Acronis

acronis.com

Acronis Cyber Files

9.0

Administratoranleitung

REVISION: 01.10.2024

Index

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

Z

Inhaltsverzeichnis

Die Verwendung dieser Hilfe

Diese Hilfe passt sich dynamisch an das Gerät an, mit dem Sie die Hilfe anschauen.

Desktop-Geräte und Laptops

Durch die Inhalte navigieren

Auf Desktop-Geräten und Laptops ist der Fensterbereich 'Navigation' (kurz: Navigationsbereich) standardmäßig erweitert und die Registerkarte **Inhalte** ausgewählt, sodass Sie die Hierarchie der Themen direkt sehen und im Inhalt navigieren können.

Wenn Sie den Fensterbereich 'Navigation' während des Lesens ausblenden wollen, klicken Sie im oberen Bereich des Fensterbereichs auf .

Der Fensterbereich wird eingeklappt und stattdessen eine Schaltfläche zum Erweitern () auf der linken Seite Ihrer Anzeige eingeblendet.

Index und Glossar

Der Index und das Glossar werden auf separaten Registerkarten im Navigationsbereich auf der linken Seite angezeigt.

Suchen

Die Suche in der oberen rechten Ecke liefert nur Ergebnisse aus Themeninhalten. Wenn Sie den Index oder das Glossar durchsuchen wollen, müssen Sie die Registerkarte wechseln und die Registerkarte 'Suche' verwenden.

Mobilgeräte

Durch die Inhalte navigieren

Auf Mobilgeräten ist der Navigationsbereich standardmäßig ausgeblendet und wird die Willkommensseite angezeigt. Sie können die Pfeile oben rechts verwenden, um zum nächsten oder vorherigen Thema zu wechseln.

Wenn Sie das Inhaltsverzeichnis einsehen wollen, klicken Sie oben links auf die Menüschaltfläche und wählen Sie **Inhalte**.

Index und Glossar

Auf den Index und das Glossar kann über das Menü im oberen linken Bereich der Anzeige zugegriffen werden.

Suchen

Die Hauptsuche liefert nur Ergebnisse aus den Themeninhalten. Wenn Sie den Index oder das Glossar durchsuchen wollen, müssen Sie über das Menü oben links die Registerkarte wechseln und die Registerkarte 'Suche' verwenden.

Bei der Suche wird nicht zwischen Groß- und Kleinschreibung unterschieden.

Wenn Sie nach einem bestimmten zusammenhängenden Ausdruck (Phrase) suchen wollen, müssen Sie diesen in Anführungszeichen setzen. Wenn Sie mit mehreren Wörtern suchen und diese nicht in Anführungszeichen einschließen, wird der boolesche Operator 'AND' angewendet. Wenn Sie beispielsweise nach `"Backup planen"` suchen, werden im Suchergebnis alle Themen angezeigt, die den kompletten Ausdruck "Backup planen" in genau dieser Reihenfolge enthalten (wobei nicht zwischen Groß- und Kleinschreibung unterschieden wird). Wenn Sie dagegen mit `Backup planen` (also ohne Anführungszeichen) suchen, wird diese Suchanfrage so interpretiert, dass Sie nach den unabhängigen Worten 'Backup' UND 'planen' suchen. In diesem Fall enthalten die Suchergebnisse alle Themen, die die beiden Wörter 'Backup' und 'planen' enthalten, egal wie deren deren Position zueinander ist.

Sie können nicht nach Wortteilen suchen.

Sie können boolesche Operatoren verwenden, um Ihre Suchergebnisse einzugrenzen oder zu erweitern:

- AND – findet nur Themen, die alle aufgeführten Wörter gemeinsam enthalten. Ein Leerzeichen zwischen den Wörtern wird immer als AND interpretiert, außer Sie schließen die Suchbegriffe in Anführungszeichen ein. Anführungszeichen bedeuten also, dass Sie nach einem zusammenhängenden Ausdruck (einer Phrase) suchen.
- OR – wird verwendet, um Themen zu finden, die irgendeines der aufgeführten Wörter enthalten. Dieser Operator erweitert die Suchergebnisse.

Bei den booleschen Operatoren wird nicht zwischen Groß- und Kleinschreibung unterschieden. Ob Sie also beispielsweise `AND` oder `and` in Ihrer Suchanfrage verwenden, hat keinen Einfluss auf das Suchergebnis.

Einführung

Diese Anleitung bietet Dokumentation für Acronis Cyber Files-Administratoren.

Über Cyber Files

Cyber Files ist eine sichere Access Sync & Share-Lösung, die IT-Abteilungen in Unternehmen die vollständige Kontrolle über die entsprechenden Geschäftsinhalte ermöglicht. Dabei wird volle Sicherheit, die Einhaltung von Vorschriften sowie die Nutzung privater Geräte am Arbeitsplatz (BYOD) gewährleistet. Mit Cyber Files können Mitarbeiter jedes Gerät (z. B. Desktop, Laptop, Tablet oder Smartphone) verwenden, um sicher auf Inhalte zuzugreifen und diese mit autorisierten internen und externen Personen (wie Mitarbeitern, Kunden, Partnern und Lieferanten) zu teilen.

Die Funktionalität von Cyber Files kann in zwei Kategorien unterteilt werden.

Zugriff auf Mobilgeräte

Der Zugriff auf Mobilgeräte ermöglicht es 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 anzubieten und zu verhindern, dass die Mitarbeiter riskante verbraucherbasierte Dienste und andere nicht richtlinienkonforme Alternativen verwenden.

Dank Cyber Files 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.

Hinweis

Weitere Informationen zum Zugriff auf Mobilgeräte finden Sie in der folgenden Dokumentation:

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

File Sync & Share

Die „Sync & Share“-Funktionalität ist die branchenweit einzige Unternehmenslösung, die ein Gleichgewicht zwischen dem Bedürfnis der Endbenutzer nach Einfachheit und Effektivität und dem Bedarf der Unternehmens-IT an Sicherheit, Beherrschbarkeit und Flexibilität schafft.

Mit Cyber Files kann die Unternehmens-IT steuern, wer auf Dateien zugreifen kann, und feststellen, ob die gemeinsame Nutzung von Dateien den Regeln der Organisation entspricht. Außerdem ermöglicht Cyber Files einen Grad an Transparenz und besitzt Überwachungsfunktionen, die verbraucherbasierte Lösungen nicht zu bieten haben.

Schnellstartanleitung

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

Installation

Hinweis
Sie müssen als Administrator angemeldet sein, um Acronis Cyber Files installieren zu können.

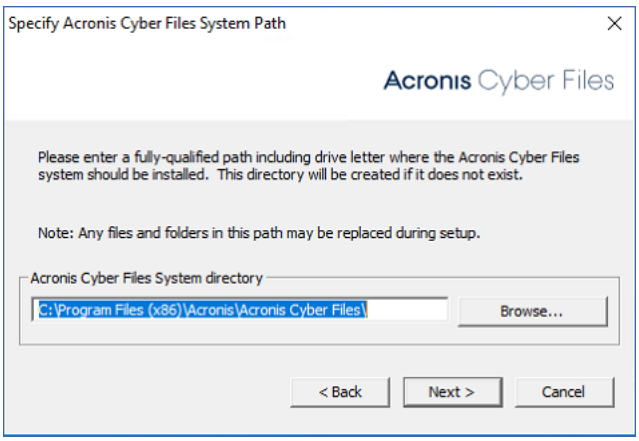
Hinweis
Acronis Cyber Files 8.8 wird standardmäßig zusammen mit PostgreSQL 11 verteilt.

Das Installationsprogramm verwenden

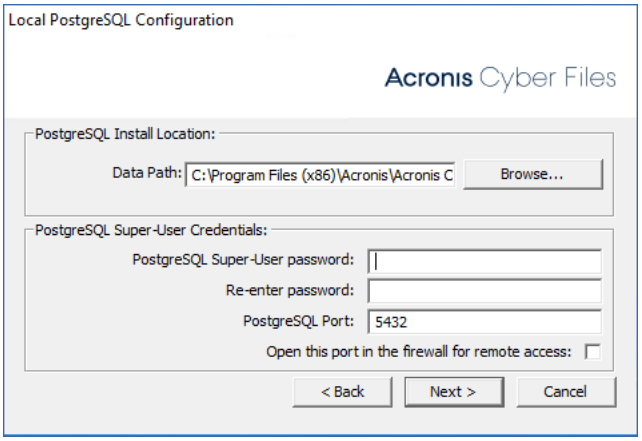
1. Laden Sie das Installationsprogramm für Acronis Cyber Files herunter.
2. Deaktivieren Sie alle vorhandenen Virenschutzprogramme, da sie unter Umständen den Installationsvorgang unterbrechen und somit eine fehlerhafte Installation verursachen können.
3. Doppelklicken Sie auf die Installationsdatei.

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 Acronis Cyber Files 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. Ein Fenster wird geöffnet, in dem alle zur Installation ausgewählten Komponenten angezeigt werden. Klicken Sie auf **OK**, um fortzufahren.
10. Klicken Sie nach Abschluss des Acronis Cyber Files-Installationsprogramms auf **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 wählen Sie 'OK', um Acronis Cyber Files aufzurufen.

Die Ersteinrichtung

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

Hinweis
Nach der Ausführung des Konfigurationswerkzeugs dauert es 30 bis 45 Sekunden, bis der Server erstmalig angezeigt wird.

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

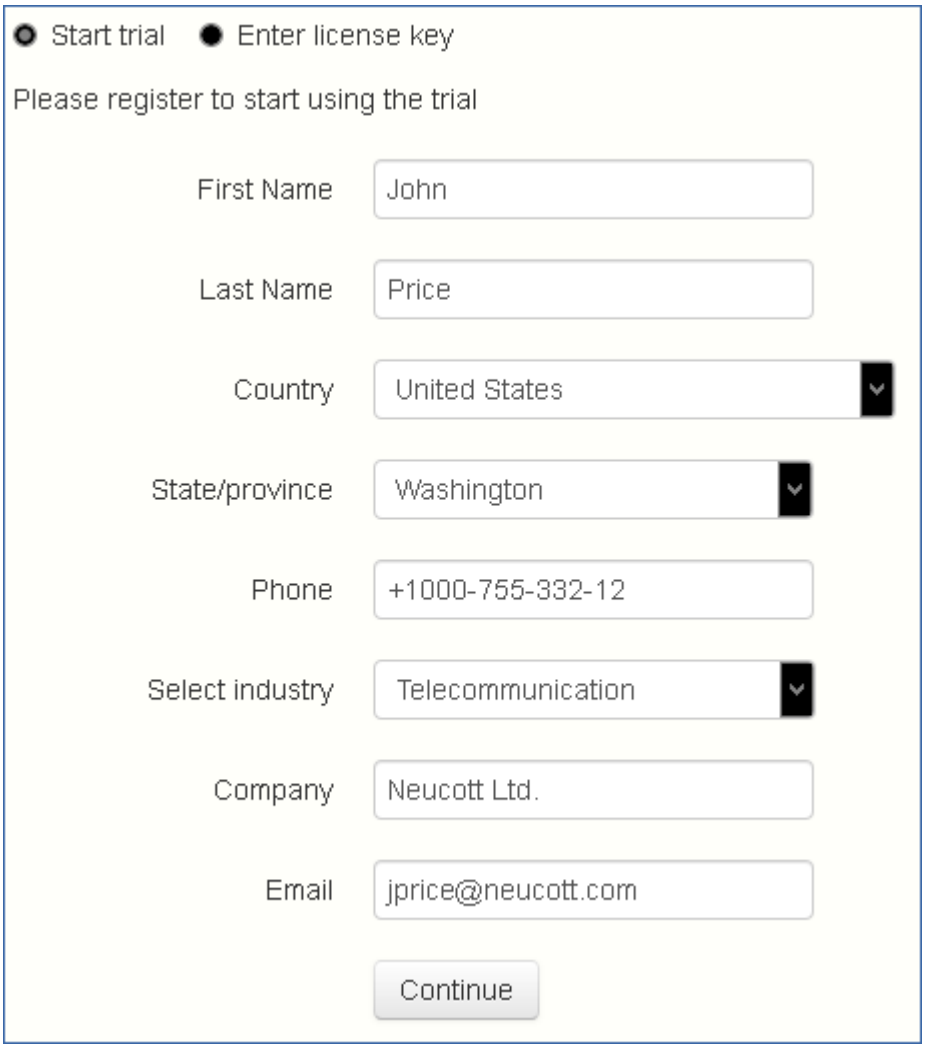
Hinweis
Wenn Sie Acronis Cyber Files mit den Standardzertifikaten ausführen anstatt Zertifikate einer Zertifizierungsstelle zu verwenden, wird ein Fehler angezeigt, dass der Server nicht vertrauenswürdig ist.

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.

Lizenzierung

So starten Sie eine Testversion:

Wählen Sie **Test starten**, geben Sie die erforderlichen Informationen ein, und wählen Sie dann **Weiter**.

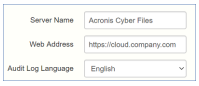


So lizenzieren Sie Ihre Acronis Cyber Files-Instanz:

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

3. Drücken Sie **Speichern**.

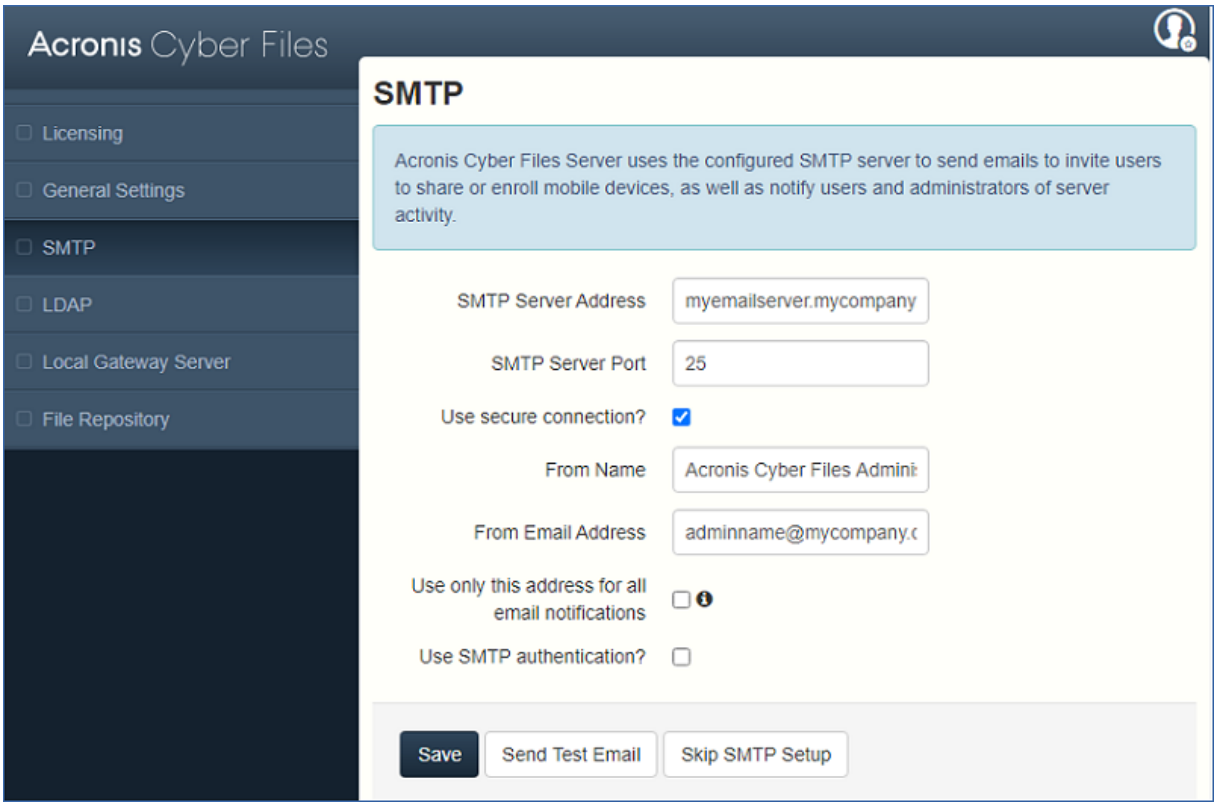
Allgemeine Einstellungen



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://).

   Wählen Sie die Standardsprache für das **Überwachungsprotokoll** aus.
3. Die aktuellen Optionen sind **Deutsch, Englisch, Französisch, Japanisch, Italienisch, Spanisch, Tschechisch, Russisch, Polnisch, Koreanisch, vereinfachtes und traditionelles Chinesisch**.
4. Drücken Sie **Speichern**.

SMTP

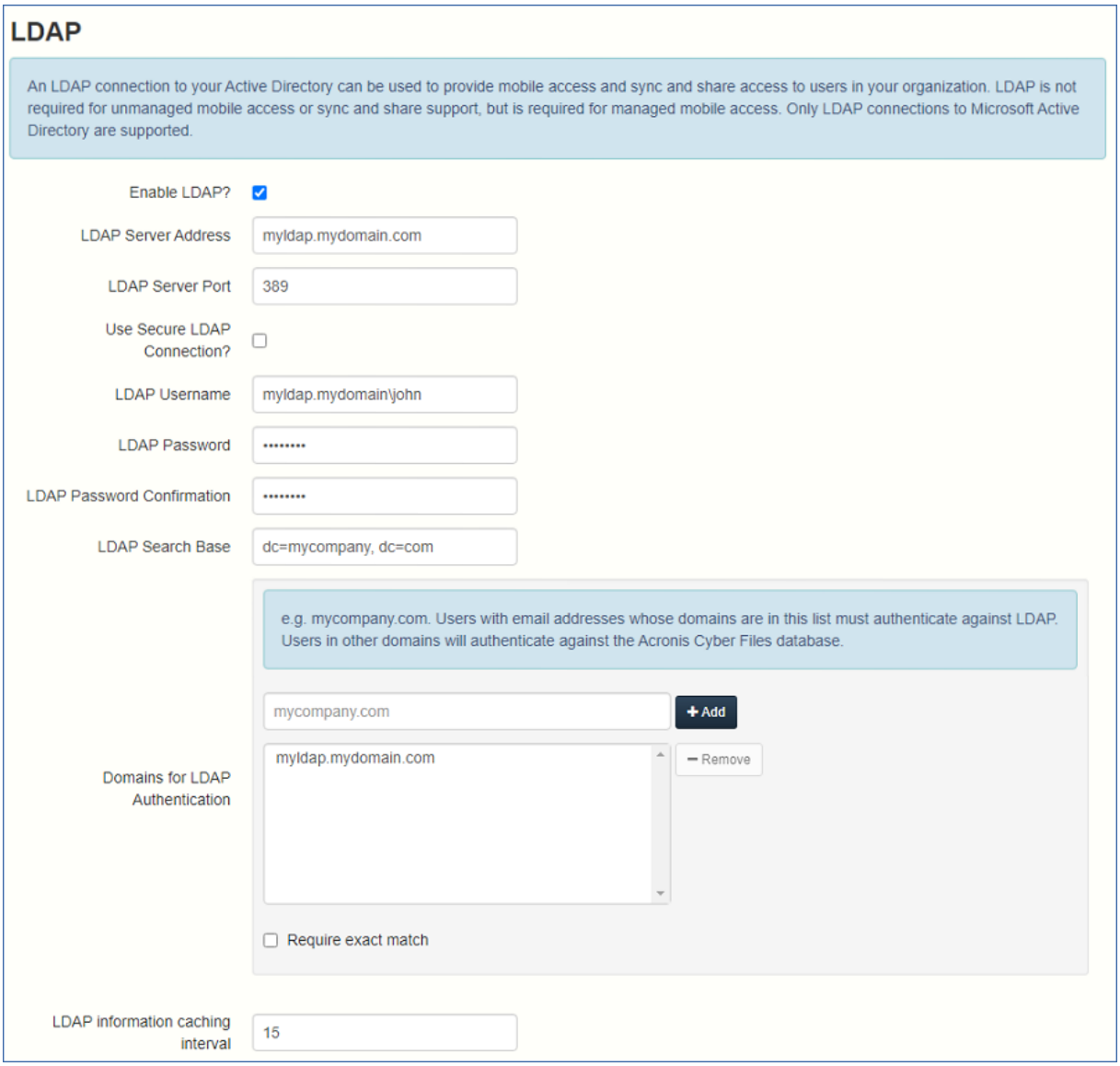


Hinweis
Sie können diesen Abschnitt überspringen und SMTP später konfigurieren.

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 Anmeldedaten 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 Acronis Cyber Files 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. (Für ein Konto mit der E-Mail-Adresse **joe@glilabs.com** würden Sie zur LDAP-Authentifizierung beispielsweise **glilabs.com** eingeben.)
8. Geben Sie die gewünschte(n) Domain(s) für die LDAP-Authentifizierung ein.
9. Drücken Sie **Speichern**.

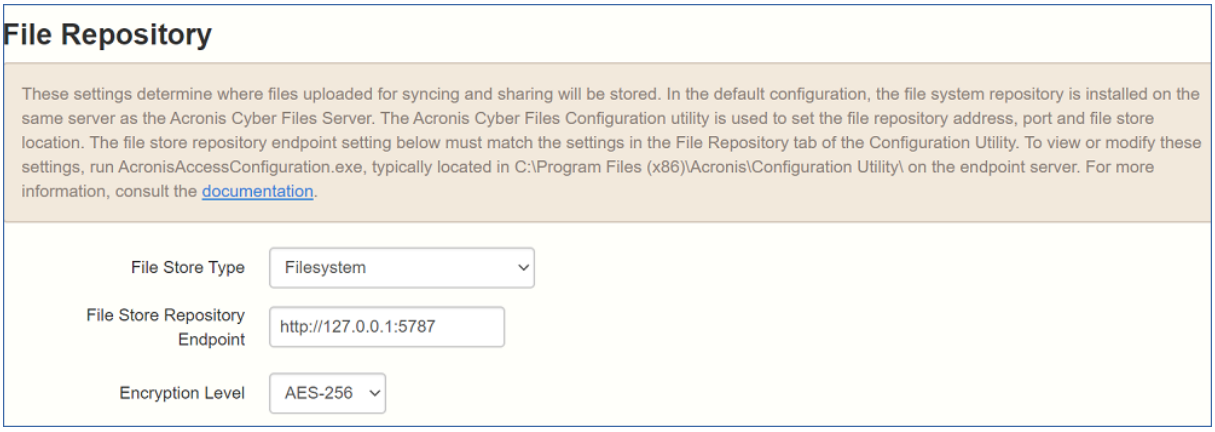
Lokaler Gateway Server

Damit KCD über mobile Clients funktioniert, ist eine Registrierung beim lokalen Gateway (das auf demselben Computer wie Tomcat installiert ist, der es verwaltet) erforderlich. Das Gateway leitet diese Anforderungen anschließend an diesen Tomcat-Server (für die Verwaltung) weiter.

Hinweis
Wenn Sie einen Gateway Server und den Acronis Cyber Files Server auf derselben Maschine installieren, wird der Gateway Server automatisch erkannt und vom Acronis Cyber Files 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



Wählen Sie einen File Store-Typ aus. Verwenden Sie **Dateisystem** für einen File Store auf Ihren Computern oder eine der folgenden Optionen für einen File Store in der Cloud: **Acronis Storage**, **Microsoft Azure Storage**, **Amazon S3**, **Swift S3**, **Ceph S3** und **andere S3-kompatible Speicherlösungen**.

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.

Hinweis
MinIO S3-Storage wird als Typ unterstützt und kann mit der Option **Anderer S3-kompatibler Storage** konfiguriert werden, er wird jedoch nicht über eine unsichere HTTP-Verbindung unterstützt.

1. Geben Sie den DNS-Namen oder die IP-Adresse des Datei-Repository-Dienstes ein.

   Hinweis
   Mit dem Cyber Files-Konfigurationswerkzeug werden die Adresse des Datei-Repository, der Port und der Speicherort festgelegt. Die Einstellung 'File Store-Repository-Endpunkt' muss den Einstellungen auf der Registerkarte 'File Repository' des Konfigurationswerkzeugs entsprechen. Um diese Einstellungen einsehen oder ändern zu können, müssen Sie 'AcronisAccessConfiguration.exe' ausführen (typischerweise auf dem Endpunkt-Server im Verzeichnis `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\Configuration Utility` zu finden).

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

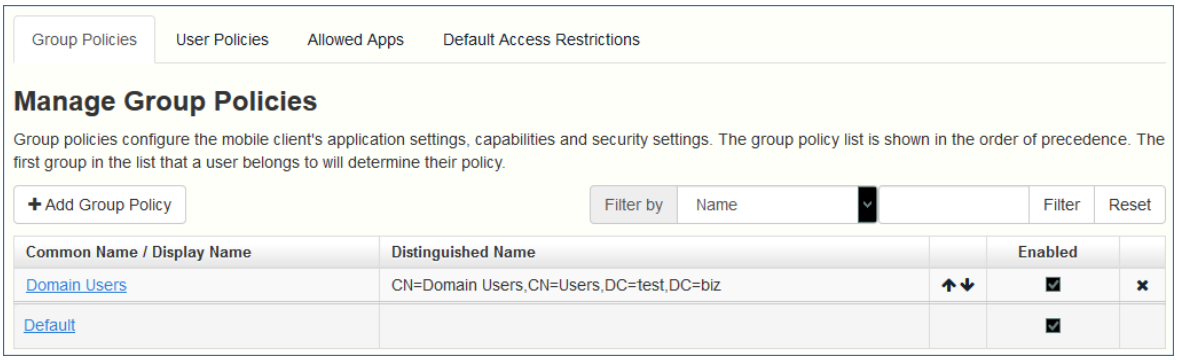
Mobiler Zugriff

Konfigurieren der Standardrichtlinie

Alle mobilen Clients, die für die Verwaltung mit dem Acronis Cyber Files 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.

Konfigurieren der Standardrichtlinie

1. Öffnen Sie die Acronis Cyber Files-Webkonsole.
2. Navigieren Sie zu **Mobile Access**-> **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.

Mobile Clients

Bei der ersten Ausführung der Acronis Cyber Files-App 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 Acronis Cyber Files-App auch dann ausprobieren, wenn ihr Unternehmen nicht über einen Acronis Cyber Files-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 Verwaltungsservers nicht vertrauenswürdig ist. Um diese Warnung zu akzeptieren und fortzufahren, können Sie auf **Immer fortsetzen** klicken.
6. Wenn für die mobile Acronis Cyber Files-App ein Kennwort zum Sperren der Applikation erforderlich ist, werden Sie aufgefordert, eines festzulegen. Möglicherweise gelten auch Anforderungen bezüglich der Komplexität des Kennworts. Diese werden gegebenenfalls angezeigt.

Wenn Ihre Verwaltungsrichtlinie das Speichern von Dateien in Acronis Cyber Files einschränkt oder Sie daran hindert, einzelne Server über die mobile Acronis Cyber Files-App hinzuzufügen, wird möglicherweise ein Bestätigungsfenster angezeigt. Falls Sie Dateien lokal in der mobilen Acronis Cyber Files-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.

Client-Anleitungen

Informationen zu Cyber Files-Clients finden Sie in den nachfolgenden Client-Anleitungen:

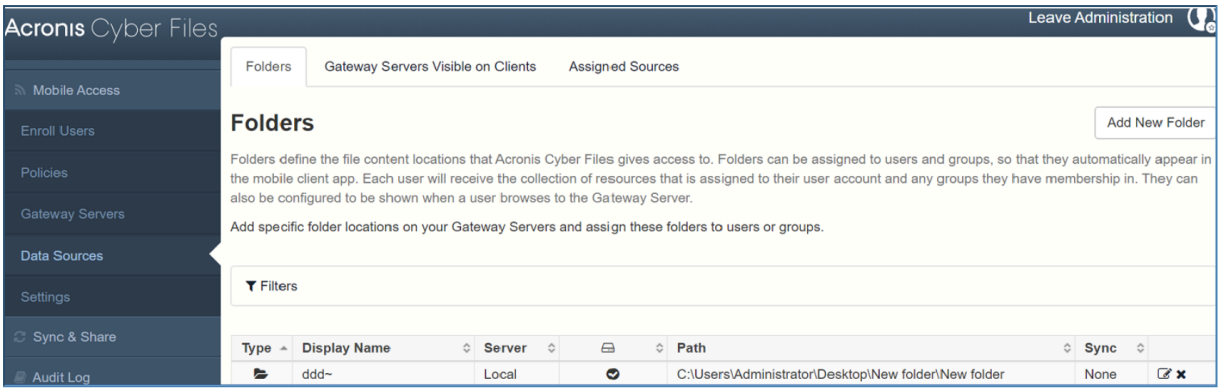
- Desktop- und Web-Clients
- iOS-App
- Android-App

Sync&Share

Sync&Share-Datenquelle

Sobald Sie AcronisCyber Files installieren und konfigurieren, wird automatisch eine Datenquelle mit dem Namen **Sync&Share** erstellt und die Gruppe **Domain-Benutzer** 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 **Domain-Benutzer** sind, und sie sind über mobile, Desktop- und Web-Clients erreichbar.

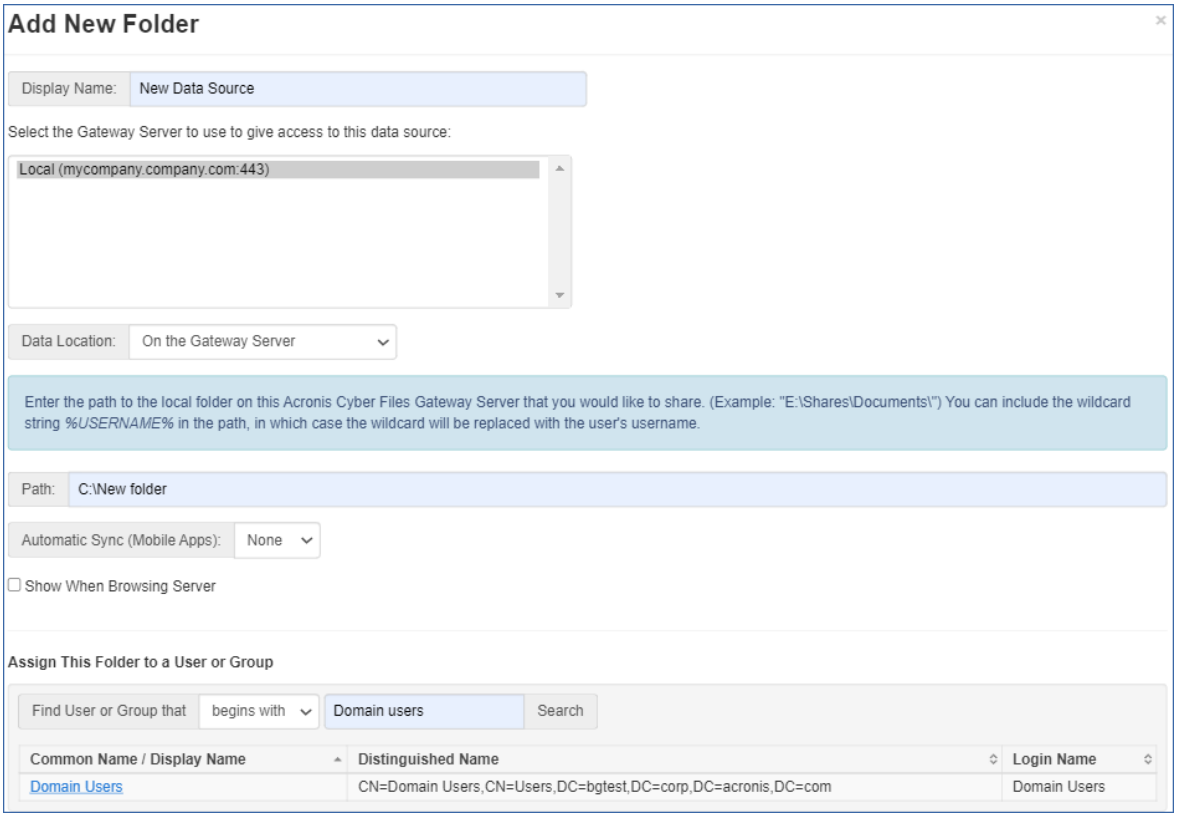


Freigeben von Inhalten für Ihre Benutzer

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

Erstellen einer Datenquelle

1. Öffnen Sie die Acronis Cyber Files-Weboberfläche.
2. Klicken Sie auf die Registerkarte **Mobile Access**.
3. Öffnen Sie die Registerkarte **Datenquellen**.
4. Wechseln Sie zu **Ordner**.
5. Klicken Sie auf **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
   Sie dürfen einen Ordner auf einem Wechselmedium nicht als freigegebenen Ordner verwenden. Wählen Sie einen Ordner von einem anderen Speicherort aus.

   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 **Sync**-Typ dieses Ordners.
11. Aktivieren Sie **Anzeigen, wenn Server durchsucht wird**, wenn diese Datenquelle beim Durchsuchen des Gateway Server durch mobile Acronis Cyber Files-Clients sichtbar sein soll.

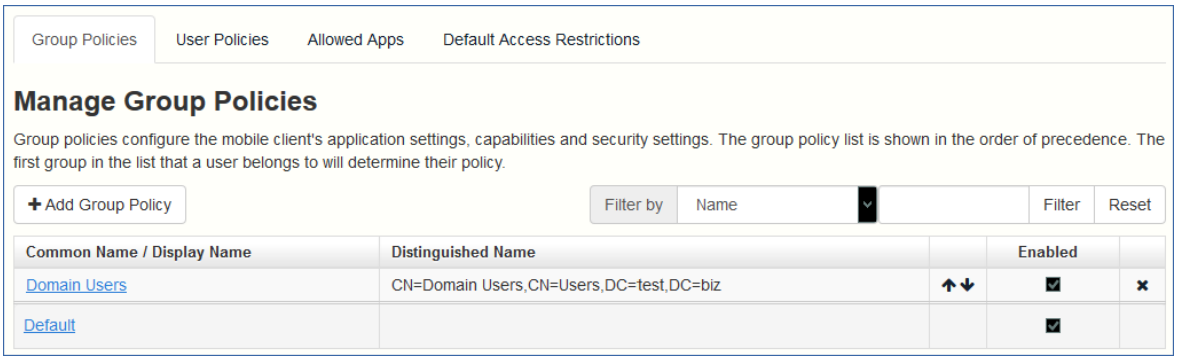
    Hinweis
    Beim Erstellen von SharePoint-Datenquellen haben Sie die Option, die Anzeige SharePoint-gefolgter Websites zu aktivieren.

12. Klicken Sie auf **Speichern**.

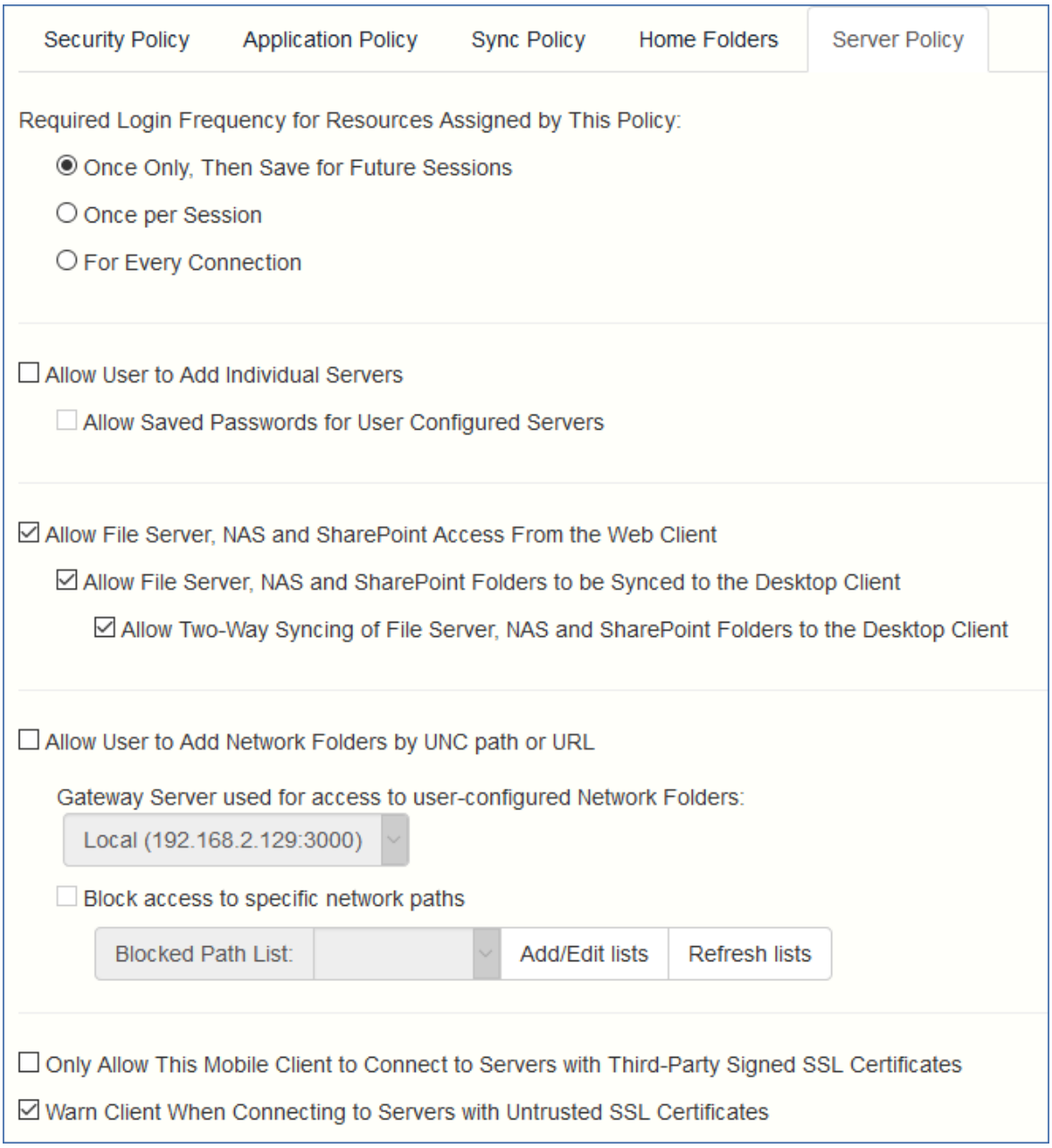
Erlauben des Zugriffs auf Dateiserver und mehr durch Web Client-Benutzer

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 **Mobile Access**--> **Richtlinien**. (Obwohl die Richtlinien primär mit den mobilen 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 erlauben**.



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-Ordnern zum Desktop Client erlauben** verwenden.
5. Klicken Sie auf **Speichern**.

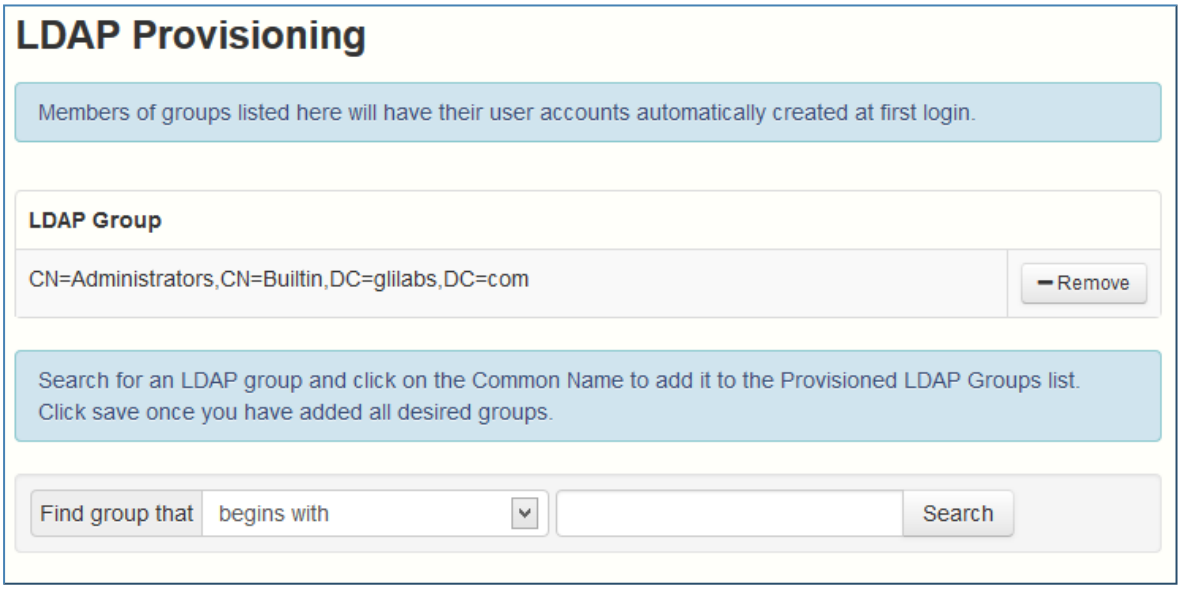
Dies wird als Richtlinieneinstellung implementiert, um mehr Flexibilität bereitzustellen. Möglicherweise möchten Sie die Einstellung auch für eine andere Gruppe oder für einzelne Richtlinien festlegen.

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. Öffnen Sie die Acronis Cyber Files-Webkonsole.
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 klicken Sie auf **Speichern**.

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

Web- und Desktop-Clients

- Der Web-Client unterstützt für alle Benutzer mit gültigen AcronisCyber Files -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.

Client-Anleitungen

Informationen zu Cyber Files-Clients finden Sie in den nachfolgenden Client-Anleitungen:

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

Installation

Anforderungen

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

Anforderungen an das Betriebssystem

Hinweis
Acronis Cyber Files 9.0 ist die letzte Version, die die Betriebssysteme Windows Server 2012 und Windows Server 2012 R2 unterstützt.

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

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

Empfohlen:

- Windows Server 2019 Standard und Datacenter

Unterstützt:

- Windows Server 2019 Standard und Datacenter
- Windows Server 2016 Standard und Datacenter
- Windows Server 2012 R2 Standard und Datacenter
- Windows Server 2012 Standard und Datacenter

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.

Voraussetzungen für mobile Clients

Unterstützte Mobilgeräte

- Apple-Geräte mit iOS oder iPadOS als Betriebssystem, die von Acronis Cyber Files unterstützt werden (wie unten aufgeführt).
- Geräte mit Android als Betriebssystem, die von Acronis Cyber Files unterstützt werden (wie unten aufgeführt).

Wichtig
Prozessoren der x86-Familie werden nicht unterstützt.

Mindestens unterstützte mobile Betriebssysteme

Hinweis
Bei Ivanti MDM- oder Microsoft Intune-Bereitstellungen hängt die Unterstützung der Betriebssystemversionen von der Unterstützung in den spezifischen SDK-Versionen ab, die in der Mobile Client App enthalten sind. Einzelheiten zu den SDK-Versionen finden Sie in den verlinkten Versionshinweisen.

- Für iOS oder iPadOS ist die niedrigste unterstützte Version die Version 14.
  Weitere Informationen zur Unterstützung neuerer Betriebssystemversionen finden Sie in den Release Notes zur Acronis Cyber Files App für iOS.
- Für Android ist die niedrigste unterstützte Version die Version 7.
  Weitere Informationen zur Unterstützung neuerer Betriebssystemversionen finden Sie in den Release Notes zur Acronis Cyber Files App für Android.

Downloads der Mobile App

- Für iOS.
- Für Android.

Hinweis
Die Standard- und MDM-Android-APK-Dateien können von der Produkt-Download-Seite heruntergeladen werden.

Minimale Hardware-Anforderungen

Beispielbereitstellungen

Diese Darstellungen gehen davon aus, dass alle Komponenten von Acronis Cyber Files 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
Acronis Cyber Files-Web-Server kann auf virtuellen Maschinen installiert werden.

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

Hinweis
Diese Werte sind unsere Anforderungen an eine Produktionsumgebung. Wenn Sie eine Testversion starten oder Acronis Cyber Files zu Testzwecken installieren wollen, können Sie mit den Hardware-Anforderungen für kleine Bereitstellungen beginnen und diese bei Bedarf erhöhen, abhängig von Ihrer Test-Auslastung.

Kleine Bereitstellungen

- Bis zu 25 Benutzer

  Hinweis
  'Benutzer' bezieht sich in diesem Zusammenhang auf die Gesamtmenge aller Benutzerkonten und Gruppenobjekte, die in der LDAP-Suchbasis enthalten sind, die Sie in Acronis Cyber Files unter **Allgemeine Einstellungen** > **LDAP** eingegeben haben.

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

Mittelgroße Bereitstellungen

- Bis zu 500 Benutzer

  Hinweis
  'Benutzer' bezieht sich in diesem Zusammenhang auf die Gesamtmenge aller Benutzerkonten und Gruppenobjekte, die in der LDAP-Suchbasis enthalten sind, die Sie in Acronis Cyber Files unter **Allgemeine Einstellungen** > **LDAP** eingegeben haben.

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

Große Bereitstellungen

- Bis zu 2.500 Benutzer

Hinweis
'Benutzer' bezieht sich in diesem Zusammenhang auf die Gesamtmenge aller Benutzerkonten und Gruppenobjekte, die in der LDAP-Suchbasis enthalten sind, die Sie in Acronis Cyber Files unter **Allgemeine Einstellungen** > **LDAP** eingegeben haben.

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

Hinweis
Bei Bereitstellungen mit mehr als 2500 Benutzern wird eine Cluster-Server-Konfiguration empfohlen.
Wenden Sie sich an den Acronis Support, wenn Sie Bereitstellungen für mehr als 2500 Benutzern planen.

Hinweis
Je nach Ihren Arbeitsabläufen und je nachdem, welche anderen Applikationen auf dem Server laufen, benötigen Sie möglicherweise wesentlich mehr Ressourcen.

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 Domain-Controller 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 usw.) weitergeleitet werden.
- Alle Computer, auf denen der Acronis Cyber Files Web Server oder der Gateway Server ausgeführt werden, müssen an das Windows Active Directory gebunden sein.
- Die Adresse des Acronis Cyber Files Web Servers, die in der Administration-Konsole unter 'Allgemeine Einstellungen' > 'Webservice' konfiguriert ist, muss für den Acronis Cyber Files Mobile Gateway Server zugänglich sein.

Es gibt zwei Komponenten, die HTTPS-Verkehr verarbeiten: der Gateway Server und der Acronis Cyber Files Web Server. Der Gateway Server wird von mobilen Clients für den Zugriff auf Dateien und Freigaben aus den Datenquellen verwendet. Der Acronis Cyber Files 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 Bereitstellung bzw. Einrichtung verlangt.

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

- **Zugriff auf die Ports 443 und 3000**: Acronis Cyber Files verwendet HTTPS für den verschlüsselten Transport, wodurch es mit den gängigen Firewall-Regeln kompatibel ist, die HTTPS-Verkehr auf den Ports 443 und 3000 erlauben. Wenn Sie den Zugriff auf den Port 443 für Ihren Acronis Cyber Files Web Server erlauben, müssen Sie auch den Zugriff auf den Port 3000 in der Firewall für den Acronis Cyber Files Gateway Service erlauben, damit sich autorisierte Mobilgeräte-Apps verbinden können, egal ob sie sich innerhalb oder außerhalb Ihrer Firewall befinden. Die Services können auch so konfiguriert werden, dass sie andere Ports verwenden, wenn Sie das bevorzugen sollten.
- **VPN:** Die Acronis Cyber Files Mobile App unterstützt Zugriffe über eine VPN-Verbindung. Sowohl der integrierte VPN-Client von iOS als auch VPN-Clients von Drittanbietern werden unterstützt. iOS-Verwaltungsprofile können optional auf Geräte angewendet werden, die MDM-Systeme (Mobile Device Management) oder das Apple iPhone-Konfigurationswerkzeug verwenden, um die zertifikatsbasierte iOS-Funktion 'VPN auf Anforderung' zu konfigurieren, die nahtlosen Zugriff auf Acronis Cyber Files Web Server und andere Unternehmensressourcen bietet.
- **Reverse-Proxy-Server:** Wenn Sie einen Reverse-Proxy-Server eingerichtet haben, können sich iPad-Clients verbinden, ohne dass ein offener Firewall-Port oder eine VPN-Verbindung erforderlich ist. Die Acronis Cyber Files Mobile App unterstützt die Reverse-Proxy-Pass-Through-Authentifizierung, die Authentifizierung mit Benutzername/Kennwort, die Authentifizierung per eingeschränkter Kerberos-Delegierung und die Zertifikatsauthentifizierung. Weitere Informationen zum Hinzufügen von Zertifikaten zur Acronis Cyber Files Mobile App finden Sie im Artikel 'Client-Zertifikate verwenden'.
- **Per MobileIron AppConnect registrierte App**: Wenn die mobile Acronis Cyber Files-App per AppConnect-Plattform von MobileIron registriert wird, kann die gesamte Netzwerkkommunikation zwischen den Clients der mobilen Acronis Cyber Files-App und Gateway-Servern über MobileIron Sentry geroutet werden. Weitere Informationen finden Sie in der Anleitung zu MobileIron AppConnect.

Zertifikate:
Acronis Cyber Files wird mit selbstsignierten Zertifikaten für Testzwecke ausgeliefert und installiert. Bei Produktionsbereitstellungen sollten ordnungsgemäße 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. Selbstsignierte Zertifikate werden in Produktionsumgebungen nicht unterstützt.

Hinweis
Wenn Sie die Funktion für sichere LDAP-Verbindungen aktivieren, schreibt Acronis Cyber Files vor, dass der vollqualifizierte Domain-Name des LDAP-Servers im Zertifikat entweder als allgemeiner Name (Common Name, CN) oder als alternativer Antragstellername (Subject Alternative Name, SAN) vorhanden sein muss.

Voraussetzungen für Desktop Client

Systemanforderungen

Unterstützte Betriebssysteme

- Windows 7, 8, 8.1, 10 und 11

  Hinweis
  Desktop-Client 7.4 ist die letzte mit Windows XP und Vista kompatible Version. Wenn Sie eine neuere Version des Acronis Cyber Files-Desktop-Clients verwenden möchten, führen Sie ein Update Ihres Windows-Betriebssystems durch. Access Advanced 7.4 ist die letzte Serverversion, die Verbindungen von Windows XP oder Vista zulässt.

  Hinweis
  Acronis Cyber Files bietet ab Version 8.6 keine Unterstützung für Windows Server 2008 R2 (Referenz zur offiziellen Ankündigung von Microsoft).

- macOS X 10.13 bis 10.15, wenn Mac mit 64-Bit-Software kompatibel ist.
- macOS 11 Big Sur und macOS 12 Monterey auf Intel x86-64 und Apple Silicon-CPUs

  Hinweis
  Desktop-Client 7.1.2 ist die letzte mit macOS X 10.6 und 10.7 kompatible Version. Der Desktop-Client 8.5 ist die letzte mit macOS X 10.12 kompatible Version. Wenn Sie eine neuere Version des Acronis Cyber Files-Desktop-Clients verwenden möchten, führen Sie ein macOS-Update durch.

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

Unterstützte Webbrowser:

- Mozilla Firefox 60 und höher
- Microsoft Edge 25 oder höher
- Google Chrome 64 und höher
- Safari 12 und höher
- Opera 72 und höher

Zusätzliche Anforderungen

Für die Installation ist Folgendes erforderlich:

- Acronis Die ausführbare Datei des Installationsprogramms für den Cyber Files Desktop Client und die entsprechenden Ausführungsrechte.
- Die Adresse des Servers, den Sie verwenden möchten (erhalten Sie von Ihrem Administrator oder per E-Mail).
- Anmeldedaten für den Server (aus Active Directory, von Ihrem Administrator oder per E-Mail).

Voraussetzungen für PostgreSQL Administrator

Die GUI-Anwendung für Acronis Cyber Files PostgreSQL Administratoren (pgAdmin) wird zusammen mit PostgreSQL installiert.

Dies erfordert, dass einer der folgenden Webbrowser auf dem Server, auf dem PostgreSQL installiert ist, ausgeführt wird.

- Chrome 90+
- Firefox 78+
- Edge 91+

Acronis Cyber Files auf Ihrem Server installieren

Mit den folgenden Schritten können Sie eine Neuinstallation durchführen und Acronis Cyber Files mit HTTPS und dem bereitgestellten selbstsignierten Zertifikat testen.

Hinweis
Anweisungen zu Upgrades finden Sie im Abschnitt zu Upgrades.

Hinweis
Anweisungen zum Installieren in einem Cluster finden Sie im Abschnitt zum Lastenausgleich.

Die Installation von Cyber Files umfasst drei Schritte:

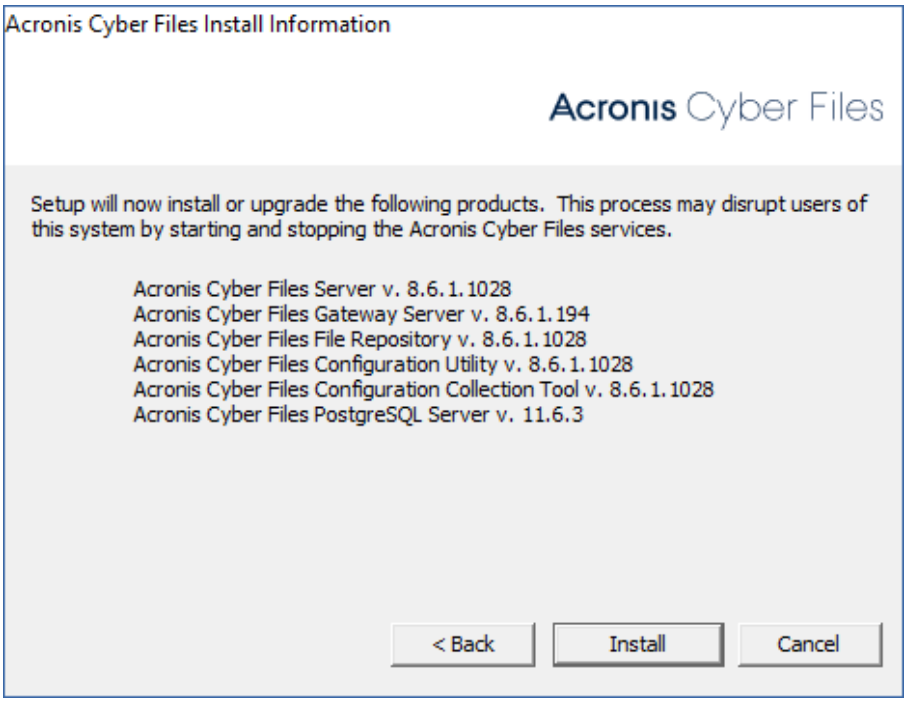
1. Installation des Installationsprogramms für den Cyber Files-Web-Server.
2. Konfiguration der vom Cyber Files-Web-Server genutzten Netzwerk-Ports und SSL-Zertifikate.
3. Nutzung des webbasierten Installationsassistenten zur Konfiguration des Servers.

Installieren von Cyber Files

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

1. Laden Sie das Installationsprogramm für Cyber Files herunter.
2. Deaktivieren Sie alle vorhandenen Virenschutzprogramme, da sie unter Umständen den Installationsvorgang unterbrechen können. Unterbrechungen können eine fehlerhafte Installation verursachen.
3. Öffnen Sie die ausführbare Datei des Installationsprogramms.
4. Wählen Sie **Weiter**.
5. Lesen und akzeptieren Sie die Lizenzvereinbarung.
6. Wählen Sie **Installieren**.

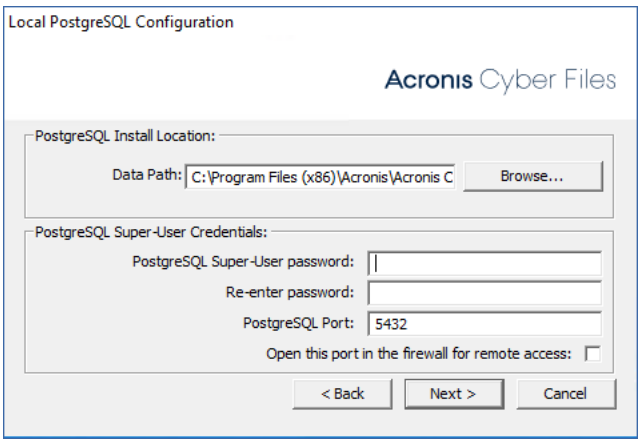
Hinweis
Wenn Sie mehrere Cyber Files-Server einsetzen oder eine nicht standardmäßige Konfiguration installieren möchten, können Sie über die Schaltfläche **Benutzerdefinierte Installation** festlegen, welche Komponenten installiert werden sollen.



7. Verwenden Sie den Standardpfad oder wählen Sie einen neuen für den Hauptordner von Cyber Files.
8. Wählen Sie **OK**.

9. Legen Sie ein Passwort für den PostgreSQL-Superuser fest.

Hinweis
Das Passwort für den PostgreSQL-Superuser darf weder Doppelpunkte (**:**), Strichpunkte (**;**) noch Sternchen (*****) enthalten.



Wichtig
Schreiben Sie das Passwort für den PostgreSQL-Superuser auf und bewahren Sie es an einem sicheren Ort auf. Sie benötigen es für Backup- und Wiederherstellungsaktionen der Datenbank.

10. Wählen Sie **OK**, um die Liste der installierten Komponenten zu schließen.
11. Wählen Sie **Beenden**, wenn das Installationsprogramm für Cyber Files ausgeführt wurde.
12. Das Konfigurationswerkzeug startet automatisch.

Hinweis
Anleitungen zur Verwendung des Konfigurationswerkzeugs finden Sie unter Das Konfigurationswerkzeug verwenden.

Mit dem Konfigurationswerkzeug

Das Acronis Cyber Files-Installationsprogramm umfasst ein Konfigurationswerkzeug, das eine schnelle und einfache Einrichtung des Zugriffs auf Cyber Files-Gateway-Server, Datei-Repository und Cyber Files-Webserver ermöglicht.

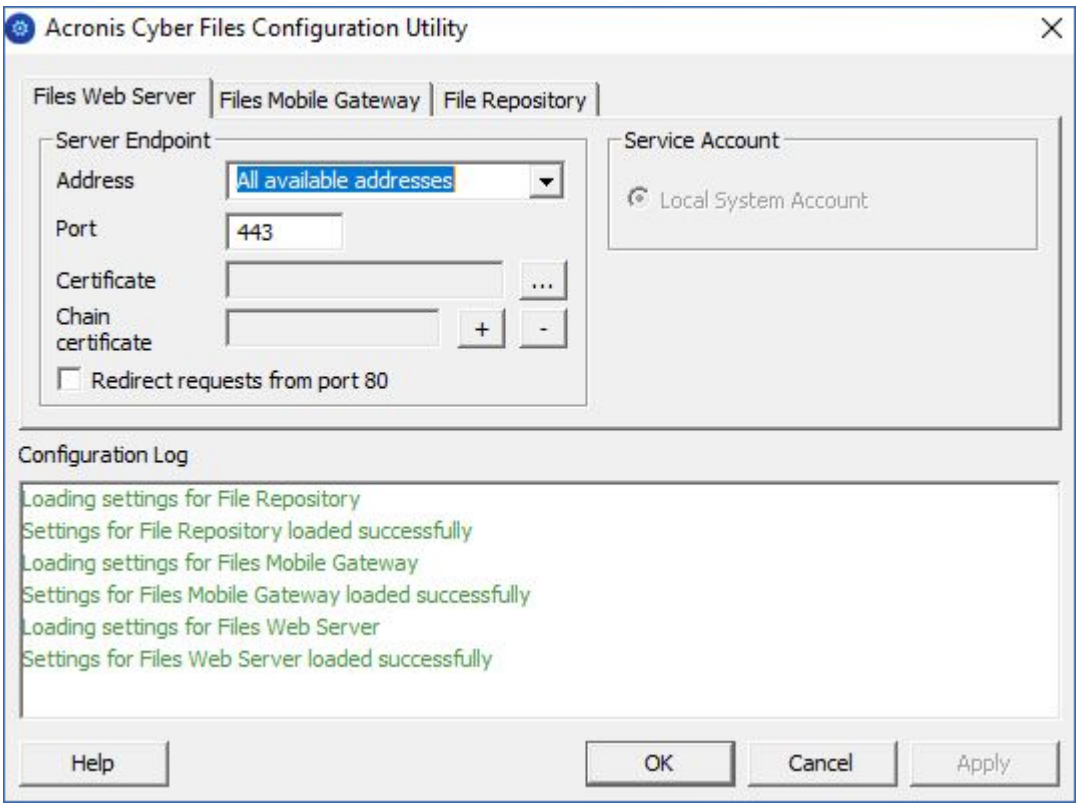
Hinweis
Im Abschnitt Netzwerkanforderungen finden Sie weitere Informationen zu den besten Verfahren für die Konfiguration der IP-Adressen von Cyber Files.

Hinweis
Weitere Informationen zum Hinzufügen Ihres Zertifikats zum Microsoft Windows Certificate Store finden Sie im Artikel Zertifikate verwenden.

Übersicht über Konfigurationswerkzeug

Die Einstellungen im Konfigurationswerkzeug 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 werden neu gestartet.

Registerkarte Files Web Server



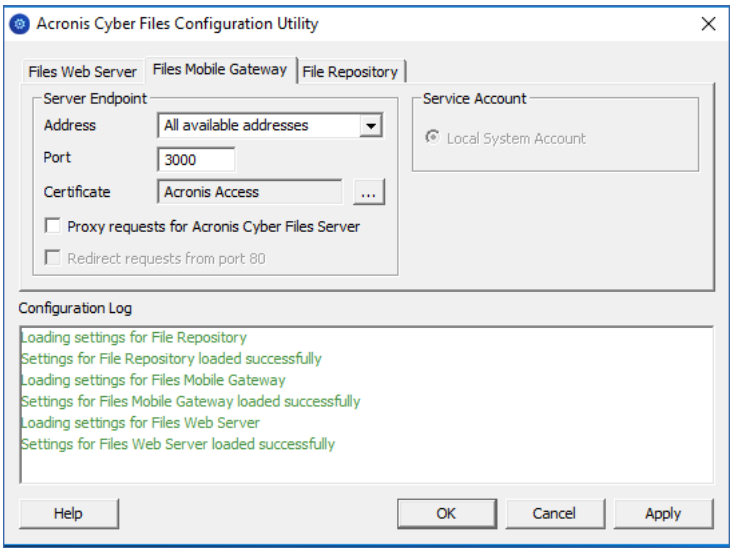
Der Cyber Files-Webserver stellt die Weboberfläche für Cyber Files-Clients zur Verfügung und ist darüber hinaus die Verwaltungskonsole für Mobile Access und Sync & Share.

- **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 Certificate Store auswählen.
- **Kettenzertifikat** – Der Pfad zum Zwischenzertifikat für Ihre Weboberfläche. Sie können ein solches Zertifikat aus dem Microsoft Windows-Zertifikatsspeicher auswählen. Dieses Zertifikat wird nur dann benötigt, wenn Ihre Zertifizierungsstelle (CA) Ihnen ebenfalls ein Zwischenzertifikat ausgestellt hat.
- **Umleitungsanforderung von Port 80** – Wenn Sie diese Option aktivieren, lauscht Tomcat auf eingehenden Datenverkehr am ungesicherten Port 80 und leitet diesen an den oben

spezifizierten HTTPS-Port weiter. Wenn ein anderes Programm den Port 80 überwachen sollte, sollten Sie diese Option nicht aktivieren.

- **Dienstkonto –** Ermöglicht, dass der Cyber Files-Webserver-Dienst im Kontext eines anderen Kontos ausgeführt werden kann. Dies ist in typischen Installationen normalerweise nicht erforderlich.

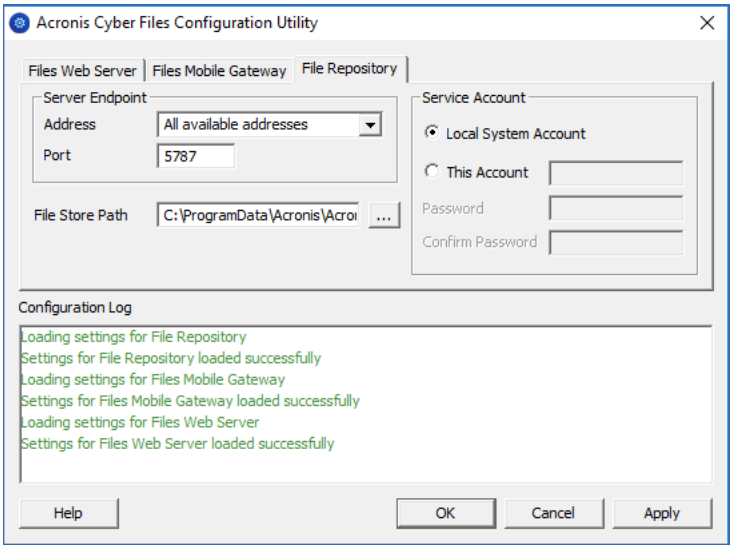
Registerkarte Files Mobile Gateway



Der Gateway Server wird von mobilen 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 –** Port Ihres Gateway Server.
- **Zertifikat –** Pfad zum Zertifikat Ihres Gateway Server. Sie können ein Zertifikat aus dem Microsoft Windows Certificate Store 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 Cyber Files Server** – Wenn diese Option aktiviert ist, verbinden sich die Benutzer mit dem Gateway Server, der sie dann als Proxy zum Cyber Files Server weiterleitet. Diese Option ist verfügbar, wenn Sie einen Cyber Files Server und einen Gateway Server auf derselben Maschine installiert haben.
- **Umleitungsanforderung von Port 80** – Wenn Sie diese Option aktivieren, lauscht Tomcat auf eingehenden Datenverkehr am ungesicherten Port 80 und leitet diesen an den oben spezifizierten HTTPS-Port weiter. Wenn ein anderes Programm den Port 80 überwachen sollte, sollten Sie diese Option nicht aktivieren.

File Repository – Registerkarte



Das File 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 File Store 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 Schnittstellen abgehört werden sollen. Wenn Sie eine IP- oder DNS-Adresse festlegen, sollte die gleiche Adresse auch im Abschnitt **File Repository** der Weboberfläche festgelegt werden. Weitere Informationen darüber finden Sie im Artikel File Repository.
- **Port –** Der Port Ihres Datei-Repositorys. Der gleiche Port sollte auch im Abschnitt **File Repository** der Weboberfläche festgelegt werden. Weitere Informationen darüber finden Sie im Artikel File Repository.
- **File Store-Pfad –** UNC-Pfad des File Store. Wenn Sie den File Store-Pfad ändern, müssen Sie alle Dateien, die sich bereits am ursprünglichen File Store-Speicherort befinden, manuell an den neuen Speicherort kopieren.

  Hinweis
  Wenn Sie den File Store 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 File Store befand, um sicherzustellen, dass Sie auch vom neuen Speicherort aus auf alle Dateien des ursprünglichen Speicherorts zugreifen können.

- **Dienstkonto –** Befindet sich der Datei-Storage für das Repository auf einer Remote-Netzwerkfreigabe, muss das Dienstkonto so konfiguriert werden, dass es Berechtigungen für diese Netzwerkfreigabe aufweist. Das Konto benötigt auch Lese- und Schreibzugriff auf den lokalen Repository-Ordner (z.B. `C:\Program Files (x86)\Acronis\Acronis Cyber Files\File`

`Repository\Repository`), um in das Protokoll zu schreiben.

Hinweis
Wenn Sie ein bestimmtes Konto für den Dienst anstelle von **Lokales Systemkonto** verwenden, müssen Sie die Systemsteuerungsoption **Dienste** öffnen, die Eigenschaften für den Dienst des **Cyber Files-Datei-Repository** öffnen und die Registerkarte **Anmelden** bearbeiten. Sie müssen das Konto und das entsprechende Kennwort manuell in den entsprechenden Feldern eingeben.

Öffnen des Installationsassistenten

Wenn die entsprechenden Felder ausgefüllt wurden, werden nach dem Auswählen von **Anwenden** oder **OK** die Dienste neu gestartet, die Sie geändert haben.

Hinweis
Es kann nach dem Starten der Dienste 30 bis 45 Sekunden dauern, bis der Cyber Files-Webserver verfügbar ist.

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

Wichtig
Notieren Sie das Passwort für den Administrator. Wenn es vergessen wird, kann es nicht zugeschickt werden!

Verwenden des Installationsassistenten

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 AcronisCyber Files-Server konfigurieren. Der Installationsassistent leitet den Administrator durch eine Reihe von Schritten, um die grundlegenden Funktionen des Servers einzurichten.

Hinweis
Nach der Ausführung des Konfigurationswerkzeugs dauert es 30 bis 45 Sekunden, bis der Server erstmalig angezeigt wird.

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!

Durchlaufen der Erstkonfiguration

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

Hinweis
Später können zusätzliche Administratoren konfiguriert werden. Weitere Informationen hierzu finden Sie im Abschnitt Server-Administration.

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.

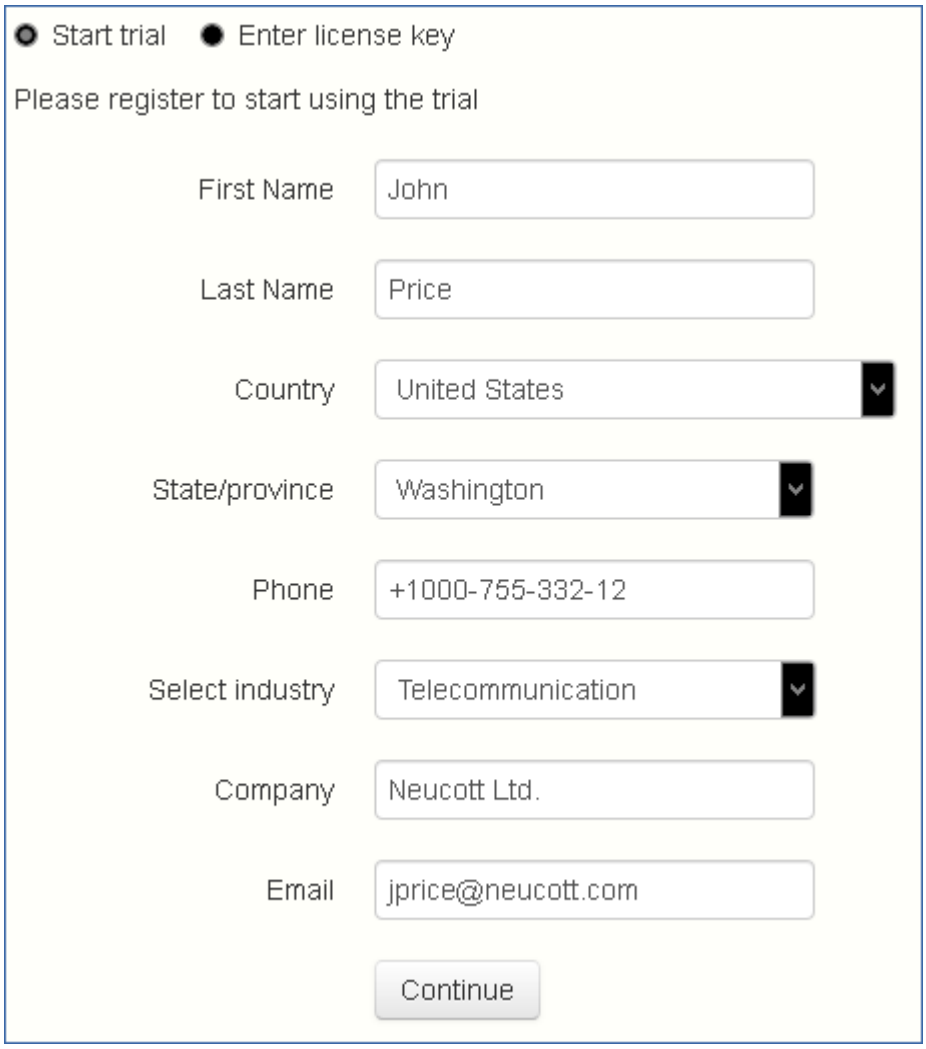
SMTP-Einstellungen betreffen die Funktionalität in den Funktionen Mobile Access und Sync & Share. Bei Mobile Access wird der SMTP-Server verwendet, wenn Registrierungseinladungen versendet werden. Sync & Share-Funktionen verwenden den SMTP-Server für das Versenden von Ordnereinladungen, Warnungen und 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.

Lizenzierung

So starten Sie eine Testversion:

Wählen Sie **Test starten**, geben Sie die erforderlichen Informationen ein, und klicken Sie auf **Weiter**.

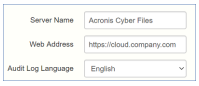


So lizenzieren Sie Ihre Acronis Cyber Files-Instanz:

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

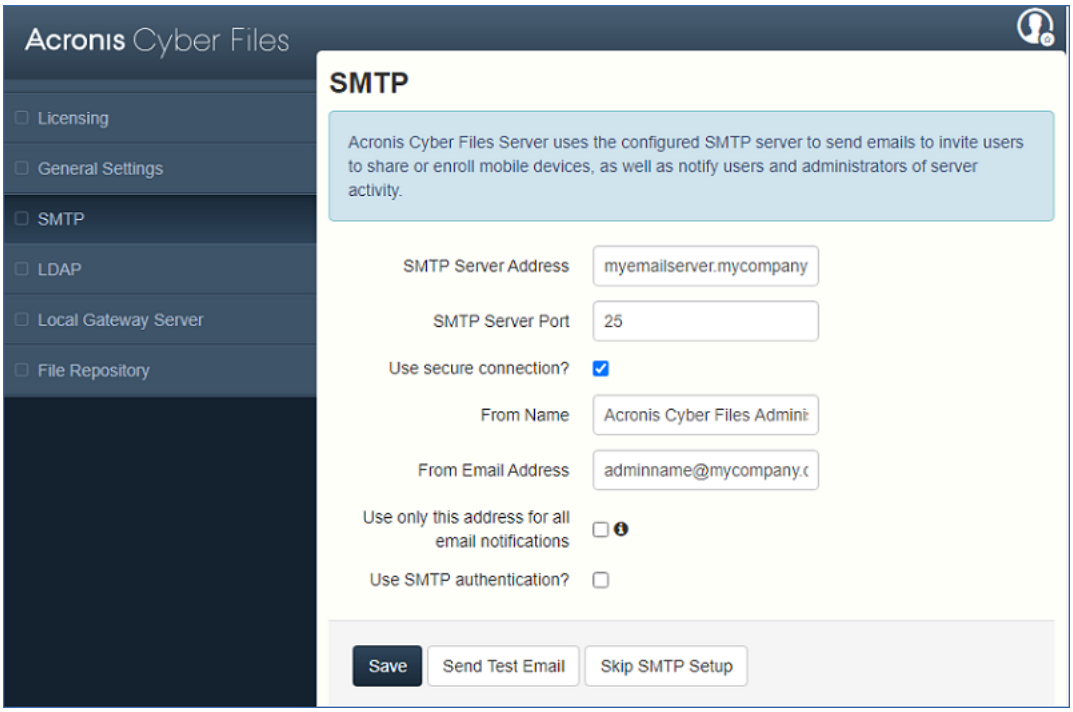
3. Klicken Sie auf **Speichern**.

Allgemeine Einstellungen



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

SMTP



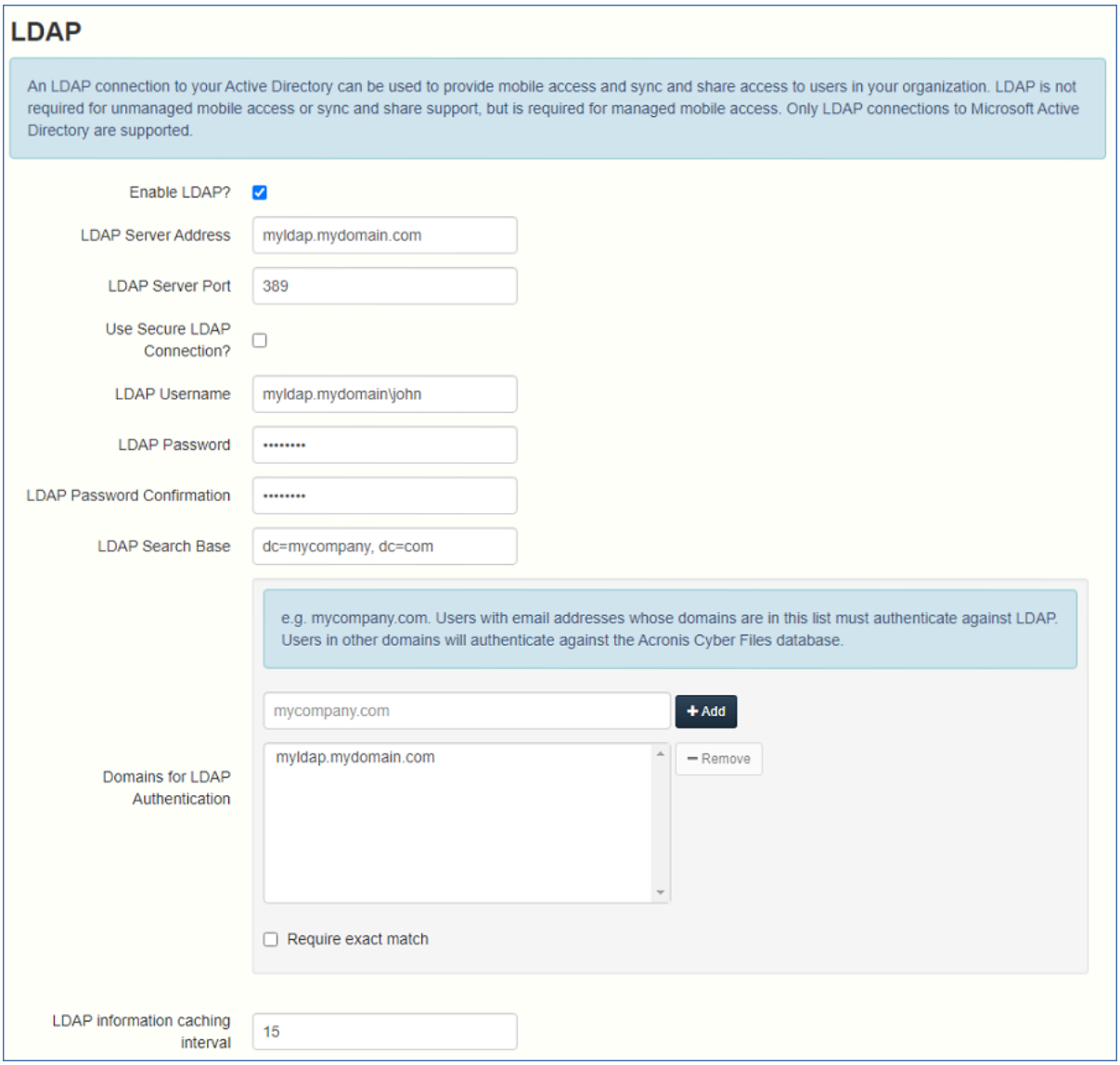
Hinweis
Sie können diesen Abschnitt überspringen und SMTP später konfigurieren.

1. Geben Sie den DNS-Namen oder die IP-Adresse Ihres SMTP-Servers ein.
2. Geben Sie den SMTP-Port Ihres Servers ein.
3. Wenn Sie keine Zertifikate für den SMTP-Server verwenden, deaktivieren Sie die Option **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, wählen Sie **SMTP-Authentifizierung verwenden?** aus, und geben Sie Ihre Anmeldedaten ein.
7. Klicken Sie auf **Test-E-Mail senden**, um eine Test-E-Mail an die in Schritt 5 festgelegte Adresse zu

senden.

8. Klicken Sie auf **Speichern**.

LDAP



Hinweis

Sie können diesen Abschnitt überspringen und LDAP später konfigurieren, aber einige der Funktionen von Acronis Cyber Files stehen dann nicht zur Verfügung.

1. Wählen Sie **LDAP aktivieren** aus.
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, wählen Sie **Sichere LDAP-Verbindung verwenden** aus.

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**.

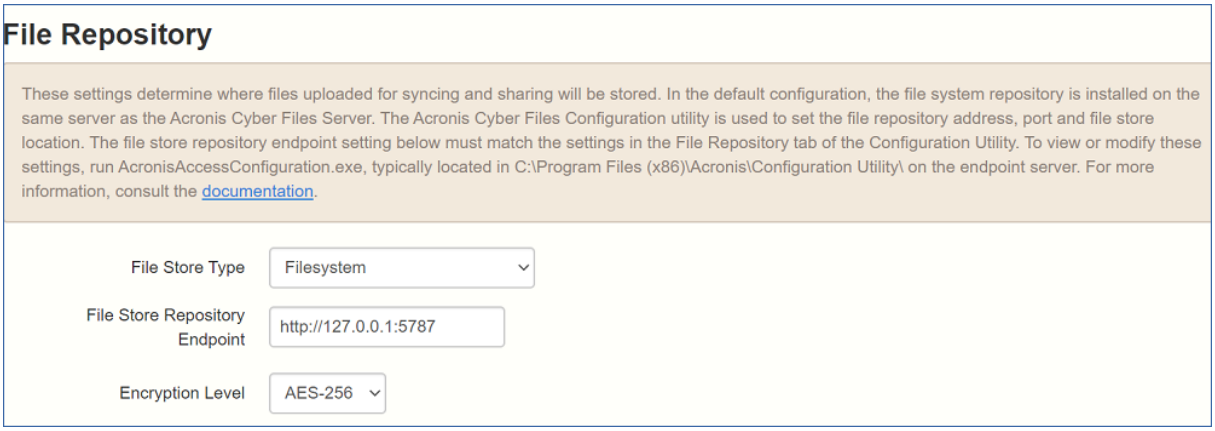
Lokaler Gateway Server

Damit KCD über mobile Clients funktioniert, ist eine Registrierung beim lokalen Gateway (das auf demselben Computer wie Tomcat installiert ist, der es verwaltet) erforderlich. Das Gateway leitet diese Anforderungen anschließend an diesen Tomcat-Server (für die Verwaltung) weiter.

Hinweis
Wenn Sie einen Gateway Server und den Acronis Cyber Files Server auf demselben Computer installieren, wird der Gateway Server automatisch erkannt und von letzterem 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 File Store-Typ aus. Verwenden Sie **Dateisystem** für einen File Store auf Ihren Computern oder eine der folgenden Optionen für einen File Store in der Cloud: **Acronis Storage**, **Microsoft Azure Storage**, **Amazon S3**, **Swift S3**, **Ceph S3** und **andere S3-kompatible Speicherlösungen**.

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.

Hinweis
MinIO S3-Storage wird als Typ unterstützt und kann mit der Option **Anderer S3-kompatibler Storage** konfiguriert werden, er wird jedoch nicht über eine unsichere HTTP-Verbindung unterstützt.

2. Geben Sie den DNS-Namen oder die IP-Adresse des Datei-Repository-Dienstes ein.

Hinweis
Mit dem Acronis Cyber Files-Konfigurationswerkzeug werden die Adresse des Datei-Repository, der Port und der File Store-Speicherort festgelegt. Die Einstellung 'File Store-Repository-Endpunkt' muss den Einstellungen auf der Registerkarte 'File Repository' des Konfigurationswerkzeugs entsprechen. Um diese Einstellungen einsehen oder ändern zu können, müssen Sie 'AcronisAccessConfiguration.exe' ausführen (typischerweise auf dem Endpunkt-Server im Verzeichnis `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\Configuration Utility` zu finden).

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. Klicken Sie auf **Speichern**.

Clustern von Acronis Cyber Files

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

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

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

Lastenausgleich

Acronis Cyber Files unterstützt Lastenausgleich.

Hinweis

Weitere Informationen finden Sie unter Installieren von Acronis Cyber Files in einer Konfiguration mit Lastenausgleich, Migrieren zu einer Konfiguration mit Lastenausgleich und Cluster-Gruppen.

Durchführen eines Upgrades

Durchführen eines Upgrades von Acronis Cyber Files auf eine neuere Version

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

Hinweis
Vor-Ort-Upgrades von Betriebssystemen werden nicht unterstützt. Bei Fragen wenden Sie sich bitte an den Acronis Mobility Technical Support.

Hinweis
Wenn Sie ein Upgrade von einer Version von Acronis Cyber Files (ehemals Acronis Access) vor 7.5 durchführen, wenden Sie sich an den Support von Acronis unter https://support.acronis.com/mobility/.

Hinweis
Sehen Sie sich die minimalen Hardware-Anforderungen 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 Acronis Cyber Files und benutzerdefinierte Installationen können die Ordnerstrukturen Ihrer Bereitstellung beeinflussen.

Hinweis
Beim Upgrade auf Acronis Cyber Files Version 8.6 oder höher wird PostgreSQL nicht automatisch auf Version 11 aktualisiert. Weitere Informationen dazu finden Sie unter Durchführen eines PostgreSQL-Upgrades auf eine neuere Hauptversion.

Sichern der wichtigen Komponenten

Apache Tomcat-Ordner

Beim Upgrade wird Apache Tomcat unter Umständen auch aktualisiert, und alle zugehörigen Konfigurations- und Protokolldateien werden entfernt. Wir empfehlen, eine Kopie des Apache Tomcat-Ordners anzulegen. Dieser befindet sich standardmäßig unter: `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\`.

Wir empfehlen Ihnen, die Datei **web.xml** vor dem Aktualisieren zu sichern. Ihre Datei **web.xml** wird beim Upgrade überschrieben. Für Version 8.6 und höher finden Sie ein Backup unter: `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Access Server\Web Application\WEB-INF\<timestamp>.previous.web.xml`.
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- die entsprechenden Änderungen bleiben erhalten).

Unnötige Überwachungsprotokolle entfernen

Wenn Sie die automatische Entfernung von Protokollen nicht eingerichtet haben, sind auf Ihrem Server möglicherweise viele Protokolle vorhanden, die den Backup-Prozess 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 gehen Sie zum Ordner `11.21\bin`, der sich im Installationsverzeichnis von PostgreSQL befindet.
   Beispielsweise: `cd "C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\PostgreSQL\11.21\bin"`
2. Sobald Sie als Verzeichnis für die Eingabeaufforderung den Ordner **bin** festgelegt haben, geben Sie die Zeile
   `pg_dump -U postgres -f mybackup.sql acronisaccess_production`
   ein, wobei `mybackup.sql` der gewünschte Dateiname für die von Ihnen erstellte Backup-Datei ist. 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 derAcronis Cyber Files-Datenbank ist.

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

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

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

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

```
pg_dumpall -U postgres > alldbs.sql
```

Dabei gibt `alldbs.sql` die generierte Backup-Datei an. Sie können auch einen vollständigen Pfad angeben, zum Beispiel `D:\Backups\alldbs.sql`

Die vollständige Syntax für diesen Befehl finden Sie unter: https://www.postgresql.org/docs/11/app-pg-dumpall.htm

Hinweis
Weitere Informationen zum Backup-Verfahren für PostgreSQL und zur Befehlssyntax finden Sie unter: https://www.postgresql.org/docs/11/backup.html

Die Gateway Server-Datenbank(en)

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

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

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

Acronis Cyber Files-Konfigurationsdatei

1. Navigieren Sie zum Acronis Cyber Files-Installationsordner, der die Konfigurationsdatei enthält.

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

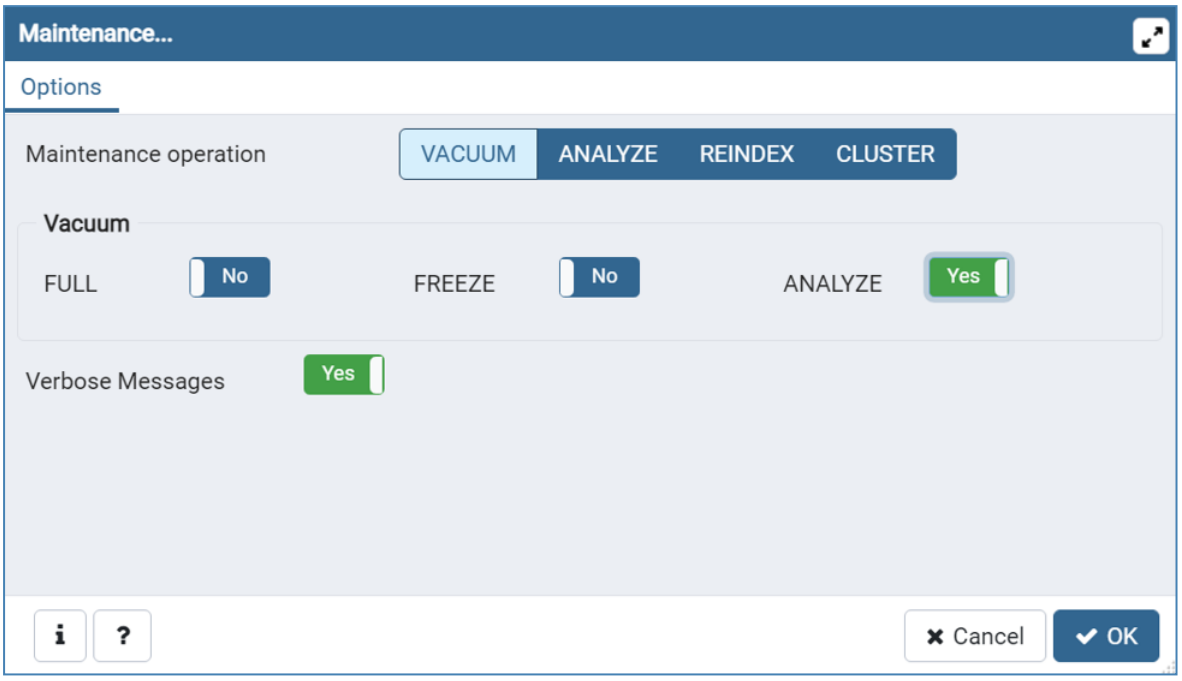
2. Kopieren Sie die Datei **acronisaccess.cfg** und fügen Sie diese in einen sicheren Speicherort ein.

Die Datenbank vor dem Upgrade bereinigen

Hinweis
Bitte sehen Sie sich die folgenden Empfehlungen an, bevor Sie die Schritte unten ausführen.

1. Öffnen Sie das PostgreSQL Administrator-Tool von Acronis Cyber Files. Es befindet sich im Startmenü, im Acronis Cyber Files-Ordner. Doppelklicken Sie auf **localhost**, um eine Verbindung zum Server herzustellen.

2. Klicken Sie mit der rechten Maustaste auf die Datenbank `acronisaccess_production` und wählen Sie **Wartung**.
3. Wählen Sie **BEREINIGEN** und legen Sie **ANALYSIEREN** mit 'Ja' fest.



Warnung!
Das Vakuum kann eine Weile andauern. Führen Sie dieses Verfahren durch, wenn die Serverauslastung niedrig ist.

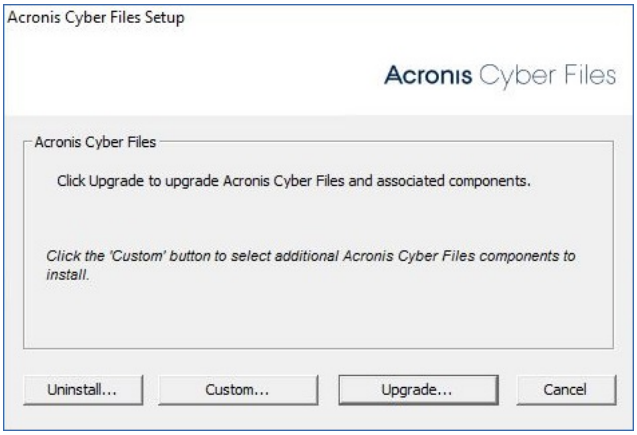
4. Klicken Sie auf **OK**.
5. Wenn der **Bereinigungs**prozess beendet wird, klicken Sie auf **Fertig**.
6. Schließen Sie das PostgreSQL-Administrator-Tool.

