OTP コードを使用した Remote Desktop のセキュア 2要素 ログイン認証

Rohos Logon Key は、携帯端末やワンタイム パスワードトークン（OTP）を使用することで、 Windows Remote Desktop での安全なに要素認証を提供します。

2要素認証の種類:

- 携帯端末と Google Authenticator アプリ を使用する場合
- 携帯端末に SMS またはメールで一度きりのパスワードトークン（OTP）を送信する場合
- サードパーティ OTP コード配達サービスや GSM モデムの統合を許可する場合
- Yubikey/SecureID/SafeNet/Feitian 等の OTP 生成ハードウェアを使用する場合
- それぞれのユーザー アカウントに対して、異なる二要素認証の方法を設定することもできます。

Remote Desktop の二要素認証の利点:

- ユーザーは、ログイン毎に、新しい OTP コードを入力する必要があります。
- 生成される OTP コードは、すべて固有のものであるため、複製されることはありません。
- Remote Desktop アクセスをユーザー一覧やユーザー グループによって制限できます。
- ログインするクライアント PC/デバイスに Rohos をインストールする必要がありません。
- ユーザー一覧、Active Directory グループの一員、IP アドレスのフィルターによって2要素認証を適用します。

株式会社ネクステッジテクノロジー
www.shareEDGE.com

- 既存のどの SIEM にでも再考察し、2要素認証を含めることができます。

Rohos Logon Key は、良く知られていて安全なワンタイム パスワード（OTP）認証技術を使用して、Windows Remote Desktop へのアクセスを許可します。脆弱なパスワードによるログインに変わるものとなります。

どのように機能するのか

Rohos Logon Key をターミナル サーバーにインストール

ユーザー アカウントに2要素認証を有効にする方法

Google Authenticator で複数のユーザーを登録する方法

自動2要素認証を使用して、OTP コードを SMS で送信

ユーザー アカウントの2要素認証を無効にするまたはリセットする方法

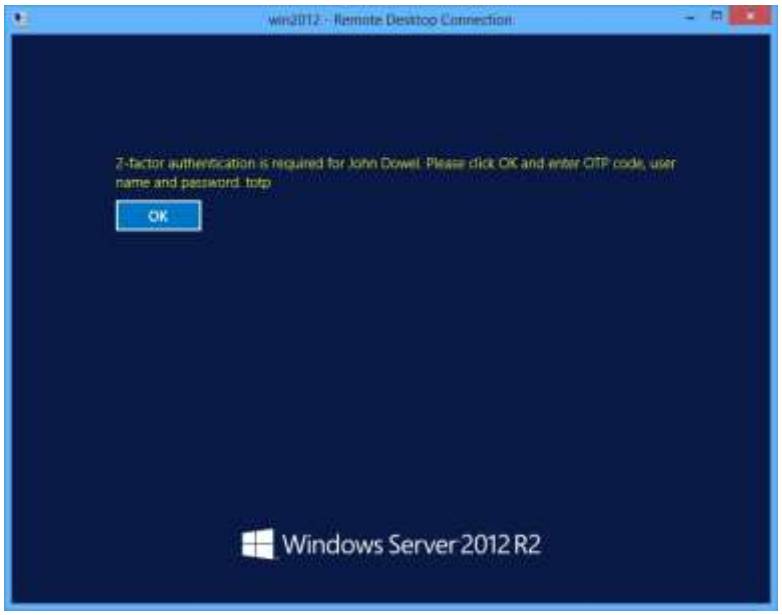
クライアント IP フィルターを使用して2要素認証を有効にする

Rohos Logon Key のライセンスの種類

どのように機能するのか

Rohos Logon Key は、Windows リモートデスクトップ サービス（旧称: ターミナル サービス）の認証プロバイダーと統合または代わりとなります。既存の認証基礎構造に、2要素認証レベルを追加します。追加後は、遠隔セッションへのログインは、2要素認証が必須になります(OTP コードと通常のログイン データ)。

2要素認証を求める Rohos Logon Key のメッセージ :



