USB キーを使用して Windows リモート デスクトップへのセキュアなログインを実現

Rohos Logon Key 2 要素認証(2FA)ソフトウェアが、ターミナル サーバーを保護し、パスワードとハードウェア USB トークンを使用してリモート デスクトップにログインを可能にします。

Rohos Logon Key は、OTP 技術を含む、様々な認証デバイスをサポートしており、柔軟な 2 要素認証の操作を可能にします。

本情報の英語版

株式会社ネクステッジテクノロジー
www.shareEDGE.com

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）のログイン画面に統合されます。既存の認証基礎構造に、2 要素認証レベルを追加します。2 要素認証適用後は、追加のセキュリティ デバイスさえあれば、リモート デスクトップ セッションにログインできます。

リモート デスクトップ アクセス操作の利点:

- 2 要素認証の対象を、ユーザーの一覧、Active Directory のユーザー グループ、リモート デスクトップ ユーザーのみ、等に限定することができます。
- ユーザーは、ログインの度に、USB トークンを差し込む必要があります。
- 生成されるキーは、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。
- リモート デスクトップやローカル管理者 PC 経由でターミナル サーバーの USB キーを設定できます。.
- 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。
- 異なる開発元の PKCS#11 トークンを同時に使用することができます。

高いセキュリティ レベルを可能にする 2 要素認証の種類:

- ユーザー ログイン + USB キー（例えば、 SafeNet、eToken、iKey、ePass、他の PKCS#11 トークン）
- ユーザー ログイン + USB フラッシュドライブ
- 暗号化されたパスワードのみが USB トークンに保存されます。
- ワンタイム パスワード（OTP）すべて: Google Authenticator、Yubikey、SMS 認証、従来の OTP トークン

2 要素認証の種類とサポートしているデバイス

USB キーを使用した Remote Desktop ログインを試すには、Rohos Logon Key の 15 日間試用版をダウンロードしてください。**ダウンロード**

試用していただくには、ターミナル サーバーに Windows 2003 から 2016 サーバーが必要です。

始める前に、2 要素認証の種類を確認してください。

ターミナル サーバーへの認証の種類	認証デバイスの種類	Rohos Logon Key をクライアント PC と/または サーバーにインストール	
		クライアント Windows XP–10	**ターミナル サーバー** Windows 2003–2016
1) 2 要素認証: 物理的なキー + Windows パスワード (NLA)	eToken、iKey 等の USB トークン (PKCS#11) スマートカード JavaCard OTP、SMS、Yubikey、Google 認証 USB フラッシュドライブ*	–	+
2) 物理的なキーのみ (または PIN コードを含むキー)	USB フラッシュドライブ USB トークン (PKCS#11) Java-Card、Mifare 1K	+	+
3) 高速かつスムーズなログインのため、クライアントの側にのみキーを使用します。ターミナル サーバーでは、USB キーを確認しません。	すべての種類のキー	+	–

* USB フラッシュドライブをキー デバイスとして使用する場合:管理者が、Rohos Management Tools をローカル PC にインストールする必要があります。
* ワンタイムパスワード（OTP）技術を使用した 2 要素認証のセットアップ

サポートしているセキュリティ デバイスの一覧:

1. スマートカード Java-Card、RFID カード Mifare 1K/4K
2. PKCS11 トークンすべて:SafeNet eToken、Securetoken ST3/4、senseLock trueToken、RuToken、uaToken、iKey、ePass、Crypto Identity トークン モデル/販売元が異なっていれば、同時に使用することができます。
3. OTP トークン、Google 認証、Yubikey、SMS を使用した認証
4. 通常の USB フラッシュドライブ

