GAuthLogon 設定データの同期

設定マニュアル

1. ドメイン環境 2
1.1 フォルダリダイレクト 2
1.1.1 リダイレクト先の設定が「全員のフォルダを同じ場所にリダイレクトする」ー「ルートパスの下に各ユーザのフォルダを作成する」の場合 3
1.1.2 リダイレクト先の設定が「全員のフォルダを同じ場所にリダイレクトする」ー「ルートパスの下に各ユーザのフォルダを作成する」以外の場合 4
1.1.2.1 クライアント PC のレジストリで AD ユーザの属性 userSharedFolderOther を参照するようにします。 4
1.1.2.2 ドメインユーザの userSharedFolderOther 属性にリダイレクト先のパスを指定します。 5
1.1.2.3 SetUserAttr.exe - ユーザ属性への値設定ツール 7
1.2 移動プロファイル 8
2. クラウドストレージを利用した設定共有/同期 9
2.1 設定方法 9
2.1.1 Rclone 設置 9
2.1.2 Rclone を使ったクラウドストレージの設定 10
2.1.3 GAuthLogon フォルダに Rclone.exe をコピー 12

概要

GAuthLogon をインストールした複数のコンピュータに同じ設定でログオンすることができます。いずれか 1 台で Autheniticator アプリを設定したら、設定データを共有/同期するどのコンピュータでも Autheniticator アプリが表示するコードでログインできます。いずれか 1 台のコンピュータで Authenticator の設定を更新すると、他のコンピュータには設定は同期/共有されます。

ドメイン環境でフォルダリダイレクト/移動プロファイルを設定してあれば、それを利用できます。クラウドストレージを利用する共有/同期は、どの環境でも有効化可能です。

1. ドメイン環境

ドメイン環境でフォルダリダイレクト、又は、移動プロファイルを設定してあれば、GAuthLogon 設定は異なるコンピュータで同期可能です。フォルダリダイレクトと Roaming Profile を同時に設定してある場合、フォルダリダイレクト設定が優先されます。

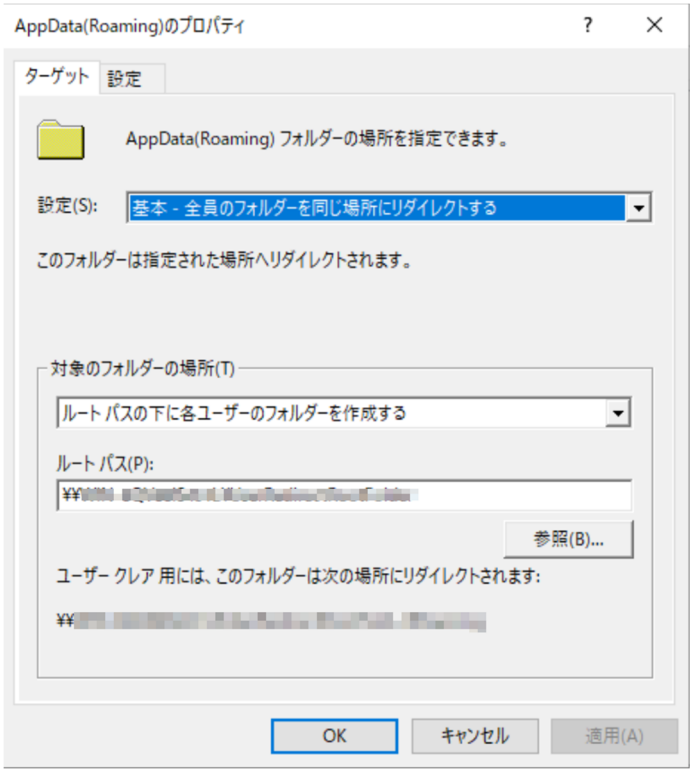
1.1 フォルダリダイレクト

GAuthLogon 設定は AppData(Roaming)に保存されます。AppData(Roaming)をフォルダリダイレクトすることで、ドメインユーザはどのコンピュータにも同一設定で GAuthLogon 経由ログインが可能になります。ここでは AppData(Roaming)のフォルダリダイレクトが動作しているものとして、GAuthLogon の設定方法を説明します。

