Cyber Protect Connect

1.2

User Guide

REVISION: 7/4/2024

Table of contents

Acronis Cyber Protect Connect 7
NEAR protocol 7
H.264 7
Adaptive Codec 7
Sound Transfer 8
Logon Methods 8
Multiuser Access on Mac 8
Unicode Input 8
Security 8
Cyber Protect Connect console 9
Cyber Protect Connect agent 9
Setting up remote access 10
Setting up remote access on macOS 10
Acquiring permissions for remote access on macOS 12
Screen Recording Permission 12
Accessibility Permission 13
Microphone Permission 14
Full Disk Access Permission 15
Change Your Mind 17
Setting up remote access on Windows 19
Enabling desktop sharing on Windows 21
Configuring permissions for remote access on macOS 10.14 Mojave 23
Microphone Permission 26
Acquiring Permissions for Remote Access on Mac with macOS 10.15 Catalina 27
SCREEN RECORDING PERMISSIONS 28
ACCESS PERMISSIONS 30
OTHER PERMISSIONS 31
Configuring permissions for remote access on macOS 10.14 Mojave 32
Microphone Permission 34
OTHER PERMISSIONS 34
Common tasks 35
Helping someone once 35
Sharing aremote computer with colleagues 36
Configuring remote sound 39
How to get remote sound from a Mac 39

How to get remote sound from a PC 39

How to get remote sound from a Linux 39

Changing the access code 39

Changing computer ID 41

Uninstalling Acronis Cyber Protect Connect agent 42

Cyber Protect Connect console 43

Cyber Protect Connect licensing 43

Working with licenses 43

Cyber Protect Connect console main features 44

Overview 44

Reports 45

Map 45

Chat 45

Screenshot 46

Account settings 46

Using Teams functionality 48

Team user roles 48

Logging in with Single sign-on 49

Working with Teams as an Admin user 49

Working with Teams as a User 57

Cyber Protect Connect Quick Assist 58

User account control on remote Windows workloads 59

Cyber Protect Connect agent for Mac 61

Main window 61

Your ID and Access Code 61

Computer Name 61

Trusted Users 62

AcronisCyber Protect Connect console 62

Remote Connections 62

Status Line 62

Trusted users 63

Cyber Protect Connect console 63

Remote connections 64

Settings 64

Cyber Protect Connect agent for Windows 65

Main window 65

Your ID and Access Code 65

Computer Name 66
Trusted Users 66
AcronisCyber Protect Connect console 66
Remote Connections 66
Status Line 66
Trusted users 67
Cyber Protect Connect console 67
Remote connections 68
Settings 68
Cyber Protect Connect agent for Linux 69
Cyber Protect Connect agent for Linux 69
How to install Acronis Cyber Protect Connect agent on Linux 69
Installing from a repository 69
Installing from a package 69
Checking dependencies on Linux 71
Video codec 71
Audio codec 71
Connecting to a headless Linux 71
Cyber Protect Connect client 73
Cyber Protect Connect client user interface 74
Main window reference 74
Viewer window reference 77
Cyber Protect Connect client menu in the system menu 82
Preferences window reference 83
Multi-viewer window reference 85
Protect confidential data with master password 87
Player window reference 88
Cyber Protect Connect Cloud 90
Connecting via Acronis Cloud 90
Connecting via Cyber Protect Connect account 91
Using Cyber Protect Connect Quick Assist in Acronis Cloud 91
Connecting to remote computers 91
Creating a connection 91
Using common credentials 92
Finding remote computers 95
Managing stored server lists 97
Observeing multiple servers 98

About URL syntax and *.vncloc files 100
Optimizing image transmission for Retina displays 103
Security 103
Interacting with remote computers 108
Connecting to remote workloads using Acronis Cyber Protect Connect Quick Assist 108
Controlling or observing a single computer 108
Viewing the remote desktop 110
Adjusting quality for slow connections 111
Enabling automatic reconnect to the remote computer 112
Displaying connection info panel 112
Screen sharing virtual displays 114
Screen sharing server scaling 115
Sharing clipboards between the remote and local computers 115
Transferring data between the remote and local computers in Screen Sharing mode 116
Transferring data between client and server in NEAR connection mode using the clipboard 117
RDP performance options, file, sound and printer sharing 117
Capturing a remote desktop screen to a file 119
Recording sessions 119
Setting up a server for remote access 120
Install VNC, RDP or Screen Sharing server 120
Make a server accessible 123
Enable SSH on Mac 126
Perform silent installation 126
HTTP API for Cyber Protect Connect client 127
Working with groups: 127
Working with connections: 128
Working with cloud computers: 129
Actions 130
Cyber Protect Connect client for iOS 131
Cyber Protect Connect client overview 131
Introduction 131
Main Screen 132
Computer settings 136
Common settings 136
Connection settings 136
Supported servers and authentication modes 141
NEAR 141

VNC servers 141

RDP servers 141

How to set up a computer you are connecting to 142

NEAR 142

VNC 142

RDP 142

Make your computer accessible outside the local network 144

Connection 145

Viewer 145

External Keyboard 149

Tips and Tricks (ScreenSharing) 149

File Transfer 150

Cyber Protect Connect client for Android 151

Cyber Protect Connect client overview 151

Introduction 151

Main Screen 152

Computer Settings 156

Common settings 156

Connection settings 157

Supported servers and authentication modes 161

NEAR 161

VNC servers 161

RDP servers 161

How to set up a computer you are connecting to 162

NEAR 162

VNC 162

RDP 162

Make your computer accessible outside the local network 164

Connection 165

Viewer 165

External Keyboard 169

Tips and Tricks (ScreenSharing) 169

File Transfer 169

Index 170

Acronis Cyber Protect Connect

Acronis Cyber Protect Connect is easy to use and convenient for users who need to manage remote computers.

To get started

1. Create an account for the Acronis Cyber Protect Connect console.
2. On the **remote computer**:
   a. Download and install Acronis Cyber Protect Connect agent.
   b. Once installed, open Trusted Users list in Acronis Cyber Protect Connect agent and add your Cyber Protect Connect account as a trusted one.
   c. If the remote computer is running macOS, grant all required permissions to the Agent for it to allow remote control.
3. On your **local computer**:
   a. Download and install the Acronis Cyber Protect Connect client.
   b. Log in to the Acronis Cyber Protect Connect client with your Acronis Cyber Protect Connect account.
   c. Open the **All Computers** section.

Now the remote computer is listed there and is available for connecting. To start a remote control session, double-click it.

NEAR protocol

NEAR is an Acronis proprietary low-latency remote desktop protocol. It features:

H.264

NEAR implements three quality modes: smooth, balanced and sharp. In "smooth" mode it uses hardware H.264 on macOS and Windows to encode your desktop picture and falling back to software encoder if hardware encoder is not available. The picture size is currently limited to Full HD resolution (1920x1080).

Adaptive Codec

In "balanced" and "sharp" quality modes, NEAR uses Nulana Adaptive codec, which provides full picture quality in 32 bit, compared to "video" mode used by H.264. In "balanced" mode, picture quality is automatically adjusted according to your current network conditions and retaining current framerate. In "sharp" mode, you always get the full quality picture, but probably with reduced FPS, if your network or processor/video card are overloaded.

Adaptive Codec is using OpenCL on macOS and Windows if it is available in your graphics drivers.

Sound Transfer

NEAR is capable of capturing the remote computer sound and transfer that to host. On Windows, this works out of the box. On macOS, you must install sound capture driver (SoundFlower or Blackhole) on the computers to which you will be connecting.

Logon Methods

You can use the following ways to log on to the remote computer:

- **Access Code:** this is similar to the VNC password. The code can be configured in Acronis Cyber Protect Connect agent. This way always connects you to the console session of the currently logged in user.
- **System Logon:** use your Windows or macOS credentials to authenticate. On Windows, you always connect to the console session of the current user or logon window. On macOS, separate session is created for each different user.
- **Ask for observe/ask for control:** user on the console will be asked to allow or deny your connection.
- **No authentication:** if you are listed among the trusted users, and Acronis Cyber Protect Connect agent is configured to allow trusted users to log in without credentials. You always connect to the console session.

Multiuser Access on Mac

With NEAR, you can use your Mac as a terminal server. When you log in to macOS with System Logon authentication type, NEAR can log you into a separate session for each user credentials. This functionality works quite similar to Apple Screen Sharing. However, this requires a user to be logged in previously. To create new sessions remotely, open the macOS Login Window and enter new user's credentials manually.

To secure your operations from the remote user, you can use Screen Lock/Curtain Mode to lock the screen.

Note: if you are logged to a separate off-console session, the sound transfer will not work.

Unicode Input

For mobile clients where hardware keyboard is typically unavailable, NEAR provides a complete Unicode input. That means, there are no more hassles with matching the keyboards on mobile and host computer. Just type using your mobile keyboard and it will just work.

Security

Your data is always two-way encrypted with AES encryption in NEAR.

Cyber Protect Connect console

The Acronis Cyber Protect Connect console is a centralized web-based solution to monitor and manage multiple computers. You can use it within your organization or help your clients across different locations. From the console, you can:

- Get an overview on the remote computer: online status, currently logged in user, the Agent version, and status of remote control services.
- Obtain a full computer hardware report on memory, storage, network, graphics, USB & printer devices.
- View the list of issues with the machine, like a dying battery, failing HDD, or an outdated operating system.
  You can also set the console to send you daily notifications about these issues.
- Perform actions like logging out, putting the computer to sleep, restarting or shutting down, and emptying trash for all users at once.
- See the computer location on the map.
- Chat with the user of the computer.
- Start a remote control session.

Cyber Protect Connect agent

Acronis Cyber Protect Connect agent is a free lightweight application that serves two purposes.

First, it helps to establish a secure connection between the Acronis Cyber Protect Connect client and the remote computer, so you do not have to adjust any NAT, router, or firewall settings. Second, it aids with the Cyber Protect Connect console functionality.

With Cyber Protect Connect agent installed, you can:

- Receive outside remote desktop connections.
- Provide an outside access with an access code or by authorizing a Cyber Protect Connect Cloud user.
- Keep an eye on security of incoming connections by managing an access code.
- Send reports, screenshots and location info to the Cyber Protect Connect console.
- Allow remote executing of shell commands and performing administrator actions.
- Chat with other users connected to your Cyber Protect Connect Cloud.

In order to get access to a computer over the Cyber Protect Connect Cloud, you need a purchased copy of the Cyber Protect Connect client on your device. The Cyber Protect Connect client is currently available for Windows, macOS, iOS, and Android.

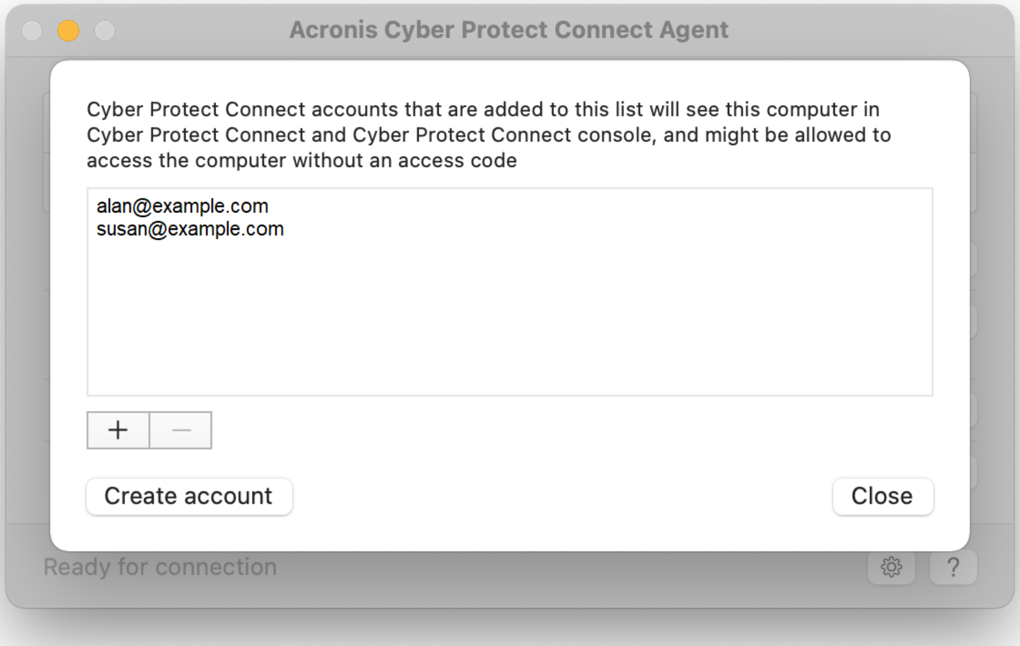
Setting up remote access

This section provides comprehensive instructions for configuring remote access to your devices, allowing you to control them from anywhere.

Setting up remote access on macOS

To establish a connection over Acronis Cyber Protect Connect Cloud, you must install Acronis Cyber Protect Connect agent on your Mac.

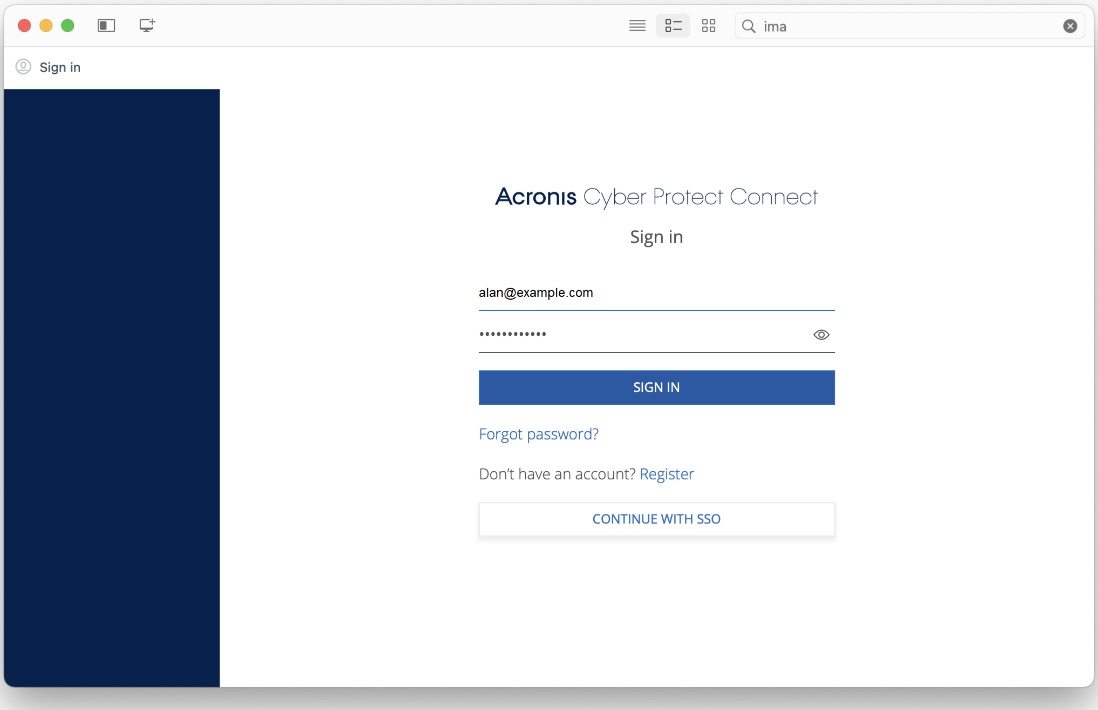
1. Download and install Acronis Cyber Protect Connect Agent for Mac on the Mac you want to connect.
2. Create a account for the Acronis Cyber Protect Connect console, if you do not have one yet.
3. Start the Agent. To allow controlling your Mac remotely, go to **System Preferences > Security & Privacy > Privacy > Accessibility** and let Cyber Protect Connect agent access your computer.
   – If your Mac is running macOS 10.14 Mojave, you will be asked for additional permissions for Cyber Protect Connect agent to work. For more information, see Controlling a Mac running Mojave.
   – If your Mac is running macOS 10.15 Catalina or later, you will be asked for more additional permissions for Cyber Protect Connect agent to work. For more information, see Acquire permissions to control a Mac.
4. In Cyber Protect Connect agent, go to the **Users** section and add your Cyber Protect Connect Cloud account to the **Trusted Users** list.

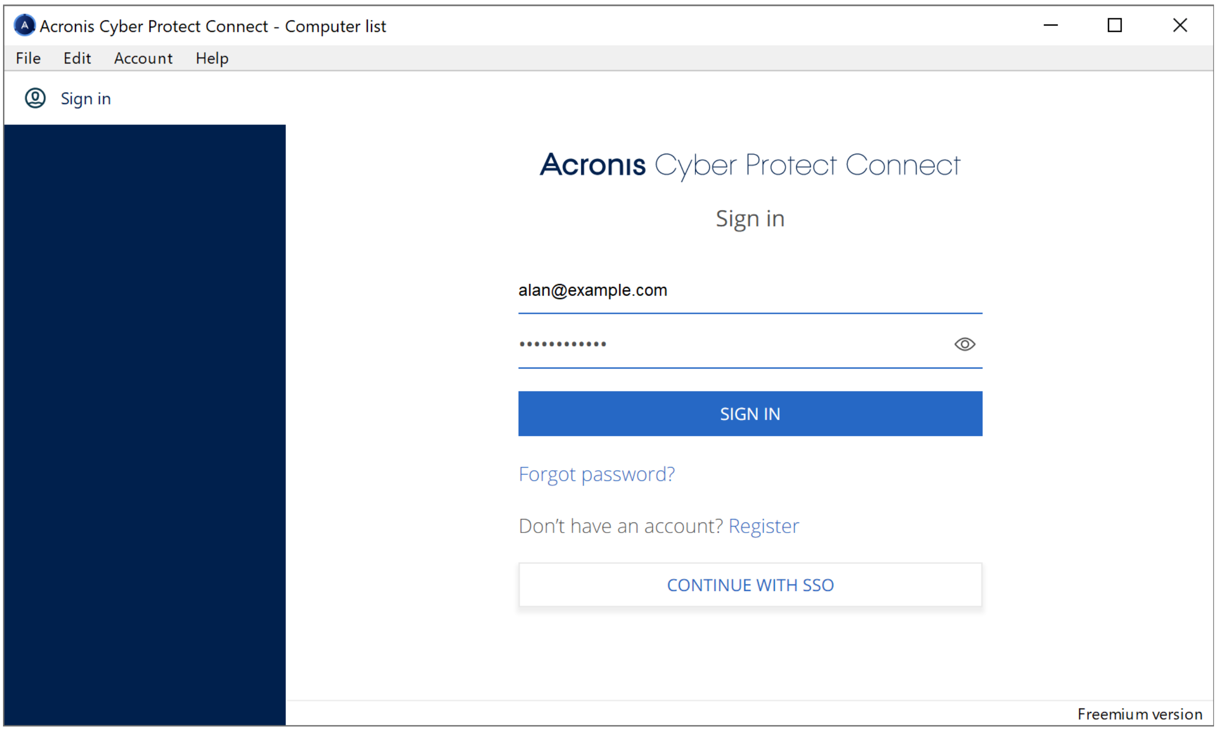


Cyber Protect Connect accounts that are added to this list will see this computer in Cyber Protect Connect and Cyber Protect Connect console, and might be allowed to access the computer without an access code

alan@example.com
susan@example.com

5. Open the Acronis Cyber Protect Connect client and log in with your Acronis Cyber Protect Connect Cloud account.





You now have remote access to a computer with a macOS.

Acquiring permissions for remote access on macOS

Starting with 10.15 Catalina, macOS requires all remote control providing applications like Acronis Cyber Protect Connect agent to have a whole variety of special rights to control the computer. Without this, you will not be able to view the remote computer's screen, to control it, and to access it in an unattended mode.

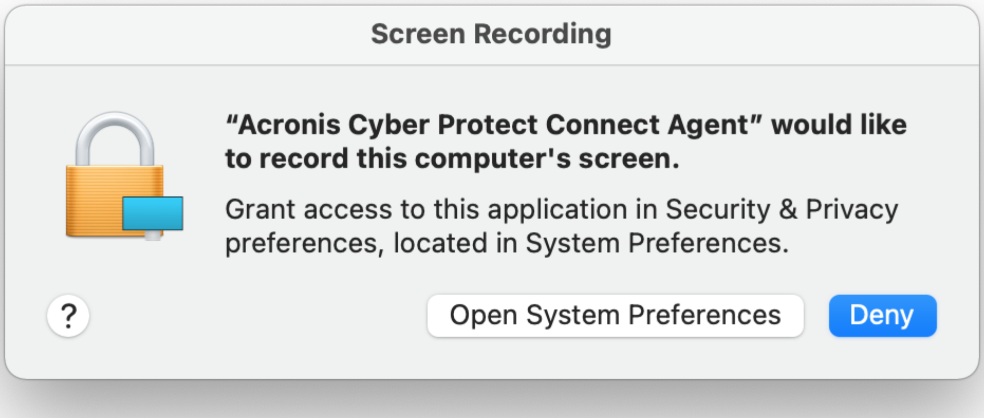
After you start Cyber Protect Connect agent on a Mac, it will check if it has these rights and will ask you to grant the permission, if needed.

If no dialog emerges when you click the buttons, you have most likely previously denied to give the permission, or ignored the dialog. For more information, see change your mind.

Screen Recording Permission

To make your Mac available to be observed remotely with NEAR

1. When asked for permissions, click **Request Screen Recording Permission**.
2. In the **Screen Recording** dialog window, click **Open System Preferences**.



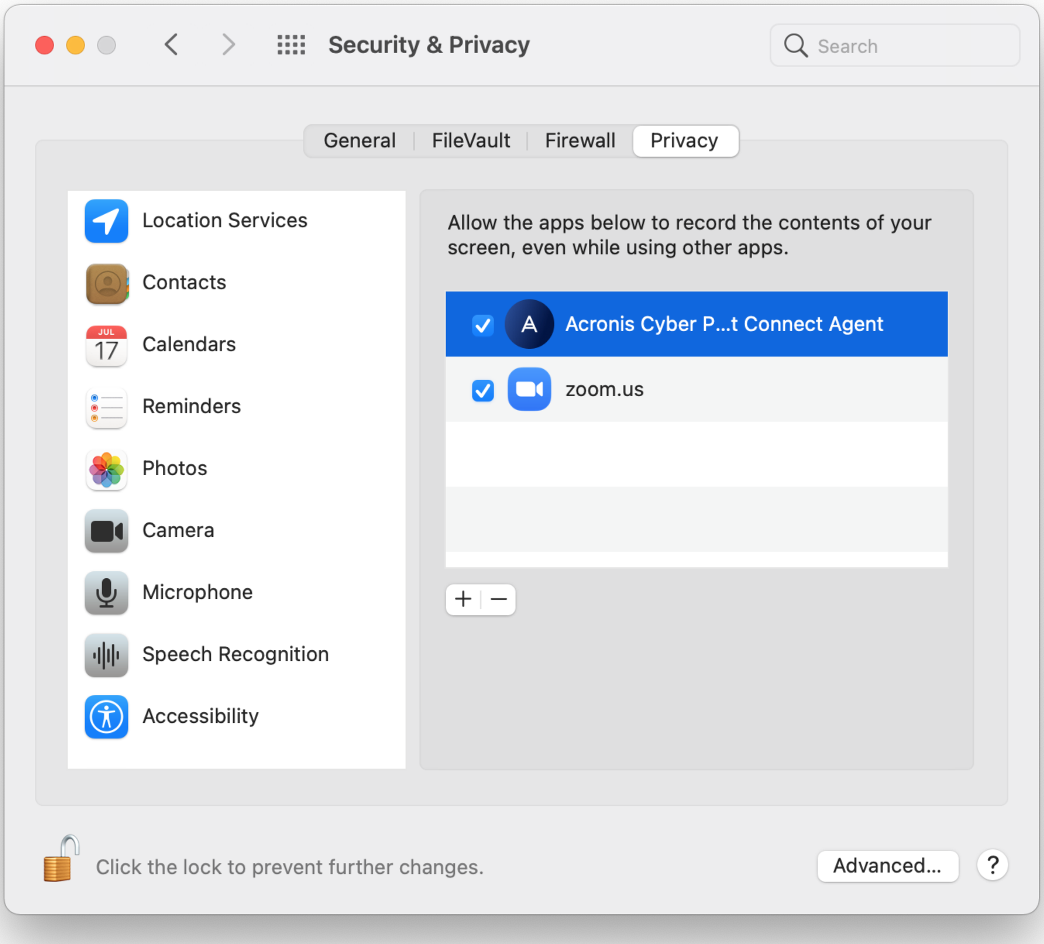
Screen Recording

“Acronis Cyber Protect Connect Agent” would like to record this computer's screen.

Grant access to this application in Security & Privacy preferences, located in System Preferences.

This will open **Security & Privacy > Privacy > Screen Recording** in the **System Preferences** app.

4. Select Acronis Cyber Protect Connect agent to give it access.



Allow the apps below to record the contents of your screen, even while using other apps.

☑ Acronis Cyber P...t Connect Agent

☑ zoom.us

Click the lock to prevent further changes.

Now your Mac's screen can be observed remotely.

If Cyber Protect Connect agent does not have the permission at the moment you try to access the Mac remotely, it will show the **Screen Recording** permission request dialog. Please note that these dialogs may be answered only by a local user. It will be impossible to click any buttons in the permission request dialog remotely.

Accessibility Permission

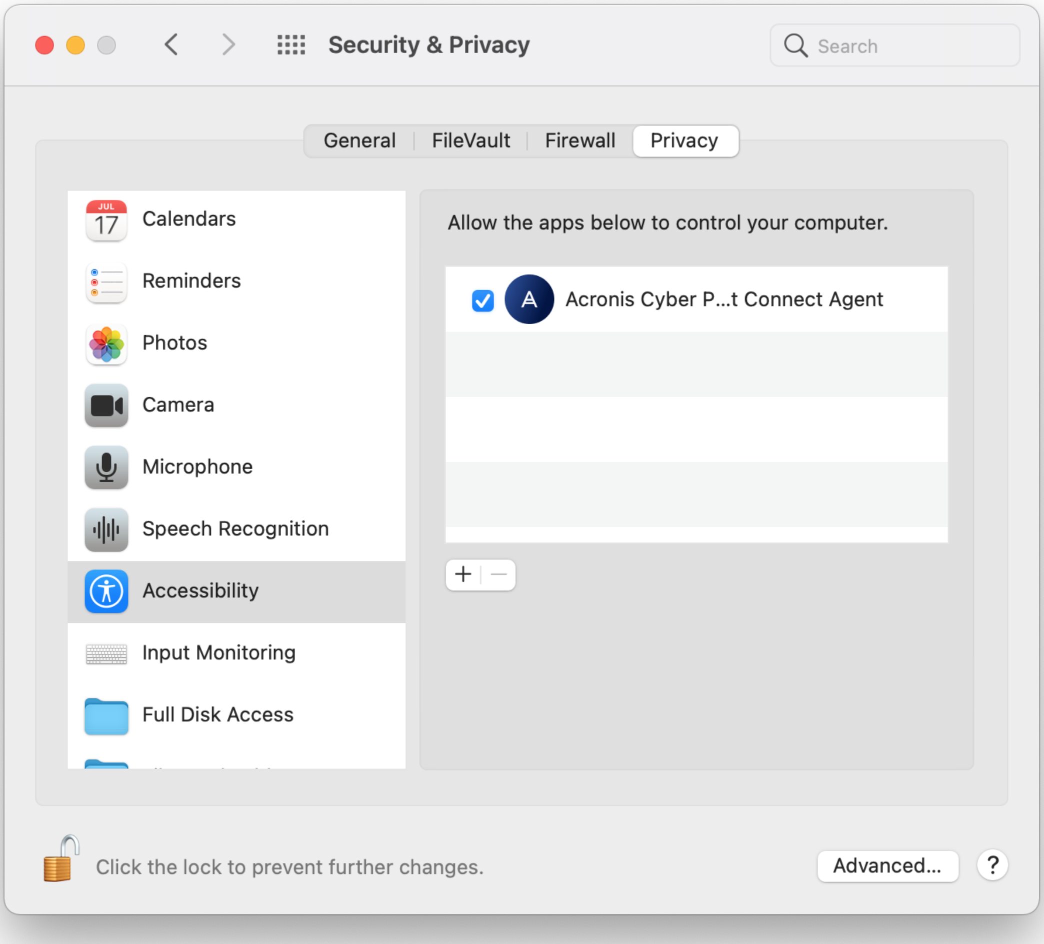
To make your Mac available to be observed and controlled remotely with NEAR

1. In an opened window, click **Request Accessibility Permission»**.
2. In the **Accessibility Access** dialog, click **Open System Preferences**.

This will open **Security & Privacy > Privacy > Accessibility** in the **System Preferences** app.

4. Click the Lock icon in the bottom-left corner of the window so that it changes to an unlocked one. The system will ask you for an administrator password to make changes.

5. Select Acronis Cyber Protect Connect agent.



Allow the apps below to control your computer.

☑ Acronis Cyber P...t Connect Agent

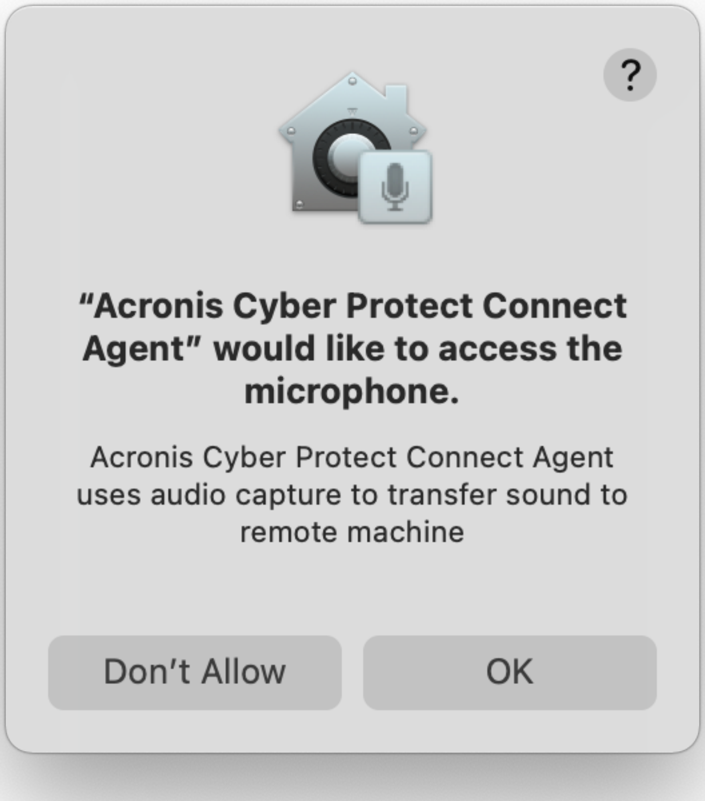
Click the lock to prevent further changes.

6. Now your Mac can be controlled remotely with NEAR.

Microphone Permission

To make your Mac able to redirect its sound to Acronis Cyber Protect Connect agent for NEAR connections

1. In an opened window, click **Request Microphone Permission**.
2. Click **OK** to give Acronis Cyber Protect Connect agent the required permission.



"Acronis Cyber Protect Connect Agent" would like to access the microphone.

Acronis Cyber Protect Connect Agent uses audio capture to transfer sound to remote machine

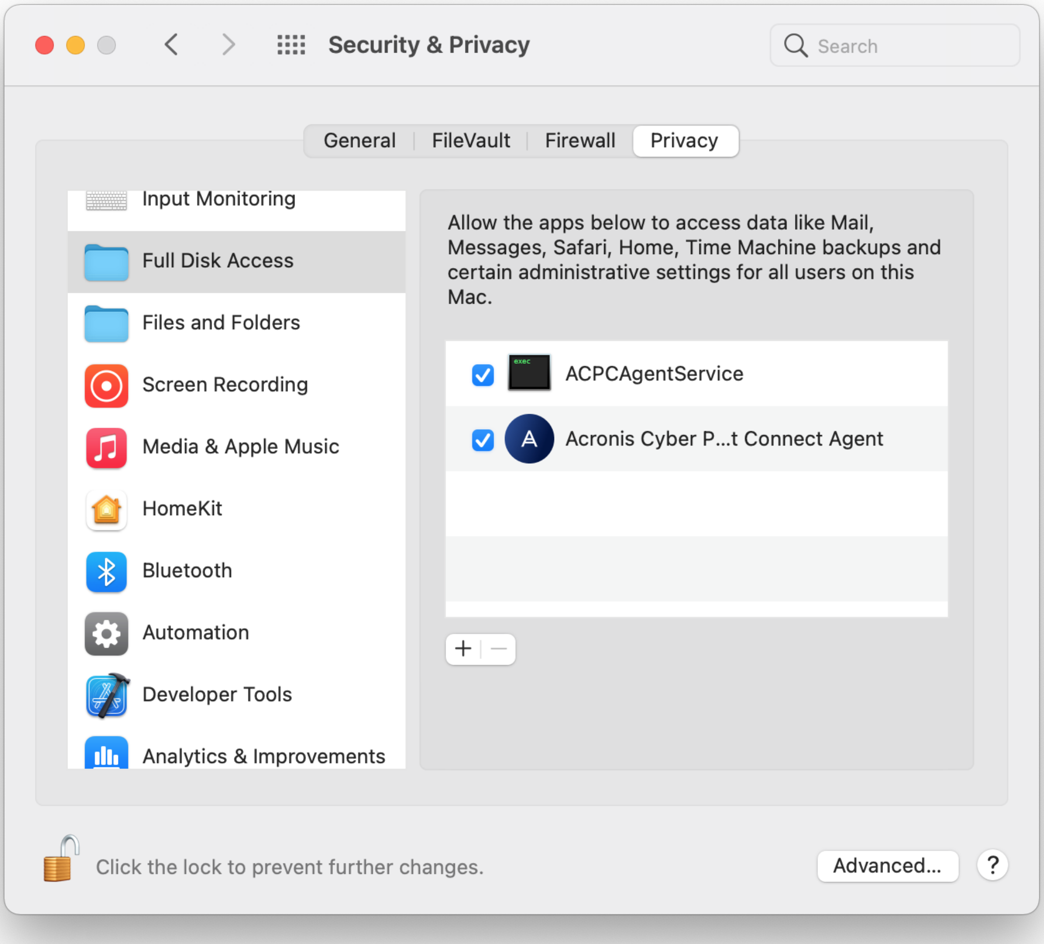
3. Now Cyber Protect Connect agent is added to the **Microphone** section in **Security & Privacy > Privacy** in **System Preferences** and it can capture the sound.
You must also install a sound capture driver on this Mac to let Cyber Protect Connect agent utilize the given permission and get the sound of your Mac redirected.

Full Disk Access Permission

Besides remote control capabilities, Cyber Protect Connect agent provides a File Transfer protocol.

If you want to be able to get all files from this Mac unattendendly, including files from users home folders and system ones

1. In an opened window, click **Full Disk Access**.
2. This will open **Security & Privacy > Privacy > Full Disk Access** in the **System Preferences** app.
3. Click the Lock icon in the bottom-left corner of the window so that it changes to an unlocked one. The system will ask you for an administrator password to make changes.
4. Select Acronis Cyber Protect Connect agent to give it access.



Allow the apps below to access data like Mail, Messages, Safari, Home, Time Machine backups and certain administrative settings for all users on this Mac.

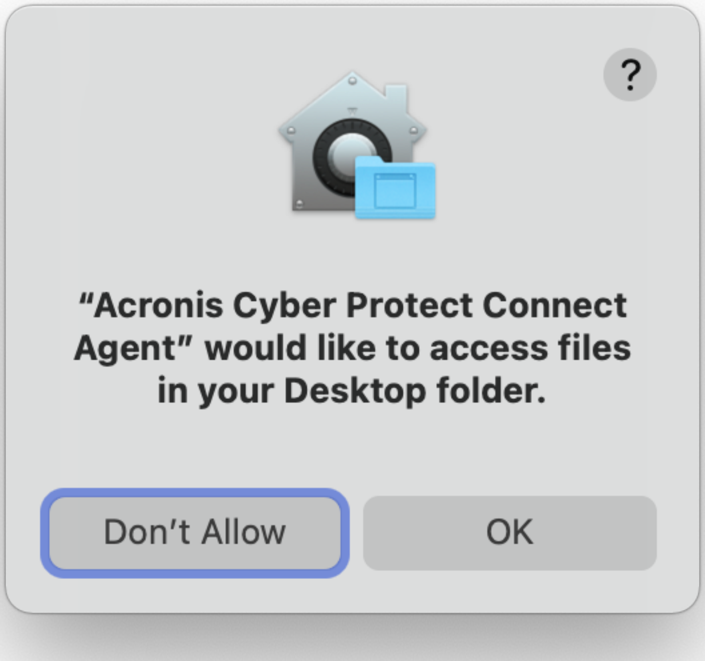
☑ ACPCAgentService

☑ Acronis Cyber P...t Connect Agent

Click the lock to prevent further changes.

5. If there is no Acronis Cyber Protect Connect agent application in the list, click **+** below to add it. By default, the app should be located in **\Applications\Acronis Cyber Protect Connect agent**.

Note that if you decide not to grant Full Disk Access to Acronis Cyber Protect Connect agent, any attempt to access user files remotely will halt until a local user accepts the file transfer request.

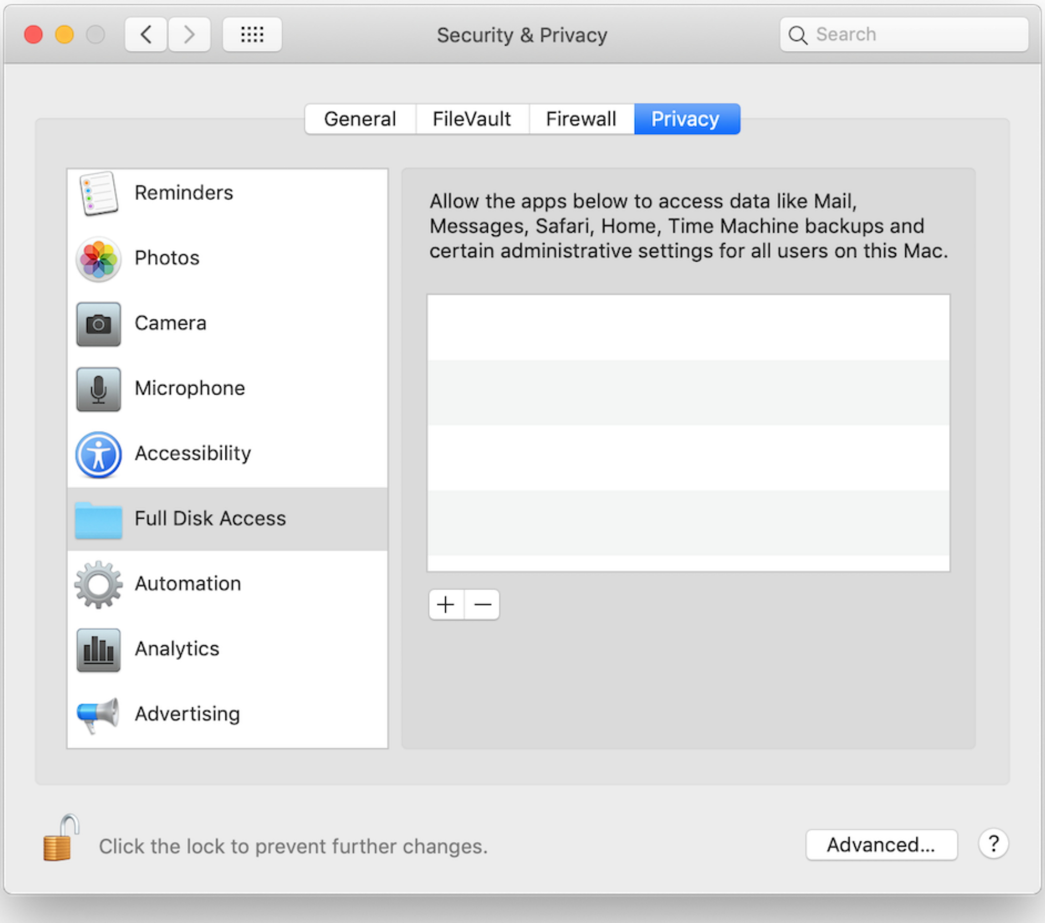


“Acronis Cyber Protect Connect Agent” would like to access files in your Desktop folder.

Change Your Mind

If you have previously denied to grant the permissions, macOS will not let Cyber Protect Connect agent ask you about it again. However, you can change this manually.

1. Open the right section of System Preferences:
   a. Open **System Preferences** app.
   b. Click the **Privacy** tab in **Security & Privacy** pane.



Allow the apps below to access data like Mail, Messages, Safari, Home, Time Machine backups and certain administrative settings for all users on this Mac.

