Rohos Logon Key を Active Directory で使用

Rohos Logon Key アプリは、スタンドアロンのワークステーションと Active Directory（AD）に統合されているドメインの両方をサポートしています。この記事では、後者、つまり Rohos Logon Key が AD ドメインにインストールされている場合について説明します。AD ドメインにインストールされていることにより、ローカル コンソール ログインまたは複数の TS ホストを持つターミナル サービス環境の遠隔デスクトップ ログオンについて、強力な二要素認証を行うことができます。

始めに

1. 使用する認証方法を、ハードウェア セキュリティ デバイス、ワンタイム パスワード ジェネレーター、UID RFID カードのいずれかを選択します。 AD 環境で使用できることを確認します。環境には、キーの一元管理、適用できるのであれば遠隔デスクトップ接続が含まれます。

2. Rohos に実装可能な二要素認証（2FA）保護方法の種類について理解する必要があります。

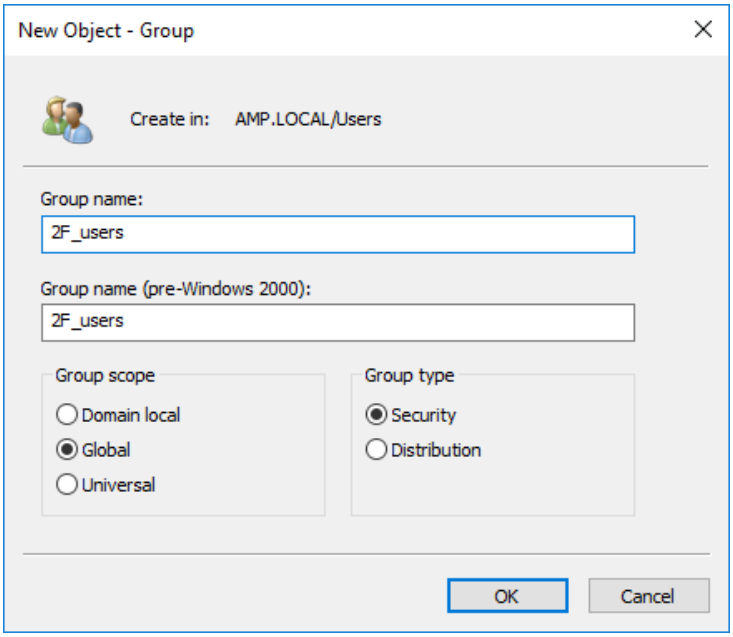
- **AD ユーザー グループのメンバー**: 特別に作成した AD グループに含まれているすべてのユーザーに対して、ワークステーションにログインまたはロック解除する場合に二要素認証が求められます。このオプションの使用を推奨。
- リストに含まれているユーザー: 二要素認証が要求されるユーザーの一覧が AD 二要素認証パーティションに保存されます。
- 遠隔デスクトップ ユーザー: 遠隔デスクトップ セッションのみ、二要素認証が求められます。追加の IP フィルタリングを使用することもできます。

AD 内に二要素認証ユーザー グループを作成

例えば、ドメイン名に DNS-name AMP.**local** や NetBIOS-name **AMP** を使用することができます。**Admin1** というユーザーが二要素認証でのログインが許可されており、パスワードのみでのログインができないと仮定します。新しいグループを作成し、**2FA_users** と名前を付け、**Admin1** をそのグループに追加します。

翻訳: 株式会社ネクステッジテクノロジー
www.shareEDGE.com

つまり、このユーザーは、同時に2つのグループ、つまりDomain users と 2FA_users のメンバーということになります。



注意: 二要素認証に別の名前を付けることができます。

二要素認証データベースを ACTIVE DIRECTORY に作成

Rohos は、MS Active Directory が提供するデータ ストレージ技術を活用して、二要素認証のデータ、ユーザーの一覧、携帯端末の一覧、その他 Rohos のドメイン全体の設定すべてを保存するための AD アプリケーション パーティション（データベース）を作成します。追加の二要素認証スキーマ要素の追加は、他の AD/LDAP オブジェクトのパフォーマンスに影響を与えることは一切ありません。詳細...

