Some Help With

Screen Privacy

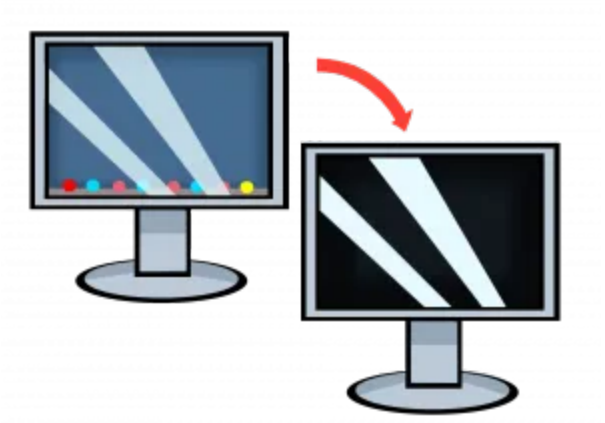
TABLE OF CONTENT

- Compatibility
- Exceptions
- Multiple sessions
- Use Case
- Known Issues

“Screen Privacy” or Privacy Mode is a feature to hide the contents of a session by disabling the remote display.

While screen privacy or privacy mode is on, the screen contents are hidden from anyone with physical access to the remote device.

Furthermore, input and sound from the remote side are also blocked while privacy mode is enabled until either the session ends or privacy mode is disabled manually.



privacy-300x225

However, screen privacy will not hide actions from the operating system or any history on the local or remote device.

 © 2026 www.somehelpwith.com

For privacy mode to be enabled, it requires permission from the clients on both ends of the session.

First, the remote client needs to give the connecting user the ability to “Enable privacy mode”. See Permissions.

Once the remote client has given the connecting client the correct permissions, the connecting client can enable privacy mode within the session via “Permissions” in the AnyDesk toolbar.

If “Remember individual settings for each Desk” is enabled on the connecting AnyDesk client, enabling “Screen Privacy” will be remembered even after closing the session and will automatically be applied again the next time the AnyDesk client connects to the same device.

Additionally, the address bar will display the “Screen Privacy” status.

Back to Top

Compatibility

The screen privacy feature is available for **Windows 8.1+**, **macOS 10.13+,** and **Linux**.
Please also ensure that the graphics drivers are also up-to-date.

In the case of several graphics adapters, it is important to make sure AnyDesk is running on the same adapter as the main display as this can prevent privacy mode from starting.

Exceptions

Under certain circumstances, privacy mode may not work due to OS security architecture.
Thus, either input may not be blocked, the screen contents are not hidden, or both:

- During UAC dialog
- After sending Ctrl + Alt + Del
- After logout
- During user switch
- After the desktop has been locked

Note: Leaving those screens is supposed to restore Privacy Mode, thus the remote screen is hidden again and the remote user’s input be blocked.

A request to enter Privacy Mode may be rejected for various reasons:

- The remote client is not installed
- The remote client does not allow using Privacy Mode
- The remote client does not support Privacy Mode (Windows 7 or outdated client version).

- The remote client is not able to enter Privacy Mode due to missing privileges required by the operating system.
- The remote client is not able to enter Privacy Mode due to missing hardware support.
- The remote client has the same ID as the local client.

Multiple sessions

In case multiple users are connected to the same client and at least two of them request Privacy Mode:

1. Privacy Mode is entered on the first request (if possible),
2. Privacy Mode should be left either in case
   a. the last user that requested Privacy Mode requested to leave it.
   b. the last user that requested Privacy Mode closed the corresponding session.

Use Case

Home Office

Working from Home on confidential or customer-related documents?

With Screen Privacy, no one in the Office can see what you are working on and cannot interfere as local input and audio is disabled.

Known Issues

On Windows 8 and 10 Privacy Mode may be disabled if the local connecting user switches to a monitor with a rotated screen on the remote device being controlled.

It is restored, when switching to a non-rotated monitor.