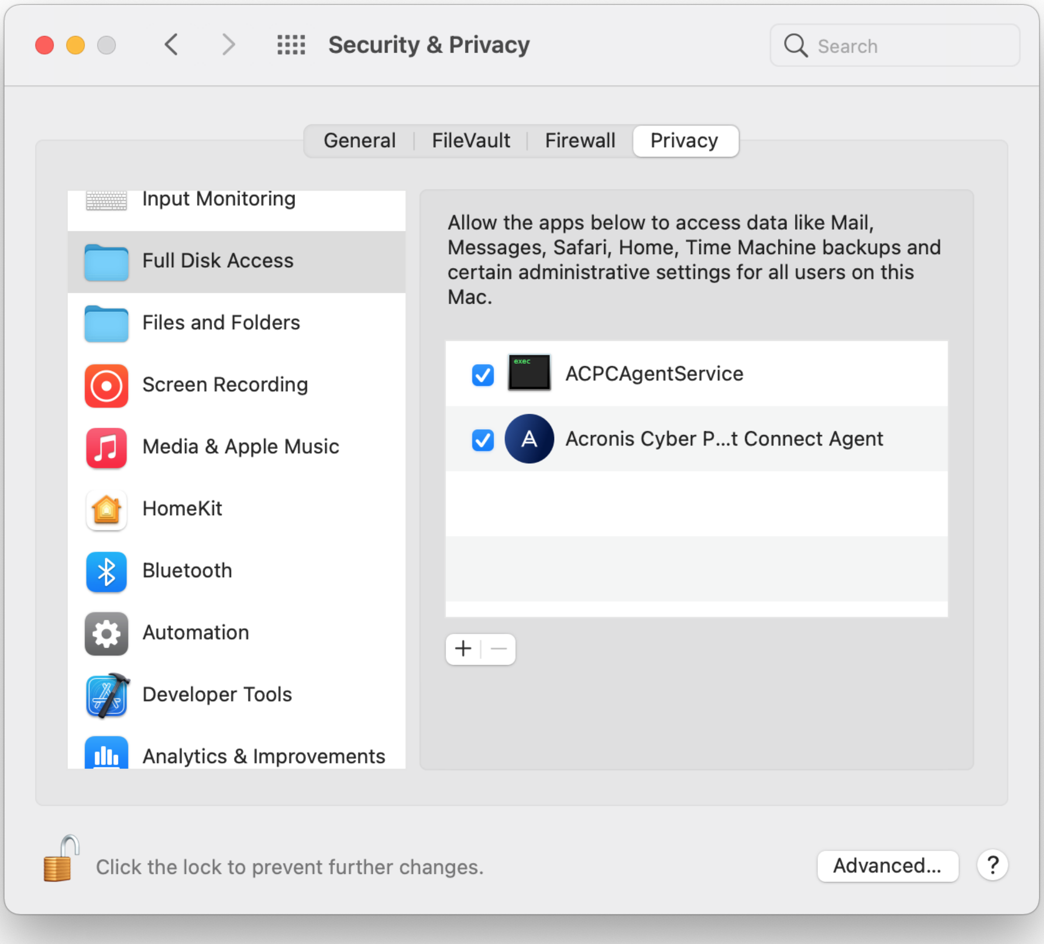
Click the lock to prevent further changes.

2. Select the corresponding section in the sidebar to the left:

- **Screen Recording** for remote screen access.
- **Accessibility** for remote control.
- **Microphone** for remote sound.
- **Full Disk Access** for file transfer.

3. Click the **Lock** icon in the bottom left corner of the window if needed to make changes.

4. Select Acronis Cyber Protect Connect agent to give it access.



Allow the apps below to access data like Mail, Messages, Safari, Home, Time Machine backups and certain administrative settings for all users on this Mac.

☑ ACPCAgentService

☑ Acronis Cyber P...t Connect Agent

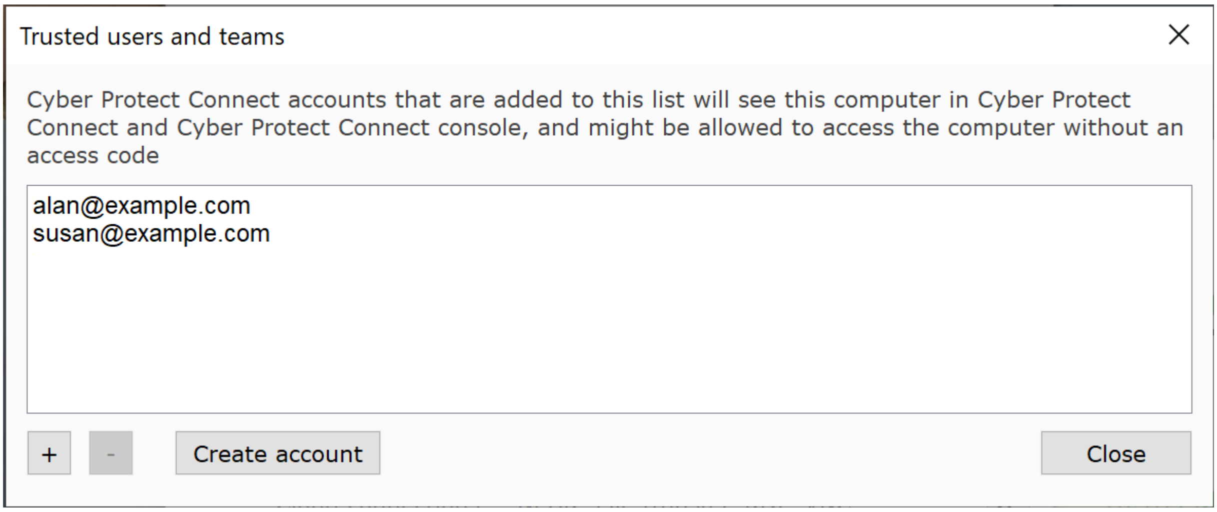
Click the lock to prevent further changes.

Setting up remote access on Windows

To make a computer be available to connect remotely, install Acronis Cyber Protect Connect agent and set up desktop sharing.

1. Download and install Acronis Cyber Protect Connect Agent for Windows.

   Your computer is now ready for NEAR connections. If you want to connect via RDP or VNC, check Enabling RDP or installing VNC server on Windows PC for details.
2. Register an account in Acronis Cyber Protect Connect Cloud, if you do not have it yet.
3. Add your Acronis Cyber Protect Connect Cloud account to Users list.

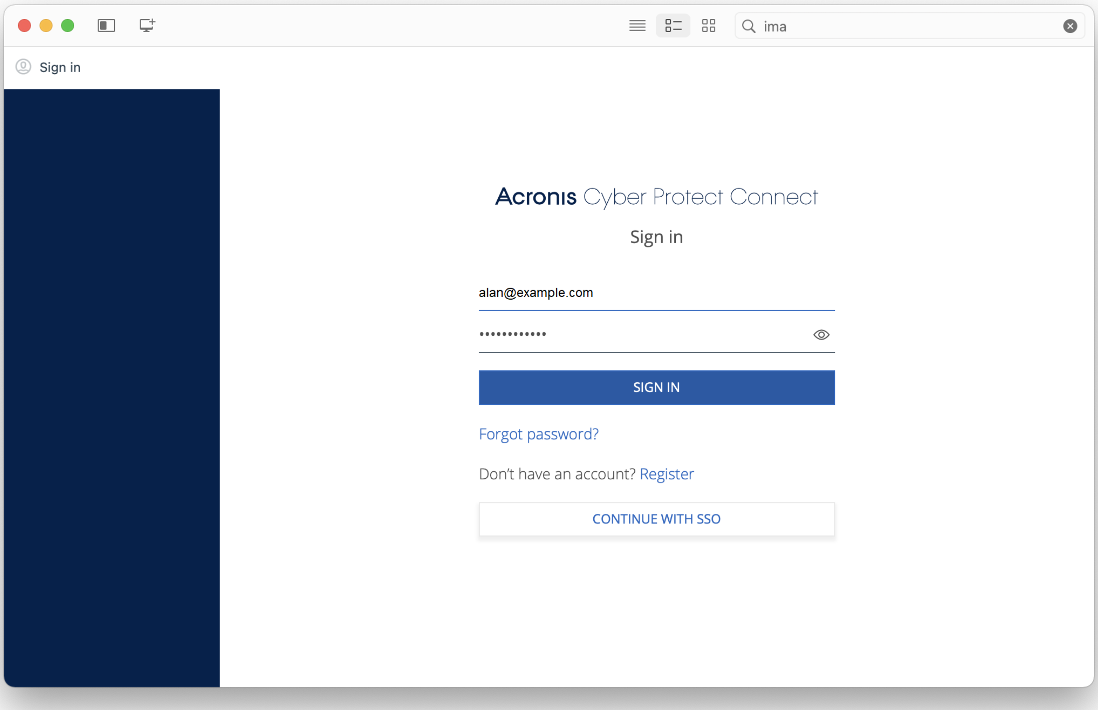


Trusted users and teams

Cyber Protect Connect accounts that are added to this list will see this computer in Cyber Protect Connect and Cyber Protect Connect console, and might be allowed to access the computer without an access code

alan@example.com
susan@example.com

5. Open the Acronis Cyber Protect Connect client and authorize with your Acronis Cyber Protect Connect Cloud.

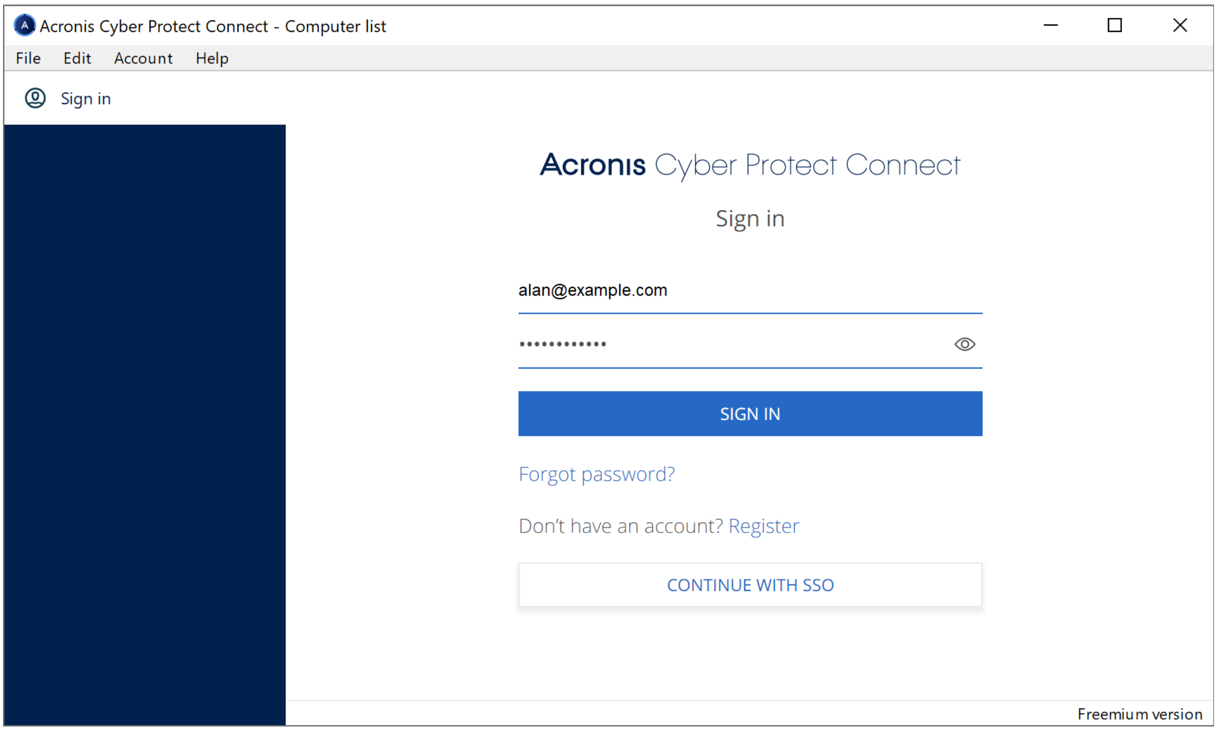


Acronis Cyber Protect Connect

Sign in

alan@example.com

••••••••••••


Acronis Cyber Protect Connect - Computer list
File
Edit
Account
Help
Sign in
Acronis Cyber Protect Connect
Sign in

alan@example.com

••••••••••••

SIGN IN
Forgot password?
Don't have an account? Register
CONTINUE WITH SSO
Freemium version

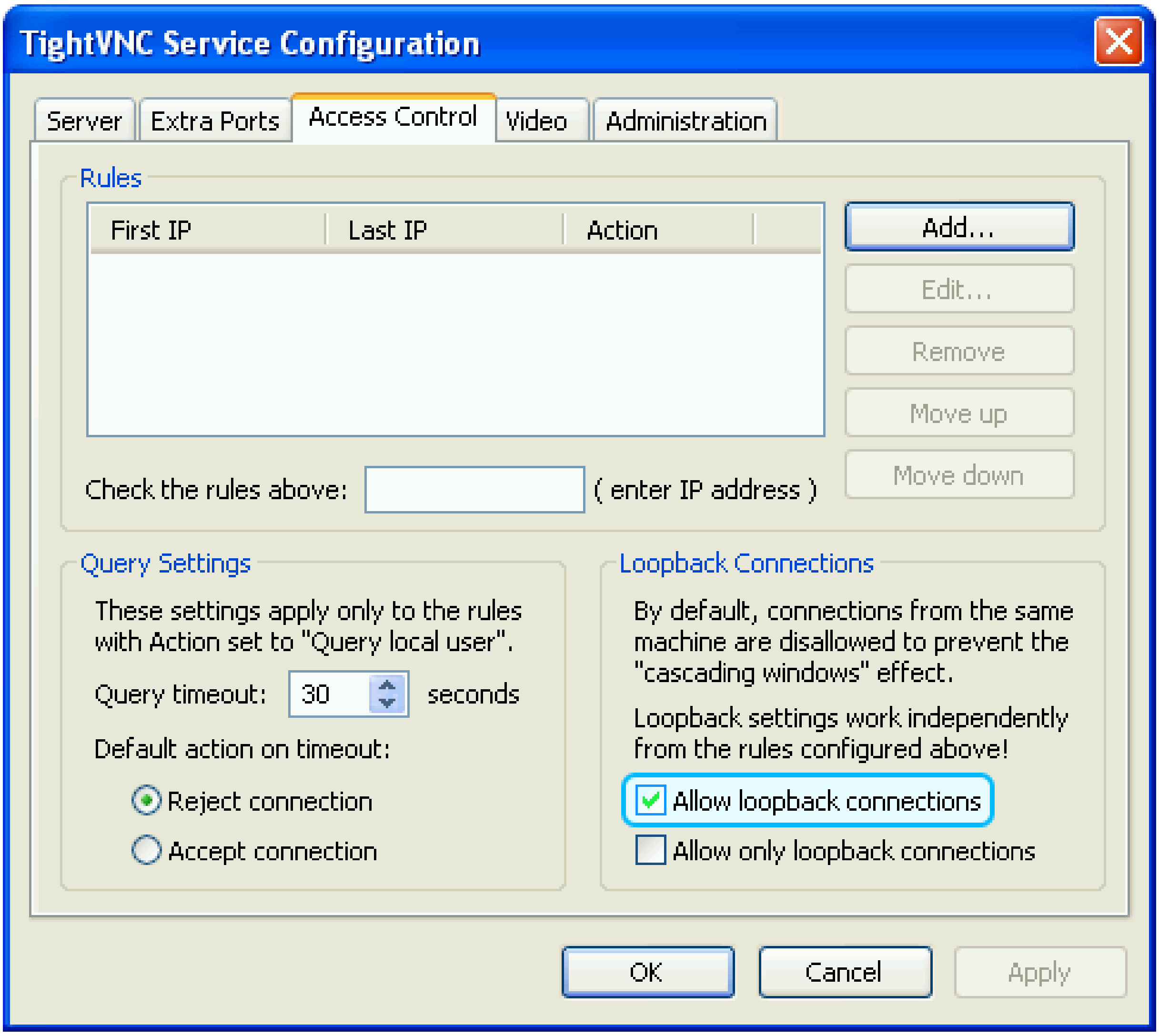
The remote PC appears in Cyber Protect Connect Cloud pane, so you can now connect to it from anywhere.

Enabling desktop sharing on Windows

Latest versions of the Acronis Cyber Protect Connect client and Acronis Cyber Protect Connect agent support NEAR protocol, which does not require any additional configuration from your side.

With NEAR, you connect to the current console session or logon window, as opposed to RDP, where each user gets a separate session. Should you require RDP, you can configure it by the steps below. Note that RDP access may not be available on certain Windows versions, like Home, Starter or Basic editions. In this case, your only options are using NEAR or installing third-party VNC server.

- Enable RDP access:
  1. Open the **Services** tab in Acronis Cyber Protect Connect agent.
  2. Enable **Allow RDP**.
- Enable VNC access:
  1. Install a third party VNC server like **TightVNC** or **UltraVNC**.
  2. Enable Loopback access in VNC server preferences.



TightVNC Service Configuration

Server | Extra Ports | Access Control | Video | Administration

Rules

First IP	Last IP	Action

Add... | Edit... | Remove | Move up | Move down

Check the rules above: (enter IP address)

Query Settings

These settings apply only to the rules with Action set to "Query local user".

Query timeout: 30 seconds

Default action on timeout:

● Reject connection

○ Accept connection

Loopback Connections

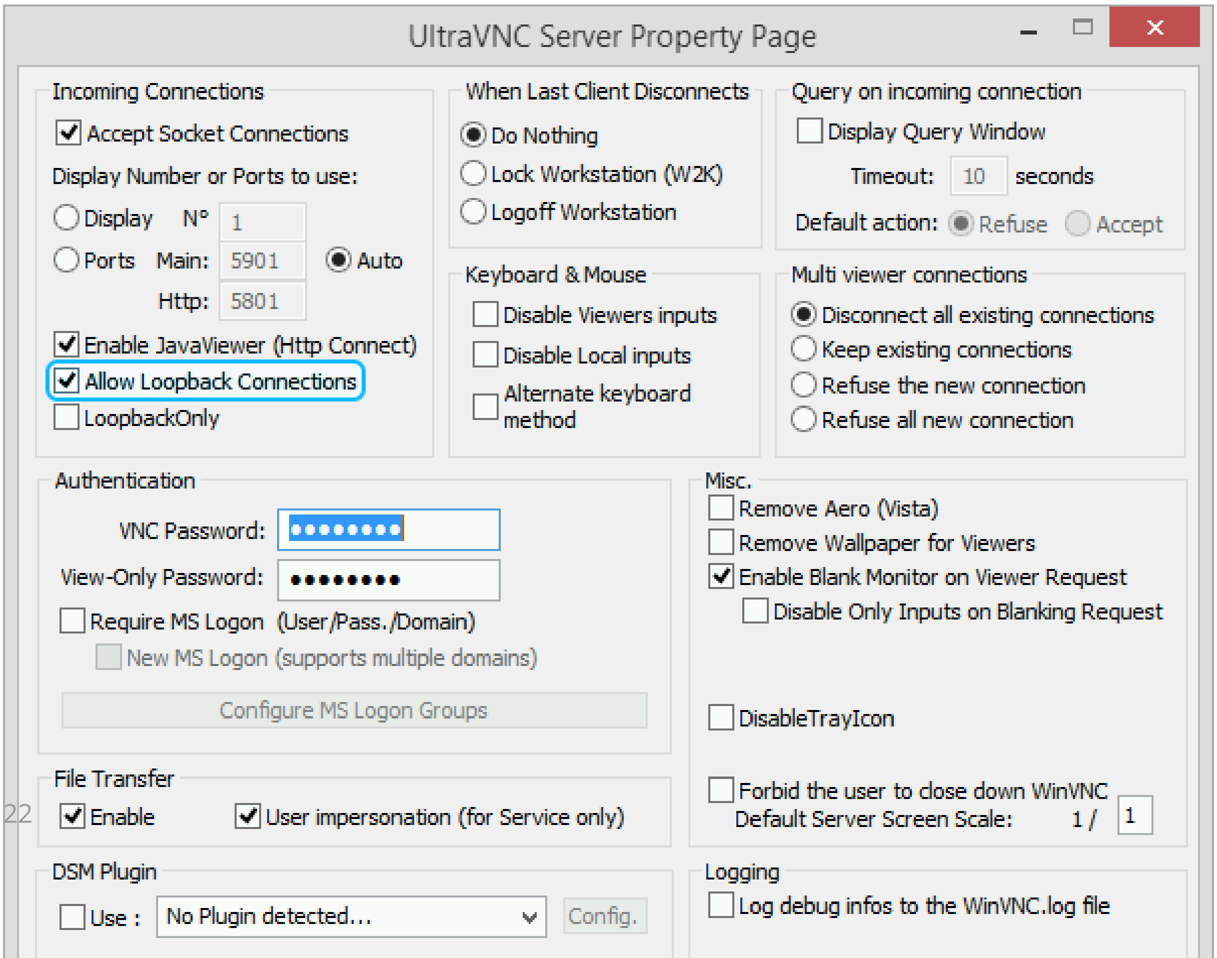
By default, connections from the same machine are disallowed to prevent the "cascading windows" effect.

Loopback settings work independently from the rules configured above!

☑ Allow loopback connections

□ Allow only loopback connections

OK | Cancel | Apply



UltraVNC Server Property Page

Incoming Connections

☑ Accept Socket Connections

Display Number or Ports to use:

○ Display N° 1

○ Ports Main: 5901 ● Auto

Http: 5801

☑ Enable JavaViewer (Http Connect)

☑ Allow Loopback Connections

□ LoopbackOnly

When Last Client Disconnects

● Do Nothing

○ Lock Workstation (W2K)

○ Logoff Workstation

Keyboard & Mouse

□ Disable Viewers inputs

□ Disable Local inputs

□ Alternate keyboard method

Query on incoming connection

□ Display Query Window

Timeout: 10 seconds

Default action: ● Refuse ○ Accept

Multi viewer connections

● Disconnect all existing connections

○ Keep existing connections

○ Refuse the new connection

○ Refuse all new connection

Authentication

VNC Password: ••••••••

View-Only Password: ••••••••

□ Require MS Logon (User/Pass./Domain)

□ New MS Logon (supports multiple domains)

Configure MS Logon Groups

Misc.

□ Remove Aero (Vista)

□ Remove Wallpaper for Viewers

☑ Enable Blank Monitor on Viewer Request

□ Disable Only Inputs on Blanking Request

□ DisableTrayIcon

□ Forbid the user to close down WinVNC

Default Server Screen Scale: 1 / 1

File Transfer

☑ Enable ☑ User impersonation (for Service only)

DSM Plugin

□ Use : No Plugin detected... Config.

Logging

□ Log debug infos to the WinVNC.log file

3. Open Cyber Protect Connect agent and go to **Services** .

4. Enable **Allow VNC**.

Configuring permissions for remote access on macOS 10.14 Mojave

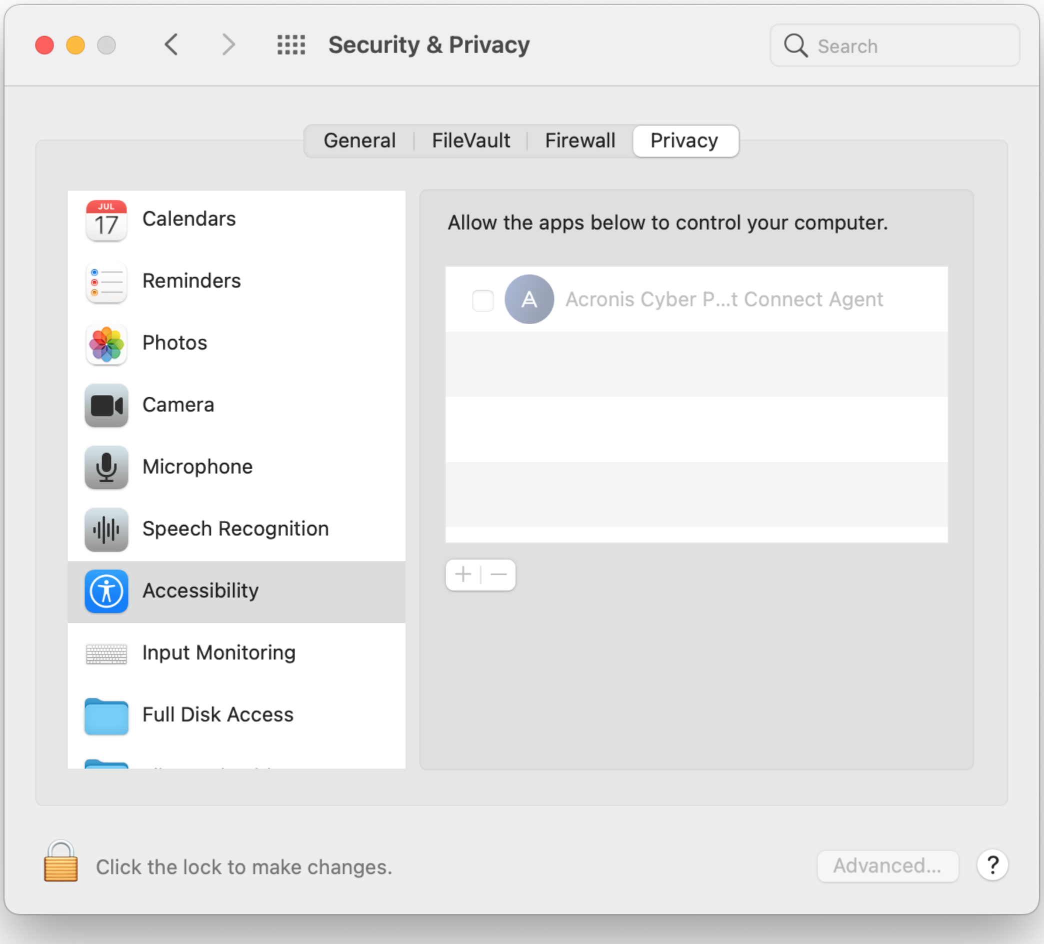
Since 10.14 Mojave, macOS requires all remote control applications like the Acronis Cyber Protect Connect client to have special rights to control the computer. Without this access, you will only be able to view the remote computer's screen but will not have the ability to control its keyboard, nor the mouse.

Once you launch Acronis Cyber Protect Connect agent on a Mac, it will check if it has these rights and will ask you to grant access if needed. To make your Mac available for control with NEAR, do as follows:

1. In an opened window, click the **Request permission** button that will open a system dialog.

2. In the **Accessibility Access** dialog window, click **Open System Preferences**.

This will open **Security & Privacy > Privacy > Accessibility** in the **System Preferences** app.



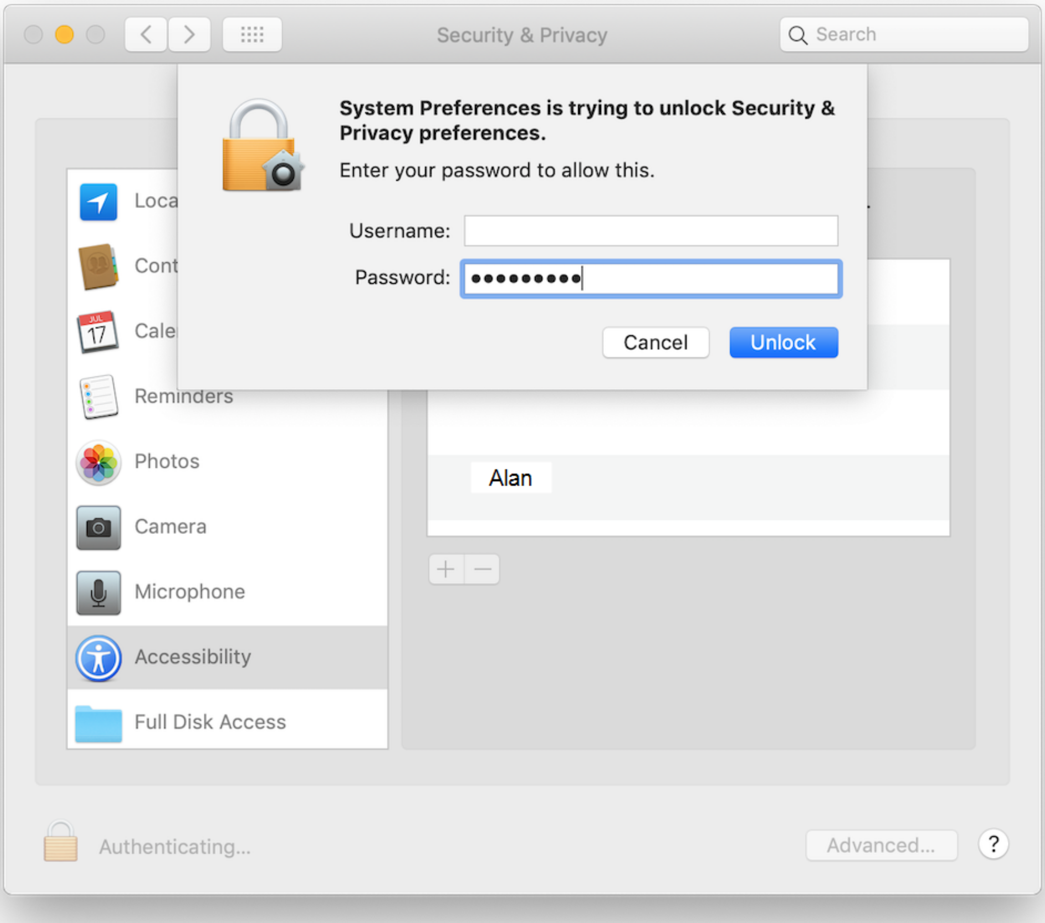
Security & Privacy

Allow the apps below to control your computer.

□ Acronis Cyber P...t Connect Agent

Click the lock to make changes.

4. Click the Lock icon in the bottom-left corner of the window so that it changes to an unlocked one. The system will ask you for an administrator password to make changes.



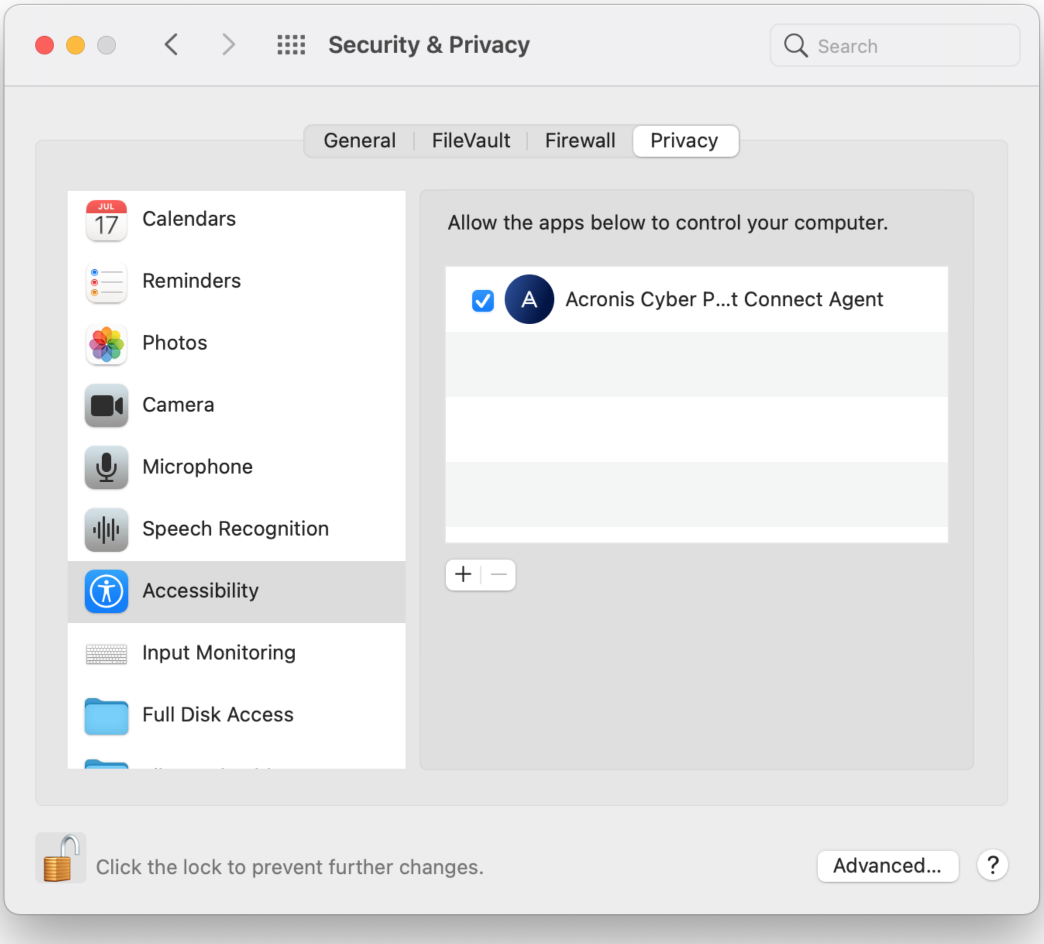
System Preferences is trying to unlock Security & Privacy preferences.

Enter your password to allow this.

Username:

Password: ●●●●●●●●●●

5. Select Acronis Cyber Protect Connect agent to give it access.



Allow the apps below to control your computer.

☑ Acronis Cyber P...t Connect Agent

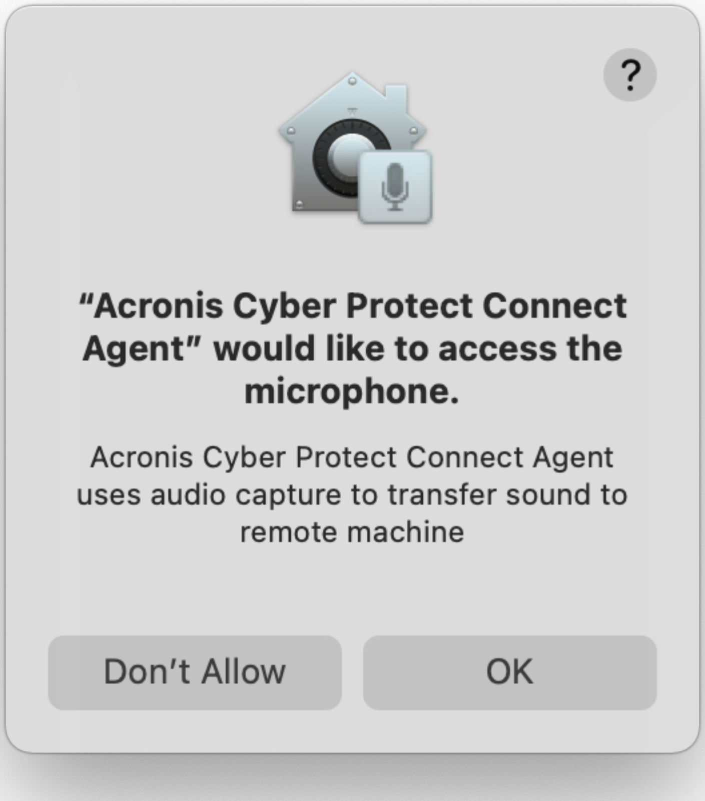
Click the lock to prevent further changes.

Now your Mac can be controlled remotely.

Microphone Permission

To make your Mac able to redirect its sound to Cyber Protect Connect agent for NEAR connections

1. In an opened window, click the **Request Microphone Permission** button.
2. Click **OK** to give Acronis Cyber Protect Connect agent the required permission.



"Acronis Cyber Protect Connect Agent" would like to access the microphone.

Acronis Cyber Protect Connect Agent uses audio capture to transfer sound to remote machine

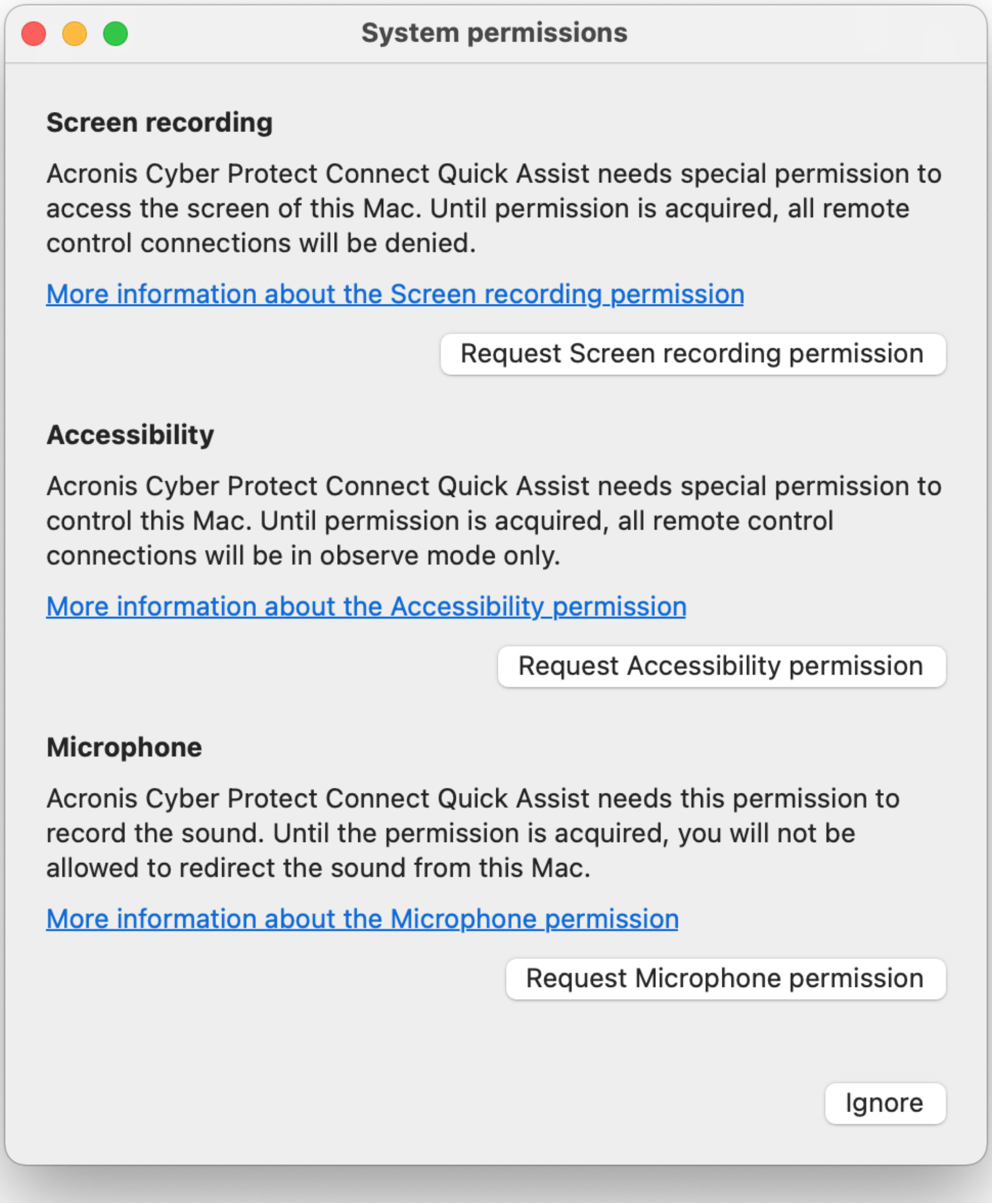
Now Acronis Cyber Protect Connect agent is added to the **Microphone** section in **Security & Privacy > Privacy** in **System Preferences** and it can capture the sound.

Note that you will also need a third-party sound capture driver like Soundflower or Blackhole to let the Agent utilize this permission and transmit the sound of your Mac.

Acquiring Permissions for Remote Access on Mac with macOS 10.15 Catalina

Starting with macOS 10.15 Catalina, remote desktop applications such as Acronis Cyber Protect Connect Quick Assist require a large number of additional permissions before they are granted access to the host computer. Otherwise, any access to the computer will be denied.

After you start Cyber Protect Connect Quick Assist on Mac, the OS checks the necessary permissions and asks whether you want to grant them if needed.



Screen recording

Acronis Cyber Protect Connect Quick Assist needs special permission to access the screen of this Mac. Until permission is acquired, all remote control connections will be denied.

More information about the Screen recording permission

Accessibility

Acronis Cyber Protect Connect Quick Assist needs special permission to control this Mac. Until permission is acquired, all remote control connections will be in observe mode only.

More information about the Accessibility permission

Microphone

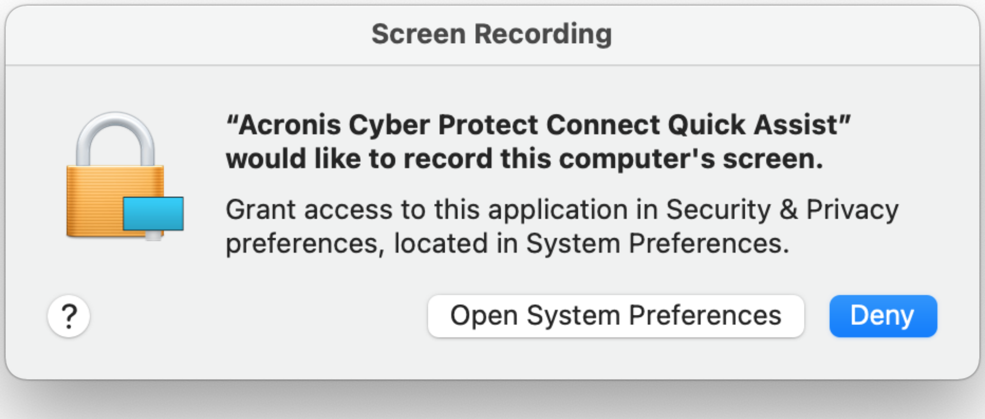
Acronis Cyber Protect Connect Quick Assist needs this permission to record the sound. Until the permission is acquired, you will not be allowed to redirect the sound from this Mac.

More information about the Microphone permission

SCREEN RECORDING PERMISSIONS

To enable screen sharing on your Mac via the NEAR protocol

1. When you receive the permission request, click **Request Screen Recording Permission**.
2. In the **Screen Recording** dialog window, click **Open System Preferences**.

