



Tectia[®] PrivX Desktop 7.1

Quick Start Guide

18 September 2026

Tectia® PrivX Desktop 7.1: Quick Start Guide

18 September 2026

Copyright © 1995–2026 SSH Communications Security Corporation

This software and documentation are protected by international copyright laws and treaties. All rights reserved.

ssh® and Tectia® are registered trademarks of SSH Communications Security Corporation in the United States and in certain other jurisdictions.

SSH and Tectia logos and names of products and services are trademarks of SSH Communications Security Corporation. Logos and names of products may be registered in certain jurisdictions.

All other names and marks are property of their respective owners.

No part of this publication may be reproduced, published, stored in an electronic database, or transmitted, in any form or by any means, electronic, mechanical, recording, or otherwise, for any purpose, without the prior written permission of SSH Communications Security Corporation.

THERE IS NO WARRANTY OF ANY KIND FOR THE ACCURACY, RELIABILITY OR USEFULNESS OF THIS INFORMATION EXCEPT AS REQUIRED BY APPLICABLE LAW OR EXPRESSLY AGREED IN WRITING.

For Open Source Software acknowledgements, see appendix *Open Source Software License Acknowledgements* in the *User Manual*.

SSH Communications Security Corporation
Karvaamokuja 2D, FI-00380 Helsinki, Finland

Table of Contents

1. Overview	5
2. Launching the Application	7
3. Usage	9
3.1. Connecting to Hosts	9
3.2. Connection Profiles	11
4. PrivX Authentication	13
5. Summary	15

Chapter 1 Overview

PrivX Desktop provides a secure SSH-based environment for connecting to remote systems, transferring files, and managing privileged access.

Chapter 2 Launching the Application

You can open PrivX Desktop as follows:

- Windows: via the Start menu.
- MacOS: via Applications, Launchpad, or Spotlight.
- Linux: via Applications or desktop launcher.



Note

On Linux, you will need to have the following libraries installed before you can launch PrivX Desktop.

- On Ubuntu/SUSE/Debian: `libxcb-cursor0`
- On RHEL/Rocky: `xcb-util-wm`, `xcb-util-keysyms`, and `xcb-util-cursor` (You need to enable the EPEL repository to obtain all the packages.)

Chapter 3 Usage

PrivX Desktop functionality is split under the following tabs:

View	Description
New Connection	Create new connections via Quick Connect . Connect to hosts defined in saved Profiles or Recent Connections .
SFTP (File Transfer)	Securely transfer files to and from remote hosts.
Terminal	CLI for securely performing commands on remote hosts.

3.1 Connecting to Hosts

To make your first SSH connection, provide the remote-host address and user name in **New Connection**→**Quick Connect**. If the SSH server on the remote host is on a port other than 22, also provide that port.

The screenshot shows the 'New Connection' dialog box with the 'Quick Connect' tab selected. The dialog has a dark blue header with a close button (x) and a plus sign (+). Below the header are three tabs: 'Quick Connect' (selected), 'Profiles', and 'Recent Connections'. The main area contains the following fields and options:

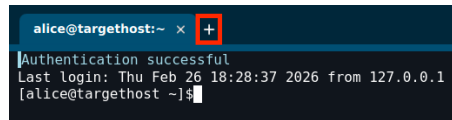
- Host**: A text input field containing 'targethost.example.com'.
- Port**: A text input field containing '22'.
- User**: A text input field containing 'alice'.
- Authentication method**: A dropdown menu showing 'Default Settings'.
- ☐ Exclusive connection
- Start with:**
 - ☒ Terminal
 - ☐ File Transfer

At the bottom right of the dialog is a blue 'Connect' button.

