The Basics: How to Manage Credentials

MANAGING CREDENTIALS IN RDM

When it comes to managing credentials in RDM, there's no "one size fits all" method. The optmal approach depends on several factors, including your organization's security policies and compliance requirements.

However, there are some fundamental considerations that should guide your strategy. These include:

» Password Visibility

Ensure that your entry type aligns with password visibility requirements by asking: Who should be able to see the credentials? Will the credentials be used for a privilege account? Should end-users be able to modify the credentials?

Based on your analysis, you may decide to choose a Username/password type entry, which would make the password usable, but not visible. Or, you may decide to use an Information/Login (Account) type entry, which would make the password completely accessible to end users.

» Inherited Credentials

If you need to use the same credentials across a whole branch of network infrastructure, you may want to take advantage of RDM's inherited credentials feature. In this case, you simply define your credentials directly on a folder. Then, all of the sessions defined in that folder would automatically go up the ladder and inherit those credentials.

» Entry Location

When storing a credential entry in your tree view, users with view permission for that entry — or who have inherited permission to the folder where the entry is stored— will be able to use it. However, they will not be able to edit it.

» Private Vault

You can allow each of your users to store and manage their personal passwords through their own Private Vault, which is RDM's user-specific repository.

» User Specific Settings

User Specific Settings are overrides for certain entry settings and are primarily used for credentials. When applying an override, you can choose the type, or you can link to a credential stored in an end user's Private Vault.

SCENARIOS

Now that you're familiar with the fundamentals, here are some scenarios to help you see how they could be applied in your environment:

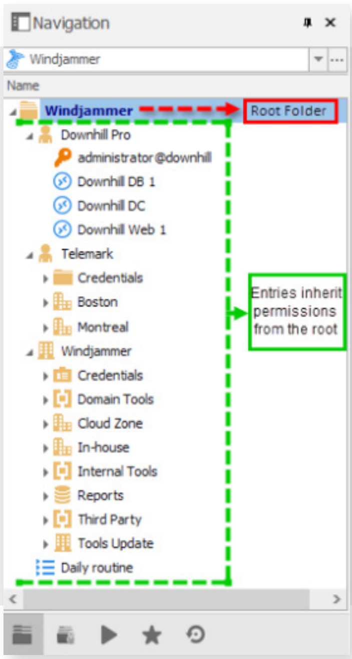
Background: You are the administrator of an IT company with 25 employees, all of which are using RDM to connect to sessions, credentials and privileged accounts.

Scenario 1

You want all 25 employees to use the same set of credentials to connect to a server, or to access a specific folder.

Solution

Define the credentials on the root settings folder and set all the children folders to **Inherited Credentials**. By default, lower level folders inherit security from higher folders until reaching the root. As such, the entry will climb up the tree until it has access to a set of credentials.



Root Folder

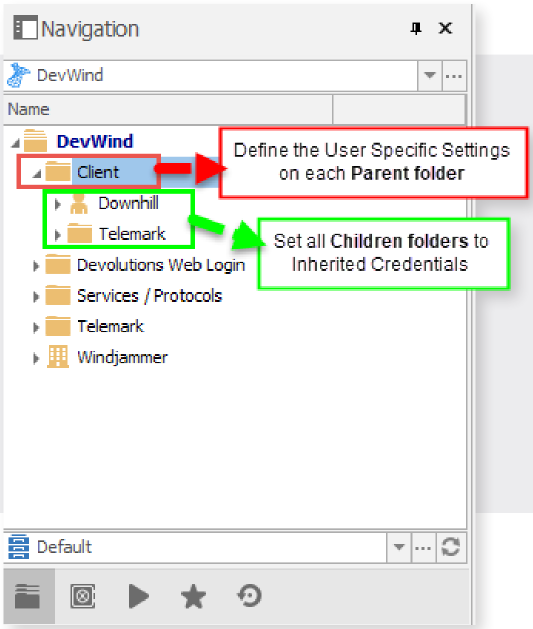
Entries inherit permissions from the root

Scenario 2

Each user has their own set of credentials for multiple folders.

Solution

Define the User Specific Settings on each parent folder and then set all the children folders to Inherited Credentials.



Define the User Specific Settings on each **Parent folder**

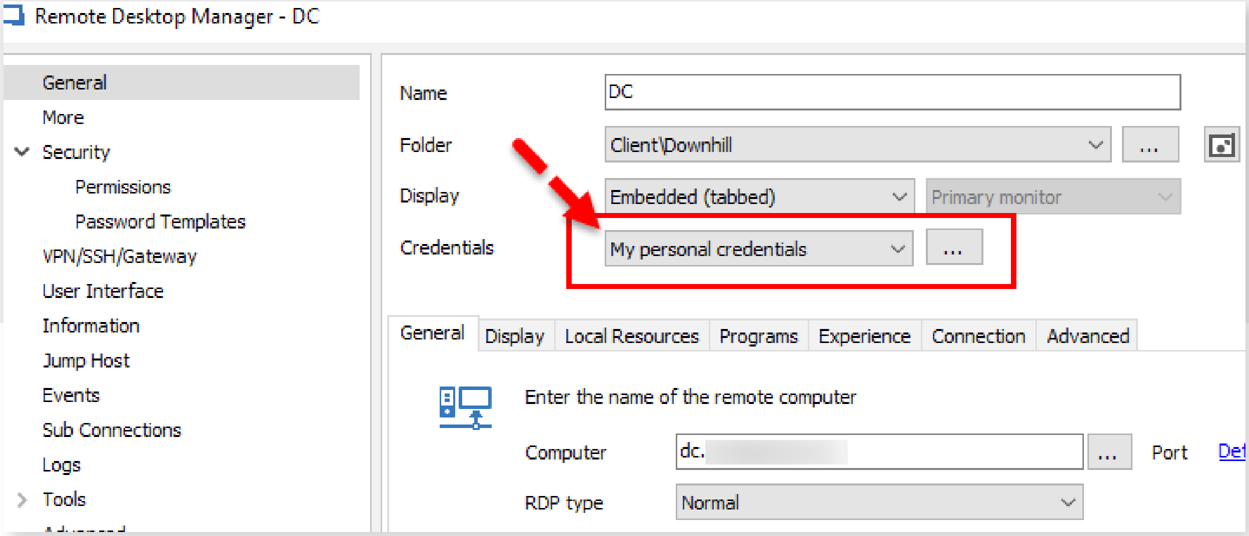
Set all **Children folders** to Inherited Credentials

Scenario 3

Each of your 25 users needs their own domain account.

Solution

Configure entries to use **My Personal Credentials**, which is a single credential entry locally stored on your computer in your Windows profile. Each user will then be prompted to define their credentials once on each workstation they use.



Name: DC

Folder: Client\Downhill

Display: Embedded (tabbed) | Primary monitor

Credentials: My personal credentials

Computer: dc.[redacted]

RDP type: Normal

And there you go folks! Obviously, there are many more scenarios, but these are some of the most common ones. If you need advice on a different scenario, we're always here to help. Please post your question below, or contact us for support.

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.