ACP ThinManager Tech Notes

# Active Directory and TermSecure

Use the **F1** button on any page of a ThinManager wizard to launch Help for that page.

Visit www.thinmanager.com/technotes/ to download the manual, manual chapters, or the ThinManual.

TermSecure is an additional layer of security provided by ThinManager. It can either hide applications from un-authorized users, called **SecureAccess**, or it can grant access to a user's personal applications at any location, called **SmartContext**.

Administrators want to tie the TermSecure account to Active Directory and have a single place to manage passwords. This Tech Note will show how to do this when using the SmartContext method of TermSecure to provide access to an application from any terminal in the system.

☐ Launch the **TermSecure User Terminal Configuration Wizard** by right clicking on the **TermSecure Users** branch in the ThinManager tree and selecting *Add TermSecure User*.
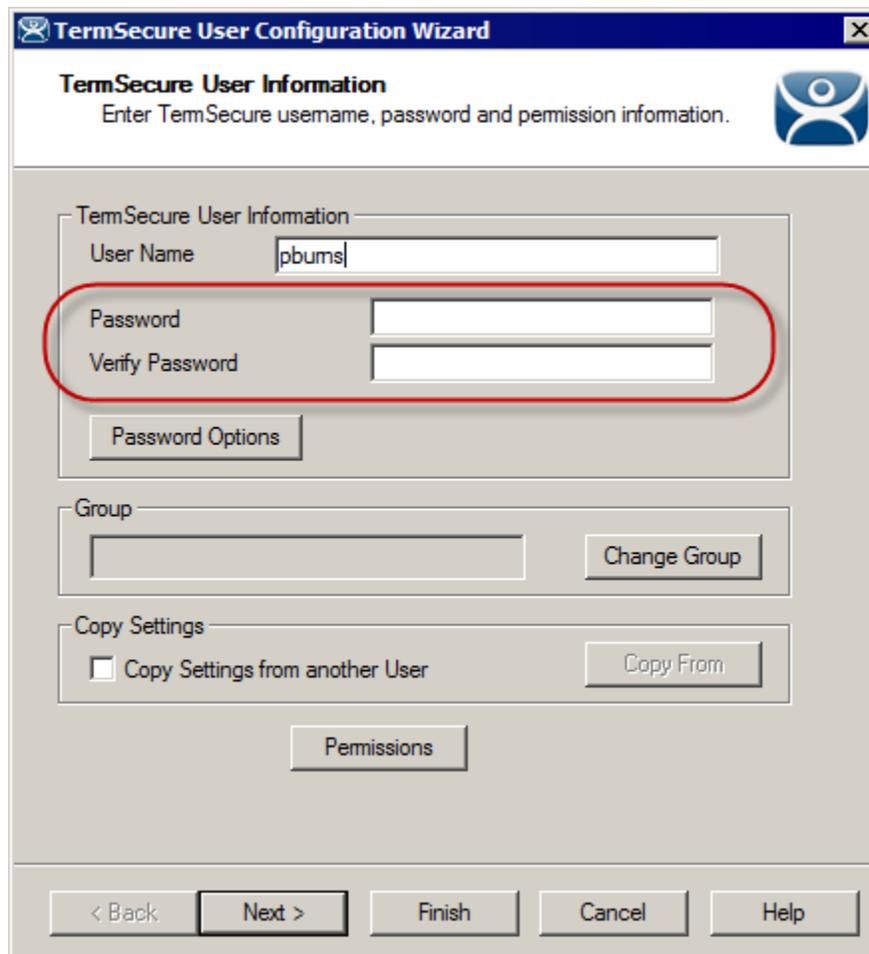
TermSecure User Terminal Configuration Wizard

☐ Enter the **Windows User** account in the *User Name* field on the **TermSecure User Information** page.

