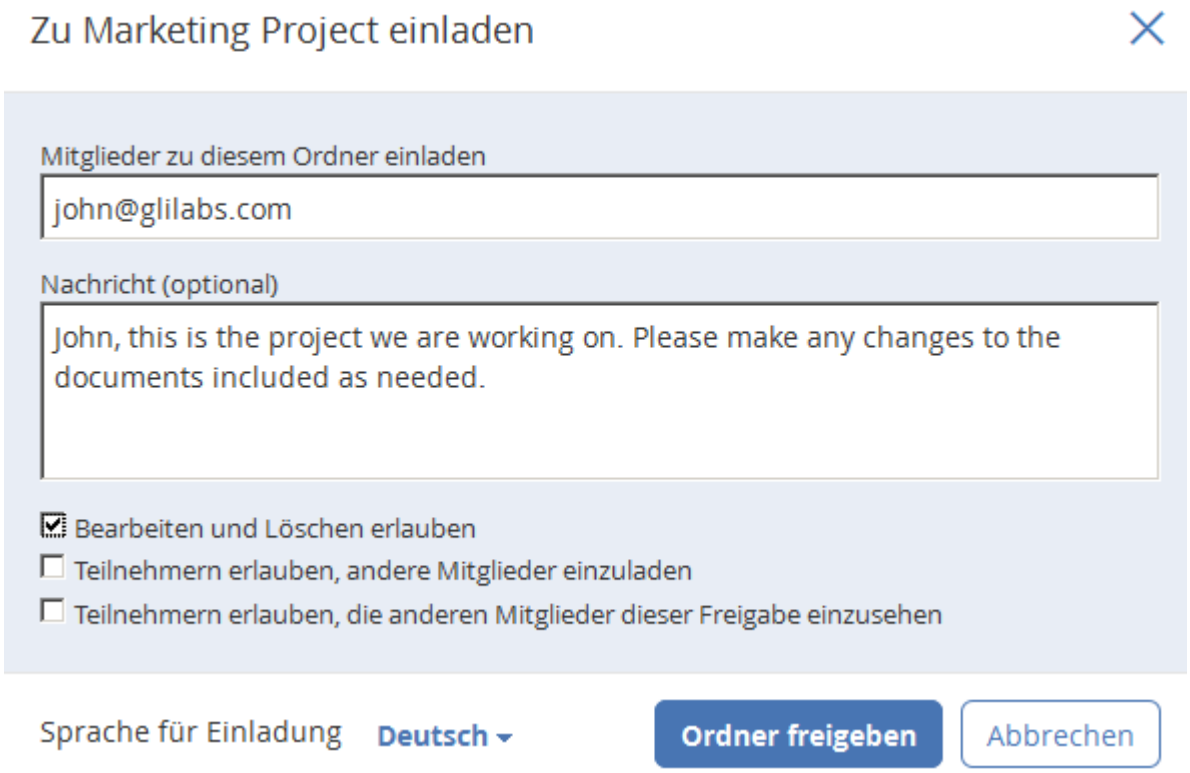
Einen Ordner freigeben

Hinweis: *Falls Sie eine Datei oder einen Ordner freigeben möchten, die bzw. den ein anderer Benutzer für Sie freigegeben hat, benötigen Sie die Berechtigungen, andere Benutzer zu dieser Freigabe einzuladen. Falls Sie nicht zum Einladen anderer Benutzer berechtigt sind, können Sie die Dateien und Ordner nicht für einen anderen Benutzer freigeben. Die Option* ***Freigeben*** *in der rechten Seitenleiste wird ebenfalls nicht sichtbar sein.*

Gehen Sie wie folgt vor, um einen Ordner mit einem Kollegen oder Geschäftspartner zu teilen:

1. Klicken Sie auf **Sync&Share** oder auf **Netzwerk**, je nach Speicherort des Ordners. Je nach Ihrer Verwaltungsrichtlinie haben Sie unter Umständen keinen Zugriff auf die Registerkarte **Netzwerk**.
2. Klicken Sie auf den Ordner, den Sie freigeben möchten, und wählen Sie **Freigeben** in der Seitenleiste.

3. Geben Sie in der Lightbox **Freigeben** eine E-Mail-Adresse und eine entsprechende Textnachricht ein. Eine E-Mail mit Ihren Informationen und Zugriffsanweisungen wird generiert und an den Empfänger gesendet.



Hinweis: *Wenn das Kontrollkästchen* ***Bearbeiten und Löschen erlauben*** *deaktiviert ist, können eingeladene Benutzer nur solche Dokumente herunterladen und lesen, die im freigegebenen Ordner enthalten sind.*

Eine einzelne Datei freigeben

Hinweis: *Falls Sie eine Datei oder einen Ordner freigeben möchten, die bzw. den ein anderer Benutzer für Sie freigegeben hat, benötigen Sie die Berechtigungen, andere Benutzer zu dieser Freigabe einzuladen. Falls Sie nicht zum Einladen anderer Benutzer berechtigt sind, können Sie die Dateien und Ordner nicht für einen anderen Benutzer freigeben. Die Option* ***Freigeben*** *in der rechten Seitenleiste wird ebenfalls nicht sichtbar sein.*

1. Rufen Sie die Acronis Access-Weboberfläche auf.
2. Wenn Sie sich mit einem Administratorkonto angemeldet haben, drücken Sie in der oberen rechten Ecke **Administration verlassen**.
3. Navigieren Sie zur gewünschten Datei, und klicken Sie auf die Zeile neben dem Namen.

a) **Link per E-Mail senden**

   a. Wählen Sie die Option **Link senden** in der Seitenleiste.
   b. Geben Sie die gewünschte Ablaufzeit und Sprache für die Einladung an.
   c. Geben Sie die E-Mail-Adressen der Benutzer ein, an die Sie den Download-Link senden möchten.
   d. Klicken Sie auf **Senden**.

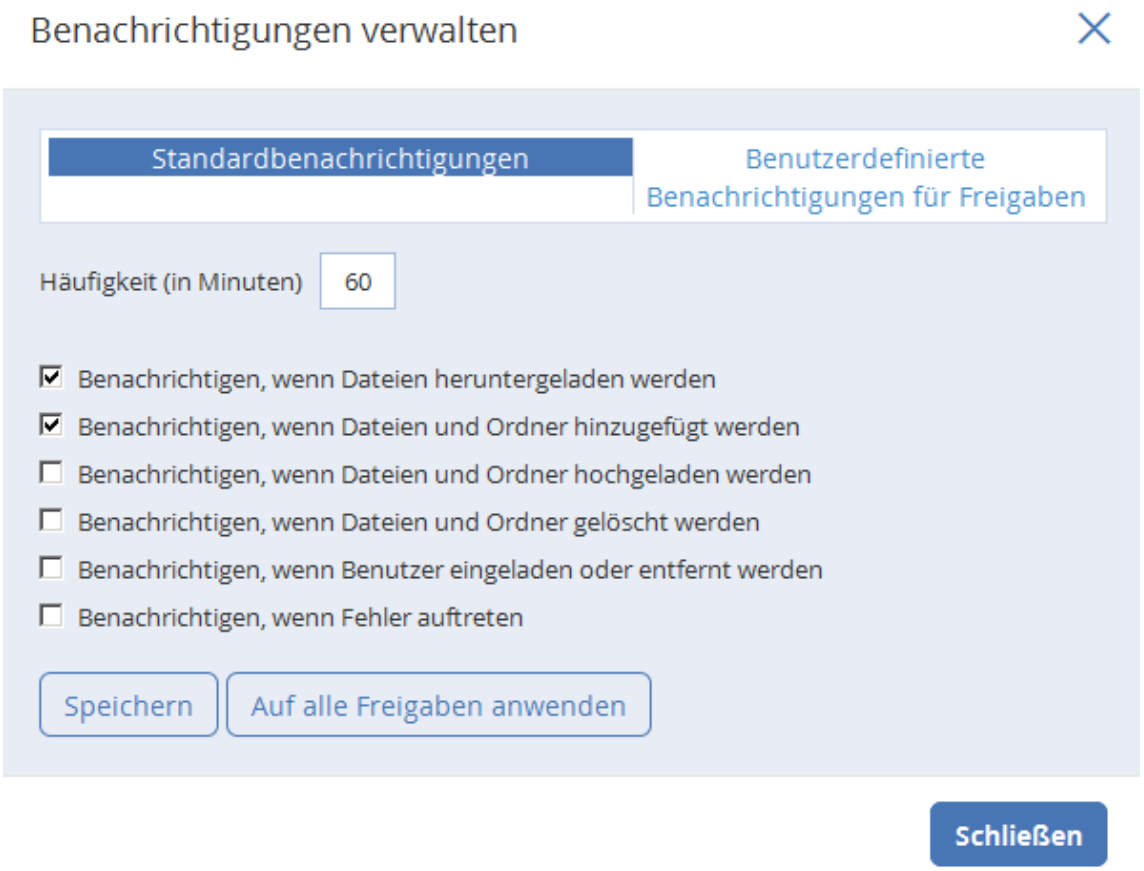
b) **Einen Link mittels anderer Methoden senden**

   a. Wählen Sie die Option **Link abrufen** in der Seitenleiste.
   b. Geben Sie die gewünschte Ablaufzeit und Sprache für die Einladung an.
   c. Klicken Sie auf **Link kopieren**.
   d. Geben Sie den Link mittels einer von Ihnen bevorzugten Methode frei.

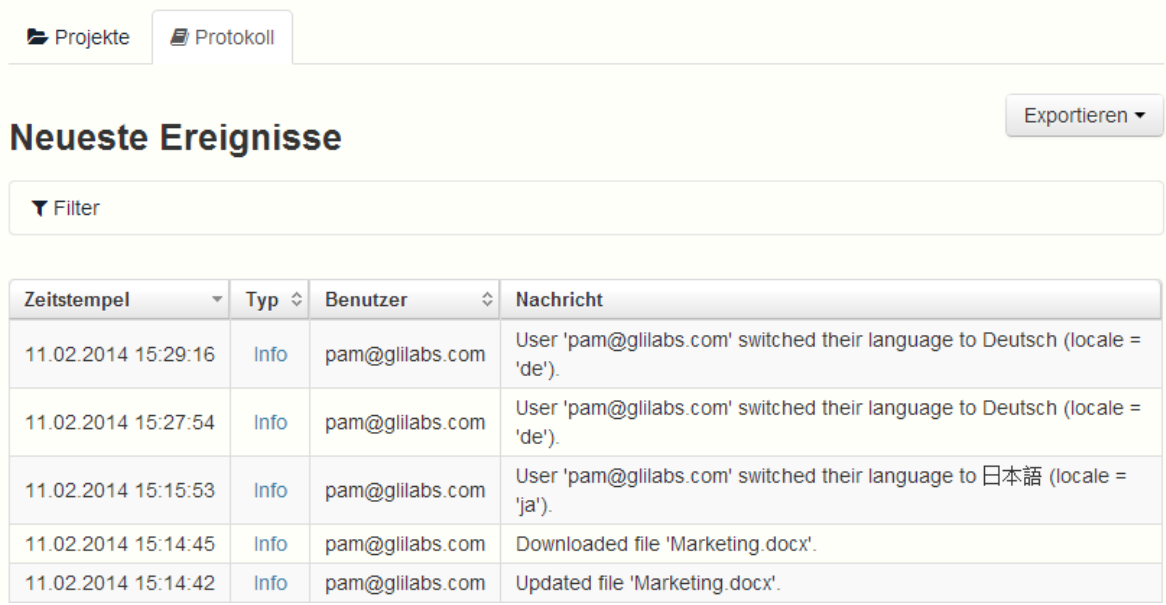
E-Mail-Benachrichtigungen abonnieren

Sie können E-Mail-Benachrichtigungen für Ordner abonnieren, die für Sie freigegeben wurden.

1. Geben Sie dafür einfach den freigegebenen Ordner ein, und klicken Sie in der Seitenleiste auf **Benachrichtigungen**.
2. Wählen Sie die Bedingungen aus, unter denen Sie benachrichtigt werden möchten, und klicken Sie auf **Speichern**.



Sie können den Verlauf der Ereignisse nachverfolgen, indem Sie die Registerkarte **Log** öffnen. Es sind Such- und Filteroptionen verfügbar. Die Wichtigkeit der Ereignisse ist mithilfe verschiedener Farben markiert.

