Acronis

Acronis Files Advanced 8.5

ADMINISTRATION GUIDE

Revision: 4/11/2019

目次

1　はじめに

このガイドでは、Files Advanced とそのすべての機能について説明します。クライアントのマニュアルについては、「クライアントガイド 『165ページ 』」セクションを参照してください。

Files Advanced について

Files Advanced は、セキュリティ保護されたアクセス、同期、および共有のソリューションです。これらのソリューションにより、エンタープライズの IT 部門はビジネスコンテンツを完全に制御でき、セキュリティの確保、コンプライアンスの遵守、BYOD の導入を実現できます。Files Advanced により、従業員は、デスクトップ、ラップトップ、タブレット、スマートフォンなど、あらゆるデバイスを使用してコンテンツに安全にアクセスし、また、同僚、顧客、パートナー、ベンダなど社内外の承認された関係者とコンテンツを共有できます。

Files Advanced の機能は、主に「モバイル アクセス」と「同期・共有」の 2 つのカテゴリに分けることができます。

モバイル アクセスについて

Files Advanced のモバイル アクセス機能により、企業の IT 部門は、社内のファイル サーバー、SharePoint デバイス、および NAS デバイスへのシンプルでセキュアな管理されたアクセスをモバイル デバイス ユーザーに提供できるようになります。IT 部門では、リスクを伴うコンシューマベースのサービスやその他のコンプライアンス違反のサービスを従業員が利用しようとすることから生じる問題が解決します。IT 部門で Files Advanced を利用すれば、モバイル ユーザーによるコンテンツへのアクセスをセキュリティで保護し統制しながら、業務に必要なコンテンツ、ファイル、資料へのアクセスを提供できるようになります。

同期・共有について

Files Advanced の同期・共有機能は、エンド ユーザーによるシンプルさと効果へのニーズと企業の IT 部門が必要とするセキュリティ、管理の容易さ、柔軟性との間でバランスを維持する業界唯一のエンタープライズ ファイル共有および同期ソリューションです。

Files Advanced により、企業の IT 部門は、ファイルにアクセスできるユーザーを管理でき、ファイル共有アクティビティが組織のコンプライアンスとセキュリティの要件を満たしているかどうかを判断できるようになります。Files Advanced では、コンシューマベースのソリューションでは提供されないレベルの可視性と監視を実現できます。

2 クイック スタート

このガイドでは、Files Advanced のインストールおよび実行に関する最も簡単で迅速な方法を紹介します。設定をカスタマイズする場合、本ガイドは実用的ではありません。各コンポーネントの詳細および手順については、マニュアルの該当セクションを確認してください。

セクションの内容

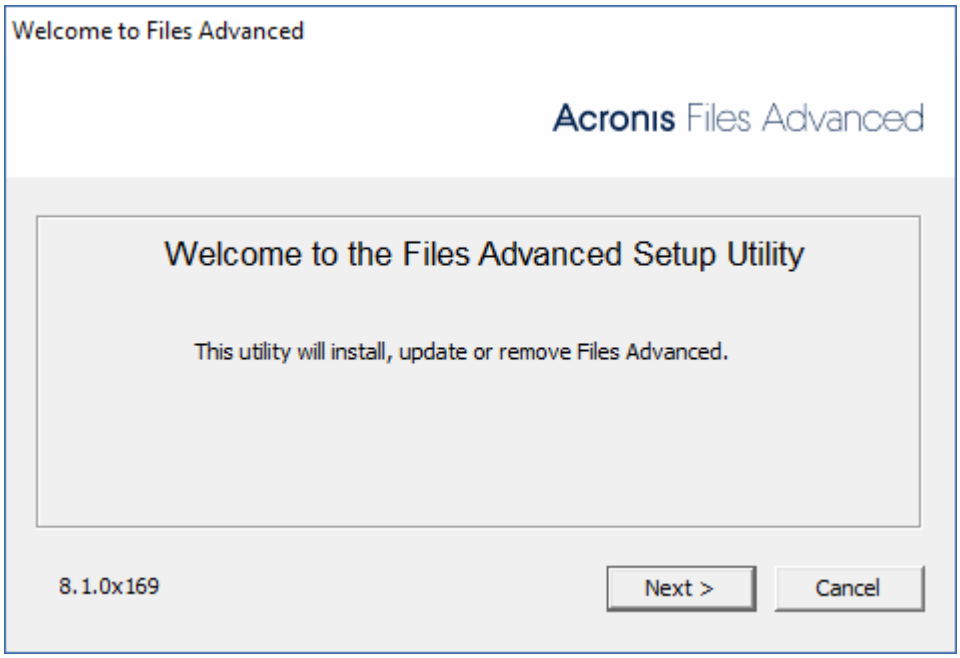
2.1 インストール

注意: 管理者としてログインしていることを確認してから Files Advanced をインストールしてください。

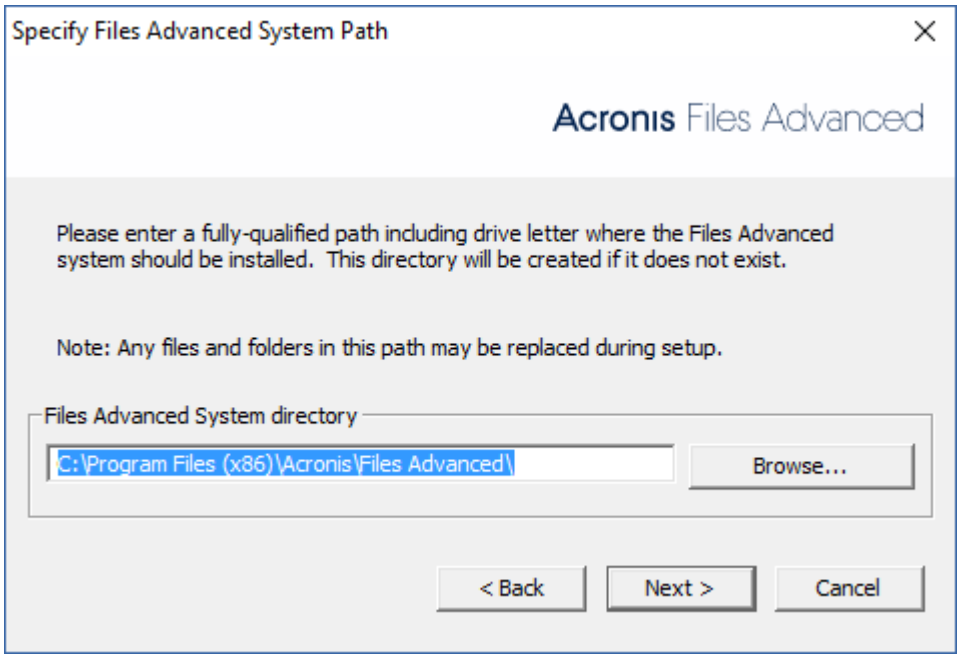
インストーラの使用

1. Files Advanced のインストーラをダウンロードします。
2. インストールされているウイルス対策ソフトウェアをすべて無効にしてください。無効にしない場合は、インストール手順が中断され、インストールが失敗する可能性があります。

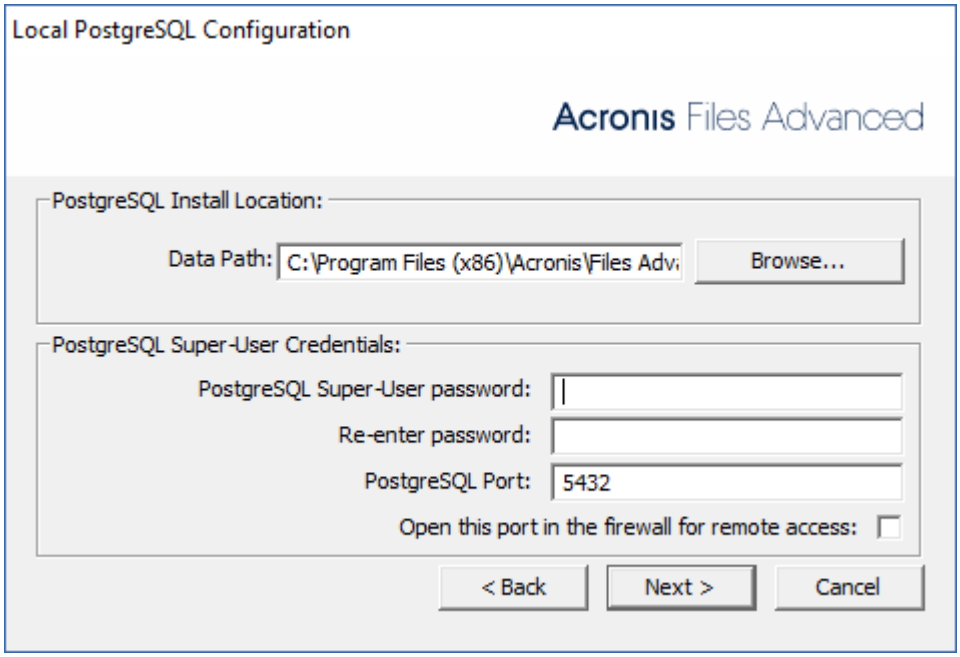
3. 実行可能なインストーラをダブルクリックします。



4. **[次へ]** を押して開始します。
5. 使用許諾契約を読み、承諾します。
6. **[インストール]** を押します。
7. Files Advanced のメイン フォルダのデフォルト パスを使用する場合は、**[OK]** を押します。



8. ユーザー Postgres のパスワードを設定し、書き留めておきます。このパスワードは、データベースのバックアップと復旧に必要となります。



9. インストールされるコンポーネントがすべてリストされたウィンドウが表示されます。続行するには、**[OK]** を押します。
10. Files Advanced のインストーラが完了したら、**[終了]** を押します。
11. 設定ユーティリティが自動的に起動し、インストールが完了します。

設定ユーティリティの使用

注意: 設定ユーティリティの設定内容は後で変更できます。

各タブでデフォルト値を使用し、[OK] を押して Files Advanced を起動します。

2.2 初期設定

設定ウィザードは、管理者に一連の手順を案内し、サーバーの基本的な機能が動作するようにします。

注意: 設定ユーティリティを実行した後に、サーバーが最初に起動するまで 30～45 秒かかります。

ネットワーク アダプタの IP アドレスおよび目的のポートを使用して、Files Advanced のウェブ インターフェイスに移動します。デフォルトの管理者アカウントにパスワードを設定するように求めるメッセージが表示されます。

注意: 認証機関からの証明書ではなく、デフォルトの証明書を使用して Files Advanced を実行すると、サーバーが信頼されていないことを示すエラーが表示されます。

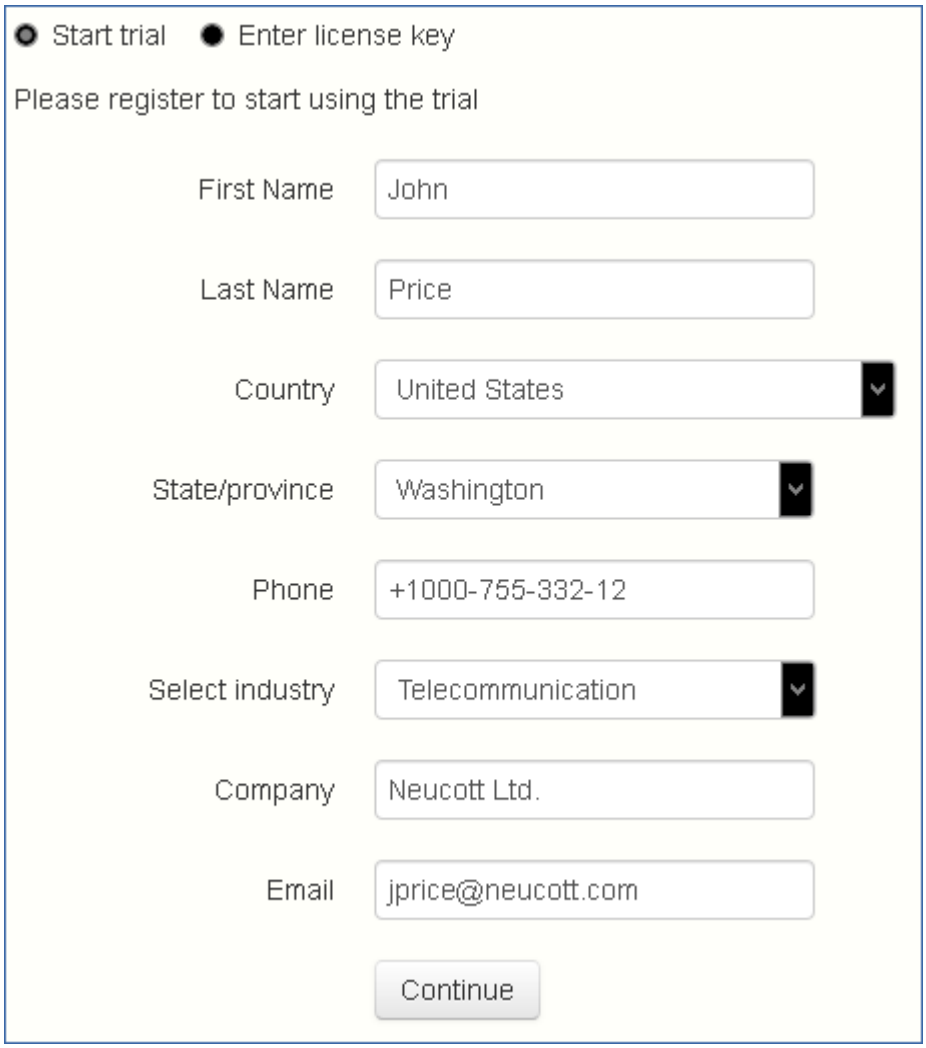
注意: [初期設定] ページに表示されるすべての設定は、設定の完了後にも確認することができます。設定の詳細については、「サーバー管理 『166ページ 』」の資料を参照してください。

注意: Internet Explorer 8 はサポートされていません。

ライセンス

試用版を開始するには:

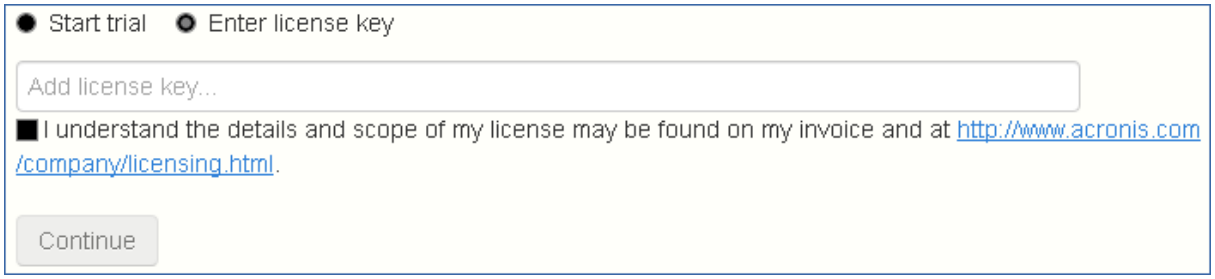
1. **[試用を開始]** を選択し、必要な情報を入力して **[送信]** を押します。



2.

Files Advanced インスタンスにライセンスを付与するには:

1. **[プロダクト キーを入力します]** を選択します。
2. プロダクトキーを入力し、チェックボックスを選択します。

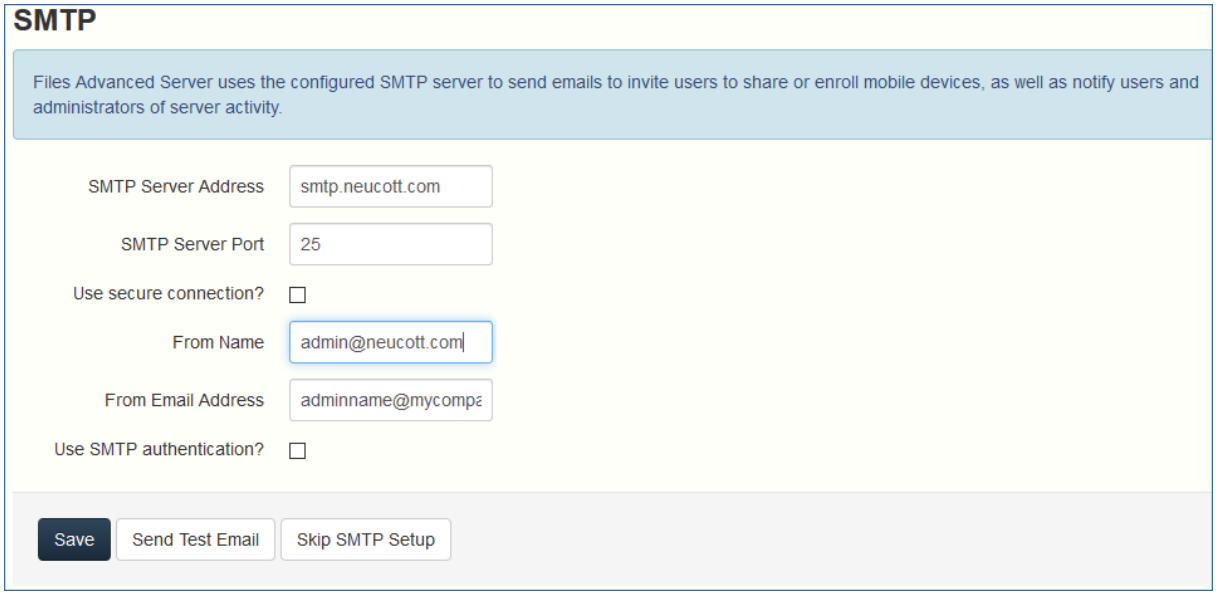


3. **[保存]** を押します。

全般設定

1. [サーバー名] にサーバー名を入力します。
2. ユーザーが (http:// または https:// で始まる)ウェブ サイトにアクセスできる FQDN または IP アドレスを指定します。
3. **[監査ログ]** のデフォルトの言語を選択します。現在のオプションは、**[英語]、[ドイツ語]、[フランス語]、[日本語]、[イタリア語]、[スペイン語]、[チェコ語]、[ロシア語]、[ポーランド語]、[韓国語]、[中国語（繁体字)]、[中国語（簡体字)]** です。
4. **[保存]** を押します。

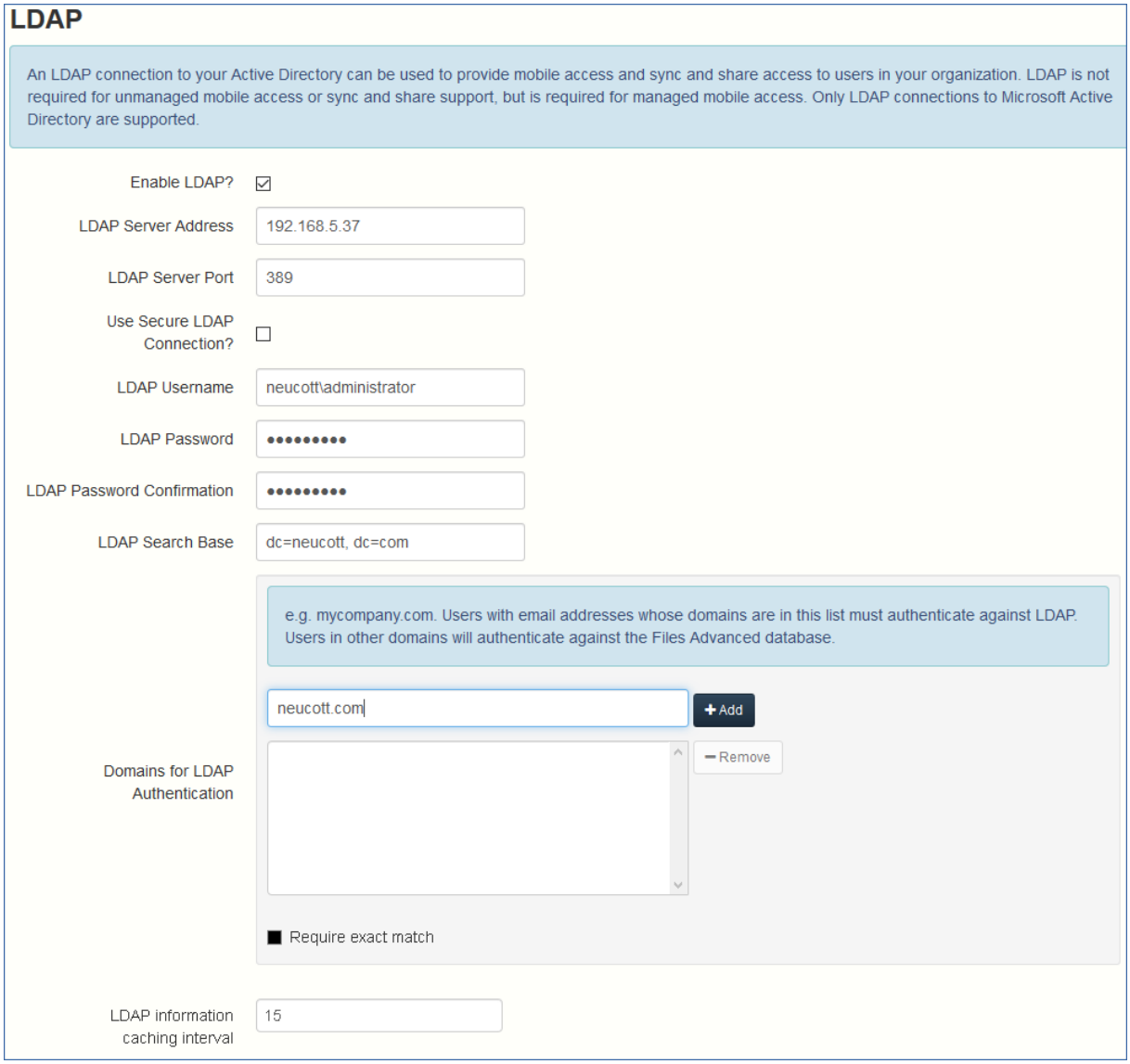
SMTP



注意: この手順をスキップして、後で SMTP を構成することもできます。

1. SMTP サーバーの FQDN または IP アドレスを入力します。
2. サーバーの SMTP ポートを入力します。
3. SMTP サーバーの証明書を使用しない場合は、**[セキュリティで保護された接続を使用しますか？]** のチェックを外します。
4. サーバーによって送信される電子メールの「差出人」行に表示されるユーザー名を入力します。
5. サーバーから送信される電子メールのアドレスを入力します。
6. SMTP サーバーでユーザー名やパスワードの認証を使用している場合は、**[認証を使用しますか？]** をチェックし、認証情報を入力してください。
7. **[テスト用の電子メールの送信]** を押して電子メールを手順 5 で指定したテスト用の電子メール アドレスに送信します。
8. **[保存]** を押します。

LDAP

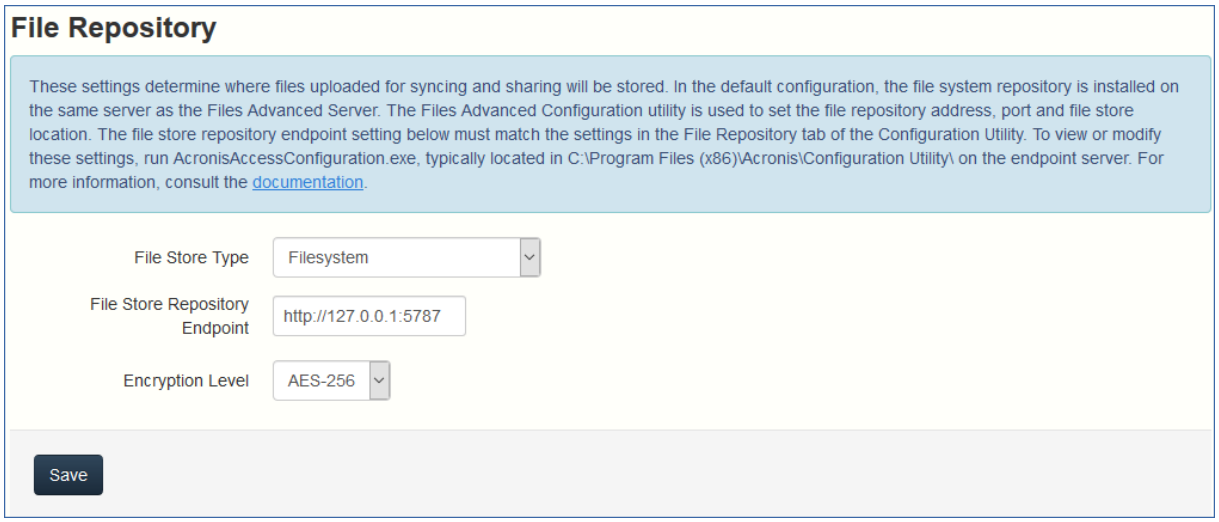


注意: この手順をスキップして、後で LDAP を構成することもできます。しかし、一部の Files Advanced 機能は構成するまで使用できません。

1. **[LDAP を有効にしますか？]** をチェックします。
2. LDAP サーバーの FQDN または IP アドレスを入力します。
3. LDAP サーバーのポートを入力します。
4. LDAP サーバーとの接続に証明書を使用する場合は、**[セキュリティで保護された LDAP 接続を使用しますか？]** をチェックします。
5. LDAP の資格情報をドメインも含めて入力します（例: acronis¥hristo)。
6. LDAP 検索ベースを入力します。

7. LDAP 認証のドメインを入力します （例えば、電子メール **joe@glilabs.com** のアカウントの LDAP 認証を有効にするには、**glilabs.com** と入力します)。
8. **[保存]** を押します。

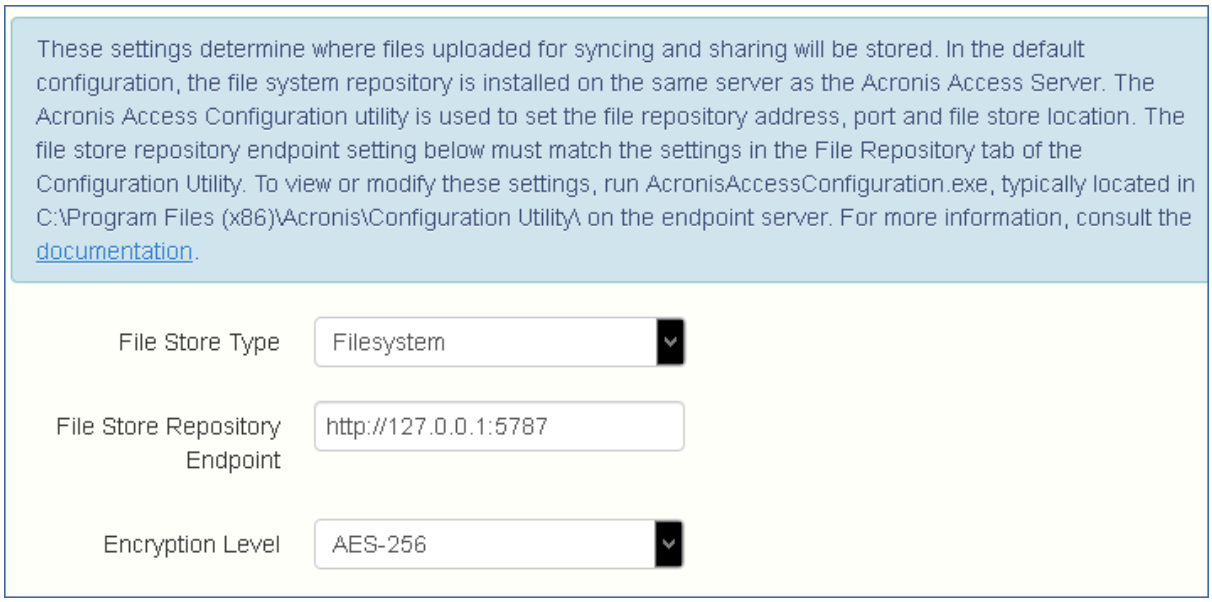
ローカル ゲートウェイ サーバー



注意: 同じコンピュータにゲートウェイ サーバーと Files Advanced サーバーの両方をインストールする場合、ゲートウェイ サーバーが自動的に検出され、Files Advanced サーバーに管理されます。クライアントがアクセス可能なローカル ゲートウェイ サーバーの FQDN または IP アドレスを設定するように指示するメッセージが表示されます。このアドレスは後から変更できます。

1. ローカル ゲートウェイ サーバーの FQDN または IP アドレスを設定します。
2. **[保存]** を押します。

ファイル リポジトリ



1. ファイル ストア タイプを選択します。お使いのコンピュータのファイルストアの場合は **[ファイルシステム]** を、クラウドのファイルストアの場合は **[Amazon S3]** を使います。
2. ファイル リポジトリ サービスの FQDN または IP アドレスを入力します。

   注意: ファイルリポジトリのアドレス、ポート、およびファイルストアのロケーションを設定するには、Files Advanced 設定ユーティリティを使用します。ファイルストアリポジトリエンドポイントの設定は、設定ユーティリティの [ファイル リポジトリ] タブの設定と一致していなければなりません。設定値を表示または変更するには、AcronisAccessConfiguration.exe を実行します。通常、このファイルはエンドポイントサーバーの **C:\Program Files (x86)\Acronis\Files Advanced\Common\Configuration Utility** にあります。
3. 暗号化レベルを選択します。**[なし]**、**[AES-128]**、**[AES-256]** から選択してください。
4. サーバーがユーザーに警告を送信する最小限の空き領域を選択してください。
5. **[保存]** を押します。

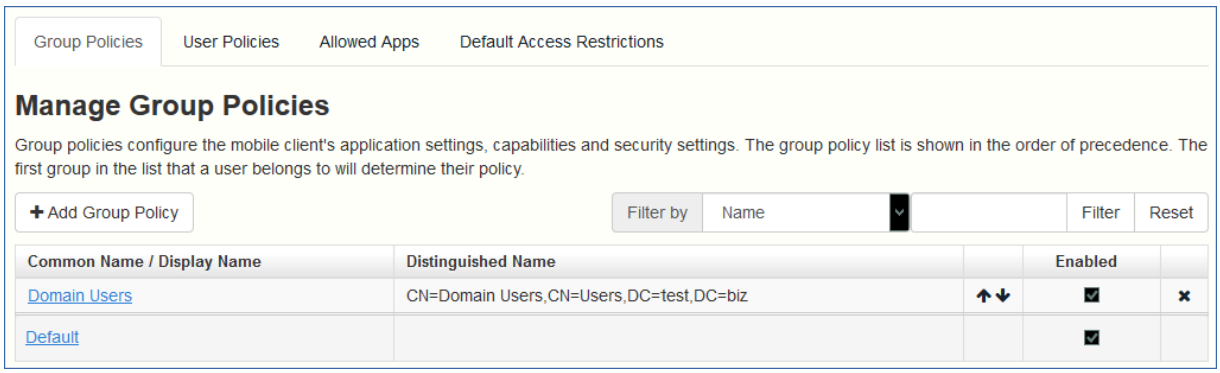
3 モバイル アクセス

セクションの内容

Files Advanced Web サーバーの管理に登録されているすべてのモバイル クライアントでは、ユーザー ポリシーまたはグループ ポリシーによって機能が管理および制御されます。デフォルトのポリシーは、インストール時に自動的に作成され、最も低い優先度が適用されます（最も高い優先度は個人的なユーザー ポリシーになります)。ユーザー ポリシーが適用されておらず、グループ ポリシーのメンバーにも登録されていないすべてのユーザーにデフォルト ポリシーが適用されます。デフォルト ポリシーはデフォルトで有効になっています。

デフォルト ポリシーの設定

1. Files Advanced ウェブ コンソールを開きます。
2. **[モバイル アクセス]** → **[ポリシー]** → **[グループ ポリシー]** に移動します。



3. **[有効]** フィールドのチェックボックスがオンになっていることを確認し、**[デフォルト]** ポリシーをクリックします。
4. 設定を表示し、必要に応じて変更します。設定の各項目に関する詳細については、「ポリシー 『70ページ 』」セクションを参照してください。

Files Advanced アプリを初めて実行するときに、デモモードでアプリを試用するか、会社のサーバーに接続するかを選択できます。

デモモードでアプリを試用する

デモモードでは、お勤めの会社に Files Advanced Web サーバーが用意されていない場合でも、Files Advanced アプリを試用することができます。デモモードの環境設定は試用を目的としているため、一部の機能は利用できません。

1. アプリをインストールし、起動します。
2. ようこそ画面の後に **[デモサーバーに接続する]** を選択します。
3. デモサーバーに接続されます。

   注意: デモサーバーに接続されると、デモサーバー上の一部の共有フォルダおよび同期フォルダへの読み取り専用アクセス権が付与されます。これらのフォルダには、PDF や画像ファイルなどのサンプルファイルが含まれています。これらのファイルの参照、検索、表示、編集を実行したり、必要に応じて編集済みファイルをアプリ内（ローカル)に保存したりできます。

4. いつでも会社のサーバーに切り替えることができます。

会社のサーバーに登録するには

1. アプリをインストールし、起動します。
2. ようこそ画面の後に **[会社のサーバーに接続する]** を選択します。
3. サーバーのアドレス、PIN コード（必要な場合)、ユーザー名、パスワードを入力します。
4. フォーム全体に入力した後で、**[登録]** ボタンをタップします。
5. 社内のサーバーの設定によっては、管理サーバーのセキュリティ証明書が信頼されていないことを示す警告が表示されることがあります。この警告を受け入れて続行するには、**[常に続行]** をクリックします。
6. Files Advanced モバイルアプリにアプリケーションロックパスワードが必要な場合は、パスワードを設定するように要求されます。パスワードの複雑性の要件が適用されている場合があり、必要な場合はそれが表示されます。
7. 管理ポリシーで Files Advanced でのファイルの保存が制限されているか、Files Advanced モバイルアプリ内で個別のサーバーを追加する機能が無効にされている場合、確認ウィンドウが表示されることがあります。Files Advanced モバイルアプリで

ローカルに保存したファイルがある場合は、**[マイファイル]** ローカルファイルストレージ内のファイルが削除されることを確認するよう求めるメッセージが表示されます。[いいえ] を選択すると、管理登録処理がキャンセルされ、ファイルは変更されずに残ります。

Files Advanced クライアントの使用については、下のリストにあるアプリ専用のクライアントガイドマニュアルを参照してください。

- デスクトップおよびウェブクライアント
- iOS アプリ
- Android アプリ
- Windows モバイルアプリ

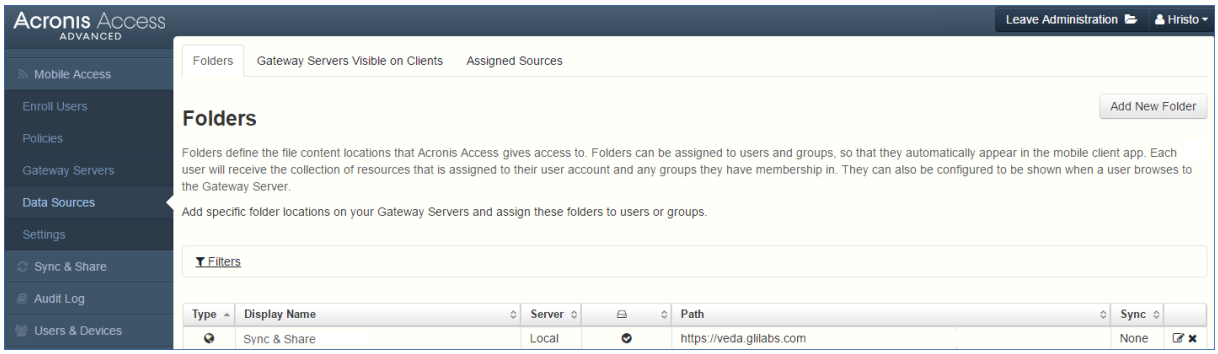
3.1 同期・共有

セクションの内容

3.1.1 Sync&Share データソース

Files Advanced をインストールして設定すると、自動的に「**Sync&Share**」という名前のデータソースが作成され、割り当てられたユーザーとグループのリストにデフォルトで **Domain Users** グループが追加されます。管理者は、このデータソースフォルダをいつでも変更または削除できます。

このデフォルトのデータソースは、**Domain Users** グループの一部として新しく作成するすべてのユーザーが使用することができ、モバイル、デスクトップ、およびウェブクライアント経由で利用できます。



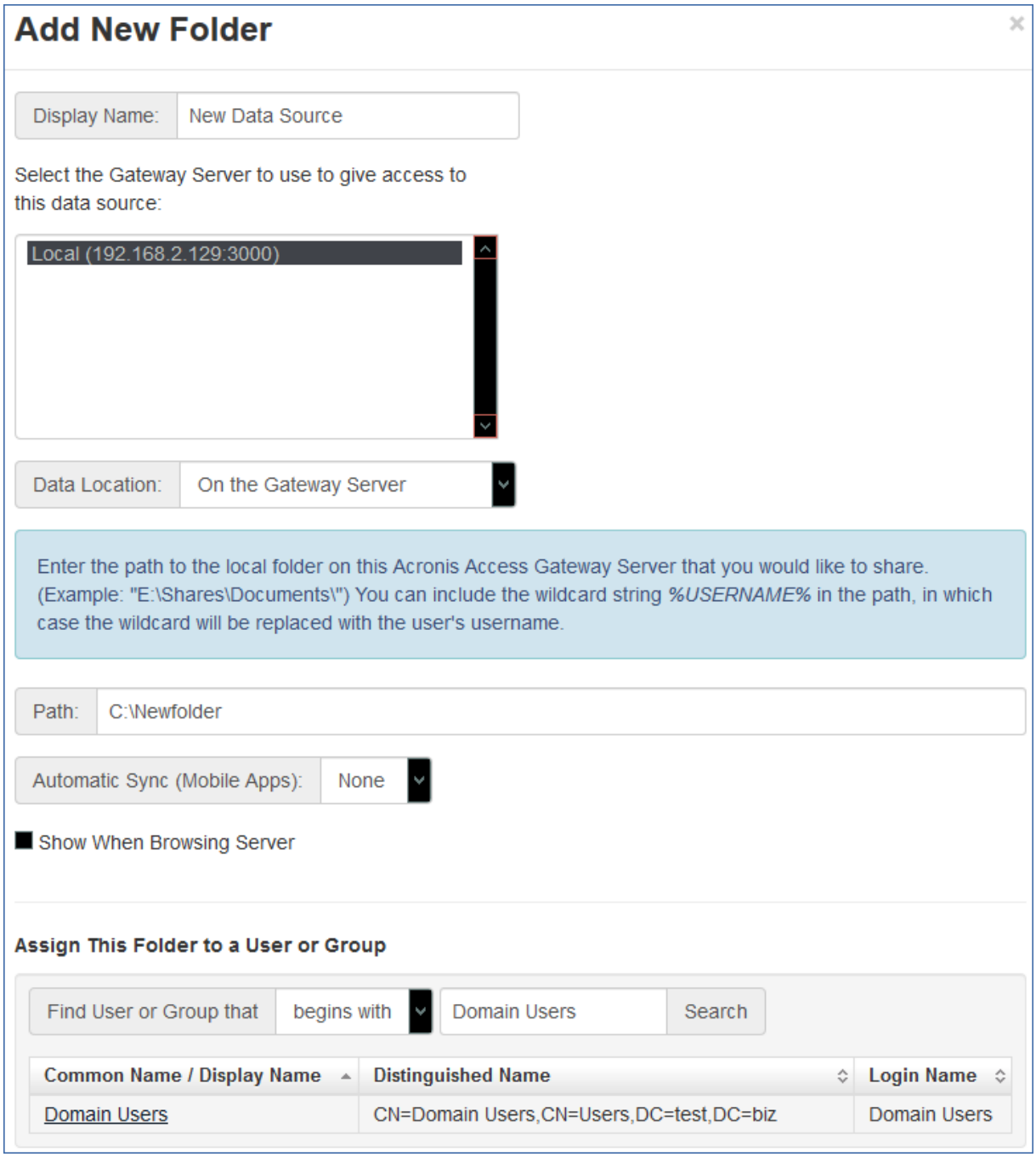
セクションの内容

既存のコンテンツを共有するには、そのコンテンツのデータソースを設定して、対象とするユーザーやグループにそのデータソースを割り当てることだけが必要です。

データ ソースの作成

1. Files Advanced ウェブ インターフェイスを開きます。
2. **[モバイル アクセス]** タブを選択します。
3. **[データ ソース]** タブを開きます。
4. **[フォルダ]** に移動します。

5. **[新しいフォルダの追加]** ボタンを押します。



6. フォルダの表示名を入力します。
7. フォルダへのアクセスを提供するゲートウェイ サーバーを選択します。
8. データのロケーションを選択します。ロケーションとして、実際のゲートウェイ サーバー、他の SMB サーバー、SharePoint サイトまたはライブラリ、同期と共有サーバー上を選択できます。

注意: 同期と共有を選択するときは、必ずサーバーのフル パスをポート番号と共に入力してください（例: https://mycompany.com:3000)。

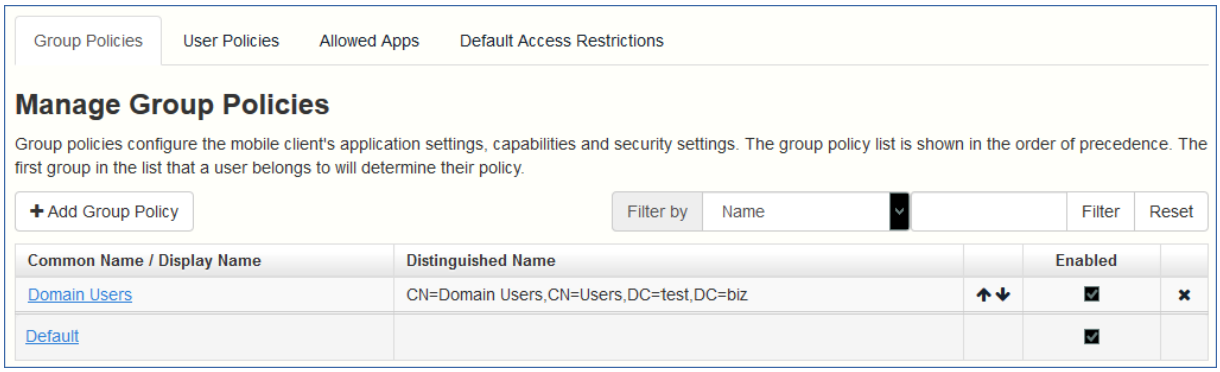
9. ロケーションの選択に基づき、フォルダ、サーバー、サイトまたはライブラリへのパスを入力します。
10. フォルダの**同期**タイプを選択します。
11. Files Advanced モバイル クライアントがゲートウェイ サーバーを参照した場合に、このデータ ソースが表示されるようにするには **[サーバーの参照時に表示する]** を有効にします。

注意: SharePointのデータソースを作成するときに、SharePointフォローサイトの表示を有効化するオプションがあります。

12. [保存] ボタンをクリックします。

デフォルトでは、ユーザーは NAS、File Servers、および SharePoint のリソースをウェブクライアントから開くことができません。しかし、それを可能にすることは容易であり、そうすることでウェブユーザーが行えることの可能性は広がります。

1. ウェブインターフェイスを開き、**[モバイルアクセス]** -> **[ポリシー]** に移動します。（モバイルアプリには主にポリシーが関連付けられていますが、ウェブアクセスの設定も関係することに注意してください。）
2. 変更するポリシーを選択します。新しいポリシーを何も作成していない場合は、**デフォルト**ポリシーを選択してください。



3. **[サーバーポリシー]** タブで、**[ウェブクライアントからファイルサーバー、NAS、および SharePoint へのアクセスを許可する]** ボックスをオンにします。

4. デスクトップ同期を有効にするかどうかも検討し、選択したポリシーについて、サブオプション **[ファイル サーバー、NAS および SharePoint のフォルダからデスクトップ クライアントへの同期を許可する]** および **[ファイル サーバー、NAS および SharePoint のフォルダとデスクトップ クライアントの双方向同期を許可する]** を使用して設定してください。
5. **[保存]** をクリックします。

ポリシーごとの設定として実装されているので、より柔軟な設定が可能です。別のグループの設定やいくつかの個々のポリシーの設定を有効にすることもできます。

3.1.2 LDAP プロビジョニング

LDAP プロビジョニングを有効にすることで、管理者によるユーザーごと（またはグループごと)への招待が不要になり、ユーザーは LDAP の資格情報でログインすることができ、アカウントも自動的に作成されるようになります。これらのアカウントはライセンス プールのライセンスから抽出されるため、特定の LDAP グループ（複数のグループも可)をプロビジョニング用に選択してください。

LDAP プロビジョニングを有効にする

1. Files Advanced ウェブ コンソールを開きます。
2. **[同期・共有]** → **[LDAP プロビジョニング]** に移動します。

3. 1 つまたは複数の LDAP グループ名を入力します。
4. 目的のグループを選択し、**[保存]** を押します。

選択されたグループのユーザーは、LDAP の資格情報で Files Advanced へのログインを試行すると、Files Advanced アカウントが自動的に生成されます。

3.2 ウェブクライアントとデスクトップクライアント

- ウェブクライアントでは、Files Advanced の有効な資格情報を持つすべてのユーザーが、任意のブラウザからファイルやフォルダにアクセスしたり共有したりすることができます。
- デスクトップクライアントでは、サイズの大きなファイルを簡単に共有したり、ファイルを常に最新の状態に維持したりすることができます。

Files Advanced クライアントの使用については、下のリストにあるアプリ専用のクライアントガイドマニュアルを参照してください。

- デスクトップおよびウェブクライアント
- iOS アプリ

- Android アプリ
- Windows モバイルアプリ

4 インストール

セクションの内容

4.1 要件

Files Advanced をインストールする前に、管理者としてログインする必要があります。サーバーが次の要件を満たしていることを確認します。

セクションの内容

4.1.1 オペレーティング システムの要件

注: Files Advanced 7.2.3 は 32 ビットオペレーティングシステムをサポートする最後のバージョンです。Files Advanced の新しいバージョンは、64 ビットオペレーティングシステムのみをサポートします。

注: Files Advanced 7.4.x は、Windows XP および Vista をサポートする最後のバージョンです。これより新しいバージョンの Files Advanced は、これらのオペレーティングシステムからの接続をサポートしていません。

推奨:

- Windows Server 2016 Standard Edition および Datacenter Edition
- Windows Server 2012 R2 Standard Edition および Datacenter Edition
- Windows Server 2008 R2 Standard Edition、Enterprise Edition および Datacenter Edition（Service Pack 1）

サポート対象:

- Windows Server 2016 Standard
- Windows Server 2012 R2 Standard Edition および Datacenter Edition
- Windows Server 2012 Standard Edition および Datacenter Edition
- Windows Server 2008 R2 Standard Edition、Enterprise Edition および Datacenter Edition（Service Pack 1）
- Windows Server 2008 Standard Edition、Enterprise Edition および Datacenter Edition（32 ビット版および 64 ビット版/Service Pack 2）

注意: テスト用にシステムをインストールして、Windows 7 以降で実行することができます。これらのデスクトップ クラスの構成は、本番環境ではサポートされません。

4.1.2 モバイルクライアントの要件

サポートされるデバイス:

- Apple iPad 第 4 世代以降。
- Apple iPad mini 第 2 世代以降。
- Apple iPad Pro 第 1 世代以降。
- Apple iPhone 5 以降。
- Apple iPod Touch 第 6 世代以降。
- Android スマートフォンおよびタブレット（x86 プロセッサアーキテクチャのデバイスはサポートされていません）。
- Windows のスマートフォンおよびタブレット（Windows RT はサポートされていません）。

注意: Windows デバイスが Files Advanced サーバーのバージョン 6.0 以降で利用できるようになりました。

サポートされる OS:

- iOS 10 以降
- Android 4.1 以降（x86 プロセッサアーキテクチャのデバイスはサポートされていません)。
- Windows 8.1 以降（Windows RT はサポートされていません)。

注意: Windows デバイスが Files Advanced サーバーのバージョン 6.0 以降で利用できるようになりました。

Files Advanced アプリケーションは次のウェブサイトからダウンロードできます。

- iOS の場合 http://www.grouplogic.com/web/meappstore。
- Android の場合 https://play.google.com/store/apps/details?id=com.grouplogic.mobilecho。
- Windows の PC およびタブレットまたはスマートフォンの場合。

4.1.3 推奨される最小ハードウェア構成

デプロイサンプル

これらのデプロイ構成図は、すべての Files Advanced コンポーネントが同一の仮想コンピュータまたは物理サーバー上で実行されることを前提としています。

注意: 推奨ディスク領域は、削除済みリビジョンの古いファイルがファイルリポジトリで消去されることを前提にしたものです。

注意: 推奨ディスクサイズは最小構成によるものです。ユーザーが同期しているファイルのサイズおよび数によっては、ディスクサイズを増やす必要があります。

注意: Files Advanced Web サーバーは仮想コンピュータにインストールできます。

注意: Files Advanced インストーラを実行するための十分な領域があることを確認してください。インストーラを実行するには、1 GB の空き領域が必要です。

注意: これらは本番環境で推奨される値です。試用版のご利用、あるいはテスト目的での Files Advanced のインストールをお考えの場合には、テスト負荷に合わせてハードウェア構成のランクを下げることができます。

小規模デプロイ

- 最大 25 ユーザー
- CPU: Intel i7 Xeon（4 コア)クラス、あるいは同等の AMD 製 CPU。
- RAM: 16GB
- ディスク領域: 100GB

中規模デプロイ

- 最大 500 ユーザー
- CPU: Intel i7 Xeon（8 コア)クラス、あるいは同等の AMD 製 CPU。
- RAM: 40 GB
- ディスク領域: 2TB RAID

大規模デプロイ

- 最大 2,500 ユーザー
- CPU: Intel i7 Xeon（16 コア)クラス、あるいは同等の AMD 製 CPU。
- RAM: 64 GB
- ディスク領域: 10TB RAID

注意: 2,500 ユーザーを超えるデプロイでは、クラスタ化されたサーバー構成を推奨します。2,500 ユーザーを超えるデプロイについては、Acronis サポートにお問い合わせください。

4.1.4 ネットワーク要件

- 1 つの静的 IP アドレス。一部の構成では、2 つの IP アドレスが必要になることがあります。
- 任意（推奨): 上記の IP アドレスに対応する FQDN。
- Active Directory（LDAP)の使用をご検討の場合のドメインコントローラへのネットワークアクセス。
- 電子メール通知および招待メッセージ用の SMTP サーバーへのネットワークアクセス。
- アドレス **127.0.0.1** はモバイルアプリの内部で使用するため、VPN、MobileIron、BlackBerryDynamics などのトンネルを経由して転送しないでください。
- Files Advanced Web サーバーまたはゲートウェイサーバーが実行されているコンピュータはすべて、Windows Active Directory にバインドされていなければなりません。

HTTPS トラフィックを処理する 2 つのコンポーネントとして、ゲートウェイ サーバーと Files Advanced Web サーバーがあります。ゲートウェイ サーバーは、モバイル クライアントからファイルとデータ ソースの共有の両方にアクセスするのに使われます。Files Advanced Web サーバーは、「同期・共有」クライアントのウェブユーザーインターフェイスを提供すると同時に、「モバイルアクセス」と「同期と共有」の両方の管理コンソールにもなります。

多くの場合、デプロイでは両方のサーバーで 1 つの IP アドレスを使用することが推奨されますが、ポートと DNS エントリは別個のものを使用してください。多くのインストールでは、このように、IP アドレス設定は 1 つで十分です。 特定のデプロイまたはセットアップで必要な場合には、コンポーネントごとに別個の IP アドレスを使用してサーバーを設定することがあります。

モバイル デバイスがファイアウォールの外部からアクセスできるようにする場合は、次のようないくつかのオプションがあります。

- **ポート 443 アクセス**: Files Advanced は暗号化された転送に HTTPS を使用するため、ポート 443 で HTTPS トラフィックを許可する一般的なファイアウォール ルールに自然に適合します。ポート 443 から Files Advanced Web サーバーへのアクセスを

許可すると、権限のある iPad クライアントをファイアウォールの内外で接続できます。アプリは、優先する他のポートを使用するように設定することもできます。

- **VPN**: Files Advanced モバイルアプリは VPN 接続を介したアクセスをサポートします。組み込みの iOS VPN クライアントとサードパーティの VPN クライアントの両方がサポートされています。Mobile Device Management（MDM)システムまたは Apple iPhone 構成ユーティリティを使用して iOS 管理プロファイルをオプションでデバイスに適用し、証明書ベースの iOS「VPN オンデマンド」機能を構成し、Files Advanced Web サーバーや会社の他のリソースへのシームレスなアクセスを実現できます。
- **リバース プロキシ サーバー:** リバース プロキシ サーバーが設定されている場合は、開かれたファイアウォール ポートまたは VPN 接続がなくても iPad クライアントを接続できます。Files Advanced モバイルアプリは、リバースプロキシのパススルー認証、ユーザー名/パスワード認証、Kerberos 制約付き認証委任、および証明書認証をサポートします。Files Advanced モバイルアプリへの証明書追加の詳細については、「クライアント証明書の使用」の記事を参照してください。
- **BlackBerry Dynamics 対応アプリ:** Files Advanced モバイルアプリを BlackBerry Dynamics プラットフォームに登録して管理する機能が用意されています。この構成では、Files Advanced モバイルアプリとゲートウェイサーバーの間のすべてのネットワーク通信が、BlackBerry Dynamics のセキュリティで保護された通信チャネルと BlackBerry Proxy サーバーを経由して転送されます。詳細については、「BlackBerry Dynamics 用 『409ページ 』 Files Advanced モバイルアプリ」マニュアルページを参照してください。
- **MobileIron AppConnect に登録されたアプリ**: Files Advanced モバイルアプリが MobileIron の AppConnect プラットフォームに登録されている場合は、Files Advanced モバイルアプリクライアントとゲートウェイサーバー間のすべてのネットワーク通信が MobileIron Sentry を経由して転送できます。詳細については、『MobileIron AppConnect『370ページ 』』のマニュアル ページを参照してください。

証明書:

Files Advanced には、テスト目的の自己署名証明書が付属しており、インストールされます。本稼動時には、適切な CA 証明書を実装する必要があります。

- **注意:** 自己署名証明書を使用する際、一部のウェブ ブラウザに警告メッセージが表示されます。これらのメッセージを非表示にすると、システムを問題なく使用できます。本番環境で自己署名証明書を使用することはお勧めしません。

4.1.5 デスクトップ クライアント要件

サポートされるオペレーティング システム:

- Windows 7、Windows 8 および 8.1、Windows 10

  注意: デスクトップクライアントバージョン 7.4 は、Windows XP および Vista と互換性がある最後のバージョンです。Files Advanced デスクトップクライアントのより新しいバージョンを使用するには、Windows OS をアップデートする必要があります。Files Advanced 7.4 は Windows XP または Vista から接続が可能な最後のバージョンです。

- Mac OS X 10.8 以降および 64 ビットソフトウェアと互換性のある Mac

  注意: デスクトップクライアントバージョン 7.1.2 は、Mac OS X 10.6 および 10.7 と互換性がある最後のバージョンです。より新しい Files Advanced デスクトップクライアントバージョンを使用するには、Mac OS をアップデートする必要があります。

  注意: Files Advanced デスクトップクライアントをインストールする際に、作成する同期フォルダが別のソフトウェアで同期されるフォルダ内に含まれないようにしてください。既知の競合のリストについては、「ソフトウェアの競合 『236ページ 』」を参照してください。

サポート対象ウェブブラウザ:

- Mozilla Firefox 6 以降
- Internet Explorer 9 以降

  注意: Internet Explorer を使用する場合、ファイルをダウンロードするためには、[**暗号化されたページをディスクに保存しない**] にチェック マークが付いていない状態にしておく必要があります。この設定は、[**インターネット オプション**] → [**詳細設定**] → [**セキュリティ**] にあります。

  注意: Internet Explorer 11 以前の場合、4 GB より大きなファイルのアップロードはサポートされていません。

- Google Chrome 4.1.249.1042 以降。
- Safari 5.1.10 以降。

4.2 お使いのサーバーに Files Advanced をインストールする

次の手順では、提供された自己署名証明書を使用して HTTPS で Files Advanced を新規インストールしてテストできます。

注意: アップグレード手順については、「アップグレード 『49ページ 』」のセクションを参照してください。

注意: クラスタでのインストール手順については、「負荷分散 『247ページ 』」のセクションを参照してください。

Files Advanced のインストールは次の 3 ステップで行います。

1. Files Advanced Web サーバーインストーラのインストール。
2. Files Advanced Web サーバーが使用するネットワーク ポートおよび SSL 証明書の構成
3. ウェブベースのセットアップ ウィザードによる、用途に合わせたサーバーの構成

Files Advanced のインストール

管理者としてログインしていることを確認してから Files Advanced をインストールしてください。

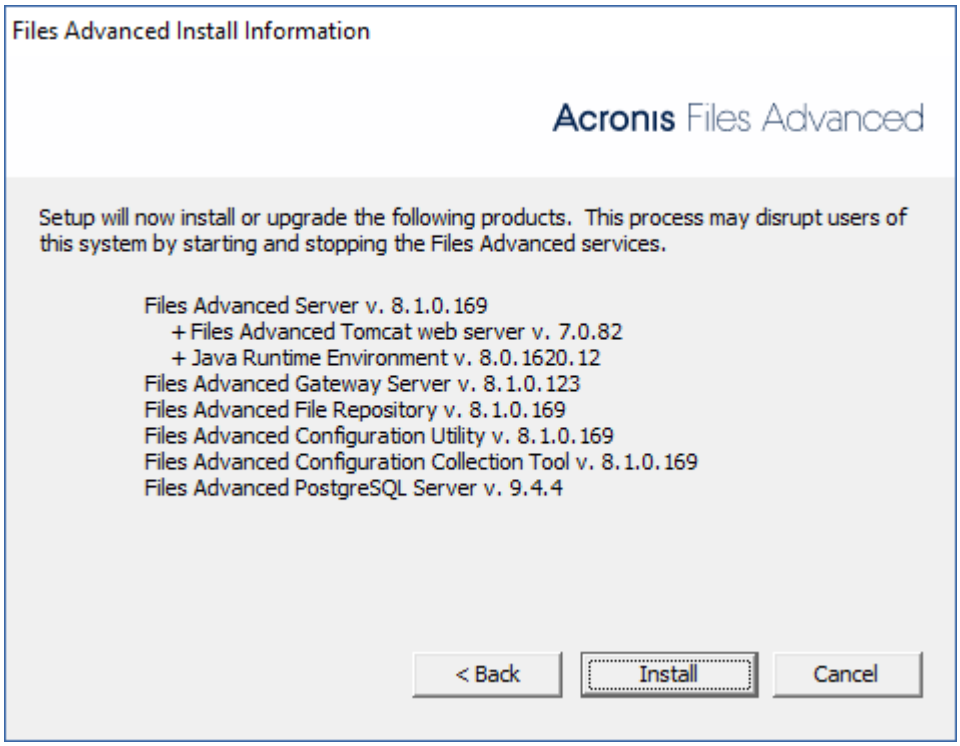
1. Files Advanced のインストーラをダウンロードします。
2. インストールされているウイルス対策ソフトウェアをすべて無効にしてください。無効にしない場合は、インストール手順が中断され、インストールが失敗する可能性があります。
3. 実行可能なインストーラをダブルクリックします。

4. **[次へ]** を押して開始します。

   使用許諾契約を読み、承諾します。
5. **[インストール]** を押します。

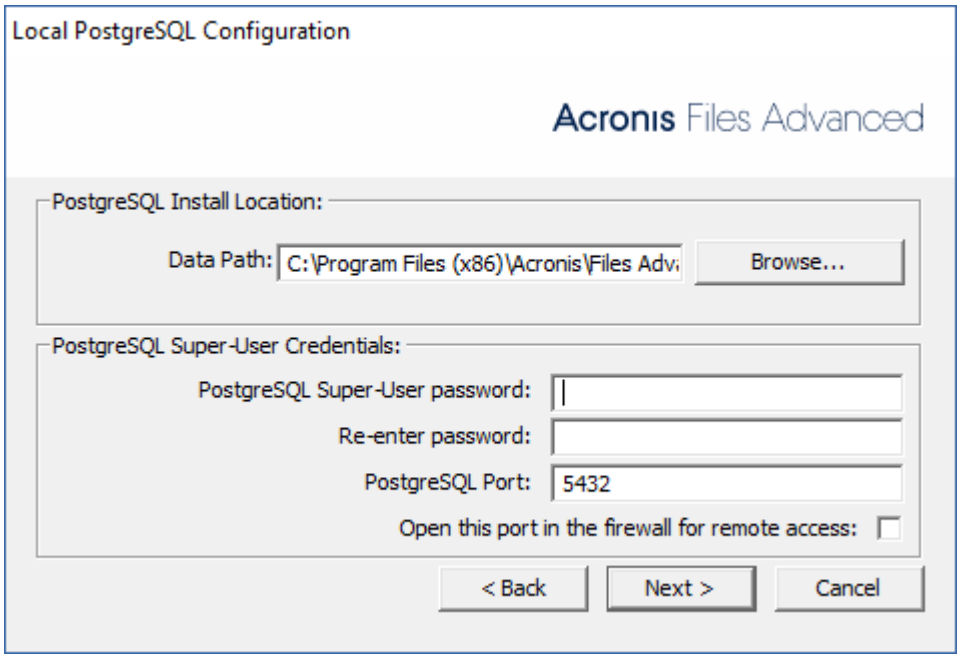
注意: 複数の Files Advanced サーバーを配置する場合や、標準構成以外でインストールを行う場合は、**[カスタム インストール]** ボタンからインストールするコンポーネントを選択することができます。

6. Files Advanced メインフォルダのデフォルトパスを使用するか新しいパスを選択し、[OK] を押します。



7. ユーザー Postgres のパスワードを設定し、書き留めておきます。このパスワードは、データベースのバックアップと復旧に必要となります。

8.



9. インストールされるコンポーネントがすべてリストされたウィンドウが表示されます。続行するには、**[OK]** を押します。
10. Files Advanced のインストーラが完了したら、**[終了]** を押します。
11. 設定ユーティリティが自動的に起動し、インストールが完了します。

設定ユーティリティの使用方法については、「設定ユーティリティの使用 『36ページ 』」ページを参照してください。

4.3 設定ユーティリティの使用

Files Advanced インストーラには、設定ユーティリティを付属しています。このユーティリティを使用すると、Files Advanced ゲートウェイ サーバー、ファイル リポジトリおよび Files Advanced Web サーバーへのアクセスをすばやく、簡単に設定できます。

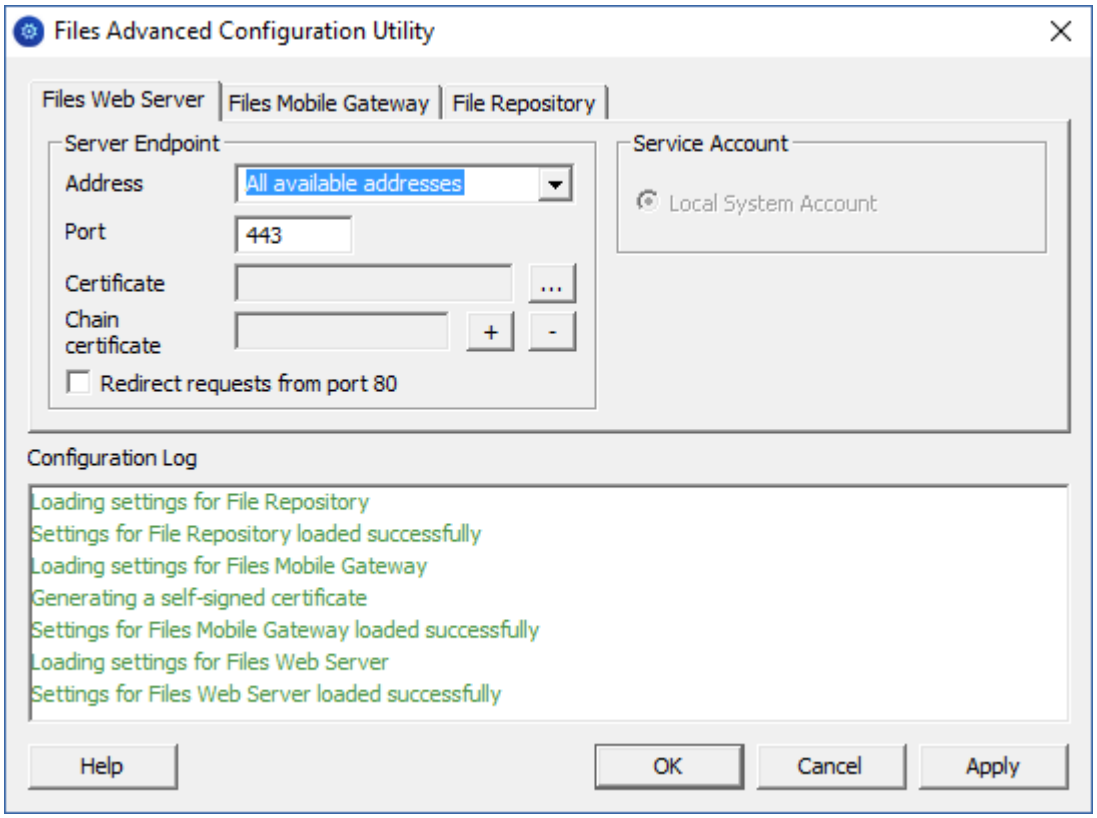
注意: Files Advanced の IP アドレス設定のベスト プラクティスに関する詳細については、「ネットワーク要件 『31ページ 』」セクションを参照してください。

注意: Microsoft Windows 証明書ストアに証明書を追加する方法については、「証明書の使用 『324ページ 』」を参照してください。

構成ユーティリティの概要

構成ユーティリティ内の設定は、いつでもユーティリティを起動して必要な変更を加えることによって変更できます。自動的に必要な設定ファイルを調整し、サービスを再起動します。

[ウェブサーバー] タブ

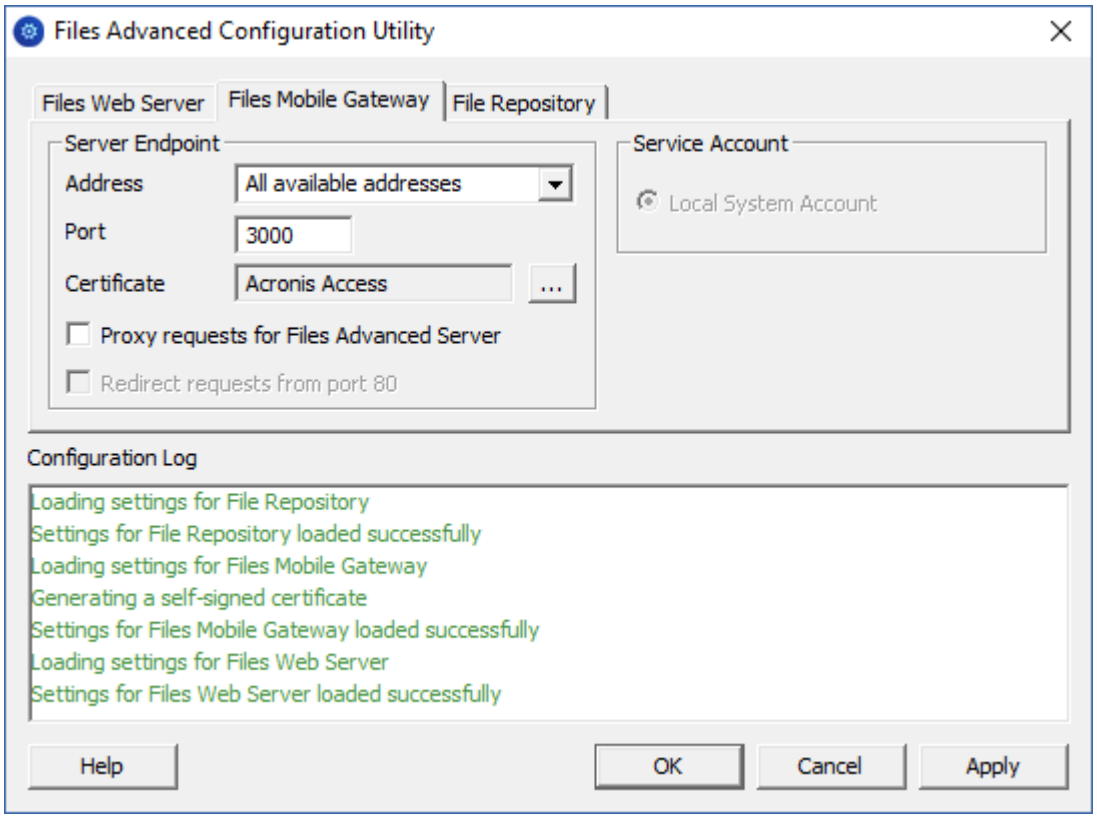


Files Advanced Web サーバーは、Files Advanced クライアントにウェブユーザーインターフェイスを提供すると同時に、モバイルアクセス 『68ページ 』と同期・共有の両方の管理コンソールにもなります。

- **アドレス**: ウェブインターフェイスの IP アドレス。利用可能なすべてのインターフェイスでリッスンするには **[すべてのアドレス]** を選択します。
- **ポート**: ウェブ インターフェイスのポート。
- **証明書**: ウェブ インターフェイスの証明書のパス。Microsoft Windows 証明書ストアから証明書を選択できます。
- **チェーン証明書**: ウェブインターフェイスの中間証明書のパス。Microsoft Windows 証明書ストアから証明書を選択できます。証明機関でも中間証明書が発行されている場合にのみ、この証明書が必要になります。
- **ポート 80 での接続を許可します**: このオプションが選択されている場合、Tomcat は、セキュアでないポート 80 で着信トラフィックをリッスンし、それを上記で指定された HTTPS ポートにリダイレクトします。ポート 80 上でリッスンする別のプログラムがある場合は、このボックスをオンにしないでください。

- **サービスアカウント**: これにより、Files Advanced Web サーバーサービスを別のアカウントのコンテキストで実行できます。 通常のインストールでは必要ありません。

[Mobile Gateway] タブ



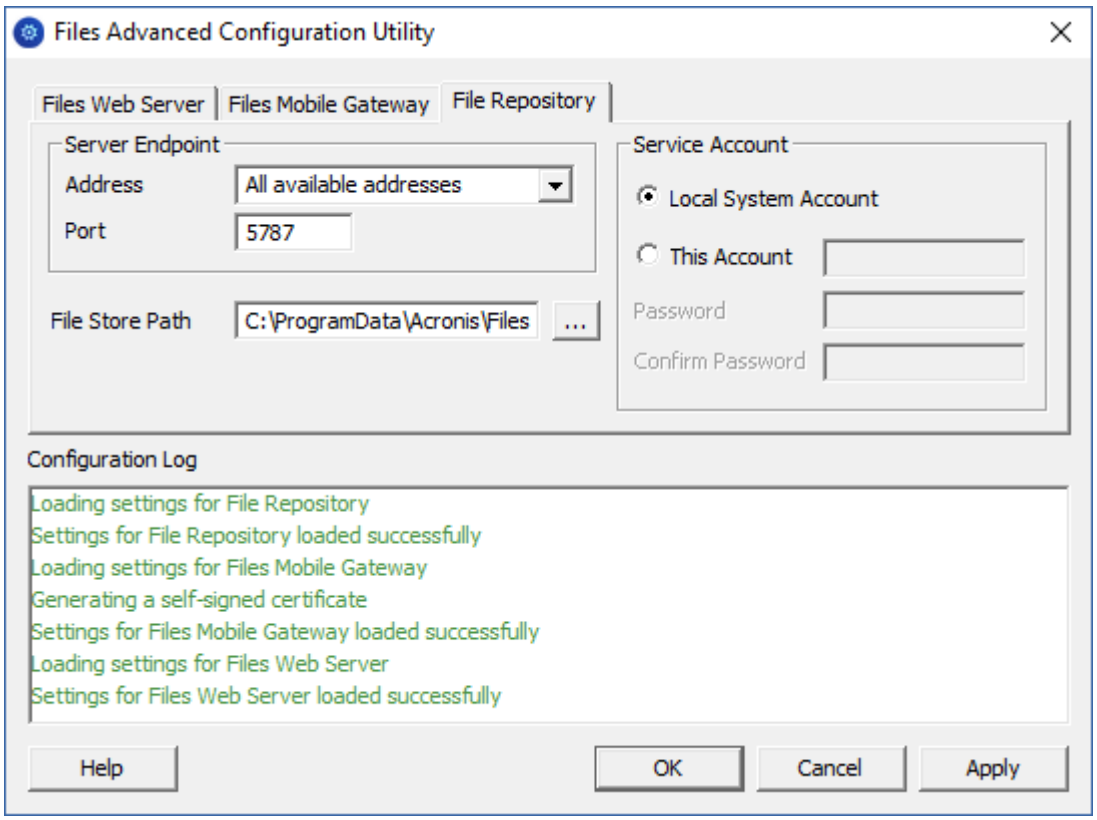
ゲートウェイサーバーは、モバイルクライアントからファイルと共有の両方にアクセスするのに使われます。

- **アドレス**: ゲートウェイサーバーの IP アドレス。すべてのインターフェイスでリッスンするには **[すべてのアドレス]** を選択します。
- **ポート**: ゲートウェイサーバーのポート。
- **証明書**: ゲートウェイサーバーの証明書のパス。Microsoft Windows 証明書ストアから証明書を選択できます。
- **サービスアカウント:** ゲートウェイサーバーサービスを別のアカウントのコンテキストで実行できます。 通常のインストールでは必要ありません。
- **Files Advanced サーバーに対するプロキシ要求**: このオプションをオンにすると、ユーザーはゲートウェイサーバーに接続され、ゲートウェイサーバーが Access サーバーのプロキシサーバーとして機能します。このオプションを使用できるのは、Files

Advanced サーバーとゲートウェイサーバーが同じマシン上にインストールされている場合です。

- **ポート 80 での接続を許可します**: このオプションが選択されている場合、Tomcat は、セキュアでないポート 80 で着信トラフィックをリッスンし、それを上記で指定された HTTPS ポートにリダイレクトします。ポート 80 上でリッスンする別のプログラムがある場合は、このボックスをオンにしないでください。

[ファイル リポジトリ]タブ



ファイルリポジトリは、同期・共有機能で使用します。同期・共有機能をまだ有効にしていない場合は、標準の値を適用できます。同期・共有を使用している場合、ファイルストアのパスとして、ストレージに使用するディスクのロケーションを指定する必要があります。ストレージに Amazon S3 を使用する計画がある場合、デフォルトの値でかまいません。

- **アドレス**: ファイルリポジトリの IP アドレス。すべてのインターフェイスでリッスンするには **[すべてのアドレス]** を選択します。IP または DNS アドレスを指定する場合、同じアドレスをを、ウェブ インターフェイスの [**ファイル リポジトリ**] セクションに

も指定する必要があります。詳しくは、「ファイル リポジトリ 『154ページ 』」の記事を参照してください。

- **ポート:** ファイル リポジトリのポート。同じポートをを、ウェブ インターフェイスの [**ファイル リポジトリ**] セクションにも指定する必要があります。詳しくは、「ファイル リポジトリ 『154ページ 』」の記事を参照してください。
- **ファイル ストアのパス:** [ファイル ストア] の UNC パス。ファイル ストアのパスを変更する場合は、元のファイル ストアの場所に既に存在するファイルすべてを、新しい場所に手動でコピーする必要があります。

  注意: ファイル ストアを別の場所に移動する場合は、新しいファイルが正しく新しい場所に移動されるようにアップロードする必要があります。また、ファイル ストアに既に存在していたファイルをダウンロードして、元の場所にあったファイルのすべてが新しい場所でもアクセス可能な状態にしておく必要があります。

- **サービス アカウント:** リポジトリのファイル ストレージがリモート ネットワーク共有にある場合、サービス アカウントがそのネットワーク共有へのアクセス許可を持つように設定する必要があります。このアカウントには、ログファイルを書き込むため、リポジトリフォルダ（たとえば、**C:\Program Files (x86)\Acronis\Files Advanced\File Repository\Repository**)への読み取り/書き込みアクセス権限も必要です。

  注意: ローカルシステムアカウントではなく、このサービスに固有のアカウントを使用する場合は、**[サービス]** コントロールパネルを開き、**Files Advanced ファイルリポジトリ**サービスのプロパティを開いて、**[ログオン]** タブを編集してください。アカウントとパスワードは対応するフィールドに手動で入力してください。

セットアップウィザードに進む

必要なフィールドのすべてに入力した後、[**適用**] または [**OK**] を押すと、変更を加えたサービスが再起動します。

注意: サービスが開始されてから 30～45 秒経つと、Files Advanced Web サーバーが利用できるようになります。

1. 構成ユーティリティの初期セットアップが完了すると、ウェブブラウザで自動的に Files Advanced ウェブインターフェイスが開きます。

2. ログインページで、**管理者**パスワードを設定するよう促すメッセージが表示されます。セットアップウィザード 『41ページ 』が表示され、そこでセットアッププロセスを実行できます。

管理者パスワードを書き留めておいてください。忘れた場合はパスワードを復元することができません。

4.4 セットアップ ウィザードの使用

ソフトウェアをインストールし、設定ユーティリティを実行してネットワーク ポートと SSL 証明書を設定した後、管理者は Files Advanced サーバーを設定する必要があります。設定ウィザードは、管理者に一連の手順を案内し、サーバーの基本的な機能が動作するようにします。

注意: 設定ユーティリティを実行した後、サーバーが最初に起動するまで 30～45 秒かかります。

以前のステップで管理者アカウントをセットアップしなかった場合は、ログインページで、**管理者**パスワードを設定するよう促すメッセージが表示されます。

管理者パスワードを書き留めておいてください。忘れた場合はパスワードを復元することができません。

初期構成プロセスを進める

設定ユーティリティで指定した IP アドレスとポートを使用して、Files Advanced のウェブ インターフェイスに移動します。デフォルトの管理者アカウントにパスワードを設定するように求めるメッセージが表示されます。

注意: 追加の管理者は後から設定できます。詳細については、「サーバーの管理 『166ページ 』」セクションを参照してください。

このウィザードにより、製品の主要な機能を設定できます。

- [全般設定] では、言語、カラー スキーム、管理者通知で使用されるサーバー名、ライセンス、管理者など、ウェブ インターフェイス自体の設定を行います。
- [LDAP] の設定では、製品で Active Directory の資格情報、ルール、ポリシーを使用できるようにします。

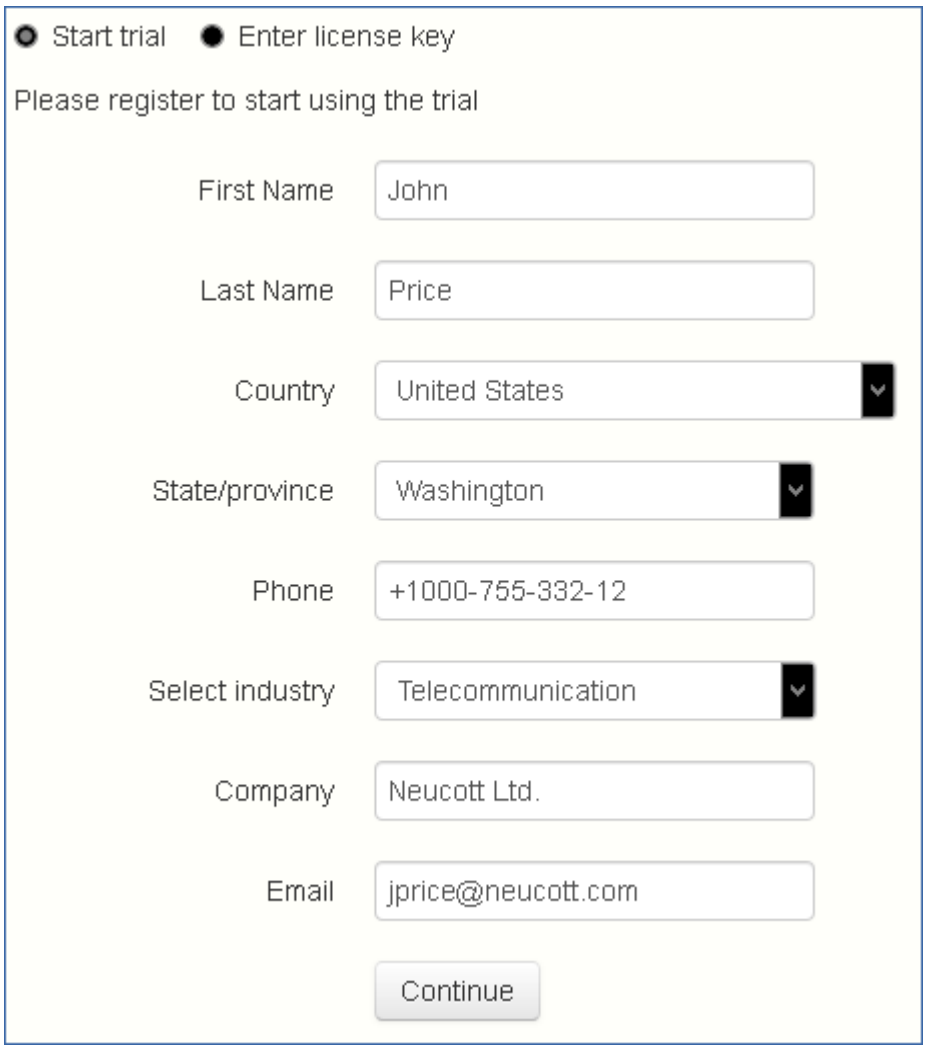
- [SMTP] の設定では、モバイル アクセス機能、および同期と共有機能の設定を行います。モバイル アクセスでは、登録招待の送信時に SMTP サーバーが使用されます。同期と共有機能は、フォルダへの招待、警告、エラーの概要を送信するために SMTP サーバーを使用します。

[初期構成] ページで見ることができるすべての設定は、構成の完了後にも確認することができます。設定の詳細については、「サーバー管理 『166ページ 』」の資料を参照してください。

ライセンス

試用版を開始するには:

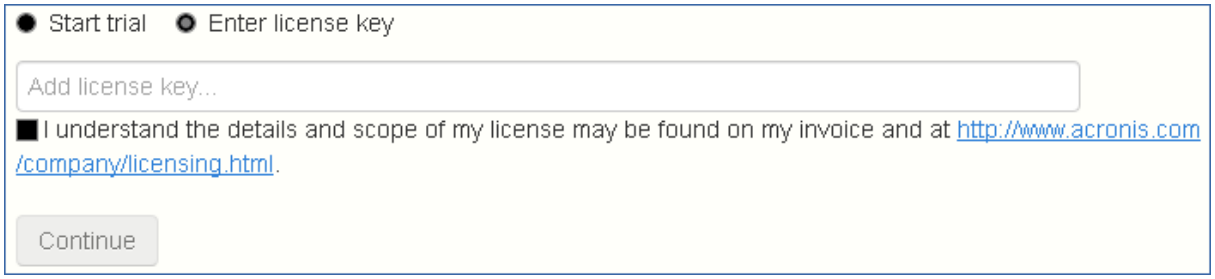
1. **[試用を開始]** を選択し、必要な情報を入力して **[送信]** を押します。



2.

Files Advanced インスタンスにライセンスを付与するには:

1. **[プロダクト キーを入力します]** を選択します。
2. プロダクトキーを入力し、チェックボックスを選択します。

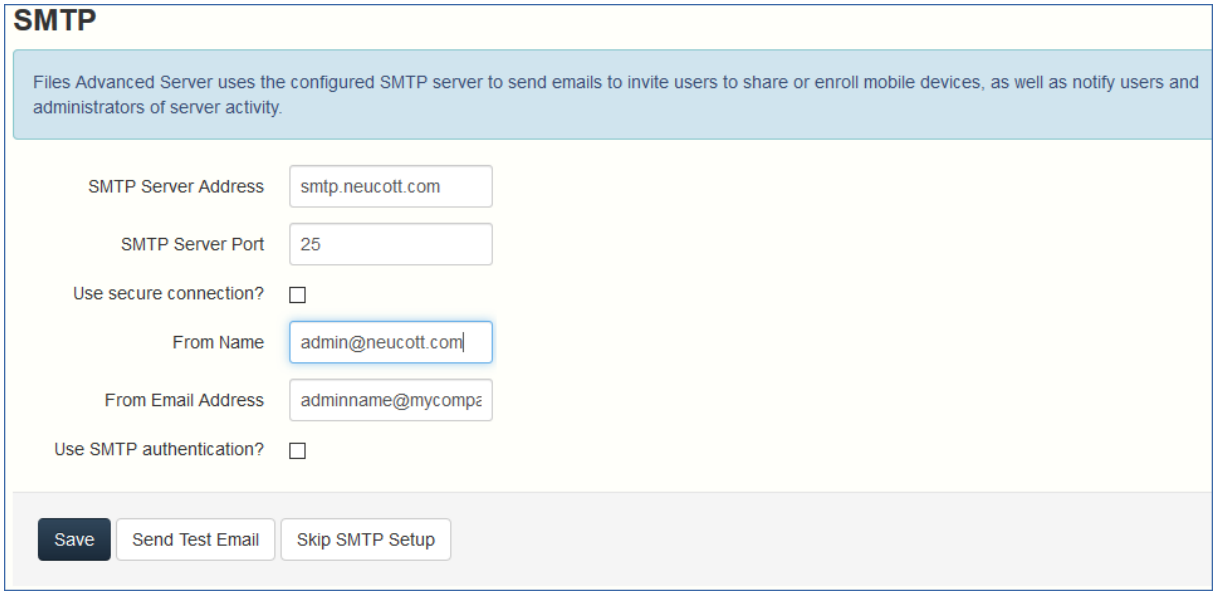


3. **[保存]** を押します。

全般設定

1. [サーバー名] にサーバー名を入力します。
2. ユーザーが (http:// または https:// で始まる)ウェブ サイトにアクセスできる FQDN または IP アドレスを指定します。
3. **[監査ログ]** のデフォルトの言語を選択します。現在のオプションは、**[英語]、[ドイツ語]、[フランス語]、[日本語]、[イタリア語]、[スペイン語]、[チェコ語]、[ロシア語]、[ポーランド語]、[韓国語]、[中国語（繁体字)]、[中国語（簡体字)]** です。
4. **[保存]** を押します。

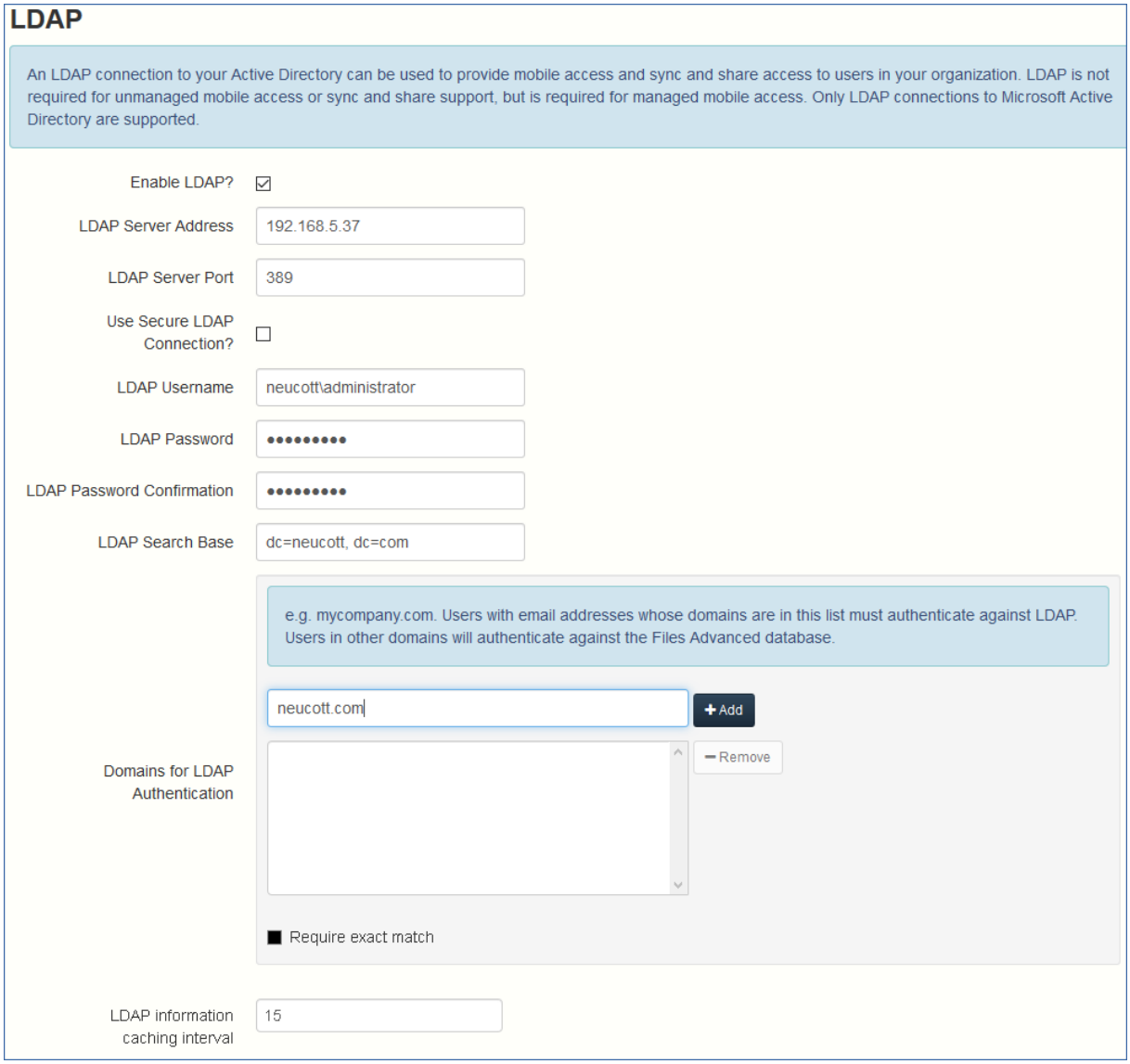
SMTP



注意: この手順をスキップして、後で SMTP を構成することもできます。

1. SMTP サーバーの FQDN または IP アドレスを入力します。
2. サーバーの SMTP ポートを入力します。
3. SMTP サーバーの証明書を使用しない場合は、**[セキュリティで保護された接続を使用しますか？]** のチェックを外します。
4. サーバーによって送信される電子メールの「差出人」行に表示されるユーザー名を入力します。
5. サーバーから送信される電子メールのアドレスを入力します。
6. SMTP サーバーでユーザー名やパスワードの認証を使用している場合は、**[認証を使用しますか？]** をチェックし、認証情報を入力してください。
7. **[テスト用の電子メールの送信]** を押して電子メールを手順 5 で指定したテスト用の電子メール アドレスに送信します。
8. **[保存]** を押します。

LDAP

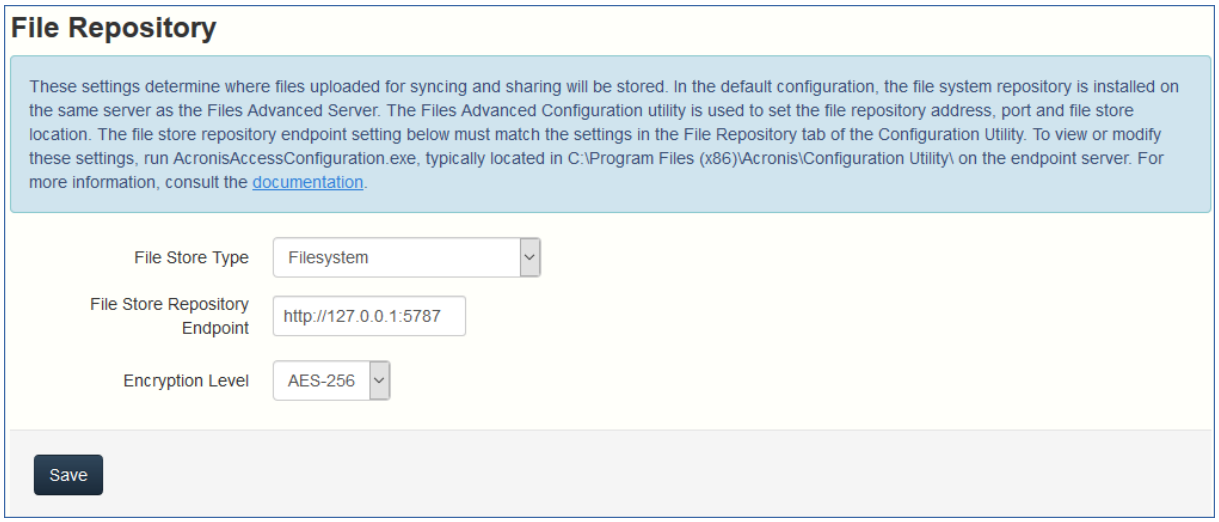


注意: この手順をスキップして、後で LDAP を構成することもできます。しかし、一部の Files Advanced 機能は構成するまで使用できません。

1. **[LDAP を有効にしますか？]** をチェックします。
2. LDAP サーバーの FQDN または IP アドレスを入力します。
3. LDAP サーバーのポートを入力します。
4. LDAP サーバーとの接続に証明書を使用する場合は、**[セキュリティで保護された LDAP 接続を使用しますか？]** をチェックします。
5. LDAP の資格情報をドメインも含めて入力します（例: acronis¥hristo)。
6. LDAP 検索ベースを入力します。

7. LDAP 認証のドメインを入力します （例えば、電子メール **joe@glilabs.com** のアカウントの LDAP 認証を有効にするには、**glilabs.com** と入力します)。
8. **[保存]** を押します。

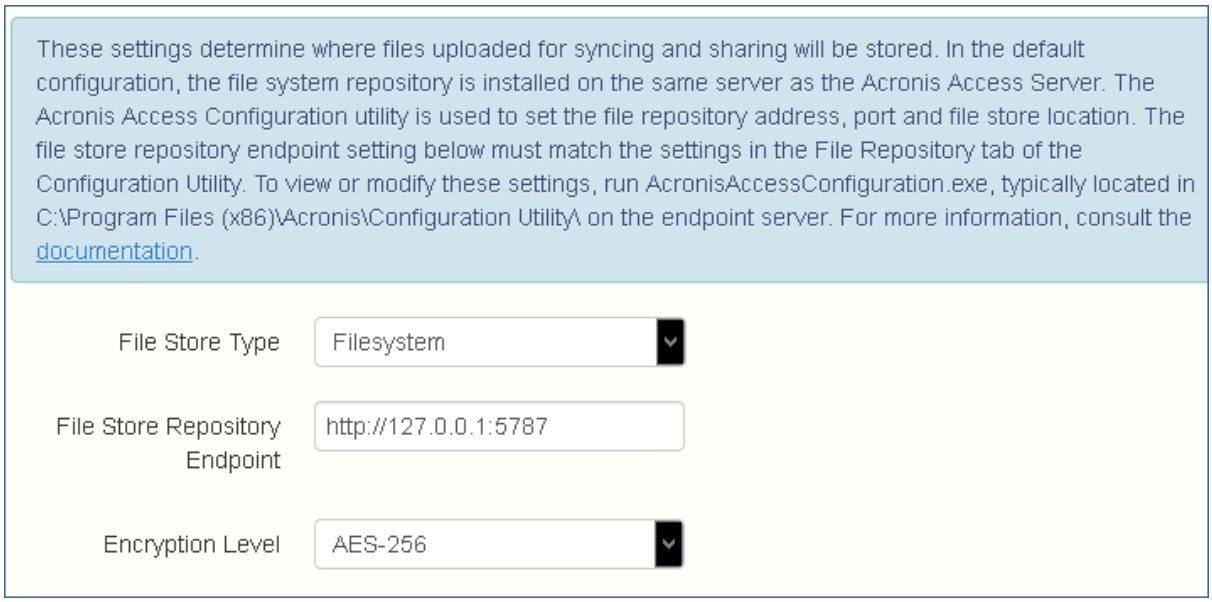
ローカル ゲートウェイ サーバー



注意: 同じコンピュータにゲートウェイ サーバーと Files Advanced サーバーの両方をインストールする場合、ゲートウェイ サーバーが自動的に検出され、Files Advanced サーバーに管理されます。クライアントがアクセス可能なローカル ゲートウェイ サーバーの FQDN または IP アドレスを設定するように指示するメッセージが表示されます。このアドレスは後から変更できます。

1. ローカル ゲートウェイ サーバーの FQDN または IP アドレスを設定します。
2. **[保存]** を押します。

ファイル リポジトリ



1. ファイル ストア タイプを選択します。お使いのコンピュータのファイルストアの場合は **[ファイルシステム]** を、クラウドのファイルストアの場合は **[Amazon S3]** を使います。
2. ファイル リポジトリ サービスの FQDN または IP アドレスを入力します。

   注意: ファイルリポジトリのアドレス、ポート、およびファイルストアのロケーションを設定するには、Files Advanced 設定ユーティリティを使用します。ファイルストアリポジトリエンドポイントの設定は、設定ユーティリティの [ファイル リポジトリ] タブの設定と一致していなければなりません。設定値を表示または変更するには、AcronisAccessConfiguration.exe を実行します。通常、このファイルはエンドポイントサーバーの **C:\Program Files (x86)\Acronis\Files Advanced\Common\Configuration Utility** にあります。
3. 暗号化レベルを選択します。**[なし]**、**[AES-128]**、**[AES-256]** から選択してください。
4. サーバーがユーザーに警告を送信する最小限の空き領域を選択してください。
5. **[保存]** を押します。

4.5 Files Advanced のクラスタリング

Files Advanced では、サードパーティのクラスタリング ソフトウェアを使用せずに、可用性の高い設定を行うことができます。設定には、Files Advanced 5.1 で導入された新しいクラスタ グループ機能を使用します。設定手順はシンプルで、Files Advanced ゲートウェイ サーバーには高い可用性がもたらされますが、ゲートウェイ サーバーは負荷が最も高いコンポーネントです。設定のすべては、Files Advanced サーバーを通して管理されます。

クラスタ グループの詳細や設定手順に関する詳細については、「クラスタ グループ 『131ページ 』」の記事を参照してください。

組み込みのクラスタ グループ機能を使用することをお勧めいたしますが、Files Advanced では Microsoft Failover Clustering もサポートされています。こちらの詳細については、「補足資料 『236ページ 』」セクションを参照してください。

4.6 Files Advanced の負荷分散

Files Advanced では負荷分散がサポートされています。詳細については、Files Advanced の負荷分散 『247ページ 』、負荷分散構成での Files Advanced のインストール 『257ページ 』、負荷分散環境への移行 『265ページ 』、クラスタグループ 『131ページ 』に関する各記事を参照してください。

5 アップグレード

セクションの内容

5.1 Files Advanced の新しいバージョンへのアップグレード

Files Advanced を以前のバージョンからアップグレードする手順は、簡単で、設定の必要もほとんどありません。

注意: Files Advanced 7.0 より前のバージョンを使用している場合は、アクロニスサポート http://www.acronis.com/en-us/mobilitysupport/までお問い合わせください。

注意: アップグレードする前に、最小ハードウェア要件 『29ページ 』を確認してください。

注意: 導入環境によっては、この記事で使用されている一部のパスがご使用のパスと異なる可能性があります。以前のバージョンの Files Advanced からのアップグレードやカスタムインストールにより、導入環境のフォルダ構造に影響が現れる可能性があります。

重要なコンポーネントのバックアップ

Apache Tomcat フォルダ

アップグレード時に Apache Tomcat がアップグレードされ、現在の Tomcat のすべての設定ファイル およびログ ファイルが削除されます。Apache Tomcat フォルダのコピーを作成することをお勧めします。デフォルトでは、このフォルダは次の場所にあります:

C:\Program Files (x86)\Acronis\Files Advanced\Common\.

web.xml ファイルは更新する前にバックアップしておくことをお勧めします。**web.xml** ファイルはアップグレード時に上書きされます。バージョン 7.1.2 以降のバックアップの保存場所は **C:\Program Files (x86)\Acronis\Files Advanced\Access Server\Web Application\WEB-INF\<timestamp>.previous.web.xml** です。維持しておきたい特定の変更（シングルサインオン 『284ページ 』は除きます。この変更は保存されます)がある場合は、古いファイルからその変更を手動でコピーし貼り付けてください。

不要な監査ログの消去

自動ログ消去 『170ページ 』を設定していない場合は、サーバーにログがたまって、バックアッププロセスの速度が低下する可能性があります。データベースのバックアップを実行する前に、古いログをエクスポートまたは消去することをお勧めします。

PostgreSQL データベース

次の手順を実行すると、元のデータベースのテキスト表示が格納された *.sql ファイルを作成することができます。

1. コマンド プロンプト ウィンドウを開き、PostgreSQL のインストール ディレクトリ（例: **cd "C:\PostgreSQL\9.2\bin"**)内にある **9.2\bin** フォルダに移動します。
2. 現在のコマンド プロンプト ウィンドウのディレクトリを **bin** フォルダに移動したら、次のコマンドを入力してください。

   pg_dump -U postgres -f mybackup.sql acronisaccess_production
   mybackup.sql は、生成されたバックアップ ファイルのファイル名です。
   D:\Backups\mybackup.sql のように、バックアップ ファイルを作成するロケーションのフル パスを含めることもできます。

   注記: acronisaccess_production は Files Advanced データベースの名前に表示されるとおりに正確に入力する必要があります。

3. 「Password:」という行が表示されます。Files Advanced のインストール プロセス中に設定した postgres のパスワードを入力してください。

   注記: パスワードを入力しても、コマンド プロンプト ウィンドウの視覚的な変化はまったくありません。

4. 出力ファイルにほかのディレクトリへのフル パスが指定されていない限り、バックアップ ファイルは、デフォルトで **bin** フォルダに作成されます。

注記: PostgreSQL データベース全体のバックアップを行う場合は、次のコマンドを使用してください。

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

alldbs.sql は作成されるバックアップ ファイルです。**D:\Backups\alldbs.sql** のようにフルパスを指定することも可能です。

このコマンドの完全な構文の詳細については、
http://www.postgresql.org/docs/9.2/static/app-pg-dumpall.html
http://www.postgresql.org/docs/9.1/static/app-pg-dumpall.html（英語)を参照してください。

情報: PostgreSQL のバックアップ手順とコマンド構文の詳細については、
http://www.postgresql.org/docs/9.2/static/backup.html
http://www.postgresql.org/docs/9.1/static/backup.html（英語)を参照してください。

ゲートウェイ サーバー データベース

1. Files Advanced ゲートウェイ サーバーがインストールされているサーバーを参照します。
2. データベースを含むフォルダに移動します。

   注意: デフォルトのロケーションは、 **C:\Program Files (x86)\Acronis\Access\Gateway Server\database** です。

3. **mobilEcho.sqlite3** ファイルをコピーして、安全な場所に貼り付けます。

Files Advanced の設定ファイル

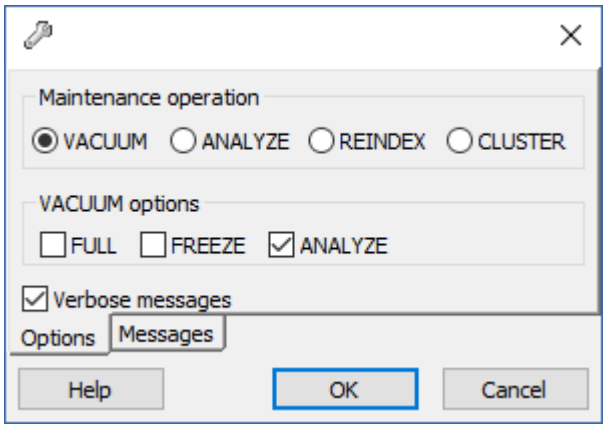
1. 設定ファイルが含まれる Files Advanced のインストール フォルダに移動します。

   注意: デフォルトの場所は、**C:\Program Files (x86)\Acronis\Files Advanced\Access Server** です。

2. **acronisaccess.cfg** ファイルをコピーして、安全な場所に貼り付けます。

アップグレード前のデータベースのバキューム

1. Files Advanced PostgreSQL 管理者ツール（PgAdmin ともいう)を開き、**localhost** をダブルクリックしてサーバーに接続します。
2. **acronisaccess_production** データベースを右クリックして、**[メンテナンス]** を選択します。
3. **[バキューム]** ラジオボタンと **[分析]** チェックボックスをオンにします。



警告: 非常に大きなデータベースの場合には、バキューム処理にしばらく時間がかかる場合があります。この処理はサーバーへの負荷が低い時間帯に行うことをおすすめします。

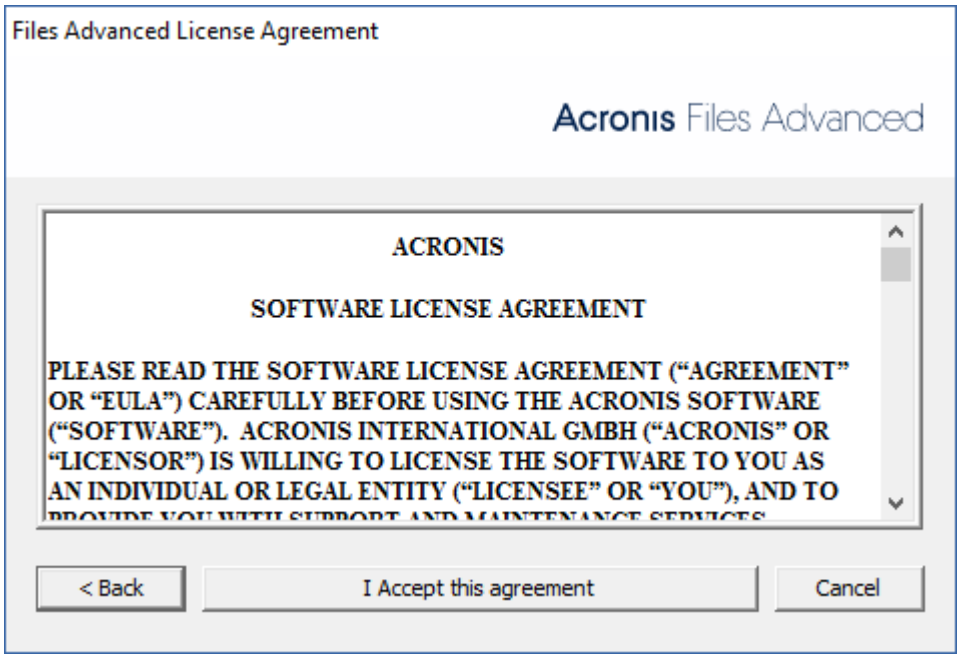
4. **[OK]** を押します。
5. **[バキューム]** プロセスが終わると、**[完了]** を押します。
6. PostgreSQL 管理ツールを閉じます。

アップグレード

1. インストールされているウイルス対策ソフトウェアをすべて無効にしてください。無効にしない場合は、インストール手順が中断され、インストールが失敗する可能性があります。
2. 実行可能なインストーラをダブルクリックします。

3. **[次へ]** を押して開始します。

4. 使用許諾契約を読み、承諾します。



5. **[アップグレード]** を押します。
6. インストールするコンポーネントを確認して、**[インストール]** をクリックします。
7. インストールされたコンポーネントを確認して、インストーラを閉じます。
8. 設定ユーティリティを開くように求められたら、**[OK]** を押します。
9. 設定ユーティリティの設定が変更されていないことを確認します。すべての設定が希望の設定と同じであることを確認したら、**[OK]** を押して設定ユーティリティを閉じ、Files Advanced サービスを開始します。

5.2 mobilEcho バージョン 4.5 以前からのアップグレード

mobilEcho からアップグレードするには、アクロニステクニカルサポート（http://www.acronis.com/mobilitysupport)にお問い合わせください。

5.3 activEcho バージョン 2.7 以前からのアップグレード

activEcho からアップグレードするには、アクロニステクニカルサポート（http://www.acronis.com/mobilitysupport)にお問い合わせください。

5.4 ゲートウェイクラスタのアップグレード

Files Advanced のクラスタ構成をアップグレードするには、Files Advanced Web サーバーとクラスタ グループ 『131ページ 』のゲートウェイ サーバーの両方をアップグレードする必要があります。

注意: Microsoft Failover Clustering 構成のアップグレードの詳細については、「補足資料 『236ページ 』」セクションを参照してください。

注意: Files Advanced Web サーバーのアップグレードの方法については、「Files Advanced の新しいバージョンへのアップグレード 『49ページ 』」の記事を参照してください。

ゲートウェイサーバーごとに、次のアップグレード手順を実行する必要があります。

アップグレードを実行する前に、「バックアップ 『200ページ 』」の記事を確認してから構成をバックアップしてください。

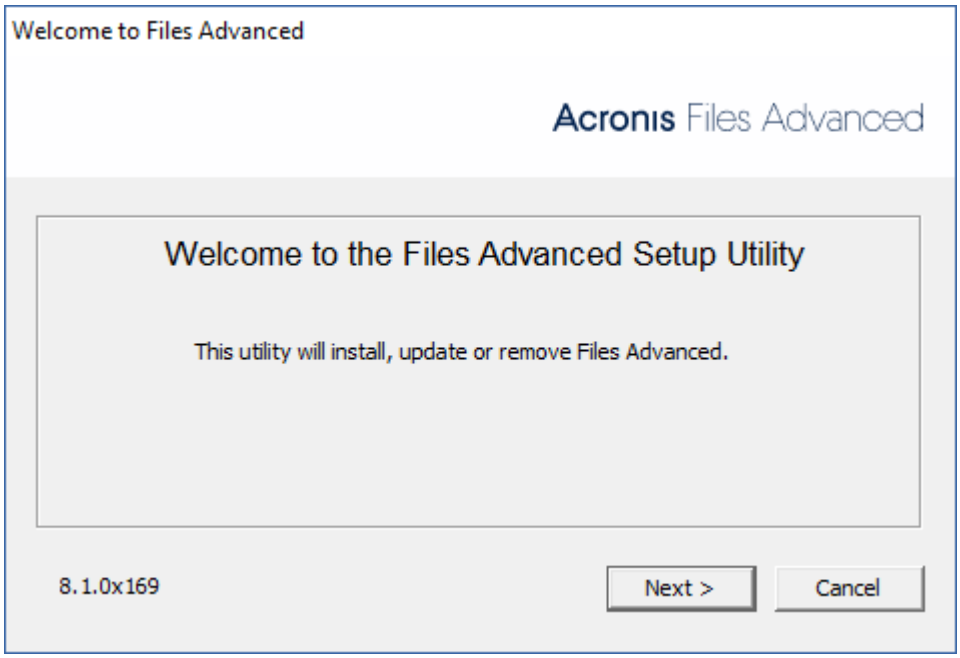
注意: アップグレードする前に、最小ハードウェア要件 『29ページ 』を確認してください。

注意: 導入環境によっては、この記事で使用されている一部のパスがご使用のパスと異なる可能性があります。以前のバージョンの Files Advanced からのアップグレードやカスタムインストールにより、導入環境のフォルダ構造に影響が現れる可能性があります。

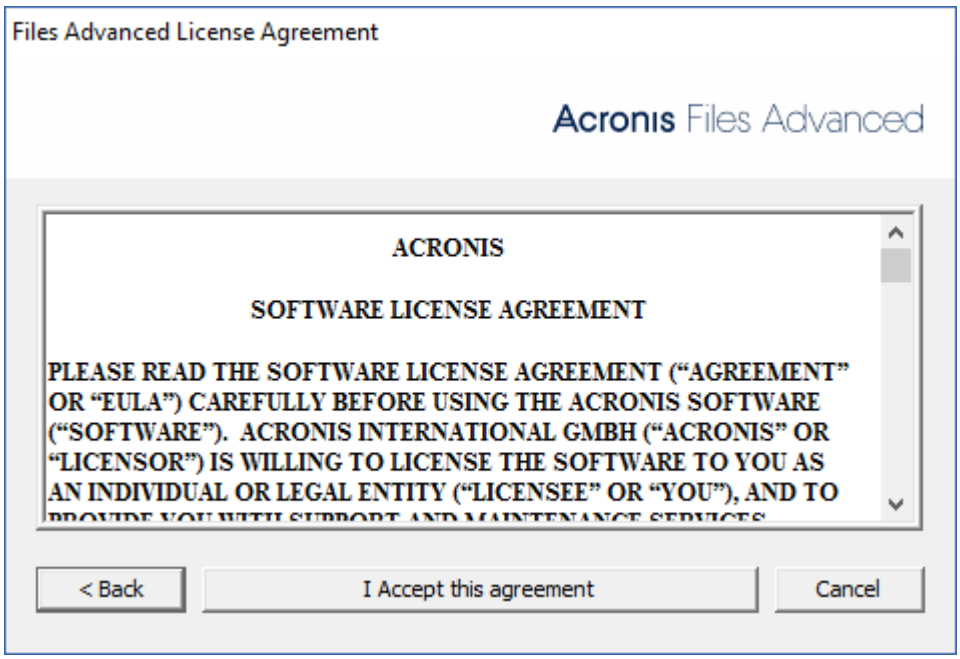
ゲートウェイ サーバーのアップグレード

対象のサーバーで Files Advanced インストーラを実行します。

1. **[ようこそ]** 画面で **[次へ]** をクリックします。

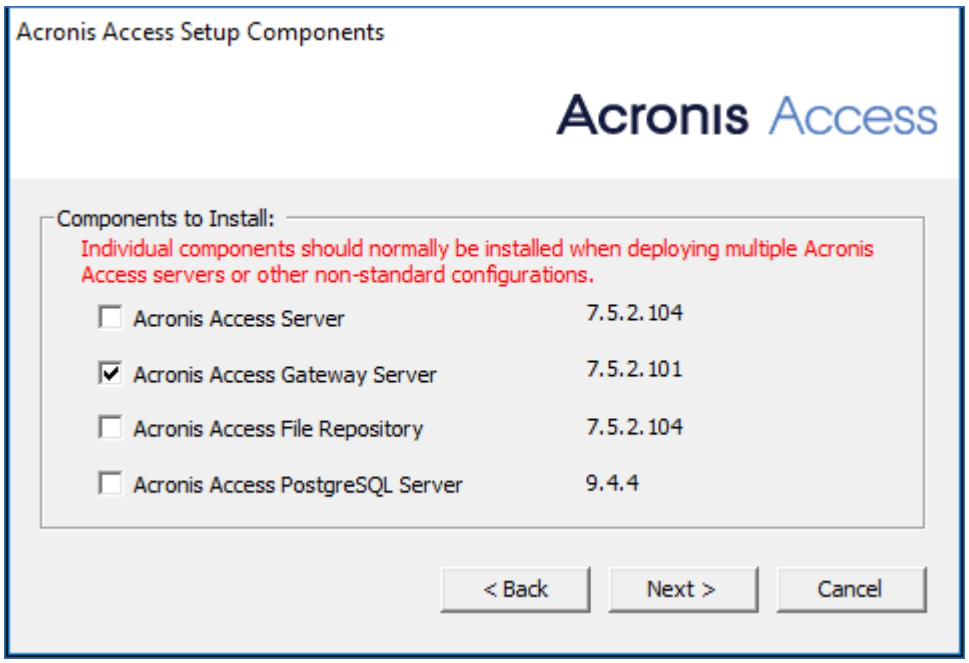


2. 使用許諾契約を読み、承諾します。



3.
4. **[カスタム]** を選択します。

5. **[Files Advanced ゲートウェイサーバー]** コンポーネントのみを選択して、**[次へ]** をクリックします。



6. コンポーネントを確認し、**[インストール]** を押します。
7. インストールの完了後、**概要**を確認してからインストーラを閉じます。
8. **設定ユーティリティ**を開くように求められたら、設定ユーティリティを開き、ゲートウェイ サーバーの以前の設定がすべて保持されていることを確認します。必要に応じて変更を加え、[OK] を押します。

5.5 ロードバランス設定のアップグレード

このガイドでは、Files Advanced のロードバランシング、およびそのコンポーネントすべてのデプロイについて説明します。

アップグレードを実行する前に、「バックアップ 『*200*ページ 』」の記事を確認してから構成をバックアップしてください。

注意: アップグレードする前に、最小ハードウェア要件 『29ページ 』を確認してください。

注意: 導入環境によっては、この記事で使用されている一部のパスがご使用のパスと異なる可能性があります。以前のバージョンの Files Advanced からのアップグレードやカスタムインストールにより、導入環境のフォルダ構造に影響が現れる可能性があります。

セクションの内容

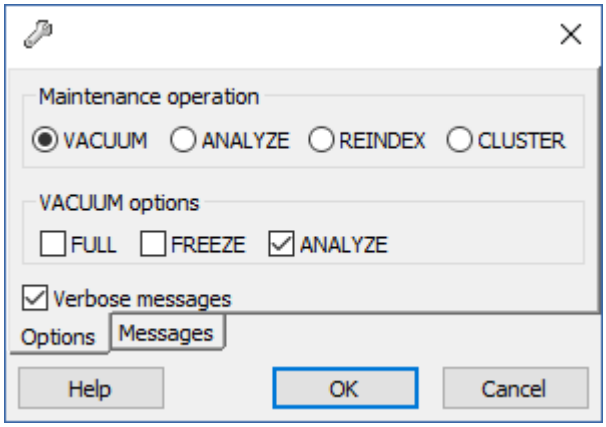
プライマリとして機能する Files Advanced Web サーバーコンピュータの 1 つを選択します。このコンピュータは、最初にアップグレードされ、変更/設定が PostgreSQL データベースに移行されるという意味においてのみ**プライマリ**ノードです。非常に大きなデータベースの場合は、これらの移行に数分かかることがあります。

警告!: プライマリサーバーがアップグレードされ、ウェブインターフェイスにログインしてそのサーバーを試すことができるようになるまで、他の Tomcat サーバーをアップグレードしないでください。

データベースのバキューム

これにより、データベースを最適化することでバックアップと復元のプロセスが高速化されます。

1. Files Advanced PostgreSQL 管理者ツール（PgAdmin ともいう)を開き、**localhost** をダブルクリックしてサーバーに接続します。
2. **acronisaccess_production** データベースを右クリックして、**[メンテナンス]** を選択します。
3. **[バキューム]** ラジオボタンと **[分析]** チェックボックスをオンにします。



警告: 非常に大きなデータベースの場合には、バキューム処理にしばらく時間がかかる場合があります。この処理はサーバーへの負荷が低い時間帯に行うことをおすすめします。

4. **[OK]** を押します。
5. **[バキューム]** プロセスが終わると、**[完了]** を押します。
6. PostgreSQL 管理ツールを閉じます。

バックアップと復元の手順の詳細については、『Files Advanced のバックアップと復元 『*200*ページ 』』の記事を参照してください。

PostgreSQLデータベースのバックアップ

1. すべての Files Advanced Tomcat サービスを停止します。
2. Files Advanced PostgreSQL Administrator アプリケーションを開き、データベースサーバーに接続します。**postgres** ユーザーのパスワード入力を求められる場合があります。
3. **[データベース]**を展開し、**acronisaccess_production** データベースを右クリックします。
4. **[メンテナンス]** を選択して、**[バキューム]** ラジオボタンを選択し、**[分析]** チェックボックスをオンにします。**[OK]** を押します。
5. データベース、**[スキーマ]**、**[Public]**の順に展開します。**[テーブル]**セクションの数字をメモします。これにより、復旧後にデータベースが正常に復元されたことを確認できます。
6. PostgreSQL Administrator を閉じ、管理者特権でのコマンドプロンプトを開きます。
7. このコマンドプロンプトで、PostgreSQL の bin ディレクトリに移動します。

   例: `cd "C:\Program Files(x86)\Acronis\Access\Common\PostgreSQL\9.3\bin"`
8. 次のコマンドを入力します: **`pg_dumpall --host localhost --port 5432 --username postgres --file alldbs.sql`**
   - バックアップのファイル名は **`alldbs.sql`** になります。これは PostgreSQL の bin ディレクトリに保存されます。別の場所に保存する必要がある場合は、上記のコマンド内でパスを使用できます。たとえば、コマンドの末尾を次のように変更します: **`--file D:\Backups\alldbs.sql`**
   - デフォルト以外のポートを使用している場合は、**`5432`** を正しいポート番号に変更します。

- デフォルトの PSQL 管理者アカウント **postgres** を使用していない場合は、上記コマンド内の **postgres** をご使用の管理者アカウント名に変更してください。
- この手順では、**postgres** ユーザーのパスワードを何回か入力するように求められる場合があります。そのたびにパスワードを入力して Enter キーを押してください。

注意: パスワードを入力しても、コマンドプロンプトウィンドウの視覚的な変化はまったくありません。

9. バックアップファイルを安全な場所にコピーします。
10. PostreSQL 自体はアップグレードされないため、Postgres サービスはシャットダウン**しない**でください。

その他の重要なコンポーネントのバックアップ

1. Tomcat の **conf** フォルダと **logs** フォルダをバックアップします。デフォルトでは **C:\Program Files (x86)\Acronis\Files Advanced\Common\apache-tomcat-<version>**にあります。

   注意: <version> は Files Advanced Tomcat インスタンスの正しいバージョンに置き換えて、**\apache-tomcat.70.0.70** のようにしてください。

2. **acronisaccess.cfg** ファイルをバックアップします。デフォルトでは **C:\Program Files (x86)\Acronis\Files Advanced\Access Server** にあります。
3. デフォルトで **C:\Program Files (x86)\Acronis\Files Advanced\Access Server\Web Application\WEB-INF** に存在するすべての **web.xml** ファイルをバックアップします。
4. **newrelic.yml** ファイルをバックアップします。このファイルの場所は保存した場所に依存します。New Relic 監視を使用していない場合は、このステップをスキップできます。

ゲートウェイサーバーのデータベースのバックアップ

1. すべての Files Advanced ゲートウェイサービスをオフにします。
2. ゲートウェイデータベースフォルダ（デフォルトで **C:\Program Files (x86)\Acronis\Files Advanced\Gateway Server\database**)に移動します。
3. **mobilEcho.sqlite3** ファイルのバックアップを作成します。

4. ゲートウェイサーバーごとにこれらのステップを繰り返します。

すべてのコンピュータ上のすべてのFiles Advancedサービスを停止します。

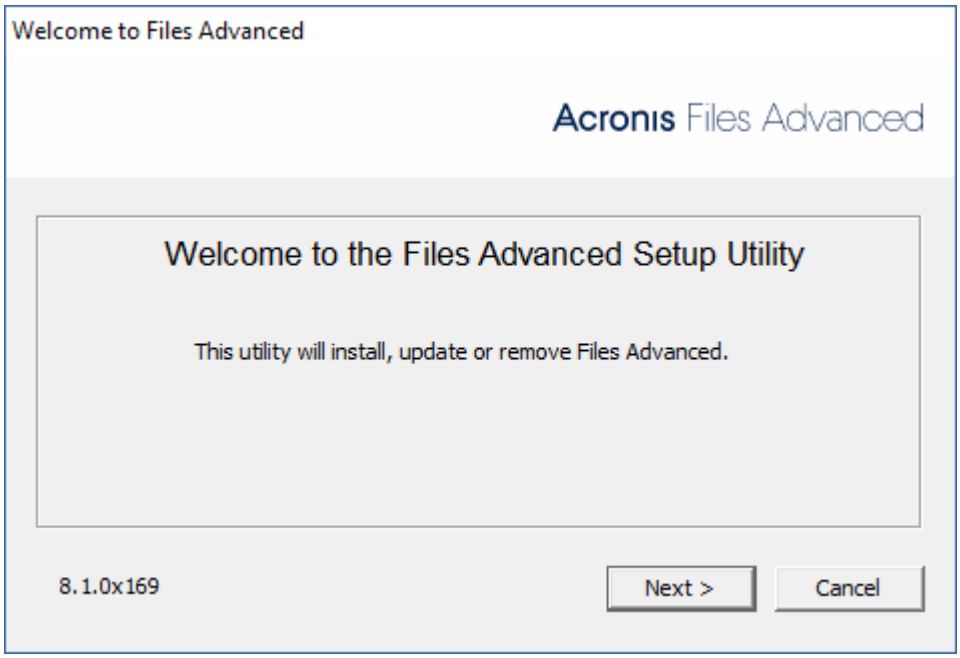
アップグレード前にすべての Files Advanced Tomcat サービスを停止することが不可欠です。実行したままにする必要がある PostgreSQL サービスを除いて、他のすべての Files Advanced サービスも停止することをお勧めします。

どこに存在するかに関係なく、まずファイルリポジトリをアップグレードします。

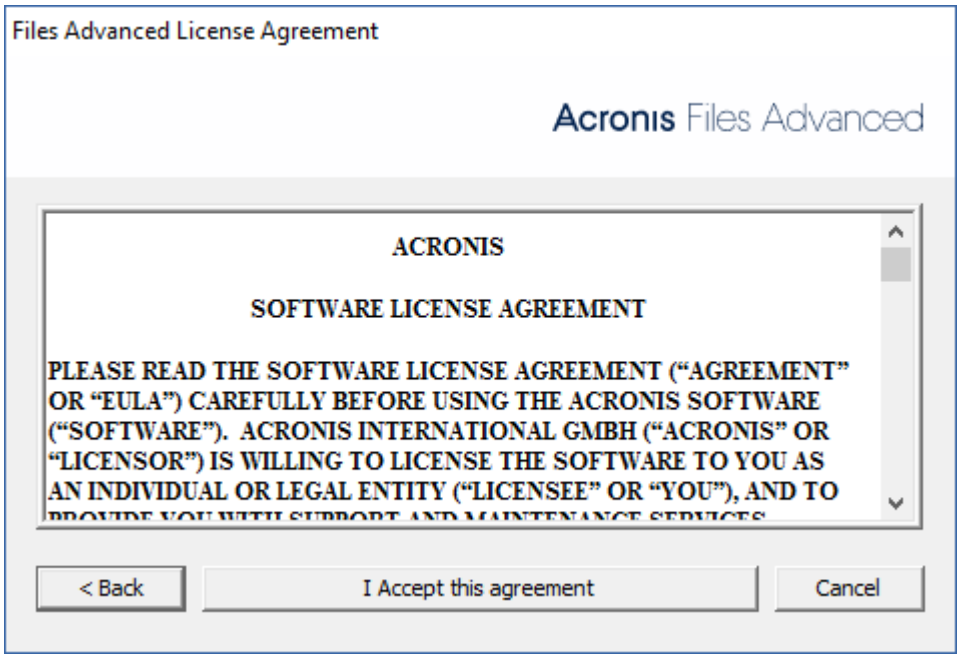
1. Files Advanced インストーラをファイルリポジトリコンポーネントが存在するコンピュータにコピーして実行します。

   注意: 複数のファイルリポジトリサービスを使用している場合は、他のコンポーネントに進む前に、すべてのリポジトリに対してこれらのステップを繰り返します。

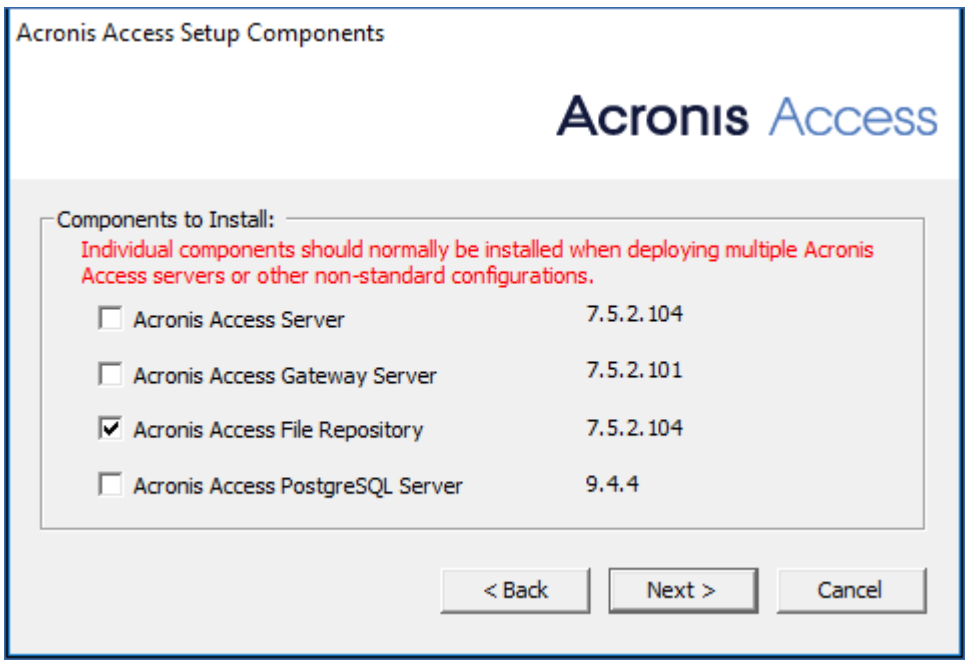
2. **ようこそ**画面で、**[次へ]** をクリックします。



3. 使用許諾契約に同意します。

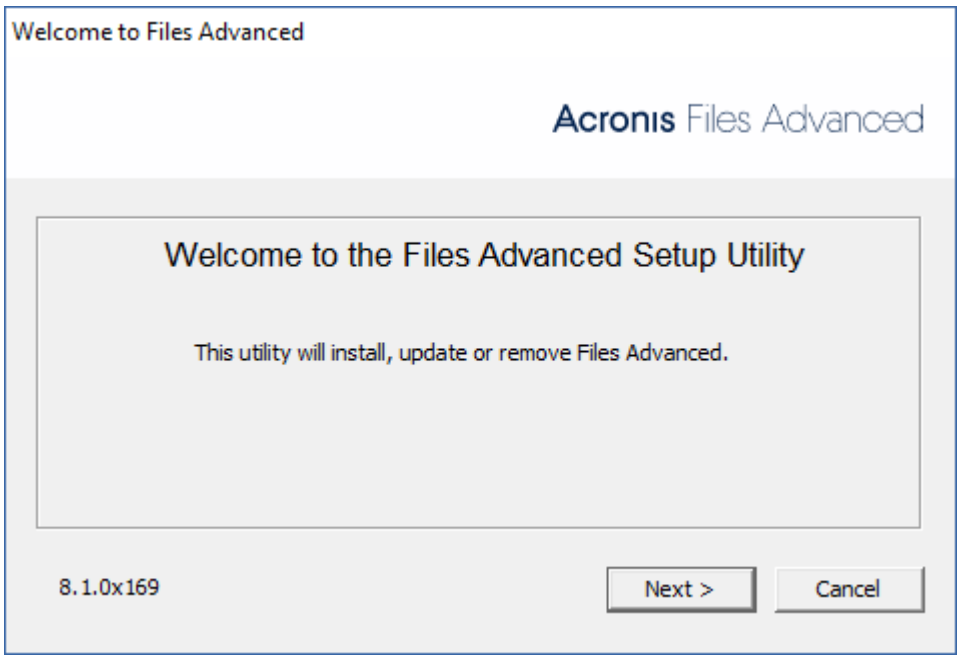


4. **[カスタム...]** を選択して、アップグレードする**Files Advanced ファイルリポジトリ**のみを選択します。

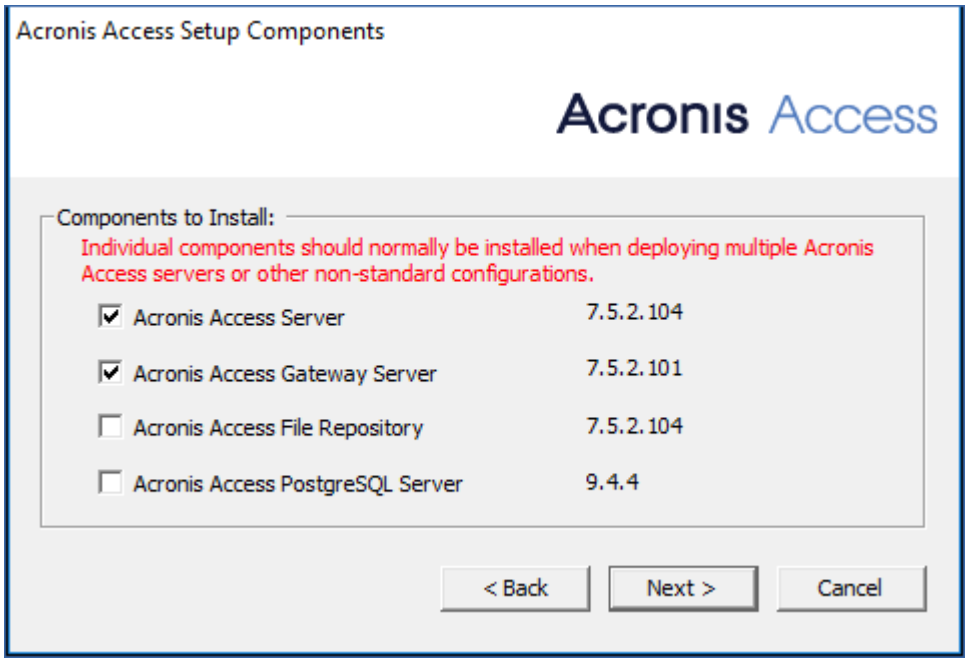


5. **[次へ]** をクリックして、インストールの内容を確認し、**[インストール]** をクリックします。
6. アップグレードが完了したら、**[終了]** をクリックします。設定ユーティリティが起動したら、**[OK]** をクリックします。
7. 対応するコンピュータ上の**プライマリ** Files Advanced Web サーバーのアップグレードに進みます。