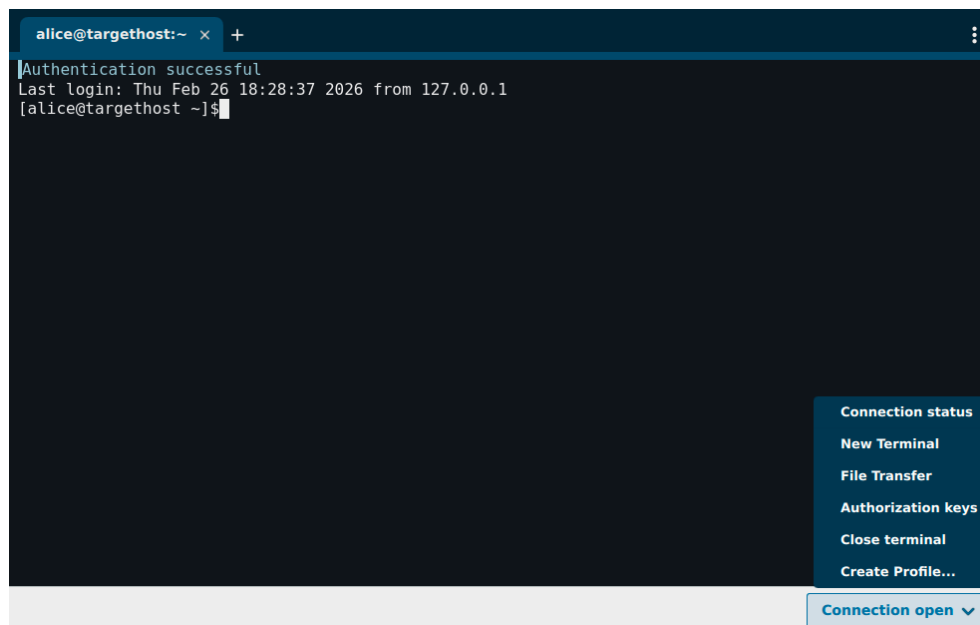
You can choose to **Start with:**

- **Terminal** - Lets you perform command-line actions on the remote host.
- **File Transfer** - Lets you drag and drop files to and from the remote host.

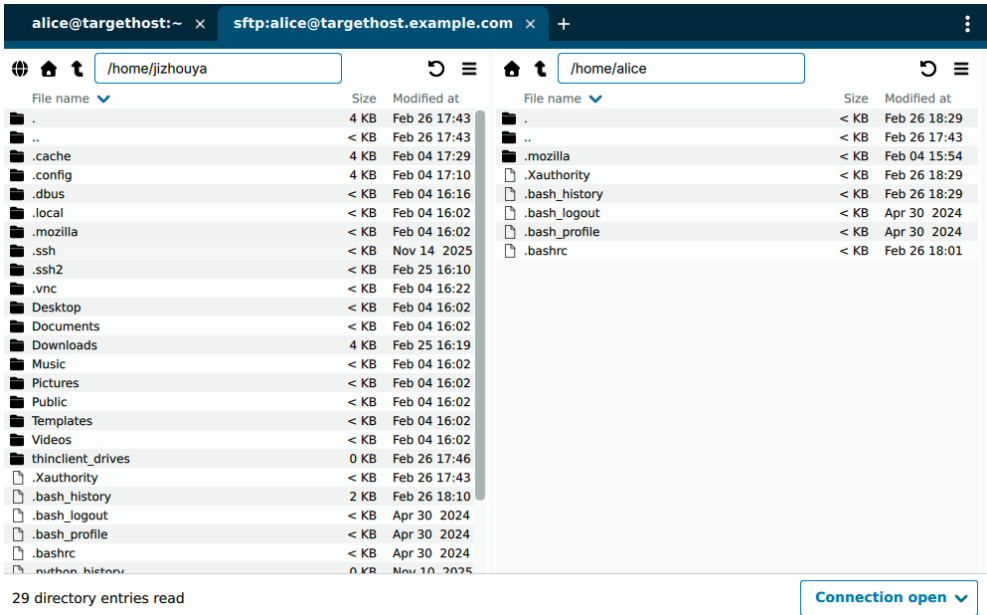
You can have multiple connections open simultaneously. To open additional connections, click + next to your existing connection tabs.



After you have an open connection to a host, you can open additional views to the same host via the **Connection Menu** at the bottom right.



For example, by clicking **File Transfer**, you will open a file-transfer view to the same user and target host.



3.2 Connection Profiles

To simplify repeat connections to a host, you can save its connection information to a profile. There's a few ways to create a profile:

- If you already have an open connection to the host, you can open the **Connection Menu** and select **Create Profile**.
- You can add profiles via settings. To do this, click **#** and select **Configuration**. Go to **Connection Profiles** to add a new profile.

