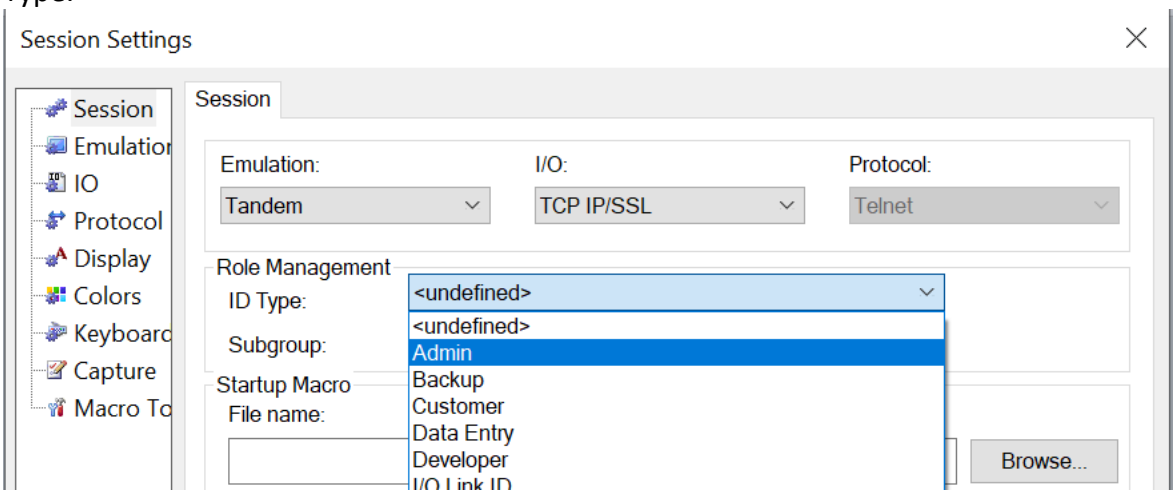
A Useful Feature You May Not Know About

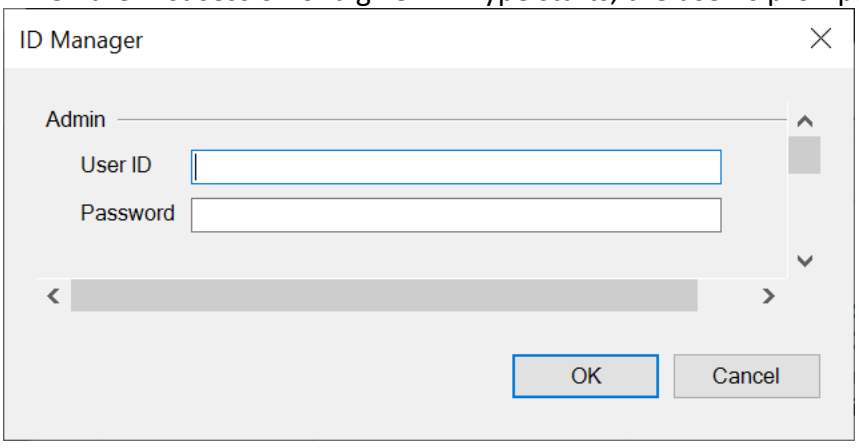
#5 Identity Management and Session Cloning

Identity Management is a labor-saving mechanism to reduce repetitive logging in throughout the day.
In many organizations, individuals perform different roles throughout the day. The user might be a system administrator, database administrator, or end user at different times. OutsideView Role Management enables you to map those roles ("ID Type") to specific user IDs and passwords. You assign the role to a session when you create it. A role can be set during the creation of the session file. Users will be prompted once for their credentials when they start that session. All subsequent sessions (using the same role "ID Type") opened or reconnected will be logged in automatically. Credentials are stored (encrypted) in RAM while the OutsideView instance is running and getting purged upon OutsideView termination.

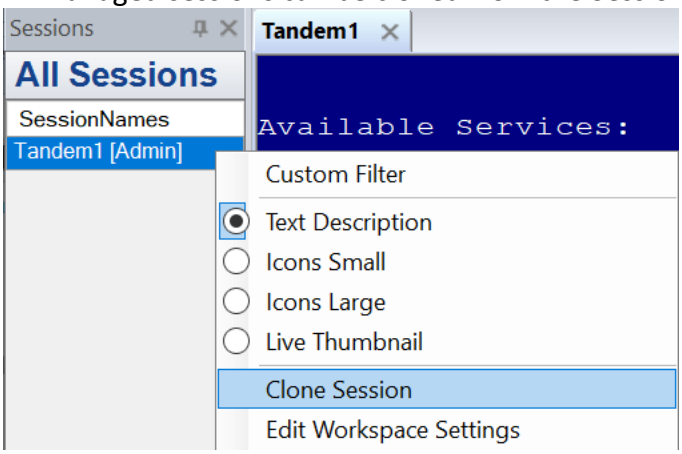
When setting session properties, select the same ID Type for all sessions where you want the same credentials. (For instance, assume you have three hosts but use the same login for all. You would create three session files, each with a different host address but all with the same ID Type.



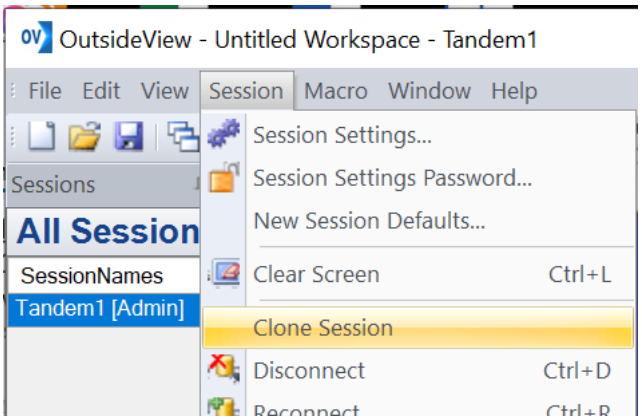
When the first session of a given ID Type starts, the user is prompted for their credentials:



These credentials are then stored (encrypted) in RAM. Whenever a session with this ID type is opened or (optionally) reconnected, OutsideView will automatically login to that session using the stored credentials.
ID Managed sessions can be cloned from the Session Bar right-click or Session menu.



or



Need help configuring OutsideView? Contact: support@crystalpoint.com