1. Files Advanced Advanced インストーラを**プライマリ** Files Advanced Web サーバーコンピュータにコピーします。
2. **プライマリ**ノードで、Files Advanced インストーラを開始します。



3. ようこそ画面で **[次へ]** を押してから、**[カスタム]** を押します。これにより、他のインストールを必要とせず、既にコンピュータにインストール済みの必要なサービスのみをアップグレードすることができます。
4. アップグレードする Files Advanced サービスを選択します。Files Advanced Web サーバーと既にコンピュータ上に存在するすべてのコンポーネントだけを選択します。



注意: この製品のインストーラでは、PostgreSQL はアップデートされません。ご使用の PostgreSQL のバージョンをアップデートするには、アップデート処理の前にこの主題に関する記事 『230ページ 』を読み、アクロニスサポートにお問い合わせください。

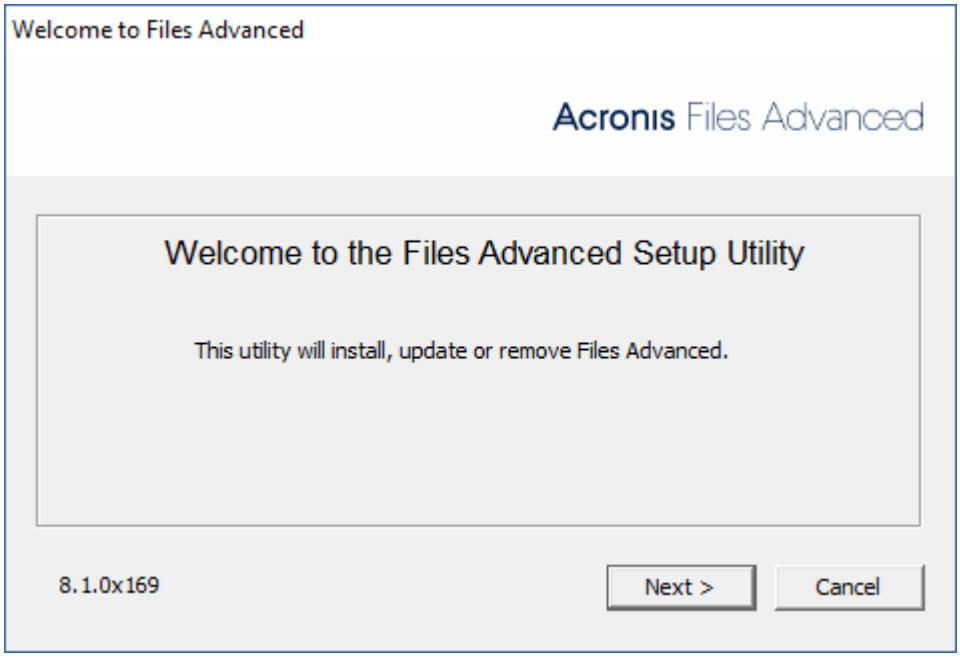
5. **[インストール]** を押してインストーラを終了し、**設定ユーティリティ**を起動します。

注意: 設定ユーティリティで設定を変更しないでください。設定を変更すると、構成に問題が生じる可能性があります。

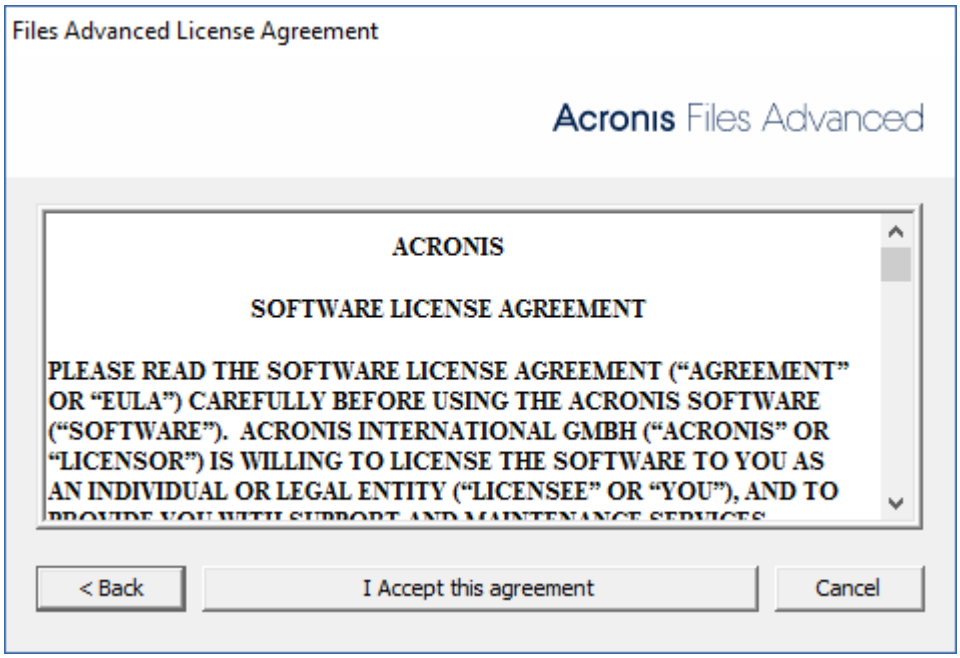
6. 設定ユーティリティですべての必要なサービスを開始して、データベース移行が終了したら、**プライマリ**サーバーで Files Advanced ウェブインターフェイスが想定どおりに動作することを確認します。ウェブブラウザが自動的に起動して、Files Advanced サーバーのログイン画面が表示されます。
7. 管理者としてログインし、設定が同じで、変更や問題がないことを確認します。
8. 他のコンポーネントのアップデート中は、Files Advanced のこのインスタンスを実行したままにします。

警告!: プライマリサーバーがバックアップされ、その正しい動作を確認するまでは、他の Files Advanced Tomcat サーバーをアップグレードまたは開始しないでください。

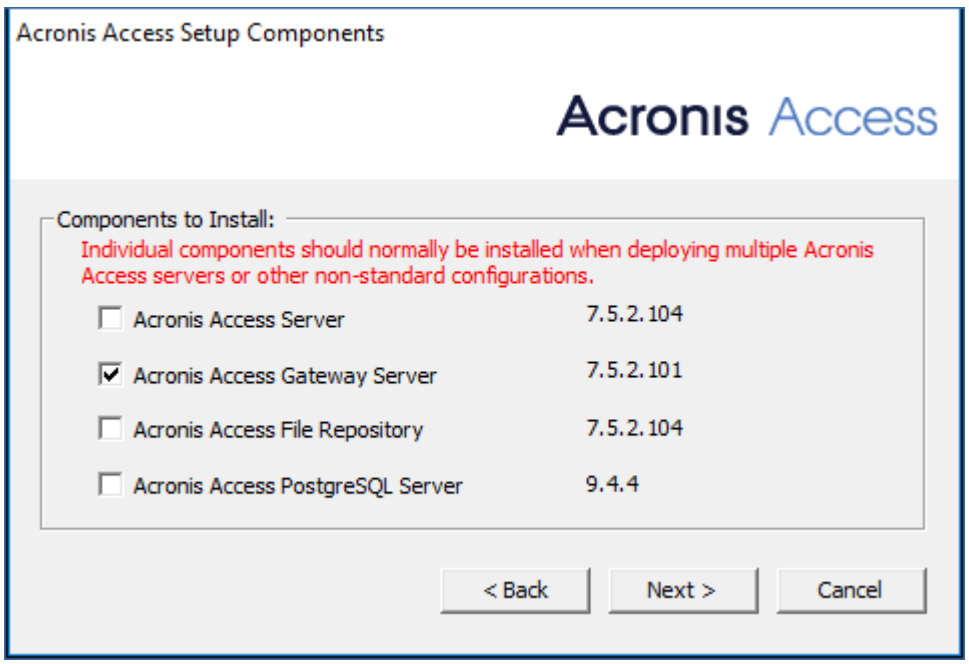
1. Files Advanced Advanced インストーラをゲートウェイサーバーのみを含むコンピュータにコピーして実行します。
2. ようこそ画面で、**[次へ]** をクリックします。



3. 使用許諾契約に同意します。



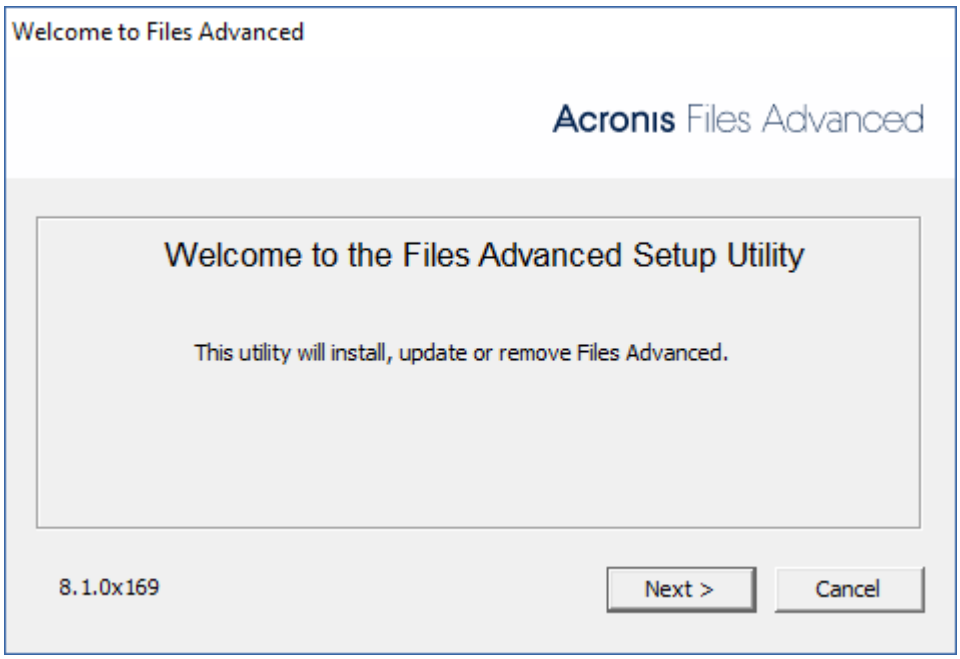
4. **[カスタム...]** を選択して、アップグレードする Files Advanced ゲートウェイサーバーのみを選択します。



5. **[次へ]** をクリックして、インストールの内容を確認し、**[インストール]** をクリックします。
6. アップグレードが完了したら、**[終了]** をクリックします。設定ユーティリティが起動したら、**[OK]** をクリックします。

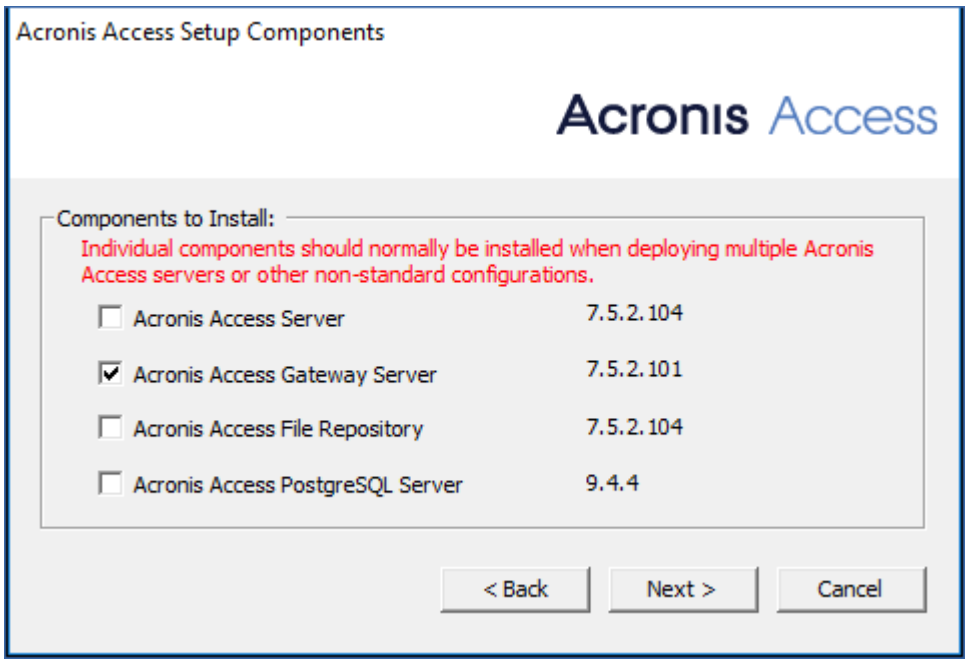
プライマリ Files Advanced ノード、すべてのファイル・リポジトリ・サーバー、およびすべてのゲートウェイサーバーのアップデートに成功したら、残りの Files Advanced サーバーのアップグレードに進みます。

1. アップグレード対象のノードに Files Advanced インストーラをコピーして実行します。

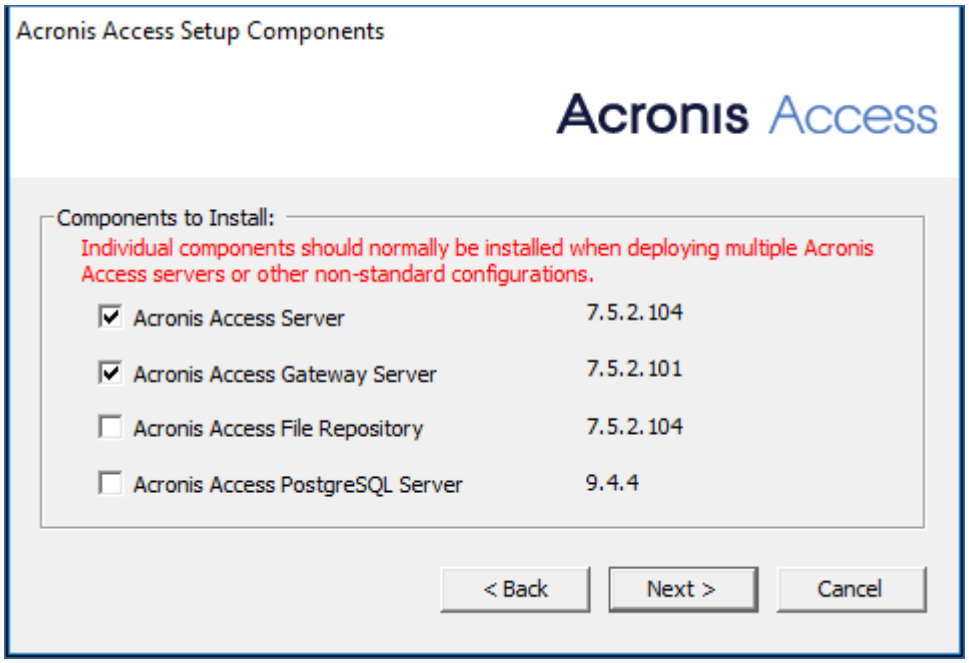


2. ようこそ画面で **[次へ]** を押してから、**[カスタム]** を押します。これにより、他のインストールを必要とせず、既にコンピュータにインストール済みの必要なサービスのみをアップグレードすることができます。
3. アップグレードする Files Advanced サービスを選択します。既にコンピュータに存在するサービスのみを選択します。

例: インストールされたゲートウェイサーバーが 1 台のみである場合には、インストーラではゲートウェイサーバーコンポーネントのみを選択します。



例: ゲートウェイサーバーとFiles Advanced サーバーが存在する場合は、両方を選択します。



注意: この製品のインストーラでは、PostgreSQL はアップデートされません。ご使用の PostgreSQL のバージョンをアップデートするには、アップデート処理の前にこの主題に関する記事 『230ページ 』を読み、アクロニスサポートにお問い合わせください。

4. **[インストール]** を押してインストーラを終了し、**設定ユーティリティ**を起動します。

注意: 設定ユーティリティで設定を変更しないでください。設定を変更すると、構成に問題が生じる可能性があります。

5. 設定ユーティリティですべての必要なサービスを開始した後に、このノードで Files Advanced コンポーネントが期待どおり動作することを確認します。

6 モバイル アクセス

このセクションのウェブ インターフェイスには、モバイル デバイス ユーザーに影響を与えるすべての設定と構成が含まれています。

セクションの内容

6.1 コンセプト

Files Advanced モバイルクライアントはサードパーティ製のサービスを利用するのではなく、直接サーバーに接続されるため、ユーザーは制御状態を維持します。Files Advanced サーバーは既存のファイルサーバーと同じネットワークにインストールできるため、iPad、iPhone、Windows、および Android の各デバイスからそのネットワーク上に配置されているファイルにアクセスできます。これらのファイルは通常、PC で Windows ファイル共有機能を使用して既に利用できるようになっているファイルや、Mac で Files Connect サーバーを使用して既に利用できるようになっているファイルと同じです。

クライアントは Active Directory のユーザー アカウントを使用して Files Advanced サーバーにアクセスします。Files Advanced 内で追加のアカウントを設定する必要はありません。AD 以外のユーザーにアクセス権を付与する必要がある場合に備えて、Files Advanced アプリは、Files Advanced が実行されている Windows サーバー上で構成されたローカルコンピュータアカウントを使用したファイルアクセスもサポートします。後に説明するクライアント管理機能には AD のユーザー アカウントが必要です。

導入の最小構成は、Files Advanced のデフォルトのインストールを実行する 1 台の Windows サーバーで構成されます。このデフォルトのインストールには、Files Advanced サーバーコンポーネントとローカル Files Advanced ゲートウェイサーバーが含まれます。

このシナリオでは、Files Advanced ユーザーがこの 1 台のファイルサーバーに接続して、モバイルデバイス上でクライアントを管理できるようになります。クライアント管理が不要な場合、データソースをローカルゲートウェイサーバーにセットアップでき、Files Advanced モバイルクライアントはこれらのデータソースにアクセスできますが、ユーザーがそのアプリケーション設定を管理します。

図 1. 単一の Files Advanced サーバーとローカルゲートウェイサーバー

任意の数のゲートウェイサーバーを後でネットワークに追加して、Access クライアントからのアクセスを設定できます。

注記: Files Advanced のインストールの詳細は、本書の「インストール 『27ページ 』」セクションに記載されています。ゲートウェイ サーバーとデータ ソースの構成は、「モバイル アクセス 『68ページ 』」のセクションで説明しています。

モバイルクライアントをリモート管理する場合、Files Advanced Management を使用して、Active Directory のユーザーまたはグループごとにポリシーを作成することができます。Files Advanced サーバーが 1 台だけ必要であり、ポリシーによって以下が可能になります。

- 一般的なアプリケーションの設定を構成する
- クライアント アプリケーションに表示されるサーバー、フォルダ、ホーム ディレクトリを割り当てる
- ファイルで実行できる操作を制限する
- Files Advanced ファイルを開くことができる他のサードパーティアプリを制限する
- セキュリティ要件（サーバー ログインの頻度、アプリケーション ロック パスワードなど)を設定する
- デバイスにファイルを保存する機能を無効にする
- Files Advanced ファイルを iTunes バックアップに含める機能を無効にする
- ユーザーのアプリケーション ロック パスワードをリモートからリセットする
- モバイルアプリのローカルデータと設定のリモートワイプを実行する

- その他の多くの設定およびセキュリティ オプション

一般的なネットワーク使用クライアント管理では、Files Advanced サーバーと Files Advanced Gateway サーバー コンポーネントがインストールされた 1 台のサーバーと、ファイル サーバーとして機能する複数の追加ゲートウェイ サーバーが含まれます。このシナリオでは、すべてのモバイルクライアントが、Files Advanced サーバーで管理されるように構成され、Files Advanced アプリケーションが起動されるたびにこのサーバーに接続して、設定変更をチェックし、必要な場合にはアプリケーションロックパスワードのリセットやリモートワイプコマンドを受け入れます。

Files Advanced のクライアントには、クライアントの管理ポリシーで、サーバーのリスト、共有ボリューム内の特定のフォルダ、およびホーム ディレクトリを割り当てることができます。これらのリソースは、Files Advanced アプリケーションに自動的に表示され、クライアント アプリケーションはファイル アクセスの必要性に応じてこれらのサーバーに直接接続します。

注記: クライアント管理の有効化と構成は、本書の「ポリシー 『70ページ 』」と「モバイル デバイス 『157ページ 』」の管理のセクションに記載されています。

図 2. 1 台のゲートウェイサーバー、1 台のゲートウェイサーバー+Files Advanced サーバー

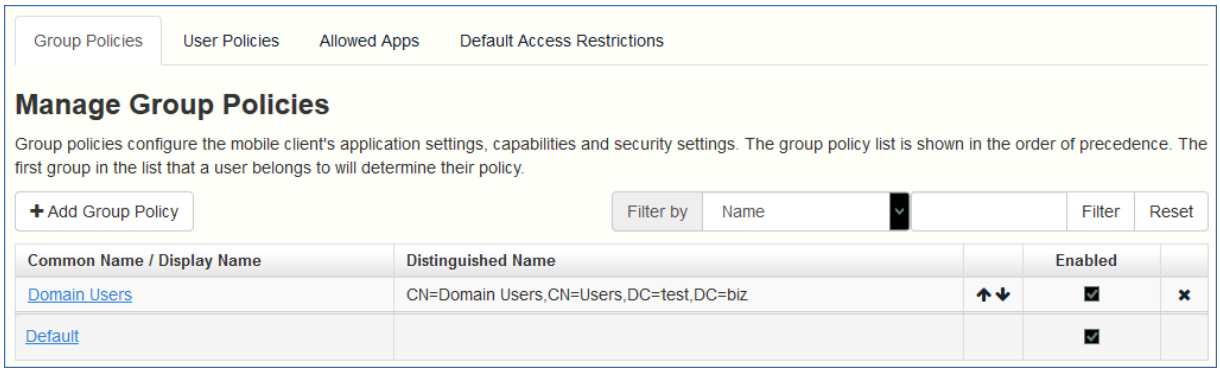
6.2 ポリシー

Files Advanced では、Active Directory のグループにポリシーを割り当てることができます。グループ ポリシーは通常、ほとんどすべてのクライアント管理要件を満たします。グループ ポリシーのリストは優先順位順に表示され、リスト内の一番上のグループの優先順位が最も高くなります。ユーザーが Files Advanced サーバーに接続したときには、ユーザーがメンバーになっている最も優先順位が高い 1 つのグループ ポリシーによって設定が決定されます。

ユーザー ポリシーはグループ ポリシーより優先順位が高いため、ユーザーが属するグループとは無関係に、ユーザーに特定の設定を実行されたときにユーザー ポリシーを使用します。ユーザー ポリシーは、グループ ポリシーより優先されます。

グループの管理に関するヒント

すべて、またはほとんどのユーザーに同じポリシー設定を適用する場合、**[デフォルト]** グループポリシーを使用できます。グループポリシーのメンバーではなく、明示的なユーザーポリシーがないすべてのユーザーは、**[デフォルト]** グループのメンバーになります。デフォルトでは、**[デフォルト]** グループが有効になっています。特定のユーザーのグループによる Files Advanced 管理へのアクセスを拒否する場合、それらのユーザーがどの設定済みグループ ポリシーのメンバにもなっていないことを確認します。ユーザー アカウントがいずれかのグループ ポリシーと一致しない限り、それらのユーザーは Files Advanced クライアント管理への登録を拒否されます。



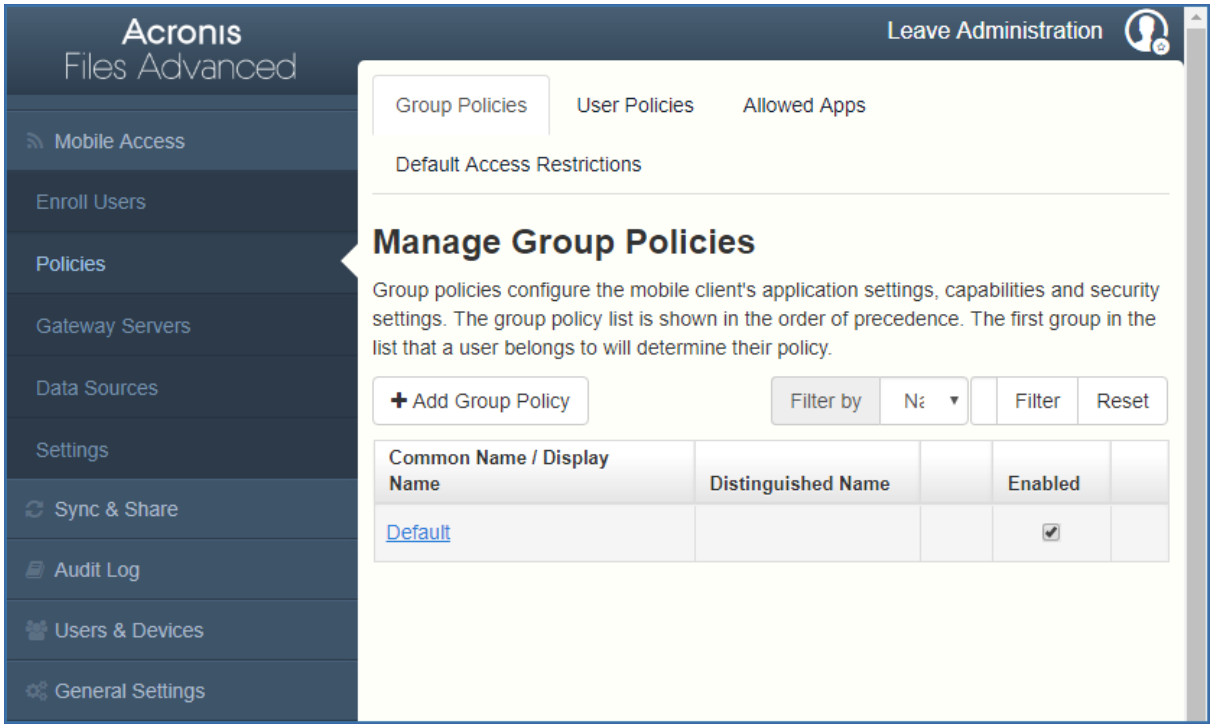
セクションの内容

6.2.1 新しいポリシーの追加

新しいグループ ポリシーを追加するには

1. **[グループ ポリシー]** タブを選択します。

2. 新しいグループ ポリシーを追加するには、**[新しいポリシーの追加]** ボタンをクリックします。これにより、**[新しいグループポリシーの追加]** ページが表示されます。

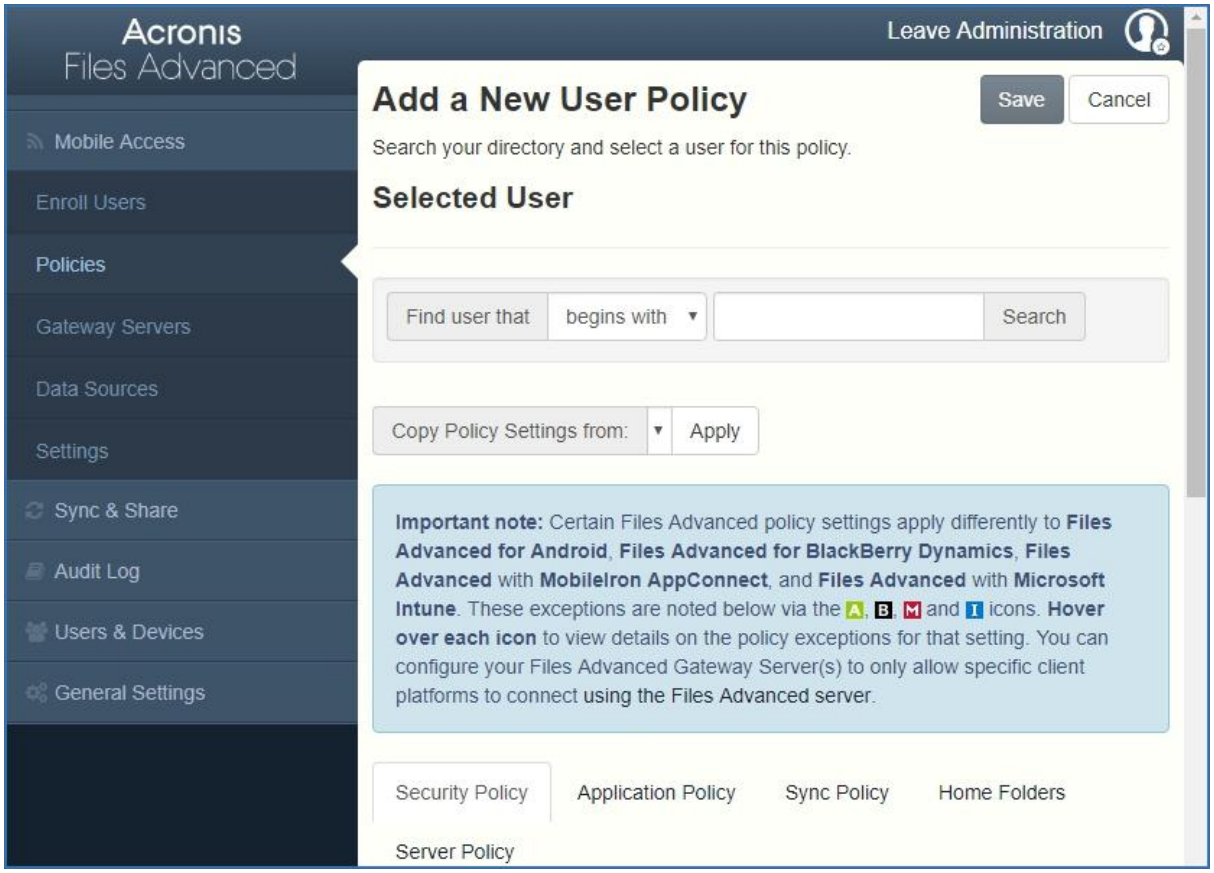


3. **[次に該当するグループを検索]** フィールドに、ポリシーを作成する対象の Active Directory グループ名の一部または全部を入力します。[**先頭の文字**] または [**含まれる文字**] 検索を Active Directory グループに対して実行できます。[先頭の文字] の検索は、[含まれる文字] の検索よりも短時間で完了します。
4. **[検索]** をクリックし、表示される結果でグループ名を見つけてクリックします。
5. [セキュリティ 『75ページ 』]、[アプリケーション 『79ページ 』]、[同期 『87ページ 』]、[ホーム フォルダ 『89ページ 』]、および [サーバー 『91ページ 』] の各タブで必要な設定をしてから [**保存**] をクリックします。

新しいユーザー ポリシーを追加するには

1. **[ユーザー ポリシー]** タブを選択します。

2. 新しいユーザー ポリシーを追加するには、**[新しいポリシーの追加]** ボタンをクリックします。これにより、**[新しいユーザーポリシーの追加]** ページが開きます。



3. **[ユーザーの検索]** フィールドに、ポリシーを作成する対象の Active Directory ユーザー名の一部または全部を入力します。[**先頭の文字**] または [**含まれる文字**] 検索を Active Directory ユーザーに対して実行できます。[先頭の文字] の検索は、[含まれる文字] の検索よりも短時間で完了します。
4. **[検索]** をクリックし、表示される結果でユーザー名を見つけてクリックします。
5. [セキュリティ 『75ページ 』]、[アプリケーション 『79ページ 』]、[同期 『87ページ 』]、[ホーム フォルダ 『89ページ 』]、および [サーバー 『91ページ 』] の各タブで必要な設定をしてから [**保存**] をクリックします。

6.2.2 ポリシーの変更

既存のポリシーをいつでも変更することができます。ポリシーの変更は、関連するモバイルアプリユーザーが次にモバイルアプリを起動したときにユーザーに適用されます。

接続要件

Files Advanced クライアントが、プロファイルのアップデート、リモート パスワードのリセット、およびリモート ワイプの指示を受け取るには、Files Advanced サーバーへのネットワーク アクセスが必要です。クライアントが、Files Advanced にアクセスする前に VPN に接続する必要がある場合は、管理コマンドを受け付ける前に VPN に接続する必要があります。

グループ ポリシーを変更するには、次の操作を行います。

1. トップ メニュー バーの **[グループ ポリシー]** オプションをクリックします。
2. 変更するグループをクリックします。
3. **[グループ ポリシーの編集]** ページで必要な変更を加え、**[保存]** を押します。
4. ポリシーを一時的に無効にするには、目的のグループの **[有効]** 列のチェックボックスをオフにします。この変更は即座に有効になります。
5. グループの優先順位を変更するには、[Manage Group Profiles] リストで上向きまたは下向きの矢印をクリックします。これにより、プロファイルのレベルが 1 つ上または下に移動します。

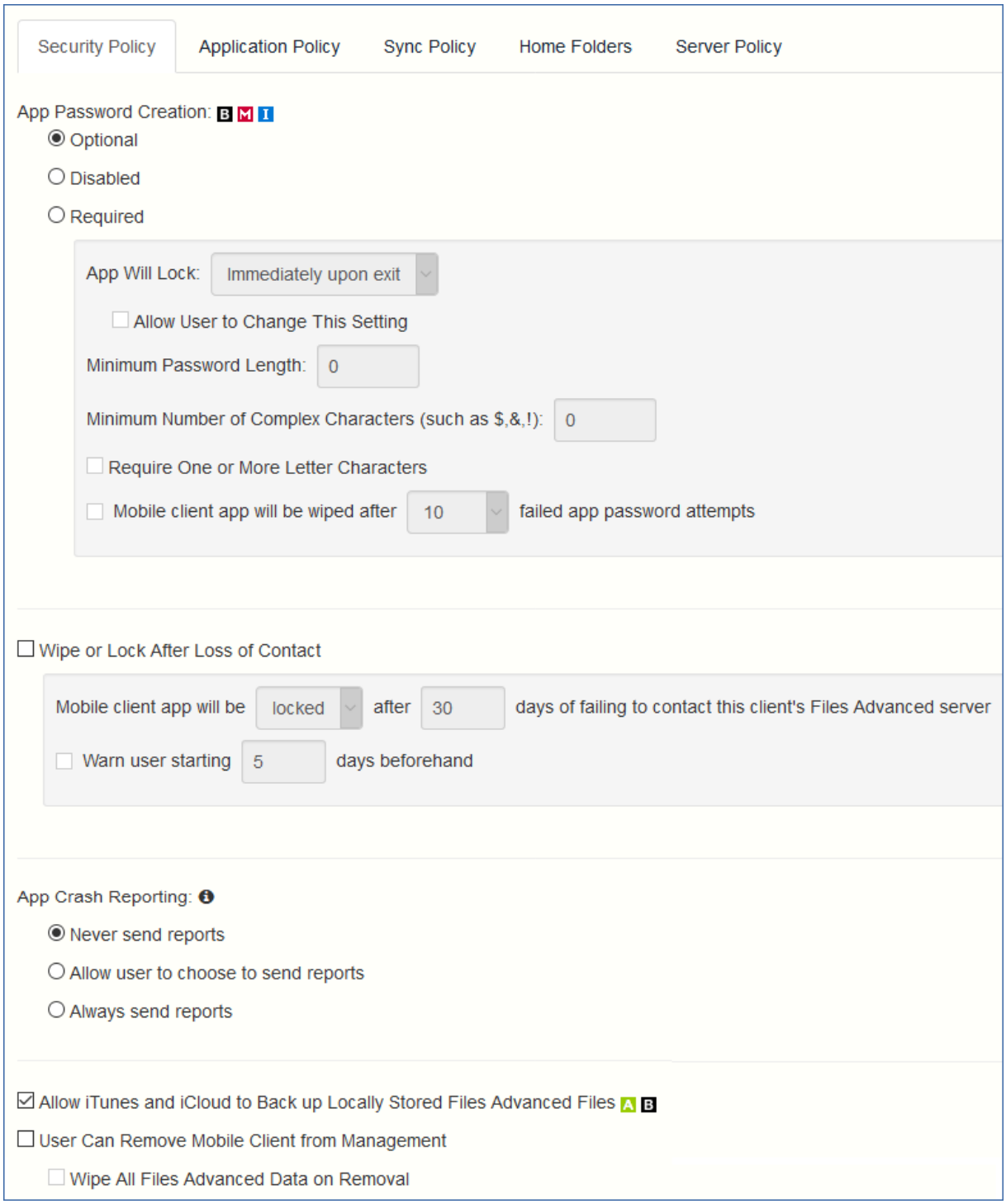
ユーザー ポリシーを変更するには、次の操作を行います。

1. **[ユーザー ポリシー]** タブを選択します。
2. 変更するユーザーをクリックします。
3. **[ユーザー ポリシーの編集]** ページで必要な変更を加え、**[保存]** を押します。
4. ポリシーを一時的に無効にするには、目的のユーザーの **[有効]** 列のチェックボックスをオフにします。すぐに無効化されます。

6.2.3 ポリシーの設定

セクションの内容

6.2.3.1 セキュリティ ポリシー



- **アプリのパスワードの作成**: モバイルアプリケーションにロックパスワードを設定して、そのパスワードを最初に入力しなければアプリケーションを起動できないようにすることができます。

- **オプション**: この設定は、アプリケーション ロック パスワードの設定をユーザーに強制しませんが、必要な場合にアプリケーションの **[設定]** メニューからパスワードを設定できます。
- **無効**: この設定は、アプリケーションの **[設定]** メニューからアプリケーション ロック パスワードを設定する機能を無効にします。これは、共有されているモバイルデバイスで、あるユーザーがアプリケーションパスワードを設定して他のユーザーがモバイルアプリを使用できなくなるという状況を防ぐ場合に役に立つことがあります。
- **必須**: この設定は、ユーザーがアプリケーション ロック パスワードを設定していない場合に、設定を強制します。オプションのアプリケーション パスワードの複雑さの要件およびパスワード試行失敗による消去の設定は、**[アプリのパスワードの作成]**を **[必須]** に設定した場合のみ適用されます。
  - **アプリのロックのタイミング**: アプリケーション パスワードの入力が免除される時間を設定します。ユーザーがデバイス上で Files Advanced モバイルアプリから別のアプリケーションに切り替えた後、この猶予時間が切れる前にこのモバイルアプリに戻る場合は、アプリケーションロックパスワードを入力する必要がなくなります。パスワードを毎回入力することを必須にするには、**[終了時]** を選択します。ユーザーがモバイルアプリの設定で **[アプリのロックのタイミング]** 設定を変更できるようにする場合は、**[ユーザーが設定を変更できるようにする]** を選択します。
  - **最低パスワード長**: アプリケーション ロック パスワードとして許可される最小文字数。
  - **最低限含めなければならない文字の種類の数**: アプリケーション ロック パスワードに必要な文字および数字以外の文字の最小数。
  - **1 つ以上の文字が必要**: アプリケーション パスワード内に 1 つ以上の文字が含まれるようにします。
  - **アプリのパスワードの試行を X 回失敗した場合、モバイルクライアントアプリをワイプする**: このオプションを有効にすると、指定した回数連続してアプリのパスワードの入力に失敗した場合、モバイルアプリの設定とデータがワイプされます。

- **接続がない場合にワイプまたはロックする**: 一定の日数にわたり Files Advanced サーバーへの接続が行われなかった場合、モバイルアプリを自動的にワイプまたはロックするには、この設定を有効にします。

  警告: 何らかの理由でアプリがサーバーへの認証に失敗した場合、サーバーが到達可能であったとしても、サーバーに接続しているとはみなされません。

  - 後でロックされたクライアントがサーバーに正常に接続した場合、自動的にロック解除されます。
  - クライアントが消去された場合、モバイルアプリに保存されているすべてのローカルファイルとクライアント管理ポリシーが削除され、すべての設定がデフォルトにリセットされます。消去されたクライアントがゲートウェイ サーバーにアクセスするには、管理に再登録する必要があります。
- **このクライアントの Files Advanced サーバーへのアクセスに X 日間失敗したらモバイル クライアント アプリをロックする/ワイプする**: 指定された日数の間にクライアントがこの Files Advanced サーバーに接続しない場合のデフォルトの操作を設定します。
- **[ ] 日前からユーザーに警告**: Mobile アプリでは、「接続がない」ためにワイプまたはロックが実行される日が近づいたときに、オプションでユーザーに警告することができます。これにより、ネットワーク接続を再び確立し、Mobile アプリが Files Advanced サーバーに接続して、ロックまたはワイプを防ぐ機会が得られます。

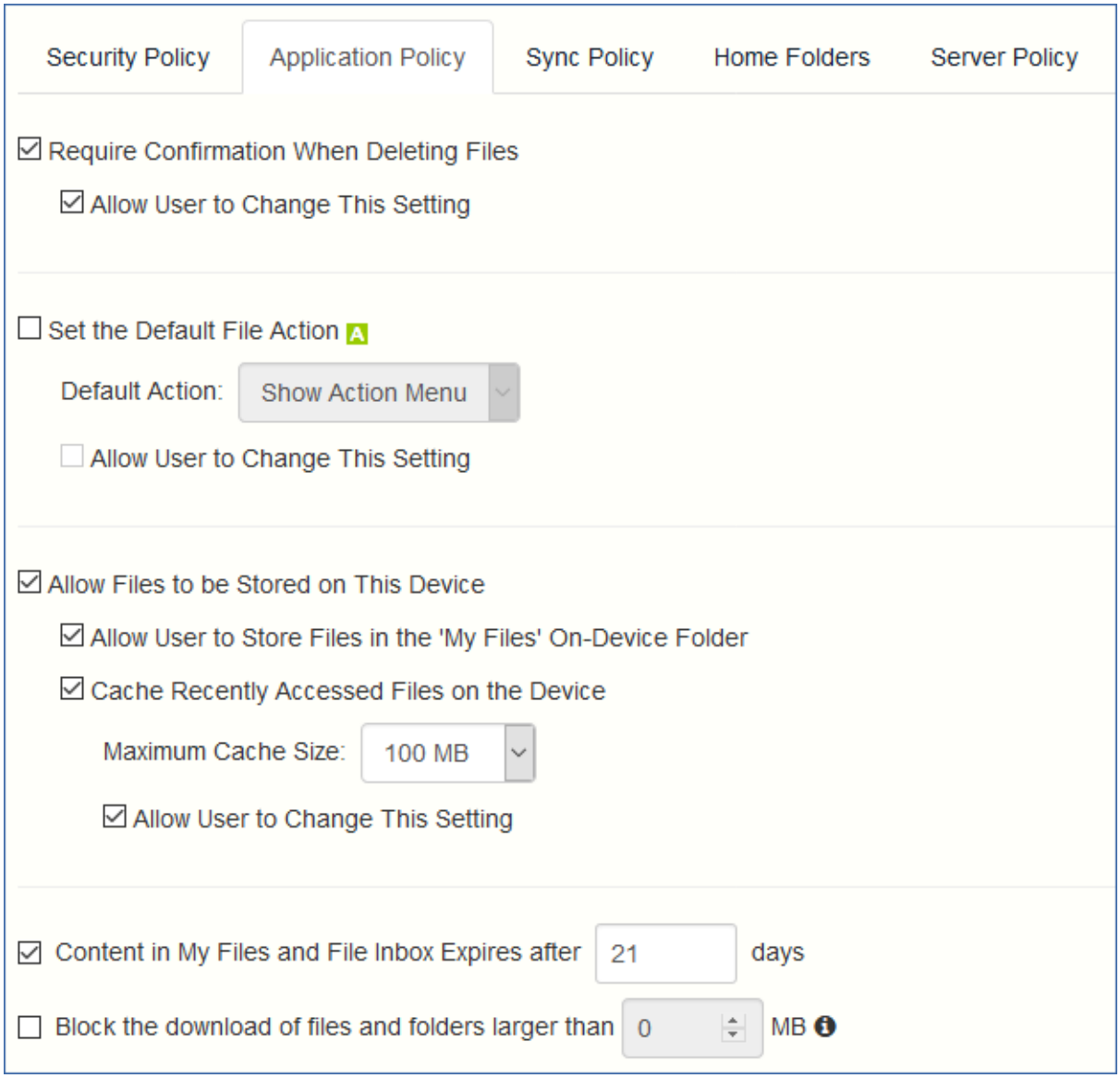
- **アプリのクラッシュレポート**: モバイルアプリがクラッシュした場合に Acronis にレポートを送信します。個人データまたは識別情報は送信されません。
  - **レポートを送信しない**
  - **レポート送信を許可する**
  - **常にレポート送信する**

- **iTunes と iCloud でローカルに保存された Files Advanced ファイルをバックアップできるようにする**: この設定が無効になっている場合、モバイルアプリは iTunes または iCloud へファイルをバックアップできません。これにより、Files Advanced のセ

キュリティで保護されたデバイスのストレージ内のファイルがバックアップにコピーされなくなります。

- **ユーザーがモバイル クライアントを管理から削除できる**: Files Advanced ユーザーが Files Advanced 内の自分の管理ポリシーをアンインストールできるようにする場合はこの設定を有効にします。このオプションを設定することで、アプリケーションの完全な機能が戻り、ポリシーによって変更された構成を復元することができます。
  - **削除されたときにすべての Files Advanced データをワイプする**: ユーザーによるポリシーの削除が有効になっている場合に、このオプションを選択できます。有効になっている場合、プロファイルが管理から削除された場合に、モバイルアプリケーション内にローカルで保存されているすべてのデータが消去されます。これにより、管理されていないクライアント上に会社のデータが存在しないようにすることができます。

6.2.3.2　アプリケーション ポリシー



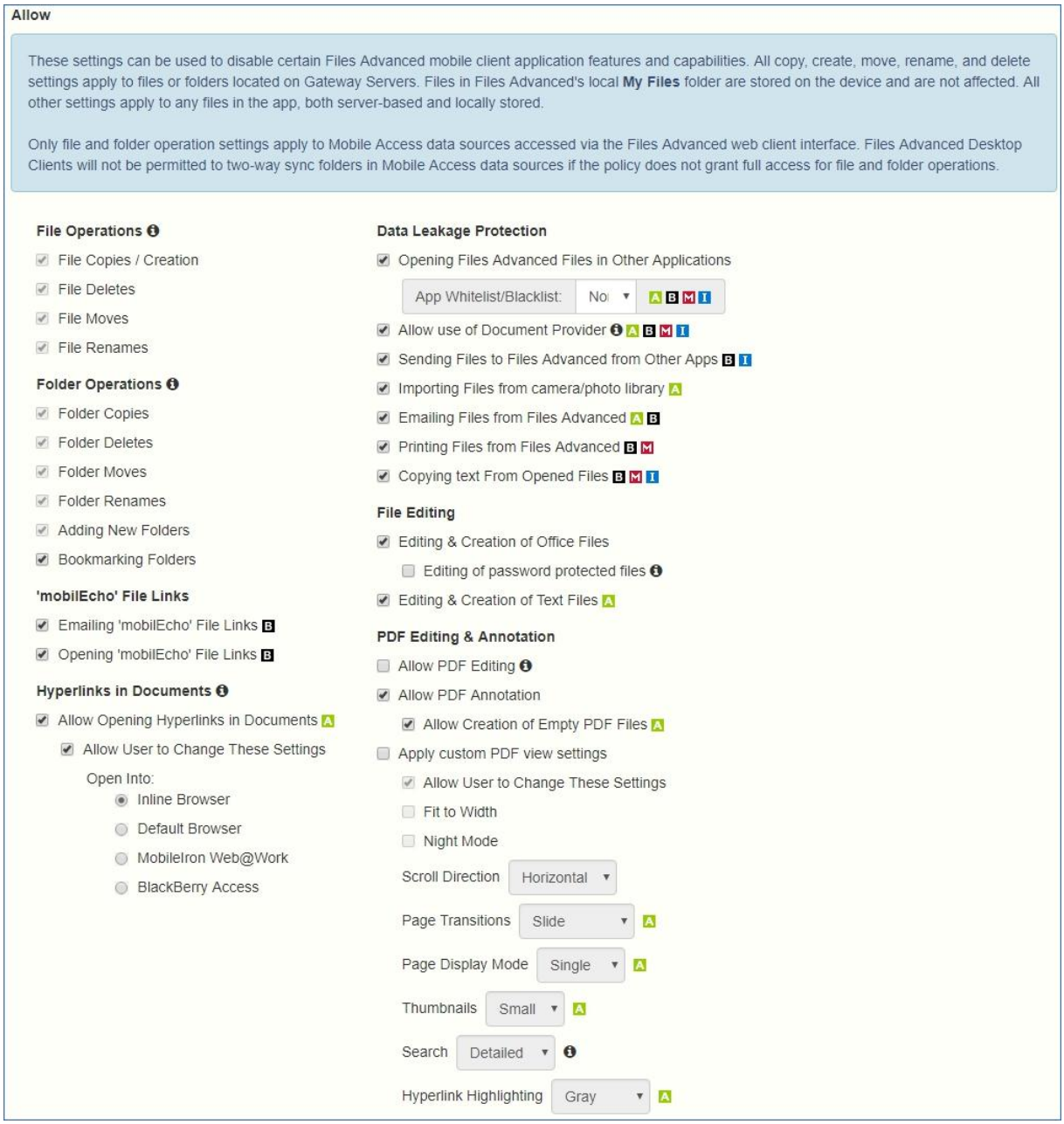
- **ファイルを削除するときに確認を必須にする**: 有効の場合、ユーザーはファイルを削除するたびに確認を求められます。ユーザーがこの設定を後で変更できるようにするには、**[ユーザーが設定を変更できるようにする]** を選択します。
- **デフォルトのファイル操作を設定する**: これは、ユーザーが Mobile アプリケーションでファイルをタップしたときの操作を決定するオプションです。このオプションが設定されていない場合、**[操作メニュー]** がクライアント アプリケーションのデフォルトとして使用されます。ユーザーがこの設定を後で変更できるようにするには、**[ユーザーが設定を変更できるようにする]** を選択します。
- **このデバイスにファイルを保存できるようにする**: この設定はデフォルトで有効になっています。有効の場合、ファイルをデバイス上（Files Advanced のサンドボックス化さ

れたストレージ内)に残すことができます。ファイルをローカルに保存するための機能（マイ ファイル フォルダ、同期フォルダ、最近アクセスしたファイルのキャッシュ)を有効または無効にするには、追加のポリシー設定が必要です。このオプションが無効な場合、デバイスにはファイルが保存されません。これにより、デバイスの紛失や盗難の際、会社のデータがデバイスに残っていないことを保証できます。この設定が無効な場合、ユーザーはファイルを保存または同期してオフラインで使用すること、ファイルをキャッシュしてパフォーマンスを向上させること、[他のアプリで開く] 機能を使用して、別のアプリケーションから Files Advanced モバイル クライアントにファイルを送信することができません。

- **ユーザーがデバイスの 'マイ ファイル' フォルダにファイルを保存できるようにする**: 有効の場合、ファイルを 'マイ ファイル' フォルダにコピーして、オフラインでのアクセスや編集が可能になります。これは Files Advanced のデバイス上にあるストレージ サンドボックス内の汎用ストレージ エリアです。
- **最近アクセスしたファイルをデバイスにキャッシュする**: 有効の場合、最近アクセスしたサーバーベースのファイルが、デバイスのローカル キャッシュに保存され、もう一度アクセスしたときに変更されていなければ、使用できるようになります。これは、パフォーマンスの向上と帯域幅の節約に役立ちます。**[最大キャッシュ サイズ]** を指定し、後でユーザーがこの設定を変更できるようにしておくこともできます。

- **[マイファイル] と [ファイル受信トレイ] のコンテンツは、X 日後に有効期限が切れます**: このオプションが有効の場合、設定した日数が経過すると、**マイファイル**内のファイルがデバイスから削除されます。
- **X MB より大きいファイルおよびフォルダのダウンロードをブロックする**: このオプションを有効にすると、設定された容量より大きいファイルやフォルダは、モバイルアプリでダウンロードされなくなります。

許可



これらの設定を使用して特定の Mobile アプリケーションの機能を無効にすることができます。コピー、作成、移動、名前の変更、および削除のすべての設定は、ゲートウェイ サーバーに置かれているファイルまたはフォルダに適用されます。モバイル クライアントのローカルの [マイ ファイル] フォルダ内にあるファイルはデバイスに保存され、影響を受けません。他のすべての設定は、サーバーベースかクライアント上にローカルに保存されているかを問わず、Files Advanced のすべてのファイルに適用されます。

ファイルの操作

- **ファイルのコピー/作成**: このオプションを無効にすると、ユーザーは他のアプリケーションや iPad 写真ライブラリからゲートウェイ サーバーにファイルを保存できません。また、ゲートウェイ サーバーに新しいファイルやフォルダをコピーまたは作成することもできません。この設定は、クライアントにファイルの作成を許可する NTFS アクセス権よりも優先されます。
- **ファイルの削除**: このオプションを無効にすると、ゲートウェイ サーバーからファイルを削除できなくなります。この設定は、クライアントにファイルの削除を許可する NTFS アクセス権よりも優先されます。
- **ファイルの移動**: このオプションを無効にすると、ゲートウェイサーバー上のあるロケーションから別のロケーションへ、またはゲートウェイサーバーから Mobile アプリケーションのローカル [マイファイル] ストレージへファイルを移動することができなくなります。この設定は、クライアントにファイルまたはフォルダの移動を許可する NTFS アクセス権よりも優先されます。
- **ファイル名の変更**: このオプションを無効にすると、ゲートウェイ サーバーのファイルの名前が変更できなくなります。この設定は、クライアントにファイル名の変更を許可する NTFS アクセス権よりも優先されます。

フォルダの操作

- **フォルダのコピー**: このオプションを無効にすると、ユーザーはゲートウェイ サーバーでフォルダをコピーしたり、ゲートウェイ サーバーにフォルダをコピーすることができません。この設定は、クライアントにフォルダの作成を許可する NTFS アクセス権よりも優先されます。この設定を有効にするには、**[ファイルのコピー/作成]** を有効にする必要があります。
- **フォルダの削除**: このオプションを無効にすると、ゲートウェイ サーバーからフォルダを削除できなくなります。この設定は、クライアントにフォルダの削除を許可する NTFS アクセス権よりも優先されます。
- **フォルダの移動**: このオプションを無効にすると、ゲートウェイサーバー上のあるロケーションから別のロケーションへ、またはゲートウェイサーバーから Files Advanced モバイルアプリケーションのローカル [マイ ファイル] ストレージへフォルダを移動す

ることができません。この設定は、クライアントにファイルまたはフォルダの移動を許可する NTFS アクセス権よりも優先されます。この設定を有効にするには、**[フォルダのコピー]** を有効にする必要があります。

- **フォルダ名の変更**: このオプションを無効にすると、ゲートウェイ サーバーのフォルダの名前を変更できなくなります。この設定は、クライアントにフォルダ名の変更を許可する NTFS アクセス権よりも優先されます。
- **新しいフォルダを追加**: このオプションを無効にすると、ユーザーはゲートウェイ サーバーで新しい空のフォルダを作成できません。
- **フォルダのブックマーク**: このオプションを無効にすると、ユーザーはデバイス上またはサーバー上の Files Advanced フォルダにすばやくアクセスするためのブックマークを登録することができなくなります。

'mobilEcho' ファイルのリンク

- **'mobilEcho' ファイルのリンクを電子メールで送信する**: このオプションを無効にすると、ユーザーは Files Advanced ファイルまたはフォルダへの mobilEcho:// URL を、他の Files Advanced ユーザーに送信することができなくなります。このようなリンクは、受信者が Files Advanced モバイル クライアントをインストールしており、サーバーを構成しているデバイス、またはリンクロケーションへのアクセス権を持つフォルダを割り当てたデバイスで開いた場合のみ正常に動作します。また、このユーザーには、アイテムを読み取るための、ファイル/フォルダ レベルのアクセス権も必要です。
- **'mobilEcho' ファイルのリンクを開く**: このオプションを無効にすると、ユーザーは Files Advanced ファイルまたはフォルダへの mobilEcho:// URL を開くことができなくなります。

ドキュメント内のハイパーリンク

- **ドキュメント内のハイパーリンクの参照を許可する**: 有効にすると、ドキュメント内にあるすべてのハイパーリンクを開くことができます。
  - **ユーザーが設定を変更できるようにする**: 有効にすると、設定に基づいて機能を有効化、無効化できます。

他のアプリで開く:

- **インラインブラウザ**: ハイパーリンクは、Files Advanced アプリで直接開かれます。
- **デフォルトのブラウザ**: ハイパーリンクは、デバイスで選択されたデフォルトのブラウザで開かれます。
- **MobileIron Web@Work**: ハイパーリンクは、MobileIron Web@Work アプリで開かれます。
- **[Blackberry Access]**: ハイパーリンクが BlackBerry Access アプリで開かれます。

データ漏えいの防止

- **Files Advanced ファイルを別のアプリケーションで開く**: このオプションを無効にすると、Mobile アプリケーションに **[他のアプリで開く]** ボタンが表示されなくなります。したがって、Files Advanced 内のファイルを別のアプリケーションで開くことができなくなります。別のアプリケーションで開かれたファイルは、そのアプリケーションのデータ ストレージ エリアにコピーされ、Files Advanced では制御できなくなります。
  - **アプリ ホワイトリスト/ブラックリスト**: デバイスで Files Advanced ファイルを読み込むことのできるサード パーティ アプリケーションを制限するために、あらかじめ定義されているホワイトリストまたはブラックリストを選択します。ホワイトリストまたはブラックリストを作成するには、トップ メニュー バーの **[許可されたアプリ]** をクリックします。
- **ドキュメントプロバイダの使用を許可**: モバイルデバイスが Files Advanced のドキュメントプロバイダ拡張機能を使用できるようにします。ドキュメントプロバイダ拡張機能は、特定の設定の影響を受ける場合があります。
  a. クライアントが古いサーバーで管理される場合、**[Files Advanced ファイルを別のアプリケーションで開く]** が**無効**に設定されるか、**有効**なホワイトリスト/ブラックリストがある限り、ドキュメントプロバイダ拡張機能は有効になります。
  b. クライアントが新しいサーバー（バージョン 7.3.1 以降)で管理され、**[ドキュメントプロバイダの使用を許可]** が有効に設定されている場合、**[Files Advanced ファイ**

ルを別のアプリケーションで開く] が**無効**に設定されるか、**有効**なホワイトリスト/ブラックリストがある場合でも、ユーザーは他のアプリとファイルを共有することができます。特別にブロックされたファイルも含む。

c. **[ドキュメントプロバイダの使用を許可]** が有効に設定されているが、ファイルの作成が無効である場合には、ドキュメントプロバイダ拡張は機能するものの、ユーザーは他のアプリから Files Advanced データソースにファイルを保存することができません。

- **他のアプリケーションから Files Advanced にファイルを送信する**: このオプションを無効にすると、Mobile アプリケーションは、別のアプリケーションの **[他のアプリで開く]** 機能から送信されたファイルを受け入れなくなります。
- **カメラまたは写真ライブラリからファイルをインポートする**: 有効にすると、写真およびビデオをデバイスの写真ライブラリから Files Advanced に直接インポートできます。
- **Files Advanced からファイルを電子メールで送信する**: このオプションを無効にすると、Mobile アプリケーションに **[ファイルを電子メールで送信]** ボタンが表示されなくなります。したがって、Files Advanced からファイルを電子メールで送信することができなくなります。

  注意: Android プラットフォームには、無効にできる組み込みの電子メールアプリケーションや機能がありません。そのため、電子メールにファイルを移動できないようにするには、[他のアプリで Files Advanced ファイルを開く] を無効にする必要があります。

- **Files Advanced からファイルを印刷する**: このオプションを無効にすると、Mobile アプリケーションに **[印刷]** ボタンが表示されなくなります。したがって、Files Advanced でファイルを印刷することができなくなります。
- **開いているファイルからテキストをコピーする**: このオプションを無効にすると、ユーザーは、モバイルアプリで開いている文書からテキストを選択して、コピー/貼り付け操作を行うことができません。これにより、別のアプリケーションへのデータのコピーを防ぐことができます。

ファイルの編集

- **Office ファイルの編集と作成**: このオプションを無効にすると、統合されている SmartOffice エディタで文書を編集できなくなります。

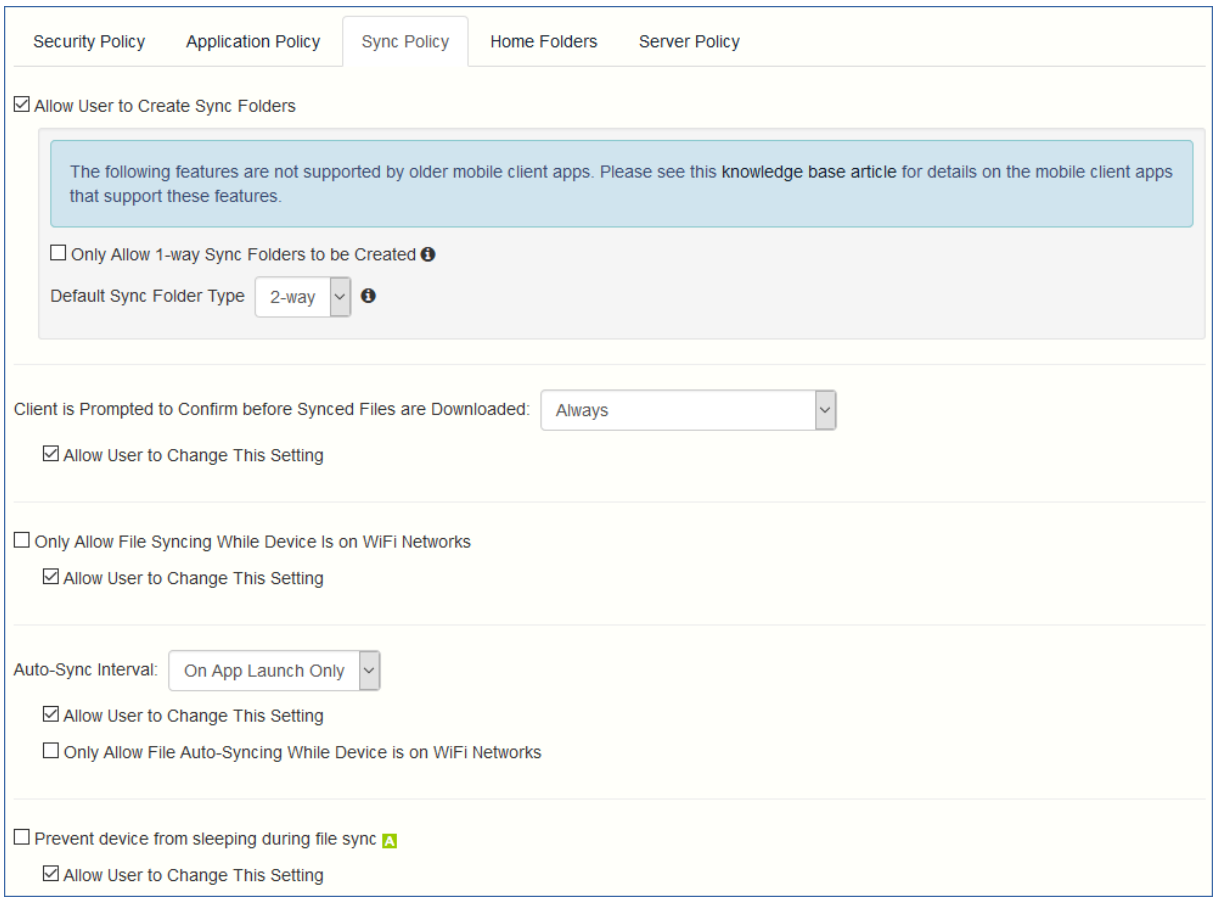
- **パスワードで保護されたファイルの編集**: このオプションを無効にすると、ユーザーはパスワードで保護されたファイルを編集できなくなります。
- **テキストファイルの編集と作成**: このオプションを無効にすると、ユーザーは組み込みのテキストエディタを使用して.txt ファイルを編集できなくなります。

PDF の編集と注釈

- **PDF の編集を許可**: この設定が有効な場合、ユーザーはページの新規作成、ファイルの複製、コピーと貼り付け、並べ替え、回転、削除、選択したページのサブセットからの新しいドキュメントの作成など、多くの PDF 編集機能を利用できるようになります。
- **PDF の注釈を使用できるようにする**: このオプションを無効にすると、モバイル アプリで PDF に注釈を付けることができなくなります。
  - **空の PDF ファイルの作成を許可する**: 有効にすると、注釈作成用の空の PDF ファイルを作成できます。
- **PDF のカスタム表示設定を適用する**: このオプションを有効にすると、すべてのユーザーおよびすべての PDF に、すべてのサブ設定が適用されます。
  - **ユーザーが設定を変更できるようにする**: 有効にすると、ユーザーは自分の PDF 表示設定を変更できるようになります。
  - **[幅に合わせる]**: 有効にすると、デバイス画面の幅に合わせてページのサイズが変更されます。
  - **[ナイトモード]**: 有効にすると、薄暗い場所での表示が快適になるように、デバイスでナイトモードカラースキームが使用されます。
  - **[スクロール方向]**: ページを縦にスクロールするか横にスクロールするかを選択できます。
  - **[ページトランジション]**: トランジションの視覚効果を選択できます。**[スライド]**: 単にページが変更されます。**[スクロール]**: ページが 1 つにつながっているかのようにスクロールされます。**[カール]**: ページが本のようにめくられます。
  - **[ページ表示モード]**: PDF を 2 ページ表示にするか単ページ表示にするかを選択できます。

- **[サムネイル]**: PDF を開いたときの、ページのサムネイルサイズを設定します。**[小]**、**[大]**、**[なし]**から選択できます。
- **[検索]**: 組み込みの PDF ビューアによって提供される検索結果の表示形式を設定します。3 種類の検索結果の表示形式があります。
  - **[シンプル]**: 結果がハイライト表示され、矢印アイコンでスクロールできます。
  - **[詳細]**: すべての結果がドロップダウンリストに表示され、タップして参照できます。
  - **[ダイナミック]**: 検索結果表示形式を iPhone では **[シンプル]** に設定し、iPads では **[詳細]** に設定します。
- **[ハイパーリンクハイライト]**: ハイパーリンクのハイライト表示カラーを選択できます。**[無効]**を選択してハイライトを無効にすることもできます。

6.2.3.3 同期ポリシー

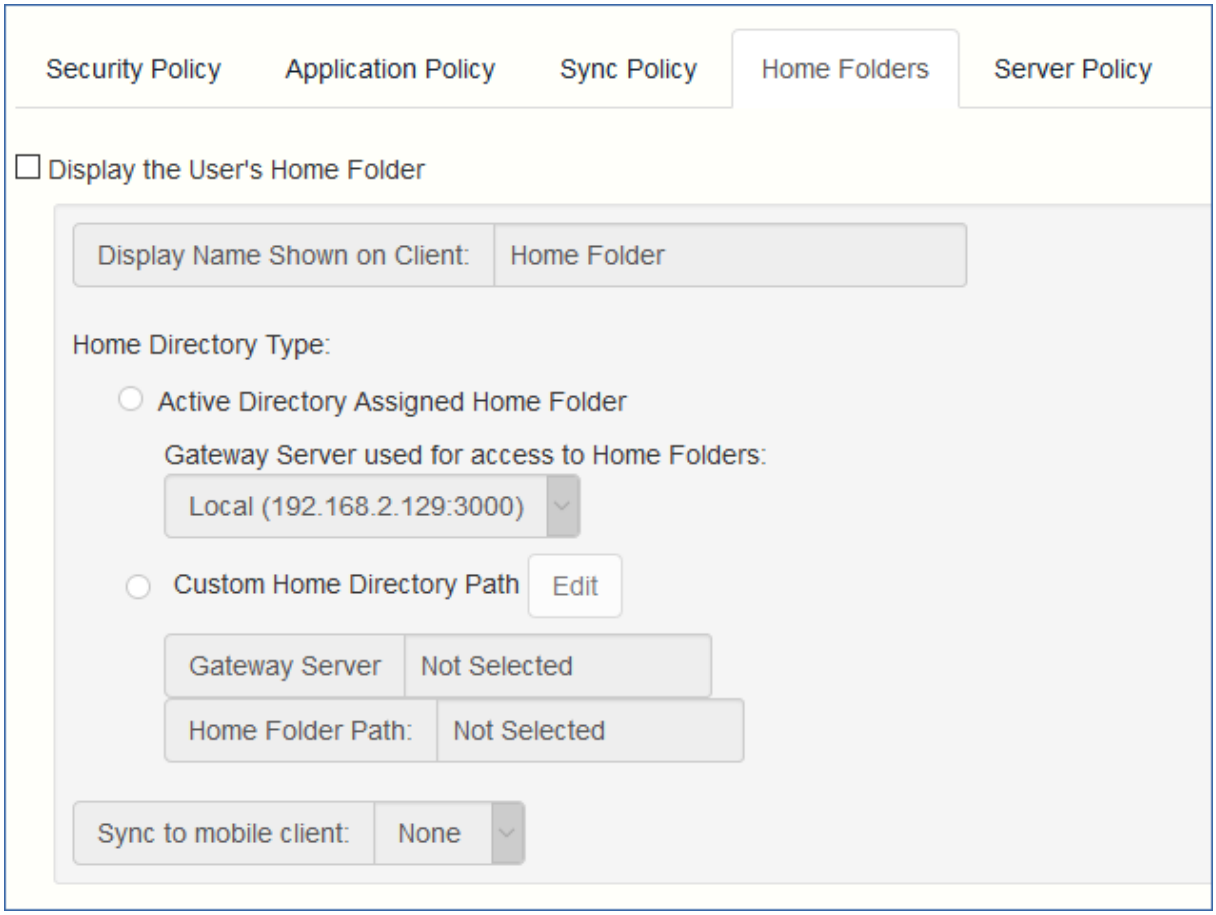


- **ユーザーに同期フォルダの作成を許可:** ユーザーが独自の同期フォルダを作成することを許可します。

- **一方向同期フォルダのみ作成を許可する**: ユーザーは一方向同期フォルダのみ作成できます。
- **デフォルトの同期フォルダタイプ**: デフォルトの同期フォルダタイプとして、一方向または双方向のいずれかを設定します。

- **同期ファイルがダウンロードされる前にクライアントに確認を求めるメッセージを表示**: 同期されたフォルダ内のファイルをダウンロードする前にユーザーが確認する必要がある状況の条件を選択します。オプションは、**[常に]**、**[携帯ネットワーク使用時のみ]**、**[確認しない]** です。**[ユーザーが設定を変更できるようにする]** が有効な場合、クライアントは確認オプションを変更できます。
- **デバイスが WiFi ネットワークに接続されている場合のみファイルの同期を許可する**: このオプションを有効にすると、Files Advanced では携帯接続を介したファイルの同期が許可されません。**[ユーザーが設定を変更できるようにする]** が有効な場合、クライアントは WiFi ネットワーク上にいる間、自動ファイル同期を有効または無効にできます。
- **自動同期間隔**: このオプションを有効にすると、Files Advanced は自動同期を**設定しない**か、**アプリ起動時のみ**に実行するか、さまざまな**時間間隔**で実行します。
  - **ユーザーが設定を変更できるようにする**: このオプションが有効になっている場合は、ユーザーは Files Advanced モバイルアプリから時間間隔を変更できます。
  - **デバイスが WiFi ネットワークに接続されている場合のみファイルの自動同期を許可する**: このオプションが有効になっている場合、ユーザーが WiFi に接続していなければ自動同期は行われません。
- **ファイル同期中のデバイスのスリープを許可しない**: この設定を有効にした場合、ファイル同期の実行中にロックやスリープが起こりません。**[ユーザーが設定を変更できるようにする]** が有効な場合、クライアントは確認オプションを変更できます。

6.2.3.4　ホームフォルダ



- **ユーザーのホームフォルダを表示する**: このオプションを選択すると、ユーザーの個人用ホームディレクトリが Mobile アプリに表示されます。
  - **クライアントに表示する表示名**: Mobile アプリでのホームフォルダ項目の表示名を設定します。**%USERNAME%**ワイルドカードを使用して、表示されるフォルダ名にユーザーのユーザー名を含めることができます。

注意: その他のデータソースタイプでは、**%USERNAME%**ワイルドカードを使用してユーザーのユーザー名を表示することはできません。Active Directory で割り当てられたホームフォルダのみで使用できます。

  - **Active Directory が割り当てられたホームフォルダ**: Mobile アプリに表示されるホームフォルダから、AD アカウントプロファイルで定義されたサーバー/フォルダのパスにユーザーが接続されます。ホーム フォルダには、選択したゲートウェイを介してアクセスすることができます。
  - **カスタムホームディレクトリのパス**: Mobile アプリに表示されるホームフォルダから、この設定で定義されたサーバーおよびパスにユーザーが接続されま

す。**%USERNAME%**ワイルドカードを使用して、ユーザー名をその他のデータソースタイプのホームフォルダのパスに含めることができます。%USERNAME% は大文字にする必要があります。

- **モバイルクライアントへの同期**: このオプションにより、ホームディレクトリの同期の種類が選択されます。

注意: このオプションは、ユーザーのホーム フォルダとデスクトップ クライアントとの同期機能には影響**しません**。

6.2.3.5 サーバー ポリシー

- **このポリシーによって割り当てられるリソースの必要なログイン頻度**: このポリシーによって割り当てられたサーバーにユーザーがログインする必要がある頻度を設定します。
  - **1 回のみ、将来のセッション用に保存する**: ユーザーは管理サーバーに最初に登録するときにパスワードを入力します。このパスワードは保存され、その後に開始するすべてのファイル サーバーへの接続で使用されます。

- **セッションごと**: Files Advanced モバイルの起動後、ユーザーは、最初のサーバーに接続するときにパスワードの入力が求められます。ユーザーは、Files Advanced モバイルアプリケーションから移動するまで、パスワードを再入力せずに追加のサーバーに接続することができます。Files Advanced モバイルを終了してから再び起動した場合は、時間の長さにかかわらずパスワードをもう一度入力して最初のサーバーに接続する必要があります。
- **接続するたび**: ユーザーは、サーバーに接続するたびにパスワードを入力する必要があります。

- **ユーザーが個別のサーバーを追加できるようにする**: このオプションが有効になっている場合、ユーザーは、サーバーの DNS 名または IP アドレスを知っていれば、Files Advanced モバイルアプリケーションでサーバーを手動で追加することができます。ユーザーのポリシーで**割り当て済みのサーバー**のみをユーザーが使用できるようにする場合は、このオプションを無効のままにします。
  - **ユーザーが設定したサーバーに接続するためのパスワードを保存できるようにする**: ユーザーが個別のサーバーの追加を許可されている場合、このサブオプションでそれらのサーバーに対するパスワードを保存できるようにするかどうかを決定します。
- **ウェブ クライアントからファイル サーバー、NAS、および SharePoint へのアクセスを許可する**: 有効にした場合、ウェブ クライアントは、モバイル データ ソースの表示とアクセスも実行できるようになります。
  - **ファイル サーバー、NAS および SharePoint のフォルダからデスクトップ クライアントへの同期を許可する**: このオプションが有効な場合、デスクトップ クライアントでは **[ネットワーク]** のコンテンツへの一方向同期が可能になります。
    - **ファイル サーバー、NAS および SharePoint のフォルダとデスクトップ クライアントの双方向同期を許可する**: このオプションが有効な場合、デスクトップ クライアントでは **[ネットワーク]** のコンテンツとの双方向同期が可能になります。

注意: デスクトップ クライアントで **[ネットワーク]** のコンテンツとの双方向同期を有効にするには、**[アプリケーション ポリシー]** タブでファイルとフォルダの操作の**作成**（フォルダの**追加**）、**コピー**、**削除**、**移動**、および**名前の変更**を事前に許可しておく必要があります。

- **ユーザーが UNC パスまたは URL を指定してネットワーク フォルダを追加できるようにする**: このオプションが有効な場合、モバイル クライアント ユーザーは、ネットワーク フォルダおよび SharePoint サイトのうち、自分に割り当てられているのではないもの、または既存のデータ ソースではアクセスできないものを追加してアクセスすることが可能になります。選択するゲートウェイ サーバーには、それらの SMB 共有または SharePoint サイトへのアクセス権が付与されていなければなりません。
  - **特定のネットワーク パスへのアクセスをブロックする**: 有効にすると、ユーザーによる自己プロビジョニングが許可されていないネットワーク パスのブラックリストを管理者が作成して使用できるようになります。
- **このモバイルクライアントのみがサードパーティ署名済み SSL 証明書を使用してサーバーに接続できるようにする**: このオプションが有効な場合、Access Mobile Client Files Advanced モバイルのみが、サードパーティの署名済み SSL 証明書を使用したサーバーへの接続を許可されます。

  注意: 管理サーバーにサードパーティの証明書がない場合、クライアントは初期設定の後に管理サーバーに接続できません。このオプションを有効にする場合は、すべてのゲートウェイ サーバーにサードパーティの証明書があることを確認してください。

- **信頼されていない SSL 証明書を使用してサーバーに接続するときにクライアントに警告する**: ユーザーが自己署名証明書を使用するサーバーに頻繁に接続する場合は、これらのサーバーに接続するときに表示されるクライアント側の警告ダイアログ メッセージを無効にすることができます。
- **サーバーからの応答がない場合のクライアント タイムアウト**: このオプションは、サーバーが応答しない場合のクライアント ログイン接続のタイムアウトを設定します。クライアントのデータ接続速度が特に遅い場合、またはゲートウェイ サーバーに接続する前に VPN オンデマンド ソリューションを利用して接続を確立している場合、このタイムアウトをデフォルトの 30 秒より長い値に設定することができます。クライアントが Files Advanced モバイルアプリを使用してこの値を変更できるようにするには、**[ユーザーが設定を変更できるようにする]** をオンにします。

6.2.3.6 ポリシー設定の例外

Files Advanced mobile for Android、**Files Advanced mobile for Good Dynamics**(iOS)、および **Files Advanced mobile with Mobile Iron AppConenct** ア

プリケーションを実行している場合、モバイルアプリケーションへの Files Advanced 管理ポリシーの適用方法にいくつかの例外があります。Android の場合、iOS クライアントのいくつかの機能がまだサポートされていないため、関連するポリシーは適用されません。Good Dynamics の場合、Good Control サーバー上で構成される Good Dynamics システムおよび Good Dynamics ポリシーセットに対していくつかの標準の Files Advanced モバイルポリシー機能が定義されています。MobileIron の場合、MobileIron AppConnect プラットフォームに対して一部の標準的な Files Advanced ポリシー機能が定義されます。これらの例外については、Files Advanced ポリシー設定のページを参照してください。Good、Android、MobileIron のロゴの上にマウスのポインターを移動すると、個別のポリシーの例外に関する詳細が表示されます。

6.2.4 ブロック対象のパスのリストの作成

ブラックリストを作成して、ユーザーによるモバイル デバイスからの自己プロビジョニングを不可にするパスを指定できます。これらのリストはユーザー ポリシーまたはグループ ポリシーに割り当てる必要があります。自己プロビジョニングのパスに対してのみ有効です。リストを作成して適切なユーザー、グループ、またはその両方に割り当てたら、適用するユーザー ポリシーまたはグループ ポリシーの **[特定のネットワーク パスへのアクセスをブロックする]** をそれぞれ有効にする必要があります。

リストを作成するには、次の操作を実行します。

1. 管理者としてウェブ インターフェイスを開きます。
2. ポリシー 『70ページ 』 ページを開きます。
3. 目的のユーザー ポリシーまたはグループ ポリシーをクリックします。
4. [サーバー ポリシー] 『91ページ 』 タブを開きます。
5. **[特定のネットワーク パスへのアクセスをブロックする]** チェックボックスをオンにします。

> **注意:** ブラックリストをユーザー ポリシーまたはグループ ポリシーに割り当てるたびに、この手順を実行する必要があります。

6. **[リストの追加/編集]** を押します。
7. **[ブロック対象のパスのリスト]** ページで **[リストの追加]** を押します。
8. このリストの名前を入力します。
9. ブラックリストに含めるパスまたはパスのリストを入力します。各エントリは、新しい行に入力する必要があります。
10. **[ユーザーまたはグループに適用する]** タブを開きます。
11. 目的のユーザーまたはグループにリストを割り当てます。
12. **[保存]** を押します。

ユーザー ポリシーまたはグループ ポリシーのブラックリストを有効にするには、次の操作を実行します。

1. 管理者としてウェブ インターフェイスを開きます。
2. ポリシー 『70ページ 』 ページを開きます。
3. 目的のユーザー ポリシーまたはグループ ポリシーをクリックします。
4. [サーバー ポリシー] 『91ページ 』 タブを開きます。
5. **[特定のネットワーク パスへのアクセスをブロックする]** チェックボックスをオンにします。

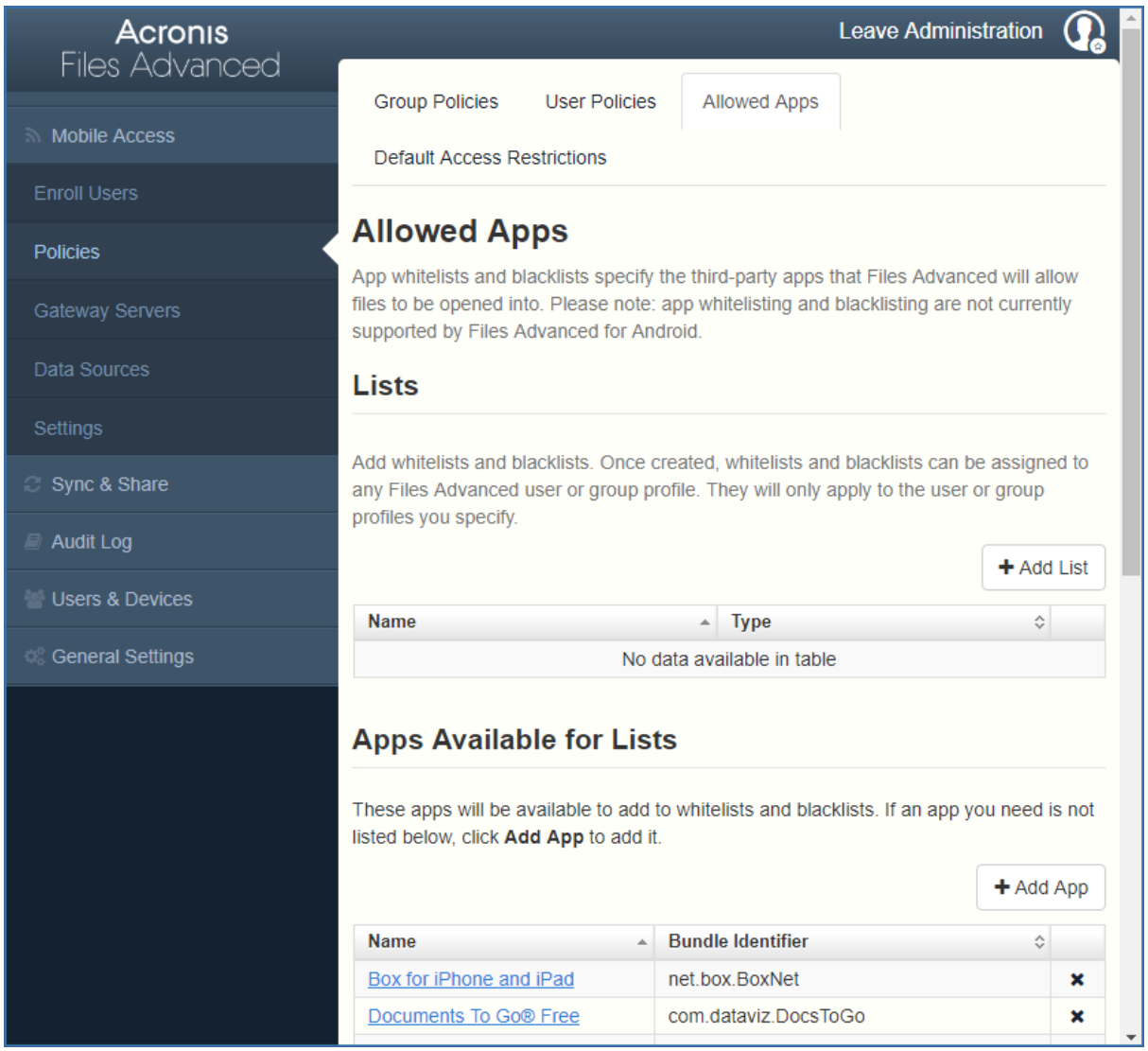
   注意: ブラックリストをユーザー ポリシーまたはグループ ポリシーに割り当てるたびに、この手順を実行する必要があります。

6. ドロップダウン メニューから目的のリストを選択します。

   注意: [リストの更新] を押すと、ドロップダウン メニューのオプションが更新されます。

7. **[保存]** を押すと、ポリシーを保存して終了します。

6.2.5　許可されたアプリ



Files Advanced Client Management を使用すると、モバイルデバイス上の他のアプリケーションでファイルを開く Files Advanced モバイルの機能を制限するホワイトリストまたはブラックリストを作成することができます。これらを使用して、Files Advanced モバイルを介してアクセスできるファイルがセキュリティで保護された信頼済みアプリケーションでのみ開けるようにすることができます。

ホワイトリスト: Files Advanced ファイルを開くことを許可されるアプリケーションのリストを指定できます。他のすべてのアプリケーションはアクセスを拒否されます。

ブラックリスト: Files Advanced ファイルを開くことを許可されないアプリケーションのリストを指定できます。他のすべてのアプリケーションはアクセスを許可されます。

Files Advanced で特定のアプリケーションが識別されるようにするには、そのアプリケーションの**バンドル ID** を Files Advanced に認識させる必要があります。一般的なアプリケーションおよびそれらのバンドル ID のリストは、デフォルトで Files Advanced Web Interface に含まれています。ホワイトリストまたはブラックリストに必要なアプリケーションが含まれていない場合、リストに追加する必要があります。

注意: アプリケーションのホワイトリストとブラックリストは、Files Advanced mobile for Android では現在サポートされていません。

リスト

ホワイトリストおよびブラックリストを追加します。作成したホワイトリストおよびブラックリストは、任意の Files Advanced ユーザー ポリシーまたはグループ ポリシーに割り当てることができます。リストは、指定したユーザー ポリシーまたはグループ ポリシーにのみ適用されます。

- **名前**: 管理者が設定したリストの名前を表示します。
- **タイプ**: リストのタイプを表示します（ホワイトリスト/ブラックリスト）
- **リストの追加**: [新しいホワイトリストまたはブラックリストの追加] メニューを開きます。

セクションの内容

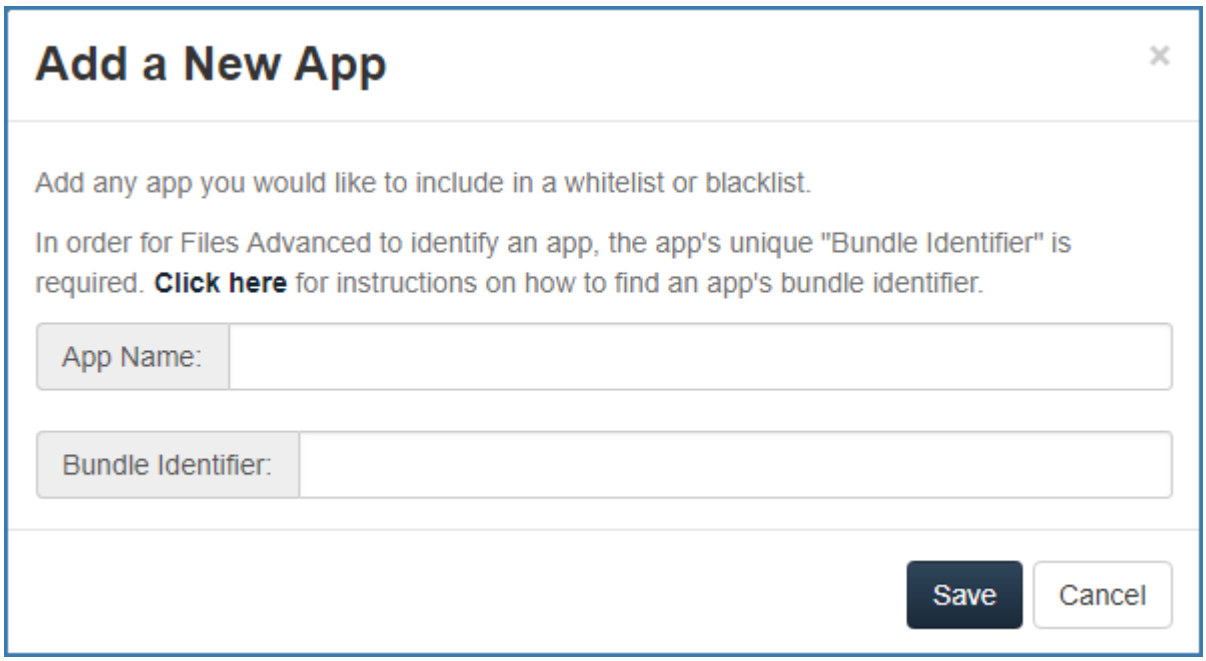
6.2.5.1 リストで使用できるアプリの追加

ホワイトリストまたはブラックリストに含めるアプリケーションを追加するには、次の操作を実行します。

1. トップ メニュー バーの **[許可されたアプリ]** をクリックします。
2. **[リストで使用できるアプリ]** セクションで **[アプリの追加]** をクリックします。
3. **アプリケーション名**を入力します。これには、App Store に表示されるアプリケーションの名前または選択した代替の名前を入力できます。

4. アプリケーションの**バンドル ID** を入力します。これは、目的のアプリケーション バンドル ID と正確に一致している必要があります。一致していないとホワイトリストまたはブラックリストに追加されません。
5. **[保存]** をクリックします。

バンドル ID は、デバイスでファイルを参照して確認できます。また、iTunes ライブラリで表示することもできます。



6.2.5.2 アプリケーションのバンドル ID の確認

デバイス上のファイルを参照することによるアプリケーションのバンドル ID の確認

デバイスのストレージの内容を参照できるソフトウェアを使用している場合は、デバイス上でアプリケーションを見つけて**バンドル ID** を確認することができます。このために使用できるアプリケーションの 1 つに iExplorer があります。

1. USB でデバイスをコンピュータに接続し、iExplorer または同様のユーティリティを起動します。
2. デバイスの Apps フォルダを開き、必要なアプリケーションを見つけます。
3. アプリケーションのフォルダを開き、**iTunesMetadata.plist** ファイルを見つけます。
4. この PLIST ファイルをテキスト エディタで開きます。

5. リスト内で **softwareVersionBundleId** キーを見つけます。
6. その下にある**文字列**値が、Files Advanced で入力する必要があるアプリケーションのバンドル ID の値です。通常、これらの値は「**com.companyname.appname**」という形式になっています。

iTunes ライブラリでアプリのバンドル ID を検索するには

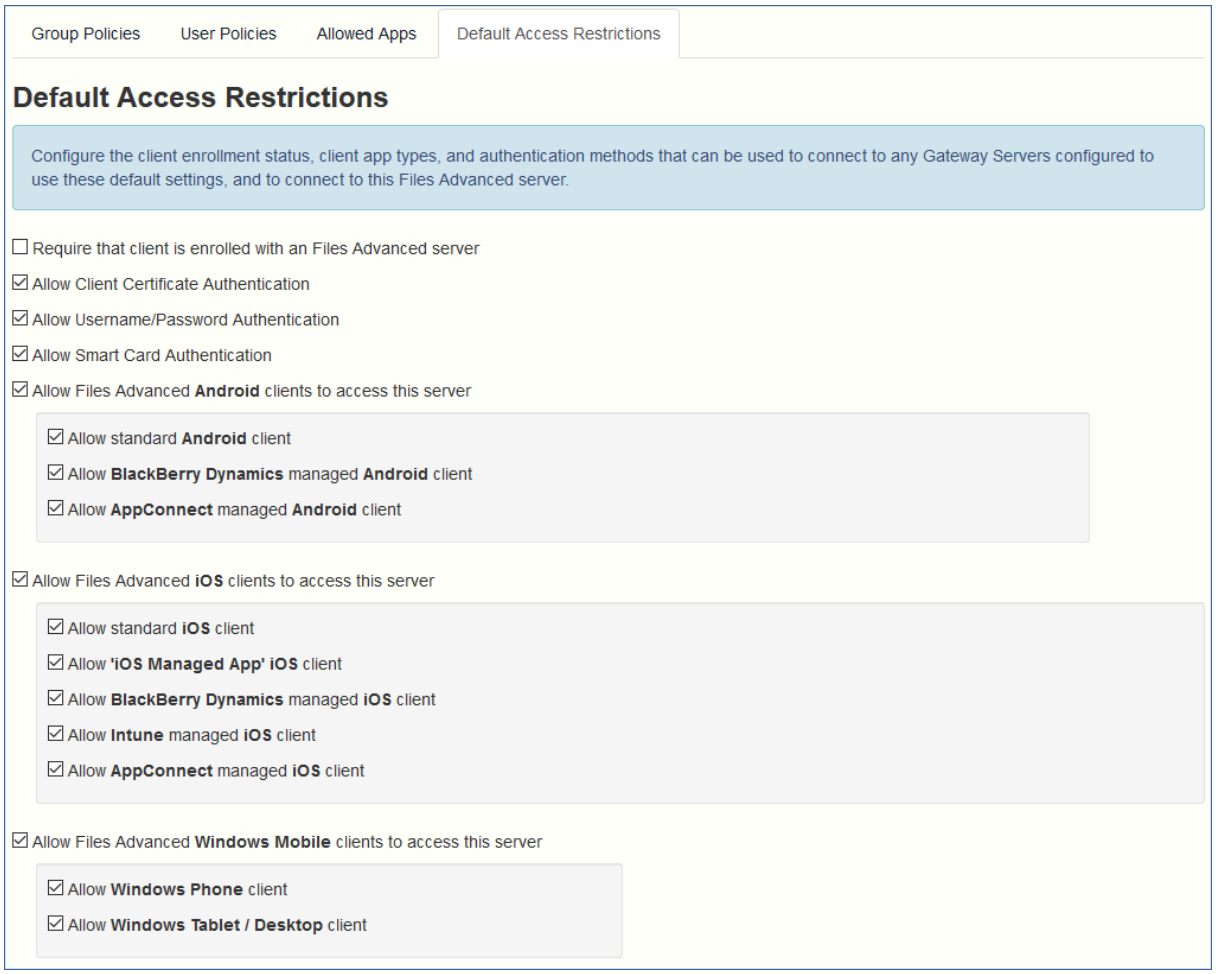
デバイスと iTunes が同期されており、目的のアプリがデバイス上にあるか、または iTunes からダウンロードされたものである場合、そのアプリはコンピュータのハード ドライブに配置されます。**バンドル ID** を見つけるには、まずハード ドライブでこのアプリを探し、アプリの中を確認します。

1. iTunes ライブラリに移動し、**Mobile Applications** フォルダを開きます。
2. Mac では、通常、ホーム ディレクトリの ~/Music/iTunes/Mobile Applications/ にあります。
3. Windows 7 PC の場合は一般的に **C:\Users\username\My Music\iTunes\Mobile Applications/** です。
4. デバイスにアプリをインストールしたばかりの場合は、iTunes の同期を実行してから、次の手順に進んでください。
5. **Mobile Applications** フォルダで必要なアプリを見つけます。
6. このファイルを複製し、拡張子を .ZIP に変更します。
7. 新しく作成されたこの ZIP ファイルを解凍すると、アプリケーション名の付いたフォルダが作成されます。
8. このフォルダの中には、**iTunesMetadata.plist** という名前のファイルがあります。
9. この PLIST ファイルをテキスト エディタで開きます。
10. リスト内で **softwareVersionBundleId** キーを見つけます。
11. その下にある**文字列**値が、Files Advanced で入力する必要があるアプリケーションのバンドル ID の値です。通常、これらの値は「**com.companyname.appname**」という形式になっています。

6.2.6　デフォルトのアクセス制限

このセクションでは、管理サーバーと接続されるクライアントに制限を設定することができます。このような制限は、ゲートウェイ サーバーに対するデフォルトの制限にもなります。

注意: ゲートウェイ サーバーに対するカスタム アクセス制限の設定の詳細については、「ゲートウェイ サーバーの管理」セクションの「ゲートウェイ サーバーの編集 『119ページ 』」の記事を参照してください。



クライアントの登録状態、クライアント アプリケーションのタイプ、および認証方法を構成します。認証方法は、この Files Advanced サーバーと、デフォルトのアクセス制限を使うように構成された任意のゲートウェイ サーバーの接続に使うことができます。

- **Files Advanced サーバーにクライアントの登録を要求**: このオプションを選択すると、このサーバーに接続しているすべての Files Advanced モバイルは、使用可能な Files Advanced サーバーの下に一覧表示される Files Advanced サーバーによって管

理される必要があります。このオプションによって、サーバーにアクセスするすべてのクライアントに、必要な設定とセキュリティオプションが反映されます。入力するサーバー名は、Mobile アプリで設定した管理サーバー名と同じである必要があります。名前の一部を使用して、たとえばドメイン内の複数のクライアント管理サーバーを許可することもできます。名前の一部を使用する場合、ワイルドカードを使用する必要はありません。

- **クライアント証明書認証を許可**: このオプションをオフにすると、証明書を使った接続ができなくなり、クライアントのユーザー名とパスワード、またはスマートカードを使って接続できるようになります。
- **ユーザー名/パスワード認証を許可**: このオプションをオフにすると、ユーザー名とパスワードを使った接続ができなくなり、クライアントの証明書、またはスマートカードを使って接続できるようになります。
- **スマートカード認証を許可**: このオプションをオフにすると、スマートカードを使った接続ができなくなり、クライアントのユーザー名とパスワード、または証明書を使って接続できるようになります。
- **Files Advanced Android クライアントにこのサーバーへのアクセスを許可**: このオプションをオフにすると、Android デバイスから Files Advanced サーバーに接続できなくなり、管理にアクセスすることもできなくなります。このオプションをオンにすると、以下のオプションでクライアントの接続条件を細かく設定することができます。
  - **標準 Android クライアントを許可**: このオプションをオンにすると、標準の Android Files Advanced クライアントアプリを実行しているユーザーにこの Files Advanced サーバーへの接続を許可します。Android ユーザーにこの Files Advanced サーバーへのアクセスを許可しない場合、この設定をオフにします。
  - **AppConnect が管理する Android クライアントを許可**: このオプションをオンにすると、Files Advanced クライアントを MobileIron に登録された Android ユーザーに、この Files Advanced サーバーへのアクセスを許可します。MobileIron に登録された Android ユーザーにこの Files Advanced サーバーへのアクセスを許可しない場合、この設定をオフにします。
  - **Blackberry Dynamics が管理する Android クライアントを許可**: このオプションをオンにすると、Android Files Advanced モバイル Good Dynamics が管理するクライアントを使用しているユーザーに、この Files Advanced サーバーへの接

続を許可します。Android Access Mobile Client Files Advanced モバイル Files Advanced モバイル Files Advanced モバイル Good Dynamics クライアントのユーザーに、この Files Advanced サーバーへのアクセスを許可しない場合、この設定をオフにします。

- **Files Advanced iOS クライアントにこのサーバーへのアクセスを許可**: このオプションをオフにすると、iOS デバイスから Files Advanced サーバーへの接続ができなくなり、管理にアクセスすることもできません。このオプションをオンにすると、以下のオプションでクライアントの接続条件を細かく設定することができます。
  - **標準 iOS クライアントを許可**: このオプションをオンにすると、標準 iOS Access Mobile Client Files Advanced モバイル Files Advanced モバイル Files Advanced モバイル appMobile アプリを実行しているユーザーにこの Files Advanced サーバーへの接続を許可します。iOS ユーザーにこの Files Advanced サーバーへのアクセスを許可しない場合、この設定をオフにします。
  - **「iOS 管理対象アプリ」iOS クライアントを許可**: このオプションをオンにすると、Files Advanced 管理対象 iOS Access アプリを実行しているユーザーに、この Files Advanced サーバーへの接続を許可します。この状態にするには、クライアントがパラメータを 1 つ以上含む管理対象アプリケーションの設定 『368ページ 』を受け取る必要があります。管理対象 iOS のユーザーにこの Acronis Files Advanced サーバーへのアクセスを許可しない場合は、この設定をオフにします。
  - **Blackberry Dynamics が管理する iOS クライアントを許可**: このオプションをオンにすると、iOS Files Advanced モバイル Good Dynamics が管理するクライアントを使用しているユーザーに、この Files Advanced サーバーへの接続を許可します。iOS Files Advanced モバイル Good Dynamics クライアントのユーザーに、この Files Advanced サーバーへのアクセスを許可しない場合、この設定をオフにします。
  - **Intune が管理する iOS クライアントを許可**: このオプションをオンにすると、iOS Access Mobile Client Files Advanced モバイル Files Advanced モバイル Files Advanced モバイル Intune が管理するクライアントを使用しているユーザーに、この Files Advanced サーバーへの接続を許可します。Intune が管理するユーザーにこの Files Advanced サーバーへのアクセスを許可しない場合は、この設定をオフにします。

- **AppConnect が管理する iOS クライアントを許可**: このオプションをオンにすると、MobileIron の Access Mobile Client Files Advanced モバイル Files Advanced モバイル Files Advanced モバイルに登録した iOS ユーザーが、この Files Advanced サーバーにアクセスすることを許可します。MobileIron に登録された iOS ユーザーにこの Files Advanced サーバーへのアクセスを許可しない場合、この設定をオフにします。

- **Files Advanced Windows Mobile クライアントにこのサーバーへのアクセスを許可**:
  - **Windows Phone クライアントを許可**: このオプションをオンにすると、Windows Mobile 版の Files Advanced アプリを実行している携帯電話ユーザーに、この Files Advanced サーバーへの接続を許可します。Windows Mobile ユーザーにこの Files Advanced サーバーへのアクセスを許可しない場合、この設定をオフにします。
  - **Windows タブレット/デスクトップクライアントを許可**: このオプションをオンにすると、Windows Mobile Files Advanced アプリを実行しているタブレットユーザーに、この Files Advanced サーバーへの接続を許可します。Windows Mobile ユーザーにこの Files Advanced サーバーへのアクセスを許可しない場合、この設定をオフにします。

6.3 モバイル デバイスの登録

Files Advanced モバイルアプリを開始するに当たり、ユーザーは App Store - iTunes、Google Play、または Windows ストアからアプリをインストールする必要があります。会社がクライアント管理を使用している場合、ユーザーも Files Advanced サーバーでデバイスに Files Advanced モバイルアプリを登録する必要があります。登録を行うと、モバイルクライアントの構成、セキュリティ設定、および機能が、Files Advanced のユーザー ポリシーまたはグループ ポリシーによって制御されるようになります。

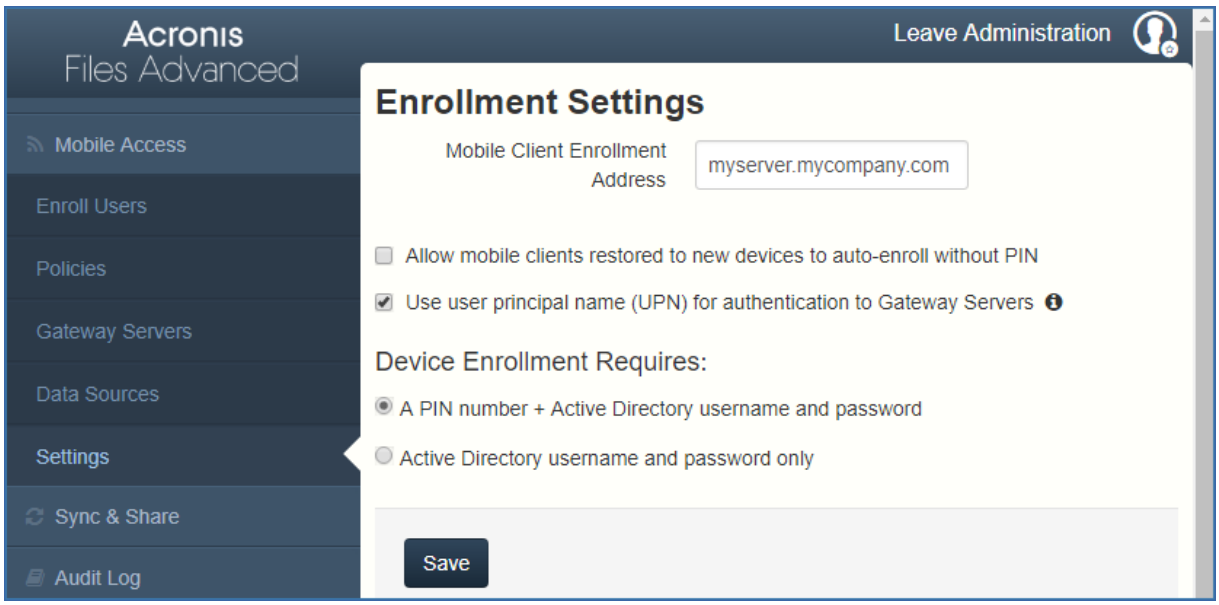
次のようなモバイルアプリケーションの設定と機能が管理ポリシーによって制御されます。

- Files Advanced アプリケーションロックパスワードを要求する
- アプリのパスワードの複雑性に関する要件
- Files Advanced アプリケーションを管理から削除する機能

- Files Advanced アプリケーションからのファイルの電子メール送信および印刷を許可する
- ファイルをデバイスに保存することを許可する
- Files Advanced アプリケーションのデバイス上のファイルを iTunes バックアップに含めることを許可する
- 他のアプリケーションから Files Advanced へのファイルの送信を許可する
- 他のアプリケーションで Files Advanced ファイルを開くことを許可する
- Files Advanced ファイルを開くことができる他のアプリケーションを制限する
- PDF 注釈を許可する
- ファイルやフォルダの作成、名前の変更、および削除を許可する
- ファイルの移動を許可する
- 削除するときの確認を必須にする
- サーバー、フォルダ、ホームディレクトリを割り当てて Files Advanced アプリに自動的に表示されるようにする
- 割り当てられたフォルダを設定してサーバーとの一方向または双方向同期を実行できるようにする

セクションの内容

6.3.1　サーバー側の管理登録処理



1. Files Advanced ウェブ インターフェイスを開きます。
2. 管理者としてログインします。
3. **[モバイル アクセス]** タブを選択します。
4. **[設定]** タブを開きます。
5. デバイス登録要件を選択します

登録設定

モバイルクライアントを新しいデバイスに復元した場合でも、PIN コードなしで自動登録されるようにする:

ユーザープリンシパル名（UPN)を使用したゲートウェイサーバーの認証: オンにすると、ドメイン/ユーザー名の代わりに username@domain.com を使用して認証を行います。

デバイス登録モード

Files Advanced には、2 つのデバイス登録モード オプションがあります。このモードは、すべてのクライアント登録で使用されます。要件に適したオプションを選択する必要があります。

- **PIN コード + Active Directory のユーザー名とパスワード**: ユーザーは、自分の Files Advanced アプリケーションをアクティブ化して Files Advanced サーバーにアクセスするために、有効期限が設定されたワンタイム PIN コードと有効な Active Directory ユーザー名およびパスワードの入力が求められます。このオプションを使用する場合、ユーザーは、IT 管理者によって発行された PIN コードを受け取った後に 1 台のデバイスのみ登録することができます。このオプションは、2 つの要素によるデバイス登録でセキュリティを強化する必要がある場合に推奨されます。
- **Active Directory のユーザー名とパスワードのみ**: ユーザーは Active Directory のユーザー名とパスワードのみを使用して Files Advanced アプリケーションをアクティブ化することができます。このオプションを使用すると、ユーザーが今後いつでも 1 台または複数のデバイスを登録することができます。ユーザーには、Files Advanced クライアント管理サーバーの名前、または Files Advanced クライアント管理サーバーをポイントする URL のみを提供する必要があります。この情報は、ウェブ サイトに掲示したり電子メールで送信したりできるので、多数のユーザーへの Files Advanced の導入を簡素化することができます。このオプションは、2 つの要素による登録が不要な環境や、多くのユーザーがいつでも Files Advanced にアクセスする必要がある環境（学生用の導入など)に推奨されます。

ユーザーへの登録招待

ユーザーは通常、Files Advanced Administrator から送信される電子メールによって、Files Advanced サーバーでの登録に招待されます。ユーザーが必要とする場合は、設定可能な日数だけ有効なワンタイム PIN コードをこの電子メールに含めます。この PIN コードを使用して、1 つのデバイスでのみ Mobile アプリに登録することができます。ユーザーが複数のデバイスを持っている場合は、アクセスが必要なデバイスごとに招待メールを受け取る必要があります。この電子メールには、Mobile アプリを初めてインストールする必要がある場合のために、App Store 内の Mobile アプリへのリンクが含まれています。さらに、2 つ目のリンクが含まれており、デバイスでこのリンクをタップすると Files Advanced モバイルが開き、Files Advanced サーバーの名前、固有の登録 PIN コード、およびユーザーのユーザー名を使用して、クライアントの登録が自動的に完了します。このリンクを使用すると、ユーザーがアカウントのパスワードを入力するだけでクライアントの登録が完了します。

- 登録招待メールが生成されると、招待されるユーザーが **[登録招待メール]** ページに表示されます。自動電子メール以外の方法で伝える必要がある場合のために、各ユーザーの PIN コードが一覧表示されます。
- ユーザーがワンタイム PIN コードを使用して Files Advanced モバイルに正常に登録すると、そのユーザーはこのリストに表示されなくなります。
- ユーザーの招待 PIN コードを無効にするには、[削除] をクリックしてリストから削除します。

PINコードが不要な場合の基本的なURL登録リンクの使用

クライアントの登録に PIN コードを必要としないようにサーバーが設定されている場合、モバイル デバイスでタップしたときに登録処理を自動的に開始する標準の URL をユーザーに提供することができます。

管理サーバーの登録 URL を判別するには、**[モバイルアクセス]** タブを開き、**[ユーザーの登録]** タブを開きます。URL はこのページに表示されます。

注記: 2 つのモードの詳細については、「設定 『143ページ 』」セクションを参照してください。

Files Advanced の登録招待を生成するには:

1. [**モバイル アクセス**] タブを開き、[**ユーザーの登録**] タブを開きます。
2. **[登録招待メールを送信する]** ボタンを押します。
3. Active Directory のユーザー名もしくはグループ名を入力し、[検索] をクリックします。グループを選択した場合に [追加] を押すと、[招待するユーザー] リストのグループに各電子メール アドレスが表示されます。これにより、グループ内のすべてのメンバを一括招待することができます。オプションで、招待を送信する前に 1 人または複数のグループ メンバを削除することができます。[先頭の文字] または [含まれる文字] 検索を Active Directory グループに対して実行できます。[先頭の文字] の検索は、[含まれる文字] の検索よりも短時間で完了します。
4. 最初のユーザーまたはグループを追加したら、新しい検索を実行し、さらにユーザーまたはグループをリストに追加することができます。

5. 招待するユーザーのリストを確認します。リストから任意のユーザーを削除することができます。
6. ユーザーのアカウントに電子メール アドレスが関連付けられていない場合は、[電子メールアドレス] 列に **[電子メールアドレスが割り当てられていません。ここをクリックして編集してください]** と表示されます。これらのエントリのいずれかをクリックして、そのユーザーの代替電子メール アドレスを手動で入力することができます。**[電子メールアドレスが割り当てられていません]** と表示されても、それらのユーザーの PIN コードが生成され、[ユーザーの登録] ページに表示されます。それらのユーザーが Files Advanced モバイルに登録するには、その前にこの PIN コードを別の方法でユーザーに伝える必要があります。

   注記: 登録 PIN コードを手動でユーザーに伝える場合は、**[指定したアドレスを使用して登録招待メールを各ユーザーに送信する]** チェック ボックスをオフにします。各 PIN コードは、**[登録招待メール]** ページに表示されます。

7. [招待の期限が切れるまでの日数] フィールドで、招待の有効期間の日数を選択します。
8. 招待リストで各ユーザーに送信する PIN コードの数を選択します。これは、ユーザーが 2、3 台のデバイスを持っている場合に使用できます。ユーザーは、固有のワンタイム PIN コードが含まれる個別の電子メールを受信します。

   注意: Files Advanced ライセンスを使用すると、ライセンス取得済みユーザーは最大 3 台のデバイスをアクティブ化することができます。4 台目以降のデバイスは、ライセンス上の新規ユーザーとして追加できます。

9. ユーザーがダウンロードしてデバイスにインストールする Files Advanced モバイルのバージョンを選択します。iOS、Android、または両方を選択できます。Files Advanced for Good Dynamics を使用している場合、このオプションを選択すると、Good Dynamics バージョンの Files Advanced モバイルのみをダウンロードが可能であることをユーザーに指定できます。
10. [送信] を押します。

    注記: 送信時にエラー メッセージが表示された場合、[全般設定] にある [SMTP] タブの SMTP 設定が適切であることを確認してください。また、**セキュリティで保護された接続**を使っている場合、自分が使用している証明書が、SMTP サーバーのホスト名と一致していることを確認します。

mobilEcho 4.5 以前により過去に登録されているユーザーの招待

mobilEcho 2.X では、クライアントを Client Management システムへ登録するために PIN コードは必要ありません。mobilEcho 2.X クライアントを Files Advanced の管理システムに移行するためのオプションは 2 つあります。デフォルトでは、mobilEcho サーバーを 2.X からアップグレードすると、過去にその 2.X サーバーによって管理されたことがあるクライアントが自動登録され、PIN コードを入力しなくても Files Advanced **デバイス**リストに表示されます。システムにアクセスするすべてのデバイスが PIN コード付きで登録されるようにする場合、この設定を無効にします。無効にすると、**[ユーザーがモバイルクライアントを管理から削除できる]** 権限がない場合、ユーザーが PIN コードを使用して登録を行うには、デバイスから Files Advanced を削除して App Store から再インストールする必要があります。

また、この自動登録設定を有効にすると、mobilEcho 2.X の管理対象となっているバージョンまたは 3.0 が実行されているデバイスの iTunes バックアップを実行したり、そのバックアップを新しいデバイスに復元したりすることができます。また、ユーザーが関連するアカウントで Active Directory のユーザー名とパスワードを有効にしている場合に限り、新しいデバイスを PIN コードなしでクライアント管理に自動的に登録することができます。

過去に管理対象となったことがあるすべてのクライアントが一通り管理サーバーにアクセスしたら、自動登録設定を無効にすることをお勧めします。すべてのクライアントがアクセスすると、それらのクライアントは [デバイス] リストに表示されます。

mobilEcho クライアント管理サーバーを Files Advanced サーバーにアップグレードした後、mobilEcho 2.X Client Management に既に登録されている mobilEcho クライアントが自動的に登録されるようにするには、**[2.X サーバーによって以前に管理されていた mobilEcho クライアントおよび新しいデバイスに復元された管理対象の mobilEcho クライアントが、PIN コードを使用せずに自動登録できるようにする]** 設定を有効にします。

6.3.2　ユーザー側の管理登録処理

管理登録招待メールを送信した各ユーザーは、次の情報が含まれる電子メールを受け取ります。

- Apple App Store から Files Advanced モバイルをインストールするためのリンク
- Mobile アプリを起動し、登録処理を自動化するために使用するリンク
- ワンタイム PIN コード
- 管理サーバーのアドレス
- 電子メールの指示に従って、Files Advanced モバイルをインストールし、登録情報を入力します。

Mobile アプリが既にインストールされていて、デバイスでこの電子メールを表示している間にユーザーが [自動的に登録を開始するにはこのリンクをタップ...] オプションをタップした場合、Files Advanced が自動的に起動し、登録フォームが表示されます。ユーザーのサーバー アドレス、PIN コード、およびユーザー名もこの URL でエンコードされているため、登録フォーム内のこれらのフィールドは自動的に入力されます。この時点で、ユーザーがパスワードを入力するだけで登録処理が完了します。

必要なユーザー名とパスワードは、ユーザーの Active Directory のユーザー名とパスワードです。これらのログイン情報は、ゲートウェイ サーバーへのアクセスのために適切なユーザーまたはグループの管理ポリシーを照合するのに使用され、また、Files Advanced サーバー ログインのためのログイン情報を保存するため（管理ポリシーで許可されている場合)に使用されます。

管理ポリシーでアプリケーション ロック パスワードが必須になっている場合は、パスワードを入力するように要求するメッセージが表示されます。この初期パスワードの設定時および将来のアプリケーション ロック パスワードの変更時には、ポリシーで設定されているすべてのパスワードの複雑さの要件を満たす必要があります。

デバイスにローカルでファイルを保存することがポリシーで制限されている場合は、既存のファイルが削除されることを示す警告が表示され、削除する前に操作する必要があるファイルがある場合は、管理設定処理をキャンセルすることができます。

管理に登録するには

登録用電子メールを使った自動登録

1. IT 管理者から送信された電子メールを開き、Files Advanced をまだインストールしていない場合は「**Files Advanced をインストールするにはここをクリック**」というリンクをクリックします。
2. Files Advanced がインストールされたら、デバイスで招待メールに戻り、電子メールの手順 2 の「**自動的に登録を開始するにはこのリンクをクリック**」をタップします。
3. 登録フォームが表示されます。招待メール内のリンクを使用して登録処理を開始する場合は、サーバーのアドレス、PIN コード、およびユーザー名は自動的に入力されます。

   注記:サーバーで PIN コードが不要な場合は、登録フォームに表示されません。

4. パスワードを入力し、**[今すぐ登録]** をタップして続行します。

   注記: ユーザー名とパスワードは会社の標準のユーザー名とパスワードです。これは、コンピュータまたは電子メールにログインするために使用するパスワードと同じ場合があります。

5. フォーム全体に入力した後で、**[登録]** ボタンをタップします。
6. 社内のサーバーの設定によっては、管理サーバーのセキュリティ証明書が信頼されていないことを示す警告が表示されることがあります。この警告を受け入れて続行するには、**[常に続行]** をクリックします。
7. Files Advanced モバイルアプリにアプリケーションロックパスワードが必要な場合は、パスワードを設定するように要求されます。パスワードの複雑性の要件が適用されている場合があり、必要な場合はそれが表示されます。
8. 管理ポリシーで Files Advanced でのファイルの保存が制限されているか、Files Advanced モバイルアプリ内で個別のサーバーを追加する機能が無効にされている場合、確認ウィンドウが表示されることがあります。Files Advanced モバイルアプリでローカルに保存したファイルがある場合は、**[マイファイル]** ローカルファイルストレージ内のファイルが削除されることを確認するよう求めるメッセージが表示されます。[いいえ] を選択すると、管理登録処理がキャンセルされ、ファイルは変更されずに残ります。

手動登録

1. Files Advanced アプリケーションを開きます。
2. **[設定]** を開きます。
3. **[登録]** をタップします。
4. サーバーのアドレス、PIN コード（必要な場合)、ユーザー名、パスワードを入力します。
5. フォーム全体に入力した後で、**[登録]** ボタンをタップします。
6. 社内のサーバーの設定によっては、管理サーバーのセキュリティ証明書が信頼されていないことを示す警告が表示されることがあります。この警告を受け入れて続行するには、**[常に続行]** をクリックします。
7. Files Advanced モバイルアプリにアプリケーションロックパスワードが必要な場合は、パスワードを設定するように要求されます。パスワードの複雑性の要件が適用されている場合があり、必要な場合はそれが表示されます。

管理ポリシーで Files Advanced でのファイルの保存が制限されているか、Files Advanced モバイルアプリ内で個別のサーバーを追加する機能が無効にされている場合、確認ウィンドウが表示されることがあります。Files Advanced モバイルアプリでローカルに保存したファイルがある場合は、**[マイファイル]** ローカルファイルストレージ内のファイルが削除されることを確認するよう求めるメッセージが表示されます。[いいえ] を選択すると、管理登録処理がキャンセルされ、ファイルは変更されずに残ります。

継続的な管理の更新

初期管理設定の後、Files Advanced モバイルは、クライアントアプリが起動されるたびに管理サーバーに接続しようとします。設定変更、サーバーまたはフォルダの割り当ての変更、アプリケーション ロック パスワードのリセット、またはリモート ワイプは、そのときにクライアントに受け入れられます。

接続要件

Files Advanced クライアントが、プロファイルのアップデート、リモート パスワードのリセット、およびリモート ワイプの指示を受け取るには、Files Advanced サーバーへのネットワーク アクセ

スが必要です。クライアントが、Files Advanced にアクセスする前に VPN に接続する必要がある場合は、管理コマンドを受け付ける前に VPN に接続する必要があります。

管理の削除

Files Advanced モバイルを管理から削除する場合、次の 2 つのオプションを使用できます。

- [管理を使用] オプションをオフにする（ポリシーで許可されている場合)
- Mobile アプリケーションを削除する

Files Advanced の管理ポリシーの設定によっては、Files Advanced モバイルを管理から削除する権限が与えられている場合があります。削除すると、通常は社内のファイル サーバーにアクセスできなくなります。この操作が許可されている場合、以下の手順に従ってデバイスを非管理にします。

デバイスを管理するには、次の操作を行います。

1. **[設定]** メニューをタップします。
2. [**管理を使用**] オプションをオフにします。
3. デバイスを管理から削除するときに Files Advanced モバイルのデータが必ず消去されるように、プロファイルで指定されている場合があります。消去したくない場合はこの時点で処理をキャンセルできます。
4. 確認ウィンドウで **[はい]** をタップして Files Advanced を管理から削除することを確認します。

注意: Files Advanced ポリシーでクライアントを非管理にすることが許可されていない場合は、**[設定]** メニューに **[管理を使用]** オプションが表示されません。この場合、デバイスを管理から削除するには、Mobile アプリケーションをアンインストールする必要があります。アプリケーションをアンインストールすると、Files Advanced モバイルの既存のデータと設定がすべて消去されます。アプリケーションを再インストールすると、設定がデフォルトに戻ります。

Files Advanced モバイル アプリケーションをアンインストールするには、次の操作を行います。

iOS の場合:

1. Mobile アプリのアイコンが揺れ始めるまでアイコンを指で押し続けます。
2. Mobile アプリケーションの **[X]** ボタンをタップし、アンインストール処理を確認します。

Windows の場合:

1. アプリアイコンをタップ&ホールドします。
2. **[アンインストール]** を選択します。

Android の場合:

注意: Android デバイスのソフトウェアにはさまざまな種類があるため、設定は若干異なる場合があります。

---

1. [アプリ] メニューを開き、**[編集/削除]** を選択します。
2. Files Advanced アプリを見つけて選択します。
3. **[削除]** を押します。

6.4 ゲートウェイ サーバーの管理

Files Advanced ゲートウェイサーバーは、ファイルサーバー、SharePoint リポジトリ、および同期と共有ボリュームにあるファイルとフォルダについて、それらへのアクセスと操作を処理する Files Advanced モバイルアプリから参照されるサーバーです。ゲートウェイサーバーは、モバイル クライアントにとって、ファイルへの「ゲートウェイ」となります。

Files Advanced サーバーは、1 つ以上のゲートウェイ サーバーの管理と構成を、同じ管理コンソールから実行することができます。管理下に置かれているゲートウェイ サーバーは、[**モバイル アクセス**] メニューの [**ゲートウェイ サーバー**] セクションに表示されます。

- **タイプ**: ゲートウェイのタイプを表示します。現在、[サーバー] タイプのみ選択できます。
- **名前**: ゲートウェイの作成時に与えられた表示名。

- **アドレス**: ゲートウェイの FQDN または IP アドレス。
- **バージョン**: Files Advanced ゲートウェイ サーバーのバージョンを表示します。
- **ステータス**: サーバーがオンラインかオフラインかを表示します。
- **アクティブ セッション**: このゲートウェイ サーバーに対して現在アクティブなセッションの数。
- **使用ライセンス**: 使用済みのライセンスの数と、使用可能なライセンスの数。
- **ライセンス**: ゲートウェイ サーバーに使われているライセンスの現在のタイプを表示します。

[新しいゲートウェイ サーバーの追加] ボタンを使用すると、新しいゲートウェイ サーバーを登録できます。各ゲートウェイ サーバーの [操作] メニューから、管理者はサーバーとそのパフォーマンスに関する詳細の取得、構成の編集、サーバーに対するアクセス制限の変更、サーバーのライセンスの変更、ゲートウェイ サーバーの削除を行うことができます。

要件

Files Advanced は、**Windows Search** を使用して、ネットワークデータソース内の検索を可能にしています。**Windows Search** は、Windows Server の組み込み機能ですが、デフォルトで有効になりません。

次の手順に従って有効にする必要があります。

- サーバーマネージャで **ファイルサービス** という名前の役割を追加/インストールします。
- **Windows Search サービス**を有効にして開始する必要があります。

注意: 要件が満たされない場合は、ネットワークデータソースで検索を実行できません。

ファイル名検索のローカル データ ソースのインデックスを作成

デフォルトでは、インデックス検索がすべてのゲートウェイ サーバーで有効です。インデックス検索は、ゲートウェイの [**サーバーの編集**] ダイアログでゲートウェイサーバーごとに無効または有効にすることができます。

デフォルト パス

スタンドアロンサーバーのデフォルトでは、Files Advanced は Files Advanced ゲートウェイサーバーアプリケーションフォルダ内の **Search Indexes** ディレクトリにインデックス ファイルを保存します。別の場所にインデックス ファイルを保存する場合は、新しいフォルダのパスを入力します。

利用可能な場合、Microsoft Windows Search を使用してコンテンツ検索をサポート

共有フォルダのコンテンツ検索のサポートはデフォルトで有効になっており、このオプションを有効することによって有効または無効にすることができます。コンテンツ検索は、ゲートウェイサーバーごとに有効または無効にすることができます。

Windows Search で必要なデータソースをインデックス化するように設定するには、スタートバーの [Windows Search] アイコンを右クリックし、**[Windows Search のオプション]** を選択します。Windows の Reshare で Windows のコンテンツ検索を実行できますが、リモート コンピュータはゲートウェイ サーバーと同じドメインに参加している必要があります。

注意: Windows の Reshare でコンテンツ検索を使用する場合は、データ ソースのボリューム パスはホスト名か完全な修飾子名にする必要があります。IP アドレスは Windows Search ではサポートされていません。

その他の構成

コンテンツ検索インデックス化は、特定のファイルタイプのコンテンツのみをインデックス化するように設定できます。

1. ゲートウェイサーバーをホストしているサーバーで、**[コントロール パネル]** -> **[インデックスのオプション]** を開きます。
2. **[詳細設定]** を選択して、**[ファイルの種類]** タブを開きます。
3. コンテンツ検索を有効/無効にするファイルの種類（**doc** や **txt**)を探します。

必要なファイルの種類を選択して、**[このファイルのインデックスの作成方法]** で、このファイルの種類のコンテンツ検索を有効にする場合は **[プロパティとファイルのコンテンツのインデックスを作成する]** を、無効にする場合は **[プロパティのみインデックスを作成する]** を選択します。必要なすべてのファイルの種類に対してこのステップを繰り返します。

SharePoint

これらの認証情報の入力は一般的な SharePoint のサポートでは任意ですが、サイト コレクションを列挙するには必須です。たとえば、http://sharepoint.example.com および http://sharepoint.example.com/SeparateCollection という 2 つのサイト コレクションがあるとします。資格情報を入力しないと、http://sharepoint.example.com をポイントするボリュームを作成する場合、ボリュームを列挙するときに SeparateCollection というフォルダが表示されません。アカウントには、ウェブ アプリケーションに対するすべて読み取りアクセスが必要です。

セクションの内容

6.4.1 新しいゲートウェイ サーバーの登録

管理ウェブ アプリケーションと同じコンピュータで実行しているゲートウェイ サーバーの自動登録を例外として、ゲートウェイ サーバーの登録は、複数の手順からなる、手動プロセスです。

1. ゲートウェイ サービスがインストールされているコンピュータを参照します。
2. **https://localhost/gateway_admin** を開きます。

注意: デフォルトのポート番号は、3000 です。デフォルトのポートを変更した場合は、「localhost」の後ろにポート番号を追加してください。

3. **[管理キー]** を書き留めます。

4. Files Advanced ウェブ インターフェイスを開きます。
5. **[モバイル アクセス]** タブを選択します。
6. **[ゲートウェイ サーバー]** ページを開きます。
7. **[新しいゲートウェイ サーバーの追加]** ボタンを押します。

8. ゲートウェイ サーバーの表示名を入力します。
9. ゲートウェイ サーバーの FQDN または IP アドレスを入力します。

   注記: リバース プロキシ サーバーまたはロードバランサを経由してモバイル クライアントをゲートウェイに接続する場合、**[クライアント接続用に別のアドレスを使用する]** を有効にして、リバース プロキシ サーバーまたはロードバランサの FQDN または IP アドレスを入力してください。

10. **[管理キー]** を入力します。
11. 必要に応じて、**[自己署名した証明書を使用した Files Advanced サーバーからの接続を許可]** を有効にして、自己署名した証明書を使用することで、このゲートウェイに接続することができます。
12. **[保存]** ボタンを押します。

ゲートウェイ サーバーを登録した後、このゲートウェイ サーバーにカスタムのアクセス制限を設定できます。この点に関する詳細については、「ゲートウェイ サーバーの編集 『119 ページ 』」セクションを参照してください。

6.4.2 サーバーの詳細

ゲートウェイ サーバーの **[詳細]** ページを開くと、特定のサーバーとそのユーザーに関する多くの有用な情報が得られます。

ステータス

[ステータス] セクションでは、ゲートウェイ サーバー自体に関する情報が得られます。オペレーティング システム、ライセンスの種類、使用されているライセンスの数、ゲートウェイ サーバーのバージョンなどの情報です。

アクティブ ユーザー

現在、ゲートウェイ サーバーでアクティブなすべてのユーザーの表が表示されます。

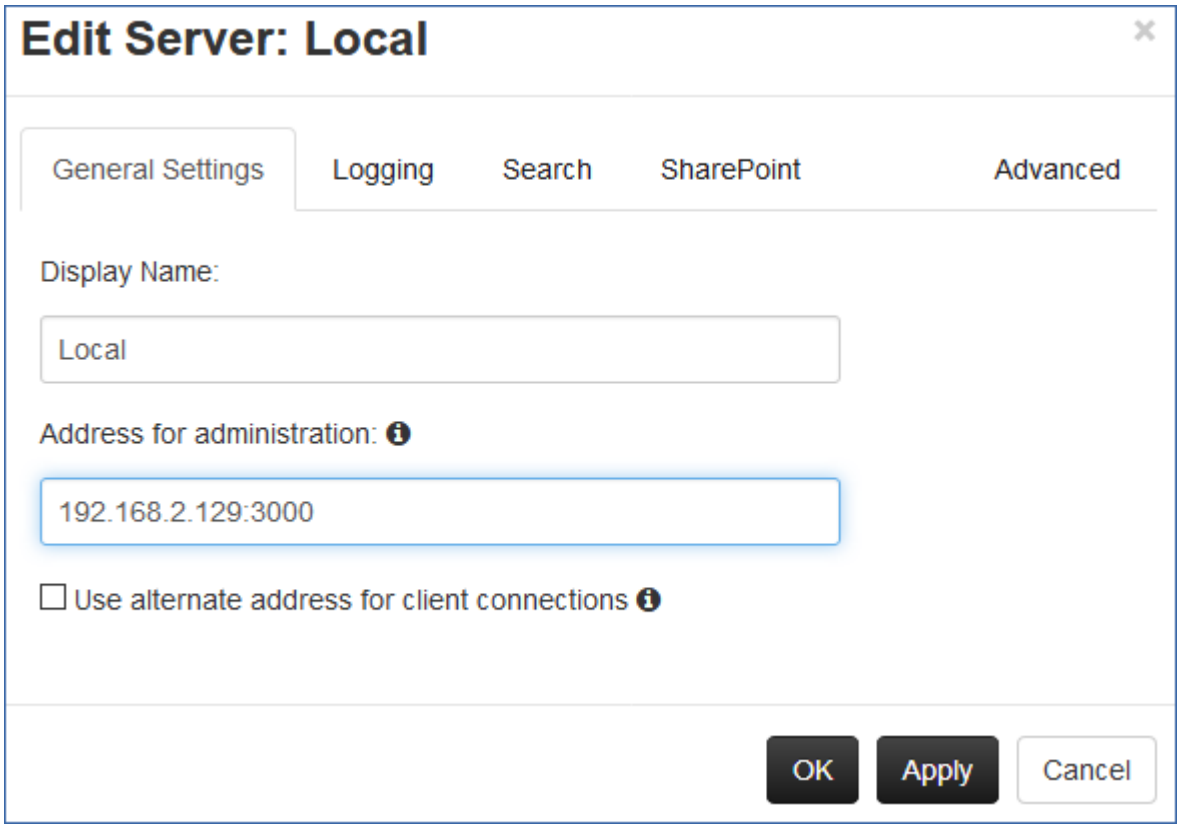
- **ユーザー**: ユーザーの Active Directory 名（フル)を表示します。
- **ロケーション**: デバイスの IP アドレスを表示します。
- **デバイス**: ユーザーが設定したデバイス名を表示します。
- **モデル**: デバイスのタイプ/モデルを表示します。
- **OS**: デバイスのオペレーティング システムを表示します。
- **クライアントのバージョン**: デバイスにインストールされている Files Advanced アプリケーションのバージョンを表示します。
- **ポリシー**: デバイスが使用するアカウントのポリシーを表示します。
- **アイドル時間**: ユーザーがゲートウェイに接続した状態で経過した時間を表示します。

6.4.3 ゲートウェイサーバー構成

ゲートウェイサーバーの構成を変更するには、設定メニューに入力する必要があります。

1. **[モバイルアクセス]** → **[ゲートウェイサーバー]** タブに移動します。
2. 必要なサーバーの **[詳細]** の横にある矢印をクリックします。
3. **[編集]** を選択します。

セクションの内容



- **表示名**: ゲートウェイ サーバーの表示名を設定します。この名前はあくまでも表示用であり、サーバーを区別しやすいようにするために使用されます。
- **管理のアドレス**: Files Advanced サーバーとモバイルクライアントがアクセス可能なゲートウェイサーバーのデフォルトアドレスを設定します。IP アドレスではなく、DNS アドレスを使用することをおすすめします。

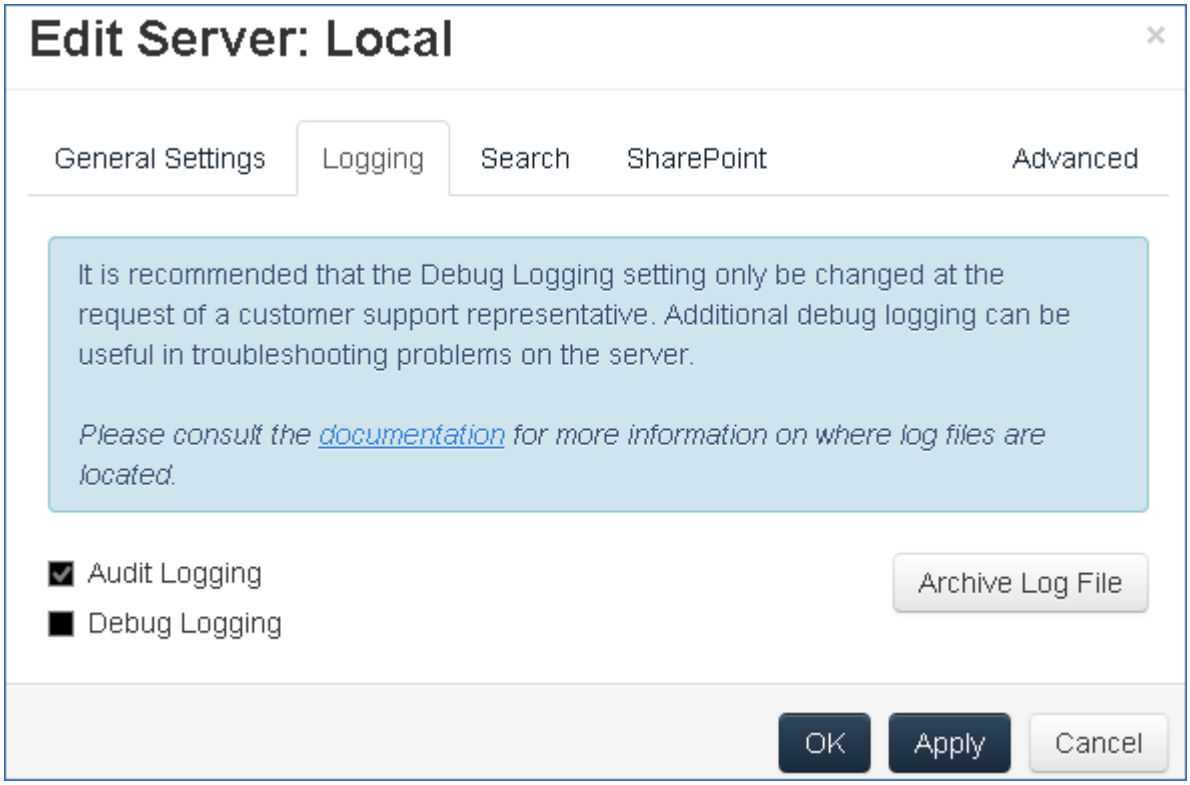
  注意: これは、**[クライアント接続に代替アドレスを使用]** が有効にされていない限り、モバイルクライアントがゲートウェイサーバーに接続する際のデフォルトアドレスです。

- **クライアント接続に代替アドレスを使用**: 有効にすると、モバイルクライアントがゲートウェイサーバーに接続する際に使用するアドレスを上書きできます。

  注意: この設定は、負荷分散装置または何らかのプロキシ（BlackBerry Dynamics、MobileIron など)経由でプロキシゲートウェイサーバーに接続する特定の構成のみで使用してください。通常の導入環境では、この設定を有効にする必要はありません。

  - **クライアント接続のアドレス**: **[クライアント接続に代替アドレスを使用]** を有効にした場合、このアドレスが、モバイルクライアントでゲートウェイサーバーに接続するために使用するアドレスになります。IP アドレスではなく、DNS アドレスを使用することをおすすめします。

[ログ] セクションでは、この特定のゲートウェイサーバーのログイベントを監査ログに表示するかどうかを制御でき、またこのサーバーのデバッグ ログを有効にできます。



特定のゲートウェイ サーバーに対して監査ログを有効にするには:

1. ウェブ インターフェイスを開きます。
2. 管理者としてログインします。
3. **[モバイル アクセス]** タブを選択します。
4. **[ゲートウェイ サーバー]** タブを開きます。
5. **[監査ログ]** を有効にするサーバーを検索します。
6. **[詳細]** ボタンの横にある下向き矢印を押し、**[編集]** を選択します。
7. **[ログ]** セクションで、**[監査ログ]** をオンにします。
8. **[保存]** ボタンをクリックします。

特定のゲートウェイ サーバーに対してデバッグ ログを有効にするには:

注意: デバッグログのデフォルトのロケーションは **`C:\Program Files (x86)\Acronis\Access\Gateway Server\Logs\AcronisAccessGateway`** です。

---

1. ウェブ インターフェイスを開きます。
2. 管理者としてログインします。
3. **[モバイル アクセス]** タブを選択します。
4. **[ゲートウェイ サーバー]** タブを開きます。
5. **[デバッグ ログ]** を有効にするサーバーを検索します**。**
6. **[詳細]** ボタンの横にある下向き矢印を押し、**[編集]** を選択します。
7. **[ログ]** セクションで、**[デバッグ ログ]** をオンにします。
8. **[保存]** ボタンをクリックします。

要件

Files Advanced は、**Windows Search** を使用して、ネットワークデータソース内の検索を可能にしています。**Windows Search** は、Windows Server の組み込み機能ですが、デフォルトで有効になりません。

次の手順に従って有効にする必要があります。

- サーバーマネージャで **ファイルサービス** という名前の役割を追加/インストールします。
- **Windows Search サービス**を有効にして開始する必要があります。

注意: 要件が満たされない場合は、ネットワークデータソースで検索を実行できません。

ファイル名検索のローカル データ ソースのインデックスを作成

デフォルトでは、インデックス検索がすべてのゲートウェイ サーバーで有効です。インデックス検索は、ゲートウェイの [**サーバーの編集**] ダイアログでゲートウェイサーバーごとに無効または有効にすることができます。

デフォルト パス

スタンドアロンサーバーのデフォルトでは、Files Advanced は Files Advanced ゲートウェイサーバーアプリケーションフォルダ内の **Search Indexes** ディレクトリにインデックス

ファイルを保存します。別の場所にインデックス ファイルを保存する場合は、新しいフォルダのパスを入力します。

利用可能な場合、Microsoft Windows Search を使用してコンテンツ検索をサポート

共有フォルダのコンテンツ検索のサポートはデフォルトで有効になっており、このオプションを有効することによって有効または無効にすることができます。コンテンツ検索は、ゲートウェイサーバーごとに有効または無効にすることができます。

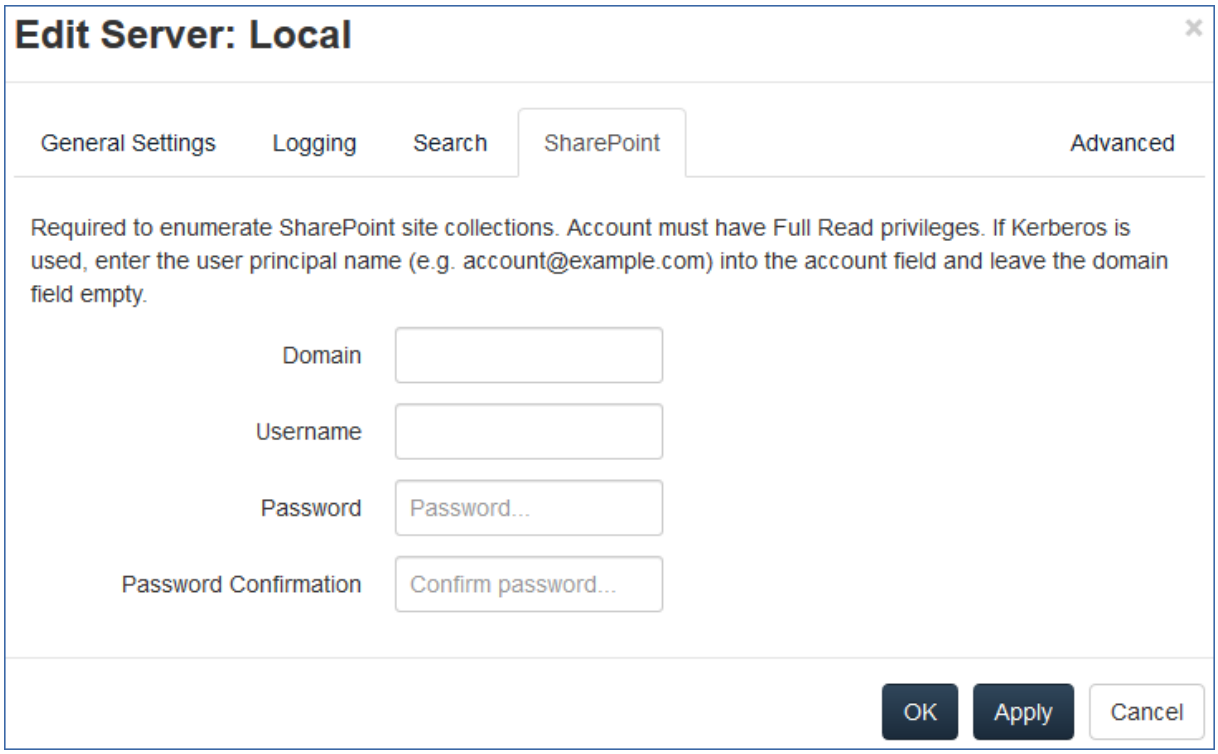
Windows Search で必要なデータソースをインデックス化するように設定するには、スタートバーの [Windows Search] アイコンを右クリックし、**[Windows Search のオプション]** を選択します。Windows の Reshare で Windows のコンテンツ検索を実行できますが、リモート コンピュータはゲートウェイ サーバーと同じドメインに参加している必要があります。

注意: Windows の Reshare でコンテンツ検索を使用する場合は、データ ソースのボリューム パスはホスト名か完全な修飾子名にする必要があります。IP アドレスは Windows Search ではサポートされていません。

その他の構成

コンテンツ検索インデックス化は、特定のファイルタイプのコンテンツのみをインデックス化するように設定できます。

1. ゲートウェイサーバーをホストしているサーバーで、**[コントロール パネル]** -> **[インデックスのオプション]** を開きます。
2. **[詳細設定]** を選択して、**[ファイルの種類]** タブを開きます。
3. コンテンツ検索を有効/無効にするファイルの種類（**doc** や **txt**)を探します。
4. 必要なファイルの種類を選択して、**[このファイルのインデックスの作成方法]** で、このファイルの種類のコンテンツ検索を有効にする場合は **[プロパティとファイルのコンテンツのインデックスを作成する]** を、無効にする場合は **[プロパティのみインデックスを作成する]** を選択します。必要なすべてのファイルの種類に対してこのステップを繰り返します。



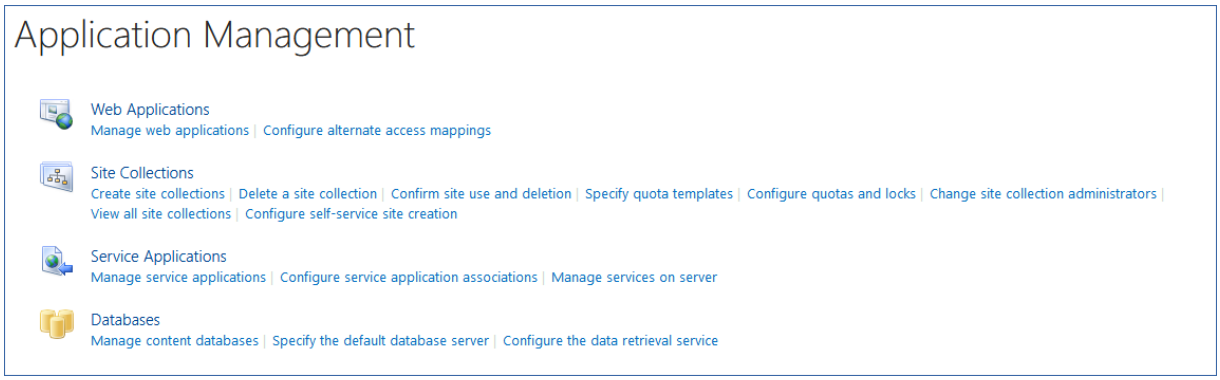
これらの認証情報の入力は一般的な SharePoint のサポートでは任意ですが、サイト コレクションを列挙するには必須です。たとえば、次の 2 つのサイトコレクションがあるとします。

http://sharepoint.example.com および
http://sharepoint.example.com/SeparateCollection.