ユーザがログインしていれば、AppData(Roaming)への読み書きは自動でサーバ上のリダイレクト先への操作になります。AddToken の設定データは自動でリダイレクト先のサーバに保存され、他のコンピュータにログインすると最新の設定データが読み込まれます。

しかし、GAuthLogon はユーザを認証するプログラムで、ユーザがログインしていない状態で動作しますユーザコンテキストで動作しません。そのためユーザの AppData(Roaming)フォルダがどこにリダイレクトされているのか知ることができません。なんらかの方法でフォルダのリダイレクト先を知らせなければなりません。

GAuthLogon にはレジストリと AD ユーザの属性でリダイレクト先を伝えます。



1.1.1 リダイレクト先の設定が「全員のフォルダを同じ場所にリダイレクトする」ー「ルートパスの下に各ユーザのフォルダを作成する」の場合

ルートパスを GAuthLogon に伝える設定をします。GAuthLogon はルートパスが分かれば、そのパスにユーザ名を追加してユーザのリダイレクトフォルダを生成できます。

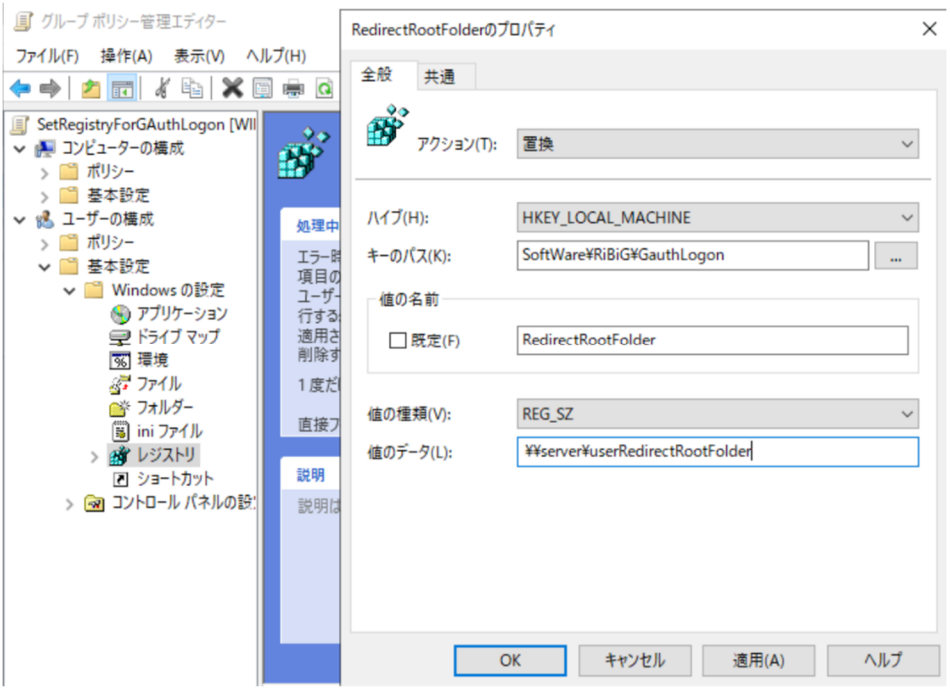
レジストリキー

HKEY_LOCAL_MACHINE¥SOFTWARE¥RiBiG¥GAuthLogon

値:

RedirectRootFolder　REG_SZ

RedirectRootFolder にルートパスを設定してください。



1.1.2 リダイレクト先の設定が「全員のフォルダを同じ場所にリダイレクトする」ー「ルートパスの下に各ユーザのフォルダを作成する」以外の場合

ユーザ毎に異なるリダイレクト先が設定される可能性があるため、ユーザ毎にリダイレクト先を伝えるようにします。

1.1.2.1 クライアント PC のレジストリで AD ユーザの属性 userSharedFolderOther を参照するようにします。

レジストリキー

HKEY_LOCAL_MACHINE¥SOFTWARE¥RiBiG¥GAuthLogon

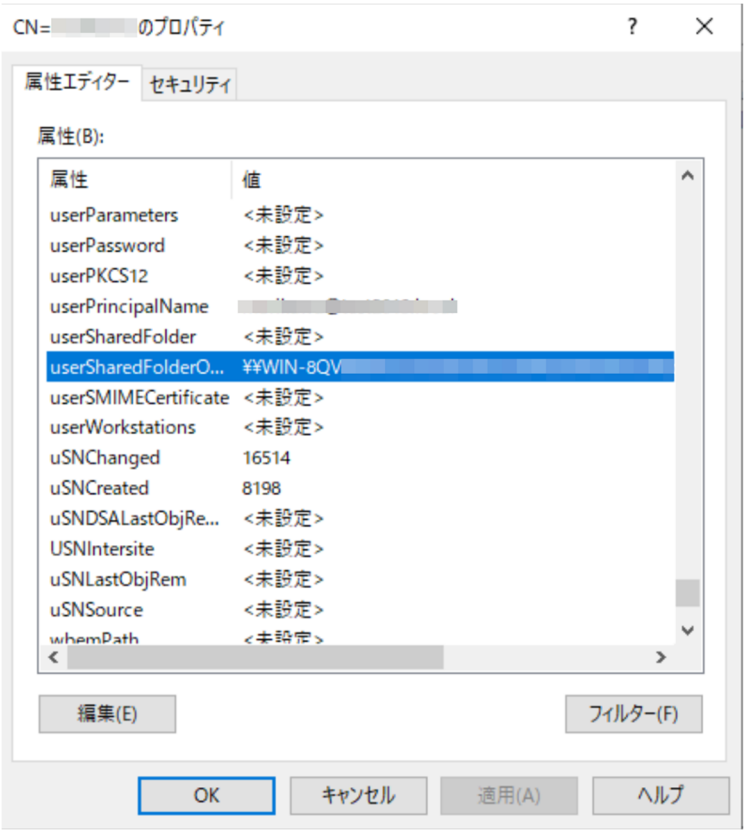
値:

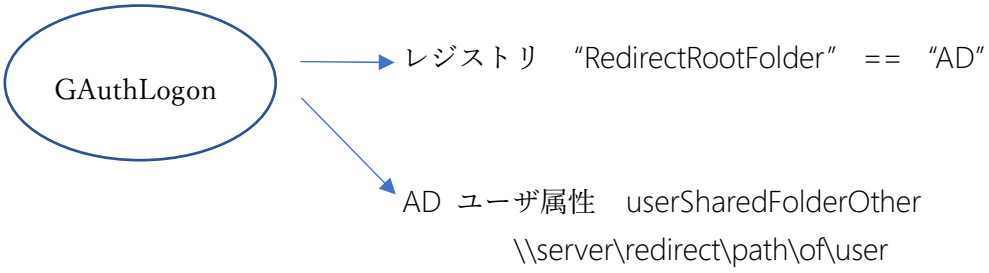
RedirectRootFolder　REG_SZ

RedirectRootFolder に “AD” と設定。既定では ユーザの userSharedFolderOther を見に行きます。

1.1.2.2 ドメインユーザの userSharedFolderOther 属性にリダイレクト先のパスを指定します。

ADSI エディターでユーザコンテナ（CN=Users)を選択して、ユーザを選択後、プロパティを表示. userSharedFolderOther にリダイレクト先パスを設定してください。





既に userSharedFolderOther 属性を他の目的で使っている場合、他の既存属性にリダイレクト先のパスを設定するか、新規属性をユーザクラスに追加してその属性にリダイレクト先パスを設定してください。

新規属性の追加方法

https://social.technet.microsoft.com/wiki/contents/articles/51121.active-directory-how-to-add-custom-attribute-to-schema.aspx