Upgrade

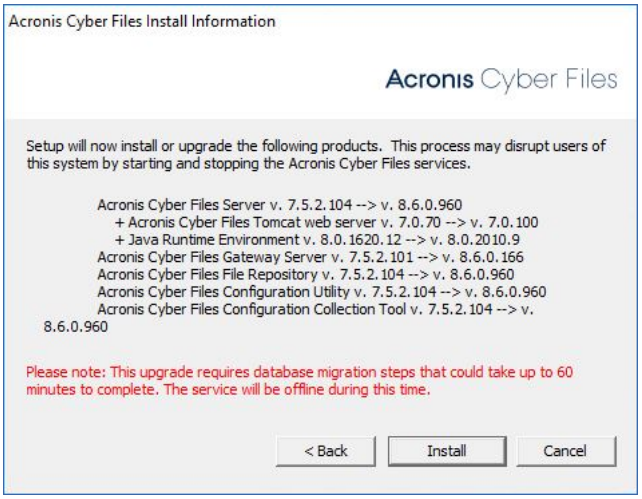
Hinweis
Deaktivieren Sie alle vorhandenen Virenschutzprogramme, da sie unter Umständen den Vorgang unterbrechen und somit eine fehlerhafte Installation verursachen können.

1. Doppelklicken Sie auf die Installationsdatei.

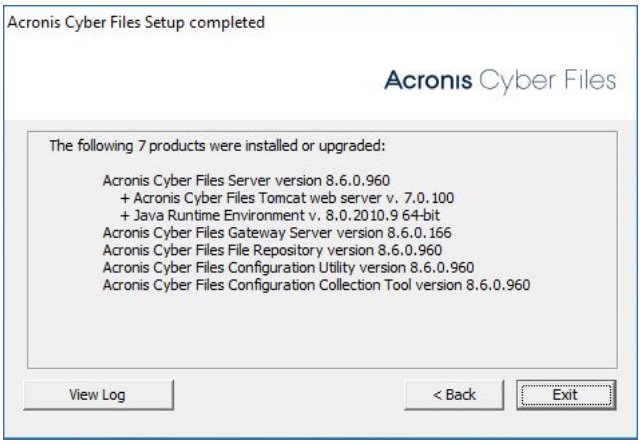
2. Wählen Sie auf dem Bildschirm, der als Nächstes angezeigt wird, **Upgrade** aus.



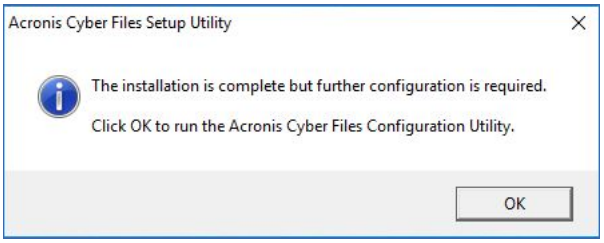
3. Überprüfen Sie die zur Installation ausgewählten Komponenten, und klicken Sie auf **Installieren**.



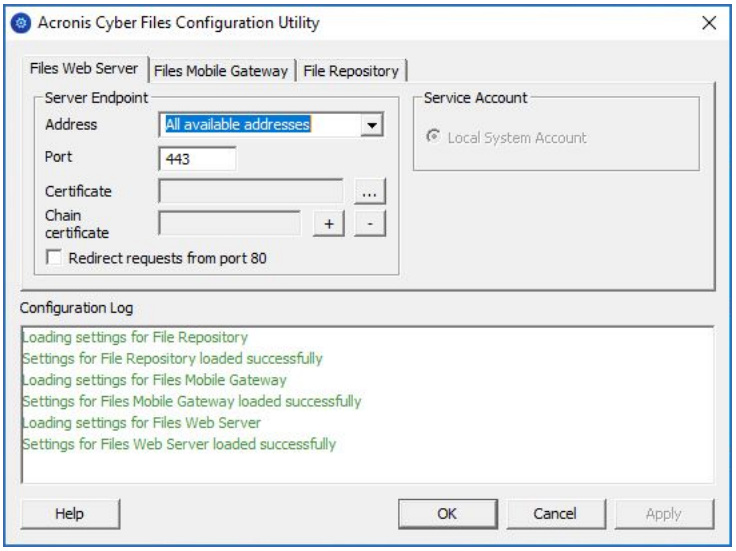
4. Prüfen Sie die bereits installierten Komponenten, und schließen Sie das Installationsprogramm.



5. Die folgende Meldung bestätigt, dass das Upgrade abgeschlossen ist:



6. Sie werden aufgefordert, das Konfigurationswerkzeug zu öffnen. Klicken Sie auf **OK**.
7. Vergewissern Sie sich, dass die Einstellungen im Konfigurationsdienstprogramm die richtigen Werte aufweisen. Wenn dies der Fall ist, wählen Sie **OK**, um das Konfigurationsdienstprogramm zu schließen und die Acronis Cyber Files-Dienste zu starten.



Warnung!
Datenbankmigrationen finden unmittelbar nach dem Upgradevorgang statt. Während dieser Zeit stehen die eigentliche Website und alle zugehörigen Dienste nicht zur Verfügung. Alle diese wichtigen Vorgänge können länger als eine Stunde dauern, wenn Sie beispielsweise länger kein Upgrade durchgeführt haben. Es wird dringend empfohlen, Server-Neustarts oder Dienstunterbrechungen so lange zu vermeiden, bis die Website wieder in einem Browser verfügbar ist.

Durchführen eines Upgrades von Gateway-Clustern

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

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

Hinweis
Anweisungen zum Upgrade desAcronis Cyber Files Web Server finden Sie im Artikel Durchführen eines Upgrades von Acronis Cyber Files auf eine neuere Version.

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

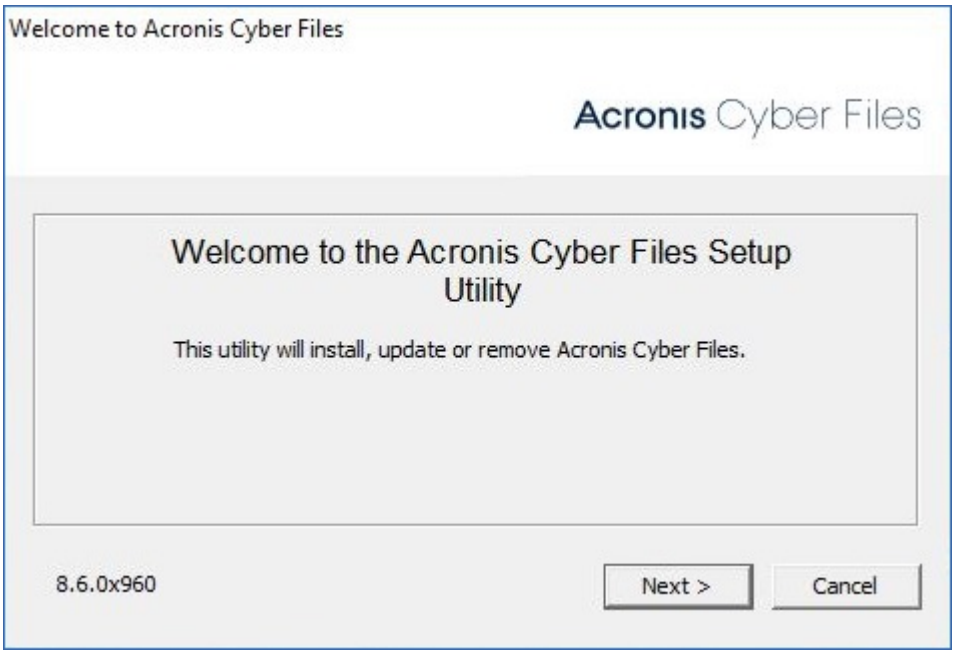
Sehen Sie sich vor der Durchführung eines Upgrades unsere Artikel zum Thema Backup an, und sichern Sie Ihre Konfiguration.

Hinweis
Sehen Sie sich die minimalen Hardware-Anforderungen an, bevor Sie ein Upgrade durchführen.

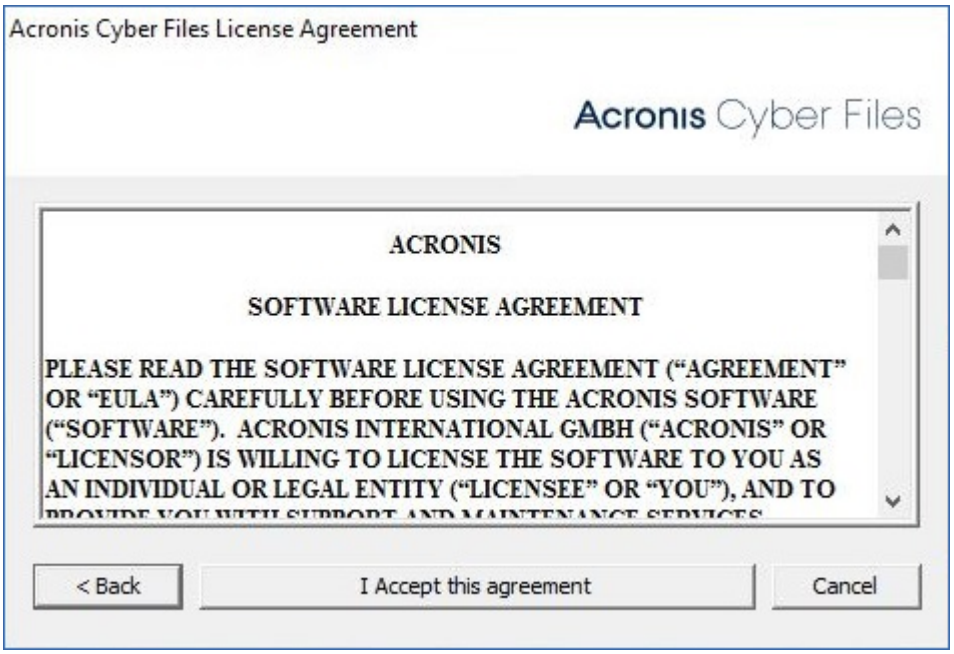
Hinweis
Abhängig von Ihrer Bereitstellung können einige der in diesem Artikel erwähnten Pfade von Ihren Pfaden abweichen. Aktualisierungen von vorherigen Versionen von Acronis Cyber Files und benutzerdefinierte Installationen können die Ordnerstrukturen Ihrer Bereitstellung beeinflussen.

Durchführen eines Upgrades eines Gateway Servers

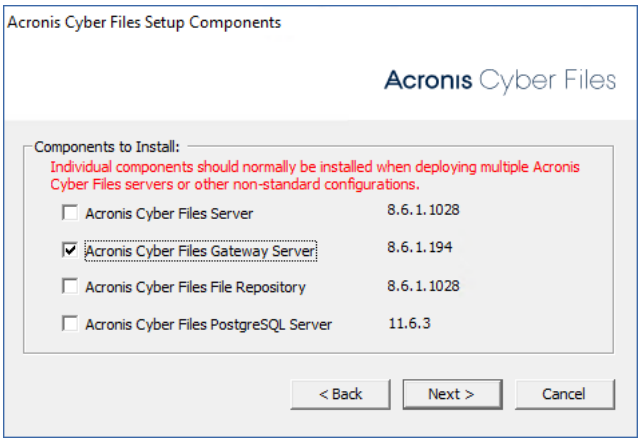
1. Führen Sie das Acronis Cyber Files-Installationsprogramm auf dem gewünschten Server aus.
2. Klicken Sie im Begrüßungsbildschirm auf **Weiter**.



3. Lesen und akzeptieren Sie die Lizenzvereinbarung.



4. Klicken Sie auf **Benutzerdefiniert**.
5. Wählen Sie nur die Komponente **Acronis Cyber Files 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**.

Durchführen eines Upgrades von Lastenausgleichskonfigurationen

Diese Anleitung ist für Bereitstellungen gedacht, die lastenausgleichend für Acronis Cyber Files und alle zugehörigen Komponenten sind.

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

Hinweis
Sehen Sie sich die minimalen Hardware-Anforderungen 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 Acronis Cyber Files und benutzerdefinierte Installationen können die Ordnerstrukturen Ihrer Bereitstellung beeinflussen.

Vor Beginn

Warnung!
Acronis Cyber Files 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-Team.

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

Alle auf dieser Seite aufgeführten Pfade entsprechen den Standardspeicherorten. Ihre Pfade können abweichen, wenn Sie ein Upgrade oder eine benutzerdefinierte Installation durchgeführt haben. Verwenden Sie in solchen Fällen den [Name des Diensts]-Eintrag in den Windows-Diensten, um den genauen Pfad zum Ordner mit der ausführbaren Programmdatei ausfindig zu machen.

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

- Werden der Acronis Cyber Files Server und der PostgreSQL-Server auf demselben 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**.

  Warnung!
  Stellen Sie sicher, dass Ihre neue PostgreSQL-Installation über dieselbe **Codierung** und denselben **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 aktuellen Servers? Diese Nummer ermitteln Sie am einfachsten anhand des Ordners im PostgreSQL-Hauptordner (standardmäßig: `C:\Program`

`Files (x86)\Acronis\Cyber Files\Common\PostgreSQL`). Der Name dieses Ordners ist die Nummer der PostgreSQL-Hauptversion (z.B. 9.2, 9.3, 9.4).

- Für Kunden, die ein Upgrade auf Acronis Cyber Files von älteren Produktversionen durchführen, wie Access oder Files Advanced, sehen die Verzeichnispfade evtl. anders aus.
  Beispiel:
  - `C:\Program Files (x86)\Acronis\Access\Common\PostgreSQL`
  - `C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL`
  - `C:\Program Files\PostgreSQL\`
- Stellen Sie sicher, dass alle erforderlichen Berechtigungen im/in den Dateisystem(en) konfiguriert sind.

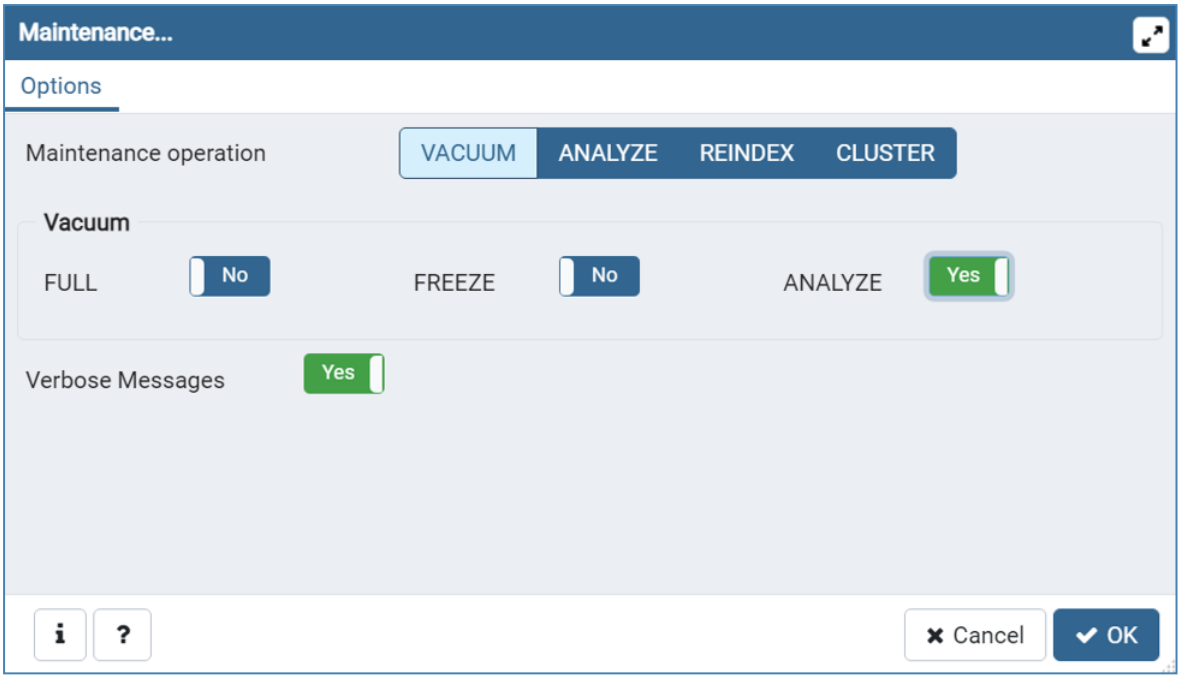
Wählen Sie, welcher der Acronis Cyber Files Web Server-Rechner als **Primärserver** dienen soll. Dieser Computer ist nur dahingehend der **Primärknoten**, als dass er zuerst aktualisiert wird und er alle Änderungen/Einstellungen zur PostgreSQL-Datenbank migriert. Wenn die Datenbank sehr groß ist, können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

Warnung!
HINWEIS: 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 PostgreSQL Administrator-Tool von Acronis Cyber Files. Es befindet sich im Startmenü, im Acronis Cyber Files-Ordner. Doppelklicken Sie auf **localhost**, um eine Verbindung zum Server herzustellen.
2. Klicken Sie mit der rechten Maustaste auf die Datenbank `acronisaccess_production` und wählen Sie **Wartung**.
3. Wählen Sie **BEREINIGEN** und legen Sie **ANALYSIEREN** mit 'Ja' fest.



Warnung!
Das Vakuum kann eine Weile andauern. Führen Sie dieses Verfahren durch, wenn die Serverauslastung niedrig ist.

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

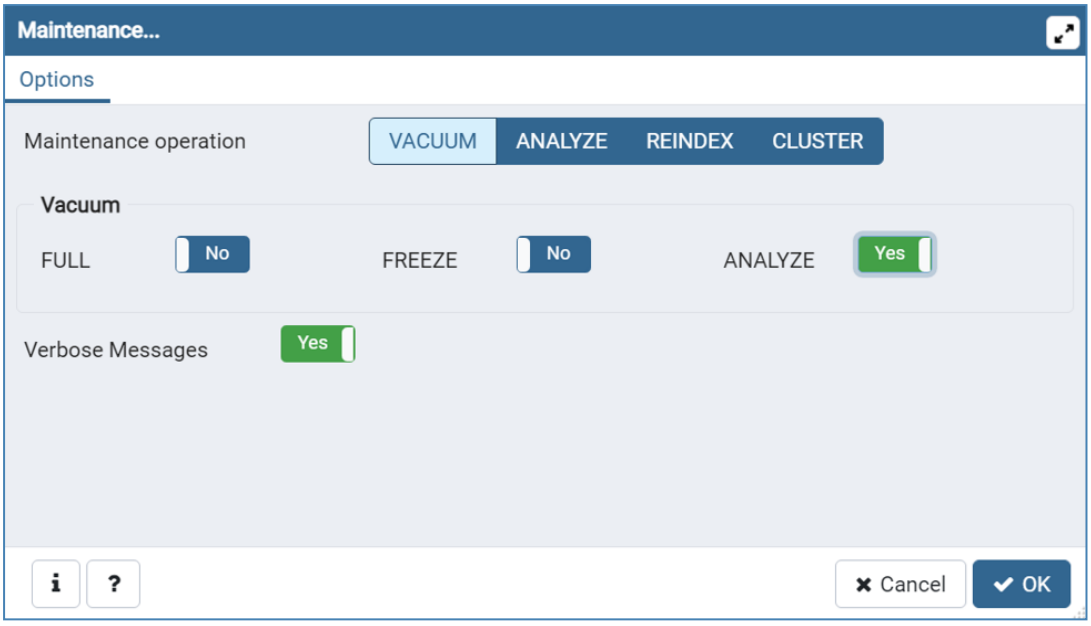
Sichern der Lastenausgleichskomponenten

Detaillierte Informationen zu den Backup- und Wiederherstellungsprozessen finden Sie im Artikel Sichern und Wiederherstellen von Acronis Cyber Files.

Backup der PostgreSQL-Datenbank erstellen

1. Stoppen Sie alle Acronis Cyber Files Tomcat-Dienste.
2. Öffnen Sie das PostgreSQL Administrator-Tool von Acronis Cyber Files. Sie finden es im Startmenü von Windows im Ordner von Acronis Cyber Files. 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 **Maintenance**.

5. Wählen Sie **BEREINIGEN** und legen Sie **ANALYSIEREN** mit 'Ja' fest.



6. Klicken Sie auf **OK**.
7. 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.
8. Schließen Sie PostgreSQL Administrator, und öffnen Sie eine Eingabeaufforderung mit erweiterten Benutzerrechten.
9. Navigieren Sie in der Eingabeaufforderung zum PostgreSQL-Verzeichnis 'bin'.

   z.B.`cd "C:\Program Files(x86)\Acronis\Acronis Cyber Files\Common\PostgreSQL\<version>\bin"`

Hinweis

Sie müssen den Pfad so bearbeiten, dass er auf den PostgreSQL-Ordner 'bin' verweist, wenn Sie eine ältere oder eine benutzerdefinierte Installation verwenden (z.B. `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\PostgreSQL\9.4\bin\`).

1. Geben Sie den folgenden Befehl ein: `pg_dumpall --host localhost --port 5432 --username postgres --file alldbs.sql`.
   - `alldbs.sql` ist der Dateiname des Backups. Dieses wird im PostgreSQL-Bin-Verzeichnis gespeichert. Sie können einen Pfad im obigen Befehl verwenden, wenn Sie das Backup an einem anderen Ort speichern wollen. Ändern Sie dazu folgendermaßen den letzten Teil des oberen Befehls: `--file D:\Backups\alldbs.sql`
   - Wenn Sie nicht den Standard-Port verwenden, müssen Sie statt `5432` die richtige Portnummer eingeben.
   - Wenn Sie nicht das standardmäßige PSQL-Administratorkonto `postgres` verwenden, muss `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 Fenster mit der Eingabeaufforderung.

2. Kopieren Sie die Backup-Datei an einen sicheren Speicherort.
3. Beenden Sie **NICHT** den Postgres-Dienst, da PostgreSQL selbst nicht aktualisiert wird.

Backup weiterer wichtiger Komponenten erstellen

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

Hinweis
Ersetzen Sie <Version> durch die korrekte Version Ihrer Acronis Cyber Files Tomcat-Instanz, z.B. `\apache-tomcat.70.0.70\`

2. Erstellen Sie ein Backup der Datei **acronisaccess.cfg**. Standardspeicherort: `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Access Server`
3. Sichern Sie alle **web.xml**-Dateien, die sich standardmäßig in `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Access Server\Web Application\WEB-INF\` befinden.
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. Schalten Sie alleAcronis Cyber Files Gateway-Dienste ab
2. Greifen Sie auf die Gateway Datenbankordner zu, standardmäßig unter `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Gateway Server\database`.
3. Erstellen Sie ein Backup der Datei **mobilEcho.sqlite3**.
4. Wiederholen Sie diese Schritte für jeden Gateway Server.

Alle Acronis Cyber Files-Dienste auf allen Rechnern stoppen

Es ist äußerst wichtig, dass alle Acronis Cyber Files Tomcat-Dienste vor einem Upgrade gestoppt werden. Wir empfehlen, auch alle anderen AcronisCyber Files-Dienste zu stoppen, der PostgreSQL-Dienst muss jedoch weiterhin ausgeführt werden.

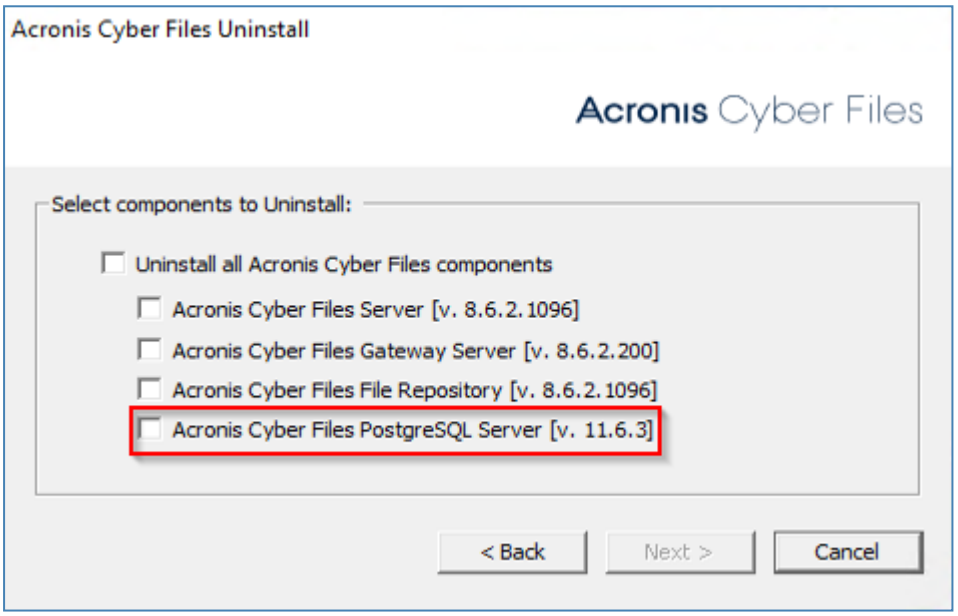
Durchführen eines Upgrades von PostgreSQL

Schritt 1: PostgreSQL deinstallieren

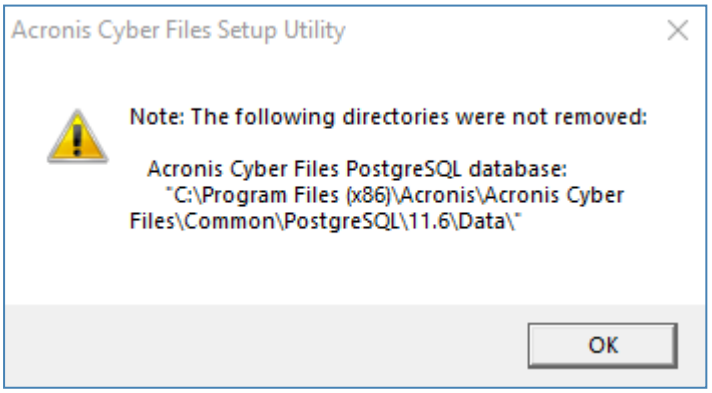
Starten Sie das Installationsprogramm des alten Acronis Cyber Files Server.

Klicken Sie im Begrüßungsbildschirm auf **Weiter**.

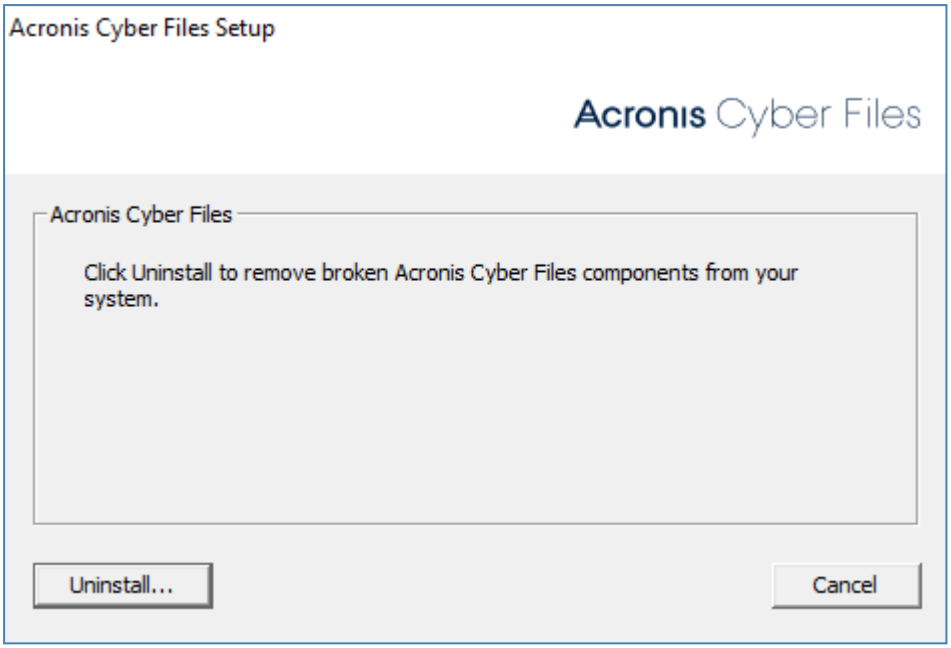
1. Lesen Sie das End User License Agreement (EULA), und klicken Sie auf **OK**, um es zu akzeptieren.
2. Klicken Sie auf **Deinstallieren**.
3. Wählen Sie nur den Acronis Cyber Files PostgreSQL Server, und klicken Sie auf **Weiter**.



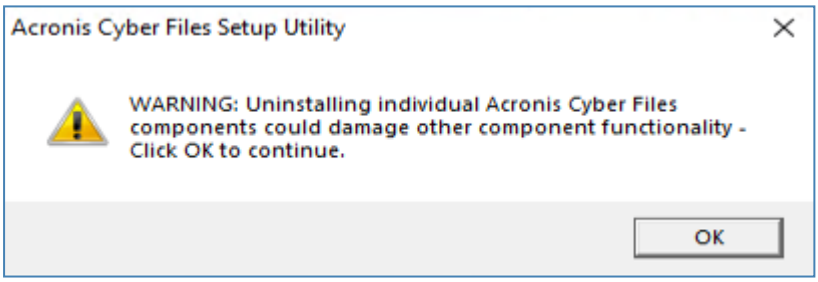
4. Nach der Deinstallation wird das folgende Warnungsdialogfeld angezeigt.



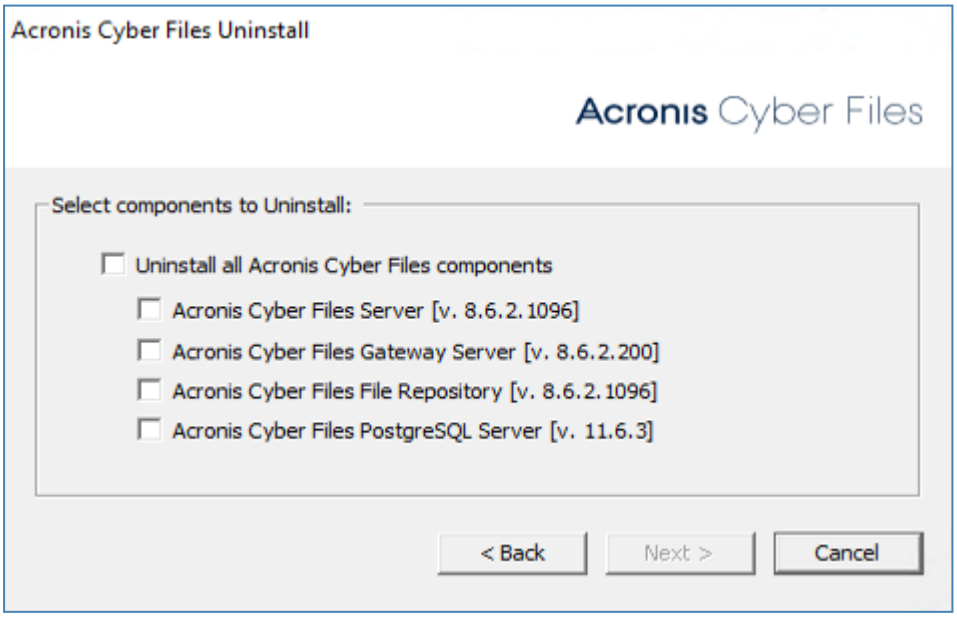
5. Klicken Sie auf **OK**.
   Das folgende Fenster wird angezeigt.



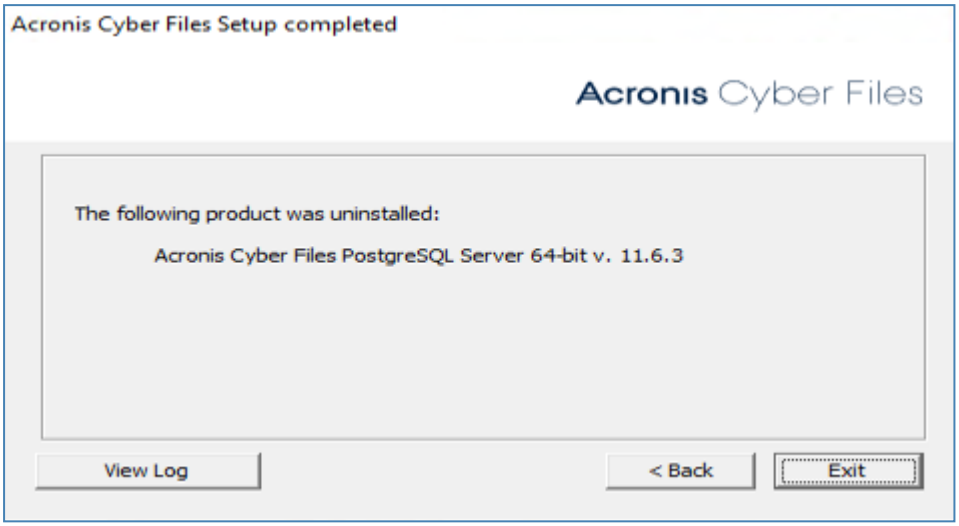
6. Klicken Sie auf **Deinstallieren...**. .
   Das folgende Warnungsdialogfeld wird angezeigt.



7. Klicken Sie auf **OK**.
   Das anfängliche Fenster zur Deinstallation vonAcronis Cyber Files wird wieder angezeigt.



8. Klicken Sie auf **Abbrechen**.
   Das folgende Bestätigungsfenster wird angezeigt.



9. Klicken Sie auf **Beenden**.
10. Starten Sie den Serverrechner neu.
11. Navigieren Sie zu `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common`, und löschen Sie den `PostgreSQL`-Ordner, wie in Schritt 6 angegeben.

Hinweis
Nach der Deinstallation sollte **AcronisAccessPostgreSQL** nicht mehr bei den Windows-Diensten aufgelistet sein.

Schritt 2: Neue Version von PostgreSQL installieren

So installieren Sie die neuere Version von PostgreSQL

1. Öffnen Sie die Systemsteuerung **Dienste**, und stoppen Sie Acronis Cyber Files Tomcat.
2. Starten Sie das Installationsprogramm für den neuen Acronis Cyber Files Server.

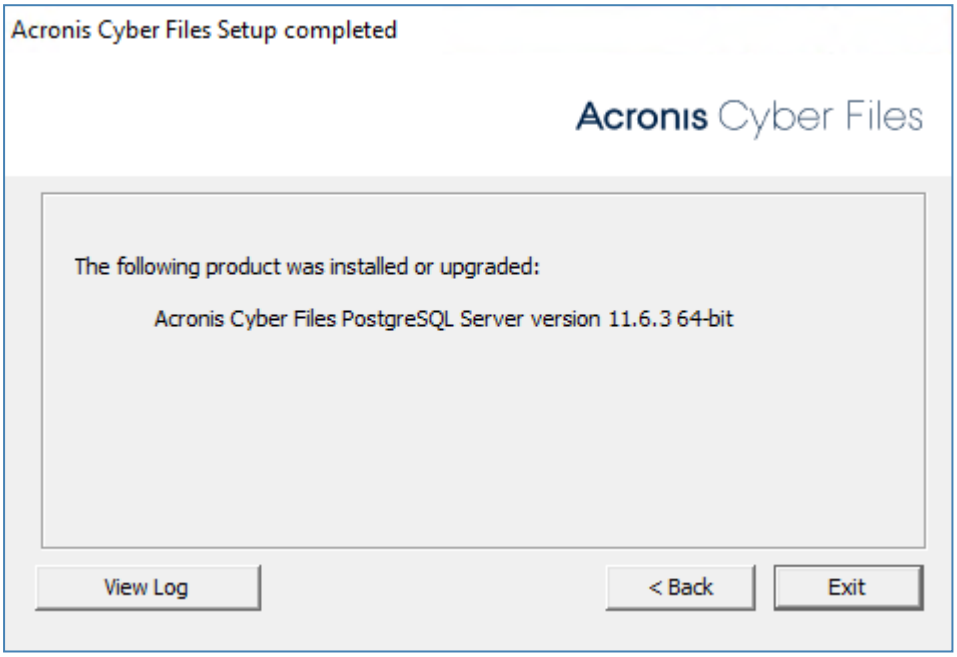
   Hinweis
   Die aktuelle Version des Installationsprogramms für den Acronis Cyber Files Server kann unter https://www.acronis.com/products/file-sync-and-share-downloads/ heruntergeladen werden. Oder kontaktieren Sie unseren technischen Support unter https://support.acronis.com/mobility.

3. Klicken Sie im Begrüßungsbildschirm auf **Weiter**.
4. Lesen Sie das End User License Agreement (EULA), und klicken Sie auf **OK**, um es zu akzeptieren.
5. Klicken Sie auf **Benutzerdefiniert**.
6. Wählen Sie nur die Acronis Cyber Files PostgreSQL Server-Komponente, und klicken Sie auf **Weiter**.
7. Bestätigen Sie den Standardspeicherort, an dem die DB installiert werden soll, und klicken Sie auf **Weiter**.

8. Legen Sie ein DB-Kennwort fest, und klicken Sie auf **Weiter**.
9. Klicken Sie auf **Installieren**, um die Installation der PostgreSQL-DB zu starten.

Hinweis
Die Dauer dieses Vorgangs ist von den Serverressourcen abhängig.

Nach der Installation wird das folgende Fenster angezeigt.



10. Klicken Sie auf **Beenden**.

Hinweis
Nach der Installation sollte **AcronisAccessPostgreSQL** wieder bei den Windows-Diensten aufgelistet sein.

Schritt 3: DB-Inhalt importieren

So importieren Sie den DB-Inhalt

1. Öffnen Sie die Acronis Cyber Files PostgreSQL Administrator-Anwendung, verbinden Sie sich mit dem lokalen Datenbankserver, und wählen Sie **Datenbanken**.
2. Bestätigen Sie, dass die Datenbank `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.

Hinweis
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 PostgreSQL Administrator, und öffnen Sie eine Eingabeaufforderung mit erweiterten Benutzerrechten.
6. Gehen Sie in der Eingabeaufforderung zum PostgreSQL-Bin-Verzeichnis.
   Beispiel:`cd "C:\Program Files\Acronis\Acronis Cyber Files\Common\PostgreSQL\<version>\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 das `postgres`-Kennwort ein, wenn Sie dazu aufgefordert werden.

Hinweis
Die Wiederherstellung kann einige Zeit dauern. Dies ist von der Größe Ihrer Datenbank abhängig.

10. Schließen Sie das Fenster mit der Eingabeaufforderung, wenn die Wiederherstellung beendet ist.
11. Öffnen Sie **Acronis Cyber Files PostgreSQL Administrator** erneut, und stellen Sie eine Verbindung mit dem lokalen Datenbankserver her.
12. Wählen Sie **Datenbanken** aus.
13. Erweitern Sie die Datenbank `acronisaccess_production`, erweitern Sie **Schemas**, und erweitern Sie **Öffentlich**. Überprüfen Sie, ob die Anzahl der **Tabellen** der Anzahl auf dem ursprünglichen Server entspricht.
14. Starten Sie den Datenbankdienst AcronisCyber Files PostgreSQL Server.

Aktualisieren des File Repository

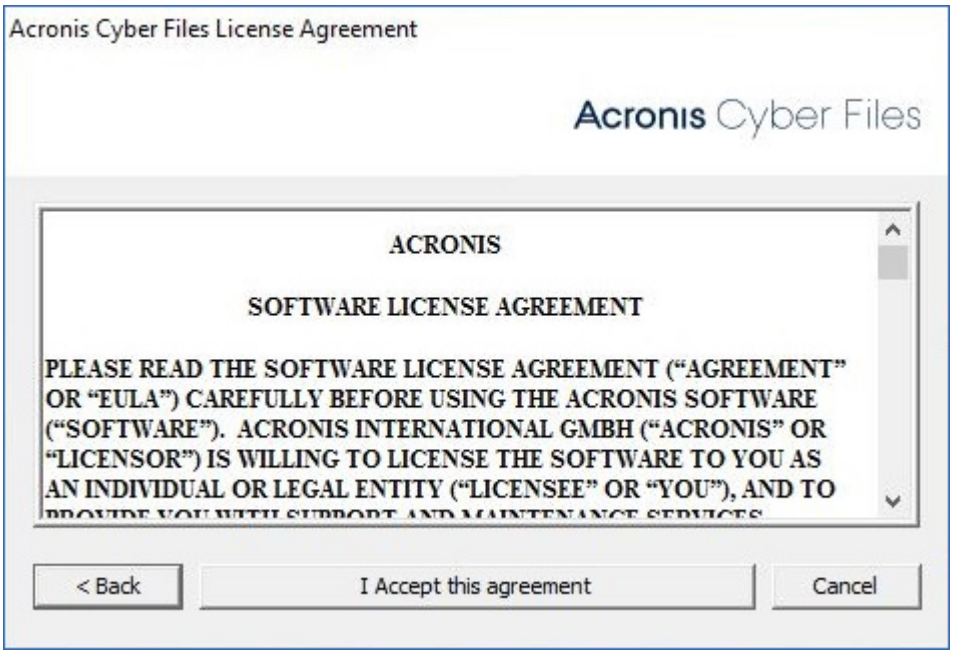
Aktualisieren Sie, ungeachtet des Speicherorts, zuerst das File Repository.

1. Kopieren Sie das Installationsprogramm von Acronis Cyber Files auf den Computer mit der File Repository-Komponente, und starten Sie die Installation.

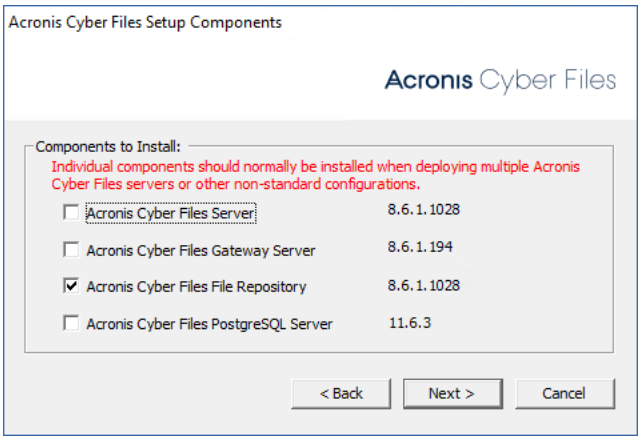
Hinweis
Wenn Sie über mehrere File Repository-Dienste verfügen, wiederholen Sie diese Schritte für alle Repositorys, bevor Sie mit den anderen Komponenten fortfahren.

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

3. Akzeptieren Sie die Lizenzvereinbarung.



4. Wählen Sie **Benutzerdefiniert...** und anschließend nur das **Acronis < PRODUCT_NAME>-File Repository** aus, für das ein Upgrade durchgeführt werden soll.



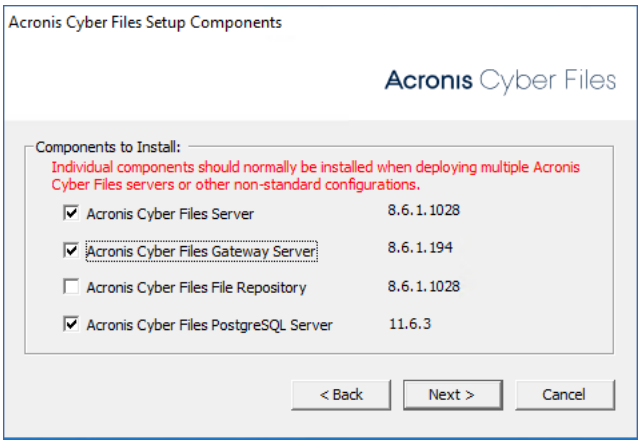
5. Klicken Sie auf **Weiter**, überprüfen Sie, was installiert werden soll, und klicken Sie auf **Installieren**.
6. Klicken Sie nach der Aktualisierung auf **Beenden**. Wenn das Konfigurationsdienstprogramm startet, klicken Sie auf **OK**.
7. Fahren Sie fort, indem Sie Ihren **primären** Acronis Cyber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

Durchführen eines Upgrades des Cyber Files-Primärservers

1. Kopieren Sie den Acronis Cyber Files Advanced Installer auf die Maschine mit dem **primären** Acronis Cyber Files Web Server.
2. Starten Sie das Acronis Cyber Files-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 Acronis Cyber Files-Dienste, für die Sie ein Upgrade durchführen möchten. Wählen Sie nur den Acronis Cyber Files Web Server und die Komponenten, die sich bereits auf dem Computer befinden.



5. Klicken Sie auf **Installieren,** lassen Sie das Installationsprogramm den Vorgang abschließen, und starten Sie das **Konfigurationsdienstprogramm**.

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

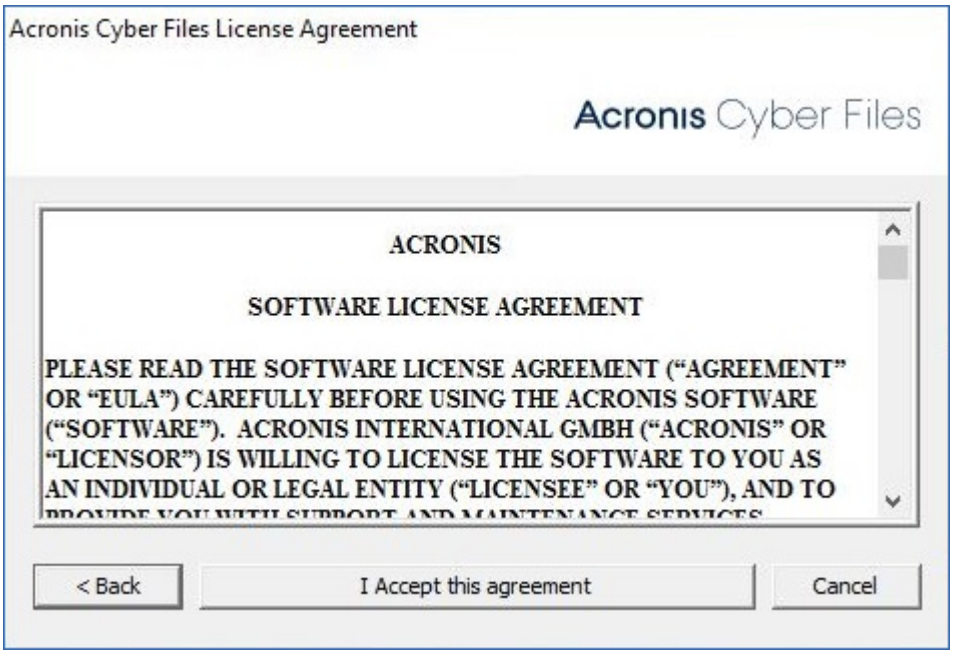
6. Nachdem das Konfigurationsdienstprogramm alle notwendigen Dienste gestartet hat und die Datenbankmigrationen beendet sind, überprüfen Sie, ob die Acronis Cyber Files-Weboberfläche des **Primärservers** ordnungsgemäß funktioniert. Ein Webbrowser mit dem Anmeldebildschirm für den Acronis Cyber Files-Server 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. Führen Sie diese Instanz von Acronis Cyber Files weiter aus, während Sie alle anderen Komponenten aktualisieren.

Warnung!
Upgraden oder starten Sie andere Acronis Cyber Files-Tomcat-Server erst, wenn der Tomcat-Primärserver ausgeführt wird und Sie überprüft haben, dass er ordnungsgemäß funktioniert.

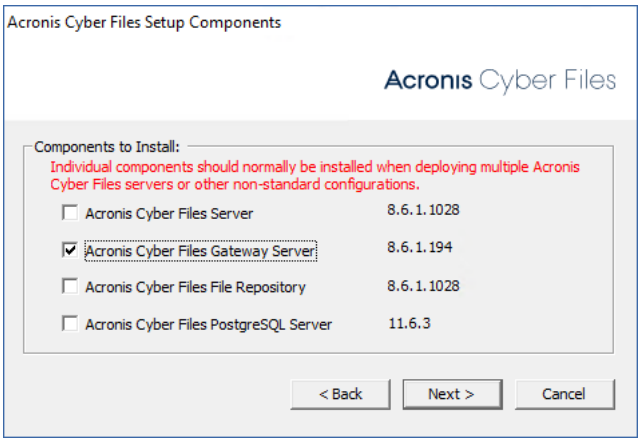
Durchführen eines Upgrades von Gateway Servern

1. Kopieren Sie das Acronis Cyber Files-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 Acronis Cyber Files 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**.

Durchführen eines Upgrades aller anderen Knoten

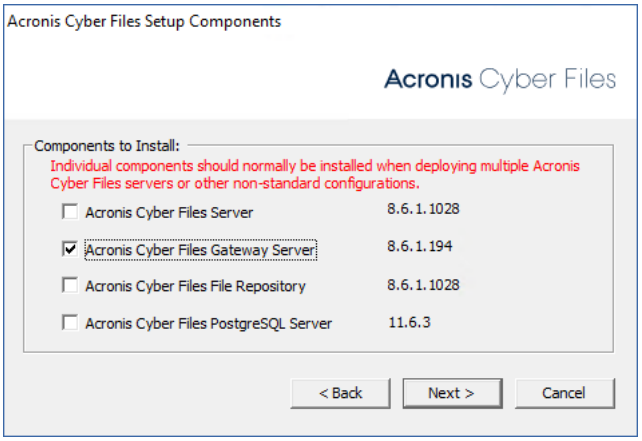
Nachdem Sie den **primären** Knoten von Acronis Cyber Files sowie alle Datei-Repository-Server und alle Gateway Server erfolgreich aktualisiert haben, müssen Sie damit fortfahren, die restlichen Acronis Cyber Files Server zu aktualisieren.

1. Kopieren Sie das AcronisCyber Files-Installationsprogramm in den gewünschten Knoten, und starten Sie ihn.

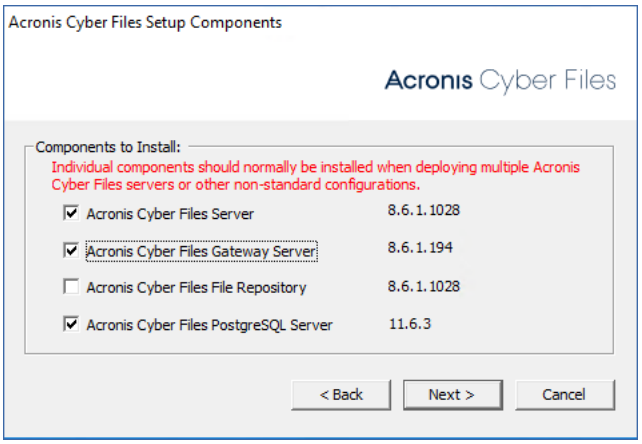
2. Klicken Sie im Begrüßungsbildschirm auf **Weiter** und dann auf **Benutzerdefiniert**. Dadurch können Sie nur die notwendigen Dienste upgraden, die sich bereits auf dem Computer befinden, ohne weitere zu installieren.

3. Wählen Sie einen AcronisCyber Files-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 Server als auch ein Acronis Cyber Files Server vorhanden ist, wählen Sie beide aus.



4. Klicken Sie auf **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, dass die AcronisCyber Files-Komponenten auf diesem Knoten wie erwartet arbeiten.

Mobiler Zugriff

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

Begrifflichkeiten

Acronis Mobile Cyber Files-Clients stellen direkt eine Verbindung zu Ihrem Server her und verwenden keinen Dienst eines Drittanbieters, sodass Sie weiterhin die Kontrolle behalten. Acronis Cyber Files-Server können in demselben Netzwerk installiert werden wie vorhandene Dateiserver, sodass iPads, iPhones und Android-Geräte auf Dateien zugreifen können, die sich in dem betreffenden 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 Acronis Cyber Files-Server zu. In Acronis Cyber Files müssen keine zusätzlichen Konten konfiguriert werden. Die Acronis Cyber Files-App unterstützt darüber hinaus den Dateizugriff mit lokalen Computerkonten, die auf dem Windows-Server konfiguriert wurden, auf dem Acronis Cyber Files 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.

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

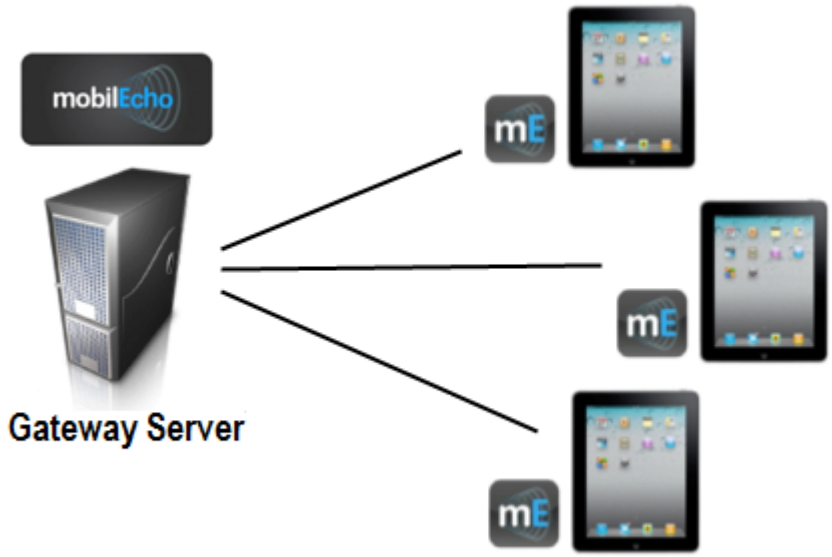


Abb. 1. Einzelner Acronis Cyber Files-Server mit einem lokalen Gateway Server

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

Hinweis
Einzelheiten zur Installation von Acronis Cyber Files finden Sie im Bereich Installieren dieser Anleitung. Die Konfiguration von Gateway Servern und Datenquellen wird im Bereich Mobile Access erläutert.

Wenn Sie die mobilen Clients remote verwalten möchten, können Sie mit der Acronis Cyber Files-Verwaltung Richtlinien jeweils pro Active Directory-Benutzer oder -Gruppe erstellen. Es ist nur ein Acronis Cyber Files 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 Acronis Cyber Files 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, Acronis Cyber Files-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 Clientverwaltung besteht aus einem Server, auf dem die Komponenten Acronis Cyber Files Server und Acronis Cyber Files Gateway Server installiert sind, sowie einigen weiteren Gateway Servern, die als Dateiserver fungieren. In diesem Szenario sind alle mobilen Clients so konfiguriert, dass sie vom Acronis Cyber Files Server verwaltet werden. Sie kontaktieren diesen Server bei jedem Start der Acronis Cyber Files-Applikation, um gegebenenfalls nach Änderungen in den Einstellungen zu suchen, zurückgesetzte Kennwörter zum Sperren der Applikation zu akzeptieren und Befehle zum standortfernen Löschen auszuführen.

Acronis Cyber Files-Clients können in ihrer Verwaltungsrichtlinie eine Liste von Servern, bestimmte Ordner in freigegebenen Volumes und Basisverzeichnisse zugewiesen werden. Diese Ressourcen erscheinen automatisch in der Acronis Cyber Files-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 und Mobile Geräte verwalten.

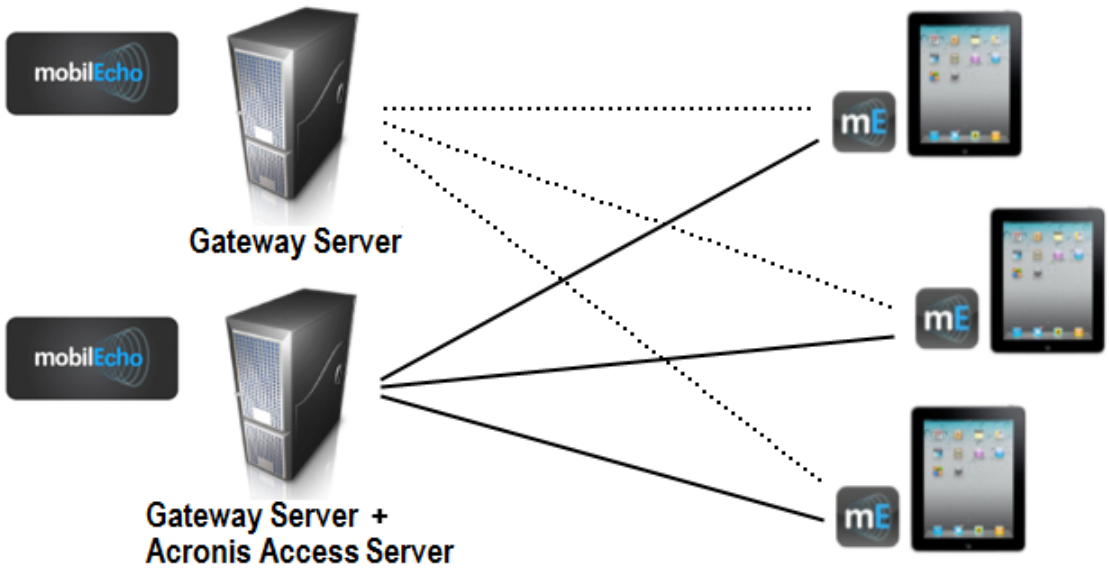


Abb. 2. Ein Gateway Server, ein Gateway Server + Acronis Cyber Files Server

Richtlinien

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

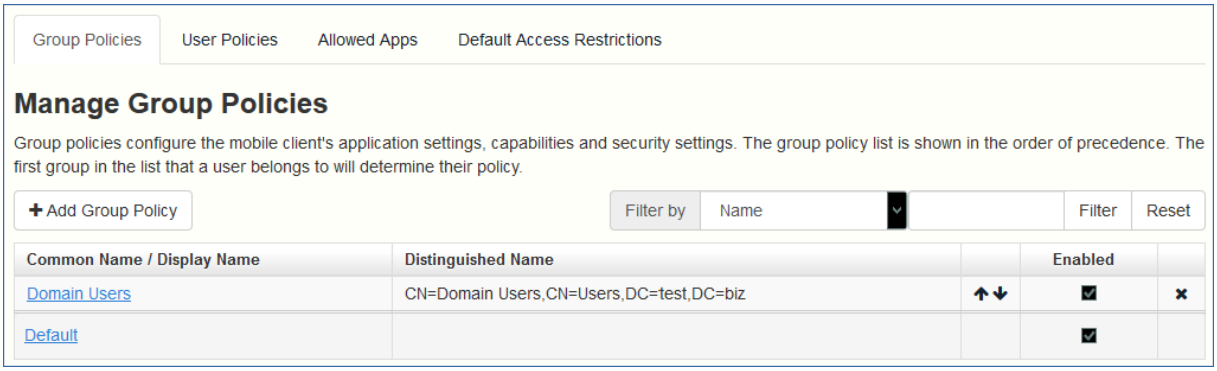
Server kontaktieren, werden ihre Einstellungen durch die einzelne Gruppenrichtlinie mit der höchsten Priorität bestimmt, deren Mitglied sie sind.

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.

Hinweis

Tipps zur Gruppenverwaltung

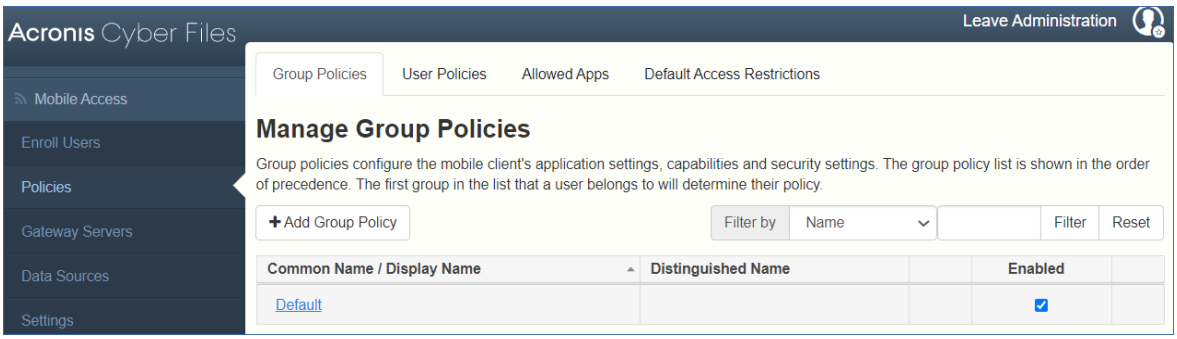
Wenn Sie möchten, dass für alle oder die meisten Ihrer Benutzer dieselben Richtlinieneinstellungen gelten, können Sie die **Standard**-Gruppenrichtlinie aktivieren. Wenn diese aktiviert ist, werden alle Benutzer, die nicht Mitglieder einer Gruppenrichtlinie sind und für die keine spezifische Benutzerrichtlinie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



Hinzufügen einer neuen Richtlinie

So fügen Sie eine neue Gruppenrichtlinie hinzu:

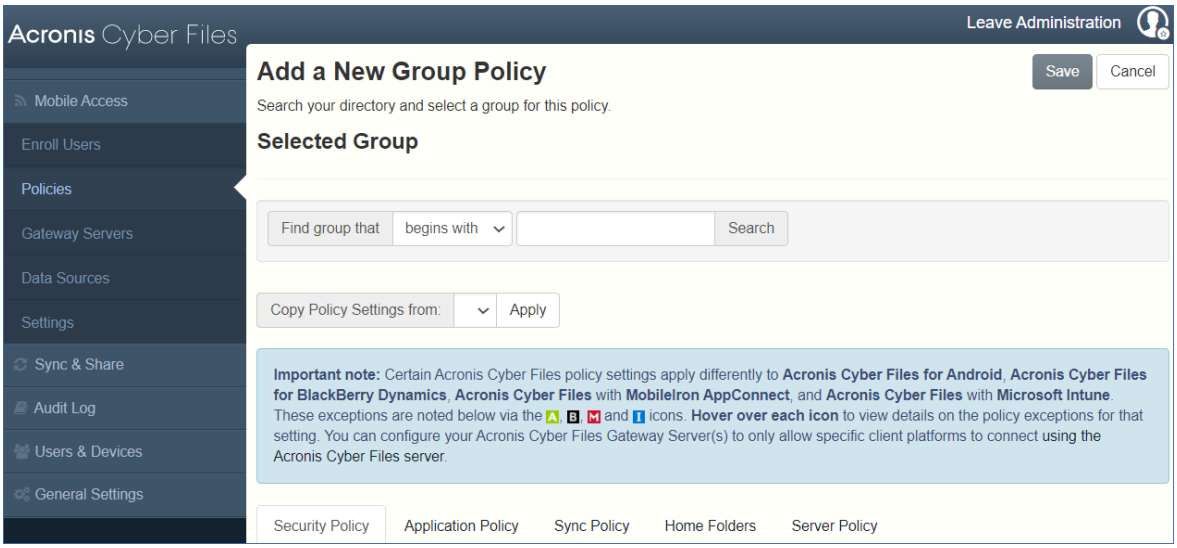
1. Öffnen Sie die Registerkarte **Gruppenrichtlinien**.
2. Klicken Sie auf die Schaltfläche **Neue Richtlinie hinzufügen**, um eine neue Gruppenrichtlinie hinzuzufügen. Die Seite **Eine neue Gruppenrichtlinie hinzufügen** wird geöffnet.



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, Applikation, Synchronisierung, Basisordner und Server), und klicken Sie auf **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, Applikation, Synchronisierung, Basisordner und Server), und klicken Sie auf **Speichern**.

Ändern von Richtlinien

Bestehende Richtlinien können jederzeit geändert werden. Änderungen an Richtlinien werden auf den entsprechenden Benutzer der mobilen App angewendet, sobald ein Benutzer die mobile App das nächste Mal startet.

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

So ändern Sie eine Gruppenrichtlinie:

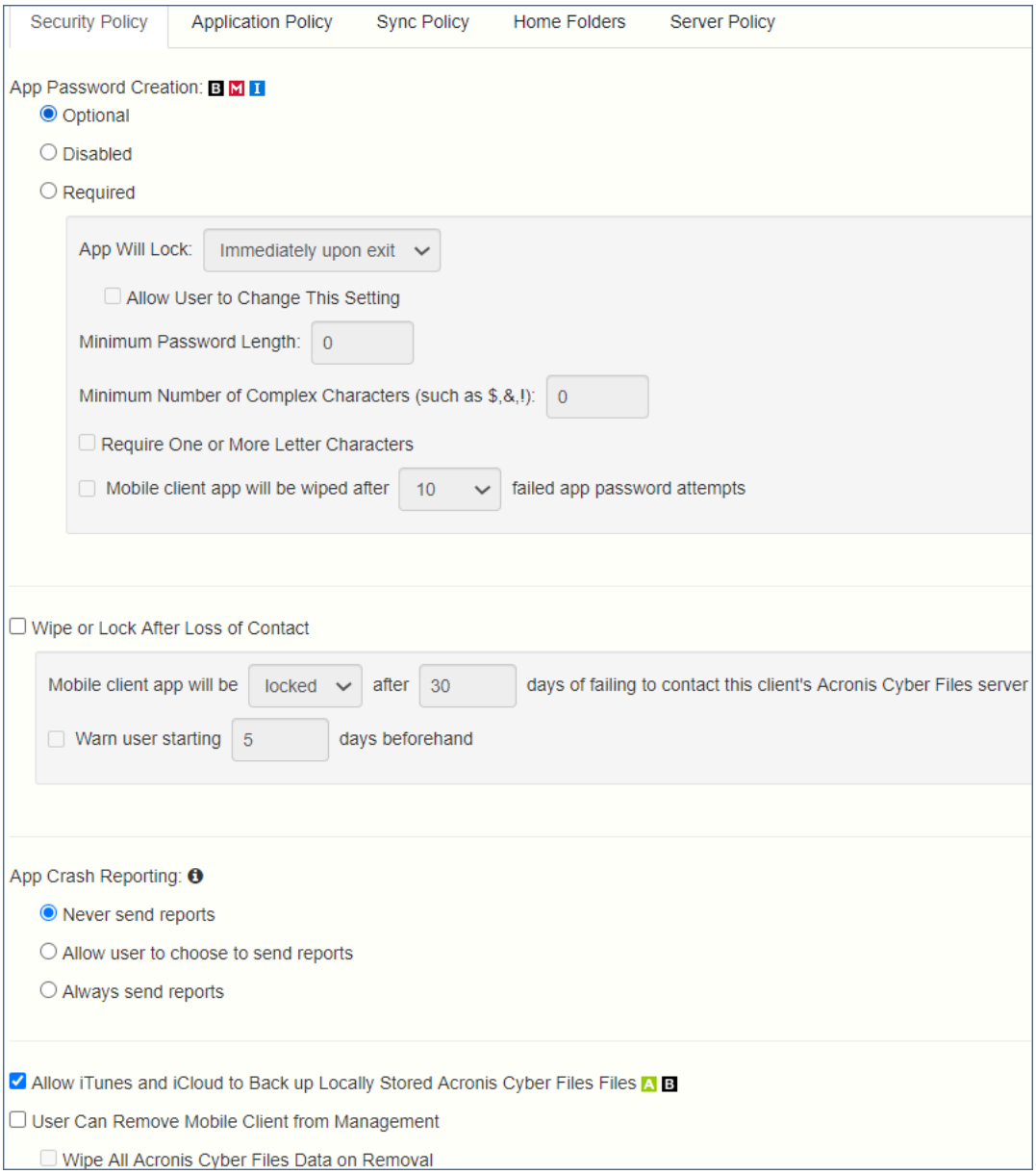
1. Klicken Sie in der oberen Menüleiste auf **Gruppenrichtlinien**.
2. Klicken Sie auf die Gruppe, die Sie ändern möchten.
3. Nehmen Sie die erforderlichen Änderungen auf der Seite **Gruppenrichtlinie bearbeiten** vor und drücken Sie **Speichern**.
4. Um eine Richtlinie vorübergehend zu deaktivieren, 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. Öffnen Sie die Registerkarte **Benutzerrichtlinien**.
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.

Richtlinieneinstellungen

Sicherheitsrichtlinie



- **App-Kennwort erstellen** – Die Mobile App kann mit einem Sperrkennwort versehen werden, das eingegeben werden muss, wenn die Applikation gestartet wird.
  - **Optional** – Wenn diese Option aktiviert ist, muss der Benutzer nicht zwangsläufig ein Sperrkennwort für die Applikation konfigurieren, kann aber bei Bedarf ein Kennwort in der App über das Menü **Einstellungen** festlegen.
  - **Deaktiviert** – Diese Einstellung deaktiviert die Möglichkeit, ein Kennwort zum Sperren der App über das Menü **Einstellungen** zu konfigurieren. Dies kann nützlich sein, wenn Mobilgeräte

gemeinsam genutzt werden und Sie verhindern wollen, dass einer dieser Benutzer ein App-Kennwort festlegt und damit andere Benutzer von der App aussperren kann.

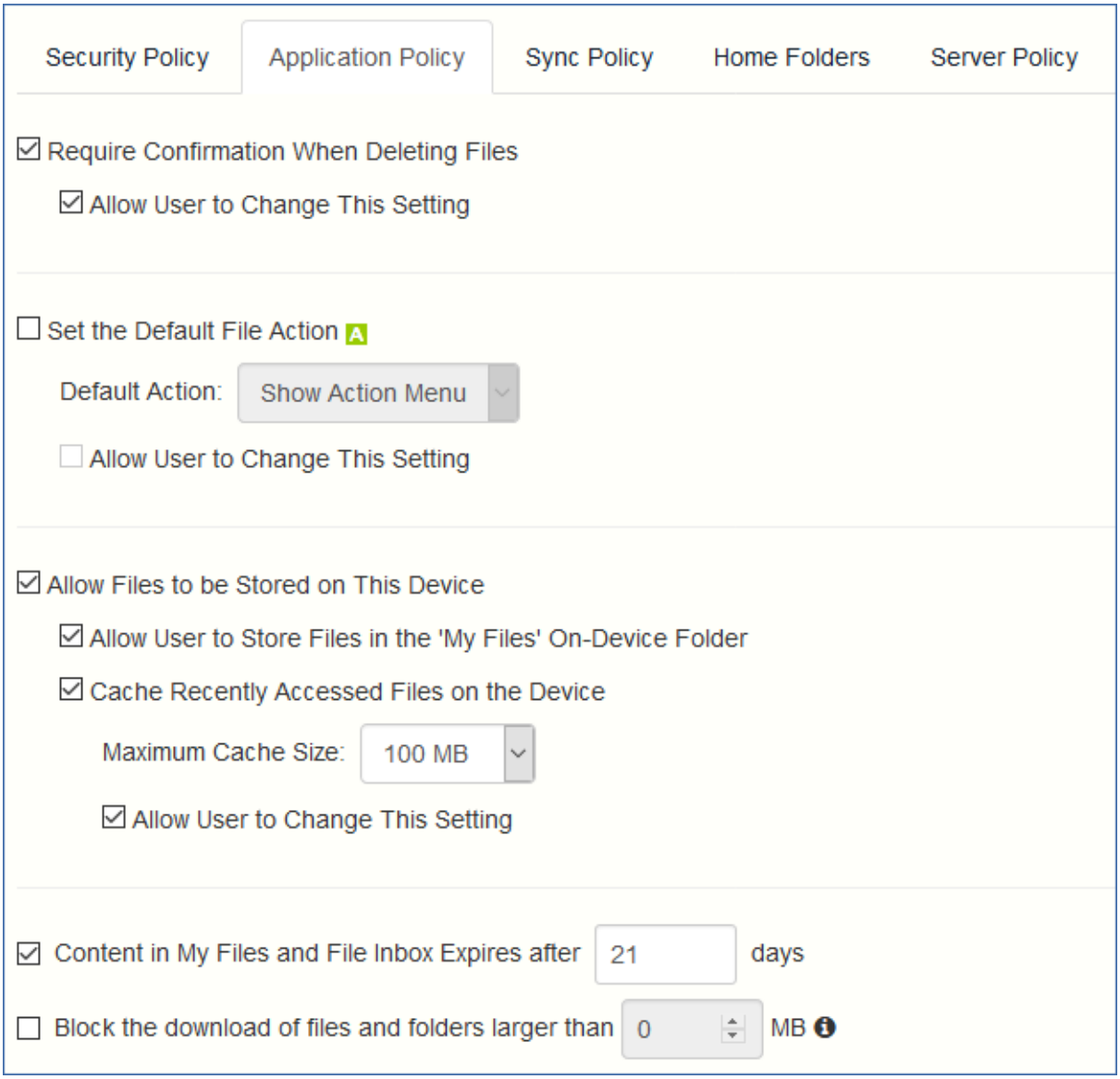
- **Erforderlich** – Diese Einstellung zwingt den Benutzer, ein Sperrkennwort für die App zu konfigurieren, wenn er noch keines hat. Die optionalen Kennwort-Komplexitätsanforderungen für die Applikation und die Einstellung zum Löschen bei fehlgeschlagenen Kennwortversuchen gelten nur, wenn die Option **App-Kennwort erstellen** auf **Erforderlich** festgelegt ist.
  - **App wird sich sperren** – Diese Einstellung konfiguriert die Gültigkeitsdauer des App-Kennworts. Wenn ein Benutzer auf seinem Gerät von der Acronis Cyber Files Mobile App zu einer anderen App wechselt, wird er nicht aufgefordert, das Kennwort für die Sperrung der App einzugeben, wenn er innerhalb dieser Gültigkeitsdauer zur Mobile App zurückkehrt. Wenn Sie wollen, dass das Kennwort jedes Mal eingegeben werden muss, wählen Sie **Sofort beim Beenden**. Wenn Sie wollen, dass der Benutzer die Einstellung **App wird sich sperren** in den Einstellungen der Mobile App ändern kann, wählen Sie **Benutzer erlauben, diese Einstellung zu ändern**.
  - **Minimale Kennwortlänge** – Die erlaubte Mindestlänge für das Kennwort zur Sperrung der Applikation.
  - **Mindestanzahl an komplexen Zeichen** – Die Mindestanzahl an Sonderzeichen (Nicht-Buchstaben und Nicht-Zahlen) für das Kennwort zum Sperren 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 Kontaktverlust zurücksetzen 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 AcronisCyber Files-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 mobilen App gespeicherten Dateien unmittelbar gelöscht, die Richtlinie zur Clientverwaltung 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 Acronis Cyber Files Server dieses Clients** – Legen Sie die Standardaktion fest, wenn der Client diesen Acronis Cyber Files Server für eine bestimmte

Anzahl von Tagen nicht kontaktieren konnte.
    - **Benutzer [ ] Tage vorher warnen** – Die Mobile-App kann den Benutzer optional warnen, wenn in naher Zukunft ein Remote-Löschen oder -Sperren aufgrund eines 'Kontaktverlusts' durchgeführt wird. Dadurch erhält der Benutzer die Möglichkeit, eine Netzwerkverbindung wiederherzustellen, über die die Mobile-App Kontakt zu seinem Acronis Cyber Files Server aufnehmen kann, um das Sperren oder Löschen zu verhindern.
- **App-Absturzbericht** – Sendet Berichte an Acronis, wenn die Mobile Apps abstürzen. Dabei werden keine privaten Daten oder Identifizierungsinformationen gesendet.
    - **Keine Berichte senden**
    - **Benutzer kann Versenden einzeln entscheiden**
    - **Immer Berichte senden**
- **iTunes und iCloud erlauben, lokal gespeicherte Acronis Cyber Files-Dateien per Backup zu sichern** – Wenn diese Einstellung deaktiviert ist, unterbindet es die Mobile App, dass iTunes oder iCloud ein Backup ihrer Dateien erstellen kann. Dadurch wird sichergestellt, dass keine Dateien aus dem sicheren Storage von Acronis Cyber Files in Backups kopiert werden.
- **Benutzer kann Mobile Client aus der Verwaltung entfernen** – Aktivieren Sie diese Einstellung, wenn die AcronisCyber Files-Benutzer die Möglichkeit haben sollen, ihre Verwaltungsrichtlinie in AcronisCyber Files zu deinstallieren. Hierdurch wird die vollständige Funktionalität der Applikation wiederhergestellt und alle Änderungen an der Konfiguration werden durch die Richtlinie zurückgesetzt.
    - **Beim Entfernen alle Acronis Cyber Files-Daten vollständig löschen** – Wenn das Entfernen von Richtlinien durch den Benutzer aktiviert ist, kann diese Option ausgewählt werden. Wenn diese Option aktiviert ist, werden alle lokal in der Mobile App gespeicherten Daten gelöscht, wenn diese aus der Verwaltung entfernt wird. Auf diese Weise wird sichergestellt, dass keine Unternehmensdaten auf einem nicht verwalteten Client verbleiben.

Anwendungsrichtlinie

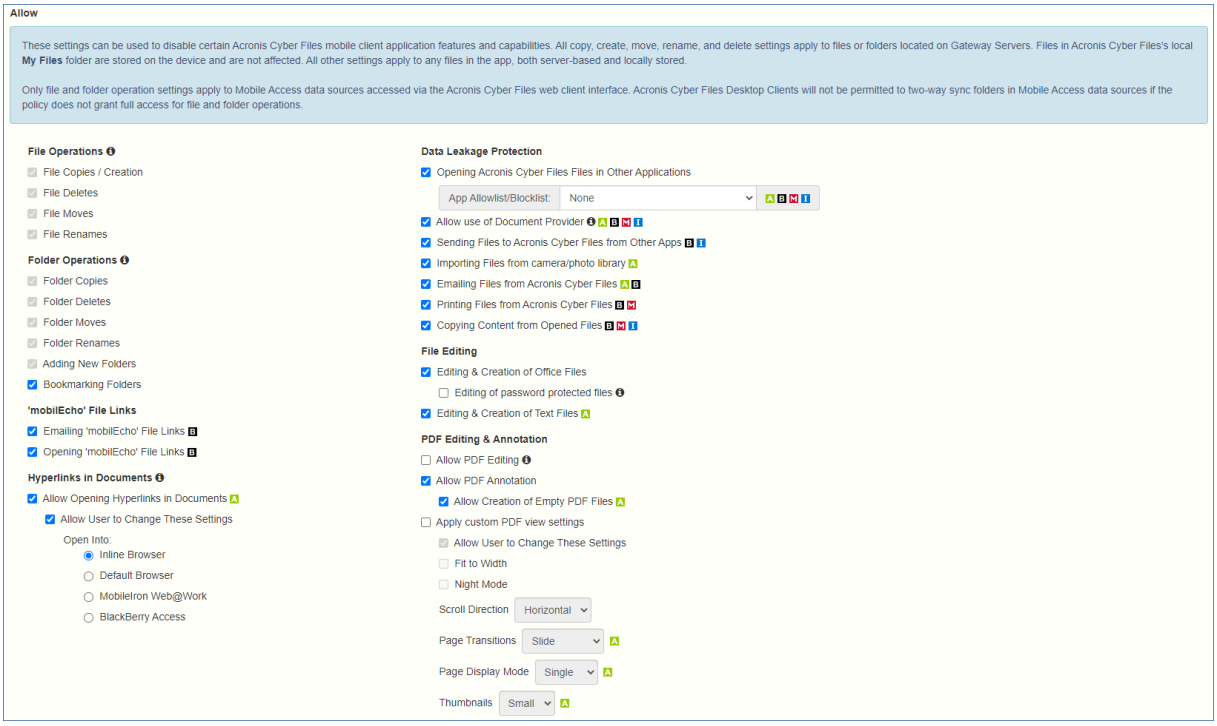


- **Bestätigung beim Löschen von Dateien verlangen** – Wenn diese Option aktiviert ist, wird der Benutzer jedes Mal, wenn er eine Datei löscht, um eine Bestätigung gebeten. Wenn Sie möchten, dass der Benutzer diese Einstellung später ändern kann, wählen Sie **Benutzer erlauben, diese Einstellung zu ändern**.
- **Die Standarddateiaktion festlegen** – Diese Option bestimmt, was passiert, wenn ein Benutzer in der Mobile-Applikation auf eine Datei tippt. Wenn dies nicht festgelegt ist, wird die Client-Applikation standardmäßig das **Aktionsmenü** aufrufen. Wenn Sie möchten, dass der Benutzer diese Einstellung später ändern kann, wählen Sie **Benutzer erlauben, diese Einstellung zu ändern**.
- **Erlauben, dass Dateien auf diesem Gerät gespeichert werden** – Diese Einstellung ist standardmäßig aktiviert. Wenn sie aktiviert ist, dürfen Dateien auf dem Gerät innerhalb des Sandbox-Storage von Cyber Files gespeichert werden. Individuelle Funktionen, die Dateien lokal

speichern (z.B. im Ordner 'Meine Dateien', im Synchronisierungsordner oder im Cache für zuletzt verwendete Dateien), können über zusätzliche Richtlinieneinstellungen aktiviert oder deaktiviert werden. Wenn diese Option deaktiviert ist, werden keine Dateien auf dem Gerät gespeichert, was sicherstellt, dass keine Unternehmensdaten auf dem Gerät sind, wenn dieses verloren gehen oder gestohlen werden sollte. Wenn diese Einstellung deaktiviert ist, kann der Benutzer keine Dateien speichern oder synchronisieren, um diese offline zu verwenden, keine Dateien cachen, um die Performance zu verbessern, oder Dateien aus anderen Applikationen über die Funktio 'Öffnen mit' an den Cyber Files Mobile Client senden.

  - **Benutzern erlauben, Dateien im Geräteordner 'Meine Dateien' zu speichern** – Wenn diese Option aktiviert ist, können Dateien in den Ordner 'Meine Dateien' kopiert werden, um diese offline verfügbar zu haben und bearbeiten zu können. Dies ist ein allgemeiner Speicherbereich innerhalb des Sandbox-Storage von Cyber Files auf dem Gerät.
  - **Kürzlich verwendete Dateien auf dem Gerät zwischenspeichern (cachen)** – Wenn diese Option aktiviert ist, werden serverbasierte Dateien, auf die kürzlich zugegriffen wurde, in einem lokalen Cache auf dem Gerät zwischengespeichert, um bei erneutem Zugriff (sofern sie nicht verändert wurden) Performance- und Bandbreiten-Einsparungen zu ermöglichen. Es kann eine **Maximale Cache-Größe** spezifiziert werden und der Benutzer optional berechtigt werden, diese Einstellung zu ändern.
- **Inhalte in 'Meine Dateien' und 'Datei-Inbox' verfallen nach X Tagen** – Wenn diese Option aktiviert ist, werden Dateien in **Meine Dateien** nach einer 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-Anwendung 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 Cyber Files, also sowohl für serverbasierte als auch für lokal auf dem Client gespeicherte Dateien.

Dateivorgänge

- **Dateien kopieren / erstellen** – Wenn diese Option deaktiviert ist, kann der Benutzer keine Dateien von anderen Applikationen oder aus der iPad-Foto-Bibliothek auf einem Gateway Server speichern. Er kann auch keine Dateien oder Ordner auf dem Gateway Server kopieren oder erstellen. Diese Einstellung hat Vorrang vor etwaigen NTFS-Berechtigungen, die der Client haben könnte, um Dateien erstellen zu dürfen.
- **Dateien löschen** – Wenn diese Option deaktiviert ist, können Benutzer keine Dateien vom Gateway Server löschen. Diese Einstellung überschreibt sämtliche Berechtigungen in NTFS, aufgrund derer der Client möglicherweise Dateien löschen darf.
- **Dateien verschieben** – Wenn diese Option deaktiviert ist, kann der Benutzer keine Dateien von einem Speicherort zu einem anderen auf dem Gateway Server verschieben oder vom Server zum lokalen 'Meine Dateien'-Storage der Mobile-Applikation. Diese Einstellung hat Vorrang vor allen NTFS-Berechtigungen, die der Client möglicherweise hat und die das Verschieben von Dateien oder Ordnern erlauben.
- **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, kann der Benutzer keine Ordner auf dem Gateway Server kopieren. Diese Einstellung hat Vorrang vor etwaigen NTFS-Berechtigungen, die der Client haben könnte, um Ordner erstellen zu dürfen. **Dateien kopieren / erstellen** muss eingeschaltet sein, damit diese Einstellung aktiviert werden kann.
- **Ordner löschen** – Wenn diese Option deaktiviert ist, kann der Benutzer keine Ordner vom Gateway Server löschen. Diese Einstellung hat Vorrang vor etwaigen NTFS-Berechtigungen, die der Client haben kann, um Ordner löschen zu dürfen.
- **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 mobilen Acronis Cyber Files-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, kann der Benutzer keine Ordner vom Gateway Server umbenennen. Diese Einstellung hat Vorrang vor etwaigen NTFS-Berechtigungen, die der Client haben kann, um Ordner umbenennen zu dürfen.

- **Neue Ordner hinzufügen** – Wenn diese Option deaktiviert ist, können Benutzer keine neuen und damit leeren Ordner auf dem Gateway Server erstellen.
- **Ordner als Lesezeichen** – Wenn diese Option deaktiviert ist, kann der Benutzer keine Lesezeichen für Acronis Cyber Files-Ordner auf dem Gerät oder auf dem Server setzen, um schnell auf diese Ordner per Shortcut zugreifen zu können.

'mobilEcho'-Datei-Links

- **'mobilEcho'-Dateilinks per E-Mail versenden** – Wenn diese Option deaktiviert ist, können Benutzer keine mobilEcho://-URLs auf Acronis Cyber Files-Dateien oder -Ordner an andere Acronis Cyber Files-Benutzer senden. Diese Links funktionieren nur, wenn sie von einem Gerät aus geöffnet werden, auf dem der Empfänger den Acronis Cyber Files Mobile Client installiert hat und mit einem Server oder zugewiesenen Ordner konfiguriert ist, der Zugriff auf den Link-Speicherort hat. Der Benutzer muss außerdem über eine Berechtigung auf Datei-/Ordnerebene verfügen, um das Element lesen zu können.
- **'mobilEcho'-Datei-Links öffnen** – Wenn diese Option deaktiviert ist, können die Benutzer keine mobilEcho://-URLs auf Acronis Cyber Files-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 je nach Bedarf zu aktivieren oder zu deaktivieren.

  Öffnen in:
  - **Interner Browser** – Hyperlinks werden direkt in der Acronis Cyber Files App geöffnet.
  - **Standard-Browser** – Hyperlinks werden in dem auf Ihrem Gerät ausgewählten Standardbrowser geöffnet.
  - **MobileIron Web@Work** – Hyperlinks werden in der MobileIron Web@Work App geöffnet.

Schutz vor Datenverlust

- **Acronis Cyber Files-Dateien in anderen Applikationen öffnen** – Wenn diese Option deaktiviert ist, wird die Mobile-Applikation die **Öffnen in**-Schaltfläche nicht anzeigen und es nicht erlauben, dass Dateien in Acronis Cyber Files in anderen Applikationen geöffnet werden. Denn wenn eine Datei in einer anderen Applikation geöffnet wird, wird diese Datei dann in den Datenspeicherbereich dieser Applikation kopiert und gerät damit aus dem Kontrollbereich von Acronis Cyber Files.
  - **Positivliste/Blockliste für Apps** – Wählen Sie eine vordefinierte Positivliste oder Blockliste aus, die Drittanbieter-Apps einschränkt, in denen Acronis Cyber Files-Dateien auf dem Gerät geöffnet werden könnten. Wenn Sie eine Positivliste oder Blockliste erstellen wollen, klicken Sie in der oberen Menüleiste auf **Erlaubte Apps**.
- **Dokument-Provider-Nutzung erlauben** – Ermöglicht Mobilgeräten, die Document Provider Extension für Acronis Cyber Files zu verwenden. Die Document Provider Extension kann von bestimmten Konfigurationen beeinflusst werden:

a. Wenn ein Client von einem älteren Server verwaltet wird, ist die Document Provider Extension deaktiviert, es sei denn, die Option **AcronisCyber Files-Dateien in anderen Applikationen öffnen** ist **deaktiviert** oder eine Block- oder Positivliste ist **aktiviert**.
b. Wenn ein Client von einem neuen Server (Version 7.3.1 und höher) verwaltet wird und die Option **Document Provider-Nutzung erlauben** aktiviert ist, können die Benutzer nach wie vor Dateien mit anderen Apps gemeinsam nutzen, selbst wenn die Option **Acronis Cyber Files-Dateien in anderen Applikationen öffnen deaktiviert** oder eine Block- oder Positivliste **aktiviert** ist. Das gilt selbst für eigens gesperrte Apps.
c. Wenn die Option **Document 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 AcronisCyber Files-Datenquellen speichern.

- **Dateien von anderen Apps aus an Acronis Cyber Files senden** – Wenn diese Option deaktiviert ist, akzeptiert die Mobile-Applikation keine Dateien, die von anderen Applikationen über die Funktion **Öffnen in** 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 Acronis Cyber Files importieren.
- **Dateien von Acronis Cyber Files aus per E-Mail senden** – Wenn diese Option deaktiviert ist, zeigt die Mobile-Applikation nicht die Schaltfläche **Datei per E-Mail senden** an und unterbindet es, dass Dateien in Acronis Cyber Files aus der Applikation heraus per E-Mail versendet werden können.

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

- **Dateien von Acronis Cyber Files aus drucken** – Wenn diese Option deaktiviert ist, zeigt die Mobile-Applikation nicht die Schaltfläche **Drucken** an und unterbindet es, dass Dateien in Acronis Cyber Files ausgedruckt werden können.
- **Text aus geöffneten Dateien kopieren** – Wenn diese Option deaktiviert ist, erlaubt die Mobile App Benutzern nicht, Text in geöffneten Dokumenten für Kopieren-/Einfügen-Aktionen auszuwählen. Dadurch wird verhindert, dass Daten zu anderen Applikationen kopiert werden können.

Warnung!
Wenn eine MobileIron-Richtlinie aktiv ist, überschreibt die Einstellung `Allow Copy/Paste To` diese Einstellung.

Dateibearbeitung

- **Bearbeiten & Erstellen von Office-Dateien** – Wenn diese Option deaktiviert ist, können Benutzer keine Dokumente mit dem integrierten Polaris-Editor bearbeiten.

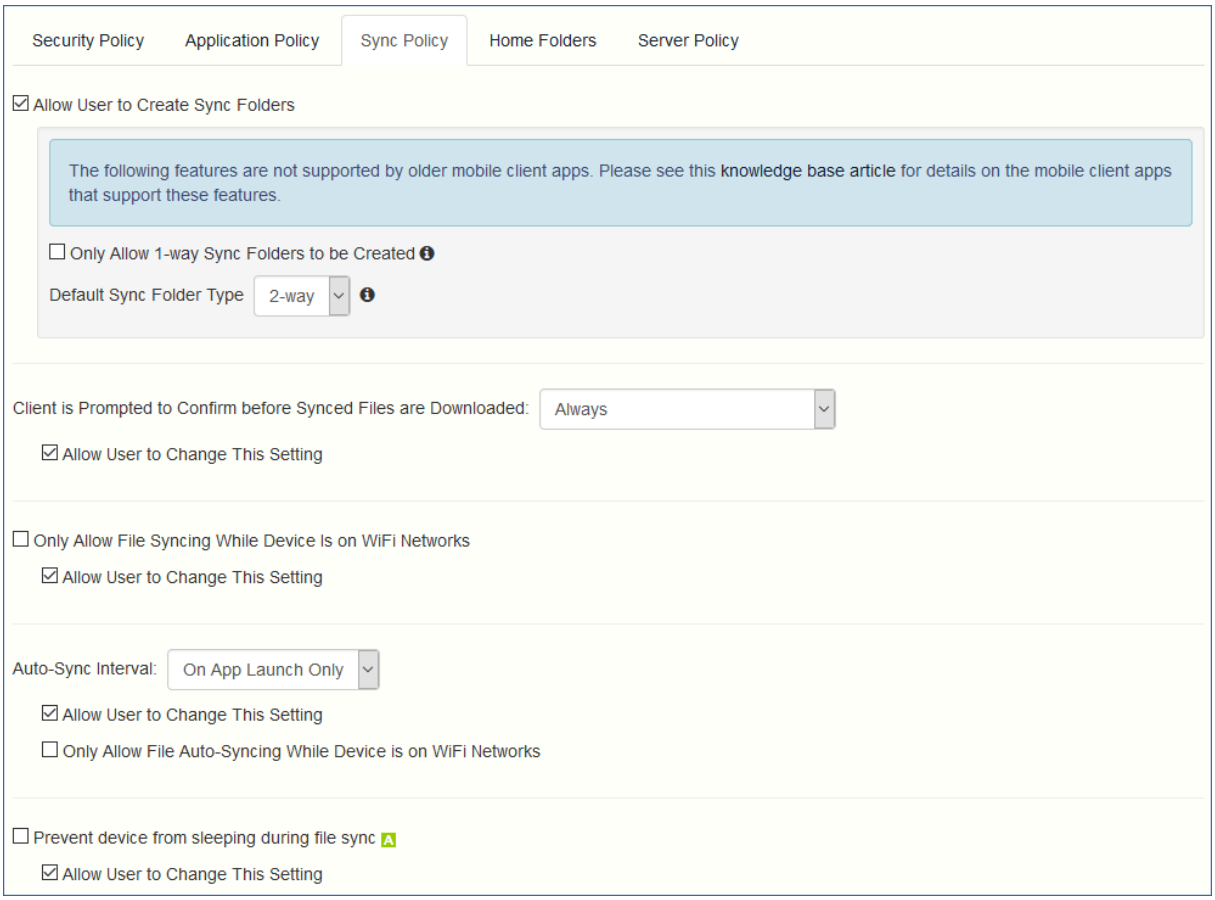
- **Bearbeiten von kennwortgeschützten Dateien** – Wenn diese Option aktiviert ist, können Benutzer keine kennwortgeschützten Dateien bearbeiten.
- **Bearbeiten & Erstellen von Textdateien** – Wenn diese Option deaktiviert ist, können Benutzer keine txt-Dateien mit dem integrierten Texteditor bearbeiten.