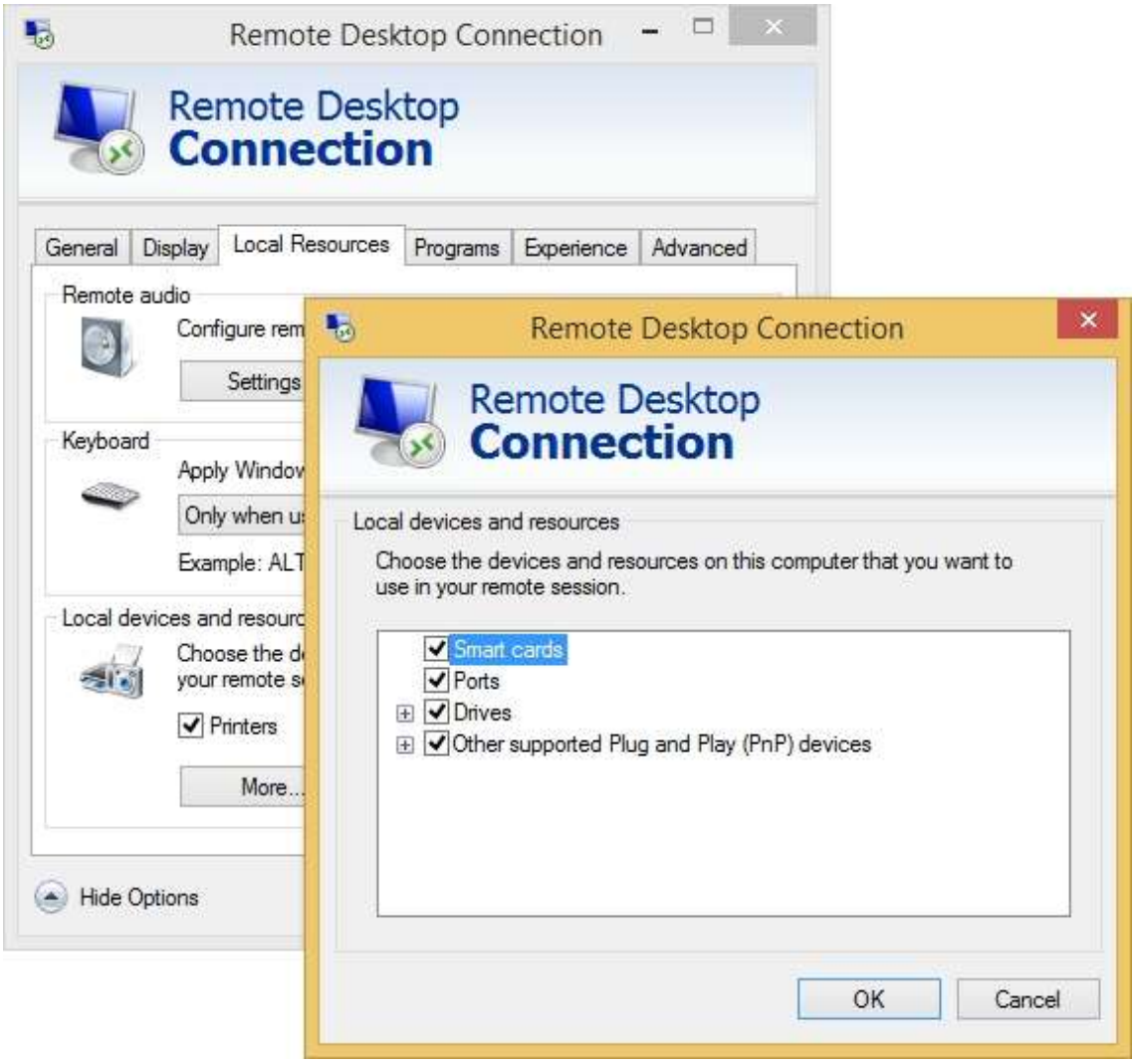
USB トークンの設定方法

1.Rohos Logon Key をターミナル サーバーにインストール

2.Rohos Management Tools を管理者のコンピューターにインストール

3.USB トークンを認証用に設定:

Microsoft リモート デスクトップ接続の接続設定で、ローカルの USB ドライブまたはスマートカード リーダーを Remote Desktop に変更します。



株式会社ネクステッジテクノロジー
www.shareEDGE.com

リモート デスクトップで、**Rohos Logon Key** を開きます。
[USB キーの設定]ボタンをクリックします。変更された USB キー検出されます。Windows パスワードを入力して、[セットアップ]をクリックします。

[ユーザーとキー] コマンドを選択すると、既にキーを設定したユーザーの一覧が表示されます。

– これで、USB キーはログインに使用する準備ができました。ターミナル サーバー セッションを閉じ、USB キーを使用してログインをお試しください。

(USB フラッシュドライブに関する注意:“Rohos Logon Key (RDC setup).exe” ファイルは、セットアップ後、自動的に USB ドライブにコピーされます。携帯可能な Rohos コンポーネントとして、Rohos Logon Key をインストールしていない PC でもこのキーを使用できます。使用方法は、以下を参照してください。)

4.2 要素認証の適用

Rohos Logon Key を開き、[オプション] > [USB キーによるログインのみ許可する] > **[一覧内のユーザーが対象]**または**[リモート デスクトップ ログインが対象]**を選択します。USB キーを使用しない認証を無効にすることで、安全性が上がります。

利用可能な選択肢:

- **なし**

すべてのユーザーが、パスワードの入力または USB キーを使用してログインできます。ターミナル サーバーでの使用は推奨されません。

- **すべてのユーザーが対象**

[USB キーによるログインのみ許可する]オプションと同じです。すべてのユーザーが、ログイン時に USB キーの使用を求められます。

- **一覧内のユーザーが対象**

一覧内のユーザーのみが、ログイン時に USB キーの使用を求められます。その他のユーザーは、パスワードを使用してログインできます。一覧は、ユーザーに対して USB キーが作成されると自動的に作成されます。詳細は、**[ユーザーとキー]**ダイアログボックスの項目を参照してください。

- **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に、 USB キーを使用した認証が求められます。.Rohos グループに含まれているかの確認が行われ、Rohos グループに含まれていない場合は、パスワードを使用してログインできます。

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

- **リモート デスクトップ ログインが対象**

ローカル ユーザーは、USB キーなしでログインできます。遠隔ログインには、USB キーが必要になります。

- **ローカル ネットワーク外のリモート デスクトップ ログインが対象**

LAN 内のリモート デスクトップ ログインは、USB キーの使用/不使用のどちらも可能です。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、USB キーが必要になります。

