Remote Desktop Manager Startup Checklist for Teams

Devolutions

WE HAVE CREATED SOMETHING THAT MANY OF YOU HAVE BEEN ASKING FOR

Remote Desktop Manager offers a wide range of features and options for teams. To simplify and streamline your on-boarding experience, we have created something that many of you have been asking for. Please dim the lights, start the drum roll, and feel free to "ooh and aah" with anticipation, because it's finally here: The Remote Desktop Manager Startup Checklist for Teams.

CHECKLIST FOR TEAMS	
Step 1 – Register your License	
Step 2 – Choose your Data Source	
Step 3 – Select your Security Provider	
Step 4 – Setup a Team Folder for Default Settings	
Step 5 – Create your Default Settings	
Step 6 – Create Users	
Step 7 – Create Roles	
Step 8 – Create Top Level Folders	
Step 9 – Grant Permissions	
Step 10 – Import your Data	

STEP 1 REGISTER YOUR LICENSE

Start by registering your version of Remote Desktop Manager. Go to Help – Register Version, and enter your user name, email address and serial number. Please note that you need to enter the information exactly the way it is listed in the email that you received.

STEP 2 CHOOSE YOUR DATA SOURCE

Choose your advanced data source. This is necessary since, in a team environment, you'll need your data source to support attachments, connection logs, offline mode and security management. Here is a table to help you choose the right data source to meet your requirements:

	Devolutions Server	SQL Server	SQL Azure	MySQL/ MariaDB	Devolutions Online DB Professional	Devolutions Online DB Enterprise
The database must not be accessible to end users	✓	✓**			✓	✓
Active Directory accounts are used for authentication	✓	✓				
Active Directory group membership is used to assign permissions	✓					
Data is stored on premises	✓	✓	✓	✓		
Activity Logs are required	✓	✓	✓	✓		✓
Data must be accessible globally	✓***		✓		✓	✓
Optional local cache of connections	✓	✓	✓	✓	✓	✓

** The database will not be accessible to end users when using custom SQL authentication. *** The data will be accessible globally when exposing the server instance to the internet.

STEP 3
SELECT YOUR SECURITY PROVIDER

It's important to select your security provider before importing or creating any data in your database so nobody can read your entry configuration data, even when people have direct access to your database. Regardless of the security provider you select, the passwords stored in your database are always encrypted using AES 256 bit encryption.

- Go to **Administration – Security Provider – Change security settings.**
- Select your preferred Security Provider type.
- Click on Apply to save and apply the changes made to your Security Provider.

STEP 4
SETUP A TEAM FOLDER FOR DEFAULT SETTINGS

Create a team folder to store your default settings template. Modify your path to point directly to your network share. Don't forget that if you have remote workers, you will need to make sure they have offline access to the network share (Windows 10 - sync center). Here's how:

- Access your server drive (such as \\servercommon).
- Create a new folder for your team default settings.
- Go to **Options – Path – Default Templates.**
- Point the path to your newly created folder stored on your server drive.
- Enable the **Make available offline** option on the share.

STEP 5
CREATE YOUR DEFAULT SETTINGS

To create your organization's default settings, follow **File – Templates – Default Settings** and select the default settings template you wish to create. You can also modify the template to fit your organization's requirements. Your template will automatically be saved in a newly created team folder on your shared server.

You can also create, edit or reset your default settings whenever a new entry is created. Each entry type is supported, and can have a default template defined.

STEP 6
CREATE USERS

Remote Desktop Manager supports advanced user rights management. User accounts must be created manually by an administrator of the database.

- Go to **Administration – Users**.
- Click on **Add User**.
- Enter all the required information.

STEP 7
CREATE ROLES

Create Roles to easily manage your security system. You can then assign users to Roles; this makes it easy to grant permissions to a set of users instead of having to manage permissions individually. Please note that some visibility control access depends on the active data source, and in order to create roles and assign permissions, you must be an administrator of the database.

- Go to **Administration – Roles.**
- Create your new Role and give it a name.
- Click on **Assign Roles** and select every user you wish to add to the Roles.

STEP 9
GRANT PERMISSIONS

The next step is to grant permissions for your Role based security system.

- Edit your folder properties
- In the **Permissions** side menu of your folder, set the Permissions option to **Custom**
- Select the type of permission you wish to grant: View, Add, Edit or Delete
- Select **Custom** in the drop-down menu next to the permission
- Click on the ellipsis and select your Role.

The permissions granted on the folder will then be inherited by each entry set under that folder. If you are using integrated security (Active Directory), please follow this link for more information.

Remember that all entries without security are considered public, which means that they will be available to all of your data source users.

STEP 8
CREATE TOP LEVEL FOLDERS

Top level folders are the foundation of a solid security structure. Your folder structure should represent your company structure.

For example, you can create a folder for your Production team, one for your Staging team and one for your Testing team. From **Edit – New Entry**, select Group/Folder, the type you wish to use and then enter a name.

STEP 10
IMPORT YOUR DATA

The last step is to import your data into RDM. There are a few simple ways you can do this: **Excel/CSV**. Are all of your credentials and passwords in Excel? (Hey we're not judging, we're just asking. :)) If so, then here's what to do:

- Ensure the column headers match with fields of RDM, please refer to **Import Strategies file format** for more details.
- Save the file in the CSV format
- Go to File - Import – Import Entries
- Select your CSV file and click Open

And that's it. All your entries will be automatically imported into RDM. **Active Directory Synchronizer**. The handy Active Directory Synchronizer will create sessions for computers located in your Active Directory structure. For more information, please follow this link.

If your preferred import method isn't listed above, don't worry: there are many ways to get your sessions, logins and contacts into RDM. Click here for more information. 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.