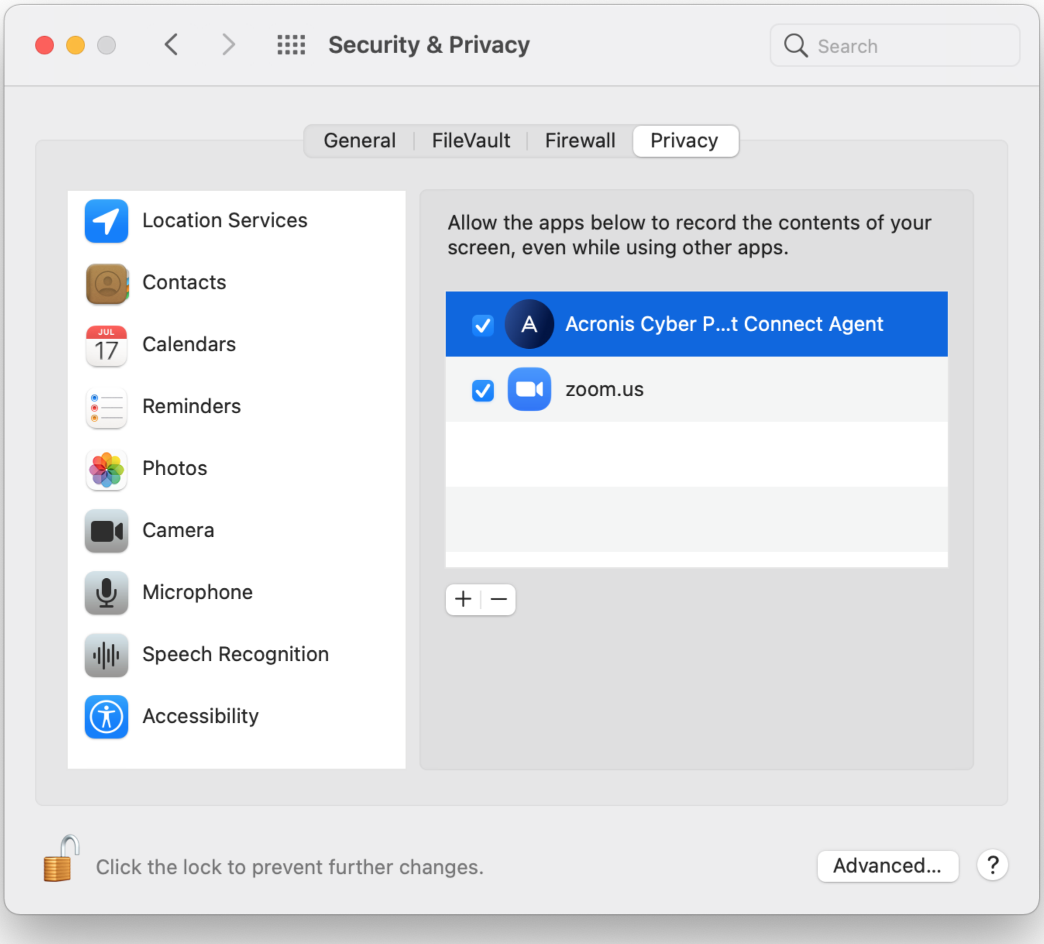

Screenshot: Screen Recording

"Acronis Cyber Protect Connect Quick Assist" would like to record this computer's screen.

Grant access to this application in Security & Privacy preferences, located in System Preferences.

This will open **Security & Privacy** > **Privacy** > **Screen Recording** in **System Preferences**.

4. Select Acronis Cyber Protect Connect Quick Assist to grant access rights to the application.


Screenshot: Security & Privacy

Allow the apps below to record the contents of your screen, even while using other apps.

☑ Acronis Cyber P...t Connect Agent

☑ zoom.us

Click the lock to prevent further changes.

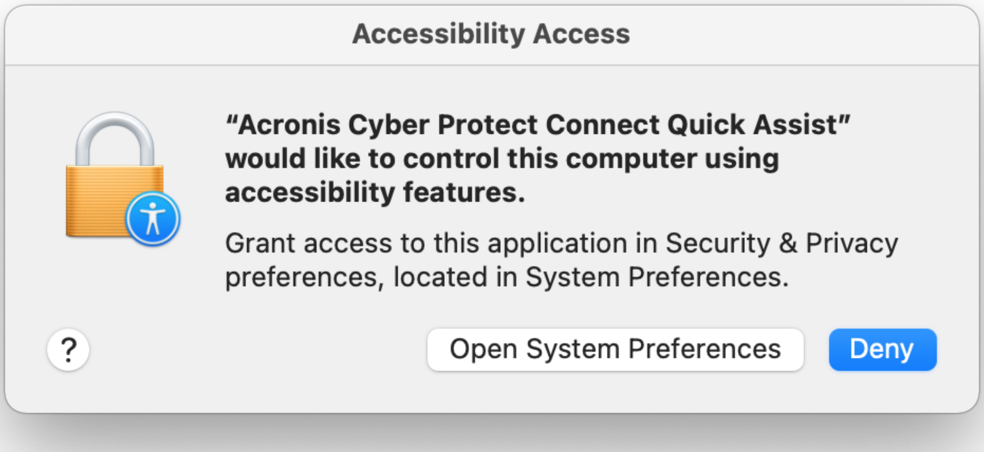
Now you can view your Mac screen remotely.

If you do not have the required permissions for remote access, Cyber Protect Connect Quick Assist will display a prompt asking for a permission to allow screen recording. Please note that such a permission can only be granted by the local user of the Mac you are trying to access.

ACCESS PERMISSIONS

With NEAR, you can not only view a shared screen, but also control your Mac remotely.

1. Open a window and click **Request Accessibility Permission**.
2. In the **Accessibility Access** dialog, click **Open System Preferences**.



Accessibility Access

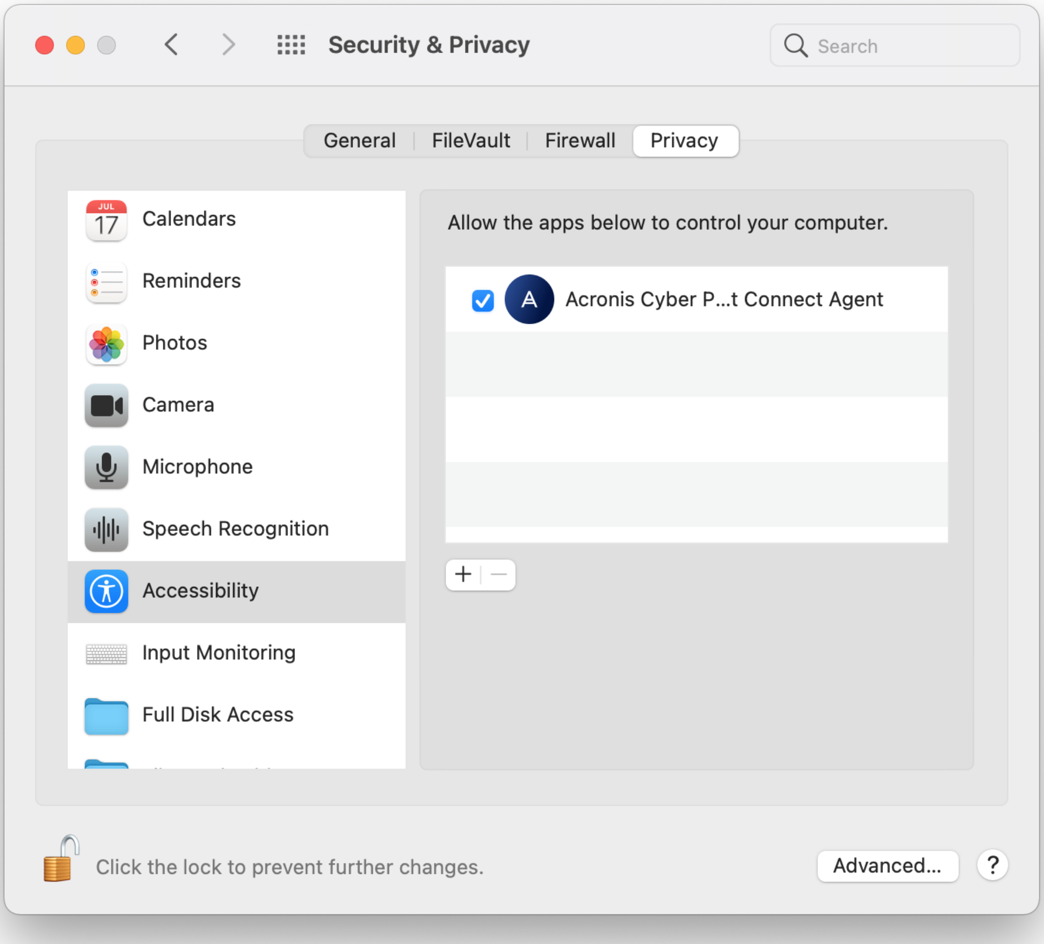
"Acronis Cyber Protect Connect Quick Assist" would like to control this computer using accessibility features.

Grant access to this application in Security & Privacy preferences, located in System Preferences.

This will open **Security & Privacy > Privacy > Accessibility** in **System Preferences**.

4. Click the Lock icon in the bottom-left corner of the window to unlock it. You will then have to enter your administrator password before making any changes.

5. Select AcronisCyber Protect Connect Quick Assist to grant access rights to the application.



Security & Privacy

General | FileVault | Firewall | Privacy

Allow the apps below to control your computer.

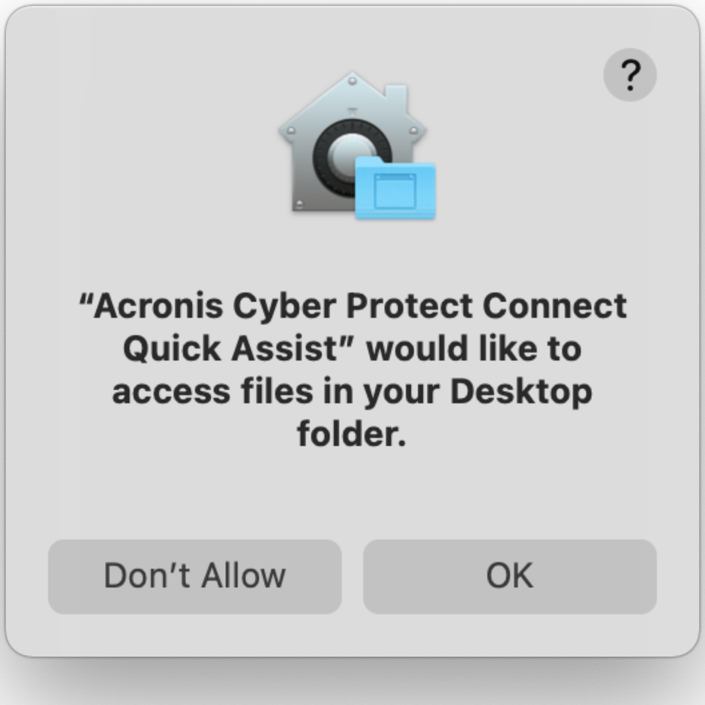
☑ Acronis Cyber P...t Connect Agent

Click the lock to prevent further changes.

Now your Mac can be controlled remotely with NEAR.

OTHER PERMISSIONS

Acronis Cyber Protect Connect Quick Assist also lets you transfer files, just like Acronis Cyber Protect Connect agent. For security reasons, macOS version 10.15 Catalina and higher will not let you gain remote access to user or system files automatically. Each time you're trying to access a user folder, your file transfer request will have to be granted by the local user.



"Acronis Cyber Protect Connect Quick Assist" would like to access files in your Desktop folder.

Unlike Cyber Protect Connect agent, Cyber Protect Connect Quick Assist cannot grant you full remote disk access, since using Cyber Protect Connect Quick Assist usually implies there is a local user behind the target Mac at the moment. If you want to gain full remote access to local files on another Mac, install Cyber Protect Connect agent instead.

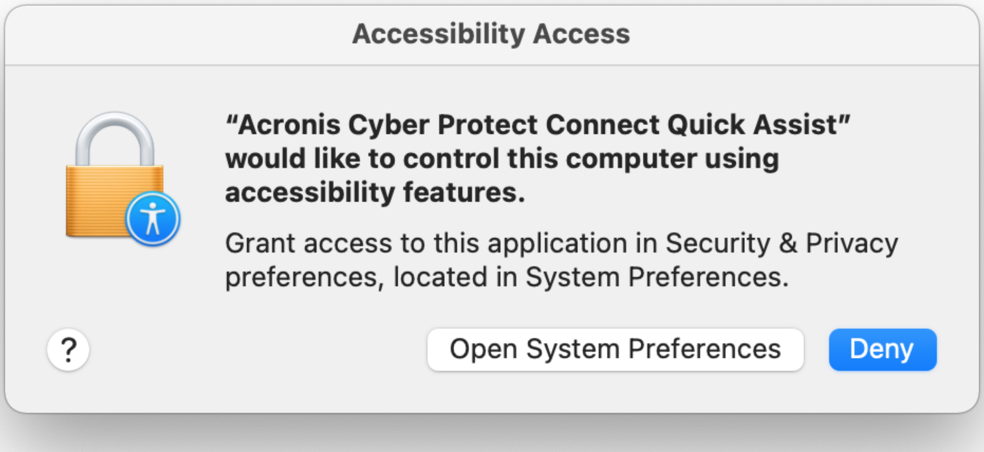
Configuring permissions for remote access on macOS 10.14 Mojave

Since 10.14 Mojave, macOS requires all remote control applications like the Acronis Cyber Protect Connect client to have special rights to control the computer. Without this access, you will only be able to view the remote computer's screen but will not have the ability to control its keyboard, nor the mouse.

Once you start Acronis Cyber Protect Connect Quick Assist on a Mac, it will check if it has these rights and will ask you to grant the access if needed.

To make your Mac available for control with NEAR

1. Open a window and click **Request Accessibility Permission**.
2. In the **Accessibility Access** dialog, click **Open System Preferences**.



Accessibility Access

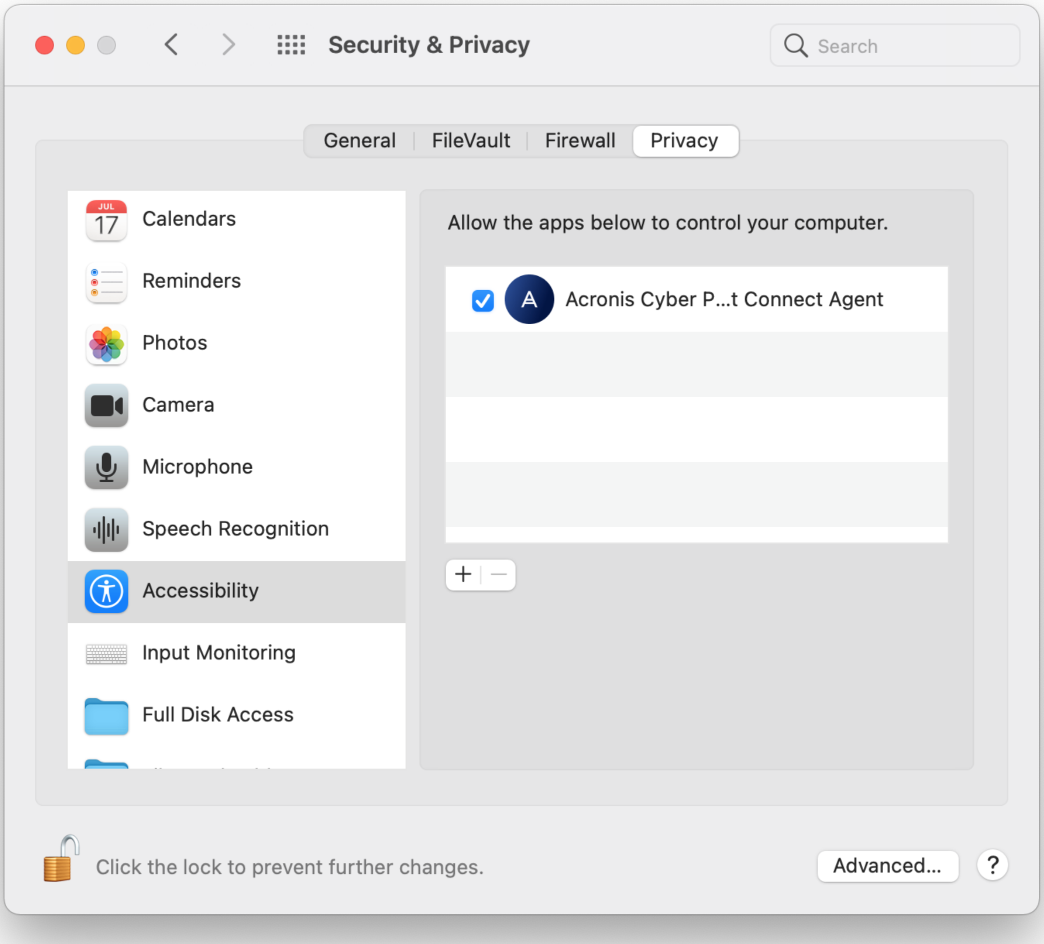
“Acronis Cyber Protect Connect Quick Assist” would like to control this computer using accessibility features.

Grant access to this application in Security & Privacy preferences, located in System Preferences.

This will open **Security & Privacy** > **Privacy** > **Accessibility** in **System Preferences**.

4. Click the Lock icon in the bottom-left corner of the window to unlock it. You will then have to enter your administrator password before making any changes.

5. Select Acronis Cyber Protect Connect Quick Assist to grant access rights to the application.



Allow the apps below to control your computer.

☑ Acronis Cyber P...t Connect Agent

Click the lock to prevent further changes.

Now your Mac can be controlled remotely with NEAR.

Microphone Permission

To make your Mac able to redirect its sound to Cyber Protect Connect Quick Assist for NEAR connections

1. In an opened window, click **Request Microphone Permission**.
2. Click **OK** to give Cyber Protect Connect Quick Assist the required permission.

   Now Cyber Protect Connect Quick Assist is added to **Microphone** section in **Security & Privacy** > **Privacy** in **System Preferences** and it will be able to capture the sound.

OTHER PERMISSIONS

Unlike Acronis Cyber Protect Connect agent, Acronis Cyber Protect Connect Quick Assist cannot grant you full remote disk access, since using Cyber Protect Connect Quick Assist usually implies there is a local user behind the target Mac at the moment. If you want to gain full remote access to local files on another Mac, install Cyber Protect Connect agent instead.

Common tasks

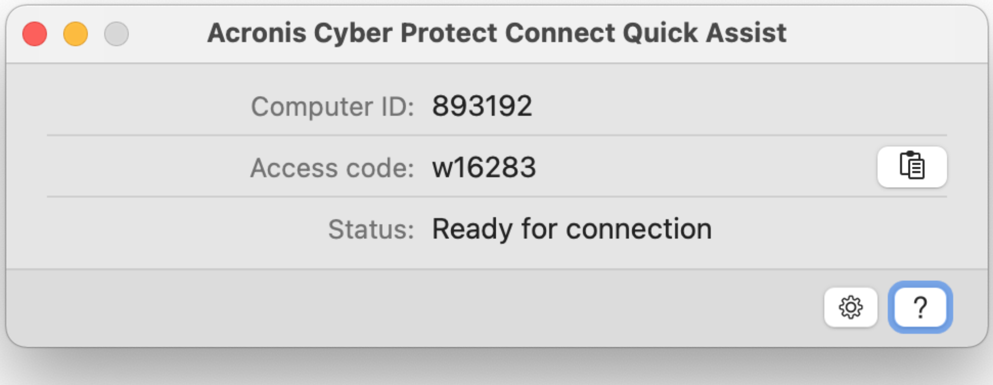
Helping someone once

If a user needs help only once, Acronis Cyber Protect Connect Quick Assist may be the best decision. The user should only download and start the application. It does not need any configuration.

If a user needs help on a regular basis, you may prefer using the full version of Acronis Cyber Protect Connect agent for Mac, Windows or Linux.

To connect to a user's computer remotely

1. Give user a link to the Cyber Protect Connect Quick Assist download page: https://go.acronis.com/qa.
2. Ask the remote user to download and start the application.
3. Ask the user for the **Computer ID** and **Access Code** that are displayed in Cyber Protect Connect Quick Assist.

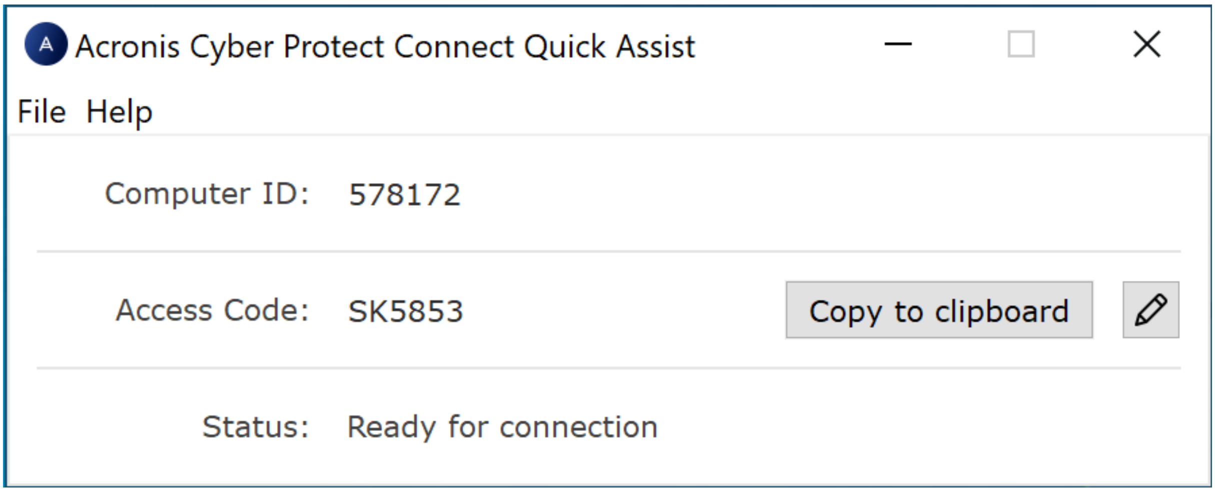


Acronis Cyber Protect Connect Quick Assist

Computer ID: 893192

Access code: w16283

Status: Ready for connection



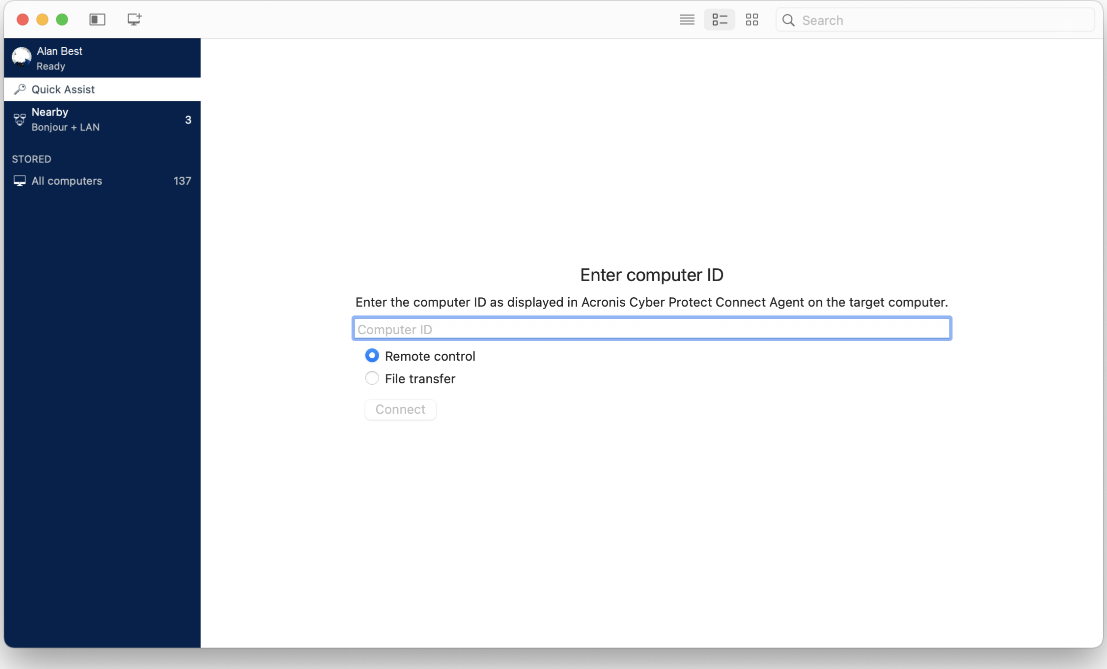
Acronis Cyber Protect Connect Quick Assist

Computer ID: 578172

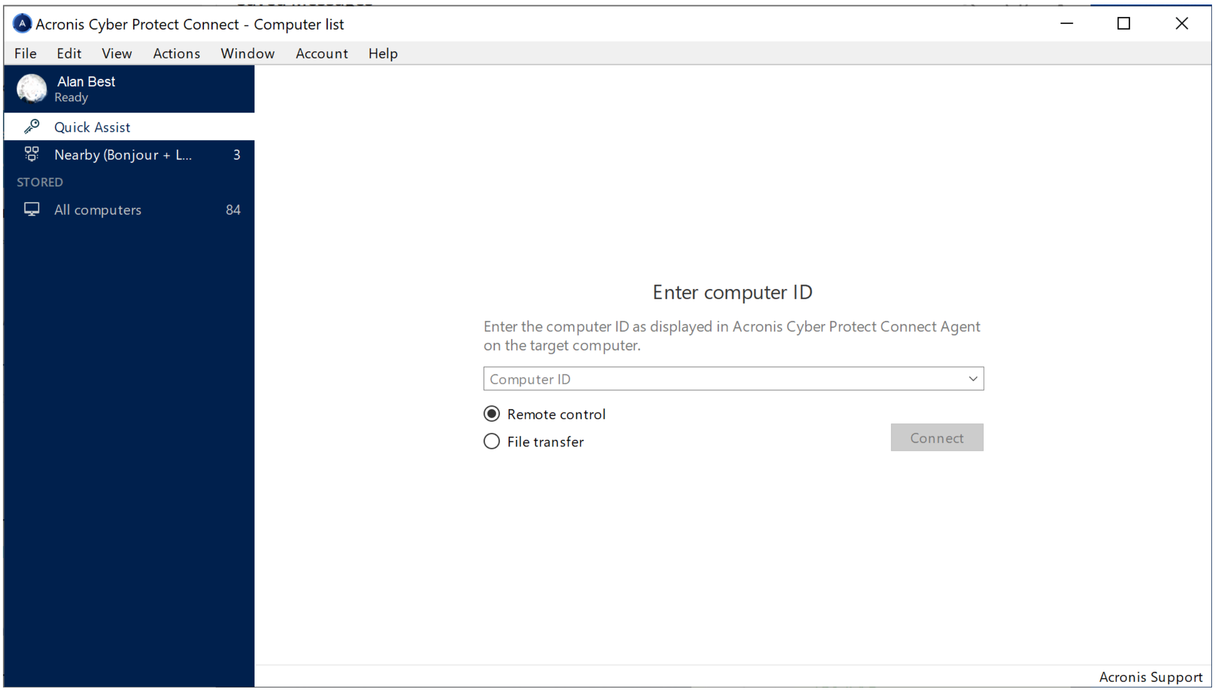
Access Code: SK5853

Status: Ready for connection

4. In the AcronisCyber Protect Connect client, open the **Quick Connect** pane, and enter the **Computer ID** and **Access Code**.



Enter the computer ID as displayed in Acronis Cyber Protect Connect Agent on the target computer.



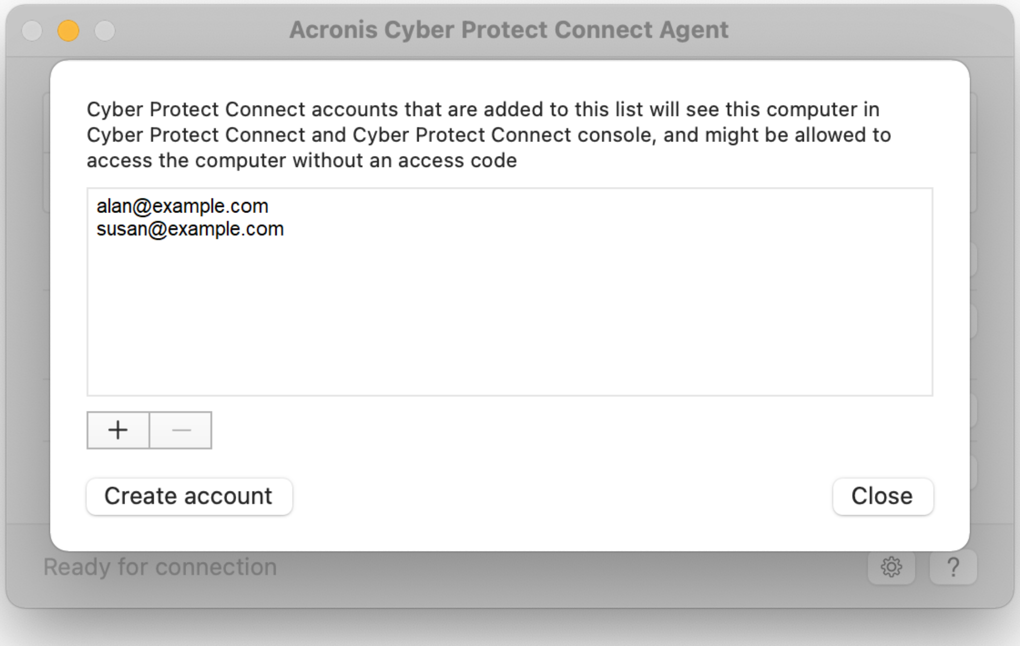
Enter the computer ID as displayed in Acronis Cyber Protect Connect Agent on the target computer.

5. Click **Connect**.

Sharing aremote computer with colleagues

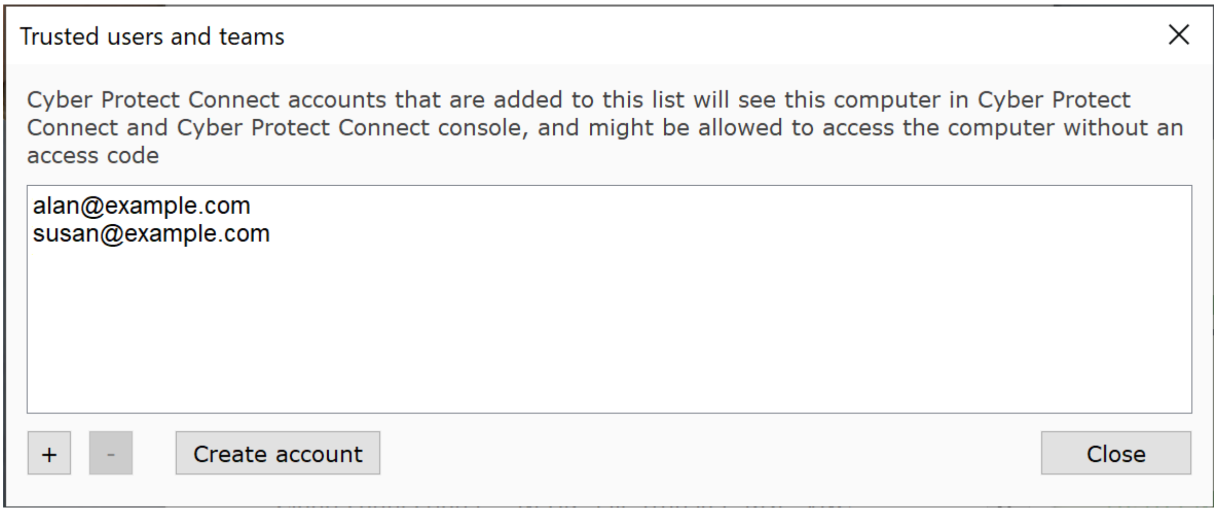
You and your colleagues can share a computer for work or entertainment purposes.

1. Install Acronis Cyber Protect Connect agent for macOS or Acronis Cyber Protect Connect agent for Windows on the remote computer you want to share.
2. Each team member accessing a remote computer must register in Acronis Cyber Protect Connect Cloud.
3. Add each Acronis Cyber Protect Connect Cloud ID to the **Users** list in Cyber Protect Connect agent.



Cyber Protect Connect accounts that are added to this list will see this computer in Cyber Protect Connect and Cyber Protect Connect console, and might be allowed to access the computer without an access code

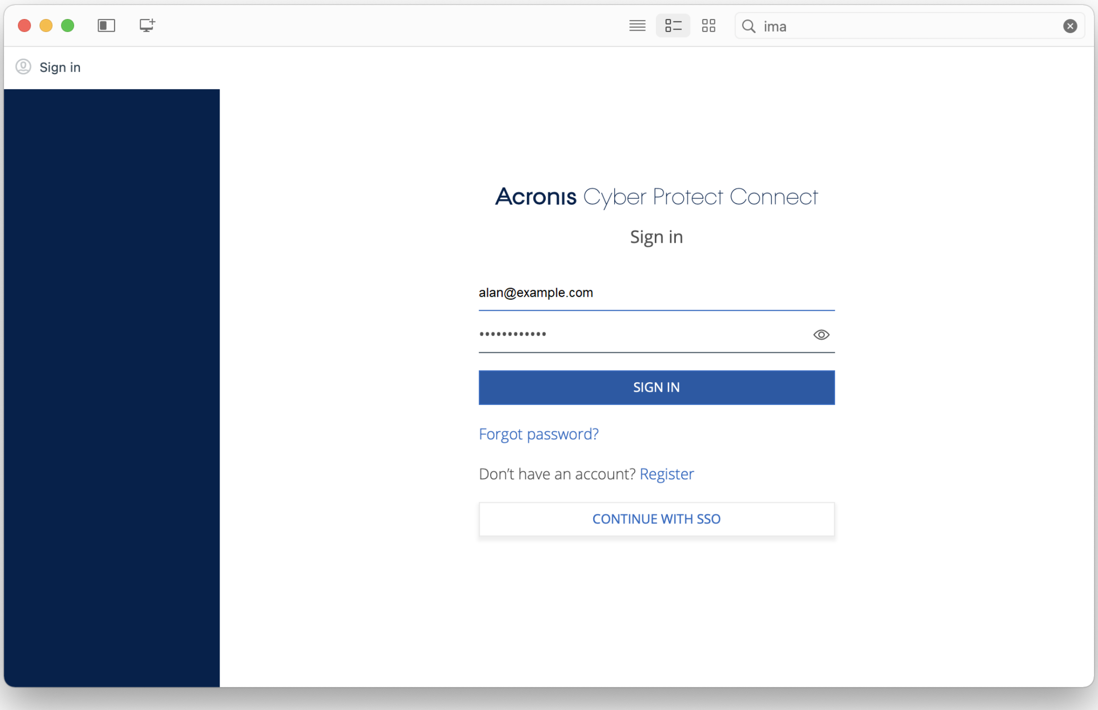
alan@example.com
susan@example.com



Cyber Protect Connect accounts that are added to this list will see this computer in Cyber Protect Connect and Cyber Protect Connect console, and might be allowed to access the computer without an access code

alan@example.com
susan@example.com

Each team member must log in using his or her Cyber Protect Connect Cloud ID in the Acronis Cyber Protect Connect Cloud in the Acronis Cyber Protect Connect client.



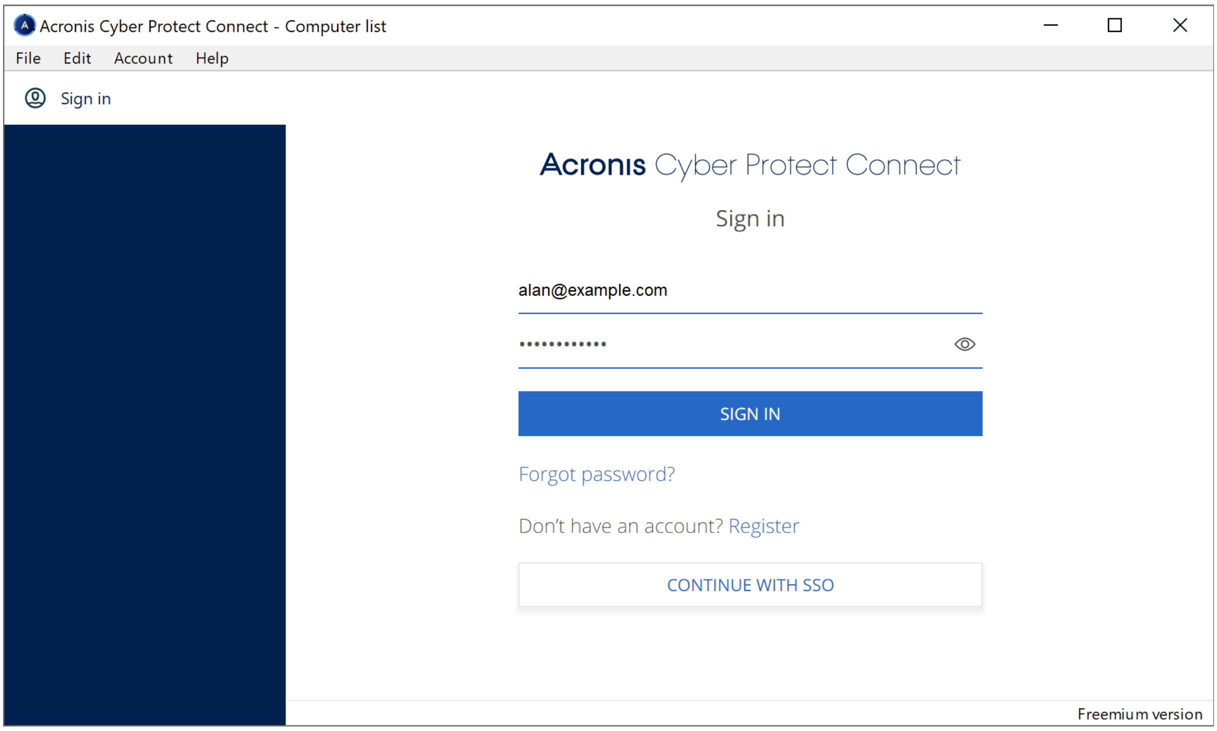
Acronis Cyber Protect Connect

Sign in

alan@example.com

••••••••••••

Don't have an account? Register



Acronis Cyber Protect Connect

Sign in

alan@example.com

••••••••••••

Don't have an account? Register

The computer will automatically appear under Acronis Cyber Protect Connect Cloud scanner in the Cyber Protect Connect client for each team member.

Configuring remote sound

The Acronis Cyber Protect Connect client supports audio streaming with the NEAR protocol. While Windows had it in RDP for ages, this is a long-awaited feature for Macs that have no sound support in their built-in Screen Sharing protocol.

How to get remote sound from a Mac

To get the sound redirection working, you need to install a sound capture driver and use the NEAR connection protocol with Acronis Cyber Protect Connect agent installed on your Mac. If you are using macOS 10.15 Catalina, you must grant the Microphone permission to the Agent when asked to.

Starting with version 1.4, Cyber Protect Connect agent works with either of two sound capture drivers: Soundflower and Blackhole.

The installation process on the newest versions of macOS is a bit tricky due to Apple security measures. It is described in detail on the Blackhole wiki page: https://github.com/ExistentialAudio/BlackHole/wiki/Installation.
Please note that you must install the 2-channel version of Blackhole, because the Acronis Cyber Protect Connect client currently does not support the 16-channel version.

You can also install Blackhole with the `brew install --cask blackhole-2ch` command if you have Homebrew installed.

Note that remote sound redirection from Macs stops the remote user from hearing any sound while you are connected.

How to get remote sound from a PC

On Windows, the remote sound should be transmitted automatically. If you do not have sound output devices connected to the remote PC, connect any sound output device (speakers or headphones).

How to get remote sound from a Linux

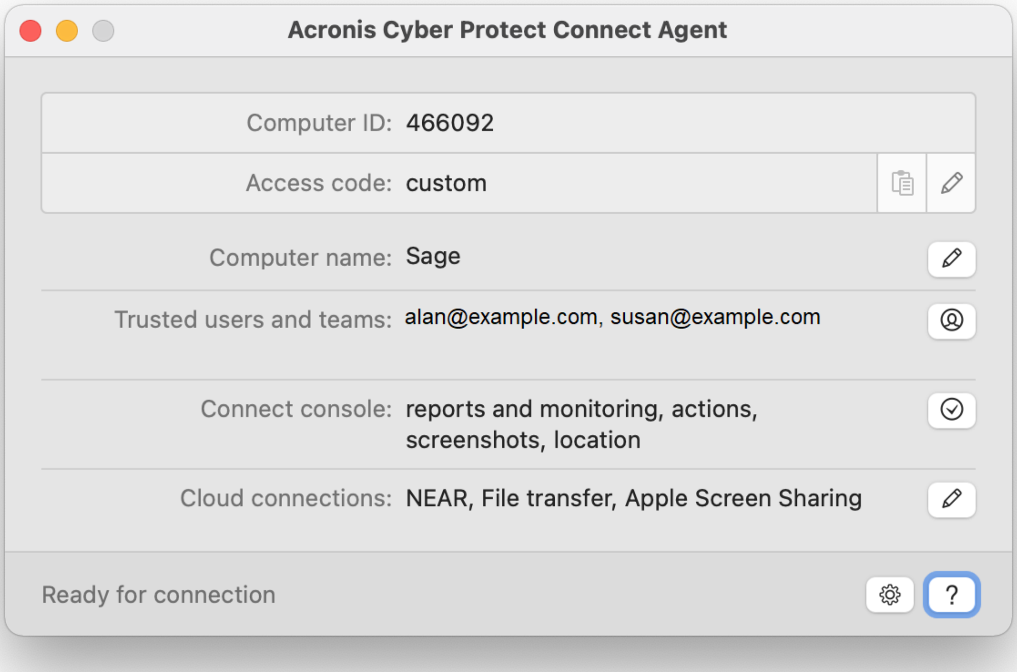
The remote sound redirection should work automatically with most Linux distributions. If you are unable to hear remote sound from a Linux, installing PulseAudio driver should help: `sudo apt-get install pulseaudio`.

Changing the access code

The **Access Code** is used to protect your security. It is a password-like code that will be required from people willing to access your desktop by Computer. By default, the access code is set to a randomly generated 6-symbol code and changes automatically every 6 hours.

If you want the code to be changed more or less often or to set your own one instead, you can choose one of the following options:

- **Custom code**: unformatted text up to 255 characters long. If you are fine with self-managing passwords, this might be the best choice.
- **Auto-generated code**: 6-symbol code generated automatically by the Agent. You can choose how often to change it: every week, every day, every 6 hours, or every hour. If you want to turn off automatic change, select **Never**.
- **Disable access code authentication**: for security reasons you may disable **Access Code** access completely. If disabled, only users in the trusted users list would be able to connect to your computer.