☐ Leave the *Password* field blank. This is a key component.
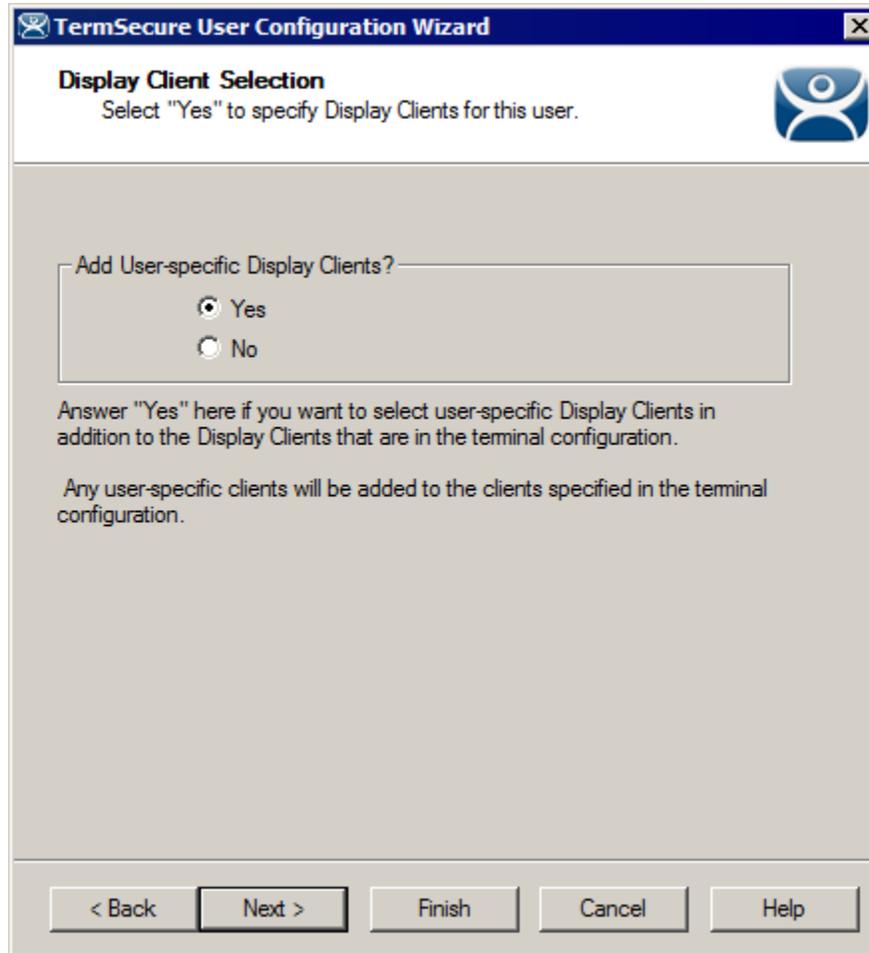
Display Client Selection Page

☐ Select **Yes** for the **Add User-specific Display Clients?** radio button on the Display Client Selection page of the **TermSecure User Configuration Wizard** .

This will give then the ability to have access to a user-specific application from any terminal.