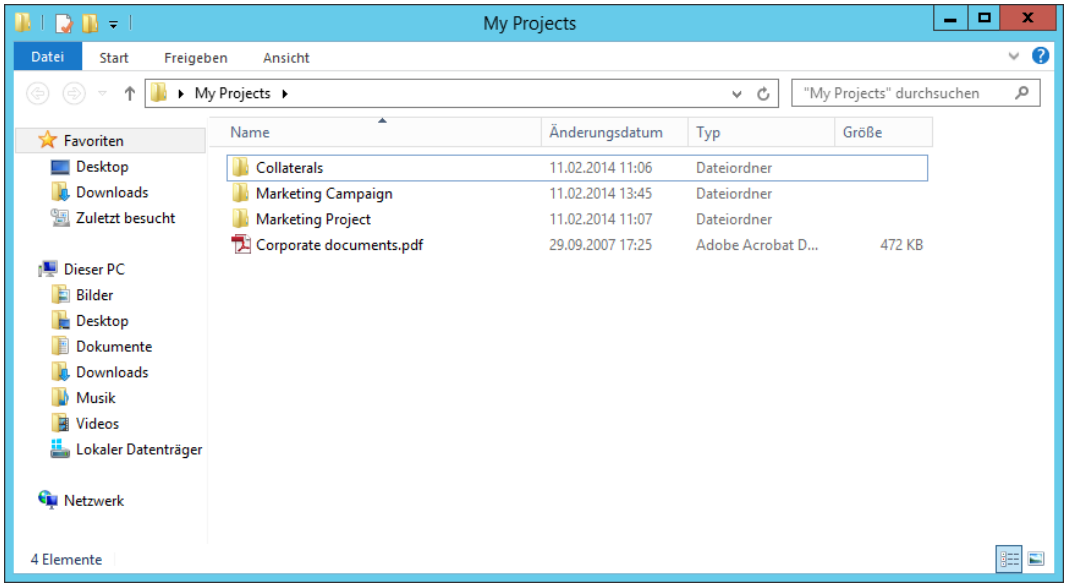


8.1 Den Desktop-Client verwenden

Erste Schritte

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

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

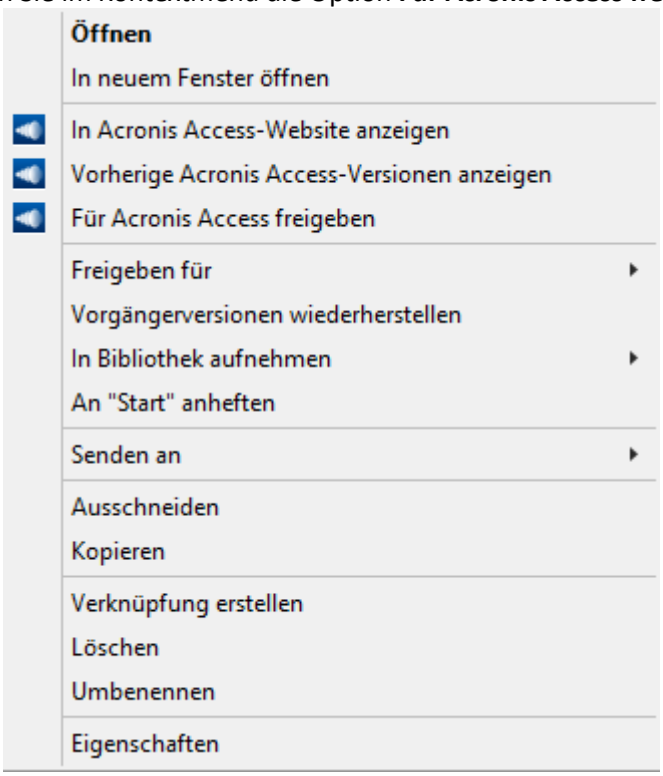


5. Legen Sie einige Dateien darin ab, indem Sie sie von Ihrem Computer kopieren.

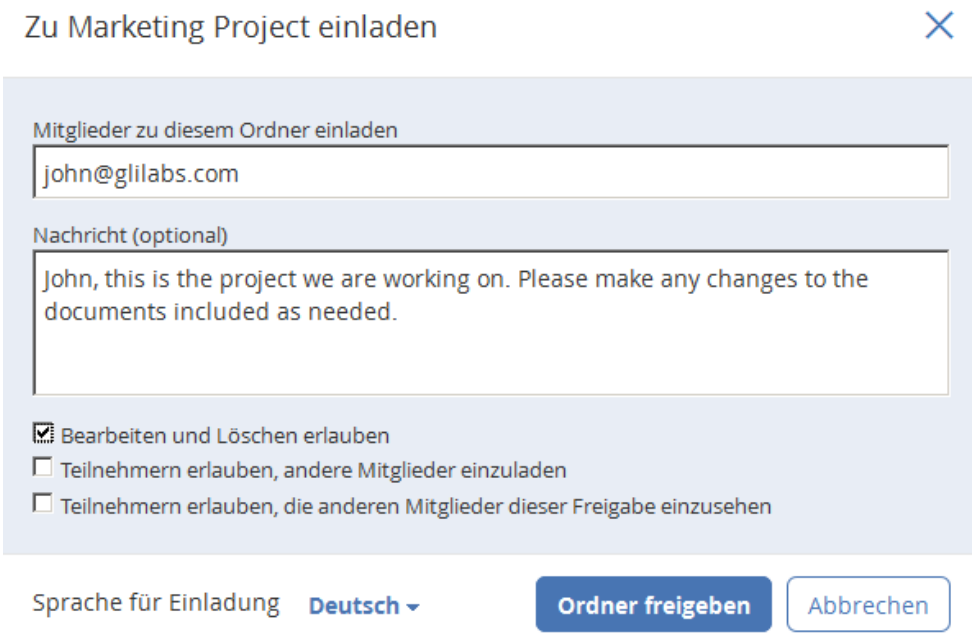
6. Nun können Sie einen Ordner für einen Kollegen freigeben. Hierbei sind zwei unterschiedliche Methoden möglich: direkt über Windows Explorer oder mithilfe Ihres Webbrowsers. Führen Sie Schritt 7 aus, um Inhalte von Ihrem Desktop über Windows Explorer freizugeben, oder befolgen Sie Schritt 8, um Inhalte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

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

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



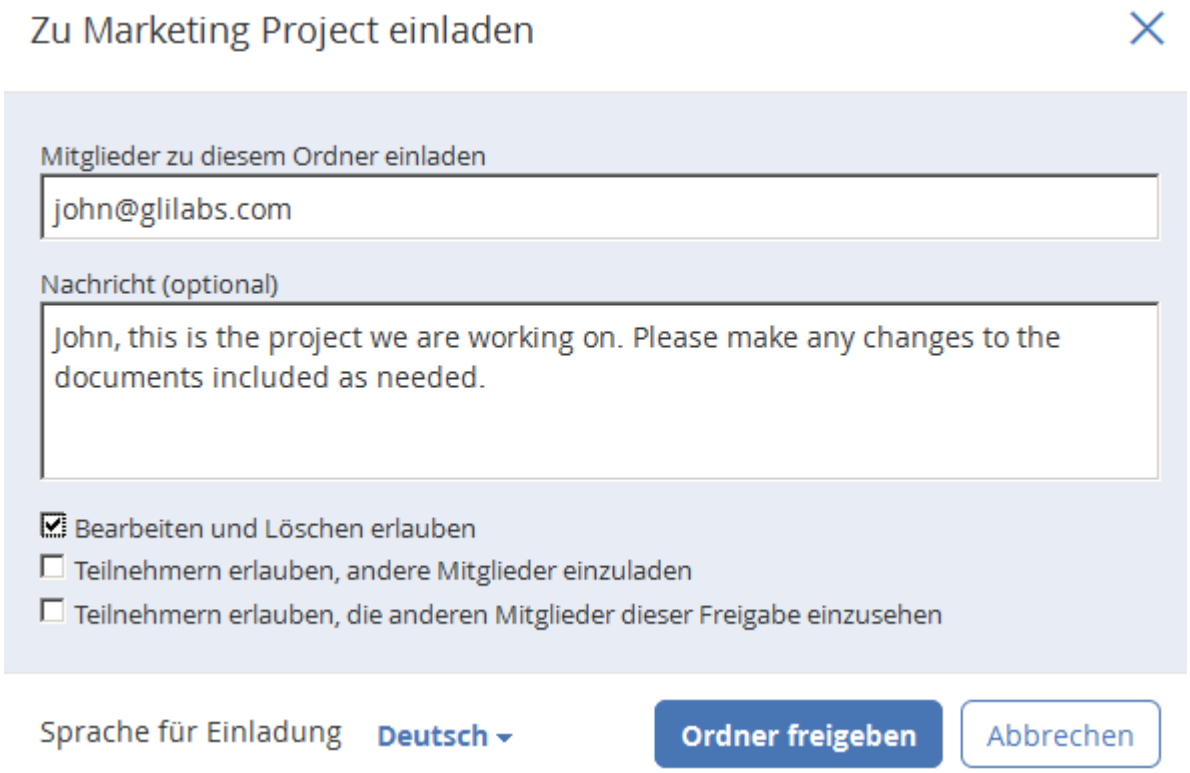
   c. Dadurch wird ein Webbrowser gestartet und das Dialogfeld 'Einladen' angezeigt.
   d. Geben Sie im Dialogfeld **Andere einladen** eine E-Mail-Adresse und eine entsprechende Textnachricht ein.



Für den Fall, dass Sie stattdessen Ihren Webbrowser verwenden möchten:

1. Öffnen Sie https://server.com/ https://server.com/, wobei **server.com** die Adresse des Acronis Access Servers ist, und melden Sie sich mit Ihrem Benutzernamen und Kennwort an.
2. Klicken Sie auf **Sync&Share** oder auf **Netzwerk**, je nach Speicherort des Ordners. Je nach Ihrer Verwaltungsrichtlinie haben Sie unter Umständen keinen Zugriff auf die Registerkarte **Netzwerk**.
3. Klicken Sie auf den Ordner, den Sie freigeben möchten, und wählen Sie **Freigeben** in der Seitenleiste.

4. Geben Sie in der Lightbox **Freigeben** eine E-Mail-Adresse und eine entsprechende Textnachricht ein. Eine E-Mail mit Ihren Informationen und Zugriffsanweisungen wird generiert und an den Empfänger gesendet.



Hinweis: *Wenn das Kontrollkästchen* ***Bearbeiten und Löschen erlauben*** *deaktiviert ist, können eingeladene Benutzer nur solche Dokumente herunterladen und lesen, die im freigegebenen Ordner enthalten sind.*

Unabhängig von der zum Einladen einer Person verwendeten Methode, erhält der Empfänger eine oder zwei E-Mails. Dies hängt davon ab, ob es sich um einen internen (Active Directory) oder externen Benutzer handelt.

a. Für einen externen Benutzer enthält die erste E-Mail mit dem Betreff **Sie wurden zu Acronis Access eingeladen.** einen Link zum Festlegen eines persönlichen Kennworts.
b. Die zweite E-Mail mit dem Betreff **Sie haben Zugriff auf die Marketing-Kampagne erhalten** enthält Ihre Nachricht und einen Link zum Zugriff auf die freigegebenen Dateien.

Sobald der eingeladene Benutzer auf den Link klickt, um auf das System zuzugreifen (und bei Bedarf sein Kennwort festzulegen), geben Sie und Ihr Kollege den Zugriff auf die Dateien im Ordner **Marketing-Kampagne** frei.

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

1. **Hinweis:** Die maximale Pfadlänge ist bei Mac OS X und Windows unterschiedlich. Dies kann bei plattformübergreifenden Bereitstellungen zu Synchronisierungsfehlern führen. Unter dem Betriebssystem Windows ist der gesamte Pfad einschließlich des Teils '**`C:\mysharefolder`**' auf 260 Zeichen (MAX_PATH) beschränkt. Dateinamen haben unter Windows daher eine maximale Länge von 260 - [Pfadlänge Freigabeordner] - 1 (für das Abschlusszeichen NULL).

   Beispiel: Der Benutzer gibt C:\my_shared_documents frei und versucht, eine Datei nach C:\my_shared_documents\this_is_a_folder\ herunterzuladen. Die maximale Dateinamenlänge für dieses Unterverzeichnis wäre dann 260 - 40 - 1 = 219 Zeichen. Bei Mac OS X ist die Pfadlänge auf 1024 Zeichen beschränkt.

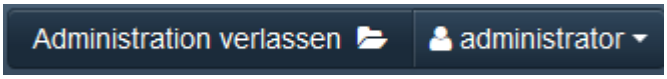
9 Server-Administration

Themen

Server verwalten 92
Administratoren und Berechtigungen 92
Überwachungsprotokoll 94
Server 96
SMTP 98
LDAP 99
E-Mail-Vorlagen 101
Lizenzierung 103
Debug-Protokollierung 104
Überwachung 105

9.1 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 wieder zur Administration zurückzukehren, drücken 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.*

9.2 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.