Acronis Cyber Protect Connect Agent

Computer ID: 466092

Access code: custom

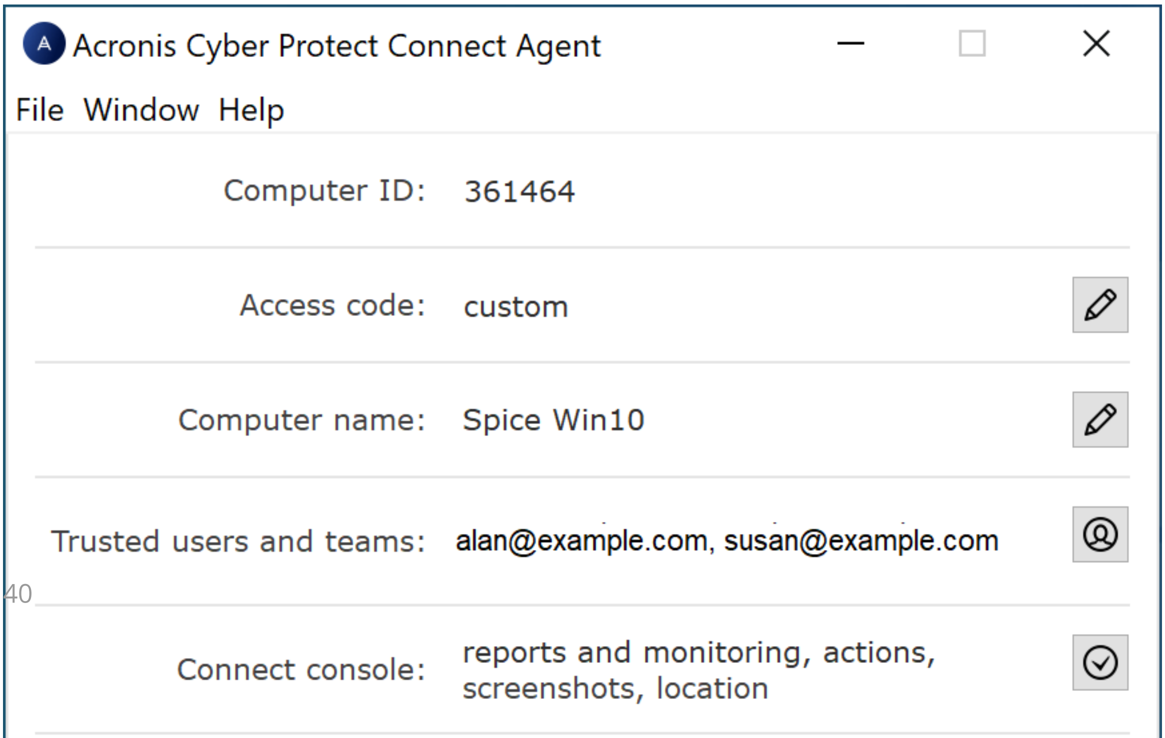
Computer name: Sage

Trusted users and teams: alan@example.com, susan@example.com

Connect console: reports and monitoring, actions, screenshots, location

Cloud connections: NEAR, File transfer, Apple Screen Sharing

Ready for connection



Acronis Cyber Protect Connect Agent

Computer ID: 361464

Access code: custom

Computer name: Spice Win10

Trusted users and teams: alan@example.com, susan@example.com

Connect console: reports and monitoring, actions, screenshots, location

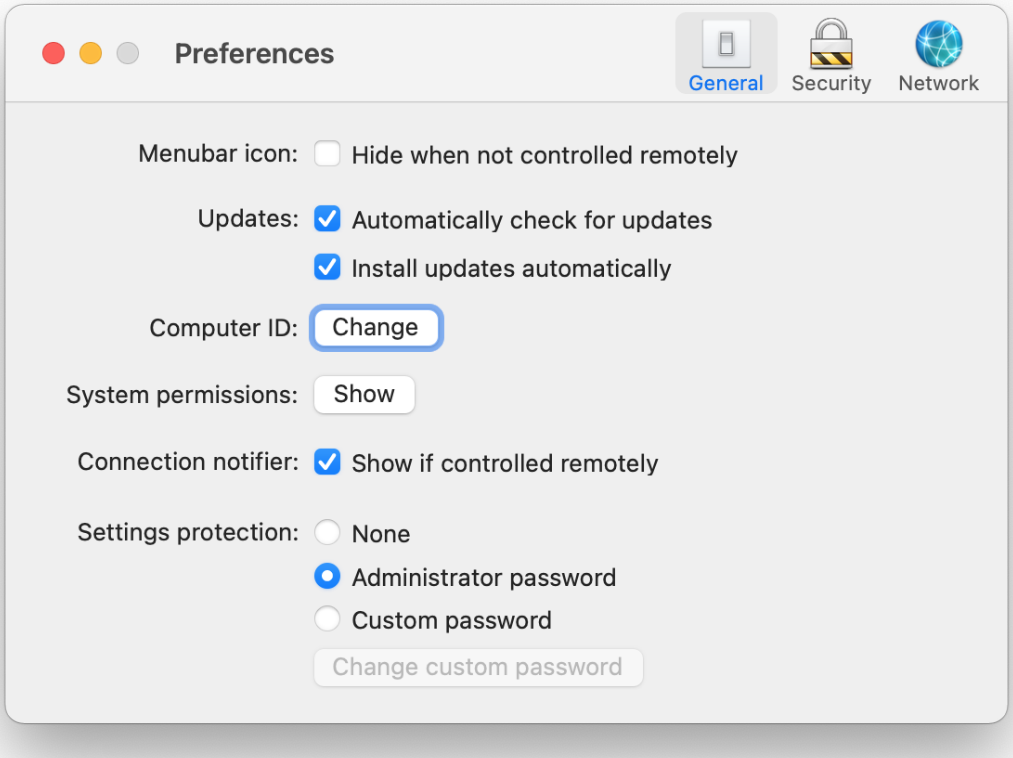
Changing computer ID

Computer ID is used to identify a computer among all other computers connected to the Acronis Cyber Protect Connect servers. You may find yourself in need of changing that ID, for example, if you have cloned a virtual machine that has Acronis Cyber Protect Connect agent installed. In this case you must change the ID so that the new machine does not stop the original one from connecting to the Cyber Protect Connect servers.

To change the Computer ID

1. Open Acronis Cyber Protect Connect agent.
2. Open **Preferences**.
3. In the **Computer ID:** section, click **Change**.
4. Confirm the changes.

Note that you will not be able to connect to this computer using the old Computer ID anymore.



Menubar icon: □ Hide when not controlled remotely

Updates: ☑ Automatically check for updates

☑ Install updates automatically

Computer ID: Change

System permissions: Show

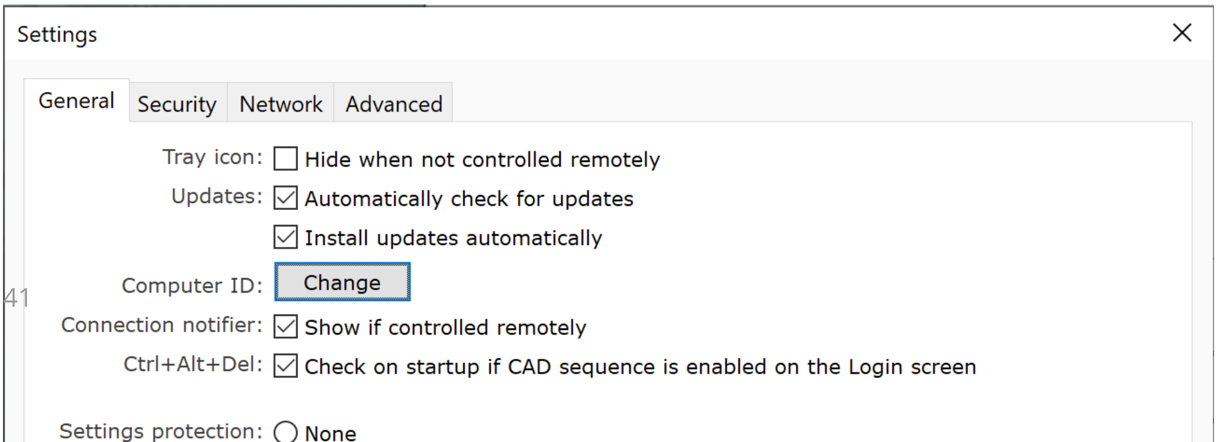
Connection notifier: ☑ Show if controlled remotely

Settings protection: ○ None

● Administrator password

○ Custom password

Change custom password



Tray icon: □ Hide when not controlled remotely

Updates: ☑ Automatically check for updates

☑ Install updates automatically

Computer ID: Change

Connection notifier: ☑ Show if controlled remotely

Ctrl+Alt+Del: ☑ Check on startup if CAD sequence is enabled on the Login screen

Settings protection: ○ None

Uninstalling Acronis Cyber Protect Connect agent

To uninstall Acronis Cyber Protect Connect agent

- On a Mac:
  1. **Quit** Acronis Cyber Protect Connect agent.
  2. Open **Terminal.app**.
  3. Execute the following commands one by one:
     a. `cd /Library/Application Support/com.nulana.rxagentmac/`
     b. `sudo ./uninstall.sh`

        When asked, provide an administrator password and wait for the script to proceed.

        If you see the **[Process completed]** message, Cyber Protect Connect agent is successfully uninstalled.
  4. To delete all the traces of Cyber Protect Connect agent ,run the following commands.
     a. `sudo defaults delete com.nulana.rxagentmac`

        , and then for each user on this Mac:
     b. `defaults delete com.nulana.rxagentmac`
     c. `rm -rf ~/Library/Logs/com.nulana.rxagentmac`

- On Windows PC:
  1. Open **Control Panel** > **Programs** > **Programs and Features**.
  2. Find Acronis Cyber Protect Connect agent in the list of programs, and double-click it.
  3. Follow the uninstallation steps.

Cyber Protect Connect console

Cyber Protect Connect licensing

The Acronis Cyber Protect Connect licenses are available on a subscription basis and are valid for a period of one or three years. The subscription is renewed automatically. If the subscription is canceled and expired, the console will automatically be degraded to the free version with limited capabilities.

You can compare the different product plans of the console in the following table.

Acronis Cyber Protect Connect console version	Description
Professional	One or three year subscription per-user basis Commercial use All features Multi-tenancy support (Teams) Includes technical support and product upgrades
Personal	One year subscription per-user basis Non-commercial use All features Includes technical support and product upgrades
Free	Free to use Limited feature set Possibility to upgrade to trial or paid subscription

Working with licenses

On the **Licensing** page, the root administrator can manage the licensing of the company, by performing the following actions.

License activation and deactivation

Admin users can manually activate or deactivate the Acronis Cyber Protect Connect license for the console account.

If a user purchases an Acronis Cyber Protect Connect license online from Acronis, the license for the specified account (email address) is activated automatically.

If the user purchases a license offline, from a reseller, the license requires manual activation. In this case, the admin can activate the license from the **Licensing** page.

Linking billing account to console account

To see all purchased Acronis Cyber Protect Connect licenses in the console, the admin must link his console account to his billing account. After that, the admin will see information about all purchased Cyber Protect Connect licenses that are associated with the billing account. The admin can browse the license key details in the list of license keys. These details include purchase date, expiration, next charge date, and others.

Note
The billing account is the account which you use to access the e-commerce system for purchasing Acronis Cyber Protect Connect licenses. The billing account is created automatically when youpurchase a license online.

The console account is the account with which you log in to the Acronis Cyber Protect Connect console.

Browsing and distributing license keys

On the **Licensing** page, the admin with a Professional license can view the list of users from all created teams and the list of all purchased keys.

To allow team users to work with the product, the admin should assign the Professional licenses keys to the team users. Keys distribution or revoking is possible from the **Licensing** page.

Cyber Protect Connect console main features

Overview

On the **Overview** page in the Acronis Cyber Protect Connect console, you can find a essential details about the remote computer, such as:

- operating system
- hardware information
- online status
- Acronis Cyber Protect Connect agent version.

Actions

You can also perform the following administrator actions on the remote computer.

- **Shut down**
- **Log out** a selected user
- **Restart**

- **Sleep**
- **Empty trash** (for all users on a Mac, or for a selected user on Windows PC).

Reports

On the **Reports** page, you can view comprehensive information about the remote computer. If issues are detected, they are also highlighted in **Reports** section.

The **System Report** section in the **Overview** tab displays an overall summary of all systems.

You can use the following tabs to view detailed information about a component.

- **Memory**: view the amount of memory installed and how many memory slots are available for a memory upgrade.
- **Storage**: view how much of storage devices is being used.
- **Network**: view which network interfaces are enabled and the amount of data transmitted.
- **Graphics**: view information about graphic cards and the connected displays.
- **Devices**: view the devices connected over USB and the available slots.
- **Firewall**: view the firewall status.
- **Battery**: view battery status & health.
- **Printers**: view the installed printers, scanners, and fax machines.

You can export the reports as a .pdf or .csv file, and configure monitoring settings.

Map

If you manage a huge amount of portable computers, you might want to know the computer location before performing any actions.

The Acronis Cyber Protect Connect console will show all computers that have location service enabled on a map, so you get a quick idea of the stock whereabouts. The marker color depends on the online status.

- **Green** markers for online computers.
- **Red** for offline.
- **Blue** for the one selected.

Note that Acronis Cyber Protect Connect agent needs access to the computer location. For instructions on setup, see Apple instructions for Mac macOS or refer to Microsoft Windows help.

Chat

The built-in interactive chat helps you communicate with the remote user or provide a personal assistance.

To start a chat session

1. Click a remote computer from the list.
2. Select the **Chat** screen.
3. Type the message, and then press **Enter**.

The remote user will see the message in a **Chat** window in Acronis Cyber Protect Connect agent, and will be able to reply.

Note
You can only chat with a remote user who has added you to the Cyber Protect Connect agent **Access List** on the user's computer.

Screenshot

If you want to monitor a remote user activity without connecting, you can use the **Screenshot** page in the Acronis Cyber Protect Connect console. It shows a static screenshot of the remote computer. The screenshot updates twice a minute.

- To choose which screen to see, select one of currently active user sessions in the top left corner.
- To choose screenshot image quality and refresh rate, select one of available options to the top of the screenshot image.

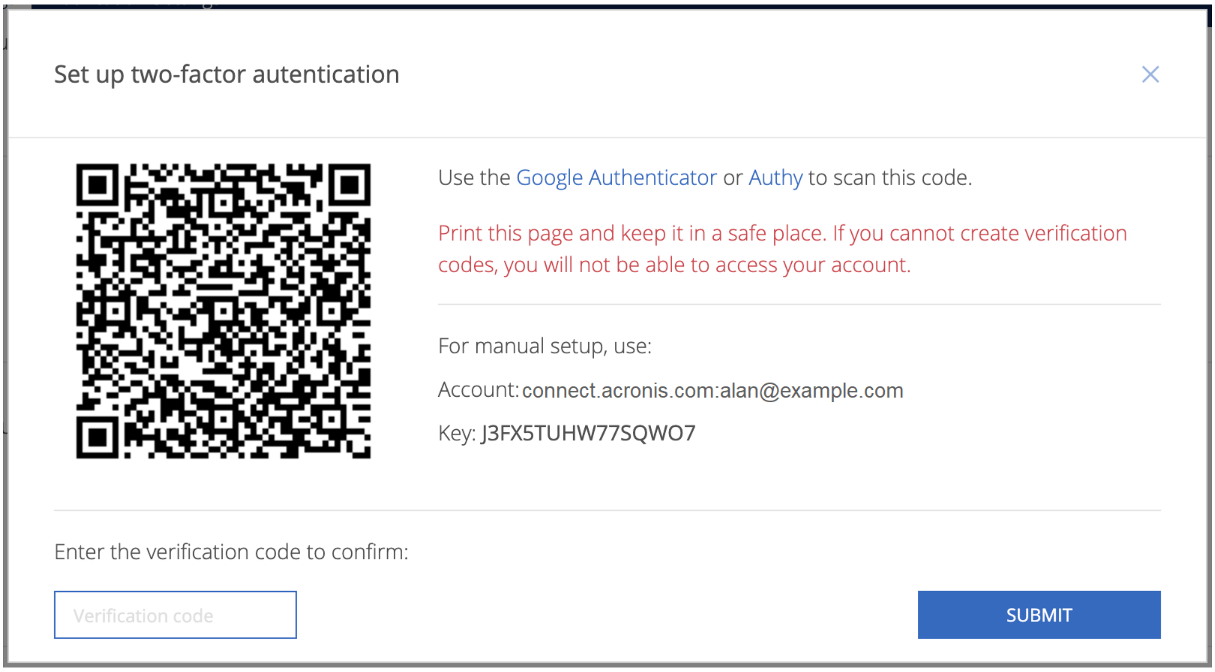
When you exit the page, the screen will stop transmitting.

Account settings

- Account password management
- Time zone
- Two-factor authentication setup

Two-Factor Authentication

You can optionally protect your Acronis Cyber Protect Connect console with two-factor authentication on the **Account settings** page (available in the drop-down menu from the Account icon).


Set up two-factor autentication

Use the Google Authenticator or Authy to scan this code.

Print this page and keep it in a safe place. If you cannot create verification codes, you will not be able to access your account.

For manual setup, use:

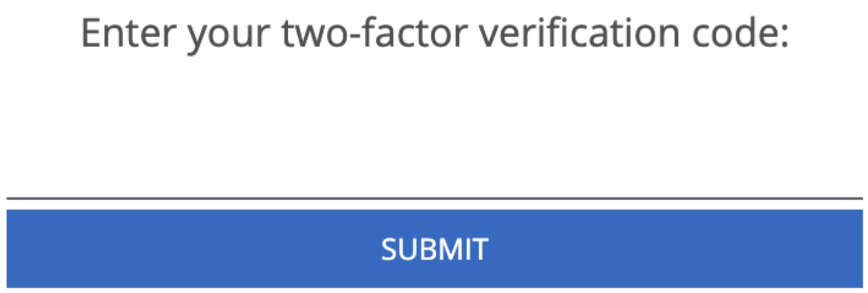
Account: connect.acronis.com:alan@example.com

Key: J3FX5TUHW77SQWO7

Enter the verification code to confirm:

Remember to save the QR-code and/or secret key and account name, so you can setup any other authorizing app in case you lose one.

After you enable two-factor authentication, you must enter an additional code every time you log in to the Cyber Protect Connect console.


Enter your two-factor verification code:

We use Time-based One-Time Password (TOTP) protocol. To generate a PIN you can use any application that implements it: Google Authenticator or Authy. You can also learn more about TOTP in Wikipedia.

Using Teams functionality

The Teams functionality in the Acronis Cyber Protect Connect console requires the Professional license.

The functionality is designed for companies that need to manage multiple computers or groups of computers, and to control access rights for groups of users. It features:

- team user management
- team workloads management
- access group management
- team activity log
- team session history
- custom agent configuration and builds
- setting up SSO

Team user roles

Team users are the people who will be allowed to perform different actions related to the team, depending on their user role.

Admin role

By default, the creator of the team becomes the first user in the team. The admin role is automatically assigned to the creator of the team.

Admin users can perform the following actions:

- create or delete a team
- configure team settings
- manage invited team users (invite, remove from team, block, change role, and grant permissions)
- manage manually added users (add, delete, block, change password, rename, change role, and grant permissions)
- manage team computers (import or remove)
- monitor team computers
- configure access groups

User role

Regular users can monitor the computers to which the user has access, according to the access groups. The information that they see depend on the permissions that they are granted by the Admin users.

Logging in with Single sign-on

Prerequisites

Single sign-on (SSO) is configured successfully in the Acronis Cyber Protect Connect console.

To log in to the Acronis Cyber Protect Connect console

1. On the Acronis Cyber Protect Connect console login screen, click **Continue with SSO**.
2. Enter your team alias.
3. Click **Submit**.

Working with Teams as an Admin user

Creating a new team

You might need to create a new team - a group of computers that would be accessed and managed by a specific group of users.

To create a new team

1. Click **New team**.
2. In the **Enter team name** field, enter the name of the new team.
3. Click **Create**.

The new team is created. The new team has no computers, and you are added in the team as a default Admin user.

Note
The **Team ID** of the new team is generated automatically, and displayed on the team's **Dashboard** page. To provide the team users with access rights to a remote computer, add the **Team ID** to the **Trusted users** list in Acronis Cyber Protect Connect agent.

Configuring Single sign-on (SSO) access

As a team administrator, you can configure SSO access for the team.

To configure SSO access for the team

1. On the team's **Dashboard** screen, click **Set up SSO**.
2. In the **SSO Setup Wizard**, click **Set up**.
3. Enter a team alias, and then click **Next**.

   Note
   The team alias must be unique for the system. It can only consist of letters, digits, or dashes.

4. Select the **SSO protocol**.
5. Select the **SSO provider**.
6. Click **Next**.
7. Enter the **Provider-specific settings**.

   For more information about the provider-specific settings, see "Single sign-on providers" (p. 50).
8. Click **Next**.
9. Enter the **Custom claims mapping**.

   For more information about custom claim mappings, see "Custom claims mapping" (p. 53).
10. Click **Save**.
11. Add the Callback URL to the provider's list of Authorized redirect URIs.
12. Click **Close**.

SSO protocols

The Single sign-on (SSO) protocol is a protocol that is used between the server and the identity provider (IDP) to authorize users. The SSO protocols are supported by different SSO providers.

Acronis Cyber Protect Connect console supports the following SSO protocols:

- **OAuth**. For more information about OAuth2, see https://oauth.net/2/.
- **SAML**. SAML is a complicated protocol. It requires a TLS private key, a related TLS certificate, and an IDP metadata file.

Single sign-on providers

The **SSO Provider** is an identity provider (IDP) that supports an **SSO protocol**. The various SSO providers use slightly different flow and parameters.

Note that the callback URL, required by most providers, will be available only after you configure the IDP settings.

SSO provider	Supported SSO protocol	Required parameters
Google: https://support.google.com/cloud/answer/6158849?hl=en	**OAuth**	**Client ID**—Usually, administrators can obtain them during the application registration on the IDP's site. **Client secret**—Usually, administrators can obtain them during the application registration on the IDP's site.
Okta: https://developer.okta.com/docs/guides/implement-oauth-for-okta/main/	**OAuth**	**Client ID**—Usually, administrators can obtain them during the application

SSO provider	Supported SSO protocol	Required parameters
		registration on the IDP's site. **Client secret**—Usually, administrators can obtain them during the application registration on the IDP's site. **Origin**—An Okta-related field that usually means the company URL, for example, `https://company.okta.com`. **Scope**—OAuth2-related information; the set of claims that IDP should provide. The server usually tries to obtain the `openid`, `email`, and `profile` scopes, which should be allowed on the IDP side. You can specify additional scopes related to specific IDP, but the `email` claim is mandatory. Ensure that the IDP can return it.
Auth0: https://auth0.com/docs/login/authentication	**OAuth**	**Client key**—Usually, administrators can obtain them during the application registration on the IDP's site. **Client secret**—Usually, administrators can obtain them during the application registration on the IDP's site. **Domain**—An Auth0 domain name. For more information, see the Auth0 documentation. **Scopes**—The scope is a set of related claims. The server always sends the OpenID, Email, and Profile scopes. You can add more scopes using comma separated values, or you can leave the field empty.
Azure AD:	**OAuth**	**Client key**—Usually,

SSO provider	Supported SSO protocol	Required parameters
https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/auth-oauth2		administrators can obtain them during the application registration on the IDP's site. **Client secret**—Usually, administrators can obtain them during the application registration on the IDP's site. **Resources**—An Azure AD-related setting. For more information, see https://docs.microsoft.com/en-us/graph/api/resources/azure-ad-overview?view=graph-rest-1.0. **Scopes**—The server always sends the OpenID, Email, and Profile scopes. You can add more scopes using comma separated values, or you can leave the field empty.
OpenID Connect	**OAuth**	**Auto-discovery URL**—An OpenID Connect URL that the IDP provides to the public. It contains information about authorization methods and endpoints.
SAML	**SAML**	**Private key file**—Choose the file containing the private key. If you do not have keys, you can generate them. For example, `openssl req -x509 -newkey rsa:2048 -keyout service.key -out service.cert -days 365 -nodes -subj "/CN=service.example.com"` **Certificate file**—Choose the file containing the certificate. **IDP metadata file**—Choose

SSO provider	Supported SSO protocol	Required parameters
		the file containing the IDP metadata. **Force authn**—Forces the user to log in again even if IDP providers usually allow to reuse the login state. This setting will work only if the IDP side supports it. **Allow IDP-initiated login**—Enable this option if you want to allow the IDP to start the login process. After the setup is completed, you can download the SP part of the metadata and feed it to the IDP. After that, your SAML SSO is fully configured.

Custom claims mapping

Custom claims are used in Single sign-on (SSO) protocols to get data for specific fields from the SSO providers.

With some SSO providers, you might need to map the field names that are used in the console to the field names that are used by the SSO providers. Currently, each provider has a predefined set of claims mapping. For example, a mail claim usually gets the user's email address. If you send claims that the SSO provider does not recognize, you might encounter errors during the login process. You can manually set the mapping of the claims and avoid such errors.

The name of fields that Acronis Cyber Protect Connect console tries to get from the provider are the following:

- **Unique user ID**
- **First name**
- **Last name**
- **Email**
- **Phone number**
- **User role**

Configuring email-based two-factor authentication for a team

On a team level, you can enable login by using email-based two-factor authentication (2FA) and specify the time period for automatic session timeout. In that way, when the session timeout expires the system will automatically log out team members from the console and will require them to log in to the console again by using a two-step process: entering username and password, and providing a verification code which the system sends to user's email address.

2FA provides an additional level of protection against unauthorized access to the team's information.

To configure email-based two-factor authentication for the team

1. In the Cyber Protect Connect console, open the team's **Dashboard** page.
2. In **Force email-based 2FA**, select the appropriate time interval after which the system will automatically log out the team users and require their re-authentication using email-based 2FA.

   Note
   If you select the **Once after login** option, the system will require authentication using email-based 2FA only once when the user logs in, and will not automatically log out the user.

Managing team users

As an admin user, you can add or invite users to the team, limit their access to computers by adding them to different access groups, delete or block users, change user roles, and configure user permissions.

Inviting a user to the team

You can send an email invitation to a user to join the team.

Note
The actions that admin users can perform on invited users differ from the actions that they can perform on the created users.

Admin users cannot delete accounts of invited users, and cannot change their names or passwords.

Admin users can remove invited users from the team, but their console accounts and managed computers (if any) will not be deleted.

To invite a user to the team

1. On the team's **Dashboard** page, click **Invite users**.
2. Click the **Invite users** tab.
3. Enter the email address of the user that you want to invite to the team.
4. Click **Invite**.

An email invitation to join the team is sent to the specified email address. The user is added to the team's **Users** list. An **invitation sent** label indicates that the user has not accepted the invitation yet.

Creating a new team user

You can manually create a new team user.

To create a new team user

1. On the team's **Dashboard** page, click **Invite users**.
2. Click the **New user** tab.
3. Enter the name of the user.
4. Enter the email address of the user.
5. Select the **Role** of the user.
6. Enter a password for the user.
7. Click **Add**.

Configuring user permissions

You can configure if a functionality will be available for a certain user by enabling or disabling the feature in the user's **Info** page.

To configure user's permissions

1. On the team's **Users** page, click the user.
2. In the **Permissions** section, enable or disable the switch to configure if the user will be allowed to use each of the following functionalities.
   - **Remote actions**
   - **Chat**
   - **Edit computers**
   - **Remote control**
   - **Location**
   - **Report**
   - **Screenshots**

Adding users to an access group

You can create an access group and add users to it. In this way, you can limit the access to certain computers and allow only the selected users to access and manage them. All users of an access group have access to all computers that belong to the group.

For example, you can use access groups to group people and computers working on the same project. If some users leave one project and start working on another one, you can change their access group, and will not need to add and remove the users manually from each of the affected computers. The same applies to adding or removing computers from the access group.

To create an access group

1. On the team's **Access groups** page, click **Add access group**.
2. Enter a name for the access group, and click **Add**.
3. In the **Users** section of the access group, click **Add**.
4. Select the users that you want to add to the access group, and then click **Save**.
5. In the **Computers** section of the access group, click **Add**.
6. Select the computers that you want to add to the access group, and then click **Save**.

Adding computers to the team

You can select computers from the **COMPUTERS** list, and add them to the team.

To add computers to the team

1. On the team's **Dashboard** page, click **Import computers**.
2. In the **Import computers** list, select all computers that you want to add to the team.
3. Click **Import**.

   The computers you selected are added to the team. You can view them in the team's **Computers** page.

   Note
   The functionality that is implemented in the team's **Computers** page is the same as the functionality that is implemented in the **All computers** page, but usually there are less computers in the team, only the ones that are managed by the team.

Team activity log

In the team's **Activity log** page, you can view detailed information about the team actions, such as:

- time when the action was performed
- user who performed the action
- IP address of the computer from which the user performed the action
- additional information about the action. For example, if the action was completed successfully.

If you are interested in a specific action, you can set filters and limit the number of activities that are displayed in the page.

Adding a custom agent configuration

You can define and create a custom agent configuration by using the **Add Configuration** button from the team's **Custom agents page**.

In this case, the system will create the custom agent build with your configuration. You can download this build from the console and distribute it to the appropriate computers.

Note
Custom agent builds are supported only for Windows and macOS.

Automatic distribution of custom agent configuration updates

When you update an existing custom agent configuration, the changes are automatically distributed and applied to all workloads on which this custom agent configuration is installed. This happens without any manual actions on the workloads, such as downloading the new build, and installing it.

Prerequisites

At least one custom agent configuration is available and is applied to at least one workload in the team.

To update a custom agent configuration and distribute it automatically

1. Open the **Custom agents** page of the team.
2. Click the name of the custom agent configuration.
3. Click **Edit settings**.
4. Update the configuration as needed, and then click **Save**.

   The Acronis Cyber Protect Connect console displays a warning with the number of workloads that will be affected by the change.
5. Click **Save**.

Viewing session history

On the **Session history** page, you can view the following information about the team or specific users:

- the sessions that were established
- the time of the sessions
- the source and target computer
- the duration of the session.

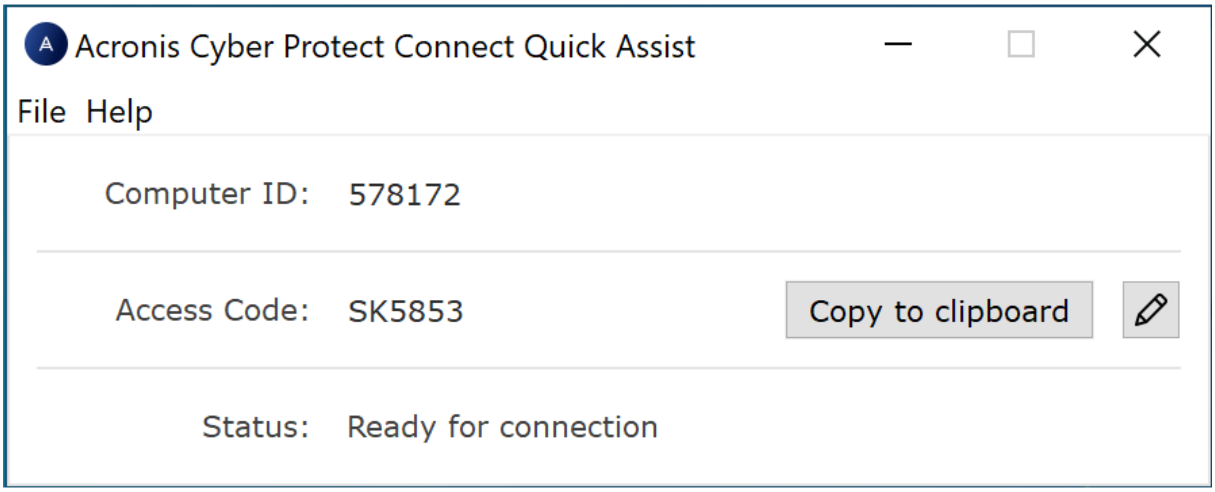
Working with Teams as a User

Team users who are assigned the **User** role can use the features described in "Cyber Protect Connect console main features" (p. 44).

The number of team computers that the users will see, and the actions that they will be able to perform on them, depend on the permissions that the users were granted, and the access groups to which the users belong.

Cyber Protect Connect Quick Assist

Acronis Cyber Protect Connect Quick Assist is a tiny portable application with zero configuration. While running, it enables remote connections to the target computer.

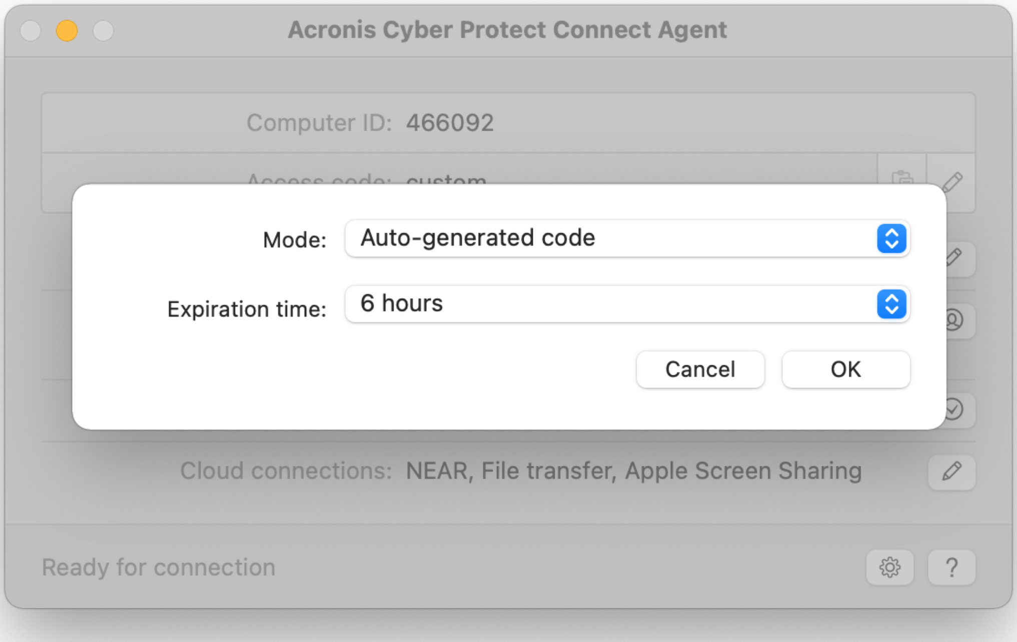


Computer ID: 578172

Access Code: SK5853

Status: Ready for connection

To let someone access your computer remotely over the Cloud, tell them your **Computer ID** and **Access Code** that are shown in Cyber Protect Connect Quick Assist. The parameters of the access code are configurable. You can also set your own code.



Computer ID: 466092

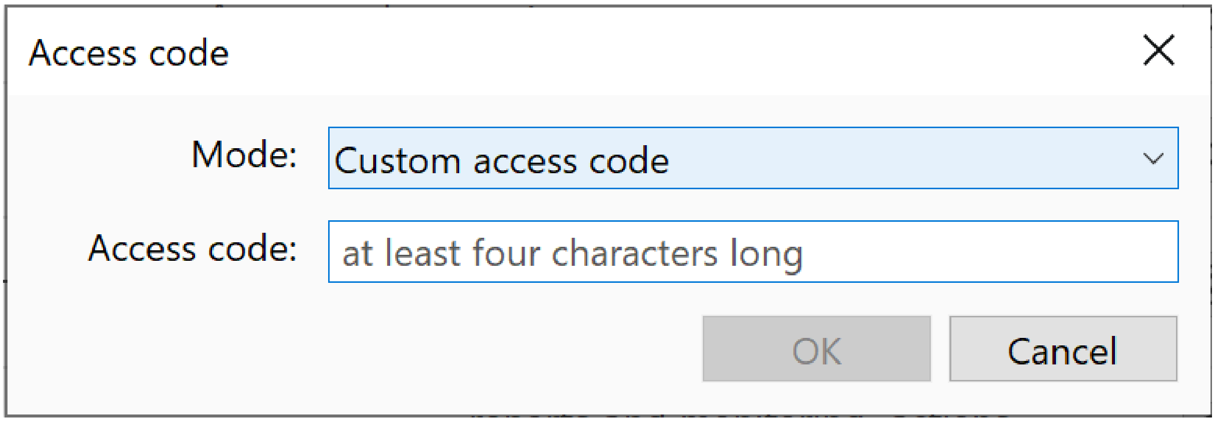
Access code: custom

Mode: Auto-generated code

Expiration time: 6 hours

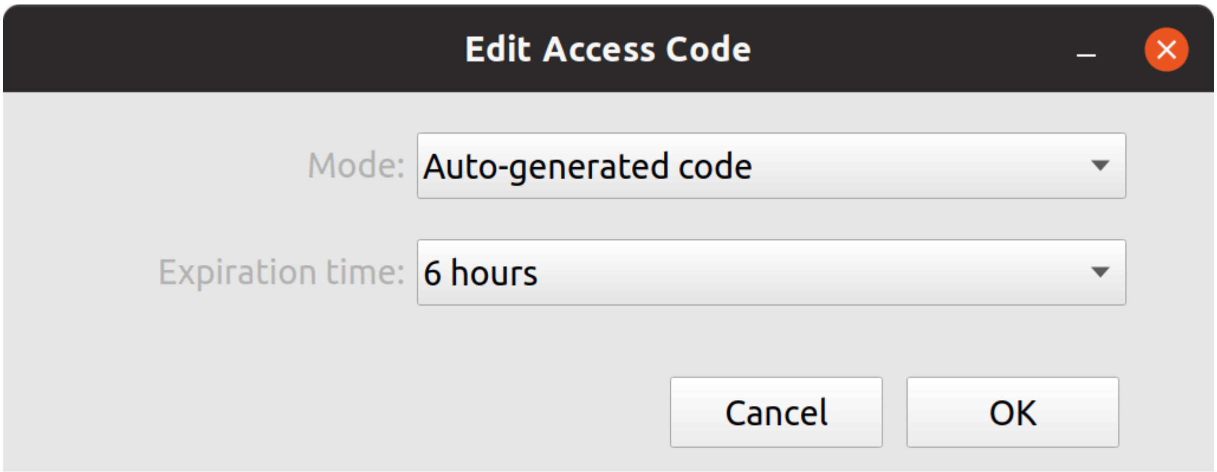
Cloud connections: NEAR, File transfer, Apple Screen Sharing

Ready for connection



Mode: Custom access code

Access code: at least four characters long



Mode: Auto-generated code

Expiration time: 6 hours

- To copy **Computer ID** and **Access Code** to clipboard, click **Copy to Clipboard**.

User account control on remote Windows workloads

Acronis Cyber Protect Connect Quick Assist supports UAC on remote Windows workloads. Using UAC, administrators (IT technicians) can perform tasks that require administrator rights on the remote workloads.

Prerequisites

- User Account Control (UAC) is enabled on the remote Windows workload.
- Cyber Protect Connect Quick Assist is run on the remote workload.
- The administrator connects to the remote workload using the system logon authentication option. For more information, see "Connecting to remote workloads using Acronis Cyber Protect Connect Quick Assist" (p. 108).
- The administrator uses local administrator credentials for authentication when establishing the remote connection to the workload.

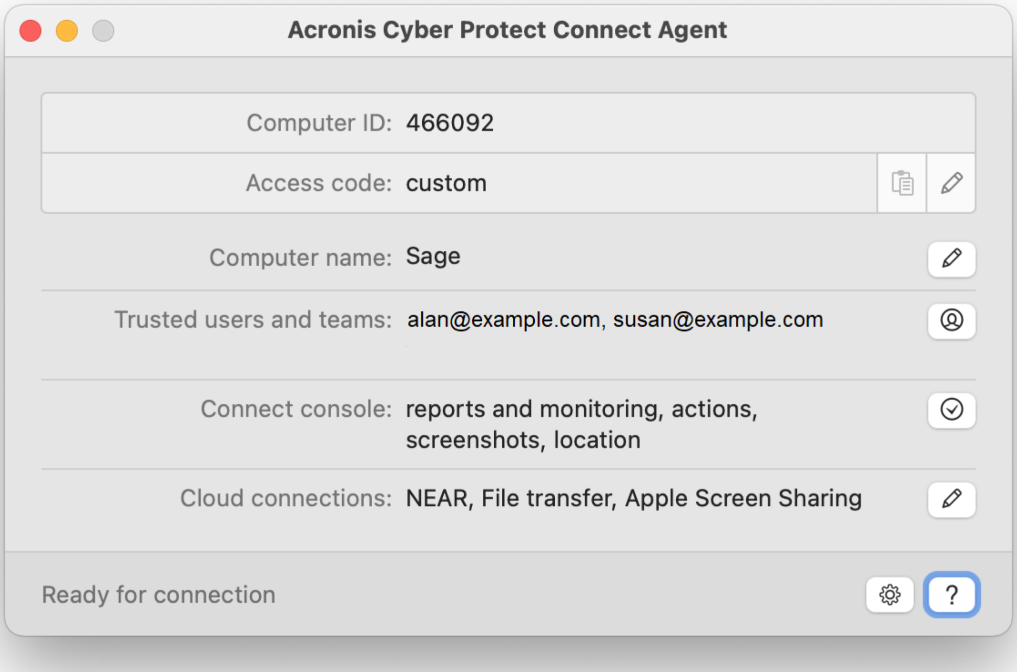
If the administrator connects to a standard (non-administrator) user session on the remote workload and attempts performing a task that requires administrator rights, the system will show a

UAC credential prompt. After providing the password of the default Administrator account of the remote workload, the administrator will be allowed to perform the task.

If the administrator connects to an administrator user session on the remote workload and attempts performing a task that requires administrator rights, the system will show a UAC consent prompt. After confirming the message, the administrator will be allowed to perform the task.

Cyber Protect Connect agent for Mac

Main window



Computer ID: 466092

Access code: custom

Computer name: Sage

Trusted users and teams: alan@example.com, susan@example.com

Connect console: reports and monitoring, actions, screenshots, location

Cloud connections: NEAR, File transfer, Apple Screen Sharing

Ready for connection

Your ID and Access Code

To give someone a remote access to your computer over the Acronis Cyber Protect Connect Cloud, tell them your **Computer ID** and **Access Code** that are shown to the right.

