Acronis

Acronis Files Advanced 8.5

ADMINISTRATION GUIDE

Revision: 4/11/2019

Inhaltsverzeichnis

1 Einführung

Dieser Leitfaden stellt die Dokumentation für Files Advanced und all seine Funktionen bereit. Die Clientdokumentation finden Sie im Abschnitt Client-Anleitungen (S. 124).

Über Files Advanced

Files Advanced ist die Lösung für sicheren Zugriff, Synchronisierung und Freigabe. Sie gibt der Unternehmens-IT die volle Kontrolle über Geschäftsinhalte, um Sicherheit und Compliance herzustellen und BOYD zu aktivieren. Mit Files Advanced können Mitarbeiter über jedes Gerät – Desktop, Laptop, Tablet oder Smartphone – sicher auf Inhalte zugreifen und sie mit internen und externen Beteiligten, wie Mitarbeitern, Kunden, Partnern und Lieferanten, teilen.

Die Funktionen von Files Advanced lassen sich grob in zwei Hauptkategorien unterteilen: Mobiler Access und Sync & Share.

Mobile Access

Files Advanced Mobile Access ermöglicht den IT-Abteilungen von Unternehmen, den Benutzern von mobilen Geräten einen einfachen, geschützten und verwalteten Zugriff auf die unternehmenseigenen Dateiserver, SharePoint-Server und NAS-Geräte zu ermöglichen. Dabei werden die üblichen Sorgen von IT-Abteilungen aufgelöst, die darauf beruhen, dass Mitarbeiter möglicherweise riskante, verbraucherbasierte Dienste und andere nicht richtlinienkonforme Alternativen verwenden. Dank Files Advanced können IT-Abteilungen den Zugriff auf Inhalte absichern und kontrollieren und dabei gleichzeitig sicherstellen, dass die Benutzer mobiler Geräte auf alle Inhalte, Dateien und Materialien zugreifen können, die sie für ihre Arbeit benötigen.

Sync & Share

Sync & Share von Files Advanced ist die branchenweit einzige Unternehmenslösung zur gemeinsamen Nutzung und Synchronisierung von Dateien, die zwischen den Bedürfnissen der Endbenutzer nach Einfachheit und Effektivität und den Anforderungen der Unternehmens-IT nach Sicherheit, Verwaltbarkeit und Flexibilität einen Ausgleich schafft.

Mit Files Advanced kann die Unternehmens-IT steuern, wer auf Dateien zugreifen kann. Außerdem kann sie feststellen, ob die gemeinsame Nutzung von Dateien den Regeln der Organisation entspricht. Zudem ermöglicht Files Advanced einen Grad an Sichtbarkeit und Überwachung, wie sie verbraucherbasierte Lösungen nicht bieten.

2 Schnellstartanleitung

Diese Anleitung enthält die einfachste und schnellste Vorgehensweise zur schnellen Installation und Inbetriebnahme von Files Advanced. Sie eignet sich nicht für benutzerdefinierte Konfigurationen. Lesen Sie für detaillierte Informationen und Anweisungen zu den einzelnen Komponenten den entsprechenden Abschnitt der umfassenden Dokumentation.

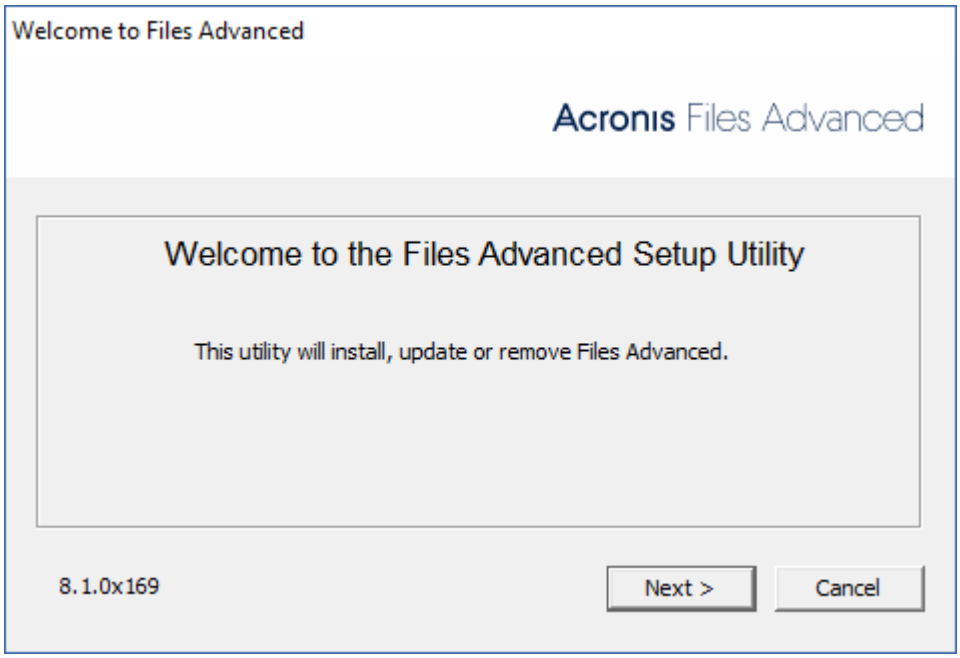
Themen

2.1 Installation

Hinweis: *Sie müssen als Administrator angemeldet sein, um Files Advanced installieren zu können.*

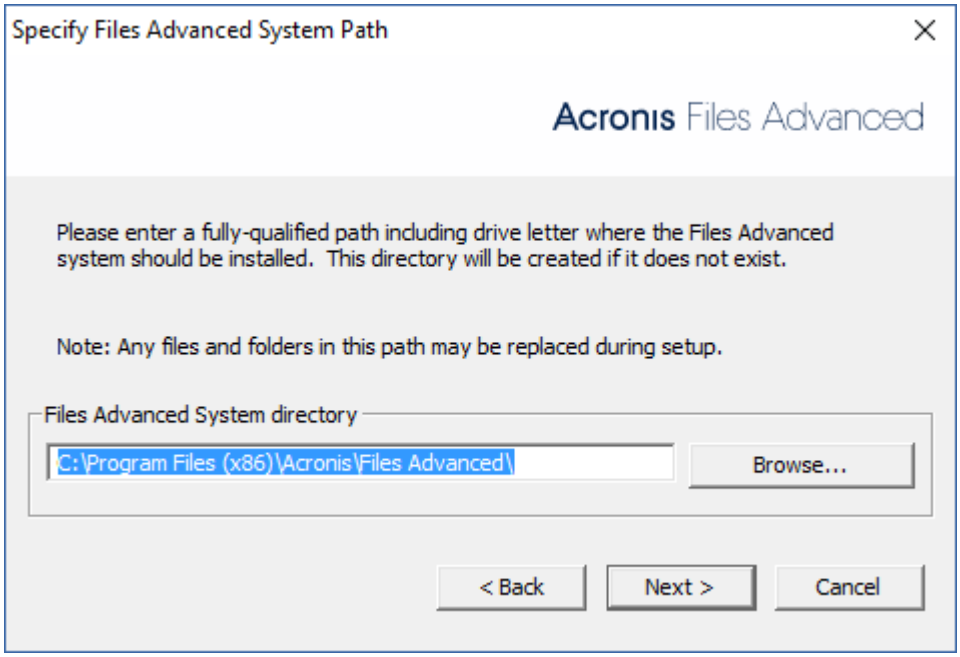
Das Installationsprogramm verwenden

1. Laden Sie das Installationsprogramm für Files Advanced 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 Installationsdatei.

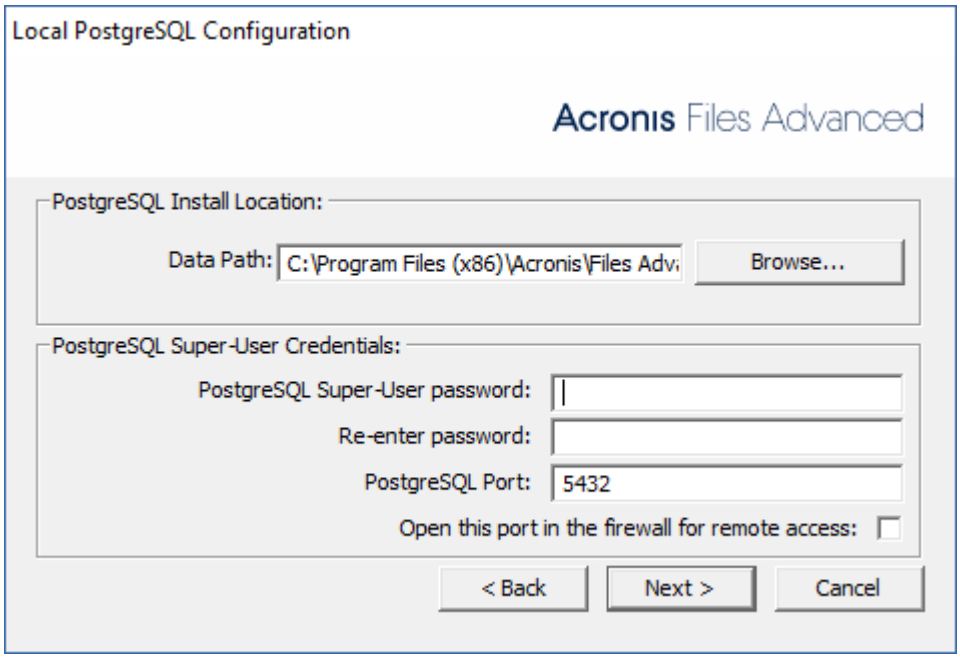


4. Drücken Sie **Weiter**, um zu beginnen.
5. Lesen und akzeptieren Sie die Lizenzvereinbarung.
6. Klicken Sie auf **Installieren**.

7. Drücken Sie auf **OK**, um den Standardpfad für den Hauptordner von Files Advanced zu verwenden.



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



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

Das Konfigurationswerkzeug verwenden

Hinweis: *Die Einstellungen im Konfigurationsdienstprogramm können später geändert werden.*

Übernehmen Sie die Standardwerte für die einzelnen Registerkarten und drücken Sie auf 'OK', um Files Advanced aufzurufen.

2.2 Die Ersteinrichtung

Der Installationsassistent leitet den Administrator durch eine Reihe von Schritten, um die grundlegenden Funktionen des Servers einzurichten.

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

Navigieren Sie zur Weboberfläche von Files Advanced unter Verwendung der IP-Adresse Ihres Netzwerkadapters und des Ports. Sie werden zum Einrichten des Kennworts für das Standard-Administratorkonto aufgefordert.

Hinweis: *Wenn Sie Files Advanced mit den Standardzertifikaten ausführen anstatt Zertifikate einer Zertifizierungsstelle zu verwenden, wird ein Fehler angezeigt, dass der Server nicht vertrauenswürdig ist.*

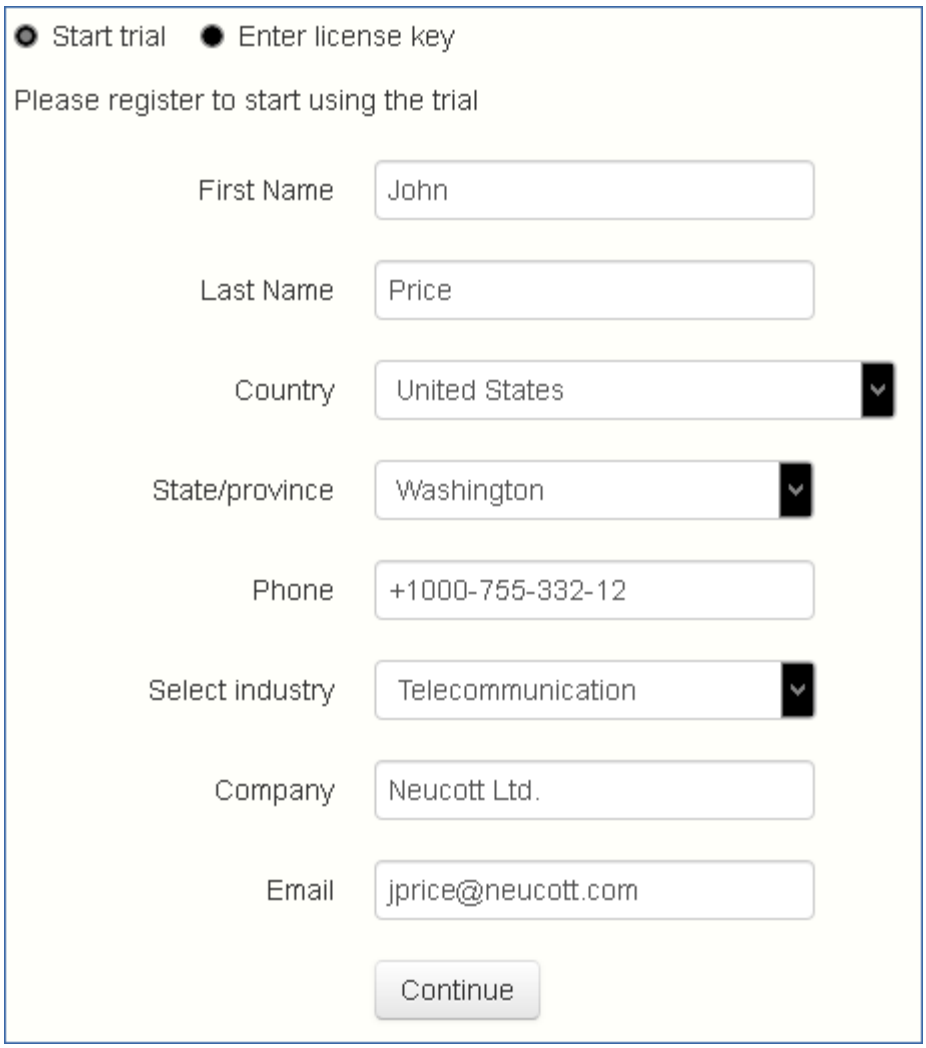
Hinweis: *Alle auf der Seite 'Erstkonfiguration' angezeigten Einstellungen sind auch nach Abschluss der Erstkonfiguration verfügbar. Weitere Informationen über diese Einstellungen finden Sie in den Artikeln zum Thema Server-Administration (S. 126).*

Hinweis: *Der Internet Explorer 8 wird nicht unterstützt.*

Lizenzierung

So starten Sie eine Testversion:

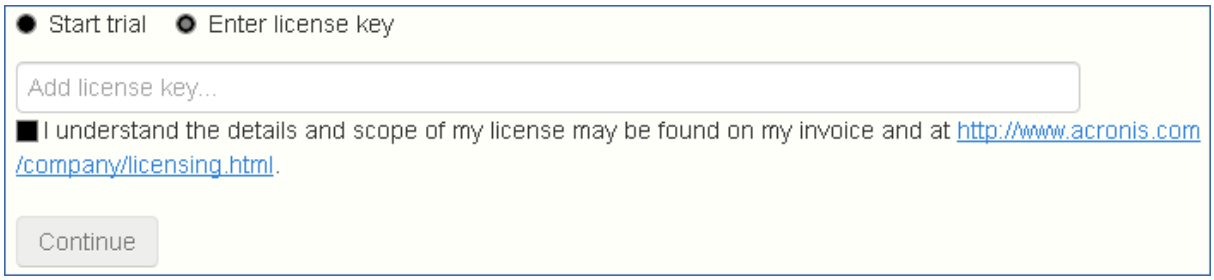
1. Wählen Sie **Test starten** aus, geben Sie die erforderlichen Informationen ein und drücken Sie **Übermitteln**.



2.

Lizenzierung Ihrer Files Advanced Instanz:

1. Wählen Sie **Lizenzschlüssel eingeben**.
2. Geben Sie Ihren Lizenzschlüssel ein und aktivieren Sie das Kontrollkästchen.

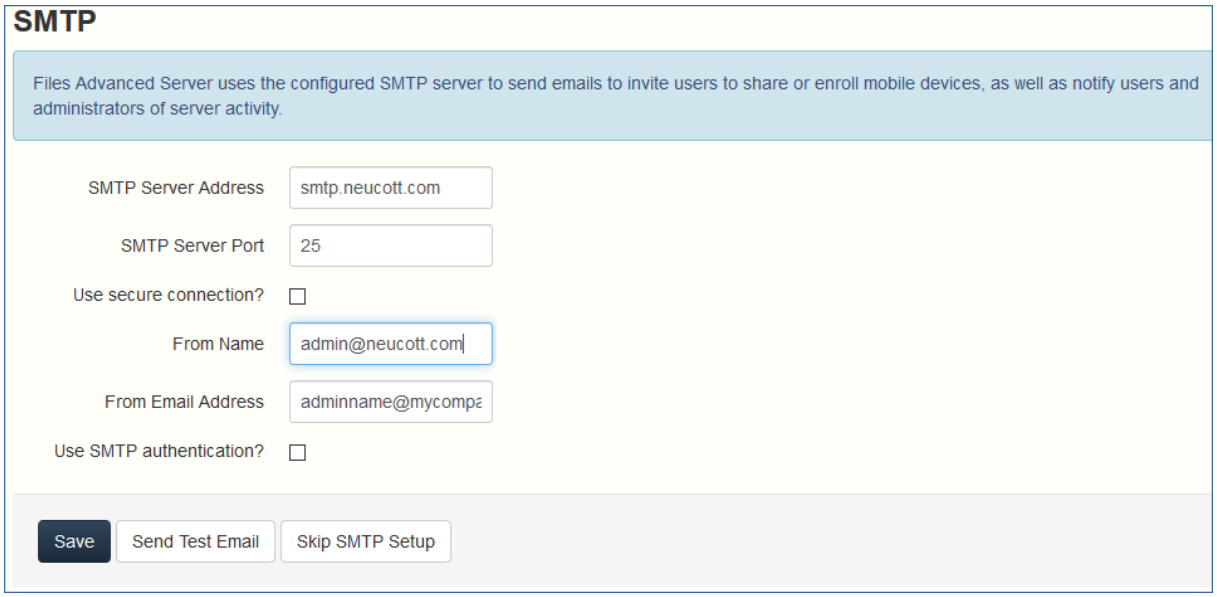


3. Drücken Sie **Speichern**.

Allgemeine Einstellungen

1. Geben Sie einen Servernamen ein.
2. Geben Sie den DNS-Stammnamen oder die IP-Adresse ein, über den bzw. die Benutzer auf die Website zugreifen (beginnend mit http:// oder https://).
3. Wählen Sie die Standardsprache für das **Überwachungsprotokoll** aus. Die aktuellen Optionen sind **Deutsch, Englisch, Französisch, Japanisch, Italienisch, Spanisch, Tschechisch, Russisch, Polnisch, Koreanisch, vereinfachtes und traditionelles Chinesisch**.
4. Drücken Sie **Speichern**.

SMTP

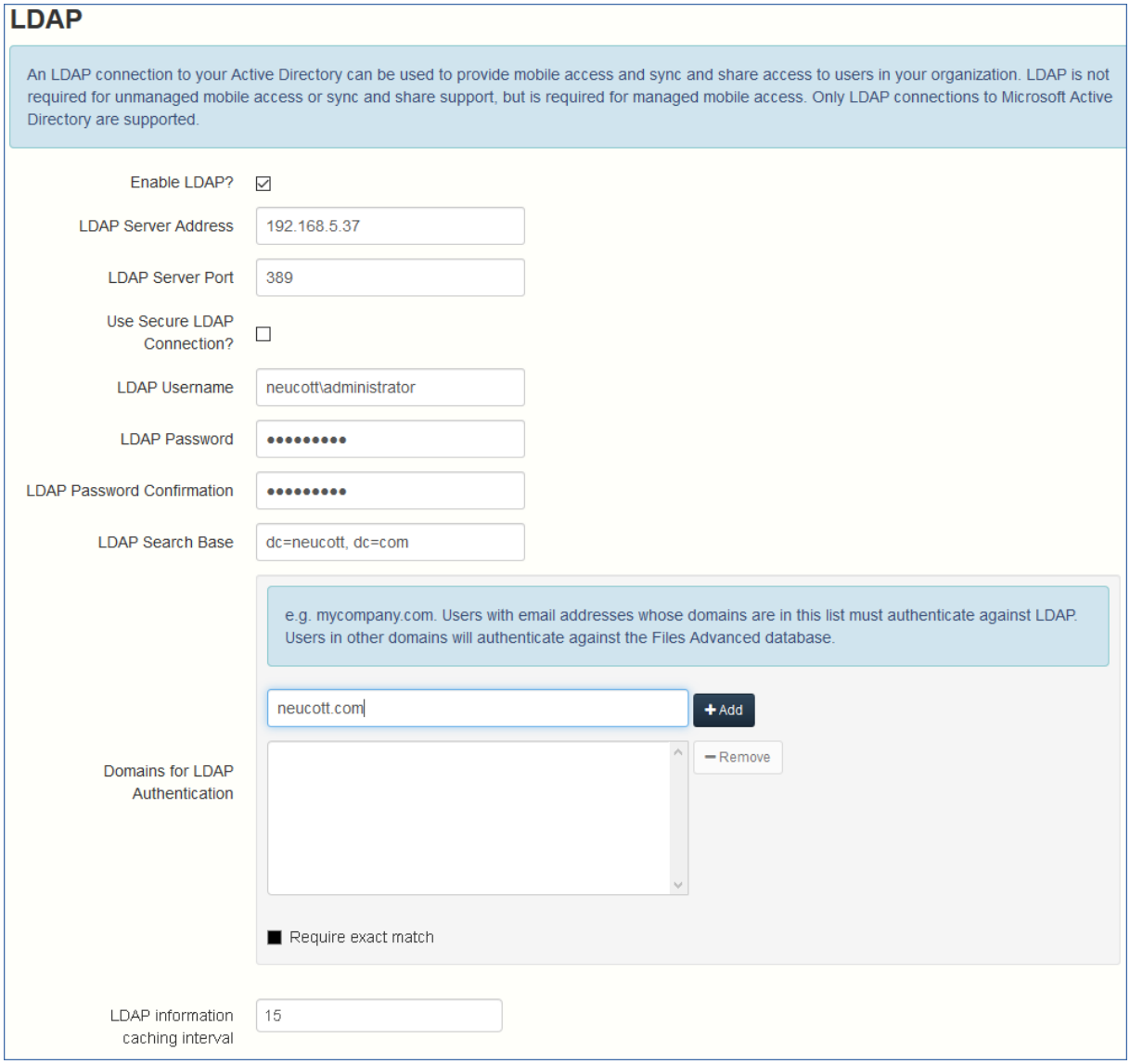


Hinweis: *Sie können diesen Abschnitt überspringen und SMTP später konfigurieren.*

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

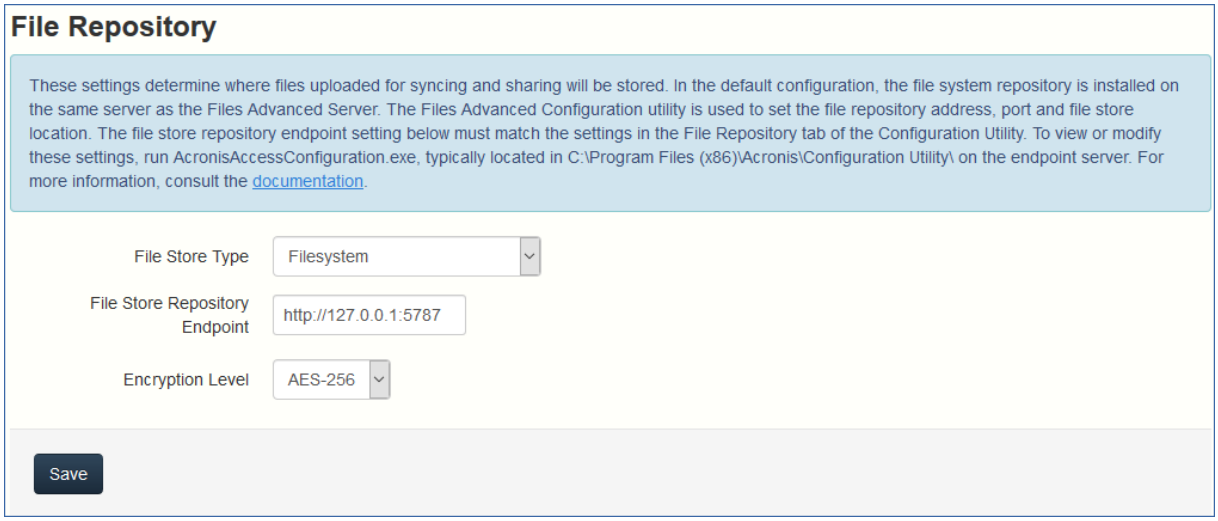


Hinweis: *Sie können diesen Abschnitt überspringen und LDAP später konfigurieren, aber einige der Funktionen von Files Advanced werden dann nicht zur Verfügung stehen.*

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

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

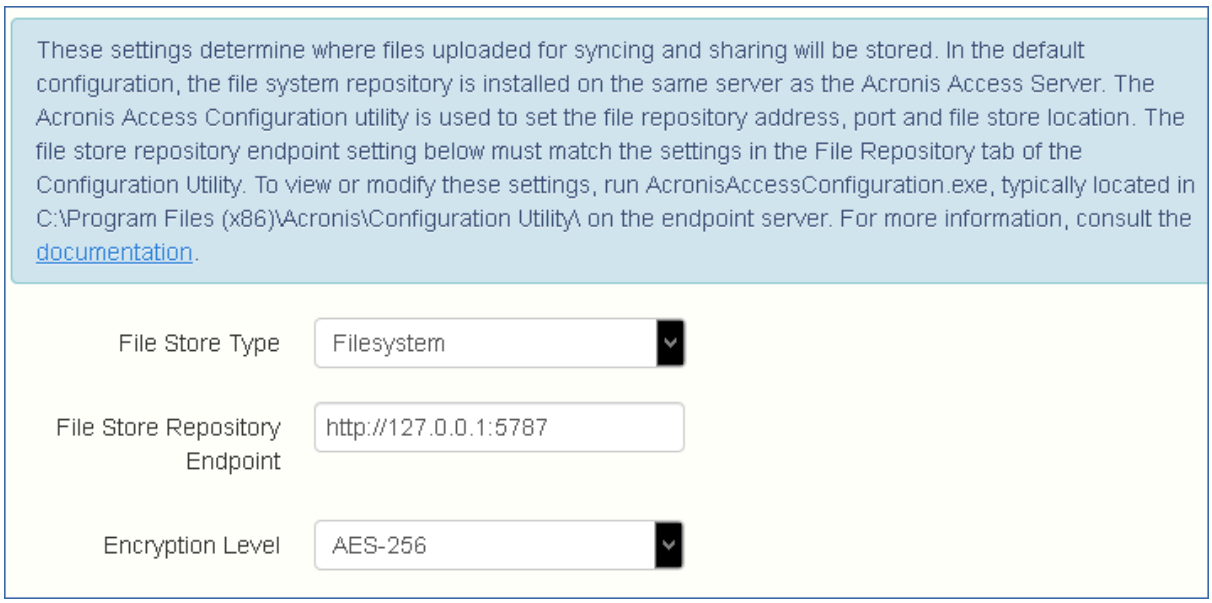
Lokaler Gateway Server



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

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

Datei-Repository



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

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

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

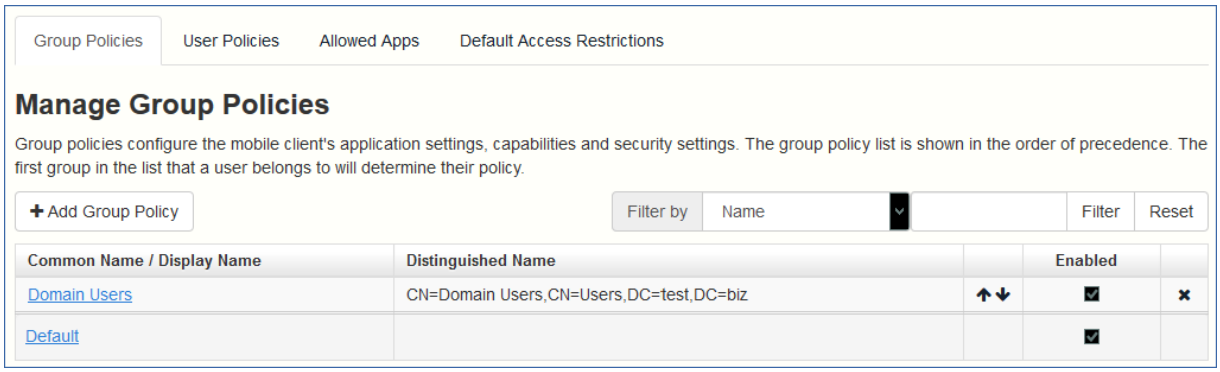
3 Mobiler Zugriff

Themen

Alle mobilen Clients, die für das Management mit dem Files Advanced Web Server registriert sind, unterliegen den Bestimmungen einer Benutzer- oder Gruppenrichtlinie. Die Standardrichtlinie wird automatisch bei der Installation erstellt und verfügt über die niedrigste Priorität (die Benutzerrichtlinie hat die höchste Priorität). Sie wird jedoch auf alle Benutzer angewendet, die keine Benutzerrichtlinie haben und keiner Gruppenrichtlinie zugewiesen sind. Die Standardrichtlinie ist standardmäßig aktiviert.

Die Standardrichtlinie konfigurieren

1. Rufen Sie die Files Advanced Webkonsole auf.
2. Navigieren Sie zu **Mobiler Zugriff**-> **Richtlinien** -> **Gruppenrichtlinien**.



3. Vergewissern Sie sich, dass das Feld **Aktiviert** markiert ist und klicken Sie auf die **Standard**-Richtlinie.
4. Überprüfen Sie die Einstellungen und nehmen Sie bei Bedarf erforderliche Änderungen vor. Eine detaillierte Übersicht für alle Einstellungen finden Sie im Abschnitt Richtlinien (S. 55).

Bei der ersten Ausführung der Files Advanced-Applikation können Sie die App entweder im Demomodus ausprobieren oder Sie können sich an Ihrem Unternehmensserver registrieren.

So testen Sie die App im Demomodus

Im Demomodus können Benutzer die Files Advanced-Applikation auch dann ausprobieren, wenn ihr Unternehmen über keinen Files Advanced Web Server verfügt. Hierbei handelt es sich um eine Umgebungskonfiguration zur Demonstrationszwecken. Es stehen nicht alle Funktionen zur Verfügung.

1. Installieren Sie die Applikation und öffnen Sie sie.
2. Wählen Sie nach der Anzeige des Begrüßungsbildschirms die Option **Unseren Demo-Server verwenden**
3. Daraufhin werden Sie am Demoserver registriert.

__Hinweis:__ Nach der Registrierung verfügen Sie über Nur-Lese-Zugriff auf einige freigegebene Ordner auf dem Demoserver sowie auf einige Synchronisierungsordner. Diese Ordner enthalten Beispieldateien, PDF-Dateien, Bilddateien usw. Sie können diese verfügbaren Dateien durchsuchen, suchen, anzeigen und bearbeiten und auch die bearbeiteten Dateien gegebenenfalls lokal in der Applikation speichern.

4. Sie können jederzeit auf Ihren Unternehmensserver wechseln.

So melden Sie sich am Server Ihres Unternehmens an

1. Installieren Sie die Applikation und öffnen Sie sie.
2. Wählen Sie nach der Anzeige des Begrüßungsbildschirms die Option **Unternehmens-Server verwenden**
3. Geben Sie Ihre Serveradresse, Ihre PIN (falls erforderlich), Benutzernamen und Kennwort ein.
4. Tippen Sie nach dem Ausfüllen des gesamten Formulars auf die Schaltfläche **Registrieren**.
5. 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.
6. Wenn für die Files Advanced Mobile-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.
7. Wenn Ihre Verwaltungsrichtlinie das Speichern von Dateien in Files Advanced einschränkt oder Sie daran hindert, einzelne Server über die Files Advanced Mobile-App hinzuzufügen, wird möglicherweise ein Bestätigungsfenster angezeigt. Falls Sie Dateien lokal in der Files Advanced Mobile-App gespeichert haben, werden Sie aufgefordert, zu bestätigen, dass alle Dateien im lokalen Dateispeicherbereich **Meine Dateien** gelöscht werden. Wenn Sie hier 'Nein' wählen, wird der Verwaltungsregistrierungsvorgang abgebrochen und Ihre Dateien bleiben unverändert.

Informationen zur Verwendung von Files Advanced Clients finden Sie in der jeweiligen Dokumentation zum Client für Ihre App aus der untenstehenden Liste:

- Desktop- und Web-Clients
- iOS-App
- Android-App
- Windows Mobile-App

3.1 Sync&Share

Themen

3.1.1 Sync&Share-Datenquelle

Sobald Sie Files Advanced installieren und konfigurieren, wird automatisch eine Datenquelle mit dem Namen '**Sync&Share**' erstellt und die **Domain-Benutzer-**Gruppe wird standardmäßig zur Liste mit den zugeordneten Benutzern und Gruppen hinzugefügt. Administratoren können jederzeit diesen Datenquellenordner ändern oder entfernen.

Die Standard-Datenquellen sind für alle neu erstellten Benutzer verfügbar, die Teil der neu erstellten Gruppe **Domänenbenutzer** sind, und sie sind über Mobile-, Desktop- und Web-Clients erreichbar.

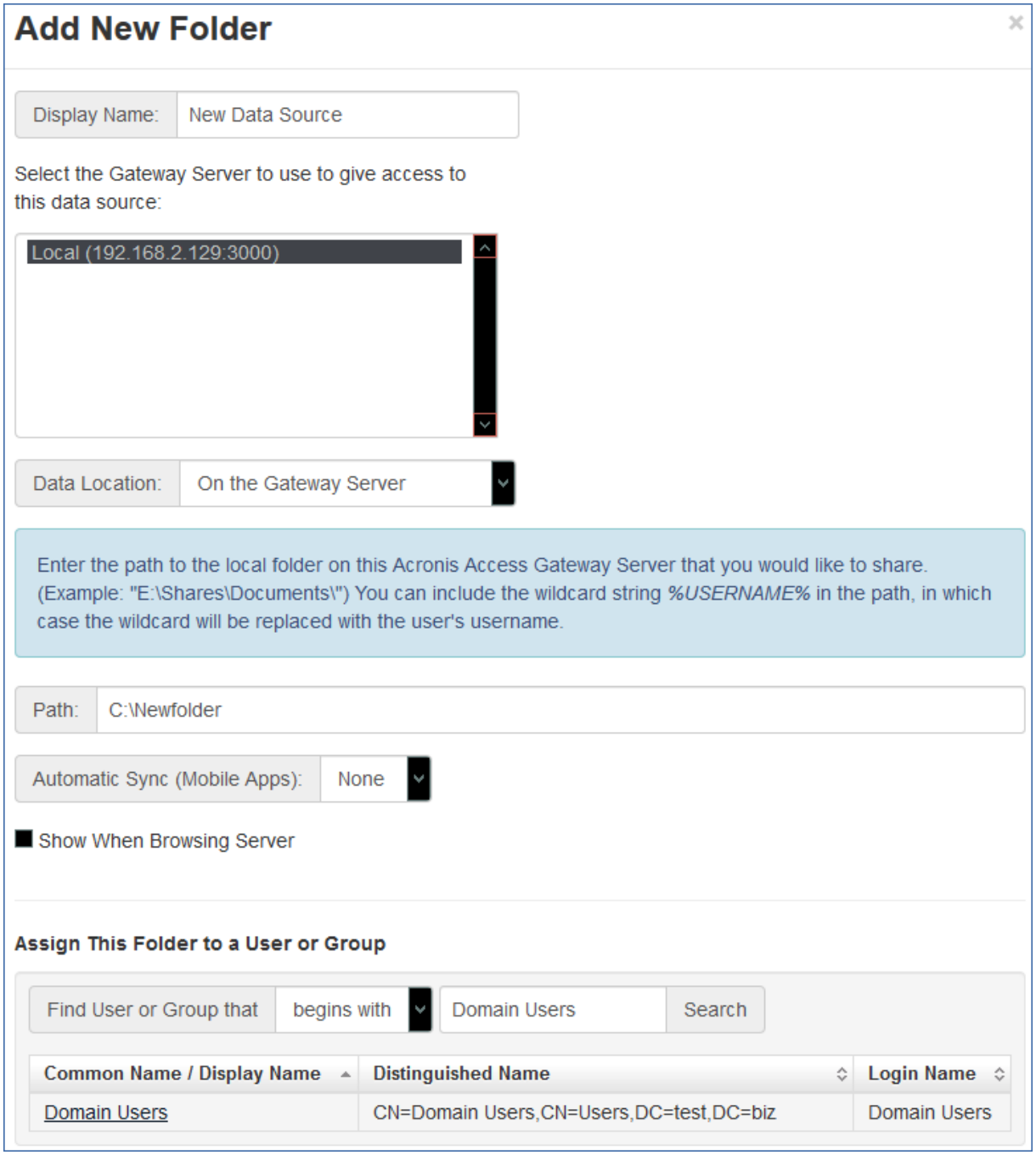
Themen

Für das Freigeben von bestehendem Inhalt ist das Einrichten einer Datenquelle und das Zuweisen dieser Datenquelle zu den gewünschten Benutzern oder Gruppen erforderlich.

Datenquellen erstellen

1. Öffnen Sie die Files Advanced 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.

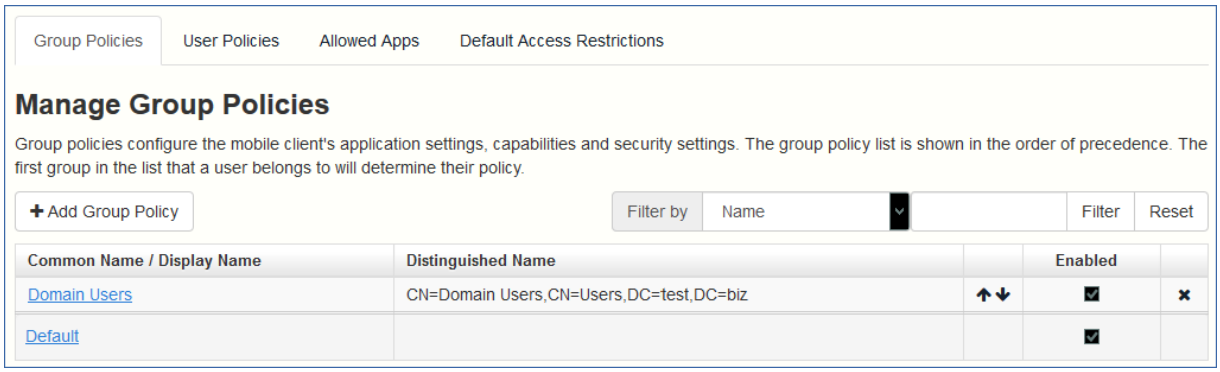
11. Aktivieren Sie **Anzeigen, wenn Server durchsucht wird**, wenn diese Datenquelle sichtbar sein soll, wenn mobile Files Advanced-Clients den Gateway Server durchsuchen.

    Hinweis: *Beim Erstellen von SharePoint-Datenquellen haben Sie die Option, die Anzeige SharePoint-gefolgter Websites zu aktivieren.*

12. Drücken Sie 'Speichern'.

Standardmäßig können Benutzer nicht über den Web Client auf NAS-, Dateiserver- und SharePoint-Ressourcen zugreifen. Die Aktivierung ist allerdings einfach und bietet den Webbenutzern weitere Möglichkeiten.

1. Öffnen Sie die Weboberfläche und navigieren Sie zu **Mobiler Zugriff**--> **Richtlinien**. (Obwohl die Richtlinien primär mit den Mobile-Apps verbunden sind, befindet sich dort auch die Einstellung für den Webzugriff.)
2. Wählen Sie die zu ändernde Richtlinie aus. Wenn Sie noch keine neuen Richtlinien erstellt haben, wählen Sie die Richtlinie **Standard** aus.



3. Aktivieren Sie auf der Registerkarte **Server-Richtlinie** das Kontrollkästchen **Zugriff auf File Server, NAS und Sharepoint über Web Client zulassen**.

4. Überlegen Sie, ob Sie auch die Desktop-Synchronisierung aktivieren möchten, indem Sie die untergeordneten Optionen **Erlauben, dass Datei-Server-, NAS- und SharePoint-Ordner zum Desktop Client synchronisieren werden** und **2-Wege-Synchronisierung von Datei-Server-, NAS- und SharePoint-Odnern zum Desktop Client erlauben** verwenden.
5. Klicken Sie auf **Speichern**.

Dies wird als Richtlinieneinstellung implementiert, um mehr Flexibilität bereitzustellen. Möglicherweise möchten Sie die Einstellung auch für eine andere Gruppe oder für einzelne Richtlinien festlegen.

3.1.2 LDAP-Bereitstellung

Mit der Aktivierung der LDAP-Bereitstellung können sich Ihre Benutzer mit ihren LDAP-Anmeldedaten anmelden und ihre Konten automatisch erstellen lassen, anstatt vom Administrator jeden Benutzer (oder jede Gruppe) einladen zu lassen. Da für diese Konten eine Lizenz aus Ihrem Lizenzpool verwendet wird, sollten Sie eine bestimmte LDAP-Gruppe (oder mehrere Gruppen) zur Bereitstellung wählen.

LDAP-Bereitstellung aktivieren

1. Rufen Sie die Files Advanced Webkonsole auf.
2. Navigieren Sie zu **Sync&Share** -> **LDAP-Bereitstellung**.
3. Geben Sie den Namen einer LDAP-Gruppe (oder mehrerer Gruppen) ein.
4. Wählen Sie die gewünschte(n) Gruppen(n) aus und drücken Sie auf **Speichern**.

Für die Benutzer in der ausgewählten Gruppe beziehungsweise den ausgewählten Gruppen werden die Files Advanced Konten jetzt automatisch erstellt, sobald sie sich mit ihren LDAP-Anmeldedaten bei Files Advanced anmelden.

3.2 Web- und Desktop Clients

- Der Web-Client unterstützt für alle Benutzer mit gültigen Files Advanced-Anmeldedaten den Zugriff und die Freigabe von Dateien und Ordnern aus ihrem bevorzugten Browser.
- Mit dem Desktop Client können Benutzer große Dateien einfach freigeben und sicherstellen, dass ihre Dateien jederzeit aktuell sind.

Informationen zur Verwendung von Files Advanced Clients finden Sie in der jeweiligen Dokumentation zum Client für Ihre App aus der untenstehenden Liste:

- Desktop- und Web-Clients
- iOS-App
- Android-App
- Windows Mobile-App

4 Installation

Themen

4.1 Anforderungen

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

Themen

4.1.1 Anforderungen an das Betriebssystem

Hinweis: *Files Advanced 7.2.3 ist die letzte Version, die 32-Bit-Betriebssysteme unterstützt. Neuere Versionen von Files Advanced unterstützen ausschließlich 64-Bit-Betriebssysteme.*

Hinweis: *Files Advanced 7.4.x ist die letzte Version, die Windows XP und Vista unterstützt. Neuere Versionen von Files Advanced bieten keine Unterstützung für Verbindungen über diese Betriebssysteme.*

Empfohlen:

- Windows Server 2016 Standard und Datacenter
- Windows Server 2012 R2 Standard und Datacenter
- Windows Server 2008 R2 Standard, Enterprise und Datacenter, mit Service Pack 1

Unterstützt:

- Windows Server 2016 Standard
- Windows Server 2012 R2 Standard und Datacenter
- Windows Server 2012 Standard und Datacenter
- Windows Server 2008 R2 Standard, Enterprise und Datacenter, mit Service Pack 1
- Windows Server 2008 Standard, Enterprise und Datacenter, 32- und 64-Bit-Editionen, mit Service Pack 2

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.*

4.1.2 Anforderungen für den mobilen Client

Unterstützte Geräte:

- Apple iPad der 4. Generation oder höher
- Apple iPad mini der 2. Generation oder höher
- Apple iPad Pro der 1. Generation oder höher
- Apple iPhone 5 oder höher
- Apple iPod Touch der 6. Generation oder höher
- Android-Smartphones und -Tablets (Geräte mit x86-Prozessorarchitektur werden nicht unterstützt)
- Windows-Smartphones und -Tablets (Windows RT wird nicht unterstützt)

Hinweis: *Windows-Geräte funktionieren mit Files Advanced-Servern Version 6.0 und höher.*

Unterstützte Betriebssysteme:

- iOS 10 oder höher.
- Android 4,1 oder höher (Geräte mit x86-Prozessorarchitektur werden nicht unterstützt)
- Windows 8.1 oder höher (Windows RT wird nicht unterstützt)

Hinweis: *Windows-Geräte funktionieren mit Files Advanced-Servern Version 6.0 und höher.*

Die Files Advanced-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.
- Für Windows PC und Tablet oder Phones.

4.1.3 Minimale Hardware-Empfehlungen

Beispielbereitstellungen

Diese Darstellungen gehen davon aus, dass alle Komponenten von Files Advanced auf derselben virtuellen Maschine oder demselben physischen Server ausgeführt werden.

Hinweis: *Beim empfohlenen Speicherplatz wird davon ausgegangen, dass die Dateibereinigung des Datei-Repositorys alter und gelöschter Versionen konfiguriert ist.*

Hinweis: *Die empfohlene Laufwerksgröße stellt nur einen Ausgangspunkt dar und muss abhängig von der Größe und Anzahl der vom Benutzer synchronisierten Dateien erweitert werden.*

Hinweis: *Files Advanced Web Server kann auf virtuellen Maschinen installiert werden.*

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

Hinweis: *Diese Werte sind unsere Empfehlung für eine Produktionsumgebung. Wenn Sie planen, einen Test zu starten oder Files Advanced für Testzwecke zu installieren, können Sie die Hardware abhängig von Ihrer Testlast stufenweise senken.*

Kleine Bereitstellungen

- Bis zu 25 Benutzer
- CPU: Intel i7 Xeon mit 4 Kernen oder AMD-Äquivalent.
- RAM: 16 GB
- Speicherplatz: 100 GB

Mittelgroße Bereitstellungen

- Bis zu 500 Benutzer
- CPU: Intel i7 Xeon mit 8 Kernen oder AMD-Äquivalent.
- RAM: 40 GB
- Speicherplatz: 2 TB RAID

Große Bereitstellungen

- Bis zu 2.500 Benutzer
- CPU: Intel i7 Xeon mit 16 Kernen oder AMD-Äquivalent.
- RAM: 64 GB
- Speicherplatz: 10 TB RAID

Hinweis: *Bei Bereitstellungen für mehr als 2.500 Benutzer wird eine Cluster-Serverkonfiguration empfohlen. Bitte wenden Sie sich bei Bereitstellungen für mehr als 2.500 Benutzer an den Acronis Support.*

4.1.4 Netzwerkanforderungen

- 1 Statische IP-Adresse. Für bestimmte Konfigurationen werden 2 IP-Adressen benötigt.
- Optional, jedoch empfohlen: DNS-Namen für die obigen IP-Adressen.
- Greifen Sie über das Netzwerk auf Ihren Domänencontroller zu, wenn Sie Active Directory (LDAP) nutzen möchten.
- Greifen Sie für E-Mail-Benachrichtigungen und Einladungen über das Netzwerk auf einen SMTP-Server zu.
- Die Adresse **127.0.0.1** wird von der Mobile-App intern verwendet und darf nicht durch einen Tunnel gleich welcher Art (VPN, MobileIron, BlackBerryDynamics usw.) weitergeleitet werden.
- Alle Computer, auf denen der Files Advanced Web Server oder der Gateway Server ausgeführt werden, müssen an das Windows Active Directory gebunden sein.

Es gibt zwei Komponenten, die HTTPS-Verkehr verarbeiten: der Gateway Server und der Files Advanced Web Server. Der Gateway Server wird von mobilen Clients für den Zugriff auf Dateien und Freigaben aus den Datenquellen verwendet. Der Files Advanced Web Server stellt die Webbenutzeroberfläche für Sync & Share-Clients bereit und fungiert zudem als Verwaltungskonsole sowohl für Mobile Access als auch für Sync & Share.

Bei den meisten Bereitstellungen wird empfohlen, für beide Server eine IP-Adresse, jedoch mit unterschiedlichen Ports und separaten DNS-Einträgen zu verwenden. Diese Konfiguration mit nur einer IP-Adresse ist für die meisten Installationen ausreichend. Der Server kann so konfiguriert werden, dass für jede Komponente separate IP-Adressen verwendet werden, wenn es Ihre Einstellung bzw. Einrichtung verlangt.

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

- **Zugriff über Port 443**: Da Files Advanced 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 Files Advanced Web Server zulassen, können autorisierte iPad-Clients innerhalb oder außerhalb der Firewall eine Verbindung aufbauen. Die App kann jedoch auch für die Verwendung eines anderen Ports Ihrer Wahl konfiguriert werden.
- **VPN:** Die Files Advanced-Mobile-App unterstützt den Zugriff über eine VPN-Verbindung. Sowohl der integrierte iOS VPN-Client als auch VPN-Clients von Drittanbietern werden unterstützt. iOS-Verwaltungsprofile können optional auf Geräte angewendet werden, die MDM-Systeme (Mobile Device Management) oder das Apple iPhone-Konfigurationswerkzeug verwenden, um die zertifikatsbasierte iOS-Funktion 'VPN auf Anforderung' zu konfigurieren, die nahtlosen Zugriff auf Files Advanced Web 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 Files Advanced Mobile-App unterstützt die Reverse-Proxy-Pass-Through-Authentifizierung, die Authentifizierung mit Benutzername/Kennwort, die Authentifizierung per eingeschränkter Kerberos-Delegierung und die Zertifikatsauthentifizierung. Detaillierte Informationen zum Hinzufügen von Zertifikaten zur Files Advanced Mobile-App finden Sie im Artikel Client-Zertifikate verwenden.
- **Für BlackBerry Dynamics aktivierte App:** Die Files Advanced Mobile-App bietet die Möglichkeit, sich auf der BlackBerry Dynamics-Plattform zu registrieren und von dieser verwaltet zu werden. Bei dieser Konfiguration wird die gesamte Netzwerkkommunikation zwischen Files Advanced Mobile-Apps und Gateway Servern über den sicheren Kommunikationskanal von BlackBerry Dynamics und den BlackBerry Proxy Server umgeleitet. Weitere Informationen finden Sie in der Anleitung zur Files Advanced Mobile-App für BlackBerry Dynamics (S. 305).
- **Per MobileIron AppConnect registrierte App**: Wenn die Files Advanced Mobile-App per AppConnect-Plattform von MobileIron registriert wird, kann die gesamte Netzwerkkommunikation zwischen den Files Advanced Mobile-App-Clients und Gateway Servern über MobileIron Sentry geroutet werden. Weitere Informationen finden Sie in der Anleitung zu MobileIron AppConnect (S. 275).

Zertifikate:
Files Advanced 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.

4.1.5 Voraussetzungen für Desktop Client

Unterstützte Betriebssysteme:

- Windows 7, Windows 8 und 8.1, Windows 10

Hinweis: *Die Version 7.4 ist die aktuelle Version des Desktop Client, die mit Windows XP und Vista kompatibel ist. Wenn Sie eine neuere Version des Files Advanced Desktop Client verwenden wollen, müssen Sie ein Update Ihres Windows-Betriebssystems veranlassen. Files Advanced 7.4 ist die letzte Serverversion, die Verbindungen von Windows XP oder Vista zulässt.*

- Mac OS X 10.8 und höher, wenn Mac mit 64-Bit-Software kompatibel ist.

Hinweis: *Der Desktop Client, Version 7.1.2, ist die letzte mit Mac OS X 10.6 und 10.7 kompatible Version. Wenn Sie eine neuere Version des Files Advanced Desktop Client verwenden wollen, müssen Sie ein Update Ihres Mac-Betriebssystems veranlassen.*

Hinweis: *Stellen Sie bei der Installation des Files Advanced 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. 180).*

Unterstützte Webbrowser:

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

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****.*

Hinweis: *Internet Explorer 11 und frühere Versionen unterstützen keinen Upload von Dateien, die größer als 4 GB sind.*

- Google Chrome 4.1.249.1042 und höher.
- Safari 5.1.10 und höher.

4.2 Files Advanced auf Ihrem Server installieren

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

Hinweis: *Anweisungen zu Upgrades finden Sie im Abschnitt zu Upgrades (S. 38).*

Hinweis: *Anweisungen zum Installieren in einem Cluster finden Sie im Abschnitt Lastenausgleich (S. 188).*

Die Installation von Files Advanced besteht aus drei Schritten:

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

Files Advanced installieren

Sie müssen als Administrator angemeldet sein, um Files Advanced installieren zu können.

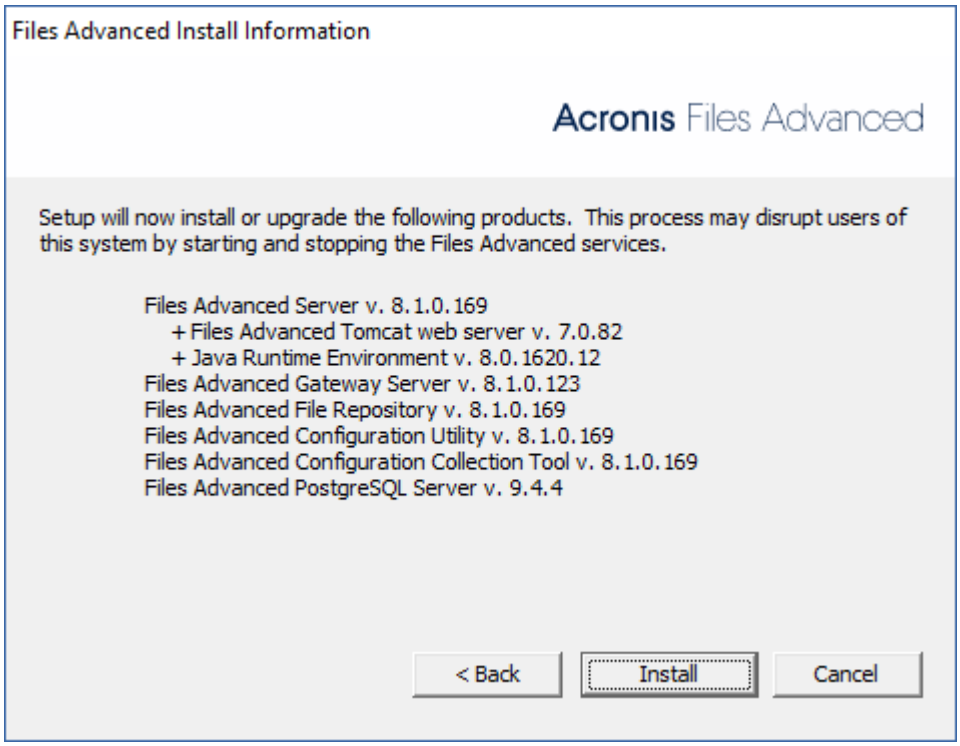
1. Laden Sie das Installationsprogramm für Files Advanced herunter.
2. Deaktivieren Sie alle vorhandenen Virenschutzprogramme, da sie unter Umständen den Installationsvorgang unterbrechen und somit eine fehlerhafte Installation verursachen können.
3. Doppelklicken Sie auf die ausführbare Installationsdatei.
4. Drücken Sie **Weiter**, um zu beginnen.

Lesen und akzeptieren Sie die Lizenzvereinbarung.

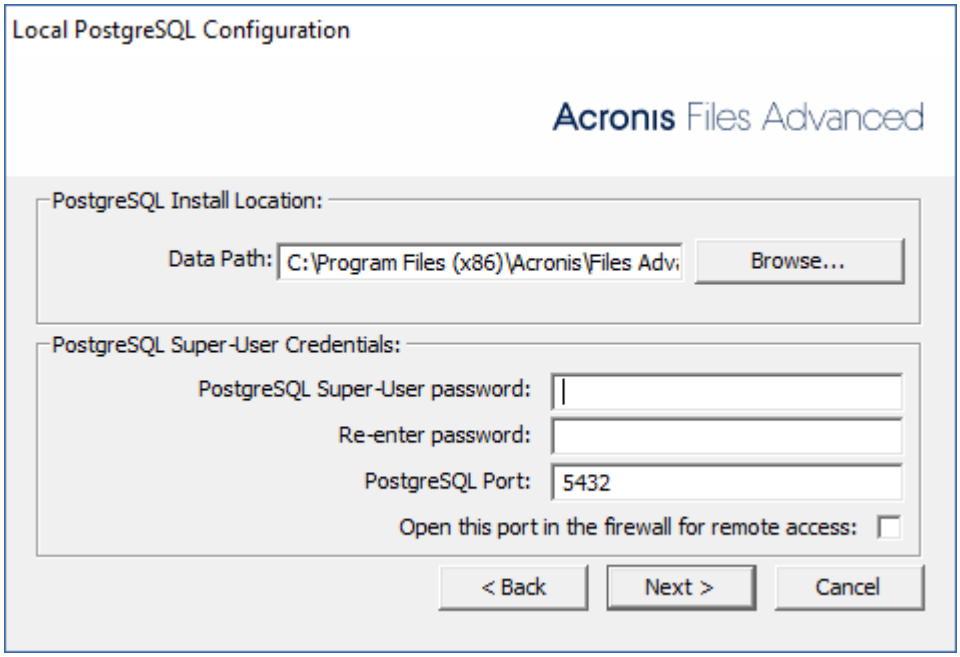
5. Drücken Sie **Installieren**.

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

6. Verwenden Sie den Standardpfad oder wählen Sie einen neuen aus dem Hauptordner von Files Advanced und drücken Sie OK.



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



8.

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

10. Wenn der Installationsvorgang für Files Advanced abgeschlossen ist, drücken Sie **Beenden**.
11. Das Konfigurationswerkzeug wird automatisch gestartet und schließt die Installation ab.

Weitere Anleitungen zur Verwendung des Konfigurationswerkzeugs finden Sie auf der Seite Das Konfigurationswerkzeug verwenden (S. 28).

4.3 Das Konfigurationswerkzeug verwenden

Das Files Advanced Installationsprogramm umfasst ein Konfigurationswerkzeug, das eine schnelle und einfache Einrichtung des Zugriffs auf Ihren Files Advanced Gateway Server, Ihr Datei-Repository und den Files Advanced Web Server ermöglicht.

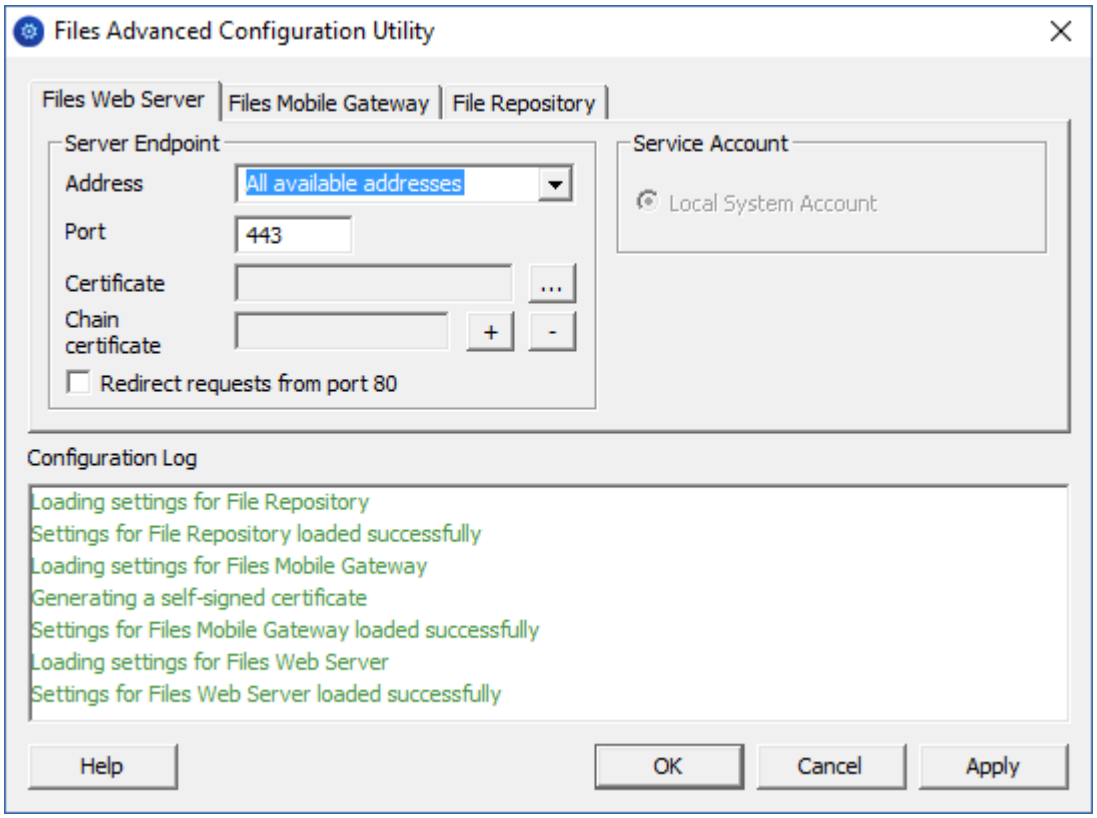
Hinweis: *Im Abschnitt Netzwerkanforderungen (S. 24) finden Sie weitere Informationen zu optimalen Vorgehensweisen für die IP-Adressenkonfigurationen von Files Advanced.*

Hinweis: *Weitere Informationen zum Hinzufügen Ihres Zertifikats zum Microsoft Windows-Zertifikatspeicher finden Sie im Artikel Zertifikate verwenden (S. 243).*

Konfigurationsdienstprogramm – Übersicht

Die Einstellungen im Konfigurationsdienstprogramm können jederzeit geändert werden, indem das Dienstprogramm ausgeführt wird und die notwendigen Änderungen vorgenommen werden. Die notwendigen Konfigurationsdateien werden für Sie angepasst und die Dienste neu gestartet.

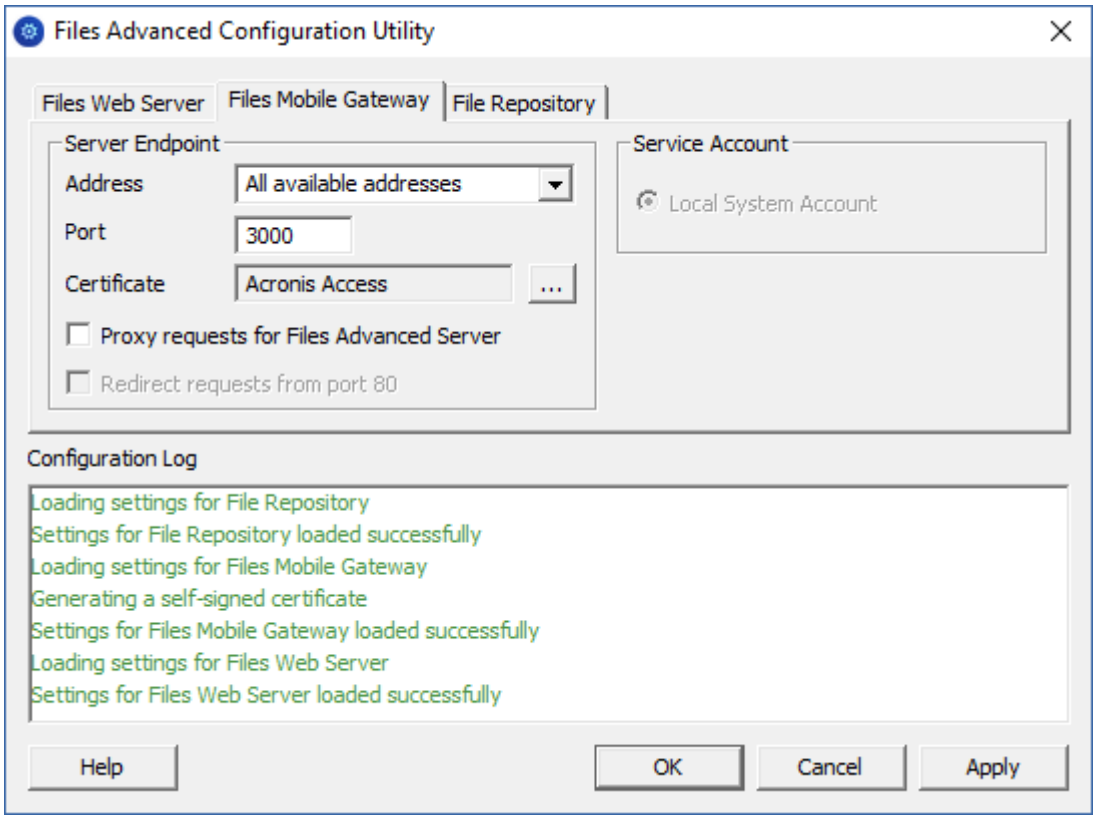
Web Server – Registerkarte



Der Files Advanced Web Server stellt die Weboberfläche für Files Advanced Clients zur Verfügung und ist darüber hinaus die Verwaltungskonsole für Mobile Access (S. 53) und Sync & Share.

- **Adresse** – Die IP-Adresse Ihrer Weboberfläche. Sie können auch **Alle Adressen** auswählen, wenn alle verfügbaren Oberflächen abgehört werden sollen.
- **Port** – Der Port Ihrer Web-Benutzeroberfläche.
- **Zertifikat** – Der Pfad für das Zertifikat Ihrer Weboberfläche. Sie können ein Zertifikat aus dem Microsoft Windows-Zertifikatspeicher wählen.
- **Kettenzertifikat** – Der Pfad für das Zwischenzertifikat Ihrer Weboberfläche. Sie können eines aus dem Zertifikatspeicher von Microsoft Windows auswählen. Dieses Zertifikat ist nur erforderlich, wenn Ihre Zertifikatsstelle Ihnen auch ein Zwischenzertifikat ausgestellt hat.
- 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.
- **Dienstonto –** Ermöglicht, dass der Files Advanced Web Server-Dienst im Kontext eines anderen Kontos ausgeführt werden kann. Dies ist in typischen Installationen normalerweise nicht erforderlich.

Mobile Gateway – Registerkarte

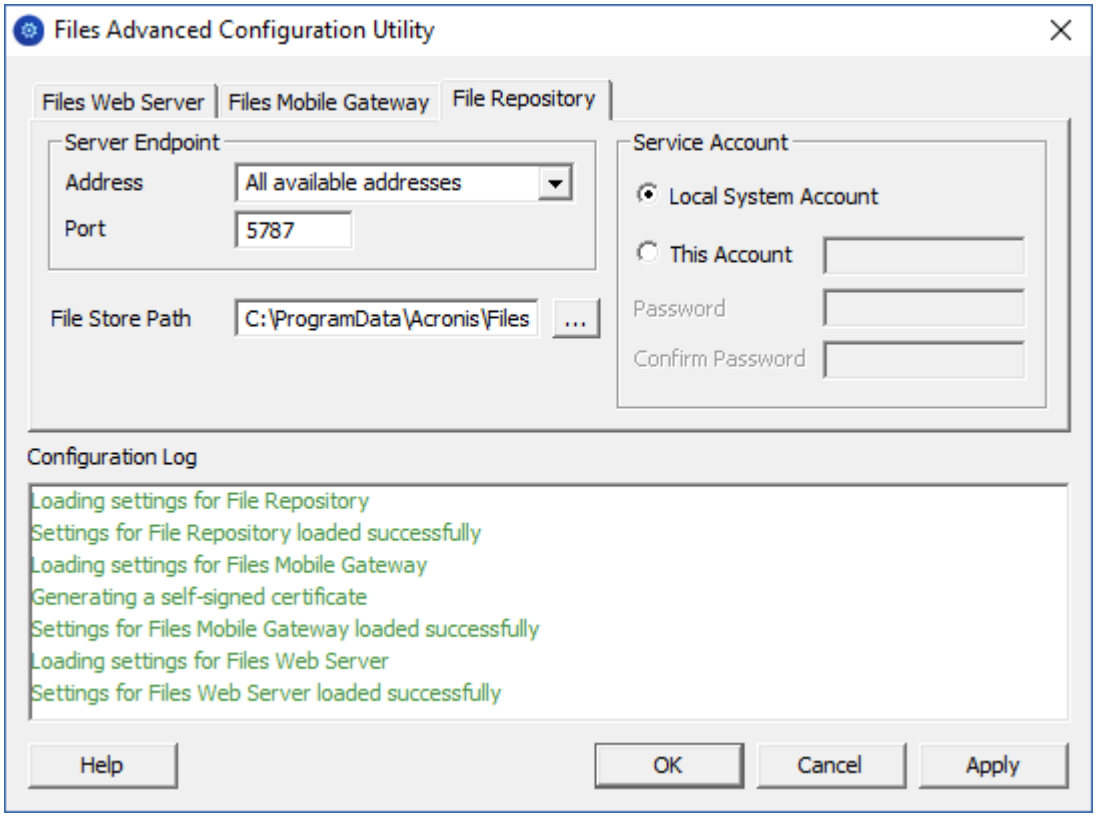


Der Gateway Server wird von Mobile Clients für den Zugriff auf Dateien und Freigaben verwendet.

- **Adresse –** Die IP-Adresse Ihres Gateway Servers. Sie können auch **Alle Adressen** auswählen, wenn alle Oberflächen abgehört werden sollen.
- **Port –** Der Port Ihres Gateway Servers.
- **Zertifikat –** Der Pfad für das Zertifikat Ihres Gateway Servers. Sie können ein Zertifikat aus dem Zertifikatspeicher von Microsoft Windows auswählen.
- **Dienstkonto –** Ermöglicht, dass der Gateway Server-Dienst im Kontext eines anderen Kontos ausgeführt werden kann. Dies ist in typischen Installationen normalerweise nicht erforderlich.

- **Proxy-Anforderungen für Files Advanced Server** – Wenn aktiviert, verbinden sich Benutzer mit dem Gateway Server, der ihnen daraufhin Proxy-Zugriff auf den Access Server einräumt. Dies ist verfügbar, wenn Sie einen Files Advanced Server sowie einen Gateway Server auf demselben Computer installiert haben.
- 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.

Datei-Repository – Registerkarte



Das Datei-Repository wird von den Sync & Share-Funktionen verwendet. Wenn Sie Sync & Share nicht aktiviert haben, können Sie die Standardwerte übernehmen. Wenn Sie Sync & Share verwenden, sollte im Pfad für den Dateispeicherort das Laufwerk für die Speicherung angegeben werden. Wenn Amazon S3 für die Speicherung verwendet werden soll, können Sie die Standardwerte übernehmen.

- **Adresse –** Die IP-Adresse Ihres Datei-Repositorys. Sie können auch **Alle Adressen** auswählen, wenn alle Oberflächen abgehört werden sollen. Bei Angabe einer IP- oder DNS-Adresse, dieselbe Adresse: auch im Abschnitt **Datei-Repository** der Weboberfläche festgelegt. Weitere Informationen darüber finden Sie im Artikel Datei-Repository (S. 116).
- **Port –** Der Port Ihres Datei-Repositorys. Derselbe Port: auch im Abschnitt **Datei-Repository** der Weboberfläche festgelegt. Weitere Informationen darüber finden Sie im Artikel Datei-Repository (S. 116).
- **Dateispeicherpfad –** UNC-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.

- **Dienstkonto –** Befindet sich der Dateispeicher für das Repository auf einer Remote-Netzwerkfreigabe, muss das Service-Konto so konfiguriert werden, dass es Berechtigungen für diese Netzwerkfreigabe aufweist. Das Konto muss auch über Lese- und Schreibzugriff für den Repository-Ordner verfügen (z.B. **`C:\Program Files (x86)\Acronis\Files Advanced\File Repository\Repository`**), um in die Protokolldatei schreiben zu können.

__Hinweis:__ Wenn Sie für den Dienst ein spezielles Konto anstelle der Option __Lokales Systemkonto__ verwenden, müssen Sie die Systemsteuerung für __Dienste__ öffnen, dann die Eigenschaften für den Dienst __Files Advanced Datei-Repository__ öffnen und die Registerkarte __Anmeldung__ bearbeiten. Sie müssen das Konto und das entsprechende Kennwort manuell in den entsprechenden Feldern eingeben.

Öffnen des Installationsassistenten

Nach dem Ausfüllen der entsprechenden Felder werden nach dem Drücken auf **Anwenden** oder **OK** die Dienste neu gestartet, die Sie geändert haben.

__Hinweis:__ Es kann, nachdem die Dienste gestartet wurden, 30 bis 45 Sekunden dauern, bis der Files Advanced Web Server verfügbar ist.

1. Sobald Sie die erstmalige Einrichtung des Konfigurationsdienstprogramms abgeschlossen haben, öffnet ein Webbrowser automatisch die Files Advanced Weboberfläche.
2. Auf der Anmeldeseite werden Sie aufgefordert, ein Kennwort für den **Administrator** festzulegen, und anschließend führt Sie der Installationsassistent (S. 31) durch das Einrichtungsverfahren.

Notieren Sie sich das Administratorkennwort, da es nicht wiederhergestellt werden kann, wenn Sie es vergessen!

4.4 Den Installationsassistenten verwenden

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

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

Falls Sie das Administratorkonto im vorherigen Schritt nicht eingerichtet haben, werden Sie auf der Anmeldeseite aufgefordert, das **Administrator**kennwort festzulegen.

Notieren Sie sich das Administratorkennwort, da es nicht wiederhergestellt werden kann, wenn Sie es vergessen!

Den Prozess der Erstkonfiguration durchlaufen

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

Hinweis: *Zusätzliche Administratoren können später konfiguriert werden. Weitere Informationen hierzu finden Sie im Abschnitt Server-Administration (S. 126).*

Dieser Assistent unterstützt Sie bei den wichtigsten Einstellungen für die Funktionalität Ihres Produkts.

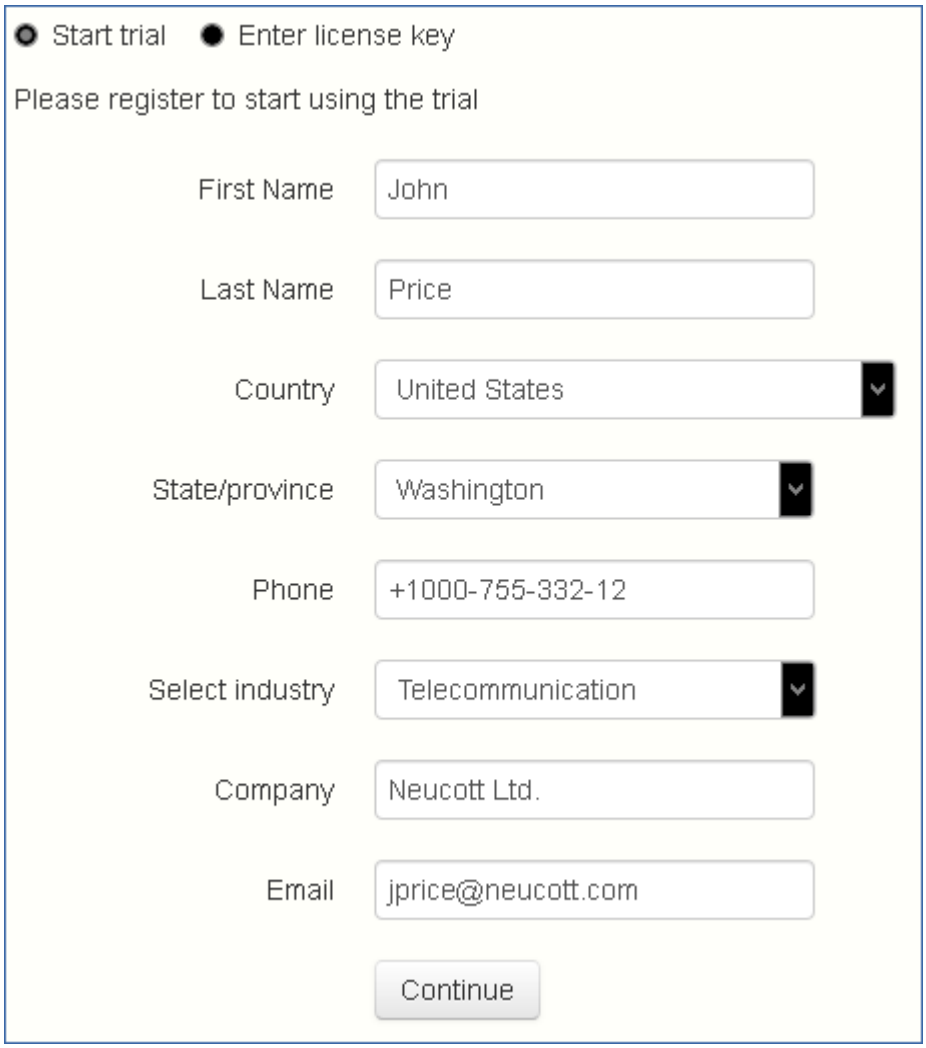
- In den allgemeinen Einstellungen werden die Einstellungen der Weboberfläche, wie die Sprache, das Farbschema, der Servername, der in Admin-Benachrichtigung verwendet wird, die Lizenzierung und Administratoren festgelegt.
- LDAP-Einstellungen ermöglichen Ihnen, Active Directory-Anmeldedaten, Regeln und Richtlinien mit unserem Produkt zu verwenden.
- SMTP-Einstellungen betreffen die Funktionalität in den Funktionen Mobile Access und Sync & Share. Bei Mobile Access wird der SMTP-Server verwendet, wenn Registrierungseinladungen versendet werden. Sync & Share-Funktionen verwenden den SMTP-Server für das Versenden 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. 126).

Lizenzierung

So starten Sie eine Testversion:

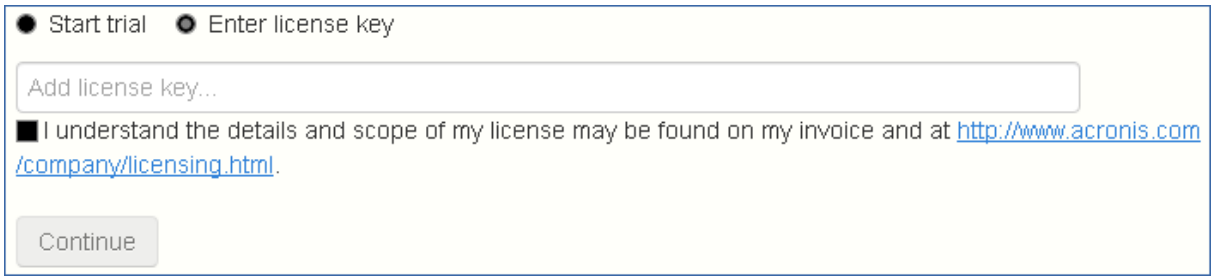
1. Wählen Sie **Test starten** aus, geben Sie die erforderlichen Informationen ein und drücken Sie **Übermitteln**.



2.

Lizenzierung Ihrer Files Advanced Instanz:

1. Wählen Sie **Lizenzschlüssel eingeben**.
2. Geben Sie Ihren Lizenzschlüssel ein und aktivieren Sie das Kontrollkästchen.

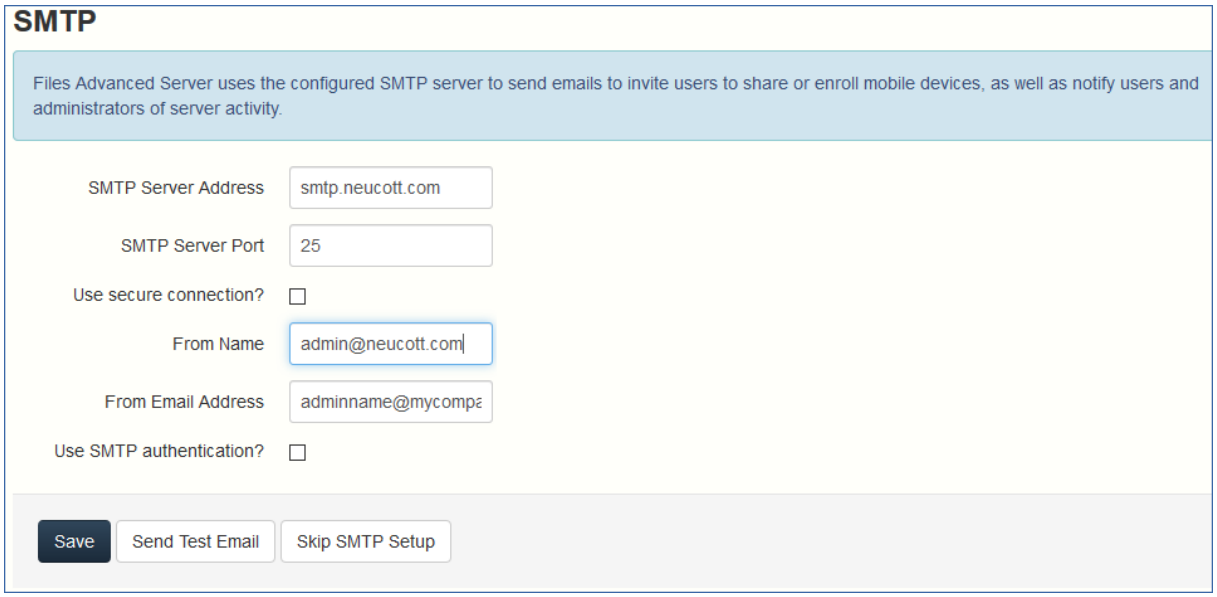


3. Drücken Sie **Speichern**.

Allgemeine Einstellungen

1. Geben Sie einen Servernamen ein.
2. Geben Sie den DNS-Stammnamen oder die IP-Adresse ein, über den bzw. die Benutzer auf die Website zugreifen (beginnend mit http:// oder https://).
3. Wählen Sie die Standardsprache für das **Überwachungsprotokoll** aus. Die aktuellen Optionen sind **Deutsch, Englisch, Französisch, Japanisch, Italienisch, Spanisch, Tschechisch, Russisch, Polnisch, Koreanisch, vereinfachtes und traditionelles Chinesisch**.
4. Drücken Sie **Speichern**.

SMTP

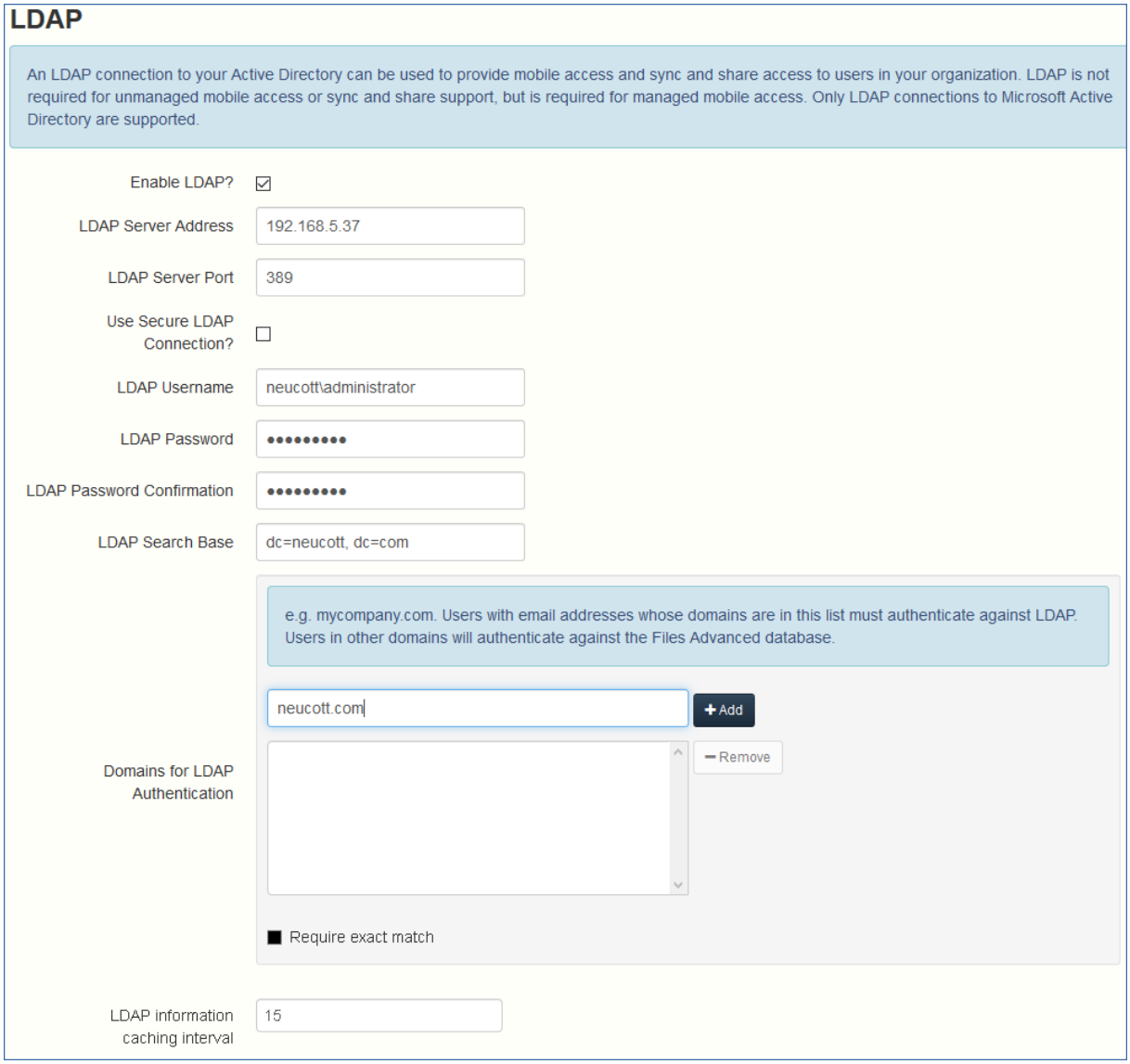


Hinweis: *Sie können diesen Abschnitt überspringen und SMTP später konfigurieren.*

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

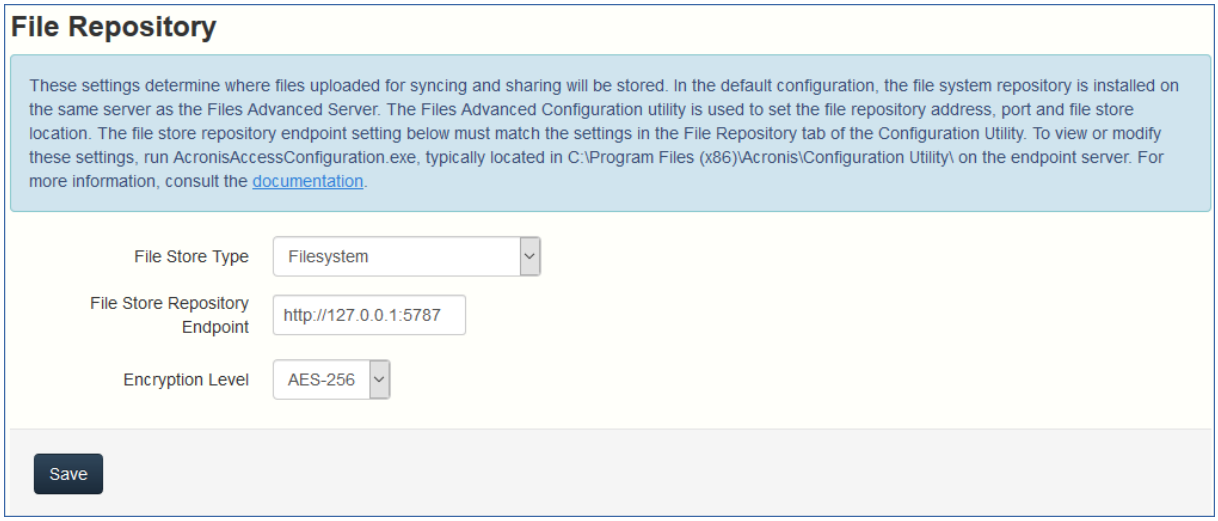


Hinweis: *Sie können diesen Abschnitt überspringen und LDAP später konfigurieren, aber einige der Funktionen von Files Advanced werden dann nicht zur Verfügung stehen.*

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

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

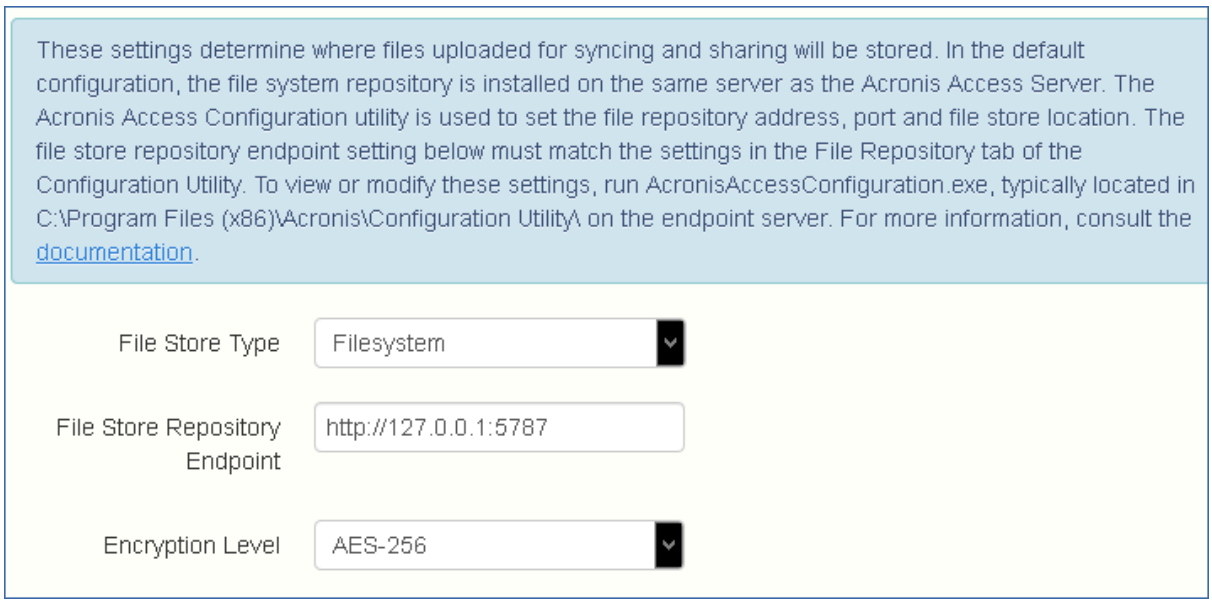
Lokaler Gateway Server



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

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

Datei-Repository



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

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

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

4.5 Clustering von Files Advanced

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

Weitere Informationen und Anweisungen zum Einrichten einer Cluster-Gruppe finden Sie im Artikel Cluster-Gruppen (S. 99).

Zwar empfiehlt sich der Einsatz der integrierten Cluster-Gruppen-Funktion, doch unterstützt Files Advanced auch das Microsoft Failover-Clustering. Weitere Informationen finden Sie im Artikel Ergänzendes Material (S. 180).

4.6 Lastenausgleich für Files Advanced

Files Advanced unterstützt den Lastenausgleich. Weitere Informationen finden Sie in den Artikeln Lastenausgleich für Files Advanced (S. 188),Installieren von Files Advanced in einer Konfiguration mit Lastenausgleich (S. 196) , Migrieren zu einer Konfiguration mit Lastenausgleich (S. 201) und Cluster-Gruppen (S. 99).

5 Upgrades

Themen

5.1 Upgrade von Files Advanced auf eine neuere Version

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

Hinweis: *Wenn Sie ein Upgrade für eine Version von Files Advanced vor Version 7.0 durchführen, wenden Sie sich an den Support von Acronis unter http://www.acronis.com/mobilitysupport/*

Hinweis: *Sehen Sie sich die Minimalen Hardware-Anforderungen (S. 23) an, bevor Sie ein Upgrade durchführen.*

Hinweis: *Abhängig von Ihrer Bereitstellung können einige der in diesem Artikel erwähnten Pfade von Ihren Pfaden abweichen. Aktualisierungen von vorherigen Versionen von Files Advanced und benutzerdefinierte Installationen können die Ordnerstrukturen Ihrer Bereitstellung beeinflussen.*

Sichern der wichtigen Komponenten

Der Apache Tomcat-Ordner

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:\Program Files (x86)\Acronis\Files Advanced\Common\`**.

Wir empfehlen Ihnen, die Datei **web.xml** vor dem Aktualisieren zu sichern. Ihre Datei **web.xml** wird beim Upgrade überschrieben. Unter der Version 7.1.2 und höher finden Sie unter **`C:\Program Files (x86)\Acronis\Files Advanced\Access Server\Web Application\WEB-INF\<timestamp>.previous.web.xml`** ein Backup. Wenn Sie spezifische Änderungen vorgenommen haben, die Sie beibehalten möchten, müssen Sie sie manuell aus der alten Datei kopieren und dann einfügen (ausgenommen Single Sign-On (S. 214)- die entsprechenden Änderungen bleiben erhalten).

Unnötige Überwachungsprotokolle entfernen

Wenn Sie nicht die automatische Entfernung von Protokollen (S. 129) eingerichtet haben, sind auf Ihrem Server möglicherweise viele Protokolle vorhanden, die den Sicherungsprozess verlangsamen. Es wird empfohlen, die älteren Protokolle zu exportieren und zu entfernen, bevor Sie mit dem Sichern der Datenbank fortfahren.

Die PostgreSQL-Datenbank

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

1. Öffnen Sie ein Eingabeaufforderungsfenster und navigieren Sie zum Ordner **`9.2\bin`** im PostgreSQL-Installationsverzeichnis.
   z. B. **`cd "C:\PostgreSQL\9.2\bin"`**
2. Sobald Sie als Verzeichnis für die Eingabeaufforderung den Ordner **bin** festgelegt haben, geben Sie die folgende Zeile ein:

   `pg_dump -U postgres -f mybackup.sql acronisaccess_production`
   Dabei ist **`mybackup.sql`** der gewünschte Dateiname für die von Ihnen erstellte Backup-Datei. Dies kann die vollständige Pfadangabe für den Speicherort einschließen, an dem die Backup-Datei erstellt werden soll, zum Beispiel: **`D:\Backups\mybackup.sql`**

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

3. Eine Zeile 'Password:' wird angezeigt. Geben Sie das postgres-Kennwort ein, das Sie während der Installation von Files Advanced 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

Die Gateway Server-Datenbank(en)

1. Wechseln Sie zu dem Server, auf dem Ihr Files Advanced Gateway Server installiert ist.
2. Navigieren Sie zu dem Ordner mit der Datenbank.

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

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

Die Files Advanced Konfigurationsdatei

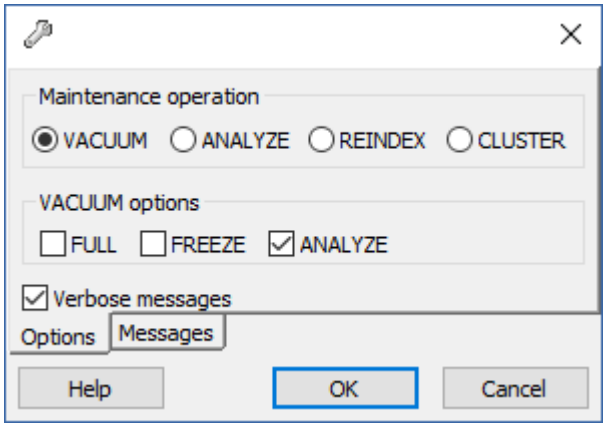
1. Navigieren Sie zum Files Advanced Installationsordner, der die Konfigurationsdatei enthält.

   Hinweis: *Der Standardspeicherort lautet:* ***`C:\Program Files (x86)\Acronis\Files Advanced\Access Server`***

2. Kopieren Sie die Datei **acronisaccess.cfg** und fügen Sie diese in einen sicheren Speicherort ein.

Die Datenbank vor dem Upgrade bereinigen

1. Öffnen Sie das Files Advanced PostgreSQL Administrator-Werkzeug (PgAdmin) und doppelklicken Sie auf **localhost**, um eine Verbindung zum Server herzustellen.
2. Klicken Sie mit der rechten Maustaste auf die **`acronisaccess_production`**-Datenbank, und wählen Sie **Wartung**.
3. Wählen Sie das Aktionsfeld **BEREINIGEN** und aktivieren Sie das Kontrollkästchen **ANALYSIEREN**.



   Warnung! *Wenn Ihre Datenbank sehr groß ist, kann die Bereinigung einige Zeit dauern. Dieser Prozess sollte während niedriger Serverauslastung durchgeführt werden.*

4. Wählen Sie **OK**.
5. Wenn der **Bereinigungs**prozess beendet wird, klicken Sie auf **Fertig**.
6. Schließen Sie das PostgreSQL-Administrator-Tool.

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 ausführbare Installationsdatei.

3. Drücken Sie **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. Überprüfen Sie, dass keine der Einstellungen im Konfigurationswerkzeug geändert wurde. Nach dem Überprüfen der Einstellungen drücken Sie **OK**, um das Konfigurationswerkzeug zu schließen und die Files Advanced Dienste zu starten.

5.2 Upgrade von mobilEcho 4.5 oder früheren Versionen

Für ein Upgrade von mobilEcho wenden Sie sich bitte an den technischen Support von Acronis unter http://www.acronis.de/mobilitysupport.

5.3 Upgrade von activEcho 2.7 oder früheren Versionen

Für ein Upgrade von activEcho wenden Sie sich bitte an den technischen Support von Acronis unter http://www.acronis.de/mobilitysupport.

5.4 Upgrade Gateway-Cluster

Um das Upgrade einer geclusterten Konfiguration von Files Advanced durchzuführen, müssen Sie sowohl für den Files Advanced Web Server als auch für die Gateway Server in der Cluster-Gruppe (S. 99) ein Upgrade durchführen.

Note: *Informationen zum Upgrade einer Microsoft Failover-Clustering-Konfiguration finden Sie im Abschnitt Ergänzendes Material (S. 180).*

Hinweis: *Anweisungen zum Upgrade von Files Advanced Web Server finden Sie unter Upgrade von Files Advanced auf eine neuere Version (S. 38).*

Sie müssen für jeden Gateway Server das folgende Upgrade-Verfahren durchführen:

Sehen Sie sich vor der Durchführung eines Upgrades unsere Artikel zum Thema Backup (S. 153) an, und sichern Sie Ihre Konfiguration.

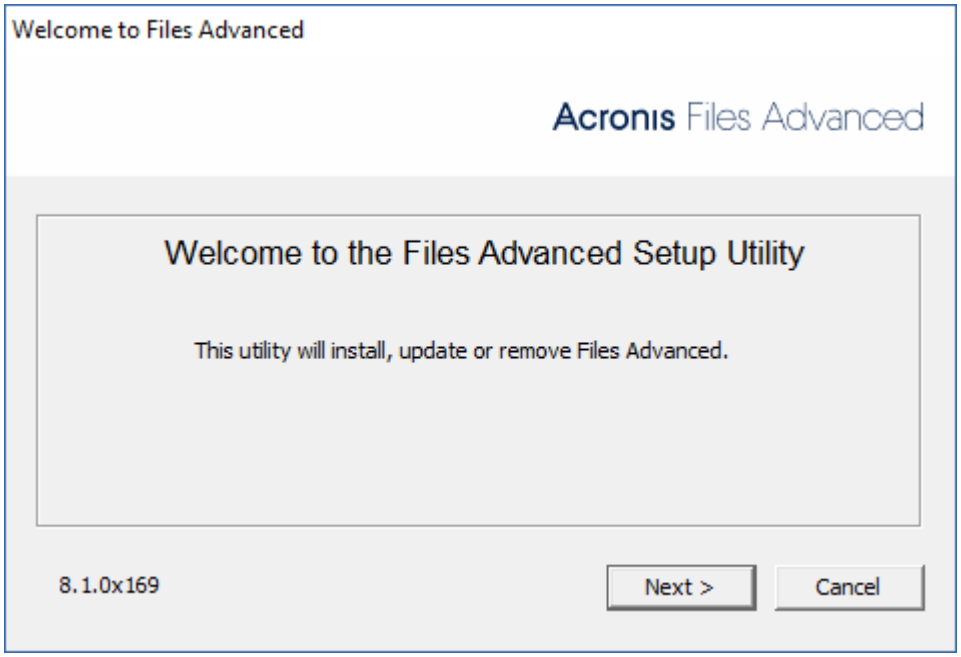
Hinweis: *Sehen Sie sich die Minimalen Hardware-Anforderungen (S. 23) an, bevor Sie ein Upgrade durchführen.*

Hinweis: *Abhängig von Ihrer Bereitstellung können einige der in diesem Artikel erwähnten Pfade von Ihren Pfaden abweichen. Aktualisierungen von vorherigen Versionen von Files Advanced und benutzerdefinierte Installationen können die Ordnerstrukturen Ihrer Bereitstellung beeinflussen.*

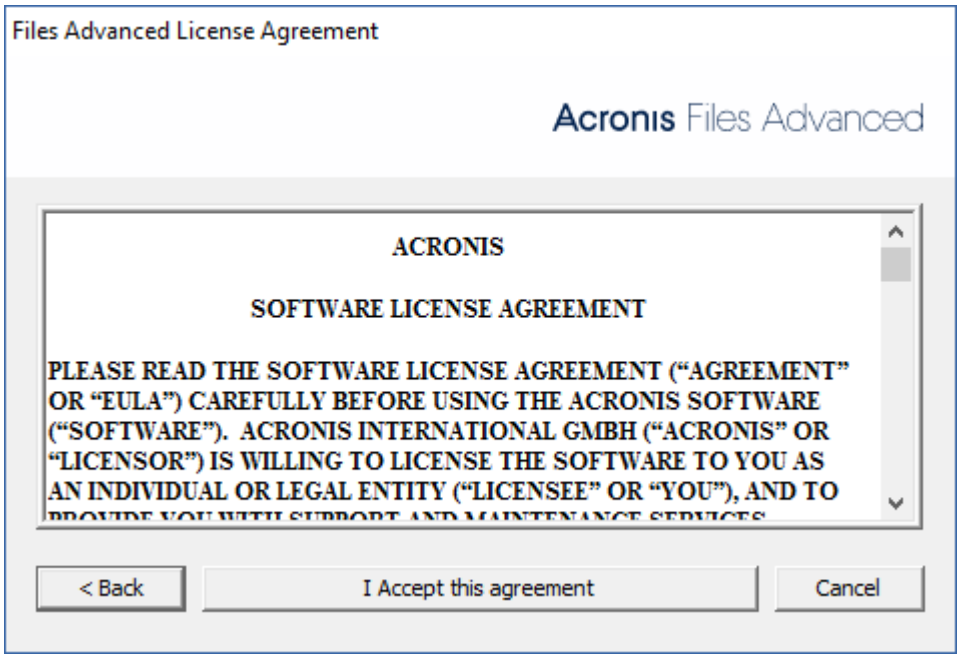
Upgrade eines Gateway Servers

Führen Sie das Files Advanced Installationsprogramm auf dem gewünschten Server aus.

1. Klicken Sie auf der Seite **Willkommen** auf **Weiter**.

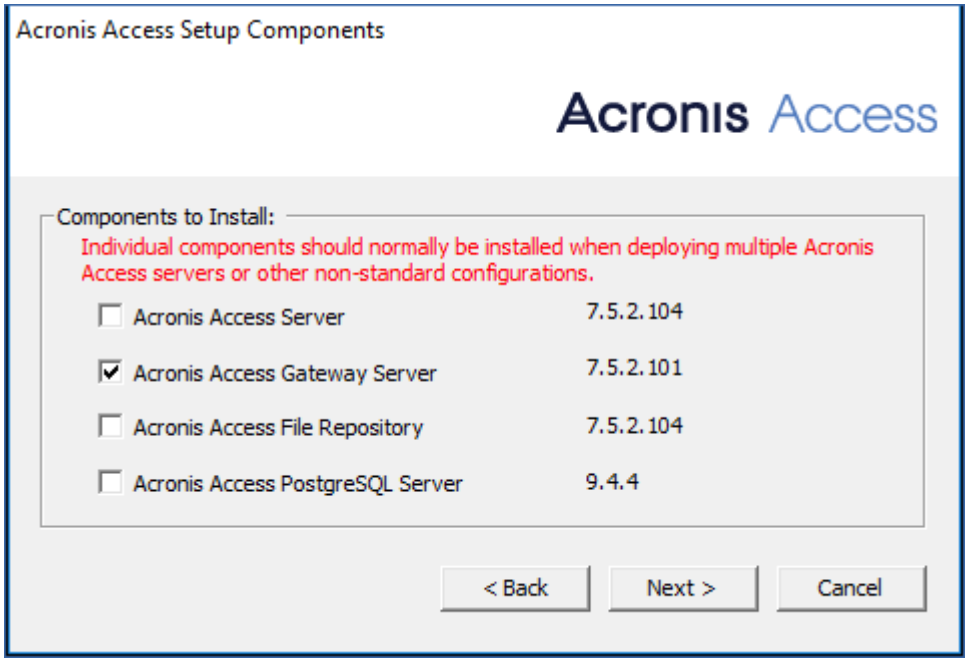


2. Lesen und akzeptieren Sie die Lizenzvereinbarung.



3.
4. Klicken Sie auf **Benutzerdefiniert**.

5. Wählen Sie nur die Komponente **Files Advanced Gateway Server** aus und klicken Sie auf **Weiter**.



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

5.5 Upgrade von Lastenausgleichskonfigurationen

Dieser Leitfaden ist für Einrichtungen, die lastenausgleichend für Files Advanced und alle zugehörigen Komponenten sind.

Sehen Sie sich vor der Durchführung eines Upgrades unsere Artikel zum Thema Backup (S. 153) an, und sichern Sie Ihre Konfiguration.

Hinweis: *Sehen Sie sich die Minimalen Hardware-Anforderungen (S. 23) an, bevor Sie ein Upgrade durchführen.*

Hinweis: *Abhängig von Ihrer Bereitstellung können einige der in diesem Artikel erwähnten Pfade von Ihren Pfaden abweichen. Aktualisierungen von vorherigen Versionen von Files Advanced und benutzerdefinierte Installationen können die Ordnerstrukturen Ihrer Bereitstellung beeinflussen.*

Themen

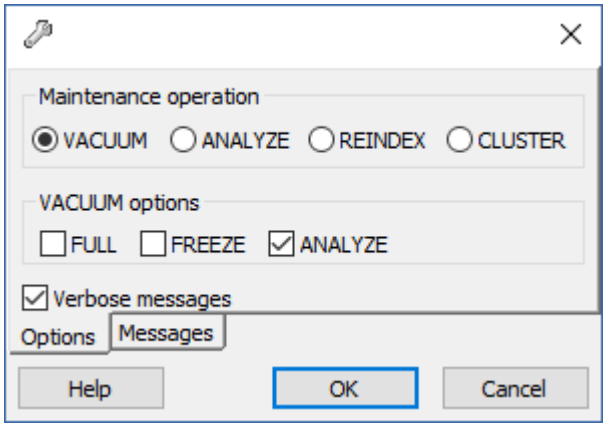
Wählen Sie, welcher der Server-Rechner von Files Advanced Web Server als **Primärserver** dienen soll. Dieser Computer ist nur dahingehend der **Primärknoten**, als dass er zuerst aktualisiert wird und er alle Änderungen/Einstellungen zur PostgreSQL-Datenbank migriert. Wenn die Datenbank sehr groß ist, können diese Migrationen mehrere Minuten dauern.

Warnung!: *Aktualisieren Sie andere Tomcat-Server erst,* ***NACHDEM*** *der* ***Primärserver*** *aktualisiert wurde und Sie sich bei der Weboberfläche anmelden können, um einen Test durchzuführen.*

Bereinigen der Datenbank

Auf diese Weise werden der Backup- und der Wiederherstellungsvorgang durch die Optimierung Ihrer Datenbank beschleunigt.

1. Öffnen Sie das Files Advanced PostgreSQL Administrator-Werkzeug (PgAdmin) und doppelklicken Sie auf **localhost**, um eine Verbindung zum Server herzustellen.
2. Klicken Sie mit der rechten Maustaste auf die `acronisaccess_production`-Datenbank, und wählen Sie **Wartung**.
3. Wählen Sie das Aktionsfeld **BEREINIGEN** und aktivieren Sie das Kontrollkästchen **ANALYSIEREN**.



Warnung! *Wenn Ihre Datenbank sehr groß ist, kann die Bereinigung einige Zeit dauern. Dieser Prozess sollte während niedriger Serverauslastung durchgeführt werden.*

4. Wählen Sie **OK**.
5. Wenn der **Bereinigungs**prozess beendet wird, klicken Sie auf **Fertig**.
6. Schließen Sie das PostgreSQL-Administrator-Tool.

Detaillierte Informationen zu den Backup- und Wiederherstellungsprozessen finden Sie im Artikel Backup und Wiederherstellung von Files Advanced ***(S. 153).***

Backup der PostgreSQL-Datenbank erstellen

1. Stoppen Sie alle Files Advanced Tomcat-Dienste.
2. Öffnen Sie die PostgreSQL Administratorapplikation von Files Advanced und stellen Sie eine Verbindung zum Datenbankserver her. Sie werden ggf. aufgefordert, das Kennwort für den `postgres` Benutzer einzugeben.
3. Erweitern Sie **Datenbanken** und klicken Sie mit der rechten Maustaste auf die Datenbank **acronisaccess_production**.
4. Wählen Sie **Wartung** und das Aktionsfeld **Bereinigen** und aktivieren Sie dann das Kästchen **ANALYSIEREN**. Wählen Sie **OK**.
5. Erweitern Sie die Datenbank und dann **Schemas** und **Öffentlich**. Notieren Sie die Anzahl im Abschnitt **Tabellen**. Dies kann Ihnen bei der Überprüfung helfen, ob die Datenbankwiederherstellung nach einem Recovery erfolgreich war.
6. Schließen Sie die PostgreSQL-Administratorapplikation und öffnen Sie eine Eingabeaufforderung mit erweiterten Benutzerrechten.

7. Navigieren Sie in der Eingabeaufforderung zum PostgreSQL-Verzeichnis 'bin'.

   Beispiel: `cd "C:\Program Files(x86)\Acronis\Access\Common\PostgreSQL\9.3\bin"`

8. Geben Sie den folgenden Befehl ein: `pg_dumpall --host localhost --port 5432 --username postgres --file alldbs.sql`
   - `alldbs.sql` ist der Dateiname des Backups. Es wird im PostgreSQL-Verzeichnis 'bin' gespeichert. Sie können mit dem obigem Befehl auch einen anderen Pfad zum Speichern des Backups eingeben – ändern Sie z.B. den letzten Teil des obigen Befehls wie folgt: `--file D:\Backups\alldbs.sql`
   - Wenn Sie nicht den Standard-Port verwenden, müssen Sie statt **5432** die richtige Portnummer eingeben.
   - Wenn Sie nicht das Standard-Administratorkonto von PSQL, `postgres`, verwenden, muss im obigen Befehl `postgres` durch den Namen des Administratorkontos ersetzt werden.
   - Während dieses Vorgangs werden Sie mehrmals aufgefordert, das `postgres` -Kennwort des Benutzers einzugeben. Geben Sie bei jeder Aufforderung das Kennwort ein und drücken Sie die Eingabetaste.

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

9. Kopieren Sie die Backup-Datei an einen sicheren Speicherort.
10. Beenden Sie **NICHT** den Postgres-Dienst, da PostreSQL selbst nicht aktualisiert wird.

Backup weiterer wichtiger Komponenten erstellen

1. Erstellen Sie ein Backup der Tomcat-Ordner **conf** und **logs**. Standardmäßig unter: `C:\Program Files (x86)\Acronis\Files Advanced\Common\apache-tomcat-<version>\`

   Hinweis: *Ersetzen Sie <version> durch die korrekte Version Ihrer Files Advanced Tomcat-Instanz, z. B.* `\apache-tomcat.70.0.70\`

2. Erstellen Sie ein Backup der Datei **acronisaccess.cfg**. Standardmäßig unter: `C:\Program Files (x86)\Acronis\Files Advanced\Access Server`
3. Erstellen Sie ein Backup aller **web.xml**-Dateien (standardmäßig unter `C:\Program Files (x86)\Acronis\Files Advanced\Access Server\Web Application\WEB-INF\`).
4. Erstellen Sie ein Backup der Datei **newrelic.yml**. Der Speicherort ist der von Ihnen gewählte Speicherort. Sie können diesen Schritt überspringen, wenn Sie die New Relic-Überwachung nicht verwenden.

Backup der Gateway-Server-Datenbanken erstellen

1. Beenden Sie alle Gateway-Services von Files Advanced.
2. Greifen Sie auf die Gateway Datenbank-Ordner zu, standardmäßig unter `C:\Program Files (x86)\Acronis\Files Advanced\Gateway Server\database`.
3. Erstellen Sie ein Backup der Datei **mobilEcho.sqlite3**.
4. Wiederholen Sie diese Schritte für jeden Gateway Server.

Halten Sie alle Files Advanced-Dienste auf allen Rechnern an.

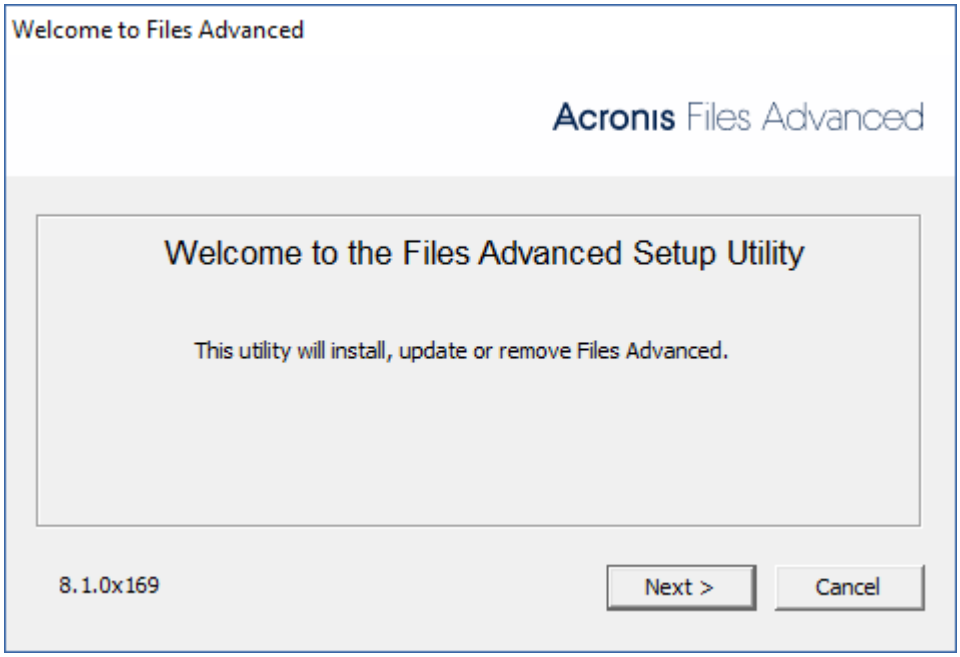
Es ist äußerst wichtig, dass alle Files Advanced Tomcat-Dienste vor einem Upgrade angehalten werden. Wir empfehlen, auch alle anderen Files Advanced-Dienste anzuhalten, der PostgreSQL-Dienst muss jedoch weiterhin ausgeführt werden.

Aktualisieren Sie, ungeachtet des Speicherorts, zuerst das Datei-Repository.

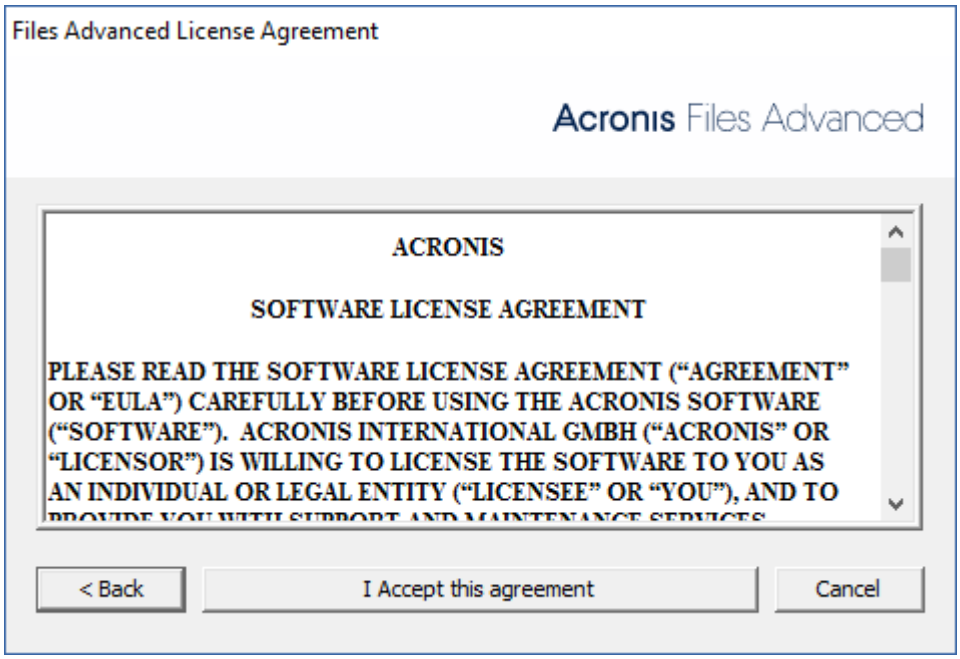
1. Kopieren Sie das Installationsprogramm von Files Advanced auf den Computer mit der Datei-Repository-Komponente und starten Sie die Installation.

   Hinweis: *Wenn Sie über mehrere Datei-Repository-Dienste verfügen, wiederholen Sie diese Schritte für alle Repositorys, bevor Sie mit den anderen Komponenten fortfahren.*

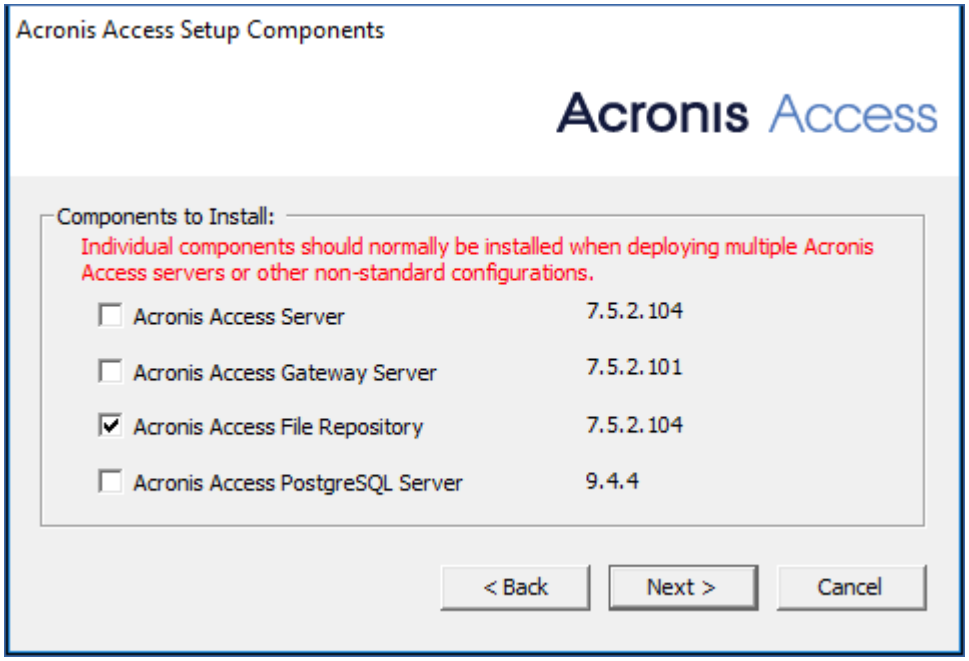
2. Klicken Sie im Fenster **Willkommen** auf **Weiter**.



3. Akzeptieren Sie die Lizenzvereinbarung.

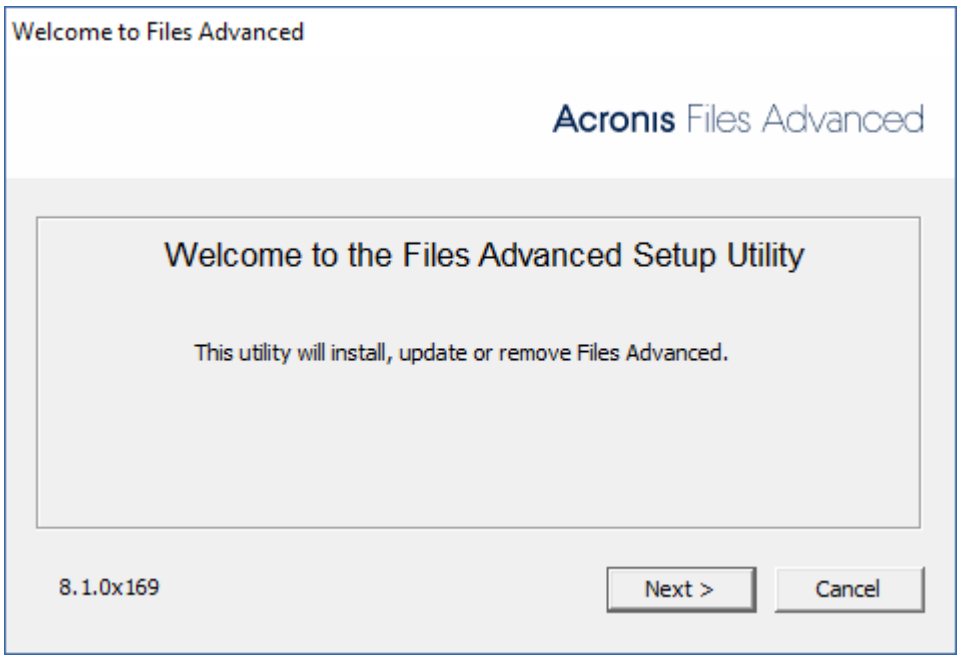


4. Wählen Sie **Benutzerdefiniert...** und anschließend nur das **Files Advanced Datei-Repository** aus, das aktualisiert werden soll.

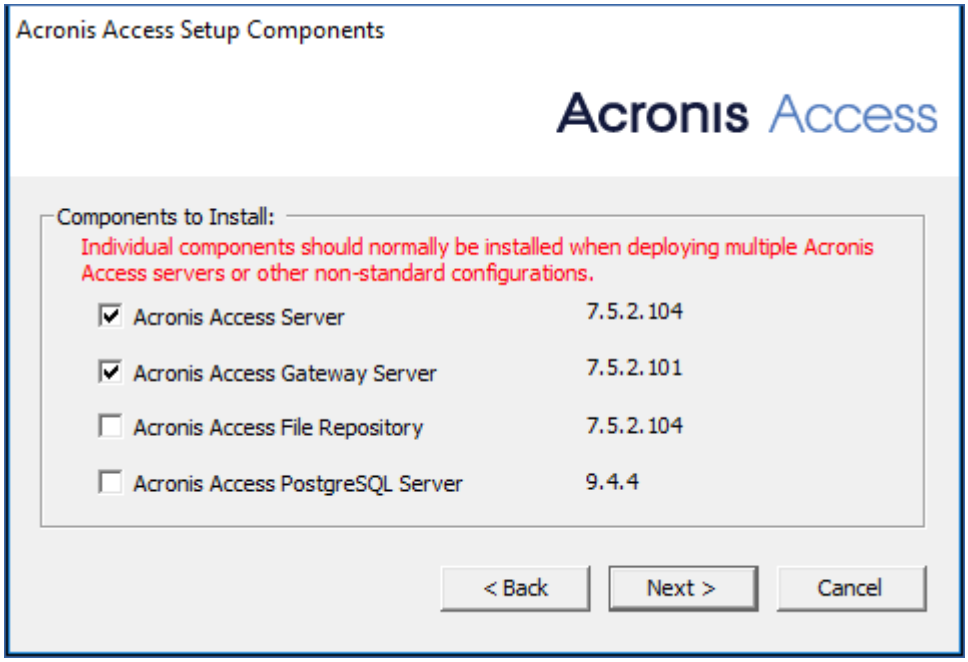


5. Klicken Sie auf **Weiter**, überprüfen Sie, was installiert werden soll, und klicken Sie auf **Installieren**.
6. Klicken Sie nach der Aktualisierung auf **Beenden**. Wenn das Konfigurationsdienstprogramm startet, klicken Sie auf **OK**.
7. Fahren Sie fort, indem Sie den **Primärserver** von Files Advanced Web Server auf dem entsprechenden Computer aktualisieren.

1. Kopieren Sie das Files Advanced Advanced-Installationsprogramm auf den Computer mit dem **primären** Files Advanced Web Server.
2. Starten Sie das Files Advanced Installationsprogramm auf dem **Primärknoten**.



3. Klicken Sie im Begrüßungsbildschirm auf **Weiter** und dann auf **Benutzerdefiniert**. Dadurch können Sie nur die notwendigen Dienste upgraden, die sich bereits auf dem Computer befinden, ohne weitere zu installieren.
4. Wählen Sie die Files Advanced Dienste, die Sie aktualisieren möchten. Wählen Sie nur den Files Advanced Server und die Komponenten, die sich bereits auf dem Computer befinden.



Hinweis: *Das Installationsprogramm führt kein Update von PostgreSQL durch. Wenn Sie ein Update Ihrer PostgreSQL-Version durchführen möchten, lesen Sie bitte unseren Artikel zu diesem Thema (S. 175) und wenden Sie sich an den Acronis-Support, ehe Sie fortfahren.*

5. Drücken Sie **Installieren** und lassen Sie das Installationsprogramm den Vorgang abschließen und das **Konfigurationsdienstprogramm** starten.

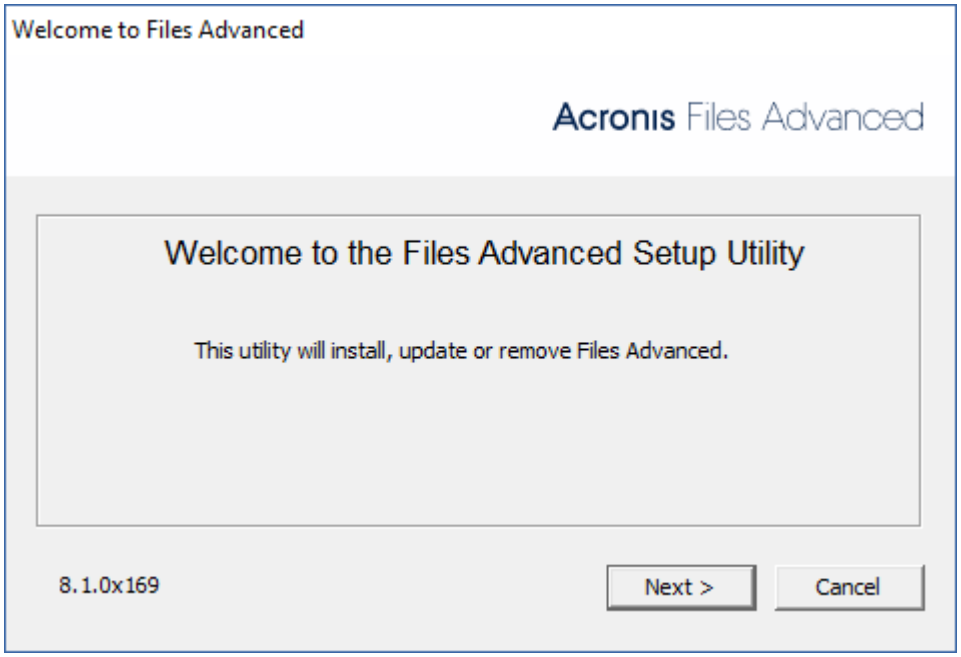
Hinweis: *Ändern Sie keine Einstellungen des **Konfigurationsdienstprogramms**! Geänderte Einstellungen können zu Problemen mit Ihrer Konfiguration führen.*

6. Nachdem das Konfigurationsdienstprogramm alle notwendigen Dienste gestartet hat und die Datenbankmigrationen beendet sind, überprüfen Sie, ob die Files Advanced Weboberfläche des **Primärservers** ordnungsgemäß funktioniert. Ein Webbrowser mit dem Anmeldebildschirm für den Files Advanced Server wird automatisch gestartet.
7. Melden Sie sich als Administrator an und stellen Sie sicher, dass die Einstellungen gleich sind und keine Änderungen oder Probleme vorliegen.
8. Lassen Sie diese Instanz von Files Advanced laufen, während Sie alle anderen Komponenten aktualisieren.