Note: If you select **No** then the user will only be able to unlock applications hidden on the terminal using TermSecure Permissions with SecureAccess. Since this uses the terminal's login account and not the user's account it doesn't require user-specific Active Directory access.
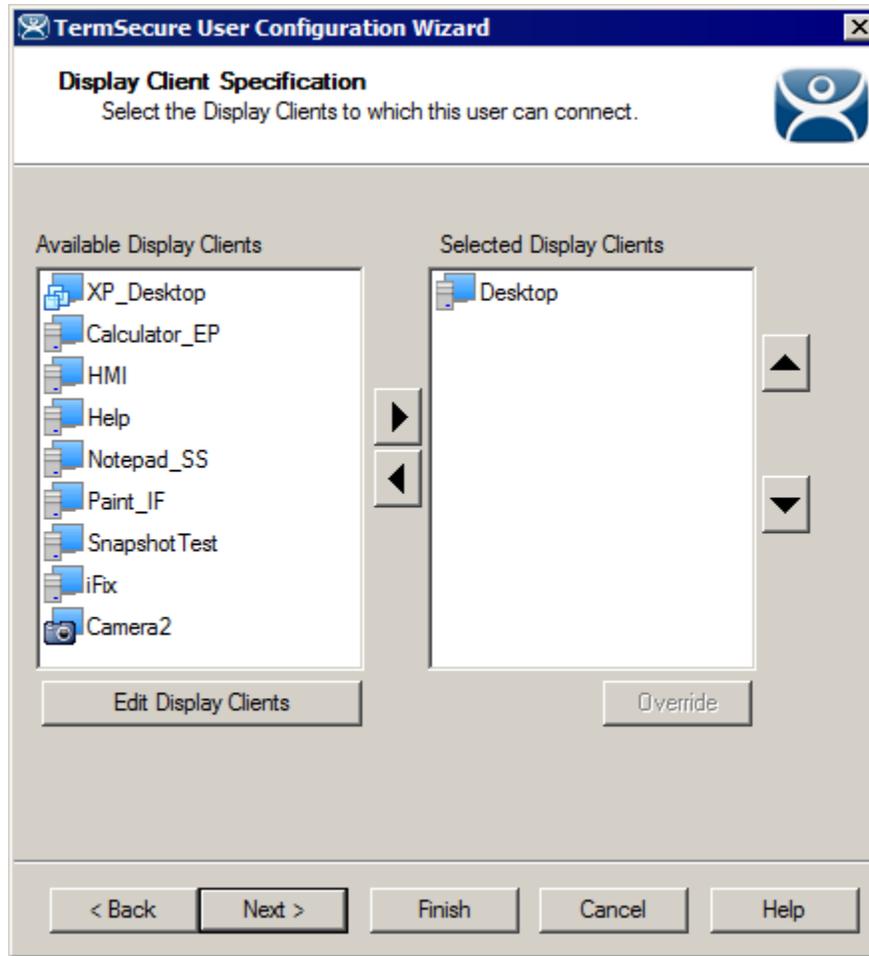
Display Client Specification Page

☐ Add the desired display client(s) to the TermSecure user on the **Display Client Specification** page of the **TermSecure User Configuration Wizard**.

Windows Log In Information Page

☐ Select the *Same as TermSecure User username/password* checkbox on the **Windows Log In Information** page of the **TermSecure User Configuration Wizard**.

☐ Enter the domain in the *Domain* field, if needed.

This will let the TermSecure user use their Windows account to access applications through TermSecure.

On the Terminal

TermSecure Main Menu on the Terminal

☐ Open the TermSecure menu, either with the Group Selector drop-down or the *CTL+m* hotkey.

☐ Select the *Log In* button on the **Main Menu**.

TermSecure Log On at the Terminal

☐ Enter your **Windows account/TermSecure** account in the **TermSecure Log In** window.

☐ Select the *OK* button.

Note: The terminal can be configured to display a virtual keyboard on the screen.

Open the Terminal Configuration Wizard, navigate to the **Terminal Interface Options** page of the **Terminal Configuration Wizard,** and launch the **Main Menu Options** window by selecting the *Main Menu Options* button.

Select the *Show Virtual Keyboard* checkbox on the **Main Menu Options** window and select *OK* to finish.

Password Request on the TermSecure Log On at the Terminal

☐ Enter your password and select the **OK** button to login and open the session.

ThinManager will pass the password to the proper terminal server when you enter the password into the field and select the **OK** button. This server will authenticate against Active Directory and log you into the session.

This password isn't stored by ThinManager but is encrypted and passed to the servers. The password is kept in the Active Directory and in the user's memory. If they forget the password then the administrator would have to reset it in Active Directory.

If the Active Directory requires the periodic changing of the password, the user only has to change it in one place, the Active Directory, since ThinManager isn't storing it.

Note: This works with HID cards and the card readers. Once the user swipes their card they will be prompted to enter their Windows account password. This adds additional security because a stolen card won't function without the password.