The **Computer ID** is assigned automatically during the first installation of Acronis Cyber Protect Connect agent. If you uninstall the Agent and then install it again, your **Compute ID** will remain the same.

- To copy your **Computer ID** and **Access Code** to the clipboard, click **Copy to Clipboard**.
- To change your **Access Code**, click **Edit Authentication Type**. For more information, see Change access code.

Computer Name

Computer name determines the name of your computer in the Acronis Cyber Protect Connect console web interface and in the Acronis Cyber Protect Connect client.

Trusted Users

Trusted Users is the list of the Cyber Protect Connect Cloud users who can connect to this computer. See Trusted Users.

AcronisCyber Protect Connect console

The Acronis Cyber Protect Connect console is the list of permissions for Acronis Cyber Protect Connect console. See Acronis Cyber Protect Connect console permissions section.

Remote Connections

The **Remote Connections** section lists all remote connection protocols enabled for a given computer. NEAR is on by default. Please refer to Remote Connections.

Status Line

The status line at the bottom displays the current Cyber Protect Connect agent status.

Status	Meaning
Ready for connection	Cyber Protect Connect agent is connected to the Cloud and is ready to receive incoming desktop sharing connections.
Remote controlled	Your computer is being controlled remotely over Cyber Protect Connect Cloud.
Turned Off	The Cyber Protect Connect Cloud connection is disabled. To enable it, click the Agent icon in the system menu and choose **Turn Agent On**.
Connecting...	Cyber Protect Connect agent is trying to establish connection to the Cyber Protect Connect Cloud.
No connection	Cyber Protect Connect agentis unable to establish a connection to Cyber Protect Connect Cloud. Check your Internet connection.
Waiting for background process...	The Cyber Protect Connect agent daemon service is unavailable. If this issue does not resolve, contact the Support team.
Agent upgrade required	Your Cyber Protect Connect agent version is too old. Update the Agent, or download the latest version from our website.
Server Error	The Cyber Protect Connect Cloud server response is incorrect. If you experience this issue for a long time, contact the Support team.

If you want to stop the Agent completely, click the Agent icon in the system menu, and then select **Turn Agent Off**.

Trusted users

This section contains a list of all Acronis Cyber Protect Connect Cloud users, who:

- are allowed to control this computer without entering **Access Code**.
- see this computer in the Acronis Cyber Protect Connect client and Acronis Cyber Protect Connect console.
- can perform actions allowed in the Cyber Protect Connect console pane.

If you enable **Allow trusted users to log in without authentication**, trusted users connecting over NEAR protocol can connect directly without entering any credentials.

To allow someone to connect to this computer without your attendance, add his or her Acronis Cyber Protect Connect Cloud account to the **Users** list.

1. Go to the **Users** pane of Acronis Cyber Protect Connect agent.
2. Click **+**.
3. Enter an existing Cyber Protect Connect Cloud account email, and then click **Add**.

   After the user ID is verified, it will appear in the **Users** list to the right of this pane.

   Now this computer will be automatically added to the computers list of the given user and would appear in the Cyber Protect Connect client and in the Cyber Protect Connect console.

Cyber Protect Connect console

The following options determine the availability of the Acronis Cyber Protect Connect console functionality for the given machine. Note that all Acronis Cyber Protect Connect Cloud users in the Users list will be able to perform all selected functions.

Option	Description
System reports & monitoring	Allow the console to request system reports about your computer. For more information, see Reports.
Remote actions	Allow remote management of this computer, like starting applications, or performing maintenance actions. For more information, see Overview.
Screenshots	Allow the console to request screenshots of your desktop. For more information, see Screenshots.
Location tracking	When enabled, Acronis Cyber Protect Connect agent will automatically send your computer location to the console. You will have to turn on the location services for Cyber Protect Connect agent in **Windows Settings**. For more information, see Map.
Chat	A built-in interactive chat helps you communicate with the remote user or provide a personal assistance.

Option	Description
	Acronis Cyber Protect Connect agent Chat page.

Remote connections

This section is designed to check and set up desktop sharing services available on your computer. For the remote access to work, you need to enable NEAR or Apple Screen Sharing.

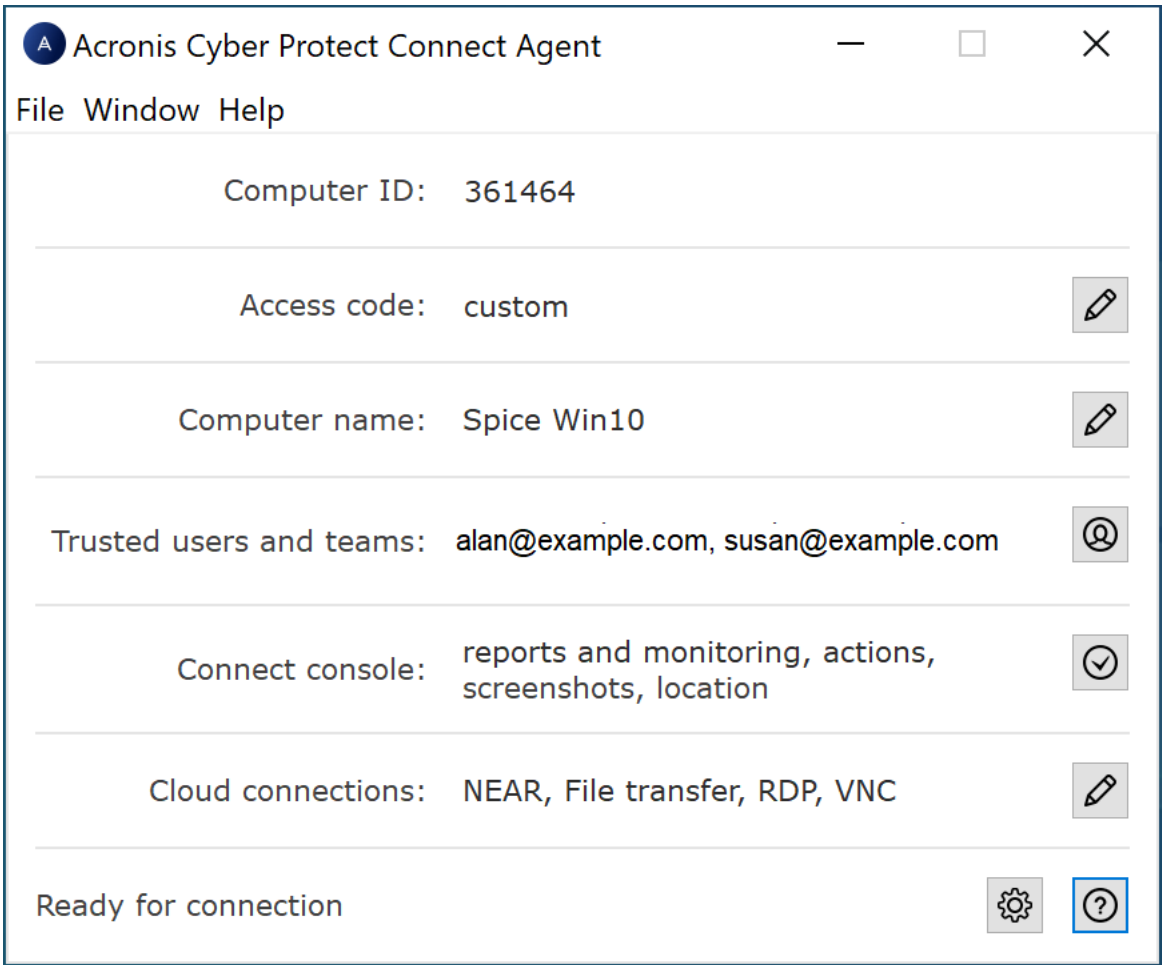
Option	Description
Allow NEAR	Enable to make your Mac controllable with NEAR, an Acronis remote control protocol. For more information, see About NEAR.
Allow File Transfer	Enable to allow file exchange between this computer and the client connected with Acronis Cyber Protect Connect.
Allow Apple Screen Sharing	Enable to make your Mac available to control with Apple built-in screen sharing protocol. Currently, macOS requires Remote Management to be enabled for Curtain mode to work, so if you enable Apple Screen Sharing using Acronis Cyber Protect Connect agent, it enables Remote Management instead of Screen Sharing. Once enabled, Apple Screen Sharing also becomes available system-wide on 5900 port.

Settings

Option	Description
Autostart at system start	Select if Acronis Cyber Protect Connect agent will open automatically at system start.
Hide main window on startup	Select if Cyber Protect Connect agent window will be visible after login.
Automatically check for updates	Select if Cyber Protect Connect agent will check and notify about the availability of updates.

Cyber Protect Connect agent for Windows

Main window



Computer ID: 361464

Access code: custom

Computer name: Spice Win10

Trusted users and teams: alan@example.com, susan@example.com

Connect console: reports and monitoring, actions, screenshots, location

Cloud connections: NEAR, File transfer, RDP, VNC

Ready for connection

Your ID and Access Code

To give someone a remote access to your computer over the Acronis Cyber Protect Connect Cloud, tell them your **Computer ID** and **Access Code** that are shown to the right.

The **Computer ID** is assigned automatically during the first installation of Acronis Cyber Protect Connect agent. If you uninstall the Agent and then install it again, your **Compute ID** will remain the same.

- To copy your **Computer ID** and **Access Code** to the clipboard, click **Copy to Clipboard**.
- To change your **Access Code**, click **Edit Authentication Type**. For more information, see Change access code.

Computer Name

Computer name determines the name of your computer in the Acronis Cyber Protect Connect console web interface and in the Acronis Cyber Protect Connect client.

Trusted Users

Trusted Users is the list of the Cyber Protect Connect Cloud users who can connect to this computer. See Trusted Users.

AcronisCyber Protect Connect console

The Acronis Cyber Protect Connect console is the list of permissions for Acronis Cyber Protect Connect console. See Acronis Cyber Protect Connect console permissions section.

Remote Connections

The **Remote Connections** section lists all remote connection protocols enabled for a given computer. NEAR is on by default. Please refer to Remote Connections.

Status Line

The status line at the bottom displays the current Cyber Protect Connect agent status.

Status	Meaning
Ready for connection	Cyber Protect Connect agent is connected to the Cloud and is ready to receive incoming desktop sharing connections.
Remote controlled	Your computer is being controlled remotely over Cyber Protect Connect Cloud.
Turned Off	The Cyber Protect Connect Cloud connection is disabled. To enable it, click the Agent icon in the system menu and choose **Turn Agent On**.
Connecting...	Cyber Protect Connect agent is trying to establish connection to the Cyber Protect Connect Cloud.
No connection	Cyber Protect Connect agentis unable to establish a connection to Cyber Protect Connect Cloud. Check your Internet connection.
Waiting for background process...	The Cyber Protect Connect agent daemon service is unavailable. If this issue does not resolve, contact the Support team.
Agent upgrade required	Your Cyber Protect Connect agent version is too old. Update the Agent, or download the latest version from our website.
Server Error	The Cyber Protect Connect Cloud server response is incorrect. If you experience this issue for a long time, contact the Support team.

If you want to stop the Agent completely, click the Agent icon in the system menu, and then select **Turn Agent Off**.

Trusted users

This section contains a list of all Acronis Cyber Protect Connect Cloud users, who:

- are allowed to control this computer without entering **Access Code**.
- see this computer in the Acronis Cyber Protect Connect client and Acronis Cyber Protect Connect console.
- can perform actions allowed in the Cyber Protect Connect console pane.

If you enable **Allow trusted users to log in without authentication**, trusted users connecting over NEAR protocol can connect directly without entering any credentials.

To allow someone to connect to this computer without your attendance, add his or her Acronis Cyber Protect Connect Cloud account to the **Users** list.

1. Go to the **Users** pane of Acronis Cyber Protect Connect agent.
2. Click **+**.
3. Enter an existing Cyber Protect Connect Cloud account email, and then click **Add**.

   After the user ID is verified, it will appear in the **Users** list to the right of this pane.

   Now this computer will be automatically added to the computers list of the given user and would appear in the Cyber Protect Connect client and in the Cyber Protect Connect console.

Cyber Protect Connect console

The following options determine the availability of the Acronis Cyber Protect Connect console functionality for the given machine. Note that all Acronis Cyber Protect Connect Cloud users in the Users list will be able to perform all selected functions.

Option	Description
System reports & monitoring	Allow the console to request system reports about your computer. For more information, see Reports.
Remote actions	Allow remote management of this computer, like starting applications, or performing maintenance actions. For more information, see Overview.
Screenshots	Allow the console to request screenshots of your desktop. For more information, see Screenshots.
Location tracking	When enabled, Acronis Cyber Protect Connect agent will automatically send your computer location to the console. You will have to turn on the location services for Cyber Protect Connect agent in **Windows Settings**. For more information, see Map.

Option	Description
Chat	A built-in interactive chat helps you communicate with the remote user or provide a personal assistance. Acronis Cyber Protect Connect agent Chat page.

Remote connections

This section is designed to check and set up desktop sharing services available on your computer. For the remote access to work you need to set up either NEAR, RDP (if available in your version of Windows) or a third-party VNC server.

By default, Acronis Cyber Protect Connect agent checks if there are any active VNC or RDP services available at default ports (5900 and 3389). If you these services working at different ports, you can address it here using **Configure ports...** button in bottom-left corner.

Option	Description
Allow NEAR	Enable to make your workload controllable with NEAR, an Acronis remote control protocol. For more information, see About NEAR.
Allow File Transfer	Enable to allow file exchange between this computer and the client connected with Acronis Cyber Protect Connect client.
Allow RDP	Enable to make your PC available to manage remotely with Windows built-in remote desktop protocol over Acronis Cyber Protect Connect Cloud. If RDP is not configured yet, there will be an **Enable RDP** link below for your convenience. Please note that RDP might be unavailable in some editions of Windows.
Allow VNC	Enable to make your PC available to connect with VNC over Cyber Protect Connect Cloud. This may come in handy when you want to control a computer by VNC, but you do not want to bother with setting a stable IP or hostname. Please note that disabling this only makes it impossible to connect over Cyber Protect Connect Cloud but does not affect the VNC server settings.

Settings

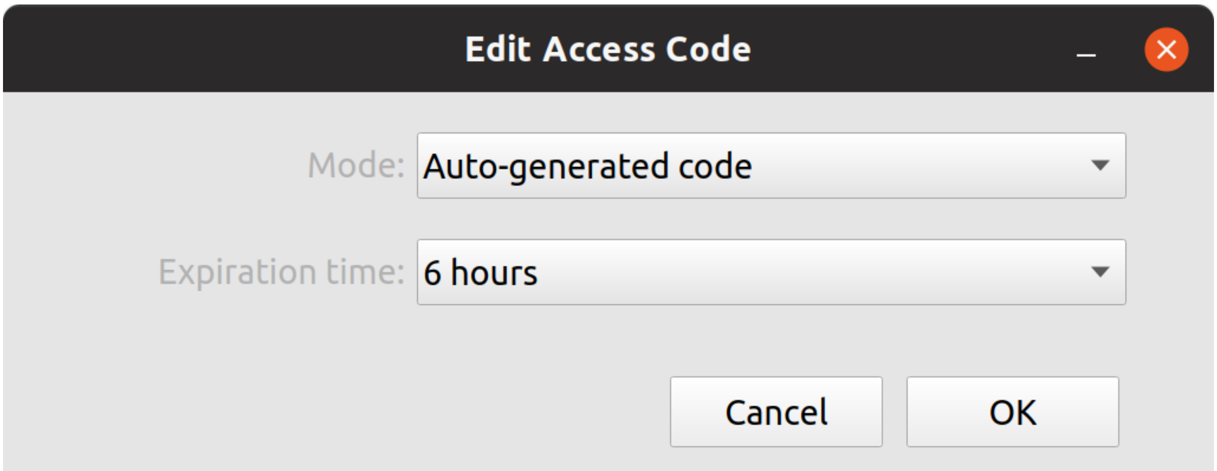
Option	Description
Autostart at system start	Select if Acronis Cyber Protect Connect agent will open automatically at system start.
Hide main window on startup	Select if Cyber Protect Connect agent window will be visible after login.
Automatically check for updates	Select if Cyber Protect Connect agent will check and notify about the availability of updates.

Cyber Protect Connect agent for Linux

Cyber Protect Connect agent for Linux

Acronis Cyber Protect Connect agent is a full-fledged helper application that provides unattended connections to a given computer.

To give someone a remote access to your computer over the Cloud, tell them your **Computer ID** and **Access Code** that are shown in Acronis Cyber Protect Connect Quick Assist. The parameters of the **Access Code** are configurable. You can also set your own **Access Code**.



Edit Access Code

Mode: Auto-generated code

Expiration time: 6 hours

- To copy the **Computer ID** and **Access Code** to the clipboard, click **Copy to Clipboard**.

How to install Acronis Cyber Protect Connect agent on Linux

Installing from a repository

The DEB and RPM packages can be installed from our repository. For more information about the installation, see linux.remotix.com.

Installing from a package

We provide different types of Acronis Cyber Protect Connect for Linux installation packages to ease the process of installing.

Installing Acronis Cyber Protect Connect agent to a Debian-Based Distribution

There is a .deb self-installing package for Ubuntu, Debian and other Debian-based Linux distributions. To get one, go to the Acronis Cyber Protect Connect agent for Linux download page.

Once downloaded, open the package to install it, or open console and run the following command:
`sudo dpkg -i <package path>`.

When installed, Acronis Cyber Protect Connect agent will appear in the **Start** menu and will become available from the console by the `acroniscpcagent --gui` command.

Installing Acronis Cyber Protect Connect Quick Assist to an RPM-Based Distribution

We also made a package for Red Hat Enterprise Linux, Fedora and CentOS distributions. To get one, go to Acronis Cyber Protect Connect agent for Linux (.rpm) download page. Once downloaded, open console and run the following command:
`sudo rpm -i <package path>`.

When installed, Acronis Cyber Protect Connect agent will appear in the **Start** menu and will become available from console by the `acroniscpcagent --gui` command.

Installing Acronis Cyber Protect Connect agent to Raspbian

There is also a separate package for Raspberry Pi-based systems. Currently, the Agent runs smoothly on Raspberry Pi 3 and 4 with Raspbian Buster. To get an installation package, go to the Acronis Cyber Protect Connect agent for Raspberry download page. Once downloaded, open the package to install it, or open console and run the following command:
`sudo dpkg -i <package path>`.

When installed, Acronis Cyber Protect Connect agent will appear in the **Start** menu and will become available from the console by the `acroniscpcagent --gui` command.

Installing Acronis Cyber Protect Connect agent to Azure SLES

(or other Linux that has no graphical desktop environment installed)

To get Acronis Cyber Protect Connect agent running on the SLES VM in Azure, install the Acronis Cyber Protect Connect agent itself (**.rpm** package) and then the graphical desktop environment:

```
sudo zypper install gnome-desktop gdm
```

After that, run the `acroniscpcagent --info` command to get computer ID and access code being logged in over SSH.

Using these ID and code, you will be able to connect with the Acronis Cyber Protect Connect client (to GDM login screen first, and then to Gnome desktop environment once you log in).

Troubleshooting

If Acronis Cyber Protect Connect agent fails to start with an error 'Failed to connect to daemon in time', run the `sudo service acroniscpcagent start` command, or reboot your computer.

Checking dependencies on Linux

Video codec

You can speed up the NVS encoding which is responsible for the **Balanced** quality mode by running some computations on GPU. To do this, install an OpenCL driver on your remote Linux.

The exact driver needed depends on your GPU. Usually, you can find an appropriate package in the repository of your GNU/Linux distro. In some cases, the driver is provided by the GPU vendor.

To verify your OpenCL installation, use the `clinfo` tool (provided by the `clinfo` package that is available for almost every distribution). It will list all the OpenCL platforms and devices available on your computer. Everything is up and ready to run if the tool reports a non-zero number of platforms AND a non-zero number of devices.

To check if Acronis Cyber Protect Connect agent works with OpenCL, start it with logging enabled:

```
acroniscpcagent --gui --nloglevel=debug | grep -i opencl
```

When connected to that computer with the **Balanced** quality chosen, you should see the following on the remote computer's console:

```
20:34:08.514 27015700 [NVSEncoder ] initializing OpenCL.
20:34:08.768 27015700 [NVSEncoder ] OpenCL encoder initialized.
```

This means that OpenCL is successfully utilized.

If you see something like `[NVSEncoder ] OpenCL initialization failed`, it means that the OpenCL initialization has failed and Cyber Protect Connect agent uses CPU computations instead.

Audio codec

The remote sound redirection should work automatically with most Linux distributions. If you are unable to hear remote sound from a Linux, install PulseAudio driver:

```
sudo apt-get install pulseaudio
```

Connecting to a headless Linux

When you try to connect to a Linux computer that does not have a monitor attached, there is no active window server ready to serve your app, and Acronis Cyber Protect Connect agent may fail to start.
To make your remote Linux ready for connection, launch Xvfb, a virtual X-Server, and a window manager. One of the most lightweight ones is fluxbox.

1. Install Xvfb: `sudo apt-get install xvfb`,
2. Connect via **ssh**,

Run the following commands:

```
export DISPLAY=:1
```

```
Xvfb :1 -screen 0 1024x768x24 &
fluxbox &
acroniscpcagent start --gui
```

Note that fluxbox is just an example of a window manager. You may run any other, or even start a full-fledged desktop environment (for exampl., Gnome).

Cyber Protect Connect client

Acronis Cyber Protect Connect is an easy full-service solution for remote desktop management. It consists of the Acronis Cyber Protect Connect client for administrators, Acronis Cyber Protect Connect agent helper application that is installed on the managed computers, and the Acronis Cyber Protect Connect console website to monitor their state remotely.

If you are not familiar with Cyber Protect Connect yet and need help on setting up, see Starter Guide.

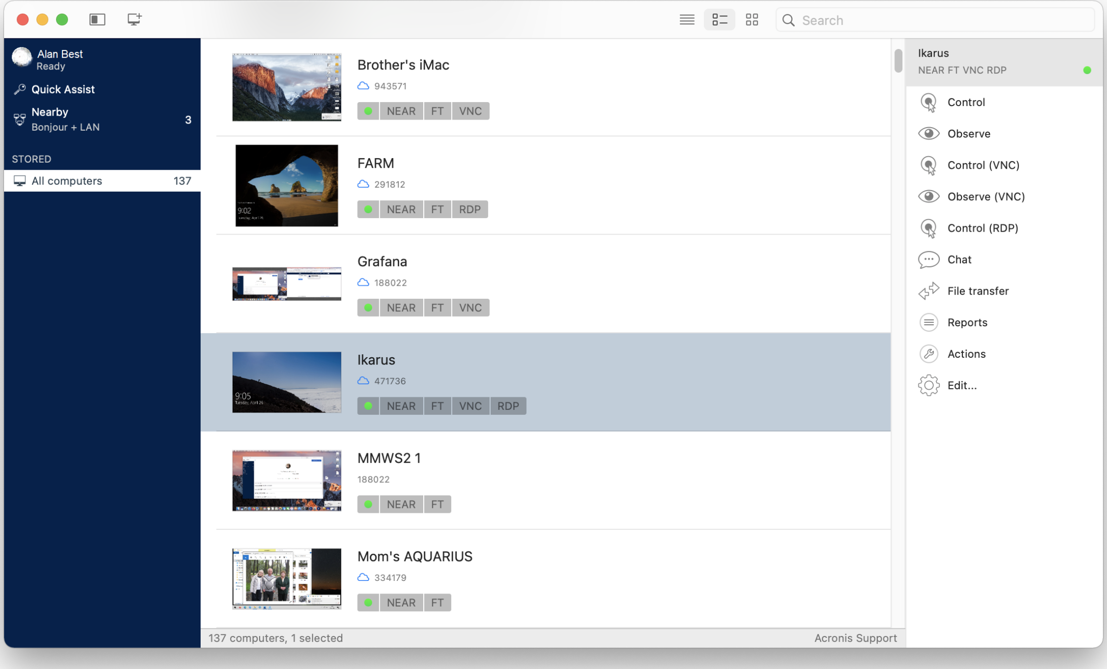
This help section relates to the Cyber Protect Connect client.

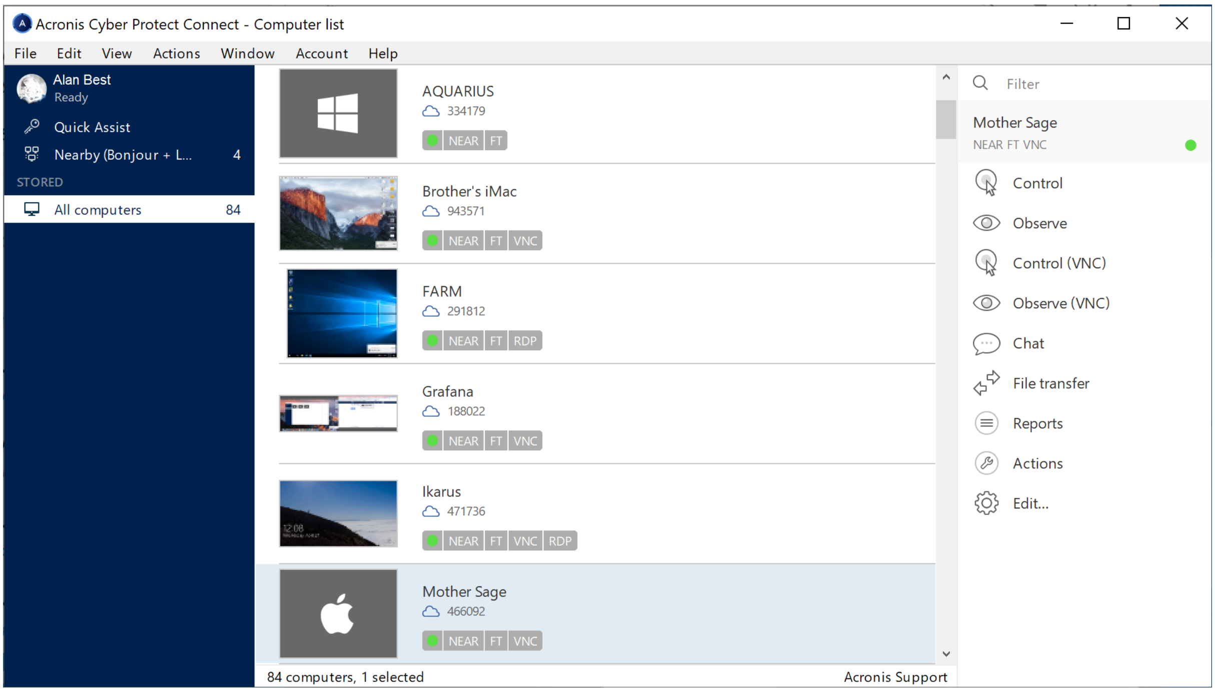
- Using the Cyber Protect Connect client
  - Main window reference
  - Preferences window reference
  - Acronis Cyber Protect Connect menu in the menu bar
  - Protect confidential data with master password
- Cyber Protect Connect Cloud
  - Connect via Acronis Cloud
  - Using Acronis Cloud account
  - Quick Assist using Acronis Cloud
- Connecting to a computer
  - Finding computers
  - Manage stored connections lists
  - Establish a secured connection
  - Connect using Remote Desktop Gateway
  - RDP Performance options, file, sound, and printer sharing
  - About URL syntax
- Interacting & observing
  - Control or observe a single computer
  - Observe multiple computers
  - View the remote desktop
  - Adjust quality for slow connections
  - Transfer files, images, and text between client and server
- Setting up remote access to a computer
  - Setting up remote access to a computer
  - Make VNC or RDP server accessible over the Internet
  - About setting a stable hostname for a computer
  - Configure the firewall to accept incoming connections
  - Configure the network router to accept incoming connections

Cyber Protect Connect client user interface

Main window reference

The main window of the Acronis Cyber Protect Connect client includes a toolbar, hideable list of scanners on the left, and the server list area to the right.





Here is the list of toolbar controls used in main window.

Control	Name and Description
	Hide / show group panel*(Mac only)* Choose whether to show the sidebar with groups.
	New connection*(Mac only)* Create a new connection and customize the settings. See Finding servers.
	View type*(Mac only)* Show found servers as icons, in a list, or in a table.
Search	**Search** Filter servers by name, address or Computer ID.

When you select a computer or a saved connection, a number of options to interact appear in the action pane to the right.

Icon and Name	Description
Control	**Control** Connect to selected computer in Control mode. See Control or observe a single server.
Observe	**Observe** Connect to a selected computer in Observe mode. See Control or observe a single server.
MultiView	**MultiView** Choose more than one computer to connect to all of them simultaneously in Observe mode. See Observe multiple computers.
Control (NEAR)	**Control (NEAR / RDP / VNC / Screen Sharing)** Connect to a selected computer with the given protocol in Control mode. Appears when the given protocol is available and set up on the remote computer. To learn how to set them all up, see: – NEAR: Set up NEAR on Mac and Set up NEAR on Windows, – RDP: Enable RDP access on Windows, – VNC, Screen Sharing: Setting up a server.

Icon and Name	Description
Curtain (NEAR)	**Curtain (NEAR / Screen Sharing)** Connect to a selected computer with NEAR or Screen Sharing in Curtain mode to keep the remote user from seeing what you are doing. Appears when the protocol is available and set up on the remote computer, and the remote computer is running macOS.
Observe (NEAR)	**Observe (NEAR / VNC / Screen Sharing)** Connect to a selected computer with the given protocol in Observe mode. Appears when the protocol is available and set up on the remote computer. Note that RDP connections are always in Control mode so they cannot be observed.
Chat	**Chat** Open chat with selected computer's user. The remote user will see your messages in the Acronis Cyber Protect Connect agent Chat window. Appears for computers that have Cyber Protect Connect agentinstalled and have you listed among Trusted users.
Reports	**Reports** Open a copy of Acronis Cyber Protect Connect Cloud > Reports section in Cyber Protect Connect tab.
Actions	**Actions** Open a copy of Acronis Cyber Protect Connect console > Actions section in a tab.
⚙	**Edit** Customize selected connection settings.
File Transfer	**File Transfer** Open a File Transfer dialog to exchange files between local and remote computers. Appears for computers that have Cyber Protect Connect agent installed.

RELATED INFORMATION

Control or observe a single computer

Preferences window reference

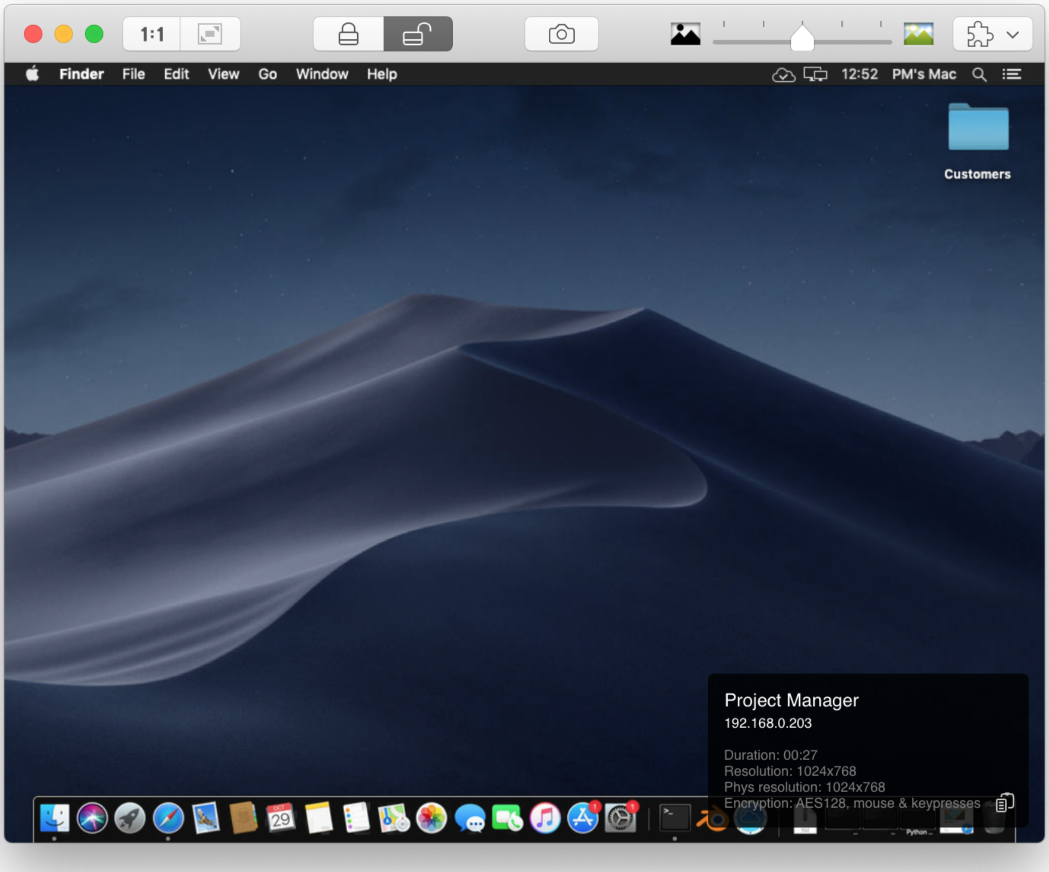
Viewer window reference

Multi-viewer window reference

Viewer window reference

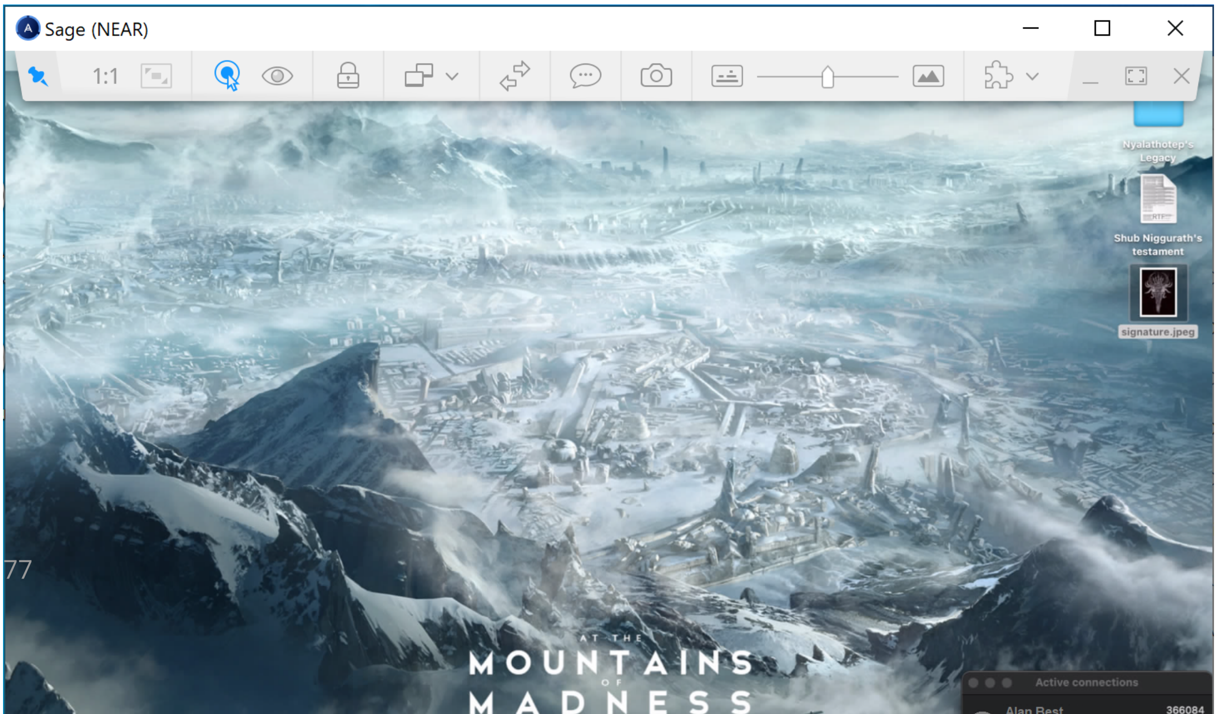
The Viewer window is the same for both controlling and observing a server. The only difference is the state of the Control or Observe toggle button. On NEAR and Apple Screen Sharing connections, you can disable controlling the remote computer by selecting Observe.

The window is resizeable, like a usual application window.

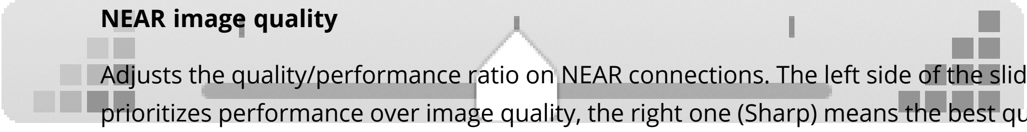
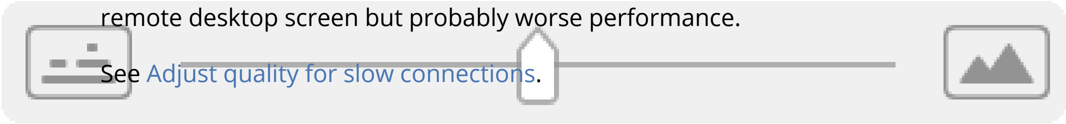
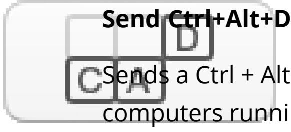
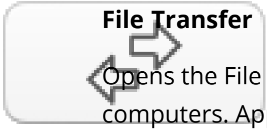
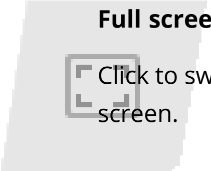
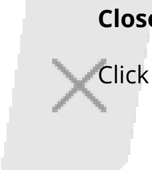


Project Manager
192.168.0.203

Duration: 00:27
Resolution: 1024x768
Phys resolution: 1024x768
Encryption: AES128, mouse & keypresses



Icon	Description
1:1	**Actual size** Click to scale the remote computer's desktop so that every pixel of the remote desktop corresponds to one pixel on the viewer screen.
	Zoom to fit Click to scale the remote computer desktop to fit the viewer window.
	Lock and **Unlock screen** Click the Lock button to show a placeholder on the remote computer's display so that the remote user could not see what you are doing. Works only in NEAR or Apple Screen Sharing connections to a Mac. See Control or observe a single server.
	Take screenshot Click to save the remote server's screen image to a local file. See Capture the remote desktop screen to a file.
	Select display Choose which of the remote computer displays you want to be shown, or select the desired resolution of any display. Appears in Apple Screen Sharing connections to a Mac and NEAR connections to any OS. If your remote computer has multiple displays, you can choose from two multi-monitor display modes: • **Combined** — all remote computer displays are shown within a single window. • **Split** — each remote computer display is shown in a separate window. When you close any of the remote computer displays in Split mode, the entire remote connection will be terminated, and you will need to reconnect to the remote computer to view the displays again. If you are using multiple displays on your local machine, you can arrange the remote computer displays between your local ones. Split mode is available for NEAR connections only.
	Desktop Scale Changes the remote computer GUI scale from 100% to 200% on RDP connections. ‘Auto' means that the remote desktop's current value will be used.
	Image quality Adjusts the remote screen image quality from black and white to the highest possible on Apple Screen Sharing connections. See Adjust quality for slow connections.

Icon	Description
	Bits per pixel Adjusts the screen color depth from 8 to 32 bits per pixel on non-Mac VNC connections. See Adjust quality for slow connections.
 	**NEAR image quality** Adjusts the quality/performance ratio on NEAR connections. The left side of the slider (Smooth) prioritizes performance over image quality, the right one (Sharp) means the best quality of remote desktop screen but probably worse performance. See Adjust quality for slow connections.
	**Send Ctrl+Alt+Del** Sends a Ctrl + Alt + Delete sequence to the remote OS. Available only when connected to computers running Windows or Linux.
	**File Transfer** Opens the File Manager window that allows you to exchange files between remote and local computers. Appears on NEAR connections only.
	Pin toolbar*(Windows only)* Turns off automatic hiding of viewer toolbar.
	**Full screen***(Windows only)* Click to switch to the full screen mode and scale the remote computer to completely fill your local screen.
	**Close***(Windows only)* Click to close the Viewer window and end the remote control session.

Depending on connection type, some options might appear in the Other section marked with a puzzle icon.

Option	Description
Start Recording… / Stop Recording	*Available on NEAR connections only* Starts or stops recording the current remote control session. See Recording sessions.

Option	Description
Clipboard Auto Sync	*Available on NEAR and Screen Sharing connections* When this option is on, the Cyber Protect Connect client will automatically synchronize your local clipboard and the clipboard of the remote computer. See Share clipboards between client and server.
Send Clipboard **Get Clipboard**	Click Send Clipboard is to replace the remote computer clipboard contents with the contents of the local clipboard. Get Clipboard is used to transfer the contents of the remote computer clipboard to the local clipboard. See Share clipboards between client and server.
Smart keyboard / Raw keys / Raw keys with all shortcuts	Choose between keyboard input modes for the current connection. Smart means that the Cyber Protect Connect client transmits Unicode codes of the locally typed symbols to the remote computer while Raw uses the raw codes of the keyboard buttons you press. ‘Raw keys with all shortcuts' mode disables local system shortcuts so that they are all also transmitted to the remote OS.
Keyboard focus on mouse hover	When turned on, the Cyber Protect Connect client only captures the keyboard input while your local mouse cursor is placed over the Cyber Protect Connect Viewer window. When disabled, the Cyber Protect Connect client captures your keyboard whenever its window is active.
Send Force Quit	*Available when connected to macOS* Click to ask remote macOS to show the Force Quit Applications window. See How to force an app to quit on your Mac.
Reports	*Appears only for Cyber Protect Connect Cloud connections* Clicking Reports opens a new tab with collected information about the computer you are connected to. The page is similar to Reports section of the Acronis Cyber Protect Connect console. See Reports.
Logout	*Appears only for Cyber Protect Connect Cloud connections* Opens a new tab with commands to manage the remote computer where you can log out the selected user. Click the action row to choose which user will be logged out. See Actions on the Overview page.
Reboot	*Appears only for Cyber Protect Connect Cloud connections* Opens a new tab with commands to manage the remote computer where you can make it to reboot. Click the action row to choose if the remote user will be allowed to save changes or cancel restart or not.