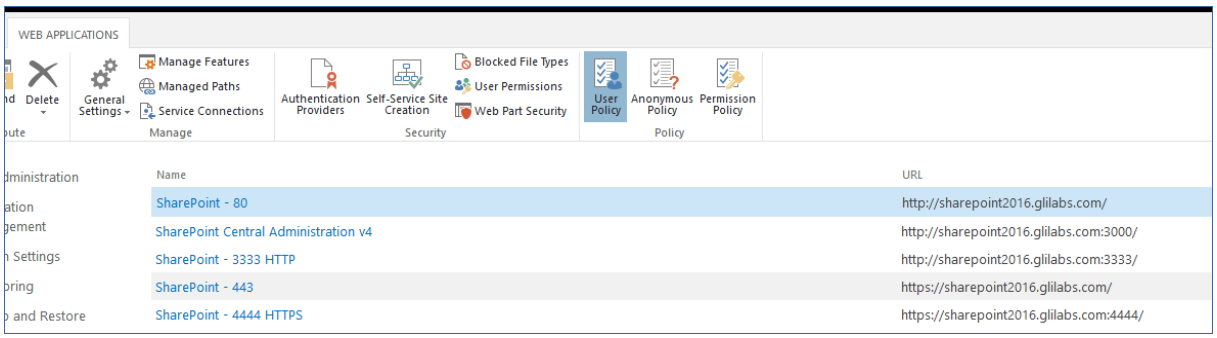
資格情報を入力しないと、**http://sharepoint.example.com** をポイントするボリュームを作成する場合、ボリュームを列挙するときに**SeparateCollection** というフォルダが表示されません。アカウントには、ウェブアプリケーションに対する**すべて読み取り**アクセスが必要です。

アカウントにすべて読み取り許可を与えるには（SharePoint 2016 および SharePoint 2010 の場合):

1. **[SharePoint のサーバー管理]** を開きます。
2. **[アプリケーション構成の管理]** をクリックします。

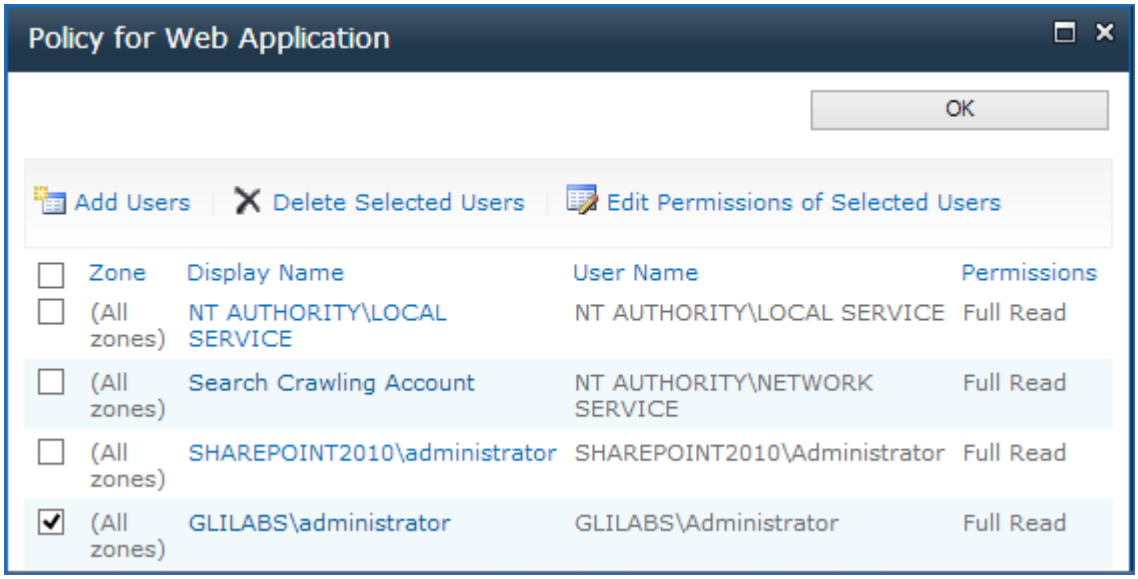


3. **[Web アプリケーション]** で **[Web アプリケーションの管理]** をクリックします。
4. ウェブ アプリケーションをリストから選択し、**[ユーザー ポリシー]** をクリックします。

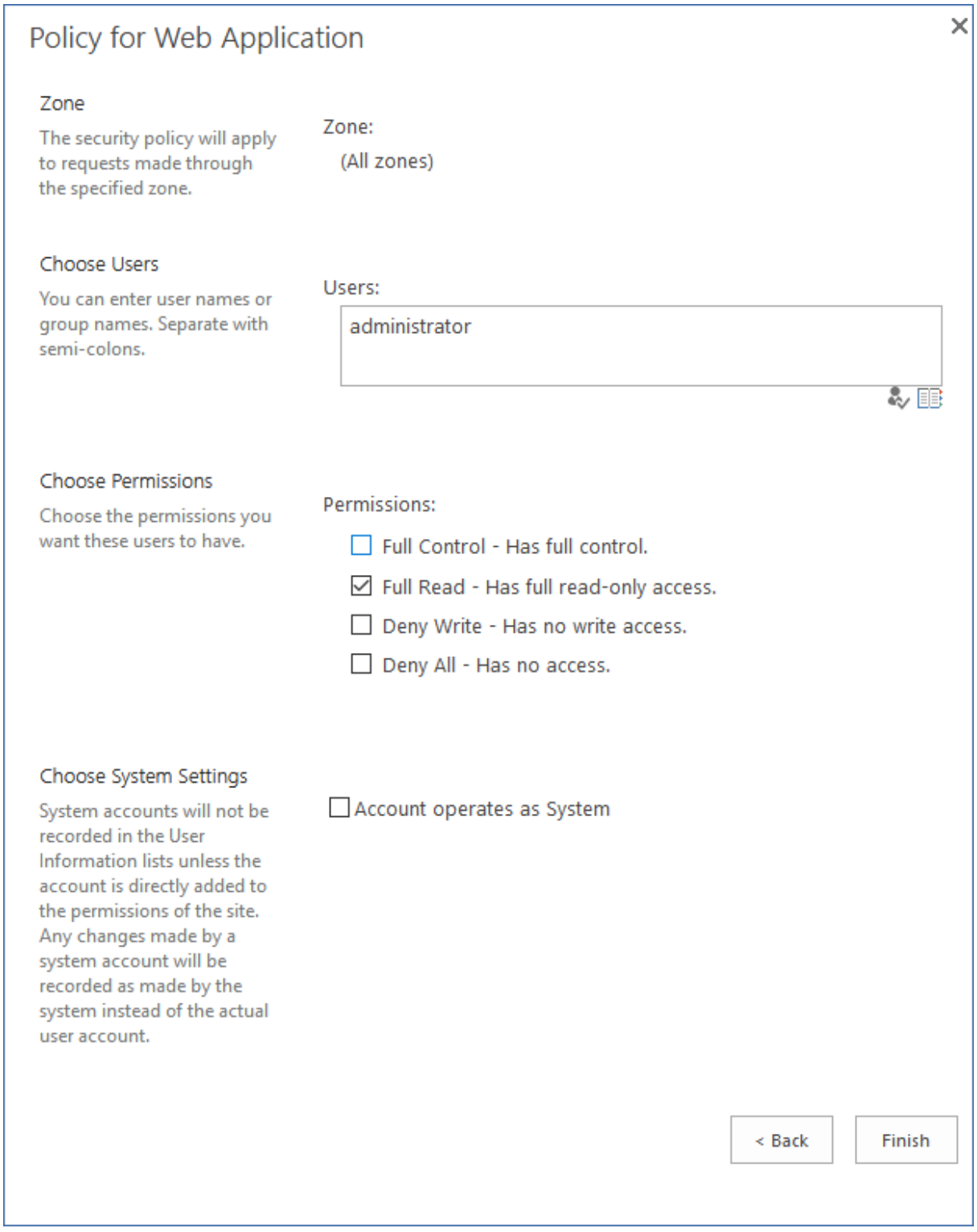


5. 権限を与えるユーザーのチェックボックスをオンにして、**[選択したユーザーの権限の編集]** をクリックします。ユーザーがリストに表示されない場合は、**[ユーザーの追加]** を

クリックしてそのユーザーを追加できます。



6. **[アクセス許可ポリシー レベル]** セクションから **[すべて読み取り - すべてに読み取り専用のアクセス権を持ちます]** のチェックボックスをオンにします。



7. **[保存]** ボタンを押します。

注意: これらの設定は、カスタマ サポート担当者の要求があった場合のみ変更することをお勧めします。

- **アクセスできない項目を非表示にする**: 有効にしている場合、 ユーザーに読み取り許可がないファイルおよびフォルダは表示されません。
- **Reshare 上のアクセスできない項目を非表示にする**: 有効にしている場合、 ユーザーに読み取り許可がない Network Reshare 上にあるファイルおよびフォルダは表示されません。

  注記: この機能を有効にすると、フォルダ閲覧中に非常に大きな悪影響があります。

- **アクセスできない SharePoint サイトを非表示にする**: 有効にしている場合、 ユーザーに必要な許可がない SharePoint サイトは表示されません。
- **最小 Android クライアント バージョン**: 有効にしている場合、 このゲートウェイ サーバーに接続しているユーザーには、Files Advanced Android クライアント アプリケーションのこれ以降のバージョンが要求されます。
- **最小 iOS クライアント バージョン**: 有効にしている場合、 このゲートウェイ サーバーに接続しているユーザーには、Files Advanced iOS クライアント アプリケーションのこれ以降のバージョンが要求されます。
- **SharePoint 認証に Kerberos を使用する**: SharePoint サーバーで Kerberos 認証が必要な場合、この設定を有効にする必要があります。また、ゲートウェイ サーバー ソフトウェアを実行している 1 台または複数の Windows サーバーの Active Directory コンピュータ オブジェクトをアップデートする必要があります。Files Advanced Windows サーバーには、ユーザーの代理として SharePoint サーバーに委任認証情報を提示する許可を与える必要があります。Files Advanced Windows サーバーによる Kerberos 委任の実行を有効にするには、次のことを実行します。

  1. [**Active Directory ユーザーとコンピュータ**] で、ゲートウェイ サーバーがインストールされている 1 台または複数の Windows サーバーを探します。それらのサーバーは、通常、**Computers** フォルダにあります。
  2. Windows サーバーの [**プロパティ**] ウィンドウを開き、[**委任**] タブを選択します。
  3. [**指定されたサービスへの委任でのみこのコンピュータを信頼する**] を選択します。
  4. [**任意の認証プロトコルを使う**] を選択します。これは SharePoint サーバーとのネゴシエーションに必要です。
  5. ここで、ユーザーが Files Advanced を使用してアクセスできるようにする任意の SharePoint サーバーを追加する必要があります。SharePoint 実装が、複数の負荷分散ノードで構成されている場合、許可を受けたコンピュータのリストに各 SharePoint/Windows ノードを追加する必要があります。[**追加...**] をクリックして、AD 内でこれらの Windows コンピュータを検索し、追加します。追加するたびに、「http」サービス タイプのみを選択します。

注記: これらの変更が AD を介して伝播し、適用されて、クライアントの接続性をテストできるようになるまで、15 ～ 20 分ほどお待ちください。変更はすぐには反映されません。

- **自己署名証明書を使用した SharePoint サーバーへの接続を許可**: 有効にしている場合、 自己署名した証明書を使用して、このゲートウェイから SharePoint サーバーへの接続を許可します。
- **ゲートウェイサーバーからの自己署名証明書を承認**: 有効にしている場合、 自己署名した証明書を使用して、このゲートウェイから Files Advanced サーバーに接続できます。
- **自己署名証明書を使用した Files Advanced サーバーへの接続を許可**: 有効にしている場合、 自己署名した証明書を使用して、他の Files Advanced サーバーへの接続を許可します。
- **非表示の SMB 共有の表示**: 有効にしている場合、 非表示のシステム SMB 共有をユーザーに表示します。
- **クライアント セッション タイムアウト（分)**: 非アクティブなユーザーがゲートウェイサーバーから排除されるまでの時間を設定します。
- **ユーザー プリンシパル名 (UPN)を使用した SharePoint サーバーの認証**: 有効にしている場合、ユーザーは各自のユーザー プリンシパル名 (例: hristo@glilabs.com)を通じて SharePoint サーバーへの認証を行います。有効にしていない場合は、ドメインとユーザー名の組み合わせ（例: glilabs/hristo)を使用して認証を行います。
- **ユーザーモードでネゴシエート/Kerberos 認証を実行します**: 有効にすると、ゲートウェイサーバーは、接続しているユーザーの Kerberos チケットを使用して、データソースに対して認証を行います。これは、Kerberos (シングルサインオンや負荷分散など)を必要とする構成でのみ使用されます。

[ポリシー] 『70ページ 』 セクションのデフォルトアクセス制限セットを使用するか、ゲートウェイサーバーごとにカスタムアクセス制限を設定できます。

特定のゲートウェイサーバーのカスタムアクセス制限の設定

1. **[モバイルアクセス]** → **[ゲートウェイサーバー]** タブに移動します。
2. 必要なサーバーの **[詳細]** の横にある矢印をクリックします。
3. **[アクセス制限]** を選択します。
4. **[カスタム設定の使用]** タブを開きます。
5. このゲートウェイサーバーに適用する、特定のアクセス制限を選択します。

6. **[適用]** を押します。

6.4.4 クラスタグループ

Files Advancedのバージョン5.1以降では、ゲートウェイサーバーのクラスタグループを作成できます。

クラスタグループは、同じ構成を共有する複数のゲートウェイサーバーの集まりです。このグループにより、グループ内のすべてのゲートウェイを一度に制御することができ、各ゲートウェイ上で個別に同じ設定をする必要がなくなります。通常、モバイルクライアントに高可用性とスケーラビリティを提供するため、これらのサーバーは負荷分散装置 『247ページ 』の背後に配置されます。

クラスタ化されたゲートウェイ設定の場合、負荷分散装置、2 つ以上のゲートウェイ、および Files Advanced サーバーが必要になります。すべてのゲートウェイ サーバーは、Files Advanced ウェブ インターフェイスでクラスタ グループに追加し、負荷分散装置の背後に配置する必要があります。Files Advanced サーバーは、管理サーバー、およびモバイル クライアントがクライアント管理に登録するサーバーとして機能します。このサーバーでは、ポリシー、デバイス、および設定のすべてが管理されます。一方、ゲートウェイでは、ファイル共有へのアクセスが提供されます。

クラスタグループを作成するには、次の手順を実行します。

続行する前に、各ゲートウェイ上で正しい**管理のアドレス**が設定済みであることを確認してください。これは、ゲートウェイ サーバーの DNS アドレスまたは IP アドレスです。

1. Files Advanced ウェブ インターフェイスを開きます。
2. **[モバイル アクセス]** タブを選択します。
3. **[ゲートウェイ サーバー]** ページを開きます。
4. **[クラスタ グループの追加]** ボタンを押します。
5. グループの表示名を入力します。
6. 負荷分散装置の FQDN または IP アドレスを入力します。

7. 必要に応じて、Files Advanced サーバー接続に別のアドレスを選択することもできます。選択する場合は、チェックボックスをオンにして、アドレスを入力します。
8. グループに含めるそれぞれのゲートウェイのチェックボックスにマークを付けます。
9. グループの設定を制御するゲートウェイを選択します。そのゲートウェイ上の既存の設定のすべて（割り当てられているデータ ソースは含まれますが、管理のアドレスは含まれません)が、グループ内の各ゲートウェイにコピーされます。
10. **[作成]** を押します。

クラスタグループの編集:

クラスタグループの編集作業は、標準的なゲートウェイを編集する作業と違いはありません。詳細については、「ゲートウェイサーバーの編集 『119ページ 』」の資料を参照してください。

既存のクラスタ グループにメンバーを追加するには、次の操作を実行します。

1. ウェブインターフェイスを開き、**[モバイルアクセス]**→**[ゲートウェイサーバー]**に移動します。
2. 目的のクラスタ グループの操作メニューを開き、選択可能な操作から **[クラスタ メンバーの追加]** を選択します。
3. リストから目的のゲートウェイ サーバーを選択し、**[追加]** を押します。

マスターゲートウェイサーバーの変更:

1. ウェブインターフェイスを開き、**[モバイルアクセス]**→**[ゲートウェイサーバー]**に移動します。
2. 目的のクラスタグループを展開します。
3. マスターに昇格させるゲートウェイサーバーを見つけます。
4. **[操作]**ボタンを押して、**[グループマスターにする]**を選択します。

6.5 データソースの管理

Files Advanced ユーザーがアクセスできるように、Windows サーバー、CMIS システム、またはリモート SMB/CIFS ファイル共有上に存在する NTFS ディレクトリを共有することができます。ユーザーが接続すると、これらのディレクトリがファイル共有ボリュームとして表示されます。

SharePoint 2007、2010、2013、2016、365 のコンテンツへのアクセス

Files Advanced を使用すると、SharePoint 2007、2010、2013、2016、および 365 サーバーのドキュメントライブラリ内に存在するファイルにアクセスできます。Files Advanced SharePoint データソースは、SharePoint サーバー全体、特定の SharePoint サイトまたはサブサイト、特定のドキュメントライブラリを指し示すことができます。これらのファイルは、従来のファイルサーバーや NAS ストレージに存在するファイルと同じように、開いたり、PDF に注釈を付けたり、編集、同期などを実行することができます。Files Advanced は、SharePoint ファイルの**チェックアウト**と**チェックイン**もサポートしています。

SharePoint の認証方法をサポート

Files Advanced は NTLMv1、NTLMv2、クレームベース、Kerberos を使用したクライアント認証が可能な SharePoint サーバーをサポートしています。SharePoint サーバーで Kerberos 認証を必要とする場合、Windows サーバー、または Files Advanced サーバーソフトウェアが実行されているサーバーの Active Directory コンピュータオブジェクトをアップデートする必要があります。Files Advanced Windows サーバーには、ユーザーの代理として SharePoint サーバーに委任認証情報を提示する許可を与える必要があります。

クレームベース認証では、認証サーバーでの認証、認証トークンの取得、SharePoint サーバーへのトークンの提供が行われます。SharePoint サーバーで直接認証が行われるわけではありません。Acronis Access では、Office 365 SharePoint サイトへのクレームベース認証がサポートされています。認証を行う場合、初めに、ゲートウェイサーバーは Microsoft Online に接続し、認証サーバーの場所を特定します。このサーバーは、Microsoft Online に

よってホストされていることもあれば、（Active Directory フェデレーション サービスを介して)企業ネットワーク内に存在することもあります。認証が完了すると、バイナリのセキュリティトークンが取得され、このトークンが SharePoint サーバーに送信されます。このことにより SharePoint から認証 Cookie が返されます。その後は、この Cookie が他のユーザーの資格情報の代わりとして SharePoint に提供されます。

OneDrive for Businessコンテンツへのアクセス

ユーザーが SharePoint データソース経由で自分個人の OneDrive for Business コンテンツにアクセスできるように、Files Advanced をセットアップすることができます。いくつかの要件と制限があります。

共有ファイルおよびフォルダの許可の変更

Files Advanced は、既存の Windows のユーザーアカウントとパスワードを使用します。Files Advanced では Windows NTFS 許可が実行されるため、通常は Windows に組み込まれているツールを使って、ディレクトリとファイルの許可を調整してください。標準の Windows ツールは、セキュリティ ポリシーを設定するための最も柔軟な手段です。

別の SMB/CIFS ファイルサーバーに存在する Files Advanced データソースは、ゲートウェイサーバーからセカンダリサーバーまたは NAS への SMB/CIFS 接続によってアクセスされます。この場合、セカンダリサーバーへのアクセスは、Access クライアントの 1 つにログインしているユーザーのコンテキストで実行されます。ユーザーがセカンダリサーバー上のファイルにアクセスできるようにするには、ユーザーのアカウントに、それらのファイルにアクセスするための「Windows 共有のアクセス許可」と NTFS セキュリティ許可の両方が必要です。

SharePoint サーバーに存在するファイルへの許可は、SharePoint サーバーで設定されている SharePoint のアクセス許可に従って管理されます。ユーザーは Files Advanced を介して許可が与えられます。この許可はウェブブラウザで SharePoint ドキュメントライブラリにアクセスする際に与えられるものと同じです。

セクションの内容

6.5.1 フォルダ

フォルダに対して Files Advanced のユーザーポリシーおよびグループポリシーを割り当てることができ、これにより、ユーザーの Files Advanced アプリにフォルダが自動的に表示されるようになります。ゲートウェイサーバー、リモート共有、CMIS ボリューム、さらには SharePoint Library であっても、そこにある任意のフォルダにポイントするように、フォルダを設定できます。そうすることでユーザーは、そのフォルダまで場所を探しながら移動する必要はなくなり、サーバー、共有ボリューム名、およびフォルダへのパスを正確に知らなくても、自分にとって重要なフォルダに直接アクセスできるようになります。

フォルダには、種類を問わず Files Advanced がアクセスを提供するコンテンツすべてをポイントできます。これにより、Files Advanced 管理内で既に構成されているゲートウェイサーバー内でのロケーションが参照されます。ロケーションには、ローカルのファイル共有ボリューム、他のファイルサーバーや NAS 上のファイルへのアクセスを提供する「Network Reshare」ボリューム、DFS 共有、CMIS ボリューム、SharePoint ボリュームなどがあります。

注意: DFS のデータ ソースを作成する場合は、次のようにフル パスを DFS に追加する必要があります。

¥¥company.com¥namespace¥share

注意: Files Advanced をクリーン インストールする際、同期と共有を有効にしていて、ゲートウェイ サーバーが存在する場合は、同期と共有のデータ ソースが自動的に作成されます。初期設定の **[サーバー]** セクションで設定した URL をポイントします。モバイル ユーザーはこのフォルダを使用して、同期と共有のファイルおよびフォルダにアクセスできるようになります。

フォルダの同期

オプションで、フォルダをクライアント デバイスに同期するように設定できます。Files Advanced フォルダ同期オプションは次のとおりです。

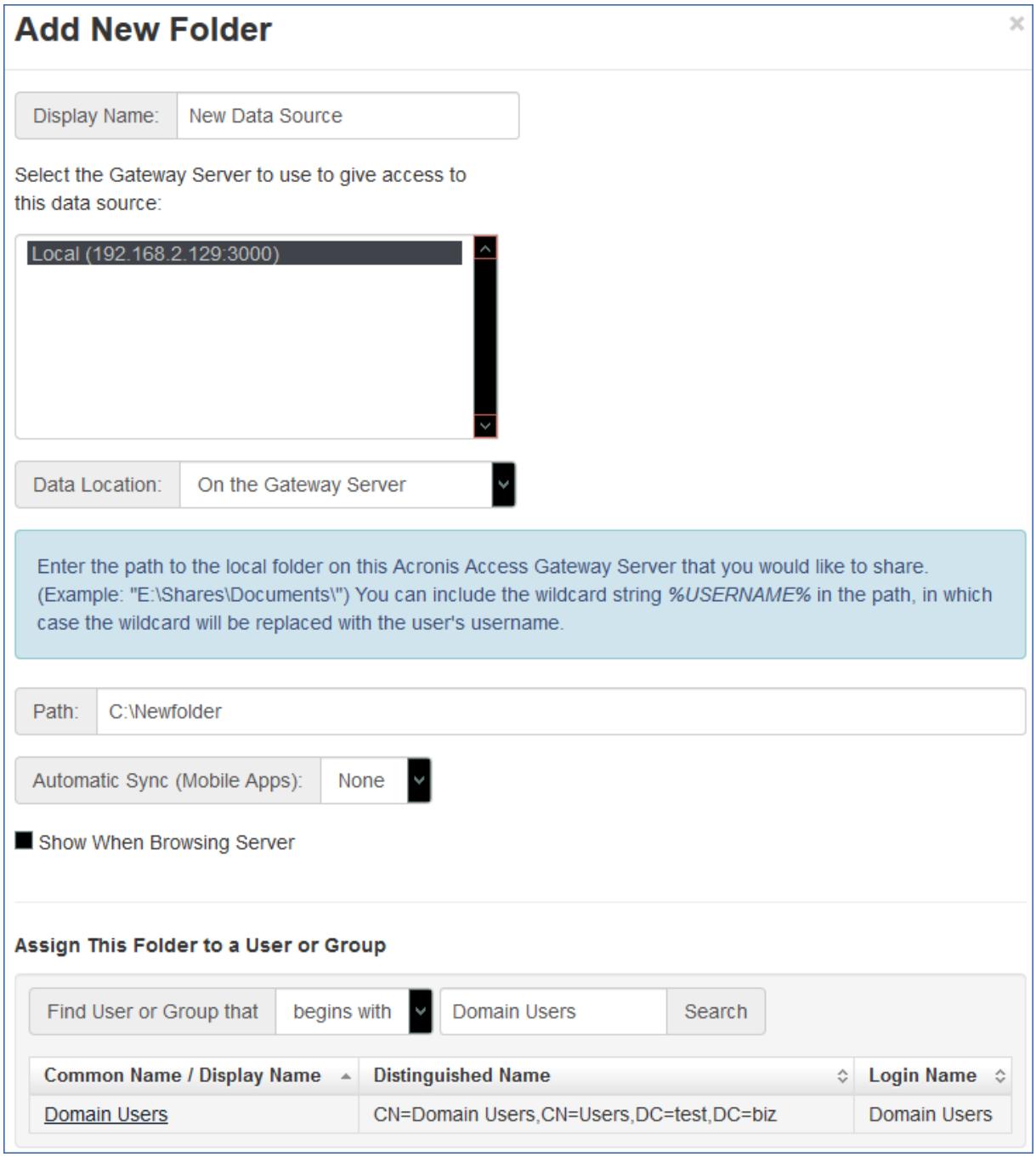
注意: この設定は、デスクトップ クライアントには影響しません。

- **なし**: フォルダは、Files Advanced アプリにネットワーク ベースのリソースとして表示され、ゲートウェイサーバーとまったく同じようにアクセスおよび操作できます。
- **一方向**: このフォルダは、Files Advanced アプリに、ローカル フォルダとして表示されます。フォルダの内容全体がサーバーからデバイスへ同期され、サーバー上のファイルの追加、変更、または削除が発生した場合、最新の状態が反映されます。このフォルダは、サーバー ベースのファイルにローカルまたはオフラインでアクセスするためのものであり、ユーザーに対しては読み込み専用フォルダとして表示されます。
- **二方向**: このフォルダは、Files Advanced アプリに、ローカル フォルダとして表示されます。最初に、フォルダの内容全体がサーバーからデバイスへ同期されます。デバイスかサーバーのどちらかでこのフォルダ内のファイルが追加、変更、または削除されると、その変更内容が対応するサーバーまたはデバイスにも同期されます。

データ ソースの作成

1. Files Advanced ウェブ インターフェイスを開きます。
2. **[モバイル アクセス]** タブを選択します。
3. **[データ ソース]** タブを開きます。
4. **[フォルダ]** に移動します。

5. **[新しいフォルダの追加]** ボタンを押します。



6. フォルダの表示名を入力します。
7. フォルダへのアクセスを提供するゲートウェイ サーバーを選択します。
8. データのロケーションを選択します。ロケーションとして、実際のゲートウェイ サーバー、他の SMB サーバー、SharePoint サイトまたはライブラリ、同期と共有サーバー上を選択できます。

注意: 同期と共有を選択するときは、必ずサーバーのフル パスをポート番号と共に入力してください（例: https://mycompany.com:3000)。

9. ロケーションの選択に基づき、フォルダ、サーバー、サイトまたはライブラリへのパスを入力します。
10. フォルダの**同期**タイプを選択します。
11. Files Advanced モバイル クライアントがゲートウェイ サーバーを参照した場合に、このデータ ソースが表示されるようにするには **[サーバーの参照時に表示する]** を有効にします。

注意: SharePointのデータソースを作成するときに、SharePointフォローサイトの表示を有効化するオプションがあります。

12. [保存] ボタンをクリックします。

データソースの編集

1. **[データソース]** セクションを開いて、編集するデータソースを見つけます。
2. テーブルの右側にデータソース用に表示される **[鉛筆]** アイコンをクリックします。
3. 目的のパラメータを変更し、**[保存]** を押します。

データソースを作成することで、Files Advanced モバイルユーザーは SharePoint のサイトおよびライブラリに簡単にアクセスできるようになります。SharePoint のデータ ソースを作成する方法は 2 つあり、SharePoint の設定により異なります。

データ ソースの作成: SharePoint サイトまたはサブサイト全体

データ ソースの作成: 単一の **SharePoint サイト**または**サブサイト**の場合、**[URL]** フィールドにのみ入力する必要があります。SharePoint のサイトまたはサブサイトのアドレスを入力してください。

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

SharePoint フォローサイト

SharePoint フォローサイトは、サイトのデータソースを作成する際に有効化できます。これは [フォローサイトを表示する] チェックボックスで行います。有効化した場合、サイトをフォローするすべてのユーザー側で、Files Advanced にフォルダ「フォローサイト」が表示されます。このフォルダには、当該サイトからのアクセス許可があるリソースが含まれます。

注意: SharePoint フォローサイトは同期されません。

データ ソースの作成: 単一の SharePoint ライブラリ

データ ソースの作成: 単一の SharePoint ライブラリの場合、**[URL]** と **[ドキュメントライブラリ名]** の 2 つのフィールドに入力する必要があります。 URL フィールドには SharePoint のサイトまたはサブサイトのアドレスを入力し、[ドキュメント ライブラリ名] にはライブラリ名を入力します。

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

データ ソースの作成: SharePoint ライブラリ内の特定のフォルダ

データ ソースの作成: SharePoint ライブラリ内の特定のフォルダの場合、すべてのフィールドに入力する必要があります。 URL フィールドには SharePoint のサイトまたはサブサイトのアドレスを入力し、[ドキュメント ライブラリ名] にはライブラリ名を入力します。また、[サブパス] フィールドには指定するフォルダの名前を入力します。

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

注意: サブパスで SharePoint にポイントするデータソースを作成する場合、**[サーバーの参照時に表示する]** オプションを有効にすることはできません。

Files Advanced モバイルでは、NTLM 認証、Kerberos 制約付き委任認証、クレームベース認証、および SharePoint 365 認証がサポートされています。SharePoint の設定によっては、データ ソースへの接続に使用するゲートウェイ サーバーで追加設定が必要になる場合があります。詳細については、「ゲートウェイサーバーの編集 『119ページ 』」の資料を参照してください。

サポートされている CMIS ボリュームは、**Alfresco（CMIS)**ボリュームと **Documentum（CMIS)**ボリュームです。また、**[汎用 CMIS（AtomPub)]** オプションで、**AtomPub** プロトコルが使用されている他の CMIS ベンダの使用を試みることもできます。このオプションは、ベンダによって機能する場合と機能しない場合があり、Acronis ではサポートされていません。

低速のネットワークでタイムアウトの発生を少なくするために、CMIS ボリュームをホストしているマシンにゲートウェイサーバーを配置することをお勧めします。

注意: CMIS ボリュームには、フォルダをコピーできないという制限があります。

OneDrive for Business は SharePoint ベースなので、Files Advanced に SharePoint データソースを作成することによって、そのコンテンツにアクセスできます。その場合でも、いくつかの制限があります。

- データソースがユーザーのメインの個人フォルダのワイルドカードをポイントしている**必要があります**。サブフォルダをポイントするデータソースを作成することはできませんが、サブフォルダへはメインフォルダからアクセスおよび参照可能です。
- ゲートウェイサーバーがアプリに手動で追加された場合は、このように設定したデータソースを使用することはできません。データソースはポリシーで割り当てる必要があります。
- Active Directory を Office 365 でリンクして Federated AD サービスを使用するか、または Active Directory を Azure AD にする必要があります。
- 各ユーザーは自分の OneDrive データのみ表示することができ、Microsoft ポータル経由で共有されてアクセス可能であっても、他のユーザーのデータにはアクセスできません。

データソースの作成

1. Files Advanced ウェブ インターフェイスを開きます。
2. **[モバイル アクセス]** タブを選択します。
3. **[データ ソース]** タブを開きます。
4. **[フォルダ]** に移動します。
5. **[新しいフォルダを追加]** ボタンを押します。
6. フォルダの表示名を入力します。
7. リソースへのアクセスを提供するゲートウェイサーバーを選択します。
8. ユーザーの OneDrive for Business メインサイトのロケーションの後に、個人フォルダのパスを**%USERNAME%**ワイルドカードを使用して入力します。

   例: **`https://mycompany.sharepoint.com/personal/%USERNAME%`**

9. **[保存]** ボタンを押します。

Active Directory統合

注意: Active Directory や Microsoft Azure の管理は Files Advanced の機能では**ありません**。Azure または Office 365 で問題が発生する場合は、**Microsoft サポート**にお問い合わせください。

Office 365 では、Azure Active Directory サービスによるクラウドベースのユーザー識別情報管理を使用して、ユーザーを管理します。すでに Azure AD サービスを使用している場合は、データソースの作成のみ必要です。

Azure AD サービスを使用していない場合は、オンプレミス環境を Office365 と同期することにより、オンプレミス Active Directory を Azure AD と統合することができます。

3 つ目のオプションは、必要なアカウントを Office 365 に手動で再作成する方法ですが、これは使用するアカウントの数が非常に少ない場合にしかお勧めできません。

6.5.2 割り当て済みのソース

このページでは、ユーザーまたはグループを検索して、どのりソースが割り当てられているかを確認できます。リソースは、2 つの表（サーバーとフォルダ)に一覧表示されます。

- サーバーの表には、ゲートウェイ サーバーの表示名、DNS または IP アドレス、およびこのサーバーが割り当てられているポリシーが一覧表示されます。
- フォルダの表には、データ ソースの表示名、ゲートウェイ サーバー、同期タイプ、パス、およびこのデータ ソースが割り当てられているポリシーが一覧表示されます。
- 管理者は**[X に割り当てられたリソースの編集]** ボタンを押すことで、このポリシーに対する割り当てをすばやく編集することができます。

6.5.3 クライアントで表示されるゲートウェイ サーバー

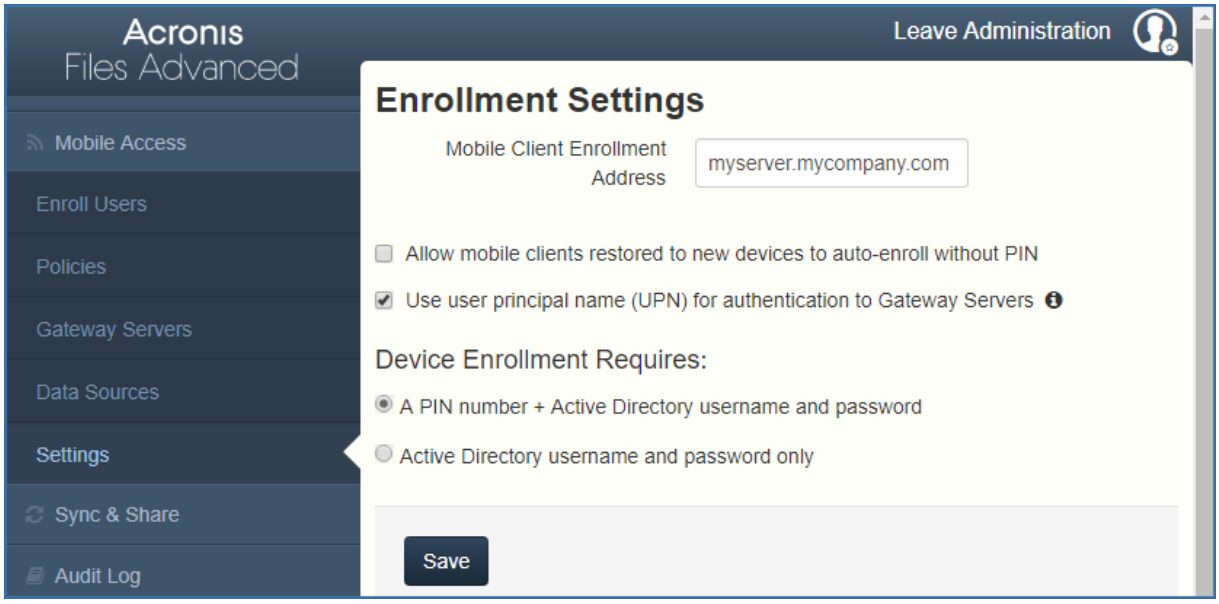
ゲートウェイ サーバーをユーザー ポリシーまたはグループ ポリシーに割り当て、データ ソースとして使用できます。このページには、ユーザーの Files Advanced モバイルアプリに表示されるすべてのゲートウェイサーバーと、それらのゲートウェイサーバーがユーザーポリシーまたはグループポリシーに割り当てられているかどうかが表示されます。この割り当てをここで編集することもできます。Files Advanced モバイルユーザーがゲートウェイ

サーバーを参照すると、**[ゲートウェイサーバーの参照時に表示]** オプションが有効になっているデータソースが表示されます。

サーバーの現在の割り当てを編集するには

1. そのサーバーの **[編集]** ボタンを押します。
   - このサーバーの割り当てをユーザーから解除する場合は、そのユーザーの **[X]** を押します。
   - 新しいユーザーまたはグループをこのサーバーに割り当てる場合は、ユーザー名またはグループ名を探してそれを押します。
2. **[保存]** ボタンを押します。

6.6 設定



登録設定

- **モバイル クライアント登録アドレス**: クライアント管理の登録時にモバイル クライアントが使用するアドレスを指定します。

  注意: モバイル クライアント登録アドレスに FQDN を使用することを強くお勧めします。クライアント管理への登録に成功すると、Files Advanced モバイル アプリによって Files Advanced サーバーのアドレスが保存されます。そのアドレスが IP アドレスで、そのアドレスが変更された場合、ユーザーはサーバーに接続できなくなり、アプリケーションを非管理にはできないため、アプリケーション全体を削除して管理に再登録する必要があります。

- **モバイル クライアントを新しいデバイスに復元した場合でも、PIN コードなしで自動登録されるようにする**: この設定を有効にすると、以前のバージョンの Files Advanced モバイルによって管理されていたユーザーが PIN コードを使用せずに新しいサーバーに登録できるようになります。
- **ユーザー プリンシパル名（UPN)を使用したゲートウェイ サーバーの認証**: この設定を有効にすると、ユーザーは UPN（例: user@company.com)を使用してゲートウェイ サーバーに対する認証を行います。無効にした場合は、ユーザーはドメイン名とユーザー名の組み合わせ（例: domain/user)を使用して認証を行います。

デバイスの登録に必要なもの:

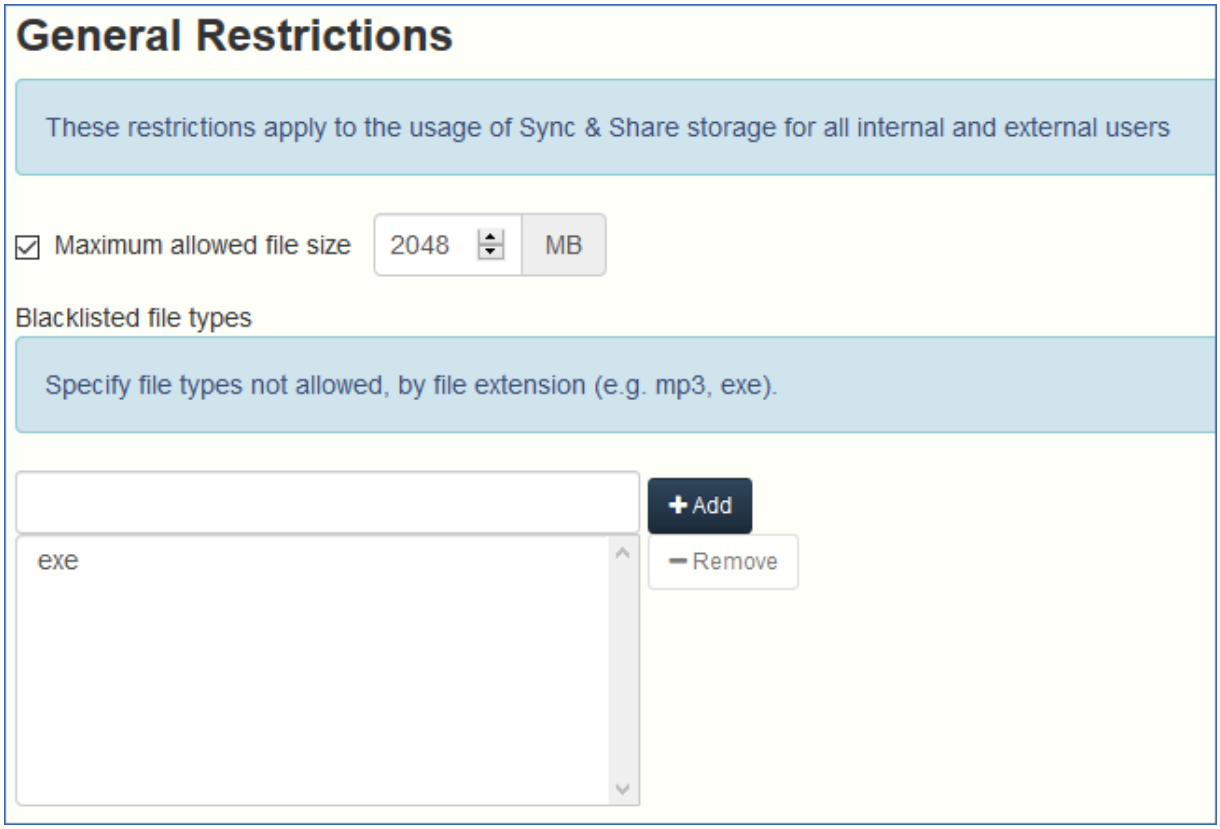
- **PIN コード + Active Directory のユーザー名とパスワード**: ユーザーは、自分の Files Advanced アプリケーションをアクティブ化して Files Advanced サーバーにアクセスするために、有効期限が設定されたワンタイム PIN コードと有効な Active Directory ユーザー名およびパスワードの入力が求められます。このオプションを使用する場合、ユーザーは、IT 管理者によって発行された PIN コードを受け取った後に 1 台のデバイスのみ登録することができます。このオプションは、2 つの要素によるデバイス登録でセキュリティを強化する必要がある場合に推奨されます。
- **Active Directory のユーザー名とパスワードのみ**: ユーザーは Active Directory のユーザー名とパスワードのみを使用して Files Advanced アプリケーションをアクティブ化することができます。このオプションを使用すると、ユーザーが今後いつでも 1 台または複数のデバイスを登録することができます。ユーザーには、Files Advanced クライアント管理サーバーの名前、または Files Advanced クライアント管理サーバーをポイントする URL のみを提供する必要があります。この情報は、ウェブ サイトに掲示したり電子メールで送信したりできるので、多数のユーザーへの Files Advanced の導入を簡素化することができます。このオプションは、2 つの要素による登録が不要な環境や、多くのユーザーがいつでも Files Advanced にアクセスする必要がある環境（学生用の導入など)に推奨されます。

7 同期・共有

ウェブ インターフェイスのこのセクションは、同期と共有機能を有効にしている場合にのみ使用できます。有効にしていない場合は、**[同期と共有サポートを有効にする]** ボタンが表示されます。

セクションの内容

7.1 一般制限事項



ファイルの種類によるブラックリストや、指定サイズを超えるファイルの制限などの、基本的な制限事項を設定できます。

許可されている最大ファイルサイズ: 同期・共有のすべてのファイルに対して最大ファイルサイズを設定できます。

ブラックリストに含まれるファイルの種類: 同期・共有機能で特定のファイルの種類を使用することをブロックできます。

ファイルの種類のブラックリストを設定するには、次の手順を実行します。

1. ウェブコンソールで **[同期・共有]** タブを展開し、**[一般制限事項]** を開きます。
2. **[ブラックリストに含まれるファイルの種類]** の **[フィールドの追加]** で、ブロックするファイルの種類をすべてカンマ区切りで入力します。
3. **[保存]** を押します。

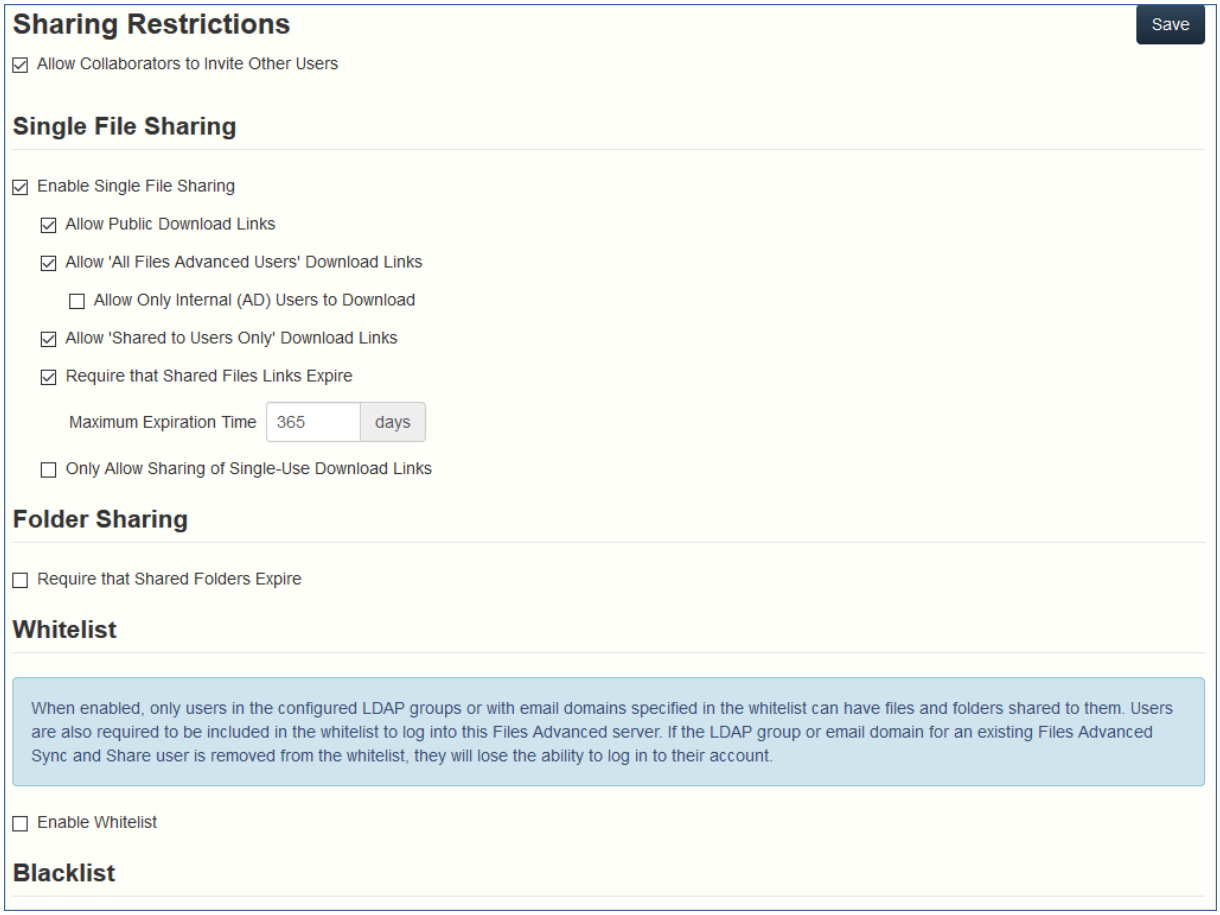
注意: 指定した種類のファイルが既に存在する場合、同期も移動もされなくなります。手動でのみ、ファイルのダウンロードおよび削除を実行できます。

ファイルの最大サイズを設定するには、次の手順を実行します。

1. ウェブコンソールで **[同期・共有]** タブを展開し、**[一般制限事項]** を開きます。
2. **[許可されている最大ファイルサイズ]** チェックボックスをオンにして、テキストフィールドに最大のファイルサイズ（MB 単位)を入力します。
3. **[保存]** を押します。

注意: 指定したファイルサイズより大きいファイルが既に存在する場合、同期も移動もされなくなります。手動でのみ、ファイルのダウンロードおよび削除を実行できます。

7.2 共有の制限



グループ作業者が他のグループ作業者を招待できるようにする: この設定が無効な場合、ユーザーをフォルダに招待するとき、**[グループ作業者が他のグループ作業者を招待できるよ**

うにする] チェックボックスは表示されません。これにより、招待されたユーザーが他のユーザーを招待できないようにします。

単一ファイル共有の有効期限

単一ファイル共有を有効にする: この設定が有効な場合、単一ファイルリンクを共有することができるようになり、ユーザーのリンクへのアクセス方法およびアクセス可能な期間を制御できます。

- **ダウンロードの公開リンクを許可する**: この設定が有効な場合、共有ファイルへのリンクを持っているすべてのユーザーがファイルにアクセスできます。
- **[すべての Files Advanced ユーザー] のダウンロードリンクを許可**: この設定が有効な場合、Files Advanced の認証情報を持っているユーザーのみが共有ファイルにアクセスできます。
  - **内部の（AD)ユーザー限定でダウンロードを許可する**: この設定が有効な場合、Files Advanced 用の Active Directory 認証情報を持っているユーザーのみが共有ファイルにアクセスすることができます。
- **共有済みユーザー専用のダウンロードリンクを許可**: この設定が有効な場合、共有済みユーザーのみがリンクを使用できます。
- **共有ファイルリンクの有効期限を必須にする**: この設定が有効な場合、ファイルリンクに有効期限が適用されます。
  - **最長有効期間**: ファイルの有効期限が終了するまでの最長期間（日単位)を制御します。
- **1 回限りのダウンロードリンクでの共有のみ許可する**: 有効にした場合、ユーザーは 1 回だけ使用できるリンクのみを送信できます。これらのリンクは 1 回目のダウンロード後に無効になります。

フォルダの共有

共有フォルダの有効期限を必須にする: この設定が有効な場合、すべての共有フォルダに有効期限を設定する必要があります。

- **最長有効期間**: フォルダの有効期限が終了するまでの最長期間（日単位)を制御します。

ホワイトリスト

ホワイトリストを有効にした場合、設定済みの LDAP グループ内のユーザーまたはリストで指定された電子メールドメイン(例: example.com)を使用するユーザーのみがログインできます。ドメインにワイルドカードを使用できます（例: *.example.com)。LDAP グループは、CN=mygroup,CN=Users,DC=mycompany,DC=com のように識別名で指定する必要があります。

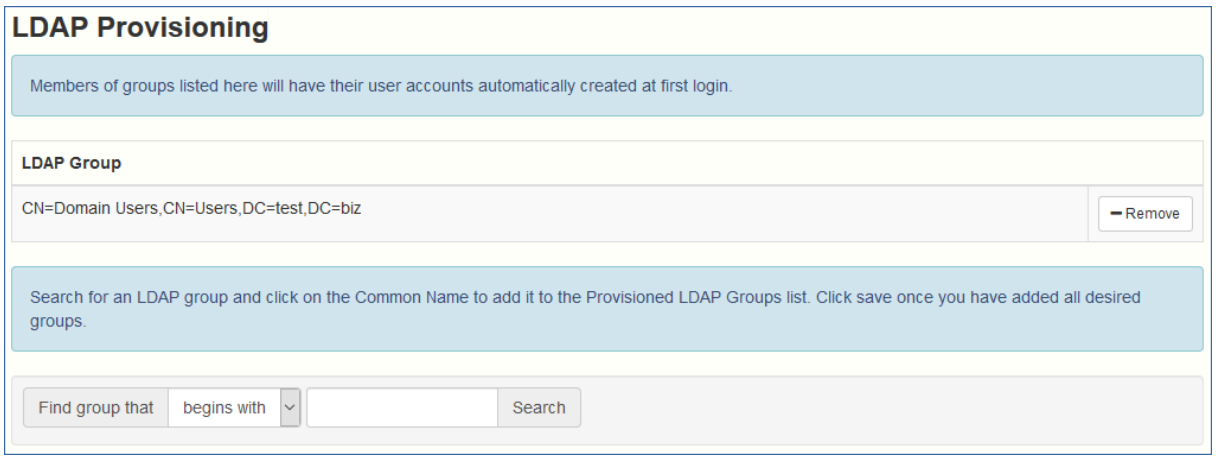
ブラックリスト

LDAP グループ内のユーザーまたはブラックリストで指定された電子メールドメイン（例: example.com)を使用するユーザーは、ホワイトリストに記載されていても、システムにログインできません。ドメインにワイルドカードを使用できます（例: *.example.com)。LDAP グループは、CN=mygroup,CN=Users,DC=mycompany,DC=com のように識別名で指定する必要があります。

注意: ワイルドカードのエントリは、* を 1 つのみ使用でき、必ず文字列の先頭に配置される必要があります。ワイルドカードの後にはピリオドが続きます（例: *.example.com、*.com)

7.3 LDAP プロビジョニング

ここに表示されているグループのメンバーは、初回ログイン時にユーザーアカウントが自動的に作成されます。そのためアカウント作成プロセスは簡単になり、管理者は各ユーザーに招待を送信する必要がありません。



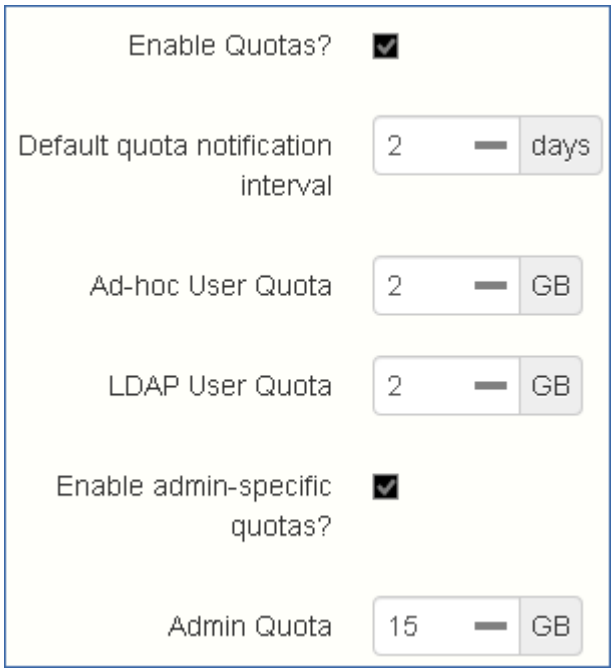
LDAP グループ

現在選択されているグループのリストです。

- **共通名/表示名** - ユーザーやグループに設定している表示名。
- **識別名** - ユーザーやグループに設定している識別名。識別名は、ディレクトリ サービスのエントリ用の固有の名前です。

7.4 クォータ

管理者は、システム内のユーザーごとに空き容量を設定できます。外部 (一時的な)ユーザーおよび内部（Active Directory - LDAP)ユーザー用の異なるデフォルト設定があります。
管理者は、個々のユーザーまたは Active Directory グループ メンバーシップに基づいて異なるクォータ値を割り当てることもできます。



- **クォータを有効にしますか？**: 有効にすると、一人のユーザーに割り当てられるクォータの最大領域が制限されます。
  - **デフォルトの通知間隔**: クォータ上限に近づいたユーザーに対する通知電子メールの受信頻度を設定する時間間隔（日単位)です。
  - **一時的なユーザーのクォータ**: 一時的ユーザーのクォータを設定します。
  - **LDAP ユーザーのクォータ**: LDAP ユーザーのクォータを設定します。

- **管理者固有のクォータを有効にしますか？**：有効にすると、管理者には他のクォータが割り当てられます。
    - **管理者のクォータ**：管理者用のクォータを設定します。

注記: 一人のユーザーが複数のグループのメンバである場合は、最大のクォータのみが適用されます。

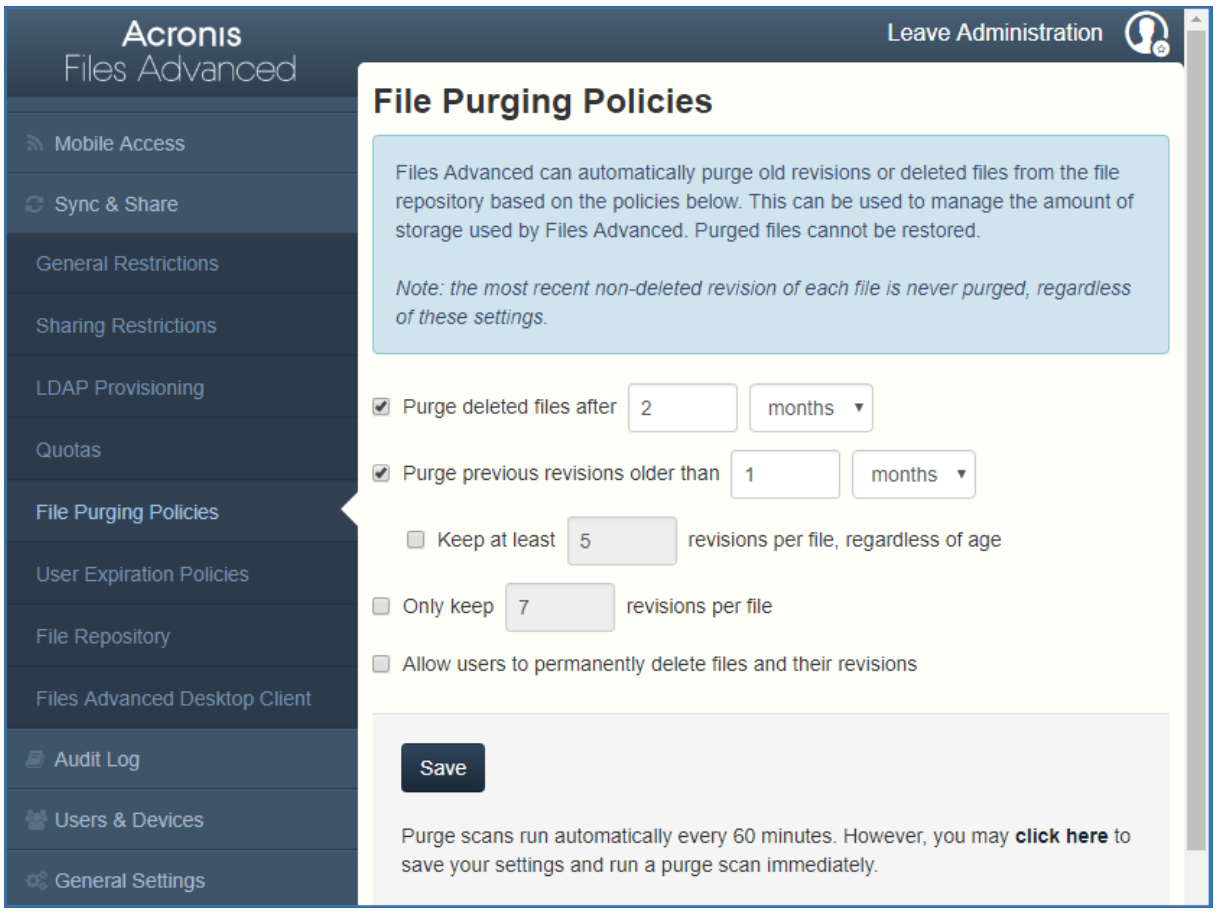
注意: クォータは個別のユーザーに対して指定できます。個別のクォータの設定は、他のすべてのクォータの設定よりも優先されます。他のユーザーの個別のユーザー クォータを追加するには、ユーザーごとに [**ユーザー**] ページでユーザーを編集します。

注意: クォータは 1 GB より小さいサイズで、メガバイト単位で設定することができます。**例:0.5**、**0.3**、**0.9** など。

7.5 ファイル消去ポリシー

Files Advanced では、ドキュメント、ファイル、フォルダは、明示的に削除されない限り、一般的にシステムに保存されます。このため、ユーザーは削除したファイルを復旧し、どのようなドキュメントでも前バージョンを維持できます。管理者は、Files Advanced により、ポリシーを定義して、削除済みファイルを維持する期間、維持するリビジョンの最大数、古いリビジョンを削除するタイミングを決めることができます。

Files Advanced では、下記のポリシーをもとにして古いリビジョンや削除されたファイルをファイル リポジトリから自動的に消去することができます。この機能を利用して Files Advanced によって使用されるストレージの容量を管理することができます。消去されたファイルは復元できません。



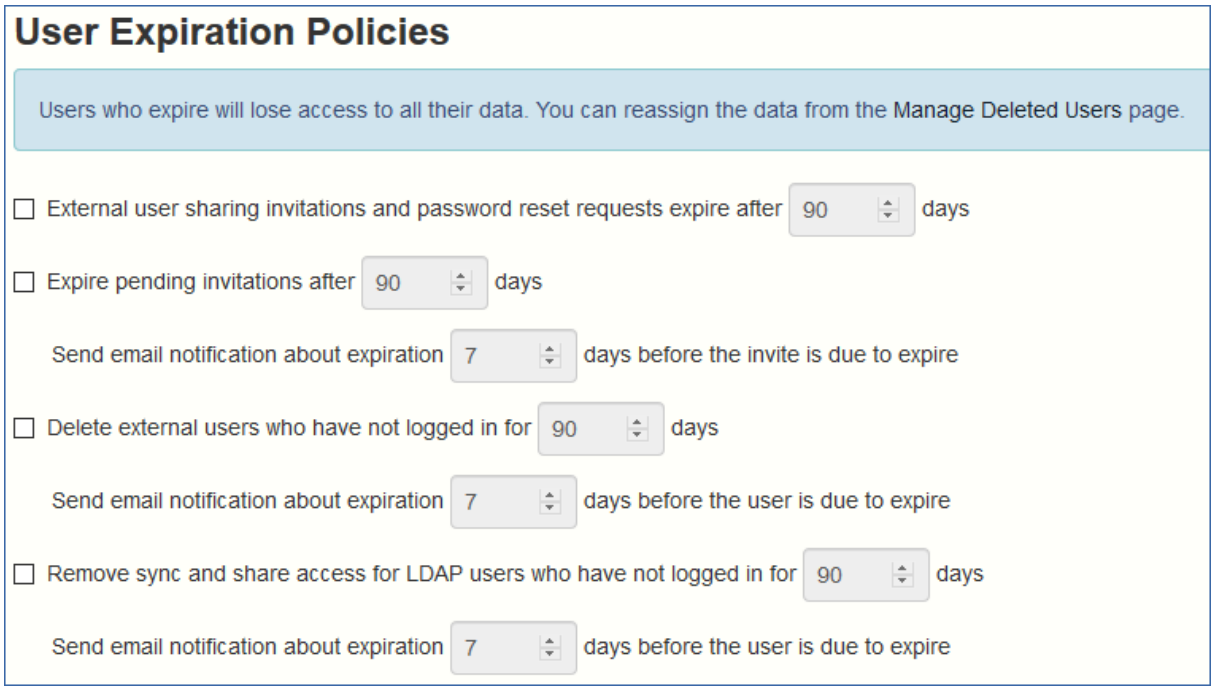
注意: 各ファイルの削除されていない最新のリビジョンは、以下の設定に関係なく消去されません。

- **削除済みファイルを消去する期限**: 有効にされている場合、この設定より古いファイルは削除されます。
- **過去のリビジョンを消去する期限**: 有効にされている場合、この設定より古いファイルのリビジョンは消去されます。
  - **ファイルごとに X 以上のリビジョンを期間に関係なく保持する**: 有効にされている場合、ファイルの経過日数に関係なく、ファイルごとに最大のリビジョン数を保持します。
- **ファイルごとに X のリビジョンのみを保持する**: 有効にされている場合、ファイルごとに保持する最大のリビジョン数が制限されます。

注意: [保存] ボタンを押すと、消去がすぐに開始されます。[保存] ボタンで消去しない限り、通常のスキャンが 60 分ごとに実行されます。

7.6 ユーザー期限切れポリシー

期限切れになったユーザーは、すべてのデータへのアクセスを失います。**[削除済みユーザーの管理]** ページからデータを再割り当てすることができます。



- **外部ユーザーの共有招待メールおよびパスワードリセットのリクエストは、X 日後に期限切れになります**: 有効にした場合、外部ユーザー用の招待メールおよびパスワードリセットのリクエストは設定した日数の経過後に有効期限切れになります。
- **X 日後に保留中の招待メールが有効期限切れになります**: 有効にした場合、設定した日数の経過後に、すべての保留中の招待メールが有効期限切れになります。
  - **招待の有効期限の X 日前に期限切れに関する電子メール通知を送信する**: 有効にされている場合、招待が期限切れになる前に、日数についての通知が送信されます。
- **ログインしていない外部ユーザーは X 日で削除されます**: 有効にした場合、設定した日数ログインしない外部ユーザーが削除されます。
  - **ユーザーの有効期限の X 日前に期限切れに関する電子メール通知を送信する**: 有効にされている場合、期限切れになる設定した日前の通知が一時ユーザーに送信されます。

- **ログインしていない LDAP ユーザーの同期および共有サポートを削除するまでの日数: X 日**: 有効にされている場合は、設定された日数ログインしなかった LDAP ユーザーの同期と共有アクセスを削除します。
  - **ユーザーの有効期限の X 日前に期限切れに関する電子メール通知を送信する**: 有効にされている場合、期限切れになる設定した日前の通知がユーザーに送信されます。

7.7 ファイル リポジトリ

この設定により、同期および共有するためにアップロードされるファイルの保存場所が決定されます。デフォルトの構成では、ファイル システム リポジトリは、Files Advanced Server と同じサーバーにインストールされます。Files Advanced の同期と共有ファイルおよび以前のリビジョンを保存するには、ファイル リポジトリを使用します。Files Advanced の設定ユーティリティ 『36ページ 』は、ファイル リポジトリのアドレス、ポート、およびファイル ストア ロケーションを設定するために使用します。下に示す **[ファイルストアリポジトリエンドポイント]** の設定は、設定ユーティリティの [ファイル リポジトリ] タブの設定と一致していなければなりません。設定値を表示または変更するには、AcronisAccessConfiguration.exe を実行します。通常、このファイルは **`C:\Program Files (x86)\Acronis\Files Advanced\Common\Configuration Utility`** にあります。

- **ファイル ストア タイプ**: 仮想ファイル システムのリポジトリで使用するストレージのロケーションを選択します。オプションは [ファイルシステム]、[Acronis Storage]、

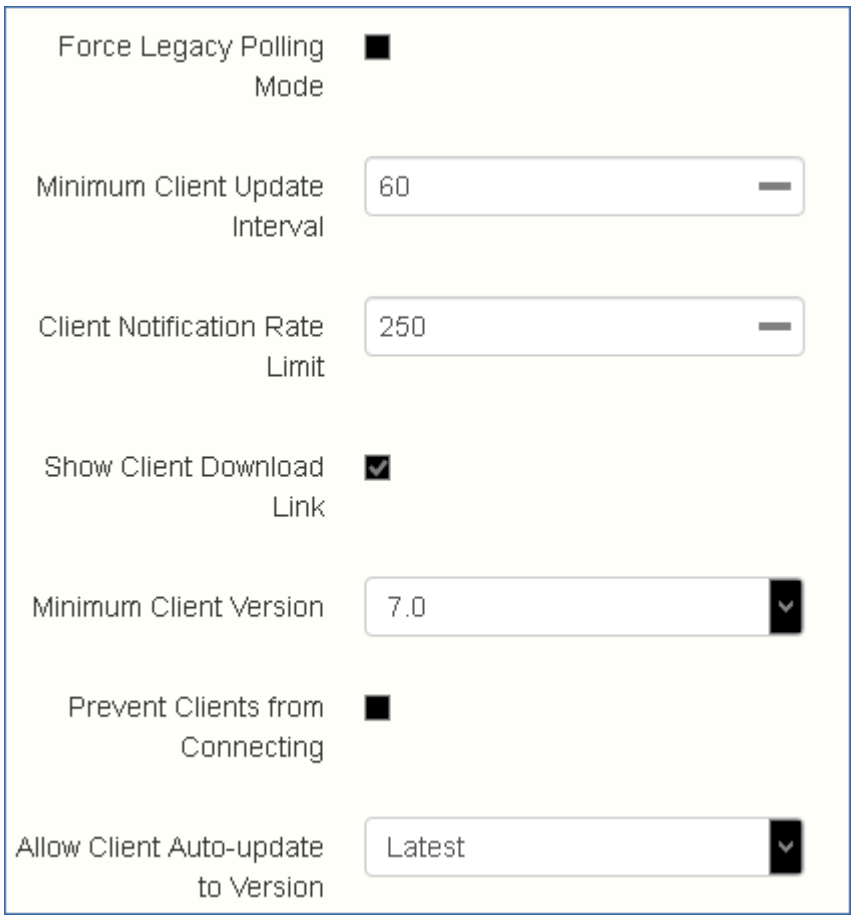
[Microsoft Azure Storage]、[Amazon S3]、[Swift S3]、[Ceph S3]、および [S3 と互換性のある他のストレージ] です。

注: [S3 と互換性のある他のストレージ] オプションでは、このリストに記載されていない S3 ストレージプロバイダを使用できます。ただし、すべての機能の正常な動作は保証されていません。

- **ファイルストアリポジトリエンドポイント**: ファイル システム リポジトリのエンドポイントの URL アドレスを設定します。
- **暗号化レベル**: 仮想ファイル システムのリポジトリに格納されるファイルを暗号化する際に使用する暗号化のタイプを指定します。オプションは、[なし]、[AES-128]、[AES-256] です。デフォルトは [AES-256] です。
- **ファイル ストア空き容量警告しきい値**: 空き容量がこのしきい値を下回ると、管理者はディスク領域不足の通知を受信します。

7.8 Files Advanced クライアント

以下はデスクトップクライアントの設定です。



- **レガシー ポーリング モードを強制**: 非同期サーバーから通知する代わりに、クライアントによって強制的にサーバーがポーリングされます。このオプションは、アクロニス サポートによって指示された場合にのみ有効にしてください。
  - **クライアント ポーリング タイム**: クライアントがサーバーをポーリングする時間の間隔を設定します。このオプションは **[レガシー ポーリング モードを強制]** が有効になっているときのみ利用できます。
- **最小クライアント アップデート間隔**: アップデートされたコンテンツを使用できることをクライアントに再通知するまでにサーバーが待機する最小時間を設定します（秒単位)。
- **クライアント通知の頻度制限**: サーバーが 1 分ごとに送信するクライアント アップデート通知の最大数を設定します。
- **クライアント ダウンロード リンクを表示**: 有効にされている場合、ウェブ ユーザーにはデスクトップ クライアントがダウンロードできるリンクが表示されます。
- **最小クライアントバージョン**: サーバーに接続できる最小クライアントバージョンを設定します。

  注: Files Advanced Server バージョン 7.5 の時点では、バージョン 6.1 以降のデスクトップクライアントのみから接続できます。
- **クライアントが接続できないようにする**: 有効にされている場合、デスクトップクライアントはサーバーに接続できません。一般的に、これは管理を目的とする場合のみ有効にしてください。ウェブ インターフェイスへの接続は妨げられません。
- **クライアントの自動バージョンアップデートを許可**: 自動バージョンアップデートチェックを使用して、すべてのデスクトップクライアントに導入されるデスクトップクライアントバージョンを設定します。クライアントの自動アップデートを禁止するには、**[アップデートを許可しない]** を選択します。

8 ユーザーとデバイス

セクションの内容

8.1 モバイル デバイスの管理

Files Advanced モバイルが Files Advanced サーバーに登録されると、そのモバイルデバイスが **[デバイス]** リストに表示されます。このリストには、PIN コードによってアクティブ化されている各デバイスの詳細なステータス情報が表示されます。

ここでは、すべての管理対象デバイスとその情報を表示できます。デバイスのワイプやアプリケーションパスワードの変更を行うこともできます。

- **表示名**: ユーザーの Active Directory（AD)のフル ネーム。
- **ユーザー名**: ユーザーの AD アカウント ユーザー名。
- **ドメイン**: ユーザーの AD アカウントがメンバとなっているドメイン。
- **デバイス名**: ユーザーが設定したデバイス名。
- **モデル**: デバイスのタイプ/モデル。
- **OS**: デバイスのオペレーティング システムのバージョン。
- **バージョン**: デバイスに存在する Files Advanced モバイル アプリケーションのバージョン。
- **ステータス**: デバイスに存在する Files Advanced Mobile アプリケーションのステータス。
- **最後の接続**: 管理サーバーとクライアント間の最後の接続の日付と時刻。
- **ポリシー**: ユーザーの管理ポリシーの名前とリンク。
- **操作**

- **詳細情報:** デバイス固有の ID や、編集可能なデバイス説明フィールドなど、デバイスに関する詳細情報が追加で表示されます。
- **アプリのパスワードのリセット**: デバイスの Files Advanced モバイル アプリケーション ロック パスワードをリモートでリセットします。ここでは、Files Advanced モバイル アプリケーションから取得したコードを入力し、確認コードを生成して、デバイス上のアプリケーションに確認コードを入力します。
- **リモート ワイプ**: 次回デバイスが管理サーバーに接続されたときに、Files Advanced モバイル アプリケーションのすべてのファイル（とその設定)が削除されます。他のアプリや OS のデータには影響を与えません。
- **リストから削除する**: デバイスを **[デバイス]** リストから削除し、そのデバイスを消去せずに管理対象から外します。Files Advanced クライアント管理サーバーに再度接続することはないと思われるデバイスを削除するために実行するのが一般的です。[モバイル クライアントを新しいデバイスに復元した場合でも、PIN コードなしで自動登録されるようにする] を有効にしている場合、リストから削除したデバイスがその後サーバーに接続されると、そのデバイスは自動的に再表示され、再び管理対象となります。

セクションの内容

8.1.1 リモート アプリケーション パスワード リセットの実行

Files Advanced の起動時にアプリケーションロックパスワードの入力を必須にするよう設定することで、Files Advanced モバイルを保護することができます。ユーザーがこのパスワードを忘れた場合、Files Advanced を使用できなくなります。モバイルアプリパスワードは、Active Directory のアカウントパスワードとは無関係です。

パスワードを忘れた場合は、リモートアプリケーションパスワードリセットを実行するか、デバイスから Files Advanced をアンインストールし、再度インストールするしかありません。アンインストールすると、既存のデータおよび設定はすべて削除されます。これによっ

てセキュリティは確保されますが、ユーザーは新しい管理招待メールが送られるまで Files Advanced サーバーにアクセスできなくなります。

アプリケーション パスワードのリセット

デバイス上の Files Advanced ファイルは、Apple Data Protection（ADP)ファイル暗号化を使用して常に保護されています。iTunes および iCloud にバックアップされているデバイス上のファイルと、デバイス レベルのロック コードが有効になっていないデバイス上のファイルの保護を強化として、および一般的なセキュリティ強化機能として、Files Advanced アプリケーションによって直接適用されるフルタイムのカスタム暗号化の 2 つ目の階層が導入されました。この暗号化の影響の 1 つとして、Files Advanced 5.0 以降では、アプリケーション ロック パスワードを無線でリセットすることができなくなりました。このことにより、Files Advanced による設定データベースの暗号化解除、およびユーザーに新しいアプリケーション パスワードの設定を可能にするため、デバイス ユーザーと Files Advanced IT 管理者の間でパスワード リセット コードおよび確認コードを交換する必要があります。

Files Advanced for iOS/Android のアプリケーション パスワードをリセットするには:

1. エンド ユーザーが管理者に Files Advanced アプリケーション パスワードのリセットを要求するときに、ユーザーの**パスワード リセット コード**を提供します。
2. **[モバイル アクセス]** タブを選択します。
3. **[デバイス]** タブを開きます。
4. **[デバイスの管理]** ページで、アプリケーション パスワードのリセットを実行するデバイスを見つけて、**[操作]** ボタンをクリックします。
5. **[アプリのパスワードのリセット...]** を押します。
6. ユーザーによって提供された**パスワード リセット コード**を入力し、**[確認の生成]** をクリックします。
7. 表示される**確認コード**を電話または電子メールでユーザーに伝えます。
8. ユーザーがアプリケーションのパスワード リセット ダイアログにこのコードを入力すると、新しいパスワードを設定するように指示されます。ユーザーが適切なアプリケーション パスワードを設定せずにこの処理を中断した場合、ユーザーは Access モバイル クライアントへのアクセスを引き続き拒否され、アプリケーション パスワードのリセット処理を繰り返す必要があります。

8.1.2　リモート ワイプの実行

Files Advanced では、Mobile アプリケーションに対してリモートワイプを実行することができます。このリモート ワイプの使用を選択すれば、ローカルに保存されている、または Files Advanced アプリケーション内にキャッシュされているすべてのファイルが削除されます。すべてのアプリケーション設定がリセットされてデフォルト設定に戻り、アプリケーションに設定されているすべてのサーバーが削除されます。

リモート ワイプのキューイング

1. **[モバイル アクセス]** タブを選択します。
2. **[ユーザーとデバイス]** タブを開きます。
3. リモート ワイプを実行するデバイスを見つけて、**[操作]** ボタンを押します。
4. **[リモート ワイプ...]** を押します。
5. **[消去]** を押して、リモート ワイプを確定します。
6. **[リモートワイプの保留中]** ステータスが、そのデバイスの **[ステータス]** 列に表示されます。リモート ワイプがデバイスによって受け入れられると、そのことが **[ステータス]** に反映されます。

   注記:クライアントが次に管理サーバーに接続するまでいつでもリモート ワイプをキャンセルすることができます。このオプションは、リモート ワイプが実行された後に **[操作]** メニューに表示されます。

接続要件

Files Advanced クライアントが、プロファイルのアップデート、リモート パスワードのリセット、およびリモート ワイプの指示を受け取るには、Files Advanced サーバーへのネットワーク アクセスが必要です。クライアントが、Files Advanced にアクセスする前に VPN に接続する必要がある場合は、管理コマンドを受け付ける前に VPN に接続する必要があります。

8.2 ユーザーの管理

このセクションから、すべての同期・共有ユーザーを管理できます。**[ユーザーの追加]** ボタンから新規ユーザーを招待したり、[操作] ボタンから現在のユーザーの編集や削除を実行することができます。ユーザーの編集時に、管理者権限の付与 (権限がある場合)、電子メールの変更、パスワードの変更、アカウントの有効/無効の切り替えなどを実行できます。クォータを有効にしている場合、ユーザーに同期・共有のアクセス権がある場合のみ、そのユーザーに対してカスタムクォータを設定できます。

同期・共有のユーザーには 3 つのタイプに分けられます。

- **外部**ユーザーは、メール招待や共有フォルダへの招待によって作成できます。確認の電子メールを受け取ったユーザーは、その電子メールからアカウントをアクティブ化する必要があります。このようなユーザーにはデフォルトではライセンスが与えられず、管理者が手動でライセンス取得済みの状態に変更する必要があります。ユーザーがライセンスを取得していない場合、他のユーザーと共有されているフォルダ内のフォルダおよびファイルの作成、編集、削除、アップロードのみを実行できます。非ライセンス ユーザーは、自身のコンテンツを作成したりアップロードすること、およびデスクトップ クライアントを使用することはできません。　ライセンスを取得していないユーザーは、権限が付与されていても、他のメンバーを**招待**したり**表示**したりすることはできません。次の機能を使用するには、ライセンスを取得する必要があります。
- LDAP ユーザーと管理権限を持つユーザーには、作成時に自動的にライセンスが与えられます。これらのユーザーは、ファイルとフォルダの作成とアップロードができ、ファイルとフォルダを他のユーザーと共有することもできます。また、デスクトップクライアントも使用できます。プロビジョニング済み LDAP グループ 『149ページ 』をセットアップしていない限り、一時的なユーザーと同じ方法で LDAP ユーザーを作成してください。ただし、手動でライセンスを付与する必要はありません。同期・共有が許可されていない管理者は、電子メールアドレスを設定しておく必要はありません。各自の LDAP 資格情報を使用してログインできます。このような管理者は、Files Advanced サーバーの SMTP の設定をしなくても追加できます。詳細については、「管理者と権限『167ページ 』」を参照してください。
- **アクセス権なし**のユーザーは、同期・共有のウェブクライアントへのアクセス権がなく、デフォルトでライセンスが与えられない管理ユーザーです。このタイプのユーザー

は、通常のユーザーのようにモバイルアプリケーションやモバイルアクセスの機能を使用できます。LDAP ユーザーまたは一時的なユーザーのどちらでも構いません。

- **名前**: サーバーへのログインに使用する名前を表示します。
- **電子メール**: ユーザーの電子メールアドレスが表示されます。
- **同期・共有**
  - **ステータス**: ユーザーが使用しているライセンスの種類が表示されます。
  - **使用量**: ユーザーのコンテンツの合計サイズが表示されます。
- **最後のログイン**: 最後のログインの時刻と日付。
- **操作**
  - **詳細情報**: ユーザーに関する詳細な情報が表示されます。
  - **利用デバイスを表示**: このユーザーが使用しているデバイスに関する情報が表示されます。
  - **同期・共有のパスワードをリセット**: パスワードリセットの電子メールを送信します。
  - **ライセンス取得済みに変更**: 無料ユーザーをライセンス取得済みユーザーに変更します。これには 1 が使用されます。
  - **ユーザーの編集**: このユーザーを編集できます。
  - **削除**: ユーザーを削除します。

一時的なユーザーの追加

1. Files Advanced ウェブ インターフェイスを開きます。
2. 管理者アカウントでログインします。**ユーザー管理**権限があるアカウントのユーザーも同様の操作を実行できます。
3. **[同期・共有]** タブを開きます。
4. **[ユーザー]** タブを開きます。
5. **[ユーザーの追加]** ボタンを押します。

6. ユーザーの電子メールを入力します。
7. ユーザーに管理者権限を付与するかを選択します。
8. 招待メールの言語を選択します。
9. **[追加]** ボタンを押します。

ユーザーにリンクが記載された電子メールが送信されます。リンクを開くと、パスワードを設定するように求められます。アカウントの確認を行うための電子メールを受信します。電子メールに記載されたリンクを開くと、アカウントの登録が完了します。

LDAP ユーザーの追加

1. Files Advanced ウェブ インターフェイスを開きます。
2. 管理者アカウントでログインします。**ユーザー管理**権限があるアカウントのユーザーも同様の操作を実行できます。
3. **[同期・共有]** タブを開きます。
4. **[ユーザー]** タブを開きます。
5. **[ユーザーの追加]** ボタンを押します。
6. ユーザーの電子メールを入力します。
7. ユーザーに管理者権限を付与するかを選択します。
8. 招待メールの言語を選択します。
9. **[追加]** ボタンを押します。

LDAP の資格情報を使用してログインできるようになります。ユーザーがログインすると、アカウントの追加は完了になります。

注記: LDAP が有効にされており、LDAP 管理者グループがプロビジョニングされている場合は、その LDAP グループのユーザーは、LDAP 資格情報で直接ログインでき、完全な管理者権限が付与されます。

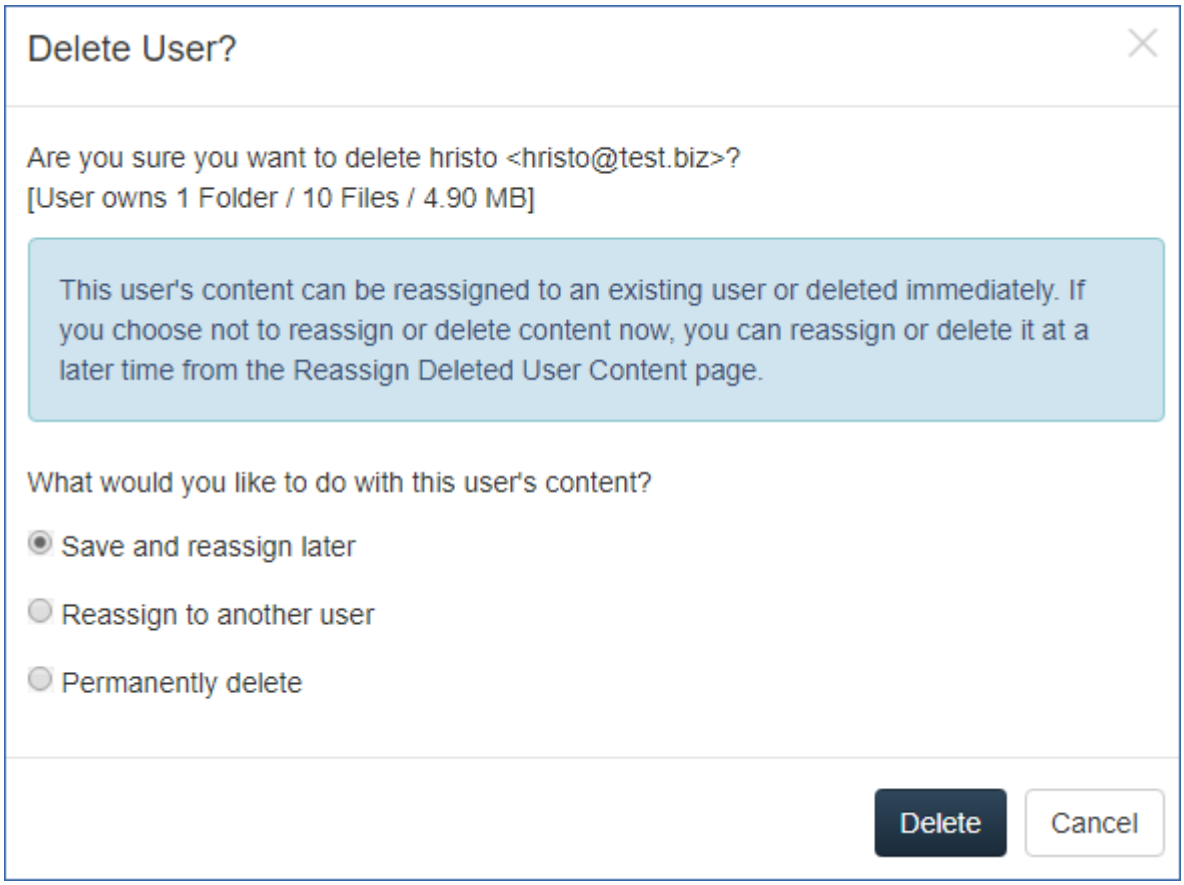
カスタムクォータを設定するには、次の手順を実行します。

同期・共有へのアクセス権があるユーザーには、カスタムクォータを設定できます。これを実行するには:

1. ウェブインターフェイスで、**[ユーザーとデバイス]** タブを開きます。
2. 目的のユーザーを見つけ、**[操作]** ボタンをクリックします。
3. **[ユーザーの編集]** を選択し、**[カスタムクォータを使用]** を有効にします。
4. 目的のクォータサイズを入力し、**[保存]** を押します。

8.3 削除済みユーザーコンテンツを再割り当てする

コンテンツがない削除されたユーザーは、完全に削除されます。コンテンツのあるユーザーを削除するときに、対象のユーザーのコンテンツに対して行う操作を確認するウィンドウが表示されます。



- **保存して後で再割り当てする**: ユーザーのコンテンツは再割り当てまたは削除のためにそのまま残ります。後で管理者は **[削除済みユーザーコンテンツを再割り当てする]** ページで、再割り当てまたは削除を待機しているコンテンツのある削除済みユーザーのリストにアクセスできます。

  注意: このコンテンツには引き続き、アクティブなユーザーと同じように消去ポリシーが適用されます。

- **別のユーザーに再割り当てする**: 別のユーザーをすぐに選択し、そのユーザーにコンテンツを再割り当てします。コンテンツが再割り当てされたユーザーには、**[DeletedUserName <deletedusersemail> から継承したコンテンツ]** という名前の同期・共有フォルダが作成され、このユーザーが、継承されたすべてのコンテンツの所有者にもなります。継承されるコンテンツには、削除済みユーザーによって共有されたフォルダも含まれます。
- **完全に削除する**: 対象アカウントとコンテンツを削除します。

9 クライアント ガイド

Files Advanced クライアントの使用については、下のリストにあるアプリ専用のクライアントガイドマニュアルを参照してください。

- デスクトップおよびウェブクライアント
- iOS アプリ
- Android アプリ
- Windows モバイルアプリ

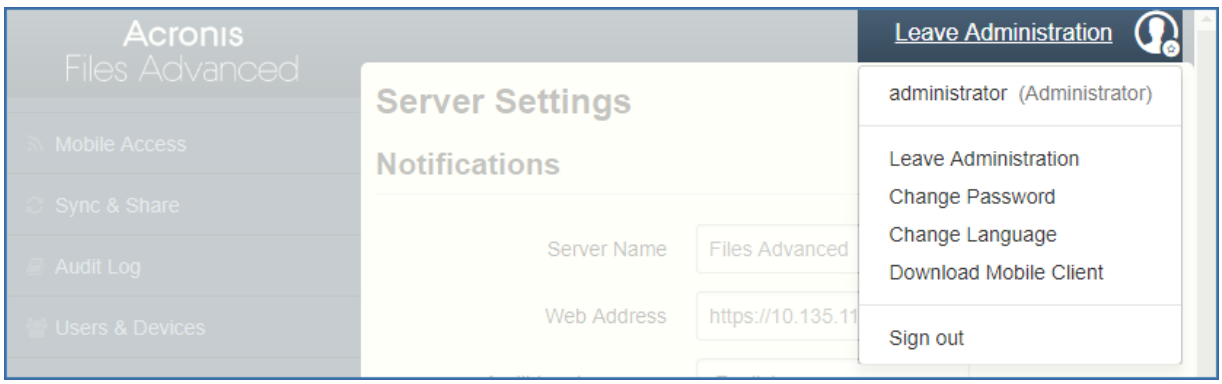
10 サーバーの管理

セクションの内容

10.1 サーバーの管理

管理者の場合、ウェブインターフェイスにログインすると、**管理**モードと**ユーザー**モードを切り替えることができます。

- **管理**モードに入るには、ユーザーアイコンをクリックして、**[管理コンソール]** を押します。
- **ユーザー**モードに入るには、右上にある **[管理画面を閉じる]** ボタンを押します。



注意: 管理者は、API ドキュメントにアクセスできます。管理モードが有効になっている場合、Access ウェブインターフェイスのフッターにそのリンクが表示されます。

10.2 管理者と権限

管理ページのアクセス制限

- **構成済みの IP アドレス範囲からの接続のみに管理ページへのアクセスを許可する**: 管理者が特定の IP アドレスのみに管理ウェブインターフェイスへのアクセスを許可できるようになります。
  - **管理ページへのアクセスを許可する IP アドレス**: **管理**ページにアクセスできる IP アドレスを管理者が入力します。カンマ区切りの IP、サブネット、または IP 範囲を使用できます。

  例: 10.1.2.3, 10.4.*, 10.10.1.1-10.10.1.99

  注意: localhost からの管理者アクセス権を制限することはできません。

  注意: この機能は、ゲートウェイサーバーを使用して Files Advanced サーバーへの要求をプロキシしているサーバーでは機能**しません**。

プロビジョニング済み LDAP 管理者グループ

このセクションでは、管理グループを管理することができます。これらのグループ内のユーザーは、グループの管理者権限を自動的に受け取ります。すべての権限は表に表示され、現在有効な権限には緑のマークが付けられます。

[操作] ボタンを使って、グループの削除または編集ができます。グループの権利権限を編集できます。

プロビジョニング済みの LDAP 管理者グループを追加するには

1. **[プロビジョニング済みグループの追加]** を押します。

2. グループに同期と共有の機能を付与する場合はチェックします。
3. グループ ユーザーに付与するすべての管理者権限をチェックします。
4. グループを検索します。
5. グループ名をクリックします。
6. **[保存]** を押します。

管理ユーザー

このセクションでは、管理者権限を持つすべてのユーザー、認証タイプ（アドホックまたはLDAP)、同期と共有の権限の有無、およびその状態（無効または有効)を一覧表示します。

[管理者の追加] ボタンを使って、完全な権限または部分的な権限を持つ新しいユーザーを招待できます。**[操作]** ボタンを使って、ユーザーの削除または編集ができます。管理者権限、状態、またはパスワードを編集できます。

1 人の管理者を招待する

1. Files Advanced ウェブ インターフェイスを開きます。
2. 管理者アカウントでログインします。
3. **[全般設定]** タブを展開して、**[管理者]** ページを開きます。
4. **[管理者の追加]** で **[管理ユーザー]** ボタンを押します。
5. どのタイプのユーザーを招待するのかと、招待するユーザーに何を管理させるのかに応じて、[Active Directory/LDAP] か [電子メールによる招待] を選択します。電子メールを使用できない LDAP ユーザーには同期と共有の機能を付与できません。

a) **Active Directory/LDAP を通じて招待する場合は、次のことを実行します。**

   1. Active Directory に追加するユーザーを検索し、ユーザーの [共通名] をクリックして選択します。

      注意: [LDAP ユーザー] フィールドと [電子メール] フィールドは自動的に入力されます。

   2. 同期と共有を有効/無効にする機能です。
   3. ユーザーに持たせる管理者権限を選択します。
   4. [追加] を押します。

b) **電子メールを通じて招待する場合は、次のことを実行します。**

1. 管理者として追加するユーザーの電子メール アドレスを入力します。

注意: 電子メールで招待されるアドホック ユーザーには、常に同期と共有の機能が付属します。

2. このユーザーにライセンスを供与するかどうかを選択します。
3. ユーザーに持たせる管理者権限を選択します。
4. 招待電子メールの言語を選択します。
5. [追加] を押します。

管理者権限

- **完全な管理者権限**: ユーザーに完全な管理者権限を付与します。
- **ユーザーを管理する**: ユーザーを管理する権限をユーザーに付与します。これには、新しいユーザーの招待、LDAP グループ プロビジョニング、Files Advanced 登録招待の送信、および接続されているモバイル デバイスの管理が含まれます。
- **モバイル データ ソースを管理する**: モバイル データ ソースを管理する権限をユーザーに付与します。これには、新しいゲートウェイ サーバーとデータ ソースの追加、割り当て済みソース、クライアントで表示可能なゲートウェイ、およびレガシー データ ソースの管理が含まれます。
- **モバイル ポリシーを管理する**: モバイル ポリシーを管理する権限をユーザーに付与します。これには、ユーザーとグループのポリシー、許可されたアプリケーション、およびデフォルトのアクセス制限の管理が含まれます。
- **監査ログを表示する**: 監査ログを表示する権限をユーザーに付与します。

注意: プロビジョニング済み LDAP 管理者グループと、プロビジョニング済みの同期と共有の LDAP グループの両方に属する新しいユーザーには、まとめられた許可が与えられます。

ユーザーに管理者権限を付与するには:

1. **[同期・共有]** タブを開きます。
2. **[ユーザー]** タブを開きます。
3. 編集するファイルの **[操作]** ボタンを押します。

4. **[編集]** を押します。
5. ユーザーに付与するすべての管理者権限をチェックします。
6. **[保存]** を押します。

管理者の固有の権限を付与するには:

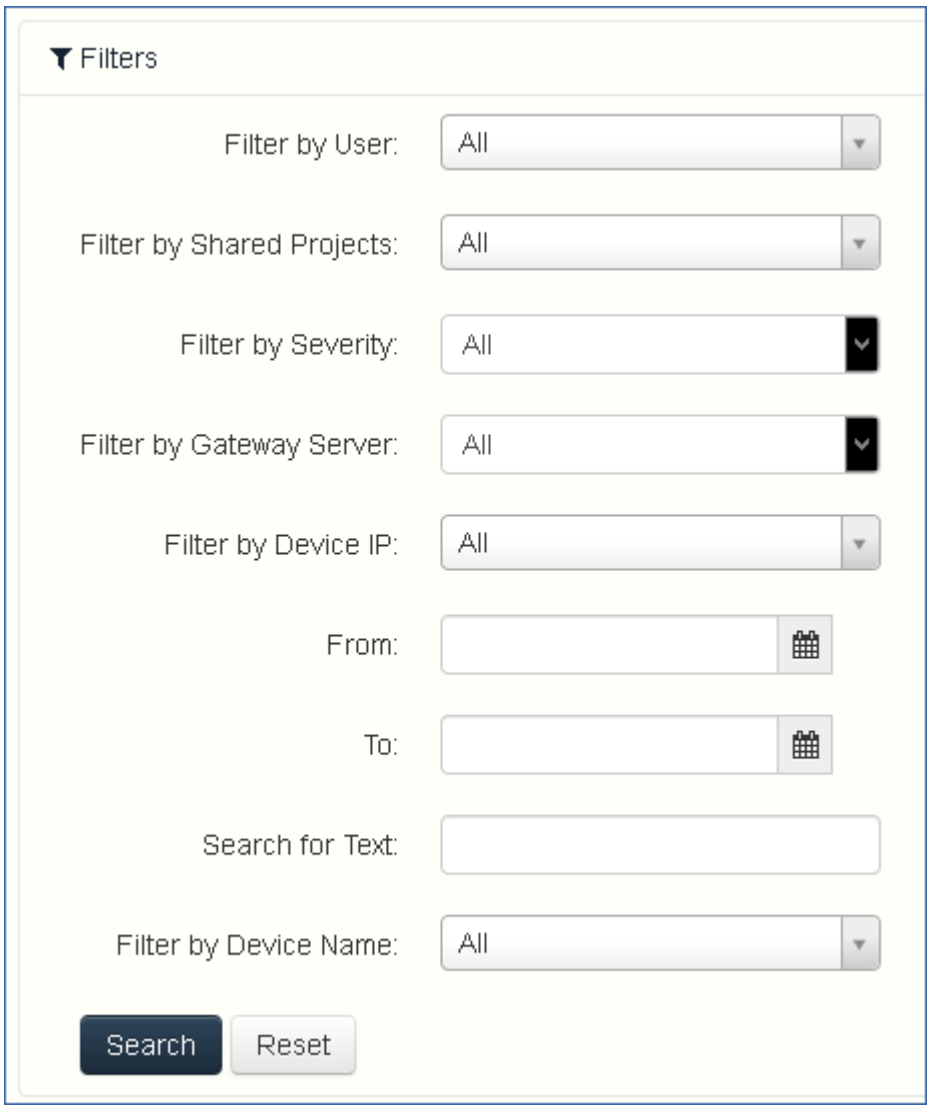
1. 編集するファイルの **[操作]** ボタンを押します。
2. **[編集]** を押します。
3. ユーザーに付与するすべての管理者権限をチェックします。
4. **[保存]** を押します。

10.3 監査ログ

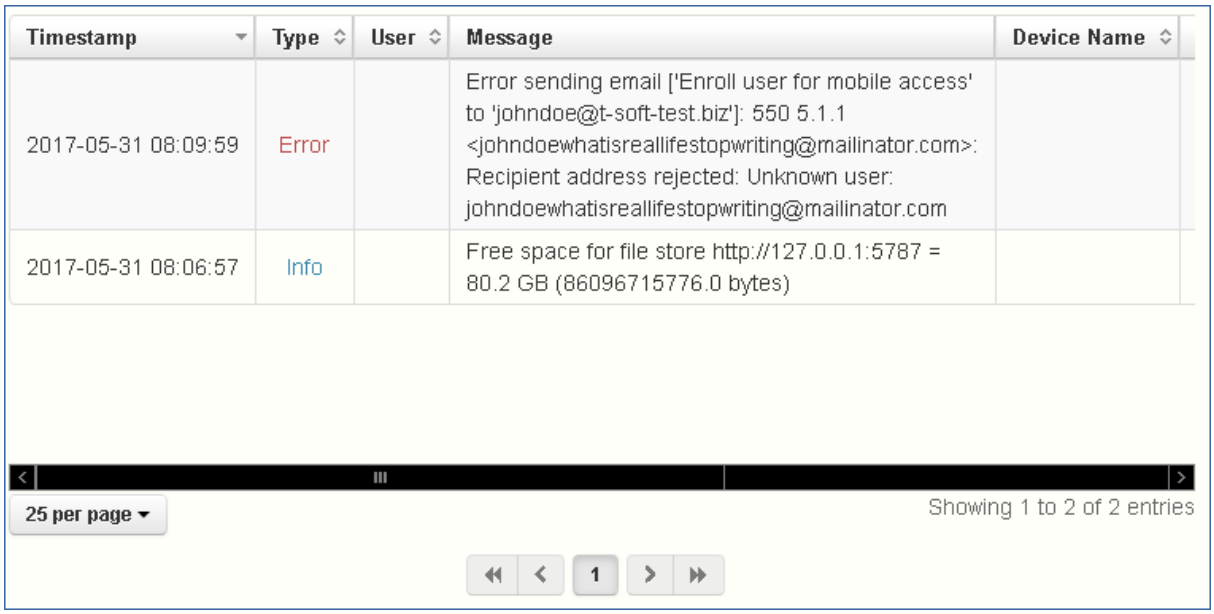
10.3.1 ログ

ここでは、最近のイベント (消去ポリシーにより、時間制限が異なることがあります)、ログの元となったユーザー、操作について説明するメッセージをすべて確認できます。

注意: ゲートウェイ サーバーのログとログのレベルを設定する方法については、「ゲートウェイサーバーのログ 『121ページ 』」を参照してください。



- **ユーザーでフィルタを適用する**: ユーザーでログをフィルタします。**[すべて]** または **[ユーザーなし]** を選択するか、使用可能ないずれかのユーザーを選択できます。
- **共有プロジェクトでフィルタを適用する**: 共有プロジェクトでログをフィルタします。**[すべて]** または **[共有しない]** を選択するか、使用可能ないずれかの共有プロジェクトを選択できます。
- **重要度でフィルタを適用する**: タイプでログをフィルタします。**[すべて]**、**[Info]**、**[警告]**、**[エラー]**、**[Fatal]** というタイプがあります。
- **日時**: 日時でフィルタします。
- **テキストを検索**: ログ メッセージの内容でフィルタします。

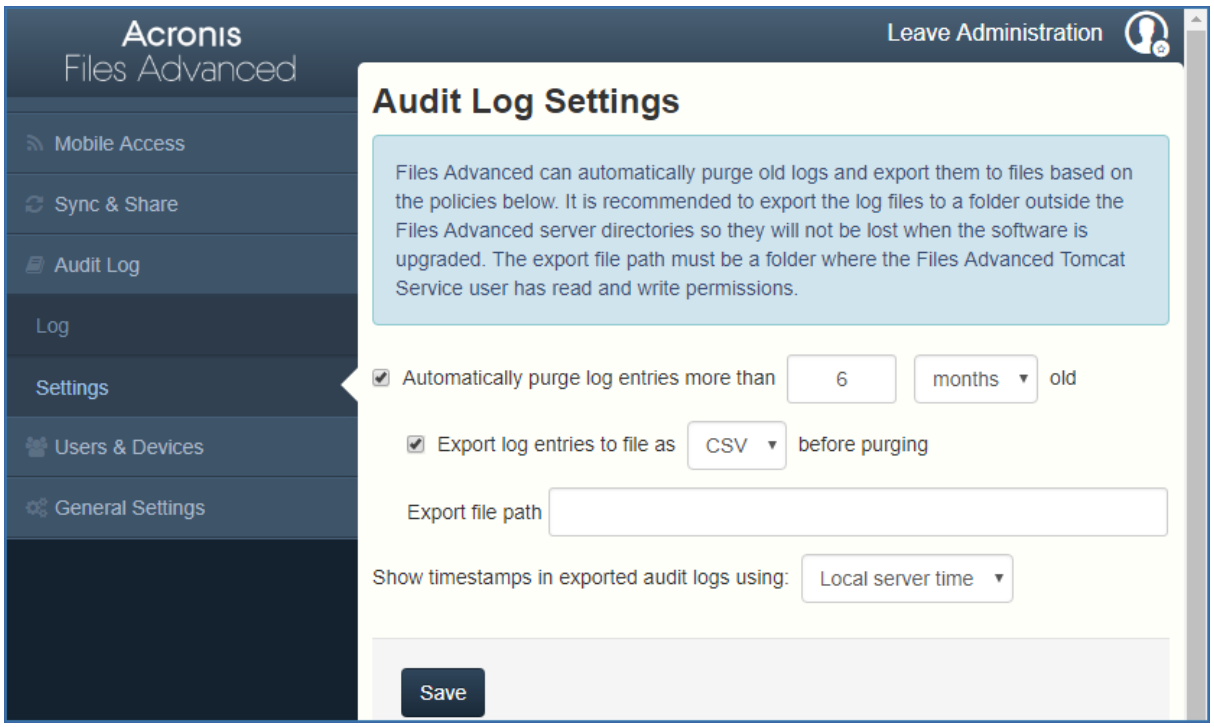


- **タイムスタンプ**: イベントの日時を示します。
- **タイプ**: イベントの重大度を示します。
- **ユーザー**: イベントの責任を負うユーザー アカウントを示します。
- **メッセージ**: 発生したことに関する情報を示します。

ゲートウェイ サーバーで監査ログを有効にした場合、モバイル クライアントのアクティビティも表示されます。デスクトップ クライアントやウェブ クライアントからモバイル データ ソースにアクセスできるようにした場合、これらの設定はログにも反映されます。

- **デバイス名** – 接続されているデバイスの名前。
- **デバイス IP** – 接続されているデバイスの IP アドレスを表示します。
- **ゲートウェイ サーバー** – デバイスが接続されているゲートウェイ サーバーの名前を表示します。
- **ゲートウェイ サーバーのパス** – ゲートウェイ サーバー上のデータ ソースへのパスを表示します。

10.3.2 設定



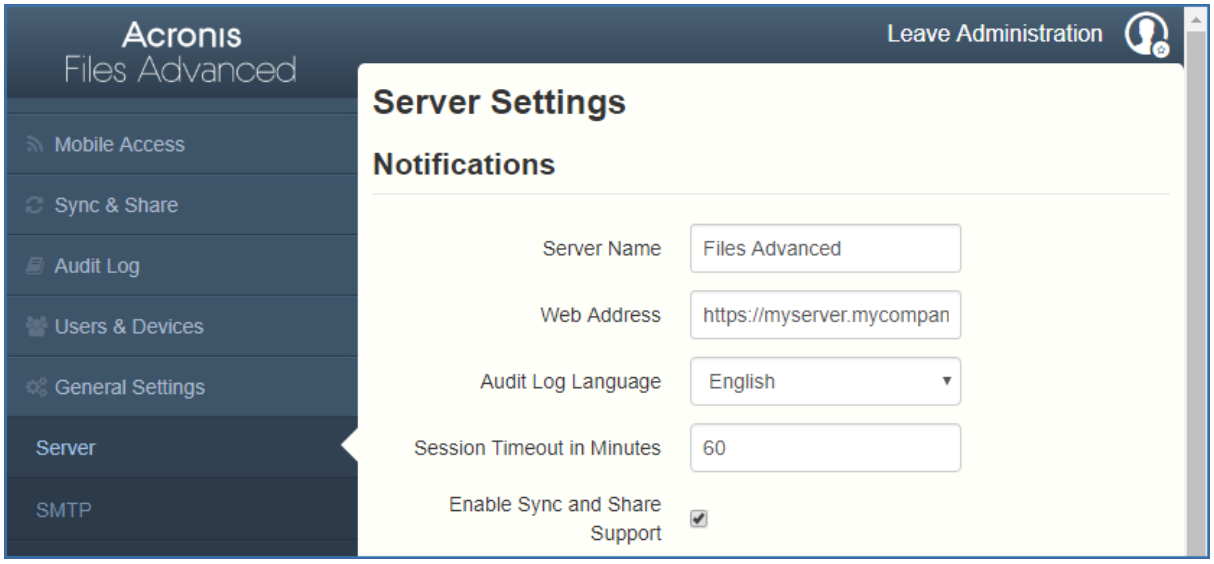
Files Advanced では、特定のポリシーに基づき、古いログを自動的に消去したりファイルにエクスポートすることができます。

- **X Y 経過したログ エントリを自動的に消去する**: 有効にした場合、指定した日数、週数、または月数を経過したログが自動的に消去されます。
  - **消去する前に X のファイル形式でログ エントリをエクスポートする**: 有効にした場合、ログが消去される前に CSV、TXT、または XML のいずれかの形式でコピーがエクスポートされます。エクスポートはサーバーのローカルタイムで 03:00 に自動的に設定されます。この設定は変更できません。
    - **ファイル パスをエクスポートする**: ログのエクスポート先を設定します。

注意: アップグレード時にログが失われないように、Files Advanced のインストールフォルダ以外のフォルダにログをエクスポートすることをお勧めします。指定するフォルダには、Files Advanced Tomcat サービスを実行するユーザーアカウントの読み取り/書き込みのアクセス権が必要です。デフォルト設定を変更していない場合、アカウントはローカルシステムアカウントになります。

- **エクスポート済みの監査ログのタイムスタンプを表示する（X を使用)**: 監査ログでサーバーのローカルタイム形式を使用するか別の時間形式（UTC)を使用するかを選択できます。

10.4 サーバー

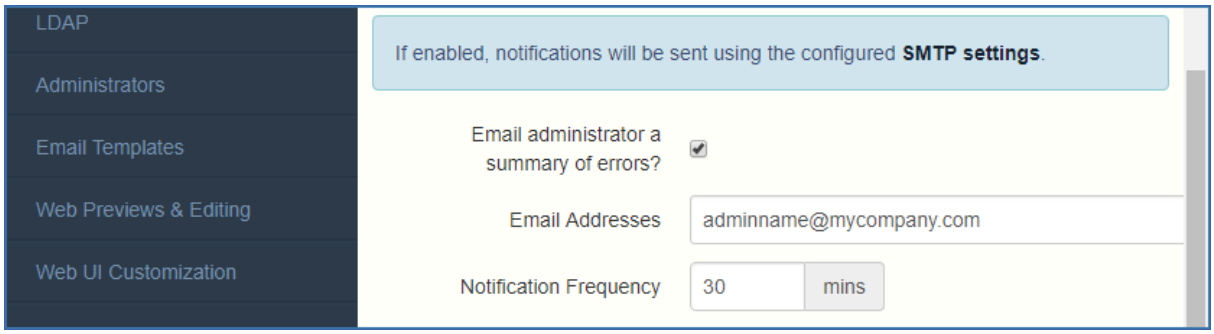


サーバーの設定

- **サーバー名**: ウェブ サイトのタイトルとして使用され、管理者への通知メールでこのサーバーを識別するためにも使用される、表示用のサーバー名。
- **ウェブ アドレス**: ユーザーが（http:// または https:// で始まる)ウェブ サイトにアクセスできる FQDN または IP アドレスを指定します。ここでは「localhost」を使用しないでください。このアドレスは、電子メール招待リンクでも使用されます。
- **監査ログの言語**: 監査ログのデフォルト言語を選択します。現在のオプションは、**[英語]**、**[ドイツ語]**、**[フランス語]**、**[日本語]**、**[イタリア語]**、**[スペイン語]**、**[チェコ語]**、**[ロシア語]**、**[ポーランド語]**、**[韓国語]**、**[中国語（繁体字)]**、**[中国語（簡体字)]** です。 デフォルト値は **[英語]** です。
- **セッションタイムアウト（分)**: 非アクティブユーザーがログアウトされるまでの時間の長さを設定します。選択された期間内にアクションが実行されなかった場合は、アクションを実行するかログアウトを行うよう促す時限ダイアログが表示されます。

  注意: ユーザーがセッションタイムアウトより長い時間がかかるアップロードまたはダウンロードを開始した場合は、アップロードが終了するまでログイン状態が維持されます。