userSharedFolderOther 属性以外を使う場合：

レジストリ設定

レジストリキー

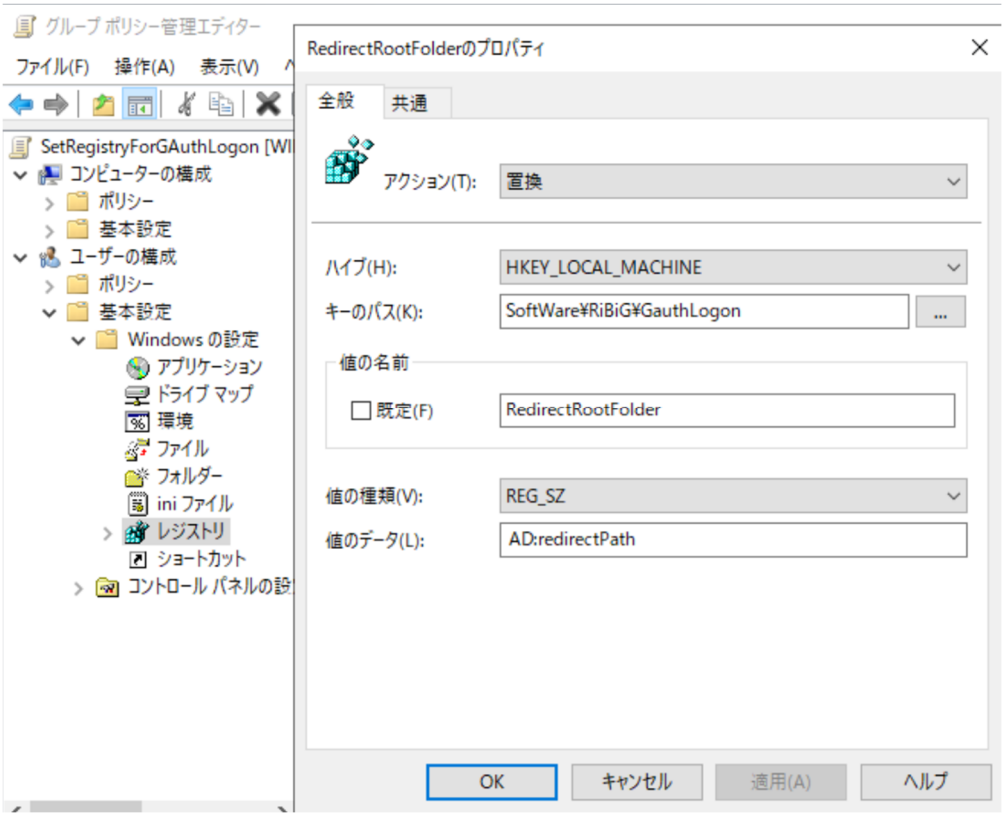
HKEY_LOCAL_MACHINE¥SOFTWARE¥RiBiG¥GAuthLogon

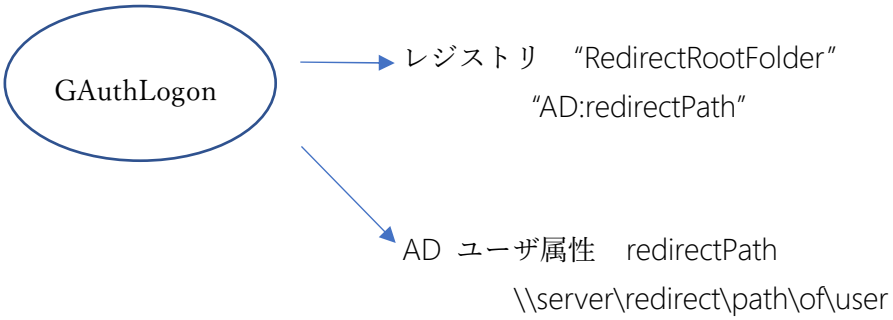
値:

RedirectRootFolder　REG_SZ

RedirectRootFolder に “AD:(属性名)” と設定。

例えば属性が RedirectPath であれば “AD:RedirectPath”





1.1.2.3 SetUserAttr.exe - ユーザ属性への値設定ツール

ADSI エディターを使って手動で AD ユーザ属性に値を設定する代わりに、このコマンドラインツールで設定することが可能です。このツールは実行するユーザの権限で AD にログインして属性値をセットします。必ず、AD ユーザ属性の読み書き権限をもったユーザでログインして本ツールを実行してください。AD をホストするコンピュータで実行する場合、管理者コマンドプロンプトで実行する必要があります。

コマンド引数

>setUserAttr -a (属性名) -u (ユーザ名) -f (ユーザのリダイレクトフォルダパス)

-a パスを設定する属性名。属性を指定しなければ既定の
userSharedFolderOther”に書き込みます。
-f ユーザのリダイレクト先パス

-u リダイレクトパスを設定するユーザ
又は
-g グローバルグループ
又は
-G ローカルグループ

例：

>setUserAttr -u user -f ¥¥server¥redirect¥user
>setUserAttr -a redirectPath -u user -f ¥¥server¥redirect¥%username%
>setUserAttr -a redirectPath -g “Folder Redirection Users” -f ¥¥server¥path