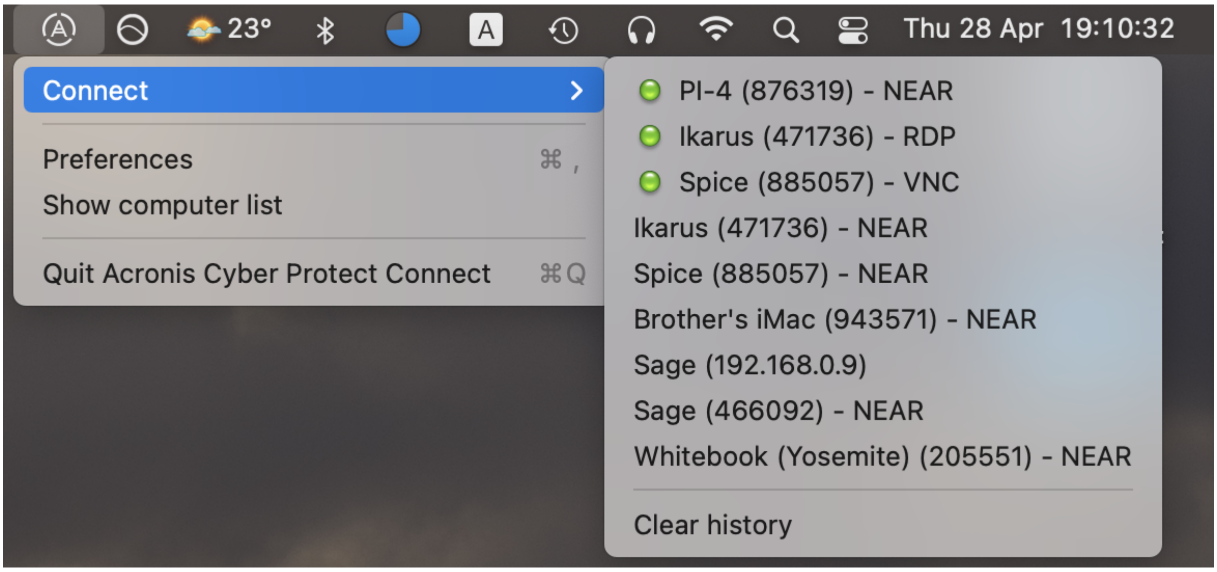
Option	Description
	See Actions on the Overview page.
Sleep	*Appears only for Cyber Protect Connect Cloud connections* Opens a new tab with commands to manage the remote computer where you can put the remote computer to sleep. See Actions on the Overview page.
Shutdown	*Appears only for Cyber Protect Connect Cloud connections* Opens a new tab with commands to manage the remote computer where you can make it to shut down. Click the action row to choose if the remote user will be allowed to save changes or cancel shutdown. See Actions on the Overview page.
Empty Trash	*Appears only for Cyber Protect Connect Cloud connections* Opens a new tab with commands to manage the remote computer where you can choose to empty trash for all users on the target computer. See Actions on the Overview page.
Show Connection Info / Hide Connection Info	When Show Connection Info is selected, a small information panel will appear over the remote desktop screen, showing the most essential information about current connection. See Connection info panel.
Remote Sound	*Available on NEAR connections only* Enables the Cyber Protect Connect client to redirect the sound from the remote computer to the local one. See Remote sound in NEAR.
Local Cursor	Choose whether to show a local mouse pointer over a remote computer's screen. You may want to turn this off e.g. when connected to some older versions of macOS that render the remote pointer into the remote desktop image to avoid seeing two pointers at once.
Don't Hide Cursor	Choose whether to ignore the remote OS instruction to hide mouse pointer. This comes useful on Windows connections if there is no physical mouse connected remotely so the remote Windows forces the pointer to hide.
Show Main Window	Click to show the Cyber Protect Connect client's main window (the computer list).

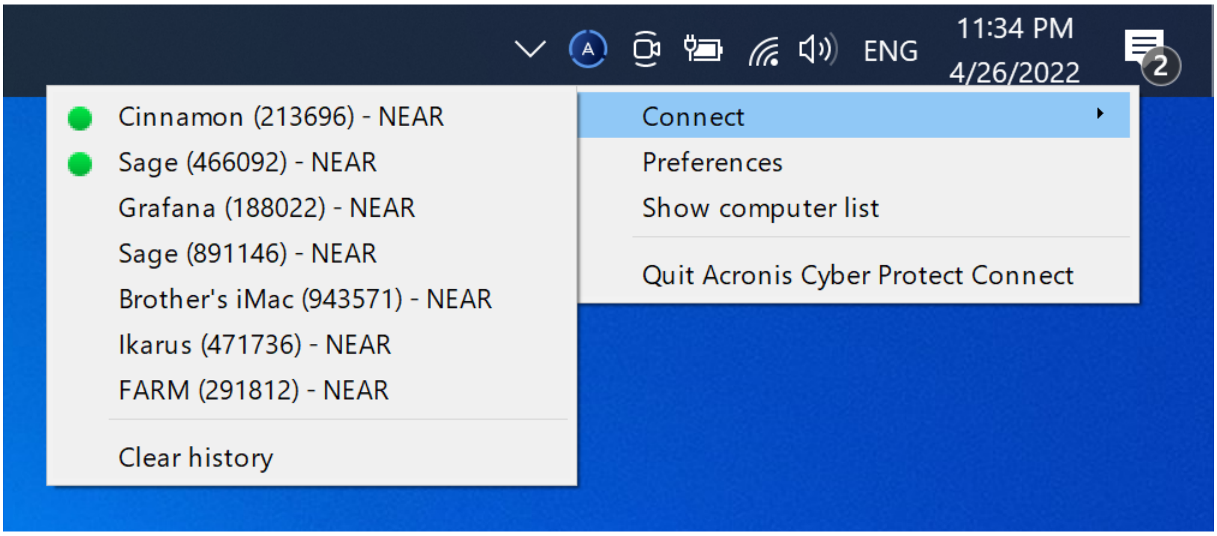
RELATED INFORMATION

Control or observe a single server

Cyber Protect Connect client menu in the system menu

The Acronis Cyber Protect Connect client provides an icon in the system menu (menu bar on macOS, or tray menu on Windows) with links to the most-used Cyber Protect Connect features.





When the Cyber Protect Connect client is open or closed, click the Cyber Protect Connect client icon in the system menu, and then select an option from the menu.

- To quickly connect to one of the ten most recently used servers, click one of them in the **Connect** menu.
- To display the Cyber Protect Connect preferences window, click **Preferences**.
- To show Cyber Protect Connect main window, click **Show Computer List**.
- To quit the application, click **Quit Cyber Protect Connect**.

RELATED INFORMATION

Preferences window reference

Preferences window reference

Use Cyber Protect Connect preferences to set options that affect how you interact with remote servers.

Select **Cyber Protect Connect** > **Preferences...** on a Mac, or **Edit** > **Preferences...** on Windows and set any of the options in the tables below.

General pane

Option	Description
Show icon in Menu Bar *(Mac)* / Show icon in tray *(Windows)*	Choose whether to show Acronis Cyber Protect Connect client icon in the system menu bar or tray. See Acronis Cyber Protect Connect menu in the system menu.
Start Cyber Protect Connect at system startup	Choose whether to launch the Cyber Protect Connect client on system start.
Show Computer List at startup	Choose whether to hide main window at startup.
Install updates automatically	Allow to let the Cyber Protect Connect client keep itself up-to-date without your attention.
Offer beta updates	Enable to get informed about beta versions of the Cyber Protect Connect client available for download.
Acronis Cyber Protect Connect HTTP API	Enable to utilize Acronis Cyber Protect Connect HTTP API for routine actions.
Write verbose logs	Select to allow the Cyber Protect Connect client to write verbose logs. If disabled, the Cyber Protect Connect client only writes general information to the log file.

Security pane

Option	Description
Master password	Set or change master password to protect stored credentials. See Protect confidential data with master password.
Stored passwords	Click **Reset All** to remove all stored passwords from the Cyber Protect Connect client . This action cannot be undone.
Offer saving credentials by default	If enabled, the Cyber Protect Connect client will offer to save credentials for any successful connection automatically.

Viewer pane

Option	Description
Open new viewers as tabs	Select if you prefer new connections to be opened in tabs of the Cyber Protect Connect client main window, or in new windows.
When connected use	Select whether to control the mouse, trackpad, keyboard, and clipboard when connecting to a new computer. See Control or observe a single computer
When controlling	Select whether to allow remote user control of mouse, trackpad and keyboard while you are connected.
When minimized	Select whether to pause Viewer activity to reduce CPU load.
Clipboard transfer indicator	Enable showing the Clipboard transfer indicator in the Viewer window whenever you copy or paste text and images.
Keyboard Mode indicator	Enable showing the Input mode indicator in the Viewer window title whenever mouse and keyboard events are being sent to the remote computer.
Send keyboard events	Choose whether to grab your local keyboard input whenever the Cyber Protect Connect client window is active or only when your local mouse pointer is over it.
Background color	Change the Viewer window background color.

Connection pane

Option	Description
Auto synchronize Clipboard by default	Enable automatic clipboard synchronization when available. See Share clipboards between client and server.
Autoreconnect	Allow the Cyber Protect Connect client to try to re-establish the connection automatically if the connection has been interrupted. See Automatic reconnect.
Enable HEVC *(currently unavailable)*	Select whether to enable HEVC encoder for higher resolutions.

Keyboard pane

Option	Description
Modifier mappings	Change the behavior of modifier keys with a pop-up menu. These settings are stored separately for Apple Screen Sharing, Windows RDP and other VNC connections.
Input mode	For each type of connection (selected in the header of pane), select the default keyboard input mode.

Synchronization

Option	Description
Store computers	Locally / In Cyber Protect Connect Cloud
Cyber Protect Connect Cloud Keychain	Enabled / Disabled
Connections	Upload Session info to Cloud

SSH Tunnels

Option	Description
Connection settings	Host and port settings
Authentification	Type of authentification, username, password

RD Gateways

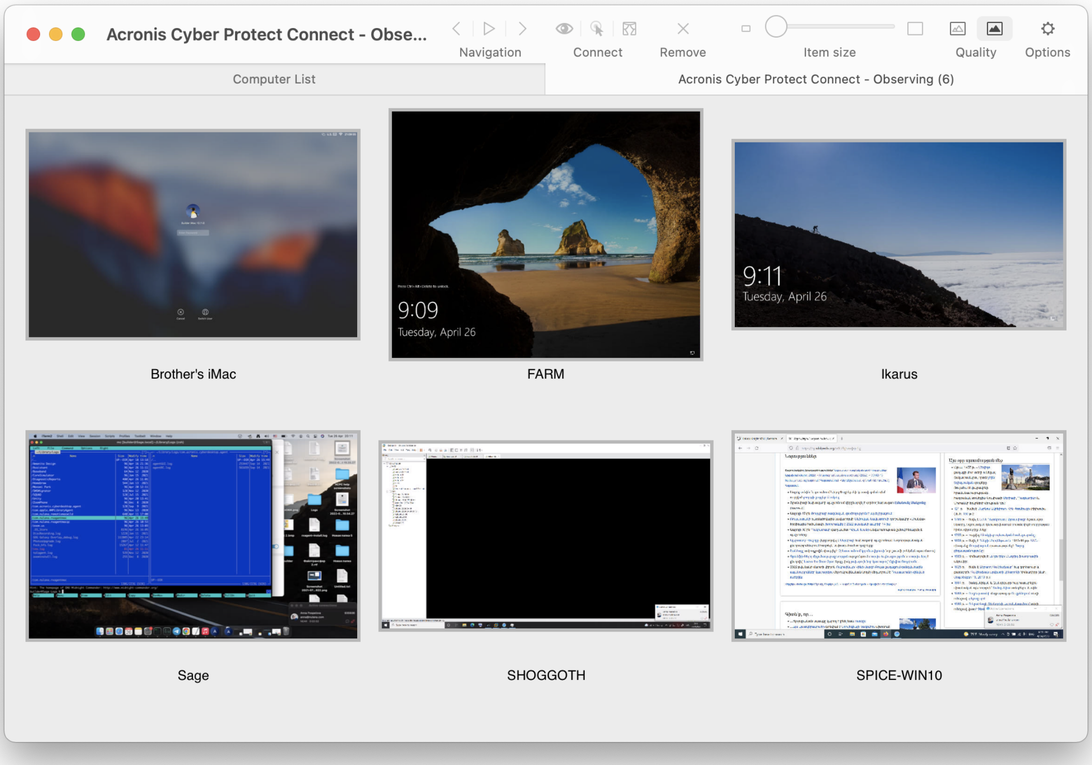
Option	Description
Connection settings	Host, port
Credentials	Username, password, domain.

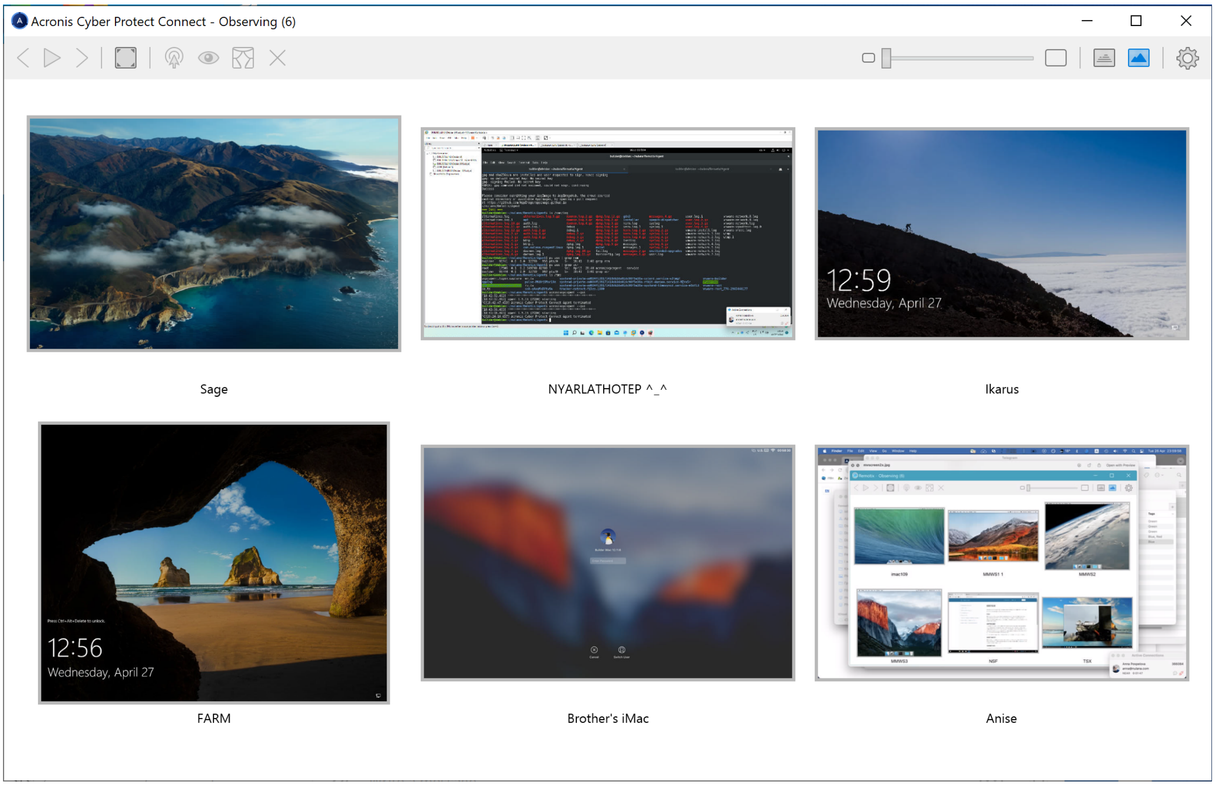
Network

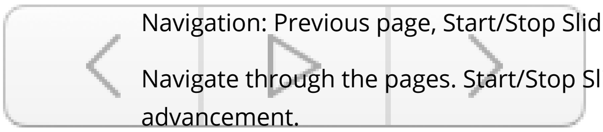
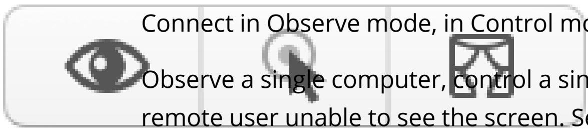
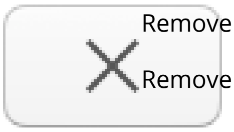
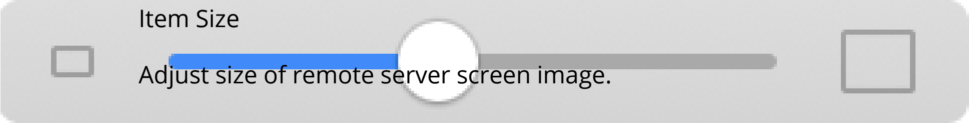
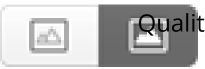
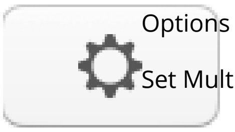
Option	Description
Proxy settings	System proxy / Custom SOCKSS proxy, address, port, username, password
Acronis Cyber Protect Connect Gateway	Acronis Cyber Protect Connect Cloud or other

Multi-viewer window reference

When you observe several servers at the same time, they all appear in the same window. If you are observing more servers than can fit in a window, they are divided across several pages.


Acronis Cyber Protect Connect - Obse...
Navigation
Connect
Remove
Item size
Quality
Options
Computer List
Acronis Cyber Protect Connect - Observing (6)
9:09
Tuesday, April 26
9:11
Tuesday, April 26
Brother's iMac
FARM
Ikarus
Sage
SHOGGOTH
SPICE-WIN10


Acronis Cyber Protect Connect - Observing (6)
12:59
Wednesday, April 27
12:56
Wednesday, April 27
Sage
NYARLATHOTEP ^_^
Ikarus
FARM
Brother's iMac
Anise

Control	Name and Description
	Navigation: Previous page, Start/Stop Slideshow, Next Page Navigate through the pages. Start/Stop Slideshow button toggles an automatic page advancement.
	Connect in Observe mode, in Control mode, or in Curtain mode Observe a single computer, control a single computer or control a single computer with the remote user unable to see the screen. See Control or observe a single server.
	Remove Remove a server from the multi-viewer window.
	Item Size Adjust size of remote server screen image.
	Quality Choose between black-and-white and normal image quality. Lower quality will reduce network and CPU load.
	Options Set Multi-viewer specific options. See Observe multiple servers.

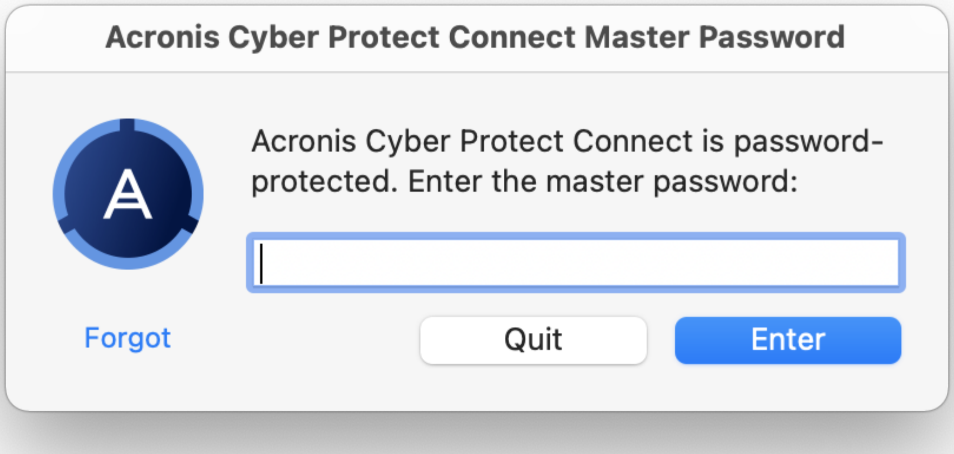
RELATED INFORMATION

Observe multiple servers

Viewer window reference

Protect confidential data with master password

It is possible to protect all the confidential data stored in the Acronis Cyber Protect Connect client with a master password. If the master password is set, the Cyber Protect Connect client will ask user to enter it at every application start. The server list window will be only shown after validating the master password.



Acronis Cyber Protect Connect Master Password

Acronis Cyber Protect Connect is password-protected. Enter the master password:

If forget your master password, you can reset it from the master password request dialog. Note that resetting the password will also reset all credentials stored in the Cyber Protect Connect client, and this action cannot be undone.

Master password is managed from the application preferences (Security pane). To remove master password, enter the old password while leaving the New Password and Confirm Password fields blank.

RELATED INFORMATION

Preferences window reference

Player window reference

The Player window resembles the Acronis Cyber Protect Connect client Viewer where the recordings are made, but without the controlling buttons.

By default, the Cyber Protect Connect client opens the Player in a tab instead of a new window. To make it a separate window, drag the tab out of the tab panel.

There are few toolbar controls available in Player.

Icon	Description
1:1	**Actual size** Click to scale the remote computer desktop so that every pixel of the remote desktop corresponds to one pixel on the viewer screen.

Icon	Description
⤢	**Zoom to fit** Click this button to scale the remote screen image to fit the viewer window.
ⓘ	**Connection Info** Click small information panel will appear over the remote desktop screen, showing the most essential information about current connection. See Connection info panel.
📌	**Pin toolbar***(Windows only)* Turns off automatic hiding of viewer toolbar.
⛶	**Fullscreen***(Windows only)* Click to switch to the full screen mode and scale the remote computer to completely fill your local screen.
✕	**Close***(Windows only)* Click to close the Player window and stop viewing the recording.

The Cyber Protect Connect client player has onscreen playback controls that let you play or pause your recording, and adjust the playback speed.

Icon	Description
↻	tart playback ets the playback and starts it again from the beginning.
▷	s the playback, or resumes it if it was on pause.
🔇	Mute / Unmute Sets the remote sound volume to zero or back to its previous state.
━●─	Volume Allows adjusting the remote sound volume.

Icon	Description
«	Decrease speed Decreases the playback speed by a factor of two, down to 1/4x.
4x	Current speed Shows the currently set playback speed.
»	Increase speed Increases the playback speed twofold, up to 64x. The actual speed boost depends on your CPU capabilities.
01:20 02:08	Shows the current playback position and overall length of the recording.

RELATED INFORMATION

Recording sessions

Cyber Protect Connect Cloud

Connecting via Acronis Cloud

In case the remote computer is behind NAT or firewall, you can use Acronis Cloud to get rid of public IP addresses and firewall configuring. Acronis Cloud is a fast and secure tunneling technology for connecting to remote computers.

Cyber Protect Connect provides two connect options:

- **Acronis Cloud**
  If your Acronis Cyber Protect Connect account has been added to the **Trusted Users** list in Acronis Cyber Protect Connect agent on a certain computer, you can access that computer without entering the **Access Code**. Note that Acronis Cloud provides tunneling only, so in order to get access to the user session, you must know the credentials. See Account.
- Acronis Cyber Protect Connect Quick Assist
  If you have not been granted a trusted access in the Acronis Cyber Protect Connect agent, or you do not have a Cyber Protect Connect account, you can set up a tunnel use by entering the **Computer ID** and **Access Code** for the remote computer. Note that the **Access Code** changes randomly every 30 minutes. See Acronis Cyber Protect Connect Quich Assist using Acronis Cloud.

RELATED INFORMATION

Make VNC or RDP server accessible over the Internet

Finding remote computers

Connecting via Cyber Protect Connect account

To access servers stored in your Acronis Cyber Protect Connect account, you must be logged in.

To log in to Cyber Protect Connect from the Acronis Cyber Protect Connect client

1. In the navigation panel to the left, select **Sign in**.
2. Enter your Cyber Protect Connect credentials in the login form.
3. Once you are logged in, the login form will be replaced with a list of available servers, and your username will appear at the top of the navigation panel to the left.

To log out

1. In the navigation panel to the left, right-click the profile icon.
2. Click **Log out**.

RELATED INFORMATION

Connect via Acronis Cloud

Using Cyber Protect Connect Quick Assist in Acronis Cloud

Acronis Cyber Protect Connect Quick Assist is useful when you need connect to a certain remote computer only for a few times, or if you do not have an Acronis Cyber Protect Connect account.

1. In the navigation panel to the left, select **Quick Assist**.
2. Enter the **Computer ID** and **Access Code** of the target computer.

Note that Acronis Cloud provides tunneling only, so in order to get access to the user session, you must know the credentials.

RELATED INFORMATION

Connect via Acronis Cloud

Connecting to remote computers

Creating a connection

You can either use the built-in scanners of the Acronis Cyber Protect Connect client to find a remote computer, or create a connection manually.

Creating a connection knowing the target Computer ID

To manually add a remote computer that has Acronis Cyber Protect Connect agent installed to the Stored list

1. Choose **File > New Connection** (on a Mac, you can also click **Create New Connection** button in the toolbar).
2. Choose the desired connection type: VNC, RDP or NEAR.

3. In an opened window, fill in the required fields.
4. Ensure that **Use Cyber Protect Connect Cloud** is set to **Yes**.
5. Specify the **Computer ID** of the remote computer and the **Port**. If you leave the **Port** field blank, Acronis Cyber Protect Connect will use the default value (3389 for RDP, 5900 for VNC and 5850 for NEAR).
6. Click **Save**.

   This computer is now stored in the **All Computers** list under the **Stored** section.

Adding a remote computer by IP address

To manually add a connection when you know the IP address or hostname of the target computer

1. Choose **File > New Connection** (on a Mac you can instead click **Create New Connection** button in the toolbar).
2. Choose the desired connection type: VNC, RDP or NEAR.
3. In an opened window, fill in the required fields.
4. Make sure that you have **Use Acronis Cloud** set to **No**.
5. Specify the **IP address** (or hostname) of the remote computer and **Port**. If you leave the **Port** field blank, Acronis Cyber Protect Connect will use the default value (3389 for RDP, 5900 for VNC and 5850 for NEAR).
6. Click **Save**.

   This computer is now stored in the **All Computers** list under the **Stored** section.

RELATED INFORMATION

Control or observe a single server

Finding computers

Using common credentials

In the Acronis Cyber Protect Connect client, you can add credentials (username and password, or NEAR access code), save them in the local credentials store, and then use them for automatic authentication when connecting to the workloads that you manage. In other words, after you specify the credentials on multiple workloads, instead of entering the credentials manually every time during the authentication step for the connection, you can add these credentials to the credentials store once, assign them for multiple different connections, and then the client will use these common credentials for automatic authentications for these connections. For more information about adding common credentials, see "Adding credentials" (p. 93).

You can enable synchronization with the cloud and ensure that the common credentials are available in all Cyber Protect Connect client instances on which you are logged in with the same account. For more information about enabling synchronization, see "Enabling synchronization with the Cloud" (p. 94).

Adding credentials

You can add credentials and then use them for remote connections to multiple workloads.

To add credentials

1. In the Acronis Cyber Protect Connect client, click **Edit** > **Preferences**.
2. Click the **Credentials** tab.
3. Click **Add**.
4. Enter the credentials.

Field	Description
Name	Identifier of the credentials that will be visible in the credentials store in the left part of the **Credentials** tab. Required field for all credentials.
Username	Username that will be used for remote connections to the target workload. If you want to add credentials for a NEAR connection using an access code, leave the field empty.
Password	Password that will be used for remote connections to the target workload. If you want to add credentials for a NEAR connection using an access code, enter the workload's access code in this field. Required field for all credentials.
Comment	A free text field that you can use to add comments or additional information. This field is not required.

5. Click **OK**.

   The credentials are saved on the local workload. If you are using your account with more than one Cyber Protect Connect client instance on several workloads, you can enable synchronization with the cloud and ensure that the credentials are synchronized to all client instances.

Assigning credentials for automatic authentication to a workload

After you add credentials, you can use them to authenticate automatically when you connect to a workload that you manage.

To assign saved credentials for automatic authentication to a workload

1. In the Acronis Cyber Protect Connect client, click **All computers**.
2. Click the connection from the list, and then click **Edit**.
3. For all supported protocols (VNC, Screen Sharing, RDP, or NEAR)
   a. Click **Authentication**.
   b. In the **Use credentials** list, select the credentials that you want to use for remote connection to this workload using this protocol.
4. Click **Save**.

Connecting to a remote workload using saved credentials

After you assign credentials to a workload, you can easily establish remote connections to the remote workloads that you manage without the need to manually enter the required username and password, or access code.

To connect to a remote workload using saved credentials

1. In the Acronis Cyber Protect Connect client, click **All computers**.
2. Click the connection from the list, and then click the appropriate remote connection or file transfer action.

Editing credentials

You can edit credentials that are saved in the credentials store.

To edit credentials

1. In the AcronisCyber Protect Connect client, click **Edit** > **Preferences**.
2. Click the **Credentials** tab.
3. Click the credentials in the credentials store, and then edit them.
4. Click **OK**.

Deleting credentials

You can delete credentials that are not needed anymore.

To delete credentials from the credentials store

1. In the Acronis Cyber Protect Connect client, click **Edit** > **Preferences**.
2. Click the **Credentials** tab.
3. Click the credentials in the credentials store, and then click **Remove**.
4. Click **OK**.

Enabling synchronization with the Cloud

You can enable synchronization for the locally saved credentials. In that way, the saved credentials on your local workload will be synchronized with Acronis Cloud, and then with the other Acronis Cyber Protect Connect client instances with synchronization enabled on which you are logged in using the same account.

Note

The Cyber Protect Connect client uses the following colors in the **Credentials** tab to distinguish between credentials that are available only locally and credentials that are synchronized with the cloud.

- Gray color is used for credentials that are not synchronized with the cloud and are available only locally.
- Black color is used for credentials that are synchronized with the cloud.

To enable synchronization of locally saved credentials

1. In the Acronis Cyber Protect Connect client, click **Edit** > **Preferences**.
2. Click the **Sync** tab.
3. Set **Store computers** to Acronis Cloud.
4. Enable **Acronis Cloud keychain**.
5. Enter the Acronis Cyber Protect Connect keychain password, and then click **OK**.
6. Click **OK**.

Finding remote computers

Acronis Cyber Protect Connect provides several ways to find computers available to connect.

Connect using Acronis Cyber Protect Connect Cloud

If you are a registered user in the Acronis Cyber Protect Connect console, you can use it to connect to a remote computer regardless of its location. For more information, see Starter Guide and Connect via Acronis Cyber Protect Connect Cloud.

1. Select **All Computers** under the **Stored** section in the Cyber Protect Connect sidebar.
2. Computers with yourCyber Protect Connect account listed among the Trusted Users in their Cyber Protect Connect agent will appear in the list. They will be marked with a blue cloud icon.
3. **Double-click** one of these computers.
4. **Authenticate** by providing a username and password.
5. After a successful connection, the credentials will be saved for future use.

Connect using Acronis Cyber Protect Connect Quick Assist

You can use Acronis Cyber Protect Connect Cloud to connect to a remote computer by its Cyber Protect Connect Cloud ID. For more information, see Connect via Acronis Cyber Protect Connect Cloud.

1. Select Acronis Cyber Protect Connect Quick Assist in the Cyber Protect Connect sidebar.
2. Enter a **Computer ID** and access code of the target computer.
3. Authenticate by providing a username and a password.

Note: these connections will not be saved in Stored.

Add a remote computer by Computer ID

You can manually add a remote computer with Acronis Cyber Protect Connect agent installed to the Stored list.

1. Choose **File** > **New Connection** (on a Mac, you can instead click the **Create New Connection** button in the toolbar).
2. Choose connection type (VNC, RDP, or NEAR).
3. In an opened window, specify the new connection name.
4. Ensure that **Use AcronisCyber Protect Connect Cloud** is set to **Yes**.
5. Specify the **Computer ID** and the **Port** of the remote computer. If you leave the **Port** field blank, Cyber Protect Connect will use the default value (3389 for RDP, 5900 for VNC, and 5850 for NEAR).
6. Click **Save**.
7. This computer is now stored in the **All Computers** list under the **Stored** section.

Find a computer in the local area network

The Nearby scanner displays a list of computers on the local subnet available to connect via VNC, RDP, or NEAR. It combines the capabilities of Bonjour technology used by some computers to announce themselves with a NetBIOS scanner for the local area network.

1. Choose a **Nearby (Bonjour + LAN)** scanner in the Cyber Protect Connect sidebar.
2. Double-click one of the found computers.
3. Authenticate by providing a username and password.
4. After a successful connection, the server will appear in the All Computers group in the **Stored** section in the Cyber Protect Connect sidebar.

Add a remote computer by IP address

You can manually add a connection if you know an IP address or hostname of the target computer.

1. Choose **File** > **New Connection** (on a Mac, you can instead click the **Create New Connection** button in the toolbar).
2. Choose connection type (VNC, RDP, or NEAR).
3. In an opened window, specify the new connection name.
4. Ensure that **Use Acronis Cloud** is set to **No**.
5. Specify the IP address (or hostname) of the remote computer and **Port**. If you leave the **Port** field blank, Cyber Protect Connect will use the default value (3389 for RDP, 5900 for VNC, and 5850 for NEAR).
6. Click **Save**.

   This computer is now stored in the **All Computers** list under the **Stored** section.

Connect using Back to My Mac

Back to My Mac is a feature that allows Mac users to connect to their devices across the Internet without bothering about network configuration. It requires user to have Apple ID and iCloud set up in **System Preferences**.

These instructions assume that you have an Apple ID set up on both server and client Macs, as you have Back to My Mac feature enabled.

1. Open the Cyber Protect Connect server list.
2. Select the **Nearby (Bonjour + LAN)** scanner to the left.
3. Select a Mac found via Back to My Mac.
4. Double-click the "iCloud" note under its name.

For detailed instructions on how to set up Back to My Mac, see Share your computer's screen using Back to My Mac and About Back to My Mac security.

RELATED INFORMATION

About URL syntax
Control or observe a single server

Managing stored server lists

You can divide stored server connections into categories. By default, all servers that you have located and authenticated to are saved into the first category under the **Stored** section.

You can create as many categories as you want. Group servers in any way you like: by company, location, hardware type, and even owner's age.

To create a new server category

1. Click "+" button in the left bottom corner of Cyber Protect Connect window.
2. Select **Add category**.
3. Name the category.
4. Click **OK**.

Delete a server category

1. Select a category.
2. Right click its name, then select **Delete**. You can also press the **Delete** key.

   When you confirm the deletion, the category will be removed with all servers within. This is action cannot be undone.

View and edit server categories

- To view all the servers in a category, select the category in the sidebar.
- To edit a category name, right click the name, then select **Rename...** and type a new name.

- To refresh information about servers in a category, right click its name, then select **Refresh**.

Copy stored servers to another computer

You can copy your saved connections into another copy of the Acronis Cyber Protect Connect client. When you import or export stored server connections, the authentication credentials are not exported. Once you import the servers on another machine, you must authenticate to the remote computers to start controlling them.

1. Select **File > Export Cyber Protect Connect servers...**.
2. Select a folder for the exported files.
3. Click Open.A number of .rxserver files will be created in the desired location, each server in a separate file.
4. Copy the exported files to the desired computer.
5. On the new computer, open the Cyber Protect Connect client.
6. Select **File > Import Cyber Protect Connect servers...**.
7. Locate the folder with exported files, then click **Open**. All servers will be imported into Unsorted category. You must now authenticate to the client computers before you can control or observe them.

RELATED INFORMATION

Finding servers

Main window reference

Observeing multiple servers

You can observe multiple remote computers running Acronis Cyber Protect Connect agent, VNC or Apple Screen Sharing in the same window. In this way you can monitor many screens without having to select each one individually.

The Acronis Cyber Protect Connect client will need authentication credentials for each server to display the remote computer screens.

To observe multiple computers

1. In the Cyber Protect Connect **Computer List** window, select a group of stored connections, and then select two or more connections.
2. In the **Actions** pane to the right, click **MultiView**.

   Cyber Protect Connect opens a Multi-Viewer tab, showing live images of all remote computer's desktops in the same window.
   If you have stored credentials for a connection before opening it in a MultiView, Cyber Protect Connect will use them for authentication.

If you are observing more computers than can fit in the window, they are divided across several pages.

- Click **Start Slideshow** button in the toolbar to automatically cycle through the groups of screens.
- To move to the previous or next group of screens manually, click **Previous Page** or **Next Page**. You can also use swipe to the left or right to move between groups of screens.

Authenticate on multiple servers

Whenever you start a new observe session for multiple servers, the Cyber Protect Connect client connects to each of them in Observe mode — which requires valid credentials to be sent. If you start a multi-view session from scanner, and selected servers match the ones you have stored, the Cyber Protect Connect client will use the saved credentials. If there is no stored authentication data, you will be asked to provide one for each server.

When you connect in Observe mode to a group of servers that accept the same credentials, you may enter them once for all.

- When asked for an authentication, enable Use on remaining computers below the Password field.

You may also skip or cancel the authentication step for one or more servers, leaving them black in the Multi-viewer window until the correct credentials are provided.

- When asked for an authentication, click Skip or Cancel for each server.
- To cancel all authentication requests, hold down Alt and click Cancel.

Change observe settings

While you are observing multiple servers, you can adjust the observe settings.

1. In the Multi-Viewer toolbar, click **Options**.
2. Change the observe settings:
   Slideshow page delay: set the the amount of time that should elapse before the Cyber Protect Connect client advances to the next page.
   Show computer information: enable information labels for each connection listed in the Multi-Viewer.
   Name/Address: choose whether to display the stored connection name or remote computer address in the information block.
   Show user icon: enable to display an account picture of the currently logged in user (works on Apple Screen Sharing connections only).
   Wake screensaver: enable Move mouse on connect to allow the Cyber Protect Connect client to wake the remote computer from screensaver.

Zoom in a server

To zoom in a remote desktop picture

1. Select a server in Multi-viewer window.
2. Press Spacebar, or double-click a server thumbnail.
3. Navigate through the servers using keyboard cursor keys, mouse scroll, swipe right and left on multitouch trackpad, or Navigate buttons in the toolbar.

Connect to a server

You can connect to a server right from the Multi-viewer window to begin interaction with it.

1. Select a server in Multi-viewer window.
2. Click **Connect in Observe Mode**, **Connect in Control Mode**, or **Connect in Curtain Mode** in the toolbar.

Add a server to an already opened Multi-viewer window

1. Drag the Multi-Viewer out of the tab bar to make it a separate window.
2. Select a connection in the Cyber Protect Connect client main window.
3. Drag and drop the connection from Computel List to the Multi-Viewer window.

Remove a server from Multi-viewer window

1. Select a server in Multi-viewer window.
2. Click **Delete**, or click **Remove** in the toolbar.

RELATED INFORMATION

Multi-viewer window reference

About URL syntax and *.vncloc files

The Acronis Cyber Protect Connect client can open links starting with `vnc://`, `rdp://` and `acronisconnect://`. If you are using `acronisconnect://` scheme, you have to specify the connection type using "type" parameter.

It is possible to combine all connection parameters into one valid link that can be opened by Cyber Protect Connect. The syntax is:

```
acronisconnect://servername:port/?parameter1=value&parameter2=value
```

For example. if you have Screen Sharing enabled on your MacBook, with user *Martha* that has password *ohMyMac!*, using this link will let you to connect there immediately:

```
acronisconnect://MacBook.local.:5900/?type=vnc&appleUsername=Martha&applePassword=ohMyMac!
```

Here is a list of parameters common to VNC or RDP connections.

Note: Percent-encoding is used for all strings. For more information on URL notation, see Percent-encoding.

Parameter	Format	Meaning
serverName	Host name (server.domain.com), or IP address (xxx.xxx.xxx.xxx)	Server address
port	Number in range from 0 to 65535	Port number for VNC or RDP connections. VNC default is 5900 and RDP default is 3389.
type	"rdp", "vnc" or "near"	Connection type. Specify it for acronisconnect:// links.

Parameter	Format	Meaning
		Apple Screen Sharing is counted as VNC type.
sshTunnelHost	Host name (server.domain.com), or IP address (xxx.xxx.xxx.xxx). Might be the same as the serverName.	Address of server that will perform SSH tunneling.
sshTunnelPort	Number in range from 0 to 65535	Port number for SSH tunneling. Default is 22.
sshTunnelUsername	Case-sensitive string	The username that you will use to log in via SSH.
sshTunnelPassword	Case-sensitive string	Corresponding SSH password

NEAR specific parameters:

Parameter	Format	Meaning
quality	"smooth", "balanced" or "sharp"	Image quality setting to be used when connecting
username	Case-sensitive string	Username you would use to log in to remote OS
password	Case-sensitive string	Matching password for the username above

Apple Screen Sharing and VNC specific parameters:

Parameter	Format	Meaning
appleUsername	Case-sensitive string	macOS user login
applePassword	Case-sensitive string	macOS user password
ultraUsername	Case-sensitive string	Windows user login (UltraVNC)
ultraPassword	Case-sensitive string	Windows user password (UltraVNC)
unixUsername	Case-sensitive string	Unix user login (VeNCrypt TLS)
unixPassword	Case-sensitive string	Unix user password (VeNCrypt TLS)

Allowed RDP parameters:

Parameter	Format	Meaning
serverName	Hostname (MacBook.local.), or IP address (xxx.xxx.xxx.xxx)	RDP server address
port	Number in range from 0 to 65535	Port number for RDP connection
rdpUsername	Case-insensitive string	Windows user login for RDP

Parameter	Format	Meaning
rdpPassword	Case-insensitive string	Windows user password for RDP
rdpDomain	Case-insensitive string	Windows domain name
rdgUsername	Case-insensitive string	RD gateway user login
rdgPassword	Case-insensitive string	RD gateway user password
rdgDomain	Case-insensitive string	RD gateway domain
rdpDesktopWidth	Number	Predefined remote desktop width
rdpDesktopHeight	Number	Predefined remote desktop height

You can also connect to one of the stored servers via the link:

`acronisconnect://stored/?byName=connectionname`, where `connectionname` stands for the name of the server in Acronis Cyber Protect Connect Stored list.