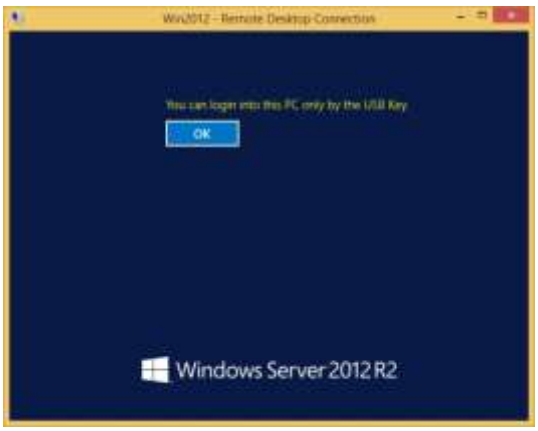
USB トークンを使用した Remote Desktop 接続

Rohos Logon Key をクライアント PC にインストールしているか、Rohos Logon key の携帯可能なアプリを USB フラッシュドライブから起動する必要があります。

リモート デスクトップ接続での認証情報確認画面

この段階では、有効なログインとパスワードを提供する必要があります。
認証キーを使用することもできます（Rohos USB Key Manager を使って設定されたものに限る）。

Rohos Logon Key は、リモート デスクトップ接続時に、2 要素認証方法(2FA)を確認し、接続された認証キーを確認します。:



株式会社ネクステッジテクノロジー
www.shareEDGE.com

持ち運び可能な Rohos Logon Key

USB フラッシュドライブの使用と、最初の認証方法を選択した場合、Rohos Logon key をすべてのワークステーションにインストールする必要はありません。この無料で携帯可能なアプリケーションをインストールするだけです。

取得方法

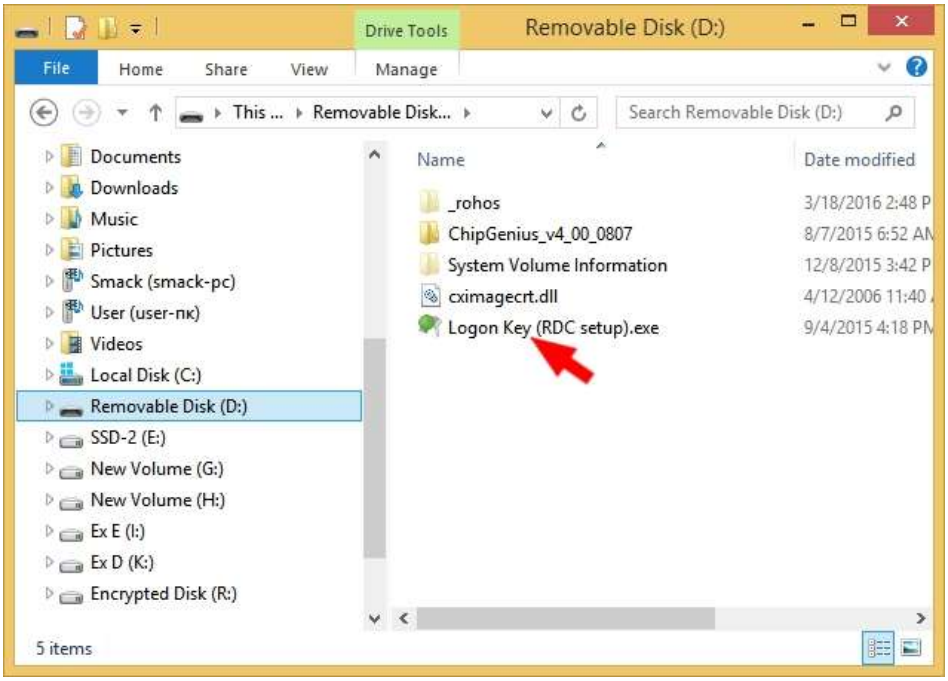
持ち運び可能な Rohos Logon Key をダウンロード

USB key manager アプリケーションの追加オプションとしても用意されており、 Rohos Remote Login を USB ドライブにコピーできます。USB key manager の**[Remote Desktop]**ボタンをご利用下さい。

USB key manager についての詳細（英語サイト）

ユーザーは、**Logon Key (RDP セットアップ)** アプリケーションを Windows 7/8 のクライアント PC で一度実行する必要があります。その後、リモート デスクトップ アプリケーションを起動する必要があります。

株式会社ネクステッジテクノロジー
www.shareEDGE.com



リモート デスクトップ接続用 ROHOS LOGON KEY アプリケーションのライセンス

- **Rohos サーバー ライセンス** は、 Rohos Logon Key をインストールしたターミナル サーバー PC、リモート デスクトップ接続アクセスが可能な Windows 2003、2008、2012 で必要になります。
- リモート デスクトップ接続アクセスが可能なワークステーション（他の Windows バージョン）には、**PRO ライセンス**が必要です。
- Rohos Logon Key をローカル PC にインストールする場合（2 つ目と 3 つ目の認証方法）、それぞれの PC 毎に **パーソナル ライセンス**が必要です。

株式会社ネクステッジテクノロジー
www.shareEDGE.com