Mit der Schaltfläche **Aktionen** können Sie die Gruppe löschen oder 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. Suchen Sie die Gruppe.
4. Klicken Sie auf den Gruppennamen.
5. Drücken 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 Sprache der Einladungs-E-Mail aus.
   4. Klicken Sie auf 'Hinzufügen'

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. Aktivieren Sie für alle **Volle Administratorrechte**.
6. Drücken Sie auf **Speichern**.

9.3 Überwachungsprotokoll

9.3.1 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. Wenn Sie zugelassen haben, dass Desktop- und Web-Clients auf mobile Datenquellen zugreifen können, werden diese auch im Log angezeigt.

- **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**.

9.3.2 Einstellungen

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

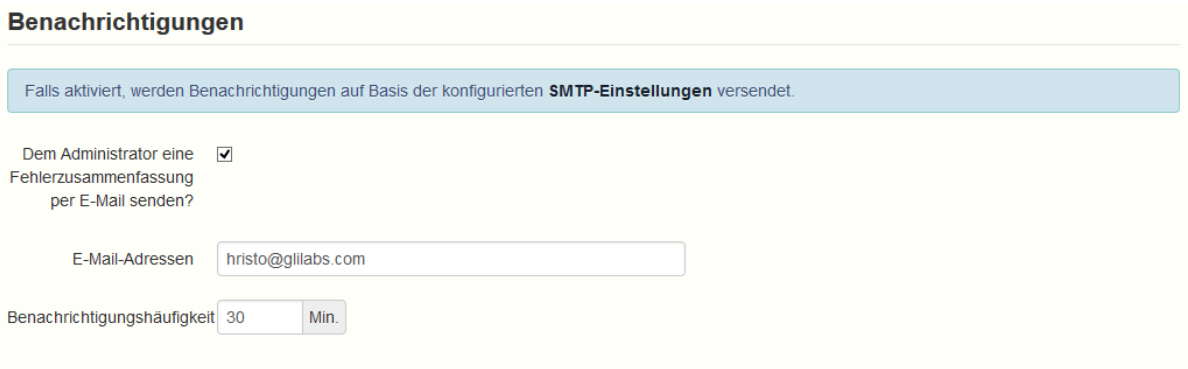
- **Protokolleinträge automatisch bereinigen, die älter als X Y sind** – Wenn diese Option aktiviert ist, werden Protokolle, die älter sind als eine bestimmte Anzahl Tage/Wochen/Monate automatisch bereinigt.
  - **Protokolleinträge vor der Bereinigung als Datei im Format X exportieren** – Wenn diese 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.

9.4 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.

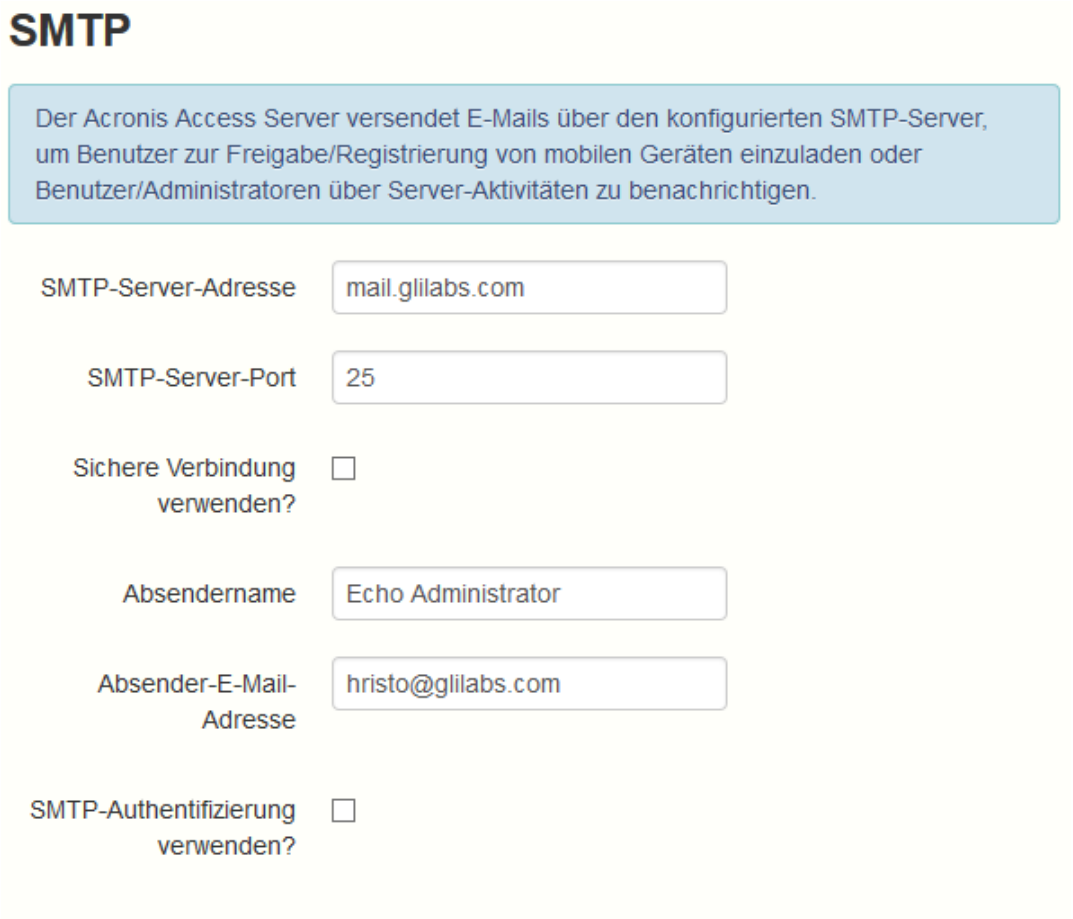


Benachrichtigungseinstellungen

- **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.

9.5 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.

9.6 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

Eine LDAP-Verbindung zu Ihrem Active Directory kann verwendet werden, um den Benutzern in Ihrer Organisation mobilen Zugriff sowie Sync & Share-Zugriff bereitzustellen. LDAP ist für unverwaltete mobile Zugriffe oder Sync & Share-Unterstützung nicht erforderlich, jedoch für verwaltete mobile Zugriffe. Es werden nur LDAP-Verbindungen zum Microsoft Active Directory unterstützt.

LDAP aktivieren?	☑
LDAP-Server-Adresse	myldap.com
LDAP-Server-Port	389
Sichere LDAP-Verbindung verwenden?	☐
LDAP-Benutzername	company\Administrator
LDAP-Kennwort	**********
LDAP-Kennwortbestätigung	**********
LDAP-Suchbasis	dc=company, dc=com
Domains für LDAP-Authentifizierung	company.com
Cache-Intervall für LDAP-Informationen	15
LDAP-E-Mail-Adressen proaktiv auflösen	☐
LDAP-Lookup zur automatischen Vervollständigung von Einladungen und Download-Links verwenden.	☑
Mitgliedschaft in geschachtelter Verteilergruppe einschließen	☐

Speichern

LDAP-Benutzer und -Gruppen werden zur Performance-Steigerung zwischengespeichert. Sollten neuere LDAP-Updates nicht berücksichtigt werden, dann klicken Sie hier, um den LDAP-Cache direkt zu löschen.

- **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-Suchdatenbank** – 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.
    - **Exakte Übereinstimmung erforderlich** - Wenn diese Option aktiviert ist, werden nur Benutzer aus den unter **Domains für LDAP-Authentifizierung** eingegebenen Domänen als LDAP-Benutzer behandelt. Benutzer, die Mitglieder anderer Domänen und Unterdomänen sind, werden als Ad-hoc-Benutzer behandelt.
  - **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.

9.7 E-Mail-Vorlagen

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.

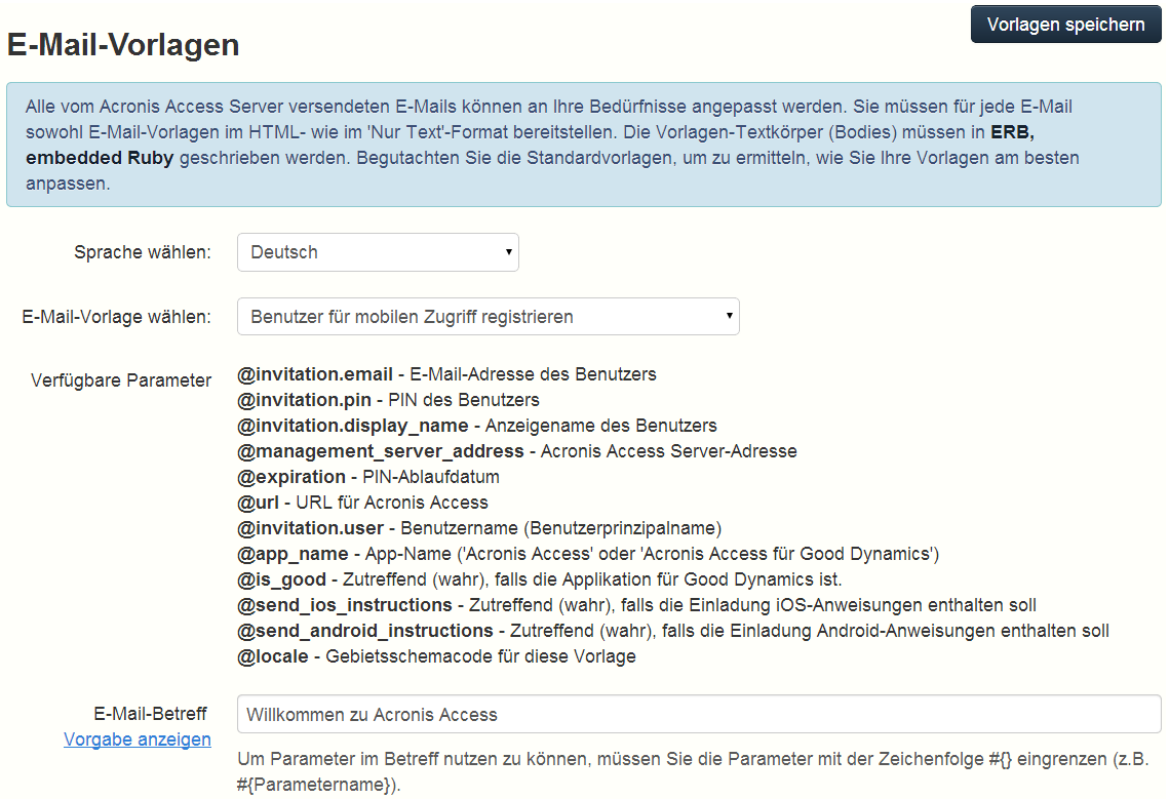
- **Sprache wählen** – Wählen Sie die Standardsprache für Einladungs-E-Mails.

  ***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.*

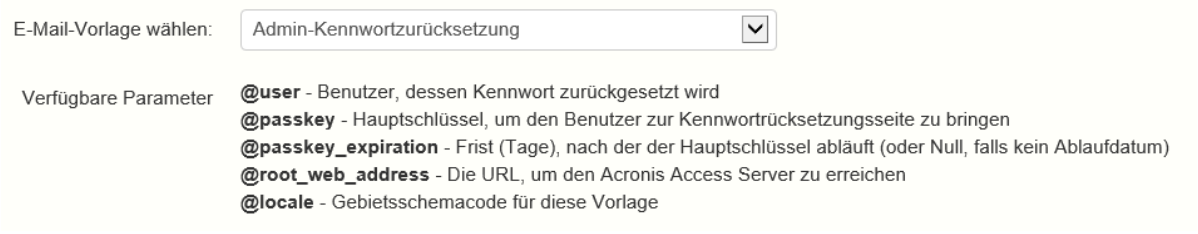
- **E-Mail-Vorlage wählen** – wählen Sie die Vorlage aus, die Sie anzeigen bzw. bearbeiten möchten. Jede der Vorlagen dient einem bestimmten Zweck (z.B. einen Benutzer für mobilen Zugriff registrieren, das Kennwort eines Benutzers zurücksetzen).
- **Verfügbare Parameter** – welche Parameter verfügbar 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.

