<u>Rohos Logon Key を Active Directory で使用</u>

- 1. <u>始める前に</u>
- 2. Rohos 管理ツールを使用して、二要素認証データベースを作成
- 3. Rohos Key Manager を使用して認証キーを設定
- 4. Rohos Logon Key をインストール
- 5. <u>ライセンス使用許可</u>

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

 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。 <u>AD 環境で使用できることを確認します</u>。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。Ad min1 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。

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。

New Object - Group		Х
Create in: AMP.LOCAL/U	Jsers	
Group name:		
2F_users		
Group name (pre-Windows 2000);		
2F_users		
Group scope	Group type	
O Domain local	 Security 	
 Global 	Oistribution	
OUniversal		
	OK Cancel	

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 <u>Rohos Mana</u> <u>gement Tools</u> 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 "net dom 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

Setup authentication key		Tools
The list of registered users (keys): 100 / Test100; 100 / User1001; 1003 / Admin 123; 1005 / Admin 123; 1005 / Admin 123;	Type of authentication device to use: PKCS#11 token Authentication key removal behaviour Lock computer	2-factor authentication control: For user group in Active Directory 2FA group name: 2F_users
10051 / Test123 101 / test101; 102 / User102; 103 / User 103; 11022 / UserC 11023 / UserC 11023 / UserD 11023 / UserB 19830AED / Admin123; 11021 / UserB 1105256771 / Test; 1112 / 1234;user1112;	 ✓ Write log files for troubleshooting purposes Write log file for all authentication events Enable rohos in Credential Prompt dialog Protect Safe Mode boot with authentication key also 	2FA IP filter for remote desktop login: 1FA IP filter for remote desktop login: 192, 192. 2FA for local accounts (comma separated): Mantenimiento,Administrator,superuser
4142239A / Admin123 5001 / User5001	Setup Emergency Logon	Set Rohos logon icon image
/10001 / 1651.25;Admin 12.5; 80000224 / Admin;Alex;Admin321;Admin 123; 80000224 / Admin;Alex;Admin321;Admin 123;Test1 80000224 / Admin;Alex;Admin321;Admin 123;Test1 Admin 123 [ms-otp] admin 123 [totp] Admin 321 [totp]	License key	Logon notice: Please use USB token to login (contact IT department) When network connection lost (offline mode): Allows login only for local accounts

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 (プライマリニ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。

	P token	×
174 🔮	You can setup Google Authenticator or Yubikey HOTP as a login method to your computer. In order to log into Windows you will need to enter OTP or OTP + Password.	
	User: Alex, Select user	
	Setup the type of OTP authentication:	
	Google Authenticator TOTP Display QR code, Copy code	
	O Yubikey HOTP Copy secret key	
	O By Email or SMS :	
	O Token secret key:	
	OTP refresh time: 30	
	Please enter the user Windows password (optional) :	
View the	log of created users	
View the OTP Set	log of created users tings	
View the OTP Set	log of created users tings	

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。<u>詳細...</u>

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)