If you have a stored server named "Mom's PC", you can connect to it using the following link:

`acronisconnect://stored/?byName=Mom%27s%20PC`.

If you want to connect with other credentials, you may include them in the link using a similar template:

`acronisconnect://stored/?byName=<servername>[&vncPassword=][&appleUsername=][&applePassword=][&ultraUsername=][&ultraPassword=][&sshTunnelPassword=]`

After a successful connection, the stored server preferences will be updated with the parameters passed in the link.

To connect to Acronis Cyber Protect Connect Cloud computers , use <Computer ID>.acroniscloud.com as a hostname. An access code may also be passed through the link: `acronisconnect://100500.acronis.com/?type=near&accessCode=IM1337`.

Cyber Protect Connect can also establish connections described in *.vncloc files. These are usually created by Screen Sharing.app (the default macOS VNC client) and contain information that can be used to connect to the remote server.

1. In the file's context menu, select **Open with**.
2. Select **Cyber Protect Connect client**.

You can also assign the Cyber Protect Connect client as a default program to open *.vncloc files on macOS:

1. In the file's context menu, select **Get Info**.
2. In the appeared window, expand the **Open with:** section.

3. Select **Cyber Protect Connect client**.
4. Click **Change all...** to open the confirmation dialog.
5. Click **Continue**.

Optimizing image transmission for Retina displays

You can enable the setting that optimizes the image transmission for Retina display, so that when you connect from your macOS workload to a Windows workload using direct or cloud RDP connections, the image you see on your workload remains sharp and clear.

To enable the setting

1. In the **All computers** page, select the Windows workload for which you want to enable the setting.
2. Click **Edit**.
3. Click the **Performance** tab for the RDP connection.
4. Select **Optimize for Retina displays**.
5. Click **Save**.

Security

Establishing a secured connection

VNC protocol uses encryption only while making an initial connection and authorization. Once connected, all data transmitted is unencrypted, and a malicious user could snoop the VNC session, unless you are using Screen Sharing with encryption set to on. The Acronis Cyber Protect Connect client supports tunneling of VNC and RDP connections over SSH, a network protocol for secure data communication.

When you connect to a server over SSH, an SSH server will establish a connection to the VNC or RDP server instead of you and transmit all remote screen data to the Cyber Protect Connect client through a secured SSH channel.

To establish an SSH connection, you have to provide SSH credentials in addition to the VNC or RDP login information.

Acronis Cyber Protect Connect client supports two types of SSH authentication:

- Password: requires the password associated with the provided SSH username.
- Public Key: requires a pair of keys. See Connect to a Mac using authentication key for SSH.

The public key authentication is more secure and is a good protection against man-in-the-middle attacks. This also comes useful when you have several servers since it allows you to authenticate on all servers via the same personal private key. To use public key authentication in the Cyber Protect Connect client, choose the public key authentication type in connection settings and specify a private key's location.

To use password authentication for SSH

1. In the **Stored** list, select a connection, or create a new one.
   For more information, see Finding servers.
2. Click **Edit**.
3. Open the **SSH Tunnel** pane.
4. Enable **Use SSH Tunnel**.
5. Enter the SSH server hostname and port.
6. Enter the SSH authentication credentials.
   If you are using a Mac as an SSH server, these will be your OS X username and password.
7. Click **Save**.

To use public key authentication for SSH

1. In the **Stored** list, select a connection, or create a new one.
   For more information, see Finding servers.
2. Click **Edit**.
3. Open **SSH Tunnel** pane.
4. Enable **Use SSH Tunnel**.
5. Enter the SSH server hostname and port.
6. Select **Public Key authentication type**.
7. Enter SSH username.
8. Specify the private key file location.
9. Click **Save**.

For more information about SSH protocol and SSH tunneling, see Secure Shell, Secure shell tunneling.

RELATED INFORMATION

Enable SSH on Mac

Connect to a Mac using authentication key for SSH

Securing transmitted data

When you connect to the OS X 10.6 and higher, all your mouse and keyboard events and authentication credentials are encrypted by default. Screen Sharing server also supports full encryption since OS X 10.8 Mountain Lion.

You can enable the secure mode where all the data transmitted between the Acronis Cyber Protect Connect client and remote computer will be encrypted. Note that it might slightly affect the performance.

Select a server in the list of stored servers.

1. Click **Edit...**.
2. Open the **VNC Settings** pane.
3. Select **All Data (slower)** in the list of the encryption types.
4. Click **Save**.

RELATED INFORMATION

Viewer window reference

About virtual displays

Connecting to Mac using SSH authentication key

The Acronis Cyber Protect Connect client supports SSH authentication by a pair of keys.

The advantage of this method is that you do not need different passwords to log on different servers. Once the public key is installed on the server, access will be granted with no password question. You can also authenticate via the personal private key on all servers, needing not to remember several passwords.

After you create two associated keys, the public key has to be stored on the remote computer host, and the private key should be stored securely on your device.

You can generate a pair of keys on a Mac using a built-in utility.

1. Open **Terminal.app**.
2. Run `ssh-keygen`.
3. Enter a passphrase that will be the password needed to use your private key.
4. Repeat the passphrase.
5. Open the folder where your pair of keys is saved.
   If you used the default location, you may go there using this command: open `~/.ssh/`

To install the public key on the server, add contents of your `~/.ssh/id_rsa.pub` to the server's `~/.ssh/authorized_keys`.

1. Open **Terminal.app**.
2. Run cat `~/.ssh/id_rsa.pub >> ~/.ssh/authorized_keys`.

When you connect to this Mac, choose the public key authentication type in connection settings and specify a private key's location.

RELATED INFORMATION

Enable SSH on Mac

Connecting using Remote Desktop Gateway

The Acronis Cyber Protect Connect Desktop Gateway service component can tunnel the RDP session using a HTTPS channel. This increases the security of RDP connections by encapsulating the session with Transport Layer Security (TLS).

When you are connecting to a remote computer located in a closed corporate network that is inaccessible from the internet by default, RD Gateway may come helpful. In these cases, you need to set up an RD Gateway in Acronis Cyber Protect Connect connection options.

1. Choose a server in the list of stored servers.
2. Click **Edit...**.

3. In the **Connection pane**, set the **Connection type** to **RDP**.
4. Open the **RD Gateway** pane.
5. Enable **Use RD Gateway**.
6. Set a host name and port number for the RD Gateway server.
7. Enter the login and password for the gateway.
   If the credentials are the same for RD Gateway and the target RDP server, enable **Use the same credentials**.
8. Click **Save**.

If you travel to and out from the corporate network with the Acronis Cyber Protect Connect client onboard, you may want to ignore RD Gateway tunneling whenever you are in the same network with the target computer.

1. Choose a server in the list of stored servers.
2. Click **Edit...**.
3. Open the **RD Gateway** pane.
4. Enable **Bypass for local connections**.
5. Click **Save**.

Note
You may only use RD Gateway when SSH tunneling is disabled, and vice versa.

For more information on Remote Desktop Gateway, see What is a Remote Desktop Gateway server? and Overview of Remote Desktop Gateway.

RELATED INFORMATION

Observe multiple servers

About authentication types

When you connect to a remote server, there are numerous possibilities of how to check your identity to let you in. These vary mainly depending on type of desktop sharing protocol, for example, Apple Screen Sharing, Microsoft RDP, or VNC. Each type of server provides its own set of authentication fields.

The following authentication types are supported by Acronis Cyber Protect Connect.

Connecting to an Apple Screen Sharing server

While connecting to an OS X built-in desktop sharing server, you can use a VNC password or an existing OS X user login/password pair. For information on how to set up a Screen Sharing server on a Mac, see Setting up a server.

When you connect to a Mac with your own credentials while an another user session is active, a Session Select window will appear, asking you which user's desktop you prefer. Choose if you want to start a separate session leaving the remote user's work uninterrupted, or to assist the user in his/her session. (See About virtual displays.)

If you do not have the credentials for a remote computer, it is still possible to connect by asking the currently logged-in user to share his screen. You may ask the remote user for:

- Share screen permission, providing you full control over the remote computer.
- Observe permission, allowing to view remote screen without any interaction.

In both cases, the currently logged in user will have to accept the connection request.

When you connect by asking for an observe permission, you will be in Observe mode regardless of "Initially Observe" setting state in the Cyber Protect Connect client preferences. You will also be unable to send contents of your clipboard to a remote computer while in observe mode. For information, see Control or observe a single server.

Apple Screen Sharing also supports additional data encryption. For information, see Secure transmitted data.

Connecting to a Microsoft RDP server

Remote Desktop Protocol is a proprietary protocol developed by Microsoft, which provides a graphical interface to connect to a Windows-running computer over a network connection. To set up an RDP server, make sure that your copy of Windows supports Remote Desktop Services and refer to Microsoft documentation on topic.

The only way to authenticate on RDP server is to enter a remote user credentials:

- **Username:** local Windows username.
- **Password:** local Windows password.
- **Domain:** an optional field, needed in some cases when the target computer belongs to a domain.

While connecting to a Windows PC, you can control only currently logged in user's screen.

The Cyber Protect Connect client also supports connection to an RDP server via Remote Desktop Gateway. For information, see Connect using Remote Desktop Gateway.

Connecting to a VNC server

Virtual Network Computing (VNC) software is available for a variety of computing platforms, making it possible to establish VNC connections between different operating systems.

For information on how to set up a VNC server, see Setting up a server.

The main authentication type in VNC is VNC password set in the VNC server software on the remote computer. Some servers support additional authentication types, for example UltraVNC username/password.

In most cases, only authentication data is transmitted over the Internet securely. If you want to protect all connection data, see Establish a secured connection.

RELATED INFORMATION

Control or observe a single server

About virtual displays

Interacting with remote computers

Connecting to remote workloads using Acronis Cyber Protect Connect Quick Assist

Using Acronis Cyber Protect Connect, you can quickly connect to remote computers on which Acronis Cyber Protect Connect agent is not installed and provide support on demand.

To connect to a remote workload using Quick Assist

1. In the Cyber Protect Connect client, click **Quick Assist**.
2. Enter the Computer ID that the remote user provided you (as displayed in Acronis Cyber Protect Connect Quick Assist on the remote workload).
3. Select **Remote control**, and then click **Connect**.
4. Select an authentication option and enter the required credentials (if any).

Option	Description
with system logon	Use this option, if you want to use username and password for authentication when establishing a connection to the remote workload.
with access code	Use this option, if you want to use the access code (as displayed in Cyber Protect Connect Quick Assist on the remote workload) for authentication when establishing a connection to the remote workload.
by asking to observe	Use this option if you want to request a permission from the user who is currently logged in on the remote workload to observe their desktop without performing any actions on the workload.
by asking to control	Use this option if you want to request a permission from the user who is currently logged in on the remote workload to observe their desktop and perform actions on the workload.

5. Click **Connect**.

Controlling or observing a single computer

You can control a screen of a remote computer to assist a user with a problem or to perform activities on a computer that doesn't have a display as if you were sitting in front of it. It is possible to control or observe any computer that has an Apple Screen Sharing, Remote Desktop Connection or VNC server configured. For more information, see Setting up a server.

Control or observe a server

1. In the Cyber Protect Connect main window, select a list of stored connections .
2. Select a connection in the list.

3. Double click it, or press **Enter**, or select the needed option from the action pane to the right. See Main window reference.
4. Use your mouse and keyboard to perform actions on the remote computer.
5. To customize the control window and session, see Viewer window reference.

For more information on different types of authentication, see About authentication types.

Switch between control and observe modes

Each connection session can be switched to an observe mode, in which the controlled computer no longer takes mouse and keyboard input from your computer. This lets you give control to a user at the remote computer or observe a remote computer without accidentally affecting its mouse or keyboard.

- Click the Switch to Control Mode / Switch to Observe Mode toggle button in the Viewer window toolbar.

Lock a user's screen

While controlling a Mac, you can lock a remote computer's screen to prevent the user from seeing what you are doing.

- Click **Lock Remote Screen** button in the toolbar, then enter a message to display while the screen is locked.

Capture the remote desktop screen to a file

You can take a screenshot of the remote screen and save it to a file. The file is saved to your computer, and is the same resolution and color depth as the controlled screen in the Viewer window.

1. In the toolbar, click **Screenshot**.
2. Name the file.
3. Click **Save**.

Control and observe in full screen mode

You can control a computer either in a window, or using the entire screen. To control a computer in full screen mode:

- Select **View > Enter Full Screen** in the menu, or click **Zoom** in the upper-left corner of the viewer window.

To exit full screen mode, select **View > Exit Full Screen**, or click **Exit Full Screen** at the right end of the menu bar.

Share clipboards between client and server

You can transfer data between your clipboard and the clipboard of the remote computer. For example, you may want to copy some text from a file on the remote computer and paste it into a document open on your computer, and vice versa. The Acronis Cyber Protect Connect client can also transfer rich clipboard contents between local and remote computers while connected with NEAR, RDP or Apple Screen Sharing.

By default, the contents of your clipboard and the remote computer's clipboard are set to be synchronized automatically. If you'd like to change this setting, go to **Other > Clipboard Auto Sync** in the Viewer toolbar.

When the automatic sychronization of the clipboards is disabled, you can send or get the clipboard contents manually.

- Select **Other > Get Clipboard** in the Viewer toolbar to get the remote computer's clipboard content.
- Select **Other > Send Clipboard** in the Viewer toolbar to replace the remote computer's clipboard content with contents of your local clipboard.

View multiple displays on a client computer

When the remote computer has more than one display, you can choose whether you want to view one of the available displays, or a combined picture.

- Click the Display drop-down menu in the toolbar to choose which display to view.

View multiple displays on a client computer When the remote computer has more than one display, you can choose whether you want to view one of the available displays, or a combined picture. You can also choose the desired resolution when connected with NEAR.

- Click the Display drop-down menu in the toolbar to choose which display to view.
- Click the Display drop-down menu in the toolbar to change resolution of one or several displays.

Adjust screen image quality

When controlling or observing a server, you can adjust the quality of the remote desktop image.

- Drag the Quality slider in the toolbar to the left to reduce image quality, or to the right to increase image quality. See Adjust quality for slow connections for detailed information.

Share control with a user when connected with Apple Screen Sharing

You can choose whether to take complete control of the keyboard, trackpad, and mouse of the remote computer or share control with a remote user.

- Change the default setting in Cyber Protect Connect Preferences > Viewer > When controlling...

RELATED INFORMATION

Finding servers

Viewer window reference

Viewing the remote desktop

When you are connected to a remote desktop, its screen is displayed in a separate tab of the same window. You can drag this tab out of the Acronis Cyber Protect Connect client to make it a separate window.

When the remote screen's size exceeds the size of the Viewer window, the Cyber Protect Connect client provides an automatic panning. It scrolls the remote desktop automatically whenever your cursor gets close to the Viewer window's edge.

Adjust zoom of the remote screen

The Cyber Protect Connect client provides two options to zoom the remote screen:

- Click Zoom to Fit on the toolbar to zoom out the remote screen to fit the size of the Viewer window.
- Click Actual Size on the toolbar to zoom in the remote screen to achieve a pixel-to-pixel match.

RELATED INFORMATION

Viewer window reference

Adjusting quality for slow connections

When you are controlling the screen of another computer over the Internet, you can adjust your connection settings to improve the performance. Different remote controlling protocols support different ways to compress the image data to be transmitted to the viewer.

The most effective way to reduce the amount of data to be transferred over the network is to reduce the image quality.

NEAR provides three quality options:

- **Smooth** means that the Acronis Cyber Protect Connect client will receive the remote computer's screen contents as an h.264 video stream. In this case, the screen resolution is limited to Full HD (1920x1080).
- **Balanced** adjusts the image quality dynamically depending on the connection speed. With this setting, you may sometimes get a blurry image but the delay should be minimal– just like with ‘Auto' quality on Youtube.
- **Sharp** prioritizes quality over performance which means that you get the best possible quality of the image regardless of the connection speed. This setting ensures the best experience on fast networks but may be laggy with slower connections.

macOS built-in VNC server allows you to choose between five variants of image quality:

- **Black and white**
- **Grayscale**
- **Adaptive**
  Use this option if your computer is connected to a slower network. Adaptive quality changes depending on network speed.
- **Medium**
- **Full**

Most VNC servers do not support the quality adjustment, and instead allow you to choose between three levels of color depth:

- 8 bits per pixel
- 16 bits per pixel
- 32 bits per pixel

To change the image quality

1. Start a remote control session. See Control or observe a single server for detailed information.
2. Change image quality using the slider to the right of the Viewer toolbar.

Note: you do not have this setting in RDP sessions.

RELATED INFORMATION

Enable Server Scaling

Viewer window reference

Enabling automatic reconnect to the remote computer

You may allow the Acronis Cyber Protect Connect client to re-establish an interrupted connection automatically whenever it has been lost. When enabled, the Cyber Protect Connect client will try to reach the remote server and log back in with the same credentials as used before disconnect.

To enable automatic reconnect

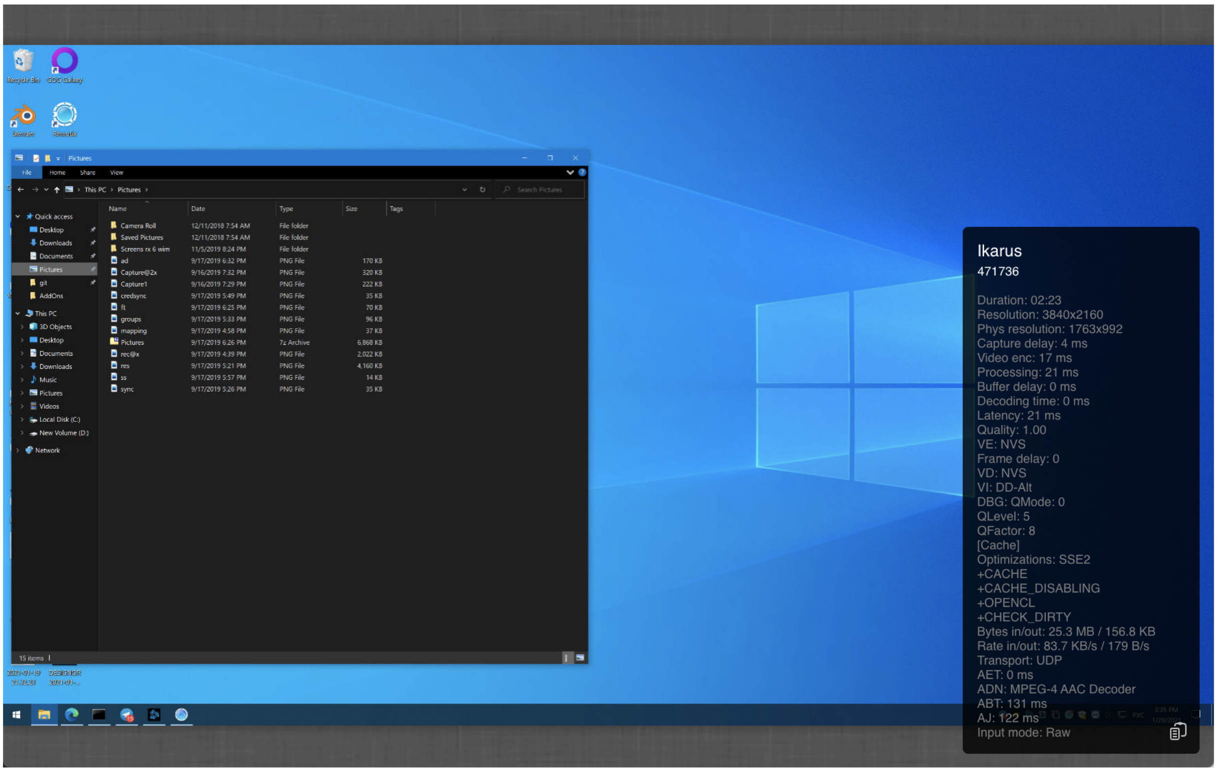
1. In the menu, select **Cyber Protect Connect> Preferences...**.
2. Open the **Viewer** pane.
3. Select **Enable automatic reconnect**.

RELATED INFORMATION

Preferences window reference

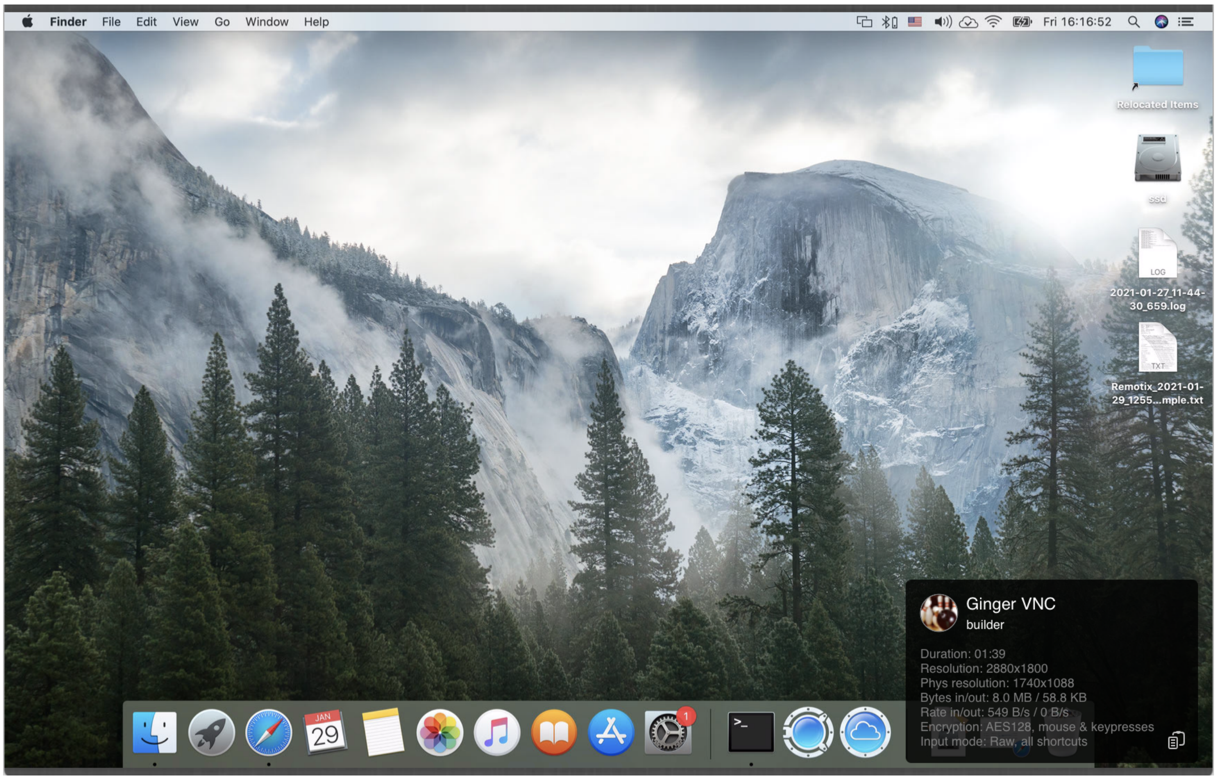
Displaying connection info panel

The Acronis Cyber Protect Connect client can show a small overlay panel in the Viewer window, showing the most essential information about the current connection.



```
Ikarus
471736

Duration: 02:23
Resolution: 3840x2160
Phys resolution: 1763x992
Capture delay: 4 ms
Video enc: 17 ms
Processing: 21 ms
Buffer delay: 0 ms
Decoding time: 0 ms
Latency: 21 ms
Quality: 1.00
VE: NVS
Frame delay: 0
VD: NVS
VI: DD-Alt
DBG: QMode: 0
QLevel: 5
QFactor: 8
[Cache]
Optimizations: SSE2
+CACHE
+CACHE_DISABLING
+OPENCL
+CHECK_DIRTY
Bytes in/out: 25.3 MB / 156.8 KB
Rate in/out: 83.7 KB/s / 179 B/s
Transport: UDP
AET: 0 ms
ADN: MPEG-4 AAC Decoder
ABT: 131 ms
AJ: 122 ms
Input mode: Raw
```


Finder
File
Edit
View
Go
Window
Help
Fri 16:16:52
Relocated Items
SSD
2021-01-27 11-44-30_659.log
Remotix_2021-01-29 1255...mple.txt

```
Ginger VNC
builder

Duration: 01:39
Resolution: 2880x1800
Phys resolution: 1740x1088
Bytes in/out: 8.0 MB / 58.8 KB
Rate in/out: 549 B/s / 0 B/s
Encryption: AES128, mouse & keypresses
Input mode: Raw, all shortcuts
```

To display the panel

1. While connected to a remote computer, click the **Other** button on the **Viewer** toolbar.
2. Click **Show Connection Info**.

The possible types of information are described below. You may also copy all the connection information to your computer pasteboard using **Copy to pasteboard** icon in the bottom right corner.

Row	Description
Title	Shows name of the connection as stored in the Acronis Cyber Protect Connect client.
Subtitle	Shows currently logged in user name for Apple Screen Sharing connections, remote computer Cloud ID for NEAR ones, and remote server address for the others.
Duration	Shows the current connection duration in [HHH:]MM:SS format.
Resolution	Shows the remote screen original resolution.
Phys Resolution	Shows the scaled image resolution whenever Server Scaling option is enabled. See Enable Server Scaling.
Bytes in/out	Shows the amount of data received and sent during the current connect session. It will not appear when you are connected over SSH.
Rate in/out	Shows current connection speed rate for incoming and outcoming traffic. It will not appear when you are connected over SSH.
Encryption	If the remote computer supports VNC encryption, it will show current encryption method and what is encrypted. See Secure transmitted data.
Latency	Delay between time when the remote computer's screen actually changes and when it is displayed in the Acronis Cyber Protect Connect client.
Transport	Indicates if the connection is established via Cloud or RDP and the type of transport.

Some lines may only appear on certain types of connection, like NEAR.

Row	Description
Capture delay	Delay between actual change of image on the remote screen and its capture. Shows up only on NEAR connections.
Video enc	Time spent on encoding the frame which is currently shown on the screen. Shows up only on NEAR connections.
Processing	Sum of the capture delay + encoding time. Shows up only on NEAR connections.
Buffer delay	Time between the first bytes of the frame data has been received and start of the decoding process. Shows up only on NEAR connections.
Decoding time	Time spent on decoding frame which is currently shown on the screen.

Screen sharing virtual displays

When you connect to an OS X 10.7 or higher, you can choose to control the screen of the currently logged in user, or the virtual screen of another user on the computer. This virtual display would be the same as the desktop experience of that person.

When you authenticate on a Mac as a different user than a currently logged in person, you can choose between two available screens:

- The screen of the currently logged in user.
- The virtual screen of the user you did authenticate as.

If you choose to control the display of the currently logged in user, he or she will be asked for a permission.

If you choose to control a virtual display, the currently logged in user will continue to work uninterrupted while you have full access to an another user's desktop.

RELATED INFORMATION

Control or observe a single server

About authentication types

Screen sharing server scaling

OS X Screen Sharing server also provides a server scaling option, in addition to image quality adjustment.

When you are viewing the remote desktop at the reduced size, the Acronis Cyber Protect Connect client shows you the scaled image. In the common case, the Cyber Protect Connect client gets the full-resolution image over the Internet and then reduces it to the smaller size. With server scaling enabled, OS X Screen Sharing server will reduce the image before sending it to you, thus reducing the network traffic.

The server scaling is enabled by default on all Mac-based connections.

To disable server scaling

1. Start a remote control session. For more information, see Control or observe a single server.
2. In the menu, select **View** > **Disable Server Scaling**.

RELATED INFORMATION

Adjust quality for slow connections

Viewer window reference

Sharing clipboards between the remote and local computers

You can transfer data between your clipboard and the clipboard of the remote computer. For example, you may want to copy some text from a file on the remote computer and paste it into a document open on your computer, and the opposite.

1. Start a remote control session.
   For more information, see Control or observe a single server.
2. In the **Viewer** toolbar, click **Get Clipboard** to get the remote computer's clipboard content.

3. Click **Send Clipboard** to replace the remote computer's clipboard content with contents of your local clipboard.

If you want the contents of your clipboard and the remote computer's one to be synchronized automatically, in the **Viewer** toolbar, select **Clipboard AutoSync**.

RELATED INFORMATION

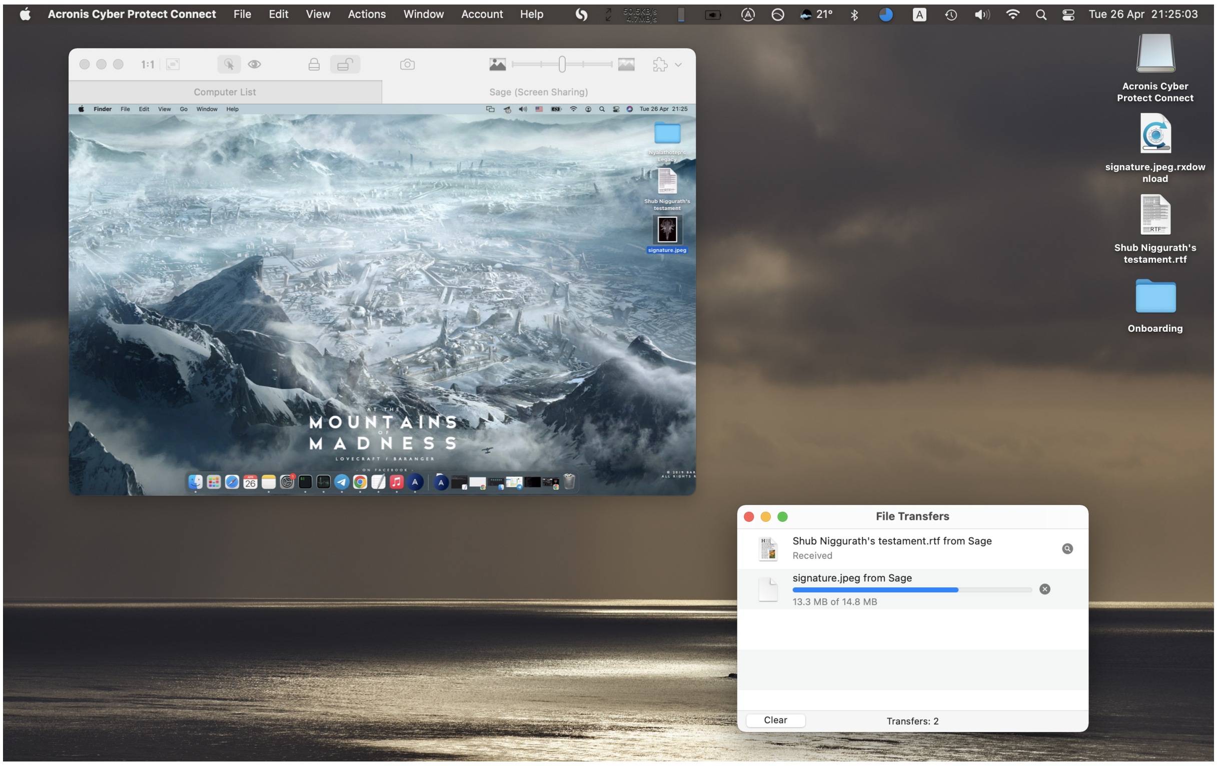
Transfer files, images and text between client and server

Viewer window reference

Transferring data between the remote and local computers in Screen Sharing mode

When you are connected to a Mac via Screen Sharing, you can use drag and drop to transfer files, images and text between the remote computer and your computer.

For example, if you need to copy a file or a folder (or a group of them) from the remote computer, you just need to drag it out of the viewer window and drop to the destination folder, and vice versa. the Acronis Cyber Protect Connect client will immediately start to download selected items.



Shub Niggurath's testament.rtf from Sage
Received

signature.jpeg from Sage
13.3 MB of 14.8 MB

Transfers: 2

When the files are ready to be transmitted, a file transfer window will appear, so you can track the state of every item.

For information on file transfer and other advanced options of RDP connections, see RDP Performance options, file, sound and printer sharing.

RELATED INFORMATION

Share clipboards between client and server

Viewer window reference

Transferring data between client and server in NEAR connection mode using the clipboard

When you are using a NEAR connection, you can transfer text, files and folders between the remote computer and yours using the clipboard.

To transfer files or folders in NEAR connection mode from a local computer to the remote one using the clipboard:

1. Ensure a NEAR connection is established between the remote computer and the local computer.
2. Copy the file or folder. On the local computer, locate the file or folder you want to copy, and do one of the following:
   - Select the file and press **Ctrl+C**.
   - Right-click the file and select **Copy** from the context menu.
3. Confirm file transfer. On the remote computer, on the notification window **You have copied files into pasteboard**, press **Send to remote computer**.
4. Paste the file or folder. On the remote computer, open the destination folder where you want to paste, and do one of the following:
   - On an empty space inside the folder, press **Ctrl+V**.
   - Right-click any empty space inside the folder, and select **Paste** from the context menu.

To copy files and folders from the remote computer to the local computer, reverse the process. Copy the file from the remote computer, then paste it to the local computer.

RELATED INFORMATION

Share clipboards between client and server

Viewer window reference

RDP performance options, file, sound and printer sharing

The Acronis Cyber Protect Connect client supports a certain number of performance options for RDP connections. In Auto mode, the Cyber Protect Connect client assumes you are connecting to an RDP server under the same Local Area Network. When you are on 3G, or have a slow internet connection, you can also select a Custom profile and set up the details manually.

These options are set in RDP server connection settings.

Performance

- **Performance options in Custom mode:**
  - **Wallpaper:** determines whether desktop background would be drawn.
  - **Full Window Drag:** if set, windows are moved with contents, otherwise only the outline will be displayed during drag.
  - **Menu Animations:** determines whether menus would appear immediately or animated.

  - **Theming:** if set, your Windows theme will be applied.
  - **Cursor Shadow:** sets the cursor shadow drawing.
  - **Cursor Blinking:** enables or disables cursor blinking.
  - **Font Smoothing:** determines whether font smoothing will be in use.
  - **Desktop Composition:** enables or disables desktop composition.
- **Compression**
  Set to "On" if you want the Cyber Protect Connect client to compress all RDP traffic.
- **Color Depth**
  Determines the number of colors in the picture RDP would transfer. Higher value requires higher bandwidth.

Audio Options

- **Audio Playback**
  Selects audio mode.
  - **None:** no audio will be played or redirected.
  - **Play on Computer:** audio will be played on the remote computer.
  - **Dynamic Quality:** audio will be redirected to your Mac and audio quality will be chosen automatically.
  - **Medium Quality:** audio will be redirected to your Mac with medium quality.
  - **High Quality:** audio will be redirected to your Mac with high quality.
- **Audio Recording**
  Determines whether audio recording (speaking to the microphone) will be transferred to a remote computer.

Printer Redirection

If you select "Redirect Printers", printers from your Mac will be automatically available on the remote computer.

Folder & File Redirection

You may share the folder from your Mac to remote Windows computer. Select folder to share:

- **None** no files will be redirected.
- **All Files** all files and disks will be redirected.
- **Home Folder** current user home folder will be redirected.
- **Documents Folder** current user Documents folder will be redirected.
- **Custom Folder** user selected folder will be redirected.

On remote computer, the redirected folder will be available as Acronis Cyber Protect Connect disk drive under My Computer.

RELATED INFORMATION

Connect using Remote Desktop Gateway

Control or observe a single server

Capturing a remote desktop screen to a file

You can take a screenshot of the remote screen, and save it to a file. The file is saved to your computer and is the same resolution and color depth as the controlled screen in the Viewer window.

1. Start a remote control session.
   For more information, see Control or observe a single server.
2. In the menu, select **View > Take screenshot**, or click **Screenshot** in the toolbar.
3. Name the file.
4. Click **Save**.

RELATED INFORMATION

Viewer window reference

Recording sessions

It is possible to record a NEAR remote control session in the Acronis Cyber Protect Connect client.

To record a remote connection session

1. On the **Viewer** toolbar in the Acronis Cyber Protect Connect client, click **Other**, and select **Start Recording**.
2. Select a name and location for the record.

   By default, the file will be named with the current date and time and located in the **Documents** folder in the current user home directory.

   While the recording is active, in the **Viewer** toolbar you will see a flashing red circle over the top right corner of the remote screen and the recording timer.
3. To stop the recording, click **Other > Stop Recording**. On a Mac, you can also click **Stop** on the toolbar.

All **.crec** files made by the Acronis Cyber Protect Connect will be automatically assigned to open with Acronis Cyber Protect Connect client by default.

To play a recording

1. Locate a recording file.
2. Open it.
3. A Cyber Protect Connect Recording Player will open in a new tab of the Cyber Protect Connect client.
   Note that it is not possible to navigate through the recording. To find a certain moment in the recording, wait until the player reaches it.
4. To adjust playback speed, use the **<<** and **>>** icons in the playback controls section.

The recording is stored as a sequence of events that have been transmitted to and from the remote server during a connection. This ensures the best quality of the recording at the minimum file size.

However, this also means that it is not possible to navigate through the recording. At the moment it is also not possible to convert the recordings to a video format.

RELATED INFORMATION

Player window reference

Setting up a server for remote access

Install VNC, RDP or Screen Sharing server

Setting up VNC, RDP and Screen Sharing server

The Acronis Cyber Protect Connect client needs a Screen Sharing, RDP or VNC server running on the remote computer to be able to access its desktop. VNC server is a special software that can transmit the remote desktop image to the VNC client as well as receive mouse movements and keyboard key pressings. Thus, you are able to interact with a remote computer as though it is right next to you.

VNC server software varies depending on operating system. OS X is the only one with an integrated VNC server, easy to configure and use. Users of other operating systems have to find and install VNC server in order to use the Cyber Protect Connect client. For more information about VNC, see Virtual Network Computing.

The Cyber Protect Connect client needs Acronis Cyber Protect Connect agent installed or a third-party remote connection service to be configured on the remote computer to be able to access its desktop. Such services are a special software that can transmit the remote desktop image to the client application as well as receive mouse movements and keyboard key pressings. Thus, you are able to interact with a remote computer as though it is right next to you. This software varies depending on operating system.

The best way to use the Cyber Protect Connect client is to equip your remote computers with Cyber Protect Connect agent which is designed to provide anywhere access to any desktop and to organize your computer lists in the most convenient way. If you prefer using third-party services, you can also set up another kind of server software.

Configure Acronis Cyber Protect Connect agent on a remote computer

The easiest and most convenient way to enable remote access to a machine is to install Cyber Protect Connect agent. This will save you the trouble of dealing with static address, proxies, and so on.

- If the remote computer is a Mac, see Set up anywhere access on Mac.
- If the remote computer is a Windows PC, see Set up anywhere access to Windows PC.
- If the remote computer is running Linux, see How to install Acronis Cyber Protect Connect Quick Assist on Linux.

Enable Screen Sharing on OS X

Starting with 10.5, macOS includes a built-in Screen Sharing component, which is based on VNC and provides an advanced desktop sharing experience. The easiest way to make a Mac accessible via VNC is to enable Remote Management.

1. In the **Apple** menu, select **System Preferences**, and then click **Sharing**.
2. Select **Remote Management**.
3. Next to "Allow access for", select all users.
4. Click **Computer settings...**, and enable **Anyone may request permission to control screen**.

You may also enable Screen Sharing instead of Remote Management but it provides less remote control opportunities than Remote Management and may work worse in some cases.

Enable RDP access on Windows

Windows provides an advanced desktop sharing via its own Remote Desktop protocol. You have to enable Remote Desktop Connection in System Preferences in order to make a Windows computer accessible via RDP.

1. Go to the **System** section of the **Control Panel**.
2. Select **Remote**.
3. Enable **Allow remote connections**.

For detailed instructions on setting it up on different versions of Windows, see Enable RDP access on Windows.

Set up another VNC server

VNC server is a third-party software that can transmit the remote desktop image to the VNC client as well as receive mouse movements and keyboard key pressings. VNC server software varies depending on operating system. OS X is the only one with an integrated VNC server, easy to configure and use. Users of other operating systems have to find and install VNC server in order to use the Cyber Protect Connect client.

To configure a VNC server

1. Download and install the VNC server software.
2. Configure the security settings, like password or user rights.
3. Ensure that the VNC port is accessible over the Internet.

The most popular ones for Windows are Ultra VNC and Tight VNC. Here are the instructions for configuring them.

To configure a Tight VNC server

1. Download the Self-installing package for Windows from the Tight VNC website.
2. Install the package using the default installation settings.
3. Start TightVNC in Service mode if it did not start automatically.

   You should see a TightVNC service icon in tray, informing you that VNC service started successfully.

Configure an Ultra VNC server

1. Download the latest version of Full installer from the Ultra VNC download page.
2. Start the installation. On the **Select Additional Tasks** step, select the first two check boxes (**Register UltraVNC Server as a system service** and **Start or restart UltraVNC service**).
3. After installing, go to server preferences and set your own VNC password.
4. If you want to enable access by using your Windows username and password:

a. Enable **Require MS Logon** and **New MS Logon**.
b. Click **Configure MS Logon Groups** and enable full control for the user you will log in as.
c. In Windows XP you must disable Force Guest option in registry by running the .reg file: disableforceguest.reg.zip.

RELATED INFORMATION

Make VNC or RDP server accessible over the Internet

Configure the network router to accept incoming connections

Enable RDP access on Windows

Remote Desktop protocol is a proprietary protocol developed by Microsoft, which provides a graphical interface to connect to a Windows-running computer over a network connection. To set up an RDP server, make sure that your copy of Windows supports Remote Desktop Services.

Steps to enable an RDP access vary slightly, depending on Windows version.

Windows XP and Windows Server 2003

1. Open **Control Panel**, and click **Switch to Classic View**.
2. Select **System**.
3. Select **Remote** pane.
4. Enable **Allow users to connect remotely to this computer**.
5. Click **Remote Desktop Users** and select users that would be allowed to use RDP on this local computer.