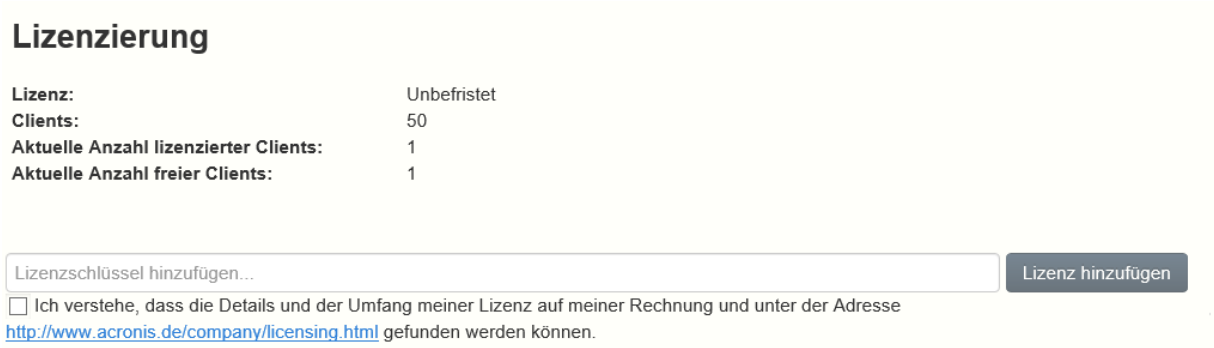


Hinweis: *Wenn Sie auf* ***Vorgabe anzeigen*** *drücken, wird die Standardvorlage angezeigt.*

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

9.8 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**.

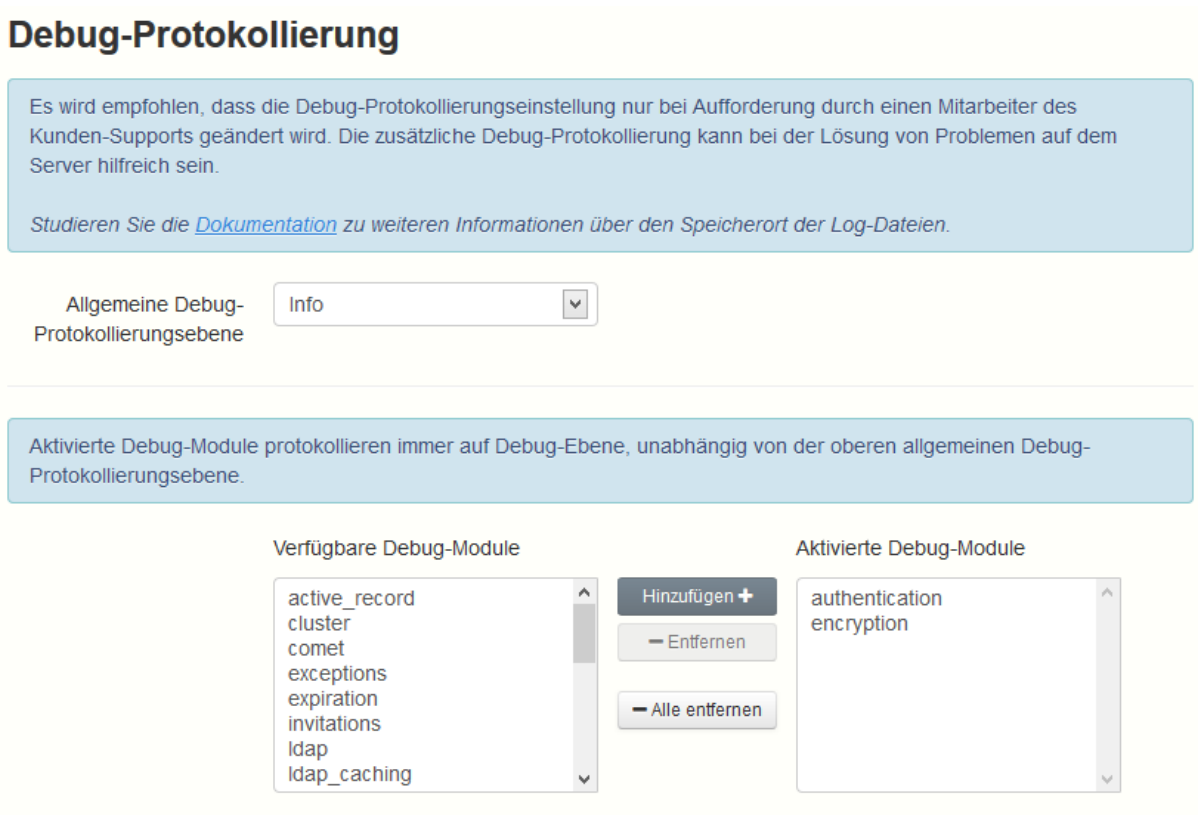
Hinweis: *Die unterstützte Anzahl an lizenzierten Clients beträgt 50 und 100. Wenn Sie eine Benutzerlizenz mit 50 erworben haben, können Sie ein Upgrade auf 100 durchführen.*

Hinweis: *Sie können für Ihre Instanz von Acronis Access ein Upgrade auf Acronis Access Advanced durchführen, indem Sie einen Acronis Access Advanced Lizenzschlüssel verwenden. Alle Ihre aktuellen Einstellungen und Konfigurationen werden gespeichert.*

9.9 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. 49).*



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.*

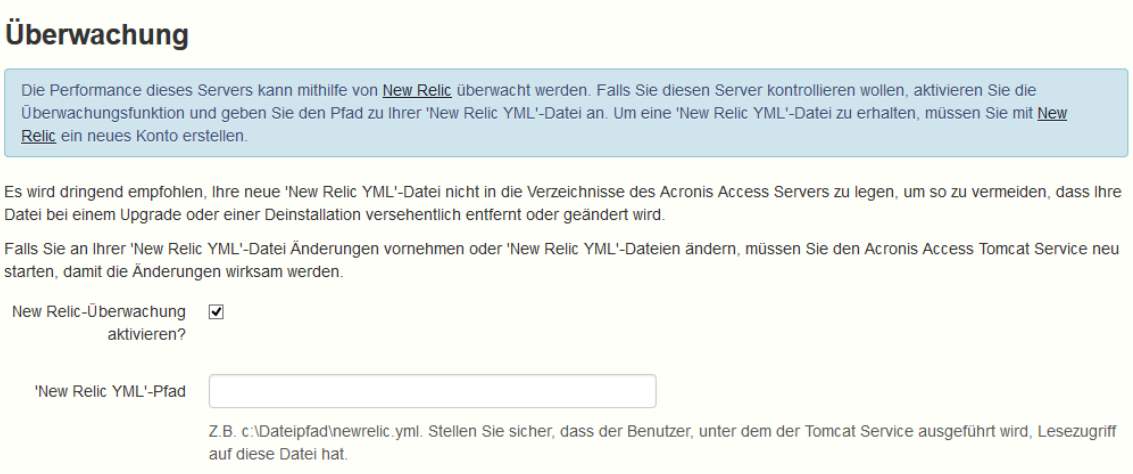
- **Verfügbare Debug-Module** – zeigt eine Liste der verfügbaren Module an.
- **Aktivierte Debug-Module** – Zeigt die aktiven Module an.

Hinweis: *Falls es sich bei dem Produkt um ein Update 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 sich die Log-Dateien im Ordner* ***C:\Programme (x86)\Acronis\Access\Common\apache-tomcat-7.0.42\logs***

9.10 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.

10 Ergänzendes Material

Themen

In Konflikt stehende Software....107
Vertrauenswürdige Server-Zertifikate mit Acronis Access verwenden....107
Acronis Access Tomcat SSL-Codierschlüssel ändern....110
So unterstützen Sie verschiedene Access Desktop Client-Versionen....110
Weboberfläche anpassen....111
Ablageordner erstellen....112
Acronis Access mit New Relic überwachen....113
Drittanbietersoftware für Acronis Access....114

10.1 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.

10.2 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.*

Eine Zertifikatanforderung erstellen

Hinweis: *Das Erstellen von Zertifikaten ist weder aktuell noch zukünftig eine Funktion von Acronis Access. Diese Zertifikatanforderung ist für den Einsatz von Acronis Access nicht zwingend notwendig, wird von Zertifikatanbietern jedoch vorausgesetzt.*

Eine Zertifikatanforderung mit IIS erzeugen:

Weitere Informationen zu diesem Verfahren finden Sie im folgenden Microsoft Knowledge Base-Artikel: http://technet.microsoft.com/de-de/library/cc732906(v=ws.10).aspx

Eine Zertifikatanforderung mit OpenSSL erzeugen:

Hinweis: *Für diese Anleitung muss OpenSSL installiert sein.*

Hinweis: *Weitere Informationen und Hilfe zu diesem Verfahren erhalten Sie bei Ihrem bevorzugten Zertifikatanbieter.*

So erzeugen Sie ein Schlüsselpaar für den Webserver "AAServer", das aus einem privaten Schlüssel und einem öffentlichen Certificate Signing Request (CSR) besteht:

1. Öffnen Sie eine Eingabeaufforderung mit erhöhten Benutzerrechten und geben Sie den folgenden Befehl ein:

```
openssl req -new -nodes -keyout myserver.key -out AAServer.csr -newkey rsa:2048
```

   Daraufhin werden zwei Dateien erstellt. Die Datei **myserver.key** enthält einen privaten Schlüssel. Legen Sie diese Datei nicht gegenüber Dritten offen. Sie sollten eine Sicherungskopie des privaten Schlüssels erstellen, da dieser bei Verlust nicht wiederhergestellt werden kann. Der private Schlüssel wird als Eingabe zum Erzeugen eines **Certificate Signing Request (CSR)** verwendet.

   Hinweis: *Wenn die Fehlermeldung **WARNUNG: Konfigurationsdatei kann nicht geöffnet werden: /usr/local/ssl/openssl.cnf** angezeigt wird, führen Sie den folgenden Befehl aus: **set OPENSSL_CONF=C:\OpenSSL-Win64\bin\openssl.cfg**. Geben Sie dabei den OpenSSL-Installationspfad an. Nachdem Sie dieses Verfahren abgeschlossen haben, führen Sie Schritt 1 erneut aus.*

2. Dabei werden Sie aufgefordert, die erforderlichen Details in Ihr CSR einzugeben. Verwenden Sie den Namen des Webservers als **Common Name (CN)**. Lautet der Domänen-Name **mydomain.com**, hängen Sie die Domäne an den Hostnamen an (verwenden Sie dabei den vollständig qualifizierten Domänen-Namen).
3. Die Felder für E-Mail-Adresse, optionaler Firmenname und Kennwort-Sicherheitsabfrage dürfen für ein Webserver-Zertifikat leer bleiben.
4. Ihr CSR wurde nun erstellt. Öffnen Sie die Datei **server.csr** in einem Texteditor und kopieren Sie den Inhalt, um ihn auf Anforderung des Zertifikatanbieters in das Online-Registrierungsformular einzufügen.

Zertifikat im Windows-Zertifikatspeicher installieren

Voraussetzungen

Das verwendete Zertifikat muss seinen privaten Schlüssel enthalten. Das Zertifikat muss entweder im **.PFX**- oder im **.P12** -Format vorliegen.

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.

10.3 Acronis Access Tomcat SSL-Codierschlüssel ändern

Codierschlüssel ändern:

Dieses Verfahren ist nur dann notwendig, wenn Sie mit einem benutzerdefinierten Satz an SSL-Codierschlüsseln arbeiten möchten. Dies kann erforderlich sein, um die Webschnittstelle in Internet Explorer 8 oder den Acronis Access Desktop Client unter Windows XP zu unterstützen, ist jedoch nicht empfehlenswert. Änderungen der Codierschlüssel können Ihren Server angreifbar machen und sind grundsätzlich unsicher.

1. Navigieren Sie zum Tomcat-Installationsordner von Acronis Access (z.B. **`C:\Program Files (x86)\Acronis\Access\Common\apache-tomcat-7.0.55\conf`**).
2. Erstellen Sie eine Kopie der Datei **`server.xml`**, bevor Sie sie bearbeiten.
3. Öffnen Sie die Datei **`server.xml`**.
4. Suchen Sie die folgende Zeile: **`SSLCipherSuite`**=""
5. Ersetzen Sie den Inhalt zwischen den beiden Anführungszeichen durch Ihren bevorzugten Codierschlüssel.

   Hinweis: *Möchten Sie eine unsichere Version von Internet Explorer 8 oder den Acronis Access Desktop Client unter Windows XP unterstützen, geben Sie Folgendes ein:*

   `ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM`

   z. B.:
   `SSLCipherSuite="ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM"`
6. Speichern Sie die an der Datei **`server.xml`** vorgenommenen Änderungen. Starten Sie den Acronis Access Tomcat-Dienst anschließend neu.

10.4 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\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* ***\Acronis\Access\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****').*

10.5 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. Drücken 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. 96).
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. Drücken Sie auf **Speichern**.

10.6 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. 33).
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.

10.7 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.

10.8 Drittanbietersoftware für Acronis Access

Themen

PostgreSQL 114
Apache Tomcat 115
New Relic 115

10.8.1 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.

10.8.2 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.

10.8.3 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. 113).