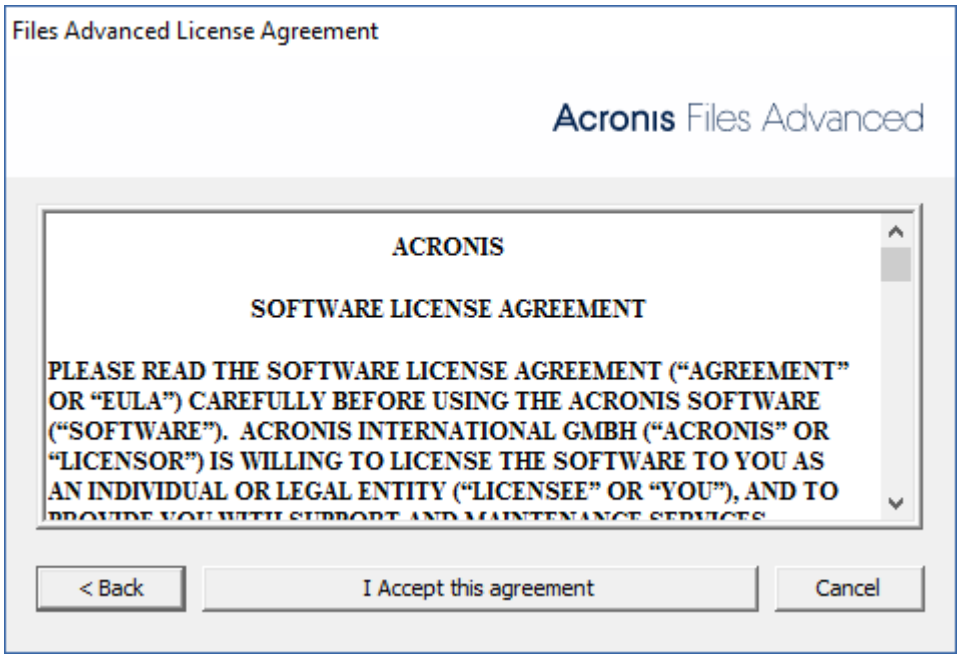
Warnung!: *Aktualisieren oder starten Sie andere Files Advanced Tomcat-Server ERST, wenn der **Primärserver** wieder betriebsbereit ist und Sie überprüft haben, dass er ordnungsgemäß funktioniert.*

1. Kopieren Sie das Files Advanced Advanced-Installationsprogramm auf einen Computer mit nur einem Gateway Server und führen Sie die Installation durch.

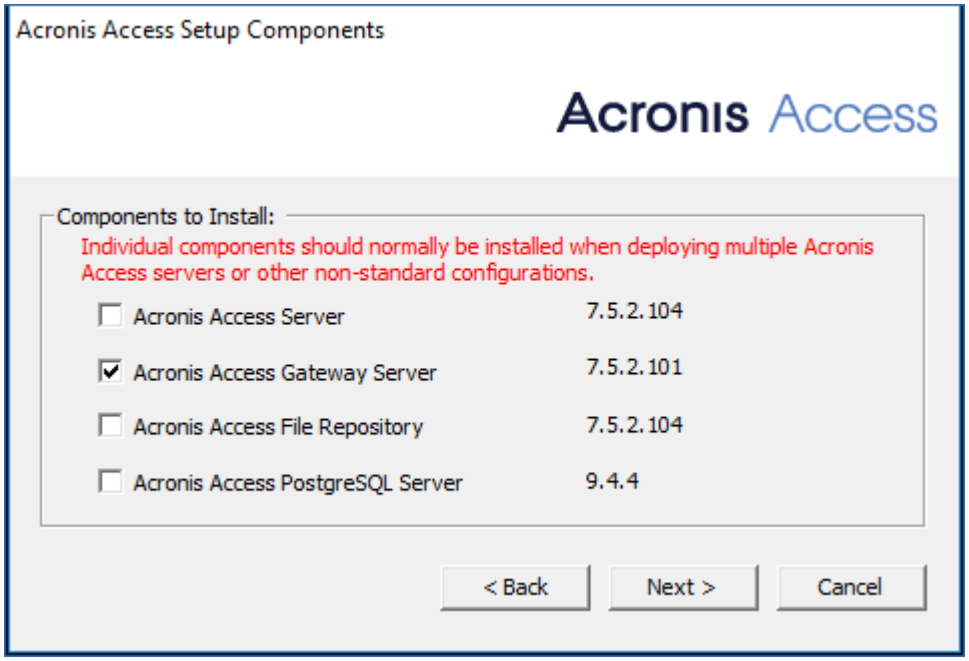
2. Klicken Sie im Begrüßungsbildschirm auf **Weiter**.



3. Akzeptieren Sie die Lizenzvereinbarung.



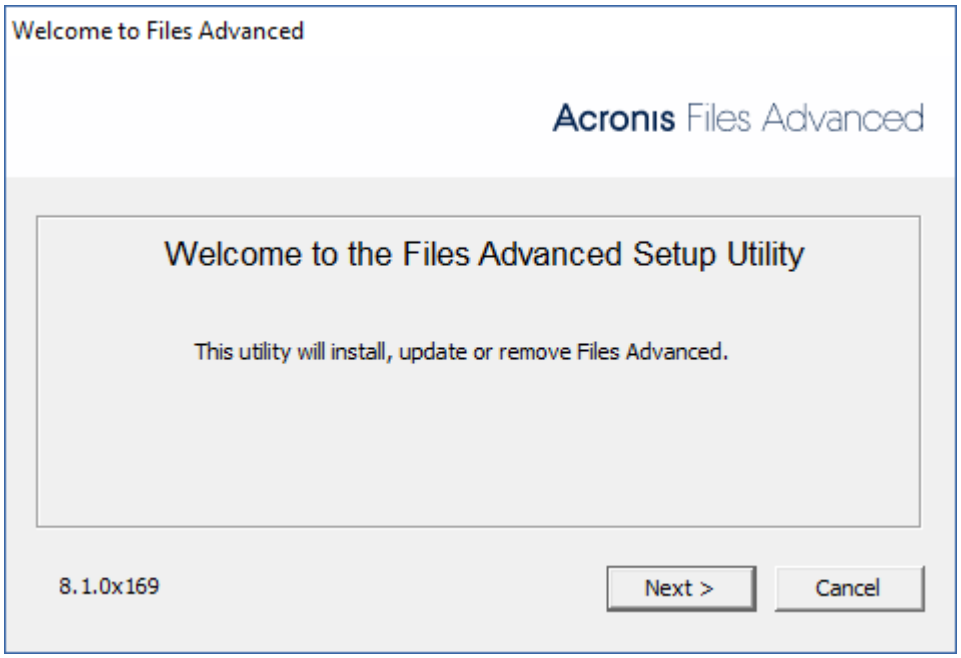
4. Wählen Sie **Benutzerdefiniert...** und anschließend nur den Files Advanced Gateway Server aus, der aktualisiert werden soll.



5. Klicken Sie auf **Weiter**, überprüfen Sie, was installiert werden soll, und klicken Sie auf **Installieren**.
6. Klicken Sie nach der Aktualisierung auf **Beenden**. Wenn das Konfigurationsdienstprogramm startet, klicken Sie auf **OK**.

Nachdem Sie den Files Advanced-**Primärknoten**, alle Datei-Repository-Server und alle Gateway Server erfolgreich aktualisiert haben, fahren Sie fort, indem Sie die restlichen Files Advanced-Server aktualisieren.

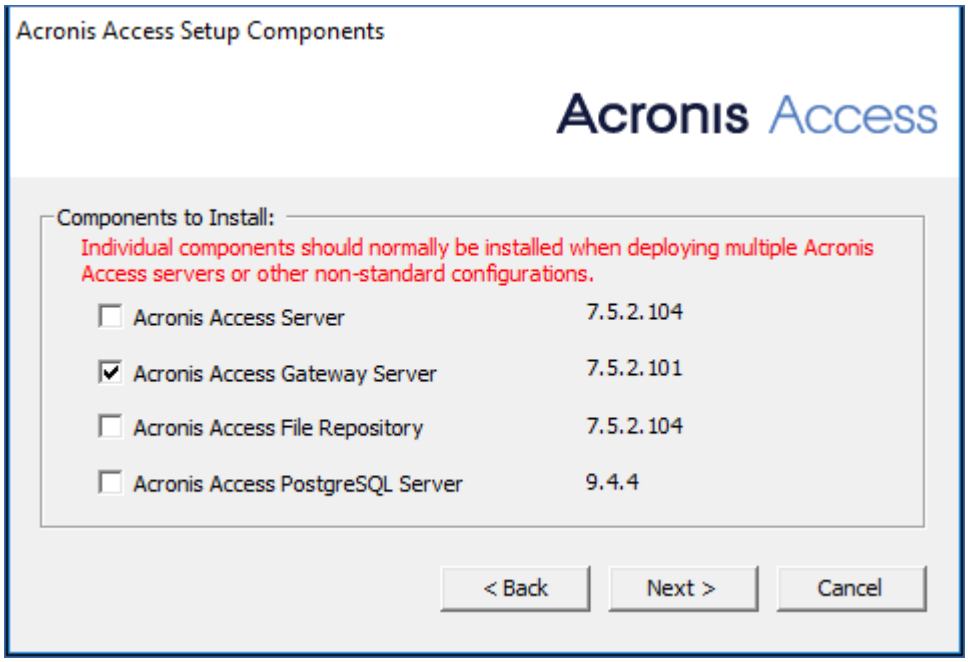
1. Kopieren Sie den Files Advanced-Installer in den gewünschten Knoten und starten Sie ihn.



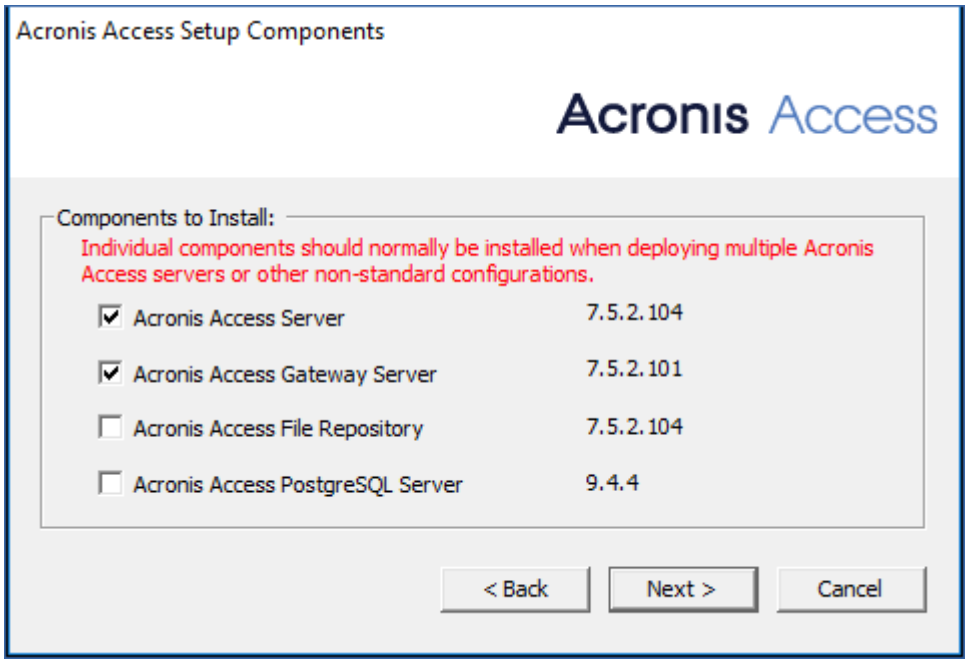
2. Klicken Sie im Begrüßungsbildschirm auf **Weiter** und dann auf **Benutzerdefiniert**. Dadurch können Sie nur die notwendigen Dienste upgraden, die sich bereits auf dem Computer befinden, ohne weitere zu installieren.

3. Wählen Sie einen Files Advanced-Dienst, den Sie upgraden möchten. Wählen Sie nur diejenigen, die sich bereits auf dem Computer befinden.

   Beispiel: Falls nur ein Gateway Server installiert ist, wählen Sie nur die Gateway Server-Komponente im Installationsprogramm aus.



   Beispiel: Wenn sowohl ein Gateway als auch ein Files Advanced Server vorhanden ist, wählen Sie beide aus.



   Hinweis: *Das Installationsprogramm führt kein Update von PostgreSQL durch. Wenn Sie ein Update Ihrer PostgreSQL-Version durchführen möchten, lesen Sie bitte unseren Artikel zu diesem Thema (S. 175) und wenden Sie sich an den Acronis-Support, ehe Sie fortfahren.*

4. Drücken Sie **Installieren** und lassen Sie das Installationsprogramm den Vorgang abschließen und das **Konfigurationsdienstprogramm** starten.

   Hinweis: *Ändern Sie keine Einstellungen des* ***Konfigurationsdienstprogramms****! Geänderte Einstellungen können zu Problemen mit Ihrer Konfiguration führen.*

5. Sobald das Konfigurationsdienstprogramm alle notwendigen Dienste startet, verifizieren Sie, das die Files Advanced-Komponenten auf diesem Knoten wie erwartet arbeiten.

6 Mobiler Zugriff

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

Themen

6.1 Begrifflichkeiten

Mobile Clients von Files Advanced stellen direkt eine Verbindung zu Ihrem Server her und verwenden keinen Dienst eines Drittanbieters, sodass Sie weiterhin die Kontrolle behalten. Files Advanced Server können auf demselben Netzwerk installiert werden wie vorhandene Dateiserver, die es iPads, iPhones, Windows- und Android-Geräten erlauben, auf die Dateien zuzugreifen, die sich auf diesem Netzwerk befinden. Dies sind in der Regel dieselben Dateien, die bereits für PCs über die Windows-Dateifreigabe und für Mac-Computer über Files Connect Server zur Verfügung stehen.

Clients greifen über ihr Active Directory-Benutzerkonto auf Files Advanced Server zu. In Files Advanced müssen keine zusätzlichen Konten konfiguriert werden. Die Files Advanced App unterstützt darüber hinaus den Dateizugriff mit lokalen Computerkonten, die auf dem Windows-Server konfiguriert wurden, auf dem Files Advanced ausgeführt wird. Dies ist für den Fall wichtig, dass Sie Nicht-AD-Benutzern Zugriff gewähren müssen. Für die im Folgenden beschriebenen Funktionen zur Client-Verwaltung sind AD-Benutzerkonten erforderlich.

Eine minimale Bereitstellung besteht aus einem einzigen Windows-Server, auf dem eine Standardinstallation von Files Advanced ausgeführt wird. Die Standardinstallation umfasst die installierte Files Advanced Server-Komponente und den installierten lokalen Files Advanced Gateway Server. In diesem Szenario können Files Advanced-Benutzer Verbindungen mit diesem einzelnen Dateiserver herstellen, außerdem ist eine Client-Verwaltung für Mobilgeräte möglich. Ist die Client-Verwaltung nicht erforderlich, können Datenquellen auf dem lokalen Gateway Server eingerichtet werden. Mobile Clients von Files Advanced können so auf diese Datenquellen zugreifen, aber die Benutzer behalten weiterhin die Kontrolle über ihre App-Einstellungen.

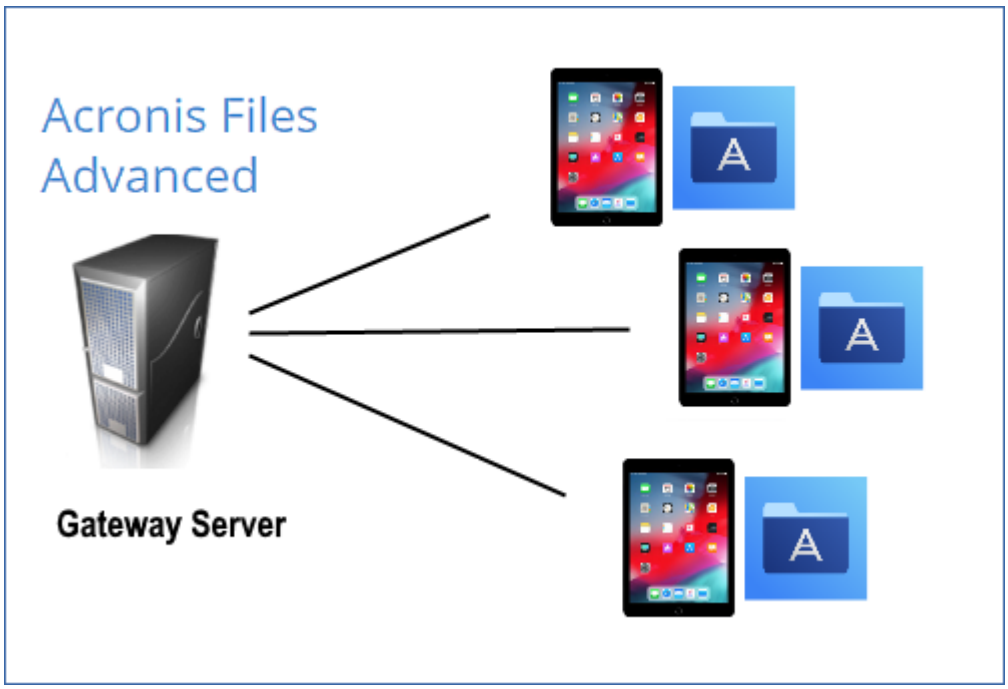


Abb. 1. Einzelner Files Advanced Server mit einem lokalen Gateway Server

Dem Netzwerk können später beliebig viele Gateway Server hinzugefügt und für den Zugriff über die Access Clients konfiguriert werden.

Hinweis: *Einzelheiten zur Installation von Files Advanced finden Sie im Bereich Installation (S. 22) dieser Anleitung. Die Konfiguration von Gateway Servern und Datenquellen wird im Bereich Mobiler Zugriff (S. 53) erläutert.*

Wenn Sie die Mobile Clients remote verwalten möchten, können Sie mit der Files Advanced-Verwaltung Richtlinien jeweils pro Active Directory-Benutzer oder -Gruppe erstellen. Es ist nur ein Files Advanced Server erforderlich. Diese Richtlinien können:

- Allgemeine Einstellungen der Applikation konfigurieren
- Server, Ordner und Basisverzeichnisse zuweisen, die in der Client-App angezeigt werden sollen
- Mit Dateien durchführbare Aktionen einschränken
- Die Apps von Drittanbietern einschränken, in denen Dateien von Files Advanced geöffnet werden können
- Sicherheitseinstellungen festlegen (Häufigkeit der Anmeldung beim Server, Kennwort zum Sperren der Applikation usw.)
- Die Möglichkeit zum Speichern von Dateien auf dem Gerät deaktivieren
- Die Möglichkeit deaktivieren, Files Advanced Dateien in iTunes-Sicherungen aufzunehmen

- Kennwörter von Benutzern zum Sperren der Applikation remote zurücksetzen
- Eine Remote-Löschung der lokalen Daten und Einstellungen der Mobile-App durchführen
- Und viele weitere Konfigurations- und Sicherheitsoptionen

Eine typische netzwerkbasierte Client-Verwaltung besteht aus einem Server, auf dem die Komponenten Files Advanced Server und Files Advanced Gateway Server installiert sind, sowie einigen weiteren Gateway Servern, die als Dateiserver fungieren. In diesem Szenario sind alle mobile Clients so konfiguriert, dass sie vom Files Advanced Server verwaltet werden. Sie kontaktieren diesen Server bei jedem Start der Files Advanced Applikation, um gegebenenfalls nach Änderungen in den Einstellungen zu suchen, zurückgesetzte Kennwörter zum Sperren der Applikation zu akzeptieren und Befehle zum standortfernen Löschen auszuführen.

Files Advanced Clients können in ihrer Verwaltungsrichtlinie eine Liste von Servern, bestimmte Ordner in freigegebenen Volumes und Basisverzeichnisse zugewiesen werden. Diese Ressourcen erscheinen automatisch in der Files Advanced 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. 55) und Mobile Geräte verwalten (S. 119).*

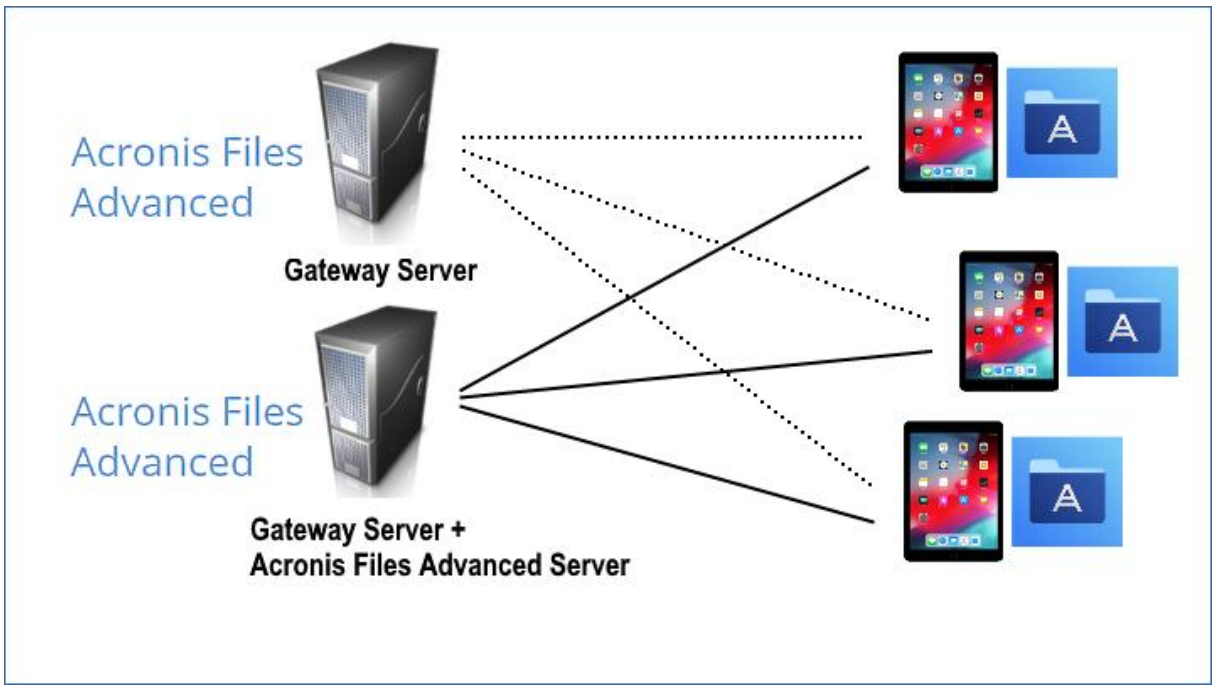


Abb. 2. Ein Gateway Server, ein Gateway Server + Files Advanced Server

6.2 Richtlinien

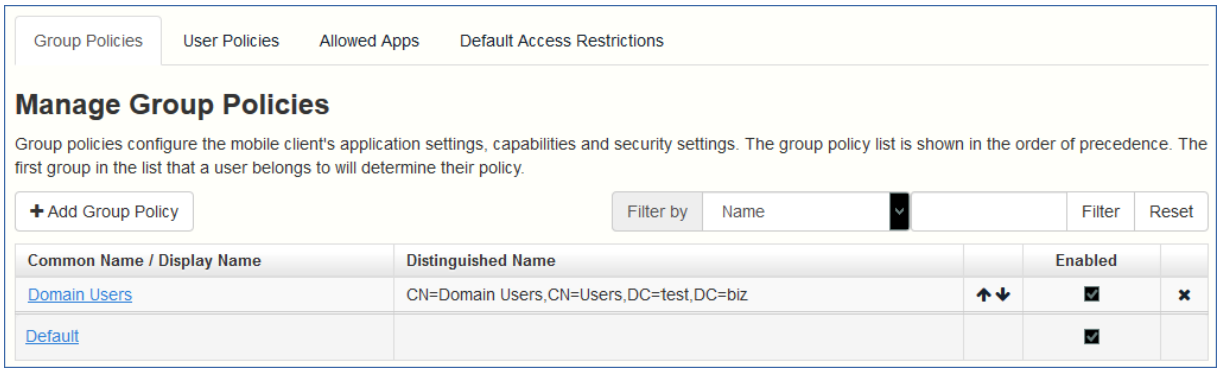
Files Advanced ermöglicht die Zuweisung von Richtlinien zu Active Directory-Gruppen. Gruppenrichtlinien erfüllen normalerweise die meisten oder alle Anforderungen der Client-Verwaltung. Die Gruppenrichtlinienliste wird in der Reihenfolge der Priorität angezeigt, d.h., die erste Gruppe in der Liste besitzt die höchste Priorität. Wenn Benutzer den Files Advanced-Server

kontaktieren, werden ihre Einstellungen durch die einzelne Gruppenrichtlinie mit der höchsten Priorität bestimmt, deren Mitglied sie sind.

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

Tipps zur Gruppenverwaltung

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



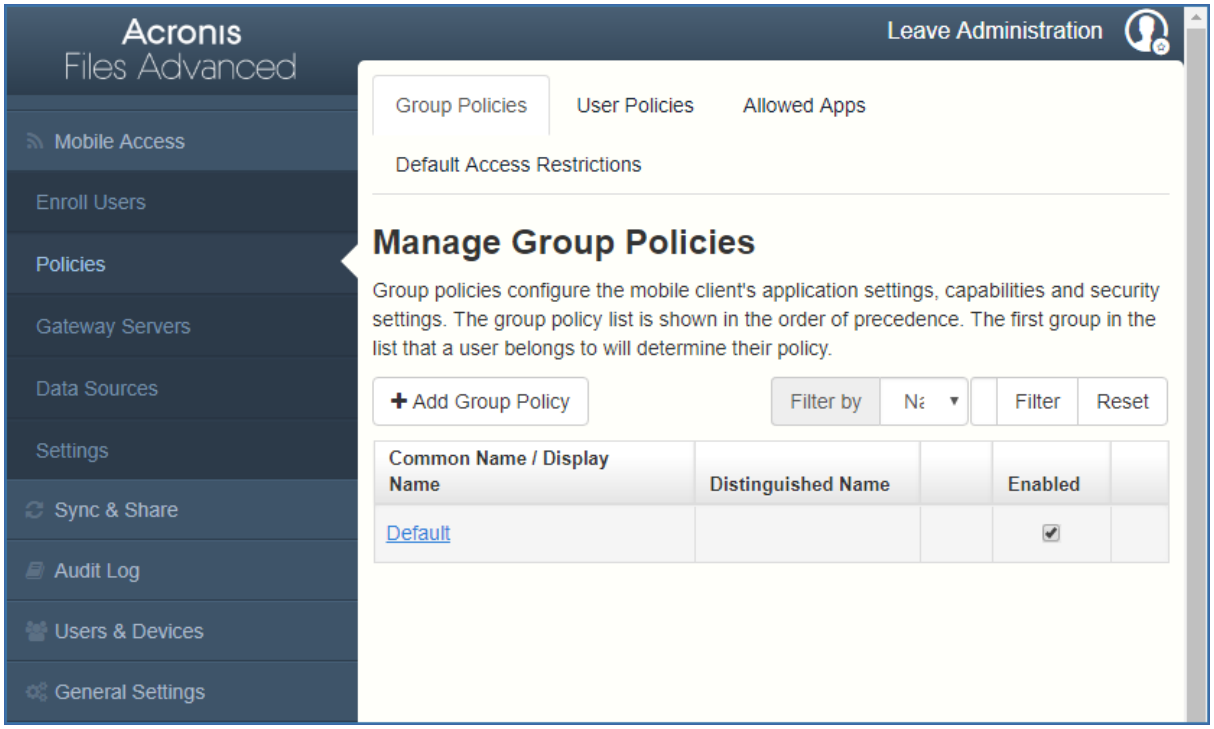
Themen

6.2.1 Eine neue Richtlinie hinzufügen

So fügen Sie eine neue Gruppenrichtlinie hinzu:

1. Öffnen Sie die Registerkarte **Gruppenrichtlinien**.

2. Klicken Sie auf die Schaltfläche **Neue Richtlinie hinzufügen**, um eine neue Gruppenrichtlinie hinzuzufügen. Die Seite **Eine neue Gruppenrichtlinie hinzufügen** wird geöffnet.

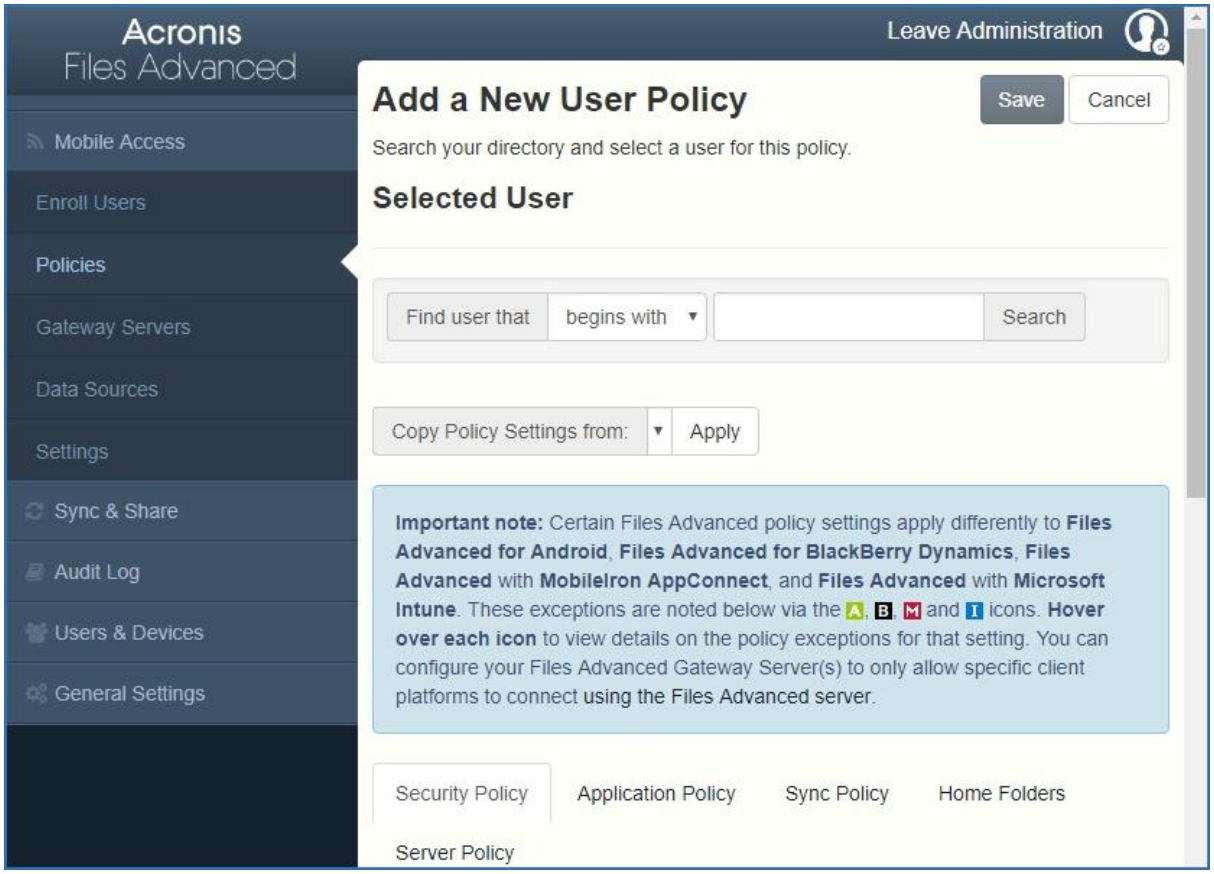


3. Geben Sie im Feld **Gruppe suchen** den Active Directory-Gruppennamen, für den Sie eine Richtlinie erstellen möchten, ganz oder teilweise ein. Die Suche nach Active Directory-Gruppen können Sie mit den Einschränkungen '**beginnt mit**' oder '**enthält**' ausführen. Suchvorgänge mit der Einschränkung 'beginnt mit' sind viel schneller als solche mit 'enthält'.
4. Klicken Sie auf **Suche** und klicken Sie in den aufgeführten Ergebnissen auf den gewünschten Gruppennamen.
5. Nehmen Sie die erforderlichen Konfigurationen auf den jeweiligen Registerkarten vor (Sicherheit (S. 60), Applikation (S. 63), Synchronisierung (S. 69), Basisordner (S. 71) und Server (S. 72)) und drücken Sie **Speichern**.

So fügen Sie eine neue Benutzerrichtlinie hinzu:

1. Öffnen Sie die Registerkarte **Benutzerrichtlinien**.

2. Klicken Sie auf die Schaltfläche **Neue Richtlinie hinzufügen**, um eine neue Benutzerrichtlinie hinzuzufügen. Die Seite **Eine neue Benutzerrichtlinie hinzufügen** wird geöffnet.



3. Geben Sie im Feld **Benutzer suchen** den Active Directory-Benutzernamen, für den Sie eine Richtlinie erstellen möchten, ganz oder teilweise ein. Die Suche nach Active Directory-Benutzern können Sie mit den Einschränkungen '**beginnt mit**' oder '**enthält**' ausführen. Suchvorgänge mit der Einschränkung 'beginnt mit' sind viel schneller als solche mit 'enthält'.
4. Klicken Sie auf **Suche** und klicken Sie in den aufgeführten Ergebnissen auf den gewünschten Benutzernamen.
5. Nehmen Sie die erforderlichen Konfigurationen auf den jeweiligen Registerkarten vor (Sicherheit (S. 60), Applikation (S. 63), Synchronisierung (S. 69), Basisordner (S. 71) und Server (S. 72)) und drücken Sie **Speichern**.

6.2.2 Richtlinien ändern

Bestehende Richtlinien können jederzeit geändert werden. Änderungen an Richtlinien werden auf den entsprechenden Mobile-App-Benutzer angewandt, sobald ein Benutzer die Mobile-App das nächste Mal startet.

Anforderungen bezüglich der Verbindung

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

So ändern Sie eine Gruppenrichtlinie:

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

So ändern Sie eine Benutzerrichtlinie:

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

6.2.3 Richtlinieneinstellungen

Themen

6.2.3.1 Sicherheitsrichtlinie

Security Policy | Application Policy | Sync Policy | Home Folders | Server Policy

App Password Creation: B M I

- (•) Optional
- ( ) Disabled
- ( ) Required

App Will Lock: Immediately upon exit

[ ] Allow User to Change This Setting

Minimum Password Length: 0

Minimum Number of Complex Characters (such as $,&,!): 0

[ ] Require One or More Letter Characters

[ ] Mobile client app will be wiped after 10 failed app password attempts

[ ] Wipe or Lock After Loss of Contact

Mobile client app will be locked after 30 days of failing to contact this client's Files Advanced server

[ ] Warn user starting 5 days beforehand

App Crash Reporting:

- (•) Never send reports
- ( ) Allow user to choose to send reports
- ( ) Always send reports

[x] Allow iTunes and iCloud to Back up Locally Stored Files Advanced Files A B

[ ] User Can Remove Mobile Client from Management

[ ] Wipe All Files Advanced Data on Removal

- **App-Kennwort erstellen** – Die mobile-Applikation kann mit einem Sperrkennwort versehen werden, das eingegeben werden muss, wenn die Applikation gestartet wird.
  - **Optional** – Diese Einstellung zwingt den Benutzer nicht zum Konfigurieren eines Sperrkennworts für die Applikation, aber er kann ein Kennwort über das Menü **Einstellungen** in der App festlegen, wenn dies gewünscht ist.
  - **Deaktiviert** – Diese Einstellung deaktiviert die Möglichkeit, ein Sperrkennwort für die Applikation über das Menü **Einstellungen** in der App zu konfigurieren. Dies kann nützlich sein

bei gemeinsam genutzten mobilen Geräten, wenn Sie nicht wollen, dass einer der Benutzer ein Kennwort festlegt und damit den Zugang zur mobile-App für andere Benutzer sperrt.

- **Erforderlich** – Diese Einstellung zwingt den Benutzer dazu, ein Sperrkennwort für die Applikation festzulegen, wenn noch kein Kennwort vorliegt. Die optionalen Kennwortkomplexitätsanforderungen und die Einstellung für fehlgeschlagene Kennworteingaben gelten nur, wenn **App-Kennwort erstellen** auf **Erforderlich** festgelegt ist.
  - **App wird sich sperren** – Diese Einstellung legt die Gültigkeitsdauer für das Applikationskennwort fest. Wenn ein Benutzer von der Files Advanced-Mobile-App zu einer anderen Applikation auf seinem Gerät wechselt und zur Mobile-App zurückkehrt, bevor dieser Verlängerungszeitraum abgelaufen ist, muss er das Sperrkennwort nicht erneut eingeben. Um festzulegen, dass das Kennwort immer eingegeben werden muss, wählen Sie **Sofort beim Beenden** aus. Wenn Sie möchten, dass der Benutzer die Einstellung für **App-Sperrung** in der mobile-App ändern kann, aktivieren Sie die Option **Benutzer erlauben, diese Einstellung zu ändern**.
  - **Minimale Kennwortlänge** – Die erlaubte Mindestlänge für das Sperrkennwort der Applikation.
  - **Mindestanzahl an komplexen Zeichen** – Die Mindestanzahl an Nicht-Buchstaben und Nicht-Zahlen für das Sperrkennwort der Applikation.
  - **Ein oder mehrere Buchstaben verlangen** – Stellt sicher, dass mindestens ein Buchstabe im Applikationskennwort vorkommt.
  - **Die Mobile Client App wird nach X fehlgeschlagenen Eingabeversuchen des App-Kennworts zurückgesetzt** – Wird diese Option aktiviert, werden die Einstellungen und Daten in der mobile-App nach der angegebenen Anzahl der aufeinanderfolgenden fehlgeschlagenen Kennworteingaben zurückgesetzt.

- **Nach Verbindungsverlust löschen oder sperren** – Wenn Sie diese Option aktivieren, wird die mobile-App automatisch gelöscht oder gesperrt, falls diese für eine zu spezifizierende Anzahl von Tagen keinen Kontakt zum Files Advanced-Server aufgenommen hat.

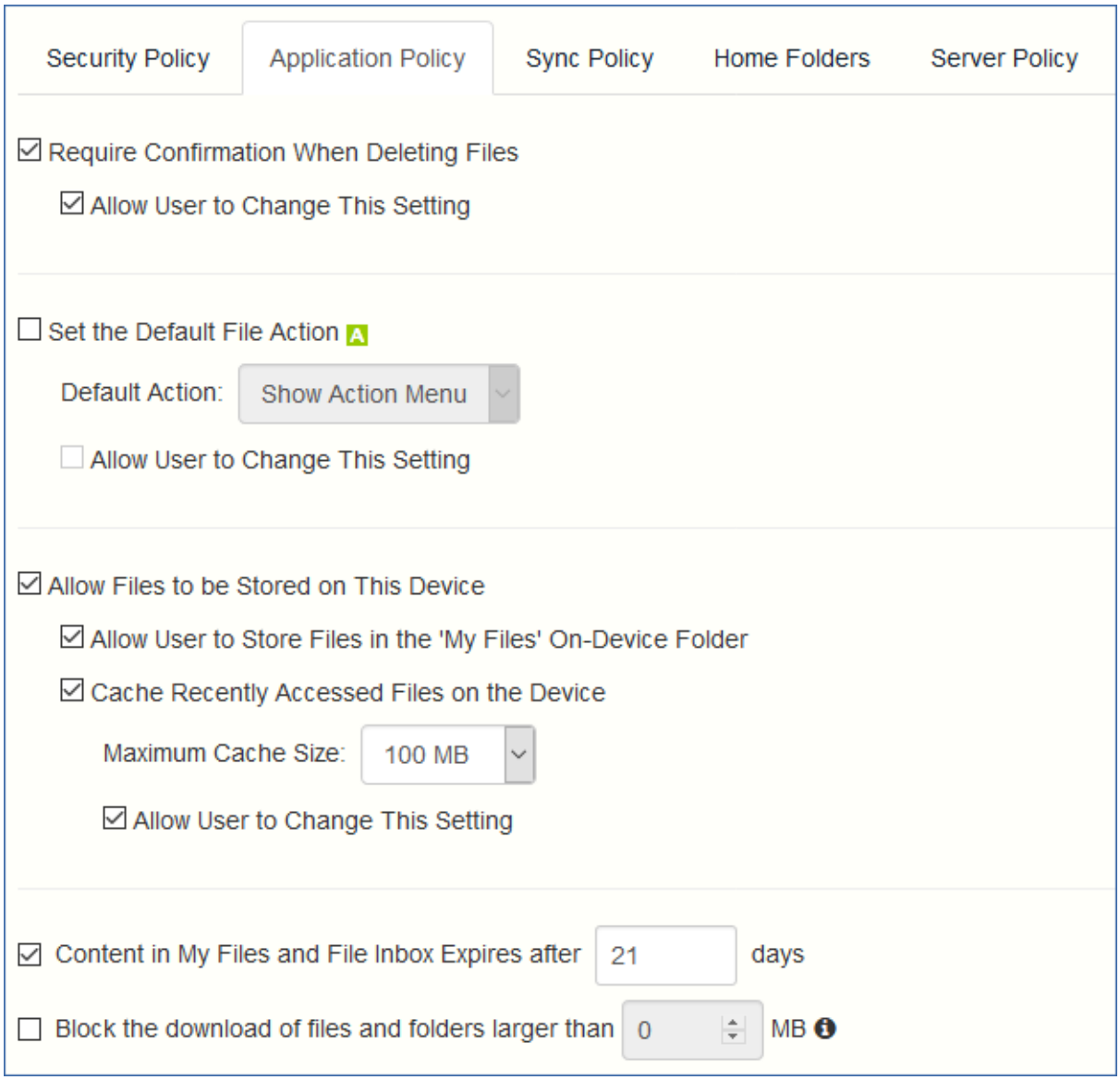
  Warnung! *Wenn die App aus irgendeinem Grund nicht beim Server authentifiziert werden kann, gilt der Vorgang auch dann nicht als eine Kontaktaufnahme mit dem Server, wenn der Server erreichbar ist.*

  - Gesperrte Clients werden automatisch entsperrt, wenn sie den Server später erfolgreich kontaktieren.
  - Bei gelöschten Clients werden alle lokal in der mobile-App gespeicherten Dateien unmittelbar gelöscht, die Client Management-Richtlinie wird entfernt und sämtliche Einstellungen auf die Standardwerte zurückgesetzt. Zurückgesetzte Clients müssen erneut bei der Verwaltung registriert werden, um Zugriff auf Gateway Server zu erlangen.
- **Die Mobile Client App wird gesperrt/zurückgesetzt – und zwar nach X Tagen vergeblichen Kontakts mit dem Files Advanced Server dieses Clients** – Legen Sie die Standardaktion für den Fall fest, dass der Client diesen Files Advanced Server für eine bestimmte Anzahl von Tagen nicht kontaktiert.
- **Benutzer [ ] Tage vorher warnen** – Bei dieser Option warnt die Mobile-App den Benutzer vor einer bevorstehenden Sperrung bzw. Löschung der App. Der Benutzer hat nun die Gelegenheit, eine Netzwerkverbindung herzustellen, damit die mobile-App Kontakt mit dem Files Advanced Server aufnehmen kann, um die Sperrung bzw. Löschung zu verhindern.

- **App-Absturzbericht** – Sendet Berichte an Acronis, wenn die Mobile-Apps abstürzen. Es werden keine privaten Daten oder Informationen gesendet, die eine Identifizierung ermöglichen.
  - **Keine Berichte senden**
  - **Benutzer kann Versenden einzeln entscheiden**
  - **Immer Berichte senden**

- **iTunes und iCloud erlauben, lokal gespeicherte Files Advanced-Dateien per Backup zu sichern** – Wenn diese Einstellung deaktiviert ist, erlaubt die Mobile-App kein Sichern der Dateien per Backup durch iTunes oder iCloud. Damit wird sichergestellt, dass Dateien im geschützten Gerätespeicher von Files Advanced nicht in die Backups kopiert werden.
- **Benutzer kann den Mobile Client aus der Verwaltung entfernen**- Aktivieren Sie diese Einstellung, wenn die Files Advanced-Benutzer die Möglichkeit haben sollen, ihre Verwaltungsrichtlinie in Files Advanced zu deinstallieren. Hierdurch wird die vollständige Funktionalität der Applikation wiederhergestellt und alle Änderungen an der Konfiguration werden durch die Richtlinie zurückgesetzt.
  - **Beim Entfernen alle Files Advanced-Daten vollständig löschen** – Wenn das Entfernen von Richtlinien durch den Benutzer aktiviert ist, kann diese Option ausgewählt werden. Wenn Sie sie aktivieren, werden alle lokal in der mobilen Applikation gespeicherten Daten gelöscht, wenn sie aus der Verwaltung entfernt wird. Hierdurch wird verhindert, dass Unternehmensdaten auf einem nicht verwalteten Gerät vorhanden sind.

6.2.3.2 Applikationsrichtlinie



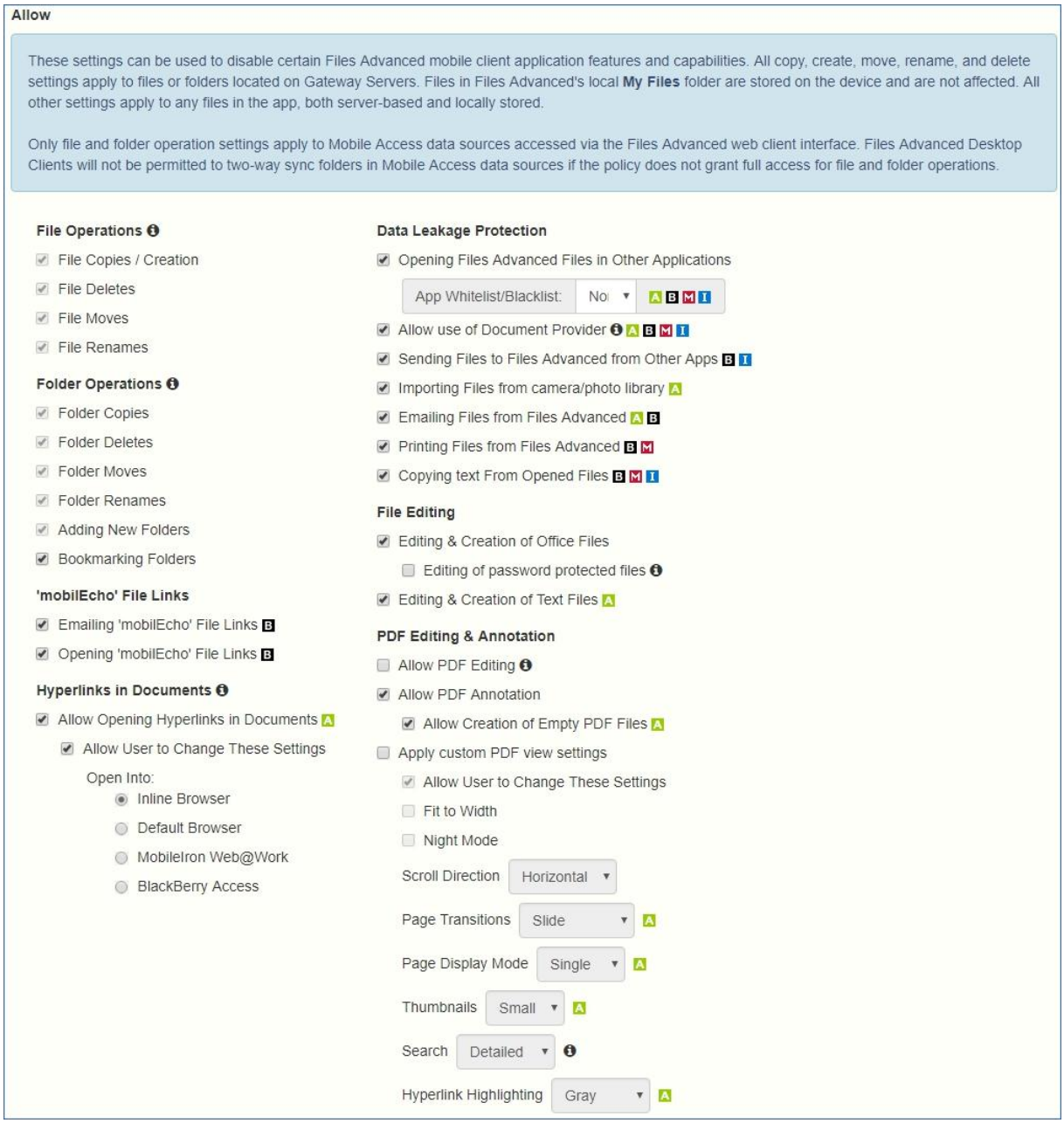
- **Bestätigung beim Löschen von Dateien verlangen** – Bei Aktivierung wird der Benutzer bei jedem Löschvorgang für eine Datei um Bestätigung gebeten. Wenn der Benutzer in der Lage sein soll, diese Einstellung später zu ändern, wählen Sie **Benutzer erlauben, diese Einstellung zu ändern**.
- **Die Standarddateiaktion festlegen** – Diese Option bestimmt, was geschieht, wenn ein Benutzer in der Mobile-Applikation auf eine Datei tippt. Wenn die Option nicht festgelegt ist, übernimmt die Client-Applikation den Standardwert aus dem Menü **Aktion**. Wenn der Benutzer in der Lage sein soll, diese Einstellung später zu ändern, wählen Sie **Benutzer erlauben, diese Einstellung zu ändern**.
- **Erlauben, dass Dateien auf diesem Gerät gespeichert werden** – Diese Einstellung ist standardmäßig aktiviert. Ist diese Option aktiviert, können Dateien im abgeschirmten Files Advanced-Speicher auf dem Gerät bleiben. Einzelne Funktionen, die Dateien lokal speichern (Ordner 'Meine Dateien', Synchronisierungsordner, Cache für zuletzt verwendete Dateien), können über zusätzliche Richtlinieneinstellungen aktiviert oder deaktiviert werden. Wenn diese Option deaktiviert ist, werden auf dem Gerät keine Dateien gespeichert, um sicherzustellen, dass sich keine Unternehmensdaten auf dem Gerät befinden, falls dieses verloren geht oder gestohlen wird. Wenn diese Einstellung deaktiviert ist, kann der Benutzer Dateien nicht zur

Offline-Verwendung speichern oder synchronisieren, zur Verbesserung der Leistung im Cache speichern oder mit der Funktion 'Öffnen in' aus anderen Applikationen an den mobilen Files Advanced Client senden.

- **Benutzern erlauben, Dateien im Geräteordner 'Meine Dateien' zu speichern** – Wenn diese Option aktiviert ist, können Dateien für den Offline-Zugriff und zur Bearbeitung in den Ordner 'Meine Dateien' kopiert werden. Dies ist ein Universalspeicherbereich im abgeschirmten Gerätespeicher von Files Advanced.
- **Kürzlich verwendete Dateien auf dem Gerät zwischenspeichern (cachen)** – Bei Aktivierung werden serverbasierte Dateien, auf die zuletzt zugegriffen wurde, in einem lokalen Cache auf dem Gerät gespeichert, sodass sie, sofern sie nicht geändert wurden, bei Bedarf schnell wieder verfügbar sind. Dies dient der Leistungssteigerung und der Einsparung von Bandbreite. **Maximale Cache-Größe** – Kann angegeben werden; optional können Änderungen durch Benutzer zugelassen werden.

- **Inhalte in 'Meine Dateien' und 'Datei-Inbox' verfallen nach X Tagen** – Wenn diese Option aktiviert ist, werden Dateien in **Meine Dateien** nach der eingestellten Anzahl von Tagen vom Gerät gelöscht.
- **Herunterladen von Dateien und Ordnern mit einer Größe über X MB blockieren** – Ist diese Option aktiviert, werden Dateien und Ordner mit einer Größe über dem eingestellten Wert von den mobilen Apps nicht heruntergeladen.

Zulassen



Diese Einstellungen können verwendet werden, um bestimmte Funktionen und Fähigkeiten der Mobile-Applikation zu deaktivieren. 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 Mobile Clients werden dagegen auf dem Gerät gespeichert und sind daher von den Einstellungen nicht betroffen. Alle anderen Einstellungen gelten für alle Dateien in Files Advanced, also sowohl für serverbasierte als auch für lokal auf dem Client gespeicherte Dateien.

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

'mobilEcho'-Datei-Links

- **'mobilEcho'-Datei-Links per E-Mail senden** – Wenn diese Option deaktiviert ist, können die Benutzer keine mobilEcho://-URLs für Files Advanced Dateien oder Ordner an andere Files Advanced Benutzer senden. Diese Links funktionieren nur, wenn sie auf einem Gerät geöffnet werden, auf dem der Empfänger den mobilen Files Advanced Client installiert und mit einem Server oder zugewiesenen Ordner mit Zugriff auf den verlinkten Speicherort konfiguriert hat. Der

Benutzer muss zudem Berechtigungen auf Datei-/Ordnerebene besitzen, um das betreffende Element lesen zu können.

- **'mobilEcho'-Datei-Links öffnen** – Wenn diese Option deaktiviert ist, können die Benutzer keine mobilEcho://-URLs für Files Advanced Dateien oder Ordner öffnen.

Hyperlinks in Dokumenten

- **Öffnen von Hyperlinks in Dokumenten erlauben** – Wenn diese Option aktiviert ist, können Benutzer in Dokumenten gespeicherte Hyperlinks öffnen.
  - **Benutzer erlauben, diese Einstellungen zu ändern** – Wenn diese Option aktiviert ist, sind Benutzer in der Lage, diese Funktion nach Wahl zu aktivieren oder zu deaktivieren.

  Öffnen in:
  - **Interner Browser** – Hyperlinks werden direkt in der Files Advanced App geöffnet.
  - **Standard-Browser** – Hyperlinks werden in dem auf Ihrem Gerät gewählten Standardbrowser geöffnet.
  - **MobileIron Web@Work** – Hyperlinks werden in der MobileIron Web@Work App geöffnet.
  - **Blackberry Access** – Hyperlinks werden in der BlackBerry Access App geöffnet.

Schutz vor Datenverlust

- **Files Advanced-Dateien in anderen Applikationen öffnen** – Wenn diese Option deaktiviert ist, zeigt die Mobile-Applikation die Schaltfläche **Öffnen in** nicht an und lässt das Öffnen von Dateien aus Files Advanced in anderen Applikationen nicht zu. 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 Files Advanced unterliegt.
  - **Whitelist/Blacklist für Apps** – Wählen Sie eine vordefinierte Whitelist oder Blacklist aus, mit der Drittanbieter-Apps eingeschränkt werden, in denen Files Advanced Dateien auf dem Gerät geöffnet werden können. Zum Erstellen einer Whitelist oder Blacklist klicken Sie in der oberen Menüleiste auf **Erlaubte Apps**.
- **Dokument-Provider-Nutzung erlauben** – Mobilgeräte können die Document Provider Extension für Files Advanced verwenden. Bestimmte Konfigurationen können Einfluss auf die Document Provider Extension haben:
  a. Wenn ein Client von einem älteren Server verwaltet wird, ist die Document Provider Extension deaktiviert, es sei denn, die Option **Files Advanced-Dateien in anderen Applikationen öffnen** ist **deaktiviert** oder eine Blacklist/Whitelist ist **aktiviert**.
  b. Wenn ein Client von einem neuen Server (Version 7.3.1 und höher) verwaltet wird und die Option **Dokument-Provider-Nutzung erlauben** aktiviert ist, können die Benutzer nach wie vor Dateien mit anderen Apps gemeinsam nutzen, selbst wenn die Option **Files Advanced-Dateien in anderen Applikationen öffnen deaktiviert** oder eine Blacklist/Whitelist **aktiviert** ist. Das gilt selbst für eigens gesperrte Apps.
  c. Wenn die Option **Dokument-Provider-Nutzung erlauben** aktiviert, aber die Erstellung von Dateien deaktiviert ist, funktioniert die Document Provider Extension zwar, aber die Benutzer können keine Dateien von anderen Apps in Files Advanced-Datenquellen speichern.
- **Dateien von anderen Apps aus an Files Advanced senden** – Wenn diese Option deaktiviert ist, akzeptiert die Mobile-Applikation keine Dateien, die über die Funktion **Öffnen in** von anderen Applikationen an sie gesendet wurden.

- **Dateien von Kamera/Fotobibliothek importieren** – Wenn diese Option aktiviert ist, können Benutzer Fotos und Videos aus der Fotobibliothek ihres Geräts direkt in Files Advanced importieren.
- **Dateien von Files Advanced aus per E-Mail senden** – Wenn diese Option deaktiviert ist, zeigt die Mobile-Applikation die Schaltfläche **Datei per E-Mail senden** nicht an und das Versenden von Dateien aus Files Advanced wird unterbunden.

  Hinweis: *Die Android-Plattform weist keine integrierte E-Mail-App oder -Funktion auf, die deaktiviert werden kann. Um zu verhindern, dass Benutzer Dateien in E-Mails verschieben, müssen Sie stattdessen die Option 'Files Advanced-Dateien in anderen Applikationen öffnen' deaktivieren.*

- **Dateien von Files Advanced aus drucken** – Wenn diese Option deaktiviert ist, zeigt die Mobile-Applikation die Schaltfläche **Drucken** nicht an und das Drucken von Dateien aus Files Advanced wird unterbunden.
- **Text aus geöffneten Dateien kopieren** – Wenn diese Option deaktiviert ist, verhindert die Mobile-App, dass Benutzer in geöffneten Dokumenten Texte für Kopieren-/Einfügen-Aktionen auswählen können. Damit wird verhindert, dass Daten in andere Applikationen kopiert werden.

Dateibearbeitung

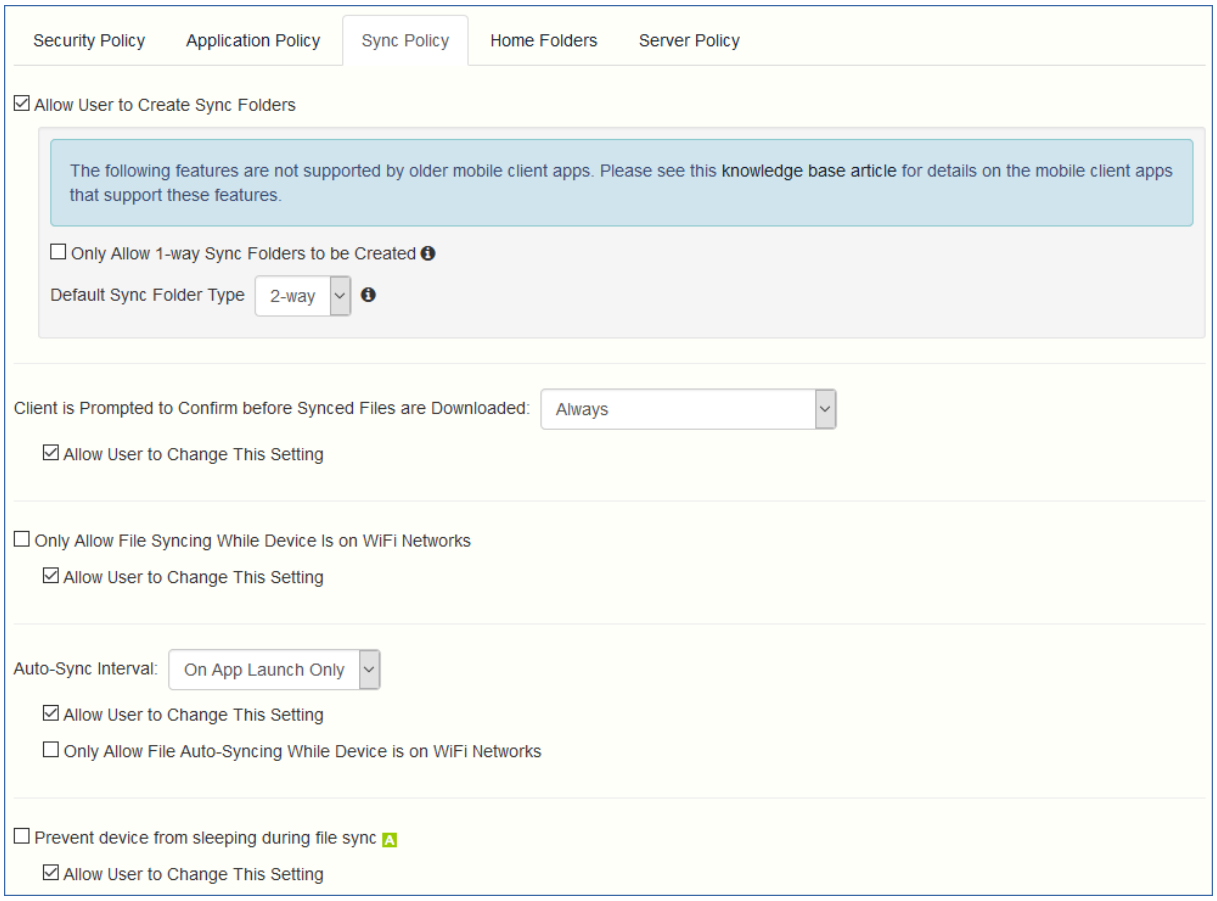
- **Bearbeiten & Erstellen von Office-Dateien** – Wenn diese Option deaktiviert ist, können Benutzer keine Dokumente mit dem integrierten SmartOffice-Editor bearbeiten.
  - **Bearbeiten von kennwortgeschützten Dateien** – Wenn diese Option aktiviert ist, können Benutzer kennwortgeschützte Dateien nicht bearbeiten.
- **Bearbeiten & Erstellen von Textdateien** – Wenn diese Option deaktiviert ist, können Benutzer keine txt-Dateien mit dem integrierten Texteditor bearbeiten.

PDF-Bearbeitung und -Anmerkung

- **PDF-Bearbeitung erlauben** – Wenn diese Option aktiviert ist, können Benutzer viele PDF-Bearbeitungsfunktionen verwenden, wie das Erstellen von neuen Seiten, Duplizieren von Seiten, Kopieren und Einfügen, Neuordnen, Rotieren, Löschen und Verwenden von neuen Dokumenten aus einer Teilmenge von ausgewählten Seiten.
- **PDF-Anmerkungen erlauben** – Wenn diese Option deaktiviert ist, kann die mobile App keine PDF-Dateien mit Anmerkungen versehen.
  - **Erstellen von leeren PDF-Dateien erlauben** – Wenn diese Option aktiviert ist, können Benutzer leere PDF-Dateien erstellen und diese mithilfe von Anmerkungen bearbeiten.
- **Benutzerdefinierte PDF-Anzeigeeinstellungen anwenden** – Wenn diese Option aktiviert ist, gelten alle Untereinstellungen für alle Benutzer und alle PDF-Dateien.
  - **Benutzer erlauben, diese Einstellungen zu ändern** – Wenn diese Option aktiviert ist, sind Benutzer in der Lage, ihre PDF-Anzeigeeinstellungen zu ändern.
  - **An Breite anpassen** – Wenn diese Option aktiviert ist, wird die Seite auf die gesamte Bildschirmbreite Ihres Geräts vergrößert.
  - **Nachtmodus** – Wenn diese Option aktiviert ist, verwendet das Gerät das Farbschema für den Nachtmodus, sodass die Anzeige auch bei schlechter Beleuchtung gut erkennbar ist.
  - **Bildlaufrichtung** – Hiermit können Sie festlegen, ob die Seiten vertikal oder horizontal bewegt werden.

- **Seitenübergänge** – Hiermit können Sie die visuellen Effekte bei Übergängen festlegen. **Diashow** zeigt die Seiten einzeln nacheinander an, mit **Kontinuierlich** können Sie die Seiten scrollen, als würde es sich um eine einzelne, durchgängige Seite handeln, und mit **Umblättern** blättern Sie die Seiten weiter wie in einem Buch.
- **Seitenanzeigemodus** – Sie können wählen, ob die PDF-Datei als zwei Seiten oder als einzelne Seite angezeigt werden soll.
- **Miniaturbilder (Thumbnails)** – Bestimmt beim Öffnen einer PDF-Datei, wie groß die Thumbnails der Seiten sind. Sie können zwischen **Klein**, **Groß** und **Ohne** wählen.
- **Suchen** – Konfiguriert das Anzeigeformat der Suchergebnisse des integrierten PDF-Viewers. Es gibt drei Typen bei der Anzeige der Suchergebnisse:
  - **Einfach** – Hebt die Ergebnisse hervor und Sie können sie mit den Pfeilsymbolen durchblättern.
  - **Ausführlich** – Zeigt eine Dropdown-Liste aller Ergebnisse an und Sie können durch Tippen durch die Liste navigieren.
  - **Dynamisch** – Legt die Anzeige der Suchergebnisse für iPhones auf **Einfach** und für iPads auf **Ausführlich** fest.
- **Hyperlink-Hervorhebung** – Damit legen Sie die Farbe fest, mit der Hyperlinks hervorgehoben werden. Alternativ können Sie die Hervorhebung durch Wahl von **Deaktiviert** auch ausschalten.

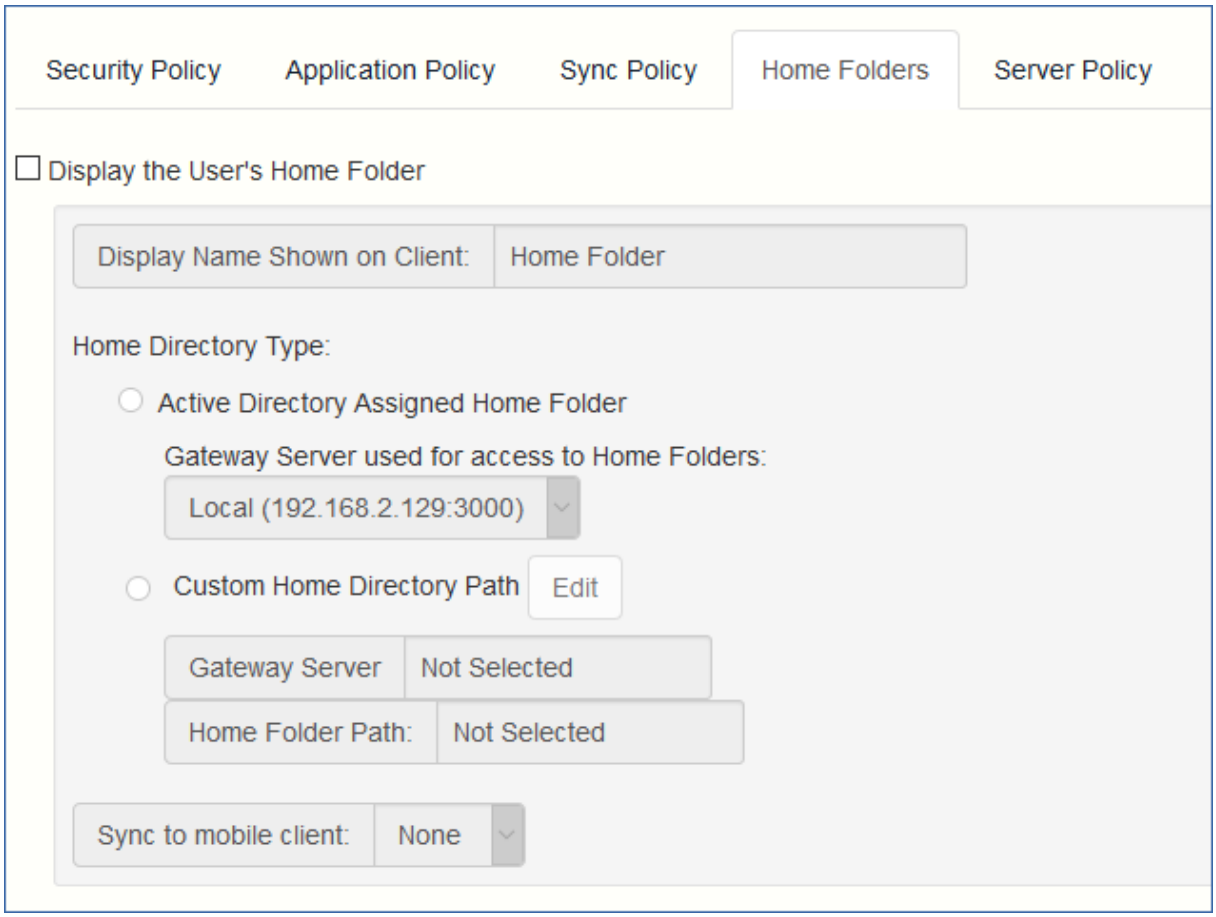
6.2.3.3 Sync-Richtlinie



- **'Vom Benutzer erstellte Sync-Ordner' erlauben** – Erlaubt dem Benutzer, seine eigenen Synchronisierungsordner zu erstellen.

  - **Nur das Erstellen von 1-Weg-Sync-Ordner erlauben** – Benutzer können nur 1-Weg-Sync-Ordner erstellen.
  - **Standardtyp für den Sync-Ordner** – Legt entweder '1-Weg' oder '2-Wege' als Standardtyp für den Sync-Ordner fest.
- **Bestätigungsaufforderung an Client, bevor synchronisierte Dateien heruntergeladen werden** – Wählen Sie die Bedingungen aus, unter denen der Benutzer das Herunterladen von Dateien in synchronisierten Ordnern bestätigen muss. Es gibt folgende Optionen: **Immer**, **Nur in Mobilfunknetzen** und **Nie**. Wird **Benutzer erlauben, diese Einstellung zu ändern** aktiviert, können Clients die Bestätigungsoptionen ändern.
- **Dateisynchronisierung nur erlauben, wenn Gerät per WLAN verbunden ist** – Wenn diese Option aktiviert ist, lässt Files Advanced 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.
- **Auto-Sync-Intervall** – Wenn diese Option aktiviert ist, führt Files Advanced eine automatische Synchronisierung **Nie**, **Nur beim App-Start** oder in verschiedenen **Zeitintervallen** aus.
  - **Benutzer erlauben, diese Einstellung zu ändern** – Wenn diese Option aktiviert ist, kann der Benutzer das Zeitintervall in der Files Advanced-Mobile-App selbst einstellen.
  - **Datei-Auto-Sync nur erlauben, wenn Gerät per WLAN verbunden ist** – Wenn diese Option aktiviert ist, wird die automatische Synchronisierung erst bei einer bestehenden WiFi-Verbindung ausgeführt.
- **Gerät daran hindern, während Datei-Sync in Standby zu gehen** – Wird diese Option aktiviert, gehen Geräte, die diese Einstellung unterstützen, nicht in den Sperr-/Standbymodus, wenn Dateisynchronisierungen durchgeführt werden. Wird **Benutzer erlauben, diese Einstellung zu ändern** aktiviert, können Clients die Bestätigungsoptionen ändern.

6.2.3.4 Basisordner



- **Basisordner des Benutzers anzeigen** – Ist diese Option aktiviert, wird das persönliche Basisverzeichnis eines Benutzers in der Mobile-App angezeigt.
  - **Den auf dem Client gezeigten Namen anzeigen** – Legt den Anzeigenamen des Basisordners in der Mobile-App fest. Der Platzhalter **%USERNAME%** kann verwendet werden, um den Namen des Benutzers in den Ordnernamen aufzunehmen, der angezeigt wird.

  Hinweis: *Der Platzhalter **%USERNAME%** kann nicht verwendet werden, um den Benutzernamen oder einen anderen Datenquellentyp anzuzeigen. Er ist ausschließlich für zugewiesene Active Directory-Basisordner verwendbar.*

  - **Zugewiesener Active Directory-Basisordner** – Der in der Mobile-App angezeigte Basisordner verbindet den Benutzer mit dem in seinem AD-Kontoprofil festgelegten Server-/Ordnerpfad. Der Zugriff auf den Basisordner erfolgt über das ausgewählte Gateway.
  - **Benutzerdefinierter Basisordnerpfad** – Der in der Mobile-App angezeigte Basisordner verbindet den Benutzer mit dem Serverpfad, der in dieser Einstellung festgelegt wird. Der Platzhalter **%USERNAME%** kann verwendet werden, um den Benutzernamen des Benutzers in den Pfad für den Basisordner aufzunehmen. %USERNAME% muss in Großbuchstaben eingegeben werden.
  - **Mit mobilem Client synchronisieren -** Über diese Option können Sie den Synchronisierungstyp für das Basisverzeichnis festlegen.

    Hinweis: *Diese Option hat **keinen** Einfluss auf die Fähigkeit der Benutzer, ihren Basisordner mit dem Desktop Client zu synchronisieren.*

6.2.3.5 Server-Richtlinie

- **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 Files Advanced Mobile muss der Benutzer sein Kennwort eingeben, sobald er mit dem ersten Server eine Verbindung herstellt. Bis er die Files Advanced Mobile-Applikation verlässt, kann der Benutzer dann eine Verbindung zu weiteren Servern herstellen, ohne das Kennwort erneut eingeben zu müssen. Verlässt er den Files Advanced Mobile 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, kann der Benutzer Server innerhalb der Files Advanced Mobile-Applikation durch Angabe von DNS-Name und IP-Adresse manuell hinzufügen. Wenn dem Benutzer nur die Server zur Verfügung stehen sollen, die ihm unter **Zugewiesene Server** 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.
    - **Erlauben, dass Datei-Server-, NAS- und SharePoint-Ordner zum Desktop Client synchronisieren werden** – Wenn aktiviert, dürfen Desktop Clients eine 1-Weg-Synchronisierung von **Netzwerk**-Inhalten durchführen.
        - **2-Wege-Synchronisierung von Datei-Server-, NAS- und SharePoint-Odnern zum Desktop Client erlauben** – Wenn aktiviert, dürfen Desktop Clients eine 2-Wege-Synchronisierung von **Netzwerk**-Inhalten durchführen.

    Hinweis: *Um die 2-Wege-Synchronisierung von* ***Netzwerk****-Inhalten für die Desktop Clients nutzen zu können, müssen Sie außerdem folgende Datei- und Ordner-Aktionen in der Registerkarte* ***Applikationsrichtlinie*** *erlauben:* ***Erstellen*** *(****Hinzufügen*** *für Ordner),* ***Kopien****,* ***Löschungen****,* ***Verschiebungen*** *und* ***Umbenennungen****.*

- **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 ClientFiles Advanced Mobile 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 Sie möchten, dass der Benutzer dies über die Files Advanced-Mobile-App ändern kann, aktivieren Sie die Option **Benutzer erlauben, diese Einstellung zu ändern**.

6.2.3.6 Ausnahmen für Richtlinieneinstellungen

Für Benutzer der Apps **Files Advanced Mobile für Android**, **Files Advanced Mobile für Good Dynamics** (iOS) und **Files Advanced Mobile mit Mobile Iron AppConnect** gibt es einige Ausnahmen hinsichtlich der Art, auf die mobilEcho Client Management-Richtlinien auf die jeweilige mobilEcho Client-Applikation angewendet werden. Im Fall von Android werden einige Funktionen des iOS-Clients nicht unterstützt, sodass die entsprechenden Richtlinien nicht angewendet werden. Im Fall von Good Dynamics werden einige standardmäßige Files Advanced Mobile-Richtlinienfunktionen zugunsten des Systems von Good Dynamics und der Richtliniensätze von Good Dynamics zurückgestellt, die Sie auf dem Server von Good Control konfiguriert haben. Bei MobileIron werden einige der standardmäßigen Files Advanced-Richtlinienfunktionen auf die MobileIron AppConnect-Plattform übertragen. Diese Ausnahmen werden auf den Seiten zur Files Advanced-Richtlinienkonfiguration vermerkt. Weitere Details zu den einzelnen Richtlinienausnahmen werden angezeigt, wenn Sie den Mauszeiger über das Logo von Good, Android oder MobileIron führen.

6.2.4 Erstellen einer Liste mit blockierten Pfaden

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

So erstellen Sie eine Liste:

1. Öffnen Sie die Weboberfläche als Administrator.
2. Öffnen Sie die Seite Richtlinien (S. 55).
3. Klicken Sie auf die gewünschte Benutzer- oder Gruppenrichtlinie.
4. Öffnen Sie die Registerkarte Server-Richtlinie (S. 72).
5. Aktivieren Sie das Kontrollkästchen **Zugriff auf bestimmte Netzwerkpfade blockieren**.

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

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

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

1. Öffnen Sie die Weboberfläche als Administrator.
2. Öffnen Sie die Seite Richtlinien (S. 55).

3. Klicken Sie auf die gewünschte Benutzer- oder Gruppenrichtlinie.
4. Öffnen Sie die Registerkarte Server-Richtlinie (S. 72).
5. Aktivieren Sie das Kontrollkästchen **Zugriff auf bestimmte Netzwerkpfade blockieren**.

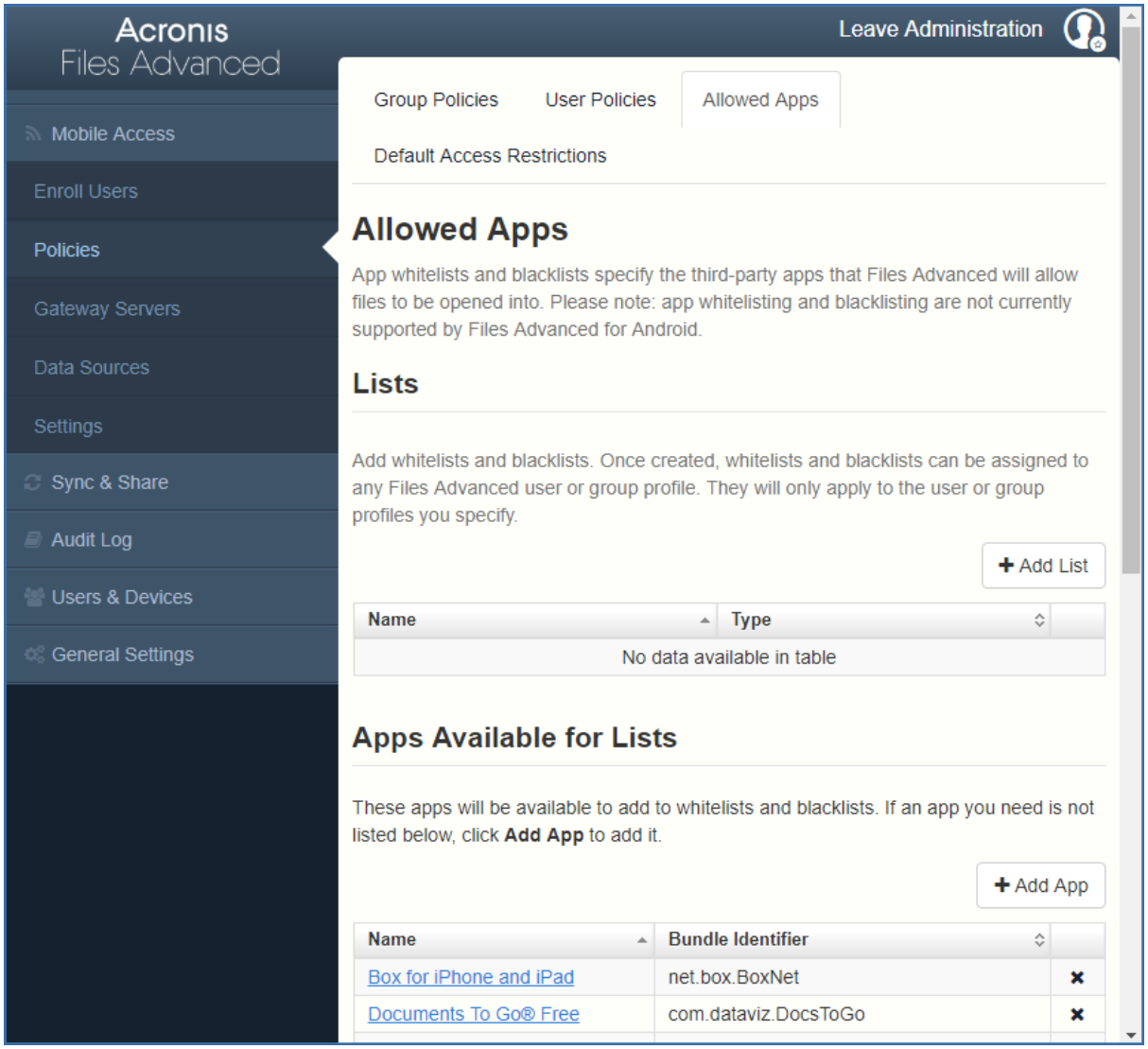
   Hinweis: *Sie müssen diesen Schritt für jede Benutzer-/Gruppenrichtlinie durchführen, die Sie der Blacklist hinzufügen möchten.*

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

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

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

6.2.5 Erlaubte Apps



In Files Advanced Client Management können Sie Whitelists und Blacklists erstellen, mit denen die Fähigkeit von Files Advanced Mobile eingeschränkt wird, Dateien in anderen Apps auf einem mobilen Gerät zu öffnen. Mit diesen Listen können Sie sicherstellen, dass Dateien, auf die über den Files Advanced Mobile zugegriffen werden kann, nur in sicheren, vertrauenswürdigen Apps geöffnet werden können.

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

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

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

Hinweis: *App-Whitelists und -Blacklists werden derzeit von Files Advanced Mobile für Android nicht unterstützt.*

Listen

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

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

Themen

6.2.5.1 Für die Listen verfügbare Apps hinzufügen

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

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

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

6.2.5.2 Bundle Identifier einer App suchen

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

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

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

Den Bundle Identifier einer App in einer iTunes Library ermitteln

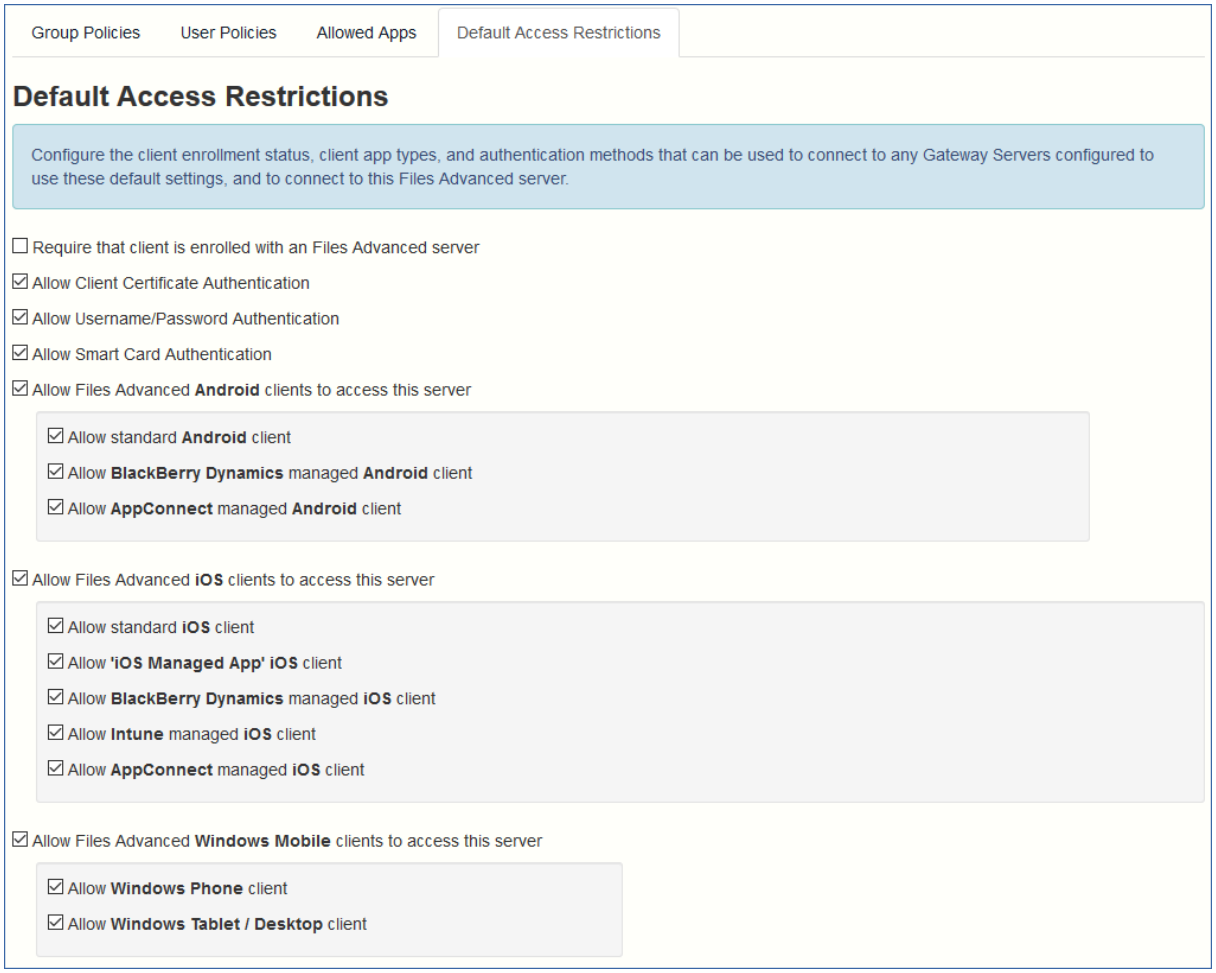
Wenn Sie Ihr Gerät mit iTunes synchronisieren und sich die gewünschte App entweder auf Ihrem Gerät befindet oder über iTunes heruntergeladen wurde, existiert sie auf der Festplatte Ihres Computers. Sie können auf Ihrer Festplatte danach suchen und dann innerhalb der App den **Bundle Identifier** ermitteln.

1. Navigieren Sie zur iTunes Library, und öffnen Sie den Ordner **Mobile Applications**.
2. Auf einem Mac befindet sich dieser normalerweise in ~/Music/iTunes/Mobile Applications/
3. Auf einem Windows 7 PC befindet er sich für gewöhnlich in **`C:\Users\username\My Music\iTunes\Mobile Applications/`**
4. Falls Sie die App erst kürzlich auf Ihrem Gerät installiert haben, sollten Sie unbedingt eine iTunes-Synchronisierung durchführen, bevor Sie fortfahren.
5. Suchen Sie nach der benötigten App im Ordner **Mobile Applications**.
6. Duplizieren Sie die Datei und benennen Sie die Erweiterung in .ZIP um.
7. Wenn Sie diese neu erstellte ZIP-Datei dekomprimieren, erhalten Sie einen Ordner mit dem Applikationsnamen.
8. Innerhalb dieses Ordners befindet sich eine Datei namens **iTunesMetadata.plist**.
9. Öffnen Sie diese PLIST-Datei in einem Texteditor.
10. Suchen Sie nach dem **softwareVersionBundleId**-Schlüssel in der Liste.
11. Die darunter stehende **Zeichenfolge** ist der Wert des Bundle Identifier, den Sie für die App in Files Advanced eingeben müssen. Diese Zeichenfolgen sind gewöhnlich wie folgt formatiert: **com.firmenname.appname**

6.2.6 Standardzugriffsbeschränkungen

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

Hinweis: *Informationen zum Einstellen von benutzerdefinierten Beschränkungen für Ihre Gateway Server finden Sie im Artikel Gateway Server bearbeiten (S. 90) im Abschnitt 'Gateway Server verwalten'.*



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

- **Verlangen, dass der Client für einen Files Advanced Server registriert ist** – Wenn Sie diese Option auswählen, müssen alle Files Advanced Mobiles mit Verbindung zu diesem Server von einem Files Advanced Server verwaltet werden, der unter 'Zulässige Files Advanced Server' aufgeführt ist. Diese Option stellt sicher, dass alle Clients, die auf den Server zugreifen, über die erforderlichen Einstellungen und Sicherheitsoptionen verfügen. Der eingegebene Servername muss dem in der Mobile-App konfigurierten Namen des Management-Servers entsprechen. Es können auch unvollständige Namen verwendet werden, um beispielsweise mehrere Client-Management-Server in einer Domain zu erlauben. Bei unvollständigen Namen sind keine Platzhaltersymbole erforderlich.
- **Client-Zertifikatsauthentifizierung erlauben** – Wenn Sie das Kontrollkästchen für diese Option deaktivieren, können Benutzer nicht über ein Zertifikat verbunden werden; sie können aber per Benutzername und Kennwort des Clients oder per Smartcard verbunden werden.
- **Authentifizierung per Benutzername/Kennwort erlauben** – Wenn Sie das Kontrollkästchen für diese Option deaktivieren, können Benutzer nicht per Benutzername und Kennwort verbunden werden; sie können aber per Client-Zertifikat oder Smartcard verbunden werden.

- **Smartcard-Authentifizierung erlauben** – Wenn Sie das Kontrollkästchen für diese Option deaktivieren, können Benutzer nicht per Smartcard verbunden werden; sie können aber per Benutzername und Kennwort des Clients oder per Zertifikat verbunden werden.
- **Files Advanced-Android-Clients den Zugriff auf diesen Server erlauben** – Wenn Sie diese Option deaktivieren, können Android-Geräte keine Verbindung mit dem Files Advanced-Server herstellen, und Sie können zudem nicht auf die Managementfunktion zugreifen. Wenn Sie diese Option auswählen, können Sie mit den unten aufgeführten Optionen weiter festlegen, welche Clients eine Verbindung herstellen können.
  - **Android-Standard-Clients erlauben** – Wenn Sie diese Option auswählen, lässt der Files Advanced Server Verbindungen von Benutzern zu, die die Android-Standard-Client-App von Files Advanced verwenden. Wenn Android-Benutzer nicht auf diesen Files Advanced-Server zugreifen sollen, können Sie diese Einstellung deaktivieren.
  - **Per AppConnect verwaltete Android-Clients erlauben** – Wenn Sie diese Option auswählen, lässt der Server Files Advanced Android-Benutzer mit Files Advanced Clients zu, die in MobileIron registriert sind. Wenn Android-Benutzer,die in MobileIron registriert sind, nicht auf diesen Files Advanced-Server zugreifen sollen, können Sie diese Einstellung deaktivieren.
  - **Per Blackberry Dynamics verwaltete Android-Clients erlauben** – Wenn Sie diese Option auswählen, lässt der Files Advanced Server Verbindungen von Benutzern zu, die den per Good Dynamics verwalteten Android-Client von Files Advanced Mobile verwenden. Wenn Benutzer mit dem per Good Dynamics verwalteten Android Access Mobile ClientFiles Advanced MobileFiles Advanced MobileFiles Advanced Mobile Good Dynamics-Client nicht auf diesen Files Advanced-Server zugreifen sollen, können Sie diese Einstellung deaktivieren.
- **Files Advanced-iOS-Clients den Zugriff auf diesen Server erlauben** – Wenn Sie diese Option deaktivieren, können iOS-Geräte keine Verbindung mit dem Files Advanced-Server herstellen, und Sie können zudem nicht auf die Managementfunktion zugreifen. Wenn Sie diese Option auswählen, können Sie mit den unten aufgeführten Optionen weiter festlegen, welche Clients eine Verbindung herstellen können.
  - **iOS-Standard-Clients erlauben** – Wenn Sie diese Option auswählen, lässt der Files Advanced Server Verbindungen von Benutzern zu, die die iOS-Standard-App von Access Mobile ClientFiles Advanced MobileFiles Advanced MobileFiles Advanced Mobile verwenden. Wenn iOS-Benutzer nicht auf diesen Files Advanced Server zugreifen sollen, können Sie diese Einstellung deaktivieren.
  - **iOS-Clients mit 'Verwalteter iOS-App' erlauben** – Wenn Sie diese Option auswählen, lässt der Files Advanced-Server Verbindungen von Benutzern zu, die die von Files Advanced verwaltete iOS-Access-App verwenden. Um in diesem Status zu sein, muss ein Client eine Konfiguration für die verwaltete App (S. 273) mit mindestens einem Parameter erhalten haben. Wenn iOS-Benutzer nicht auf diesen von Acronis Files Advanced verwalteten Server zugreifen sollen, können Sie diese Einstellung deaktivieren.
  - **Per Blackberry Dynamics verwaltete iOS-Clients erlauben** – Wenn Sie diese Option auswählen, lässt der Files Advanced Server Verbindungen von Benutzern zu, die den per Good Dynamics verwalteten iOS-Client von Files Advanced Mobile verwenden. Wenn Sie Benutzern mit dem iOS Files Advanced Mobile Good Dynamics-Client den Zugriff auf diesen Files Advanced Server nicht erlauben möchten, können Sie diese Einstellung deaktivieren.
  - **Per Intune verwaltete iOS-Clients erlauben** – Wenn Sie diese Option auswählen, lässt der Files Advanced-Server Verbindungen von Benutzern zu, die den per Intune verwalteten iOS Access Mobile ClientFiles Advanced MobileFiles Advanced MobileFiles Advanced Mobile-Client verwenden. Wenn per Intune verwaltete Benutzer nicht auf diesen von Files Advanced verwalteten Server zugreifen sollen, können Sie diese Einstellung deaktivieren.

- **Per AppConnect verwaltete iOS-Clients erlauben** – Wenn Sie diese Option auswählen, lässt der Files Advanced-Server iOS-Benutzer mit Access Mobile ClientFiles Advanced MobileFiles Advanced MobileFiles Advanced Mobile zu, die in MobileIron registriert sind. Wenn iOS-Benutzer, die in MobileIron registriert sind, nicht auf diesen Files Advanced-Server zugreifen sollen, können Sie diese Einstellung deaktivieren.

- **Files Advanced-Windows-Mobile-Clients den Zugriff auf diesen Server erlauben** –
  - **Windows Phone-Client erlauben** – Wenn Sie diese Option auswählen, lässt der Files Advanced-Server Verbindungen von Telefonbenutzern zu, die die Windows Mobile-App von Files Advanced verwenden. Wenn Windows Mobile-Benutzer nicht auf diesen Files Advanced-Server zugreifen sollen, können Sie diese Einstellung deaktivieren.
  - **Windows Tablet/Desktop Client erlauben** – Wenn Sie diese Option auswählen, lässt der Files Advanced Server Verbindungen von Tablet-Benutzern zu, die die Windows Mobile-App von Files Advanced verwenden. Wenn Windows Mobile-Benutzer nicht auf diesen Files Advanced-Server zugreifen sollen, können Sie diese Einstellung deaktivieren.

6.3 Integration mobiler Geräte

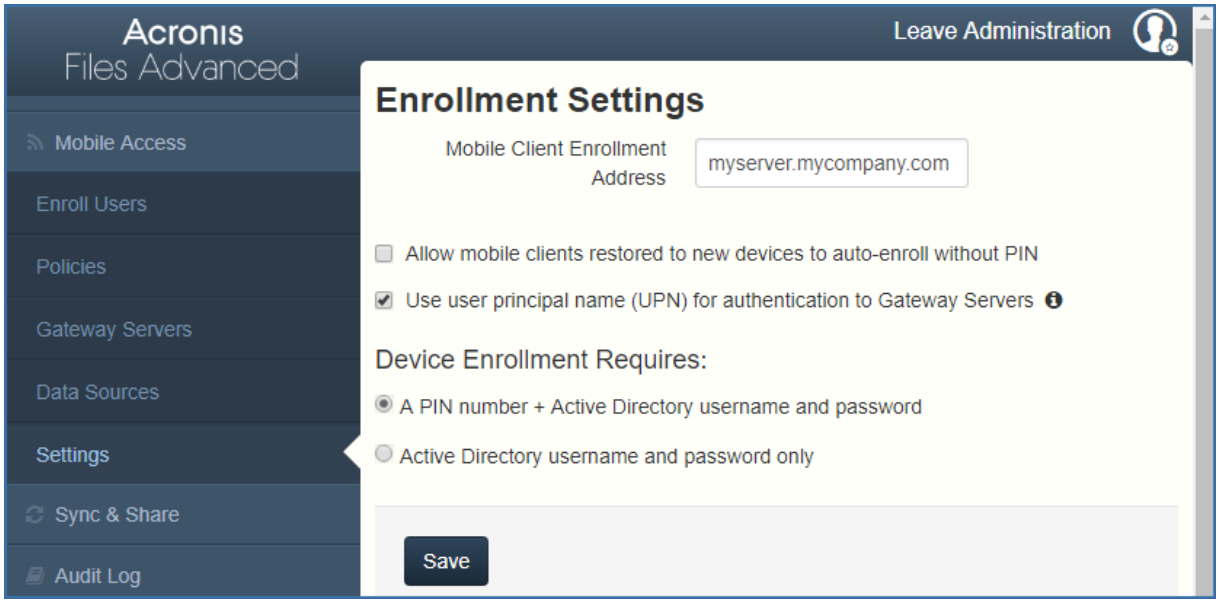
Um die Files Advanced-Mobile-App verwenden zu können, müssen Benutzer die App über ihren entsprechenden App Store (iTunes, Google Play oder Windows Store) installieren. Bei Verwendung der Client-Verwaltung in Ihrem Unternehmen müssen die Benutzer zudem die Files Advanced-Mobile-App auf ihrem Gerät beim Files Advanced Server registrieren. Nach der Registrierung werden die Konfiguration des mobilen Clients, die Sicherheitseinstellungen und Funktionen von der Files Advanced-Benutzer- oder Gruppenrichtlinie gesteuert.

Zu den Einstellungen und Funktionen in der Mobile-Anwendung, die durch die Verwaltungsrichtlinie vorgegeben werden, gehören:

- Kennwort zum Sperren der Files Advanced-Anwendung erforderlich
- Komplexitätsanforderungen für das Kennwort
- Möglichkeit, die Files Advanced App aus der Verwaltung zu entfernen
- Drucken und Senden von Dateien aus der Files Advanced-App erlauben
- Speichern von Dateien auf dem Gerät erlauben
- iTunes erlauben, lokale Dateien der Files Advanced-App zu sichern
- Senden von Dateien aus anderen Apps an Files Advanced erlauben
- Öffnen von Files Advanced-Dateien in anderen Anwendungen erlauben
- Anwendungen einschränken, in denen Files Advanced-Dateien geöffnet werden dürfen
- PDF-Anmerkungen erlauben
- Erstellen, Umbenennen und Löschen von Dateien und Ordnern zulassen
- Verschieben von Dateien zulassen
- Bestätigung beim Löschen von Dateien verlangen
- Zuweisung von Servern, Ordnern und Basisverzeichnissen, damit diese automatisch in der Files Advanced-App angezeigt werden
- Konfiguration von Ordnern für die 1-Weg- oder 2-Wege-Synchronisierung mit dem Server

Themen

6.3.1 Serverseitiger Verwaltungsregistrierungsvorgang



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

Registrierungseinstellungen

Mobilen Clients, die auf neuen Geräten wiederhergestellt wurden, eine automatische Registrierung ohne PIN erlauben –

Benutzerprinzipalname (UPN) zur Authentifizierung an Gateway Servern verwenden – Ist diese Option aktiviert, wird 'benutzername@domain.com' anstelle von Domain/Benutzername für die Authentifizierung verwendet.

Geräteregistrierungsmodus

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

- **PIN-Nummer + Active Directory-Benutzername und Kennwort** – Um die Files Advanced-App zu aktivieren und Zugriff auf Files Advanced-Server zu erhalten, muss der Benutzer eine einmalig verwendbare PIN-Nummer mit Ablaufdatum sowie einen gültigen Active Directory-Benutzernamen und ein gültiges Kennwort eingeben. Mit dieser Option wird sichergestellt, dass Benutzer nur ein Gerät und erst nach Erhalt einer vom IT-Administrator ausgestellten PIN-Nummer registrieren können. Diese Option wird empfohlen, wenn die erhöhte Sicherheit der Zwei-Faktoren-Geräteregistrierung gefordert wird.
- **Nur Active Directory-Benutzername und -Kennwort** – ein Benutzer kann die Files Advanced-App nur mit dem Active Directory-Benutzernamen und -Kennwort aktivieren. Diese Option ermöglicht

es dem Benutzer, ein Gerät oder mehrere Geräte zu einem beliebigen Zeitpunkt in der Zukunft zu registrieren. Dazu muss den Benutzern lediglich der Name des Files Advanced Client Management Servers mitgeteilt werden oder eine URL, die auf den Files Advanced Client Management Server zeigt. Diese kann auf einer Website veröffentlicht oder per E-Mail bereitgestellt werden, was die Einführung von Files Advanced bei einer großen Anzahl von Benutzern vereinfacht. Diese Option wird in Umgebungen bevorzugt, in denen eine Zwei-Faktor-Registrierung nicht erforderlich ist und möglicherweise viele Benutzer jederzeit Zugriff auf Files Advanced benötigen, zum Beispiel bei einem Einsatz im studentischen Umfeld.

Benutzer zum Registrieren einladen

Benutzer werden normalerweise über eine E-Mail, die vom Files Advanced Administrator gesendet wird, eingeladen, sich beim Files Advanced Server zu registrieren. Falls vom Server verlangt, enthält diese E-Mail eine einmalig zu verwendende PIN-Nummer, die für eine konfigurierbare Anzahl von Tagen gültig ist. Über diese PIN-Nummer ist die Registrierung der Mobile-App auf nur einem Gerät möglich. 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 Mobile-App im App Store ein, falls die App zunächst installiert werden muss. Sie schließt auch einen zweiten Link ein. Wenn Sie auf dem Gerät darauf tippen, wird Files Advanced Mobile geöffnet und das Client-Registrierungsformular automatisch mit dem Namen des Files Advanced Servers, der einmaligen PIN-Nummer für die Registrierung und dem Benutzernamen des Benutzers ausgefüllt. Bei Verwendung dieses Links muss der Benutzer lediglich sein Kontokennwort eingeben, um die Client-Registrierung abzuschließen.

- Sobald eine Registrierungseinladung generiert wurde, werden eingeladene Benutzer auf der Seite **Registrierungseinladungen** angezeigt. Für den Fall, dass Sie mit einem Benutzer auf einem anderen Weg als über die automatische E-Mail kommunizieren müssen, wird die PIN-Nummer jedes Benutzers aufgeführt.
- Sobald ein Benutzer seinen Files Advanced Mobile mit der einmaligen PIN-Nummer erfolgreich registriert hat, wird er nicht mehr in dieser Liste aufgeführt.
- Um die Einladungs-PIN-Nummer eines Benutzers zu widerrufen, drücken Sie 'Löschen', um die Angabe aus der Liste zu entfernen.

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

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

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

Hinweis: *Weitere Informationen zu den beiden Modi finden Sie im Bereich Einstellungen (S. 107).*

So erstellen Sie eine Files Advanced-Registrierungseinladung:

1. Rufen Sie die Registerkarte **Mobiler Zugriff** und die Registerkarte **Benutzer registrieren** auf.
2. Drücken Sie die Schaltfläche **Registrierungseinladung senden**.

3. Geben Sie einen Active Directory-Benutzernamen oder -Gruppennamen ein und klicken Sie auf 'Suchen'. Wenn eine Gruppe ausgewählt wird, können Sie 'Hinzufügen' drücken, um die jeweilige E-Mail-Adresse in der Gruppe in der Liste einzuladender Benutzer anzuzeigen. Auf diese Weise können Sie alle Mitglieder in einer Gruppe gleichzeitig einladen. Sie können auf Wunsch auch einzelne Gruppenmitglieder ausschließen, bevor Sie die Einladungen versenden. Die Suche nach Active Directory-Gruppen können Sie mit den Einschränkungen 'beginnt mit' oder 'enthält' ausführen. Suchvorgänge mit der Einschränkung 'beginnt mit' sind viel schneller als solche mit 'enthält'.
4. Sobald Sie den ersten Benutzer oder die erste Gruppe hinzugefügt haben, können Sie eine neue Suche starten und weitere Benutzer oder Gruppen zu der Liste hinzufügen.
5. Überprüfen Sie die Liste der einzuladenden Benutzer. Sie können nicht erwünschte Benutzer aus der Liste löschen.
6. Falls mit dem Konto eines Benutzers keine E-Mail-Adresse verknüpft ist, wird in der Spalte 'E-Mail-Adresse' die Meldung **Keine E-Mail-Adresse zugewiesen – zum Bearbeiten hier klicken** angezeigt. Sie können auf jeden dieser Einträge klicken, um manuell eine alternative E-Mail-Adresse für diesen Benutzer einzugeben. Falls für einen Benutzer **Keine E-Mail-Adresse zugewiesen** angezeigt wird, so wird dennoch eine PIN-Nummer für ihn generiert, die auf der Seite 'Benutzer registrieren' angezeigt wird. Sie müssen diese PIN-Nummer dem Benutzer auf andere Weise mitteilen, damit er seinen Files Advanced Mobile registrieren kann.

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

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

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

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

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

Bisher bei mobilEcho 4.5 oder früher registrierte Benutzer einladen

In mobilEcho 2.X musste keine PIN-Nummer eingegeben werden, um einen Client im Client Management-System zu registrieren. Für die Migration von mobilEcho 2.X Clients auf das Files Advanced Management-System sind zwei Optionen verfügbar. Standardmäßig erlauben es von 2.X aktualisierte mobilEcho Server den zuvor vom Server der Version 2.X verwalteten Clients, sich automatisch zu registrieren sowie in der Liste der Files Advanced **Geräte** angezeigt zu werden, ohne dass eine PIN-Nummer eingegeben werden muss. Wenn Sie sicherstellen möchten, dass alle Geräte,

die auf das System zugreifen, mit einer PIN-Nummer registriert wurden, können Sie diese Einstellung deaktivieren. Wenn der Benutzer nicht über die Berechtigung **Benutzer kann den Mobile Client aus der Verwaltung entfernen** verfügt, muss er in diesem Fall Files Advanced vom Gerät löschen und eine neue Kopie aus dem App Store neu installieren, bevor die Registrierung mit einer PIN-Nummer möglich ist.

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

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

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

6.3.2 Benutzerseitiger Verwaltungsregistrierungsvorgang

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

- Link zur Installation des Files Advanced Mobile über den Apple App Store
- Einen Link zum Starten der Mobile-App und zum Automatisieren des Registrierungsvorgangs
- Eine einmalige PIN-Nummer
- Die Adresse des Management-Servers
- Die E-Mail begleitet die Benutzer bei der Installation des Files Advanced Mobile und der Eingabe der Registrierungsinformationen.

Wenn die Mobile-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 Files Advanced automatisch gestartet, und das Registrierungsformular wird angezeigt. Die Server-Adresse, PIN-Nummer und der Benutzername des Benutzers sind ebenfalls in dieser URL kodiert, daher werden diese Felder im Registrierungsformular automatisch ausgefüllt. Zu diesem Zeitpunkt muss der Benutzer lediglich sein Kennwort 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 richtigen Benutzer- oder Gruppenverwaltungsrichtlinie zuzuordnen, den Zugriff auf Gateway Server zu ermöglichen und die Anmeldedaten für Files Advanced-Server-Anmeldungen zu speichern, falls die Verwaltungsrichtlinie der Benutzer dies zulässt.

Wenn die Verwaltungsrichtlinie ein Kennwort zur Sperrung der Applikation verlangt, werden die Benutzer aufgefordert, das Kennwort einzugeben. Alle Anforderungen bezüglich der Komplexität von

Kennwörtern in der Richtlinie des Benutzers werden für dieses erstmalige Kennwort sowie für jede zukünftige Änderung des Kennworts zur Sperrung der Applikation erzwungen.

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

So erfolgt die Registrierung für die Verwaltung

Automatisch per Registrierungs-E-Mail registrieren

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

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

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

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

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

Manuelle Registrierung

1. Öffnen Sie die Files Advanced-App.
2. Öffnen Sie **Einstellungen**.
3. Tippen Sie auf **Registrieren**.
4. Geben Sie Ihre Serveradresse, Ihre PIN (falls erforderlich), Benutzernamen und Kennwort ein.
5. Tippen Sie nach dem Ausfüllen des gesamten Formulars auf die Schaltfläche **Registrieren**.

6. Abhängig von der Konfiguration Ihres Unternehmensservers werden Sie unter Umständen gewarnt, dass das Sicherheitszertifikat des Management Servers nicht vertrauenswürdig ist. Um diese Warnung zu akzeptieren und fortzufahren, können Sie auf **Immer fortsetzen** klicken.
7. Wenn für die Files Advanced Mobile-App ein Kennwort zum Sperren der Applikation erforderlich ist, werden Sie aufgefordert, eines festzulegen. Möglicherweise gelten auch Anforderungen bezüglich der Komplexität des Kennworts. Diese werden gegebenenfalls angezeigt.

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

Fortlaufende Management-Updates

Nach der erstmaligen Management-Einrichtung versuchen Files Advanced Mobiles, bei jedem Starten der Client-App Kontakt mit dem Management-Server aufzunehmen. 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

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

Verwaltung entfernen

Es gibt zwei Optionen, den Files Advanced Mobile aus der Verwaltung zu entfernen:

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

Je nach Ihren Richtlinien für die Files Advanced-Verwaltung haben Sie eventuell das Recht, den Files Advanced Mobile 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 Files Advanced Mobile-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 Files Advanced aus der Verwaltung, indem Sie im Bestätigungsfenster auf **JA** tippen.

***Hinweis**: Wenn Ihre Files Advanced-Richtlinie das Entfernen des Clients aus der Verwaltung nicht zulässt, wird die Option **Verwaltung verwenden** im Menü **Einstellungen** nicht angezeigt. In diesem Fall besteht die einzige Möglichkeit, die Verwaltung für das Gerät aufzuheben, darin, die Mobile-Applikation zu deinstallieren. Durch Deinstallieren der Applikation werden alle Files Advanced Mobile-Daten und -Einstellungen gelöscht, und der Benutzer verfügt nach der erneuten Installation wieder über die Standardeinstellungen für die Applikation.*

Gehen Sie folgendermaßen vor, um die mobile Files Advanced-App zu deinstallieren:

Für iOS:

1. Halten Sie das Symbol der Mobile-Applikation solange gedrückt, bis es zu wackeln beginnt.
2. Tippen Sie auf der Mobile-Applikation auf das Symbol **X** und bestätigen Sie die Deinstallation.

Für Windows:

1. Tippen und halten Sie das App-Symbol.
2. Wählen Sie **Deinstallieren** aus.

Für Android:

***Hinweis:** Die Software bei Android-Geräten variiert, sodass Ihre Einstellungen leicht abweichen können.*

1. Öffnen Sie das App-Menü, und wählen Sie **Bearbeiten/Entfernen** aus.
2. Suchen Sie die Files Advanced-App, und wählen Sie diese aus.
3. Drücken Sie auf **Entfernen**.

6.4 Gateway Server verwalten

Der Files Advanced-Gateway-Server wird von der Files Advanced-Mobile-App 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 Files Advanced Server kann einen oder mehrere Gateway Server über dieselbe Managementkonsole verwalten und konfigurieren. Die verwalteten Gateway Server erscheinen im Bereich **Gateway Server** des Menüs **Mobiler Zugriff**.

- **Dateityp** – 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 Files Advanced Gateway Servers an.
- **Status** – gibt an, ob der Server online oder offline ist.
- **Aktive Sitzungen** – Anzahl der gegenwärtig aktiven Sitzungen auf diesem Gateway Server.
- **Verwendete Lizenzen** – Anzahl der verwendeten Lizenzen und Anzahl der verfügbaren Lizenzen.
- **Lizenz** – zeigt die gegenwärtig vom Gateway Server verwendeten Lizenzen an.

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

Anforderungen

Files Advanced nutzt die **Windows-Suche** zur Suche in Netzwerk-Datenquellen. **Windows-Suche** ist in Windows Server integriert, aber nicht standardmäßig aktiviert.

Sie können es wie folgt aktivieren:

- Installieren Sie die Rolle mit der Bezeichnung **Dateidienste** im Server-Manager bzw. fügen Sie diese hinzu.
- Der **Windows-Suchdienst** muss aktiviert sein und gestartet werden.

Hinweis: *Falls die Anforderungen nicht erfüllt werden, können Sie keine Suchen in Netzwerk-Datenquellen durchführen.*

Index für lokale Datenquellen für Dateinamensuche

Standardmäßig ist die indizierte Suche auf allen Gateway Servern aktiviert. Sie können die indizierte Suche für jeden Gateway Server im Dialogfeld **Server bearbeiten** des Gateway Servers aktivieren oder deaktivieren.

Standardpfad

Standardmäßig speichert Files Advanced Indexdateien auf einem eigenständigen Server im Verzeichnis **Suchindex** im Applikationsordner des Files Advanced Gateway Servers. Wenn die Indexdateien in einem anderen Verzeichnis gespeichert werden sollen, geben Sie den gewünschten Ordnerpfad ein.

Inhaltesuche mit Microsoft Windows Search unterstützen (wo verfügbar)

Die Unterstützung für Inhaltssuche in freigegebenen Ordnern ist standardmäßig aktiviert und kann durch Auswahl dieser Option aktiviert oder deaktiviert werden. Sie können Inhalte aktivieren und deaktivieren und so einzeln nach jedem Gateway Server suchen.

Die **Windows-Suche** kann so konfiguriert werden, dass die erforderlichen Datenquellen indiziert werden, wenn Sie mit der rechten Maustaste auf das Symbol für die Windows-Suche in der Startleiste klicken und die **Optionen für die Windows-Suche** auswählen. 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.*

Zusätzliche Konfigurationen

Die Indizierung bei der Inhaltssuche kann so konfiguriert werden, dass nur die Inhalte bestimmter Dateitypen indiziert werden.

1. Öffnen Sie auf Ihrem Server, auf dem der Gateway Server gehostet wird, **Systemsteuerung** -> **Indizierungsoptionen**.
2. Wählen Sie **Erweitert** und öffnen Sie die Registerkarte **Dateitypen**.
3. Suchen Sie nach den Dateitypen, für die Sie die Inhaltssuche aktivieren/deaktivieren möchten (z.B. **doc**, **txt** usw.).

Wählen Sie den gewünschten Dateityp aus, und wählen Sie unter **Wie soll diese Datei indiziert werden Indizierungseigenschaften und Dateiinhalte** aus, um die Inhaltssuche für diesen Dateityp zu aktivieren, oder **Indizierungseigenschaften**, um sie zu deaktivieren. Wiederholen Sie diesen Schritt für alle gewählten Dateitypen.

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

6.4.1 Neue Gateway-Server registrieren

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

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

   Hinweis: *Der Port 3000 ist der Standard-Port. Falls Sie den Standard-Port geändert haben, geben Sie im Anschluss an localhost Ihre Portnummer ein.*

3. Notieren Sie den **Administrationsschlüssel**.

4. Rufen Sie die Files Advanced-Weboberfläche auf.
5. Öffnen Sie die Registerkarte **Mobiler Zugriff**.
6. Öffnen Sie die Seite **Gateway Server**.
7. Drücken Sie die Schaltfläche **Einen neuen Gateway Server hinzufügen**.

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

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

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

Nachdem Sie Ihren Gateway-Server registriert haben, können Sie individuelle Zugriffsbeschränkungen für diesen Gateway-Server konfigurieren. Weitere Informationen hierzu finden Sie im Abschnitt Gateway-Server bearbeiten (S. 90).

6.4.2 Server-Details

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

Status

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

Aktive Benutzer

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

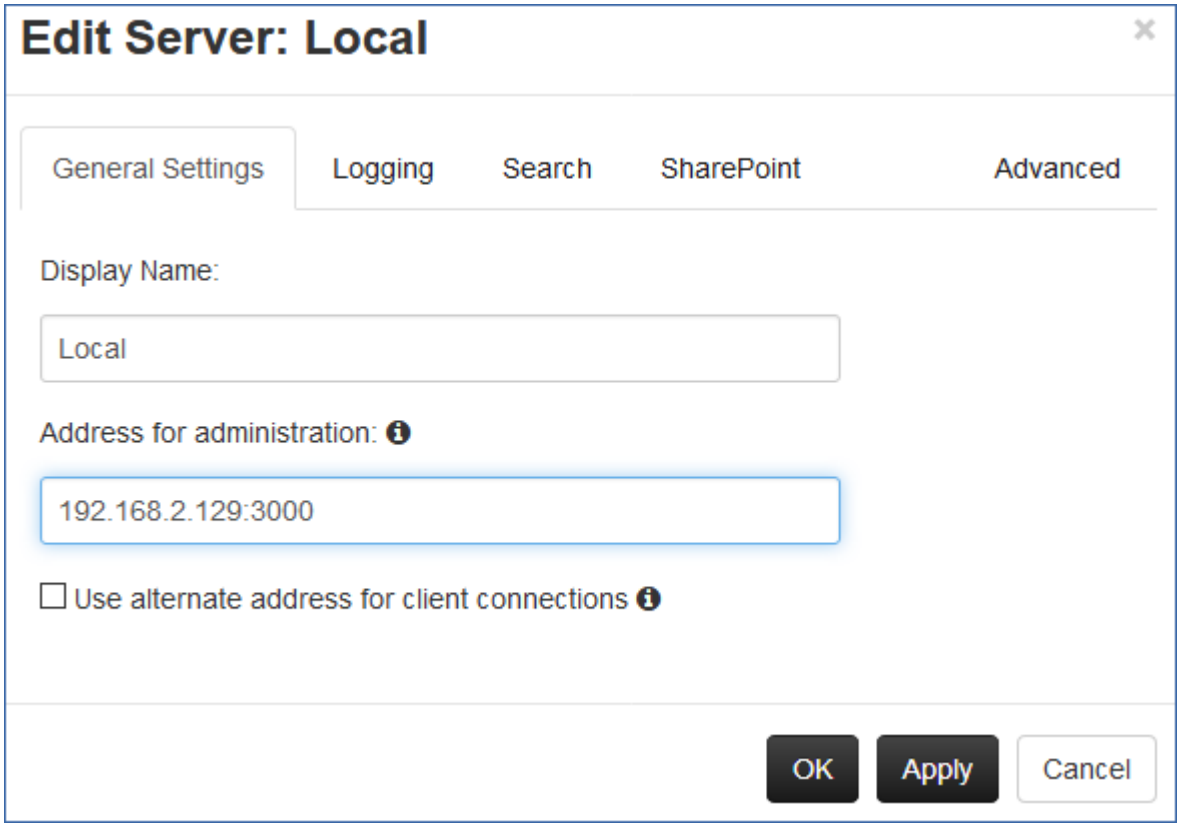
- **Benutzer** – zeigt den vollständigen Namen des Benutzers im Active Directory (AD) an.
- **Speicherort** – zeigt die IP-Adresse des Geräts an.
- **Gerät** – zeigt den Namen an, der diesem Gerät vom Benutzer zugewiesen wurde.
- **Modell** – zeigt den Typ und das Modell des Geräts an.
- **Betriebssystem** – zeigt das Betriebssystem des Geräts an.
- **Client-Version** – zeigt die Version der auf dem Gerät installierten Files Advanced-App.
- **Richtlinie** – zeigt die Richtlinie für das vom Gerät verwendete Konto an.
- **Leerlaufzeit** – zeigt an, wie lange der Benutzer mit dem Gateway verbunden ist.

6.4.3 Konfigurationen des Gateway Servers

Zur Änderung der Konfiguration Ihres Gateway Servers müssen Sie das Einstellungsmenü öffnen.

1. Navigieren Sie zur Registerkarte **Mobiler Zugriff** -> **Gateway Server**.
2. Klicken Sie auf den Pfeil neben **Details** für den gewünschten Server.
3. Wählen Sie **Bearbeiten** aus.

Themen



- **Anzeigename** – Legt den Anzeigenamen für den Gateway Server fest. Der Name ist rein kosmetisch und dient nur zur einfachen Unterscheidung zwischen Servern.
- **Adresse für Administration** – Legt die Standardadresse fest, unter welcher der Gateway Server vom Files Advanced Server und mobilen Clients erreicht werden kann. Wir empfehlen die Verwendung einer DNS-Adresse anstelle einer IP-Adresse.

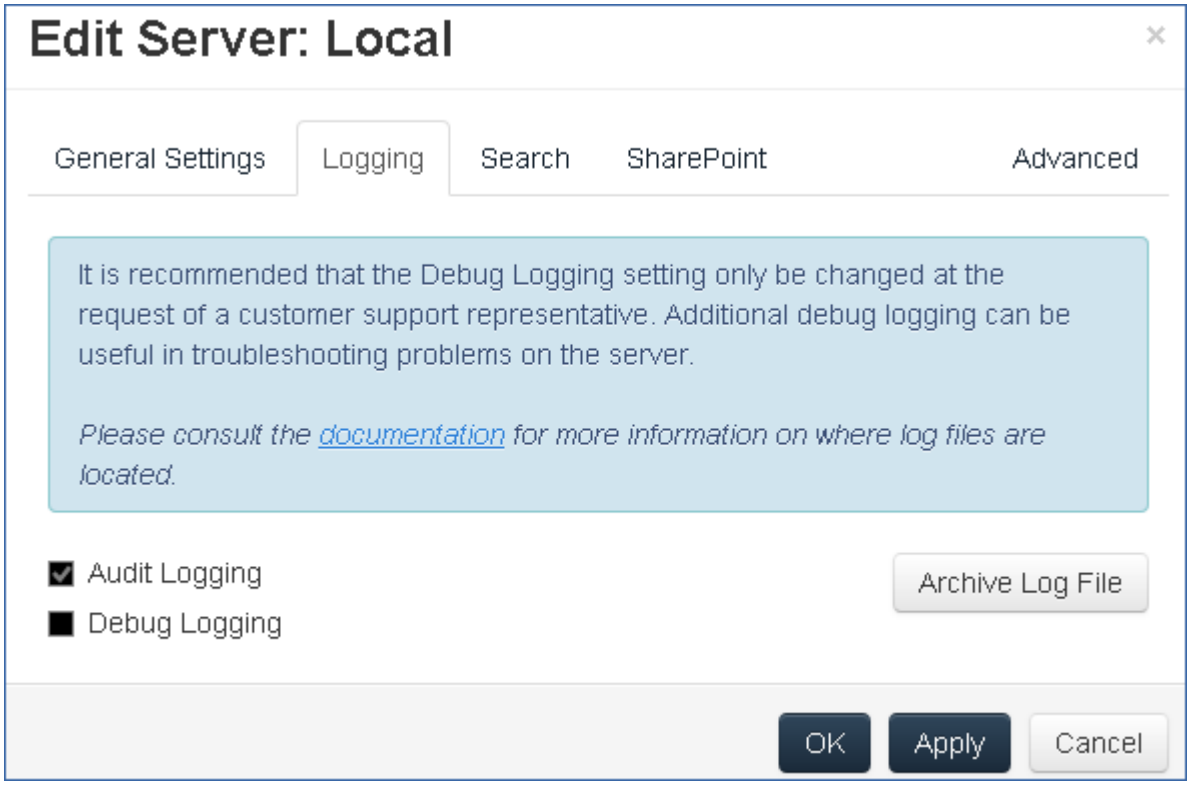
  Hinweis *Dies ist die Standardadresse, unter der mobile Clients eine Verbindung zum Gateway Server herstellen, es sei denn,* ***Alternative Adresse für Client-Verbindungen verwenden*** *wurde aktiviert.*

- **Alternative Adresse für Client-Verbindungen verwenden** – Bei Aktivierung wird die Adresse außer Kraft gesetzt, über die mobile Clients eine Verbindung zum Gateway Server herstellen.

  Hinweis: *Diese Einstellung sollte nur in spezifischen Konfigurationen verwendet werden, in denen Verbindungen zu Ihren Gateway Servern ein Lastenausgleichsmodul oder jegliche Art von Proxy durchlaufen (z.B. BlackBerry Dynamics, MobileIron usw.). Bei gängigen Bereitstellungen sollte diese nicht aktiviert werden.*

  - **Adresse für Client-Verbindungen** – Wenn **Alternative Adresse für Client-Verbindungen verwenden** aktiviert ist, wird dies die Adresse, die mobile Clients verwenden, um eine Verbindung zum Gateway Server herzustellen. Wir empfehlen die Verwendung einer DNS-Adresse anstelle einer IP-Adresse.

Im Abschnitt mit der Protokollierung können Sie festlegen, ob die Protokollierungsereignisse auf dem jeweiligen Gateway Server im Überwachungsprotokoll angezeigt werden und ob Debug-Protokollierung für diesen Server aktiviert wird.



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. Rufen Sie die Registerkarte **Gateway Server** auf.
5. Suchen Sie den Server, für den Sie **Audit Logs aktivieren möchten.**
6. Drücken Sie auf den Pfeil neben der Schaltfläche **Details** und wählen Sie **Bearbeiten** aus.
7. Aktivieren Sie im Bereich **Protokollierung** die Option **Überwachungsprotokollierung**.
8. Klicken Sie auf 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. Klicken Sie auf 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. Drücken Sie auf den Pfeil neben der Schaltfläche **Details** und wählen Sie **Bearbeiten** aus.

7. Aktivieren Sie im Bereich **Protokollierung** die Option **Debug-Protokollierung**.
8. Klicken Sie auf die Schaltfläche **Speichern**.

Anforderungen

Files Advanced nutzt die **Windows-Suche** zur Suche in Netzwerk-Datenquellen. **Windows-Suche** ist in Windows Server integriert, aber nicht standardmäßig aktiviert.

Sie können es wie folgt aktivieren:

- Installieren Sie die Rolle mit der Bezeichnung **Dateidienste** im Server-Manager bzw. fügen Sie diese hinzu.
- Der **Windows-Suchdienst** muss aktiviert sein und gestartet werden.

Hinweis: *Falls die Anforderungen nicht erfüllt werden, können Sie keine Suchen in Netzwerk-Datenquellen durchführen.*

Index für lokale Datenquellen für Dateinamensuche

Standardmäßig ist die indizierte Suche auf allen Gateway Servern aktiviert. Sie können die indizierte Suche für jeden Gateway Server im Dialogfeld **Server bearbeiten** des Gateway Servers aktivieren oder deaktivieren.

Standardpfad

Standardmäßig speichert Files Advanced Indexdateien auf einem eigenständigen Server im Verzeichnis **Suchindex** im Applikationsordner des Files Advanced Gateway Servers. Wenn die Indexdateien in einem anderen Verzeichnis gespeichert werden sollen, geben Sie den gewünschten Ordnerpfad ein.

Inhaltesuche mit Microsoft Windows Search unterstützen (wo verfügbar)

Die Unterstützung für Inhaltssuche in freigegebenen Ordnern ist standardmäßig aktiviert und kann durch Auswahl dieser Option aktiviert oder deaktiviert werden. Sie können Inhalte aktivieren und deaktivieren und so einzeln nach jedem Gateway Server suchen.