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, können Benutzer ihre PDF-Anzeige-Einstellungen ändern.
  - **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.
  - **Seitenanzeige** – Hiermit können Sie den Anzeigemodus wählen – jeweils eine oder zwei Seiten gleichzeitig.
  - **Miniaturbilder (Thumbnails)** – Hiermit wird die Größe für die Miniaturbilder der PDF-Seiten festgelegt. Sie können zwischen **Klein**, **Groß** und **Ohne** wählen.
  - **Suchmodus** – 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** – Hiermit können Sie die Farbe zum Hervorheben von Hyperlinks festlegen. Alternativ können Sie die Hervorhebung durch Wahl von **Deaktiviert** auch ausschalten.
  - **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.

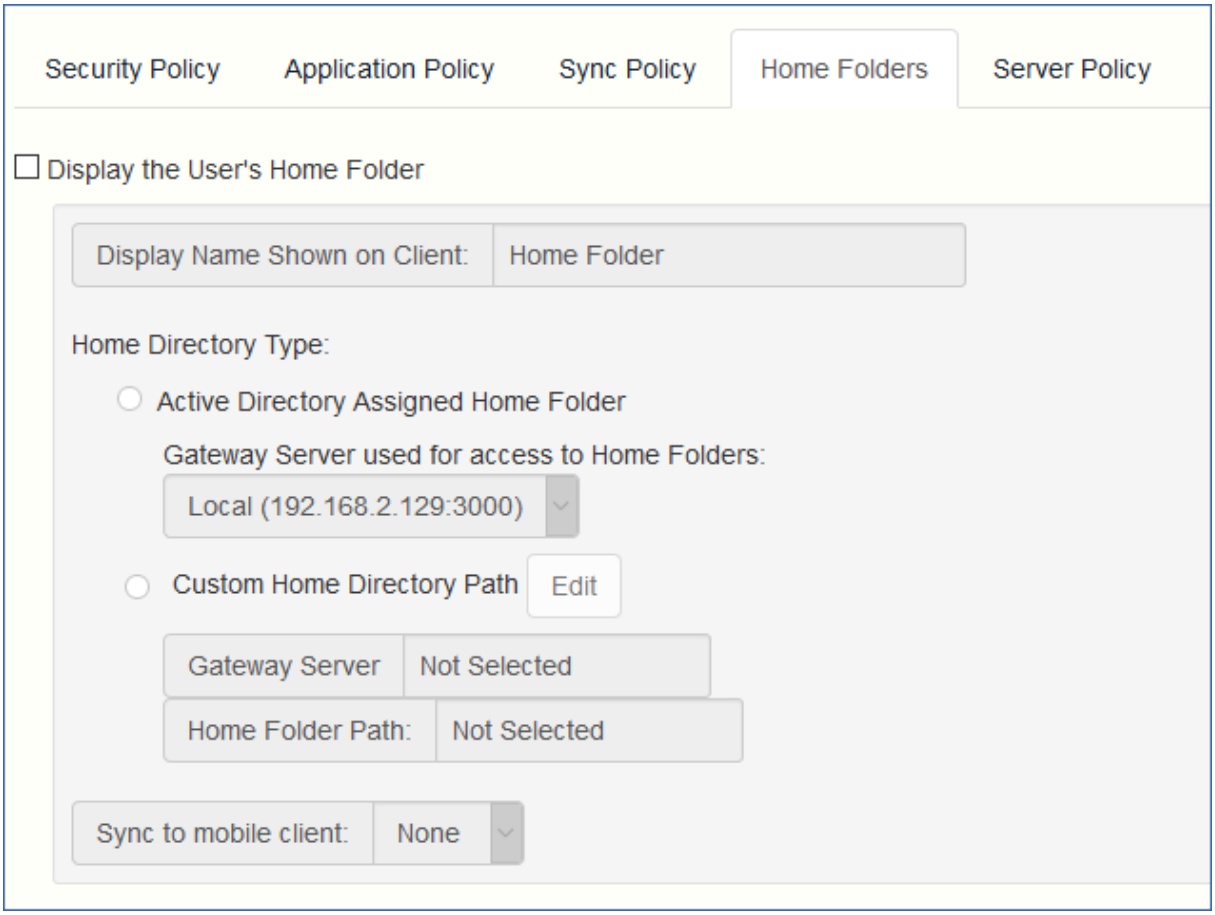
Sync-Richtlinie



- **Benutzern erlauben, Sync-Ordner zu erstellen** – Erlaubt dem Benutzer, eigene Synchronisierungsordner zu erstellen.
  - **Nur das Erstellen von 1-Weg-Sync-Ordnern 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.
- **Client wird vor dem Herunterladen synchronisierter Dateien zur Bestätigung aufgefordert** – Wählen Sie die Bedingungen aus, unter denen der Benutzer bestätigen muss, bevor Dateien in synchronisierten Ordnern heruntergeladen werden. Die Optionen sind: **Immer**, **Nur bei Mobilfunk** und **Nie**. Wenn die Option **Benutzer erlauben, diese Einstellung zu ändern** aktiviert ist, können Clients diese Bestätigungsoptionen ändern.
- **Dateisynchronisierung nur erlauben, wenn Gerät per WLAN verbunden ist** – Wenn diese Option aktiviert ist, wird Acronis Cyber Files keine Dateien über Mobilfunk-Verbindungen synchronisieren. Wenn die Option **Benutzer erlauben, diese Einstellung zu ändern** aktiviert ist, können Clients die automatische Dateisynchronisierung bei WLAN-Verbindungen aktivieren oder deaktivieren.

- **Auto-Sync-Intervall** – Wenn diese Option aktiviert ist, wird Acronis Cyber Files die automatischen Synchronisierungen **Nie**, **Nur beim App-Start** oder bestimmten **Zeitintervallen** ausführen.
  - **Benutzer erlauben, diese Einstellung zu ändern** – Wenn diese Option aktiviert ist, kann der Benutzer das Zeitintervall in der Acronis Cyber Files Mobile App selbst einstellen.
  - **Datei-Auto-Sync nur erlauben, wenn Gerät per WLAN-Netzwerk verbunden ist** – Wenn diese Option aktiviert ist, wird die automatische Synchronisierung erst bei einer bestehenden WLAN-Verbindung ausgeführt.
- **Gerät daran hindern, während Datei-Sync in Standby zu gehen** – Wenn diese Option aktiviert ist, werden Geräte, die diese Einstellung unterstützen, nicht gesperrt oder in den Ruhezustand versetzt, wenn Datei-Synchronisierungen ausgeführt werden. Wenn **Benutzer erlauben, diese Einstellung zu ändern** aktiviert ist, können die Clients die Bestätigungsoptionen ändern.

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.

Sie können den Platzhalter %USERNAME% als Teil des Pfades verwenden. Der Platzhalter wird durch den Namen des Hauptordners des Benutzers ersetzt. %USERNAME% muss großgeschrieben werden.

Hinweis
Der Platzhalter %USERNAME% kann nicht für die Anzeige des Benutzernamens auf einem anderen Datenquellentyp verwendet werden. 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 Basisverzeichnispfad** – Der in der Mobile App angezeigte Basisordner verbindet den Benutzer mit dem Serverpfad, der in dieser Einstellung festgelegt wird.

  Sie können den Platzhalter %USERNAME% als Teil des Pfades verwenden. Der Platzhalter wird durch den Namen des Hauptordners des Benutzers ersetzt. %USERNAME% muss großgeschrieben 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.

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 erstmals im Management registriert wird. Dieses Kennwort wird dann gespeichert und für alle später initiierten Verbindungen zum Datei-Server verwendet.
  - **Einmal pro Sitzung** – Nach dem Starten der Acronis Cyber Files Mobile App muss der Benutzer sein Kennwort eingeben, wenn er sich mit dem ersten Server verbindet. Solange die

Acronis Cyber Files Mobile App nicht beendet wird, kann der Benutzer eine Verbindung mit weiteren Servern herstellen, ohne sein Kennwort erneut eingeben zu müssen. Wenn der Benutzer die Acronis Cyber Files Mobile App für eine gewisse Zeit beendet und dann wieder startet, muss er sein Kennwort erneut eingeben, um sich mit dem ersten Server verbinden zu können.
    - **Für jede Verbindung** – Der Benutzer muss das Kennwort jedes Mal eingeben, wenn er eine Verbindung zu einem Server herstellt.
- **Benutzer erlauben, einzelne Server hinzuzufügen** – Wenn diese Option aktiviert ist, können Benutzer Server manuell über die Acronis Cyber Files Mobile App hinzufügen, solange sie den DNS-Namen oder die IP-Adresse des Servers kennen. Wenn Sie wollen, dass dem Benutzer nur die Richtlinie **Zugewiesene Server** zur Verfügung steht, 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.
- **Webclient erlauben, auf Datei-Server, NAS und SharePoint zuzugreifen** – Wenn aktiviert, können Benutzer des Webclients auch mobile Datenquellen sehen und darauf zugreifen.
    - **Erlauben, dass Dateiserver-, 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 diese Option aktiviert ist, können Desktop Clients die Inhalte von **Netzwerk**-Ordnern in beide Richtungen synchronisieren.

        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), **Kopieren**, **Löschen**, **Verschieben** und **Umbenennen**.

- **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 Blocklisten von Netzwerkpfaden erstellen und verwenden, die von den Benutzern nicht selbst bereitgestellt werden dürfen.
- **Diesem Mobile Client nur die Verbindung mit Servern erlauben, die von Drittanbietern signierte SSL-Zertifikate haben** – Wenn diese Option aktiviert ist, kann der Access Mobile Client Acronis Cyber Files Mobile nur Verbindungen mit Servern herstellen, die über von Drittanbietern signierte SSL-Zertifikate verfügen.

Hinweis
Falls der Verwaltungsserver nicht über ein Drittanbieter-Zertifikat verfügt, kann der Client nach der Erstkonfiguration keine Verbindung zum Verwaltungsserver 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 ein Zeitüberschreitungswert für Client-Verbindungen bei nicht reagierenden Servern festgelegt werden. Wenn sich Ihre Clients in besonders langsamen Datenverbindungen befinden oder wenn sie auf eine VPN-on-Demand-Lösung angewiesen sind, um zuerst eine Verbindung herzustellen, bevor ein Gateway Server erreichbar ist, kann dieses Timeout auf einen Wert größer als den Standardwert von 30 Sekunden festgelegt werden. Wenn Sie wollen, dass der Client diese Einstellung über die Acronis Cyber Files Mobile App ändern kann, aktivieren Sie das Kontrollkästchen **Benutzer erlauben, diese Einstellung zu ändern**.

Ausnahmen für Richtlinieneinstellungen

Für Benutzer der Apps **Acronis Cyber Files Mobile für Android** und **Acronis Cyber Files Mobile mit Mobile Iron AppConnect** gibt es einige Ausnahmen hinsichtlich der Art, auf die Acronis Cyber Files-Management-Richtlinien auf die jeweilige Mobile-App angewendet werden. Im Fall von Android werden einige Funktionen noch nicht unterstützt, sodass die entsprechenden Richtlinien nicht angewendet werden. Bei MobileIron werden einige der standardmäßigen Acronis Cyber Files-Richtlinienfunktionen auf die MobileIron AppConnect-Plattform übertragen. Diese Ausnahmen werden auf den Seiten zur Acronis Cyber Files-Richtlinienkonfiguration vermerkt. Weitere Details zu den einzelnen Richtlinienausnahmen werden angezeigt, wenn Sie den Mauszeiger über das Logo von Android oder MobileIron führen.

Erstellen einer Liste mit blockierten Pfaden

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

   Hinweis
   Sie müssen diesen Schritt für jede Benutzer-/Gruppenrichtlinie durchführen, die Sie zur Blockliste 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 Sie zur Blockliste hinzufügen möchten. 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 Blockliste für eine Benutzer- oder Gruppenrichtlinie:

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

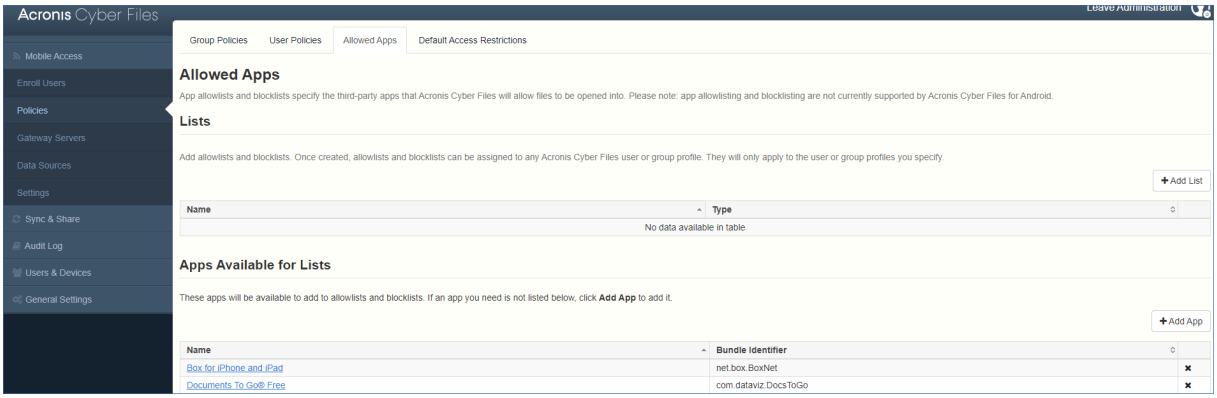
   Hinweis
   Sie müssen diesen Schritt für jede Benutzer-/Gruppenrichtlinie durchführen, die Sie zur Blockliste hinzufügen möchten.

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

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

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

Erlaubte Apps



Acronis In Cyber Files Client Management können Sie Positivlisten und Blocklisten erstellen, mit denen die Fähigkeit der mobilenAcronis Cyber Files-App eingeschränkt wird, Dateien in anderen Apps auf einem mobilen Gerät zu öffnen. Mit diesen Listen können Sie sicherstellen, dass Dateien, auf die über die mobile Acronis Cyber Files-App zugegriffen werden kann, nur in sicheren, vertrauenswürdigen Apps geöffnet werden können.

Positivlisten – ermöglichen Ihnen, eine Liste von Apps zu spezifizieren, in die Acronis Cyber Files-Dateien geöffnet werden dürfen. Allen anderen Apps wird der Zugriff verweigert.

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

Damit Acronis Cyber Files eine bestimmte App identifizieren kann, muss es den **Bundle Identifier** der App kennen. Eine Liste häufig verwendeter Apps und ihrer Bundle Identifier ist standardmäßig auf der Acronis Cyber Files-Weboberfläche enthalten. Wenn eine App, die Sie erlauben oder blockieren möchten, noch nicht in der entsprechenden Liste enthalten ist, müssen Sie sie hinzufügen.

Hinweis
Positivlisten und Blocklisten für Apps werden derzeit von der mobilen Acronis Cyber Files-App für Android nicht unterstützt.

Listen

Positivlisten und Blocklisten hinzufügen. Nach der Erstellung können Positiv- und Blocklisten zu beliebigen Benutzer- oder Gruppenrichtlinien in Acronis Cyber Files zugewiesen werden. Sie gelten nur für die von Ihnen spezifizierten Benutzer- oder Gruppenprofile.

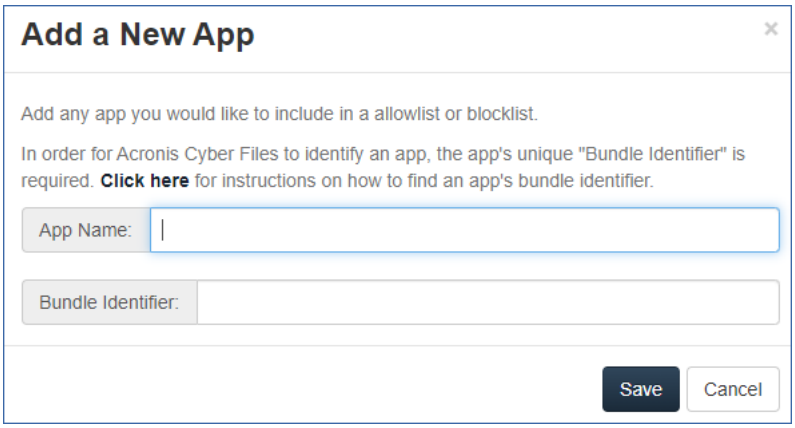
- **Name** – Zeigt den vom Administrator festgelegten Namen der Liste an.
- **Typ** – Zeigt den Typ der Liste an (Positivliste/Blockliste).
- **Liste hinzufügen** – Öffnet das Menü, in dem Sie eine neue Positiv- oder Blockliste hinzufügen können.

Hinzufügen von für Listen verfügbaren Apps

So fügen Sie eine App zu einer Positiv- oder Blockliste hinzu:

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, um sie in die Positiv- oder Blockliste aufnehmen zu können.
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.



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 Acronis Cyber Files eingeben müssen. Diese Zeichenfolgen sind gewöhnlich wie folgt formatiert: **com.firmenname.appname**

Den Bundle Identifier einer App in einer iTunes Library ermitteln

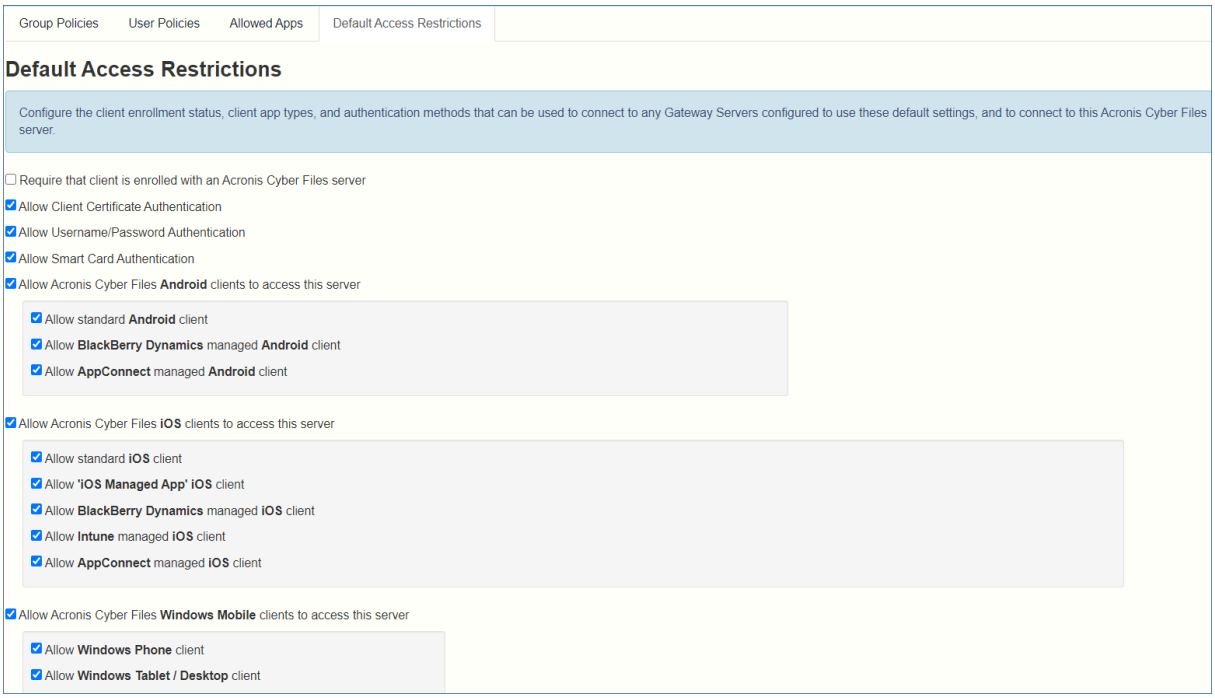
Wenn Sie Ihr Gerät mit iTunes synchronisieren und sich die gewünschte App entweder auf Ihrem Gerät befindet oder über iTunes heruntergeladen wurde, existiert sie auf der Festplatte Ihres Computers. Sie können auf Ihrer Festplatte danach suchen und dann innerhalb der App den **Bundle Identifier** ermitteln.

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 Acronis Cyber Files eingeben müssen. Diese Zeichenfolgen sind gewöhnlich wie folgt formatiert: **com.firmenname.appname**

Standardzugriffsbeschränkungen

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

Hinweis
Informationen zum Einstellen von benutzerdefinierten Beschränkungen für die Gateway-Server finden Sie im Artikel Gateway-Server bearbeiten im Abschnitt 'Gateway-Server verwalten'.



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

- **Verlangen, dass der Client für einen Acronis Cyber Files Server registriert ist** – Wenn Sie diese Option auswählen, müssen alle Acronis Cyber Files Mobile Apps, die sich mit diesem Server verbinden, von einem Acronis Cyber Files Server verwaltet werden, der einer Liste mit zulässigen Acronis Cyber Files Server aufgeführt ist. Diese Option stellt sicher, dass alle auf den Server zugreifenden Clients die von Ihnen geforderten Einstellungen und Sicherheitsoptionen haben. Der eingegebene Servername muss mit dem Namen des Management Servers übereinstimmen, der in der Mobile App konfiguriert ist. Es können auch Teilnamen verwendet werden, um beispielsweise mehrere Server zur Client-Verwaltung in einer Domain zuzulassen. Für Teilnamen werden keine Platzhalterzeichen benötigt.
- **Clientzertifikat-Authentifizierung 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 mehr per Smartcard verbunden werden. Sie können aber per Benutzername und Kennwort des Clients oder per Zertifikat verbunden werden.
- **Acronis Cyber Files-Android-Clients den Zugriff auf diesen Server erlauben** – Wenn Sie diese Option deaktivieren, können Android-Geräte keine Verbindung mit dem Acronis Cyber Files-Server herstellen, und Sie können zudem nicht auf die Verwaltungsfunktion 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, wird dieser Acronis Cyber Files Server entsprechenden Benutzern, die die Standard-Android-Client-App von Acronis Cyber Files verwenden, erlauben, eine Verbindung herzustellen. Wenn Sie Android-Benutzern den Zugriff auf diesen Acronis Cyber Files Server verbieten wollen, können Sie diese Einstellung deaktivieren.
- **Per AppConnect verwaltete Android-Clients erlauben** – Wenn Sie diese Option auswählen, wird dieser Acronis Cyber Files Server Android-Benutzer zulassen, die in MobileIron registrierte Acronis Cyber Files Clients verwenden. Wenn Sie Android-Benutzern, die über MobileIron registriert sind, den Zugriff auf diesen Acronis Cyber Files Server verbieten wollen, können Sie diese Einstellung deaktivieren.

- **Acronis Cyber Files-iOS-Clients den Zugriff auf diesen Server erlauben –** Wenn Sie diese Option deaktivieren, können iOS-Geräte keine Verbindung mit dem AcronisCyber Files-Server herstellen, und Sie können zudem nicht auf die Verwaltungsfunktion 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 dieser Acronis Cyber Files-Server Verbindungen mit Benutzern zu, die die standardmäßige mobile Acronis Cyber Files-iOS-App ausführen. Wenn iOS-Benutzer nicht auf diesen Acronis Cyber Files-Server zugreifen sollen, können Sie diese Einstellung deaktivieren.
  - **iOS-Clients mit 'Verwalteter iOS-App' erlauben** – Wenn Sie diese Option auswählen, lässt der Acronis Cyber Files-Server Verbindungen von Benutzern zu, die die von Acronis Cyber Files verwaltete iOS-App verwenden. Um in diesem Status zu sein, muss ein Client eine Konfiguration für die verwaltete App mit mindestens einem Parameter erhalten haben. Wenn iOS-Benutzer nicht auf diesen von Acronis Cyber Files verwalteten Server zugreifen sollen, können Sie diese Einstellung deaktivieren.
  - **Per Intune verwaltete iOS-Clients erlauben** – Wenn Sie diese Option auswählen, lässt der Acronis Cyber Files-Server Verbindungen von Benutzern zu, die den per Intune verwalteten mobilen Acronis Cyber Files-Client verwenden. Wenn per Intune verwaltete Benutzer nicht auf diesen von Acronis Cyber Files verwalteten Server zugreifen sollen, können Sie diese Einstellung deaktivieren.
  - **Per AppConnect verwaltete iOS-Clients erlauben** – Wenn Sie diese Option auswählen, lässt der Acronis Cyber Files-Server iOS-Benutzer mit mobiler Acronis Cyber Files-App (registriert in MobileIron) zu. Wenn iOS-Benutzer, die in MobileIron registriert sind, nicht auf diesen Acronis Cyber Files-Server zugreifen sollen, können Sie diese Einstellung deaktivieren.

Integrieren mobiler Geräte

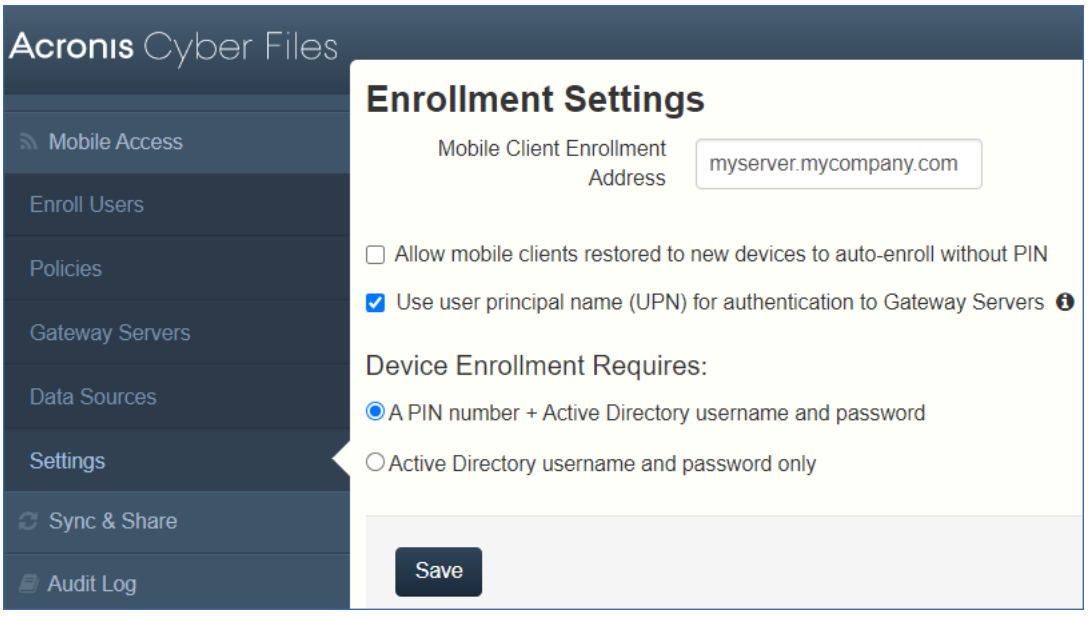
Um die Acronis Cyber Files Mobile App einsetzen zu können, müssen Benutzer die App über ihren jeweiligen App Store (iTunes oder Google Play) installieren. Wenn Ihr Unternehmen eine Client-Verwaltug verwendet, müssen sich die Benutzer außerdem mit dem Acronis Cyber Files Server für die Acronis Cyber Files Mobile App registrieren. Nach der Registrierung werden die Konfigurationen,

Sicherheitseinstellungen und Fähigkeiten des jeweiligen Mobile Clients durch ihre Benutzer- oder Gruppenrichtlinie in Acronis Cyber Files kontrolliert.

Zu den Einstellungen und Funktionen in der mobilen Applikation, die durch die Verwaltungsrichtlinie vorgegeben werden, gehören:

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

Serverseitiger Verwaltungsregistrierungsvorgang



1. Öffnen Sie die Acronis Cyber Files-Weboberfläche.
2. Melden Sie sich als Administrator an.
3. Klicken Sie auf die Registerkarte **Mobile Access**.
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 – Wenn diese Option aktiviert ist, können sich Benutzer, die von älteren Versionen der Acronis Cyber Files Mobile App 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).

Geräteregistrierungsmodus

Acronis Cyber Files 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** – Ein Benutzer muss eine zeitlich begrenzte, einmalig verwendbare PIN-Nummer sowie gültige Active Directory-Anmeldedaten (Benutzername und Kennwort) eingeben, um seine Acronis Cyber Files App aktivieren und auf die Acronis Cyber Files Server zugreifen zu können. Mit dieser Option wird sichergestellt, dass ein Benutzer nur ein (1) Gerät anmelden kann, und das auch nur, nachdem er eine von seinem IT-Administrator ausgestellte PIN-Nummer erhalten hat. Diese Option wird empfohlen, wenn die eine Zwei-Faktor-Geräte-Registrierung zur Gewährleistung einer höheren Sicherheit erforderlich ist.
- **Nur Active Directory-Benutzername und -Kennwort** – Ein entsprechender Benutzer kann seine Acronis Cyber Files-App nur über seine Active Directory-Anmeldedaten (Benutzername, Kennwort) aktivieren. Diese Option ermöglicht es einem Benutzer, zu einem beliebigen Zeitpunkt in der Zukunft ein oder mehrere Geräte zu registrieren. Den Benutzern muss nur der Name ihres jeweiligen Acronis Cyber Files Servers mitgeteilt werden oder eine URL, die auf diesen Acronis Cyber Files Server verweist. Diese Informationen können über eine Website oder per E-Mail bereitgestellt werden, was es wiederum vereinfacht, Acronis Cyber Files für eine größere Benutzeranzahl bereitzustellen. Diese Option wird für Umgebungen empfohlen, für die keine Zwei-Faktor-Registrierung erforderlich ist und viele Benutzer möglicherweise jederzeit auf Acronis Cyber Files zugreifen müssen (wie z.B. bei Bereitstellungen für Schüler bzw. Studierende).

Einladen von Benutzern zum Registrieren

Benutzer werden normalerweise über eine E-Mail, die vom Acronis Cyber Files Administrator gesendet wird, eingeladen, sich beim Acronis Cyber Files 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 die mobileAcronis Cyber Files-App geöffnet und das Client-Registrierungsformular automatisch mit dem Namen des Acronis Cyber Files Server, 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 Clientregistrierung 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 seine mobileAcronis Cyber Files-App 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.

Verwenden einfacher URL-Registrierungs-Links, wenn keine PIN-Nummern benötigt werden

Wenn Ihr Server so konfiguriert ist, dass für die Clientregistrierung 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 Verwaltungsserver öffnen Sie die Registerkarte **Mobile Access** und die Registerkarte **Benutzer registrieren**. Die URL wird auf dieser Seite angezeigt.

Hinweis
Weitere Informationen zu den beiden Modi finden Sie im AbschnittEinstellungen.

So erstellen Sie eine Acronis Cyber Files Registrierungseinladung:

1. Öffnen Sie die Registerkarte **Mobile Access** und die Registerkarte **Benutzer registrieren**.
2. Klicken Sie auf 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. Wenn einem Benutzerkonto keine E-Mail-Adresse zugeordnet ist, wird in der Spalte 'E-Mail-Adresse' die Meldung **Keine E-Mail-Adresse zugewiesen - zum Bearbeiten hier klicken** angezeigt. Sie können auf einen dieser Einträge klicken, um für den Benutzer eine alternative E-Mail-Adresse manuell einzugeben. Wenn einem Benutzer die Meldung **Keine E-Mail-Adresse zugewiesen** hat, wird eine PIN für ihn generiert, die auf der Seite 'Benutzer registrieren' angezeigt wird. Sie müssen dem Benutzer diese PIN auf anderem Wege mitteilen, bevor er seine Acronis Cyber Files Mobile App registrieren kann.

   Hinweis
   Falls Sie die PIN-Nummern für die Registrierung den Benutzern lieber manuell zukommen lassen möchten, deaktivieren Sie die Option **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
   Acronis Im Rahmen der Cyber Files-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 der mobilen Acronis Cyber Files-App, die die Benutzer herunterladen und auf ihrem Gerät installieren sollen. Sie können 'iOS', 'Android' oder 'Beide' wählen.
10. Klicken Sie auf **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.

Benutzerseitiger Verwaltungsregistrierungsvorgang

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

- Link zur Installation der mobilenAcronis Cyber Files-App über den Apple App Store
- Link zum Starten der Mobile-App und zum Automatisieren des Registrierungsvorgangs
- Eine einmalige PIN-Nummer
- Adresse des Verwaltungsservers
- Die E-Mail begleitet die Benutzer bei der Installation der mobilen Acronis Cyber Files-App 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 Acronis Cyber Files automatisch gestartet und das Registrierungsformular 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 Anmeldungen des Acronis Cyber Files-Servers 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

Einrichtungsvorgang für die Verwaltung 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 AcronisCyber Files hier tippen**, wenn Sie Acronis Cyber Files noch nicht installiert haben.
2. Sobald Acronis Cyber Files 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 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 Verwaltungsservers nicht vertrauenswürdig ist. Um diese Warnung zu akzeptieren und fortzufahren, können Sie auf **Immer fortsetzen** klicken.
7. Wenn für die mobile Acronis Cyber Files-App ein Kennwort zum Sperren der Applikation erforderlich ist, werden Sie aufgefordert, eines festzulegen. Möglicherweise gelten auch Anforderungen bezüglich der Komplexität des Kennworts. Diese werden gegebenenfalls angezeigt.

Wenn Ihre Verwaltungsrichtlinie das Speichern von Dateien in Acronis Cyber Files einschränkt oder Sie daran hindert, einzelne Server über die mobile Acronis Cyber Files-App hinzuzufügen, wird möglicherweise ein Bestätigungsfenster angezeigt. Falls Sie Dateien lokal in der mobilen Acronis Cyber Files-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 Acronis Cyber Files-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 Verwaltungsservers nicht vertrauenswürdig ist. Um diese Warnung zu akzeptieren und fortzufahren, können Sie auf **Immer fortsetzen** klicken.
7. Wenn für die mobile Acronis Cyber Files-App ein Kennwort zum Sperren der Applikation erforderlich ist, werden Sie aufgefordert, eines festzulegen. Möglicherweise gelten auch Anforderungen bezüglich der Komplexität des Kennworts. Diese werden gegebenenfalls angezeigt.

Wenn Ihre Verwaltungsrichtlinie das Speichern von Dateien in Acronis Cyber Files einschränkt oder Sie daran hindert, einzelne Server über die mobile Acronis Cyber Files-App hinzuzufügen, wird möglicherweise ein Bestätigungsfenster angezeigt. Falls Sie Dateien lokal in der mobilen Acronis Cyber Files-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 Verwaltungsupdates

Nach der erstmaligen Verwaltungseinrichtung versuchen mobile Acronis Cyber Files-Apps, bei jedem Starten der Client-App Kontakt mit dem Verwaltungsserver aufzunehmen. Jegliche Änderungen der Einstellungen, von Server- oder Ordnerzuordnungen, Zurücksetzungen des Kennworts zur Sperrung der Applikation oder Remote-Löschungen werden zu diesem Zeitpunkt von der Client-App akzeptiert.

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

Entfernen der Verwaltung

Es gibt zwei Optionen, die mobile Acronis Cyber Files-App 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 Acronis Cyber Files Verwaltung haben Sie eventuell das Recht, die mobile Acronis Cyber Files-App 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, die Daten Ihrer mobilen Acronis Cyber Files-App zu löschen, wenn Sie das Gerät aus der Verwaltung entfernen. Sie können den Vorgang hier abbrechen, wenn Sie nicht möchten, dass Ihre Dateien verlorengehen.
4. Bestätigen Sie das Entfernen von Acronis Cyber Files aus der Verwaltung, indem Sie im Bestätigungsfenster auf **JA** tippen.

Hinweis
Wenn Ihre AcronisCyber Files-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 Daten und Einstellungen der mobilen Acronis Cyber Files-App gelöscht, und der Benutzer verfügt nach der erneuten Installation wieder über die Standardeinstellungen für die Applikation.

Gehen Sie folgendermaßen vor, um die Acronis Cyber Files Mobile-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 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 AcronisCyber Files-App, und wählen Sie diese aus.
3. Drücken Sie auf **Entfernen**.

Gateway-Server verwalten

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

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

- **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 Acronis Cyber Files-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.

Administratoren können über das Menü **Aktionen** für jeden Gateway Server Folgendes ausführen:

- Abrufen weiterer Details zu einem Server und seiner Performance
- Bearbeiten der Konfiguration
- Ändern der Zugriffsbeschränkungen für den Server
- Ändern der Lizenzierung für den Server
- Entfernen des Servers

Warnung!
Lesezeichen für Datenquellen gehen nach Entfernung des Gateway Servers, in dem sie sich befinden, irreversibel verloren. Auch das erneute Hinzufügen des Servers und dazugehöriger Datenquellen zur Cyber Files Server-Administration-Konsole kann diese Aktion nicht rückgängig machen.

Hinweis
Der Gateway-Server verwendet den Windows-Dienst `HTTP.sys` und erzwingt die relevanten Windows-Einstellungen auf dem Computer, einschließlich der Einstellungen für Microsoft Secure Channel (schannel), mit denen die TLS-Verschlüsselungssicherheit verwaltet wird.
Kunden, die die Sicherheit des Gateway-Server-Diensts ändern möchten, müssen ein nicht von Acronis bereitgestelltes Tool verwenden, z.B. IIS Crypto, um diese Windows-Einstellungen zu verwalten.

Suchoptionen für den Gateway-Server

Anforderungen

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

Gehen Sie folgendermaßen vor, um die Funktion zu aktivieren:

- Installieren Sie die Rolle mit der Bezeichnung **Dateidienste** im Server-Manager bzw. fügen Sie diese hinzu.
- Stellen Sie sicher, dass der **Windows-Suchdienst** aktiviert und gestartet ist.

Hinweis
Falls die oben genannten Anforderungen nicht erfüllt sind, können Sie keine Suchen in Netzwerk-Datenquellen durchführen.

Die Suche wird auch in den folgenden Fällen *nicht* unterstützt:

- für NAS-Dateiserver, CMIS- und SharePoint-Datenspeicherorte. SMB/CIFS-Dateiserver werden jedoch unterstützt.
- im Stamm von Dateiservern (`//server`). Sie funktioniert vielmehr nur in tatsächlichen Freigaben innerhalb des Stamms (`//server/share`).
- wenn das Dienstkonto auf dem Gateway-Computer keinen Zugriff (Windows-Berechtigungen) auf den Computer hat, auf dem die Remote-Freigabe gehostet wird. Führen Sie den Gateway-Dienst mit einem Administratordienstkonto aus, um dies zu überprüfen.

Das Feld **Suche** ist deaktiviert, wenn:

- eine Suche aus irgendeinem Grund nicht möglich ist.
- das indizierte Verzeichnis leer ist.

Index für lokale Datenquellen für Dateinamensuche

Die Suche in Netzwerk-Datenquellen benötigt den Acronis Cyber Files-Gateway-Server und den Windows-Suchindex. Wenn der Windows-Suchindex für das gewünschte Volume aktiviert und indiziert wurde, kann sowohl eine erweiterte als auch eine Inhaltssuche durchgeführt werden.

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.

1. Öffnen Sie die Acronis Cyber Files-Verwaltungskonsole.
2. Navigieren Sie zu **Mobile Access** > **Gateway-Server** > **Bearbeiten** > **Suche**.
3. Aktivieren Sie:
   - das Kontrollkästchen **Index für lokale Datenquellen für Dateinamensuche**.
   - optional das Kontrollkästchen **Inhaltssuche mit Microsoft Windows-Suche unterstützen (wo verfügbar)**.

Standardpfad

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

Inhaltssuche mit Microsoft Windows-Suche unterstützen (wo verfügbar)

Die Unterstützung für die Inhaltssuche in freigegebenen Ordnern ist standardmäßig aktiviert und kann mit 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.

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 Webapplikation haben.

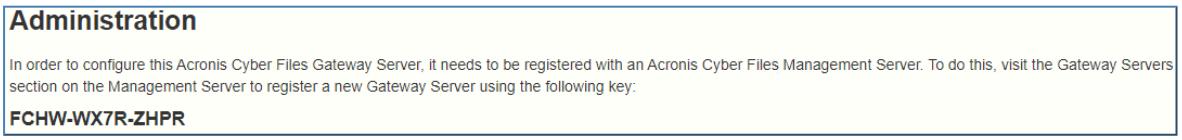
Registrieren neuer Gateway Server

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

1. Greifen Sie auf den Computer zu, auf dem der Gateway Server installiert ist.
2. Gehen Sie je nach Einstellungen des **Konfigurationsdienstprogramms** folgendermaßen vor:
   a. Wenn Sie **Alle verfügbaren Adressen** ausgewählt haben, öffnen Sie **https://localhost:3000/gateway_admin**.
   b. Wenn Sie eine bestimmte IP-Adresse ausgewählt haben, öffnen Sie **https://<bestimmte_IP-Adresse>:3000/gateway_admin**.

   Hinweis
   Port 3000 ist der Standard-Port. Falls Sie den Standard-Port geändert haben, geben Sie nach 'localhost' oder der IP-Adresse Ihre Portnummer ein.

3. Notieren Sie den **Administrationsschlüssel**.



4. Öffnen Sie die Acronis Cyber Files-Weboberfläche.
5. Klicken Sie auf die Registerkarte **Mobile Access**.
6. Öffnen Sie die Seite **Gateway Server**.

7. Klicken Sie auf die Schaltfläche **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 Clientverbindungen verwenden**, und geben Sie den DNS-Namen oder die IP-Adresse des Reverse-Proxy-Servers bzw. Loadbalancers ein.

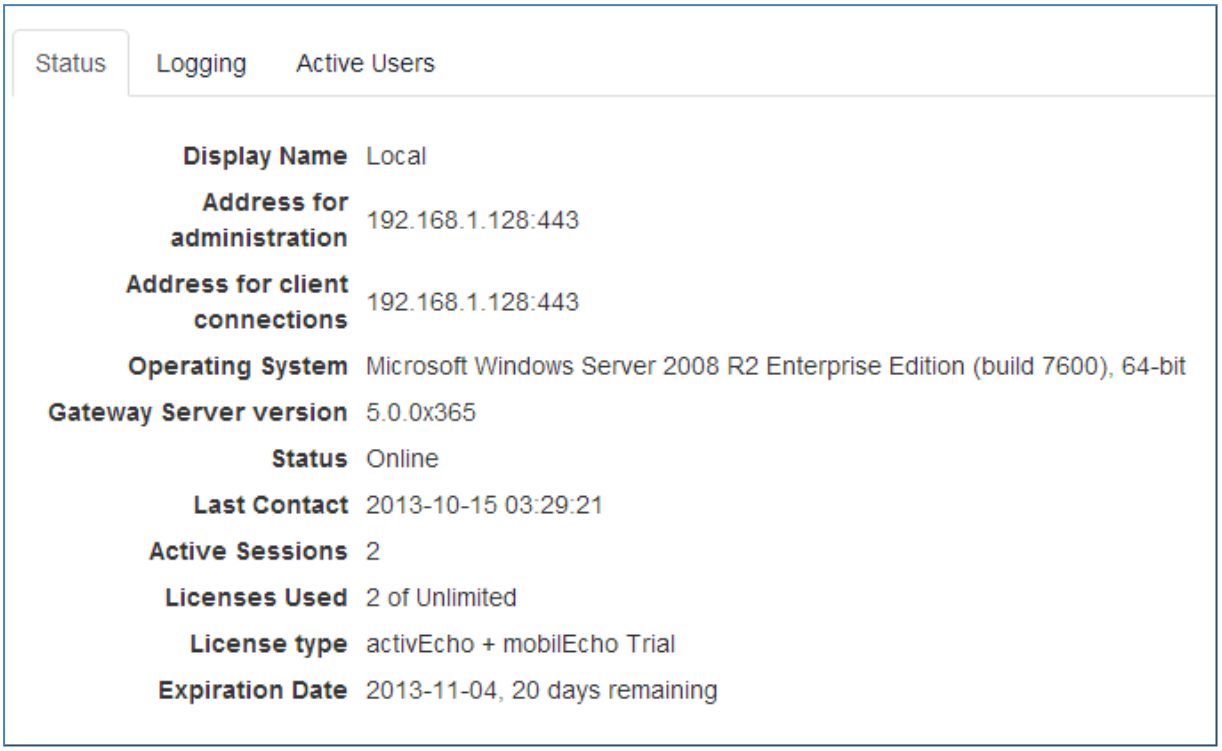
10. Geben Sie den **Administrationsschlüssel** ein.
11. Erlauben Sie bei Bedarf Verbindungen mit selbstsignierten Zertifikaten zu diesem Gateway. Aktivieren Sie dazu die Option **Verbindungen von Acronis Cyber Files-Servern mit selbstsignierten Zertifikaten erlauben**.
12. Klicken Sie auf **Speichern**.

Nachdem Sie Ihren Gateway Server registriert haben, können Sie individuelle Zugriffsbeschränkungen für diesen Gateway Server konfigurieren. Weitere Informationen hierzu finden Sie im Abschnitt Bearbeiten von Gateway Servern.

Server-Details

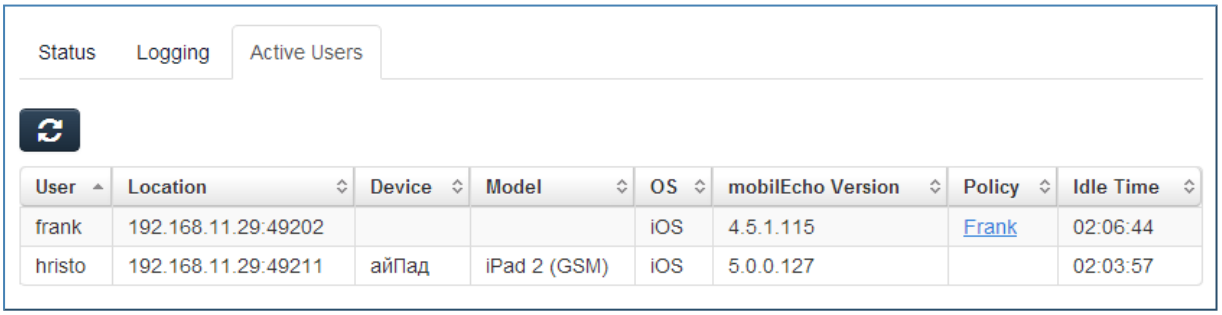
Auf der Seite **Details** eines Gateway Servers erhalten Sie zahlreiche nützliche Informationen zu dem spezifischen Server und seinen Benutzern.

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.
- **Clientversion** – Zeigt die Version der auf dem Gerät installierten AcronisCyber Files-App an.

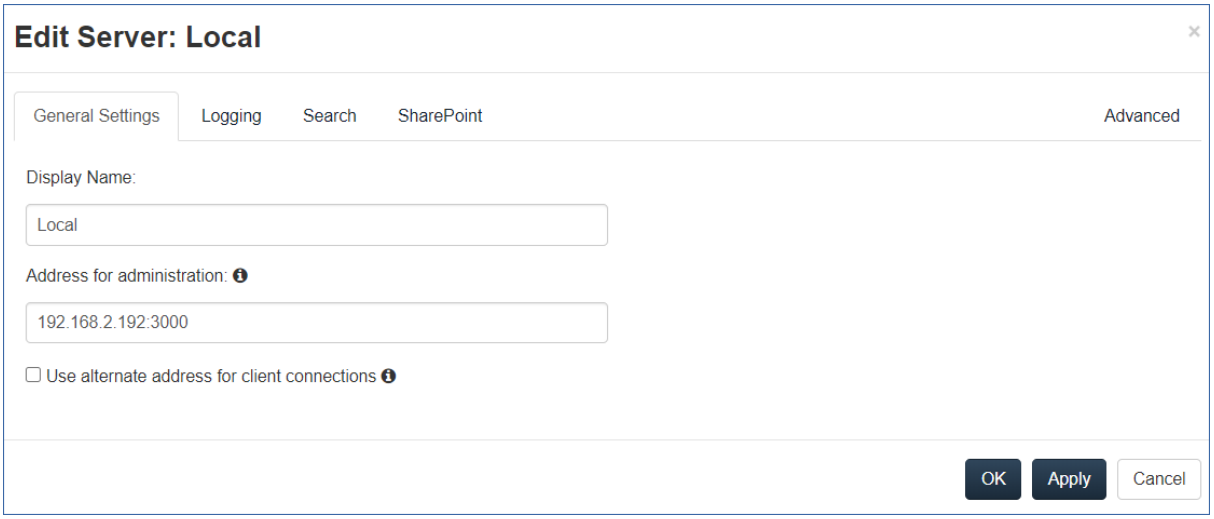
- **Richtlinie** – Zeigt die Richtlinie für das vom Gerät verwendete Konto an.
- **Leerlaufzeit** – Zeigt an, wie lange der Benutzer mit dem Gateway verbunden ist.

Konfigurationen des Gateway-Servers

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

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

Allgemeine Einstellungen



- **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 Acronis Cyber Files-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.

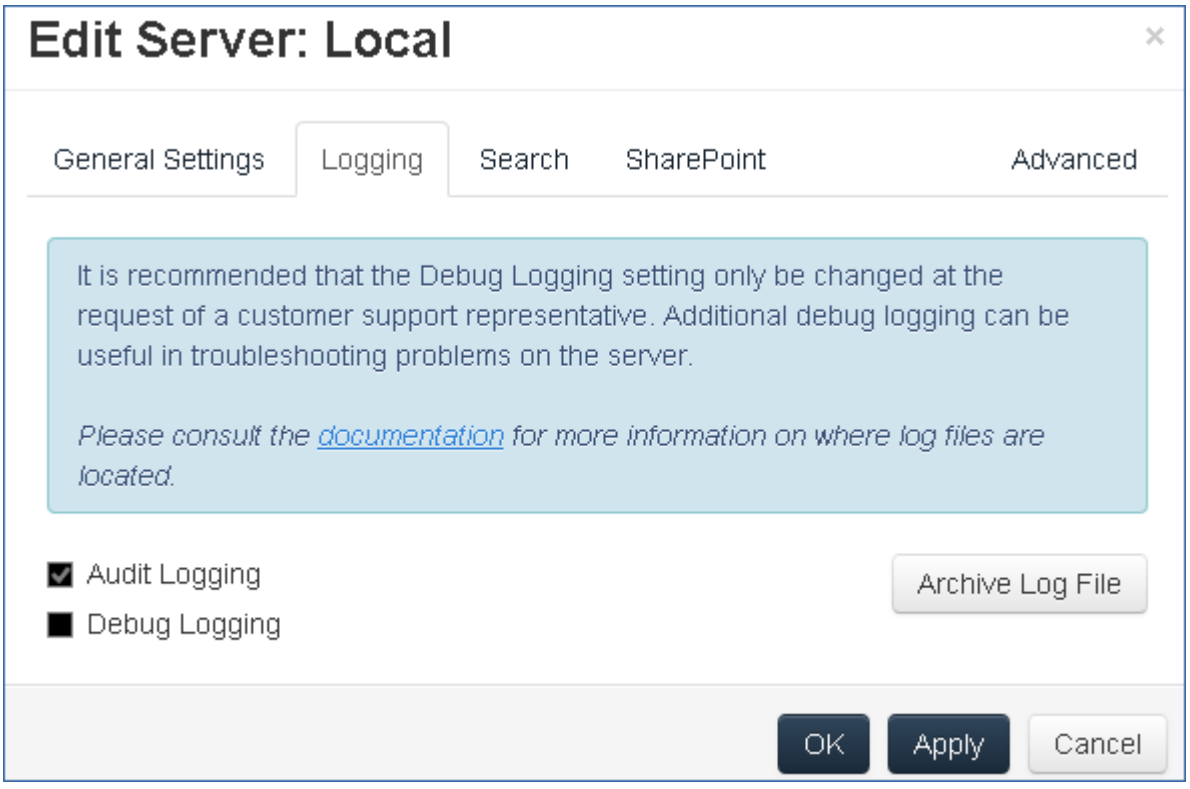
- **Alternative Adresse für Client-Verbindungen verwenden** – Wenn diese Option aktiviert ist, wird die Adresse überschrieben, über die Mobile Clients eine Verbindung zum Gateway Server herstellen.

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. 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 zum Verbinden mit dem Gateway Server verwenden. Wir empfehlen, eine DNS-Adresse statt einer IP-Adresse zu verwenden.

Gateway-Server-Protokollierung

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. Klicken Sie auf die Registerkarte **Mobile Access**.
4. Rufen Sie die Registerkarte **Gateway Server** auf.
5. Suchen Sie den Server, für den Sie **Audit Logs aktivieren möchten.**

6. Klicken Sie auf die Schaltfläche **Details**.
7. Aktivieren Sie im Bereich **Protokollierung** die Option **Überwachungsprotokollierung**.
8. Klicken Sie auf **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 **Mobile Access**.
4. Rufen Sie die Registerkarte **Gateway Server** auf.
5. Suchen Sie den Server, für den Sie die **Debug-Protokollierung aktivieren möchten.**
6. Klicken Sie auf die Schaltfläche **Details**.
7. Aktivieren Sie im Bereich **Protokollierung** die Option **Debug-Protokollierung**.
8. Klicken Sie auf **Speichern**.

Suchoptionen für den Gateway-Server

Anforderungen

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

Gehen Sie folgendermaßen vor, um die Funktion zu aktivieren:

- Installieren Sie die Rolle mit der Bezeichnung **Dateidienste** im Server-Manager bzw. fügen Sie diese hinzu.
- Stellen Sie sicher, dass der **Windows-Suchdienst** aktiviert und gestartet ist.

Hinweis
Falls die oben genannten Anforderungen nicht erfüllt sind, können Sie keine Suchen in Netzwerk-Datenquellen durchführen.

Die Suche wird auch in den folgenden Fällen *nicht* unterstützt:

- für NAS-Dateiserver, CMIS- und SharePoint-Datenspeicherorte. SMB/CIFS-Dateiserver werden jedoch unterstützt.
- im Stamm von Dateiservern (`//server`). Sie funktioniert vielmehr nur in tatsächlichen Freigaben innerhalb des Stamms (`//server/share`).

- wenn das Dienstkonto auf dem Gateway-Computer keinen Zugriff (Windows-Berechtigungen) auf den Computer hat, auf dem die Remote-Freigabe gehostet wird. Führen Sie den Gateway-Dienst mit einem Administratordienstkonto aus, um dies zu überprüfen.

Das Feld **Suche** ist deaktiviert, wenn:

- eine Suche aus irgendeinem Grund nicht möglich ist.
- das indizierte Verzeichnis leer ist.

Index für lokale Datenquellen für Dateinamensuche

Die Suche in Netzwerk-Datenquellen benötigt den Acronis Cyber Files-Gateway-Server und den Windows-Suchindex. Wenn der Windows-Suchindex für das gewünschte Volume aktiviert und indiziert wurde, kann sowohl eine erweiterte als auch eine Inhaltssuche durchgeführt werden.

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.

1. Öffnen Sie die Acronis Cyber Files-Verwaltungskonsole.
2. Navigieren Sie zu **Mobile Access** > **Gateway-Server** > **Bearbeiten** > **Suche**.
3. Aktivieren Sie:
   - das Kontrollkästchen **Index für lokale Datenquellen für Dateinamensuche**.
   - optional das Kontrollkästchen **Inhaltssuche mit Microsoft Windows-Suche unterstützen (wo verfügbar)**.

Standardpfad

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

Inhaltssuche mit Microsoft Windows-Suche unterstützen (wo verfügbar)

Die Unterstützung für die Inhaltssuche in freigegebenen Ordnern ist standardmäßig aktiviert und kann mit 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.

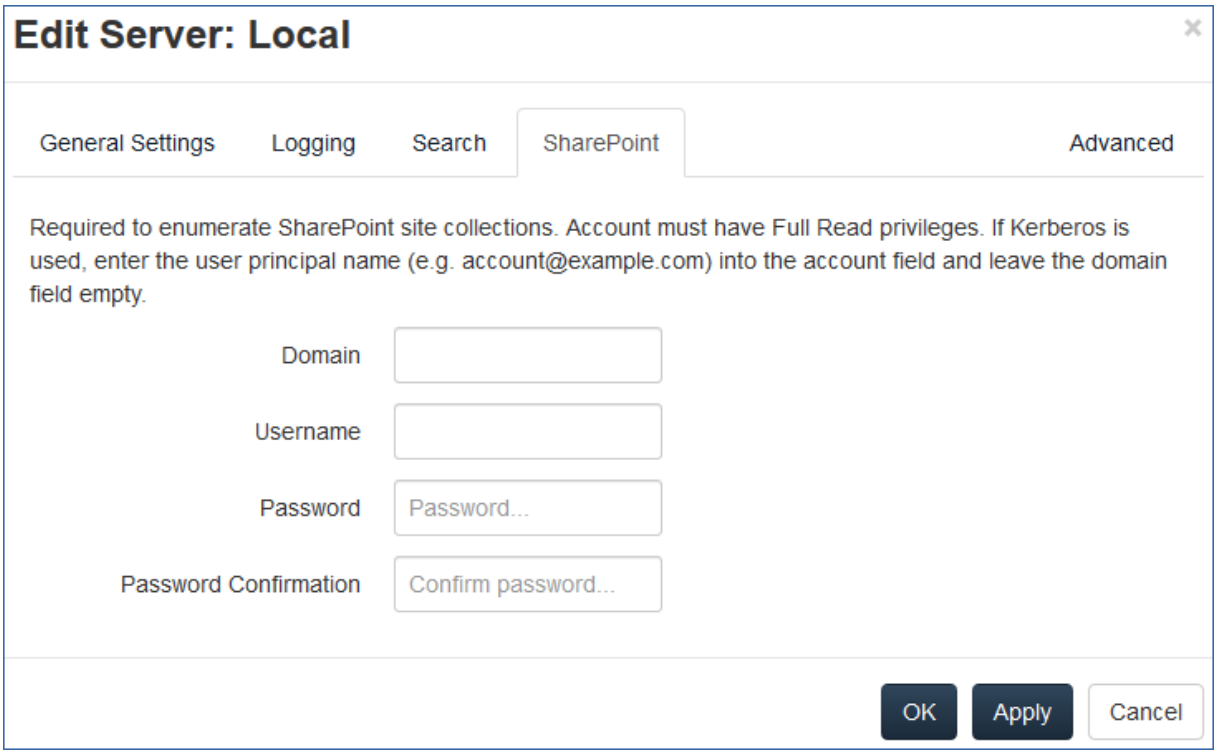
Hinweis
Der Volume-Pfad der Datenquelle muss ein Host-Name oder vollständig qualifizierter Name sein, damit die Inhaltssuche für Windows-Freigabeweiterleitungen verwendet werden kann. IP-Adressen werden von der Windows-Suche nicht unterstützt.

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.

SharePoint-Einstellungen



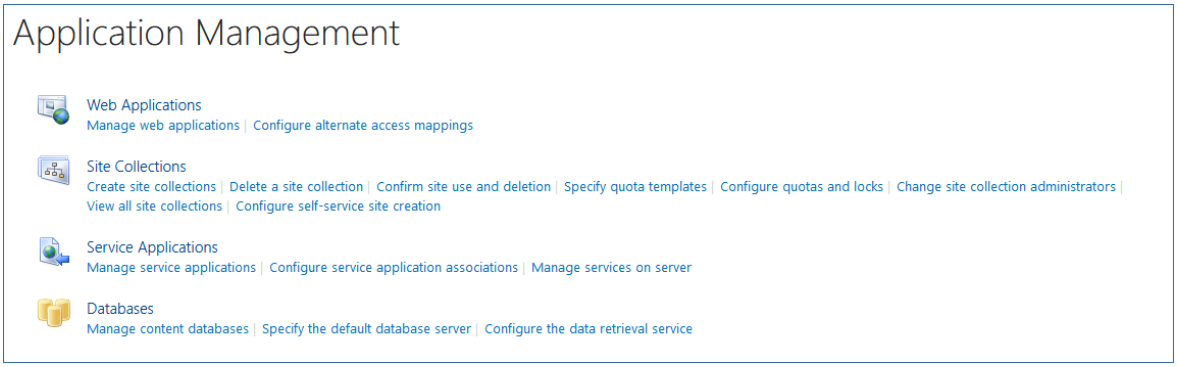
Für die allgemeine Unterstützung von SharePoint ist die Eingabe dieser Zugangsdaten optional. Sie ist aber erforderlich, um Websitesammlungen aufzulisten. Sie haben beispielsweise zwei Websitesammlungen:

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

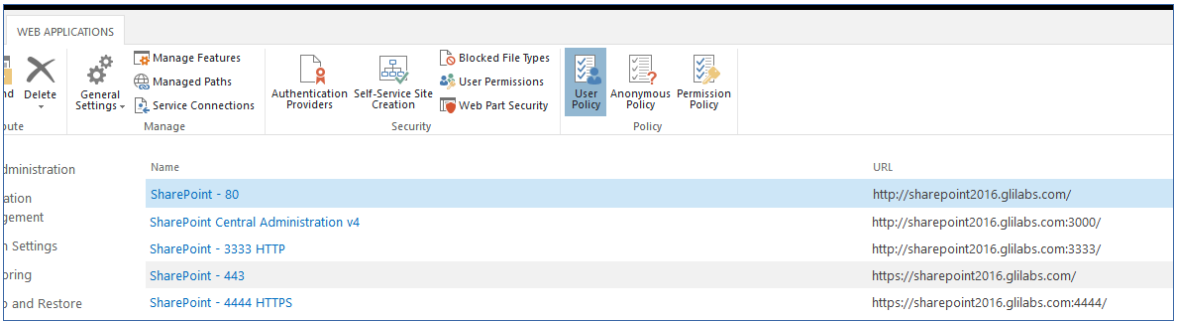
Ohne die Eingabe der Zugangsdaten sehen Sie, wenn Sie ein Volume mit Verweis auf **http://sharepoint.beispiel.com** erstellen, beim Auflisten des Volumes nicht den Ordner mit dem Namen **SeparateSammlung**. Das Konto muss **vollen Lesezugriff** auf die Webapplikation haben.

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 **Applikationsverwaltung**.

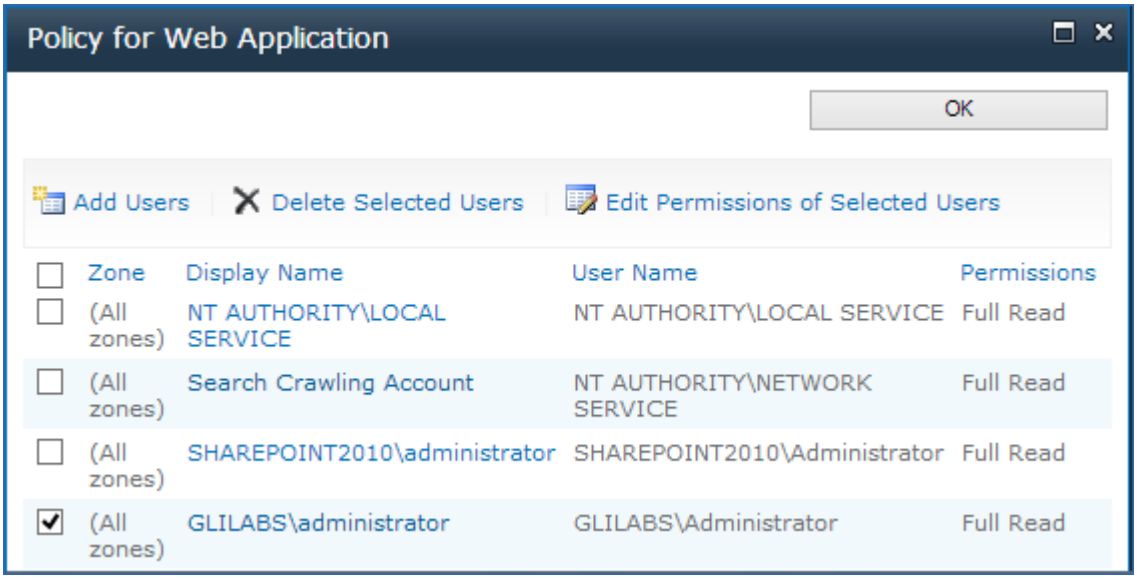


3. Klicken Sie unter **Webapplikationen** auf **Webapplikationen verwalten**.
4. Wählen Sie Ihre Webapplikation aus der Liste aus, und klicken Sie auf **Benutzerrichtlinie**.

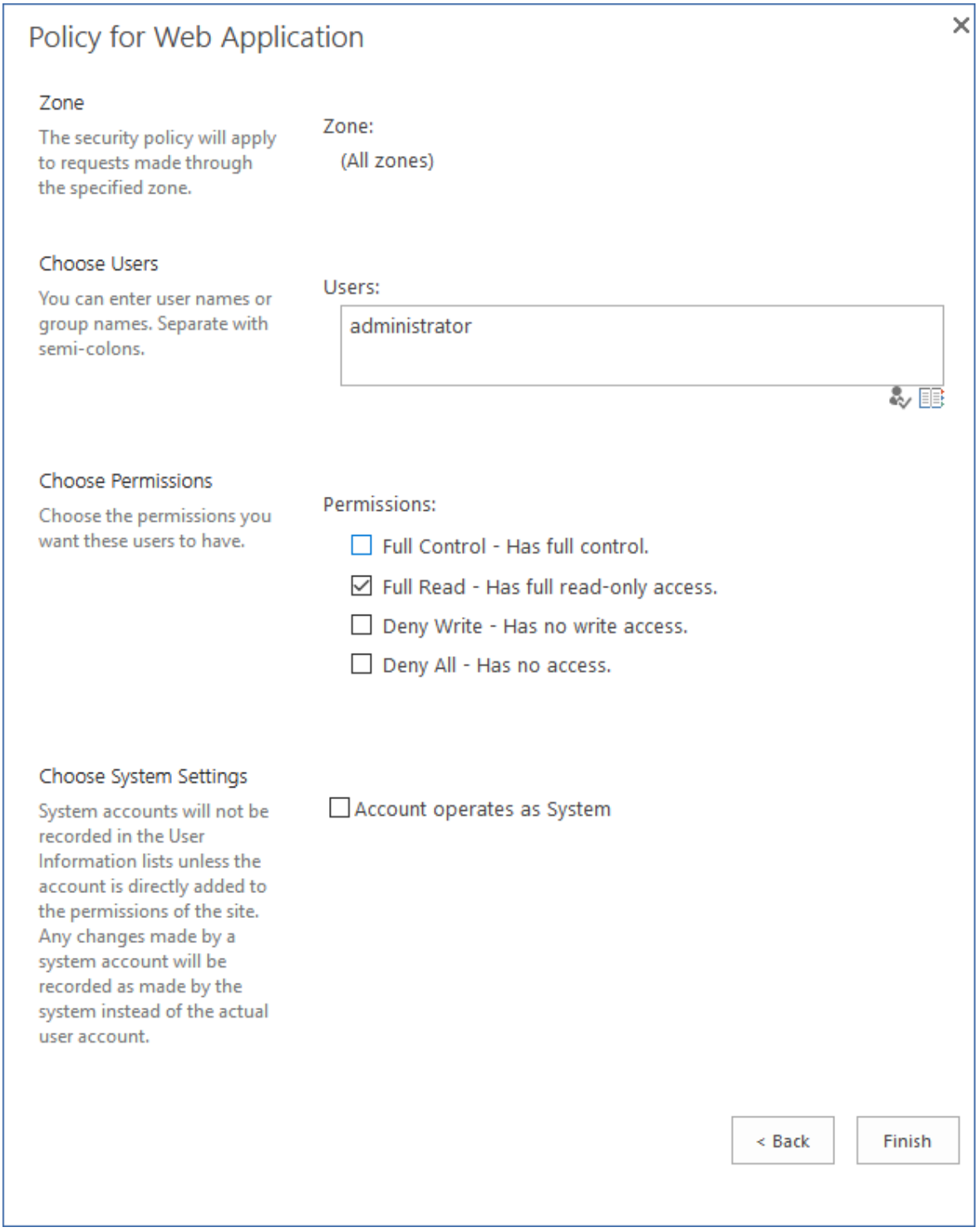


5. Aktivieren Sie das Kontrollkästchen für den Benutzer, dem Sie Berechtigungen gewähren möchten, und klicken Sie dann auf **Berechtigungen der ausgewählten Benutzer bearbeiten**. Taucht der Benutzer in der Liste nicht auf, können Sie ihn durch Anklicken von **Benutzer**

hinzufügen hinzufügen.

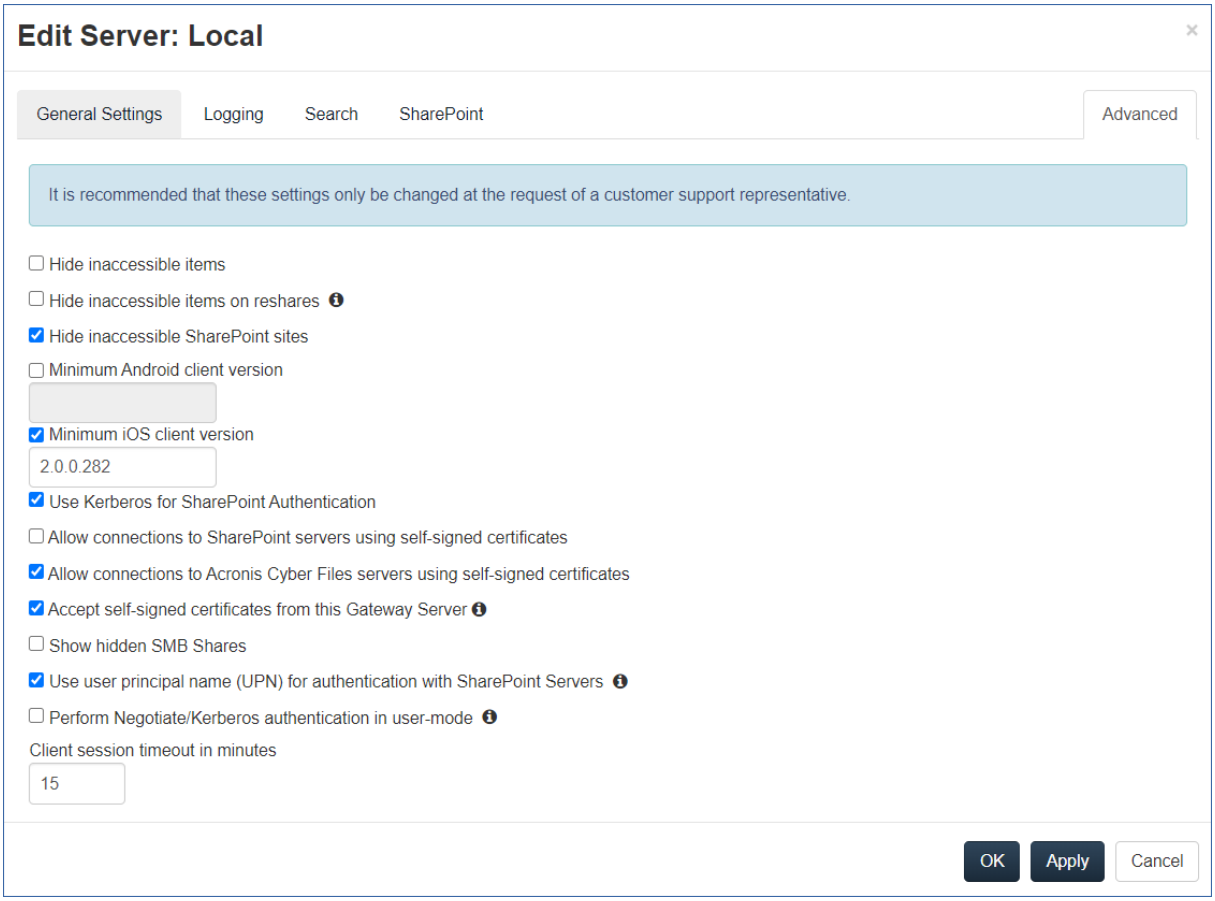


6. Aktivieren Sie unter **Richtlinienstufen für Berechtigungen** das Kontrollkästchen **Alles lesen – Verfügt über vollständigen schreibgeschützten Zugriff**.



7. Klicken Sie auf **Speichern**.

Erweiterte Einstellungen



Hinweis
Es wird empfohlen, diese Einstellungen nur bei Aufforderung durch einen Mitarbeiter des Kunden-Supports zu ändern.

- **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 die notwendigen Berechtigungen besitzt, werden nicht angezeigt.
- **Minimale Android-Client-Version** – Wenn aktiviert,Benutzer, die eine Verbindung mit diesem Gateway herstellen, benötigen diese oder eine höhere Version der Acronis Cyber Files Client-App für Android.

- **Minimale iOS-Client-Version** – Wenn aktiviert,Benutzer, die eine Verbindung mit diesem Gateway herstellen, benötigen diese oder eine spätere Version der Acronis Cyber Files Client-App für iOS.
- **Kerberos für SharePoint-Authentifizierung verwenden** – Wenn Ihr SharePoint-Server eine Kerberos-Authentifizierung erfordert, sollten Sie diese Einstellung aktivieren. Sie müssen außerdem ein Update für das Active Directory-Computerobjekt des Windows-Servers oder der Windows-Server durchführen, auf denen die Gateway Server-Software ausgeführt wird. Dem Acronis Cyber Files Windows-Server muss die Berechtigung erteilt werden, dass er im Namen Ihrer Benutzer delegierte Anmeldedaten an Ihren SharePoint-Server übergeben kann. Kerberos-Delegierung auf Acronis Cyber Files-Windows-Server aktivieren:
  1. Suchen Sie in **Active Directory-Benutzer und -Computer** den oder die Windows-Server, auf dem oder denen der Gateway Server installiert ist. Sie befinden sich meist im Ordner **Computer**.
  2. Öffnen Sie das Fenster **Eigenschaften** für den Windows-Server und wählen Sie die Registerkarte **Delegierung**.
  3. Wählen Sie **Computer bei Delegierungen angegebener Dienste vertrauen**.
  4. Wählen Sie **Beliebiges Authentifizierungsprotokoll verwenden**, dies ist für die Aushandlung mit dem SharePoint-Server erforderlich.
  5. Sie müssen jetzt SharePoint-Server hinzufügen, auf die die Benutzer mit Acronis Cyber Files 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, erlaubt Verbindungen von diesem Gateway zu SharePoint-Servern mit selbstsignierten Zertifikaten.
- **Selbstsignierte Zertifikate von diesem Gateway Server akzeptieren** – Wenn Sie diese Option aktivieren, werden Verbindungen von diesem Acronis Cyber Files Server zu diesem Gateway Server auch dann erlaubt, wenn der Gateway Server ein selbstsigniertes Zertifikat verwendet.
- **Verbindungen zu Acronis Cyber Files Servern mit selbstsignierten Zertifikaten erlauben** – Wenn diese Option aktiviert ist, werden Verbindungen von diesem Gateway Server zu Acronis Cyber Files Servern auch dann erlaubt, wenn die Acronis Cyber Files Server selbstsignierte Zertifikate verwenden.
- **Versteckte SMB-Freigaben anzeigen** – Wenn aktiviert, zeigt den Benutzern versteckte SMB-System-Freigaben 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** – Wenn diese Option aktiviert ist, können Benutzer ihren Benutzerprinzipalnamen (z. B. hristo@glilabs.com) für die Authentifizierung an SharePoint-Servern verwenden. Andernfalls verwenden sie für die Authentifizierung die Kombination Domain/Benutzername (z.B. glilabs/hristo).
- **Aushandeln/Kerberos-Authentifizierung im Benutzermodus durchführen** – Wenn diese Option aktiviert ist, authentifiziert sich der Gateway Server bei den Datenquellen mithilfe des Kerberos-Tickets des verbindenden Benutzers. Diese Option wird nur für Konfigurationen verwendet, die Kerberos erfordern (z.B. Einzelanmeldung (SSO), Lastenausgleich usw.).

Benutzerdefinierte Zugriffsbeschränkungen

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

Benutzerdefinierte Zugriffsbeschränkungen für einen bestimmten Gateway Server festlegen

1. Navigieren Sie zur Registerkarte **Mobile Access** -> **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**.

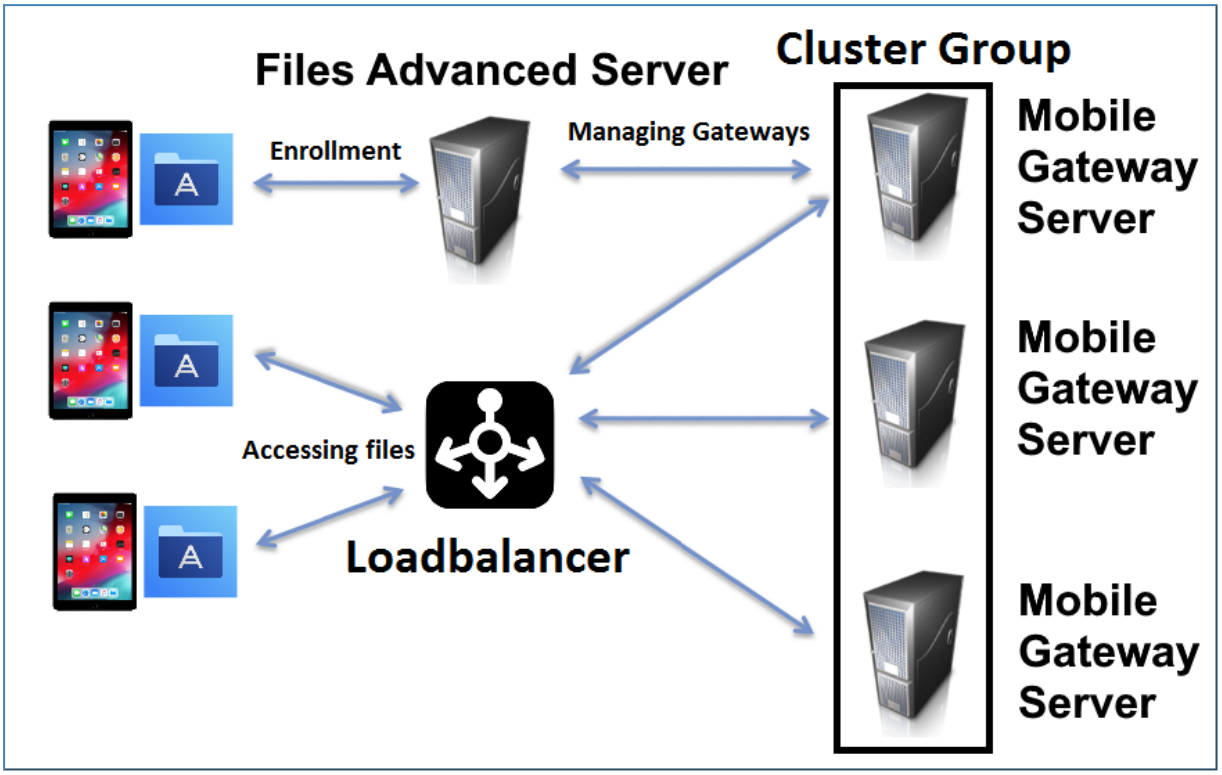
Cluster-Gruppen

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

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

Für eine geclusterte Gateway-Konfiguration benötigen Sie ein Lastenausgleichsmodul, mindestens zwei Gateways und einen Acronis Cyber Files Server. Alle Gateway Server sollten in der Weboberfläche von Acronis Cyber Files einer Cluster-Gruppe hinzugefügt und hinter dem Lastenausgleichsmodul platziert werden. Der Acronis Cyber Files Server fungiert als Verwaltungsserver und als Server, bei dem sich mobile Clients in der Clientverwaltung 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. Hierbei handelt es sich um die DNS- oder IP-Adresse des Gateway-Servers.

1. Öffnen Sie die Acronis Cyber Files-Weboberfläche.
2. Klicken Sie auf die Registerkarte **Mobile Access**.
3. Öffnen Sie die Seite **Gateway Server**.
4. Klicken Sie auf 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 Acronis Cyber Files 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. Klicken Sie auf **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.

Mitglieder zu einer bestehenden Cluster-Gruppe hinzufügen:

1. Öffnen Sie die Weboberfläche und navigieren Sie zu **Mobile Access**-> **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 **Mobile Access**-> **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**.

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 Acronis Cyber Files-Benutzer freigeben. Wenn sich Benutzer verbinden, werden diese Verzeichnisse als Dateifreigabe-Volumes angezeigt.

Zugriff auf SharePoint 2007, 2010, 2013 und 2016

Acronis Cyber Files bietet Zugriff auf Dateien, die in Dokumentbibliotheken auf SharePoint 2007, 2010, 2013 und 2016 gespeichert sind. Eine SharePoint-Datenquelle von Acronis Cyber Files 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. Acronis Cyber Files unterstützt auch das **Auschecken** und **Einchecken** von SharePoint-Dateien.

Unterstützte SharePoint-Authentifizierungsmethoden

Acronis Cyber Files 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 Acronis Cyber Files-Serversoftware ausgeführt wird. Der Acronis Cyber Files-Windows-

Server muss die Berechtigung erhalten, delegierte Zugangsdaten zu Ihrem SharePoint-Server für Ihre Benutzer anzuzeigen.

Zugriff auf Inhalt von OneDrive for Business

Acronis Cyber Files 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

Acronis Cyber Files verwendet die bestehenden Benutzerkonten und Kennwörter von Windows. Da Acronis Cyber Files 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.

Acronis Der Zugriff auf Cyber Files-Datenquellen, die sich auf einem anderen SMB/CIFS-Dateiserver befinden, erfolgt über eine SMB/CIFS-Verbindung vom Gateway-Server zum sekundären Server oder NAS-Gerät. In diesem Fall wird der Zugriff auf den sekundären Server im Kontext des Benutzers durchgeführt, der an einem der Acronis Cyber Files-Clients 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 Acronis Cyber Files wie beim Zugriff auf SharePoint-Dokumentbibliotheken bei Verwendung eines Webbrowsers.

Ordner

Ordner können zu den Benutzer- und Gruppenrichtlinien von Acronis Cyber Files hinzugefügt werden, sodass sie automatisch in der Acronis Cyber Files-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 Acronis Cyber Files Zugriff gewährt, sofern sich diese nicht auf einem Wechselmedium befinden. Sie verweisen einfach auf Speicherorte auf Gateway-Servern, die bereits innerhalb der Verwaltung von Acronis Cyber Files 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 Acronis Cyber Files aktivieren und ein Gateway-Server vorhanden ist, wird automatisch eine Sync & Share-Datenquelle 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 Acronis Cyber Files-Synchronisierung von Ordnern zur Verfügung:

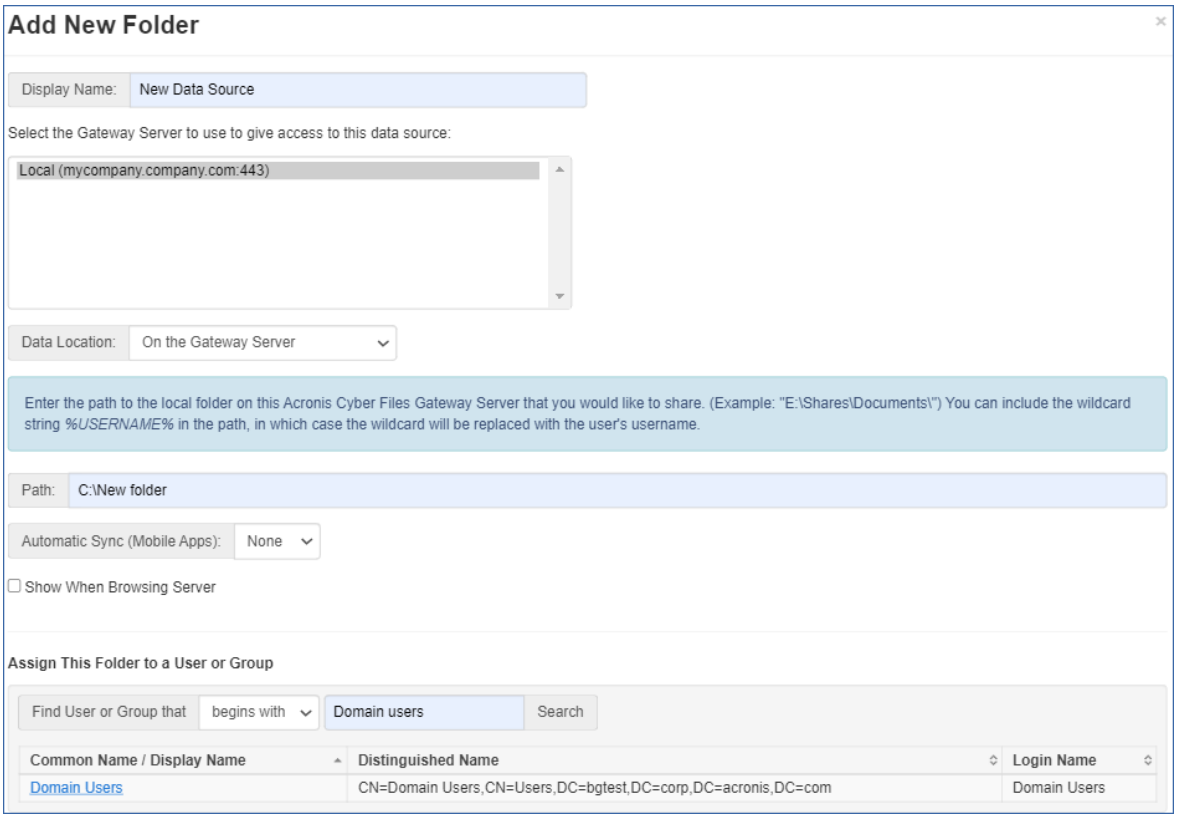
Hinweis
Diese Einstellung hat keinen Einfluss auf den Desktop Client.

- **Keine** – Der Ordner wird als netzwerkbasierte Ressource in der Acronis Cyber Files-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 Acronis Cyber Files App angezeigt. Sein kompletter Inhalt wird vom Server zum Gerät synchronisiert und wird immer auf dem neuesten Stand gehalten, wenn Dateien auf dem Server hinzugefügt, geändert oder gelöscht werden sollten. Dieser Ordner soll einen lokalen und auch offline Zugriff auf bestimmte serverbasierte Dateien ermöglichen und wird dem Benutzer als schreibgeschützt angezeigt.
- **2-Wege** – Der Ordner wird als lokaler Ordner in der Acronis Cyber Files App angezeigt. Sein kompletter Inhalt wird zunächst vom Server zum Gerät synchronisiert. Wenn Dateien in diesem Ordner hinzugefügt, geändert oder gelöscht werden (egal ob auf dem Gerät oder auf dem Server), werden diese Änderungen wieder mit dem Server oder Gerät synchronisiert.

Erstellen und Bearbeiten einer Datenquelle

Erstellen einer Datenquelle

1. Öffnen Sie die Acronis Cyber Files-Weboberfläche.
2. Klicken Sie auf die Registerkarte **Mobile Access**.
3. Öffnen Sie die Registerkarte **Datenquellen**.
4. Wechseln Sie zu **Ordner**.
5. Klicken Sie auf **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
   Sie dürfen einen Ordner auf einem Wechselmedium nicht als freigegebenen Ordner verwenden. Wählen Sie einen Ordner von einem anderen Speicherort aus.

   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 **Sync**-Typ dieses Ordners.
11. Aktivieren Sie **Anzeigen, wenn Server durchsucht wird**, wenn diese Datenquelle beim Durchsuchen des Gateway Server durch mobile Acronis Cyber Files-Clients sichtbar sein soll.

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

12. Klicken Sie auf **Speichern**.

Bearbeiten einer Datenquelle

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**.

SharePoint-Websites und -Bibliotheken

Durch Erstellen einer Datenquelle können Sie den Benutzern der mobilen Acronis Cyber Files-App mühelos Zugriff auf SharePoint-Websites und -Bibliotheken erteilen. Es gibt verschiedene Möglichkeiten zum Erstellen von SharePoint-Datenquellen. Diese hängen von der SharePoint-Konfiguration ab.

Hinweis
Vergewissern Sie sich jedes Mal, wenn Sie eine URL angeben, dass deren Stammverzeichnis die Standard-Website-Sammlung ist.

Eine Datenquelle für eine komplette SharePoint-Website oder Unterwebsite erstellen

Wenn Sie eine Datenquelle für eine **SharePoint-Website** oder **Unterwebsite** erstellen, müssen Sie nur das Feld **URL** ausfüllen. Dies sollte die Adresse Ihrer SharePoint-Website oder Unterwebsite sein.

```
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 Acronis Cyber Files den Ordner 'Gefolgte Websites', der die Ressourcen enthält, auf die sie von diesen Websites zugreifen dürfen.

Hinweis
SharePoint-gefolgte Websites können nicht synchronisiert werden.

Hinweis
Sie können den Platzhalter `%USERNAME%` als Teil des Pfades verwenden. Der Platzhalter wird durch den Namen des Hauptordners des Benutzers ersetzt. `%USERNAME%` muss großgeschrieben werden.

Sie können auch den Platzhalter `%USERNAME%` als Teil von URLs verwenden.

Eine Datenquelle für eine SharePoint-Bibliothek erstellen

Wenn Sie eine Datenquelle für eine SharePoint-Bibliothek erstellen, müssen Sie sowohl das Feld **URL** als auch das Feld **Dokumentenbibliotheksname** ausfüllen. Geben Sie im URL-Feld die Adresse Ihrer SharePoint-Website oder Unterwebsite ein und im Feld Dokumentbibliotheksname den Namen Ihrer Bibliothek.

```
z.B. URL: https://sharepoint.meinefirma.com:43222
z.B. Name der Dokumentbibliothek: Meine Bibliothek
```

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

Wenn Sie eine Datenquelle für einen bestimmten Ordner innerhalb einer SharePoint-Bibliothek erstellen, 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 für das Unterpfad-Feld müssen Sie den Namen des gewünschten Ordners eingeben.