11 Sync & Share

Themen

Freigabebeschränkungen 116
LDAP-Bereitstellung 116
Quotas 117
Dateibereinigungsrichtlinien 118
Benutzerablaufrichtlinien 119
Datei-Repository 120
Acronis Access-Client 121

11.1 Freigabebeschränkungen

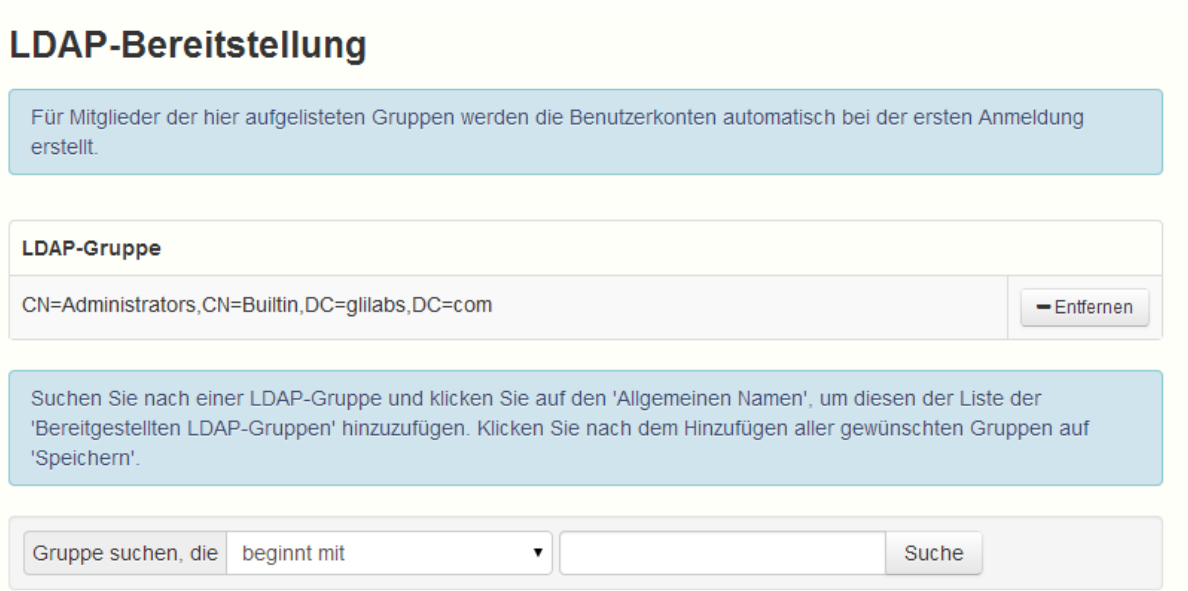
Einladen von Teilnehmern zulassen – Wenn diese Einstellung deaktiviert ist, wird das Kontrollkästchen **Teilnehmern erlauben, andere Teilnehmer einzuladen** nicht angezeigt, wenn Benutzer zu Ordnern eingeladen werden. Dadurch wird verhindert, dass Benutzer andere Benutzer einladen können.

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.

11.2 LDAP-Bereitstellung



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

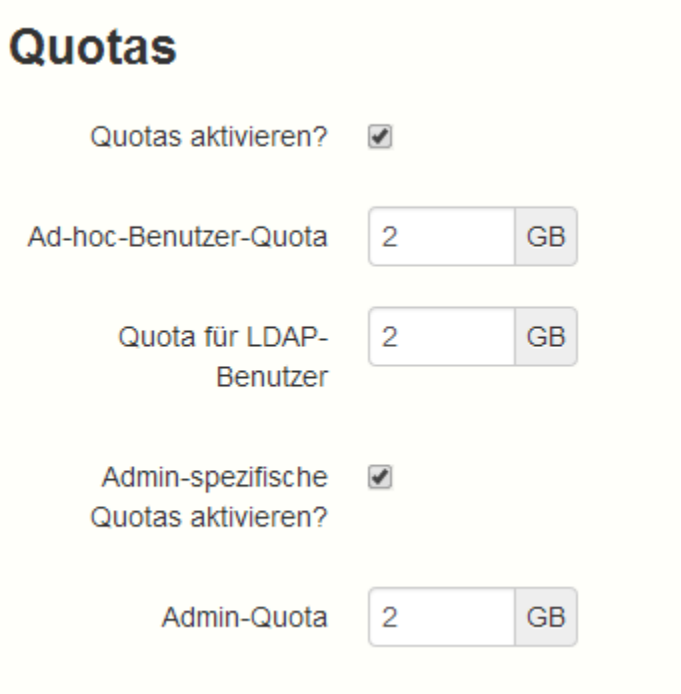
LDAP-Gruppe

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.

11.3 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.

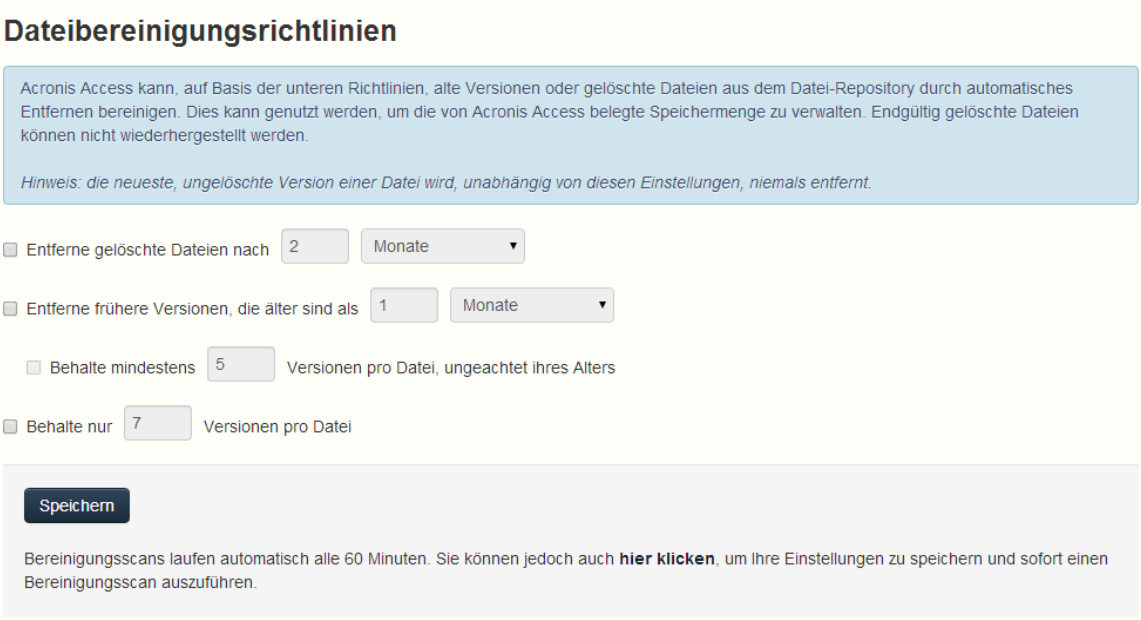
- **Quotas aktivieren?** – Wenn diese Option aktiviert ist, wird der maximale Speicherplatz, der einem Benutzer zur Verfügung steht, durch ein Kontingent beschränkt.
  - **Ad-hoc-Benutzer-Quota** – legt das Kontingent für Ad-hoc-Benutzer fest.
  - **LDAP-Benutzer-Quota** – legt das Kontingent für LDAP-Benutzer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

11.4 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.

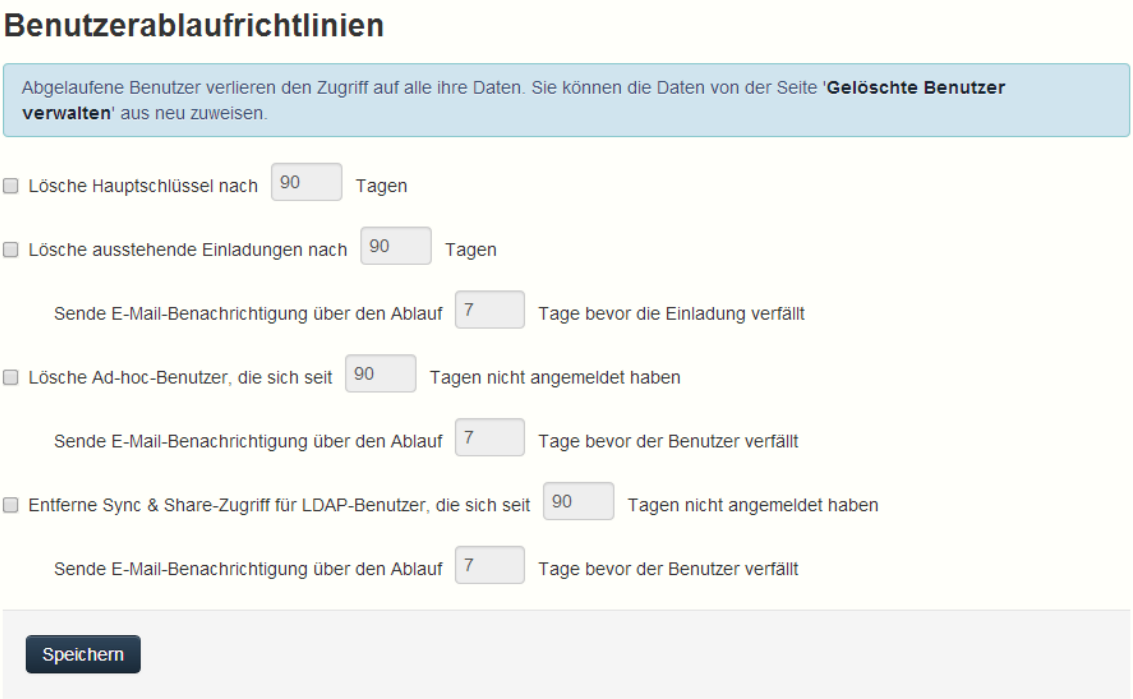
Hinweis: *Die neueste, ungelöschte Version einer Datei wird, unabhängig von diesen Einstellungen, niemals entfernt.*

- **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.*

11.5 Benutzerablaufrichtlinien

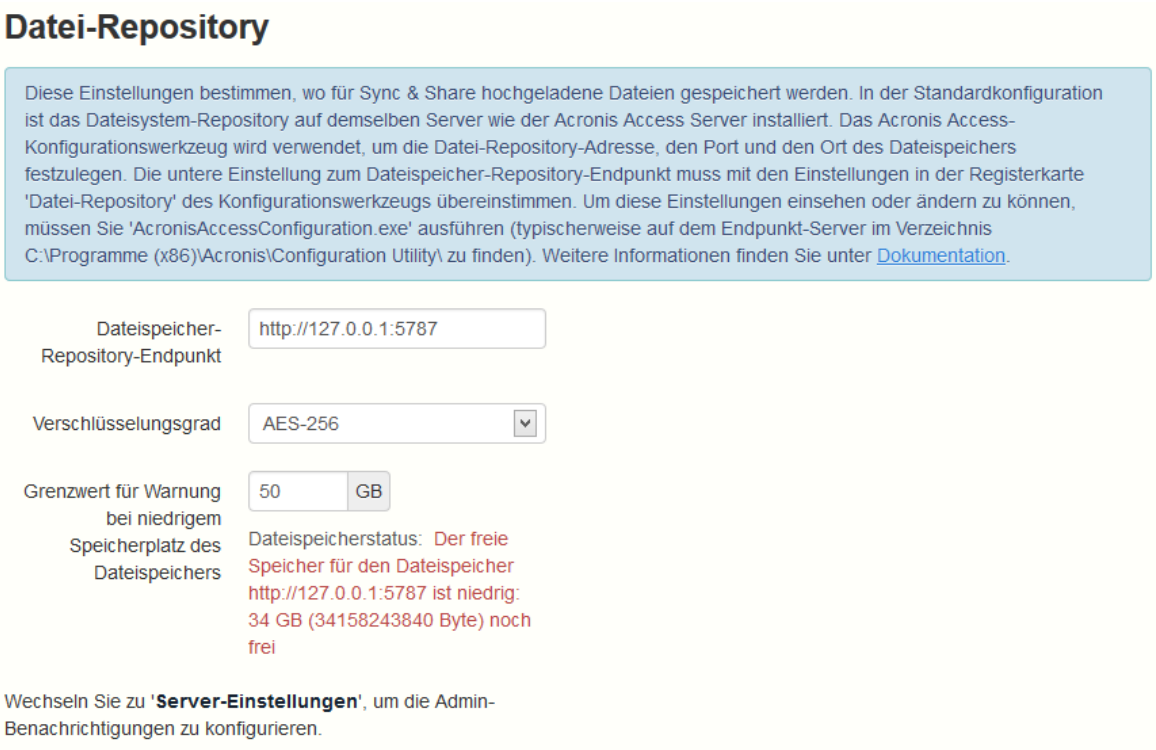
Benutzer, die ablaufen, verlieren den Zugriff auf alle ihre Daten. Sie können die Daten auf der Seite **Gelöschte Benutzer verwalten** neu zuweisen.