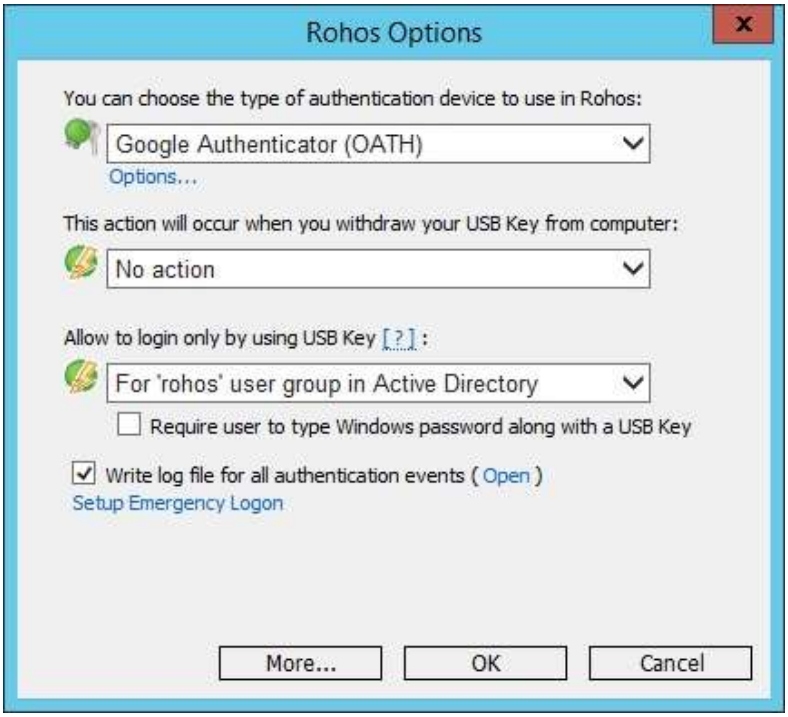
OTP コードの入力により、Remote Desktop にログイン:

Rohos Logon Key をターミナル サーバーにインストール

1. Rohos Logon Key を Windows 2008/2012 ターミナル サーバーにインストールします:

Rohos Logon Key の試用版（15日利用可能）をダウンロード

2.OTP を使用した2要素認証を有効にします。[オプション]を開き、[Google Authenticator（OATH）]を有効な2要素認証に設定します。



3. 2要素認証の方法を選択します。

- **一覧内のユーザーが対象**

  設定されたユーザーのみが、2要素認証の使用を求められます。その他のユーザーは、通常通り、パスワードを使用してログインできます。ユーザーの一覧は、[キーを設定]ダイアログボックスによって自動的に作成されます。確認するには、[ユーザーとキー]ダイアログボックスを開きます。

- **Active Directory の Rohos ユーザー グループが対象**

  Rohos グループ内のすべてのユーザーが、 Remote Desktop ログインの際に2要素認証を求められます。.

  注意:Rohos ユーザー グループは、Active Directory Administrator の管理者が作成する必要があります。

- **Remote Desktop ログインが対象**

  すべての Remote Desktop セッションで、2要素認証が求められます。
- **ローカル ネットワーク外の Remote Desktop ログインが対象**

