Remote Desktop Manager Basics: How to Set Up a Security Provider

Devolutions

SHARED ADVANCED DATA SOURCES SHOULD ALWAYS BE SECURED WITH A SECURITY PROVIDER

When we start something new, it's always important to follow the right steps. I mean, have you ever tried assembling a wardrobe from IKEA without the instructions? It's a recipe for disaster. Instead of ending up with a nice piece of furniture to store your clothes, you'll be lucky if you don't wind up with a portal to Narnia.

In the same sense, getting the most out of RDM involves taking care of the basics – and one of the essential steps in the process is setting up your Security Provider.

About Security Providers

A Security Provider enables you to encrypt an advanced data source, ensure that hackers (and all other unauthorized users) cannot access configuration information associated with your various entries – even if they have direct access to the database or a backup of the database.

Shared advanced data sources should always – I repeat, always! – be secured with a Security Provider; especially when using the Devolutions Online Database. With that being said, keep in mind that regardless of the Security Provider you choose, passwords stored in data sources are ALWAYS protected with AES 256-bit encryption.

Getting Prepared

Before setting up a Security Provider (or making changes to an existing Security Provider), you need to get prepared by doing the following:

1. Ensure all users are disconnected from the data source.

2. If you already have entries in your database, we strongly recommend creating a backup before continuing. The new Security Provider will apply to the ENTIRE database – not just new entries.

3. If dealing with a great number of entries in your database, we strongly recommend performing all clean up tasks (logs, entries, deleted history and pack data source).

Setting Up a Security Provider

Now you're ready to set everything up. Here's what to do:

1. Go to **Administration– Security Provider– Change Security Settings**.

2. Click on the dropdown menu and select the security type you wish to use. Your options are Default, Shared Passphrase or Certificate. Here is a summary of each:

> **Default:** This is the legacy Security Provider. Data will be encrypted if the entry configuration is set accordingly in the advanced settings of the entries.
>
> **Shared Passphrase:** This will encrypt your entry configuration data using a mix of keys stored in Remote Desktop Manager and the passphrase that you've entered. The passphrase is only required when configuring the data source. However, you can also enable a policy to prompt users for the passphrase every time they connect to the data source. Important: don't forget your passphrase! If that happens, then absolutely NOTHING can be done to recover your data. Even Aslan from Narnia can't help you. Make sure to keep your passphrase in a safe and secure location.
>
> **Certificate:** This will encrypt your entry configuration data using a mix of keys stored in Remote Desktop Manager and the private key contained in the certificate.

3. Once you've selected your Security Provider, simply click **Apply** to save your changes. Keep in mind that it may take some time if you are changing a data source that has many entries. But trust me: the extra security and peace of mind is worth it. You'll be as happy as the IKEA man!

As always, please let us know your thoughts by using the comment feature of the blog. You can also visit our forums to get help and submit feature requests, you can find them here.