- **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.

11.6 Datei-Repository

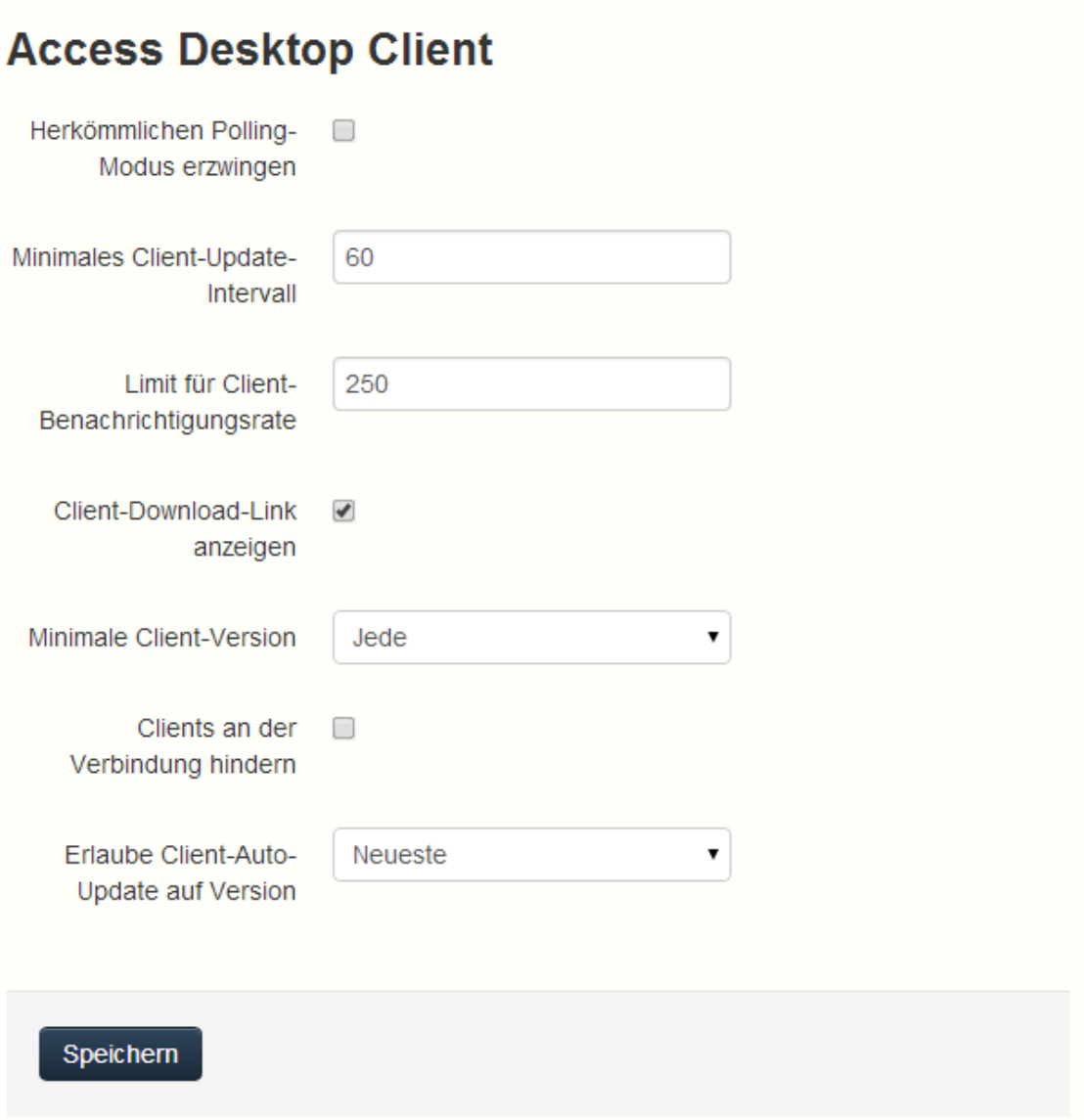
Diese Einstellungen bestimmen, wo für Sync & Share hochgeladene Dateien gespeichert werden. Das Dateisystem-Repository ist auf demselben Server wie der Acronis Access Server installiert. Im Datei-Repository werden Acronis Access Sync & Share-Dateien und frühere Versionen gespeichert. Mit dem Acronis 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).



- **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 sind 'Ohne', 'AES-128' und 'AES-256'. Der Standard ist 'AES-128'.
- **Grenzwert für Warnung bei niedrigem Speicherplatz des Dateispeichers** – unterschreitet der freie Speicherplatz diesen Schwellenwert, erhält der Administrator eine entsprechende Warnung.

11.7 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.

12 Upgrades

Themen

Upgrade von Acronis Access auf eine neuere Version 123

12.1 Upgrade von Acronis Access auf eine neuere Version

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

Hinweis: *Dieser Vorgang kann nur für Versionen verwendet werden, die neuer als Acronis Access 7.0 sind.*

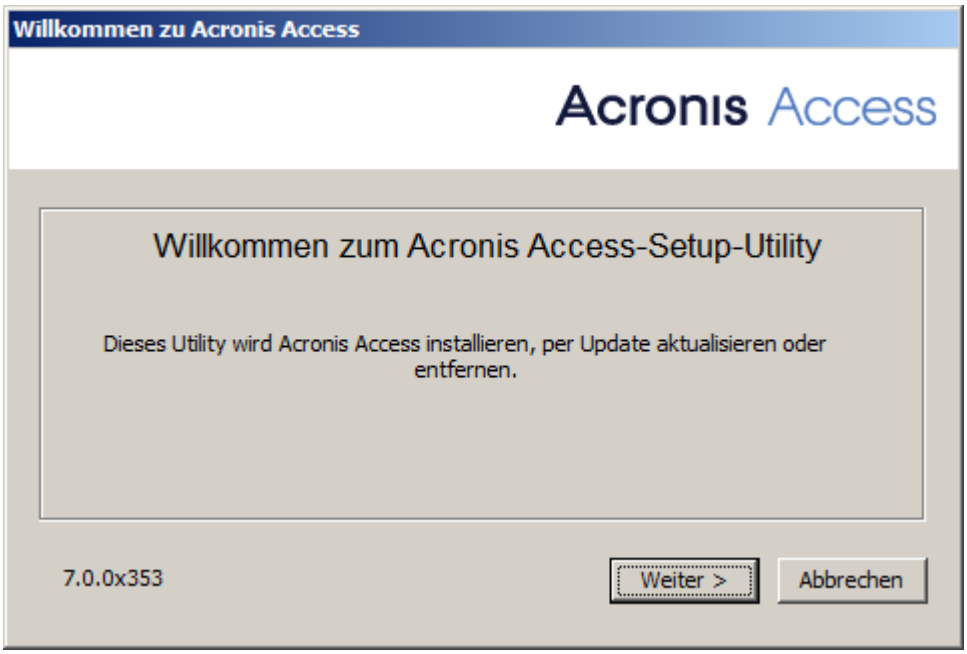
Benutzer, die ein Upgrade von Versionen durchführen, die älter als Acronis Access 7.0 sind, sollten ein Upgrade auf Acronis Access Advanced durchführen. Weitere Informationen finden Sie in der Dokumentation zu Acronis Access Advanced.

Apache Tomcat-Ordner per Backup sichern

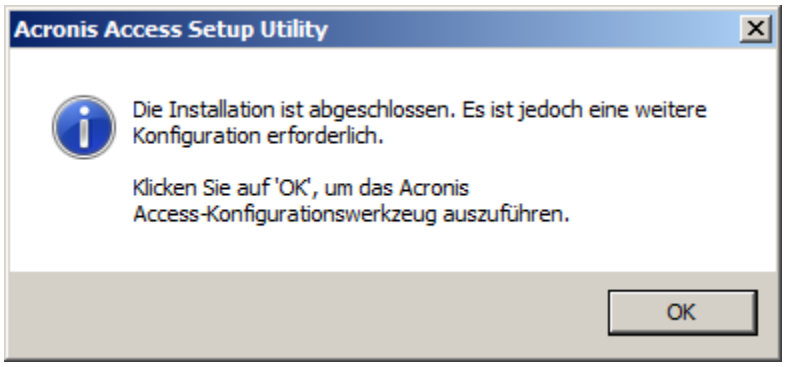
Beim Upgrade wird möglicherweise ein Upgrade für Apache Tomcat und für alle aktuellen Tomcat-Konfigurationsdateien durchgeführt und die Protokolldateien werden entfernt. Es empfiehlt sich, eine Kopie des Apache Tomcat-Ordners anzulegen. Dieser befindet sich standardmäßig hier: **C:\Programme (x86)\Acronis\Access\Common**.

Upgrade

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



3. Klicken Sie auf **Weiter**, um zu beginnen.
4. Lesen und akzeptieren Sie die Lizenzvereinbarung.
5. Drücken Sie **Upgrade**.
6. Überprüfen Sie die zur Installation ausgewählten Komponenten und klicken Sie auf **Installieren**.
7. Prüfen Sie die installierten Komponenten, und schließen Sie den Installer.
8. Wenn Sie aufgefordert werden, das Konfigurationswerkzeug zu öffnen, drücken Sie **OK**.



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

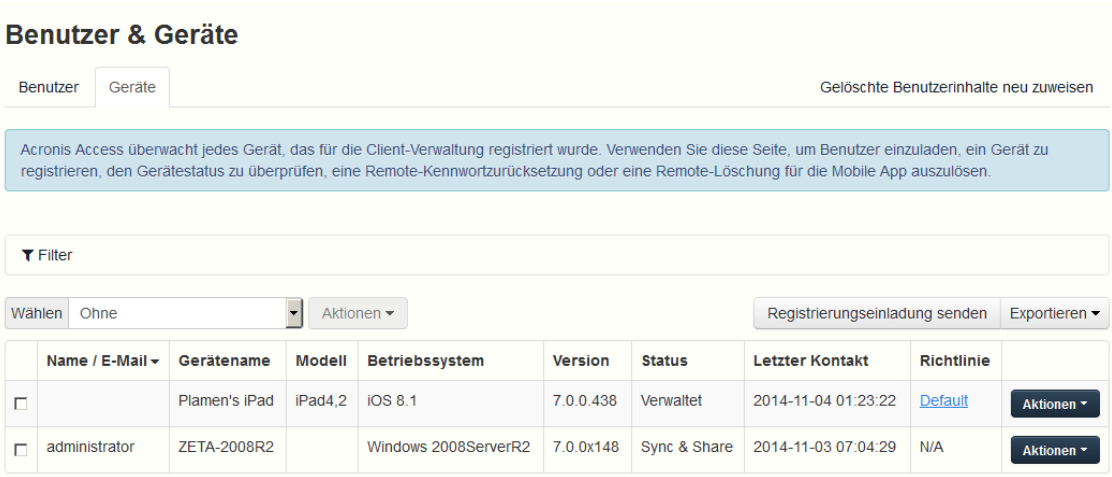
13 Benutzer und Geräte

Themen

Mobile Geräte verwalten 125
Benutzer verwalten 128

13.1 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 enthält detaillierte Statusinformationen für jedes verwaltete Gerät. Sie können das Gerät auch löschen oder das Kennwort seiner App ändern.



- **Wählen**
  - **Alle** – wählt alle Einträge aus.
  - **Keine** – wählt alle Einträge ab.
  - **Aktionen** – führt die ausgewählte Aktion für alle ausgewählten Einträge aus. Die verfügbaren Aktionen sind **Remote-Löschung**, **Remote-Löschung abbrechen** (diese haben keine Auswirkungen auf Sync & Share-Benutzer) und **Aus Liste entfernen**.
- **Name/E-Mail** – Anzeigename oder E-Mail-Adresse des Benutzers.
- **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** – der Status der Registrierung 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 Access 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

Kennwort-Resets für die Remote-Applikation durchführen 126
Remote-Löschungen durchführen 127

13.1.1 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.