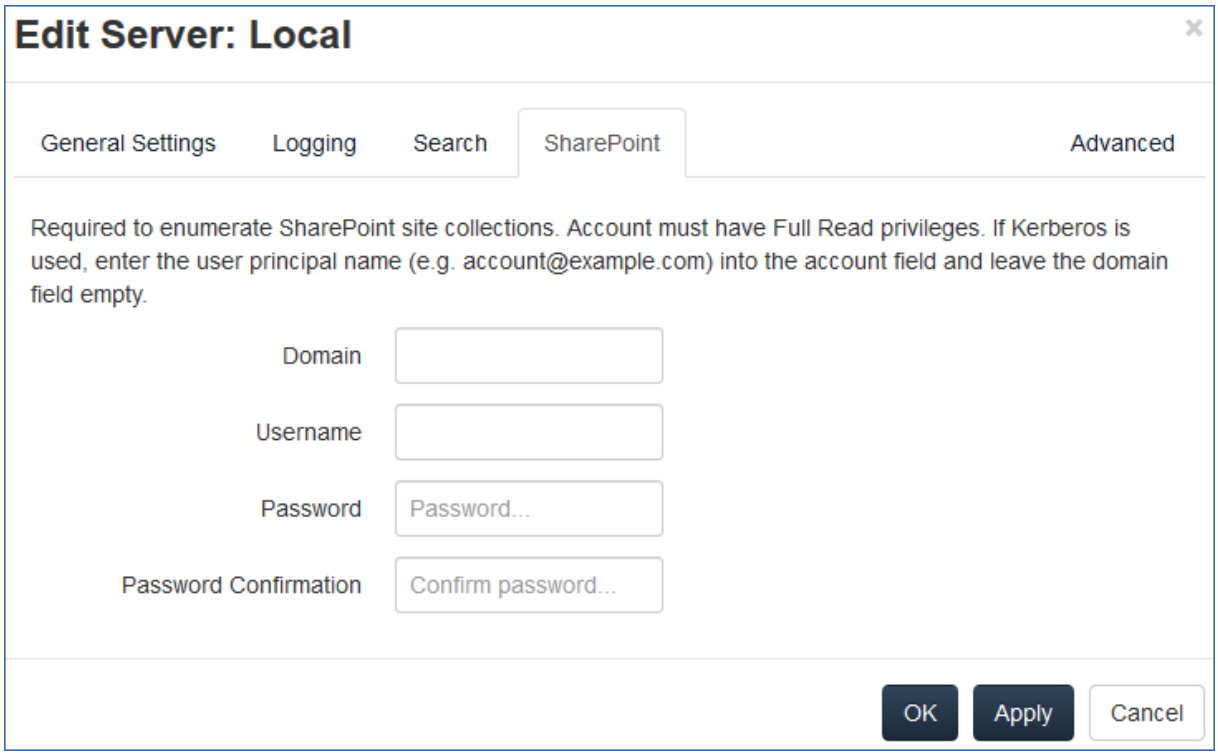
Die **Windows-Suche** kann so konfiguriert werden, dass die erforderlichen Datenquellen indiziert werden, wenn Sie mit der rechten Maustaste auf das Symbol für die Windows-Suche in der Startleiste klicken und die **Optionen für die Windows-Suche** auswählen. Sie können Windows-Inhaltssuchvorgänge in 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.*

Zusätzliche Konfigurationen

Die Indizierung bei der Inhaltssuche kann so konfiguriert werden, dass nur die Inhalte bestimmter Dateitypen indiziert werden.

1. Öffnen Sie auf Ihrem Server, auf dem der Gateway Server gehostet wird, **Systemsteuerung** -> **Indizierungsoptionen**.
2. Wählen Sie **Erweitert** und öffnen Sie die Registerkarte **Dateitypen**.
3. Suchen Sie nach den Dateitypen, für die Sie die Inhaltssuche aktivieren/deaktivieren möchten (z.B. **doc**, **txt** usw.).
4. Wählen Sie den gewünschten Dateityp aus, und wählen Sie unter **Wie soll diese Datei indiziert werden Indizierungseigenschaften und Dateiinhalte** aus, um die Inhaltssuche für diesen Dateityp zu aktivieren, oder **Indizierungseigenschaften**, um sie zu deaktivieren. Wiederholen Sie diesen Schritt für alle gewählten Dateitypen.



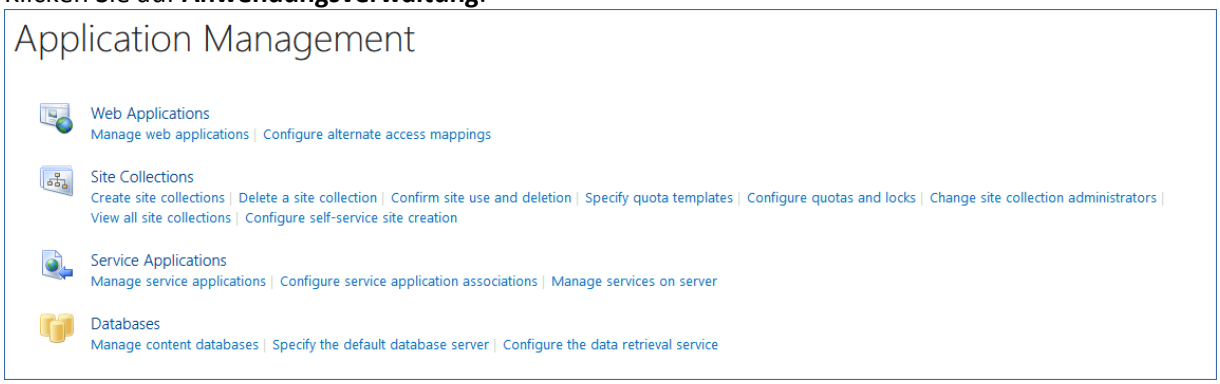
Für die allgemeine Unterstützung von SharePoint ist die Eingabe dieser Zugangsdaten optional. Sie ist aber erforderlich, um Websitesammlungen aufzulisten. Sie haben beispielsweise zwei Websitesammlungen:

`http://sharepoint.example.com` und
`http://sharepoint.example.com/SeparateCollection.`

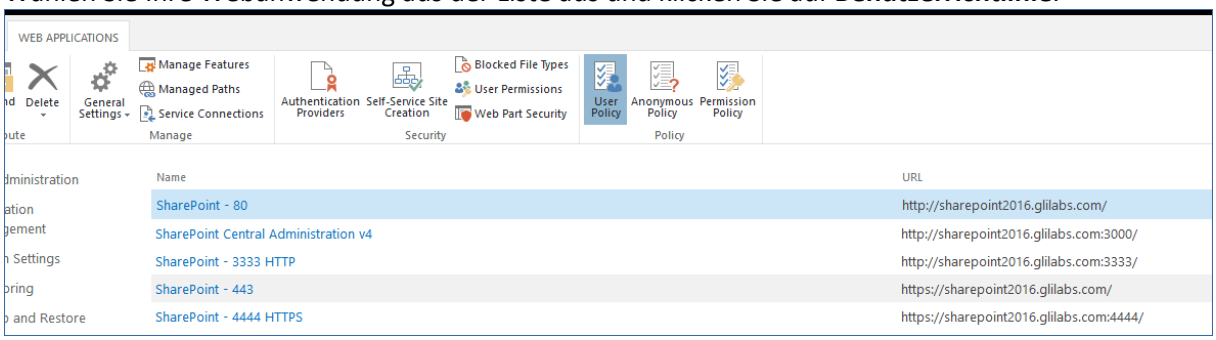
Ohne die Eingabe der Zugangsdaten sehen Sie, wenn Sie ein Volume mit Verweis auf **http://sharepoint.beispiel.com** erstellen, beim Auflisten des Volumes nicht den Ordner mit dem Namen **SeparateSammlung**. Das Konto muss **vollen Lesezugriff** auf die Webanwendung haben.

Führen Sie die folgenden Schritte (für SharePoint 2016 und SharePoint 2010) aus, um für Ihr Konto den vollständigen Lesezugriff zu konfigurieren:

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

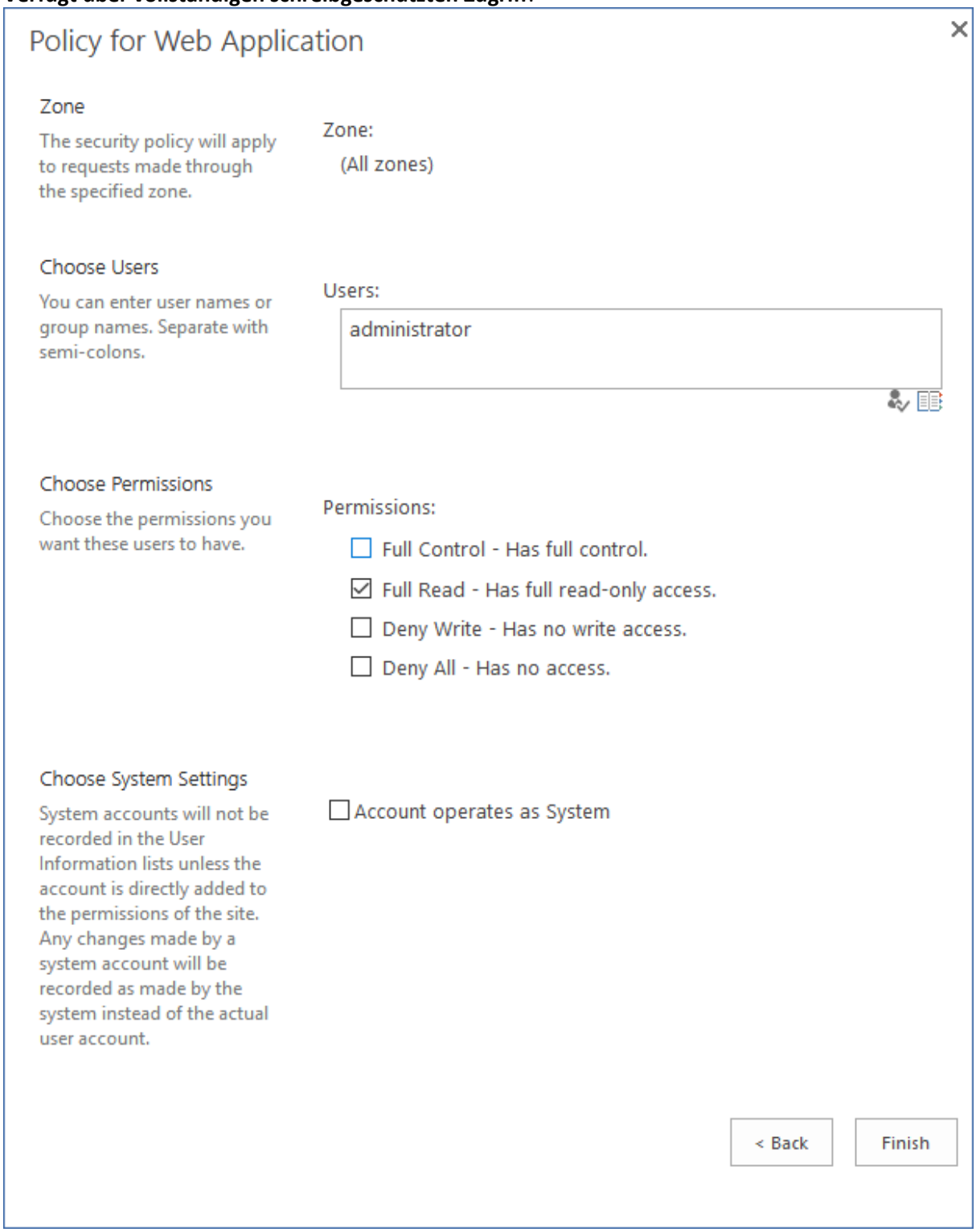


3. Klicken Sie unter **Webanwendungen** auf **Webanwendungen verwalten**.
4. Wählen Sie Ihre Webanwendung aus der Liste aus und klicken Sie auf **Benutzerrichtlinie**.



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**.

***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 Reshares 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 Files Advanced-Android-Client-App.

- **Minimale iOS-Client-Version** - Wenn aktiviert, Benutzer, die eine Verbindung mit diesem Gateway herstellen, benötigen diese oder eine spätere Version der Files Advanced-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 Files Advanced Windows-Server muss die Berechtigung erhalten, delegierte Zugangsdaten zu Ihrem SharePoint-Server für Ihre Benutzer anzuzeigen. Kerberos-Delegierung auf Files Advanced-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 Files Advanced zugreifen können sollen. Wenn Ihre SharePoint-Implementierung aus mehreren Knoten mit Lastenausgleich besteht, müssen Sie dieser Liste zugelassener Computer jeden SharePoint-/Windows-Knoten hinzufügen. Klicken Sie auf **Hinzufügen**, um in AD nach diesen Windows-Computern zu suchen und sie hinzuzufügen. Für jeden Computer muss nur der Diensttyp 'http' ausgewählt werden.

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

- **Verbindungen zu SharePoint-Servern mit selbstsignierten Zertifikaten erlauben** – Wenn aktiviert, ermöglicht Verbindungen von diesem Gateway zu SharePoint-Servern mithilfe selbstsignierter Zertifikate.
- **Selbstsignierte Zertifikate von diesem Gateway Server akzeptieren** – Wenn aktiviert, ermöglicht Verbindungen von diesem Gateway zu Files Advanced-Servern mithilfe selbstsignierter Zertifikate.
- **Verbindungen zu Files Advanced Servern mit selbstsignierten Zertifikaten erlauben** – Wenn aktiviert, ermöglicht Verbindungen zu anderen Files Advanced 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).
- **Aushandeln/Kerberos-Authentifizierung im Benutzermodus durchführen** – Wenn diese Option aktiviert ist, wird der Gateway Server mithilfe des Kerberos-Tickets des verbindenden Benutzers bei Datenquellen authentifiziert. Dies wird nur für Konfigurationen verwendet, bei denen Kerberos erforderlich ist (z. B. Single Sign-On und Lastenausgleich).

Sie können entweder die unter Richtlinien (S. 55) festgelegten Standardzugriffsbeschränkungen verwenden oder eigene Beschränkungen für jeden Gateway Server festlegen.

Benutzerdefinierte Zugriffsbeschränkungen für einen bestimmten Gateway Server festlegen

1. Navigieren Sie zur Registerkarte **Mobiler Zugriff** -> **Gateway Server**.
2. Klicken Sie auf den Pfeil neben **Details** für den gewünschten Server.
3. Wählen Sie **Zugriffsbeschränkungen** aus.
4. Rufen Sie die Registerkarte **Benutzerdefinierte Einstellungen verwenden** auf.
5. Wählen Sie die gewünschten Zugriffsbeschränkungen für diesen Gateway Server aus.
6. Klicken Sie auf **Anwenden**.

6.4.4 Cluster-Gruppen

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

Eine Cluster-Gruppe ist eine Sammlung von Gateway Servern mit derselben Konfiguration. Auf diese Weise können Sie alle Gateways in dieser Gruppe gleichzeitig steuern, ohne dieselben Einstellungen auf jedem Gateway einzeln konfigurieren zu müssen. Diese Server befinden sich normalerweise hinter einem Lastenausgleichsmodul (S. 188), um mobilen Clients eine hohe Verfügbarkeit und Skalierbarkeit zu bieten.

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

So erstellen Sie eine Cluster-Gruppe:

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

1. Rufen Sie die Files Advanced-Weboberfläche auf.
2. Öffnen Sie die Registerkarte **Mobiler Zugriff**.
3. Öffnen Sie die Seite **Gateway Server**.
4. Drücken Sie die Schaltfläche **Cluster-Gruppe hinzufügen**.
5. Geben Sie einen Anzeigenamen für die Gruppe ein.
6. Geben Sie den DNS-Namen oder die IP-Adresse des Lastenausgleichsmoduls ein.
7. Wählen Sie gegebenenfalls eine alternative Adresse für Files Advanced Server-Verbindungen aus, indem Sie das Kontrollkästchen wieder aktivieren und die Adresse eingeben.
8. Aktivieren Sie das Kontrollkästchen für jedes Gateway, das in die Gruppe aufgenommen werden soll.

9. Wählen Sie das Gateway, das die Einstellungen der Gruppe steuert. Alle bereits festgelegten Einstellungen dieses Gateways (einschließlich zugewiesener Datenquellen, jedoch nicht die Adresse für Administration) werden auf alle anderen Gateways in der Gruppe kopiert.
10. Drücken Sie **Erstellen**.

So bearbeiten Sie eine Cluster-Gruppe:

Das Bearbeiten von Cluster-Gruppen unterscheidet sich nicht vom Bearbeiten herkömmlicher Gateways. Weitere Informationen hierzu finden Sie im Artikel Gateway Server bearbeiten (S. 90).

Mitglieder zu einer bestehenden Cluster-Gruppe hinzufügen:

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

Master Gateway Server ändern:

1. Öffnen Sie die Weboberfläche und navigieren Sie zu **Mobiler Zugriff**-> **Gateway Server**.
2. Erweitern Sie die gewünschte Clustergruppe.
3. Suchen Sie den Gateway Server, der zum Masterserver hochgestuft werden soll.
4. Klicken Sie auf die Schaltfläche **Aktionen** und dann auf **Gruppen-Master werden**.

6.5 Datenquellen verwalten

Sie können NTFS-Verzeichnisse, die sich auf Ihrem Windows-Server befinden, auf CMIS-Systemen oder auf einer entfernten SMB/CIFS-Dateifreigabe für den Zugriff durch Ihre Files Advanced Benutzer freigeben. Wenn sich Benutzer verbinden, werden diese Verzeichnisse als Dateifreigabe-Volumes angezeigt.

Zugriff auf Inhalt von SharePoint 2007, 2010, 2013, 2016 und 365

Files Advanced bietet Zugriff auf Dateien, die in Dokumentbibliotheken auf Servern von SharePoint 2007, 2010, 2013, 2016 und 365 gespeichert sind. Eine SharePoint-Datenquelle von Files Advanced kann auf einen kompletten SharePoint-Server, eine bestimmte SharePoint-Website oder -Unterwebsite oder auf eine bestimmte Dokumentbibliothek verweisen. Diese Dateien können geöffnet, in PDF kommentiert, bearbeitet und synchronisiert werden – genau wie Dateien, die auf traditionellen Servern oder NAS-Speichern gespeichert sind. Files Advanced unterstützt auch die Funktionen **Auschecken** und **Einchecken** von SharePoint-Dateien.

Unterstützte SharePoint-Authentifizierungsmethoden

Files Advanced unterstützt SharePoint-Server, die die Client-Authentifizierung mit NTLMv1, NTLMv2, mit Claims-basierter Authentifizierung und Kerberos ermöglichen. Wenn für Ihren SharePoint-Server die Kerberos-Authentifizierung erforderlich ist, müssen Sie eine Aktualisierung des Active Directory-Computerobjekts für den Windows-Server oder für Server durchführen, auf denen die Files

Advanced Serversoftware ausgeführt wird. Der Files Advanced Windows-Server muss die Berechtigung erhalten, delegierte Zugangsdaten zu Ihrem SharePoint-Server für Ihre Benutzer anzuzeigen.

Bei der Claims-basierten Authentifizierung wird die Authentifizierung mit einem Authentifizierungsserver durchgeführt und der so erhaltene Authentifizierungstoken wird an den SharePoint-Server weitergegeben. Es erfolgt keine Authentifizierung mit dem SharePoint-Server direkt. Acronis Access unterstützt die Claims-basierte Authentifizierung für Office 365 SharePoint-Websites. Bei der Authentifizierung kontaktiert der Gateway Server zunächst Microsoft Online, um den Speicherort des Authentifizierungsservers zu ermitteln. Dieser Server kann von Microsoft Online gehostet sein oder kann sich im Unternehmensnetzwerk befinden (über Active Directory-Verbunddienste). Nach der Authentifizierung und dem Erhalt eines binären Sicherheitstokens wird dieser Token an den SharePoint-Server gesendet, der ein Authentifizierungs-Cookie zurückgibt. Dieses Cookie wird dann anstelle von anderen Anmeldeinformationen der Benutzer an SharePoint gesendet.

Zugriff auf Inhalt von OneDrive for Business

Files Advanced kann eingerichtet werden, um Benutzern den Zugriff auf ihren persönlichen OneDrive for Business-Inhalt über eine SharePoint-Datenquelle zu ermöglichen. Es gibt einige Anforderungen und Beschränkungen.

Berechtigungen für freigegebene Dateien und Ordner ändern

Files Advanced verwendet die bestehenden Benutzerkonten und Kennwörter von Windows. Da Files Advanced die Windows NTFS-Berechtigungen durchsetzt, sollten Sie normalerweise die integrierten Tools von Windows für das Anpassen der Verzeichnis- und Dateiberechtigungen verwenden. Die Standardtools von Windows bieten die größte Flexibilität beim Festlegen Ihrer Sicherheitsrichtlinie.

Der Zugriff auf Files Advanced Datenquellen, die sich auf einem anderen SMB/CIFS-Dateiserver befinden, erfolgt über eine SMB/CIFS-Verbindung vom Gateway Server zum zweiten Server oder NAS-Gerät. In diesem Fall wird der Zugriff auf den sekundären Server im Kontext des Benutzers durchgeführt, der an einem der Access-Cients angemeldet ist. Damit diese Benutzer Zugriff auf die Dateien auf dem sekundären Server haben, müssen ihre Konten die 'Windows-Freigabeberechtigungen' und die NTFS-Sicherheitsberechtigungen für den Zugriff auf diese Dateien aufweisen.

Die Berechtigungen für Dateien, die sich auf den SharePoint-Servern befinden, werden in Übereinstimmung mit den SharePoint-Berechtigungen festgelegt, die auf dem SharePoint-Server konfiguriert werden. Benutzer erhalten dieselben Berechtigungen über Files Advanced wie beim Zugriff auf SharePoint-Dokumentbibliotheken bei Verwendung eines Webbrowsers.

Themen

6.5.1 Ordner

Ordner können zu den Benutzer- und Gruppenrichtlinien von Files Advanced hinzugefügt werden, sodass sie automatisch in der Files Advanced App eines Benutzers angezeigt werden. Ordner können so konfiguriert werden, dass sie auf alle Ordner verweisen, die sich auf einem Gateway Server, einer Remote-Freigabe, einem CMIS-Volume oder einer SharePoint-Bibliothek befinden. So können Sie Benutzern direkten Zugriff auf alle möglicherweise wichtigen Ordner gewähren, ohne dass Benutzer zu diesem Ordner navigieren müssen oder den genauen Server, den Namen des freigegebenen Volumes oder den Pfad zu diesem Ordner kennen müssen.

Ordner können auf beliebige Inhaltstypen zeigen, auf die Files Advanced Zugriff gewährt. Sie verweisen einfach auf Speicherorte auf Gateway Servern, die bereits innerhalb der Verwaltung von Files Advanced konfiguriert wurden. Dies kann ein lokales Volume für Dateifreigaben, ein Network Reshare-Volume mit Zugriff auf Dateien auf einem anderen Dateiserver oder NAS-Gerät, eine DFS-Freigabe, ein CMIS-Volume 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

Hinweis: *Wenn Sie Sync & Share bei einer Neuinstallation von Files Advanced 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.*

Synchronisieren von Ordnern

Ordner können so konfiguriert werden, dass sie mit dem Client-Gerät synchronisiert werden. Folgende Optionen stehen für die Files Advanced Synchronisierung von Ordnern zur Verfügung:

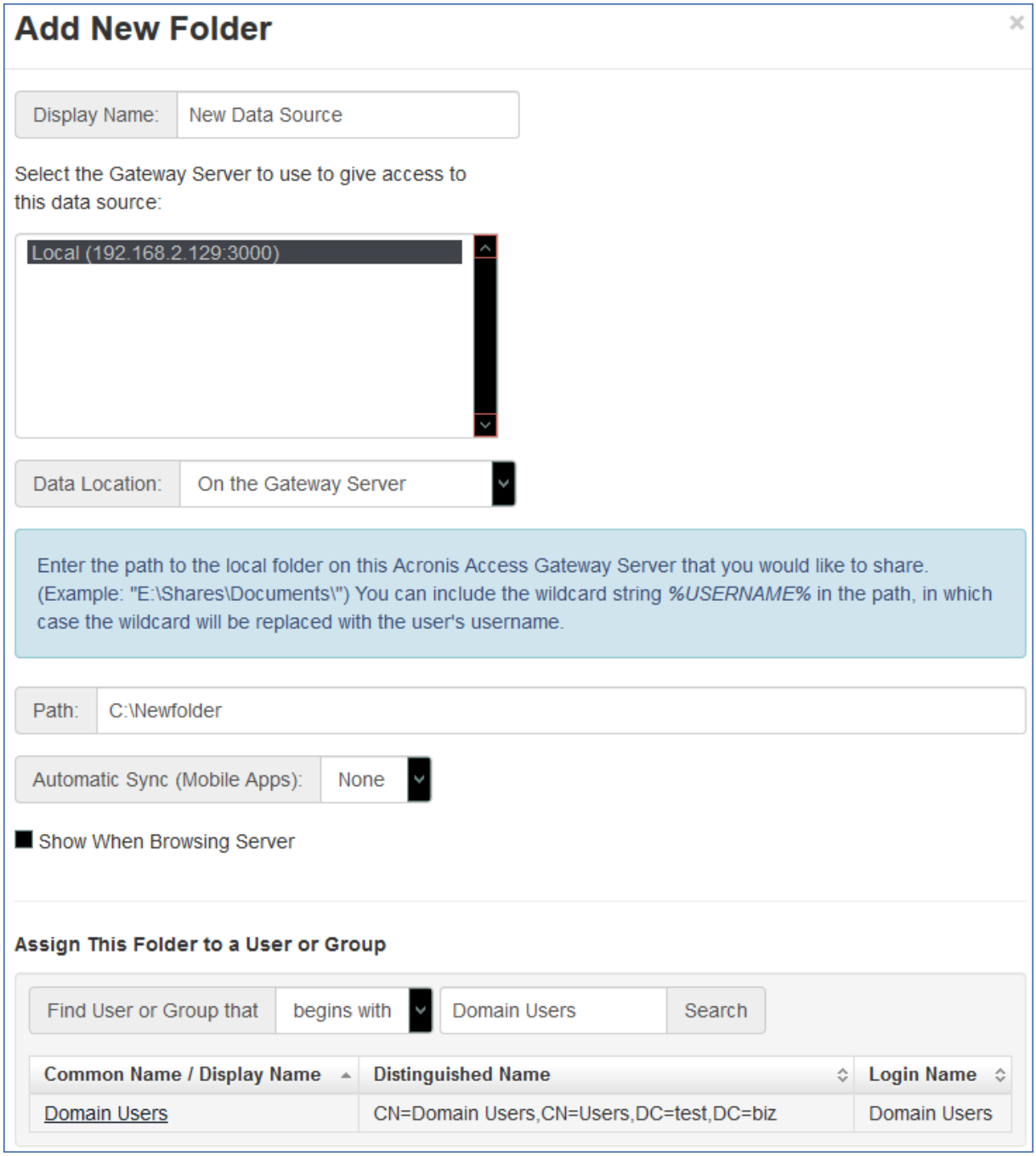
Hinweis: *Diese Einstellung hat keinen Einfluss auf den Desktop Client.*

- **Keine** – Der Ordner wird als netzwerkbasierte Ressource in der Files Advanced App angezeigt und es kann wie bei einem Gateway Server auf ihn zugegriffen und mit ihm verfahren werden.
- **1-Weg** – Der Ordner wird als lokaler Ordner in der Files Advanced App 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-Weg** – Der Ordner wird als lokaler Ordner in der Files Advanced App 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.

Datenquellen erstellen

1. Öffnen Sie die Files Advanced 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 Files Advanced-Clients den Gateway Server durchsuchen.

    Hinweis: *Beim Erstellen von SharePoint-Datenquellen haben Sie die Option, die Anzeige SharePoint-gefolgter Websites zu aktivieren.*

12. Drücken Sie 'Speichern'.

Datenquellen bearbeiten

1. Öffnen Sie den Abschnitt **Datenquellen** und machen Sie die Datenquelle ausfindig, die Sie bearbeiten möchten.
2. Klicken Sie auf das **Bleistiftsymbol** für Ihre Datenquelle auf der rechten Seite der Tabelle.
3. Ändern Sie alle gewünschten Parameter und drücken Sie auf **Speichern**.

Durch Erstellen einer Datenquelle können Sie den Files Advanced 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 füreine **SharePoint-Website** oder **-Unterwebsite** - Sie müssen 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
```

SharePoint-gefolgte Websites

SharePoint-gefolgte Websites können aktiviert werden, wenn Sie die Datenquelle für Ihre Website erstellen. Dies geschieht über das Kontrollkästchen 'Gefolgte Websites anzeigen'. Nach der Aktivierung sehen alle Benutzer, die Websites folgen, in Files Advanced den Ordner 'Gefolgte Websites', der die Ressourcen enthält, auf die sie von diesen Websites zugreifen dürfen.

Hinweis: *SharePoint-gefolgte Websites können nicht synchronisiert werden.*

Datenquelle erstellen für eine SharePoint-Bibliothek

Beim Erstellen einer Datenquelle für eine SharePoint-Bibliothek 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 Files Advanced Mobile 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. 90).

Unterstützte CMIS-Volumes sind **Alfresco (CMIS)**- und **Documentum (CMIS)**-Volumes. Sie können auch versuchen, andere CMIS-Anbieter zu verwenden, die das **AtomPub**-Protokoll mit der Option **Allgemeiner CMIS (AtomPub)** einsetzen. Diese Option funktioniert für Ihren Anbieter nicht und wird von Acronis nicht unterstützt.

Auf dem Gerät, das die CMIS-Volumes hostet, sollte ein Gateway-Server vorhanden sein, um Zeitüberschreitungen in langsamen Netzwerken zu reduzieren.

Hinweis: *CMIS-Volumes verfügen über eine Beschränkung, die das Kopieren von Ordnern nicht gestattet.*

Da OneDrive for Business auf SharePoint basiert, kann auf den Inhalt zugegriffen werden, wenn eine SharePoint Datenquelle in Files Advanced erstellt wird. Hierfür gelten jedoch einige Beschränkungen.

- Die Datenquelle **muss** auf den Platzhalter für einen persönlichen Hauptordner des Benutzers verweisen. Es können keine Datenquellen erstellt werden, die auf untergeordnete Ordner verweisen. Es kann jedoch über den Hauptordner darauf zugegriffen werden und sie können durchsucht werden.
- Diese Datenquellen arbeiten nicht, wenn der Gateway Server manuell in die App aufgenommen wird. Er muss über eine Richtlinie zugewiesen werden.
- Active Directory muss mit Office 365 verknüpft werden. Verwenden Sie AD-Verbunddienste oder ein Azure-AD.
- Ein Benutzer kann nur die eigenen OneDrive-Daten anzeigen und hat keinen Zugriff auf die Daten von anderen Benutzern. Dies ist unabhängig davon, ob diese über das Microsoft-Portal freigegeben wurden bzw. über das Portal darauf zugegriffen werden kann.

Datenquellen erstellen

1. Öffnen Sie die Files Advanced 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 diese Ressourcen erfolgt.
8. Geben Sie den Speicherort der OneDrive for Business-Hauptwebsite und anschließend den Pfad für einen persönlichen Ordner mit dem Platzhalter **%USERNAME%** ein.

   Beispiel: `https://mycompany.sharepoint.com/personal/%USERNAME%`
9. Drücken Sie auf **Speichern**.

Integration von Active Directory

Hinweis: *Das Verwalten von Active Directory oder Microsoft Azure ist* ***keine*** *Funktion von Files Advanced! Wenn Sie Probleme mit Azure oder Office 365 haben, wenden Sie sich an den* ***Microsoft Support.***

Office 365 verwendet die cloudbasierte Benutzeridentitätsverwaltung vom Azure Active Directory Service für die Verwaltung von Benutzern. Wenn Sie bereits die Azure AD-Dienste verwenden, müssen Sie nur die Datenquelle erstellen.

Andernfalls können Sie Ihr lokales Active Directory mit Azure AD integrieren, indem sie Ihre lokale Umgebung mit Office 365 synchronisieren.

Eine dritte Option besteht in der manuellen Neuerstellung der notwendigen Konten im Verwaltungsbereich von Office 365. Diese Methode wird jedoch nur empfohlen, wenn Sie nur sehr wenige Konten verwenden.

6.5.2 Zugewiesene Quellen

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

- In der Server-Tabelle sind der Anzeigename, der DNS-Name oder die IP-Adresse des Gateway-Servers sowie die Richtlinien aufgeführt, denen der Server zugewiesen ist.
- In der Ordner-Tabelle sind der Anzeigename der Datenquelle, der Gateway Server, der Synchronisierungstyp, der Pfad und die Richtlinien aufgeführt, auf die diese Datenquelle zugewiesen ist.
- Wenn Sie auf die Schaltfläche **An %1 zugewiesene Ressourcen bearbeiten** klicken, kann der Administrator die Zuweisungen für diese Richtlinie schnell bearbeiten.

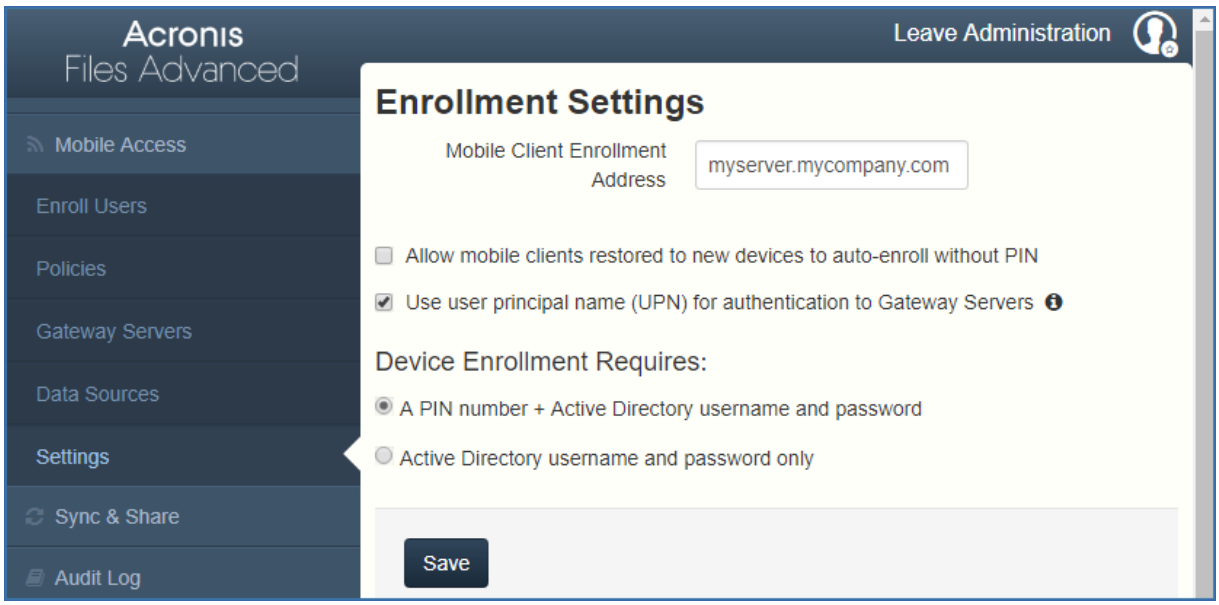
6.5.3 Auf Clients sichtbare Gateway Server

Gateway Server können Benutzer- oder Gruppenrichtlinien zugewiesen und als Datenquellen eingesetzt werden. Auf dieser Seite werden alle Gateway Server angezeigt, die in der Files Advanced Mobile-App eines Benutzers vorliegen, und es wird angezeigt, ob diesen Gateway Servern Benutzer- oder Gruppenrichtlinien zugewiesen wurden. Außerdem können Sie diese Zuordnungen hier bearbeiten. Wenn die Files Advanced Mobile-Benutzer einen Gateway Server durchsuchen, sehen sie die Datenquellen, für welche die Option **Anzeigen, wenn Gateway Server durchsucht wird** aktiviert ist.

So ändern Sie die aktuelle Zuordnung eines Servers:

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

6.6 Einstellungen



Registrierungseinstellungen

- **Registrierungsadresse für Mobile Client** – 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 Client Management speichert die mobile Files Advanced-App die Adresse des Files Advanced-Servers. Wenn es sich hierbei um eine IP-Adresse handelt und sich diese ändert, können die Benutzer den Server nicht erreichen, die Verwaltung der App kann nicht aufgehoben werden und die Benutzer müssen die gesamte App löschen und sich erneut zur Verwaltung registrieren.*

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

Geräteregistrierung erfordert:

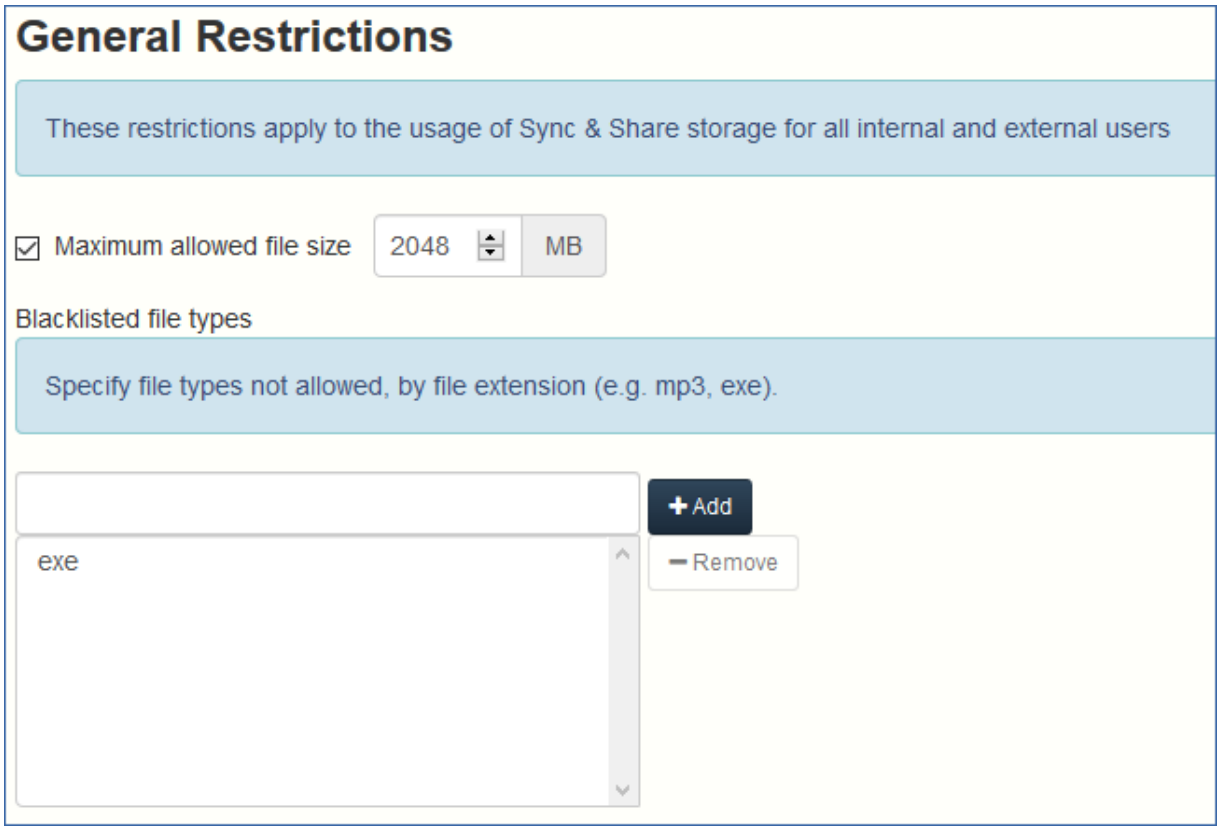
- **PIN-Nummer + Active Directory-Benutzername und Kennwort** – Um die Files Advanced-App zu aktivieren und Zugriff auf Files Advanced-Server zu erhalten, muss der Benutzer eine einmalig verwendbare PIN-Nummer mit Ablaufdatum sowie einen gültigen Active Directory-Benutzernamen und ein gültiges Kennwort eingeben. Mit dieser Option wird sichergestellt, dass Benutzer nur ein Gerät und erst nach Erhalt einer vom IT-Administrator ausgestellten PIN-Nummer registrieren können. Diese Option wird empfohlen, wenn die erhöhte Sicherheit der Zwei-Faktoren-Geräteregistrierung gefordert wird.
- **Nur Active Directory-Benutzername und -Kennwort** – ein Benutzer kann die Files Advanced-App nur mit dem Active Directory-Benutzernamen und -Kennwort aktivieren. Diese Option ermöglicht es dem Benutzer, ein Gerät oder mehrere Geräte zu einem beliebigen Zeitpunkt in der Zukunft zu registrieren. Dazu muss den Benutzern lediglich der Name des Files Advanced Client Management Servers mitgeteilt werden oder eine URL, die auf den Files Advanced Client Management Server zeigt. Diese kann auf einer Website veröffentlicht oder per E-Mail bereitgestellt werden, was die Einführung von Files Advanced bei einer großen Anzahl von Benutzern vereinfacht. Diese Option wird in Umgebungen bevorzugt, in denen eine Zwei-Faktor-Registrierung nicht erforderlich ist und möglicherweise viele Benutzer jederzeit Zugriff auf Files Advanced benötigen, zum Beispiel bei einem Einsatz im studentischen Umfeld.

7 Synchronisieren und Freigeben

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

Themen

7.1 Allgemeine Beschränkungen



Sie können grundlegende Beschränkungen festlegen, wie zum Beispiel das Hinzufügen bestimmter Dateitypen und von Dateien ab einer bestimmten Größe zu einer Blacklist.

Maximal erlaubte Dateigröße - Diese Option ermöglicht das Festlegen einer maximalen Dateigröße für alle Sync & Share-Dateien.

Gesperrte Dateitypen - Mit dieser Option können Sie bestimmte Dateitypen von der Sync & Share-Funktion ausschließen.

Gehen Sie folgendermaßen vor, um eine Blacklist für Dateitypen anzulegen:

1. Erweitern Sie in der Webkonsole die Registerkarte **Sync & Share**, und öffnen Sie **Allgemeine Beschränkungen**.
2. Geben Sie im **Feld zum Hinzufügen** unter **Gesperrte Dateitypen** eine mit Komma getrennte Liste aller Dateitypen ein, die gesperrt werden sollen.
3. Drücken Sie **Speichern**.

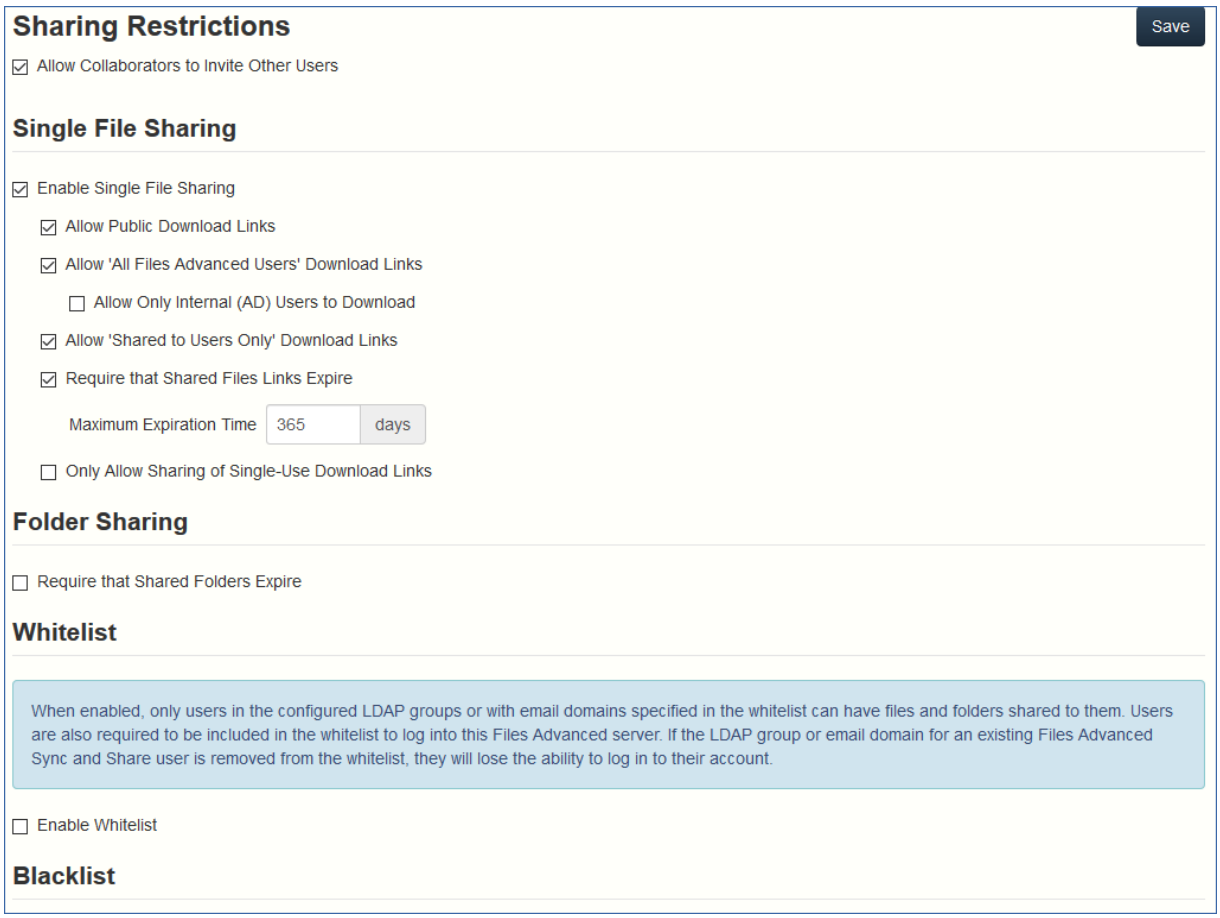
Hinweis: *Alle bereits vorhandenen Dateien dieses Typs werden nicht mehr synchronisiert und können nicht verschoben werden. Sie können sie nur manuell herunterladen oder entfernen.*

So legen Sie einen Grenzwert für eine maximale Dateigröße fest:

1. Erweitern Sie in der Webkonsole die Registerkarte **Sync & Share**, und öffnen Sie **Allgemeine Beschränkungen**.
2. Aktivieren Sie das Kontrollkästchen **Maximal erlaubte Dateigröße**, und geben Sie die gewünschte maximale Dateigröße in das Textfeld ein (in MB).
3. Drücken Sie **Speichern**.

Hinweis: *Alle bereits vorhandenen Dateien mit einer größeren Dateigröße werden nicht mehr synchronisiert und können nicht verschoben werden. Sie können sie nur manuell herunterladen oder entfernen.*

7.2 Freigabebeschränkungen



Teilnehmern erlauben, andere Benutzer einzuladen – 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

Freigabe einzelner Dateien aktivieren – Wenn diese Option aktiviert ist, können einzelne Datei-Links freigegeben werden, und Sie können festlegen, wie viele Benutzer darauf zugreifen und wie lange der Zugriff darauf möglich ist.

- **Öffentliche Download-Links erlauben** – Wenn diese Option aktiviert ist, kann jeder, der über den entsprechenden Link verfügt, auf die freigegebene Datei zugreifen.
- **Download-Links für 'Alle Files Advanced-Benutzer' unterstützen** – Wenn diese Option aktiviert ist, können nur Benutzer mit Anmeldedaten für Files Advanced auf die freigegebene Datei zugreifen.
  - **Download nur internen (AD-)Benutzern erlauben**– Wenn diese Option aktiviert ist, können nur Benutzer mit Achtive Directory-Anmeldedaten für Files Advanced auf die freigegebene Datei zugreifen.
- **Download-Links nur für bestimmte Benutzer unterstützen** – Wenn diese Option aktiviert ist, können Links verwendet werden, die nur für die Benutzer nutzbar sind, für die sie freigegeben wurden.
- **Verlangen, dass Dateifreigabelinks verfallen** – Ist diese Option aktiviert, müssen Dateilinks ein Ablaufdatum haben.
  - **Maximale Ablaufzeit** – Mit dieser Option wird die maximale Zeit (in Tagen) festgelegt, die Benutzer für den Ablauf von Dateien angeben können.
- **Freigaben nur mit Einmal-Download-Links erlauben** – Bei Aktivierung können Benutzer nur Links zur einmaligen Verwendung senden. Diese Links werden nach dem ersten Download gesperrt.

Ordnerfreigabe

Verlangen, dass Ordnerfreigaben verfallen – Ist diese Option aktiviert, müssen alle Ordnerfreigaben ein Ablaufdatum haben.

- **Maximale Ablaufzeit** – Diese Option steuert die maximale Zeit (in Tagen) bis zum Ablaufdatum des Ordners.

Whitelist

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

Blacklist

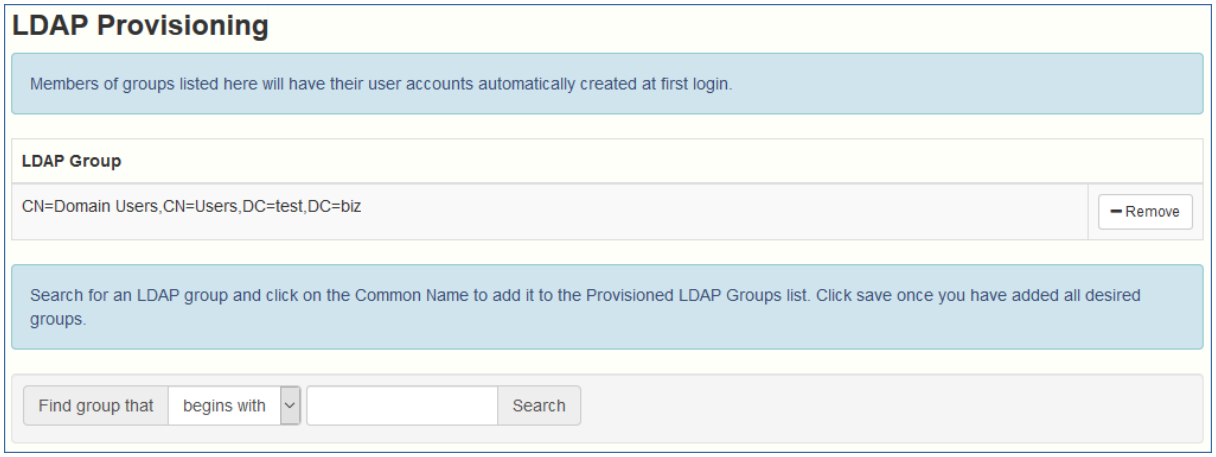
Benutzer in den LDAP-Gruppen oder mit den in der Blacklist spezifizierten E-Mail-Domains (z. B. beispiel.com) können sich nicht beim System anmelden, selbst wenn sie auf der Whitelist stehen. Für

Domains können Platzhalterzeichen verwendet werden (z.B. *.firma.com). LDAP-Gruppen müssen über ihre definierten Namen (Distinguished Names) spezifiziert werden, beispielsweise CN=meinegruppe,CN=Benutzer,DC=meinefirma,DC=com.

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

7.3 LDAP-Bereitstellung

Für Mitglieder der hier aufgelisteten Gruppen werden die Benutzerkonten automatisch bei der ersten Anmeldung erstellt. Dies erleichtert die Kontoerstellung, sodass der Administrator nicht jedem Benutzer eine Einladung senden muss.



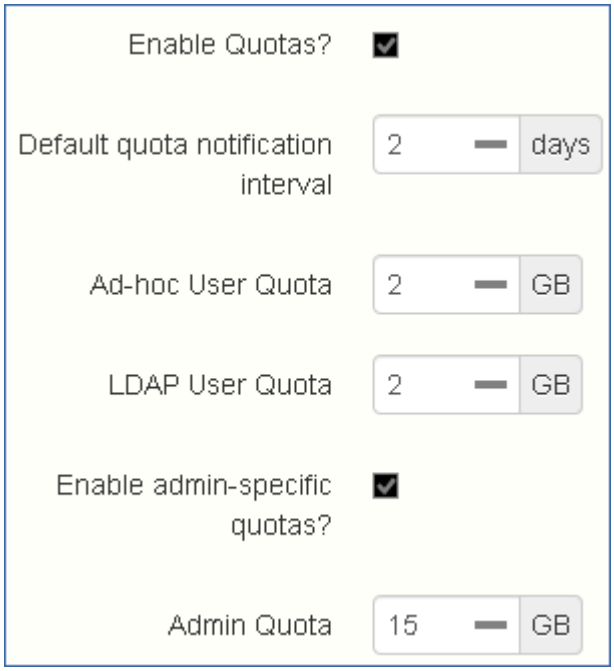
LDAP-Gruppe

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.

7.4 Quotas

Administratoren können die Menge an Speicherplatz festlegen, die 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 verschiedene Quota-Werte basierend auf einzelnen Benutzern oder der Active Directory-Gruppenmitgliedschaft zuweisen.



- **Quotas aktivieren?** – Wenn diese Option aktiviert ist, wird der maximale Speicherplatz, der einem Benutzer zur Verfügung steht, durch eine Quota beschränkt.
  - **Standard-Benachrichtigungsintervall** – Zeitintervall in Tagen, mit dem festgelegt wird, wie oft Benutzer, die sich ihrer Quota-Begrenzung nähern, Benachrichtigungs-E-Mails erhalten.
  - **Ad-hoc-Benutzer-Quota** – Legt die Quota für Ad-hoc-Benutzer fest.
  - **Quota für LDAP-Benutzer** – Legt die Quota für LDAP-Benutzer fest.
  - **Admin-spezifische Quotas aktivieren?**– Wenn diese Option aktiviert ist, wird Administratoren eine separate Quota zugewiesen.
    - **Admin-Quota** – Legt die Quota für Administratoren fest.

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

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

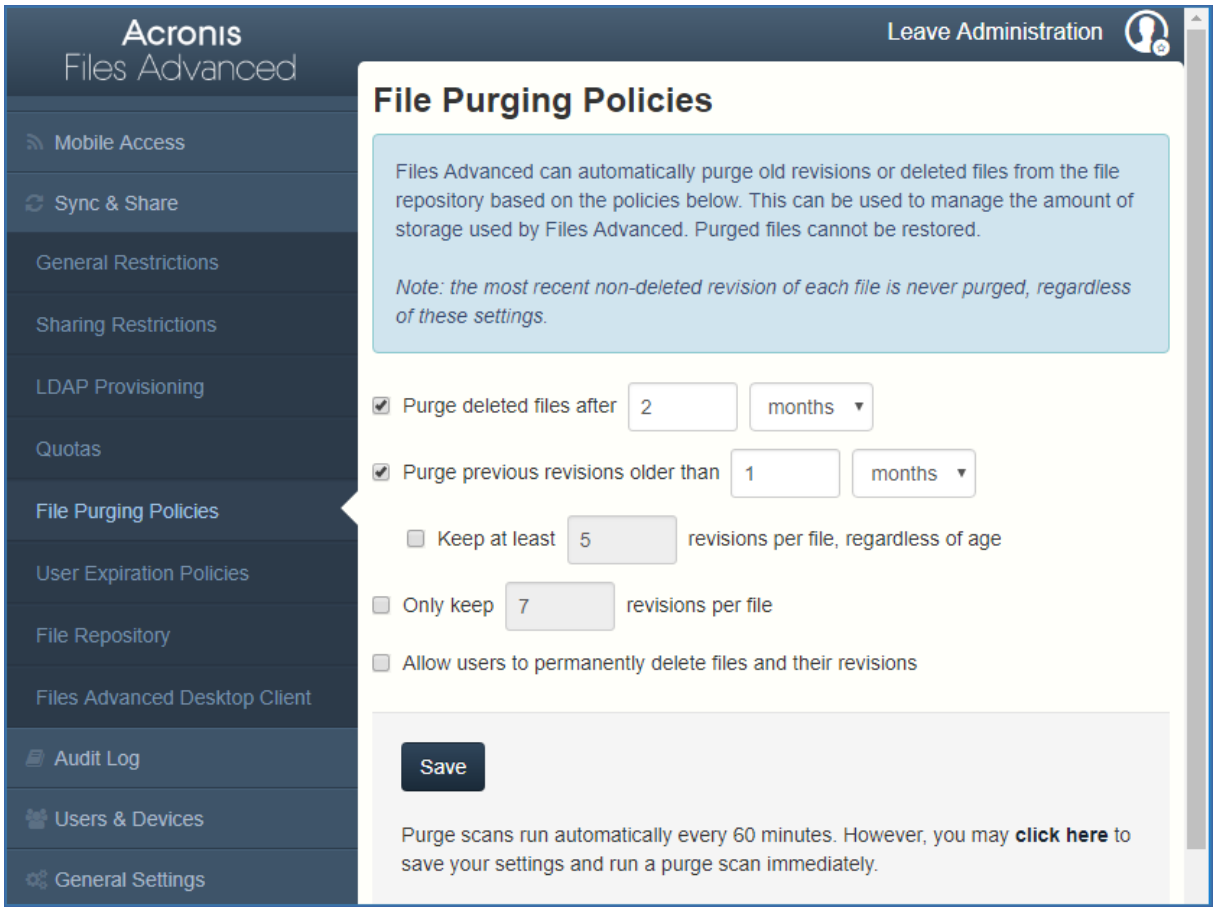
Hinweis: *Quotas können in Megabite festgelegt werden, indem eine Größe von weniger als 1 GB spezifiziert wird.* ***z. B. 0,5, 0,3, 0,9*** *usw.*

7.5 Dateibereinigungsrichtlinien

In Files Advanced werden Dokumente, Dateien und Ordner normalerweise im System aufbewahrt, bis sie ausdrücklich entfernt werden. So können Benutzer gelöschte Dateien wiederherstellen und vorherige Versionen eines Dokuments verwahren. Files Advanced ermöglicht es Administratoren,

Richtlinien zu definieren, um festzulegen, wie lange gelöschte Dateien verwahrt werden, die maximale Anzahl und wann ältere Versionen gelöscht werden sollen.

Files Advanced kann, auf Basis der unten angegebenen Richtlinien, alte Versionen oder gelöschte Dateien aus dem Datei-Repository durch automatisches Entfernen bereinigen. Dies kann genutzt werden, um die von Files Advanced belegte Speichermenge zu verwalten. Endgültig gelöschte Dateien können nicht wiederhergestellt werden.



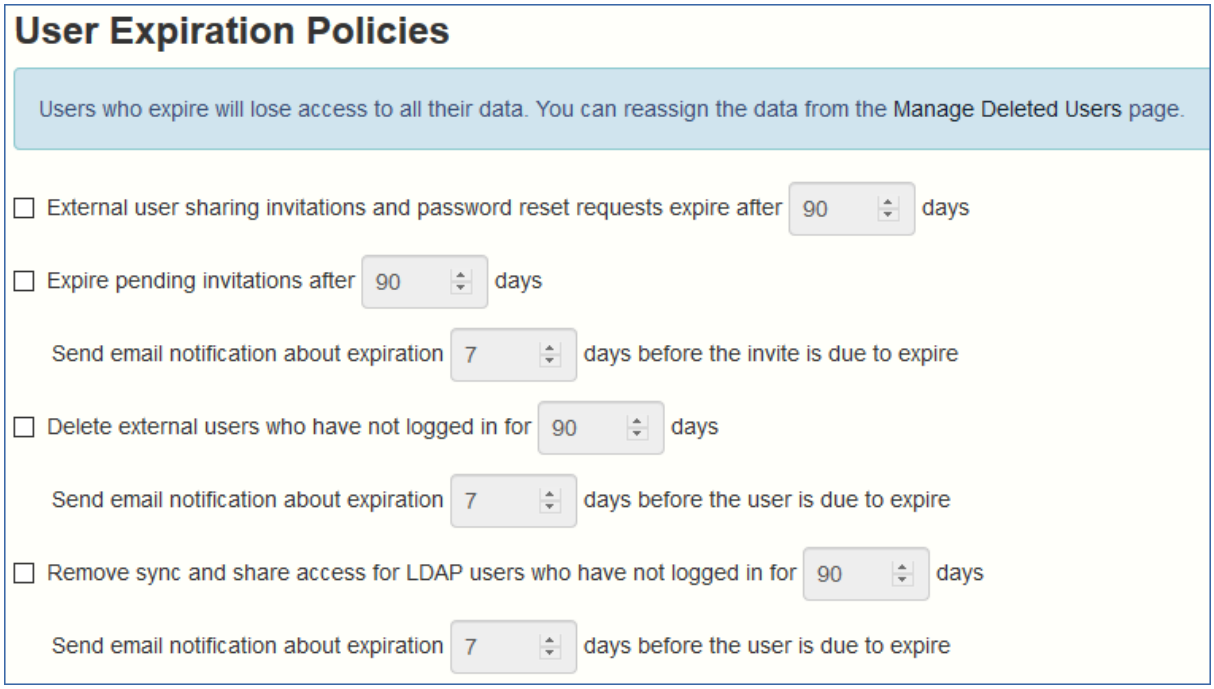
Hinweis: *Die neueste, ungelöschte Version einer Datei wird, unabhängig von diesen Einstellungen, niemals entfernt.*

- **Gelöschte Dateien entfernen nach** – Bei Aktivierung werden Dateien gelöscht, die älter sind als der festgelegte Wert.
- **Frühere Versionen entfernen, die älter sind als** – Bei Aktivierung werden Dateiversionen gelöscht, die älter sind als der festgelegte Wert.
  - **Behalte mindestens X Versionen pro Datei, ungeachtet ihres Alters** – Bei Aktivierung wird eine Mindestanzahl der Versionen behalten, unabhängig vom Alter.
- **Behalte nur X Versionen pro Datei** – Bei Aktivierung wird die maximale 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.*

7.6 Benutzerablaufrichtlinien

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



- **Externe Benutzer, die Einladungen und Aufforderungen zur Kennwortzurücksetzung teilen, verfallen nach X Tagen** – Wenn diese Option aktiviert ist, verfallen Einladungen und Anforderungen zum Zurücksetzen von Kennwörtern für externe Benutzer nach einer bestimmten Zahl von Tagen.
- **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.
- **Externe Benutzer löschen, die sich seit X Tagen nicht angemeldet haben** – Wenn diese Option aktiviert ist, werden externe 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.

7.7 Datei-Repository

Diese Einstellungen bestimmen, wo für Sync & Share hochgeladene Dateien gespeichert werden. In der Standardkonfiguration ist das Dateisystem-Repository auf demselben Server wie der Files Advanced Server installiert. Im Datei-Repository werden Files Advanced Sync & Share-Dateien und frühere Versionen gespeichert. Mit dem Files Advanced-Konfigurationswerkzeug (S. 28) 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. Führen Sie die Datei 'AcronisAccessConfiguration.exe' aus, die sich in der Regel im Verzeichnis **`C:\Program Files (x86)\Acronis\Files Advanced\Common\Configuration Utility`** befindet, um diese Einstellungen anzuzeigen oder zu ändern.

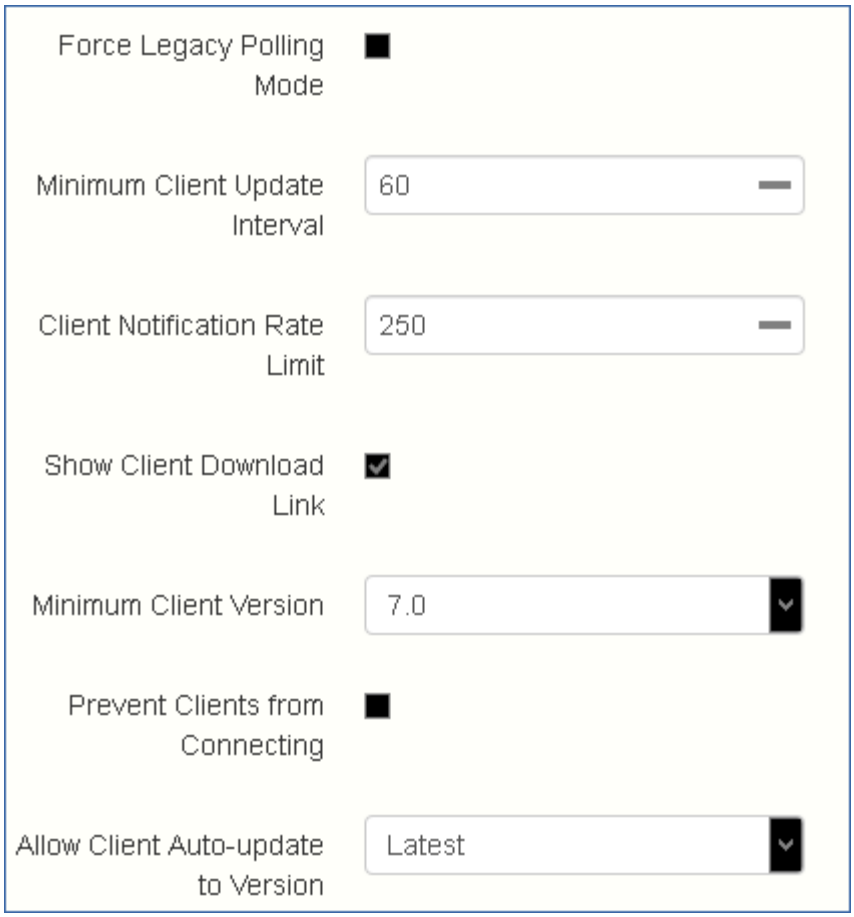
- **Dateispeichertyp** – wählen Sie den Speicherort aus, der für das Repository des virtuellen Dateisystems verwendet werden soll. Die Optionen lauten 'Dateisystem', 'Acronis Storage', 'Microsoft Azure Storage', 'Amazon S3', 'Swift S3', 'Ceph S3' und 'Anderer S3-kompatibler Storage'.

  Hinweis: *Bei nicht in der Liste aufgeführten Anbietern von S3-Storage können Sie die Option* ***Anderer S3-kompatibler Storage*** *verwenden. In diesem Fall kann allerdings keine Garantie dafür übernommen werden, dass alle Optionen ordnungsgemäß funktionieren.*

- **Dateispeicher-Repository-Endpunkt** – legen Sie die URL für den Dateisystem-Repository-Endpunkt fest.
- **Verschlüsselungsgrad** – geben Sie den Verschlüsselungstyp an, der zur Verschlüsselung von Dateien im Repository des virtuellen Dateisystems verwendet werden soll. Die Optionen lauten 'Keine', 'AES-128' und 'AES-256'. Die Standardeinstellung ist 'AES-256'.
- **Grenzwert für Warnung bei niedrigem Speicherplatz des Dateispeichers** – Unterschreitet der freie Speicherplatz diesen Schwellenwert, erhält der Administrator eine entsprechende Warnung.

7.8 Files Advanced-Client

Diese Einstellungen gelten für den 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.

  Hinweis: *Seit Files Advanced Server-Version 7.5 können nur Desktop Clients angeschlossen werden, die neuer als Version 6.1 sind.*

- **Clients an der Verbindung hindern** – Wenn diese Option aktiviert ist, sind Desktop Clients nicht in der Lage, sich mit dem Server zu verbinden. Dies sollte normalerweise nur zu administrativen Zwecken aktiviert werden. Es verhindert keine Verbindungen zur Weboberfläche.

- **Erlaube Client-Auto-Update auf Version** – Legt die Desktop Client-Version fest, die auf allen Desktop Clients über Auto-Update-Prüfungen bereitgestellt wird. Wählen Sie **Keine Updates erlauben**, um ein Auto-Update der Clients komplett zu verhindern.

8 Benutzer und Geräte

Themen

8.1 Mobile Geräte verwalten

Wenn ein Files Advanced Mobile beim Files Advanced Server registriert wurde, wird das zugehörige mobile Gerät in der Liste **Geräte** angezeigt. Die Liste enthält detaillierte Statusinformationen zu jedem Gerät, das mit einer PIN-Nummer aktiviert wurde.

Hier können Sie alle verwalteten Geräte und die zugehörigen Informationen anzeigen. Sie können außerdem Löschungen für Geräte durchführen oder das App-Kennwort ändern.

- **Anzeigename** – der vollständige Name des Benutzers im Active Directory (AD)
- **Benutzername** – der Konto-Benutzername des Benutzers im AD
- **Domain** – die Domäne, in der das AD-Konto des Benutzers Mitglied ist
- **Gerätename** – der vom Benutzer festgelegte Gerätename
- **Modell** – das Modell/der Typ des Geräts
- **Betriebssystem** – Betriebssystemversion des Geräts.
- **Version** – Version der Files Advanced Mobile-App auf dem Gerät.
- **Status** – Status der Files Advanced 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 Files Advanced Mobile-Applikation auf dem Gerät remote zurücksetzen. Hier geben Sie den Code ein, den Sie von der Files Advanced 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 Files Advanced 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 Files Advanced Client Management Server auszugehen ist. Wenn Sie 'Mobilen Clients, die auf neuen Geräten wiederhergestellt wurden, eine automatische Registrierung ohne PIN erlauben' aktiviert haben, wird ein aus der Liste entferntes Gerät automatisch erneut angezeigt und verwaltet, sobald es den Server kontaktiert.

Themen

8.1.1 Kennwort-Resets für die Remote-Applikation durchführen

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

Falls ein Kennwort verloren geht, sind die einzigen verfügbaren Optionen ein Zurücksetzen des Kennworts für die Remote-Applikation oder die Deinstallation von Files Advanced und erneute Installation durch den Benutzer auf dessen Gerät. Durch die Deinstallation werden vorhandene Daten und Einstellungen gelöscht, sodass die Sicherheit gewahrt bleibt. Die Benutzer haben jedoch wahrscheinlich erst dann wieder Zugriff auf Files Advanced-Server, wenn sie eine neue Verwaltungseinladung erhalten.

Kennwort für die Applikation zurücksetzen

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

So setzen Sie ein Kennwort für die Applikation Files Advanced für iOS oder Android zurück:

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

8.1.2 Remote-Löschungen durchführen

Mit Files Advanced kann eine Remote-Löschung einer Mobile-Applikation durchgeführt werden. Bei dieser selektiven Remote-Löschung werden alle in der Files Advanced-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. Klicken Sie auf 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. Der Status **Remote ausstehend** wird in der Spalte **Status** für das Gerät 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 Menü* ***Aktionen*** *angezeigt, nachdem ein Remote-Löschvorgang aufgerufen wurde.*

Anforderungen bezüglich der Verbindung

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

8.2 Benutzer verwalten

Über diesen Bereich können Sie alle Sync & Share-Benutzer verwalten. Sie können über die Schaltfläche **Benutzer hinzufügen** neue Benutzer einladen oder über die Schaltfläche 'Aktionen' 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. Dies gilt jedoch nur dann, wenn der Benutzer über einen Sync & Share-Zugang verfügt.

Sync & Share-Benutzer werden in 3 Typen unterteilt:

- **Freie externe** Benutzer können mit verschiedenen Methoden erstellt werden – über eine E-Mail-Einladung oder eine Einladung zu einem freigegebenen Ordner. Benutzern wird eine Bestätigungs-E-Mail zugesendet. Sie müssen dann über diese E-Mail ihr Konto aktivieren. 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. Nicht lizenzierte Benutzer können andere Mitglieder nicht **einladen** oder **anzeigen**, selbst wenn diese ihnen die Rechte gegeben haben. Benutzer müssen lizenziert sein, um diese Funktionen nutzen zu können.

- 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. 112) 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 Files Advanced Server einzurichten. Weitere Informationen finden Sie im Artikel Administratoren und Berechtigungen (S. 126).
- **Kein Zugriff**-Benutzer sind administrative Benutzer, die keinen Zugriff auf den Sync & Share-Web-Client haben und die nicht standardmäßig lizenziert werden. Diese können die Funktionen der mobilen App und von Mobile Access wie reguläre Benutzer verwenden. Die Benutzer werden entweder unter LDAP oder unter Ad-Hoc geführt.

- **Name** – Zeigt den Namen an, mit dem sich der Benutzer beim Server anmeldet.
- **E-Mail** – Zeigt die E-Mail-Adresse des Benutzers an.
- **Sync & Share**
  - **Status** – Zeigt den von dem Benutzer verwendeten Lizenztyp an.
  - **Verwendung** – Zeigt 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 verwendet
  - **Benutzer bearbeiten** – Erlaubt das Bearbeiten dieses Benutzers.
  - **Löschen** – Der Benutzer wird gelöscht.

Hinzufügen eines Ad-hoc-Benutzers

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

9. Klicken Sie auf die Schaltfläche **Hinzufügen**.

Der Benutzer erhält eine E-Mail mit Link. Sobald er den Link öffnet, wird er gebeten, ein Kennwort festzulegen. Der Benutzer erhält eine E-Mail zur Bestätigung des Kontos. Sobald er den Link in der E-Mail öffnet, ist die Kontoregistrierung abgeschlossen.

Hinzufügen eines LDAP-Benutzers

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

Der Benutzer kann sich jetzt mit seinen LDAP-Anmeldedaten anmelden. Seine Kontoerstellung ist abgeschlossen, sobald er sich anmeldet.

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

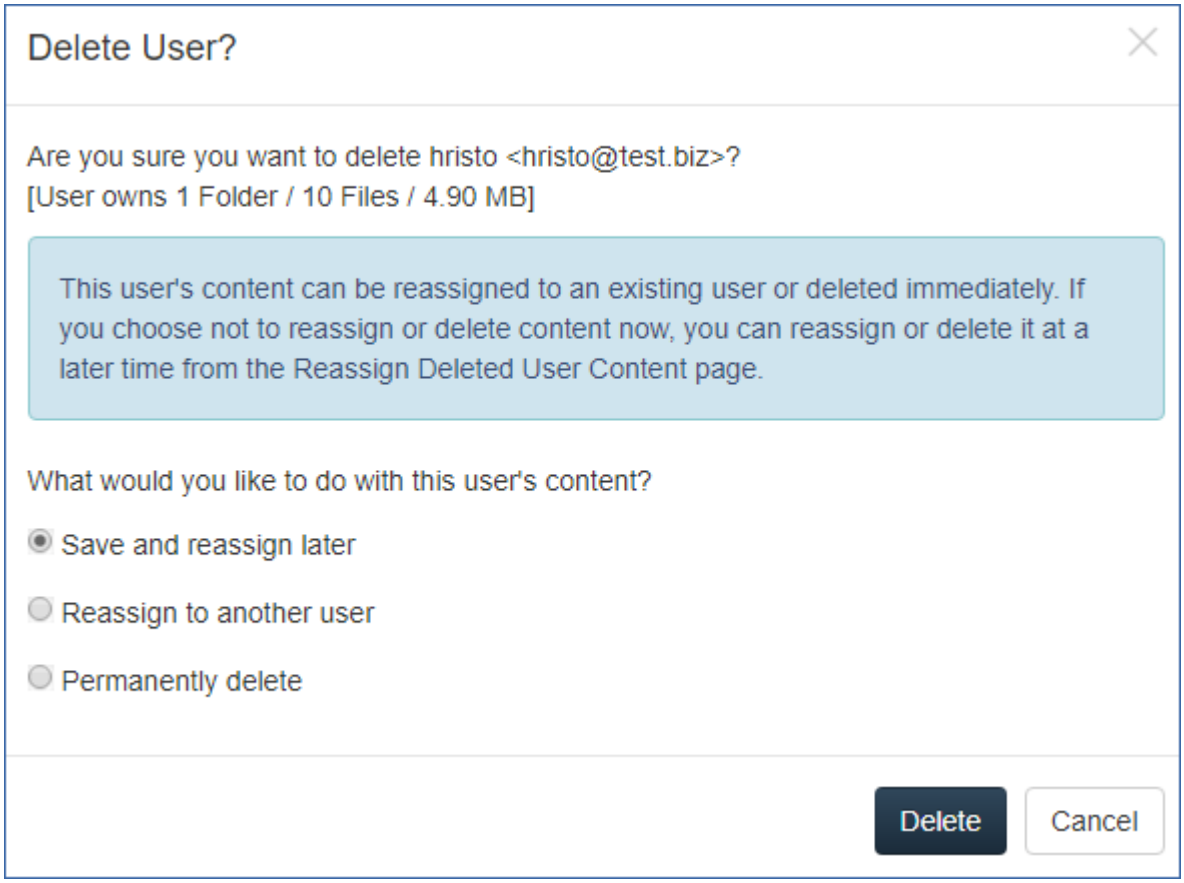
Eine benutzerdefinierte Quota festlegen

Sie können für jeden Benutzer mit Sync & Share-Zugang eine benutzerdefinierte Quota festlegen. Gehen Sie hierfür folgendermaßen vor:

1. Öffnen Sie über die Weboberfläche die Registerkarte **Benutzer & Geräte**.
2. Suchen Sie den gewünschten Benutzer, und klicken Sie auf die Schaltfläche **Aktionen**.
3. Wählen Sie **Benutzer bearbeiten**, und aktivieren Sie **Benutzerdefinierte Quota verwenden?**.
4. Geben Sie die gewünschte Größe für die Quota ein, und klicken Sie auf **Speichern**.

8.3 Gelöschte Benutzerinhalte neu zuweisen

Gelöschte Benutzer ohne Inhalte werden vollständig entfernt. Beim Löschen eines Benutzers mit Inhalt werden Sie gefragt, was Sie mit dem Inhalt des Benutzers tun möchten.



- **Speichern und später neu zuweisen** – Die Benutzerinhalte werden gespeichert, damit sie später neu zugewiesen oder gelöscht werden können. Administratoren können später die Liste der gelöschten Benutzer mit Inhalten aufrufen, die auf eine Neuzuweisung oder das Löschen von der Seite **Gelöschte Benutzerinhalte neu zuweisen** warten.

  Hinweis: *Bereinigungsrichtlinien gelten weiterhin für diese Inhalte wie auch für aktive Benutzer.*

- **Einem anderen Benutzer neu zuweisen** – Wählen Sie sofort einen anderen Benutzer, und weisen Sie ihm die Inhalte neu zu. Dieser Benutzer verfügt dann über einen Sync & Share-Ordner mit der Bezeichnung **Inhalte von DeletedUserName <deletedusersemail> übernommen**, und er ist auch Eigentümer aller übernommenen Inhalte. Dies beinhaltet vom gelöschten Benutzer freigegebene Ordner.
- **Endgültig löschen** – Löschen Sie das Konto und die Inhalte.

9 Client-Anleitungen

Informationen zur Verwendung von Files Advanced Clients finden Sie in der jeweiligen Dokumentation zum Client für Ihre App aus der untenstehenden Liste:

- Desktop- und Web-Clients
- iOS-App
- Android-App

- Windows Mobile-App

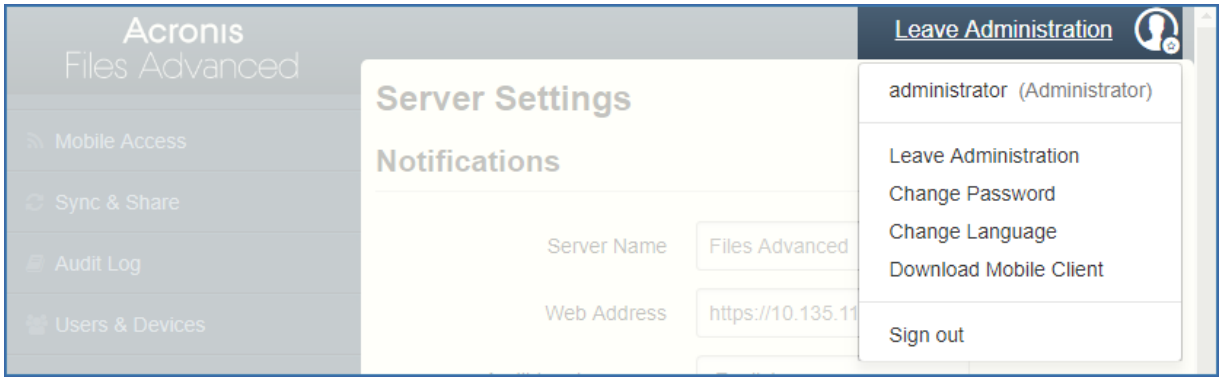
10 Server-Administration

Themen

10.1 Server verwalten

Wenn Sie sich als Administrator an der Weboberfläche anmelden, können Sie zwischen den Modi **Administration** und **Benutzer** wechseln.

- Um den Modus **Administration** anzugeben, klicken Sie auf das Benutzersymbol und drücken **Verwaltungskonsole**.
- Um den Modus **Benutzer** auszuwählen, drücken Sie oben rechts die Schaltfläche **Administration verlassen**.



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

10.2 Administratoren und Berechtigungen

Zugriffsbeschränkungen für die Verwaltungsseite

- **Nur Verbindungen, die von konfigurierten IP-Adressbereichen erfolgen, dürfen auf die Administrationsseiten zugreifen** – Hiermit kann der Administrator festlegen, dass nur von bestimmten IP-Adressen auf die Administrations-Weboberfläche zugegriffen werden darf.

- **IP-Adressen, die auf die Administrationsseiten zugreifen dürfen** – Der Administrator gibt die IP-Adressen ein, von denen auf die Seite **Administration** zugegriffen werden kann. Dies können durch Kommata getrennte IPs, Teilnetze oder IP-Bereiche sein.

z.B.: 10.1.2.3, 10.4.*, 10.10.1.1-10.10.1.99

Hinweis: *Der Administrator-Zugriff von 'localhost' kann nicht beschränkt werden.*

Hinweis: *Diese Funktion gilt* ***nicht*** *für Server, die den Gateway Server als Proxy für Anforderungen des Files Advanced Servers verwenden.*

Bereitgestellte LDAP-Administrator-Gruppen

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

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

So fügen Sie eine bereitgestellte LDAP-Administratorgruppe hinzu:

1. Klicken Sie auf die Schaltfläche **Bereitgestellte Gruppe hinzufügen**.
2. Markieren Sie, ob die Gruppe über die Funktion 'Sync & Share' verfügen soll.
3. Markieren Sie alle administrativen Rechte, die die Gruppenbenutzer erhalten sollen.
4. Suchen Sie die Gruppe.
5. Klicken Sie auf den Gruppennamen.
6. Drücken Sie **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 Files Advanced-Weboberfläche auf.
2. Melden Sie sich mit einem Administratorkonto an.
3. Erweitern Sie die Registerkarte **Allgemeine Einstellungen**, und öffnen Sie die Seite **Administratoren**.
4. Klicken Sie auf die Schaltfläche **Administrator hinzufügen** unter **Administrative Benutzer**.

5. Wählen Sie entweder die Registerkarte 'Active Directory/LDAP' oder 'Per E-Mail einladen' aus, je nachdem, welchen Typ von Benutzer Sie einladen und was von diesem Benutzer verwaltet werden soll. LDAP-Benutzern ohne E-Mail-Adresse können die Sync & Share-Funktionen nicht zugewiesen werden.

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

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

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

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

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

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

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

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

Administratorrechte

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

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

So geben Sie Benutzern administrative Rechte:

1. Öffnen Sie die Registerkarte **Sync & Share**.
2. Öffnen Sie die Registerkarte **Benutzer**.
3. Klicken Sie dann für den Benutzer, den Sie bearbeiten möchten, auf die Schaltfläche **Aktionen**.

4. Klicken Sie auf **Bearbeiten**.
5. Markieren Sie alle administrativen Rechte, die der Benutzer erhalten soll.
6. Drücken Sie **Speichern**.

So geben Sie Benutzern spezifische Rechte:

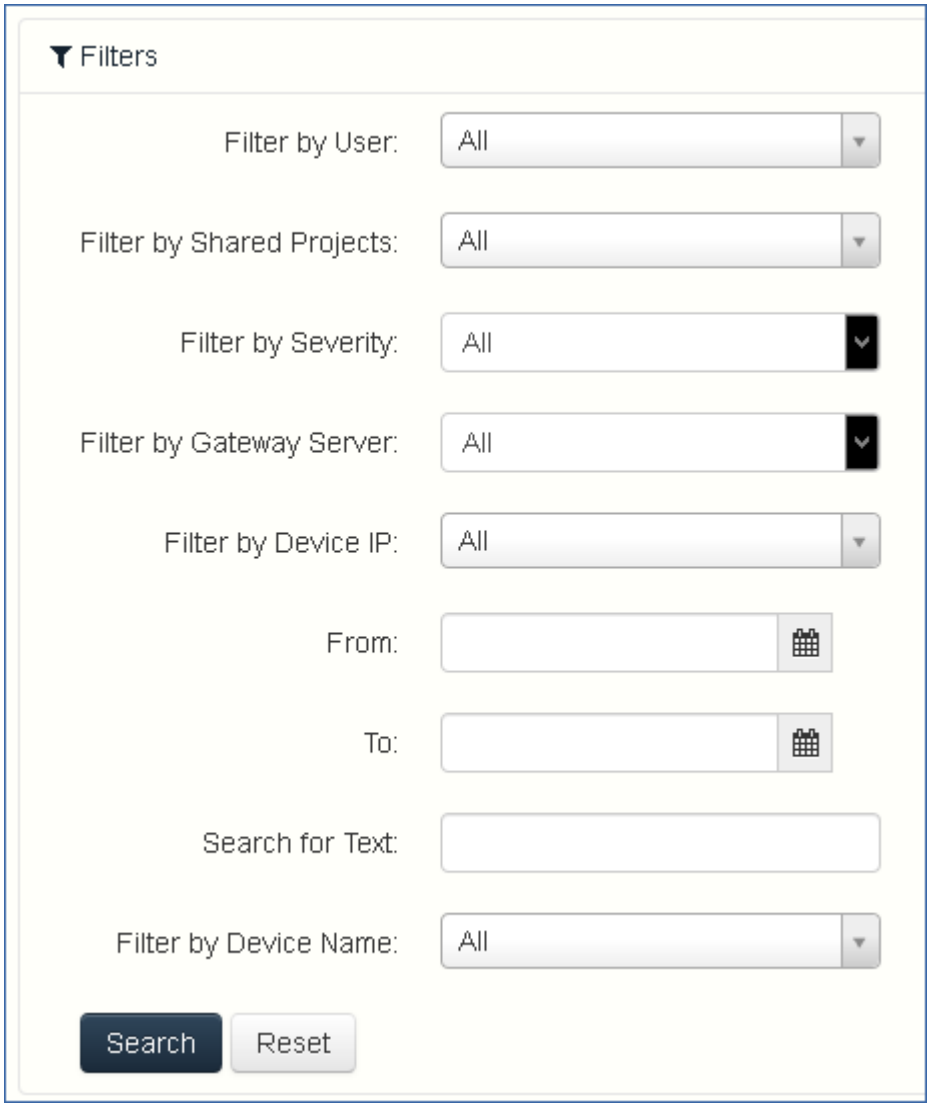
1. Klicken Sie dann für den Benutzer, den Sie bearbeiten möchten, auf die Schaltfläche **Aktionen**.
2. Klicken Sie auf **Bearbeiten**.
3. Markieren Sie alle administrativen Rechte, die der Benutzer erhalten soll.
4. Drücken Sie **Speichern**.

10.3 Überwachungsprotokoll

10.3.1 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.

Hinweis: *Wenn Sie die Protokollierung und die Protokollierungsebene für einen Gateway Server konfigurieren möchten, navigieren Sie zu Gateway Server-Protokollierung (S. 92).*



- **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.

Timestamp	Type	User	Message	Device Name
2017-05-31 08:09:59	Error		Error sending email ['Enroll user for mobile access' to 'johndoe@t-soft-test.biz']: 550 5.1.1 <johndoewhatisreallifestopwriting@mailinator.com>: Recipient address rejected: Unknown user: johndoewhatisreallifestopwriting@mailinator.com	
2017-05-31 08:06:57	Info		Free space for file store http://127.0.0.1:5787 = 80.2 GB (86096715776.0 bytes)	

25 per page

Showing 1 to 2 of 2 entries

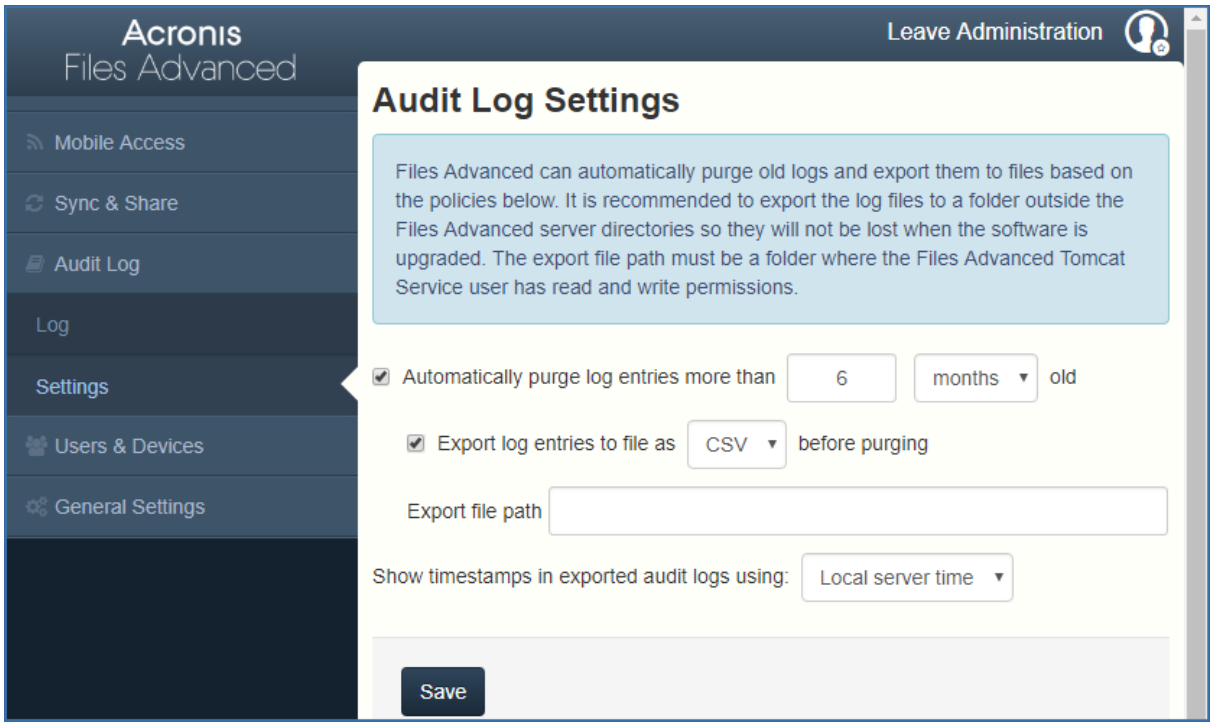
1

- **Zeitstempel** – Zeigt Datum und Uhrzeit des Ereignisses an.
- **Dateityp** – 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 den Zugriff auf mobile Datenquellen für Desktop- und Webclients gestattet haben, wird dies ebenfalls in das Protokoll aufgenommen.

- **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.

10.3.2 Einstellungen



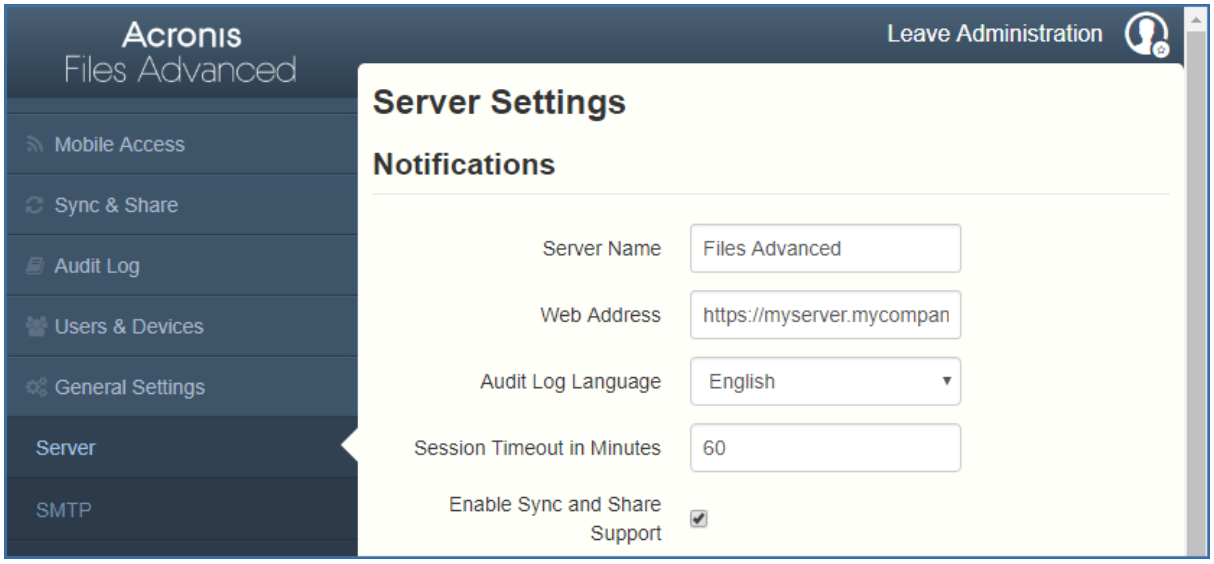
Files Advanced kann auf Basis bestimmter Richtlinien alte Protokolle bereinigen und diese als Dateien exportieren.

- **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. Der Export wird automatisch auf 03:00 Uhr lokale Serverzeit festgelegt. Diese Einstellung kann nicht geändert werden.
    - **Exportdateipfad** – Legt den Ordner fest, in dem exportierte Protokolle gespeichert werden.

Hinweis: *Wir empfehlen den Export der Protokolle in einen Ordner, der sich nicht im Installationsordner von Files Advanced befindet, damit sie im Fall einer Aktualisierung nicht verloren gehen. Der von Ihnen angegebene Ordner benötigt Lese-/Schreibzugriff für das Benutzerkonto, unter dem der Files Advanced-Tomcat-Dienst ausgeführt wird. Haben Sie die Standardwerte nicht geändert, ist dieses Konto das lokale Systemkonto.*

- **Anzeigen von Zeitstempeln in exportierten Überwachungsprotokollen in X** – Sie können wählen, ob die lokale Serverzeit oder ein anderes Zeitformat (UTC) für Überwachungsprotokolle verwendet werden soll.

10.4 Server

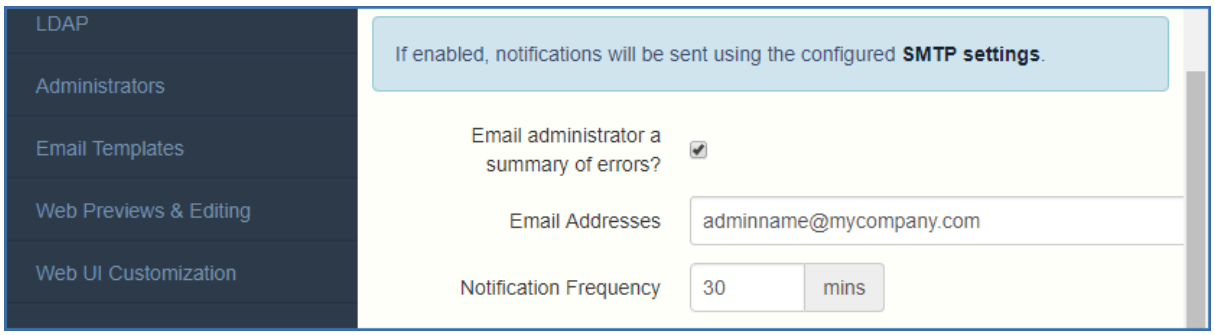


Server-Einstellungen

- **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.
- **Sprache für Überwachungsprotokoll** – Wählen Sie die Standardsprache für das Überwachungsprotokoll. Die aktuellen Optionen sind **Deutsch, Englisch, Französisch, Japanisch, Italienisch, Spanisch, Tschechisch, Russisch, Polnisch, Koreanisch, vereinfachtes und traditionelles Chinesisch**. Die Standardeinstellung ist **Englisch**.
- **Sitzungs-Zeitlimit in Minuten** – zur Festlegung der Dauer, bevor inaktive Benutzer abgemeldet werden. Falls für die ausgewählte Dauer keine Aktionen durchgeführt werden, wird dem Benutzer ein zeitlich festgelegter Dialog angezeigt, in dem er aufgefordert wird, eine Aktion durchzuführen oder sich abzumelden.

  Hinweis: *Falls der Benutzer einen Upload oder Download gestartet hat, der länger dauert als die Sitzungszeitüberschreitung, bleibt der Benutzer angemeldet, bis der Upload abgeschlossen ist.*

- **Sync & Share-Unterstützung aktivieren** – Mit diesem Kontrollkästchen werden die Sync & Share-Funktionen aktiviert/deaktiviert.



Benachrichtigungseinstellungen

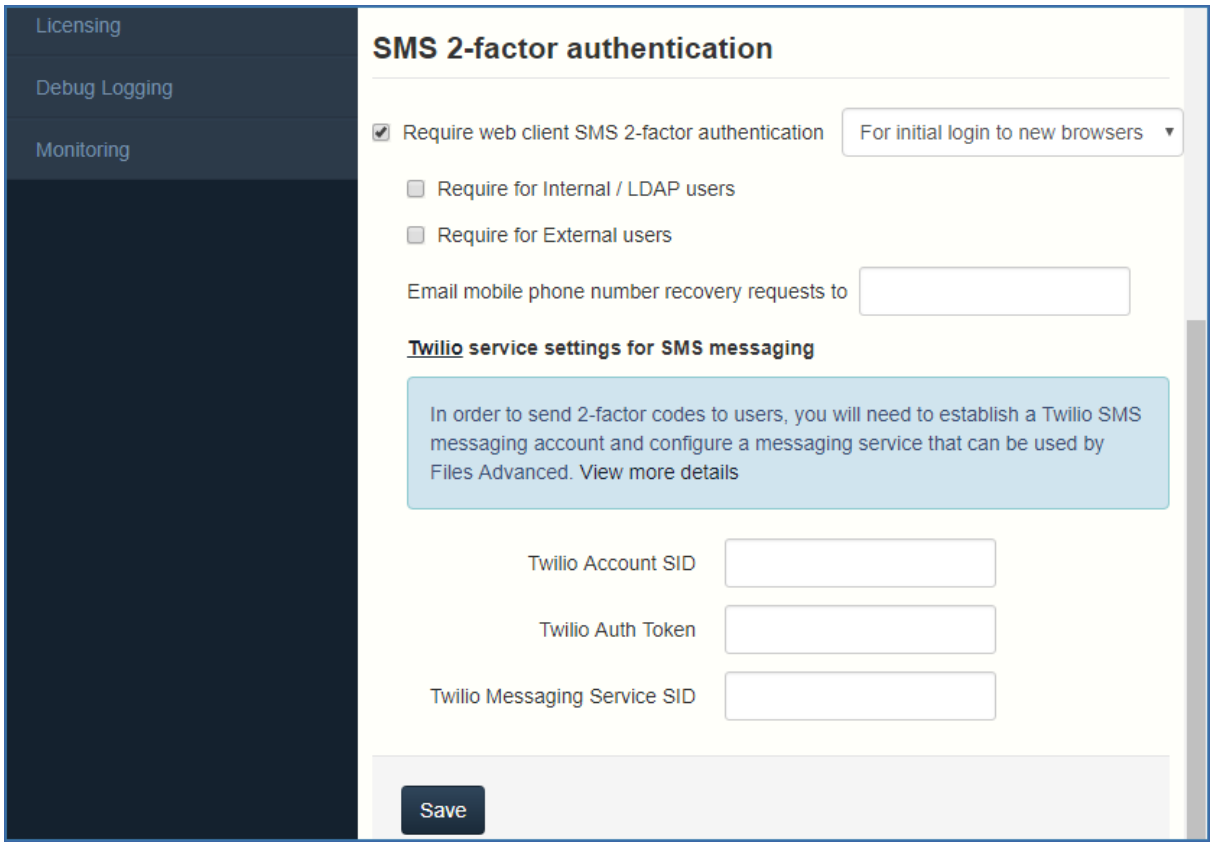
- **Dem Administrator eine Fehlerzusammenfassung per E-Mail senden?** – Wenn diese Option aktiviert ist, wird eine Fehlerzusammenfassung an die angegebenen E-Mail-Adressen gesendet.
  - **E-Mail-Adressen** – Eine oder mehrere E-Mail-Adressen, die eine Fehlerzusammenfassung erhalten.
  - **Benachrichtigungshäufigkeit**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

Themen

Es ist eine Option zur Zwei-Faktor-Authentifizierung per SMS für die Web-Client-Anmeldung enthalten. Sie können AD-Mobiltelefonnummern oder vom Benutzer angegebene Telefonnummern verwenden. Zwei-Faktor-Authentifizierung kann bei jeder Anmeldung, in bestimmten Zeitintervallen oder nur für die Anmeldung von neuen Browsern angefordert werden.

Für das Senden von SMS-Codes muss ein Konto mit dem Twilio SMS-Messagingdienst eingerichtet werden. Weitere Informationen finden Sie auf https://www.twilio.com/sms. Informationen zum Ausführen einer Testversion von Twilio finden Sie auf Twilio Free Trial.

Hinweis: *Sie benötigen nur ein Konto für Twilio, und dieses Konto wird vom Files Advanced Server genutzt, sodass Sie nicht für jeden Benutzer ein Konto benötigen.*



Zwei-Faktor-Authentifizierung per SMS für Webclient verlangen:

- **Für Erst-Anmeldung mit neuen Browsern** – verlangt beim erstmaligen Öffnen der Files Advanced-Server-Webseite Authentifizierung per SMS. Nachdem Sie den Verifizierungscode

eingegeben und Ihren Browser registriert haben, werden Sie aufgefordert, erneut einen SMS-Code einzugeben, bis Sie einen anderen Browser oder Computer verwenden.

  - **In einem bestimmten Intervall** – verlangt eine Authentifizierung per SMS in einem bestimmten Zeitintervall, ungeachtet der Anzahl der Anmeldeversuche.
  - **Bei jeder Anmeldung** – verlangt bei jedem Verbindungsversuch des Benutzers eine Authentifizierung per SMS.
- **Für interne / LDAP-Benutzer verlangen:**
  - **Files Advanced-Konto** – Wenn diese Option ausgewählt ist, werden die Telefonnummern der Benutzer von ihren Files Advanced-Konten abgerufen.
  - **Active Directory** – Wenn diese Option ausgewählt ist, werden die Telefonnummern der Benutzer von ihren Active Directory-Konten abgerufen.

__Hinweis:__ Es wird die Telefonnummer des __Mobiltelefons__ der Registerkarte __Telefone__ im Active Directory verwendet.

  - **Rückfall-Verhalten: –** Mit dieser Option wird die Standardaktion festgelegt, wenn Active Directory ausgewählt ist, der Benutzer jedoch keine Telefonnummer festgelegt hat.
    - **Files Advanced Konto verwenden** – Der Benutzer wird aufgefordert, eine Telefonnummer einzugeben.
    - **Anmeldung ohne Zwei-Faktor-Authentifizierung erlauben** – Erlaubt Anmeldungen ohne Zwei-Faktor-Authentifizierung.
    - **Keine Anmeldung erlauben** – Benutzer ohne Telefonnummern im Active Directory können sich nicht anmelden.
- **Für externe Benutzer verlangen** – Wenn diese Option aktiviert ist, wird von externen Benutzern ebenfalls die Authentifizierung per SMS verlangt.
- **E-Mail für Mobiltelefonnummer-Recovery-Anforderungen senden an** – Alle Mobiltelefonnummer-Recovery-Anforderungen werden an diese E-Mail-Adresse gesendet.

Twilio-Einstellungen:

- **Twilio-Konto-SID** – Die Sicherheitskennung Ihres Unternehmens für Ihr Twilio-Konto (SID).
- **Twilio-Authentifizierungs-Token** – Das Twilio-Authentifizierungs-Token Ihres Unternehmens.

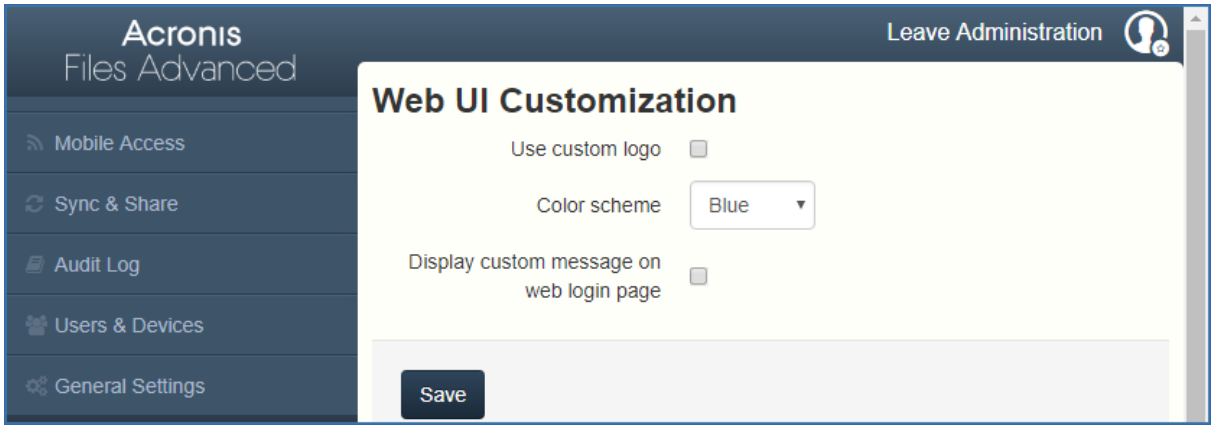
  Beides finden Sie in der Twilio-Konsole auf https://www.twilio.com/console.
- **Twilio-Messaging-Service-SID** – Die Sicherheitskennung Ihres Messaging-Dienstes mit Zwei-Faktor-Authentifizierung. Diese SID finden Sie auf https://www.twilio.com/console/sms/dashboard. Wenn Sie über mehrere Twilio-Messaging-Dienste verfügen, verwenden Sie nur die SID für den Service, den Sie auch für die Zwei-Faktor-Authentifizierung nutzen. Wenn Sie einen Twilio-Messaging-Dienst für einen **Anwendungsfall** erstellen, geben Sie gar nichts ein oder wählen Sie Zwei-Faktor-Authentifizierung.

__Hinweis:__ In der Twilio-Konsole müssen Sie die Länder auswählen, die den Messaging-Service verwenden dürfen. Aktivieren Sie für die gewünschten Länder einfach die entsprechenden Kontrollkästchen.

10.5 Web UI-Anpassung

Sie können die Logos und das Farbschema Ihres Files Advanced Servers problemlos anpassen.

Hinweis: Sie können diese Anpassungen auch über die Files Advanced-API vornehmen. Weitere Informationen erhalten Sie unter Web UI-API-Anpassung.



Benutzerdefinierte Logos verwenden

1. Rufen Sie die Weboberfläche von Files Advanced auf und melden Sie sich als Administrator an.
2. Navigieren Sie zu **Allgemeine Einstellungen** -> **Web UI-Anpassung**.
3. Aktivieren Sie das Kontrollkästchen **Benutzerdefiniertes Logo verwenden**.
4. Wählen Sie die Dateien für die zu ändernden Logos und stellen Sie sicher, dass sie im Dropdown-Menü ausgewählt sind.

   Hinweis: *Die Größenbeschränkung für die Bilder ist in Klammern* ***()*** *angegeben.*

5. Drücken Sie **Speichern**.

Benutzerdefinierte Begrüßung verwenden

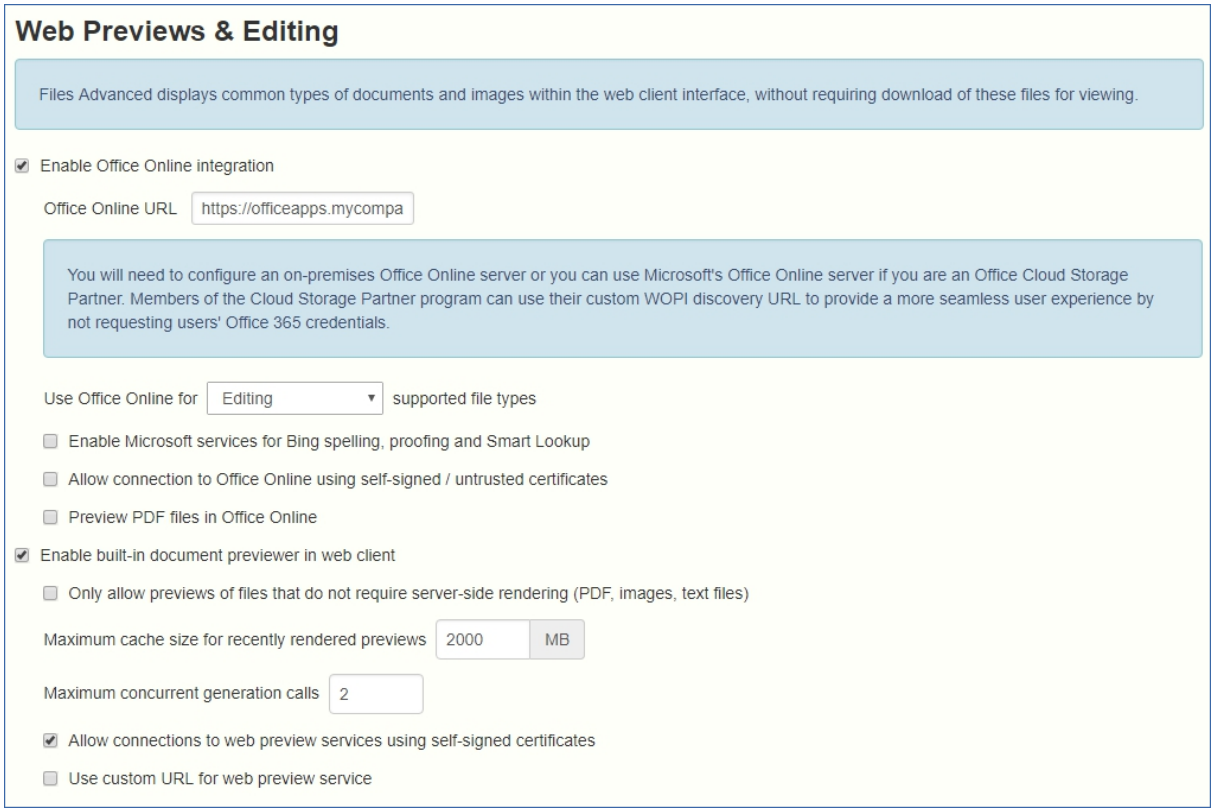
1. Rufen Sie die Weboberfläche von Files Advanced auf und melden Sie sich als Administrator an.
2. Navigieren Sie zu **Allgemeine Einstellungen** -> **Web UI-Anpassung**.
3. Aktivieren Sie das Kontrollkästchen **Benutzerdefinierte Nachricht auf der Webanmeldeseite anzeigen** .
4. Geben Sie die gewünschte Nachricht in das Textfeld ein, und klicken Sie auf **Speichern**.

Farbschemen verwenden

1. Rufen Sie die Weboberfläche von Files Advanced auf und melden Sie sich als Administrator an.
2. Navigieren Sie zu **Allgemeine Einstellungen** -> **Web UI-Anpassung**.
3. Klicken Sie auf das Dropdown-Menü **Farbschema** und wählen Sie ein Schema aus.
4. Drücken Sie **Speichern**.

10.6 Webvorschau und Bearbeitung

Files Advanced kann übliche Dokumente und Bilddateien in der Web Client-Oberfläche anzeigen, ohne diese Dateien herunterzuladen.



Office Online-Integration aktivieren – Aktiviert die integrierten Funktionen von Office Online.

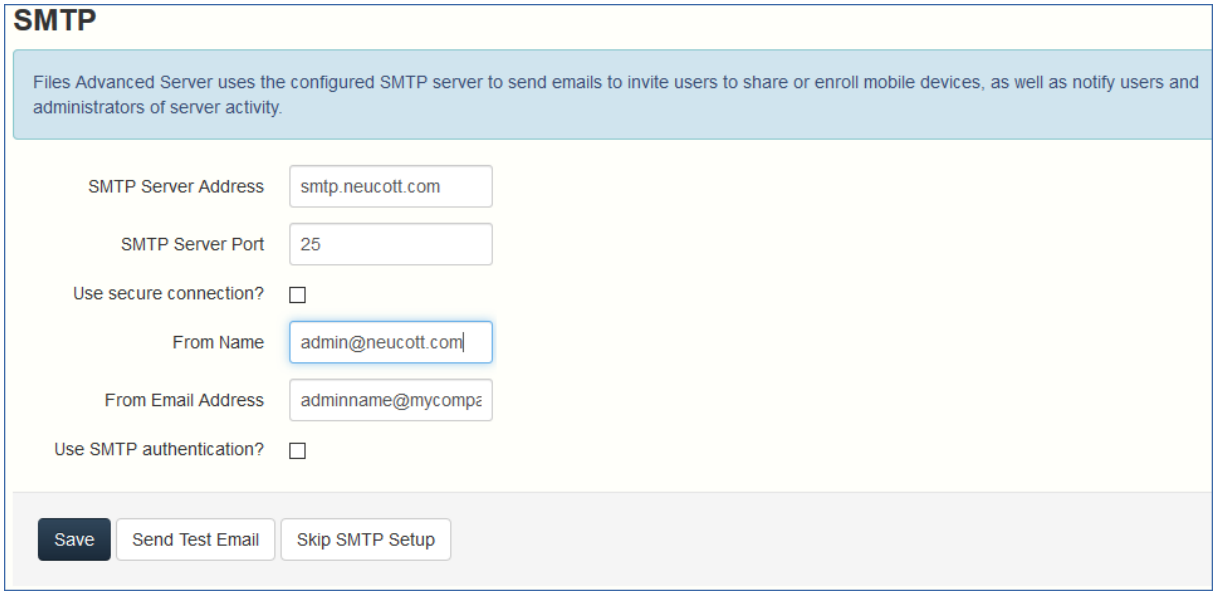
- **Office Online-URL** – Geben Sie Ihre WOPI-Such-URL von Office Online ein. Bei lokalen Files Advanced-Installationen müssen Sie ein lokales Office Online-Setup verwenden, um diese URL bereitstellen zu können. Der Microsoft Office Online-Clouddienst darf nur von Serviceanbietern verwendet werden und ist ohne spezielle Zertifizierung und ohne Whitelisting nicht öffentlich zugänglich.
- **Office Online verwenden für** – **Bearbeitung** ermöglicht Ihnen, die Dateien von Microsoft Office zu bearbeiten – **DOCX**, **PPTX**, **XSLX** – während **Anzeigen und Bearbeiten** das Bearbeiten dieser Dateien und auch eine Vorschau der **DOC-**, **XLS-** und **PPT**-Dateien ermöglicht. Wenn diese Einstellung deaktiviert ist, werden alle Office-Dateien und PDF-Dateien in der internen Files Advanced-Ansicht angezeigt.
- **Microsoft-Dienste für Bing-Rechtschreibung, Korrektur und intelligente Suche aktivieren** – Verwendet die Bing-Dienste von Microsoft für die Rechtschreibfunktionen.
- **Verbindungen zu Office Online mit selbstsignierten / nicht vertrauenswürdigen Zertifikaten erlauben** – Wird diese Option aktiviert, können Benutzer auf Office Online-Server zugreifen, die nicht vertrauenswürdige Zertifikate verwenden.
- **Vorschau von PDF-Dateien in Office Online** – Wird diese Option aktiviert, können Benutzer PDF-Dateien in Office Online anzeigen, sofern **Office Online verwenden für** auf **Anzeigen und Bearbeiten** festgelegt ist. In allen anderen Fällen werden PDF-Dateien in der internen Vorschau von Files Advanced angezeigt.

Integrierte Dokumentenvorschau im Webclient aktivieren – Aktiviert die Vorschau im Web.

- **Vorschau nur für solche Dateien erlauben, die kein serverseitiges Rendering erfordern (PDF, Bilder, Textdateien)** – Verringert die durch eine Webvorschau verursachte Last dadurch, dass eine Vorschau nur von Dateien, für die kein zusätzliches Rendering erforderlich ist, angezeigt wird. Hierbei handelt es sich um PDF-, Bild- und einfache Textdateien.
- **Maximale Cache-Größe für kürzlich gerenderte Dateivorschauen** – Legt die maximale Größe des Cache fest, der bei der Vorschau einer Datei gespeichert wird. Dies erhöht deutlich die Geschwindigkeit beim Öffnen von Dateien für die Vorschau, die kürzlich geöffnet wurden.
- **Maximale Anzahl gleichzeitiger Generierungsaufrufe** – Legt die maximale Anzahl der gleichzeitigen Aufrufe für die Vorschau fest.
- **Verbindungen zu Webvorschau-Diensten mit selbstsignierten Zertifikaten erlauben** – Ermöglicht den Kontakt zu Webvorschaudiensten, die selbstsignierte Zertifikate verwenden. Dies sind andere Tomcat-Dienste von Files Advanced.
- **Benutzerdefinierte URL für Webvorschau-Dienst verwenden** – Aktivieren Sie diese Option, wenn Sie über mehrere Files Advanced-Server verfügen und festlegen möchten, mit welchem Server die Webvorschau durchgeführt werden soll.

10.7 SMTP

Der Files Advanced Server versendet E-Mails über den konfigurierten SMTP-Server, um Benutzer zur Freigabe/Registrierung von Mobilgeräten einzuladen oder Benutzer/Administratoren über Server-Aktivitäten zu benachrichtigen.

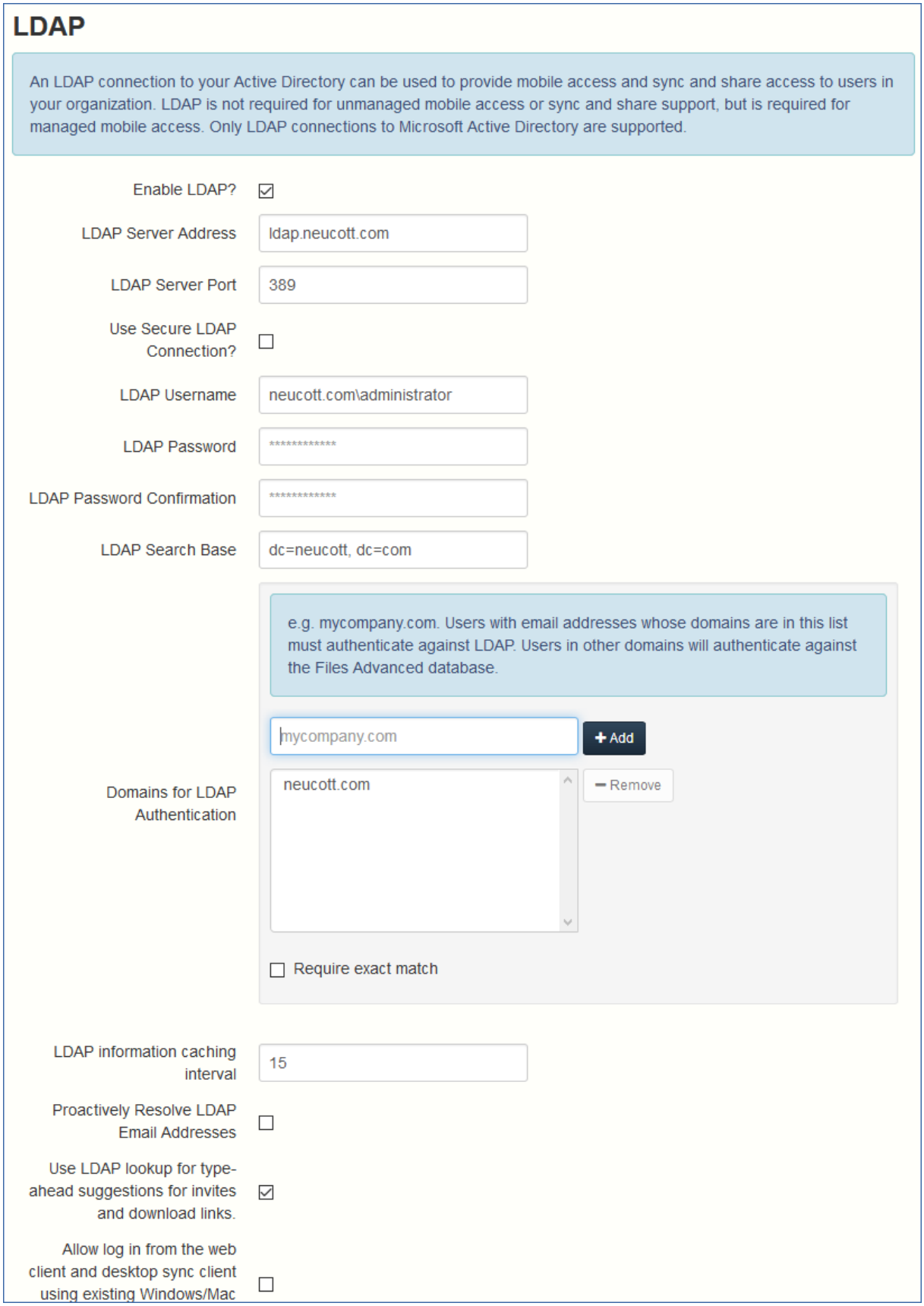


- **SMTP-Serveradresse** – Geben Sie den DNS-Namen des SMTP-Servers ein, über den E-Mail-Einladungen an Benutzer gesendet werden sollen.
- **SMTP-Serverport** – Geben Sie den SMTP-Serverport ein. Die Standardeinstellung ist Port 587.
- **Sichere Verbindung verwenden?** – Über diese Option können Sie 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.

10.8 LDAP

Microsoft Active Directory kann verwendet werden, um den 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 für verwaltete mobile Zugriffe. Andere Active Directory-Produkte (z. B. Open Directory) werden derzeit nicht unterstützt.



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

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

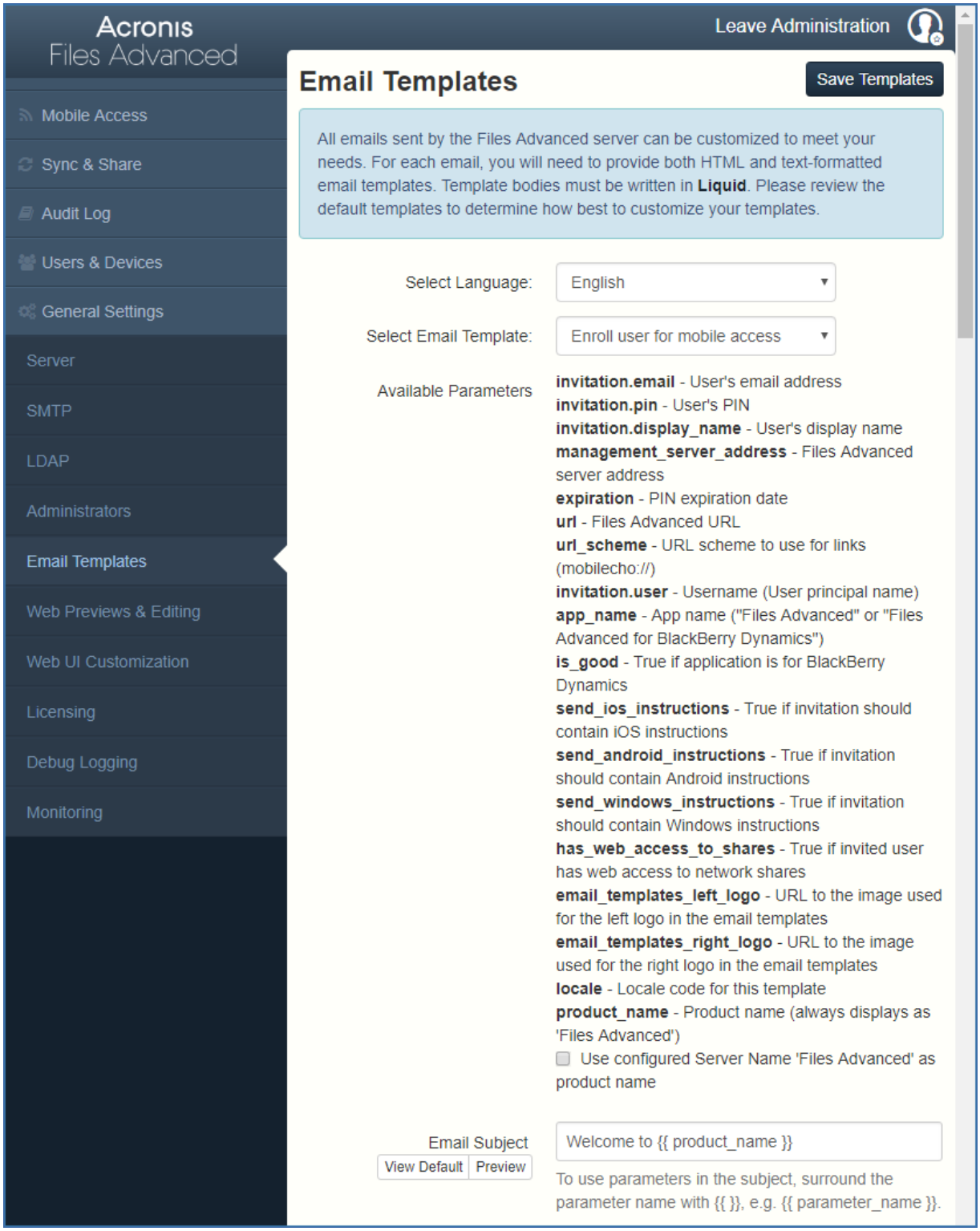
  Hinweis: *Wenn Sie mehrere Domains unterstützen, empfiehlt es sich, den Port für den globalen Katalog zu verwenden.*

- **Sichere LDAP-Verbindung verwenden?**– Ist standardmäßig deaktiviert. Aktivieren Sie das Kontrollkästchen, um Verbindungen mit Active Directory über sicheres LDAP herzustellen.
- **LDAP-Benutzername/-Kennwort** – diese Anmeldedaten werden für alle LDAP-Abfragen verwendet. Fragen Sie Ihren AD-Administrator, ob Ihnen Dienstkonten zugewiesen wurden, die verwendet werden müssen.
- **LDAP-Suchbasis** – geben Sie die Stammebene ein, auf der Suchvorgänge nach Benutzern und Gruppen beginnen sollen. Wenn Sie die gesamte Domain durchsuchen möchten, geben Sie die Zeichenfolge 'dc=domainname, dc=domainsuffix' ein.
- **Domains für LDAP-Authentifizierung** – Benutzer mit E-Mail-Adressen, deren Domains in dieser per Komma getrennten Liste aufgeführt sind, müssen sich über LDAP authentifizieren. (Für ein Konto mit der E-Mail-Adresse **joe@glilabs.com** würden Sie zur LDAP-Authentifizierung beispielsweise **glilabs.com** eingeben.). Benutzer mit anderen Domains müssen sich über die Files Advanced-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 Files Advanced die Active Directory-Struktur im Cache speichert.
- **LDAP-E-Mail-Adressen proaktiv auflösen** – wenn diese Einstellung aktiviert ist, wird Active Directory von Files Advanced 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.

10.9 E-Mail-Vorlagen

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

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



Hinweis: *Ab Files Advanced, Version 7.3, ist Liquid die standardmäßige Vorlagenauszeichnung. Sollten Sie benutzerdefinierte, in ERB geschriebene Vorlagen haben, wird ERB die standardmäßige Vorlagenauszeichnung für Ihren Server, selbst nach einer Aktualisierung.*

Hinweis: *Wenn Sie benutzerdefinierte Bilder in E-Mail-Vorlagen verwenden, sollten diese Bilder gehostet werden und an einer beliebigen Stelle im Internet verfügbar sein.*

Nach einem Upgrade von mobilEcho werden die Änderungen an den E-Mail-Vorlagen nicht migriert, sodass Sie die neuen Vorlagen anpassen müssen. Eine Kopie der vorherigen mobilEcho Vorlagen finden Sie im Ordner **Legacy mobilEcho files**, der sich standardmäßig hier befindet: **`C:\Program Files (x86)\Group Logic\Access Server\Legacy mobilEcho files`**. Die Dateien haben die folgenden Namen: **invitation.html.erb** und **invitation.txt.erb**.

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

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

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

  Hinweis: *Benutzerdefinierte Vorlagen werden **nicht** automatisch aktualisiert, wenn Sie Files Advanced aktualisieren. Wenn Sie diese Updates von Acronis nutzen wollen, müssen Sie sie manuell in Ihre benutzerdefinierten Vorlagen einbringen. Das betrifft alle Sprachen, die Sie unterstützen und nutzen.*

- **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.
- **Vorlage für Text-E-Mails** – Zeigt die E-Mail-Vorlage im Format 'Nur Text' 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.*

10.10 Lizenzierung

Eine Liste aller Lizenzen wird angezeigt.

- **Lizenz** – Der Typ der Lizenz (Test, Abonnement etc.).
- **Sync & Share – Lizenzierter Client – Verwendung** – Anzahl der aktuell verwendeten Sync & Share-LDAP-Benutzerlizenzen.
- **Sync & Share – Freier Client – Verwendung** – Anzahl der aktuell verwendeten freien externen Sync & Share-Benutzerlizenzen.

- **Access Mobile Client – Verwendung** – Anzahl der aktuell verwendeten Mobile Client-Lizenzen.

Eine neue Lizenz hinzufügen

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

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

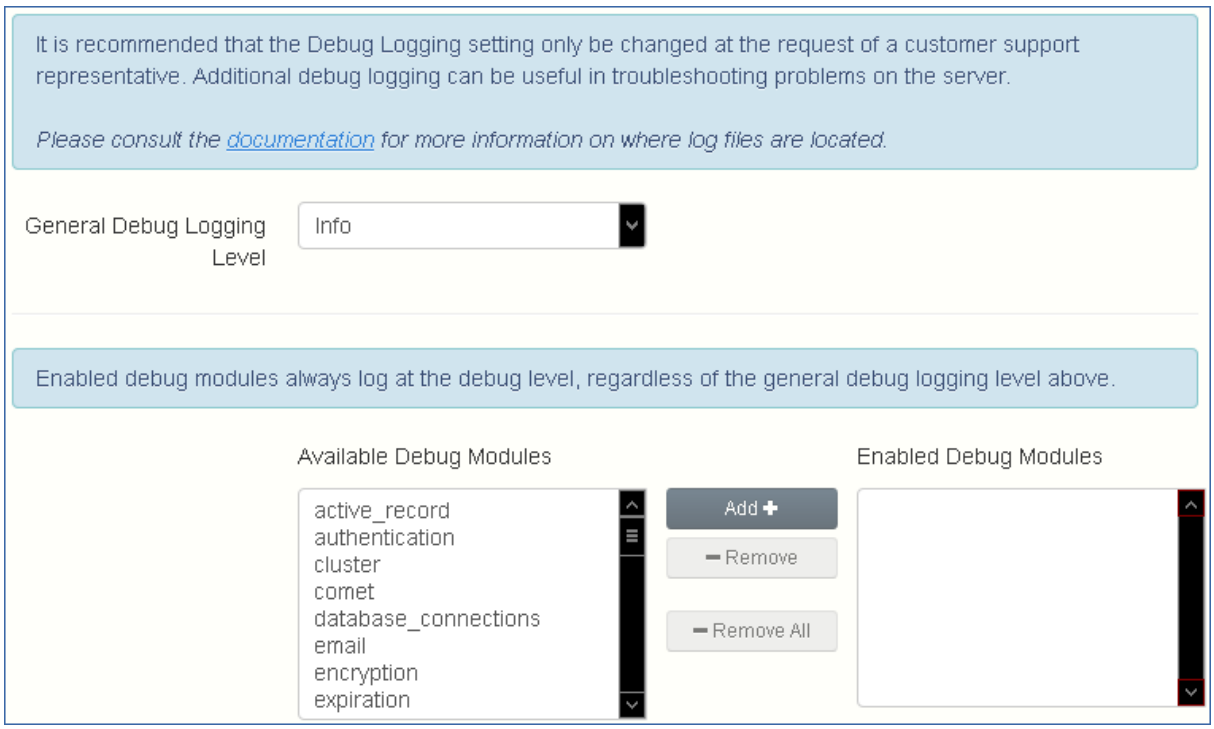
Das Hinzufügen einer neuen Lizenz für einen Gateway Server ist nicht erforderlich

Ab Files Advanced-Version 6.0 gilt für den Files Advanced-Server und die Gateway Server die gleiche Lizenz. Sie müssen den Gateway Servern Lizenzen daher nicht manuell hinzufügen.

10.11 Debug-Protokollierung

Über die Einstellungen auf dieser Seite können erweiterte Protokollierungsinformationen aktiviert werden, die bei der Konfiguration und Fehlerbehebung von Files Advanced 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 Artikel Bearbeiten von Gateway-Servern (S. 90).*



Ab Version 7.0 von Files Advanced Server wurde das Modul **Ausnahmen** aus der Liste der verfügbaren Module entfernt und wird immer standardmäßig aktiviert. Benutzer, die ein Upgrade aus einer Vorgängerversion von Files Advanced durchgeführt haben, können das Modul **Ausnahmen** weiterhin in der Liste sehen. Sobald Sie eine Änderung an den Protokollierungsoptionen durchführen und auf **Speichern** drücken, wird es ausgeblendet.

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

- **Allgemeine Debug-Protokollierungsebene** – Legt die Hauptebene für die Protokollierung fest (Info, Warnungen, Kritische Fehler usw.).

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

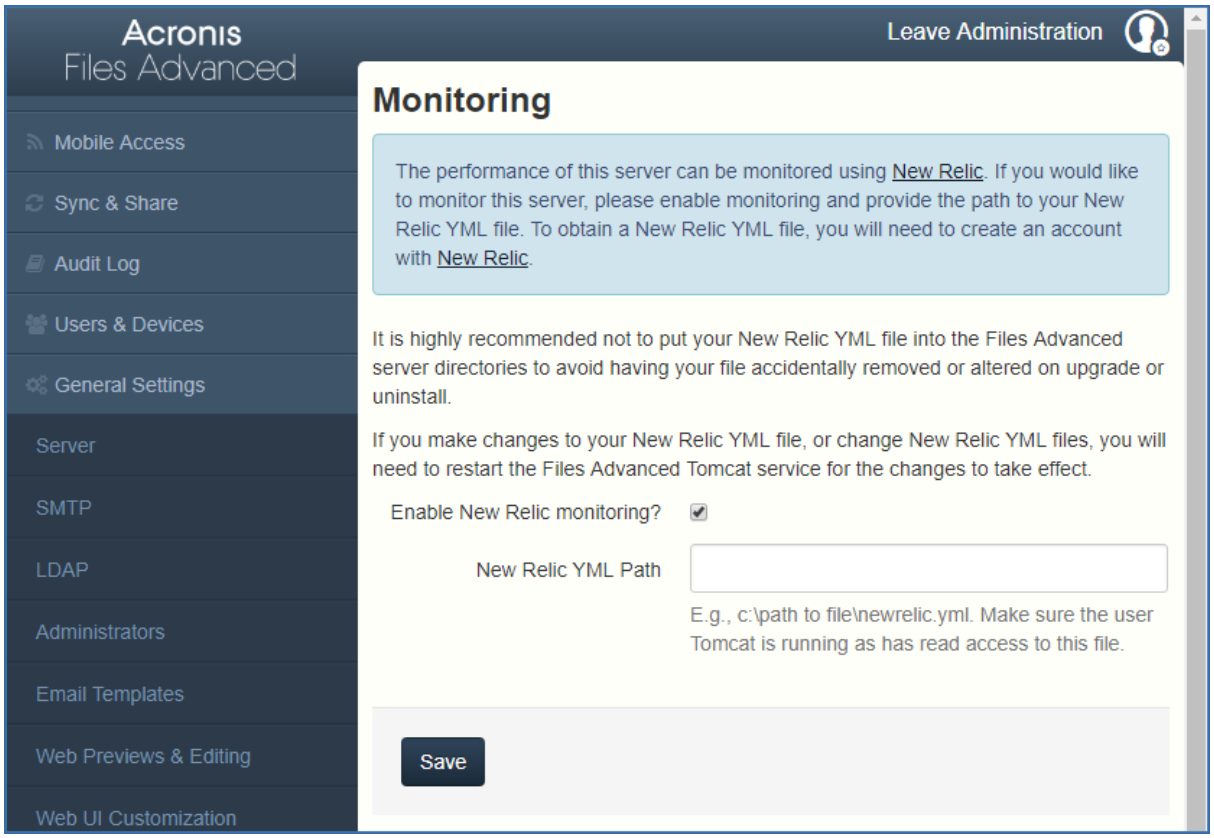
- **Verfügbare Debug-Module** – Zeigt eine Liste der verfügbaren Module an.
- **Aktivierte Debug-Module** – Zeigt die aktiven Module an.

Hinweis: *Falls es sich bei dem Produkt um ein Update und nicht um eine Neuinstallation handelt, befinden sich die Protokolldateien in* ***`C:\Program Files (x86)\Group Logic\Common\apache-tomcat-7.0.42\logs`***.

Hinweis: *Bei einer Neuinstallation von Files Advanced befinden sich die Protokolldateien unter* ***`C:\Program Files (x86)\Acronis\Files Advanced\Common\apache-tomcat-7.0.42\logs`***

10.12 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 Files Advanced 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 Files Advanced 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 Files Advanced 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, oder melden Sie sich mit einem bestehenden Konto an. Fahren Sie anschließend mit der Konfiguration Ihrer Applikation fort.
2. Wählen Sie unter 'Applikationstyp' die Option **APM** aus.
3. Markieren Sie unter 'Plattform' den Eintrag **Ruby**.
4. Laden Sie das in Schritt 3 der Startanleitung für 'New Relic' genannte Skript 'New Relic' herunter (newrelic.yml).
5. Öffnen Sie die Webkonsole von Files Advanced.
6. Navigieren Sie zu **Einstellungen** -> **Überwachung**.
7. 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 Files Advanced, sodass sie bei einem Upgrade oder einer Deinstallation nicht entfernt oder geändert werden.
8. Klicken Sie auf **Speichern** und warten Sie einige Minuten oder so lange, bis auf der New Relic-Website die Schaltfläche **Aktive Applikation(en)** verfügbar wird.
9. Wenn mehr als 10 Minuten vergehen, starten Sie den Files Advanced Tomcat-Dienst neu, und warten Sie einige Minuten. Die Schaltfläche sollte dann aktiv sein.
10. Sie sollten den Files Advanced Server auf der New Relic-Website überwachen können.

*Alle vom Files Advanced 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.

11 Wartungsaufgaben

Falls Sie ein Backup aller Elemente von Files Advanced erstellen möchten und um die Best Practices und Backup-Verfahren einzuhalten, sollten Sie den Artikel Richtlinien zum Desaster-Recovery (S. 149) lesen.

Themen

11.1 Richtlinien für Desaster-Recovery

Hohe Verfügbarkeit und schnelle Wiederherstellungen sind für geschäftskritische Applikationen wie Files Advanced 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 Files Advanced wieder in einen funktionsfähigen Zustand zu versetzen.

Einführung:

Für geschäftskritische Applikationen wie Files Advanced 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 Files Advanced 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 Files Advanced:

Files Advanced ist eine Lösung, die mehrere separate, jedoch miteinander verbundene Elemente umfasst:

Files Advanced Gateway Server

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

Files Advanced Server

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

Files Advanced Konfigurationswerkzeug

Hinweis**: Befindet sich normalerweise hier: **`C:\Program Files (x86)\Acronis\Files Advanced\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 Files Advanced installiert und verwendet wird. Die Files Advanced 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 Files Advanced 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 Files Advanced, 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 Files Advanced 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 Files Advanced 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 Files Advanced 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 Files Advanced 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 Files Advanced Datenbank wieder her.
7. Starten Sie den Files Advanced 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.

11.2 Best Practices

1. Regelmäßige Backups der Datenbank erstellen

Backups Ihrer Datenbank zu erstellen ist einer der wichtigsten Aspekte bei der Verwaltung von Files Advanced. Der Backup-Prozess (S. 153) kann völlig automatisiert werden, (S. 162) um Ihnen dabei zu helfen, Ihre Backups auf dem neuesten Stand zu halten.

Für Einrichtungen mit sehr großen Files Advanced-Serverdatenbanken werden möglicherweise andere als die angegebenen Backup- und Wiederherstellungsmethoden verwendet.

Einrichtungen mit Datenbanken von Gigabyte-Größe können einige zusätzliche Konfigurationen während des **Backup&Wiederherstellen**-Prozesses erfordern, um sie zu Beschleunigen oder sie anderweitig zu verbessern. Wenn Sie Unterstützung mit Ihrer spezifischen Konfiguration benötigen,

wenden Sie sich bezüglich Hilfe und Anleitungen bitte an unseren technischen Support unter http://www.acronis.com/en-us/mobilitysupport/.

2. Wir empfehlen, dass sehr große Einrichtungen ihre Datenbank(en) monatlich 'bereinigen' und 'analysieren'.

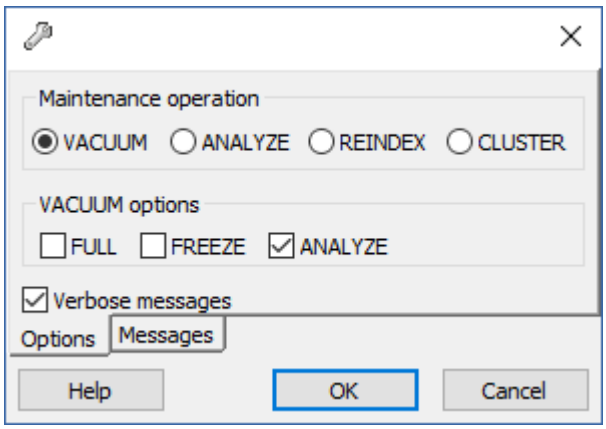
PostgreSQL-Datenbanken erfordern regelmäßige Wartung, bekannt als **`vacuuming`**. Der **VACUUM**-Befehl muss regelmäßig für jede Tabelle durchgeführt werden, um:

- Speicherplatz, der von gelöschten oder aktualisierten Zeilen belegt wird, wiederherzustellen und wieder zu verwenden.
- Vor dem Verlust sehr alter Daten zu schützen.
- Datenstatistiken zu aktualisieren und den Index-Scan zu beschleunigen.

Der **ANALYSIEREN-**Befehl erfasst Statistiken über die Inhalte der Tabellen in der Datenbank und speichert die Ergebnisse. Danach verwendet der Abfragenplaner diese Statistiken, um die effizientesten Ausführungspläne für die Abfragen festzulegen.

Um Ihre Datenbank(en) manuell zu bereinigen und zu analysieren, machen Sie Folgendes:

1. Öffnen Sie das Files Advanced PostgreSQL Administrator-Werkzeug (PgAdmin) und doppelklicken Sie auf **localhost**, um eine Verbindung zum Server herzustellen.
2. Klicken Sie mit der rechten Maustaste auf die **`acronisaccess_production`**-Datenbank, und wählen Sie **Wartung**.
3. Wählen Sie das Aktionsfeld **BEREINIGEN** und aktivieren Sie das Kontrollkästchen **ANALYSIEREN**.



Warnung! *Wenn Ihre Datenbank sehr groß ist, kann die Bereinigung einige Zeit dauern. Dieser Prozess sollte während niedriger Serverauslastung durchgeführt werden.*

4. Wählen Sie **OK**.
5. Wenn der **Bereinigungs**prozess beendet wird, klicken Sie auf **Fertig**.
6. Schließen Sie das PostgreSQL-Administrator-Tool.

Wenn Sie eine automatische Bereinigung festlegen möchten, lesen Sie bitte unseren Artikel unter: **Automatische Datenbankbereinigung (S. 163)**

3. Für große Einrichtungen sollten Sie die Ausführung einer Lastenausgleichseinstellung (S. 188) oder eines Clustering-Gateway-Servers (S. 99) erwägen.

11.3 Backup und Wiederherstellung von Files Advanced

Dies ist erforderlich, wenn Sie ein Upgrade, Update oder eine Wartung des Files Advanced Servers durchführen. In diesem Artikel werden Ihnen die Grundlagen vermittelt, um ein Backup und eine Wiederherstellung der Datenbank durchzuführen. Für Lastenausgleichskonfigurationen ist das Verfahren fast vollständig mit einem regelmäßigen Backup und einer Wiederherstellung identisch. Besonderheiten werden in den relevanten Schritten beschrieben.

Hinweis: *Wenn die Server-Datenbank von Files Advanced sehr groß ist (mehrere Gigabyte), empfiehlt sich möglicherweise eine andere Methode für das Backup und die Wiederherstellung der Datenbank. Für Unterstützung und Anweisungen steht unser technischer Support unter http://www.acronis.com/en-us/mobilitysupport/ zur Verfügung.*

Hinweis: *In einem Microsoft-Failovercluster können sich einige der Pfade unterscheiden, der Backup-Prozess ist jedoch gleich. Er sollte am aktiven Knoten durchgeführt werden, und Sie müssen sicherstellen, dass kein Failover der Rolle stattfindet und die Rolle während des Backups startet.*

Wir empfehlen dringend, ein Test-Backup/eine Test-Wiederherstellung in einer Testumgebung durchzuführen, bevor Sie mit dem Backup/der Wiederherstellung Ihrer Produktionsumgebung fortfahren.

Themen

7.

1. Stoppen Sie den Files Advanced Tomcat-Dienst.

   Hinweis: *Wenn Sie einen Lastenausgleich für mehrere Files Advanced-Tomcat-Dienste vornehmen, stoppen Sie alle.*

2. Öffnen Sie die PostgreSQL Administratorapplikation von Files Advanced und stellen Sie eine Verbindung zum Datenbankserver her. Sie werden ggf. aufgefordert, das Kennwort für den `postgres` Benutzer einzugeben.
3. Erweitern Sie **Datenbanken** und klicken Sie mit der rechten Maustaste auf die Datenbank **acronisaccess_production**.
4. Wählen Sie **Wartung** und das Aktionsfeld **Bereinigen** und aktivieren Sie dann das Kästchen **ANALYSIEREN**. Wählen Sie **OK**.
5. Erweitern Sie die Datenbank und dann **Schemas** und **Öffentlich**. Notieren Sie die Anzahl im Abschnitt **Tabellen**. Dies kann Ihnen bei der Überprüfung helfen, ob die Datenbankwiederherstellung nach einem Recovery erfolgreich war.
6. Schließen Sie die PostgreSQL-Administratorapplikation und öffnen Sie eine Eingabeaufforderung mit erweiterten Benutzerrechten.
7. Navigieren Sie in der Eingabeaufforderung zum PostgreSQL-Verzeichnis 'bin'.

   Beispiel: `cd "C:\Program Files(x86)\Acronis\Access\Common\PostgreSQL\9.3\bin"`

8. Geben Sie den folgenden Befehl ein: **pg_dumpall --host localhost --port 5432 --username postgres --file alldbs.sql**
   - **alldbs.sql** ist der Dateiname des Backups. Es wird im PostgreSQL-Verzeichnis 'bin' gespeichert. Sie können mit dem obigem Befehl auch einen anderen Pfad zum Speichern des Backups eingeben – ändern Sie z.B. den letzten Teil des obigen Befehls wie folgt: **--file D:\Backups\alldbs.sql**
   - Wenn Sie nicht den Standard-Port verwenden, müssen Sie statt **5432** die richtige Portnummer eingeben.
   - Wenn Sie nicht das Standard-Administratorkonto von PSQL, **postgres**, verwenden, muss im obigen Befehl **postgres** durch den Namen des Administratorkontos ersetzt werden.
   - Während dieses Vorgangs werden Sie mehrmals aufgefordert, das **postgres** -Kennwort des Benutzers einzugeben. Geben Sie bei jeder Aufforderung das Kennwort ein und drücken Sie die Eingabetaste.

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

9. Kopieren Sie die Backup-Datei an einen sicheren Speicherort.
10. Navigieren Sie zu der **postgresql.conf**-Datei und kopieren Sie diese an einen sicheren Ort, da sie wichtige Einstellungen enthalten kann. Sie befindet sich im PostgreSQL-Datenordner – standardmäßig unter **C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL\<version>\Data**.

1. Stoppen Sie den Files Advanced Gateway-Dienst.
2. Wechseln Sie zum Datenbankordner des Gateway Servers. Sie finden ihn standardmäßig an folgendem Speicherort:

   C:\Program Files (x86)\Acronis\Files Advanced\Gateway Server\database
3. Kopieren Sie die Datei **mobilEcho.sqlite3** an einen sicheren Speicherort.
4. Wenn Sie mehrere Gateway Server besitzen, wiederholen Sie diesen Vorgang für jeden Server und stellen Sie sicher, dass die Datenbankdateien nicht durcheinander geraten.

Wenn Sie Änderungen an den nachfolgenden Dateien vorgenommen haben, wird empfohlen, Backups zu erstellen, damit Sie Ihre Einstellungen beim Wiederherstellen oder Migrieren des Produkts Files Advanced übernehmen können.

- Die Datei **postgresql.conf**, da diese wichtige Einstellungen enthalten kann, die für Ihre Datenbank relevant sind. Sie befindet sich in der Regel unter **C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL\<version>\Data**.
- Datei: **web.xml**. Standardspeicherort: **C:\Program Files (x86)\Acronis\Files Advanced\Access Server\Web Application\WEB-INF**. Enthält Einstellungen für die Einzelanmeldung (Single Sign-On).
- Datei: **server.xml**. Standardspeicherort: **C:\Program Files (x86)\Acronis\Files Advanced\Common\apache-tomcat-<version>\conf**. Enthält Einstellungen für Tomcat.
- Datei: **krb5.conf**. Standardspeicherort: **C:\Program Files (x86)\Acronis\Files Advanced\Common\apache-tomcat-<version>\conf**. Enthält Einstellungen für die Einzelanmeldung (Single Sign-On).
- Datei: **login.conf**. Standardspeicherort: **C:\Program Files (x86)\Acronis\Files Advanced\Common\apache-tomcat-<version>\conf**.
- Ihre für Files Advanced verwendeten Zertifikate und Schlüssel.
- Datei: **acronisaccess.cfg**. Standardspeicherort: **C:\Program Files (x86)\Acronis\Files Advanced\Access Server**.

- Benutzerdefinierte Farbschemas. Standardspeicherort: **C:\Program Files (x86)\Acronis\Files Advanced\Access Server\Web Application\customizations**.
- Datei: **pg_hba.conf**. Standardspeicherort: **C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL\<version>\Data**.
- Datei: **newrelic.yml** . Wenn Sie den Files Advanced Server mit **New Relic** überwachen.

1. Öffnen Sie die Systemsteuerung **Dienste** und stoppen Sie den Tomcat-Dienst von Files Advanced.

   Hinweis: *Halten Sie für Lastenausgleichskonfigurationen alle Files Advanced Tomcat-Dienste an.*

2. Öffnen Sie die PostgreSQL-Administrator-Applikation von Files Advanced und stellen Sie eine Verbindung mit dem lokalen Datenbankserver her. Wählen Sie **Datenbanken** aus und vergewissern Sie sich, dass eine Datenbank mit dem Namen **acronisaccess_production** vorhanden ist.
3. Klicken Sie mit der rechten Maustaste auf die Datenbank, und wählen Sie **Aktualisieren**.
4. Erweitern Sie diese, und erweitern Sie **Schemas**. Erweitern Sie **Öffentlich**, und vergewissern Sie sich, dass keine (0) **Tabellen** vorhanden sind.
   - Sind Tabellen in der Datenbank enthalten, klicken Sie mit der rechten Maustaste auf die Datenbank, und benennen Sie sie um in **oldacronisaccess_production**. Gehen Sie abschließend zu **Datenbanken**, klicken Sie mit der rechten Maustaste, und erstellen Sie eine neue Datenbank mit dem Namen **acronisaccess_production**.
5. Schließen Sie die PostgreSQL-Administratorapplikation und öffnen Sie eine Eingabeaufforderung mit erweiterten Benutzerrechten.
6. Navigieren Sie in der Eingabeaufforderung zum PostgreSQL-Verzeichnis 'bin'.

   Beispiel: cd "C:\Program Files\Acronis\Access\Common\PostgreSQL\9.3\bin"
7. Kopieren Sie die Datenbank-Backupdatei **alldbs.sql** (oder den von Ihnen dafür verwendeten Namen) in das Verzeichnis **bin** .
8. Geben Sie in der Eingabeaufforderung den folgenden Befehl ein: **psql -U postgres -f alldbs.sql**
9. Geben Sie Ihr **postgres** Kennwort ein, wenn Sie dazu aufgefordert werden.

   Hinweis: *Je nachdem, wie groß Ihre Datenbank ist, kann die Wiederherstellung einige Zeit dauern.*

   Schließen Sie das Fenster mit der Eingabeaufforderung, wenn die Wiederherstellung beendet ist.
10. Öffnen Sie erneut die PostgreSQL Administratorapplikation von Files Advanced und stellen Sie eine Verbindung zum lokalen Datenbankserver her.
11. Wählen Sie **Datenbanken** aus.
12. Erweitern Sie die **acronisaccess_production**-Datenbank und dann **Schemata** und **Öffentlich**. Überprüfen Sie, ob die Anzahl der **Tabellen** mit der in Schritt 5 des Abschnitts „Backup der Files Advanced-Datenbank“ übereinstimmt.

Hinweis: *Wenn die Server-Version von Files Advanced, in der Sie die Datenbank wiederherstellen, neuer ist als die Version aus Ihrer Datenbanksicherung und der Tomcat-Dienst von Files Advanced bereits gestartet wurde, könnte die Anzahl der Tabellen in der neuen Files Advanced-Datenbank größer sein als die Anzahl, über die Sie während der Durchführung der Sicherung verfügten.*

1. Stoppen Sie den Files Advanced Gateway-Dienst.
2. Kopieren Sie das Gateway Server-Datenbank-Backup **mobliEcho.sqlite3** in den Datenbankordner des neuen Gateway Servers (standardmäßig **C:\Program Files (x86)\Acronis\Files Advanced\Gateway Server\database**), und ersetzen Sie damit die vorhandene Datei.

3. Wiederholen Sie dieses Verfahren für alle Gateway Server.

Stellen Sie sicher, dass sämtliche an den Konfigurationsdateien (web.xml, server.xml, krb5.conf, Zertifikate, benutzerdefinierte Farbschemen, E-Mail-Vorlagen, pg_hba.conf oder newrelic.yml) von Files Advanced vorgenommene Anpassungen kopiert werden und verschieben Sie diese zu den neuen Dateien.

Nachdem Sie erfolgreich ein Backup/eine Wiederherstellung oder eine Migration auf einen anderen Computer durchgeführt haben, sollten Sie Files Advanced wieder online schalten und überprüfen, ob alle Einstellungen korrekt sind.

Herkömmliche Bereitstellungen online schalten

1. Starten Sie das Konfigurationsprogramm von Files Advanced und vergewissern Sie sich, dass alle Einstellungen dort korrekt sind.
2. Drücken Sie auf „OK“, um alle Dienste zu starten.
3. Alle Dienste werden gleichzeitig online geschaltet, und alle Funktionen von Files Advanced werden wiederhergestellt.
4. Wenn sich Komponenten auf einem separaten Rechner befinden, greifen Sie auf diesen Rechner zu, um diese ebenfalls zu starten. In diesem Fall muss der PostgreSQL-Dienst ausgeführt werden, damit der Tomcat-Dienst von Files Advanced fehlerfrei startet.

Bereitstellungen mit Lastenausgleich online schalten

1. Wählen Sie, welcher der Server von Files Advanced als Primärserver dienen soll. Primär bedeutet in diesem Fall nur, dass der Server als Erster online geschaltet wird.
2. Befindet sich der PostgreSQL-Dienst auf einem anderen Computer, muss dieser zuerst gestartet werden, da dies den Server von Files Advanced beeinflusst.
3. Greifen Sie auf den Computer mit dem Primärserver von Files Advanced zu und starten Sie das Konfigurationsdienstprogramm von Files Advanced.
4. Stellen Sie sicher, dass dort alle Einstellungen korrekt sind. Wenn keine Probleme vorliegen, drücken Sie OK, um alle Dienste zu starten.
5. Rufen Sie die Webkonsole von Files Advanced auf und melden Sie sich als Administrator an. Überprüfen Sie, ob alle Einstellungen korrekt sind.
6. Wenn Sie die Einstellungen überprüft haben, greifen Sie auf jeden Computer mit einer Komponente von Files Advanced zu und starten Sie diese über das Konfigurationsdienstprogramm.

11.4 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\Files Advanced\Common\apache-tomcat-7.0.34\logs**"
Files Advanced speichert seine eigenen Logs im gleichen Verzeichnis als separate Dateien.

*Die Logdateien von Files Advanced haben den Namen **acronisaccess_date**.*

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

***Info:** Informationen zu ForFiles einschließlich Befehlssyntax und Beispielen finden Sie unter*
http://technet.microsoft.com/en-us/library/cc753551(v=ws.10).aspx
http://technet.microsoft.com/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:** Das Beispielskript (Batchdatei) funktioniert unter Windows Server 2008. Klicken Sie hier, um dieses Skript herunterzuladen.*
Sie können das Skript auf Wunsch auch kopieren, in ein leeres Textdokument einfügen und unter 'AASTomcatLogPurge.bat' speichern.

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