  （実験的な機能）

  ダイアルアップ、DSL 接続、または他のネットワークからログインしようとしているユーザーにのみ、2要素認証が求められます。

試用していただくには、ターミナル サーバーに Windows 2003/ 2008/ 2012 サーバーのいずれかが必要です。

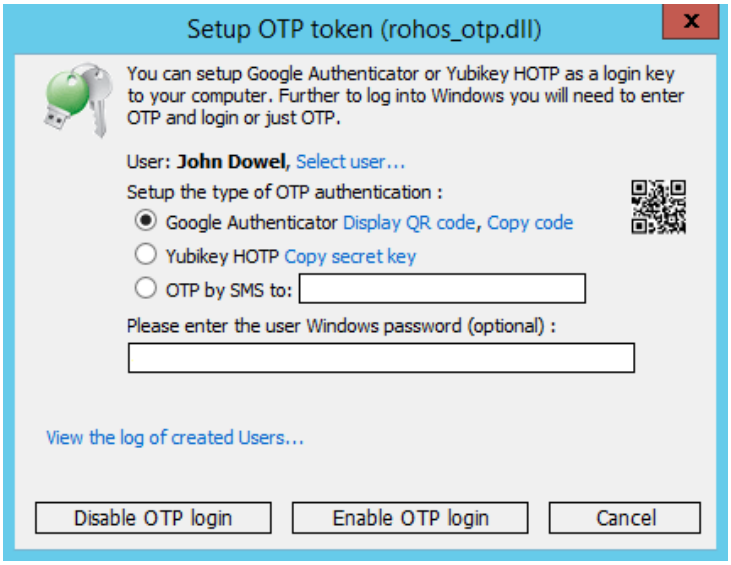
4.緊急時ログインを設定

2要素認証方針によるターミナル サーバー ログインのロックアウトを防ぐため、緊急時ログイン オプションを設定することをお勧めします。これにより、管理者は、ターミナル サーバーのコンソール/リモート デスクトップに、ユーザー名、秘密の質問、パスワード、を使用してログインできるようになります。緊急時ログインは、2要素認証が求められません。緊急時ログインは、Server Console へのアクセスの可能性がある場合には、設定しなくてもいいでしょう。

ユーザー アカウントに2要素認証を設定する方法

2要素は各ユーザー アカウントに対して個別に適用されます。自動設定は、[OTP コードを SMS で送信]オプションを選択時にのみ行われます。

ユーザー アカウントに対して2要素認証を設定するには、Rohos Logon Key の[キーの設定]を開きます。



1. ユーザー アカウントを選択します。
2. OTP を何で生成するかを選択します。
3. パスワード フィールドは空欄のままにします。
4. [OTP ログインを有効にする]をクリックして、設定を適用します。

[QRコードを表示] と[コードをコピー]をクリックして設定を行うか、Google Authenticator 設定をユーザーにメールで送ります。

[メール/SMS で OTPを送信]オプションを使用する場合

- 携帯を入力するか、AD ユーザー アカウント プロパティの携帯の欄が入力されていることを確認してください
- または、ユーザーのメールアドレスを入力してください。
- [Rohos Logon] > [オプション] > [Google Authenticator]オプションで、OTP 送信方法を正しく設定していることを確認してください。

Google Authenticator で複数のユーザーを登録する方法

Rohos 管理ツールによって、安全、わかりやすい、カスタマイズ可能は方法で、Google Authenticator 二要素認証で複数のユーザーを設定したり、メールや SMS で2要素認証の設定を送信したりできます。

Rohos 管理ツールで可能なこと

- Google Authenticator 2要素認証でユーザー グループを設定できます。
- Google Authenticator 設定をユーザーにメールで送信できます。
-SMS / テキスト ファイル / Web サーバー公開等、カスタマイズされた送信方法を設定できます。
- 登録されている2要素認証ユーザーの2要素認証の設定を再送または削除します。