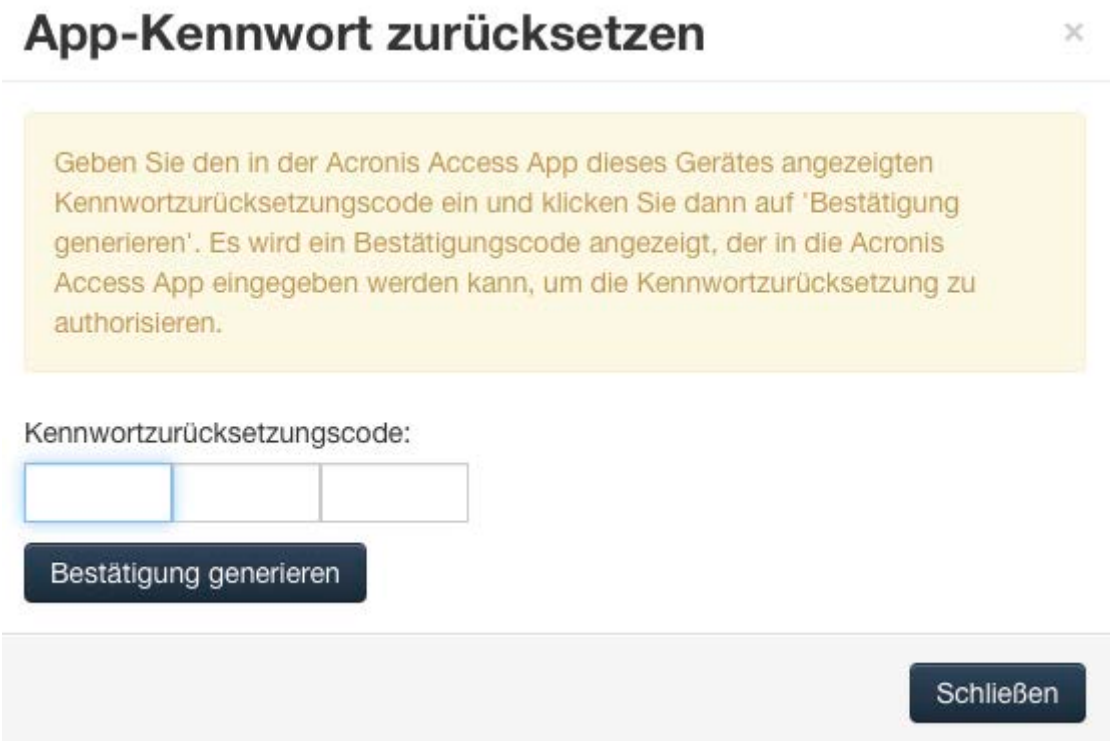
Kennwort für die Applikation zurücksetzen

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 Acronis Access Clients das Kennwort zum Sperren der Applikation über Datenfunk (Over the Air) nicht zurückzusetzen können. 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. Öffnen Sie die Registerkarte **Benutzer und Geräte**.

3. Rufen Sie die Registerkarte **Geräte** auf.
4. Suchen Sie nach dem Gerät, dessen Kennwort zurückgesetzt werden soll, und klicken Sie auf die Schaltfläche **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.



13.1.2 Remote-Löschungen durchführen

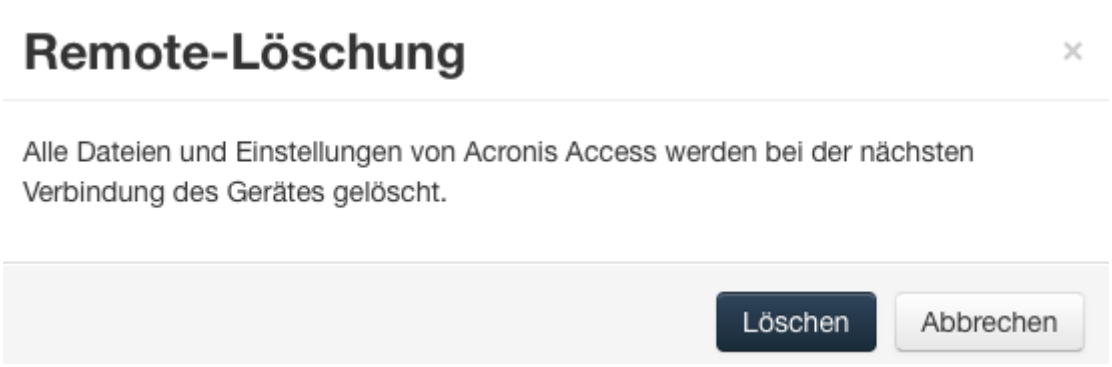
Mit Acronis Access kann eine Remote-Löschung einer Access Mobile Client-Applikation durchgeführt werden. Bei dieser selektiven Remote-Löschung werden alle in der Acronis Access-App lokal gespeicherten oder zwischengespeicherten Dateien entfernt. Alle App-Einstellungen werden auf die vorherigen Standardeinstellungen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

Remote-Löschvorgang in Warteschlange stellen

1. Öffnen Sie die Registerkarte **Mobiler Zugriff**.
2. Öffnen Sie die Registerkarte **Benutzer und Geräte**.
3. Suchen Sie nach dem Gerät, für das eine Remote-Löschung durchgeführt werden soll, und klicken Sie auf 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

Acronis Access Clients benötigen Netzwerkzugriff auf den Acronis Access 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 erhält, so wird diese Verbindung zum VPN auch benötigt, bevor Verwaltungsbefehle akzeptiert werden.

13.2 Benutzer verwalten

Über diesen Bereich können Sie alle Benutzer verwalten. Sie können über die Schaltfläche **Sync- & Share-Benutzer hinzufügen** neue Benutzer einladen oder über die Schaltfläche **Aktionen** aktuelle 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. 116) 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. 92).

- **Name** – zeigt den Namen an, mit dem sich der Benutzer beim Server anmeldet.
- **E-Mail** – Zeigt die E-Mail-Adresse des Benutzers an.
- **Richtlinie** – Zeigt die aktuell von dem Benutzer verwendete mobile Richtlinie an. Wenn der Benutzer sich nicht im Client Management registriert hat, zeigt die Registerkarte **Richtlinie** den Eintrag **Nicht aufgelöst** an.
- **Sync & Share**
  - **Status** – Zeigt den von dem Benutzer verwendeten Lizenztyp an.
  - **Verwendung** – Zeigt die Anzahl der Ordner und Dateien sowie die Gesamtgröße der Inhalte des Benutzers an.
- **Letzte Anmeldung** – Datum und Uhrzeit der letzten Anmeldung.
- **Aktionen**
  - **Weitere Informationen** – Zeigt zusätzliche Informationen zu dem Benutzer an.
  - **Geräte anzeigen** – Zeigt Informationen zu den von dem Benutzer verwendeten Geräten an.
  - **Sync & Share-Kennwort zurücksetzen** – Sendet eine E-Mail für die Kennwortzurücksetzung.
  - **Zu 'Lizenziert' konvertieren** – Konvertiert einen freien Benutzer zu einem lizenzierten Benutzer. Hierzu wird 1 Lizenz verwendet.
  - **Benutzer bearbeiten** – Erlaubt das Bearbeiten dieses Benutzers.
  - **Löschen** – der Benutzer wird gelöscht.

Hinzufügen eines Ad-hoc-Benutzers

1. Rufen Sie die Acronis Access-Weboberfläche auf.
2. Melden Sie sich mit einem Administratorkonto an.

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 Link. Sobald er den Link öffnet, wird er aufgefordert, einen Namen und ein Kennwort festzulegen, und sein Konto ist erstellt. Name und Kennwort können nach der erfolgreichen Anmeldung durch den Benutzer geändert werden.

Hinzufügen eines LDAP-Benutzers

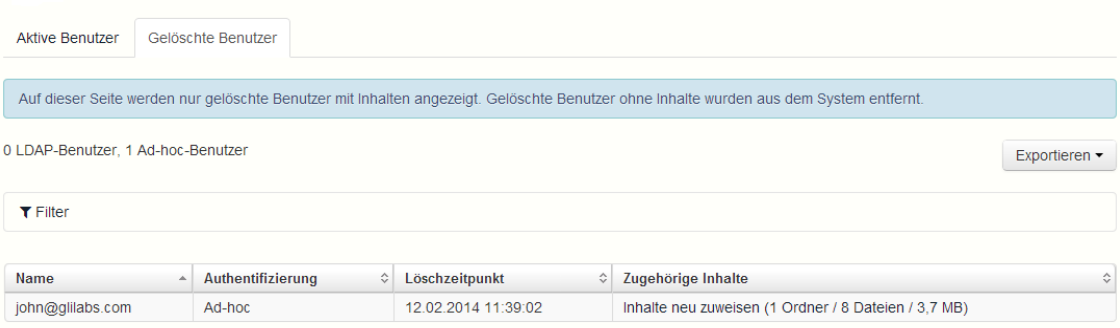
1. Rufen Sie die Acronis Access-Weboberfläche auf.
2. Melden Sie sich mit einem Administratorkonto an.
3. Öffnen Sie die Registerkarte **Sync & Share**.
4. Öffnen Sie die Registerkarte **Benutzer**.
5. Drücken Sie **Benutzer hinzufügen**.
6. Geben Sie die E-Mail-Adresse des Benutzers ein.
7. Geben Sie 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. Seine Kontoerstellung ist abgeschlossen, sobald er sich anmeldet.

Hinweis: *Wenn Sie LDAP aktiviert und eine LDAP-Administratorgruppe bereitgestellt haben, können Benutzer sich in dieser LDAP-Gruppe direkt mit ihren LDAP-Anmeldedaten anmelden und haben alle Administratorrechte.*

Inhalte neu zuweisen

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.

14 Neuerungen

Themen

Neuerungen in Acronis Access Server 132
Neuerungen in der Acronis Access-App..... 149

14.1 Neuerungen in Acronis Access Server

Hinweis: *Zahlen wie "[DE1013, US552, #2717]" beziehen sich auf das interne Änderungsnachverfolgungssystem von Acronis.*

Hinweis: *Zahlen wie "[7.0.1x18]" weisen auf den konkreten Build hin, in dem eine Änderung eingeführt wurde.*

Acronis Access 7.0.1

VERBESSERUNGEN:

- Verschiedene Optimierungen der Webclient-Oberfläche.
- Acronis Access Server und Acronis Access Desktop Clients für Mac und PC sind nun in russischer Sprache verfügbar.
- Apache Tomcat 7.0.57 wird mit dieser Version verwendet (DE11653).
- In dieser Version wird Java 7 Update 71 verwendet.
- Die zulässige Mindestablaufzeit für freigegebene Links zum Datei-Download beträgt standardmäßig mindestens einen Tag für Neuinstallationen von Acronis Access Server. Bisher betrug die Mindestablaufzeit für Links 30 Tage. (DE13079).
- Das Durchsuchen von Netzwerkdatenquellen mit dem Webclient wurde für Ordner mit zahlreichen Elementen verbessert (DE13056).
- Verbesserungen beim Konfliktlösungsverhalten.

BUG-FIXES:

- Durchgängige Verwendung des „¥“-Symbols für die Protokollierung in Access Server Web Client (DE13031).
- Die Aktualisierung auf Acronis Access 7.0.1 von mobilEcho 4.5 wird nun unterstützt. (DE12984).
- Feste Verknüpfung mit dem Acronis Access Tomcat-Servicekonfigurationstool im Startmenü nach der Aktualisierung von Acronis Access 6.1 (DE12966).
- Für freigegebene Ordner werden jetzt Benachrichtigungen im rechten Menü angezeigt (DE12948).
- Nutzen einige Ihrer Endbenutzer Internet Explorer 8, empfiehlt sich möglicherweise eine Aktualisierung auf einen sichereren Browser. Administratoren können die SSL-Bindungen ändern, um Internet Explorer 8-Benutzer mit den folgenden Einschränkungen zu unterstützen (DE12649):
  - Benutzer mit Internet Explorer 8 werden automatisch zur Access 6 Style Webclient-Oberfläche umgeleitet.
  - Internet Explorer 8 wird von der neu designten Access 7 Weboberfläche nicht unterstützt.

- Die Benutzer haben über die Webclient-Oberfläche keinen Zugriff auf Dateiserver, NAS- und SharePoint-Datenquellen.
- Internet Explorer 8 wird zur Server-Administration nicht unterstützt.

- Von Zeit zu Zeit auftretende Abstürze in Access Desktop Client für Mac wurden behoben (DE12879).

BEKANNTE PROBLEME:

- Bei der Verwendung einer Access Gateway Server mit einem Port könnte ein Problem mit der Verarbeitung von Pfaden mit mehr als 256 Zeichen auftreten.