```
ECHO OFF

 REM Script: aETomcatLogsPurge.bat

 REM 2012-05-12: Version: 1.0: MEA: Created

ECHO This script will delete files older than a number of days from a directory

 ECHO Run it from the command line or from a scheduler

 ECHO Make sure the process has permissions to delete files in the target folder

REM ===== CONFIGURATIONS ====================================================

REM Note: all paths containing spaces must be enclosed in double quotes

 REM Edit this file and set LogPath and NumDays below

REM Path to the folder where all Tomcat logs are

 set LogPath="C:\Program Files (x86)\Group Logic\Common\apache-tomcat-7.0.34\logs"


REM NumDays - Log files older than NumDays will be processed

 set NumDays=14
```

```
REM ===== END OF CONFIGURATIONS =======================

ECHO

ECHO ===== START ============

REM ForFiles options:

 REM       "/p": the path where you want to delete files.

 REM       "/s": recursively look inside other subfolders present in the folder
mentioned in the batch file path

 REM       "/d": days for deleting the files older than the present date. For instance
"/d -7" means older than 7 days

 REM       "/c": command to execute to actually delete files: "cmd /c del @file".

forfiles /p %LogPath% /s /d -%NumDays% /c "cmd /c del @FILE"

:End

ECHO ===== BATCH FILE COMPLETED ============================================
```

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

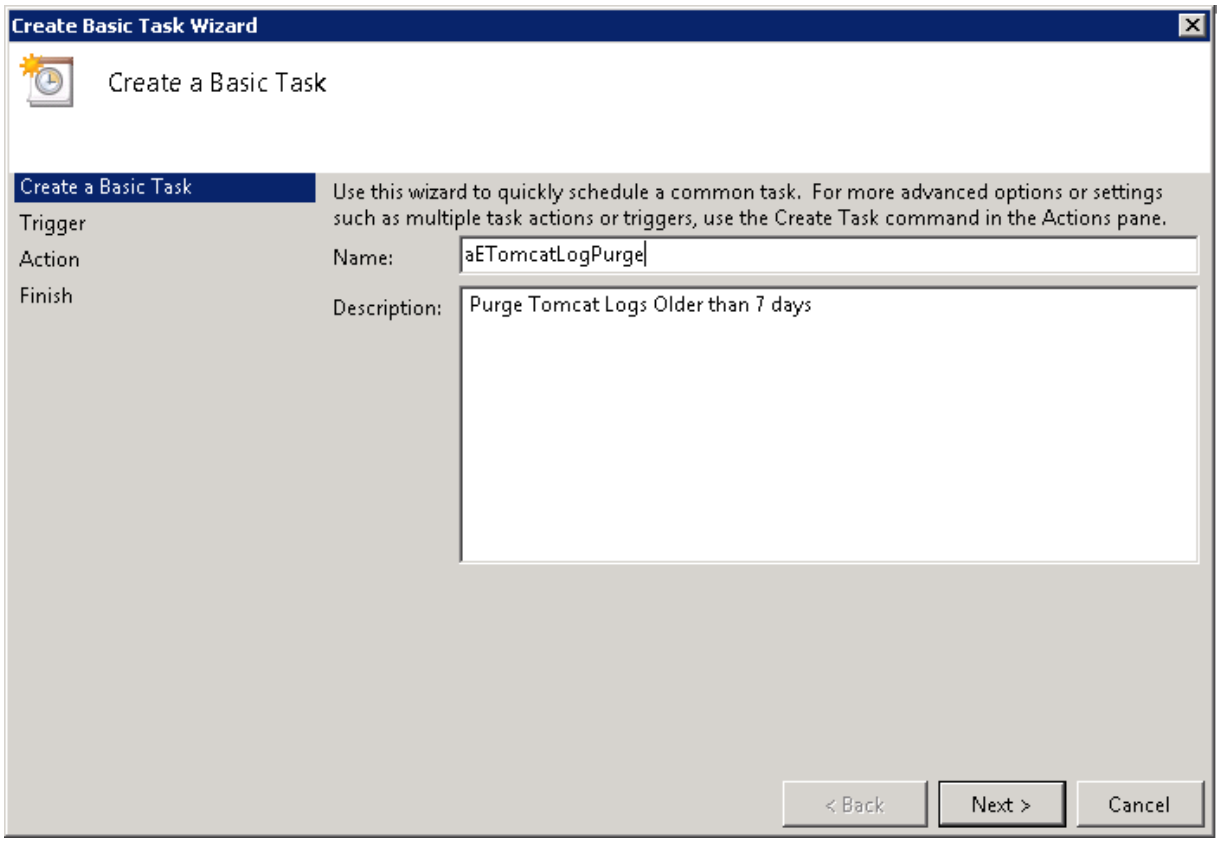
Schritte

1. Kopieren Sie das Skript auf den Computer, auf dem Files Advanced (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:

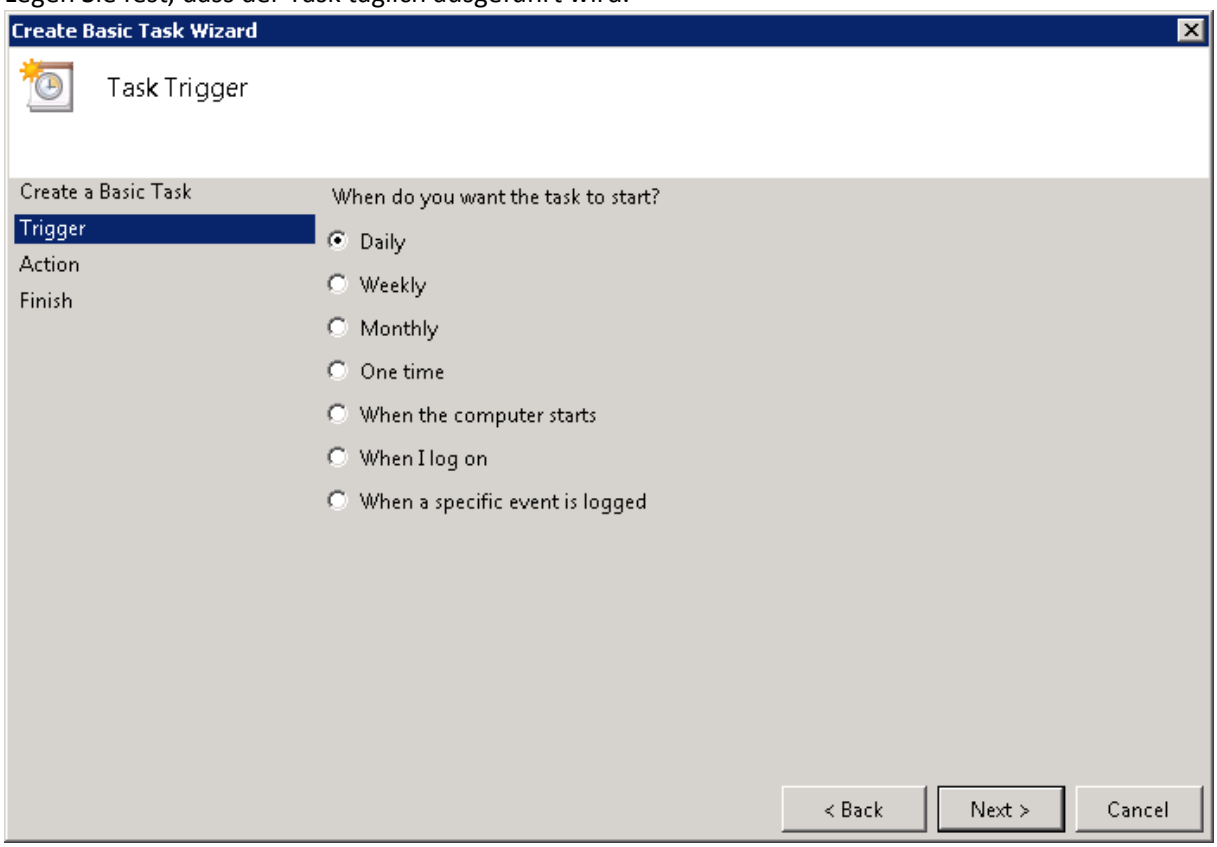
```
REM ===== CONFIGURATIONS ====================================================
REM Note: all paths containing spaces must be enclosed in double quotes
 REM Edit this file and set LogPath and NumDays below
REM Path to the folder where all Tomcat logs are
 set LogPath="C:\Program Files (x86)\Group Logic\Common\apache-tomcat-7.0.34\logs"

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

   In Files Advanced werden die Logdateien im gleichen Ordner wie diejenigen von Tomcat gespeichert. (***C:\Program Files (x86)\Acronis\Files Advanced\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.

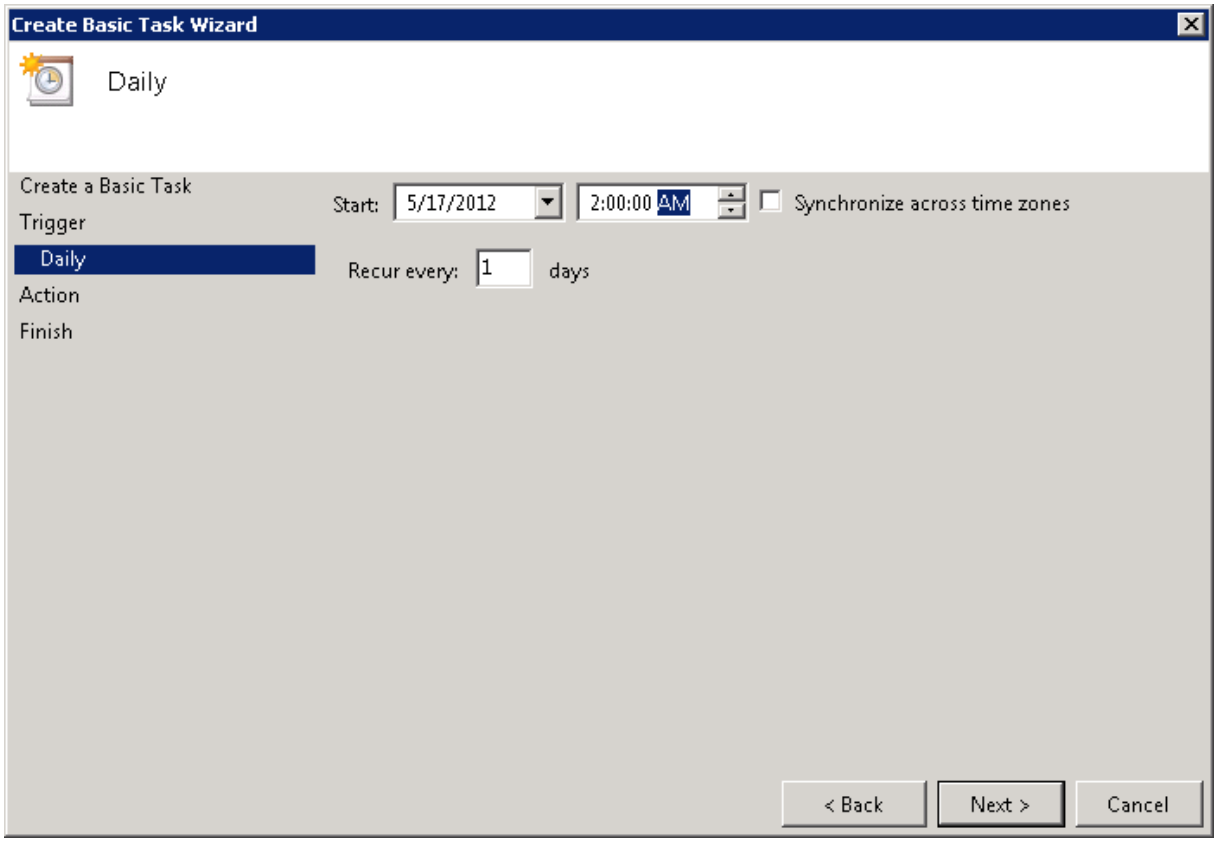


5. Legen Sie fest, dass der Task täglich ausgeführt wird.

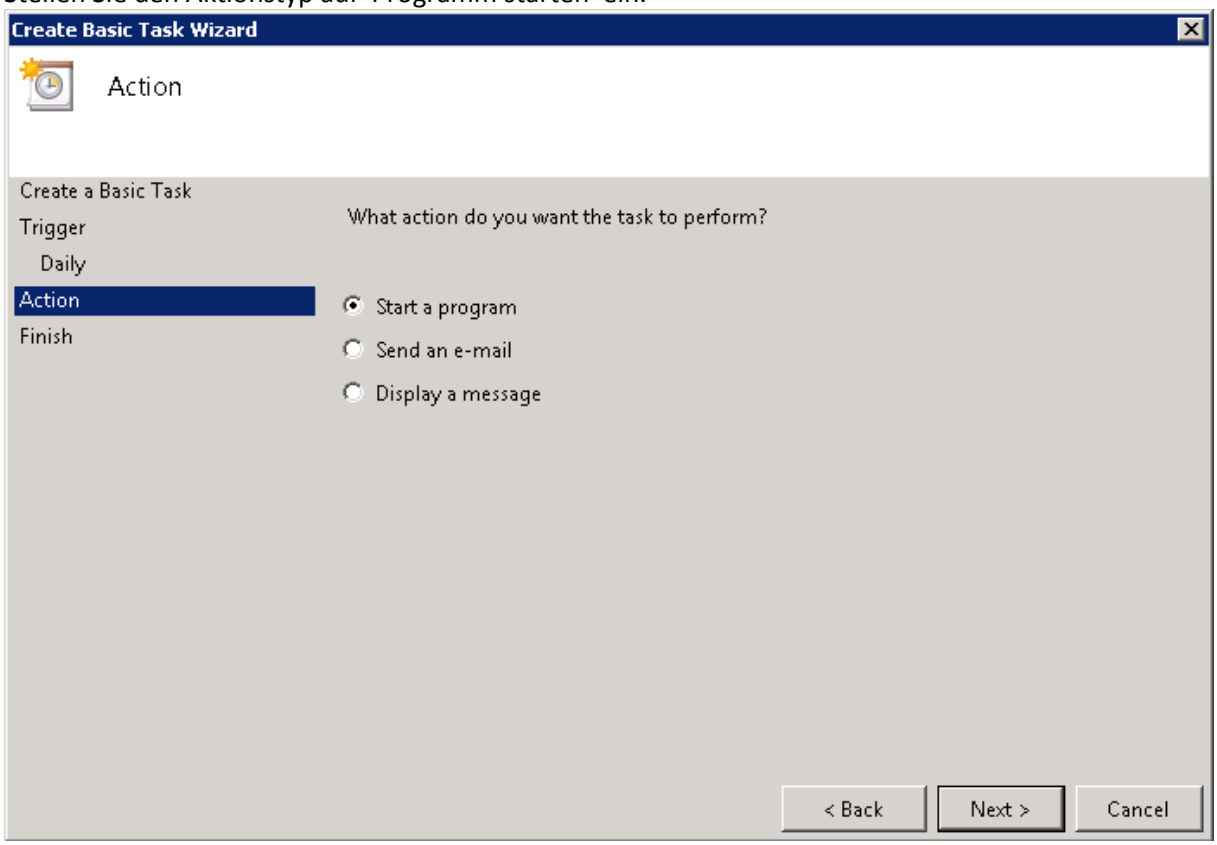


6. Geben Sie an, zu welcher Uhrzeit die Task starten soll. Es wird empfohlen, diesen Prozess nicht auszuführen, wenn das System extrem belastet ist oder andere Wartungsprozesse ausgeführt

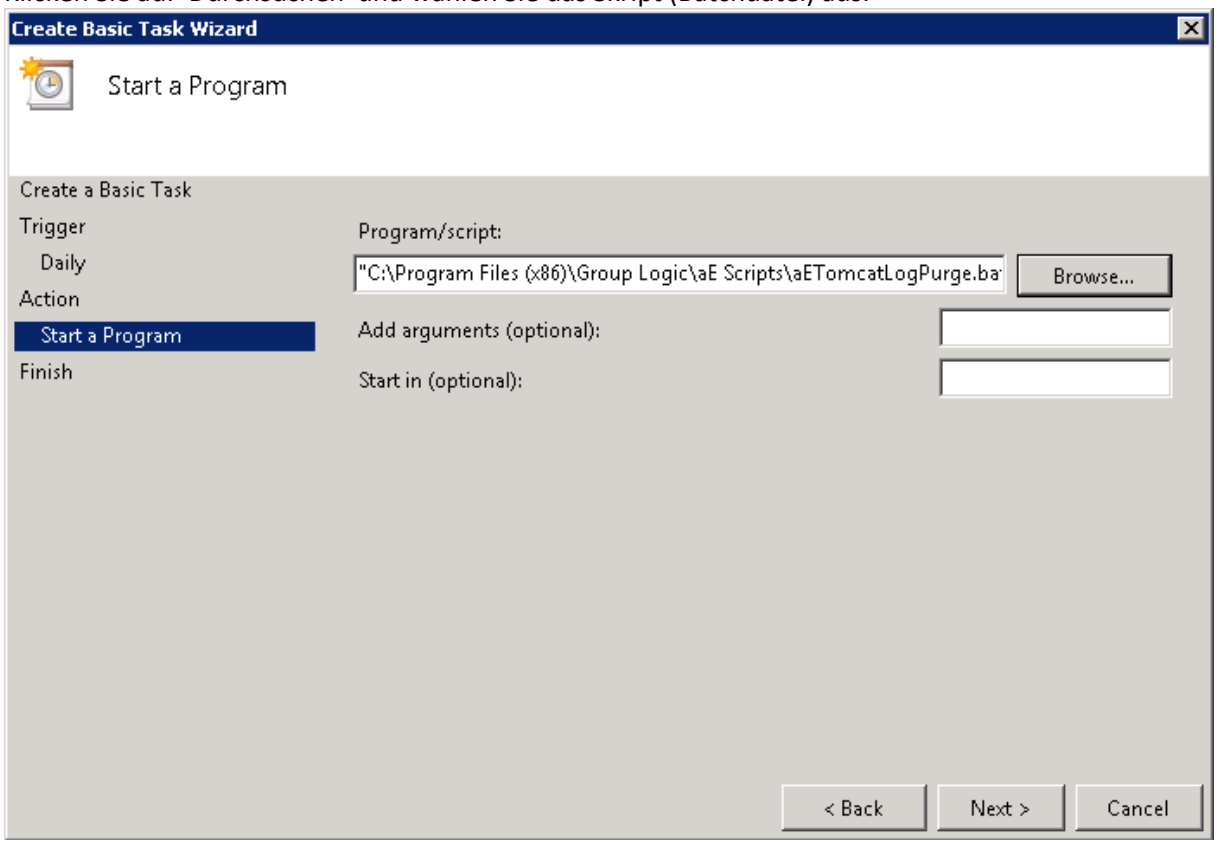
werden.



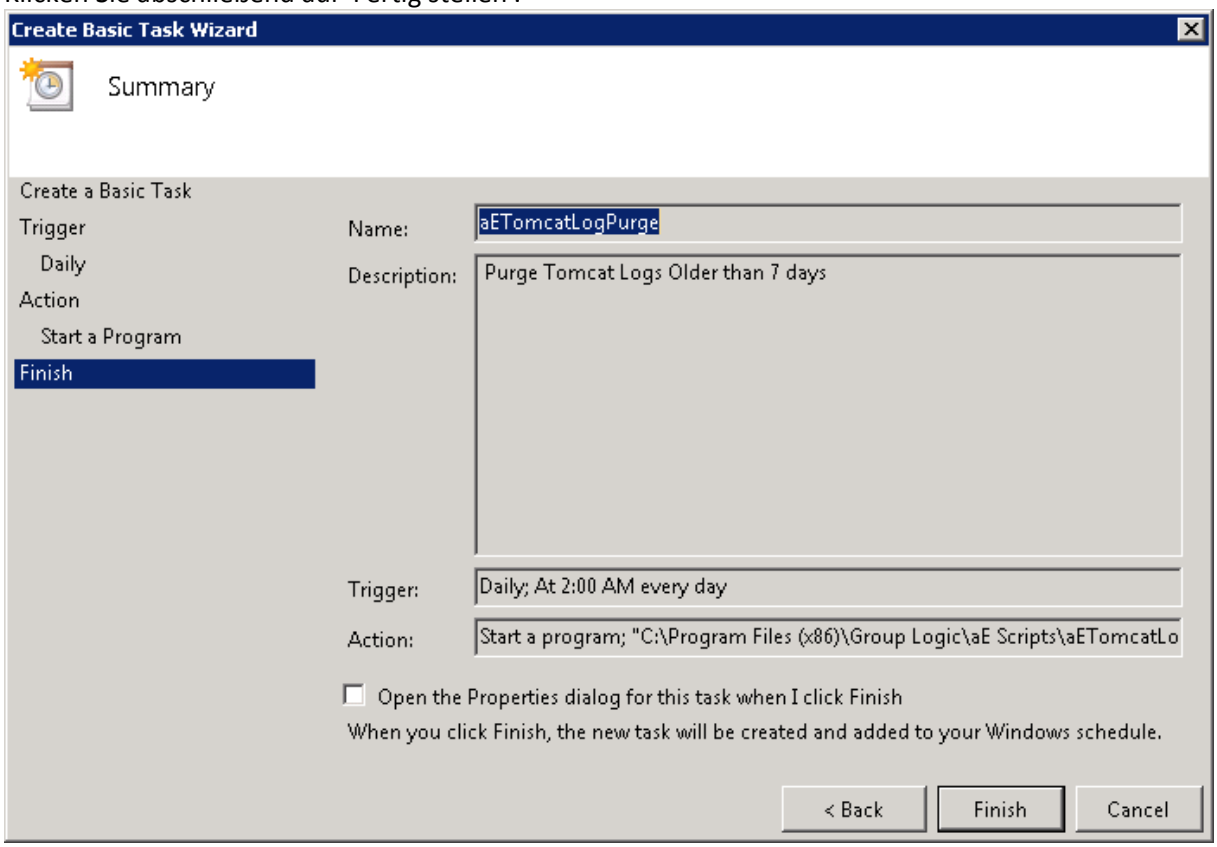
7. Stellen Sie den Aktionstyp auf 'Programm starten' ein.



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.

11.5 Automatische Datenbanksicherung

Mithilfe des Windows Task Scheduler können Sie auf einfache Weise einen automatischen Sicherungszeitplan für Ihre Files Advanced-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 Files Advanced 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 die **Aufgabenplanung**.
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 abgelegt ist. Beispiel: Wenn der Pfad des Skripts **`C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL\9.3\PSQL.bat`** lautet, geben Sie **`C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL\9.3\`** ein.
5. Wählen Sie **OK**.
6. Konfigurieren Sie auf den übrigen Registerkarten beliebige zusätzliche Einstellungen und wählen Sie **OK**.
7. Sie werden aufgefordert, die Anmeldedaten für das aktuelle Konto einzugeben.

11.6 Automatische Datenbankbereinigung

Dieser Leitfaden wird Ihnen bei der Erstellung geplanter Tasks, die die PostgreSQL-Datenbank ausführen und bereinigen, behilflich sein. Die Bereinigung ist ein wichtiger Prozess, besonders dann, wenn Ihre Einrichtung über eine große Datenbank verfügt.

Hinweis: *PostgreSQL ist in der Konfigurations-Datei auf automatische Bereinigung eingestellt. Bei Einrichtungen unter großer Last ist es jedoch möglich, dass die automatische Bereinigung niemals ausgeführt wird, denn sie wurde so konzipiert, dass sie nicht ausgeführt wird, wenn der Server unter hoher Last steht. Für dieses Fälle ist es am besten, einen geplanten Task festzulegen, um die Bereinigung mindesten einmal im Monat auszuführen.*

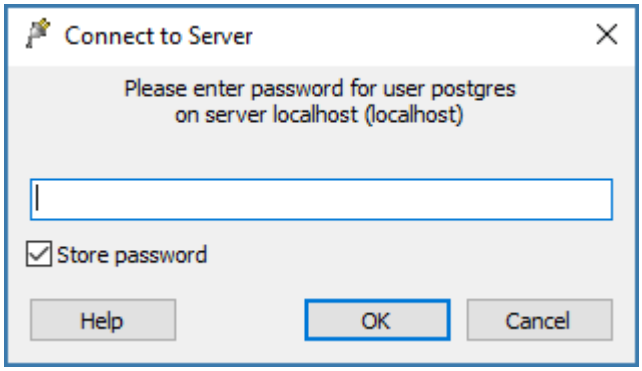
Konfiguration von PostgreSQL und Erstellung des Skripts

Sicherstellen, dass der Task ausgeführt werden kann

Sie müssen sicherstellen, dass das Postgres-Benutzerkennwort in der Pgpass-Datei gespeichert ist, ansonsten kann das Skript nicht ausgeführt werden. Der einfachste Weg ist über das Files Advanced PostgreSQL Administrator-Tool:

1. Öffnen Sie den Files Advanced PostgreSQL-Administrator. Sie finden ihn im Startmenü von Windows im Ordner von Files Advanced.
2. Stellen Sie eine Verbindung zur Datenbank her, setzen Sie ein Häkchen bei **Kennwort speichern** in der Dialogbox, die sich zur Eingabe des Kennwortes öffnet und klicken Sie auf **OK**. Das Postgres-Benutzerkennwort wurde nun in der Pgpass-Datei gespeichert. Diese Datei wird in **`C:\Users\<currentUser>\AppData\Roaming\postgresql`** erstellt.

   Hinweis: *Möglicherweise sehen Sie ein Dialogfeld mit Informationen zum Speichern von Kennwörtern. Das ist so vorgesehen. Drücken Sie OK.*

   - Alternativ können Sie eine Datei namens **pgpass.conf** manuell erstellen und den folgenden Text eingeben **`localhost:5432:*:postgres:yourpassword`**
   - Stellen Sie sicher, dass Sie Ihr **tatsächliches** Postgres-Benutzerkennwort und den richtigen Pfad eingeben. Speichern Sie die Datei.

3. Für das Beispiel wird die Datei **pgpass.conf** in den Ordner **D:\Backup** kopiert. Der Benutzer, der den geplanten Task ausführt, muss Lesezugriff auf die Datei haben.

Erstellung des Skripts.

Im folgenden Beispiel ist der PostgreSQL-**`bin`** Verzeichnispfad auf **`C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL\<VERSION>\bin\`** festgelegt.

*Hinweis: Sie müssen den Pfad so bearbeiten, dass er auf den PostgreSQL-**`bin`** Ordner verweist, wenn Sie einen älteren Ordner oder eine benutzerdefinierte Installation verwenden (Beispiel: C:\Program Files (x86)\Acronis\Access\Common\PostgreSQL\9.4\bin\).*

1. Erstellen Sie einen Ordner, in dem die Protokolldateien gespeichert werden, und weisen Sie dem Benutzer, der die Task ausführen, Lese-, Schreib- und Ausführberechtigungen für den Ordnen zu. Wir empfehlen, dass Sie den Administrator des Computers als Benutzer wählen. In unserem Beispiel ist der Log-Ordner **`D:\Backup\`**.

2. Öffnen Sie den gewünschten Text-Editor (z.B. Notepad) und fügen Sie das folgende Beispiel-Skript ein:

```
SET PGPASSFILE=D:\Backup\pgpass.conf
"C:\Program Files (x86)\Acronis\Files
Advanced\Common\PostgreSQL\9.4\bin\psql.exe" --host=localhost --port 5432
--username=postgres -d acronisaccess_production -c "VACUUM VERBOSE ANALYZE"
>"D:\Backup\vacuum_report_%date:/=.%.log" 2>&1
```

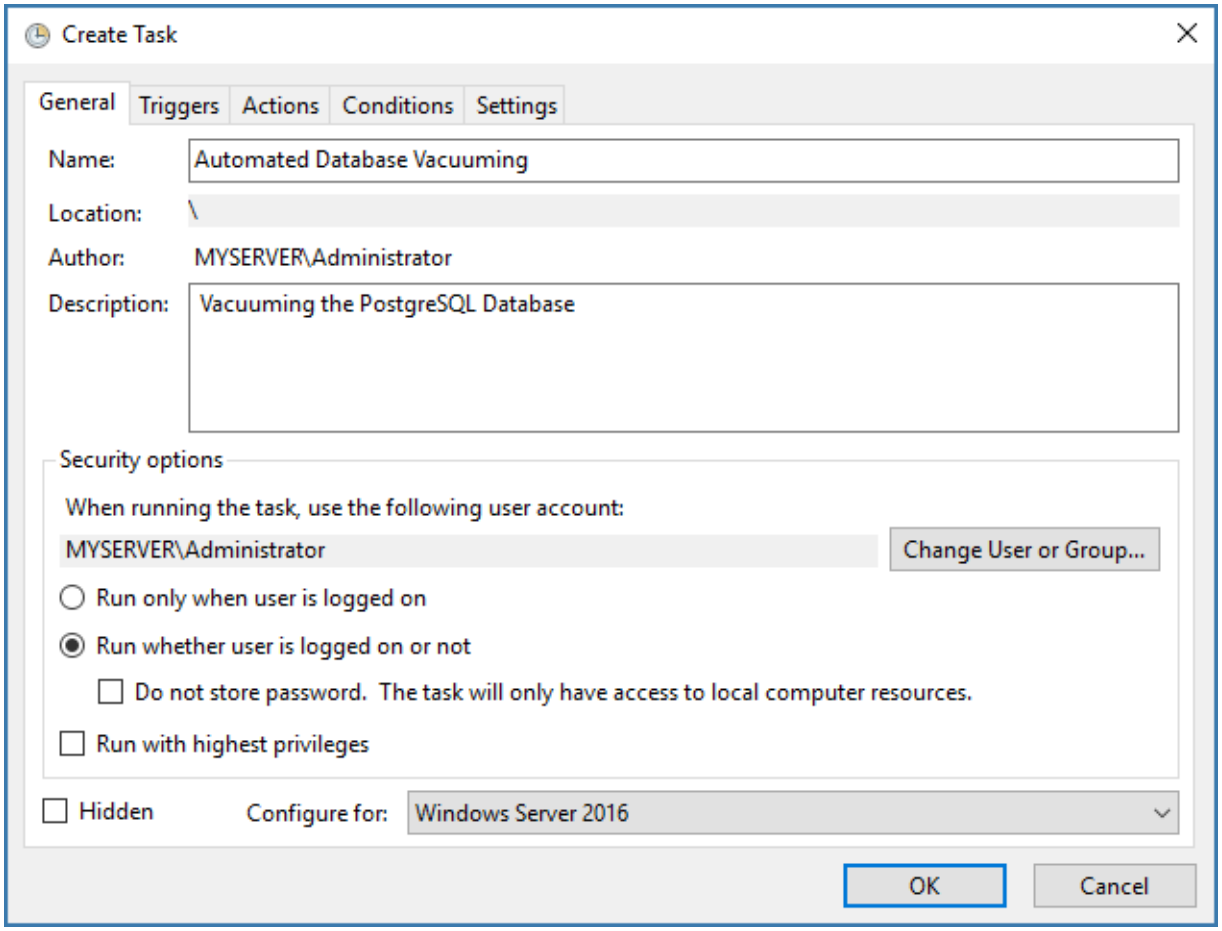
3. Bearbeiten Sie dieses Skript, sodass es zu Ihrer Einrichtung passt.
   - Ersetzen Sie den Pfad zur **`psql.exe`** -Datei mit Ihrem Dateipfad.
   - Ändern Sie die **`--port`**-Einstellung in die korrekte Port-Nummer, wenn Sie den Standardeinstellung geändert haben.
   - Wenn Sie einen anderen PostgreSQL-Benutzer verwenden, ändern Sie den **`--username=`**, indem Sie **`postgres`** mit dem gewünschten Benutzer ersetzen.
   - Ändern Sie den **`D:\Backup\`** -Teil des Pfads für die Logs zu Ihrem gewünschten Log-Ordner.
   - Ändern Sie den **`D:\Backup\`**-Teil des Pfads für die Datei pgpass.conf zu dem Pfad der Datei.
4. Speichern Sie die Datei als **vacuum.bat**. Stellen Sie sicher, dass Sie unter **Speichern als Dateityp Alle Dateitypen** ausgewählt haben.

***HINWEIS**: Abhängig von Ihrem Datumsformat, kann diese **.log**-Dateierstellung fehlschlagen. Um das Datumsformat zu finden, können Sie eine Eingabeaufforderung öffnen und ausführen: Wenn im Datum einige unzulässige Zeichen, wie Schrägstriche, enthalten sind, müssen diese umgewandelt werden. Im Beispiel oben ist der Zusatz **`:/=`**. der Konvertierungsteil. Sollten Probleme auftreten, kontaktieren Sie den Acronis Support.*

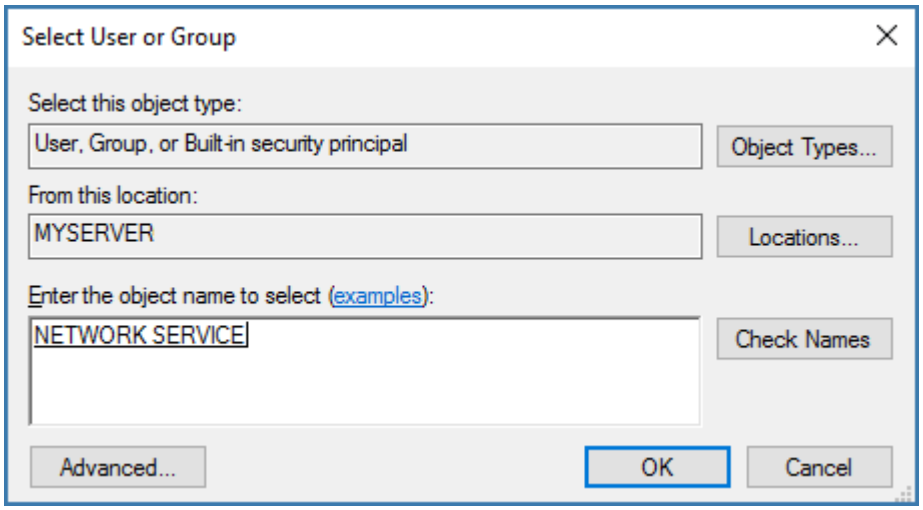
Konfiguration des Task Schedulers.

1. Öffnen Sie den **Task Scheduler** in der **Systemsteuerung** -> **Verwaltung** -> **Task Scheduler**.

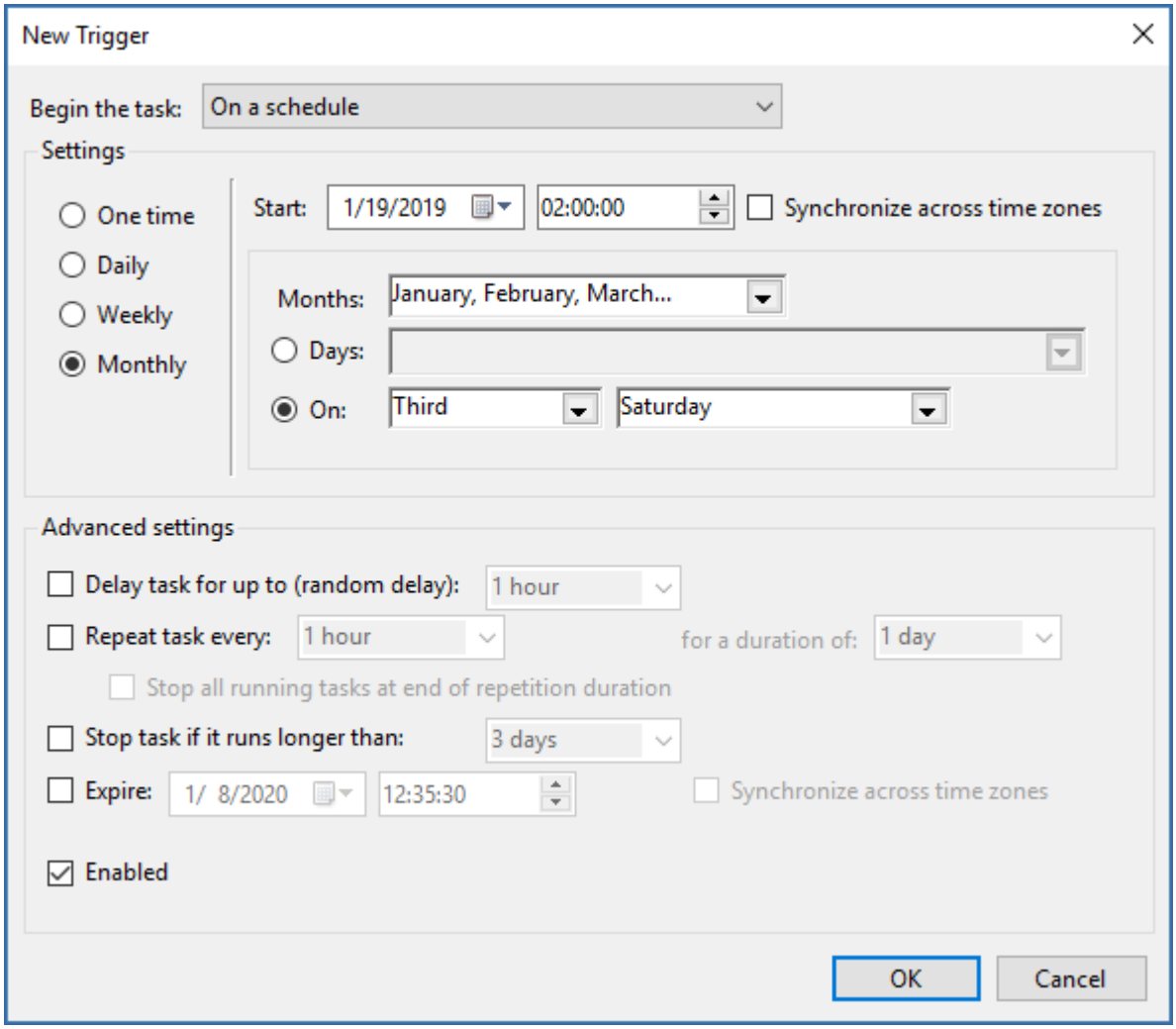
2. Klicken Sie mit der rechten Maus auf **Task Scheduler (lokal)** und wählen Sie **Task erstellen**.



3. Gehen Sie auf der Registerkarte **Allgemein** wie folgt vor:
   - Legen Sie den **Namen** und die **Beschreibung** fest.
   - Wählen Sie **Unabhängig von Anmeldung des Benutzers ausführen**.
   - Legen Sie das **Benutzerkonto** fest, mit dem der Task ausgeführt wird. Wir empfehlen, das NETZWERKDIENST-Konto der Maschine zu verwenden.

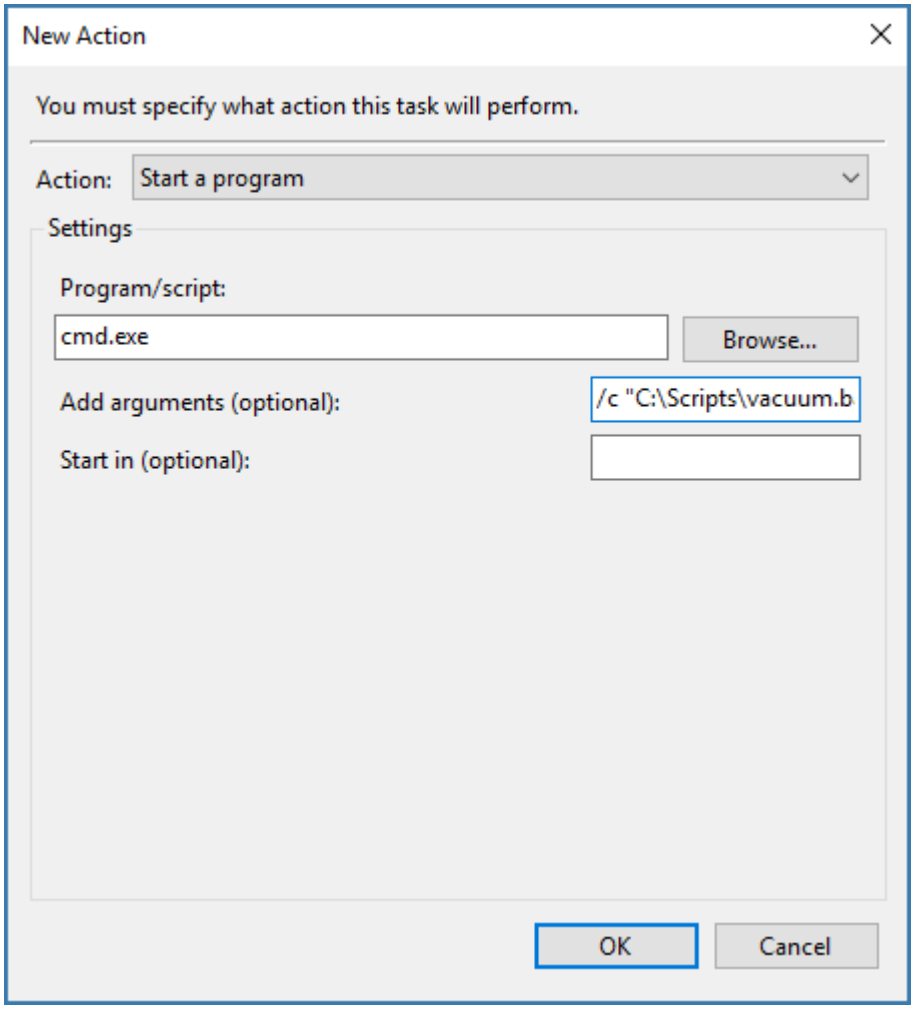


4. Gehen Sie in der Registerkarte **Auslöser** wie folgt vor:



- Klicken Sie auf **Neu** und legen Sie den Termin, an dem Sie die Bereinigung ausführen wollen, fest. Zu diesem Zeitpunkt sollte der Server wenig ausgelastet sein. Wir empfehlen, mindestens einmal im Monat eine Bereinigung durchzuführen.

5. Gehen Sie in der Registerkarte **Aktionen** wie folgt vor:



- Klicken Sie auf **Neu** und bei den **Aktionen** wählen Sie **Ein Programm starten**.
- Bei **Programm/Skript** geben Sie ein
- Bei **Argumente hinzufügen** geben Sie ein: **`/c "C:\Scripts\vacuum.bat"`**

Hinweis: *Stellen Sie sicher, dass Sie den Pfad in dieser Eingabe bearbeiten, damit der tatsächliche Pfad zu Ihrer vacuum.bat-Datei abgebildet wird.*

- Belassen Sie alle Standardeinstellungen für die Registerkarten **Bedingungen** und **Einstellungen**.
- Klicken Sie auf **OK**, um den neuen Task zu speichern Sie werden möglicherweise aufgefordert, ein Administratorenkennwort einzugeben.

Verifizieren Sie, dass der Task wie erwartet arbeitet.

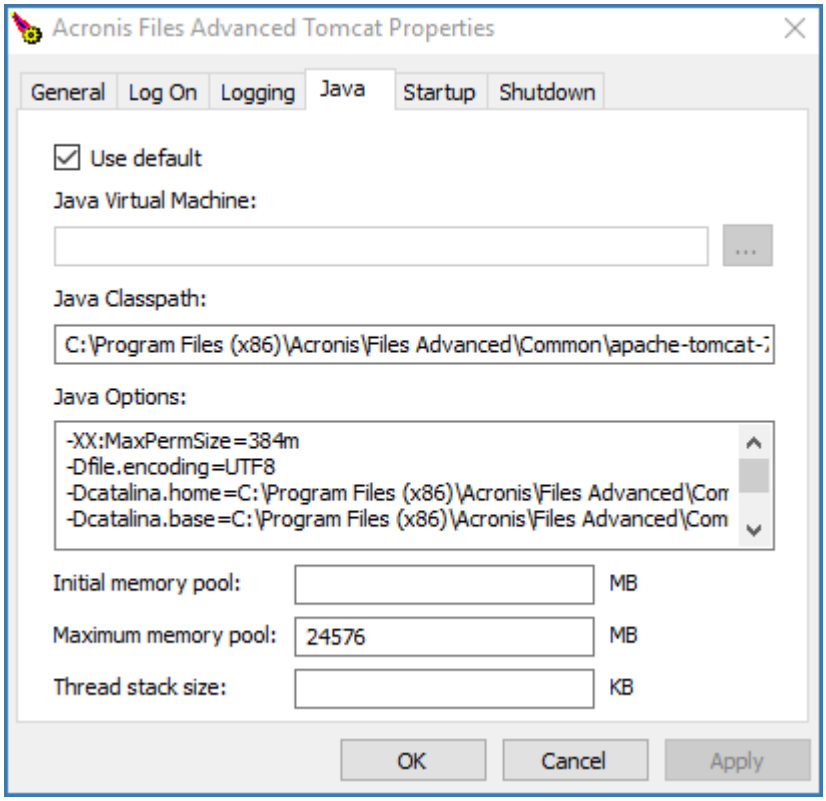
1. Führen Sie den Bereinigungs-Task zu Testzwecken manuell aus dem Task Scheduler heraus aus und stellen Sie sicher, dass die Log-Datei im richtigen Ordner abgelegt wird.
2. Überprüfen Sie, ob der Task zum geplanten Termin ausgeführt wird.

11.7 Maximalen Speicherpool für Java in Tomcat für Files Advanced erhöhen

Der Standardwert für den maximalen Speicherpool für Java in Files Advanced Tomcat beträgt bei einem 64-Bit-Betriebssystem 24 GB. Je nach Bereitstellung benötigen Sie einen größeren Pool.

So vergrößern Sie den maximalen Speicherpool:

1. Klicken Sie auf "Start" -> **Alle Programme** -> Files Advanced.
2. Klicken Sie auf die Option **Files Advanced 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 Files Advanced Tomcat-Dienst neu.

11.8 Files Advanced zu einem anderen Server migrieren

Diese Anleitung unterstützt Sie dabei, Ihre vorhandene Files Advanced-Einrichtung auf andere Computer zu verschieben.

Es wird dringend empfohlen, vor der Migration des Produktionsservers die entsprechenden Schritte in einer Testumgebung auszuführen. Die Testbereitstellung muss dieselbe Architektur wie die Produktionsserver aufweisen und über einige Desktop und Mobile Clients für Testbenutzer verfügen, damit die Kompatibilität in der Produktionsumgebung sichergestellt ist.

Themen

11.8.1 Vor Beginn

Hinweis: Es wird dringend empfohlen, das Backup/die Wiederherstellung außerhalb der Produktionsumgebung zu testen.

Wichtige Punkte zu Ihrer aktuellen Konfiguration, die Sie beachten bzw. notieren sollten:

- Befinden sich der Files Advanced Web Server, Postgres, das Gateway und das Datei-Repository auf demselben Computer?
- Notieren Sie sich den DNS-Namen, die IP-Adresse und den Port des Files Advanced Web Servers.
- Notieren Sie sich den DNS-Namen, die IP-Adresse und den Port des Gateway Servers.
- Notieren Sie sich die Adresse und den Port des Datei-Repositorys.
- Notieren Sie sich den Ort des Dateispeichers.
- Notieren Sie sich die Nummer der PostgreSQL-Version Ihres aktuelles Servers.

  Diese Nummer ermitteln Sie am einfachsten anhand des Ordners im PostgreSQL-Hauptordner (standardmäßig **`C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL`**), der Ordnername ist die PostgreSQL-Hauptversionsnummer (z.B. **9.2**; **9.3**; **9.4**).

Viele dieser Informationen finden Sie im Konfigurationswerkzeug.

Grundlegender Ablauf des Migrationsvorgangs:

Stellen Sie vor der Migration sicher, dass Sie alle nachfolgenden Schritte ausführen können.

1. Ändern Sie die DNS-Einträge, sodass sie auf den neuen Servercomputer verweisen.
2. Erstellen Sie ein Backup Ihrer aktuellen Datenbankdateien und Zertifikate.
3. Verschieben Sie die Datenbankdateien und Zertifikate auf den neuen Computer.
4. Migrieren Sie den Dateispeicher.
5. Installieren Sie Files Advanced Web Server auf dem neuen Computer.
6. Verschieben Sie die Zertifikate auf den neuen Computer.
7. Verschieben Sie die Datenbankdateien in die neue Installation des Files Advanced Web Servers.
8. Starten Sie den neuen Files Advanced Web Server über das Konfigurationswerkzeug.
9. Bestätigen Sie, dass die Adresse von Files Advanced Mobile Gateway korrekt ist.
10. Testen Sie die neue Konfiguration.

11.8.2 Files Advanced Web Server- und Gateway-Datenbanken migrieren

Gehen Sie auf dem ursprünglichen Server, auf dem Tomcat/Gateway/PostgreSQL aktuell ausgeführt werden, wie folgt vor:

Hinweis: *Wenn die Server-Datenbank von Files Advanced Web Server sehr groß ist (mehrere Gigabyte), empfiehlt sich möglicherweise eine andere Methode für das Backup und die Wiederherstellung der Datenbank. Für Unterstützung und Anweisungen steht unser technischer Support unter https://www.acronis.de/mobilitysupport/ https://support.acronis.com/mobility zur Verfügung.*

1. Stoppen Sie den Files Advanced Tomcat-Dienst.
2. Öffnen Sie die PostgreSQL Administratorapplikation von Files Advanced und stellen Sie eine Verbindung zum Datenbankserver her. Sie werden ggf. aufgefordert, das Kennwort für den **`postgres`** Benutzer einzugeben.
3. Erweitern Sie **Datenbanken** und klicken Sie mit der rechten Maustaste auf die Datenbank **acronisaccess_production**.
4. Wählen Sie **Wartung** und das Aktionsfeld **Bereinigen** und aktivieren Sie dann das Kästchen **ANALYSIEREN**. Wählen Sie **OK**.
5. Erweitern Sie die Datenbank und dann **Schemas** und **Öffentlich**. Notieren Sie die Anzahl im Abschnitt **Tabellen**. Dies kann Ihnen bei der Überprüfung helfen, ob die Datenbankwiederherstellung nach einem Recovery erfolgreich war.
6. Schließen Sie die PostgreSQL-Administratorapplikation und öffnen Sie eine Eingabeaufforderung mit erweiterten Benutzerrechten.
7. Navigieren Sie in der Eingabeaufforderung zum PostgreSQL-Verzeichnis 'bin'.

   Beispiel: **`cd "C:\Program Files(x86)\Acronis\Access\Common\PostgreSQL\9.3\bin"`**
8. Geben Sie den folgenden Befehl ein: **`pg_dumpall --host localhost --port 5432 --username postgres --file alldbs.sql`**
   - **`alldbs.sql`** ist der Dateiname des Backups. Es wird im PostgreSQL-Verzeichnis 'bin' gespeichert. Sie können mit dem obigem Befehl auch einen anderen Pfad zum Speichern des Backups eingeben – ändern Sie z.B. den letzten Teil des obigen Befehls wie folgt: **`--file D:\Backups\alldbs.sql`**
   - Wenn Sie nicht den Standard-Port verwenden, müssen Sie statt **`5432`** die richtige Portnummer eingeben.
   - Wenn Sie nicht das Standard-Administratorkonto von PSQL, **`postgres`**, verwenden, muss im obigen Befehl **`postgres`** durch den Namen des Administratorkontos ersetzt werden.
   - Während dieses Vorgangs werden Sie mehrmals aufgefordert, das **`postgres`** -Kennwort des Benutzers einzugeben. Geben Sie bei jeder Aufforderung das Kennwort ein und drücken Sie die Eingabetaste.
   - **Hinweis:** Die Eingabe des Kennworts bewirkt keine sichtbaren Änderungen im Fester mit der Eingabeaufforderung.
9. Kopieren Sie die Backup-Datei auf den neuen Computer, auf dem der Access Server gehostet werden soll.
10. Kopieren Sie die Zertifikate, die Sie für den Access Server verwenden, auf den neuen Computer.
11. Sofern Sie den Dateispeicher migrieren möchten, kopieren Sie die entsprechenden Dateien herüber. Bei einem großen Dateispeicher kann dies etwas länger dauern. Weitere Informationen finden Sie unter FileStore an einen anderen Speicherort verschieben (S. 246).

Backup der Gateway Server-Datenbank

1. Stoppen Sie den **Acronis Access Gateway**-Dienst.
2. Wechseln Sie zum Datenbankordner des Gateway Servers. Sie finden ihn standardmäßig an folgendem Speicherort:

   `C:\Program Files (x86)\Acronis\Access\Gateway Server\database`
3. Kopieren Sie die Datei **`mobilEcho.sqlite3`** auf den neuen Computer, auf dem der Gateway Server gehostet werden soll.

Wenn Sie Änderungen an den nachfolgenden Dateien vorgenommen haben, wird empfohlen, Backups zu erstellen, damit Sie Ihre Einstellungen beim Wiederherstellen oder Migrieren des Produkts Files Advanced übernehmen können.

- Die Datei **`postgresql.conf`**, da diese wichtige Einstellungen enthalten kann, die für Ihre Datenbank relevant sind. Sie befindet sich in der Regel unter **`C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL\<version>\Data`**.
- Datei: **`web.xml`**. Standardspeicherort: **`C:\Program Files (x86)\Acronis\Files Advanced\Access Server\Web Application\WEB-INF\`**. Enthält Einstellungen für die Einzelanmeldung (Single Sign-On).
- Datei: **`server.xml`**. Standardspeicherort: **`C:\Program Files (x86)\Acronis\Files Advanced\Common\apache-tomcat-<version>\conf`**. Enthält Einstellungen für Tomcat.
- Datei: **`krb5.conf`**. Standardspeicherort: **`C:\Program Files (x86)\Acronis\Files Advanced\Common\apache-tomcat-<version>\conf`**. Enthält Einstellungen für die Einzelanmeldung (Single Sign-On).
- Datei: **`login.conf`**. Standardspeicherort: **`C:\Program Files (x86)\Acronis\Files Advanced\Common\apache-tomcat-<version>\conf`**.
- Ihre für Files Advanced verwendeten Zertifikate und Schlüssel.
- Datei: **`acronisaccess.cfg`**. Standardspeicherort: **`C:\Program Files (x86)\Acronis\Files Advanced\Access Server`**.
- Benutzerdefinierte Farbschemas. Standardspeicherort: **`C:\Program Files (x86)\Acronis\Files Advanced\Access Server\Web Application\customizations\`**.
- Datei: **`pg_hba.conf`**. Standardspeicherort: **`C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL\<version>\Data`**.
- Datei: **`newrelic.yml`** . Wenn Sie den Files Advanced Server mit **New Relic** überwachen.

Gehen Sie auf dem neuen Server, auf dem der Files Advanced-Server gehostet werden soll, wie folgt vor:

Files Advanced installieren

1. Starten Sie das Installationsprogramm von Files Advanced Advanced und klicken Sie auf **Weiter**. Lesen und akzeptieren Sie die Lizenzvereinbarung.
2. Wählen Sie **Installieren** aus, und durchlaufen Sie die Bildschirme des Installationsprogramms.

   Hinweis: *Wenn der Files Advanced Web Server, PostgreSQL und das Gateway auf separaten Computern installiert werden sollen, klicken Sie auf* ***Benutzerdef.*** *, und wählen Sie die gewünschten Komponenten aus.*

3. Geben Sie auf der Seite 'PostgreSQL-Konfiguration' das Kennwort für den PostgreSQL-Superuser ein, das auch auf dem ursprünglichen Server verwendet wurde. Klicken Sie auf **Weiter**.
4. Überprüfen Sie die zu installierenden Komponenten, und klicken Sie auf **Installieren**.
5. Klicken Sie nach Abschluss des Installationsprogramms auf **Beenden**. Daraufhin wird ein Dialogfeld mit der Information angezeigt, dass als Nächstes das Konfigurationswerkzeug ausgeführt wird.
6. Wenn das Konfigurationswerkzeug geöffnet wird, lassen Sie es geöffnet, ohne auf **OK** oder **Anwenden** zu klicken.

1. Öffnen Sie die Systemsteuerung **Dienste** und stoppen Sie den Tomcat-Dienst von Files Advanced.

   Hinweis: *Halten Sie für Lastenausgleichskonfigurationen alle Files Advanced Tomcat-Dienste an.*

2. Öffnen Sie die PostgreSQL-Administrator-Applikation von Files Advanced und stellen Sie eine Verbindung mit dem lokalen Datenbankserver her. Wählen Sie **Datenbanken** aus und vergewissern Sie sich, dass eine Datenbank mit dem Namen **`acronisaccess_production`** vorhanden ist.
3. Klicken Sie mit der rechten Maustaste auf die Datenbank, und wählen Sie **Aktualisieren**.
4. Erweitern Sie diese, und erweitern Sie **Schemas**. Erweitern Sie **Öffentlich**, und vergewissern Sie sich, dass keine (0) **Tabellen** vorhanden sind.
   - Sind Tabellen in der Datenbank enthalten, klicken Sie mit der rechten Maustaste auf die Datenbank, und benennen Sie sie um in **`oldacronisaccess_production`**. Gehen Sie abschließend zu **Datenbanken**, klicken Sie mit der rechten Maustaste, und erstellen Sie eine neue Datenbank mit dem Namen **`acronisaccess_production`**.
5. Schließen Sie die PostgreSQL-Administratorapplikation und öffnen Sie eine Eingabeaufforderung mit erweiterten Benutzerrechten.
6. Navigieren Sie in der Eingabeaufforderung zum PostgreSQL-Verzeichnis 'bin'.

   Beispiel: `cd "C:\Program Files\Acronis\Access\Common\PostgreSQL\9.3\bin"`
7. Kopieren Sie die Datenbank-Backupdatei **`alldbs.sql`** (oder den von Ihnen dafür verwendeten Namen) in das Verzeichnis **bin** .
8. Geben Sie in der Eingabeaufforderung den folgenden Befehl ein: **`psql -U postgres -f alldbs.sql`**
9. Geben Sie Ihr **`postgres`** Kennwort ein, wenn Sie dazu aufgefordert werden.

   Hinweis: *Je nachdem, wie groß Ihre Datenbank ist, kann die Wiederherstellung einige Zeit dauern.*

10. Schließen Sie das Fenster mit der Eingabeaufforderung, wenn die Wiederherstellung beendet ist.
11. Öffnen Sie die **PostgreSQL-Administrator-Applikation von Files Advanced** erneut, und stellen Sie eine Verbindung mit dem Datenbankserver her.
12. Wählen Sie **Datenbanken** aus.
13. Erweitern Sie die **`acronisaccess_production`** -Datenbank und dann **Schemata** und **Öffentlich**. Überprüfen Sie, ob die Anzahl der **Tabellen** der Anzahl auf dem ursprünglichen Server entspricht.

    Hinweis: *Wenn die Files Advanced Web Server-Version, in der Sie die Datenbank wiederherstellen, neuer ist als die Files Advanced Web Server-Version aus Ihrer Datenbanksicherung und der Tomcat-Dienst von Files Advanced bereits gestartet wurde, könnte die Anzahl der Tabellen in der neuen Files Advanced Web Server-Datenbank größer sein als die Anzahl, über die Sie während der Durchführung der Sicherung verfügten.*

Gateway Server-Datenbank wiederherstellen

1. Kopieren Sie die Gateway Server-Datenbank **`mobliEcho.sqlite3`** des alten Servers in den Datenbankordner des neuen Gateway Servers (standardmäßig **`C:\Program Files (x86)\Acronis\Files Advanced\Gateway Server\database`**), und ersetzen Sie damit die vorhandene Datei.

Neuen Server konfigurieren

Hinweis: *Es wird dringend empfohlen, die von Files Advanced verwendeten DNS-Namen nicht zu ändern, sondern nur die IP-Adressen, auf die sie verweisen. In den folgenden Anweisungen wird davon ausgegangen, dass Sie die DNS-Namen der früheren Instanz von Files Advanced weiterverwenden.*

1. Wechseln Sie zurück zum noch geöffneten Konfigurationsdienstprogramm von Files Advanced und legen Sie die Einstellungen für den Gateway Server, den Files Advanced Web Server und das Datei-Repository fest.
2. Klicken Sie auf **Anwenden** und dann auf **OK**. Klicken Sie im nächsten Dialogfeld auf **OK**. Daraufhin wird in einem Browser die Weboberfläche von Files Advanced gestartet.
3. Melden Sie sich beim Access Server an.
4. Klicken Sie auf **Administration**. Navigieren Sie zur Seite **Mobiler Zugriff** -> **Gateway Server**.
5. Ihr Gateway Server sollte in der Liste der Gateway Server aufgeführt sein.
6. Wenn es sich bei der Adresse für Ihren Gateway Server um einen DNS-Eintrag handelt, müssen Sie keine Änderungen für den Server vornehmen, sofern der DNS-Eintrag auf den neuen Server-Computer verweist. Handelt es sich bei der Adresse für Ihren Gateway um eine IP-Adresse, müssen Sie den Gateway Server ändern.

Administrationseinstellungen von Files Advanced überprüfen

Nach erfolgreicher Wiederherstellung der Datenbank wird Folgendes dringend empfohlen, bevor Sie weitere Schritte ausführen: Melden Sie sich bei der Weboberfläche an und vergewissern Sie sich, dass Ihre Einstellungen übernommen wurden und immer noch relevant sind. Dazu einige Beispiele wichtiger Elemente, die unbedingt geprüft werden müssen:

- Überwachungsprotokollierung – Prüfen Sie, ob der neue Ordner für Files Advanced Protokolle über alle benötigten Berechtigungen verfügt, sodass Protokolle geschrieben werden können.
- New Relic – Wenn Sie mit 'New Relic' arbeiten, kopieren Sie die Datei **`newrelic.yml`** vom alten Computer auf diesen Computer und vergewissern sich, dass der Pfad in der Weboberfläche von Files Advanced auf diese Datei verweist.
- Administrationseinstellungen – Vergewissern Sie sich, dass alle LDAP-, SMTP- und allgemeinen Administrationseinstellungen korrekt sind.
- Gateway Server und Datenquellen – Vergewissern Sie sich, dass alle Ihre Gateway Server weiterhin unter den korrekten Adressen erreichbar sind und alle Ihre Datenquellen gültige Pfade haben.

11.8.3 Neue Konfiguration testen

Vergewissern Sie sich nach der Einrichtung des neuen Servers, dass alles funktioniert, indem Sie einige einfache Aktionen ausführen:

- Navigieren Sie durch die Weboberfläche, und überprüfen Sie, ob alles wie erwartet funktioniert. Überprüfen Sie, ob Ihre Einstellungen vorhanden sind und nicht geändert wurden.
- Laden Sie über die Weboberfläche eine Datei in den Bereich 'Sync & Share' hoch, und führen Sie den gleichen Schritt für ggf. eingerichtete Netzwerkknoten aus.
- Stellen Sie mit einer Desktop Client- und einer Mobile Client-Applikation eine Verbindung mit dem Server her.
- Laden Sie mit dem Desktop Client bzw. dem Mobile Client einige Dateien hoch und runter.

11.8.4 Ursprünglichen Server bereinigen

Wenn sichergestellt ist, dass der neue Server einwandfrei ausgeführt wird, und keine weitere Verwendung des alten Servers geplant ist, wird empfohlen, Files Advanced vom alten Computer zu deinstallieren.

Öffnen Sie das Installationsprogramm von Files Advanced, akzeptieren Sie die Lizenzvereinbarung, und klicken Sie auf 'Deinstallieren'. Wählen Sie alle Komponenten aus, und klicken Sie auf 'Deinstallieren'. Hierdurch werden alle Komponenten von Files Advanced vom Computer entfernt.

Hinweis: *Wenn Sie über kein Installationsprogramm von Files Advanced verfügen, öffnen Sie die Systemsteuerung und deinstallieren Sie die folgenden Komponenten: Files Advanced PostgreSQL Server, Files Advanced Gateway Server, Datei-Repository-Server (Files Advanced File Repository Server), Files Advanced Web Server, Konfigurations-Sammlungswerkzeug (Files Advanced Configuration Collection Tool), Konfigurationswerkzeug (Files Advanced Configuration Utility) und LibreOffice.*

- Beim PostgreSQL Server wird das zugehörige Verzeichnis **Daten** nicht automatisch entfernt. Entfernen Sie das gesamte PostgreSQL-Verzeichnis manuell. Sie finden es standardmäßig am folgenden Ort:**`C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL\`**

  *Hinweis: Sie müssen den Pfad bearbeiten, wenn Sie eine ältere oder eine benutzerdefinierte Installation verwenden (Beispiel: **`C:\Program Files\Acronis\Access\Common\PostgreSQL\`**).*

- Es empfiehlt sich auch. Java zu entfernen, das für den Access Server installiert wurde. Auch Java kann ebenfalls über die Systemsteuerung entfernt werden.

11.9 Durchführen eines PostgreSQL-Upgrades auf eine neuere Hauptversion

Mit Veröffentlichungen für Major PostgreSQL werden häufig neue Funktionen hinzugefügt, durch die einige der internen Arbeitsvorgänge von PostgreSQL verändert werden. Es gibt zwei Hauptmöglichkeiten für die Durchführung eines Upgrades Ihrer PSQL-Instanzen: Erstellen eines Speicherabbilds Ihrer kompletten Datenbank und Wiedereinfügen dieser Datenbank in die neue Instanz **`pg_dumpall`**) oder mit dem neuen Befehl **`pg_upgrade`**. Beide Methoden haben Ihre Vor- und Nachteile.

- Um die Integrität der Daten zu gewährleisten, ist es in der Regel am besten, mit **`pg_dumpall`** ein Speicherabbild der kompletten Datenbank zu erstellen und dieses dann in die neue Instanz zu integrieren, aber bei großen Datenbanken kann dieser Vorgang sehr lange dauern.
- **`pg_upgrade`** zu verwenden, geht um einiges schneller, als ein Speicherabbild der gesamten Datenbank zu erstellen, allerdings ist dies bei älteren Versionen von PSQL nicht möglich.

Warnung: *Da PostgreSQL ein Produkt eines Drittanbieters ist, kann Acronis nicht garantieren, dass diese Methoden bei allen Benutzern gleich funktionieren. Überprüfen Sie in der PostgreSQL-Dokumentation immer Ihre Version von PostgreSQL, bevor Sie etwas in Ihre Produktionsumgebung implementieren.*

Hinweis: *Bitte sehen Sie in der PostgreSQL-Dokumentation nach, wenn* ***pg_upgrade*** *für Ihre Version von PostgreSQL und die neue Version, die Sie verwenden möchten, verwendbar ist.*

Files Advanced unterstützt keine Versionen von Tomcat, Java und PostgreSQL, die neuer als die jedem Release beigefügten Versionen sind. Informationen zu einer bestimmten Version erhalten Sie vom Acronis Support.

Hinweis: *Es wird dringend empfohlen, das Upgrade außerhalb der Produktionsumgebung zu testen.*

Wichtige Punkte zu Ihrer aktuellen Konfiguration, die Sie beachten bzw. notieren sollten:

- Werden der Files Advanced Server und der PostgreSQL-Server auf dem gleichen Computer ausgeführt?
- Auf welchem Port wird PostgreSQL ausgeführt?
- An welchem Standort befindet sich Ihre aktuelle PostgreSQL-Installation? Sie können dies überprüfen, indem Sie das PostgreSQL-Administrationstool öffnen und auf die Datenbank acronisaccess_production klicken. Rechts unter Eigenschaften finden Sie die **Codierung** und den **Zeichentyp**.

  Achtung: *Stellen Sie sicher, dass Ihre neue PostgreSQL-Installation über die gleiche* ***Codierung*** *und den gleichen* ***Zeichentyp*** *verfügt, da das Upgrade ansonsten nicht erfolgreich durchgeführt werden kann.*

- Wie lautet der IP- bzw. DNS-Name des Computers, auf dem PostgreSQL ausgeführt wird?
- Wie lautet die PostgreSQL-Versionsnummer Ihres aktuelles Servers? Diese Nummer ermitteln Sie am einfachsten anhand des Ordners im PostgreSQL-Hauptordner (standardmäßig **`C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL`**), der Ordnername ist die PostgreSQL-Hauptversionsnummer (z.B. 9.2; 9.3; 9.4).
- Stellen Sie sicher, dass alle erforderlichen Berechtigungen im/in den Dateisystem(en) konfiguriert sind.
- Stellen Sie sicher, dass der Zugriff zwischen den beiden Instanzen über **`pg_hba.conf`** zugelassen wird. Dies ist sehr wichtig, wenn Ihre neue PostgreSQL-Instanz nicht auf dem gleichen Computer installiert ist.

Erstellen eines Speicherabbilds der Datenbank von der alten Instanz

Hinweis: *Es wird dringend empfohlen, das Backup/die Wiederherstellung außerhalb der Produktionsumgebung zu testen.*

1. Stoppen Sie den Files Advanced Tomcat-Dienst.
2. Stellen Sie sicher, dass die alte Instanz von PostgreSQL ausgeführt und die neue Instanz angehalten wird.
3. Öffnen Sie die PostgreSQL Administratorapplikation von Files Advanced und stellen Sie eine Verbindung zum Datenbankserver her. Sie werden ggf. aufgefordert, das Kennwort für den **`postgres`** Benutzer einzugeben.
4. Erweitern Sie **Datenbanken** und klicken Sie mit der rechten Maustaste auf die Datenbank **`acronisaccess_production`** .
5. Wählen Sie **Wartung** -> **Vacuum** aus und klicken Sie auf **OK**.
6. Erweitern Sie die Datenbank und dann **Schemas** und **Öffentlich**. Notieren Sie die Anzahl im Abschnitt **Tabellen**. Hieran können Sie später erkennen, ob der Datenbanktransfer erfolgreich war.
7. Schließen Sie die PostgreSQL-Administratorapplikation und öffnen Sie eine Eingabeaufforderung mit erweiterten Benutzerrechten.
8. Navigieren Sie in der Eingabeaufforderung zum PostgreSQL-Verzeichnis 'bin'.

Beispiel: **`cd "C:\Program Files(x86)\Acronis\Files Advanced\Common\PostgreSQL\9.3\bin"`**

9. Geben Sie den folgenden Befehl ein: **`pg_dumpall --host localhost --port 5432 --username postgres --file alldbs.sql`**
   - **`alldbs.sql`** ist der Dateiname des Backups. Es wird im PostgreSQL-Verzeichnis **`bin`** gespeichert. Sie können mit dem obigem Befehl auch einen anderen Pfad zum Speichern des Backups eingeben – ändern Sie z.B. den letzten Teil des obigen Befehls wie folgt: **`--file D:\Backups\alldbs.sql`**
   - Wenn Sie nicht den Standard-Port verwenden, müssen Sie statt **`5432`** die richtige Portnummer eingeben.
   - Wenn Sie nicht die Postgres des Standard-Administratorkontos von PSQL verwenden, müssen die Postgres im obigen Befehl durch den Namen des Administratorkontos ersetzt werden.
   - Während dieses Vorgangs werden Sie mehrmals aufgefordert, das **`postgres`** -Kennwort des Benutzers einzugeben. Geben Sie bei jeder Aufforderung das Kennwort ein und drücken Sie die **Eingabetaste**.

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

10. Wenn Sie festgestellt haben, dass das Speicherabbild vollständig erstellt wurde, halten Sie die alte Instanz von PostgreSQL an und starten Sie eine neue.

Einfügen der Datenbank in die neue Instanz

1. Stellen Sie sicher, dass die neue Instanz von PostgreSQL ausgeführt und die alte Instanz angehalten wird.
2. Öffnen Sie die PostgreSQL-Administrator-Applikation von Files Advanced und stellen Sie eine Verbindung mit dem lokalen Datenbankserver her. Wählen Sie **Datenbanken** aus, und prüfen Sie, ob eine Datenbank mit dem Namen **`acronisaccess_production`** vorhanden ist. Wenn die Datenbank nicht vorhanden ist, müssen Sie sie erstellen.
3. Klicken Sie mit der rechten Maustaste auf die Datenbank, und wählen Sie **Aktualisieren**.
4. Erweitern Sie diese, und erweitern Sie **Schemas**. Erweitern Sie **Öffentlich**, und vergewissern Sie sich, dass keine (0) **Tabellen** vorhanden sind.
5. Sind Tabellen in der Datenbank enthalten, klicken Sie mit der rechten Maustaste auf die Datenbank, und benennen Sie sie um in **`oldacronisaccess_production`**. Gehen Sie abschließend zu **Datenbanken**, klicken Sie mit der rechten Maustaste, und erstellen Sie eine neue Datenbank mit dem Namen **`acronisaccess_production`**.
6. Schließen Sie die PostgreSQL-Administratorapplikation und öffnen Sie eine Eingabeaufforderung mit erweiterten Benutzerrechten.
7. Kopieren Sie die Datenbank-Backupdatei **`alldbs.sql`** (oder den von Ihnen dafür verwendeten Namen) in das Verzeichnis 'bin' der neuen Instanz.
8. Navigieren Sie in der Eingabeaufforderung zum PostgreSQL-Verzeichnis **`bin`** .

   Beispiel: **`cd "C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL\9.3\bin"`**
9. Geben Sie den folgenden Befehl ein: **`psql -U postgres -f alldbs.sql`**
10. Geben Sie Ihr **`postgres`** Kennwort ein, wenn Sie dazu aufgefordert werden.

    Hinweis: *Je nachdem, wie groß Ihre Datenbank ist, kann die Wiederherstellung einige Zeit dauern.*

11. Schließen Sie das Fenster mit der Eingabeaufforderung, wenn die Wiederherstellung beendet ist.

Überprüfen Sie, ob die neue Instanz die richtige Datenbank enthält.

1. Öffnen Sie die PostgreSQL Administratorapplikation von Files Advanced und stellen Sie eine Verbindung zum neuen Datenbankserver her. Sie werden ggf. aufgefordert, das Kennwort für den **postgres** Benutzer einzugeben.
2. Erweitern Sie **Datenbanken** und klicken Sie mit der rechten Maustaste auf die Datenbank **acronisaccess_production** .
3. Erweitern Sie die Datenbank und dann **Schemas** und **Öffentlich**.
4. Überprüfen Sie, ob der Abschnitt **Tabellen** die gleiche Anzahl an Tabellen wie zuvor enthält.

Der Upgrade-Vorgang

1. Stoppen Sie den Files Advanced Tomcat-Dienst.
2. Stellen Sie sicher, dass beide Instanzen von PostgreSQl ausgeführt werden. Die neue Instanz wählt normalerweise einen anderen Port, wenn die alte Instanz auf dem Standard-Port ausgeführt wird.
3. Öffnen Sie die PostgreSQL Administratorapplikation von Files Advanced und stellen Sie eine Verbindung zum alten Datenbankserver her. Sie werden ggf. aufgefordert, das Kennwort für den **postgres** Benutzer einzugeben.
4. Erweitern Sie **Datenbanken**, erweitern Sie die Datenbank, erweitern Sie **Schemas** und erweitern Sie **Öffentlich**. Notieren Sie die Anzahl im Abschnitt **Tabellen**. Hieran können Sie später erkennen, ob der Datenbanktransfer erfolgreich war.
5. Schließen Sie den PostgreSQL-Administrator.
6. Stellen Sie sicher, dass beide PostgreSQL-Instanzen aufeinander zugreifen können. Dies können Sie tun, indem Sie überprüfen, ob die Datei **pg_hba.conf** über einen Eintrag für **localhost** (127.0.0.1/32) mit **Trust** als Authentifizierungsmethode verfügt.

   Hinweis: *Wenn es sich bei der neuen Instanz um eine andere Maschine handelt, müssen Sie den Zugriff auf diese Maschine konfigurieren.*

7. Öffnen Sie eine Eingabeaufforderung mit erweiterten Benutzerrechten und navigieren Sie mit dem Befehl **cd** zum neuen PostgreSQL-**bin** -Verzeichnis.

   Beispiel: **cd C:\Program Files(x86)\Acronis\Files Advanced\Common\PostgreSQL\9.5\bin**
8. Verwenden Sie den Befehl **pg_upgrade** mit den folgenden Paramentern:

   pg_upgrade -b <OLD_BIN_FOLDER> -B <NEW_BIN_FOLDER> -d <OLD_DATA_FOLDER> -D <NEW_DATA_FOLDER> -U postgres

   Hinweis: OLD_BIN_FOLDER *bezieht sich auf den bin-Ordner der PostgreSQL-Installation, für die Sie das Upgrade durchführen möchten. Das gleiche gilt für den Datenordner.*

   Hinweis: NEW_BIN_FOLDER *bezieht sich auf den bin-Ordner der neuen PostgreSQL-Installation. Das gleiche gilt für den Datenordner.*

Überprüfen Sie, ob die neue Instanz die richtige Datenbank enthält.

1. Öffnen Sie die PostgreSQL Administratorapplikation von Files Advanced und stellen Sie eine Verbindung zum neuen Datenbankserver her. Sie werden ggf. aufgefordert, das Kennwort für den **postgres** Benutzer einzugeben.

2. Erweitern Sie **Datenbanken** und klicken Sie mit der rechten Maustaste auf die Datenbank **`acronisaccess_production`** .
3. Wählen Sie **Wartung** -> **Vacuum** aus und klicken Sie auf **OK**.
4. Klicken Sie mit der rechten Maustaste erneut auf die **`acronisaccess_production`** -Datenbank.
5. Wählen Sie **Wartung** -> **Neu indizieren** aus und klicken Sie auf **OK**.
6. Erweitern Sie die Datenbank und dann **Schemas** und **Öffentlich**.
7. Überprüfen Sie, ob der Abschnitt **Tabellen** die gleiche Anzahl an Tabellen wie zuvor enthält.

12 Ergänzendes Material

Themen

12.1 In Konflikt stehende Software

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

- **VMware View™ Persona Management** – Diese Applikation verursacht Probleme mit dem Synchronisierungsprozess des Files Advanced-Desktop Clients und Probleme beim Löschen von Dateien. Wenn Sie den Files Advanced-Synchronisierungsordner außerhalb des **Persona Management-Benutzerprofils** platzieren, sollten die bekannten Konflikte sich vermeiden lassen.
- **Virenschutzprogramme** sollten keine Synchronisierungsordner prüfen, da dies zu Konflikten mit dem Synchronisierungsprozess führen kann. Es wird empfohlen, den Files Advanced FileStore-Ordner Ihrer Ignorieren-Liste oder White-Liste Ihres Virenschutzprogramms hinzuzufügen. Wenn Sie die Verschlüsselung nicht deaktiviert haben, werden alle im FileStore-Ordner enthaltenen Elemente verschlüsselt, und das Virenschutzprogramm kann nichts erkennen. Es kann jedoch zu Problemen mit einigen Elementen führen.

12.2 Für den Files Advanced Server

Themen

12.2.1 Integrieren von Microsoft Azure

Integrieren von Files Advanced in Microsoft Azure

Microsoft Azure bietet Enterprise-Kunden eine einfache Methode zur Bereitstellung ihrer bevorzugten Software in der Cloud mit umfangreichem Support verschiedener Betriebssysteme und Software, während Benutzer weiterhin überwacht werden können. Wenn Sie Files Advanced in Microsoft Azure integrieren, profitieren Sie auch ohne dedizierte physische Maschinen voll und ganz von den Vorteilen der Funktionen von Files Advanced. Das gesamte Produkt kann ohne Beeinträchtigung der Funktionalität innerhalb der Microsoft Azure-Cloud ausgeführt werden.

12.2.1.1 Vor Beginn

Sie müssen sicherstellen, dass einige wichtige Elemente bereits eingerichtet und betriebsbereit sind, bevor Sie Files Advanced installieren:

- Für das Erstellen der Azure Virtual Machine für die Bereitstellung von Files Advanced wird Windows Server 2012 R2 oder Windows Server 2008 R2 empfohlen.
- Ein virtuelles Netzwerk, das die virtuelle Maschine verwendet. Azure Verzeichnisdienste erfordern ein virtuelles Netzwerk **(klassisch)**, um zu funktionieren, und Sie müssen die virtuelle Maschine so konfigurieren, dass sie ein virtuelles Netzwerk **(klassisch)** nutzen kann.
- Sie benötigen die Gruppe 'AAD DC Administrators'. Falls Sie diese Gruppe noch nicht erstellt haben, müssen Sie sie nun erstellen. Die Benutzer in dieser Gruppen können Maschinen in die Domäne einbinden.
- In Azure muss ein Verzeichnisdienst ausgeführt werden, damit Sie die virtuelle Maschine, auf der Files Advanced ausgeführt wird, in das Azure Active-Verzeichnis einbinden können.

12.2.1.2 Verwalten des Azure Active-Verzeichnisdienstes

Erstellen der Gruppe 'AAD DC Administrators'

Erstellen Sie im Azure-Verwaltungsportal eine Gruppe mit dem Namen 'AAD DC Administrators' und fügen Sie alle Benutzer hinzu, die in der verwalteten Domain als Administrator fungieren sollen. Diese Administratoren können Maschinen zu der Domain hinzufügen und die Gruppenrichtlinie für die Domain konfigurieren.

12.2.1.3 Auswählen oder Erstellen des virtuellen Azure-Netzwerks

Wählen (oder erstellen) Sie das virtuelle Azure-Netzwerk, in dem die Azure AD-Domain-Dienste aktiviert werden sollen.

Wenn Sie die Azure AD-Domain-Dienste aktivieren, müssen Sie angeben, in welchem virtuellen Azure-Netzwerk die Domain-Dienste zur Verfügung gestellt werden sollen. Wählen Sie ein Netzwerk aus, das die folgenden Kriterien erfüllt:

- Azure Verzeichnisdienste erfordern ein virtuelles Netzwerk **(klassisch)**, um zu funktionieren.
- Das virtuelle Netzwerk gehört zu einer von den Azure AD Domain-Diensten unterstützten Region. Weitere Einzelheiten dazu finden Sie auf der Regionen-Seite.
- Stellen Sie sicher, dass das virtuelle Netzwerk ein regionales virtuelles Netzwerk ist und nicht die herkömmlichen Bezugsgruppen-Mechanismen verwendet.
- Stellen Sie sicher, dass die Arbeitslasten des Azure-Infrastrukturdienstes mit diesem virtuellen Netzwerk verbunden sind.

- Notieren Sie sich für später den Namen des virtuellen Netzwerkes.

12.2.1.4 Aktivieren der Azure AD Domänendienste für Ihren Azure AD-Mandanten

Die Aktivierung Ihrer Azure AD Domänendienste für Ihren Azure AD-Mandanten ist ganz einfach.

Hinweis: *Sie können auch Ihre Active Directory-Instanz mit* ***Azure AD Connect*** *synchronisieren. Weitere Informationen finden Sie im entsprechenden Abschnitt der Dokumentation für Microsoft Azure.*

Hinweis: *Stellen Sie bei Verwendung von Azure AD sicher, dass die Lizenzstufe Ihrer Benutzer* ***Online austauschen*** *umfasst (z.B. Office 365 Business Essentials), sodass Ihre Benutzer über eine gültige E-Mail-Adresse für ihr Konto verfügen. Für einige Files Advanced Funktionen ist eine gültige E-Mail-Adresse in der AD erforderlich.*

1. Navigieren Sie zum Azure AD-Mandanten und klicken Sie in Ihrem Verzeichnis auf die Registerkarte **Konfigurieren**. Dort befindet sich ein neuer Abschnitt mit der Bezeichnung **Domain-Dienste**.
2. Schalten Sie die Auswahl **Domain-Dienste für dieses Verzeichnis aktivieren** auf **Ja**, um weitere Konfigurationsoptionen anzuzeigen.
3. Geben Sie einen Domänennamen für die Domäne ein, die Sie mit den **Azure AD-Domänendiensten** erstellen. Sie können den voreingestellten Domänennamen (*.onmicrosoft.com) oder einen anderen der Domänennamen aus der Registerkarte 'Domains' Ihres Verzeichnisses wählen. Alternativ können Sie auch einen eigenen Domänennamen festlegen, indem Sie den Namen in das Textfeld eingeben.
4. Wählen Sie im Dropdown-Menü das virtuelle Netzwerk, in dem die **Domänendienste** zur Verfügung gestellt werden sollen.
5. Klicken Sie unten auf der Seite auf **Speichern**, wenn Sie fertig sind.
6. Die **Azure AD-Domänendienste** starten nun die Bereitstellung einer Domäne für Ihren Mandanten, und auf der Seite sollte der Status 'Ausstehend...' erscheinen. Die Domänendienste werden bereitgestellt und mit dem von Ihnen gewählten virtuellen Netzwerk verbunden.

   Hinweis: *Ein Neustart von* ***Domänendienste****, wenn Files Advanced konfigurierte wurde und über aktive Benutzer verfügt, ist nicht empfehlenswert, da der Files Advanced Server die inneren Abläufe der Azure-****Domänendienste*** *von Microsoft nicht berücksichtigen kann.*

7. Die IP-Adressen der **Azure AD-Domänendienste** werden auf der Seite angezeigt, sobald diese online gestellt werden. Die **Azure AD-Domänendienste** bieten eine hohe Verfügbarkeit, und es sollten zwei IP-Adressen angezeigt werden, sobald die Dienste vollständig für Ihre Domäne bereitgestellt wurden. Es kann 20 bis 30 Minuten dauern, bevor die erste IP-Adresse angezeigt wird, und weitere 20 bis 30 Minuten, bevor die zweite IP verfügbar ist.
8. Sie können nun die IP-Adressen und DNS-Server für das virtuelle Netzwerk festlegen, in dem Sie die Azure AD Domain-Dienste aktiviert haben. Auf diese Weise können virtuelle Maschinen innerhalb dieses virtuellen Netzwerkes die Domain 'sehen' und sich für einen Domain-Beitritt, für LDAP, für eine Authentifizierung usw. mit ihr verbinden,

Hinweis: *Wenn Sie weitere Informationen und Hilfe zu Active Directory benötigen, wenden Sie sich bitte an den technischen Support von Microsoft.*

12.2.1.5 Erstellen einer virtuellen Maschine von Files Advanced über den Azure Marketplace

Die einfachste Möglichkeit, mit einem Files Advanced-Abonnement zu beginnen, ist der Einsatz eines Image direkt vom Azure Marketplace. Das Image ist bei Files Advanced bereits installiert und Sie müssen es nur so konfigurieren, dass es Ihren Anforderungen an die Bereitstellung entspricht.

Erstellen einer virtuellen Maschine mit einem Files Advanced-Image

Erstellen der virtuellen Maschine:

1. Öffnen Sie das Azure Portal und melden Sie sich an.
2. Öffnen Sie die Registerkarte **Virtuelle Maschinen** und drücken Sie **Hinzufügen**.
3. Geben Sie **Files Advanced** im Suchfeld ein und drücken Sie die **Eingabetaste**.
4. Wählen Sie **Files Advanced Advanced**.
5. Drücken Sie **Erstellen**. Stellen Sie sicher, dass **Resource Manager** das **Bereitstellungsmodell** ist.

Konfigurieren der Einstellungen der virtuellen Maschine:

Hinweis: *All diese Einstellungen werden von Microsoft kontrolliert. Wenn Probleme auftreten sollten oder Sie einige der Optionen nicht verstehen, schlagen Sie in der Dokumentation zu Microsoft Azure nach oder kontaktieren Sie den Microsoft-Support.*

Grundlagen:

1. Geben Sie einen Namen für die virtuelle Maschine ein.
2. Wählen Sie einen Laufwerktyp – SSD oder HDD.
3. Geben Sie einen Benutzernamen und ein Kennwort für die virtuelle Maschine ein. Diese werden für die Verbindung zur virtuellen Maschine über den Remote-Desktop verwendet.
4. Bei **Abonnement** wählen Sie **Nutzungsbasierte Zahlung**.
5. Verwenden Sie entweder eine bestehende **Ressourcengruppe**, oder wählen Sie **Neu erstellen** und geben Sie einen Namen für die Gruppe ein.
6. Wählen Sie den **Standort**, der Ihrem geografischen Standort am nächsten ist. Dadurch verbessert sich die Leistung und die Verbindungsqualität.
7. Drücken Sie auf OK, wenn Sie mit den **Grundeinstellungen** zufrieden sind.

Größe:

Wählen Sie einen der empfohlenen Dimensionierungspläne. Wenn keiner der empfohlenen Pläne für Ihre Bereitstellung reicht, drücken Sie auf **Alle anzeigen**, und wählen Sie einen davon aus.

Hinweis: *Der Plan, den Sie wählen, sollte nicht kleiner als die empfohlenen Pläne sein! Weitere Information finden in den Files Advanced-Hardwareanforderungen (S. 23).*

Einstellungen:

- **Storage**
  - Wählen Sie ein bestehendes Storage-Konto oder erstellen Sie ein neues Konto.

- **Netzwerk**
  - Wählen Sie ein bestehendes virtuelles Netzwerk oder erstellen Sie ein neues virtuelles Netzwerk.
  - Wählen Sie ein Teilnetz für das virtuelle Netzwerk.
  - Legen Sie eine öffentliche IP-Adresse fest, wenn Sie wünschen, dass die virtuelle Maschine außerhalb des virtuellen Netzwerks zugänglich sein soll.
  - Wählen Sie eine Netzwerksicherheitsgruppe für die virtuelle Maschine.
- **Erweiterungen**
  - Fügen Sie beliebige Erweiterungen für die Azure-VM hinzu oder behalten Sie die Einstellung **Keine Erweiterungen** bei, wenn Sie mit Erweiterungen nicht vertraut sind.
- **Hohe Verfügbarkeit**
  - Wählen Sie die gewünschte Verfügbarkeitseinstellung, falls zutreffend.
- **Überwachung**
  - Deaktivieren oder aktivieren Sie die Diagnose für Ihre virtuelle Maschine.
  - Falls Sie Diagnosen verwenden, wählen Sie ein Diagnosespeicherkonto.

Prüfen Sie die Parameter und Abonnements der virtuellen Maschine. Wenn alles so ist, wie gewünscht, können Sie mit dem Erwerb fortfahren.

Files Advanced konfigurieren

1. Sobald die virtuelle Maschine erstellt wurde, können Sie sich dort anmelden. Nach der Anmeldung wird ein offener Browser mit der geöffneten Files Advanced-Konsole aufgerufen.
2. Wählen Sie ein Kennwort für das Administratorkonto.
3. Ihnen wird der Files Advanced-Installationsassistent angezeigt.

12.2.1.6 Files Advanced konfigurieren

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

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

Navigieren Sie mit dem DNS-Namen/der IP-Adresse der virtuellen Maschine und dem im Konfigurationsdienstprogramm angegebenen Port zur Files Advanced-Weboberfläche. Sie werden zum Einrichten des Kennworts für das Standard-Administratorkonto aufgefordert.

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

Den Prozess der Erstkonfiguration durchlaufen

Lizenzierung

- So starten Sie eine Testversion:
  a. Wählen Sie **Test starten** aus, geben Sie die erforderlichen Informationen ein und drücken Sie **Übermitteln**.
- So lizenzieren Sie den Server:
  a. Wählen Sie **Lizenzschlüssel eingeben**.
  b. Geben Sie Ihren Lizenzschlüssel ein, und aktivieren Sie das Kontrollkästchen.
  c. Drücken Sie **Speichern**.

Allgemeine Einstellungen

1. Geben Sie unter **Server-Name** einen Namen 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 die Standardsprache für das **Überwachungsprotokoll** aus.
5. Drücken Sie **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 Zeile **Von** in vom Server gesendeten E-Mails angezeigt wird.
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. Dies kann Ihr normaler Domänencontroller mit einem Active Directory-Server (der mit Azure synchronisiert wird) oder Ihr Azure-Domänencontroller sein.
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 Domäne ein (z.B. acronis\hristo).
6. Geben Sie die LDAP-Suchbasis ein.
7. Geben Sie die gewünschte(n) Domäne(n) 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. Drücken Sie **Speichern**.

Lokaler Gateway Server

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

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

Datei-Repository

1. Wählen Sie einen Dateispeichertyp aus. Verwenden Sie **Dateisystem** für einen Dateispeicher auf Ihren Computern und Acronis Storage S3, Swift S3, Ceph S3 oder Amazon S3 für einen Dateispeicher in der Cloud. Sie können andere Speicherdienste wählen, die mit S3 kompatibel sind, aber wird können deren Funktion nicht garantieren.
2. Geben Sie den DNS-Namen oder die IP-Adresse des Datei-Repository-Dienstes ein.

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

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

12.2.1.7 Öffnen der notwendigen Ports auf Azure

Damit Files Advanced auch von außerhalb des privaten virtuellen Netzwerkes erreichbar ist, müssen Sie einige **Endpunkte** einrichten.

1. Melden Sie sich bei Microsoft Azure an und öffnen Sie die Registerkarte 'Virtuelle Maschinen'. Wenn Sie sowohl virtuelle Maschinen als auch klassische virtuelle Maschinen verwenden, öffnen Sie die Registerkarte des entsprechenden Typs der virtuellen Maschine.
2. Klicken Sie auf die virtuelle Maschine, auf der sich Files Advanced befindet.
3. Wählen Sie im Menü **Einstellungen** auf der rechten Seite **Endpunkte** aus.
4. Klicken Sie auf **Hinzufügen**, geben Sie einen Namen für den Endpunkt ein und wählen Sie 'TCP' als Protokoll aus.
5. Geben Sie die Ports ein, die von Ihren Files Advanced Diensten verwendet werden. Für jeden Dienst wird jeweils ein Endpunkt benötigt. (Files Advanced Tomcat und Files Advanced Gateway). Files Advanced verwendet standardmäßig Port 443 für den Tomcat-Dienst und Port 3000 für den Gateway-Dienst.

12.2.1.8 Integrieren von SharePoint Online und OneDrive for Business

Files Advanced unterstützt sowohl SharePoint Online als auch OneDrive for Business. Wenn Sie diese Dienste integrieren möchten, müssen Sie sie als Datenquellen hinzufügen.

Hinzufügen von SharePoint Online als Datenquelle

1. Rufen Sie die Weboberfläche von Files Advanced auf und melden Sie sich als Administrator an.
2. Gehen Sie zur Registerkarte **Mobiler Zugriff** , und klicken Sie auf **Datenquellen**.
3. Drücken Sie auf **Neuen Ordner hinzufügen**.
4. Geben Sie einen Namen für den **Ordner** ein.
5. Wählen Sie den Gateway für die Verbindungen aus. In der Regel sollte es sich dabei um einen lokal installierten Gateway handeln.
6. Wählen Sie eine SharePoint-Website als **Datenstandort** aus geben Sie den Link für die SharePoint Online-Website Ihres Teams ein. Beispiel: **`https://company.sharepoint.com`**
7. Wählen Sie den **Sync**-Typ aus und legen Sie fest, ob der **Ordner** angezeigt werden soll, wenn eine Person den Server durchsucht.
8. Geben Sie den Namen der Benutzer/Gruppen ein und wählen Sie ihn aus, um diesen Benutzern/Gruppen den Ordner zuzuweisen.
9. Drücken Sie **Speichern**.
10. Wenn Sie eine **Datenquelle** für eine SharePoint-Bibliothek erstellen, müssen Sie die Felder 'URL' und 'Dokumentbibliotheksname' ausfüllen. Geben Sie in das Feld 'URL' die Adresse Ihrer SharePoint-Website oder -Unterwebsite und im Feld 'Dokumentbibliotheksname' den Namen Ihrer Bibliothek ein.

    Beispiel: **URL**: **`https://company.sharepoint.com:43222`**

    Beispiel: **Dokumentbibliotheksname**: **`Projects`**

Hinzufügen von OneDrive for Business als Datenquelle

Die Verfahrensweise ähnelt sehr der Verfahrensweise zum Hinzufügen eines SharePoint, doch da dieses Produkt für die persönliche Nutzung durch Mitarbeiter gedacht ist, gibt es keinen universellen

Link, der von allen verwendet werden kann. Sie müssen einen Platzhalter verwenden (%USERNAME%). Der Link, den Sie eingeben müssen, sieht folgendermaßen aus:

`https://YOURDOMAIN-my.sharepoint.com/personal/%USERNAME%_YOURDOMAIN_onmicrosoft_com`

Auf diese Weise wird eine Datenquelle erstellt, mit der alle Benutzer mit ihren eigenen OneDrive-Elementen in Files Advanced arbeiten können.

Hinweis: *Geben Sie die vollständige URL in das Feld SharePoint-Website ein; verwenden Sie nicht die Felder 'Unterpfad' oder 'Bibliothek'.*

Hinweis: *Das Gerät muss von Files Advanced verwaltet werden, das der Platzhalter ansonsten nicht funktioniert und Benutzer nicht auf OneDrive-Elemente zugreifen können.*

Wichtig ist auch zu wissen, dass Benutzer anderen Benutzern aufgrund der Verwendung des Platzhalters keinen Zugriff auf ihre Dateien gewähren können. Administratoren können eine Datenquelle für jeden einzelnen Benutzer erstellen und dann ggf. bestimmen, wer für wen Dateien freigeben kann.