株式会社ネクステッジテクノロジー
www.shareEDGE.com

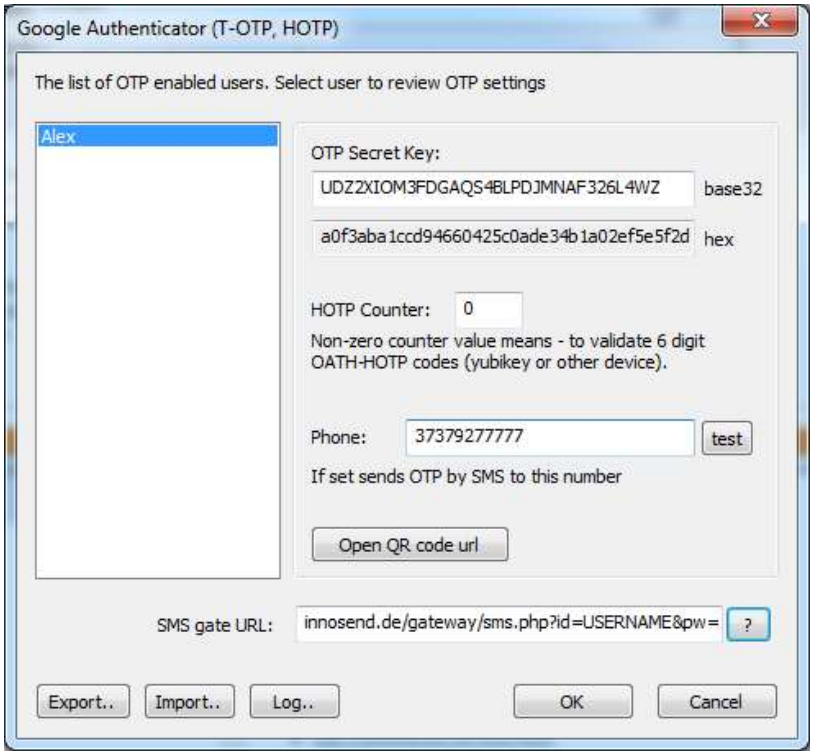
SMS による自動2要素認証を有効にする

Rohos Logon Key は、Remote Desktop ユーザーに対して、自動2要素認証の利用を可能にします。Remote Desktop ログイン時に、Rohos は自動で、OTP コードをユーザーの電話番号に SMS で送ります。

ターミナル サーバーが次の条件を満たしている必要があります。

- 電話/携帯番号の欄にユーザーの携帯電話番号が入力されていること
- Rohos Logon Key が SMS ゲートウェイ サービスによって設定されていること

SMS ゲートウェイまたは他の OTP配達方法を設定



1. お住いの国で利用可能な SMS ゲートウェイ サービス（有料サービス）を選択してください。
2. SMS ゲートウェイ送信リクエスト HTTP URL の設定を、[Rohos] > [オプション] > [Google Authenticator] > [オプション…] > [編集]で行います。
3. URL を %phone% と %text% パラメーターを使用して設定します。

URLの一例 :

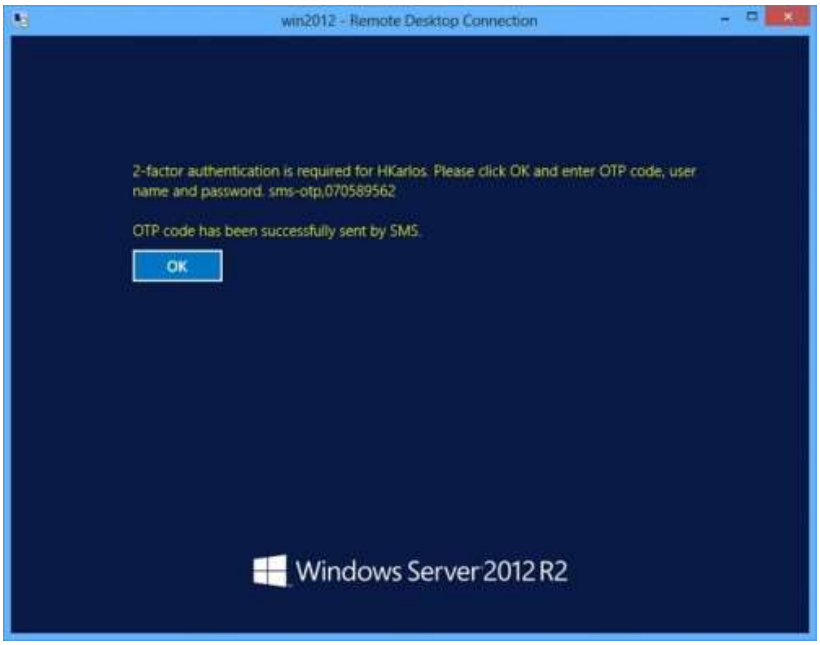
innosend.de/gateway/sms.php?id=USERNAME&pw=PASSWORD&text=%text%&empfaenger=%phone%&type=2

URL の、%phone% と %text% はユーザーの電話番号と OTP コードのテキストに置き換えられます。

電話番号またはメールアドレスを入力して、[テスト送信]ボタンをクリックすると、OTP コードを指定した方法で送信できます。

送信方法の設定に関する詳細

Remote Desktop ログインの SMS 認証を有効にする:



2要素認証の無効化、またはリセットを行う方法

サーバー全体、また選択したユーザー アカウントに対して、2要素認証を無効にする、またはリセットする方法は何通りかります。

2要素認証の方法を無効にする:

- Rohos Logon Key のアンインストールにより、パスワードでの認証またはパススルー認証にレストアされます。
- [なし]または[USB キーでのログインを許可]オプションを設定することで、一時的にすべてのユーザーの2要素認証を無効にすることができます。

ユーザー アカウントの2要素認証をリセット/変更/無効にする:

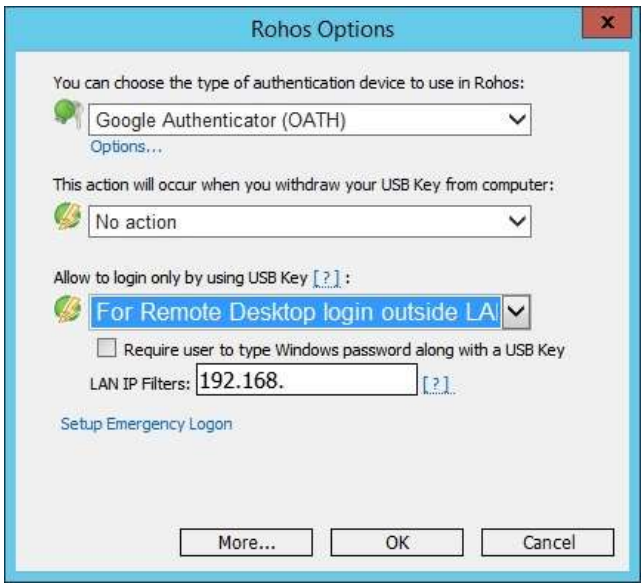
1. Rohos AD グループからユーザー アカウントを削除すると、ユーザーに対する2要素認証の要求が無効になります(万が一の場合に備えて、Rohos グループには2要素認証を要求)
2. Rohos で、キーダイアログボックスの設定を行い、ユーザー アカウントの選択後に[OTP ログインを無効にする]をクリックします。これにより、ユーザーの2要素認証がリセットされます。OTP を生成している Google Authenticator、 Yubikey 等が無効になります。
3. Rohos を開き、[ユーザーとキー]ダイアログボックスでユーザーを探し、一覧柄削除します。ユーザーに対する2要素認証の要求が無効になります (万が一の場合に備えて、Rohos グループには2要素認証を要求)

クライアント IP フィルターを使用して2要素認証を有効にする

Rohos Logon Key の実験的な機能では、 Remote Desktop 接続をクライアントの IP アドレスによってフィルタリングし、IP マスクによって2要素認証を求めることができます。

Remote Desktop の2要素認証に IP フィルターを使用する方法:

1. Remote Desktop セッションで、Rohos Logon Key の[オプション]を開きます。
2. [USBキーによるログインのみ許可する]オプションを[ローカル ネットワーク外の Remote Desktop ログインが対象]に設定します。
3. [?] をクリックすることで、Rohos がクライアント WAN IP アドレスを認識できたか確認できます。
4. [LAN IP フィルター]を指定します。ローカル LAN のプレフィックスになります。このプレフィックス Rohos を使用することで、LAN と WAN 接続を区別し、WAN IP を使用しているクライアントに2要素認証を求めることができます。



Rohos Logon Key のライセンスの種類

- **Rohos Logon Key Server** ライセンスは、Rohos Logon Key のそれぞれのターミナル サーバー ホストに対して必要になります。ユーザーの制限数なく保護でき、認証キーの数制限もありません。
- **Rohos Logon Key Small Server** は、最大15 ユーザーを保護できます。

SMS での認証に必要なサードパーティ SMS ゲートウェイ サービスは、Rohos Logon Key に含まれていませんのでご注意ください。

Rohos Logon Key Server Edition 詳細は、こちら

http://www.shareedge.com/modules/shareware/view_shareware.php?lid=20090525-002&gid=7