  Hinweise zum Beheben dieses Problems finden Sie im folgenden KB-Artikel (DE12405): http://support.microsoft.com/kb/820129

Acronis Access 7.0

VERBESSERUNGEN

- Neu designte und verbesserte Access Webclient-Benutzeroberfläche.
- **Acronis Access** heißt jetzt **Acronis Access Advanced** und ist der Upgradepfad auf Acronis Access 6 oder früher für vorhandene Benutzer. Es wurde ebenfalls eine neue, auf kleine und mittlere Unternehmen zugeschnittene Version mit einfacheren Anforderungen eingeführt. Die neue Version heißt Acronis Access.
- Während der Neuinstallation versucht der Konfigurationsassistent jetzt, Systemkonfigurationsoptionen, wie SMTP-Server und AC- (LDAP-)Server, zu erkennen.
- Acronis Access und Acronis Access Advanced können jetzt während der Installation so konfiguriert werden, dass sie einen einzigen offenen Port für Clientverbindungen nutzen. Bei dieser Konfiguration verwenden alle Access Clients (mobile App, Desktop Sync Client, Webclient-Oberfläche) dieselbe Netzwerkadresse und denselben Port für die Verbindung mit dem Access Server.
- Ordner und Dateien auf den Dateiservern, NAS- und SharePoint-Servern können jetzt durchsucht werden, und der Zugriff ist über die Access Webclient-Oberfläche möglich. Diese Funktion kann auf Benutzer- oder Gruppenebene aktiviert bzw. deaktiviert werden.
- Aktualisiertes grafisches Design von Standard-E-Mail-Vorlagen. Neu designte Benachrichtigungs- und Einladungs-E-Mail-Vorlagen.
- Die Verwaltungsseite für Benutzer und die Verwaltungsseite für Geräte sind jetzt in einer einzigen Admin-Konsolen-Seite zusammengeführt.
- Der Zugriff bietet jetzt eine Konfliktlösung für Sync & Share-Dateien und -Ordner. Falls sich Dateiänderungen von Benutzern überlappen und in Konflikt treten, werden diese Konflikt verursachenden Dateien mit dem Namen des Benutzer und dem aktuellen Datum umbenannt, so dass die Konflikt verursachende Datei offenkundig wird und nach Bedarf behandelt werden kann. Vor Access 7.0 wurden solche Konflikt verursachenden Dateien als neue Versionen abgespeichert.
- Sync & Share-Dateien können jetzt zwischen Sync & Share-Ordnern über die Webclient-Oberfläche kopiert werden.
- Download-Links für Sync & Share-Dateien können jetzt für eine Verwendung generiert werden, ohne dass einen E-Mail vom Access-Server gesendet werden muss. Die Option eines Datei-Download-Links kann aktiviert bzw. deaktiviert werden.

- Benutzernamen können jetzt externen Ad-hoc-Benutzern zugewiesen werden. Alle Sync & Share-Benutzer werden in der Regel durch Benutzernamen identifiziert, und nicht durch E-Mail-Adressen.
- Die Access Client-Version wird jetzt im Bereich für Benutzer und Geräte auf der Access Server-Admin-Seite angezeigt. (US8696)
- Java Version 7 U71 wird mit diesem Release verwendet. (US9486)
- Verbesserte Überwachungsprotokollierung, wenn Dateien aus dem direkten Download-Link heruntergeladen werden. (DE10961)
- Ein Sortieren von Dateien nach Typ ist jetzt in der Webclient-Oberfläche möglich. (US6836)
- Postgres kann jetzt über die Systemsteuerung "Programme hinzufügen/entfernen" entfernt werden. (US8270)
- Es gibt jetzt eine neue globale Einstellung, die die Möglichkeit deaktiviert, Dateien über den direkten Download-Link freizugeben. (US8347)
- Die standardmäßige Schwelle und das Intervall für die Benutzerbenachrichtigung können jetzt bei Annäherung an die Quota für Sync & Share konfiguriert werden. (US8605)
- Apache Tomcat 7.0.56 wird mit diesem Release verwendet. (US9801)
- OepnSSL Version 1.0.1 wird mit diesem Release verwendet. (DE11653)
- Zusätzlicher Support für Batch-Aktionen in der Tabelle "Geräte" (Remote-Löschung, Remote-Löschung abbrechen usw.). (US8875)

BUG-FIXES

- Es wurde ein PostgreSQL-Installationsfehler behoben, welcher auftreten kann, wenn eine lokale Benutzergruppe über nicht genügend Berechtigungen verfügt.
- Es wurde ein Problem mit LDAP-Abfragen behoben, das bei aktivierter Debug-Protokollierung gelegentlich zu einem Fehler bei einigen der UTF-8-Benutzernamen führen konnte.
- Die Verwendung der Variable @display_name für die Einladungs-E-Mails zu Acronis Access wurde verbessert.

BEKANNTE PROBLEME

- Internet Explorer 8 wird in der Erstversion des Acronis Access 7.0 Web-Clients nicht unterstützt. IE8-Benutzer sind nicht in der Lage, sich am Acronis Access Web-Client anzumelden. Es wird erwartet, dass die Unterstützung für IE8 in einem späteren Release wieder aufgenommen wird, auch wenn für die IE8-Benutzer in dem späteren Release die vorherige Weboberfläche von Access 6 bereitgestellt wird und sie die neuen Funktionen von Access 7 nicht werden nutzen können. Wenn Sie Endbenutzer unter dem Internet Explorer 8 betreiben, sollten Sie ein Upgrade auf einen sichereren Browser in Erwägung ziehen oder warten, bis eine Unterstützung mit dem bevorstehenden Access Server-Update hinzugefügt wird. (DE12649)
- Windows XP-Benutzer sind nicht in der Lage, den Acronis Desktop Sync-Client oder den Web-Client zu verwenden, nachdem ein Upgrade des Access Servers auf 7.0 oder höher durchgeführt wurde. Dies ist auf eine Inkompatibilität von XP und IE8 mit den sicheren SSL-Bindungen zurückzuführen, welche der Access Server aktuell verwendet. Zur Unterstützung von XP-Benutzern können Administratoren die SSL-Bindungen ändern. Details finden Sie hier: Acronis Access Tomcat SSL-Codierschlüssel ändern (S. 110). Beachten Sie, dass Änderungen an diesen Codierschlüsseln Ihren Server angreifbar machen können und daher grundsätzlich unsicher sind.

- Windows Server 2003 wird nicht mehr unterstützt. (US9572)
- Für Benutzer des Access servers werden Netzwerkordner für einen mobilen Zugriff auf der Webclient-Oberfläche nicht angezeigt. Diese Funktion wird in einem späteren Release unterstützt werden. (US9733)
- Hat der Benutzer mehrere Dateien für den Upload ausgewählt, werden diese nacheinander, nicht gleichzeitig hochgeladen. (DE12512)
- Ein- und Auschecken bei SharePoint wird auf der Webclient-Oberfläche noch nicht unterstützt. Diese Funktion wird in einem späteren Release unterstützt werden. (US8282)

Ein Upgrade von mobilEcho 4.5 wird in der Erstversion von Acronis Access 7.0 nicht unterstützt. Es ist zu erwarten, dass die Unterstützung für ein Upgrade von mobilEcho 4.5 in einem späteren Release wieder aufgenommen wird. (DE12971)

Acronis Access 6.1.3

VERBESSERUNGEN

- Die Standard-SSL-Bindungen von Acronis Access unterstützen keine Internet Explorer 8-Client-Verbindungen mehr. Hinweise zur Aktivierung von unsicheren Internet Explorer 8-Verbindungen in einer neuen Installation finden Sie im folgenden Artikel: Acronis Access Tomcat SSL-Codierschlüssel ändern (S. 110). (US8460)
- New Relic-Agent auf Version 3.9.0.229 aktualisiert. New Relic kann erst nach einem Upgrade auf diese Version wieder verwendet werden.
- Leistungsoptimierungen in Access Server zum Umgang mit einer großen Zahl von selbst bereitgestellten Ordnern. (DE11452)
- Verbesserte Web UI-Anmeldung mit einem Link zu einem Knowledge Base-Artikel, falls Java Cryptography Extensions nicht korrekt installiert sind. Details finden Sie unter https://kb.acronis.com/content/47618. (US9226)
- Acronis Access Client für Mac unterstützt nun auch Mac OS X 10.9.5. (US9249)
- Das Installationsprogramm umfasst Java Version 7 Update 51.
- Apache Tomcat aktualisiert auf 7.0.55. (US9392)

BUG-FIXES

- Es wurde ein Problem mit LDAP-Abfragen behoben, das bei aktivierter Debug-Protokollierung zu einem Fehler bei der Bereitstellung von Benutzern führen konnte. (DE11545)
- Bei der Installation bzw. beim Upgrade werden unabhängig von der Java-Version immer die Java Cryptography Extension-Dateien installiert. Auf diese Weise wird dafür gesorgt, dass immer die richtigen JCE-Bibliotheken verwendet werden, auch wenn eine höhere Java-Version als 7.0.51 auf dem System installiert ist. (DE11219)

Acronis Access 6.1.2

VERBESSERUNGEN

- Es wurde ein Problem behoben, das beim Hochladen großer Dateien über die Access-Web-Client-Oberfläche auftreten kann.

- "Die Option "**Exakte Übereinstimmung erforderlich**" wurde zur Liste "**Domains für LDAP-Authentifizierung**" hinzugefügt. Wenn E-Mails mit Accesss-Freigabeeinladungen an Benutzer gesendet werden, deren E-Mail-Adressen-Domäne mit den in der Einstellung '**Domains für LDAP-Authentifizierung**' aufgelisteten Domänen übereinstimmt, werden diese angewiesen, sich mit ihren internen LDAP-Anmeldedaten (Active Directory) anzumelden. Benutzer, deren Domäne nicht mit '**Domains für LDAP-Authentifizierung**' übereinstimmt, werden eingeladen, ein Acronis Access-Konto für externe Benutzer zu erstellen. Benutzer, deren E-Mail-Domäne eine Unterdomäne eines Eintrags in '**Domains für LDAP-Authentifizierung**' ist, erhalten E-Mails mit LDAP-Anweisungen für interne Benutzer, vorausgesetzt, das Kontrollkästchen '**Exakte Übereinstimmung erforderlich' ist aktiviert**. Dieses Kontrollkästchen ist standardmäßig sowie für Ugrades deaktiviert.
- Die Verwaltungsseite **Applikationsrichtlinie** wurde angepasst, um Änderungen in der Applikation Acronis Access für Android 3.2.3 zu berücksichtigen.
- Beim Versuch, auf einen Sync & Share-Ordner zuzugreifen, auf den Sie keinen URL-Zugriff haben, wird zusätzlich zur Verweigerung des Zugriffs und nachfolgender Umleitung eine Fehlermeldung angezeigt.
- Das Überwachungsprotokoll zeigt dem Besitzer eines freigegebenen Ordners nun an, wenn ein Mitglied des freigegebenen Ordners Download-Links an andere Mitglieder sendet.
- Das Konfigurationswerkzeug wurde für die Verwendung von OpenSSL 1.0.1h aktualisiert.
- Die Tomcat-Version wurde auf 7.0.54 aktualisiert.
- In dieser Version wird Java 7 Update 51 verwendet.

BUG-FIXES

- Ein Problem beim Herunterladen von **Sync & Share**-Dateien aus einem Amazon S3-Repository wurde behoben.
- Ein Problem beim Unterscheiden mehrerer nicht mit einer E-Mail-Adresse verknüpfter Access Server Ad-hoc-Administratoren wurde behoben.
- Ein Problem beim Definieren des Werts **owner_name** in den exportierten Protokollen wurde behoben.
- Folgendes Problem wurde behoben: Einige bereitgestellte Administratorgruppen konnten sich nach einem Upgrade nicht anmelden.
- Ein Request Timeout-Problem wurde behoben, das bei der Registrierung eines mobilen Clients in einem großen Active Directory auftreten kann.
- Ein Problem bei der automatischen Dienst-Ausführung wurde behoben, das nach der Installation auf einem Windows-Server aufgetreten ist, der kein Mitglied einer Domäne ist.
- Eine Fehlermeldung zur Lizenzierung wurde behoben, die bei Ausführung mehrerer Gateway-Server in demselben Netzwerk unter Verwendung derselben Seriennummer ausgegeben wurde.
- Folgendes Problem wurde behoben: Vorübergehende SSL-Fehler in der mobilen Acronis Access-App beim Zugriff auf **Sync & Share**-Ordner.
- Einige Java-Erkennungsprobleme im Installationsprogramm wurden behoben.
- Folgendes Problem wurde behoben: Der Client meldete eine Python-Ausnahme, anstatt eine Fehlermeldung zum tatsächlichen Problem auszugeben.

BEKANNTE PROBLEME

- Bei einem Upgrade von Access Server 6.1 mit eingestellter Option "**Umleitung für Port 80 auf Apache Tomcat**" wird diese nicht gespeichert. Aktivieren Sie diese Option nach dem Upgrade manuell im Konfigurationswerkzeug.

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 Access Server Cluster-Gruppe wurde behoben.
- Behandelt ein Abhängigkeitsproblem, das möglicherweise verhindert, dass 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. 111).
- 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 und Upgrade von Acronis Access in einem Cluster.

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.

14.2 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.