12.2.2 Lastenausgleich für Files Advanced

Es gibt zwei Hauptmöglichkeiten für den Lastenausgleich von Files Advanced:

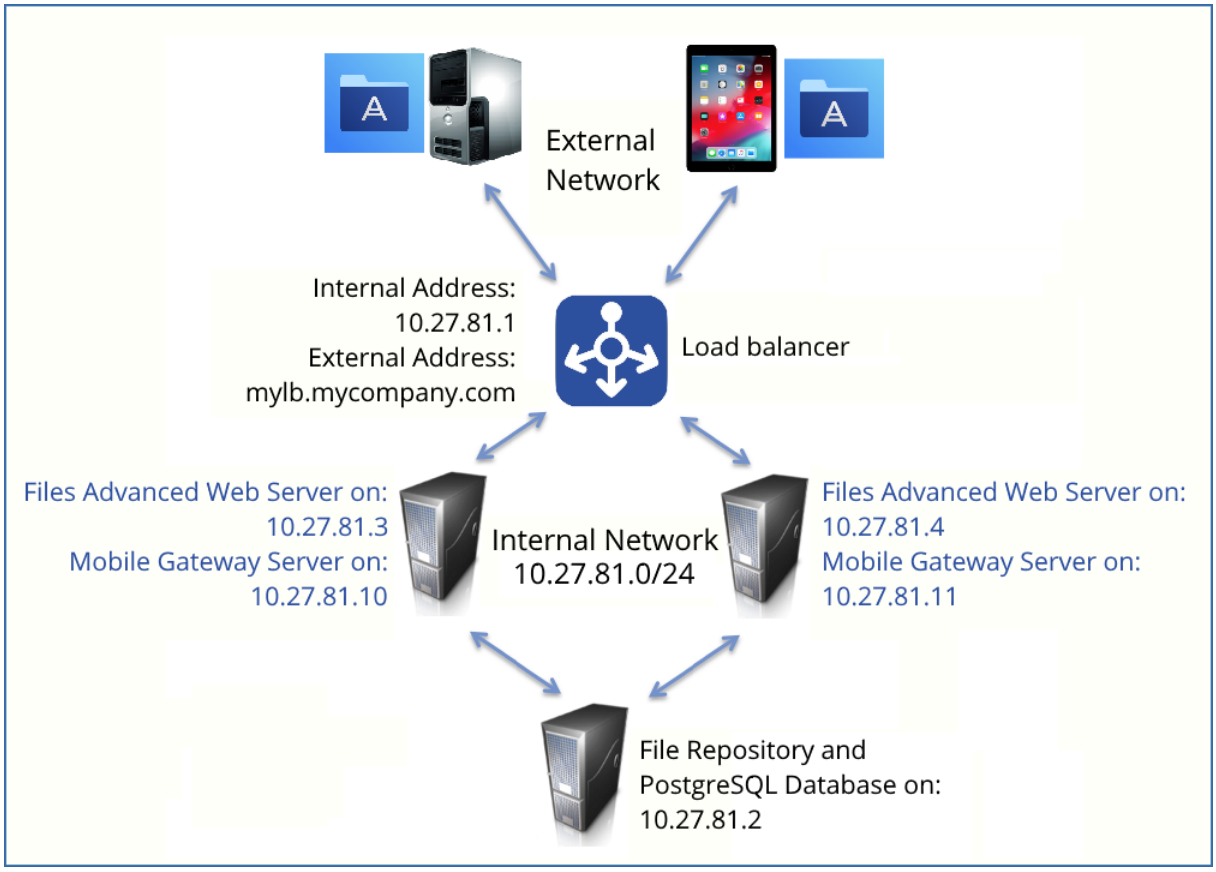
Lastenausgleich nur für Files Advanced Mobile Gateways vornehmen

Diese Konfiguration stellt sicher, dass für die Komponenten mit der höchsten Belastung (die Files Advanced Mobile Gateway Server) ein Lastenausgleich vorgenommen wird und sie für die mobilen Clients stets verfügbar sind. Der Files Advanced Server befindet sich nicht hinter dem Lastenausgleichsmodul, da er nicht benötigt wird, um für nicht verwalteten Zugriff eine Verbindung zu den Files Advanced Mobile Gateways herzustellen. Weitere Informationen finden Sie im Artikel Cluster-Gruppen (S. 99).

Lastenausgleich für alle Komponenten von Files Advanced vornehmen

Bei dieser Konfiguration wird ein Lastenausgleich für alle Komponenten von Files Advanced vorgenommen und hohe Verfügbarkeit für alle Benutzer gewährleistet. Um dieses Setup zu testen, benötigen Sie mindestens zwei getrennte Maschinen. Viele der Einstellungen beim Konfigurieren des Lastenausgleichs unterscheiden sich bei unterschiedlicher Soft- und Hardware. Daher werden sie in dieser Anleitung nicht behandelt.

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



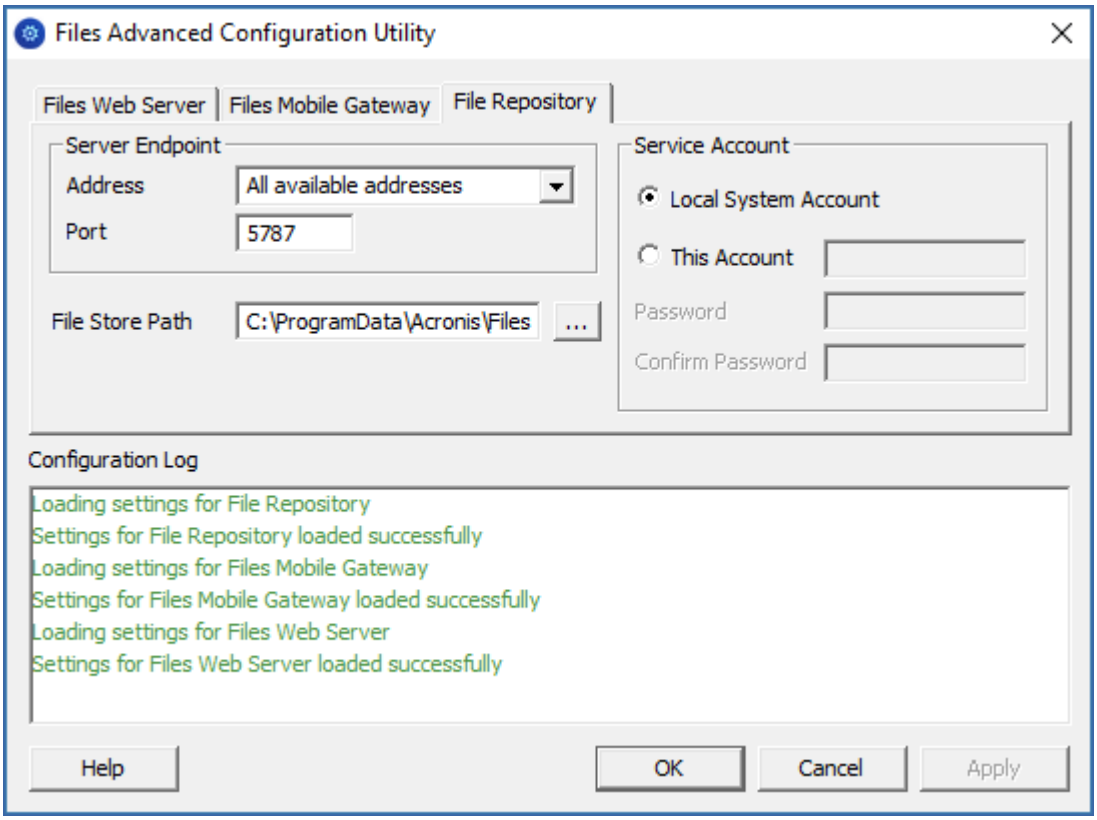
Diese Anleitung enthält alle notwendigen Details, um den Lastenausgleich für das Produkt Files Advanced in Ihrer Umgebung ordnungsgemäß vorzunehmen.

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

1. Starten Sie das Installationsprogramm von Files Advanced, und klicken Sie auf **Weiter**. Lesen und akzeptieren Sie die Lizenzvereinbarung.
2. Wählen Sie im Files Advanced-Installationsprogramm **Benutzerdefiniert**. Wählen Sie **Files Advanced Datei-Repository** und **PostgreSQL Database Server** aus, und klicken Sie auf **Weiter**.
3. Wählen Sie den Speicherort aus, an dem das Datei-Repository und das Konfigurationswerkzeug installiert werden sollen.
4. Wählen Sie den Speicherort aus, an dem PostgreSQL installiert werden soll, und geben Sie ein Kennwort für den Super-User **postgres** ein.
5. Öffnen Sie den TCP-Port 5432. Mit dessen Hilfe greifen Sie von den Remote-Maschinen aus auf die PostgreSQL-Datenbank zu.
6. Fahren Sie nach Abschluss des Installationsvorgangs mit dem Konfigurationswerkzeug (S. 28) fort.
   a. Sie werden aufgefordert, das Konfigurationswerkzeug zu öffnen. Drücken Sie **OK**.
   b. Wählen Sie die Adresse und den Port für den Zugriff auf das Datei-Repository aus.

Hinweis: *Sie müssen dieselbe Adresse und denselben Port in der Weboberfläche von Files Advanced festlegen. Weitere Informationen finden Sie in den Artikeln Das Konfigurationswerkzeug verwenden (S. 28) und Datei-Repository (S. 116).*

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



d. Klicken Sie auf **OK,** um die Änderungen zu übernehmen und schließen Sie das **Konfigurationswerkzeug**.

7. Navigieren Sie zum Installationsverzeichnis von PostgreSQL (z.B. **`C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL\<VERSION>\data\`**), und bearbeiten Sie **pg_hba.conf** mit einem Texteditor.

8. Beziehen Sie die Host-Einträge für alle Files Advanced Server unter Verwendung ihrer internen Adressen ein, und speichern Sie die Datei. Die Datei **pg_hba.conf** (HBA steht für host-basierte Authentifizierung) steuert die Client-Authentifizierung und wird im Datenverzeichnis des Datenbank-Clusters gespeichert. Darin geben Sie an, welche Server eine Verbindung herstellen dürfen und welche Berechtigungen sie haben sollen, z.B.:

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

9. Wenn Sie den Remote-Zugriff zu dieser PostgreSQL-Instanz aktivieren möchten, müssen Sie die **postgresql.conf**-Datei bearbeiten. Gehen Sie folgendermaßen vor:

a. Gehen Sie zu und öffnen Sie die Datei **postgresql.conf**. Der Ordner befindet sich standardmäßig unter: **`C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL\<VERSION>\Data\postgresql.conf`**

b. Finden Sie die Zeile **`#listen_addresses = 'localhost'`**

c. Aktivieren Sie diesen Befehl, indem Sie das **#**-Symbol am Beginn der Zeile entfernen.

d. Ersetzen Sie **`localhost`** mit *****, um an allen verfügbaren Adressen abzurufen. Wenn Sie PostgreSQL nur an einer bestimmten Adresse abrufen möchten, geben Sie die IP-Adresse statt ***** an.

- **z.B. `listen_addresses = '*'`** - Das bedeutet, dass PostgreSQL an allen verfügbaren Adressen abgerufen werden kann.
- **Beispiel: `listen_addresses = '192.168.1.1'`** – Das bedeutet, dass PostgreSQL nur an dieser Adresse abgerufen werden kann.

e. Speichern Sie alle Änderungen an **postgresql.conf**.

f. Starten Sie den Files Advanced PostgreSQL-Dienst neu.

10. Öffnen Sie das **Files Advanced PostgreSQL Administrator-Werkzeug** (PgAdmin). Sie finden es im Startmenü von Windows im Ordner von Files Advanced. Stellen Sie eine Verbindung zum lokalen Server her. Wählen Sie **Datenbanken** aus, und klicken Sie entweder mit der rechten Maustaste, oder wählen Sie **Neue Datenbank** im Menü **Bearbeiten** -> **Neues Objekt** aus, um eine neue Datenbank zu erstellen. Nennen Sie sie **acronisaccess_production**.

Hinweis: *PostgreSQL verwendet standardmäßig Port 5432. Stellen Sie sicher, dass dieser Port in jeder Firewall oder Routing-Software geöffnet ist.*

Gehen Sie auf den beiden Servern, die als Files Advanced Server und Files Advanced Gateways fungieren, wie folgt vor:

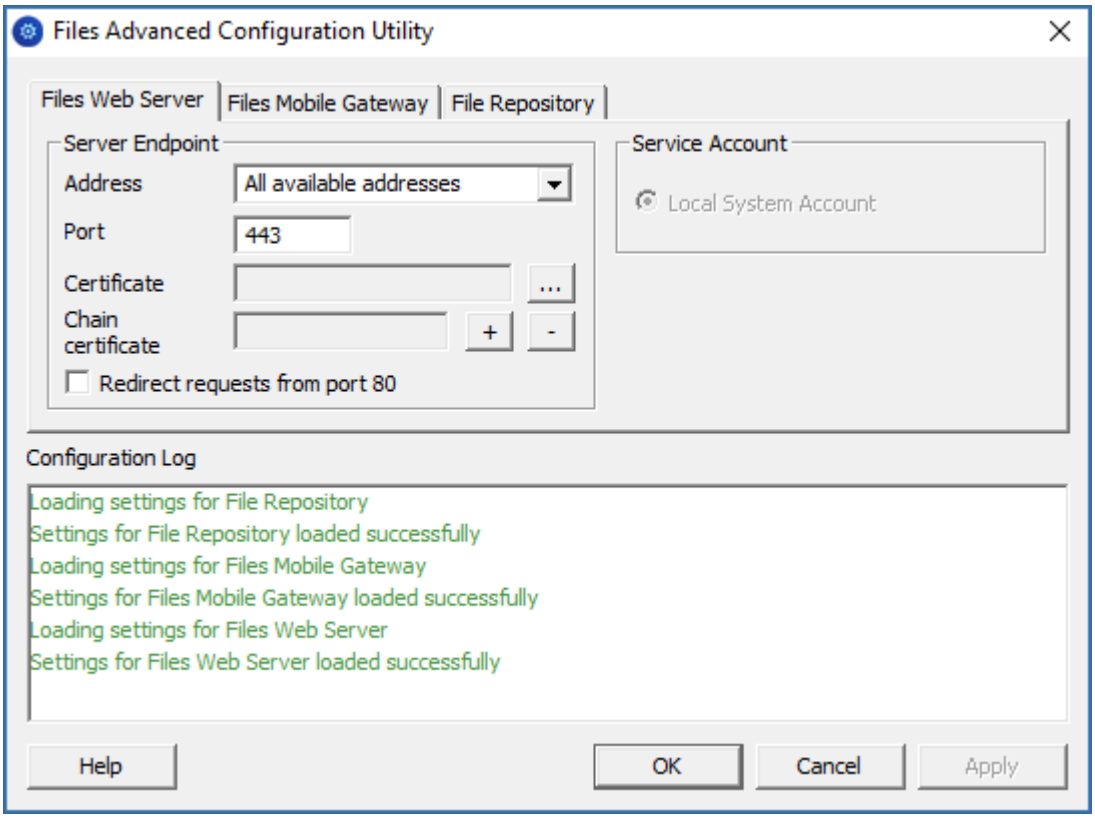
1. Starten Sie das Installationsprogramm von Files Advanced, und klicken Sie auf **Weiter**. Lesen und akzeptieren Sie die Lizenzvereinbarung.
2. Wählen Sie im Files Advanced-Installationsprogramm **Benutzerdefiniert**. Wählen Sie nur **Files Advanced Web Server** und **Files Advanced Mobile Gateway** aus, und fahren Sie mit dem Installationsvorgang fort.
3. Fahren Sie nach Abschluss des Installationsvorgangs mit dem Konfigurationswerkzeug (S. 28) fort.

   a. Sie werden aufgefordert, das Konfigurationswerkzeug zu öffnen. Drücken Sie **OK**.

   b. **Auf der Registerkarte 'Files Advanced Web Server':**

   - Geben Sie die Adresse und den Port für den Zugriff auf den Files Advanced Management Server ein (z.B. 10.27.81.3 und 10.27.81.4).
   - Wählen Sie das Zertifikat aus. Dabei sollte es sich um dasselbe SSL-Zertifikat handeln, das an die DNS-Adresse des Lastenausgleichsmoduls gebunden ist.
   - Klicken Sie auf **Anwenden**.

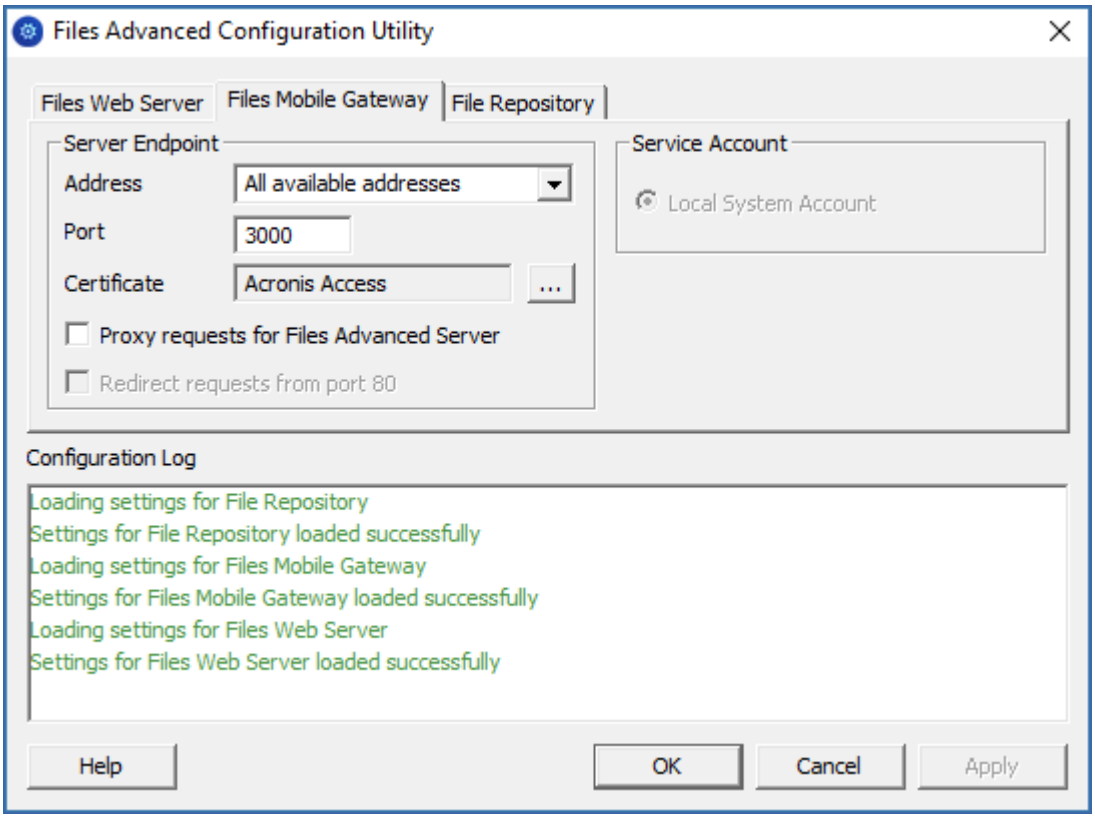
Hinweis: *Wenn Sie über kein Zertifikat verfügen, wird ein selbstsigniertes Zertifikat von Files Advanced erstellt. Dieses Zertifikat sollte NICHT in Produktionsumgebungen verwendet werden.*



c. **Auf der Registerkarte 'Files AdvancedMobile Gateway':**

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

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



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

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

6. Öffnen Sie Services.msc, und starten Sie die Files Advanced-Dienste neu.

Gehen Sie auf einem der Files Advanced Web Server und mobilen Files Advanced Gateways wie folgt vor:

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

1. Öffnen Sie Services.msc, und starten Sie den **Files Advanced Tomcat**-Dienst neu. Hierdurch wird die erstellte Datenbank gefüllt.

2. Öffnen Sie https://myaccess (d.h. https://10.27.81.3 oder https://10.27.81.4) in Ihrem Webbrowser und führen Sie den Installationsassistenten (S. 31) aus.
   a. **Auf der Registerkarte 'Lizenzierung':**
      - Geben Sie Ihren Lizenzschlüssel ein, aktivieren Sie das Kontrollkästchen, und klicken Sie auf **Fortsetzen**.
   b. **Auf der Registerkarte 'Allgemeine Einstellungen':**
      - Geben Sie einen Servernamen ein.
      - Die Webadresse sollte die externe Adresse des Lastenausgleichsmoduls sein (z.B. mylb.company.com). Wenn Sie nicht Port 443 verwenden, müssen Sie auch den Port eintragen.
      - Die Adresse für die Registrierung von Clients sollte die externe Adresse des Lastenausgleichsmoduls sein (z.B. mylb.company.com).
      - Wählen Sie das Farbschema aus.
      - Wählen Sie die Sprache für die Überwachungsprotokollnachrichten aus.
   c. **Auf der Registerkarte 'SMTP':**
      - Geben Sie den DNS-Namen oder die IP-Adresse Ihres SMTP-Servers ein.
      - Geben Sie den Port des SMTP-Servers ein.
      - Wenn Sie keine Zertifikate für den SMTP-Server verwenden, deaktivieren Sie **Sichere Verbindung verwenden?**.
      - Geben Sie den Namen ein, der in der 'Von'-Zeile von E-Mails angezeigt wird, die vom Server gesendet werden.
      - Geben Sie die Adresse ein, die als Absender der vom Server gesendeten E-Mails verwendet wird.
      - Falls Sie für den SMTP-Server eine Authentifizierung per Benutzername/Kennwort verwenden, aktivieren Sie 'SMTP-Authentifizierung verwenden?', und geben Sie Ihre Anmeldedaten ein.
      - Drücken Sie **Speichern**.
   d. **Auf der Registerkarte 'LDAP':**

*Markieren Sie **LDAP aktivieren**.*

      - Geben Sie den DNS-Namen oder die IP-Adresse des LDAP-Servers ein.
      - Geben Sie den Port des LDAP-Servers ein.
      - Falls Sie ein Zertifikat für Verbindungen mit dem LDAP-Server verwenden, markieren Sie **Sichere LDAP-Verbindung verwenden**.
      - Geben Sie Ihre LDAP-Anmeldedaten einschließlich der Domäne ein (beispielsweise mycompany\myname).
      - Geben Sie die LDAP-Suchbasis ein.
      - Geben Sie die gewünschte(n) Domäne(n) 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.)
      - Drücken Sie **Speichern**.
   e. **Auf der Registerkarte 'Lokales Gateway':**

Hinweis: *Wenn Sie einen Files Advanced Mobile Gateway und den Files Advanced Web Server auf derselben Maschine installieren, wird der Gateway Server automatisch erkannt und vom Files Advanced Web Server verwaltet.*

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

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

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

1. Nachdem Sie den Installationsassistenten abgeschlossen haben, klicken Sie auf **Fertig stellen** und navigieren zu **Mobiler Zugriff** -> **Gateway Server**.
2. Nun können Sie den zweiten Gateway Server registrieren:
   a. Geben Sie einen Anzeigenamen für das zweite Gateway ein.
   b. Die **Adresse für Administration** sollte eine interne Adresse hinter dem Lastenausgleichsmodul sein (z.B. 10.27.81.11).
   c. Geben Sie den **Administrationsschlüssel** ein. Diesen können Sie ermitteln, indem Sie auf der Maschine, auf der das hinzuzufügende Gateway installiert ist, zu https://mygateway:443 (d.h. https://10.27.81.10 oder https://10.27.81.11) navigieren. Dort wird der Schlüssel angezeigt. Weitere Informationen hierzu finden Sie im Artikel Neue Gateway Server registrieren (S. 89).
   d. Drücken Sie **Speichern**.
3. Erstellen Sie eine Cluster-Gruppe, und fügen Sie ihr alle Gateway Server hinzu. Der Primärserver sollte der Server sein, für den Sie bereits den Installationsassistenten ausgeführt haben. Weitere Informationen finden Sie im Artikel Cluster-Gruppen (S. 99).

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

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

Im Lastenausgleichsmodul:

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

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

12.2.3 Installieren von Files Advanced in einer Einrichtung mit Lastenausgleich

Diese Anleitung wird als allgemeine Übersicht zu den Anforderungen einer Einrichtung mit Lastenausgleich und den Prozessen für den Einsatz von Files Advanced in einer Umgebung mit Lastenausgleich bereitgestellt. Ihre Einrichtung kann gegebenenfalls von unserem Beispiel abweichen, jedoch sind Art und Weise, wie die Komponenten interagieren, gleich.

Die empfohlene Konfiguration besteht darin, alle Teile des Files Advanced Server auf verschiedene Computer zwischen den Lastenausgleichen aufzuteilen. Das Datei-Repository und der Dateispeicher können sich auf demselben Computer befinden.

Es wird dringend empfohlen, dass diese Schritte in einer Testumgebung durchgeführt werden. Die Testbereitstellung muss dieselbe Architektur wie die geplante Produktionseinrichtung aufweisen und über einige Desktop und Mobile Clients für Testbenutzer verfügen, damit die Kompatibilität in Ihrer Umgebung sichergestellt ist.

Themen

12.2.3.1 Systemanforderungen

Hardwareanforderungen

In einer Produktionsumgebung empfehlen wir Ihnen die Verwendung von mindestens drei (3) Files Advanced Tomcat Servern und drei (3) Gateway Servern, sodass bei Ausfall eines Servers weiterhin eine Lastenverteilung auf zwei aktive Server gewährleistet ist.

Hinweis: *Bei dieser vorgeschlagenen Einrichtung wird davon ausgegangen, dass diese Server auf einem Virtual Machine Server gehostet werden. Bei Verwendung von mehreren Server empfehlen wir die Verwendung von Interconnects mit geringer Latenz zwischen den Gast-Virtual Machines.*

- 1 Lastenausgleichsmodul für die Files Advanced Web Server.
- 1 Lastenausgleichsmodul für die Files Advanced Gateway Server.
- 3 Files Advanced Tomcat Server, jeweils mit 32 GB RAM und einer 16-Kern-CPU.
- 3 Files Advanced Gateway Server, jeweils mit 8 GB RAM und einer 4-Kern-CPU.

  Hinweis: *Für den Gateway Server sind Festplatten- und Netzwerkgeschwindigkeiten relevanter als CPU oder Speicher.*

- 1 PostgreSQL Server mit 32 GB RAM und einer 16-Kern-CPU.
- 1 Datei-Repository-Dienst + Dateispeicher. Die Parameter dieses Servers sind nicht besonders wichtig.

Netzwerkverbindungen

- Der Lastenausgleich für die Files Advanced Tomcat Server muss so konfiguriert werden, dass die DNS-Adresse des aktuellen Files Advanced Servers verwendet wird.
- Der Lastenausgleich für die Gateway Server muss so konfiguriert werden, dass die DNS-Adresse des aktuellen Gateway Servers verwendet wird.
- Der Tomcat Server muss mit dem Gateway Lastenausgleich verbunden werden, damit der Desktop-Netzwerkknoten synchronisiert wird und damit Netzwerkknoten an der Web-Schnittstelle durchsucht werden. In dieser geclusterten Einrichtung auf den Seiten der Files Advanced webUI Administration und Gateway Server ist 'Adresse für Client-Verbindungen' die Adresse des externen Lastenausgleichs. Für die Gateway Server verwenden wir auch die Einstellung 'Alternative Adresse für Files Advanced Server Verbindungen verwenden', und in 'Adresse für Files Advanced Web Server Verbindungen' ist die interne Adresse des Gateway Lastenausgleichs.
- Der Gateway Server muss mit dem Tomcat Lastenausgleich für die mobilen Client-Verbindungen verbunden werden.

Hinweis: *Für die Sync&Share-Datenquelle müssen Sie die Adresse zur Adresse des Tomcat Lastenausgleichs ändern.*

Installieren der PostgreSQL Server-Komponente

1. Starten Sie das Installationsprogramm von Files Advanced, und klicken Sie auf **Weiter**. Lesen und akzeptieren Sie die Lizenzvereinbarung.
2. Klicken Sie auf **Benutzerdefiniert** und wählen Sie nur den PostgreSQL Datenbank-Server aus. Klicken Sie auf **Weiter**.
3. Wählen Sie den Speicherort aus, an dem PostgreSQL installiert werden soll, geben Sie ein Kennwort für den Super-User **`postgres`** ein, und klicken Sie auf 'Weiter'.
4. Wählen Sie **Offener Port 5432 in der Firewall** aus. Sie verwenden diesen Port für den Fernzugriff auf die PostgreSQL-Datenbank.
5. Schließen Sie die Installation ab.

Herstellen der Verbindung durch Tomcat Server zulassen

1. Sobald die Installation abgeschlossen ist, navigieren Sie zum Ordner 'PostgreSQL **Daten**' (standardmäßig **`C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL\<version>\Data`**) und öffnen Sie **`pg_hba.conf`** mit einem Texteditor.
2. Beziehen Sie die Host-Einträge für Ihre Files Advanced Tomcat Server mittels ihrer internen Adressen ein und speichern Sie die Datei.

   Die**`pg_hba.conf`**-Datei (HBA steht für host-basierte Authentifizierung) steuert die Client-Authentifizierung und wird im Datenverzeichnis des Datenbank-Clusters gespeichert. Darin geben Sie an, welche Server eine Verbindung herstellen dürfen und welche Berechtigungen sie haben sollen, z.B.:

```
# TYPE DATABASE USER ADDRESS METHOD
# Loadbalancer1 (First Files Advanced & Gateway server)
host acronisaccess_production postgres 10.144.70.247/32 md5
```

*__Hinweis:__ In diesem Beispiel kann das Benutzerkonto mit der Bezeichnung **`postgres`** vom Server unter 10.144.70.247 eine Verbindung herstellen und mit vollständigen Berechtigungen auf die Datenbank **`acronisaccess_production`** (mit Ausnahme der Berechtigung **Replikation**) über eine **`md5 encrypted`** Verbindung zugreifen.*

Einstellen der korrekten Verbindungszahl

1. Suchen und ändern Sie **`max_connections`** zu **`510`**.
2. Entfernen Sie das vorangestellte **#** aus der folgenden Zeile: **`#listen_addresses = 'localhost'.`** Ersetzen Sie **`localhost`** durch **`*`**. Diese muss wie folgt aussehen: **`listen_addresses = '*'`**
3. Entfernen Sie das vorangestellte **#** aus der folgenden Zeile: **`#effective_cache_size = 128MB`** und ersetzen Sie **128MB** durch **12GB**. Diese muss wie folgt aussehen: **`effective_cache_size = 12GB`**
4. Ergänzen Sie den folgenden Hinweis: - **`#NOTE: this tuning setting assumes that PostgreSQL is running by itself on a #VM with at least 16 GB RAM. More information at #https://wiki.postgresql.org/wiki/Tuning_Your_PostgreSQL_Server`**
5. Speichern und schließen Sie die Datei **postgresql.conf**.
6. Starten Sie den Dienst Files Advanced PostgreSQL Server neu.

Nur den Files Advanced Web Server installieren

1. Starten Sie das Files Advanced Installationsprogramm und akzeptieren Sie die Lizenzvereinbarung.
2. Wählen Sie **Benutzerdefiniert** aus, und wählen Sie NUR den Files Advanced Tomcat Server aus.

   __Hinweis:__ Durch Anklicken des Tomcat Servers wird automatisch auch der PostgreSQL Server ausgewählt, Sie können ihn jedoch mit einem Klick deaktivieren.

3. Schließen Sie die Installation ab, und vergewissern Sie sich, dass der Files Advanced Tomcat-Dienst angehalten wurde.

Serverkonfiguration

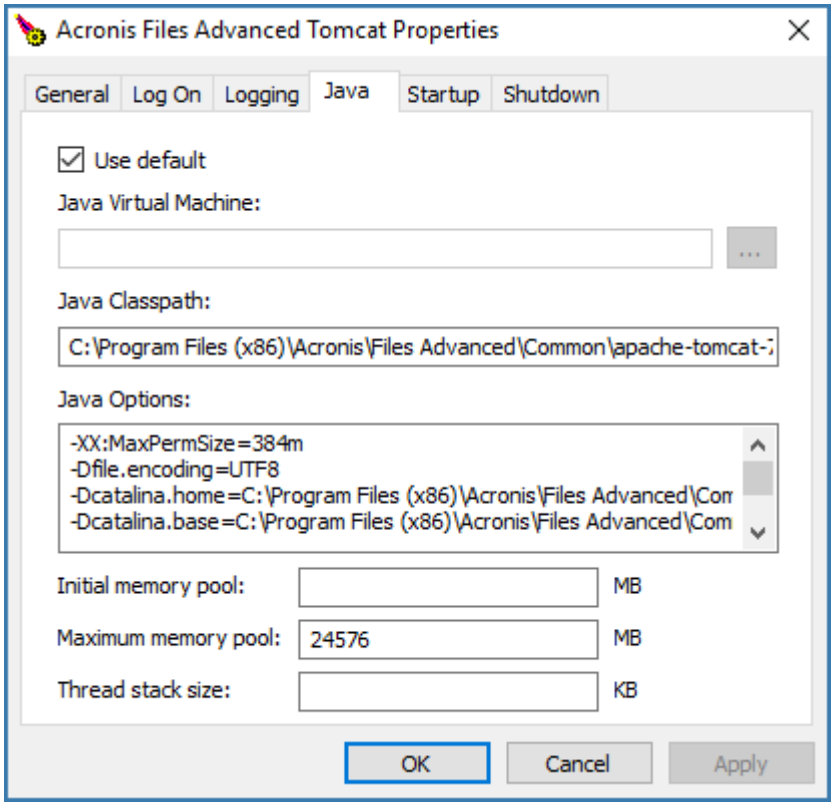
Alle Einstellungen, die Sie auf einem Files Advanced Web Server ändern, müssen auch auf allen anderen Files Advanced Web Servern geändert werden.

*__Hinweis:__ Vergessen Sie nicht, einen Eintrag in der Datei **`pg_hba.conf`** für jeden Files Advanced Web Server vorzunehmen!*

Konfigurieren der maximalen Speichernutzung von Tomcat

1. Starten Sie das Tool **Files Advanced Tomcat Service-Konfiguration** von Ihrem Desktop. Falls es sich nicht dort befindet, wechseln Sie zu **Start** –> **Alle Programme** –> **Files Advanced** und klicken Sie auf die Verknüpfung.
2. Klicken Sie auf die Registerkarte **Java**.

3. Erhöhen Sie die Einstellung '**Maximaler Speicherpool**' auf **24576** und klicken Sie auf **OK**.



Konfigurieren des Servers zur Verbindung mit der richtigen Datenbank

1. Navigieren Sie zum Ordner des Files Advanced Web Servers (Standard: **`C:\Program Files(x86)\Acronis\Files Advanced\Access Server`**), und öffnen Sie die Datei **`acronisaccess.cfg`** . Diese Datei teilt dem Server mit, wo sich der PostgreSQL Datenbankdienst befindet.
2. Stellen Sie diese Werte ein:

   `DB_HOSTNAME =10.144.70.248`

   `DB_PORT =5432`

   `DB_POOLSIZE =250`

   Hinweis: DB_HOSTNAME *ist die IP-Adresse, unter der PostgreSQL jetzt ausgeführt wird. In unserem Beispiel ist dies 10.144.70.248.*

   Hinweis: *Wir empfehlen,* ***DB_POOLSIZE*** *auf mindestens 250 einzustellen.*

3. Speichern Sie die Datei.

Konfigurieren der Maximalzahl an Threads

In einer Tomcat Einrichtung mit Lastenausgleich ist es wichtig, dass die Gesamtzahl aller Threads, die von allen Tomcat Instanzen erstellt werden können, nicht die Maximalzahl an Verbindungen überschreitet, für die die PostgreSQL Datenbank konfiguriert ist.

Dies wird von 3 wichtigen Einstellungen bestimmt:

- In der Datei **`acronisaccess.cfg`** : **`DB_POOLSIZE = 200`**. Es wird empfohlen, diesen Wert auf mindestens 250 einzustellen.

- In der Tomcat Datei **`server.xml`**: **`maxThreads = 150.`** Es wird empfohlen, diese Einstellung auf dem Standardwert von 150 zu belassen.
- In der Datei **`postgresql.conf`** : **`max_connections`**. Dies sollte bereits in den vorherigen Schritten konfiguriert worden sein. Es sollte nicht weniger als die Summe aller Tomcat DB_POOLSIZE Werte betragen, die für jeden Files AdvancedWeb Server eingestellt wurden + 10, zum Beispiel 510 für 2 Tomcat Server und 760 für 3 Tomcat Server usw.

Hinweis: *An dieser Datei vorgenommene Änderungen erfordern einen Neustart der entsprechenden Dienste.*

Konfigurieren einer ordnungsgemäßen Protokollierung

In einer Konfiguration mit Lastenausgleich ordnet der Files Advanced Tomcat Dienst nicht die richtigen IP-Adressen in den Protokollen zu. Zur Gewährleistung, dass alle Verbindungen richtig protokolliert werden, müssen Sie die folgenden Änderungen vornehmen:

1. Suchen Sie in der Datei server.xml nach der Zeile **`<Valve className=”org.apache.catalina.valves.AccessLogValve” directory=”logs” prefix=”localhost_access_log.” suffix=”.txt” pattern=”%h %l %u %t "%r" %s %b”/>.`**
2. Fügen Sie am Ende **`requestAttributesEnabled=”true”`** hinzu.
3. Ergänzen Sie unter derselben Zeile Folgendes:

   `<Valve className="org.apache.catalina.valves.RemoteIpValve" remoteIpHeader="X-Forwarded-For" protocolHeader="X-Forwarded-Proto"/>`
4. Speichern Sie die Datei und starten Sie den Files Advanced-Tomcat-Dienst anschließend neu.

Einen neuen Gateway Server installieren

1. Führen Sie auf einem neuen Computer das Files Advanced Installationsprogramm aus und akzeptieren Sie die Lizenzvereinbarung.
2. Wählen Sie **Benutzerdefiniert** und installieren Sie nur die Gateway Server-Komponente. Schließen Sie die Installation ab.
3. Legen Sie im Konfigurationswerkzeug Gateway-Adresse, Port und Zertifikat fest. Dabei sollte es sich um dasselbe SSL-Zertifikat handeln, das an die DNS-Adresse des Gateway-Lastenausgleichs gebunden ist.

12.2.3.2 Einstellungen von Dateispeicher und Datei-Repository

Falls Sie planen, den S3-Speicher zu verwenden, müssen Sie den Datei-Repository-Dienst nicht installieren, da der Dateispeicher im S3-Speicher Ihrer Wahl gespeichert wird.

Installieren der Datei-Repository-Dienstes

1. Kopieren Sie das Installationsprogramm von Files Advanced auf den Computer, auf dem sich Datei-Repository und Dateispeicher befinden.
2. Starten Sie das Installationsprogramm, akzeptieren Sie die Lizenzvereinbarung und wählen Sie 'Benutzerdefiniert' aus.
3. Wählen Sie nur die Option 'Datei-Repository' aus und klicken Sie auf 'Weiter'.
4. Wählen Sie die gewünschten Installationspfade aus und klicken Sie auf 'Weiter'.
5. Befolgen Sie die Eingabeaufforderungen, bis die Installation abgeschlossen ist.

6. Das Konfigurationsdienstprogramm wird gestartet. Wählen Sie die Adresse und den Port, über die der Datei-Repository-Dienst verfügbar sein wird.
7. Wählen Sie den Zielordner für den Dateispeicher aus. Der Standardspeicherort ist: **`C:\ProgramData\Acronis\Files Advanced\FileStore`**.

   Hinweis: *Befindet sich der Dateispeicher auf einer Remote-Netzwerkfreigabe, muss der Computer, auf dem der Dienst Datei-Repository ausgeführt wird, über die die vollen Berechtigungen für den Ordner Dateispeicher auf der Netzwerkfreigabe verfügen.*

   Das Konto muss auch über Lese- und Schreibzugriff auf den lokalen Repository-Ordner verfügen (z.B. C:\Program Files (x86)\Acronis\Files Advanced\File Repository\Repository), um in das Protokoll zu schreiben.

8. Starten Sie den Files Advanced Datei-Repository-Dienst.

Files Advanced Einstellungen

1. Rufen Sie die Weboberfläche von Files Advanced auf und melden Sie sich als Administrator an.
2. Navigieren Sie zu Sync&Share -> Datei-Repository und vergewissern Sie sich, dass die Adresse des Dateispeicher-Repository-Endpunkts dieselbe ist, die Sie im Konfigurationsdienstprogramm ausgewählt haben.

12.2.3.3 Spezifische Einstellungen für den Lastenausgleich

1. Öffnen Sie https://mylb.company.com in einem Browser, um sich zu vergewissern, dass die Konfiguration funktioniert.
2. Aktivieren Sie die dauerbasierte Sitzungs-Stickiness (oder die entsprechende Einstellung Ihres Lastenausgleichsmoduls) im Lastenausgleichsmodul, und konfigurieren Sie sie so, dass sie nicht abläuft.
3. Wenn eine Integritätsprüfung erforderlich ist (bei der der HTTP-Status 200 zurückgegeben werden sollte), reicht ein Ping an https://INTERNALSERVERNAME:MANAGEMENTPORT/signin (z.B. https://myaccessserver.company.com/signin and https://myaccessserver.company.com/api/v1/server_version).
4. Zum Sicherstellen der korrekten Protokollierung von IP-Adressen und Verbindungen in einer Einrichtung mit Lastenausgleich müssen Sie Ihren Lastenausgleich zur Einstellung der folgenden Kopfzeilen konfigurieren:
   - **`X-Forwarded-For`** Auf diese Weise wird die richtige IP-Adresse der Clients angegeben, die eine Verbindung herstellen, anstelle von einzelnen Verbindungen, in denen die IP-Adresse des Lastenausgleichs angezeigt wird.
   - **`X-Forwarded-Proto`** Auf diese Weise wird das tatsächlich verwendete Protokoll angezeigt.

12.2.4 Migrieren zu einer Konfiguration mit Lastenausgleich

Diese Anleitung wird als allgemeine Übersicht zu den Anforderungen einer Einrichtung mit Lastenausgleich und den Prozessen für die Migration zu einer Bereitstellung mit Lastenausgleich bereitgestellt. Ihre Einrichtung kann gegebenenfalls von unserem Beispiel abweichen, jedoch sind Art und Weise, wie die Komponenten interagieren, und ihre Einstellungen gleich.

Die empfohlene Konfiguration besteht darin, alle Teile des Files Advanced Server auf verschiedene Computer zwischen den Lastenausgleichen aufzuteilen. Das Datei-Repository und der Dateispeicher können sich auf demselben Computer befinden.

Es wird dringend empfohlen, vor der Migration des Produktionsservers die entsprechenden Schritte in einer Testumgebung auszuführen. Die Testbereitstellung muss dieselbe Architektur wie die Produktionsserver aufweisen und über einige Desktop und Mobile Clients für Testbenutzer verfügen, damit die Kompatibilität in Ihrer Umgebung sichergestellt ist.

Diese Anleitung enthält eine Beispieleinrichtung von Files Advanced, das in einer Standardbereitstellung ausgeführt wird, wobei alle Komponenten auf demselben Computer installiert sind.

Hinweis: *In unserem Beispiel setzen wir den ursprünglichen Files Advanced Tomcat-Dienst fort und verknüpfen ihn mit der neuen Konfiguration. Dies ist nicht obligatorisch.*

Lesen Sie unsere Artikel Backup & Recovery (S. 153), bevor Sie Änderungen an unserer Bereitstellung vornehmen.

Themen

12.2.4.1 Systemanforderungen

Hardwareanforderungen

In einer Produktionsumgebung empfehlen wir Ihnen die Verwendung von mindestens drei (3) Files Advanced Tomcat Servern und drei (3) Gateway Servern, sodass bei Ausfall eines Servers weiterhin eine Lastenverteilung auf zwei aktive Server gewährleistet ist.

Hinweis: *Bei dieser vorgeschlagenen Einrichtung wird davon ausgegangen, dass diese Server auf einem Virtual Machine Server gehostet werden. Bei Verwendung von mehreren Server empfehlen wir die Verwendung von Interconnects mit geringer Latenz zwischen den Gast-Virtual Machines.*

- 1 Lastenausgleichsmodul für die Files Advanced Web Server.
- 1 Lastenausgleichsmodul für die Files Advanced Gateway Server.
- 3 Files Advanced Tomcat Server, jeweils mit 32 GB RAM und einer 16-Kern-CPU.
- 3 Files Advanced Gateway Server, jeweils mit 8 GB RAM und einer 4-Kern-CPU.

  Hinweis: *Für den Gateway Server sind Festplatten- und Netzwerkgeschwindigkeiten relevanter als CPU oder Speicher.*

- 1 PostgreSQL Server mit 32 GB RAM und einer 16-Kern-CPU.
- 1 Datei-Repository-Dienst + Dateispeicher. Die Parameter dieses Servers sind nicht besonders wichtig.

Netzwerkverbindungen

- Der Lastenausgleich für die Files Advanced Tomcat Server muss so konfiguriert werden, dass die DNS-Adresse des aktuellen Files Advanced Servers verwendet wird.

- Der Lastenausgleich für die Gateway Server muss so konfiguriert werden, dass die DNS-Adresse des aktuellen Gateway Servers verwendet wird.
- Der Tomcat Server muss mit dem Gateway Lastenausgleich verbunden werden, damit der Desktop-Netzwerkknoten synchronisiert wird und damit Netzwerkknoten an der Web-Schnittstelle durchsucht werden. In dieser geclusterten Einrichtung auf den Seiten der Files Advanced webUI Administration und Gateway Server ist 'Adresse für Client-Verbindungen' die Adresse des externen Lastenausgleichs. Für die Gateway Server verwenden wir auch die Einstellung 'Alternative Adresse für Files Advanced Server Verbindungen verwenden', und in 'Adresse für Files Advanced Web Server Verbindungen' ist die interne Adresse des Gateway Lastenausgleichs.
- Der Gateway Server muss mit dem Tomcat Lastenausgleich für die mobilen Client-Verbindungen verbunden werden.

Hinweis: *Für die Sync&Share-Datenquelle müssen Sie die Adresse zur Adresse des Tomcat Lastenausgleichs ändern.*

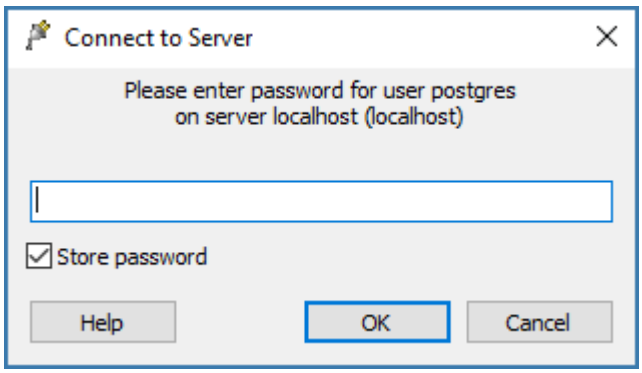
12.2.4.2 Migrieren des PostgreSQL Servers

Ihre Datenbank ist die wichtigste Komponente und muss zuerst migriert werden.

Themen

Konfiguration auf Ihrem vorhandenen PostgreSQL Server

1. Öffnen Sie die Systemsteuerung **Dienste** (`services.msc`) und stoppen Sie den Dienst **Files Advanced Tomcat**.
2. Öffnen Sie die Applikation **Files Advanced PostgreSQL Administrator** und stellen Sie eine Verbindung zum Datenbankserver her. Klicken Sie auf **+** neben **Datenbanken**.
3. Klicken Sie mit der rechten Maustaste auf die `acronisaccess_production`-Datenbank, und wählen Sie **Wartung** -> **Bereinigen** -> **OK**.



4. Öffnen Sie eine Eingabeaufforderung mit erweiterten Benutzerrechten und navigieren Sie mit dem Befehl **cd** zum Postgres **bin**-Verzeichnis. (standardmäßig `C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL\<version>\bin`).
5. Sobald Ihr aktuelles Eingabeaufforderungsverzeichnis der **bin**-Ordner ist, geben Sie den folgenden Befehl ein:

   `pg_dumpall --host localhost --port 5432 --username postgres --file alldbs.sql`

Hinweis: alldbs.sql *wird die generierte Backup-Datei sein und wird im* ***bin****-Ordner gespeichert. Sie kann einen vollständigen Pfad beinhalten, falls Sie andernorts gespeichert werden soll, zum Beispiel* ***D:\Backups\alldbs.sql.***

Hinweis: *Falls Sie einen anderen Port bzw. einen anderen Benutzer verwenden, ändern Sie den Befehl entsprechend.*

6. Sobald das Backup abgeschlossen ist, stoppen und deaktivieren Sie den Dienst **Files Advanced PostgreSQL Server**.
7. Kopieren und verschieben Sie die Backup-Datei auf den neuen Computer, der PostgreSQL hostet.

Konfigurationen auf Ihrem neuen PostgreSQL Server

1. Starten Sie das Installationsprogramm von Files Advanced, und klicken Sie auf **Weiter**. Lesen und akzeptieren Sie die Lizenzvereinbarung.
2. Klicken Sie auf **Benutzerdefiniert** und wählen Sie nur den PostgreSQL Datenbank-Server aus. Klicken Sie auf **Weiter**.
3. Wählen Sie den Speicherort aus, an dem PostgreSQL installiert werden soll, und geben Sie ein Kennwort für den Super-User **`postgres`** ein.

   Hinweis: *Der Speicherort muss für alle anderen Server erreichbar sein, und das Kennwort sollte dasselbe sein wie zuvor auf dem ursprünglichen PostgreSQL Server verwendet.*

4. Wählen Sie **Offener Port 5432 in der Firewall** aus und setzen Sie die Installation fort. Sie verwenden diesen Port für den Fernzugriff auf die PostgreSQL-Datenbank.

Konfigurieren des Zugriffs auf die PostgreSQL-Datenbank

1. Sobald die Installation abgeschlossen ist, navigieren Sie zum Ordner 'PostgreSQL **Daten**' (standardmäßig **`C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL\<version>\Data`**) und öffnen Sie **`pg_hba.conf`** mit einem Texteditor.
2. Beziehen Sie die Host-Einträge für Ihre Access Tomcat Server mittels ihrer internen Adressen ein und speichern Sie die Datei. Wenn Sie nicht alle Serveradressen kennen, können Sie die Datei zu einem späteren Zeitpunkt bearbeiten, bevor Sie dies jedoch tun, können die Server keine Verbindung zur Datenbank herstellen.

   Die**`pg_hba.conf`**-Datei (HBA steht für host-basierte Authentifizierung) steuert die Client-Authentifizierung und wird im Datenverzeichnis des Datenbank-Clusters gespeichert. Darin geben Sie an, welche Server eine Verbindung herstellen dürfen und welche Berechtigungen sie haben sollen, z.B.:

```
# TYPE DATABASE USER ADDRESS METHOD
# Loadbalancer1 (First Files Advanced & Gateway server)
host acronisaccess_production postgres 10.144.70.247/32 md5
```

   Hinweis: *In diesem Beispiel kann das Benutzerkonto mit der Bezeichnung* ***`postgres`*** *vom Server unter 10.144.70.247 eine Verbindung herstellen und mit vollständigen Berechtigungen auf die Datenbank* ***`acronisaccess_production`*** *(mit Ausnahme der Berechtigung* ***Replikation****) über eine* ***`md5 encrypted`*** *Verbindung zugreifen.*

Öffnen Sie die Datei postgresql.conf und nehmen Sie folgende Änderungen vor

1. Entfernen Sie das vorangestellte **#** aus der folgenden Zeile: **`#listen_addresses = 'localhost'.`** Ersetzen Sie **`localhost`** durch **`*`**. Diese muss wie folgt aussehen: **`listen_addresses = '*'`**
2. Entfernen Sie das vorangestellte **#** aus der folgenden Zeile: **`#effective_cache_size = 128MB`** und ersetzen Sie **128MB** durch **12GB**. Diese muss wie folgt aussehen: **`effective_cache_size = 12GB`**
3. Ergänzen Sie den folgenden Hinweis: - **`#NOTE: this tuning setting assumes that PostgreSQL is running by itself on a #VM with at least 16 GB RAM. More information at #https://wiki.postgresql.org/wiki/Tuning_Your_PostgreSQL_Server`**
4. Suchen und ändern Sie **`max_connections`** auf den korrekten Wert. Dieser sollte nicht geringer als alle Tomcat **DB_POOLSIZE** Einstellungen sein, die für jeden Access Server Knoten konfiguriert sind + 10. Wir empfehlen die Einstellung von **DB_POOLSIZE** auf **250**.

   In unserem Beispiel haben wir **`DB_POOLSIZE to 250`** eingestellt, und wir haben zwei Access Tomcat Server, sodass **`max_connections`** auf **510** eingestellt werden muss. Für drei Access Tomcat Server wäre dies **760**.
5. Speichern und schließen Sie die Datei **postgresql.conf**.
6. Starten Sie den Dienst Files Advanced PostgreSQL Server neu.

Importieren Ihrer Datenbank

Auf den neuen PostgreSQL Server

1. Öffnen Sie die PostgreSQL-Administrator-Applikation von Files Advanced und stellen Sie eine Verbindung mit dem lokalen Datenbankserver her. Wählen Sie **Datenbanken** aus und vergewissern Sie sich, dass eine Datenbank mit dem Namen **`acronisaccess_production`** vorhanden ist.
2. Kopieren Sie die Backup-Datenbankdatei **alldbs.sql** in das **bin**-Verzeichnis Ihrer PostgreSQL Installation. (standardmäßig **`C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL\<version>\bin`**)
3. Öffnen Sie ein Fenster für die Eingabeaufforderung mit erweiterten Benutzerrechten und navigieren Sie mit dem Befehl **cd** zum PostgresSQL **bin**-Verzeichnis.
4. Geben Sie den folgenden Befehl ein: **`psql -U postgres -f alldbs.sql`**
5. Geben Sie bei Aufforderung das Kennwort für den **`postgres`** -Benutzer ein. Hierdurch wird die Datenbank vom alten PostgreSQL Server auf dem neuen PostgreSQL Server wiederhergestellt.

12.2.4.3 Files Advanced Serverkonfigurationen

Themen

Verbinden zusätzlicher Files Advanced Server

Nur den Files Advanced Web Server installieren

1. Starten Sie das Files Advanced Installationsprogramm und akzeptieren Sie die Lizenzvereinbarung.

2. Wählen Sie **Benutzerdefiniert** aus, und wählen Sie NUR den Files Advanced Web Server aus.

   Hinweis: *Durch Anklicken des Files Advanced Web Servers wird automatisch auch der PostgreSQL Server ausgewählt. Sie können ihn jedoch mit einem Klick deaktivieren.*

3. Schließen Sie die Installation ab, und vergewissern Sie sich, dass der Files Advanced Tomcat-Dienst angehalten wurde.

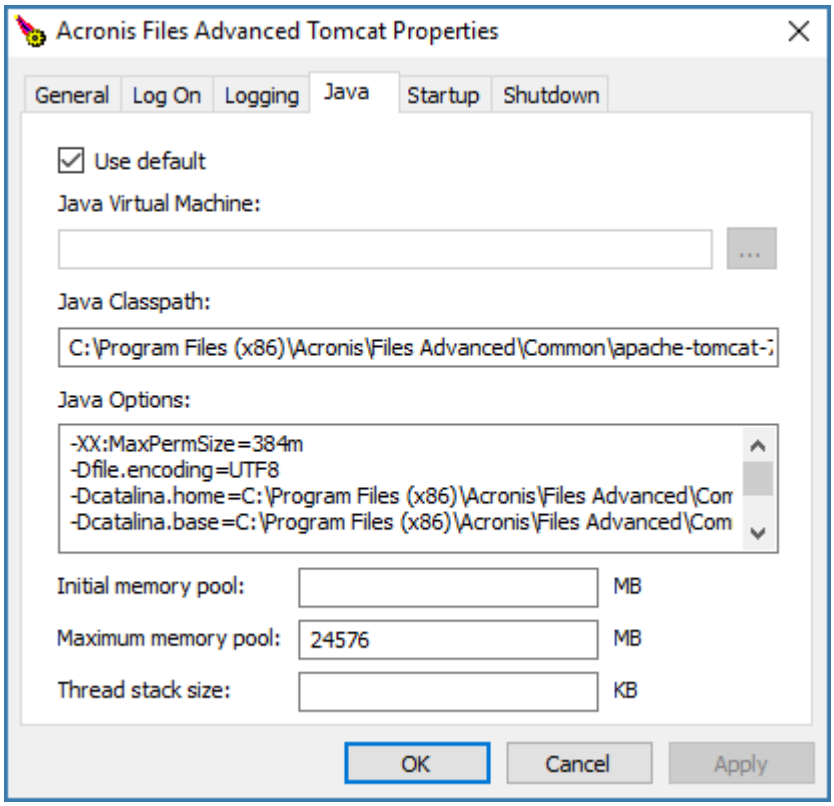
Serverkonfiguration

Alle Einstellungen, die Sie auf einem Files Advanced Web Server ändern, müssen auch auf allen anderen Files Advanced Web Servern geändert werden.

Hinweis: *Vergessen Sie nicht, einen Eintrag in der Datei* ***`pg_hba.conf`*** *für jeden Files Advanced Web Server vorzunehmen!*

Konfigurieren der maximalen Speichernutzung von Tomcat

1. Starten Sie das Tool **Files Advanced Tomcat Service-Konfiguration** von Ihrem Desktop. Falls es sich nicht dort befindet, wechseln Sie zu **Start** –> **Alle Programme** –> **Files Advanced** und klicken Sie auf die Verknüpfung.
2. Klicken Sie auf die Registerkarte **Java**.
3. Erhöhen Sie die Einstellung '**Maximaler Speicherpool**' auf **24576** und klicken Sie auf **OK**.



Konfigurieren des Servers zur Verbindung mit der richtigen Datenbank

1. Navigieren Sie zum Ordner des Files Advanced Web Servers (Standard: **`C:\Program Files (x86)\Acronis\Files Advanced\Access Server`**), und öffnen Sie die Datei **`acronisaccess.cfg`** . Diese Datei teilt dem Server mit, wo sich der PostgreSQL Datenbankdienst befindet.

2. Stellen Sie diese Werte ein:

   DB_HOSTNAME =10.144.70.248

   DB_PORT =5432

   DB_POOLSIZE =250

   Hinweis: DB_HOSTNAME *ist die IP-Adresse, unter der PostgreSQL jetzt ausgeführt wird. In unserem Beispiel ist dies 10.144.70.248.*

   Hinweis: *Wir empfehlen,* ***DB_POOLSIZE*** *auf mindestens 250 einzustellen.*

3. Speichern Sie die Datei.

Konfigurieren der Maximalzahl an Threads

In einer Tomcat Einrichtung mit Lastenausgleich ist es wichtig, dass die Gesamtzahl aller Threads, die von allen Tomcat Instanzen erstellt werden können, nicht die Maximalzahl an Verbindungen überschreitet, für die die PostgreSQL Datenbank konfiguriert ist.

Dies wird von 3 wichtigen Einstellungen bestimmt:

- In der Datei **acronisaccess.cfg** : **DB_POOLSIZE = 200**. Es wird empfohlen, diesen Wert auf mindestens 250 einzustellen.
- In der Tomcat Datei **server.xml**: **maxThreads = 150.** Es wird empfohlen, diese Einstellung auf dem Standardwert von 150 zu belassen.
- In der Datei **postgresql.conf** : **max_connections**. Dies sollte bereits in den vorherigen Schritten konfiguriert worden sein. Es sollte nicht weniger als die Summe aller Tomcat DB_POOLSIZE Werte betragen, die für jeden Files AdvancedWeb Server eingestellt wurden + 10, zum Beispiel 510 für 2 Tomcat Server und 760 für 3 Tomcat Server usw.

  Hinweis: *An dieser Datei vorgenommene Änderungen erfordern einen Neustart der entsprechenden Dienste.*

Konfigurieren einer ordnungsgemäßen Protokollierung

In einer Konfiguration mit Lastenausgleich ordnet der Files Advanced Tomcat Dienst nicht die richtigen IP-Adressen in den Protokollen zu. Zur Gewährleistung, dass alle Verbindungen richtig protokolliert werden, müssen Sie die folgenden Änderungen vornehmen:

1. Suchen Sie in der Datei server.xml nach der Zeile **<Valve className=”org.apache.catalina.valves.AccessLogValve” directory=”logs” prefix=”localhost_access_log.” suffix=”.txt” pattern=”%h %l %u %t "%r" %s %b”/>.**
2. Fügen Sie am Ende **requestAttributesEnabled=”true”** hinzu.
3. Ergänzen Sie unter derselben Zeile Folgendes:

   <Valve className="org.apache.catalina.valves.RemoteIpValve" remoteIpHeader="X-Forwarded-For" protocolHeader="X-Forwarded-Proto"/>
4. Speichern Sie die Datei und starten Sie den Files Advanced-Tomcat-Dienst anschließend neu.

Herstellen einer Verbindung zum alten Files Advanced Server

Wenn Sie Ihren vorhandenen Files Advanced Server weiterhin verwenden möchten, können Sie dies tun. Hierfür müssen Sie jedoch eine Verbindung zur neuen Datenbank herstellen.

Verbinden von Files Advanced mit der Remote-Datenbank

1. Navigieren Sie zum Ordner des Files Advanced Servers (Standard: **`C:\Program Files (x86)\Acronis\Files Advanced\Access Server`**), und öffne Sie die Datei **`acronisaccess.cfg`** . Diese Datei teilt dem Server mit, wo sich der PostgreSQL Datenbankdienst befindet.
2. Stellen Sie die Werte wie folgt ein:

   `DB_HOSTNAME =10.144.70.248`

   `DB_PORT =5432`

   `DB_POOLSIZE = 250`

   Hinweis:DB_HOSTNAME *legt die IP-Adresse fest, unter der sich die PostgreSQL Datenbank befindet. In diesem Beispiel ist dies 10.144.70.248.*

3. Speichern Sie die Datei und starten Sie anschließend den **Files Advanced Tomcat-Dienst** in der **Dienste**steuerung (services.msc).
4. Alle nicht verwendeten Files Advanced Komponenten können deinstalliert werden.

12.2.4.4 Migration von Dateispeicher und Datei-Repository

Lesen Sie unsere Anleitung Verschieben von Dateispeicher und Datei-Repository (S. 246). Die einzige zusätzliche Einstellung, die Sie ggf. überprüfen müssen, ist, dass alle Files Advanced Komponenten über einen Zugriff auf den Computer verfügen, der Datei-Repository und Dateispeicher hostet.

Falls Sie planen, den S3-Speicher zu verwenden, müssen Sie den Datei-Repository-Dienst nicht installieren, da der Dateispeicher im S3-Speicher Ihrer Wahl gespeichert wird.

Falls Sie planen, Datei-Repository und Dateispeicher an ihrem Ort zu belassen, müssen Sie nur sicherstellen, dass Ihre neuen Files Advanced Server auf den richtigen Repository-Endpunkt verweisen.

12.2.4.5 Ihren Gateway Server migrieren

Einen neuen Gateway Server installieren

1. Führen Sie auf einem neuen Computer das Files Advanced Installationsprogramm aus und akzeptieren Sie die Lizenzvereinbarung.
2. Wählen Sie **Benutzerdefiniert** und installieren Sie nur die Gateway Server-Komponente. Schließen Sie die Installation ab.
3. Legen Sie im Konfigurationswerkzeug Gateway-Adresse, Port und Zertifikat fest. Dabei sollte es sich um dasselbe SSL-Zertifikat handeln, das an die DNS-Adresse des Gateway-Lastenausgleichs gebunden ist.

Migrieren aller Einstellungen vom vorherigen Gateway Server

1. Öffnen Sie auf dem alten Computer mit Tomcat sowie Gateway die Files Advanced Weboberfläche, und öffnen Sie die Seite 'Gateway Server'. Ihnen wird ein Eintrag für den alten Gateway angezeigt.
2. Fügen Sie den neuen Gateway hinzu, indem Sie auf **Gateway Server hinzufügen** klicken und alle entsprechenden Daten eingeben.
3. Klicken Sie auf **Cluster-Gruppe hinzufügen**.
   - Geben Sie einen Display-Namen ein.

- Geben Sie die **Adresse für Client-Verbindungen** ein. Im Cluster ist '**Adresse für Client-Verbindungen**' die Adresse des externen Lastenausgleichs. Klicken Sie auf '**Alternative Adresse für Files Advanced Server Verbindungen verwenden**', und geben Sie in '**Adresse für PRODUCT_NAME> Server Verbindungen**' die interne Adresse des Gateway Lastenausgleichs ein.

4. Aktivieren Sie unter **Zum Clustering verfügbare Gateway Server** das Kontrollkästchen **Einschließen** für beide Gateway Server.
5. Wählen Sie unter **Für Einstellungen zu nutzender Gateway Server** den alten Gateway Server aus.
6. Klicken Sie auf **Hinzufügen**, und auf der Seite 'Gateway Server' wird Ihnen der neue Cluster angezeigt. Erweitern Sie diesen mit dem +.
7. Es sollten jetzt alle Einstellungen in den neuen Gateway migriert worden sein. Machen Sie den neuen Gateway zum Master des Clusters, indem Sie auf das entsprechende Dropdown-Menü **Aktionen** klicken und **Gruppen-Master werden** auswählen.
8. Sie können den alten Gateway unverändert lassen, ihn aus der Cluster-Gruppe 'Entfernen' oder 'Entfernen und löschen'. Wir empfehlen, ihn als Teil des Clusters zu behalten, bis Ihre Einrichtung vollständig und korrekt ausgeführt wird.

12.2.4.6 Log-Verwaltung und Bereinigung

Stellen Sie nach der Installation zusätzlicher Files Advanced Server sicher, dass Sie den Ordner öffnen, in dem sich Files Advanced Tomcat-Logs befinden, und stellen Sie für diese Ordner die korrekten Berechtigungen ein, sodass Logs geschrieben und bereinigt werden können.

12.2.4.7 Spezifische Einstellungen für den Lastenausgleich

1. Öffnen Sie https://mylb.company.com in einem Browser, um sich zu vergewissern, dass die Konfiguration funktioniert.
2. Aktivieren Sie die dauerbasierte Sitzungs-Stickiness (oder die entsprechende Einstellung Ihres Lastenausgleichsmoduls) im Lastenausgleichsmodul, und konfigurieren Sie sie so, dass sie nicht abläuft.
3. Wenn eine Integritätsprüfung erforderlich ist (bei der der HTTP-Status 200 zurückgegeben werden sollte), reicht ein Ping an https://INTERNALSERVERNAME:MANAGEMENTPORT/signin (z.B. https://myaccessserver.company.com/signin and https://myaccessserver.company.com/api/v1/server_version).
4. Zum Sicherstellen der korrekten Protokollierung von IP-Adressen und Verbindungen in einer Einrichtung mit Lastenausgleich müssen Sie Ihren Lastenausgleich zur Einstellung der folgenden Kopfzeilen konfigurieren:
   - **`X-Forwarded-For`** Auf diese Weise wird die richtige IP-Adresse der Clients angegeben, die eine Verbindung herstellen, anstelle von einzelnen Verbindungen, in denen die IP-Adresse des Lastenausgleichs angezeigt wird.
   - **`X-Forwarded-Proto`** Auf diese Weise wird das tatsächlich verwendete Protokoll angezeigt.

12.2.4.8 Ursprüngliche(n) Server bereinigen

Wenn Sie den Files Advanced Tomcat weiterhin verwenden, d.h. auf dem ursprünglichen Produktionsserver, empfehlen wir, dass Sie die Files Advanced Elemente deinstallieren, die auf diesem Server nicht mehr verwendet werden.

Über die Systemsteuerung können Sie den Files Advanced PostgreSQL Server, den Files Advanced Gateway Server und den Files Advanced Datei-Repository Server (falls vorhanden) deinstallieren.

12.2.5 Die Weboberfläche über die API anpassen

Die Nutzung der API zur Aktualisierung des Farbschemas Ihrer Weboberfläche kann einfach durchgeführt werden, erfordert keinen Neustart der Dienste und verursacht keine Ausfallzeiten. Einige dieser Anpassungen können über die Weboberfläche von Files Advanced (S. 135) vorgenommen werden.

Installieren von CURL

1. Sie müssen Curl installieren, um API-Befehle nutzen zu können.
   a. Laden Sie Curl von der offiziellen Website herunter: https://curl.haxx.se/download.html

   Hinweis: *Laden Sie eine Version herunter, die SSL unterstützt!*

   b. Folgen Sie den Eingabeaufforderungen im Curl-Installer bis die Installation abgeschlossen ist oder extrahieren Sie nur das Curl-Archiv.

Erstellen eines benutzerdefinierten Farbschemas

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

```
curl -X PUT -F
customization_settings[color_scheme_administration_css_file]=@<path_to_
file> -F
customization_settings[color_scheme_client_scss_file]=@<path_to_file> -u
<user>:<password> https://<your_site>/api/v1/settings/customization -v
```

   Hinweis: *Die Dateinamen müssen eine spezifische Benennungssyntax enthalten!* ***color_scheme_<name_of_scheme>****.css für die Verwaltungskonsole und* ***web_client_<name_of_scheme>****.scss für die Web Client-Konsole.* ***<name_of_scheme>*** *ist der Name Ihres neuen Schemas, das auf der Oberfläche von Files Advanced angezeigt wird, und dieser muss für beide Dateien gleich sein.*

   Der obige Befehl bewirkt Folgendes:

   - Auswahl einer **.css**-Datei für die Verwaltungskonsole.
   - Auswahl einer **.scss**-Datei für die Web Client-Konsole.
   - Erstellung eines neuen Designs, das im Dropdown-Menü **Farbschema** in der Web-Schnittstelle auswählbar ist.

   Hinweis: *Falls Sie bei Eingabe des obigen Befehls nur einen Teil eines Farbschemas ändern möchten, müssen Sie das neue .css-Schema für den geänderten Teil und das vorhandene .css-Schema für den unveränderten Teil verwenden.*

2. Dieses Beispiel zeigt, wie der Befehl aussieht, wenn Sie ein Schema für den Verwaltungsteil der Oberfläche und ein Schema für den Web-Client hochladen möchten.
3. In diesem Beispiel befinden sich beide Dateien unter **D:\WebUI**, und wir wählen **NewColor** als Namen des Farbschemas, das in der Web-Oberfläche angezeigt wird:

```
curl -X PUT -F
customization_settings[color_scheme_administration_css_file]=@D:\WebUI\
color_scheme_NewColor.css -F
customization_settings[color_scheme_client_scss_file]=@D:\WebUI\web_cli
ent_NewColor.scss -u administrator:123456
https://myCompany.com/api/v1/settings/customization
```


4. Sie können auch den Befehl **-F customization_settings[color_scheme]=<name_of_scheme>** zum Umschalten zwischen Ihrem aktuellen Design und dem neuen Design, das Sie hinzufügen, verwenden. Wird dieser Befehl zum Rest hinzugefügt, sieht es wie folgt aus:

```
curl -X PUT -F
customization_settings[color_scheme_administration_css_file]=@D:\WebUI\
color_scheme_NewColor.css -F
customization_settings[color_scheme_client_scss_file]=@D:\WebUI\web_cli
ent_NewColor.scss -F customization_settings[color_scheme]=NewColor -u
administrator:123456 https://myCompany.com/api/v1/settings/customization
-v
```

Fehlerbehebung

- Der Befehl wird ausgeführt, das neue Design ist jedoch nicht auf der Oberfläche sichtbar

  Vergewissern Sie sich, dass die Dateinamen der korrekten Syntax von **color_scheme_<name_of_scheme>.css** und **web_client_<name_of_scheme>.scss** folgen
- Anzeige der Fehlermeldung **Protokoll https nicht unterstützt oder in libcurl deaktiviert**

  Entfernen Sie sämtliche einfachen Anführungszeichen ('), die Ihre Adresse umgeben. Falls Sie Anführungszeichen verwenden müssen, verwenden Sie stattdessen doppelte Anführungszeichen ("), z.B. "https://myCompany.com/api/v1/settings/customization"
- Anzeige eines Zertifikatfehlers

  Falls Sie selbstsignierte Zertifikate verwenden oder die Befehle mittels einer IP-Adresse ausführen, müssen Sie am Ende des Befehls die Kennzeichnung **-k** hinzufügen, damit Zertifikatfehler ignoriert werden.

12.2.6 Unbeaufsichtigte Desktop Client-Konfiguration

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

Das Gruppenrichtlinienobjekt erstellen und konfigurieren:

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

Unbeaufsichtigte Installation des Clients

Dieser Abschnitt hilft Ihnen dabei, den Files Advanced Desktop Client bei der Benutzeranmeldung auf allen gewünschten Computern im Verborgenen zu installieren.

Einen Verteilungspunkt für den Installer erstellen

Alle Computer, auf denen der Client installiert wird, müssen auf den Installer zugreifen können. Erstellen Sie hierzu einen Ordner, geben Sie ihn für die gewünschte Benutzergruppe frei, und legen Sie den Installer in diesem Ordner ab.

1. Klicken Sie mit der rechten Maustaste auf den Ordner mit dem Installer, und wählen Sie **Eigenschaften**.
2. Öffnen Sie die Registerkarte **Freigeben**, und wählen Sie **Freigeben**.
3. Geben Sie die Domänengruppe, die Organisationseinheit oder die Benutzer ein, auf denen der Access Client installiert wird. Diese Gruppe (o.ä.) sollte mit der für das **Gruppenrichtlinienobjekt** ausgewählten identisch sein.
4. Wählen Sie **OK**/**Fertig**, und schließen Sie alle restlichen Dialogfelder.

Hinweis: *Stellen Sie sicher, dass die gewünschten Computer über die Netzwerkadresse (z.B.* ***`\\WIN2008\Software\AAClientInstaller.msi`****) auf den Installer zugreifen können.*

Den Installer auf den Benutzercomputer übertragen

1. Erweitern Sie auf dem Domain Controller den Bereich **Gruppenrichtlinienobjekte**, und klicken Sie mit der rechten Maustaste auf Ihr neues Richtlinienobjekt.
2. Wählen Sie **Bearbeiten**, und erweitern Sie **Benutzerkonfiguration** -> **Einstellungen**-> **Windows-Einstellungen** -> **Dateien**.
3. Klicken Sie mit der rechten Maustaste auf 'Dateien', und wählen Sie 'Neu' -> 'Datei'.
4. Wählen Sie **Erstellen** als **Aktion**.
5. Für **Quelldatei** klicken Sie entweder auf die Schaltfläche 'Durchsuchen' und gehen zum Installer für den Access Client, oder geben Sie den vollständigen Pfad ein. (z.B. \\WIN2008\Software\AAClientInstalelr.msi)
6. Für **Zieldatei** geben Sie den Zielordner und den Zieldateinamen ein. Dadurch wird der Installer für den Access Client in der Netzwerkfreigabe kopiert und bei der Anmeldung in den Zielordner auf dem Computer des Benutzers eingefügt.

   Hinweis: *Wenn Sie beispielsweise* ***C:\Ordner\DieseDatei.msi*** *eingeben, wird der Client-Installer auf das Laufwerk* ***C****, in den Ordner 'Ordner' des Benutzers kopiert und* ***DieseDatei.msi*** *benannt.*

7. Wählen Sie **OK**.

Den Client installieren

Das Installationsskript erstellen

1. Erstellen Sie eine leere Textdatei, und kopieren Sie folgendes Skript in die Datei:

```
msiexec /i "C:\AAC.msi" /quiet
sleep 180
```



```
DEL /F /S /Q /A "C:\AAC.msi"
```

Dieses Skript öffnet eine Eingabeaufforderung, installiert den Access Client, ohne etwas anzuzeigen, und löscht das Installationsprogramm für den Access Client nach drei Minuten.

2. Ändern Sie an beiden Stellen den Pfad **`C:\AAC.msi`** in den Pfad um, den Sie im Feld **Zieldatei** eingegeben haben, und klicken Sie auf **Datei** -> **Speichern unter**.
3. Geben Sie einen Namen für das Skript ein. Stellen Sie sicher, dass die Dateiendung **.bat** lautet. Wählen Sie im Feld **Dateityp** die Option **Alle Dateien**. Stellen Sie sicher, dass sich die Datei entweder auf dem Domain Controller befindet oder dass dieser darauf zugreifen kann. Diese Datei ist wichtig und darf nicht geändert oder gelöscht werden. Speichern Sie sie also an einem Speicherort, der nicht geändert wird.

Das Skript bei der Benutzeranmeldung verwenden

1. Öffnen Sie die **Gruppenrichtlinienverwaltung**, und erweitern Sie den Bereich **Gruppenrichtlinienobjekte**. Klicken Sie mit der rechten Maustaste auf Ihr neues **Richtlinienobjekt**.
2. Wählen Sie **Bearbeiten**, und erweitern Sie **Benutzerkonfiguration** -> **Richtlinien**-> **Windows-Einstellungen** -> **Skripts (Anmelden/Abmelden)**.
3. Doppelklicken Sie auf **Anmelden**, und wählen Sie dann **Hinzufügen**.
4. Wählen Sie im Dialogfeld **Skript hinzufügen** die Option **Durchsuchen (...)**, und navigieren Sie zu dem Ordner, in dem Sie das Skript gespeichert haben.
5. Wählen Sie das Skript aus, und klicken Sie **Öffnen**.
6. Wählen Sie **OK** und im nächsten Dialogfeld erneut **OK**.
7. Fertig. Für alle Benutzer in der angegebenen Gruppe oder Organisationseinheit wird nun bei der Anmeldung der Files Advanced Client installiert.

Ordner und Registrierungseinträge erstellen:

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

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

Synchronisierungsordner erstellen:

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

Registrierung erstellen:

1. Klicken Sie mit der rechten Maustaste auf **Registrierung** und wählen Sie **Neu** -> **Registrierungselement**.

2. Setzen Sie die **Aktion** auf **Erstellen**.
3. Wählen Sie für **Struktur HKEY_CURRENT_USER**.
4. Geben Sie als Pfad Folgendes ein: **`Software\Group Logic, Inc.\activEcho Client\`**
5. Führen Sie jetzt für die gewünschten Einträge Folgendes durch:
6. Für den Benutzernamen:
   a. Für **Wertnamen** '**Benutzername**'.
   b. Für **Werttyp** **REG_SZ**.
   c. Für **Wertdaten** das folgende Token: **`%USERNAME%@%USERDOMAIN%`**

   Hinweis: *Wenn Sie **Einzelanmeldung (Single Sign-on)** verwenden möchten, konfigurieren Sie das Token für den Benutzernamen **nicht**. Gehen Sie stattdessen folgendermaßen vor:*

   - **Für SSO**:
   - Geben Sie für **Wertname** den Namen '**AuthenticateViaSSO**' ein.
   - Wählen Sie für **Werttyp** die Option **REG_SZ**.
   - Geben Sie für **Wertdaten** die Zahl **1** ein.
7. Für die Server-URL:
   a. Für **Wertnamen** '**Server-URL**'.
   b. Für **Werttyp** **REG_SZ**.
   c. Für **Wertdaten** die Adresse Ihres Files Advanced Servers, z.B. **https://myaccess.com**
8. Für den Synchronisierungsordner:
   a. Für **Wertnamen** '**activEcho-Ordner**'.
   b. Für **Werttyp** **REG_SZ**.
   c. Für **Wertdaten** folgendes Token und folgenden Pfad: **`%USERPROFILE%\Desktop\AAS Data Folder`**
9. Für das Auto-Update:
   a. Für **Wertnamen** '**AutoCheckForUpdates**'.
   b. Für **Werttyp** **DWORD**.
   c. Für **Wertdaten** '**00000001**'. Mit dem Wert '**1**' wird diese Einstellung aktiviert und der Client prüft automatisch auf Updates. Wird der Wert auf '**0**' festgelegt, wird die Einstellung deaktiviert.
10. Für die Zertifikate:
    a. Für **Wertnamen** '**AllowInvalidCertificates**'.
    b. Für **Werttyp** **DWORD**.
    c. Für **Wertdaten** '**00000000**'. Mit dem Wert '**0**' wird diese Einstellung deaktiviert und der Client kann keine Verbindung mehr zu Files Advanced Servern mit ungültigen Zertifikaten herstellen. Wird der Wert auf '**1**' festgelegt, wird die Einstellung aktiviert.

12.2.7 Einzelanmeldung (Single Sign-On) konfigurieren

Dieser Leitfaden führt Sie durch eine erweiterte Konfiguration, um die Funktion für Einzelanmeldungen für Files Advanced zu aktivieren.

Hinweis: *Die Einzelanmeldung kann nur in einer funktionierenden Domäne verwendet werden.*

Hinweis: *Die Einzelanmeldung funktioniert **NICHT** , wenn Sie Files Advanced in einer Konfiguration mit nur einem Port verwenden (wenn der Gateway Server als Proxy für die Files Advanced Server-Anforderungen fungiert).*

Hinweis: *Die Einzelanmeldung funktioniert* ***NICHT*** *, wenn Files Advanced auf dem Domänencontroller installiert ist. Ganz abgesehen von den SSO-Beschränkungen empfehlen wir auch aus Leistungsgründen dringend, den Files Advanced Server nicht auf dem Domänencontroller zu installieren.*

Mit der Single Sign-On-Funktion können sich gültige LDAP-Benutzer an der Weboberfläche und am Desktop Client anmelden, ohne ihre Anmeldedaten eingeben zu müssen. Der Benutzer muss über ein Files Advanced-Konto verfügen, oder die LDAP-Bereitstellung muss auf dem Server aktiviert sein.

- Files Advanced zeigt auf der Anmeldeseite einen Link an, über den der Benutzer mit dem Konto angemeldet wird, das für die Anmeldung bei diesem Computer verwendet wurde.

  Hinweis: *Sie müssen die Oberfläche von Files Advanced mithilfe des FQDN (z.B. https://access.company.com) öffnen, damit SSO funktioniert. Einzelanmeldung (Single Sign-on) funktioniert* ***NICHT*** *, wenn Sie die Oberfläche über die IP-Adresse öffnen.*

- Für den Desktop Client steht ein neues Aktionsfeld zur Aktivierung von SSO zur Verfügung. Benutzer müssen nur die URL des Files Advanced Servers eingeben. Damit werden sie automatisch mit dem Konto angemeldet, das sie für die Anmeldung an ihrem Computer verwendet haben.

  Hinweis: *Das funktioniert nur für den Windows-Client. Mac-Unterstützung wird in einem späteren Release zur Verfügung stehen.*

Themen

12.2.7.1 Files Advanced Web Server und Gateway auf demselben Computer

Diese Konfiguration ist die gebräuchlichste und besteht aus 1 Files Advanced Web Server und 1 Files Advanced Gateway Server, die beide auf demselben Computer gehostet sind. Dies ist die standardmäßige Installation.

Themen

Dies ist ein einmaliger Schritt, der für die Registrierung von Files Advanced Web Server für den Kerberos-Server in der Domäne ausgeführt werden muss. Wir geben mit 'setspn.exe' an, welches LDAP-Konto für SSO-Authentifizierungsprüfungen abgefragt wird.

Hinweis: *Wenn Sie* ***mobile Clients mit Zertifikatsauthentifizierung*** *verwenden möchten, dürfen die DNS-Einträge für die Access- und Gateway Server* ***NICHT*** *mit dem Namen des Computers identisch sein. Wenn der SPN des Files Advanced Servers nur im Namen des Computers enthalten ist, behandelt der Gateway Server den Files Advanced Server, als wäre er auf seinem Gerät installiert und versucht daher keine Kerberos-Authentifizierung.*

z.B.: ***`machineAccess.domain.com / machineGW.domain.com`*** *funktioniert*

*z.B.: **machine.domain.com/ computer.domain.com will** funktioniert NICHT*

Das LDAP-Konto konfigurieren, das SSO handhabt

***Hinweis:** Wenn Sie SMB- oder SharePoint-Datenquellen nutzen möchten, müssen Sie das Active Directory-Konto so konfigurieren, dass Kerberos-Delegierung für all Ihre SMB- und SharePoint-Datenquellen erlaubt wird. Weitere Informationen finden Sie im Artikel Erweiterte Delegierungskonfigurationen.*

1. Öffnen Sie eine Eingabeaufforderung.

   ***Hinweis:** Sie müssen mit einem Domänenkonto angemeldet sein und über die Rechte zur Verwendung von **setspn** verfügen.*

2. Geben Sie den Befehl **setspn –s HTTP/Computername.Domänenname.com Kontoname** ein.

   Beispiel: Ist Ihr Files Advanced Web Server unter **ahsoka.acme.com** installiert und möchten Sie **john@acme.com** als vorab authentifiziertes LDAP-Konto zur Gewährung von Kerberos-Tickets verwenden, sieht der Befehl folgendermaßen aus:

   ```
   setspn -s HTTP/ahsoka.acme.com john
   ```

   ***Hinweis:** Der im obigen Befehl verwendete LDAP-Kontoname **MUSS** mit dem Konto übereinstimmen, das Sie über die Eigenschaft **spnego.preauth.username** in **web.xml** angeben.*

   ***Hinweis:** Dieses Konto entspricht in der Regel dem vom Administrator in der Files Advanced-Weboberfläche unter **Allgemeine Einstellungen** -> **LDAP** -> **LDAP-Benutzername** / **LDAP-Kennwort** angegebenen LDAP-Konto. Dies ist jedoch nicht zwingend der Fall.*

3. Wird Ihr Files Advanced Web Server auf einem Nicht-Standard-Port (d. h., einem anderen Port als 443) ausgeführt, sollten Sie auch einen SPN mit der Portnummer registrieren.

   Beispiel: Läuft Ihr Server an Port 444, lautet der Befehl folgendermaßen:

   ```
   setspn -s HTTP/ahsoka.acme.com:444 john
   ```

   ***Hinweis**: **HTTP** in den voranstehenden Befehlen bezieht sich auf die **HTTP**-Dienstklasse und nicht auf das **HTTP**-Protokoll. Die **HTTP**-Dienstklasse verarbeitet **HTTP**- und **HTTPS**-Anforderungen. Sie müssen und **sollten KEINEN** SPN mit **HTTPS** als Dienstklassenname erstellen.*

4. Wechseln Sie zum Domain-Controller und öffnen Sie **Active Directory-Benutzer und -Computer**.
5. Suchen Sie den in den voranstehenden Befehlen verwendeten Benutzer (in diesem Beispiel **john**).
6. Klicken Sie auf die Registerkarte **Delegierung** und wählen Sie **Diesem Benutzer für die Delegierung an jeden beliebigen Dienst trauen (nur Kerberos)** aus.
7. Wählen Sie **OK**.

Den SPN für den Gateway Server konfigurieren

Damit der KDC („Key Distribution Center“) Kerberos-Server Benutzer für den Gateway-Server authentifizieren kann, muss der Gateway-Dienst für den KDC registriert werden. Hierzu müssen „setspn“ und der Hostname des Servers angegeben werden, auf dem er als 'user' im setspn-Befehl läuft.

Für diese Konfiguration müssen Sie einen zusätzlichen DNS-Eintrag für Ihren Gateway-Server festlegen.

1. Öffnen Sie auf Ihrem DNS-Server die **Vorwärtssuchbereiche** für Ihre Domäne, klicken Sie mit der rechten Maustaste, und erstellen Sie einen neuen **Host**-Eintrag **`(A record)`** für den Gateway-Server.
2. Geben Sie einen Namen ein. Dabei handelt es sich um die DNS-Adresse, die zum Erreichen des Gateway-Servers verwendet wird.

   Beispiel: `ahsoka-gw.acme.com`
3. Geben Sie die IP-Adresse des Gateway Servers ein (ohne den Port). Wenn Sie den Gateway und den Files Advanced Server unter derselben IP-Adresse ausführen, geben Sie diese IP-Adresse ein.
4. Wählen Sie **Zugewiesenen Pointer (PTR)-Datensatz erstellen** und drücken Sie **Host hinzufügen**.
5. Wechseln Sie zurück zum Computer mit Files Advanced.
6. Öffnen Sie die Eingabeaufforderung.
7. Geben Sie den folgenden **setspn**-Befehl ein: **`setspn -s HTTP/GatewayDNS.Domäne.com Computername`**

   Führen Sie beispielsweise für den Fall, dass Ihr Gateway Server auf Host **`'ahsoka'`** in der Domäne läuft und Ihr DNS-Eintrag **`ahsoka-gw.acme.com`** lautet, folgenden Befehl aus:

   `setspn -s HTTP/ahsoka-gw.acme.com ahsoka`
8. Läuft Ihr Gateway Server nicht an einem Standard-Port (d. h. an einem anderen Port als 443), müssen Sie auch einen SPN mit der Portnummer registrieren, z. B. dann, wenn Ihr Gateway Server an Port 444 läuft:

   `setspn -s HTTP/ahsoka-gw.acme.com:444 ahsoka`
9. Ändern Sie die gewünschte **Adresse für Administration** und **Adresse für Client-Verbindungen** des Gateway Server in den DNS-Eintrag des neuen Gateway Servers, den Sie in Schritt 4 erstellt haben.

   Hinweis: *Die Adressen sollten identisch und in den richtigen DNS-Eintrag geändert worden sein.*

Einrichten des Domänenkontos für eine SSO-Authentifizierung

1. Navigieren Sie zu **`C:\Program Files (x86)\Acronis\Files Advanced\Access Server\Web Application\WEB-INF\`**
2. Suchen und öffnen Sie die Datei **`web.xml`**. In dieser Datei geben Sie den Benutzernamen und das Kennwort für die Domäne an, unter der der SSO-Dienst läuft. Das Konto **muss** mit dem Konto übereinstimmen, das Sie im Abschnitt **In der Domäne** zur Registrierung des HTTP-Dienstes für Kerberos verwendet haben.
3. In **`web.xml`** müssen zwei Eigenschaften eingerichtet werden – der vom SSO-Dienst zu verwendende Benutzername für die Domäne und das zugehörige Kennwort. Suchen Sie die folgenden Zeilen:

```
<init-param>
    <param-name>spnego.preauth.username</param-name>
    <param-value>ihrbenutzername</param-value>
 </init-param>
 <init-param>
    <param-name>spnego.preauth.password</param-name>
    <param-value>ihrkennwort</param-value>
 </init-param>
```

4. Ersetzen Sie **ihrbenutzername** durch den gewünschten LDAP-Benutzernamen.

5. Ersetzen Sie **ihrkennwort** durch das LDAP-Kennwort für das zuvor angegebene LDAP-Konto. Wenn Ihr Kennwort eines der fünf folgenden Sonderzeichen enthält, **&**, **>**, **"**, ' , or **<**, dann müssen Sie diese zunächst im XML-Dokument escapen. Dazu müssen Sie sie folgendermaßen ersetzen:
   - **<** durch **<**
   - **>** durch **>**
   - **'** durch **"**
   - **,** durch **'**
   - **&** durch **&**

   Wenn Ihr Passwort also **`<my&best'password"`** lautet, müssen Sie es in der Datei **`web.xml`** folgendermaßen schreiben: **`<my&best'password"`**

Einrichten der Kerberos-Domänensuche

1. Navigieren Sie zu **`C:\Program Files (x86)\Acronis\Files Advanced\Common\apache-tomcat-7.0.59\conf`**
2. Suchen und öffnen Sie die Datei **`krb5.conf`**
3. In **`krb5.conf`** gibt es nur zwei Eigenschaften, die der Administrator angeben muss:
   a. Die Domäne für SSO (z.B. **`ACME.COM`**). Beachten Sie, dass es sich um den Namen Ihrer Domäne handelt, **nicht** um den DNS-Namen des Servers.

   Hinweis: *Die Domäne in* ***`krb5.conf`*** *muss immer in* ***GROSSBUCHSTABEN*** *angegeben werden. Andernfalls schlagen Suchen nach Kerberos-Tickets möglicherweise fehl.*

   b. Die Adresse des Kerberos Key Distribution Centers (entspricht üblicherweise der Adresse Ihres primären Domänencontrollers, z.B. **`acmedc.ACME.COM`**)
4. Die von uns installierte **`krb5.conf`**-Datei sieht folgendermaßen aus:

```
[libdefaults]
        default_realm = ACME.COM
        default_tkt_enctypes = aes128-cts rc4-hmac des3-cbc-sha1 des-cbc-md5
des-cbc-crc
        default_tgs_enctypes = aes128-cts rc4-hmac des3-cbc-sha1 des-cbc-md5
des-cbc-crc
        permitted_enctypes   = aes128-cts rc4-hmac des3-cbc-sha1 des-cbc-md5
des-cbc-crc

    [realms]
        ACME.COM = {
            kdc = acmedc.ACME.COM
            default_domain = ACME.COM

    [domain_realm]
        .ACME.COM = ACME.COM
```

5. Ersetzen Sie alle Instanzen von **`ACME.COM`** durch Ihre Domäne (**in Großbuchstaben!**). Beachten Sie, dass es sich um den Namen Ihrer Domäne handelt, **nicht** um den DNS-Namen des Servers.

6. Ersetzen Sie den Wert für '**kdc =**' durch den Namen Ihres Domänencontrollers. Die Domäne muss in Großbuchstaben angegeben werden, z.B. **`kdc = yourdc.YOURDOMAIN.COM`**
7. Nach der Aktualisierung der oben genannten Konfigurationsdateien muss der Files Advanced Server (der Files Advanced Tomcat-Dienst) neu gestartet werden, damit die Änderungen wirksam werden.

Single Sign-On in der Weboberfläche aktivieren:

1. Rufen Sie die Weboberfläche von Files Advanced auf und melden Sie sich als Administrator an.
2. Erweitern Sie die Registerkarte **Allgemeine Einstellungen**, und öffnen Sie die Seite **LDAP**.
3. Aktivieren Sie unten auf der Seite das Kontrollkästchen **Anmelden vom Webclient und Desktop Sync Client mit vorhandenen Windows-/Mac-Anmeldedaten erlauben**.
4. Drücken Sie **Speichern**.

Hinweis: *Diese Schritte können nur durchgeführt werden, wenn sich die Computer, welche die Gateway Server hosten, in derselben Domäne befinden wie der Files Advanced Web Server.*

Damit der KDC („Key Distribution Center“) Kerberos-Server Benutzer für den Gateway-Server authentifizieren kann, muss der Gateway-Dienst für den KDC registriert werden. Hierzu müssen „setspn“ und der Hostname des Servers angegeben werden, auf dem er als 'user' im setspn-Befehl läuft.

Gateway Server, die auf anderen Computern als dem Files Advanced Web Server gehostet werden

1. Öffnen Sie die Eingabeaufforderung.
2. Geben Sie den folgenden **setspn**-Befehl ein: **`setspn -s HTTP/Computername.Domäne.com Computername`**

   Führen Sie beispielsweise für den Fall, dass Ihr Gateway Server auf Host **`'cody'`** in der Domäne läuft, folgenden Befehl aus:

   `setspn -s HTTP/cody.acme.com cody`
3. Läuft Ihr Gateway Server nicht an einem Standard-Port (d. h. an einem anderen Port als 443), müssen Sie auch einen SPN mit der Portnummer registrieren, z. B. dann, wenn Ihr Gateway Server an Port 444 läuft:

   `setspn -s HTTP/cody.acme.com:444 cody`
4. Wiederholen Sie diesen Abschnitt für alle weiteren Gateway-Server.

Auf dem Computer eines Benutzers

Hierbei handelt es sich um eine kleine, einmalig auf dem Client-Computer durchzuführende Konfiguration zur Aktivierung der Single Sign-On-Unterstützung für Ihren Browser.

Hinweis: *Die nachfolgenden Schritte müssen für jeden Benutzer auf jedem Computer ausgeführt werden.*

Hinweis: *Wenn Dienste in mehreren Domänen vorliegen, wiederholen Sie den Abschnitt für Ihren Browser mit dem zweiten Domänennamen.* ***Beispiel:*** *Sowohl* ***`*.acme.com`*** *als auch* ***`*.tree.com`*** *hinzufügen.*

Windows:

Für Internet Explorer:

- Rufen Sie Internet Explorer auf, wechseln Sie zu **Extras** -> **Internetoptionen** -> **Sicherheit** -> **Lokales Intranet** -> **Sites** -> **Erweitert**, und fügen Sie die Adresse Ihres Files Advanced Servers hinzu, z. B. **`https://ahsoka.acme.com`** **(** oder einfach **`*.acme.com`**), und starten Sie den Browser neu.

Für Chrome:

Chrome verwendet dieselben Einstellungen wie **Internet Explorer**. Nach der Konfiguration von IE für SSO funktioniert **Chrome** ebenfalls. Zur Aktivierung der Delegierung von Anmeldedaten, die für das Durchsuchen von Netzwerkknoten von der Weboberfläche aus erforderlich ist, müssen Sie **Chrome** konfigurieren, damit dies unterstützt wird (**Internet Explorer** unterstützt dies standardmäßig):

1. Rufen Sie den Registry-Editor (**regedit32.exe**) auf
2. Navigieren Sie zu **`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome`**
3. Erstellen Sie die **`Google\Chrome`** -Schlüssel, falls diese noch nicht vorhanden sind.
   a. Klicken Sie mit der rechten Maustaste auf den Ordner 'Richtlinien', und wählen Sie **Neu** -> **Schlüssel**.
   b. Geben Sie als Ordnernamen **Google** ein.
   c. Klicken Sie mit der rechten Maustaste auf den Ordner **Google** , und wählen Sie **Neu** -> **Schlüssel**.
   d. Geben Sie als Ordnernamen **Chrome** ein.
   e. Klicken Sie auf den Ordner 'Chrome', und klicken Sie mit der rechten Maustaste im weißen Bereich rechts auf **Neu** -> **Zeichenfolgewert**.
   f. Geben Sie den Schlüsselnamen ein: **`AuthNegotiateDelegateWhitelist`**.
4. Legen Sie Ihren Domänennamen (z. B. **`ahsoka.acme.com`** oder **`*.acme.com`**) als Wert für den **`AuthNegotiateDelegateWhitelist`**-Registrierungsschlüssel fest.
5. Starten Sie Chrome neu.

Für Firefox:

1. Geben Sie **`about:config`** in die Adressleiste ein, und drücken Sie die Eingabetaste.
2. Suchen und bearbeiten Sie die Einstellung **`network.negotiate-auth.trusted-uris`** , und fügen Sie **`https://ahsoka.acme.com`** oder **`just .acme.com`** hinzu [die Liste ist komma-getrennt].

   Hinweis: *Verwenden Sie zum Hinzufügen aller Unterdomänen das Format „**`.example.com`**“ (**NICHT** **`*.example.com`**)*

3. Zur Aktivierung der Unterstützung von **Datenquellen** im Netzwerk müssen Sie auch **`network.negotiate-auth.delegation-uris`** bearbeiten, indem Sie **`ahsoka.acme.com`** oder einfach nur den Domänennamen (**`acme.com`**) hinzufügen.
4. Starten Sie **Firefox** neu.

Mac:

Hinweis: *Die nachfolgenden Schritte müssen für jeden Benutzer auf jedem Computer ausgeführt werden.*

Für Safari:

Der Vorgang funktioniert.

Für Firefox:

1. Geben Sie **`about:config`** in die Adressleiste ein, und drücken Sie die Eingabetaste.
2. Suchen und bearbeiten Sie die Einstellung **`network.negotiate-auth.trusted-uris`** , und fügen Sie **`https://ahsoka.acme.com`** oder **`just .acme.com`** hinzu [die Liste ist komma-getrennt].

   Hinweis: *Verwenden Sie zum Hinzufügen aller Unterdomänen das Format „**`.example.com`**“ (**NICHT** **`*.example.com`**)*

3. Zur Aktivierung der Unterstützung von **Datenquellen** im Netzwerk müssen Sie auch **`network.negotiate-auth.delegation-uris`** bearbeiten, indem Sie **`ahsoka.acme.com`** oder einfach nur den Domänennamen (**`acme.com`**) hinzufügen.
4. Starten Sie **Firefox** neu.

Für Chrome:

1. Mit der **Ticket Viewer**-Anwendung (**/System/Library/CoreServices/Ticket Viewer**) können Sie überprüfen, ob Sie über ein Kerberos-Ticket verfügen, und eines erstellen, sollte dies nicht automatisch erstellt worden sein.

   Hinweis: *Dies ist über das **Terminal** durch Eingabe von **`kinit`** und Ihres Kennworts möglich.*

2. Öffnen Sie zur Konfiguration der Chrome Whitelist für die Unterstützung der Authentifizierung für alle von Ihnen verwendeten Domänen das **Terminal**, und führen Sie die folgenden Befehle aus:

   ```
   $ defaults write com.google.Chrome AuthServerWhitelist “*.acme.com”
   $ defaults write com.google.Chrome AuthNegotiateDelegateWhitelist
   “*.acme.com”
   ```

3. Starten Sie den Chrome-Browser neu.

12.2.7.2 Files Advanced Server und Gateway auf unterschiedlichen Computern

Themen

Dies ist ein einmaliger Schritt, der für die Registrierung von Files Advanced Server für den Kerberos-Server in der Domäne ausgeführt werden muss. Wir geben mit 'setspn.exe' an, welches LDAP-Konto für SSO-Authentifizierungsprüfungen abgefragt wird.

Hinweis: *Wenn Sie* ***mobile Clients mit Zertifikatsauthentifizierung*** *verwenden möchten, dürfen die DNS-Einträge für die Access- und Gateway Server* ***NICHT*** *mit dem Namen des Computers identisch sein. Wenn der SPN des Files Advanced Servers nur im Namen des Computers enthalten ist, behandelt der Gateway Server den Files Advanced Server, als wäre er auf seinem Gerät installiert und versucht daher keine Kerberos-Authentifizierung.*

z.B.: ***`machineAccess.domain.com / machineGW.domain.com`*** *funktioniert*

z.B.: ***`machine.domain.com/ computer.domain.com will`*** *funktioniert NICHT*

Das LDAP-Konto konfigurieren, das SSO handhabt

Hinweis: *Wenn Sie SMB- oder SharePoint-Datenquellen nutzen möchten, müssen Sie das Active Directory-Konto so konfigurieren, dass Kerberos-Delegierung für all Ihre SMB- und SharePoint-Datenquellen erlaubt wird. Weitere Informationen finden Sie im Artikel Erweiterte Delegierungskonfigurationen.*

1. Öffnen Sie eine Eingabeaufforderung.

   Hinweis: *Sie müssen mit einem Domänenkonto angemeldet sein und über die Rechte zur Verwendung von* ***setspn*** *verfügen.*

2. Geben Sie den Befehl **`setspn -s HTTP/Computername.Domänenname.com Kontoname`** ein.

   z. B. Ist Ihr Files Advanced Server unter **`ahsoka.acme.com`** installiert und möchten Sie **`john@acme.com`** als vorab authentifiziertes LDAP-Konto zur Gewährung von Kerberos-Tickets verwenden, sieht der Befehl folgendermaßen aus:

   ```
   setspn -s HTTP/ahsoka.acme.com john
   ```

   Hinweis: *Der im obigen Befehl verwendete LDAP-Kontoname* ***MUSS*** *mit dem Konto übereinstimmen, das Sie über die Eigenschaft* ***`spnego.preauth.username`*** *in* ***`web.xml`*** *angeben.*

   Hinweis: *Dieses Konto entspricht in der Regel dem vom Administrator in der Files Advanced-Weboberfläche unter* ***Allgemeine Einstellungen*** *->* ***LDAP*** *->* ***LDAP-Benutzername*** */* ***LDAP-Kennwort*** *angegebenen LDAP-Konto. Dies ist jedoch nicht zwingend der Fall.*

3. Wird Ihr Files Advanced Server auf einem Nicht-Standard-Port (d. h., einem anderen Port als 443) ausgeführt, sollten Sie auch einen SPN mit der Portnummer registrieren.

   Beispiel: Läuft Ihr Server an Port 444, lautet der Befehl folgendermaßen:

   ```
   setspn -s HTTP/ahsoka.acme.com:444 john
   ```

   Hinweis*:* ***HTTP*** *in den voranstehenden Befehlen bezieht sich auf die* ***HTTP****-Dienstklasse und nicht auf das* ***HTTP****-Protokoll. Die* ***HTTP****-Dienstklasse verarbeitet* ***HTTP****- und* ***HTTPS****-Anforderungen. Sie müssen und* ***sollten KEINEN*** *SPN mit* ***HTTPS*** *als Dienstklassenname erstellen.*

4. Wechseln Sie zum Domain-Controller und öffnen Sie **Active Directory-Benutzer und -Computer**.
5. Suchen Sie den in den voranstehenden Befehlen verwendeten Benutzer (in diesem Beispiel **john**).
6. Klicken Sie auf die Registerkarte **Delegierung** und wählen Sie **Diesem Benutzer für die Delegierung an jeden beliebigen Dienst trauen (nur Kerberos)** aus.
7. Wählen Sie **OK**.

Den SPN für den Gateway Server konfigurieren

Damit der KDC („Key Distribution Center“) Kerberos-Server Benutzer für den Gateway-Server authentifizieren kann, muss der Gateway-Dienst für den KDC registriert werden. Hierzu müssen

„setspn“ und der Hostname des Servers angegeben werden, auf dem er als 'user' im setspn-Befehl läuft.

Gateway Server, die auf anderen Computern als dem Files Advanced Server gehostet werden

1. Öffnen Sie die Eingabeaufforderung.
2. Geben Sie den folgenden **setspn**-Befehl ein: **`setspn -s HTTP/Computername.Domäne.com Computername`**

   Führen Sie beispielsweise für den Fall, dass Ihr Gateway Server auf Host **`'cody'`** in der Domäne läuft, folgenden Befehl aus:

   `setspn -s HTTP/cody.acme.com cody`
3. Läuft Ihr Gateway Server nicht an einem Standard-Port (d. h. an einem anderen Port als 443), müssen Sie auch einen SPN mit der Portnummer registrieren, z. B. dann, wenn Ihr Gateway Server an Port 444 läuft:

   `setspn -s HTTP/cody.acme.com:444 cody`
4. Wiederholen Sie diesen Abschnitt für alle Gateway-Server.

Gateway Server auf demselbem Computer wie der Files Advanced Server

Dies ist nur erforderlich, wenn der Gateway Server auf demselben Computer wie der Files Advanced Server gehostet wird. Ist dies nicht der Fall, überspringen Sie diesen Abschnitt. Für diese Konfiguration müssen Sie einen zusätzlichen DNS-Eintrag für Ihren Gateway-Server festlegen.

1. Öffnen Sie auf Ihrem DNS-Server die **Vorwärtssuchbereiche** für Ihre Domäne, klicken Sie mit der rechten Maustaste, und erstellen Sie einen neuen **Host**-Eintrag **`(A record)`** für den Gateway-Server.
2. Geben Sie einen Namen ein. Dabei handelt es sich um die DNS-Adresse, die zum Erreichen des Gateway-Servers verwendet wird.

   Beispiel: `codygw.acme.com`
3. Geben Sie die IP-Adresse des Gateway Servers ein (ohne den Port). Wenn Sie den Gateway und den Files Advanced Server unter derselben IP-Adresse ausführen, geben Sie diese IP-Adresse ein.
4. Wählen Sie **Zugewiesenen Pointer (PTR)-Datensatz erstellen** und drücken Sie **Host hinzufügen**.
5. Wechseln Sie zurück zum Computer mit Files Advanced.
6. Öffnen Sie die Eingabeaufforderung.
7. Geben Sie den folgenden **setspn**-Befehl ein: **`setspn -s HTTP/GatewayDNS.Domäne.com Computername`**

   Führen Sie beispielsweise für den Fall, dass Ihr Gateway Server auf Host **`'cody'`** in der Domäne läuft und Ihr DNS-Eintrag **`codygw.acme.com`** lautet, folgenden Befehl aus:

   `setspn -s HTTP/codygw.acme.com cody`
8. Läuft Ihr Gateway Server nicht an einem Standard-Port (d. h. an einem anderen Port als 443), müssen Sie auch einen SPN mit der Portnummer registrieren, z. B. dann, wenn Ihr Gateway Server an Port 444 läuft:

   `setspn -s HTTP/codygw.acme.com:444 cody`
9. Falls nicht bereits geschehen, müssen Sie die **Adresse für die Administration** Ihres gewünschten Gateway-Servers in den in Schritt 4 erstellten Gateway Server-DNS-Eintrag ändern.

Die Datei `web.xml` **bearbeiten:**

1. Navigieren Sie zu **`C:\Program Files (x86)\Acronis\Files Advanced\Access server\Web Application\WEB-INF\`**
2. Suchen und öffnen Sie die Datei **`web.xml`**. In dieser Datei geben Sie den Benutzernamen und das Kennwort für die Domäne an, unter der der SSO-Dienst läuft. Das Konto **muss** mit dem Konto übereinstimmen, das Sie im Abschnitt **In der Domäne** zur Registrierung des HTTP-Dienstes für Kerberos verwendet haben.
3. In **`web.xml`** müssen zwei Eigenschaften eingerichtet werden – der vom SSO-Dienst zu verwendende Benutzername für die Domäne und das zugehörige Kennwort. Suchen Sie die folgenden Zeilen:

```
<init-param>
    <param-name>spnego.preauth.username</param-name>
    <param-value>ihrbenutzername</param-value>
 </init-param>
 <init-param>
    <param-name>spnego.preauth.password</param-name>
    <param-value>ihrkennwort</param-value>
 </init-param>
```

4. Ersetzen Sie **ihrbenutzername** durch den gewünschten LDAP-Benutzernamen.
5. Ersetzen Sie **ihrkennwort** durch das LDAP-Kennwort für das zuvor angegebene LDAP-Konto. Wenn Ihr Kennwort eines der fünf folgenden Sonderzeichen enthält, **&**, **>**, **"**, ' , or **<**, dann müssen Sie diese zunächst im XML-Dokument escapen. Dazu müssen Sie sie folgendermaßen ersetzen:
   - **<** durch **<**
   - **>** durch **>**
   - **'** durch **"**
   - **,** durch **'**
   - **&** durch **&**

   Wenn Ihr Passwort also **`<my&best'password"`** lautet, müssen Sie es in der Datei **`web.xml`** folgendermaßen schreiben: **`<my&best'password"`**

Die Datei `krb5.conf` **bearbeiten:**

1. Navigieren Sie zu **`C:\Program Files (x86)\Acronis\Files Advanced\Common\apache-tomcat-7.0.59\conf`**
2. Suchen und öffnen Sie die Datei **`krb5.conf`**
3. In **`krb5.conf`** gibt es nur zwei Eigenschaften, die der Administrator angeben muss:
   a. Die Domäne für Single Sign-On (z.B. **`ACME.COM`**)

   Hinweis: *Die Domäne in* ***`krb5.conf`*** *muss immer in* ***GROSSBUCHSTABEN*** *angegeben werden. Andernfalls schlagen Suchen nach Kerberos-Tickets möglicherweise fehl.*

   b. Die Adresse des Kerberos Key Distribution Centers (entspricht üblicherweise der Adresse Ihres primären Domänencontrollers, z.B. **`acmedc.ACME.COM`**)
4. Die von uns installierte **`krb5.conf`**-Datei sieht folgendermaßen aus:

```
[libdefaults]
    default_realm = ACME.COM
```

```
        default_tkt_enctypes = aes128-cts rc4-hmac des3-cbc-sha1 des-cbc-md5
des-cbc-crc
        default_tgs_enctypes = aes128-cts rc4-hmac des3-cbc-sha1 des-cbc-md5
des-cbc-crc
        permitted_enctypes   = aes128-cts rc4-hmac des3-cbc-sha1 des-cbc-md5
des-cbc-crc

    [realms]
        ACME.COM = {
            kdc = acmedc.ACME.COM
            default_domain = ACME.COM

    [domain_realm]
        .ACME.COM = ACME.COM
```

5. Ersetzen Sie alle Instanzen von **ACME.COM** durch Ihre Domäne (**in Großbuchstaben!**).
6. Ersetzen Sie den Wert für '**kdc =**' durch den Namen Ihres Domänencontrollers. Die Domäne muss in Großbuchstaben angegeben werden, z.B. **kdc = yourdc.YOURDOMAIN.COM**
7. Nach der Aktualisierung der oben genannten Konfigurationsdateien muss der Files Advanced Server (der Files Advanced Tomcat-Dienst) neu gestartet werden, damit die Änderungen wirksam werden.

Single Sign-On in der Weboberfläche aktivieren:

1. Rufen Sie die Weboberfläche von Files Advanced auf und melden Sie sich als Administrator an.
2. Erweitern Sie die Registerkarte **Allgemeine Einstellungen**, und öffnen Sie die Seite **LDAP**.
3. Aktivieren Sie unten auf der Seite das Kontrollkästchen **Anmelden vom Webclient und Desktop Sync Client mit vorhandenen Windows-/Mac-Anmeldedaten erlauben**.
4. Drücken Sie **Speichern**.

Auf dem Computer eines Benutzers

Hierbei handelt es sich um eine kleine, einmalig auf dem Client-Computer durchzuführende Konfiguration zur Aktivierung der Single Sign-On-Unterstützung für Ihren Browser.

Hinweis: *Die nachfolgenden Schritte müssen für jeden Benutzer auf jedem Computer ausgeführt werden.*

Hinweis: *Wenn Dienste in mehreren Domänen vorliegen, wiederholen Sie den Abschnitt für Ihren Browser mit dem zweiten Domänennamen.* ***Beispiel:*** *Sowohl* ****.acme.com*** *als auch* ****.tree.com*** *hinzufügen.*

Windows:

Für Internet Explorer:

- Rufen Sie Internet Explorer auf, wechseln Sie zu **Extras** -> **Internetoptionen** -> **Sicherheit** -> **Lokales Intranet** -> **Sites** -> **Erweitert**, und fügen Sie die Adresse Ihres Files Advanced Servers hinzu, z. B. **https://ahsoka.acme.com (** oder einfach ***.acme.com)**, und starten Sie den Browser neu.

Für Chrome:

Chrome verwendet dieselben Einstellungen wie **Internet Explorer**. Nach der Konfiguration von IE für SSO funktioniert **Chrome** ebenfalls. Zur Aktivierung der Delegierung von Anmeldedaten, die für das Durchsuchen von Netzwerkknoten von der Weboberfläche aus erforderlich ist, müssen Sie **Chrome** konfigurieren, damit dies unterstützt wird (**Internet Explorer** unterstützt dies standardmäßig):

1. Rufen Sie den Registry-Editor (**regedit32**.**exe**) auf
2. Navigieren Sie zu **`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome`**
3. Erstellen Sie die **`Google\Chrome`** -Schlüssel, falls diese noch nicht vorhanden sind.
   a. Klicken Sie mit der rechten Maustaste auf den Ordner 'Richtlinien', und wählen Sie **Neu** -> **Schlüssel**.
   b. Geben Sie als Ordnernamen **Google** ein.
   c. Klicken Sie mit der rechten Maustaste auf den Ordner **Google** , und wählen Sie **Neu** -> **Schlüssel**.
   d. Geben Sie als Ordnernamen **Chrome** ein.
   e. Klicken Sie auf den Ordner 'Chrome', und klicken Sie mit der rechten Maustaste im weißen Bereich rechts auf **Neu** -> **Zeichenfolgewert**.
   f. Geben Sie den Schlüsselnamen ein: **`AuthNegotiateDelegateWhitelist`**.
4. Legen Sie Ihren Domänennamen (z. B. **`ahsoka.acme.com`** oder **`*.acme.com`**) als Wert für den **`AuthNegotiateDelegateWhitelist`**-Registrierungsschlüssel fest.
5. Starten Sie Chrome neu.

Für Firefox:

1. Geben Sie **`about:config`** in die Adressleiste ein, und drücken Sie die Eingabetaste.
2. Suchen und bearbeiten Sie die Einstellung **`network.negotiate-auth.trusted-uris`** , und fügen Sie **`https://ahsoka.acme.com`** oder **`just .acme.com`** hinzu [die Liste ist komma-getrennt].

   Hinweis: *Verwenden Sie zum Hinzufügen aller Unterdomänen das Format „**`.example.com`**“ (**NICHT** **`*.example.com`**)*

3. Zur Aktivierung der Unterstützung von **Datenquellen** im Netzwerk müssen Sie auch **`network.negotiate-auth.delegation-uris`** bearbeiten, indem Sie **`ahsoka.acme.com`** oder einfach nur den Domänennamen (**`acme.com`**) hinzufügen.
4. Starten Sie **Firefox** neu.

Mac:

Hinweis: *Die nachfolgenden Schritte müssen für jeden Benutzer auf jedem Computer ausgeführt werden.*

Für Safari:

Der Vorgang funktioniert.

Für Firefox:

1. Geben Sie **`about:config`** in die Adressleiste ein, und drücken Sie die Eingabetaste.

2. Suchen und bearbeiten Sie die Einstellung **`network.negotiate-auth.trusted-uris`**, und fügen Sie **`https://ahsoka.acme.com`** oder **`just .acme.com`** hinzu [die Liste ist komma-getrennt].

   Hinweis: *Verwenden Sie zum Hinzufügen aller Unterdomänen das Format „**`.example.com`**“ (**NICHT** **`*.example.com`**)*

3. Zur Aktivierung der Unterstützung von **Datenquellen** im Netzwerk müssen Sie auch **`network.negotiate-auth.delegation-uris`** bearbeiten, indem Sie **`ahsoka.acme.com`** oder einfach nur den Domänennamen (**`acme.com`**) hinzufügen.
4. Starten Sie **Firefox** neu.

Für Chrome:

1. Mit der **Ticket Viewer**-Anwendung (**/System/Library/CoreServices/Ticket Viewer**) können Sie überprüfen, ob Sie über ein Kerberos-Ticket verfügen, und eines erstellen, sollte dies nicht automatisch erstellt worden sein.

   Hinweis: *Dies ist über das **Terminal** durch Eingabe von **`kinit`** und Ihres Kennworts möglich.*

2. Öffnen Sie zur Konfiguration der Chrome Whitelist für die Unterstützung der Authentifizierung für alle von Ihnen verwendeten Domänen das **Terminal**, und führen Sie die folgenden Befehle aus:

   ```
   $ defaults write com.google.Chrome AuthServerWhitelist “*.acme.com”
   $ defaults write com.google.Chrome AuthNegotiateDelegateWhitelist
   “*.acme.com”
   ```

3. Starten Sie den Chrome-Browser neu.

12.2.7.3 Files Advanced in einer Domänengesamtstruktur

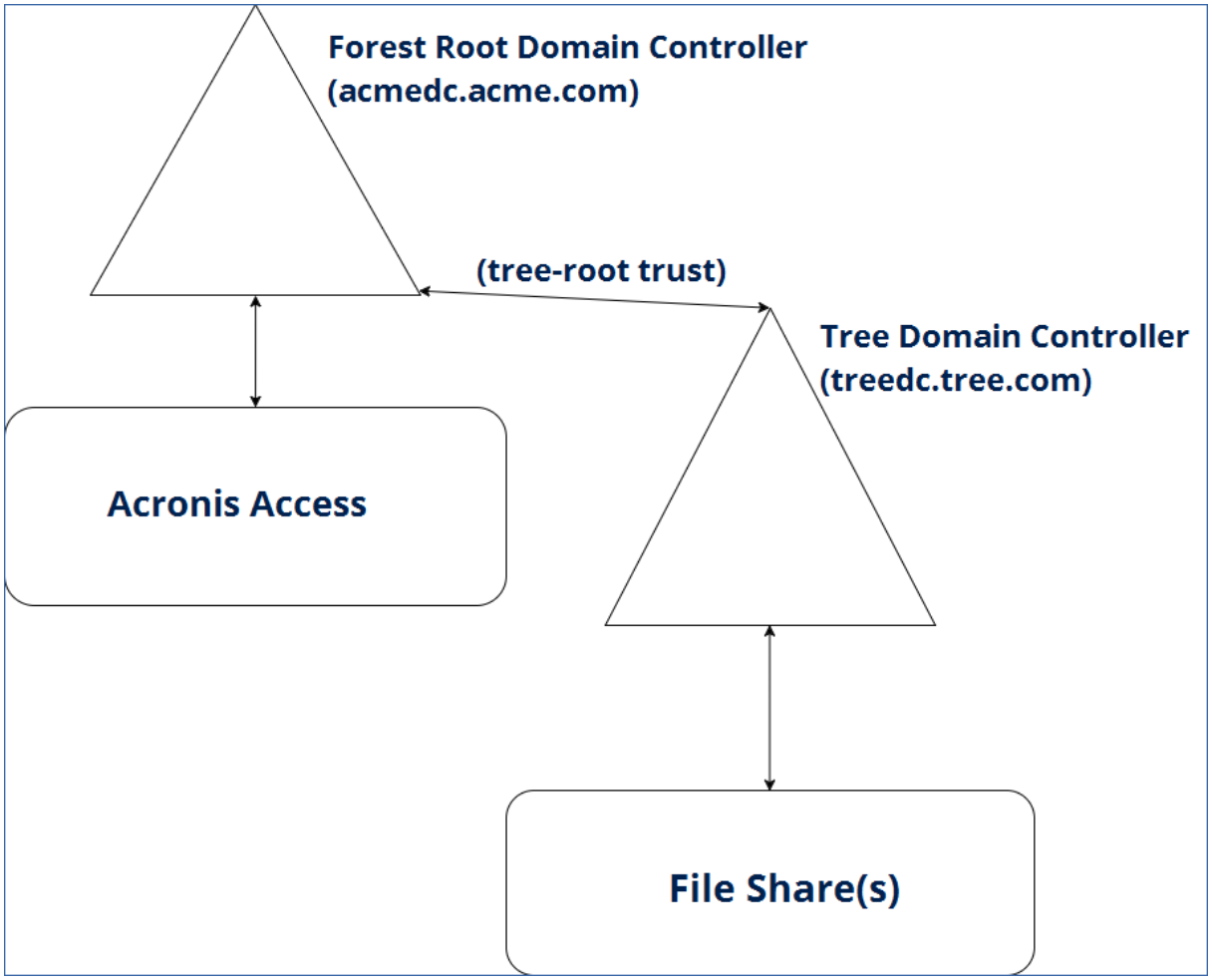
Ab Windows Server 2012 hat Microsoft die **Ressourcenbasierte eingeschränkte Kerberos-Delegierung** hinzugefügt, mit der die Delegierung in Gesamtdomänen durchgeführt werden kann. Damit können Bereitstellungen Single Sign-on auch verwenden, wenn sie Ressourcen in mehreren Domänen haben (in derselben Struktur), ohne dass ein Gateway Server auf den Ressourcen installiert werden muss.

Hinweis: *Damit diese Funktion verwendet werden kann, müssen alle Domänen in der Gesamtstruktur mindestens in der **Domänenfunktionsebene 2012** ausgeführt werden.*

Dieser Artikel leitet Sie durch folgende Verfahren:

- Einrichten des Files Advanced Server für SSO.
- Einrichten des Gateway Servers für SSO.
- Alle Konfigurationen in Ihrer Domäne, damit die eingeschränkte Delegierung in der Gesamtstruktur durchgeführt werden kann.

- Das Setup, das Benutzer durchführen müssen, um SSO verwenden zu können.



Themen

Anforderungen

Diese Anleitung ist für die Konfiguration in mehreren Domänen in einer einzigen Gesamtstruktur bestimmt. Es wird daher vorausgesetzt, dass LDAP ordnungsgemäß konfiguriert wurde, dass Benutzer sich an der Domäne problemlos anmelden können und dass die Konnektivität zwischen den Domänen in der Gesamtstruktur ordnungsgemäß konfiguriert wurde.

- Dieser Typ der eingeschränkten Delegierung ist nur bei Domänencontrollern verfügbar, die mindestens in der **Domänenfunktionsebene 2012** ausgeführt werden. Windows Server 2012 ist das erste Programm, das die ressourcenbasierte eingeschränkte Kerberos-Delegierung erlaubt.
- Der **Globale Katalog** muss aktiviert sein und ausgeführt werden.

Auf dem Computer eines Benutzers

Hierbei handelt es sich um eine kleine, einmalig auf dem Client-Computer durchzuführende Konfiguration zur Aktivierung der Single Sign-On-Unterstützung für Ihren Browser.

Hinweis: *Die nachfolgenden Schritte müssen für jeden Benutzer auf jedem Computer ausgeführt werden.*

Hinweis: *Wenn Dienste in mehreren Domänen vorliegen, wiederholen Sie den Abschnitt für Ihren Browser mit dem zweiten Domänennamen.* ***Beispiel:*** *Sowohl* ***`*.acme.com`*** *als auch* ***`*.tree.com`*** *hinzufügen.*

Windows:

Für Internet Explorer:

- Rufen Sie Internet Explorer auf, wechseln Sie zu **Extras** -> **Internetoptionen** -> **Sicherheit** -> **Lokales Intranet** -> **Sites** -> **Erweitert**, und fügen Sie die Adresse Ihres Files Advanced Servers hinzu, z. B. **`https://ahsoka.acme.com`** (oder einfach **`*.acme.com`**), und starten Sie den Browser neu.

Für Chrome:

Chrome verwendet dieselben Einstellungen wie **Internet Explorer**. Nach der Konfiguration von IE für SSO funktioniert **Chrome** ebenfalls. Zur Aktivierung der Delegierung von Anmeldedaten, die für das Durchsuchen von Netzwerkknoten von der Weboberfläche aus erforderlich ist, müssen Sie **Chrome** konfigurieren, damit dies unterstützt wird (**Internet Explorer** unterstützt dies standardmäßig):

1. Rufen Sie den Registry-Editor (**regedit32**.**exe**) auf
2. Navigieren Sie zu **`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome`**
3. Erstellen Sie die **`Google\Chrome`** -Schlüssel, falls diese noch nicht vorhanden sind.
   a. Klicken Sie mit der rechten Maustaste auf den Ordner 'Richtlinien', und wählen Sie **Neu** -> **Schlüssel**.
   b. Geben Sie als Ordnernamen **Google** ein.
   c. Klicken Sie mit der rechten Maustaste auf den Ordner **Google** , und wählen Sie **Neu** -> **Schlüssel**.
   d. Geben Sie als Ordnernamen **Chrome** ein.
   e. Klicken Sie auf den Ordner 'Chrome', und klicken Sie mit der rechten Maustaste im weißen Bereich rechts auf **Neu** -> **Zeichenfolgewert**.
   f. Geben Sie den Schlüsselnamen ein: **`AuthNegotiateDelegateWhitelist`**.
4. Legen Sie Ihren Domänennamen (z. B. **`ahsoka.acme.com`** oder **`*.acme.com`**) als Wert für den **`AuthNegotiateDelegateWhitelist`**-Registrierungsschlüssel fest.
5. Starten Sie Chrome neu.

Für Firefox:

1. Geben Sie **`about:config`** in die Adressleiste ein, und drücken Sie die Eingabetaste.
2. Suchen und bearbeiten Sie die Einstellung **`network.negotiate-auth.trusted-uris`** , und fügen Sie **`https://ahsoka.acme.com`** oder **`just .acme.com`** hinzu [die Liste ist komma-getrennt].

__Hinweis:__ Verwenden Sie zum Hinzufügen aller Unterdomänen das Format „__.example.com__“ (__NICHT__ __.example.com__)*

3. Zur Aktivierung der Unterstützung von **Datenquellen** im Netzwerk müssen Sie auch **network.negotiate-auth.delegation-uris** bearbeiten, indem Sie **ahsoka.acme.com** oder einfach nur den Domänennamen (**acme.com**) hinzufügen.
4. Starten Sie **Firefox** neu.

Mac:

__Hinweis:__ Die nachfolgenden Schritte müssen für jeden Benutzer auf jedem Computer ausgeführt werden.

Für Safari:

Der Vorgang funktioniert.