- **同期・共有のサポートを有効にする**: このチェックボックスで同期・共有の機能を有効または無効にします。



通知の設定

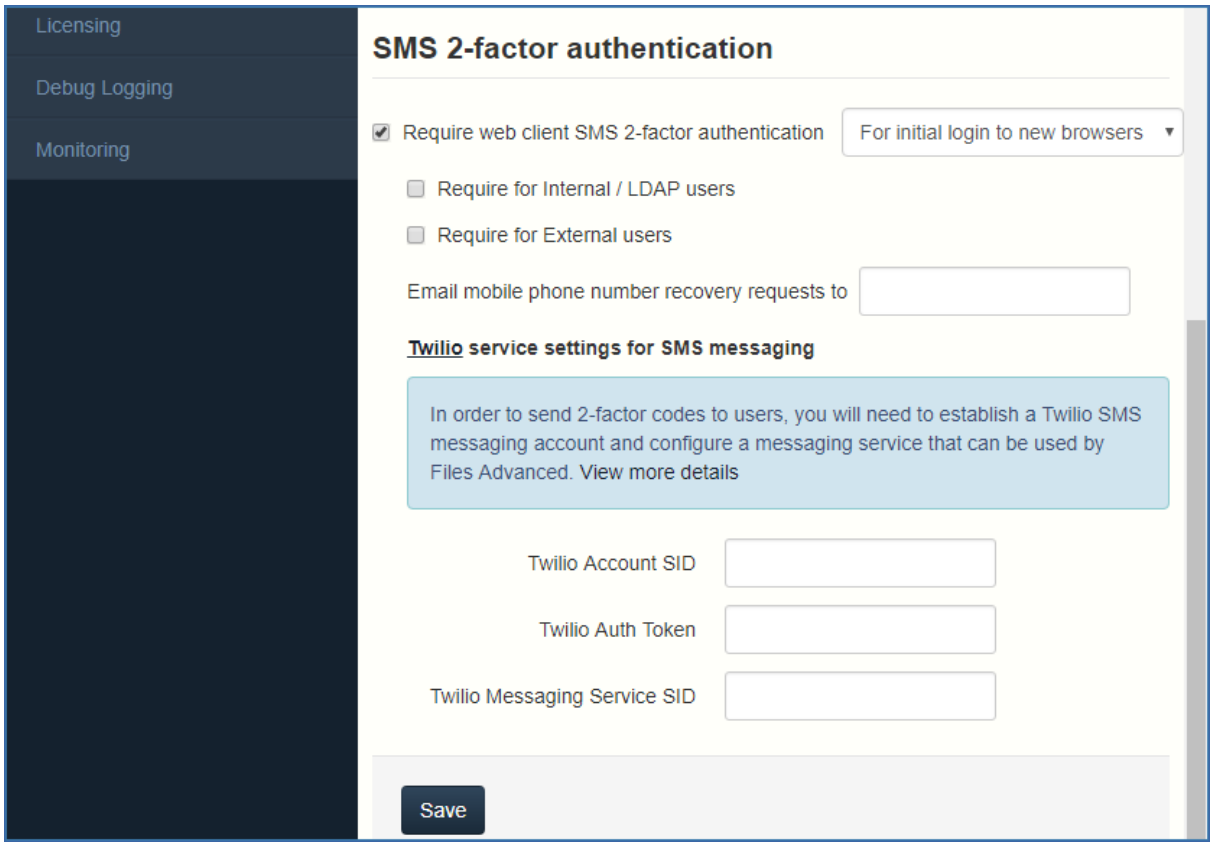
- **エラーの概要を管理者に電子メールで送信しますか？**: 有効にされている場合は、指定された電子メール アドレスにエラーの概要が送信されます。
  - **電子メールアドレス**: エラーの概要を受信する 1 つ以上の電子メール アドレス。
  - **通知頻度**: エラーの概要を送信する頻度。エラーがある場合にのみ電子メールが送信されます。

セクションの内容

Web クライアントログインで SMS による 2 要素認証のオプションが組み込まれました。AD 携帯電話番号またはユーザー指定の電話番号を使用することができます。2 要素認証を要求するのは、毎回のログイン時、指定した期間の経過後、または新しいブラウザからのログイン時のみにすることができます。

SMS コードの送信には、Twilio SMS メッセージングサービスでアカウントを確立しておくことが必要になります。詳細については、https://www.twilio.com/sms を参照してください。Twilio の試用版の実行方法については、Twilio 無料試用を参照してください。

注意: Twilio では 1 つのアカウントしか必要ありません。そのアカウントが Files Advanced サーバーで使用されるため、すべてのユーザーのアカウントを用意する必要がありません。



ウェブクライアントに SMS 2 要素認証を要求する:

- **新しいブラウザへの初期ログインの場合**: 新しいユーザーが Files Advanced サーバーのウェブページを初めて開くときに SMS 認証を要求します。確認コードを入力してブラウザを登録したら、別のブラウザまたはコンピュータを使用しない限り、二度と SMS コードを入力するように要求されることはありません。
- **指定した間隔で**: ログイン試行の回数に関係なく、指定した時間間隔で SMS 認証を要求します。
- **毎回のログインで**: ユーザーが接続を試行するたびに SMS 認証を要求します。

- **内部ユーザー/LDAP ユーザーに要求:**
  - **Files Advanced アカウント**: これをオンにすると、ユーザーの携帯電話番号がユーザーの Files Advanced アカウントから取得されます。
  - **Active Directory**: これをオンにすると、ユーザーの携帯電話番号がユーザーの Active Directory アカウントから取得されます。

注意: 使用される電話番号は、Active Directory 内の **[電話番号]** タブの **[携帯電話番号]** の番号です。

- **フォールバック動作: -** このオプションによって、Active Directory が選択されたが、ユーザーの電話番号が設定されていない場合のデフォルトアクションが決定されます。
  - **Files Advanced アカウントの使用**: ユーザーに電話番号の入力を要求します。
  - **2 要素認証なしでログインを許可**: 2 要素認証を使用しないログインを許可します。
  - **ログインを許可しない**: Active Directory 内に電話番号がないユーザーはログインを許可されません。
- **外部ユーザーに要求**: これをオンにすると、外部ユーザーにも SMS 認証が要求されます。
- **復元要求を携帯電話番号にメールで送る**: すべての携帯電話番号の復元要求が、このメールアドレスに送信されます。

Twilio の設定:

- **Twilio アカウントの SID**: 会社の Twilio アカウントセキュリティ識別子（SID)。
- **Twilio 認証トークン**: 会社の Twilio 認証トークン。

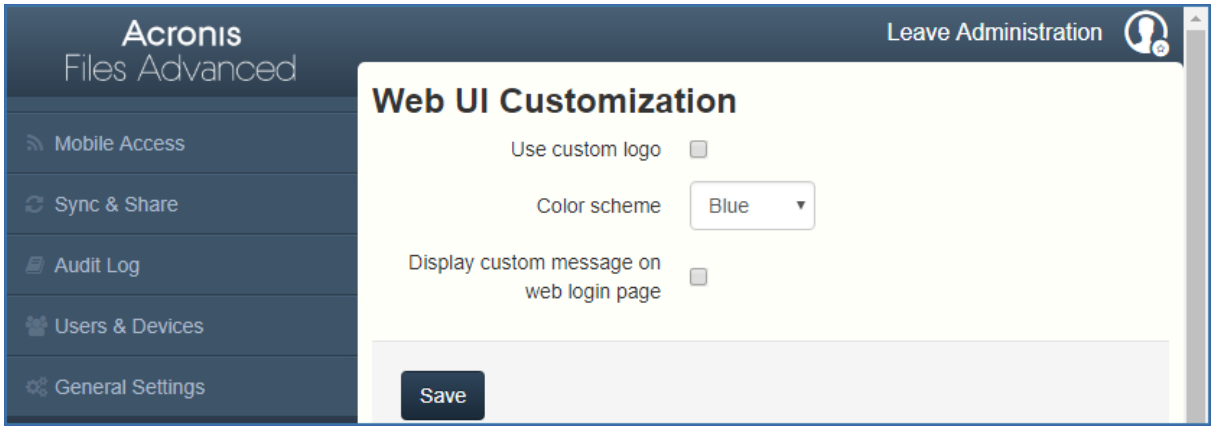
  これらの両方が https://www.twilio.com/console にある Twilio コンソールで見つかります。
- **Twillio メッセージングサービス SID**: 2 要素認証メッセージングサービスの SID。この SID は https://www.twilio.com/console/sms/dashboard にあります。複数の Twilio メッセージングサービスを使用している場合は、2 要素認証に使用するサービスの SID だけを使用します。Twilio メッセージングサービスを作成するときに、**[ユースケース]** を空白のままにするか、2 要素認証を選択します。

注意: Twilio コンソールで、メッセージングサービスの使用を許可する国を選択する必要があります。希望する国のチェックボックスを選択してください。

10.5 ウェブ UI のカスタマイズ

Files Advanced サーバーのロゴやカラースキームを簡単にカスタマイズできます。

注意: これらのカスタマイズを、Files Advanced API を介して実行することもできます。詳細については、ウェブ UI API カスタマイズを参照してください。



カスタム ロゴの使用

1. Files Advanced ウェブ インターフェイスを開き、管理者としてログインします。
2. **[全般設定]** → **[ウェブ UI のカスタマイズ]** に移動します。
3. **[カスタム ロゴを使用]** チェックボックスをオンにします。
4. 変更後のロゴ ファイルを選択し、ドロップダウン メニューで選択されていることを確認します。

   注意: 画像の最大サイズが括弧 **()** 内に示されます。

5. **[保存]** を押します。

カスタムのようこそメッセージを使用する

1. Files Advanced ウェブ インターフェイスを開き、管理者としてログインします。
2. **[全般設定]** → **[ウェブ UI のカスタマイズ]** に移動します。
3. **[ウェブのログインページにカスタムメッセージを表示します]** チェックボックスをオンにします。
4. テキストボックスに任意のメッセージを入力して、**[保存]** を押します。

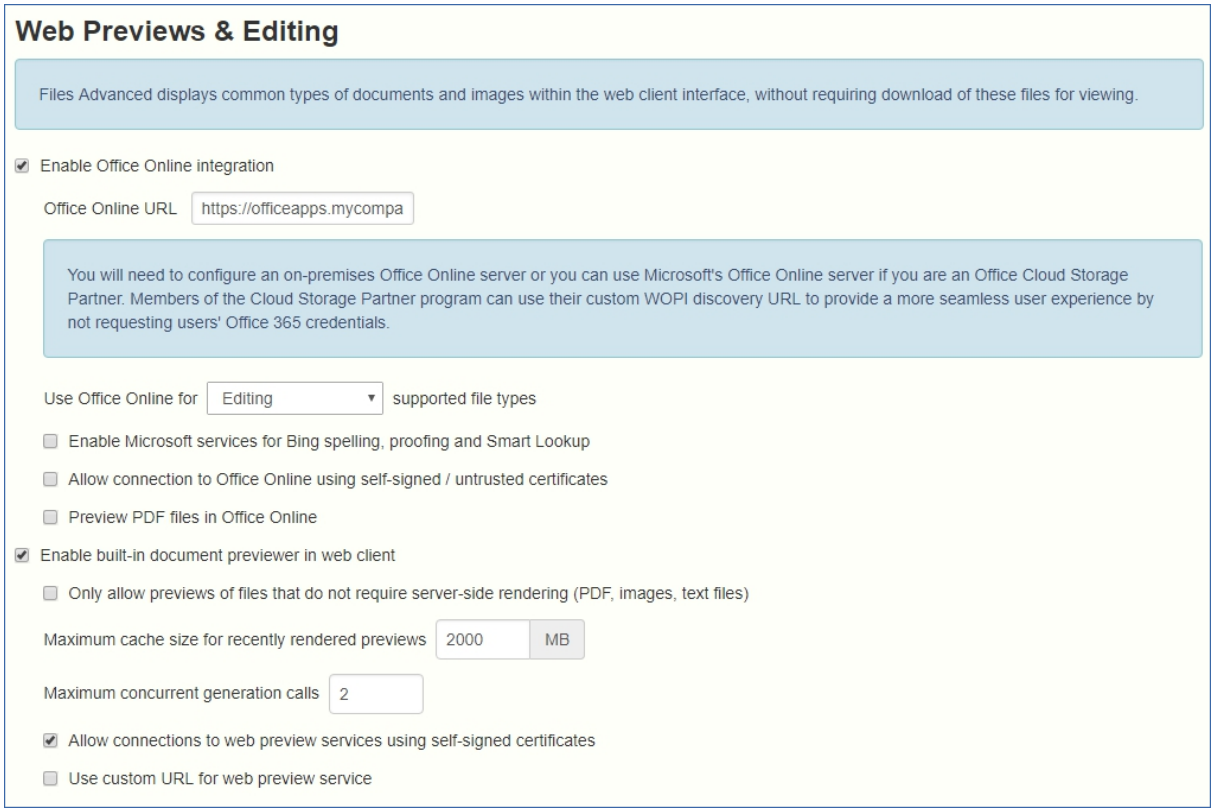
カラー スキームの使用

1. Files Advanced ウェブ インターフェイスを開き、管理者としてログインします。

2. **[全般設定]** → **[ウェブ UI のカスタマイズ]** に移動します。
3. **[カラー スキーム]** ドロップダウンをクリックし、スキームを選択します。
4. **[保存]** を押します。

10.6 ウェブのプレビューと編集

Files Advanced では、一般的なタイプのドキュメントや画像がウェブクライアントをインターフェイス内で表示できます。ファイルをダウンロードする必要はありません。



Office Online との統合を有効にする: Office Online 統合機能を有効にします。

- **Office Online URL**: Office Online の WOPI 検出 URL を入力します。オンプレミスの Files Advanced インストールの場合、この URL を利用できるようにするには、オンプレミスの Office Online セットアップのいずれかを使用している必要があります。Microsoft's Office Online クラウドサービスは、プロバイダーでの用途に使用が制限されており、特殊な証明書とホワイトリストがなければ一般のアクセスはできません。
- **[Office Online の使用]**: **[編集]** を使用すると、Microsoft Office ファイル（**DOCX**、**PPTX**、**XSLX**)を編集することができ、**[表示および編集]** を使用する

と、前述のファイルの編集と **DOC**、**XLS** および **PPT** ファイルのプレビューもできます。この設定を無効にすると、Office ファイルと PDF ファイルはすべて Files Advanced 内部プレビュー機能で開きます。

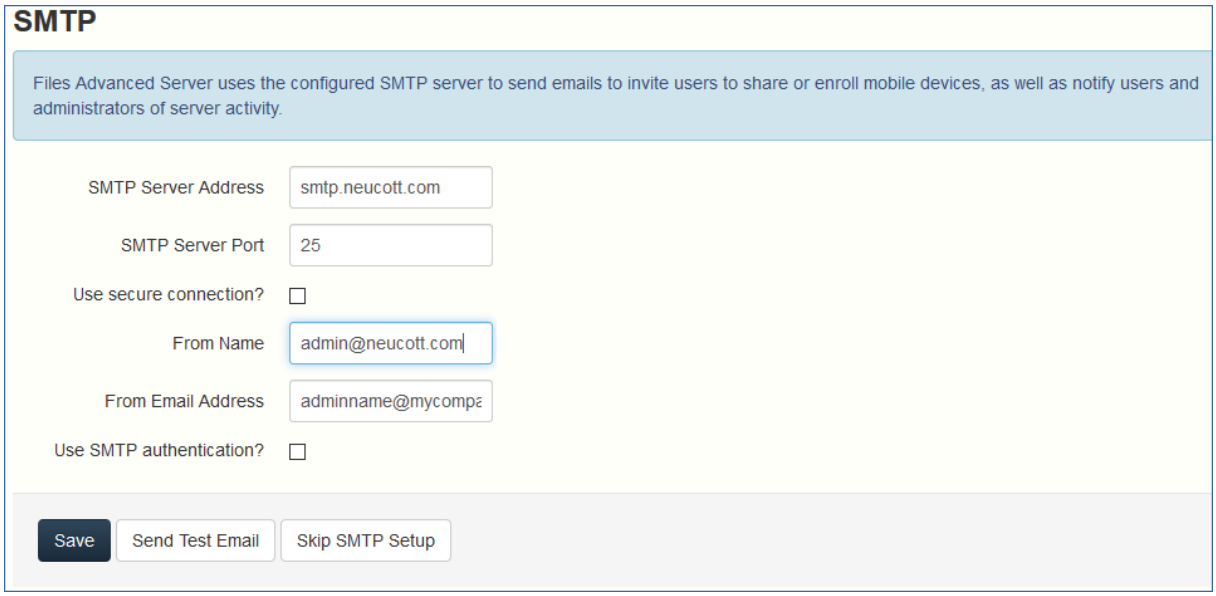
- **[Bing によるスペル、プルーフ、スマート検索用に Microsoft サービスを有効にする]**: スペルチェック機能に Microsoft の Bing サービスを使用します。
- **[自己署名証明書または信頼されていない証明書を使用した Office Online への接続を許可]**: 有効にすると、信頼されていない証明書を使用する Office Online サーバーにユーザーがアクセスできます。
- **[Office Online で PDF ファイルをプレビュー]**: 有効にすると、**[Office Online の使用]** が **[表示および編集]** に設定されている場合に、ユーザーが Office Online で PDF ファイルをプレビューできます。その他の場合はすべて、PDF ファイルは Files Advanced 内部プレビュー機能でプレビューされます。

[ウェブクライアントで組み込みのドキュメントプレビューアーを有効にする]: ウェブをプレビューできます。

- **サーバー側での表示を必要としないファイル（PDF、画像、テキストファイル)のプレビューのみを許可**: 追加の表示を必要としないファイルのプレビューのみを許可することで、ウェブプレビューにより生じる負荷を軽減します。対象となるファイルは、PDF、画像、シンプルテキストファイルです。
- **最近表示されたプレビューの最大キャッシュサイズ**: ファイルをプレビューしたときに保存されるキャッシュの最大サイズを設定します。これにより、最近開いたファイルをプレビューしたときの速度が大幅に向上します。
- **[最大同時生成呼び出し数]**: 同時のプレビュー生成要求の最大数を設定します。
- **自己署名証明書を使用したウェブプレビューのサービスへの接続を許可**: 自己署名証明書を使用しているウェブプレビューサービスへの接続を許可します。これらは他の Files Advanced Tomcat サービスです。
- **ウェブプレビューのサービスにカスタム URL を使用**: 複数の Files Advanced サーバーを使用している場合に、ウェブプレビューを処理するサーバーを指定できます。

10.7 SMTP

Files Advanced サーバーは、構成された SMTP サーバーを使用して電子メールを送信し、ファイルの共有やデバイスの登録のためにユーザーを招待したり、ユーザーや管理者にサーバーアクティビティを通知したりします。

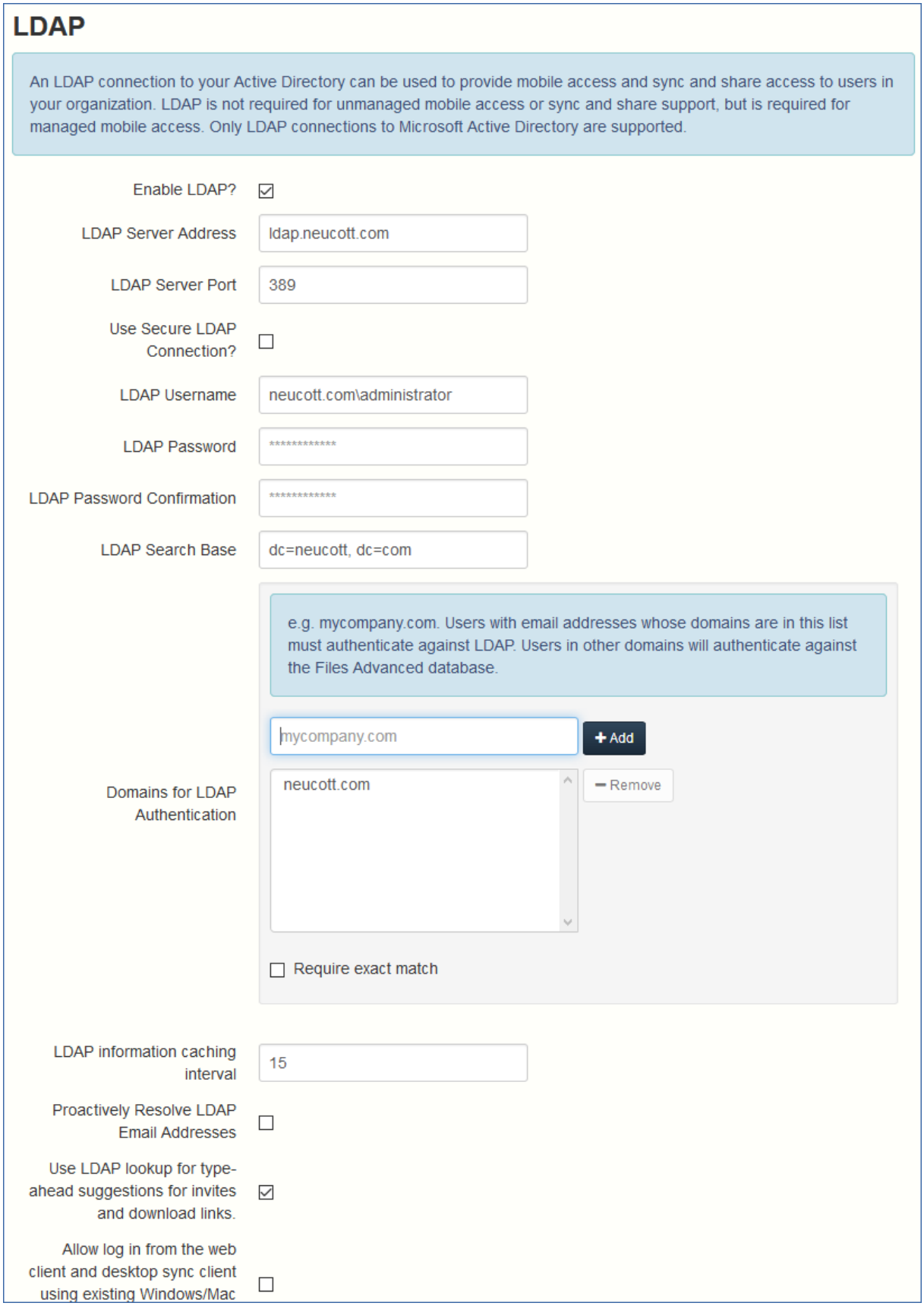


- **SMTP サーバー アドレス**: 招待メールをユーザーに送信する際に使用される SMTP サーバーの FQDN を入力します。
- **SMTP サーバー ポート**: SMTP サーバー ポートを入力します。この設定のデフォルト値はポート 587 です。
- **セキュリティで保護された接続を使用しますか？**: SMTPサーバーに対してセキュリティで保護された SSL 接続を使用するオプションを有効にします。デフォルトでは、この設定は有効になっています。セキュリティで保護された SMTP を無効にするには、ボックスをオフにします。
- **差出人名**: サーバーによって送信される電子メールの「差出人」行に表示されるユーザー名です。
- **SMTP 認証を使用しますか？** : SMTP ユーザー名とパスワードによる接続を有効にするか、SMTP ユーザー名とパスワードを使用しない接続を無効にします。
  - **SMTP ユーザー名**: SMTP 認証用のユーザー名を入力します。
  - **SMTP パスワード**: SMTP 認証用のパスワードを入力します。
  - **SMTP パスワードの確認入力**: SMTP パスワードを再入力して確認します。

- **テスト用の電子メールの送信**: すべての設定が想定通りに機能していることを確認するために、電子メールを送信します。

10.8 LDAP

組織内のユーザーにモバイル アクセス、同期アクセス、および共有アクセスを提供するには、Microsoft Active Directory を使用することができます。LDAP は、管理対象外のモバイル アクセスや、同期および共有サポートに対しては不要ですが、管理対象のモバイル アクセスには必要になります。その他の Active Directory 製品（Open Directory など)は現時点では使用できません。



- **LDAP を有効にしますか？** - 有効にすると、LDAP を構成できます。

- **LDAP サーバー アドレス**: アクセスの規制に使用する Active Directory サーバーの FQDN または IP アドレスを入力します。
- **LDAP サーバー ポート** - デフォルトの Active Directory ポートは 389 です。通常はこれを変更する必要はありません。

  注意: 複数のドメインをサポートしている場合、グローバル カタログ ポートを使用する必要がある可能性があります。

- **セキュリティで保護された LDAP 接続を使用しますか？**: デフォルトで無効になっています。セキュリティで保護された LDAP を使用して Active Directory に接続するには、このボックスをオンにします。
- **LDAP ユーザー名/パスワード** - このログイン資格情報は、すべての LDAP クエリに使用されます。指定サービス アカウントがあってそれを使用する必要があるかどうかについては、AD 管理者に問い合わせてください。
- **LDAP 検索ベース**: ユーザーとグループの検索を始めるルート レベルを入力します。ドメイン全体を検索する場合は、「dc=domainname, dc=domainsuffix」と入力します。
- **LDAP 認証のためのドメイン**: このカンマ区切りリストに含まれるドメインの電子メール アドレスを使用しているユーザーは、LDAP に対して認証する必要があります。 （例えば、電子メール **joe@glilabs.com** のアカウントの LDAP 認証を有効にするには、**glilabs.com** と入力します)。他のドメインのユーザーは、Files Advanced データベースに対して認証します。
  - **完全に一致している必要があります**: 有効にしている場合、**[LDAP 認証のためのドメイン]** で入力されているドメインのユーザーのみが LDAP ユーザーとして処理されます。他のドメインやサブドメインのメンバーであるユーザーは、一時的なユーザーとして処理されます。
- **LDAP 情報をキャッシュする間隔**: Files Advanced で Active Directory 構造がキャッシュされる間隔を設定します。
- **LDAP 電子メール アドレスを事前に解決する**: この設定を有効にすると、Files Advanced は、ログイン イベント時と招待イベント時に、電子メール アドレスが一致するユーザーを Active Directory で検索します。これによりユーザーは自分の電子メール アドレスでログインした直後に招待メールでフィードバックを取得できますが、LDAP カタログが非常に大きい場合は実行に時間がかかることがありま

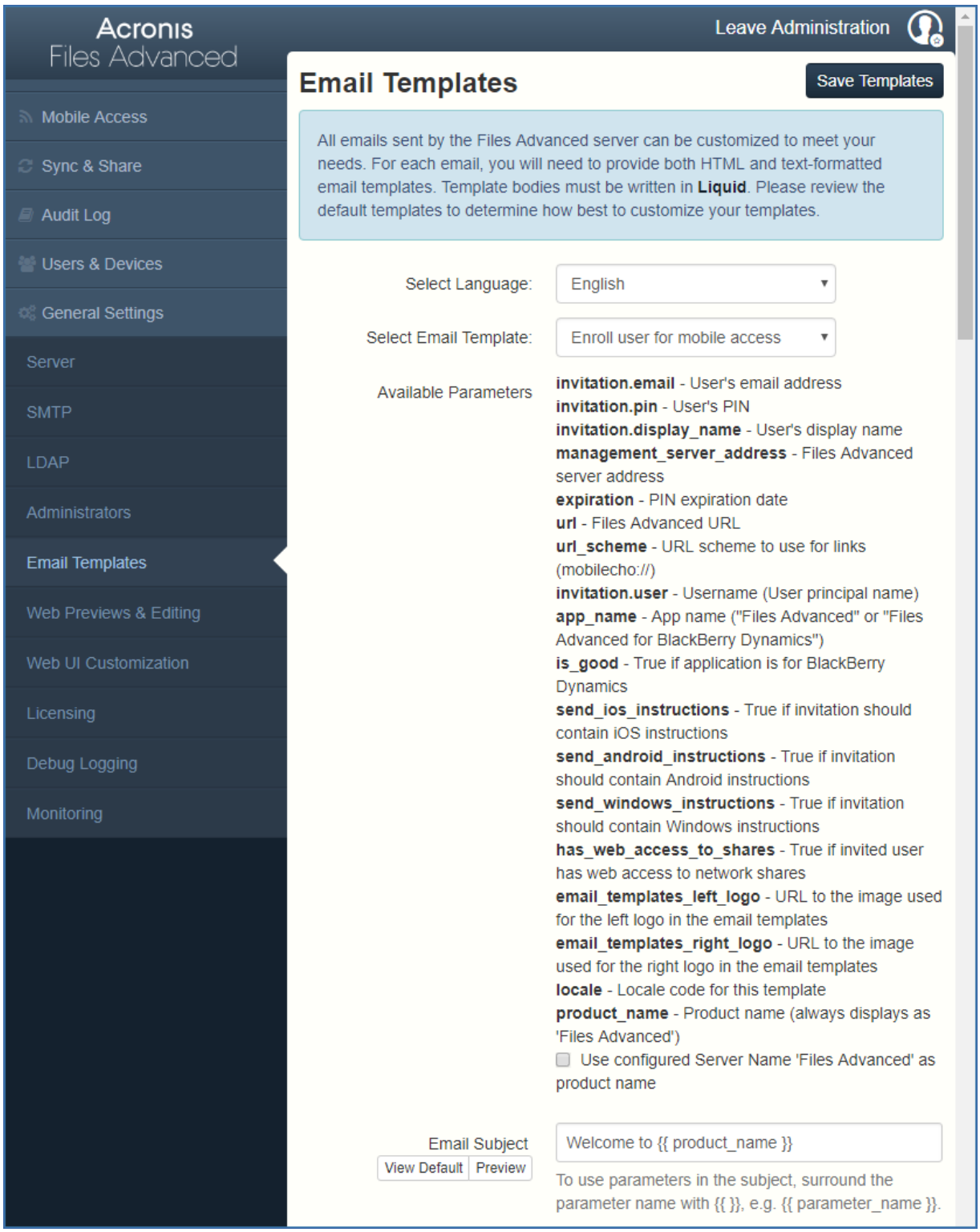
す。認証または招待でパフォーマンスの問題が発生するか応答が遅い場合は、この設定をオフにします。

- **招待およびダウンロード リンクで先行入力候補の LDAP 参照を使用します。**: LDAP ルックアップを使用してオート コンプリートを参照し、電子メール アドレスが一致するユーザーを検索します。大きな LDAP カタログの場合、この検索に時間がかかることがあります。先行入力でパフォーマンスの問題が発生した場合は、この設定をオフにしてください。

10.9 電子メール テンプレート

Files Advanced は電子メール メッセージを広範囲に使用し、ユーザーと管理者に情報をダイナミックに提供します。それぞれのイベントには、HTML 形式とテキスト形式のテンプレートがあります。[電子メール テンプレート] プル ダウン メニューをクリックすると、イベントを選択して両方のテンプレートを編集できます。

Files Advanced サーバーによって送信されるすべての電子メールはニーズに合わせてカスタマイズできます。各電子メールについて、HTML とテキスト形式の電子メール テンプレートを指定する必要があります。テンプレートの本文は、Liquid 内に記述する必要があります。デフォルトのテンプレートを確認して、テンプレートの最適なカスタマイズ方法を判断してください。



注意: Files Advanced のバージョン 7.3 以降では、Liquid がデフォルトのテンプレートマークアップです。ERB に書き込まれているカスタムテンプレートがある場合は、サーバーをアップグレードしていても、ERB がデフォルトのテンプレートマークアップになります。

注意: 電子メールテンプレートにカスタム画像を使用している場合は、これらの画像をインターネット上でホストし、アクセス可能な状態にしておく必要があります。

mobilEcho からアップグレードした場合、電子メール テンプレートに対して加えたカスタマイズは移行されないため、新しいテンプレートをカスタマイズすることが必要になります。前の mobilEcho テンプレートのコピーは、**Legacy mobilEcho files** フォルダにあります。デフォルトでは、そのロケーションは **`C:\Program Files (x86)\Group Logic\Access Server\Legacy mobilEcho files`** です。ファイルの名前は、**invitation.html.erb** および **invitation.txt.erb** です。

- **言語の選択**: 招待メールのデフォルト言語を選択します。

  注意: 登録招待または共有招待を送信する場合、または単一のファイルを共有する場合は、招待ダイアログで別の言語を選択できます。

- **電子メール テンプレートの選択**: 表示または編集するテンプレートを選択します。各テンプレートは特定のイベントに使用します（ユーザーのモバイル アクセスの登録、ユーザーのパスワードの再設定など)。

  注意: Files Advanced をアップデートしたときに、カスタムテンプレートが自動的にアップデートされることは**ありません**。Acronis によるアップデートを使用する場合は、アップデートをカスタムテンプレートに手動で実装する必要があります。この作業は、サポートおよび使用するすべての言語に対して実行する必要があります。

- **使用可能なパラメータ**: 使用可能パラメータはテンプレートごとに異なり、選択したテンプレートに基づいて変わります。
- **電子メールの件名**: 招待メールの件名。**[デフォルトの表示]** のリンクを押すと、その言語でのデフォルトの件名および電子メール テンプレートが表示されます。
- **HTML 電子メール テンプレート**: HTML コードの電子メール テンプレートが表示されます。有効な HTML コードを入力すると、それが表示されます。**[プレビュー]** ボタンをクリックすると、現在のテンプレートのプレビューが表示されます。

- **テキスト電子メール テンプレート**: テキストベースの電子メール テンプレートが表示されます。**[プレビュー]** ボタンをクリックすると、現在のテンプレートのプレビューが表示されます。

注意: テンプレートの編集が終わったら、必ず **[テンプレートの保存]** ボタンをクリックしてください。

注意: 英語のテンプレートを編集しても、他の言語を編集することにはなりません。言語ごとに個別のテンプレートを編集する必要があります。

テンプレートでは、パラメータを組み込んでダイナミックな情報を含めることができます。メッセージが配信されるとき、このパラメータは適切なデータで置き換えられます。

使用できるパラメータは、イベントごとに異なります。

注意: [デフォルトの表示]ボタンをクリックすると、デフォルトテンプレートが表示されます。

10.10 ライセンス

すべてのライセンスのリストが表示されます。

- **ライセンス**: ライセンスのタイプ（試用版、サブスクリプションなど)。
- **同期・共有のライセンス取得済みクライアントの使用**: 現在使用されている同期・共有 LDAP ユーザーライセンス。
- **同期・共有の無料クライアントの使用**: 現在使用されている同期・共有の無料外部ユーザーライセンス。
- **モバイルアクセスクライアントの使用**: 現在使用されているモバイルクライアントのライセンス。

新しいライセンスの追加

1. プロダクト キーをコピーします。
2. **[プロダクト キーの追加]** フィールドに貼り付けます。
3. ライセンス契約を読み、チェックボックスをオンにして同意します。
4. **[ライセンスの追加]** を押します。

注意: ライセンスの固有 ID が同一である場合、許可されているユーザーの数は合計されます。

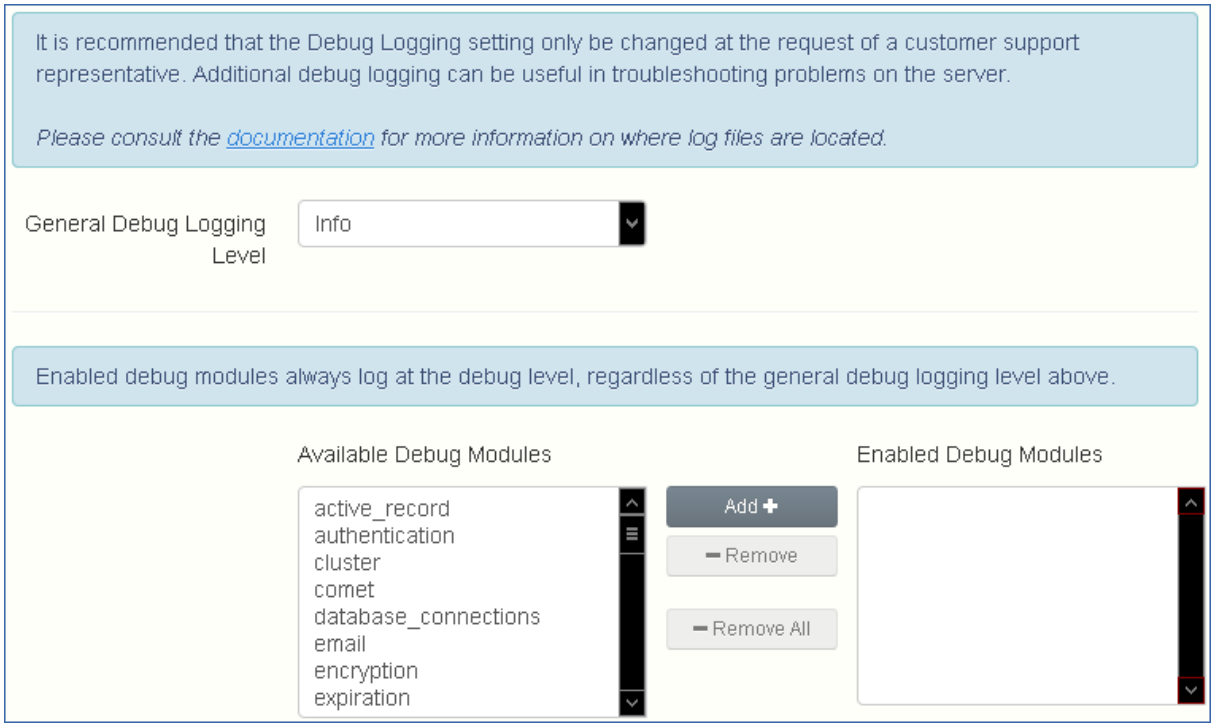
ゲートウェイサーバー用に新しいライセンスを追加する必要はありません

Files Advanced バージョン 6.0 から起動する場合は、Files Advanced サーバーとゲートウェイ サーバーが同じライセンスを共有します。そのため、ゲートウェイ サーバーに手動でライセンスを追加する必要はなくなります。

10.11 デバッグ ログ

このページの設定は拡張ログ情報を有効にするように設計されており、Files Advanced サーバーの構成時とトラブルシューティング時に役立つことがあります。これらの設定は、カスタマ サポート担当者の要求があった場合のみ変更することをお勧めします。追加のデバッグ ログはサーバーで発生した問題のトラブルシューティングに役立つことがあります。

注意: 特定のゲートウェイサーバーにおけるデバッグログの有効化/無効化に関する情報については、「ゲートウェイ サーバーの編集 『119ページ 』」を参照してください。



Files Advanced サーバー バージョン 7.0 以降、**exceptions** モジュールは使用可能なモジュールのリストから削除され、デフォルトで常に有効になります。以前のバージョンの Files Advanced からアップグレードしたユーザーの場合、これまでのように **exceptions**

モジュールがリストに表示されていることがあります。ログオプションを変更し、**[保存]** を押すことで、このモジュールが表示されなくなります。

警告: これらの設定は通常の運用中および本稼動環境では使用しないでください。

- **全般的なデバッグ ログ レベル**: ログに記録する主要レベル（Info、警告、Fatal エラーなど)を設定します

注記: デバッグ モジュールを有効にすると、上記の全般的なデバッグ ログ レベルに関係なく常にデバッグ レベルでログに記録されます。

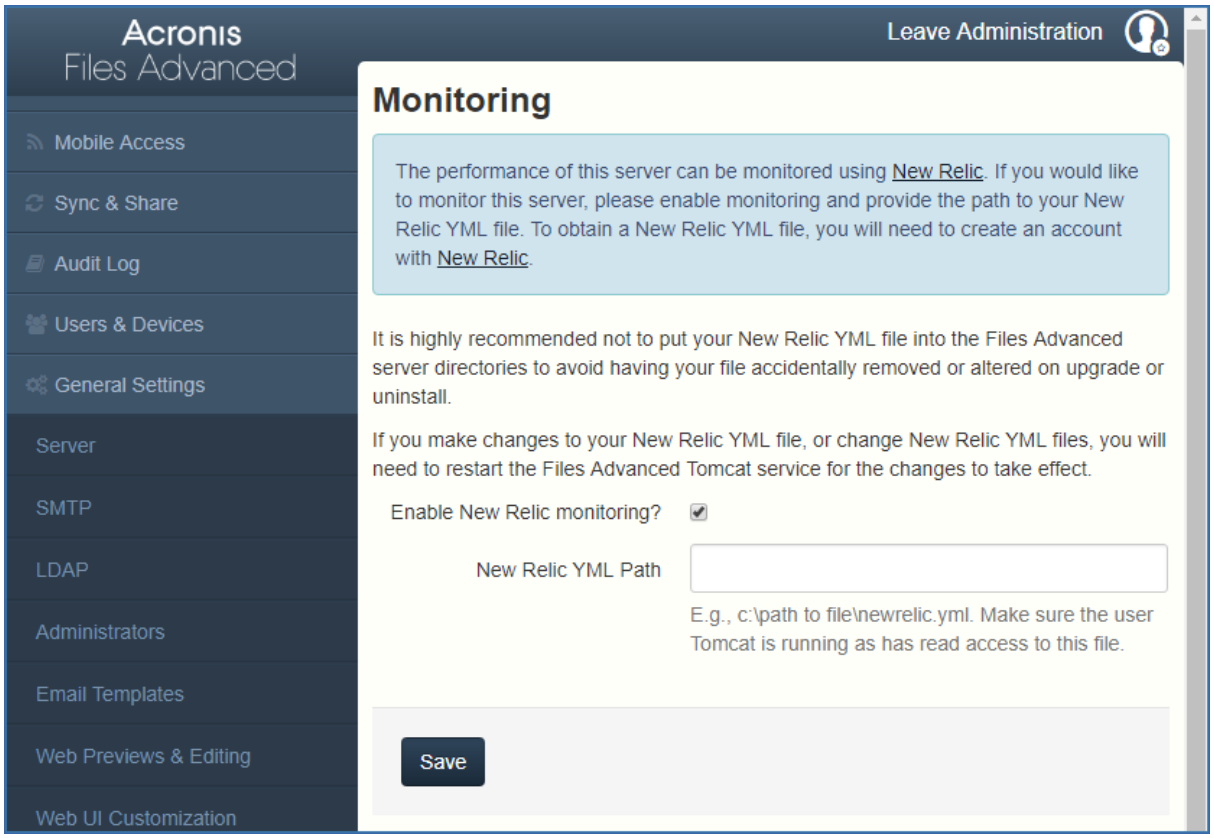
- **使用可能なデバッグ モジュール**: 使用可能なモジュールのリストを表示します。
- **有効になっているデバッグモジュール**: アクティブモジュールが表示されます。

注意: 新規インストールではなく、製品をアップデートした場合、ログ ファイルは **C:\Program Files (x86)\Group Logic\Common\apache-tomcat-7.0.42\logs** に存在します。

注意: Files Advanced をクリーン インストールした場合、ログ ファイルは, **C:\Program Files (x86)\Acronis\Files Advanced\Common\apache-tomcat-7.0.42\logs** に格納されます。

10.12　監視

New Relic を使用してこのサーバーのパフォーマンスを監視できます。このサーバーを監視する場合は、監視を有効にし、New Relic YML ファイルのパスを指定してください。New Relic YML ファイルを取得するには、New Relic でアカウントを作成する必要があります。



注記: アップグレードまたはアンインストール時にファイルが誤って削除されたり変更されたりすることを防ぐために、Files Advanced サーバーがインストールされたディレクトリに New Relic YML ファイルを置かないことをお勧めします。

注記: New Relic YML ファイルに変更を加えたり、New Relic YML ファイルを置き換えたりした場合は、変更を有効にするために Files Advanced Tomcat サービスを再起動する必要があります。

New Relic の監視を有効にしますか？: 有効化した場合は、**New Relic** の構成ファイル（newrelic.yml)へのパスを指定する必要があります。

New Relicのインストール

このインストール方法では、Files Advanced サーバー アプリケーションがインストールされている実際のコンピュータではなく、Files Advanced サーバー アプリケーションを監視できます。

1. http://newrelic.com/ http://newrelic.com/ を開き、New Relic アカウントを作成するか、既存のアカウントでログインします。上記の手順を完了すると、アプリケーションの設定画面に進みます。
2. アプリケーション タイプには **[APM]** を選択します。
3. プラットフォームには **[Ruby]** を選択します。
4. New Relic Starting Guide の手順 3 に示されている New Relic のスクリプト（newrelic.yml)をダウンロードします。
5. Files Advanced ウェブ コンソールを開きます。
6. **[設定]** → **[監視]** に移動します。
7. 拡張子も含めて、newrelic.yml へのパスを入力します（**`C:\software\newrelic.yml`** など)。Files Advanced フォルダ以外のフォルダにもこのファイルを保存して、アップグレード時やアンインストール時に削除や変更されないようにすることをお勧めします。
8. **[保存]** をクリックし、New Relic サイトで **[Active application(s)]** ボタンが有効になるまで数分間待機します。
9. 10 分以上経過したら、Files Advanced Tomcat サービスを再起動して数分待機します。これでボタンがアクティブになります。
10. New Relic ウェブサイトで Files Advanced サーバーを監視できます。

New Relic への接続や監視の設定に関して Files Advanced サーバーがログに記録するすべての情報は、**`C:\Program Files (x86)\Acronis\Common\apache-tomcat-7.0.34\logs`** にある **newrelic_agent.log** というファイルにあります。問題が発生した場合は、このログ ファイルで情報を検索できます。

頻繁に発生する警告やエラーは、次のように始まります。

警告: IP アドレスをキャッシュ中に DNS エラーが発生しました: Errno::ENOENT: このようなファイルまたはディレクトリはありません - C:/etc/hosts which

---

これは、New Relic の別のバグのパッチに使用されているコードの副次的な影響であり、問題はありません。

実際のコンピュータも監視する場合は、次の手順に従います

1. http://newrelic.com/ http://newrelic.com/ を開き、自分のアカウントでログインします。
2. [サーバー] を押し、オペレーティング システムに合った New Relic インストーラをダウンロードします。
3. New Relic モニタをサーバーにインストールします。
4. New Relic サーバー モニタには Microsoft .NET Framework 4 が必要です。New Relic インストーラのリンクは Microsoft .NET Framework 4 Client Profile 専用です。New Relic Server Monitor インストーラを実行する前に、Microsoft Download Center に移動してインターネットから .NET 4 Framework 全体をダウンロードしてインストールする必要があります。

- New Relic がサーバーを検出するまで待機します。

11 メンテナンス タスク

Files Advanced のすべての構成要素をバックアップしたり、ベスト プラクティスの一環やバックアップ プロセスの一部としてバックアップを行う場合、「災害復旧ガイドライン 『195ページ 』」の記事が有用な場合があります。

セクションの内容

11.1 災害復旧ガイドライン

高可用性と迅速な復旧は、Files Advanced のようにミッション クリティカルなアプリケーションにおいて、非常に重要です。ローカルのハードウェアのエラーからネットワークの切断、メンテナンス タスクなど、Files Advanced は、想定内のまたは想定外の状況に陥ることがあります。このため、非常に短い時間で、Files Advanced を稼動状態に復旧させる手段を事前に検討しておくことが必要です。

はじめに:

高可用性は、Files Advanced のようにミッション クリティカルなアプリケーションにおいては、非常に重要です。ローカルのハードウェアのエラーからネットワークの切断、メンテナンス タスクなど、Files Advanced は、さまざまな状況に陥ることがあります。このため、非常に短い時間で、Files Advanced を稼動状態に復旧させる手段を事前に検討しておくことが必要です。

災害復旧の実装には、バックアップの復元、イメージング、視覚化やクラスタリングなど、さまざまな方法があります。次のセクションで、バックアップの復元の手順を説明します。

Files Advanced の構成要素の説明:

Files Advanced は数々の個別の要素で構成されたシソリューションですが、要素は相互に繋がりを持っています。

Files Advanced ゲートウェイ サーバー

注記: 通常は **C:\Program Files (x86)\Acronis\Files Advanced\Gateway Server** に保存されます。

Files Advanced サーバー

注記: 通常は **C:\Program Files (x86)\Acronis\Files Advanced\Access Server** に保存されます。

Files Advanced 構成ユーティリティ

注記: 通常は **C:\Program Files (x86)\Acronis\Files Advanced\Configuration Utility** に保存されます。

ファイル ストア

ファイル ストアのロケーションは、**構成ユーティリティ**を初めて使用したときのインストール中に設定されます。

注記: FileStore は、暗号化形式のユーザー ファイルで構成されています。FileStore 構成は、一般的なファイル コピー ツール（robocopy や xtree)のいずれを使用してもコピーやバックアップを取ることができます。通常、これらの構成は高い可用性のネットワーク ボリュームや NAS に配置され、デフォルトのロケーションとは異なる場合があります。

PostGreSQL データベース。これは Windows サービスとして実行される独立した要素です。Files Advanced にインストールされ使用されます。Files Advanced データベースは、すべての構成、ユーザーとファイルの関連付け、ファイルのメタデータなどを保持しているため、もっとも重要な構成要素の 1 つです。

これらすべてのコンポーネントは、Files Advanced の動作するインスタンスを作成するために必要です。

迅速な復旧プロセスの実装に必要なリソース

災害復旧プロセスを実行するために必要なリソースは、次のとおりです。

- オペレーティング システム、アプリケーション、そのデータをホストする適切なハードウェア。アプリケーションのシステムとソフトウェアの要件に対応したハードウェア。
- 切り替えが必要とされるときにすべてのソフトウェアとデータ要素が確実に、利用できるようにするバックアップと復元プロセスの配置。
- クライアント設定を変更しないか、最小限のクライアント設定の変更で、内部および外部のファイアウォールとユーザーに新しいノードへのアクセス許可するルーティングの規則を含む、ネットワーク接続。
- Active Directory ドメイン コントローラと SMTP サーバーにアクセスするための Files Advanced のネットワーク アクセス。
- セカンダリ ノードへの受信リクエストをリダイレクトする、高速のまたは自動化された DNS 切り替え機能。

手順

バックアップ設定

安全で迅速な復旧シナリオを用意するのに推奨される手法は次のとおりです。

1. セカンダリ、リストア、ノードのすべての要素を Files Advanced のインストールに含めます。用意できない場合は、代わりに（元の)コンピュータの完全なバックアップやイメージを用意します。仮想環境では、定期的にスナップショットを取ることで効果的かつ安価に対応することができます。
2. Files Advanced サーバー ソフトウェア スイート（Apache Software ブランチすべてを含む、前述したすべての構成要素)を定期的にバックアップします。バックアップ タスクには、任意の一般的な、企業向けバックアップ ソリューションを使用します。
3. FileStore は可能な限り頻繁にバックアップしてください。標準的なバックアップ ソリューションを使用できますが、対象となるデータの量によっては、自動化された差分コ

ピー ツールを使用した方が良い選択であったり、ときには望ましい代替の選択である場合もあります。差分コピーを取る方法は、元の FileStore と対象の FileStore 間で異なるデータをアップデートすることにより、作業にかかる時間を最小限に抑えることが可能です。

4. Files Advanced データベースは可能な限り頻繁にバックアップしてください。このタスクは、Windows のタスク スケジューラで実行されるデータベースの自動ダンプ スクリプトによって実行されます。次に、データベース ダンプを一般的なバックアップ ツールでバックアップします。

リカバリ

前述のセクションで示した要件を満たし、実装されている場合は、バックアップ リソースをオンラインに移行するプロセスは比較的シンプルです。

1. 復旧ノードをブートします。必要に応じて IP アドレスなどのネットワークの設定を調整します。Active Directory の接続と SMTP へのアクセスをテストします。
2. 必要に応じて、最新の Files Advanced ソフトウェア スイート バックアップを復旧します。
3. Windows コントロール パネルやサービスを使用して、Tomcat が実行されていないことを確認します。
4. 必要に応じて、FileStore を復元します。FileStore の相対ロケーションが元のコンピュータと同一のロケーションにあることを確認してください。ロケーションが異なる場合は、構成ユーティリティを使用して、ロケーションを調整してください。
5. Windows コントロール パネルやサービスを使用して、PostgreSQL サービスが実行されていることを確認します。
6. Files Advanced データベースを復元します。
7. Files Advanced Tomcat サービスを起動します。
8. DNS を新しいノードのポイントに移行します。
9. Active Directory と SMTP が正常に動作していることを確認します。

11.2 ベストプラクティス

1. データベースの定期的なバックアップ

データベースの継続的なバックアップは、Files Advanced 管理の最も重要な側面の 1 つです。バックアップ処理 『200ページ 』はすべて自動化 『213ページ 』されているため、バックアップを常に最新の状態にできます。

Files Advanced サーバーの非常に大きなデータベースでのデプロイでは、提供するものとは異なるバックアップおよび復元方法を使用する場合があります。

数ギガバイト以上のデータベースでのデプロイでは、**バックアップおよび復元**処理の間にスピードを上げるため、または機能向上のための追加設定が必要となる場合があります。特定の構成に関するヘルプや手順については、当社のテクニカルサポート（http://www.acronis.com/ja-jp/mobilitysupport/)にお問い合わせください。

2. 非常に大規模なデプロイでは、1カ月ごとにデータベースに [バキューム] および [分析] 機能を適用することをおすすめします。

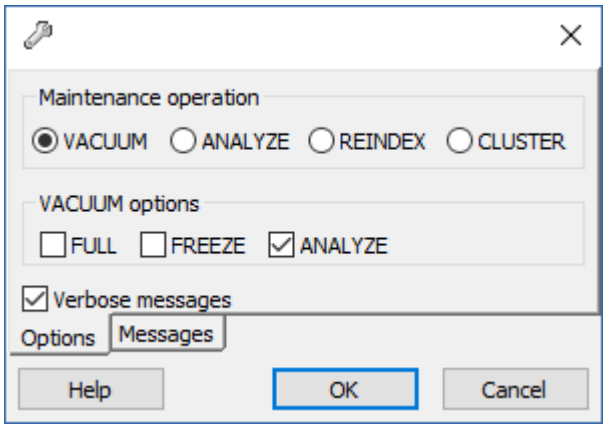
PostgreSQL データベースでは、**vacuuming** という定期メンテナンスが必要です。**バキューム**コマンドは各テーブルに定期的に実行する必要があります。

- 削除またはアップデートされた行で占められるディスク領域は復旧するか再利用してください。
- 非常に古いデータの損失を回避します。
- データ統計をアップデートしてインデックススキャンをスピードアップします。

分析コマンドでは、データベース内のテーブルのコンテンツに関する統計を収集し、結果を保存します。その後、クエリプランナがこれらの統計を使用してクエリの最適な実行プランを決定します。

データベースのバキューム処理や分析を手動で行うには、次の手順を実行します。

1. Files Advanced PostgreSQL 管理者ツール（PgAdmin ともいう)を開き、**localhost** をダブルクリックしてサーバーに接続します。
2. **acronisaccess_production** データベースを右クリックして、**[メンテナンス]** を選択します。
3. **[バキューム]** ラジオボタンと **[分析]** チェックボックスをオンにします。



警告: 非常に大きなデータベースの場合には、バキューム処理にしばらく時間がかかる場合があります。この処理はサーバーへの負荷が低い時間帯に行うことをおすすめします。

4. **[OK]** を押します。
5. **[バキューム]** プロセスが終わると、**[完了]** を押します。
6. PostgreSQL 管理ツールを閉じます。

自動バキュームを設定するには、次の記事を参照してください: **データベースの自動バキューム** **『215ページ 』**

3. 大きなデプロイでは、ロードバランス設定 『247ページ 』またはGateway サーバーのクラスタ化 『131ページ 』の実行を検討してください。

11.3 Files Advanced のバックアップと復元

アップグレードする場合は、Files Advanced サーバーのアップデートまたはメンテナンスを行います。この記事では、データベースのバックアップと復元の基本について説明しま

す。負荷分散構成では、このプロセスは通常のバックアップと復元とほぼ同じです。特定の仕様が関連するステップに追加されます。

注意: Files Advanced サーバーのデータベースが非常に大きく、数ギガバイトに達する場合は、別のバックアップおよび復元の方法が必要になることがあります。ヘルプや手順については、当社のテクニカルサポート（http://www.acronis.com/ja-jp/mobilitysupport/)にお問い合わせください。

注意: Microsoft フェールオーバークラスタでは、一部のパスが異なる場合がありますが、バックアッププロセスは同じです。この処理はアクティブノードで実行する必要があります。また、役割がバックアップ中にフェールオーバーしたり開始しないことを確認する必要があります。

本番環境のバックアップ/復元に進む前に、テスト環境でテストバックアップ/復元を実行することを強くお勧めします。

セクションの内容

7.

1. Files Advanced Tomcat サービスを停止します。

   注意: 複数の Files Advanced Tomcat サービスを負荷分散している場合は、それらをすべて停止します。

2. Files Advanced PostgreSQL Administrator アプリケーションを開き、データベースサーバーに接続します。**postgres** ユーザーのパスワード入力を求められる場合があります。
3. **[データベース]**を展開し、**acronisaccess_production** データベースを右クリックします。
4. **[メンテナンス]** を選択して、**[バキューム]** ラジオボタンを選択し、**[分析]** チェックボックスをオンにします。**[OK]** を押します。
5. データベース、**[スキーマ]**、**[Public]**の順に展開します。**[テーブル]**セクションの数字をメモします。これにより、復旧後にデータベースが正常に復元されたことを確認できます。
6. PostgreSQL Administrator を閉じ、管理者特権でのコマンドプロンプトを開きます。
7. このコマンドプロンプトで、PostgreSQL の bin ディレクトリに移動します。

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

8. 次のコマンドを入力します: **pg_dumpall --host localhost --port 5432 --username postgres --file alldbs.sql**
   - バックアップのファイル名は **alldbs.sql** になります。これは PostgreSQL の bin ディレクトリに保存されます。別の場所に保存する必要がある場合は、上記のコマンド内でパスを使用できます。たとえば、コマンドの末尾を次のように変更します: **--file D:\Backups\alldbs.sql**
   - デフォルト以外のポートを使用している場合は、**5432** を正しいポート番号に変更します。
   - デフォルトの PSQL 管理者アカウント **postgres** を使用していない場合は、上記コマンド内の **postgres** をご使用の管理者アカウント名に変更してください。
   - この手順では、**postgres** ユーザーのパスワードを何回か入力するように求められる場合があります。そのたびにパスワードを入力して Enter キーを押してください。

   注意: パスワードを入力しても、コマンドプロンプトウィンドウの視覚的な変化はまったくありません。

9. バックアップファイルを安全な場所にコピーします。
10. **postgresql.conf** ファイルには重要な設定が含まれているため、このファイルに移動して安全な場所にコピーします。このファイルは PostgreSQL のデータフォルダ内にあります（デフォルトでは **C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL\<version>\Data**）。
1. Files Advanced ゲートウェイサービスを停止します。
2. ゲートウェイサーバーの database フォルダに移動します。デフォルトでは次の場所にあります。
   C:\Program Files (x86)\Acronis\Files Advanced\Gateway Server\database
3. **mobilEcho.sqlite3** ファイルを安全な場所にコピーします。
4. 複数のゲートウェイサーバーを使用している場合は、それぞれに対してこのプロセスを繰り返し、データベースファイルが取り違えられないようにします。

以下のファイルで変更を加えたものがある場合は、Files Advanced 製品を復元または移行した際に設定を転送できるように、バックアップを作成しておくことをお勧めします。

- **postgresql.conf** ファイル。このファイルには、データベース関連の重要な設定が含まれている場合があります。通常、このファイルは **C:\Program Files**

(x86)\Acronis\Files Advanced\Common\PostgreSQL\<version>\Data にあります。

- **web.xml**。デフォルトの場所は **C:\Program Files (x86)\Acronis\Files Advanced\Access Server\Web Application\WEB-INF**です。シングルサインオンの設定が含まれています。
- **server.xml**。デフォルトの場所は **C:\Program Files (x86)\Acronis\Files Advanced\Common\apache-tomcat-<version>\conf** です。Tomcat の設定が含まれています。
- **krb5.conf**。デフォルトの場所は **C:\Program Files (x86)\Acronis\Files Advanced\Common\apache-tomcat-<version>\conf** です。シングルサインオンの設定が含まれています。
- **login.conf**。デフォルトの場所は **C:\Program Files (x86)\Acronis\Files Advanced\Common\apache-tomcat-<version>\conf** です。
- Files Advanced に使用する証明書とキー。
- **acronisaccess.cfg**。デフォルトの場所は **C:\Program Files (x86)\Acronis\Files Advanced\Access Server** です。
- カスタムカラースキーム。デフォルトの場所は **C:\Program Files (x86)\Acronis\Files Advanced\Access Server\Web Application\customizations**です。
- **pg_hba.conf**。デフォルトの場所は **C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL\<version>\Data** です。
- **newrelic.yml** ファイル。Files Advanced サーバーのチェックに **New Relic** を使用している場合。

1. **[サービス]** コントロールパネルを開いて、Files Advanced Tomcat サービスを停止します。

   注意: 負荷分散構成では、すべての Files Advanced Tomcat サービスを停止します。

2. Files Advanced PostgreSQL Administrator アプリケーションを開き、ローカルデータベースサーバーに接続し、**[データベース]** を選択して **acronisaccess_production** という名前のデータベースがあることを確認します。
3. データベースを右クリックして、**[更新]** を選択します。

4. データベース、**[スキーマ]**、**[Public]** の順に展開して、**[テーブル]** に項目がないことを確認します。
   - データベースにテーブルがある場合は、データベースを右クリックして、名前を **oldacronisaccess_production** に変更します。最後に、**[データベース]** に移動し、右クリックして **acronisaccess_production** という名前の新しいデータベースを作成します。
5. PostgreSQL Administrator を閉じ、管理者特権でのコマンドプロンプトを開きます。
6. このコマンドプロンプトで、PostgreSQL の bin ディレクトリに移動します。

   例: cd "C:\Program Files\Acronis\Access\Common\PostgreSQL\9.3\bin"
7. データベースのバックアップファイル **alldbs.sql**（またはユーザーが付けたファイル名)を **bin** ディレクトリにコピーします。
8. コマンドプロンプトで、次のコマンドを実行します: **psql -U postgres -f alldbs.sql**
9. **postgres** パスワードを求められたら入力します。

   注意: データベースサイズによっては、復元にしばらく時間がかかることがあります。

   復元が完了したら、コマンドプロンプトのウィンドウを閉じます。
10. Files Advanced PostgreSQL Administrator アプリケーションを再度開き、ローカル・データベース・サーバーに接続します。
11. **[データベース]** を選択します。
12. **acronisaccess_production** データベースを開き、**[スキーマ]**、**[Public]** の順に展開します。**[テーブル]** の数が、「Files Advanced のデータベースのバックアップ」セクションの手順 5 と同じであることを確認します。

注意: データベースを復元する Files Advanced サーバーのバージョンが、データベースバックアップのバージョンより新しく、Files Advanced Tomcat サービスが既に開始されている場合、新しい Files Advanced サーバーのデータベース内のテーブル数がバックアップ実行時のテーブル数より多い場合があります。

1. Files Advanced ゲートウェイサービスを停止します。
2. **mobliEcho.sqlite3** ゲートウェイサーバーデータベースのバックアップを新しいゲートウェイサーバーの database フォルダ（デフォルトでは **C:\Program Files (x86)\Acronis\Files Advanced\Gateway Server\database**)にコピーし、既存のファイルと置き換えます。

3. すべてのゲートウェイサーバーに対してこのプロセスを繰り返します。

Files Advanced の構成ファイル（web.xml、server.xml、krb5.conf、証明書、カスタムカラースキーム、電子メールテンプレート、pg_hba.conf、または newrelic.yml)へのすべてのカスタマイズをコピーして、新しいファイルに加えてください。

バックアップ/復元または別のコンピュータへの移行に成功したら、Files Advanced をオンラインに戻し、すべての設定が正しいことを確認します。

通常導入のオンライン化

1. Files Advanced 設定ユーティリティを起動して、すべての設定が正しいことを確認してください。
2. すべてのサービスを開始するには、[OK] を押します。
3. これにより、すべてのサービスが同時にオンラインになり、すべての Files Advanced 機能が復元されるはずです。
4. 一部のコンポーネントが別のコンピュータ上に存在する場合は、そのコンピュータに移動してそれらを開始する必要があります。この場合は、PostgreSQL サービスが実行していないと、Files Advanced Tomcat サービスが正常に開始されません。

負荷分散導入のオンライン化

1. プライマリとして機能する Files Advanced サーバーの 1 つを選択します。このサーバーは、最初にオンライン化するという意味でのみプライマリになります。
2. PostgreSQL サービスが別のコンピュータ上に存在する場合は、そのサービスを最初に開始して、Files Advanced サーバーに影響を与えないようにします。
3. プライマリ Files Advanced サーバー用のコンピュータに移動して、Files Advanced 設定ユーティリティを開始します。
4. そこにあるすべての設定が正しいことを確認します。問題がなければ、[OK] を押してすべてのサービスを開始します。
5. Files Advanced ウェブコンソールを開き、管理者としてログインします。すべての設定が正しいことを確認します。

6. 設定を確認したら、Files Advanced コンポーネントが存在する各コンピュータの調査に進んで、設定ユーティリティ経由でそれらのコンポーネントを開始します。

11.4 Windows での Tomcat ログ管理

Tomcat は通常の動作の一部として情報を作成し、複数のログ ファイルに書き込みます。

定期的に消去されない限り、これらのファイルは蓄積していき、貴重な容量を消費します。一般的に近年の IT 業界では、これらのログが提供する情報の価値が低いと考えられるようになりました。特定のポリシーを伴う法規のような他の要素が関係していない限り、これらのログ ファイルはある程度の日数の間システムに保持しておきます。

はじめに

Tomcat は通常の動作の一部として情報を作成し、複数のログ ファイルに書き込みます。Windows では、これらのファイルは通常次のディレクトリに保存されています。

“ **C:\Program Files (x86)\Acronis\Files Advanced\Common\apache-tomcat-7.0.34\logs**”
Files Advanced のログは、同一のディレクトリに別個のファイルとして保存されています。

Files Advanced のログ ファイルは **acronisaccess_date** という名前です。

不要なログ ファイルの削除のタスクを自動化する機能を持つツールは多数用意されています。たとえば、Windows に組み込まれている ForFiles コマンドを使用することができます。

情報: ForFiles の構文と例の詳細については、
http://technet.microsoft.com/ja-jp/library/cc753551%28v=ws.10%29.aspx
http://technet.microsoft.com/ja-jp/library/cc753551(v=ws.10).aspx を参照してください。

サンプルプロセス

このサンプル プロセスでは、特定の日数経過したログ ファイルを自動的に消去する手順を説明します。サンプルのバッチ ファイル内にはこの数値がパラメータとして定義されており、数々の適用されているポリシーに適合するように変更させることが可能です。

情報: サンプルスクリプト（バッチ)ファイルは Windows Server 2008 で動作するように設計されています。スクリプトをダウンロードするにはこちらをクリックしてください。
または、スクリプトコードをコピーして、空のテキストドキュメントに貼り付けることもできます。「AASTomcatLogPurge.bat」と名前を付けて保存してください。

完全なバッチ スクリプト コードを入手するにはここをクリック...

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


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

警告: このサンプルはガイドラインとして提供するものです。ユーザーの実装環境の要件に基づいて必要なプロセスを計画し、導入してください。サンプル、すべての条件や環境ではテストされていません。また適合するものではありません。サンプルは基礎としてご利用いただき、ファイル削除の実作業はユーザーの責任に基づき行ってください。**サンプルは、オフラインであらかじめ完全にテストしていない限り、本稼動環境で使用しないでください。**

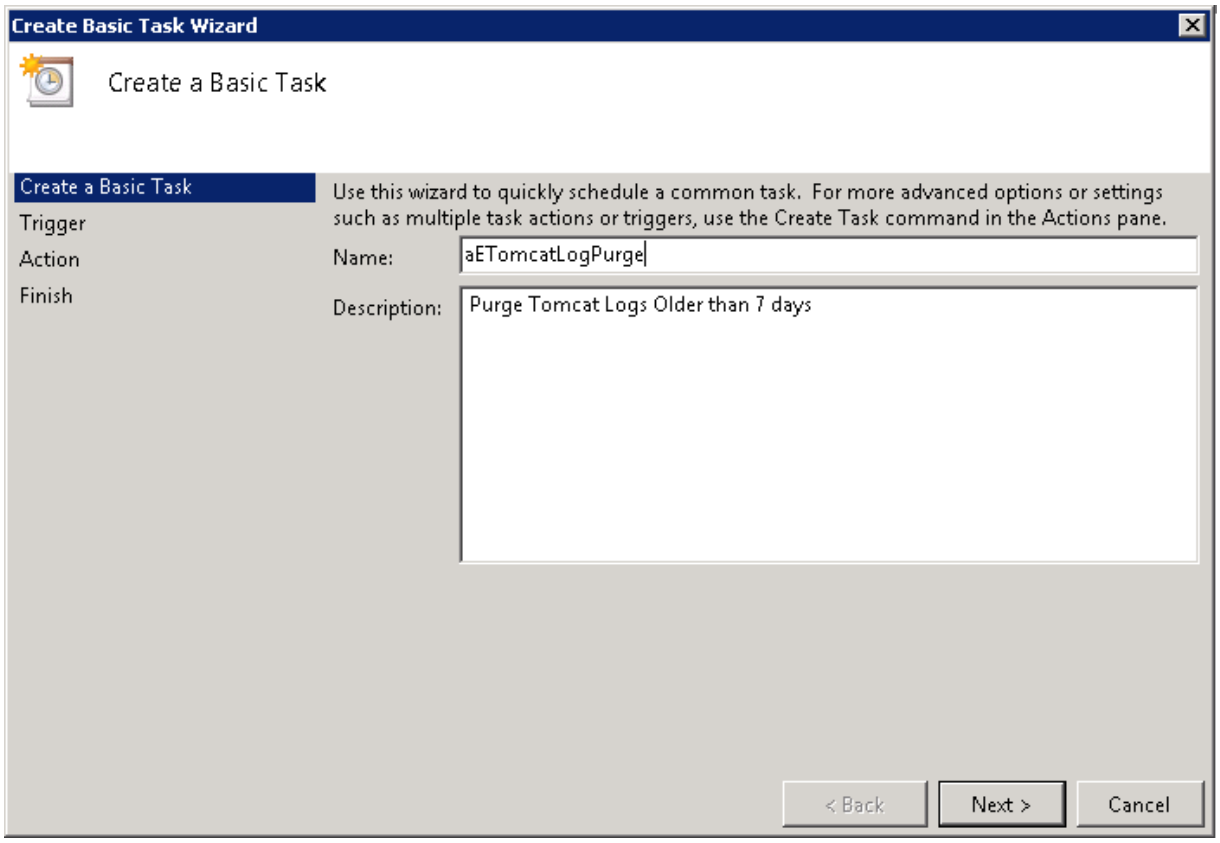
手順

1. Files Advanced（Tomcat)が動作しているコンピュータにスクリプトをコピーし、メモ帳か、適切なシンプルなテキスト エディタを使用して開きます。
2. 下図に示されたセクションを探して、LogPath の値と NumDays の値をユーザー固有のパスとファイル保持の設定の値に編集します。

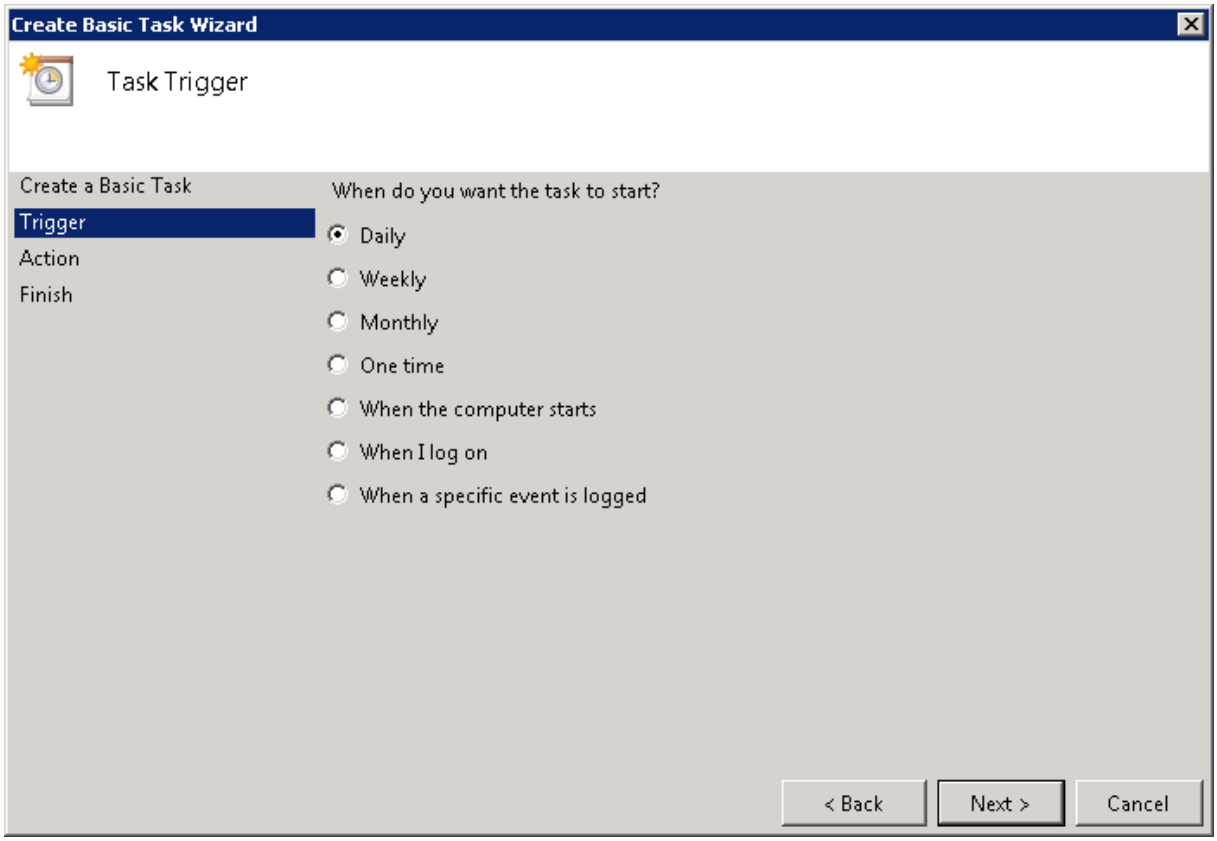
```
REM ===== CONFIGURATIONS ==================================================
REM Note: all paths containing spaces must be enclosed in double quotes
 REM Edit this file and set LogPath and NumDays below
REM Path to the folder where all Tomcat logs are
 set LogPath="C:\Program Files (x86)\Group Logic\Common\apache-tomcat-7.0.34\logs"

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

Files Advanced では、Tomcat と同一のフォルダにログ ファイルが保存されています（**C:\Program Files (x86)\Acronis\Files Advanced\Common\apache-tomcat-7.0.34\logs**）。

3. ファイルを保存します。
4. プロセスを自動化するには、タスク スケジューラを開き、タスクを新しく作成してください。タスクの新しい名前と説明を定義します。

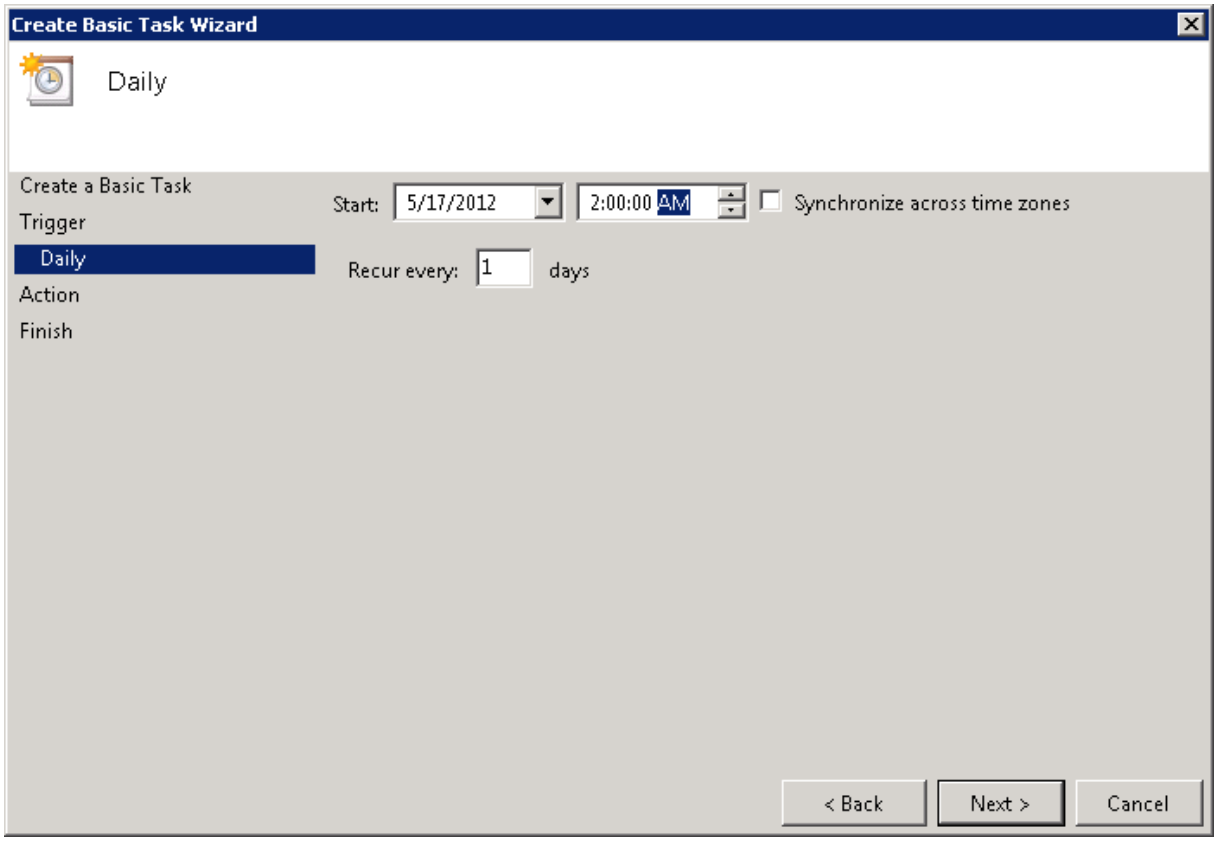


5. タスクが毎日実行されるように設定します。

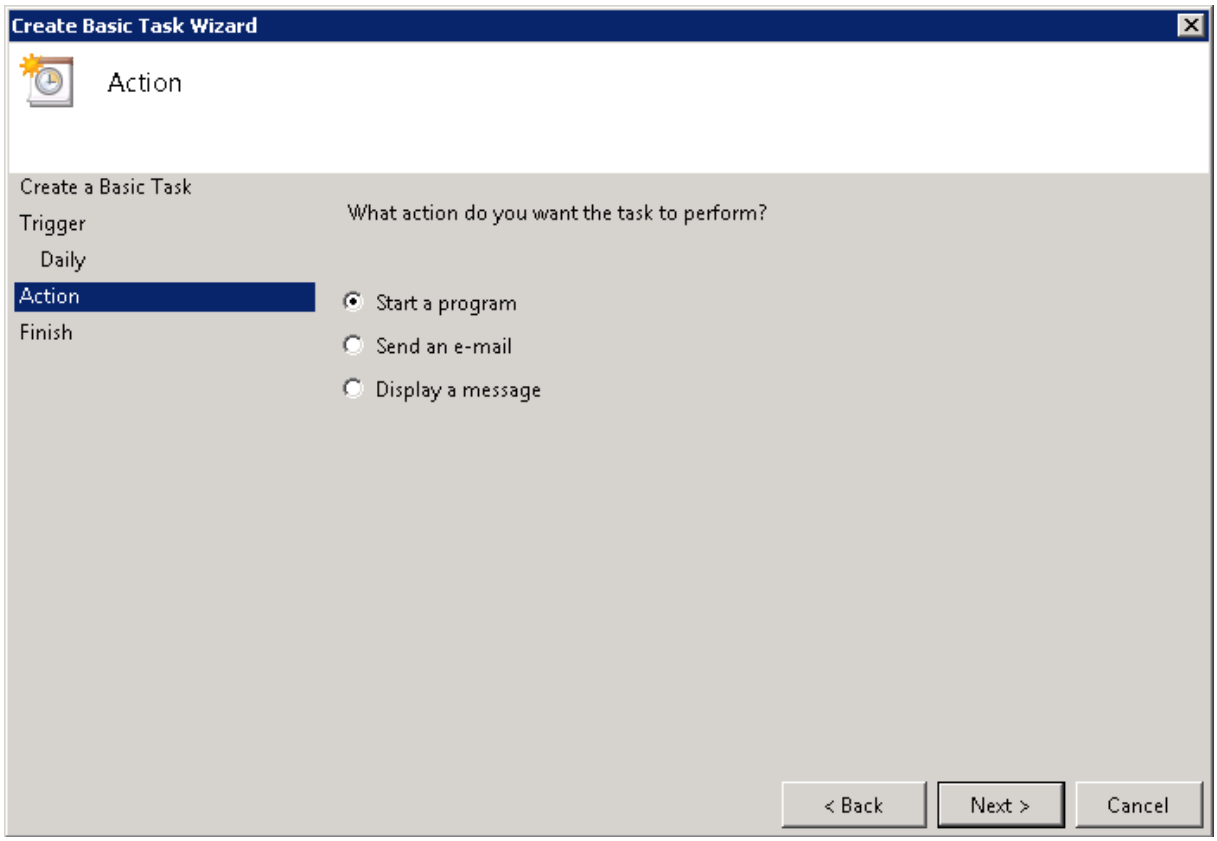


6. タスクが開始される時刻を定義します。このプロセスは、システムに極めて高い負荷がかかっている状態や、他のメンテナンス プロセスが実行中でないときに実行することを

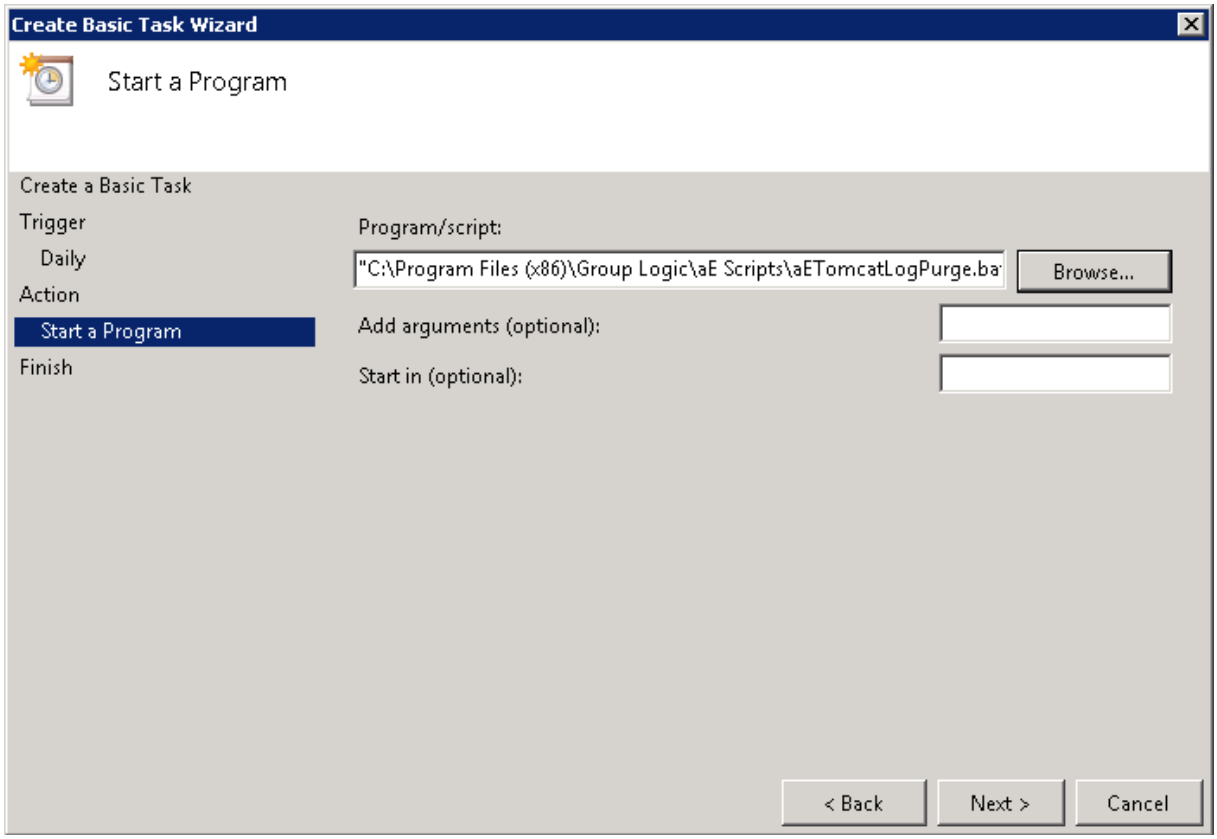
お勧めします。



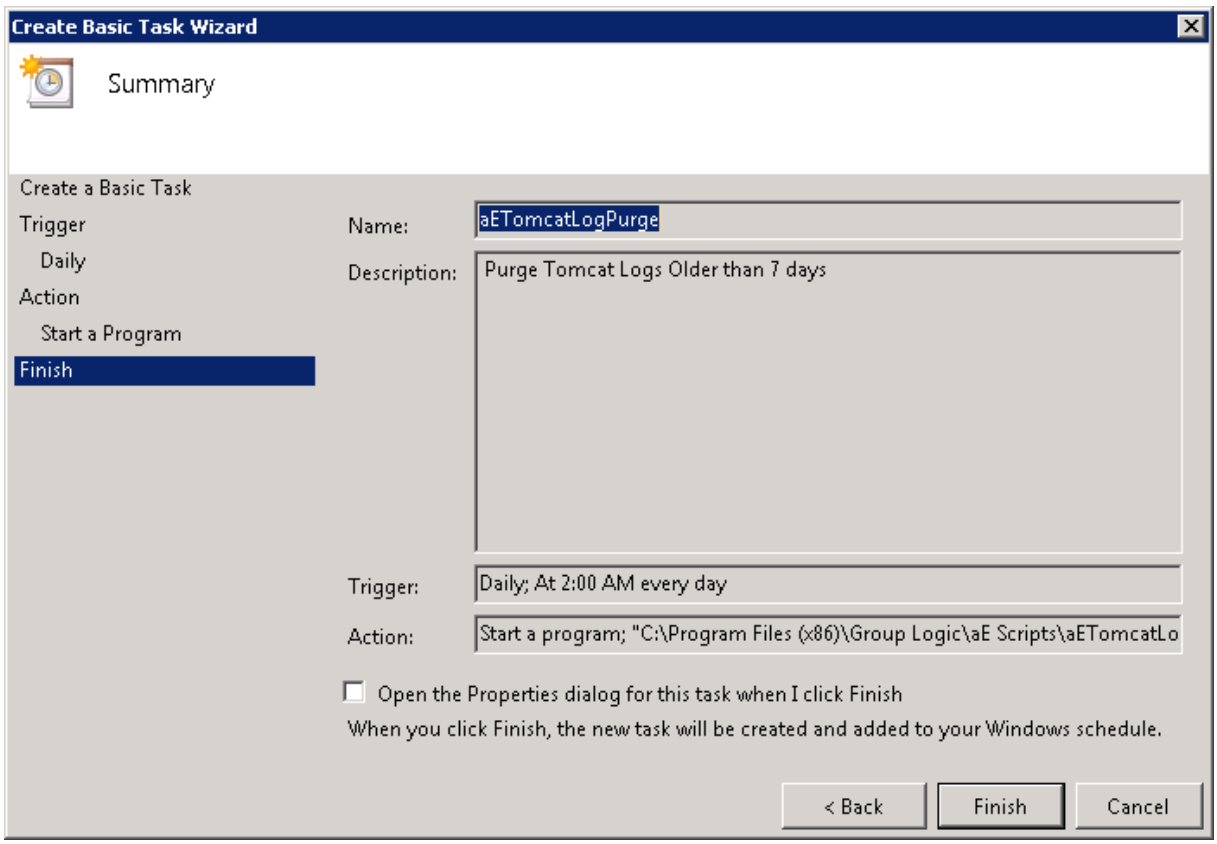
7. アクション タイプを「プログラムの開始」に設定します。



8. [参照] ボタンをクリックし、スクリプト（バッチ)ファイルを参照して選択します。



9. 終わったら [完了] をクリックします。



10. タスク リストでタスクを右クリックすると、プロパティを選択し、ユーザーのログイン状態に関わらず、たとえユーザーがログインしていなくても、タスクが実行されるか検証することができます。
11. タスクを選択して右クリックし、[実行] を選択することで、タスクが正常に構成され、適切に実行されるかを確認することができます。スケジューラのログには、開始や停止、すべてのエラーが報告されます。

11.5 データベースの自動バックアップ

Windows タスク スケジューラを活用して、Files Advanced データベースの自動バックアップ スケジュールを簡単に設定できます。

データベース バックアップ スクリプトの作成

1. **メモ帳**（または他のテキスト エディタ)を開き、以下を入力します。

```
@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. Files Advanced のインストール時に入力した **postgres** ユーザーのパスワードで "**password**" を置き換えます。
3. バックアップを保存するフォルダへのパスで **C:¥destination folder** を置き換えます。
4. ファイル名を **DatabaseBackup.bat** にし、ファイルの種類で **[すべてのファイル]** を選択して保存します（拡張子が重要です)。
5. バージョン番号のディレクトリ（¥9.3¥ など)にある PostgreSQL のインストール フォルダにファイルを移動します。

スケジュール タスクの作成

1. **[コントロール パネル]** を開き、**[管理ツール]** を開きます。
2. **[タスク スケジューラ]** を開きます。
3. **[操作]** をクリックし、**[タスクの作成]** を選択します。

[全般] タブで次の操作を実行します。

1. タスクの名前と説明を入力します（例: AAS Database Backup)。
2. **[ユーザーがログオンしているかどうかにかかわらず実行する]** を選択します。

[トリガー] タブで次の操作を実行します。

1. **[新規]** をクリックします。
2. **[タスクの開始] で [スケジュールに従う]** を選択します。
3. [毎日] を選択し、スクリプトを実行する時間と、スクリプトの再実行頻度（データベースをバックアップする頻度)を選択します。
4. **[詳細設定]** で **[有効]** を選択し、**[OK]** を押します。

[操作] タブで次の操作を実行します。

1. **[新規]** をクリックします。
2. **[操作]** で **[プログラムの開始]** を選択します。

3. **[プログラム/スクリプト]** で **[参照]** を押し、**DatabaseBackup.bat** ファイルを選択します。
4. **[開始 (オプション)]** で、スクリプトがあるフォルダへのパスを入力します。スクリプトへのパスが **C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL\9.3\PSQL.bat** の場合は、「 **C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL\9.3**」と入力します。
5. **[OK]** を押します。
6. 他のタブで追加の設定を設定し、**[OK]** を押します。
7. 現在のアカウントの認証情報が要求されます。

11.6 データベースの自動バキューム

このガイドでは、PostgreSQL データベースを実行し、バキュームするスケジュールタスクを作成する方法について説明します。 特にデプロイに大きなデータベース（数ギガバイト)がある場合には、バキューム処理が重要となります。

注: PostgreSQL は自動バキュームを実行するように設定ファイルで設定されています。サーバーの負荷が高い場合には処理を行わないように設計されているため、高負荷のデプロイにおいては自動バキュームが実行されない可能性があります。このような場合には、最低月に 1 回はバキューム処理を実行するようにスケジュールタスクを設定するのが最善策です。

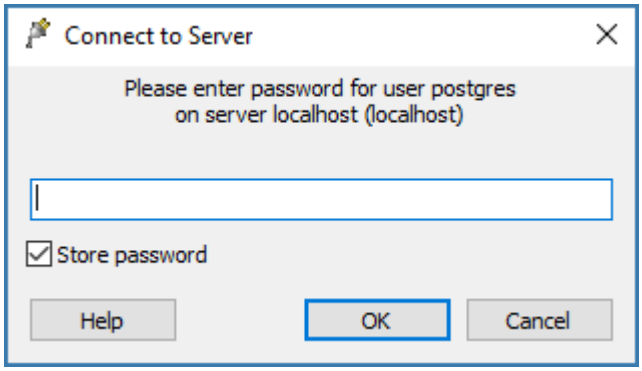
PostgreSQLの構成とスクリプトの作成

タスクが実行可能なことの確認

ご自身の PostgreSQL のパスワードが、pgpass ファイルに保存されていることを確認する必要があります。保存されていない場合には、スクリプトが動作しません。簡単に確認するには、Files Advanced PostgreSQL 管理ツールを使用します。

1. Files Advanced PostgreSQL Administrator を開きます。これは Windows の [スタート] メニューの [Files Advanced] フォルダにあります。
2. データベースに接続し、ダイアログが開くとパスワードを入力します。**[パスワードを保存]** チェックボックスを有効にして、**[OK]** をクリックします。PostgreSQLのパスワードが pgpass ファイルに保存されます。このファイルは **C:\Users\<currentUser>\AppData\Roaming\postgresql** 内に作成されます。

注: 保存パスワードに関する情報を示したダイアログが表示されることがありますが、これは正常です。[OK] を押します。



- または、手動で **pgpass.conf** という名前のファイルを作成し、テキスト **localhost:5432:*:postgres:yourpassword** をファイルに入力して保存することもできます。
- このとき、必ず**実際の** postgres ユーザーパスワードと正しいポートを入力してください。ファイルを保存します。

3. この例では、**pgpass.conf** ファイルをコピーして **D:¥Backup¥**フォルダに置きます。スケジュールタスクを実行するユーザーは、このファイルに対する読み取りアクセス権を持っている必要があります。

スクリプトの作成

以下の例では、PostgreSQL の **bin** ディレクトリのパスは **C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL\<VERSION>\bin**に設定されています。

注意: カスタム インストールまたは古いインストールを使用する場合には PostgreSQL **bin** フォルダを指すようにパスを編集する必要があります（例: C:¥Program Files (x86)¥Acronis¥Access¥Common¥PostgreSQL¥9.4¥bin¥)。

1. ログファイルを保存するフォルダを作成し、タスクを実行するユーザーにこのフォルダに対する読み取り、書き込み、および実行アクセス権を与えます。コンピュータの管理者として操作することをおすすめします。この例では、ログフォルダは **D:\Backup**です。
2. 任意のテキストエディタ（例: メモ帳)を開き、以下のスクリプトを貼り付けます。

```
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
```

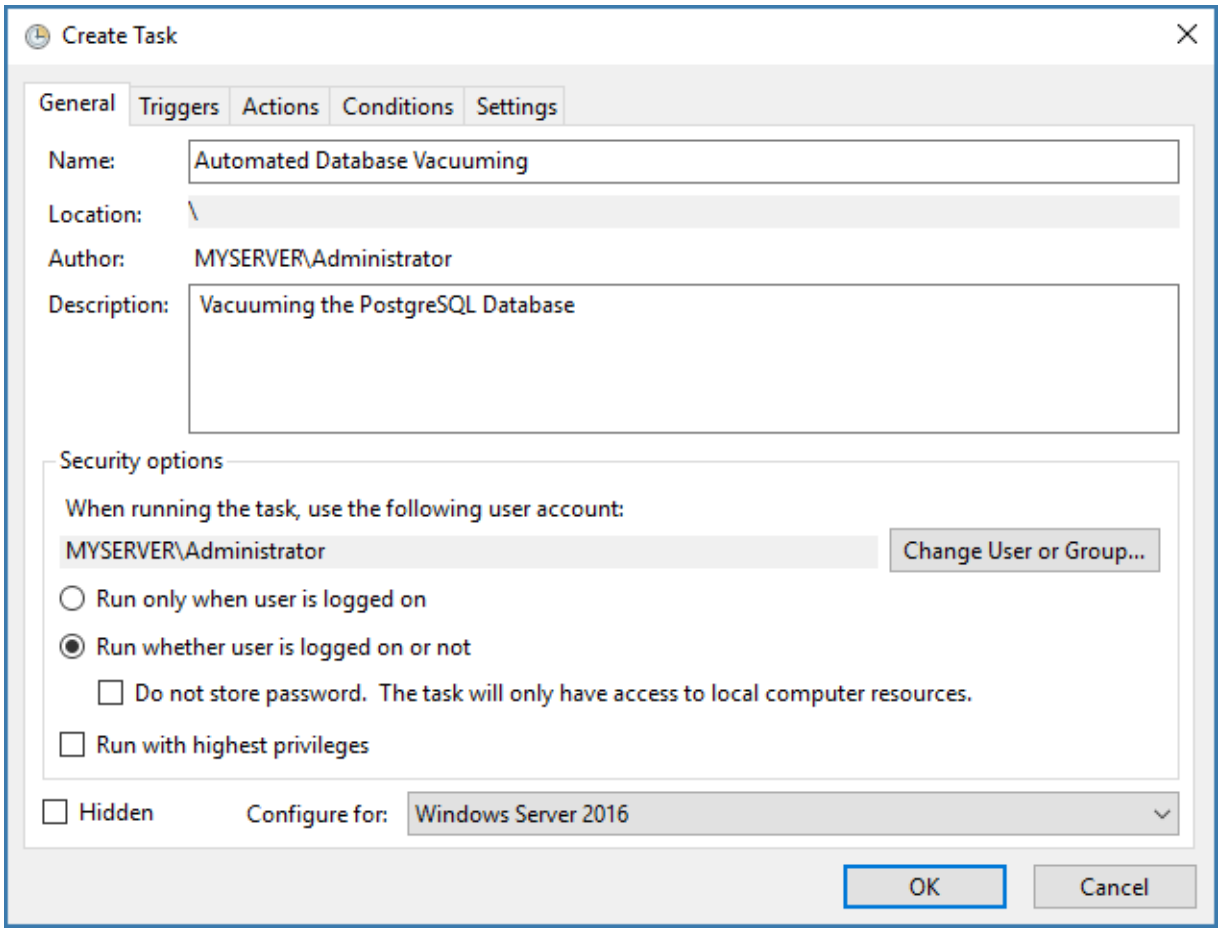
3. このスクリプトをデプロイ環境に合うように編集します。
   - 実際に **psql.exe** があるパスに変更します。
   - デフォルトのポート番号を変更している場合には、**--port** の設定を正しいポート番号に変更します。
   - 別の PostgreSQL ユーザーを使用している場合には、 **--username=**の設定を **postgres** から対象のユーザー名に変更します。
   - パスの **D:\Backup** の部分を、ログを格納する任意のログフォルダの場所に変更します。
   - pgpass.conf ファイルに対するパスの **D:\Backup**の部分を、このファイルに対するパスに変更します。
4. **vacuum.bat** という名前でファイルを保存します。保存する際には、**[ファイルの種類]** で **[すべてのファイル]** を選択していることを確認してください。

注: 日付の形式によっては、この**.log** ファイルの作成に失敗する場合があります。日付の形式を確認するには、コマンドプロンプトを開いてコマンド **echo %date%** を実行してください。日付にフォワードスラッシュなどの不正な文字が含まれている場合には、他の文字に変更する必要があります。上記の例では、**:/=.**は変更する部分です。問題が発生した場合は、アクロニスサポートにお問い合わせください。

タスクスケジューラの設定

1. **[コントロールパネル]** → **[管理ツール]** → **[タスク スケジューラ]** の順にクリックして **[タスク スケジューラ]** を開きます。

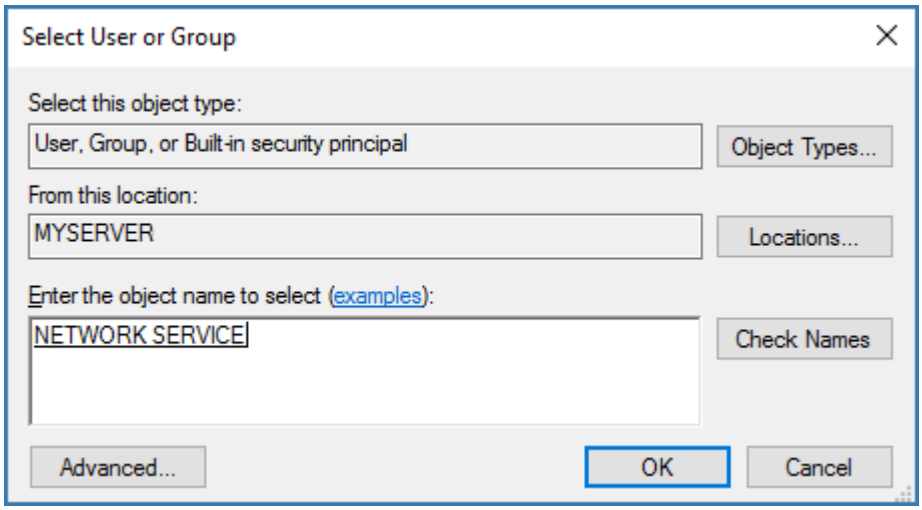
2. **[タスク スケジューラ (ローカル)]** を右クリックし、**[タスクの作成]** を選択します。



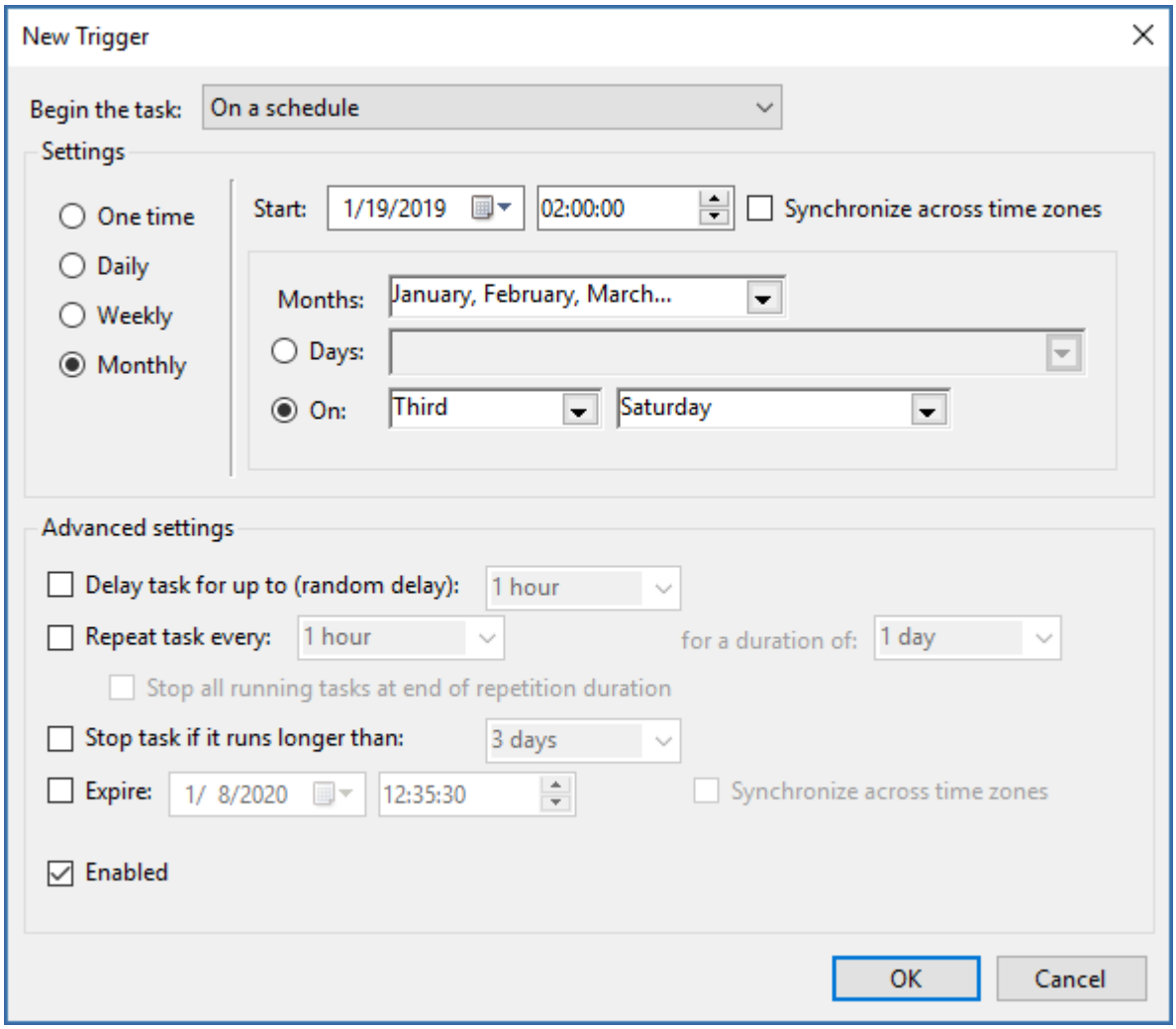
3. **[全般]** タブの設定:

   - **[名前]** と **[説明]** を入力します。
   - **[ユーザーがログオンしているかどうかにかかわらず実行する]** を選択します。

- **[タスクの実行時に使うユーザー アカウント]**を、このタスクを実行するユーザーに設定します。コンピュータの NETWORK SERVICE アカウントを使用することをおすすめします。

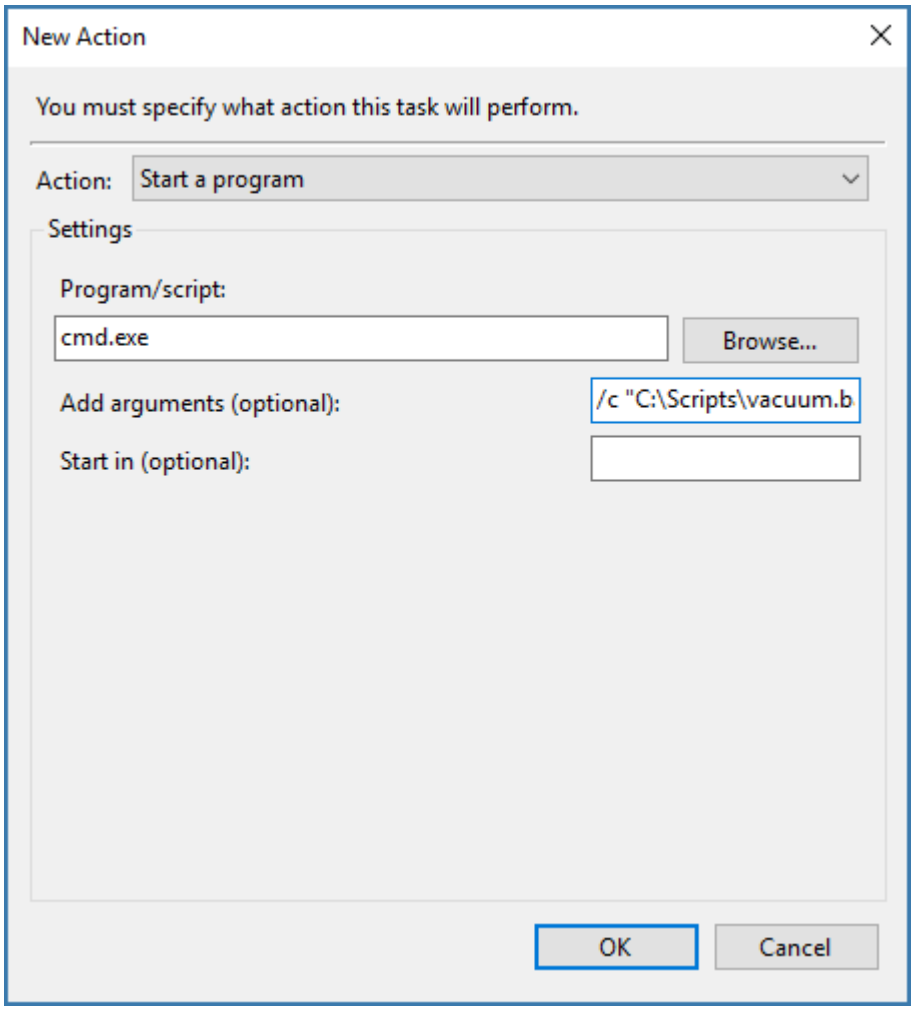


4. **[トリガー]** タブの設定:



- **[新規]** をクリックして、バキュームを実行するスケジュールを設定します。サーバーへの負荷が低い時間帯に行うことをおすすめします。バキューム処理は、最低月に 1 回実行することをおすすめします。

5. **[操作]** タブの設定:



- **[新規]** をクリックし、**[操作]** で **[プログラムの開始]** を選択します。
- **[プログラム/スクリプト]** に **`cmd.exe`** を指定します。
- **[引数の追加]** に次のとおり入力します: **`/c "C:\Scripts\vacuum.bat"`**

注意: このコマンドに指定するパスを編集し、vacuum.bat ファイルの実際のパスを反映するようにしてください。

- **[条件]** タブおよび **[設定]** タブはデフォルト設定のままにします。
- **[OK]** を押して、新しいタスクを保存します。管理者パスワードの入力を求められます。

タスクの想定どおりの動作を確認

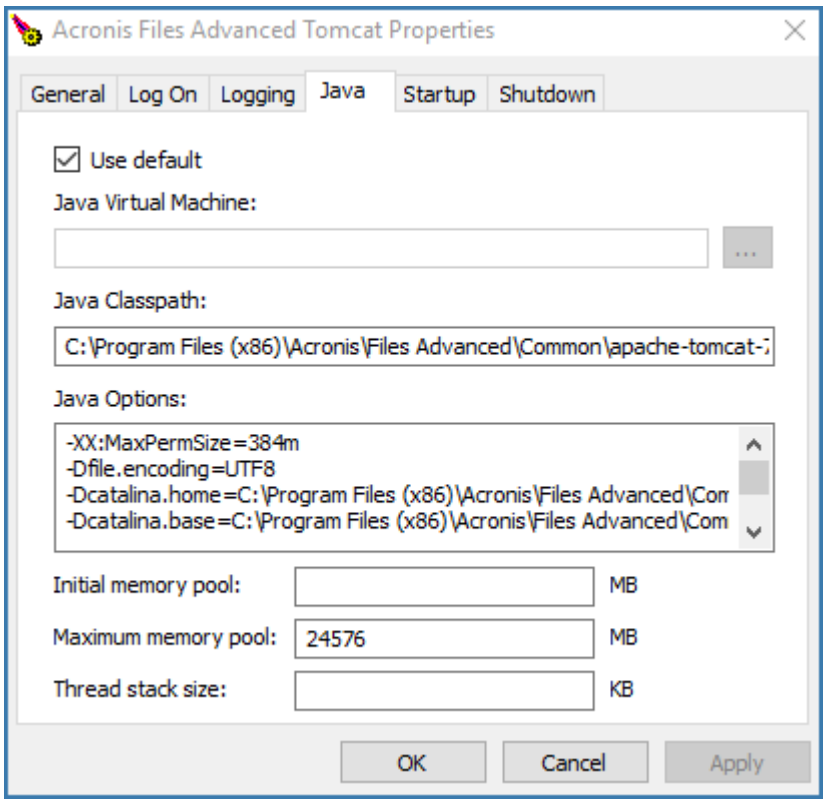
1. [タスク スケジューラ] からバキュームタスクを手動で実行してテストし、適切なフォルダにログファイルが作成されることを確認します。
2. スケジュールされたタスクが設定した時刻に実行されることを確認します。

11.7 Files Advanced Tomcat の Java のメモリ プールの最大サイズの拡張

デフォルトでは、64 ビットのオペレーティングシステムの場合、Files Advanced Tomcat の Java メモリプールの最大サイズは 24 GB です。配置によっては、さらに必要になる場合があります。

メモリ プールの最大サイズを拡張するには、次の操作を実行します。

1. [スタート] メニューをクリックし、**[すべてのプログラム]** → Files Advanced の順に移動します。
2. **Files Advanced Tomcat の設定** ツールのショートカットをクリックします。



3. **[Java]** タブを開きます。
4. **[メモリ プールの最大サイズ]** を必要なサイズに変更して、**[OK]** をクリックします。
5. Files Advanced Tomcat サービスを再起動します。

11.8 別のサーバーへの Files Advanced の移行

このガイドでは、既存の Files Advanced セットアップを新しいコンピュータに移行する方法について説明します。

本番サーバーに移行する前に、テスト環境でこれらの手順を実行することを強くお勧めします。テスト環境は本番サーバーと同じアーキテクチャにするほか、テスト用のユーザーデスクトップとモバイルクライアントをいくつか用意して、本番環境との互換性を確保してください。

セクションの内容

11.8.1 始める前に

注意: 本番環境外でのテストバックアップ/復元の実行を強くおすすめします。

現在の構成でメモする必要がある重要事項:

- Files Advanced Web サーバー、Postgres、ゲートウェイとファイルリポジトリがすべて 1 台のコンピュータ上にありますか？
- Files Advanced Web サーバーの DNS、IP、ポートをメモします。
- ゲートウェイサーバーの DNS、IP、ポートをメモします。
- ファイルリポジトリのアドレスとポートをメモします。
- ファイルストアのロケーションをメモします。
- 現在のサーバーの PostgreSQL バージョン番号をメモします。

PostgreSQL のメインフォルダ（デフォルトで **C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL**)の中のフォルダ名（**9.2**、**9.3**、**9.4** など)が PostgreSQL のメジャー バージョン番号になっているので簡単に確認できます。

これらの情報の大半は設定ユーティリティで確認できます。

移行プロセスの基本概要:

移行を開始する前に、これらの手順のすべてを実行する準備を整えておいてください。

1. 新しいサーバーコンピュータをポイントするように DNS エントリを変更します。
2. 現在のデータベースファイルと証明書をバックアップします。
3. データベースファイルと証明書を新しいコンピュータに移動します。
4. ファイルストアを移行します。
5. Files Advanced Web サーバーを新しいマシンにインストールします。
6. 証明書を新しいコンピュータに移動します。
7. データベースファイルを新しい Files Advanced Web サーバーのインストール環境に配置します。
8. 設定ユーティリティを使用して新しい Files Advanced Web サーバーを起動します。
9. Files Advanced モバイルゲートウェイのアドレスが正しいか確認します。
10. 新しい構成をテストします。

11.8.2 Files Advanced Web サーバーとゲートウェイデータベースの移行

Tomcat/ゲートウェイ/PostgreSQLが現在稼働している元のサーバーで、次の手順を実行します。

注意: Files Advanced Web サーバーのデータベースが非常に大きく、数ギガバイトに達する場合は、別のバックアップおよび復元の方法が必要になることがあります。ヘルプや手順については当社のテクニカルサポート（https://www.acronis.co.jp/mobilitysupport/ https://support.acronis.com/mobility)にお問い合わせください。

1. Files Advanced Tomcat サービスを停止します。
2. Files Advanced PostgreSQL Administrator アプリケーションを開き、データベースサーバーに接続します。**postgres** ユーザーのパスワード入力を求められる場合があります。
3. **[データベース]**を展開し、**acronisaccess_production** データベースを右クリックします。
4. **[メンテナンス]** を選択して、**[バキューム]** ラジオボタンを選択し、**[分析]** チェックボックスをオンにします。**[OK]** を押します。
5. データベース、**[スキーマ]**、**[Public]**の順に展開します。**[テーブル]**セクションの数字をメモします。これにより、復旧後にデータベースが正常に復元されたことを確認できます。
6. PostgreSQL Administrator を閉じ、管理者特権でのコマンドプロンプトを開きます。
7. このコマンドプロンプトで、PostgreSQL の bin ディレクトリに移動します。

   例: `cd "C:\Program Files(x86)\Acronis\Access\Common\PostgreSQL\9.3\bin"`
8. 次のコマンドを入力します: **`pg_dumpall --host localhost --port 5432 --username postgres --file alldbs.sql`**
   - バックアップのファイル名は **`alldbs.sql`** になります。これは PostgreSQL の bin ディレクトリに保存されます。別の場所に保存する必要がある場合は、上記のコマンド内でパスを使用できます。たとえば、コマンドの末尾を次のように変更します: **`--file D:\Backups\alldbs.sql`**
   - デフォルト以外のポートを使用している場合は、**`5432`** を正しいポート番号に変更します。
   - デフォルトの PSQL 管理者アカウント **`postgres`** を使用していない場合は、上記コマンド内の **`postgres`** をご使用の管理者アカウント名に変更してください。
   - この手順では、**`postgres`** ユーザーのパスワードを何回か入力するように求められる場合があります。そのたびにパスワードを入力して Enter キーを押してください。
   - **注意:** パスワードを入力しても、コマンドプロンプトウィンドウの視覚的な変化はまったくありません。
9. バックアップファイルを Access サーバーのホストとなる新しいコンピュータにコピーします。
10. Access サーバーに使用する証明書を新しいコンピュータにコピーします。

11. ファイルストアを移行する予定の場合は、それらのファイルをコピーします。ファイルストアが大きい場合、しばらく時間がかかる場合があります。詳細については、FileStore を別のロケーションに移動する方法 『330ページ 』を参照してください。

ゲートウェイサーバーのデータベースのバックアップ

1. **Acronis Access ゲートウェイ**サービスを停止します。
2. ゲートウェイサーバーの database フォルダに移動します。デフォルトでは次の場所にあります。
   C:\Program Files (x86)\Acronis\Access\Gateway Server\database
3. **mobilEcho.sqlite3** ファイルをゲートウェイサーバーのホストとなる新しいコンピュータにコピーします。

以下のファイルで変更を加えたものがある場合は、Files Advanced 製品を復元または移行した際に設定を転送できるように、バックアップを作成しておくことをお勧めします。

- **postgresql.conf** ファイル。このファイルには、データベース関連の重要な設定が含まれている場合があります。通常、このファイルは **C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL\<version>\Data** にあります。
- **web.xml**。デフォルトの場所は **C:\Program Files (x86)\Acronis\Files Advanced\Access Server\Web Application\WEB-INF**です。シングルサインオンの設定が含まれています。
- **server.xml**。デフォルトの場所は **C:\Program Files (x86)\Acronis\Files Advanced\Common\apache-tomcat-<version>\conf** です。Tomcat の設定が含まれています。
- **krb5.conf**。デフォルトの場所は **C:\Program Files (x86)\Acronis\Files Advanced\Common\apache-tomcat-<version>\conf** です。シングルサインオンの設定が含まれています。
- **login.conf**。デフォルトの場所は **C:\Program Files (x86)\Acronis\Files Advanced\Common\apache-tomcat-<version>\conf** です。
- Files Advanced に使用する証明書とキー。

- **acronisaccess.cfg**。デフォルトの場所は **C:\Program Files (x86)\Acronis\Files Advanced\Access Server** です。
- カスタムカラースキーム。デフォルトの場所は **C:\Program Files (x86)\Acronis\Files Advanced\Access Server\Web Application\customizations**です。
- **pg_hba.conf**。デフォルトの場所は **C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL\<version>\Data** です。
- **newrelic.yml** ファイル。Files Advanced サーバーのチェックに **New Relic** を使用している場合。

Files Advancedサーバーのホストとなる新しいサーバー上で、次の手順を実行します。

Files Advanced のインストール

1. Files Advanced Advanced インストーラを開始して、**[次へ]** を押します。使用許諾契約を読み、承諾します。
2. **[インストール]** を選択し、インストーラ画面の指示に従います。

   注意: Files Advanced Web サーバー、PostgreSQL、ゲートウェイを別々のコンピュータで実行している場合は、**[カスタム]** を選択して、目的のコンポーネントを選択します。
3. [PostgreSQL の構成] 画面で、元のサーバーで使用していたのと同じ PostgreSQL スーパーユーザー用パスワードを入力します。**[次へ]** を押します。
4. インストールされるコンポーネントを確認し、**[インストール]** を押します。
5. インストールが完了したら、**[終了]** を押します。次に設定ユーティリティを実行する旨のダイアログが表示されます。
6. 設定ユーティリティが表示されたら、**[OK]** も **[適用]** も押さずに開いたままにします。

1. **[サービス]** コントロールパネルを開いて、Files Advanced Tomcat サービスを停止します。

   注意: 負荷分散構成では、すべての Files Advanced Tomcat サービスを停止します。

2. Files Advanced PostgreSQL Administrator アプリケーションを開き、ローカルデータベースサーバーに接続し、**[データベース]** を選択して **acronisaccess_production** という名前のデータベースがあることを確認します。
3. データベースを右クリックして、**[更新]** を選択します。
4. データベース、**[スキーマ]**、**[Public]** の順に展開して、**[テーブル]** に項目がないことを確認します。
   - データベースにテーブルがある場合は、データベースを右クリックして、名前を **oldacronisaccess_production** に変更します。最後に、**[データベース]** に移動し、右クリックして **acronisaccess_production** という名前の新しいデータベースを作成します。
5. PostgreSQL Administrator を閉じ、管理者特権でのコマンドプロンプトを開きます。
6. このコマンドプロンプトで、PostgreSQL の bin ディレクトリに移動します。

   例: `cd "C:\Program Files\Acronis\Access\Common\PostgreSQL\9.3\bin"`
7. データベースのバックアップファイル **alldbs.sql**（またはユーザーが付けたファイル名)を **bin** ディレクトリにコピーします。
8. コマンドプロンプトで、次のコマンドを実行します: `psql -U postgres -f alldbs.sql`
9. **postgres** パスワードを求められたら入力します。

   注意: データベースサイズによっては、復元にしばらく時間がかかることがあります。
10. 復元が完了したら、コマンドプロンプトのウィンドウを閉じます。
11. **Files Advanced PostgreSQL Administrator** を再び開き、ローカルデータベースサーバーに接続します。
12. **[データベース]** を選択します。
13. **acronisaccess_production** データベースを開き、**[スキーマ]**、**[Public]** の順に展開します。**テーブル**の数が元のサーバーと同じであることを確認します。

    注意: データベースを復元する Files Advanced Web サーバーのバージョンが、データベースバックアップからの Files Advanced Web サーバーのバージョンより新しく、Files Advanced Tomcat サービスが既に開始されている場合、新しい Files Advanced Web サーバーデータベース内のテーブル数がバックアップ実行時のテーブル数より多くなる場合があります。

ゲートウェイサーバーデータベースの復元

1. 古いサーバーからコピーした **mobliEcho.sqlite3** ゲートウェイサーバーデータベースを新しいゲートウェイサーバーの database フォルダ（デフォルトでは **C:\Program Files (x86)\Acronis\Files Advanced\Gateway Server\database**)にコピーし、既存のファイルと置き換えます。

新しいサーバーの設定

注意: Files Advanced が使用する FQDN は変更せずに、それらがポイントする IP アドレスのみを変更することを強くおすすめします。以下の手順では、Files Advanced の以前のインスタンスで使用していた FQDN を再使用することを前提としています。

1. 開いたままにしておいた Files Advanced 設定ユーティリティに戻り、ゲートウェイサーバー、Files Advanced Web サーバー、ファイルリポジトリを設定します。
2. **[適用]**、**[OK]** とクリックします。次のダイアログで **[OK]** をクリックすると、Files Advanced ウェブインターフェイスを持つブラウザが起動します。
3. Access サーバーにログインします。
4. **[管理画面]** をクリックします。**[モバイルアクセス]** → **[ゲートウェイサーバー]** ページに移動します。
5. ゲートウェイサーバーのリストに、使用しているゲートウェイサーバーが表示されます。
6. ゲートウェイサーバーのアドレスが DNS エントリの場合は、この DNS エントリが新しいサーバーマシンを指しているため、サーバーを変更する必要はありません。ゲートウェイのアドレスが IP アドレスの場合は、ゲートウェイサーバーを編集する必要があります。

Files Advanced の管理設定の確認

データベースの復元が成功したら、他の操作を行う前にウェブインターフェイスにログインし、設定が引き継がれたこと、および設定が依然として適切なことを確認するよう強くおすすめします。確認する重要なアイテムの例を次に示します。

- 監査ログ: 新しい Files Advanced ログフォルダに、ログの書き込みに必要なすべてのアクセス権が設定されていることを確認します。
- New Relic: New Relic を使用している場合は、**`newrelic.yml`** ファイルを古いコンピュータから新しいコンピュータへとコピーし、Files Advanced ウェブインターフェイスがこのファイルをポイントしていることを確認します。
- 管理設定: すべての LDAP、SMTP、全般的な管理設定が正しいことを確認します。
- ゲートウェイサーバーとデータソース: 正しいアドレスでゲートウェイサーバーにアクセスできること、およびデータソースのパスが有効なことを確認します。

11.8.3 新しい構成のテスト

新しいサーバーの設定が完了したら、いくつかの簡単な操作を実行して、すべて順調に機能するか確認します。

- ウェブインターフェイスのナビゲーション操作を実行して、すべて問題なく動作するか確認します。設定が変更されていないか確認します。
- ウェブインターフェイスから [同期・共有] セクションにファイルをアップロードします。また、ネットワークノードを設定した場合には、そのすべてに対して同様の操作を実行します。
- デスクトップクライアントとモバイルクライアントアプリケーションを使用して新しいサーバーに接続します。
- デスクトップクライアントまたはモバイルクライアント（もしくはその両方)からいくつかのファイルをアップロードおよびダウンロードします。

11.8.4 元のサーバーのクリーンアップ

新しいサーバーが正常に稼働していることを確認し、古いサーバーを再度使用する予定がない場合には、古いコンピュータから Files Advanced をアンインストールすることをお勧めします。

Files Advanced のインストーラを開き、使用許諾契約に同意して [アンインストール] をクリックします。すべてのコンポーネントを選択し、[アンインストール] を押します。これで、すべての Files Advanced コンポーネントがコンピュータから削除されます。

注意: Files Advanced のインストーラがない場合は、コントロールパネルを開き、Files Advanced PostgreSQL サーバー、Files Advanced ゲートウェイサーバー、Files Advanced File Repository サーバー、Files Advanced Web サーバー、Files Advanced 設定コレクションツール、Files Advanced 設定ユーティリティ、および LibreOffice をアンインストールしてください。

- PostgreSQL サーバーの**データ**ディレクトリは自動的には削除されません。デフォルトで **C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL** にある PostgreSQL ディレクトリ全体を手動で削除してください。

  注意: 古いインストールまたはカスタム インストールをご使用の場合には、パス（例: **C:\Program Files\Acronis\Access\Common\PostgreSQL**)を編集する必要があります。

- Access サーバー用にインストールされた Java を削除することもできます。Java もコントロールパネルから削除できます。

11.9 PostgreSQL の新しいメジャーバージョンへのアップグレード

PostgreSQL のメジャーリリースでは、PostgreSQL の一部の内部動作を変える新機能が追加されることが多くあります。PSQL のインスタンスをアップグレードする方法は主に 2 つあり、データベース全体のダンプを生成して新しいインスタンスに再度挿入する（**pg_dumpall**)か、新しい **pg_upgrade** コマンドを使用します。どちらの方法も、それぞれ長所と短所があります。

- 通常は、**pg_dumpall** を使用し、データベース全体のダンプを生成して新しいインスタンスに再度挿入する方法が、データの整合性が保たれるため最適ですが、大規模なデータベースでは処理速度が非常に遅くなることがあります。
- **pg_upgrade** による方法は、データベース全体のダンプを生成するよりはずっと高速になりますが、旧バージョンの PSQL では使用できません。

警告: PostgreSQL はサードパーティ製品であるため、Acronis は、これらの方法がすべてのユーザーの環境で正常に機能することを保証しません。本番環境で何らかの実装を行う場合には、必ずお使いのバージョンの PostgreSQL に付属する PostgreSQL のドキュメントを事前に参照してください。

注意: PostgreSQL のドキュメントを参照して、お使いのバージョンの PostgreSQL と、使用予定の新しいバージョンで、**pg_upgrade** が使用できるかどうかを確認してください。

Files Advanced では、各リリースに組み込まれているバージョンより新しいバージョンの Tomcat、Java、および PostgreSQL はサポートされません。特定のバージョンに関する情報が必要な場合は、アクロニスサポートまでご連絡ください。

注意: 本番環境外でのテストアップグレードの実行を強くおすすめします。

現在の構成でメモする必要がある重要事項:

- Files Advanced サーバーと PostgreSQL サーバーが同じコンピュータに存在しますか？
- PostgreSQL がどのポートで実行されていますか？
- 現在インストールされている PostgreSQL のロケールは何ですか？これを確かめるには、PostgreSQL 管理ツールを開いて acronisaccess_production データベースをクリックします。右側の [プロパティ] に、[**エンコーディング**] と [**文字の種類**] が表示されます。

  警告: 新しくインストールした PostgreSQL でも [**エンコーディング**] と [**文字の種類**] が同じになっていることを確認してください。同じでない場合、正常にアップグレードできません。

- PostgreSQL を実行しているコンピュータの IP や FQDN は何ですか？
- 現在のサーバーの PostgreSQL バージョン番号は何ですか？PostgreSQL のメインフォルダ（デフォルトで **`C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL`**)の中のフォルダ名（9.2、9.3、9.4 など)が PostgreSQL のメジャー バージョン番号になっているので簡単に確認できます。
- ファイルシステムについての必要なアクセス許可がすべて設定されていることを確認します。
- 2 つのインスタンス間のアクセスが **`pg_hba.conf`** を介して許可されていることを確認します。このことは、新しい PostgreSQL インスタンスが同じコンピュータにない場合に非常に重要です。

古いインスタンスからのデータベースのダンプ生成

注意: 本番環境外でのテストバックアップ/復元の実行を強くおすすめします。

1. Files Advanced Tomcat サービスを停止します。

2. PostgreSQL の「古い」インスタンスが実行されていることと、「新しい」インスタンスが停止していることを確認します。
3. Files Advanced PostgreSQL Administrator アプリケーションを開き、データベースサーバーに接続します。**postgres** ユーザーのパスワード入力を求められる場合があります。
4. **[データベース]** を展開し、**acronisaccess_production** データベースを右クリックします。
5. **[メンテナンス]** → **[バキューム]** と選択して、**[OK]** を押します。
6. データベース、**[スキーマ]**、**[Public]**の順に展開します。**[テーブル]**セクションの数字をメモします。これにより、データベースの転送の成否を確認できます。
7. PostgreSQL Administrator を閉じ、管理者特権でのコマンドプロンプトを開きます。
8. このコマンドプロンプトで、PostgreSQL の bin ディレクトリに移動します。

   例: **cd "C:\Program Files(x86)\Acronis\Files Advanced\Common\PostgreSQL\9.3\bin"**
9. 次のコマンドを入力します: **pg_dumpall --host localhost --port 5432 --username postgres --file alldbs.sql**
   - バックアップのファイル名は **alldbs.sql** になります。これは PostgreSQL の **bin** ディレクトリに保存されます。別の場所に保存する必要がある場合は、上記のコマンド内でパスを使用できます。たとえば、コマンドの末尾を次のように変更します: **--file D:\Backups\alldbs.sql**
   - デフォルト以外のポートを使用している場合は、**5432** を正しいポート番号に変更します。
   - デフォルトの PSQL 管理者アカウントの postgres を使用していない場合は、上記コマンド内の postgres をご使用の管理者アカウント名に変更してください。
   - この手順では、**postgres** ユーザーのパスワードを何回か入力するように求められる場合があります。そのたびにパスワードを入力して **Enter** キーを押してください。

   注意: パスワードを入力しても、コマンドプロンプトウィンドウの視覚的な変化はまったくありません。
10. ダンプ処理が完了したことを確認したら、「古い」PostgreSQL インスタンスを停止し、「新しい」インスタンスを起動します。

新しいインスタンスへのデータベースの挿入

1. PostgreSQL の「新しい」インスタンスが実行されていることと、「古い」インスタンスが停止していることを確認します。
2. Files Advanced PostgreSQL Administrator アプリケーションを開き、ローカルデータベースサーバーに接続し、**[データベース]** を選択して **acronisaccess_production** という名前のデータベースがあることを確認します。データベースがない場合には、作成する必要があります。
3. データベースを右クリックして、**[更新]** を選択します。
4. データベース、**[スキーマ]**、**[Public]** の順に展開して、**[テーブル]** に項目がないことを確認します。
5. データベースにテーブルがある場合は、データベースを右クリックして、名前を **oldacronisaccess_production** に変更します。最後に、**[データベース]** に移動し、右クリックして **acronisaccess_production** という名前の新しいデータベースを作成します。
6. PostgreSQL Administrator を閉じ、管理者特権でのコマンドプロンプトを開きます。
7. データベースのバックアップファイル **alldbs.sql**（またはユーザーが付けたファイル名）を、新しいインスタンスの bin ディレクトリにコピーします。
8. コマンドプロンプトで、PostgreSQL の **bin** ディレクトリに移動します。