```
Z.B. die URL: https://sharepoint.meinefirma.com:43222
z. B. der Dokumentbibliotheksname: Marketing-Bibliothek
z. B. der Unterpfad: Verkaufsbericht
```

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.

Die Acronis Cyber Files Mobile App unterstützt die NTLM-, die anspruchsbasierte und die SharePoint 365-Authentifizierung sowie die Authentifizierung mit eingeschränkter Kerberos-Delegierung. Je nach Ihrer SharePoint-Einrichtung müssen Sie möglicherweise einige zusätzliche Konfigurationen am Gateway Server vornehmen, der zur Verbindung mit diesen Datenquellen verwendet wird. Weitere Informationen finden Sie im Artikel Gateway Server bearbeiten.

CMIS-Volumes (Content Management Interoperability Services)

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.

OneDrive für Business

Da OneDrive for Business auf SharePoint basiert, kann auf den Inhalt zugegriffen werden, indem eine SharePoint-Datenquelle in Acronis Cyber Files 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 funktionieren nicht, wenn der Gateway Server manuell in der App hinzugefügt wird. Er muss stattdessen über eine Richtlinie zugewiesen werden.
- Ihre Active Directory muss entweder AD-Verbunddienste verwenden oder eine Azure-AD sein.
- 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.

Erstellen der Datenquelle

1. Öffnen Sie die Acronis Cyber Files-Weboberfläche.
2. Klicken Sie auf die Registerkarte **Mobile Access**.
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. Wählen Sie im Feld**Datenspeicherort** die Option**SharePoint** aus. Die folgenden Felder werden angezeigt:
   - **URL** – geben Sie den SharePoint-Speicherort des OneDrive for Business-Servers, der Website oder der Unterwebsite ein, auf die Sie Zugriff gewähren möchten. Beispiel:
     `https://sharepoint.company.com/mysite/mysubsite/%USERNAME%`
     Diese URL darf nicht auf Verweise verweisen, die über die Subsite-Ebene hinausgehen (Sie dürfen `default.aspx` nicht einschließen).
     Sie können den Platzhalter `%USERNAME%` als Teil des Pfades verwenden. Der Platzhalter wird durch den Namen des Hauptordners des Benutzers ersetzt. `%USERNAME%` muss großgeschrieben werden.

- [Optional] **Dokumentbibliotheksname** – dieses Feld kann den Namen einer bestimmten Dokumentbibliothek spezifizieren.
- [Optional] **Unterpfad** – dieses Feld kann Ordner-Namen innerhalb einer bestimmten Dokumentenbibliothek enthalten. Verwenden Sie Schrägstriche (/) als Trennzeichen. Beispiel: `Sales/Documents`.

9. Drücken Sie **Speichern**.

Zugewiesene Quellen

Auf dieser Seite können Sie nach einem Benutzer oder einer Gruppe suchen, um festzustellen, welche Ressourcen diesen zugewiesen wurden. Die Ressourcen werden in 2 Tabellen aufgelistet – 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 **Ressourcen bearbeiten, die zugewiesen sind an** klicken, kann der Administrator die Zuweisungen für diese Richtlinie schnell bearbeiten.

Auf Clients sichtbare Gateway-Server

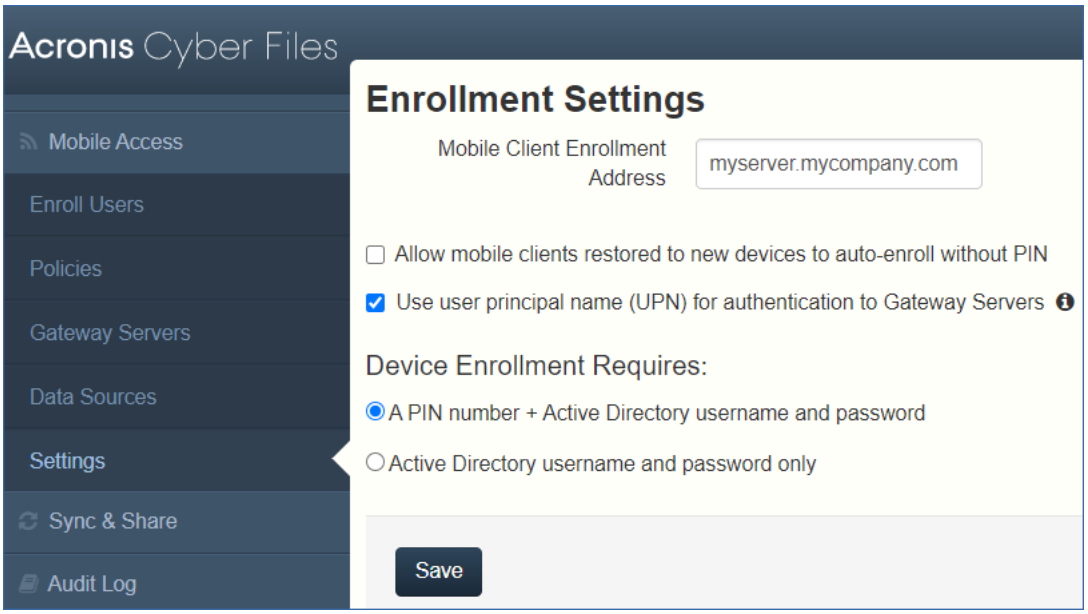
Gateway-Server können Benutzer- oder Gruppenrichtlinien zugewiesen und als Datenquellen eingesetzt werden. Auf dieser Seite werden alle Gateway-Server angezeigt, die in der Acronis Cyber Files-Mobile-App eines Benutzers vorliegen, und es wird angezeigt, ob diesen Gateway-Servern Benutzer- oder Gruppenrichtlinien zugewiesen wurden. Außerdem können Sie diese Zuordnungen hier bearbeiten. Wenn die mobilen Anwender von Acronis Cyber Files 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. Klicken Sie auf dem Server auf die Schaltfläche **Bearbeiten**.
   - Zum Aufheben der Zuweisung zwischen diesem Server und einem Benutzer klicken Sie auf das **X** für den jeweiligen Benutzer.
   - Zum Zuweisen eines neuen Benutzers oder einer neuen Gruppe für diesen Server suchen Sie nach dem Benutzer-/dem Gruppennamen und klicken Sie darauf.
2. Klicken Sie auf **Speichern**.

Hinweis
Wenn Sie einen Gateway Server aus der Cyber Files Server-Administrations-Konsole entfernen, werden alle mobilen Lesezeichen des Benutzers für Datenquellen auf diesem Server dauerhaft gelöscht. Es ist keine Wiederherstellung möglich. Selbst dann nicht, wenn der gleiche Server und die Datenquellen erneut hinzugefügt werden.

Einstellungen



Registrierungseinstellungen

- **Registrierungsadresse für den Mobile Client** – gibt die Adresse an, die Mobile Clients verwenden sollten, wenn sie sich für das Client-Management registrieren.

  Hinweis
  Es wird dringend empfohlen, einen DNS-Namen als Adresse für die Registrierung mobiler Clients zu verwenden. Nach erfolgreicher Registrierung in Client Management speichert die mobile AcronisCyber Files-App die Adresse des Acronis Cyber Files-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 AcronisCyber Files-Apps verwaltet werden, ohne PIN bei dem neuen Server registrieren.
- **Benutzerprinzipalname (UPN) zur Authentifizierung an Gateway Servern verwenden** – Wenn diese Option aktiviert ist, authentifizieren sich Benutzer an den Gateway Servern mit ihrem

UPN (z. B. Benutzername@firma.com). Wenn diese Option deaktiviert ist, authentifizieren sich Benutzer mit ihrem Domain- und Benutzernamen (z. B. Domain/Benutzer).

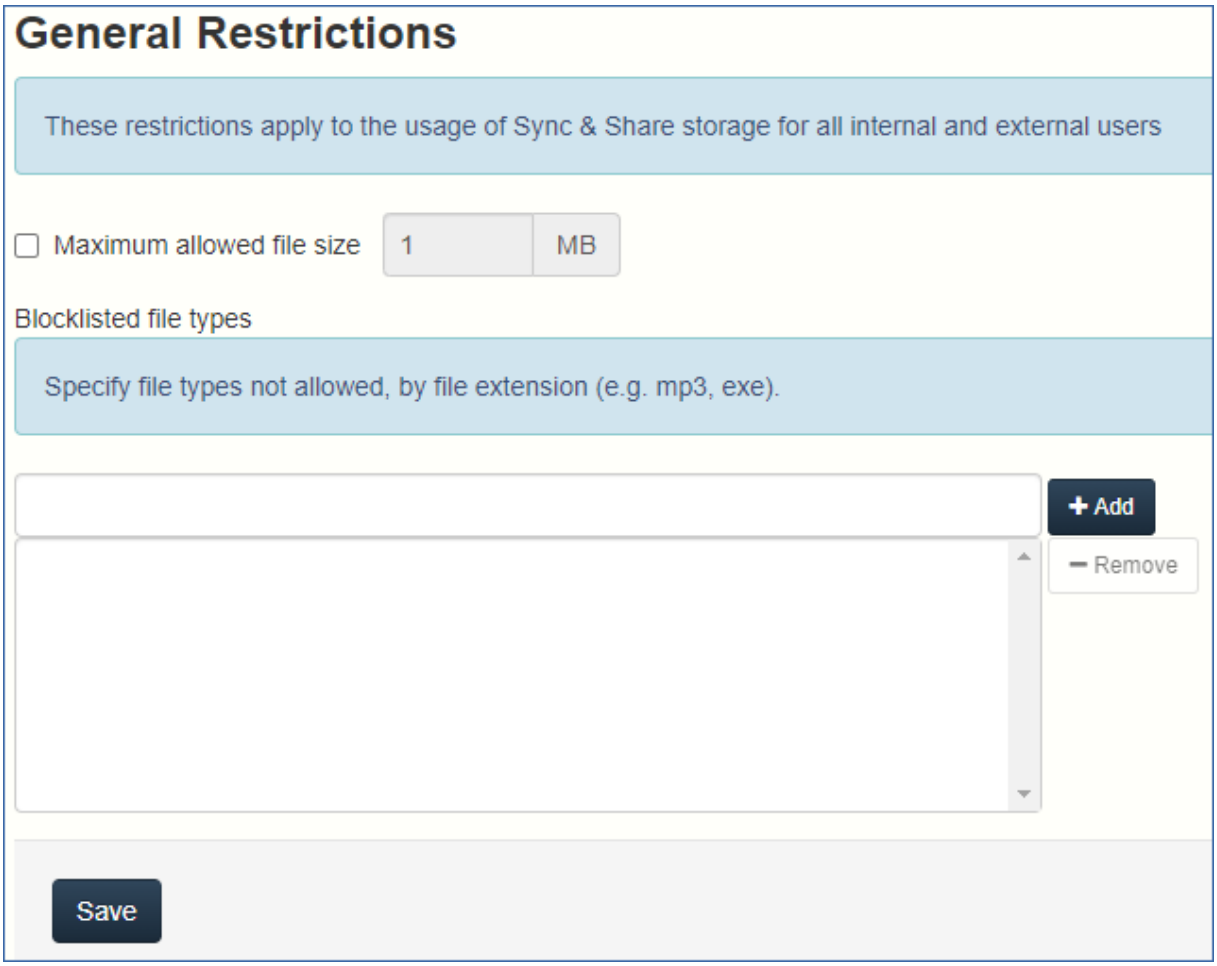
Geräteregistrierung erfordert:

- **PIN-Nummer + Active Directory-Benutzername und -Kennwort** – Ein Benutzer muss eine zeitlich begrenzte, einmalig verwendbare PIN-Nummer sowie gültige Active Directory-Anmeldedaten (Benutzername und Kennwort) eingeben, um seine Acronis Cyber Files App aktivieren und auf die Acronis Cyber Files Server zugreifen zu können. Mit dieser Option wird sichergestellt, dass ein Benutzer nur ein (1) Gerät anmelden kann, und das auch nur, nachdem er eine von seinem IT-Administrator ausgestellte PIN-Nummer erhalten hat. Diese Option wird empfohlen, wenn die eine Zwei-Faktor-Geräte-Registrierung zur Gewährleistung einer höheren Sicherheit erforderlich ist.
- **Nur Active Directory-Benutzername und -Kennwort** – Ein entsprechender Benutzer kann seine Acronis Cyber Files-App nur über seine Active Directory-Anmeldedaten (Benutzername, Kennwort) aktivieren. Diese Option ermöglicht es einem Benutzer, zu einem beliebigen Zeitpunkt in der Zukunft ein oder mehrere Geräte zu registrieren. Den Benutzern muss nur der Name ihres jeweiligen Acronis Cyber Files Servers mitgeteilt werden oder eine URL, die auf diesen Acronis Cyber Files Server verweist. Diese Informationen können über eine Website oder per E-Mail bereitgestellt werden, was es wiederum vereinfacht, Acronis Cyber Files für eine größere Benutzeranzahl bereitzustellen. Diese Option wird für Umgebungen empfohlen, für die keine Zwei-Faktor-Registrierung erforderlich ist und viele Benutzer möglicherweise jederzeit auf Acronis Cyber Files zugreifen müssen (wie z.B. bei Bereitstellungen für Schüler bzw. Studierende).

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.

Allgemeine Beschränkungen



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

Maximal erlaubte Dateigröße – Diese Option ermöglicht es, eine maximale Dateigröße für alle Sync & Share-Dateien festzulegen.

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

So legen Sie eine Blockliste für Dateitypen an:

1. Erweitern Sie in der Webkonsole die Registerkarte **Sync & Share**, und öffnen Sie **Allgemeine Beschränkungen**.

2. Geben Sie im Feld zum **Hinzufügen** unter **Blockierte Dateitypen** eine mit Komma getrennte Liste aller Dateitypen ein, die blockiert werden sollen.
3. Klicken Sie auf **Speichern**.

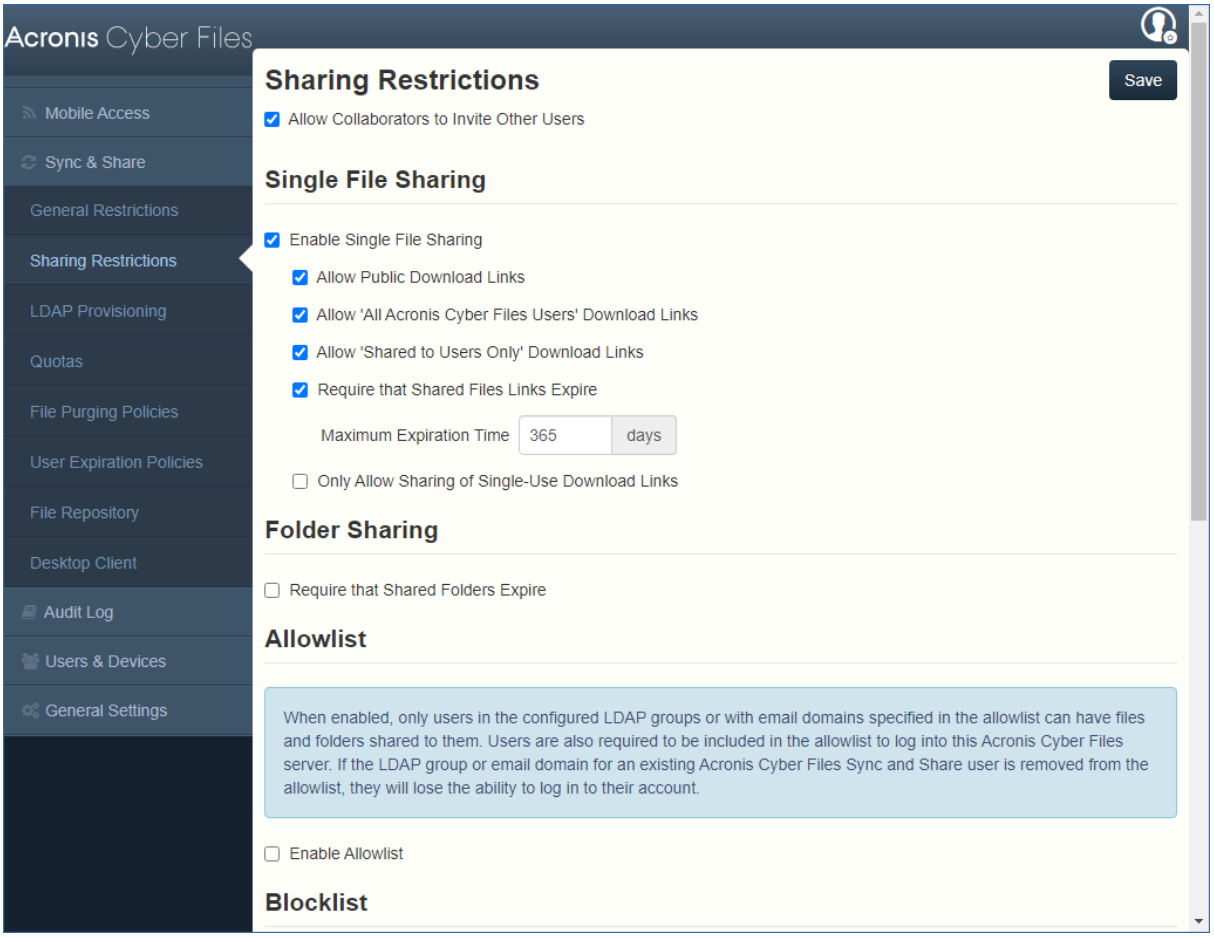
Hinweis
Alle bereits vorhandenen Dateien dieses Typs werden nicht mehr synchronisiert und können nicht verschoben werden. Sie können sie nur manuell herunterladen oder entfernen.

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. Klicken Sie auf **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.

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 können und wie lange der Zugriff darauf möglich sein soll.

- **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 Acronis Cyber Files-Benutzern' erlauben** – Wenn diese Option aktiviert ist, können nur Benutzer mit Anmeldedaten für Acronis Cyber Files auf die freigegebene Datei zugreifen.
  - **Download nur internen Benutzern (AD) erlauben** – Wenn diese Option aktiviert ist, können nur Benutzer mit Active Directory-Anmeldedaten für Acronis Cyber Files auf die freigegebene

Datei zugreifen.

- **Download-Links 'Nur für bestimmte Benutzer' erlauben** – Wenn diese Option aktiviert ist, können nur die Benutzer, für die diese Links freigegeben wurden, diese Links auch tatsächlich verwenden.
- **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** – Wenn diese Option aktiviert ist, können Benutzer nur Einmal-Links senden. Diese Links werden nach dem ersten Download widerrufen.

Ordnerfreigabe

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

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

Positivliste

Wenn die Positivliste aktiviert ist, können sich nur Benutzer in den konfigurierten LDAP-Gruppen oder mit den in der Liste angegebenen 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.

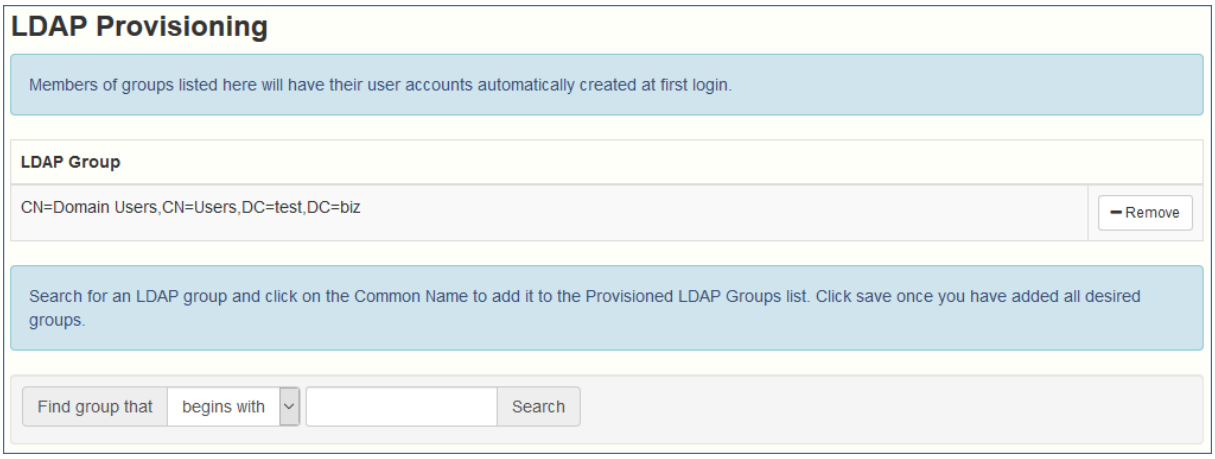
Blockliste

Benutzer in den LDAP-Gruppen oder mit den in der Blockliste spezifizierten E-Mail-Domains (z. B. beispiel.com) können sich nicht beim System anmelden, selbst wenn sie auf der Positivliste 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 durch einen Punkt platziert werden (z.B. *.beispiel.com, *.com).

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.



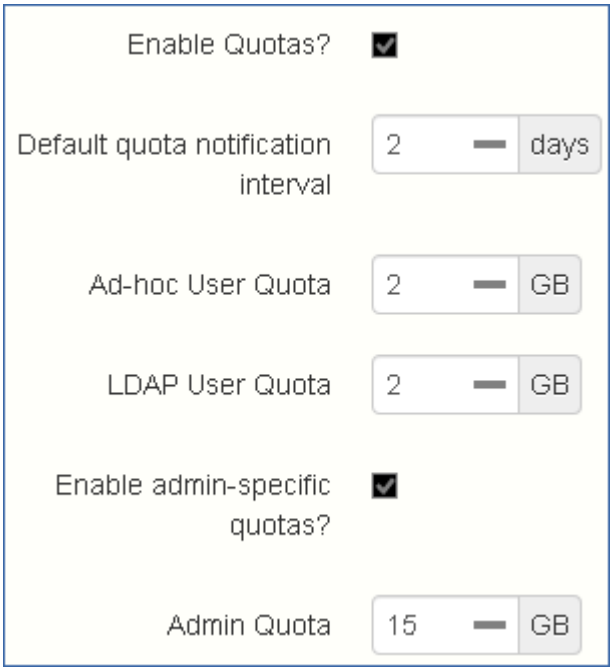
LDAP-Gruppe

Dies ist die Liste der aktuell ausgewählten Gruppen.

- **Allgemeiner Name/Anzeigename** – Der Anzeigename des Benutzers oder der Gruppe.
- **Distinguished Name** – Der Distinguished Name, der dem Benutzer oder der Gruppe zugewiesen wird. Ein Distinguished Name ist ein eindeutiger Name für einen Eintrag im Verzeichnisdienst (Directory Service).

Quotas

Administratoren können den Speicherplatz festlegen, der jedem Benutzer im System zugewiesen wird. Es gibt unterschiedliche Standardeinstellungen für externe (ad-hoc) und interne (Active Directory – LDAP) Benutzer.
Administratoren können zudem unterschiedliche Quota-Werte basierend auf einzelnen Benutzern oder Active Directory-Gruppenmitgliedschaften zuweisen.



- **Quotas aktivieren?** – Wenn diese Option aktiviert ist, wird der maximale Speicherplatz, der einem Benutzer zur Verfügung steht, durch eine Quota beschränkt.
  - **Standard-Quota-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.

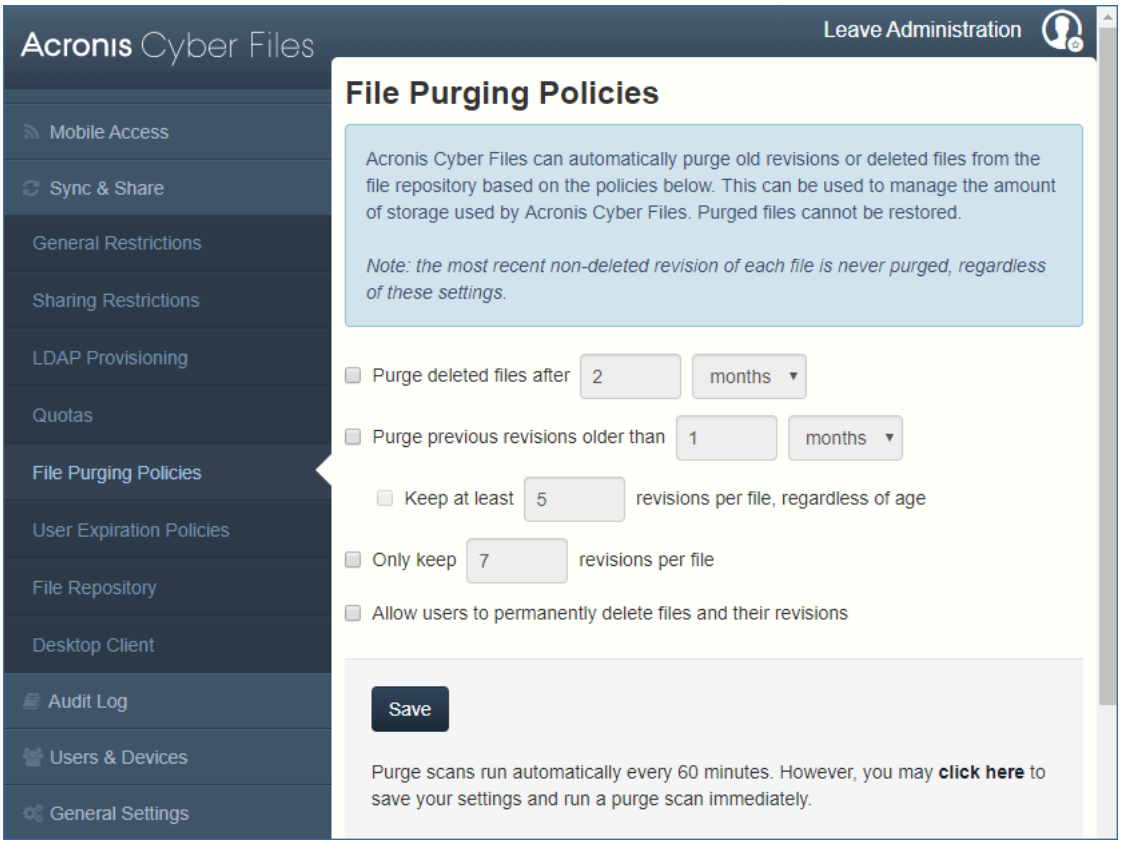
Hinweis
Quotas können auch für einzelne Benutzer spezifiziert werden. Die Einstellungen für einzelne Quotas überschreiben alle anderen Quota-Einstellungen. Um einzelne Quotas für andere Benutzer hinzuzufügen, müssen Sie den Benutzer auf der Seite **Benutzer** bearbeiten.

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

Dateibereinigungsrichtlinien

In Acronis Cyber Files werden Dateien normalerweise so lange im System aufbewahrt, bis sie explizit dauerhaft gelöscht werden. Dadurch können Benutzer einfach gelöschte Dateien weiterhin wiederherstellen und so auch auf frühere Dokumentversionen zugreifen. Administratoren können mit Acronis Cyber Files Richtlinien definieren, die bestimmen, wie lange gelöschte Dateien gespeichert, wie viele maximale Dateiversionen aufbewahrt und wann alte Dateiversionen gelöscht werden sollen.

Acronis Cyber Files 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 Acronis Cyber Files belegte Speichermenge zu verwalten. Endgültig gelöschte Dateien können nicht wiederhergestellt werden.



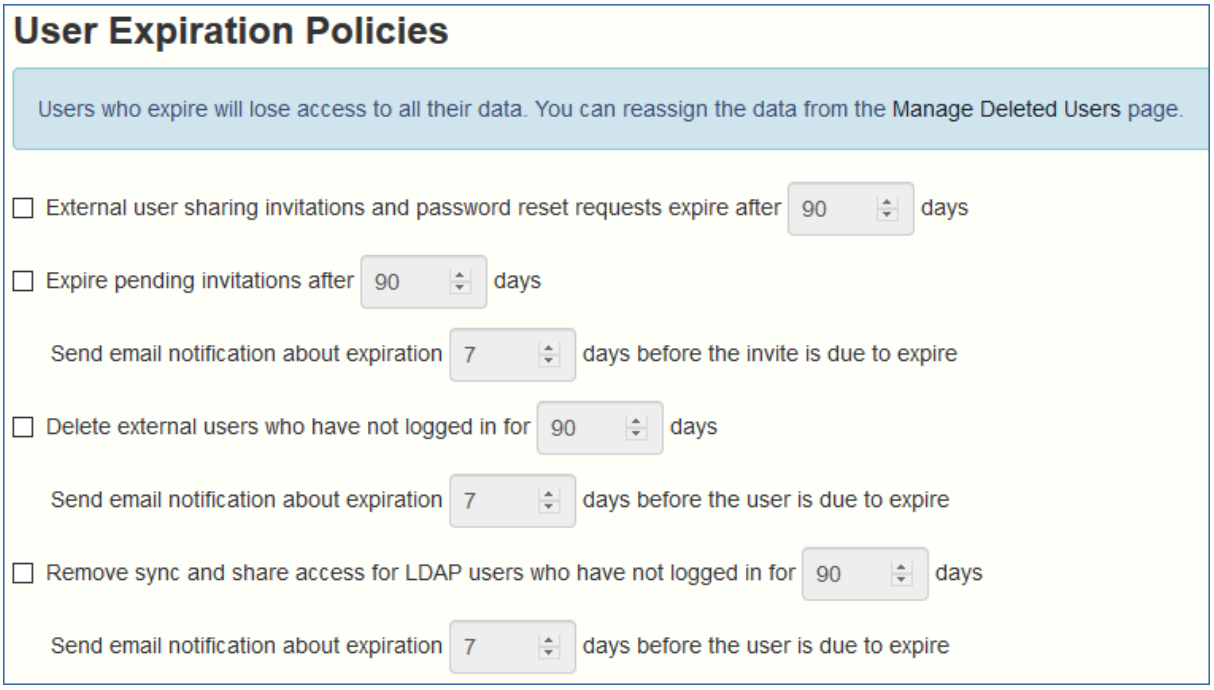
Hinweis
Die neueste ungelöschte Version einer Datei wird, unabhängig von diesen Einstellungen, niemals entfernt.

- **Gelöschte Dateien entfernen nach** – Wenn diese Option aktiviert ist, werden Dateien, die älter als die hier eingestellte Zeit sind, gelöscht.
- **Frühere Versionen entfernen, die älter sind als** – Wenn diese Option aktiviert ist, werden Dateiversionen gelöscht, die älter sind als der festgelegte Wert.
  - **Behalte mindestens X Versionen pro Datei, ungeachtet ihres Alters** – Wenn diese Option aktiviert ist, wird eine Mindestanzahl der Versionen behalten, unabhängig vom Alter.
- **Behalte nur X Versionen pro Datei** – Wenn diese Option aktiviert ist, wird die Anzahl der Versionen pro Datei beschränkt.
- **Benutzern erlauben, Dateien und deren Versionen dauerhaft zu löschen** – Wenn diese Option aktiviert ist, werden alle Dateien und deren Versionen dauerhaft gelöscht und können nicht wiederhergestellt werden.

Hinweis
Speichern Sie Ihre Einstellungen mit der Schaltfläche **Speichern**. Um zusätzlich zum Speichern der Einstellungen sofort eine Bereinigung durchzuführen, verwenden Sie die Option **hier klicken**, ansonsten wird ein regulärer Scan alle 60 Minuten durchgeführt.

Benutzerablaufrichtlinien

Sie können festlegen, dass Einladungen und Benutzerkonten nach einem bestimmten Zeitraum der Inaktivität ablaufen.



- **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 ausstehenden 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 eine bestimmte Anzahl von Tagen, bevor die Gültigkeit des Adhoc-Benutzers abläuft, eine Benachrichtigung gesendet.
- **Sync & Share-Zugriff für LDAP-Benutzer entfernen, 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, wieder entfernt.

- **Sende E-Mail-Benachrichtigung über den Ablauf X Tage bevor der Benutzer verfällt** – Wenn diese Option aktiviert ist, wird eine bestimmte Anzahl von Tagen, bevor die Gültigkeit des Benutzers abläuft, eine Benachrichtigung gesendet.

Was geschieht mit Inhalten abgelaufener Benutzerkonten?

Benutzer, deren Konten ablaufen, verlieren den Zugriff auf und das Eigentum an allen ihren Inhalten. Die Inhalte werden jedoch im System gespeichert.

Sie müssen die Inhalte entweder anderen Benutzern neu zuweisen oder dauerhaft löschen.

Wichtig
Sie müssen den Inhalt eines abgelaufenen Benutzerkontos erst dauerhaft löschen, bevor der Speicherplatz freigegeben werden kann. Durch das Entfernen von Dateien werden nur Inhalte entfernt, die der abgelaufene Benutzer zuvor gelöscht hat.

Datei-Repository

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

- **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.

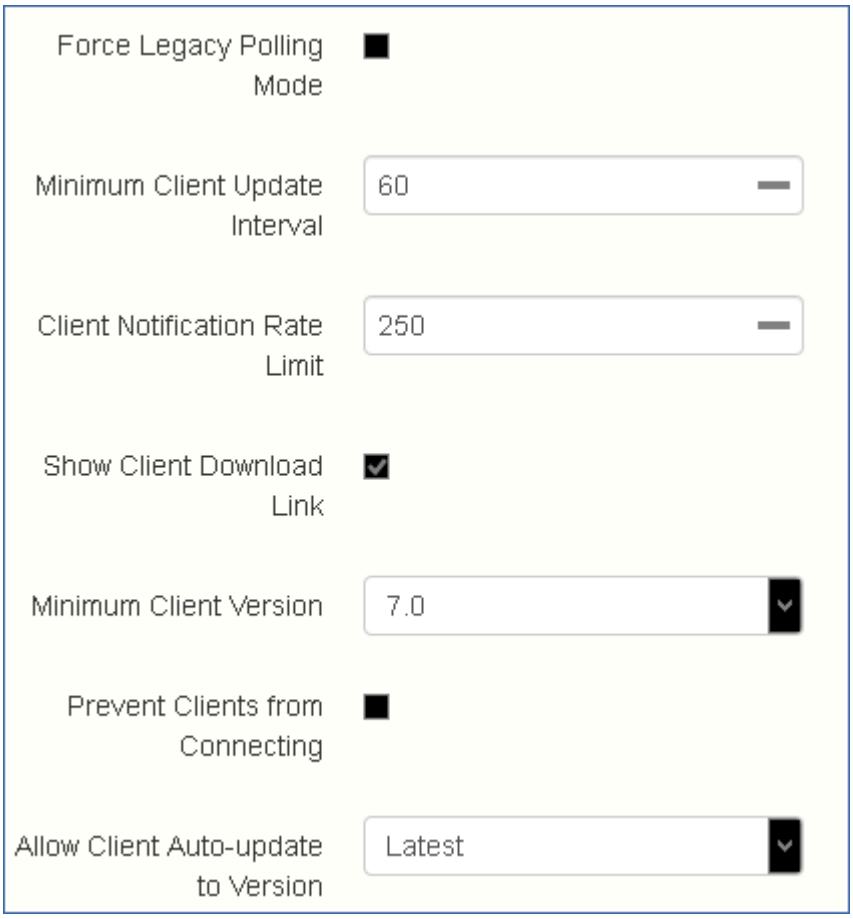
  Hinweis
  MinIO S3-Storage wird als Typ unterstützt und kann mit der Option **Anderer S3-kompatibler Storage** konfiguriert werden, er wird jedoch nicht über eine unsichere HTTP-Verbindung unterstützt.

  Hinweis
  Wenn mehrere Benutzer die gleiche Datei hochladen, entspricht der insgesamt genutzte Speicher der Anzahl dieser Benutzer multipliziert mit der Dateigröße, d.h. der genutzte Speicher ist proportional zur Anzahl der Benutzer und Uploads. Der genutzte Speicher entspricht der Gesamtzahl aller von den teilnehmenden Benutzern hochgeladenen Dateien. Die Größe des belegten Speichers hängt jedoch nicht von der Art bzw. den Arten des verwendeten Back-End-Storage ab, ebenso wenig wie von der Tatsache, dass die gleiche Datei hochgeladen wird.

- **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.

Acronis Cyber Files-Client

Diese Einstellungen gelten für den Desktop Client.



- **Herkömmlichen Polling-Modus erzwingen** – Erzwingt, dass die Clients den Server abfragen, anstatt asynchron vom Server benachrichtigt zu werden. Sie sollten diese Option nur aktivieren, wenn Sie vom Acronis Support dazu aufgefordert werden.
  - **Client-Polling-Dauer** – Legt die Zeitintervalle fest, in denen der Client den Server abfragen wird. 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 den Webbenutzern ein Link zum Download des Desktop Clients angezeigt.
- **Minimale Client-Version** – Legt die niedrigste Client-Version fest, die sich mit diesem Server verbinden darf.

Hinweis
Seit Acronis Cyber Files 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, können Desktop Clients keine Verbindung mit dem Server herstellen. Diese Option sollte im Allgemeinen nur zu administrativen Zwecken aktiviert werden. Diese Option unterbindet jedoch nicht die Verbindung zur Weboberfläche.
- **Erlaube Client-Auto-Update auf Version** – Legt die Desktop Client-Version fest, die per automatischer Update-Prüfungen für alle Desktop Clients bereitgestellt wird. Wählen Sie **Keine Updates erlauben**, um zu bewirken, dass Clients gar keine Auto-Update durchführen dürfen.

Benutzer und Geräte

Geräte verwalten

Sobald Acronis Cyber Files-Benutzer eine Verbindung zum Acronis Cyber Files-Web-Server herstellen, werden ihre Geräte in der Liste **Geräte** aufgeführt.

Hier werden detaillierte Statusinformationen zu allen verwendeten Geräten angezeigt. Sie können die Acronis Cyber Files-App auch löschen oder ihr Kennwort ändern.

- **Benutzername** – Active Directory (AD)-Anzeigename für einen LDAP-Benutzer oder ein von einem Ad-hoc-Benutzer gewählter Name.
- **Gerätename** – der vom Benutzer festgelegte Gerätename.
- **Modell** – Produktname des mobilen Geräts des Benutzers.
- **Betriebssystem** – Typ und Version des Betriebssystems auf einem Desktop oder mobilen Gerät.
- **Version** – Version der Acronis Cyber Files-App oder des verwendeten Desktop-Clients.
- **Status** – Status der Acronis Cyber Files-App. Zu den möglichen Werten zählen:
  - Verwaltet;
  - Verwaltet, ausstehende Remote-Löschung;
  - Nicht verwaltet, Remote-Löschung erfolgreich;
  - Nicht verwaltet, ausstehende Remote-Löschung;
  - Vom Benutzer nicht verwaltet;
  - Gelöscht nach Eingabe des falschen Kennworts durch den Benutzer.

Für den Desktop-Client ist 'Sync & Share' der einzige Status.

- **Letzter Kontakt** – Datum und Uhrzeit der letzten Verbindung zwischen Management Server und Acronis Cyber Files-App/-Desktop-Client.
- **Richtlinie** – Name und Link der auf einen Benutzer angewendeten Verwaltungsrichtlinie.
- **Aktionen**
  - **Weitere Informationen** – Zeigt weitere Details zum Gerät und ein bearbeitbares Feld für **Notizen** für das Gerät an.
  - **App-Kennwort zurücksetzen** (nur für mobile Geräte) – Setzt das Kennwort zum Sperren der Acronis Cyber Files-App auf dem ausgewählten Gerät zurück. Sie müssen hierzu einen Bestätigungscode generieren, indem Sie den auf dem Gerätebildschirm des Benutzers angezeigten Kennwortzurücksetzungscode verwenden.
  - **Remote-Löschung** (nur für mobile Geräte) – Wenn diese Option ausgewählt ist, werden alle Dateien in der Acronis Cyber Files-App und deren Einstellungen gelöscht, sobald das Gerät eine Verbindung zum Management Server herstellt. Daten anderer Apps oder des Betriebssystems sind nicht betroffen.

- **Aus Liste entfernen** – Mit dieser Option wird ein Desktop-Client aus der **Geräteliste** entfernt. Bei mobilen Geräten wird hierdurch das ausgewählte Gerät aus der Liste entfernt. Die Verwaltung für dieses Gerät wird aufgehoben, ohne es zu löschen. Damit werden meist Geräte entfernt, bei denen von keinem weiteren Kontakt mit dem Acronis Cyber Files-Management-Server auszugehen ist. Wenn Sie die Option **'Mobilen Clients, die auf neuen Geräten wiederhergestellt wurden, eine automatische Registrierung ohne PIN erlauben'** aktiviert haben, werden diese neuen Geräte automatisch als verwaltet angezeigt, sobald sie eine Verbindung zum Server herstellen.

Daten zu Geräten exportieren

Die Daten zu allen Geräten in dieser Liste können als txt-, csv- oder xml-Datei exportiert werden.

Klicken Sie dazu auf die Schaltfläche **Exportieren** und wählen Sie das gewünschte Dateiformat aus.

Exportierte Daten enthalten Folgendes:

1. Benutzername
2. Name des verwendeten mobilen Geräts oder Computers
3. Modell des mobilen Geräts
4. Typ und Version des Betriebssystems auf dem Gerät
5. Acronis Version der Cyber Files-App oder des Desktop-Clients
6. Status des mobilen Geräts oder des Desktop-Clients
7. Datum und Uhrzeit der Registrierung der Acronis Cyber Files-App beim Acronis Cyber Files-Web-Server
8. Datum und Uhrzeit des letzten Kontakts zwischen der Acronis Cyber Files-App oder dem Desktop-Client und dem Acronis Cyber Files-Web-Server
9. Name der angewendeten Benutzerrichtlinie
10. Notizen

Durchführen von Kennwortzurücksetzungen für die Remote-Applikation

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

Falls ein Kennwort zum Sperren der App verloren geht, sind die einzigen verfügbaren Optionen die Remote-Zurücksetzung des Kennworts oder die Deinstallation und erneute Installation der Acronis Cyber Files-App 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 Acronis Cyber Files-Server, wenn sie eine neue Verwaltungseinladung erhalten.

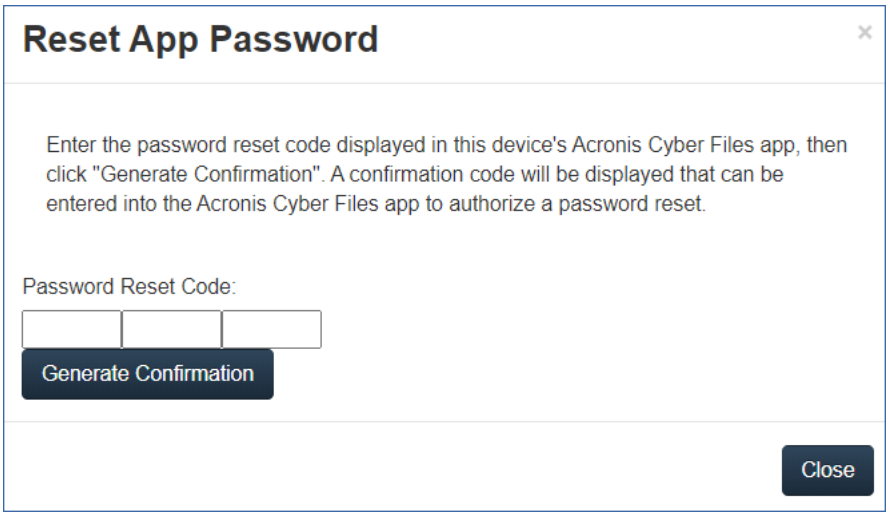
Zurücksetzen des Kennworts für die Applikation

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

Ein Aspekt dieser Verschlüsselung besteht darin, dass Benutzer der Acronis Cyber Files-App das Kennwort zum Sperren der Applikation nicht über Datenfunk (Over the Air) zurückzusetzen können. Stattdessen müssen zwischen dem Benutzer und dem IT-Administrator von Acronis Cyber Files ein Kennwortzurücksetzungscode und ein Bestätigungscode ausgetauscht werden, damit Acronis Cyber Files seine Einstellungsdatenbank entschlüsseln und der Benutzer ein neues App-Kennwort festlegen kann.

So setzen Sie das Kennwort für die Acronis Cyber Files-App für iOS oder Android zurück:

1. Ein Endbenutzer bittet Sie um das Zurücksetzen seines Kennworts für die Acronis Cyber Files-App und teilt Ihnen den **Kennwortzurücksetzungscode** mit, der auf seinem Gerätebildschirm angezeigt wird.
2. Öffnen Sie die Registerkarte **Benutzer und Geräte**.
3. Rufen Sie die Registerkarte **Geräte** auf.
4. Suchen Sie nach dem Gerät, dessen App-Kennwort zurückgesetzt werden soll, und klicken Sie auf die Schaltfläche **Aktionen**.
5. Drücken Sie **App-Kennwort zurücksetzen...**.
6. Geben Sie den **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 in das entsprechende Dialogfeld für das Zurücksetzen des App-Kennworts ein und wird dann aufgefordert, ein neues Kennwort festzulegen. Wenn der Benutzer diesen Vorgang abbricht, ohne ein neues App-Kennwort festzulegen, wird ihm der Zugriff auf die Acronis Cyber Files-App verweigert und er muss den Vorgang zum Zurücksetzen des Kennworts wiederholen.



Durchführen von Remote-Löschungen

Acronis Cyber Files ermöglicht die Remote-Löschung einer mobilen App. Hierbei werden alle in der Acronis Cyber Files-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.

Gehen Sie hierfür folgendermaßen vor:

1. Öffnen Sie die Acronis Cyber Files-Weboberfläche.
2. Öffnen Sie die Registerkarte **Benutzer und Geräte**, und navigieren Sie zu **Geräte**.
3. Suchen Sie nach dem Gerät, für das Sie die Remote-Löschung durchführen möchten, und wählen Sie **Aktionen**.
4. Wählen Sie **Remote-Löschung...**
5. Bestätigen Sie die Remote-Löschung durch Drücken von **Löschen**.
6. In der Spalte **Status** für das Gerät wird der Status **'Ausstehende Remote-Löschung'** angezeigt.

   Hinweis
   Der Administrator kann eine ausstehende Remote-Löschung abbrechen, solange die App noch keine Verbindung zum Verwaltungsserver hergestellt hat. Diese Option wird im Menü **Aktionen** angezeigt, nachdem ein Remote-Löschvorgang aufgerufen wurde.

7. Die Remote-Löschung wird abgeschlossen, sobald das Gerät erneut eine Verbindung zum Server herstellt. Dieser Schritt kann nicht rückgängig gemacht werden.

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

Benutzer verwalten

Über den Bereich **Benutzer** 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 Benutzer bearbeiten, können Sie ihnen administrative Rechte zuweisen (falls Sie dazu berechtigt sind), ihre E-Mail-Adressen ändern, ihre Kennwörter ändern oder ihre Konten deaktivieren bzw. aktivieren.

Wenn Quotas aktiviert sind, können Sie für bestimmte Benutzer einen benutzerdefinierten Quota-Wert festlegen. Dies ist jedoch nur dann möglich, wenn der Benutzer über einen Sync & Share-Zugang verfügt.

Beim Löschen von Benutzern müssen Sie auch deren Inhalte verwalten. Wenn ein Benutzer gelöscht wird, fordert Sie das System auf, folgende alternative Maßnahmen vorzunehmen:

- Weisen Sie die Inhalte des Benutzers einem anderen bestehenden Benutzer zu und stellen Sie so sicher, dass die Daten verfügbar bleiben.
- Die Inhalte dauerhaft zu löschen, was das Benutzerkonto und alle zugehörigen Dateien des Benutzers aus dem System entfernt.

Bei Benutzern, die bereits gelöscht wurden, können Sie deren verbleibende Inhalte über die Registerkarte **Gelöschte Benutzerinhalte neu zuweisen** im Bereich **Benutzer & Geräte** verwalten. Auf diese Weise können Sie die Inhalte entweder neu zuordnen oder später endgültig löschen. Weitere Informationen finden Sie unter Benutzer und deren Inhalte löschen.

Typen von Sync & Share-Benutzern

Es gibt drei Typen von Sync & Share-Benutzerkonten:

Externe (Ad-hoc-)Benutzerkonten

Diese Konten müssen über eine vom Administrator gesendete E-Mail-Einladung oder über eine Einladung eines anderen Benutzers zu freigegebenen Inhalten (Datei oder Ordner) manuell erstellt werden.

Es gibt zwei Untertypen externer Konten: **Frei** und **Lizenziert**.

Standardmäßig ist ein neu erstelltes externes Konto ein freies Konto. Nur ein Acronis Cyber Files-Administrator kann ein freies externes Konto in ein lizenziertes externes Konto konvertieren.

Benutzer mit einem lizenzierten Konto können Dateien und Ordner im eigenen Sync & Share-Bereich erstellen, hochladen, bearbeiten und löschen. Sie können zudem ihre Inhalte für andere freigeben.

Benutzer mit einem freien Konto haben keinen Sync & Share-Bereich. Wenn Benutzern mit freien Konten die entsprechenden Rechte gewährt werden, können sie neue Dateien erstellen, Dateien von einem anderen Speicherort hochladen und ausschließlich Dateien in einem für sie freigegebenen Ordner bearbeiten und löschen. Wenn diesen Benutzern 'Nur Lesen'-Berechtigungen gewährt wurden, können sie keine Dateien erstellen, hochladen, bearbeiten oder löschen. Sie können ausschließlich die in dem für sie freigegebenen Ordner enthaltenen Dateien durchsuchen, herunterladen und eine Vorschau für diese anzeigen.

Benutzer mit freien Konten können weder neue Benutzer zu der freigegebenen Ressource einladen noch sehen, für wen diese Ressource freigegeben ist, auch wenn ihnen solche Rechte bei der Kontoerstellung gewährt wurden.

Wenn eine Datei für einen Benutzer mit einem freien Konto freigegeben wird, kann er diese Daten nur herunterladen oder eine Vorschau anzeigen.

Benutzer mit freien Konten können weder den Desktop-Client noch die mobilen Apps von Acronis Cyber Files verwenden.

Hinweis
Alle neu erstellten externen Konten müssen manuell aktiviert werden. Benutzer erhalten eine E-Mail mit entsprechenden Anweisungen.

Interne (LDAP-)Benutzerkonten

Diese Konten basieren auf der Integration in Active Directory (AD). Sie werden entweder wie die externen manuell erstellt, oder ein Administrator kann eine bereitgestellte LDAP-Gruppe einrichten und zulassen, dass die Konten für AD-Benutzer automatisch beim ersten Anmelden bei Acronis Cyber Files erstellt werden.

Die internen Konten werden bei Erstellung automatisch zu lizenzierten Konten.

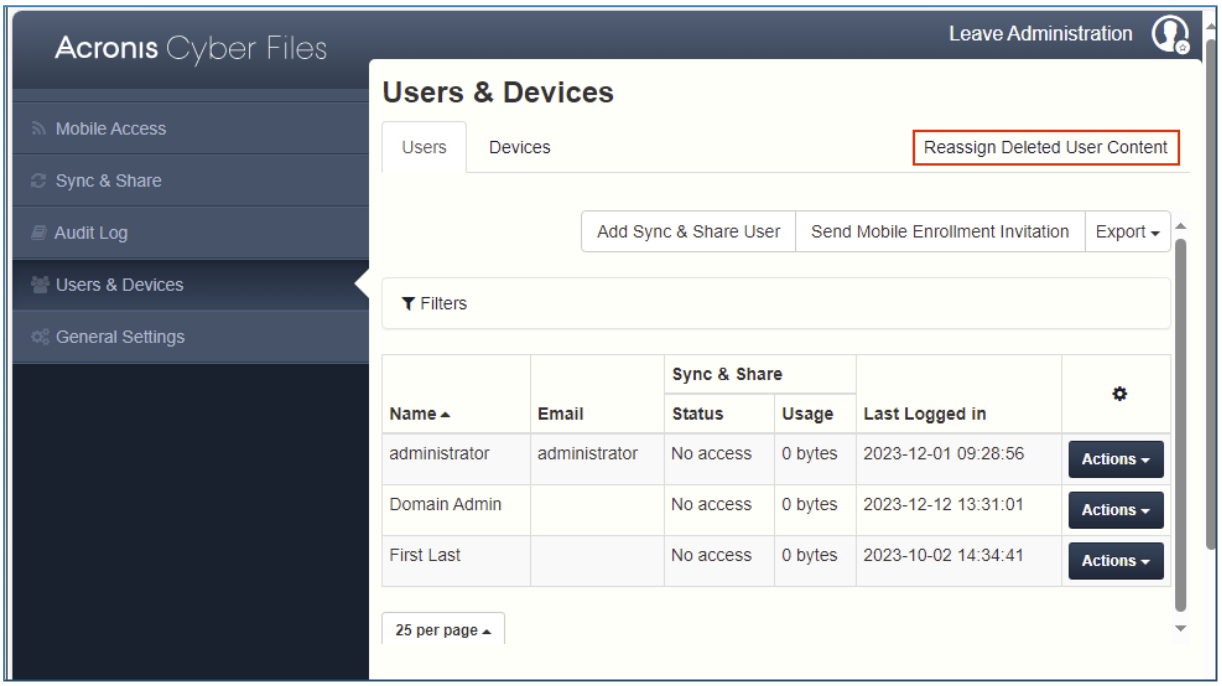
Benutzer mit internen Konten können Dateien und Ordner im eigenen Sync & Share-Bereich oder in den für sie freigegebenen Ordnern erstellen, hochladen, bearbeiten und löschen. Sie können zudem ihre Inhalte für andere freigeben.

Sie können den Desktop-Client und die mobilen Apps von Acronis Cyber Files verwenden.

Benutzerkonten ohne Zugriff

Dies sind administrative Konten ohne Sync & Share-Zugriff. Sie sind standardmäßig nicht lizenziert. Benutzer mit diesen Konten können weder den Desktop-Client noch die mobilen Apps von Acronis Cyber Files verwenden.

Hinweis
Administratoren ohne Sync & Share-Zugriff müssen keine E-Mail-Adresse für ihr Konto festlegen. Sie können sich einfach mit ihren LDAP-Anmeldedaten anmelden. Diese Konten können erstellt werden, ohne zuvor SMTP für den AcronisCyber Files Server einzurichten. Weitere Informationen finden Sie unter Administratoren und Berechtigungen.



Auf der Registerkarte **Benutzer** werden die folgenden Informationen angezeigt:

- **Name** – Zeigt den Namen des Benutzers (Active Directory (AD)-Anzeigename für LDAP-Benutzer oder ein von einem Ad-hoc-Benutzer gewählter Name) an.
- **Benutzername** (optional) – Zeigt den Anmeldenamen der LDAP-Benutzer an.
- **Benutzerprinzipalname (UPN)** (optional) – Zeigt den Benutzerprinzipalnamen der LDAP-Benutzer an.
- **Domain** (optional) – Zeigt die Domain der LDAP-Benutzer an.
- **E-Mail** – Zeigt die E-Mail-Adresse des Benutzers an.
- **Sync & Share**
  - **Status** – Gibt den verwendeten Lizenztyp an.
  - **Verwendung** – Zeigt die Gesamtgröße der Inhalte des Benutzers an.
- **Letzte Anmeldung** – Zeigt Datum und Uhrzeit der letzten Anmeldung an.
- **Aktionen**
  - **Weitere Informationen** – Zeigt zusätzliche Informationen zum Benutzer an.
  - **Geräte anzeigen** – Zeigt Informationen zu den von diesem Benutzer verwendeten Geräten an.
  - **Sync & Share-Kennwort zurücksetzen** – Sendet eine E-Mail für die Kennwortzurücksetzung.

- **Zu 'Lizenziert' konvertieren** – Konvertiert einen freien Benutzer in einen lizenzierten Benutzer.
- **Benutzer bearbeiten** – Ermöglicht das Bearbeiten dieses Benutzers, darunter das Ändern der E-Mail-Adresse, Deaktivieren oder Aktivieren des Kontos, Gewähren voller oder bestimmter Administratorrechte oder Festlegen benutzerdefinierter Quotas für das Konto. Für externe Benutzer können Sie ihre Mobiltelefonnummern ändern, die für 2FA verwendet werden.
- **Löschen** – Löscht den Benutzer.
- **Gelöschte Benutzerinhalte neu zuweisen** – Mit dieser Option können Administratoren die Inhalte von Benutzern verwalten, die aus dem System gelöscht wurden. Statt die Daten dieser Benutzer ebenfalls umgehend zu entfernen, können Administratoren mit dieser Funktion diese Inhalte entweder an einen anderen Benutzer übertragen oder sie erst nach einer gewissen Zeit endgültig löschen.

Exportieren der Benutzerdaten

Die Daten zu registrierten Benutzern können als txt-, csv- oder xml-Datei exportiert werden.

Klicken Sie dazu auf die Schaltfläche **Exportieren**, und wählen Sie das gewünschte Dateiformat aus.

Exportierte Daten enthalten Folgendes:

1. Name des Benutzers
2. Anmeldename des Benutzers (für LDAP-Benutzer)
3. Benutzerprinzipalname (für LDAP-Benutzer)
4. LDAP-Domain (für LDAP-Benutzer)
5. E-Mail
6. Richtlinienname
7. Ausstehend (Status)
8. Administrative Berechtigungen
9. Lizenzierter Benutzer (Status)
10. Deaktivierter Benutzer (Status)
11. LDAP-Authentifizierung
12. Anzahl der Ordner, die der Benutzer besitzt
13. Anzahl der Dateien, die der Benutzer besitzt
14. Größe der Inhalte des Benutzers (in Byte)
15. Quota-Größe des Benutzers (in Byte)
16. Datum und Uhrzeit der letzten Anmeldung

Hinzufügen eines externen (Ad-hoc-)Benutzers

So fügen Sie einen externen (Ad-hoc-)Benutzer hinzu:

1. Öffnen Sie die Acronis Cyber Files-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 **Benutzer und Geräte**.
4. Öffnen Sie die Registerkarte **Benutzer**.
5. Wählen Sie die Schaltfläche **Sync & Share-Benutzer hinzufügen** aus.
6. Geben Sie die E-Mail-Adresse des Benutzers ein.
7. Wählen Sie die Sprache der Einladung.
8. Drücken Sie **Hinzufügen**.

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

Hinzufügen eines internen (LDAP-)Benutzers

So fügen Sie einen internen (LDAP-)Benutzer hinzu:

1. Öffnen Sie die Acronis Cyber Files-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 **Benutzer und Geräte**.
4. Öffnen Sie die Registerkarte **Benutzer**.
5. Wählen Sie die Schaltfläche **Sync & Share-Benutzer hinzufügen** aus.
6. Geben Sie die E-Mail-Adresse des Benutzers ein.
7. Wählen Sie die Sprache der Einladung.
8. Drücken Sie **Hinzufügen**.

Der Benutzer kann sich nun mit den LDAP-Anmeldedaten anmelden. Sobald sich der Benutzer angemeldet hat, ist die Kontoregistrierung abgeschlossen.

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

Festlegen einer benutzerdefinierten Quota

Sie können für Benutzer mit Sync & Share-Zugriff benutzerdefinierte Quotas festlegen.

Gehen Sie hierfür folgendermaßen vor:

1. Öffnen Sie über die Weboberfläche die Registerkarte **Benutzer & Geräte**.
2. Suchen Sie nach dem 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**.

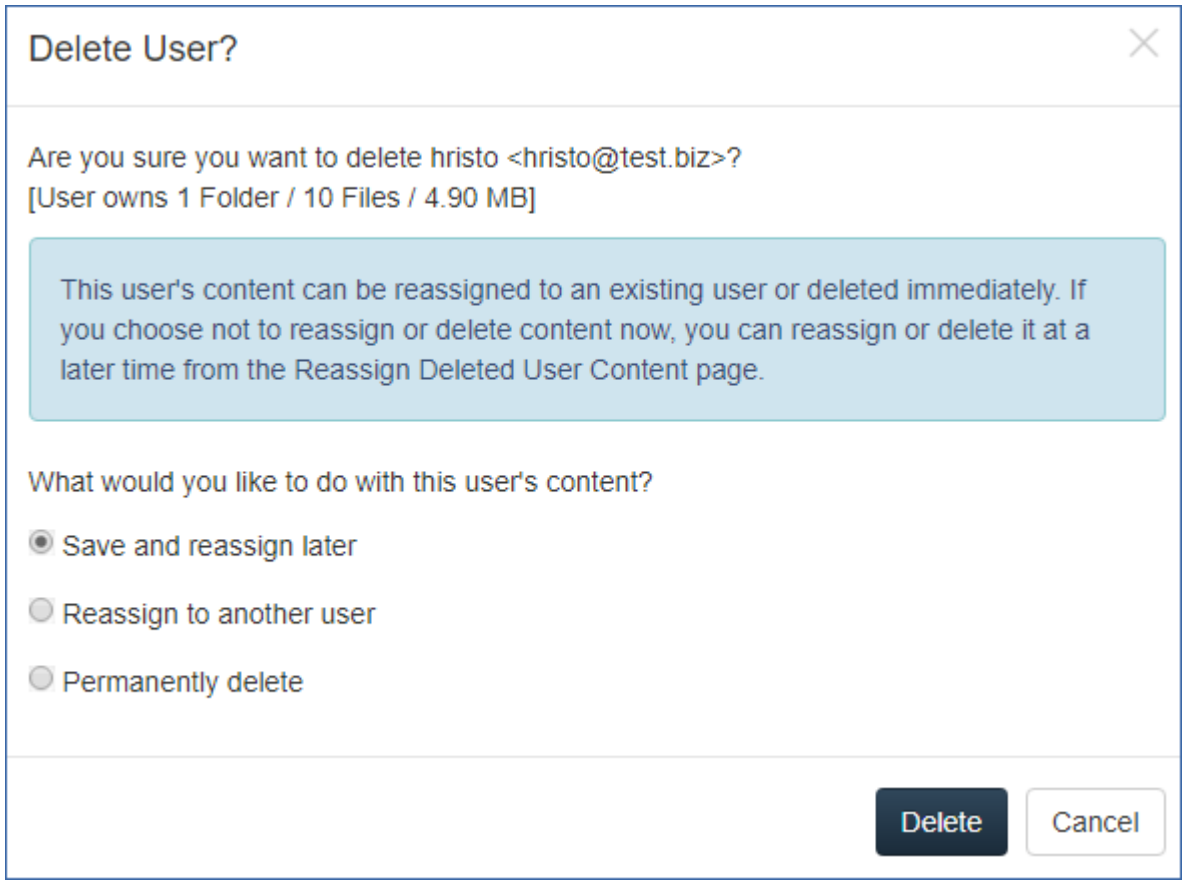
Hinweis
Das Kontrollkästchen **Benutzerdefinierte Quota verwenden?** steht nur zur Verfügung, wenn die globale Option **Quotas aktivieren?** im Vorfeld aktiviert wurde.

Benutzer und deren Inhalte löschen

Sie können Benutzer aus Acronis Cyber Files löschen. Der Prozess variiert jedoch je nachdem, ob der Benutzer mit seinem Konto verknüpften Inhalt hatte.

Wird ein Benutzer gelöscht, der keinen Content besitzt, führt zum vollständigen Entfernen des Kontos.

Beim Löschen eines Benutzers mit Inhalt (einschließlich alter Benutzer) müssen Sie entscheiden, was Sie mit dem Inhalt machen möchten.



- **Speichern und später neu zuweisen** – Die Inhalte des Benutzers werden vorübergehend im System belassen und können über die Registerkarte **Gelöschte Benutzerinhalte neu zuweisen**

verwaltet werden. Solche Inhalte können entweder neu zugewiesen oder dauerhaft gelöscht werden.

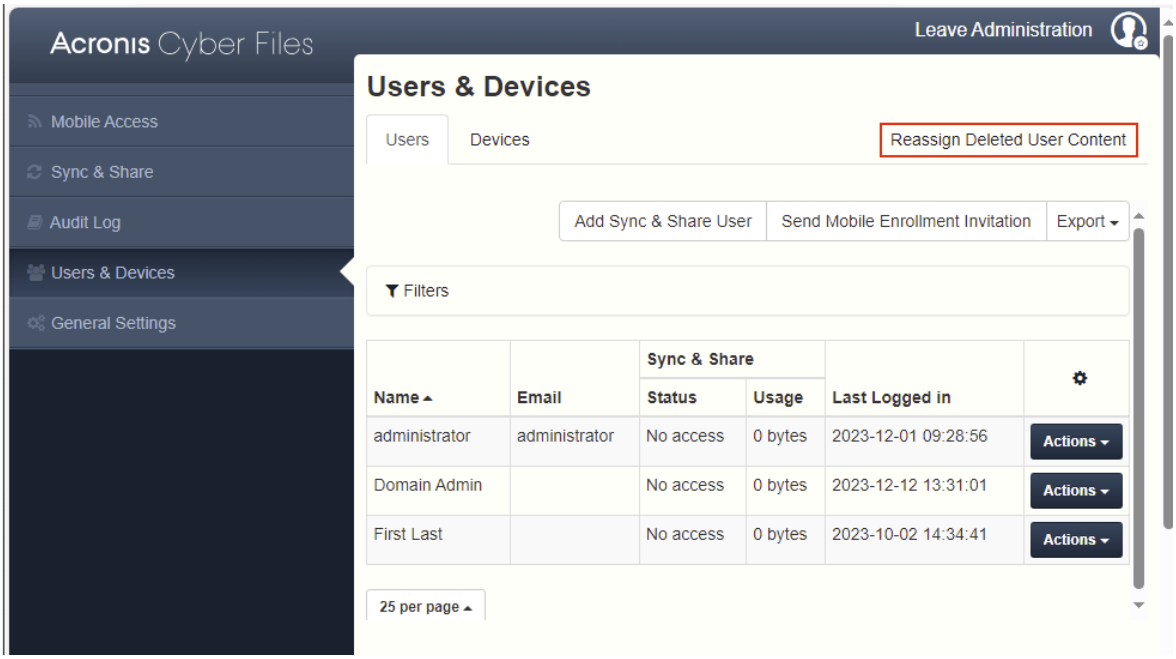
Hinweis
Bereinigungsrichtlinien gelten weiterhin für diese Inhalte wie auch für Inhalte von aktiven Benutzern.

- **Einem anderem Benutzer neu zuweisen** – Die Inhalte werden sofort einem von Ihnen festgelegten Benutzer neu zugewiesen. Dafür wird in dessen -Bereich ein neuer Ordner mit dem Namen **`Inhalte von DeletedUserName <deletedusersemail> übernommen`** erstellt. Der neu festgelegte Benutzer wird zum Besitzer der vererbten Inhalte. Dazu gehören auch die Ordner, die zuvor von dem gelöschten Benutzer freigegeben wurden.
- **Dauerhaft löschen** – Die Inhalte des Benutzers und dessen Konto werden umgehend gelöscht.

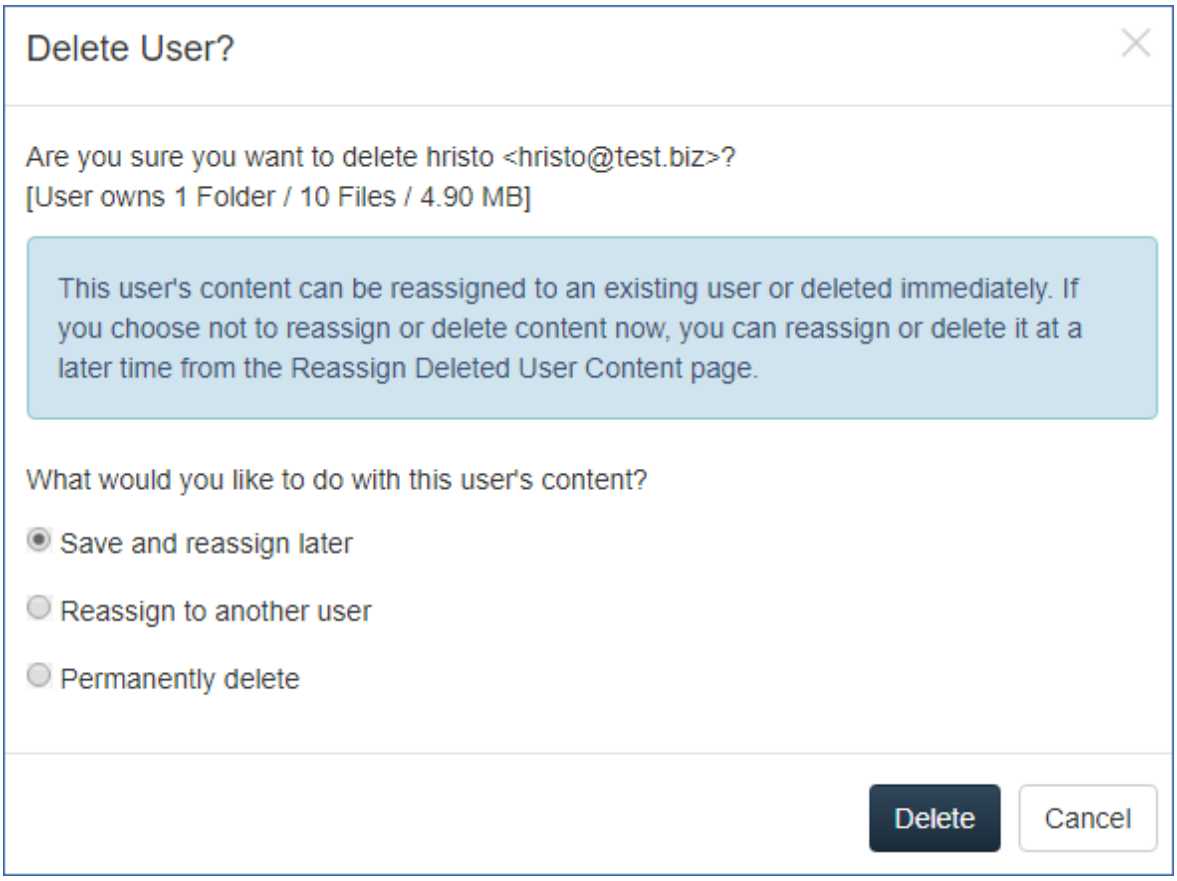
Einen Benutzer und dessen Inhalte dauerhaft löschen

So können Sie einen Benutzer und dessen Inhalte dauerhaft löschen

1. Gehen Sie in der Acronis Cyber Files-Konsole im Hauptmenü links zum Bereich **Benutzer & Geräte**.



2. Ermitteln Sie im Bereich **Benutzer** den zu löschenden Benutzer.
   Sie können die Suchleiste oder auch Filter verwenden, um die Liste der Benutzer einzugrenzen.
3. Klicken Sie neben dem Namen des Benutzers auf die Schaltfläche **Aktionen**.
4. Wählen Sie im Dropdown-Menü **Benutzer löschen**.
   Es wird ein Bestätigungsfenster angezeigt, in dem Sie aufgefordert werden, zu entscheiden, was mit den Inhalten des Benutzers geschehen soll.



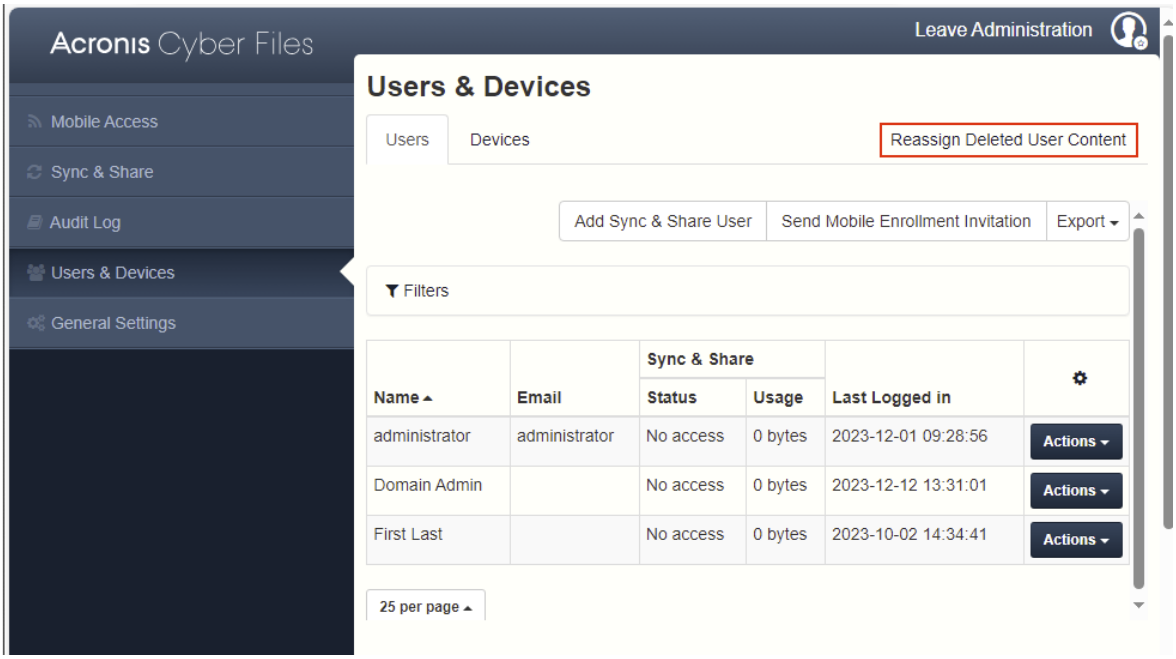
5. Wählen Sie **Dauerhaft löschen**.

Das Benutzerkonto und dessen Inhalte werden umgehend gelöscht.

Die Inhalte gelöschter Benutzer anderen Benutzern zuweisen

So können Sie die Inhalte gelöschter Benutzer anderen Benutzern zuweisen

1. Gehen Sie in der Acronis Cyber Files-Konsole im Hauptmenü links zum Bereich **Benutzer & Geräte**.
2. Klicken Sie oben auf der Seite auf die Registerkarte **Gelöschte Benutzerinhalte neu zuweisen**.



Ihnen wird eine Liste von Benutzern angezeigt, deren Inhalte neu zugewiesen werden können.

3. Wählen Sie den Benutzer aus, dessen Inhalte Sie neu zuweisen wollen.

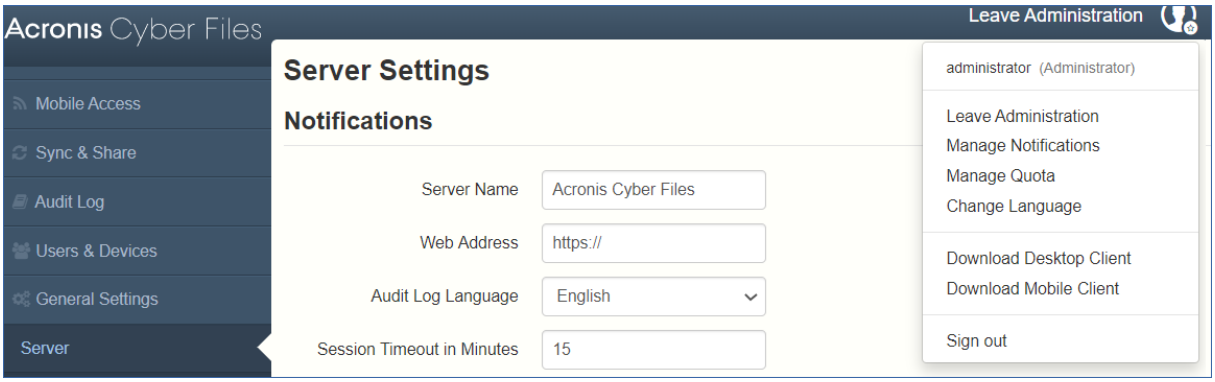
   Sie werden in einem neu angezeigten Bestätigungsfenster aufgefordert, alle Inhalte, die dem gelöschten Benutzer gehören, neu zuzuweisen.
4. Wählen Sie aus dem Listenfeld denjenige Benutzer aus, dem Sie die Inhalte zuweisen wollen.
5. Klicken Sie auf **Neu zuweisen**, um die Neuzuweisung zu bestätigen.
6. Überprüfen Sie die neu zugewiesenen Inhalte. Der neue Besitzer erhält einen Ordner in seinem Speicherbereich, der mit `Content inherited from DeletedUserName <deletedusersemail>` gekennzeichnet ist.

Server-Administration

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 Weboberfläche.

Administratoren und Berechtigungen

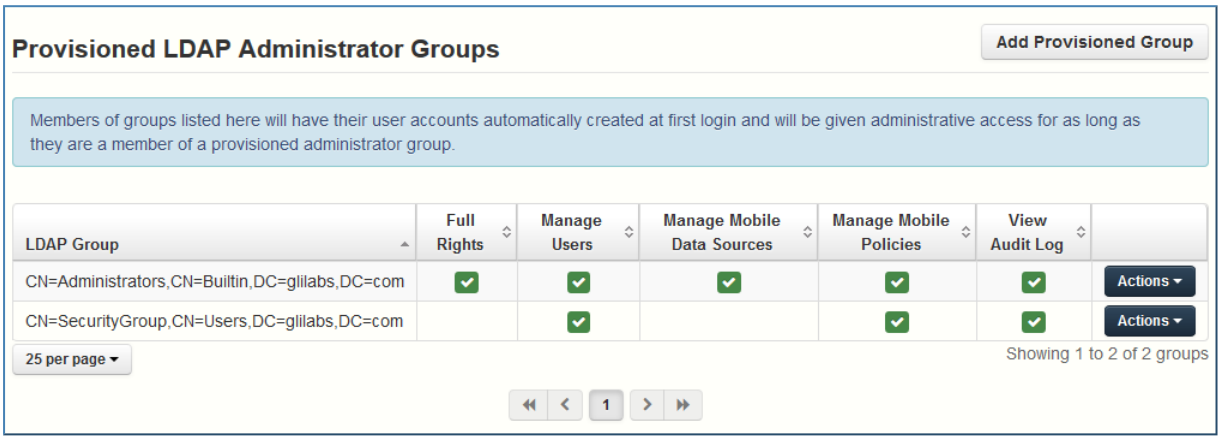
Zugriffsbeschränkungen für die Verwaltungsseite

- **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, die auf die **Administration**-Seite zugreifen dürfen. Es können kommaseparierte IPs, Subnetze oder IP-Bereiche sein (**z.B.**10.1.2.3, 10.4.*, 10.10.1.1-10.10.1.99).

Hinweis
Ein Administratorzugriff von 'localhost' aus kann nicht unterbunden werden.

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

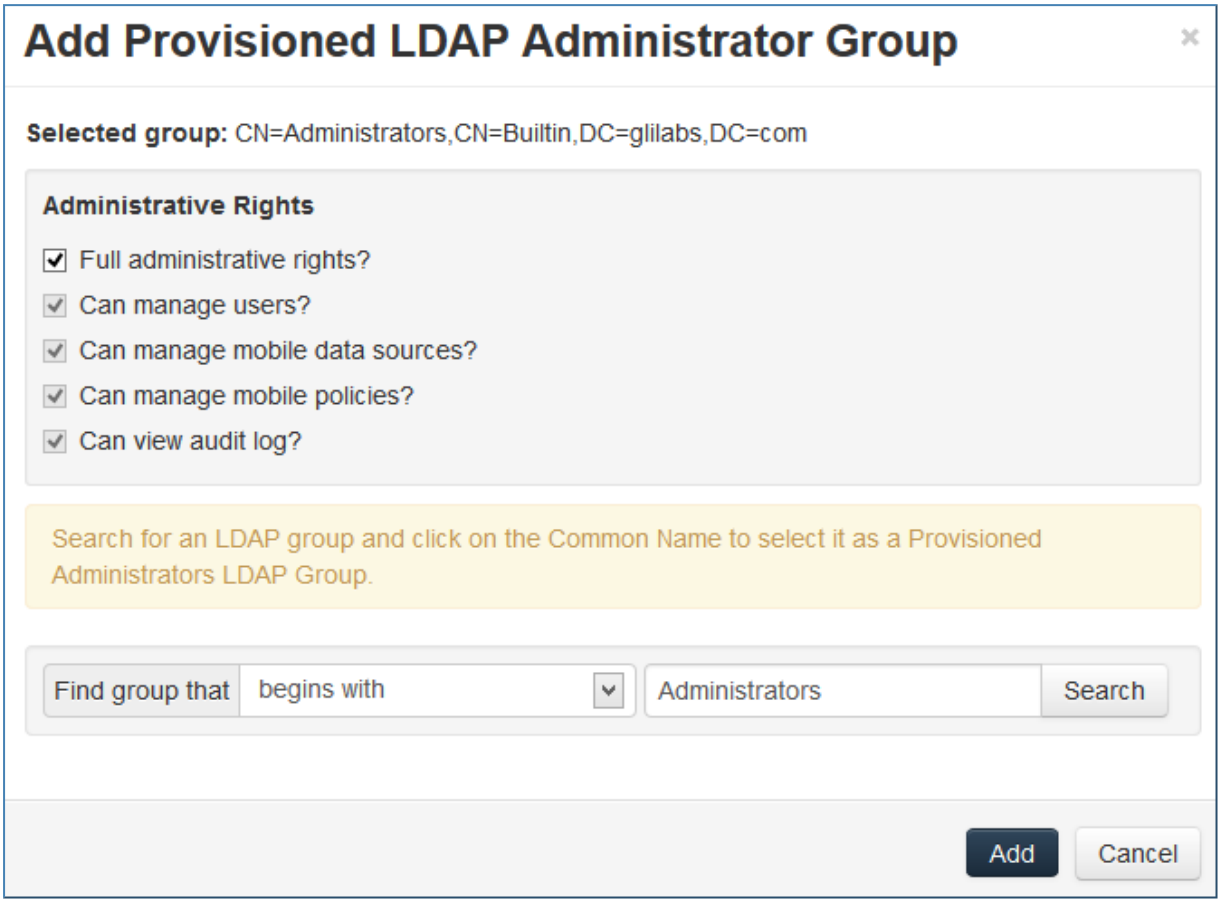
Bereitgestellte LDAP-Administrator-Gruppen



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

Administrative Benutzer

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

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

Einladen eines einzelnen Administrators

1. Öffnen Sie die Acronis Cyber Files-Weboberfläche.
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.
   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 administrative Rechte.
- **Kann Benutzer verwalten** – gewährt dem Benutzer das Recht, Benutzer zu verwalten. Hierzu gehören das Einladen neuer Benutzer, das Bereitstellen von LDAP-Gruppen, das Senden von Acronis Cyber Files-Registrierungseinladungen sowie das Verwalten der verbundenen mobilen Geräte.
- **Kann mobile Datenquellen verwalten** – Stattet den Benutzer mit dem Recht aus, mobile Datenquellen zu verwalten. Dazu gehört das Hinzufügen neuer Gateway Server und Datenquellen, das Verwalten der zugewiesenen Quellen, der auf den Clients sichtbaren Gateways und alter Datenquellen.
- **Kann Richtlinien für mobile Geräte verwalten** – Stattet den Benutzer mit dem Recht aus, Richtlinien für mobile Geräte zu verwalten. Dazu gehört das Verwalten von Benutzer- und Gruppenrichtlinien, zulässiger Apps und standardmäßiger Zugriffsbeschränkungen.
- **Kann Überwachungsprotokoll einsehen** – Stattet den Benutzer mit dem Recht aus, das Überwachungsprotokoll einzusehen.

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

So geben Sie Benutzern administrative Rechte:

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

So geben Sie Benutzern spezifische Rechte:

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

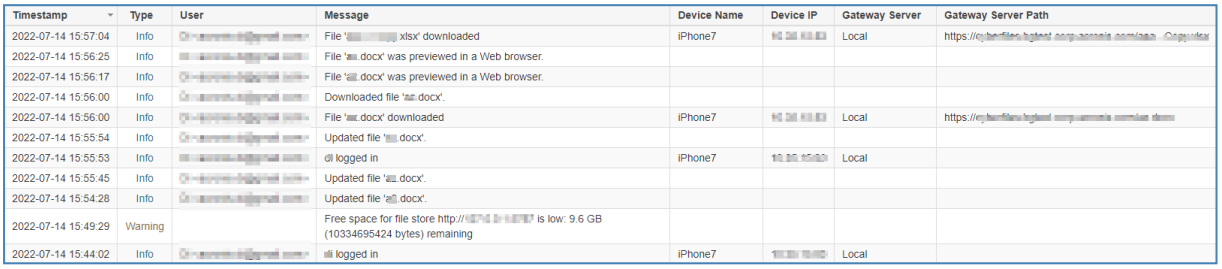
Überwachungsprotokoll

Protokoll

Hier können Sie Details zu den letzten Ereignissen (je nach Bereinigungsrichtlinie kann die Zeitbeschränkung unterschiedlich sein) einsehen, die einen Log-Eintrag generiert haben.

Hinweis
Wenn Sie die Protokollierung und die Protokollierungsebene für einen Gateway-Server konfigurieren möchten, rufen Sie Gateway-Server-Protokollierung auf.

Die Log-Liste



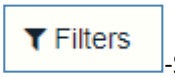
Timestamp	Type	User	Message	Device Name	Device IP	Gateway Server	Gateway Server Path
2022-07-14 15:57:04	Info		File '[redacted].xlsx' downloaded	iPhone7	[redacted]	Local	https://[redacted]
2022-07-14 15:56:25	Info		File '[redacted].docx' was previewed in a Web browser.				
2022-07-14 15:56:17	Info		File '[redacted].docx' was previewed in a Web browser.				
2022-07-14 15:56:00	Info		Downloaded file '[redacted].docx'.				
2022-07-14 15:56:00	Info		File '[redacted].docx' downloaded	iPhone7	[redacted]	Local	https://[redacted]
2022-07-14 15:55:54	Info		Updated file '[redacted].docx'.				
2022-07-14 15:55:53	Info		[redacted] logged in	iPhone7	[redacted]	Local	
2022-07-14 15:55:45	Info		Updated file '[redacted].docx'.				
2022-07-14 15:54:28	Info		Updated file '[redacted].docx'.				
2022-07-14 15:49:29	Warning		Free space for file store http://[redacted] is low: 9.6 GB (10334695424 bytes) remaining				
2022-07-14 15:44:02	Info		[redacted] logged in	iPhone7	[redacted]	Local	

- **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** – Zeigt die IP-Adresse des verbundenen Geräts an.
- **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.

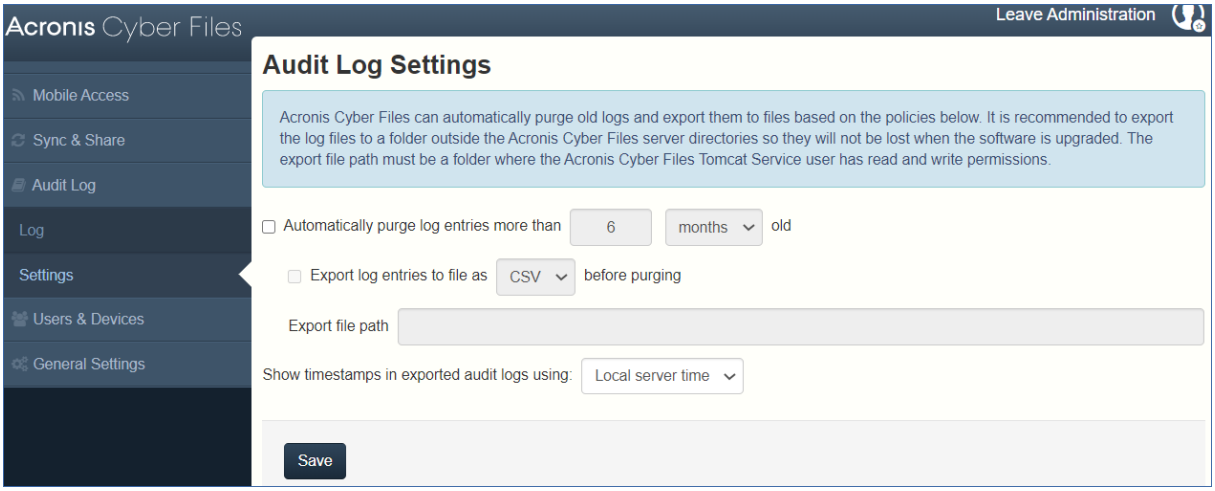
Filtern der Log-Liste

Sie können die Log-Einträge filtern, die in der Log-Tabelle angezeigt werden. Öffnen und schließen Sie die Filtereinstellungen durch das Anklicken des 

-Symbols oben auf der Seite.

- **Nach Benutzer filtern** – Sie können **Alle**, **Kein Benutzer** oder einen der verfügbaren Benutzer auswählen.
- **Nach freigegebenen Projekten filtern** – Sie können **Alle**, **Nicht freigegeben** oder eines der verfügbaren freigegebenen Projekte auswählen.
- **Nach Schweregrad filtern** – Verfügbare Typen sind **Alle**, **Info**, **Warnung**, **Fehler** und **Fatal**.
- **Nach Gateway Server filtern** – Sie können **Alle**, **Kein Server** oder einen Ihrer Gateway Server auswählen.
- **Nach Geräte-IP filtern** – Sie können **Alle**, **Keine Geräte-IP** oder eine der Geräte-IPs auswählen, die einen Protokoll-Eintrag generiert hat.
- **Von/Bis** – Filtert nach Datum und Uhrzeit.
- **Nach Text suchen** – Filtert nach dem Inhalt der Lognachrichten.
- **Nach Gerätenamen filtern** – Sie können **Alle**, **Kein Gerätename** oder einen der Gerätenamen auswählen, die einen Protokoll-Eintrag generiert haben.

Einstellungen



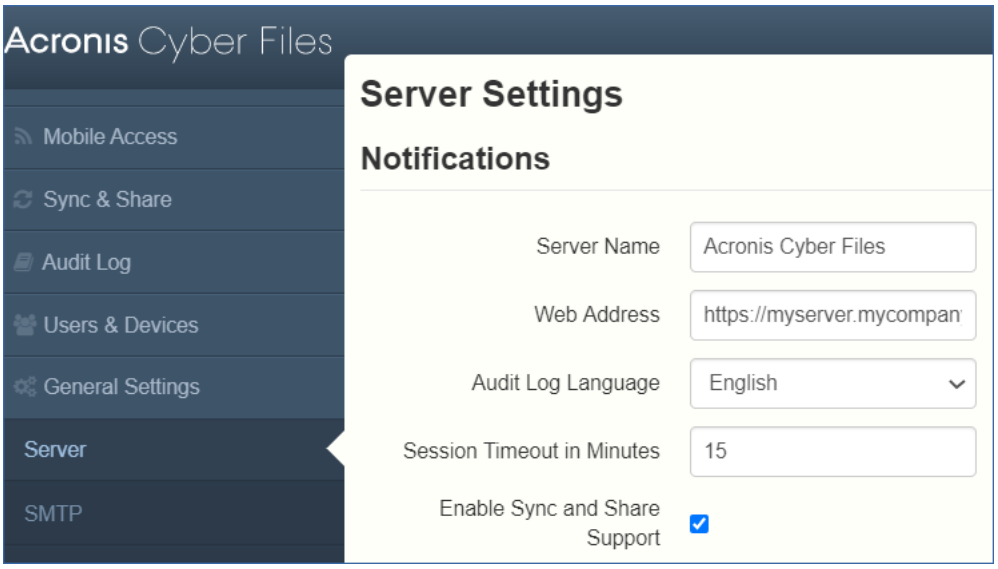
Acronis Cyber Files kann auf Basis bestimmter Richtlinien alte Protokolle bereinigen und diese als Dateien exportieren.

- **Protokolleinträge automatisch entfernen, die älter als X Y sind** – Wenn diese Option aktiviert ist, werden Protokolleinträge, die älter als eine bestimmte Anzahl von Tagen/Wochen/Monaten sind, automatisch entfernt.
  - **Protokolleinträge vor der Bereinigung als Datei im Format X exportieren** – Wenn aktiviert, wird eine Kopie der Protokolle vor dem Löschen in das angegebene Format (CSV, TXT oder XML) exportiert. Der Export wird automatisch für 03:00 Uhr (lokale Serverzeit) eingestellt. Diese Einstellung kann nicht geändert werden.
    - **Exportdateipfad** – Legt den Ordner fest, in dem exportierte Protokolle gespeichert werden.

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

- **Zeitstempel in exportierten Überwachungsprotokollen nach folgender Zeit anzeigen**: **X** – Damit können Sie wählen, ob Ihre Überwachungsprotokolle die lokale Server-Zeit oder ein anderes Zeitformat (UTC) verwenden sollen.

Server

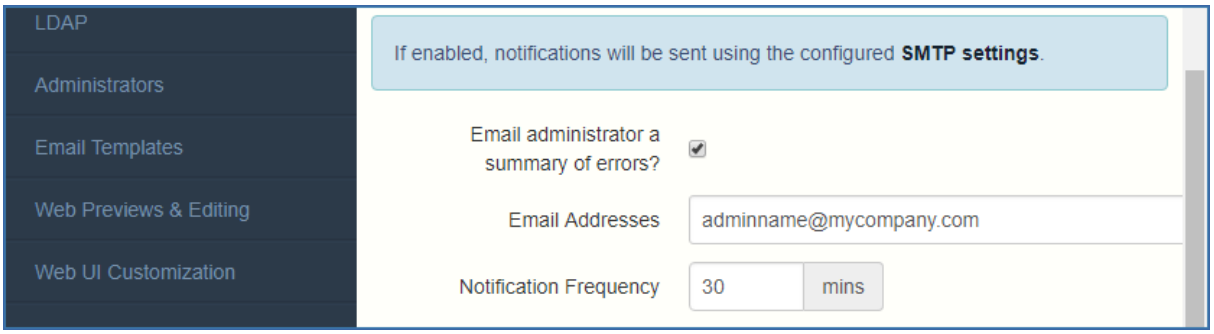


Server-Einstellungen

- **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

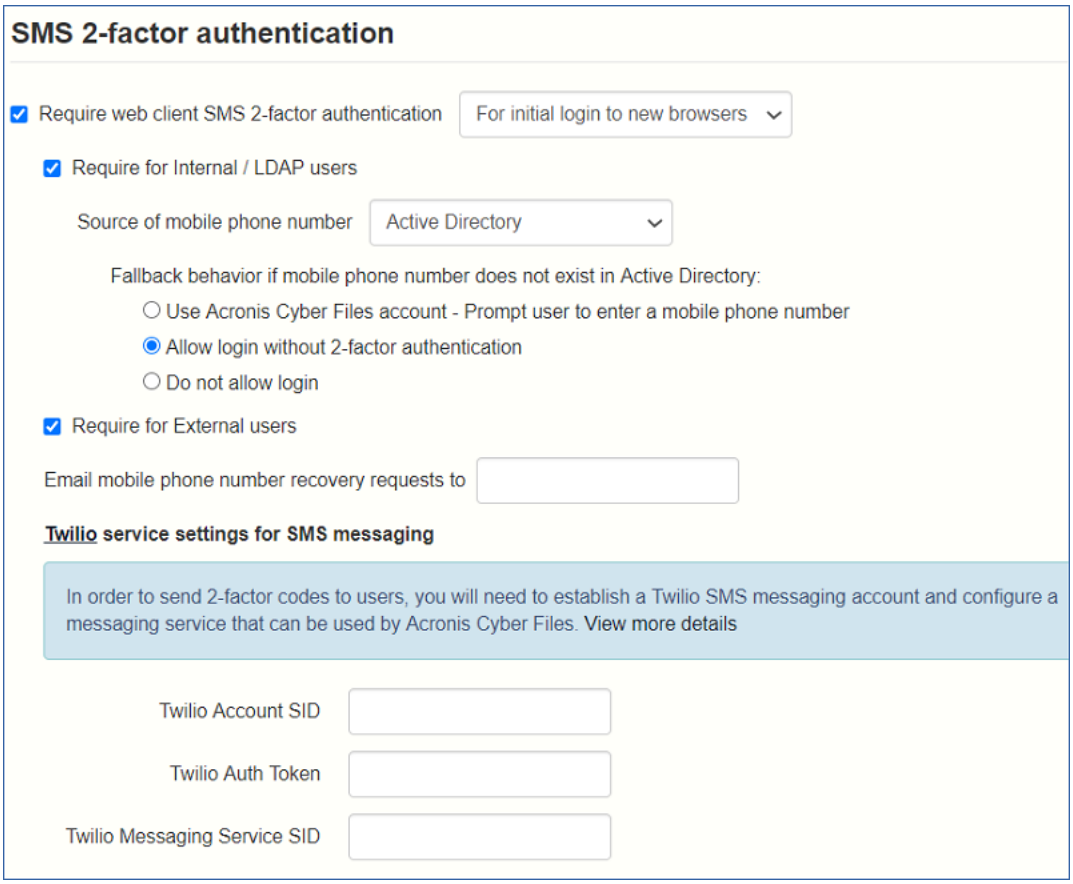
- **Dem Administrator eine Fehlerzusammenfassung per E-Mail senden?** – Wenn diese Option aktiviert ist, wird eine Fehlerzusammenfassung an die angegebenen E-Mail-Adressen gesendet.
  - **E-Mail-Adressen** – Eine oder mehrere E-Mail-Adressen, die eine Fehlerzusammenfassung erhalten.
  - **Benachrichtigungshäufigkeit**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

Zwei-Faktor-Authentifizierung per SMS

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 Acronis Cyber Files Server genutzt, sodass Sie nicht für jeden Benutzer ein Konto benötigen.



Hinweis
Mindestens eine der folgenden Optionen muss ausgewählt werden: **Für interne/LDAP-Benutzer verlangen** oder **Für externe Benutzer verlangen**.

Zwei-Faktor-Authentifizierung per SMS für Web-Client verlangen:

- **Für die erstmalige Anmeldung an neuen Browsern** – Erfordert eine SMS-Authentifizierung, wenn ein neuer Benutzer die Acronis Cyber Files Server-Webseite öffnet. Sobald Sie den Verifizierungscode eingegeben und Ihren Browser registriert haben, werden Sie nicht mehr aufgefordert, einen SMS-Code einzugeben, es sei denn, Sie verwenden einen anderen Browser oder Computer.
- **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.

Twilio-Einstellungen:

- **Twilio-Konto-SID** – Die Sicherheitskennung (SID) Ihres Unternehmens für Ihr Twilio-Konto.
- **Twilio-Authentifizierungs-Token** – Das Twilio-Authentifizierungs-Token Ihres Unternehmens. Beides finden Sie in der Twilio-Konsole auf https://www.twilio.com/console.

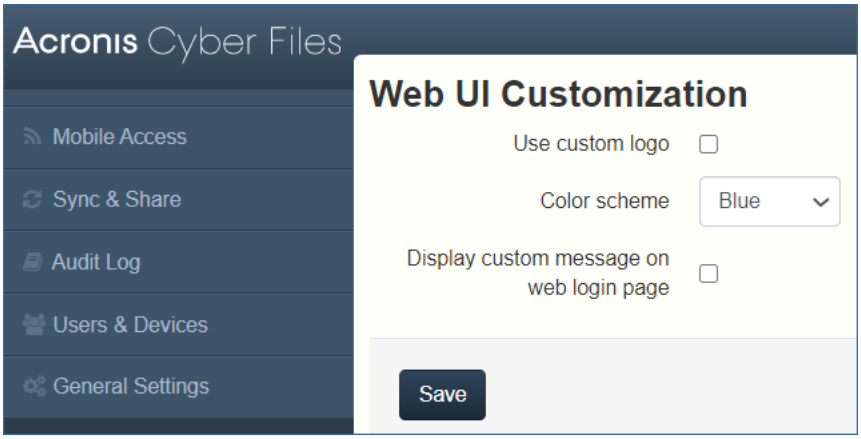
- **Twilio-Messaging-Dienst-SID** – Die SID Ihres Twilio Messaging-Dienstes für die Zwei-Faktor-Authentifizierung. Diese SID befindet sich unter https://www.twilio.com/console/sms/dashboard. Wenn Sie mehrere Twilio Messaging-Dienste haben, verwenden Sie nur die SID desjenigen, den Sie für die Zwei-Faktor-Authentifizierung verwenden. Wenn Sie einen Twilio Messaging-Dienst erstellen, lassen Sie das Feld **Anwendungsfall** leer oder wählen Sie 'Zwei-Faktor-Authentifizierung' aus.

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.

Web UI-Anpassung

Sie können die Logos und das Farbschema Ihres Acronis Cyber Files-Servers problemlos anpassen.

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



Verwenden benutzerdefinierter Logos

1. Öffnen Sie die Weboberfläche von AcronisCyber Files, 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. Klicken Sie auf **Speichern**.

Verwenden einer benutzerdefinierten Begrüßung

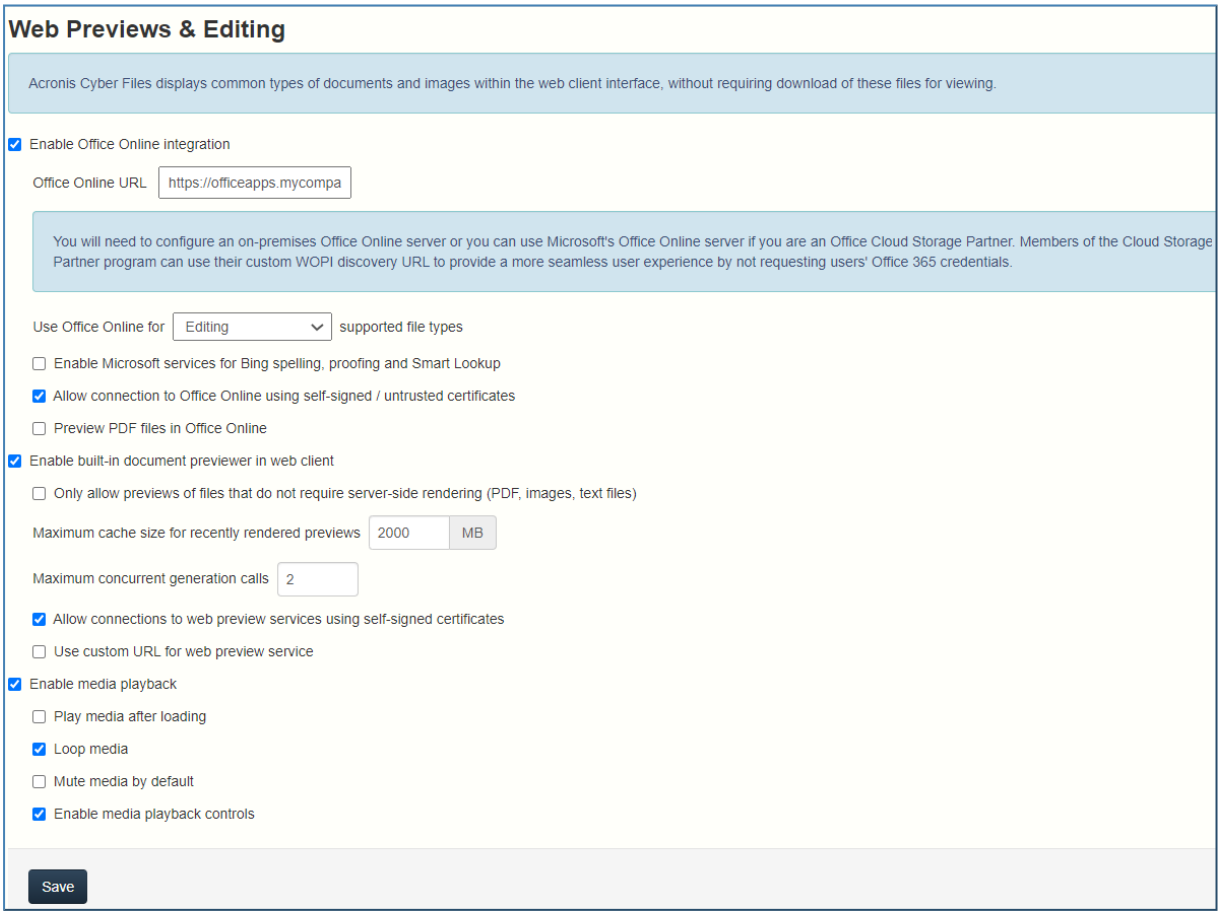
1. Öffnen Sie die Weboberfläche von AcronisCyber Files, und melden Sie sich als Administrator an.
2. Navigieren Sie zu **Allgemeine Einstellungen** -> **Web UI-Anpassung**.
3. Aktivieren Sie das Kontrollkästchen **Benutzerdefinierte Nachricht auf der Webanmeldeseite** anzeigen.
4. Geben Sie die gewünschte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

Verwenden von Farbschemas

1. Öffnen Sie die Weboberfläche von AcronisCyber Files, 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. Klicken Sie auf **Speichern**.

Webvorschau und Bearbeitung

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



- **Office Online-Integration aktivieren** – Aktiviert die integrierte Office Online-Funktionalität.
  - **Office Online-URL** – Geben Sie die WOPI-Such-URL Ihres Office Online ein. Bei lokalen Installationen von Acronis Cyber Files müssen Sie ein lokales Office Online-Setup verwenden, um diese URL bereitstellen zu können. Microsofts Office Online Cloud Service ist auf die Verwendung mit Service-Providern beschränkt und ohne spezielle Zertifizierung und Positivliste nicht öffentlich zugänglich.
  - **Office Online verwenden für** – **Bearbeiten** ermöglicht Ihnen, Microsoft Office-Dateien (**DOCX**, **PPTX**, **XSLX**) zu bearbeiten. Bei **Anzeigen und Bearbeiten** können Sie die genannten Dateien bearbeiten und zudem **DOC**-, **XLS**- und **PPT**-Dateien per Vorschau anzeigen lassen. Wenn diese Einstellung deaktiviert ist, werden alle Office- und PDF-Dateien über den internen Vorschaumodus (Previewer) von Acronis Cyber Files geöffnet.
  - **Microsoft-Dienste für Bing-Rechtschreibung, Korrektur und intelligente Suche aktivieren** – Verwendet die Dienste von Microsoft Bing zur Rechtschreibprüfung.
  - **Verbindungen zu Office Online mit selbstsignierten / nicht vertrauenswürdigen Zertifikaten erlauben** – Wenn diese Option aktiviert ist, können Benutzer auf Office Online-Server zugreifen, die nicht vertrauenswürdige Zertifikate verwenden.
  - **Vorschau von PDF-Dateien in Office Online** – Wenn diese Option aktiviert ist, können Benutzer entsprechende PDF-Dateien in Office Online per Vorschau einsehen, sofern die Option **Office Online verwenden für** mit der Einstellung **Anzeigen und Bearbeiten** festgelegt ist. Anderenfalls werden die PDF-Dateien über den internen Vorschaumodus von Acronis Cyber Files angezeigt.
- **Integrierte Dokumentenvorschau im Webclient aktivieren** – Aktiviert die entsprechende Webvorschau.

  Hinweis
  Für kennwortgeschützte Dateien sind keine Miniaturbilder und keine Vorschau vorhanden.

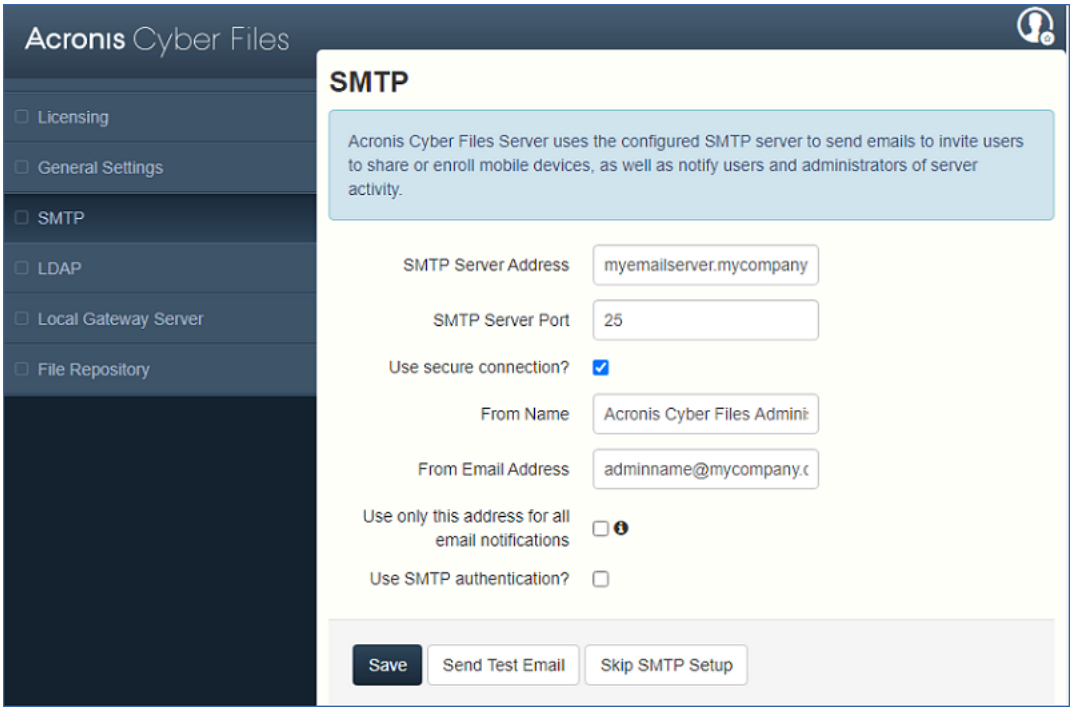
  - **Vorschau nur für solche Dateien erlauben, die kein serverseitiges Rendering erfordern (PDF, Bilder, Textdateien)** – Verringert die Belastung durch die Webvorschau, indem nur solche Dateien angezeigt werden, die kein zusätzliches Rendering erfordern. Bei diesen Dateien handelt es sich um PDFs, Bilder und einfache Textdateien.
  - **Maximale Cache-Größe für kürzlich gerenderte Dateivorschauen** – Legt eine maximale Größe für den Cache fest, der angelegt wird, wenn Sie eine Datei per Vorschau betrachten. Dadurch kann die Geschwindigkeit, mit der Dateien für eine Vorschau geöffnet werden, deutlich erhöht werden, wenn die Dateien erst kürzlich geöffnet wurden.
  - **Maximale Anzahl gleichzeitiger Generierungsaufrufe** – Legt die maximale Anzahl der gleichzeitigen Aufrufe für die Vorschau-Funktion fest.
  - **Verbindungen zu Webvorschau-Diensten mit selbstsignierten Zertifikaten erlauben** – Mit dieser Option können Sie Webvorschau-Dienste kontaktieren, die selbstsignierte Zertifikate verwenden. Das sind andere Acronis Cyber Files Tomcat-Dienste.

- **Benutzerdefinierte URL für Webvorschau-Dienst verwenden** – Aktivieren Sie diese Option, wenn Sie über mehrere Acronis Cyber Files Server verfügen und festlegen möchten, mit welchem Server die Webvorschau durchgeführt werden soll.

- **Medienwiedergabe aktivieren** – Mit dieser Option können Sie die Standardeinstellungen für die Medienwiedergabe steuern und eine Videovorschau in einem Browser ermöglichen, ohne dass Sie die gesamte Datei herunterladen müssen.
  - **Medien nach dem Laden abspielen** – Startet das Video automatisch, ohne dass Sie auf die **Wiedergabe**-Schaltfläche klicken müssen.
  - **Endlosschleife für Medien** – Das Video wird nach jedem Durchlauf automatisch wiederholt.
  - **Medien standardmäßig stummschalten** – Spezifiziert, ob der Ton zusammen mit dem Video abgespielt wird. Wenn diese Option aktiviert ist, wird das Video ohne Ton abgespielt.
  - **Medienwiedergabesteuerung aktivieren** – Ermöglicht die Verwendung von Schaltflächen, (**Wiedergabe/Pause**, **Lautstärke +/-** usw.), um die Video-Wiedergabe zu steuern.

SMTP

Acronis Der Cyber Files Server versendet E-Mails über den konfigurierten SMTP-Server, um Benutzer zu einer freigegebenen Ressource oder zur Registrierung von mobilen Geräten einzuladen oder Benutzer und Administratoren über Serveraktivitäten zu benachrichtigen.

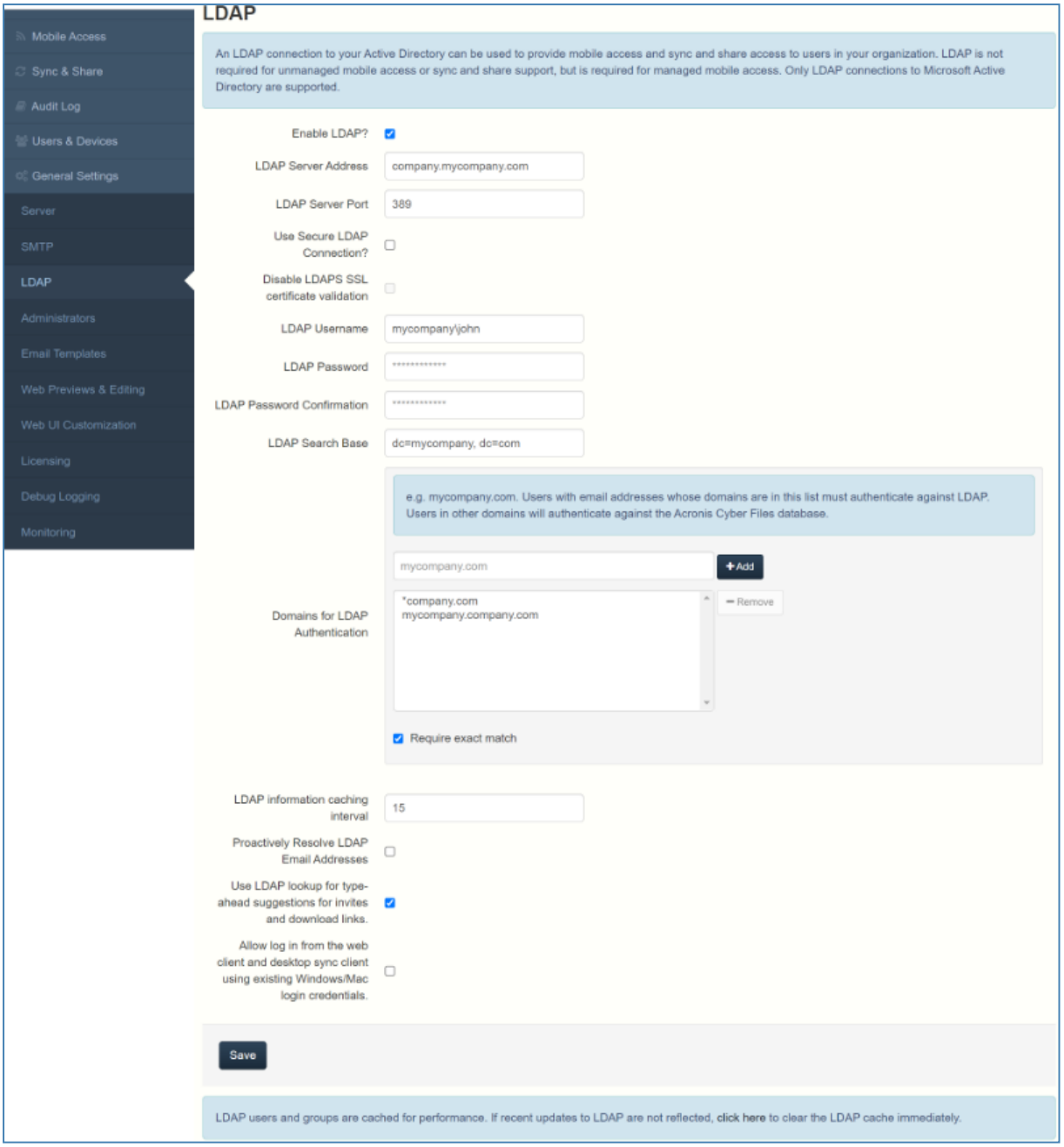


- **SMTP-Serveradresse** – Geben Sie den DNS-Namen des SMTP-Servers ein, über den E-Mail-Einladungen an Benutzer gesendet werden sollen.
- **SMTP-Serverport** – Geben Sie den SMTP-Serverport ein. Die Standardeinstellung ist Port 587.

- **Sichere Verbindung verwenden?** – Diese Einstellung ermöglicht eine sichere SSL-Verbindung zum SMTP-Server. Diese Einstellung 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.
- **Absender-E-Mail-Adresse** – Dies ist die E-Mail-Adresse, die in der 'Von'-Zeile von E-Mails angezeigt wird, die vom Server gesendet werden.
- **Nur diese Adresse für alle E-Mail-Benachrichtigungen verwenden** – Wenn diese Option aktiviert ist, sendet Acronis Cyber Files alle E-Mail-Benachrichtigungen ausschließlich von dieser E-Mail-Adresse.
- **SMTP-Authentifizierung verwenden?** – Aktivieren Sie diese Option, um eine Verbindung mit einem SMTP-Benutzernamen und -Kennwort herzustellen, oder deaktivieren Sie sie, um eine Verbindung ohne diese 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.

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?** – standardmäßig deaktiviert. Aktivieren Sie das Kontrollkästchen, um eine Verbindung mit dem Active Directory über eine sichere LDAP-Verbindung (auch als LDAPS bekannt) herzustellen.

  Hinweis
  Wenn Sie die Funktion für sichere LDAP-Verbindungen aktivieren, schreibt Acronis Cyber Files vor, dass der vollqualifizierte Domänenname des LDAP-Servers im Zertifikat entweder als allgemeiner Name (Common Name, CN) oder als alternativer Antragstellername (Subject Alternative Name, SAN) vorhanden sein muss.

- **LDAPS-SSL-Zertifikatsvalidierung deaktivieren –** aktivieren Sie dieses Kontrollkästchen, wenn Sie das LDAPS-Zertifikat nicht überprüfen wollen, wenn Sie sich mit einem LDAP-Server verbinden. Dies ist praktisch, wenn das LDAP-Server-Zertifikat nicht von einer öffentlichen Zertifizierungsstelle als vertrauenswürdig eingestuft wurde.
  Seit Version 8.7.0 ist diese Option bei Neuinstallationen standardmäßig deaktiviert (LDAPS-Zertifikate werden überprüft). Die Funktion ist jedoch nach dem Upgrade von älteren Versionen auf 8.7.0 aktiviert, und LDAPS-Zertifikate werden nicht überprüft. Bei Upgrades von Version 8.7.0 und höher wird die vorhandene Einstellung beibehalten.

  Hinweis
  Deaktivieren Sie diese Option nicht, wenn Sie nicht genau wissen, welche Art von Zertifikat Sie verwenden, oder wenn Ihre LDAPS-Zertifikate nicht von einer vertrauenswürdigen öffentlichen Zertifizierungsstelle stammen.

- **LDAP-Benutzername / -Kennwort** – diese Anmeldedaten werden für alle LDAP-Abfragen verwendet. Fragen Sie Ihren AD-Administrator, ob es spezielle Dienstkonten gibt, die verwendet werden sollen.
- **LDAP-Suchbasis** – geben Sie das Stammverzeichnis ein, von der aus die Suche nach Benutzern und Gruppen beginnen soll. Wenn Sie Ihre gesamte Domain durchsuchen wollen, geben Sie "dc=domainname, dc=domainsuffix" ein.
- **Domains für LDAP-Authentifizierung** – Benutzer mit E-Mail-Adressen, deren Domains in dieser kommaseparierten Liste enthalten sind, müssen sich über LDAP authentifizieren. Benutzer in anderen Domains authentifizieren sich über die Acronis Cyber Files-Datenbank.

  Hinweis
  Interne Domains werden nicht unterstützt. Es sind nur E-Mail-Domains mit öffentlichen Namen zulässig.

  - **Exakte Übereinstimmung erforderlich** - Wenn diese Option aktiviert ist, werden nur Benutzer aus den unter **Domains für LDAP-Authentifizierung** eingegebenen Domänen als LDAP-Benutzer behandelt. Benutzer, die Mitglieder anderer Domänen und Unterdomänen sind, werden als Ad-hoc-Benutzer behandelt.
- **Cache-Intervall für LDAP-Informationen** – legt das Intervall fest, in dem Acronis Cyber Files die Active Directory-Struktur per Cache zwischenspeichert.

- **LDAP-E-Mail-Adressen proaktiv auflösen** – Wenn diese Einstellung aktiviert ist, wird Acronis Cyber Files das Active Directory nach dem Benutzer mit der passenden E-Mail-Adresse durchsuchen, wenn dieser sich anmeldet oder zu Ereignissen eingeladen wird. Dadurch können sich Benutzer mit ihren E-Mail-Adressen anmelden und sofortiges Feedback zu Einladungen erhalten. Die Ausführung kann jedoch langsam sein, wenn der LDAP-Katalog sehr groß ist. Wenn Sie auf Authentifizierungs- oder Einladungsprobleme stoßen, deaktivieren Sie diese Einstellung.
- **LDAP-Lookup zur automatischen Vervollständigung von Einladungen und Download-Links verwenden –** Die Suchfunktion 'LDAP-Lookup zur automatischeb Vervollständigung' durchsucht das LDAP nach Benutzern mit übereinstimmenden E-Mail-Adressen. Diese Suche kann bei großen LDAP-Katalogen langsam sein. Wenn Sie Performance-Probleme mit der automatischen Vervollständigung feststellen, sollten Sie diese Einstellung deaktivieren.
- **Anmelden vom Webclient und Desktop Sync Client mit vorhandenen Windows-/Mac-Anmeldedaten erlauben.** Ermöglicht es allen gültigen LDAP-Benutzern, sich an der Weboberfläche und am Desktop-Client anzumelden, ohne ihre Anmeldedaten eingeben zu müssen. Siehe Konfigurieren von Single-Sign-on.

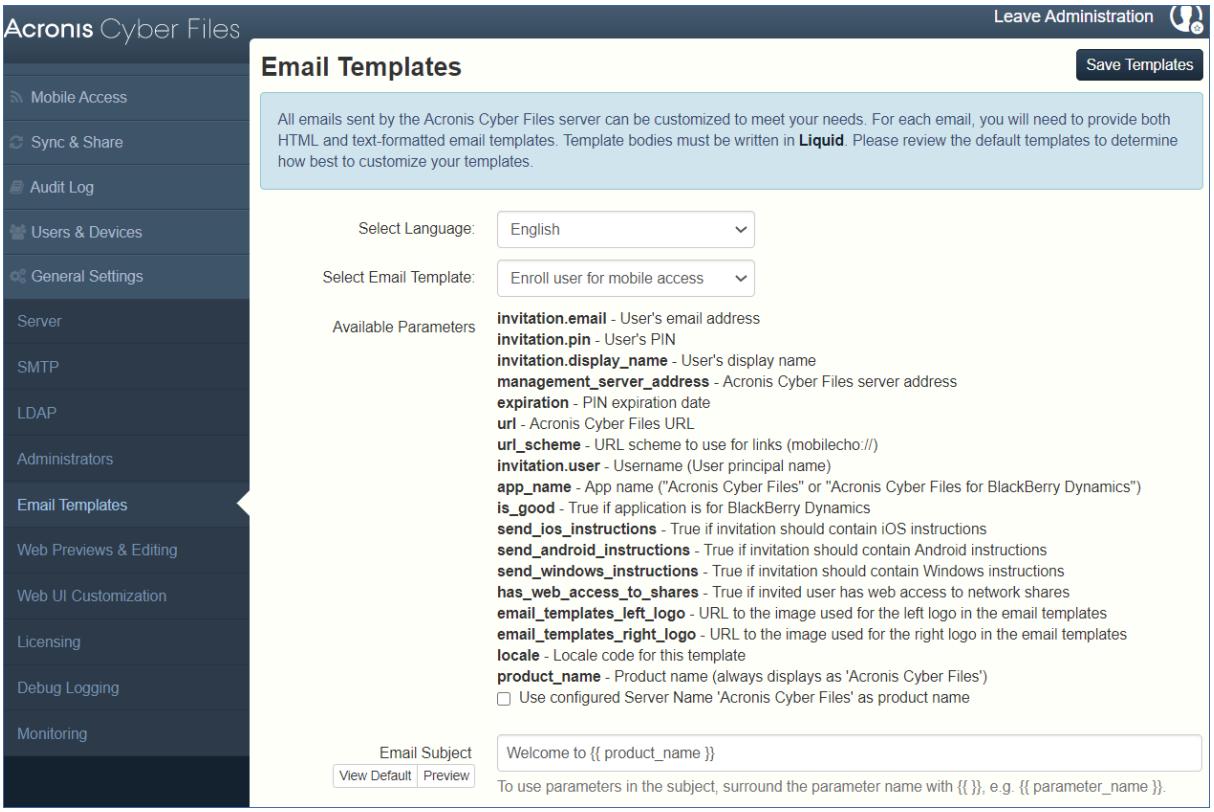
Löschen des LDAP Caches

Alle aktuellen LDAP-Änderungen werden an den LDAP-Server weitergeleitet. Bei der Aktualisierung des LDAP-Caches im Speicher gibt es jedoch eine kurze Verzögerung. Klicken Sie auf die Nachrichtenleiste unten auf der Seite, um den LDAP-Cache zu löschen. LDAP-Änderungen werden umgehend durchgeführt.

E-Mail-Vorlagen

Acronis Cyber Files 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 Cyber Files-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 Acronis Access 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 den E-Mail-Vorlagen verwenden, sollten diese Bilder gehostet werden und unter einem bestimmten Speicherort im Internet verfügbar sein.

- **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 Cyber Files aktualisieren. Wenn Sie diese Updates von Acronis nutzen möchten, 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.
  Wenn Sie auf **Vorschau** klicken, sehen Sie eine Vorschau für Ihre aktuelle Vorlage.
- **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 **Standard anzeigen** klicken, wird die Standardvorlage angezeigt.

Lizenzierung

Eine Liste aller Lizenzen wird angezeigt.

- **Lizenz** – Der Typ der Lizenz (Test, Abonnement usw.).
- **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 die Lizenzen dieselbe eindeutige ID verwenden, wird die Anzahl der zulässigen Benutzer addiert.

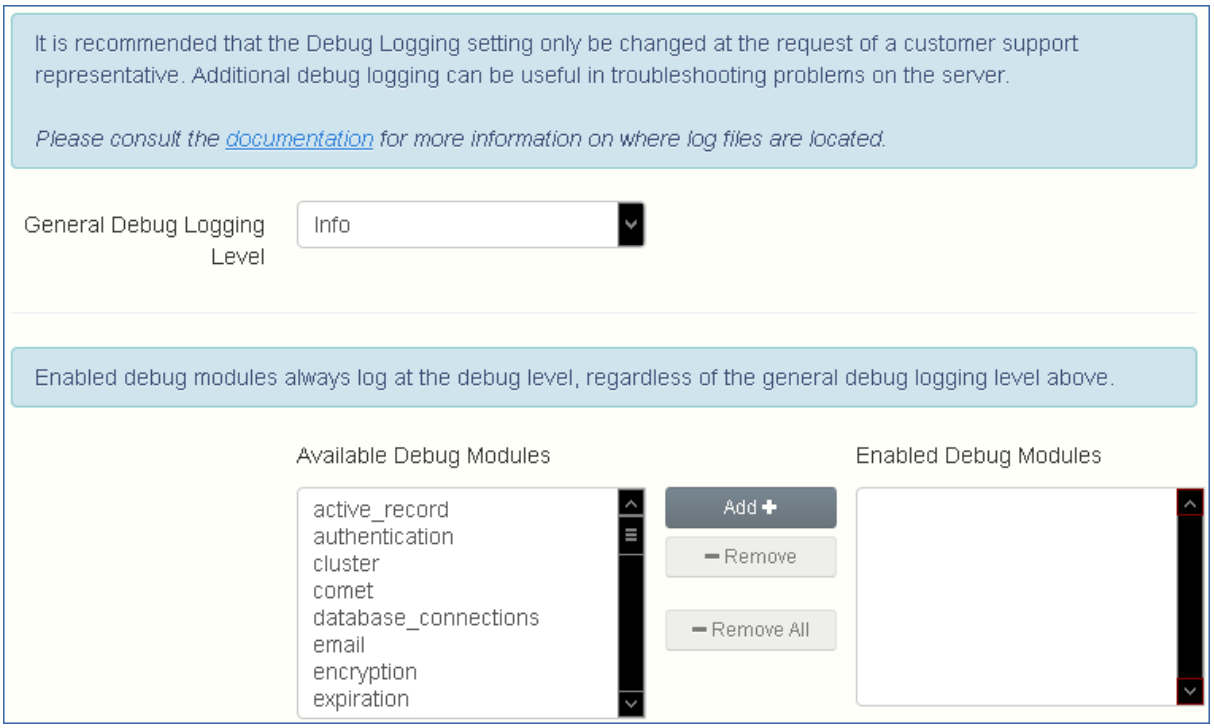
Das Hinzufügen einer neuen Lizenz für einen Gateway-Server ist nicht erforderlich

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

Debug-Protokollierung

Über die Einstellungen auf dieser Seite können erweiterte Protokollierungsinformationen aktiviert werden, die bei der Konfiguration und Fehlerbehebung von Acronis Cyber Files 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.



Ab Version 7.0 des Acronis Cyber Files-Servers wurde das Modul **Ausnahmen** aus der Liste der verfügbaren Module entfernt und wird immer standardmäßig aktiviert. Benutzer, die ein Upgrade aus einer Vorgängerversion von Acronis Cyber Files 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 während des normalen Betriebs und unter 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.

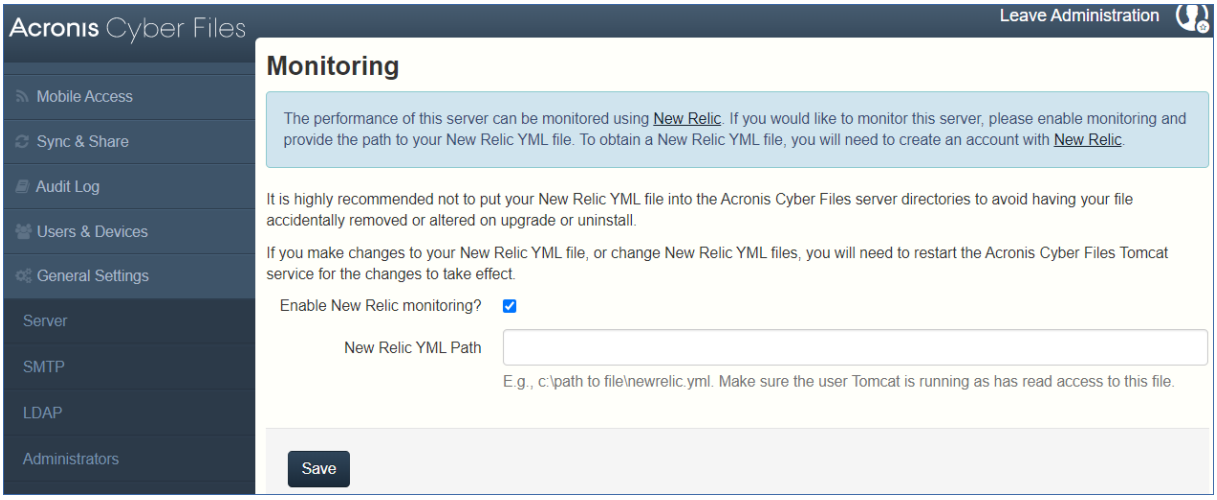
Hinweis
Wenn es sich bei dem Produkt um eine Aktualisierung und nicht um eine Neuinstallation handelt, befinden sich die Protokolldateien unter `C:\Program Files (x86)\Group Logic\Common\apache-tomcat-7.0.42\logs`.

Hinweis

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

Überwachen

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 'New Relic YML'-Datei nicht in den Verzeichnissen des Acronis Cyber Files-Servers abzulegen, um 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 Acronis Cyber Files Tomcat 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.

Installieren von New Relic Überwachen von Acronis Cyber Files mit New Relic

Überwachen von Acronis Cyber Files mit New Relic

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

1. Öffnen Sie 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 AcronisCyber Files.
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 AcronisCyber Files, 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 Acronis Cyber Files Tomcat neu, und warten Sie einige Minuten. Die Schaltfläche sollte dann aktiv sein.
10. Sie sollten den Acronis Cyber Files-Server auf der New Relic-Website überwachen können.

Hinweis
Alle Informationen, die der Acronis Cyber Files Server über den Verbindungsversuch zu New Relic und die Konfiguration des Monitorings protokolliert, sind in einer Datei namens **newrelic_agent.log** zu finden, die sich in diesem Verzeichnis befindet: `C:\Program Files (x86)\Acronis\Common\apache-tomcat-7.0.34\logs`. Bei Problemen können Sie in dieser Protokolldatei nach Informationen suchen.

Hinweis
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. Das ist ein harmloser Nebeneffekt des Codes, der zum Beheben eines anderen New-Relic-Fehlers verwendet wurde.

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

1. Öffnen Sie 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.

Wartungsaufgaben

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

Richtlinien für Desaster-Recovery

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

Einführung:

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

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

Beschreibung der Elemente von Acronis Cyber Files:

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

Acronis Cyber Files Gateway-Server

Hinweis
Der Standardspeicherort lautet: `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Gateway Server`.

Acronis Cyber Files Server

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

Acronis Cyber Files Konfigurationswerkzeug

Hinweis
Der Standardspeicherort lautet: `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Configuration Utility`

Dateispeicher

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

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

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

Alle diese Komponenten werden benötigt, um eine funktionsfähige Instanz von Acronis Cyber Files zu bilden.

Zum Implementieren eines schnellen Wiederherstellungsprozesses benötigte Ressourcen

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

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

Der Prozess

Backup-Setup

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

1. Stellen Sie eine Installation von Acronis Cyber Files einschließlich aller Elemente auf dem sekundären Wiederherstellungsknoten bereit. Wenn dies nicht möglich ist, ist eine vollständige Sicherungskopie bzw. ein Image des Quellgeräts eine angemessene Alternative. In virtualisierten Umgebungen sind periodische Snapshots eine wirksame und kostengünstige Alternative.
2. Legen Sie regelmäßig Backups der Acronis Cyber Files-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 FileStore 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-FileStore gesichert werden.
4. Legen Sie so oft wie möglich Backups der Acronis Cyber Files-Datenbank an. Dies erfolgt durch ein automatisiertes Datenbank-Dump-Skript, das vom Windows Task Scheduler ausgelöst wird. Der Datenbank-Dump sollte anschließend mit einem standardmäßigen Backup-Tool gesichert werden.

Wiederherstellung

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

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

Optimale Vorgehensweisen

1. Regelmäßige Backups der Datenbank erstellen

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

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

Einrichtungen mit Datenbanken von Gigabyte-Größe können einige zusätzliche Konfigurationen während des **Backup&Restore**-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/de-de/mobilitysupport/.

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

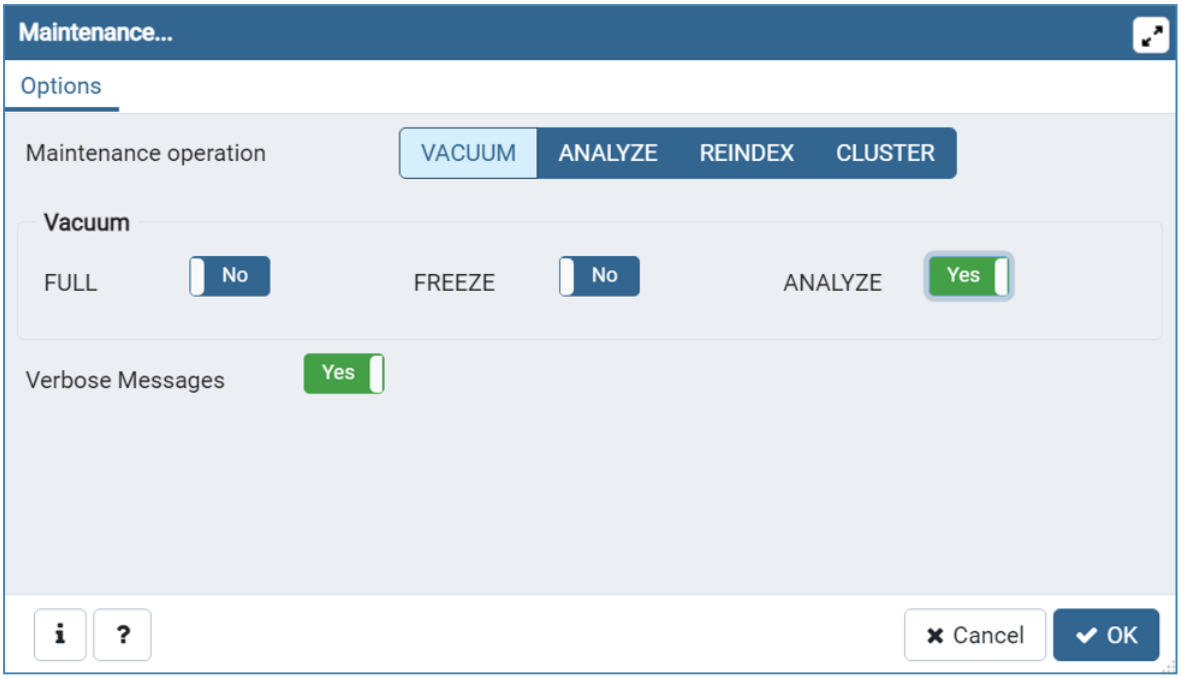
PostgreSQL-Datenbanken erfordern regelmäßige Wartung, bekannt als `vacuuming`. Der **VACUUM**-Befehl muss regelmäßig für jede Tabelle durchgeführt werden, um:

- 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 PostgreSQL Administrator-Tool von Acronis Cyber Files. Es befindet sich im Startmenü, im Acronis Cyber Files-Ordner. Doppelklicken Sie auf **localhost**, um eine Verbindung zum Server herzustellen.
2. Klicken Sie mit der rechten Maustaste auf die Datenbank `acronisaccess_production` und wählen Sie **Wartung**.
3. Wählen Sie **BEREINIGEN** und legen Sie **ANALYSIEREN** mit 'Ja' fest.



Warnung!
Das Vakuum kann eine Weile andauern. Führen Sie dieses Verfahren durch, wenn die Serverauslastung niedrig ist.

4. Klicken Sie auf **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

3. Bei großen Bereitstellungen sollten Sie die Ausführung einer Einrichtung mit Lastenausgleich oder eines Clustering-Gateway-Servers erwägen.

Sichern und Wiederherstellen von Acronis Cyber Files

Dies ist erforderlich, wenn Sie ein Upgrade, Update oder eine Wartung des Acronis Cyber Files-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 Ihre Acronis Cyber Files-Server-Datenbank 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://support.acronis.com/mobility zur Verfügung.

Hinweis
In einem Microsoft Failover Cluster 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.

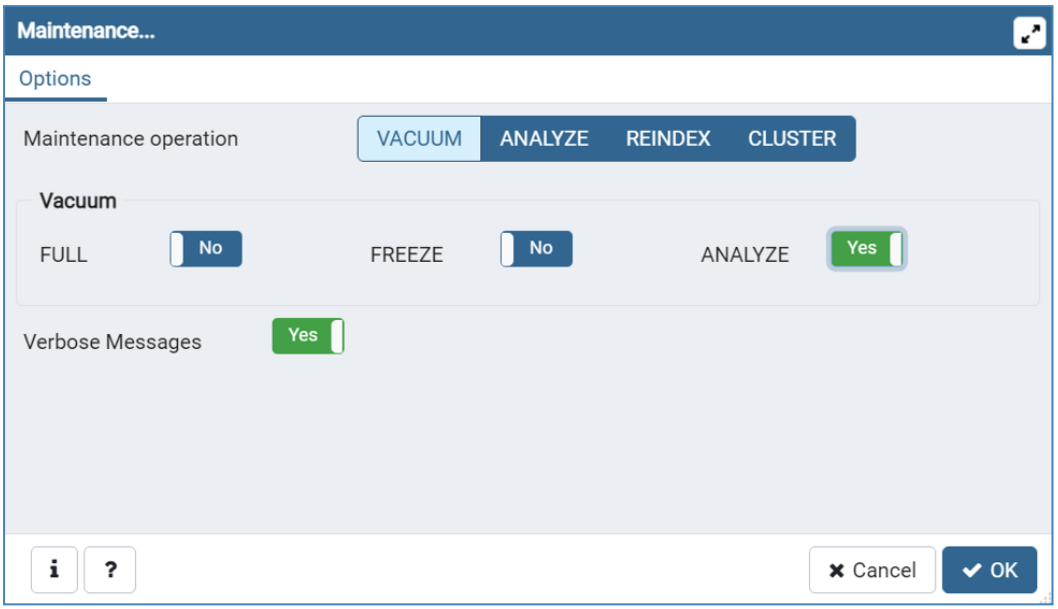
Sichern der Cyber Files-Datenbank

1. Stoppen Sie Acronis Cyber Files Tomcat.

   Hinweis
   Wenn Sie einen Lastenausgleich für mehrere Acronis Cyber Files Tomcat-Dienste vornehmen, stoppen Sie alle.

2. Öffnen Sie das PostgreSQL Administrator-Tool von Acronis Cyber Files. Sie finden es im Startmenü von Windows im Ordner von Acronis Cyber Files. 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 **Maintenance**.

5. Wählen Sie **BEREINIGEN** und legen Sie **ANALYSIEREN** mit 'Ja' fest.



6. Drücken Sie **OK**.
7. 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.
8. Schließen Sie PostgreSQL Administrator, und öffnen Sie eine Eingabeaufforderung mit erweiterten Benutzerrechten.
9. Navigieren Sie in der Eingabeaufforderung zum PostgreSQL-Verzeichnis 'bin', **z.B.**`cd "C:\Program Files(x86)\Acronis\Acronis Cyber Files\Common\PostgreSQL\<version>\bin"`.

   Hinweis
   Sie müssen den Pfad so bearbeiten, dass er auf den PostgreSQL-Ordner 'bin' verweist, wenn Sie eine ältere oder eine benutzerdefinierte Installation verwenden (z.B. `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\PostgreSQL\9.4\bin\`).

10. Geben Sie den folgenden Befehl ein: `pg_dumpall --host localhost --port 5432 --username postgres --file alldbs.sql`.
    - `alldbs.sql` ist der Dateiname des Backups. Dieses wird im PostgreSQL-Bin-Verzeichnis gespeichert. Sie können einen Pfad im obigen Befehl verwenden, wenn Sie das Backup an einem anderen Ort speichern wollen. Ändern Sie dazu folgendermaßen den letzten Teil des oberen Befehls: `--file D:\Backups\alldbs.sql`
    - Wenn Sie nicht den Standard-Port verwenden, müssen Sie statt `5432` die richtige Portnummer eingeben.
    - Wenn Sie nicht das standardmäßige PSQL-Administratorkonto `postgres` verwenden, muss `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 Fenster mit der Eingabeaufforderung.

11. Kopieren Sie die Backup-Datei an einen sicheren Speicherort.
12. Gehen Sie zu einem sicheren Speicherort und kopieren Sie dorthin die Datei `postgresql.conf`, da diese wichtige Einstellungen enthalten kann. Sie befindet sich im PostgreSQL-Datenordner – der standardmäßig unter `C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL\<version>\Data` liegt.

Sichern der Gateway Server-Datenbank

1. Stoppen Sie den Acronis Cyber Files 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.

Weitere Dateien, von denen ein Backup erstellt werden muss

Wenn Sie Änderungen an den nachfolgenden Dateien vorgenommen haben, wird empfohlen, Backups zu erstellen, damit Sie Ihre Einstellungen beim Wiederherstellen oder Migrieren des Acronis Cyber Files-Produkts 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\Acronis Cyber Files\Common\PostgreSQL\<Version>\Data`.

- `web.xml` standardmäßig hier: `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Access Server\Web Application\WEB-INF\`. Enthält Einstellungen für Single Sign-On.
- `server.xml`-Standardspeicherort: `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\apache-tomcat-<Version>\conf`. Enthält Einstellungen für Tomcat.
- `krb5.conf`-Standardspeicherort: `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\apache-tomcat-<Version>\conf`. Enthält Einstellungen für Single Sign-On.
- `login.conf`-Standardspeicherort: `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\apache-tomcat-<Version>\conf`.
- Ihre für Acronis Cyber Files verwendeten Zertifikate und Schlüssel.
- `acronisaccess.cfg`-Standardspeicherort: `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Access Server`.

- Standardspeicherort für benutzerdefinierte Farbschemas: `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Access Server\Web Application\customizations\`.
- `pg_hba.conf`-Standardspeicherort: `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\PostgreSQL\<Version>\Data`.
- Datei `newrelic.yml`, wenn Sie **New Relic** zum Überwachen Ihres Acronis Cyber Files-Servers verwenden.

Wiederherstellen der Cyber Files-Datenbank

1. Öffnen Sie die Systemsteuerung **Dienste**, und stoppen Sie Acronis Cyber Files Tomcat Service.

   Hinweis
   Stoppen Sie für Lastenausgleichskonfigurationen alle Acronis Cyber Files Tomcat Service.

2. Öffnen Sie die PostgreSQL Administrator-Anwendung von Acronis Cyber Files, 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 PostgreSQL Administrator, und öffnen Sie eine Eingabeaufforderung mit erweiterten Benutzerrechten.
6. Navigieren Sie in der Eingabeaufforderung zum PostgreSQL-Verzeichnis 'bin'.
   Beispiel:`cd "C:\Program Files\Acronis\Acronis Cyber Files\Common\PostgreSQL\<version>\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 das `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 erneut die PostgreSQL Administrator-Applikation von Acronis Cyber Files, und stellen Sie eine Verbindung zum lokalen Datenbankserver her.
12. Wählen Sie **Datenbanken** aus.

13. Erweitern Sie die Datenbank `acronisaccess_production`, erweitern Sie **Schemas**, und erweitern Sie **Öffentlich**. Überprüfen Sie, ob die Anzahl der **Tabellen** mit der in Schritt 5 des Abschnitts „Sichern der AcronisCyber Files-Datenbank“ übereinstimmt.

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

Wiederherstellen der Gateway Server-Datenbank

1. Stoppen Sie den Acronis Cyber Files Gateway-Dienst.
2. Kopieren Sie das Datenbank-Backup `mobliEcho.sqlite3` des Gateway Server in den Datenbankordner des neuen Gateway Server (standardmäßig `C:\Program Files (x86)\Acronis\Files Advanced\Gateway Server\database`), und ersetzen Sie die vorhandene Datei.
3. Wiederholen Sie dieses Verfahren für alle Gateway Server.

Wiederherstellen zusätzlicher Dateien und Anpassungen

Stellen Sie sicher, dass sämtliche an den Acronis Cyber Files-Konfigurationsdateien (web.xml, server.xml, krb5.conf, Zertifikate, benutzerdefinierte Farbschemas, E-Mail-Vorlagen, pg_hba.conf oder newrelic.yml) vorgenommenen Anpassungen kopiert werden, und verschieben Sie diese in die neuen Dateien.

Testen des wiederhergestellten Cyber Files Server

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

Onlineschalten herkömmlicher Bereitstellungen

1. Starten Sie das Konfigurationsprogramm von Acronis Cyber Files, und vergewissern Sie sich, dass alle Einstellungen dort korrekt sind.
2. Wählen Sie 'OK', um alle Dienste zu starten.
3. Alle Dienste werden gleichzeitig online geschaltet und alle Funktionen von Acronis Cyber Files 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 Acronis Cyber Files Tomcat-Dienst fehlerfrei startet.

Onlineschalten von Bereitstellungen mit Lastenausgleich

1. Wählen Sie, welcher der Server von Acronis Cyber Files 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 Acronis Cyber Files Server beeinflusst.
3. Greifen Sie auf den Computer mit dem Primärserver von Acronis Cyber Files zu, und starten Sie das Konfigurationsdienstprogramm von Acronis Cyber Files.
4. Stellen Sie sicher, dass dort alle Einstellungen korrekt sind. Wenn keine Probleme vorliegen, drücken Sie OK, um alle Dienste zu starten.
5. Öffnen Sie die Webkonsole von Acronis Cyber Files, 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 Acronis Cyber Files-Komponente zu, und starten Sie diese über das Konfigurationsdienstprogramm.

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\Acronis Cyber Files\Common\apache-tomcat-7.0.34\logs`
Acronis Cyber Files speichert seine eigenen Logs im selben Verzeichnis als separate Dateien.

Hinweis
Acronis Die Logdateien von Cyber Files 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.

Hinweis
Informationen zu ForFiles einschließlich Befehlssyntax und Beispielen finden Sie unter 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.

Hinweis
Das Beispielskript (Batchdatei) funktioniert unter Windows Server 2008. Klicken Sie hier, um dieses Skript herunterzuladen.
Optional können Sie das Skript auch kopieren, in ein leeres Textdokument einfügen und unter 'AASTomcatLogPurge.bat' speichern.

Vollständiger Code des Batch-Skripts:

```
ECHO OFF

REM-Skript: aETomcatLogsPurge.bat

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

ECHO Dieses Skript löscht Dateien aus einem Verzeichnis, die älter als eine bestimmte Anzahl von Tagen sind

ECHO Sie können das Skript per Befehlszeile oder über einen Scheduler ausführen

ECHO Vergewissern Sie sich, dass der Prozess berechtigt ist, Dateien im Zielordner zu löschen

REM ===== KONFIGURATIONEN ==================================================

REM Note: Alle Pfade, die Leerzeichen enthalten, müssen in doppelte Anführungszeichen gesetzt werden

REM Bearbeiten Sie diese Datei und legen Sie LogPath und NumDays unten fest

REM Pfad zu dem Ordner, in dem alle Tomcat-Protokolle gespeichert sind

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

REM NumDays - Protokolldateien, die älter als 'NumDays' sind, werden verarbeitet

set NumDays=14

REM ===== KONFIGURATIONSENDE ======================

ECHO

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

REM ForFiles-Optionen:

REM "/p": der Pfad, wo Sie Dateien löschen wollen.

REM "/s": rekursiv in andere Unterordner schauen, die sich in dem Ordner befinden, der im Pfad der Batch-Datei angegeben ist

REM "/d": Tage zum Löschen von Dateien, die älter als das aktuelle Datum sind. Beispielsweise bedeutet "/d -7", dass Dateien gelöscht werden, die älter als 7 Tage sind.
```

```
REM "/c": Ausführungsbefehl, um die Dateien tatsächlich zu löschen: "cmd /c del @file".

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

:End

ECHO ===== BATCH-DATEI ABGESCHLOSSEN ========================================
```

Warnung!

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

Schritte

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

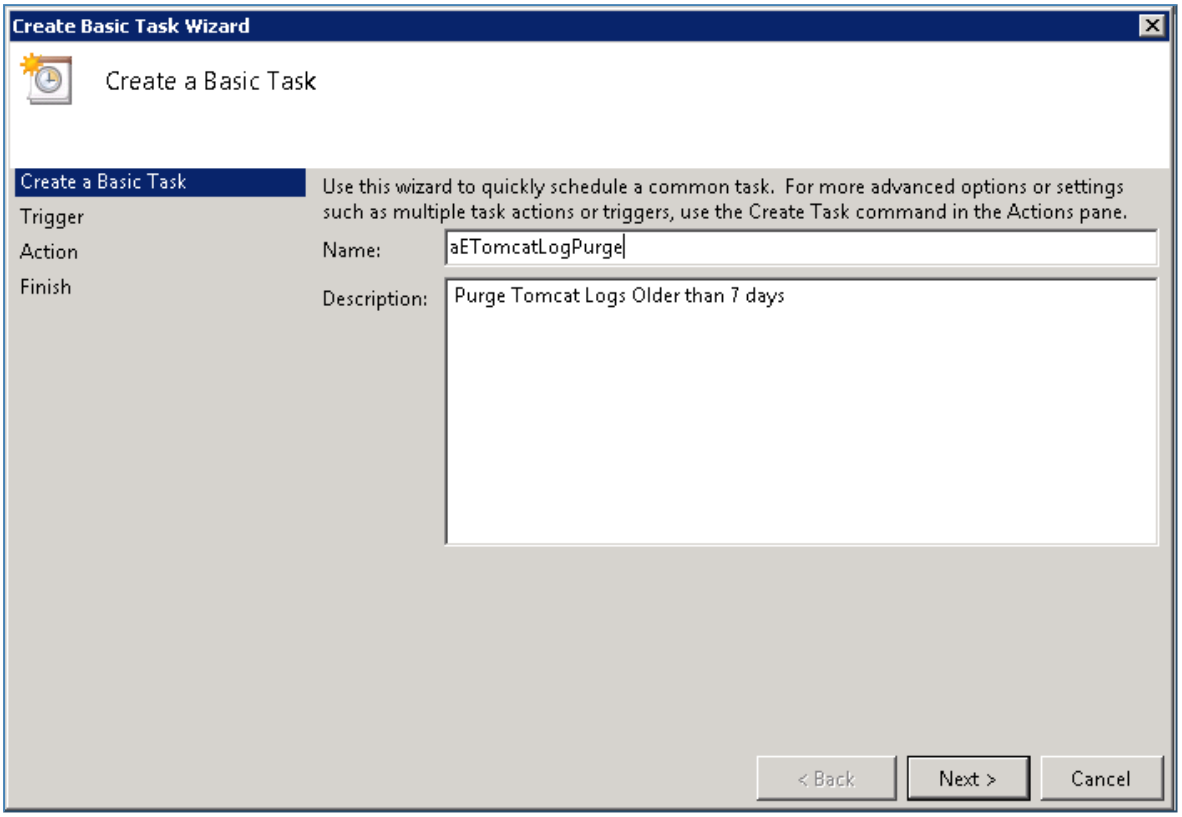
```
REM ===== CONFIGURATIONS ===================================================
REM Note: all paths containing spaces must be enclosed in double quotes
 REM Edit this file and set LogPath and NumDays below
REM Path to the folder where all Tomcat logs are
 set LogPath="C:\Program Files (x86)\Group Logic\Common\apache-tomcat-7.0.34\logs"

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

Hinweis

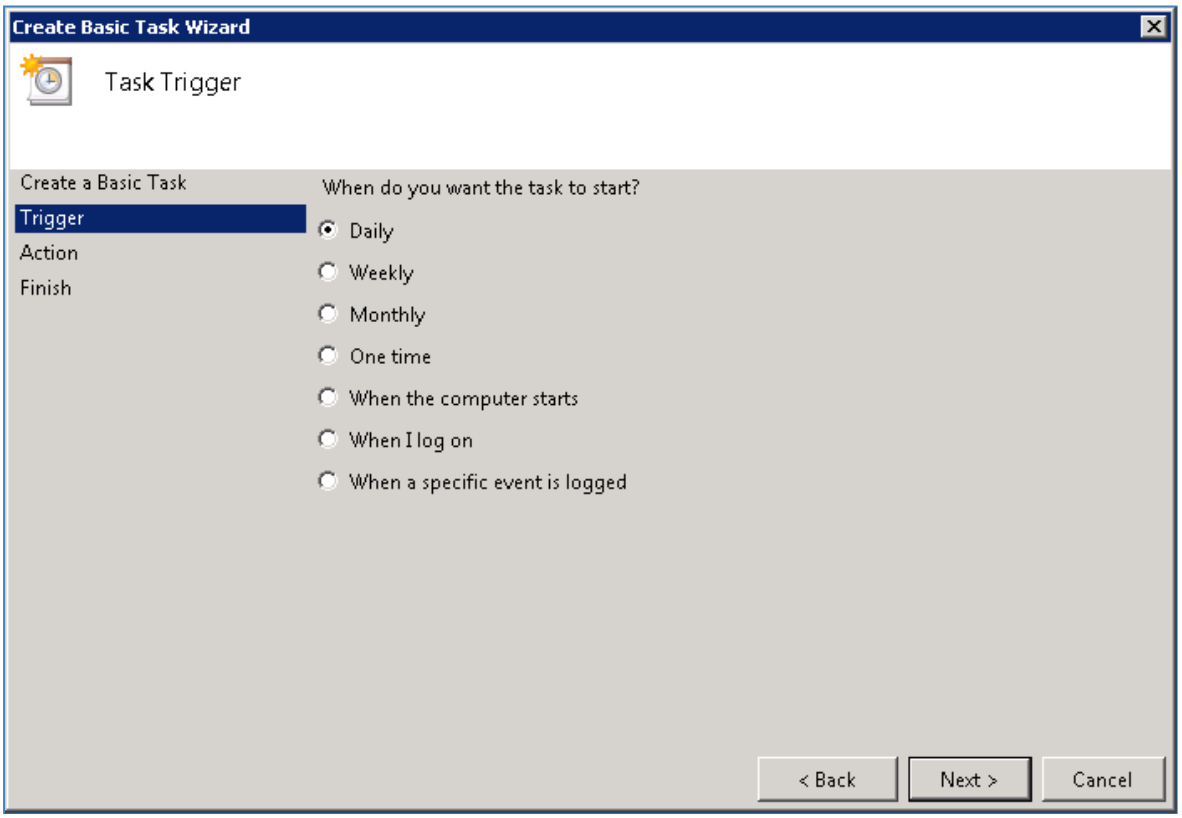
In Acronis Cyber Files werden die Logdateien im selben Ordner wie die von Tomcat gespeichert (`C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\apache-tomcat-7.0.34\logs`).

3. Speichern Sie die Datei.

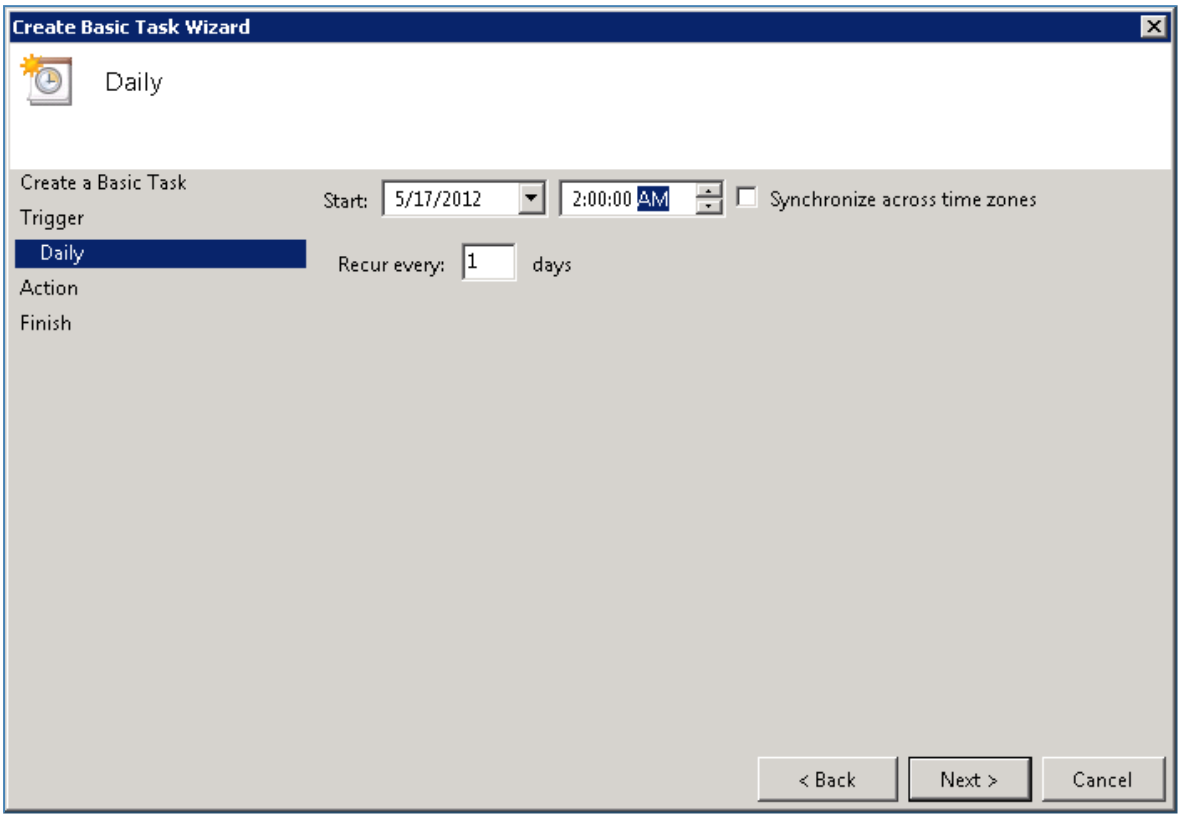
4. Öffnen Sie zum Automatisieren des Prozesses den **Task Scheduler**, und erstellen Sie einen neuen Task. Definieren Sie einen Namen und eine Beschreibung für den Task.



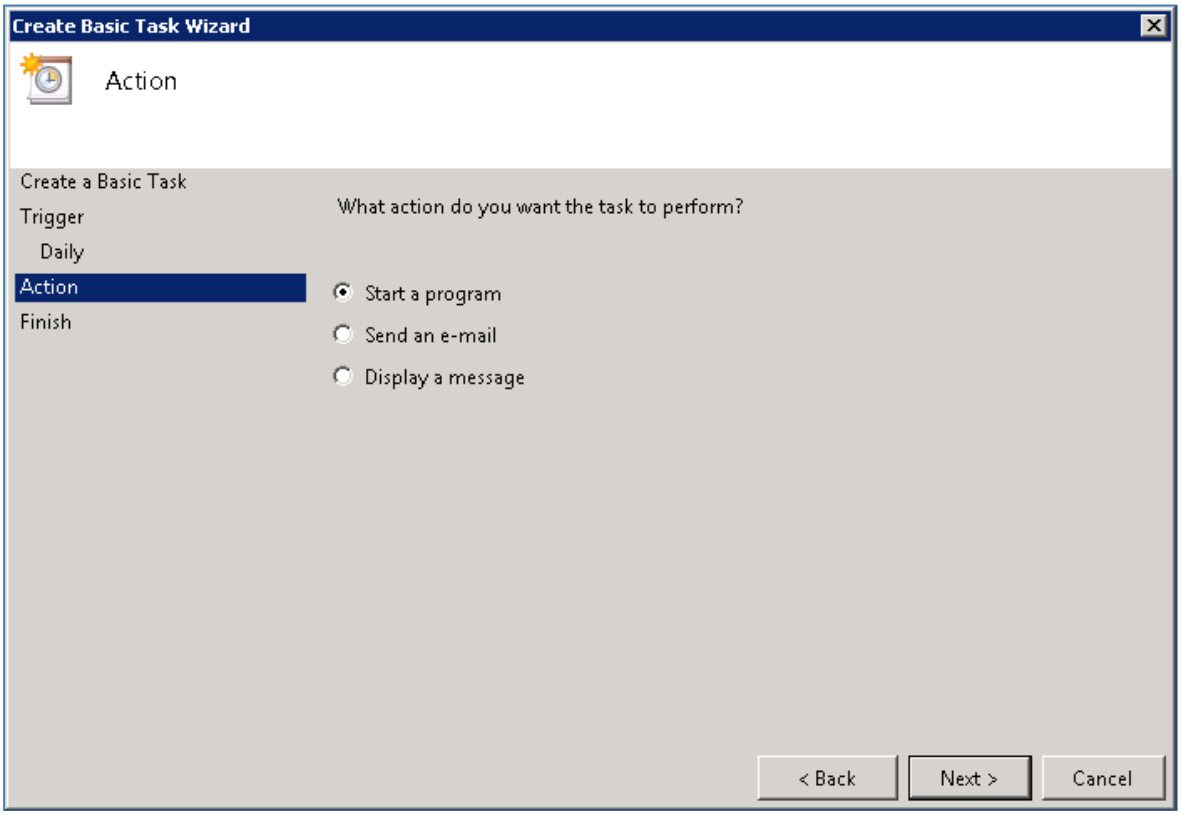
5. Legen Sie fest, dass der Task täglich ausgeführt wird.



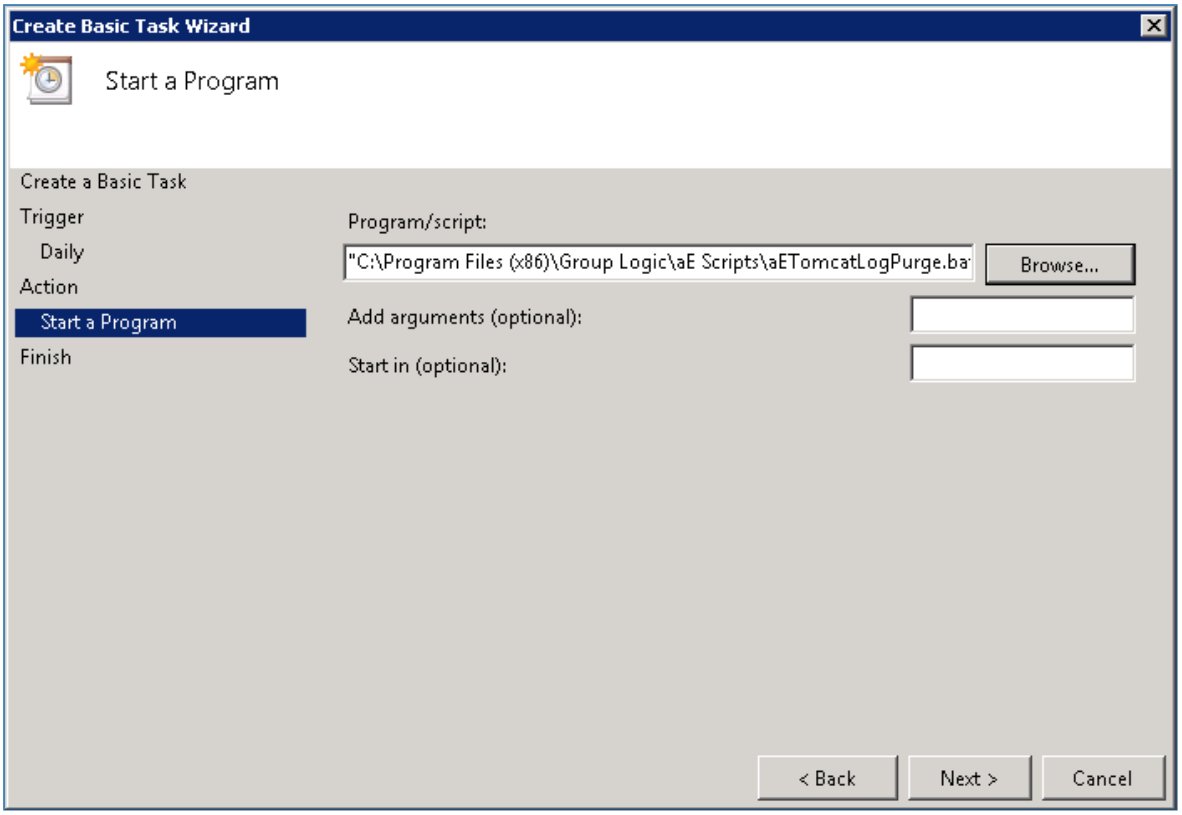
6. Geben Sie an, zu welcher Uhrzeit der Task starten soll. Es wird empfohlen, diesen Prozess nicht auszuführen, wenn das System extrem belastet ist oder andere Wartungsprozesse ausgeführt werden.



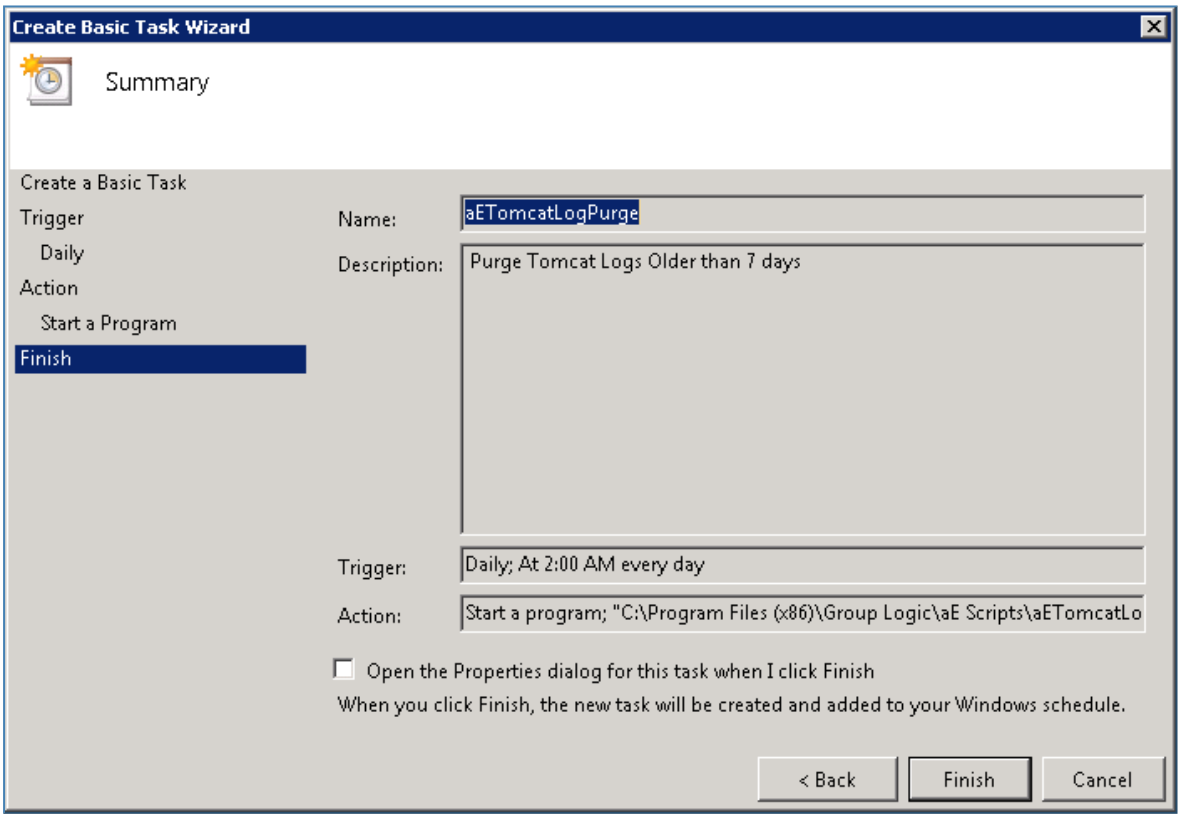
7. Legen Sie den Aktionstyp auf **Programm starten** fest.



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 einen Task klicken, 'Eigenschaften' auswählen und sich vergewissern, dass der Task ausgeführt wird, ob der Benutzer angemeldet ist oder nicht.
11. Sie können sich überzeugen, dass der Task korrekt konfiguriert ist und ordnungsgemäß funktioniert, indem Sie den Task auswählen, mit der rechten Maustaste darauf klicken und 'Ausführen' wählen. Im Scheduler-Log sollten Start, Stopp sowie etwaige Fehler aufgezeichnet werden.

Automatische Datenbanksicherung

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

Erstellen des Datenbanksicherungsskripts

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 AcronisCyber Files 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\).

Erstellen der geplanten Task

1. Öffnen Sie die **Systemsteuerung** und öffnen Sie anschließend **Verwaltung**.
2. Öffnen Sie die **Aufgabenplanung**.
3. Klicken Sie auf **Aktion** und wählen Sie **Task erstellen**.

Auf der Registerkarte Allgemein:

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**.

Auf der Registerkarte Auslöser:

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**.

Auf der Registerkarte Aktionen:

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 zum Ordner ein, in dem das Skript gespeichert ist. Lautet der Pfad zum Skript beispielsweise `C:\Program Files (x86)\Acronis\Files`

`Advanced\Common\PostgreSQL\9.3\PSQL.bat`, geben Sie `C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL\9.3\` ein.

5. Klicken Sie auf **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.

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 diese Fälle ist es am besten, einen geplanten Task festzulegen, um die Bereinigung mindesten einmal im Monat auszuführen.

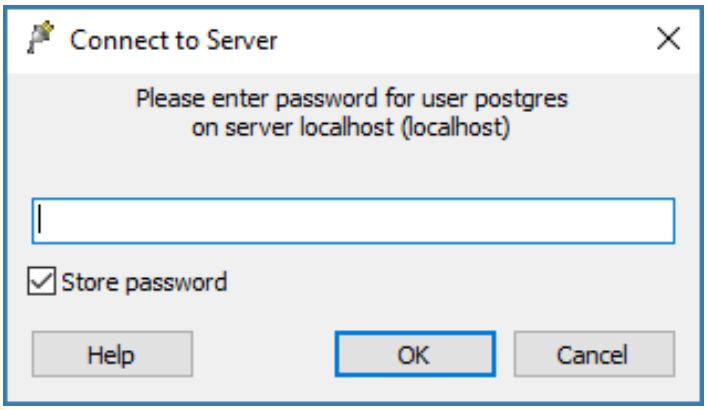
Konfigurieren von PostgreSQL und Erstellen des Skripts

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 Acronis Cyber Files PostgreSQL Administrator-Tool:

1. Öffnen Sie den Acronis Cyber Files PostgreSQL Administrator. Sie finden ihn im Startmenü von Windows im Ordner von Acronis Cyber Files.
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\<aktueller Benutzer>\AppData\Roaming\postgresql` erstellt.

   Hinweis
   Möglicherweise sehen Sie ein Dialogfeld mit Informationen zum Speichern von Kennwörtern. Das ist so vorgesehen. Klicken Sie auf **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.

Erstellen des Skripts

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

Hinweis
Hinweis: Sie müssen den Pfad so bearbeiten, dass er auf den PostgreSQL-Ordner `bin` verweist, wenn Sie eine ältere 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 Datei `psql.exe` mit Ihrem Dateipfad.
   - Ändern Sie die `--port`-Einstellung in die korrekte Port-Nummer, wenn Sie die Standardeinstellung geändert haben.
   - Wenn Sie einen anderen PostgreSQL-Benutzer verwenden, ändern Sie `--username=`, indem Sie `postgres` mit dem gewünschten Benutzer ersetzen.

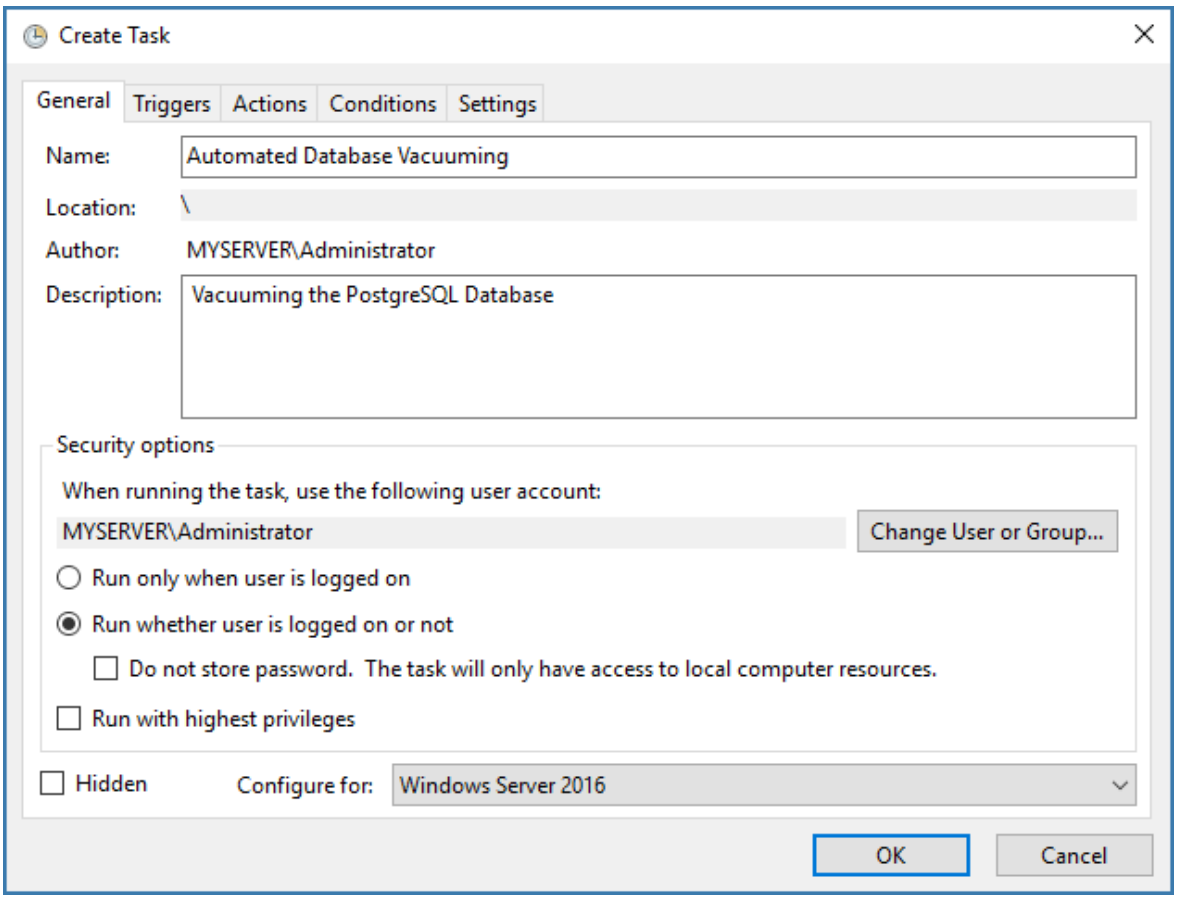
- Ändern Sie den Teil `D:\Backup\` des Pfads für die Logs in Ihren gewünschten Log-Ordner.
- Ändern Sie den Teil `D:\Backup\` des Pfads für die Datei 'pgpass.conf' in den Pfad der Datei.

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: `echo %date%`. 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.

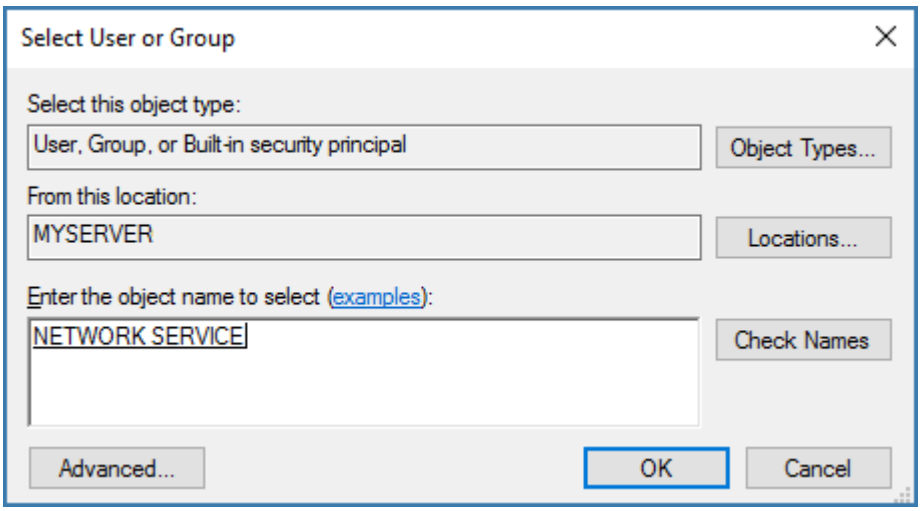
Konfigurieren des Task Scheduler

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**.

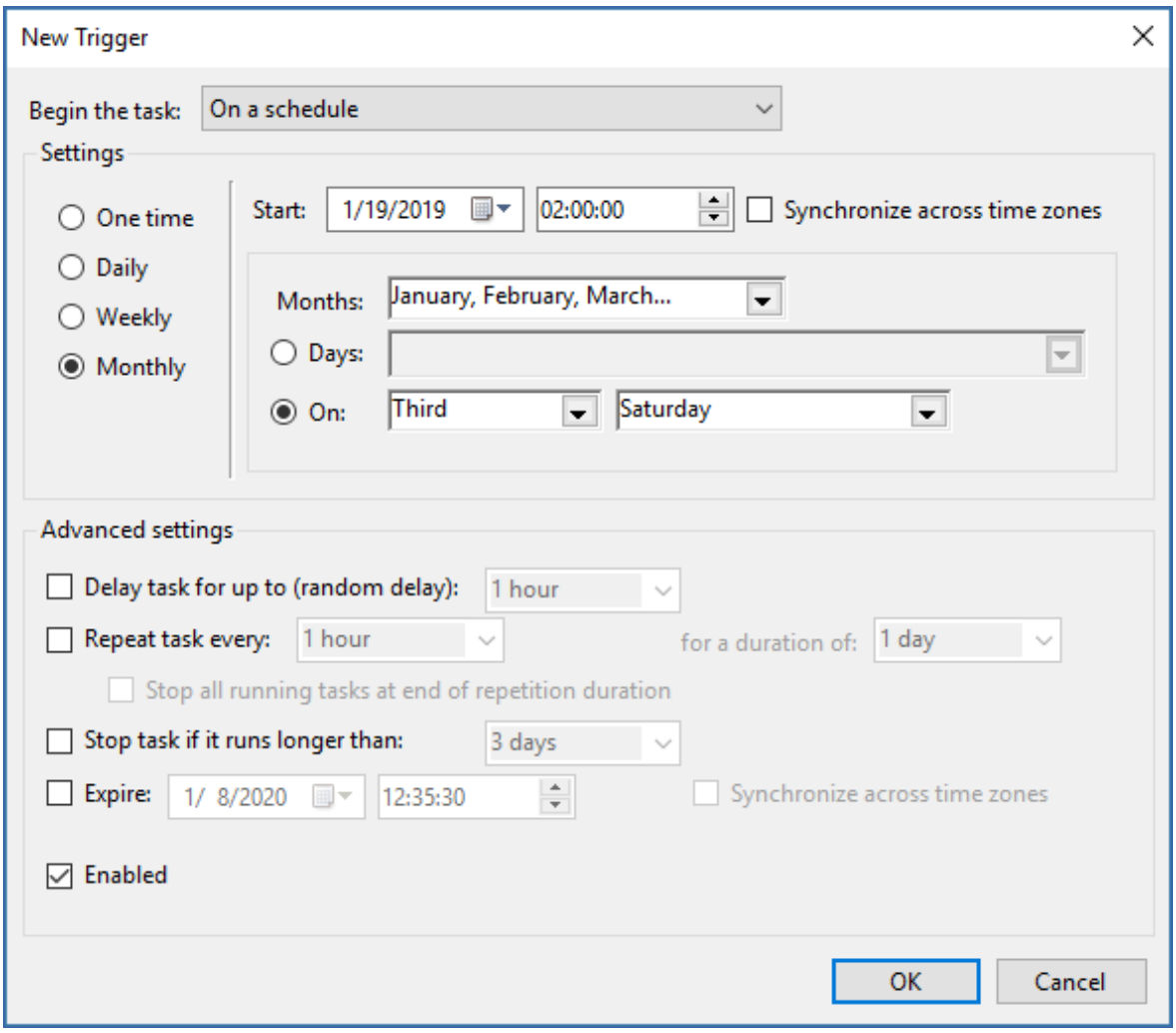


3. Gehen Sie auf der Registerkarte **Allgemein** wie folgt vor:
   - Legen Sie den **Namen** und die **Beschreibung** fest.
   - Wählen Sie **Unabhängig von Anmeldung des Benutzers ausführen**.

- Legen Sie das **Benutzerkonto** fest, mit dem der Task ausgeführt wird. Wir empfehlen, das NETZWERKDIENST-Konto der Maschine zu verwenden.