1. スキーママスターの役割を持つプライマリ AD ドメイン コントローラー（FSMO）に Rohos Management Tools をインストールします。
    - [Rohos Remote Config]ダイアログボックスが表示されます。AD に二要素認証データベース作成をするかどうか確認メッセージが表示されますので、[YES]をクリックします。
    - 現在のドメイン コントローラー（DC）が FSMO であるかどうかを確認するために “netdom query fsmo” コマンドラインを使用します。
    - 二要素認証設定を DC に複製し、それによって冗長機能を Windows AD 指針に沿って追加するには、Rohos Management Tools をセカンダリ DC にインストールする必

要があります。[Rohos Remote Config]ダイアログボックスに、セカンダリ DC に二要素認証データベースの複製を作成するかどうか自動で通知されます。

2. Rohos Remote configuration ツールを開き、Rohos Logon Key 二要素認証オプションのための AD データベース作成を確認します。

3. 二要素認証のオプション設定:

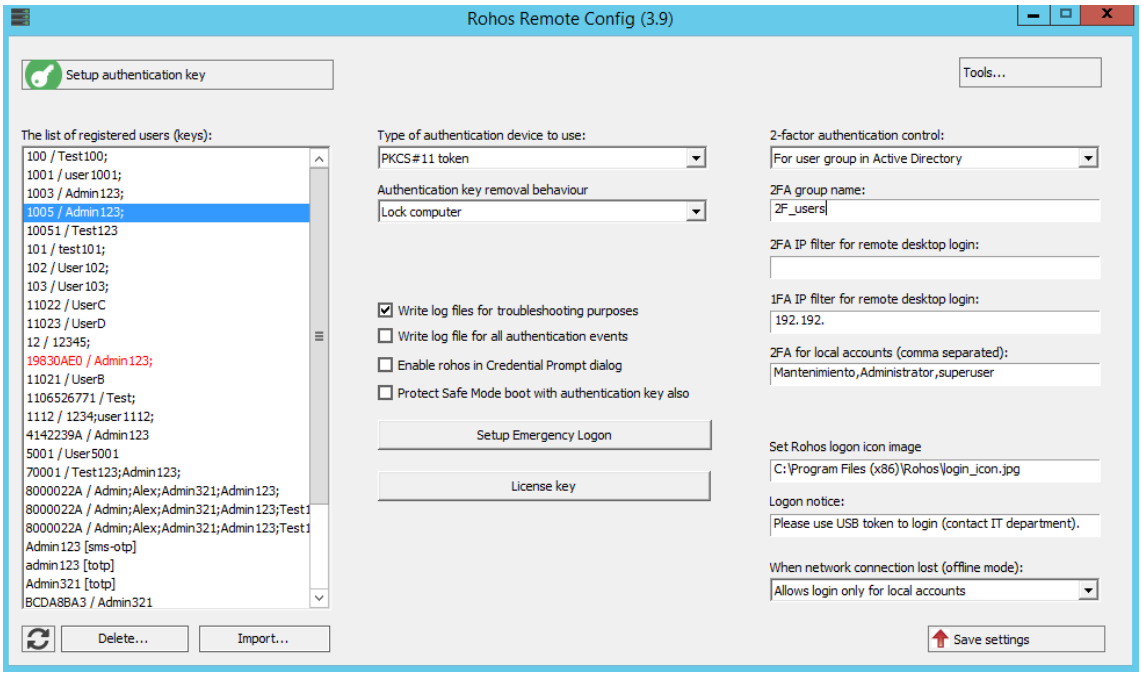
二要素認証用携帯端末/認証方法、

二要素認証方法の種類

二要素認証ユーザーの一覧を保存する二要素認証グループ名

ローカル アカウントの二要素認証方法...等

4.



5. [Rohos Remote Config]ダイアログボックスには、二要素認証用携帯端末が関連するユーザーアカウントと共に一覧表示され、特定の二段階認証方法を選択できます。

設定も保存できます。

AD 管理者権限を持つローカルのワークステーションに Rohos Management Tools をインストールすると、Rohos や接続されている認証用携帯端末の設定を引き続き行うことができます。

6. [認証キーの設定]をクリックすると、どのユーザーの認証キーや認証方法でも設定を行うことができます。

特定のユーザー グループ用の認証キーをすべて作成し終えたら、[Rohos Remote config]ダイアログボックスの**[Refresh all]**をクリックします。クリックすると、二要素認証データベースに、作成したキーが表示されます。

Rohos 管理ツールの詳細はこちら>>>

KEY MANAGER を使用して認証キーを設定

[認証キーの設定]をクリックして、Rohos Key Manager ツールまたは OTP 設定ダイアログボックスを開きます（プライマリ二要素認証方法に応じて）。

二要素認証を使用するか、パスワードを置き換える方法を使用するかを選びます。Rohos 二要素認証の種類:

1. 認証携帯端末または ワンタイム パスワード(OTP) と Windows パスワード
2. 認証携帯端末と PIN コード
3. 認証携帯端末のみ（パスワードの置き換え）