   例: **cd "C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL\9.3\bin"**
9. 次のコマンドを入力します: **psql -U postgres -f alldbs.sql**
10. **postgres** パスワードを求められたら入力します。

    注意: データベースサイズによっては、復元にしばらく時間がかかることがあります。
11. 復元が完了したら、コマンドプロンプトのウィンドウを閉じます。

新しいインスタンスに正しいデータベースが設定されたことを確認します。

1. Files Advanced PostgreSQL Administrator アプリケーションを開き、「新しい」データベースサーバーに接続します。**postgres** ユーザーのパスワード入力を求められる場合があります。

2. **[データベース]** を展開し、**acronisaccess_production** データベースを右クリックします。
3. データベース、**[スキーマ]**、**[Public]**の順に展開します。
4. **[テーブル]** セクションに、前と同じ数のテーブルがあることを確認します。

アップグレード手順

1. Files Advanced Tomcat サービスを停止します。
2. PostgreSQL の両方のインスタンスが実行中であることを確認します。「古い」インスタンスがデフォルトポートで実行中の場合、通常は新しいインスタンスによって別のポートが選択されます。
3. Files Advanced PostgreSQL Administrator アプリケーションを開き、「古い」データベースサーバーに接続します。**postgres** ユーザーのパスワード入力を求められる場合があります。
4. **[データベース]** を開き、データベースを展開して、**[スキーマ]**、**[Public]** の順に展開します。**[テーブル]**セクションの数字をメモします。これにより、データベースの転送の成否を確認できます。
5. PostgreSQL Administrator を閉じます。
6. PostgreSQL の両方のインスタンスが互いにアクセスできることを確認します。それには、**pg_hba.conf** ファイルに **localhost** （127.0.0.1/32)に対応するエントリが存在し、認証方法が **Trust** になっているかどうかを確かめます。

   注意: 「新しい」インスタンスが別のコンピュータにある場合は、そのコンピュータへのアクセスを設定する必要があります。

7. 管理者特権でのコマンドプロンプトを開き、**cd** コマンドで「新しい」PostgreSQL の **bin** ディレクトリに移動します。

   例: **cd C:\Program Files(x86)\Acronis\Files Advanced\Common\PostgreSQL\9.5\bin**
8. **pg_upgrade** コマンドで、次のパラメータを指定します。

   pg_upgrade -b <古い bin フォルダ> -B <新しい bin フォルダ> -d <古いデータフォルダ> -D <新しいデータフォルダ> -U postgres

   注意: **古い bin フォルダ**とは、アップグレードする PostgreSQL インストールでの bin フォルダのことです。データフォルダについても同様です。

注意: **新しい bin フォルダ**とは、新しい PostgreSQL インストールでの bin フォルダのことです。データフォルダについても同様です。

新しいインスタンスに正しいデータベースが設定されたことを確認します。

1. Files Advanced PostgreSQL Administrator アプリケーションを開き、「新しい」データベースサーバーに接続します。**postgres** ユーザーのパスワード入力を求められる場合があります。
2. **[データベース]** を展開し、**acronisaccess_production** データベースを右クリックします。
3. **[メンテナンス]** → **[バキューム]** と選択して、**[OK]** を押します。
4. もう一度 **acronisaccess_production** データベースを右クリックします。
5. **[メンテナンス]** → **[再インデックス]** と選択して、**[OK]** を押します。
6. データベース、**[スキーマ]**、**[Public]**の順に展開します。
7. **[テーブル]** セクションに、前と同じ数のテーブルがあることを確認します。

12 補足資料

セクションの内容

12.1 ソフトウェアの競合

Files Advanced で問題となる可能性があるソフトウェア製品がいくつかあります。現在確認されている競合は次のとおりです。

- **VMware View™ Persona Management**: このアプリケーションは、Files Advanced デスクトップ クライアントの同期プロセスおよびファイルの削除で問題となります。Files Advanced 同期フォルダを **Persona Management ユーザー プロファイル**の外に配置すると、この競合を避けることができます。
- **ウイルス対策ソフトウェア**で同期フォルダをスキャンしないでください。同期プロセスと競合する場合があります。Files Advanced の Filestore フォルダを、ウイルス対策ソフトウェアで無視に設定する、またはホワイトリストに追加することをお勧めします。暗号化をオフにしない限り、Filestore フォルダの項目がすべて暗号化されるため、ウイルス対策ソフトウェアは何も検出できませんが、一部の項目で問題が発生することがあります。

12.2 Files Advanced サーバー上

セクションの内容

12.2.1 Microsoft Azure の統合

Microsoft Azure での Files Advanced の統合

Microsoft Azure には、エンタープライズのお客様用に、ご希望のソフトウェアをクラウドにデプロイする簡単な方法が用意されています。また、各種オペレーティングシステムやソフトウェアが幅広くサポートされており、従来と同様にユーザーを管理することが可能です。Microsoft Azure に Files Advanced を統合すると、専用の物理コンピュータを準備しなくても、Files Advanced の機能をフル活用できるようになります。Microsoft Azure クラウドで、Acronis Access の機能を余すところなく実行できます。

12.2.1.1 始める前に

Files Advanced をインストールする前に、既にセットアップして実行していることを確認する必要がある重要な項目がいくつかあります。

- Files Advanced をホストする Azure Virtual Machine を作成するときには、Windows Server 2012 R2 または Windows Server 2008 R2 をおすすめします。
- Virtual Machine が使用する仮想ネットワーク。Azure Directory Services が機能するためには、仮想ネットワーク **(クラシック)**が必要です。また、仮想マシンは、仮想ネットワーク **(クラシック)**と連動できるように設定する必要があります。

- 「AAD DC Administrators」グループが必要になります。まだこのグループを作成していない場合には、作成する必要があります。このグループに属するユーザーは、コンピュータをドメインにバインドできます。
- Azure では、ディレクトリサービスを実行しておく必要があります。これにより、Files Advanced が実行される仮想コンピュータを Azure Active Directory にバインドできるようになります。

12.2.1.2 Azure Active Directory サービスの管理

「AAD DC 管理者」グループの作成

Azure 管理ポータルを使用して「AAD DC 管理者」というグループを作成し、管理対象ドメインで管理者にする必要のあるユーザーすべてを追加します。追加された管理者は、マシンをドメインに参加させることができ、ドメインのグループポリシーを設定することもできます。

12.2.1.3 Azure 仮想ネットワークの選択および作成

Azure 仮想ネットワークを選択 (または作成)して Azure AD ドメインサービスを有効にする

Azure AD ドメインサービスを有効にする場合、Azure 仮想ネットワークを指定してドメインサービスを使用可能な状態にする必要があります。次の条件を満たす仮想ネットワークを選択してください。

- Azure Active Directory では、仮想ネットワーク **(クラシック)**が機能することが必要となります。
- 仮想ネットワークが、Azure AD ドメインサービスによってサポートされるリージョンに属している。詳細については、リージョンのページを参照してください。
- 仮想ネットワークがリージョンの仮想ネットワークであり、旧式のアフィニティグループの仕組みを使用していないことを確認してください。
- Azure インフラストラクチャサービスに展開するワークロードがこの仮想ネットワークに接続することを確認します。
- 後で使用するため、仮想ネットワークの名前を控えておきます。

12.2.1.4 Azure AD テナント用の Azure AD ドメインサービスの有効化

Azure AD テナント用の Azure AD ドメインサービス有効化の手順は簡単です。

注意: Active Directory インスタンスを **Azure AD Connect** と同期することもできます。詳細については、この件に関する Microsoft Azure のマニュアルを参照してください。

注意: Azure AD を使用する場合、ユーザーのライセンスレベルに **Exchange Online**（Office 365 Business Essentials など)が含まれており、ユーザーが各自のアカウントで有効な電子メールアドレスを持っていることを確認してください。一部の Files Advanced 機能には、AD 内の有効な電子メールアドレスが必要です。

---

1. Azure AD テナントに移動し、ディレクトリの **[設定]** タブをクリックします。
   「Domain Services」というタイトルの新しいセクションがあります。
2. **[このディレクトリ用にドメインサービスを有効にする]** を **[はい]** に切り替えて、その他の設定オプションを表示します。
3. **Azure AD ドメインサービス**を使用して作成するドメインの名前を指定します。組み込みのドメイン名（*.onmicrosoft.com)を使用することも、ディレクトリの [ドメイン] タブで使用できる任意のドメイン名を使用することもできます。または、カスタムのドメイン名をテキストボックスに入力して指定することもできます。
4. **ドメインサービス**で使用可能な状態にする仮想ネットワークをドロップダウンで選択します。
5. 作業を終えたら、ページ下部の **[保存]** をクリックします。
6. この時点で **Azure AD ドメインサービス**が開始され、ドメインがテナント用にプロビジョニングされて、ページに「保留中...」状態が表示されます。この間、ドメインサービスがプロビジョニングされ、選択した仮想ネットワークに接続されます。

   注意: Microsoft Azure **ドメインサービス**の内部処理は、Files Advanced サーバーからは不明です。そのため、Files Advanced を設定してアクティブなユーザーがいる状態になってから**ドメインサービス**を再開することはおすすめしません。

   ---

7. **Azure AD ドメインサービス**がオンラインになるにしたがって、IP アドレスがページに表示され始めます。**Azure AD ドメインサービス**によって高可用性が提供され、サービスがドメイン用に完全にプロビジョニングされると、2 つの IP アドレスが表示されます。1 つ目の IP アドレスが表示されるまでに 20～30 分かかる可能性があり、2 つ目の IP アドレスが使用可能になるまでにさらに 20～30 分かかる可能性があります。

8. この時点で、これらの IP アドレスを、前に Azure AD ドメインサービスを有効にしておいた仮想ネットワークの DNS サーバーとして設定できます。これで、仮想ネットワーク内の仮想コンピュータからドメインを参照して接続できるようになり、ドメインへの参加、LDAP、認証などが有効になります。

注意: Active Directory に関する詳細情報やヘルプについては、Microsoft のテクニカルサポートにお問い合わせください。

12.2.1.5 Azure Marketplace を利用した Files Advanced 仮想マシンの作成

Files Advanced サブスクリプションの使用を開始する最も簡単な方法は、Azure Marketplace からイメージを直接利用することです。イメージには Files Advanced が既にインストールされており、実装環境に合わせて設定するだけで使用できます。

Files Advancedイメージを使用した仮想マシンの作成

仮想マシンを作成します:

1. Azure ポータルを開いてログインします。
2. **[仮想マシン]** タブを開き、**[追加]** を押します。
3. 検索フィールドに「**Files Advanced**」と入力し、**Enter** を押します。
4. 「**Files Advanced Advanced**」を選択します。
5. **[作成]** を押します。**[Resource Manager]** が **[デプロイメントモデル]** になっていることを確認してください。

仮想マシンの設定を行います:

注: これらの設定はすべて Microsoft の管理下にあります。問題が起きた場合や、理解できないオプションがある場合は、Microsoft Azure のマニュアルを参照するか、Microsoft サポートに問い合わせてください。

基本:

1. 仮想マシンの名前を入力します。
2. ディスクの種類（SSD または HDD)を選択します。

3. 仮想マシンのユーザー名とパスワードを入力します。この情報は、リモートデスクトップ経由で仮想マシンに接続するために使用します。
4. **[サブスクリプション]** で、**[従量課金制]** を選択します。
5. 既存の **[リソースグループ]** を使用するか、**[新規作成]** を選択してグループの名前を入力します。
6. システムの所在地に最も近い **[場所]** を選択します。これにより、パフォーマンスと接続性が向上します。
7. **[基本]** の設定が終了したら、[OK] を押します。

サイズ:

推奨されているサイズ設定プランから 1 つを選択します。推奨されているプランの中に実装環境に適したプランがない場合は、**[すべて表示]** を押してからプランの 1 つを選択します。

注: 推奨されているサイズより小さいプランは選択しないでください。詳細については、Files Advanced のハードウェア要件 『29ページ 』を参照してください。

[設定]:

- **ストレージ**
  - 既存のストレージアカウントを選択するか、新しいストレージを作成します。
- **ネットワーク**
  - 既存の仮想ネットワークを選択するか、新しい仮想ネットワークを作成します。
  - 仮想ネットワークのサブネットを選択します。
  - 仮想ネットワークの外側から仮想マシンにアクセスできるようにするには、パブリック IP アドレスを設定します。
  - VM のネットワークセキュリティグループを選択します。
- **拡張機能**
  - Azure 仮想マシンの任意の拡張機能を追加するか、拡張機能についてよくわからない場合は、この設定を **[拡張機能が追加されていません]** のままにします。

- **高可用性**
  - 必要であれば、希望する可用性セットを選択します。
- **監視**
  - 仮想マシンの診断を有効または無効にします。
  - 診断を使用する場合は、診断ストレージアカウントを選択します。

仮想マシンのパラメータとサブスクリプションを確認し、必要な設定になっていれば、購入に進みます。

Files Advanced の設定

1. 仮想マシンの作成が終わったら、仮想マシンにログインします。ブラウザが開いて歓迎され、Files Advanced コンソールが開きます。
2. 管理者アカウントのパスワードを選択します。
3. Files Advanced セットアップウィザードが始まります。

12.2.1.6 Files Advanced の設定

ソフトウェアをインストールし、設定ユーティリティを実行してネットワーク ポートと SSL 証明書を設定した後、管理者は Files Advanced サーバーを設定する必要があります。設定ウィザードは、管理者に一連の手順を案内し、サーバーの基本的な機能が動作するようにします。

注意: 設定ユーティリティを実行した後、サーバーが最初に起動するまで 30～45 秒かかります。

仮想コンピュータに割り当てられた DNS 名/IP アドレスと、設定ユーティリティで指定したポートを使用して、Files Advanced のウェブインターフェイスに移動します。デフォルトの管理者アカウントにパスワードを設定するように求めるメッセージが表示されます。

[初期構成] ページで見ることができるすべての設定は、構成の完了後にも確認することができます。設定の詳細については、「サーバー管理」の資料を参照してください。

初期構成プロセスを進める

ライセンス

- 試用版を開始するには:
  a. **[試用を開始]** を選択し、必要な情報を入力して **[送信]** を押します。
- サーバーにライセンスを付与するには:
  a. **[プロダクト キーを入力します]** を選択します。
  b. プロダクトキーを入力し、チェックボックスにマークを付けます。
  c. **[保存]** を押します。

全般設定

1. **[サーバー名]** を入力します。
2. ユーザーが (http:// または https:// で始まる)ウェブ サイトにアクセスできる FQDN または IP アドレスを指定します。
3. モバイル ユーザーが登録する FQDN または IP アドレスを指定します。
4. **[監査ログ]** のデフォルトの言語を選択します。
5. **[保存]** を押します。

SMTP

注意: この手順をスキップして、後で SMTP を構成することもできます。

1. SMTP サーバーの FQDN または IP アドレスを入力します。
2. サーバーの SMTP ポートを入力します。
3. SMTP サーバーの証明書を使用しない場合は、**[セキュリティで保護された接続を使用しますか？]** のチェックを外します。

4. サーバーから送信される電子メールの「**差出人**」の行に表示されるユーザー名を入力します。
5. サーバーから送信される電子メールのアドレスを入力します。
6. SMTP サーバーでユーザー名やパスワードの認証を使用している場合は、**[SMTP 認証を使用しますか？]** をチェックし、認証情報を入力してください。
7. **[テスト用の電子メールの送信]** を押して、手順 5 で指定したテスト用の電子メールアドレスに電子メールを送信します。
8. **[保存]** を押します。

LDAP

注意: この手順をスキップして、後で LDAP を構成することもできます。

1. **[LDAP を有効にしますか？]** をチェックします。
2. LDAP サーバーの FQDN または IP アドレスを入力します。この入力は、Active Directory サーバー（Azure と同期)または Azure Domain Controller で使用する通常のドメインコントローラとなります。
3. サーバーの LDAP ポートを入力します。
4. LDAP サーバーとの接続に証明書を使用する場合は、**[LDAP のセキュリティで保護された接続を使用しますか?]** をチェックします。
5. LDAP の資格情報をドメインも含めて入力します（例: acronis¥hristo)。
6. LDAP 検索ベースを入力します。
7. LDAP 認証のドメインを入力します。（たとえば、「joe@glilabs.com」という電子メールアカウントの LDAP 認証を有効にするには、「glilabs.com」と入力します)。
8. **[保存]** を押します。

ローカル ゲートウェイ サーバー

注意: 同じコンピュータにゲートウェイ サーバーと Files Advanced サーバーの両方をインストールする場合、ゲートウェイ サーバーが自動的に検出され、Files Advanced サーバーに管理されま

す。クライアントがアクセス可能なローカル ゲートウェイ サーバーの FQDN または IP アドレスを設定するように指示するメッセージが表示されます。このアドレスは後から変更できます。

1. ローカル ゲートウェイ サーバーの FQDN または IP アドレスを設定します。
2. **[保存]** を押します。

ファイル リポジトリ

1. ファイル ストア タイプを選択します。ご使用のコンピュータのファイルストアの場合には **[ファイルシステム]** を、クラウドのファイルストアの場合には Acronis Storage S3、Swift S3、Ceph S3、Amazon S3 を使用します。S3 と互換性のあるその他のストレージサービスも使用できますが、正常な動作は保証されていません。
2. ファイル リポジトリ サービスの FQDN または IP アドレスを入力します。

   注意: ファイルリポジトリのアドレス、ポート、およびファイルストアのロケーションを設定するには、Files Advanced 設定ユーティリティを使用します。ファイルストアのリポジトリエンドポイントの設定は、設定ユーティリティの **[ファイルリポジトリ]** タブの設定と一致する必要があります。設定値を表示または変更するには、AcronisAccessConfiguration.exe を実行します。通常、このファイルはエンドポイントサーバーの **C:\Program Files (x86)\Acronis\Files Advanced\Common\Configuration Utility** にあります。
3. 暗号化レベルを選択します。[なし]、[AES-128]、[AES-256] から選択してください。
4. サーバーがユーザーに警告を送信する最小限の空き領域を選択してください。
5. **[保存]** を押します。

12.2.1.7 Azure で必要なポートを開く

Files Advanced にプライベート仮想ネットワークの外部から到達できるようにするには、いくつかの**エンドポイント**の設定が必要になります。

1. Microsoft Azure にログインして、[仮想コンピュータ] タブを開きます。仮想コンピュータ（クラシック)と仮想コンピュータの両方がある場合には、仮想コンピュータの種類に応じて適切なタブを開いてください。
2. Files Advanced をホストする仮想コンピュータをクリックします。
3. 右側の **[設定]** メニューで、**[エンドポイント]** を選択します。
4. **[追加]** を押し、エンドポイントの名前を入力して、プロトコルに TCP を選択します。

5. Files Advanced サービスで使用するポートを入力します。サービスごとにエンドポイントが 1 つずつ必要になります。（Files Advanced Tomcat および Files Advanced ゲートウェイ)。デフォルトでは、Files Advanced は Tomcat サービスにポート 443、ゲートウェイサービスにポート 3000 を使用します。

12.2.1.8 SharePoint Online と OneDrive for Business の統合

Files Advanced は、SharePoint Online と OneDrive for Business の両方をサポートしています。これらのサービスを統合するには、データソースとして追加する必要があります。

SharePoint Online をデータソースとして追加する

1. Files Advanced ウェブ インターフェイスを開き、管理者としてログインします。
2. **[モバイルアクセス]** タブを開き、**[データソース]** をクリックします。
3. **[新しいフォルダを追加]** を押します。
4. **フォルダ** の名前を入力します。
5. 接続を処理するゲートウェイを選択します。通常は、ローカルにインストールされているゲートウェイを選択します。
6. **[データのロケーション]** として SharePoint サイトを選択し、チームの SharePoint Online サイトへのリンク（**`https://company.sharepoint.com`** など)を入力します。
7. 他のユーザーがサーバーを参照する際に**フォルダ**を表示するには、**同期**の種類を選択します。
8. このフォルダを割り当てるユーザー/グループの名前を入力して選択します。
9. **[保存]** を押します。
10. SharePoint ライブラリの**データソース**を作成する場合は、[URL] と [ドキュメントライブラリ名] の両方のフィールドに入力する必要があります。[URL] フィールドには SharePoint サイトまたはサブサイトのアドレスを入力し、[ドキュメントライブラリ名] フィールドにはライブラリの名前を入力します。

    URL の例: **`https://company.sharepoint.com:43222`**

    ドキュメント ライブラリ名: **`Projects`**

データソースとして OneDrive for Business を追加する

この手順は、全般的に SharePoint サイトの追加手順と同様です。ただし、この製品は従業員の個人使用を想定しているため、全員が使用できる共通のリンクはありません。ワイルドカード（%USERNAME%)を使用する必要があります。たとえば、次のようなリンクを入力する必要があります。

https://YOURDOMAIN-my.sharepoint.com/personal/%USERNAME%_YOURDOMAIN_onmicrosoft_com

これで、データソースが作成され、すべてのユーザーが Files Advanced を通じて各自の OneDrive アイテムを使用できるようになります。

> **注意:** [SharePoint サイト] フィールドには URL 全体を入力してください。[サブパス] フィールドや [ライブラリ] フィールドは使用しないでください。
>
> **注意:** デバイスは Files Advanced で管理する必要があります。そうでないと、ワイルドカードが機能せず、ユーザーが OneDrive アイテムにアクセスできなくなります。

また、ワイルドカードを使用するため、ユーザーは自分のファイルへのアクセス権を他のユーザーに付与できないことに注意してください。管理者は、各ユーザーのデータソースをユーザー単位で作成でき、共有を望むユーザーを管理できます。

12.2.2 Files Advanced の負荷分散

Files Advanced を負荷分散する方法は 2 つあります。

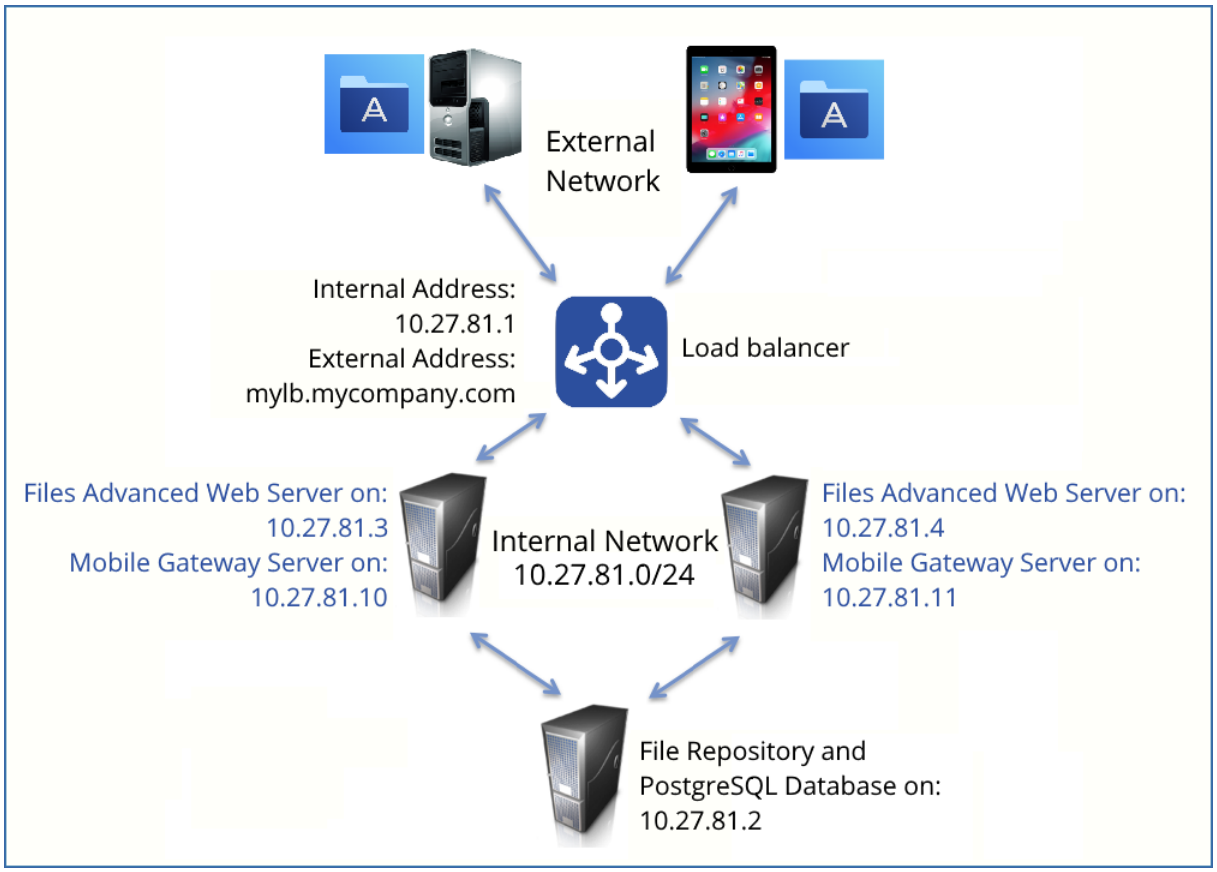
Files Advanced モバイル ゲートウェイのみ負荷分散する

この設定によって、負荷が最も高くなる Files Advanced モバイル ゲートウェイ サーバーのコンポーネントが負荷分散され、モバイル クライアントは常時アクセス可能な状態になります。管理対象外のアクセスに対して Files Advanced モバイル ゲートウェイに接続する必要がない場合は、Files Advanced サーバーは負荷分散装置の背後に配置されません。詳細については、「クラスタ グループ 『131ページ 』」の記事を参照してください。

Files Advanced のすべてを負荷分散する

この設定によって、Files Advanced コンポーネントのすべてが負荷分散され、すべてのユーザーに対して高可用性が確保されます。この設定をテストするには、2 つ以上のコンピュータが必要になります。負荷分散の設定時の設定項目の多くは、ソフトウェアやハードウェアにより異なるため、このガイドでは説明しません。

この設定例では、3 つのコンピュータを使用します。1 つはファイルリポジトリおよびデータベースとして機能し、他の 2 つは Files Advanced Web サーバーおよび Files Advanced モバイル ゲートウェイとして機能します。この設定の構成方法について以下に示します。



このガイドでは、ご使用の環境で Files Advanced 製品を適切に負荷分散するために必要な詳細情報について説明します。

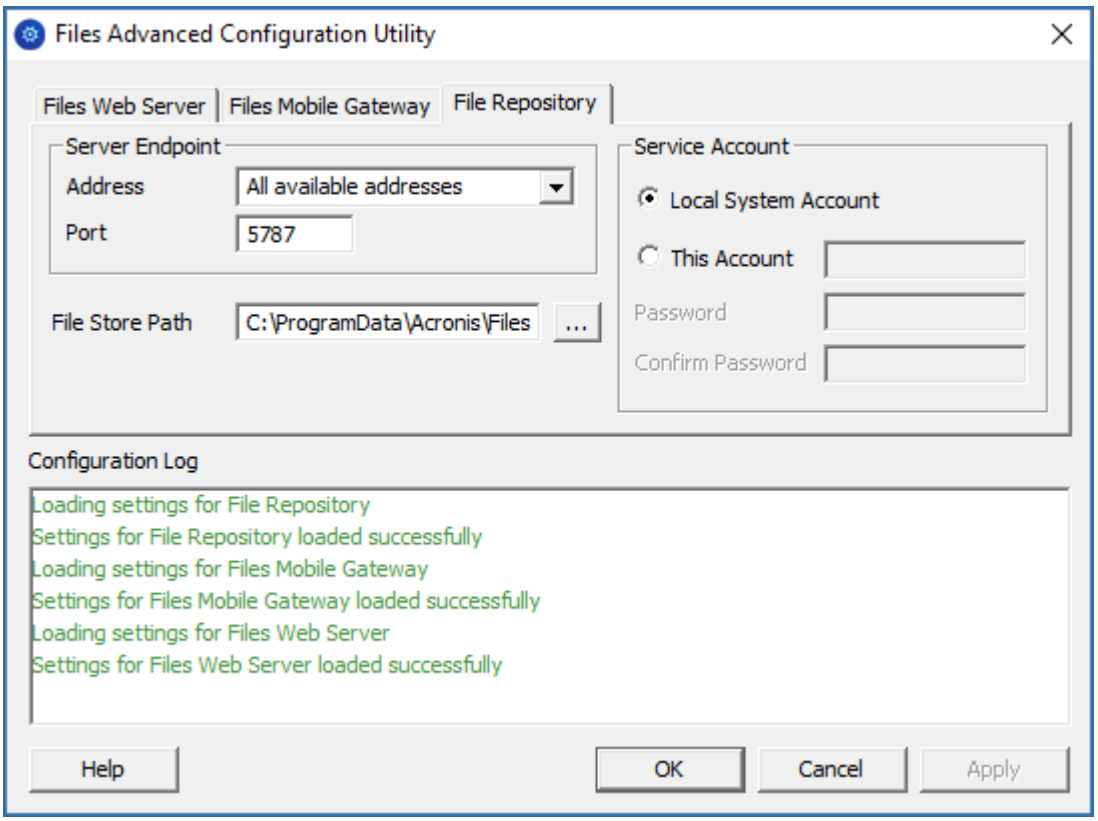
PostgreSQL データベースおよびファイル リポジトリをホストするサーバーの場合、次の手順を実行します。

1. Files Advanced のインストーラを起動して、**[次へ]** を押します。使用許諾契約を読み、承諾します。

2. Files Advanced インストーラで **[カスタム]** を選択し、**[Files Advanced ファイル リポジトリ]** と **[PostgreSQL Database Server]** を選択して **[次へ]** を押します。
3. ファイル リポジトリと設定ユーティリティをインストールする場所を選択します。
4. PostgreSQL をインストールする場所を選択し、スーパーユーザー（**postgres**)のパスワードを入力します。
5. TCP ポート 5432 を開きます。このポートは、リモート コンピュータから PostgreSQL データベースにアクセスする際に使用されます。
6. インストール手順が完了したら、設定ユーティリティ 『36ページ 』で設定を続行します。
   a. 設定ユーティリティを開くように求められたら、**[OK]** を押します。
   b. アクセスできるようにするファイル リポジトリのアドレスとポートを選択します。

   注意: Files Advanced ウェブ インターフェイスで同じアドレスとポートを設定する必要があります。詳細については、「設定ユーティリティの使用 『*36*ページ 』」および「ファイル リポジトリ 『*154*ページ 』」の記事を参照してください。

   c. ファイル ストアへのパスを選択します。このパスに実際のファイルが保存されます。



d. **[OK]** をクリックして変更を適用し、**設定ユーティリティ**を閉じます。

7. PostgreSQL インストール ディレクトリ（例: **C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL\<VERSION>\data**)に移動し、テキスト エディタで **pg_hba.conf** を編集します。
8. 内部アドレスを使用してそれぞれの Files Advanced サーバーにホストエントリを追加し、ファイルを保存します。**pg_hba.conf** ファイル（HBA はホストベース認証の略)ではクライアント認証が制御されます。データベースクラスタのデータディレクトリにファイルが保存されます。このファイルで、接続を許可するサーバーと権限を指定します。たとえば、次のように指定します。

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

9. PostgreSQL インスタンスへのリモートアクセスを可能にするには、**postgresql.conf** ファイルを編集する必要があります。以下の手順を実行してください。
   a. 移動して、**postgresql.conf** を開きます。デフォルトの場所: **C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL\<VERSION>\Data\postgresql.conf**
   b. 行「**#listen_addresses = 'localhost'**」を検索します。
   c. 行の先頭にある「**#**」記号を削除してコマンドを有効にします。
   d. 利用可能なアドレスすべてをリッスンするために、「**localhost**」を「*****」に置き換えます。PostgreSQL で特定のアドレスのみをリッスンするには、「*****」のかわりに IP アドレスを入力します。
      - **例 listen_addresses = '*'** : PostgreSQL が利用可能なアドレスすべてをリッスンします。
      - **例: listen_addresses = '192.168.1.1'** : PostgreSQL がこのアドレスのみをリッスンします。
   e. **postgresql.conf** に加えた変更を保存します。
   f. Files Advanced PostgreSQL サービスを再起動します。

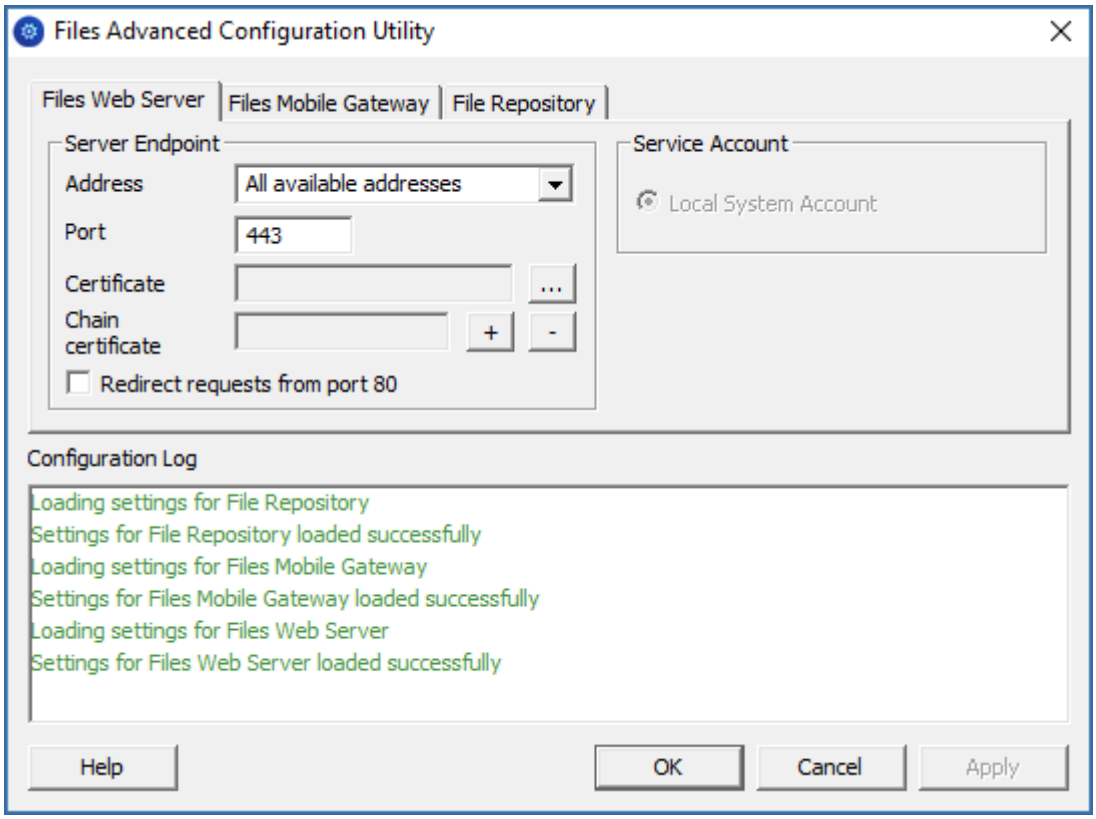
10. **Files Advanced PostgreSQL 管理者ツール**（PgAdmin とも呼ばれます)を開きます。これは Windows の [スタート] メニューの [Files Advanced] フォルダにあります。ローカル サーバーに接続して、**[データベース]**を選択します。右クリックするか、**[編集]** → **[新規オブジェクト]** のメニューから **[新規データベース]** を選択して新しいデータベースを作成します。「**acronisaccess_production**」という名前を付けます。

注: PostgreSQL は、デフォルトでポート 5432 を使用します。使用するすべてのファイアウォールまたはルーティングソフトウェアでこのポートが開放されていることを確認してください。

Files Advanced サーバーおよび Files Advanced ゲートウェイとして機能する2つのサーバーの両方で、次の手順を実行します。

1. Files Advanced のインストーラを起動して、**[次へ]** を押します。使用許諾契約を読み、承諾します。
2. Files Advanced インストーラで、**[カスタム]** を選択し、**[Files Advanced Web サーバー]** と **[Files Advanced モバイル ゲートウェイ]** のみを選択して、インストール手順を続行します。
3. インストール手順が完了したら、設定ユーティリティ 『36ページ 』で設定を続行します。
   a. 設定ユーティリティを開くように求められたら、**[OK]** を押します。
   b. **Files Advanced Web サーバータブ上:**
      - アクセスできるようにする Files Advanced 管理サーバーのアドレスとポートを入力します（例: 10.27.81.3 および 10.27.81.4)。
      - 証明書を選択します。負荷分散装置の DNS アドレスに関連付けられている SSL 証明書と同じものを選択する必要があります。
      - **[適用]** を押します。

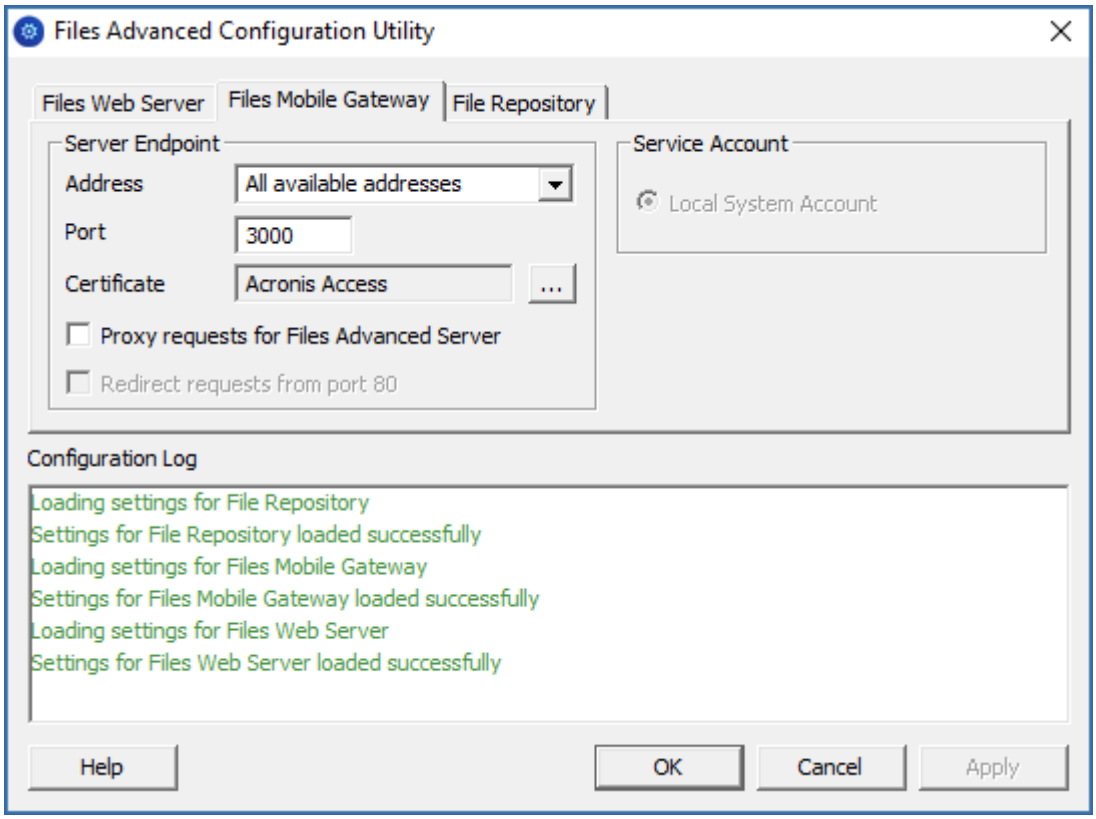
注意: 証明書がない場合は、Files Advanced によって自己署名証明書が作成されます。この証明書は実働環境では使用しないでください。



c. **Files Advanced モバイル ゲートウェイ タブ上:**

- アクセスできるようにするゲートウェイ サーバーのアドレスとポートを入力します（例: 10.27.81.10 および 10.27.81.11)。
- 証明書を選択します。負荷分散装置の DNS アドレスに関連付けられている SSL 証明書と同じものを選択する必要があります。
- **[適用]** を押します。

注意: 証明書がない場合は、Files Advanced によって自己署名証明書が作成されます。この証明書は実働環境では使用しないでください。



4. Files Advanced インストール ディレクトリ（例: C:¥Program Files (x86)¥Acronis¥Files Advanced¥Acess Server¥)に移動し、テキスト エディタで **acronisaccess.cfg** を編集します。
5. ユーザー名、パスワード、PostgreSQL データベースを実行するサーバーの内部アドレスを設定し、ファイルを保存します。これにより、Files Advanced サーバーがリモートの PostgreSQL データベースに接続するよう設定されます。たとえば、次のように設定します。

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

6. Services.msc を開き、Files Advanced サービスを再起動します。

Files Advanced Web サーバーまたは Files Advanced モバイル ゲートウェイで、次の手順を実行します。

これは最初に設定するサーバーです。このサーバーの設定は、他のすべてのサーバーにわたって複製されます。設定が複製されると、すべてのサーバーは同じ設定になります。どのサーバーを選択したかは問われません。

1. Services.msc を開き、**Files Advanced Tomcat** サービスを再起動します。作成したデータベースが使用されます。
2. ウェブブラウザで https://myaccess（例: https://10.27.81.3、https://10.27.81.4 など)にアクセスして、設定ウィザード 『41ページ 』を完了します。
   a. **[ライセンス] タブでの作業:**
      - プロダクト キーを入力し、チェックボックスにマークを付け、**[続行]** を押します。
   b. **[全般設定] タブでの作業:**
      - [サーバー名] にサーバー名を入力します。
      - [ウェブ アドレス] には負荷分散装置の外部アドレスを指定してください（例: mylb.company.com)。ポート 443 を使用していない場合は、ポートも入力する必要があります。
      - [クライアント登録アドレス] には負荷分散装置の外部アドレスを指定してください（例: mylb.company.com)。
      - カラー スキームを選択します。
      - 監査ログ メッセージの言語を選択します。
   c. **[SMTP] タブでの作業:**
      - SMTP サーバーの FQDN または IP アドレスを入力します。
      - SMTP サーバーのポートを入力します。
      - SMTP サーバーの証明書を使用しない場合は、**[セキュリティで保護された接続を使用しますか？]** のチェックを外します。
      - サーバーから送信される電子メールの「差出人」行に表示されるユーザー名を入力します。

- サーバーから送信される電子メールのアドレスを入力します。
- SMTP サーバーでユーザー名やパスワードの認証を使用している場合は、[SMTP 認証を使用しますか？] をチェックし、認証情報を入力します。
- **[保存]** を押します。

d. **[LDAP] タブでの作業:**

[LDAP を有効にしますか？] をチェックします。

- LDAP サーバーの FQDN または IP アドレスを入力します。
- サーバーの LDAP ポートを入力します。
- LDAP サーバーとの接続に証明書を使用する場合は、**[LDAP のセキュリティで保護された接続を使用しますか?]** をチェックします。
- LDAP の資格情報をドメインも含めて入力します（例: mycompany¥myname)。
- LDAP 検索ベースを入力します。
- LDAP 認証のドメインを入力します。（たとえば、「joe@glilabs.com」という電子メールアカウントの LDAP 認証を有効にするには、「glilabs.com」と入力します)。
- **[保存]** を押します。

e. **[ローカル ゲートウェイ サーバー] タブでの作業:**

注意: 同じコンピュータに Files Advanced モバイル ゲートウェイと Files Advanced Web サーバーの両方をインストールする場合、ゲートウェイが自動的に検出され、Files Advanced Web サーバーに管理されます。

- ローカル ゲートウェイ サーバーの FQDN または IP アドレスを設定します。これは、負荷分散装置の背後の内部アドレスです（例: 10.27.81.10)。
- **[保存]** を押します。

a. **[ファイル リポジトリ] タブでの作業:**

- ファイル リポジトリのアドレスには、ファイル リポジトリの役割として作成したサーバーの内部アドレスを指定する必要があります（例: 10.27.81.2)。

1. 設定ウィザードの設定が完了したら、**[完了]** を押し、**[モバイルアクセス]** → **[ゲートウェイサーバー]** に移動します。

2. 次に 2 つ目のゲートウェイ サーバーを登録します。
   a. 2 つ目のゲートウェイの表示名を入力します。
   b. **[管理のアドレス]** には、負荷分散装置の背後の内部アドレスを指定する必要があります（例: 10.27.81.11)。
   c. **[管理キー]** を入力します。管理キーを取得するには、追加するゲートウェイがインストールされているコンピュータで https://mygateway:443（例: https://10.27.81.10、https://10.27.81.11 など)にアクセスして、キーを表示します。詳細については、「新しいゲートウェイ サーバーの登録 『117ページ 』」の記事を参照してください。
   d. **[保存]** を押します。
3. クラスタ グループを作成し、すべてのゲートウェイ サーバーを追加します。プライマリ サーバーは、設定ウィザードが完了しているサーバーにする必要があります。詳細については、「クラスタ グループ 『131ページ 』」の記事を参照してください。

   注意: 続行する前に、各ゲートウェイ上で正しい管理のアドレスが構成済みであることを確認してください。これは、ゲートウェイ サーバーの DNS アドレスまたは IP アドレスです。

   a. **[モバイル アクセス]** タブを展開します。
   b. **[ゲートウェイ サーバー]** ページを開きます。
   c. **[クラスタ グループの追加]** ボタンを押します。
   d. グループの表示名を入力します。
   e. 負荷分散装置の内部の FQDN または IP アドレスを入力します (例: 10.27.81.1)。
   f. グループに含めるそれぞれのゲートウェイのチェックボックスにマークを付けます。
   g. グループの設定を制御するゲートウェイを選択します。最初に設定したゲートウェイを選択してください。そのゲートウェイ上の既存の設定のすべて（割り当てられているデータ ソースは含まれますが、管理のアドレスは含まれません)が、グループ内の各ゲートウェイにコピーされます。

負荷分散装置での作業:

1. 負荷分散装置で時間ベースのセッション スティッキネス（またはご使用の負荷分散装置での同等の設定)を有効にし、期限切れにならないように設定します。
2. ヘルスチェック（HTTP ステータス 200 が返されることを確認する)が必要な場合は、https://INTERNALSERVERNAME:MANAGEMENTPORT/signin に ping を送信することで可能になります（例: https://myaccessserver1.company.com/signin および https://myaccessserver2.company.com/signin)。

ブラウザで https://mylb.company.com を開き、設定が機能していることを確認します。

12.2.3 負荷分散型セットアップでの Files Advanced のインストール

このガイドは、負荷分散型セットアップの要件および負荷分散環境への Files Advanced 導入に伴うプロセスに関する一般的な概要として提供されています。実際のセットアップはここに記載する例と異なる場合がありますが、コンポーネントが相互作用する方法は同じです。

推奨される構成は、Files Advanced サーバーを個々のパーツに分けて、各パーツを負荷分散装置の背後にある個別のマシンに配置するという構成です。ファイルリポジトリとファイルストアは同じマシン上に配置できます。

これらの手順は、テスト環境で実行することを強くおすすめします。テスト環境は予定されている本番のセットアップと同じアーキテクチャにするほか、テスト用のユーザーデスクトップとモバイルクライアントをいくつか用意して、使用する環境との互換性を確保してください。

セクションの内容

12.2.3.1 システム要件

ハードウェア要件

本番環境では、少なくとも 3 台の Files Advanced Tomcat サーバーと 3 台のゲートウェイサーバーを使用することをおすすめします。このようにすると、いずれかのサーバーで障害が発生したとしても、他の 2 台のアクティブサーバーで負荷を分散できます。

注意: このセットアップ案では、これらのサーバーが仮想マシンサーバー上でホストされることが前提となります。複数のサーバーを使用する場合、ゲスト仮想マシン間では低レイテンシの相互接続をおすすめします。

- Files Advanced ウェブサーバー用の 1 台の負荷分散装置。
- Files Advanced ゲートウェイサーバー用の 1 台の負荷分散装置。
- Files Advanced Tomcat サーバー用に 3 台（それぞれ 32 GB の RAM と 16 コアの CPU を搭載したもの)。
- Files Advanced ゲートウェイサーバー用に 3 台（それぞれ 8 GB の RAM と 4 コアの CPU を搭載したもの)。

  注意: ゲートウェイサーバーでは、CPU やメモリよりもディスクおよびネットワーク速度のほうが重要になります。

- PostgreSQL サーバー用に 1 台（32GB の RAM と 16 コアの CPU を搭載したもの)。
- ファイルリポジトリサービスおよびファイルストア用に 1 台。このサーバーのパラメータはそれほど重要ではありません。

ネットワーク接続

- Files Advanced Tomcat サーバー用の負荷分散装置が現在の Files Advanced の DNS アドレスを使用するように構成する必要があります。
- ゲートウェイサーバー用の負荷分散装置が現在のゲートウェイサーバーの DNS アドレスを使用するように構成する必要があります。
- Tomcat サーバーをゲートウェイ負荷分散装置に接続して、デスクトップネットワークノードを同期し、ウェブインターフェイス上のネットワークノードを参照できるようにします。このクラスタセットアップでは、Files Advanced ウェブ UI の [管理] ページと [ゲートウェイサーバー] ページの [クライアント接続のアドレス] は、外部負荷分散

装置のアドレスになります。ゲートウェイサーバーのウェブでも、[Files Advanced サーバー接続に代替アドレスを使用] 設定を使用し、[Files Advanced ウェブサーバー接続用アドレス] にゲートウェイ負荷分散装置の内部アドレスを設定しています。

- モバイルクライアント接続に対応するために、ゲートウェイサーバーを Tomcat 負荷分散装置に接続します。

注意: 同期・共有データソースについて、アドレスを Tomcat 負荷分散装置のアドレスに変更する必要があります。

PostgreSQL サーバーコンポーネントのインストール

1. Files Advanced のインストーラを起動して、**[次へ]** を押します。使用許諾契約を読み、承諾します。
2. **[カスタム]** をクリックし、PostgreSQL Database Server だけを選択します。**[次へ]** を押します。
3. PostgreSQL をインストールする場所を選択し、スーパーユーザー (**postgres**)のパスワードを入力して、[次へ] を押します。
4. **[ファイアウォールでポート 5432 を開く]** を選択します。このポートを、PostgreSQL データベースにリモートからアクセスするために使用します。
5. インストールを終了します。

Tomcat サーバーの接続許可

1. インストールが完了したら、PostgreSQL の **data** フォルダ（デフォルトでは、**C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL\<version>\Data**)に移動し、 **pg_hba.conf** をテキストエディタで開きます。
2. Files Advanced Tomcat サーバーそれぞれのホストエントリを、内部アドレスを使用して組み込み、ファイルを保存します。

   pg_hba.conf（HBA はホストベース認証を表します)ファイルは、クライアント認証を制御するもので、データベースクラスタのデータディレクトリに保存されます。このファイル内に、接続を許可するサーバーと権限を指定します。たとえば、次のように指定します。

```
# TYPE DATABASE USER ADDRESS METHOD
# Loadbalancer1 (First Files Advanced & Gateway server)
host acronisaccess_production postgres 10.144.70.247/32 md5
```

注意: この例では、**postgres** という名前のユーザーアカウントが **md5 encrypted** 接続を使用して、10.144.70.247 にあるサーバーから接続し、完全な権限（**レプリケーション**権限を除く）で **acronisaccess_production** データベースにアクセスできます。

適切な接続数のセットアップ

1. **max_connections** を見つけて **510** に変更します。
2. 行 **#listen_addresses = 'localhost'.** から先頭の **#** を削除し、**localhost** を ***** で置き換えます。変更後は、以下のようになるはずです。**listen_addresses = '*'**
3. 行 **#effective_cache_size = 128MB** から先頭の **#** を削除し、**128MB** を **12GB** で置き換えます。変更後は、以下のようになるはずです。 **effective_cache_size = 12GB**
4. 以下の注釈を追加します。**#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. すべての変更を保存して、**postgresql.conf** ファイルを閉じます。
6. Files Advanced PostgreSQL サーバーサービスを再起動します。

Files Advanced ウェブサーバーのみのインストール

1. Files Advanced インストーラを起動し、使用許諾契約に同意します。
2. **[カスタム]** を選択し、Files Advanced Tomcat サーバーのみを選択します。

注: Tomcat サーバーをクリックすると自動的に PostgreSQL サーバーも選択されますが、クリックして選択を解除できます。

3. インストールを完了し、Files Advanced Tomcat サービスが停止していることを確認します。

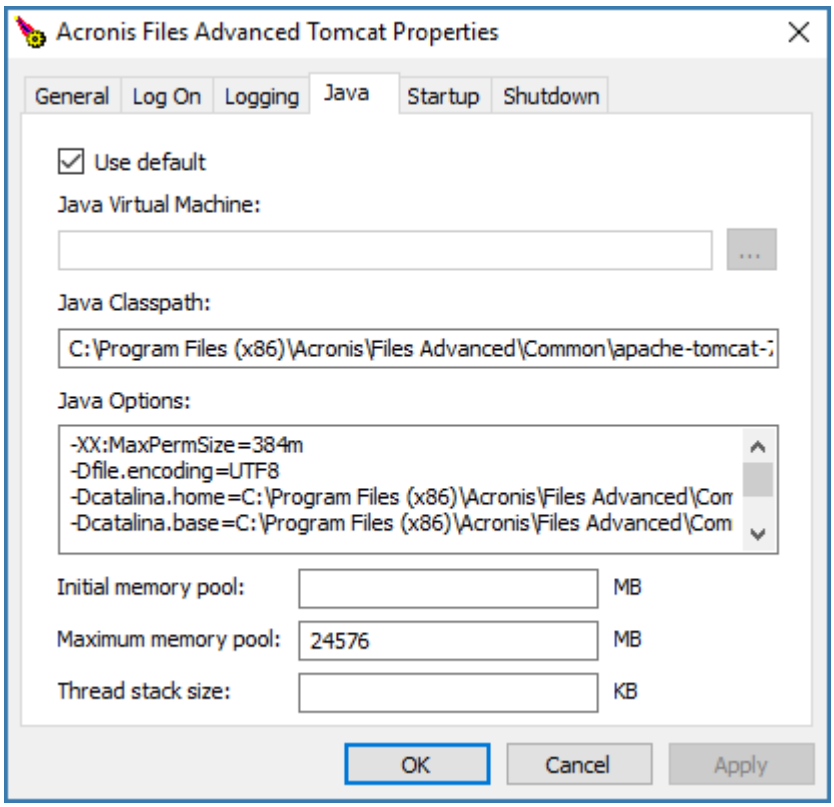
サーバーの設定

Files Advanced ウェブサーバーで変更したすべての設定は、その他すべての Files Advanced ウェブサーバーでも同じ変更を行う必要があります。

注意: `pg_hba.conf` ファイルに各 Files Advanced ウェブサーバーのエントリを追加することを忘れないでください。

Tomcat の最大メモリ使用量の構成

1. デスクトップから、**Files Advanced Tomcat サービス設定**ツールを起動します。このツールがデスクトップにない場合は、**[スタート]** -> **[すべてのプログラム]**- > **Files Advanced** に移動し、該当するショートカットをクリックします。
2. **[Java]** タブをクリックします。
3. **[メモリプールの最大サイズ]** 設定を **24576** に変更して、**[OK]** をクリックします。



適切なデータベースに接続するようサーバーを構成する

1. Files Advanced ウェブサーバーフォルダ（デフォルトでは **`C:\Program Files(x86)\Acronis\Files Advanced\Access Server`**)に移動し、**`acronisaccess.cfg`** ファイルを開きます。このファイルは、サーバーに PostgreSQL データベースサービスの場所を指示します。
2. 以下の値を設定します。

```
DB_HOSTNAME =10.144.70.248
DB_PORT =5432
```

DB_POOLSIZE =250

注意: DB_HOSTNAME は、PostgreSQL が現在実行されている IP アドレスです。この例では、10.144.70.248 となっています。

注意: DB_POOLSIZE は、250 以上の値に設定することをおすすめします。

3. ファイルを保存します。

最大スレッド数の構成

Tomcat の負荷分散型セットアップでは、すべての Tomcat インスタンスによって生成される可能性のあるスレッドの合計数が、PostgreSQL データベースで受け入れるように構成された最大接続数を超えないようにすることが重要です。

スレッドの合計数を決定する重要な 3 つの設定は、以下のとおりです。

- **acronisaccess.cfg** ファイル内の **DB_POOLSIZE = 200**。250 以上の値に設定することをおすすめします。
- Tomcat の **server.xml** ファイル内の **maxThreads = 150.**。この設定は、デフォルトの 150 のままにすることをおすすめします。
- **postgresql.conf** ファイル内の **max_connections**。この設定は、前の手順で構成済みになっているはずです。この設定の値は、すべての Files Advanced ウェブサーバーに設定されている Tomcat の DB_POOLSIZE 値の合計に 10 を足した値以上でなければなりません。たとえば、Tomcat サーバーが 2 台の場合は 510、3 台の場合は 760 となります。

注意: これらのファイルに変更を加えた場合、対応するサービスを再起動する必要があります。

適切なロギングの構成

負荷分散構成では、Files Advanced Tomcat サービスによる IP アドレスのマッピングがログ内で適切に行われません。各接続が適切にログに記録されるよう、以下の変更を行う必要があります。

1. server.xml ファイル内で、次の行を見つけます。**<Valve**

   className=”org.apache.catalina.valves.AccessLogValve” directory=”logs” prefix=”localhost_access_log.” suffix=”.txt” pattern=”%h %l %u %t "%r" %s %b”/>.

2. 行の末尾に **requestAttributesEnabled=”true”** を追加します。
3. 同じ行の下に、以下を追加します。

   ```
   <Valve className="org.apache.catalina.valves.RemoteIpValve"
   remoteIpHeader="X-Forwarded-For" protocolHeader="X-Forwarded-Proto"/>
   ```
4. ファイルを保存し、Files Advanced Tomcat サービスを再起動します。

新しいゲートウェイサーバーのインストール

1. 新しいコンピュータ上で、Files Advanced インストーラを起動し、使用許諾契約に同意します。
2. **[カスタム]** を選択し、ゲートウェイサーバーコンポーネントのみをインストールします。インストールを終了します。
3. 設定ユーティリティで、ゲートウェイのアドレス、ポート、証明書を設定します。設定する証明書は、ゲートウェイ負荷分散装置の DNS アドレスに関連付けられている SSL 証明書と同じものでなければなりません。

12.2.3.2 ファイルストアとファイルリポジトリの設定

S3 ストレージを使用する予定の場合、選択する S3 ストレージ内でファイルストアがホストされることになるため、ファイルリポジトリサービスをインストールする必要はありません。

ファイルリポジトリサービスのインストール

1. Files Advanced インストーラを、ファイルリポジトリとファイルストアを配置するコンピュータにコピーします。
2. インストーラを起動し、使用許諾契約に同意してから、[カスタム] を選択します。
3. [ファイルリポジトリ] オプションのみを選択して、[次へ] を押します。
4. 目的のインストールパスを選択してから [次へ] を押します。
5. インストールが完了するまで、画面の指示に従います。
6. 設定ユーティリティが起動します。ファイルリポジトリサービスにアクセスするためのアドレスとポートを選択します。

7. ファイルストアのインストール先を選択します。デフォルトのロケーションは、**C:\ProgramData\Acronis\Files Advanced\FileStore** です。

   注意: ファイルストアがリモートネットワーク共有にある場合は、ファイルリポジトリサービスが実行されているコンピュータまたはユーザーアカウントに、ネットワーク共有のファイルストアフォルダに対する完全なアクセス権が必要です。

   このアカウントには、ログファイルを書き込むため、ローカルリポジトリフォルダ（たとえば、C:¥Program Files (x86)¥Acronis¥Files Advanced¥File Repository¥Repository)への読み取り/書き込みアクセス権限も必要です。

8. Files Advanced File Repository サービスを起動します。

Files Advancedの設定

1. Files Advanced ウェブインターフェイスを開き、管理者としてログインします。
2. [共有・同期] -> [ファイルリポジトリ] に移動し、[ファイルストアリポジトリエンドポイント] に設定ユーティリティで選択したアドレスと同じアドレスが設定されていることを確認します。

12.2.3.3 負荷分散装置固有の設定

1. ブラウザで https://mylb.company.com を開き、設定が機能していることを確認します。
2. 負荷分散装置で時間ベースのセッションスティッキネス（またはご使用の負荷分散装置での同等の設定)を有効にし、期限切れにならないように設定します。
3. ヘルスチェック（HTTP ステータス 200 が返されることを確認する)が必要な場合は、https://INTERNALSERVERNAME:MANAGEMENTPORT/api/v1/server_version に ping します（例: https://myaccessserver.company.com/signin および https://myaccessserver.company.com/api/v1/server_version)。
4. 負荷分散型セットアップで IP アドレスと接続が適切にログに記録されるようにするには、負荷分散装置を構成して以下のヘッダーを設定する必要があります。
   - **X-Forwarded-For** これにより、各接続で負荷分散装置の IP アドレスが表示される代わりに、接続しているクライアントの実際の IP アドレスが表示されるようになります。

- **X-Forwarded-Proto** これにより、実際に使用されているプロトコルが表示されます。

12.2.4 負荷分散構成への移行

このガイドは、負荷分散型セットアップおよび負荷分散環境への移行に伴うプロセスに関する一般的な概要として提供されています。実際のセットアップはここに記載する例と異なる場合がありますが、コンポーネントが相互作用する方法およびコンポーネントの設定は同じです。

推奨される構成は、Files Advanced サーバーを個々のパーツに分けて、各パーツを負荷分散装置の背後にある個別のマシンに配置するという構成です。ファイルリポジトリとファイルストアは同じマシン上に配置できます。

本番サーバーに移行する前に、テスト環境でこれらの手順を実行することを強くお勧めします。テスト環境は本番サーバーと同じアーキテクチャにするほか、テスト用のユーザーデスクトップとモバイルクライアントをいくつか用意して、使用する環境との互換性を確保してください。

このガイドでは例として、すべてのコンポーネントがマシン上にインストールされた、標準的な導入環境で動作する Files Advanced のセットアップを使用します。

注意: この例では、元の Files Advanced Tomcat サービスを引き続き実行し、このサービスを新しい構成に接続します。このステップは必須ではありません。

導入環境に変更を加える前に、「バックアップと復旧 『*200*ページ 』」の記事を参照してください。

セクションの内容

12.2.4.1 システム要件

ハードウェア要件

本番環境では、少なくとも 3 台の Files Advanced Tomcat サーバーと 3 台のゲートウェイサーバーを使用することをおすすめします。このようにすると、いずれかのサーバーで障害が発生したとしても、他の 2 台のアクティブサーバーで負荷を分散できます。

注意: このセットアップ案では、これらのサーバーが仮想マシンサーバー上でホストされることが前提となります。複数のサーバーを使用する場合、ゲスト仮想マシン間では低レイテンシの相互接続をおすすめします。

- Files Advanced ウェブサーバー用の 1 台の負荷分散装置。
- Files Advanced ゲートウェイサーバー用の 1 台の負荷分散装置。
- Files Advanced Tomcat サーバー用に 3 台（それぞれ 32 GB の RAM と 16 コアの CPU を搭載したもの)。
- Files Advanced ゲートウェイサーバー用に 3 台（それぞれ 8 GB の RAM と 4 コアの CPU を搭載したもの)。

  注意: ゲートウェイサーバーでは、CPU やメモリよりもディスクおよびネットワーク速度のほうが重要になります。

- PostgreSQL サーバー用に 1 台（32GB の RAM と 16 コアの CPU を搭載したもの)。
- ファイルリポジトリサービスおよびファイルストア用に 1 台。このサーバーのパラメータはそれほど重要ではありません。

ネットワーク接続

- Files Advanced Tomcat サーバー用の負荷分散装置が現在の Files Advanced の DNS アドレスを使用するように構成する必要があります。
- ゲートウェイサーバー用の負荷分散装置が現在のゲートウェイサーバーの DNS アドレスを使用するように構成する必要があります。
- Tomcat サーバーをゲートウェイ負荷分散装置に接続して、デスクトップネットワークノードを同期し、ウェブインターフェイス上のネットワークノードを参照できるように

します。このクラスタセットアップでは、Files Advanced ウェブ UI の [管理] ページと [ゲートウェイサーバー] ページの [クライアント接続のアドレス] は、外部負荷分散装置のアドレスになります。ゲートウェイサーバーのウェブでも、[Files Advanced サーバー接続に代替アドレスを使用] 設定を使用し、[Files Advanced ウェブサーバー接続用アドレス] にゲートウェイ負荷分散装置の内部アドレスを設定しています。

- モバイルクライアント接続に対応するために、ゲートウェイサーバーを Tomcat 負荷分散装置に接続します。

注意: 同期・共有データソースについて、アドレスを Tomcat 負荷分散装置のアドレスに変更する必要があります。

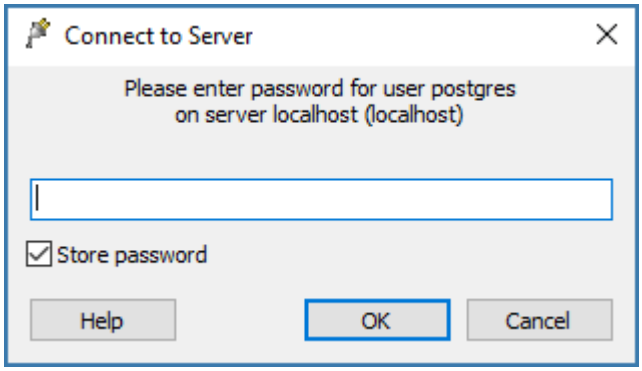
12.2.4.2 PostgreSQL サーバーの移行

データベースは最も重要なコンポーネントであるため、最初に移行してください。

セクションの内容

既存の PostgreSQL サーバー上での構成

1. **[サービス]** コントロールパネル（**services.msc**)を開いて、**Files Advanced Tomcat** サービスを停止します。
2. **Files Advanced PostgreSQL Administrator** アプリケーションを開き、データベースサーバーに接続します。**[データベース]** の横にある **[+]** をクリックします。
3. **acronisaccess_production** データベースを右クリックして、**[メンテナンス]** -> **[バキューム]**-> **[OK]** の順に選択します。



4. 管理者特権でコマンドプロンプトを開き、**cd** コマンドで Postgres の **bin** ディレクトリに移動します。（デフォルトでは **C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL\<version>\bin** にあります)。
5. 現在のコマンドプロンプトディレクトリが **bin** フォルダに変更されたら、以下のコマンドを入力します。

   pg_dumpall --host localhost --port 5432 --username postgres --file alldbs.sql

   注意: alldbs.sql というバックアップファイルが生成されて、**bin** フォルダに保存されます。このファイルに含まれる完全なパスは、必要に応じて別の場所（たとえば、**D:¥Backups¥alldbs.sql**)に保存できます。

   注意: 別のポートや別のユーザーを使用している場合、それに応じてコマンドを変更してください。
6. バックアップが完了したら、**Files Advanced PostgreSQL サーバー**サービスを停止して無効にします。
7. バックアップファイルを、PostgreSQL をホストする新しいコンピュータにコピーして移動します。

新しい PostgreSQL サーバー上での構成

1. Files Advanced のインストーラを起動して、**[次へ]** を押します。使用許諾契約を読み、承諾します。
2. **[カスタム]** をクリックし、PostgreSQL Database Server だけを選択します。**[次へ]** を押します。
3. PostgreSQL をインストールする場所を選択し、スーパーユーザー（**postgres**)のパスワードを入力します。

   注意: この場所は、他のすべてのサーバーが到達可能な場所でなければなりません。パスワードは、元の PostgreSQL サーバーで前に使用していたパスワードと同じものにしてください。
4. **[ファイアウォールでポート 5432 を開く]** を選択して、インストールを続行します。このポートを、PostgreSQL データベースにリモートからアクセスするために使用します。

PostgreSQL データベースへのアクセスの構成

1. インストールが完了したら、PostgreSQL の **data** フォルダ（デフォルトでは、**C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL\<version>\Data**)に移動し、 **pg_hba.conf** をテキストエディタで開きます。
2. Access Tomcat サーバーそれぞれのホストエントリを、内部アドレスを使用して組み込み、ファイルを保存します。すべてのサーバーのアドレスがわかっているわけではない場合、後でこのファイルに戻って編集できますが、それまでは、アドレスのわからないサーバーがデータベースに接続することはできません。

   pg_hba.conf（HBA はホストベース認証を表します)ファイルは、クライアント認証を制御するもので、データベースクラスタのデータディレクトリに保存されます。このファイル内に、接続を許可するサーバーと権限を指定します。たとえば、次のように指定します。

```
# TYPE DATABASE USER ADDRESS METHOD
# Loadbalancer1 (First Files Advanced & Gateway server)
host acronisaccess_production postgres 10.144.70.247/32 md5
```

注意: この例では、**postgres** という名前のユーザーアカウントが **md5 encrypted** 接続を使用して、10.144.70.247 にあるサーバーから接続し、完全な権限（**レプリケーション**権限を除く）で **acronisaccess_production** データベースにアクセスできます。

postgresql.conf ファイルを開き、以下の変更を加えます。

1. 行 **#listen_addresses = 'localhost'.** から先頭の **#** を削除し、**localhost** を ***** で置き換えます。変更後は、以下のようになるはずです。**listen_addresses = '*'**
2. 行 **#effective_cache_size = 128MB** から先頭の **#** を削除し、**128MB** を **12GB** で置き換えます。変更後は、以下のようになるはずです。 **effective_cache_size = 12GB**
3. 以下の注釈を追加します。**#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. **max_connections** を見つけて適切な値に変更します。これは、すべての Access サーバーノードに構成されている Tomcat の **DB_POOLSIZE** 設定値の合計に 10 を足した値以上でなければなりません。**DB_POOLSIZE** は、**250** に設定することをおすすめします。

   この例では **DB_POOLSIZE to 250** が設定されています。Access Tomcat サーバーは 2 台あることから、**max_connections** を **510** に設定する必要があります。Access Tomcat サーバーが 3 台ある場合は、**760** に設定することになります。
5. すべての変更を保存して、**postgresql.conf** ファイルを閉じます。
6. Files Advanced PostgreSQL サーバーサービスを再起動します。

データベースのインポート

新しい PostgreSQL サーバー上

1. Files Advanced PostgreSQL Administrator アプリケーションを開き、ローカルデータベースサーバーに接続し、**[データベース]** を選択して **acronisaccess_production** という名前のデータベースがあることを確認します。
2. データベースのバックアップファイル **alldbs.sql** を、PostgreSQL インストールの **bin** ディレクトリにコピーします。（デフォルトでは **C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL\<version>\bin** にあります）。
3. 管理者特権でコマンドプロンプトウィンドウを開き、**cd** コマンドで PostgreSQL の **bin** ディレクトリに移動します。
4. 次のコマンドを入力します: **psql -U postgres -f alldbs.sql**
5. パスワードの入力を求められたら、**postgres** ユーザーのパスワードを入力します。これにより、以前の PostgreSQL サーバーのデータベースが新しい PostgreSQL サーバーに復元されます。

12.2.4.3 Files Advanced サーバーの構成

セクションの内容

追加の Files Advanced サーバーの接続

Files Advanced ウェブサーバーのみのインストール

1. Files Advanced インストーラを起動し、使用許諾契約に同意します。
2. **[カスタム]** を選択し、Files Advanced ウェブサーバーのみを選択します。

   注意: Files Advanced ウェブサーバーをクリックすると、自動的に PostgreSQL サーバーも選択されますが、クリックして選択を解除できます。

3. インストールを完了し、Files Advanced Tomcat サービスが停止していることを確認します。

サーバーの設定

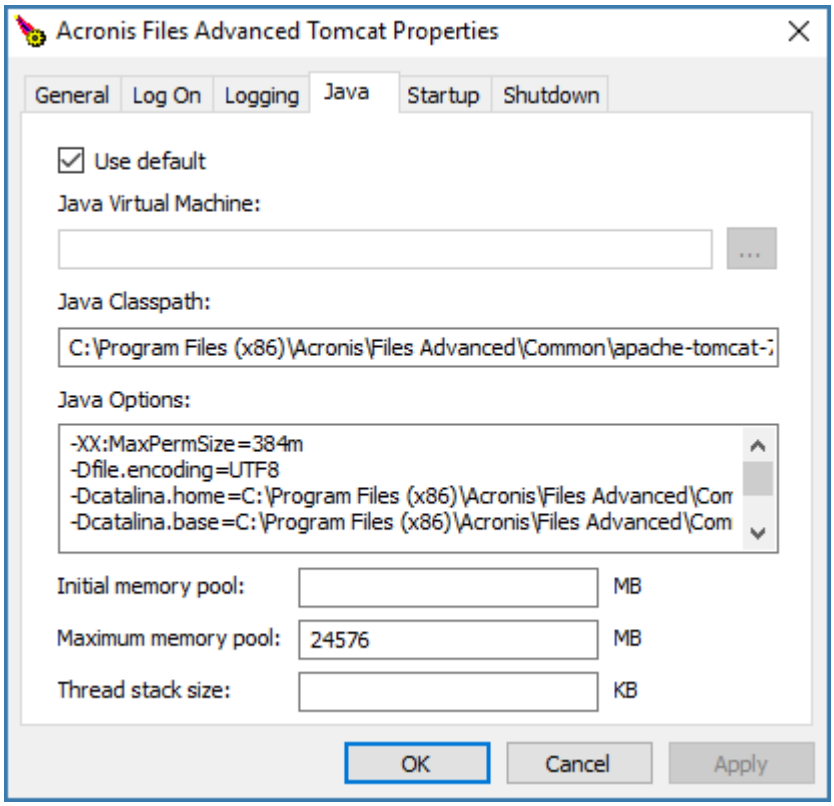
Files Advanced ウェブサーバーで変更したすべての設定は、その他すべての Files Advanced ウェブサーバーでも同じ変更を行う必要があります。

注意: `pg_hba.conf` ファイルに各 Files Advanced ウェブサーバーのエントリを追加することを忘れないでください。

Tomcat の最大メモリ使用量の構成

1. デスクトップから、**Files Advanced Tomcat サービス設定**ツールを起動します。このツールがデスクトップにない場合は、**[スタート]** -> **[すべてのプログラム]**- > **Files Advanced** に移動し、該当するショートカットをクリックします。
2. **[Java]** タブをクリックします。

3. **[メモリプールの最大サイズ]** 設定を **24576** に変更して、**[OK]** をクリックします。



適切なデータベースに接続するようサーバーを構成する

1. Files Advanced ウェブサーバーフォルダ（デフォルトでは **C:\Program Files (x86)\Acronis\Files Advanced\Access Server**)に移動し、**acronisaccess.cfg** ファイルを開きます。このファイルは、サーバーに PostgreSQL データベースサービスの場所を指示します。
2. 以下の値を設定します。

   DB_HOSTNAME =10.144.70.248
   DB_PORT =5432
   DB_POOLSIZE =250

   注意: DB_HOSTNAME は、PostgreSQL が現在実行されている IP アドレスです。この例では、10.144.70.248 となっています。

   注意: DB_POOLSIZE は、250 以上の値に設定することをおすすめします。
3. ファイルを保存します。

最大スレッド数の構成

Tomcat の負荷分散型セットアップでは、すべての Tomcat インスタンスによって生成される可能性のあるスレッドの合計数が、PostgreSQL データベースで受け入れるように構成された最大接続数を超えないようにすることが重要です。

スレッドの合計数を決定する重要な 3 つの設定は、以下のとおりです。

- **acronisaccess.cfg** ファイル内の **DB_POOLSIZE = 200**。250 以上の値に設定することをおすすめします。
- Tomcat の **server.xml** ファイル内の **maxThreads = 150.**。この設定は、デフォルトの 150 のままにすることをおすすめします。
- **postgresql.conf** ファイル内の **max_connections**。この設定は、前の手順で構成済みになっているはずです。この設定の値は、すべての Files Advanced ウェブサーバーに設定されている Tomcat の DB_POOLSIZE 値の合計に 10 を足した値以上でなければなりません。たとえば、Tomcat サーバーが 2 台の場合は 510、3 台の場合は 760 となります。

注意: これらのファイルに変更を加えた場合、対応するサービスを再起動する必要があります。

適切なロギングの構成

負荷分散構成では、Files Advanced Tomcat サービスによる IP アドレスのマッピングがログ内で適切に行われません。各接続が適切にログに記録されるよう、以下の変更を行う必要があります。

1. server.xml ファイル内で、次の行を見つけます。**<Valve**
   className=”org.apache.catalina.valves.AccessLogValve” directory=”logs” prefix=”localhost_access_log.” suffix=”.txt” pattern=”%h %l %u %t "%r" %s %b”/>.
2. 行の末尾に **requestAttributesEnabled=”true”** を追加します。
3. 同じ行の下に、以下を追加します。

   <Valve className="org.apache.catalina.valves.RemoteIpValve" remoteIpHeader="X-Forwarded-For" protocolHeader="X-Forwarded-Proto"/>
4. ファイルを保存し、Files Advanced Tomcat サービスを再起動します。

旧 Files Advanced サーバーの接続

必要に応じて、既存の Files Advanced サーバーを引き続き使用することもできますが、それにはそのサーバーを新しいデータベースに接続する必要があります。

リモートデータベースへの Files Advanced の接続

1. Files Advanced Server フォルダ（デフォルトでは **C:\Program Files (x86)\Acronis\Files Advanced\Access Server**)に移動し、**acronisaccess.cfg** ファイルを開きます。このファイルは、サーバーに PostgreSQL データベースサービスの場所を指示します。
2. 以下の値に設定します。

   ```
   DB_HOSTNAME =10.144.70.248
   DB_PORT =5432
   DB_POOLSIZE = 250
   ```

   注意: **DB_HOSTNAME** には、PostgreSQL データベースが位置する IP アドレスを設定します。この例では、10.144.70.248 となっています。
3. ファイルを保存してから、**[サービス]** コントロールパネル（services.msc)で **Files Advanced Tomcat サービス**を起動します。
4. 未使用の Files Advanced コンポーネントはすべてアンインストールできます。

12.2.4.4 ファイルストアとファイルリポジトリの移行

「ファイルストアとファイルリポジトリの移動『330ページ 』」ガイドを参照してください。確認しなければならない唯一の追加設定として、すべての Files Advanced コンポーネントがファイルリポジトリとファイルストアをホストする予定のコンピュータにアクセスできることを確認します。

S3 ストレージを使用する予定の場合、選択する S3 ストレージ内でファイルストアがホストされることになるため、ファイルリポジトリサービスをインストールする必要はありません。

ファイルリポジトリとファイルストアを現在の場所に維持することを予定している場合、必要な作業となるのは、新しい Files Advanced サーバーが適切なリポジトリエンドポイントを指し示していることを確認することだけです。

12.2.4.5 ゲートウェイサーバーの移行

新しいゲートウェイサーバーのインストール

1. 新しいコンピュータ上で、Files Advanced インストーラを起動し、使用許諾契約に同意します。
2. **[カスタム]** を選択し、ゲートウェイサーバーコンポーネントのみをインストールします。インストールを終了します。
3. 設定ユーティリティで、ゲートウェイのアドレス、ポート、証明書を設定します。設定する証明書は、ゲートウェイ負荷分散装置の DNS アドレスに関連付けられている SSL 証明書と同じものでなければなりません。

以前のゲートウェイサーバーのすべての設定の移行

1. Tomcat とゲートウェイの両方を実行していた前のコンピュータ上で、Files Advanced ウェブインターフェイスを開き、[ゲートウェイサーバー] ページを開きます。以前のゲートウェイのエントリが表示されます。
2. 新しいゲートウェイを追加するために、**[ゲートウェイサーバーの追加]** をクリックし、該当するすべてのデータを入力します。
3. **[クラスタグループの追加]** をクリックします。
   - 表示名を入力します。
   - **[クライアント接続のアドレス]** に値を入力します。クラスタでは、**[クライアント接続のアドレス]** に外部負荷分散装置のアドレスを入力します。入力し終わったら、**[Files Advanced サーバー接続に代替アドレスを使用]** をクリックし、**[Files Advanced サーバー接続用アドレス]** にゲートウェイ負荷分散装置の内部アドレスを入力します。
4. **[クラスタ化に使用できるゲートウェイ サーバー]** で、両方のゲートウェイサーバーの **[追加]** ボックスをオンにします。
5. **[設定に使用するゲートウェイサーバー]** で、旧ゲートウェイサーバーを選択します。
6. **[追加]** をクリックします。[ゲートウェイサーバー] ページに新しいクラスタが表示されます。[+] を使用してクラスタを展開します。

7. 新しいゲートウェイに、すべての設定が移行されているはずです。新しいゲートウェイをクラスタのマスターにするために、**[操作]** ドロップダウンメニューをクリックし、**[グループマスターにする]** を選択します。
8. 以前のゲートウェイはそのままにすることも、クラスタグループから除外することも、除外して削除することもできます。セットアップが正常に動作するようになるまで、クラスタの一部として残しておくことをおすすめします。

12.2.4.6 ログの管理と消去

追加の Files Advanced サーバーをインストールした後、Files Advanced Tomcat ログが維持されているフォルダに移動し、それらのフォルダに対する適切な権限を設定して、ログの書き込みおよび消去を行えるようにしてください。

12.2.4.7 負荷分散装置固有の設定

1. ブラウザで https://mylb.company.com を開き、設定が機能していることを確認します。
2. 負荷分散装置で時間ベースのセッションスティッキネス（またはご使用の負荷分散装置での同等の設定)を有効にし、期限切れにならないように設定します。
3. ヘルスチェック（HTTP ステータス 200 が返されることを確認する)が必要な場合は、https://INTERNALSERVERNAME:MANAGEMENTPORT/api/v1/server_version に ping します（例: https://myaccessserver.company.com/signin および https://myaccessserver.company.com/api/v1/server_version)。
4. 負荷分散型セットアップで IP アドレスと接続が適切にログに記録されるようにするには、負荷分散装置を構成して以下のヘッダーを設定する必要があります。
   - **X-Forwarded-For** これにより、各接続で負荷分散装置の IP アドレスが表示される代わりに、接続しているクライアントの実際の IP アドレスが表示されるようになります。
   - **X-Forwarded-Proto** これにより、実際に使用されているプロトコルが表示されます。

12.2.4.8 元のサーバーのクリーンアップ

元の本番サーバー上の Files Advanced Tomcat を引き続き使用する場合は、そのサーバーで使用されなくなった Files Advanced 項目をアンインストールすることをおすすめします。

コントロールパネルから、Files Advanced PostgreSQL サーバー、Files Advanced ゲートウェイサーバー、および（存在する場合)Files Advanced ファイルリポジトリサーバーをアンインストールできます。

12.2.5 API でウェブインターフェイスをカスタマイズする

API によるウェブインターフェイスのカラースキームのアップデートは、サービスの再起動が不要でダウンタイムを生じさせず、簡単に行うことができます。これらのカスタマイズには、Files Advanced のウェブインターフェイス 『177ページ 』から実行できるものもあります。

CURL のインストール

1. API コマンドを使用するには Curl をインストールする必要があります。
   a. 次のオフィシャルサイトから Curl をダウンロードしてください。
      https://curl.haxx.se/download.html

   注意: SSL をサポートするバージョンをダウンロードしてください！

   b. インストールが終了するまで、または単に Curl アーカイブが抽出されるまでは、Curl インストーラの表示に従ってください。

カスタムカラースキームの作成

1. 管理者特権でコマンドプロンプトを開き、次のコマンドを入力します。

```
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
```

注意: ファイル名には特定の命名構文を使用する必要があります。管理コンソールでは **color_scheme_<name_of_scheme>**.css を、ウェブクライアントコンソールでは

web_client_<name_of_scheme>.scss を使用する必要があります。

<**name_of_scheme**> は、Files Advanced インターフェイスに表示される新しいスキームの名前で、両方のファイルで同じにする必要があります。

上記コマンドは次のように動作します。

- 管理コンソールでは **.css** ファイルを選択します。
- ウェブクライアントコンソールでは **.scss** ファイルを選択します。
- ウェブインターフェイスの **[カラースキーム]** ドロップダウンから選択可能な新しいテーマを作成します。

注意: カラースキームの一部分だけを変更する場合は、上記コマンドを入力する際に、変更する部分には新しい .css スキームを使用し、変更しない部分には既存の .css スキームを使用する必要があります。

---

2. ここで、インターフェイスの管理部分用の配置されているスキームとウェブクライアント用の配置されているスキームをアップロードするコマンドの例を示します。
3. この例では、両方のファイルが **D:\WebUI** に配置されており、ウェブインターフェイスに表示されるカラースキーム名として **NewColor** を選択します。

```
curl -X PUT -F
customization_settings[color_scheme_administration_css_file]=@D:\WebUI\
color_scheme_NewColor.css -F
customization_settings[color_scheme_client_scss_file]=@D:\WebUI\web_cli
ent_NewColor.scss -u administrator:123456
https://myCompany.com/api/v1/settings/customization
```

4. **-F customization_settings[color_scheme]=<name_of_scheme>** コマンドを使用して、現在のスキームを、追加する新しいスキームに切り替えることもできます。後ろにこのコマンドを追加すると次のようになります。

```
curl -X PUT -F
customization_settings[color_scheme_administration_css_file]=@D:\WebUI\
color_scheme_NewColor.css -F
customization_settings[color_scheme_client_scss_file]=@D:\WebUI\web_cli
ent_NewColor.scss -F customization_settings[color_scheme]=NewColor -u
administrator:123456 https://myCompany.com/api/v1/settings/customization
-v
```

トラブルシューティング

- コマンドは実行されるが、インターフェイスに新しいテーマが表示されない

ファイル名が **color_scheme_<name_of_scheme>.css** と **web_client_<name_of_scheme>.scss** の正しい構文に従っていることを確認します。

- 「**libcurl でプロトコル https がサポートされていないか、無効になっています**」というエラーが表示される

  アドレスを囲んでいる単一引用符（'')を削除します。引用符を使用する必要がある場合は、代わりに、"https://myCompany.com/api/v1/settings/customization" のように二重引用符（"")を使用します。

- 証明書エラーが表示される

  自己署名証明書を使用している場合または IP アドレスを使用してコマンドを実行している場合は、コマンドの最後に **-k** フラグを追加して証明書エラーを無視する必要があります。

12.2.6 デスクトップ クライアントの無人設定

Microsoft のグループポリシー管理を使用することで、Files Advanced デスクトップクライアントを複数のコンピュータにリモートから簡単にインストールして設定することができます。エンドユーザーが行うのは、クライアントの起動とパスワードの入力だけです。また、グループ ポリシー管理では、エンド ユーザーが正しい設定を誤って変更したり置き換えたりすることはできません。誤って変更してしまった場合、ユーザーはログオフするだけで、正しい設定が次回のログイン時に再適用されます。

グループ ポリシー管理オブジェクトの作成および設定:

1. ドメイン コントローラで **[グループ ポリシー管理コンソール]** を開きます。
2. 目的のドメインを右クリックし、**[このドメインに GPO を作成し、このコンテナにリンクする...]** を選択します。
3. 名前を入力して **[OK]** をクリックします。
4. **[グループ ポリシー オブジェクト]** セクションを展開し、新しいポリシーを選択します。
5. **[スコープ]** タブで目的のサイト、ドメイン、OU、グループ、ユーザー、およびコンピュータを選択します。

クライアントの無人インストール

このセクションでは、ユーザーのログイン時に目的のすべてのコンピュータに Files Advanced デスクトップクライアントをサイレントインストールする方法について説明します。

インストーラ配布ポイントの作成

クライアントをインストールするすべてのコンピュータに、インストーラへのアクセス権が必要です。このためには、フォルダを作成し、目的のユーザーグループと共有してから、そのフォルダにインストーラを置きます。

1. インストーラがあるフォルダを右クリックして **[プロパティ]** を選択します。
2. **[共有]** タブを開き、**[共有]** を押します。
3. Access クライアントをインストールするドメイングループ、OU、またはユーザーを入力します。このグループ(または OU、ユーザー)は **[グループポリシーオブジェクト]** で選択したものと同じである必要があります。
4. **[OK]**/**[完了]** を押して残りのダイアログをすべて閉じます。

注意: 目的のコンピュータがネットワークアドレス(**`\\WIN2008\Software\AAClientInstaller.msi`** など)でインストーラにアクセスできることを確認します。

ユーザーのコンピュータへのインストーラの保存

1. ドメインコントローラで、**[グループポリシーオブジェクト]** セクションを展開し、新しいポリシーオブジェクトを右クリックします。
2. **[編集]** を選択し、**[ユーザーの構成]** → **[基本設定]** → **[Windows の設定]** → **[ファイル]** の順に展開します。
3. [ファイル] を右クリックし、[新規] → [ファイル] の順に選択します。
4. **[操作]** で **[作成]** を選択します。

5. **[ソースファイル]** で、[参照] ボタンをクリックしてアクセスクライアントのインストーラに移動するか、インストーラの完全なパスを入力します（¥¥WIN2008¥Software¥AAClientInstalelr.msi など)。
6. **[宛先ファイル]** に、宛先フォルダと宛先ファイル名を入力します。これで、ネットワーク共有から Access クライアントのインストーラがコピーされ、ログオンしているユーザーのコンピュータの宛先フォルダに保存されます。

   注: たとえば、**C:¥Folder¥ThisFile.msi** と入力すると、クライアントのインストーラがユーザーの **C** ドライブ上の Folder フォルダに **ThisFile.msi** という名前で保存されます。
7. **[OK]** を押します。

クライアントのインストール

インストールスクリプトの作成

1. 空のテキストファイルを作成し、次のスクリプトを貼り付けます。

   ```
   msiexec /i "C:\AAC.msi" /quiet
   sleep 180
   DEL /F /S /Q /A "C:\AAC.msi"
   ```

   このスクリプトによってコマンドプロンプトが開きます。プロンプトに何も表示されずに Access クライアントがインストールされ、3 分後に Access クライアントのインストーラが削除されます。
2. 両方の場所でパス **C:\AAC.msi** を、**[宛先ファイル]** フィールドに入力したパスに変更し、**[ファイル]** → **[名前を付けて保存]** の順に押します。
3. スクリプトの名前を入力し、拡張子が**.bat** であることを確認します。**[ファイルの種類:]** フィールドで、**[すべてのファイル]** を選択します。ファイルがドメインコントローラ上にあるか、ドメインコントローラがファイルにアクセスできることを確認します。このファイルは重要です。変更したり削除したりせず、変更されない特定の場所に保存してください。

ユーザーログオン時のスクリプトの使用

1. **[グループポリシーマネージャ]** を開き、**[グループポリシーオブジェクト]** セクションを展開して、新しい**ポリシーオブジェクト**を右クリックします。

2. **[編集]** を選択し、**[ユーザーの構成]** → **[基本設定]** → **[Windows の設定]** → **[スクリプト（ログオン/ログオフ)]** の順に展開します。
3. **[ログオン]** をダブルクリックして **[追加]** を押します。
4. **[スクリプトの追加]** ダイアログで、**[参照...]** を押し、スクリプトを保存したフォルダに移動します。
5. スクリプトを選択して **[開く]** を押します。
6. **[OK]** を押し、次のダイアログで **[OK]** をもう一度押します。
7. 操作は完了です。指定したグループまたは OU 内のすべてのユーザーに、ログオン時に Files Advanced クライアントがインストールされます。

フォルダおよびレジストリ エントリの作成:

次の例では、ユーザー名、同期フォルダ、サーバー URL、自動アップデートのチェックボックスのエントリ、およびクライアントによる自己署名証明書でのサーバーへの接続を必須にするエントリを作成します。

1. **[グループ ポリシー オブジェクト]** セクションを展開し、新しいポリシー オブジェクトを右クリックします。
2. **[編集]** を選択し、**[ユーザーの構成]** → **[基本設定]** → **[Windows の設定]** の順に展開します。

同期フォルダの作成:

1. **[フォルダ]** を右クリックし、**[新規]** → **[フォルダ]** の順に選択します。
2. **[操作]** を **[作成]** に設定します。
3. パスに次のトークンを入力します: **`%USERPROFILE%\Desktop\AAS Data Folder`**。

レジストリの作成:

1. **[レジストリ]** を右クリックし、**[新規]** → **[レジストリ項目]** の順に選択します。
2. **[操作]** を **[作成]** に設定します。
3. **[ハイブ]** で **[HKEY_CURRENT_USER]** を選択します。

4. パスに「**Software\Group Logic, Inc.\activEcho Client**」と入力します。
5. 目的のエントリで次の操作を実行します。
6. ユーザー名:
   a. **[値の名前]** に「**Username**」と入力します。
   b. **[値の種類]** に **REG_SZ** を選択します。
   c. **[値データ]** に 次のトークンを入力します。**%USERNAME%@%USERDOMAIN%**

   注意: シングルサインオンを使用する場合は、Username トークンを設定**しないでください**。代わりに、次の操作を実行します。

   - **SSO**:
   - **[値の名前]** に「**AuthenticateViaSSO**」と入力します。
   - **[値の種類]** で **[REG_SZ]** を選択します。
   - **[値データ]** に「**1**」と入力します。
7. サーバー URL:
   a. **[値の名前]** に「**Server URL**」と入力します。
   b. **[値の種類]** に **REG_SZ** を選択します。
   c. **[値データ]** に Files Advanced サーバーのアドレス（例: **https://myaccess.com**)を入力します。
8. 同期フォルダ:
   a. **[値の名前]** に「**activEcho Folder**」と入力します。
   b. **[値の種類]** に **REG_SZ** を選択します。
   c. **[値データ]** に トークンとパス「**%USERPROFILE%\Desktop\AAS Data Folder**」を入力します。
9. 自動アップデート:
   a. **[値の名前]** に「**AutoCheckForUpdates**」と入力します。
   b. **[値の種類]** に **DWORD** を選択します。
   c. **[値データ]** に「**00000001**」と入力します。値「**1**」でこの設定が有効になり、クライアントは自動的にアップデートを確認します。値を「**0**」に設定すると、この設定は無効になります。
10. 証明書:

a. **[値の名前]** に「**AllowInvalidCertificates**」と入力します。

b. **[値の種類]** に **DWORD** を選択します。

c. **[値データ]** に「**00000000**」と入力します。値「**0**」でこの設定が無効になり、クライアントは無効な証明書で Files Advanced サーバーに接続できなくなります。値を「**1**」に設定すると、この設定は有効になります。

12.2.7 シングルサインオンの設定

このガイドでは、Files Advanced でシングルサインオンの機能を有効化するための詳細設定の方法について説明します。

注意: シングルサインオンは有効なドメインでのみ使用できます。

注意: Files Advanced を単一ポート設定で実行している場合（ゲートウェイサーバーが Files Advanced サーバーの要求をプロキシ処理している場合)、シングルサインオンは**機能しません**。

注意: Files Advanced がドメインコントローラにインストールされている場合、シングルサインオンは**機能しません**。また、SSO の制限事項を無視する場合でも、パフォーマンス上の理由から、Files Advanced サーバーをドメインコントローラにインストールしないことを強くおすすめします。

シングルサインオンの機能を使用すると、有効な LDAP ユーザーはすべて、資格情報を入力しなくてもウェブインターフェイスおよびデスクトップクライアントにログインできます。ユーザーは Files Advanced アカウントが必要になります。または、LDAP プロビジョニングがサーバーで有効にされている必要があります。

- Files Advanced のログインページにリンクが表示されます。ユーザーは、このコンピュータへのログインに使用しているアカウントでログインします。

  注意: SSO の正常な動作のために、FQDN（https://access.company.com など)を使用して Files Advanced インターフェイスを開く必要があります。IP アドレスを使用してインターフェイスを開く場合、シングルサインオンは**機能しません**。

- デスクトップクライアントの場合、SSO を有効にできる新しいラジオボタンがあります。ユーザーは、Files Advanced サーバーの URL を入力すればよいだけです。この機能により、コンピュータへのログインに使用しているアカウントで自動的にログインできます。

注意: この機能はWindowsクライアントでのみ利用できます。Macでのサポートは今後のリリースで追加されます。

セクションの内容

12.2.7.1 同一コンピュータでの Files Advanced Web サーバーおよびゲートウェイサーバーの構成

構成はほぼ共通で、同一マシンにある 1 台の Files Advanced Web サーバーおよび 1 台の Files Advanced ゲートウェイサーバーです。これは、デフォルトのインストールです。

セクションの内容

Files Advanced Web サーバーと、ドメインの Kerberos サーバーを登録するために実行する必要がある手順を説明します。この手順を実行するのは一度だけです。SSO 認証チェックのクエリ送信先になる LDAP アカウントを指定するには、「setspn.exe」を使用します。

注意: 証明書認証を使用してモバイルクライアントを使用する場合、Access サーバーとゲートウェイサーバーの DNS エントリにコンピュータ名を使用することは**できません**。Files Advanced サーバーの SPN がマシン名と同じである場合、ゲートウェイサーバーでは Files Advanced サーバーを「同じマシン上にあるもの」として扱うため、Kerberos 認証の実行は試行されません。

例: 「**machineAccess.domain.com / machineGW.domain.com** 」は機能します。

例: 「**machine.domain.com / computer.domain.com will** 」は機能しません。

SSOを処理するLDAPアカウントの設定

注意: SMB または SharePoint のデータソースを使用する場合は、Active Directory アカウントを設定して、SMB および SharePoint データソースそれぞれへの Kerberos 委任を許可してください。詳細については、「詳細委任設定」を参照してください。

1. コマンドプロンプトを開きます。

   注意: ドメインアカウントでログインし、**setspn** を使用できるアクセス権が付与されている必要があります。

2. コマンド **`setspn -s HTTP/`computername.domain.com account name** を入力します。

   例: Files Advanced Web サーバーが **`ahsoka.acme.com`** にインストールされており、認証済みの LDAP アカウントとして **`john@acme.com`** を使用し Kerberos チケットを取得する場合、コマンドは次のようになります。

   ```
   setspn -s HTTP/ahsoka.acme.com john
   ```

   注意: 上記のコマンドで使用する LDAP アカウント名は、**`web.xml`** の **`spnego.preauth.username`** プロパティで指定するアカウントと**一致する**必要があります。

   注意: 通常、このアカウントは、Files Advanced のウェブインターフェイス（**[全般設定]** → **[LDAP]** → **[LDAP ユーザー名/LDAP パスワード]**)の管理者によって指定されている LDAP アカウントと一致します。ただし、必ずしも一致させる必要はありません。

3. Files Advanced Web サーバーがデフォルト以外のポート（443 以外のポート)で実行されている場合、ポート番号を使用して SPN を登録する必要もあります。

   例: サーバーがポート 444 で動作している場合、コマンドは次のようになります。

   ```
   setspn -s HTTP/ahsoka.acme.com:444 john
   ```

   注意: 上記のコマンドの **HTTP** は、**HTTP** プロトコルではなく、**HTTP** サービスクラスを指しています。**HTTP** サービスクラスでは、**HTTP** と **HTTPS** の両方のリクエストが処理されます。サービスクラスの名前に **HTTPS** を使用して SPN を作成する必要はありません。また、**作成しないでください**。

4. ドメインコントローラにアクセスし、**[Active Directory ユーザーとコンピュータ]** を開きます。
5. 上記のコマンドで使用されているユーザーを検索します（この場合、**john**)。

6. **[委任]** タブをクリックし、**[任意のサービスへの委任でこのユーザーを信頼する（Kerberos のみ)]** を選択します。
7. **[OK]** を押します。

ゲートウェイサーバーのSPNの設定

KDC（「キー配布センター」)Kerberos サーバーによるゲートウェイサーバーへのユーザー認証を可能にするには、setspn を実行してゲートウェイサーバーを KDC サーバーに登録し、「ユーザー」として実行されているサーバーのホスト名を setspn コマンドで指定する必要があります。

この設定が機能するためには、ゲートウェイサーバーに追加の DNS エントリを設定する必要があります。

1. DNS サーバーで、ドメインの **[前方参照ゾーン]** を開いて右クリックし、ゲートウェイサーバーに新しい**ホスト**エントリ**(A record)**を作成します。
2. 名前を入力します。これは、ゲートウェイサーバーへのアクセスに使用される DNS アドレスになります。

   例: ahsoka-gw.acme.com
3. ゲートウェイサーバーの IP アドレスを入力します (ポートは入力しません)。同じ IP アドレスでゲートウェイサーバーと Files Advanced サーバーを実行している場合は、その IP アドレスを入力します。
4. **[関連付けられたポインタ（PTR)レコードを作成する]** を選択し、**[ホストの追加]** を押します。
5. Files Advanced がインストールされているマシンに戻ります。
6. コマンドプロンプトを開きます。
7. **setspn** のコマンド、 **setspn -s HTTP/gatewaydns.domain.com computername** を入力します。

   たとえば、ゲートウェイサーバーがドメインのホスト**'ahsoka'** で実行されていて、DNS エントリが **ahsoka-gw.acme.com** の場合は、次のコマンドを実行します。

   setspn -s HTTP/ahsoka-gw.acme.com ahsoka

8. ゲートウェイサーバーがデフォルト以外のポート（443 以外のポート)で実行されている場合、ポート番号を使用して SPN を登録する必要もあります。たとえば、ゲートウェイサーバーがポート 444 で実行されている場合、次のように登録します。

   setspn -s HTTP/ahsoka-gw.acme.com:444 ahsoka

9. 目的のゲートウェイサーバーの **[管理のアドレス]** と **[クライアント接続のアドレス]** を、手順 4 で作成した新しいゲートウェイサーバーの DNS エントリに変更します。

   注意: 両方のアドレスを同じにする必要があり、また正しい DNS エントリに更新する必要もあります。

シングルサインオン認証で使用されるドメインアカウントの設定

1. **C:\Program Files (x86)\Acronis\Files Advanced\Access Server\Web Application\WEB-INF**に移動します。
2. **web.xml** ファイルを検索して開きます。このファイルに、SSO サービスが実行されるドメインのユーザー名およびパスワードを設定します。このアカウントは、「**ドメイン上**」のセクションで、Kerberos に HTTP サービスを登録するときに使用したアカウントと一致している**必要があります**。
3. **web.xml** には、設定が必要になる 2 つのプロパティ（SSO サービスが使用するドメインのユーザー名およびパスワード)があります。 次の行を検索します。

```
<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. **yourusername** を目的の LDAP ユーザー名に置き換えます。
5. **yourpassword** を、上記で指定した LDAP アカウントの LDAP パスワードに置き換えます。パスワードに 5 つの特殊文字、**&**、**>**、**"**、**'**、**<**のいずれかが含まれている場合は、XML ドキュメント内で正しくエスケープしておく必要があります。これを行うには、次のように置き換える必要があります。
   - **<**は**<**
   - **>**は**>**

- **"**は**"**
- **'**は**'**
- **&**は**&**

たとえば、パスワードが **<my&best'password"** の場合、 **web.xml** ファイルには次のように書き込む必要があります。**<my&best'password"**

Kerberos ドメインルックアップの設定

1. **C:\Program Files (x86)\Acronis\Files Advanced\Common\apache-tomcat-7.0.59\conf** に移動します。
2. **krb5.conf** ファイルを検索して開きます。
3. **krb5.conf** には、管理者から受け取る必要があるプロパティが 2 つだけあります。
   a. シングルサインオン用のドメイン （例: **ACME.COM**)。サーバーの DNS 名**ではなく**、ご使用のドメインの名前であることに注意してください。

   注意: krb5.conf のドメインには必ず**大文字**を使用してください。大文字を使用しない場合、Kerberos チケットの参照が失敗する可能性があります。

   b. Kerberos キー配布センターのアドレス（通常、プライマリドメインコントローラのアドレスと一致します。例: **acmedc.ACME.COM**)
4. インストールする **krb5.conf** ファイルの内容は次のようになります。

```
[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. **ACME.COM** のすべてのインスタンスをドメイン（**大文字**)に置き換えます。サーバーの DNS 名**ではなく**、ご使用のドメインの名前であることに注意してください。
6. "**kdc =**"の値をドメインコントローラの名前に置き換えます。ドメインは大文字にする必要があります（例: **kdc = yourdc.YOURDOMAIN.COM**)。
7. 上記の設定ファイルのアップデート後、変更内容を適用するために、Files Advanced サーバー（Files Advanced Tomcat サービス)を再起動する必要があります。

ウェブインターフェイスでのシングルサインオンの有効化:

1. Files Advanced ウェブインターフェイスを開き、管理者としてログインします。
2. **[全般設定]** タブを展開して、**[LDAP]** ページを開きます。
3. ページの最下部で、**[Windows/Mac の既存のログイン資格情報を使用してウェブクライアントおよびデスクトップ同期クライアントからログインすることを許可します]** のチェックボックスをオンにします。
4. **[保存]** を押します。

注意: ゲートウェイサーバーをホストするマシンが Files Advanced Web サーバーと同じドメイン内にある場合にのみ、以下の手順が使えます。

KDC（「キー配布センター」)Kerberos サーバーによるゲートウェイサーバーへのユーザー認証を可能にするには、setspn を実行してゲートウェイサーバーを KDC サーバーに登録し、「ユーザー」として実行されているサーバーのホスト名を setspn コマンドで指定する必要があります。

ゲートウェイサーバーが Files Advanced Web サーバーとは異なるマシンに存在する場合

1. コマンドプロンプトを開きます。
2. **setspn** のコマンド、 **setspn -s HTTP/computername.domain.com computername** を入力します。

   たとえば、ゲートウェイサーバーがドメインのホスト**'cody'** で実行されている場合は、次のコマンドを実行します。

   ```
   setspn -s HTTP/cody.acme.com cody
   ```

3. ゲートウェイサーバーがデフォルト以外のポート（443 以外のポート)で実行されている場合、ポート番号を使用して SPN を登録する必要もあります。たとえば、ゲートウェイサーバーがポート 444 で実行されている場合、次のように登録します。

   `setspn -s HTTP/cody.acme.com:444 cody`
4. 追加のゲートウェイサーバーすべてにこのセクションの手順を繰り返します。

ユーザーマシン上

ブラウザのシングルサインオンのサポートを有効にするには、クライアントマシンで簡単な設定を 1 回だけ行う必要があります。

注意: それぞれのマシンでユーザーごとに実行する必要があります。

注意: 複数のドメインにサービスがある場合は、ブラウザのセクションを 2 つ目のドメイン名を使用して繰り返してください。**たとえば、`*.acme.com`** と**`*.tree.com`** の両方を追加します。

Windows:

Internet Explorer の場合:

- Internet Explorer を開き、**[ツール]** → **[インターネットオプション]** → **[セキュリティ]** → **[ローカルイントラネット]** → **[サイト]** → **[詳細設定]** の順に選択し、Files Advanced サーバーのアドレス（例: **`https://ahsoka.acme.com (`** または **`*.acme.com)`**)を追加して、ブラウザを再起動します。

Chrome の場合:

Chrome では **Internet Explorer** と同様の設定が使用されます。そのため、SSO 用に Internet Explorer を設定すると、**Chrome** も同じように機能します。ただし、資格情報の委任 (ウェブインターフェイスからネットワークノードを参照する際に必要)を有効にするには、**Chrome** で委任を許可するように設定する必要があります（**Internet Explorer** ではデフォルトで許可されます)。

1. レジストリエディタ（**regedit32.exe**)を開きます。
2. **`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome`** に移動します。
3. まだ存在しない場合には **`Google\Chrome`** キーを作成します。
   a. ポリシーフォルダを右クリックし、**[新規]** → **[キー]** の順に選択します。

b. フォルダ名に「**Google**」と入力します。

c. **Google** フォルダを右クリックし、**[新規]** → **[キー]** の順に選択します。

d. フォルダ名に「**Chrome**」と入力します。

e. Chrome フォルダをクリックし、右側にあるホワイトパネルで右クリックして **[新規]** → **[キー]** の順に選択します。

f. キーの名前を入力します: **AuthNegotiateDelegateWhitelist**。

4. ドメイン名（たとえば、**ahsoka.acme.com** や ***.acme.com**)を **AuthNegotiateDelegateWhitelist** レジストリキーの値として設定します。
5. Chrome を再起動します。

Firefox の場合:

1. アドレスバーに **about:config** と入力し、Enter キーを押します。
2. **network.negotiate-auth.trusted-uris** の設定を検索して編集し、**https://ahsoka.acme.com** または **just .acme.com**（カンマ区切りのリスト)を追加します。

   注意: すべてのサブドメインを追加するには、「**.example.com**」の形式を使用します（***.example.com ではありません**)。

3. ネットワークの**データソース**サポートを有効にするには、**network.negotiate-auth.delegation-uris** を編集する必要もあります。編集では、**ahsoka.acme.com** またはドメイン **acme.com** を追加します。
4. **Firefox** を再起動します。

Mac:

注意: それぞれのマシンでユーザーごとに実行する必要があります。

Safari の場合:

そのまま動作します。

Firefox の場合:

1. アドレスバーに **about:config** と入力し、Enter キーを押します。
2. **network.negotiate-auth.trusted-uris** の設定を検索して編集し、**https://ahsoka.acme.com** または **just .acme.com**（カンマ区切りのリスト)を追加します。

   注意: すべてのサブドメインを追加するには、「**.example.com**」の形式を使用します（***.example.com ではありません**)。
3. ネットワークの**データソース**サポートを有効にするには、**network.negotiate-auth.delegation-uris** を編集する必要もあります。編集では、**ahsoka.acme.com** またはドメイン **acme.com** を追加します。
4. **Firefox** を再起動します。

Chrome の場合:

1. **Ticket Viewer** アプリケーション（**/System/Library/CoreServices/Ticket Viewer**)を使用して、Kerberos チケットがあるどうかを確認し、自動的に作成されていなかった場合は作成することができます。

   注意: kinit とパスワードを入力してから、**ターミナル**経由でチケットを作成することもできます。
2. 使用するすべてのドメインに対する認証を許可するために Chrome のホワイトリストを設定するには、**ターミナル**を開いて次のコマンドを実行します。

   ```
   $ defaults write com.google.Chrome AuthServerWhitelist “*.acme.com”
   $ defaults write com.google.Chrome AuthNegotiateDelegateWhitelist “*.acme.com”
   ```
3. Chrome ブラウザを再起動します。

12.2.7.2 異なるマシンでの Files Advanced サーバーおよびゲートウェイサーバーの構成

セクションの内容

Files Advanced サーバーと、ドメインの Kerberos サーバーを登録するために実行する必要がある手順を説明します。この手順を実行するのは一度だけです。SSO 認証チェックのクエリ送信先になる LDAP アカウントを指定するには、「setspn.exe」を使用します。

注意: 証明書認証を使用してモバイルクライアントを使用する場合、Access サーバーとゲートウェイサーバーの DNS エントリにコンピュータ名を使用することは**できません**。Files Advanced サーバーの SPN がマシン名と同じである場合、ゲートウェイサーバーでは Files Advanced サーバーを「同じマシン上にあるもの」として扱うため、Kerberos 認証の実行は試行されません。

例: 「**machineAccess.domain.com / machineGW.domain.com** 」は機能します。

例: 「**machine.domain.com / computer.domain.com will** 」は機能しません。

SSOを処理するLDAPアカウントの設定

注意: SMB または SharePoint のデータソースを使用する場合は、Active Directory アカウントを設定して、SMB および SharePoint データソースそれぞれへの Kerberos 委任を許可してください。詳細については、「詳細委任設定」を参照してください。

1. コマンドプロンプトを開きます。

   注意: ドメインアカウントでログインし、**setspn** を使用できるアクセス権が付与されている必要があります。

2. コマンド **setspn -s HTTP/computername.domain.com account name** を入力します。

   例: Files Advanced サーバーが **ahsoka.acme.com** にインストールされており、認証済みの LDAP アカウントとして **john@acme.com** を使用し Kerberos チケットを取得する場合、コマンドは次のようになります。

   setspn -s HTTP/ahsoka.acme.com john

   注意: 上記のコマンドで使用する LDAP アカウント名は、**web.xml** の **spnego.preauth.username** プロパティで指定するアカウントと**一致する**必要があります。

   注意: 通常、このアカウントは、Files Advanced のウェブインターフェイス（**[全般設定]** → **[LDAP]** → **[LDAP ユーザー名/LDAP パスワード]**)の管理者によって指定されている LDAP アカウントと一致します。ただし、必ずしも一致させる必要はありません。

3. Files Advanced サーバーがデフォルト以外のポート（443 以外のポート)で実行されている場合、ポート番号を使用して SPN を登録する必要もあります。

   例: サーバーがポート 444 で動作している場合、コマンドは次のようになります。

   ```
   setspn -s HTTP/ahsoka.acme.com:444 john
   ```

   注意: 上記のコマンドの **HTTP** は、**HTTP** プロトコルではなく、**HTTP** サービスクラスを指しています。**HTTP** サービスクラスでは、**HTTP** と **HTTPS** の両方のリクエストが処理されます。サービスクラスの名前に **HTTPS** を使用して SPN を作成する必要はありません。また、**作成しないでください**。

4. ドメインコントローラにアクセスし、**[Active Directory ユーザーとコンピュータ]** を開きます。
5. 上記のコマンドで使用されているユーザーを検索します（この場合、**john**)。
6. **[委任]** タブをクリックし、**[任意のサービスへの委任でこのユーザーを信頼する（Kerberos のみ)]** を選択します。
7. **[OK]** を押します。

ゲートウェイサーバーのSPNの設定

KDC（「キー配布センター」)Kerberos サーバーによるゲートウェイサーバーへのユーザー認証を可能にするには、setspn を実行してゲートウェイサーバーを KDC サーバーに登録し、「ユーザー」として実行されているサーバーのホスト名を setspn コマンドで指定する必要があります。

ゲートウェイサーバーが Files Advanced サーバーとは異なるマシンに存在する場合

1. コマンドプロンプトを開きます。
2. **setspn** のコマンド、 **`setspn -s HTTP/`computername.domain.com computername** を入力します。

   たとえば、ゲートウェイサーバーがドメインのホスト**`'cody'`** で実行されている場合は、次のコマンドを実行します。

   ```
   setspn -s HTTP/cody.acme.com cody
   ```

3. ゲートウェイサーバーがデフォルト以外のポート（443 以外のポート)で実行されている場合、ポート番号を使用して SPN を登録する必要もあります。たとえば、ゲートウェイサーバーがポート 444 で実行されている場合、次のように登録します。

   setspn -s HTTP/cody.acme.com:444 cody
4. すべてのゲートウェイサーバーにこのセクションの手順を繰り返します。

ゲートウェイサーバーが Files Advanced サーバーと同じコンピュータに存在する場合

ゲートウェイサーバーが Files Advanced サーバーと同じコンピュータに存在する場合にのみ、この手順を実行する必要があります。その他の場合には、このセクションをスキップしてください。この設定が機能するためには、ゲートウェイサーバーに追加の DNS エントリを設定する必要があります。

1. DNS サーバーで、ドメインの **[前方参照ゾーン]** を開いて右クリックし、ゲートウェイサーバーに新しい**ホスト**エントリ**(A record)**を作成します。
2. 名前を入力します。これは、ゲートウェイサーバーへのアクセスに使用される DNS アドレスになります。

   例: codygw.acme.com
3. ゲートウェイサーバーの IP アドレスを入力します (ポートは入力しません)。同じ IP アドレスでゲートウェイサーバーと Files Advanced サーバーを実行している場合は、その IP アドレスを入力します。
4. **[関連付けられたポインタ（PTR)レコードを作成する]** を選択し、**[ホストの追加]** を押します。
5. Files Advanced がインストールされているマシンに戻ります。
6. コマンドプロンプトを開きます。
7. **setspn** のコマンド、 **setspn -s HTTP/gatewaydns.domain.com computername** を入力します。

   たとえば、ゲートウェイサーバーがドメインのホスト**'cody'** で実行されていて、DNS エントリが **codygw.acme.com** の場合は、次のコマンドを実行します。

   setspn -s HTTP/codygw.acme.com cody

8. ゲートウェイサーバーがデフォルト以外のポート（443 以外のポート)で実行されている場合、ポート番号を使用して SPN を登録する必要もあります。たとえば、ゲートウェイサーバーがポート 444 で実行されている場合、次のように登録します。

   setspn -s HTTP/codygw.acme.com:444 cody
9. まだ実行しない場合は、目的のゲートウェイサーバーの**管理のアドレス**を、手順 4 で作成したゲートウェイサーバーの DNS エントリに変更する必要があります。

`web.xml` **ファイルの編集**:

1. **C:\Program Files (x86)\Acronis\Files Advanced\Access server\Web Application\WEB-INF**に移動します。
2. **web.xml** ファイルを検索して開きます。このファイルに、SSO サービスが実行されるドメインのユーザー名およびパスワードを設定します。このアカウントは、「**ドメイン上**」のセクションで、Kerberos に HTTP サービスを登録するときに使用したアカウントと一致している**必要があります**。
3. **web.xml** には、設定が必要になる 2 つのプロパティ（SSO サービスが使用するドメインのユーザー名およびパスワード)があります。 次の行を検索します。

```
<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. **yourusername** を目的の LDAP ユーザー名に置き換えます。
5. **yourpassword** を、上記で指定した LDAP アカウントの LDAP パスワードに置き換えます。パスワードに 5 つの特殊文字、**&**、**>**、**"**、**'**、**<**のいずれかが含まれている場合は、XML ドキュメント内で正しくエスケープしておく必要があります。これを行うには、次のように置き換える必要があります。
   - **<**は**<**
   - **>**は**>**
   - **"**は**"**
   - **'**は**'**

- **&**は**&**

たとえば、パスワードが **<my&best'password"** の場合、 **web.xml** ファイルには次のように書き込む必要があります。**<my&best'password"**

krb5.conf **ファイルの編集**:

1. **C:\Program Files (x86)\Acronis\Files Advanced\Common\apache-tomcat-7.0.59\conf** に移動します。
2. **krb5.conf** ファイルを検索して開きます。
3. **krb5.conf** には、管理者から受け取る必要があるプロパティが 2 つだけあります。
   a. シングルサインオン用のドメイン（例: **ACME.COM**）

   注意: krb5.conf のドメインには必ず**大文字**を使用してください。大文字を使用しない場合、Kerberos チケットの参照が失敗する可能性があります。

   b. Kerberos キー配布センターのアドレス（通常、プライマリドメインコントローラのアドレスと一致します。例: **acmedc.ACME.COM**）
4. インストールする **krb5.conf** ファイルの内容は次のようになります。

```
[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. **ACME.COM** のすべてのインスタンスをドメイン（**大文字**)に置き換えます。

6. "**kdc =**"の値をドメインコントローラの名前に置き換えます。ドメインは大文字にする必要があります（例: **kdc = yourdc.YOURDOMAIN.COM**)。
7. 上記の設定ファイルのアップデート後、変更内容を適用するために、Files Advanced サーバー（Files Advanced Tomcat サービス)を再起動する必要があります。

ウェブインターフェイスでのシングルサインオンの有効化:

1. Files Advanced ウェブインターフェイスを開き、管理者としてログインします。
2. **[全般設定]** タブを展開して、**[LDAP]** ページを開きます。
3. ページの最下部で、**[Windows/Mac の既存のログイン資格情報を使用してウェブクライアントおよびデスクトップ同期クライアントからログインすることを許可します]** のチェックボックスをオンにします。
4. **[保存]** を押します。

ユーザーマシン上

ブラウザのシングルサインオンのサポートを有効にするには、クライアントマシンで簡単な設定を 1 回だけ行う必要があります。

注意: それぞれのマシンでユーザーごとに実行する必要があります。

注意: 複数のドメインにサービスがある場合は、ブラウザのセクションを 2 つ目のドメイン名を使用して繰り返してください。**たとえば、*.acme.com** と***.tree.com** の両方を追加します。

Windows:

Internet Explorer の場合:

- Internet Explorer を開き、**[ツール]** → **[インターネットオプション]** → **[セキュリティ]** → **[ローカルイントラネット]** → **[サイト]** → **[詳細設定]** の順に選択し、Files Advanced サーバーのアドレス（例: **https://ahsoka.acme.com (** または ***.acme.com)**)を追加して、ブラウザを再起動します。

Chrome の場合:

Chrome では **Internet Explorer** と同様の設定が使用されます。そのため、SSO 用に Internet Explorer を設定すると、**Chrome** も同じように機能します。ただし、資格情報の委任 (ウェブインターフェイスからネットワークノードを参照する際に必要)を有効にするには、**Chrome** で委任を許可するように設定する必要があります（**Internet Explorer** ではデフォルトで許可されます)。

1. レジストリエディタ（**regedit32.exe**)を開きます。
2. **HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome** に移動します。
3. まだ存在しない場合には **Google\Chrome** キーを作成します。
   a. ポリシーフォルダを右クリックし、**[新規]** → **[キー]** の順に選択します。
   b. フォルダ名に「**Google**」と入力します。
   c. **Google** フォルダを右クリックし、**[新規]** → **[キー]** の順に選択します。
   d. フォルダ名に「**Chrome**」と入力します。
   e. Chrome フォルダをクリックし、右側にあるホワイトパネルで右クリックして **[新規]** → **[キー]** の順に選択します。
   f. キーの名前を入力します: **AuthNegotiateDelegateWhitelist**。
4. ドメイン名（たとえば、**ahsoka.acme.com** や ***.acme.com**)を **AuthNegotiateDelegateWhitelist** レジストリキーの値として設定します。
5. Chrome を再起動します。

Firefox の場合:

1. アドレスバーに **about:config** と入力し、Enter キーを押します。
2. **network.negotiate-auth.trusted-uris** の設定を検索して編集し、**https://ahsoka.acme.com** または **just .acme.com**（カンマ区切りのリスト)を追加します。

注意: すべてのサブドメインを追加するには、「**.example.com**」の形式を使用します（***.example.com ではありません**)。

3. ネットワークの**データソース**サポートを有効にするには、**network.negotiate-auth.delegation-uris** を編集する必要もあります。編集では、**ahsoka.acme.com** またはドメイン **acme.com** を追加します。
4. **Firefox** を再起動します。

Mac:

注意: それぞれのマシンでユーザーごとに実行する必要があります。

Safari の場合:

そのまま動作します。

Firefox の場合:

1. アドレスバーに **about:config** と入力し、Enter キーを押します。
2. **network.negotiate-auth.trusted-uris** の設定を検索して編集し、**https://ahsoka.acme.com** または **just .acme.com**（カンマ区切りのリスト)を追加します。

   注意: すべてのサブドメインを追加するには、「**.example.com**」の形式を使用します（***.example.com** **ではありません**)。
3. ネットワークの**データソース**サポートを有効にするには、**network.negotiate-auth.delegation-uris** を編集する必要もあります。編集では、**ahsoka.acme.com** またはドメイン **acme.com** を追加します。
4. **Firefox** を再起動します。

Chrome の場合:

1. **Ticket Viewer** アプリケーション（**/System/Library/CoreServices/Ticket Viewer**)を使用して、Kerberos チケットがあるどうかを確認し、自動的に作成されていなかった場合は作成することができます。

   注意: **kinit** とパスワードを入力してから、**ターミナル**経由でチケットを作成することもできます。

2. 使用するすべてのドメインに対する認証を許可するために Chrome のホワイトリストを設定するには、**ターミナル**を開いて次のコマンドを実行します。

```
$ defaults write com.google.Chrome AuthServerWhitelist “*.acme.com”
$ defaults write com.google.Chrome AuthNegotiateDelegateWhitelist
“*.acme.com”
```

3. Chrome ブラウザを再起動します。

12.2.7.3 ドメインフォレスト内の Files Advanced

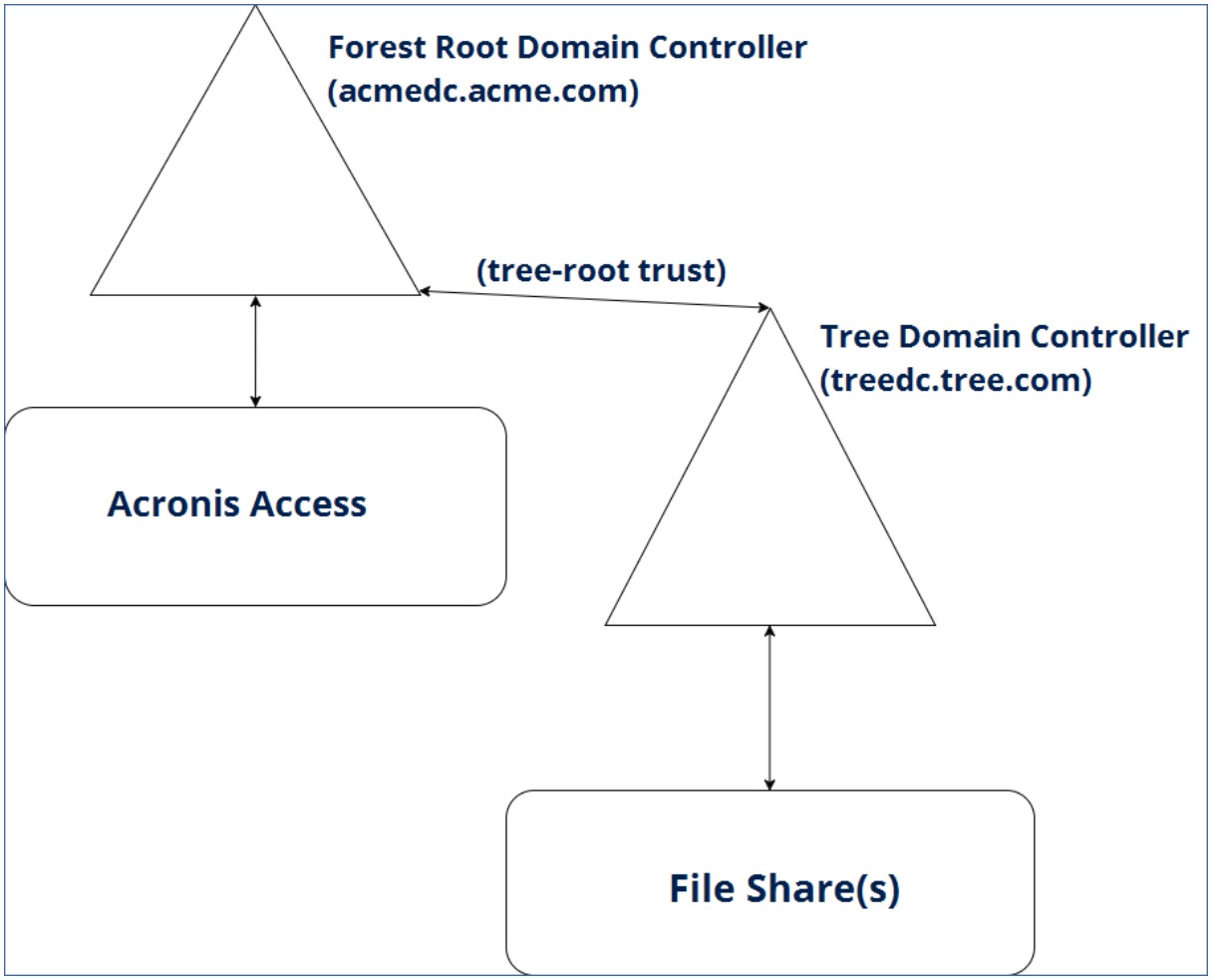
Windows Server 2012 には Microsoft からリソースベースの **Kerberos 制約付き委任**が追加されており、これによりフォレスト間制約付き委任が可能になっています。そのため、導入環境で (同一フォレスト内の)複数のドメインにリソースがある場合でもシングルサインオンを使用することができ、リソースにゲートウェイサーバーをインストールする必要がありません。

注意: この機能を利用するには、フォレスト内のすべてのドメインが**ドメイン機能レベル 2012** 以上で稼働している必要があります。

この記事では、以下の作業を行う方法を説明します。

- Files Advanced サーバーを SSO 用にセットアップする。
- ゲートウェイサーバーを SSO 用にセットアップする。
- フォレスト間制約付き委任を動作させるためのドメインでのすべての構成。

- SSO を使用するためにユーザーが行う必要のあるセットアップ。



セクションの内容

要件

このガイドでは、単一のフォレスト内でマルチドメインを稼働させるための構成について説明します。現状で、LDAP が正しく構成されており、ユーザーが問題なくドメインにログインでき、フォレスト内のドメイン間の接続が正しく構成されていることを前提としています。

- このタイプの制約付き委任は、**ドメイン機能レベル 2102** 以上で稼働するドメインコントローラでのみ利用可能です。リソースベースの Kerberos 制約付き委任は、Windows Server 2012 で初めて可能になりました。
- **[グローバルカタログ]** が有効で動作している必要があります。

ユーザーマシン上

ブラウザのシングルサインオンのサポートを有効にするには、クライアントマシンで簡単な設定を 1 回だけ行う必要があります。

注意: それぞれのマシンでユーザーごとに実行する必要があります。

注意: 複数のドメインにサービスがある場合は、ブラウザのセクションを 2 つ目のドメイン名を使用して繰り返してください。**たとえば、`*.acme.com`** と**`*.tree.com`** の両方を追加します。

Windows:

Internet Explorer の場合:

- Internet Explorer を開き、**[ツール]** → **[インターネットオプション]** → **[セキュリティ]** → **[ローカルイントラネット]** → **[サイト]** → **[詳細設定]** の順に選択し、Files Advanced サーバーのアドレス（例: **`https://ahsoka.acme.com`** (または **`*.acme.com`**))を追加して、ブラウザを再起動します。

Chrome の場合:

Chrome では **Internet Explorer** と同様の設定が使用されます。そのため、SSO 用に Internet Explorer を設定すると、**Chrome** も同じように機能します。ただし、資格情報の委任 (ウェブインターフェイスからネットワークノードを参照する際に必要)を有効にするには、**Chrome** で委任を許可するように設定する必要があります（**Internet Explorer** ではデフォルトで許可されます)。

1. レジストリエディタ（**regedit32.exe**)を開きます。
2. **`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome`** に移動します。
3. まだ存在しない場合には **`Google\Chrome`** キーを作成します。
   a. ポリシーフォルダを右クリックし、**[新規]** → **[キー]** の順に選択します。

b. フォルダ名に「**Google**」と入力します。

c. **Google** フォルダを右クリックし、**[新規]** → **[キー]** の順に選択します。

d. フォルダ名に「**Chrome**」と入力します。

e. Chrome フォルダをクリックし、右側にあるホワイトパネルで右クリックして **[新規]** → **[キー]** の順に選択します。

f. キーの名前を入力します: **AuthNegotiateDelegateWhitelist**。

4. ドメイン名（たとえば、**ahsoka.acme.com** や ***.acme.com**)を **AuthNegotiateDelegateWhitelist** レジストリキーの値として設定します。
5. Chrome を再起動します。

Firefox の場合:

1. アドレスバーに **about:config** と入力し、Enter キーを押します。
2. **network.negotiate-auth.trusted-uris** の設定を検索して編集し、**https://ahsoka.acme.com** または **just .acme.com**（カンマ区切りのリスト)を追加します。

   注意: すべてのサブドメインを追加するには、「**.example.com**」の形式を使用します（***.example.com ではありません**)。

3. ネットワークの**データソース**サポートを有効にするには、**network.negotiate-auth.delegation-uris** を編集する必要もあります。編集では、**ahsoka.acme.com** またはドメイン **acme.com** を追加します。
4. **Firefox** を再起動します。

Mac:

注意: それぞれのマシンでユーザーごとに実行する必要があります。

Safari の場合:

そのまま動作します。

Firefox の場合:

1. アドレスバーに **about:config** と入力し、Enter キーを押します。
2. **network.negotiate-auth.trusted-uris** の設定を検索して編集し、**https://ahsoka.acme.com** または **just .acme.com**（カンマ区切りのリスト)を追加します。

   注意: すべてのサブドメインを追加するには、「**.example.com**」の形式を使用します（***.example.com ではありません**)。
3. ネットワークの**データソース**サポートを有効にするには、**network.negotiate-auth.delegation-uris** を編集する必要もあります。編集では、**ahsoka.acme.com** またはドメイン **acme.com** を追加します。
4. **Firefox** を再起動します。

Chrome の場合:

1. **Ticket Viewer** アプリケーション（**/System/Library/CoreServices/Ticket Viewer**)を使用して、Kerberos チケットがあるどうかを確認し、自動的に作成されていなかった場合は作成することができます。

   注意: kinit とパスワードを入力してから、**ターミナル**経由でチケットを作成することもできます。
2. 使用するすべてのドメインに対する認証を許可するために Chrome のホワイトリストを設定するには、**ターミナル**を開いて次のコマンドを実行します。

   ```
   $ defaults write com.google.Chrome AuthServerWhitelist “*.acme.com”
   $ defaults write com.google.Chrome AuthNegotiateDelegateWhitelist “*.acme.com”
   ```
3. Chrome ブラウザを再起動します。

Files Advanced サーバー上

セクションの内容

4.