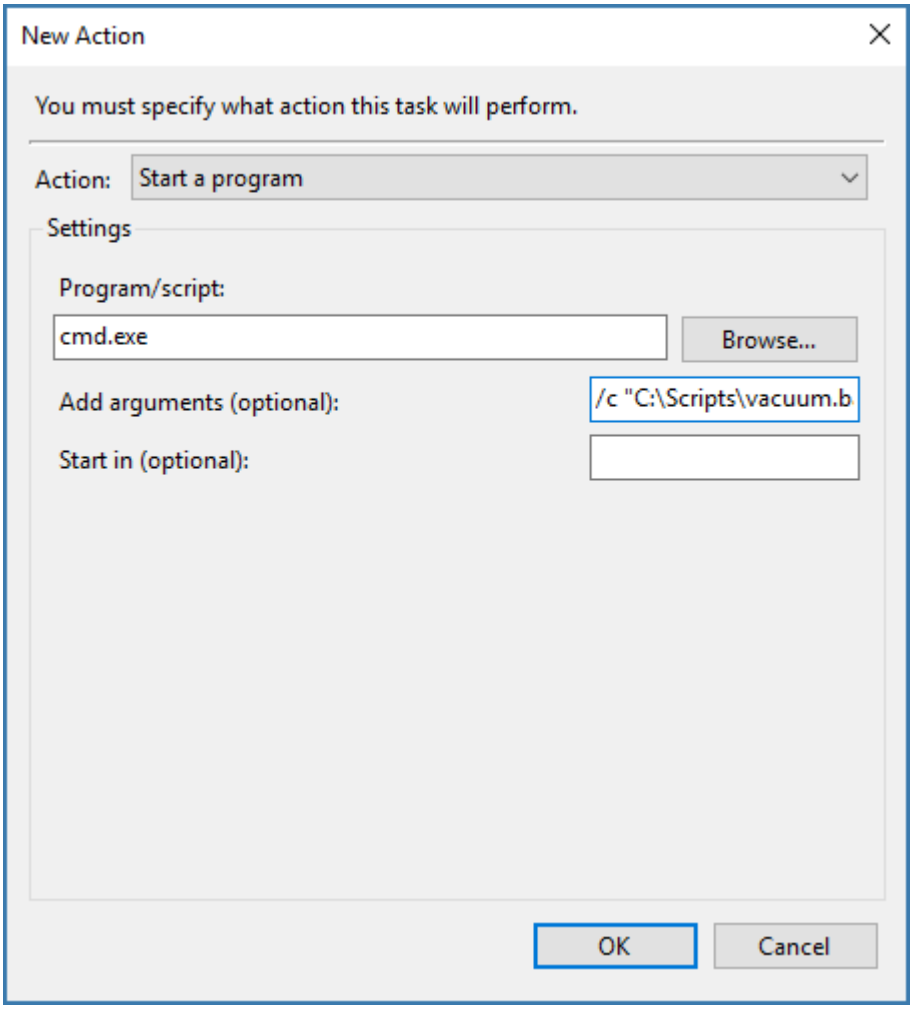


4. Gehen Sie in der Registerkarte **Auslöser** wie folgt vor:



- 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**.
- Für **Programm/Skript** geben Sie `cmd.exe` ein.
- Bei **Argumente hinzufügen** geben Sie `/c "C:\Scripts\vacuum.bat"` ein.

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 Administratorkennwort 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.

Migration von Acronis Cyber Files auf demselben Server

Dieser Leitfaden unterstützt Sie bei der Migration Ihres Acronis Cyber Files-Setups auf den aktuellen Rechnern.

Wichtig
Es wird dringend empfohlen, vor der Migration der Produktionsserver diese 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.

Vor dem Beginn mit einer Migration auf demselben Server

Warnung!
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 Cyber Files Web Server, PostgreSQL, Gateway und File Repository auf demselben Computer?
- Notieren Sie sich den DNS-Namen, die IP-Adresse und den Port des Cyber Files Web Server.
- Notieren Sie sich den DNS-Namen, die IP-Adresse und den Port des Gateway-Servers.
- Notieren Sie sich die Adresse und den Port des File Repository.
- Notieren Sie sich den Ort des File Store.
- Notieren Sie sich die Nummer der PostgreSQL-Version Ihres aktuellen 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**).

Hinweis
Viele dieser Informationen finden Sie im Konfigurationswerkzeug.

Grundlegender Ablauf des Migrationsvorgangs auf demselben Server

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

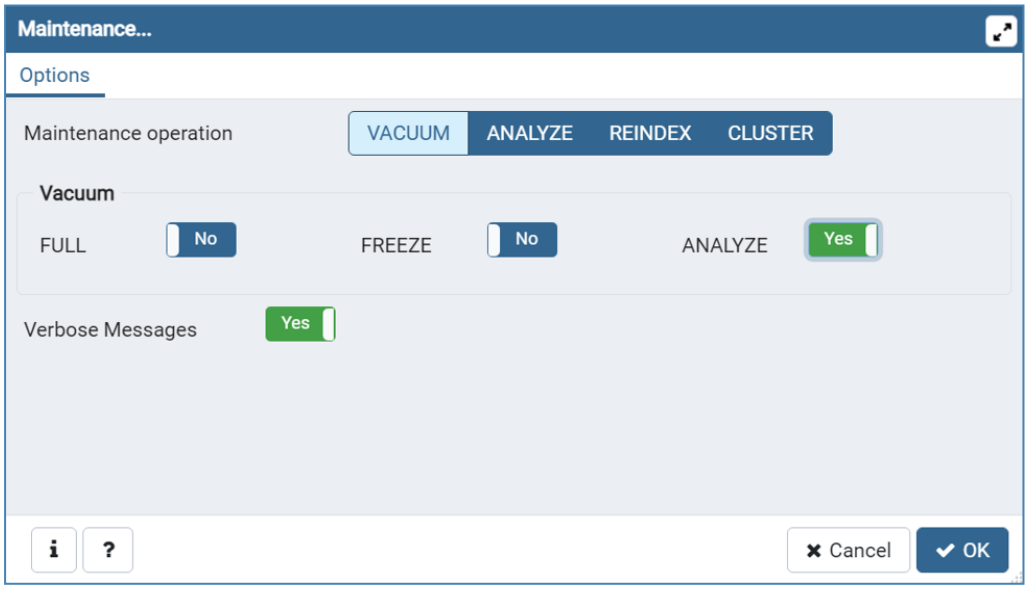
1. Erstellen Sie ein Backup von PostgreSQL.
2. Erstellen Sie ein Backup der Gateway Server-Datenbank.
3. Erstellen Sie ein Backup einiger weiterer Dateien.
4. Deinstallieren Sie Acronis Cyber Files.
5. Entfernen Sie das PostgreSQL-Datenverzeichnis.

6. [Optional] Entfernen Sie Java.
7. Installieren Sie Acronis Cyber Files mit demselben Versionsinstallationsprogramm wie für die Deinstallation.
8. Stellen Sie den Gateway Server-Datenbank wieder her.
9. Konfigurieren Sie den Server.
10. Überprüfen Sie die Administrationseinstellungen von Acronis Cyber Files.
11. Testen Sie die neue Konfiguration.

Migrieren von Acronis Cyber Files

So migrieren SieAcronis Cyber Files

1. ***Backup von PostgreSQL erstellen***
   a. Öffnen Sie die Systemsteuerung **Dienste**, und stoppen Sie Acronis Cyber Files Tomcat.
   b. Öffnen Sie das PostgreSQL Administrator-Tool von Acronis Cyber Files. Sie finden es im Startmenü von Windows im Ordner von Acronis Cyber Files. Stellen Sie eine Verbindung zum Datenbankserver her. Sie werden ggf. aufgefordert, das Kennwort für den `postgres`-Benutzer einzugeben.
   c. Erweitern Sie **Datenbanken**, und klicken Sie mit der rechten Maustaste auf die Datenbank `acronisaccess_production`.
   d. Wählen Sie **Maintenance**.
   e. Wählen Sie **VACUUM** und setzen Sie **ANALYZE** auf 'Ja'.



   f. Klicken Sie auf **OK**.
   g. 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.

h. Schließen Sie PostgreSQL Administrator, und öffnen Sie eine Eingabeaufforderung mit erweiterten Benutzerrechten.

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

Beispiel:`cd "C:\Program Files(x86)\Acronis\Acronis Cyber Files\Common\PostgreSQL\<version>\bin"`

Hinweis

Hinweis: Sie müssen den Pfad so bearbeiten, dass er auf den PostgreSQL-Ordner 'bin' verweist, wenn Sie eine ältere oder eine benutzerdefinierte Installation verwenden (z.B. `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\PostgreSQL\9.4\bin\`).

j. Geben Sie den folgenden Befehl ein: `pg_dumpall --host localhost --port 5432 --username postgres --file alldbs.sql`.

- `alldbs.sql` ist der Dateiname des Backups. Dieses wird im PostgreSQL-Bin-Verzeichnis gespeichert. Sie können einen Pfad im obigen Befehl verwenden, wenn Sie das Backup an einem anderen Ort speichern wollen. Ändern Sie dazu folgendermaßen den letzten Teil des oberen Befehls: `--file D:\Backups\alldbs.sql`
- Wenn Sie nicht den Standard-Port verwenden, müssen Sie statt `5432` die richtige Portnummer eingeben.
- Wenn Sie nicht das standardmäßige PSQL-Administratorkonto `postgres` verwenden, muss `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 Fenster mit der Eingabeaufforderung.

2. *Backup der Gateway Server-Datenbank erstellen*

a. Stoppen Sie den **Acronis Cyber Files Gateway**-Dienst.

b. Wechseln Sie zum Datenbankordner des Gateway Servers. Sie finden ihn standardmäßig an folgendem Speicherort:

`C:\Program Files (x86)\Acronis\Acronis Cyber Files\Gateway Server\database`

c. Erstellen Sie ein Backup der Datei `mobilEcho.sqlite3`.

3. ***Weitere Dateien, von denen ein Backup erstellt werden muss***

Wenn Sie Änderungen an den nachfolgenden Dateien vorgenommen haben, wird empfohlen, Backups zu erstellen, damit Sie Ihre Einstellungen beim Wiederherstellen oder Migrieren des Acronis Cyber Files-Produkts 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\Acronis Cyber Files\Common\PostgreSQL\<version>\Data`.

- `web.xml` standardmäßig hier: `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Access Server\Web Application\WEB-INF\`. Enthält Einstellungen für Single Sign-On.
- `server.xml`-Standardspeicherort: `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\apache-tomcat-<version>\conf`. Enthält Einstellungen für Tomcat.
- `krb5.conf`-Standardspeicherort: `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\apache-tomcat-<version>\conf`. Enthält Einstellungen für Single Sign-On.
- `login.conf`-Standardspeicherort: `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\apache-tomcat-<version>\conf`.
- Ihre für Acronis Cyber Files verwendeten Zertifikate und Schlüssel.
- `acronisaccess.cfg`-Standardspeicherort: `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Access Server`.
- Standardspeicherort für benutzerdefinierte Farbschemas: `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Access Server\Web Application\customizations\`.
- `pg_hba.conf`-Standardspeicherort: `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\PostgreSQL\<version>\Data`.

4. ***Deinstallieren Sie Acronis Cyber Files.***
   a. Öffnen Sie den Acronis Cyber Files-Installer.
   b. Akzeptieren Sie die Lizenzvereinbarung, und klicken Sie auf **Deinstallieren**.
   c. Wählen Sie alle Komponenten aus, und klicken Sie auf **Deinstallieren**.
5. ***PostgreSQL-Datenverzeichnis entfernen***
   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\`).

6. ***[Optional] Java entfernen***
   Möglicherweise möchten Sie auch Java entfernen, das für den Acronis Cyber Files Web Server installiert wurde.
   Auch Java kann ebenfalls über die Systemsteuerung entfernt werden.
7. ***Installieren Sie*** *Acronis Cyber Files* ***neu***
   a. Starten Sie den neuenAcronis Cyber Files-Installer und klicken Sie auf **Weiter**.
   b. Lesen und akzeptieren Sie die Lizenzvereinbarung.
   c. Wählen Sie **Installieren** aus, und durchlaufen Sie die Bildschirme des Installationsprogramms.

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

d. Geben Sie auf der Seite „PostgreSQL-Konfiguration“ das Kennwort für den PostgreSQL-Superuser ein, das auch ursprünglich verwendet wurde.
e. Klicken Sie auf **Weiter**.
f. Überprüfen Sie die zu installierenden Komponenten, und klicken Sie auf **Installieren**.
g. Klicken Sie nach Abschluss des Installationsprogramms auf **Beenden**. Daraufhin wird ein Dialogfeld mit der Information angezeigt, dass als Nächstes das Konfigurationswerkzeug ausgeführt wird.
h. Wenn das Konfigurationswerkzeug geöffnet wird, lassen Sie es geöffnet, ohne auf **OK** oder **Anwenden** zu klicken.
i. Öffnen Sie die Systemsteuerung **Dienste**, und stoppen Sie Acronis Cyber Files Tomcat.

Hinweis
Stoppen Sie für Lastenausgleichskonfigurationen alle Acronis Cyber Files Tomcat-Dienste.

j. Öffnen Sie die PostgreSQL Administrator-Applikation von Acronis Cyber Files, 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.
k. Klicken Sie mit der rechten Maustaste auf die Datenbank, und wählen Sie **Aktualisieren**.
l. 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 dann zu **Datenbanken**, klicken Sie mit der rechten Maustaste, und erstellen Sie eine neue Datenbank mit dem Namen `acronisaccess_production`.
m. Schließen Sie PostgreSQL Administrator, und öffnen Sie eine Eingabeaufforderung mit erweiterten Benutzerrechten.
n. Navigieren Sie in der Eingabeaufforderung zum PostgreSQL-Verzeichnis 'bin'.
   Beispiel: `cd "C:\Program Files\Acronis\Acronis Cyber Files\Common\PostgreSQL\<version>\bin"`
o. Kopieren Sie die Datenbank-Backupdatei `alldbs.sql` (oder den von Ihnen dafür verwendeten Namen) in das Verzeichnis **bin**.
p. Geben Sie in der Eingabeaufforderung den folgenden Befehl ein: `psql -U postgres -f alldbs.sql`.
q. Geben Sie Ihr `postgreSQL`-Kennwort ein, wenn Sie dazu aufgefordert werden.

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

r. Schließen Sie das Fenster mit der Eingabeaufforderung, wenn die Wiederherstellung beendet ist.
s. Öffnen Sie die **PostgreSQL-Administrator-Applikation von Files Advanced** erneut, und stellen Sie eine Verbindung mit dem Datenbankserver her.
t. Wählen Sie **Datenbanken** aus.
u. Erweitern Sie die Datenbank `acronisaccess_production`, erweitern Sie **Schemas**, und erweitern Sie **Öffentlich**.
Überprüfen Sie, ob die Anzahl der **Tabellen** der ursprünglichen Anzahl entspricht.

8. ***Gateway Server-Datenbank wiederherstellen***
Kopieren Sie die von Ihnen erstellte Backup-Datei der Gateway-Server-Datenbank `mobilEcho.sqlite3` in den Datenbankordner des neuen Gateway-Servers (standardmäßig `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Gateway Server\database`) und ersetzen Sie damit die vorhandene Datei.
9. ***Server konfigurieren***

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

a. Wechseln Sie zurück zum noch geöffneten Konfigurationsdienstprogramm von Acronis Cyber Files und legen Sie die Einstellungen für den Gateway-Server, den Acronis Cyber Files-Web-Server und das Datei-Repository fest.
b. Klicken Sie auf **Anwenden** und dann auf **OK**.
c. Klicken Sie im nächsten Dialogfeld auf **OK.** Daraufhin wird in einem Browser die Weboberfläche von Acronis Cyber Files gestartet.
d. Melden Sie sich beim Access Server an.
e. Klicken Sie auf **Administration**.
f. Navigieren Sie zur Seite **Mobile Access** -> **Gateway-Server**.
g. Ihr Gateway-Server sollte in der Liste der Gateway-Server aufgeführt sein.
h. 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 Ihren Server-Computer verweist. Handelt es sich bei der Adresse für Ihren Gateway um eine IP-Adresse, stellen Sie sicher, dass diese die IP-Adresse des Gateway-Servers ist.

10. ***Administrationseinstellungen von Acronis Cyber Files überprüfen***

Nachdem die Wiederherstellung der Datenbank abgeschlossen ist, wird Folgendes dringend empfohlen, bevor Sie weitere Schritte ausführen: Melden Sie sich bei der Weboberfläche an und vergewissern Sie sich, dass Ihre Einstellungen korrekt 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 Acronis Cyber Files-Protokolle über alle benötigten Berechtigungen verfügt, damit die Protokolle auch geschrieben werden können.
- 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.

Testen der neuen Konfiguration

Vergewissern Sie sich nach dem Durchführen der Migration, dass alles funktioniert, indem Sie diese einfachen Aktionen ausführen:

- Navigieren Sie durch die Weboberfläche, und überprüfen Sie, ob alles wie erwartet funktioniert. Überprüfen Sie, dass Ihre Einstellungen vorhanden sind und nicht geändert wurden.
- Laden Sie über die Weboberfläche eine Datei in den Bereich Synchronisieren und Freigeben hoch. Führen Sie diesen Schritt für ggf. eingerichtete Netzwerkknoten aus.
- Laden Sie eine Synchronisieren und Freigeben-Datei herunter, die vor der Migration vorhanden war. So bestätigen Sie, dass die Verbindung zum vorhandenen Dateispeicher noch funktioniert.
- Stellen Sie mit einem Desktop-Client und/oder einem mobilen Client eine Verbindung zur neuen Konfiguration her.
- Laden Sie mit dem Desktop-Client und/oder dem mobilen Client einige Dateien hoch und runter.

Acronis Cyber Files zu einem anderen Server migrieren

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

Wichtig
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.

Vor Beginn

Warnung!
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 Cyber Files Web Server, PostgreSQL, Gateway und File Repository auf demselben Computer?
- Notieren Sie sich den DNS-Namen, die IP-Adresse und den Port des Cyber Files Web Server.
- Notieren Sie sich den DNS-Namen, die IP-Adresse und den Port des Gateway-Servers.
- Notieren Sie sich die Adresse und den Port des File Repository.
- Notieren Sie sich den Ort des File Store.
- Notieren Sie sich die Nummer der PostgreSQL-Version Ihres aktuellen 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**).

Hinweis
Viele dieser Informationen finden Sie im Konfigurationswerkzeug.

Grundlegender Ablauf des Migrationsvorgangs:

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

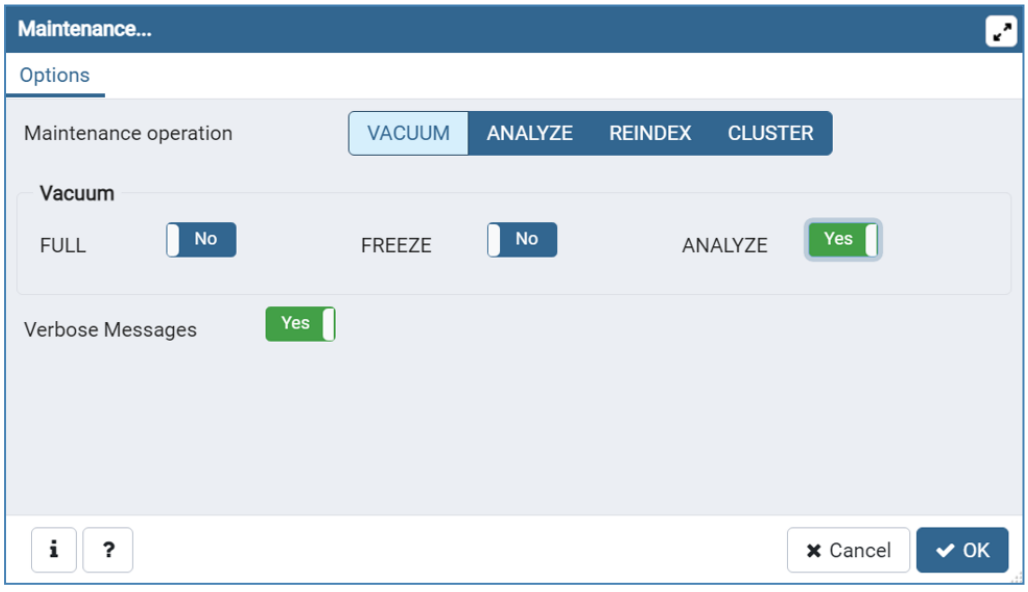
1. Ändern Sie die DNS-Einträge, sodass sie auf den neuen Servercomputer verweisen.
2. Erstellen Sie ein Backup Ihrer aktuellen Datenbankdateien und Zertifikate.
3. Verschieben Sie die Datenbankdateien und Zertifikate auf den neuen Computer.
4. Migrieren Sie den File Store.
5. Installieren Sie Acronis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

Acronis Cyber Files-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 Acronis Cyber Files-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://support.acronis.com/mobility zur Verfügung.

1. Stoppen Sie den Acronis Cyber Files-Tomcat-Dienst.
   i. Öffnen Sie das PostgreSQL Administrator-Tool von Acronis Cyber Files. Sie finden es im Startmenü von Windows im Ordner von Acronis Cyber Files. Stellen Sie eine Verbindung zum Datenbankserver her. Sie werden ggf. aufgefordert, das Kennwort für den `postgres`-Benutzer einzugeben.
   ii. Erweitern Sie **Datenbanken**, und klicken Sie mit der rechten Maustaste auf die Datenbank `acronisaccess_production`.
   iii. Wählen Sie **Maintenance**.
   iv. Wählen Sie **VACUUM** und setzen Sie **ANALYZE** auf 'Ja'.



   v. Klicken Sie auf **OK**.
   vi. 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.

vii. Schließen Sie PostgreSQL Administrator, und öffnen Sie eine Eingabeaufforderung mit erweiterten Benutzerrechten.

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

Beispiel:`cd "C:\Program Files(x86)\Acronis\Acronis Cyber Files\Common\PostgreSQL\<version>\bin"`

Hinweis

Hinweis: Sie müssen den Pfad so bearbeiten, dass er auf den PostgreSQL-Ordner 'bin' verweist, wenn Sie eine ältere oder eine benutzerdefinierte Installation verwenden (z.B. `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\PostgreSQL\9.4\bin\`).

ix. Geben Sie den folgenden Befehl ein: `pg_dumpall --host localhost --port 5432 --username postgres --file alldbs.sql`.

- `alldbs.sql` ist der Dateiname des Backups. Dieses wird im PostgreSQL-Bin-Verzeichnis gespeichert. Sie können einen Pfad im obigen Befehl verwenden, wenn Sie das Backup an einem anderen Ort speichern wollen. Ändern Sie dazu folgendermaßen den letzten Teil des oberen Befehls: `--file D:\Backups\alldbs.sql`
- Wenn Sie nicht den Standard-Port verwenden, müssen Sie statt `5432` die richtige Portnummer eingeben.
- Wenn Sie nicht das standardmäßige PSQL-Administratorkonto `postgres` verwenden, muss `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 Fenster mit der Eingabeaufforderung.

2. ***Backup der Gateway Server-Datenbank***
   a. Stoppen Sie den **AcronisCyber Files Gateway**-Dienst.
   b. Wechseln Sie zum Datenbankordner des Gateway Servers. Sie finden ihn standardmäßig an folgendem Speicherort:
   `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Gateway Server\database`
3. Kopieren Sie die Datei `mobilEcho.sqlite3` auf den neuen Computer, auf dem der Gateway-Server gehostet werden soll.

Weitere Dateien, von denen ein Backup erstellt werden muss

Wenn Sie Änderungen an den nachfolgenden Dateien vorgenommen haben, wird empfohlen, Backups zu erstellen, damit Sie Ihre Einstellungen beim Wiederherstellen oder Migrieren des Acronis Cyber Files-Produkts 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\Acronis Cyber Files\Common\PostgreSQL\<Version>\Data`.

- `web.xml` standardmäßig hier: `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Access Server\Web Application\WEB-INF\`. Enthält Einstellungen für Single Sign-On.
- `server.xml`-Standardspeicherort: `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\apache-tomcat-<Version>\conf`. Enthält Einstellungen für Tomcat.
- `krb5.conf`-Standardspeicherort: `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\apache-tomcat-<Version>\conf`. Enthält Einstellungen für Single Sign-On.
- `login.conf`-Standardspeicherort: `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\apache-tomcat-<Version>\conf`.
- Ihre für Acronis Cyber Files verwendeten Zertifikate und Schlüssel.
- `acronisaccess.cfg`-Standardspeicherort: `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Access Server`.
- Standardspeicherort für benutzerdefinierte Farbschemas: `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Access Server\Web Application\customizations\`.
- `pg_hba.conf`-Standardspeicherort: `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\PostgreSQL\<Version>\Data`.
- Datei `newrelic.yml`, wenn Sie **New Relic** zum Überwachen Ihres Acronis Cyber Files-Servers verwenden.

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

Installieren Sie Acronis Cyber Files.

1. Starten Sie das Installationsprogramm von Acronis Cyber Files, 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 Acronis Cyber Files-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.
7. Öffnen Sie die Systemsteuerung **Dienste**, und stoppen Sie Acronis Cyber Files Tomcat Service.

   Hinweis
   Stoppen Sie für Lastenausgleichskonfigurationen alle Acronis Cyber Files Tomcat Service.

8. Öffnen Sie die PostgreSQL Administrator-Anwendung von Acronis Cyber Files, 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.
9. Klicken Sie mit der rechten Maustaste auf die Datenbank, und wählen Sie **Aktualisieren**.
10. 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`.
11. Schließen Sie PostgreSQL Administrator, und öffnen Sie eine Eingabeaufforderung mit erweiterten Benutzerrechten.
12. Navigieren Sie in der Eingabeaufforderung zum PostgreSQL-Verzeichnis 'bin'.
    Beispiel: `cd "C:\Program Files\Acronis\Acronis Cyber Files\Common\PostgreSQL\<version>\bin"`
13. Kopieren Sie die Datenbank-Backupdatei `alldbs.sql` (oder den von Ihnen dafür verwendeten Namen) in das Verzeichnis **bin**.
14. Geben Sie in der Eingabeaufforderung den folgenden Befehl ein: `psql -U postgres -f alldbs.sql`.
15. Geben Sie das `postgres`-Kennwort ein, wenn Sie dazu aufgefordert werden.

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

16. Schließen Sie das Fenster mit der Eingabeaufforderung, wenn die Wiederherstellung beendet ist.
17. Öffnen Sie die **PostgreSQL-Administrator-Applikation von Files Advanced** erneut, und stellen Sie eine Verbindung mit dem Datenbankserver her.
18. Wählen Sie **Datenbanken** aus.
19. Erweitern Sie die Datenbank `acronisaccess_production`, erweitern Sie **Schemas**, und erweitern Sie **Öffentlich**. Überprüfen Sie, ob die Anzahl der **Tabellen** der Anzahl auf dem ursprünglichen Server entspricht.

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

Gateway Server-Datenbank wiederherstellen

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

Neuen Server konfigurieren

Hinweis
Es wird dringend empfohlen, die von Acronis Cyber Files 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 Acronis Cyber Files weiterverwenden.

1. Wechseln Sie zurück zum noch geöffneten Konfigurationsdienstprogramm von Acronis Cyber Files und legen Sie die Einstellungen für den Gateway-Server, den Acronis Cyber Files-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 Acronis Cyber Files gestartet.
3. Melden Sie sich beim Access Server an.
4. Klicken Sie auf **Administration**. Navigieren Sie zur Seite **Mobile Access** -> **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 Acronis Cyber Files 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 Acronis Cyber Files-Protokolle über alle benötigten Berechtigungen verfügt, damit die Protokolle auch geschrieben

werden können.

- New Relic – Wenn Sie mit 'New Relic' arbeiten, kopieren Sie die Datei `newrelic.yml` von der alten Maschine auf diese und vergewissern sich, dass der Pfad in der Acronis Cyber Files-Weboberfläche 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.

Testen der neuen Konfiguration

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 einem Desktop-Client und einem mobilen Client eine Verbindung mit dem Server her.
- Laden Sie mit dem Desktop-Client bzw. dem mobilen Client einige Dateien hoch und runter.

Ursprünglichen Server bereinigen

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

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

Hinweis
Wenn Sie nicht über ein Acronis Cyber Files-Installationsprogramm verfügen, öffnen Sie die Systemsteuerung, und deinstallieren Sie die folgenden Komponenten: Acronis Cyber Files PostgreSQL Server, Acronis Cyber Files Gateway Server, Acronis Cyber Files File Repository Server, Acronis Cyber Files Web Server, Acronis Cyber Files-Konfigurations-Sammlungswerkzeug, Acronis Cyber Files-Konfigurationswerkzeug 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\`).

- Möglicherweise möchten Sie auch Java entfernen, das für den Acronis Cyber Files Web Server installiert wurde. Auch Java kann ebenfalls über die Systemsteuerung entfernt werden.

Durchführen eines PostgreSQL-Upgrades auf eine neuere Hauptversion

Mit Releases für Major PostgreSQL werden häufig neue Funktionen hinzugefügt, durch die einige der internen Arbeitsvorgänge von PostgreSQL verändert werden.

Für Einzelserver-Installationen können die Schritte zur Migration auf demselben Server verwendet werden.

Wichtig
Acronis Cyber Files unterstützt Upgrades von PostgreSQL nur über den Cyber Files-Installer. Die offizielle PostgreSQL-Distribution wird nicht unterstützt. Es wird ausschließlich die Version unterstützt, die ausgeliefert wird.

Hinweis
Das Upgraden von PostgreSQL kann sehr zeitaufwendig sein.

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

Ergänzendes Material

In Konflikt stehende Software

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

- **VMware View™ Persona Management** – Diese Applikation kann Probleme mit dem Synchronisierungsprozess des Acronis Cyber Files Desktop Clients und beim Löschen von Dateien verursachen. Wenn Sie den Acronis Cyber Files Sync-Ordner außerhalb des **Persona Management-Benutzerprofils** platzieren, sollten die bekannten Konflikte vermieden werden.
- **Virenschutzprogramme** sollten keine Synchronisierungsordner prüfen, da dies zu Konflikten mit dem Synchronisierungsprozess führen kann. Wir empfehlen, den Acronis Cyber Files FileStore-Ordner zur Ignorieren- oder Positivliste 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.

Für Acronis Cyber Files-Server

Lastverteilung für Acronis Cyber Files

Es gibt zwei Hauptmöglichkeiten der Lastverteilung für Acronis Cyber Files:

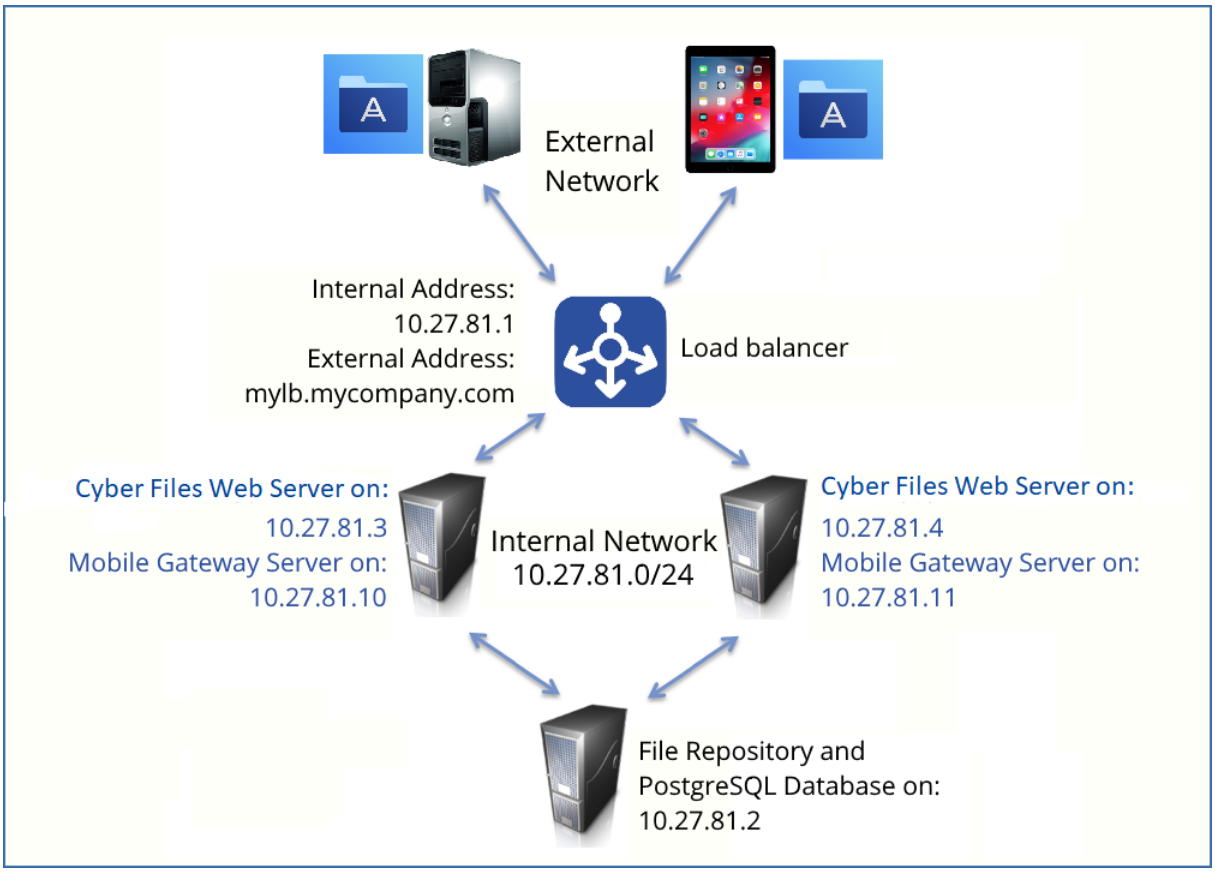
Lastenausgleich nur für Acronis Cyber Files-Mobile-Gateways vornehmen

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

Lastverteilung für alle Komponenten von AcronisCyber Files

Bei dieser Konfiguration wird eine Lastverteilung für alle Komponenten von Acronis Cyber Files vorgenommen und hohe Verfügbarkeit für alle Benutzer sichergestellt. 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 Acronis Cyber Files-Web-Server und Acronis Cyber Files-Mobile-Gateways. Nachfolgend finden Sie eine Anleitung zur Konfiguration dieses Setups.



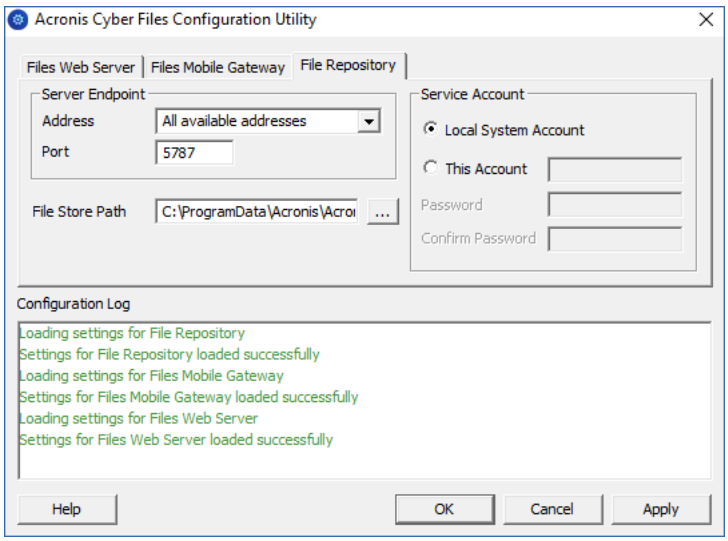
Diese Anleitung enthält alle notwendigen Details, um den Lastenausgleich für das Acronis Cyber Files-Produkt in Ihrer Umgebung ordnungsgemäß vorzunehmen.

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

1. Starten Sie das Installationsprogramm von Acronis Cyber Files, und klicken Sie auf **Weiter**. Lesen und akzeptieren Sie die Lizenzvereinbarung.
2. Wählen Sie im Acronis Cyber Files-Installationsprogramm **Benutzerdefiniert**. Wählen Sie **Acronis Cyber Files-Datei-Repository** und **PostgreSQL Database Server** aus, und klicken Sie auf **Weiter**.
3. Wählen Sie den Speicherort aus, an dem das Datei-Repository und das Konfigurationswerkzeug installiert werden sollen.
4. Wählen Sie den Speicherort aus, an dem PostgreSQL installiert werden soll, und geben Sie ein Kennwort für den Super-User **postgres** ein.
5. Öffnen Sie den TCP-Port 5432. Mit dessen Hilfe greifen Sie von den Remote-Maschinen aus auf die PostgreSQL-Datenbank zu.
6. Fahren Sie nach Abschluss des Installationsvorgangs mit dem Konfigurationswerkzeug fort.
   a. Sie werden aufgefordert, das Konfigurationswerkzeug zu öffnen. Drücken Sie **OK**.
   b. Wählen Sie die Adresse und den Port für den Zugriff auf das Datei-Repository aus.

Hinweis
Sie müssen dieselbe Adresse und denselben Port in der Weboberfläche von Acronis Cyber Files festlegen. Weitere Informationen finden Sie in den Artikeln Das Konfigurationswerkzeug verwenden und Datei-Repository.

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 Acronis Cyber Files-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
# Erster Acronis Cyber Files & Gateway Server
host all all 10.27.81.3/32 md5
# Zweiter Acronis Cyber Files & Gateway Server
host all all 10.27.81.4/32 md5
```

In diesen Beispielen können alle Benutzer, die mit dem ersten Acronis Cyber Files-Server (10.27.81.3/32) und dem zweiten Acronis Cyber Files-Server (10.27.81.4/32) verbunden sind, über eine MD5-verschlüsselte Verbindung auf die Datenbank mit vollen Berechtigungen (außer der Berechtigung zur Replikation) zugreifen.

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 Standardspeicherort ist `C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL\<VERSION>\Data\postgresql.conf`.

b. Suchen Sie die Zeile `#listen_addresses = 'localhost'`.

c. Aktivieren Sie diesen Befehl, indem Sie das **#**-Symbol am Beginn der Zeile entfernen.

d. Ersetzen Sie `localhost` durch *****, 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 = '*'` – Dies bedeutet, dass PostgreSQL alle verfügbaren Adressen überwacht.
- **z.B.**`listen_addresses = '192.168.1.1'` – Dies bedeutet, dass PostgreSQL diese Adresse überwacht.

e. Speichern Sie alle Änderungen an **postgresql.conf**.

f. Starten Sie den Acronis Cyber Files-PostgreSQL-Dienst neu.

10. Öffnen Sie das **Acronis Cyber Files PostgreSQL Administrator-Tool**. Sie finden es im Startmenü von Windows im Ordner von Acronis Cyber Files. Stellen Sie eine Verbindung zum lokalen Server her. Wählen Sie **Datenbanken** und klicken Sie entweder mit der rechten Maustaste oder wählen Sie **Neue Datenbank** im Menü **Bearbeiten** -> **Neues Objekt**, um eine neue Datenbank zu erstellen. Nennen Sie diese **acronisaccess_production**.

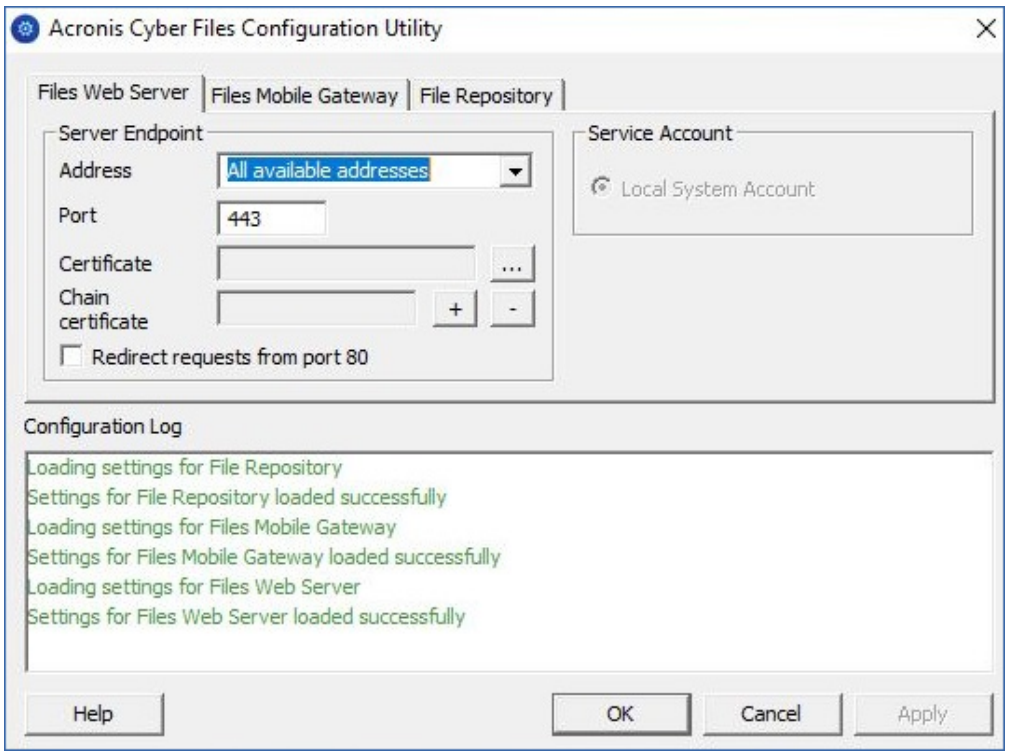
Hinweis
PostgreSQL verwendet standardmäßig Port 5432. Stellen Sie sicher, dass dieser Port in jeder Firewall oder Routing-Software geöffnet ist.

Gehen Sie auf den beiden Servern, die als Acronis Cyber Files-Server und Acronis Cyber Files-Gateways fungieren, wie folgt vor:

1. Starten Sie das Installationsprogramm von Acronis Cyber Files, und klicken Sie auf **Weiter**. Lesen und akzeptieren Sie die Lizenzvereinbarung.
2. Wählen Sie im Acronis Cyber Files-Installationsprogramm **Benutzerdefiniert** aus. Wählen Sie nur **Acronis Cyber Files-Web-Server** und **Acronis Cyber Files-Mobile-Gateway** aus und fahren Sie mit dem Installationsvorgang fort.
3. Fahren Sie nach Abschluss des Installationsvorgangs mit dem Konfigurationswerkzeug fort.
   a. Sie werden aufgefordert, das Konfigurationswerkzeug zu öffnen. Drücken Sie **OK**.
   b. **Auf der Registerkarte 'AcronisCyber Files-Web-Server':**
      - Geben Sie die Adresse und den Port für den Zugriff auf den Acronis Cyber Files-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.

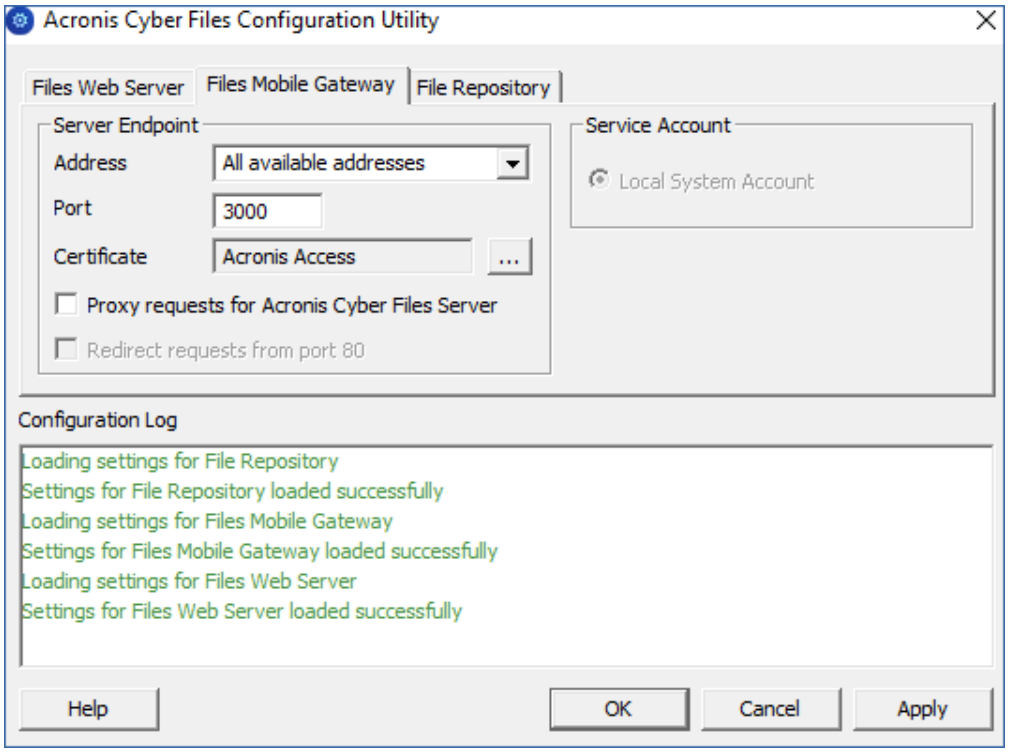
- Klicken Sie auf **Anwenden**.

Hinweis
Wenn Sie kein Zertifikat haben, wird ein selbstsigniertes Zertifikat von Acronis Cyber Files erstellt. Dieses Zertifikat sollte NICHT in Produktionsumgebungen verwendet werden.



c. **Auf der Registerkarte 'Acronis Cyber Files-Mobile-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 kein Zertifikat haben, wird ein selbstsigniertes Zertifikat von Acronis Cyber Files erstellt. Dieses Zertifikat sollte NICHT in Produktionsumgebungen verwendet werden.



4. Navigieren Sie zum Installationsverzeichnis von Acronis Cyber Files (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 Acronis Cyber Files-Server so konfiguriert, dass er eine Verbindung zur PostgreSQL-Remote-Datenbank herstellt, z.B.:

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

6. Öffnen Sie 'Services.msc' und starten Sie die Acronis Cyber Files-Dienste neu.

Gehen Sie auf einem der Acronis Cyber Files-Web-Server und Acronis Cyber Files-Mobile-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 **Acronis Cyber Files-Tomcat**-Dienst neu. Hierdurch wird die erstellte Datenbank gefüllt.

2. Öffnen Sie https://myaccess (d.h. https://10.27.81.3 oder https://10.27.81.4) in Ihrem Webbrowser und führen Sie den Installationsassistenten aus.
   a. **Auf der Registerkarte 'Lizenzierung':**
      - Geben Sie Ihren Lizenzschlüssel ein, aktivieren Sie das Kontrollkästchen, und klicken Sie auf **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 Ihren 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 Ihren SMTP-Server eine Authentifizierung per Benutzername/Kennwort verwenden, aktivieren Sie 'SMTP-Authentifizierung verwenden?', und geben Sie Ihre Anmeldedaten ein.
      - Klicken Sie auf **Speichern**.
   d. **Auf der Registerkarte 'LDAP':**
      - Markieren Sie **LDAP aktivieren**.
      - Geben Sie den DNS-Namen oder die IP-Adresse des LDAP-Servers ein.
      - Geben Sie den Port des LDAP-Servers ein.
      - Falls Sie ein Zertifikat für Verbindungen mit dem LDAP-Server verwenden, markieren Sie Sichere LDAP-Verbindung verwenden.
      - Geben Sie Ihre LDAP-Anmeldedaten einschließlich der Domain ein. (beispielsweise mycompany\myname).
      - Geben Sie die LDAP-Suchbasis ein.
      - Geben Sie die gewünschte(n) Domain(s) für die LDAP-Authentifizierung ein. (Für ein Konto mit der E-Mail-Adresse joe@glilabs.com würden Sie zur LDAP-Authentifizierung

beispielsweise glilabs.com eingeben.)

- Klicken Sie auf **Speichern**.

e. **Unter der Registerkarte Lokales Gateway**:

> **Hinweis**
> Wenn Sie ein Files Advanced-Mobile-Gateway und den Acronis Cyber Files-Web-Server auf demselben Computer installieren, wird das Gateway automatisch erkannt und vom Acronis Cyber Files-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).
- Klicken Sie auf **Speichern**.

f. **Unter der Registerkarte Datei-Repository**:

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

3. Nachdem Sie den Installationsassistenten abgeschlossen haben, klicken Sie auf **Fertig stellen** und navigieren zu **Mobile Access** -> **Gateway-Server**.
4. Nun können Sie den zweiten Gateway-Server registrieren:
   a. Geben Sie einen **Anzeigename** 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'.
   d. Klicken Sie auf **Speichern**.
5. Erstellen Sie eine Cluster-Gruppe, und fügen Sie ihr alle Gateway-Server hinzu. Der Primärserver sollte der Server sein, für den Sie bereits den Installationsassistenten ausgeführt haben. Weitere Informationen finden Sie im Artikel 'Cluster-Gruppen'.

> **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 **Mobile Access**.
   b. Öffnen Sie die Seite **Gateway Server**.
   c. Klicken Sie auf 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.

Installieren von Acronis Cyber Files 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 Acronis Cyber Files 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 Acronis Cyber Files 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.

Systemanforderungen

Hardwareanforderungen

In einer Produktionsumgebung empfehlen wir Ihnen die Verwendung von mindestens drei (3) Acronis Cyber Files 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 Servern empfehlen wir die Verwendung von Interconnects mit geringer Latenz zwischen den Gast-Virtual Machines.

- 1 Lastenausgleichsmodul für die Acronis Cyber Files Web-Server.
- 1 Lastenausgleichsmodul für die Acronis Cyber Files Gateway-Server.
- 3 Acronis Cyber Files Tomcat-Server, jeweils mit 32 GB RAM und einer 16-Kern-CPU.
- 3 Acronis Cyber Files 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 File Repository-Dienst + File Store. Die Parameter dieses Servers sind nicht besonders wichtig.

Netzwerkverbindungen

- Der Lastenausgleich für die Acronis Cyber Files Tomcat Server muss so konfiguriert werden, dass die DNS-Adresse des aktuellen Acronis Cyber Files-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 Administration und Gateway Server der Acronis Cyber Files-Webbenutzeroberfläche ist 'Adresse für Clientverbindungen' die Adresse des externen Lastenausgleichs. Für die Gateway Server verwenden wir auch die Einstellung 'Alternative Adresse für Acronis Cyber Files Server-Verbindungen verwenden', und in 'Adresse für Verbindungen des Acronis Cyber Files Web Server ist die interne Adresse des Gateway-Lastenausgleichs.
- Der Gateway Server muss mit dem Tomcat-Lastenausgleich für die mobilen Clientverbindungen verbunden werden.

Hinweis
Für die Sync&Share-Datenquelle müssen Sie die Adresse zur Adresse des Tomcat-Lastenausgleichs ändern.

Installieren und Konfigurieren von PostgreSQL

Installieren der PostgreSQL Server-Komponente

1. Starten Sie das Installationsprogramm von Acronis Cyber Files, 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. Wählen Sie dann 'Weiter" aus.
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 PostgreSQL-Ordner **data** (standardmäßig unter `C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL\<version>\Data`) und öffnen Sie die Datei `pg_hba.conf` in einem Editor.
2. Beziehen Sie die Host-Einträge für Ihre Acronis Cyber Files-Tomcat-Server mittels ihrer internen Adressen ein und speichern Sie die Datei.

   Die Datei `pg_hba.conf` ('HBA' steht für 'host-basierte Authentifizierung') steuert die Clientauthentifizierung 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 (Erster Acronis Cyber Files & 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 **replication**) über eine mit `md5 encrypted` Verbindung zugreifen.

Einstellen der korrekten Verbindungszahl

1. Suchen Sie `max_connections`, und ändern Sie dies zu `510`.
2. Entfernen Sie das vorangestellte `#` aus der folgenden Zeile: `#listen_addresses = 'localhost'`. Ersetzen Sie `localhost` durch `*`. Dies muss nun wie folgt aussehen: `listen_addresses = '*'`
3. Entfernen Sie das vorangestellte `#` aus der folgenden Zeile: `#effective_cache_size = 128MB`, und ersetzen Sie **128MB** durch **12GB**. Dies sollte wie folgt aussehen: `effective_cache_size = 12GB`

4. Ergänzen Sie 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 Acronis Cyber Files-PostgreSQL Server-Dienst neu.

Installieren von Acronis Cyber Files-Servern

Nur den Acronis Cyber Files-Web-Server installieren

1. Starten Sie das Acronis Cyber Files-Installationsprogramm, und akzeptieren Sie die Lizenzvereinbarung.
2. Wählen Sie **Benutzerdefiniert** aus, und wählen Sie NUR den Acronis Cyber Files-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 Acronis Cyber Files-Tomcat-Dienst angehalten wurde.

Serverkonfiguration

Alle Einstellungen, die Sie auf einem Acronis Cyber Files Web Server ändern, müssen auch auf allen anderen Acronis Cyber Files Web Servern geändert werden.

Hinweis
Vergessen Sie nicht, einen Eintrag in der Datei `pg_hba.conf` für jeden Acronis Cyber Files Web Server vorzunehmen!

Konfigurieren des Servers zur Verbindung mit der richtigen Datenbank

1. Navigieren Sie zum Ordner des Acronis Cyber Files-Web-Servers (standardmäßig `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 festzulegen.

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, für diese Einstellung den Standardwert 150 beizubehalten.
- 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-Werte für DB_POOLSIZE + 10 betragen, die für jeden Acronis Cyber Files Web Server festgelegt wurden, zum Beispiel 510 für 2 Tomcat-Server und 760 für 3 Tomcat-Server usw.

Hinweis
An diesen Dateien vorgenommene Änderungen erfordern einen Neustart der entsprechenden Dienste.

Konfigurieren einer ordnungsgemäßen Protokollierung

In einer Konfiguration mit Lastenausgleich ordnet der Acronis Cyber Files-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 &quot;%r&quot; %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 Acronis Cyber Files-Tomcat-Dienst anschließend neu.

Installieren von Gateway-Servern

Einen neuen Gateway-Server installieren

1. Führen Sie auf einem neuen Computer das Acronis Cyber Files-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.

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 Acronis Cyber Files 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 lautet: `C:\ProgramData\Acronis\Acronis Cyber Files\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.

   Hinweis
   Das Konto benötigt auch Lese- und Schreibzugriff auf den lokalen Repository-Ordner (z. B. C:\Programme (x86)\Acronis\Access\File Repository\Repository), um in das Protokoll zu schreiben.

8. Starten Sie den Acronis Cyber Files-Datei-Repository-Dienst.

Acronis Cyber Files-Einstellungen

1. Öffnen Sie die Weboberfläche von Acronis Cyber Files, 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.

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 und 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.

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 Acronis Cyber Files 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 Acronis Cyber Files, das in einer Standardbereitstellung ausgeführt wird, wobei alle Komponenten auf demselben Computer installiert sind.

Hinweis
In unserem Beispiel setzen wir den ursprünglichen Acronis Cyber Files-Tomcat-Dienst fort und verknüpfen ihn mit der neuen Konfiguration. Dies ist nicht obligatorisch.

Lesen Sie unsere Artikel Backup & Recovery, bevor Sie Änderungen an unserer Bereitstellung vornehmen.

Systemanforderungen

Hardwareanforderungen

In einer Produktionsumgebung empfehlen wir Ihnen die Verwendung von mindestens drei (3) Acronis Cyber Files 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 Servern empfehlen wir die Verwendung von Interconnects mit geringer Latenz zwischen den Gast-Virtual Machines.

- 1 Lastenausgleichsmodul für die Acronis Cyber Files Web-Server.
- 1 Lastenausgleichsmodul für die Acronis Cyber Files Gateway-Server.
- 3 Acronis Cyber Files Tomcat-Server, jeweils mit 32 GB RAM und einer 16-Kern-CPU.
- 3 Acronis Cyber Files 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 File Repository-Dienst + File Store. Die Parameter dieses Servers sind nicht besonders wichtig.

Netzwerkverbindungen

- Der Lastenausgleich für die Acronis Cyber Files Tomcat Server muss so konfiguriert werden, dass die DNS-Adresse des aktuellen Acronis Cyber Files-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 Administration und Gateway Server der Acronis Cyber Files-Webbenutzeroberfläche ist 'Adresse für Clientverbindungen' die Adresse des externen Lastenausgleichs. Für die Gateway Server verwenden wir auch die Einstellung 'Alternative Adresse für Acronis Cyber Files Server-Verbindungen verwenden', und in 'Adresse für Verbindungen des Acronis Cyber Files Web Server ist die interne Adresse des Gateway-Lastenausgleichs.

- Der Gateway Server muss mit dem Tomcat-Lastenausgleich für die mobilen Clientverbindungen verbunden werden.

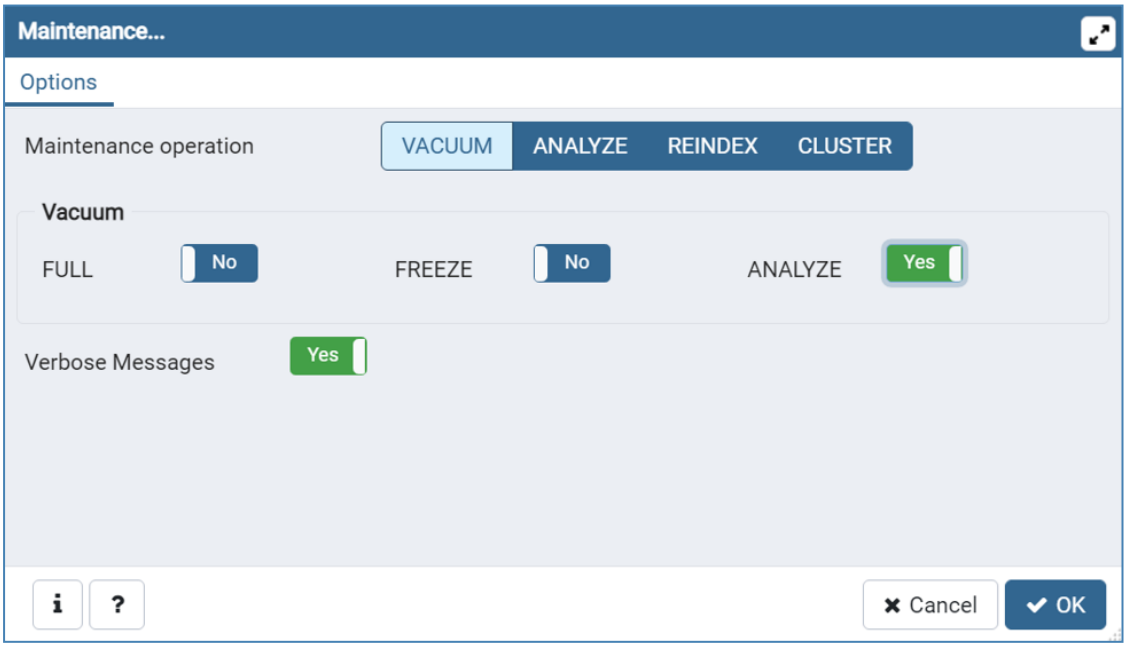
Hinweis
Für die Sync&Share-Datenquelle müssen Sie die Adresse zur Adresse des Tomcat-Lastenausgleichs ändern.

Migrieren des PostgreSQL Servers

Ihre Datenbank ist die wichtigste Komponente und muss zuerst migriert werden.

Konfiguration auf Ihrem vorhandenen PostgreSQL Server

1. Öffnen Sie die Systemsteuerung **Dienste** (`services.msc`), und stoppen Sie **AcronisCyber Files Tomcat**.
2. Öffnen Sie die **PostgreSQL Administrator-Applikation vonAcronisCyber Files**, und stellen Sie eine Verbindung zum Datenbankserver her. Klicken Sie auf **+** neben **Datenbanken**.
3. Klicken Sie mit der rechten Maustaste auf die Datenbank `acronisaccess_production`.
4. Wählen Sie **Maintenance**.
5. Wählen Sie **BEREINIGEN** und legen Sie **ANALYSIEREN** mit 'Ja' fest.



6. Klicken Sie auf **OK**.

7. 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`).
8. 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 ist die generierte Backup-Datei und wird im Ordner **bin** 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.

9. Sobald das Backup abgeschlossen ist, stoppen und deaktivieren Sie den **Acronis Cyber Files PostgreSQL Server**-Dienst.
10. 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 Acronis Cyber Files, 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 PostgreSQL-Ordner **data** (standardmäßig unter `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\PostgreSQL\<version>\Data`), und öffnen Sie die Datei `pg_hba.conf` in 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 Datei `pg_hba.conf` ('HBA' steht für 'host-basierte Authentifizierung') steuert die Clientauthentifizierung 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 (Erster Acronis Cyber Files & 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 **replication**) über eine mit `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 `*`. Dies muss nun wie folgt aussehen: `listen_addresses = '*'`
2. Entfernen Sie das vorangestellte # aus der folgenden Zeile: `#effective_cache_size = 128MB`, und ersetzen Sie **128MB** durch **12GB**. Dies sollte wie folgt aussehen: `effective_cache_size = 12GB`
3. Ergänzen Sie 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` in den korrekten Wert. Dieser sollte nicht geringer als alle Tomcat-Einstellungen für `DB_POOLSIZE` sein, die für jeden Access Server-Knoten + 10 konfiguriert sind. Wir empfehlen die Einstellung von `DB_POOLSIZE` auf `250`.

   In unserem Beispiel haben wir `DB_POOLSIZE to 250` festgelegt, und wir haben zwei Access Tomcat Server, sodass `max_connections` auf `510` festgelegt werden sollte. Für drei Access Tomcat Server wäre dies `760`.
5. Speichern und schließen Sie die Datei **postgresql.conf**.
6. Starten Sie den Acronis Cyber Files-PostgreSQL Server-Dienst neu.

Importieren Ihrer Datenbank

Auf den neuen PostgreSQL Server

1. Öffnen Sie die PostgreSQL Administrator-Applikation von Acronis Cyber Files, 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\Acronis Cyber Files\Common\PostgreSQL\<version>\bin`)
3. Öffnen Sie ein Fenster für die Eingabeaufforderung mit erweiterten Benutzerrechten und navigieren Sie mit dem Befehl **cd** zum PostgreSQL **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.

Acronis Cyber Files-Serverkonfigurationen

Verbinden zusätzlicher Acronis Cyber Files Server

Nur den Acronis Cyber Files-Web-Server installieren

1. Starten Sie das Acronis Cyber Files-Installationsprogramm, und akzeptieren Sie die Lizenzvereinbarung.
2. Wählen Sie **Benutzerdefiniert** aus, und wählen Sie NUR den Acronis Cyber Files Web Server aus.

   Hinweis
   Durch Klicken auf den Acronis Cyber Files Web Server 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 Acronis Cyber Files Tomcat-Dienst angehalten wurde.

Serverkonfiguration

Alle Einstellungen, die Sie auf einem Acronis Cyber Files Web Server ändern, müssen auch auf allen anderen Acronis Cyber Files Web Servern geändert werden.

Hinweis
Vergessen Sie nicht, einen Eintrag in der Datei `pg_hba.conf` für jeden Acronis Cyber Files Web Server vorzunehmen!

Konfigurieren des Servers zur Verbindung mit der richtigen Datenbank

1. Navigieren Sie zum Ordner des Acronis Cyber Files Web Server (standardmäßig `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 festzulegen.

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, für diese Einstellung den Standardwert 150 beizubehalten.
- 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-Werte für DB_POOLSIZE + 10 betragen, die für jeden Acronis Cyber Files Web Server festgelegt wurden, zum Beispiel 510 für 2 Tomcat-Server und 760 für 3 Tomcat-Server usw.

Hinweis
An diesen Dateien vorgenommene Änderungen erfordern einen Neustart der entsprechenden Dienste.

Konfigurieren einer ordnungsgemäßen Protokollierung

In einer Konfiguration mit Lastenausgleich ordnet der Acronis Cyber Files-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"/>
   ```

Warnung!
Wenn zudem die Funktion für IP-Adresseinschränkungen verwendet wird, wird empfohlen, den XFF-Header nicht festzulegen, da sich dies auf die Benutzersicherheit auswirken kann, welche mit dieser Funktion zusammenhängt. Stattdessen wird empfohlen, die Lastverteilung so zu konfigurieren, dass sie XFF-Adressen vertraut, die von einem Proxy hinzugefügt werden. In diesem Fall wird der XFF-Header aus den Anforderungen ebenfalls kopiert (falls zutreffend).

4. Speichern Sie die Datei, und starten Sie den Acronis Cyber Files-Tomcat-Dienst anschließend neu.

Herstellen einer Verbindung zum alten Acronis Cyber Files-Server

Wenn Sie Ihren vorhandenen Acronis Cyber Files-Server weiterhin verwenden möchten, können Sie dies tun. Hierfür müssen Sie jedoch eine Verbindung zur neuen Datenbank herstellen.

Verbinden von Acronis Cyber Files mit der Remote-Datenbank

1. Navigieren Sie zum Ordner des Acronis Cyber Files Server (standardmäßig `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 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 **Acronis Cyber Files Tomcat-Dienst** in der Systemsteuerung **Dienste** (services.msc).
4. Alle nicht verwendeten Acronis Cyber Files-Komponenten können deinstalliert werden.

Migration von Dateispeicher und Datei-Repository

Lesen Sie unsere Anleitung Verschieben von Dateispeicher und Datei-Repository. Die einzige zusätzliche Einstellung, die Sie ggf. überprüfen müssen, ist, dass alle Acronis Cyber Files-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 Acronis Cyber Files-Server auf den richtigen Repository-Endpunkt verweisen.

Ihren Gateway-Server migrieren

Einen neuen Gateway-Server installieren

1. Führen Sie auf einem neuen Computer das Acronis Cyber Files-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 -

1. Öffnen Sie auf dem alten Computer mit Tomcat sowie dem Gateway die Acronis Cyber Files-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 ... Server-Verbindungen verwenden**', und geben Sie unter '**Adresse für Acronis Cyber Files -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 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.

Log-Verwaltung und Bereinigung

Stellen Sie nach der Installation zusätzlicher AcronisCyber Files-Server sicher, dass Sie den Ordner öffnen, in dem sich AcronisCyber Files-Tomcat-Logs befinden, und stellen Sie für diese Ordner die korrekten Berechtigungen ein, sodass Logs geschrieben und bereinigt werden können.

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 und 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.

Ursprüngliche(n) Server bereinigen

Wenn Sie Acronis Cyber Files Tomcat weiterhin verwenden, d.h. auf dem ursprünglichen Produktionsserver, empfehlen wir, dass Sie die Acronis Cyber Files-Elemente deinstallieren, die auf diesem Server nicht mehr verwendet werden.

Über die Systemsteuerung können Sie den Acronis Cyber Files PostgreSQL Server, den Acronis Cyber Files Gateway Server und den Acronis Cyber Files File Repository Server (falls vorhanden) deinstallieren.

Anpassen der Weboberfläche über die API

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 AcronisCyber Files 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
   Stellen Sie sicher, dass Sie eine Version herunterladen, 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_des_Schemas>**.css für die Administrationskonsole und `web_client_`<**Name_des_Schemas>**.scss für die Web-Client-Konsole. <**<Name_des_Schemas>** ist der Name Ihres neuen Schemas, das auf der Acronis Cyber Files-Oberfläche angezeigt wird und 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_client_NewColor.scss -u administrator:123456
https://myCompany.com/api/v1/settings/customization
```

4. Sie können auch den Befehl `-F customization_settings[color_scheme]=<Schemaname>` zum Umschalten zwischen Ihrem aktuellen Design und dem neuen Design, das Sie hinzufügen, verwenden. Wird dieser Befehl zum Rest hinzugefügt, sieht dies 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_client_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.

Unbeaufsichtigte Desktop-Client-Konfiguration

Mit der Gruppenrichtlinienverwaltung von Microsoft können Sie auf einfache Weise eine Remote-Installation und -Einrichtung des Acronis Cyber Files-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 Domain-Controller die **Gruppenrichtlinien-Verwaltungskonsole**.
2. Klicken Sie mit der rechten Maustaste auf die gewünschte Domain, 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, Domains, Organisationseinheiten, Gruppen, Benutzer bzw. Computer aus.

Unbeaufsichtigte Installation des Clients

Dieser Abschnitt hilft Ihnen dabei, den Acronis Cyber Files-Desktop-Client bei der Benutzeranmeldung auf allen gewünschten Computern im Verborgenen zu installieren.

Erstellen eines Verteilungspunkts für das Installationsprogramm

Alle Computer, auf denen der Client installiert wird, müssen auf das Installationsprogramm zugreifen können. Erstellen Sie hierzu einen Ordner, geben Sie ihn für die gewünschte Benutzergruppe frei, und legen Sie das Installationsprogramm in diesem Ordner ab.

1. Klicken Sie mit der rechten Maustaste auf den Ordner mit dem Installationsprogramm, und wählen Sie **Eigenschaften**.
2. Öffnen Sie die Registerkarte **Freigeben**, und wählen Sie **Teilen**.
3. Geben Sie die Domain-Gruppe, 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 das Installationsprogramm zugreifen können.

Übertragen des Installationsprogramms auf den Benutzercomputer

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 Installationsprogramm 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 das Installationsprogramm 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 das Client-Installationsprogramm im Laufwerk **C** im Ordner 'Folder' des Benutzers platziert und **DieseDatei.msi** genannt.

7. Drücken Sie **OK**.

Installieren des Clients

Erstellen des Installationsskripts

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.

Verwenden des Skripts bei der Benutzeranmeldung

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 Acronis Cyber Files-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. Geben Sie für **Wertname** '**Benutzername**' ein.
   b. Wählen Sie für **Werttyp** die Option **REG_SZ**.
   c. Geben Sie für **Wertdaten** das folgende Token ein: `%USERNAME%@%USERDOMAIN%`.

   Hinweis
   Wenn Sie **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. Geben Sie für **Wertname** '**Server-URL**' ein.
   b. Wählen Sie für **Werttyp** die Option **REG_SZ**.
   c. Geben Sie für **Wertdaten** die Adresse Ihres Acronis Cyber Files-Servers ein, z.B. **https://myaccess.com**.
8. Für den Synchronisierungsordner:
   a. Geben Sie für **Wertname** '**activEcho-Ordner**' ein.
   b. Wählen Sie für **Werttyp** die Option **REG_SZ**.
   c. Geben Sie für **Wertdaten** das folgende Token und den folgenden Pfad ein: `%USERPROFILE%\Desktop\AAS Data Folder`.
9. Für das Auto-Update:
   a. Geben Sie für **Wertname** '**AutoCheckForUpdates**' ein.
   b. Wählen Sie für **Werttyp** die Option **DWORD**.

c. Geben Sie für **Wertdaten** '**00000001**' ein. 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. Geben Sie für **Wertname** '**AllowInvalidCertificates**' ein.
    b. Wählen Sie für **Werttyp** die Option **DWORD**.
    c. Geben Sie für **Wertdaten** '**00000000**' ein. Mit dem Wert **0** wird diese Einstellung deaktiviert, und der Client kann keine Verbindung mehr zu Acronis Cyber Files-Servern mit ungültigen Zertifikaten herstellen. Wenn der Wert auf **1** festgelegt wird, wird die Einstellung aktiviert.

Konfigurieren von Single Sign-On

Dieser Leitfaden führt Sie durch eine erweiterte Konfiguration, um die Funktion Single Sign-On für Acronis Cyber Files zu aktivieren.

Hinweis
Single Sign-On kann nur in einer funktionierenden Domain verwendet werden.

Hinweis
Single Sign-On funktioniert **NICHT**, wenn Sie Acronis Cyber Files in einer Konfiguration mit nur einem Port verwenden (wenn der Gateway Server als Proxy für die Acronis Cyber Files Server-Anforderungen fungiert).

Hinweis
Single Sign-On funktioniert **NICHT**, wenn Acronis Cyber Files auf dem Domain-Controller installiert ist. Ganz abgesehen von den SSO-Beschränkungen empfehlen wir auch aus Leistungsgründen dringend, den Acronis Cyber Files Server nicht auf dem Domain-Controller 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 Acronis Cyber Files-Konto verfügen, oder die LDAP-Bereitstellung muss auf dem Server aktiviert sein.

- Acronis Cyber Files 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 Acronis Cyber Files mithilfe des FQDN (z.B. https://access.company.com) öffnen, damit SSO funktioniert. Single Sign-On funktioniert **NICHT**, wenn Sie die Oberfläche über eine IP-Adresse öffnen.

  UPNs und das SSO-Hauptsetup sollten sich in derselben Domain befinden, damit Benutzer in mobilen Anwendungen per KCD auf ihren Sync & Share-Ordner zugreifen können.

- Für den Desktop Client steht ein neues Aktionsfeld zur Aktivierung von SSO zur Verfügung. Benutzer müssen nur die URL des Acronis Cyber Files-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 einer späteren Version zur Verfügung stehen.

  Hinweis
  Für einmaliges Anmelden über einen Desktop Client ist der Zugriff auf das Unternehmensnetzwerk erforderlich. Dies bedeutet, dass SSO-Benutzer zudem Zugriff auf das eigene Netzwerk haben sollten.

Acronis Cyber Files-Web-Server und -Gateway auf demselben Computer

Diese Konfiguration ist die gebräuchlichste und besteht aus 1 Acronis Cyber Files-Web-Server und 1 Acronis Cyber Files-Gateway-Server, die beide auf demselben Computer gehostet sind. Dies ist die standardmäßige Installation.

In der Domain

Dies ist ein einmaliger Schritt, der für die Registrierung des Acronis Cyber Files Web Server für den Kerberos-Server in der Domain 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, darf der DNS-Eintrag für den Acronis Cyber Files Web Server **nicht** mit dem Namen des Computers identisch sein. Wenn der SPN des Acronis Cyber Files Web Server nur im Namen des Computers enthalten ist, behandelt der Gateway-Server den Acronis Cyber Files Web Server, als wäre er auf seinem Gerät installiert, und versucht daher keine Kerberos-Authentifizierung.
Beispiel: `computerAccess.domain.com/computer.domain.com` und `computerAccess.domain.com/computerGW.domain.com` funktioniert und `computer.domain.com/computerGW.domain.com` funktioniert NICHT.

Konfigurieren des LDAP-Kontos für SSO

Hinweis
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. Weitere Informationen finden Sie im Artikel Erweiterte Delegierungskonfigurationen.

1. Öffnen Sie eine Eingabeaufforderung.

   Hinweis
   Sie müssen mit einem Domain-Konto angemeldet sein und über die Rechte zur Verwendung von **setspn** verfügen.

2. Befehl `setspn -s HTTP/`**computername.domain.com account name** eingeben
   Beispiel: Wenn Ihr Acronis Cyber Files Web Server auf `ahsoka.acme.com` installiert ist und und Sie `john@acme.com` als vorab authentifiziertes LDAP-Konto verwenden wollen, um Kerberos-Tickets gewähren zu können, sieht der Befehl folgendermaßen aus:
   `setspn -s HTTP/ahsoka.acme.com john`

   Hinweis
   Der im voranstehenden Befehl verwendete LDAP-Kontoname **MUSS** mit dem von der Eigenschaft `spnego.preauth.username` in `web.xml` festgelegten Konto übereinstimmen.

   Hinweis
   Dieses Konto entspricht in der Regel dem vom Administrator in der Acronis Cyber Files-Weboberfläche unter **Allgemeine Einstellungen** -> **LDAP** -> **LDAP-Benutzername**/**LDAP-Kennwort** angegebenen Konto. Dies ist jedoch nicht zwingend der Fall.

3. Wird Ihr Acronis Cyber Files Web Server auf einem nicht standardmäßigen Port (d.h., einem anderen Port als 443) ausgeführt, sollten Sie auch einen SPN mit der Portnummer registrieren.
   Beispiel: Wird Ihr Server auf Port 444 ausgeführt, lautet der Befehl folgendermaßen:
   `setspn -s HTTP/ahsoka.acme.com:444 john`

   Hinweis
   HTTPin 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. Ermitteln Sie den in den voranstehenden Befehlen verwendeten Benutzer (was in diesem Beispiel **john** ist).
6. Klicken Sie auf die Registerkarte **Delegierung** und wählen Sie **Diesem Benutzer für die Delegierung an jeden beliebigen Dienst trauen (nur Kerberos)** aus.
7. Drücken Sie **OK**.

Konfigurieren des SPN für den Gateway Server

Damit das KDC ('Key Distribution Center') Kerberos-Server Benutzer beim Gateway-Server authentifizieren kann, muss der Gateway-Dienst beim KDC-Server registriert werden. Hierzu

müssen 'setspn' ausgeführt und der Hostname des Servers, auf dem er ausgeführt wird, als 'user' im setspn-Befehl angegeben werden.

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 Domain, 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.

   z.B. `ahsoka-gw.acme.com`
3. Geben Sie die IP-Adresse des Gateway Server ein (ohne den Port). Wenn Sie das Gateway und den Acronis Cyber Files Server unter derselben IP-Adresse ausführen, geben Sie diese IP-Adresse ein.
4. Wählen Sie **Zugewiesenen Pointer-Datensatz (PTR) erstellen**, und drücken Sie **Host hinzufügen**.
5. Wechseln Sie zurück zum Computer mit Acronis Cyber Files.
6. Öffnen Sie die Eingabeaufforderung.
7. Geben Sie den folgenden **setspn**-Befehl ein: `setspn -s HTTP/`**gatewaydns.domain.com computername**

   Wenn Ihr Gateway Server beispielsweise auf dem Host `'ahsoka'` in einer Domain läuft und Ihr DNS-Eintrag `ahsoka-gw.acme.com` lautet, führen Sie folgenden Befehl aus:

   ```
   setspn -s HTTP/ahsoka-gw.acme.com ahsoka
   ```
8. Wird Ihr Gateway-Server nicht auf einem Standard-Port ausgeführt (d.h. auf einem anderen Port als 443), müssen Sie auch einen SPN mit der Portnummer registrieren, z.B. dann, wenn Ihr Gateway-Server auf Port 444 ausgeführt wird:

   ```
   setspn -s HTTP/ahsoka-gw.acme.com:444 ahsoka
   ```
9. Ändern Sie die gewünschte **Adresse für Administration** und **Adresse für Clientverbindungen** des Gateway Server in den DNS-Eintrag des neuen Gateway Server, den Sie in Schritt 4 erstellt haben.

Hinweis
Die Adressen sollten identisch und in den richtigen DNS-Eintrag geändert worden sein.

Auf dem Acronis Cyber Files-Server

Festlegen des Domain-Kontos für eine SSO-Authentifizierung

1. Zu `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Access Server\Web Application\WEB-INF\` navigieren
2. Suchen und öffnen Sie die Datei `web.xml`. In dieser Datei geben Sie den Benutzernamen und das Kennwort für die Domain an, unter der der SSO-Dienst ausgeführt wird. Das Konto **muss** mit

dem Konto übereinstimmen, das Sie im Abschnitt **In der Domain** 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 Domain und das zugehörige Kennwort. Suchen Sie folgende Zeilen:

```
<init-param>
<param-name>spnego.preauth.username</param-name>
<param-value>yourusername</param-value>
</init-param>
<init-param>
<param-name>spnego.preauth.password</param-name>
<param-value>yourpassword</param-value>
</init-param>
```

4. Ersetzen Sie **yourusername** durch den gewünschten LDAP-Benutzernamen.
5. Ersetzen Sie **yourpassword** durch das LDAP-Kennwort für das zuvor angegebene LDAP-Konto. Wenn Ihr Kennwort eines der fünf folgenden Sonderzeichen enthält (**&**, **>**, **"**, ' oder **<**), 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 wie folgt in der Datei `web.xml` schreiben: `<my&best&apos;password&quot;`

Festlegen der Kerberos-Domain-Suche

1. Zu `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\apache-tomcat-7.0.59\conf` navigieren
2. Datei `krb5.conf` suchen und öffnen
3. In `krb5.conf` gibt es nur zwei Eigenschaften, die der Administrator angeben muss:
   a. Domain für Single Sign-On (z.B. `ACME.COM`). Beachten Sie, dass es sich um den Namen Ihrer Domain handelt, **nicht** um den DNS-Namen des Servers.

   Hinweis
   Die Domain in `krb5.conf` muss immer in **GROSSBUCHSTABEN** angegeben werden. Andernfalls schlagen Suchen nach Kerberos-Tickets möglicherweise fehl.

   b. Adresse des Kerberos Key Distribution Centers (entspricht üblicherweise der Adresse Ihres primären Domain-Controllers, z.B. `acmedc.ACME.COM`)

4. Die von uns installierte Datei `krb5.conf` 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 Domain (in **Großbuchstaben!**). Beachten Sie, dass es sich um den Namen Ihrer Domain handelt, **nicht** um den DNS-Namen des Servers.
6. Ersetzen Sie den Wert für "`kdc =`" durch den Namen Ihres Domain-Controllers. Die Domain muss in Großbuchstaben angegeben werden, z.B. `kdc = yourdc.YOURDOMAIN.COM`.
7. Nach der Aktualisierung der oben genannten Konfigurationsdateien muss der Acronis Cyber Files-Server (Acronis Cyber Files Tomcat) neu gestartet werden, damit die Änderungen wirksam werden.

Single Sign-On in der Weboberfläche aktivieren:

1. Öffnen Sie die Weboberfläche von Acronis Cyber Files, 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 Web-Client und Desktop-Sync-Client mit vorhandenen Windows-/Mac-Anmeldedaten erlauben**.
4. Klicken Sie auf **Speichern**.

Hinzufügen weiterer Gateway Server

Hinweis
Diese Schritte können nur durchgeführt werden, wenn sich die Computer, welche die Gateway Server hosten, in derselben Domain befinden wie der Acronis Cyber Files Web Server.

Damit das KDC ('Key Distribution Center') Kerberos-Server Benutzer beim Gateway-Server authentifizieren kann, muss der Gateway-Dienst beim KDC-Server registriert werden. Hierzu müssen 'setspn' ausgeführt und der Hostname des Servers, auf dem er ausgeführt wird, als 'user' im setspn-Befehl angegeben werden.

Gateway Server, die auf anderen Computern als dem Acronis Cyber Files Web Server gehostet werden

1. Öffnen Sie die Eingabeaufforderung.
2. Geben Sie den folgenden **setspn**-Befehl ein: `setspn -s HTTP/`**computername.domain.com computername**

   Führen Sie beispielsweise für den Fall, dass Ihr Gateway-Server auf Host `'cody'` in der Domain ausgeführt wird, folgenden Befehl aus:

   ```
   setspn -s HTTP/cody.acme.com cody
   ```
3. Wird Ihr Gateway-Server nicht auf einem Standard-Port ausgeführt (d.h. auf einem anderen Port als 443), müssen Sie auch einen SPN mit der Portnummer registrieren, z.B. dann, wenn Ihr Gateway-Server auf Port 444 ausgeführt wird:

   ```
   setspn -s HTTP/cody.acme.com:444 cody
   ```
4. Wiederholen Sie diesen Abschnitt für alle weiteren Gateway-Server.

Browser für Einmalanmeldung (Single-Sign-On, SSO) konfigurieren

Hierbei handelt es sich um eine kleine, einmalige Konfiguration zur Aktivierung der Single Sign-On-Unterstützung für den Browser.

Wichtig
Sie muss für jeden Benutzer auf jedem Computer ausgeführt werden.

Hinweis
In den Konfigurationsanweisungen verwenden wir *acme.com* als Beispiel. Wenn Sie Services in mehreren Domains haben, wiederholen Sie die Schritte, die *acme.com* spezifizieren, für alle Ihre Domains. (**z.B.** fügen Sie `*.acme.com` und `*.another.com` und `*.yetanother.com` hinzu).

Acronis Cyber Files-Server und -Gateway auf unterschiedlichen Computern

In der Domain

Dies ist ein einmaliger Schritt, der für die Registrierung von Acronis Cyber Files Server für den Kerberos-Server in der Domain 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, darf der DNS-Eintrag für den Acronis Cyber Files-Web-Server **nicht** mit dem Namen des Computers identisch sein. Wenn der SPN des Acronis Cyber Files Web Server nur im Namen des Computers enthalten ist, behandelt der Gateway-Server den Acronis Cyber Files Web Server, als wäre er auf seinem Gerät installiert, und versucht daher keine Kerberos-Authentifizierung.
Beispiel:
`computerAccess.domain.com/computer.domain.com` und
`computerAccess.domain.com/computerGW.domain.com` funktioniert und
`computer.domain.com/computerGW.domain.com` funktioniert NICHT.

Konfigurieren des LDAP-Kontos für SSO

Hinweis
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. Weitere Informationen finden Sie im Artikel Erweiterte Delegierungskonfigurationen.

1. Öffnen Sie eine Eingabeaufforderung.

   Hinweis
   Sie müssen mit einem Domain-Konto angemeldet sein und über die Rechte zur Verwendung von **setspn** verfügen.

2. Befehl `setspn -s HTTP/`**computername.domain.com account name** eingeben
   Beispiel: Wenn Ihr Acronis Cyber Files Server auf `ahsoka.acme.com` installiert ist und und Sie `john@acme.com` als vorab authentifiziertes LDAP-Konto verwenden wollen, um Kerberos-Tickets gewähren zu können, sieht der Befehl folgendermaßen aus:
   `setspn -s HTTP/ahsoka.acme.com john`

   Hinweis
   Der im voranstehenden Befehl verwendete LDAP-Kontoname **MUSS** mit dem von der Eigenschaft `spnego.preauth.username` in `web.xml` festgelegten Konto übereinstimmen.

   Hinweis
   Dieses Konto entspricht in der Regel dem vom Administrator in der Acronis Cyber Files-Weboberfläche unter **Allgemeine Einstellungen** -> **LDAP** -> **LDAP-Benutzername**/**LDAP-Kennwort** angegebenen Konto. Dies ist jedoch nicht zwingend der Fall.

3. Wird Ihr Acronis Cyber Files-Server auf einem nicht standardmäßigen Port (d.h., einem anderen Port als 443) ausgeführt, sollten Sie auch einen SPN mit der Portnummer registrieren.
   Beispiel: Wird Ihr Server auf Port 444 ausgeführt, lautet der Befehl folgendermaßen:

```
setspn -s HTTP/ahsoka.acme.com:444 john
```

Hinweis
HTTPin 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. Ermitteln Sie den in den voranstehenden Befehlen verwendeten Benutzer (was in diesem Beispiel **john** ist).
6. Klicken Sie auf die Registerkarte **Delegierung** und wählen Sie **Diesem Benutzer für die Delegierung an jeden beliebigen Dienst trauen (nur Kerberos)** aus.
7. Drücken Sie **OK**.

Konfigurieren des SPN für den Gateway Server

Damit das KDC ('Key Distribution Center') Kerberos-Server Benutzer beim Gateway-Server authentifizieren kann, muss der Gateway-Dienst beim KDC-Server registriert werden. Hierzu müssen 'setspn' ausgeführt und der Hostname des Servers, auf dem er ausgeführt wird, als 'user' im setspn-Befehl angegeben werden.

Gateway Server, die auf anderen Computern als dem Acronis Cyber Files Server gehostet werden

1. Öffnen Sie die Eingabeaufforderung.
2. Geben Sie den folgenden **setspn**-Befehl ein: `setspn -s HTTP/`**computername.domain.com computername**
   Führen Sie beispielsweise für den Fall, dass Ihr Gateway-Server auf Host `'cody'` in der Domain ausgeführt wird, folgenden Befehl aus:
   ```
   setspn -s HTTP/cody.acme.com cody
   ```
3. Wird Ihr Gateway-Server nicht auf einem Standard-Port ausgeführt (d.h. auf einem anderen Port als 443), müssen Sie auch einen SPN mit der Portnummer registrieren, z.B. dann, wenn Ihr Gateway-Server auf Port 444 ausgeführt wird:
   ```
   setspn -s HTTP/cody.acme.com:444 cody
   ```
4. Wiederholen Sie diesen Abschnitt für alle Gateway-Server.

Gateway Server auf demselben Computer wie der Acronis Cyber Files Server

Dies ist nur erforderlich, wenn der Gateway Server auf demselben Computer wie der Acronis Cyber Files 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 Domain, 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.

   z.B.`codygw.acme.com`
3. Geben Sie die IP-Adresse des Gateway Server ein (ohne den Port). Wenn Sie das Gateway und den Acronis Cyber Files Server unter derselben IP-Adresse ausführen, geben Sie diese IP-Adresse ein.
4. Wählen Sie **Zugewiesenen Pointer-Datensatz (PTR) erstellen**, und drücken Sie **Host hinzufügen**.
5. Wechseln Sie zurück zum Computer mit Acronis Cyber Files.
6. Öffnen Sie die Eingabeaufforderung.
7. Geben Sie den folgenden **setspn**-Befehl ein: `setspn -s HTTP/`**gatewaydns.domain.com computername**

   Wenn Ihr Gateway Server beispielsweise auf dem Host `'cody'` in einer Domain läuft und Ihr DNS-Eintrag `codygw.acme.com` lautet, führen Sie folgenden Befehl aus:

   ```
   setspn -s HTTP/codygw.acme.com cody
   ```
8. Wird Ihr Gateway-Server nicht auf einem Standard-Port ausgeführt (d.h. auf einem anderen Port als 443), müssen Sie auch einen SPN mit der Portnummer registrieren, z.B. dann, wenn Ihr Gateway-Server auf Port 444 ausgeführt wird:

   ```
   setspn -s HTTP/codygw.acme.com:444 cody
   ```
9. Falls nicht bereits geschehen, müssen Sie die **Adresse für die Administration** Ihres gewünschten Gateway Server in den in Schritt 4 erstellten Gateway Server-DNS-Eintrag ändern.

Auf dem Acronis Cyber Files-Server

Datei `web.xml` bearbeiten:

1. Zu `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Access server\Web Application\WEB-INF\` navigieren
2. Suchen und öffnen Sie die Datei `web.xml`. In dieser Datei geben Sie den Benutzernamen und das Kennwort für die Domain an, unter der der SSO-Dienst ausgeführt wird. Das Konto **muss** mit dem Konto übereinstimmen, das Sie im Abschnitt **In der Domain** 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 Domain und das zugehörige Kennwort. Suchen Sie folgende Zeilen:

   ```
   <init-param>
     <param-name>spnego.preauth.username</param-name>
     <param-value>yourusername</param-value>
   ```