認証携帯端末を接続します。USB キー マネージャーの**メイン ウィンドウ**には、キーと関連付けられている/保存されているプロファイルの一覧を確認できます。**[ログオン プロファイルを追加]**ボタンをクリックします。

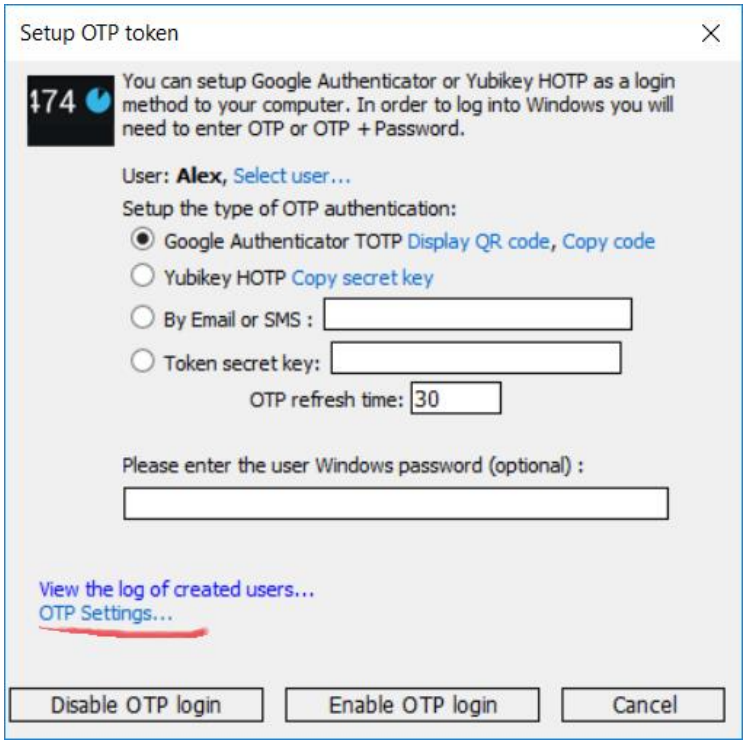
プロファイルを編集するには、選択して、**[編集]**ボタンをクリックします。キーをすでに Rohos Logon Key アプリケーションで生成済みの場合、パスワードが暗号化されます。このプロファイルは、ドメイン コンピューターの認証には適しません。右側の[*]ボタンをクリックすると、パスワードが表示されます。両方のフィールドで非暗号化に変更して、[OK]をクリックします。

- AD を使用していない場合、**[ドメイン]**フィールドは、空欄のままで構いません。キーを使って、ログインのコンビネーションとパスワードが揃っている どの PC にでもログインできるようになります。
- 二要素認証キーと Windows パスワードの両方を使用したい場合は、パスワード フィールドを空欄のままにします。ユーザーは、ログイン時に USB キーとパスワードの両方が求められます。

[パスワード]フィールドを空欄のままにすると、認証の際に、認証キーの他に、パスワードを必ず手入力するよう求められます。キーがあることにより、パスワードを変更した場合でも、ユーザーを認証することができます。

プライマリ認証方法として、Google Authenticator OTP を選択した場合

[認証キーのセットアップ]をクリックすると、 OTP 設定ダイアログが表示されます。



ユーザー アカウントを選択し、OTP メソッドを選択後、[OTP ログインを有効にする]をクリックします。
複数のユーザー アカウントを Google Authenticator に登録し、OTP 設定をメールで送ることもできます。詳細...

ROHOS LOGON KEY アプリをインストール

二要素認証による保護を適用するには、二要素認証が必要となるすべてのワークステーションとターミナルサーバーに Rohos Logon Key
アプリケーションをインストールする必要があります。インストール後、Rohos Logon Key アプリケーションは、コンピューターがドメインに接続されている場合に、AD 二要素認証設定を検出します。

Rohos Logon Key をダウンロード

二要素認証データベースを DC に複製し、それによって冗長機能を Windows AD 指針に沿って追加するには、Rohos Management Tools をセカンダリ DC にインストールする必要があります。[Rohos Re

mote Config]ダイアログボックスに、セカンダリ DC に二要素認証データベースの複製を作成するかどうか自動で通知されます。

ドメイン コンピューター用の ROHOS ライセンス

- **Pro ライセンス**: 各ドメイン ワークステーション
- **サーバー ライセンス**: ターミナル サーバー、 Windows 2003, 2008, 2012 の 遠隔デスクトップ接続 (RDC)