1. **C:\Program Files (x86)\Acronis\Files Advanced\Access Server\Web Application\WEB-INF**に移動します。
2. **web.xml** ファイルを検索して開きます。このファイルに、SSO サービスが実行されるドメインのユーザー名およびパスワードを設定します。

   このアカウントは、以降のセクションで Kerberos に **HTTP** サービスを登録するときに使用するアカウントと一致している**必要がある**ので、ここで書き留めておくことをお勧めします。
3. **web.xml** には、設定が必要になる 2 つのプロパティ (SSO サービスが使用するドメインのユーザー名およびパスワード)があります。 次の行を検索します。

```
<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. **yourusername** を目的の LDAP ユーザー名に置き換えます。
5. **yourpassword** を、上記で指定した LDAP アカウントの LDAP パスワードに置き換えます。パスワードに 5 つの特殊文字、**&**、**>**、**"**、**'**、**<**のいずれかが含まれている場合は、XML ドキュメント内で正しくエスケープしておく必要があります。これを行うには、次のように置き換える必要があります。
   - **<**は**<**
   - **>**は**>**
   - **"**は**"**
   - **'**は**'**
   - **&**は**&**

   例: パスワードが**<my&best'password"**である場合、 **web.xml** ファイルには次のように書き込む必要があります。**<my&best'password"**

1. **C:\Program Files (x86)\Acronis\Files Advanced\Common\apache-tomcat-7.0.59\conf** に移動します。
2. **krb5.conf** ファイルを検索して開きます。

3. **krb5.conf** には、管理者から受け取る必要があるプロパティが 2 つだけあります。
   a. シングルサインオン用のドメイン （例: **ACME.COM**)。
      - これは、Files Advanced Web サーバーとゲートウェイサーバーがあるドメインである必要があります。
      - サーバーの DNS 名**ではなく**、ご使用のドメインの名前であることに注意してください。

注意: krb5.conf のドメインには必ず**大文字**を使用してください。大文字を使用しない場合、Kerberos チケットの参照が失敗する可能性があります。

   b. Kerberos キー配布センターのアドレス（通常、プライマリドメインコントローラの **DNS** アドレスと一致します。例: **acmedc.ACME.COM**)これは、Files Advanced とそのコンポーネントがあるドメイン内のドメインコントローラのアドレスです。
4. インストールする **krb5.conf** ファイルの内容は次のようになります。

```
[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. **ACME.COM** のすべてのインスタンスをドメイン（**大文字**)に置き換えます。サーバーの DNS 名**ではなく**、ご使用のドメインの名前であることに注意してください。
6. "**kdc =**"の値をドメインコントローラの DNS 名に置き換えます。ドメイン部分は大文字にする必要があります（例: **kdc = yourdc.YOURDOMAIN.COM**)。

7. 上記の設定ファイルのアップデート後、変更内容を適用するために、Files Advanced サーバー（Files Advanced Tomcat サービス)を再起動する必要があります。

1. Files Advanced ウェブインターフェイスを開き、管理者としてログインします。
2. **[全般設定]** タブを展開して、**[LDAP]** ページを開きます。
3. ページの最下部で、**[Windows/Mac の既存のログイン資格情報を使用してウェブクライアントおよびデスクトップ同期クライアントからログインすることを許可します]** のチェックボックスをオンにします。
4. **[保存]** を押します。

Files Advanced Web サーバーの追加 DNS エントリの構成

同じコンピュータにゲートウェイサーバーがある場合は、Files Advanced Web サーバー用に別個の DNS エントリが必要です。

1. DNS サーバーで、ドメインの **[前方参照ゾーン]** を開いて右クリックし、Files Advanced Web サーバーに新しい**ホスト**エントリ**(A record)**を作成します。
2. 名前を入力します。これは、Files Advanced Web サーバーへのアクセスに使用される DNS アドレスになります。

   例: ahsokaccess.acme.com
3. Files Advanced Web サーバーの IP アドレスを入力します（ポートは入力しません)。同じ IP アドレスでゲートウェイサーバーと Files Advanced Web サーバーを実行している場合は、その IP アドレスを入力します。
4. **[関連付けられたポインタ（PTR)レコードを作成する]** を選択し、**[ホストの追加]** を押します。

Files Advanced Web サーバーの SPN の設定

1. Files Advanced が実行されているコンピュータで、コマンドプロンプトを開きます。

   注意: ドメインアカウントでログインし、**setspn** を使用できるアクセス権が付与されている必要があります。
2. コマンド **setspn -s HTTP/access_DNS_name.domain.com account name** を実行します。

注意: 上記のコマンドに使用する LDAP アカウント名は、**web.xml** ファイルで指定したアカウントと一致させる**必要があります**。

- たとえば、Files Advanced Web サーバーが **ahsoka.acme.com** にインストールされており、認証済みの LDAP アカウントとして **john@acme.com** を使用して Kerberos チケットを付与する場合、コマンドは次のようになります。
  setspn -s HTTP/ahsokaaccess.acme.com john
- たとえば、Files Advanced Web サーバーが **ahsoka.acme.com** にインストールされており、認証済みの LDAP アカウントとして **jane@tree.com** を使用して Kerberos チケットを付与する場合、コマンドは次のようになります。
  setspn -s HTTP/ahsokaaccess.acme.com tree\jane

注意: 通常、このアカウントは、Files Advanced のウェブインターフェイスの管理者によって **[LDAP の設定]**で指定されている LDAP アカウントと一致します。ただし、必ずしも一致させる必要はありません。

3. Files Advanced Web サーバーがデフォルト以外のポート（443 以外のポート)で実行されている場合、ポート番号を使用して SPN を登録する必要もあります。

   例: サーバーがポート 444 で動作している場合、コマンドは
   setspn -s HTTP/ahsokaaccess.acme.com:444 john または
   setspn -s HTTP/ahsokaaccess.acme.com:444 tree\jane になります。

   注意: 上記のコマンドの **HTTP** は、**HTTP** プロトコルではなく、**HTTP** サービスクラスを指しています。**HTTP** サービスクラスでは、**HTTP** と **HTTPS** の両方のリクエストが処理されます。サービスクラスの名前に **HTTPS** を使用して SPN を作成する必要はありません。また、**作成しないでください**。

4. ユーザーが利用しているドメインコントローラにアクセスし、**[Active Directory ユーザーとコンピュータ]** を開きます。ユーザーが利用するドメインが複数ある場合は、前のステップで使用したユーザーが含まれるドメインを開きます。
5. 上記のコマンドで使用されているユーザーを検索します（この場合、**john** または **jane**)。
6. **[委任]** タブをクリックし、**[任意のサービスへの委任でこのユーザーを信頼する（Kerberos のみ)]** を選択します。この設定を有効にすると、LDAP オブジェクトが認証を任意のサービスに委任できるようになります。ここでは、ゲートウェイサーバーサービスに委任します。

7. **[OK]** を押します。

Files Advanced にログインできることを確認する

1. ドメインコントローラまたは Files Advanced Web サーバー以外のコンピュータに移動します。
2. Files Advanced ウェブコンソールを開き、ログインページのパスワードフィールドの下にあるリンクを使用します。

注意: Files Advanced に招待されたドメインユーザー、すでにログインしているドメインユーザー、またはプロビジョニング済み LDAP グループのメンバーであるドメインユーザーとして、そのコンピュータにログインしている必要があります。

注意: ブラウザが SSO リクエストを受け入れるために、「ユーザーマシン上」セクションの手順をすべて行う必要があります。

ゲートウェイサーバー上

セクションの内容

KDC（「キー配布センター」)Kerberos サーバーによるゲートウェイサーバーへのユーザー認証を可能にするには、**setspn** を実行してゲートウェイサービスを KDC サーバーに登録し、「ユーザー」として実行されているサーバーのホスト名を **setspn** コマンドで指定する必要があります。

ゲートウェイサーバーの追加 DNS エントリの構成

この構成が機能するためには、ゲートウェイサーバーの DNS エントリも別個に設定する必要があります。

1. DNS サーバーで、ドメインの **[前方参照ゾーン]** を開いて右クリックし、ゲートウェイサーバーに新しい**ホスト**エントリ**(A record)**を作成します。
2. 名前を入力します。これは、ゲートウェイサーバーへのアクセスに使用される DNS アドレスになります。

   例: codygw.acme.com

3. ゲートウェイサーバーの IP アドレスを入力します (ポートは入力しません)。同じ IP アドレスでゲートウェイサーバーと Files Advanced サーバーを実行している場合は、その IP アドレスを入力します。
4. **[関連付けられたポインタ（PTR)レコードを作成する]** を選択し、**[ホストの追加]** を押します。

ローカルゲートウェイサーバーの SPN の構成

1. Files Advanced がインストールされているコンピュータに戻ります。
2. コマンドプロンプトを開きます。
3. ゲートウェイサーバーの SPN の設定:
   a. ゲートウェイサーバーがローカルシステムアカウントとして実行している場合のコマンドは次のようになります。
   b. **`setspn -s HTTP/gatewaydns.domain.com computername`**

   たとえば、ゲートウェイサーバーがドメインのホスト**`'cody'`** で実行されていて、DNS エントリが **`codygw.acme.com`** の場合は、次のコマンドを実行します。
   `setspn -s HTTP/codygw.acme.com cody`
   c. ゲートウェイサーバーがデフォルト以外のポート（443 以外のポート)で実行されている場合、ポート番号を使用して SPN を登録する必要もあります。たとえば、ゲートウェイサーバーがポート 444 で実行されている場合は、次のように登録します。
   `setspn -s HTTP/codygw.acme.com:444 cody`
4. まだ実行していない場合は、希望するゲートウェイサーバーの**管理のアドレス**を、作成したゲートウェイサーバーDNS エントリ（**`codygw.acme.com`**)に変更する必要があります。

SPN がゲートウェイ用に正しく設定されたことを確認する

1. ローカルゲートウェイ用のローカルボリュームがある場合、SSO を使用してログインすることにより、SPN と委任が機能していることを確認できます。この確認作業は、Files Advanced サーバーとドメインコントローラ以外のコンピュータで行います。そうしないと、SSO は機能しません。

2. ローカルゲートウェイのボリュームを参照します。参照できるなら、次に進みます。参照できない場合は、適切なオブジェクトに適切な SPN が正しく構成されているかを確認してください。

   注意: リモートファイルサーバー上のボリュームを参照しようとすると、アクセス拒否エラーになります。

注意: このタイプの制約付き委任は、ドメイン機能レベル 2102R2 以上で稼働するドメインコントローラでのみ利用可能です。ドメイン間の Kerberos 制約付き委任は、Windows Server 2012 で初めて可能になりました。

リソースベース制約付き委任を使用して、ファイルサーバーまたは別のドメインにある他のネットワークリソースへのアクセス権をユーザーに付与することができます。

1. ファイルサーバーがあるドメインのドメインコントローラに移動して、**PowerShell** を開きます。
2. ゲートウェイサービスが **LocalSystem** アカウントとして実行している場合のコマンドは次のようになります。
   a. **$computer1 = Get-ADComputer -Identity <gateway_server_computer> -server <domain_controller_for_this_domain>**
      例: `$computer1 = Get-ADComputer -Identity cody -server dc.acme.com`
      このコマンドはゲートウェイサーバーのコンピュータオブジェクトを取得し、接続する AD ドメインサービスインスタンスを指定し、その情報を**$computer1** 変数に保存します。
   b. **Set-ADComputer <file_server_computer> -PrincipalsAllowedToDelegateToAccount $computer1**
      例: `Set-ADComputer cody -PrincipalsAllowedToDelegateToAccount $computer1`
      このコマンドはファイルサーバーコンピュータオブジェクトの **[Principals Allowed To Delegate To Account]** プロパティをゲートウェイサーバーのコンピュータオブジェクトに設定します。このように設定することにより、ゲートウェイサーバーコンピュータはファイルサーバーのコンピュータに委任することができます。
3. ゲートウェイサービスが**ユーザーアカウント**として実行している場合のコマンドは次のようになります。

a. **$user1 = Get-ADUser -Identity <logon_user_of_the_gateway_service> -server <domain_controller_for_this_domain>**

   例: `$user1 = Get-ADUser -Identity jane -server dc.acme.com`

   このコマンドはゲートウェイサーバーが実行するときのユーザーのオブジェクトを取得し、接続する AD ドメインサービスインスタンスを指定し、その情報を**$user1** 変数に保存します。

b. **Set-ADComputer <file_server_computer> -PrincipalsAllowedToDelegateToAccount $user1**

   例: `Set-ADComputer cody -PrincipalsAllowedToDelegateToAccount $user1`

   このコマンドはファイルサーバーコンピュータオブジェクトの **[Principals Allowed To Delegate To Account]** プロパティをゲートウェイサーバーが実行するときのユーザーオブジェクトに設定します。このように設定することにより、選択したユーザーはファイルサーバーのコンピュータに委任することができます。

4. ゲートウェイユーザーアカウントが資格情報の委任先になり得るアカウントとして追加されたことを確認するには、次のコマンドを実行します。

   Get-ADComputer <file_server_machine> -Properties PrincipalsAllowedToDelegateToAccount

   例: `Get-ADComputer omega -Properties PrincipalsAllowedToDelegateToAccount`

5. すべてのファイルサーバーにこれらのステップを繰り返します。

委任が伝播するにはいくらか時間がかかります。小規模な LDAP 導入であれば 10〜15 分、大規模な構造であればそれ以上の時間がかかります。

注意: ゲートウェイサーバーをホストするマシンが Files Advanced Web サーバーと同じドメイン内にある場合にのみ、以下の手順が使えます。

KDC（「キー配布センター」)Kerberos サーバーによるゲートウェイサーバーへのユーザー認証を可能にするには、setspn を実行してゲートウェイサーバーを KDC サーバーに登録し、「ユーザー」として実行されているサーバーのホスト名を setspn コマンドで指定する必要があります。

ゲートウェイサーバーが Files Advanced Web サーバーとは異なるマシンに存在する場合

1. コマンドプロンプトを開きます。
2. **setspn** のコマンド、 **setspn -s HTTP/computername.domain.com computername** を入力します。

   たとえば、ゲートウェイサーバーがドメインのホスト**'cody'** で実行されている場合は、次のコマンドを実行します。

   setspn -s HTTP/cody.acme.com cody
3. ゲートウェイサーバーがデフォルト以外のポート（443 以外のポート)で実行されている場合、ポート番号を使用して SPN を登録する必要もあります。たとえば、ゲートウェイサーバーがポート 444 で実行されている場合、次のように登録します。

   setspn -s HTTP/cody.acme.com:444 cody
4. 追加のゲートウェイサーバーすべてにこのセクションの手順を繰り返します。

リソースベース Kerberos 制約付き委任へのアクセス権がない場合、リモート共有および別のドメインにあるリソースへの SSO を構成する別の方法は、そのドメイン内のコンピュータにゲートウェイサーバーをインストールする方法です。これにより、通常の Kerberos 制約付き委任を使用することができ、**機能レベル 2008 のドメインでも作業できます**。

対象のドメインのコンピュータにゲートウェイサーバーをインストールする

1. Files Advanced インストーラをダウンロードして、対象のコンピュータにインストーラを移動します。
2. Files Advanced インストーラを起動し、使用許諾契約に同意してから、**[次へ]** を押します。
3. **[カスタム...]** インストールを選択して、ゲートウェイサーバーのチェックボックスのみを選択します。
4. **[インストール]** を押します。インストールが終了したら、インストーラを閉じます。
5. **設定ユーティリティ**で、ゲートウェイの IP アドレスとポートを設定します。

ゲートウェイサービスがユーザーアカウントとして実行するように設定する

1. **[コントロールパネル]** -> **[管理ツール]** -> **[サービス]** を開きます。

2. Files Advanced ゲートウェイサーバーサービスを検索して右クリックし、**[プロパティ]** を選択します。
3. **[ログオン]** タブを選択し、**[このアカウント]** ラジオボタンを選択します。
4. **[参照]** を押して検索するか、またはユーザーのユーザー名とパスワードを入力して、サービスを実行するときのユーザーを選択します。選択するユーザーは、Files Advanced がインストールされているのと同じドメインのユーザー**でなければなりません**。Files Advanced サーバーの SPN に使用するアカウントではなく、専用のアカウントを使用することをお勧めします。
5. **[OK]** を押して、**[サービス]** コントロールパネルを閉じます。選択したユーザーアカウントに必要な許可が設定されていない状態ではサービスが起動しないので、まだサービスは再起動しないでください。

選択したユーザーに必要な権限を付与する

1. サービスをユーザーとして実行するには、ユーザーに**オペレーティング システムの一部として機能**が付与され、ユーザーがローカル管理者グループに含まれている必要があります。
2. **[ローカルセキュリティポリシー]** を開いて、**[ローカルポリシー]** -> **[ユーザー権利の割り当て]** に移動します。この変更は、導入環境によっては **[グループポリシーマネージャー]** で行う必要があります。
3. **[オペレーティング システムの一部として機能]** オブジェクトを開き、**[ユーザーを追加]** または **[グループ]** を押します。
4. ゲートウェイサービスの専用ユーザーを選択します。
5. 開いているすべてのダイアログを閉じて、**[コントロールパネル]** -> **[ユーザーアカウント]** -> **[アカウントの管理]** を開きます。
6. **[追加]** を押して、専用アカウントのドメインとユーザー名を入力します。
7. これで、**[サービス]** コントロールパネルで Files Advanced ゲートウェイサービスを再起動できます。

リモートゲートウェイサーバーのSPNの構成

1. Files Advanced サーバーがあるドメインの任意のコンピュータに移動します。

2. コマンドプロンプトを開きます。
3. SPN を構成するために実行するコマンドは、次のとおりです。**setspn – s HTTP/gatewaydns.domain.com useraccountfor_gw**

   例:ゲートウェイサーバーを **tree.com** ドメインのホスト **'magpie'** で稼働し、かつ **acme.com** ドメインの **peter** ユーザーアカウントとして実行する場合は、次のコマンドを実行します。

   setspn -s HTTP/magpie.tree.com peter

   ゲートウェイサーバーがデフォルト以外のポート（443 以外のポート)で実行されている場合、ポート番号を使用して SPN を登録する必要もあります。たとえば、ゲートウェイサーバーがポート 444 で実行されている場合は、次のように登録します。

   setspn -s HTTP/magpie.tree.com:444 peter
4. まだ実行していない場合は、希望するゲートウェイサーバーの**管理のアドレス**を、作成したゲートウェイサーバーDNS エントリ（**magpie.tree.com**)に変更する必要があります。
5. ゲートウェイサーバーの **[ユーザーモードでネゴシエート/Kerberos 認証を実行します]** 『119ページ 』 が有効になっていることを確認してください。この設定を有効にした後、Files Advanced ゲートウェイサービスを再起動する必要があります。
6. 2 番目のドメインのリソース用に**データソース**を作成する際、同じドメインにあるゲートウェイサーバーを必ず使用してください。

   例: ユーザーに **repository.tree.com** ファイルに対するアクセス権を付与する場合は、**tree.com** にあるゲートウェイサーバー（**magpie.tree.com** など)を指定する必要があります。

SPN がゲートウェイ用に正しく設定されたことを確認する

1. ローカルゲートウェイ用のローカルボリュームがある場合、SSO を使用してログインすることにより、SPN と委任が機能していることを確認できます。
2. ローカルゲートウェイのボリュームを参照します。参照できない場合は、適切なオブジェクトに適切な SPN が正しく設定されているかを確認してください。
3. 委任の変更が伝播するのに時間がかかる場合があります（小規模な LDAP 導入の場合は 10～15 分、大規模な LDAP 導入の場合はそれ以上)。

12.2.7.4 SPN 登録の確認

対象のSPNが適切に登録されたかどうかを確認するには、次の手順に従ってクエリを実行します。

1. [管理者特権でのコマンドプロンプト] を開きます。
2. **setspn -Q HTTP/computername.domain.com** コマンドを入力します。

   例: **setspn -Q HTTP/ahsoka.acme.com**
3. 特定のドメインユーザーに登録されている SPN にクエリを実行するには、**-l**（小文字の L)スイッチを使用します。

   例: **setspn -l john**
4. SPN の登録後、SSO を使用して認証できるようにするには、クライアントマシンを再起動するか、クライアントマシンで次のコマンドを実行する必要があります。

   klist purge

12.2.7.5 SMB または SharePoint データソースの使用

SMB または SharePoint のデータソースを使用する場合、Active Directory アカウントを設定して、SMB および SharePoint データソースごとに Kerberos 委任を許可してください。

ネットワーク共有と SharePoint サーバーの場合の手順

次の手順を実行すると、ゲートウェイ サーバーからターゲット サーバーへの委任が可能になります。

1. **[Active Directory ユーザーとコンピューター]** を開きます。
2. ゲートウェイ サーバーに対応するコンピュータ オブジェクトを特定します。

   注意: User アカウントを使用してゲートウェイサーバーを稼働させている場合は、代わりにその **User** オブジェクトを選択してください。
3. ユーザーを右クリックし、[プロパティ] を選択します。
4. **Delegation** タブを開きます。
5. **[指定されたサービスへの委任でのみこのコンピューターを信頼する]** を選択します。

6. このセクションで、**Use any authentication protocol** を選択します。
7. **Add** をクリックします。
8. **Users or Computers** をクリックします。
9. SMB 共有または SharePoint サーバーのサーバー オブジェクトを検索し、**[OK]** をクリックします。
   - SMB 共有の場合、**[cifs]** サービスを選択します。
   - SharePoint の場合、**[http]** サービスを選択します。
10. Files Advanced ゲートウェイサーバーがアクセスする必要があるサーバーごとに上記の手順を繰り返します。
11. ゲートウェイサーバーごとに上記のプロセスを繰り返します。

委任を変更する場合、ドメインフォレストのサイズによっては、反映が完了するまで数分かかることがあります。変更内容が有効になるまで、15 分程度（場合によっては 15 分以上）待機する必要がある場合があります。15 分経過しても機能しない場合は、Files Advanced ゲートウェイサービスを再起動してください。

12.2.7.6 クライアント証明書認証でモバイルクライアントを使用する

これは、実行が必要な追加手順です。ゲートウェイサーバーと Files Advanced サーバーが同じマシン上にあるかどうかにかかわらず、ゲートウェイサーバーから Files Advanced サーバーへの委任を設定する必要があります。

Kerberos 制約付き委任

この委任タイプは、Files Advanced サーバーとゲートウェイサーバーが同じドメイン内に存在する場合に機能します。

1. これを行うには、ドメインコントローラ上の Active Directory を開きます。
2. ゲートウェイサーバーのコンピュータオブジェクトを検索して編集し、委任タブに移動します。
3. **[指定されたサービスへの委任でのみこのコンピューターを信頼する]** および **[任意の認証プロトコルを使う]** を選択します。

4. Files Advanced サーバーの SPN を選択するには、[追加] をクリックして、Files Advanced サーバーの **HTTP** SPN に関連付けられているアカウントのユーザー名を入力します。

   注意: Files Advanced サーバーが実行されているコンピュータを検索するのではなく、ユーザー名で検索する必要があります。

   注意: Files Advanced サーバーへの Kerberos 認証は、単一ポートモードとの互換性がありません。

5. ユーザーを検索すると **HTTP** サービスが表示されるため、これらのサービスを選択します（SPN をポート付きとポートなしで 2 回登録している場合は、サービスが 2 つ表示されることがあります)。
6. **[適用]** を押してすべてのダイアログを閉じます。

リソースベースの Kerberos 制約付き委任

この委任タイプは、Access サーバーとゲートウェイサーバーがドメインフォレスト内の別々のドメインにある場合に機能します。

注意: この機能を利用するには、Files Advanced がアクセスするすべてのドメインを**ドメイン機能レベル 2012** 以上で稼働する必要があります。

1. Files Advanced サーバー専用で、SPN を設定した DNS エントリが実際に [データソース] ページで S&S ボリュームのアドレスとして設定されていることを再確認してください。
2. ゲートウェイサーバーと Files Advanced サーバーの間の委任を設定します。今回、委任はゲートウェイサーバーから Files Advanced サーバーに渡されます。
3. 以下のユーザーに対して次のコマンドを実行します。

   $pc1 = Get-ADComputer -Identity <ゲートウェイマシンの名前>

   Set-ADUser <Access_SSO ユーザーアカウント>
   -PrincipalsAllowedToDelegateToAccount $pc1

   例: `$pc1 = Get-ADComputer -Identity ahsoka`

   `Set-ADUser john -PrincipalsAllowedToDelegateToAccount $pc1`
4. ゲートウェイをユーザーアカウントとして実行している場合は、次のコマンドを使用して、2 つのユーザーアカウントの間の委任として設定する必要があります。

$user1 = Get-ADUser -Identity <ゲートウェイユーザーアカウント>

Set-ADUser <Access_SSO ユーザーアカウント>

-PrincipalsAllowedToDelegateToAccount $user1

例: `$user1 = Get-ADUser -Identity gwuser`

`Set-ADUser john -PrincipalsAllowedToDelegateToAccount $user1`

委任が伝播するにはいくらか時間がかかります。小規模な LDAP 導入であれば 10～15 分、大規模な構造であればそれ以上の時間がかかります。

12.2.7.7 負荷分散環境

ゲートウェイサーバーではオプションとして、ウェブサーバーによる Kerberos/ネゴシエート認証を試行するのではなく、すべての HTTP 認証をユーザーモードで実行することを選択できます。このオプションは、単一または複数のゲートウェイの SSO 処理を負荷分散装置の背後で実行する場合に必要になります。

この機能を有効にするには、ウェブインターフェイスを開いて、**[モバイルアクセス]** → **[ゲートウェイサーバー]** の順に移動し、クラスタグループの **[編集]** オプションをクリックし、**[詳細設定]** に移動して、チェックボックス **[ユーザーモードでネゴシエート/Kerberos 認証を実行します]** をオンにします。

ネットワークノードの有効化

SSO の使用中にウェブ内のネットワークノードにアクセスできるようにするためには、いくつかの変更が必要になります。ゲートウェイサーバーは負荷分散装置の背後で実行されているため、Kerberos への登録でコンピュータ名ではなくユーザーアカウントを使用する必要があります。

このためには、ゲートウェイサービスをユーザーアカウントの下で実行する必要があります。Files Advanced サーバーが登録されている同じ LDAP ユーザーを使用するか、ゲートウェイサービス専用の新規の LDAP ユーザーを選択できます。

どちらの場合も、選択したユーザーに対して、ゲートウェイサーバーがインストールされているコンピュータ上でオペレーティングシステムの一部として機能するための権限を与える必要があります。

オペレーティングシステムの一部として機能するユーザーの選択

1. ゲートウェイサーバーがインストールされているコンピュータで **[スタート]** → **[ファイル名を指定して実行]** の順にクリックします。
2. 「**gpedit.msc**」と入力し、**[OK]** を押します。
3. **[Windows の設定]** → **[セキュリティの設定]** の順に展開します。
4. **[ローカル ポリシー]** を展開し、**[ユーザー権利の割り当て]** をクリックします。
5. リストで **[オペレーティング システムの一部として機能]** を右クリックし、**[プロパティ]** を選択します。
6. このウィンドウで、ユーザーおよびグループの追加や削除ができます。目的のユーザー名を入力し、[OK] を押します。
7. 残りのウィンドウをすべて閉じ、変更を有効にするためにサーバーを再起動します。

ゲートウェイサーバーのサービスを選択したユーザーアカウントとして実行する

サービスとして実行するユーザーを追加したら、ゲートウェイサービスをそれらのユーザーとして実行するように設定する必要があります。これを行うには、次の手順に従います。

1. ゲートウェイサーバーがインストールされているコンピュータで **[スタート]** → **[ファイル名を指定して実行]** の順にクリックします。
2. 「**services.msc**」と入力し、**[OK]** を押します。または、**[コントロール パネル]** を開き、**[管理ツール]** → **[サービス]** の順に移動します。
3. リストで **[Files Advanced ゲートウェイ]** を右クリックし、**[プロパティ]** を選択します。
4. **[ログオン]** タブをクリックします。
5. **[このアカウント:]** ラジオボタンを選択し、オペレーティングシステムの権限を与えたユーザーの資格情報を入力します。
6. **[OK]** をクリックしてすべてのウィンドウを閉じます。

ゲートウェイサーバーのSPNの設定

キー配布センターKerberos サーバーによるゲートウェイクラスタへのユーザーの認証を可能にするためには、それぞれのゲートウェイサーバーとゲートウェイの負荷分散装置を KDC サーバーに登録する必要があります。それには、**setspn** を実行してアカウント名を指定します（サービスはこのアカウントとして実行されます)。

1. コマンドプロンプトを開きます。
2. 次のコマンドを入力します。

   setspn -s HTTP/computername.domain.com username

   たとえば、ゲートウェイサービスがユーザー**john** として実行されている場合のコマンドは次のようになります。

   setspn -s HTTP/gatewayserver1.acme.com john
3. ゲートウェイサーバーがデフォルト以外のポート（443 以外のポート)で実行されている場合、ポート番号を使用して SPN を登録する必要もあります。たとえば、ゲートウェイサーバーがポート 444 で実行されている場合、次のように登録します。

   setspn -s HTTP/gatewayserver1.acme.com:444 john
4. それぞれのゲートウェイサーバーと負荷分散装置について、上記の手順を繰り返します。負荷分散装置の SPN は次のようになります。

   setspn -s HTTP/gwloadbalancerdns.acme.com john

- デスクトップクライアントまたはウェブクライアントのユーザーは、Files Advanced サーバーを実行しているコンピュータとは別の（ただし、同じドメイン内の)コンピュータを使用する必要があります。そうでなければ、SSO を使用できません。
- サーバーへのアクセスには、SPN の場合とまったく同じ FQDN を使用してください（**https://ahsoka.acme.com** など)。他の DNS 名や IP アドレスは使用できません（**https://localhost** 、**https://10.20.56.33** など)。
- SSO を使用せずに、クライアントの Windows コンピュータとまったく同じ LDAP 資格情報を入力して Files Advanced サーバーにログインできることを確認します。これにより、SSO の設定にかかわらず、アカウントの資格情報が Files Advanced に対して有効であることが確認されます。
- SSO を使用せず、LDAP のログインアカウントと同じ資格情報を使用して、すべてのデータソースにアクセスできることを確認します。

- SSO を介してログインできない場合は、接続先の FQDN に対して SSO 用のウェブブラウザを設定していること、ドメインアカウントを使用してクライアントコンピュータにログインしていることを再確認してください。
- Files Advanced サーバーがドメインコントローラで実行されている場合、シングルサインオンは機能しません。
- ドメインコントローラのコンピュータからアクセスする場合、Files Advanced で SSO は機能しません。

  注意: Kerberos の仕様により、ドメインコントローラまたは Files Advanced サーバー上で実行されているクライアントアプリケーションやウェブブラウザからは、SSO 認証を行うことができません。

  また、Files Advanced サーバーがドメインコントローラ上で実行されている場合、Files Advanced サーバーからドメインコントローラへの認証を行うことはできません。

- SSO を使用してログインする際に **401 エラー**が発生する場合には、**web.xml** ファイル内のユーザー名およびパスワードを確認し、特殊文字を適切にエスケープしてください。特殊文字は **&**、**>**、**"**、**'**、または **<** です。これらのエスケープ方法については、**「web.xml ファイルの編集」セクションの手順 5 を参照してください。**

12.2.8 Files Advanced での信頼されたサーバー証明書の使用

このセクションでは、信頼できるサーバー証明書を使用して Files Advanced を設定する方法について説明します。

デフォルトで、Files Advanced はテスト目的の自己生成 SSL 証明書を提供します。信頼できる証明機関によって署名された証明書を使用することにより、サーバーの識別情報が確立され、エラーなしにクライアントが接続できるようになります。

注意: 自己署名証明書を使用している場合、ウェブブラウザで警告メッセージが表示されます。これらのメッセージを無視すると、テスト目的でシステムを使用できます。

本番環境での自己署名証明書の使用はサポートされていません。本稼動時には、適切な CA 証明書を実装する必要があります。

注意: 証明書の作成は、現在 Files Advanced の機能ではなく、今後もその予定はありません。証明書要求は、証明書ベンダから求められるものであり、Files Advanced の操作には必要ありません。

注意: ベンダーからサーバータイプを選択するよう求められた場合は、**IIS** を選択してください。証明書を Windows 証明書ストアにインストールして、Files Advanced が証明書を使用できるようにする必要があります。

IIS を介して証明書要求を作成する

この手順に関する詳細については、Microsoft のナレッジベースの記事（http://technet.microsoft.com/ja-jp/library/cc732906(v=ws.10).aspx)を参照してください。

OpenSSL を介して証明書要求を作成する

注意: このガイドでは、OpenSSL がインストールされている必要があります。

注意: この手順に関する詳細やサポートについては、希望する証明書ベンダにお問い合わせください。

ウェブサーバー「AAServer」用の秘密キーおよび公開 CSR（証明書署名要求)のペアを生成するには、次の手順を実行します。

1. 管理者特権でコマンドプロンプトを開き、次のコマンドを入力します。

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

このコマンドにより 2 つのファイルが作成されます。**myserver.key** のファイルには秘密キーが含まれています。このファイルは公開しないでください。秘密キーを紛失した場合、秘密キーのバックアップ以外にリカバリできる方法はないため、必ずバックアップを実行するようにしてください。**CSR（証明書署名要求)**を生成するには、秘密キーをコマンドの入力として使用します。

注意: 「**警告: 構成ファイル: /usr/local/ssl/openssl.cnf を開くことができません**」のようなエラーが表示された場合は、コマンド「**set OPENSSL_CONF=C:¥OpenSSL-Win64¥bin¥openssl.cfg**」を実行し、OpenSSL がインストールされている場所に応じて、パスを変更してください。この手順を完了した後に、最初の手順をもう一度実行してください。

2. CSR に登録される詳細情報を入力するように要求されます。ウェブ サーバーの名前を**コモンネーム（CN)**として使用します。ドメイン名が **mydomain.com** である場合は、そのドメイン名にホスト名を追加します（完全修飾ドメイン名を使用してください)。

3. ウェブサーバー証明書の場合、電子メールアドレス、任意の会社名、およびチャレンジパスワードのフィールドは空白にすることができます。
4. CSR が作成されました。証明書ベンダから要求された場合は、**server.csr** をテキストエディタで開き、内容をコピーしてオンライン登録フォームに貼り付けます。

要件

使用する証明書には証明書の秘密キーが含まれている必要があります。証明書ファイルは、**.PFX** または **.P12** のいずれかのファイル形式である必要があります。 これらは互換であるため、どちらを使用しても問題ありません。

注意: 証明書ベンダーから証明書とキーが 2 つの別々のファイルとして提供された場合、次のコマンドを使用して、それらのファイルを 1 つの **.PFX** ファイルに結合することができます。

openssl pkcs12 -export -in <yourcertificate.extension> -inkey <yourkey.extension> -out <newfile.pfx>

例: openssl pkcs12 -export -in acmecert.crt -inkey acmecertkey.key -out acmecombined.pfx

このコマンドを実行するには、OpenSSL がインストールされている必要があります。

Windows 証明書ストアへの証明書のインストール

注意: 使用している証明書が Files Advanced サーバーとゲートウェイサーバーで異なる場合は、両方の証明書に次の手順を行ってください。

---

1. サーバーで **[スタート]**、**[ファイル名を指定して実行]** の順にクリックします。
2. **[開く]** ボックスに「**mmc**」と入力し、**[OK]** をクリックします。
3. **[ファイル]** メニューの **[スナップインの追加と削除]** をクリックします。
4. **[スナップインの追加と削除]** ダイアログ ボックスで **[追加]** をクリックします。
5. **[スタンドアロン スナップインの追加]** ダイアログ ボックスで **[証明書]** をクリックしてから **[追加]** をクリックします。
6. **[証明書スナップイン]** ダイアログ ボックスで **[コンピュータ アカウント]** をクリックしてから（デフォルトでは選択されていません)**[次へ]** をクリックします。
7. **[コンピュータの選択]** ダイアログ ボックスで **[ローカル コンピュータ]**（このコンソールを実行しているコンピュータ)をクリックしてから **[完了]** をクリックします。

8. **[スタンドアロン スナップインの追加]** ダイアログ ボックスで **[閉じる]** をクリックします。
9. **[スナップインの追加と削除]** ダイアログ ボックスで **[OK]** をクリックします。
10. コンソールの左側のウィンドウで **[証明書 (ローカル コンピュータ)]** をダブルクリックします。
11. **[個人]** を右クリックして **[すべてのタスク]** をポイントし、**[インポート]** をクリックします。
12. **[証明書のインポート ウィザードの開始]** ページで **[次へ]** をクリックします。
13. **[インポートするファイル]** ページで **[参照]** をクリックし、証明書ファイルを探して **[次へ]** をクリックします。

    注意: PFX ファイルをインポートする場合は、ファイルフィルタを「**Personal Information Exchange（*.pfx, *.p12)**」に変更して、このファイルの種類を表示する必要があります。
14. 証明書にパスワードがある場合は、**[パスワード]** ページにパスワードを入力してから **[次へ]** をクリックします。
15. 以下のチェックボックスをオンにします。
    a. **このキーをエクスポート可能にする**
    b. **すべての拡張プロパティを含める**
16. **[証明書ストア]** ページで **[証明書をすべて次のストアに配置する]** をクリックし、**[次へ]** をクリックします。
17. **[完了]** をクリックしてから **[OK]** をクリックし、インポートが正常に実行されたことを確認します。

Files Advanced 設定ユーティリティを使用するとき、Windows 証明書ストアで正常にインストールされた証明書はすべて使用できます。

Windows 証明書ストアに証明書を正常にインストールしたら、その証明書を使用するように Files Advanced を設定する必要があります。

1. Files Advanced 設定ユーティリティを起動します。Windows の [スタート] メニューにショートカットがあるはずです。

注意: デフォルトでは、設定ユーティリティは **C:¥Program Files (x86)¥Acronis¥Access¥Configuration Utility** にあります。

2. **[ウェブサーバー]** タブで **[...]** ボタンを押して、リストから証明書を選択します。
3. **[モバイルゲートウェイ]** タブで **[...]** ボタンを押して、リストから証明書を選択します。
4. **[適用]** をクリックします。これにより、ウェブ サービスが再起動し、約 1 分後にはオンラインに戻って、選択した証明書が使用された状態になります。正しい証明書が使用されているかを確認できます。

証明機関により証明書と共に中間証明書が発行されている場合、設定ユーティリティで Files Advanced サーバーに追加する必要があります。

注意: 設定ユーティリティは**中間証明書**証明書ストア内のみを検索します。証明書が他のいずれかのストアにインストールされている場合は、**certmgr.msc** を開いて、中間証明書を今あるストアから **中間証明書認証局 -> 証明書**ストアに移動します。

1. Files Advanced 設定ユーティリティを起動します。Windows の [スタート] メニューにショートカットがあるはずです。

   注意: デフォルトでは、設定ユーティリティは **C:¥Program Files (x86)¥Acronis¥Access¥Configuration Utility** にあります。

2. **[ウェブサーバー]** タブで **[...]** ボタンを押して、リストから証明書を選択します。
3. **[チェーン証明書]** フィールドの横にあるプラス（**+**)ボタンを押して、使用する**中間証明書**をリストから選択します。希望する証明書がリストにない場合は、その証明書が正しくインストールされたか、およびどのストアにインストールされたかを確認してください。
4. **[モバイルゲートウェイ]** タブで **[...]** ボタンを押して、リストから証明書を選択します。中間証明書には、それ以上の追加の手順は必要ありません。
5. **[適用]** をクリックします。その後サービスが再起動するので、オンラインに戻ったら、選択した証明書が使用されているか確認できます。

12.2.9 複数のデスクトップクライアントバージョンのサポート

最新バージョンとは別のバージョンの Files Advanced デスクトップクライアントを使用する場合は、次の手順に従ってください。

1. 使用するバージョンのデスクトップクライアントをダウンロードします。次の 4 つのファイルがあることを確認します。
   - AcronisAccessMac.zip
   - AAClientInstaller.msi
   - AcronisAccessInstaller.dmg
   - AcronisAccessClientInstaller.exe
2. ファイルをコピーします。
3. サーバーで Files Advanced デスクトップクライアントフォルダ（**C:\Program Files (x86)\Acronis\Files Advanced\Access Server\Web Application\clients**)を開きます。
4. クライアントのこのバージョン用にサブフォルダを作成します。**2.7.0x167**、**2.6.0.x140**、**2.7.1x145** のように、**クライアントのバージョン番号**で名前を付けてください。
5. 作成したサブフォルダに 4 つのファイルを貼り付けます。
6. 次に、Files Advanced サーバーの**ウェブ ユーザー インターフェイス**を開きます。
7. **管理者**としてログインして [**同期・共有**] タブに移動し、[**Files Advanced クライアント**] ページを開きます。
8. **[クライアントの自動バージョン アップデートを許可]** 設定を探します。
9. ドロップダウン メニューから、目的のバージョンを選択します。

注意: アカウントの**操作メニュー**のダウンロード リンクでは、利用可能な最新の Files Advanced デスクトップ クライアント バージョンがダウンロードされます。ユーザーが最新バージョンをダウンロードしないようにするには、**¥Acronis¥Files Advanced¥Access Server¥Web Application¥clients** フォルダに移動し、最新のクライアント バージョン（**3.0.3x102** など)のフォルダ名を「**(バージョン番号)は使わない**」（「**3.0.3x102 は使わない**」など)に変更します。

12.2.10　デフォルト以外のロケーションへの FileStore の移動。

サービスがローカルシステムアカウントとして実行している

1. Files Advanced がインストールされているコンピュータに移動します。
2. **Files AdvancedFile Repository サーバー**と **Files Advanced Tomcat** サービスを停止します。
3. **構成ユーティリティ**で選択したフォルダに、現在の **FileStore** が見つかります。デフォルトのロケーションは、**C:\ProgramData\Acronis\Files Advanced\FileStore** です。
4. **FileStore** フォルダ全体をそのすべての内容とともに、希望するロケーションにコピーするか移動します。

   たとえば、**D:\MyCustom Folder\FileStore**　です。

   注意: ファイルストアがリモートネットワーク共有にある場合は、**ファイルリポジトリ**サービスが実行中であるコンピュータに、ネットワーク共有の**ファイルストア**フォルダに対する完全なアクセス権が必要です。
5. **設定ユーティリティ**を開きます。
6. **[ファイルリポジトリ]** タブで、**FileStore** フォルダを移動した新しいパスに **FileStore** のパスを変更します。
7. **Files Advanced File Repository サーバー**サービスを起動します。
8. **Files Advanced Tomcat** サービスを起動して、**[サービス]** コントロールパネルを閉じます。

サービスがユーザーアカウントとして実行している

1. Files Advanced がインストールされているコンピュータに移動します。
2. **Files AdvancedFile Repository サーバー**と **Files Advanced Tomcat** サービスを停止します。
3. **構成ユーティリティ**で選択したフォルダに、現在の **FileStore** が見つかります。デフォルトのロケーションは、**C:\ProgramData\Acronis\Files Advanced\FileStore** です。

4. **FileStore** フォルダ全体をそのすべての内容とともに、希望するロケーションにコピーするか移動します。

   たとえば、**`D:\MyCustom Folder\FileStore`** です。

5. **設定ユーティリティ**を開きます。
6. **[ファイルリポジトリ]** タブで、**FileStore** フォルダを移動した新しいパスに **FileStore** のパスを変更します。
7. **ファイルストア**がリモートネットワーク共有にある場合は、**ファイルリポジトリ**サービスが実行中であるユーザーアカウントに、ネットワーク共有の**ファイルストア**フォルダに対する完全なアクセス権が必要です。
8. このアカウントには、ログファイルを書き込むため、ローカル**リポジトリ**フォルダ（例えば、**`C:\Program Files (x86)\Acronis\Files Advanced\File Repository\Repository`**）への読み取り/書き込みアクセス権限も必要です。
9. **Files Advanced File Repository サーバー**サービスを起動します。
10. **Files Advanced Tomcat** サービスを起動して、**[サービス]** コントロールパネルを閉じます。

12.2.11 New Relic を使用した Files Advanced の監視

このインストール方法では、Files Advanced サーバー アプリケーションがインストールされている実際のコンピュータではなく、Files Advanced サーバー アプリケーションを監視できます。

1. http://newrelic.com/ http://newrelic.com/ を開き、New Relic アカウントを作成するか、既存のアカウントでログインします。上記の手順を完了すると、アプリケーションの設定画面に進みます。
2. アプリケーション タイプには **[APM]** を選択します。
3. プラットフォームには **[Ruby]** を選択します。
4. New Relic Starting Guide の手順 3 に示されている New Relic のスクリプト（newrelic.yml)をダウンロードします。
5. Files Advanced ウェブ コンソールを開きます。
6. **[設定]** → **[監視]** に移動します。

7. 拡張子も含めて、newrelic.yml へのパスを入力します（**C:\software\newrelic.yml** など)。Files Advanced フォルダ以外のフォルダにもこのファイルを保存して、アップグレード時やアンインストール時に削除や変更されないようにすることをお勧めします。
8. **[保存]** をクリックし、New Relic サイトで **[Active application(s)]** ボタンが有効になるまで数分間待機します。
9. 10 分以上経過したら、Files Advanced Tomcat サービスを再起動して数分待機します。これでボタンがアクティブになります。
10. New Relic ウェブサイトで Files Advanced サーバーを監視できます。

New Relic への接続や監視の設定に関して Files Advanced サーバーがログに記録するすべての情報は、**C:\Program Files (x86)\Acronis\Common\apache-tomcat-7.0.34\logs** にある **newrelic_agent.log** というファイルにあります。問題が発生した場合は、このログ ファイルで情報を検索できます。

頻繁に発生する警告やエラーは、次のように始まります。

警告: IP アドレスをキャッシュ中に DNS エラーが発生しました: Errno::ENOENT: このようなファイルまたはディレクトリはありません - C:/etc/hosts which

これは、New Relic の別のバグのパッチに使用されているコードの副次的な影響であり、問題はありません。

実際のコンピュータも監視する場合は、次の手順に従います

1. http://newrelic.com/ http://newrelic.com/ を開き、自分のアカウントでログインします。
2. [サーバー] を押し、オペレーティング システムに合った New Relic インストーラをダウンロードします。
3. New Relic モニタをサーバーにインストールします。
4. New Relic サーバー モニタには Microsoft .NET Framework 4 が必要です。New Relic インストーラのリンクは Microsoft .NET Framework 4 Client Profile 専用です。New Relic Server Monitor インストーラを実行する前に、Microsoft Download Center に移動してインターネットから .NET 4 Framework 全体をダウンロードしてインストールする必要があります。

5. New Relic がサーバーを検出するまで待機します。

12.2.12 複数のポートでの Files Advanced Tomcat の実行

設定ユーティリティがサポートする Tomcat サービスの設定は 1 つのポートだけに限られますが、Tomcat 自体は複数のポートで実行するように構成できます。それは、Tomcat の server.xml ファイルに追加のコネクタと希望するポートを追加することにより行うことができます。アップグレードや設定ユーティリティによる Tomcat サービスの再起動を行っても、新しいコネクタへの影響はありません。

注意: この構成は、すでに 1 回は設定ユーティリティを実行しており、Tomcat サービスが正常に開始した後に行うことをお勧めします。

追加のTomcatコネクタの構成

1. Files Advanced Tomcat サービスが実行中である場合は、このサービスを停止します。
2. **server.xml** ファイルを検索して開きます。デフォルトの場所は **C:\Program Files (x86)\Acronis\Files Advanced\Common\apache-tomcat-7.0.59\conf** です。

   注意: パスに含まれている番号（7.0.59)は、使用している Tomcat のバージョンによって異なります。

3. ファイルを参照して、次のような **Connector** セクションを探します。

```
<Connector maxHttpHeaderSize="65536" maxThreads="150"
enableLookups="false" disableUploadTimeout="true" acceptCount="100"
scheme="https" secure="true" SSLEnabled="true"
SSLProtocol="TLSv1+TLSv1.1+TLSv1.2" SSLCertificateFile="$
{catalina.base}/conf/AAServer_LocalHost.crt"
SSLCertificateKeyFile="${catalina.base}
/conf/AAServer_LocalHost.key" SSLHonorCipherOrder="true"
SSLCipherSuite="ECDH+AESGCM:ECDH+AES256:ECDH+AES128:RSA+AESGCM:RSA+AES:
!aNULL:!eNULL:!LOW:!3DES:!RC4:!MD5:!EXP:!PSK:!SRP:!DSS"
connectionTimeout="-1" URIEncoding="UTF-8" address="0.0.0.0" port="443"/>
```

   注意: 使用するテキストエディタによっては、**server.xml** を開いたときに、上記のコードが 1 行で表示される場合があります。

   注意: **設定ユーティリティ** で **443** 以外のポートを選択した場合は、上の例にある **Connector** セクションにそのポートがリストされます。

4. **Connector** セクション全体をコピーして、コピーを元のセクションの下に貼り付けてください。両方のセクションが同じレベルのインデントでなければなりません。
5. **443**（または**設定ユーティリティ**で選択したポート)を、Tomcat を起動させるために希望する 2 番目のポートに置き換えます。例:

```
<Connector maxHttpHeaderSize="65536" maxThreads="150"
enableLookups="false" disableUploadTimeout="true" acceptCount="100"
scheme="https" secure="true" SSLEnabled="true"
SSLProtocol="TLSv1+TLSv1.1+TLSv1.2" SSLCertificateFile="$
{catalina.base}/conf/AAServer_LocalHost.crt"
SSLCertificateKeyFile="${catalina.base}
/conf/AAServer_LocalHost.key" SSLHonorCipherOrder="true"
SSLCipherSuite="ECDH+AESGCM:ECDH+AES256:ECDH+AES128:RSA+AESGCM:RSA+AES:
!aNULL:!eNULL:!LOW:!3DES:!RC4:!MD5:!EXP:!PSK:!SRP:!DSS"
connectionTimeout="-1" URIEncoding="UTF-8" address="0.0.0.0"
port="4430"/>
```

注意: 新しい**Connector**のコードが既存のコードと同じように書かれていること、つまり古いコードが単一の行で書かれている場合は、新しい行も同じようになっていることを確認します。

6. Files Advanced ウェブインターフェイスを開き、**[全般設定]** → **[サーバー設定]** に移動します。
7. **[ウェブアドレス]** フィールドに指定されているアドレスに、Connector セクションに指定されているポートのいずれかが使用されていることを確認します。これは、ユーザーへの招待メールに表示されるアドレスで、それに選択できるポートは 1 つだけです。

12.2.13 Files Advanced のマルチホーム設定

Files Advanced ゲートウェイと Files Advanced サーバーのマルチホームは、設定ユーティリティを使用して簡単に設定できます。

必要となるのは、2 つの別々のネットワークインターフェイスと IP アドレスのみです。

マルチホームの設定

1. Files Advanced 設定ユーティリティを開きます。
2. **[ウェブサーバー]** タブを開き、1 つ目の IP アドレスと 443 ポートを入力します。
3. **[ゲートウェイサーバー]** タブを開き、2つ目のIPアドレスと443ポートを入力します。
4. **[OK]** を押します。

注意: Microsoft では、Windows Server 2008 で TCP/IP スタックの動作方法を完全に変更しました。単一の IP トランスポートで複数のレイヤがサポートされ、「プライマリ」IP アドレスはなくなりました。このため、単一インターフェイスに複数の IP アドレスを割り当てると、すべてのアドレスは均等に扱われて、すべて DNS に登録されます。言い換えると、この動作はバグではなくて設計によるものです。ただし、これについて何の対処も行わないと、使用する IP アドレスはラウンドロビン（DNS)になるため、この動作は問題の原因となります。

NIC でダイナミック DNS 登録を無効にしてホスト DNS エントリを手動で作成すると、この問題を回避できます。**KB975808（http://support.microsoft.com/?kbid=975808)**に記載されている修正プログラムをインストールして、簡単に回避することもできます。修正プログラムをインストールしたら、**netsh skipassource** フラグを使用できるようになります。新しいアドレスを追加しているときにこのフラグを使用すると、新しいアドレスを発信パケットに使用しないようにスタックに指示することになります。このため、これらの IP アドレスは DNS サーバーで登録されません。次の例を参考にしてください。

```
netsh int ipv4 add address "Local Area Connection" 192.168.1.2 skipassource=true
```

12.2.14 複数のウェブプレビューサーブレットのデプロイ

Files Advanced のウェブプレビュー機能を使用すれば、ファイル全体をダウンロードしなくてもファイルの内容を確認できます。ユーザーが多い場合には、パフォーマンスが低下することがあります。これに対処するために、ウェブプレビューサーブレットを使用して追加の Tomcat サーバーをセットアップできます。これにより、ウェブプレビューを処理し、メインの Files Advanced Advanced サーバーを支援できます。

負荷分散装置を一連の Tomcat サーバーの前方に配置して、ウェブプレビューサーブレットの負荷をさらに分散させることができます。プレビューリクエストにはどの状態も必要ないため、負荷分散装置の特別な構成は必要ありません。

セクションの内容

12.2.14.1 サーブレットのインストールと構成

Tomcat のインストール

Apache Tomcat 7 サーバーは、.zip ファイルからまたはインストール実行可能ファイルを使用してインストールできます。インストーラの使用をお勧めしますが、.zip アーカイブも機能します。唯一の違いは、Apache Tomcat 7 サーバーを設定する方法です。

両方のシナリオの要件:

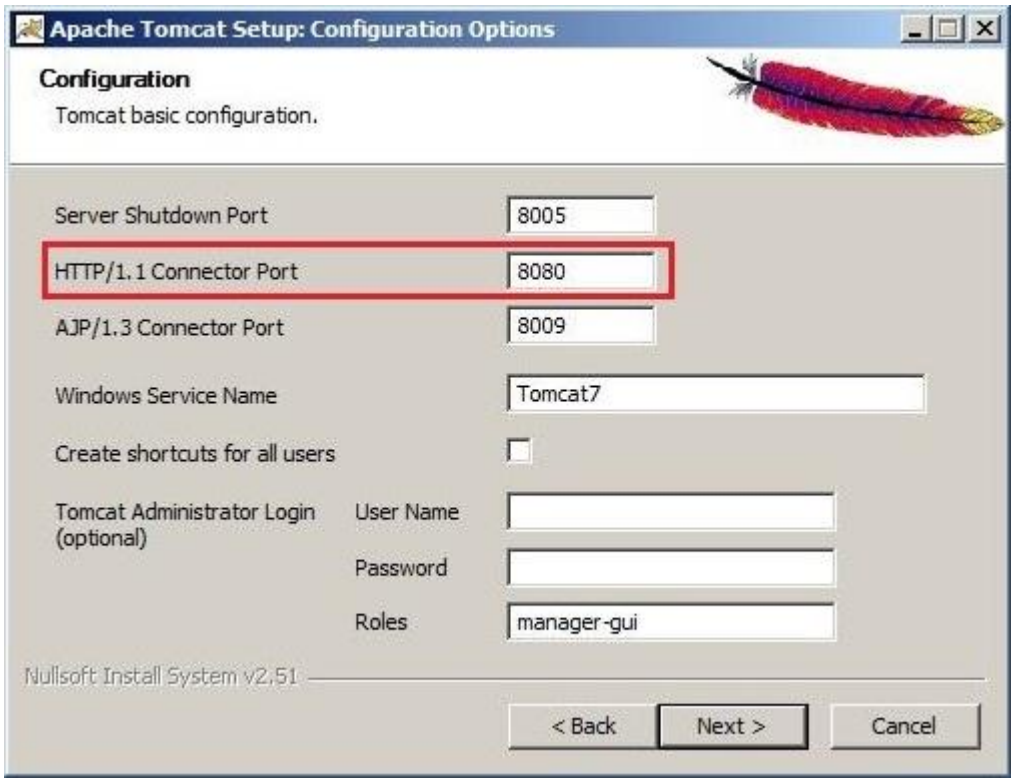
1. 64 ビットの Java Runtime Environment(JRE)がインストールされていることを確認します。64 ビットの Java Development Kit(JDK)でも問題ありません。Java はバージョン 8 以降を使用する必要があります。
2. 64 ビットバージョンの Apache Tomcat 7 をダウンロードします。Files Advanced でサポートされているものよりも新しいバージョンは使用しないでください。Files Advanced で使用されるバージョンは、新機能 『432ページ 』のセクションに記載されています。

セクションの内容

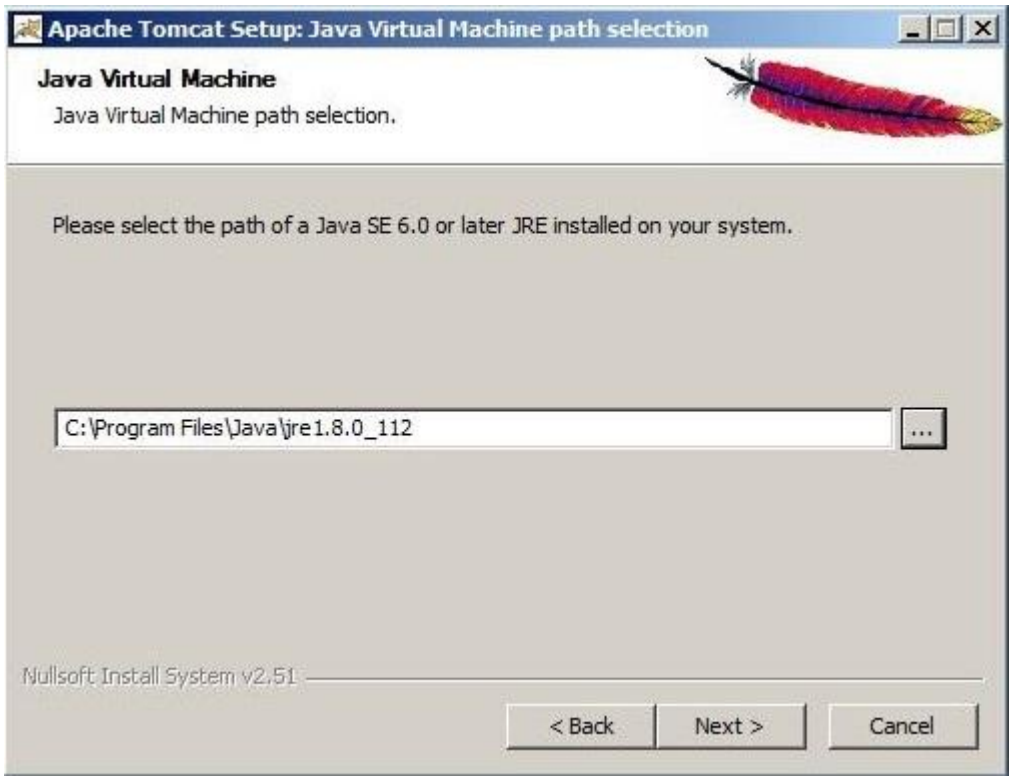
3.

1. 64 ビットバージョンの Apache Tomcat 7 を含むインストールファイルをダウンロードします。バージョンのリストは Apache Tomcat のサイトで見つかります。必要なバージョンを探してそれをクリックしてから、bin フォルダを開き、.exe ファイル（**apache-tomcat-7.0.50.exe** など)をダウンロードします。

2. インストーラを開始して、インストールウィザードの手順に従います。デフォルト設定のすべてを使用できます。必要に応じてリッスンポートを変更できます。デフォルトは 8080 です。



注意: インストーラが自動的に Java インストールフォルダを取得します。



3. インストールが完了したら、Files Advanced がインストールされているコンピュータ上で、Files Advanced のインストールフォルダ（デフォルトで **C:\Program Files (x86)\Acronis\Files Advanced\Access Server**)に移動します。
4. **AccessPreviewServlet** フォルダを Apache Tomcat がインストールされた新しいコンピュータにコピーして、Tomcat の **webapps** フォルダ（デフォルトで C:¥Program Files¥Apache Software Foundation¥Tomcat 7.0¥webapps)に貼り付けます。
5. Apache Tomcat インストールの **conf** フォルダ（デフォルトで C:¥Program Files¥Apache Software Foundation¥Tomcat 7.0¥conf)に移動し、**server.xml** ファイルをバックアップします。
6. このファイルを開いて、**<Host name="localhost" appBase="webapps" unpackWARs="true" autoDeploy="true">**行を探し、そのすぐ下に以下を追加します。

```
<!-- for Access Web preview -->
<Context path="/AccessPreviewServlet" docBase="C:\Program Files\Apache Software Foundation\Tomcat 7.0\webapps\AccessPreviewServlet">
</Context>
```

注意: デフォルト以外の場所に Apache Tomcat をインストールした場合は、インストールの正しいパスを反映するように **docBase=""**パスを編集する必要があります。

7. ファイルを保存して終了します。
8. Tomcat Service を開始するには。**[コントロール パネル]** -> **[管理ツール]** -> **[サービス]** を開いて、Apache Tomcat Service を開始します。

1. 64 ビットバージョンの Apache Tomcat 7 を含む**.zip** ファイルをダウンロードします。バージョンのリストは Apache Tomcat のサイトで見つかります。必要なバージョンを探してそれをクリックしてから、bin フォルダを開き、主要な.zip ファイル（**apache-tomcat-7.0.50.zip** など)をダウンロードします。
2. アーカイブの内容を **C:¥Program Files¥Apache Tomcat** などの好きな場所に展開します。
3. **C:¥Program Files¥Apache Tomcat¥apache-tomcat-<version>**に移動して、**bin** フォルダを開きます。

注意: 展開先のフォルダ名にはバージョン番号が含まれているため、**<version>**を Tomcat のバージョンで置き換え、**C:¥Program Files¥Apache Tomcat¥apache-tomcat-7.0.75**のようにします。

4. テキスト編集プログラムで **startup.bat** を開き、**setlocal** 行を探します。
5. その下に次の行を追加します。

   set "CATALINA_HOME=Your Tomcat Folder"

   e.g. set "CATALINA_HOME=C:\Program Files\Apache Tomcat\apache-tomcat-7.0.75"

   注意: これにより、すべての設定にデフォルトの Tomcat フォルダが設定されます。Apache Tomcat フォルダの適切なパスを使用します。

   set "JRE_HOME=Java main folder location"

   e.g. set "JRE_HOME=C:\Program Files\Java\jre1.8.0_112"

   注意: これにより、すべての設定にデフォルトの JRE フォルダが設定されます。Java フォルダの適切なパスを使用します。

   注意: JDKを使用している場合は、コマンドが**JRE_HOME**ではなく**JAVA_HOME**になります。
6. ファイルに加えた変更を保存します。
7. インストールが完了したら、Files Advanced がインストールされているコンピュータ上で、Files Advanced のインストールフォルダ（デフォルトで **C:\Program Files (x86)\Acronis\Files Advanced\Access Server**)に移動します。
8. **AccessPreviewServlet** フォルダを Apache Tomcat ををインストールした新しいコンピュータにコピーして、Tomcat の **webapps** フォルダ（デフォルトでは **C:\Program Files\Apache Tomcat\apache-tomcat-7.0.75\webapps** にあります)。
9. Apache Tomcat インストールの **conf** フォルダ（**C:¥Program Files¥Apache Tomcat¥apache-tomcat-7.0.75¥conf** など)に移動し、**server.xml** ファイルをバックアップします。
10. このファイルを開いて、**<Host name="localhost" appBase="webapps" unpackWARs="true" autoDeploy="true">**行を探し、そのすぐ下に以下を追加します。

    ```
    <!-- for Access Web preview -->
    <Context path="/AccessPreviewServlet" docBase="C:\Program Files\Apache Tomcat\apache-tomcat-7.0.75\webapps\AccessPreviewServlet">
    </Context>
    ```
11. 正しいインストールのパスを反映するように **docBase=""**パスを編集します。ファイルを保存して終了します。

    注意: サーバーがリッスンしているデフォルトポートを変更しなかった場合は、サーブレットは **8080** 上でリッスンします。ポート変更するには、**server.xml** ファイルで次の行を探します。

```
<Connector port="8080" protocol="HTTP/1.1"
           connectionTimeout="20000"
           redirectPort="8443" />
```

8080 を必要なポート番号に置き換えます。

12. Tomcat サービスを開始するには、bin フォルダに移動して、**startup.bat** ファイルをダブルクリックします。Tomcat の実行中は、黒色の DOS ウィンドウを開いたままにする必要があります。

12.2.14.2 Files Advanced サーバーの構成

1. Files Advanced ウェブインターフェイスを開き、**[全般設定]** -> **[ウェブのプレビュー]** を開きます。
2. **[ウェブプレビューのサービスにカスタム URL を使用]** を有効にし、新しいウェブプレビューサーブレットのアドレスを入力します(**例:** **http://accesswp.company.com:8080**)。指定した URL にポート番号が含まれている必要があります。負荷分散構成またはクラスタ構成を使用している場合、この URL にロードバランサのアドレスを入力します。
3. ウェブプレビューサーブレットを実行するようにセットアップしたサーバーの台数によっては、Files Advanced Server に設定する **[最大同時生成呼び出し数]** の値を増やす必要があります。
4. **[最大同時生成呼び出し数]** 設定を探して、それに適切な値を設定します。

   デフォルト値は 2 です。ドキュメントのレンダリングに 1 つのプロセッサコアの大部分が使用される可能性があります。レンダリングスレッドの数は、使用可能なプロセッサコアの 50%以下に設定する必要があります。この推奨値を超えた場合は、サーバー上の他のサービスのパフォーマンスが低下する可能性があります。

12.2.14.3 ウェブのプレビューサーブレットの負荷分散

[ウェブのプレビュー] サーブレットはロードバランサの背後に配置する必要があります。

1. 負荷分散装置で時間ベースのセッション スティッキネス（またはご使用の負荷分散装置での同等の設定)を有効にし、期限切れにならないように設定します。

2. ヘルスチェック（HTTP ステータス 200 が返されることを確認する)が必要な場合は、**http://servername.yourdomain.com:port/AccessPreviewServlet/generate_preview/**に ping を送信することで可能になります。

   例: **`https://servlet1.acme.com/AccessPreviewServlet/generate_preview`** および **`https://servlet2.acme.com/AccessPreviewServlet/generate_preview`**。

3. ブラウザでロードバランサのアドレスを開き、構成が機能していることを確認します。

   例: **`https://loadbalancer.yourdomain.com`**

12.2.15　PostgreSQL のストリーミングレプリケーション

このドキュメントの目的は、2 台の PostgreSQL サーバー間でストリーミングレプリケーションを構成する手順を詳細に説明することです。ストリーミングレプリケーションは、PostgreSQL データベースのオンライン状態を維持するために存在する多くの方法の 1 つです。その他の方法については、ここでは取り上げません。

注意: このドキュメントでは、PostgreSQL や Files Advanced のインストール処理については説明しません。ストリーミングレプリケーションの構成のみを説明します。

ストリーミングレプリケーション

ストリーミングレプリケーションは、ログ先行書き込み（WAL)セグメントに基づいています。WAL は、データの整合性を確認する標準的な方法です。WAL の基本的な概念とは、データファイル (テーブルおよびインデックスがおかれる場所)への変更は、必ずそれらの変更がログに記録された後（つまり、変更を記述したログレコードが永続的ストレージに書き込まれた後)に行われるということです。この手順に従えば、クラッシュが起きてもログを使用してデータベースを復元できるので、トランザクションのコミットのたびにデータページをディスクにフラッシュする必要はありません。データページに適用されなかったすべての変更は、ログレコードから再生できます。

WAL を使用すれば、ディスクへの書き込みが大幅に低減されます。ディスクにログファイルをフラッシュするだけでトランザクションのコミットを保証できるため、トランザクションで変更されたデータファイルをすべてフラッシュする必要がなくなります。ログファイルはシーケンシャル書き込みのため、ログファイルの同期のコストはデータページのフラッシュのコストよりもかなり低くなります。

WAL により、オンラインバックアップ、特定時点の復元とレプリケーションのサポートも可能になります。ストリーミングレプリケーションとは、レプリケーション接続で walsender プロトコルを使用し、プライマリサーバーとスタンバイサーバーの間の TCP/IP 接続を介して WAL レコードを継続的に送信することです。ストリーミングレプリケーションは同期も可能ですが、同期処理に必要なリソースおよびパフォーマンスへの影響を考えた結果、効果的なシナリオとして非同期ストリーミングレプリケーションのみを考慮することにしました。

要件:

- 2 台の PotsgreSQL サーバー: この手順内では、アクティブサーバーを「プライマリサーバー」と呼び、パッシブサーバーを「スタンバイサーバー」と呼びます。

  注意: **Files Advanced の接続には、プライマリサーバーしか使用できません。**スタンバイサーバーを使用できるのは、フェイルオーバーが発生し、スタンバイサーバーがプライマリに昇格した場合のみです。

- PostgreSQL 9.4: 「レプリケーションスロット」など、PostgreSQL 9.4 を必要とする機能を実装します。このバージョンは、実際に Acronis Access Advanced 7.2 に組み込まれており、新規インストールの場合にのみインストールされます（アップグレードの際はインストールされません)。
- 1 つの仮想 IP（任意): この仮想 IP は、Files Advanced サーバーの役割を実行するすべてのフロントエンドで使用され、常にアクティブホスト（プライマリサーバー)によって所有される必要があります。
- 事前に Files Advanced をインストールし、プライマリサーバーのデータベースを初期化しておくことをおすすめします。

セクションの内容

12.2.15.1 プライマリサーバー上

レプリケーションユーザーの作成

このユーザーは、レプリケーション処理で WAL をプライマリサーバーからスタンバイサーバーに送信する際に使用されます。セキュリティ上の理由から、デフォルトのスーパーユーザーアカウント（例: **postgres**)ではなく、レプリケーションのアクセス許可を持つ専用ユーザーを作成することをおすすめします。

1. プライマリサーバーで次のコマンドを実行します。

   psql -c "CREATE USER replicator REPLICATION LOGIN ENCRYPTED PASSWORD 'XXXXX';" -U postgres

   次のオプションを使用して、リモートからこのコマンドを実行することもできます。

   psql -c "CREATE USER replicator REPLICATION LOGIN ENCRYPTED PASSWORD 'XXXXX';" -h <IP_OF_PRIMARY_SERVER> -U postgres

   注意: PSQL は、PostgreSQL のインストールフォルダの **bin** サブフォルダ内にあります。PATH 環境変数によっては、コマンドの実行前に、コマンドへのパスの指定や、正しいディレクトリへの移動が必要になることがあります。この注意は、この手順で使用する以下のコマンドにも適用されます。

アクセス権の構成

プライマリサーバー上のアクセス制御を編集して、スタンバイサーバーからの接続を許可します。

1. そのためには、**pg_hba.conf** ファイル（**data** サブフォルダ内)を編集して、次の行を追加します。

   host replication replicator <hostssl replication replicator <スタンバイサーバーの IP>/32 md5>/32 trust

2. データベースサーバー間でより高いセキュリティが求められる場合には、認証の際にクライアントに暗号化パスワード（md5)を要求するか、SSL 暗号化（**hostssl**)のみを許可するか、またはその両方を設定することができます。例:

   host replication replicator <hostssl replication replicator <スタンバイサーバーの IP>/32 md5>/32 md5

hostssl replication replicator <hostssl replication replicator <スタンバイサーバーの IP>/32 md5>/32 md5

ストリーミングレプリケーションの構成

1. PostgreSQL のインストールフォルダに移動します。デフォルトでは、**C:\Program Files (x86)\Acronis\Access\Common\PostgreSQL\9.4** にあります。
2. **Data** フォルダに移動して、**postgresql.conf** ファイルを修正します。次の行を検索して編集します。

   注意: これらの行の前に#記号が付いていないことを確認してください。付いている場合、コマンドがコメントと見なされ、有効になりません。

   - **listen_address = 'プライマリサーバーの IP,** 127.0.0.1'
   - **wal_level = hot_standby**
   - **max_wal_senders = 3**
   - **checkpoint_segments = 8**
   - **wal_keep_segments = 8**
   - **max_replication_slots = 3**
3. 上記の変更を加えた後で、PostgreSQL サービスを再開します。

レプリケーションスロットの作成

1. プライマリサーバーで次のコマンドを実行します。

   ```
   psql -U postgres -c "SELECT * FROM
   pg_create_physical_replication_slot('access_slot');"
   ```
2. 次のコマンドを使用して、スロットが作成されていることを確認します。

   ```
   psql -U postgres -c "SELECT * FROM pg_replication_slots;"
   ```

12.2.15.2 スタンバイサーバー上

必要なすべてのサーバーの相互アクセスの確認

フェイルオーバーの際には、スタンバイサーバーがプライマリサーバーに昇格し、すべての Files Advanced サーバーのリクエストに応答します。

すべての Files Advanced サーバーのスタンバイサーバーに対するアクセスを今すぐ設定することをおすすめします。設定すると、フェイルオーバーの際にスタンバイサーバー上の PostgreSQL サービスの再起動が不要になります。

注意: スタンバイサーバーがスタンバイモードのときは、そのデータベースは読み取り専用モード(ホットスタンバイ)です。誤ってスタンバイサーバーが本番データベースとして設定され、使用されることはありません。

1. スタンバイサーバー上のアクセス制御を編集して、すべての Files Advanced サーバーからの接続を許可します。
2. そのためには、PostgreSQL のインストールフォルダに移動し、**pg_hba.conf** ファイル（**data** サブフォルダ内)を編集して、各サーバーについて次の行を追加します。

   ```
   host replication replicator <IP_OF_ACCESS_SERVER_1>/32 md5
   host replication replicator <IP_OF_ACCESS_SERVER_2>/32 md5
   ```

ストリーミングレプリケーションの構成

1. PostgreSQL のインストールフォルダに移動します。デフォルトでは、**C:\Program Files (x86)\Acronis\Access\Common\PostgreSQL\9.4** にあります。
2. **Data** フォルダに移動して、**postgresql.conf** ファイルを修正します。次の行を検索して編集します。

   注意: これらの行の前に**#**記号が付いていないことを確認してください。付いている場合、コマンドがコメントと見なされ、有効になりません。

   - **listen_address = 'スタンバイサーバーの IP,** 127.0.0.1'
   - **wal_level = hot_standby**
   - **max_wal_senders = 3**
   - **checkpoint_segments = 8**
   - **wal_keep_segments = 8**
   - **max_replication_slots = 3**
   - **hot_standby = on**

   hot_standby 設定では、ストリーミングレプリケーション中に接続してクエリを実行できるかどうかを指定できます。この設定を有効にすると、データベースは読み取り専用リクエストを受け入れるため、データベース参照が可能になります。そして、データベーステーブルの内容を参照してレプリケーション処理が動作していることを確認できます。

注意: **pg_hba.conf** で指定された認証方法として **md5** または **password** を使用する場合は、その接続のためにパスワードが必要になります。このパスワードを「入力」するには、スタンバイサーバーの **recovery.conf** ファイルに次のコマンドを追加する必要があります。

primary_conninfo = 'host=<プライマリサーバーの IP アドレス**> port=<**プライマリサーバーのポート**> user=<**ユーザー名**> password=<**ユーザー名のパスワード**>'**

たとえば、IP 10.0.0.1 のポート 5432 で、ユーザー**replicator** とパスワード **1234** で実行されている Postgres を探す場合には、 **primary_conninfo = 'host=10.0.0.1 port=5432 user=replicator password=1234'**となります。

3. **データベースの初期シーディングを実行してストリーミングレプリケーション処理を開始するには、プライマリサーバー上の PostgreSQL サービスを停止してください。**

構成ファイルのバックアップ

pg_hba.conf、**postgresql.conf**、**pg_ident.conf** を含むすべての**.conf** 構成ファイルのバックアップを作成します。これらのファイルは初期シーディングの処理で上書きされるため、この手順の後に復元する必要はありません。

dataディレクトリのクリーンアップ

data サブフォルダを削除（または単に名前を変更)します。フォルダの名前変更は、以前の構成のコピーを維持するには良い手段です。フォルダの名前変更により、初期シーディング中またはデータベースの起動時に問題が発生した場合に、スタンバイサーバーのデータベースを整合性のとれた状態に戻すことができます。

初期シーディング

初期シーディングは、プライマリデータベースのバックアップを使用して、スタンバイサーバー上のフォルダで行われます。

1. プライマリサーバーがアクティブで、使用中でないことを確認してください。Files Advanced Tomcat サービスをいったん停止し、シーディングが完了したら開始するのが最も簡単な方法です。

2. スタンバイサーバーレベルで初期シーディングを開始するには、次のコマンドを使用します。

   pg_basebackup.exe -h <IP_OF_PRIMARY_SERVER> -D <PATH_TO_NEW_DATA_DIR> -U replicator -v -P --xlog-method=stream

   注意: **<PATH_TO_NEW_DATA_DIR>** には名前変更済み、または削除済みの **Data** フォルダへのパス（**C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL\9.4\Data** など）を指定してください。

構成ファイルの復元

すべての**.conf** 構成ファイル（**pg_hba.conf**、**postgresql.conf**、**pg_ident.conf** を含む）を、バックアップフォルダから新しい **Data** フォルダにコピーして、既存のすべてのファイルを上書きします。

ストリーミングレプリケーションの制御

1. Data フォルダを開き、**recovery.conf** ファイルを作成（または修正)します。
2. まだ存在しない場合には次の行を追加します。
   - **standby_mode = 'on'**
   - **primary_conninfo = 'host=<プライマリサーバーの IP> port=5432 user=replicator password= <レプリケーションユーザー用に使用するパスワード>'**
   - **primary_slot_name = 'access_slot'**
   - **trigger_file = '<trigger_file = '<トリガーファイルのパス>' # As an example 'failover.trigger'>' # As an example 'failover.trigger'**
   - **recovery_min_apply_delay = 5min**
3. 上記の変更を加えた後に、スタンバイサーバー上で PostgreSQL サービスを開始します。

   注意: フェイルオーバーの場合、**recovery.conf** ファイルの名前が **recovery.done** に変更されます。

追加情報

- **standby_mode** 設定で、PostgreSQL サーバーをスタンバイとして開始する指定ができます。この場合、アーカイブされた WAL の末尾に達してもサーバーは復元を停止しません。**primary_conninfo** 設定（スタンバイサーバーからプライマリサーバーへの接続文字列)で指定されたプライマリサーバーに接続し、新しい WAL セグメントを取得して復元を継続しようとします。
- **primary_slot_name** 設定を使用して、プライマリサーバー上で以前のステップで作成されたレプリケーションスロットを使用します。
- **trigger_file** 設定は、トリガーファイル（存在するとスタンバイサーバーでの復元が終了してスタンバイサーバーがプライマリサーバーになる)を指定します。この設定はフェイルオーバーの処理中に使用されます。
- 任意で、**recovery_min_apply_delay** 設定も使用できます。デフォルトでは、スタンバイサーバーはプライマリサーバーから可能な限り早く WAL レコードを復元します。データの遅延コピーを使用すると、データ損失エラーを修正する機会が得られ、有用な場合があります。このパラメータを使用して、指定した期間復元を遅延できます。単位を指定しない場合、ミリ秒とみなされます。

  このパラメータに「5 min」を指定すると、プライマリサーバーからレポートされたコミット時刻がスタンバイサーバーのシステム時刻よりも 5 分以上過去のトランザクションである場合のみ、スタンバイサーバーによってトランザクションコミットが再発行されます。

  サーバー間のレプリケーション遅延がこのパラメータ値を超えている可能性もあります。そのような場合、遅延は追加されません。遅延は、プライマリサーバーで書き込まれた WAL タイムスタンプと、スタンバイサーバーの現在時刻で計算されることに注意してください。ネットワークラグやカスケードレプリケーション構成を原因とする転送遅延によって、実際の待機時間が大きく短縮されることがあります。プライマリサーバーとスタンバイサーバーのシステム時刻が同期していない場合には、復元時に予期するより早くレコードが適用される可能性があります。ただし、サーバー間の一般的な時刻差よりも、このパラメータで実用的とされる設定のほうがはるかに大きいため、大きな問題にはなりません。

12.2.15.3 フェイルオーバーのテスト

フェイルオーバーを本番のセットアップで実装する場合は、事前に上記の設定でテストを行い、フェイルオーバーが正常に機能することを確認することをおすすめします。

プライマリサーバーがダウンしていない場合は、先にプライマリサーバーを停止し、それから、プライマリサーバーの役割を引き継ぐようにスタンバイサーバーを設定する必要があります。これは、プライマリサーバーがクエリの処理を続けることで生じる問題の発生を回避するためです。

スタンバイサーバーをプライマリサーバーにするには、**recovery.conf** に記載されているトリガーファイルを作成します。プライマリサーバーの役割がスタンバイサーバーに引き継がれたら、Files Advanced サーバーがスタンバイサーバーを使用するように設定されていることを確認します。

> **注意:** フェイルオーバーのプロセスが起動されて正常に完了すると、**recovery.conf** ファイルの名前が **recovery.done** に変更されます。

この操作を行うには、**C:\Program Files (x86)\Acronis\Files Advanced\Access Server** に移動して **acronisaccess.cfg** を編集します。**DB_HOSTNAME** と **DB_PORT** が、現在プライマリサーバーになっている方の PostgreSQL サーバーのアドレスとポートを指していることを確認します。変更を加えた場合には、Files Advanced Tomcat サービスを再開する必要があります。

12.2.16 リモートアクセス用 PostgreSQL の構成

PostgreSQL の複数のインスタンスを管理する場合、またはデータベースを単にリモートで管理したい場合には、リモートアクセスが役立ちます。

このPostgreSQLインスタンスへのリモートアクセスを有効にするには、次の手順を実行してください。

1. PostgreSQL のインストールディレクトリ（**C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL\9.4\Data**）に移動します。
2. **pg_hba.conf** をテキストエディタで編集します。

3. リモートアクセスを有効にする各コンピュータのホストエントリを、内部アドレスを使用して組み込み、ファイルを保存します。**pg_hba.conf**（HBA はホストベース認証を表します)ファイルは、クライアント認証を制御するもので、データベースクラスタのデータディレクトリに保存されます。このファイルで、接続を許可するサーバーと権限を指定します。たとえば、次のように指定します。

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

4. 移動して、**postgresql.conf** を開きます。デフォルトの場所: **C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL\9.4\Data**
   a. 行「**#listen_addresses = 'localhost'**」を検索します。
   b. 行の先頭にある「**#**」記号を削除してコマンドを有効にします。
   c. 利用可能なアドレスすべてをリッスンするために、「**localhost**」を「*****」に置き換えます。PostgreSQL で特定のアドレスのみをリッスンするには、「*****」のかわりに IP アドレスを入力します。
      - **例 listen_addresses = '*'** : PostgreSQL が利用可能なアドレスすべてをリッスンします。
      - **例: listen_addresses = '192.168.1.1'** : PostgreSQL がこのアドレスのみをリッスンします。
5. **postgresql.conf** に加えた変更を保存します。
6. Files Advanced PostgreSQL サービスを再起動します。

注: PostgreSQL は、デフォルトでポート 5432 を使用します。使用するすべてのファイアウォールまたはルーティングソフトウェアでこのポートが開放されていることを確認してください。

12.2.17 HTTP モードでの Files Advanced の実行

Files Advanced と内部サービス（負荷分散ソリューションやプロキシソリューションなど)の間で暗号化されていない HTTP 通信を使用する必要がある場合に備えた設定が用意されています。セキュリティで保護されていないローカルネットワークやインターネットで通信

を行う Files Advanced サーバーは、常に HTTPS モードで動作する必要があります。内部で HTTP モードで動作していると、内部ネットワークにアクセス可能であれば、誰でも Files Advanced ネットワークトラフィックを簡単に見ることができるようになってしまいます。

HTTPS から HTTP に切り替えるには、次のファイルで一部の設定を変更する必要があります。

- Tomcat の **server.xml** ファイル（**C:\Program Files (x86)\Acronis\Files Advanced\Common\apache-tomcat-7.0.75\conf** にあります）。

  注意: Tomcat のバージョン番号は、使用中の Files Advanced のバージョンによって異なる場合があります。

- **acronisaccess.cfg** ファイル（**C:\Program Files (x86)\Acronis\Files Advanced\Access Server** にあります）。

server.xml ファイルの編集

このファイル内で、適切な HTTP コネクタを設定し、HTTPS コネクタを無効にする必要があります。

1. ファイルをテキストエディタで開き、既存の HTTPS コネクタを見つけます。以下のような内容になっているはずです。

   ```
   <Connector maxHttpHeaderSize="65536" maxThreads="150"
   enableLookups="false" disableUploadTimeout="true" acceptCount="100"
   scheme="https" secure="true" SSLEnabled="true"
   SSLProtocol="TLSv1+TLSv1.1+TLSv1.2"
   SSLCertificateFile="${catalina.base}/conf/AAServer_LocalHost.crt"
   SSLCertificateKeyFile="${catalina.base}/conf/AAServer_LocalHost.key"
   SSLHonorCipherOrder="true"
   SSLCipherSuite="ECDH+AESGCM:ECDH+AES256:ECDH+AES128:RSA+AESGCM:RSA+AES:
   !aNULL:!eNULL:!LOW:!3DES:!RC4:!MD5:!EXP:!PSK:!SRP:!DSS"
   connectionTimeout="-1" URIEncoding="UTF-8" bindOnInit="false" port="443"
   address="0.0.0.0"/>
   ```

2. HTTPS コネクタを無効にするために、**<!--** と **-->** で囲みます。つまり、**<Connector maxHttp.** の前に **<!--** を追加し、**-->** を **address="0.0.0.0"/>** の後ろに追加します。

3. 以下のような新しい HTTP コネクタを作成します。

```
<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. デフォルト以外のポートを選択することもできます。また、使用可能なすべてのアドレスがサービスに使用されないよう、接続用のアドレスを特定のアドレスに制限することもできます。
5. 使用するポートがファイアウォールで開かれていることを確認してください。
6. server.xml ファイルに、以下のリダイレクトコネクタが含まれているかどうかを確認します。

```
<!--  <Connector port="80" connectionTimeout="20000" protocol="HTTP/1.1"
redirectPort="443"/> -->
```

7. リダイレクトコネクタが含まれている場合、ポート 80 を使用するには、上述のように **<!-** と **->** を使用してコメント化することによって、リダイレクトコネクタを無効にします。
8. 必要な変更を行った後、ファイルを保存します。

acronisaccess.cfg の編集

このファイルで更新しなければならないのは、ファイルの末尾にある **REQUIRE_SSL** だけです。この設定を **true** から **false** に変更します。変更後は以下のようになります。

```
REQUIRE_SSL = false
```

1. 必要な変更を行った後、ファイルを保存します。
2. すべての変更が有効になるように、Files Advanced Tomcat サービスを再起動します。

HTTP モードの制限事項

- ゲートウェイは **HTTPS** で動作する必要があるため、**HTTP** モードではゲートウェイサーバーとの通信がサポートされません。ウェブ UI またはモバイルクライアントを介してネットワークノードにアクセスすることはできません。
- シングルサインオンはサポートされません。

- デスクトップクライアントを使用している場合、サーバーアドレスフィールドに手動で **HTTP** を指定する必要があります。このようにしなければ、接続が失敗します。例: **`http://myaccess.com:3000`**

12.2.18 Microsoft フェールオーバー クラスタ上での Files Advanced のアップグレード

Files Advanced Server クラスタを Files Advanced のさらに新しいバージョンにアップグレードするには、次のステップが役立ちます。

注意: アップグレードを実行する前に、「バックアップ 『200ページ 』」の記事を確認してから構成をバックアップしてください。

1. アクティブ ノードに移動します。
2. **[Cluster Administrator]/[フェイルオーバー クラスタ管理]** を開きます。
3. Files Advanced のサービスをすべて (**postgres-some-version** も含む)停止します。共有ディスクがオンラインでなければなりません。
4. インストールされているウイルス対策ソフトウェアをすべて無効にしてください。無効にしない場合は、インストール手順が中断され、インストールが失敗する可能性があります。
5. 実行可能なインストーラをダブルクリックします。
6. **[次へ]** を押して開始します。
7. 使用許諾契約を読み、承諾します。
8. **[アップグレード]** を押します。
9. インストールするコンポーネントを確認して、**[インストール]** をクリックします。
10. **postgres** スーパーユーザーのパスワードを入力して、**[次へ]** を押します。
11. インストールが終了したら、**[終了]** を押してインストーラを閉じます。

警告: クラスタグループをオンラインにしないでください。

12.クラスタ グループを第 2 ノードに移動します。

13.第 2 のノード上で、同じインストール手順を実行します。

14.Files Advanced のサービスをすべてオンラインにします。

12.2.19 Microsoft フェールオーバー クラスタ上での Files Advanced のインストール

警告: Files Advanced フェールオーバー クラスタリングは、5.0.3 より前のバージョンではサポートされていません。それより前のバージョンを使用している場合、何らかのクラスタの設定を続行する前に、5.0.3 以降のバージョンにアップグレードする必要があります。

Files Advanced をクラスタ上にインストールするには、以下のガイドが役立ちます。

セクションの内容

12.2.19.1 Windows 2008 (R2)Microsoft フェールオーバー クラスタ上での Files Advanced のインストール

Files Advanced のインストール

ドメイン管理者としてログインしていることを確認してから Files Advanced をインストールしてください。

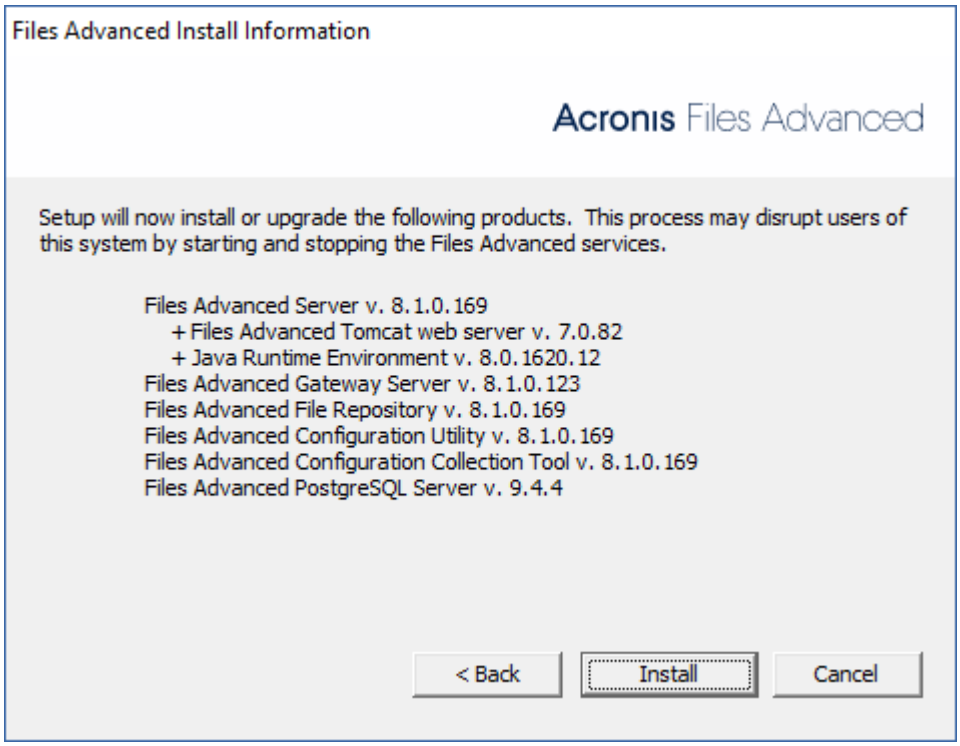
1. Files Advanced のインストーラをダウンロードします。
2. インストールされているウイルス対策ソフトウェアをすべて無効にしてください。無効にしない場合は、インストール手順が中断され、インストールが失敗する可能性があります。
3. 実行可能なインストーラをダブルクリックします。

4. **[次へ]** を押して開始します。

   使用許諾契約を読み、承諾します。
5. **[インストール]** を押します。

注意: 複数の Files Advanced サーバーを配置する場合や、標準構成以外でインストールを行う場合は、**[カスタム インストール]** ボタンからインストールするコンポーネントを選択することができます。

6. Files Advanced メインフォルダのデフォルトパスを使用するか新しいパスを選択し、[OK] を押します。



7. ユーザー Postgres のパスワードを設定し、書き留めておきます。このパスワードは、データベースのバックアップと復旧に必要となります。
8. 共有ディスクのうち **Postgres データ** フォルダのためのロケーションを選択して [**次へ**] をクリックします。
9. インストールされるコンポーネントがすべてリストされたウィンドウが表示されます。続行するには、**[OK]** を押します。

Files Advanced のインストーラが完了したら、[終了]**を押します。**

サービス グループの作成

1. [**フェールオーバー クラスタ マネージャ**] を開き、使用するクラスタを展開します。
2. [**サービスとアプリケーション**] を右クリックし、[**他の操作**] を選択します。

3. [**空のサービスまたはアプリケーションの作成**] を選択して [**次へ**] をクリックします。サービス グループに適切な名前を付けます。（Files Advanced、AAS クラスタなど)。

アクティブ ノードでの設定

1. ゲートウェイ サーバーのデータベースが共有ディスク上のロケーションとなるように設定します。
   a. **C:\Program Files (x86)\Acronis\Access\Gateway Server** に移動します。
   b. **database.yml** ファイルを見つけ、テキスト エディタで開きます。
   c. **database_path: './database/'** の行を見つけ、**./database/** を、使用するパスに置き換えます（例: **database_path: 'S:/access_cluster/database/'**)。

   注意: パスの区切りにはスラッシュ（/)を使用します。

   注意: 第 1 ノードで設定した database.yml をコピーして、第 2 ノードに貼り付けることができます。

必要なすべてのサービスを Files Advanced サービス グループに追加する

AcronisAccessGateway、AcronisAccessPostgreSQL（Files Advanced のバージョンに応じて異なる)、AcronisAccessRepository、および AcronisAccessTomcat の各サービスについて、以下の手順を実行します。

1. Files Advanced サービス グループを右クリックして、[**リソースの追加**] を選択します。
2. [**汎用サービス**] を選択します。
3. 適切なサービスを選択して [**次へ**] をクリックします。
4. 確認ウィンドウで [**次へ**] をクリックします。
5. **[レジストリ設定のレプリケート]** ウィンドウで **[次へ]** をクリックします。
6. 概要ウィンドウで [**完了**] をクリックします。

クライアント アクセス ポイントの設定

1. Files Advanced サービス グループを右クリックして、[**リソースの追加**] を選択します。
2. [**クライアント アクセス ポイント**] を選択します。

3. このアクセス ポイントの名前を入力します。
4. ネットワークを選択します。

5. IP アドレスを入力して [**次へ**] をクリックします。
6. 確認ウィンドウで [**次へ**] をクリックします。
7. 概要ウィンドウで [**完了**] をクリックします。

共有ディスクの追加

1. Files Advanced のサービス グループを右クリックして、**[ストレージの追加]** を選択します。
2. 目的の共有ドライブを選択します。

3. 確認ウィンドウで [**次へ**] をクリックします。
4. 概要ウィンドウで [**完了**] をクリックします。

依存関係の設定

1. Files Advanced サービス グループをダブルクリックします。

PostgreSQL および Files Advanced ファイル リポジトリ サービスについて、次の操作を実行します。

1. 適切なサービスを右クリックし、[**プロパティ**] を選択します。
2. [**依存関係**] タブをクリックします。
3. [**リソース**] をクリックし、追加した共有ディスクを選択します。

4. [**適用**] をクリックしてウィンドウを閉じます。

PostgreSQL では、次の操作も実行します。

1. **[レジストリ レプリケーション]** タブをクリックします。
2. **[追加]** を押し、
   SYSTEM\CurrentControlSet\Services\AcronisAccessPostgreSQL のように入力します（旧バージョンの Files Advanced の場合、サービスが **postgresql-x64-9.2** のように異なることがあります)。

Files Advanced ゲートウェイ サーバー サービスでは、次の操作を実行します。

1. 適切なサービスを右クリックし、[**プロパティ**] を選択します。
2. [**依存関係**] タブをクリックします。
3. [**リソース**] をクリックしてから、追加した共有ディスク、および**ネットワーク名**（クライアント アクセス ポイントの名前)を選択します。

4. [**適用**] をクリックしてウィンドウを閉じます。

Files Advanced Tomcat サービスでは、次の操作を実行します。

1. 適切なサービスを右クリックし、[**プロパティ**] を選択します。
2. [**依存関係**] タブをクリックします。
3. [**リソース**] をクリックし、依存関係として、PostgreSQL および Files Advanced ゲートウェイ サーバーのサービスを選択します。[**適用**] をクリックしてウィンドウを閉じます。

注意: ゲートウェイ サーバーと Access サーバーを異なる IP アドレスで実行する場合は、Files Advanced サービス グループに第 2 IP をリソースとして追加し、ネットワーク名の依存関係として設定します。

サービス グループをオンラインにし、設定ユーティリティを使用する

1. Files Advanced サービス グループを右クリックし、**[Bring this application or service group online]** を押します。

2. 設定ユーティリティを起動します。クリーン インストールの場合、通常このユーティリティは **C:\Program Files (x86)\Acronis\Access\Configuration Utility** にあります。
3. Files Advanced ゲートウェイ サーバー サービスが、IP アドレス上で Files Advanced サービス グループをリッスンするように設定します。
4. Files Advanced サーバー サービスが、IP アドレス上で Files Advanced サービス グループをリッスンするように設定します。

   注意: [ポート 80 での接続を許可します] が選択されている場合、Tomcat は、セキュアでないポート 80 で着信トラフィックをリッスンし、それを上記で指定された HTTPS ポートにリダイレクトします。ポート 80 上でリッスンする別のプログラムがある場合は、このボックスをオンにしないでください。
5. Files Advanced ファイル リポジトリが localhost 上でリッスンするように設定し、FileStore へのパスが共有ディスク上になるように変更します。このパスは、2 つのノードで同じにする必要があります。
6. **[OK]** をクリックすると、設定が完了し、サービスが再起動します。

第 2 ノードでのインストールおよび設定

1. インストールされているウイルス対策ソフトウェアをすべて無効にしてください。無効にしない場合は、インストール手順が中断され、インストールが失敗する可能性があります。
2. 第 2 ノードに Files Advanced をインストールします。ただし、今回は、デフォルトの **Postgres データ** ロケーション、および第 1 ノードと同じ postgres ユーザー パスワードを使用します。
3. インストールを実行します。
4. ゲートウェイ サーバーのデータベースが共有ディスク上のロケーションとなるように設定します。
   a. **C:\Program Files (x86)\Acronis\Access\Gateway Server** に移動します。

b. **database.yml** ファイルを見つけ、テキスト エディタで開きます。

c. **database_path: './database/'** の行を見つけ、**./database/** を、使用するパスに置き換えます（例: **database_path: 'S:/access_cluster/database/'**）。

注意: パスの区切りにはスラッシュ（/)を使用します。

注意: 第 1 ノードで設定した database.yml をコピーして、第 2 ノードに貼り付けることができます。

注意: このパスは第 1 ノードで設定されているパスと同じでなければなりません。

5. Files Advanced サービス グループを第 2 ノードに移動します。そのためには、そのサービス グループを右クリックして [**第 2 ノードに移動**] をクリックします。
6. 設定ユーティリティを起動します。クリーン インストールの場合、通常このユーティリティは **C:\Program Files (x86)\Acronis\Access\Configuration Utility** にあります。
7. Files Advanced ゲートウェイ サーバー サービスが、IP アドレス上で Files Advanced サービス グループをリッスンするように設定します。
8. Files Advanced サーバー サービスが、IP アドレス上で Files Advanced サービス グループをリッスンするように設定します。

注意: [ポート 80 での接続を許可します] が選択されている場合、Tomcat は、セキュアでないポート 80 で着信トラフィックをリッスンし、それを上記で指定された HTTPS ポートにリダイレクトします。ポート 80 上でリッスンする別のプログラムがある場合は、このボックスをオンにしないでください。

9. Files Advanced ファイル リポジトリが localhost 上でリッスンするように設定し、FileStore へのパスが共有ディスク上になるように変更します。このパスは、2 つのノードで同じにする必要があります。
10. **[OK]** をクリックすると、設定が完了し、サービスが再起動します。

12.2.19.2 Windows 2012 (R2)Microsoft フェールオーバー クラスタ上での Files Advanced のインストール

Files Advanced のインストール

ドメイン管理者としてログインしていることを確認してから Files Advanced をインストールしてください。

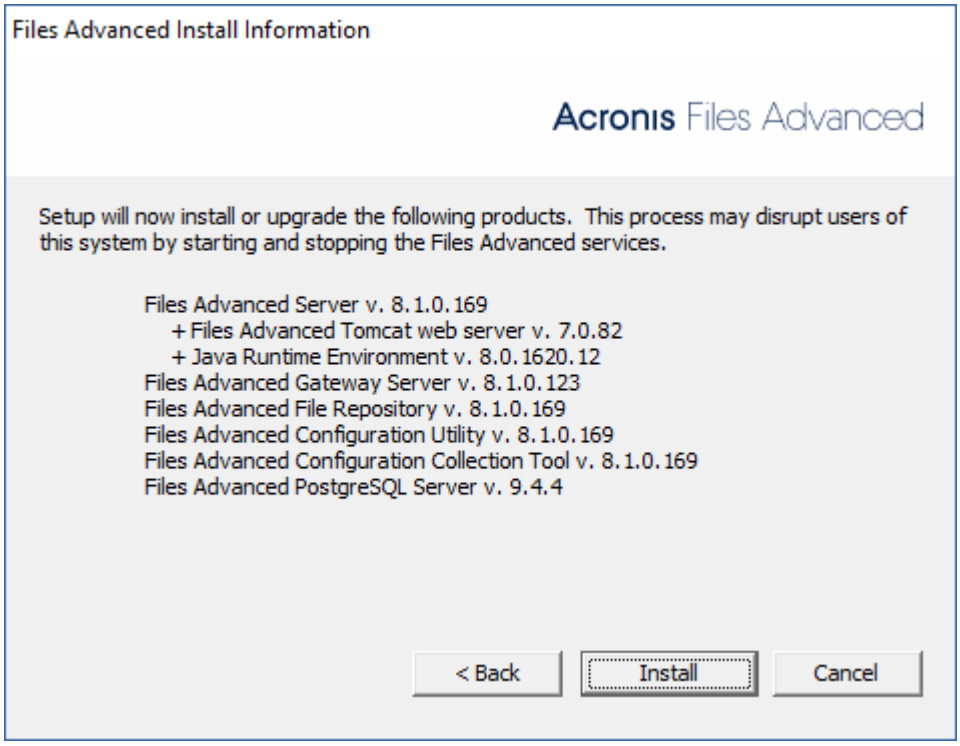
1. Files Advanced のインストーラをダウンロードします。
2. インストールされているウイルス対策ソフトウェアをすべて無効にしてください。無効にしない場合は、インストール手順が中断され、インストールが失敗する可能性があります。
3. 実行可能なインストーラをダブルクリックします。

4. **[次へ]** を押して開始します。

   使用許諾契約を読み、承諾します。
5. **[インストール]** を押します。

注意: 複数の Files Advanced サーバーを配置する場合や、標準構成以外でインストールを行う場合は、**[カスタム インストール]** ボタンからインストールするコンポーネントを選択することができます。

6. Files Advanced メインフォルダのデフォルトパスを使用するか新しいパスを選択し、[OK] を押します。



7. ユーザー Postgres のパスワードを設定し、書き留めておきます。このパスワードは、データベースのバックアップと復旧に必要となります。
8. 共有ディスクのうち **Postgres データ** フォルダのためのロケーションを選択して [**次へ**] をクリックします。
9. インストールされるコンポーネントがすべてリストされたウィンドウが表示されます。続行するには、**[OK]** を押します。

Files Advanced のインストーラが完了したら、**[終了]** を押します。

役割の作成

1. [**フェールオーバー クラスタ マネージャ**] を開き、[**役割**] を右クリックします。
2. [**空の役割の作成**] を選択します。役割に適切な名前を付けます（Files Advanced、AAS クラスタなど)。

アクティブ ノードでの設定

1. ゲートウェイ サーバーのデータベースが共有ディスク上のロケーションとなるように設定します。
   a. **C:\Program Files (x86)\Acronis\Access\Gateway Server** に移動します。
   b. **database.yml** ファイルを見つけ、テキスト エディタで開きます。
   c. **database_path: './database/'** の行を見つけ、**./database/** を、使用するパスに置き換えます（例: **database_path: 'S:/access_cluster/database/'**）。

   注意: パスの区切りにはスラッシュ（/)を使用します。

   注意: 第 1 ノードで設定した database.yml をコピーして、第 2 ノードに貼り付けることができます。

必要なすべてのサービスを Files Advanced 役割に追加する

AcronisAccessGateway、AcronisAccessPostgreSQL（Files Advanced のバージョンに応じて異なる)、AcronisAccessRepository、および AcronisAccessTomcat の各サービスについて、以下の手順を実行します。

1. Files Advanced 役割を右クリックして、[**リソースの追加**] を選択します。
2. [**汎用サービス**] を選択します。
3. 適切なサービスを選択して [**次へ**] をクリックします。
4. 確認ウィンドウで [**次へ**] をクリックします。
5. 概要ウィンドウで [**完了**] をクリックします。

アクセス ポイントの設定

1. Files Advanced 役割を右クリックして、[**リソースの追加**] を選択します。
2. [**クライアント アクセス ポイント**] を選択します。
3. このアクセス ポイントの名前を入力します。

4. ネットワークを選択します。

5. IP アドレスを入力して [**次へ**] をクリックします。
6. 確認ウィンドウで [**次へ**] をクリックします。
7. 概要ウィンドウで [**完了**] をクリックします。

共有ディスクの追加

1. Files Advanced 役割を右クリックして、[**ストレージの追加**] を選択します。
2. 共有ドライブを選択します。

依存関係の設定

1. Files Advanced の役割を選択し、[**リソース**] タブをクリックします。

PostgreSQL および Files Advanced ファイル リポジトリ サービスについて、次の操作を実行します。

1. 適切なサービスを右クリックし、[**プロパティ**] を選択します。
2. [**依存関係**] タブをクリックします。
3. [**リソース**] をクリックし、追加した共有ディスクを選択します。

4. [**適用**] をクリックしてウィンドウを閉じます。

Files Advanced ゲートウェイ サーバー サービスについて、次のことを実行します。

1. 適切なサービスを右クリックし、[**プロパティ**] を選択します。
2. [**依存関係**] タブをクリックします。
3. [**リソース**] をクリックしてから、追加した共有ディスク、および**ネットワーク名**（クライアント アクセス ポイントの名前)を選択します。

4. [**適用**] をクリックしてウィンドウを閉じます。

Files Advanced Tomcat サービスについて、次のことを実行します。

1. 適切なサービスを右クリックし、[**プロパティ**] を選択します。
2. [**依存関係**] タブをクリックします。
3. [**リソース**] をクリックし、依存関係として、PostgreSQL および Files Advanced ゲートウェイ サーバーのサービスを選択します。[**適用**] をクリックしてウィンドウを閉じます。

注意: ゲートウェイ サーバーとアクセス サーバーを異なる IP アドレスで実行する場合は、第 2 IP をリソースとして Files Advanced 役割に追加し、それをネットワーク名の依存関係として設定します。

役割の開始と設定ユーティリティの使用

1. Files Advanced 役割を右クリックして、[**役割の開始**] を押します。
2. 設定ユーティリティを起動します。クリーン インストールの場合、通常このユーティリティは **C:\Program Files (x86)\Acronis\Access\Configuration Utility** にあります。
3. Files Advanced ゲートウェイ サーバー サービスが、IP アドレス上で Files Advanced サービス グループをリッスンするように設定します。

4. Files Advanced サーバー サービスが、IP アドレス上で Files Advanced サービス グループをリッスンするように設定します。

注意: [ポート 80 での接続を許可します] が選択されている場合、Tomcat は、セキュアでないポート 80 で着信トラフィックをリッスンし、それを上記で指定された HTTPS ポートにリダイレクトします。ポート 80 上でリッスンする別のプログラムがある場合は、このボックスをオンにしないでください。

5. Files Advanced ファイル リポジトリが localhost 上でリッスンするように設定し、FileStore へのパスが共有ディスク上になるように変更します。このパスは、2 つのノードで同じにする必要があります。

6. **[OK]** をクリックすると、設定が完了し、サービスが再起動します。

第 2 ノードでのインストールおよび設定

1. インストールされているウイルス対策ソフトウェアをすべて無効にしてください。無効にしない場合は、インストール手順が中断され、インストールが失敗する可能性があります。
2. 第 2 ノードに Files Advanced をインストールします。ただし、今回は、デフォルトの **Postgres データ** ロケーション、および第 1 ノードと同じ postgres ユーザー パスワードを使用します。
3. インストールを実行します。
4. ゲートウェイ サーバーのデータベースが共有ディスク上のロケーションとなるように設定します。
   a. **C:\Program Files (x86)\Acronis\Access\Gateway Server** に移動します。
   b. **database.yml** ファイルを見つけ、テキスト エディタで開きます。
   c. **database_path: './database/'** の行を見つけ、**./database/** を、使用するパスに置き換えます（例: **database_path: 'S:/access_cluster/database/'**）。

   注意: パスの区切りにはスラッシュ（/)を使用します。

   注意: 第 1 ノードで設定した database.yml をコピーして、第 2 ノードに貼り付けることができます。

   注意: このパスは第 1 ノードで設定されているパスと同じでなければなりません。

PostgreSQL では、次の操作を実行します。

1. **[フェイルオーバークラスタ管理]** を開きます。
2. PostgreSQL 汎用サービスリソースを探して選択します。
3. アカウントを右クリックして、**[プロパティ]** を選択します。
4. **[レジストリ レプリケーション]** タブをクリックします。
5. **[追加]** を押し、**SYSTEM\CurrentControlSet\Services\AcronisAccessPostgreSQL** のように入力し

ます（旧バージョンの Files Advanced の場合、サービスが **postgresql-x64-9.2** のように異なることがあります)。

6. Files Advanced 役割を第 2 ノードに移動します。

第 2 ノードの設定ユーティリティの使用

1. 設定ユーティリティを起動します。クリーン インストールの場合、通常このユーティリティは **C:\Program Files (x86)\Acronis\Access\Configuration Utility** にあります。
2. Files Advanced ゲートウェイ サーバー サービスが、IP アドレス上で Files Advanced サービス グループをリッスンするように設定します。

3. Files Advanced サーバー サービスが、IP アドレス上で Files Advanced サービス グループをリッスンするように設定します。

   注意: [ポート 80 での接続を許可します] が選択されている場合、Tomcat は、セキュアでないポート 80 で着信トラフィックをリッスンし、それを上記で指定された HTTPS ポートにリダイレクトします。ポート 80 上でリッスンする別のプログラムがある場合は、このボックスをオンにしないでください。

4. Files Advanced ファイル リポジトリが localhost 上でリッスンするように設定し、FileStore へのパスが共有ディスク上になるように変更します。このパスは、2 つのノードで同じにする必要があります。

5. **[OK]** をクリックすると、設定が完了し、サービスが再起動します。

12.3 モバイルクライアントの場合

セクションの内容

12.3.1 iOS 管理対象アプリケーションの設定機能の使用

Files Advanced モバイルでは、iOS 7 の管理対象アプリの設定機能がサポートされています。以下に示されている要件を満たしている場合は、MDM 構成に特定のキーを追加することで、Files Advanced モバイルに適用することができます。

- デバイスは MDM サーバーで管理されている必要があります。
- Files Advanced アプリケーション バイナリが MDM サーバーによってデバイス上にインストールされている必要があります。
- MDM サーバーで、**ApplicationConfiguration** 設定、および **ManagedApplicationFeedback** コマンドがサポートされている必要があります。

次のキーの使用がサポートされています。

- **enrollmentServer**: このキーの値は、ユーザーが登録する Files Advanced サーバーの DNS アドレスに設定する必要があります。
- **enrollmentPIN**: このキーは任意指定です。Files Advanced サーバーがクライアント登録に PIN コードを要求する場合は、Files Advanced 登録フォームの PIN コード フィールドにこの値を自動入力できます。この PIN 要件は、**Files Advanced** ウェブ コンソールの **[設定]** ページ 『143ページ 』で設定します。
- **userName**：このキーは任意指定です。このキーの値は、Files Advanced 登録フォームの [ユーザー名] フィールドに挿入されます。変数を使用すると、特定ユーザーのユーザー名でこの値を自動入力できます。

plistファイルの作成

plist はアプリケーションデータ保存用のフォーマットです。元は Apple が iPhone デバイスでの使用のために定義したものですが、今では他のアプリケーションでも使用されています。plist は実際には XML ファイルであるため、一般的なテキストエディタを使用して作成、編集できます。

plist ファイルの作成

1. 任意のテキストエディタを起動します。
2. 次のとおり入力します。

```
<?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>
         ご希望のキーをここに入力します
   </dict>
</plist>
```

例:

```
<dict>
   <key>enrollmentServer</key>
   <string>server.example.com</string>
   <key>userName</key>
   <string>username</string>
      <key>enrollmentPIN</key>
      <string>11Y9KL</string>
</dict>
```

3. **plist.xml** という名前でファイルを保存します。

MobileIronへのplistファイルのアップロード

1. MobileIron 管理ポータルを開きます。
2. **[ポリシーと設定]** → **[設定]** → **[新規追加]** → **[iOS と OS X]** → **[管理対象アプリケーションの設定]** の順に移動し、plist ファイルをアップロードします。

Microsoft Intuneへのplistファイルのアップロード

注意: 詳細については、この件に関する Microsoft Intune のドキュメントを参照してください。

1. Microsoft Intune 管理コンソールで、**[ポリシー]** > **[概要]** > **[ポリシーの追加]** と選択します。

2. ポリシーリストで、**[iOS]** を展開し、**[モバイルアプリ構成]**、**[ポリシーを作成する]** の順に選択します。
   - **[ポリシーを作成する]** ページの [全般] セクションで、モバイルアプリ構成ポリシーの名前と説明（オプション)を指定します。
   - ページの [モバイルアプリ構成ポリシー] セクションにあるボックスに、アプリ構成設定が含まれる XML プロパティリストを入力または貼り付けます。
3. [検証] をクリックし、入力したXMLのプロパティリスト形式が有効であることを確認します。
4. 完了後、**[ポリシーの保存]** をクリックします。

12.3.2 MobileIron AppConnect のサポート

セクションの内容

12.3.2.1 はじめに

Acronis と MobileIron が提携し、Files Advanced のモバイル ファイル管理が MobileIron AppConnect プラットフォームにもたらされました。この Files Advanced の機能により、AppConnect で定義したポリシーを使って、標準的な Mobile アプリ、およびその他の AppConnect 対応アプリをオプションで自動構成および管理することができます。また、Files Advanced では、MobileIron AppTunnel により、企業データセンター内にある Files Advanced ゲートウェイサーバーへのリモートアクセスがサポートされます。

Files Advanced with MobileIron AppConnect のコンポーネントは次のとおりです。

- **MobileIron Virtual Smartphone プラットフォーム(VSP)**: 企業が AppConnect 対応アプリケーションへのクライアント アクセスを有効にしたり、このようなアプリケーションを自動構成したり、アプリケーションの機能を規定するポリシーを作成したり、特定のデバイスで AppConnect 対応アプリケーションへのアクセスを無効にするか AppConnect 対応アプリケーションをワイプしたりできるようにするサーバーベース コンソール。
- **MobileIron Sentry**: Files Advanced ゲートウェイ サーバーなどの社内アプリケーション サーバーとの通信に必要となる、AppConnect 対応アプリケーションのネットワーク アクセスを提供するには、このサービスを使用します。
- **MobileIron Mobile@Work アプリケーション**: このアプリケーションは、AppConnect 対応アプリケーションの認証と構成を橋渡しします。AppConnect 対応アプリケーションを構成して管理する前に、モバイル デバイスにインストールする必要があります。
- **Files Advanced iOS アプリケーション**: Files Advanced for iOS の標準バージョン（バージョン 5.0 以降)であり、Apple App Store で利用できます。AppConnect で構成して管理し、AppTunnel で Files Advanced ゲートウェイ サーバーと通信できます。
- **Files Advanced Android アプリ** - 特別な MobileIron 版のアプリが必要です。http://support.grouplogic.com/?page_id=4566 からダウンロードできます。このバージョンのアプリを **Apps@Work** ストアに追加する必要があります。
- **Files Advanced サーバー**: Files Advanced サーバーの標準バージョン（バージョン 5.0 以降)には、AppConnect によって管理される Access Mobile Client との完全な互換性があります。

12.3.2.2 試用版の Files Advanced と AppConnect のテスト

Files Advanced with AppConnect の試用プロセスは、標準の Files Advanced の試用とまったく同じです。

1. サーバー側ソフトウェアの試用版は、試用版ページにアクセスして要求できます。この要求フォームを送信すると、Files Advanced サーバー試用版のインストーラをダウンロードするリンクと、初期設定時に参照すると便利な『mobilEcho クイック スタート ガイド』へのリンクが記載された電子メールが届きます。

2. Files Advanced iOS クライアント アプリケーションは、Apple App Store http://www.grouplogic.com/web/meappstore から無償でダウンロードできます。
3. Files Advanced Android アプリは弊社サポートサイト http://support.grouplogic.com/?page_id=4566 のいずれかから無償でダウンロードできます。
4. Files Advanced ゲートウェイサーバーにアクセスするように Files Advanced モバイルアプリを自動設定するには、Files Advanced モバイルアプリに MobileIron Virtual Smartphone platform（VSP)で作成された AppConnect の構成とポリシーが存在している必要があります。
5. また、AppConnect 対応アプリをアクティブ化したり、Files Advanced アプリをインストールしたりするには、モバイルデバイスに MobileIron Mobile@Work アプリがインストールされている必要があります。Mobile@Work は、Apple App Store および Google Play ストアの両方から無償でダウンロードできます。
6. AppConnect 対応 Files Advanced モバイルクライアントをアクティブ化する準備ができたら、このドキュメントの次のセクションに進んでください。

12.3.2.3 Files Advanced Android クライアントと MobileIron の統合

1. Files Advanced Android が MobileIron デバイス管理と連携するには、特別バージョンを http://www.grouplogic.com/web/aalatest の **`Files Advanced Client Installers`** からダウンロードする必要があります。

   注意: ダウンロードするバージョンにご使用のバージョンの MobileIron の **Secure Apps Manager** との互換性があることを確認してください。

2. MobileIron コアコンソールにログインします。
3. **[Apps]** タブを開いて、**[App Catalog]** を選択します。
4. **[Add+]** を押して、**[In-House]** を選択します。
5. **[Browse]** を押し、**`Files Advanced Android .apk`** まで移動してこのファイルを選択します。

6. **[次へ]** を押します。アプリの説明を入力して、**[次へ]** を押します。

7. **アプリストア**の場合は、**[Apps@Work Catalog]** -> **[Feature this App in the Apps@Work catalog]** が有効になっていることを確認して、**[次へ]** を押します。

8. このアプリがすべてのユーザーに必須のインストールかどうかを選択して、**[完了]** を押します。

12.3.2.4 Files Advanced iOS アプリの MobileIron との統合

注意: この作業は、アプリのバンドル ID を書かずに、アプリが Apps@Work ストアに表示されるようにして MobileIron コンソールからアプリの選択が行えるようにする場合にのみ必要です。

1. MobileIron コアコンソールにログインします。
2. **[Apps]** タブを開いて、**[App Catalog]** を選択します。
3. **[Add+]** を押して、**[iTunes]** を選択します。
4. 検索ボックスに **Files Advanced** と入力して **[参照]** を押し、最新のバージョンの Files Advanced を選択します。
5. **[次へ]** を押します。アプリの説明を入力して、**[次へ]** を押します。
6. **アプリストア**の場合は、**[Apps@Work Catalog]** -> **[Feature this App in the Apps@Work catalog]** が有効になっていることを確認して、**[次へ]** を押します。

   注意: [This is a free app] アプリを有効にすることが必要な場合もあります。

7. **[App Configuration]** で、希望する追加の構成を選択して、**[完了]** を押します。

12.3.2.5 MobileIron VSP で Files Advanced 用に AppConnect 構成とポリシーを作成する

Files Advanced ユーザーのオンボード 『103ページ 』を始める前に次の 2 つの項目を MobileIron VSP で作成する必要があります。

1. モバイル アプリケーションの**構成**: AppConnect がモバイル アプリケーションを自動構成することを許可し、Files Advanced の「登録フォーム」の一部またはすべてに入力し、Files Advanced ユーザー招待プロセスを代行します。

2. モバイル アプリケーション **コンテナ ポリシー**: このポリシーでは、Files Advanced の一部の機能を制限できます。

セクションの内容

モバイル アプリケーション構成の作成

1. MobileIron VSP ウェブコンソールにログインし、**[Policies & Configs]** タブを選択します。
2. **[Configurations]** タブをクリックして [Add New] を押します。
3. ドロップダウンメニューで、**[AppConnect]** に移動します。、**[App Configuration]** を選択します。

4. この新しい **AppConnect アプリケーション構成**で、次の情報を入力します。

名前: この構成に任意の名前を付けることができます。複数の構成を作成し、別々の MobileIron ラベルにその構成を割り当てることができます。

説明: 任意の説明を入力できます。

アプリケーション: リストから Files Advanced アプリを選択します。iOS デバイスと Android デバイスの両方を使用している場合は、必ず対象のクライアントに適したアプリを選択してください。

AppTunnel: **AppTunnel** 設定は任意です。**AppTunnel** を使用して Files Advanced サーバーへのアクセスを提供する場合に限り必要になります。

- **Sentry**- どの MobileIron Sentry サーバーを使用するかを選択します。
- **Service** - この構成のアプリケーションが **AppTunnel** を使用して接続できるサービスを選択します。**<ANY>**を選択してアプリケーションがすべての内部サービスに接続できるようにするか、Files Advanced 用に専用**サービス**を選択することができ

ます。専用サービスオプションを選択する場合は、Files Advanced サーバー用のカスタム**サービス**を追加しておく必要があります。

注意: <TCP_ANY>は**<ANY>**と同じではなく、<TCP_ANY>を選択しても動作しません！

注意: カスタムサービスを追加するには、**[Services]** -> **[Sentry]** の順に選択して、希望する **Sentry** で **[Edit]** を押します。その後、**[AppTunnelConfiguration]** セクションで、**[Services]** の下にある**+**ボタンを押します。**サービス名**を入力し、認証方法を選択し、**[TLS Enabled]** チェックボックスが選択されていることを確認して、**[Server List]** に Files Advanced サーバーまたはゲートウェイ（あるいはその両方)の DNS アドレスを入力します。

- **URL Wildcard**: Files Advanced サーバーまたはドメイン全体の DNS アドレス。（例、***.domain.com**）
- **Port**- Files Advanced のサービスはデフォルトでポート 443 と 3000 を使用します。ユーザーが登録するサービスに応じて、どちらか必要なポート番号を入力してください。

App-specific Configurations: このセクションでは、この構成が適用されるユーザー用の Files Advanced 登録フォームの自動入力に使用する値を MobileIron ラベルに基づいて指定できます。次の**キー**を追加できます。

- **enrollmentServerName**: このキー フィールドは必須です。 このキーの値は、ユーザーが登録する Files Advanced サーバーの DNS アドレスに設定する必要があります。
- **enrollmentPIN**: このキーは任意指定です。Files Advanced サーバーがクライアント登録に PIN コードを要求する場合は、Files Advanced 登録フォームの PIN コード フィールドにこの値を自動入力できます。AppConnect は、ワンタイム PIN コードではなく、ユーザーがアクセスを取得する前の認証の二次要因として機能できるので、通常 Files Advanced サーバーの PIN 要求は無効になっています。この PIN 要件は、**Files Advanced** ウェブ コンソールの **[設定]** ページ 『143ページ 』で設定します。
- **enrollmentAutoSubmit**: このキーはオプションです。 このキーにより、登録フォームが自動的に送信されるため、ユーザーは登録時に [今すぐ登録] ボタンをタップする必要がなくなります。 このキーを有効にするには、値を **Yes** にします。

- **requirePIN**: このキーは任意指定です。Files Advanced モバイル ユーザーが Files Advanced 登録フォームに手動で入力する必要がある PIN を Files Advanced モバイル ユーザーに配信している場合は、このキーの値を **Yes** に設定して、PIN フィールドがフォームにすぐに表示されるように指定できます。
- **enrollmentUserName**: このキーは任意指定です。このキーの値は、Files Advanced 登録フォームの [ユーザー名] フィールドに挿入されます。MobileIron の**$USERID$**ワイルドカードを使用することができます。このワイルドカードを使用すると、Mobile@Work アプリをセットアップするときにユーザーが入力したユーザー名がフィールドに自動記入されます。
- **enrollmentPassword**: このキーは任意指定です。このキーの値は、Files Advanced 登録フォームの [パスワード] フィールドに挿入されます。MobileIron の**$PASSWORD$**ワイルドカードを使用することができます。このワイルドカードを使用すると、Mobile@Work アプリをセットアップするときにユーザーが入力したパスワードがフィールドに自動記入されます。

Files Advanced アプリケーション コンテナ ポリシーの作成

1. MobileIron VSP ウェブコンソールにログインし、**[Policies & Configs]** タブを選択します。
2. **[Configurations]** タブをクリックして [Add New] を押します。
3. ドロップダウンメニューで、**[AppConnect]** に移動します。、**[Container Policy]** を選択します。
4. この新しい**コンテナポリシー**で次の情報を入力します。

名前: この構成に任意の名前を付けることができます。複数の構成を作成し、別々の MobileIron ラベルにその構成を割り当てることができます。

説明: 任意の説明を入力できます。

アプリケーション: リストから Files Advanced アプリを選択します。iOS デバイスと Android デバイスの両方を使用している場合は、必ず対象のクライアントに適したアプリを選択してください。

Exempt from AppConnect passcode policy: ユーザーが AppConnect パスコードで先に認証せずに Files Advanced を開くことができるようにする場合は、このオプションを選択します。

Allow Copy/Paste To: ユーザーが、Files Advanced モバイルに表示されるドキュメントのテキストをコピーして、AppConnect によって管理されていないデバイスのその他のアプリケーションに貼り付けることを許可する場合は、このオプションを選択します。

Allow Print: Files Advanced ユーザーが利用可能な AirPrint 対応プリンタでドキュメントを印刷することを許可する場合は、このオプションを選択します。

スクリーン キャプチャを許可: このオプションは、AppConnect SDK ではまだサポートされていません。Files Advanced モバイルの場合、ユーザーは、MDM 構成によってデバイス全体で画面の取り込みが無効になっていなければ、常に画面を取り込むことができます。

Allow Open In: Files Advanced ユーザーがデバイスの別のアプリケーションでファイルを開くことを許可する場合は、このオプションを選択します。このオプションを選択すると、許可するアプリケーションのリストを指定できるようになります。

新しい Configuration と Container Policy へのラベルの割り当て

この新しいポリシーをモバイル デバイスに適用するには、必要なユーザーの MobileIron ラベルを **Configuration** と **Container Policy** の両方に割り当ててください。

12.3.2.6 AppConnect による Files Advanced iOS クライアントのアクティブ化

注意: Files Advanced アプリをアクティブ化するこの方法は iOS バージョンにのみ適用され、MobileIron VSP コンソールのアプリのリストに Files Advanced アプリが追加されておらず、ユーザーがまだ Files Advanced を使用していない場合にのみ必要です。

アプリが MobileIron コンソールを使用して追加されている場合には、設定に応じて、ユーザーはアプリを **Apps@Work** ストアからダウンロードすることができるか、またはデバイスに自動でインストールされます。

MobileIron VSP で必要な構成とコンテナ ポリシーを作成したら、Files Advanced をクライアント デバイスにインストールして設定できます。

Mobile@Work がインストールされていて設定されていることを確認する

Access Mobile Client をインストールまたはアクティブ化する前に、MobileIron Mobile@Work iOS アプリケーション https://itunes.apple.com/app/mobileiron-mobile-work-client/id320659794をデバイスにインストールしたことを確認してください。このアプリケーションは、Files Advanced が MobileIron VSP と通信して、AppConnect の構成とコマンドを受信する経路として機能します。

インストール後、ユーザー アカウント情報および VSP サーバーのアドレスで Mobile@Work を設定する必要があります。

Mobile@Work をインストールして構成したら、Files Advanced の設定を進めることができます。AppConnect で Files Advanced を設定するシナリオには次の 3 つがあります。

セクションの内容

Files Advanced は既にデバイスにインストールされているが、まだ Files Advanced サーバーに登録されていない

このシナリオでは、Mobile@Work と AppConnect VSP の構成が設定される前に、Files Advanced iOS アプリが予めデバイスにインストールされ、開始されていることがあります。Files Advanced モバイルを開始しただけでは、AppConnect の設定処理は開始されない場合があります。この場合は、Files Advanced アプリの [設定] メニュー を開き、設定リストの下部にある [MobileIron AppConnect] オプションをタップし、[有効] ボタンを選択すると、AppConnect の設定処理を手動で開始できます。AppConnect の設定が直ちに開始されない場合は、開始できるように、しばらく Files Advanced アプリを開いたままにしてください。設定が開始されると、処理は前のシナリオで示したように進みます。

Mobile@Work アプリがデバイスに存在しない場合、Files Advanced は、**[有効]** ボタンを表示せず、この **[設定]** メニューに警告を表示します。

Files Advanced は既にデバイスにインストールされ、Files Advanced サーバーに登録されている

このシナリオは前のシナリオに似ています。ただ 1 つの違いは、Mobile アプリを自動登録するために AppConnect Files Advanced の構成が使用されないという点です。Mobile アプリが既に Files Advanced サーバーに登録されている場合は、元の構成が維持されます。

Files Advanced が、管理に AppConnect を使用するため、および AppConnect のパスコードおよび許可コンテナポリシーの使用を開始するために、ユーザーはまず Files Advanced アプリを開き、**[設定]** -> **[Partner Features]** -> **[MobileIron]** に移動し、**[Enable AppConnect]** をタップします。その後少し待ってから、アプリを再起動する必要があります。

ユーザーに対して別の Files Advanced サーバーへの登録を求める場合は、AppConnect による構成が可能になるように、Files Advanced アプリのアンインストールと再インストールが必要になります。

Files Advanced がまだデバイスにインストールされていない

このシナリオでは、Apple App Store または MobileIron Apps@Work から Files Advanced をインストールする必要があります。

インストール後、Files Advanced を起動します。

Files Advanced は、構成済みの Mobile@Work アプリケーションの存在を確認し、一時的に Mobile@Work アプリケーションに切り替えた後、もう一度 Files Advanced に切り替えます。有効な Files Advanced AppConnect 構成が見つかると、Files Advanced は自動的に登録モードに入り、Files Advanced モバイル登録フォームをユーザーに提示します。AppConnect 構成に含まれるフィールドは、自動的に入力されます。ユーザーは通常、フォームに AD パスワードを入力し、送信するだけですみます。これが完了すると、関連する Files Advanced Client Management ポリシーが Files Advanced に適用され、ユーザーは、アプリケーションの使用を開始する準備が整います。

Files Advanced の有効な構成が VSP に存在しないか、Mobile@Work アプリケーションのインストールまたは構成が終わっていない場合は、ユーザーはエラー メッセージを受信します。Mobile@Work がインストールされていない場合は、Files Advanced は単に標準モードで起動し、AppConnect は有効化されません。

12.3.2.7 Files Advanced モバイルの継続的な AppConnect 管理

Files Advanced が AppConnect によってアクティブに管理されるようになると、Files Advanced がデバイス上の Mobile@Work アプリケーションにチェックインしたときに、適用可能なコンテナポリシーに対する変更が Files Advanced モバイルによって受信されます。このチェックインの間隔は MobileIron VSP で設定され、Files Advanced アプリケーションは一時的に Mobile@Work に切り替えてチェックインを実行します。これによりユーザー操作が中断するため、アプリケーションの使用を頻繁に阻害することのないように、チェックインの間隔を十分な長さに設定することをお勧めします。

コンテナ ポリシーへの変更、Files Advanced へのアクセスの取り消しなどは、次回のチェックイン時にアプリケーションに適用されます。

12.3.2.8 Kerberos 制約付き委任を使用した AppConnect の使用

この記事では、Kerberos 制約付き委任で認証を処理し、MobileIron AppTunnel を通じてプロキシ経由で Files Advanced iOS モバイルアプリを Files Advanced サーバーに接続するために必要なシステムコンポーネントの設定方法について説明します。

Android モバイルアプリと Windows モバイルアプリは、この構成をサポートしません。

注意: 設定作業を支援するために、Kerberos 制約付き委任を対象とした MobileIron の設定方法に関するドキュメントが提供されています。ただし、Sentry が KDC の Kerberos チケットを受信しているかを確認するまでの手順は、すべて MobileIron ソフトウェアに関する手順に限られています。一連の手順を完了したり、Kerberos チケットを正常に受信したりするのが困難な場合は、**MobileIron** のサポートにお問い合わせください。

複雑な設定になるため、エラーの削減とトラブルシューティングの簡素化を目的として、設定を 2 段階で行います。第 1 段階では、Acronis Files Advanced サーバーへの認証にユーザー名とパスワードを使用して、AppTunnel を設定します。このインフラストラクチャ

は、第 2 段階で Kerberos 制約付き委任を実装するための基盤となります。問題の特定手順を省くために、ユーザー名とパスワードによる認証でトンネルが正常に機能するかをテストしてから、Kerberos の段階に進むことを強くお勧めします。

始める前に

- Kerberos 制約付き委任（KCD)を使用することにより、Kerberos 以外の認証方法で ID が設定されると、ユーザーは Kerberos によるネットワーク リソースへの認証が可能になります。Files Advanced の場合、MobileIron で配布された iOS デバイスレベルの ID を使用して認証できます。KCD を使用しない場合、Files Advanced アプリで使用できる証明書は、アプリに直接インストールされた証明書に限られます。

  注意: KCD に関連する設定は、すべて MobileIron と Windows で行います。Files Advanced 自体で特別な変更は行いません。

- キー配布センター（KDC)は、Active Directory ドメイン内でセッション チケットと一時セッション キーを発行するネットワーク サービスです。
- Kerberos 認証はゲートウェイ サーバーのみが行うことができます。Files Advanced サーバーでは行うことができません。
  - Files Advanced モバイルアプリは、ゲートウェイサーバーを使用してクライアント管理に登録する必要があります。Files Advanced サーバーでクライアントを登録すると、正常にログインできません。
  - Kerberos 認証を使用したモバイルクライアントは、ネットワーク共有、同期・共有フォルダ、および SharePoint サイトへの認証を行うことができます。

前提条件

次のソフトウェアを事前にインストールして設定する必要があります。

- MobileIron VSP（このドキュメントでは 5.9 を使用)
- Kerberos が正常に機能するには、Kerberos をサポートするよう設定された Active Directory から VSP のユーザー アカウントを取得する必要があります。
- MobileIron Sentry（このドキュメントでは 4.8 を使用)
- インストール済みの Files Advanced サーバー（このドキュメントでは 6.0.2 を使用)

- サーバーの相互運用性
  - VSP、Sentry、ドメインコントローラ、Files Advanced サーバーの時刻をすべて同期させる必要があります（NTP を推奨)。
  - ドメイン名の解決（DNS)。Sentry は、接続用に設定された FQDN に基づいて、KDC のチケットを要求します。FQDN は、Kerberos 委任用に設定されたコンピュータ名と一致する必要があります。一致していない場合、KDC はチケットの発行を拒否します。
  - VSP は、Sentry に接続できる必要があります（デフォルトではポート 9090 と 443、その他のポートの場合は必要な設定に基づきます)。
  - Sentry は、Active Directory と Files Advanced サーバーに接続できる必要があります（ポート 88、389、636)。
  - Active Directory と Sentry 間のポート 88（UDP、TCP)とポート 389（TCP)を開いて、通信を許可する必要があります（SSL 対応 Active Directory を使用している場合は TCP 用のポート 636 を開きます)。 ポート 88 は、Kerberos プロトコルの通信に使用されます。 ポート 389（または 636)は、KDC の IP が Active Directory の IP と同じであることを確認するために、Sentry と KDC 間の LDAP ping に使用されます。
  - Windows Server 2003 を使用している場合、KDC は TCP の代わりに UDP を使用して、ポート 88 の要求をリッスンすることがあります。 Kerberos で UDP ではなく TCP を使用するよう強制するには、レジストリ エディタで MaxPacketSize を 0 から 1 に変更します。 この変更方法の詳細については、Microsoft サポート技術情報の記事（http://support.microsoft.com/kb/244474 http://support.microsoft.com/kb/244474)を参照してください。
- iOS デバイスは、VSP と Sentry に接続できる必要があります。
- iOS デバイスを VSP に登録します。
- Mobile@Work をデバイスにインストールし、VSP に登録します。登録時には MDM プロファイルを適切にインストールします。

セクションの内容

13 ユーザー名/パスワード認証による Files Advanced モバイルと Files Advanced サーバー間の AppConnect トンネルの設定

Acronis Files Advanced モバイルと Acronis Files Advanced サーバー間の AppConnect トンネルを設定する最初のステップとして、Sentry を VSP に追加して設定します。この設定は、複数の手順からなるプロセスで、次の段階に分類されます。

- 新しいローカル CA の生成
- 新しい SCEP の作成
- Sentry の追加と設定
- VSP での Files Advanced の構成

代替認証機関 (CA)と SCEP (Simple Certificate Enrollment Protocol)プロバイダを利用している場合がありますが、このガイドでは説明を省略します。サード パーティの CA と SCEP プロバイダの設定方法については、MobileIron のドキュメントを参照してください。

セクションの内容

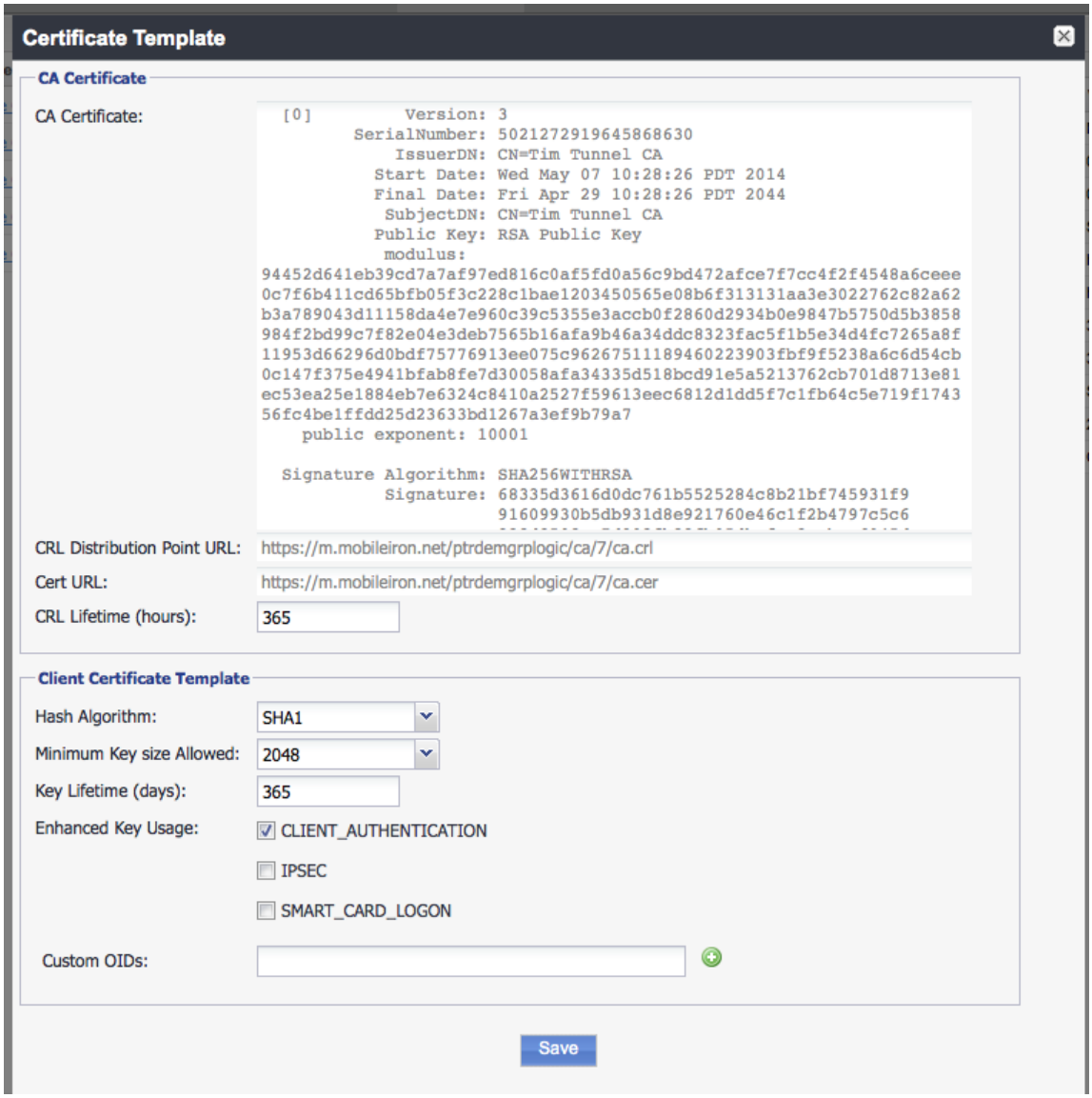
5.

1. MobileIron VSP Admin Portal を開きます。
2. **[Settings]** を選択し、**[Local CA]** を開きます。

3. **[Add New]** を押し、**[Generate Self-Signed Cert]** を選択します。

- **Local CA Name**: 必要な設定に基づいて、名前を入力します。
- **Key Length**: **[2048]** を選択します。
- **Issuer Name**: 必要な設定に基づいて、名前を入力します。名前の先頭には、**CN=** を使用する必要があります。

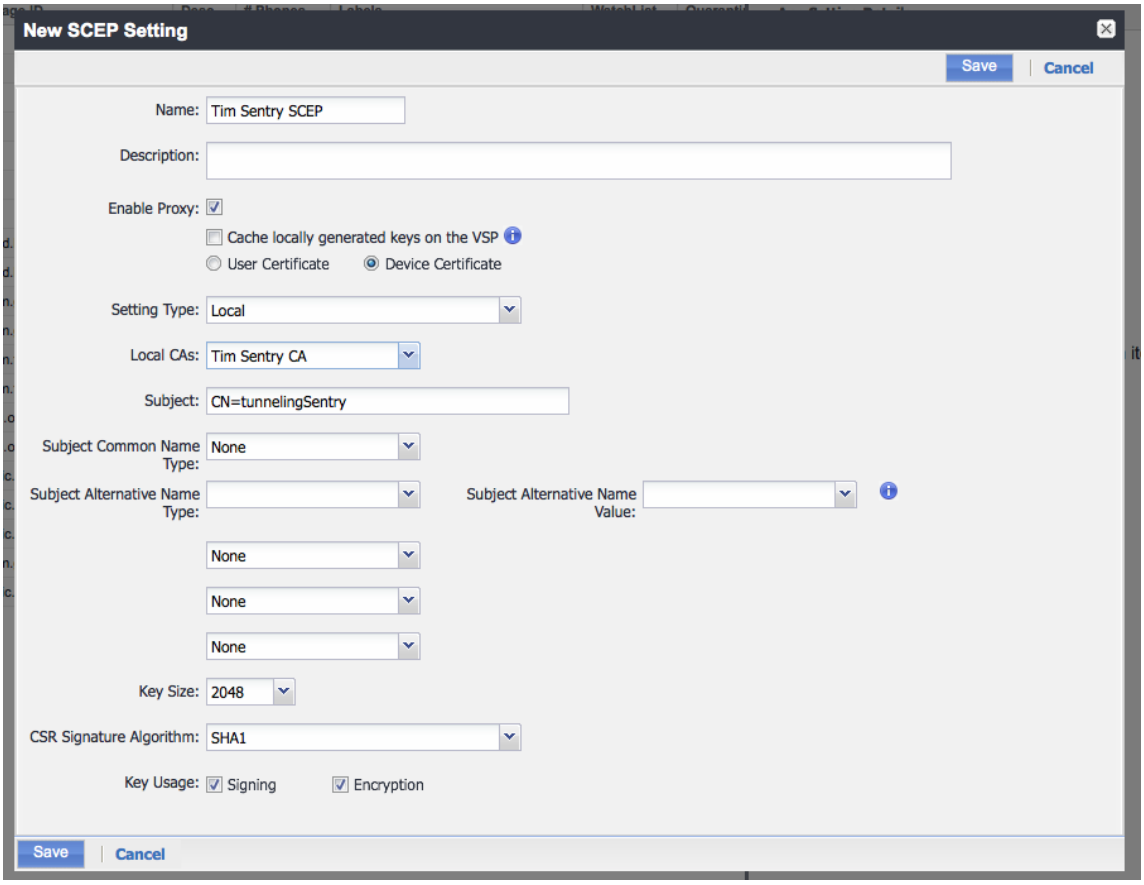
4. **[Generate]** をクリックします。



5. **[Save]** をクリックします。
6. 新しい CA の **[View Certificate]** をクリックします。
7. 証明書を新しいテキスト ファイルにコピーし、デスクトップに保存します。

1. MobileIron VSP Admin Portal を開きます。
2. **[Policies & Configs]** を選択し、**[Configuration]** を開きます。

3. **[Add New]** を押し、**[SCEP]** を選択します。

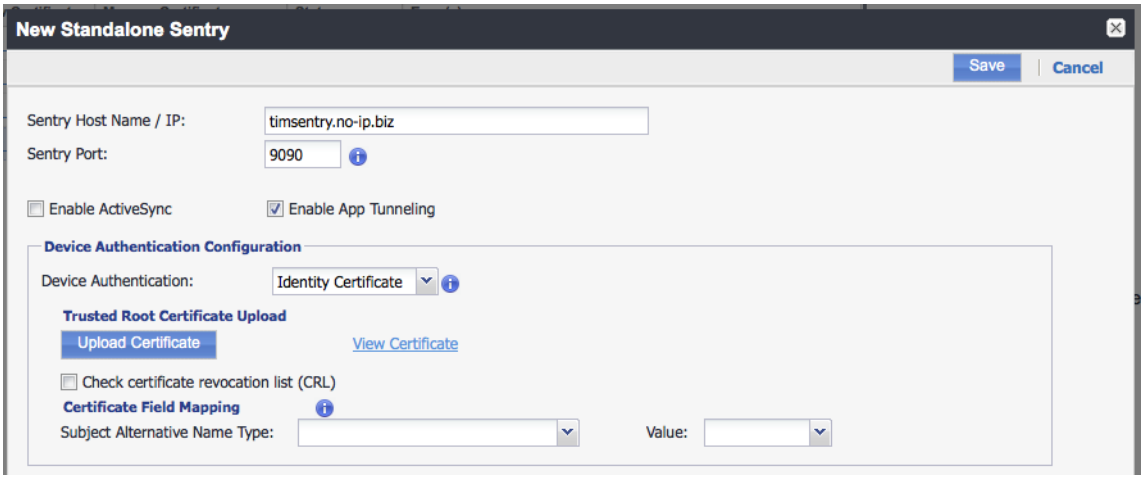


- **Name**: 必要な設定に基づいて、名前を入力します。
- **Setting Type**: **[Local]** を選択します。
- **Local CAs**:「新しいローカル CA の生成」で作成した CA の名前。
- **Subject**: 必要な設定に基づいて、名前を入力します（例: CN=tunneling)。名前の先頭には、**CN=** を使用する必要があります。
- **Key Size**: CA の生成時に選択した値と同じ値を選択します。この場合、**[2048]** を選択します。

4. **[保存]** をクリックします。

1. MobileIron VSP Admin Portal を開いたまま、**[Settings]** を選択し、**[Sentry]** を開きます。

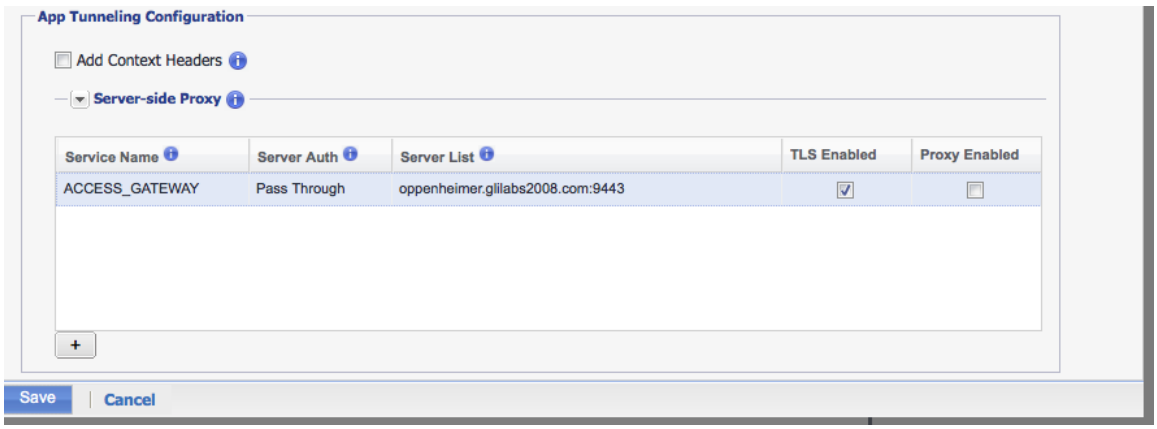
2. **[Add New]** を押し、**[Standalone Sentry]** を選択します。



- **Sentry Host Name/IP**: Sentry をインストールした FQDN。MobileIron VSP からアクセスできる必要があります。
- **Sentry Port**: MobileIron VSP からの接続用の開いたポート（デフォルトは 9090）。
- **Enable App Tunneling**: このチェックボックスをオンにします。
- **Device Authentication**: **[Identity Certificate]** を選択します。

3. **[Upload Certificate]** をクリックします。
4. 「新しいローカル CA の生成」でデスクトップに保存したテキスト ファイルを参照して選択します。
5. **[Upload Certificate]** をクリックします。

このセクションでは、Files Advanced ゲートウェイ サーバーへのマッピングを行うサービスを設定します。管理サーバーは Kerberos 制約付き委任認証をサポートしていません。ただし、管理サーバーと同じコンピュータにインストールされているゲートウェイを使用して、登録を行うことはできます。この場合、Kerberos 制約付き委任認証を使用した登録をサポートする設定を使用する必要があります。



- **Service Name**: 必要な設定に基づいて、名前を入力します。
- **Server Auth**: **[Pass Through]** を選択します。これは、このガイドの後の部分で変更します。
- **Server List**: サーバーのセミコロン区切りのリストです。このドキュメントでは、1 つのサーバーを使用します。これは、Files Advanced ゲートウェイ サーバーの DNS アドレスおよびそのサーバーがリッスンするポートになります。
- **TLS Enabled**: チェックボックスをオンにします。

[保存] をクリックします。

新しい Sentry エントリの **[View Certificate]** をクリックします。VSP と Sentry 間の通信がテストされます。証明書を取得できない場合は、VSP と Sentry 間の接続とポートを確認してください。正常に通信できるようになるまで、先に進まないでください。

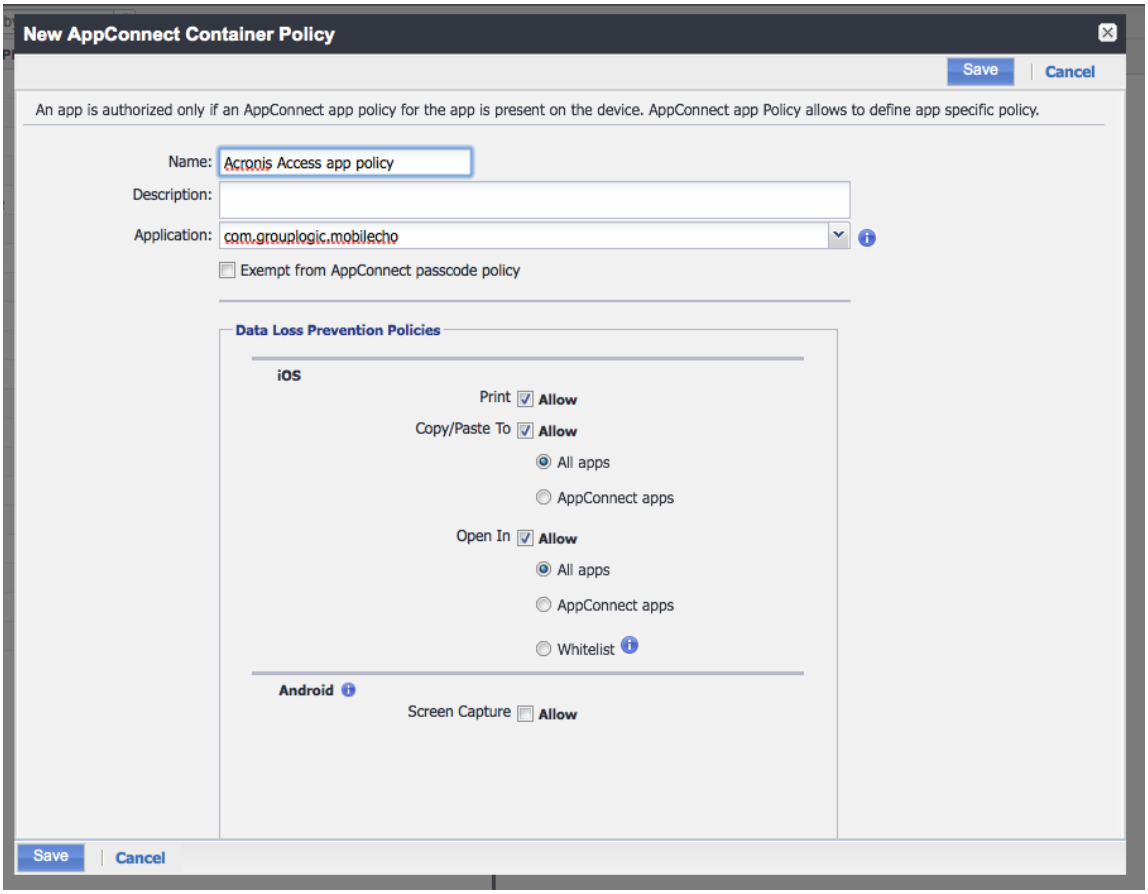
VSP での Files Advanced の構成

Sentry の設定が完了したら、Files Advanced 用にアプリケーションポリシーとアプリケーション設定を作成する必要があります。一連の設定は、次の複数の手順からなるプロセスです。

セクションの内容

6.

1. MobileIron VSP Admin Portal を開いたまま、**[Policies & Configs]** を選択し、**[Configurations]** を開きます。
2. **[Add New]** を押し、**[AppConnect]** を選択して、**[Container Policy]** を選択します。

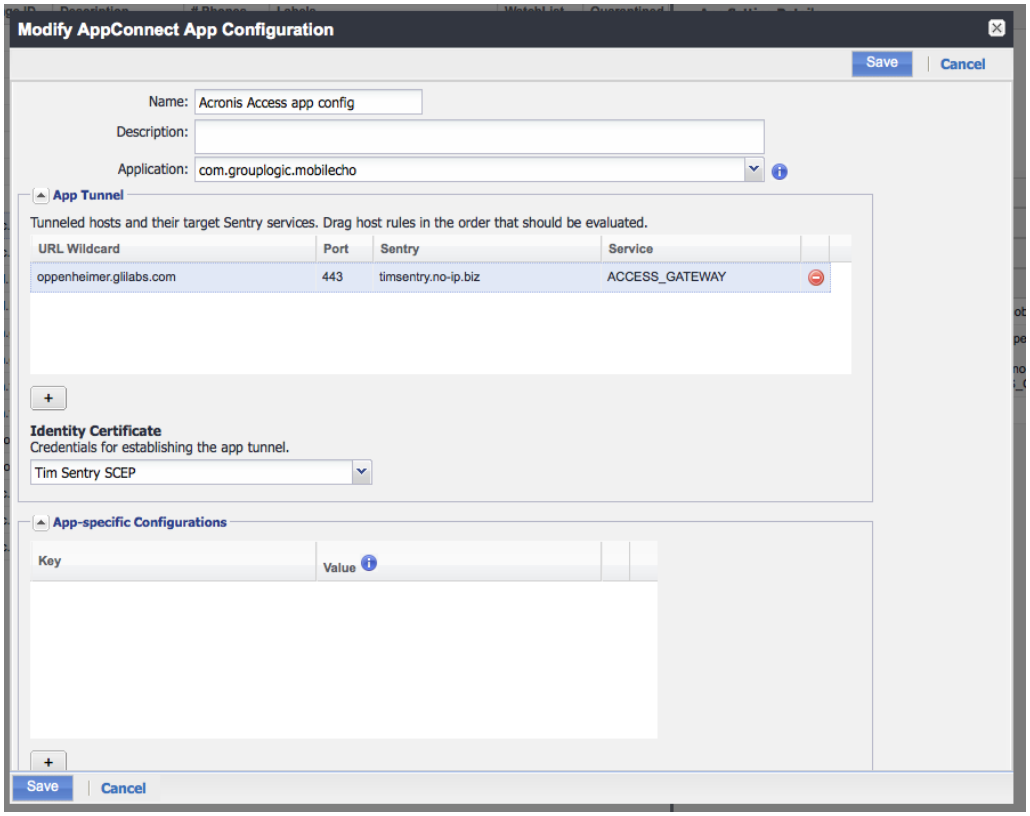


- **Name**: 必要な設定に基づいて、名前を入力します。
- **Application**: 「**com.grouplogic.mobilecho**」と入力します。iOS App Store からのバンドル ID です。
- **Policies**: Files Advanced の管理に使用する任意の MobileIron ポリシーを設定します。

3. **[保存]** をクリックします。

1. MobileIron VSP Admin Portal を開いたまま、**[Policies & Configs]** を選択し、**[Configurations]** を開きます。

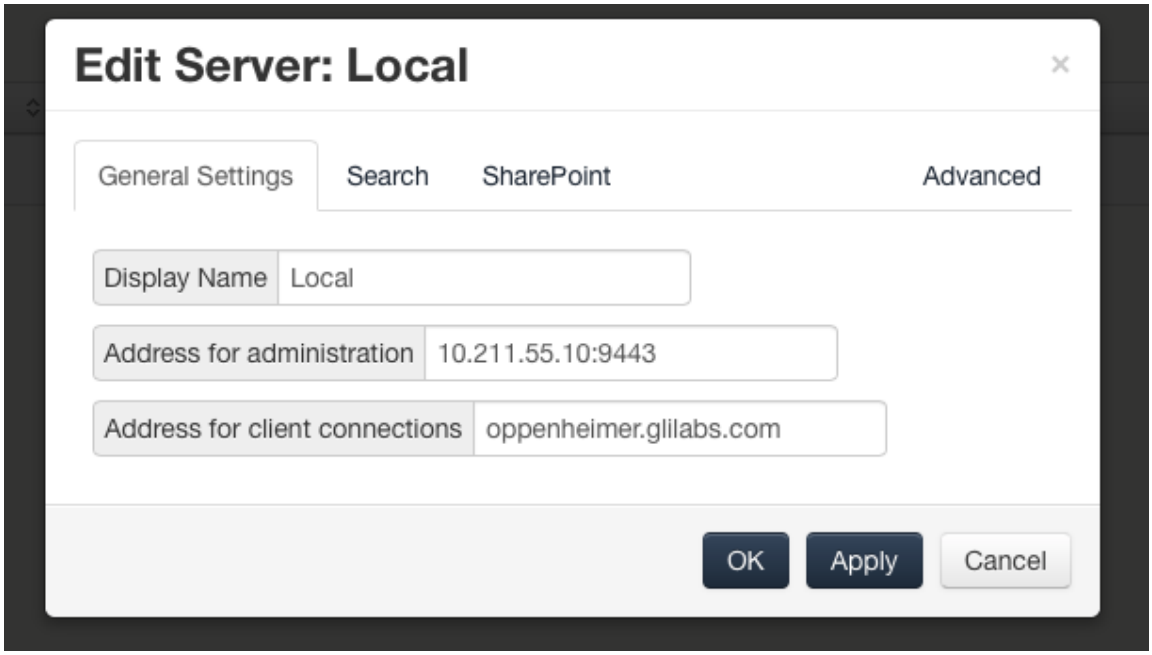
2. **[Add New]** を押し、**[AppConnect]** を選択して、**[Configuration]** を選択します。



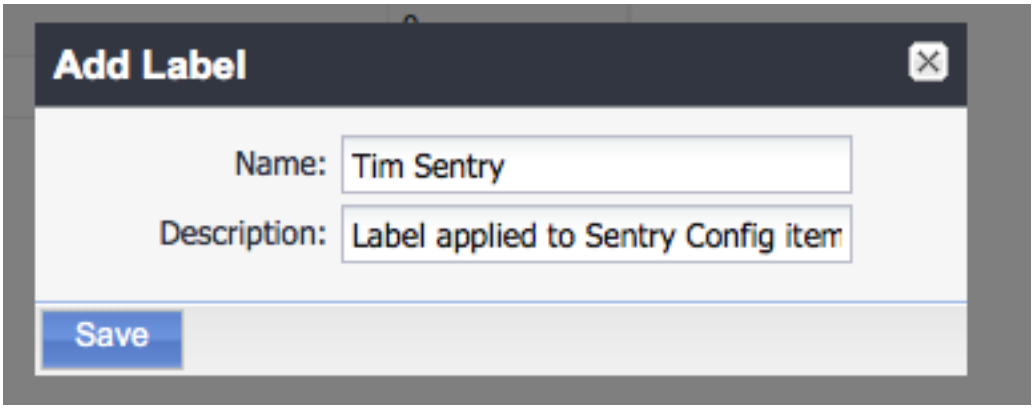
- **Name**: 必要な設定に基づいて、名前を入力します。
- **Application**: 「com.grouplogic.mobilecho」と入力します。これは、Apple App Store に表示されるバンドル ID です。
- **App Tunnel**
  - **URL Wildcard**: クライアントが Files Advanced ゲートウェイ サーバーへの接続を試行する URL です。この URL は、Files Advanced の管理者用インターフェイスでゲートウェイサーバーに設定した [クライアント接続のアドレス] と一致する必要があります。このフィールドでは、複数のゲートウェイと照合するために正規表現を使用できます。ただし、このドキュメントでは、正確なホスト名を入力します。*
  - **Port**: クライアントが接続を試行するポート（デフォルトでは 443)。
  - **Sentry**:「Sentry の追加と設定」で作成した Sentry。
  - **Service**:「Sentry の追加と設定」ゲートウェイに設定したサービス。
  - **Identity Certificate**:「新しい SCEP の作成」で作成した SCEP。

3. **[保存]** をクリックします。

*Files Advanced ウェブインターフェイスからのクライアント接続のアドレス。このアドレスは、ファイル システムとの接続を確立するためにモバイル クライアントに送信されるプロファイルで使用されます。Sentry の **[URL Wildcard]** の値は、このアドレスと Sentry 経由で接続をルーティングするポートに一致する必要があります。

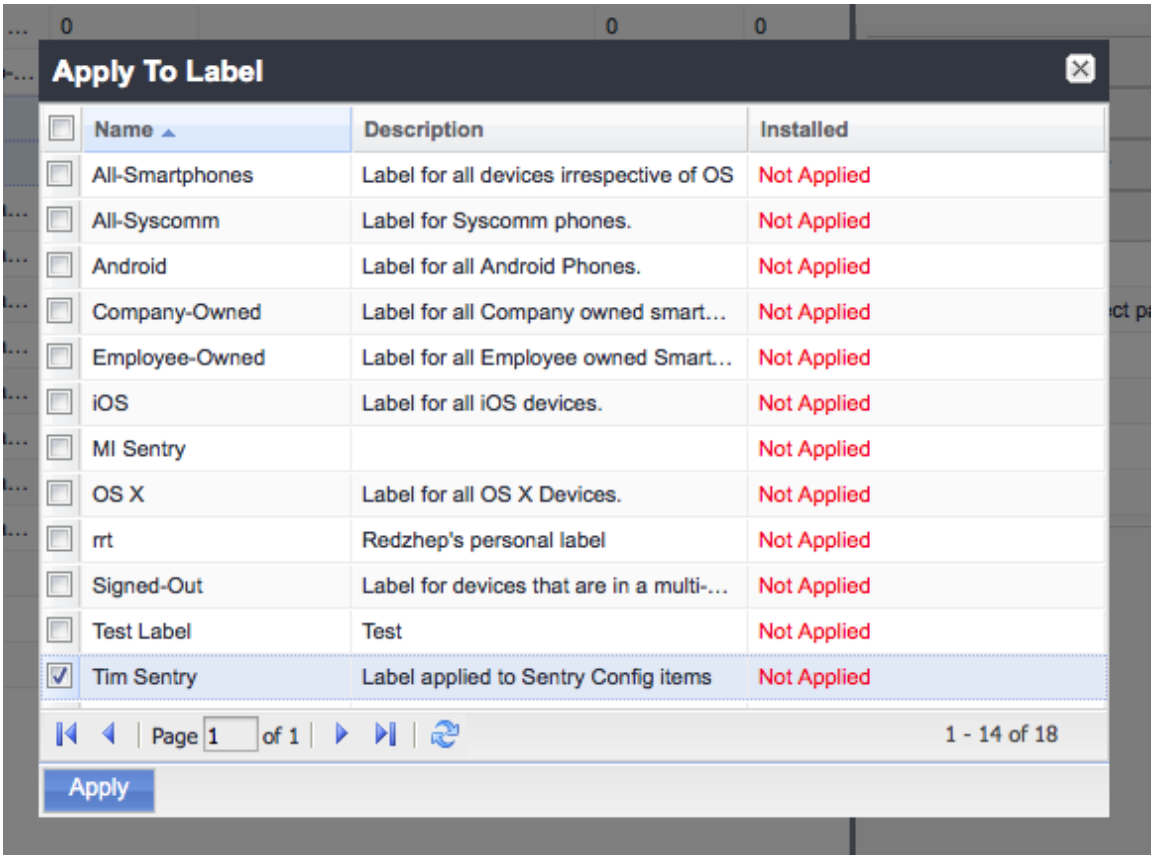


1. MobileIron VSP Admin Portal を開いたまま、**[Users & Devices]** を選択し、**[Labels]** を開きます。
2. **[Add new]** を押します。



   - **Name**: 必要な設定に基づいて、名前を入力します。
   - **Description**: 必要な設定に基づいて、説明を入力します。
3. **[保存]** をクリックします。

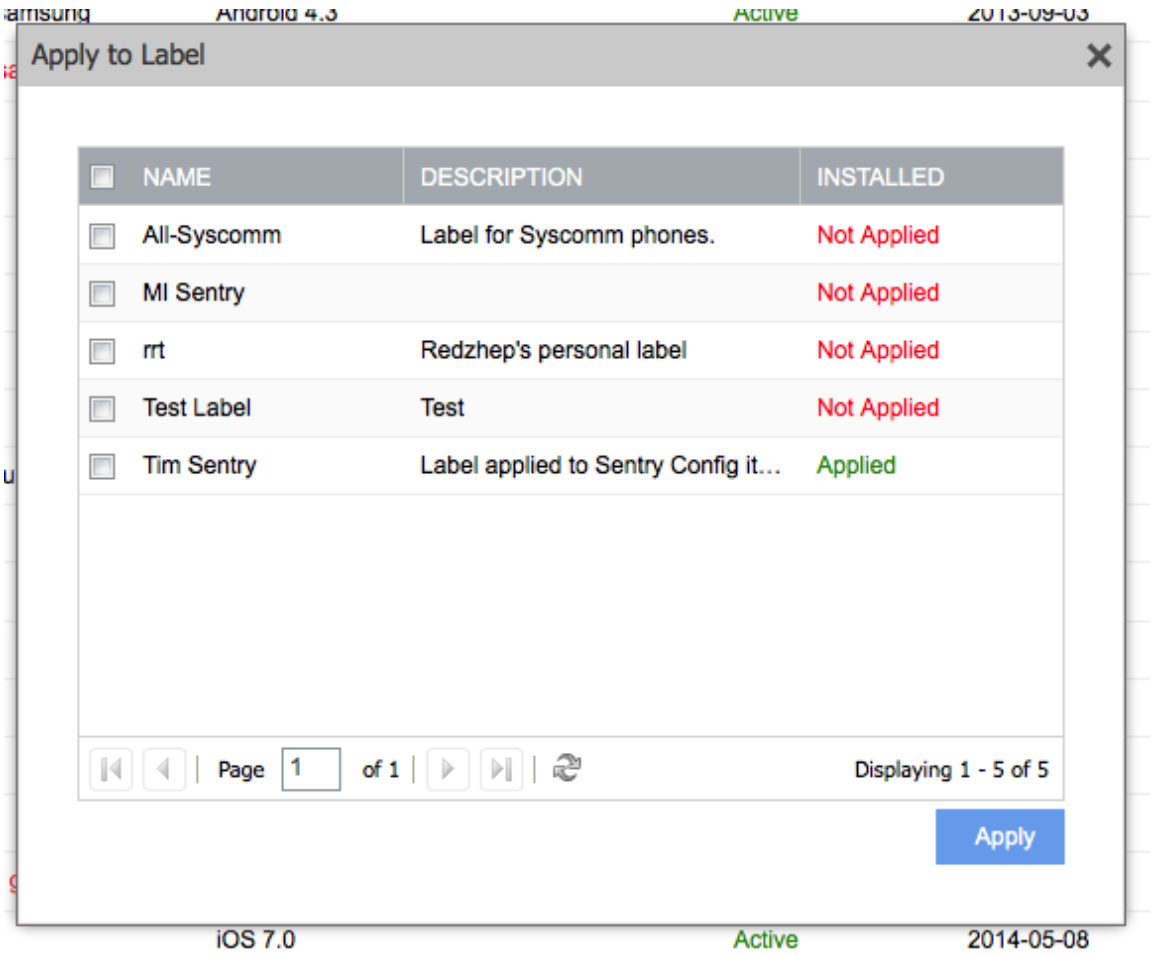
1. MobileIron VSP Admin Portal を開いたまま、**[Policies & Configs]** を選択します。
2. このドキュメントに従って作成した SCEP、AppConnect ポリシー、AppConnect 設定にチェック マークを付けます。**[Configurations]** を開き、チェックした項目を一覧表示します。



3. **[More Actions]** を押し、**[Apply to Label]** を選択します。
4. 「新しいラベルの作成」で作成したラベルにチェック マークを付けます。
5. **[適用]** をクリックします。

1. MobileIron VSP Admin Portal を開いたまま、**[Users & Devices]** を選択し、**[Devices]** を開きます。

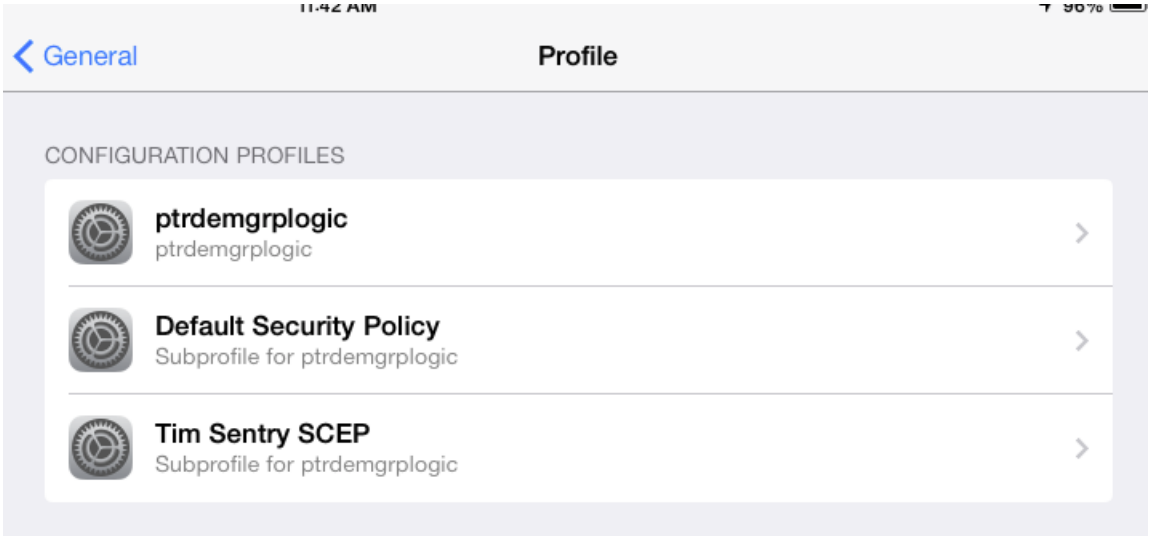
2. Sentry のテストに使用する iOS デバイスにチェック マークを付けます。



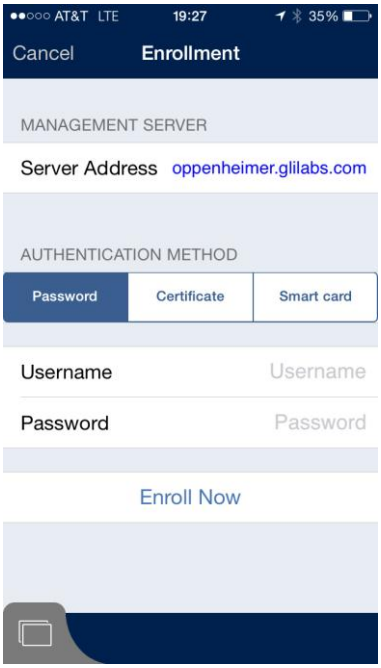
3. **[Actions]** → **[Apply to Label]** の順に選択します。
4. 「新しいラベルの作成」で作成したラベルにチェック マークを付けます。
5. **[適用]** をクリックします。

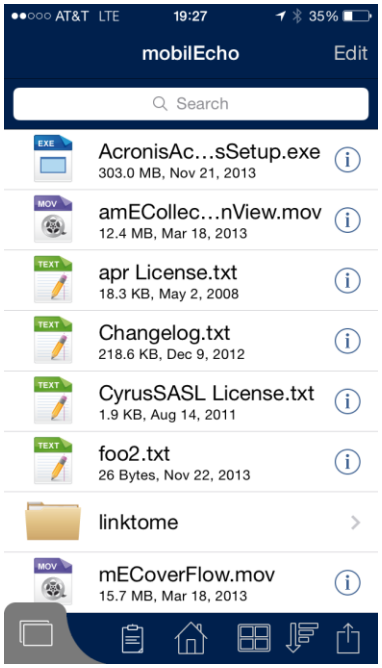
1. Mobile@Work アプリケーションを開き、**[Settings]** を開きます。
2. [Check for Updates] をタップします。

3. **[Force Device Check-In]** をタップします。正常な場合、このドキュメントで設定した SCEP が、**[Settings]** → **[General]** → **[Profiles]** のデバイス設定に表示されます。



4. App Store から Acronis Files Advanced をインストールして起動します。
5. ようこそ画面で **[今すぐ登録]** を選択するか、**[設定]** に移動して **[登録]** まで下にスクロールします。





6. <Files Advanced> ゲートウェイとのクライアント接続に使用し、**AppConnect の設定**で設定したアドレスを入力します。実際のテスト用のため、この URL はモバイル クライアントからアクセスできません（セルラー ネットワークか外部のネットワークを使用します)。

7. **[続行]** をタップします。
8. **ユーザー名**と**パスワード**を入力して、**[今すぐ登録]** をタップします。

「Files Advanced クライアント管理を使用して登録が完了しました。」と表示されます。

プロファイルのデータソースが、Sentry を経由するよう設定した Files Advanced ゲートウェイの一部である場合、この時点で、AppTunnel 経由でも同じデータソースを参照できるようになります。

AppTunnel の使用状況の確認

このトラフィックが AppTunnel を経由することを確認するには、MobileIron Sentry System Manager にログインします。

1. [Troubleshooting] を選択し、**[Logs]** を開きます。
2. **[Sentry]**、**[To/From Device]**、**[To/From Service]**、**[Level 4]** の各チェックボックスをオンにします。
3. **[Apply]** を選択します。
4. **[View Module Logs]** で、**[Sentry]** を選択します。

5. モバイル デバイスからのトラフィックの場合、Sentry のログをスクロールすると、設定したホスト名に関連するエントリが表示されます。

14 Kerberos 制約付き委任認証の追加

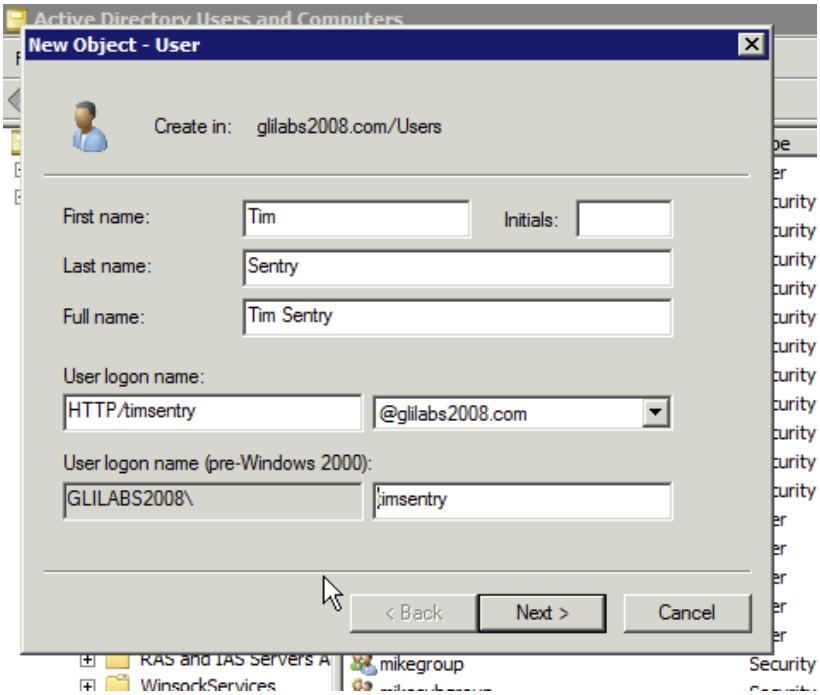
Files Advanced のユーザー名とパスワード認証を使用した AppTunnel の設定と動作確認が完了したら、作成した設定を変更して、Files Advanced ゲートウェイへの Kerberos 制約付き委任認証を実行できるようになります。設定を適切に行うと、管理サーバーへの登録やデータ ソースの参照にユーザー名やパスワードを入力する必要がなくなります。

このドキュメントでは、基本設定を行い、管理サーバーと同じサーバー上で実行している 1 つの Files Advanced ゲートウェイサーバーへの委任を行って、対象のローカル管理サーバーに登録したり、対象のゲートウェイに設定されたデータソースを参照したりできるようにします。ゲートウェイ、SharePoint サーバー、再共有を追加する場合、委任を追加する必要があります。

同じ iOS デバイスを使用して、Kerberos 制約付き委任認証をテストする場合は、テスト時に Acronis Files Advanced モバイルをアンインストールすることをおすすめします。

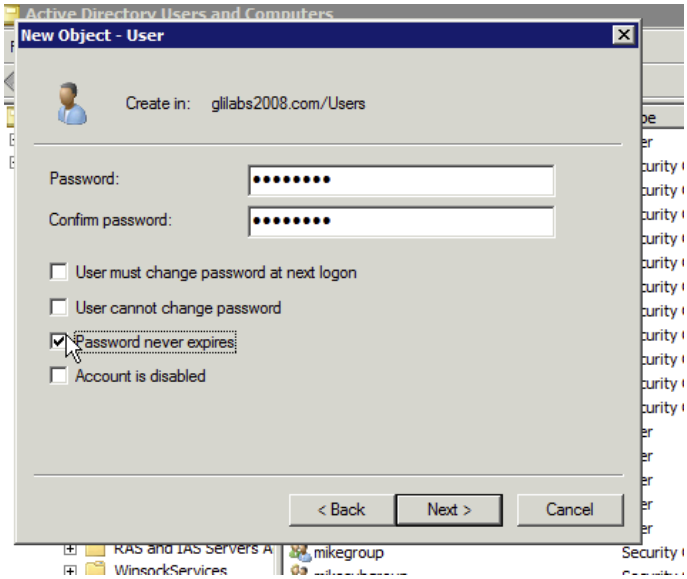
1. KDC サーバーに管理者としてログインします。
2. Windows の [スタート] メニューから、**All Programs** を選択し、**Administrative Tools** → **Active Directory Users and Computers** の順に選択します。
3. 新しく開いたコンソールで、ドメインを展開します (Kerberos では、ドメインを領域と呼びます)。

4. **Users** を右クリックし、**New** → **User** の順に選択します。



- Kerberos サービス アカウントの **Name]** と **User Logon Name** を入力します。**User Logon Name** には、通常の英数字を使用します。空白は使用しないでください。この値は、ガイドで後述するコマンド プロンプトでも入力します。 名前は **HTTP/**で開始する必要があります。**[ユーザー ログオン名](Windows 2000 以前)** の横に **HTTP/** が自動的に表示される場合は、このフィールドから HTTP/ を削除してください。
- **User Logon Name** フィールドの横にあるフィールドで、正しいドメイン名が選択されていることを確認します。正しいドメインが選択されていない場合は、**User Logon Name** フィールドの横にあるドロップダウン リストから正しいドメイン名を選択します。

5. **Next** をクリックします。



- **Password**: パスワードを入力します。
- **Password never expires**: [ユーザーは次回ログオン時にパスワード変更が必要] が選択されていないことを確認します。通常、企業の場合、**User cannot change password** と **Password Never Expires** を選択する必要があります。

6. **Next** をクリックします。
7. **Finish** をクリックします。

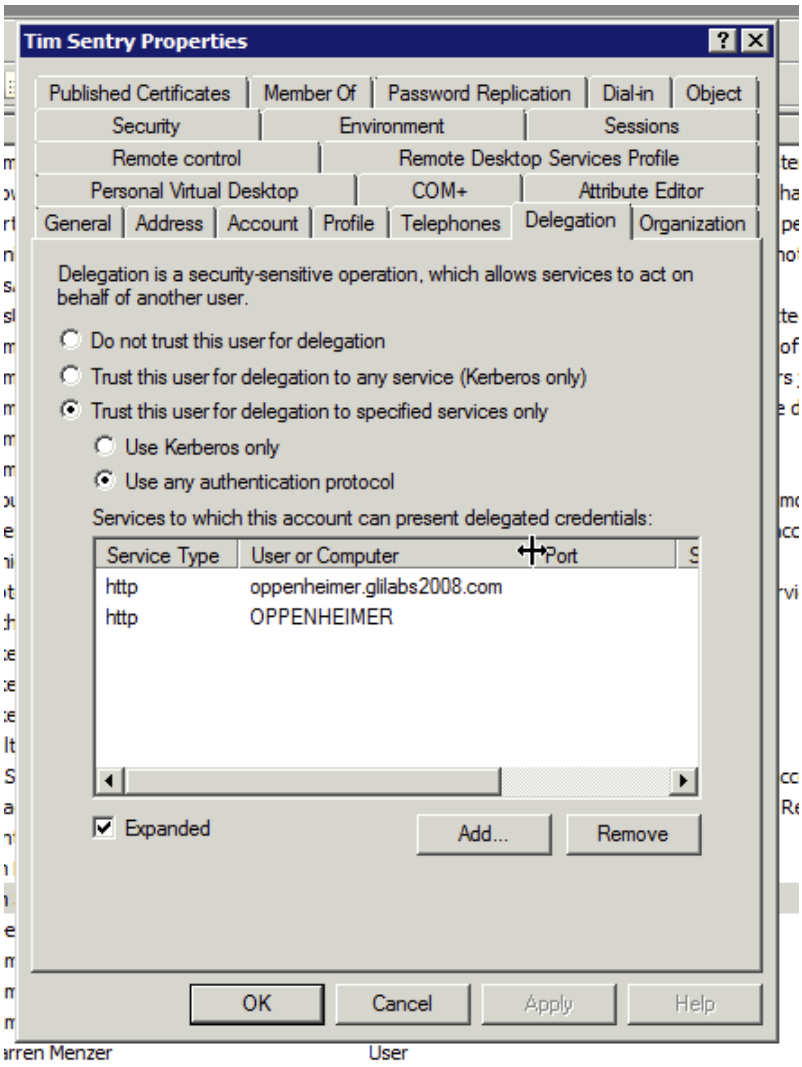
キータブを作成する際、同時に Sentry サービス アカウントが **servicePrincipalName** にマッピングされます。

1. KDC サーバーで、コマンド プロンプト ウィンドウを開きます。
2. プロンプトで、次のコマンドを入力します: **ktpass /out nameofsentry.keytab /mapuser nameofuser@domain /princ HTTP/nameofuser /pass password**

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

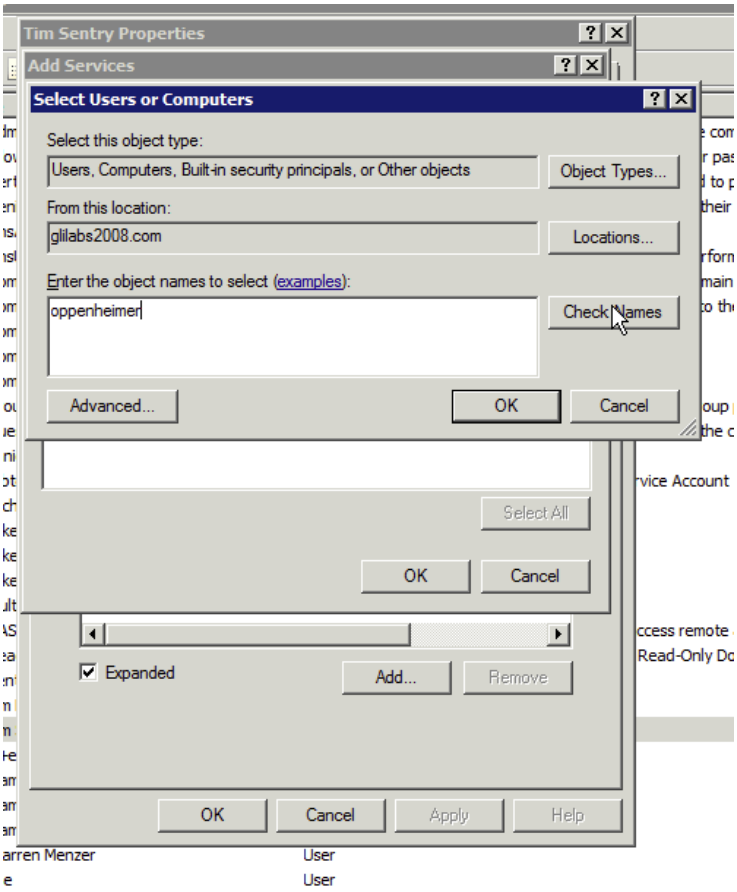
この警告は無視してかまいません。

1. Windows の [スタート] メニューから、**[すべてのプログラム]** を選択し、**[管理ツール]** → **[Active Directory ユーザーとコンピュータ]** の順に開きます。
2. 新しく開いたコンソールで、領域（ドメイン)を展開します。
3. **[ユーザー]** をクリックします。
4. 「Kerberos サービス アカウントの作成」で作成した Kerberos ユーザー アカウントを探して選択します。
5. アカウントを右クリックし、**[プロパティ]** を選択します。
   - **[委任]** タブをクリックします。
   - **[指定されたサービスへの委任でのみこのユーザーを信頼する]** を選択します。
   - **[任意の認証プロトコルを使う]** を選択します。



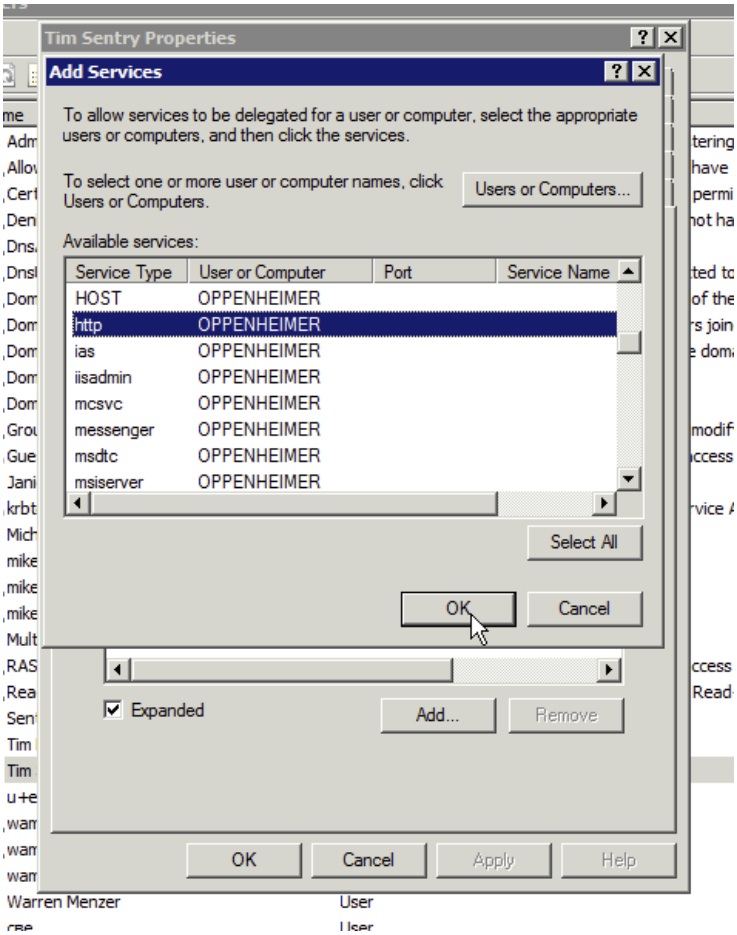
6. **[追加...]** を押します。
7. **[ユーザーまたはコンピュータ]** を押します。

- Files Advanced ゲートウェイサーバーのコンピュータ名を入力します。
- **[名前の確認]** をクリックします。
- 適切なコンピュータ名がオブジェクト名ボックスに表示されます。



8. **[OK]** をクリックします。

9. **[サービスの追加]** ウィンドウで「**http**」サービスを探して選択します。



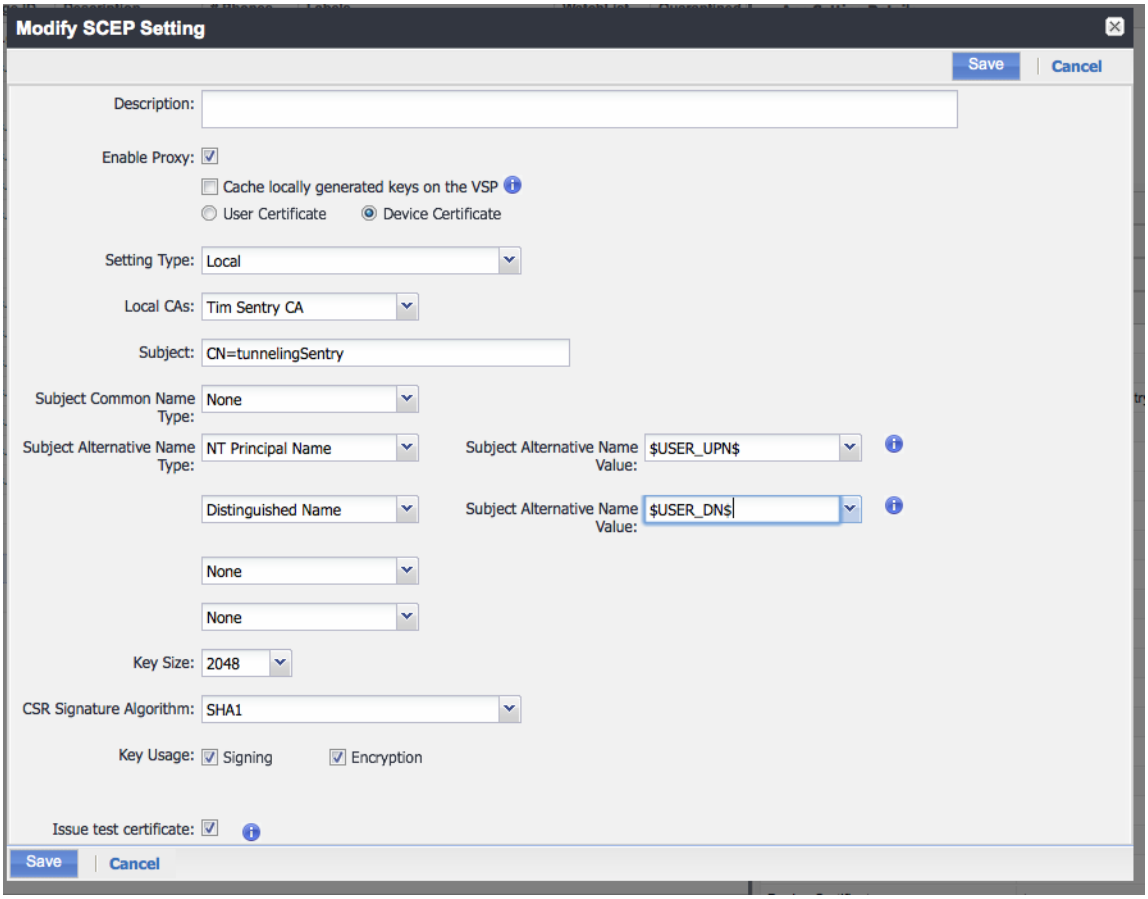
10. **[OK]** をクリックします。

注意: 複数のゲートウェイ サーバーで構成される大規模な展開の場合、ゲートウェイ サーバーごとに手順 6～10 を繰り返す必要があります。ただし、初期設定の場合は、複数のローカル テスト フォルダをホストする単一のゲートウェイ サーバーから始めることをお勧めします。ローカル テスト フォルダへのアクセスを確認した後に、追加のゲートウェイ サーバーおよびローカル フォルダ以外のフォルダへと拡張できます。

---

1. MobileIron VSP Admin Portal を開きます。
2. **[Policies & Configs]** を選択し、**[Configurations]** を開きます。
3. 「新しい SCEP の作成」で作成した SCEP を特定します。

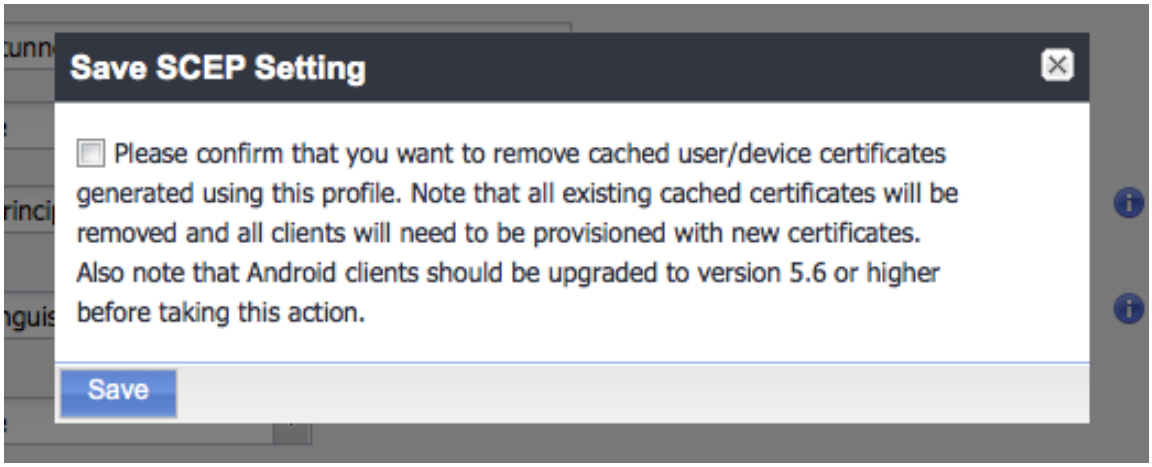
4. SCEP 名をクリックし、右側のパネルの **[編集]** をクリックします。



- 2 つの **[サブジェクト代替名のタイプ]** を入力します。
  - **NT Principal Name**: **$USER_UPN$**
  - **Distinguished Name**: **$USER_DN$**

注意: 上記の各エントリでは、Active Directory から VSP のユーザー アカウントを取得し、各変数に指定する必要があります。具体的な設定方法については、このドキュメントでは割愛いたします。

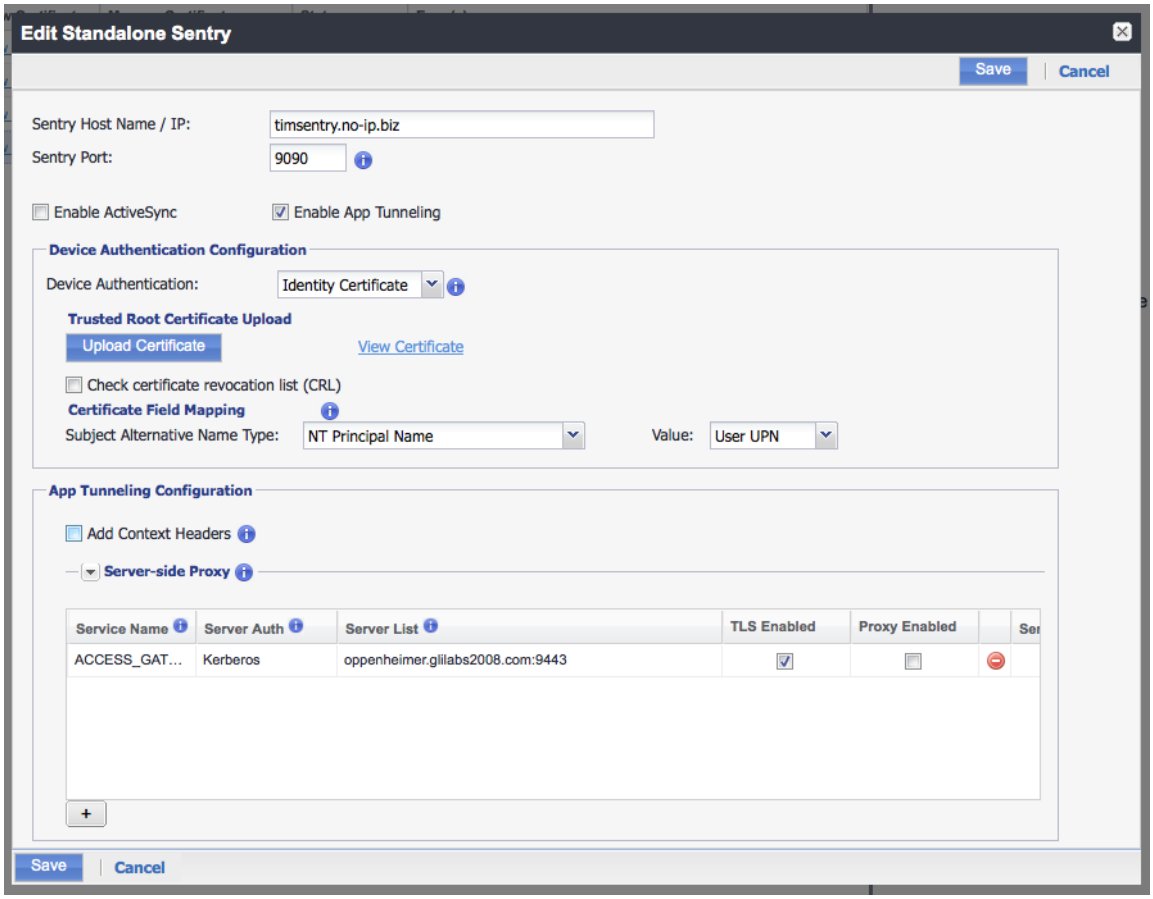
5. **[保存]** をクリックします。



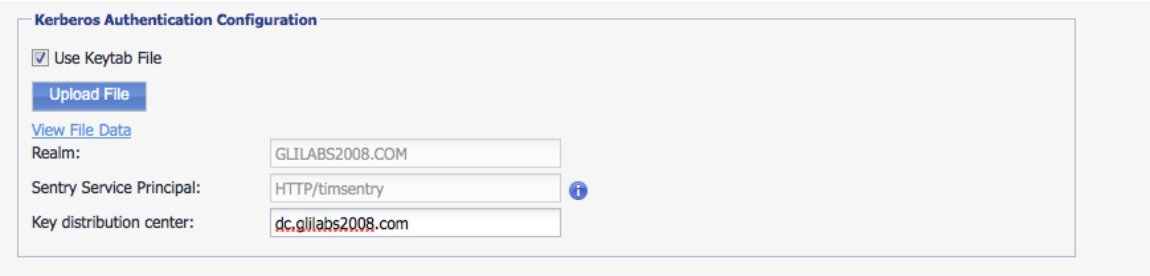
6. SCEP を変更したため、Mobile@Work でデバイスを再プロビジョニングしてから、iOS クライアントをテストする必要があります。

1. MobileIron VSP Admin Portal を開いたまま、**[Settings]** を選択し、**[Sentry]** を開きます。
2. 「Sentry の追加と設定」で作成した **Sentry** を特定します。

3. **[Edit]** アイコンをクリックします。



- **[Device Authentication Configuration]** の **[Certificate Field Mapping]** で次の項目を選択します。
  - **Subject Alternative Name Type**: **NT Principal Name**
  - **Value**: **User UPN**
- **[App Tunneling Configuration]** で、**[Server Authentication]** の値を [Kerberos] に変更します。



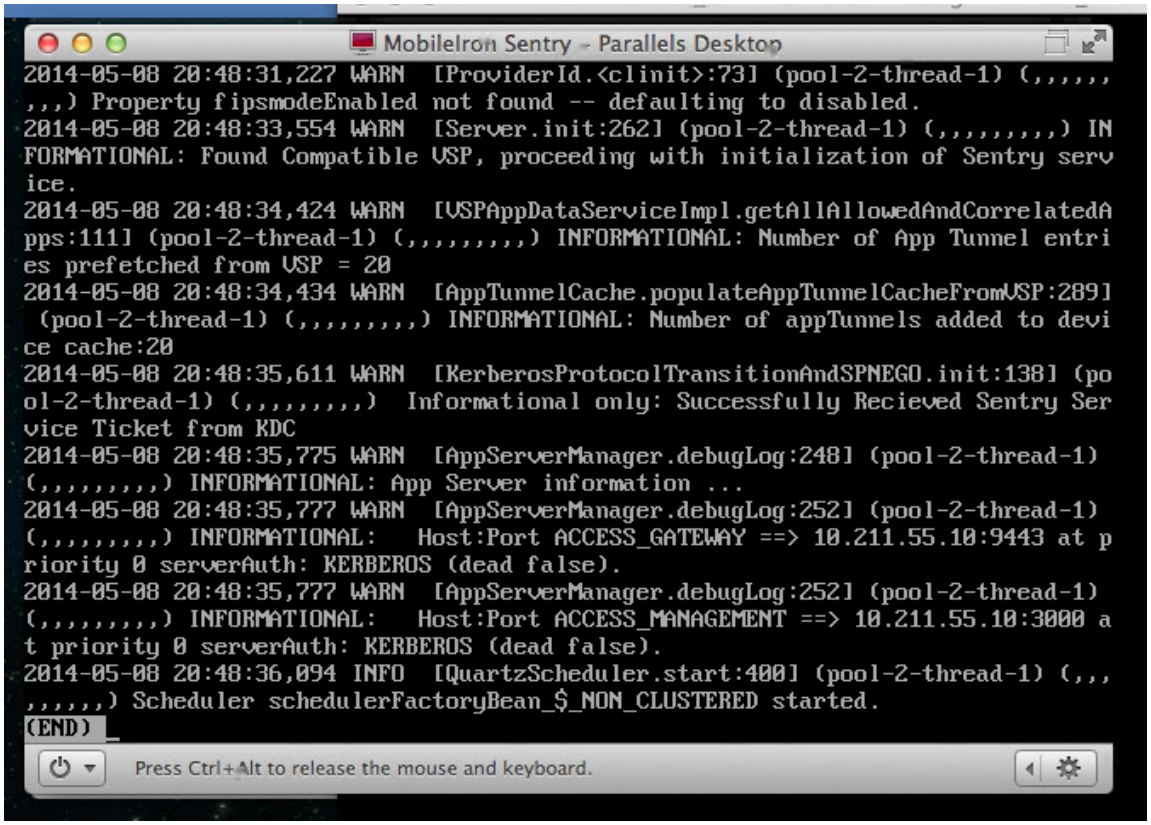
- **[Kerberos Authentication Configuration]** セクションで、次の手順を実行します。
  - **[Use Keytab File]** チェックボックスをオンにします。

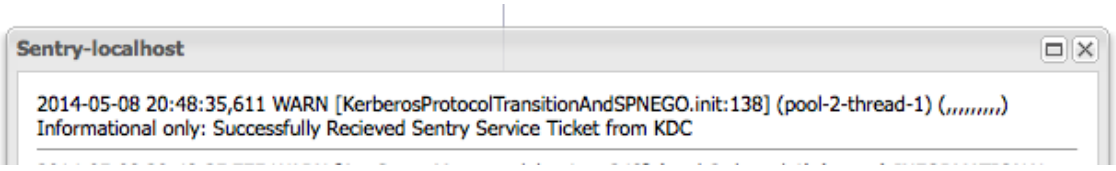
- **[Upload File]** をクリックします。
- 「Kerberos サービス アカウント用のキータブの作成」で作成したキータブ ファイルをアップロードします。
- ドメイン コントローラをキー配布センターに配置します。

4. **[保存]** をクリックします。

[System Manager] の **Sentry EXEC** または Sentry ログを使用して、Sentry が KDC の Kerberos チケットを送受信できているかを確認します。

「**Informational only: Successfully Received Sentry Service Ticket from KDC**」の行を探します。この行が表示されることで、Sentry が KDC に正常に接続して通信できることを確認できます。

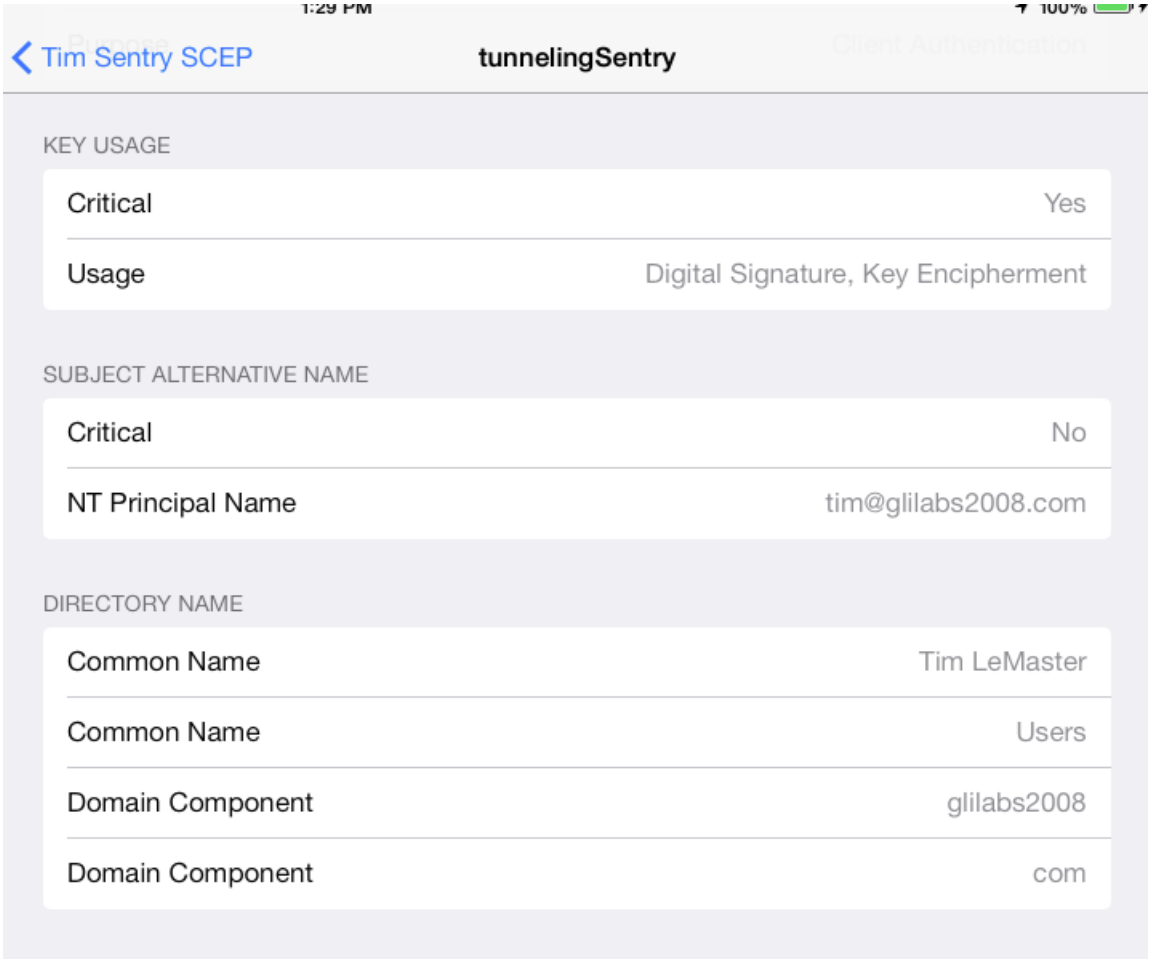




SCEP の変更内容は iOS デバイスに適用する必要があります。Sentry に対して変更を行った場合、変更内容が適用されるまで数分かかることがあります。

デバイスで、[AppConnect app] → [Settings] → [Check for updates] の順に開き、[Re-Enroll Device] をタップして画面の指示に従います。

iOS 設定アプリケーションを使用して、SCEP が適切にアップデートされているかを確認できます。[設定] → [一般] → [プロファイル] → 作成した SCEP 名 → [詳細] → [証明書] → SCEP の対象者名に入力した CN= より後の部分で、[サブジェクト代替名] と [ディレクトリ名] のエントリが表示されます。情報が Active Directory から適切に取得された場合、Mobile@Work のアクティブ化に使用したユーザーと一致します。



取得した情報が正しい場合は、Acronis Files Advanced モバイルを再インストールします。前回と同じ登録手順を繰り返します。ただし、ユーザー名とパスワードのフィールドは空白のままにします。すべて正常に完了すると、先ほど確認したプロファイルの NT プリンシパル名と一致するアカウントを使用して登録されます。

ネットワーク共有と SharePoint での委任

この記事では、ネットワーク共有と SharePoint サイトで MobileIron 資格情報の委任を設定する方法について説明します。このガイドでは、MobileIron および Files Advanced、両者の相互運用性、認証を委任する各 Active Directory アカウントの設定が既に完了していることを前提としています。

ネットワーク共有と SharePoint サーバーの場合の手順

次の手順を実行すると、ゲートウェイ サーバーからターゲット サーバーへの委任が可能になります。

1. **[Active Directory ユーザーとコンピューター]** を開きます。
2. ゲートウェイ サーバーに対応するコンピュータ オブジェクトを特定します。

   注意: User アカウントを使用してゲートウェイサーバーを稼働させている場合は、代わりにその **User** オブジェクトを選択してください。
3. ユーザーを右クリックし、[プロパティ] を選択します。
4. **Delegation** タブを開きます。
5. **[指定されたサービスへの委任でのみこのコンピューターを信頼する]** を選択します。
6. このセクションで、**Use any authentication protocol** を選択します。
7. **Add** をクリックします。
8. **Users or Computers** をクリックします。
9. SMB 共有または SharePoint サーバーのサーバー オブジェクトを検索し、**[OK]** をクリックします。
   - SMB 共有の場合、**[cifs]** サービスを選択します。
   - SharePoint の場合、**[http]** サービスを選択します。
10. Files Advanced ゲートウェイサーバーがアクセスする必要があるサーバーごとに上記の手順を繰り返します。
11. ゲートウェイサーバーごとに上記のプロセスを繰り返します。

委任を変更する場合、ドメインフォレストのサイズによっては、反映が完了するまで数分かかることがあります。変更内容が有効になるまで、15 分程度（場合によっては 15 分以上）待機する必要がある場合があります。15 分経過しても機能しない場合は、Files Advanced ゲートウェイサービスを再起動してください。

14.1.1 Files Advanced for BlackBerry Dynamics

セクションの内容

14.1.1.1 iOS の場合

セクションの内容

はじめに

Files Advanced と BlackBerry Technology が提携することで、Files Advanced のモバイルファイルマネジメントが BlackBerry Dynamics プラットフォームで行えるようになりました。このオプションの Files Advanced 機能により、BlackBerry Dynamics のポリシーとサービスの統一されたセットを使用して、Files Advanced モバイルアプリをその他の BlackBerry 対応アプリと一緒に管理できます。

BlackBerry Dynamics プラットフォームのコンポーネントは次のとおりです。

- **BlackBerry Control サーバー**: サーバーベースのコンソールであり、企業が BlackBerry Dynamics 対応アプリへのクライアント アクセスを有効にできるようにしたり、アプリケーションの権限およびアプリケーションの実行が許可されるデバイス タイプを規定するポリシー セットを作成したり、特定のデバイスで BlackBerry Dynamics アプリへのアクセスを取り消すか BlackBerry Dynamics アプリをワイプできるようにしたりします。
- **BlackBerry Proxy サーバー**: このサービスはオンプレミスサーバーにインストールされます。Files Advanced ゲートウェイサーバーなどのオンプレミスアプリケーション サーバーとの通信を必要とする BlackBerry Dynamics アプリにネットワークアクセスを提供するためにこのサービスを使用します。
- **Files Advanced for BlackBerry Dynamics アプリ** - **Files Advanced for BlackBerry Dynamics** などの BlackBerry Dynamics 対応アプリには BlackBerry Dynamics サービスが組み込まれており、BlackBerry Dynamics プラットフォームを使用してアプリをリモートから管理でき、FIPS 140-2 認定オンデバイス暗号化セキュアストレージおよび BlackBerry セキュア通信をアプリに提供することもできます。

Files Advanced for BlackBerry Dynamics には次のものが必要です。

- **Files Advanced forBlackBerry Dynamics クライアントアプリ** - Apple App Store で入手可能な Files Advanced for BlackBerry Dynamics クライアントアプリ http://www.grouplogic.com/web/megoodappstoreは、BlackBerry Dynamics 統合アプリケーションとして特別に設計されたものです。Files Advanced for BlackBerry Dynamics アプリをデバイスに初めてインストールして実行すると、ユーザーは BlackBerry Dynamics でアプリをアクティブ化するように求められます。ユーザーが Files Advanced サーバーにアプリケーションを登録してファイルにアクセスするには、このアクティブ化が必要です。
- **Files Advanced サーバー**: Files Advanced for BlackBerry Dynamics は、標準の Files Advanced と同じサーバー側ソフトウェアを使用します。サーバー側を変更しなくても、Files Advanced サーバーが BlackBerry Dynamics 対応 Files Advanced クライアントと連動します。これを利用すると、Files Advanced ファイルにアクセスできるすべての Files Advanced を BlackBerry Dynamics で管理できます。

Files Advanced for BlackBerry Dynamics クライアントを BlackBerry Dynamics で登録すると、ゲートウェイサーバーとのすべての通信が BlackBerry Dynamics のセキュア通信チャネル経由でルーティングされます。

試用版の Files Advanced for BlackBerry Dynamics のテスト

Files Advanced for BlackBerry Dynamics の試用プロセスは、標準の Files Advanced の試用とまったく同じです。

1. サーバー側ソフトウェアの試用版は、Acronis のサイトにアクセスして要求できます。この要求フォームを送信すると、Files Advanced サーバー試用版のインストーラをダウンロードするリンクと、初期設定時に参照すると便利な『クイックスタートガイド 『9 ページ 』』へのリンクが記載された電子メールが届きます。
2. Files Advanced for BlackBerry Dynamics クライアントアプリは、Apple App Store http://www.grouplogic.com/web/megoodappstore から無償でダウンロードできます。

注意: ゲートウェイサーバーにアクセスするように Files Advanced for BlackBerry Dynamics クライアントアプリケーションを設定するには、クライアントアプリケーションを BlackBerry Dynamics システムで有効化する必要があります。Files Advanced を BlackBerry Dynamics に登録する準備ができたら、このドキュメントの次のセクションに進んでください。

BlackBerry Control での Files Advanced の要求と構成

Files Advanced for BlackBerry Dynamics クライアント アプリを BlackBerry Dynamics に登録できるようにするには、Files Advanced を BlackBerry Control サーバーの **[管理アプリケーション]** リストに追加する必要があります。このためには、BlackBerry Dynamics の **Communities** サイトを使用して、**Files Advanced for Good** アプリへのアクセスを要求する必要があります。このサイトの登録メンバーでない場合は、組織の別のメンバーがこのサイトにおけるベンダーとの関係を管理することができます。あるいは、BlackBerry へのアカウント登録が必要になる場合があります。

セクションの内容

Files Advanced for BlackBerry へのアクセスを要求するには、BlackBerry Marketplace（https://begood.good.com/marketplace.jspa https://begood.good.com/marketplace.jspa、英語)にアクセスし、利用可能な BlackBerry **Dynamics** アプリのリストから **Files Advanced for** BlackBerry を見つけます。

Files Advanced for https://begood.good.com/gd-app-details.jspa?ID=248978BlackBerry アプリのページで、[試用を開始] ボタンをクリックして試用版のアプリケーションを要求するか、ライセンス版のアプリケーションを入手します。 https://begood.good.com/gd-app-details.jspa?ID=248978

試用版のアプリケーションを選択した場合は、アクセスは数分以内に許可されます。リクエストが受け入れられると、**Files Advanced for** BlackBerry アプリが BlackBerry Control サーバーにパブリッシュされたことを示す通知を BlackBerry サイトから受信します。

注意: アクセス許可を受信しない場合は、BlackBerry Dynamics のサポートにお問い合わせください。

通知を受信したら、BlackBerry Control サーバーにログインし、左側のメニューの **[アプリケーションの管理]** をクリックします。これで、Files Advanced がアプリケーションのリストに表示されます。一覧に表示されていない場合は、15 分ほど待つか、再度確認します。これにより、サーバーに伝搬するための移行時間が与えられます。

Files Advanced が BlackBerry Proxy サーバーを介して Files Advanced ゲートウェイサーバーにアクセスできるようにするには、Files Advanced ゲートウェイサーバーが配置されているドメインへのアクセスを構成する必要があります。これは、Good Control コンソールの **[クライアント接続]** ページで行います。

ドメインからのアクセスの許可

この設定では、すべての BlackBerry クライアントが、指定されたドメインのすべてのサーバーに接続できるようにします。この設定を行わない場合は、代わりに **[その他のサーバー]** を設定します。

1. 左側のメニューから **[クライアント接続]** 設定を開きます。
2. **[許可されたドメイン]** を展開します。**[すべてのドメインを許可]** を有効にしない場合、プラス（+)アイコンを押して、ドメインの名前を入力します（例: mycompany.com)。
3. **[送信]** を押します。

接続のデフォルトドメインとしてのドメインの割り当て

1. **[デフォルトドメイン]** を展開します。
2. プラス（+)アイコンを押して、ドメインの名前を入力します。
3. **[送信]** を押します。

特定のサーバーへの接続の許可

ドメイン内のすべてのサーバーではなく、特定のサーバーのみに Good クライアントを接続する場合は、**[許可されたドメイン]** の代わりに、この設定を使用します。

1. 左側のメニューから **[クライアント接続]** 設定を開きます。
2. **[その他のサーバー]** を展開します。
3. プラス（+)アイコンを押して、アクセスを許可するサーバーの FQDN とポートを入力します。BlackBerry クライアントを接続するすべての Files Advanced サーバーについて、この手順を繰り返します。

BlackBerry Dynamics のポリシーセットと Files Advanced

Files Advanced for BlackBerry Dynamics アプリは、ユーザーに割り当てられた**ポリシーセット**に含まれるポリシー設定に従います。ポリシーセットは BlackBerry Control サーバーで構成されます。

注意: ユーザーの**ポリシーセット**で BlackBerry ポータルの FIPS を有効にすると、Files Advanced アプリは IP アドレスでサードパーティ証明書を使用するゲートウェイサーバーにアクセスできなくなります。

次のような設定があります。

- アプリケーション ロック パスワード要件
- ロック スクリーン ポリシー
- データ漏えいの防止
- 許可されている OS バージョンおよびハードウェアモデル
- 接続確認
- ジェイルブレイク/ルート検出

データ漏えいの防止の効果と制限

ポリシーセットで **[データ漏えいの防止]** を有効にした場合、Files Advanced アプリでは次のことを実行できなくなります。

- デバイスの標準的なサードパーティ製アプリケーションでファイルを開く
- デバイスのその他の標準的なサードパーティ製アプリケーションからファイルを受信する
- デフォルトの電子メールクライアントを使用してファイルを電子メールで送信する
- ファイルを印刷する
- 開いたファイルからテキストをコピーして貼り付ける

これらの機能が必要な場合は、適用される BlackBerry ポリシーセットで **[データ漏えいの防止の無効化]** チェックボックスを有効にする必要があります。

Files Advanced for BlackBerry Dynamics には、「Secure Docs」という BlackBerry Dynamics 機能があります。これにより、Files Advanced for BlackBerry Dynamics アプリと BlackBerry for Enterprise アプリケーションの間でファイルを転送できるようになります。BlackBerry for Enterprise アプリでファイルを一度開くと、その他のサードパーティ製 BlackBerry Dynamics 対応アプリのうち、この機能が組み込まれているものでそのファイルを開くことが可能になります。

BlackBerry Control の**データ漏えいの防止**ポリシー設定を有効にしていても、この機能は使用できます。

BlackBerry Dynamics ユーザーまたはグループに Files Advanced アクセス権を与える

ユーザーは、BlackBerry Dynamics で Files Advanced アプリを登録する前に、ユーザーアカウントの**許可済みアプリケーション**リストまたはユーザーが所属する許可済み**アプリケーショングループ**に Files Advanced アプリケーションを追加する必要があります。また、固有の**アクセス キー**をユーザーに送信し、登録プロセス中に Files Advanced アプリケーションに入力できるようにする必要があります。

展開に関する重要な注意事項: BlackBerry Dynamics アプリケーションへのアクセスを個人ユーザーに割り当てるときには、許可するアプリの特定のバージョン番号を選択する必要があります。ユーザーレベルでアクセスを管理する場合は、Files Advanced for BlackBerry の新バージョンがリリースされたら、ユーザーの BlackBerryControl 構成に戻って新バージョンを追加し、ユーザーがそのバージョンを実行できるようにする必要があります。

BlackBerry Control コンソールの**グループ管理**機能を使用して、BlackBerry Dynamics アプリへのアクセスを許可することを**強くお勧めします**。BlackBerry Control ではアプリのすべてのバージョンへのグループ アクセス権を与えることができるので、IT 管理者が介入せずに今後のバージョンを許可できます。

ユーザーアカウントまたはアプリケーショングループの許可済みアプリケーションリストに Files Advanced アプリケーションを追加するには、次のように操作します。

1. BlackBerry Control コンソールの左側のメニューから **[アプリケーショングループ]** または **[ユーザー管理]** を選択します。
2. Files Advanced for BlackBerry へのアクセス権を付与して編集を許可するグループまたはユーザーを選択します。
3. **[アプリケーション]** セクションで、**[さらに追加]** ボタンをクリックします。
4. 使用可能アプリケーションのリストから **Files Advanced for** BlackBerry を選択し、**[OK]** をクリックします。

ユーザーが **Files Advanced for BlackBerry** アプリを BlackBerry Dynamics に登録できるようにするアクセスキーを生成するには、次のように操作します。

1. BlackBerry Control コンソールの左側のメニューから **[ユーザー管理]** を選択します。
2. **アクセスキー**を作成して編集を許可するユーザーを選択します。
3. **[アクセスキー]** タブで、新しい**アクセスキー**を押します。

ユーザーは、**アクセスキー**および BlackBerry Dynamics の基本的な説明を含む電子メールを受信します。

Files Advanced クライアントアプリを BlackBerry Dynamics に登録する

Apple App Store で利用可能な Files Advanced for http://www.grouplogic.com/web/megoodappstore BlackBerry クライアントアプリ http://www.grouplogic.com/web/megoodappstoreは、BlackBerry Dynamics 統合アプリケーションとして構築されています。デバイスに初めてインストールすると、Files Advanced アプリが起動し、ユーザーに BlackBerry Dynamics システムでアクティブ化するように要求します。

Files Advanced クライアントアプリを **BlackBerry** Dynamics に登録するには、次のように操作します。

注意: [**簡易アクティベーション**] で正常にアクティブ化を行うには、少なくとも 1 つの BlackBerry アプリケーション（BlackBerry Work、BlackBerry Access、または BlackBerry Agent)がインストールされている必要があります。サードパーティ製のアプリケーションを使用して有効化され、以前のバージョンの Files Advanced からアップグレードされたアプリケーションの機能は問題なく使用することができます

---

1. デバイスで **Files Advanced for** BlackBerry **Dynamics** を起動します。
2. IT 管理者が電子メールで送信した**電子メールアドレス**と**アクセスキー**を入力します。
3. アプリが BlackBerry Dynamics に登録される間、進行状況が表示されます。

4. 社内のBlackBerry Dynamicsポリシーによっては、アプリケーションロックパスワードの設定を求めるメッセージが表示される場合があります。BlackBerry for Enterprise も使用している場合、Files Advanced では、BlackBerry for Enterprise にログインして Files Advanced アプリにアクセスしなければならないことがあります。このプロセスが完了すると、Files Advanced アプリケーションのホーム画面が表示されます。

それ以降、Files Advanced アプリを起動すると、以前に設定した Files Advanced for BlackBerry Dynamics アプリケーションパスワードの入力を求められるか、Files Advanced が開く前に BlackBerry for Enterprise で認証を求められることがあります。

このように求められることを除けば、Files Advanced for BlackBerry Dynamics は標準的な Files Advanced アプリと同じように機能します。アプリの一部の機能は、BlackBerry Dynamics ポリシーセットに基づいて制限されることがあります。この制限には、他のサードパーティ製アプリケーションで Files Advanced ファイルを開くこと、ファイルを電子メールで送信したり印刷したりすること、Files Advanced ファイルからテキストをコピーして貼り付けることなどが含まれます。

注意: Files Advanced for BlackBerry Dynamics アプリを BlackBerry Dynamics で有効化すると、無効化できなくなります。Files Advanced の標準バージョンに切り替える必要がある場合は、Files Advanced for BlackBerry Dynamics アプリを削除して、標準の Files Advanced アプリを再インストールする必要があります。

Files Advanced のサイドローディング

Files Advanced アプリの BlackBerry Dynamics バージョンで、**iTunes ファイル共有**機能がサポートされるようになりました。この機能を使用すると、アプリのサンドボックス内の Documents フォルダに、ファイルやフォルダを直接コピーできます。ファイルやフォルダがアプリのサンドボックスに入ると、アプリの暗号化ストレージ内の適切な同期フォルダに自動的にインポートされます。

ファイルのサイドローディングは、デバイス上のストレージ空き容量の制限を受けます。サイドローディング処理を完了するには、インポートされる最大ファイルサイズ以上の追加空き容量が必要になります。この機能は双方向ファイル転送を意図したもので、ユーザーにはファイルの読み取りやコピーの権限は付与されません。

注意: Files Advanced アプリは、iTunes ファイル共有のファイル転送処理に積極的に関与するものではありません。

注意: この手順には、管理登録されていない Files Advanced for BlackBerry Dynamics の新規インストールが必要です。

サイドローディング用のドキュメントの準備

注意: サイドローディングの前には十分なストレージ空き領域があることを確認してください。また、同期処理の開始後は中断しないでください。

1. Files Advanced Advanced ウェブ管理で、[モバイルアクセス]→[データソース] に移動します。
2. 使用するデータソースが既にある場合には、一方向または双方向同期としてマークされていることを確認してください。サイドロードするデータソースがない場合には、新しく作成します。
3. サイドロードを実行する iOS デバイスのユーザーが含まれるグループに、データソースを割り当てます。この例では、Reference という名前でフォルダを作成します。
4. コンピュータ上で、To Import という名前でフォルダを作成し、この中に目的のフォルダをコピーします。この例では、To Import フォルダ内に Reference フォルダが含まれ、Reference フォルダには、サーバーが通常インターネット経由で iOS デバイスに同期しようとするドキュメントが含まれます。

   注意: To Import フォルダ内のフォルダは、データソースの表示名と全く同じ名前にする必要があります。たとえば、Reference というデータソースがある場合には、To Import フォルダ内に Reference という名前でフォルダを作成します。
5. Windows コンピュータでこの手順を実行する場合は、iTunes をインストールする必要があります。

iTunesを介したアイテムの同期

1. Files Advanced for BlackBerry Dynamics アプリをインストールします。
2. ケーブルを使用して、iOS デバイスをコンピュータに接続します。デバイスの充電のみに対応しているケーブルは使用できません。

3. iTunes を開いてデバイスを選択します。信頼するかどうかを確認するプロンプトが表示されたら、コンピュータおよびデバイスで[信頼]をクリックします。
4. iTunes でデバイスアイコンをクリックし、左のサイドバーにある[App]セクションをクリックします。
5. ページの [ファイル共有] セクションまでスクロールダウンし、[Files Advanced] を選択します。
6. 作成済みの To Import フォルダを、iTunes の [Files Advanced ドキュメント] セクションにドラッグします。
7. [同期]をクリックします。必要に応じて、iTunes のその他のプロンプトに従い、同期を完了します。

サイドロードしたドキュメントの登録とインポート

1. iTunes の同期が完了したら、Files Advanced for BlackBerry アプリを起動します。

   注意: Files Advanced アプリが Files Advanced Server に登録される前に、ファイルおよびフォルダのインポートが実行されます。この手順は、クリーンインストールした上で実行する必要があります。

   注意: この機能では、同期フォルダの初回読み込みを実行します。その後は、フォルダ同期の役割が Files Advanced アプリに引き継がれます。以後のすべての同期は通常どおり処理されます。

2. BlackBerry の電子メールアドレスおよびユーザーのアクセスキーを入力します。
3. ウィザードに従って、Files Advancedサーバーでの登録を完了します。Files Advanced ユーザー名とパスワードの入力を求められます。
4. 初回実行時に表示されるチュートリアルを閉じます。
5. インポート処理が開始されます。この時点で、セキュアコンテナにサイドロードされていたドキュメントが、Files Advanced アプリによってインポートされます。その後、サーバーに問い合わせて、対応する同期フォルダと一致するドキュメントが確認されます。すべて同一であれば、サイドロードされた同期フォルダについて、デバイスはサーバーと同期されます。

重要な注意事項

- 指定の同期フォルダが、To Import フォルダ内に対応するフォルダを持たない場合、そのフォルダは無視されます。インポート処理の完了後に、標準的な無線による初回の完全同期が実行されます。
- To Import フォルダ内にあるフォルダが指定のネットワーク同期フォルダに一致しない場合、そのフォルダは無視され、デバイスから削除されます。
- インポートの実行中にアプリの操作から離れた場合、インポートは最大 10 分間バックグラウンドで継続されます。この時間は、Files Advanced による制御ではなく、iOS のアプリの管理で決定されます。Files Advanced アプリが iOS またはエンドユーザーによってシャットダウンされた場合、アプリを次回起動したときに、前回インポート処理が中断した箇所から継続されます。
- 事前に読み込まれたファイルとフォルダが適切な同期フォルダにコピーされると、アプリで無線による同期が実行されます。初回の同期中に、サーバー上のファイルサイズとアプリにサイドロードされたファイルのサイズが同じであれば、最新の状態であると判断されます。ファイルのタイムスタンプの一致は求められません。サイズが一致すれば、サーバー上のバージョンのタイムスタンプと一致するように、ローカルファイルのタイムスタンプがアップデートされます。サイズが一致しない場合、サーバーのファイルで自動的に置き換えられます。競合検出動作はトリガーされません。
- Files Advanced（BlackBerry Control サーバー上)の BlackBerry Dynamics アプリケーションポリシーセクションに、サイドローディング動作をアクティブにするかどうかを決定するポリシー設定が追加されます。デフォルトでは、この機能は無効です。BlackBerry Dynamics ポリシーでこの機能を無効にすると、iTunes ファイル共有経由でドキュメントフォルダにコピーされたすべてのファイルとフォルダは、登録/アクティブ化された Files Advanced for BlackBerry アプリが起動するたびに削除されます。

14.1.1.2 Android の場合

セクションの内容

はじめに

Acronis と BlackBerry Technology が提携することで、Files Advanced のモバイルファイル管理が BlackBerry Dynamics プラットフォームで行えるようになりました。このオプションの Files Advanced 機能により、BlackBerry Dynamics のポリシーとサービスの統一されたセットを使用して、Files Advanced モバイルアプリをその他の BlackBerry 対応アプリと一緒に管理できます。

BlackBerry Dynamics プラットフォームのコンポーネントは次のとおりです。

- **BlackBerry Control サーバー**: サーバーベースのコンソールであり、企業が BlackBerry Dynamics 対応アプリへのクライアント アクセスを有効にできるようにしたり、アプリケーションの権限およびアプリケーションの実行が許可されるデバイス タイプを規定するポリシー セットを作成したり、特定のデバイスで BlackBerry Dynamics アプリへのアクセスを取り消すか BlackBerry Dynamics アプリをワイプできるようにしたりします。
- **BlackBerry Proxy サーバー**: このサービスはオンプレミスサーバーにインストールされます。Files Advanced ゲートウェイサーバーなどのオンプレミスアプリケーション サーバーとの通信を必要とする BlackBerry Dynamics アプリにネットワークアクセスを提供するためにこのサービスを使用します。
- **Files Advanced for BlackBerry Dynamics アプリ** - **Files Advanced for BlackBerry Dynamics** などの BlackBerry Dynamics 対応アプリには BlackBerry Dynamics サービスが組み込まれており、BlackBerry Dynamics プラットフォームを使用してアプリをリモートから管理でき、FIPS 140-2 認定オンデバイス暗号化セキュアストレージおよび BlackBerry セキュア通信をアプリに提供することもできます。

Files Advanced for BlackBerry Dynamics には次のものが必要です。

- **Files Advanced forBlackBerry Dynamics クライアントアプリ** - Apple App Store で入手可能な Files Advanced for BlackBerry Dynamics クライアントアプリ http://www.grouplogic.com/web/megoodappstoreは、BlackBerry Dynamics 統合

アプリケーションとして特別に設計されたものです。Files Advanced for BlackBerry Dynamics アプリをデバイスに初めてインストールして実行すると、ユーザーは BlackBerry Dynamics でアプリをアクティブ化するように求められます。ユーザーが Files Advanced サーバーにアプリケーションを登録してファイルにアクセスするには、このアクティブ化が必要です。

- **Files Advanced サーバー**: Files Advanced for BlackBerry Dynamics は、標準の Files Advanced と同じサーバー側ソフトウェアを使用します。サーバー側を変更しなくても、Files Advanced サーバーが BlackBerry Dynamics 対応 Files Advanced クライアントと連動します。これを利用すると、Files Advanced ファイルにアクセスできるすべての Files Advanced モバイルクライアントを BlackBerry Dynamics で管理できます。

Files Advanced for BlackBerry Dynamics クライアントを BlackBerry Dynamics で登録すると、ゲートウェイサーバーとのすべての通信が BlackBerry Dynamics のセキュア通信チャネル経由でルーティングされます。

BlackBerry Control での Files Advanced の要求と構成

Files Advanced for BlackBerry Dynamics クライアント アプリを BlackBerry Dynamics に登録できるようにするには、Files Advanced を BlackBerry Control サーバーの **[管理アプリケーション]** リストに追加する必要があります。このためには、BlackBerry Dynamics の **Communities** サイトを使用して、**Files Advanced for Good** アプリへのアクセスを要求する必要があります。このサイトの登録メンバーでない場合は、組織の別のメンバーがこのサイトにおけるベンダーとの関係を管理することができます。あるいは、BlackBerry へのアカウント登録が必要になる場合があります。

セクションの内容

Files Advanced for BlackBerry へのアクセスを要求するには、BlackBerry Marketplace（https://begood.good.com/marketplace.jspa https://begood.good.com/marketplace.jspa、英語)にアクセスし、利用可能な BlackBerry **Dynamics** アプリのリストから **Files Advanced for** BlackBerry を見つけます。

Files Advanced for https://begood.good.com/gd-app-details.jspa?ID=248978BlackBerry アプリのページで、[試用を開始] ボタンをクリックして試用版のアプリケーションを要求するか、ライセンス版のアプリケーションを入手します。https://begood.good.com/gd-app-details.jspa?ID=248978

試用版のアプリケーションを選択した場合は、アクセスは数分以内に許可されます。リクエストが受け入れられると、**Files Advanced for** BlackBerry アプリが BlackBerry Control サーバーにパブリッシュされたことを示す通知を BlackBerry サイトから受信します。

注意: アクセス許可を受信しない場合は、BlackBerry Dynamics のサポートにお問い合わせください。

通知を受信したら、BlackBerry Control サーバーにログインし、左側のメニューの **[アプリケーションの管理]** をクリックします。これで、Files Advanced がアプリケーションのリストに表示されます。一覧に表示されていない場合は、15 分ほど待つか、再度確認します。これにより、サーバーに伝搬するための移行時間が与えられます。

Files Advanced が BlackBerry Proxy サーバーを介して Files Advanced ゲートウェイサーバーにアクセスできるようにするには、Files Advanced ゲートウェイサーバーが配置されているドメインへのアクセスを構成する必要があります。これは、Good Control コンソールの **[クライアント接続]** ページで行います。

ドメインからのアクセスの許可

この設定では、すべての BlackBerry クライアントが、指定されたドメインのすべてのサーバーに接続できるようにします。この設定を行わない場合は、代わりに **[その他のサーバー]** を設定します。

1. 左側のメニューから **[クライアント接続]** 設定を開きます。
2. **[許可されたドメイン]** を展開します。**[すべてのドメインを許可]** を有効にしない場合、プラス（+)アイコンを押して、ドメインの名前を入力します（例: mycompany.com)。
3. **[送信]** を押します。

接続のデフォルトドメインとしてのドメインの割り当て

1. **[デフォルトドメイン]** を展開します。
2. プラス（+)アイコンを押して、ドメインの名前を入力します。
3. **[送信]** を押します。

特定のサーバーへの接続の許可

ドメイン内のすべてのサーバーではなく、特定のサーバーのみに Good クライアントを接続する場合は、**[許可されたドメイン]** の代わりに、この設定を使用します。

1. 左側のメニューから **[クライアント接続]** 設定を開きます。
2. **[その他のサーバー]** を展開します。
3. プラス（+)アイコンを押して、アクセスを許可するサーバーの FQDN とポートを入力します。BlackBerry クライアントを接続するすべての Files Advanced サーバーについて、この手順を繰り返します。

BlackBerry Dynamics のポリシーセットと Files Advanced

Files Advanced for BlackBerry Dynamics アプリは、ユーザーに割り当てられた**ポリシーセット**に含まれるポリシー設定に従います。ポリシーセットは BlackBerry Control サーバーで構成されます。

注意: ユーザーの**ポリシーセット**で BlackBerry ポータルの FIPS を有効にすると、Files Advanced アプリは IP アドレスでサードパーティ証明書を使用するゲートウェイサーバーにアクセスできなくなります。

次のような設定があります。

- アプリケーション ロック パスワード要件
- ロック スクリーン ポリシー
- データ漏えいの防止
- 許可されている OS バージョンおよびハードウェアモデル
- 接続確認
- ジェイルブレイク/ルート検出

データ漏えいの防止の効果と制限

ポリシーセットで **[データ漏えいの防止]** を有効にした場合、Files Advanced アプリでは次のことを実行できなくなります。

- デバイスの標準的なサードパーティ製アプリケーションでファイルを開く
- デバイスのその他の標準的なサードパーティ製アプリケーションからファイルを受信する
- デフォルトの電子メールクライアントを使用してファイルを電子メールで送信する
- ファイルを印刷する
- 開いたファイルからテキストをコピーして貼り付ける

これらの機能が必要な場合は、適用される BlackBerry ポリシーセットで **[データ漏えいの防止の無効化]** チェックボックスを有効にする必要があります。

Files Advanced for BlackBerry Dynamics には、「Secure Docs」という BlackBerry Dynamics 機能があります。これにより、Files Advanced for BlackBerry Dynamics アプリと BlackBerry for Enterprise アプリケーションの間でファイルを転送できるようになります。BlackBerry for Enterprise アプリでファイルを一度開くと、その他のサードパーティ製 BlackBerry Dynamics 対応アプリのうち、この機能が組み込まれているものでそのファイルを開くことが可能になります。

BlackBerry Control の**データ漏えいの防止**ポリシー設定を有効にしていても、この機能は使用できます。

BlackBerry Dynamics ユーザーまたはグループに Files Advanced アクセス権を与える

ユーザーは、BlackBerry Dynamics で Files Advanced アプリを登録する前に、ユーザーアカウントの**許可済みアプリケーション**リストまたはユーザーが所属する許可済み**アプリケーショングループ**に Files Advanced アプリケーションを追加する必要があります。また、固有の**アクセス キー**をユーザーに送信し、登録プロセス中に Files Advanced アプリケーションに入力できるようにする必要があります。

展開に関する重要な注意事項: BlackBerry Dynamics アプリケーションへのアクセスを個人ユーザーに割り当てるときには、許可するアプリの特定のバージョン番号を選択する必要があります。ユーザーレベルでアクセスを管理する場合は、Files Advanced for BlackBerry の新バージョンがリリースされたら、ユーザーの BlackBerryControl 構成に戻って新バージョンを追加し、ユーザーがそのバージョンを実行できるようにする必要があります。

BlackBerry Control コンソールの**グループ管理**機能を使用して、BlackBerry Dynamics アプリへのアクセスを許可することを**強くお勧めします**。BlackBerry Control ではアプリのすべてのバージョンへのグループ アクセス権を与えることができるので、IT 管理者が介入せずに今後のバージョンを許可できます。

ユーザーアカウントまたはアプリケーショングループの許可済みアプリケーションリストに Files Advanced アプリケーションを追加するには、次のように操作します。

1. BlackBerry Control コンソールの左側のメニューから **[アプリケーショングループ]** または **[ユーザー管理]** を選択します。
2. Files Advanced for BlackBerry へのアクセス権を付与して編集を許可するグループまたはユーザーを選択します。
3. **[アプリケーション]** セクションで、**[さらに追加]** ボタンをクリックします。
4. 使用可能アプリケーションのリストから **Files Advanced for** BlackBerry を選択し、**[OK]** をクリックします。

ユーザーが **Files Advanced for BlackBerry** アプリを BlackBerry Dynamics に登録できるようにするアクセスキーを生成するには、次のように操作します。

1. BlackBerry Control コンソールの左側のメニューから **[ユーザー管理]** を選択します。
2. **アクセスキー**を作成して編集を許可するユーザーを選択します。
3. **[アクセスキー]** タブで、新しい**アクセスキー**を押します。

ユーザーは、**アクセスキー**および BlackBerry Dynamics の基本的な説明を含む電子メールを受信します。

14.1.2 Microsoft Intune

Microsoft Intune は、モバイルデバイス、モバイルアプリケーション、および PC をクラウドから管理する機能を提供します。組織で Intune を利用すると、社内情報をセキュリティで保護しながら、従業員がほぼすべてのデバイスで、事実上どこからでも、社内のアプリケーション、データ、およびリソースにアクセスできるようになります。モバイルデバイスを登録するためには、Intune をモバイルデバイスの機関として設定し、管理を必要とするプラットフォームをサポートするようにインフラストラクチャを設定する必要があります。これには、デバイスとの信頼関係の確立が必要になります。

注意: この機能は、Files Advanced iOS クライアント、バージョン 7.0.5 以降でのみサポートされています。

注意: デバイスポリシーを適用するには、**Microsoft Intune Company Portal** を使用して **Files Advanced** をインストールし、Files Advanced の **[デフォルトのアクセス制限]**（**[モバイルアクセス]** -> **[ポリシー]** -> **[デフォルトのアクセス制限]**）または各ゲートウェイの［アクセス制限］で **[Intune が管理する iOS クライアントを許可]** と **[「iOS 管理対象アプリ」iOS クライアントを許可]** を有効にする必要があります。

注意: [アプリケーションポリシー] を適用し、Files Advanced を Intune で管理するには、Files Advanced サーバーから **[Intune Mobile Application Management の登録をトリガーする] を有効にする必要があります**（**[モバイルアクセス]** -> **[ポリシー]** -> **[サーバーポリシー]**）。

セクションの内容

14.1.2.1 Active Directory グループの作成

1. Microsoft Azure ポータルを開きます。
2. **[すべてのサービス]** をクリックし、検索ボックスに「**azure**」と入力して **[Azure Active Directory]** を選択します。
3. **[グループ]** を開き、**[新しいグループ]** を選択して、必要な情報を入力します。
4. グループの目的のメンバーを選択し、**[作成]** を押します。

14.1.2.2 Intune への Files Advanced アプリケーションの追加

Intune の**デバイスポリシー**を使用する場合、Intune 社内ポータルから Files Advanced をインストールする必要があります。

これを実行するには、まず Files Advanced アプリをポータルに追加する必要があります。

1. Microsoft Azure ポータルを開きます。
2. **[すべてのサービス]** をクリックし、検索ボックスに「**Intune**」と入力して **[Microsoft Intune]** を選択します。
3. Intune ポータルで、**[Mobile Apps]** を開いてから **[アプリ]** を開きます。
4. **[追加]** を押して、**[アプリの追加]** オプションを選択します。
   - **[アプリの種類]** で **[iOS]** を選択します。
   - **[アプリストアを検索]** をクリックし、**Files Advanced** を検索します。アプリを選択します。
   - **[アプリ情報]** をクリックして、希望する構成変更を行います。

5. **[会社のポータルでおすすめアプリとして表示します]** を有効にし、**[OK]** を押してアプリの追加を終了します。
6. リストのアプリをクリックし、**[割り当て]** を選択します。
7. このアプリに割り当てるユーザーまたはグループを選択します。

14.1.2.3 デバイスポリシーの作成

1. Microsoft Azure ポータルを開きます。
2. **[すべてのサービス]** をクリックし、検索ボックスに「**Intune**」と入力して [Microsoft Intune] を選択します。
3. **[デバイス構成]** -> **[プロファイル]** を開き、**[プロファイルの作成]** を選択します。
4. 名前を入力し、**[プラットフォーム]** として **[iOS]** を選択して、デバイスに適用する制限を選択します。
5. Files Advanced アプリでは、次の制限のみをサポートします。
   - **アプリ ストア、ドキュメント表示、ゲーム -> 管理対象外のアプリでの社内ドキュメントの表示**。管理対象アプリの **[他のアプリで開く]/[他のアプリに保存]** リストに管理対象外アプリを表示させたくない場合、このオプションの **[ブロック]** を選択します。
   - **アプリ ストア、ドキュメント表示、ゲーム -> 社内アプリでの社外ドキュメントの表示**。管理対象外アプリの **[他のアプリで開く]/[他のアプリに保存]** リストに管理対象アプリを表示させたくない場合、このオプションの **[ブロック]** を選択します。
6. アプリがリストに追加されたら、そのアプリをタップして、**[割り当て]** を選択し、割り当てるユーザー/グループを選択します。

デバイスポリシー**をアプリに割り当てるには、社内ポータルからそのアプリをダウンロードする必要があります。**

14.1.2.4 アプリ保護ポリシーの作成

注意: このポリシーは、モバイルアプリ管理ポリシーとしても機能します。

1. Microsoft Azure ポータルを開きます。
2. **[すべてのサービス]** をクリックし、検索ボックスに「**Intune**」と入力して **[Microsoft Intune]** を選択します。

3. **[モバイルアプリ]** を開き、**[アプリ保護ポリシー]** を開きます。
4. **[ポリシーの追加]** を選択し、ポリシーの名前を入力して、必須アプリとして **Files Advanced** を選択します。
5. **[設定]** をタップし、適用する保護ポリシーを選択します。
6. アプリがリストに追加されたら、そのアプリをタップして、**[割り当て]** を選択し、割り当てるユーザー/グループを選択します。

注意: [アプリがデータを他のアプリに転送することを許可する]/[アプリで他のアプリからのデータの受信を許可する] を **[ポリシーで管理されているアプリ]** に設定した場合、**Files Advanced ドキュメントプロバイダ拡張機能**がその他の Microsoft Intune 管理対象アプリで動作するように、**IntuneMAMUPN** キーを使用して**アプリ構成ポリシー**を Intune 管理対象アプリと Files Advanced アプリの両方に適用します。ただし、**IntuneMAMUPN** キーを持つポリシーが存在する場合、[アプリがデータを他のアプリに転送することを許可する]/[アプリで他のアプリからのデータの受信を許可する] のオプションが機能しなくなります。

ファイルをポリシー管理対象アプリに制限するアプリ保護ポリシーを書き込みます。その他の Microsoft Intune 管理対象アプリで Files Advanced ドキュメントプロバイダ拡張機能が機能するように、IntuneMAMUPN キーを使用してアプリ構成ポリシーを Intune 管理対象アプリと Files Advanced アプリの両方に適用する必要があります。ただし、デバイスが IntuneMAMUPN キーを持つ MDM の管理対象と見なされる場合、アプリ保護ポリシーの [アプリがデータを他のアプリに転送することを許可する] 設定が無効になり、MDM 構成の [管理対象外のアプリでの社内ドキュメントの表示] 設定が有効になります。ファイルがポリシー管理対象アプリに正しく制限されるように、デバイスポリシーを適用してください。

注意: Files Advanced から Word（またはその他の Microsoft アプリ)でファイルを開くには、目的の Microsoft アプリケーション用に別の Intune **アプリ保護ポリシー**を用意する必要があります。また、**[すべての種類を対象とする]** を **[はい]** に設定する必要があります。

14.1.2.5 アプリ構成ポリシーの作成

Intune の資格情報で自動的に登録するには、**[アプリ構成ポリシー]** を作成するか、以下の変更を既存のポリシーに追加する必要があります。

1. Microsoft Azure ポータルを開きます。
2. **[すべてのサービス]** をクリックし、検索ボックスに「**Intune**」と入力して **[Microsoft Intune]** を選択します。
3. **[モバイルアプリ]** を開き、**[アプリ構成ポリシー]** を開きます。

4. **[追加]** を押して、ポリシーの名前を入力します。
5. **[デバイス登録の種類]** として **[マネージド デバイス]**、**[プラットフォーム]** として **[iOS]** を選択し、この構成に配置する必要なアプリを選択します。
6. **[構成]** 設定では、**[XML]** または **[構成デザイナー]** の 2 つのオプションから選択できます。
   - **[XML]** を選択する場合、次のように入力します。

```
<dict>
<key>IntuneMAMUPN</key>
<string>{{userprincipalname}}</string>
</dict>
```

   - **[構成デザイナー]** を選択する場合、次のように入力します。
     - **[構成キー]** には、「**IntuneMAMUPN**」と入力します。
     - **[構成値]** には、「**{{userprincipalname}}**」と入力します。
     - **[値の型]** には **[文字列]** を選択します。
7. Files Advanced の資格情報で自動登録する場合、**[XML]** で次のキーを使用できます。