Für Firefox:

1. Geben Sie **about:config** in die Adressleiste ein, und drücken Sie die Eingabetaste.
2. Suchen und bearbeiten Sie die Einstellung **network.negotiate-auth.trusted-uris** , und fügen Sie **https://ahsoka.acme.com** oder **just .acme.com** hinzu [die Liste ist komma-getrennt].

   __Hinweis:__ Verwenden Sie zum Hinzufügen aller Unterdomänen das Format „__.example.com__“ (__NICHT__ __.example.com__)*

3. Zur Aktivierung der Unterstützung von **Datenquellen** im Netzwerk müssen Sie auch **network.negotiate-auth.delegation-uris** bearbeiten, indem Sie **ahsoka.acme.com** oder einfach nur den Domänennamen (**acme.com**) hinzufügen.
4. Starten Sie **Firefox** neu.

Für Chrome:

1. Mit der **Ticket Viewer**-Anwendung (**/System/Library/CoreServices/Ticket Viewer**) können Sie überprüfen, ob Sie über ein Kerberos-Ticket verfügen, und eines erstellen, sollte dies nicht automatisch erstellt worden sein.

   __Hinweis:__ Dies ist über das __Terminal__ durch Eingabe von __kinit__ und Ihres Kennworts möglich.

2. Öffnen Sie zur Konfiguration der Chrome Whitelist für die Unterstützung der Authentifizierung für alle von Ihnen verwendeten Domänen das **Terminal**, und führen Sie die folgenden Befehle aus:

   $ defaults write com.google.Chrome AuthServerWhitelist “*.acme.com”

   $ defaults write com.google.Chrome AuthNegotiateDelegateWhitelist “*.acme.com”

3. Starten Sie den Chrome-Browser neu.

Für den Files Advanced Server

Themen

4.

1. Navigieren Sie zu **C:\Program Files (x86)\Acronis\Files Advanced\Access Server\Web Application\WEB-INF**
2. Suchen und öffnen Sie die Datei **web.xml**. In dieser Datei geben Sie den Benutzernamen und das Kennwort für die Domäne an, unter der der SSO-Dienst läuft.

   Dieses Konto **muss** dem Konto entsprechen, dass Sie verwenden, um den **HTTP**-Dienst mit Kerberos in den folgenden Abschnitten zu registrieren. Es wird daher empfohlen, es zu notieren.
3. In **web.xml** müssen zwei Eigenschaften eingerichtet werden – der vom SSO-Dienst zu verwendende Benutzername für die Domäne und das zugehörige Kennwort. Suchen Sie die folgenden Zeilen:

```
<init-param>
    <param-name>spnego.preauth.username</param-name>
    <param-value>ihrbenutzername</param-value>
 </init-param>
 <init-param>
    <param-name>spnego.preauth.password</param-name>
    <param-value>ihrkennwort</param-value>
 </init-param>
```

4. Ersetzen Sie **ihrbenutzername** durch den gewünschten LDAP-Benutzernamen.
5. Ersetzen Sie **ihrkennwort** durch das LDAP-Kennwort für das zuvor angegebene LDAP-Konto. Wenn Ihr Kennwort eines der fünf folgenden Sonderzeichen enthält, **&**, **>**, **"**, ' , or **<**, dann müssen Sie diese zunächst im XML-Dokument escapen. Dazu müssen Sie sie folgendermaßen ersetzen:
   - **<** durch **<**
   - **>** durch **>**
   - **'** durch **"**
   - **,** durch **'**
   - **&** durch **&**

   Beispiel: Wenn Ihr Kennwort **<my&best'password"** ist, müssen Sie es in der Datei **web.xml** wie folgt schreiben: **<my&best'password"**
1. Navigieren Sie zu **C:\Program Files (x86)\Acronis\Files Advanced\Common\apache-tomcat-7.0.59\conf**
2. Suchen und öffnen Sie die Datei **krb5.conf**
3. In **krb5.conf** gibt es nur zwei Eigenschaften, die der Administrator angeben muss:
   a. Die Domäne für SSO (z.B. **ACME.COM**).
      - Dies muss die Domäne sein, in der sich der Files Advanced Web Server und die Gateway Server befinden.
      - Beachten Sie, dass es sich um den Namen Ihrer Domäne handelt, **nicht** um den DNS-Namen des Servers.

   Hinweis: *Die Domäne in* ***krb5.conf*** *muss immer in* ***GROSSBUCHSTABEN*** *angegeben werden. Andernfalls schlagen Suchen nach Kerberos-Tickets möglicherweise fehl.*

   b. Die Adresse des Kerberos Key Distribution Centers (entspricht üblicherweise der **DNS**-Adresse Ihres primären Domänencontrollers, z. B. **acmedc.ACME.COM**) Dies ist die Adresse des Domänencontrollers in der Domäne, in der sich Files Advanced und die zugehörigen Komponenten befinden.
4. Die von uns installierte **krb5.conf**-Datei sieht folgendermaßen aus:

```
[libdefaults]
```

```
        default_realm = ACME.COM
        default_tkt_enctypes = aes128-cts rc4-hmac des3-cbc-sha1 des-cbc-md5
des-cbc-crc
        default_tgs_enctypes = aes128-cts rc4-hmac des3-cbc-sha1 des-cbc-md5
des-cbc-crc
        permitted_enctypes   = aes128-cts rc4-hmac des3-cbc-sha1 des-cbc-md5
des-cbc-crc

    [realms]
        ACME.COM = {
            kdc = acmedc.ACME.COM
            default_domain = ACME.COM

    [domain_realm]
        .ACME.COM = ACME.COM
```

5. Ersetzen Sie alle Instanzen von **`ACME.COM`** durch Ihre Domäne (**in Großbuchstaben!**). Beachten Sie, dass es sich um den Namen Ihrer Domäne handelt, **nicht** um den DNS-Namen des Servers.
6. Ersetzen Sie den Wert für '**`kdc =`**' durch den DNS-Namen Ihres Domänencontrollers. Der Domänenanteil muss in Großbuchstaben angegeben werden, z. B. **`kdc = yourdc.YOURDOMAIN.COM`**.
7. Nach der Aktualisierung der oben genannten Konfigurationsdateien muss der Files Advanced Server (der Files Advanced Tomcat-Dienst) neu gestartet werden, damit die Änderungen wirksam werden.

1. Rufen Sie die Weboberfläche von Files Advanced auf und melden Sie sich als Administrator an.
2. Erweitern Sie die Registerkarte **Allgemeine Einstellungen**, und öffnen Sie die Seite **LDAP**.
3. Aktivieren Sie unten auf der Seite das Kontrollkästchen **Anmelden vom Webclient und Desktop Sync Client mit vorhandenen Windows-/Mac-Anmeldedaten erlauben**.
4. Drücken Sie **Speichern**.

Einen zusätzlichen DNS-Eintrag für den Files Advanced Web Server konfigurieren

Wenn auf diesem Computer ein Gateway Server vorliegt, müssen Sie einen separaten DNS-Eintrag für den Files Advanced Web Server haben.

1. Öffnen Sie auf Ihrem DNS-Server die **Vorwärtssuchbereiche** für Ihre Domäne, klicken Sie mit der rechten Maustaste, und erstellen Sie einen neuen **Host**-Eintrag **`(A record)`** für den Files Advanced Web Server.
2. Geben Sie einen Namen ein. Dabei handelt es sich um die DNS-Adresse, die zum Erreichen des Files Advanced Web Servers verwendet wird.

   Beispiel: `ahsokaccess.acme.com`
3. Geben Sie die IP-Adresse des Files Advanced Web Server ein (ohne den Port). Wenn Sie den Gateway und den Files Advanced Web Server unter derselben IP-Adresse ausführen, geben Sie diese IP-Adresse ein.
4. Wählen Sie **Zugewiesenen Pointer (PTR)-Datensatz erstellen** und drücken Sie **Host hinzufügen**.

Geben Sie den SPN für den Files Advanced Web Server ein.

1. Öffnen Sie auf dem Computer, auf dem Files Advanced ausgeführt wird, die Eingabeaufforderung.

   Hinweis: *Sie müssen mit einem Domänenkonto angemeldet sein und über die Rechte zur Verwendung von* ***setspn*** *verfügen.*

2. Geben Sie folgenden Befehl ein: **`setspn –s HTTP/access_DNS_name.domain.com account name`**

   Hinweis: *Der im obigen Befehl verwendete LDAP-Kontoname* ***MUSS*** *mit dem Konto übereinstimmen, das Sie in der Datei* ***`web.xml`*** *angegeben haben.*

   - Ist Ihr Files Advanced Web Server beispielsweise unter **`ahsoka.acme.com`** installiert und möchten Sie **`john@acme.com`** als vorab authentifiziertes LDAP-Konto zur Gewährung von Kerberos-Tickets verwenden, sieht der Befehl folgendermaßen aus:
     `setspn -s HTTP/ahsokaaccess.acme.com john`
   - Ist Ihr Files Advanced Web Server beispielsweise unter **`ahsoka.acme.com`** installiert und möchten Sie **`jane@tree.com`** als vorab authentifiziertes LDAP-Konto zur Gewährung von Kerberos-Tickets verwenden, sieht der Befehl folgendermaßen aus:
     `setspn -s HTTP/ahsokaaccess.acme.com tree\jane`

   Hinweis: *Dieses Konto entspricht typischerweise dem LDAP-Konto, das vom Administrator in der Files Advanced Weboberfläche in den* ***LDAP-Einstellungen*** *festgelegt wurde, ist aber nicht obligatorisch.*

3. Wird Ihr Files Advanced Web Server auf einem Nicht-Standard-Port (d. h., einem anderen Port als 443) ausgeführt, sollten Sie auch einen SPN mit der Portnummer registrieren.

   Beispiel: Läuft Ihr Server an Port 444, lautet der Befehl folgendermaßen:
   `setspn -s HTTP/ahsokaaccess.acme.com:444 john` ODER
   `setspn -s HTTP/ahsokaaccess.acme.com:444 tree\jane`

   Hinweis*:* ***HTTP*** *in den voranstehenden Befehlen bezieht sich auf die* ***HTTP****-Dienstklasse und nicht auf das* ***HTTP****-Protokoll. Die* ***HTTP****-Dienstklasse verarbeitet* ***HTTP****- und* ***HTTPS****-Anforderungen. Sie müssen und* ***sollten KEINEN*** *SPN mit* ***HTTPS*** *als Dienstklassenname erstellen.*

4. Wechseln Sie zum Domain-Controller, auf dem sich Ihre Benutzer befinden, und öffnen Sie **Active Directory-Benutzer und -Computer**. Wenn Sie mehrere Domänen mit Benutzern haben, öffnen Sie die mit dem Benutzer, der in den vorherigen Schritten verwendet wurde.
5. Suchen Sie den in den voranstehenden Befehlen verwendeten Benutzer (in diesem Beispiel **john** oder **jane**).
6. Klicken Sie auf die Registerkarte **Delegierung** und wählen Sie **Diesem Benutzer für die Delegierung an jeden beliebigen Dienst trauen (nur Kerberos)** aus. Durch das Aktivieren dieser Einstellung kann das LDAP-Objekt die Authentifizierung an alle Dienste delegieren. In unserem Fall ist dies der Gateway Server-Dienst.
7. Wählen Sie **OK**.

Überprüfen, ob Sie sich bei Files Advanced anmelden können

1. Wechseln Sie zu einem anderen Computer als dem Domänencontroller oder Ihrem Files Advanced Web Server.
2. Öffnen Sie die Files Advanced Webkonsole und verwenden Sie den Link unter dem Kennwortfeld auf der Anmeldeseite.

Hinweis: *Sie müssen an dem Computer mit einem Domänenbenutzer angemeldet sein, der entweder für Files Advanced eingeladen wurde, bereits angemeldet ist oder ein Mitglied einer bereitgestellten LDAP-Gruppe ist.*

Hinweis: *Führen Sie die Verfahren unter Auf dem Computer eines Benutzers durch, damit Ihr Browser die SSO-Anforderungen erfüllen kann.*

Für den Gateway Server

Themen

Damit der KDC ('Key Distribution Center') Kerberos-Server Benutzer für den Gateway Server authentifizieren kann, muss der Gateway-Dienst für den KDC registriert werden. Hierzu müssen **setspn** und der Hostname des Servers angegeben werden, auf dem er als 'user' im **setspn**-Befehl läuft.

Einen zusätzlichen DNS-Eintrag für den Gateway Server konfigurieren

Damit diese Konfiguration funktioniert, müssen Sie auch über einen separaten DNS-Eintrag für Ihren Gateway Server verfügen.

1. Öffnen Sie auf Ihrem DNS-Server die **Vorwärtssuchbereiche** für Ihre Domäne, klicken Sie mit der rechten Maustaste, und erstellen Sie einen neuen **Host**-Eintrag **`(A record)`** für den Gateway-Server.
2. Geben Sie einen Namen ein. Dabei handelt es sich um die DNS-Adresse, die zum Erreichen des Gateway-Servers verwendet wird.

   Beispiel: `codygw.acme.com`
3. Geben Sie die IP-Adresse des Gateway Servers ein (ohne den Port). Wenn Sie den Gateway und den Files Advanced Server unter derselben IP-Adresse ausführen, geben Sie diese IP-Adresse ein.
4. Wählen Sie **Zugewiesenen Pointer (PTR)-Datensatz erstellen** und drücken Sie **Host hinzufügen**.

Den SPN für den lokalen Gateway Server konfigurieren

1. Wechseln Sie zum Computer mit Files Advanced.
2. Öffnen Sie die Eingabeaufforderung.
3. Den SPN für den Gateway Server einrichten:
   a. Wenn Ihr Gateway Server als lokales Systemkonto ausgeführt wird, lautet der Befehl:
   b. **`setspn -s HTTP/gatewaydns.domain.com computername`**

   Führen Sie beispielsweise für den Fall, dass Ihr Gateway Server auf Host **`'cody'`** in der Domäne läuft und Ihr DNS-Eintrag **`codygw.acme.com`** lautet, folgenden Befehl aus:
   `setspn -s HTTP/codygw.acme.com cody`
   c. Läuft Ihr Gateway Server nicht an einem Standard-Port (d. h. an einem anderen Port als 443), müssen Sie auch einen SPN mit der Portnummer registrieren, z. B. dann, wenn Ihr Gateway Server an Port 444 läuft:
   `setspn -s HTTP/codygw.acme.com:444 cody`
4. Falls nicht bereits geschehen, müssen Sie die **Adresse für die Administration** Ihres gewünschten Gateway Servers in den erstellten Gateway Server-DNS-Eintrag ändern (z. B. **`codygw.acme.com`**).

Überprüfen Sie, dass die SPNs korrekt für das Gateway festgelegt wurden.

1. Wenn ein lokales Volume für das lokale Gateway vorliegt, können Sie überprüfen, dass SPNs und die Delegierung funktionieren, indem Sie sich mit SSO anmelden. Dies muss auf einem anderen Computer stattfinden als auf dem Files Advanced Server und dem Domänencontroller, da SSO ansonsten nicht funktioniert.
2. Durchsuchen Sie das Volume des lokalen Gateway Servers. Wenn dies funktioniert, können Sie fortfahren. Ansonsten überprüfen Sie, ob Sie die richtigen SPNs für die jeweiligen Objekte konfiguriert haben.

   Hinweis: *Wenn Sie ein Volume auf einem Remote-Dateiserver ausprobieren, sollten Sie einen Fehler über einen verweigerten Zugriff erhalten.*

Hinweis: *Dieser Typ der eingeschränkten Delegierung ist nur bei Domänencontrollern verfügbar, die mindestens in der Domänenfunktionsebene 2012R2 ausgeführt werden. Windows Server 2012 ist das erste Programm, das die eingeschränkte Kerberos-Delegierung in Domänenstrukturen erlaubt.*

Sie können die ressourcenbasierte eingeschränkte Kerberos-Delegierung verwenden, um Benutzern Zugriff auf Dateiserver zu gewähren oder auf andere Netzwerkressourcen, die sich in einer anderen Domänen befinden.

1. Wechseln Sie zu dem Domänencontroller für die Domäne, in der sich der Dateiserver befindet, und öffnen Sie **PowerShell**.
2. Wenn Ihr Gateway Server als **Lokales System**konto ausgeführt wird:
   a. **$computer1 = Get-ADComputer -Identity <Gateway_server_computer> -server <Domänencontroller_für_diese_Domäne>**
      Beispiel: **`$computer1 = Get-ADComputer -Identity cody -server dc.acme.com`**
      Dieser Befehl ruft das Computerobjekt für den Gateway Server ab, gibt die AD-Domain-Diensteinstanz für die Verbindung an und speichert diese Information in der Variablen **$computer1**.
   b. **Set-ADComputer <Datei_server_computer> -PrincipalsAllowedToDelegateToAccount $computer1**
      Beispiel: **`Set-ADComputer cody -PrincipalsAllowedToDelegateToAccount $computer1`**
      Dieser Befehl setzt die Eigenschaft **Principals Allowed To Delegate To Account** des Computerobjekts für den Dateiserver auf das Computerobjekt für den Gateway Server. So kann der Computer des Gateway Servers an den Computer des Dateiservers delegieren.
3. Wenn Ihr Gateway Server als **Benutzerkonto** ausgeführt wird:
   a. **$user1 = Get-ADUser -Identity <Anmeldung_Benutzer_von_Gatewaydienst> -server <Domänencontroller_für_diese_Domäne>**
      Beispiel: **`$user1 = Get-ADUser -Identity jane -server dc.acme.com`**
      Dieser Befehl ruft das Benutzerobjekt für den Benutzer ab, der den Gateway Server ausführt, gibt die AD-Domain-Diensteinstanz für die Verbindung an und speichert diese Information in der Variablen **$user1**.
   b. **Set-ADComputer <Datei_server_computer> -PrincipalsAllowedToDelegateToAccount $user1**
      Beispiel: **`Set-ADComputer cody -PrincipalsAllowedToDelegateToAccount $user1`**
      Dieser Befehl setzt die Eigenschaft **Principals Allowed To Delegate To Account** des Computerobjekts für den Dateiserver auf das Benutzerobjekt für den Gateway Server. So kann der ausgewählte Benutzer an den Computer des Dateiservers delegieren.

4. Überprüfen Sie, ob das Benutzerkonto des Gateways als Konto hinzugefügt wurde, dem Anmeldeinformationen delegiert werden können, indem Sie den folgenden Befehl ausführen:

   Get-ADComputer <Datei_server_Computer> -Properties PrincipalsAllowedToDelegateToAccount

   Beispiel: **`Get-ADComputer omega -Properties PrincipalsAllowedToDelegateToAccount`**
5. Wiederholen Sie diese Schritte für alle Dateiserver.

Es ist ein wenig Zeit nötig, bis die Delegierung propagiert wird. Bei kleinen LDAP-Bereitstellungen muss mit 10 bis 15 Minuten gerechnet werden und bei größeren Strukturen kann es sogar noch länger dauern.

Hinweis: *Diese Schritte können nur durchgeführt werden, wenn sich die Computer, welche die Gateway Server hosten, in derselben Domäne befinden wie der Files Advanced Web Server.*

Damit der KDC („Key Distribution Center“) Kerberos-Server Benutzer für den Gateway-Server authentifizieren kann, muss der Gateway-Dienst für den KDC registriert werden. Hierzu müssen „setspn“ und der Hostname des Servers angegeben werden, auf dem er als 'user' im setspn-Befehl läuft.

Gateway Server, die auf anderen Computern als dem Files Advanced Web Server gehostet werden

1. Öffnen Sie die Eingabeaufforderung.
2. Geben Sie den folgenden **setspn**-Befehl ein: **`setspn -s HTTP/Computername.Domäne.com Computername`**

   Führen Sie beispielsweise für den Fall, dass Ihr Gateway Server auf Host **`'cody'`** in der Domäne läuft, folgenden Befehl aus:

   `setspn -s HTTP/cody.acme.com cody`
3. Läuft Ihr Gateway Server nicht an einem Standard-Port (d. h. an einem anderen Port als 443), müssen Sie auch einen SPN mit der Portnummer registrieren, z. B. dann, wenn Ihr Gateway Server an Port 444 läuft:

   `setspn -s HTTP/cody.acme.com:444 cody`
4. Wiederholen Sie diesen Abschnitt für alle weiteren Gateway-Server.

Wenn Sie keinen Zugriff auf die **Ressourcenbasierte eingeschränkte Kerberos-Delegierung** haben, besteht eine andere Methode für die SSO-Konfiguration für Remote-Freigaben und Ressourcen, die sich in einer anderen Domäne befinden, darin, einen Gateway Server auf einem Computer in dieser Domäne zu installieren. So können Sie die reguläre eingeschränkte Kerberos-Delegierung verwenden. **Geeignet in Domänenfunktionsebene 2008**.

Einen Gateway Server auf einem Computer in der gewünschten Domäne installieren

1. Laden Sie das Installationsprogramm von Files Advanced herunter und verschieben Sie es auf den Computer.
2. Starten Sie das Installationsprogramm von Files Advanced, akzeptieren Sie die Lizenzvereinbarung und klicken Sie auf **Weiter**.
3. Wählen Sie **Benutzerdefiniert...** als Installation aus und aktivieren Sie nur das Kontrollkästchen für den Gateway Server.

4. Klicken Sie auf **Installieren**. Nach Abschluss der Installation schließen Sie das Installationsprogramm.
5. Legen Sie im **Konfigurationswerkzeug** die IP-Adresse des Gateways und den Port fest.

Führen Sie den Gateway-Dienst als Benutzerkonto aus

1. Öffnen Sie die **Systemsteuerung** -> **Verwaltung** -> **Dienste**.
2. Klicken Sie mit der rechten Maustaste auf den Gateway Server-Dienst für Files Advanced und wählen Sie **Eigenschaften** aus.
3. Wählen Sie die Registerkarte **Anmeldung** aus und aktivieren Sie das Aktionsfeld **Dieses Konto**.
4. Wählen Sie den Benutzer für die Ausführung des Dienstes aus, indem Sie **Durchsuchen** drücken und danach suchen oder indem Sie einfach den Benutzernamen und das Kennwort des Benutzers eingeben. Der Benutzer **muss** aus der Domäne stammen, in der Files Advanced installiert wurde. Es wird empfohlen, ein dediziertes Konto zu verwenden und nicht das, das für die SPNs des Files Advanced Servers verwendet wurde.
5. Drücken Sie **OK** und schließen Sie das Modul **Dienste** der Systemsteuerung. Starten Sie den Dienst noch nicht neu, da er ohne die erforderlichen Berechtigungen für das Benutzerkonto nicht startet.

Weisen Sie dem ausgewählten Benutzer die nötigen Berechtigungen zu.

1. Damit der Dienst als Benutzer ausgeführt werden kann, muss diesem Benutzer die Berechtigung **Einsetzen als Teil des Betriebssystems** gewährt werden und er muss Teil der Gruppe der lokalen Administratoren sein.
2. Öffnen Sie **Lokale Sicherheitsrichtlinie** und navigieren Sie zu **Lokale Richtlinien** -> **Zuweisen von Benutzerrechten**. Möglicherweise müssen Sie je nach Bereitstellung diese Änderung in der **Gruppenrichtlinienverwaltung** durchführen.
3. Öffnen Sie das Objekt **Einsetzen als Teil des Betriebssystems** und drücken Sie **Benutzer hinzufügen** oder **Gruppe**.
4. Wählen Sie den dedizierten Benutzer für den Gateway-Dienst aus.
5. Schließen Sie alle offenen Dialogfelder und öffnen Sie die **Systemsteuerung** -> **Benutzerkonten** -> **Konten verwalten**.
6. Drücken Sie **Hinzufügen** und geben Sie die Domäne und den Benutzernamen für das dedizierte Konto an.
7. Sie können jetzt den Files Advanced Gateway-Dienst in der Stystemsteuerung unter **Dienste** neu starten.

Den SPN für den Remote-Gateway Server konfigurieren

1. Wechseln Sie zu einem der Computer in der Domäne, in der sich der Files Advanced Server befindet.
2. Öffnen Sie die Eingabeaufforderung.
3. Für die Konfiguration des SPN lautet der Befehl: **setspn –s HTTP/gatewaydns.domain.com useraccountfor_gw**

   Beispiel: Wenn Ihr Gateway Server auf dem Host **`'magpie'`** in der Domäne **tree.com** ausgeführt wird und als Benutzerkonto **`peter`** aus der Domäne **acme.com** ausgeführt wird, führen Sie den folgenden Befehl aus:

setspn –s HTTP/magpie.tree.com peter

Läuft Ihr Gateway Server nicht an einem Standard-Port (d. h. an einem anderen Port als 443), müssen Sie auch einen SPN mit der Portnummer registrieren, z. B. dann, wenn Ihr Gateway Server an Port 444 läuft:

setspn -s HTTP/magpie.tree.com:444 peter

4. Falls nicht bereits geschehen, müssen Sie die **Adresse für die Administration** Ihres gewünschten Gateway Servers in den erstellten Gateway Server-DNS-Eintrag ändern (z. B. **magpie.tree.com**).
5. Überprüfen Sie, dass für den Gateway Server **Aushandeln/Kerberos-Authentifizierung im Benutzermodus durchführen** (S. 90) aktiviert wurde. Sie müssen den Files Advanced Gateway-Dienst neu starten, nachdem Sie diese Einstellung aktiviert haben.
6. Wenn Sie **Datenquellen** für die Ressourcen in der zweiten Domäne erstellen, müssen Sie den Gateway Server verwenden, der sich in dieser Domäne befindet.

   Beispiel: Wenn Sie Ihren Benutzern Zugriff auf die Dateien auf **repository.tree.com** gewähren möchten, müssen Sie den Gateway Server auswählen, der sich in **tree.com** befindet (z. B. **magpie.tree.com**).

Überprüfen Sie, dass die SPNs korrekt für das Gateway festgelegt wurden.

1. Wenn ein lokales Volume für das lokale Gateway vorliegt, können Sie überprüfen, dass SPNs und die Delegierung funktionieren, indem Sie sich mit SSO anmelden.
2. Durchsuchen Sie das Volume des lokalen Gateway Servers. Wenn dies nicht funktioniert, überprüfen Sie, ob sie die richtigen SPNs für die jeweiligen Objekte konfiguriert haben.
3. Delegierungsänderungen benötigen einige Zeit, bis sie propagiert werden (bei kleinen LDAP-Bereitstellungen muss mit 10 bis 15 Minuten gerechnet werden und bei größeren Strukturen kann es sogar noch länger dauern).

12.2.7.4 Überprüfen, dass der SPN registriert ist

So fragen Sie ab, ob der gewünschte SPN richtig registriert ist:

1. Öffnen Sie eine Eingabeaufforderung mit erweiterten Benutzerrechten.
2. Geben Sie den Befehl **setspn –Q HTTP/Computername.Domäne.com** ein.

   Beispiel: **setspn -Q HTTP/ahsoka.acme.com**
3. Verwenden Sie zur Abfrage der für eine bestimmte Domäne registrierten SPNs den Switch **-l** (Kleinbuchstabe **L**);

   Beispiel: **setspn -l john**
4. Nach der Registrierung des SPN müssen Sie vor der Authentifizierung mit SSO entweder den Clientcomputer neu starten oder diesen Befehl auf dem Clientcomputer ausführen:

   klist purge

12.2.7.5 Verwenden von SMB- oder SharePoint-Datenquellen

Falls Sie SMB- oder SharePoint-Datenquellen verwenden möchten, müssen Sie das Active Directory-Konto so konfigurieren, dass eine Kerberos-Delegierung zu jedem Ihrer SMB- und SharePoint-Datenquellen zulässt.

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

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

1. Öffnen Sie **Active Directory-Benutzer und -Computer**.
2. Suchen Sie das Computerobjekt, das dem Gateway-Server entspricht.

   Hinweis: *Wenn Sie den Gateway Server unter einem* ***Benutzer****konto ausführen, wählen Sie dieses* ***Benutzer****objekt stattdessen aus.*

3. Klicken Sie mit der rechten Maustaste auf den Benutzer und wählen Sie "Eigenschaften".
4. Rufen Sie die Registerkarte **Delegation** auf.
5. Wählen Sie **Diesem Computer nur für die Delegierung für bestimmte Dienste vertrauen** aus.
6. Wählen Sie darunter die Option **Use any authentication protocol**.
7. Klicken Sie auf **Add**.
8. Klicken Sie auf **Users or Computers**.
9. Suchen Sie nach dem Serverobjekt für die SMB-Freigabe oder den SharePoint-Server und klicken Sie auf **OK**.
   - Wählen Sie für SMB-Freigaben den Dienst **cifs** aus.
   - Wählen Sie für SharePoint den Dienst **http** aus.
10. Wiederholen Sie die Schritte für jeden Server, für den der Files Advanced Gateway Server Zugriff benötigt.
11. Wiederholen Sie dieses Verfahren für jeden Gateway Server.

Diese Delgierungsänderungen benötigen, je nach Größe der Domänengesamtstruktur, möglicherweise einige Minuten für das Propagieren. Es kann bis zu 15 Minuten (oder mehr) dauern, bis die Änderungen in Kraft treten. Werden die Änderungen nicht nach 15 Minuten angezeigt, versuchen Sie, den Files Advanced Gateway-Dienst neu zu starten.

12.2.7.6 Verwenden von mobilen Clients mit Client-Zertifikatsauthentifizierung

Dies ist ein zusätzlich auszuführender Schritt. Sie müssen die Delegierung vom Gateway Server zum Files Advanced Server auch dann einrichten, wenn diese sich auf demselben Computer befinden.

Eingeschränkte Kerberos-Delegierung

Diese Art der Delegierung wird durchgeführt, wenn sich der Files Advanced Server und der Gateway Server in derselben Domäne befinden.

1. Öffnen Sie dazu das Active Directory auf dem Domänencontroller.
2. Suchen und bearbeiten Sie das Computerobjekt des Gateway Servers, und öffnen Sie die Registerkarte 'Delegierung'.
3. Wählen Sie **Computer bei Delegierungen angegebener Dienste vertrauen** und **Beliebiges Authentifizierungsprotokoll verwenden**.
4. Um den SPN des Files Advanced Servers auszuwählen, klicken Sie auf 'Hinzufügen' und geben den Benutzernamen des Kontos ein, das mit dem **HTTP-**SPN des Files Advanced Servers verknüpft ist.

Hinweis: *Suchen Sie nicht nach dem Computer, auf dem der Files Advanced Server ausgeführt wird. Suchen Sie stattdessen nach dem Benutzernamen.*

Hinweis: *Eine Kerberos-Authentifizierung für den Files Advanced Server ist nicht mit dem Einzelport-Modus kompatibel.*

5. Sobald Sie nach dem Benutzer suchen, sollten die **HTTP-**Services angezeigt werden. Wählen Sie sie aus (es können zwei Services sein, wenn Sie den SPN zweimal registriert haben – einmal mit Port und einmal ohne).
6. Drücken Sie auf **Anwenden**, und schließen Sie alle Dialogfelder.

Ressourcenbasierte eingeschränkte Kerberos-Delegierung

Dieser Delegierungstyp funktioniert auch, wenn sich die Access und Gateway Server in unterschiedlichen Domänen einer Domänengesamtstruktur befinden.

Hinweis: *Damit diese Funktion verwendet werden kann, müssen alle Domänen, auf die Files Advanced zugreifen kann, mindestens in der* ***Domänenfunktionsebene 2012*** *ausgeführt werden.*

1. Überprüfen Sie erneut, dass die DNS-Eingabe für den Files Advanced Server, für den Sie einen SPN festgelegt haben, als Adresse für Ihr S&S-Volume auf der Seite der Datenquellen festgelegt wurde.
2. Konfigurieren Sie die Delegierung zwischen dem Gateway Server und dem Files Advanced Server. Jetzt wird die Delegierung zwischen dem Gateway Server und dem Files Advanced Server durchgeführt.
3. Führen Sie die nachstehenden Befehle für die folgenden Benutzer aus:

   $pc1 = Get-ADComputer -Identity <Name_des_Gateway_Computers>

   Set-ADUser <Access_SSO_Benutzerkonto> -PrincipalsAllowedToDelegateToAccount $pc1

   Beispiel: **`$pc1 = Get-ADComputer -Identity ahsoka`**

   `Set-ADUser john -PrincipalsAllowedToDelegateToAccount $pc1`
4. Wenn Ihr Gateway als Benutzerkonto ausgeführt wird, müssen Sie die Delegierung mit den folgenden Befehlen zwischen zwei Benutzerkonten festlegen:

   $user1 = Get-ADUser -Identity <Gateway_Benutzerkonto>

   Set-ADUser <Access_SSO_Benutzerkonto> -PrincipalsAllowedToDelegateToAccount $user1

   Beispiel: **`$user1 = Get-ADUser -Identity gwuser`**

   `Set-ADUser john -PrincipalsAllowedToDelegateToAccount $user1`

Es ist ein wenig Zeit nötig, bis die Delegierung propagiert wird. Bei kleinen LDAP-Bereitstellungen muss mit 10 bis 15 Minuten gerechnet werden und bei größeren Strukturen kann es sogar noch länger dauern.

12.2.7.7 Für Umgebungen mit Lastenausgleich

Der Gateway Server verfügt über eine Option, bei der anstelle eines Aushandeln-/Kerberos-Authentifizierungsversuchs durch den Webserver alle HTTP-Authentifizierungen im Benutzermodus durchgeführt werden. Dies ist notwendig, damit SSO bei Gateways hinter einem Lastenausgleichsmodul funktionieren kann.

Öffnen Sie zur Aktivierung dieser Funktion die Weboberfläche, und wechseln Sie zu **Mobiler Zugriff** -> **Gateway Server**. Klicken Sie in der Cluster-Gruppe auf die Option **Bearbeiten**, wechseln Sie zu **Erweitert**, und aktivieren Sie das Kontrollkästchen **Aushandeln-/Kerberos-Authentifizierung im Benutzermodus durchführen**.

Netzwerkknoten aktivieren

Damit bei einer Verwendung von SSO auf Netzwerkknoten im Web zugegriffen werden kann, sind mehrere Änderungen erforderlich. Da sich die Gateway Server hinter einem Lastenausgleichsmodul befinden, muss die Kerberos-Registrierung statt mit einem Computernamen mit einem Benutzerkonto erfolgen.

Damit dies funktioniert, müssen die Gateway-Dienste unter einem Benutzerkonto ausgeführt werden. Sie können entweder den LDAP-Benutzer verwenden, unter dem der Files Advanced Tomcat Server registriert ist, oder einen neuen, für die Gateway-Dienste reservierten auswählen.

Unabhängig davon, wofür Sie sich entscheiden, muss der ausgewählte Benutzer die Berechtigung erhalten, auf den Computern mit den installierten Gateway Servern als Teil des Betriebssystems zu agieren.

Benutzer auswählen, der als Teil des Betriebssystems agiert

1. Klicken Sie auf dem Computer mit dem Gateway Server auf **Start** -> **Ausführen**.
2. Geben Sie **gpedit.msc** ein, und klicken Sie auf **OK**.
3. Erweitern Sie **Windows-Einstellungen** und dann **Sicherheitseinstellungen**.
4. Erweitern Sie **Lokale Richtlinien**, und klicken Sie auf **Zuweisen von Benutzerrechten**.
5. Klicken Sie mit der rechten Maustaste in der Liste auf **Einsetzen als Teil des Betriebssystems**, und wählen Sie **Eigenschaften** aus.
6. In diesem Fenster können Sie Benutzer und Gruppen hinzufügen oder sie entfernen. Geben Sie den gewünschten Benutzernamen ein, und klicken Sie auf 'OK'.
7. Schließen Sie alle noch offenen Fenster, und starten Sie den Server neu, damit die Änderung wirksam wird.

Gateway Server-Dienst mit dem ausgewählten Benutzerkonto ausführen

Nachdem Sie den Benutzer zum Ausführen des Gateway-Diensts hinzugefügt haben, müssen Sie festlegen, dass der Dienst mit diesem Benutzer ausgeführt werden soll. Gehen Sie dazu folgendermaßen vor:

1. Klicken Sie auf dem Computer mit dem installierten Gatewayserver auf **Start**, und wählen Sie **Ausführen** aus.
2. Geben Sie **services.msc** ein, und klicken Sie auf **OK**. Alternativ können Sie die **Systemsteuerung** öffnen und dann **Verwaltung** -> **Dienste** auswählen.
3. Klicken Sie mit der rechten Maustaste in der Liste auf **Files Advanced Gateway**, und wählen Sie **Eigenschaften** aus.
4. Klicken Sie auf die Registerkarte **Anmelden**.
5. Wählen Sie das Optionsfeld für **Dieses Konto** aus, und geben Sie die Anmeldedaten des Benutzers ein, dem Sie Betriebssystemrechte gewährt haben.
6. Klicken Sie auf **OK**, und schließen Sie alle Fenster.

SPNs für den Gateway-Cluster konfigurieren

Damit der Kerberos Key Distribution Center-Server (KDC) Benutzer für den Gateway-Cluster authentifizieren kann, müssen alle Gateway Server und das Lastenausgleichsmodul für die Gateways beim KDC-Server registriert werden. Hierzu muss **setspn** mit dem Kontonamen ausgeführt werden, unter dem der Dienst laufen soll.

1. Öffnen Sie die Eingabeaufforderung.
2. Geben Sie den folgenden Befehl ein:

   `setspn -s HTTP/computername.domain.com username`

   Wird der Gateway-Dienst beispielsweise mit dem Benutzer **john** ausgeführt, lautet der Befehl:

   `setspn -s HTTP/gatewayserver1.acme.com john`
3. Läuft Ihr Gateway Server nicht an einem Standard-Port (d. h. an einem anderen Port als 443), müssen Sie auch einen SPN mit der Portnummer registrieren, z. B. dann, wenn Ihr Gateway Server an Port 444 läuft:

   `setspn -s HTTP/gatewayserver1.acme.com:444 john`
4. Wiederholen Sie diese Schritte für alle Gateway Server und das Lastenausgleichsmodul. Der SPN-Befehl für das Lastenausgleichsmodul lautet wie folgt:

   `setspn -s HTTP/gwloadbalancerdns.acme.com john`

- Benutzer von Desktop- oder Web-Clients müssen auf einem anderen Computer als auf dem arbeiten, auf dem Files Advanced Server ausgeführt wird (aber innerhalb der Domain), sonst funktioniert SSO nicht.
- Sie müssen für den Zugriff auf den Server denselben FQDN verwenden, den der SPN verwendet, z.B. **`https://ahsoka.acme.com`**. Sie können keine anderen DNS-Namen oder IP-Adressen wie etwa **`https://localhost`** oder **`https://10.20.56.33`** verwenden.
- Stellen Sie sicher, dass Sie sich beim Files Advanced Server ohne Verwendung von SSO anmelden können, indem Sie genau dieselben LDAP-Anmeldedaten eingeben, die Ihr Windows-Clientcomputer verwendet. So wird sichergestellt, dass die Anmeldedaten Ihres Kontos für Files Advanced gültig sind, unabhängig von SSO-Konfigurationen.
- Stellen Sie sicher, dass Sie ohne Einzelanmeldung und mit den Anmeldedaten Ihres LDAP-Kontos auf alle Datenquellen zugreifen können.
- Wenn Sie sich nicht über SSO anmelden können, überprüfen Sie, ob Sie Ihren Webbrowser für SSO zu dem FQDN konfiguriert haben, zu dem Sie eine Verbindung herstellen möchten. Stellen Sie außerdem sicher, dass Sie sich mithilfe eines Domain-Kontos auf Ihrem Clientcomputer angemeldet haben.
- Die Einzelanmeldung funktioniert nicht, wenn der Files Advanced-Server auf dem Domänencontroller läuft.
- Files Advanced funktioniert nicht mit SSO, wenn Sie versuchen, über den Computer, der auch der Domänencontroller ist, darauf zuzugreifen.

  Hinweis: *Aufgrund der Funktionsweise von Kerberos können Sie sich nicht über Client-Applikationen oder Webbrowser, die auf dem Domänencontroller oder dem Files Advanced Server ausgeführt werden, über SSO authentifizieren.*

  Zudem kann der Files Advanced Server den Domänencontroller nicht authentifizieren, wenn der Files Advanced Server auf dem Domäncontroller ausgeführt wird.

- Sie erhalten den Fehler **401 Error** , wenn Sie versuchen, sich über SSO anzumelden. Prüfen Sie Benutzername und Kennwort in der Datei **web.xml**, und stellen Sie sicher, dass alle

Sonderzeichen richtig geschützt sind. Die Sonderzeichen sind: **&**, **>**, **"**, **'** oder **<**. Informationen dazu, wie Sie Sonderzeichen schützen, finden Sie in **Schritt 5** des Abschnitts **Bearbeiten der Datei 'web.xml'**.

12.2.8 Vertrauenswürdige Server-Zertifikate mit Files Advanced verwenden

In diesem Abschnitt wird erläutert, wie Files Advanced mit vertrauenswürdigen Server-Zertifikaten konfiguriert wird.

Files Advanced stellt zu Testzwecken standardmäßig ein selbst generiertes SSL-Zertifikat bereit. Bei Verwendung eines von einer vertrauenswürdigen Zertifizierungsstelle signierten Zertifikats wird die Identität des Servers festgestellt, und Clients können eine Verbindung herstellen, ohne dass Fehler angezeigt werden.

Hinweis: *Webbrowser zeigen bei Verwendung von selbstsignierten Zertifikaten eine Warnmeldung an. Wenn Sie diese Warnmeldungen schließen, können Sie das System zu Testzwecken verwenden.*

Die Verwendung von selbstsignierten Zertifikaten unter Produktionsbedingungen wird nicht unterstützt. Für Produktionsumgebungen sollten geeignete CA-Zertifikate verwendet werden.

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

Note: *Wenn Sie vom Anbieter aufgefordert werden, einen Servertyp anzugeben, wählen Sie **IIS** aus. Die Zertifikate müssen im Zertifikatspeicher von Windows installiert werden, bevor Files Advanced sie verwenden kann.*

Eine Zertifikatanforderung mit IIS erzeugen:

Weitere Informationen zu diesem Verfahren finden Sie im folgenden Microsoft Knowledge Base-Artikel: http://technet.microsoft.com/en-us/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.

Voraussetzungen

Das verwendete Zertifikat muss seinen privaten Schlüssel enthalten. Das Zertifikat muss entweder im **.PFX**- oder im **.P12** -Format vorliegen. Es spielt keine Rolle, welches Sie verwenden, da sie austauschbar sind.

Hinweis: *Wenn Sie von Ihrem Zertifikatanbieter ein Zertifikat erhalten haben und ein Schlüssel zwei separate Dateien aufweist, können Sie diese mit dem folgenden Befehl in einer* ***.PFX****-Datei kombinieren:*

openssl pkcs12 -export -in <yourcertificate.extension> -inkey <yourkey.extension> -out <newfile.pfx>

Beispiel: openssl pkcs12 -export -in acmecert.crt -inkey acmecertkey.key -out acmecombined.pfx

Für diesen Befehl muss OpenSSL installiert werden.

Das Zertifikat im Windows-Zertifikatspeicher installieren

Hinweis: *Wenn Ihre Files Advanced und Gateway Server verschiedene Zertifikate verwenden, wiederholen Sie diese Schritte für beide Server.*

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 vorliegt, geben Sie es 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 klicken Sie dann auf **Weiter**.
17. Klicken Sie auf **Fertig stellen** und klicken Sie dann auf **OK**, um den erfolgreichen Import zu bestätigen.

Alle erfolgreich im Windows-Zertifikatspeicher installierten Zertifikate stehen bei der Verwendung des Files Advanced Konfigurationswerkzeugs zur Verfügung.

Nachdem Sie das Zertifikat im Windows-Zertifikatspeicher installiert haben, müssen Sie Files Advanced für die Verwendung dieses Zertifikats konfigurieren.

1. Starten Sie das Files Advanced Konfigurationswerkzeug. Im Startmenü von Windows sollte eine Verknüpfung angezeigt werden.

   Hinweis: *Das Konfigurationswerkzeug befindet sich standardmäßig unter **C:\Program Files (x86)\Acronis\Access\Configuration Utility**.*

2. Drücken Sie auf der Registerkarte **Web Server** auf die Schaltfläche **[...]**, und wählen Sie Ihr Zertifikat aus der Liste aus.
3. Drücken Sie auf der Registerkarte **Mobile Gateway** auf die Schaltfläche **[...]**, und wählen Sie Ihr Zertifikat aus der Liste aus.
4. Klicken Sie auf **Anwenden**. Dadurch werden die Webdienste neu gestartet und sollten nach ungefähr einer Minute wieder online sein und mit Ihrem Zertifikat ausgeführt werden. Sie können überprüfen, ob die richtigen Zertifikate verwendet werden.

Hat die Zertifizierungsstelle Ihnen zusammen mit Ihrem Zertifikat ein Zwischenzertifikat ausgestellt, muss dieses über das Konfigurationsdienstprogramm ebenfalls dem Files Advanced-Server hinzugefügt werden.

Hinweis: *Das Konfigurationswerkzeug sucht nur im Zertifikatspeicher für **Zwischenzertifikate**. Wenn Ihr Zertifikat in einem der anderen Speicher installiert wurde, öffnen Sie **certmgr.msc** und verschieben Sie Ihr Zwischenzertifikat von diesem Speicher in den Speicher **Zwischenzertifizierungsstellen -> Zertifikate**.*

1. Starten Sie das Files Advanced Konfigurationswerkzeug. Im Startmenü von Windows sollte eine Verknüpfung angezeigt werden.

   Hinweis: *Das Konfigurationswerkzeug befindet sich standardmäßig unter **C:\Program Files (x86)\Acronis\Access\Configuration Utility**.*

2. Drücken Sie auf der Registerkarte **Web Server** auf die Schaltfläche **[...]**, und wählen Sie Ihr Zertifikat aus der Liste aus.
3. Drücken Sie auf die Plus-Schaltfläche (**+**) neben dem Feld **Kettenzertifikat** und wählen Sie das **Zwischenzertifikat** aus der Liste, das Sie verwenden möchten. Befindet sich das gewünschte Zertifikat nicht in der Liste, überprüfen Sie, ob es ordnungsgemäß und in welchem Speicher es installiert wurde.
4. Drücken Sie auf der Registerkarte **Mobile Gateway** auf die Schaltfläche **[...]**, und wählen Sie Ihr Zertifikat aus der Liste aus. Es sind keine weiteren Schritte für Zwischenzertifikate erforderlich.
5. Klicken Sie auf **Anwenden**. Der Dienst wird erneut gestartet und wenn er wieder online ist, können Sie überprüfen, ob die ausgewählten Zertifikate zur Verfügung stehen.

12.2.9 Unterstützung verschiedener Desktop Client-Versionen

Wenn Sie eine ältere Version von Files Advanced Desktop Client verwenden möchten, gehen Sie folgendermaßen vor:

1. Laden Sie die gewünschte Version des Desktop-Clients herunter. 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 Ordner für den Files Advanced Desktop Client (**`C:\Program Files (x86)\Acronis\Files Advanced\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 Files Advanced Servers.
7. Melden Sie sich als **Administrator** an, gehen Sie zur Registerkarte **Sync & Share**, und öffnen Sie die Seite **Files Advanced 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 Files Advanced Desktop Client-Version herunterladen. Wenn Benutzer nicht die aktuelle Version herunterladen sollen, gehen Sie zum Ordner **\Acronis\Files Advanced\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**').*

12.2.10 Verschieben des Dateispeichers an einen nicht standardmäßigen Speicherort.

Der Dienst wird als lokales Systemkonto ausgeführt.

1. Wechseln Sie zu dem Computer, auf dem Files Advanced installiert ist.
2. Beenden Sie die Dienste **Files Advanced Datei-Repository-Server** und **Files Advanced Tomcat**.

3. Sie finden den aktuellen **Dateispeicher** in dem Ordner, den Sie mit dem **Konfigurationswerkzeug** ausgewählt haben. Der Standardspeicherort ist: **`C:\ProgramData\Acronis\Files Advanced\FileStore`**.
4. Kopieren oder verschieben Sie den gesamten Ordner **FileStore** (Dateispeicher) mit dem kompletten Inhalt an den gewünschten Speicherort.

   Beispiel: **`D:\MyCustom Folder\FileStore`**

   Hinweis: *Befindet sich der **Dateispeicher** auf einer Remote-Netzwerkfreigabe, muss der Computer, auf dem der Dienst **Datei-Repository** ausgeführt wird, über die vollen Berechtigungen für den Ordner **Dateispeicher** auf der Netzwerkfreigabe verfügen.*

5. Öffnen Sie das **Konfigurationswerkzeug**.
6. Ändern Sie auf der Registerkarte **Datei-Repository** den Pfad für den **Dateispeicher** in den neuen Pfad, in den Sie den Ordner **FileStore** (Dateispeicher) verschoben haben.
7. Starten Sie den Dienst **Files Advanced Datei-Repository-Server**.
8. Starten Sie den Dienst **Files Advanced Tomcat** und schließen Sie die Systemsteuerung für die **Dienste**.

Der Dienst wird als Benutzerkonto ausgeführt

1. Wechseln Sie zu dem Computer, auf dem Files Advanced installiert ist.
2. Beenden Sie die Dienste **Files Advanced Datei-Repository-Server** und **Files Advanced Tomcat**.
3. Sie finden den aktuellen **Dateispeicher** in dem Ordner, den Sie mit dem **Konfigurationswerkzeug** ausgewählt haben. Der Standardspeicherort ist: **`C:\ProgramData\Acronis\Files Advanced\FileStore`**.
4. Kopieren oder verschieben Sie den gesamten Ordner **FileStore** (Dateispeicher) mit dem kompletten Inhalt an den gewünschten Speicherort.

   Beispiel: **`D:\MyCustom Folder\FileStore`**
5. Öffnen Sie das **Konfigurationswerkzeug**.
6. Ändern Sie auf der Registerkarte **Datei-Repository** den Pfad für den **Dateispeicher** in den neuen Pfad, in den Sie den Ordner **FileStore** (Dateispeicher) verschoben haben.
7. Befindet sich der **Dateispeicher** auf einer Remote-Netzwerkfreigabe, muss das Benutzerkonto, mit dem der Dienst **Datei-Repository** ausgeführt wird, über die vollen Berechtigungen für den Ordner **Dateispeicher** auf der Netzwerkfreigabe verfügen.
8. Das Konto muss auch über Lese- und Schreibzugriff für den lokalen Ordner **Repository** verfügen (z.B. **`C:\Program Files (x86)\Acronis\Files Advanced\File Repository\Repository`**), um in die Protokolldatei schreiben zu können.
9. Starten Sie den Dienst **Files Advanced Datei-Repository-Server**.
10. Starten Sie den Dienst **Files Advanced Tomcat** und schließen Sie die Systemsteuerung für die **Dienste**.

12.2.11 Überwachen von Files Advanced mit New Relic

Bei diesem Installationstyp überwachen Sie Ihre Files Advanced 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, oder melden Sie sich mit einem bestehenden Konto an. Fahren Sie anschließend mit der Konfiguration Ihrer Applikation fort.

2. Wählen Sie unter 'Applikationstyp' die Option **APM** aus.
3. Markieren Sie unter 'Plattform' den Eintrag **Ruby**.
4. Laden Sie das in Schritt 3 der Startanleitung für 'New Relic' genannte Skript 'New Relic' herunter (newrelic.yml).
5. Öffnen Sie die Webkonsole von Files Advanced.
6. Navigieren Sie zu **Einstellungen** -> **Überwachung**.
7. 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 Files Advanced, sodass sie bei einem Upgrade oder einer Deinstallation nicht entfernt oder geändert werden.
8. Klicken Sie auf **Speichern** und warten Sie einige Minuten oder so lange, bis auf der New Relic-Website die Schaltfläche **Aktive Applikation(en)** verfügbar wird.
9. Wenn mehr als 10 Minuten vergehen, starten Sie den Files Advanced Tomcat-Dienst neu, und warten Sie einige Minuten. Die Schaltfläche sollte dann aktiv sein.
10. Sie sollten den Files Advanced Server auf der New Relic-Website überwachen können.

*Alle vom Files Advanced 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.

12.2.12 Files Advanced Tomcat an mehreren Ports ausführen

Während das Konfigurationswerkzeug nur das Einstellen des Tomcat-Dienstes für einen Port unterstützt, kann Tomcat selber für die Ausführung an mehreren Ports konfiguriert werden. Dies wird durch das Hinzufügen von zusätzlichen Konnektoren zu den gewünschten Ports in der Tomcat-Datei 'server.xml' durchgeführt. Das Durchführen von Upgrades und das Neustarten des Tomcat-Dienstes mit der Konfigurationswerkzeug beeinträchtigt nicht die neuen Konnektoren.

***Hinweis:** Es wird empfohlen, diese Konfiguration durchzuführen, nachdem Sie bereits einmal das Konfigurationswerkzeug ausgeführt haben und der Tomcat-Dienst erfolgreich gestartet wurde.*

Einen zusätzlichen Tomcat-Konnektor konfigurieren

1. Beenden Sie den Files Advanced Tomcat-Dienst, wenn er ausgeführt wird.
2. Navigieren Sie zur Datei **server.xml** und öffnen Sie diese. Sie befindet sich standardmäßig unter: **C:\Program Files (x86)\Acronis\Files Advanced\Common\apache-tomcat-7.0.59\conf**.

   Hinweis: *Die Zahl im Pfad (7.0.59) kann abweichen, je nach Ihrer Tomcat-Version.*

3. Durchsuchen Sie die Datei, bis Sie den Abschnitt zum **Konnektor** finden, der wie folgt aussieht:

```
<Connector maxHttpHeaderSize="65536" maxThreads="150"
enableLookups="false" disableUploadTimeout="true" acceptCount="100"
scheme="https" secure="true" SSLEnabled="true"
SSLProtocol="TLSv1+TLSv1.1+TLSv1.2" SSLCertificateFile="$
{catalina.base}/conf/AAServer_LocalHost.crt"
SSLCertificateKeyFile="${catalina.base}
/conf/AAServer_LocalHost.key" SSLHonorCipherOrder="true"
SSLCipherSuite="ECDH+AESGCM:ECDH+AES256:ECDH+AES128:RSA+AESGCM:RSA+AES:
!aNULL:!eNULL:!LOW:!3DES:!RC4:!MD5:!EXP:!PSK:!SRP:!DSS"
connectionTimeout="-1" URIEncoding="UTF-8" address="0.0.0.0" port="443"/>
```

   Hinweis: *Je nach Texteditor werden Sie den oben gezeigten Code wahrscheinlich in einer einzigen Zeile sehen, wenn Sie* ***server.xml*** *öffnen.*

   Hinweise: *Wenn Sie einen anderen Port als* ***443*** *im* ***Konfigurationswerkzeug*** *ausgewählt haben, weist Ihr* ***Konnektor*** *den Port auf, der in dem Beispiel weiter oben aufgeführt ist.*

4. Kopieren Sie den gesamten Abschnitt zum **Konnektor** und fügen Sie ihn direkt unter dem Originalabschnitt ein. Beide Abschnitte sollten identisch eingerückt sein.
5. Ersetzen Sie **443** (bzw. den Port, den Sie im **Konfigurationswerkzeug** ausgwählt haben) durch den gewünschten zweiten Port für Tomcat, z. B.:

```
<Connector maxHttpHeaderSize="65536" maxThreads="150"
enableLookups="false" disableUploadTimeout="true" acceptCount="100"
scheme="https" secure="true" SSLEnabled="true"
SSLProtocol="TLSv1+TLSv1.1+TLSv1.2" SSLCertificateFile="$
{catalina.base}/conf/AAServer_LocalHost.crt"
SSLCertificateKeyFile="${catalina.base}
/conf/AAServer_LocalHost.key" SSLHonorCipherOrder="true"
SSLCipherSuite="ECDH+AESGCM:ECDH+AES256:ECDH+AES128:RSA+AESGCM:RSA+AES:
!aNULL:!eNULL:!LOW:!3DES:!RC4:!MD5:!EXP:!PSK:!SRP:!DSS"
connectionTimeout="-1" URIEncoding="UTF-8" address="0.0.0.0" port="4430"/>
```

   Hinweis*: Stellen Sie sicher, dass der Code für den neuen* ***Konnektor*** *dem bestehendem Code entspricht. Wenn der alte Code beispielsweise in einer Zeile geschrieben ist, muss der neue Code auch so formatiert sein.*

6. Öffnen Sie die Files Advanced Weboberfläche und navigieren Sie zu **Allgemeine Einstellungen** -> **Server-Einstellung**.
7. Stellen Sie im Feld **Webadresse** sicher, dass die bereitgestellte Adresse einen der Ports für die Konnektoren verwendet. Das ist die Adresse, die Benutzer in den E-Mail-Einladungen sehen, und Sie können nur einen Port dafür auswählen.

12.2.13 Multi-Homing für Files Advanced

Multi-Homing für Files Advanced Gateway und Files Advanced Server ist eine einfache Aufgabe, die mithilfe des Konfigurationswerkzeugs durchzuführen ist.

Die einzige Anforderung besteht darin, dass Sie über zwei separate Netzwerkschnittstellen und IP-Adressen verfügen müssen.

Multi-Homing konfigurieren

1. Öffnen Sie das Files Advanced Konfigurationswerkzeug.
2. Öffnen Sie die Registerkarte **Web Server**, und geben Sie die erste IP-Adresse und den Port 443 ein.
3. Öffnen Sie die Registerkarte **Gateway Server**, und geben Sie die zweite IP-Adresse und den Port 443 ein.
4. Klicken Sie auf **OK**.

Hinweis: *Microsoft hat das Verhalten des TCP/IP-Stacks in Windows Server 2008 grundlegend geändert. Ein einzelner IP-Transport unterstützt jetzt mehrere Schichten, und es gibt keine 'primäre' IP-Adresse mehr. Wenn also mehrere IP-Adressen einer einzelnen Schnittstelle zugewiesen werden, werden alle Adressen gleich behandelt und alle im DNS registriert. Dieses Verhalten ist also kein Fehler, sondern beabsichtigt. Das Verhalten verursacht jedoch Probleme, denn wenn Sie nichts dagegen tun, ist die verwendete IP-Adresse ein Round-Robin (DNS).*

Sie können dies umgehen, indem Sie die dynamische DNS-Registrierung auf der Netzwerkkarte deaktivieren und den Host-DNS-Eintrag dann manuell erstellen. Eine weitere leichte Umgehung dieses Problems ist die Installation des in KB975808 referenzierten HotFix: ***http://support.microsoft.com/?kbid=975808****. Sobald Sie den HotFix installiert haben, können Sie den* ***`netsh skipassource`****-Flag verwenden. Wenn Sie diesen Flag beim Hinzufügen neuer Adressen verwenden, weisen Sie den Stack damit an, die neue Adresse nicht für ausgehende Pakete zu verwenden. Diese IP-Adressen werden daher nicht auf den DNS-Servern registriert. Beispiel:*

```
netsh int ipv4 add address "Local Area Connection" 192.168.1.2 skipassource=true
```

12.2.14 Separate Webvorschau-Servlets bereitstellen

Mit der Webvorschaufunktion von Files Advanced können Benutzer Dateiinhalte einsehen, ohne die Datei komplett herunterladen zu müssen. In Umgebungen mit zahlreichen Benutzern kann dadurch die Bereitstellungsleistung erheblich beeinträchtigt werden. Das können Sie vermeiden, indem Sie mit unserem Webvorschau-Servlet zusätzliche Tomcat-Server einrichten, die sich um die Webvorschau kümmern und den (die) Files Advanced Advance Hauptserver unterstützen.

Ein Lastenausgleichsmodul kann vor einer Reihe von Tomcat-Servern bereitgestellt werden, um den Lastenausgleich für die Webvorschau-Servlets vorzunehmen. Da für die Vorschauanforderungen kein Status benötigt wird, sind für das Lastenausgleichsmodul keine besonderen Konfigurationen notwendig.

Themen

12.2.14.1 Servlet installieren und konfigurieren

Tomcat-Installation

Sie können einen Apache Tomcat 7-Server entweder aus einer .zip-Datei oder mit einer ausführbaren Installationsdatei installieren. Wir empfehlen die Verwendung der ausführbaren Installationsdatei, aber die Installation über das .zip-Archiv ist ebenfalls möglich. Der einzige Unterschied liegt in der Konfigurationsweise des Apache Tomcat 7-Servers.

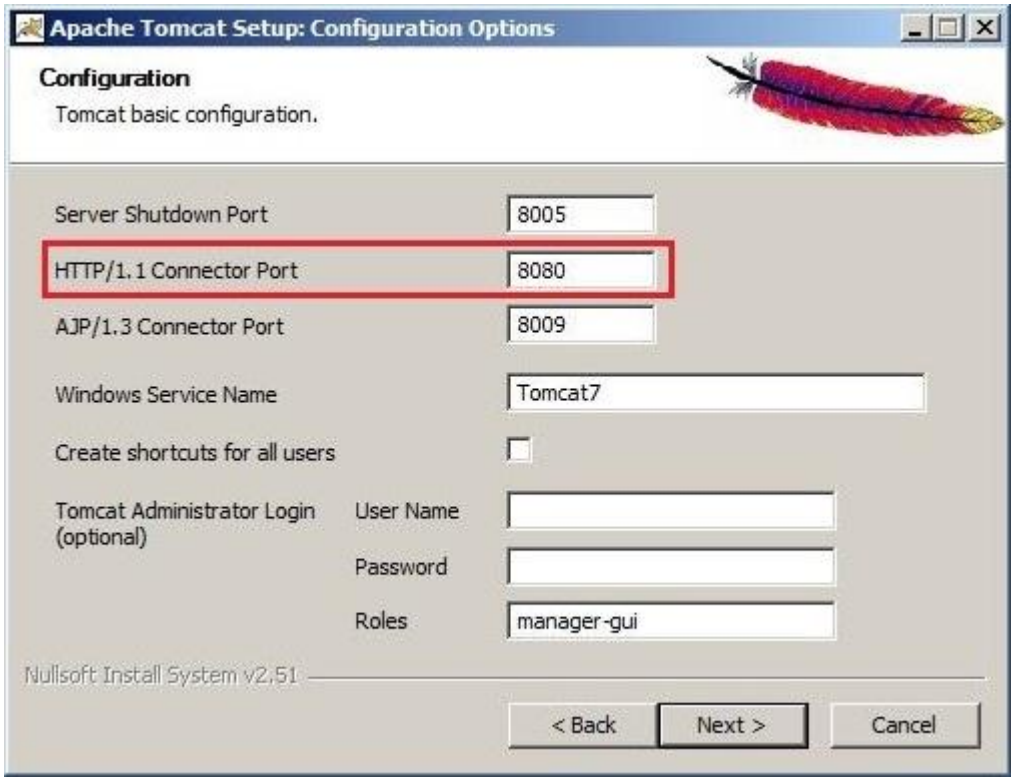
Anforderungen für beide Szenarien:

1. Vergewissern Sie sich, dass Sie eine 64-Bit-Version der Java-Laufzeitumgebung (Java Runtime Environment; JRE) installiert haben. Eine 64-Bit-Version des Java Development Kit (JDK) kann ebenfalls verwendet werden. Sie müssen über die Java-Version 8 oder höher verfügen.
2. Laden Sie eine 64-Bit-Version von Apache Tomcat 7 herunter. Vergewissern Sie sich, dass die Version, die Sie verwenden möchten, nicht neuer ist als die von Files Advanced unterstützte Version. Die von Files Advanced verwendete Version ist im Abschnitt Neuerungen (S. 322) aufgelistet.

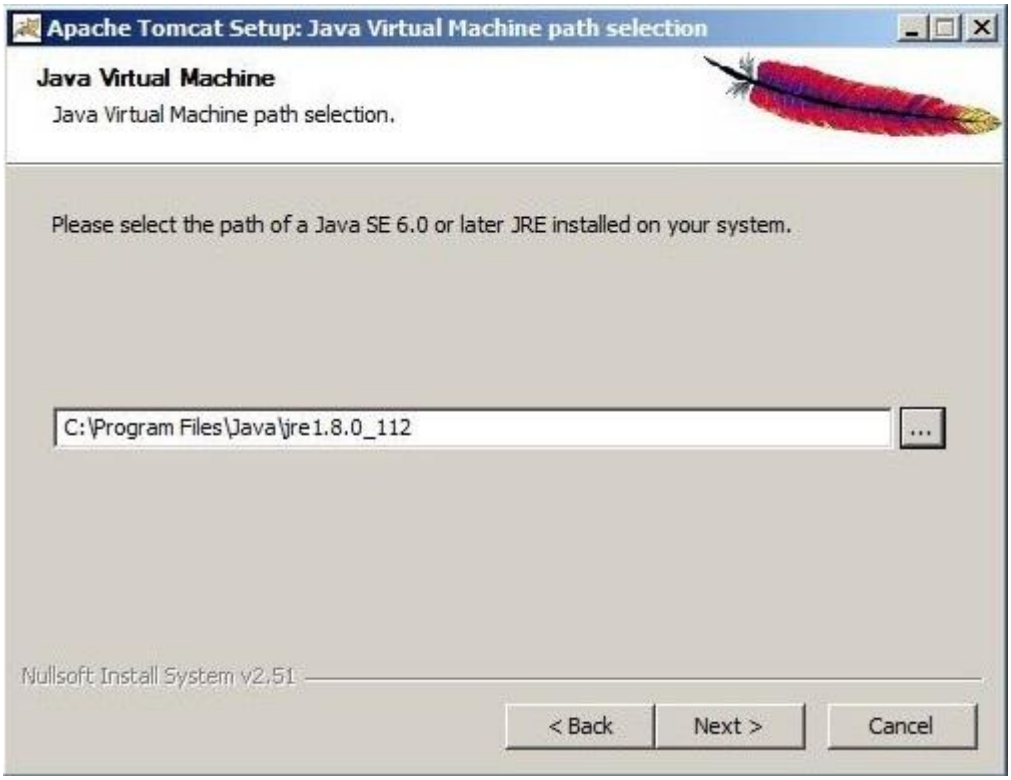
Themen

3.

1. Laden Sie mit der 64-Bit-Version von Apache Tomcat 7 eine Installationsdatei herunter. Die Liste der Versionen finden Sie auf der Website von Apache Tomcat. Suchen Sie die gewünschte Version und klicken Sie darauf. Öffnen Sie dann den bin-Ordner und laden Sie die .exe-Datei (z.B. **apache-tomcat-7.0.50.exe**) herunter.
2. Starten Sie das Installationsprogramm und befolgen Sie die Schritte des Installationsassistenten. Sie können alle Standardeinstellungen verwenden. Sie können den aufgeführten Port bei Bedarf ändern. Der Standard-Port ist 8080.



Hinweis: *Das Installationsprogramm wählt automatisch den Java-Installationsordner aus.*



3. Nachdem die Installation abgeschlossen wurde, navigieren Sie auf Ihrem Computer mit Files Advanced zum Installationsordner von Files Advanced (standardmäßig **`C:\Program Files (x86)\Acronis\Files Advanced\Access Server\`**).
4. Kopieren Sie den Ordner **AccessPreviewServlet** in den Ordner Tomcat-**webapps** des neuen Computer, auf dem Sie Apache Tomcat installiert haben. (standardmäßig C:\Programme\Apache Software Foundation\Tomcat 7.0\webapps)
5. Navigieren Sie zum Ordner **conf** Ihrer Apache Tomcat-Installation (standardmäßig C:\Programme\Apache Software Foundation\Tomcat 7.0\conf) und sichern Sie die Datei **server.xml**.
6. Öffnen Sie jetzt die Datei, suchen Sie die Zeilen **`<Host name="localhost" appBase="webapps" unpackWARs="true" autoDeploy="true">`** und platzieren Sie direkt darunter Folgendes:

```
<!-- for Access Web preview -->
<Context path="/AccessPreviewServlet" docBase="C:\Program Files\Apache Software Foundation\Tomcat 7.0\webapps\AccessPreviewServlet">
</Context>
```

Hinweis: *Wenn Sie Apache Tomcat an einem anderen Speicherort als dem Standardverzeichnis installiert haben, müssen Sie den Pfad* ***docBase=""*** *in den korrekten Pfad Ihrer Installation abändern.*

7. Speichern und schließen Sie die Datei.
8. Zum Starten des Tomcat-Dienstes öffnen Sie **Systemsteuerung** -> **Verwaltung** -> **Dienste**und starten den Apache Tomcat-Dienst.

1. Laden Sie mit der 64-Bit-Version von Apache Tomcat 7 eine **.zip**-Datei herunter. Die Liste der Versionen finden Sie auf der Website von Apache Tomcat. Suchen Sie die gewünschte Version und klicken Sie darauf. Öffnen Sie dann den bin-Ordner und laden Sie die Core-zip-Datei (z.B. **apache-tomcat-7.0.50.zip**) herunter.

2. Extrahieren Sie die Inhalte des Archivs an einem Speicherort Ihrer Wahl, z.B. **C:\Programme\Apache Tomcat.**
3. Navigieren Sie zu **C:\Programme\Apache Tomcat\apache-tomcat-<version>** und öffnen Sie den **bin**-Ordner.

   Hinweis**: Der extrahierte Ordnername enthält eine Versionsnummer. Ersetzen Sie **<version>** durch die Version Ihres Tomcat, z.B. **C:\Programme\Apache Tomcat\apache-tomcat-7.0.75

4. Öffnen Sie **startup.bat** mit einem Textbearbeitungsprogramm und suchen Sie die Zeile **setlocal**.
5. Fügen Sie die folgenden Zeilen darunter ein:

   `set "CATALINA_HOME=Your Tomcat Folder"`

   `e.g. set "CATALINA_HOME=C:\Program Files\Apache Tomcat\apache-tomcat-7.0.75"`

   ***Hinweis:** Damit wird für alle Einstellungen der Tomcat-Standardordner festgelegt. Verwenden Sie den richtigen Pfad für Ihren Apache Tomcat-Ordner.*

   `set "JRE_HOME=Java main folder location"`

   `e.g. set "JRE_HOME=C:\Program Files\Java\jre1.8.0_112"`

   ***Hinweis:** Damit wird für alle Einstellungen der JRE-Standardordner festgelegt. Verwenden Sie den richtigen Pfad für Ihren Java-Ordner.*

   ***Hinweis**: Wenn Sie ein JDK verwenden, lautet der Befehl **JAVA_HOME** statt **JRE_HOME**.*

6. Speichern Sie alle Änderungen an der Datei.
7. Anschließend navigieren Sie auf Ihrem Computer mit Files Advanced zum Installationsordner von Files Advanced (standardmäßig **`C:\Program Files (x86)\Acronis\Files Advanced\Access Server\`**).
8. Kopieren Sie den Ordner **AccessPreviewServlet** in den Ordner Tomcat-**webapps** des neuen Computers, auf dem Sie Apache Tomcat installiert haben (standardmäßig **`C:\Program Files\Apache Tomcat\apache-tomcat-7.0.75\webapps`**).
9. Navigieren Sie zum Ordner **conf** der Apache Tomcat-Installation (z. B. **C:\Program Files\Apache Tomcat\apache-tomcat-7.0.75\conf)** und sichern Sie die Datei **server.xml**.
10. Öffnen Sie jetzt die Datei, suchen Sie die Zeilen **`<Host name="localhost" appBase="webapps" unpackWARs="true" autoDeploy="true">`** und platzieren Sie direkt darunter Folgendes:

```
<!-- for Access Web preview -->
<Context path="/AccessPreviewServlet" docBase="C:\Program Files\Apache Tomcat\apache-tomcat-7.0.75\webapps\AccessPreviewServlet">
</Context>
```

11. Ändern Sie den Pfad **`docBase=""`** in den korrekten Pfad Ihrer Installation. Speichern und schließen Sie die Datei.

    ***Hinweis:** Wenn Sie den Standard-Port, von dem der Server abgehört wird, nicht ändern, wird der Servlet von **8080** abgehört. Zum Ändern des Ports suchen Sie in der Datei **server.xml** die folgenden Zeilen:*

```
<Connector port="8080" protocol="HTTP/1.1"
           connectionTimeout="20000"
           redirectPort="8443" />
```

    *Ersetzen Sie **8080** durch die gewünschte Port-Nummer.*

12. Starten Sie den Tomcat-Dienst, indem Sie zum bin-Ordner navigieren und auf die Datei **startup.bat** doppelklicken. Das schwarze DOS-Fenster muss offen bleiben, während Tomcat ausgeführt wird.

12.2.14.2 Files Advanced Serverkonfigurationen

1. Rufen Sie die Weboberfläche von Files Advanced auf und öffnen Sie **Allgemeine Einstellungen** -> **Webvorschau**.
2. Aktivieren Sie **Benutzerdefinierte URL für Webvorschau-Dienst verwenden** und geben Sie die Adresse für das neue Webvorschau-Servlet ein. (**Beispiel:** **`http://accesswp.company.com:8080`**). Die Port-Nummer muss in der von Ihnen angegebenen URL enthalten sein. Bei Installationen mit Lastenausgleich oder Clusterinstallationen ist die URL die Adresse des Lastausgleichsmodul.
3. Je nach der Anzahl der Server, die Sie für die Ausführung des Webvorschau-Servlet einrichten, möchten Sie möglicherweise die eingestellte Anzahl der Aufrufe für die **Maximale gleichzeitige Generierung** des Files Advanced Server erhöhen.
4. Suchen Sie die Einstellung **Maximale Anzahl gleichzeitiger Generierungsaufrufe** und stellen Sie den entsprechenden Wert ein.

   Der Standardwert ist 2. Das Rendering eines Dokuments kann den Großteil eines Prozessorkerns verbrauchen. Die Anzahl der Rendering-Threads sollte auf maximal 50 % Ihres verfügbaren Prozessorkerns eingestellt werden. Eine Überschreitung dieses empfohlenen Wertes kann zur Verschlechterung anderer Dienste auf dem Server führen.

12.2.14.3 Lastenausgleich für Ihre Webvorschau-Servlets

Ihre **Webvorschau**-Servlets müssen hinter einem Lastenausgleichsmodul platziert werden.

1. Aktivieren Sie die dauerbasierte Sitzungs-Stickiness (oder die entsprechende Einstellung Ihres Lastenausgleichsmoduls) im Lastenausgleichsmodul, und konfigurieren Sie sie so, dass sie nicht abläuft.
2. Wenn eine Integritätsprüfung erforderlich ist (bei der der HTTP-Status 200 zurückgegeben werden sollte), reicht ein Ping an **http://servername.yourdomain.com:port/AccessPreviewServlet/generate_preview/**.

   Beispiel:**`https://servlet1.acme.com/AccessPreviewServlet/generate_preview`** und **`https://servlet2.acme.com/AccessPreviewServlet/generate_preview`**.
3. Öffnen Sie bei Verwendung eines Browsers Ihr lokales Lastenausgleichsmodul, um zu überprüfen, ob die Konfiguration funktioniert.

   Beispiel: **`https://loadbalancer.yourdomain.com`**

12.2.15 PostgreSQL Streaming Replication

Zweck dieses Dokuments ist die Beschreibung der verschiedenen Schritte, die bei der Konfiguration der Streaming Replication (SR) zwischen zwei PostgreSQL-Servern auszuführen sind. Streaming Replication ist eine von vielen Methoden, mit denen eine PostgreSQL-Datenbank online bereitgehalten werden kann. Andere Methoden werden in diesem Dokument allerdings nicht beschrieben.

Hinweis: *In diesem Dokument wird nicht die Installation von PostgreSQL oder Files Advanced, sondern lediglich die Konfiguration der Streaming Replication beschrieben.*

Streaming Replication

Das Streaming-Replication-Verfahren basiert auf WAL-Segmenten (Write-Ahead Logging). WAL ist eine Standardverfahren, das die Integrität der Daten gewährleistet. Das Grundprinzip der WAL-Technologie ist, dass Änderungen an Datendateien (in denen sich Tabellen und Indizes befinden) erst geschrieben werden dürfen, nachdem diese Änderungen protokolliert worden sind. Zuerst müssen Protokolldatensätze, in denen die Änderungen beschrieben werden, in den dauerhaften Speicher geleert worden sein. Wenn dieser Ablauf eingehalten wird, brauchen nicht bei jedem Transaktionscommit Datenseiten auf das Laufwerk geleert zu werden, denn bei einem Absturz kann die Datenbank anhand des Protokolls wiederhergestellt werden: Änderungen, die noch nicht auf die Datenseiten angewendet worden sind, können anhand der Protokolldatensätze nachgetragen werden.

Bei Verwendung des WAL-Mechanismus fällt eine deutlich geringe Anzahl Laufwerkschreibvorgänge an. Das erklärt sich dadurch, dass für die Ausführung eines Transaktionscommits nicht jede einzelne von der Transaktion geänderte Datendatei auf das Laufwerk geleert zu werden braucht, sondern nur die Protokolldatei. Die Protokolldatei wird sequenziell geschrieben. Deshalb ist der Aufwand für die Synchronisierung des Protokolls deutlich geringer als für das Leeren der Datenseiten.

Mit der WAL-Technologie können außerdem Online-Backups, Zeitpunktwiederherstellung und Replikationen unterstützt werden. Streaming Replication bezeichnet die fortlaufende Übertragung von WAL-Datensätzen über eine TCP/IP-Verbindung zwischen einem Primärserver und einem Standbyserver. Diese Übertragung erfolgt mit dem Walsender-Protokoll über Replikationsverbindungen. Streaming Replication kann zwar synchron ablaufen, allerdings haben wir angesichts der benötigten Ressourcen und Auswirkungen eines synchronen Prozesses auf die Leistung beschlossen, nur die asynchrone Streaming Replication als praktikables Szenario zu akzeptieren.

Anforderungen:

- Zwei PotsgreSQL-Server: Bei diesem Verfahren wird der aktive Server als "Primärserver" und der passive Server als "Standbyserver" bezeichnet.

  ***Hinweis**: **Nur der Primärserver kann für Files Advanced Verbindungen verwendet werden.** Der Standbyserver kann nur verwendet werden, wenn bei einem Failover zum Primärserver hochgestuft wird.*

- PostgreSQL 9.4: Da Funktionen wie "Replikations-Slot" eingeführt werden, wird PostgreSQL 9.4 benötigt. Diese Version ist derzeit in Acronis Access Advanced 7.2 integriert und wird nur bei Neuinstallationen (nicht bei Upgrades) installiert.
- Eine virtuelle IP (optional): Diese virtuelle IP-Adresse wird in allen Front-Ends verwendet, die als Files Advanced Server fungieren. Der Eigentümer muss immer der aktive Host (der Primärserver) sein.
- Zu empfehlen sind folgende Vorbereitungen: Files Advanced ist bereits installiert und die Datenbank des Primärservers ist initialisiert worden.

Themen

12.2.15.1 Auf dem Primärserver

Einen Replikationsbenutzer erstellen

Der Replikationsprozess verwendet diesen Benutzer, um WAL-Segmente vom Primärserver zum Standbyserver zu senden. Aus Sicherheitsgründen wird empfohlen, einen bestimmten Benutzer mit Replikationsrechten zu erstellen, statt ein Standard-Superuser-Konto (d.h. **postgres**) zu verwenden.

1. Führen Sie auf dem Primärserver den folgenden Befehl aus:

   ```
   psql -c "CREATE USER replicator REPLICATION LOGIN ENCRYPTED PASSWORD 'XXXXX';" -U postgres
   ```

   Dieser Befehl kann auch remote mit folgenden Optionen ausgeführt werden:

   ```
   psql -c "CREATE USER replicator REPLICATION LOGIN ENCRYPTED PASSWORD 'XXXXX';" -h <IP_OF_PRIMARY_SERVER> -U postgres
   ```

   Hinweis: *PSQL befindet sich im Unterordner **bin** des Installationsordners von PostgreSQL. Abhängig von der Umgebungsvariablen PATH müssen Sie möglicherweise den Pfad zu dem Befehl angeben oder zu dem richtigen Verzeichnis gehen, bevor Sie den Befehl ausführen können. Dieser Hinweis betrifft auch die nächsten bei diesem Vorgang verwendeten Befehle.*

Zugriff konfigurieren

Bearbeiten Sie die Zugriffssteuerung auf dem Primärserver, sodass vom Standbyserver aus eine Verbindung hergestellt werden kann.

1. Fügen Sie dazu in der Datei **pg_hba.conf** (befindet sich im Unterordner **data**) folgende Zeile hinzu:

   ```
   host replication replicator <IP_OF_STANDBY_SERVER>/32 trust
   ```

2. Wenn die Sicherheit zwischen den Datenbankservern erhöht werden muss, kann der Server im Zuge der Authentifizierung aufgefordert werden, ein verschlüsseltes Kennwort (md5) zu übergeben bzw. nur die SSL-Verschlüsselung (**hostssl**) zuzulassen. Beispiel:

   ```
   host replication replicator <IP_OF_STANDBY_SERVER>/32 md5
   hostssl replication replicator <IP_OF_STANDBY_SERVER>/32 md5
   ```

Streaming Replication konfigurieren

1. Navigieren Sie zum PostgreSQL-Installationsordner. Der Ordner befindet sich standardmäßig unter `C:\Program Files (x86)\Acronis\Access\Common\PostgreSQL\9.4`
2. Navigieren Sie zum Ordner `Data` und ändern Sie die Datei `postgresql.conf`. Suchen und bearbeiten Sie folgende Zeilen:

   Hinweis: *Stellen Sie sicher, dass diese Zeilen nicht mit dem Symbol **#** beginnen. Zeilen, die mit diesem Symbol beginnen, werden als Kommentare betrachtet und haben keinerlei Auswirkungen.*

   - `listen_address = 'IP_OF_PRIMARY_SERVER,` 127.0.0.1'
   - `wal_level = hot_standby`
   - `max_wal_senders = 3`
   - `checkpoint_segments = 8`
   - `wal_keep_segments = 8`
   - `max_replication_slots = 3`
3. Starten Sie den PostgreSQL-Dienst neu, nachdem Sie die Änderungen oben ausgeführt haben.

Replikations-Slot erstellen

1. Führen Sie auf dem Primärserver den folgenden Befehl aus:

   ```
   psql -U postgres -c "SELECT * FROM
   pg_create_physical_replication_slot('access_slot');"
   ```

2. Prüfen Sie mit folgendem Befehl, ob der Slot erstellt worden ist:

   ```
   psql -U postgres -c "SELECT * FROM pg_replication_slots;"
   ```

12.2.15.2 Auf dem Standbyserver

Prüfen Sie, ob alle notwendigen Server aufeinander zugreifen können

Bei einem Failover wird der Standbyserver zum Primärserver hochgestuft und beantwortet alle Anfragen von Files Advanced Servern.

Es wird empfohlen, für alle Files Advanced Server den Zugriff auf den Standbyserver bereits jetzt zu konfigurieren, damit der PostgreSQL-Dienst während des Failover-Vorgangs nicht auf einem Standbyserver neu gestartet werden muss.

Hinweis: *Wenn der Standbyserver sich im Bereitschaftsmodus befindet, ist die Datenbank schreibgeschützt (Hot Standby). Es ist also nicht möglich, den Standbyserver versehentlich als Produktionsdatenbank zu konfigurieren und zu verwenden.*

1. Bearbeiten Sie die Zugriffssteuerung auf dem Standbyserver, sodass von allen Files Advanced Servern aus eine Verbindung hergestellt werden kann.
2. Navigieren Sie hierfür zum PostgreSQL-Installationsordner, und fügen Sie dazu in der Datei **pg_hba.conf** (befindet sich im Unterordner **`data`**) für jeden Server folgende Zeile hinzu:

   ```
   host replication replicator <IP_OF_ACCESS_SERVER_1>/32 md5
   host replication replicator <IP_OF_ACCESS_SERVER_2>/32 md5
   ```

Streaming Replication konfigurieren

1. Navigieren Sie zum PostgreSQL-Installationsordner. Der Ordner befindet sich standardmäßig unter **`C:\Program Files (x86)\Acronis\Access\Common\PostgreSQL\9.4`**
2. Navigieren Sie zum Ordner **`Data`** und ändern Sie die Datei **`postgresql.conf`**. Suchen und bearbeiten Sie folgende Zeilen:

   Hinweis: *Stellen Sie sicher, dass diese Zeilen nicht mit dem Symbol **#** beginnen. Zeilen, die mit diesem Symbol beginnen, werden als Kommentare betrachtet und haben keinerlei Auswirkungen.*

   - **`listen_address = 'IP_OF_STANDBY_SERVER,`** 127.0.0.1**'**
   - **`wal_level = hot_standby`**
   - **`max_wal_senders = 3`**
   - **`checkpoint_segments = 8`**
   - **`wal_keep_segments = 8`**
   - **`max_replication_slots = 3`**
   - **`hot_standby = on`**

   Die Einstellung von **`hot_standby`** bestimmt, ob während der Streaming Replication Verbindungen hergestellt und Abfragen ausgeführt werden können. Bei Aktivierung akzeptiert die Datenbank Anfragen mit Nur-Lese-Zugriff, sodass die Datenbanktabellen eingesehen werden

können und anhand der Inhalte geprüft werden kann, ob der Replikationsvorgang ordnungsgemäß abläuft.

Hinweis: *Wenn Sie* ***md5*** *oder* ***password*** *in* ***pg_hba.conf*** *als Authentifizierungsmethode angeben möchten, wird für die Verbindung ein Kennwort benötigt. Sie müssen den folgenden Befehl zur Datei* ***recovery.conf*** *auf dem Standbyserver hinzufügen, um dieses Kennwort 'eingeben' zu können.*

primary_conninfo = 'host=<*IP_ADDRESS_OF_PRIMARY_SERVER****> port=<****PORT_OF_PRIMARY_SERVER****> user=<****USERNAME****> password=<****PASSWORD_FOR_USERNAME****>'***

So würde beispielsweise der Befehl lauten, wenn Postgres auf IP 10.0.0.1, Port 5432 mit dem Benutzer ***replicator*** *und dem Kennwort* ***1234****:* ***primary_conninfo = 'host=10.0.0.1 port=5432 user=replicator password=1234'*** *ausgeführt würden.*

3. **Halten Sie den PostgreSQL-Dienst auf dem Primärserver an, um das erste Seeding der Datenbank auszuführen und dann den Streaming-Replication-Vorgang zu starten.**

Konfigurationsdateien sichern

Erstellen Sie ein Backup aller **.conf**-Konfigurationsdateien, wie z.B.: **pg_hba.conf**, **postgresql.conf**, **pg_ident.conf**. Diese Dateien werden bei dem anfänglichen Seeding-Vorgang überschrieben und müssen im Anschluss an diesen Schritt wiederhergestellt werden.

Verzeichnis 'data' bereinigen

Löschen Sie den Unterordner **data** , oder benennen Sie ihn um. Das Umbenennen des Ordners bietet sich an, wenn Sie eine Kopie der vorherigen Konfiguration behalten möchten. Dann kann die Datenbank des Standbyservers in einem konsistenten Zustand wiederhergestellt werden, wenn während des anfänglichen Seedings oder bei Hochfahren der Datenbank Probleme auftreten sollten.

Anfängliches Seeding

Für das anfängliche Seeding wird ein Backup der primären Datenbank in einem Ordner auf dem Standbyserver erstellt.

1. Stellen Sie sicher, dass der Primärserver nicht aktiv verwendet wird. Am einfachsten geht dies, indem Sie den Files Advanced Tomcat-Dienst anhalten und ihn wieder starten, sobald der Seeding-Vorgang abgeschlossen wurde.
2. Das anfängliche Seeding wird auf Standbyserver-Ebene mit folgendem Befehl gestartet:

   pg_basebackup.exe -h <IP_OF_PRIMARY_SERVER> -D <PATH_TO_NEW_DATA_DIR> -U replicator -v -P --xlog-method=stream

   Hinweis: ***<PATH_TO_NEW_DATA_DIR>*** *sollte der Pfad zum umbenannten/gelöschten Ordner* ***Data*** *sein, z.B.:* ***C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL\9.4\Data***

Konfigurationsdateien wiederherstellen

Kopieren Sie alle **.conf**-Konfigurationsdateien (einschließlich **pg_hba.conf**, **postgresql.conf**, **pg_ident.conf**) aus dem Backup-Ordner in den neuen **Data** -Ordner, und überschreiben Sie dabei alle vorhandenen Dateien.

Streaming-Replication-Befehle

1. Öffnen Sie den Datenordner und erstellen (oder ändern) Sie die Datei **recovery.conf**.
2. Fügen Sie die folgenden Zeilen hinzu, falls diese noch nicht vorhanden sind:
   - **standby_mode = 'on'**
   - **primary_conninfo = 'host=<IP_OF_PRIMARY_SERVER> port=5432 user=replicator password= <PASSWORD_USED_FOR_REPLICATOR_USER>'**
   - **primary_slot_name = 'access_slot'**
   - **trigger_file = '<PATH_TO_TRIGGER_FILE>' # As an example 'failover.trigger'**
   - **recovery_min_apply_delay = 5min**
3. Starten Sie den PostgreSQL-Dienst auf dem Standbyserver, nachdem Sie die Änderungen oben gespeichert haben.

   Hinweis: *Im Falle eines Failovers wird die Datei* ***recovery.conf*** *in* ***recovery.done*** *umbenannt.*

Zusätzliche Informationen

- Die Einstellung **standby_mode** bestimmt, dass der PostgreSQL-Server als Standbyserver gestartet wird. In diesem Fall hält der Server die Wiederherstellung auch dann nicht an, wenn das Ende der archivierten WAL-Segmente erreicht ist. Er versucht weiterhin, die Wiederherstellung durch Abrufen neuer WAL-Segmente fortzusetzen und die Verbindung zum Primärserver herzustellen. Dabei verwendet er die bei **primary_conninfo** festgelegte Zeichenfolge (vom Standbyserver für die Verbindung zum Primärserver zu verwenden).
- An dieser Stelle ist der in den vorherigen Schritten auf dem Primärserver erstellte Replikations-Slot entsprechend der Einstellung **primary_slot_name** zu verwenden.
- Die Einstellung **trigger_file** nennt eine Trigger-Datei, die die Wiederherstellung auf dem Standbyserver beendet und ihn zum Primärserver macht. Diese Datei wird während des Failover-Vorgangs verwendet.
- Optional können auch **recovery_min_apply_delay**-Einstellungen festgelegt werden. Standardmäßig stellt ein Standbyserver vom Primärserver kommende WAL-Datensätze umgehend wieder her. Empfehlenswert ist, eine zeitverzögerte Kopie der Daten bereitzuhalten, sodass ggf. Datenverluste korrigiert werden können. Dieser Parameter erlaubt es, die Wiederherstellung um eine bestimmte Zeitspanne zu verzögern. Wenn keine Einheit festgelegt ist, erfolgt die Angabe in Millisekunden.

  Wenn Sie für diesen Parameter beispielsweise 5 Minuten angeben, wird der Standbyserver jeden Transaktionscommit erst wiedergeben, wenn die Systemzeit auf dem Standbyserver mindestens fünf Minuten weiter ist als die vom Primärserver gemeldete Commitzeit.

  Es ist möglich, dass die Replikationsverzögerung zwischen Servern den Wert dieses Parameters überschreitet. In diesem Fall wird keine Verzögerung hinzugefügt. Hinweis: Die Verzögerung wird anhand des vom Primärserver aufgebrachten WAL-Zeitstempels und der aktuellen Zeit auf dem Standbyserver berechnet. Verzögerungen bei der Übertragung, die durch Zeitverzögerungen auf dem Netzwerk oder durch überlappende Replikationskonfigurationen verursacht werden, können die effektive Wartezeit erheblich verkürzen. Wenn die Systemuhren auf dem Primärserver und dem Standbyserver nicht synchron laufen, werden Datensätze bei der Wiederherstellung möglicherweise früher als erwartet angewendet. Das ist allerdings kein größeres Problem, denn die Einstellungen dieses Parameters sind viel höher als die typischen Zeitabweichungen zwischen Servern.

12.2.15.3 Testen des Failovers

Wir empfehlen, die Einstellungen oben zu testen und sicherzustellen, dass der Failover funktioniert, bevor Sie ihn in Ihre Produktionskonfiguration implementieren.

Der Primärserver wurde nicht heruntergefahren, halten Sie ihn daher an, bevor Sie den Standbyserver für die Rolle als Primärserver konfigurieren. Dies ist notwendig, damit der Primärserver keine weiteren Abfragen verarbeitet, was zu Problemen führen würde.

Sie können den Standbyserver ganz einfach zum Primärserver machen, indem Sie die in der Datei **recovery.conf** genannte Trigger-Datei erstellen. Da der Standbyserver nun die Rolle des Primärservers übernommen hat, sollten Sie sicherstellen, dass die Files Advanced-Server für die Verwendung dieses Servers konfiguriert wurden.

Hinweis: *Nachdem der Failover-Vorgang ausgelöst und erfolgreich durchgeführt wurde, wird die Datei* ***`recovery.conf`*** *in* ***`recovery.done`*** *umbenannt.*

Navigieren Sie dazu zu **`C:\Program Files (x86)\Acronis\Files Advanced\Access Server`** und bearbeiten Sie **`acronisaccess.cfg`**. Stellen Sie sicher, dass **DB_HOSTNAME** und **DB_PORT** auf die Adresse und den Port ausgerichtet sind, deren PostgreSQL-Server derzeit der Primärserver ist. Wenn Sie Änderungen vornehmen, müssen Sie den Files Advanced Tomcat-Dienst neu starten.

12.2.16 PostgreSQL für Remote-Zugriff konfigurieren

Remote-Zugriff kann Ihnen behilflich sein, wenn Sie mehrere PostgreSQL-Instanzen verwalten oder Sie Ihre Datenbank gerne per Remote-Zugriff verwalten möchten.

Um den Remote-Zugriff für diese PostgreSQL-Instanz zu aktivieren, befolgen Sie die unten aufgeführten Schritte:

1. Navigieren Sie zum PostgreSQL-Installationsverzeichnis: **`C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL\9.4\Data\`**
2. Bearbeiten Sie **pg_hba.conf** mit einem Texteditor.
3. Beziehen Sie die Host-Einträge für jeden Computer ein, der mittels der internen Adresse Remote-Zugriff erhält, und speichern Sie die Datei. Die **pg_hba.conf**-Datei (HBA steht für host-basierte Authentifizierung) steuert die Client-Authentifizierung und wird im Datenverzeichnis des Datenbank-Clusters gespeichert. Darin geben Sie an, welche Server eine Verbindung herstellen dürfen und welche Berechtigungen sie haben sollen, z.B.:

   ```
   # TYPE  DATABASE  USER  ADDRESS              METHOD
   # First Files Advanced & Gateway server
   host      all        all   10.27.81.3/32     md5
   # Second Files Advanced & Gateway server
   host      all        all   10.27.81.4/32     md5
   In these examples all users connecting from the first computer (10.27.81.3/32)
   and the second computer (10.27.81.4/32) can access the database with full
   privileges (except the replication privilege) via a md5 encrypted connection.
   ```
4. Gehen Sie zu und öffnen Sie die Datei **postgresql.conf**. Der Ordner befindet sich standardmäßig unter: **`C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL\9.4\Data\`**
   a. Finden Sie die Zeile **`#listen_addresses = 'localhost'`**
   b. Aktivieren Sie diesen Befehl, indem Sie das **#**-Symbol am Beginn der Zeile entfernen.

c. Ersetzen Sie **`localhost`** mit *, um an allen verfügbaren Adressen abzurufen. Wenn Sie PostgreSQL nur an einer bestimmten Adresse abrufen möchten, geben Sie die IP-Adresse statt * an.

   - **z.B. `listen_addresses = '*'`** - Das bedeutet, dass PostgreSQL an allen verfügbaren Adressen abgerufen werden kann.
   - **Beispiel: `listen_addresses = '192.168.1.1'`** – Das bedeutet, dass PostgreSQL nur an dieser Adresse abgerufen werden kann.

5. Speichern Sie alle Änderungen an **postgresql.conf**.
6. Starten Sie den Files Advanced PostgreSQL-Dienst neu.

Hinweis: *PostgreSQL verwendet standardmäßig Port 5432. Stellen Sie sicher, dass dieser Port in jeder Firewall oder Routing-Software geöffnet ist.*

12.2.17 Files Advanced in HTTP-Modus ausführen

Diese Einstellungen werden für Situationen bereitgestellt, in denen Sie unverschlüsselte HTTP-Kommunikation zwischen Files Advanced und internen Diensten verwenden müssen, z.B. Lastenausgleich und Proxy-Lösungen. Files Advanced Server, die über unsichere lokale Netzwerke und über das Internet kommunizieren, sollten immer im HTTPS-Modus betrieben werden. Bei interner Ausführung im HTTP-Modus ist der Files Advanced Netzwerk-Traffic für alle Parteien mit Zugriff auf das interne Netzwerk leicht sichtbar.

Zum Umschalten von HTTPS zu HTTP müssen Einstellungen in den folgenden Dateien bearbeitet werden:

- Tomcat **`server.xml`** -Datei, unter **`C:\Program Files (x86)\Acronis\Files Advanced\Common\apache-tomcat-7.0.75\conf`**

  Hinweis: *Die Tomcat Versionsnummer kann sich je nach der von Ihnen verwendeten Version von Files Advanced unterscheiden.*

- Die Datei **`acronisaccess.cfg`**, unter **`C:\Program Files (x86)\Acronis\Files Advanced\Access Server`**.

Bearbeiten der Datei server.xml

In dieser Datei müssen der geeignete HTTP-Konnektor eingestellt und die HTTPS-Konnektoren deaktiviert werden.

1. Öffnen Sie die Datei mit einem Texteditor und suchen Sie nach dem vorhandenen HTTPS-Konnektor. Dieser muss wie folgt aussehen:

```
<Connector maxHttpHeaderSize="65536" maxThreads="150"
enableLookups="false" disableUploadTimeout="true" acceptCount="100"
scheme="https" secure="true" SSLEnabled="true"
SSLProtocol="TLSv1+TLSv1.1+TLSv1.2"
SSLCertificateFile="${catalina.base}/conf/AAServer_LocalHost.crt"
SSLCertificateKeyFile="${catalina.base}/conf/AAServer_LocalHost.key"
SSLHonorCipherOrder="true"
SSLCipherSuite="ECDH+AESGCM:ECDH+AES256:ECDH+AES128:RSA+AESGCM:RSA+AES:
!aNULL:!eNULL:!LOW:!3DES:!RC4:!MD5:!EXP:!PSK:!SRP:!DSS"
connectionTimeout="-1" URIEncoding="UTF-8" bindOnInit="false" port="443"
address="0.0.0.0"/>
```


2. Deaktivieren Sie den HTTPS-Konnektor, indem Sie ihn mit **<!--** und **-->** umgeben. Fügen Sie also **<!--** vor **<Connector maxHttp.**.... und **-->** hinter ... ein. **address="0.0.0.0"/>**
3. Erstellen Sie einen neuen HTTP-Konnektor, der wie folgt aussieht:

   ```
   <Connector maxHttpHeaderSize="65536" maxThreads="150"
   enableLookups="false" disableUploadTimeout="true" acceptCount="100"
   scheme="http" secure="true" connectionTimeout="-1" URIEncoding="UTF-8"
   port="80" address="0.0.0.0"/>
   ```
4. Sie können einen anderen Port neben dem Standard auswählen und die Adressen für die Verbindung mit einem bestimmten Port beschränken, sodass der Dienst nicht alle verfügbaren Adressen verwendet.
5. Stellen Sie sicher, dass der Port, den Sie verwenden möchten, in Ihrer Firewall offen ist.
6. Überprüfen Sie, ob Sie über diesen Umleitungskonnektor in Ihrer Datei server.xml verfügen:

   ```
   <!--  <Connector port="80" connectionTimeout="20000" protocol="HTTP/1.1"
   redirectPort="443"/> -->
   ```
7. Ist dies der Fall, und möchten Sie Port 80 verwenden, deaktivieren Sie diesen durch Kommentieren mit **<!–** und **–>**, wie oben beschrieben.
8. Speichern Sie die Datei, nachdem Sie die erforderlichen Änderungen vorgenommen haben.

Bearbeiten von acronisaccess.cfg

Hier muss nur die **REQUIRE_SSL** am Ende der Datei von **wahr** auf **falsch** eingestellt werden, sodass sie wie folgt aussieht:

```
REQUIRE_SSL = false
```

1. Speichern Sie die Datei, nachdem Sie die erforderlichen Änderungen vorgenommen haben.
2. Starten Sie den Files Advanced Tomcat-Dienst neu, damit alle Änderungen übernommen werden.

Beschränkungen des HTTP-Modus

- Im **HTTP**-Modus wird die Kommunikation mit dem Gateway Server nicht unterstützt, da der Gateway erfordert, dass **HTTPS** funktioniert. Netzwerkknotenzugriff über die Web UI oder mobile Clients funktionieren nicht.
- Einzelanmeldung wird nicht unterstützt.
- Bei Verwendung von Desktop Clients muss **HTTP** manuell im Serveradressenfeld angegeben werden, da die Verbindung ansonsten fehlschlägt. Zum Beispiel **http://myaccess.com:3000**

12.2.18 Upgrade von Files Advanced auf einem Microsoft Failover Cluster durchführen

Die folgenden Schritte helfen Ihnen dabei, ein Upgrade Ihres Files Advanced Server-Clusters auf eine neue Version von Files Advanced durchzuführen.

Hinweis: *Sehen Sie sich vor der Durchführung eines Upgrades unsere Artikel zum Thema Backup (S. 153) an, und sichern Sie Ihre Konfiguration.*

1. Gehen Sie zum aktiven Knoten.
2. Öffnen Sie die **Clusterverwaltung**/den **Failovercluster-Manager**.

3. Halten Sie alle Files Advanced Dienste an (darunter auch **postgres-beliebige-version**). Das freigegebene Laufwerk muss online geschaltet sein.

4. Deaktivieren Sie alle vorhandenen Virenschutzprogramme, da sie unter Umständen den Installationsvorgang unterbrechen und somit eine fehlerhafte Installation verursachen können.
5. Doppelklicken Sie auf die ausführbare Installationsdatei.

6. Drücken Sie **Weiter**, um zu beginnen.
7. Lesen und akzeptieren Sie die Lizenzvereinbarung.
8. Drücken Sie **Upgrade**.

9. Überprüfen Sie die zur Installation ausgewählten Komponenten und klicken Sie auf **Installieren**.

10. Geben Sie das Kennwort des **postgres**-Super-Users ein und drücken Sie **Weiter**.
11. Drücken Sie nach Abschluss der Installation **Beenden**, um den Installer zu schließen.

    Warnung! *Schalten Sie die Cluster-Gruppe nicht online!*

12. Verschieben Sie die Cluster-Gruppe zum zweiten Knoten.
13. Schließen Sie denselben Installationsvorgang auf dem zweiten Knoten ab.
14. Schalten Sie alle Files Advanced Dienste online.

12.2.19 Files Advanced auf einem Microsoft Failover Cluster installieren

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

Die nachfolgend aufgeführten Anleitungen helfen Ihnen beim Installieren von Files Advanced in einem Cluster.

Themen

12.2.19.1 Files Advanced auf einem Microsoft Windows 2008 (R2)-Failover-Cluster installieren

Files Advanced installieren

Sie müssen als Domänenadministrator angemeldet sein, um Files Advanced installieren zu können.

1. Laden Sie das Installationsprogramm für Files Advanced 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 ausführbare Installationsdatei.

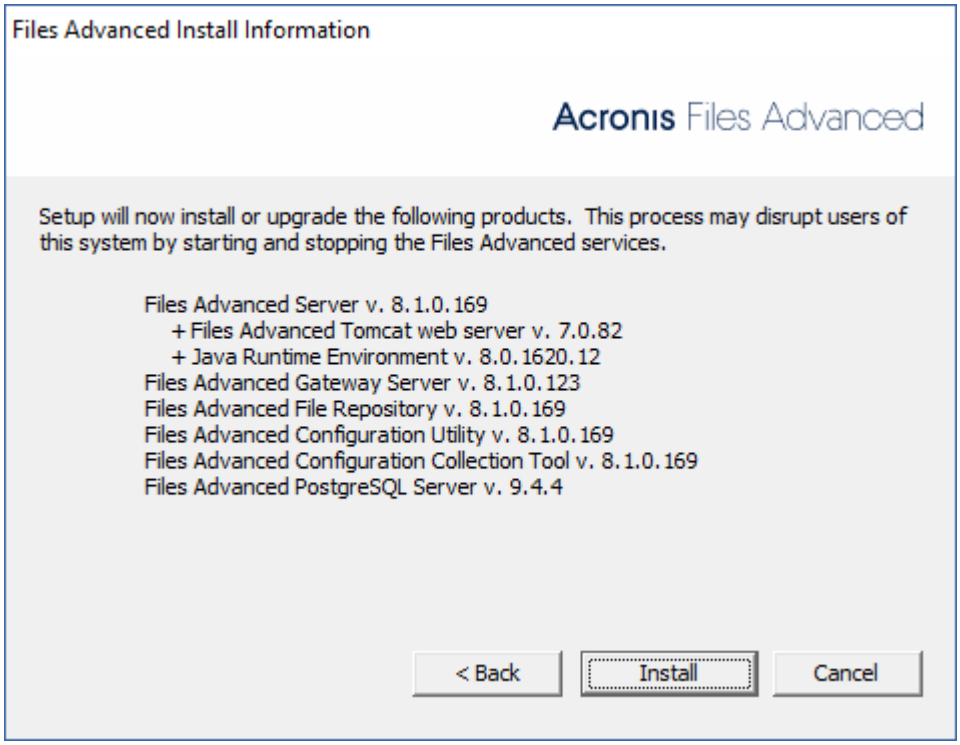
4. Drücken Sie **Weiter**, um zu beginnen.

   Lesen und akzeptieren Sie die Lizenzvereinbarung.

5. Drücken Sie **Installieren**.

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

6. Verwenden Sie den Standardpfad oder wählen Sie einen neuen aus dem Hauptordner von Files Advanced und drücken Sie OK.



7. Legen Sie ein Kennwort für den Benutzer 'Postgres' fest, und notieren Sie es. Sie benötigen dieses Kennwort für Backup- und Wiederherstellungsaktionen der Datenbank.
8. Wählen Sie auf einem freigegebenen Laufwerk einen Speicherort für den Ordner **Postgres Data** und drücken Sie **Weiter**.

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

Wenn der Installationsvorgang für Files Advanced abgeschlossen ist, drücken Sie Beenden.

Die Dienstgruppe erstellen

1. Öffnen Sie die **Failover-Clusterverwaltung** und erweitern Sie Ihr Cluster.
2. Klicken Sie mit der rechten Maustaste auf **Dienste und Anwendungen** und wählen Sie **Weitere Aktionen**.
3. Wählen Sie die Option **Leeren Dienst oder leere Anwendung erstellen** und drücken Sie **Weiter**. Geben Sie der Dienstgruppe einen geeigneten Namen (Beispiel: Files Advanced, AAS Cluster).

Konfigurationen auf dem aktiven Knoten

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

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

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

Alle erforderlichen Dienste der Files Advanced Dienstgruppe hinzufügen

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

1. Klicken Sie mit der rechten Maustaste auf die Files Advanced Dienstgruppe und wählen Sie **Ressource hinzufügen**.
2. Wählen Sie **Allgemeiner Dienst** aus.
3. Wählen Sie den geeigneten Dienst aus und drücken Sie **Weiter**.
4. Drücken Sie im Bestätigungsfenster **Weiter**.
5. Drücken Sie im Fenster **Registrierungseinstellungen replizieren Weiter**.
6. Drücken Sie im Zusammenfassungsfenster **Fertig stellen**.

Einen Clientzugriffspunkt festlegen

1. Klicken Sie mit der rechten Maustaste auf die Files Advanced Dienstgruppe und wählen Sie **Ressource hinzufügen**.
2. Wählen Sie **Clientzugriffspunkt** aus.
3. Geben Sie einen Namen für diesen Zugriffspunkt ein.
4. Wählen Sie ein Netzwerk.
5. Geben Sie die IP-Adresse ein und drücken Sie **Weiter**.
6. Drücken Sie im Bestätigungsfenster **Weiter**.
7. Drücken Sie im Zusammenfassungsfenster **Fertig stellen**.

Ein freigegebenes Laufwerk hinzufügen

1. Klicken Sie mit der rechten Maustaste auf die Files Advanced-Dienstgruppe und wählen Sie **Speicher hinzufügen**.
2. Wählen Sie das gewünschte freigegebene Laufwerk aus.
3. Drücken Sie im Bestätigungsfenster **Weiter**.

4. Drücken Sie im Zusammenfassungsfenster **Fertig stellen**.

Abhängigkeiten konfigurieren

1. Doppelklicken Sie auf die Files Advanced Dienstgruppe.

Führen Sie für PostgreSQL und das Files Advanced Datei-Repository-Dienste Folgendes durch:

1. Klicken Sie mit der rechten Maustaste auf den entsprechenden Dienst und wählen Sie **Eigenschaften**.
2. Klicken Sie auf die Registerkarte **Abhängigkeiten**.
3. Klicken Sie auf **Ressource** und wählen Sie das freigegebene Laufwerk aus, das Sie hinzugefügt haben.

4. Drücken Sie **Anwenden** und schließen Sie das Fenster.

Führen Sie für PostgreSQL außerdem Folgendes aus:

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

Führen Sie für den Files Advanced Gateway Server-Dienst Folgendes aus:

1. Klicken Sie mit der rechten Maustaste auf den entsprechenden Dienst und wählen Sie **Eigenschaften**.
2. Klicken Sie auf die Registerkarte **Abhängigkeiten**.
3. Klicken Sie auf **Ressource** und wählen Sie das freigegebene Laufwerk aus, das Sie hinzugefügt haben, sowie den **Netzwerknamen** (der zugleich der Name des Clientzugriffspunkts ist).

4. Drücken Sie **Anwenden** und schließen Sie das Fenster.

Führen Sie für den Files Advanced Tomcat-Dienst Folgendes aus:

1. Klicken Sie mit der rechten Maustaste auf den entsprechenden Dienst und wählen Sie **Eigenschaften**.
2. Klicken Sie auf die Registerkarte **Abhängigkeiten**.
3. Klicken Sie auf **Ressource** und wählen Sie die PostgreSQL und Files Advanced Gateway Server-Dienste als Abhängigkeiten aus. Drücken Sie **Anwenden** und schließen Sie das Fenster.

Hinweis: *Wenn die Gateway und Access Server auf verschiedenen IP-Adressen ausgeführt werden sollen, fügen Sie die zweite IP-Adresse der Files Advanced Dienstgruppe als Ressource hinzu und legen Sie sie als Abhängigkeit für den Netzwerknamen fest.*

Dienstgruppe online schalten und Konfigurationswerkzeug verwenden

1. Klicken Sie mit der rechten Maustaste auf die Files Advanced Dienstgruppe und wählen Sie **Diese Anwendung oder Dienstgruppe online schalten**.

2. Starten Sie das Konfigurationswerkzeug. Bei einer Neuinstallation befindet sich dies normalerweise unter **`C:\Program Files (x86)\Acronis\Access\Configuration Utility`**
3. Konfigurieren Sie den Files Advanced Gateway Server-Dienst, um an allen IP-Adressen nach der Files Advanced Dienstgruppe abzuhören.

4. Konfigurieren Sie den Files Advanced Server-Dienst, um an allen IP-Adressen nach der Files Advanced Dienstgruppe abzuhören.

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

5. Konfigurieren Sie das Files Advanced Datei-Repository, um localhost abzuhören, und ändern Sie den Dateispeicherpfad in ein Verzeichnis auf dem freigegebenen Laufwerk. Beide Knoten sollten den gleichen Pfad haben.

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

Installation und Konfiguration auf dem zweiten Knoten

1. Deaktivieren Sie alle vorhandenen Virenschutzprogramme, da sie unter Umständen den Installationsvorgang unterbrechen und somit eine fehlerhafte Installation verursachen können.
2. Installieren Sie Files Advanced auf dem zweiten Knoten, verwenden Sie jedoch diesmal den Standardspeicherort für **Postgres Data** sowie dasselbe postgres-Benutzerkennwort wie für den ersten Knoten.
3. Schließen Sie die Installation ab.
4. Konfigurieren Sie die Gateway Server-Datenbank, sodass sie sich auf einem freigegebenen Laufwerk befindet.
   a. Navigieren Sie zu **`C:\Program Files (x86)\Acronis\Access\Gateway Server\`**
   b. Suchen Sie die Datei **database.yml** und öffnen Sie sie mit einem Texteditor.
   c. Suchen Sie nach folgender Zeile: **`database_path: './database/'`** und ersetzen Sie **./database/** durch den gewünschten Pfad (z.B. **`database_path: 'S:/access_cluster/database/'`**).

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

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

   Hinweis: *Der Pfad sollte mit dem Pfad auf dem ersten Knoten übereinstimmen.*

5. Verschieben Sie die Files Advanced Dienstgruppe in den zweiten Knoten. Klicken Sie dazu mit der rechten Maustaste auf die Dienstgruppe und klicken Sie auf **In den zweiten Knoten verschieben**.
6. Starten Sie das Konfigurationswerkzeug. Bei einer Neuinstallation befindet sich dies normalerweise unter **`C:\Program Files (x86)\Acronis\Access\Configuration Utility`**
7. Konfigurieren Sie den Files Advanced Gateway Server-Dienst, um an allen IP-Adressen nach der Files Advanced Dienstgruppe abzuhören.

8. Konfigurieren Sie den Files Advanced Server-Dienst, um an allen IP-Adressen nach der Files Advanced Dienstgruppe abzuhören.

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

9. Konfigurieren Sie das Files Advanced Datei-Repository, um localhost abzuhören, und ändern Sie den Dateispeicherpfad in ein Verzeichnis auf dem freigegebenen Laufwerk. Beide Knoten sollten den gleichen Pfad haben.

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

12.2.19.2 Files Advanced auf einem Microsoft Windows 2012 (R2)-Failover-Cluster installieren

Files Advanced installieren

Sie müssen als Domänenadministrator angemeldet sein, um Files Advanced installieren zu können.

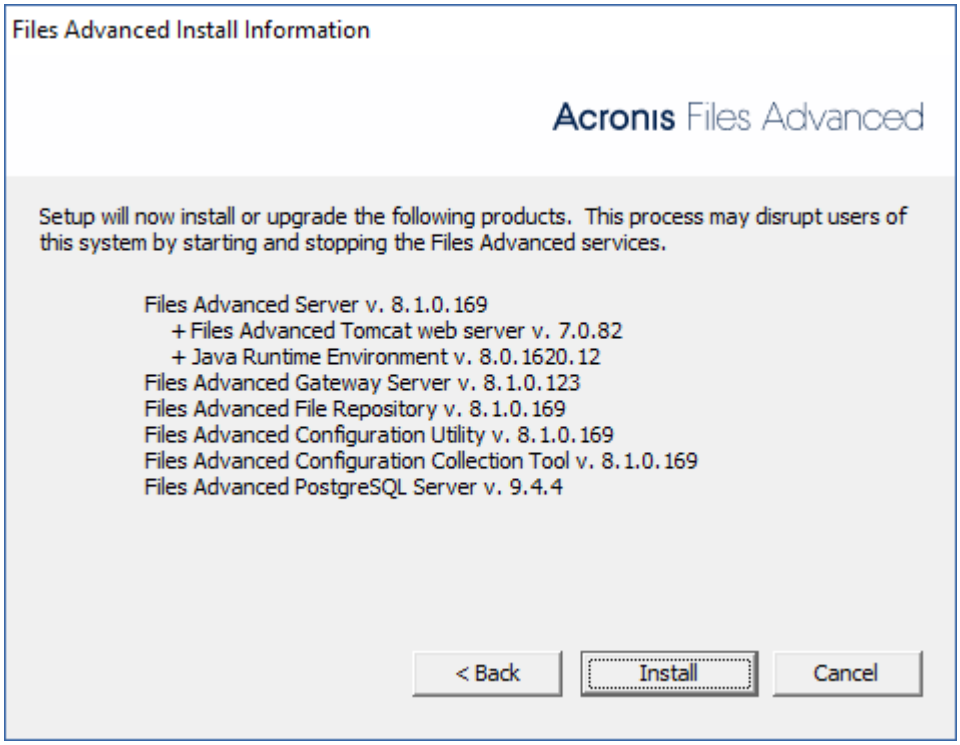
1. Laden Sie das Installationsprogramm für Files Advanced herunter.
2. Deaktivieren Sie alle vorhandenen Virenschutzprogramme, da sie unter Umständen den Installationsvorgang unterbrechen und somit eine fehlerhafte Installation verursachen können.
3. Doppelklicken Sie auf die ausführbare Installationsdatei.

4. Drücken Sie **Weiter**, um zu beginnen.

   Lesen und akzeptieren Sie die Lizenzvereinbarung.
5. Drücken Sie **Installieren**.

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

6. Verwenden Sie den Standardpfad oder wählen Sie einen neuen aus dem Hauptordner von Files Advanced und drücken Sie OK.



7. Legen Sie ein Kennwort für den Benutzer 'Postgres' fest, und notieren Sie es. Sie benötigen dieses Kennwort für Backup- und Wiederherstellungsaktionen der Datenbank.
8. Wählen Sie auf einem freigegebenen Laufwerk einen Speicherort für den Ordner **Postgres Data** und drücken Sie **Weiter**.

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

Wenn der Installationsvorgang für Files Advanced abgeschlossen ist, drücken Sie **Beenden**.

Rolle erstellen

1. Öffnen Sie die **Failover-Clusterverwaltung** und klicken Sie mit der rechten Maustaste auf **Rollen**.
2. Wählen Sie **Leere Rolle erstellen**. Geben Sie der Rolle einen geeigneten Namen (z.B. Files Advanced, AAS Cluster).

Konfigurationen auf dem aktiven Knoten

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

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

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

Alle erforderlichen Dienste der Files Advanced Rolle hinzufügen

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

1. Klicken Sie mit der rechten Maustaste auf die Files Advanced Rolle und wählen Sie **Ressource hinzufügen**.
2. Wählen Sie **Allgemeiner Dienst** aus.
3. Wählen Sie den geeigneten Dienst aus und drücken Sie **Weiter**.
4. Drücken Sie im Bestätigungsfenster **Weiter**.
5. Drücken Sie im Zusammenfassungsfenster **Fertig stellen**.

Zugriffspunkt festlegen

1. Klicken Sie mit der rechten Maustaste auf die Files Advanced Rolle und wählen Sie **Ressource hinzufügen**.
2. Wählen Sie **Clientzugriffspunkt** aus.
3. Geben Sie einen Namen für diesen Zugriffspunkt ein.
4. Wählen Sie ein Netzwerk.
5. Geben Sie die IP-Adresse ein und drücken Sie **Weiter**.
6. Drücken Sie im Bestätigungsfenster **Weiter**.
7. Drücken Sie im Zusammenfassungsfenster **Fertig stellen**.

Freigegebenes Laufwerk hinzufügen

1. Klicken Sie mit der rechten Maustaste auf die Files Advanced Rolle und wählen Sie **Speicher hinzufügen**.
2. Wählen Sie das gewünschte freigegebene Laufwerk aus.

Abhängigkeiten konfigurieren

1. Wählen Sie die Files Advanced Rolle aus und klicken Sie auf die Registerkarte **Ressourcen**.

Führen Sie für PostgreSQL und das Files Advanced Datei-Repository-Dienste Folgendes durch:

1. Klicken Sie mit der rechten Maustaste auf den entsprechenden Dienst und wählen Sie **Eigenschaften**.
2. Klicken Sie auf die Registerkarte **Abhängigkeiten**.
3. Klicken Sie auf **Ressource** und wählen Sie das freigegebene Laufwerk aus, das Sie hinzugefügt haben.

4. Drücken Sie **Anwenden** und schließen Sie das Fenster.

Führen Sie für den Files Advanced Gateway Server-Dienst Folgendes durch:

1. Klicken Sie mit der rechten Maustaste auf den entsprechenden Dienst und wählen Sie **Eigenschaften**.
2. Klicken Sie auf die Registerkarte **Abhängigkeiten**.
3. Klicken Sie auf **Ressource** und wählen Sie das freigegebene Laufwerk aus, das Sie hinzugefügt haben, sowie den **Netzwerknamen** (der zugleich der Name des Clientzugriffspunkts ist).

4. Drücken Sie **Anwenden** und schließen Sie das Fenster.

Führen Sie für den Files Advanced Tomcat-Dienst Folgendes durch:

1. Klicken Sie mit der rechten Maustaste auf den entsprechenden Dienst und wählen Sie **Eigenschaften**.
2. Klicken Sie auf die Registerkarte **Abhängigkeiten**.
3. Klicken Sie auf **Ressource** und wählen Sie die PostgreSQL und Files Advanced Gateway Server-Dienste als Abhängigkeiten aus. Drücken Sie **Anwenden** und schließen Sie das Fenster.

   Hinweis: *Wenn die Gateway und Access Server unter verschiedenen IP-Adressen ausgeführt werden sollen, fügen Sie die zweite IP-Adresse der Files Advanced Rolle als Ressource hinzu und legen Sie sie als Abhängigkeit für den Netzwerknamen fest.*

Rolle starten und Konfigurationswerkzeug verwenden

1. Klicken Sie mit der rechten Maustaste auf die Files Advanced Rolle und drücken Sie **Rolle starten**.
2. Starten Sie das Konfigurationswerkzeug. Bei einer Neuinstallation befindet sich dies normalerweise unter **`C:\Program Files (x86)\Acronis\Access\Configuration Utility`**
3. Konfigurieren Sie den Files Advanced Gateway Server-Dienst, um an allen IP-Adressen nach der Files Advanced Dienstgruppe abzuhören.

4. Konfigurieren Sie den Files Advanced Server-Dienst, um an allen IP-Adressen nach der Files Advanced Dienstgruppe abzuhören.

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

5. Konfigurieren Sie das Files Advanced Datei-Repository, um localhost abzuhören, und ändern Sie den Dateispeicherpfad in ein Verzeichnis auf dem freigegebenen Laufwerk. Beide Knoten sollten den gleichen Pfad haben.

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

Installation und Konfiguration auf dem zweiten Knoten

1. Deaktivieren Sie alle vorhandenen Virenschutzprogramme, da sie unter Umständen den Installationsvorgang unterbrechen und somit eine fehlerhafte Installation verursachen können.
2. Installieren Sie Files Advanced auf dem zweiten Knoten, verwenden Sie jedoch diesmal den Standardspeicherort für **Postgres Data** sowie dasselbe postgres-Benutzerkennwort wie für den ersten Knoten.
3. Schließen Sie die Installation ab.
4. Konfigurieren Sie die Gateway Server-Datenbank, sodass sie sich auf einem freigegebenen Laufwerk befindet.
   a. Navigieren Sie zu **`C:\Program Files (x86)\Acronis\Access\Gateway Server\`**
   b. Suchen Sie die Datei **database.yml** und öffnen Sie sie mit einem Texteditor.
   c. Suchen Sie nach folgender Zeile: **`database_path: './database/'`** und ersetzen Sie **./database/** durch den gewünschten Pfad (z.B. **`database_path: 'S:/access_cluster/database/'`**).

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

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

   Hinweis: *Der Pfad sollte mit dem Pfad auf dem ersten Knoten übereinstimmen.*

Führen Sie für PostgreSQL Folgendes aus:

1. Öffnen Sie den **Failovercluster-Manager**.
2. Suchen und wählen Sie die Ressource PostgreSQL Allgemeiner Dienst aus.
3. Klicken Sie mit der rechten Maustaste darauf und wählen Sie **Eigenschaften**.
4. Klicken Sie auf die Registerkarte **Registrierungsreplikation**.
5. Drücken Sie **Hinzufügen** und geben Sie Folgendes ein: **`SYSTEM\CurrentControlSet\Services\AcronisAccessPostgreSQL\`**(Für ältere Versionen von Files Advanced kann der Service unterschiedlich sein, z. B. **postgresql-x64-9.2**)
6. Verschieben Sie die Files Advanced Rolle in den zweiten Knoten.

Verwenden des Konfigurationswerkzeugs auf dem zweiten Knoten

1. Starten Sie das Konfigurationswerkzeug. Bei einer Neuinstallation befindet sich dies normalerweise unter **`C:\Program Files (x86)\Acronis\Access\Configuration Utility`**
2. Konfigurieren Sie den Files Advanced Gateway Server-Dienst, um an allen IP-Adressen nach der Files Advanced Dienstgruppe abzuhören.

3. Konfigurieren Sie den Files Advanced Server-Dienst, um an allen IP-Adressen nach der Files Advanced Dienstgruppe abzuhören.

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

4. Konfigurieren Sie das Files Advanced Datei-Repository, um localhost abzuhören, und ändern Sie den Dateispeicherpfad in ein Verzeichnis auf dem freigegebenen Laufwerk. Beide Knoten sollten den gleichen Pfad haben.

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

12.3 Für den mobilen Client

Themen

12.3.1 Konfigurationsfunktionen für verwaltete Apps von iOS verwenden

Der Files Advanced Mobile unterstützt die Konfigurationsfunktionen für verwaltete Apps von iOS 7. Wenn die unten aufgeführten Voraussetzungen erfüllt sind, können Sie Ihrer MDM-Konfiguration bestimmte Schlüssel hinzufügen, die sich auf den Files Advanced Mobile auswirken.

- Ihr Gerät muss von einem MDM-Server verwaltet werden.
- Die Binärdatei der Applikation Files Advanced muss vom MDM-Server auf dem Gerät installiert werden.
- Der MDM-Server muss die Einstellung **ApplicationConfiguration** und **ManagedApplicationFeedback**-Befehle unterstützen.

Der Einsatz der folgenden Schlüssel wird unterstützt:

- **enrollmentServer**: Der Wert dieses Schlüssels muss auf die DNS-Adresse des Files Advanced-Servers eingestellt werden, bei dem sich der Benutzer registrieren muss.
- **enrollmentPIN** – Dieser Schlüssel ist optional. Wenn der Files Advanced Server für die Client-Registrierung eine PIN-Nummer verlangt, können Sie mit diesem Wert das Feld für die PIN-Nummer auf dem Files Advanced-Registrierungsformular automatisch ausfüllen lassen. Diese PIN-Anforderung wird auf der Seite **Einstellungen** (S. 107) der **Files Advanced-**Webkonsole konfiguriert.
- **userName**: Dieser Schlüssel ist optional. Der Wert dieses Schlüssels wird in das Feld 'Benutzername' im Files Advanced-Registrierungsformular eingefügt. Sie können eine Variable zum automatischen Vervollständigen dieses Werts mit dem Benutzernamen des betreffenden Benutzers verwenden.

Erstellen einer plist-Datei

plist ist ein Format zum Speichern von Anwendungsdaten. Ursprünglich von Apple zur Verwendung in iPhone-Geräten definiert, wurde es später auch an anderen Anwendungen verwendet. Da Plists eigentlich XML-Dateien sind, kann ein einfacher Text-Editor zur Erstellung und Bearbeitung verwendet werden.