%username% が指定されていると GAuthLogon はログインドメインユー

ザ名に置き換えます。
属性値を削除するには -f を指定しないようにします。

>setUserAttr -a redirectPath -g “Folder Redirection Users”
*グループのユーザの redirectPath 属性値を未設定にする

細かなグループメンバーの選択操作は PowerShell で行い、PowerShell スクリプトで setUserAttr を呼び出してください。

1.2 移動プロファイル

移動プロファイルが設定されている環境では GAuthLogon の設定は不要です。 GAuthLogon はログイン処理でサーバ上のプロファイルパスを知ることができます。ただし、GAuthLogon が検出するパスは完全なものではありません。

移動プロファイルが保管されているサーバでは、Windows のバージョンにより移動プロファイルを保存するパスに異なるサフィックスが追加されます。GAuthLogon はサフィックスが付いていないパスを検出します。

Windows Client OS バージョン	Windows Server OS バージョン	サフィックス	プロファイフォルダ例
Windows NT 4.0 - Windows Vista	Windows NT Server 4.0 - Windows Server 2008	*none*	user
Windows 7	Windows Server 2008 R2	V2	user.V2
Windows 8.0 - 8.1*	Windows Server 2012 - 2012 R2*	V3	user.V3
Windows 8.1*	Windows Server 2012 R2*	V4	user.V4
Windows 10 (1507 to 1511)	Windows Server 2016	V5	user.V5
Windows 10 (1607 and later)		V6	user.V6

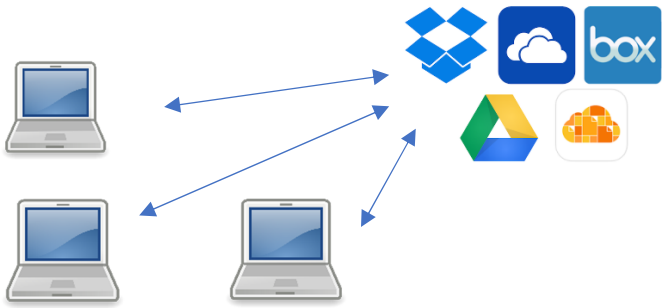
https://wiki.samba.org/index.php/Roaming_Windows_User_Profiles

GAuthLogon は、実行している OS に対応するサフィックスを検出したパスに追加する処理を行いません。代わりに、V6, V5 … V2 と順にサフィックスを追加してプロファイルフォルダを見に行き、GAuthLogon

設定が見つかったら読み取ります。動作している Windows のバージョンに一致するサーバ上のプロファイルフォルダを読み取るわけではありません。

2. クラウドストレージを利用した設定共有/同期

クラウトストレージを利用して GAuthLogon 設定を自動同期させることができます。ローカルアカウント、Microsofft アカウント、ドメインアカウント - いずれにも対応します。異なるアカウント間での共有も可能です。例えば、コンピュータ A のローカルユーザ A、コンピュータ B のローカルユーザ B、コンピュータ C の Microsofft アカウント C で同じ設定を共有できます。



このためには、コンピュータのローカルアカウント・ Microsoft アカウントをクラウトストレージのアカウントをリンクさせます。正しくリンク設定したアカウントでは、AddToken は設定データをクラウドストレージから読み込み見ます。また、ローカルに保存すると同時にリンクしたクラウドストレージにも保管します。正しくリンク設定したアカウントにログインするときには、GAuthLogon はユーザにリンクしているクラウドストレージから設定を読み込みます。

アカウント名が異なっていても、リンクしているクラウドストレージが同一であれば同じ設定が適用されます。ただし、異なるアカウント間で共有する場合、ini モードを “share”(共有)に設定しなければなりません。

2.1 設定方法

2.1.1 Rclone 設置

GAuthLogon はクラウドストレージへとのファイル転送に rclone を利用します。

https://rclone.org/ から OS に適合するバージョンをダウンロードしてください。ダウンロードした ZIP ファイル内のすべてのファイルを任意のフォルダにコピーすることで設置は完了します。

2.1.2 Rclone を使ったクラウドストレージの設定

ユーザアカウントにログインして Rclone を設置したフォルダでコマンドプロンプトを開き以下コマンドを実行してください。ユーザアカウントとクラウドストレージをリンクする処理が開始します。