```
<dict>
<key>enrollmentServerName</key>
<string>192.168.1.10</string>
<key>enrollmentUserName</key>
<string>jprice</string>
<key>enrollmentPassword</key>
<string>password123</string>
<key>enrollmentAutoSubmit</key>
<string>Yes</string>
</dict>
```

8. アプリがリストに追加されたら、そのアプリをタップして、**[割り当て]** を選択し、割り当てるユーザー/グループを選択します。

15 新機能

セクションの内容

15.1 Files Advanced サーバー

注意: 「[ASRV-2345, DE1013, US552]」などの数値は、Acronis の内部的な変更履歴システムを示しています。

Files Advanced の最新バージョンに含まれているものは次のとおりです: **Tomcat** バージョン**:** 7.0.82、**Java** バージョン**:** 8u144、**PostgreSQL** バージョン**:** 9.4

Files Advanced では、各リリースに組み込まれているバージョンより新しいバージョンの Tomcat、Java、および PostgreSQL はサポートされません。特定のバージョンに関する情報が必要な場合は、アクロニスサポートまでご連絡ください。

Files Advanced 8.1.1（リリース: 2018年7月26日)

機能強化:

- ファイルを完全に削除できるようになりました。削除したファイルは復元できません。すべての削除は、監査ログに記録されます。
- アクティブ化と通知の電子メールのヘッダーに「送信者」、「送信元」、「返信先」のデータが含まれるように改善されました。この変更により、クライアントのサーバーによってスパムとしてマークが付けられる電子メールの割合が低くなります。
- 4GB 以上の単一ファイルを含むフォルダをダウンロードできる機能が追加されました。
- [デバイス] ページで最新の Windows OS バージョンを検出する機能が追加されました。

バグ修正:

- 共有のメンバーに [メンバーを表示できる] アクセス許可が付与されている場合、通知電子メールでファイルを変更したユーザーの名前が表示されるようになりました。
- 8.0 へのアップグレード後に失われていた古い電子メールテンプレートメソッドのサポートが追加されました。
- Windowsデスクトップクライアントのバイナリおよびサービス名が新しい製品名に変更されました。
- 同期ネットワーク共有のルートにあるファイル/フォルダの名前を変更しても、内部サーバーエラーが発生しなくなりました。

Files Advanced 8.1（リリース: 2018年3月14日)

Acronis Access Advanced は Files Advanced にリブランドされました。

機能強化:

- 新しいモバイルポリシー設定で、モバイルクライアントにダウンロードを許可する最大ファイルサイズを制御できます。[ASRV-5838]
- ネットワーク共有に配置された以下の Windows .lnk ショートカットに対するサポートが追加されました。[ASRV-5837]
- ユーザーを削除すると、そのユーザーのデバイスも [デバイス] ページから削除されるようになりました。[ASRV-5845]
- 含まれる Java のバージョンが 8u162 に更新されました。[ASRV-3410]
- 大規模デプロイでの LDAP パフォーマンスが向上しています。[ASRV-6012]、[ASRV-6011]

バグ修正:

- 同期中にフォルダ名の競合が発生するとデスクトップクライアントでエラーが発生する場合があるという問題が修正されました。[ASRV-5768]
- 外部ユーザーが共有リンクにアクセスする前に適切にリダイレクトされて、そのユーザーのアカウントを検証できるようになりました。[ASRV-5304]
- "**[管理画面を閉じる]** は、同期・共有アクセス権を持たないユーザーには表示されなくなりました。[ASRV-6062]

- デバイスリストまたは招待リストのエクスポートに関する問題が修正されました。[ASRV-5802]

Acronis Access 8.0.1（リリース: 2017年12月21日)

機能強化:

- Tomcat のバージョンが 7.0.82 にアップグレードされました。
- Java のバージョンが 8u144 にアップグレードされました。

バグ修正:

- Office Online での編集中にファイルの変更を保存する際の信頼性が向上しました。
- サイズの大きいファイルでドラッグアンドドロップ操作が機能しない場合があるという問題が修正されました。
- ファイルの名前を変更する際に Delete キーでファイル削除操作をトリガーしてしまう場合があるという問題が修正されました。
- Mac および PC デスクトップ同期クライアント上でのコンテキストメニュー項目に関するいくつかの問題が修正されました。
- 管理者により制限された IP アドレス範囲形式が原因でエラーが発生する場合があるという問題が修正されました。
- その他複数のバグ修正および最適化

Acronis Access 8.0（リリース: 2017年9月21日)

Acronis Access 8.0 以降では Internet Explorer 8 をサポートしていません。Acronis Access 7.5 が Internet Explorer 8 をサポートする最後のバージョンです。

機能強化:

- ウェブクライアント内から **Office Online** を使用してファイルの表示と編集を行えるようにする、オプションの Microsoft Office Online 統合のサポートが追加されました。Office Online は **DOCX**、**XLSX** および **PPTX** ファイルをサポートします。**DOC**、**XLS** および **PPT** ファイルもサポートされていますが、編集する場合は新しい

フォーマットに変換する必要があります。オンプレミスインストールの場合、この機能を利用するには Office Online Server が使用可能でなければなりません。[ASRV-357]、[ASRV-4714]、[ASRV-4664]

- 新しい Office ファイルをウェブクライアントで作成し、Office Online で編集することができるようになりました。
- ウェブクライアントでの項目選択チェックボックス、Shift および command/Ctrl キーボードを使用した複数選択のサポートが追加されました。[ASRV-4723]、[ASRV-353]
- 同期・共有の既存の共有フォルダのサブフォルダを、個々の利用者と個別に共有できるようになりました。[ASRV-1635]
- 同期・共有のルートレベルの共有フォルダのサブフォルダを、デスクトップクライアントと同期できるようになりました。
- Intune Mobile Application Management への Acronis Access iOS アプリの登録を開始および要求するモバイルポリシー設定が追加されました。これにより、Acronis Access iOS アプリを、モバイルデバイスを Intune MDM で管理することなく Intune MAM 適用済みにすることができます。[ASRV-4510]
- アップグレードインストール中に、必須のデータベース移行が実行されることによってアップグレードにかかる時間が長くなる可能性があることが、管理者に通知されるようになりました。[ASRV-5269]

バグ修正:

- デスクトップクライアント同期の信頼性が改善しました。
- ウェブクライアントで中国語文字でのフォルダの並び替えの問題が修正されました。[ASRV-4487]
- ローカリゼーションに関するその他の修正。

Acronis Access 7.5.4（リリース: 2017年5月19日)

バグ修正:

- 共有フォルダに追加されたファイルが所有者以外のメンバーに表示されないという問題が修正されました。

- 共有フォルダの所有者以外のメンバーが共有するダウンロードリンクが正常に機能しない場合があるという問題が修正されました。
- ファイル消去プロセスでエラーが発生する場合があるという問題が修正されました。

Acronis Access 7.5.3（リリース: 2017年4月21日)

バグ修正:

- その他複数のバグ修正および最適化
- Mac OS 10.9 でのデスクトップ同期クライアントの問題が修正されました

Acronis Access 7.5.2（リリース: 2017年2月11日)

バグ修正:

- ウェブ管理コンソールで管理者ユーザーが重複表示される問題が修正されました。
- Tomcat の設定がアップグレード時に未サポートの値に変更され、サービス上の問題を引き起こす可能性のある問題が修正されました。

Acronis Access 7.5.1（リリース: 2017年1月25日)

バグ修正:

- [カスタム] カラースキームオプションを使用している場合にウェブ UI 内の検索フィールドが正しく配置されない問題が修正されました。
- ウェブ管理コンソールの監査ログページでのページングに伴う問題が修正されました。
- 期限切れの共有フォルダを含む同期・共有ストレージの参照中に発生する可能性のある「内部エラー」が修正されました。
- ゲートウェイ CURL 接続エラーのログが WARN レベルから DEBUG レベルに変更されました。
- SMS 2 要素認証の互換性が改善されました。

Acronis Access 7.5（リリース: 2017年1月12日)

機能強化:

- バージョン 6.0 より前のバージョンから Acronis Access Advanced 7.5 にアップグレードするには、アップグレードの前にいくつかの追加の手順を実行する必要があります。このアップグレードを実行するには、詳細についてアクロニスモビリティサポートまでお問い合わせください。[ASRV-350]
- ウェブクライアントとデスクトップクライアントがスペイン語にローカライズされました。
- Microsoft Azure Storage が、同期・共有のファイルリポジトリの場所としてサポートされるようになりました。[ASRV-3489]
- Web クライアントログインの SMS 2 要素認証のオプションが、今回のリリースに組み込まれました。AD の携帯電話番号またはユーザーが指定した電話番号を使用するオプションが提供されます。2 要素認証は、毎回のログイン時、指定した期間の経過後、または新しいブラウザからのログイン時のみに要求することができます。SMS コードの送信には、Twilio SMS メッセージングサービスでアカウントを確立しておくことが必要になります。[ASRV-296]
- ウェブクライアントで、ファイルとフォルダの検索を利用できるようになりました。ファイルタイプに基づいて結果をフィルタリングするオプションとして、ファイルの更新日とファイルの所有者があります。Windows Search が有効にされた Windows ファイルサーバーのネットワークデータソースでも、ファイル名またはファイルコンテンツによって検索するオプションを表示します。[ASRV-1421]
- Windows Search が有効にされた Windows ファイルサーバーのデータソースからファイルの内容を検索すると、ファイルの内容に加えて、Windows のエクスプローラのタグに基づく一致も返されるようになりました。これは、ウェブクライアントまたはモバイルアプリからの検索に適用されます。[ASRV-4221]
- ウェブ管理コンソールに移動する [管理画面] リンクが、ウェブクライアントの最上位レベルから [ユーザーメニュー] に移されました。管理者権限を持つユーザーには、右下に星印の付いた新しいユーザーアイコンがウェブ UI に表示されます。[ASRV-4093]

- 管理コンソールのすべての「Good Dynamics」設定は、「Blackberry Dynamics」という名前に変更されました。[ASRV-4074]
- モバイルゲートウェイに新しい [アクセス制限] オプションが追加され、近日中にリリースされる Android アプリ Acronis Access for Blackberry Dynamics からの接続を許可または拒否できます。[ASRV-3795]
- 追加された新しいモバイルポリシーオプションにより、組み込み PDF ビューアによって提供される検索結果の表示形式を設定できます。[ASRV-3791]
- 追加された新しいモバイルポリシーオプションにより、パスワードで保護された Office ファイルの編集を許可または拒否できます。パスワードで保護された Office ファイルの表示と編集は、近日中にリリースされるバージョンの Access Advanced モバイルクライアントでサポートされるようになります。パスワードで保護されたファイルを編集した場合、保存時にパスワードが削除されます。この理由から、この機能はデフォルトでは無効になっていますが、必要であれば有効にすることができます。[ASRV-3729]
- ウェブクライアントで表示する Office ファイルをレンダリングするために従来のリリースで使用されていた LibreOffice サービスは、レンダリング用の新しい内部ライブラリに置き換えられ、パフォーマンスが向上しました。ファイルは増分方式でレンダリングされるため、表示の応答性が良くなりました。LibreOffice サービスは、バージョン 7.5 以降にアップグレードする際に自動的にアンインストールされます。[ASRV-3867]
- ユーザーのアカウントを削除した時点でそのユーザーの同期・共有コンテンツを直ちに削除するオプションが追加されました。[ASRV-2848]
- 共有している同期・共有フォルダの所有者が、ウェブクライアントで共有フォルダのアイコンにマウスカーソルを置くと表示されるようになりました。[ASRV-3123]
- 同期・共有の [削除済みを表示] モードで、フォルダのすべてのコンテンツがサーバーから既に消去されている場合は、削除済みのフォルダが表示されなくなりました。[ASRV-16253]
- 組み込まれている Java のバージョンがバージョン 8u112 にアップデートされました。[ASRV-3409]
- Acronis Access Server API を使用して同期・共有の共有フォルダにユーザーを追加したり、そこからユーザーを削除したりする際に、影響を受けるエンドユーザーに電子メール通知を送信しないというオプションが追加されました。[ASRV-3888]

バグ修正:

- ユーザーが実際には読み書きアクセス権を持っているネットワークフォルダが、ウェブ UI に読み取り専用として表示されることがある問題を修正しました。[ASRV-4200]

Acronis Access 7.4.1（リリース: 2016年10月18日)

- その他複数のバグ修正や最適化。

Acronis Access 7.4（リリース: 2016年9月15日)

機能強化:

- 共有ファイルのランディングページに直接ジャンプできるダウンロードリンクで共有ファイルを参照する機能が追加されました。現在、表示とダウンロードのオプションが表示されています。この機能は、サーバーでウェブクライアントドキュメントのプレビューが有効になっていることを必要とします。[ASRV-3051]
- PDF 注釈用の空の PDF ファイル作成を有効化、無効化する新しいモバイルポリシーオプションが追加されました。[ASRV-3620]
- ドキュメント内の URL を Acronis Access アプリで開く方法を決める新しいモバイルポリシーオプションが追加されました。オプションの種類:「デフォルトのブラウザ」、「インラインブラウザ」、「MobileIron Web@Work」、「Good Access」、または URL の参照をブロック。[ASRV-3452]
- カメラまたは写真ライブラリからのファイルのインポートを有効化、無効化する新しいモバイルポリシーオプションが追加されました。[ASRV-2821]
- Acronis Access for iOS クライアントアプリのバージョン 7.6 に、iOS ドキュメントプロバイダ拡張機能の使用を有効化、無効化する新しいモバイルポリシーオプションが追加されました。ホワイトリスト、ブラックリストの制限がなく、既存のポリシーで「Acronis Access ファイルを別のアプリケーションで開く」を許可していない限り、この設定はデフォルトで無効になります。[ASRV-2490]
- 現在、同期・共有のストレージクォータは 1 GB 未満に設定することが可能です。[ASRV-1439]

- Mac および Windows のデスクトップ同期クライアントの設定ダイアログに、[ログフォルダを開く] ボタンが追加されました。[ASRV-2025]
- 現在、共有フォルダ変更についての通知メールには、問題になっているフォルダに直接移動できるリンクが含まれています。この変更は、「ユーザー通知」の電子メールテンプレートに適用されます。この電子メールテンプレートをカスタマイズした場合には、必要に応じてこれらの変更を手動でテンプレートに加える必要があります。[ASRV-1577]
- ウェブプレビューでの Excel ファイルの列幅表示が改善されました。[ASRV-3007]
- Mac デスクトップ同期クライアントが、ネットワーク切断およびスリープから復旧する際の信頼性およびスピードが向上しました。[ASRV-3582]、[ASRV-3353]、[ASRV-139]
- 使用する Tomcat のバージョンが 7.0.70 に更新されました。
- 使用する Java のバージョンが 8u92 に更新されました。

バグ修正:

- 削除されたユーザーの同期・共有データを再割り当てできない問題が修正されました。[ASRV-3149]
- Office のファイルが複数のクライアントで開かれ、繰り返し保存される際に、複数の競合解決用のファイルが作成される問題が修正されました。[ASRV-3024]

Acronis Access 7.3.1（リリース: 2016年6月20日)

機能強化:

- 新しいモバイルの「アプリケーションポリシー」設定が追加され、Acronis Access iOS アプリのバージョン 7.6.0 でリリースされた iOS ドキュメントプロバイダ拡張機能を有効化/無効化できるようになりました。このポリシー設定は、「Acronis Access ファイルを別のアプリケーションで開く」ポリシーが有効で、使用中のアプリのホワイトリストまたはブラックリストがない場合には、アップグレード後のサーバーでデフォルトで有効になります。アプリのホワイトリストまたはブラックリストが使用中になっているか、「Acronis Access ファイルを別のアプリケーションで開く」ポリシーが無効になっている場合には、アップグレード後のサーバーでデフォルトで無効になります。[ASRV-2490]

- 新しいモバイルの「同期ポリシー」設定が追加されました。この設定を使用すると、Acronis Access アプリによるファイルの同期中にモバイルデバイスの自動ロックを防ぐことができます。この設定はデフォルトで **[オフ]** になっており、現時点では Acronis Access for iOS のバージョン 7.6.0 以降でサポートされています。Android および Windows Mobile については、今後のアプリのリリースでサポートされる予定です。[ASRV-2988]
- [監査ログ] の [設定] に新しいオプションが追加され、エクスポートした監査ログでタイムスタンプを表示する際に、Access Server のローカルタイムゾーンで表示するか、UTC タイムゾーンで表示するかを選択できるようになりました。[ASRV-3096]
- モバイルの「同期ポリシー」に、追加のオプションとして「自動同期間隔」が追加されました。新しいオプションとして、8 時間、12 時間、24 時間、48 時間を選択できます。この設定は、現時点では Acronis Access for iOS のバージョン 7.6.0 以降でサポートされています。Android および Windows Mobile については、今後のアプリのリリースでサポートされる予定です。[ASRV-3130]
- Fabric レポートライブラリを通じて、Acronis へのアプリのクラッシュについての報告を有効化/無効化する新しいポリシー設定が追加されました。この報告機能はデフォルトでは無効になっており、ユーザーがサーバー側のポリシーを選択した場合にのみ有効化されます。有効化をおすすめします。レポートはアプリがクラッシュしたときにのみ送信され、Acronis による Access アプリの機能向上に使用されます。レポートには個人データまたは識別情報は含まれません。このレポート機能とポリシー設定は、Acronis Access for Android のバージョン 7.0.0 以降にのみ適用されます。iOS および Windows Mobile については、今後のアプリのリリースでサポートされる予定です。[ASRV-3138]
- Acronis Access は、**Internet Explorer** の **[互換性モード]** 設定の影響を受けません。管理ポータルとウェブユーザーインターフェイスのどちらも想定どおりに機能します。[ASRV-3194]

バグ修正:

- Kerberos シングルサインオンを使用するように設定された Acronis Access iOS クライアントが、不必要にパスワード入力を求める問題が修正されました。[ASRV-3111]

Acronis Access 7.3（リリース: 2016年5月5日)

機能強化:

- Access Advanced サーバーに対するイタリア語のローカリゼーションに関するサポートが追加されました。
- Acronis ストレージを同期・共有「ファイルリポジトリ」ストレージのロケーションとして使用するオプションが追加されました。[ASRV-1519]
- Swift S3、Ceph S3 および「S3 と互換性のある他のストレージ」を同期・共有「ファイルリポジトリ」ストレージのロケーションとして使用するオプションが追加されました。[ASRV-2774]
- ACRONIS ACCESS では、SharePoint ネットワークデータソース内で SharePoint「フォローサイト」が表示できるようになりました。データソースのルート内にある「フォローサイト」フォルダに表示されます。ユーザーは SharePoint のウェブクライアント内からサイトを「フォロー」できます。この機能はデフォルトでは使用できませんが、ACRONIS ACCESS のウェブ管理では SharePoint データソースの設定で有効化できます。[ASRV-2423]
- 同期・共有ストレージ内では、削除済みのフォルダとそのすべてのコンテンツをユーザーの 1 回の操作で復元することも可能になりました。また、削除済みのフォルダに移動して特定の削除済みファイルを参照して復元することもサポートされています。[ASRV-451]
- Windows や Mac のデスクトップクライアントで、ファイルパスが 260 文字を超えるファイルを同期できるようになりました。Windows Explorer を使用すると、この長さを超えるパスのファイルにアクセスできないことがあります。[ASRV-439]
- デスクトップ同期クライアントでは、サーバー側とデスクトップのファイルとでファイルの内容を比較して、ファイルの変更日が異なっていても、変更されていないファイルのアップロードやダウンロードを回避するようになります。ユーザーが同じファイルをアップロードする場合や、デスクトップ同期クライアントが一旦アンインストールされた後に再インストールされてから同じローカル同期フォルダを使用する場合、既存のファイルが比較され、余分なアップロードやダウンロードをせずに再使用されるようになりました。Acronis Access モバイルやウェブクライアントでアップロードされた同期・共有ファイルは既存のサーバー側ファイルと比較され、アップロードされたファイルが

既存のファイルと一致する場合に不要なリビジョンが作成されないようになりました。[ASRV-2734]

- Acronis Access Advanced の新規インストールで使用されるデフォルトの TCP/IP ポートが変更されました。Acronis Access ウェブクライアント/管理サービスは、デフォルトでポート 443 にインストールされるようになりました。Acronis Access ゲートウェイサービスは、デフォルトでポート 3000 にインストールされるようになりました。既存の Acronis Access Advanced サーバー上でのアップグレードインストールで、現在のポート設定が保持されるようになります。[ASRV-2810]
- 同期・共有での共有ファイルの URL が、より短い形式に簡略化されました。[ASRV-1157]
- ユーザーは、個人で取ったアクション（ダウンロード、アップロード、共有終了など)について、同期・共有のメール通知を受信することがなくなります。[ASRV-39]
- [ウェブのプレビュー] にあるウェブ管理の設定ページに、サーバー側での表示を必要としないファイルのみでウェブクライアントのプレビューを有効化する新しいオプションが追加されました。このオプションが有効化されると、Microsoft Office のファイルはウェブクライアント内でプレビューできません。[ASRV-2644]
- Acronis Access Advanced の新規インストールおよび新規作成されたモバイルアクセスポリシーでは、モバイルアクセスポリシーの設定「ウェブクライアントからファイルサーバー、NAS、および SharePoint へのアクセスを許可する」がデフォルトで有効化されるようになりました。[ASRV-2818]
- [電子メールテンプレート] ページに、設定済みの「サーバー名」を電子メールコンテンツの product_name 変数に使用する新しいオプションが追加されました。[ASRV-1942]

バグ修正:

- ウェブクライアント内で同期フォルダを追加した場合に、特定のネットワークデータソースで同期フォルダのサイズが 0 と表示されることがある問題が修正されました。[ASRV-2473]
- 多数のデータベースアイテムを処理している場合に、Acronis Access ゲートウェイサービスがスタートアップ時にタイムアウトになることがある問題が修正されました。[ASRV-2400]

- 同期・共有フォルダの「メンバー」ダイアログで、外部の無料ユーザーが名前とその横の「ゲスト」アイコンで表示されるようになりました。[ASRV-1940]
- Excel ファイルをウェブプレビューで開いた場合に、そのコンテンツのハイパーリンクが正しく表示されないことがある問題が修正されました。[ASRV-2798]
- ファイルリポジトリへのパスに漢字が含まれていると機能しない問題が修正されました。[ASRV-2810]

Acronis Access 7.2.3（リリース: 2016年2月29日)

機能強化:

- Acronis Access iOS アプリ（バージョン 7.5)で導入された新しい、そして機能向上した PDF ビューア/注釈ツールに、表示設定を構成するモバイルクライアントポリシーのオプションが追加されました。[ASRV-2103]

バグ修正:

- 同期・共有機能について、デスクトップクライアントフォルダ内でフォルダを削除または移動し、すぐに同じ名前のフォルダを作成した際に発生する同期の問題が修正されました。[ASRV-1706]

Files Advanced 7.2.2（リリース: 2016年2月2日)

機能強化:

- EMC Documentum が Files Advanced でデータソースとしてサポートされるようになりました。Files Advanced ユーザーは、CMIS プロトコルを使用して Documentum に接続することができます。ネットワークデータソースを設定する際に、データソースタイプのオプションの中に Documentum が表示されるようになりました。[ASRV-1012]
- ゲートウェイの新しいアクセス制限設定が追加されました。この設定は、Microsoft Intune によって管理される iOS クライアントへのモバイルアクセスの制限を可能にするものです。これらのクライアントには、Acronis Access の過去のバージョンからのアッ

プグレード時にデフォルトで接続することができます。ゲートウェイサーバーの [アクセス制限] 設定で、接続を許可しないようにすることもできます。[ASRV-1686]

- ユーザーに一方向同期フォルダの作成のみを許可するという、モバイルクライアント管理ポリシーの新しいオプションが追加されました。[ASRV-1846]
- モバイルクライアントで同期フォルダを作成する際に、デフォルトで選択される同期フォルダのタイプ（一方向同期または双方向同期)を設定するという、モバイルクライアント管理ポリシーの新しいオプションが追加されました。[ASRV-1846]
- テキストファイルはウェブクライアントのプレビューで、PDF に変換されず、プレーンテキストとして表示されるようになりました。[ASRV-1855]
- より大きなサイズのファイルに対応するために、ウェブプレビューにおけるファイル表示のタイムアウト時間が 120 秒に延長されました。[ASRV-1868]
- rtf、ini、log、csv、ico、jpe というファイル形式や Open Office のファイル形式(ods、odt、odp)をサポートするウェブプレビュー機能が追加されました。[ASRV-1852]

バグ修正:

- Access サーバーから Microsoft Online のログインサービスにアクセスできない場合の、SharePoint データソースへのアクセススピードが向上しました。[ASRV-374]
- Internet Explorer 11 のウェブクライアントプレビュー内での、PDF ファイルの読み込み速度が向上しました。
- 期限切れの共有ファイルのリンクが不必要に何度も監査ログに記録されるという問題が修正されました。[ASRV-1737]
- 共有フォルダ変更通知で、ファイルやフォルダを削除したユーザーが特定されないことがある問題が修正されました。この変更は、「ユーザー通知」のテンプレートに適用されます。電子メールテンプレートをカスタマイズしているユーザーは、必要に応じて、これらの変更をご自身のテンプレートに手動で加える必要があります。[ASRV-1964]
- Alfresco ファイルの修正日付が、他の Access サーバーの修正日付と一致しないという問題が修正されました。[ASRV-1586]
- ネットワークノードのファイルを同期する際に、誤って競合解決用のファイルが作成される問題が修正されました。[ASRV-2141]

- Access サーバーの FQDN が内部 DNS で解決されない場合、ウェブクライアントのプレビュー機能で Office ファイルの表示に失敗するという問題が解決されました。[ASRV-1887]
- IE 11 のブラウザで監査ログのページを更新する際に生じる問題が修正されました。[ASRV-1624]

Acronis Access 7.2.1（リリース: 2015年12月10日)

機能強化:

- 試用版を有効化する際の電子メールアドレスの検証機能が改善されました。[ASRV-2037]

バグ修正:

- シングルサインオンを使用するとデスクトップクライアントの同期が機能しなくなるというバグが修正されました。

Acronis Access 7.2（リリース: 2015年11月17日)

機能強化:

- Office ファイル、PDF、テキストファイル、画像をダウンロードしなくても、Acronis Access ウェブブラウザクライアント内で直接表示する機能が追加されました。この機能は、アップグレード時にデフォルトで有効になり、サーバーの [全般設定] の新しい [ウェブプレビュー機能] セクションで設定できます。
- CMIS プロトコルを介してコンテンツ管理システムのデータソースにアクセスする機能が追加されました。Acronis Access に、Alfresco および [汎用 CMIS] オプション向けのサポートされるデータソース設定が追加されました。Documentum のサポートは、今後のリリースで近日中に追加される予定です。[ASRV-1012]
- 使用可能な Acronis Access モバイルアプリの詳細が表示される [モバイルクライアントのダウンロード] ページが、ウェブユーザーメニューに追加されました。[ASRV-1463]

- 同期・共有ファイルダウンロードリンクを共有するときに、Access サーバーによりリンクが電子メールで送信されたユーザーのみにアクセスを制限できるようになりました。[ASRV-330]
- 新しいリンクプロパティダイアログでは、既存の共有ダウンロードリンクのリンク URL、「共有済み」ユーザー、アクセス制限、期限切れの設定を参照できます。これらの共有設定は、このダイアログで編集することもできます。[ASRV-1011]
- 同期・共有ファイルまたはフォルダに招待された新しい外部ユーザーは、アカウントにアクセスする前に、有効化電子メールリンクを通じた Acronis Access アカウントの有効化が求められるようになります。[ASRV-1184]
- Acronis Access ウェブクライアントユーザーに、新たに共有されたフォルダを同期するオプションが表示されたとき、デスクトップ同期クライアントを登録していない場合は通知が表示されるようになります。[ASRV-1509]
- Acronis Access モバイルクライアントは、証明書または Kerberos 認証を使用して同期・共有データソースにアクセスできるようになりました。[ASRV-466]
- Microsoft Intune によって管理される Acronis Access iOS クライアントアプリからの接続を許可または拒否する、新しいゲートウェイサーバーの [アクセス制限] オプションが追加されました。[ASRV-312]
- 「iOS 管理対象アプリ」機能によって管理される Acronis Access iOS クライアントアプリからの接続を許可または拒否する、新しいゲートウェイサーバーの [アクセス制限] オプションが追加されました。[ASRV-1026]
- Acronis Access 管理コンソールへのアクセスを、特定の IP アドレスまたは IP 範囲に制限できるようになりました。[ASRV-1183]
- ユーザーの [ログ] ページのページ読み込み速度が向上しました。[ASRV-1209]
- 電子メール先行入力の参照パフォーマンスが向上しました。[ASRV-1468]
- Acronis Access サーバーの試用期間が 30 日間になりました。[ASRV-1228]
- Acronis Access ウェブサーバーがモバイルクライアントとは別のネットワークアドレスを使用してクラスタグループに接続する必要がある場合に使用するゲートウェイの [クラスタグループ] 設定オプションが、[Access サーバー接続に代替アドレスを使用] に追加されました。[ASRV-243]

- アップグレード時に、カスタム Tomcat「temp」ディレクトリ設定が Acronis Access に保持されるようになりました。[ASRV-378]
- TLSv1.2 のサポートが追加されました。[ASRV-1281]
- PostgreSQL がバージョン 9.4.4-3 に更新されました。[ASRV-379]
- Java がバージョン 8u60 に更新されました。[ASRV-1327]

バグ修正:

- Access サーバーでデスクトップクライアント向けに [レガシーポーリングモードを強制] が設定されている場合、デスクトップクライアントユーザーのログインが失敗する問題が修正されました。[ASRV-278]
- Acronis Access Windows デスクトップクライアントの無人インストールの問題が修正されました。[ASRV-1192]
- Windows自動実行レジストリキーが見つからない場合に、Acronis Access Windowsデスクトップクライアントのインストール時にエラーが発生する問題が修正されました。[ASRV-1496]
- ネットワークフォルダへのウェブクライアントファイルのアップロードが完了前にキャンセルされた場合、サーバーから一時ファイルが削除されない場合がある問題が修正されました。[ASRV-1516]
- Acronis Access設定ユーティリティで設定を変更した後に、Acronis Accessゲートウェイサーバーサービスの実行に使用されるカスタムサービスアカウントが「ローカルシステム」に戻る問題が修正されました。[ASRV-1503]
- ユーザーの明示的なユーザープリンシパル名(UPN)と暗黙的な UPN が異なる場合に、シングルサインオンが失敗する問題が修正されました。[ASRV-1497]
- 新しいバージョンの Internet Explorer で「互換モード」が有効になっている場合、Acronis Access ウェブクライアントの UI が IE8 モードに戻る問題が修正されました。[ASRV-1346]
- Windowsの言語がフランス語に設定されている場合に、Acronis Access Windowsデスクトップ同期クライアントの自動アップデートが失敗する問題が修正されました。[ASRV-1229]

- Windows 10 でフォトギャラリースクリーンセーバーがアクティブになっているとき、通知を表示する互換性がないために Acronis Access Windows デスクトップ同期クライアントでエラーが発生する問題が修正されました。[ASRV-111]
- 共有ファイルダウンロードリンクの有効期限を 999999 日より長く設定するとウェブページエラーが発生する問題が修正されました。[ASRV-1219]
- Acronis Access サーバーをアップグレードしたときにシングルサインオンのカスタム Tomcat web.xml 設定が保持されない問題が修正されました。[ASRV-1059]
- アイテムの数が非常に多いネットワークホームフォルダが、モバイルクライアントで空と表示される問題が修正されました。[ASRV-1054]
- ダウンロード中にクライアントが停止したか、コンピュータが再起動した場合に、Acronis Access Windows デスクトップクライアントによるファイルのダウンロードが停止する問題が修正されました。[ASRV-1546]

Acronis Access 7.1.2（リリース: 2015年8月4日)

機能強化

- ユーザーセッションが終了しそうなときに延長のオプションが提供される場合、ウェブ UI で通知されるようになりました。オプションを選択しない場合、ユーザーは自動的にログアウトされます（US3869、DE14304)。
- [削除済みを表示] をオンにしている場合も、削除およびリポジトリから消去された同期・共有ファイルが表示されなくなりました（US10696)。
- [リンク] ウェブページで表示されるファイルリンクをフィルタリングするための設定が利用できるようになりました（US10812)。
- リンクの詳細ダイアログからリンクの有効期限の日数を変更できるようになりました（US10820)。
- リンクの詳細ダイアログからファイルリンクの公開/非公開のステータスを変更できるようになりました（US10821)。
- リンクの詳細ダイアログからリンクに対する 1 回限りのダウンロードの設定を変更できるようになりました複数回使用できるリンクを 1 回限りのダウンロードリンクに変更した場合は、この後 1 回だけファイルをダウンロードすることができます。リンクが共有

されたそれぞれのユーザーが一度ずつダウンロードできるということではないことに注意してください（US10822)。

- 複数回使用できるリンクが複数のユーザーと共有される場合、それぞれのユーザーに対して同じファイルリンクが送信されるようになりました。ユーザーごとに固有のリンクは送信されません。これは、共有リンクダイアログの使いやすさを向上するための変更です。
- Access サーバーAPI で、ユーザーの削除時にすべてのコンテンツを削除するオプションを利用できるようになりました（US10644)。
- 最新の Android クライアントアプリでのサポート機能が適用されるように、モバイルポリシーのアイコンがアップデートされました。

バグ修正

- Access サーバーの [共有の制限] 設定で許可されている場合、有効期限を設定せずにファイルリンクを共有できるようになりました（DE12851、DE13461)。
- ユーザーにフォルダへのアクセス権が付与されていない場合、そのフォルダで共有されているファイルリンクが共有済みの [リンク] ページに表示されなくなりました（DE14574)。
- ファイルが元の場所から移動された場合、そのファイルへの共有リンクはすべて自動的に無効化されるようになりました（DE14610)。
- 書き込みのアクセス権が失効になったことで共有に「他のユーザーを招待できる」アクセス権も失ったユーザーの場合、フォルダ内で共有されているファイルリンクがすべて無効化されるようになりました（DE14615、DE14623)。
- ファイルリンクを共有したユーザーがそのファイルへのアクセス権を失った場合、そのファイルリンクでのダウンロードが許可されなくなりました。たとえば、「ユーザーB」によって所有されている共有フォルダ内にあるファイルへのリンクを「ユーザーA」が共有した後に、「ユーザーB」が共有フォルダのメンバーから「ユーザーA」を削除した場合に、このような状態が発生することがあります（DE14560)。
- ユーザーが自分の共有を終了した場合、共有にアクセスできない電子メールが受信されないようになりました（US10770)。

- Access で共有されている、ログインが必要なファイルダウンロードリンクにアクセスしたユーザーが認証に SSO を使用している場合、認証後の適切なページが表示されるようになりました（DE14539)。
- SSO ログインリンクが iOS デバイスおよび Windows Phone で表示されなくなりました（DE14554)。
- SharePoint のサブパスが、ウェブクライアントでの追加時に適切に解決されるようになりました（DE14423)。
- 左側のサイドバーでスクロールが可能になりました。ネットワークデータソースのスクロールが必要な場合に利用できます（DE14429)。
- デフォルトの電子メールテンプレートのフッターのテキスト折り返しが改善されました（DE14436)。
- 自己プロビジョニングフォルダをモバイルクライアントから正常に削除できるようになりました（DE14517)。
- Internet Explorer と Firefox での韓国語のテキスト折り返しが改善されました（DE14522)。
- UPN（ユーザープリンシパル名)を持たないユーザーがモバイルクライアントから認証できないという、認証に関する問題が修正されました（DE14624)。
- ファイル名に一重引用符が含まれている場合に共有ファイルへリンク経由でアクセスするとエラーが発生するという問題が修正されました（DE14633)。
- Access サーバーから Access ゲートウェイクラスタグループへの接続時に使用すべきアドレスを指定できる新たな設定が追加されました。デフォルトでは、この値はクライアント接続のアドレスと一致しています（DE14636)。
- 多数のファイルのアップロード時におけるゲートウェイサーバーのメモリ使用量が最適化されました（DE14589)。
- SSO を使用してネットワークコンテンツを同期するときに、Kerberos チケットの有効期限が切れている場合、デスクトップクライアントで Access サーバーとの再認証が自動的に行われるようになりました（US10900)。

Acronis Access 7.1.1（リリース: 2015年7月8日)

バグ修正

- 一部の言語において Mac のデスクトップクライアントの一部のメニュー項目が適切にローカライズされていないという問題が修正されました。
- Access サーバーを古いバージョンから正常にアップグレードできないことがあるという、まれに発生する問題が修正されました。
- 単一のリンクで共有されていた単一ファイルをウェブ UI で選択するときに、右側のメニューに **[通知設定]** オプションが表示されなくなりました。このオプションは、複数のリンクで共有されている複数ファイルには適用されません。
- Kerberos チケットの有効期限が切れている場合、シングルサインオンで認証されているクライアントでネットワークノードを参照できないという問題が修正されました。

Acronis Access 7.1

機能強化

- Acronis Access で、ウェブクライアントおよび Windows デスクトップクライアント向けの統合デスクトップ認証（シングルサインオン)がサポートされるようになりました。シングルサインオンを有効にすると、既にドメインへの認証が済んでいるユーザーがコンピュータにログインする場合、ウェブインターフェイスまたは Windows デスクトップクライアントへのログイン時にユーザー名とパスワードを認証用に再入力する必要がありません。Mac のデスクトップ同期クライアントでのこの機能へのサポートは、今後のアップデートで追加される予定です。この機能には詳細な設定が必要になります。詳細については、「シングルサインオンの設定 『284ページ 』」を参照してください（US10595)。
- 1 回ダウンロードすると無効になるファイルダウンロードリンクをユーザー間で共有できるオプションが追加されました（US7172)。
- 共有済みの同期・共有フォルダの期限を、ユーザーが設定できるようになりました。有効期限日が過ぎると、共有のすべてのメンバーは共有フォルダにアクセスできなくなります（US6314、US8531)。
- 同期・共有にアップロードできるファイルのサイズおよび種類を制限する、新しい管理者オプションが使用できるようになりました。管理者は、ウェブ管理の [同期・共有] → [一般制限事項] ページでこれらの制限を有効にして、最大ファイルサイズおよび禁止するファイルの種類を指定することができます（US10587)。

- 新しい **[リンク]** ページで、[リンクの送信] や [リンクを取得] で共有した同期・共有のすべてのファイルが表示されるようになりました。このリストでは、ファイルリンクへのアクセスを無効にしたり、同期・共有の階層内のファイルに移動したりできます（US10809)。
- 特定ファイル用に共有されたファイルリンク個別の詳細リスト(リンクの送信先、リンクの制限内容、および有効期限日など)を表示できるようになりました。これらのリンクは個別に無効にできます（US10814)。
- [リンクの送信] や [リンクを取得] で共有された同期・共有ファイルでアイコンが表示されるようになりました。このアイコンはファイルおよびフォルダのリストでファイルの横に表示されます。このアイコンをクリックすると、ファイルの共有リンクの詳細を表示および変更できます（US10816)。
- Acronis Access に韓国版が追加されました（US10638)。
- ユーザーが無効になった場合、ユーザーの共有ファイルのリンクがすべて一時的に無効化されるようになりました。また、ユーザーが削除された場合は、そのユーザーのコンテンツが再割り当てされるまで共有ファイルのリンクが無効化されます。ユーザーのコンテンツが再割り当てされると、ファイルのリンクが再度有効になり、コンテンツの新しい所有者により所有されるようになります（US9870)。
- ウェブログインページに表示するカスタムメッセージを、管理者が設定できるようになりました。このメッセージは、[設定] → [ウェブ UI のカスタマイズ] ページで設定できます（US10319、US10660)。
- デフォルトのユーザー通知電子メールに、同期・共有の共有フォルダ通知電子メールを停止するためのリンクが表示されるようになりました（US10423)。
- ファイルのリンクが同時に複数のユーザーに共有された場合、パスワード情報リンクを受信するすべてのユーザーが同じリンクを受信するようになりました。これまでは、各ユーザーが個別に異なるリンクを受信していました。ただし、1 回限りのリンクは例外です。1 回限りのリンクが複数のユーザーに共有されると、各ユーザーは 1 度だけダウンロードすることができる一意のリンクを取得します（US10808)。

バグ修正

- モバイルデバイスの登録時間が大幅に短縮されました（US10712)。

- Access サーバーからアクセスできないクライアント接続アドレスのゲートウェイクラスタを（サーバーアドレスを使用して)管理できるようになりました（DE13147)。
- 同期・共有の LDAP プロビジョニング済みグループのメンバーが、モバイルデバイスから新規ユーザーとして初めてログインした場合、ウェブインターフェイス経由でログインしなくても、同期・共有へのアクセスが許可されるようになりました（DE13215)。
- 同期・共有のデータソースへのアクセスが保留中のユーザーが、モバイルデバイスから正常に登録できるようになりました（DE13379)。
- パスワードにコロンを含めている Active Directory ユーザーが、正常に認証され、デスクトップクライアントから同期済みネットワークデータソースにアクセスできるようになりました（DE14294)。
- PostgreSQL パスワードに一重引用符、コロン、パーセント記号、上位ユニコード、またはその他の特殊文字が含まれる場合に Access サーバーが起動するという問題が修正されました（DE14355)。
- 許可可能な登録サーバーのアクセス制限リストで定義されるサーバー名に、ダッシュを使用できるようになりました（DE14414)。
- 直接リンク経由での同期・共有ファイルのダウンロード時にレポートに表示される変更日が、サーバーのタイムゾーンで表示されるようになりました（DE14418)。
- 削除済みユーザーが電子メールの先行入力候補リストに表示されなくなりました（DE14508)。
- PostgreSQL パスワードにコロン、一重引用符、上位ユニコード、またはその他の特殊文字が含まれる場合でも、Access サーバーインストーラが正常に完了するようになりました（DE14433)。
- 同期の処理中にダウンロードを実行したことで同期がハングした場合にディスクのファイルが直ちにロックされるという、デスクトップクライアントでまれに発生した問題が修正されました（DE14197)。

既知の問題

- Files Advanced 7.1 は Java のバージョン 8u31 で機能しますが、8u45 が認証に使用されます。8u31 より後の Java のバージョンには既知の問題が存在し、シングルサインオ

ン機能でのエラーの原因となります。Java をアップグレードしたまま、SSO を使用する場合は、https://kb.acronis.com/content/56367 の資料を参照してください。

Acronis Access 7.0.5

機能強化

- Acronis Access に繁体字中国語版および簡体字中国語版が追加されました（US10350)。
- 多くのサブフォルダを含むネットワークデータソースのコンテンツを参照するときのパフォーマンスが向上しました（US10622)。
- ACRONIS ACCESS はデバイス証明書認証をサポートしています（US10697)。

バグ修正

- 非常に長いパスを使うと SharePoint データソースの一部が追加できないという問題が修正されました（DE14339)。
- Access Server 7.0.4 にアップグレード後、ユーザー名を指定しないユーザーがいる場合にスタートアップで発生する可能性があるエラーが修正されました（DE14352)。
- Internet Explorer 9 でのファイルアップロード時に発生する可能性があった問題が修正されました（US10636)。
- 同期されたネットワークフォルダに対してデスクトップ同期ダイアログを開き、変更をせずに保存した場合に双方向同期フォルダが一方向同期フォルダに変更される可能性があるという問題が修正されました（DE14398, DE14415)。
- 他のユーザーがネットワーク上の多くのフォルダやファイルを同期すると、新規ネットワークフォルダの同期が遅れることがあるという問題が修正されました（DE14406)。
- ウェブインターフェイスで変更を行うと、デスクトップ同期クライアントがネットワークフォルダの同期タイプをすぐにアップデートしない(一方向同期から双方向同期、またはその逆)ことがあるという問題が修正されました（DE14413)。
- Access Server がゲートウェイサーバーから監査ログを取得できないことがあるという問題が修正されました（DE14414)。
- SharePoint への Kerberos 認証の問題が修正されました（DE13289, DE14272)。

- コンピュータの別なアプリケーションで同期対象のファイルを開いているためにファイルの同期が完了できなかった場合、デスクトップクライアント上に明確な説明がなく、詳細不明な Unicode エラーを受け取るというまれに発生する問題が修正されました（DE14151, DE14289)。
- デスクトップクライアントをバージョン 2.x からバージョン 7.0.4 以降にアップグレードした際に発生することがある問題が修正されました（DE14336)。
- Visual C# プロジェクトをデスクトップクライアント上の同期・共有フォルダに保存すると、ファイルが重複することがあるという問題が修正されました（DE14353)。

Acronis Access 7.0.4

機能強化

- モバイルクライアントの「**アクセス制限**」で Windows モバイルクライアントからのアクセスを制限できるオプションが利用できるようになりました。Windows クライアントの手順やインストールのリンクなどのオプションを、登録招待ページおよび登録用電子メールで利用することも可能になりました（US8788, US10558)。
- 画面解像度の低いモバイルデバイスにおける Access のウェブインターフェイスの使いやすさが向上しました（US10270)。
- ゲートウェイサーバーがオフラインの状態でも、自己署名証明書による接続を許可するゲートウェイサーバーオプションが変更できるようになりました（US10318)。
- ウェブ UI でデスクトップクライアントへのフォルダの同期を選択する場合、同期されるフォルダの合計サイズがユーザーに表示されるようになりました。この表示内容により、ユーザーが自身のデスクトップに大容量の共有データを同期する場合に、フォルダが選択しやすくなります（US10414)。
- 設定ユーティリティで Access ファイルリポジトリのロケーションに UNC パスを指定できるようになりました（DE13733)。
- 設定ユーティリティで中間証明書を設定できるようになりました（US10315)。
- 共有にユーザーを招待する場合に自動入力される電子メールアドレスオプションには、共有メンバーのみが表示されるようになりました。また、内部 AD ユーザーも他の内部 AD ユーザー全員を閲覧できます（DE13387)。

- ファイルのダウンロードの直接リンクを **[リンクの送信]** や **[リンクを取得]** で作成する場合に、ファイルのダウンロード前に Access ユーザーのログインを必須にするという設定ができるようになりました。**[共有の制限]** の設定ページに新しいオプションが追加され、管理者が公開リンクの許可、またはログイン制限されたダウンロードリンクの許可について定義することができます。両方のタイプのリンクが許可されている場合、ユーザーは共有時にリンクの種類を選択できます。ログイン制限されたリンクへのアクセスを内部ユーザーのみに限定する管理者設定もあります（US10499)。

変更

- **ウェブ管理ページには、Internet Explorer 8 でアクセスできなくなりました**（US10471)。

バグ修正:

- モバイル登録に大規模な AD グループを招待しようとする場合に未処理のエラーが発生することがあるというバグが報告されていましたが、修正されました（US10511)。
- %USERNAME% 変数は、ウェブインターフェイスのホームディレクトリデータソースの名前と説明の中でサポートされるようになりました（DE13651)。
- Safari でウェブ UI からファイルをダウンロードする場合、小さなポップアップウィンドウが表示されなくなりました（DE13699)。
- ファイルのダウンロードの直接リンクでファイルをダウンロードする場合、共有ファイルのリンクを作成したユーザーが通知に含まれるようになりました（DE13811)。
- 一部のデータソースにアクセスできない場合でも、データソースのリストが表示されるようになりました。アクセスできないデータソースはリストに表示されません（DE13896)。
- カラースキームがダウンロードリンクのランディングページで使用されるようになりました（DE14072)。
- UPN（ユーザープリンシパル名)が設定されていないアカウントの AD ユーザーが、Access ウェブインターフェイスを使用してネットワークのデータソースにアクセスできるようになりました（DE14089)。

- 競合解決で、名前にフォワードスラッシュを含むユーザーがサポートされるようになりました。競合ファイルの作成時に、Windows ファイルシステムにおいてスラッシュは無効な文字となるため、ユーザー名に含まれるフォワードスラッシュはアンダースコアに置き換えられます（DE14133)。
- Mac でアップロードされたネットワークボリューム上のファイルとフォルダが名前にフォワードスラッシュを含む場合、ファイルおよびフォルダが Mac や Windows のデスクトップクライアントに同期されるようになりました（DE14141)。
- Access サーバーでゲートウェイ監査ログメッセージを適切に取得できないことがあるという問題が修正されました（DE14146, DE14152)。
- Access 7.0.3 へのアップグレード後、ファイルを消去したときにエラーや障害が発生することがあるという問題が修正されました（DE14195, DE14015, DE14101)。
- 単一のユーザーセッションにおいてゲートウェイサーバー上で 1 つ以上のライセンスが一時的に使用されることがあるというライセンス問題が修正されました（DE14275, DE14142)。
- クラスタのアップグレード前に PostgreSQL サービスが停止するようになりました。このことにより、クラスタがアップグレードされないというエラーを回避できます（DE11927)。
- Microsoft Office のファイルを高速で保存する場合、デスクトップクライアントは Access 内で複数のファイルコピーを作成できなくなりました（DE14014)。

Acronis Access 7.0.3

機能強化:

- ネットワークファイルおよびネットワークフォルダに関するサポートやドキュメントなど、ウェブクライアント用の API ドキュメントがアップデートされました。
- Acronis Access ウェブサイトのカラースキームを、事前に設定されているさまざまなカラースキームの中から設定できるようになりました。また、管理者は、独自のカラースキームを作成することもできます。管理者は、ウェブ UI のカスタマイズ 『177ページ 』 ページからカラースキームを設定できるようになりました。
- カスタムロゴをアップロードして、ウェブ UI の外観を変更できるようになりました。ロゴが表示される場所に応じて、3 種類の画像サイズが使用されます。既存のカスタム

ロゴがある場合は、アップグレード時にカスタムロゴが表示されるすべての場所にそのロゴが使用されます。また、適切なサイズのロゴをウェブ UI のカスタマイズ 『177ページ 』ページにアップロードすることがでます。

- ユーザーのモバイルアクセスポリシーによってウェブクライアントからのアクセスが許可されている場合、Acronis Access ウェブサイトへのリンクがデフォルトの登録招待メールに記載されるようになりました。登録招待メールのテンプレートをカスタマイズしているお客様は、必要に応じて、カスタマイズしたテンプレートにこの新しいテキストを手動で追加する必要があります。
- **[フォルダのダウンロード]** オプションによって、ユーザーが現在参照しているフォルダのコンテンツをダウンロードできるようになりました。
- Acronis Access の管理者に、初期設定 『41ページ 』時に新規インストールでゲートウェイサーバーのアドレスを明示的に指定するよう要求するメッセージが今後表示されなくなります。ゲートウェイアドレスには、Access サーバーと同じアドレスが自動的に設定されます。
- モバイルクライアントの今後のリリースに備え、デフォルトの登録招待メールテンプレートに変更が若干加えられました。電子メールテンプレートをカスタマイズしているユーザーは、必要に応じて、手動でテンプレートをアップデートする必要があります。
- 一部のメモリ設定をキャッシュすることで、ログイン時のパフォーマンスとウェブアプリケーションの全般的なパフォーマンスが向上しました。
- 同期・共有のファイルのアップロード時とダウンロード時のパフォーマンスおよびスループットを向上させるために、さまざまな点が改善されました。
- Acronis Access では Java 8u31 がインストールされます。

バグ修正:

- **`ldap_caching`** デバッグログを有効にしている場合に発生することがある、LDAP のキャッシュエラーが修正されました。
- New Relic の監視に関する問題が修正されました。
- サーバー側のネットワークフォルダが割り当て済みのデータソースから削除された場合に、ユーザーのデスクトップ上の同期済みネットワークフォルダを削除できないことがあるという問題が修正されました。

- 管理サーバーが必要な環境で、管理サーバーが非標準ポート上でリッスンしている場合に、ゲートウェイファイル共有をウェブポータルから参照できないという問題が修正されました。
- ユーザーが Acronis Access 6.x からアップグレードし、Access 7.x へのログインに成功する前にパスワードをリセットしようとした場合に発生していたエラーが修正されました。
- デスクトップクライアント上にある最上位の一方向同期フォルダの名前を変更する場合に、警告が表示されなくなりました。
- モバイルクライアントでサイズの大きいファイルをダウンロードする場合に発生することがあった、タイムアウトエラーが修正されました。

既知の問題:

- Internet Explorer 8 を実行しているエンドユーザーがいる場合は、より安全なブラウザへのアップグレードを検討してください。管理者は SSL バインドを変更して、次の制限付きで Internet Explorer 8 ユーザーをサポートできます（DE12649)。
  - Internet Explorer 8 を実行しているユーザーは、Access 6 のスタイルのウェブクライアントインターフェイスに自動的にリダイレクトされます。
  - Internet Explorer 8 は、再設計された Access 7 のウェブインターフェイスではサポートされません。
  - これらのユーザーは、ウェブクライアントインターフェイスからファイルサーバー、NAS および SharePoint のデータソースにアクセスできません。
  - Internet Explorer 8 でのサーバー管理はサポートされていません。

Acronis Access 7.0.2

機能強化:

- Mac 向けおよび PC 向けの Acronis Access サーバーと Acronis Access デスクトップ クライアントにポーランド語版が追加されました。
- Acronis Access では、Access デスクトップ クライアントを介して、ファイル サーバー、NAS、および SharePoint のフォルダと Mac や PC との同期が可能になりました。この機能は「モバイル アクセス」のポリシーで有効化/無効化を切り替えることがで

きます。また、この機能を使用する場合、これらのデータ ソースへの Access ウェブ クライアントのアクセス権を有効にしておく必要があります。

- Access ウェブ クライアントの共有ダイアログ ボックスでのユーザーおよび電子メール アドレス入力機能が強化されました。
- Access ウェブ クライアントで複数レベルのブレッドクラム トレイルが表示されるようになりました。
- Access サーバー設定ユーティリティでファイル リポジトリのターゲットとして SMB ネットワーク共有が選択できるようになりました（DE13472)。
- 適切な証明書がコンピュータの個人用証明書ストアに存在しない場合、Access サーバー設定ユーティリティで自己署名証明書がデフォルトで指定されるようになりました（DE12983)。
- GOST 暗号が Access サーバー 7.0.2 のロシア語版でサポートされるようになりました（US9922)。
- ネットワーク ホーム フォルダへのアクセスがウェブ クライアントに追加されました（US9733)。
- パスに %username% ワイルドカードを含むネットワーク データ ソースがウェブ クライアントでサポートされるようになりました（DE13206)。
- ウェブクライアントアップロードで 11 個以上のファイルを同時にアップロードできるようになりました（DE12719)。
- 本リリースで Java 7 Update 71 が使用されるようになりました。

バグ修正:

- iOS モバイル クライアントから同期・共有のファイルのダウンロード リンクをメール送信するときに発生した問題が修正されました（DE13177)。
- 通知メールおよびデスクトップ クライアントの Finder やエクスプローラのコンテキスト メニューで作成したランディング ページやフォルダへのリンクについて、ユーザーのログインが求められることがなくなりました。
- mobilEcho 4.5 からのアップグレード時にレガシー データ ソースが変換されない可能性があるという問題が修正されました（DE13188)。

既知の問題:

- サードパーティ製の Java インストーラに含まれるバグにより、英語版以外の Windows Server でのインストール時に問題が発生する可能性があります。この問題を解決するには、https://kb.acronis.com/content/54518 を参照してください（DE13473)。
- Internet Explorer 8 を実行しているエンドユーザーがいる場合は、より安全なブラウザへのアップグレードを検討してください。管理者は SSL バインドを変更して、次の制限付きで Internet Explorer 8 ユーザーをサポートできます（DE12649)。
  - Internet Explorer 8 を実行しているユーザーは、Access 6 のスタイルのウェブクライアントインターフェイスに自動的にリダイレクトされます。
  - Internet Explorer 8 は、再設計された Access 7 のウェブインターフェイスではサポートされません。
  - これらのユーザーは、ウェブクライアントインターフェイスからファイルサーバー、NAS および SharePoint のデータソースにアクセスできません。
  - Internet Explorer 8 でのサーバー管理はサポートされていません。

Acronis Access 7.0.1

機能強化:

- ウェブ クライアントのインターフェイスのさまざまな点が改善されました。
- Mac 向けおよび PC 向けの Acronis Access サーバーと Acronis Access デスクトップ クライアントにロシア語版が追加されました。
- 本リリースで、Apache Tomcat 7.0.57 が使用されるようになりました（DE11653)。
- 本リリースで Java 7 Update 71 が使用されるようになりました。
- 共有ファイルのダウンロード リンクの最短有効期間が、Acronis Access サーバーの新規インストールのデフォルトで 1 日またはそれ以上を設定できるようになりました。以前の最短有効期間のデフォルトは 30 日間でした（DE13079)。
- フォルダの項目数が多い場合のウェブ クライアントからのネットワーク データ ソースの参照が改善されました（DE13056)。
- 競合解決の操作が改善されました。

バグ修正:

- Access サーバーのウェブ クライアントへのログインでの “ ¥” 記号の使用方法が修正されました。（DE13031)。
- mobilEcho 4.5 から Acronis Access 7.0.1 へのアップグレードがサポートされるようになりました（DE12984)。
- Acronis Access 6.1 からのアップグレード後にスタート メニューに表示される Acronis Access Tomcat サービス設定ツールへのショートカットが修正されました（DE12966)。
- 共有フォルダの右側のメニューに通知が表示されるようになりました（DE12948)。
- Internet Explorer 8 を実行しているエンドユーザーがいる場合は、より安全なブラウザへのアップグレードを検討してください。管理者は SSL バインドを変更して、次の制限付きで Internet Explorer 8 ユーザーをサポートできます（DE12649)。
  - Internet Explorer 8 を実行しているユーザーは、Access 6 のスタイルのウェブクライアントインターフェイスに自動的にリダイレクトされます。
  - Internet Explorer 8 は、再設計された Access 7 のウェブインターフェイスではサポートされません。
  - これらのユーザーは、ウェブクライアントインターフェイスからファイルサーバー、NAS および SharePoint のデータソースにアクセスできません。
  - Internet Explorer 8 でのサーバー管理はサポートされていません。
- Mac 向け Access デスクトップ クライアントで不定期に発生する異常終了が修正されました（DE12879)。

既知の問題:

- 単一ポートの Access ゲートウェイ サーバーの設定を使用しているときに、256 文字より長いパスが処理される場合、問題が発生する可能性があります。次の KB 資料を参照して問題を解決してください（DE12405):
  http://support.microsoft.com/kb/820129

Acronis Access 7.0

機能強化

- Access ウェブ クライアントのユーザー インターフェイスが再設計され機能強化が追加されました。
- **Acronis Access** は、**Acronis Access Advanced** に名称が変更され、Acronis Access 6 以前のバージョンをご利用されている既存のユーザーにとってはアップグレード パスになります。よりシンプルなニーズをお持ちの中小企業を対象にした新バージョンも発売されました。この新しいバージョンの名称が Acronis Access です。
- 新規インストール時に、設定ウィザードによって SMTP サーバーや Active Directory（LDAP)サーバーなどのシステム設定オプションの検出が試行されるようになりました。
- インストール時に、クライアント接続用に単一のオープン ポートを使用して Acronis Access と Acronis Access Advanced を動作させるように構成できるようになりました。この構成では、すべての Access クライアント（モバイル アプリ、デスクトップ同期クライアント、ウェブ クライアント インターフェイス)が同一のネットワーク アドレスとポートを使って、Access サーバーに接続します。
- Access ウェブ クライアント インターフェイス内からファイル サーバー、NAS サーバー、SharePoint サーバー上にあるフォルダとファイルを参照したりアクセスすることができるようになりました。この機能は、ユーザーまたはグループごとに有効化/無効化できます。
- デフォルトの電子メール テンプレートのグラフィック デザインがアップデートされました。通知メールおよび招待メールのテンプレートが再設計されました。
- ユーザー管理ページとデバイス管理ページが、単一の管理コンソール ページに統合されました。
- Access で同期・共有のファイルおよびフォルダの競合の問題を解決できるようになりました。複数のユーザーがファイルを同時に修正して競合が発生した場合、競合しているファイルの名前が変更され、ファイル名には各ユーザーの名前と現在の日時が付加されます。このため競合しているファイルが一目で分かり、必要に応じて処理できます。Access 7.0 より前のバージョンでは、こうした競合ファイルは新しいバージョンのファイルとして保存されていました。

- ウェブ クライアント インターフェイスを使用して、同期・共有のファイルを同期・共有のフォルダ間でコピーすることができるようになりました。
- 同期・共有のファイルのダウンロード リンクの生成とコピーは、Access サーバーにより送信される電子メールを必要とせずに実行できます。ファイルのダウンロード リンク機能は、有効にすることも無効にすることもできます。
- ユーザー名を「一時的」な外部ユーザーに割り当てることができるようになりました。通常、同期・共有のすべてのユーザーは、単なる電子メール アドレスではなくユーザー名で参照されるようになります。
- Access のクライアント バージョンが、Access サーバーの管理ページの [ユーザーとデバイス] セクションで表示されるようになりました（US8696)。
- 本リリースで Java 7 Update 71 が使用されるようになりました（US9486)。
- 直接ダウンロード リンクからファイルをダウンロードする際の、監査ログが改善されました（DE10961)。
- ファイルを種類別に並べ替えることが、ウェブ クライアント インターフェイスでできるようになりました（US6836)。
- [コントロール パネル] の [プログラムの追加と削除] を使用して Postgres を削除できるようになりました（US8270)。
- 直接ダウンロード リンクでのファイル共有機能を無効化するグローバル設定が追加されました（US8347)。
- 同期・共有のクォータに近づいた際のユーザー通知のデフォルトのしきい値と間隔を設定できるようになりました（US8605)。
- 本リリースで、Apache Tomcat 7.0.56 が使用されるようになりました（US9801)。
- 本リリースで OpenSSL のバージョン 1.0.1i が使用されるようになりました（DE11653)。
- デバイス テーブルでの一括操作（リモート ワイプ、リモート ワイプのキャンセルなど）に対するサポートが追加されました（US8875)。

バグ修正

- ローカル ユーザー グループに十分な権限がない場合に発生する可能性があるという、PostgreSQL インストーラの問題が修正されました。

- デバッグ ログを有効にしている場合に一部の UTF-8 ユーザー名でエラーが発生する可能性があるという、LDAP のクエリ実行の問題が修正されました。
- Acronis Access 登録電子メールの @display_name 変数の使用方法が修正されました。

既知の問題

- Internet Explorer 8 は、Acronis Access 7.0 のウェブ クライアントの初期バージョンではサポートされていません。IE8 ユーザーは Acronis Access ウェブ クライアントにログインできません。IE8 は今後のリリースで再びサポートされる予定です。今回のリリースでは、IE8 ユーザーは以前の Access 6 のウェブ UI が提供されますが、Access 7 の新機能を使用することはできません。Internet Explorer 8 を実行しているエンドユーザーがいる場合は、より安全なブラウザにアップグレードすることや、今後の Access サーバーのアップデートにサポートが追加するまでお待ちいただくことを検討してください（DE12649)。
- Windows XP ユーザーは、Access サーバーが 7.0 以降にアップグレートされた場合、Acronis デスクトップ同期クライアントやウェブ クライアントを使用できません。これは、XP および IE8 と Access サーバーで現在使用されているセキュアな SSL バインドとの間に互換性がないためです。管理者は、SSL バインドに変更することで XP ユーザーをサポートできます。詳細については、「ACRONIS ACCESS Tomcat SSL 暗号化の変更」を参照してください。暗号化を変更することで、サーバーが脆弱性にさらされ、一般的には安全でない状態になることに注意してください。
- Windows Server 2003 はサポートされなくなりました（US9572)。
- Access サーバー上でユーザー向けに設定された「モバイル アクセス」ネットワーク ホーム フォルダは、ウェブ クライアント インターフェイスで表示されません。この問題については、今後のリリースでサポートされる予定です（US9733)。
- ユーザーがアップロードするファイルを複数選択した場合、これらのファイルは同時にアップロードされるのではなく、1 つずつ順にアップロードされます（DE12512)。
- SharePoint のチェックイン/チェックアウトは、ウェブ クライアント インターフェイスでサポートされていません。この問題については、今後のリリースでサポートされる予定です（US8282)。

mobilEcho 4.5 からのアップグレードは、Acronis Access 7.0 の初期バージョンではサポートされていません。mobilEcho 4.5 からのアップグレードについては、今後のリリースで再びサポートされる予定です（DE12971)。

Acronis Access 6.1.3

機能強化

- Acronis Access のデフォルトの SSL バインドが、Internet Explorer 8 のクライアント接続ではサポートされなくなりました。安全でない Internet Explorer 8 の接続を新規インストールで有効にするには、「ACRONIS ACCESS Tomcat SSL 暗号化の変更」の内容を参照してください（US8460)。
- New Relic エージェントがバージョン 3.9.0.229 にアップデートされました。本リリースにアップグレードするまで、New Relic の動作が停止することにご注意ください。
- 大量の自己プロビジョニング フォルダの処理時における Access サーバーのパフォーマンスが最適化されました（DE11452)。
- Java 暗号化拡張機能が適切にインストールされていない場合にナレッジベースの資料へのリンクが表示されるように、ウェブ UI ログインが強化されました。詳細については、https://kb.acronis.com/ja/content/47786 を参照してください（US9226)。
- Mac 向け Acronis Access がアップデートされ、Mac OS X 10.9.5 がサポートされるようになりました（US9249)。
- インストーラに Java Version 7 Update 51 が組み込まれました。
- Apache Tomcat が 7.0.55 にアップデートされました（US9392)。

バグ修正

- デバッグ ログを有効にしている場合にユーザーのプロビジョニングでエラーが発生する可能性があるという、LDAP のクエリ実行の問題が修正されました（DE11545)。
- インストーラのインストール時またはアップグレード時に、Java のバージョンにかかわらず、Java 暗号化拡張機能ファイルが常にインストールされるようになります。これにより、システムにインストールされる Java のバージョンが 7.0.51 より新しい場合でも、正しい JCE ライブラリが使用されるようになります（DE11219)。

Acronis Access 6.1.2

機能強化

- Access ウェブ クライアント インターフェイスを介した、サイズの大きいファイルのアップロードに関する潜在的な問題が修正されました。
- "**完全に一致している必要があります**" オプションが "**LDAP 認証のためのドメイン**" に追加されました。**[LDAP 認証のためのドメイン]** の設定でリストされているドメインと一致する電子メール アドレス ドメインのユーザーに Access の共有招待メールが送信された場合、ユーザーは内部の LDAP（Active Directory)の認証情報でログインするように要求されます。**[LDAP 認証のためのドメイン]** と一致しないユーザーは、Acronis Access の外部ユーザー アカウントを作成するように要求されます。電子メール ドメインが **[LDAP 認証のためのドメイン]** のエントリのサブドメインのユーザーは、**[完全に一致している必要があります]** のチェックボックスがオフになっている場合、内部ユーザー用の LDAP 手順が記されたメールを受信します。このチェックボックスは、デフォルトおよびアップグレード版ではオフになっています。
- **[アプリケーション ポリシー]** の管理ページが修正され、Acronis Access for Android 3.2.3 アプリケーションの変更内容が反映されました。
- URL 経由でのアクセス権限がない同期・共有フォルダへのアクセス時に、アクセスが拒否され、リダイレクトされることに加え、エラー メッセージが表示されるようになりました。
- 共有フォルダのメンバーが他のメンバーにダウンロード リンクを送信した場合、共有フォルダの所有者は監査ログを表示できるようになりました。
- 設定ユーティリティがアップデートされ、OpenSSL 1.0.1h を使用するようになりました。
- Tomcat のバージョンが 7.0.54 にアップデートされました。
- 本リリースで Java 7 Update 51 が使用されるようになりました。

バグ修正

- Amazon S3 リポジトリからの**同期・共有**ファイルのダウンロードに関する問題が修正されました。

- 電子メール アドレスが関連付けられていない一時的な Access サーバーの管理者の識別に関する問題が修正されました。
- エクスポートされたログの **owner_name** の値の入力に関する問題が修正されました。
- アップグレード後に一部のプロビジョニング済み管理者グループがログインできなかったという問題が修正されました。
- 大規模な Active Directory にモバイル クライアントを登録する場合に、発生する可能性があった要求タイムアウトの問題が修正されました。
- ドメインのメンバーではない Windows Server がインストールされた場合に発生した、サービスの自動スタートアップの問題が修正されました。
- 同じプロダクト キーを使用して同一ネットワーク上で複数のゲートウェイ サーバーを実行していた場合に発生したライセンス メッセージの問題が修正されました。
- Acronis Access モバイル アプリケーションで**同期・共有**フォルダにアクセスした場合に発生した断続的な SSL のエラーが修正されました。
- インストーラでの Java 検出に関する複数の問題が修正されました。
- クライアントで実際の問題を示すエラーのかわりに Python 例外がレポートされていた問題が修正されました。

既知の問題

- Access サーバー 6.1 からのアップグレード時に **[Apache Tomcat のポート 80 用のリダイレクト]** オプションが設定されていた場合、オプションが維持されません。アップグレード後に、設定ユーティリティでこのオプションを手動で有効にしてください。

Acronis Access 6.1.1

機能強化

- Acronis Access にログインしている大規模な Active Directory カタログでのユーザーの認証速度が改善されました。
- Access API を介してユーザーの同期・共有のクォータを設定することが、ギガバイト（GB)単位で行えるようになりました。

- ゲートウェイ サーバーと Microsoft SharePoint のインタラクションのエラー処理が改善されました。
- Mobile Access のグループ ポリシー作成時に組織単位やドメインが表示されなくなりました（サポート対象外のため)。

バグ修正

- ユーザー名に予約済みの "data" 文字列が含まれているユーザーが、モバイル アプリケーションの登録を完了できるようになりました。
- ゲートウェイ サーバーを表示可能に設定し、複数のデータ ソース フォルダも割り当てられるようにした場合、Access モバイル アプリケーションで Acronis Access ゲートウェイ サーバーがリストに複数表示される、という問題が修正されました。
- Access サーバー クラスタ グループでのログ作成の有効化/無効化が修正されました。
- Windows Server 2008R2 の再起動後に Access ゲートウェイ サービスが起動できないという依存関係の問題が解決されました。

Acronis Access 6.1

機能強化

- Acronis Access サーバー管理用のウェブ サービス API。API ドキュメントは、Access サーバーに付属しており、管理者がアクセスできます。リンクは、フッターにあります。
- Acronis Access の監査ログで、古いログ エントリの自動的なエクスポートや消去を設定できるようになりました。エクスポートと消去の設定は、[監査ログ] → [設定] ページで行えます。
- Acronis Access の設定の概要ツールが新たに導入されました。これにより Acronis サポートに送信する関連サーバーの設定に関する詳細情報が収集されます。
- 一般的なパフォーマンスの改善と Active Directory グループ メンバーシップ情報のキャッシュにより、ログイン パフォーマンスが向上しました。
- 管理者がカスタムの電子メール テンプレートを保存する前にプレビューできるオプションが追加されました。

- Acronis Access サーバーのロゴとカラー スキームを簡単にカスタマイズできるようになりました。サーバーをカスタマイズする方法については、「ウェブ インターフェイスのカスタマイズ」を参照してください。
- 同期・共有のアクセス権を持たない、新たに招待された管理者宛ての電子メールをカスタマイズするための新しい電子メール テンプレートが追加されました。
- ゲートウェイ サーバーの [ログ] タブが、[詳細] から [編集] のメニュー項目に移動しました。
- 登録の招待を追加する場合、検索結果に、ユーザーの登録済みデバイスがあるかどうかが表示されるようになりました。
- Acronis Access では、受信者の電子メール アドレスが無効のため電子メールの配信ができなかった場合、元の送信者に電子メールが送信されるようになりました。
- ホワイトリストとブラックリストを [許可されたアプリ] ページでデフォルトのプロファイルに割り当てられるようになりました。
- 管理者は LDAP 設定ページでリンクをクリックすることで、キャッシュされたすべての LDAP 情報を更新できるようになりました。
- 同期・共有のアクセス権の許可をプロビジョニング済み LDAP 管理者グループで設定できるようになりました。
- クラスタ グループのメンバーをクラスタ グループのメニューから追加できるようになりました。
- Windows 8.1 がサポートされるようになりました。
- インストーラにより、PostgreSQL が別のサーバーにある場合のインストール サポートが追加されました。
- PostgreSQL のインストール プロセスが改善されました。
- アンインストール プロセスが改善されました。
- ウェブ インターフェイスのエラー レポート機能が改善されました。

バグ修正

- [ゲートウェイ サーバー] ページの再ロード時にアクティブ セッション数が更新されるようになりました。

- 共有ファイルや共有フォルダに招待するユーザーを選択するための先行入力検索が Internet Explorer 8 でサポートされるようになりました。
- Acronis ゲートウェイ サーバー サービスが、サーバーの起動時に正常に起動するように他の主要サービスを利用するようになりました。
- クラスタ グループが無効になると、そのクラスタ グループを「マイ ネットワーク フォルダ」(ユーザーが追加した場所)にアクセスするためのゲートウェイ サーバーとして使用していたどのポリシーも、クラスタ グループのメンバーだった直前のゲートウェイ サーバーを代わりに使用するようにアップデートされます。
- 登録済みユーザーの電子メール アドレス フィルタ機能に関する問題が修正されました。
- エラー メッセージが表示された後で言語の設定を変更すると管理者に致命的なエラーのページが表示されるという問題が修正されました。
- 有効期限切れのサーバーのアップグレード後に試用版の使用延長を申請する際に管理者で発生していた問題が修正されました。
- LDAP の同期・共有ユーザーは、電子メール ドメインが LDAP 認証のドメインと一致しない場合でも、認証の正常終了後に LDAP として常に一覧表示されるようになりました。電子メール ドメインが LDAP 認証のドメインに含まれていない場合でも、管理者を LDAP から追加できるようになりました。
- 管理者が新しいユーザーや管理者を追加する際に、その追加ユーザーの電子メール アドレスが無効の場合は管理者にエラー メッセージがすぐに送信されるようになりました。
- 既存の管理ユーザーに同期・共有のアクセス権を付与するするように保留中の招待メールを正しく解決できるようになりました。
- ユーザー テーブルのエクスポートに [ライセンス取得済み] フィールドが追加されました。
- ダウンロード リンクを送信する際にブラックリスト制限とホワイトリスト制限が適用されるようになりました。
- 登録対象の新しい LDAP ユーザーの検索が非常に高速になりました。
- プロビジョニング済み LDAP 管理者グループと、プロビジョニング済みの同期・共有の LDAP グループの両方に属する新しいユーザーには許可がまとめて付与されるようになりました。

- 使用可能なデータ ソースで %USERNAME% ワイルドカードが使用されている場合、既存のデータ ソースへのホーム ディレクトリのマッピングが正常に処理されるようになりました。
- LDAP 検索で、グループ メンバーシップとして無効な選択肢である組み込みグループが表示されなくなりました。
- ホーム ディレクトリ検索に時間がかかるためモバイル ユーザーが登録できないという問題が修正されました。
- Windows 2003 R2 で証明書による割り当て済みソースの認証やアクセスを行えないことがあるという問題が修正されました。
- ライセンスを取得していないアドホック ユーザーがクライアントからサーバーへ接続できないように正しく制限されるようになりました。
- ゲートウェイ サーバーの表の情報が、サーバーの [詳細] タブを開いたときではなく、すぐにアップデートされるようになりました。
- Acronis Access から送信される電子メールの表示用 [差出人] フィールドに、差出人の実際の電子メール アドレスが表示されるようになりました。
- 新しい基本プロダクト キーが適用されると、古い Acronis Access プロダクト キーが削除されるようになりました。
- アップグレード時に、インストーラで複数のゲートウェイ サーバーのエントリが [プログラムと機能] に作成されるという問題が修正されました。
- ゲートウェイ サーバーのメモリ リークが修正されました。

Acronis Access 6.0.2

バグ修正

- **HeartBleed** の脆弱性に対応するため、OpenSSL DLL がアップグレードされました。

Acronis Access 6.0.1

機能強化

- 新しいポリシーが追加され、Active Directory で割り当てられたユーザーのホーム フォルダの共有に使用するゲートウェイまたはクラスタ グループを指定できるようになりました。Active Directory で割り当てられたホーム フォルダはゲートウェイによって

自動的に共有されるようになり、手動でデータ ソースを作成したり、[ユーザーが UNC パスまたは URL を指定してネットワーク フォルダを追加できるようにする] ポリシー設定を有効にしたりする必要がなくなりました。

- [LDAP の設定] ページに新しい設定の [LDAP 情報をキャッシュする間隔] が追加され、Acronis Access サーバーでの LDAP ユーザーおよびグループに関するキャッシュ情報のアップデート頻度を管理者が指定できるようになりました。
- [モバイル アクセスの設定] ページで新しい設定の [ユーザー プリンシパル名（UPN) を使用したゲートウェイ サーバーの認証] が利用できるようになりました。この機能を有効にした場合、登録時に使用されたユーザー名の形式に関わらず、ユーザーは UPN でゲートウェイ サーバーへの認証を行います。無効にした場合、登録時に使用されたユーザー名の形式でユーザーは認証を行います。
- LDAP グループ メンバーシップが識別されるときのパフォーマンスが向上し、登録および認証にかかる時間が短縮されました。パフォーマンス改善のため、グループ メンバーシップの識別時に、デフォルトで入れ子の LDAP 配布グループを含めないようにしました。入れ子の配布グループのメンバーを含めるように設定する必要がある場合は、LDAP 設定ページで、新しい設定の [入れ子化された配布グループのメンバーシップを含む] を有効にしてください。

バグ修正

- クライアントが大量のファイルをダウンロードまたはアップロードした場合に、Windows 上の Access デスクトップ クライアントの異常終了が発生しなくなりました。
- 新規インストールでゲートウェイ サーバーを追加した後にゲートウェイ サーバーが自動的に接続されることにより、クラスタ グループの追加や自己プロビジョニングの有効化をすぐに実行できるようになりました。
- 同期および共有機能とデータ ソースが、ライセンスの期限が切れた後の猶予期間でも継続的に利用できるようになりました。
- 監査ログ ライセンスの警告メッセージが、すべての状況において適切にローカライズされました。

- パラメータにパイプ記号 (‘ |’)が含まれている場合においてボリュームにアクセスできなくなるという問題が修正されました。
- デバイスで英語、フランス語、ドイツ語、日本語以外の言語が設定されている場合に Acronis Access モバイル アプリケーションからリンクや招待を送信できないという問題が修正されました。
- 英語版以外のインストール環境でのアップグレード時に、インストーラで複数のゲートウェイ サーバーのエントリが [プログラムと機能] に作成されるという問題が修正されました。
- Acronis Access Tomcat Service が正常に起動しない状況が定期的に発生し、クライアントが接続できるようにするには再起動が必要になるというバグが修正されました。
- サーバーを 4.x からアップグレードした後に、管理サーバーに接続した場合、「セッションごと」に資格情報が必要となるように設定されているクライアントに対してパスワードの確認が表示されるというバグが修正されました。
- プロファイルでゲートウェイ サーバーかクラスタ グループのいずれかを使用するように設定されている場合、サーバーまたはクラスタ グループのオンライン状態に関わらず、自己プロビジョニング フォルダの追加や削除を正常に実行できるようになりました。
- ポリシーの優先順位が考慮されるようになり、ユーザーは、ユーザーが登録されている優先度の高いポリシー グループを受信するようになりました。
- 同期と共有機能を有効にしていないクライアントが監査ログで「非管理」として不適切に報告されるという問題が修正されました。
- 日本語またはその他の文字がファイル名に含まれているファイルを Internet Explorer でダウンロードした場合にファイル名が変更されるという問題が修正されました。
- サブスクリプション ライセンスの期限が切れた際に、解決できないエラーと管理者に表示されるという問題が修正されました。
- Access デスクトップ クライアントの最小バージョンの一覧に 3.0 クライアント バージョンが追加され、以前のデスクトップ クライアントおよび新しいデスクトップ クライアントの両方に適用されるようになりました。
- mobilEcho 5.0 より前のバージョンからのアップグレード後にホーム ディレクトリにアクセスできなくなるという問題が修正されました。

- ローカリゼーションに関する複数の修正。

Acronis Access 6.0.0

機能強化

- mobilEcho と activEcho の 2 製品が Acronis Access Server と呼ばれる新しい単一の製品にまとめられました。 これにより、モバイル クライアントとデスクトップ クライアントだけでなく、ウェブ アプリケーションも、ブランド名や製品名が変更されています。 Acronis Access Server 6.0 は mobilEcho や activEcho に対するアップグレードとしてインストールでき、既存のライセンスは引き続き有効です。 お客様には、既存の mobilEcho ライセンスや activEcho ライセンスを新しい Acronis Access ライセンスと交換する権利が提供されます。新しいライセンスにより、統合製品のすべての機能が有効になります。 このアップグレードを希望する場合は、**このウェブ フォームを送信**してください。
- Active Directory ベースの管理者ユーザーに電子メール アドレスを割り当てる必要がなくなりました。管理者ユーザーの追加も、SMTP 用に Acronis Access Server を構成せずに行えます。
- 同期と共有機能の有効/無効の切り替えを可能にする新しいチェックボックスが、[サーバー設定] に用意されています。デフォルトでは、mobilEcho から Acronis Access Server にアップグレードすると、同期と共有（旧称 activEcho)が無効になります。
- Active Directory の配布グループを、同期と共有フォルダに招待できるようになりました。
- 同期と共有フォルダに多数のユーザーを招待する処理が、かなり高速になりました。
- サーバーの設定時に設定ユーティリティに表示される、ステータスや進行状況のメッセージの量が増えました。
- リポジトリがリモート ネットワーク ボリューム上にあるにもかかわらず、Repository Service がローカル システム アカウントの下で実行するように設定されている場合、設定ユーティリティでエラーが生成されるようになりました。Repository Service は、リモート ネットワーク ボリュームへのアクセス許可を持つアカウントの下で実行する必要があります。
- 埋め込みの秘密キーを持たない SSL 証明書が選択された場合、設定ユーティリティでエラーが表示されるようになりました。

- Java が Version 7 Update 51 にアップグレードされました。
- [サーバー設定] の「サーバー名」が、エンド ユーザーに表示されるウェブ サイトのタイトルとして使われるようになりました。
- LDAP キャッシュの更新間隔が 60 分から 15 分に変更されました。
- ゲートウェイ サーバー用の新しい詳細設定が追加されました。有効の場合、ユーザーは各自の UPN（例: username@domain.com)を使用して認証を行います。無効の場合、ユーザーは各自の別々のドメインとユーザー名（例: domain¥username)を使用して認証を行います。これは、SharePoint 365 など、一部のフェデレーションへの認証シナリオで必要になることがあります。

バグ修正

- [サーバー設定] の [デフォルトの言語] 設定の名称が変更され、デフォルトの監査ログ言語であることが明確になりました。
- Active Directory ホーム フォルダのデータ ソースを解決できない場合、!HOME_DIR_SERVER へのアクセス時にエラーが表示される代わりに、Mobile Client にホーム フォルダが表示されないようになりました。
- Acronis Access デスクトップ クライアントのその他のバグ修正。
- ローカリゼーションに関するその他の改善点。

Acronis Access 5.1.0

機能強化

- Access サーバーが HTTP ポート 80 にバインドし、設定されている HTTPS ポートに自動でリダイレクトするかどうかを、設定ユーティリティを使用して制御できるようになりました。これまではデフォルトで有効になっていましたが、現在では、クリーン インストールの際に管理者が有効にする必要があります。
- 電子メール テンプレートを編集する際に、管理者が電子メール件名のデフォルト値を表示するための新しいオプションを利用できるようになりました。
- iOS で mobilEcho 5.1 以降を使用するユーザーは、ファイル共有または SharePoint ロケーションにアクセスするため、アプリケーションから直接にデータ ソースを作成できるようになりました。ユーザーは、クライアントから UNC パスまたは SharePoint

URL を入力します。クライアントにそれらのデータ ソースの作成を許可するかどうか、またそれらの要求のためにどのゲートウェイ サーバーを使用するかを制御するための新しいポリシー設定が管理サーバーに導入されました。

- クラスタ グループにより、複数のゲートウェイ サーバーで 1 つの共通の設定を共有できるようになりました。クラスタ グループに割り当てられている設定値やポリシーに変更が加えられると、グループのすべてのメンバーにそれが自動的に適用されます。一般にこれは、可用性を高めるため、負荷分散装置の背後に複数のゲートウェイ サーバーを配置している場合に使用されます。
- ゲートウェイ サーバーで、Kerberos を使用した認証がサポートされるようになりました。これは、クライアント証明書を使用したリバース プロキシにより mobilEcho iOS クライアントの認証を実施するために Kerberos 制約付き委任を使用するシナリオにおいて使用できます。また、MobileIron AppTunnel を使用したクライアント証明書によるモバイル デバイスの認証でも使用できます。この形式の認証を使用している場合、モバイル クライアントから activEcho 共有にアクセスすることはできないという点に注意してください。
- ホーム フォルダをユーザーまたはグループ ポリシーに割り当てる際に、必要なデータ ソースが自動的に作成されるようになりました。これまでは、そのホーム ディレクトリのホスト サーバーのためのデータ ソースを、管理者が手動で作成することが必要でした。
- レガシー ゲートウェイ サーバーのアドレスを変更できるようになりました。
- Android のポリシー例外が更新され、mobilEcho Android 3.1 クライアントの機能が反映されるようになりました。

バグ修正

- 監査ログから大量のレコードをエクスポートする処理が、大幅に高速化されました。
- 一部のダイアログで表示されるエラー メッセージが、エラー条件の解消時点で正しくクリアされるようになりました。
- 設定ユーティリティは、一度に 1 つのインスタンスのみ実行可能になりました。

- Windows Server 2003 でのアンインストール プロセスにおいて、PostgreSQL が Acronis Access Server インストーラによってインストールされていないというレポートが出なくなりました。
- ゲートウェイ サービスを全アドレスの 1 つのポートにバインドするように設定し、かつ Access Server が特定のアドレスの同一のポートを使用する場合、設定ユーティリティでエラーが生成されるようになりました。
- クリーン インストールでのデフォルトとして、Tomcat はポート 8005 上でシャットダウン要求をリッスンしないよう設定されるようになりました。これにより、サーバー上の Tomcat の他のインスタンスとの競合が回避されます。Access Server Tomcat インスタンスはサービスとして実行されるため、ネットワーク ポートを通じてのシャットダウン要求は不要です。
- ローカリゼーションに関するその他の改善点。
- 非管理者ユーザーのログ表示のパフォーマンス向上
- Access Server 管理者により activEcho が無効にされている場合、ライセンス期間終了の通知が表示されなくなりました。
- 新規ユーザーに対する招待電子メールのメッセージが、パスワード変更ではなく初期パスワードの設定を求めるものになりました。
- Internet Explorer 8 または 9 を使用している場合に、[新しいファイルのアップロード] ダイアログで余分のフィールドが表示されなくなりました。
- Windows デスクトップ クライアントで、特定の状況においてユーザーのパスワードの期限が切れてそれが再入力された場合に、コンテンツが再アップロードされなくなりました。
- デスクトップ クライアントのファイル同期ロジックに関するその他の修正事項
- カスタム ホーム フォルダを伴うユーザーまたはグループ ポリシーを削除すると、ゲートウェイ サーバー上のボリュームが正しく削除されるようになりました。
- ユーザーに割り当てられているソースを表示すると、グループ メンバーシップによりそのユーザーに割り当てられているソースが表示されるようになりました。
- データソース管理ページのタブの順序が改善されました。
- ゲートウェイ サーバー管理アドレスを変更して [適用] をクリックした場合に、編集ダイアログが閉じなくなりました。

- サーバーの LDAP キャッシュにユーザーがまだ含まれていない場合、クライアント証明書を使って mobilEcho クライアントを管理のために登録しても、周期的に失敗しなくなりました。
- ゲートウェイ サーバーのアドレスに空白スペースを追加した場合に、ゲートウェイ サーバーが正しく管理対象とならなくなる現象が解消されました。
- デバイス情報ダイアログのメモが正しく保存されるようになりました。
- ポリシー リストでは、無効にされているポリシーがグレー表示されるようになりました。
- mobilEcho Server 4.5 からのアップグレードで、間違った LDAP 検索ベースを設定ウィザードに入力しても、mobilEcho ユーザーが正しくインポートされるようになりました。
- ライセンスのページにおいて、YD1 で始まるプロダクト キーが、永久ライセンスとしてではなく有効期限日を持つ試用版として正しく表示されるようになりました。
- 登録電子メール招待に含まれる Android クライアントのリンクが正しいものになりました。
- ゲートウェイ サーバーに SharePoint 接続をサポートするライセンスがない場合、そのゲートウェイ サーバーの SharePoint 資格情報の編集機能が無効にされるようになりました。

Acronis Access 5.0.3

機能強化

- ACRONIS ACCESS サーバーを Windows Server 2003 SP2、2008/2008R2 および 2012/2012R2 の Windows フェイルオーバークラスタにインストールできるようになりました。この設定でインストールまたはアップグレードを実行する手順については、「クラスタ上での ACRONIS ACCESS のインストール 『354ページ 』」および「クラスタでの ACRONIS ACCESS のアップグレード」を参照してください。

バグ修正

- カスタム テンプレートを使用していた場合、アップグレード後に電子メール通知が正しく送信されるようになりました。

- データ ソース設定時に、フォルダ名の一部としてユーザー名全体ではなく %USERNAME% トークンを使用できるようになりました。
- データ ソースが新たに作成される場合、それが検索可能かどうかのチェックがすぐに実行されるようになりました。これまでは 15 分間隔でしか実行されませんでした。
- ゲートウェイ サーバー始動後に、検索インデックスを追加するデータ ソースを検索対象とした検索が可能になりました。

Acronis Access 5.0.2

機能強化

- ACRONIS ACCESS サーバーは、Windows Server 2012 R2 の認定を取得しました。
- SMTP が設定されていない場合でも、LDAP 管理者を追加できるようになりました。
- 設定ユーティリティで変更を適用したときに、重複したファイアウォール ルールが作成されなくなりました。
- 複数のドメインを含む大規模な LDAP ツリーで、認証のパフォーマンスが大幅に向上しました。
- 大量の更新がある場合の activEcho クライアントのパフォーマンスが向上しました。
- [データ ソース] のフォルダ一覧で、割り当て済みのゲートウェイ サーバーが IP アドレスではなく表示名で表示されるようになりました。

バグ修正

- ローカライズの改善。
- Windows Server 2003 で、インストーラ アプリケーションからアンインストールを選択できるようになりました。
- インストーラでインストールする前に必要なディスクの空き領域が最低 1 GB になりました。
- 英語版以外の PostgreSQL インストールで、activEcho 2.7 から正常にアップグレードできるようになりました。
- 名前にコロンを含むデータ ソースにクライアントからアクセスできるようになりました。

- mobilEcho 4.5 からのアップグレードで、SharePoint データ ソースの移行が正しく処理されるようになりました。
- アップグレードの後、[データ ソース] の [割り当て済みのソース] タブに、ユーザーに割り当てられたリソースが正しく表示されるようになりました。
- [アクティブ ユーザー] テーブルをポリシーまたはアイドル時間で並べ替えたときに、エラーが発生しなくなりました。
- クライアントで表示できるようにプロビジョニングされたゲートウェイ サーバーや、クライアント接続用のアドレスが異なるゲートウェイ サーバーに、クライアントからアクセスできるようになりました。
- Access サーバーに同じようなパス（"¥¥homes" と "¥¥homes2" など)を持つデータ ソースが含まれている場合に mobilEcho クライアントでホーム フォルダを開くことができないバグが修正されました。

Acronis Access 5.0.1

バグ修正

- 古いバージョンの mobilEcho で作成されたデバイスのパスワードのリセットが保留になっている場合に mobilEcho 4.5 から 5.0 へデータベースを移行できない問題が修正されました。この問題のため、サーバーを起動すると ウェブ ブラウザに以下のようなエラーが表示されていました。

  ActiveRecord::JDBCError: ERROR: value too long for type character varying(255): INSERT INTO "password_resets" ....
  Customers that have this condition can upgrade to this new version of the server and the problem will be resolved automatically.
- mobilEcho 5.0 へのアップグレード後に一部のクライアントが制限モードに移行する問題を修正しました。
- 管理サーバーのデータ ソース テーブルに、ゲートウェイ サーバーの IP アドレスではなく表示名が表示されるようになりました。

Acronis Access 5.0.0

機能強化

- ACRONIS ACCESS サーバーは、mobilEcho と activEcho の両方に使用する新しい共有サーバープラットフォームです。両方の製品が同じ共有バックエンド インフラストラクチャを使用するようになりました。各製品の機能は、ライセンスに基づいて決定され、有効にされます。
- 新しい統合プラットフォーム インストーラ。ACRONIS ACCESS サーバー、mobilEcho、および activEcho は、インストーラに含まれています。インストーラ実行時インストール オプションを使用すると、管理者はどの構成要素を導入するか決定できます。
- ACRONIS ACCESS サーバーは自動的に Java JRE と必要な Java 暗号化エンジンポリシーファイルをインストールします。
- 新しいサーバー設定ユーティリティを使用すると、管理者は、特定の IP アドレスおよびポートへのバインディング、ローカル マシンのファイアウォール ルールの処理、SSL 証明書のインストールなど、ベース構成オプションを設定できます。
- ACRONIS ACCESS サーバーは、英語、ドイツ語、日本語およびフランス語でローカライズされています。
- 新しいスタートアップ ウィザードはサーバーの初期設定を簡素化します
- モバイル デバイスをサポートする応答設計を含む、再設計され、アップデートされたユーザーおよび管理ウェブ インターフェイス。
- 新しいページング テーブルは、はるかに大きいデータのセットの表示、並べ替えおよびフィルタリングをサポートします。ユーザー名の部分的入力、メッセージ タイプ別、などによるフィルタリングを含むログのフィルタリングが向上しています。
- 再設計され、使いやすくなったエンド ユーザー向け [プロジェクト] ビュー。
- activEcho クライアント（Mac/Windows)は、ドイツ語、日本語およびフランス語でローカライズされています。
- HTML5 ドラッグ アンド ドロップをサポートし、ウェブ インターフェイスに直接ファイルをアップロード。ドラッグ アンド ドロップにより 1 回の操作で 1 つまたは複数のファイルをアップロードできます。
- ウェブ インターフェイスでの進行状況インジケータやアップロードをキャンセルする機能など、ファイルのアップロード処理が向上。

- フォルダは、ウェブ UI にある [プロジェクト] ビューから ZIP ファイルとしてダウンロードできます。
- 個々のファイルは他のユーザーと共有できます。相手のユーザーはファイルをダウンロードするリンクを受け取ります。リンクには有効期限を設定できます。
- 共有招待ダイアログでは、ローカル ユーザーと Active Directory/LDAP のユーザーの両方に対して先行入力をサポートします。
- 以前のリビジョンの、検索/ダウンロード/以前のバージョンのファイルの復元の各機能が再設計され、さらに柔軟になりました。以前のリビジョンを選択して、「最新にする」ことができます。
- activEcho デスクトップ クライアント (Mac/Windows)では、同期されているファイルの進行状況インジケータが表示されるようになりました。
- 新しい [サブスクリプションの停止] ボタンが共有されるフォルダで利用できます。
- プロジェクト フォルダを閲覧するとき、エンド ユーザーが選択した並べ替え条件が保存されます。
- イベント通知をすべての共有のデフォルト設定としてグローバルに構成できるようになりました。ユーザーは、個々の共有のデフォルトを無効にできます。
- ファイルをダウンロード/同期したとき、通知が送信されるように構成できます。
- Windows の activEcho クライアントは、組み込みの Windows 証明書ストアを使用して、SSL 証明書の検証を実行できます。これにより、サード パーティ認証局との互換性が向上します。
- システムに数千のユーザーがいるときに、コンテンツの再割り当てに対応するユーザーインターフェイスの応答性が向上しました。
- 管理ページで Amazon S3 アクセス キーがプレーン テキストで表示されなくなりました。
- 多数のユーザーまたはファイルがあるとき、特にクォータが使用中のページ読み込み時間が向上しました。
- さまざまな形式の電子メール アドレスを使用するように、招待メールのサポートを向上しました。
- ブラックリストとホワイトリストを共有するため、ドメインでワイルドカードが使用できるようになりました。

- 管理者は、[グループ作業者が他のグループ作業者を招待できるようにする] チェックボックスをグローバルに非表示にできます。
- 新しい管理モードは、ユーザーの個別のプロジェクト/ログ表示と管理コンソールを切り替えます。
- mobilEcho クライアント管理が共通のウェブ管理インターフェイスに完全に統合されました。これは、activEcho のモバイル クライアントの管理に使用でき、また、mobilEcho ライセンスを指定した場合、1 台のコンソールですべての mobilEcho と activEcho 機能を管理できます。
- ユーザー リストをエクスポートできるようになりました。
- mobilEcho クライアント管理サーバーは、ACRONIS ACCESS サーバーと統合され、Apache Tomcat および PostgreSQL データベースに基づき、拡張性と復元力が向上しました。
- 以前には個々の mobilEcho サーバーを管理するために使用されていた mobilEcho Administrator は削除されました。Access ゲートウェイサーバー（旧称 mobilEcho File Access Server)は、ACRONIS ACCESS サーバーウェブ管理ユーザーインターフェイス内で直接管理されるようになりました。
- mobilEcho クライアント管理サーバー構成ファイルが削除されました。以前に構成ファイルにあった設定は自動的に移行され、ACRONIS ACCESS サーバーウェブ管理ユーザーインターフェイスを通して管理されるようになりました。
- モバイル デバイスに共有されるデータ ソースの構成（以前は割り当てられた「フォルダ」)が再設計されました。
- 「割り当て済みのソース」機能により、管理者は、特定の Active Directory ユーザーまたはグループが受け取る、割り当てられたすべてのリソースのレポートを取得できます。
- 監査ログを有効にして、複数の ACRONIS ACCESS ゲートウェイサーバー全体でモバイルユーザーのアクティビティをレポートできます。
- 管理者は、ユーザー、データ ソース、モバイル ポリシーの管理や監査ログの表示などの管理アクティビティ用権限を付与できるようになりました。これは、個々のユーザーまたは Active Directory グループのメンバーシップに基づくことができます。
- リモート ワイプやデバイス リストからのデバイスの削除などのデバイス操作を一括して実行できるようになりました。

- 構成済みの Active Directory ユーザーまたはグループ ポリシーに一致しないすべてのユーザーに適用するキャッチオール「デフォルト」ポリシーを構成できます。
- 新しいポリシー オプションでは、[マイ ファイル] フォルダおよび [ファイル受信ボックス] フォルダ内のデバイスのコンテンツが期限切れになり、一定の期間後に削除される仕様が可能です。
- Active Directory グループに登録招待メールを送信するとき、別のグループから登録済みのユーザーをフィルタして除外できます。
- 既存のユーザー/グループ ポリシーと一致しないユーザーが登録に招待されると、警告が表示されます。
- デバイス テーブルには、各デバイスで使用中のユーザーまたはグループ ポリシーが表示されます。
- ユーザーに関してキャッシュされた Active Directory/LDAP 情報が、バックグラウンドで定期的にアップデートされるようになりました。
- コンテンツ検索が、Windows Search を実行しているリモート Windows ファイル共有に対して利用できるようになりました。
- デバイスがポリシーで管理されている場合は、そのポリシーは削除できません。
- mobilEcho 登録招待メール テンプレートをウェブ管理コンソール内から直接変更できます。各テンプレートについて複数の言語がサポートされます。
- 登録招待メール テンプレートで新しいトークンを利用して、Active Directory ユーザーの表示名を含めることができます。
- デバイス リストとデバイスの詳細画面に、デバイスが Good Dynamics または MobileIron AppConnect のどちらに管理されているかが表示されるようになりました。
- Apache Tomcat ウェブ サーバーに移行したため、SSLv2 によるウェブ管理コンソールへの認証のサポートは非推奨になりました。
- New Relic によるトレース ログおよびパフォーマンス監視のサポート。

バグ修正

- Unicode 文字の TXT または CSV ファイルへのエクスポートのサポートが向上しました。
- 共有できないフォルダから、[招待...] オプションがなくなりました。
- 他のユーザーを共有に招待する許可がないユーザーでも、共有から自分たちを削除できるようになりました。
- ファイルまたはフォルダの名前が長すぎるため Windows クライアントにダウンロードできない場合、ウェブ インターフェイスで [デバイスに同期] オプションをオフにすると、共有フォルダ全体が削除されるため、エラーを解決できます。
- ファイルをアップロードしていて、ユーザーのクォータ容量が不足した場合、activEcho クライアントが適切にエラーを処理します。
- ブラックリストに記載されているユーザーでも削除できるようになりました。
- 暗号化が無効な場合、ファイルをリポジトリにアップロードできます。
- グローバル カタログを使用するように LDAP を構成したとき、ホーム ディレクトリ構成が、正しく取得されるようになりました。
- 末尾のスペースを使用したとき、Active Directory 参照の処理が向上しました。
- .CSV ファイルにエクスポートするとき、「登録日時」の日付が正しくフォーマットされるようになりました。
- ウェブ管理ユーザー インターフェイス経由での Unicode の表示サポートが向上しました。
- スペースで終わっている SharePoint フォルダをクライアントが列挙できるようになりました。
- 余分なスラッシュのある SharePoint ライブラリで、ファイル削除とコピーが正しくサポートされるようになりました。

15.2 以前のリリース

15.2.1 activEcho

activEcho 2.7.3 (Released: June 2013)

ENHANCEMENTS:

Switched to using the official AWS library file for Amazon S3 connections.

Files now can be successfully uploaded to any of the eight Amazon S3 bucket regions.

BUG FIXES:

Pending users can now be deleted without error.

Files which were not fully uploaded to the Amazon S3 file repository will now be removed from the repository if the repository is accessible after the upload failure occurs.

Files can be uploaded and downloaded when the file repository is not using encryption.

activEcho 2.7.2 (Released: May 2013)

BUG FIXES:

Files which were not fully uploaded to the file repository will now be removed from the

repository if the repository is accessible after the upload failure occurs.

Fixed a rare case where the activEcho client would fail to sync due to the structure of a system file ID.

activEcho 2.7.1 (Released: April 2013)

ENHANCEMENTS:

The activEcho web server and system can now be monitored using the New Relic monitoring tools. For more information about the new functionality and obtaining a license, refer to http://newrelic.com/

Upgrading will now maintain intermediate certificate files configured for the activEcho Tomcat installation's HTTPS connections.

Improved load speed of users page by caching content usage.

BUG FIXES:

Web users running on Internet Explorer 8 or Internet Explorer 9 in compatibility

mode will no longer receive an error that their browser is incompatible with activEcho.

Folders with names in the format YYYYMMDD will no longer fail to sync from the activEcho client to the server.

activEcho 2.7.0 (Released: February 2013)

ENHANCEMENTS:

Mac and Windows sync clients will now be notified when they have updated content available for download. These notifications will reduce load on the server and improve performance by avoiding many unnecessary requests from clients to the server to check for updates when none are available.

Mac and Windows sync clients have been made more resilient to errors on single files and folders. The client syncing process will no longer stop if a single locked file is updated. All other files which can be successfully updated will be. The client syncing process will also no longer stop is a file cannot be successfully downloaded. All other files which can be successfully downloaded will be.

Mac and Windows sync clients can now automatically download and install updates.

Download speed of large numbers of files to sync client has been improved.

Altering the preferences on the client will no longer cause a paused client to begin syncing.

Windows sync client now offers a "Show previous activEcho versions" context menu option.

The Projects tab in the web interface has been optimized for increased performance and smoother user interaction.

The Projects tab now supports pagination, sorting, filtering.

The move dialog in the web interface now loads quickly, even when the user has a large hierarchy of folders.

All client connections can be disabled for administrative purposes from the Server Settings page in the web UI.

All timestamps used for comparison or calculation will now be set to database time instead of server time to ensure proper operation in a cluster scenario.

The web interface now provides support for non-US date-time formats.

Duplicate folder updates will no longer cause multiple revisions of the folder to be created.

The default PostgreSQL installation is now configured with more carefully tuned parameters to improve performance.

User proxy AD objects can now successfully authenticate to activEcho.

Multiple domains can now be provided for LDAP configuration to be automatically pre-pended to usernames for login.

Links in emails when sharing a folder to a new user will now direct the user into the new share on the website. Note that if the default templates have been altered, the passkey paths in the notification email template will need to be modified to look like this:

```
<%= @root_web_address %>

<%= passkey_path( @passkey, { :redirect_path =>
```

show_contents_node_path(@node.uuid, {:show_sync_lightbox => true}) }) %>

Files will no longer be marked deleted if they can't be found in the repository. They will need to manually be removed.

Tomcat no longer needs to be restarted when S3 repository settings are changed.

All activEcho server logging is now written to a date-stamped activEcho.log file which is rotated daily. This log file can be found inside the Tomcat logs folder.

A configuration flag has been added to allow the activEcho web server to support HTTP connections instead of HTTPS. To allow HTTP connections, set REQUIRE_SSL to false in activEcho.cfg.

The Windows client MSI file is now available in the clients download directory.

ActivEcho's web application is now installed in the following location:

C:¥Program Files (x86)¥Group Logic¥activEcho Server¥activEcho Web Application

ActivEcho's Tomcat server is now installed in the following location:

C:¥Program Files (x86)¥Group Logic¥Common¥apache-tomcat-7.0.34

ActivEcho's Tomcat is now configured to redirect HTTP to HTTPS by default.

Customers not needing redirection refer to the online documentation:

https://docs.grouplogic.com/display/ActivEcho/activEcho+Server#activEchoServer-RedirectingHTTPrequeststoHTTPS

The list of shares has now been removed from the left panel of the projects web page to improve the page performance.

Filtering options have been added to projects page sidebar.

Improved shutdown speed of the Mac and Windows sync clients.

Upgraded default Tomcat installation to version 7.0.34 and Tomcat Native (tcnative-1.dll) to version 1.1.24.

Upgraded default version of PostgreSQL to 9.2.1.

Validation of support for Windows 2012 Server.

Validation of support for Java 7 update 15.

Validation of support for Windows 8 for the Windows sync client.

Users on IE7 will now explicitly receive an error message that IE7 is not supported.

BUG FIXES:

Fixed a couple of rare instances where the sync client could receive a database

error and could no longer sync.

Under load, client will no longer occasionally corrupt files on download and upload the corrupted versions.

Duplicate files will no longer appear in the web interface if you pause and resume the client in the middle of uploading a file.

Fixed a Mac client bug where the client receives an error when a file is deleted off the server side while the client is downloading the file.

The sync client will no longer fail to complete in rare cases where folders are aggressively renamed with similar names.

The sync client will no longer attempt to delete files repeatedly if it cannot succeed.

Tomcat settings have been changed to ensure that syncing requests from the client will succeed even when there are many top-level folders.

File and folders with names containing %, _, and ! will now be handled properly.

Multiple bug fixes to sync client context menu options to support a variety of file and folder names which previously would fail.

LDAP authentication by email will now work properly for LDAP domains where authentication by common name is not permitted.

Fixed various case-sensitivity bugs with LDAP authentication.

Adding trial server licenses will no longer occasionally fail.

Unsharing a folder with Unicode characters in the name using "Remove all" will no longer cause an error.

A pending user can now be removed from a shared folder if you have the appropriate permissions, even if you are not an administrator.

Users can no longer share deleted folders.

Improved error handling for SMTP errors.

Miscellaneous other bug fixes.

activEcho 2.6.1 (Released: October 2012)

BUG FIXES:

Reassigning content from deleted users now works when quotas are disabled.

activEcho 2.6.0 (Released: October 2012)

ENHANCEMENTS:

Log and Users tabs support pagination, sorting, filtering.

Log and Users tabs have been optimized for increased performance and smoother user interaction.

Log tab provides new start and end date display filters.

Quotas can be defined for individual Active Directory and Ad-hoc users, overriding group policies.

Quotas can now be defined specifically for administrative users.

Automatic purging of user accounts if no activity has occurred, or a specific absolute time has passed.

Support for configuring the length of time before expiration of shared links.

New share permissions allow owner to hide display of share members to non-owners, and prevent non-owners from inviting others.

New behavior when unsharing projects, local data will be deleted from the client on next connection.

New administrative setting to hide the "Download the activEcho client" link to control which users can download and install the activEcho sync client.

Users accounts can be disabled to temporarily prevent access and login to activEcho.

New administrative setting to control the minimum supported version number of the sync client.

Support provided for creating Tomcat server clusters running activEcho for load balancing and resilience.

Improved diagnostic logging provided in the file repository service.

Desktop Sync clients on Mac and Windows now provide a menu option to display recently updated files.

Clicking an entry in the list opens the folder containing the file.

Mac OS X sync client now supports Gatekeeper signing and notification center on OS X 10.8.

Recommend upgrading to the latest version of the client due to significant performance and stability improvements in both Windows and Mac desktop clients.

The sync client on Mac and Windows now sets a custom icon for the activEcho sync folder.

The server installer allows setting the user account the file repository service runs under to store the repository on network volumes.

Projects tab can now be filtered by items shared by a user, or shared with a user.

Change the default email template when inviting a user to a share to allow the user to select to start syncing the content immediately. If you have customized the invite to share template in the past, update the following items:

<%= show_contents_node_path(@node.uuid) %>

to

<%= show_contents_node_path(@node.uuid, {:show_sync_lightbox => true}) %>

Validation of support for Java 7 update 7.

BUG FIXES:

Various improvements to LDAP authentication, including case sensitivity issues with domain names and support for multiple email domains.

The domain for LDAP authentication list can use either ; or , as a delimiter.

Various improvements on syncing files and folders where an item or the parent folder(s) have been deleted.

Fixed files modification dates that were not set properly based on timezones under some circumstances.

Period is a valid character in S3 bucket names when using Amazon S3 for the file repository.

Fixed high CPU usage on both Mac and Windows desktop clients.

Miscellaneous other bug fixes.

activEcho 2.5.1 (Released: July 2012)

ENHANCEMENTS:

Support for mobilEcho 4.0 for access to activEcho using mobile devices. mobilEcho 4.0 now allows sharing of activEcho, file shares, and SharePoint servers simultaneously.

Additional license is required for accessing file shares and SharePoint with mobilEcho.

Uploading and downloading of files via mobile devices is faster.

Mobile devices can now copy files and folders within an activEcho share.

Support for Mac OS X 10.8 "Mountain Lion"

BUG FIXES:

Improved upgrade experience when automatically restarting Tomcat when there is a large amount of user data to be migrated.

Server installer now correctly upgrades activEcho when files were originally installed in a custom location.

Mobile devices can now navigate shares that have trailing spaces in their name.

Authentication of LDAP users only worked against the first entry in the Provisioned LDAP table.

Improved support for syncing files from Mac OS X with / in their filenames.

Improvements to the sync clients reduce the potential for a full re-sync being required.

Fixed issue when saving with some applications (Microsoft Publisher, TextEdit, etc.) on Windows and Mac OS X could result in a file being treated as a new file and disassociated from its revision history.

Miscellaneous other bug fixes

activEcho 2.5.0 (Released: July 2012)

The activEcho 2.5 client is not compatible with the 2.1 server. Please upgrade your server to 2.5 first, and then upgrade the clients.

The activEcho 2.1 client is compatible with the 2.5 server but will not have all of the new features available.

ENHANCEMENTS:

Support for quotas. Different quotas values can be set for Active Directory vs. ad-hoc users, as well as based on Active Directory group membership. End users can manage their quota usage by using the web to selectively purge old revisions and deleted files. See the user manual for more information.

Support for read-only ("download only") shares. This setting can be enabled when inviting members to a share, and from the Members page for the share.

Support for selective syncing. Via the web, users can pick which folders they want to have synced to their desktop vs. only accessible via the web. This allows users to have access to shared content but not necessarily have all content synced to their local desktop.

Administrators can now reassign ownership of content when deleting a user from activEcho, or can choose to delete a user and later reassign the content using the Manage Deleted Users page.

When a user's permission to share is removed from a shared folder, the folder is now removed from their client activEcho sync folder.

activEcho clients support pausing / resuming syncing.

Syncing files to Mac OS X clients is significantly faster.

The file repository can now be configured to store content on a UNC path to support network drives.

New Notification setting allows the administrator to be notified when the file repository free space goes below a set threshold.

Default email templates can now be viewed in the management settings.

Web Projects page now provides a summary of the number of files and folders.

Web Users page provides the administrator a summary of individual user's content and quota usage.

Sync clients no longer time out if the initial sync contains more than 50,000 files.

Windows client installer is now available as a MSI package for use in automate deployment.

Deleting many files at once from the web browser is much faster.

Web now provides an "Invite" button for the folder the user is viewing.

Web log view now has a reset filters button.

Master encryption key has been migrated from the Tomcat directory into the activEcho database to prevent accidental data loss if Tomcat is uninstalled without proper backups.

BUG FIXES:

Email template notification errors could occur after a user is deleted from activEcho if they were sharing content.

LDAP settings are no longer validated if LDAP has been disabled in the management settings.

When a folder is unshared, the owner can now see past events in the web log for that folder.

The web log allows filtering of past events for users who are no longer part of the shared folder.

Improved the Windows desktop sync client upgrade experience to not occasionally request that Explorer be restarted.

Email addresses containing the following characters are now valid when inviting or adding a user: ! $ & * - = ^ ` | ~ # % ' + / ? _ { }.

Tomcat web.xml configuration file can no longer be retrieved via a web browser.

Miscellaneous bug fixing in desktop syncing.

activEcho 2.1.1 (Released: June 2012)

ENHANCEMENTS:

Email addresses for LDAP authenticated users now update when the primary email address changes in LDAP.

Improved LDAP performance.

BUG FIXES:

Improved authentication against LDAP to avoid timeouts against large catalogs.

activEcho 2.1.0 (Released: May 2012)

ENHANCEMENTS:

Automatic purging of previous revisions and deleted files based on administrative rules.

Customizeable email templates.

Export log to TXT, CSV, or XML files.

Improved, administrator configurable trace logging for diagnostics.

Significantly improved performance when sharing and syncing a large number of files.

Ability to unsubscribe from shared folders as a user, or for the owner to unshare to all users.

Notifications are now available for folder changes in addition to files.

More than one email address can be provided for notifications.

Support for 64-bit Java installations.

Improved LDAP performance.

Miscellaneous usability enhancements.

BUG FIXES:

Various bug fixes related to authentication with Active Directory via email addresses.

The built-in Administrator account will now never use Active Directory for authentication.

Miscellaneous bug fixes in desktop syncing.

activEcho 2.0.2 (Released: March 2012)

BUG FIXES:

Improvements to desktop syncing when Microsoft Office files are edited directly in the activEcho Folder.

Various bug fixes in desktop syncing.

Bug fixes in activEcho server installer to fix future upgrades.

activEcho 2.0.1 (Released: March 2012)

BUG FIXES:

Improvements to the server administration user experience.

Various bug fixes in desktop syncing.

Improvements to the client installer upgrade process.

activEcho 2.0.0 (Released: February 2012)

Initial release

15.2.2 mobilEcho

mobilEcho 4.5.2 (Released: October 2013)

ENHANCEMENTS:

Added support for smart card authentication, and added a setting to allow or disallow clients using this new authentication method.

mobilEcho 4.5.1 (Released: September 2013)

ENHANCEMENTS:

The mobilEcho server now supports requiring that mobilEcho Android clients are managed by MobileIron AppConnect.

BUG FIXES:

Fixed an issue where clients could time out trying to connect to a server if mobilEcho was configured to enumerate site collections.

Fixed an issue where the mobilEcho server selected when configuring a custom home directory path could fail to save properly when saving a user or group profile.

mobilEcho 4.5 (Released: August 2013)

ENHANCEMENTS:

Added support for giving access to SharePoint Online for Office 365.

Added the ability to enumerate and browse into individual SharePoint site collections.

Added support for client certificate authentication to mobilEcho file servers.

Added profile options to enable or disable the client's ability to edit text and/or Office files, to configure an auto-sync interval, and to automatically sync a user's home folder.

Increased the maximum volume name length to 127 UTF-8 characters to allow for longer volume names when using Unicode characters.

Added separate columns to the exported .csv devices list for display name and common name to make the usernames more clear.

BUG FIXES:

Fixed an issue where the exported .csv devices list would display the domain name incorrectly if the domain name contained numerical characters.

Fixed an issue where the server would respond incorrectly to a client request to delete a folder that was the root of an SMB share.

Fixed an issue where network path mapping could fail if two path mappings were created for two similar paths (e.g. ¥¥server¥vol and ¥¥server¥vol2).

mobilEcho 4.3.2 (Released: April 2013)

BUG FIXES:

Fixed an issue where mobilEcho Administrator could fail to create an activEcho volume when the product is licensed with a Retail serial number.

Fixed an issue where a mobilEcho client could fail to open its home directory if the home directory is configured using the %USERNAME% wildcard and the server domain and the user's domain have a trust relationship.

Fixed an issue where the server could incorrectly send an error message to Android clients when those clients attempted to obtain their profile.

mobilEcho 4.3.1 (Released: April 2013)

ENHANCEMENTS:

The mobilEcho server now supports mobilEcho clients that identify themselves using a custom device identifier, rather than Apple's device identifier.

BUG FIXES:

Fixed an issue where the Users and Groups pages of the mobilEcho Client Management web console could load very slowly if there were a large number of configured profiles.

Fixed an issue where the enrollment link in client enrollment invitation emails could fail to open properly on Android clients.

Fixed an issue where iOS clients could fail to connect to the server after upgrading from 4.0.1 server or earlier to 4.3 server.

mobilEcho 4.3 (Released: March 2013)

ENHANCEMENTS:

The mobilEcho server now supports mobilEcho clients with optional support for MobileIron AppConnect activated. The server now allows administrators to require or restrict mobilEcho access to iOS clients with AppConnect enabled. This setting is located in the "Settings" window of the "mobilEcho Administrator" application, on the "Security" tab.

BUG FIXES:

Fixed an issue where clients upgrading from mobilEcho Server 4.0.x or earlier could incorrectly receive a "specified account does not have a management profile" error when attempting to retrieve their management profile.

Fixed an issue where the mobilEcho server's memory usage could increase if the "mobilEcho Administrator" was left open for a long period of time.

Fixed an issue where the client would fail to show an error or would show an incorrect error message if the user's AD account password had expired, or the account was locked out or disabled.

Fixed an issue where the server upgrade process could fail if mobilEcho had been installed to a non-system drive.

Fixed an issue where a JavaScript error would occur each time a user or group profile was added via the mobilEcho Client Management web console when using IE8.

mobilEcho 4.2 (Released: February 2013)

ENHANCEMENTS:

mobilEcho 4.2 servers now support mobilEcho 4.2 clients localized in German, French and Japanese. The 4.2 server will ensure that these clients receive server error messages in their local language. In addition, the mobilecho_manager_intl.cfg file contains settings to configure the client enrollment invitation email subjects in these three languages.

The mobilEcho Client Management service will now automatically detect crashes in the client management web application and stop the service so that administrators can properly detect these errors. Additional error information will be written to the ManagementUI¥log folder.

BUG FIXES:

Fixed a problem where the user could repeatedly be asked to enter proxy credentials when accessing the mobilEcho server through an HTTPS reverse proxy server.

Fixed a problem where the mobilEcho Client Management Server web UI could fail to restart because the client management database schema was not updated properly on upgrade. This would occur if the database was configured to be stored on a disk that was not available at upgrade time.

Sorting devices by "Last Contact" now sorts newest to oldest by default.

Fixed a problem where whitelists and blacklists could not be assigned when adding or editing a user or group profile.

Fixed a problem where files that were already on the device could sync again unnecessarily if the sync source was within an activEcho volume.

The password field on the login page of the client management web UI now has auto-complete disabled.

Removing a user or group profile now causes the name information for that user/group to be removed from cache. This ensures that re-adding a profile for that

user/group will always force the management UI to retrieve the latest name from Active Directory.

Fixed a problem where "set the default file action" and "cache recently accessed files on this device" could be enabled in profiles after upgrading mobilEcho server.

Fixed a problem where the app password reset functionality in the management server UI might not work properly in Firefox.

Fixed a problem on the Invitations page of the client management server web UI where users within distribution subgroups could fail to be found in LDAP searches.

Fixed a problem where the server check for free disk space in a folder would incorrectly check the free space at the root of the mobilEcho volume.

Fixed a problem where open file handles would not be closed for 24 hours if a client disconnected in the middle of a file transfer. These handles will now be closed when the session times out, after 15 minutes.

Fixed a problem where the "Allow iTunes and iCloud to back up locally stored mobilEcho files" profile setting would always revert to enabled after saving management profile.

mobilEcho 4.1 (Released: December 2012)

ENHANCEMENTS:

Added an alternative client management server authentication mechanism so that mobilEcho clients that are configured to not save credentials for assigned servers and folders can authenticate to the management server to retrieve their profile without requiring their Active Directory password be stored on the device.

Modified the app password reset process. This was necessary to support the new custom on-device encryption that is included in the mobilEcho 4.1 client app. If a managed client forgets their app password, they now provide their administrator with a code generated by the app. The administrator enters this code into the mobilEcho Client Management web console and receives a second code that they

give back to the client. This code allows the user to reset their app password and get into the app.

Enhanced the way resources (servers and folders) are provisioned to clients. Provisioned resources are no longer assigned directly to user/group profiles. Users or groups are now assigned directly to individual assigned resources and each user receives the full collection of resources assigned to their user account or a group they are a member of.

Added the ability to send up to three enrollment invitations to the same email address automatically for users with multiple devices.

Added a column to the LDAP search table for Distinguished Name so that users with the same name in different subdomains can be distinguished.

Added new management profile setting to allow or disallow users from opening and/or sending links to files.

Added client Good Dynamics status in the management server Devices list. Devices enrolled with Good Dynamics will no longer have the "Reset App Password" option available. The app password is managed within the Good Control console in this scenario.

BUG FIXES:

Fixed a problem where hiding inaccessible files on reshares when one of the volumes was a SharePoint volume could cause some of the volumes to fail to appear on the client.

Fixed a problem where the Client Management Administrator could fail to filter the devices or invitations tables, or could take a very long time to complete the filter. Filtering is now done without the need to perform additional LDAP requests.

Fixed a problem where attempting to read a file on an activEcho volume that no longer exists would result in a corrupted file being read rather than an error being returned.

Fixed a problem where the presence of a misconfigured or unavailable activEcho volume could cause clients to time out when attempting to retrieve the volume list.

Fixed a misleading message in the Client Management Administrator if a profile was configured to have 'App password must contain complex characters' greater than the 'Minimum password length'.

Fixed a problem when the client management server was configured to use a non-default port (i.e. not port 3000) and the server was upgraded. The first time the management server would run after upgrade it would attempt to use port 3000 rather than the configured port.

Modified the message in the Client Management Administrator when removing a currently managed client from the devices list to indicate that the client may automatically reenroll at a later time if enrollment PINs are not being used.

Fixed a problem where the Client Management Administrator could display an error if a profile was configured to use a home folder with an empty custom path.

Fixed a problem where 0-byte files would fail to download or sync with a "device not ready" error.

Content search is now automatically disabled on activEcho and SharePoint volumes since content search is not available.

Fixed a problem where users with email address beginning with underscore (e.g. "_user@example.com") could fail to receive enrollment invitations.

Client Management Administrator now returns a better error message than "unknown result" if the LDAP server requires SSL.

Fixed a problem where sessions could time out while downloading very large files.

Fixed a problem where configuring an assigned folder with an invalid path (e.g. "C:¥foo¥bar") could cause the Users page to show the error "can't modify frozen string".

Fixed a problem where selecting the "Reindex all volumes" button in the mobilEcho Administrator would generate an invalid error message.

Fixed a problem where filtering on a Unicode string in the Client Management Administrator could generate an "incompatible character encodings" error.

SharePoint "Wiki Page Gallery" libraries are now removed from site enumerations because they are not supported by mobilEcho.

Fixed a problem where new profile settings could become corrupted on upgrade.

Fixed a problem where a SharePoint document library volume would fail to work if the document library name was URL encoded, e.g. "My%20Library".

mobilEcho 4.0.3 (Release: October 2012)

ENHANCEMENTS:

Added support for SharePoint custom document libraries.

BUG FIXES:

Fixed a problem accessing SharePoint sites and document libraries whose paths are multiple levels below their parent site.

Fixed a problem accessing SharePoint sites that use Claims Based Authentication.

mobilEcho 4.0.2 (Released: September 2012)

ENHANCEMENTS:

Added support for Android clients.

Added settings to the mobilEcho Administrator for restricting access by iOS and/or Android clients.

Added support for sending enrollment instructions for iOS, Android and Good clients.

BUG FIXES:

Fixed a problem where exporting the devices list to a .csv file could result in a server error, or could result in some fields displaying as "Not found in AD".

Fixed a problem where non-Good clients could enroll with a management server that was configured to require clients be enrolled with Good Dynamics. Previously, clients could enroll, but would receive an error when contacting the server to access data. Clients are now disallowed from enrolling in the first place.

mobilEcho 4.0.1 (Released: August 2012)

ENHANCEMENTS:

Added profile settings for "Number of days to warn of pending lock" and "Number of days to warn of pending wipe". These settings relate to existing settings that can wipe or lock the mobilEcho app if the device does not contact the management server for a specified period of time.

Added pagination, filtering and sorting to the Users and Groups pages within the mobilEcho Client Management server.

BUG FIXES:

Fixed a crash that could occur when attempting to authenticate with SharePoint volumes using Kerberos authentication.

Fixed a problem where users could fail to authenticate with SharePoint volumes if their user principal name (UPN) had a different domain than their Windows 2000 domain.

Fixed a problem where users could fail to authenticate with SharePoint volumes if their username contained Unicode characters and authentication was performed using NTLM.

Fixed a problem where users could fail to authenticate with SharePoint volumes if the user was a member of a subdomain and authentication was performed using NTLM.

SharePoint document libraries will now display all items, regardless of the settings of the library's default view.

The "Last Contact Time" column on the Devices page of the mobilEcho Client Management server now properly sorts by date.

Filters in the mobilEcho Client Management server now work properly with Unicode characters.

Filters in the mobilEcho Client Management server now "stick" after pagination settings are changed.

Disabled the "Indexed Search" and "Content Search" checkboxes when adding or editing reshare volumes in the mobilEcho Administrator, since search is not supported on those volumes.

The mobilEcho Administrator now automatically fills in the existing path when editing a SharePoint, activEcho or reshare volume path.

The mobilEcho server now returns a better error code if the user attempts to overwrite a file via Save Back that is checked out to another user.

mobilEcho 4.0 (Released: July 2012)

ENHANCEMENTS:

Added support for accessing data in SharePoint 2007 and 2010 document libraries.

The mobilEcho server can now simultaneously support activEcho and other volume types. Previous versions required switching into activEcho-only mode to access activEcho data.

Improved performance of the mobilEcho Client Management server by making LDAP queries "begins with" rather than "contains" by default. Administrators may choose "contains" when searching to obtain the previous behavior.

The mobilEcho Client Management server can now filter the invitations tables by username.

The mobilEcho Client Management server can now export the devices list to a .csv file.

The mobilEcho Client Management server now sorts and paginates the devices, users, groups and invitations tables.

Added a profile setting to allow/disallow users from creating bookmarks.

Added a profile setting to disable My Files while still allowing sync folders.

Added a profile setting to automatically lock the mobilEcho app or wipe all mobilEcho data if the device does not contact the management server for a specified period of time.

Added a profile setting to prevent users from setting an app password.

Files can now be copied within activEcho volumes by transferring data through the client.

Improved performance reading and writing to activEcho volumes.

BUG FIXES:

Fixed a problem where files and folders ending in a period or space could fail to be accessible on activEcho volumes.

Fixed a problem where the Devices page could fail to load in mobilEcho Client Management server after Japanese and Chinese users have enrolled.

mobilEcho 3.7 (Released: June 2012)

ENHANCEMENTS:

Improved performance of the mobilEcho Client Management server by caching user information to minimize the number of LDAP queries.

BUG FIXES:

Active Directory distribution groups are no longer found when searching for groups on the group profile page.

Fixed a problem when the path of a provisioned folder ends with a backslash.

mobilEcho 3.6.1 (Released: May 2012)

BUG FIXES:

Fixed a problem where files on an activEcho server could fail to preview, copy or sync.

Fixed a problem where users could fail to preview, copy or sync files in a home directory if the home directory was set up with a network reshare path mapping in the mobilEcho Client Management server.

Fixed a problem where users could fail to see their home directories if the client authenticated to the management server with a user principal name (UPN) such as user@domain.com.

Fixed a problem where the "%USERNAME%" wildcard would fail to use the correct username if the client authenticated to the management server with a user principal name (UPN) such as user@domain.com.

mobilEcho 3.6 (Released: April 2012)

ENHANCEMENTS:

Improved performance of Active Directory lookups for users and groups.

Searches of Active Directory in the mobilEcho Client Management server now search on both common names and display names.

Add profile settings for allowing/denying the ability of users to create sync folders, and to perform a Quickoffice® "Save Back".

The mobilEcho Client Management server can now be configured to store database and profile information in a different location than the application directory, allowing for the management server service to be failed over to other cluster nodes.

The mobilEcho Administrator now displays the number of licenses currently being occupied, and will only display a single session for each user/device if the user has reconnected to the mobilEcho server multiple times.

The mobilEcho Administrator now automatically runs with elevated privileges.

The enrollment email subject can now be customized in the 'mobilEcho_management.cfg' file.

BUG FIXES:

mobilEcho no longer permits Active Directory "Distribution" groups to be used to create mobilEcho Client Management group policies. Distribution groups are provided by Microsoft for email purposes only. If you are using AD "Distribution" groups for any of your mobilEcho Client Management policies, please use the "Active Directory Users and Computers" control panel to convert these groups to "Security" groups.

Fixed a problem where a user that used different username formats to enroll with multiple devices would occupy multiple licenses. For example, if one device was enrolled as "user@example.com" and a second device was enrolled as "example¥user", the licensing logic would treat those as two separate user accounts for licensing purposes.

Fixed a problem where a user could fail to get the appropriate group profile if the user's Active Directory primary group was not set to the default of "Domain Users".

Fixed a problem where a user could fail to get the appropriate group profile if the user's group was a "universal" Active Directory group.

Fixed a problem where users with Unicode characters in their usernames would not have their credentials saved after enrolling with mobilEcho Client Management.

Fixed a problem where the server could allow mobilEcho clients to overwrite files that were flagged as read-only.

Fixed some mobilEcho Client Management display issues on Mac Safari.

Fixed a problem where Verizon iPad 3 devices were displayed as "AT&T" (and vice versa) in the mobilEcho Client Management devices page.

Fixed a problem where the mobilEcho Administrator could crash when viewing the list of connected users.

Fixed a problem where the invitation email would fail to show the username.

mobilEcho 3.5 (Released: February 2012)

ENHANCEMENTS:

Added support for 2-way sync folders. Client-side changes made in 2-way sync enabled folders will be synced back to the server automatically. These 2-way sync folders can be provisioned through the mobilEcho Client Management server.

Added support for reverse proxy authentication. Reverse proxy servers, such as Microsoft Forefront Threat Management Gateway (TMG), can be configured to require authentication before granting access to internal network resources. The mobilEcho client now supports both HTTP username/password and SSL Client Certificate authentication methods. To use SSL Client Certificate authentication, a certificate must be installed in the mobilEcho keychain. See this Knowledge Base article for more information: http://support.grouplogic.com/?p=3830

Added additional options for configuring mobilEcho device enrollment requirements. mobilEcho can now be optionally configured to accept enrollment requests from devices without the need for a one-time PIN. In addition, when mobilEcho is configured to require such PINs, these PINs can be viewed within the management interface.

Added support for client app whitelisting and blacklisting. A managed mobilEcho client can be configured so that files can only be opened into a restricted whitelist or blacklist of third-party iOS apps.

Improved browsing performance of network reshare volumes by disabling the filtering of inaccessible file and folders by default on such volumes.

Added support for network reshare to SMB/CIFS volumes on NetApp storage.

Added the ability to configure mobilEcho provisioned folder paths that include a username wildcard.

Added the ability to configure mobilEcho home folders with custom paths. These paths may include a username wildcard.

mobilEcho no longer requires that users have "list folder" permissions at the root of a share containing their home folder.

Added a new registry setting to control whether or not hidden shares on a network reshare are visible to mobilEcho clients. To enable this feature, set the following registry setting to 1:

HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥services¥mobilEcho¥Parameters4¥Refreshable¥Pez¥GetShowHiddenSMBShares

BUG FIXES:

Fixed a problem where the mobilEcho Client Management server would appear to allow access without a proper username and password.

Fixed a problem where files would incorrectly require a sync after a change in daylight savings time.

Fixed a problem where renamed files would continue to be returned in search results when searching under the old filename. This problem would only occur for volume that were configured to use "indexed search" (not Windows Search).

Fixed a problem where mobilEcho could fail to install or run on systems missing a system DLL (normaliz.dll).

Fixed a problem where the client could fail to copy a file to the server if the user account did not have permission to calculate the amount of free space on the volume. The client would report an error about there not being enough free space on the volume.

Removed extraneous logging from the mobilEcho LOG.TXT file.

Fixed a problem where folders could not be provisioned for servers whose display name contained parentheses.

mobilEcho 3.1 (Released: November 2011)

ENHANCEMENTS:

Client management profiles can now be configured with the following new settings:

- The number of incorrect app password attempts that can be made before the local data

within the mobilEcho app is automatically wiped. This feature is disabled by default.

- Whether the user is required to confirm before syncing occurs (options are:

"Always", "Never", and "Only on 3G").

- Whether syncing is allowed any time, or only while on WiFi networks.

- Client timeout for unresponsive servers now accepts additional values of 90, 120 and 180 seconds.

The mobilEcho Client Management server can now be configured to communicate with Active Directory via secure LDAP.

Profiles now default to allow files to be cached on the local device. If caching is disabled or if the "Allow files to be stored on this device" setting is disabled, no files will be cached.

The text of enrollment invitation emails can be customized. Please visit the GroupLogic Knowledge Base for more information: http://support.grouplogic.com/?p=3749

Added a setting to the management configuration file to control the name that enrollment invitation emails appear from (e.g. "mobilEcho Invitation <mobilEcho_invitation@example.com>". Version 3.0 only allowed an address to be specified (e.g. "mobilEcho_invitation@example.com").

The VALID_LOGIN_NAMES field of the management configuration file now supports Active Directory groups in addition to specific users that can administer the mobilEcho Client Management service.

Changing SMTP settings within the management configuration file no longer requires a restart of the mobilEcho Client Management service.

Profiles for users and groups that no longer exist in Active Directory are now marked as such in the mobilEcho Client Management service.

Added the ability to show inaccessible items only on reshare volumes. This can be useful in cases where determining file and folder accessibility is causing performance problems. This behavior can be adjusted by modifying the following registry setting and restarting the service:

HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥services¥mobilEcho¥Parameters4¥Refreshable¥Pez¥HideInaccessibleItemsOnReshares

BUG FIXES:

Fixed a problem where the mobilEcho Client Management server would not properly calculate an Active Directory home directory path if the associated 'Network reshare path mapping' included a trailing backslash.

Fixed a problem where the mobilEcho Client Management server would not properly calculate an Active Directory home directory path that only included a server and share name. (i.e. ¥¥servername¥sharename)

Fixed a problem that could prevent network reshare volumes configured with paths to the root of a server (i.e. ¥¥servername) from appearing properly in the mobilEcho client.

mobilEcho clients now always log into provisioned servers using fully qualified domain accounts. In previous versions of mobilEcho, the credentials entered at enrollment time would be used to authenticate with file servers, even if these credentials did not include a domain name (e.g. domain¥user). This could cause problems if the provisioned server was on a different domain than the management server and access to the server in the secondary domain relied on a domain trust with the primary domain. This behavior can be reverted to the previous default by setting the following registry value to 0 and restarting the service:

HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥services¥mobilEcho¥Parameters4¥Refreshable¥Pez¥DomainAndUsernameShouldBeSentToClient

Fixed a problem where the mobilEcho Client Management server did not properly sort "Last contact date" properly on the Devices page.

Fixed a problem in the mobilEcho Administrator where the Help button would not adjust properly as the Users window was resized.

mobilEcho 3.0 (Released: October 2011)

ENHANCEMENTS:

Centrally managed device enrollment. Client enrollment invitations are now generated and emailed to the user from the mobilEcho Client Management Administrator. These invitations include a one-time use PIN number required for client enrollment.

Remote wipe and remote reset of app passwords is now performed on a per-device basis.

Individual device status is now displayed in the mobilEcho Client Management Administrator. This includes device user name, device name, device type, iOS version, mobilEcho version, mobilEcho status, last contact time.

Users' Active Directory assigned network home folders can now be automatically displayed in the mobilEcho client app.

Specific mobilEcho shared volumes or folders within shared volumes can now be assigned to user or group profiles. These shared volumes or folders are then automatically displayed in the mobilEcho client app.

Shared volumes or folders assigned to user or group profiles can be configured to automatically one-way sync from server to mobilEcho client, making the contained files available for online or offline use.

BUG FIXES:

Fixed a problem where the mobilEcho server would not properly report free space for server-to-server copies.

Improved error messages and processing if a user attempts to copy or move files into the root of a network reshare.

Fixed a problem where a user could be authenticated with AD by contacting mobilEcho via a web browser. This could cause a user account to become locked.

Improved the speed of installation, particularly for upgrades.

Fixed a problem where files and folders ending a period or space could fail to copy properly.

Fixed a problem logging into the management UI with a username containing numbers, e.g. "e12345".

Updated OpenSSL library to latest version. OpenSSL libraries are used for encryption.

mobilEcho 2.1.1 (Released: July 2011)

BUG FIXES:

Fixed a bug when listing the contents of folders which may have resulted in slow performance or client timeouts if many of the folders were not accessible to the client.

mobilEcho 2.1.0 (Released: July 2011)

ENHANCEMENTS:

Added the ability to create mobilEcho shares that reshare data on a remote system. The mobilEcho reshare feature is only available for customers with an enterprise license. Reshares can be a particular share (e.g. "¥¥server¥share") or an entire server ("¥¥server¥").

The mobilEcho client can now perform copy and move operations on folders when connected to a server running mobilEcho Server 2.1 or later, and the management UI now has settings to allow or disallows these operations.

The management UI now has the ability to add a new group or user using settings from an existing user or group.

Management profiles can now be disabled so that the corresponding user or group cannot receive their profile.

Added the ability to prevent clients from connecting to servers with self-signed certificates.

Added a management setting to enable or disable copying text from a previewed document.

Added a management setting that tells the client to store files so that they are not backed up by iTunes.

mobilEcho 2.0.0 (Released: May 2011)

ENHANCEMENTS:

Added the ability to manage mobilEcho clients using server-defined profiles using mobilEcho Client Management.

Added the ability to reset mobilEcho app passwords from the server.

Added the ability to force a remote wipe for a particular mobilEcho user.

mobilEcho will now use an internal filename index for satisfying search requests if Windows Search is not installed or available.

The mobilEcho administrator now allows for volumes to be seamlessly replicated from SMB and/or ExtremeZ-IP shares.

mobilEcho 1.0.0 (Released: January 2011)

Initial release.

16 古いバージョン用のドキュメント

古いバージョンの Files Advanced ドキュメントについては、以下のリンクから確認してください。

注意: 古いバージョンのドキュメントはご希望の言語に対応していません。

- 8.1.x
- 8.0.x
- 7.5.x
- 7.4.x
- 7.3.x
- 7.2.x
- 7.1.x
- 7.0.x
  http://www.acronis.com/ja-jp/support/documentation/AcronisAccessAdvanced_7.0/index.html#26894.html
- 6.0.x
  http://www.acronis.com/ja-jp/support/documentation/AAS6.0/index.html#26894.html
- 5.0.x