Erstellen der Plist-Datei

1. Öffnen Sie den gewünschten Texteditor.
2. Geben Sie folgendes ein:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
   <dict>
         Geben Sie hier die gewünschten Schlüssel ein
   </dict>
</plist>
```

Beispiel:

```
<dict>
   <key>enrollmentServer</key>
   <string>server.example.com</string>
   <key>userName</key>
   <string>username</string>
      <key>enrollmentPIN</key>
      <string>11Y9KL</string>
</dict>
```

3. Speichern Sie die Datei als **plist.xml**.

Hochladen der plist-Datei in MobileIron

1. Öffnen Sie Ihr Administrationsportal.
2. Gehen Sie zu **Richtlinien & Konfigurationen** > **Konfigurationen** > **Neu hinzufügen** > **iOS und OSX** > **Konfiguration für verwaltete Apps** und laden Sie die Plist-Datei hoch.

Hochladen der plist-Datei in Microsoft Intune

Hinweis: *Eine umfassendere Anleitung zu diesem Thema finden Sie hier: Microsoft Intune-Dokumentation.*

1. Wählen Sie in der Verwaltungskonsole von Microsoft Intune **Richtlinie** > **Übersicht** > **Richtlinie hinzufügen**.
2. Erweitern Sie in der Liste der Richtlinien den Eintrag **iOS**, wählen Sie **Konfiguration mobiler Apps**, und wählen Sie dann **Richtlinie erstellen**.
   - Geben Sie auf der Seite **Richtlinie erstellen** im Abschnitt 'Allgemein' einen Namen und optional eine Beschreibung der Richtlinie zur Konfiguration mobiler Apps ein.
   - Geben Sie auf der Seite im Abschnitt mit der Richtlinie zur Konfiguration mobiler Apps im Feld eine XML-Eigenschaftenliste mit den App-Konfigurationseinstellungen ein bzw. kopieren Sie diese und fügen Sie sie ein.
3. Klicken Sie auf 'Überprüfen', um sicherzustellen, dass die von Ihnen eingegebene XML-Liste ein gültiges Eigenschaftenlistenformat aufweist.

4. Klicken Sie abschließend auf **Richtlinie speichern**.

12.3.2 MobileIron AppConnect-Support

Themen

12.3.2.1 Einführung

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

Zu den Komponenten von Files Advanced mit MobileIron AppConnect gehören:

- **MobileIron Virtual Smartphone-Plattform (VSP)** – Eine serverbasierte Konsole, mit der das Unternehmen den Client-Zugriff auf für AppConnect aktivierte Apps ermöglichen, diese Apps automatisch konfigurieren, Richtlinien für die App-Funktionen erstellen sowie den Zugriff auf für AppConnect aktivierte Apps auf bestimmten Geräten widerrufen und die Apps auf diesen löschen kann.
- **MobileIron Sentry** – Dieser Dienst ermöglicht den Netzwerkzugriff von AppConnect-fähigen Apps, die mit Applikations-Servern vor Ort kommunizieren müssen, z.B. einem Files Advanced Gateway Server.
- **MobileIron Mobile@Work App** – Diese App handelt die Authentifizierung und Konfiguration für AppConnect aktivierter Apps aus. Sie muss auf dem mobilen Gerät installiert werden, um für AppConnect aktivierte Apps konfigurieren und verwalten zu können.
- **Files Advanced-iOS-App** – Die Standardversion von Files Advanced für iOS (Version 5.0 oder höher), die im Apple App Store erhältlich ist, kann von AppConnect konfiguriert und verwaltet werden und über AppTunnel mit Files Advanced Gateway Servern kommunizieren.
- **Files Advanced Android-App** – Eine spezielle Version von MobileIron der App ist erforderlich. Sie kann unter http://support.grouplogic.com/?page_id=4566 heruntergeladen werden. Diese Version der App muss zu Ihrem Speicher von **Apps@Work** hinzugefügt werden.
- **Files Advanced Server** – Die Standardversion von Files Advanced Server (Version 5.0 oder später) ist vollständig kompatibel mit Mobile Clients, die von AppConnect verwaltet werden.

12.3.2.2 Eine Testversion von Files Advanced für AppConnect testen

Das Testen von Files Advanced mit AppConnect entspricht weitgehend dem Test einer normalen Files Advanced-Testversion.

1. Eine Testversion der serverseitigen Software können Sie über die Seite 'Testversion' anfordern. Sobald die Anfrage eingesendet wurde, erhalten Sie eine E-Mail mit Links zum Herunterladen des Installationsprogramms für die Testversion von Files Advanced Server sowie der Schnellstartanleitung, die Sie bei der Ersteinrichtung unterstützt.
2. Die Files Advanced-iOS-Client-App kann kostenlos aus dem Apple App Store http://www.grouplogic.com/web/meappstore heruntergeladen werden.
3. Bei der Android-App Files Advanced handelt es sich um ein kostenloses Download von einer unserer Support-Websites http://support.grouplogic.com/?page_id=4566.
4. Die Mobile-Apps von Files Advanced müssen AppConnect-Konfigurationen und -Richtlinien aufweisen, die auf Ihrer MobileIron VSP-Plattform (Virtual Smartphone Platform) erstellt wurden, bevor sie automatisch für den Zugriff auf Ihre Files Advanced Gateway Server konfiguriert werden können.
5. Auf den Mobilgeräten muss darüber hinaus die App MobileIron Mobile@Work installiert werden, bevor für AppConnect konfigurierte Apps aktiviert und bevor die Files Advanced App installiert werden kann. Mobile@Work ist als kostenloser Download im Apple App Store sowie im Google Play Store erhältlich.
6. Wenn Sie bereit sind, Files Advanced-Mobile-Clients mit AppConnect zu aktivieren, fahren Sie mit den folgenden Abschnitten dieses Dokuments fort.

12.3.2.3 Den Files Advanced Android-Client mit MobileIron integrieren

1. Damit Files Advanced Android mit der Geräteverwaltung von MobileIron arbeiten kann, müssen Sie eine besondere Version von http://www.grouplogic.com/web/aalatest unter **`Files Advanced Client Installers`** herunterladen.

   Note: *Stellen Sie sicher, dass die Version, die Sie herunterladen, mit Ihrer Version von* ***Secure Apps Manager*** *von MobileIron kompatibel ist.*

2. Melden Sie sich an der MobileIron Core-Konsole an.
3. Öffnen Sie die Registerkarte **Apps** und wählen Sie **App-Katalog** aus.
4. Drücken Sie **Hinzufügen+** und wählen Sie **In-House** aus.
5. Drücken Sie **Durchsuchen**, navigieren Sie zu **`Files Advanced Android .apk`** und wählen Sie es aus.
6. Klicken Sie auf **Weiter**. Geben Sie eine Beschreibung für die App ein und drücken Sie **Weiter**.
7. Stellen Sie bei **App Store** sicher, dass **Apps@Work Catalog** -> **Feature this App in the Apps@Work catalog** aktiviert ist und drücken Sie **Weiter**.
8. Wählen Sie aus, ob die App obligatorisch für alle Benutzer installiert werden soll und drücken Sie **Fertig stellen**.

12.3.2.4 Die Files Advanced iOS-App mit MobileIron integrieren

Hinweis: *Dies ist nur erforderlich, wenn die App in Ihrem Apps@Work-Speicher gespeichert werden soll und die Auswahl der Apps in der MobileIron-Konsole möglich sein soll, anstatt die Bundle-ID der App zu schreiben.*

1. Melden Sie sich an der MobileIron Core-Konsole an.
2. Öffnen Sie die Registerkarte **Apps** und wählen Sie **App-Katalog** aus.
3. Drücken Sie **Hinzufügen+** und wählen Sie **iTunes** aus.

4. Geben Sie **Files Advanced** im Suchenfeld ein, drücken Sie **Durchsuchen** und wählen Sie die aktuelle Version für Files Advanced aus.
5. Klicken Sie auf **Weiter**. Geben Sie eine Beschreibung für die App ein und drücken Sie **Weiter**.
6. Stellen Sie bei **App Store** sicher, dass **Apps@Work Catalog** -> **Feature this App in the Apps@Work catalog** aktiviert ist und drücken Sie **Weiter**.

   Hinweis: *Möglicherweise müssen Sie auch* ***Kostenlos*** *für die App angeben.*

7. Wählen Sie für **App-Konfiguration** alle zusätzlichen Konfigurationen aus, die Sie durchführen möchten, und drücken Sie **Fertig stellen**.

12.3.2.5 Eine AppConnect-Konfiguration und -Richtlinie für Files Advanced auf der MobileIron-VSP erstellen

Sie können erst dann mit dem Einbinden von Files Advanced-Benutzern (S. 80) beginnen, wenn Sie in MobileIron VSP zwei Elemente erstellt haben:

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

Themen

Eine Konfiguration für die Mobile-App erstellen

1. Melden Sie sich an der MobileIron VSP-Webkonsole an und wählen Sie die Registerkarte **Richtlinien und Konfigurationen** aus.
2. Klicken Sie auf die Registerkarte **Konfigurationen** und drücken Sie 'Neu hinzufügen'.
3. Navigieren Sie im Dropdownmenü zu **AppConnect** Wählen Sie dann **App-Konfiguration** aus.

4. Geben Sie in der neuen **App-Konfiguration für AppConnect** die folgenden Informationen ein:

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

Beschreibung – Diese Beschreibung können Sie beliebig wählen.

Applikation – Wählen Sie die Files Advanced App aus der Liste. Wenn Sie iOS- und Android-Geräte verwenden, stellen Sie sicher, dass Sie die richtige App für die gewünschten Clients verwenden.

AppTunnel – Die **AppTunnel**-Einstellungen sind optional und nur erforderlich, wenn Sie **AppTunnel** für den Zugriff auf Ihre Files Advanced Server verwenden.

- **Sentry** – Wählen Sie aus, welche MobileIron Sentry-Server Sie verwenden möchten.
- **Dienst** – Mit dieser Einstellung wird der Dienst ausgewählt, mit dem sich die App in dieser Konfiguration über den **AppTunnel** verbinden kann. Sie können **<BELIEBIGE>** auswählen, damit sich die App mit allen internen Diensten verbinden kann, oder einen dedizierten

Dienst für Files Advanced auswählen. Die Option für einen bestimmten Dienst setzt voraus, dass Sie einen benutzerdefinierten **Dienst** für Ihren Files Advanced Server hinzugefügt haben.

Hinweis: <TCP_ANY> *entspricht nicht* ***<BELIEBIGE>*** *und funktioniert nicht!*

Hinweis: *Um einen benutzerdefinierten Dienst hinzuzufügen navigieren Sie zu* ***Dienste*** *->* ***Sentry*** *und drücken* ***Bearbeiten*** *für die gewünschte* ***Sentry****-Option. Drücken Sie im Abschnitt* ***AppTunnelConfiguration*** *auf die Schaltfläche* ***+*** *unter* ***Dienste****. Geben Sie einen* ***Dienstnamen*** *ein, wählen Sie eine Authentifizierungsmethode aus, stellen Sie sicher, dass das Kontrollkästchen* ***TLS aktiviert*** *aktiviert ist und geben Sie für* ***Serverliste*** *die DNS-Adresse(n) für Ihren Files Advanced Server und/oder Gateway Server ein.*

- **URL-Platzhalter** – Die DNS-Adresse Ihrer Files Advanced Server oder Ihrer Domäne als Ganzes. Beispiel: ***.domain.com**
- **Port** – Files Advanced Dienste verwenden standardmäßig die Ports 443 und 3000. Geben Sie den gewünschten Port ein, je nachdem, für welchen Dienst sich die Benutzer registrieren.

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

- **enrollmentServerName** – Dieses Schlüsselfeld muss angegeben werden. Der Wert dieses Schlüssels muss auf die DNS-Adresse des Files Advanced Servers eingestellt werden, bei dem sich der Benutzer registrieren muss.
- **enrollmentPIN** – Dieser Schlüssel ist optional. Wenn der Files Advanced Server für die Client-Registrierung eine PIN-Nummer verlangt, können Sie mit diesem Wert das Feld für die PIN-Nummer auf dem Files Advanced-Registrierungsformular automatisch ausfüllen lassen. Normalerweise ist die PIN-Anforderung für den Files Advanced Server deaktiviert, da statt der einmalig zu verwendenden PIN-Nummer AppConnect als zweiter Faktor für die Authentifizierung verwendet werden kann, bevor ein Benutzer Zugriff erhält. Diese PIN-Anforderung wird auf der Seite **Einstellungen** (S. 107) der **Files Advanced-**Webkonsole konfiguriert.
- **enrollmentAutoSubmit** – Dieser Schlüssel ist optional. Dieser Schlüssel bewirkt, dass das Registrierungsformular automatisch gesendet wird, sodass der Benutzer nicht auf die Schaltfläche 'Jetzt registrieren' tippen muss, um fortzufahren. Wenn Sie diesen Schlüssel aktivieren möchten, legen Sie folgenden Wert fest: **Yes**
- **requirePIN** – Dieser Schlüssel ist optional. Wenn Sie eine PIN an mobile Files Advanced-Benutzer verteilen, die diese manuell in das Files Advanced-Registrierungsformular eingeben müssen, können Sie festlegen, dass das PIN-Feld sofort im Formular angezeigt wird. Dazu müssen Sie den Wert dieses Schlüssels auf **Ja** festlegen.
- **enrollmentUserName** – Dieser Schlüssel ist optional. Der Wert dieses Schlüssels wird in das Feld 'Benutzername' im Files Advanced-Registrierungsformular eingefügt. Sie können den **$USERID$**-Platzhalter von MobileIron verwenden, der automatisch das Feld mit dem Benutzernamen vervollständigt, den der Benutzer beim Einrichten der Mobile@Work-App angegeben hat.
- **enrollmentPassword** – Dieser Schlüssel ist optional. Der Wert dieses Schlüssels wird in das Feld 'Kennwort' im Files Advanced-Registrierungsformular eingefügt. Sie können den **$PASSWORD$**-Platzhalter von MobileIron verwenden, der automatisch das Feld mit dem Kennwort vervollständigt, das der Benutzer beim Einrichten der Mobile@Work-App angegeben hat.

Eine Container-Richtlinie für die Files Advanced-App erstellen

1. Melden Sie sich an der MobileIron VSP-Webkonsole an und wählen Sie die Registerkarte **Richtlinien und Konfigurationen** aus.
2. Klicken Sie auf die Registerkarte **Konfigurationen** und drücken Sie 'Neu hinzufügen'.
3. Navigieren Sie im Dropdownmenü zu **AppConnect** und wählen Sie dann **Container-Richtlinie** aus.
4. Geben Sie in der neuen **Container-Richtlinie** die folgenden Informationen ein:

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

Beschreibung – Diese Beschreibung können Sie beliebig wählen.

Applikation – Wählen Sie die Files Advanced App aus der Liste. Wenn Sie iOS- und Android-Geräte verwenden, stellen Sie sicher, dass Sie die richtige App für die gewünschten Clients verwenden.

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

Kopieren/Einfügen in zulassen – Wählen Sie diese Option, wenn es Benutzern gestattet sein soll, Text aus Dokumenten, die in der Files Advanced-Mobile-App angezeigt werden, in andere Apps auf dem Gerät zu kopieren und einzufügen, die nicht von AppConnect verwaltet werden.

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

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

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

Zuordnen von Labels zur neuen Konfigurations- und Container-Richtlinie

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

12.3.2.6 Den Files Advanced-iOS-Client mit AppConnect aktivieren

Hinweis: *Diese Methode der Aktivierung der Files Advanced App gilt nur für die iOS-Version und ist nur erforderlich, wenn Sie die Files Advanced App nicht zu Ihrer Liste der Apps in der MobileIron VSP-Konsole hinzugefügt haben und die Benutzer nicht bereits Files Advanced verwenden.*

Wenn die App über die MobileIron-Konsole hinzugefügt wurden, können Benutzer sie über den Speicher ***Apps@Work*** *herunterladen. Je nach Einstellung wurde sie möglicherweise auch automatisch auf den Geräten installiert.*

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

Sicherstellen, das Mobile@Work installiert und konfiguriert wurde

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

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

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

Themen

Files Advanced wurde bereits auf dem Gerät installiert, wurde jedoch noch nicht bei einem Files Advanced-Server registriert

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

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

Files Advanced wurde bereits auf dem Gerät installiert und bereits bei einem Files Advanced-Server registriert

Dieses Szenario ähnelt dem vorherigen; der einzige Unterschied besteht darin, dass die AppConnect Files Advanced-Konfiguration nicht zur automatischen Registrierung der Mobile-App verwendet wird. Wenn die Mobile-App bereits bei einem Files Advanced Server registriert ist, wird die ursprüngliche Konfiguration beibehalten.

Damit Files Advanced von AppConnect verwaltet wird und der AppConnect-Passcode und die Container-Richtlinien als Berechtigungen verwendet werden, muss der Benutzer zuerst die Files Advanced App verwenden, zu **Einstellungen** -> **Partnerfunktionen** -> **MobileIron** wechseln und auf **AppConnect aktivieren** tippen. Nach einer Weile muss die App neu gestartet werden.

Wenn sich ein Benutzer bei einem anderen Files Advanced-Server registrieren soll, muss er Files Advanced deinstallieren und die App neu installieren. Erst danach ist eine Konfiguration über AppConnect möglich.

Files Advanced wurde noch nicht auf dem Gerät installiert

In diesem Szenario müssen Sie Files Advanced aus dem Apple App Store oder aus dem MobileIron Apps@Work-Speicher installieren.

Starten Sie Files Advanced nach der Installation.

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

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

12.3.2.7 Fortlaufende AppConnect-Verwaltung von Files Advanced Mobiles

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

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

12.3.2.8 Verwenden von AppConnect mit der eingeschränkten Kerberos-Delegierung

In diesem Artikel wird erklärt, wie die erforderlichen Systemkomponenten für die Verbindung der Files Advanced iOS Mobile-App mit dem Files Advanced Serverproxy über MobileIron AppTunnel mit der Authentifizierung über die eingeschränkte Kerberos-Delegierung konfiguriert werden.

Die Android- und Windows-Mobile Apps unterstützen diese Konfiguration nicht.

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

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

Vor Beginn

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

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

- Key Distribution Center (KDC) ist ein Netzwerkdienst, der Benutzern und Computern innerhalb einer Active Directory-Domäne Sitzungstickets und temporäre Sitzungsschlüssel zur Verfügung stellt.
- Nur der Gateway Server akzeptiert eine Kerberos-Authentifizierung. Der Files Advanced Server tut dies nicht.
  - Die Files Advanced-Mobile-App muss in der Clientverwaltung bei einem Gateway-Server registriert sein. Wenn der Client beim Files Advanced Server registriert ist, schlägt die Anmeldung fehl.
  - Mobile Clients, die die Kerberos-Authentifizierung verwenden, können die Authentifizierung mit Netzwerkfreigaben, Sync&Share-Ordnern und SharePoint-Websites durchführen.

Voraussetzungen

Die folgende Software muss installiert und konfiguriert sein:

- MobileIron VSP (in diesem Dokument wird auf Version 5.9 Bezug genommen)
- Für eine ordnungsgemäße Funktion von Kerberos müssen die Benutzerkonten auf dem VSP aus dem Active Directory stammen, das zur Unterstützung von Kerberos konfiguriert wird.
- MobileIron Sentry (in diesem Dokument wird auf Version 4.8 Bezug genommen)
- Files Advanced Server installiert (6.0.2 in diesem Dokument verwendet)
- Serverinteroperabilität
  - Die Uhrzeit auf den VSP-, Sentry-, Domain Controller- und Files Advanced-Servern muss synchronisiert sein (NTP empfohlen).
  - Domänennamenauflösung (DNS). Sentry fordert ein Ticket vom KDC mithilfe des DNS-Namen an, der für den Kontakt konfiguriert ist. Dieser Name muss mit dem Computernamen übereinstimmen, der für die Kerberos-Delegierung eingerichtet wurde; ansonsten lehnt KDC die Ausgabe eines Tickets ab.

- Der VSP muss in der Lage sein, auf Sentry zuzugreifen (standardmäßig über die Ports 9090 und 443 – weitere je nach Ihrer Konfiguration).
- Sentry muss in der Lage sein, auf das Active Directory und den Files Advanced Server zuzugreifen (über die Ports 88, 389, 636).
- Die Ports 88 (UDP und TCP) und 389 (TCP) zwischen Active Directory und Sentry (oder Port 636 (TCP), wenn Sie ein SSL-aktiviertes Active Directory verwenden) müssen für den Datenverkehr geöffnet sein. Port 88 wird zur Kommunikation mit dem Kerberos-Protokoll verwendet. Port 389 (oder 636) wird für das LDAP-Ping zwischen Sentry und KDC verwendet, um zu überprüfen, ob die KDC-IP mit der Active Directory-IP identisch ist.
- Bei Verwendung von Windows Server 2003 kann der KDC auf Anforderungen am Port 88 unter Verwendung von UDP anstatt von TCP warten. Sie können erzwingen, dass Kerberos TCP statt UDP verwendet, indem Sie im Registry-Editor die MaxPacketSize von 0 in 1 ändern. Weitere Informationen zur korrekten Vorgehensweise finden Sie im folgenden Microsoft KB-Artikel: http://support.microsoft.com/kb/244474 http://support.microsoft.com/kb/244474.

- Das iOS-Gerät muss in der Lage sein, eine Verbindung mit VSP und Sentry herzustellen.
- Auf VSP registriertes iOS -Gerät.
- Mobile@Work ist auf dem Gerät installiert und auf VSP registriert. Die MDM-Profile wurden während der Registrierung ordnungsgemäß installiert.

Themen

13 Konfigurieren eines AppConnect-Tunnels zwischen dem Files Advanced Mobile und dem Files Advanced Server durch Authentifizierung per Benutzername/Kennwort

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

- Eine neue lokale Zertifizierungsstelle (CA) erstellen
- Ein neues SCEP erstellen
- Sentry hinzufügen und konfigurieren
- Konfigurieren von Files Advanced auf der VSP

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

Themen

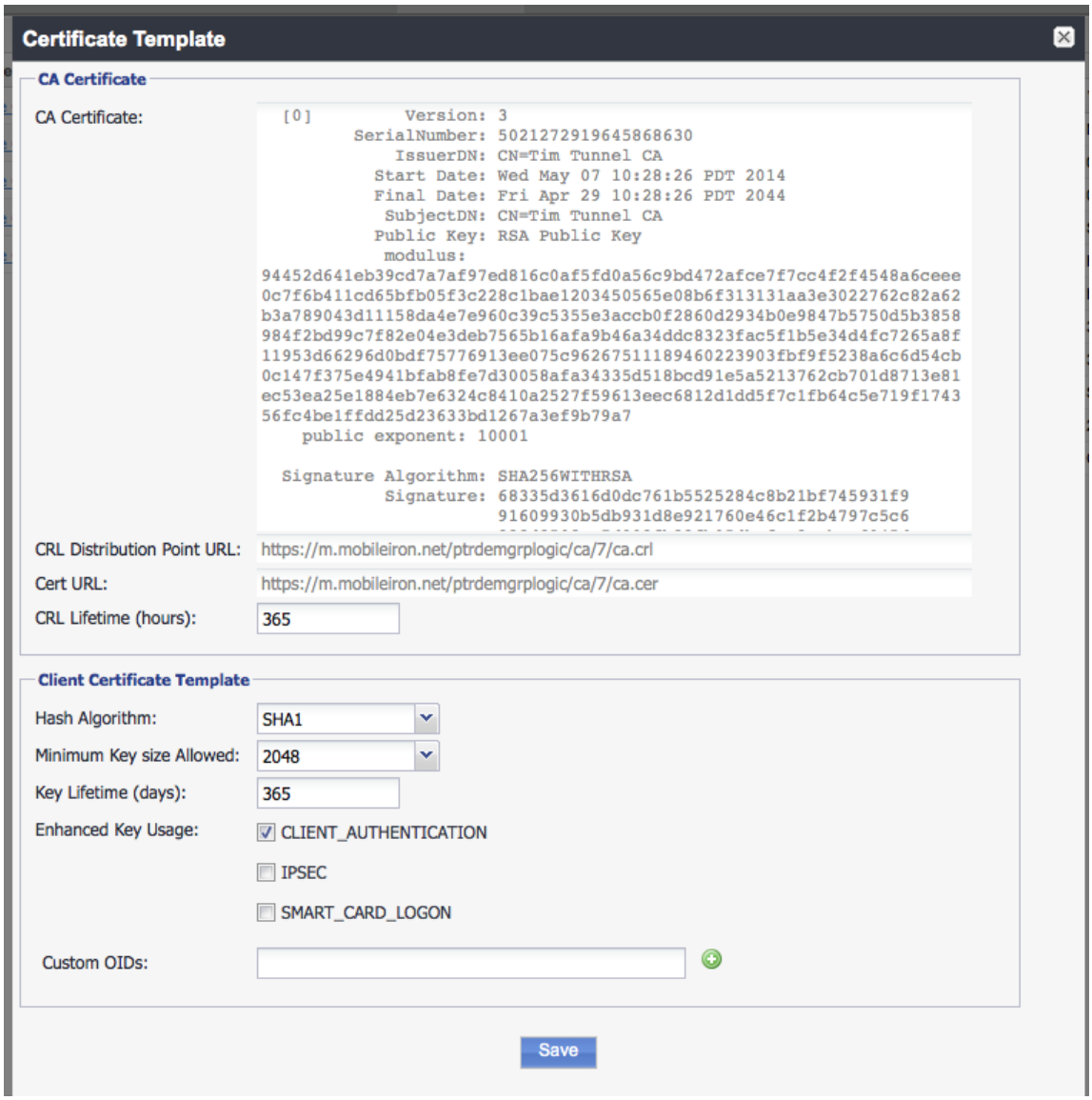
5.

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

- **Name der lokalen CA:** Geben Sie den gewünschten Namen ein.
- **Schlüssellänge**: Wählen Sie **2048**.

- **Ausstellername:** Geben Sie den gewünschten Namen ein; er muss jedoch mit **CN=** beginnen.

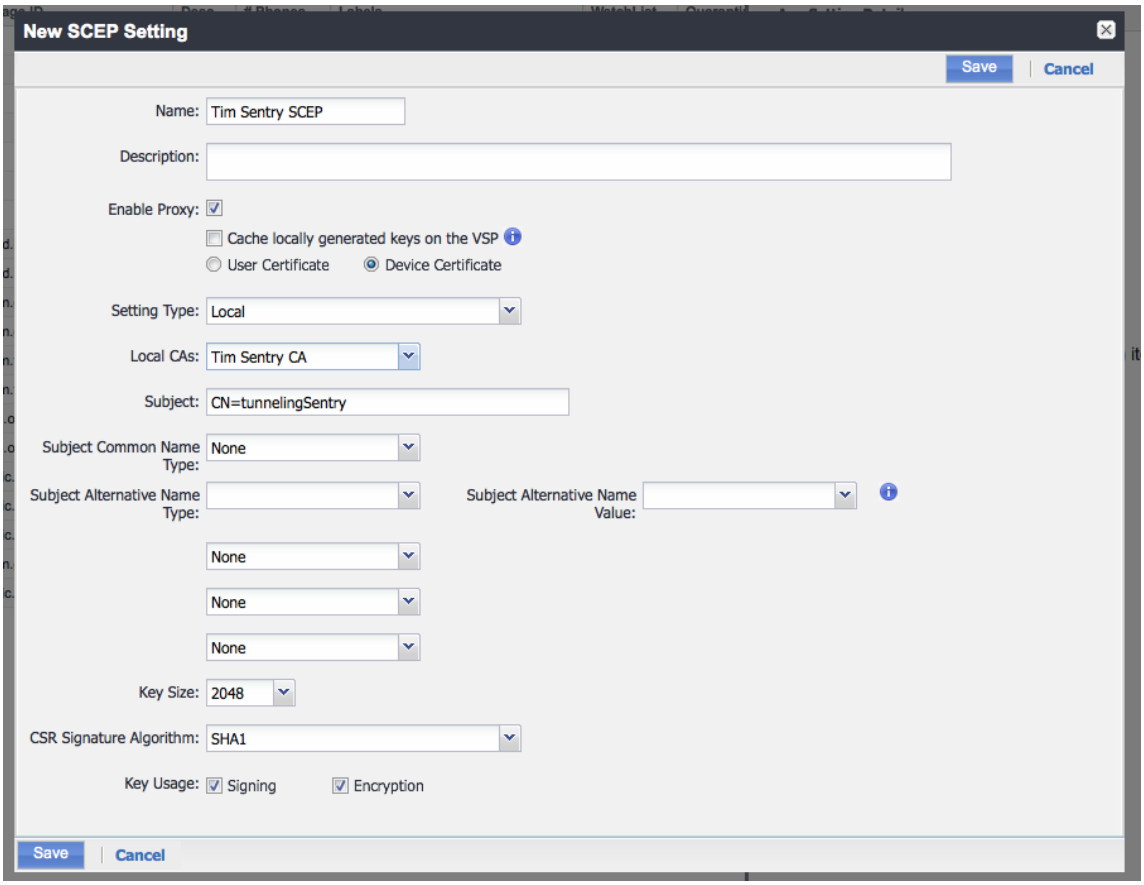
4. Klicken Sie auf **Erstellen**.



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

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

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

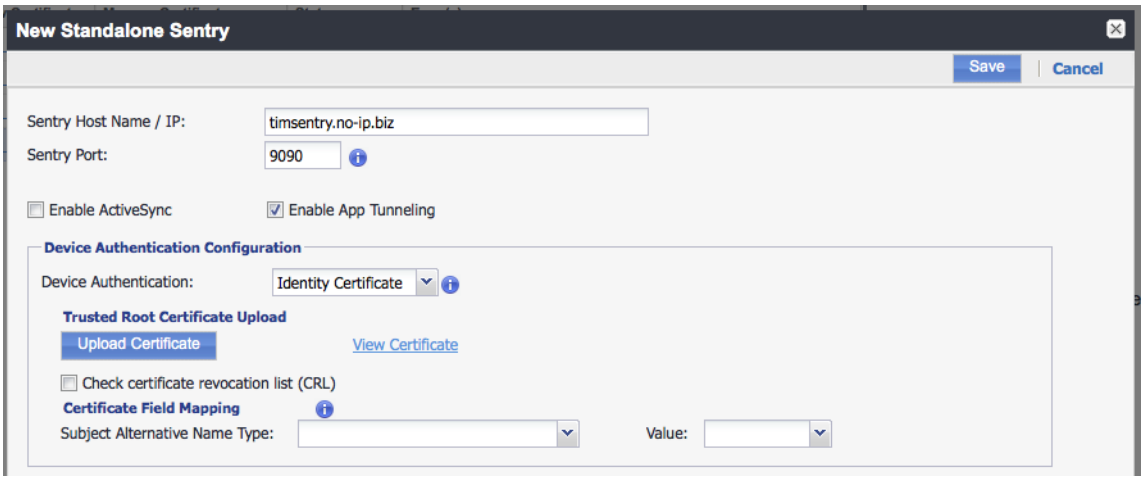


- **Name**: Geben Sie den gewünschten Namen ein.
- **Einstellungstyp**: Wählen Sie **Lokal**.
- **Lokale CA**: Name der unter "Eine neue lokale Zertifizierungsstelle (CA) erstellen" erstellte CA.
- **Betreff**: Geben Sie den gewünschten Namen ein (z. B. CN=tunneling); er muss jedoch mit **CN=** beginnen.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

4. Klicken Sie auf **Speichern**.

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

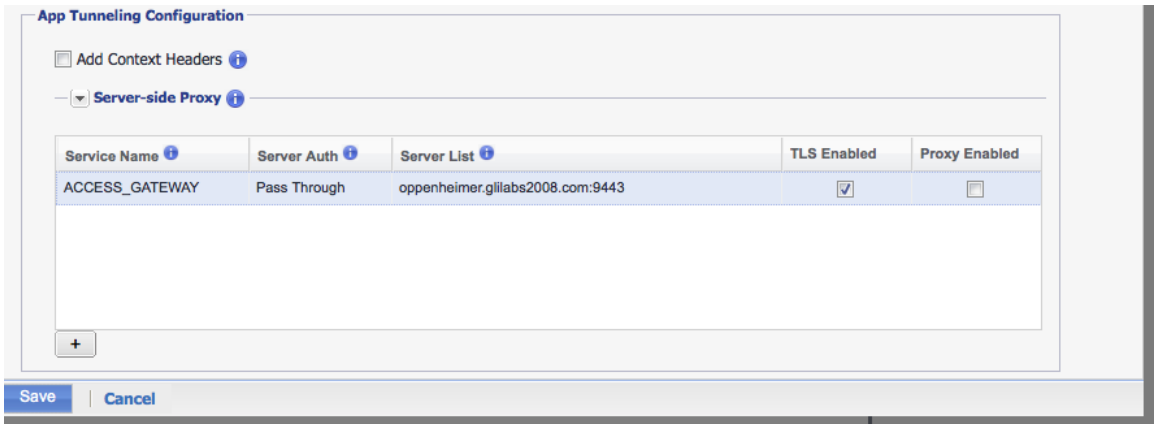
2. Drücken Sie auf **Neue hinzufügen** und wählen Sie **Standalone-Sentry**.



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

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

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



- **Dienst-Name**: Geben Sie den gewünschten Namen ein.
- **Server-Auth.**: Wählen Sie **Passthrough**. Dies wird zu einem späteren Zeitpunkt in dieser Anleitung geändert.

- **Serverliste**: Durch Semikolon getrennte Liste der Server. Für dieses Dokument verwenden wir einen einzelnen Server. Es handelt sich um die DNS-Adresse des Files Advanced Gateway Servers und um den Port, der abgehört wird.
- **TLS aktiviert**: Aktivieren Sie das Kontrollkästchen.

Klicken Sie auf **Speichern**.

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

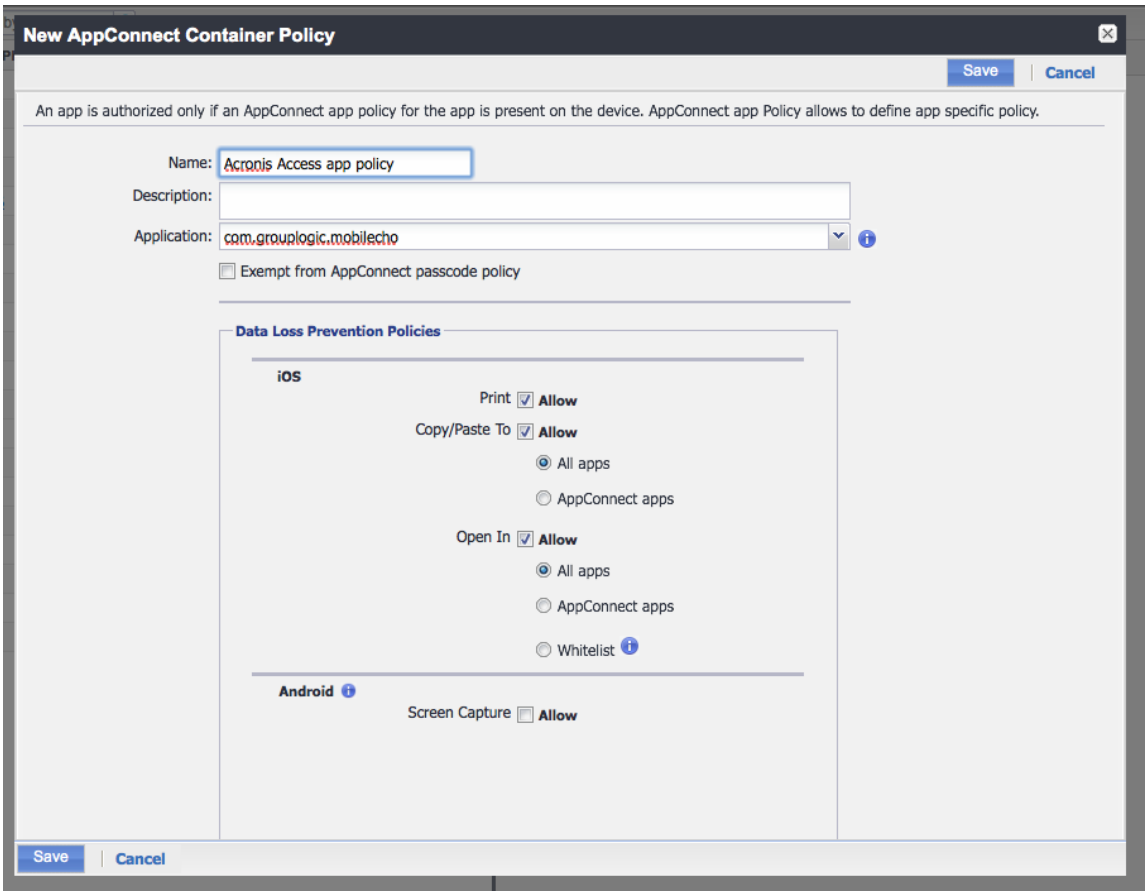
Konfigurieren von Files Advanced auf der VSP

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

Themen

6.

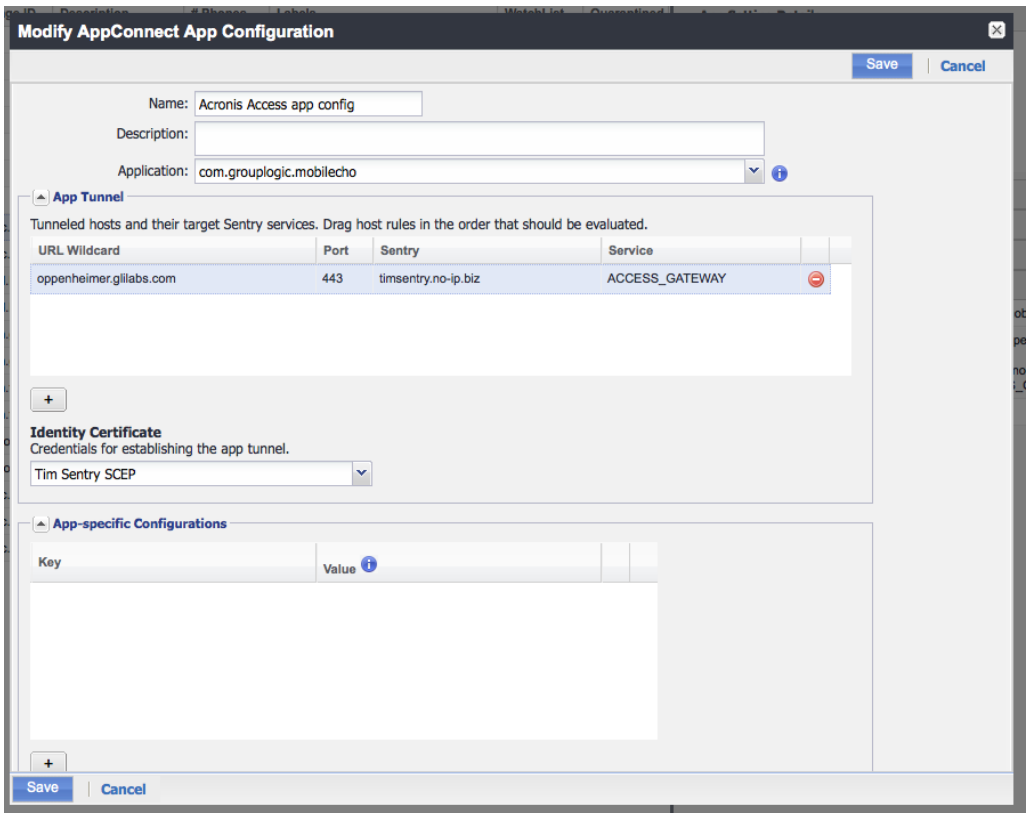
1. Wählen Sie noch innerhalb des Admin-Portals von MobileIron VSP **Richtlinien und Konfigurationen** und öffnen Sie **Konfigurationen**.
2. Klicken Sie auf **Neue hinzufügen**, wählen Sie **AppConnect** und **Container-Richtlinie**.



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

3. Klicken Sie auf **Speichern**.

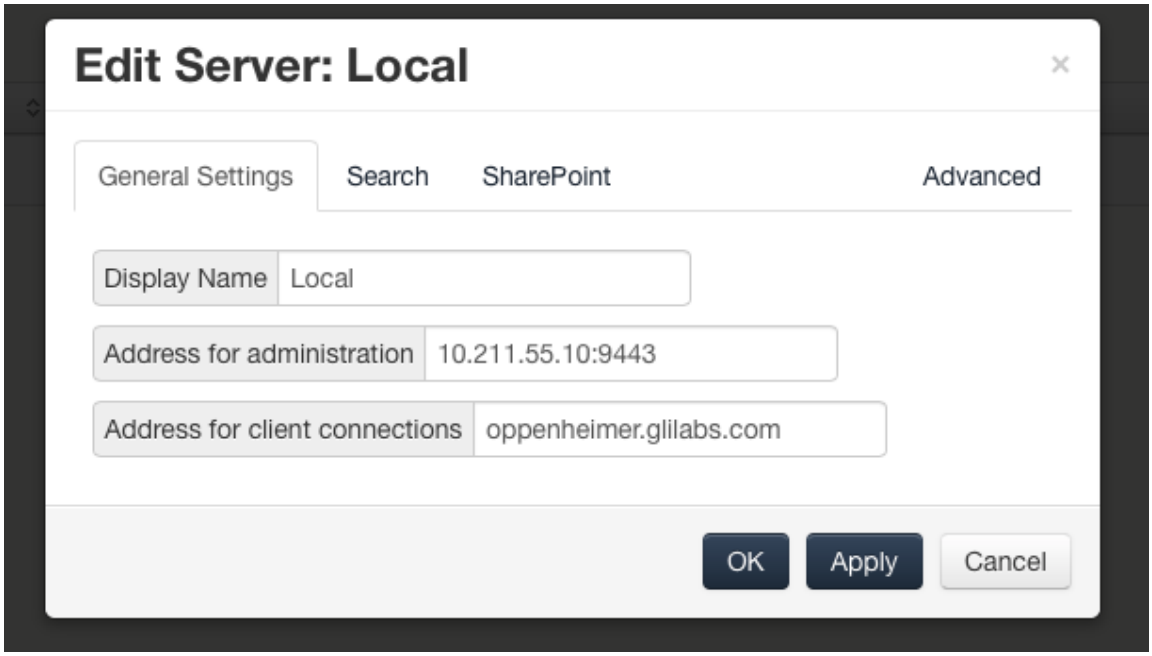
1. Wählen Sie noch innerhalb des Admin-Portals von MobileIron VSP **Richtlinien und Konfigurationen** und öffnen Sie **Konfigurationen**.
2. Drücken Sie auf **Neue hinzufügen**, wählen Sie **AppConnect** und **Konfiguration**.



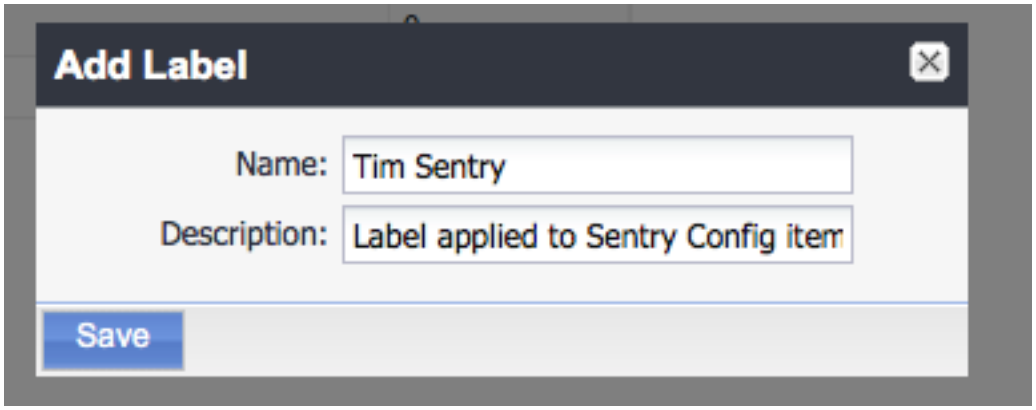
- **Name**: Geben Sie den gewünschten Namen ein.
- **Applikation**: Geben Sie com.grouplogic.mobilecho ein. Dies ist die Bundle-ID aus dem Apple Store.
- **AppTunnel**
  - **URL-Platzhalter**: Die URL, die der Client für den Verbindungsaufbau mit dem Files Advanced Gateway Server verwendet. Die für den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

3. Klicken Sie auf **Speichern**.

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



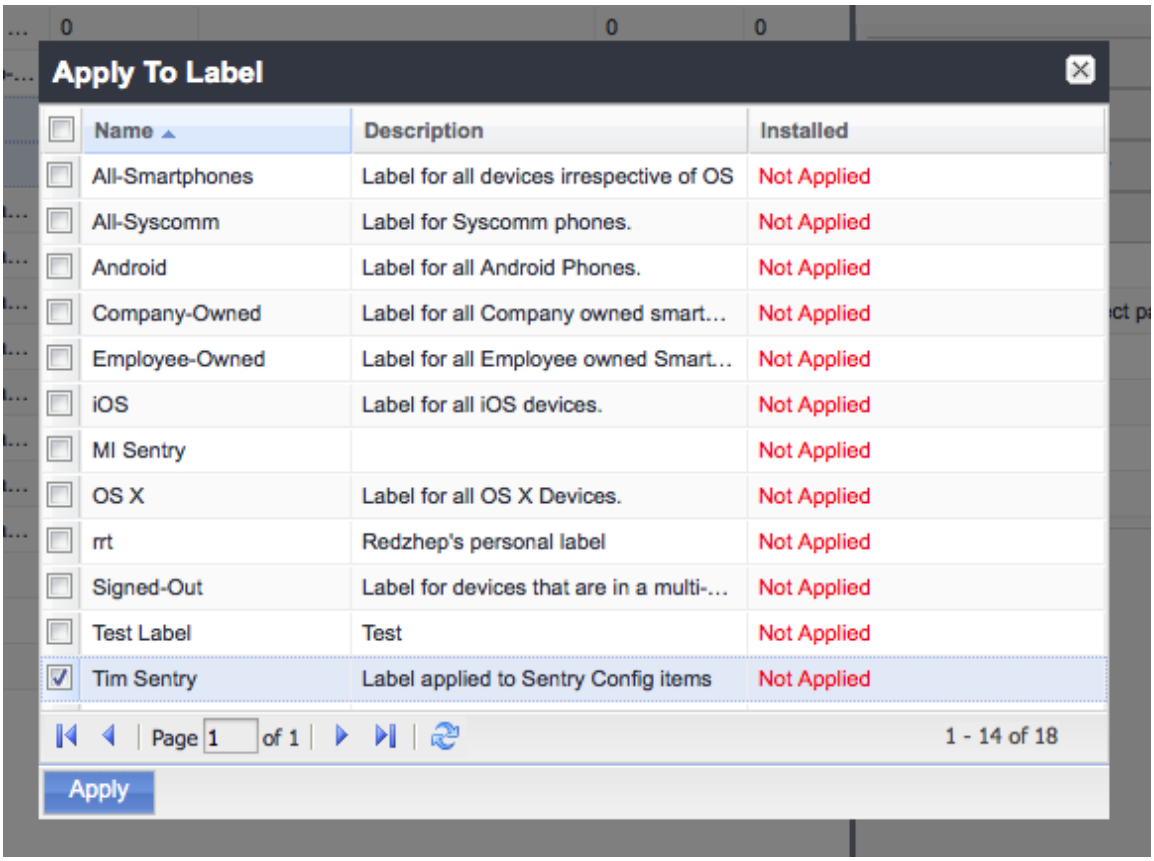
1. Wählen Sie noch innerhalb des Admin-Portals von MobileIron VSP **Benutzer und Geräte** und öffnen Sie **Label**.
2. Drücken Sie auf **Neues hinzufügen**.



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

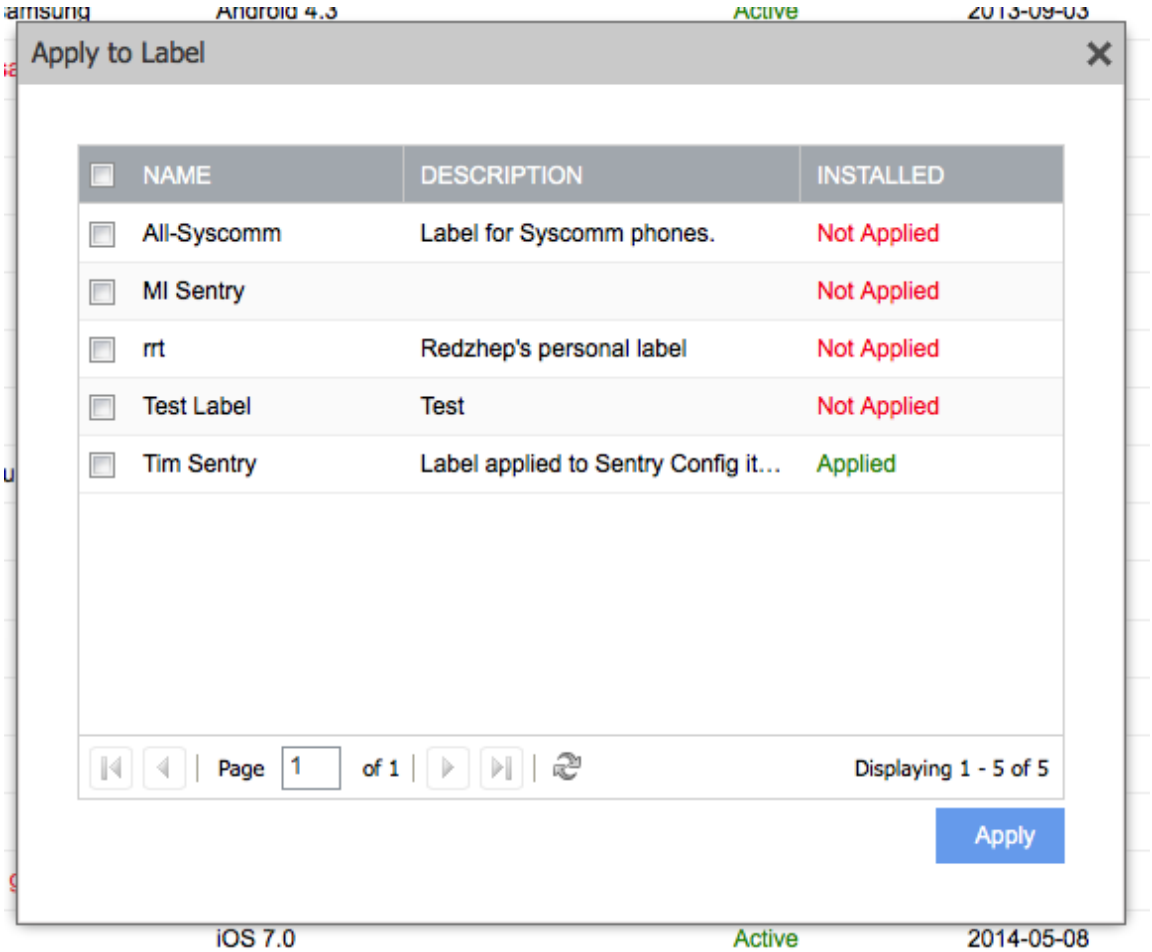
1. Während Sie sich noch im Admin-Portal von MobileIron VSP befinden, wählen Sie die Option **Richtlinien und Konfigurationen**.

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



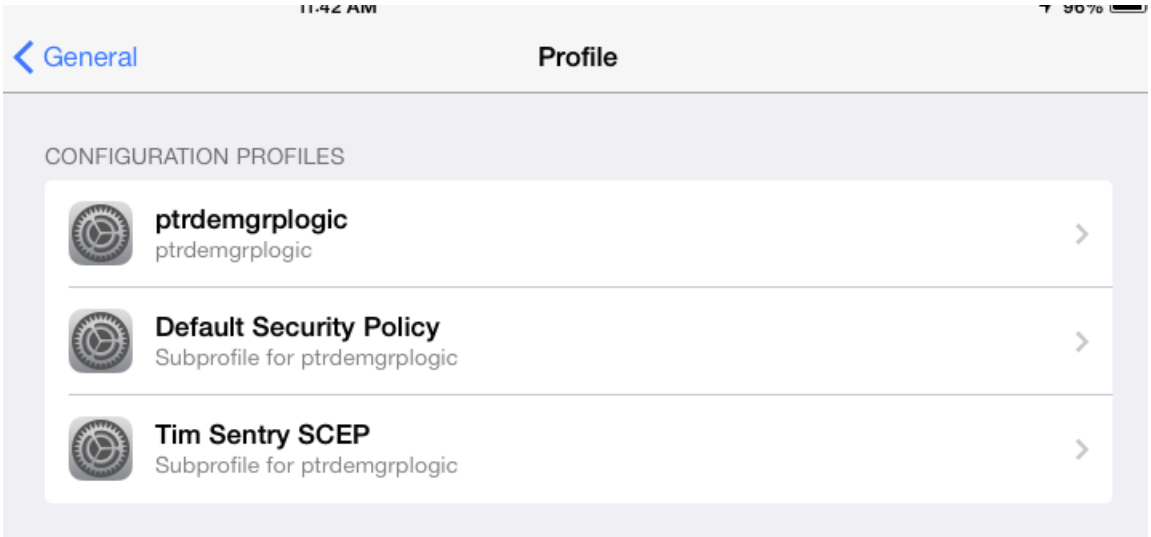
3. Drücken Sie auf **Weitere Aktionen** und wählen Sie **Für Label übernehmen**.
4. Markieren Sie das in "Ein neues Label erstellen" erstellte Label.
5. Klicken Sie auf **Anwenden**.
1. Während Sie sich noch im Admin-Portal von MobileIron VSP befinden, wählen Sie **Benutzer und Geräte** und öffnen Sie **Geräte**.

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

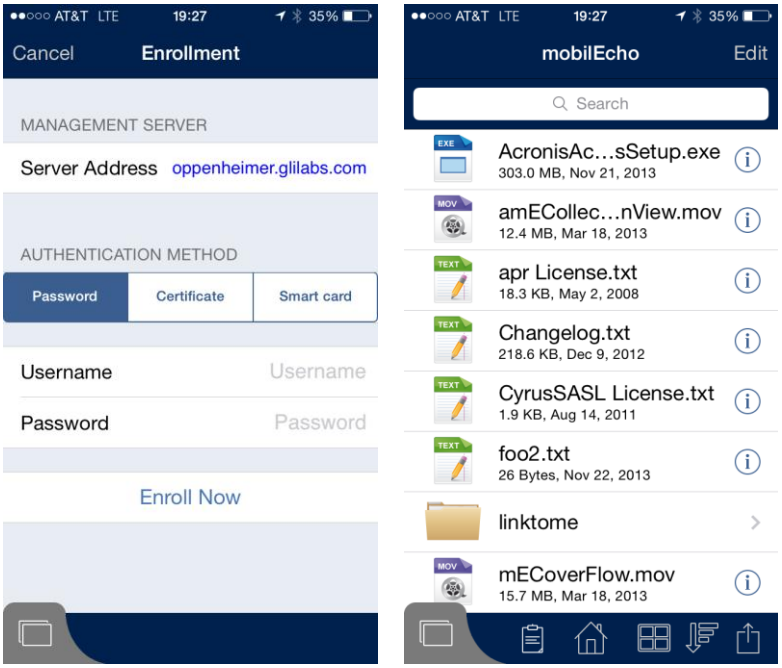


3. Wählen Sie **Aktionen** -> **Für Label übernehmen**.
4. Markieren Sie das in "Ein neues Label erstellen" erstellte Label.
5. Klicken Sie auf **Anwenden**.
1. Öffnen Sie die App Mobile@Work, und rufen Sie die **Einstellungen** auf.
2. Tippen Sie auf 'Automatisch auf Updates prüfen'.

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



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



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

Jetzt sollte 'Sie sind jetzt für das Files Advanced Client Management registriert' angezeigt werden.

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

Nutzung des AppTunnel überprüfen

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

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

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

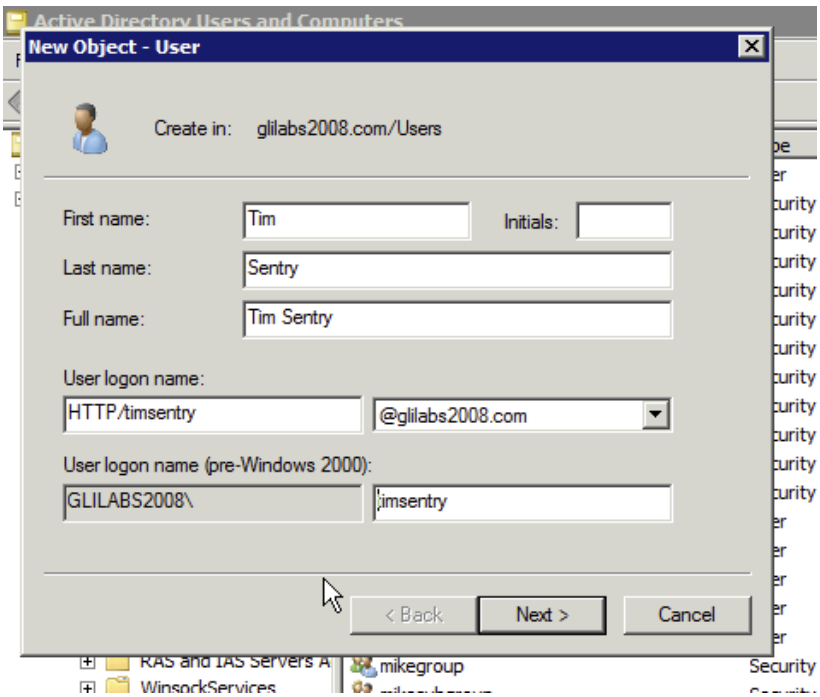
14 Hinzufügen der Authentifizierung per eingeschränkter Kerberos-Delegierung

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

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

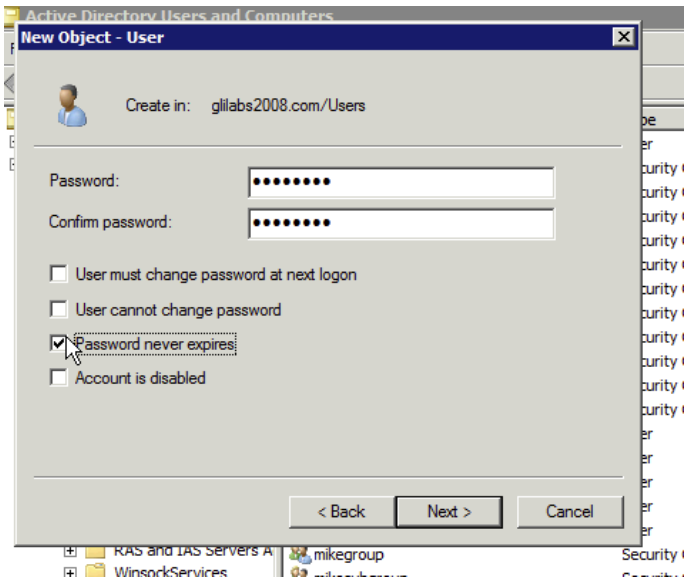
Wenn Sie das gleiche iOS-Gerät zum Testen der eingeschränkten Kerberos-Delegierung verwenden, wird empfohlen, Acronis Files Advanced Mobile zu diesem Zeitpunkt zu deinstallieren.

1. Melden Sie sich an Ihrem KDC-Server als Administrator an.
2. Wählen Sie im Windows-Startmenü **All Programs** und wählen Sie **Administrative Tools** > **Active Directory Users and Computers**.
3. Erweitern Sie in der neu geöffneten Konsole den Bereich (in Kerberos die Bezeichnung für Domäne).
4. Klicken Sie mit der rechten Maustaste auf **Users** und wählen Sie **New** > **User**.



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

5. Klicken Sie auf **Next**.



- **Password**: Geben Sie das Kennwort ein.
- **Password never expires**: Stellen Sie sicher, dass 'Benutzer muss Kennwort bei der nächsten Anmeldung ändern.' nicht ausgewählt ist. Bei der Enterprise-Bereitstellung dürfen die Felder **User cannot change password** und **Password Never Expires** nicht ausgewählt sein.

6. Klicken Sie auf **Next**.
7. Klicken Sie auf **Finish**.

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

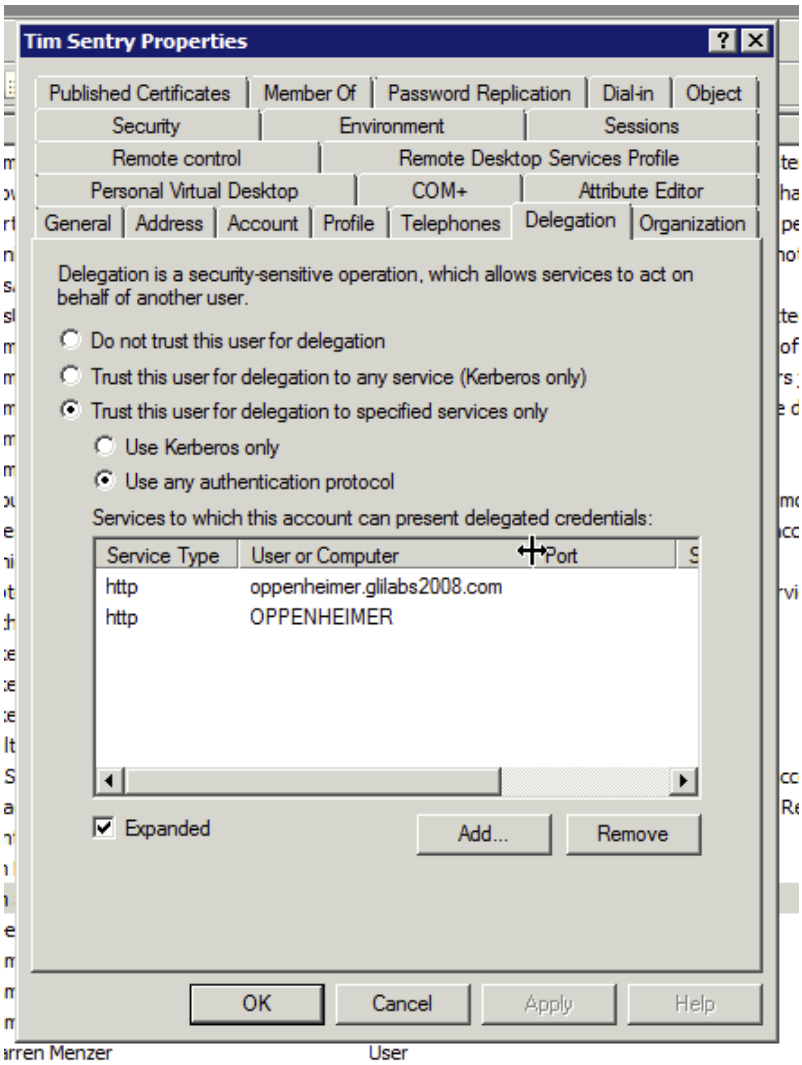
1. Öffnen Sie auf dem KDC-Server ein Fenster mit einer Eingabeaufforderung.
2. Geben Sie bei der Eingabeaufforderung den folgenden Befehl ein: **ktpass /out nameofsentry.keytab /mapuser nameofuser@domain /princ HTTP/nameofuser /pass password**

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

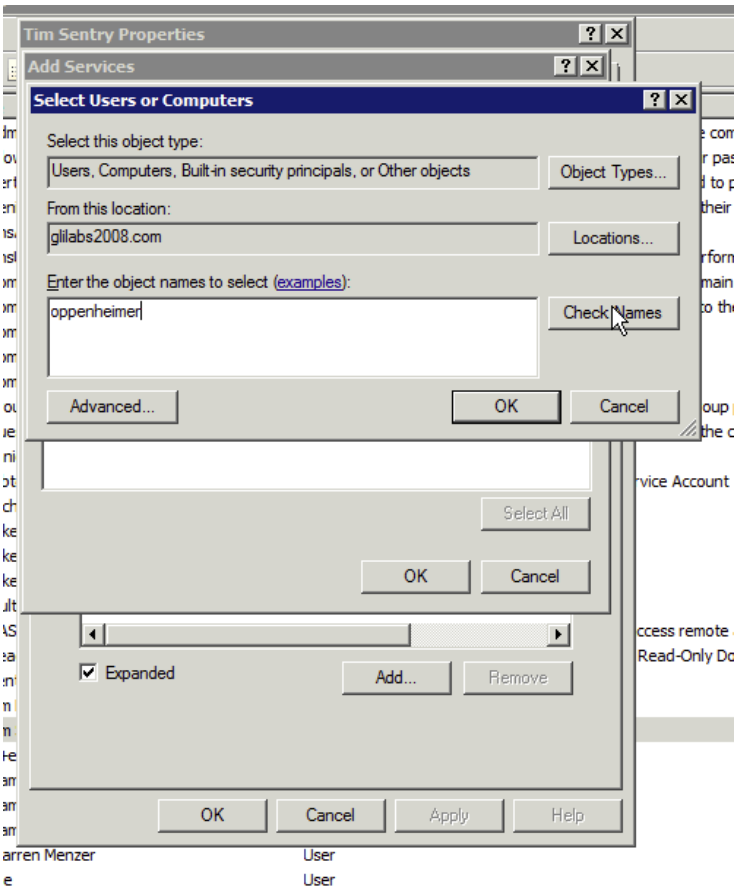
```
C:\Users\Administrator>ktpass /out timsentry.keytab /mapuser timsentry@glilabs20
08.com /princ HTTP/timsentry@glilabs2008.com /pass [redacted]
Targeting domain controller: dc.glilabs2008.com
Using legacy password setting method
Successfully mapped HTTP/timsentry to timsentry.
WARNING: pType and account type do not match. This might cause problems.
Key created.
Output keytab to timsentry.keytab:
Keytab version: 0x502
keysize 65 HTTP/timsentry@glilabs2008.com ptype 0 (KRB5_NT_UNKNOWN) vno 3 etype
0x17 (RC4-HMAC) keylength 16 (0x5c875e4d5257b48f74cc445af903ea89)
```

Diese Warnung kann ignoriert werden.

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

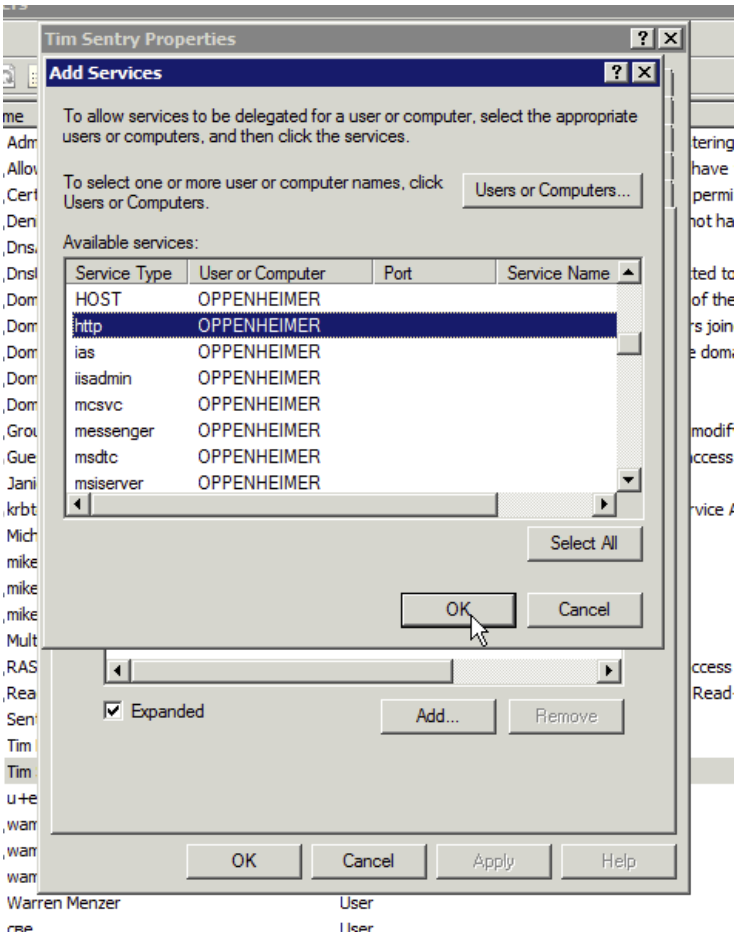


6. Klicken Sie auf **Hinzufügen**.
7. Klicken Sie auf **Benutzer oder Computer**.
   - Geben Sie die Adresse Ihres Files Advanced Gateway Servers ein.
   - Klicken Sie auf **Namen überprüfen**.
   - Der richtige Computername sollte im Kästchen 'Objektname' angezeigt werden.



8. Klicken Sie auf **OK**.

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

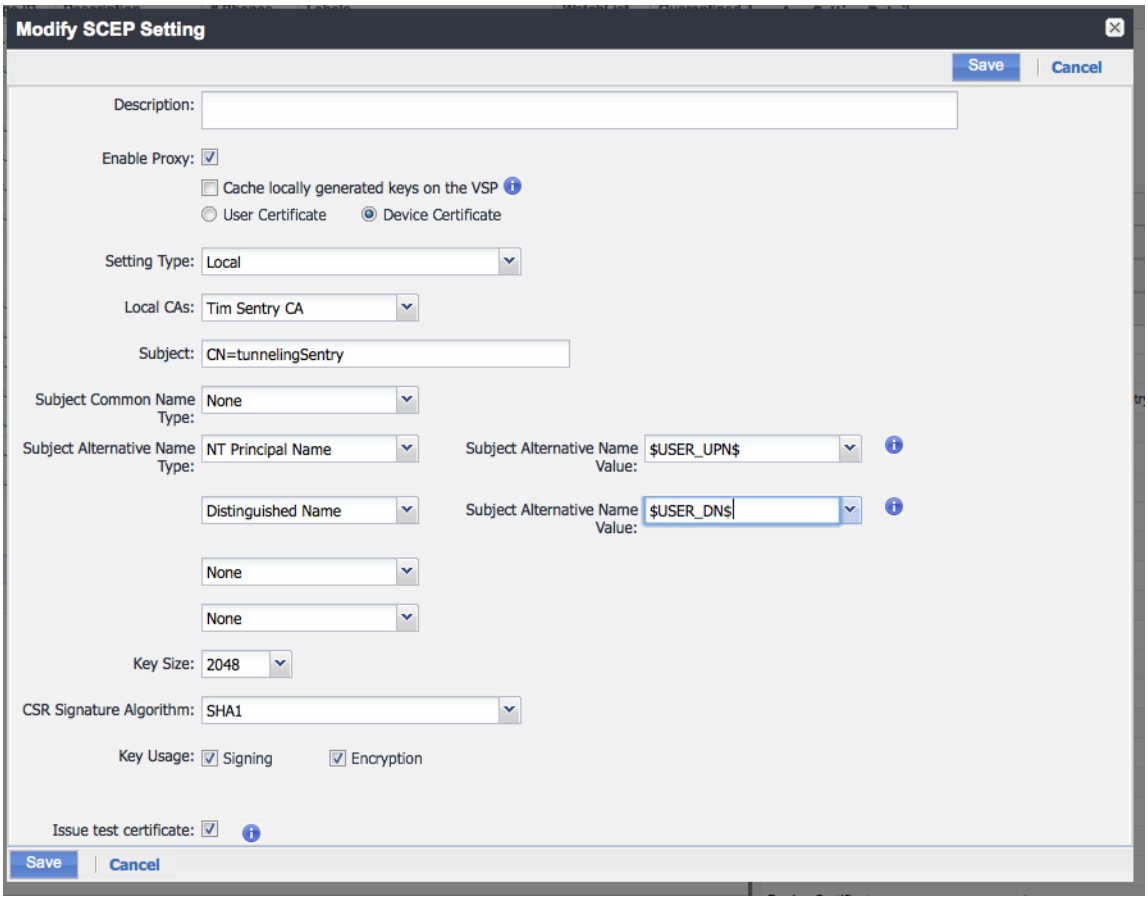


10. Klicken Sie auf **OK**.

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

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

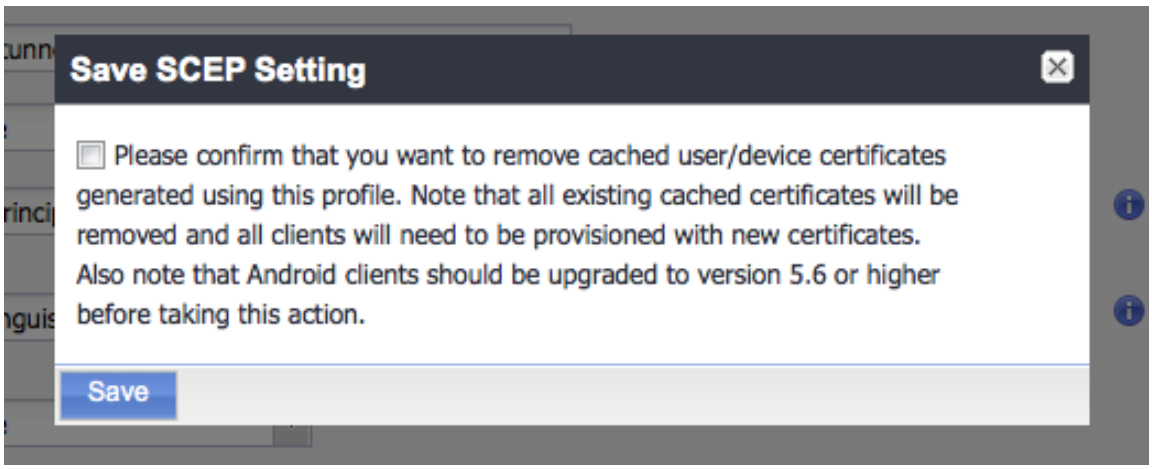
4. Klicken Sie auf dessen Namen und dann im Feld auf der rechten Seite auf **Bearbeiten**.



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

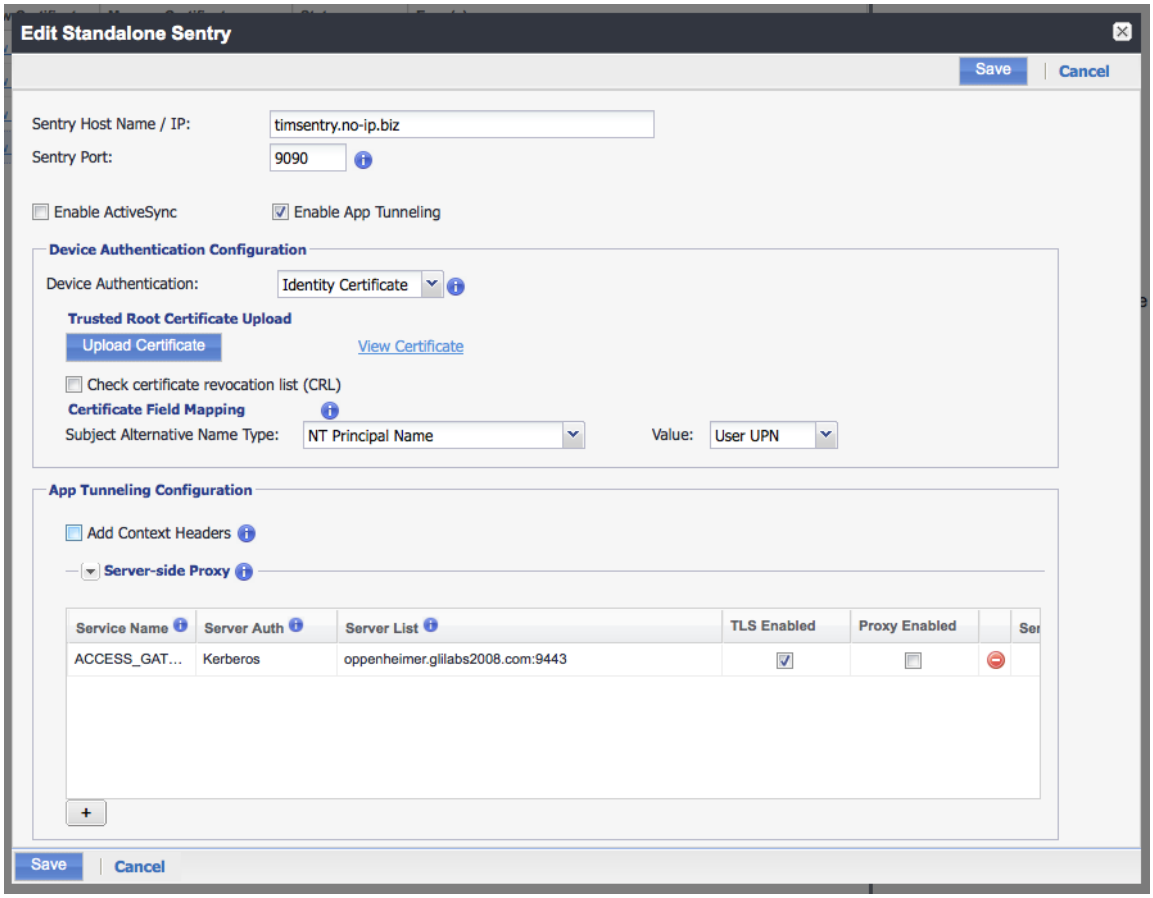
Hinweis: *Diese Einträge erfordern, dass Benutzerkonten auf dem VSP von Active Directory stammen und diese Variablen von ihm bereitgestellt werden. Diese Konfiguration sprengt den Rahmen dieses Dokuments.*

5. Klicken Sie auf **Speichern**.

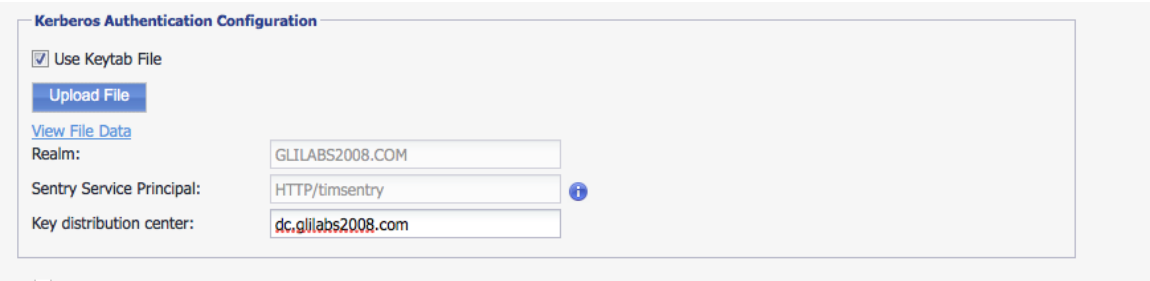


6. Da Sie das SCEP geändert haben, müssen Sie das Gerät in Mobile@Work erneut bereitstellen, bevor Sie den iOS-Client testen.

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



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



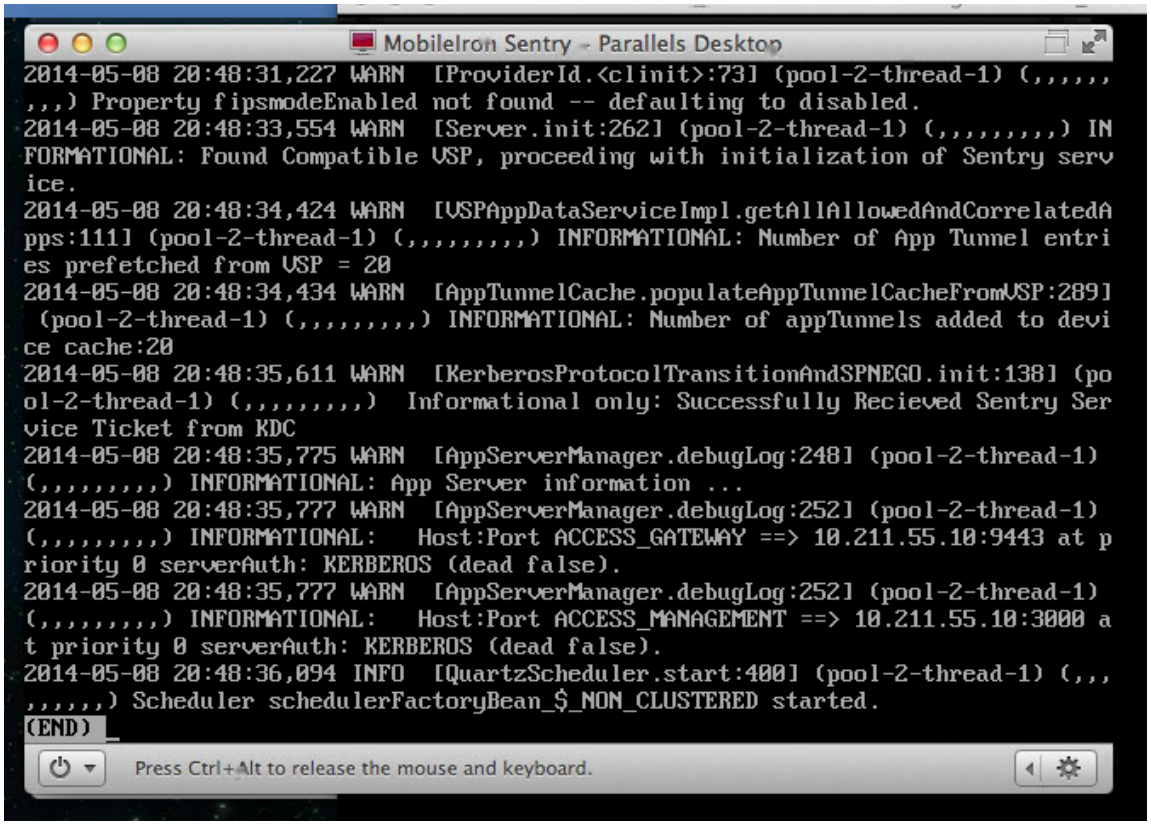
- Im Abschnitt **Konfiguration der Kerberos-Authentifizierung**.
  - Markieren Sie **Keytab-Datei verwenden**.
  - Klicken Sie auf **Datei hochladen**.

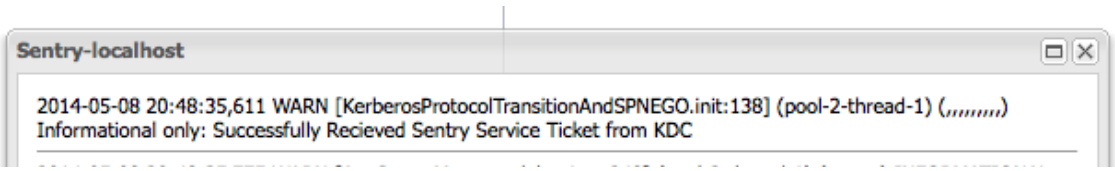
- Laden Sie die unter "Eine Keytab für das Kerberos-Dienstkonto erstellen" erstellte Keytab-Datei hoch.
- Verschieben Sie den Domain-Controller in den KDC.

4. Klicken Sie auf **Speichern**.

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

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

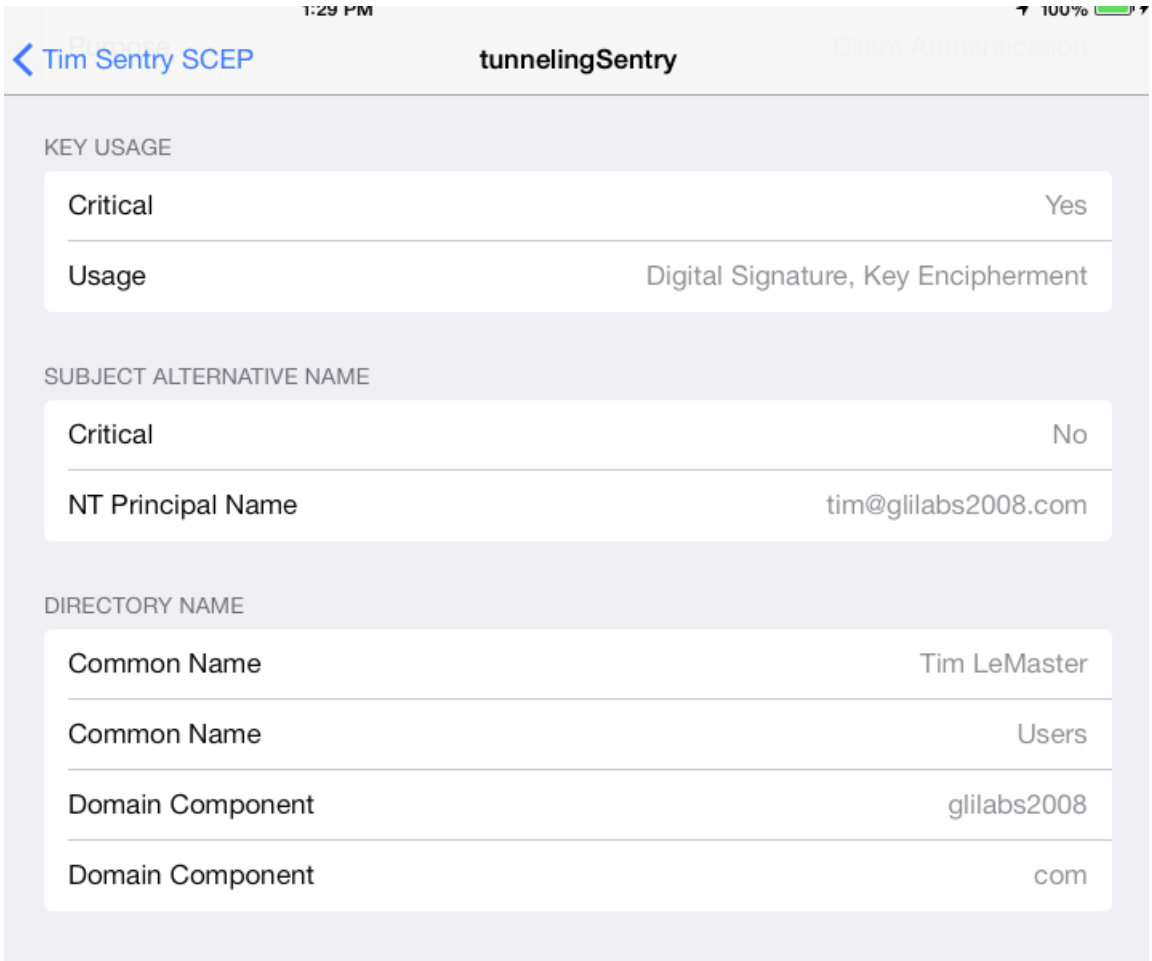




Die von uns durchgeführten Änderungen des SCEP müssen an das iOS-Gerät übertragen werden. Es kann einige Minuten dauern, bis die an Sentry durchgeführten Änderungen vollständig übertragen worden sind.

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

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



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

Delegierung für Netzwerkfreigaben und SharePoint

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

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

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

1. Öffnen Sie **Active Directory-Benutzer und -Computer**.
2. Suchen Sie das Computerobjekt, das dem Gateway-Server entspricht.

   Hinweis: *Wenn Sie den Gateway Server unter einem* ***Benutzer****konto ausführen, wählen Sie dieses* ***Benutzer****objekt stattdessen aus.*

3. Klicken Sie mit der rechten Maustaste auf den Benutzer und wählen Sie "Eigenschaften".
4. Rufen Sie die Registerkarte **Delegation** auf.
5. Wählen Sie **Diesem Computer nur für die Delegierung für bestimmte Dienste vertrauen** aus.
6. Wählen Sie darunter die Option **Use any authentication protocol**.
7. Klicken Sie auf **Add**.
8. Klicken Sie auf **Users or Computers**.
9. Suchen Sie nach dem Serverobjekt für die SMB-Freigabe oder den SharePoint-Server und klicken Sie auf **OK**.
   - Wählen Sie für SMB-Freigaben den Dienst **cifs** aus.
   - Wählen Sie für SharePoint den Dienst **http** aus.
10. Wiederholen Sie die Schritte für jeden Server, für den der Files Advanced Gateway Server Zugriff benötigt.
11. Wiederholen Sie dieses Verfahren für jeden Gateway Server.

Diese Delgierungsänderungen benötigen, je nach Größe der Domänengesamtstruktur, möglicherweise einige Minuten für das Propagieren. Es kann bis zu 15 Minuten (oder mehr) dauern, bis die Änderungen in Kraft treten. Werden die Änderungen nicht nach 15 Minuten angezeigt, versuchen Sie, den Files Advanced Gateway-Dienst neu zu starten.

14.1.1 Files Advanced für BlackBerry Dynamics

Themen

14.1.1.1 Für iOS

Themen

Einführung

Files Advanced und BlackBerry Technology sind eine Partnerschaft eingegangen, um die mobile Dateiverwaltung von Files Advanced auf die BlackBerry Dynamics-Plattform zu übertragen. Dank dieser optionalen Files Advanced-Funktion kann die Files AdvancedMobile-App zusammen mit anderen Blackberry-fähigen Apps mit einem einheitlichen Satz von BlackBerry Dynamics-Richtlinien und -Diensten verwaltet werden.

Folgende Komponenten gehören zur BlackBerry Dynamics Plattform:

- **Server von BlackBerry Control** – Eine serverbasierte Konsole, mit der das Unternehmen den Client-Zugriff auf für BlackBerry Dynamics aktivierte Apps ermöglichen, Richtliniensätze für Applikationsberechtigungen und die erlaubten Gerätetypen erstellen sowie den Zugriff auf Apps von BlackBerry Dynamics auf bestimmten Geräten widerrufen und die Apps auf diesen löschen kann.
- **BlackBerry Proxy-Server** – Dieser Dienst wird auf einem Server vor Ort installiert und bietet Netzwerkzugriff für BlackBerry Dynamics-Apps, die mit Servern vor Ort kommunizieren müssen, z. B. mit einem Files Advanced-Gateway-Server.
- **Files Advanced für BlackBerry Dynamics App** – Für BlackBerry Dynamics aktivierte Apps wie **Files Advanced für BlackBerry Dynamics** umfassen integrierte Dienste von BlackBerry Dynamics, mit denen die App entfernt über die BlackBerry Dynamics Plattform verwaltet werden kann. Ferner steht die App mit einem nach FIPS 140-2 zertifizierten lokalen verschlüsselten Sicherheitsspeicher und mit Sicherheitskommunikation von BlackBerry zur Verfügung.

Files Advanced für BlackBerry Dynamics erfordert Folgendes:

- **Files Advanced für BlackBerry Dynamics Client App** – Die im Apple App Store verfügbare Files Advanced für BlackBerry Dynamics Client-App http://www.grouplogic.com/web/megoodappstore ist speziell für die Einbindung in BlackBerry Dynamics konzipiert. Bei der ersten Installation und Ausführung der App Files Advanced für BlackBerry Dynamics auf einem Gerät, wird der Benutzer aufgefordert, die App in BlackBerry Dynamics zu aktivieren. Diese Aktivierung ist erforderlich, bevor der Benutzer mit der Registrierung der App auf dem Files Advanced-Server und dem Zugriff auf Dateien fortfahren kann.
- **Files Advanced Server** – Files Advanced für BlackBerry Dynamics verwendet dieselbe serverseitige Software wie die Standardversion von Files Advanced. Es sind keine Änderungen auf der Serverseite erforderlich, damit Files Advanced Server mit den für BlackBerry Dynamics aktivierten Files Advanced Clients arbeiten kann. So kann sichergestellt werden, dass alle Files Advanced mit Zugriff auf Files Advanced-Dateien von BlackBerry Dynamics verwaltet werden.

Nachdem ein Files Advanced für BlackBerry Dynamics Client in BlackBerry Dynamics registriert ist, wird die gesamte Kommunikation mit den Gateway Servern über den sicheren Kommunikationskanal geleitet.

Eine Testversion von Files Advanced für BlackBerry Dynamics testen

Das Testen von Files Advanced für BlackBerry Dynamics entspricht weitgehend dem Test einer normalen Files Advanced-Testversion.

1. Eine Testversion der serverseitigen Software können Sie über die Acronis-Website anfordern. Sobald das Anforderungsformular gesendet wurde, erhalten Sie eine E-Mail mit Links zum Herunterladen des Installers für die Files Advanced-Server-Testversion und zur Schnellstart-Anleitung (S. 7), die Sie bei der erstmaligen Einrichtung unterstützt.
2. Die Files Advanced für BlackBerry Dynamics-Client-App kann kostenlos aus dem Apple App Store http://www.grouplogic.com/web/megoodappstore heruntergeladen werden.

Hinweis: *Files Advanced für BlackBerry Dynamics-Client-Apps müssen im BlackBerry Dynamics-System aktiviert werden, bevor sie für den Zugriff auf Gateway Server konfiguriert werden können. Wenn Sie bereit sind, Files Advanceds in BlackBerry Dynamics zu registrieren, lesen Sie die folgenden Abschnitte in diesem Dokument.*

Files Advanced in BlackBerry Control anfordern und konfigurieren

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

Themen

Um Zugriff auf **Files Advanced für BlackBerry** anzufordern, besuchen Sie den BlackBerry-Marketplace (https://begood.good.com/marketplace.jspa https://begood.good.com/marketplace.jspa), und suchen Sie **Files Advanced für BlackBerry** in der Liste verfügbarer **BlackBerry Dynamics**-Apps.

Klicken Sie auf der Seite der Files Advanced für https://begood.good.com/gd-app-details.jspa?ID=248978 BlackBerry-App auf die Schaltfläche Start Trial', um eine Demoversion oder eine lizenzierte Version der App zu erhalten. https://begood.good.com/gd-app-details.jspa?ID=248978

Wenn Sie eine Demoversion der App anfordern, sollten Sie innerhalb weniger Minuten Zugriff darauf haben. Wenn Ihre Anforderung akzeptiert wurde, erhalten Sie von der BlackBerry-Website eine Benachrichtigung, in der Sie darüber informiert werden, dass die **Files Advanced für BlackBerry**-App auf Ihrem BlackBerry Control-Server veröffentlicht wurde.

Hinweis: *Wenn Sie keinen Zugriff erhalten, wenden Sie sich an den Support von BlackBerry Dynamics.*

Melden Sie sich danach auf dem BlackBerry Control-Server an, und klicken Sie im Menü auf der linken Seite auf **Apps verwalten (Manage Apps)**. Files Advanced sollte jetzt in der Liste der Applikationen aufgeführt werden. Ist dies nicht der Fall, warten Sie ca. eine Viertelstunde ab und überprüfen Sie die Liste dann noch einmal. Diese Zeit sollte ausreichen, um die Änderung auf dem Server umzusetzen.

Damit Files Advanced über den BlackBerry Proxy Server auf Ihren Files Advanced Gateway Server zugreifen können, müssen Sie den Zugriff auf die Domain konfigurieren, auf der sich Ihre Files Advanced Gateway Server befinden. Dies erfolgt in der Good Control-Konsole auf der Seite **Client-Verbindungen**.

Zugriff von Ihrer Domäne gestatten

Diese Einstellung gestattet allen BlackBerry-Clients, sich mit allen Servern in den angegebenen Domänen zu verbinden. Wenn Sie dies nicht wünschen, richten Sie stattdessen **Zusätzliche Server (Additional Servers)**ein.

1. Öffnen Sie im linken Menü die Einstellungen für die **Client-Verbindungen**.
2. Erweitern Sie **Zulässige Domänen (Allowed Domains)**. Sofern **Alle Domänen zulassen (Allow all domains)** nicht aktiviert ist, drücken Sie auf das Plus-Symbol (+), und geben Sie den Namen Ihrer Domäne ein (z.B. meinefirma.com).
3. Klicken Sie auf **Übermitteln (Submit)**.

Ihre Domäne als Standard-Domäne für Verbindungen zuweisen

1. Erweitern Sie **Standard-Domänen (Default Domains)**.
2. Drücken Sie auf das Plus-Symbol (+), und geben Sie den Namen Ihrer Domäne ein.
3. Drücken Sie auf **Übermitteln (Submit)**.

Bestimmten Servern die Verbindung gestatten

Verwenden Sie anstelle der **Zulässige Domänen** diese Einstellung, wenn Sie möchten, dass Ihre Good-Clients sich nur mit diesen bestimmten Servern und nicht mit allen Servern in der Domäne verbinden.

1. Öffnen Sie im linken Menü die Einstellungen für die **Client-Verbindungen**.
2. Erweitern Sie **Zusätzliche Server (Additional Servers)**.
3. Drücken Sie auf das Plus-Symbol (+), und geben Sie den DNS-Namen und Port des Servers ein, für den Sie den Zugriff gestatten möchten. Wiederholen Sie diesen Schritt für alle Files Advanced Server, mit denen sich Ihre BlackBerry-Clients verbinden sollen.

BlackBerry Dynamics-Richtliniensätze und Files Advanced

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

Hinweis: *Wenn Sie im BlackBerry-Portal für den* ***Richtliniensatz*** *eines Benutzers FIPS aktivieren, kann die Files Advanced-App nicht über Drittanbieterzertifikate nach IP-Adresse auf Gateway-Server zugreifen.*

Dazu gehören diese Einstellungen:

- Kennwortanforderungen zum Sperren der Applikation
- Richtlinien zum Sperren des Bildschirms
- Schutz vor Datenverlust
- Zulässige Betriebssystemversionen und Hardwaremodelle
- Überprüfung der Verbindung
- Jailbreak/Root-Erkennung

Auswirkungen und Beschränkungen der Schutzfunktion gegen Datenlecks

Wenn **Schutzfunktion gegen Datenlecks** in einem Richtliniensatz aktiviert ist, ist die Files Advanced-App nicht in der Lage, die folgenden Aktionen durchzuführen:

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

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

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

Files Advanced Zugriff auf BlackBerry Dynamics-Benutzer oder -Gruppen gewähren

Bevor ein Benutzer seine Files Advanced-App in BlackBerry Dynamics registrieren kann, muss er die Files Advanced-Applikation zur Liste **Erlaubte Apps** seiner Benutzerkonten oder zu einer erlaubten **Applikationsgruppe**, der er angehört, hinzufügen. Darüber hinaus muss dem Benutzer ein eindeutiger **Zugriffsschlüssel** gesendet werden, der während des Registrierungsprozesses in die Files Advanced-App eingegeben werden muss.

WICHTIGER HINWEIS ZUR BEREITSTELLUNG: *Wenn Sie einzelnen Benutzern Zugriff auf BlackBerry Dynamics-Applikationen zuweisen, müssen Sie die bestimmten Versionsnummern der App auswählen, auf die Zugriff gewährt werden soll. Wenn Sie den Zugriff auf der Benutzerebene verwalten, müssen Sie bei der Veröffentlichung neuer Versionen von Files Advanced für BlackBerry die BlackBerryControl-Konfiguration des Benutzers aufrufen und die neue Version hinzufügen. Erst danach kann diese Version verwendet werden.*

*Es wird **dringend geraten**, den Zugriff auf BlackBerry Dynamics-Apps über die Funktion **Gruppen verwalten** in der Konsole von BlackBerry Control zu gestatten. Mit BlackBerry Control sind Sie in der Lage, einer Gruppe Zugriff auf ALLE Versionen einer App zu gewähren, damit auch zukünftige Versionen ohne Eingriff durch den IT-Administrator erlaubt werden.*

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

1. Wählen Sie im Menü auf der linken Seite der Konsole von BlackBerry Control **App-Gruppen (App Groups)** oder **Benutzer verwalten**.
2. Wählen Sie die Gruppe oder den Benutzer aus, der bzw. dem Sie Zugriff auf Files Advanced für BlackBerry gestatten möchten, und bearbeiten Sie diese.
3. Klicken Sie im Abschnitt **Apps** auf die Schaltfläche **Weitere hinzufügen**.

4. Wählen Sie **Files Advanced für BlackBerry** in der Liste verfügbarer Applikationen aus, und klicken Sie auf **OK**.

So erstellen Sie einen Zugriffsschlüssel, mit dem ein Benutzer seine **Files Advanced für BlackBerry**-App bei **BlackBerry** Dynamics registrieren kann:

1. Wählen Sie im Menü auf der linken Seite der Konsole von BlackBerry Control **Benutzer verwalten**.
2. Wählen Sie den Benutzer aus, für den Sie einen **Zugriffsschlüssel** erstellen möchten, und bearbeiten Sie diesen.
3. Drücken Sie auf der Registerkarte **Zugriffsschlüssel** auf **Zugriffsschlüssel**.

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

Die Files Advanced-Client-App in BlackBerry Dynamics registrieren

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

So registrieren Sie eine Files Advanced-Client-App in **BlackBerry** Dynamics:

Hinweis: Zur einfachen Aktivierung *muss mindestens eine BlackBerry-Anwendung (BlackBerry Work, BlackBerry Access oder BlackBerry Agent) installiert sein, damit die Aktivierung gelingt. Anwendungen, die von einer früheren Version von Files Advanced aktualisiert wurden, die über die Anwendung eines Drittanbieters aktiviert wurde, sollten weiterhin wie erwartet funktionieren.*

1. Starten Sie **Files Advanced für** BlackBerry **Dynamics** auf Ihrem Gerät.
2. Geben Sie Ihre **E-Mail-Adresse** und den **Zugriffsschlüssel** ein, der Ihnen vom IT-Administrator zugeschickt wurde.
3. Während der Registrierung Ihrer App bei BlackBerry Dynamics sehen Sie eine Statusanzeige.
4. Falls von Ihrer BlackBerry Dynamics-Richtlinie verlangt, werden Sie aufgefordert, ein Kennwort zum Sperren der Applikation zu erstellen. Wenn Sie auch BlackBerry for Enterprise verwenden, verlangt Files Advanced u.U. die Anmeldung bei BlackBerry for Enterprise, damit Sie Zugriff auf die Files Advanced-App erhalten. Sobald dieser Prozess abgeschlossen ist, gelangen Sie zum Startbildschirm der Files Advanced-App.

Ab diesem Punkt müssen Sie beim Starten der Files Advanced-App eventuell das Kennwort für die Files Advanced für BlackBerry Dynamics-App eingeben, das Sie zuvor konfiguriert haben, oder Sie müssen sich bei Ihrer BlackBerry für Enterprise-App authentifizieren, bevor Files Advanced geöffnet wird.

Abgesehen von dieser Anforderung funktioniert Files Advanced für BlackBerry Dynamics auf die gleiche Weise wie die standardmäßige Files Advanced-App. Manche Funktionen sind aufgrund der festgelegten BlackBerry Dynamics-Richtlinien möglicherweise eingeschränkt. Dies betrifft Funktionen

wie das Öffnen von Files Advanced-Dateien in anderen Drittanbieter-Applikationen, das Senden von Dateien per E-Mail, das Drucken von Dateien, das Kopieren und Einfügen von Text aus Files Advanced-Dateien usw.

Hinweis: *Sobald die Files Advanced für die BlackBerry Dynamics-App in BlackBerry Dynamics aktiviert wurde, kann sie nicht mehr deaktiviert werden. Wenn Sie zu einer Standardversion von Files Advanced wechseln möchten, müssen Sie die Files Advanced für BlackBerry Dynamics-App löschen und die standardmäßige Files Advanced-App neu installieren.*

Sideload von Files Advanced

Die BlackBerry Dynamics-Version der Files Advanced-App unterstützt nun die Funktion **iTunes Dateifreigabe**. Mit dieser Funktion können Dateien und Ordner direkt in den Ordner 'Dokumente' der Sandbox der App kopiert werden. Sobald sie sich in der App-Sandbox befinden, werden sie automatisch in den verschlüsselten Speicherbereich der App und dort in die richtigen Ordner importiert.

Das Sideloaden von Dateien ist auf den freien Speicherplatz auf dem Gerät begrenzt. Um einen Sideload-Vorgang erfolgreich durchführen zu können, muss ausreichend freier Speicherplatz vorhanden sein, zumindest ausreichend für den Umfang der größten zu importierenden Datei. Diese Funktion ist für die 2-Wege-Dateiübertragung bestimmt. Die Benutzer sind weder zum Lesen noch zum Kopieren der Dateien berechtigt.

Hinweis: *Die Files Advanced-App ist an der Übertragung von Dateien mit der iTunes Dateifreigabe nicht aktiv beteiligt.*

Hinweis: *Dieser Vorgang erfordert eine neue Installation von Files Advanced für BlackBerry Dynamics, die nicht für die Verwaltung registriert ist.*

Dokumente für das Sideloaden vorbereiten

Hinweis: *Vergewissern Sie sich, dass auf dem Gerät ausreichend freier Speicherplatz zur Verfügung steht, bevor Sie das Sideloaden starten. Unterbrechen Sie auf keinen Fall eine laufende Synchronisierung.*

1. Navigieren Sie in der Webadministration von Files Advanced Advanced zu „Mobiler Zugriff“ --> „Datenquellen“.
2. Wenn Sie bestimmte, bereits vorhandene Datenquellen nutzen wollen, müssen diese als 1-Wege- oder 2-Wege-Synchronisierungsordner gekennzeichnet sein. Wenn noch keine für das Sideloaden vorgesehene Datenquellen vorhanden sind, können Sie diese erstellen.
3. Weisen Sie die Datenquellen einer Gruppe von Benutzern zu, deren iOS-Geräte für das Sideloaden vorgesehen sind. Für dieses Beispiel wird ein Ordner mit der Bezeichnung 'Referenz' erstellt.
4. Erstellen Sie auf einem Computer einen Ordner mit dem Namen 'Für Import' und kopieren Sie die gewünschten Ordner dort hinein. In diesem Beispiel enthält der Ordner 'Für Import' also den Referenzordner, in dem sich wiederum die Dokumente befinden, die der Server normalerweise über das Internet mit dem iOS-Gerät synchronisieren würde.

   Hinweis: *Die Namen der Ordner im 'Für Import'-Ordner müssen exakt mit den Anzeigenamen der Datenquellen übereinstimmen. Beispiel: Eine Datenquelle heißt 'Referenz' und im 'Für Import'-Ordner wird ein Ordner 'Referenz' angelegt.*

5. Um diesen Vorgang auf einem Windows-Computer ausführen zu können, müssen Sie iTunes installieren.

Über iTunes synchronisieren

1. Installieren Sie die App Files Advanced für BlackBerry Dynamics.
2. Schließen Sie das iOS-Gerät über ein Kabel an einen Computer an. Reine Ladekabel sind hierfür nicht geeignet.
3. Öffnen Sie iTunes und wählen Sie das Gerät aus. Klicken Sie am Computer und auf dem Gerät auf 'Vertrauen', wenn Sie dazu aufgefordert werden.
4. Klicken Sie in iTunes auf das Gerätesymbol und dann auf den Abschnitt 'Apps' in der linken Seitenleiste.
5. Scrollen Sie auf der Seite nach unten zum Abschnitt 'Dateifreigabe', und wählen Sie 'Files Advanced' aus.
6. Ziehen Sie den zuvor erstellen Ordner 'Für Import' in iTunes in den Abschnitt für die Files Advanced-Dokumente.
7. Klicken Sie auf 'Synchronisieren'. Befolgen Sie ggf. weitere Aufforderungen von iTunes und warten Sie, bis die Synchronisierung abgeschlossen ist.

Geladene Dokumente registrieren und importieren

1. Wenn die iTunes-Synchronisierung abgeschlossen ist, starten Sie die Files Advanced für BlackBerry-App.

   Hinweis: *Dateien und Ordner werden importiert, bevor die Files Advanced-App beim Files Advanced Server registriert wird. Der Vorgang muss mit einer Neuinstallation ausgeführt werden.*

   Hinweis: *Diese Funktion lädt erstmalig den Inhalt des Synchronisierungsordners und übergibt die Zuständigkeit für die Ordnersynchronisierung anschließend an die Files Advanced-App. Im Anschluss daran läuft die Synchronisierung wie üblich ab.*

2. Geben Sie die E-Mail-Adresse von BlackBerry und den Zugriffsschlüssel für Ihren Benutzer ein.
3. Befolgen Sie die Anweisungen des Assistenten und schließen Sie die Registrierung auf dem Files Advanced Server ab. Sie werden aufgefordert, Ihren Benutzernamen und Ihr Kennwort für Files Advanced einzugeben.
4. Verwerfen Sie das Lernprogramm, das beim ersten Durchlauf erscheint.
5. Der Importvorgang beginnt. Die Files Advanced-App importiert die Dokumente, die per Sideload in den sicheren Container kopiert wurden. Dann stimmt Sie mit dem Server ab, welche Dokumente dem betreffenden Synchronisierungsordner entsprechen. Wenn alle Inhalte übereinstimmen, ist das Gerät für den (die) per Sideload übertragenen Synchronisierungsordner synchron.

Wichtige Hinweise

- Zugewiesene Synchronisierungsordner, die kein Gegenstück im Ordner 'Für Import' haben, werden automatisch ignoriert. Erst nach Abschluss des Importvorgangs wird über eine Funkverbindung (Over-the-Air; OTA) eine umfassende Erstsynchronisierung durchgeführt.
- Im Ordner 'Für Import' enthaltene Ordner, die zu keinem für die Netzwerksynchronisierung zugewiesenen Ordner passen, werden automatisch ignoriert und vom Gerät gelöscht.
- Wenn der Benutzer die App während des Imports verlässt, läuft diese bis zu 10 Minuten im Hintergrund weiter. Die genaue Zeitspanne ist abhängig von der iOS-App-Verwaltung, die nicht der Kontrolle von Files Advanced unterliegt. Wenn die Files Advanced-App von iOS oder dem

Endbenutzer heruntergefahren wird, wird der Importvorgang beim nächsten Start der App dort fortgesetzt, wo er zuvor unterbrochen wurde.

- Nachdem die vorab geladenen Dateien und Ordner in die entsprechenden Synchronisierungsordner kopiert worden sind, führt die App eine OTA-Synchronisierung (Over-The-Air) durch. Während der Erstsynchronisierung betrachtet die App alle per Sideload in die App übertragenen Daten als aktuell, sofern die Serverversion der Datei dieselbe Dateigröße hat. Die Zeitstempel der Dateien müssen nicht übereinstimmen. Wenn die Dateigröße identisch ist, wird der Zeitstempel der lokalen Datei aktualisiert, sodass er mit der Serverversion übereinstimmt. Wenn die Dateigrößen abweichen, wird die betreffende Datei automatisch vom Server heruntergeladen und ausgetauscht. Dies führt in keinem Fall zur Erkennung eines Konflikts.
- In dem Richtlinienabschnitt der BlackBerry Dynamics-Applikation wird für Files Advanced (auf dem BlackBerry Control Server) eine Richtlinieneinstellung hinzugefügt, die die Sideload-Aktivierung regelt. Standardmäßig ist die Funktion deaktiviert. Bei Deaktivierung in der BlackBerry Dynamics-Richtlinie löscht die registrierte/aktivierte Files Advanced für BlackBerry-App bei jedem Hochfahren alle über die iTunes-Dateifreigabe in den Ordner 'Dokumente' kopierten Dateien und Ordner.

14.1.1.2 Für Android

Themen

Einführung

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

Folgende Komponenten gehören zur BlackBerry Dynamics Plattform:

- **Server von BlackBerry Control** – Eine serverbasierte Konsole, mit der das Unternehmen den Client-Zugriff auf für BlackBerry Dynamics aktivierte Apps ermöglichen, Richtliniensätze für Applikationsberechtigungen und die erlaubten Gerätetypen erstellen sowie den Zugriff auf Apps von BlackBerry Dynamics auf bestimmten Geräten widerrufen und die Apps auf diesen löschen kann.
- **BlackBerry Proxy-Server** – Dieser Dienst wird auf einem Server vor Ort installiert und bietet Netzwerkzugriff für BlackBerry Dynamics-Apps, die mit Servern vor Ort kommunizieren müssen, z. B. mit einem Files Advanced-Gateway-Server.
- **Files Advanced für BlackBerry Dynamics App** – Für BlackBerry Dynamics aktivierte Apps wie **Files Advanced für BlackBerry Dynamics** umfassen integrierte Dienste von BlackBerry Dynamics, mit denen die App entfernt über die BlackBerry Dynamics Plattform verwaltet werden kann. Ferner steht die App mit einem nach FIPS 140-2 zertifizierten lokalen verschlüsselten Sicherheitsspeicher und mit Sicherheitskommunikation von BlackBerry zur Verfügung.

Files Advanced für BlackBerry Dynamics erfordert Folgendes:

- **Files Advanced für BlackBerry Dynamics Client App** – Die im Apple App Store verfügbare Files Advanced für BlackBerry Dynamics Client-App http://www.grouplogic.com/web/megoodappstore ist speziell für die Einbindung in BlackBerry Dynamics konzipiert. Bei der ersten Installation und Ausführung der App Files Advanced für BlackBerry Dynamics auf einem Gerät, wird der Benutzer aufgefordert, die App in BlackBerry Dynamics zu aktivieren. Diese Aktivierung ist erforderlich, bevor der Benutzer mit der Registrierung der App auf dem Files Advanced-Server und dem Zugriff auf Dateien fortfahren kann.
- **Files Advanced Server** – Files Advanced für BlackBerry Dynamics verwendet dieselbe serverseitige Software wie die Standardversion von Files Advanced. Es sind keine Änderungen auf der Serverseite erforderlich, damit Files Advanced Server mit den für BlackBerry Dynamics aktivierten Files Advanced Clients arbeiten kann. So kann sichergestellt werden, dass alle Files Advanced Mobile Clients mit Zugriff auf Files Advanced-Dateien von BlackBerry Dynamics verwaltet werden.

Nachdem ein Files Advanced für BlackBerry Dynamics Client in BlackBerry Dynamics registriert ist, wird die gesamte Kommunikation mit den Gateway Servern über den sicheren Kommunikationskanal geleitet.

Files Advanced in BlackBerry Control anfordern und konfigurieren

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

Themen

Um Zugriff auf **Files Advanced für BlackBerry** anzufordern, besuchen Sie den BlackBerry-Marketplace (https://begood.good.com/marketplace.jspa https://begood.good.com/marketplace.jspa), und suchen Sie **Files Advanced für BlackBerry** in der Liste verfügbarer **BlackBerry Dynamics**-Apps.

Klicken Sie auf der Seite der Files Advanced für https://begood.good.com/gd-app-details.jspa?ID=248978 BlackBerry-App auf die Schaltfläche Start Trial', um eine Demoversion oder eine lizenzierte Version der App zu erhalten. https://begood.good.com/gd-app-details.jspa?ID=248978

Wenn Sie eine Demoversion der App anfordern, sollten Sie innerhalb weniger Minuten Zugriff darauf haben. Wenn Ihre Anforderung akzeptiert wurde, erhalten Sie von der BlackBerry-Website eine

Benachrichtigung, in der Sie darüber informiert werden, dass die **Files Advanced für BlackBerry**-App auf Ihrem BlackBerry Control-Server veröffentlicht wurde.

Hinweis: *Wenn Sie keinen Zugriff erhalten, wenden Sie sich an den Support von BlackBerry Dynamics.*

Melden Sie sich danach auf dem BlackBerry Control-Server an, und klicken Sie im Menü auf der linken Seite auf **Apps verwalten (Manage Apps)**. Files Advanced sollte jetzt in der Liste der Applikationen aufgeführt werden. Ist dies nicht der Fall, warten Sie ca. eine Viertelstunde ab und überprüfen Sie die Liste dann noch einmal. Diese Zeit sollte ausreichen, um die Änderung auf dem Server umzusetzen.

Damit Files Advanced über den BlackBerry Proxy Server auf Ihren Files Advanced Gateway Server zugreifen können, müssen Sie den Zugriff auf die Domain konfigurieren, auf der sich Ihre Files Advanced Gateway Server befinden. Dies erfolgt in der Good Control-Konsole auf der Seite **Client-Verbindungen**.

Zugriff von Ihrer Domäne gestatten

Diese Einstellung gestattet allen BlackBerry-Clients, sich mit allen Servern in den angegebenen Domänen zu verbinden. Wenn Sie dies nicht wünschen, richten Sie stattdessen **Zusätzliche Server (Additional Servers)**ein.

1. Öffnen Sie im linken Menü die Einstellungen für die **Client-Verbindungen**.
2. Erweitern Sie **Zulässige Domänen (Allowed Domains)**. Sofern **Alle Domänen zulassen (Allow all domains)** nicht aktiviert ist, drücken Sie auf das Plus-Symbol (+), und geben Sie den Namen Ihrer Domäne ein (z.B. meinefirma.com).
3. Klicken Sie auf **Übermitteln (Submit)**.

Ihre Domäne als Standard-Domäne für Verbindungen zuweisen

1. Erweitern Sie **Standard-Domänen (Default Domains)**.
2. Drücken Sie auf das Plus-Symbol (+), und geben Sie den Namen Ihrer Domäne ein.
3. Drücken Sie auf **Übermitteln (Submit)**.

Bestimmten Servern die Verbindung gestatten

Verwenden Sie anstelle der **Zulässige Domänen** diese Einstellung, wenn Sie möchten, dass Ihre Good-Clients sich nur mit diesen bestimmten Servern und nicht mit allen Servern in der Domäne verbinden.

1. Öffnen Sie im linken Menü die Einstellungen für die **Client-Verbindungen**.
2. Erweitern Sie **Zusätzliche Server (Additional Servers)**.
3. Drücken Sie auf das Plus-Symbol (+), und geben Sie den DNS-Namen und Port des Servers ein, für den Sie den Zugriff gestatten möchten. Wiederholen Sie diesen Schritt für alle Files Advanced Server, mit denen sich Ihre BlackBerry-Clients verbinden sollen.

BlackBerry Dynamics-Richtliniensätze und Files Advanced

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

Hinweis: *Wenn Sie im BlackBerry-Portal für den* ***Richtliniensatz*** *eines Benutzers FIPS aktivieren, kann die Files Advanced-App nicht über Drittanbieterzertifikate nach IP-Adresse auf Gateway-Server zugreifen.*

Dazu gehören diese Einstellungen:

- Kennwortanforderungen zum Sperren der Applikation
- Richtlinien zum Sperren des Bildschirms
- Schutz vor Datenverlust
- Zulässige Betriebssystemversionen und Hardwaremodelle
- Überprüfung der Verbindung
- Jailbreak/Root-Erkennung

Auswirkungen und Beschränkungen der Schutzfunktion gegen Datenlecks

Wenn **Schutzfunktion gegen Datenlecks** in einem Richtliniensatz aktiviert ist, ist die Files Advanced-App nicht in der Lage, die folgenden Aktionen durchzuführen:

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

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

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

Files Advanced Zugriff auf BlackBerry Dynamics-Benutzer oder -Gruppen gewähren

Bevor ein Benutzer seine Files Advanced-App in BlackBerry Dynamics registrieren kann, muss er die Files Advanced-Applikation zur Liste **Erlaubte Apps** seiner Benutzerkonten oder zu einer erlaubten **Applikationsgruppe**, der er angehört, hinzufügen. Darüber hinaus muss dem Benutzer ein eindeutiger **Zugriffsschlüssel** gesendet werden, der während des Registrierungsprozesses in die Files Advanced-App eingegeben werden muss.

WICHTIGER HINWEIS ZUR BEREITSTELLUNG: *Wenn Sie einzelnen Benutzern Zugriff auf BlackBerry Dynamics-Applikationen zuweisen, müssen Sie die bestimmten Versionsnummern der App auswählen, auf die Zugriff gewährt werden soll. Wenn Sie den Zugriff auf der Benutzerebene verwalten, müssen Sie bei der Veröffentlichung neuer Versionen von Files Advanced für BlackBerry die BlackBerryControl-Konfiguration des Benutzers aufrufen und die neue Version hinzufügen. Erst danach kann diese Version verwendet werden.*

*Es wird **dringend geraten**, den Zugriff auf BlackBerry Dynamics-Apps über die Funktion **Gruppen verwalten** in der Konsole von BlackBerry Control zu gestatten. Mit BlackBerry Control sind Sie in der Lage, einer Gruppe Zugriff auf ALLE Versionen einer App zu gewähren, damit auch zukünftige Versionen ohne Eingriff durch den IT-Administrator erlaubt werden.*

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

1. Wählen Sie im Menü auf der linken Seite der Konsole von BlackBerry Control **App-Gruppen (App Groups)** oder **Benutzer verwalten**.
2. Wählen Sie die Gruppe oder den Benutzer aus, der bzw. dem Sie Zugriff auf Files Advanced für BlackBerry gestatten möchten, und bearbeiten Sie diese.
3. Klicken Sie im Abschnitt **Apps** auf die Schaltfläche **Weitere hinzufügen**.
4. Wählen Sie **Files Advanced für BlackBerry** in der Liste verfügbarer Applikationen aus, und klicken Sie auf **OK**.

So erstellen Sie einen Zugriffsschlüssel, mit dem ein Benutzer seine **Files Advanced für BlackBerry**-App bei **BlackBerry** Dynamics registrieren kann:

1. Wählen Sie im Menü auf der linken Seite der Konsole von BlackBerry Control **Benutzer verwalten**.
2. Wählen Sie den Benutzer aus, für den Sie einen **Zugriffsschlüssel** erstellen möchten, und bearbeiten Sie diesen.
3. Drücken Sie auf der Registerkarte **Zugriffsschlüssel** auf **Zugriffsschlüssel**.

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

14.1.2 Microsoft Intune

Microsoft Intune stellt Funktionen zur Verwaltung von Mobilgeräten, Mobilapplikationen und PCs über die Cloud bereit. Mit Intune können Organisationen ihren Mitarbeitern den Zugriff auf Applikationen, Daten und Ressourcen des Unternehmens von praktisch jedem Ort und nahezu jedem Gerät aus ermöglichen, wobei die Sicherheit von Unternehmensinformationen gewahrt bleibt. Zum Registrieren von Mobilgeräten müssen Sie Intune als Autorität für Mobilgeräte festlegen und dann die Infrastruktur für die Unterstützung der Plattformen konfigurieren, die Sie verwalten möchten. Hierfür muss eine Vertrauensstellung mit dem Gerät eingerichtet werden.

Hinweis: *Diese Funktion wird nur vom Files Advanced iOS-Client ab Version 7.0.5 unterstützt.*

Hinweis: *Um eine* ***Geräterichtlinie*** *anzuwenden, muss* ***Files Advanced*** *über das* ***Microsoft Intune Company Portal*** *installiert werden, und* ***Per Intune verwaltete iOS-Clients erlauben und iOS-Clients mit 'Verwalteter iOS-App' erlauben*** *muss in den* ***Standardzugriffsbeschränkungen*** *von Files Advanced (****Mobiler Zugriff*** *->* ***Richtlinien*** *->* ***Standardzugriffsbeschränkungen****) oder für die Zugriffsbeschränkungen jedes Gateways aktiviert werden.*

Hinweis: *Um eine* ***Anwendungsrichtlinie*** *anzuwenden und damit Files Advanced von Intune verwaltet wird, muss die Option zum Auslösen der Registrierung für Intune Mobile-Application Management über den Files Advanced Server in* ***Mobiler Zugriff*** *->* ***Richtlinien*** *->* ***Server-Richtlinie*** *aktiviert werden.*

Themen

14.1.2.1 Erstellen einer Active Directory-Gruppe

1. Öffnen Sie das Microsoft Azure-Portal.
2. Klicken Sie auf **Alle Dienste**, geben Sie im Suchfeld **azure** ein, und wählen Sie **Azure Active Directory** aus.
3. Öffnen Sie **Gruppen**, wählen Sie **Neue Gruppe** aus, und geben Sie die erforderlichen Informationen ein.
4. Wählen Sie die gewünschten Mitglieder der Gruppe aus, und drücken Sie auf **Erstellen**.

14.1.2.2 Files Advanced-App in Intune hinzufügen

Wenn Sie eine Intune **Geräterichtlinie** verwenden möchten, sollte Files Advanced über das Intune Company Portal installiert werden.

Dazu müssen Sie zuerst die Files Advanced App zum Portal hinzufügen:

1. Öffnen Sie das Microsoft Azure-Portal.
2. Klicken Sie auf **Alle Dienste**, geben Sie im Suchfeld **Intune** ein, und wählen Sie **Microsoft Intune** aus.
3. Öffnen Sie im Intune-Portal **Mobile Apps**, und öffnen Sie **Apps**.
4. Drücken Sie **Hinzufügen**, und wählen Sie die Optionen für **App hinzufügen** aus.
   - Wählen Sie unter **App-Typ iOS** aus.
   - Klicken Sie auf **App Store durchsuchen**, und suchen Sie nach **Files Advanced**. Wählen Sie die App aus.
   - Klicken Sie auf **App-Informationen**, und nehmen Sie alle gewünschten Konfigurationsänderungen vor.
5. Aktivieren Sie die Option, um diese im Unternehmensportal als eine empfohlene App anzuzeigen, und drücken Sie auf **OK**, um den Vorgang zum Hinzufügen der App fertigzustellen.
6. Klicken Sie auf die App in der Liste, und wählen Sie **Zuweisungen** aus.
7. Wählen Sie die Benutzer oder Gruppen aus, denen Sie diese zuweisen möchten.

14.1.2.3 Erstellen einer Geräterichtlinie

1. Öffnen Sie das Microsoft Azure-Portal.
2. Klicken Sie auf **Alle Dienste**, geben Sie im Suchfeld **Intune** ein, und wählen Sie Microsoft Intune aus.
3. Öffnen Sie **Gerätekonfiguration** -> **Profile**, und wählen Sie **Profil erstellen** aus.
4. Geben Sie den Namen ein, wählen Sie **iOS** als die **Plattform** aus, und wählen Sie die Einschränkungen aus, die Sie auf das Gerät anwenden möchten.
5. Bei der Files Advanced App unterstützen wir nur die folgenden Einschränkungen:
   - **App Store, Dokumentanzeige, Gaming -> Anzeigen von Unternehmensdokumenten in nicht verwalteten Apps**. Wenn nicht verwaltete Apps nicht in den Listen **Öffnen in/Speichern unter** für verwaltete Apps angezeigt werden sollen, wählen Sie bei dieser Option **Blockieren** aus.
   - **App Store, Dokumentanzeige, Gaming -> Anzeigen von Nicht-Unternehmensdokumenten in Unternehmens-Apps**. Wenn verwaltete Apps nicht in den Listen **Öffnen in/Speichern unter** für nicht verwaltete Apps angezeigt werden sollen, wählen Sie bei dieser Option **Blockieren** aus.
6. Wenn die App zur Liste hinzugefügt wurde, tippen Sie auf die App, und wählen Sie **Zuweisungen** aus. Wählen Sie die Benutzer/Gruppen aus, denen Sie diese zuweisen möchten.

Um eine** Geräterichtlinie **auf eine App anzuwenden, muss die App von Ihrem Intune Company Portal heruntergeladen werden.

14.1.2.4 Erstellen einer App-Schutzrichtlinie

***Hinweis:** Diese Richtlinie dient auch als Ihre Mobile-App-Management-Richtlinie.*

1. Öffnen Sie das Microsoft Azure-Portal.
2. Klicken Sie auf **Alle Dienste**, geben Sie im Suchfeld **Intune** ein, und wählen Sie **Microsoft Intune** aus.
3. Öffnen Sie **Mobile Apps**, und öffnen Sie dann **App-Schutzrichtlinien**.
4. Wählen Sie **Richtlinie hinzufügen** aus, und geben Sie einen Namen für die Richtlinie ein. Wählen Sie **Files Advanced** als eine erforderliche App aus.
5. Tippen Sie auf **Einstellungen**, und wählen Sie die Schutzrichtlinien aus, die angewendet werden sollen.
6. Wenn die App zur Liste hinzugefügt wurde, tippen Sie auf die App, und wählen Sie **Zuweisungen** aus. Wählen Sie die Benutzer/Gruppen aus, denen Sie diese zuweisen möchten.

***Hinweis:** Wenn die Option, um der App zu erlauben, Daten an andere Apps zu übertragen/Daten von anderen Apps zu empfangen, auf per Richtlinie verwaltete Apps festgelegt ist, müssen Sie **App-Konfigurationsrichtlinien** mit dem **IntuneMAMUPN**-Schlüssel auf die per Intune verwaltete App und die Files Advanced App anwenden, damit **Files Advanced Document Provider Extension** in anderen Microsoft Intune Managed-Apps verwendet werden kann. Wenn Sie eine Richtlinie mit dem **IntuneMAMUPN**-Schlüssel haben, können die Optionen, um der App zu erlauben, Daten an andere Apps zu übertragen/Daten von anderen Apps zu empfangen, nicht verwendet werden.*

App-Schutzrichtlinie, die Dateien auf per Richtlinie verwaltete Apps einschränkt. Damit Files Advanced Document Provider Extension in anderen Microsoft Intune Managed-Apps verwendet werden kann, müssen Sie App-Konfigurationsrichtlinien mit dem IntuneMAMUPN-Schlüssel auf die per Intune verwaltete App und die Files Advanced-App anwenden. Wenn ein Gerät mit dem IntuneMAMUPN-Schlüssel jedoch als MDM-verwaltet gilt, ist die Einstellung in der App-Schutzrichtlinie, um der App zu erlauben, Daten an andere Apps zu übertragen, nicht mehr relevant, und die MDM-Konfigurationseinstellung zum Anzeigen von Unternehmensdokumenten in nicht verwalteten Apps wird verwendet. Stellen Sie sicher, dass Sie eine Geräterichtlinie anwenden, um Dateien ordnungsgemäß auf per Richtlinie verwaltete Apps einzuschränken.

Hinweis: *Um Dateien in Word (oder andere Microsoft-Apps) von Files Advanced aus zu öffnen, benötigen Sie eine separate Intune* ***App-Schutzrichtlinie*** *für die gewünschte Microsoft-Anwendung, und* ***Auf alle Typen anwenden*** *muss auf* ***JA*** *festgelegt sein.*

14.1.2.5 Erstellen von App-Konfigurationsrichtlinien

Um sich automatisch mit Intune-Anmeldeinformationen zu registrieren, müssen Sie eine **App-Konfigurationsrichtlinie** erstellen und Ihre eigene folgendermaßen ändern:

1. Öffnen Sie das Microsoft Azure-Portal.
2. Klicken Sie auf **Alle Dienste**, geben Sie im Suchfeld **Intune** ein, und wählen Sie **Microsoft Intune** aus.
3. Öffnen Sie **Mobile Apps**, und öffnen Sie dann **App-Konfigurationsrichtlinien**.
4. Drücken Sie auf **Hinzufügen**, und geben Sie einen Namen für die Richtlinie ein.
5. Wählen Sie **Verwaltete Geräte** als **Geräteregistrierungstyp** aus, wählen Sie **iOS** als **Plattform** aus, und wählen Sie die erforderliche App aus, auf die Sie diese Konfiguration anwenden möchten.
6. Bei den Einstellungen für die **Konfiguration** haben Sie zwei Optionen: **XML** oder **Konfigurations-Designer**.
   - Geben Sie für **XML** Folgendes ein:

```
<dict>
<key>IntuneMAMUPN</key>
<string>{{userprincipalname}}</string>
</dict>
```

   - Geben Sie für **Konfigurations-Designer** Folgendes ein:
     - **IntuneMAMUPN** für den **Konfigurationsschlüssel**.
     - **{{userprincipalname}}** für den **Konfigurationswert**.
     - Wählen Sie **Zeichenfolge** für den **Werttyp** aus.
7. Für eine automatische Registrierung mit Files Advanced-Anmeldeinformationen können Sie die folgenden Schlüssel in **XML** verwenden:

```
<dict>
<key>enrollmentServerName</key>
<string>192.168.1.10</string>
<key>enrollmentUserName</key>
<string>jprice</string>
<key>enrollmentPassword</key>
<string>password123</string>
<key>enrollmentAutoSubmit</key>
<string>Yes</string>
</dict>
```


8. Wenn die App zur Liste hinzugefügt wurde, tippen Sie auf die App, und wählen Sie **Zuweisungen** aus. Wählen Sie die Benutzer/Gruppen aus, denen Sie diese zuweisen möchten.

15 Neuerungen

Themen

15.1 Files Advanced Server

Hinweis: *Zahlen wie "[ASRV-2345, DE1013, US552]" beziehen sich auf das interne Änderungsnachverfolgungssystem von Acronis.*

In der aktuellen Version von Files Advanced ist Folgendes enthalten: ***Tomcat*** *Version: 7.0.82;* ***Java*** *Version: 8u144;* ***PostgreSQL*** *Version: 9.4*

Files Advanced unterstützt keine Versionen von Tomcat, Java und PostgreSQL, die neuer als die jedem Release beigefügten Versionen sind. Informationen zu einer bestimmten Version erhalten Sie vom Acronis Support.

Files Advanced 8.1.1 (Veröffentlicht: 26. Juli 2018)

VERBESSERUNGEN:

- Dateien können jetzt endgültig gelöscht werden, sodass sie nicht mehr wiederhergestellt werden können. Alle Löschvorgänge werden im Auditprotokoll aufgezeichnet.
- Verbesserte E-Mail-Kopfzeilen für Aktivierungen und Benachrichtigungen enthalten Angaben zum Absender, zur Absenderadresse und zur Antwortadresse. Durch diese Änderung werden weniger E-Mails vom Server des Client als Spam gekennzeichnet.
- Neu: Möglichkeit, einen Ordner mit einzelnen Dateien über 4 GB herunterzuladen.
- Neu: Erkennung für aktuelle Windows-BS-Versionen auf Geräteseite.

FEHLERBEHEBUNGEN:

- Mitgliedern von Freigaben werden in den Benachrichtigungs-E-Mails jetzt die Namen der Benutzer angezeigt, die Dateiänderungen vorgenommen haben, wenn sie über die Berechtigungen „Kann Mitglieder einsehen“ verfügen.
- Neu: Unterstützung für alte E-Mail-Vorlagenmethoden, die nach dem Upgrade auf 8.0 gefehlt haben.
- Namen der Windows Desktop Client-Binärdateien und -Services wurden in den neuen Produktnamen geändert.
- Das Umbenennen von Dateien/Ordnern im Stammverzeichnis einer synchronisierten Netzwerkfreigabe verursacht keine internen Serverfehler mehr.

Files Advanced 8.1 (Veröffentlicht: 14. März 2018)

Acronis Access Advanced wurde in Files Advanced umbenannt.

VERBESSERUNGEN:

- Eine neue Einstellung für Richtlinie für mobile Geräte regelt die maximale Dateigröße, die mobile Clients herunterladen dürfen. ASRV-5838
- Unterstützung, um Windows-Verknüpfungen (.lnk-Dateien) zu folgen, die auf Netzwerkfreigaben liegen. ASRV-5837
- Beim Löschen eines Benutzers werden jetzt auch seine Geräte von der Seite 'Geräte' entfernt. ASRV-5845
- Aktualisierung inklusive Java auf Version 8u162. ASRV-3410
- Gesteigerte LDAP-Leistung bei großen Bereitstellungen. ASRV-6012, ASRV-6011

BUG-FIXES:

- Problem behoben, bei dem beim Desktop Client ein Fehler auftritt, wenn während der Synchronisierung ein Ordnernamenkonflikt auftritt. ASRV-5768
- Externe Benutzer werden jetzt zur Bestätigung ihrer Konten korrekt weitergeleitet, bevor Sie auf freigegebene Links zugreifen können. ASRV-5304
- "**Administration verlassen**' wird Benutzern ohne Sync&Share-Zugriff nicht mehr angezeigt. ASRV-6062
- Ein Problem beim Exportieren der Geräte oder Einladungslisten wurde behoben. ASRV-5802

Acronis Access 8.0.1 (Veröffentlicht: 21. Dezember 2017)

Verbesserungen:

- Tomcat aktualisiert auf Version 7.0.82
- Java aktualisiert auf Version 8u144

Fehlerbehebungen:

- Gesteigerte Zuverlässigkeit beim Speichern von Änderungen in Dateien beim Bearbeiten mit Office Online
- Problem behoben, bei dem Drag & Drop bei großen Dateien nicht mehr funktionierte
- Problem behoben, bei dem die Entf-Taste beim Umbenennen einer Datei einen Dateilöschvorgang auslösen konnte
- Einige Probleme mit Kontextmenüelementen bei Mac- und PC-Desktop Sync-Clients behoben
- Problem behoben, bei dem das vom Admin beschränkte IP-Adressenbereichsformat einen Fehler verursachen konnte
- Verschiedene Fehlerbehebungen und Verbesserungen

Acronis Access 8.0 (Veröffentlicht: 21. September 2017)

Acronis Access 8.0 und neuer bietet keine Unterstützung mehr für Internet Explorer 8. Acronis Access 7.5 ist die letzte Version die Internet Explorer 8 unterstützt.

Verbesserungen:

- Unterstützung für eine optionale Microsoft Office Online-Integration für Dateiansicht und -bearbeitung mithilfe von **Office Online** über den Web-Client. Office Online unterstützt **DOCX**-,

XLSX- und **PPTX**-Dateien. **DOC**-, **XLS**- und **PPT**-Dateien werden ebenfalls unterstützt. Sie werden jedoch dazu aufgefordert, sie in das neue Format zu konvertieren, bevor Sie sie bearbeiten können. Bei lokalen Installationen ist für diese Funktion ein Office Online Server erforderlich. ASRV-357, ASRV-4714, ASRV-4664

- Neue Office-Dateien können nun im Web-Client erstellt und mit Office Online bearbeitet werden.
- Unterstützung für die Mehrfachauswahl von Elementen im Web-Client mithilfe von Kontrollkästchen für die Elementauswahl und Umschalt-, Befehls-/Strg-Tastaturoptionen. ASRV-4723, ASRV-353
- Unterordner von vorhandenen, freigegebenen Sync & Share-Ordnern können jetzt unabhängig voneinander für separate Zielgruppen freigegeben werden. ASRV-1635
- Unterordner von Sync & Share-Stammordnern können jetzt mit dem Desktop Client synchronisiert werden.
- Zusätzliche Einstellung für Richtlinie für mobile Geräte zur Initiierung und Vorgabe der Acronis Access iOS-App-Registrierung für Intune Mobile-Application Management. Dadurch kann in der Acronis Access iOS-App Intune MAM angewendet werden, ohne dass das mobile Gerät über Intune MDM verwaltet werden muss. ASRV-4510
- Bei der Installation von Upgrades werden Administratoren darüber informiert, wenn die erforderliche Zeit für das Upgrade durch obligatorische Datenbankmigrationen verlängert wird. ASRV-5269

Fehlerbehebungen:

- Verbesserung der Zuverlässigkeit des Desktop Sync Clients.
- Problems mit der Sortierung von Ordnern im Web-Client mit chinesischen Zeichen behoben. ASRV-4487
- Verschiedene Fehlerbehebungen im Hinblick auf Lokalisierung.

Acronis Access 7.5.4 (Veröffentlicht: 19. Mai 2017)

BUG-FIXES:

- Problem behoben, bei dem Dateien, die auf Ordnern freigegeben wurden, nicht für Nicht-Mitglieder sichtbar sind.
- Problem behoben, bei dem Links zum Download von Dateien unter Umständen nicht richtig funktionierten, wenn sie durch andere Mitglieder als dem Eigentümer eines freigegebenen Ordners freigegeben wurden.
- Problem behoben, durch das es beim Dateilöschen zu einem Fehler kommen konnte.

Acronis Access 7.5.3 (Veröffentlicht: 21. April 2017)

BUG-FIXES:

- Verschiedene Fehlerbehebungen und Verbesserungen
- Problem mit dem Desktop-Synchronisierungsclient unter Mac OS 10.9 wurde behoben

Acronis Access 7.5.2 (Veröffentlicht: 11. Februar 2017)

BUG-FIXES:

- Admin-Benutzer werden nun nicht mehr doppelt in der Webadministrator-Konsole angezeigt.
- Es wurde ein Problem behoben, bei dem eine Tomcat-Einstellung nach einem Upgrade in einen nicht unterstützten Wert umgewandelt werden konnte, was zu Serviceproblemen führte.

Acronis Access 7.5.1 (Veröffentlicht: 25. Januar 2017)

BUG-FIXES:

- Es wurde ein Problem behoben, bei dem das Suchfeld in der webbasierten Benutzeroberfläche bei der Verwendung der Farbschema-Option 'Benutzerdefiniert' falsch positioniert werden konnte.
- Ein Problem mit der Auslagerung auf der Webadministrator-Überwachungsprotokollseite wurde behoben.
- Ein 'interner Fehler', der beim Durchsuchen eines Sync & Share-Speichers mit abgelaufenen freigegebenen Ordnern auftreten konnte, wurde behoben.
- Die Protokollierung von Gateway-CURL-Verbindungsfehlern wurde von WARN zu DEBUG geändert.
- Es wurden Kompatibilitätsverbesserungen bei der Zwei-Faktor-Authentifizierung per SMS vorgenommen.

Acronis Access 7.5 (Veröffentlicht: 12. Januar 2017)

VERBESSERUNGEN:

- Wenn Sie ein Upgrade auf Acronis Access Advanced 7.5 oder höher von einer Version aus durchführen, die älter als Version 6.0 ist, sind für das Upgrade zusätzliche Schritte erforderlich. Kontaktieren Sie den Acronis Mobility-Support, um weitere Details zum Durchführen dieses Upgrades zu erhalten. ASRV-350
- Die Web- und Desktop Clients sind jetzt in spanischer Sprache verfügbar.
- Microsoft Azure Storage wird jetzt als Speicherort für das Sync & Share-Datei-Repository unterstützt. ASRV-3489
- Diese Version verfügt über eine Option zur Zwei-Faktor-Authentifizierung per SMS für die Web-Client-Anmeldung. Es sind Optionen verfügbar, die es erlauben, AD-Mobiltelefonnummern oder vom Benutzer angegebene Telefonnummern zu verwenden. 2-Faktorauthentifizierung kann bei jeder Anmeldung, in bestimmten Zeitintervallen oder nur für die Anmeldung von neuen Browsern angefordert werden. Für das Senden von SMS-Codes muss ein Konto mit dem Twilio SMS-Messagingdienst eingerichtet werden. ASRV-296
- Im Web-Client ist jetzt eine Datei- und Ordnersuche möglich. Es sind Optionen verfügbar, die das Filtern von Ergebnissen auf Basis des Dateityps, des Änderungsdatums der Datei und des Dateieigentümers erlauben. Windows File Server-Netzwerkdatenressourcen mit aktivierte Windows-Suche zeigen auch eine Option an, die das Suchen nach Dateiname oder Dateiinhalten ermöglicht. ASRV-1421
- Beim Suchen von Dateiinhalten in Windows File Server-Datenressourcen mit aktivierter Windows-Suche werden nun Übereinstimmungen angezeigt, die neben den Dateiinhalten auf

Windows Explorer-Tags basieren. Dies gilt für Suchvorgänge über den Web-Client oder über mobile Apps. ASRV-4221

- Der 'Administration'-Link zur Webadministrator-Konsole wurde von der obersten Ebene des Web-Clients ins 'Benutzermenü' verschoben. Benutzern mit Administrator-Berechtigung wird ein neues Benutzersymbol in der webbasierten Benutzeroberfläche angezeigt, das oben rechts ein Sternchen enthält. ASRV-4093
- Alle 'Good Dynamics'-Einstellungen in der Administrationskonsole wurden in 'Blackberry Dynamics' umbenannt. ASRV-4074
- Es wurde eine neue Option zur Beschränkung des mobilen Gatewayzugriffs hinzugefügt, um Verbindungen von der bevorstehenden Zugriffsbeschränkungsoption für die Blackberry Dynamics Android-App zuzulassen oder abzulehnen. ASRV-3795
- Es wurde eine neue optionale Richtlinie für Mobilgeräte zur Konfiguration des Anzeigeformats für die Suchergebnisse des integrierten PDF-Viewers hinzugefügt. ASRV-3791
- Es wurde eine neue optionale Richtlinie für Mobilgeräte hinzugefügt, die das Bearbeiten von kennwortgeschützten Office-Dateien zulässt oder ablehnt. Das Anzeigen und Bearbeiten von kennwortgeschützten Office-Dateien wird in den kommenden Versionen der mobilen Access Advanced-Clients unterstützt. Beim Bearbeiten einer kennwortgeschützten Datei wird das Kennwort beim Speichern entfernt. Aus diesem Grund wird diese Funktion standardmäßig deaktiviert, kann aber bei Bedarf aktiviert werden. ASRV-3729
- Der LibreOffice-Dienst, der in früheren Versionen für das Rendering von Office-Dateien zur Anzeige im Web-Client verwendet wurde, wurde durch eine neue interne Rendering-Bibliothek ersetzt, die eine verbesserte Leistung bietet. Dateien werden jetzt stufenweise gerendert, um einer reaktionsfähigere Anzeige zu ermöglichen. Der LibreOffice-Dienst wird automatisch deinstalliert, wenn Sie ein Upgrade auf Version 7.5 oder höher durchführen. ASRV-3867
- Es wurde eine Option hinzufügt, die das sofortige Löschen des Sync & Share-Inhalts eines Benutzers beim Löschen seines Kontos ermöglicht. ASRV-2848
- Der Besitzer eines Sync & Share-Ordners, der mit Ihnen geteilt wurde, wird jetzt im Web-Client angezeigt, wenn Sie die Maus über das Symbol für den geteilten Ordner bewegen. ASRV-3123
- Im Modus 'Gelöschte anzeigen' von Sync & Share wird ein gelöschter Ordner nicht mehr angezeigt, wenn der Server von allen Inhalten des Ordners bereinigt wurde. ASRV-16253
- Die integrierte Version von Java wurde auf Version 8u112 aktualisiert. ASRV-3409
- Es wurde eine Option hinzugefügt, mit der festgelegt wird, dass beim Hinzufügen und Entfernen von Benutzern aus einem über Sync & Share freigegebenen Ordner über die Acronis Access Server-API keine E-Mail-Benachrichtigung an betroffene Endbenutzer gesendet wird. ASRV-3888

BUG-FIXES:

- Es wurde ein Problem behoben, beim dem Netzwerkordner in der Web-Benutzeroberfläche als schreibgeschützt angezeigt werden konnte, obwohl der Benutzer eigentlich über Lese- und Schreibrechte verfügt. ASRV-4200

Acronis Access 7.4.1 (Veröffentlicht: 18. Oktober 2016)

- Verschiedene Fehlerbehebungen und Verbesserungen.

Acronis Access 7.4 (Veröffentlicht: 15. September 2016)

VERBESSERUNGEN:

- Die Fähigkeit, eine Datei, die mit Ihnen über einen Download-Link geteilt wurde, in einer Vorschau direkt auf der Zielseite der geteilten Datei anzuzeigen, wurde hinzugefügt. Optionen für Ansicht und Download werden nun angezeigt. Für diese Funktion ist die Aktivierung der Web-Client-Dokumentenvorschau auf dem Server erforderlich. ASRV-3051
- Eine neue Richtlinie für mobile Geräte zur Aktivierung oder Deaktivierung der Fähigkeit, leere PDF-Dateien für PDF-Anmerkungen zu erstellen, wurde hinzugefügt. ASRV-3620
- Eine neue Richtlinie für mobile Geräte, die bestimmt, wie URLs in Dokumenten von der Acronis Access App geöffnet werden, wurde hinzugefügt. Optionen beinhalten: 'Standard-Browser', 'Interner Browser', 'MobileIron Web@Work', 'Good Access', oder das Öffnen von URLs blockieren. ASRV-3452
- Eine neue Richtlinie für mobile Geräte zu Aktivierung oder Deaktivierung eines Datenimports von der Kamera-/Fotobibliothek wurde hinzugefügt. ASRV-2821
- Eine neue Richtlinie zur Aktivierung oder Deaktivierung der iOS-Document-Provider-Extension-Funktion auf der Client-App Acronis Access für iOS, Version 7.6, wurde hinzugefügt. Diese Einstellung ist standardmäßig deaktiviert, außer die geltende Richtlinie erlaubt das 'Öffnen von Acronis Access-Dateien in anderen Applikationen' ohne Whitelist- oder Blacklist-Beschränkungen. ASRV-2490
- Sync & Share Storage Quotas können nun auf Größen von unter 1 GB konfiguriert werden. ASRV-1439
- Die Schaltfläche 'Protokollordner öffnen' wurde im Dialog 'Einstellungen' im Mac- und Windows-Client zur Desktopsynchronisierung hinzugefügt. ASRV-2025
- Änderungsbenachrichtigungs-E-Mails für freigegebene Ordner enthalten nun einen Link, der direkt zum fraglichen Ordner weiterführt. Diese Änderung tritt in der E-Mail-Vorlage 'Benutzerbenachrichtigung' auf. Wenn Sie diese E-Mail-Vorlage angepasst haben, müssen diese Änderungen, falls gewünscht, manuell zu dieser Vorlage hinzugefügt werden. ASRV-1577
- Rendering der Spaltenbreite von in der Web-Vorschau angezeigten Excel-Dateien wurde verbessert. ASRV-3007
- Es gab eine Verbesserung der Zuverlässigkeit und Geschwindigkeit der Wiederherstellung nach Netzwerkunterbrechungen und aus dem Ruhezustand des Mac-Clients zur Desktopsynchronisierung. ASRV-3582, ASRV-3353, ASRV-139
- Aktualisierung inklusive Tomcat auf Version 7.0.70.
- Aktualisierung inklusive Java auf Version 8u92.

BUG-FIXES:

- Das Problem, dass Synch-&-Share-Daten eines gelöschten Benutzers nicht neu zugewiesen werden können, wurde gelöst. ASRV-3149
- Das Problem, dass mehrere Könfliktlösungsdateien nicht erstellt werden konnten, wenn Office-Dateien geöffnet sind und auf mehreren Clients gespeichert werden, wurde gelöst. ASRV-3024

Acronis Access 7.3.1 (Veröffentlicht: 20. Juni 2016)

VERBESSERUNGEN:

- Es wurde eine neue mobile Einstellung für die 'Applikationsrichtlinie' hinzugefügt, mit der die mit Version 7.6.0 der Acronis Access iOS-App veröffentlichte Funktion iOS Document Provider Extension aktiviert oder deaktiviert werden kann. Auf einem Server, für den ein Upgrade durchgeführt wurde, wird diese Richtlinieneinstellung standardmäßig aktiviert, wenn die Richtlinie 'Öffnen von Acronis Access-Dateien in anderen Applikationen' aktiviert ist und keine Blacklist/Whitelist für Apps verwendet wird. Auf einem Server, für den ein Upgrade durchgeführt wurde, wird die Richtlinieneinstellung deaktiviert, wenn eine Blacklist/Whitelist für Apps verwendet wird oder die Richtlinie 'Öffnen von Acronis Access-Dateien in anderen Applikationen' deaktiviert ist. ASRV-2490
- Es wurde eine neue mobile 'Sync-Richtlinieneinstellung' hinzugefügt, mit der verhindert werden kann, dass Mobilgeräte automatisch gesperrt werden, wenn die Acronis Access App-Dateien synchronisiert. Diese Einstellung ist standardmäßig **ausgeschaltet** und wird aktuell von Acronis Access für iOS ab Version 7.6.0 unterstützt. Unterstützung für Android und Windows Mobile wird in einer zukünftigen App-Version hinzugefügt. ASRV-2988
- Im Überwachungsprotokoll wurde eine neue Option hinzugefügt – Sie können nun wählen, ob auf den Zeitstempeln der exportierten Überwachungsprotokolle die lokale oder die UTC-Zeit angegeben werden soll. ASRV-3096
- Es wurden zusätzliche 'Auto-Sync-Intervall'-Optionen zur mobilen 'Sync-Richtlinie' hinzugefügt. Diese neuen Optionen sind 8, 12, 24 und 48 Stunden. Diese Einstellung wird derzeit von Acronis Access für iOS ab Version 7.6.0 unterstützt. Unterstützung für Android und Windows Mobile wird in einer zukünftigen App-Version hinzugefügt. ASRV-3130
- Es wurde eine neue Richtlinieneinstellung hinzugefügt, mit der die Berichterstattung über App-Abstürze an Acronis über die Fabric-Berichtsbibliothek aktiviert oder deaktiviert werden kann. Diese Berichterstattung ist standardmäßig deaktiviert und kann nur aktiviert werden, wenn Sie sich mit der serverseitigen Richtlinie angemeldet haben. Wir empfehlen, diese Einstellung zu aktivieren. Mit diesen Berichten kann Acronis die Access Apps verbessern, und sie werden nur versandt, wenn die App abstürzt. Sie enthalten keine privaten oder persönlich identifizierende Informationen. Die Berichtsfunktion und die Richtlinieneinstellung gelten nur für Acronis Access für Android ab Version 7.0.0. Unterstützung für iOS und Windows Mobile wird in einer zukünftigen App-Version hinzugefügt. ASRV-3138
- Acronis Access wird nicht von den Einstellungen **Kompatibilitätsmodus** für **Internet Explorer** beeinflusst. Das Administrationsportal und die Web-Benutzeroberfläche funktionieren wie erwartet. ASRV-3194

BUG-FIXES:

- Es wurde ein Fehler behoben, bei dem ein Acronis Access iOS-Client, der für die Verwendung der Einzelanmeldung über Kerberos konfiguriert wurde, den Benutzer unnötigerweise zur Eingabe eines Kennwortes aufforderte. ASRV-3111

Acronis Access 7.3 (Veröffentlicht: 5. Mai 2016)

VERBESSERUNGEN:

- Support für die italienische Lokalisierung von Access Advanced Server wurde hinzugefügt.

- Eine Option wurde hinzugefügt, um Acronis Storage als Speicherplatz für Ihr Sync & Share 'Datei-Repository' zu verwenden. ASRV-1519
- Optionen wurden hinzugefügt, um Swift S3, Ceph S3 und 'sonstigen S3-kompatiblen Massenspeicher' als Speicherplatz für Ihr Sync & Share 'Datei-Repository' zu verwenden. ASRV-2774
- ACRONIS ACCESS kann jetzt in SharePoint-Netzwerkdatenquellen SharePoint-gefolgte Websites anzeigen. Sie werden in dem Ordner 'Gefolgte Websites' im Stammverzeichnis der Datenquelle angezeigt. Benutzer können von SharePoints Web Client aus Websites 'folgen'. Diese Funktion ist standardmäßig deaktiviert und kann unter den Einstellungen einer SharePoint-Datenquelle im Webadministrator von ACRONIS ACCESS aktiviert werden. ASRV-2423
- Im Sync & Share-Speicher haben Benutzer jetzt die Option, gelöschte Ordner sowie all ihre Inhalte in einem einzigen Vorgang wiederherzustellen. Außerdem wird die Navigation zu einem gelöschten Ordner unterstützt, um nach einer bestimmten gelöschten Datei zu suchen und diese wiederherzustellen. ASRV-451
- Die Desktop Clients von Windows und Mac erlauben jetzt die Synchronisation von Dateien, deren Dateipfad länger als 260 Zeichen ist. Auf Dateien mit einem längeren Pfad als diesem kann möglicherweise nicht über Windows Explorer zugegriffen werden. ASRV-439
- Der Desktop Sync Client vergleicht nun die Dateiinhalte von serverseitigen und Desktop-Dateien, damit keine unveränderten Dateien hoch- oder heruntergeladen werden, selbst wenn sich das Bearbeitungsdatum unterscheidet. Wenn ein Benutzer eine identische Datei hochlädt oder der Desktop Sync Client deinstalliert und später neu installiert wird, um denselben lokalen Sync-Ordner zu verwenden, werden bestehende Dateien ohne weiteren Upload oder Download verglichen und wiederverwendet. Über Acronis Access Mobile oder Web Clients hochgeladene Sync & Share-Dateien werden jetzt mit bestehenden serverseitigen Dateien verglichen, um unnötige neue Versionen zu vermeiden, wenn hochgeladene Dateien mit bestehenden Dateien übereinstimmen. ASRV-2734
- Die standardmäßigen TCP-/IP-Ports, die bei neuen Installationen von Acronis Access Advanced verwendet werden, wurden geändert. Der Acronis Access Web Client/Administratordienst wird jetzt standardmäßig auf Port 443 installiert. Der Acronis Access Gateway-Dienst wird jetzt standardmäßig auf Port 3000 installiert. Bei der Installation von Aktualisierungen für bestehende Acronis Access Advanced Server wird die aktuelle Portkonfiguration beibehalten. ASRV-2810-
- Die URLs über Sync & Share freigegebener Dateien wurden zu einem kürzeren Format vereinfacht. ASRV-1157
- Ein Benutzer erhält keine Sync & Share E-Mail-Benachrichtigungen mehr über von ihm selbst vorgenommene Handlungen (herunterladen, hochladen, Abonnement kündigen usw.). ASRV-39
- Der Einstellungen-Seite des Webadministrators in der Webvorschau wurde eine neue Option hinzugefügt, die eine Web Client-Vorschau nur solcher Dateien ermöglicht, die kein serverseitiges Rendering erfordern. Ist diese Option aktiviert, kann im Web Client keine Vorschau von Microsoft Office-Dateien angezeigt werden. ASRV-2644
- Die Richtlinieneinstellung 'Zugriff auf File Server, NAS und SharePoint über Web Client zulassen' für mobilen Zugriff ist nun bei neuen Installationen von Acronis Access Advanced und neu erstellten Richtlinien für mobilen Zugriff standardmäßig aktiviert. ASRV-2818
- Auf der Seite 'E-Mail-Vorlagen' wurde eine neue Option hinzugefügt, um bei E-Mail-Inhalten den konfigurierten 'Servernamen' für die product_name-Variable zu verwenden. ASRV-1942

BUG-FIXES:

- Ein Problem wurde behoben, bei dem die Größe des Sync-Ordners für bestimmte Netzwerkdatenquellen möglicherweise als Null angezeigt wurde, wenn im Web Client ein Sync-Ordner hinzugefügt wurde. ASRV-2473
- Ein Problem wurde behoben, bei dem die Verarbeitung einer großen Menge von Datenbankelementen beim Hochfahren des Acronis Access Gateway-Dienstes eine Zeitüberschreitung verursachen konnte. ASRV-2400
- Freie externe Benutzer werden jetzt im Dialogfeld 'Mitglieder' des Sync & Share-Ordners mit einem 'Gast'-Symbol neben ihrem Namen angezeigt. ASRV-1940
- Ein Problem wurde behoben, bei dem in der Web-Vorschau geöffnete Excel-Dateien Links im Dateiinhalt möglicherweise nicht richtig anzeigten. ASRV-2798
- Ein Problem wurde behoben, bei dem Pfade zum Datei-Repository nicht funktionierten, wenn diese chinesische Schriftzeichen enthielten. ASRV-2810

Acronis Access 7.2.3 (Veröffentlicht: 29. Februar 2016)

VERBESSERUNGEN:

- Es wurden Optionen für Richtlinien mobiler Clients hinzugefügt, um die Ansichtseinstellung im neuen und verbesserten Anzeige und -Anmerkungstool für PDFs zu konfigurieren, das zur Acronis Access iOS-App (Version 7.5) hinzugefügt wurde. ASRV-2103

BUG-FIXES:

- Synchronisierungsproblem behoben, das beim Löschen oder Verschieben eines Ordners im Sync & Share-Desktopclientordner und anschließenden sofortigen Ersetzen durch einen neuen Ordner mit demselben Namen auftrat. ASRV-1706

Files Advanced 7.2.2 (Veröffentlicht: 2. Februar 2016)

VERBESSERUNGEN:

- EMC Documentum wird nun von Files Advanced als Datenquelle unterstützt. Files Advanced-Benutzer stellen über das CMIS-Protokoll eine Verbindung zu Documentum her. Documentum wird nun in den Datenquelltyp-Optionen angezeigt, wenn Sie eine Netzwerk-Datenquelle konfigurieren. ASRV-1012
- Neue Einstellung zur Beschränkung des Gatewayzugriffs hinzugefügt, die die Beschränkung des mobilen Zugriffs auf mit Microsoft Intune verwaltete iOS-Clients ermöglicht. Diese Clients können beim Upgrade von vorherigen Versionen von Acronis Access standardmäßig eine Verbindung herstellen. Sie können in den Gatewayserver-Einstellungen für die Zugriffsbeschränkungen deaktiviert werden. ASRV-1686
- Neue Option für eine Richtlinie für das Management mobiler Clients hinzugefügt, die Benutzern nur die Erstellung von 1-Weg-Sync-Ordnern ermöglicht. ASRV-1846
- Neue Option für eine Richtlinie für das Management mobiler Clients hinzugefügt, die den Sync-Ordnertyp (1-Weg oder 2-Weg) konfiguriert, der standardmäßig im mobilen Client während der Sync-Ordner-Erstellung ausgewählt wird. ASRV-1846
- Textdateien werden nun von der Web Client-Vorschau als reiner Text gerendert, statt sie in PDFs zu konvertieren. ASRV-1855

- Das Zeitlimit für das Rendern der Webvorschaudatei wurde auf 120 Sekunden erhöht, um größere Dateien verarbeiten zu können. ASRV-1868
- Webvorschau-Unterstützung für .rtf-, .ini-, .log-, .csv-, .ico-, .jpe- und Open Office-Dateien (.ods, .odt und .odp) hinzugefügt. ASRV-1852

Fehlerbehebungen:

- Schnellerer Zugriff auf SharePoint-Datenquellen, wenn der Microsoft Online-Anmeldeservice nicht durch den Zugriffsserver erreichbar ist. ASRV-374
- Schnelleres Laden von PDF-Dateien innerhalb der Web Client-Vorschau im Internet Explorer 11.
- Problem behoben, bei dem für abgelaufene gemeinsam genutzte Dateiverknüpfungen unnötigerweise und mehrfach Überwachungsprotokolle erstellt wurden. ASRV-1737
- Problem behoben, bei dem der Benutzer, der eine Datei oder einen Ordner gelöscht hat, in Änderungsbenachrichtigungen für gemeinsam genutzte Ordner nicht angegeben wurde. Diese Änderung tritt in der Vorlage "Benutzerbenachrichtigung" auf. Kunden mit benutzerdefinierten E-Mail-Vorlagen müssen diese Änderungen bei Bedarf manuell zu den benutzerdefinierten Vorlagen hinzufügen. ASRV-1964
- Problem behoben, bei dem das Alfresco-Dateiänderungsdatum nicht mit einem anderen Zugriffsserver-Änderungsdatum übereinstimmte. ASRV-1586
- Problem behoben, bei dem fälschlicherweise Konfliktlösungsdateien bei der Synchronisierung von Netzwerkknotendateien erstellt wurden. ASRV-2141
- Problem behoben, bei dem die Web Client-Vorschau keine Office-Dateien rendern und anzeigen konnte, wenn der DNS-Name des Zugriffsservers vom internen DNS nicht aufgelöst werden konnte. ASRV-1887
- Problem beim Aktualisieren der Überwachungsprotokollseite in IE11 behoben. ASRV-1624

Acronis Access 7.2.1 (Veröffentlicht: 10. Dezember 2015)

VERBESSERUNGEN:

- Verbesserte E-Mail-Adressvalidierung während der Testaktivierung. ASRV-2037

BUG-FIXES:

- Es wurde ein Fehler behoben, bei dem durch die Einzelanmeldung die Synchronisierungsfunktion des Desktop Client deaktiviert wurde.

Acronis Access 7.2 (Veröffentlicht: 17. November 2015)

VERBESSERUNGEN:

- Es ist nun möglich, Office-, PDF-, Text- sowie Bilddateien direkt im Acronis Access Webbrowser-Client anzuzeigen – ein Download ist nicht erforderlich. Diese Funktion wird nach einem Upgrade standardmäßig aktiviert und kann im neuen Abschnitt 'Webvorschau' in den allgemeinen Einstellungen des Servers konfiguriert werden.
- Es ist nun möglich, über das CMIS-Protokoll Zugriff auf die Datenquellen des Content Management-Systems zu gewähren. Acronis Access umfasst nun eine unterstützte Einstellung für

Datenquellen für Alfresco und eine 'allgemeine CMIS'-Option. Unterstützung für Dokumente wird in Kürze in einem späteren Release hinzugefügt. [ASRV-1012]

- Die Seite 'Mobilen Client herunterladen' mit den Einzelheiten zu den verfügbaren mobilen Apps von Acronis Access wurde zum Webbenutzermenü hinzugefügt. [ASRV-1463]
- Beim Teilen von Download-Links für Sync & Share-Dateien können Sie nun den Zugriff auf die Benutzer beschränken, denen die Links durch den Access Server per E-Mail gesendet werden. [ASRV-330]
- Ein neuer Dialog mit Linkeigenschaften ermöglicht die Anzeige der Link-URL, der für die Freigabe ausgewählten Benutzer, der Zugriffsbeschränkungen und der Einstellungen für den Ablauf vorhandener Download-Links für die Freigabe. Sie können die Freigabeeinstellungen in diesem Dialog ändern. [ASRV-1011]
- Neue externe Benutzer, die zu Sync & Share-Dateien und -Ordnern eingeladen wurden, müssen nun Ihr Acronis Access-Konto über einen per E-Mail gesendeten Aktivierungslink aktivieren, um Zugriff auf ihr Konto zu erhalten. [ASRV-1184]
- Wenn Benutzer des Acronis Access-Webclients zur Synchronisierung eines gerade geteilten Ordners aufgefordert werden, werden sie nun darüber informiert, falls kein Client zur Desktopsynchronisierung registriert ist. [ASRV-1509]
- Mobile Acronis Access-Clients können nun über ein Zertifikat oder eine Kerberos-Authentifizierung auf Sync & Share-Datenquellen zugreifen. [ASRV-466]
- Die neu hinzugefügte Gateway Server-Option 'Zugriffsbeschränkungen' ermöglicht es, Verbindungen von Acronis Access iOS-Client-Apps zuzulassen oder abzulehnen, die von Microsoft Intune verwaltet werden. [ASRV-312]
- Die neu hinzugefügte Gateway Server-Option 'Zugriffsbeschränkungen' ermöglicht es, Verbindungen von Acronis Access iOS-Client-Apps zuzulassen oder abzulehnen, die durch die Funktion 'Verwaltete iOS-App' verwaltet werden. [ASRV-1026]
- Der Zugriff auf die Acronis Access-Verwaltungskonsole kann nun auf bestimmte IP-Adressen bzw. -Bereiche beschränkt werden. [ASRV-1183]
- Verbesserte Leistung beim Laden der Seite für die Benutzeranmeldung. [ASRV-1209]
- Verbesserte Suchleistung bei der automatischen Vervollständigung von E-Mails. [ASRV-1468]
- Der Testzeitraum für den Acronis Access-Server beträgt nun 30 Tage. [ASRV-1228]
- Die unter 'Alternative Adresse für Access Server-Verbindungen verwenden' neu hinzugefügte Konfigurationsoption für Gateways 'Cluster-Gruppe' wird angewandt, wenn der Acronis Access-Webserver eine Verbindung zur Cluster-Gruppe über eine andere Netzwerkadresse herstellen muss als die, die für mobile Clients verwendet wird. [ASRV-243]
- Acronis Access behält nun bei Upgrades die benutzerdefinierten Tomcat-Einstellungen für temporäre Verzeichnisse bei. [ASRV-378]
- Unterstützung für TLSv1.2 hinzugefügt. [ASRV-1281]
- PostgreSQL auf Version 9.4.4-3 aktualisiert. [ASRV-379]
- Java auf Version 8u60 aktualisiert. [ASRV-1327]

BUG-FIXES:

- Problem behoben, bei dem die Anmeldung von Desktop Client-Benutzern fehlschlägt, wenn für den Access Server in Bezug auf Desktop Clients die Konfiguration 'Herkömmlichen Polling-Modus erzwingen' festgelegt ist. [ASRV-278]
- Problem mit der unbeaufsichtigten Installation des Windows-Desktop Clients von Acronis Access behoben. [ASRV-1192]

- Problem behoben, bei dem während der Installation des Windows-Desktop Clients von Acronis Access ein Fehler auftritt, wenn der Registrierungsschlüssel für den Autorun-Mechanismus von Windows nicht gefunden wurde. [ASRV-1496]
- Problem behoben, bei dem temporäre Dateien nicht vom Server gelöscht werden konnten, wenn Uploads von Webclient-Dateien in Netzwerkordner abgebrochen werden, bevor diese abgeschlossen sind. [ASRV-1516]
- Problem behoben, bei dem das benutzerdefinierte Dienst-Konto, mit dem der Gateway Server-Dienst von Acronis Access ausgeführt wird, als 'lokales Systemkonto' wiederhergestellt wird, nachdem die Einstellungen im Konfigurationsdienstprogramm von Acronis Access geändert wurden. [ASRV-1503]
- Problem behoben, bei dem die Einzelanmeldung fehlschlägt, wenn die impliziten und expliziten Benutzerprinzipalnamen (User Principle Names, UPN) eines Benutzers nicht übereinstimmen. [ASRV-1497]
- Problem behoben, bei dem die Benutzeroberfläche des Acronis Access-Webclients bei neueren Versionen des Internet Explorers zurück in den IE8-Modus versetzt wird, wenn der 'Kompatibilitätsmodus' aktiviert ist. [ASRV-1346]
- Problem behoben, bei dem die automatische Aktualisierung des Windows-Desktop-Synchronisierungsclients von Acronis Access fehlschlägt, wenn als Spracheinstellung für Windows 'Französisch' festgelegt ist. [ASRV-1229]
- Problem behoben, bei dem der Windows-Desktop-Synchronisierungsclient von Acronis Access aufgrund einer Inkompatibilität bei der Anzeige von Benachrichtigungen fehlschlägt, wenn der Bildschirmschoner der Fotogalerie in Windows 10 aktiviert ist. [ASRV-111]
- Problem behoben, bei dem ein Webseitenfehler auftritt, wenn als Ablaufdatum für den Download-Link zu einer freigegebenen Datei ein Wert über 999999 Tage festgelegt ist. [ASRV-1219]
- Problem behoben, bei dem benutzerdefinierte Tomcat-Einstellungen für web.xml für die Einzelanmeldung nicht beibehalten werden, wenn der Acronis Access-Server aktualisiert wird. [ASRV-1059]
- Problem behoben, bei dem Netzwerk-Basisordner mit zahlreichen Elementen gegenüber mobilen Benutzern ohne Inhalte angezeigt werden. [ASRV-1054]
- Problem behoben, bei dem die Ausführung des Windows-Desktop Clients von Acronis Access während des Herunterladens einer Datei unterbrochen wird, wenn der Client angehalten oder der Computer während des Download-Vorgangs neu gestartet wird. [ASRV-1546]

Acronis Access 7.1.2 (Veröffentlicht: 4. August 2015)

VERBESSERUNGEN

- Benutzer werden nun in der Weboberfläche benachrichtigt, wenn ihre Sitzungen in Kürze ablaufen. Sie haben dann die Möglichkeit, sie zu verlängern. Tun sie das nicht, werden sie automatisch abgemeldet. US3869, DE14304
- Sync & Share-Dateien, die gelöscht werden und aus dem Repository entfernt wurden, werden nicht mehr angezeigt, wenn 'gelöschte anzeigen' aktiviert ist. US10696
- Es ist nun eine Einstellung zum Filtern der Dateilinks verfügbar, die auf der Webseite 'Links' angezeigt werden. US10812
- Benutzer können nun die Tage bis zum Ablauf eines Links im Dialogfeld mit den Details zu Links ändern. US10820

- Benutzer können nun den öffentlichen oder privaten Status von Dateilinks im Dialogfeld mit den Details zu Links ändern. US10821
- Benutzer können nun die eintägige Download-Einstellung für einen Link im Dialogfeld mit den Details zu Links ändern. Beachten Sie, dass bei Konvertierung eines Links zur mehrfachen Nutzung in einen Link für einen einmaligen Download nur ein zusätzlicher Download dieser Datei möglich ist und nicht ein Download pro Benutzer, an den dieser verteilt wurde. US10822
- Wird ein Link zur mehrfachen Nutzung an mehrere Benutzer verteilt, erhält jeder Benutzer denselben Dateilink und nicht einen eindeutigen Link pro Benutzer. Mit dieser Änderung sollte die Usability der Dialogfelder mit verteilten Links verbessert werden.
- Die Access Server-API beinhaltet nun eine Option zum Löschen des gesamten Inhalts mit der Löschung eines Benutzers. US10644
- Die Symbole für mobile Richtlinien wurden aktualisiert, um die in der aktuellsten Android-Client-App unterstützten Funktionen abzubilden.

FEHLERBEHEBUNGEN

- Datei-Links können nun mit einem Ablaufdatum verteilt werden, wenn dies von den 'Freigabebeschränkungen' von Access Server unterstützt wird. DE12851, DE13461
- Hat ein Benutzer auf einen Ordner keinen Zugriff mehr, werden aus diesem Ordner freigegebene Datei-Links nicht mehr auf der Seite mit freigegebenen Links angezeigt. DE14574
- Wird eine Datei vom ursprünglichen Speicherort verschoben, werden alle freigegebenen Links für diese Datei automatisch widerrufen. DE14610
- Für Benutzer, die Schreibzugriff verlieren und somit andere Benutzer für den Zugriff auf eine Freigabe einladen können, werden alle Dateilinks, die sie in diesem Ordner freigegeben haben, widerrufen.DE14615, DE14623
- Mit einem Dateilink werden keine Downloads mehr unterstützt, wenn der Benutzer, der den Dateilink freigegeben hat, keinen Zugriff mehr auf die Datei hat. Das kann der Fall sein, wenn 'Benutzer A' einen Link zu einer Datei in einem freigegebenen Ordner freigegeben hat, der 'Benutzer B' gehört, und 'Benutzer B' zu einem späteren Zeitpunkt 'Benutzer A' als Mitglied dieses freigegebenen Ordners entfernt. DE14560
- Ein Benutzer erhält keine E-Mail mehr, dass er keinen Zugriff mehr auf eine Freigabe hat, wenn er diese selbst abbestellt hat. US10770
- Stellt ein Benutzer eine Verbindung zum Download eines mit Access freigegebenen Dateilinks her, für den eine Anmeldung erforderlich ist, und wird SSO für die Authentifizierung verwendet, wird der Benutzer nach der Authentifizierung auf die richtige Seite weitergeleitet. DE14539
- Der SSO-Anmeldelink wird auf iOS-Geräten und Windows-Phones nicht mehr angezeigt.DE14554
- SharePoint-Unterpfade werden nun richtig aufgelöst, wenn sie im Webclient hinzugefügt werden. DE14423
- In der linken Seitenleiste kann nun ein Bildlauf durchgeführt werden, wenn ausreichend Netzwerkdatenquellen dafür vorhanden sind, die das notwendig machen. DE14429
- Verbesserter Textumbruch in Fußzeilen in Standard-E-Mail-Vorlagen. DE14436
- Selbst bereitgestellte Ordner können nun erfolgreich von mobilen Clients gelöscht werden. DE14517
- Verbesserter Textumbruch in koreanischer Sprache für Internet Explorer und Firefox. DE14522
- Es wurde ein Authentifizierungsproblem behoben, das bewirkte, dass sich Benutzer ohne UPN (Benutzerprinzipalname) vom mobilen Client aus nicht authentifizieren konnten. DE14624

- Es wurde ein Problem behoben, bei dem möglicherweise ein Fehler aufgetreten ist, wenn Benutzer auf über einen Link freigegebene Dateien zugriffen und der Dateiname ein einfaches Anführungszeichen enthielt.DE14633
- Es steht eine neue Einstellung zur Verfügung, mit der die Adresse angegeben wird, die Access Server für die Kontaktaufnahme von Access Gateway-Cluster-Gruppen verwenden soll. Dieser Wert ist standardmäßig identisch mit der Adresse für Client-Verbindungen. DE14636
- Optimierte Speichernutzung auf dem Gateway Server beim Upload von mehreren tausend Dateien. DE14589
- Der Desktop Client authentifiziert sich automatisch bei Access Server bei Verwendung von SSO und bei der Synchronisierung des Netzwerkinhalts, wenn das Kerberos-Ticket abläuft. US10900

Acronis Access 7.1.1 (Veröffentlicht: 8. Juli 2015)

FEHLERBEHEBUNGEN

- Es wurde ein Problem behoben, bei dem einige Menüpunkt auf Mac-Desktop Clients für einige Sprachen nicht richtig lokalisiert waren.
- Es wurde ein selten auftretendes Problem behoben, bei dem ein erfolgreiches Upgrade von Access Server von älteren Versionen verhindert wurde.
- Bei Auswahl einer mit einem Link freigegebenen Datei in der Weboberfläche wird keine Option **Benachrichtigungen** mehr im rechten Menü angezeigt. Diese Option wird nicht auf über Links freigegebene Dateien angewendet.
- Es wurde ein Problem behoben, bei dem sich mit SSO authentifizierende Clients nach Ablauf ihres Kerberos-Tickets keine Netzwerkknoten durchsuchen konnten.

Acronis Access 7.1

VERBESSERUNGEN

- Acronis Access unterstützt jetzt integrierte Desktop-Authentifizierung (Single Sign-On) für den Web-Client und den Windows-Desktop Client. Ist die Einzelanmeldung (Single Sign-On) aktiviert, müssen Benutzer, die sich bereits bei der Anmeldung am Computer für die Domäne authentifiziert haben, ihren Benutzernamen und ihr Kennwort nicht erneut eingeben, um sich bei der Anmeldung an der Weboberfläche oder am Windows-Desktop Client zu authentifizieren. Die Unterstützung dieser Funktion für den Mac Desktop Sync Client wird ab dem nächsten Update zur Verfügung stehen. Für diese Funktion ist eine zusätzliche Konfiguration erforderlich. Weitere Informationen dazu finden Sie im Artikel Einzelanmeldung (Single Sign-On) konfigurieren (S. 214). [US10595]
- Es wurde eine Option hinzugefügt, mit der Benutzer Links zum Datei-Download weiterleiten können, die nach einem Download ablaufen. [US7572]
- Benutzer können jetzt festlegen, dass freigegebene Sync & Share-Ordner ablaufen. Nach dem Ablaufdatum haben die Mitglieder der Freigabe keinen Zugriff mehr auf den freigegebenen Ordner. [US6314, US8531]
- Es stehen neue Administrationsoptionen zur Beschränkung der Dateigröße und der Dateitypen für den Upload in Sync & Share zur Verfügung. Administratoren können diese Grenzwerte aktivieren und die maximale Dateigröße sowie die unzulässigen Dateitypen auf der Seite Sync & Share => Freigabebeschränkungen der Webadministration angeben. [US10587]
- Es steht eine neue '**Links**'-Seite zur Verfügung, auf der alle Sync & Share-Dateien aufgeführt werden, die mit 'Link senden' oder 'Link abrufen' freigegeben wurden. Mit dieser Liste können

Benutzer den Zugriff auf diese Dateilinks entziehen oder in der Sync & Share-Hierarchie zu den Dateien navigieren. [US10809]

- Benutzer können nun eine detaillierte Liste der für eine bestimmte Datei freigegebenen einzelnen Dateilinks anzeigen lassen, die auch berücksichtigt, an wen die Links gesendet wurden, welche Beschränkungen für die Links gelten und wann sie ablaufen. Diese einzelnen Links können entzogen werden. [US10814]
- Sync & Share-Dateien, die mit 'Link senden' oder 'Link abrufen' freigegeben wurden, werden nun in der Datei- und Ordnerliste mit einem Symbol angezeigt. Mit einem Klick auf dieses Symbol können Benutzer die Details der weitergeleiteten Links der Datei anzeigen lassen und ändern. [US10816]
- Acronis Access ist jetzt auch in koreanischer Sprache verfügbar. [US10638]
- Wird ein Benutzer deaktiviert, werden alle weitergeleiteten Dateilinks vorübergehend deaktiviert. Wird ein Benutzer gelöscht, werden alle weitergeleiteten Dateilinks deaktiviert, bis ihr Inhalt neu zugewiesen wird. Wird der Inhalt des Benutzers neu zugewiesen, werden die Dateilinks reaktiviert und gehen in das Eigentum des neuen Inhaltseigentümers über. [US9870]
- Administratoren können eine benutzerdefinierte Meldung konfigurieren, die auf der Webanmeldeseite angezeigt wird. Diese Meldung kann auf der Seite 'Einstellungen => Web UI-Anpassung' angepasst werden. [US10319, US10660]
- Die Standardbenachrichtigungs-E-Mails für Benutzer beinhalten nun einen Link, über den der Benutzer das Abonnement der Benachrichtigungs-E-Mails des freigegebenen Sync & Share-Ordners kündigen kann. [US10423]
- Wird ein Datei-Link mehreren Benutzern gleichzeitig zur Verfügung gestellt, erhalten alle Benutzer, die einen Hauptschlüssel-Link erhalten, denselben Link. Bisher erhielt jeder Benutzer einen anderen, individualisierten Link. Die einzige Ausnahme sind hier die Links zur einmaligen Nutzung. Wird ein Link zur einmaligen Nutzung mehreren Benutzern zur Verfügung gestellt, erhält jeder Benutzer einen eindeutigen Link, der einen einmaligen Download ermöglicht. [US10808]

FEHLERBEHEBUNGEN

- Die für die Registrierung von Mobilgeräten erforderliche Zeit wurde deutlich reduziert. [US10712]
- Gateway-Cluster mit einer Client-Verbindungsadresse, auf die nicht über den Access Server zugegriffen werden kann, können jetzt verwaltet werden (mit der Serveradresse). [DE13147]
- Ein neuer Benutzer, der sich erstmalig von einem mobilen Gerät aus anmeldet und Mitglied einer Sync & Share-LDAP-Gruppe ist, erhält nun Sync & Share-Zugriff ohne sich zunächst über die Weboberfläche anmelden zu müssen. [DE13215]
- Ausstehende Benutzer mit Zugriff auf Sync & Share-Datenquellen können sich nun erfolgreich von einem mobilen Gerät aus anmelden. [DE13379]
- Active Directory-Benutzer, deren Kennwörter einen Doppelpunkt enthalten, können sich nun erfolgreich authentifizieren, um vom Desktop Client aus Zugriff auf synchronisierte Netzwerkdaten zu erhalten. [DE14294]
- Es wurde ein Problem behoben, bei dem der Access Server gestartet wurde, wenn das PostgreSQL-Kennwort einfache Anführungszeichen, Doppelpunkte, Prozentzeichen, High Unicode-Zeichen oder andere Sonderzeichen enthielt. [DE14355]
- Gedankenstriche werden in Servernamen, die in der Liste mit den Zugriffsbeschränkungen für unterstützte Anmeldeserver definiert wurden, nicht mehr als ungültig interpretiert.[DE14414]

- Das beim Herunterladen einer Sync & Share-Datei über einen direkten Link angegebene Änderungsdatum wird nun für die Zeitzone des Servers angegeben. [DE14418]
- Gelöschte Benutzer werden nicht mehr in der Type-ahead-Liste für E-Mail-Vorschläge aufgeführt. [DE14508]
- Das Access Server-Installationsprogramm kann auch dann erfolgreich ausgeführt werden, denn das PostgreSQL-Kennwort einfache Anführungszeichen, Doppelpunkte, Prozentzeichen, High Unicode-Zeichen oder andere Sonderzeichen enthält. [DE14433]
- Es wurde ein selten auftretendes Problem im Desktop Client behoben, bei dem eine Datei, die sofort nach dem Download während der Synchronisierung auf der Festplatte gesperrt wurde, einen Absturz des Synchronisierungsvorgangs verursachen konnte. [DE14197]

BEKANNTE PROBLEME

- Files Advanced 7.1 ist in Java Version 8u31 enthalten, ist jedoch mit 8u45 zertifiziert. Es liegt ein bekanntes Problem mit den Java-Versionen ab 8u31 vor, das zu Problemen mit der Single Sign-On-Funktion führt. Sollten Sie Ihre Java-Version aktualisiert haben und SSO verwenden wollen, lesen Sie bitte den folgenden Artikel: https://kb.acronis.com/content/56367

Acronis Access 7.0.5

VERBESSERUNGEN

- Acronis Access ist nun auch in traditionellem und vereinfachtem Chinesisch verfügbar. US10350
- Verbesserte Leistung beim Durchsuchen von Inhalten von Netzwerkdatenquellen mit vielen Unterordnern. US10622
- ACRONIS ACCESS unterstützt die Authentifizierung von Gerätezertifikaten. US10697

FEHLERBEHEBUNGEN

- Problem behoben, bei dem bei einem sehr langen Pfad einige SharePoint-Datenquellen nicht hinzugefügt werden konnten. DE14339
- Problem behoben, das möglicherweise beim Start nach Upgrades auf Access Server 7.0.4 auftrat, wenn Benutzer ohne Benutzernamen angegeben waren. DE14352
- Probleme behoben, die möglicherweise beim Hochladen von Dateien mit Internet Explorer 9. US10636 auftraten
- Problem behoben, bei dem mit dem Öffnen des Desktop-Synchronisierungsdialogfelds für einen synchronisierten Netzwerkordner und dem Speichern ohne Änderungen möglicherweise ein 2-Wege-Synchronisierungsordner in einen 1-Weg-Synchronisierungsordner geändert wurde. DE14398, DE14415
- Problem behoben, bei dem sich die Synchronisierung von Netzwerkordnern verzögern konnte, wenn andere Benutzer zahlreiche Netzwerkordner und -dateien synchronisierten. DE14406
- Problem behoben, bei dem vom Desktop-Synchronisierungs-Client der Synchronisierungstyp eines Netzwerkordners (von 1-Weg-Synchronisierung in 2-Wege-Synchronisierung oder umgekehrt) möglicherweise nicht sofort geändert wurde, wenn Änderungen an der Weboberfläche vorgenommen wurden. DE14413
- Problem behoben, bei dem Access Server möglicherweise keine Überwachungsprotokolle von Gateway Servern abrufen konnte. DE14414

- Problem mit der Kerberos-Authentifizierung für SharePoint behoben. DE13289, DE14272
- Ein seltenes Problem behoben, bei dem für Desktop Clients ein seltsamer Unicode-Fehler anstatt einer eindeutigen Erklärung auf dem Desktop Client ausgegeben wurde, wenn eine Synchronisierung nicht abgeschlossen werden konnte, da eine synchronisierte Datei auf diesem Computer in einer anderen Anwendung geöffnet war. DE14151, DE14289
- Problem behoben, das auftreten konnte, wenn Desktop Clients direkt von Version 2.x auf Version 7.0.4 oder höher aktualisiert wurden. DE14336
- Problem behoben, bei dem Dateien auf dem Server dupliziert werden konnten, wenn Visual C#-Projekte im Sync & Share-Ordner auf dem Desktop Client gespeichert wurden. DE14353

Acronis Access 7.0.4

VERBESSERUNGEN

- '**Zugriffsbeschränkungen**' für mobile Clients beinhalten nun Optionen zur Beschränkung des Zugriffs von mobilen Windows-Clients aus. Auch die Seite mit Registrierungseinladungen und Registrierungs-E-Mails enthalten nun Optionen für Anweisungen und Installationslinks für Windows-Clients. US8788, US10558
- Mit der Access-Weboberfläche wurde die Benutzerfreundlichkeit auf Mobilgeräten mit geringeren Bildschirmauflösungen verbessert. US10270
- Die Gateway Server-Option für die Unterstützung der Verwendung selbstsignierter Zertifikate kann nun auch dann geändert werden, wenn der Gateway Server offline ist. US10318
- Bei Verwendung der webbasierten Benutzeroberfläche für die Auswahl der Synchronisierung eines Ordners auf dem Desktop Client sehen Benutzer nun die Gesamtgröße des zu synchronisierenden Ordners. Das ermöglicht Benutzern eine fundierte Entscheidung bei der Synchronisierung großer Freigaben auf ihrem Desktop. US10414
- Das Konfigurationsdienstprogramm unterstützt nun die Bereitstellung eines UNC-Pfads für den Speicherort des Access-Datei-Repository. DE13733
- Das Konfigurationsdienstprogramm unterstützt nun die Konfiguration von Zwischenzertifikaten. US10315
- Die während der automatischen Vervollständigung im Rahmen der Einladung von Benutzern für eine Freigabe angezeigten Optionen für E-Mail-Adressen sind nun auf Mitglieder der Freigaben beschränkt, deren Mitglieder sie sind. Zusätzlich können interne AD-Benutzer alle anderen internen AD-Benutzer sehen. DE13387
- Mit '**Link senden**' oder '**Link abrufen**' erstellte direkte Datei-Download-Links können nun konfiguriert werden, um vor dem Herunterladen einer Datei die Access-Anmeldedaten anzufordern. Die Einstellungsseite **'Freigabebeschränkungen'** enthält neue Optionen, mit denen Administratoren definieren können, ob öffentliche Links und anmeldebeschränkte Links unterstützt werden. Werden beide Link-Typen unterstützt, können Benutzer wählen, welchen Linktyp sie für eine Freigabe verwenden möchten. Zusätzlich steht eine Administrationseinstellung zur Verfügung, mit der der Zugriff auf anmeldebeschränkte Links auf interne Benutzer eingeschränkt werden kann. US10499

ÄNDERUNGEN

- **Webverwaltungsseiten können nicht mehr mit Internet Explorer 8 aufgerufen werden.** US10471

BUG-FIXES:

- Bug behoben, der beim Versuch, eine große AD-Gruppe für die mobile Registrierung einzuladen, manchmal zur Meldung nicht bearbeiteter Fehler führte. US10511
- Die Variable %USERNAME% wird nun im Namen und in der Beschreibung der Basisverzeichnis-Datenquellen in der Weboberfläche unterstützt. DE13651
- Beim Herunterladen von Dateien aus der webbasierten Benutzeroberfläche von Safari sollte kein kleines Popup-Fenster mehr angezeigt werden. DE13699
- Benachrichtigungen beinhalten nun den Benutzer, der den Link zur freigegebenen Datei erstellt hat, wenn Dateien mit einem direkten Datei-Download-Link heruntergeladen werden. DE13811
- Die Liste der Datenquellen wird nun auch dann angezeigt, wenn auf einige Datenquellen nicht zugegriffen werden kann. Die Datenquellen, auf die nicht zugegriffen werden kann, werden in der Liste einfach nicht angezeigt. DE13896
- Für die Landing Page des Datei-Download-Links werden keine Farbschemata verwendet. DE14072
- AD-Benutzer mit Konten, für die kein Benutzerprinzipalname (UPN) konfiguriert wurde, können jetzt mit der Access-Weboberfläche auf Netzwerkdatenquellen zugreifen. DE14089
- Für die Konfliktlösung werden nun Benutzer unterstützt, deren Namen einen Schrägstrich enthalten. Bei der Erstellung von Konfliktdateien werden Schrägstriche nun durch einen Unterstrich ersetzt, da Schrägstriche im Windows-Dateisystem als ungültige Zeichen gelten. DE14133
- Dateien und Ordner auf Netzwerk-Volumes, die mit einem Mac-Computer hochgeladen wurden und einen Schrägstrich enthalten, können nun mit Mac- und Windows-Desktop Clients synchronisiert werden. DE14141
- Probleme, die möglicherweise verhinderten, dass Gateway-Überwachungsprotokollnachrichten vom Access-Server genau geprüft wurden, wurden behoben. DE14146, DE14152
- Problem behoben, bei dem nach dem Upgrade auf Access 7.0.3 bei der Dateibereinigung möglicherweise Fehler gefunden wurden und diese fehlschlug. DE14195, DE14015, DE14101
- Es wurde ein Lizenzproblem behoben, das dazu führen konnte, dass für eine einzelne Benutzersitzung vorübergehend mehrere Lizenzen auf dem Gateway Server verwendet wurden. DE14275, DE14142
- Der PostgreSQL-Dienst wird nun vor dem Upgrade von Clustern angehalten, um Fehler zu vermeiden, die ein Upgrade des Clusters verhindern. DE11927
- Beim Schnellspeichern von Microsoft Office-Dateien erstellt der Desktop Client nicht mehr mehrere Kopien der Datei in Access. DE14014

Acronis Access 7.0.3

VERBESSERUNGEN:

- Die API-Dokumentation für Web-Clients wurde aktualisiert, darunter auch der Support und die Dokumentation für Netzwerkdateien und -ordner.
- Das Farbschema der Acronis Access-Website kann auf eine verschiedene vordefinierte Farbschemas festgelegt werden. Alternativ können Administratoren ihr eigenes benutzerdefiniertes Farbschema entwickeln. Administratoren können das Farbschema über die Seite Web-UI-Anpassung (S. 135) konfigurieren.

- Das Aussehen der Web-UI kann jetzt durch Hochladen von benutzerdefinierten Logos geändert werden. Es werden drei Bildgrößen für die verschiedenen Anzeigepositionen des Logos verwendet. Bei einem Upgrade wird das ggf. vorhandene benutzerdefinierte Logo für alle benutzerdefinierten Logopositionen verwendet. Über die Seite Web UI-Anpassung (S. 135) können jedoch Logos in der richtigen Größe hochgeladen werden.
- Wenn die für einen Benutzer geltenden Richtlinien für den mobilen Zugriff den Zugriff vom Web-Client aus zulassen, enthält die Standard-E-Mail mit der Registrierungseinladung jetzt einen Link zur Acronis Access-Website. Kunden, die die Vorlage der E-Mail für die Registrierungseinladung angepasst haben, müssen den zusätzlichen Text bei Bedarf manuell zur angepassten Vorlage hinzufügen.
- Benutzer können die Inhalte des Ordners, den sie gerade durchsuchen, jetzt mit der Option '**Ordner herunterladen**' herunterladen.
- Acronis Access-Administratoren werden bei einer Neuinstallation während der Erstkonfiguration (S. 31) nicht mehr zur expliziten Angabe der Adresse des Gateways-Servers aufgefordert. Die Gateway-Adresse wird automatisch auf die gleiche Adresse wie die des Access-Servers festgelegt.
- An der standardmäßigen E-Mail-Vorlage für die Registrierungseinladung wurden in Vorbereitung auf eine bevorstehende neue Version des mobilen Clients geringfügige Änderungen vorgenommen. Benutzer mit benutzerdefinierten E-Mail-Vorlagen müssen diese bei Bedarf manuell aktualisieren.
- Die Anmeldeperformance und die allgemeine Performance der Webanwendung wurden durch Zwischenspeichern einiger Einstellungen im Arbeitsspeicher verbessert.
- Es wurden verschiedene Verbesserungen zur Steigerung von Performance und Durchsatz beim Hoch- und Herunterladen von Sync & Share-Dateien vorgenommen.
- Acronis Access wird jetzt mit Java 8u31 installiert.

BUG-FIXES:

- Fehler bei der LDAP-Zwischenspeicherung, die bei aktivierter `ldap_caching`-Debug-Protokollierung auftreten konnten, wurden behoben.
- Ein Problem mit der New Relic-Überwachung wurde behoben.
- Folgendes Problem wurde behoben: Der mit dem Desktop synchronisierte Netzwerkordner eines Benutzers wurde möglicherweise nicht entfernt, wenn der serverseitige Netzwerkordner aus den zugewiesenen Datenquellen entfernt wurde.
- Folgendes Problem wurde behoben: Gateway-Dateifreigaben konnten nicht vom Webportal aus durchsucht werden, wenn ein Management Server erforderlich ist und der Management Server einen nicht standardmäßigen Port abhört.
- Wenn ein Benutzer bei einem Upgrade von Acronis Access 6.x versucht, sein Kennwort zurückzusetzen, bevor er sich erfolgreich bei Access 7.x angemeldet hat, tritt kein Fehler mehr auf.
- Beim Umbenennen eines 1-Weg-Sync-Ordners der obersten Ebene auf dem Desktop Client wird keine Warnung mehr ausgegeben.
- Ein Zeitüberschreitungsfehler, der beim Herunterladen großer Dateien über den mobilen Client auftreten konnte, wurde behoben.

BEKANNTE PROBLEME:

- Falls einige Ihrer Endbenutzer den Internet Explorer 8 verwenden, sollten Sie ein Upgrade/einen Umstieg auf einen sichereren Browser erwägen. Administratoren können die SSL-Bindungen ändern, um Internet Explorer 8-Benutzer mit folgenden Einschränkungen zu unterstützen (DE12649):
  - Benutzer mit Internet Explorer 8 werden automatisch zur Access 6 Style Web Client-Oberfläche umgeleitet.
  - Der Internet Explorer 8 wird von der neu entwickelten Access 7-Weboberfläche nicht unterstützt.
  - Diese Benutzer haben über die Web Client-Oberfläche keinen Zugriff auf Datei-Server, NAS- und SharePoint-Datenquellen.
  - Der Internet Explorer 8 wird für Server-Administration nicht unterstützt.

Acronis Access 7.0.2

VERBESSERUNGEN:

- Acronis Access Server und die Desktop Clients für Mac und PC sind nun in polnischer Sprache verfügbar.
- Acronis Access ermöglicht es nun, bestimmte Ordner von Datei-Servern, NAS-Geräten und SharePoint-Servern unter Verwendung des Access Desktop Clients mit Macs oder PCs zu synchronisieren. Diese Funktion kann in der Richtlinie 'Mobiler Zugriff' aktiviert bzw. deaktiviert werden und setzt voraus, dass auch für den Access Web Client der Zugriff auf diese Datenquellen aktiviert wurde.
- Verbesserungen beim Benutzer-/E-Mail-Adress-Eintrag im Freigabe-Dialogfeld des Access Web Clients.
- Der Access Web Client zeigt nun einen Navigationspfad (Breadcrumb Trail) über mehrere Ebenen an.
- SMB-Netzwerkfreigaben können nun als Datei-Repository-Ziele im Access Server-Konfigurationswerkzeug ausgewählt werden (DE13472).
- Das Access Server-Konfigurationswerkzeug greift nun standardmäßig auf ein selbstsigniertes Zertifikat zurück, falls im persönlichen oder Computer-Zertifikatsspeicher keine passenden Zertifikate vorhanden sind. (DE12983)
- In der russischen Lokalisierung des Access Servers 7.0.2 wird die GOST-Verschlüsselung unterstützt (US9922).
- Im Web Client ist nun der Zugriff auf Netzwerk-Basisordner enthalten (US9733).
- Der Web Client unterstützt nun Netzwerkdatenquellen, die den Platzhalter %username% in ihrem Pfad enthalten (DE13206).
- Beim Upload im Web Client können jetzt mehr als 10 Dateien gleichzeitig hochgeladen werden. (DE12719)
- In dieser Version wird Java 7 Update 71 verwendet.

BUG-FIXES:

- Es wurde ein Problem beim E-Mail-Versenden von Download-Links für Sync & Share-Dateien über den iOS Mobile Client behoben (DE13177).

- Links auf Einstiegsseiten (Landing-Pages) sowie auf Ordner von Benachrichtigungs-E-Mails und von Desktop Client Finder-/Explorer-Kontextmenüs erfordern es jetzt nicht mehr, dass der Benutzer sich gelegentlich anmelden muss.
- Es wurde ein Problem beim Upgrade von mobilEcho 4.5 behoben, bei dem Legacy-Datenquellen manchmal nicht konvertiert wurden (DE13188).

BEKANNTE PROBLEME:

- Bei der Installation auf nicht-englischen Windows-Servern kann es aufgrund eines Fehler im enthaltenen Java-Installer (stammt von einem Dritthersteller) zu einem Problem kommen. Genauere Information zum Umgang mit diesem Problem finden Sie unter der Adresse https://kb.acronis.com/content/54518. (DE13473)
- Falls einige Ihrer Endbenutzer den Internet Explorer 8 verwenden, sollten Sie ein Upgrade/einen Umstieg auf einen sichereren Browser erwägen. Administratoren können die SSL-Bindungen ändern, um Internet Explorer 8-Benutzer mit folgenden Einschränkungen zu unterstützen (DE12649):
  - Benutzer mit Internet Explorer 8 werden automatisch zur Access 6 Style Web Client-Oberfläche umgeleitet.
  - Der Internet Explorer 8 wird von der neu entwickelten Access 7-Weboberfläche nicht unterstützt.
  - Diese Benutzer haben über die Web Client-Oberfläche keinen Zugriff auf Datei-Server, NAS- und SharePoint-Datenquellen.
  - Der Internet Explorer 8 wird für Server-Administration nicht unterstützt.

Acronis Access 7.0.1

VERBESSERUNGEN:

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

BUG-FIXES:

- Ein Fehler bei der Verwendung des '¥'-Symbols bei der Protokollierung im Access Server Web Client wurde behoben (DE13031).
- Ein Upgrade von mobilEcho 4.5 auf Acronis Access 7.0.1 wird nun unterstützt. (DE12984).
- Eine nach einem Upgrade von Acronis Access 6.1 aufgetretene fehlerhafte Verknüpfung im Startmenü auf das Acronis Access Tomcat Service-Konfigurationstool wurde korrigiert (DE12966).

- Bei freigegebenen Ordnern werden jetzt Benachrichtigungen im rechten Menü angezeigt (DE12948).
- Falls einige Ihrer Endbenutzer den Internet Explorer 8 verwenden, sollten Sie ein Upgrade/einen Umstieg auf einen sichereren Browser erwägen. Administratoren können die SSL-Bindungen ändern, um Internet Explorer 8-Benutzer mit folgenden Einschränkungen zu unterstützen (DE12649):
  - Benutzer mit Internet Explorer 8 werden automatisch zur Access 6 Style Web Client-Oberfläche umgeleitet.
  - Der Internet Explorer 8 wird von der neu entwickelten Access 7-Weboberfläche nicht unterstützt.
  - Diese Benutzer haben über die Web Client-Oberfläche keinen Zugriff auf Datei-Server, NAS- und SharePoint-Datenquellen.
  - Der Internet Explorer 8 wird für Server-Administration nicht unterstützt.
- Gelegentlich auftretende Abstürze im Access Desktop Client für Mac wurden behoben (DE12879).

BEKANNTE PROBLEME:

- Wird eine Access Gateway Server-Konfiguration mit nur einem Port verwendet, kann es zu Problemen bei der Verarbeitung von Pfaden kommen, die mit mehr als 256 Zeichen enthalten. Hinweise zum Beheben dieses Problems finden Sie im folgenden KB-Artikel (DE12405): http://support.microsoft.com/kb/820129

Acronis Access 7,0

VERBESSERUNGEN

- Neu gestaltete und verbesserte Benutzeroberfläche des Access Web Clients.
- **Acronis Access** heißt jetzt **Acronis Access Advanced** und ist der Upgrade-Pfad für Benutzer von Acronis Access 6 (oder früher). Es wurde außerdem eine neue, auf kleine und mittlere Unternehmen zugeschnittene Version mit niedrigeren Anforderungen eingeführt. Diese neue Version heißt Acronis Access.
- Der Konfigurationsassistent versucht jetzt bei neuen Installationen, bestimmte Systemkonfigurationsoptionen (wie SMTP-Server und Active Directory-Server (LDAP-Server)) zu erkennen.
- Acronis Access und Acronis Access Advanced können bei einer Installation jetzt so konfiguriert werden, dass sie einen einzigen offenen Port für Client-Verbindungen nutzen. Bei dieser Konfiguration verwenden alle Access Clients (mobile App, Desktop Sync Client, Web Client-Oberfläche) dieselbe Netzwerkadresse und denselben Port zur Verbindung mit dem Access Server.
- Ordner und Dateien auf den Dateiservern, NAS- und SharePoint-Servern sind jetzt von der Access Web Client-Oberfläche aus durchsuchbar und per Zugriff verfügbar. Diese Funktion kann auf Benutzer- oder Gruppenebene aktiviert bzw. deaktiviert werden.
- Aktualisierte grafische Gestaltung der Standard-E-Mail-Vorlagen. Neu gestaltete Benachrichtigungs- und Einladungs-E-Mail-Vorlagen.
- Die Verwaltungsseite für Benutzer und die Verwaltungsseite für Geräte sind jetzt in einer einzigen Admin-Konsolen-Seite zusammengeführt.

- Access ermöglicht jetzt eine Konfliktlösung für Sync & Share-Dateien und -Ordner. Falls sich Dateiänderungen von Benutzern überlappen und in Konflikt geraten, werden diese Konflikt verursachenden Dateien unter Verwendung des Benutzernamens und aktuellen Datums umbenannt, sodass die Konflikt verursachende Datei erkennbar wird und bedarfsgerecht behandelt werden kann. Vor Access 7.0 wurden solche Konflikt verursachenden Dateien als neue Versionen gespeichert.
- Sync & Share-Dateien können jetzt zwischen Sync & Share-Ordnern über die Web Client-Oberfläche kopiert werden.
- Download-Links für Sync & Share-Dateien können jetzt zur Verwendung erstellt und kopiert werden, ohne dass einen E-Mail durch den Access Server gesendet werden muss. Die Funktion 'Datei-Download-Links' kann aktiviert oder deaktiviert werden.
- Externen Ad-hoc-Benutzern können jetzt Benutzernamen zugewiesen werden. Alle Sync & Share-Benutzer werden in der Regel über Benutzernamen und nicht einfach nur durch E-Mail-Adressen angesprochen.
- Die Access Client-Version wird jetzt im Bereich für Benutzer und Geräte auf der Access Server-Verwaltungsseite angezeigt. (US8696)
- Ab dieser Version wird Java Version 7 U71 verwendet. (US9486)
- Verbesserte Überwachungsprotokollierung, wenn Dateien über einen direkten Download-Link heruntergeladen werden. (DE10961)
- In der Web Client-Oberfläche können Dateien nun nach Typ sortiert werden. (US6836)
- Postgres kann jetzt über die Systemsteuerungsfunktion 'Programme hinzufügen/entfernen' deinstalliert werden. (US8270)
- Es gibt jetzt eine neue globale Einstellung, um die Möglichkeit zu deaktivieren, Dateien über einen direkten Download-Link freizugeben. (US8347)
- Es kann nun ein standardmäßiger Grenzwert sowie ein Intervall für die Benutzerbenachrichtigung konfiguriert werden, wenn sich Benutzer ihrer Quota für Sync & Share nähern. (US8605)
- Ab dieser Version wird Apache Tomcat 7.0.56 verwendet. (US9801)
- Ab dieser Version wird OpenSSL Version 1.0.1 verwendet. (DE11653)
- Die Tabelle 'Geräte' wurde mit einer Unterstützung für Batch-Aktionen (Remote-Löschung, Remote-Löschung abbrechen usw.) ergänzt. (US8875)

FEHLERBEHEBUNGEN

- Es wurde ein PostgreSQL-Installationsfehler behoben, der auftreten kann, wenn eine lokale Benutzergruppe über unzureichende Berechtigungen verfügt.
- Es wurde ein Problem bei LDAP-Abfragen behoben, dass es bei aktivierter Debug-Protokollierung mit einigen UTF-8-Benutzernamen gelegentlich zu einem Fehler kommen kann.
- Ein Fehler bei der Verwendung der Variable '@display_name' in Acronis Access-Einladungs-E-Mails wurde behoben.

BEKANNTE PROBLEME

- Der Internet Explorer 8 wird in der Erstversion des Acronis Access 7.0 Web-Clients nicht unterstützt. IE8-Benutzer können sich nicht am Acronis Access Web Client anmelden. Die Unterstützung für IE8 wird vermutlich in einem späteren Release wieder zurückkommen. Den IE8-Benutzer wird in diesem Release dann jedoch nur die frühere Weboberfläche von Access 6 bereitgestellt, neue Funktionen von Access 7 können nicht verwendet werden. Wenn Sie

Endbenutzer haben, die den Internet Explorer 8 einsetzen, sollten Sie ein Upgrade auf einen sichereren Browser in Erwägung ziehen – oder warten, bis mit einem kommenden Access Server-Update wieder eine Unterstützung hinzugefügt wird. (DE12649)

- Windows XP-Benutzer können den Acronis Desktop Sync-Client oder den Web-Client nicht mehr verwenden, nachdem der Access Servers per Upgrade auf Version 7.0 (oder höher) aktualisiert 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. 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)
- 'Mobiler Zugriff'-Netzwerk-Basisordner, die für Benutzer auf dem Access Server konfiguriert wurden, werden in der Web Client-Benutzeroberfläche nicht mehr angezeigt. Diese Funktion wird in einem späteren Release wieder unterstützt werden. (US9733)
- Hat der Benutzer mehrere Dateien zum Upload ausgewählt, werden diese nacheinander und nicht gleichzeitig hochgeladen. (DE12512)
- Ein- und Auschecken bei SharePoint wird auf der Web Client-Oberfläche noch nicht unterstützt. Diese Funktion wird in einem späteren Release wieder 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. (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)

FEHLERBEHEBUNGEN

- 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.

FEHLERBEHEBUNGEN

- 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.

FEHLERBEHEBUNGEN

- 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, das der Access Gateway Service nach einem Neustart von Windows Server 2008R2 automatisch startet.

Acronis Access 6,1

VERBESSERUNGEN

- Webdienste-API für die Verwaltung von Acronis Access Server. Die API-Dokumentation ist innerhalb des Access Servers verpackt und Administratoren können darauf zugreifen. Der Link befindet sich in der Fußzeile.
- Das Acronis Access Überwachungsprotokoll kann jetzt so konfiguriert werden, dass alte Protokolleinträge automatisch exportiert und bereinigt werden. Die Einstellungen für Exportieren und Bereinigen können auf der Seite 'Überwachungsprotokoll => Einstellungen' festgelegt werden.

- Neues Acronis Access Konfigurationsübersichtswerkzeug sammelt relevante Serverkonfigurationsdetails, die an den Acronis Support gesendet werden.
- Verbesserte Anmeldeleistung durch allgemeine Leistungsverbesserungen und durch Zwischenspeichern der Informationen zur Active Directory-Gruppenmitgliedschaft.
- Administratoren können jetzt eine Vorschau benutzerdefinierter E-Mail-Vorlagen anzeigen, bevor diese gespeichert werden.
- Das Logo und das Farbschema des Acronis Access Servers können jetzt ohne weiteres angepasst werden. Informationen zum Anpassen des Servers finden Sie in der folgenden Dokumentation: Weboberfläche anpassen.
- 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.

FEHLERBEHEBUNGEN

- 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

FEHLERBEHEBUNGEN

- 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.

FEHLERBEHEBUNGEN

- 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.

FEHLERBEHEBUNGEN

- Das Exportieren einer großen Menge Datensätze aus dem Überwachungsprotokoll wurde erheblich beschleunigt.
- Fehlermeldungen aus einigen Dialogfeldern werden jetzt einwandfrei gelöscht, wenn die Fehlerbedingung aufgelöst ist.
- Jetzt kann immer nur eine Instanz des Konfigurationswerkzeugs ausgeführt werden.
- Unter Windows Server 2003 wird bei der Deinstallation nicht mehr gemeldet, dass PostgreSQL vom Acronis Access Server-Installer nicht installiert wurde.
- Das Konfigurationswerkzeug erzeugt jetzt einen Fehler, wenn der Gateway-Dienst so konfiguriert ist, dass alle Adressen an einen Port und der Access Server an eine bestimmte Adresse bei demselben Port gebunden werden.
- Bei Neuinstallationen wird Tomcat standardmäßig jetzt so konfiguriert, auf Port 8005 nicht auf Anforderungen zum Herunterfahren zu warten. Dies verhindert Konflikte mit anderen Instanzen von Tomcat auf einem Server. Da die Access Server Tomcat-Instanz als Dienst ausgeführt wird, werden über Netzwerkports gesendete Anforderungen zum Herunterfahren nicht benötigt.
- Verschiedene Verbesserungen der Lokalisierung.
- Verbesserte Protokollanzeigeleistung für Nicht-Administratoren.
- Benachrichtigungen über abgelaufene Lizenzen werden nicht mehr angezeigt, wenn activEcho über den Access Server Administrator deaktiviert wurde.
- Neue Benutzer, die eine Einladungs-E-Mail erhalten, werden in einer Nachricht aufgefordert, ein Kennwort festzulegen, anstatt das Kennwort zu ändern.
- Das Dialogfeld 'Neue Dateien hochladen' enthält kein zusätzliches Feld, wenn Internet Explorer 8 oder 9 verwendet wird.
- Der Windows Desktop Client lädt in bestimmten Situationen, in denen das Kennwort des Benutzers abläuft und erneut eingegeben wird, Inhalte nicht mehr erneut hoch.
- Sonstige Fixes an der Dateisynchronisierungslogik für Desktop Client
- Durch Entfernen einer Benutzer- oder Gruppenrichtlinie mit einem benutzerdefinierten Basisordner wird jetzt das Volume auf dem Gateway Server ordnungsgemäß entfernt.
- Bei der Anzeige von 'Zugewiesene Quellen' für einen Benutzer werden jetzt Quellen angezeigt, die diesem Benutzer über die Gruppenmitgliedschaften zugewiesen wurden.
- Die Reihenfolge der Registerkarten auf der Verwaltungsseite 'Datenquellen' wurde verbessert.
- Beim Ändern der Gateway Server-Verwaltungsadresse wird das Bearbeitungsdialogfeld durch Klicken auf 'Anwenden' nicht mehr geschlossen.
- mobilEcho Clients, die mit Client-Zertifikaten für das Management registriert werden, schlagen nicht mehr regelmäßig fehl, wenn der Benutzer sich noch nicht im LDAP-Cache des Servers befand.

- Durch Einfügen von Leerstellen in Gateway Server-Adressen wird eine ordnungsgemäße Verwaltung des Gateway Servers nicht mehr behindert.
- Hinweise im Dialogfeld 'Geräteinformationen' werden jetzt ordnungsgemäß gespeichert.
- Wenn Richtlinien deaktiviert wurden, werden sie jetzt in der Richtlinienliste ausgegraut angezeigt.
- Bei einem Upgrade von mobilEcho Server 4.5 werden die mobilEcho-Benutzer jetzt ordnungsgemäß importiert, auch dann, wenn die falsche LDAP-Suchbasis im Konfigurationsassistenten eingegeben wurde.
- Lizenzschlüssel, die mit 'YD1' beginnen, werden jetzt auf der Lizenzierungsseite ordnungsgemäß als Testschlüssel mit einem Ablaufdatum angezeigt, und nicht mehr als unbefristete Lizenzen.
- Einladungs-E-Mails für die Registrierung enthalten jetzt die richtigen Links für Android-Clients.
- Die Bearbeitung von SharePoint-Anmeldeinformationen für einen Gateway Server ist jetzt deaktiviert, wenn der Gateway Server nicht über eine Lizenz verfügt, die die SharePoint-Verbindung unterstützt.

Acronis Access 5.0.3

VERBESSERUNGEN

- ACRONIS ACCESS Server kann jetzt unter Windows Server 2003 SP2, 2008/2008R2 und 2012/2012R2 auf einem Windows-Failovercluster installiert werden. Informationen zur Installation oder zum Upgrade mit dieser Konfiguration finden Sie unter ACRONIS ACCESS in einem Cluster installieren (S. 263) und Upgrade von ACRONIS ACCESS in einem Cluster.

FEHLERBEHEBUNGEN

- 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 unter 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.

FEHLERBEHEBUNGEN

- 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

FEHLERBEHEBUNGEN

- 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 bzw. 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 bzw. 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.

FEHLERBEHEBUNGEN

- 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.

15.2 Frühere Versionen

Themen

15.2.1 activEcho

Files Advanced Server 6.0

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**. For the latest information, please visit the What' New in Files Advanced Server (S. 322) article.

activEcho 5.1.0

BUG-FIXES

- 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

activEcho 5.0.3

BUG-FIXES

- E-Mail-Benachrichtigungen werden jetzt nach einem Upgrade ordnungsgemäß versandt, wenn benutzerdefinierte Vorlagen verwendet wurden.

activEcho 5.0.2

VERBESSERUNGEN

- Die Leistung des activEcho Clients bei einer großen Anzahl Updates wurde verbessert.

BUG-FIXES

- Upgrades von activEcho 2.7 funktionieren auf nicht englischen PostgreSQL-Installationen jetzt fehlerfrei.

activEcho 5.0.1

- Keine Änderungen.

activEcho 5.0.0

VERBESSERUNGEN

- 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 Reaktionsschnelligkeit der Benutzeroberfläche beim Neuzuweisen von Inhalten bei Tausenden von Benutzern im System.
- 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.

BUG-FIXES

- 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.

activEcho 2.7.3 (Released: June 2013)

ENHANCEMENTS:

Switched to using the official AWS library file for Amazon S3 connections.

Files now can be successfully uploaded to any of the eight Amazon S3 bucket regions.

BUG FIXES:

Pending users can now be deleted without error.

Files which were not fully uploaded to the Amazon S3 file repository will now be removed from the repository if the repository is accessible after the upload failure occurs.

Files can be uploaded and downloaded when the file repository is not using encryption.

activEcho 2.7.2 (Released: May 2013)

BUG FIXES:

Files which were not fully uploaded to the file repository will now be removed from the

repository if the repository is accessible after the upload failure occurs.

Fixed a rare case where the activEcho client would fail to sync due to the structure of a system file ID.

activEcho 2.7.1 (Released: April 2013)

ENHANCEMENTS:

The activEcho web server and system can now be monitored using the New Relic monitoring tools. For more information about the new functionality and obtaining a license, refer to http://newrelic.com/

Upgrading will now maintain intermediate certificate files configured for the activEcho Tomcat installation's HTTPS connections.

Improved load speed of users page by caching content usage.

BUG FIXES:

Web users running on Internet Explorer 8 or Internet Explorer 9 in compatibility

mode will no longer receive an error that their browser is incompatible with activEcho.

Folders with names in the format YYYYMMDD will no longer fail to sync from the activEcho client to the server.

activEcho 2.7.0 (Released: February 2013)

ENHANCEMENTS:

Mac and Windows sync clients will now be notified when they have updated content available for download. These notifications will reduce load on the server and improve performance by avoiding many unnecessary requests from clients to the server to check for updates when none are available.

Mac and Windows sync clients have been made more resilient to errors on single files and folders. The client syncing process will no longer stop if a single locked file is updated. All other files which can be successfully updated will be. The client syncing process will also no longer stop is a file cannot be successfully downloaded. All other files which can be successfully downloaded will be.

Mac and Windows sync clients can now automatically download and install updates.

Download speed of large numbers of files to sync client has been improved.

Altering the preferences on the client will no longer cause a paused client to begin syncing.

Windows sync client now offers a "Show previous activEcho versions" context menu option.

The Projects tab in the web interface has been optimized for increased performance and smoother user interaction.

The Projects tab now supports pagination, sorting, filtering.

The move dialog in the web interface now loads quickly, even when the user has a large hierarchy of folders.

All client connections can be disabled for administrative purposes from the Server Settings page in the web UI.

All timestamps used for comparison or calculation will now be set to database time instead of server time to ensure proper operation in a cluster scenario.

The web interface now provides support for non-US date-time formats.

Duplicate folder updates will no longer cause multiple revisions of the folder to be created.

The default PostgreSQL installation is now configured with more carefully tuned parameters to improve performance.

User proxy AD objects can now successfully authenticate to activEcho.

Multiple domains can now be provided for LDAP configuration to be automatically pre-pended to usernames for login.

Links in emails when sharing a folder to a new user will now direct the user into the new share on the website. Note that if the default templates have been altered, the passkey paths in the notification email template will need to be modified to look like this:

```
<%= @root_web_address %>

<%= passkey_path( @passkey, { :redirect_path =>

        show_contents_node_path( @node.uuid, {:show_sync_lightbox => true}    ) } ) %>
```

Files will no longer be marked deleted if they can't be found in the repository. They will need to manually be removed.

Tomcat no longer needs to be restarted when S3 repository settings are changed.

All activEcho server logging is now written to a date-stamped activEcho.log file which is rotated daily. This log file can be found inside the Tomcat logs folder.

A configuration flag has been added to allow the activEcho web server to support HTTP connections instead of HTTPS. To allow HTTP connections, set REQUIRE_SSL to false in activEcho.cfg.

The Windows client MSI file is now available in the clients download directory.

ActivEcho's web application is now installed in the following location:

C:\Program Files (x86)\Group Logic\activEcho Server\activEcho Web Application

ActivEcho's Tomcat server is now installed in the following location:

C:\Program Files (x86)\Group Logic\Common\apache-tomcat-7.0.34

ActivEcho's Tomcat is now configured to redirect HTTP to HTTPS by default.

Customers not needing redirection refer to the online documentation:

https://docs.grouplogic.com/display/ActivEcho/activEcho+Server#activEchoServer-RedirectingHTTPrequeststoHTTPS

The list of shares has now been removed from the left panel of the projects web page to improve the page performance.

Filtering options have been added to projects page sidebar.

Improved shutdown speed of the Mac and Windows sync clients.

Upgraded default Tomcat installation to version 7.0.34 and Tomcat Native (tcnative-1.dll) to version 1.1.24.

Upgraded default version of PostgreSQL to 9.2.1.

Validation of support for Windows 2012 Server.

Validation of support for Java 7 update 15.

Validation of support for Windows 8 for the Windows sync client.

Users on IE7 will now explicitly receive an error message that IE7 is not supported.

BUG FIXES:

Fixed a couple of rare instances where the sync client could receive a database

error and could no longer sync.

Under load, client will no longer occasionally corrupt files on download and upload the corrupted versions.

Duplicate files will no longer appear in the web interface if you pause and resume the client in the middle of uploading a file.

Fixed a Mac client bug where the client receives an error when a file is deleted off the server side while the client is downloading the file.

The sync client will no longer fail to complete in rare cases where folders are aggressively renamed with similar names.

The sync client will no longer attempt to delete files repeatedly if it cannot succeed.

Tomcat settings have been changed to ensure that syncing requests from the client will succeed even when there are many top-level folders.

File and folders with names containing %, _, and ! will now be handled properly.

Multiple bug fixes to sync client context menu options to support a variety of file and folder names which previously would fail.

LDAP authentication by email will now work properly for LDAP domains where authentication by common name is not permitted.

Fixed various case-sensitivity bugs with LDAP authentication.

Adding trial server licenses will no longer occasionally fail.

Unsharing a folder with Unicode characters in the name using "Remove all" will no longer cause an error.

A pending user can now be removed from a shared folder if you have the appropriate permissions, even if you are not an administrator.

Users can no longer share deleted folders.

Improved error handling for SMTP errors.

Miscellaneous other bug fixes.

activEcho 2.6.1 (Released: October 2012)

BUG FIXES:

Reassigning content from deleted users now works when quotas are disabled.

activEcho 2.6.0 (Released: October 2012)

ENHANCEMENTS:

Log and Users tabs support pagination, sorting, filtering.

Log and Users tabs have been optimized for increased performance and smoother user interaction.

Log tab provides new start and end date display filters.

Quotas can be defined for individual Active Directory and Ad-hoc users, overriding group policies.

Quotas can now be defined specifically for administrative users.

Automatic purging of user accounts if no activity has occurred, or a specific absolute time has passed.

Support for configuring the length of time before expiration of shared links.

New share permissions allow owner to hide display of share members to non-owners, and prevent non-owners from inviting others.

New behavior when unsharing projects, local data will be deleted from the client on next connection.

New administrative setting to hide the "Download the activEcho client" link to control which users can download and install the activEcho sync client.

Users accounts can be disabled to temporarily prevent access and login to activEcho.

New administrative setting to control the minimum supported version number of the sync client.

Support provided for creating Tomcat server clusters running activEcho for load balancing and resilience.

Improved diagnostic logging provided in the file repository service.

Desktop Sync clients on Mac and Windows now provide a menu option to display recently updated files.

Clicking an entry in the list opens the folder containing the file.

Mac OS X sync client now supports Gatekeeper signing and notification center on OS X 10.8.

Recommend upgrading to the latest version of the client due to significant performance and stability improvements in both Windows and Mac desktop clients.

The sync client on Mac and Windows now sets a custom icon for the activEcho sync folder.

The server installer allows setting the user account the file repository service runs under to store the repository on network volumes.

Projects tab can now be filtered by items shared by a user, or shared with a user.

Change the default email template when inviting a user to a share to allow the user to select to start syncing the content immediately. If you have customized the invite to share template in the past, update the following items:

```
<%= show_contents_node_path( @node.uuid ) %>
```

to

```
<%= show_contents_node_path( @node.uuid, {:show_sync_lightbox => true} ) %>
```

Validation of support for Java 7 update 7.

BUG FIXES:

Various improvements to LDAP authentication, including case sensitivity issues with domain names and support for multiple email domains.

The domain for LDAP authentication list can use either ; or , as a delimiter.

Various improvements on syncing files and folders where an item or the parent folder(s) have been deleted.

Fixed files modification dates that were not set properly based on timezones under some circumstances.

Period is a valid character in S3 bucket names when using Amazon S3 for the file repository.

Fixed high CPU usage on both Mac and Windows desktop clients.

Miscellaneous other bug fixes.

activEcho 2.5.1 (Released: July 2012)

ENHANCEMENTS:

Support for mobilEcho 4.0 for access to activEcho using mobile devices. mobilEcho 4.0 now allows sharing of activEcho, file shares, and SharePoint servers simultaneously.

Additional license is required for accessing file shares and SharePoint with mobilEcho.

Uploading and downloading of files via mobile devices is faster.

Mobile devices can now copy files and folders within an activEcho share.

Support for Mac OS X 10.8 "Mountain Lion"

BUG FIXES:

Improved upgrade experience when automatically restarting Tomcat when there is a large amount of user data to be migrated.

Server installer now correctly upgrades activEcho when files were originally installed in a custom location.

Mobile devices can now navigate shares that have trailing spaces in their name.

Authentication of LDAP users only worked against the first entry in the Provisioned LDAP table.

Improved support for syncing files from Mac OS X with / in their filenames.

Improvements to the sync clients reduce the potential for a full re-sync being required.

Fixed issue when saving with some applications (Microsoft Publisher, TextEdit, etc.) on Windows and Mac OS X could result in a file being treated as a new file and disassociated from its revision history.

Miscellaneous other bug fixes

activEcho 2.5.0 (Released: July 2012)

The activEcho 2.5 client is not compatible with the 2.1 server. Please upgrade your server to 2.5 first, and then upgrade the clients.

The activEcho 2.1 client is compatible with the 2.5 server but will not have all of the new features available.

ENHANCEMENTS:

Support for quotas. Different quotas values can be set for Active Directory vs. ad-hoc users, as well as based on Active Directory group membership. End users can manage their quota usage by using the web to selectively purge old revisions and deleted files. See the user manual for more information.

Support for read-only ("download only") shares. This setting can be enabled when inviting members to a share, and from the Members page for the share.

Support for selective syncing. Via the web, users can pick which folders they want to have synced to their desktop vs. only accessible via the web. This allows users to have access to shared content but not necessarily have all content synced to their local desktop.

Administrators can now reassign ownership of content when deleting a user from activEcho, or can choose to delete a user and later reassign the content using the Manage Deleted Users page.

When a user's permission to share is removed from a shared folder, the folder is now removed from their client activEcho sync folder.

activEcho clients support pausing / resuming syncing.

Syncing files to Mac OS X clients is significantly faster.

The file repository can now be configured to store content on a UNC path to support network drives.

New Notification setting allows the administrator to be notified when the file repository free space goes below a set threshold.

Default email templates can now be viewed in the management settings.

Web Projects page now provides a summary of the number of files and folders.

Web Users page provides the administrator a summary of individual user's content and quota usage.

Sync clients no longer time out if the initial sync contains more than 50,000 files.

Windows client installer is now available as a MSI package for use in automate deployment.

Deleting many files at once from the web browser is much faster.

Web now provides an "Invite" button for the folder the user is viewing.

Web log view now has a reset filters button.

Master encryption key has been migrated from the Tomcat directory into the activEcho database to prevent accidental data loss if Tomcat is uninstalled without proper backups.

BUG FIXES:

Email template notification errors could occur after a user is deleted from activEcho if they were sharing content.

LDAP settings are no longer validated if LDAP has been disabled in the management settings.

When a folder is unshared, the owner can now see past events in the web log for that folder.

The web log allows filtering of past events for users who are no longer part of the shared folder.

Improved the Windows desktop sync client upgrade experience to not occasionally request that Explorer be restarted.

Email addresses containing the following characters are now valid when inviting or adding a user: ! $ & * - = ^ ` | ~ # % ' + / ? _ { }.

Tomcat web.xml configuration file can no longer be retrieved via a web browser.

Miscellaneous bug fixing in desktop syncing.

activEcho 2.1.1 (Released: June 2012)

ENHANCEMENTS:

Email addresses for LDAP authenticated users now update when the primary email address changes in LDAP.

Improved LDAP performance.

BUG FIXES:

Improved authentication against LDAP to avoid timeouts against large catalogs.

activEcho 2.1.0 (Released: May 2012)

ENHANCEMENTS:

Automatic purging of previous revisions and deleted files based on administrative rules.

Customizeable email templates.

Export log to TXT, CSV, or XML files.

Improved, administrator configurable trace logging for diagnostics.

Significantly improved performance when sharing and syncing a large number of files.

Ability to unsubscribe from shared folders as a user, or for the owner to unshare to all users.

Notifications are now available for folder changes in addition to files.

More than one email address can be provided for notifications.

Support for 64-bit Java installations.

Improved LDAP performance.

Miscellaneous usability enhancements.

BUG FIXES:

Various bug fixes related to authentication with Active Directory via email addresses.

The built-in Administrator account will now never use Active Directory for authentication.

Miscellaneous bug fixes in desktop syncing.

activEcho 2.0.2 (Released: March 2012)

BUG FIXES:

Improvements to desktop syncing when Microsoft Office files are edited directly in the activEcho Folder.

Various bug fixes in desktop syncing.

Bug fixes in activEcho server installer to fix future upgrades.

activEcho 2.0.1 (Released: March 2012)

BUG FIXES:

Improvements to the server administration user experience.

Various bug fixes in desktop syncing.

Improvements to the client installer upgrade process.

activEcho 2.0.0 (Released: February 2012)

Initial release

15.2.2 mobilEcho

Files Advanced Server 6.0

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**. For the latest information, please visit the What' New in Files Advanced Server (S. 322) article.

mobilEcho 5.1.0

VERBESSERUNGEN

- 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

- 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.

mobilEcho 5.0.3

BUG-FIXES

- 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.

mobilEcho 5.0.2

VERBESSERUNGEN

- Die Ordnerliste auf der Seite 'Datenquellen' zeigt den zugewiesenen Gateway Server jetzt mit seinem Anzeigenamen anstatt mit der IP-Adresse an.

BUG-FIXES

- 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“)

mobilEcho 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.

mobilEcho 5.0

VERBESSERUNGEN

- Der mobilEcho Client Management Server ist in Files Advanced 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 Files Advanced 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 Files Advanced 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 Files Advanced 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

- 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.

mobilEcho 4.5.2 (Released: October 2013)

ENHANCEMENTS:

Added support for smart card authentication, and added a setting to allow or disallow clients using this new authentication method.

mobilEcho 4.5.1 (Released: September 2013)

ENHANCEMENTS:

The mobilEcho server now supports requiring that mobilEcho Android clients are managed by MobileIron AppConnect.

BUG FIXES:

Fixed an issue where clients could time out trying to connect to a server if mobilEcho was configured to enumerate site collections.

Fixed an issue where the mobilEcho server selected when configuring a custom home directory path could fail to save properly when saving a user or group profile.

mobilEcho 4.5 (Released: August 2013)

ENHANCEMENTS:

Added support for giving access to SharePoint Online for Office 365.

Added the ability to enumerate and browse into individual SharePoint site collections.

Added support for client certificate authentication to mobilEcho file servers.

Added profile options to enable or disable the client's ability to edit text and/or Office files, to configure an auto-sync interval, and to automatically sync a user's home folder.

Increased the maximum volume name length to 127 UTF-8 characters to allow for longer volume names when using Unicode characters.

Added separate columns to the exported .csv devices list for display name and common name to make the usernames more clear.

BUG FIXES:

Fixed an issue where the exported .csv devices list would display the domain name incorrectly if the domain name contained numerical characters.

Fixed an issue where the server would respond incorrectly to a client request to delete a folder that was the root of an SMB share.

Fixed an issue where network path mapping could fail if two path mappings were created for two similar paths (e.g. \\server\vol and \\server\vol2).

mobilEcho 4.3.2 (Released: April 2013)

BUG FIXES:

Fixed an issue where mobilEcho Administrator could fail to create an activEcho volume when the product is licensed with a Retail serial number.

Fixed an issue where a mobilEcho client could fail to open its home directory if the home directory is configured using the %USERNAME% wildcard and the server domain and the user's domain have a trust relationship.

Fixed an issue where the server could incorrectly send an error message to Android clients when those clients attempted to obtain their profile.

mobilEcho 4.3.1 (Released: April 2013)

ENHANCEMENTS:

The mobilEcho server now supports mobilEcho clients that identify themselves using a custom device identifier, rather than Apple's device identifier.

BUG FIXES:

Fixed an issue where the Users and Groups pages of the mobilEcho Client Management web console could load very slowly if there were a large number of configured profiles.

Fixed an issue where the enrollment link in client enrollment invitation emails could fail to open properly on Android clients.

Fixed an issue where iOS clients could fail to connect to the server after upgrading from 4.0.1 server or earlier to 4.3 server.

mobilEcho 4.3 (Released: March 2013)

ENHANCEMENTS:

The mobilEcho server now supports mobilEcho clients with optional support for MobileIron AppConnect activated. The server now allows administrators to require or restrict mobilEcho access to iOS clients with AppConnect enabled. This setting is located in the "Settings" window of the "mobilEcho Administrator" application, on the "Security" tab.

BUG FIXES:

Fixed an issue where clients upgrading from mobilEcho Server 4.0.x or earlier could incorrectly receive a "specified account does not have a management profile" error when attempting to retrieve their management profile.

Fixed an issue where the mobilEcho server's memory usage could increase if the "mobilEcho Administrator" was left open for a long period of time.

Fixed an issue where the client would fail to show an error or would show an incorrect error message if the user's AD account password had expired, or the account was locked out or disabled.

Fixed an issue where the server upgrade process could fail if mobilEcho had been installed to a non-system drive.

Fixed an issue where a JavaScript error would occur each time a user or group profile was added via the mobilEcho Client Management web console when using IE8.

mobilEcho 4.2 (Released: February 2013)

ENHANCEMENTS:

mobilEcho 4.2 servers now support mobilEcho 4.2 clients localized in German, French and Japanese. The 4.2 server will ensure that these clients receive server error messages in their local language. In addition, the mobilecho_manager_intl.cfg file contains settings to configure the client enrollment invitation email subjects in these three languages.

The mobilEcho Client Management service will now automatically detect crashes in the client management web application and stop the service so that administrators can properly detect these errors. Additional error information will be written to the ManagementUI\log folder.

BUG FIXES:

Fixed a problem where the user could repeatedly be asked to enter proxy credentials when accessing the mobilEcho server through an HTTPS reverse proxy server.

Fixed a problem where the mobilEcho Client Management Server web UI could fail to restart because the client management database schema was not updated properly on upgrade. This would occur if the database was configured to be stored on a disk that was not available at upgrade time.

Sorting devices by "Last Contact" now sorts newest to oldest by default.

Fixed a problem where whitelists and blacklists could not be assigned when adding or editing a user or group profile.

Fixed a problem where files that were already on the device could sync again unnecessarily if the sync source was within an activEcho volume.

The password field on the login page of the client management web UI now has auto-complete disabled.

Removing a user or group profile now causes the name information for that user/group to be removed from cache. This ensures that re-adding a profile for that user/group will always force the management UI to retrieve the latest name from Active Directory.

Fixed a problem where "set the default file action" and "cache recently accessed files on this device" could be enabled in profiles after upgrading mobilEcho server.

Fixed a problem where the app password reset functionality in the management server UI might not work properly in Firefox.

Fixed a problem on the Invitations page of the client management server web UI where users within distribution subgroups could fail to be found in LDAP searches.

Fixed a problem where the server check for free disk space in a folder would incorrectly check the free space at the root of the mobilEcho volume.

Fixed a problem where open file handles would not be closed for 24 hours if a client disconnected in the middle of a file transfer. These handles will now be closed when the session times out, after 15 minutes.

Fixed a problem where the "Allow iTunes and iCloud to back up locally stored mobilEcho files" profile setting would always revert to enabled after saving management profile.

mobilEcho 4.1 (Released: December 2012)

ENHANCEMENTS:

Added an alternative client management server authentication mechanism so that mobilEcho clients that are configured to not save credentials for assigned servers and folders can authenticate to the management server to retrieve their profile without requiring their Active Directory password be stored on the device.

Modified the app password reset process. This was necessary to support the new custom on-device encryption that is included in the mobilEcho 4.1 client app. If a managed client forgets their app password, they now provide their administrator with a code generated by the app. The administrator enters this code into the mobilEcho Client Management web console and receives a second code that they give back to the client. This code allows the user to reset their app password and get into the app.

Enhanced the way resources (servers and folders) are provisioned to clients. Provisioned resources are no longer assigned directly to user/group profiles. Users or groups are now assigned directly to individual assigned resources and each user receives the full collection of resources assigned to their user account or a group they are a member of.

Added the ability to send up to three enrollment invitations to the same email address automatically for users with multiple devices.

Added a column to the LDAP search table for Distinguished Name so that users with the same name in different subdomains can be distinguished.

Added new management profile setting to allow or disallow users from opening and/or sending links to files.

Added client Good Dynamics status in the management server Devices list. Devices enrolled with Good Dynamics will no longer have the "Reset App Password" option available. The app password is managed within the Good Control console in this scenario.

BUG FIXES:

Fixed a problem where hiding inaccessible files on reshares when one of the volumes was a SharePoint volume could cause some of the volumes to fail to appear on the client.

Fixed a problem where the Client Management Administrator could fail to filter the devices or invitations tables, or could take a very long time to complete the filter. Filtering is now done without the need to perform additional LDAP requests.

Fixed a problem where attempting to read a file on an activEcho volume that no longer exists would result in a corrupted file being read rather than an error being returned.

Fixed a problem where the presence of a misconfigured or unavailable activEcho volume could cause clients to time out when attempting to retrieve the volume list.

Fixed a misleading message in the Client Management Administrator if a profile was configured to have 'App password must contain complex characters' greater than the 'Minimum password length'.

Fixed a problem when the client management server was configured to use a non-default port (i.e. not port 3000) and the server was upgraded. The first time the management server would run after upgrade it would attempt to use port 3000 rather than the configured port.

Modified the message in the Client Management Administrator when removing a currently managed client from the devices list to indicate that the client may automatically reenroll at a later time if enrollment PINs are not being used.

Fixed a problem where the Client Management Administrator could display an error if a profile was configured to use a home folder with an empty custom path.

Fixed a problem where 0-byte files would fail to download or sync with a "device not ready" error.

Content search is now automatically disabled on activEcho and SharePoint volumes since content search is not available.

Fixed a problem where users with email address beginning with underscore (e.g. "_user@example.com") could fail to receive enrollment invitations.

Client Management Administrator now returns a better error message than "unknown result" if the LDAP server requires SSL.

Fixed a problem where sessions could time out while downloading very large files.

Fixed a problem where configuring an assigned folder with an invalid path (e.g. "C:\foo\bar") could cause the Users page to show the error "can't modify frozen string".

Fixed a problem where selecting the "Reindex all volumes" button in the mobilEcho Administrator would generate an invalid error message.

Fixed a problem where filtering on a Unicode string in the Client Management Administrator could generate an "incompatible character encodings" error.

SharePoint "Wiki Page Gallery" libraries are now removed from site enumerations because they are not supported by mobilEcho.

Fixed a problem where new profile settings could become corrupted on upgrade.

Fixed a problem where a SharePoint document library volume would fail to work if the document library name was URL encoded, e.g. "My%20Library".

mobilEcho 4.0.3 (Release: October 2012)

ENHANCEMENTS:

Added support for SharePoint custom document libraries.

BUG FIXES:

Fixed a problem accessing SharePoint sites and document libraries whose paths are multiple levels below their parent site.

Fixed a problem accessing SharePoint sites that use Claims Based Authentication.

mobilEcho 4.0.2 (Released: September 2012)

ENHANCEMENTS:

Added support for Android clients.

Added settings to the mobilEcho Administrator for restricting access by iOS and/or Android clients.

Added support for sending enrollment instructions for iOS, Android and Good clients.

BUG FIXES:

Fixed a problem where exporting the devices list to a .csv file could result in a server error, or could result in some fields displaying as "Not found in AD".

Fixed a problem where non-Good clients could enroll with a management server that was configured to require clients be enrolled with Good Dynamics. Previously, clients could enroll, but would

receive an error when contacting the server to access data. Clients are now disallowed from enrolling in the first place.

mobilEcho 4.0.1 (Released: August 2012)

ENHANCEMENTS:

Added profile settings for "Number of days to warn of pending lock" and "Number of days to warn of pending wipe". These settings relate to existing settings that can wipe or lock the mobilEcho app if the device does not contact the management server for a specified period of time.

Added pagination, filtering and sorting to the Users and Groups pages within the mobilEcho Client Management server.

BUG FIXES:

Fixed a crash that could occur when attempting to authenticate with SharePoint volumes using Kerberos authentication.

Fixed a problem where users could fail to authenticate with SharePoint volumes if their user principal name (UPN) had a different domain than their Windows 2000 domain.

Fixed a problem where users could fail to authenticate with SharePoint volumes if their username contained Unicode characters and authentication was performed using NTLM.

Fixed a problem where users could fail to authenticate with SharePoint volumes if the user was a member of a subdomain and authentication was performed using NTLM.

SharePoint document libraries will now display all items, regardless of the settings of the library's default view.

The "Last Contact Time" column on the Devices page of the mobilEcho Client Management server now properly sorts by date.

Filters in the mobilEcho Client Management server now work properly with Unicode characters.

Filters in the mobilEcho Client Management server now "stick" after pagination settings are changed.

Disabled the "Indexed Search" and "Content Search" checkboxes when adding or editing reshare volumes in the mobilEcho Administrator, since search is not supported on those volumes.

The mobilEcho Administrator now automatically fills in the existing path when editing a SharePoint, activEcho or reshare volume path.

The mobilEcho server now returns a better error code if the user attempts to overwrite a file via Save Back that is checked out to another user.

mobilEcho 4.0 (Released: July 2012)

ENHANCEMENTS:

Added support for accessing data in SharePoint 2007 and 2010 document libraries.

The mobilEcho server can now simultaneously support activEcho and other volume types. Previous versions required switching into activEcho-only mode to access activEcho data.

Improved performance of the mobilEcho Client Management server by making LDAP queries "begins with" rather than "contains" by default. Administrators may choose "contains" when searching to obtain the previous behavior.

The mobilEcho Client Management server can now filter the invitations tables by username.

The mobilEcho Client Management server can now export the devices list to a .csv file.

The mobilEcho Client Management server now sorts and paginates the devices, users, groups and invitations tables.

Added a profile setting to allow/disallow users from creating bookmarks.

Added a profile setting to disable My Files while still allowing sync folders.

Added a profile setting to automatically lock the mobilEcho app or wipe all mobilEcho data if the device does not contact the management server for a specified period of time.

Added a profile setting to prevent users from setting an app password.

Files can now be copied within activEcho volumes by transferring data through the client.

Improved performance reading and writing to activEcho volumes.

BUG FIXES:

Fixed a problem where files and folders ending in a period or space could fail to be accessible on activEcho volumes.

Fixed a problem where the Devices page could fail to load in mobilEcho Client Management server after Japanese and Chinese users have enrolled.

mobilEcho 3.7 (Released: June 2012)

ENHANCEMENTS:

Improved performance of the mobilEcho Client Management server by caching user information to minimize the number of LDAP queries.

BUG FIXES:

Active Directory distribution groups are no longer found when searching for groups on the group profile page.

Fixed a problem when the path of a provisioned folder ends with a backslash.

mobilEcho 3.6.1 (Released: May 2012)

BUG FIXES:

Fixed a problem where files on an activEcho server could fail to preview, copy or sync.

Fixed a problem where users could fail to preview, copy or sync files in a home directory if the home directory was set up with a network reshare path mapping in the mobilEcho Client Management server.

Fixed a problem where users could fail to see their home directories if the client authenticated to the management server with a user principal name (UPN) such as user@domain.com.

Fixed a problem where the "%USERNAME%" wildcard would fail to use the correct username if the client authenticated to the management server with a user principal name (UPN) such as user@domain.com.

mobilEcho 3.6 (Released: April 2012)

ENHANCEMENTS:

Improved performance of Active Directory lookups for users and groups.

Searches of Active Directory in the mobilEcho Client Management server now search on both common names and display names.

Add profile settings for allowing/denying the ability of users to create sync folders, and to perform a Quickoffice® "Save Back".

The mobilEcho Client Management server can now be configured to store database and profile information in a different location than the application directory, allowing for the management server service to be failed over to other cluster nodes.

The mobilEcho Administrator now displays the number of licenses currently being occupied, and will only display a single session for each user/device if the user has reconnected to the mobilEcho server multiple times.

The mobilEcho Administrator now automatically runs with elevated privileges.

The enrollment email subject can now be customized in the 'mobilEcho_management.cfg' file.

BUG FIXES:

mobilEcho no longer permits Active Directory "Distribution" groups to be used to create mobilEcho Client Management group policies. Distribution groups are provided by Microsoft for email purposes only. If you are using AD "Distribution" groups for any of your mobilEcho Client Management policies, please use the "Active Directory Users and Computers" control panel to convert these groups to "Security" groups.

Fixed a problem where a user that used different username formats to enroll with multiple devices would occupy multiple licenses. For example, if one device was enrolled as "user@example.com" and a second device was enrolled as "example\user", the licensing logic would treat those as two separate user accounts for licensing purposes.

Fixed a problem where a user could fail to get the appropriate group profile if the user's Active Directory primary group was not set to the default of "Domain Users".

Fixed a problem where a user could fail to get the appropriate group profile if the user's group was a "universal" Active Directory group.

Fixed a problem where users with Unicode characters in their usernames would not have their credentials saved after enrolling with mobilEcho Client Management.

Fixed a problem where the server could allow mobilEcho clients to overwrite files that were flagged as read-only.

Fixed some mobilEcho Client Management display issues on Mac Safari.

Fixed a problem where Verizon iPad 3 devices were displayed as "AT&T" (and vice versa) in the mobilEcho Client Management devices page.

Fixed a problem where the mobilEcho Administrator could crash when viewing the list of connected users.

Fixed a problem where the invitation email would fail to show the username.

mobilEcho 3.5 (Released: February 2012)

ENHANCEMENTS:

Added support for 2-way sync folders. Client-side changes made in 2-way sync enabled folders will be synced back to the server automatically. These 2-way sync folders can be provisioned through the mobilEcho Client Management server.

Added support for reverse proxy authentication. Reverse proxy servers, such as Microsoft Forefront Threat Management Gateway (TMG), can be configured to require authentication before granting access to internal network resources. The mobilEcho client now supports both HTTP username/password and SSL Client Certificate authentication methods. To use SSL Client Certificate authentication, a certificate must be installed in the mobilEcho keychain. See this Knowledge Base article for more information: http://support.grouplogic.com/?p=3830

Added additional options for configuring mobilEcho device enrollment requirements. mobilEcho can now be optionally configured to accept enrollment requests from devices without the need for a one-time PIN. In addition, when mobilEcho is configured to require such PINs, these PINs can be viewed within the management interface.

Added support for client app whitelisting and blacklisting. A managed mobilEcho client can be configured so that files can only be opened into a restricted whitelist or blacklist of third-party iOS apps.

Improved browsing performance of network reshare volumes by disabling the filtering of inaccessible file and folders by default on such volumes.

Added support for network reshare to SMB/CIFS volumes on NetApp storage.

Added the ability to configure mobilEcho provisioned folder paths that include a username wildcard.

Added the ability to configure mobilEcho home folders with custom paths. These paths may include a username wildcard.

mobilEcho no longer requires that users have "list folder" permissions at the root of a share containing their home folder.

Added a new registry setting to control whether or not hidden shares on a network reshare are visible to mobilEcho clients. To enable this feature, set the following registry setting to 1:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\mobilEcho\Parameters4\Refreshable\Pez\GetShowHiddenSMBShares

BUG FIXES:

Fixed a problem where the mobilEcho Client Management server would appear to allow access without a proper username and password.

Fixed a problem where files would incorrectly require a sync after a change in daylight savings time.

Fixed a problem where renamed files would continue to be returned in search results when searching under the old filename. This problem would only occur for volume that were configured to use "indexed search" (not Windows Search).

Fixed a problem where mobilEcho could fail to install or run on systems missing a system DLL (normaliz.dll).

Fixed a problem where the client could fail to copy a file to the server if the user account did not have permission to calculate the amount of free space on the volume. The client would report an error about there not being enough free space on the volume.

Removed extraneous logging from the mobilEcho LOG.TXT file.

Fixed a problem where folders could not be provisioned for servers whose display name contained parentheses.

mobilEcho 3.1 (Released: November 2011)

ENHANCEMENTS:

Client management profiles can now be configured with the following new settings:

- The number of incorrect app password attempts that can be made before the local data within the mobilEcho app is automatically wiped. This feature is disabled by default.
- Whether the user is required to confirm before syncing occurs (options are: "Always", "Never", and "Only on 3G").
- Whether syncing is allowed any time, or only while on WiFi networks.
- Client timeout for unresponsive servers now accepts additional values of 90, 120 and 180 seconds.

The mobilEcho Client Management server can now be configured to communicate with Active Directory via secure LDAP.

Profiles now default to allow files to be cached on the local device. If caching is disabled or if the "Allow files to be stored on this device" setting is disabled, no files will be cached.

The text of enrollment invitation emails can be customized. Please visit the GroupLogic Knowledge Base for more information: http://support.grouplogic.com/?p=3749

Added a setting to the management configuration file to control the name that enrollment invitation emails appear from (e.g. "mobilEcho Invitation <mobilEcho_invitation@example.com>". Version 3.0 only allowed an address to be specified (e.g. "mobilEcho_invitation@example.com").

The VALID_LOGIN_NAMES field of the management configuration file now supports Active Directory groups in addition to specific users that can administer the mobilEcho Client Management service.

Changing SMTP settings within the management configuration file no longer requires a restart of the mobilEcho Client Management service.

Profiles for users and groups that no longer exist in Active Directory are now marked as such in the mobilEcho Client Management service.

Added the ability to show inaccessible items only on reshare volumes. This can be useful in cases where determining file and folder accessibility is causing performance problems. This behavior can be adjusted by modifying the following registry setting and restarting the service:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\mobilEcho\Parameters4\Refreshable\Pez\HideInaccessibleItemsOnReshares

BUG FIXES:

Fixed a problem where the mobilEcho Client Management server would not properly calculate an Active Directory home directory path if the associated 'Network reshare path mapping' included a trailing backslash.

Fixed a problem where the mobilEcho Client Management server would not properly calculate an Active Directory home directory path that only included a server and share name. (i.e. \\servername\sharename)

Fixed a problem that could prevent network reshare volumes configured with paths to the root of a server (i.e. \\servername) from appearing properly in the mobilEcho client.

mobilEcho clients now always log into provisioned servers using fully qualified domain accounts. In previous versions of mobilEcho, the credentials entered at enrollment time would be used to authenticate with file servers, even if these credentials did not include a domain name (e.g. domain\user). This could cause problems if the provisioned server was on a different domain than the management server and access to the server in the secondary domain relied on a domain trust with the primary domain. This behavior can be reverted to the previous default by setting the following registry value to 0 and restarting the service:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\mobilEcho\Parameters4\Refreshable\Pez\DomainAndUsernameShouldBeSentToClient

Fixed a problem where the mobilEcho Client Management server did not properly sort "Last contact date" properly on the Devices page.

Fixed a problem in the mobilEcho Administrator where the Help button would not adjust properly as the Users window was resized.

mobilEcho 3.0 (Released: October 2011)

ENHANCEMENTS:

Centrally managed device enrollment. Client enrollment invitations are now generated and emailed to the user from the mobilEcho Client Management Administrator. These invitations include a one-time use PIN number required for client enrollment.

Remote wipe and remote reset of app passwords is now performed on a per-device basis.

Individual device status is now displayed in the mobilEcho Client Management Administrator. This includes device user name, device name, device type, iOS version, mobilEcho version, mobilEcho status, last contact time.

Users' Active Directory assigned network home folders can now be automatically displayed in the mobilEcho client app.

Specific mobilEcho shared volumes or folders within shared volumes can now be assigned to user or group profiles. These shared volumes or folders are then automatically displayed in the mobilEcho client app.

Shared volumes or folders assigned to user or group profiles can be configured to automatically one-way sync from server to mobilEcho client, making the contained files available for online or offline use.

BUG FIXES:

Fixed a problem where the mobilEcho server would not properly report free space for server-to-server copies.

Improved error messages and processing if a user attempts to copy or move files into the root of a network reshare.

Fixed a problem where a user could be authenticated with AD by contacting mobilEcho via a web browser. This could cause a user account to become locked.

Improved the speed of installation, particularly for upgrades.

Fixed a problem where files and folders ending a period or space could fail to copy properly.

Fixed a problem logging into the management UI with a username containing numbers, e.g. "e12345".

Updated OpenSSL library to latest version. OpenSSL libraries are used for encryption.

mobilEcho 2.1.1 (Released: July 2011)

BUG FIXES:

Fixed a bug when listing the contents of folders which may have resulted in slow performance or client timeouts if many of the folders were not accessible to the client.

mobilEcho 2.1.0 (Released: July 2011)

ENHANCEMENTS:

Added the ability to create mobilEcho shares that reshare data on a remote system. The mobilEcho reshare feature is only available for customers with an enterprise license. Reshares can be a particular share (e.g. "\\server\share") or an entire server ("\\server\").

The mobilEcho client can now perform copy and move operations on folders when connected to a server running mobilEcho Server 2.1 or later, and the management UI now has settings to allow or disallows these operations.

The management UI now has the ability to add a new group or user using settings from an existing user or group.

Management profiles can now be disabled so that the corresponding user or group cannot receive their profile.

Added the ability to prevent clients from connecting to servers with self-signed certificates.

Added a management setting to enable or disable copying text from a previewed document.

Added a management setting that tells the client to store files so that they are not backed up by iTunes.

mobilEcho 2.0.0 (Released: May 2011)

ENHANCEMENTS:

Added the ability to manage mobilEcho clients using server-defined profiles using mobilEcho Client Management.

Added the ability to reset mobilEcho app passwords from the server.

Added the ability to force a remote wipe for a particular mobilEcho user.

mobilEcho will now use an internal filename index for satisfying search requests if Windows Search is not installed or available.

The mobilEcho administrator now allows for volumes to be seamlessly replicated from SMB and/or ExtremeZ-IP shares.

mobilEcho 1.0.0 (Released: January 2011)

Initial release.

16 Dokumentation für ältere Versionen

Informationen zu älteren Versionen der Files Advanced-Dokumentation finden Sie unter folgendem Link:

Hinweis: *Für ältere Dokumentationen ist Ihre bevorzugter Sprache möglicherweise nicht verfügbar.*

- 8,1.x
- 8,0.x
- 7,5.x
- 7,4.x
- 7,3.x
- 7,2.x
- 7,1.x
- 7,0.x http://www.acronis.com/en-us/support/documentation/AcronisAccessAdvanced_7.0/index.html#26894.html
- 6,0.x http://www.acronis.com/en-us/support/documentation/AAS6.0/index.html#26894.html
- 5.0.x