To connect with an existing profile, go to **New Connection** (click **+**), select **Profiles**, then click the profile you want to connect with.

Chapter 4 PrivX Authentication

PrivX Desktop can be seamlessly used with PrivX privileged-access-management (PAM) solution to use ephemeral certificate authentication enabled with OIDC (OpenID Connect) browser-based user authentication to PrivX.

To enable Public-Key-PrivX authentication in PrivX Desktop GUI:

1. Define the PrivX Instance configuration. To do this, click # menu and select **Configuration**. Go to **User Authentication**→**PrivX Instances** to add a new instance.

- **Name** - display name, for example **PAM**.
- **URL** - complete URL, for example **https://privx.example.com** of the PrivX PAM of your company.
- **CA Certificate (optional)** - path to the trusted Certification Authority certificate file in PEM format including any issuing Certificate Authority Certificate chain if the PrivX Instance's TLS server certificate cannot be successfully validated with trusted CA Certificate(s) in the Operating System's certificate store.



Note

If the PrivX Instance's TLS Server certificate has been enrolled from your internal company CA, it is recommended to add the CA certificate(s) to the Operating System trust store so that both PrivX Desktop and the Operating System default browser can successfully validate it without additional configuration.

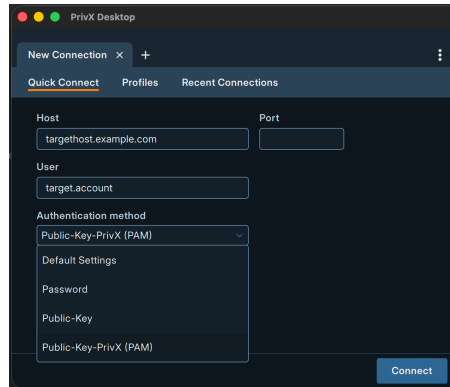
2. To verify the TLS settings and PrivX API connection, select the PrivX Instance and click **Test connectivity...** On Windows, the connection may be blocked by the Windows firewall and it has to be allowed for the PrivX authentication to work.
3. Click **Apply** to take the configuration into use.



Note

Public-Key-PrivX authentication can be configured as the preferred user authentication method by default in **General**→**Default Connection**→**Authentication**, in specific **Connection Profiles** or alternatively selected for a new connection in **Quick Connect**.

- Return to PrivX Desktop GUI. In **New Connection**→**Quick Connect**, the PrivX Instance **Public-Key-PrivX (PAM)** can now be selected as **Authentication method**.



- Connect to a remote-host that has been configured to trust the PrivX OpenSSH certificate-based authentication for the target account.
- PrivX Desktop connects directly to the target host. After the Secure Shell server has been authenticated, the server may send a banner message to accept. Once the user authentication phase begins, the default Operating System browser is launched to authenticate the PrivX user in a new tab.



Note

Typically, the PrivX user account identifies the real user and the target account is a shared role-based account.

- Once PrivX user authentication is successful, the PrivX Desktop automatically uses its ephemeral key to obtain a short-lived certificate that contains the user's roles from PrivX. This certificate is used to authenticate to the target account on the target server and it is discarded after use.



Note

If a new certificate is needed, the existing session to PrivX is used. PrivX user re-login is not needed as long as the PrivX user session is valid and the PrivX Desktop Connection Broker remains running.

Prerequisites on PrivX Instance:

- **PrivX user** a user account that maps to the intended PrivX role(s).
- **Use with PrivX agent** option enabled for the role(s) that grant access to the target(s).
- **connections-authorize** permission enabled for the role(s) that grant access to the target(s).

Chapter 5 Summary

PrivX Desktop enables secure, efficient SSH connections for both terminal and file transfer operations. By following this guide, you should now be able to establish connections to remote hosts, and transfer files to and from them.

For more detailed information, refer to:

- **Tectia Client User Manual** - for advanced configuration and troubleshooting details.
- **Tectia Server Admin Manual** - for server related, advanced configuration and troubleshooting details.
- **SSH Documentation** - <https://docs.ssh.com>