>rclone config

e) Edit existing remote
n) New remote
d) Delete remote
r) Rename remote
c) Copy remote
s) Set configuration password
q) Quit config
e/n/d/r/c/s/q>n　(n を入力してリターン)　新規作成

name>gauth　　(gauth と入力してリターン)

クラウドストレージのリストが表示されるので、利用するクラウドストレージを選択。事前にアカウントがなければなりません。 ここでは例として OneDrive を選択。 23 と入力

Storage>23 [リターン]
client_id > [リターン]
client_secret>[リターン]

残りの項目はすべて既定値を選択(何も入力せずにリターン)

Edit advanced config? (y/n)
y) Yes
n) No (default)
y/n>[リターン]

Remote config
Use auto config?
 * Say Y if not sure

* Say N if you are working on a remote or headless machine
y) Yes (default)
n) No
y/n>[リターン]

ブラウザが起動して OneDrive のアカウント入力を求められるので、利用するアカントの資格情報を入力。成功したら以下のページが表示。ブラウザを閉じる

Success!

All done. Please go back to rclone.

Choose a number from below, or type in an existing value
1 / OneDrive Personal or Business
¥ "onedrive"
2 / Root Sharepoint site
¥ "sharepoint"
3 / Type in driveID
¥ "driveid"
4 / Type in SiteID
¥ "siteid"
5 / Search a Sharepoint site
¥ "search"
Your choice>1 [1 を選択してリターン]

Found 1 drives, please select the one you want to use:
0: OneDrive (x x x x x x) id= x x x x x x x x x x x
Chose drive to use:>0 (使うドライブを選択してリターン)

Found drive 'root' of type 'XXXX', URL: https://XXXXXXX
Is that okay?
y) Yes (default)

n) No
y/n>[リターン]

y) Yes this is OK (default)
e) Edit this remote
d) Delete this remote
y/e/d>[リターン]

e) Edit existing remote
n) New remote
d) Delete remote
r) Rename remote
c) Copy remote
s) Set configuration password
q) Quit config
e/n/d/r/c/s/q>q （ q で終了 ）

設定が完了したら、以下コマンドラインでクラウドストレージのファイルが表示されることを確認してください。

rclone lsd gauth:¥ （ ルートのディレクトリ表示 ）
rclone lsf gauth:¥ (ルートのファイル表示)
rclone ls gauth:¥ (ルート以下のすべてのファイル表示)

問題なくディレクトリやファイルが表示されたら、ログインしているアカウントでのクラウドストレージへのリンクが完了したことになります。

2.1.3 GAuthLogon フォルダに Rclone.exe をコピー

%ProgramFiles%¥RiBiG¥GAuthLogon フォルダに rclone.exe をコピーしてください。
GAuthLogon はこのフォルダにある rclone.exe のみを実行します。

これでクラウドストレージへのリンクをしたアカウントではクラウドストレージを介した共有・同期設定が完了します。このアカウントでログインして AddToken で設定すると、設定ファイル gauth.conf がクラウドストレージのルートに保存されます。また、このアカウントのログインするときにクラウドストレージの gauth.conf を読み込みます。

他のコンピュータのアカウントでクラウドストレージ上の同じ設定データを利用するには、そのアカウントで同じクラウドストレージのアカウントにリンク設定をしてください。アカウントでクラウドストレージとのリンク設定を行い、%ProgramFiles%¥RiBiG¥GAuthLogon フォルダに rclone.exe をコピーします。

アカウントとクラウドストレージとのリンク設定は、設定済みのアカウントから RClone の設定データをコピーすることでも可能です。あるアカウントでクラウドストレージへのリンク設定が済んでいれば、設定ファイルが以下フォルダに見つかります

%UserProfile%¥.config¥rclone¥rclone.conf
(%UserProfile% 例： ¥Users¥tanaka, ¥Users¥hanako)

この rclone.conf を別のコンピュータのアカウントに %UserProfile%¥.config¥rclone¥rclone.conf としてコピーすることでコピー先のアカウントが同じクラウドストレージのアカウントにリンクされます。

rclone 設定ファイルのコピー、rclone.exe の GAuthLogon フォルダへのコピーはインストール時に一括で行うと手間が省けます。