```
</init-param>
<init-param>
<param-name>spnego.preauth.password</param-name>
<param-value>yourpassword</param-value>
</init-param>
```

4. Ersetzen Sie **yourusername** durch den gewünschten LDAP-Benutzernamen.
5. Ersetzen Sie **yourpassword** durch das LDAP-Kennwort für das zuvor angegebene LDAP-Konto. Wenn Ihr Kennwort eines der fünf folgenden Sonderzeichen enthält (**&**, **>**, **"**, ' oder **<**), 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 wie folgt in der Datei `web.xml` schreiben: `<my&best&apos;password&quot;`

Datei `krb5.conf` bearbeiten:

1. Zu `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\apache-tomcat-7.0.59\conf` navigieren
2. Datei `krb5.conf` suchen und öffnen
3. In `krb5.conf` gibt es nur zwei Eigenschaften, die der Administrator angeben muss:
   a. Domain für Single Sign-On (z.B. `ACME.COM`)

   Hinweis
   Die Domain in `krb5.conf` muss immer in **GROSSBUCHSTABEN** angegeben werden. Andernfalls schlagen Suchen nach Kerberos-Tickets möglicherweise fehl.

   b. Adresse des Kerberos Key Distribution Centers (entspricht üblicherweise der Adresse Ihres primären Domain-Controllers, z.B. `acmedc.ACME.COM`)
4. Die von uns installierte Datei `krb5.conf` 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 Domain (in **Großbuchstaben!**).
6. Ersetzen Sie den Wert für "`kdc =`" durch den Namen Ihres Domain-Controllers. Die Domain muss in Großbuchstaben angegeben werden, z.B. `kdc = yourdc.YOURDOMAIN.COM`.
7. Nach der Aktualisierung der oben genannten Konfigurationsdateien muss der Acronis Cyber Files-Server (Acronis Cyber Files Tomcat) neu gestartet werden, damit die Änderungen wirksam werden.

Single Sign-On in der Weboberfläche aktivieren:

1. Öffnen Sie die Weboberfläche von Acronis Cyber Files, 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 Web-Client und Desktop-Sync-Client mit vorhandenen Windows-/Mac-Anmeldedaten erlauben**.
4. Klicken Sie auf **Speichern**.

Browser für Einmalanmeldung (Single-Sign-On, SSO) konfigurieren

Hierbei handelt es sich um eine kleine, einmalige Konfiguration zur Aktivierung der Single Sign-On-Unterstützung für den Browser.

Wichtig
Sie muss für jeden Benutzer auf jedem Computer ausgeführt werden.

Hinweis
In den Konfigurationsanweisungen verwenden wir *acme.com* als Beispiel. Wenn Sie Services in mehreren Domains haben, wiederholen Sie die Schritte, die *acme.com* spezifizieren, für alle Ihre Domains. (**z.B.** fügen Sie `*.acme.com` und `*.another.com` und `*.yetanother.com` hinzu).

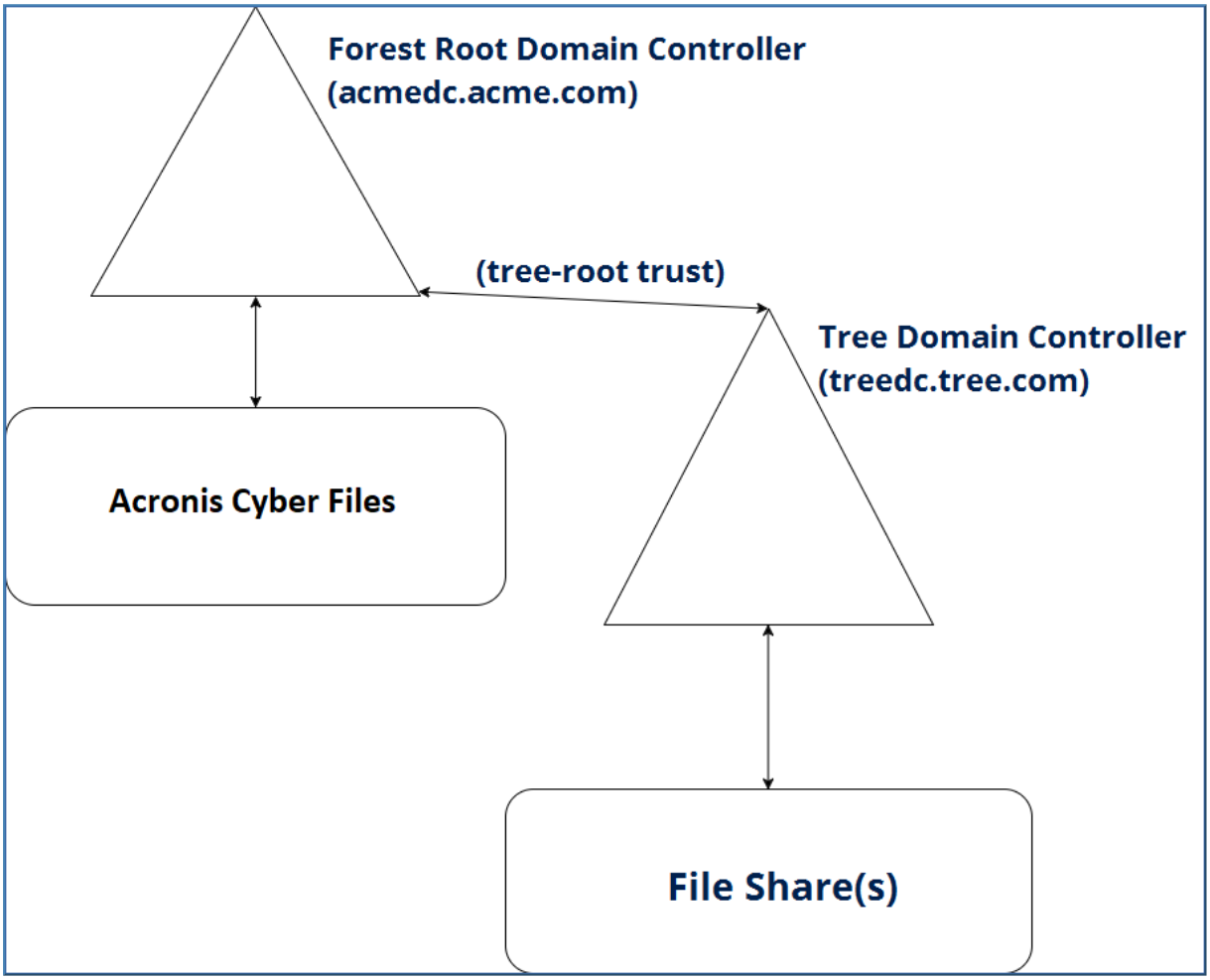
Acronis Cyber Files in einer Domänengesamtstruktur

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 Acronis Cyber Files 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.



Anforderungen

Diese Anleitung ist für die Konfiguration in mehreren Domains in einer einzigen Gesamtstruktur bestimmt. Es wird daher vorausgesetzt, dass LDAP ordnungsgemäß konfiguriert wurde, dass Benutzer sich an der Domain problemlos anmelden können und dass die Konnektivität zwischen den Domains in der Gesamtstruktur ordnungsgemäß konfiguriert wurde.

- Dieser Typ der eingeschränkten Delegierung ist nur bei Domain-Controllern verfügbar, die mindestens in der **Domain-Funktionsebene 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.

Browser für Einmalanmeldung (Single-Sign-On, SSO) konfigurieren

Hierbei handelt es sich um eine kleine, einmalige Konfiguration zur Aktivierung der Single Sign-On-Unterstützung für den Browser.

Wichtig
Sie muss für jeden Benutzer auf jedem Computer ausgeführt werden.

Hinweis
In den Konfigurationsanweisungen verwenden wir *acme.com* als Beispiel. Wenn Sie Services in mehreren Domains haben, wiederholen Sie die Schritte, die *acme.com* spezifizieren, für alle Ihre Domains. (**z.B.** fügen Sie `*.acme.com` und `*.another.com` und `*.yetanother.com` hinzu).

Einmalige Konfiguration für Windows

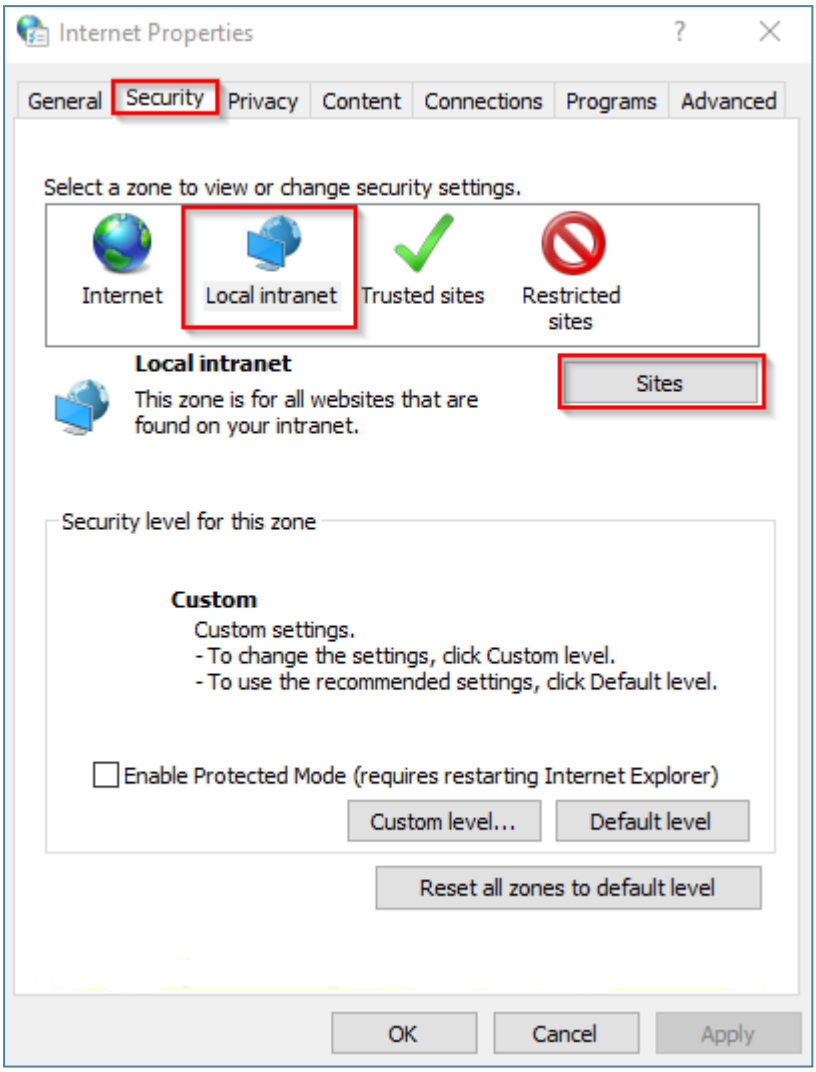
Für Microsoft Edge und Google Chrome

Die Konfiguration für Microsoft Edge und Google Chrome erfolgt über die Internetoptionen von Microsoft Windows.

Konfiguration der Windows-Internetoptionen

1. Öffnen Sie die Windows **Systemsteuerung**.
2. Wählen Sie **Internetoptionen**.

3. In der Registerkarte **Sicherheit** klicken Sie auf **Lokales Intranet**.



4. Klicken Sie auf **Sites** und dann auf **Erweitert**.
5. Fügen Sie die Adresse Ihres Acronis Cyber Files Servers hinzu (z. B. `https://ahsoka.acme.com` oder nur `*.acme.com`).
6. Klicken Sie auf **OK**.
7. Starten Sie Ihren Browser neu.

Delegierung von Anmeldedaten in Chrome

Wichtig
Die Delegierung von Anmeldedaten ist für das Durchsuchen von Netzwerkknoten von der Weboberfläche aus erforderlich. Microsoft Edge ist standardmäßig aktiviert. Zur Delegierung von Anmeldedaten in Chrome müssen Sie den Browser so konfigurieren, dass er es zulässt.

1. Registry-Editor (**regedit32.exe**) öffnen
2. Zu `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome` navigieren

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 den Domain-Namen (z.B. `ahsoka.acme.com` oder `*.acme.com`) als Wert für den Registry-Schlüssel `AuthNegotiateDelegateWhitelist` fest.
5. Starten Sie Chrome neu.

Für Firefox

1. Geben Sie `about:config` in die Adressleiste ein, und drücken Sie die Eingabetaste.
2. Suchen Sie die Einstellung `network.negotiate-auth.trusted-uris` und fügen Sie `https://ahsoka.acme.com` oder nur `just .acme.com` hinzu (die Liste wird per Komma getrennt).

   Hinweis
   Wenn Sie alle Unterdomains hinzufügen wollen, tun Sie dies im Format "`.example.com`" (aber **NICHT** im Format `*.example.com`).

3. Wenn Sie die Unterstützung für Netzwerk-**Datenquellen** aktivieren wollen, müssen Sie die Einstellung `network.negotiate-auth.delegation-uris` so bearbeiten, dass Sie `ahsoka.acme.com` oder nur den Domain-Namen (`acme.com`) hinzufügen.
4. Starten Sie **Firefox** neu.

Einmalige Konfiguration für Mac

Hinweis
Die folgenden 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 Sie die Einstellung `network.negotiate-auth.trusted-uris` und fügen Sie `https://ahsoka.acme.com` oder nur `just .acme.com` hinzu (die Liste wird per Komma getrennt).

   Hinweis
   Wenn Sie alle Unterdomains hinzufügen wollen, tun Sie dies im Format "`.example.com`" (aber **NICHT** im Format `*.example.com`).

3. Wenn Sie die Unterstützung für Netzwerk-**Datenquellen** aktivieren wollen, müssen Sie die Einstellung `network.negotiate-auth.delegation-uris` so bearbeiten, dass Sie `ahsoka.acme.com` oder nur den Domain-Namen (`acme.com`) hinzufügen.
4. Starten Sie **Firefox** neu.

Für Chrome

1. Mit der **Ticket Viewer**-Applikation (**/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-Positivliste für die Unterstützung der Authentifizierung für alle von Ihnen verwendeten Domains 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 Acronis Cyber Files-Server

Konfigurieren des Domain-Kontos, das für die Single Sign-on-Authentifizierung verwendet wird

1. Zu `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Access Server\Web Application\WEB-INF\` navigieren
2. Suchen und öffnen Sie die Datei `web.xml`. In dieser Datei geben Sie den Benutzernamen und das Kennwort für die Domain an, unter der der SSO-Dienst ausgeführt wird.
   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 Domain und das zugehörige Kennwort. Suchen Sie folgende Zeilen:

```
<init-param>
<param-name>spnego.preauth.username</param-name>
<param-value>yourusername</param-value>
</init-param>
<init-param>
<param-name>spnego.preauth.password</param-name>
<param-value>yourpassword</param-value>
</init-param>
```

4. Ersetzen Sie **yourusername** durch den gewünschten LDAP-Benutzernamen.
5. Ersetzen Sie **yourpassword** durch das LDAP-Kennwort für das zuvor angegebene LDAP-Konto. Wenn Ihr Kennwort eines der fünf folgenden Sonderzeichen enthält (**&**, **>**, **"**, ' oder **<**), 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 wie folgt in der Datei `web.xml` schreiben: `<my&best&apos;password&quot;`

Festlegen der Kerberos-Domain-Suche

1. Zu `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\apache-tomcat-7.0.59\conf` navigieren
2. Datei `krb5.conf` suchen und öffnen
3. In `krb5.conf` gibt es nur zwei Eigenschaften, die der Administrator angeben muss:
   a. Domain für Single Sign-On (z.B. `ACME.COM`).
      - Dies muss die Domain sein, in der sich der Acronis Cyber Files Web Server und die Gateway-Server befinden.
      - Beachten Sie, dass es sich um den Namen Ihrer Domain handelt, **nicht** um den DNS-Namen des Servers.

Hinweis
Die Domain 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 Domain-Controllers, z.B. `acmedc.ACME.COM`) Dies ist die Adresse des Domain-Controllers in der Domain, in der sich Acronis Cyber Files und die zugehörigen Komponenten befinden.

4. Die von uns installierte Datei `krb5.conf` 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 Domain (in **Großbuchstaben!**). Beachten Sie, dass es sich um den Namen Ihrer Domain handelt, **nicht** um den DNS-Namen des Servers.
6. Ersetzen Sie den Wert für "`kdc =`" durch den DNS-Namen Ihres Domain-Controllers. Der Domain-Teil muss in Großbuchstaben angegeben werden, z.B. `kdc = yourdc.YOURDOMAIN.COM`.
7. Nach der Aktualisierung der oben genannten Konfigurationsdateien muss der Acronis Cyber Files-Server (Acronis Cyber Files Tomcat) neu gestartet werden, damit die Änderungen wirksam werden.

Single Sign-on in der Weboberfläche aktivieren

1. Öffnen Sie die Weboberfläche von Acronis Cyber Files, 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 Web-Client und Desktop-Sync-Client mit vorhandenen Windows-/Mac-Anmeldedaten erlauben**.
4. Drücken Sie **Speichern**.

Konfigurieren des LDAP-Kontos für SSO

Zusätzlichen DNS-Eintrag für den Acronis Cyber Files Web Server konfigurieren

Wenn auf diesem Computer ein Gateway Server vorliegt, müssen Sie einen separaten DNS-Eintrag für den Acronis Cyber Files Web Server haben.

1. Öffnen Sie auf Ihrem DNS-Server die **Vorwärtssuchbereiche** für Ihre Domain, klicken Sie mit der rechten Maustaste, und erstellen Sie einen neuen **Host**-Eintrag (`A record`) für den Acronis Cyber Files Web Server.
2. Geben Sie einen Namen ein. Dabei handelt es sich um die DNS-Adresse, die zum Erreichen des Acronis Cyber Files Web-Servers verwendet wird.

   z. B. `ahsokaccess.acme.com`
3. Geben Sie die IP-Adresse des Acronis Cyber Files Web Server ein (ohne den Port). Wenn Sie den Gateway und die Acronis Cyber Files Web Server unter derselben IP-Adresse ausführen, geben Sie diese IP-Adresse ein.
4. Wählen Sie **Zugewiesenen Pointer-Datensatz (PTR) erstellen** und drücken Sie **Host hinzufügen**.

Den SPN für den **Acronis**Cyber Files-Webserver festlegen

1. Öffnen Sie auf dem Computer, auf dem Acronis Cyber Files ausgeführt wird, die Eingabeaufforderung.

   Hinweis
   Sie müssen mit einem Domain-Konto angemeldet sein und über die Rechte zur Verwendung von **setspn** verfügen.

2. Befehl `setspn -s HTTP/`**access_DNS_name.domain.com account name** eingeben

   Hinweis
   Der im obigen Befehl verwendete LDAP-Kontoname **MUSS** mit dem Konto übereinstimmen, das Sie in der Datei `web.xml` angegeben haben.

   - Beispiel: Wenn Ihr Acronis Cyber Files Web Server auf `ahsoka.acme.com` installiert ist und 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`
   - Beispiel: Wenn Ihr Acronis Cyber Files Web Server auf `ahsoka.acme.com` installiert ist und 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 Acronis Cyber Files-Weboberfläche in den **LDAP-Einstellungen** festgelegt wurde, ist aber nicht obligatorisch.

3. Wird Ihr Acronis Cyber Files Web Server auf einem nicht standardmäßigen Port (d.h., einem anderen Port als 443) ausgeführt, sollten Sie auch einen SPN mit der Portnummer registrieren.

Beispiel: Wird Ihr Server auf Port 444 ausgeführt, lautet der Befehl folgendermaßen:
`setspn -s HTTP/ahsokaaccess.acme.com:444 john` ODER
`setspn -s HTTP/ahsokaaccess.acme.com:444 tree\jane`

Hinweis
HTTPin 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 Domains 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. Klicken Sie auf **OK**.

Überprüfen, ob Sie sich bei **Acronis**Cyber Files anmelden können

1. Wechseln Sie zu einem anderen Computer als dem Domain-Controller oder Ihrem Acronis Cyber Files Web Server.
2. Öffnen Sie die Acronis Cyber Files-Webkonsole, und verwenden Sie den Link unter dem Kennwortfeld auf der Anmeldeseite.

Hinweis
Sie müssen an dem Computer mit einem Domain-Benutzer angemeldet sein, der entweder zu Acronis Cyber Files eingeladen wurde, bereits angemeldet 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

Konfigurieren des SPN für den Gateway Server

Damit das KDC ('Key Distribution Center') Kerberos-Server Benutzer für den Gateway Server authentifizieren kann, muss der Gateway-Dienst für das 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 Domain, 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.

   z.B.`codygw.acme.com`
3. Geben Sie die IP-Adresse des Gateway Server ein (ohne den Port). Wenn Sie das Gateway und den Acronis Cyber Files Server unter derselben IP-Adresse ausführen, geben Sie diese IP-Adresse ein.
4. Wählen Sie **Zugewiesenen Pointer-Datensatz (PTR) erstellen**, und drücken Sie **Host hinzufügen**.

SPN für den lokalen Gateway Server konfigurieren

1. Wechseln Sie zum Computer mit Acronis Cyber Files.
2. Öffnen Sie die Eingabeaufforderung.
3. 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**

   Wenn Ihr Gateway Server beispielsweise auf dem Host `'cody'` in einer Domain läuft und Ihr DNS-Eintrag `codygw.acme.com` lautet, führen Sie folgenden Befehl aus:
   `setspn -s HTTP/codygw.acme.com cody`
   c. Wird Ihr Gateway-Server nicht auf einem Standard-Port ausgeführt (d.h. auf einem anderen Port als 443), müssen Sie auch einen SPN mit der Portnummer registrieren, z.B. dann, wenn Ihr Gateway-Server auf Port 444 ausgeführt wird:
   `setspn -s HTTP/codygw.acme.com:444 cody`
4. Falls nicht bereits geschehen, müssen Sie die **Adresse für die Administration** Ihres gewünschten Gateway Server 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 Acronis Cyber Files Server und dem Domain-Controller, 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.

Ressourcenbasierte eingeschränkte Kerberos-Delegierung festlegen

Hinweis
Dieser Typ der eingeschränkten Delegierung ist nur bei Domain-Controllern verfügbar, die mindestens in der Domain-Funktionsebene 2012R2 ausgeführt werden. Windows Server 2012 ist das erste Programm, das die eingeschränkte Kerberos-Delegierung in Domain-Strukturen 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 Domain befinden.

1. Wechseln Sie zu dem Domain-Controller für die Domain, in der sich der Dateiserver befindet, und öffnen Sie **PowerShell**.
2. Wenn Ihr Gateway Server als **Lokales System**konto ausgeführt wird:
   a. **$computer1 = Get-ADComputer -Identity <Gateway Server-Computer> -server <Domain-Controller_für_diese_Domain>**
      Beispiel: `$computer1 = Get-ADComputer -Identity cody -server dc.acme.com`
      Dieser Befehl ruft das Computerobjekt für den Gateway-Server ab, gibt die Instanz der AD-Domain-Dienste für die Verbindung an und speichert diese Information in der Variablen**$computer1**.
   b. **Set-ADComputer <Computer_mit_Dateiserver> -PrincipalsAllowedToDelegateToAccount $computer1**
      z.B. `Set-ADComputer cody -PrincipalsAllowedToDelegateToAccount $computer1`
      Dieser Befehl legt die Eigenschaft **Principals Allowed To Delegate To Account** des Computerobjekts für den Dateiserver auf das Computerobjekt für den Gateway-Server fest. So kann der Computer des Gateway-Servers an den Computer des Dateiservers delegieren.
3. Wenn Ihr Gateway Server als **Benutzerkonto** ausgeführt wird:
   a. **$user1 = Get-ADUser -Identity <Anmeldung_Benutzer_des_Gateway-Dienstes> -server <Domain-Controller_für_diese_Domain>**
      Beispiel: `$user1 = Get-ADUser -Identity jane -server dc.acme.com`
      Dieser Befehl ruft das Benutzerobjekt für den Benutzer ab, der den Gateway-Server ausführt, gibt die AD-Domaindienste-Instanz für die Verbindung an und speichert diese Information in der Variablen **$user1**.
   b. **Set-ADComputer <Computer_mit_Dateiserver> -PrincipalsAllowedToDelegateToAccount $user1**
      z.B. `Set-ADComputer cody -PrincipalsAllowedToDelegateToAccount $user1`

Dieser Befehl legt die Eigenschaft **Principals Allowed To Delegate To Account** des Computerobjekts für den Dateiserver auf das Benutzerobjekt für den Gateway-Server fest. 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 <Dateiserver_Computer> -Properties PrincipalsAllowedToDelegateToAccount

   z.B. `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.

Hinzufügen weiterer Gateway Server

Hinweis
Diese Schritte können nur durchgeführt werden, wenn sich die Computer, welche die Gateway Server hosten, in derselben Domain befinden wie der Acronis Cyber Files Web Server.

Damit das KDC ('Key Distribution Center') Kerberos-Server Benutzer beim Gateway-Server authentifizieren kann, muss der Gateway-Dienst beim KDC-Server registriert werden. Hierzu müssen 'setspn' ausgeführt und der Hostname des Servers, auf dem er ausgeführt wird, als 'user' im setspn-Befehl angegeben werden.

Gateway Server, die auf anderen Computern als dem Acronis Cyber Files Web Server gehostet werden

1. Öffnen Sie die Eingabeaufforderung.
2. Geben Sie den folgenden **setspn**-Befehl ein: `setspn -s HTTP/`**computername.domain.com computername**

   Führen Sie beispielsweise für den Fall, dass Ihr Gateway-Server auf Host `'cody'` in der Domain ausgeführt wird, folgenden Befehl aus:

   ```
   setspn -s HTTP/cody.acme.com cody
   ```
3. Wird Ihr Gateway-Server nicht auf einem Standard-Port ausgeführt (d.h. auf einem anderen Port als 443), müssen Sie auch einen SPN mit der Portnummer registrieren, z.B. dann, wenn Ihr Gateway-Server auf Port 444 ausgeführt wird:

   ```
   setspn -s HTTP/cody.acme.com:444 cody
   ```
4. Wiederholen Sie diesen Abschnitt für alle weiteren Gateway-Server.

Konfigurieren eines Gateway Server in einer anderen Domain

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 Domain befinden, darin, einen Gateway Server auf einem Computer in dieser Domain zu installieren. So können Sie die reguläre eingeschränkte Kerberos-Delegierung verwenden. **Geeignet in Domain-Funktionsebene 2008**.

Gateway Server auf einem Computer in der gewünschten Domain installieren

1. Laden Sie das Installationsprogramm von Acronis Cyber Files herunter, und verschieben Sie es auf den Computer.
2. Starten Sie das Installationsprogramm von Acronis Cyber Files, 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 Acronis Cyber Files, 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 Acronis Cyber Files installiert wurde. Es wird empfohlen, ein dediziertes Konto zu verwenden und nicht das, das für die SPNs des Acronis Cyber Files Server 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 Domain und den Benutzernamen für das dedizierte Konto an.
7. Sie können jetzt den Acronis Cyber Files Gateway-Dienst in der Systemsteuerung unter **Dienste** neu starten.

Den SPN für den Remote-Gateway Server konfigurieren

1. Wechseln Sie zu einem der Computer in der Domain, in der sich der Acronis Cyber Files 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 Domain **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
   ```

   Wird Ihr Gateway-Server nicht auf einem Standard-Port ausgeführt (d.h. auf einem anderen Port als 443), müssen Sie auch einen SPN mit der Portnummer registrieren, z.B. dann, wenn Ihr Gateway-Server auf Port 444 ausgeführt wird:

   ```
   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** aktiviert wurde. Sie müssen den Acronis Cyber Files Gateway-Dienst neu starten, nachdem Sie diese Einstellung aktiviert haben.
6. Wenn Sie **Datenquellen** für die Ressourcen in der zweiten Domain erstellen, müssen Sie den Gateway Server verwenden, der sich in dieser Domain 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).

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.domain.com** ein.

   z.B. `setspn -Q HTTP/ahsoka.acme.com`
3. Verwenden Sie zur Abfrage der für eine bestimmte Domäne registrierten SPNs den Switch `-l` (Kleinbuchstabe `L`).

   z.B. `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
   ```

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 stattdessen dieses **Benutzer**objekt aus.
3. Klicken Sie mit der rechten Maustaste auf den Benutzer und wählen Sie "Eigenschaften".
4. Öffnen Sie die Registerkarte **Delegierung**.
5. Wählen Sie **Diesem Computer nur für die Delegierung für bestimmte Dienste vertrauen** aus.
6. Wählen Sie darunter die Option **Beliebiges Authentifizierungsprotokoll verwenden**.
7. Klicken Sie auf **Hinzufügen**.

8. Klicken Sie auf **Benutzer oder Computer**.
9. Suchen Sie nach dem Serverobjekt für die SMB-Freigabe oder den SharePoint-Server und klicken Sie auf **OK**.
   - Wählen Sie für SMB-Freigaben den Dienst **cifs** aus.
   - Wählen Sie für SharePoint den Dienst **http** aus.
10. Wiederholen Sie die Schritte für jeden Server, für den der Acronis Cyber Files Gateway-Server Zugriff benötigt.
11. Wiederholen Sie dieses Verfahren für jeden Gateway Server.

Diese Delegierungsänderungen benötigen, je nach Größe der Domain-Gesamtstruktur, 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 Acronis Cyber Files Gateway-Dienst neu zu starten.

Verwenden von mobilen Clients mit Client-Zertifikatsauthentifizierung

Dies ist ein zusätzlich auszuführender Schritt. Sie müssen die Delegierung vom Gateway Server zum Acronis Cyber Files-Server auch dann einrichten, wenn diese sich auf demselben Computer befinden.

Eingeschränkte Kerberos-Delegierung

Diese Art der Delegierung wird durchgeführt, wenn sich der Acronis Cyber Files-Server und der Gateway Server in derselben Domain befinden.

1. Öffnen Sie dazu das Active Directory auf dem Domain-Controller.
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 Acronis Cyber Files-Servers auszuwählen, klicken Sie auf 'Hinzufügen' und geben den Benutzernamen des Kontos ein, das mit dem **HTTP**-SPN des Acronis Cyber Files-Servers verknüpft ist.

Hinweis
Suchen Sie nicht nach dem Computer, auf dem der Acronis Cyber Files Server ausgeführt wird. Sie müssen stattdessen die Suche anhand des Benutzernamens durchführen.

Hinweis
Eine Kerberos-Authentifizierung für den Acronis Cyber Files-Server ist nicht mit dem Einzelport-Modus kompatibel.

5. Sobald Sie nach dem Benutzer suchen, sollten die **HTTP**-Dienste angezeigt werden. Wählen Sie diese aus (es können zwei Dienste 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 Domains einer Domain-Gesamtstruktur befinden.

Hinweis
Damit diese Funktion verwendet werden kann, müssen alle Domänen, auf die Acronis Cyber Files zugreifen kann, mindestens in der **Domänenfunktionsebene 2012** ausgeführt werden.

1. Überprüfen Sie erneut, dass die DNS-Eingabe für den Acronis Cyber Files-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 Acronis Cyber Files-Server. Jetzt wird die Delegierung zwischen dem Gateway Server und dem Acronis Cyber Files-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 $pc1
   z.B.: `$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 $user1
   z.B.: `$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.

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 **Mobile Access** -> **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 Acronis Cyber Files-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 Gateway-Server 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 in der Liste mit der rechten Maustaste auf **Acronis Cyber Files 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 als Benutzer **john** ausgeführt, lautet der Befehl:

   ```
   setspn -s HTTP/gatewayserver1.acme.com john
   ```
3. Wird Ihr Gateway-Server nicht auf einem Standard-Port ausgeführt (d.h. auf einem anderen Port als 443), müssen Sie auch einen SPN mit der Portnummer registrieren, z.B. dann, wenn Ihr Gateway-Server auf Port 444 ausgeführt wird:

   ```
   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
   ```

Hinweis
Wenn eine Lastverteilung den Datenverkehr zwischen zwei Gateways aufteilt (in diesem Fall `gwloadbalancerdns.acme.com`), sollte keine Registrierung bei diesen erfolgen, da in 50 Prozent der Fälle die Anforderungen nicht das richtige (lokale) Gateway erreichen. Wenn der Lastverteilungsserver die Anforderung an das falsche Gateway weiterleitet, schlägt die Anmeldung fehl. DNS-Namen können nach dem Start nicht auf einen anderen Dienst verweisen.

Wenden Sie sich an das Supportteam, wenn Sie weitere Unterstützung benötigen.

Beheben von Fehlern bei Single Sign-On

- Benutzer von Desktop- oder Web-Clients müssen auf einem anderen Computer als auf dem arbeiten, auf dem derAcronis Cyber Files-Server ausgeführt wird (aber innerhalb der Domain), sonst funktioniert SSO nicht.
- Für Single Sign-On über einen Desktop-Client ist eine Verbindung zum Unternehmensnetzwerk erforderlich. Dies bedeutet, dass SSO-Benutzer zudem Zugriff auf das eigene Netzwerk haben sollten.

- 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 Acronis Cyber Files-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 Acronis Cyber Files 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.
- Single Sign-On funktioniert nicht, wenn der Acronis Cyber Files Server auf dem Domain-Controller ausgeführt wird.
- Acronis Cyber Files funktioniert nicht mit SSO, wenn Sie versuchen, über den Computer, der auch der Domain-Controller ist, darauf zuzugreifen.

  Hinweis
  Aufgrund der Funktionsweise von Kerberos können Sie sich nicht über Client-Applikationen oder Webbrowser, die auf dem Domain-Controller oder dem Acronis Cyber Files-Server ausgeführt werden, über SSO authentifizieren.

  Hinweis
  Zudem kann der Acronis Cyber Files-Server den Domain-Controller nicht authentifizieren, wenn der Acronis Cyber Files-Server auf dem Domain-Controller ausgeführt wird.

- Wenn Sie bei dem Versuch, sich mit SSO anzumelden, einen **401-Fehler** erhalten, überprüfen Sie den Benutzernamen und das Kennwort in der Datei **web.xml**. Stellen Sie zudem sicher, dass alle Sonderzeichen ordnungsgemäß mit Escape-Zeichen versehen sind. Diese Sonderzeichen sind: **&**, **>**, **"**, **'** oder **<**. Informationen darüber, wie Sie diese Sonderzeichen mit Escape-Zeichen versehen, finden Sie in **Schritt 5** des Abschnitts **Die Datei web.xml bearbeiten**.

Verwenden vertrauenswürdiger Serverzertifikate mit Acronis Cyber Files

In diesem Abschnitt wird erläutert, wie Acronis Cyber Files mit vertrauenswürdigen Serverzertifikaten konfiguriert wird.

AcronisCyber Files 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.

Erstellen einer Zertifikatsanforderung

Hinweis
Das Erstellen von Zertifikaten ist keine Funktion von Acronis Cyber Files und auch in Zukunft nicht als solche geplant. Diese Zertifikatanforderung ist für den Einsatz von Acronis Cyber Files nicht zwingend notwendig, wird von Zertifikatanbietern jedoch vorausgesetzt.

Hinweis
Wenn Sie vom Anbieter aufgefordert werden, einen Servertyp anzugeben, wählen Sie **IIS** aus. Die Zertifikate müssen im Windows Certificate Store installiert werden, bevor Acronis Cyber Files sie verwenden kann.

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

Zertifikatanforderung mit OpenSSL erzeugen:

Hinweis
Für diese Anleitung müssen Sie OpenSSL installiert haben.

Hinweis
Wenden Sie sich an Ihren bevorzugten Zertifikatanbieter, um weitere Informationen oder Hilfe zu diesem Verfahren zu erhalten.

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
   ```

2. 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 **WARNING: can't open config file: /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.

3. Dabei werden Sie aufgefordert, die erforderlichen Details in Ihr CSR einzugeben. Verwenden Sie den Namen des Webservers als **Common Name (CN)**. Lautet der Domain-Name **mydomain.com**, hängen Sie die Domain an den Hostnamen an (verwenden Sie dabei den vollständig qualifizierten Domain-Namen).
4. Die Felder für E-Mail-Adresse, optionaler Firmenname und Kennwort-Sicherheitsabfrage dürfen für ein Webserver-Zertifikat leer bleiben.
5. 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.

Das Zertifikat im Windows-Zertifikatspeicher installieren

Anforderungen

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 Acronis Cyber Files- 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 in der Dialogbox **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 in der Dialogbox **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 **Privater Informationsaustausch (*.pfx, *.p12)** ändern, um die Datei 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 Acronis Cyber Files-Konfigurationswerkzeugs zur Verfügung.

Cyber Files für die Verwendung Ihres Zertifikats konfigurieren

Nachdem Sie das Zertifikat im Windows Certificate Store installiert haben, müssen Sie Acronis Cyber Files für die Verwendung dieses Zertifikats konfigurieren.

1. Starten Sie das Acronis Cyber Files-Konfigurationswerkzeug. Im Startmenü von Windows sollte eine Verknüpfung angezeigt werden.

Hinweis
Das Konfigurationswerkzeug befindet sich standardmäßig unter `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\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.

Verwenden von Zwischenzertifikaten

Hat die Zertifizierungsstelle Ihnen zusammen mit Ihrem Zertifikat ein Zwischenzertifikat ausgestellt, muss dieses über das Konfigurationsdienstprogramm ebenfalls dem AcronisCyber Files Server hinzugefügt werden.

Hinweis
Das Konfigurationswerkzeug sucht nur im Zertifikatsspeicher für **Zwischenzertifikate**. Wenn Ihr Zertifikat in einem der anderen Stores installiert wurde, öffnen Sie **certmgr.msc** und verschieben Sie Ihr Zwischenzertifikat von diesem Store in den Store **Zwischenzertifizierungsstellen** -> **Zertifikate**.

1. Starten Sie das Acronis Cyber Files-Konfigurationswerkzeug. Im Startmenü von Windows sollte eine Verknüpfung angezeigt werden.

   Hinweis
   Das Konfigurationswerkzeug befindet sich standardmäßig unter `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\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 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 Store 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.

Unterstützen verschiedener Desktop-Client-Versionen

Wenn Sie eine ältere Version des Acronis Cyber Files-Desktop-Clients 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:
   - ACFClientMac.zip
   - ACFClientInstaller.msi
   - AcronisCyberFilesInstaller.dmg
   - AcronisCyberFilesClientInstaller.exe
2. Kopieren Sie die Dateien.
3. Öffnen Sie auf dem Server den Ordner für Acronis Cyber Files Desktop Clients (`C:\Program Files (x86)\Acronis\Acronis Cyber Files\Access Server\Web Application\clients`).
4. Erstellen Sie einen Unterordner für diese Version des Clients. Dieser sollte mit der **Versionsnummer des Clients** (z. B. **8.5.0x664**, **8.6.2x632**) benannt sein.
5. Fügen Sie die vier Dateien in den eben erstellten Unterordner ein.
6. Öffnen Sie anschließend die **webbasierte Benutzeroberfläche** des Acronis Cyber Files-Servers.
7. Melden Sie sich als **Administrator** an, gehen Sie zur Registerkarte **Sync & Share**, und öffnen Sie die Seite **Acronis Cyber Files-Client**.
8. Suchen Sie die folgende Einstellung: **Client-Auto-Update auf Version erlauben**.
9. Wählen Sie Ihre gewünschte Version im Dropdown-Menü aus.

Hinweis
Über den Download-Link im Menü **Aktion** für Ihr Konto können Sie weiterhin die neueste verfügbare Version des Acronis Cyber Files-Desktop-Clients herunterladen. Wenn die Benutzer nicht die aktuelle Version herunterladen sollen, gehen Sie zum Ordner **\Acronis\Acronis Cyber Files\Access Server\Web Application\clients** und geben Sie dem Ordnernamen der aktuellen Clientversion (z. B. 8.6.2x632) den Namen '**Versionsnummer nicht verwenden**' (z.B. '**8.6.2x632 nicht verwenden**').

Verschieben des FileStore an einen nicht standardmäßigen Speicherort

Der Dienst wird als lokales Systemkonto ausgeführt.

1. Wechseln Sie zu dem Computer, auf dem Cyber Files installiert ist.
2. Stoppen Sie die **Cyber Files File Repository Server** und **Cyber Files Tomcat**-Dienste.

3. Sie finden den aktuellen **FileStore**in dem Ordner, den Sie mit dem **Konfigurationswerkzeug** ausgewählt haben. Der Standardspeicherort lautet: `C:\ProgramData\Acronis\Acronis Cyber Files\FileStore`.
4. Kopieren oder verschieben Sie den gesamten Ordner **FileStore** mit dem kompletten Inhalt an den gewünschten Speicherort.
   Beispielsweise `D:\MyCustom Folder\FileStore`.

Hinweis
Befindet sich der **Dateispeicher** auf einer Remote-Netzwerkfreigabe, muss der Computer, auf dem der Dienst **Datei-Repository** ausgeführt wird, die vollen Berechtigungen für den Ordner **Dateispeicher** auf der Netzwerkfreigabe aufweisen.

5. Öffnen Sie das **Konfigurationswerkzeug**.
6. Ändern Sie auf der Registerkarte **File Repository** den Pfad für den **FileStore**in den neuen Pfad, in den Sie den Ordner **FileStore** verschoben haben.
7. Starten Sie den **Acronis Cyber Files File Repository Server**-Dienst.
8. Starten Sie **Acronis Cyber Files Tomcat**, und schließen Sie die Systemsteuerung für **Dienste**.

Der Dienst wird als Benutzerkonto ausgeführt

1. Wechseln Sie zu dem Computer, auf dem Cyber Files installiert ist.
2. Stoppen Sie die **Cyber Files File Repository Server** und **Cyber Files Tomcat**-Dienste.
3. Sie finden den aktuellen **FileStore**in dem Ordner, den Sie mit dem **Konfigurationswerkzeug** ausgewählt haben. Der Standardspeicherort lautet: `C:\ProgramData\Acronis\Acronis Cyber Files\FileStore`.
4. Kopieren oder verschieben Sie den gesamten Ordner **FileStore** mit dem kompletten Inhalt an den gewünschten Speicherort.
   Beispielsweise `D:\MyCustom Folder\FileStore`.
5. Öffnen Sie das **Konfigurationswerkzeug**.
6. Ändern Sie auf der Registerkarte **File Repository** den Pfad für den **FileStore**in den neuen Pfad, in den Sie den Ordner **FileStore** verschoben haben.
7. Befindet sich der **File Store** auf einer Remote-Netzwerkfreigabe, muss das Benutzerkonto, mit dem der **File Repository**-Dienst ausgeführt wird, über die vollen Berechtigungen für den Ordner **File Store** auf der Netzwerkfreigabe verfügen.
8. Das Konto benötigt auch Lese- und Schreibzugriff auf den lokalen **Repository**-Ordner (zum Beispiel `C:\Program Files (x86)\Acronis\Access\File Repository\Repository`), um in das Protokoll zu schreiben.
9. Starten Sie den **Acronis Cyber Files File Repository Server**-Dienst.
10. Starten Sie **Acronis Cyber Files Tomcat**, und schließen Sie die Systemsteuerung für **Dienste**.

Überwachen von Acronis Cyber Files mit New Relic

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

1. Öffnen Sie 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 AcronisCyber Files.
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 AcronisCyber Files, 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 Acronis Cyber Files Tomcat neu, und warten Sie einige Minuten. Die Schaltfläche sollte dann aktiv sein.
10. Sie sollten den Acronis Cyber Files-Server auf der New Relic-Website überwachen können.

Hinweis
Alle Informationen, die der Acronis Cyber Files Server über den Verbindungsversuch zu New Relic und die Konfiguration des Monitorings protokolliert, sind in einer Datei namens **newrelic_agent.log** zu finden, die sich in diesem Verzeichnis befindet: `C:\Program Files (x86)\Acronis\Common\apache-tomcat-7.0.34\logs`. Bei Problemen können Sie in dieser Protokolldatei nach Informationen suchen.

Hinweis
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. Das ist ein harmloser Nebeneffekt des Codes, der zum Beheben eines anderen New-Relic-Fehlers verwendet wurde.

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

1. Öffnen Sie 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.

Ausführen vonAcronis Cyber Files Tomcat auf mehreren Ports

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 dem 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.

Konfigurieren eines zusätzlichen Tomcat-Konnektors

1. Stoppen Sie den Acronis Cyber Files Tomcat-Dienst, wenn er ausgeführt wird.
2. Gehen Sie zur Datei `server.xml`, und öffnen Sie sie. Der Standardspeicherort ist `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="TLSv1.2" 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.

Hinweis
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**(oder den von Ihnen im **Konfigurationswerkzeug** gewählten Port) durch den gewünschten zweiten Port, auf dem Tomcat ausgeführt wird. Beispiel:

```
<Connector maxHttpHeaderSize="65536" maxThreads="150" enableLookups="false"
disableUploadTimeout="true" acceptCount="100" scheme="https" secure="true"
SSLEnabled="true" SSLProtocol="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 bestehenden Code entspricht. Wenn der alte Code beispielsweise in einer Zeile geschrieben ist, muss der neue Code auch so formatiert sein.

6. Öffnen Sie die Acronis Cyber Files-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.

Multi-Homing für Acronis Cyber Files

Multi-Homing für Acronis Cyber Files Gateway und Acronis Cyber Files-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.

Konfigurieren von Multi-Homing

1. Öffnen Sie das Acronis Cyber Files-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 dieses Problem umgehen, indem Sie die dynamische DNS-Registrierung auf der Netzwerkkarte deaktivieren und dann den host-DNS-Eintrag manuell erstellen. Eine andere, einfachere Möglichkeit ist die Installation des Hotfixes, auf den im Microsoft Knowledge Base-Artikel **KB975808** verwiesen wird:**http://support.microsoft.com/?kbid=975808**. Nach der Installation des Hotfixes können Sie die Option `netsh skipassource` verwenden. Wenn Sie diese Option beim Hinzufügen neuer Adressen verwenden, teilen Sie dem Stack mit, dass die neue Adresse nicht für ausgehende Pakete verwendet wird. Daher werden diese IP-Adressen nicht auf den DNS-Servern registriert. Beispiel:

```
netsh int ipv4 add address "Local Area Connection" 192.168.1.2 skipassource=true
```

Separate Webvorschau-Servlets bereitstellen

Mit der Webvorschaufunktion von Acronis Cyber Files 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 bzw. die Acronis Cyber Files-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.

Hinweis
Für kennwortgeschützte Dateien sind keine Miniaturbilder und keine Vorschau vorhanden.

Servlet installieren und konfigurieren

Tomcat-Installation

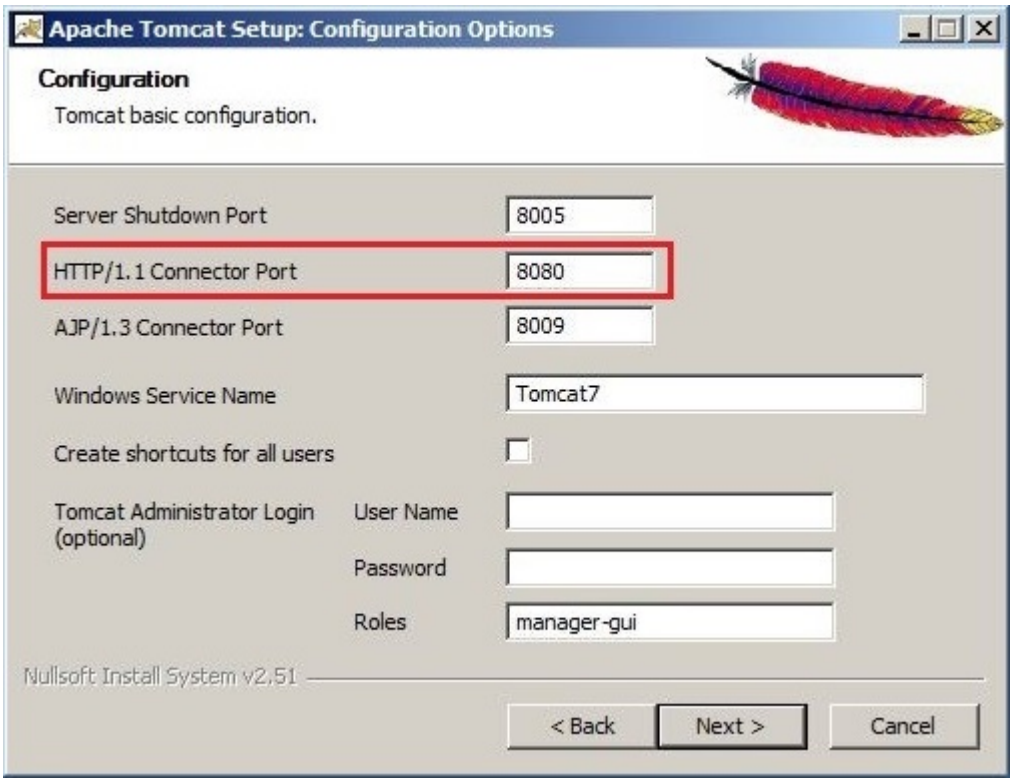
Sie können einen Apache Tomcat Server 9.0.88 entweder aus einer .zip-Datei oder über eine ausführbare Installationsdatei installieren. Wir empfehlen die Verwendung des Installers, aber das .zip-Archiv funktioniert auch. Der einzige Unterschied besteht darin, wie Sie den Apache Tomcat Server 9.0.88 konfigurieren müssen.

Anforderungen für beide Szenarien:

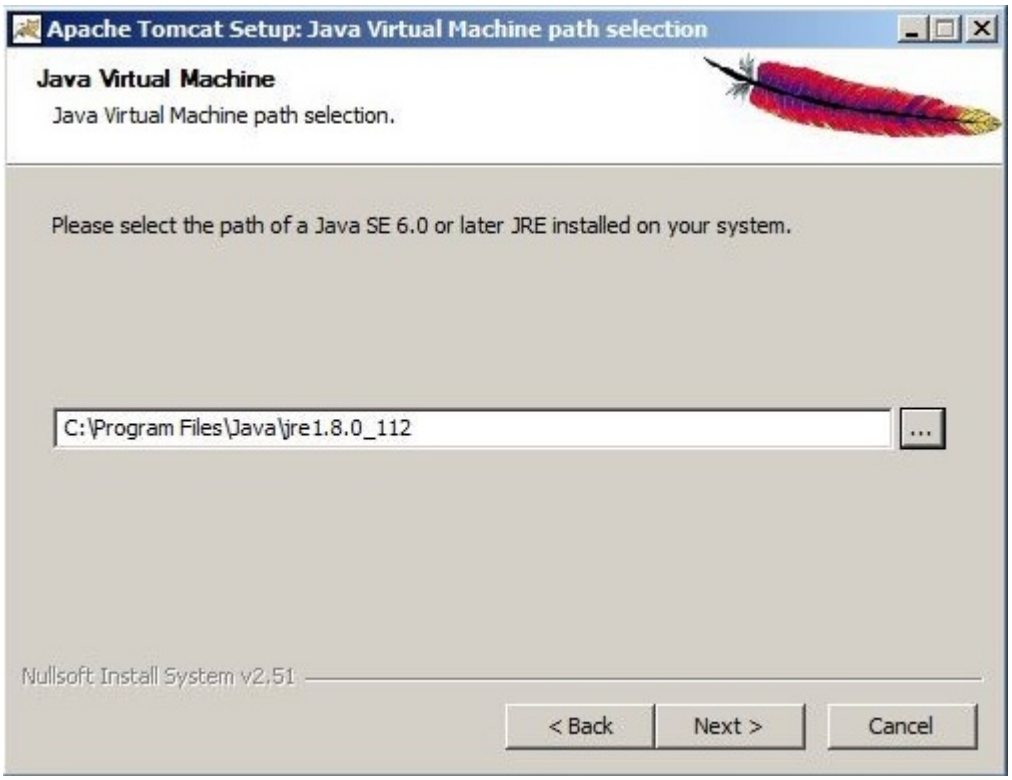
1. Stellen Sie sicher, dass Sie eine 64-Bit-Version der Java-Laufzeitumgebung (JRE) installiert haben. Ein 64-Bit-Java-Entwicklungskit (JDK) funktioniert ebenfalls. Java muss Version 8u412 oder höher sein.
2. Laden Sie eine 64-Bit-Version von Apache Tomcat 9.0.88 herunter. Stellen Sie sicher, dass die Version, die Sie verwenden wollen, nicht neuer ist als die von Acronis Cyber Files unterstützte Version. Die von Acronis Cyber Files verwendete Version ist am Anfang des Dokuments zum Acronis Cyber Files Release-Verlauf angegeben.

Verwenden einer ausführbaren Installationsdatei

1. Laden Sie eine Installationsdatei mit der 64-Bit-Version von Apache Tomcat 9.0.88 herunter. Sie finden die Versionsliste auf der Website von Apache Tomcat. Ermitteln Sie die gewünschte Version und klicken Sie auf diese, um dann den Ordner 'bin' zu öffnen und die entsprechende .zip-Datei herunterzuladen (z.B. **apache-tomcat-9.0.88.exe**).
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. Navigieren Sie nach der Installation auf Ihrem Computer mit Acronis Cyber Files zum Acronis Cyber Files-Installationsordner (standardmäßig `C:\Program Files (x86)\Acronis\Files Advanced\Access Server\`).
4. Kopieren Sie den Ordner **AccessPreviewServlet** auf die neue Maschine, auf der Apache Tomcat installiert ist, und fügen Sie ihn in den Ordner **webapps** Ihrer Tomcat-Installation ein. (Das Standardverzeichnis lautet: C:\Program Files\Apache Software Foundation\Tomcat 9.0.88\webapps)
5. Gehen Sie zum Ordner **conf** Ihrer Apache Tomcat-Installation (das Standardverzeichnis lautet: C:\Program Files\Apache Software Foundation\Tomcat 9.0.88\conf) und machen Sie ein Backup der 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 9.0.88\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 ändern.

7. Speichern und schließen Sie die Datei.
8. Zum Starten des Tomcat-Dienstes öffnen Sie **Systemsteuerung** -> **Verwaltung** -> **Dienste**und starten den Apache Tomcat-Dienst.

Verwenden einer archivierten Apache Tomcat-Installation

1. Laden Sie eine **.zip**-Datei mit der 64-Bit-Version von Apache Tomcat 9.0.88 herunter. Sie finden die Versionsliste auf der Website von Apache Tomcat. Ermitteln Sie die gewünschte Version und klicken Sie auf diese, um dann den Ordner 'bin' zu öffnen und die entsprechende .zip-Datei herunterzuladen (z.B. **apache-tomcat-9.0.88.zip**).
2. Extrahieren Sie die Inhalte des Archivs an einem Speicherort Ihrer Wahl, z.B. **C:\Programme\Apache Tomcat.**
3. Navigieren Sie zu **C:\Program Files\Apache Tomcat\apache-tomcat-<Version>**, und öffnen Sie den Ordner **bin**.

Hinweis
Der extrahierte Ordnername enthält eine Versionsnummer. Ersetzen Sie das Element **<version>** mit ihrer Tomcat-Version, beispielsweise **C:\Program Files\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-9.0.88"
```

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\jre1.8u412"
```

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 Acronis Cyber Files zum Installationsordner von Acronis Cyber Files (standardmäßig `C:\Program Files (x86)\Acronis\Files Advanced\Access Server\`).
8. Kopieren Sie den Ordner **AccessPreviewServlet** auf die neue Maschine mit Apache Tomcat und fügen Sie diesen in den Ordner **webapps** Ihrer Tomcat-Installation ein (Vorgegeben ist: `C:\Program Files\Apache Tomcat\apache-tomcat-9.0.88\webapps`).
9. Gehen Sie zum Ordner **conf** Ihrer Apache Tomcat-Installation (beispielsweise **C:\Program Files\Apache Tomcat\apache-tomcat-7.0.75\conf**) und machen Sie ein Backup der 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-9.0.88\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 Ordner 'bin' navigieren und auf die Datei **startup.bat** doppelklicken. Das schwarze DOS-Fenster muss offen bleiben, während Tomcat ausgeführt wird.

Acronis Cyber Files-Serverkonfigurationen

1. Rufen Sie die Weboberfläche von Acronis Cyber Files 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. (**z.B.**`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 Acronis Cyber Files-Servers 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.

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/**.

   z.B. `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.

   z.B. `https://loadbalancer.yourdomain.com`

PostgreSQL-Streaming-Replikation

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 AcronisCyber Files, sondern lediglich die Konfiguration der Streaming Replication beschrieben.

Streaming Replication

Das Streaming-Replication-Verfahren basiert auf WAL-Segmenten (Write-Ahead Logging). WAL ist ein 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 PostgreSQL-Server: Bei diesem Verfahren wird der aktive Server als "Primärserver" und der passive Server als "Standbyserver" bezeichnet.

  Hinweis
  Nur der Primärserver kann für Acronis Cyber Files-Verbindungen verwendet werden. Der Standbyserver kann nur verwendet werden, wenn bei einem Failover zum Primärserver hochgestuft wird.

- PostgreSQL 11.6: Wir werden Funktionen wie 'Replikationsslot' implementieren, die PostgreSQL 11.21 erfordern. Diese Version ist in Acronis Cyber Files 8.7 und höher eingebettet und wird nur bei neuen Installationen (nicht bei Upgrades) verwendet.
- Eine virtuelle IP (optional): Diese virtuelle IP-Adresse wird in allen Front-Ends verwendet, die als Acronis Cyber Files Server fungieren. Der Eigentümer muss immer der aktive Host (der Primärserver) sein.
- Zu empfehlen sind folgende Vorbereitungen: Acronis Cyber Files ist bereits installiert und die Datenbank des Primärservers initialisiert worden.

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:

   ```
   Replikator für die Host-Replikation <IP_DES_STANDBY-SERVERS>/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) mit einer zusätzlichen Option zur Anforderung von SSL-Verschlüsselung (**hostssl**) zu übergeben. Beispiel:

   ```
   Replikator für die Host-Replikation <IP_DES_STANDBY-SERVERS>/32 md5
   Replikator für die Host-SSL-Replikation <IP_DES_STANDBY-SERVERS>/32 md5
   ```

Konfigurieren von Streaming Replication

1. Gehen Sie zum PostgreSQL-Installationsordner. Der Standardspeicherort lautet:

   ```
   C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\PostgreSQL\<version>
   ```

2. Navigieren Sie im Ordner `Data` zur Datei `postgresql.conf`, um sie zu bearbeiten. Suchen und bearbeiten Sie folgende Zeile:

Hinweis
Stellen Sie sicher, dass diese Zeile nicht mit dem Symbol **#** beginnt. Zeilen, die mit diesem Symbol beginnen, werden als Kommentare behandelt und haben keinerlei Auswirkungen.

`listen_addresses = „IP_DES_PRIMÄREN_SERVERS, 127.0.0.1“`

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;"
   ```

Auf dem Standbyserver

Prüfen Sie, ob alle notwendigen Server aufeinander zugreifen können

Bei einem Failover wird der Standbyserver zum Primärserver hochgestuft und beantwortet alle Anforderungen von Acronis Cyber Files Servern.

Es wird empfohlen, für alle Acronis Cyber Files 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 Acronis Cyber Files Servern aus eine Verbindung hergestellt werden kann.
2. Navigieren Sie hierfür zum PostgreSQL-Installationsordner, und bearbeiten Sie die Datei **pg_hba.conf** (befindet sich im Unterordner `data`), indem Sie für jeden Server folgende Zeile hinzufügen:
   ```
   host all all <IP_OF_CYBER_FILES_SERVER_1>/32 md5
   host all all <IP_OF_CYBER_FILES_SERVER_1>/32 md5
   ```

Konfigurieren von Streaming Replication

1. Gehen Sie zum PostgreSQL-Installationsordner. Der Standardspeicherort lautet:

   `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\PostgreSQL\<version>.`

2. Navigieren Sie im Ordner `Data` zur Datei `postgresql.conf`, um sie zu bearbeiten. 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 behandelt und haben keinerlei Auswirkungen.

   - `listen_addresses = '`**IP_DES_STANDBY-SERVERS**, 127.0.0.1'
   - `hot_standby = on`

   Die Einstellung von `hot_standby` bestimmt, ob während der Streaming Replication Verbindungen hergestellt und Abfragen ausgeführt werden können. Wenn diese Option aktiviert ist, akzeptiert die Datenbank Anforderungen mit Nur-Lese-Zugriff, sodass die Datenbanktabellen eingesehen werden können und anhand der Inhalte geprüft werden kann, ob der Replikationsvorgang ordnungsgemäß abläuft.

   Hinweis
   Für den `listen_addresses`-Parameter ist eine Duplizierung von Zeilen in der Datei `postgresql.conf` möglich, wobei die erste (kommentierte) Zeile als Teil der Standard-Dateivorlage und die zweite (auskommentierte) Zeile vom Produktinstallationsprogramm hinzugefügt wird. Bearbeiten Sie nur die erste Zeile, und kommentieren Sie alle zusätzlichen Zeilen nicht aus, wenn vorhanden.

   Hinweis
   Wenn die Einstellung `max_connections` in der Datei `postgresql.conf` auf dem Primärserver in einen anderen Wert als den Standard geändert wurde, müssen Sie ihn auf dem Standbyserver auch ändern.

   Hinweis
   Wenn Sie `md5` oder `password` in `pg_hba.conf` als Authentifizierungsmethode angeben möchten, wird für die Verbindung ein Kennwort benötigt. Um dieses Kennwort 'einzugeben', müssen Sie folgenden Befehl zur Datei `recovery.conf` auf dem Standbyserver hinzufügen: `primary_conninfo = 'host=`<IP-ADRESSE_VON_PRIMÄRSERVER> `port=`<PORT_VON_PRIMÄRSERVER> `user=`<BENUTZERNAME> `password=`<KENNWORT_FÜR_BENUTZERNAME>`'` . So würde beispielsweise der Befehl lauten, wenn Postgres auf IP 10.0.0.1, Port 5432, mit dem Benutzer`replicator` und dem Kennwort `1234` ausgeführt würde: `primary_conninfo = 'host=10.0.0.1 port=5432 user=replicator password=1234'`

3. **Stoppen Sie den PostgreSQL-Dienst auf dem Sekundärserver, 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 Acronis Cyber Files Tomcat stoppen und 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
   --slot=access_slot
   ```

   Hinweis
   `<PATH_TO_NEW_DATA_DIR>` sollte der Pfad zum neuen `Data`-Ordner sein. z.B. `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\PostgreSQL\11.21\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.

Replikations-Slot erstellen

1. Führen Sie auf dem Sekundärserver 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;"
   ```

Streaming-Replication-Befehle

1. Öffnen Sie den Data-Ordner, 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_DES_PRIMÄREN_SERVERS**`> port=5432 user=replicator password= <`**PASSWORT_FÜR_DEN_REPLIKATOR-BENUTZER**`>'`

- `primary_slot_name = 'access_slot'`
- `trigger_file = '<`**PFAD_ZUR_TRIGGER-DATEI**`>' # 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 stoppt der Server die Wiederherstellung auch dann nicht, 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 `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.

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, stoppen Sie ihn daher, 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 AcronisCyber Files-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. Die Trigger-Datei wird gelöscht.

Navigieren Sie dazu zu `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Access Server`, und bearbeiten Sie `acronisaccess.cfg`. Stellen Sie sicher, dass `DB_HOSTNAME` und `DB_PORT` auf die Adresse und den Port verweisen, deren PostgreSQL-Server derzeit der Primärserver ist. Wenn Sie Änderungen vornehmen, müssen Sie den Acronis Cyber Files Tomcat-Dienst neu starten.

Migrieren der Instanz

1. Um dieses Upgrade durchführen zu können, müssen Sie durch das Anhalten von Acronis Cyber Files Downtime schaffen.
2. Stoppen Sie auch den Primär- und PostgreSQL-Standbyserver.
3. Führen Sie ein Upgrade des Primärservers unter Verwendung der Anweisungen von "Durchführen eines PostgreSQL-Upgrades auf eine neuere Hauptversion" (S. 237) durch.
4. Installieren Sie dieselbe PostgreSQL-Hauptversion auf dem Standbyserver.
5. Folgen Sie den Streaming Replication-Anweisungen, die für Primärserver und Standbyserver verfügbar sind.

Konfigurieren von PostgreSQL für Remote-Zugriff

Wichtig
Remote-Administration wird nur von PostgreSQL 9-Servern unterstützt.

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\Acronis Cyber Files\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 Acronis Cyber Files & Gateway server
   host all all 10.27.81.3/32 md5
   # Zweiter Acronis Cyber Files & 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 Standardspeicherort ist `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\PostgreSQL\9.4\Data\`.
   a. Suchen Sie die Zeile `#listen_addresses = 'localhost'`.
   b. Aktivieren Sie diesen Befehl, indem Sie das **#**-Symbol am Beginn der Zeile entfernen.
   c. Ersetzen Sie `localhost` durch *****, 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 = '*'` – Dies bedeutet, dass PostgreSQL alle verfügbaren Adressen überwacht.
      - **z.B.**`listen_addresses = '192.168.1.1'` – Dies bedeutet, dass PostgreSQL diese Adresse überwacht.
5. Speichern Sie alle Änderungen an **postgresql.conf**.
6. Starten Sie den Acronis Cyber Files-PostgreSQL-Dienst neu.

Hinweis
PostgreSQL verwendet standardmäßig Port 5432. Stellen Sie sicher, dass dieser Port in jeder Firewall oder Routing-Software geöffnet ist.

Das Kennwort für das 'postgres'-Konto nach der Installation von PostgreSQL 11 ändern

Befolgen Sie die nachstehenden Schritte

1. Stoppen Sie die Acronis-Dienste.
   a. Öffnen Sie das Windows-Verwaltungsinstrument 'Dienste', indem Sie Tastenkombination `Win+R` drücken, `services.msc` eingeben und dies mit der Eingabetaste bestätigen.
   b. Stoppen Sie den **Acronis Cyber Files Tomcat**-Dienst, um sicherzustellen, dass der Server die Datenbank während der Änderung nicht aktiv verwendet.
2. Sichern Sie die Konfigurationsdateien. Eine Anleitung finden Sie unter Backup der Cyber Files-Datenbank.
3. Ändern Sie das Kennwort über `pgAdmin 4`.
   a. Öffnen Sie den **Acronis Cyber Files PostgreSQL Administrator** über das **Start**-Menü.
   b. Geben Sie Ihr Master-Kennwort ein, wenn Sie dazu aufgefordert werden.
   c. Erweitern Sie im linken Fensterbereich den Eintrag **Server** und wählen Sie **localhost** aus.
   d. Klicken Sie im oberen Menü auf **Objekt** > **Kennwort ändern**.
   e. Geben Sie das alte Kennwort ein, setzen Sie ein neues Kennwort und klicken Sie auf **OK**, um die Änderungen zu speichern.
4. Aktualisieren Sie die Acronis-Konfiguration.
   a. Gehen Sie zu `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Access Server` und öffnen Sie die Datei `acronisaccess.cfg`.
   b. Suchen Sie die Zeile `DB_PASSWORD =` und aktualisieren Sie diese mit dem neu festgelegten Kennwort.
   c. Speichern Sie die Datei und ersetzen Sie die Originaldatei (möglicherweise sind dafür Administratorrechte erforderlich).
5. Starten Sie die Dienste neu.
   a. Gehen Sie zurück zum Windows-Verwaltungsinstrument 'Dienste' (geben Sie erst `Win+R` und dan `services.msc` ein) und starten Sie den **Acronis Cyber Files Tomcat**-Dienst neu.
6. Testen Sie die Änderungen.
   a. Versuchen Sie sich nach dem Neustart des Dienstes am Acronis Cyber Files Server anzumelden, um zu überprüfen, ob die Datenbankverbindung mit dem neuen Kennwort funktioniert.
   b. Wenn Probleme auftreten, machen Sie die Änderungen rückgängig, indem Sie die Konfigurationsdateien wiederherstellen und die Dienste neu starten.

Ausführen von Acronis Cyber Files im HTTP-Modus

Diese Einstellungen werden für Situationen bereitgestellt, in denen Sie unverschlüsselte HTTP-Kommunikation zwischen Acronis Cyber Files und internen Diensten verwenden müssen, z.B.

Lastenausgleich und Proxy-Lösungen. Acronis Cyber Files-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 Acronis Cyber Files-Netzwerkverkehr 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-Datei `server.xml` unter `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\apache-tomcat-7.0.75\conf`

  Hinweis
  Die Tomcat-Versionsnummer kann sich je nach der von Ihnen verwendeten Version von Acronis Cyber Files unterscheiden.

- Datei `acronisaccess.cfg` unter `C:\Program Files (x86)\Acronis\Acronis Cyber Files\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="TLSv1.2"
   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 `-->` nach `… address="0.0.0.0"/>` ein.
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 `REQUIRE_SSL` am Ende der Datei von **wahr** auf **falsch** festgelegt werden, sodass dies wie folgt aussieht:

```
REQUIRE_SSL = false
```

1. Speichern Sie die Datei, nachdem Sie die erforderlichen Änderungen vorgenommen haben.
2. Starten Sie den Acronis Cyber Files 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`.

Ausführen von Acronis Cyber Files Tomcat unter Verwendung nicht sicherer TLS-Versionen

Hinweis
Bereitstellungen, die ältere TLS-Versionen verwenden, können aufgrund von in diesem Release eingeführten Änderungen ausfallen. Unten sehen Sie einen Workaround, obwohl Acronis derartige Konfigurationen nicht mehr unterstützt.

Ab Acronis Cyber Files 8.8.0 sind alle neuen Installationen und Upgrades nur für die Verwendung von TLSv1.2 konfiguriert.

Diese werden nicht unterstützt und im Ist-Zustand bereitgestellt, um TLSv1 und TLSv1.1 für diejenigen zu aktivieren, die diese nicht sicheren TLS-Versionen evtl. verwenden müssen.

Verwalten von TLS-Konfigurationen während Tomcat 9-Upgrades

Hinweis
Verarbeitung und Update der Connector-Konfiguration ähneln den in Acronis Cyber Files in HTTP-Modus ausführen und Acronis Cyber Files Tomcat auf mehreren Ports ausführen beschriebenen Prozessen.

Hinweis
Stellen Sie vor der Aktivierung von TLSv1 und TLSv1.1 sicher, dass dies wirklich erforderlich ist. Die meisten Webbrowser haben TLSv1 und TLSv1.1 bereits außer Betrieb genommen und verwenden standardmäßig TLSv1.2. Einige andere Dienste, die in Acronis Cyber Files integriert werden können, benötigen evtl. nur ein Update, um mit TLSv1.2 zu arbeiten (Beispielsweise benötigt Office Online Patch KB5001973.)

1. Stoppen Sie Acronis Cyber Files Tomcat.
2. Gehe Sie zur Datei `server.xml`. Deren vorgegebener Speicherpfad lautet:
   `C:\Program Files (x86)\Acronis\Cyber Files\Common\apache-tomcat-9.0.88\conf`

   Hinweis
   Der Pfad kann sich ändern, wenn Sie ein Upgrade auf eine neuere Version von Acronis Cyber Files oder eine benutzerdefinierte Installation durchgeführt haben. Sie können den Acronis Cyber Files Tomcat-Eintrag in Windows-Diensten verwenden, um den Pfad zum Apache Tomcat-Ordner zu suchen, der den Ordner `conf` enthält.
3. Erstellen Sie eine Kopie der ursprünglichen, unbearbeiteten Datei `server.xml` mit einem anderen Namen, falls Sie zur unterstützten Version zurückkehren müssen.
4. Suchen Sie im Abschnitt 'Connector' derselben Datei nach dem Inhalt unten:

   ```
   <Connector maxHttpHeaderSize="65536" maxThreads="150" enableLookups="false"
   disableUploadTimeout="true" acceptCount="100" scheme="https" secure="true"
   SSLEnabled="true" SSLProtocol="TLSv1.2"
   SSLCertificateFile="${catalina.base}/conf/AACert.cer"
   SSLCertificateKeyFile="${catalina.base}/conf/AACert.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" relaxedQueryChars="[,]" port="443" address="0.0.0.0"/>
   ```
5. Ändern Sie den Text auf folgende Weise:

   Von

   ```
   SSLProtocol="TLSv1.2"
   ```

   In

   ```
   SSLProtocol=”TLSv1+TLSv1.1+TLSv1.2"
   ```
6. Speichern Sie die Datei zum Schluss.
7. Starten Sie den AcronisCyber Files Tomcat-Dienst.

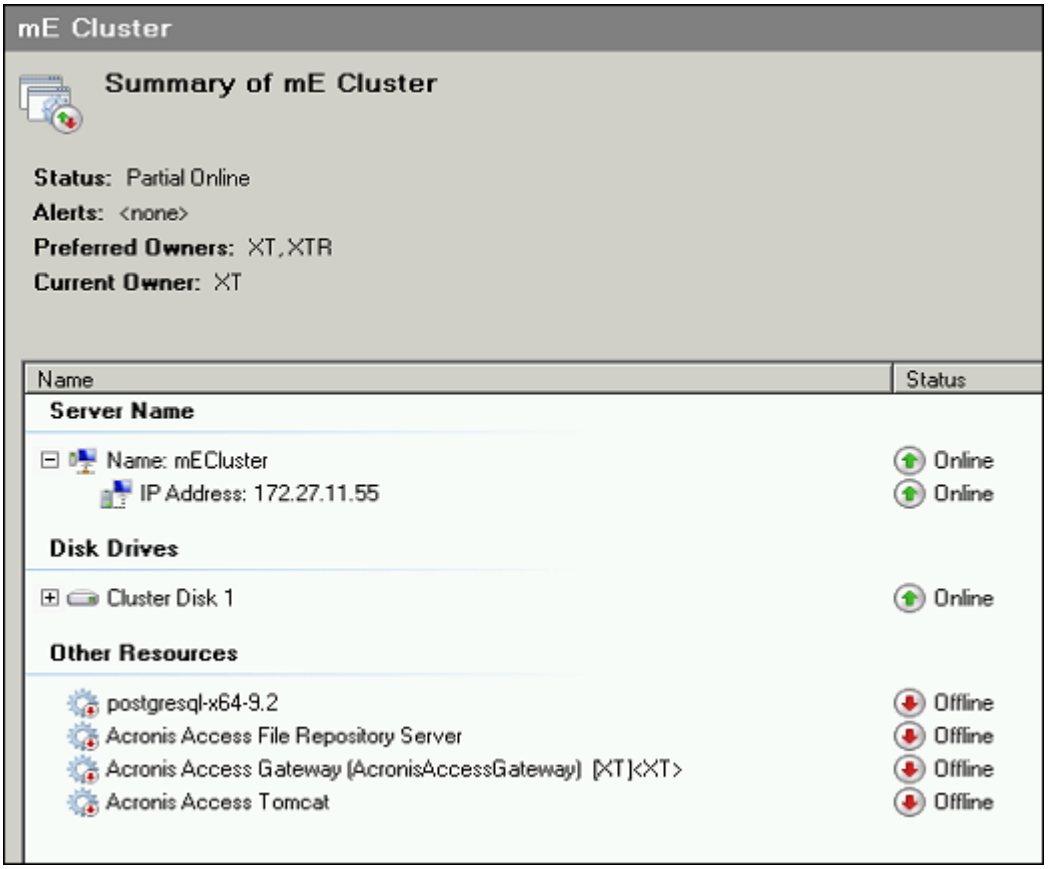
Durchführen eines Upgrades von Acronis Cyber Files auf einem Microsoft Failover Cluster

Die folgenden Schritte helfen Ihnen dabei, ein Upgrade Ihres Acronis Cyber Files Server-Clusters auf eine neuere Version von Acronis Cyber Files durchzuführen.

Hinweis

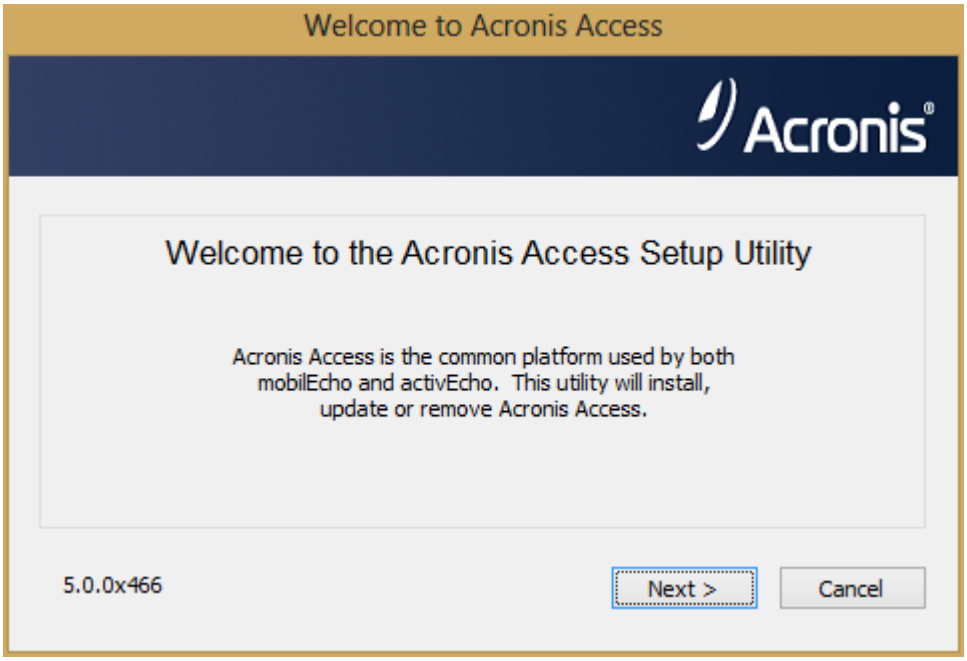
Sehen Sie sich vor der Durchführung eines Upgrades unsere Artikel zum Thema Backup an, und sichern Sie Ihre Konfiguration.

1. Gehen Sie zum aktiven Knoten.
2. Öffnen Sie die **Clusterverwaltung**/den **Failover Cluster Manager**.
3. Stoppen Sie alle Acronis Cyber Files-Dienste (darunter auch **postgres-some-version**). Das freigegebene Laufwerk muss online geschaltet sein.

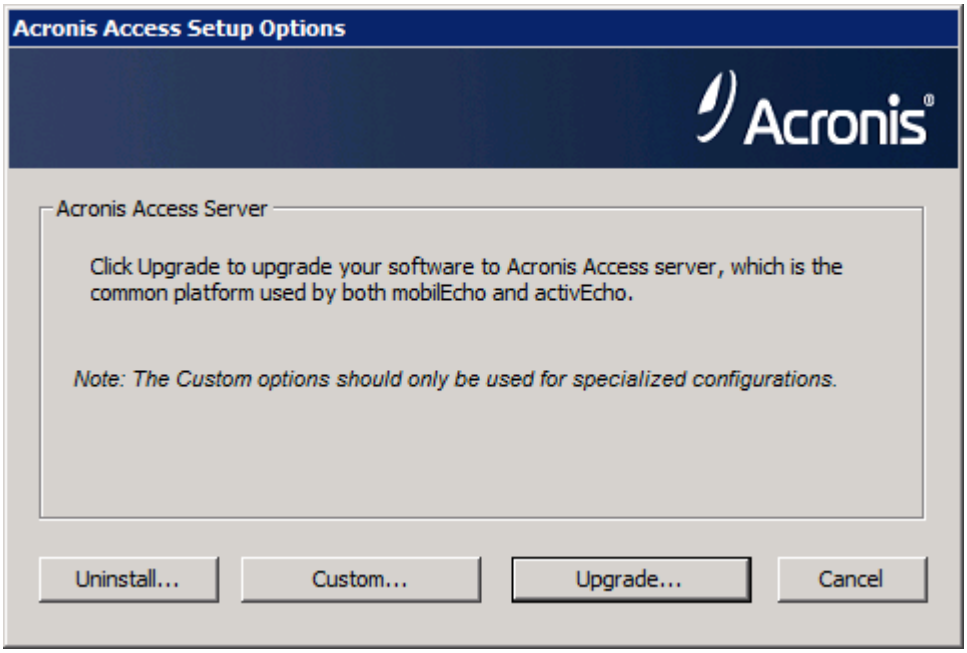


4. Deaktivieren Sie alle vorhandenen Virenschutzprogramme, da sie unter Umständen den Installationsvorgang unterbrechen und somit eine fehlerhafte Installation verursachen können.

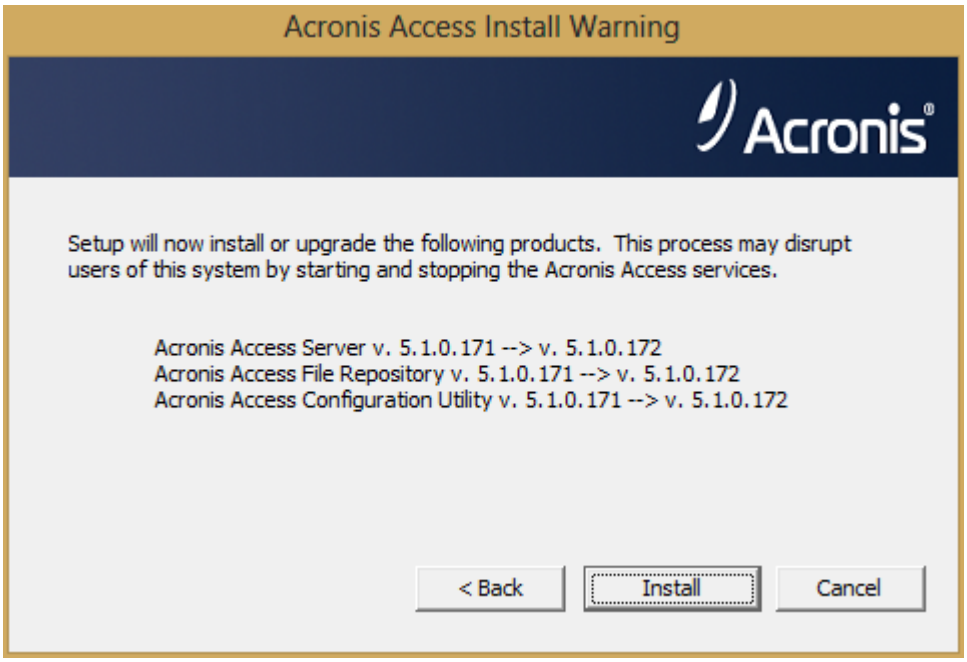
5. Doppelklicken Sie auf die Installationsdatei.



6. Klicken Sie auf **Weiter**, um zu beginnen.
7. Lesen und akzeptieren Sie die Lizenzvereinbarung.
8. Klicken Sie auf **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 das Installationsprogramm zu schließen.

Warnung!
Schalten Sie die Cluster-Gruppe nicht online!

12. Verschieben Sie die Cluster-Gruppe zum zweiten Knoten.
13. Schließen Sie denselben Installationsvorgang auf dem zweiten Knoten ab.
14. Schalten Sie alle Acronis Cyber Files-Dienste online.

Acronis Cyber Files auf einem Microsoft Failover Cluster installieren

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

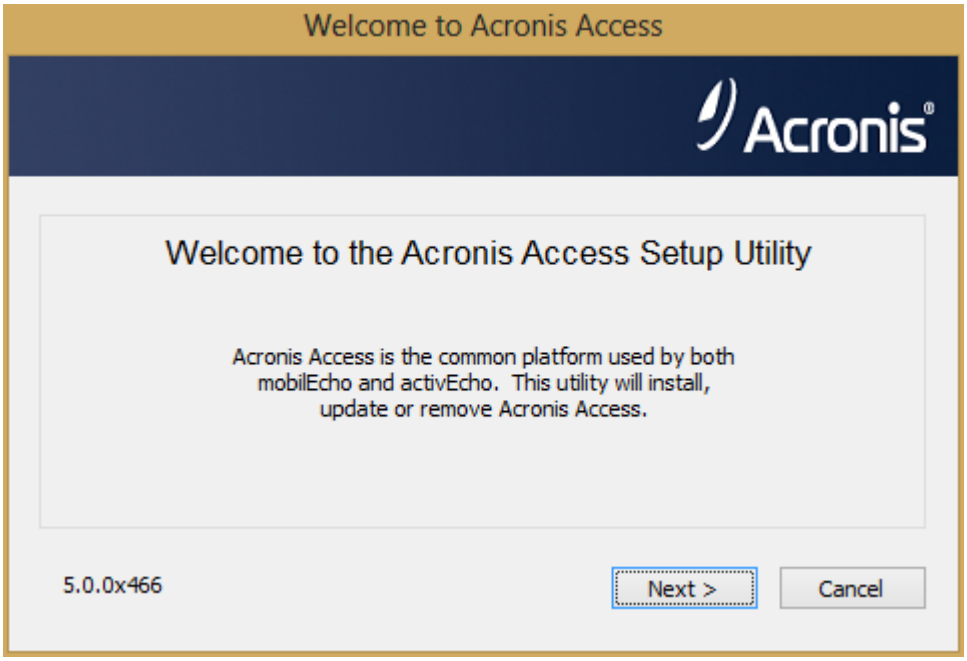
AcronisCyber Files auf einem Microsoft Windows 2012 (R2)-Failover-Cluster installieren

Installation von AcronisCyber Files

Sie müssen als Domain-Administrator angemeldet sein, bevor Sie Acronis Cyber Files installieren.

1. Laden Sie das Installationsprogramm für Acronis Cyber Files 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.

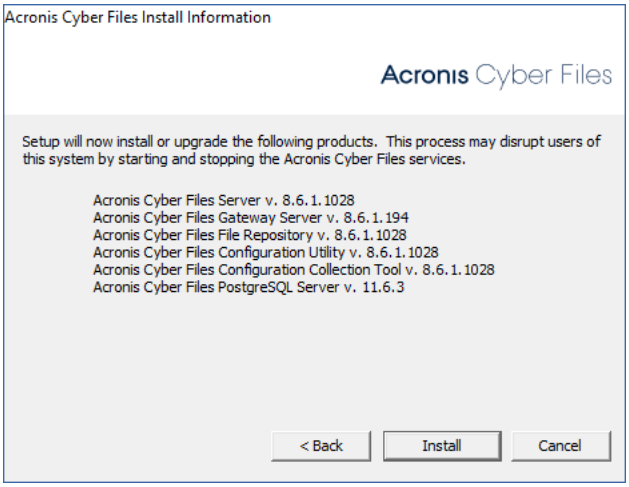


4. Klicken Sie auf **Weiter**, um zu beginnen.
   Lesen und akzeptieren Sie die Lizenzvereinbarung.

5. Klicken Sie auf **Installieren**.

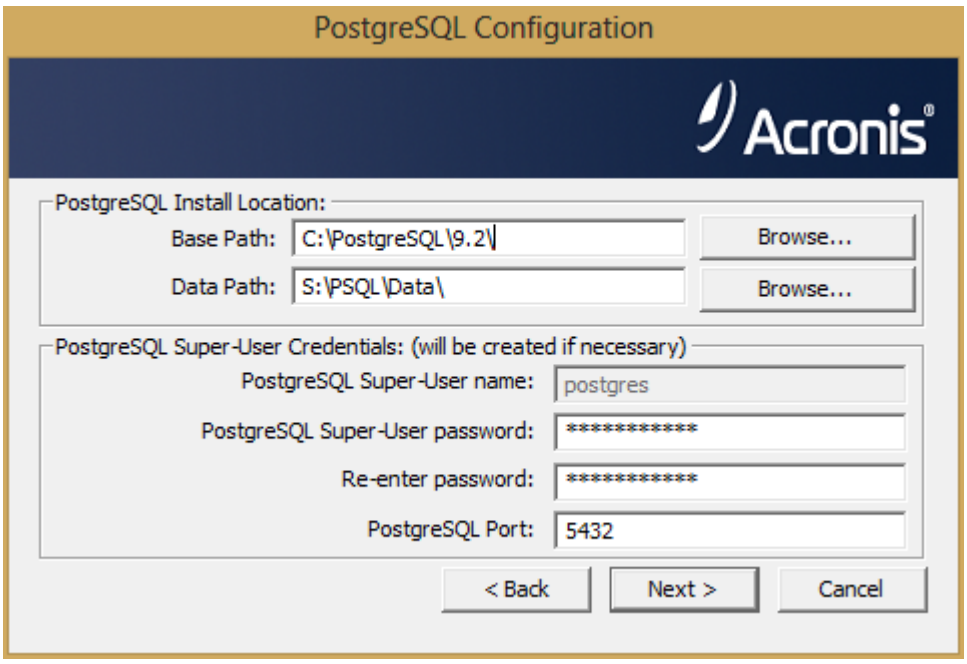
Hinweis
Wenn Sie mehrere Acronis Cyber Files-Server einsetzen oder eine nicht standardmäßige Konfiguration installieren möchten, können Sie über die Schaltfläche **Benutzerdefinierte Installation** festlegen, welche Komponenten installiert werden sollen.

6. Verwenden Sie den Standardpfad, oder wählen Sie einen neuen aus dem Hauptordner von Acronis Cyber Files aus, und klicken Sie auf **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 klicken Sie auf **Weiter**.

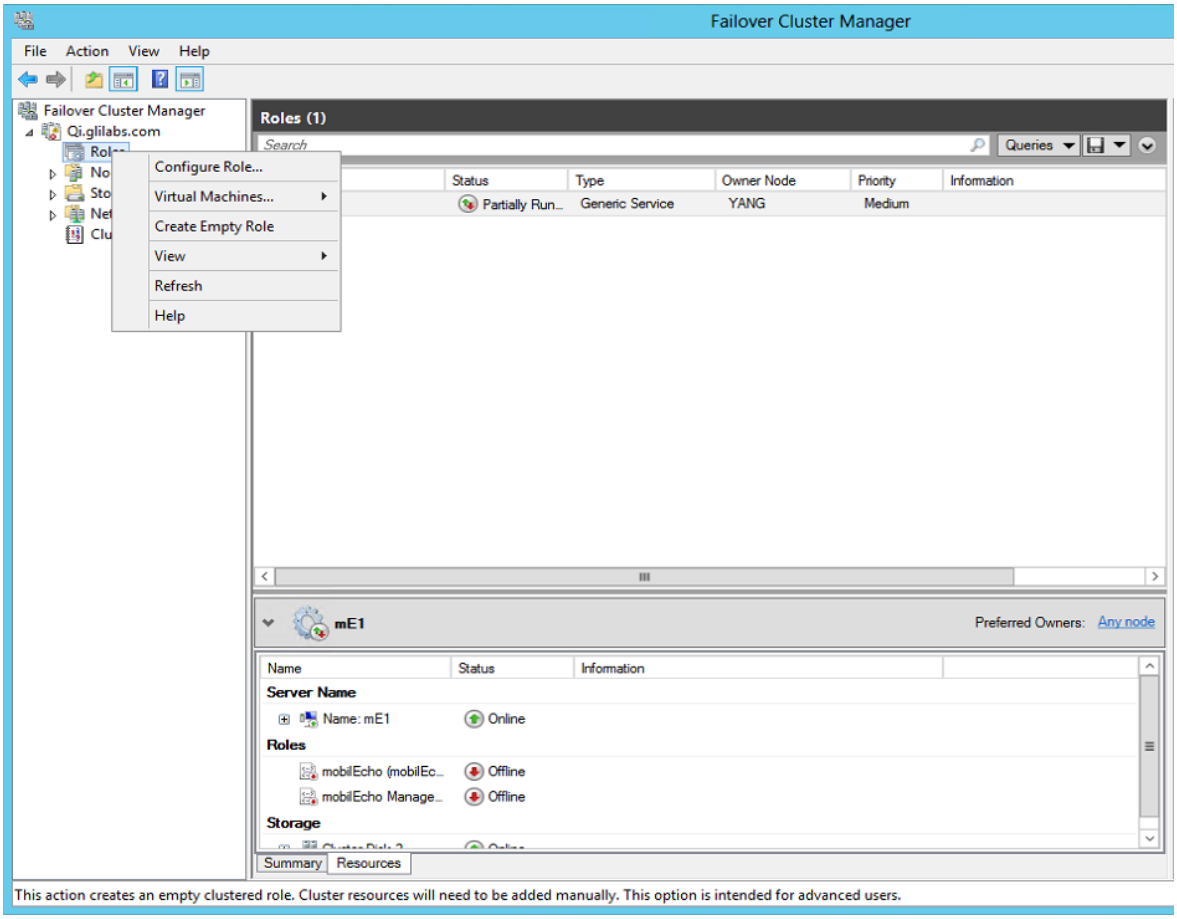


9. Ein Fenster wird geöffnet, in dem alle zur Installation ausgewählten Komponenten angezeigt werden. Klicken Sie auf **OK**, um fortzufahren.
10. Klicken Sie nach Abschluss des Acronis Cyber Files-Installationsprogramms auf **Beenden**.

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 (Beispiel:

Acronis Cyber Files, 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\Acronis Cyber Files\Gateway Server\`.
   b. Suchen Sie die Datei **database.yml** und öffnen Sie sie mit einem Texteditor.
   c. Suchen Sie nach der Zeile `database_path: './database/'`, und ersetzen Sie **./database/** durch den gewünschten Pfad (z.B. `database_path: 'S:/access_cluster/database/'`).

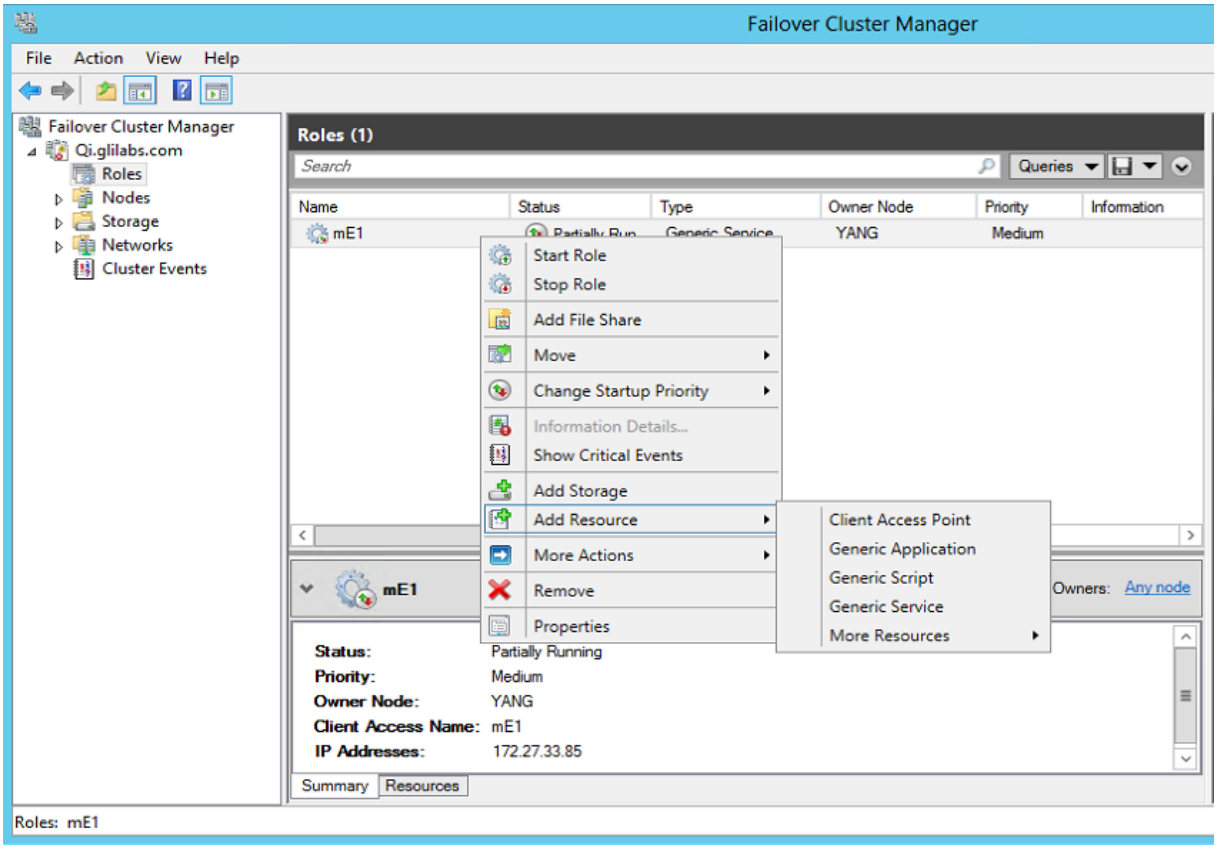
   Hinweis
   Verwenden Sie als Pfadtrennzeichen Schrägstriche (/).

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

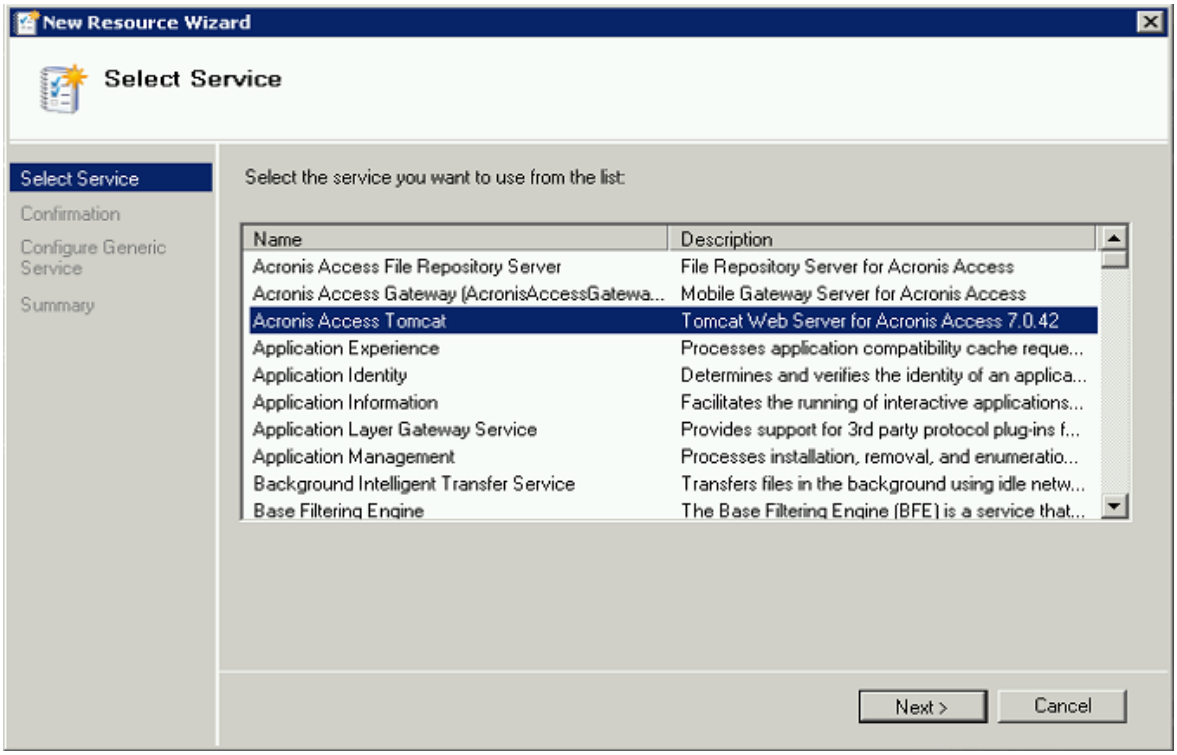
Hinzufügen aller erforderlichen Dienste zur Acronis Cyber Files-Rolle

Führen Sie das folgende Verfahren für jeden der aufgeführten Dienste aus: Acronis Cyber Files Gateway, Acronis Cyber Files PostgreSQL (abhängig von der Acronis Cyber Files Version), Acronis Cyber Files Repository und Acronis Cyber Files Tomcat.

1. Klicken Sie mit der rechten Maustaste auf die Acronis Cyber Files-Rolle, und wählen Sie **Ressource hinzufügen**.
2. Wählen Sie **Allgemeiner Dienst** aus.



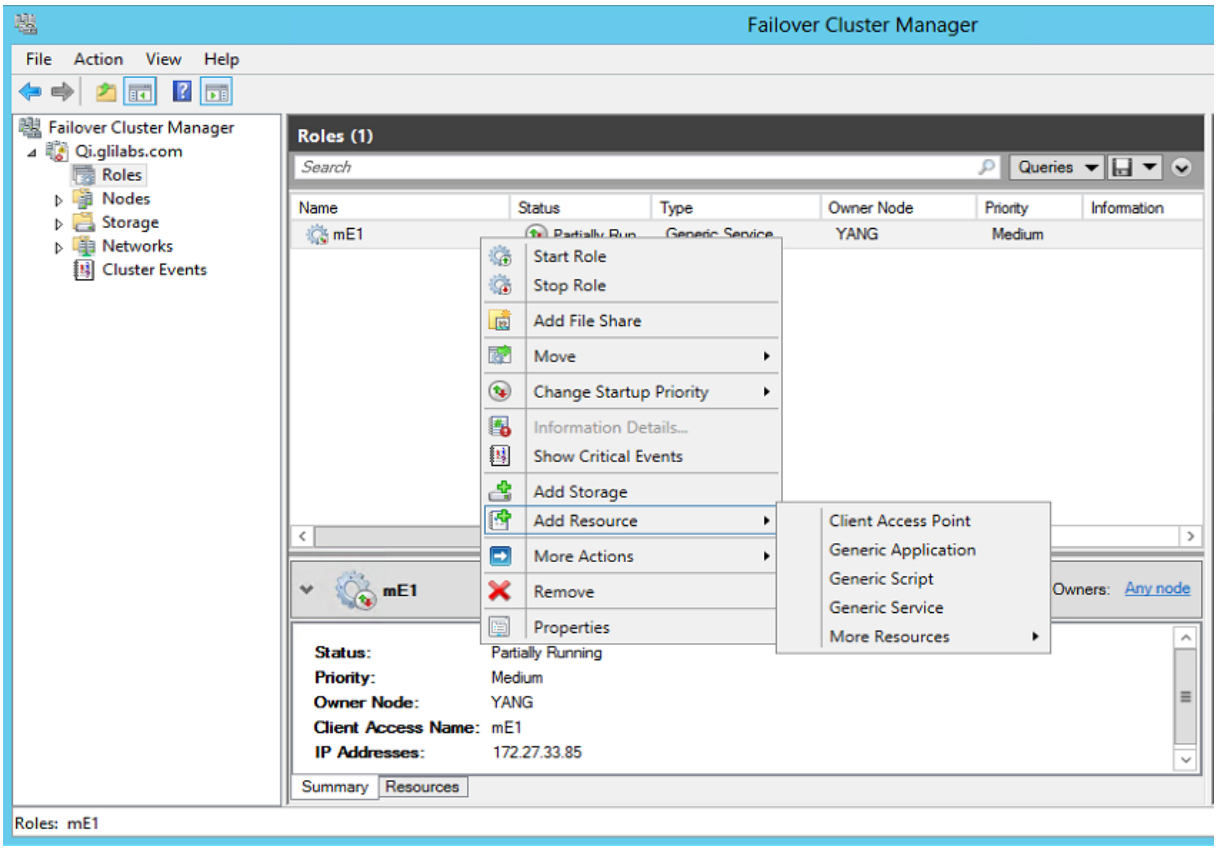
3. Wählen Sie den geeigneten Dienst aus und klicken Sie auf **Weiter**.



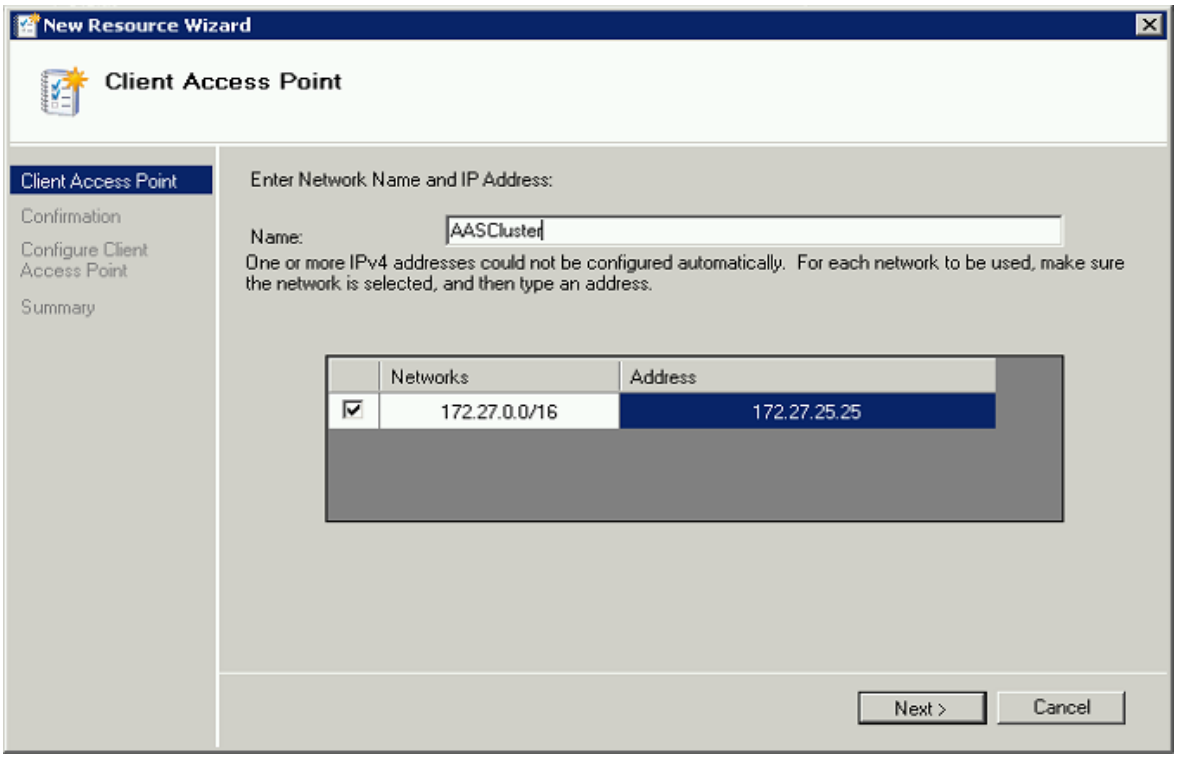
4. Klicken Sie im Bestätigungsfenster auf **Weiter**.
5. Klicken sie im Fenster 'Zusammenfassung' auf **Fertig stellen**.

Festlegen eines Zugriffspunkts

1. Klicken Sie mit der rechten Maustaste auf die Acronis Cyber Files-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.

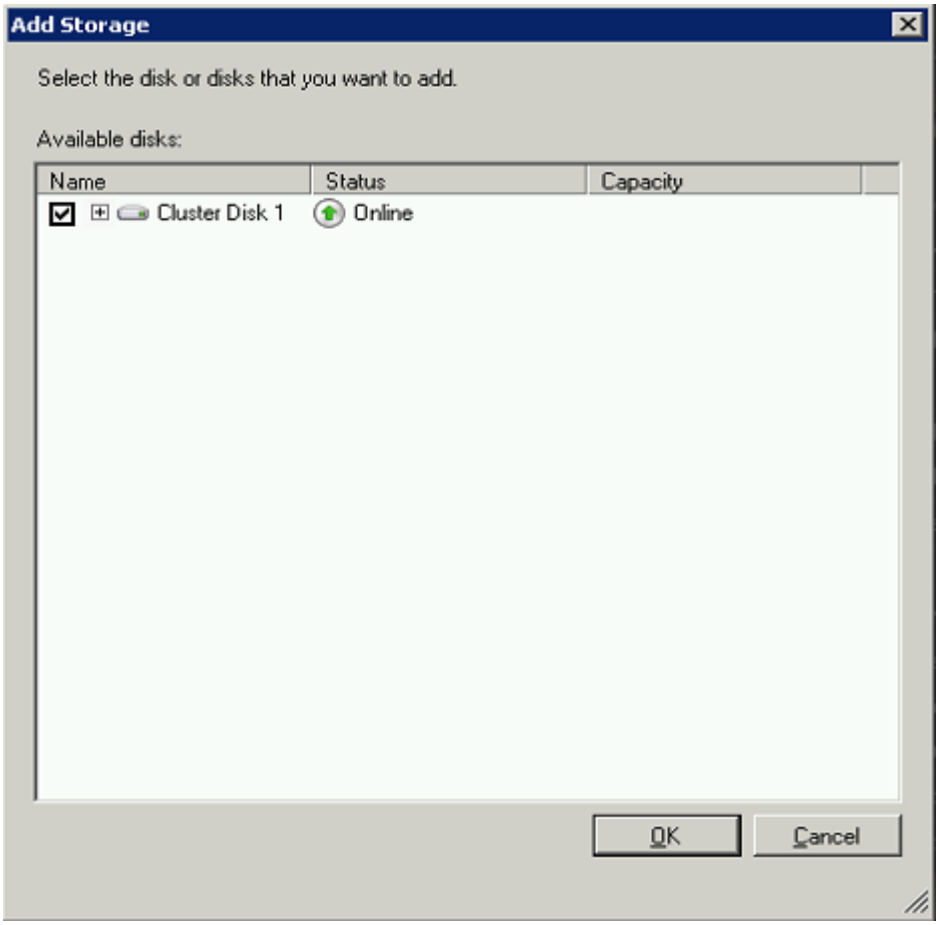


5. Geben Sie die IP-Adresse ein und klicken Sie auf **Weiter**.

6. Klicken Sie im Bestätigungsfenster auf **Weiter**.
7. Klicken sie im Fenster 'Zusammenfassung' auf **Fertig stellen**.

Hinzufügen eines freigegebenen Laufwerks

1. Klicken Sie mit der rechten Maustaste auf die Acronis Cyber Files-Rolle, und wählen Sie **Speicher hinzufügen**.
2. Wählen Sie das gewünschte freigegebene Laufwerk aus.

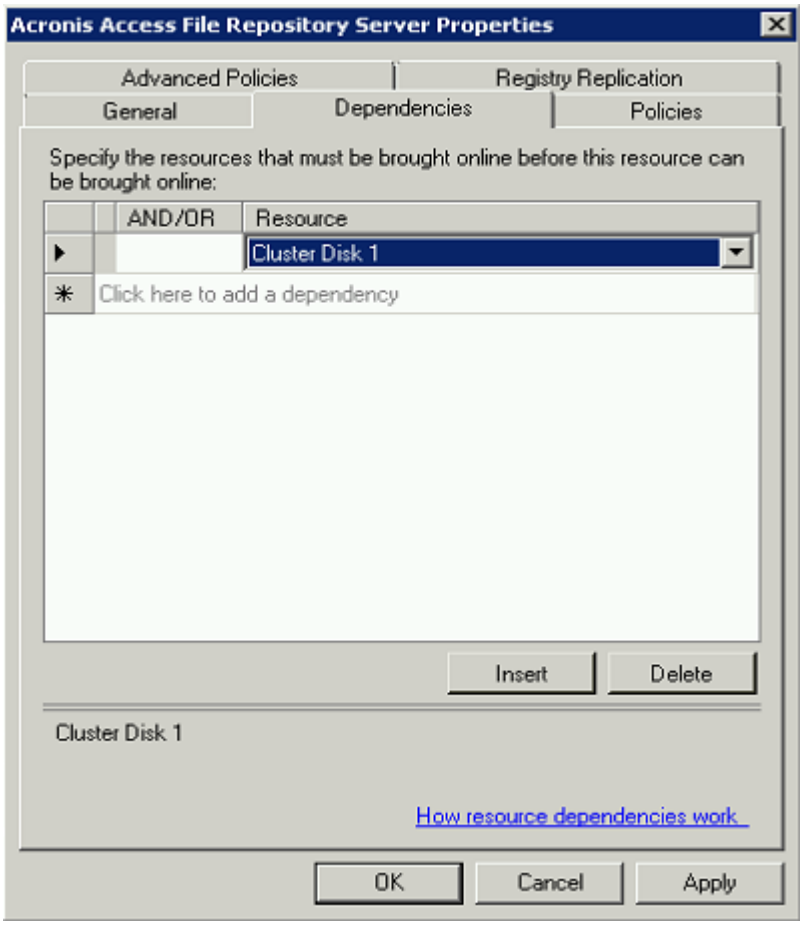


Konfigurieren von Abhängigkeiten

1. Wählen Sie die Acronis Cyber Files-Rolle aus, und klicken Sie auf die Registerkarte **Ressourcen**.

Gehen Sie für PostgreSQL- und Acronis Cyber Files File Repository-Dienste wie folgt vor:

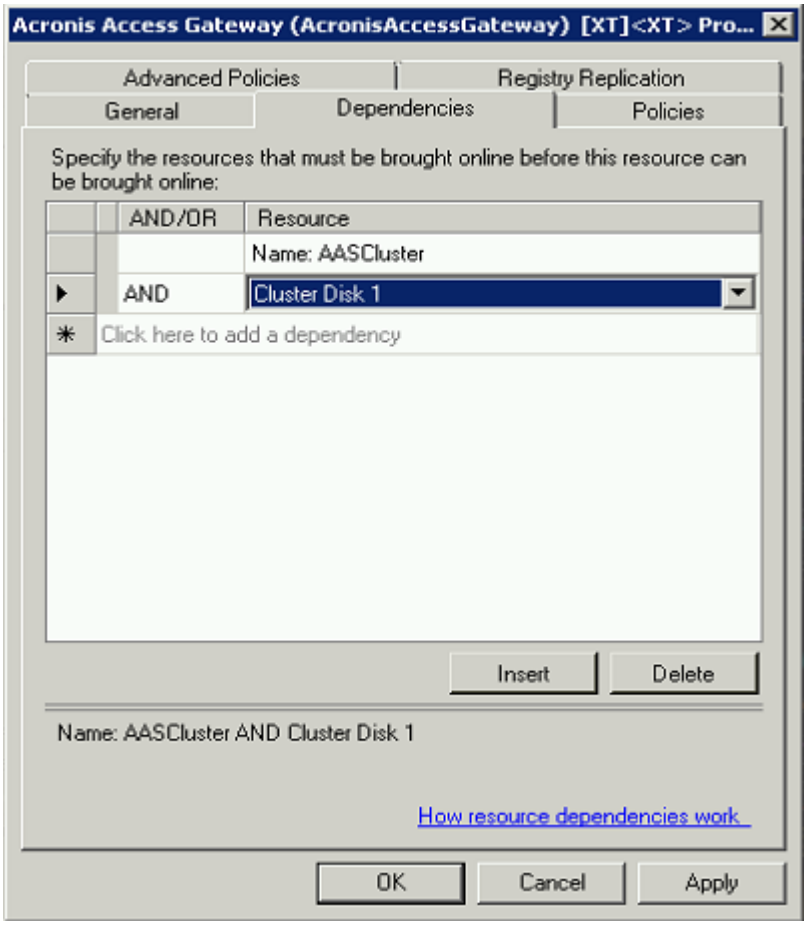
1. Klicken Sie mit der rechten Maustaste auf den entsprechenden Dienst und wählen Sie **Eigenschaften**.
2. Klicken Sie auf die Registerkarte **Abhängigkeiten**.
3. Klicken Sie auf **Ressource** und wählen Sie das freigegebene Laufwerk aus, das Sie hinzugefügt haben.



4. Drücken Sie **Anwenden** und schließen Sie das Fenster.

Gehen Sie für den Gateway Server-Dienst von Acronis Cyber Files wie folgt vor:

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).

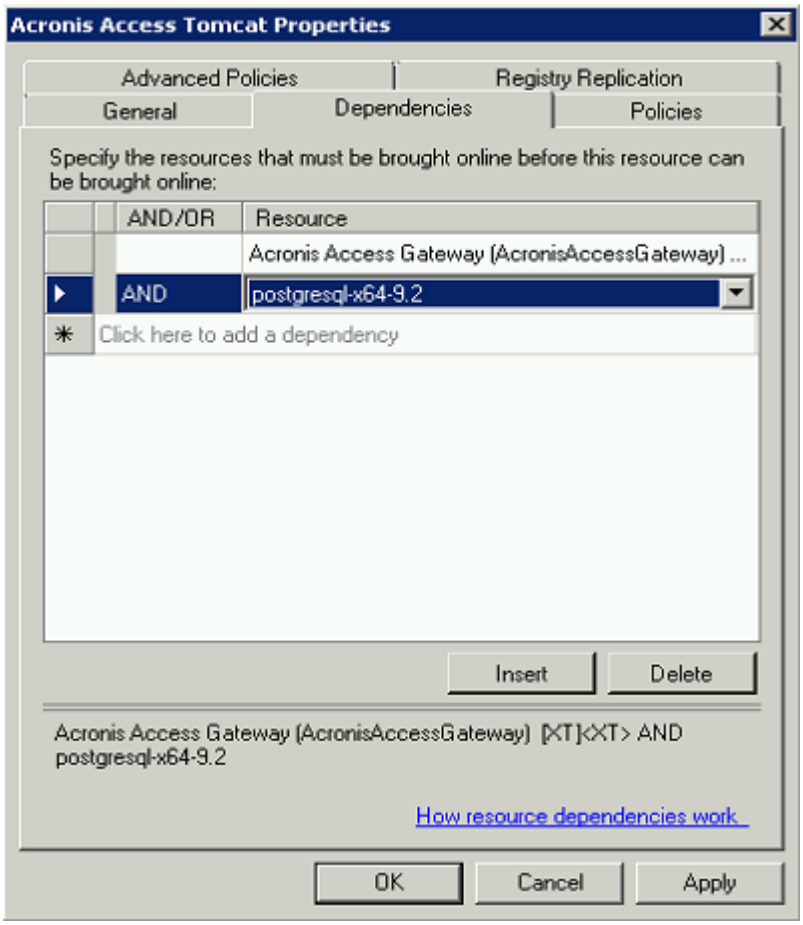


4. Drücken Sie **Anwenden** und schließen Sie das Fenster.

Gehen Sie für den Acronis Cyber Files Tomcat-Dienst wie folgt vor:

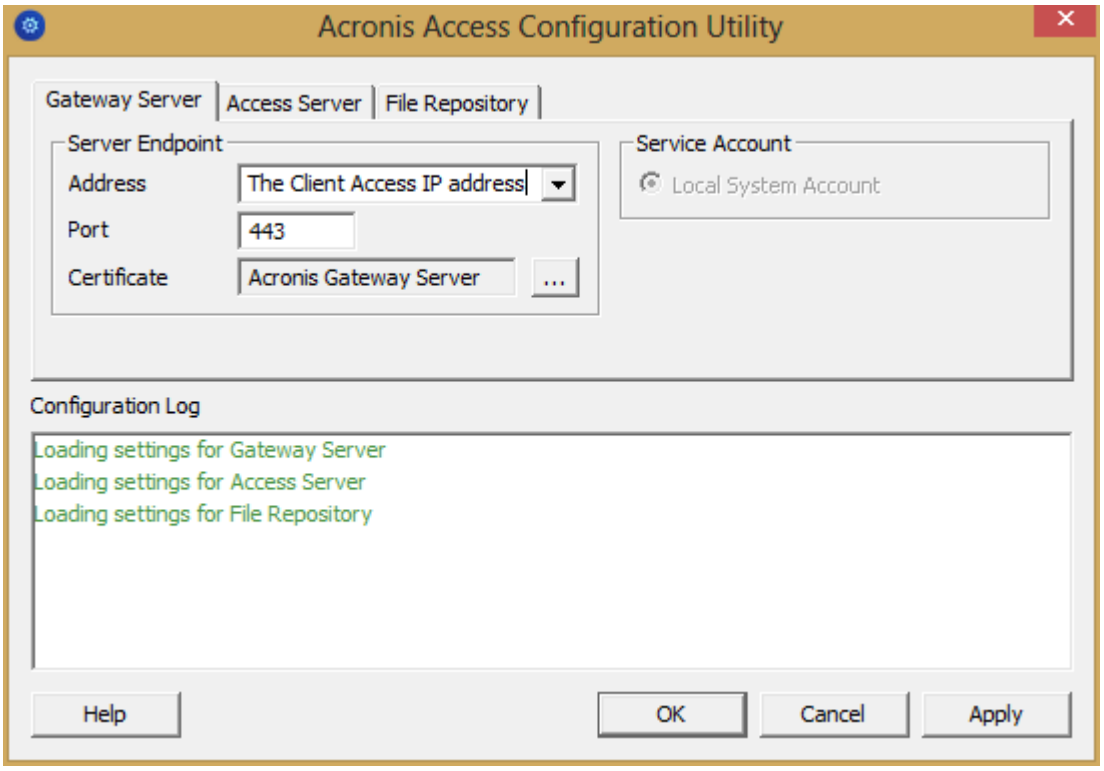
1. Klicken Sie mit der rechten Maustaste auf den entsprechenden Dienst und wählen Sie **Eigenschaften**.
2. Klicken Sie auf die Registerkarte **Abhängigkeiten**.
3. Klicken Sie auf **Ressource**, und wählen Sie die PostgreSQL- und Acronis Cyber Files Gateway Server-Dienste als Abhängigkeiten aus. Drücken Sie **Anwenden** und schließen Sie das Fenster.

Hinweis
Wenn Gateway und Web Server von Acronis Cyber Files auf verschiedenen IP-Adressen ausgeführt werden sollen, fügen Sie die zweite IP-Adresse der Acronis Cyber Files-Rolle als Ressource hinzu, und legen Sie sie als Abhängigkeit für den Netzwerknamen fest.



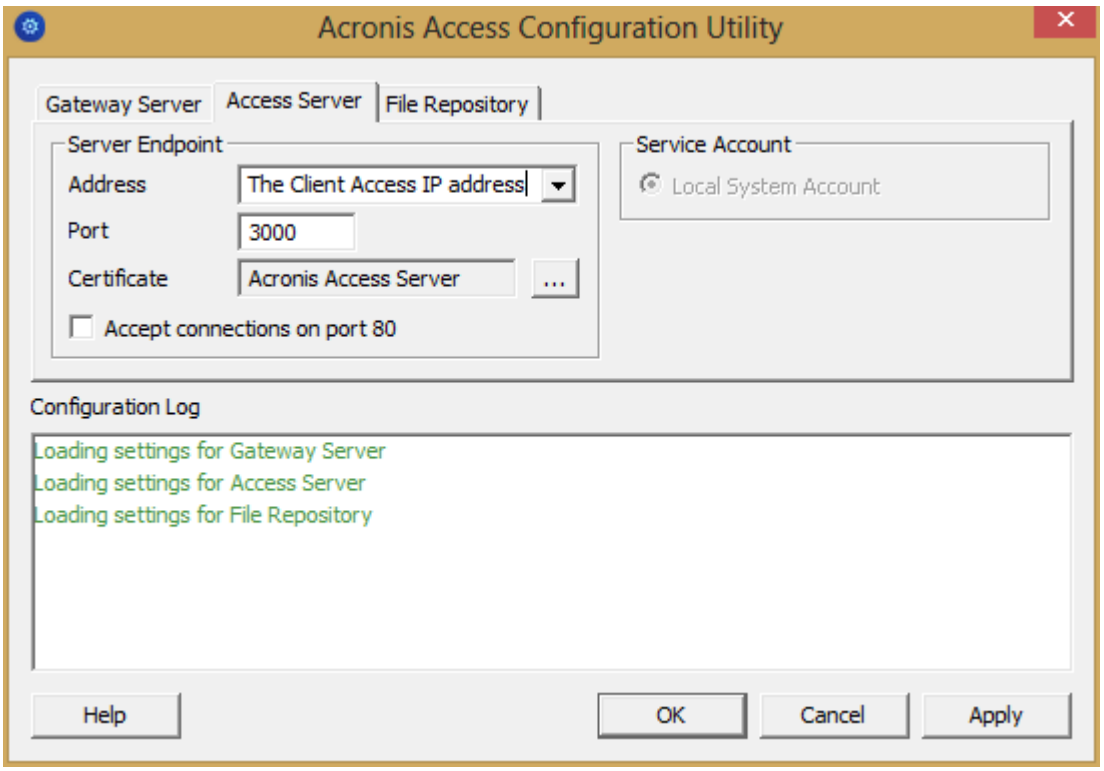
Starten der Rolle und Verwenden des Konfigurationswerkzeugs

1. Klicken Sie mit der rechten Maustaste auf die Acronis Cyber Files-Rolle, und wählen Sie **Rolle starten** aus.
2. Starten Sie das Konfigurationswerkzeug. Bei einer Neuinstallation befindet sich dies normalerweise unter `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\Configuration Utility`.
3. Konfigurieren Sie den Acronis Cyber Files Gateway Server-Dienst, um die IP-Adresse(n) für die AcronisCyber Files Service-Gruppe abzuhören.

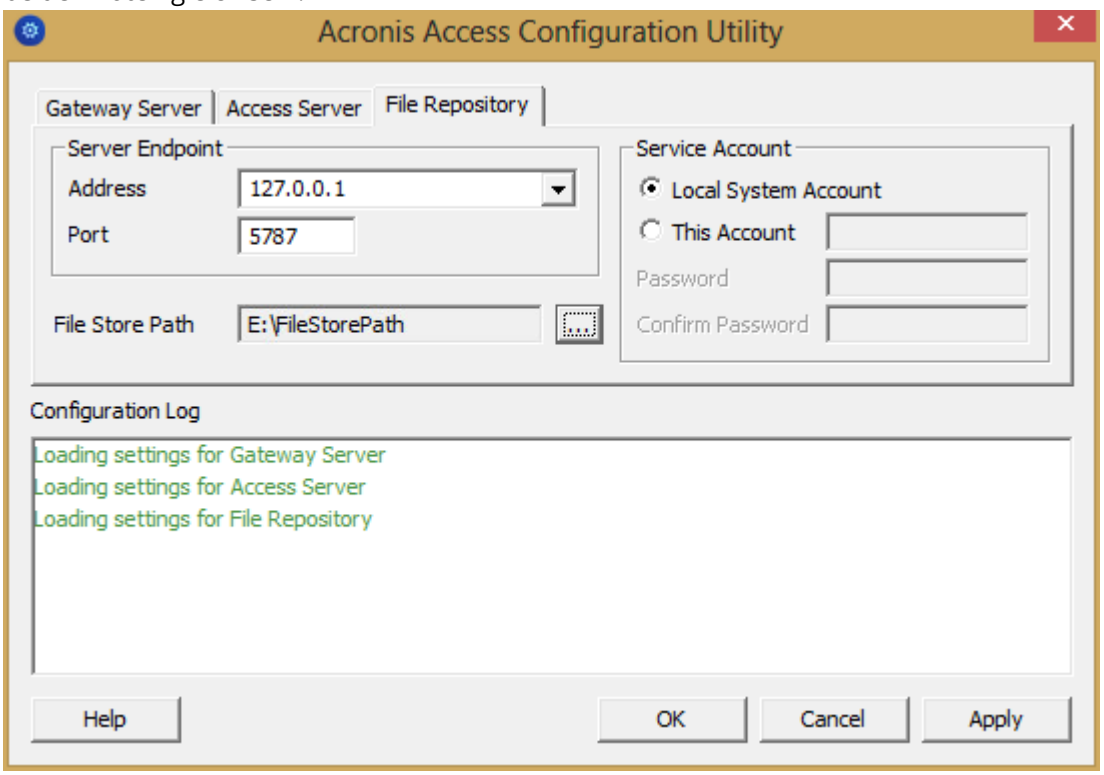


4. Konfigurieren Sie den Acronis Cyber Files Server-Dienst, um die IP-Adresse(n) für die Acronis Cyber Files Service-Gruppe abzuhören.

Hinweis
Wenn **Umleitungsanforderungen von Port 80** ausgewählt ist,



5. Konfigurieren Sie das AcronisCyber Files File Repository, um 'localhost' abzuhören, und ändern Sie den Filestore-Pfad in ein Verzeichnis auf dem freigegebenen Laufwerk. Dieser Pfad sollte für beide Knoten gleich sein.



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

Installation und Konfiguration auf dem zweiten Knoten

1. Deaktivieren Sie alle vorhandenen Virenschutzprogramme, da sie unter Umständen den Installationsvorgang unterbrechen und somit eine fehlerhafte Installation verursachen können.
2. Installieren Sie Acronis Cyber Files 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\Acronis Cyber Files\Gateway Server\`.
   b. Suchen Sie die Datei **database.yml** und öffnen Sie sie mit einem Texteditor.
   c. Suchen Sie nach der 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 (/).

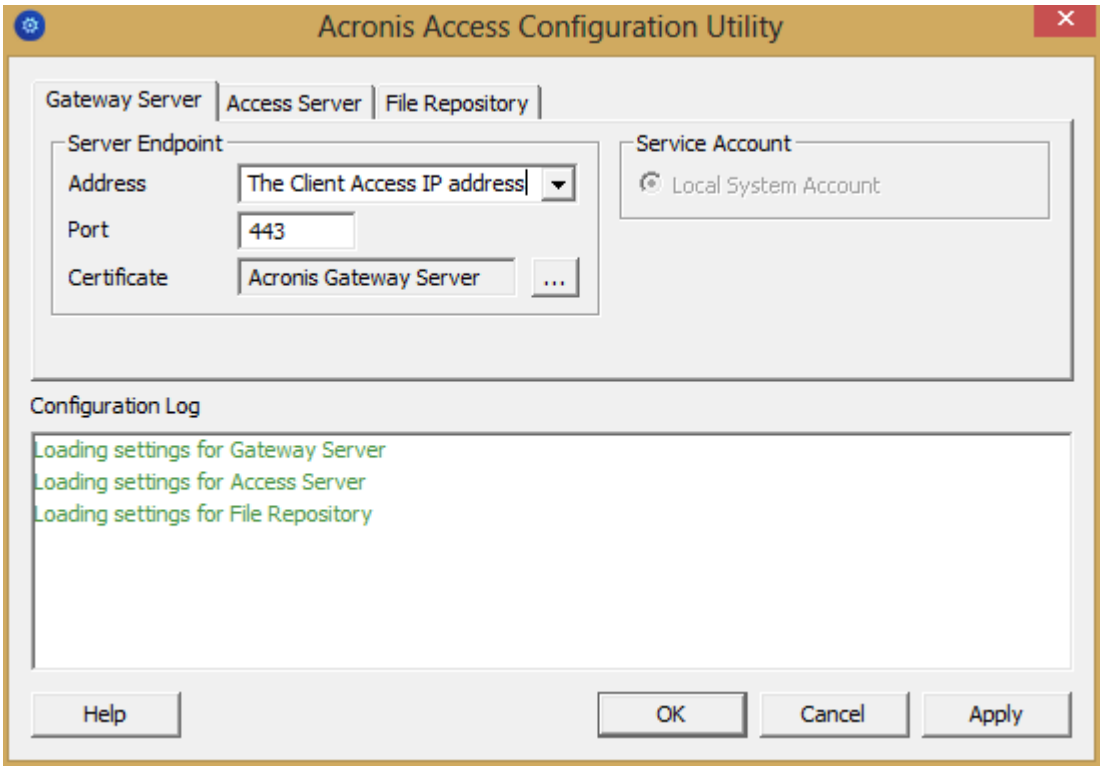
Hinweis
Sie können die konfigurierte Datei 'database.yml' aus dem ersten Knoten kopieren und im zweiten Knoten einfügen.
Der Pfad sollte mit dem Pfad auf dem ersten Knoten übereinstimmen.

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. Klicken Sie auf**Hinzufügen**, und geben Sie Folgendes ein:
   `SYSTEM\CurrentControlSet\Services\AcronisAccessPostgreSQL\`(Für ältere Versionen von Acronis Cyber Files kann der Dienst anders sein, z.B. **postgresql-x64-9.2**.)
6. Verschieben Sie die Acronis Cyber Files-Rolle in den zweiten Knoten.

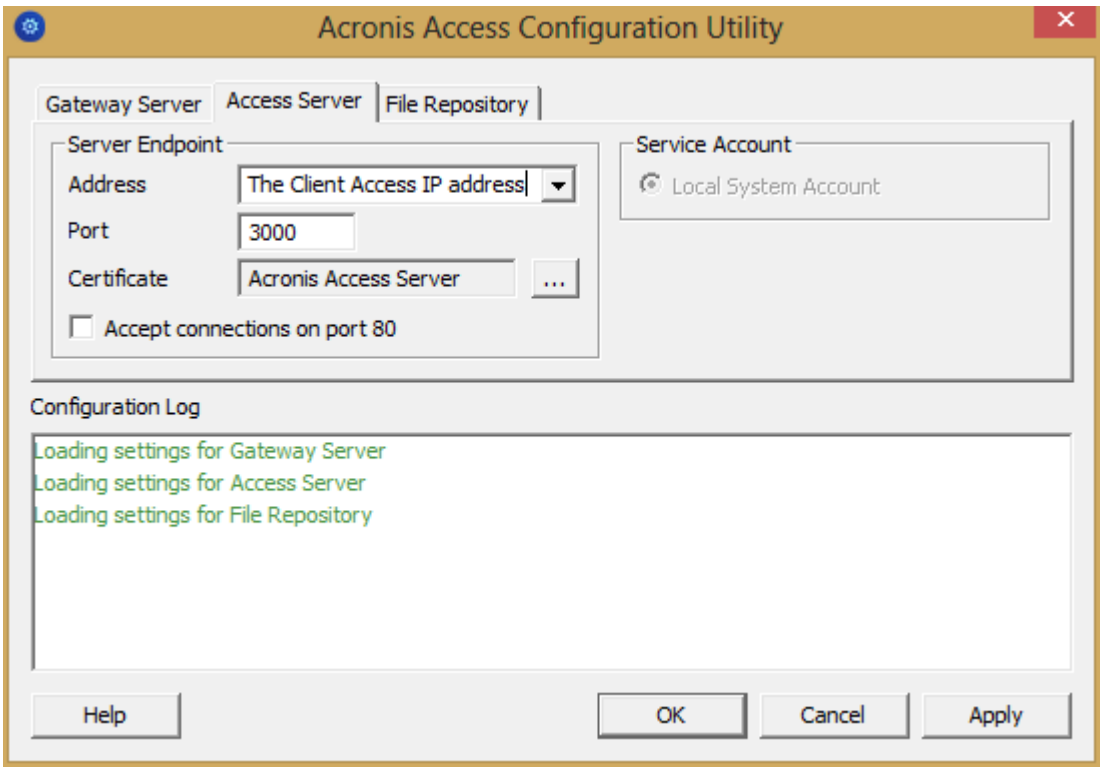
Verwenden des Konfigurationswerkzeugs auf dem zweiten Knoten

1. Klicken Sie mit der rechten Maustaste auf die Acronis Cyber Files-Rolle, und wählen Sie **Rolle starten** aus.
2. Starten Sie das Konfigurationswerkzeug. Bei einer Neuinstallation befindet sich dies normalerweise unter `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\Configuration Utility`.
3. Konfigurieren Sie den Acronis Cyber Files Gateway Server-Dienst, um die IP-Adresse(n) für die AcronisCyber Files Service-Gruppe abzuhören.

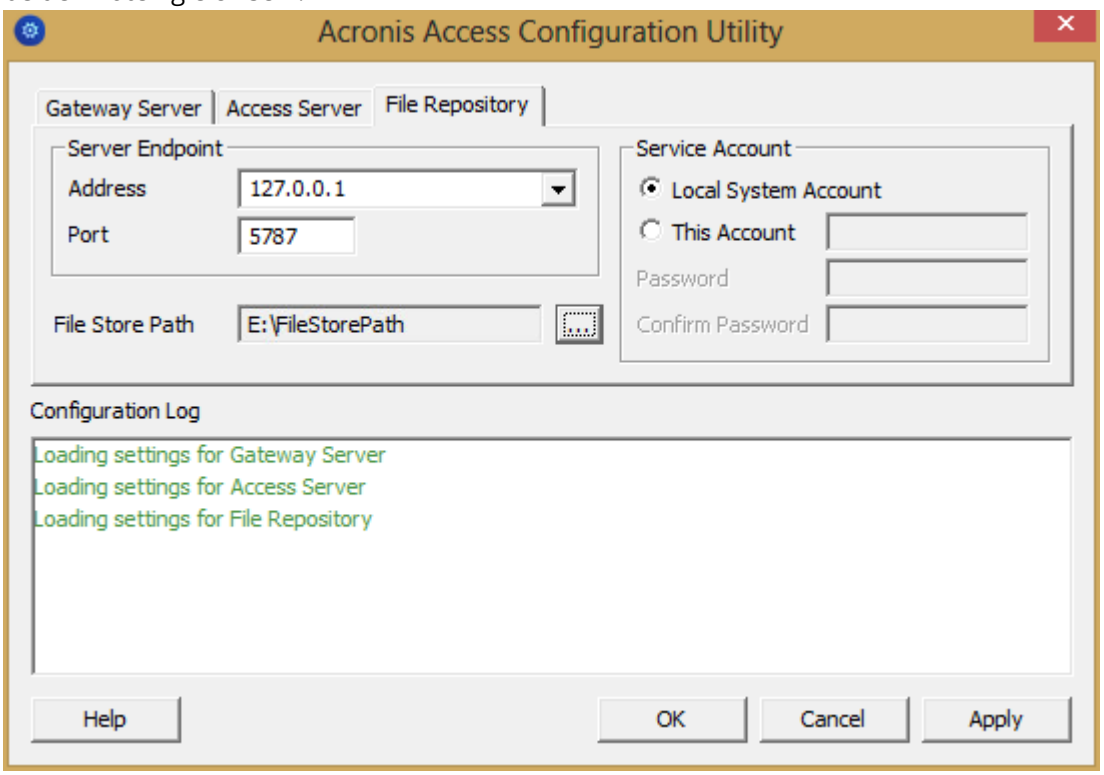


4. Konfigurieren Sie den Acronis Cyber Files Server-Dienst, um die IP-Adresse(n) für die Acronis Cyber Files Service-Gruppe abzuhören.

Hinweis
Wenn **Umleitungsanforderungen von Port 80** ausgewählt ist,



5. Konfigurieren Sie das AcronisCyber Files File Repository, um 'localhost' abzuhören, und ändern Sie den Filestore-Pfad in ein Verzeichnis auf dem freigegebenen Laufwerk. Dieser Pfad sollte für beide Knoten gleich sein.



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

IPv6-Einrichtung

Vor Beginn – bekannte Einschränkungen

Aktuell unterstützt das Konfigurationswerkzeug IPv6 nicht automatisch. Nach manuellen Änderungen an der Datei `server.xml` und den SSL-Bindings können Sie das Konfigurationswerkzeug nicht mehr verwenden, da es alle Änderungen löscht, die nicht von dieser Benutzeroberfläche unterstützt werden. Alle Neustarts und Bearbeitungen der Serverkonfiguration müssen manuell durchgeführt werden, bis das Konfigurationswerkzeug IPv6 unterstützt.

Die manuellen Änderungen an den Dateien `web.xml` und `server.xml` werden bei einem Upgrade nicht beibehalten. Stellen Sie sicher, dass Sie diese Dateien an einem Speicherort außerhalb der Acronis Cyber Files Server-Installation sichern. Nach einem Upgrade müssen Sie die manuell bearbeitete Datei mit der neu installierten Datei abgleichen und nötige Änderungen migrieren.

Alle Adressen, die über IPv6 aufgelöst werden, müssen als DNS-Adressen in der webUI angegeben werden.

Hinweis
Die Funktion „Zugriffsbeschränkungen für die Verwaltungsseite“ auf der Verwaltungsseite erfordert eine Spanne von IPs, die berechtigt sind, auf Verwaltungsseiten zuzugreifen. Das aktuelle Format der Benutzeroberfläche unterstützt nur IPv4.

IPv6-Konfiguration durchführen

Es sind drei Schritte erforderlich, um IPv6-Support zu aktivieren.

IPv6-Setup Schritt 1: Gateway-Setup

Damit das Gateway mit IPv6 funktioniert, müssen Sie eine SSL-Bindung erstellen und die gewünschten Adressen zur Liste `iplisten` hinzufügen.

Hinweis
Um diesen Schritt abschließen zu können, benötigen Sie den `thecerthash`-Wert aus dem Fingerabdruck des Acronis Access-Zertifikats, die gewünschte IPv6-IP-Adresse und den Port, den das Gateway abhören soll. Informationen darüber, wie Sie den certhash-Wert ermitteln können, finden Sie im Abschnitt Einen Acronis Access Zertifikat-Fingerabdruck abrufen.

Eine SSL-Bindung erstellen

Sie können eine Bindung für alle IPv6-Adressen oder für eine bestimmte IPv6-Adresse erstellen.

An alle IPv6-Adressen binden

Der Befehl muss wie folgt aussehen:

```
netsh http add sslcert ipport=[::]:YourPortNumber certhash=YourCerthashValue appid={72876ec6-d443-48ef-add3-fa7a0cbc4762} certstorename=MY clientcertnegotiation=enable dsmapperusage=enable
```

Wichtig
Sie sollten den Port eingeben, auf dem Ihr Gateway abhören soll. Ersetzen Sie den `certhash` mit dem Wert aus Ihrem Zertifikat.

Hinweis
Um eine Bindung für eine *bestimmte* IPv6 Adresse zu erstellen, ersetzen Sie “`::`” mit der gewünschten Adresse.

Hinweis
Wenn Sie eine SSL-Bindung löschen müssen, verwenden Sie den folgenden Befehl, um die Adresse und den Port einzugeben, die für die zu entfernenden Werte stehen sollen:
netsh http delete sslcert ipport=[**AddressToRemove**]:**PortToRemove**

Fügen Sie die gewünschte IPv6-Adresse zur Liste `iplisten` hinzu

Sie können entweder alle IP-Adressen oder eine bestimmte IP-Adresse zur `iplisten`-Liste hinzufügen.

Alle IPv6-IP-Adressen zur Liste `iplisten` hinzufügen

1. Verwenden Sie den folgenden Befehl: `netsh http add iplisten ipaddress=::`

   Hinweis
   Ersetzen Sie zum Hinzufügen einer *spezifischen* IPv6-IP-Adresse zur 'iplisten'-Liste "**::**" mit der gewünschten IPv6-IP-Adresse.
   `E.g.: netsh http add iplisten ipaddress=fd59:ffdf:9580::3`

2. Starten Sie den Gateway Service über Windows Services neu.

Hinweis
Sie sollten jetzt in der Lage sein, auf das Gateway sowohl über localhost (::1) als auch über jede beliebige IP-Adresse zuzugreifen.
Wenn Sie eine bestimmte IPv6-Adresse konfigurieren, können Sie nicht über 'localhost' auf das Gateway zugreifen. Dies ist nur über die angegebene Adresse möglich.

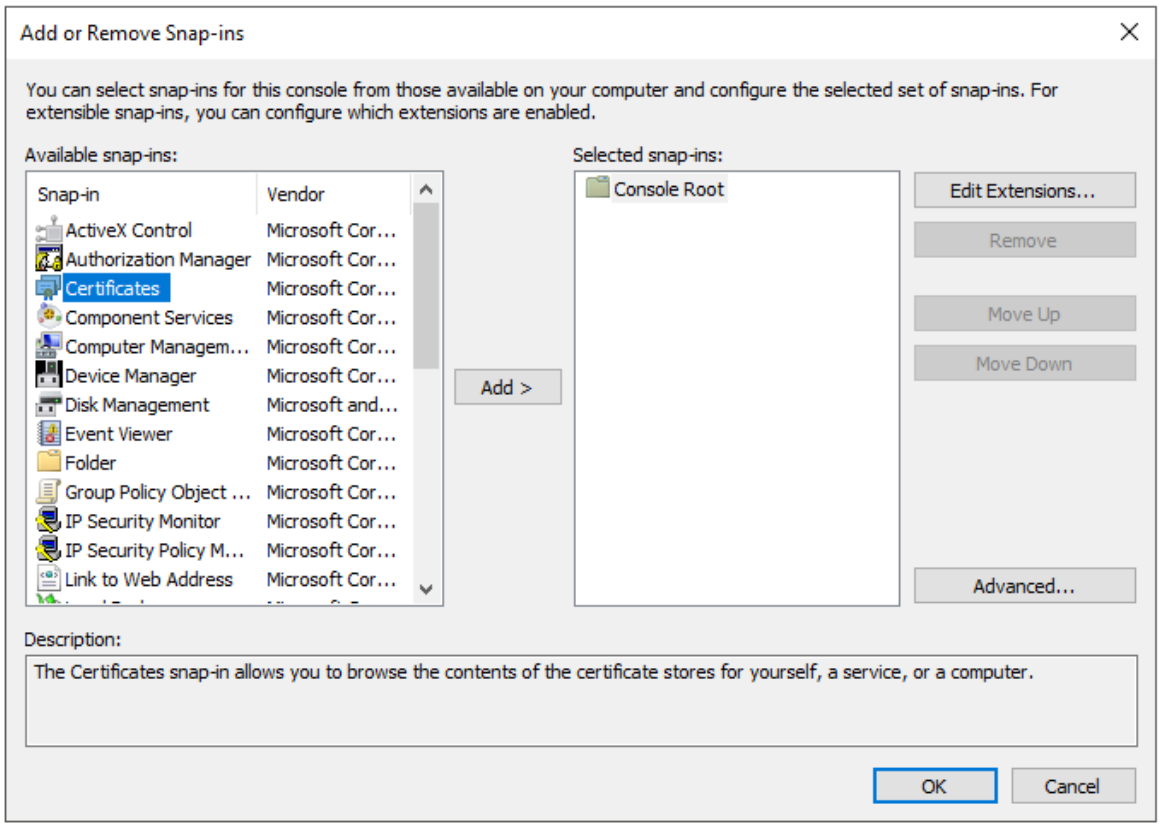
Warnung!
Wenn Sie über localhost auf das Gateway zugreifen möchten, nachdem Sie eine spezifische IP-Adresse konfiguriert haben, müssen Sie die spezifische Adresse mit dem folgenden Befehl aus der Liste `iplisten` entfernen und den Gateway Service über Windows Services erneut starten.
Beispiel: netsh http delete iplisten ipaddress=fd59:ffdf:9580::3

Den Fingerabdruck eines Acronis Access-Zertifikats abrufen

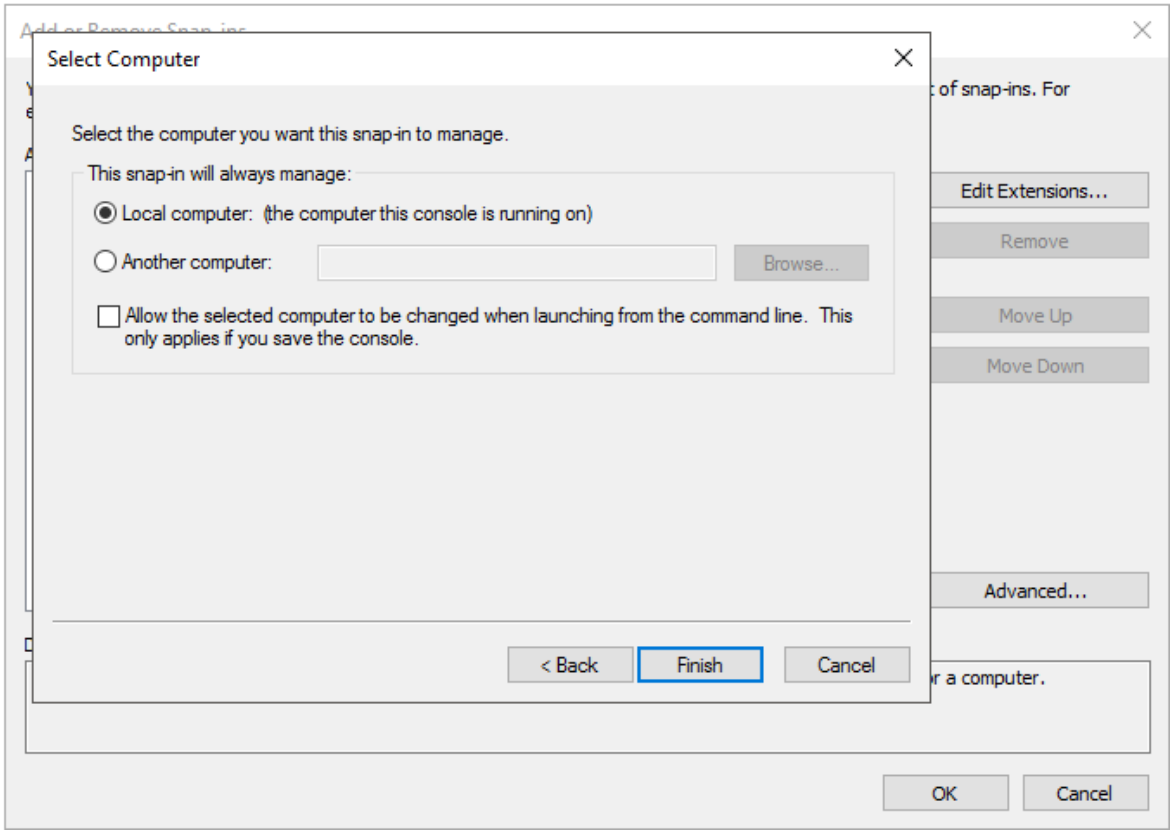
Es gibt zwei Möglichkeiten, den Fingerabdruck des Acronis Access-Zertifikats zu ermitteln. Eine Möglichkeit besteht über die Registerkarte 'Zertifikatsdetails' im Zertifikat-Snap-In. Die andere Möglichkeit besteht über eine bereits eingerichtete SSL-Bindung unter Verwendung der Eingabeaufforderung.

So können Sie den Fingerabdruck des Zertifikats über das Zertifikat-Snap-In abrufen

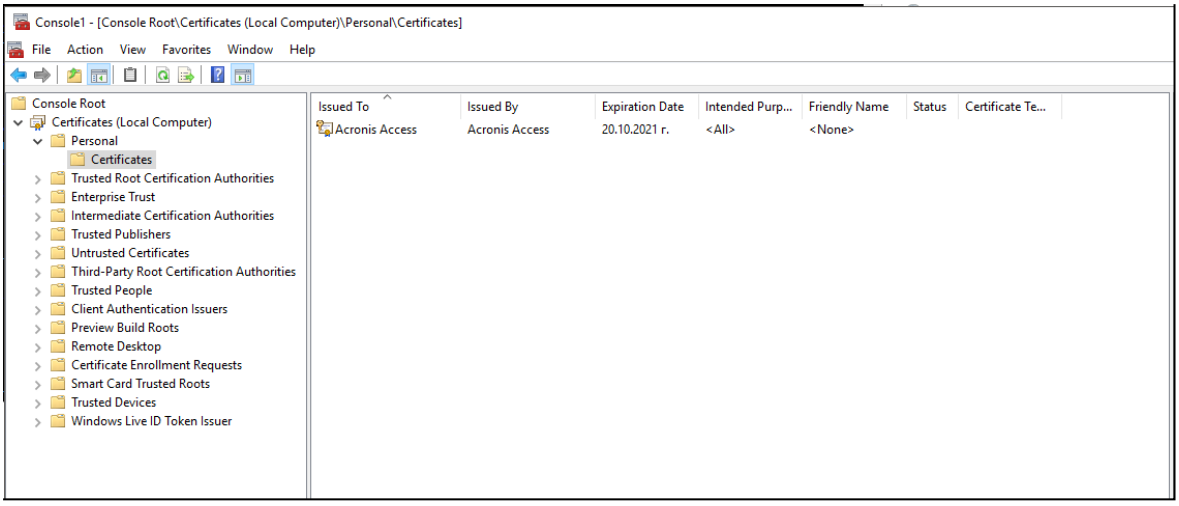
1. Öffnen Sie den Dialog **Ausführen** und geben Sie `mmc.exe` ein, um die **Microsoft Management Console** zu öffnen.
2. Klicken Sie auf **Datei -> Snap-In hinzufügen/entfernen...**
3. Wählen Sie **Zertifikate**.



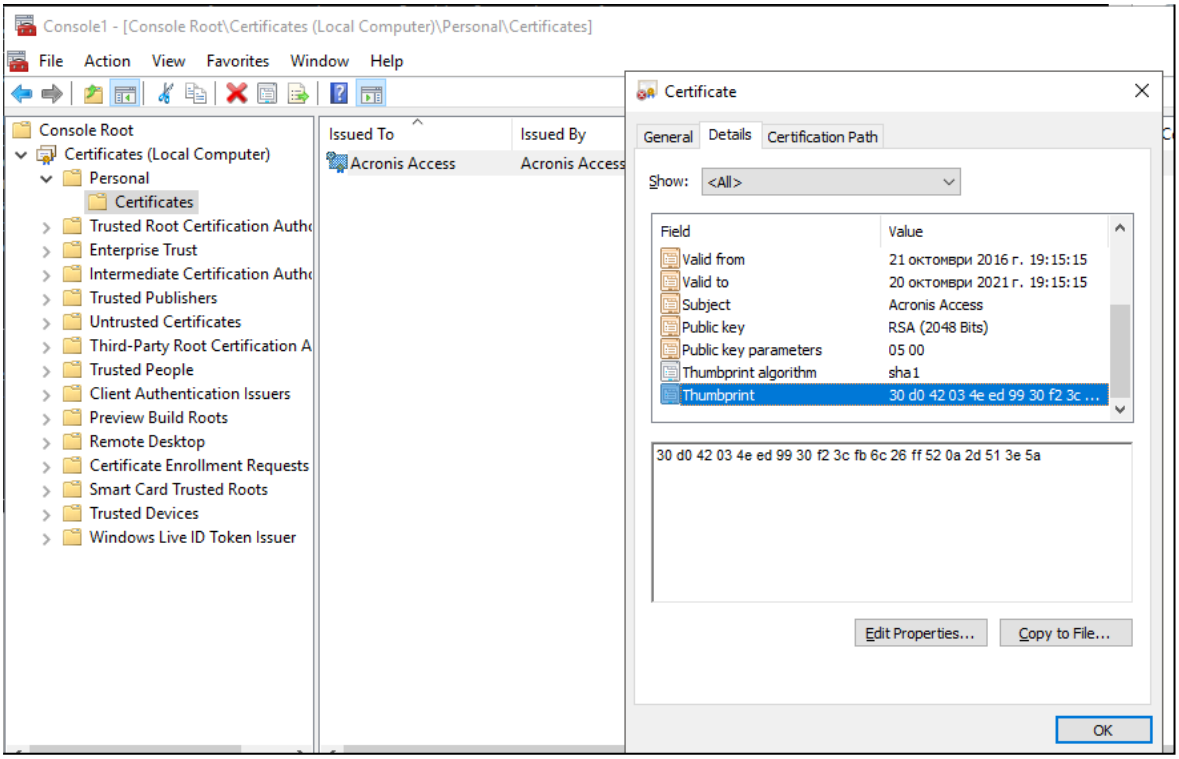
4. Klicken Sie im Dialog auf **Hinzufügen**.



5. Wählen Sie **Computerkonto**, klicken Sie auf 'Weiter', wählen Sie 'Lokaler Computer' und klicken Sie dann auf 'Fertig stellen':
6. Klicken Sie im Dialogfeld 'Snap-In hinzufügen/entfernen' auf **OK**.



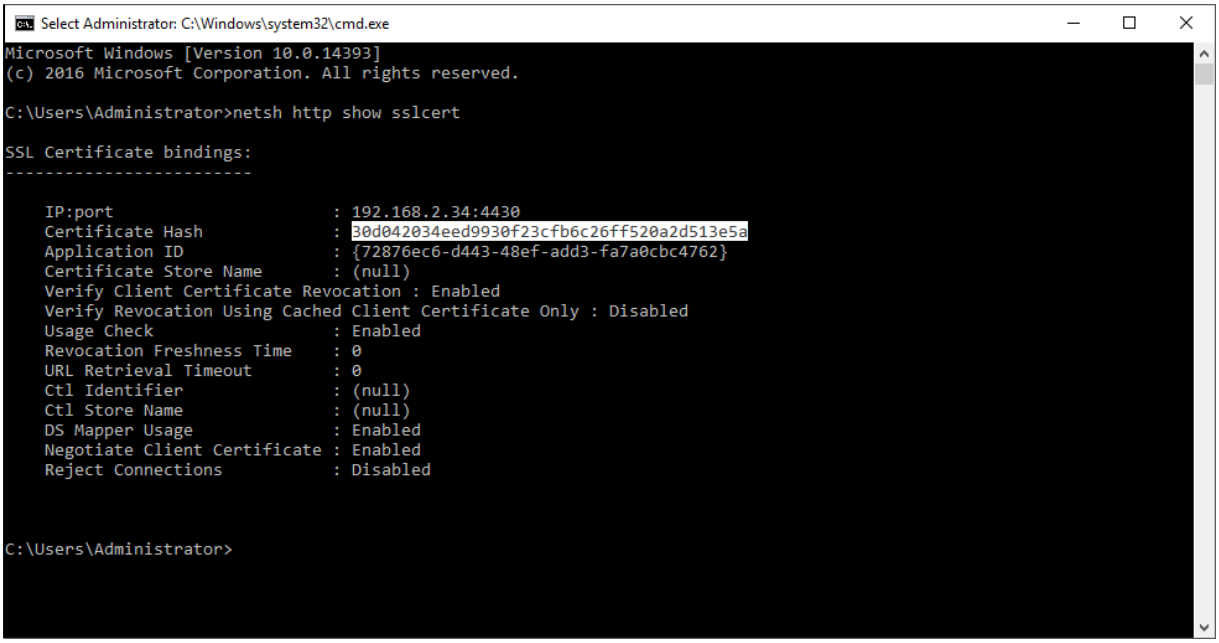
7. Erweitern Sie die Zertifikate auf der linken Seite (Persönlich -> Zertifikate). Hier sollten Sie das Acronis Access-Zertifikat sehen.



8. Doppelklicken Sie auf das Zertifikat, wählen Sie die Registerkarte **Details** und scrollen Sie zum Zertifikatfingerabdruck.
9. Kopieren Sie den Schlüssel und entfernen Sie die Leerzeichen. Sie benötigen den Schlüssel für den Befehl, der die SSL-Bindung erstellt.

So können Sie den Fingerabdruck des Zertifikats über eine bereits eingerichtete SSL-Bindung abrufen

1. Öffnen Sie eine Eingabeaufforderung.
2. Geben Sie Folgendes ein: `netsh http show sslcert`
3. Besteht bereits eine SSL-Bindung, wird sie angezeigt.



.

Hinweis
Die hervorgehobene Zeichenfolge ist der Zertifikat-Hash, den Sie benötigen.

IPv6-Einrichtung Schritt 2: Acronis Cyber Files Server

Aktivierung des Servers, um lokal auf allen IPv6-Adressen abzuhören.

Wichtig
Beachten Sie die Notiz bei Schritt 4, um eine Bindung für eine spezifische IPv6-Adresse durchzuführen.

1. Suchen Sie nach der Datei **`server.xml`**.

   Hinweis
   Standardmäßig befindet sich diese Datei im Ordner **`C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\apache-tomcat-9.0.88\conf`**
   Die Nummer im Pfad (7.0.70) kann je nach Ihrer Tomcat-Version variieren und der Pfad kann sich ändern, wenn Sie ein Upgrade durchgeführt oder eine benutzerdefinierte Installation vorgenommen haben. Sie können den Eintrag **Acronis Cyber Files Tomcat** in **Windows-Dienste** verwenden, um den Pfad zum Tomcat-Programm-Ordner zu ermitteln, der den Ordner **`conf`** enthält.

2. Erstellen Sie ein Backup von **`server.xml`**.

3. Öffnen Sie die Originaldatei **server.xml** in einem Texteditor.
4. Fügen Sie einen zusätzlichen Konnektor mit der Adresse =”::”, hinzu, um alle IPv6-Adressen zu unterstützen.
   i. Suchen Sie in **server.xml** den Teil der Datei, 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"
   bindOnInit="false" relaxedQueryChars="[,]" address="0.0.0.0" port="443"/>
   ```

   ii. Geben Sie dann in einer neuen Zeile neben dem bestehenden Konnektor diesen zusätzlichen Konnektor mit der Adresse =”::“ ein.

   ```
   <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" relaxedQueryChars="[,]" address="::" port="443"/>
   ```

   Hinweis
   Statt alle IPv6-Adressen hinzuzufügen (**::**), können Sie eine spezifische IPv6-Adresse festlegen, indem Sie “**::**” im Konnektorblock mit der gewünschten Adresse ersetzen.
   Beispiel:

   ```
   <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" relaxedQueryChars="[,]" address="fd59:ffdf:9580::3" port="443"/>
   ```

5. Speichern Sie die Änderungen und starten Sie den Acronis Cyber Files Tomcat Service über Windows Services erneut.

Wichtig
Alle Änderungen an **server.xml** erfordern einen Neustart des Acronis Cyber Files Tomcat Service.

Warnung!
Diese manuellen Änderungen werden bei einem manuellen Upgrade NICHT beibehalten. Stellen Sie sicher, dass Sie diese Dateien an einem Speicherort außerhalb der Acronis Cyber Files Server-Installation sichern. Nach einem Upgrade müssen Sie die Unterschiede zwischen den bearbeiteten und den neu installierten Dateien manuell zusammenführen und nötige Änderungen in die Datei **server.xml** migrieren.

IPv6-Einrichtung Schritt 3: Strict Transport Security (HSTS)

1. Ermitteln Sie den Speicherort der Datei**web.xml**.

   Hinweis
   Standardmäßig befindet sich **web.xml** hier: **C:\Program Files (x86)\Acronis\Acronis Cyber Files\Access Server\Web Application\WEB-INF**

2. Erstellen Sie ein Backup für die bestehende Datei **web.xml**.
3. Öffnen Sie die ursprüngliche**web.xml**-Datei in einem Text-Editor und fügen Sie folgende Zeile hinzu:

```
<filter>
      <filter-name>httpHeaderSecurity</filter-name>
      <filter-class>org.apache.catalina.filters.HttpHeaderSecurityFilter</filter-class>
     <init-param>
          <param-name>hstsMaxAgeSeconds</param-name>
          <param-value>31536000</param-value>
     </init-param>
     <init-param>
          <param-name>hstsIncludeSubDomains</param-name>
          <param-value>true</param-value>
     </init-param>
</filter>
<filter-mapping>
     <filter-name>httpHeaderSecurity</filter-name>
     <url-pattern>/*</url-pattern>
     <dispatcher>REQUEST</dispatcher>
     <dispatcher>FORWARD</dispatcher>
</filter-mapping>
```

4. Speichern Sie die Änderungen.
5. Starten Sie den Acronis Cyber Files Tomcat Service über Windows Services neu.

Hinweis
Durch die Verwendung von Entwicklungstools in einem Browser sollten Sie den Strict-Transport-Security-Header für alle Anforderungen sehen.

Warnung!
Diese manuellen Änderungen werden bei einem Upgrade NICHT beibehalten. Stellen Sie sicher, dass Sie diese Datei an einem Speicherort außerhalb der Acronis Cyber Files Server-Installation sichern. Nach einem Upgrade müssen Sie die manuell bearbeitete Datei mit der neu installierten Datei abgleichen und nötige Änderungen in die neue **`web.xml`**-Datei migrieren.

Mobile Device Management

Mit Mobile Device Management (MDM) werden die Verwendung und Sicherheit der Mobilgeräte eines Unternehmens sowie die auf diesen Geräten installierten Apps verwaltet.

Acronis hat die Cyber Files-Apps mit den folgenden MDM-Plattformen getestet:

- **Ivanti Neurons für MDM** (vormals MobileIron Cloud) für:
  - Cyber Files App für iOS.
  - Cyber Files-App für Android (ohne AppConnect-Verwaltung).
  - die Ivanti AppConnect-fähige Version von Cyber Files-App für Android.

  Hinweis
  Klicken Sie hier, um zur Dokumentation für Ivanti Neurons für MDM zu gelangen.

- **Ivanti Endpoint Manager Mobile** (vormals MobileIron Core) für:
  - Cyber Files App für iOS.
  - Cyber Files-App für Android (ohne AppConnect-Verwaltung).
  - die Ivanti AppConnect-fähige Version von Cyber Files-App für Android.

  Hinweis
  Klicken Sie hier, um zur Dokumentation für Ivanti Endpoint Manager Mobile (EPMM) zu gelangen.

- **Microsoft InTune** für:
  - Cyber Files App für iOS.

Verwaltete Konfiguration von Apps (AppConfig)

Acronis Cyber Files-Apps unterstützen die verwaltete Konfiguration von Apps (AppConfig).

Wenn die hier aufgeführten Voraussetzungen erfüllt sind, können Sie Ihrer Mobile Device Management (MDM)-Konfiguration bestimmte Schlüssel hinzufügen, die sich auf die Cyber Files-Apps auswirken.

Voraussetzungen

- Die Geräte müssen von einem MDM-Server verwaltet werden.
- Die Binärdatei der App muss vom MDM-Server auf dem Gerät installiert werden.
- Der MDM-Server muss die Einstellung **ApplicationConfiguration** und **ManagedApplicationFeedback**-Befehle unterstützen.

Unterstützte Schlüssel

Schlüsselname	Erforderlich?	Werte	Beschreibung	Anmerkungen
enrollmentServer	Obligatorisch	DN-Adresse	Sollte auf die DNS-Adresse des Cyber Files-Servers festgelegt werden, bei dem sich der Benutzer registriert.	
enrollmentPIN	Optional	PIN-Nummer	Wenn der Cyber Files-Server für die Client-Registrierung eine PIN-Nummer verlangt, können Sie mit diesem Wert das Feld für die **PIN-Nummer** auf dem Registrierungsformular automatisch ausfüllen lassen. Häufig ist die PIN-Anforderung für den Cyber Files-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. Die PIN-Anforderung wird auf der Seite **Einstellungen** der Cyber Files-Webkonsole konfiguriert.	
userName	Optional	Variable	Im Feld **Benutzername**	

			des Cyber Files-Registrierungsformulars bereitzustellen. Sie können eine Variable zum automatischen Vervollständigen dieses Werts mit dem Benutzernamen des betreffenden Benutzers verwenden. Sie können den Platzhalter `$USERID$` von Ivanti verwenden, der automatisch das Feld mit dem Benutzernamen vervollständigt, den der Benutzer beim Einrichten der Ivanti-App angegeben hat.	
enrollmentUserNameLock	Optional	Ja, Nein	Wenn **Ja** festgelegt wird, wird die Modifizierung des Felds **Benutzername** im Cyber Files-Registrierungsformular verhindert.	Felder sind nicht gesperrt, wenn: • der Sperrenschlüssel auf **Nein** festgelegt ist. • der Sperrenschlüssel überhaupt nicht konfiguriert ist. • der zu sperrende Feldwert leer ist.
enrollmentServerNameLock	Optional	Ja, Nein	Wenn **Ja** festgelegt wird, wird die Modifizierung des Felds **Server-Adresse** im Cyber Files-Registrierungsformular verhindert.	

plist-Dateien

plist-Dateien sind XML-Dateien für das Speichern von Anwendungsdaten. Sie können einen einfachen Text-Editor zur Erstellung und Bearbeitung verwenden.

Erstellen einer plist-Datei

1. Öffnen Sie einen Text-Editor Ihrer Wahl.
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 die gewünschten Schlüssel hier 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**.

Ivanti (vormals MobileIron)

Cyber Files-App für Android mit Ivanti

Ivanti AppConnect-fähig Cyber Files-App für Android

Wenn Sie Instanzen von Acronis Cyber Files-App für Android mit Ivanti AppConnect verwalten möchten, müssen Sie die Ivanti AppConnect-fähige Version verwenden.

Diese Version von Cyber Files-App für Android sollte innerhalb der Ivanti-Plattformen als 'interne' App behandelt werden.

Hinweis
Wenn Sie Unterstützung bei der Verwaltung der „In-House“-Apps benötigen, besuchen Sie die Dokumentationsseite für Ivanti-Apps.

Wichtig
Diese Version wird nicht über den Google Play Store vertrieben.
Die `.apk`-Datei für die Ivanti AppConnect-fähige Cyber Files-App für Android-Version ist auf der Download-Seite für Cyber Files erhältlich

Automatische Registrierung für Cyber Files-App für Android

Verfügbare Parameter für die automatische Registrierung für Ivanti:

- **`Servername`**
  Die URL des Servers.
- **`Benutzername`**
  Die Benutzer-ID.
- **`Client-Zertifikat`**
- **`Passwort`**
  Das Passwort des Benutzers.
- **`PIN`**
  Die PIN des Benutzers.
- **`Automatisches Übermitteln aktivieren`**
  Wenn dieser Parameter auf `Ja` festgelegt ist, müssen die Benutzer die Parameter nicht konfigurieren.

Android Enterprise

Android Enterprise ermöglicht die sichere und automatische Registrierung vonAcronis Cyber Files-App für Android-App-Benutzern.

Android Enterprise erfordert Endpoint Manager Mobile (EPMM)-Software.

Wichtig
Derzeit unterstützt Cyber Files die automatische Registrierung nur unter Verwendung von Ivanti EPMM.
Daher müssen Sie die AppConnect-fähige Version der Android-App installieren, um Android Enterprise nutzen zu können.
Wenn Sie mehr über Ivanti EPMM erfahren möchten, beziehen Sie sich auf die Ivanti-Dokumentation.

Cyber Files App für iOS mit Ivanti

Richtlinien für Cyber Files App für iOS-Container

Folgende Parameter stehen zur Verfügung:

- **Drucken erlauben** – Wählen Sie diese Option, wenn es Benutzern gestattet sein soll, Dokumente aus Acronis Cyber Files App für iOS zu drucken.
- **Kopieren/Einfügen in zulassen** – Wählen Sie diese Option, wenn es Benutzer gestatten sein soll, Text aus in Cyber Files App für iOS angezeigten Dokumenten in andere, nicht von AppConnect verwaltete Apps auf dem Gerät zu kopieren und einzufügen.

Warnung!
Wenn diese Option aktiviert ist, überschreibt sie die Cyber Files-`Einstellung für das Kopieren von Text aus geöffneten Dateien`.

- **Öffnen in erlauben** – Wählen Sie diese Option, wenn es Cyber Files App für iOS-Benutzern gestattet sein soll, Dateien in anderen Apps auf dem Gerät zu öffnen.

Aktivieren von Cyber Files App für iOS mit Ivanti

Dies ist nur erforderlich, wenn Sie die Acronis Cyber Files App für iOS-App nicht zu Ihrer App-Liste in der Avanti VSP-Konsole hinzugefügt haben und die Benutzer die App noch nicht verwenden.

Wenn die App über Ivanti hinzugefügt wurde, können Benutzer sie über den Avanti Store herunterladen. Je nach Ihren Einstellung wurde sie möglicherweise auch automatisch auf den Geräten installiert.

App installiert, nicht registriert bei Cyber Files-Server

Wenn Acronis Cyber Files App für iOS auf einem Gerät installiert und geöffnet wird, bevor Mobile@Work- und AppConnect VSP-Konfigurationen eingerichtet wurden, wird beim Starten der App möglicherweise nicht automatisch der AppConnect-Einrichtungsvorgang ausgelöst.

So starten Sie den Ivanti AppConnect-Einrichtungsvorgang für Cyber Files App für iOS manuell:

1. Öffnen Sie die App.
2. Öffnen Sie das Menü **Einstellungen**.
3. Tippen Sie auf die Option **Ivanti AppConnect** unten in der Liste.
4. Tippen Sie auf die Schaltfläche **Aktivieren**.

Hinweis
Wenn die erforderlichen Ivanti-Apps nicht auf dem Gerät installiert sind, wird eine Warnung anstelle der Schaltfläche **Aktivieren** angezeigt.

Der AppConnect-Einrichtungsvorgang kann einige Minuten dauern. Wenn dies der Fall ist, wird er gemäß der Beschreibung des vorherigen Szenarios fortgesetzt.

App installiert, registriert bei Cyber Files-Server

Dieses Szenario ähnelt dem vorherigen. Der einzige Unterschied besteht darin, dass die AppConnect Acronis Cyber Files-Konfiguration nicht zur automatischen Registrierung der App verwendet wird. Wenn die App bereits bei einem Cyber Files-Server registriert ist, wird die ursprüngliche Konfiguration beibehalten.

So verwalten Sie Cyber Files App für iOS mit AppConnect:

Hinweis
Dies ermöglicht zudem die Verwendung der Container-Richtlinien für den AppConnect-Passcode und die AppConnect-Berechtigungen.

1. Öffnen Sie Cyber Files App für iOS.
2. Wählen Sie **Einstellungen** -> **Partnerfunktionen** -> **MobileIron**.
3. Tippen Sie auf **AppConnect aktivieren**.
4. Warten Sie, bis der Prozess abgeschlossen ist.
5. Starten Sie die App neu.

Hinweis
Wenn sich ein Benutzer bei einem anderen Cyber Files-Server registrieren soll, muss dieser Benutzer Cyber Files App für iOS deinstallieren und neu installieren. Erst danach ist eine Konfiguration über AppConnect möglich.

App nicht installiert

In diesem Szenario müssen Sie Acronis Cyber Files App für iOS aus dem Apple App Store oder aus dem Ivanti Store installieren.

Wenn die App installiert ist, muss der Benutzer sie starten. Wenn eine konfigurierte Ivanti-App auf dem Gerät vorhanden ist, wird die Steuerung vorübergehend auf sie übertragen (dies wird als Check-in bezeichnet) und anschließend zurück an Cyber Files App für iOS übergeben.

Wenn eine gültige Cyber Files-AppConnect-Konfiguration gefunden wird, geht Cyber Files App für iOS automatisch in den Registrierungsmodus über und zeigt dem Benutzer das Registrierungsformular an.

Alle in der AppConnect-Konfiguration enthaltenen Felder werden automatisch ausgefüllt. Der Benutzer muss für gewöhnlich nur sein AD-Passwort in das Formular eingeben und dieses einsenden. Anschließend wird die entsprechende Cyber Files Client Management-Richtlinie auf die App angewendet und der Benutzer kann die App verwenden.

Warnung!
Wenn keine gültige Konfiguration für Cyber Files App für iOS auf der VSP existiert oder die Ivanti-App nicht konfiguriert wurde, erhält der Benutzer eine Fehlermeldung.
Wenn die Ivanti-App nicht auf dem Gerät installiert wurde, wird Cyber Files App für iOS im Standardmodus gestartet und AppConnect ist nicht aktiviert.

Ivanti Check-in

Wenn Acronis Cyber Files-Apps von Ivanti AppConnect verwaltet werden, erhalten die installierten Apps jegliche Änderungen der zutreffenden Richtlinien, sobald der nächste Check-in mit der Ivanti-App erfolgt.

Der Check-in führt dazu, dass die Cyber Files-Apps kurzzeitig zur Ivanti-App wechseln.

Daher stellen Benutzer möglicherweise eine kurze Unterbrechung fest, wenn sie zu dieser Zeit gerade aktiv sind.

Außerdem wird bei Check-ins auch der Widerruf von Zugriff auf Cyber Files-Apps angewendet. Deshalb sollten Sie die Häufigkeit der Check-ins für Ihr Unternehmen sorgfältig wählen.

Hinweis
Die Häufigkeit der Check-ins wird im Ivanti-Produkt festgelegt.

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 Acronis Cyber Files-iOS-Client ab Version 7.0.5 unterstützt.

Hinweis
Um eine **Geräterichtlinie** anzuwenden, muss Acronis Cyber Files 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 **Acronis Cyber Files** - **Standardzugriffsbeschränkungen** (**Mobile Access** > **Richtlinien** > **Standardzugriffsbeschränkungen**) oder für die Zugriffsbeschränkungen jedes Gateways aktiviert werden.

Hinweis
Um eine **Anwendungsrichtlinie** anzuwenden und damit Acronis Cyber Files von Intune verwaltet wird, muss die Option zum **Auslösen der Registrierung für Intune Mobile-Application Management** über den Acronis Cyber Files-Server in **Mobile Access** > **Richtlinien** > **Server-Richtlinie** aktiviert werden.

Active Directory-Gruppe

So erstellen Sie eine Active Directory-Gruppe:

1. Öffnen Sie das Microsoft Azure-Portal.
2. Wählen Sie **Alle Dienste**.
3. Geben Sie im Suchfeld **Azure** ein und wählen Sie **Azure Active Directory**.

4. Öffnen Sie **Gruppen**.
5. Wählen Sie **Neue Gruppe** und geben Sie die erforderlichen Informationen ein.
6. Wählen Sie die gewünschten Mitglieder der Gruppe.
7. Wählen Sie **Erstellen**.

Cyber Files App für iOS zu Intune hinzugefügt

Wenn Sie eine Intune-**Geräterichtlinie** verwenden möchten, sollte Cyber Files App für iOS über das Intune-Unternehmensportal installiert werden.

So fügen Sie Cyber Files App für iOS zu Intune hinzu:

1. Öffnen Sie das Microsoft Azure-Portal.
2. Klicken Sie auf **Alle Dienste**.
3. Geben Sie im Suchfeld **Intune** ein und wählen Sie **Microsoft Intune**.
4. Öffnen Sie **Mobile Apps im Intune-Portal.**
5. Öffnen Sie **Apps**.
6. Wählen Sie erst **Hinzufügen** und dann die Optionen für **App hinzufügen**:
   - Wählen Sie unter **App-Typ iOS** aus.
   - Klicken Sie auf **App Store durchsuchen** und suchen Sie nach **Acronis Cyber Files**. Wählen Sie die App aus.
   - Klicken Sie auf **App-Informationen** und nehmen Sie alle gewünschten Konfigurationsänderungen vor.
7. Aktivieren Sie die **Option zum Anzeigen der App als empfohlene App im Unternehmensportal**.
8. Klicken Sie auf **OK**.
9. Klicken Sie auf die App in der Liste, und wählen Sie **Zuweisungen** aus.
10. Wählen Sie die Benutzer oder Gruppen aus, denen Sie diese zuweisen möchten.

Geräterichtlinie

So fügen Sie eine Geräterichtlinie für Cyber Files App für iOS hinzu:

1. Öffnen Sie das Microsoft Azure-Portal.
2. Klicken Sie auf **Alle Dienste**.
3. Geben Sie im Suchfeld **Intune** ein und wählen Sie Microsoft Intune.
4. Öffnen Sie **Gerätekonfiguration** -> **Profile**.
5. Wählen Sie **Profil erstellen**.
6. 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.

7. Bei Cyber Files App für iOS 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**.
   - **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**.
8. Tippen Sie auf die App, nachdem Sie zur Liste hinzugefügt wurde, und wählen Sie **Zuordnungen**.
9. Wählen Sie die Benutzer/Gruppen für die Zuweisung.

Hinweis
Um eine **Geräterichtlinie** auf eine App anzuwenden, muss die App von Ihrem Intune Company Portal heruntergeladen werden.

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**.
3. Geben Sie im Suchfeld **Intune** ein und wählen Sie **Microsoft Intune**.
4. Öffnen Sie **Mobile Apps**.
5. Öffnen Sie **App-Schutzrichtlinien**.
6. Wählen Sie **Richtlinie hinzufügen**.
7. Geben Sie einen Namen für die Richtlinie ein.
8. Markieren Sie **Acronis Cyber Files** als erforderliche App.
9. Tippen Sie auf **Einstellungen**, und wählen Sie die Schutzrichtlinien aus, die angewendet werden sollen.
10. Tippen Sie auf die App, nachdem Sie zur Liste hinzugefügt wurde.
11. Wählen Sie **Zuordnungen**.
12. Wählen Sie die Benutzer/Gruppen für die Zuweisung.

Hinweis
Wenn die Option **Organisationsdaten an andere Apps senden/Daten von anderen Apps empfangen** auf **Per Richtlinie verwaltete Apps** festgelegt ist, müssen Sie separate **App-Konfigurationsrichtlinien** mit dem **IntuneMAMUPN**-Schlüssel auf die per Intune verwaltete App und die AcronisCyber Files-App anwenden, damit **Acronis Cyber Files Document Provider Extension** in anderen per Microsoft Intune verwalteten Apps verwendet werden kann.

Hinweis
Wenn ein Gerät mit dem IntuneMAMUPN-Schlüssel jedoch als MDM-verwaltet gilt, sind die Optionen **Organisationsdaten an andere Apps senden** und **Daten von anderen Apps empfangen** in der **App-Schutzrichtlinie** nicht mehr relevant, und die MDM-Einstellungen **Anzeigen von Unternehmensdokumenten in nicht verwalteten Apps** und **Anzeigen von Nicht-Unternehmensdokumenten in Unternehmens-Apps** im **Gerätekonfigurationsprofil** werden verwendet.

Um sicherzustellen, dass Unternehmensdokumente nur in per Intune verwalteten Apps geöffnet werden, müssen Sie im entsprechenden Profil zu **Eigenschaften > Einstellungen > App Store, Dokumentanzeige, Gaming** navigieren und für die Optionen **Anzeigen von Unternehmensdokumenten in nicht verwalteten Apps** und **Anzeigen von Nicht-Unternehmensdokumenten in Unternehmens-Apps** die Einstellung **Blockieren** festlegen.

Hinweis
Um die Document Provider Extension mit per Richtlinie verwalteten Apps verwenden zu können, muss die Option **Organisationsdaten an andere Apps senden** entweder auf **Per Richtlinie verwaltete Apps mit BS-Freigabe** oder auf **Alle Apps** festgelegt werden.

Hinweis
Um Dateien in Word (oder andere Microsoft-Apps) von AcronisCyber Files 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.

App-Konfigurationsrichtlinien

Um sich automatisch mit Intune-Anmeldeinformationen zu registrieren, müssen Sie eine **App-Konfigurationsrichtlinie** erstellen oder Ihre eigene Richtlinie hinzufügen:

So fügen Sie Ihre Konfigurationsrichtlinie hinzu:

1. Öffnen Sie das Microsoft Azure-Portal.
2. Klicken Sie auf **Alle Dienste** .
3. Geben Sie im Suchfeld **Intune** ein und wählen Sie **Microsoft Intune**.
4. Öffnen Sie **Mobile Apps**.
5. Öffnen Sie **App-Konfigurationsrichtlinien**.

6. Wählen Sie **Hinzufügen** und geben Sie einen Namen für die Richtlinie ein.
7. Wählen Sie **Verwaltete Geräte** als **Geräteregistrierungstyp**.
8. Wählen Sie **iOS** als **Plattform.**
9. Wählen Sie die erforderliche App, auf die Sie diese Konfiguration anwenden möchten.
10. 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.
11. Verwenden Sie für eine automatische Registrierung mit Cyber Files-Anmeldeinformationen die folgenden Schlüssel in **XML**:

    ```
    <dict>
    <key>enrollmentServerName</key>
    <string>192.168.1.10</string>
    <key>enrollmentUserName</key>
    <string>jprice</string>
    <key>enrollmentAutoSubmit</key>
    <string>Yes</string>
    </dict>
    ```

12. Wählen Sie die App, nachdem Sie zur Liste hinzugefügt wurde.
13. Wählen Sie **Zuordnungen**.
14. Wählen Sie die Benutzer/Gruppen für die Zuweisung.

Neuerungen

Weitere Informationen zum Umfang der aktuellen und früheren Versionen finden Sie in der Dokumentation zum Acronis Cyber Files-Versionsverlauf.

Bekannte Probleme

- Bei einigen Benutzern können Probleme bei der Synchronisierung von Dateien mit dem Desktop-Client auftreten. Die Abhilfe besteht darin, die Desktop-Client- Applikation erst vollständig zu deinstallieren , dann erneut zu installieren und anschließend die Verbindung zum Server wiederherzustellen.
- Wenn der Access Gateway Servers mit einer Einzel-Port-Konfiguration verwendet wird, kann es zu Problemen bei der Handhabung von Netzwerk-Knoten kommen, deren Pfad länger als 256 Zeichen ist. Informieren Sie sich im folgenden Artikel im Acronis Support-Portal darüber, wie Sie das Problem lösen können, indem Sie den Wert für `UrlSegmentMaxLength` erhöhen.
- Die Netzwerkknoten sind von der Web-Benutzeroberfläche aus nicht zugänglich, wenn eine Einmalanmeldung (SSO) verwendet wird. Wenn Sie versuchen, auf diese zuzugreifen, werden Sie abgemeldet.

Dokumentation für ältere Versionen

Informationen zu älteren Versionen der Acronis Cyber Files-Dokumentation finden Sie unter den folgenden Links:

Hinweis
Für ältere Dokumentationen ist Ihre bevorzugte Sprache möglicherweise nicht verfügbar.

- 8.9.x
- 8.8.x
- 8.7.x
- 8.6.x
- 8.9.x
- 8.8.x
- 8.5.x
- 8.1.x
- 8.0.x
- 7.5.x
- 7.4.x
- 7.3.x
- 7.2.x
- 7.1.x
- 7.0.x
- 6.0.x
- 5.0.x

Urheberrechtserklärung

GEWÄHRLEISTUNGEN, EINSCHLIESSLICH JEGLICHER STILLSCHWEIGEND MITINBEGRIFFENER GARANTIE ODER GEWÄHRLEISTUNG DER EIGNUNG FÜR DEN GEWÖHNLICHEN GEBRAUCH, DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK UND DER GEWÄHRLEISTUNG FÜR RECHTSMÄNGEL SIND AUSGESCHLOSSEN, AUSSER WENN EIN DERARTIGER GEWÄHRLEISTUNGSAUSSCHLUSS RECHTLICH ALS UNGÜLTIG ANGESEHEN WIRD.

Die Software bzw. Dienstleistung kann Code von Drittherstellern enthalten. Die Lizenzvereinbarungen für solche Drittanbieter sind in der Datei 'license.txt' aufgeführt, die sich im Stammordner des Installationsverzeichnisses befindet. Eine aktuelle Liste des verwendeten Drittanbieter-Codes sowie der dazugehörigen Lizenzvereinbarungen, die mit der Software bzw. Dienstleistung verwendet werden, finden Sie unter https://kb.acronis.com/content/7696.

Von Acronis patentierte Technologien

Die in diesem Produkt verwendeten Technologien werden durch einzelne oder mehrere U.S.-Patentnummern abgedeckt und geschützt: 7,047,380; 7,246,211; 7,275,139; 7,281,104; 7,318,135; 7,353,355; 7,366,859; 7,383,327; 7,475,282; 7,603,533; 7,636,824; 7,650,473; 7,721,138; 7,779,221; 7,831,789; 7,836,053; 7,886,120; 7,895,403; 7,934,064; 7,937,612; 7,941,510; 7,949,635; 7,953,948; 7,979,690; 8,005,797; 8,051,044; 8,069,320; 8,073,815; 8,074,035; 8,074,276; 8,145,607; 8,180,984; 8,225,133; 8,261,035; 8,296,264; 8,312,259; 8,347,137; 8,484,427; 8,645,748; 8,732,121; 8,850,060; 8,856,927; 8,996,830; 9,213,697; 9,400,886; 9,424,678; 9,436,558; 9,471,441; 9,501,234 sowie weitere, schwebende Patentanmeldungen.