Windows 7 and Windows Server 2008

1. Go to **Control Panel** and change the view to **Large Icons**.
2. Click **System**.
3. In the left menu, select **Remote Settings**.
4. Enable **Allow remote connections to this computer**.
5. Click **Select Users...** to assign who would be allowed to use RDP on this local computer.

Windows 8

1. From the Metro interface, click **Desktop** to get access to the desktop.
2. Move your mouse to the left-bottom corner and right click it.
3. In the menu, select **Control Panel** and change the view to **Large Icons**.
4. Click **System**.
5. In the left menu, select **Remote Settings**.

6. Enable **Allow remote connections to this computer**.
7. Click **Select Users...** to assign who would be allowed to use RDP on this local computer.

Windows 10

1. Right-click on the **Start** icon.
2. In the context menu, select **System**.
3. In the left menu, select **Remote Settings**.
4. Enable **Allow remote connections to this computer**.
5. Click **Select Users...** to assign who would be allowed to use RDP on this local computer.

RELATED INFORMATION

Setting up a server

Make VNC or RDP server accessible over the Internet

Make a server accessible

Make a VNC or RDP server accessible over the Internet

The easiest way to make the remote computer accessible for Acronis Cyber Protect Connect connections from anywhere is to use Acronis Cyber Protect Connect Cloud. The Cloud service will establish a secure tunnel to the remote server regardless of its location, NAT, router, and firewall settings. For information on Acronis Cyber Protect Connect Cloud, see Connect via Acronis Cyber Protect Connect Cloud.

If you want to make your Screen Sharing, VNC or RDP server accessible from outside the local network manually, you need to make its host available by a permanent address and open the corresponding port for the incoming connections.

1. Ensure that your computer has a stable host name or IP address.
2. Configure port forwarding on the network router.
3. Configure firewall on your computer.

RELATED INFORMATION

About setting a stable host name for the computer

Configure the firewall to accept incoming connections

Configure the network router to accept incoming connections

Set a stable host name for the computer

In order to set up a VNC or RDP connection, you have to specify the server address, either it is an IP address or a host name. In most cases, users of Internet have a dynamic IP that change every time you relaunch your internet connection. In addition, ISP often assign one IP address to several users. These things make it impossible to connect directly to your computer from outside the local network.

To overcome this, you can use a Dynamic DNS service. When you are registered as a DDNS user, a special software running on your computer or router keeps it available by a static host name. For more information, see Dynamic DNS.

Many home networking routers support several DDNS providers out of the box. To see if your router supports it, check your router documentation.

A list of free Dynamic DNS service providers is available at DDNS — Free Dynamic DNS Providers.

RELATED INFORMATION

Configure the firewall to accept incoming connections

Configure the network router to accept incoming connections

Configure the network router to accept incoming connections

When the server is connected to the Internet via router, it will not receive incoming connections by default. To make the server open for incoming connections, you have to enable forwarding the corresponding port from router to the target computer.

Directions for setting up port forwarding vary depending on the router's manufacturer and version of firmware, but the information you need to enter remains the same.

1. Open your router's preferences.
2. Find **Port forwarding** section. It may also be called as **Port mapping** or **Port triggering**.
3. Create a new port forwarding rule.
4. Set a name for your service.
5. Set the incoming port. (It may also be called **Start port**, **External port**, or **Port from**.)
6. Set the local IP address of the computer with VNC/RDP server as destination IP address.
7. Set the destination port. (It may also be called **End port**, **Internal port**, or **Port to**.)

For more information, refer to your router's user manual.

RELATED INFORMATION

About setting a stable host name for the computer

Configure the firewall to accept incoming connections

Connect via Acronis Cyber Protect Connect Cloud

Configure the firewall to accept incoming connections

When the computer with VNC or RDP server has a firewall software running, it requires additional configuration to be open for the incoming connections. The default TCP port numbers are 5900 for VNC protocol and 3389 for RDP protocol.

Most operating systems have built-in firewall software. OS X allows incoming Screen Sharing connections by default. Windows allows incoming connections on port 3389 automatically while RDP is enabled in system preferences, but might require an additional configuration for VNC servers.

To make Windows firewall accept incoming VNC/RDP connections.

Windows XP

1. Click **Start** > **Control panel**,
2. In the **Network and Internet Connections** category, click **Windows Firewall**.
3. Click the **Exceptions** tab.
4. Click **Add port**.
5. Set the name (for example, VNC) and port number.
6. Select a TCP protocol.
7. Click **OK**.

Windows Vista

1. Click **Start** > **Control panel**.
2. In the **Security** category, click **Allow a program through Windows Firewall**.
3. Click the**Exceptions** tab.
4. Click **Add port**.
5. Set the name (like VNC) and port number.
6. Select TCP protocol.
7. Click **OK**.

Windows 7

1. In the **Control panel**, click **System and Security**.
2. In the **Windows Firewall** section, click **Allow a program through Windows Firewall** .
3. Click **Change settings**.
4. Click **Allow another program**.
5. Select your VNC server from the list, and click **Add**.
6. Enable **Home/Work (Private)**.
7. Click **OK**.

Windows 8

1. Press the Windows key.
2. Type "firewall" and select **Settings** in the right-side panel.
3. Select Allow an app through Windows Firewall.
4. Click **Change settings**.
5. Click **Allow another app...**.
6. Select your VNC server from the list, and click **Add**.
7. Enable **Private**.
8. Click **OK**.

Windows 10

1. Press the **Windows** key.
2. Type "firewall" and select **Windows Firewall** in the right-side panel.
3. Select **Allow an app through Windows Firewall**.
4. Click **Change settings**.
5. Click **Allow another app...**.
6. Select your VNC server from the list, and click **Add**.
7. Click **Network Types...**.
8. Enable **Private**.
9. Click **OK**.

If your computer is running a third-party firewall software, refer to its documentation for information.

RELATED INFORMATION

Configure the network router to accept incoming connections

Connect via Acronis Cyber Protect Connect Cloud

Enable SSH on Mac

macOS has a built-in SSH server, but you must enable it in **System Preferences**.

1. Select **Apple menu** > **System Preferences**, and then click **Sharing**.
2. Check the **Remote Login** service.
3. Next to **Allow access for**, select all users, or select **Only these users**, and customize the list.

RELATED INFORMATION

Establish a secured connection

Connect to a Mac using authentication key for SSH

Perform silent installation

The Acronis Cyber Protect Connect client supports silent installation mode that eases and fastens the installation process. In this mode, it will not display messages or windows during the progress.

To perform such an unattended installation, invoke RemotixInstaller.exe from command line with desired options. Here is a full list of parameters that can be passed to the installer:

Parameter	Description
/S	Install silently
/Dir=<path>	Install the Cyber Protect Connect client to the specified folder
/B	Force installation of Bonjour drivers (this mean that driver package will be (re)installed even if it is already present in the system)
/NB	Omit Bonjour drivers during (un)installation process

All parameters except /Dir may also be used for uninstallation.

For example, to install the Cyber Protect Connect client silently into the "%localappdata%\Acronis Cyber Protect Connect" folder along with Bonjour drivers, you need to execute the following command:

AcronisCyberProtectConnectInstaller.exe /S /Dir="%localappdata%\Acronis Cyber Protect Connect" /B

Please note that if you have User Access Control enabled, it will appear to ask for a permission to install.

HTTP API for Cyber Protect Connect client

Starting with version 6.2.5, the Acronis Cyber Protect Connect client supports HTTP API for automating of most common routine tasks. This helps make things like regular password change on a bunch of remote computers much easier.

HTTP API is disabled by default and must be enabled in the Cyber Protect Connect client settings.

You can download a sample Python scripts to work with API here.

HTTP API uses JSON encoding in requests and responses. In case of the success, HTTP 200 OK is returned. In case of an error, HTTP status codes of 4xx are returned.

Here is the list of commands to be performed via API:

Working with groups:

Get a list of groups:

```
GET /groups
```

Get a list of items in the group:

```
GET /group/<group_uid>
```

Get the list of the connections in NEARBY pane:

```
GET /nearby
```

Create group:

```
PUT /group/
```

Body:

```
{ name: "New name" }
```

Response:

```
{ group_uid: "0123-CDEF" }
```

Update the name of the existing group:

`PUT /group/<group_uid>`

Body:

```
{ name: "New name" }
```

Delete a group:

`DELETE /group/<uid>`

Working with connections:

Create a single connection:

`PUT /connection/`

Body:

```
{ name: "New connection name", category_uid: "0123-CDEF" }
```

Response:

```
{ uid: "4567-89AB" }
```

Update an existing connection:

`PUT /connection/<uid>`

Body:

```
{ name: "New connection name", category_uid: "0123-CDEF" }
```

Update a connection's credentials:

`PUT /connection/<uid>/credentials`

Body:

```
NEAR: { "rxp.username": "new_username", "rxp.password": "new_password" }
RDP: { "rdp.username": "new_username", "rdp.password": "new_password", "rdp.domain":
"new_domain" }
Apple Screen Sharing: { "apple.username": "new_username", "apple.password": "new_
password", }
```

Delete a single connection:

`DELETE /connection/<uid>`

Delete connection credentials:

`DELETE /connection/<uid>/credentials`

Working with cloud computers:

Get the main settings of a cloud computer

`GET /computer/<computer_id>`

Get a list of actions available for a given cloud computer

`GET /computer/<computer_id>/actions`

Get a list of configured connections for a given cloud computer:

`GET /computer/<computer_id>/connections`

Get settings of a specific connection of the cloud computer:

`GET /computer/<computer_id>/<connection_type>[_<port>]`

Examples:

`GET /computer/123456/VNC`

`GET /computer/123456/RDP_3390`

`GET /computer/123456/NEAR`

Get credentials of one of the connections of cloud computer:

`GET /computer/<computer_id>/<connection_type>[_<port>]/credentials`

Update a cloud computer's main settings (name + groups it belongs to):

`PUT /computer/<computer_id>`

Body:

```
{ name: "New computer name", category_uid: "0123-CDEF" }
```

Update cloud computer connection:

`PUT /computer/<computer_id>/<connection_type>[_<port>]`

Body:

```
{ key: <value> }
```

Note that only specified fields are overridden. To delete the corresponding field (and effectively set it to the default value) use 'null' as value.

Delete a cloud computer:

```
DELETE /computer/<computer_id>
```

Note: this will remove the computer from your console and remove you as a user from a **Trusted Users** list on this computer.

Delete computer's connection settings:

```
DELETE /computer/<computer_id>/<connection_type>[_<port>]
```

Delete computer's connection credentials:

```
DELETE /computer/<computer_id>/<connection_type>[_<port>]/credentials
```

Actions

Initiate connect to an existing connection:

```
ACTION /connection/<uid>/connect
```

Initiate connect to a remote cloud computer:

```
ACTION /computer/<computer_id>/<connection_type>[_<port>]/<action>

ACTION /computer/<computer_id>/chat

ACTION /computer/<computer_id>/NEAR/control

ACTION /computer/<computer_id>/NEAR/curtain

ACTION /computer/<computer_id>/NEAR/observe

ACTION /computer/<computer_id>/NEAR/ft

ACTION /computer/<computer_id>/VNC[_<port>]/control

ACTION /computer/<computer_id>/RDP[_<port>]/control
```

Cyber Protect Connect client for iOS

Cyber Protect Connect client overview

Introduction

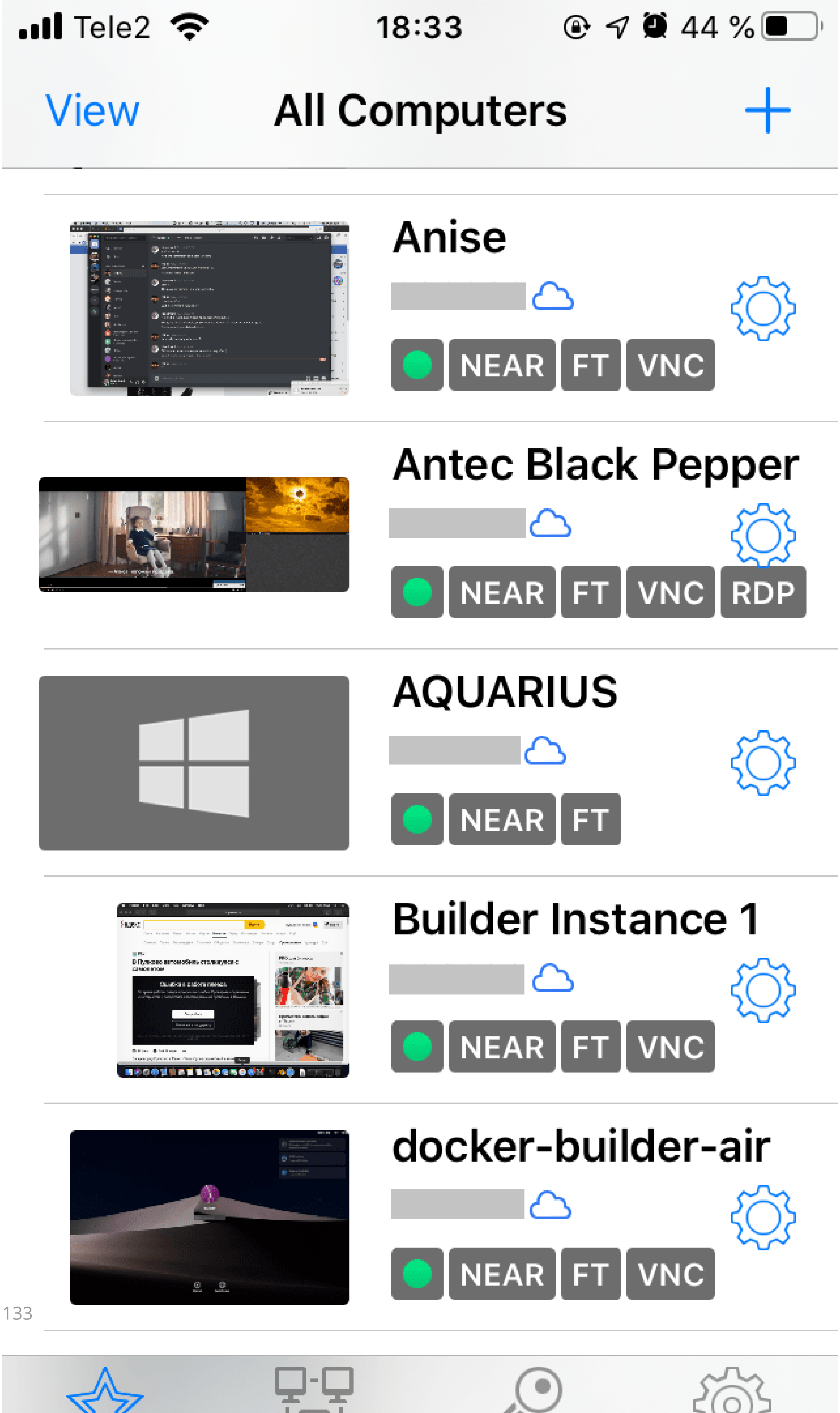
The Acronis Cyber Protect Connect client is a powerful yet simple client for remote access. You can connect to your computer from anywhere with almost zero lag via NEAR protocol.

The Cyber Protect Connect client supports

- NEAR – the Cyber Protect Connect client s own low-latency protocol
- Remote Desktop Protocol (RDP)
- Apple Screen Sharing
- Virtual Network Computing (VNC)

You can connect to any remote desktop running any operating system from your Android device.

Main Screen



Tele2 18:33 44 %

View All Computers +

Anise

[redacted]

● NEAR FT VNC

Antec Black Pepper

[redacted]

● NEAR FT VNC RDP

AQUARIUS

[redacted]

● NEAR FT

Builder Instance 1

[redacted]

● NEAR FT VNC

docker-builder-air

[redacted]

● NEAR FT VNC

Cyber Protect ConnectAccount

Register at acronis.com to get an Acronis Cyber Protect Connect Cloud account and connect to remote computers using NEAR, and store and synchronize your remote connections and credentials across all devices.

When logged in, this pane displays your account information page and notifications from the Cyber Protect Connect console.

Stored Computers

Cyber Protect Connect Stored Computers screen presents a list of stored connections available to open.

When you connect to a nearby computer for the first time, you need to choose authentication type. When you disconnect, this computer gets added to the Stored list. All settings that you have selected or changed on-the-fly, will be stored. A star icon to the right of the connection name indicates that you have this connection in the Stored list.

Connections that you have never visited before have a default "blank" thumbnail and no stored settings.

To add a connection manually

1. Press [+] button.
2. Choose the type of a new connection.
3. Enter the address (Computer ID for NEAR, and hostname or IP for VNC or RDP).

   The other fields are optional.

   If you leave the **Port** field blank, the Cyber Protect Connect client will use the default value (5900 for VNC and 3389 for RDP).

When you finish, the new connection will appear in the Stored list with a blank thumbnail.

When you disconnect after a successful connection, the Cyber Protect Connect client saves the remote screen as a thumbnail to help you recognize it later. The thumbnail gets refreshed at the end of every session. To disable thumbnail saving, set "Store thumbnail" option to Off.

Nearby

The Cyber Protect Connect client uses Bonjour and LAN scanners to discover nearby computers available to connect.

- Bonjour: nearby servers on the local subnet that announce themselves using Bonjour technology.
- LAN: IP address/port scan of all computers available on the Wi-Fi interface.

Quick Connect

You may quickly connect to a remote computer running Acronis Cyber Protect Connect agent or Acronis Cyber Protect Connect Quick Assist using this pane.

To establish a connection, enter the **Computer ID** and **Access Code** shown in the Cyber Protect Connect agent on the remote computer.

Application Settings

Computer list settings

Sort mode

Choose how to sort your stored connections: by name, address or online status.

Cyber Protect Connect Account

Cyber Protect Connect Account (iPhone only) - log in with your Cyber Protect Connect account to get access to all of your computers and set up connection and credential sync.

Synchronization - select whether you want your connections and credentials stored only locally on the current device or synchronized across all devices with the same Cyber Protect Connect account.

Upload session info to Cloud - If set, the Cyber Protect Connect client will upload session info (protocol, duration and direction) to the Cloud automatically.

Security

Master Password - turn on if you want the Cyber Protect Connect client to ask your device passcode, Touch ID or Face ID every time you start the application.

Curtain Mode on Mac Connections - turn on if you want the screen to be automatically locked when you connect to remote Mac either via NEAR or Screen Sharing.

Connection

Auto Reconnect - enables or disables automatic connection setup after disconnection, for example when you answer the call on your iPhone or switch to the other app on iPad.

Show hidden files in file transfer. Choose whether you want to see and transfer hidden and system files in the File Transfer dialog.

Offer saving credentials by default. If set, the Cyber Protect Connect client will offer saving credentials by default.

Synchronize Clipboardby default
If set, the Cyber Protect Connect client will perform automatic clipboard synchronization if the server supports it. If you copy something into the pasteboard on iOS device, the Cyber Protect

Connect client sends it to the server. The opposite is also true - copying on server would automatically transfer clipboard contents to iOS device. Supported types include text and images.

Network

Use SOCKS-proxy. If set, you can set up custom SOCKS-proxy.

Computer settings

Each stored computer in the list has its own drop-down settings menu.

Common settings

Name

Computer name determines the name of your machine in the Acronis Cyber Protect Connect console web interface and in the Acronis Cyber Protect Connect client. Type or change it here.

Store Thumbnail

The Cyber Protect Connect client saves the remote screen as a thumbnail to help you recognize it later. The thumbnail gets refreshed at the end of every session. To disable thumbnail saving, set "Store thumbnail" option to Off.

Connection settings

NEAR Settings

Authentication Options

Ask if needed

You will be asked about the authentication if it is required.

No authentication

If Acronis Cyber Protect Connect agent allows, you will connect to the computer without authentication.

Access Code

Authentication by the Access Code, as displayed in Acronis Cyber Protect Connect agent main window on the target computer.

System Logon

Uses Windows or macOS X user credentials to authenticate. Note that you will only be able to log in into logon session or the existing session of the specified user.

NEAR connection options

Quality

Select the quality depending on your current workflow.

Smooth is the best for games or video playback. It uses hardware-accelerated H.264 to encode the remote desktop. Sharp gives you the best quality picture at the sacrifice of frames per second. Balanced (the default) is optimized for the general use.

Server Scale

Enables or disables scaling of the remote desktop picture to optimize network bandwidth.

Redirect Sound

Enables or disables the playback of the remote computer sound on your device.

Hide Local Cursor

If the remote computer displays cursor as part of the remote screen you can disable the local cursor rendering.

VNC Settings

Options for Mac-based (Screen Sharing) servers

Keyboard through clipboard paste

Having this option on you do not need to switch the keyboard layout on your server. You can type any national characters from keyboard layouts installed on your device. The only drawback of this method is that system clipboard and clipboard synchronization between your device and computer will not be available.

Quality Level

To have the best experience over different network speed the Cyber Protect Connect client allows selection of the quality level. You can choose between black & white, grayscale, medium, adaptive and full quality. The least bandwidth hungry is black and white. Adaptive quality codec provided by Apple Screen Sharing™ minimizes buffering and guarantees a fast start. It also provides a fast performance on average and slow connections, although it is rather CPU hungry.

Server Scaling

You can further improve performance of the Cyber Protect Connect client on zoomed out view by setting up this option. On the connect stage the Cyber Protect Connect client sends a command to server to send back downscaled image. This will reduce required bandwidth and free your device resources.

Display

Apple Screen Sharing only. If Mac you are connecting to have multiple displays, the Cyber Protect Connect client allows selection of the active monitor. Options include "Combined" to use all displays, or each display individually.

Color Depth

This option is only available if Adaptive codec is selected. Choose 16 bit to lower CPU requirements (older devices).

Options for other VNC servers

Operating system

Selected server OS defines extended keyboard layout (OS-dependant modifiers) and Dock / taskbar icon for the corresponding gesture and ensures correct work of cut/copy/paste extended keyboard buttons.

Preferred Encodings

You may choose the preferred graphical encodings used by the Cyber Protect Connect client for every server.

If all encodings are turned off, the raw encoding will be used (which does not perform any compression and needs the widest bandwidth).

Color Depth

This option is only available if Adaptive codec is selected. You can adjust color depth of the Viewer screen. The higher the value - the greater the width of bandwidth used. You can get satisfying level of picture quality vs. performance adjusting this option, e.g. on GPRS connection or on older devices you need to set it on 8 or 16 bits.

SSH Tunneling

You may use a secured connection through SSH (SSH tunnel) to access your machine if you have SSH server available. To establish a secured connection, enable "Use SSH tunnel" option in the Cyber Protect Connect client connection preferences.

SSH username

This is the username that you will use to log in via SSH. Usually it is the same as your OS login on the remote computer.

To enable SSH connection on your Mac

1. Go to System Preferences -> Sharing pane.
2. Enable Remote Login service.

Authentication type

You may choose either interactive or public key-based way to authenticate.
For interactive, you have to enter password associated with the SSH username. For public-key based authentication, you need to have a pair of keys.

SSH password (or Private key passphrase)

You may fill it in advance, or leave blank if you want to be asked for this password on every connection attempt.

SSH host and **SSH port** determine the intermediary machine SSH connection goes through.

RDP Settings

Authentication Options

Domain
Enter Windows domain here if your computer is part of domain. If not, leave empty.

Username
Enter Windows username here.

Password
Enter Windows password here.

RDP Connection Options

Desktop Size
Select the resolution of the remote session.

Autofit mode adapts RDP resolution to match your iDevice. RDP resolution will be changed on rotations and entering/leaving fullscreen mode. Note: live resolution change only works for non-server Windows editions, starting from 8.1.

There are "Fullscreen (Portrait)" and "Fullscreen (Landscape)" options for the Cyber Protect Connect client to automatically calculate the resolution, so it fits the screen completely in Portrait or Landscape orientations correspondingly. Also, you can set up custom sizes if you select "Custom".

Desktop Scale
Select the scale factor used for desktop elements. This is especially useful on high-resolution devices, like Surface Pro.

Performance options

Performance
Select the performance profile of the connection. In "Auto" mode, the Cyber Protect Connect client detects whether you are running on Wi-Fi or 3G and selects "3G" or "LAN" correspondingly. You can also select "Custom" profile and set up the details manually:

- **Wallpaper** determines whether desktop background would be drawn
- **Full Window Drag** if set, windows are moved with contents, otherwise only the outline will be displayed during drag
- **Menu Animations** determines whether menus would appear immediately or animated
- **Theming** if set, your Windows theme will be applied
- **Cursor Shadow** sets the cursor shadow drawing
- **Cursor Settings** disables cursor blinking
- **Font Smoothing** determines whether font smoothing will be in use
- **Desktop Composition** enables or disables desktop composition.

Compression
Set to "On" if you want the Cyber Protect Connect client to compress all RDP traffic. **Note:** this can be actually slower due to increased CPU requirements on iOS device.

Color Depth
Color depth determines the number of colors in the picture RDP would transfer. Higher value requires higher bandwidth.

Enhanced Graphics (H.264) Select to use hardware-accelerated H.264 encoding provides the best picture for work, video and games.

Audio Options

Audio Playback Selects audio mode.

- **None** no audio will be played or redirected
- **Play on Computer** audio will be played on the remote computer
- **Dynamic Quality** audio will be redirected to iOS device and audio quality will be adapted automatically
- **Medium Quality** audio will be redirected to iOS device with medium quality
- **High Quality** audio will be redirected to iOS device with high quality

Audio Recording
Determines whether audio recording (speaking to the microphone) will be transferred to remote computer.

Redirection

Access your iOS files as a folder on remote computer.

Keyboard Mode

Choose unicode or keycode keyboard input mode.

Advanced Options

Console Session
Set to on if you want to connect to the existing first session on RDP server (Windows Server 2003 only).

Startup Program
Specify the path to the executable, which will be started on user logon (Windows Server only).

Working Directory
Specify the working directory for the startup program. Only applies if startup program is set. (Windows Server only)

3.8. RD Gateway

If your company is using Remote Desktop Gateway to provide an access to your machines within your company network, specify the gateway parameters here.

3.9. SSH Tunneling

You may use a secured connection through SSH (SSH tunnel) to access your machine if you have SSH server available. To establish a secured connection, enable "Use SSH tunnel" option in the Cyber Protect Connect client connection preferences.

Supported servers and authentication modes

NEAR

you can install Acronis Cyber Protect Connect agent and Acronis Cyber Protect Connect Quick Assist with NEAR on the following operating systems:

- Windows 7 or higher
- Mac OS X 10.11 or higher
- Generic Linux with X server

VNC servers

The Acronis Cyber Protect Connect client supports the following servers and authentication modes:

- Mac OS X Screen Sharing™: Ask for observe, Ask for control, Mac OS X authentication (Mac OS X username + password), VNC password;
- UltraVNC: VNC password, MS Logon II authentication (Windows username + password);
- RealVNC (without encryption): VNC password;
- TightVNC: VNC password;
- TigerVNC: VNC password;
- TurboVNC: VNC password;
- x11vnc: VNC password.

You may also connect to any of supported servers over SSH.

RDP servers

Acronis Cyber Protect Connect RDP supports the connections to the following Windows versions:

- Windows XP SP1, SP2, SP3 (starting from Professional)
- Windows Server 2003
- Windows Vista (starting from Professional)
- Windows 7 (starting from Professional)

- Windows Server 2008/2008 R2
- Windows 8/8.1
- Windows Server 2012/2012 R2
- Windows 10

You may also connect to any of the supported servers over SSH.

How to set up a computer you are connecting to

NEAR

For Acronis Cyber Protect Connect agent installation instructions, refer to the Acronis Cyber Protect Connect Cloud Help.

VNC

You own a Mac

To enable Screen Sharing on your Mac

1. Go to Sharing pane in System Preferences.
2. Select Remote Management service in the list and enable it.
3. Look to the right and make sure that access is allowed for all users.
4. Click the Options... button and enable all options in list.
5. Click the Computer settings... button and enable "Anyone may request permission to control screen" option.

After you perform these steps, your Mac appears automatically under **Bonjour** section in the Acronis Cyber Protect Connect client.

You own a PC

First, you have to choose one VNC server. The most popular ones are Ultra VNC and Tight VNC.

How to set up a Tight VNC server

How to set up an Ultra VNC server

After you perform these steps, perform rescan using **local network** or **NetBIOS** scanner to discover your machine.

RDP

Windows XP and Windows Server 2003

Do the following

1. Go to Control Panel and select "Switch to Classic View".
2. Select "System".
3. Select "Remote" tab.
4. Set the checkmark "Allow users to connect remotely to this computer".
5. Click on "Remote Desktop Users" and select users on this machine which will be allowed to use RDP.

After you perform these steps, perform rescan on LAN or NetBIOS scanner and your machine will automatically appear under corresponding section in the Cyber Protect Connect client with "RDP" label.

Windows 7 and Windows Server 2008

Do the following:

1. Go to Control Panel.
2. In the control panel, change "view by" to "Large Icons".
3. Click on "System".
4. In the left menu, select "Remote Settings".
5. Select "Allow remote connections to this computer".
6. Click on "Select Users..." and select users on this machine which will be allowed to use RDP.

Windows 8

Do the following:

1. From Metro interface, click to "Desktop" to get access to the desktop.
2. Move your mouse to the left-bottom corner and perform the right click.
3. In the menu, select "Control Panel".
4. In the control panel, change "view by" to "Large Icons".
5. Click on "System".
6. In the left menu, select "Remote Settings".
7. Select "Allow remote connections to this computer".
8. Click on "Select Users..." and select users on this computer which will be allowed to use RDP.

After you perform these steps, perform rescan on LAN or NetBIOS scanner and your computer will automatically appear under corresponding section in the Cyber Protect Connect client with "RDP" label.

Windows 10

Do the following:

1. Right click on the start menu.
2. Select "System".
3. In the left menu, select "Remote Settings".

4. Select "Allow remote connections to this computer".
5. Click on "Select Users..." and select users on this machine which will be allowed to use RDP.

After you perform these steps, perform rescan on LAN or NetBIOS scanner and your computer will automatically appear under corresponding section in the Cyber Protect Connect client with "RDP" label.

Make your computer accessible outside the local network

We recommend using Acronis Cyber Protect Connect Clouds, which makes your computer automatically accessible over internet without any additional router or port configuration.

For manual setup, if you want to connect to your computer while not being in the same subnet, you need to do the following:

1. Ensure that your computer has a stable host name or IP address.
   If you do not have static IP or a host name, use a dynamic DNS service, like dyndns.org.
2. Configure port forwarding on the network router to pass incoming connections from router to your server.
   You need to forward connections to the port of your computer (3389 for RDP, 5900 for VNC). Please refer to your router documentation for detailed instructions on how to do this.
3. Configure firewall on your computer to accept incoming connections on the port.
   macOS X enables this automatically when you turn on Screen Sharing or Remote Management. On Windows, you'll need to add the RDP port to the exception list of the Windows Firewall.
4. As alternative, you can use SSH tunnelling to access your local machine through the other machine with SSH running.

SSH tunnel using authentication key instead of password

The advantage of this method, is that you don't need different passwords to log on different servers. Once the public key is installed on the server, access will be granted with no password question. You can also authenticate via the personal private key on all servers, needing not to remember several passwords.

If target server running Windows, you can use SSH tunneling to perform secure connection from your device to intermediary machine (SSH host).

After you create two associated keys, the public key has to be stored on the remote computer host, and the private key should be stored on your device.

To generate a pair of keys on a Mac, do the following:

1. Open Terminal.app.
2. Execute this command: ssh-keygen.
3. Enter passphrase that will be the password needed to use your private key. *(This could save you from unauthorized access under your username if the device with private key is stolen.)*
4. Repeat passphrase.

5. Open the folder where your pair of keys was saved. If you used default location, you may go there using this command: open ~/.ssh/.

To install the public key on the server, simply add the contents of client's ~/.ssh/id_rsa.pub to the server's ~/.ssh/authorized_keys.
In most cases, this command will do the trick: cat ~/.ssh/id_rsa.pub >> ~/.ssh/authorized_keys.

To generate a pair of keys in Windows, do the following:

1. Download PuTTY.
2. Extract files.
3. Launch PUTTYGEN.exe.
4. Select SSH-2 RSA.
5. Click "Generate".
6. Enter passphrase that will be the password needed to use your private key. *(This could save you from unauthorized access under your username if the device with private key is stolen.)*.
7. Save public and private keys to any directory with names you like.

To save your private key to the device:

1. Connect your iOS device to your computer.
2. Open iTunes if it does not start automatically.
3. Locate the device in iTunes and go to Apps tab, then scroll down to the File Sharing section.
4. Select Acronis Cyber Protect Connect in the Apps list.
5. Drag the private key file (usually named id_rsa) to the Cyber Protect Connect client documents.

To connect securely using this key:

1. Go to Security preferences of your connection in the Cyber Protect Connect client.
2. Select Public Key authentication type.
3. Select Private key file from the list of stored keys.
4. Enter key passphrase, if needed.
5. Save connection preferences.

Connection

Viewer

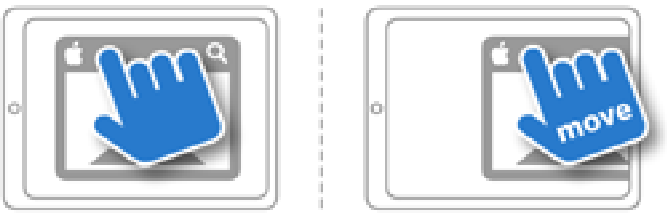
When you connect to a computer, the Acronis Cyber Protect Connect client **Viewer** screen shows the remote desktop.

NOTE: If you connect using "Ask for observe" option, the connection opens in the Observe mode so you cannot control or otherwise interact with the remote computer.

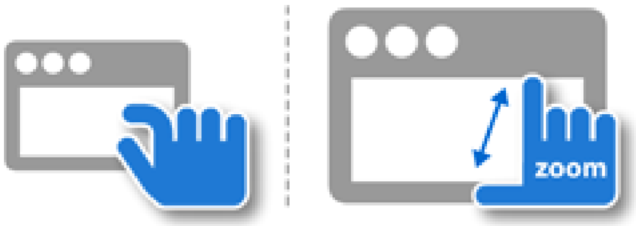
Gestures

The Cyber Protect Connect client supports multitouch gestures for the following actions:

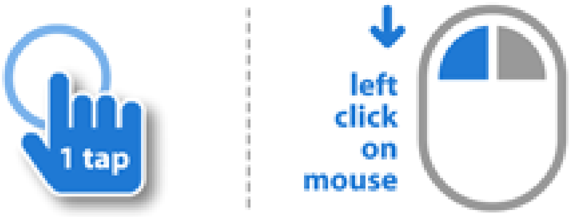
- **pan**



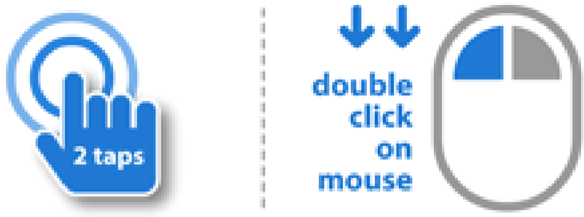
- **zoom**



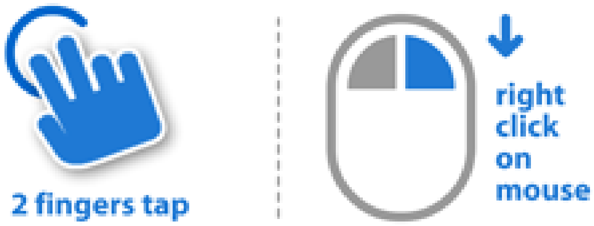
- **click**



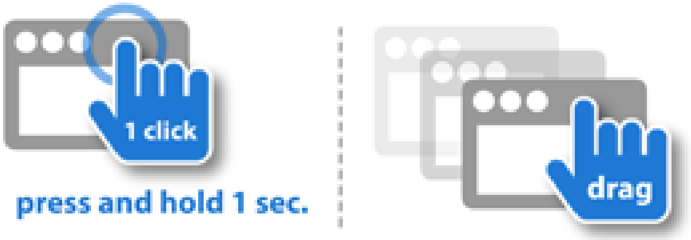
- **double click**



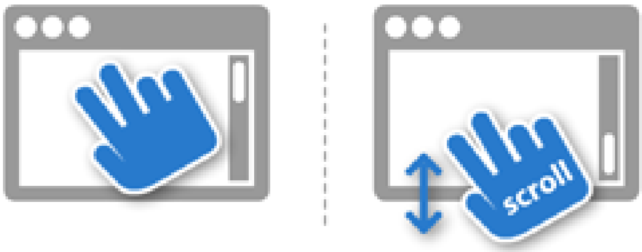
- **right click**



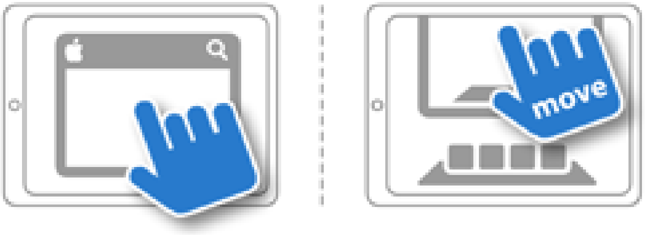
- **drag**



- **scroll**: move two fingers in the same direction to scroll. Vertical scroll is available on all kinds of connection. Horizontal scroll works on NEAR and Screen Sharing.



- **show the hiding Dock or taskbar**: pan the screen in the opposite direction.



Toolbar

The Cyber Protect Connect client toolbar contains the most useful buttons to manage your connection and to control the server.

Representation of options on the toolbar is depended of width of your screen in current device orientation. To see all use landscape orientation.

Keyboards
The Cyber Protect Connect client allows you to use two keyboards: standard Android keyboard and extended one. Extended keyboard provides you with keys that you usually cannot access through standard Android keyboard, such as F1-F10, Escape and cursor keys. Special buttons for actions like "Cut", "Copy" and "Paste" are also included.

Right & middle click mode
This button will imitate right mouse click or middle click instead of left one while it is selected. It will not be released until you do tap (e.g. panning gesture won't cause it to release).

Touchpad mode
Touchpad mode button (the hand) will switch the way you control the Cyber Protect Connect client viewer. In this mode, your finger movements would move the cursor over the screen and tapping on

the screen would actually tap at the position of the cursor. You can continue to use gestures like two finger scroll to perform scrolling and two finger click to perform the right click.

Modifiers
Modifier keys (^, ⌥, ⌘ / Ctrl, Alt, Win) are put on the toolbar. Once you press a modifier button, it stays pressed until released.
E.g.: to close a browser tab, first you press the modifier (⌘ or Ctrl), then 'T', then modifier again.
Note: if width of your screen is insufficient, modifiers buttons can be hidden. In that case try another orientation of your device.

Cursor keys
If width of your screen in current device orientation is enough - the cursor keys (← , ↓, ↑, →) are also present on the toolbar.

Settings menu

(options are depended of connection type)
Press settings menu button to get access to full screen mode, zoom pixel to pixel or to change connection settings on the fly.

Disconnect
select disconnect to terminate connection to current server

Take Screenshot
Takes the screenshot of the remote computer and allows you to share it.

Zoom 1:1
Zooms the current screen to pixel-to-pixel ratio.

Fullscreen Mode
Hides the toolbar. To get access to toolbar press "Back" button.

Show Connection Info
Displays HUD with connection information like rate, bandwidth and time connected.

Connection settings:

Display Resolution Select the resolution of the remote session.

Quality Select the quality depending on your current workflow. Smooth is the best for games or video playback. It uses hardware-accelerated H.264 to encode the remote desktop. Sharp gives you the best quality picture at the sacrifice of frames per second. Balanced (the default) is optimized for the general use.

Hide or **Always Show Local Cursor** If the remote computer displays cursor as part of the remote screen you can disable or always enable the local cursor rendering.

Synchronize Clipboard If set, the Cyber Protect Connect client will perform automatic clipboard synchronization if server supports it. If you copy something into the pasteboard on iOS device, the Cyber Protect Connect agent sends it to the server. The opposite is also true - copying on server would automatically transfer clipboard contents to iOS device. Supported types include text and images . If remote server does not support automatic clipboard synchronization (notable example is old version of Apple Screen Sharing server), you can use "Send clipboard" and "Get clipboard" actions, whose would appear in Settings menu to transfer pasteboard to and from server.

Viewer settings:

Cursor scale Choose between available mouse cursor sizes: 1x, 2x, 3x.

Invert Scrolling If set, vertical scrolling gestures will be inverted.

Don't Dim Display If set, the Cyber Protect Connect will would block display from dimming while connected.

Bluetooth mouse settings:

Mouse sensitivity Set the preferred sensitivity of mouse buttons.

Scroll sensitivity Set the preferred sensitivity of screen scrolling.

Options for VNC servers:

Lock remote screen (Apple Screen Sharing only)
Blacks out the physical screen on the machine you're connected to, preventing the others to see your actions on it.

Preferred Encodings You may choose the preferred graphical encodings used by the Cyber Protect Connect client for every server. If all encodings are turned off, the raw encoding will be used (which does not perform any compression and needs the widest bandwidth).

Color Depth This option is only available if Adaptive codec is selected. You can adjust color depth of the Viewer screen. The higher the value - the greater the width of bandwidth used. You can get satisfying level of picture quality vs. performance adjusting this option, e.g. on GPRS connection or on older devices you need to set it on 8 or 16 bits.

External Keyboard

The Cyber Protect Connect client fully supports the external keyboard, including all modifier keys, such as Shift, Command and Windows button.

Tips and Tricks (ScreenSharing)

Dual-screen setup: you can choose whether you want to work with only one display of your multimonitor setup, or with all of them together, by choosing needed display in connection preferences on-the-fly.

Spaces navigation: to move between spaces on a Mac, use the Ctrl+Arrow keys shortcut (unless you have disabled it on your Mac).

File Transfer

You can use the Cyber Protect Connect client file transfer feature to move files from any of your computers to the mobile device and back. File transfer is part of NEAR protocol, so you must install Acronis Cyber Protect Connect agent on the computer you will be connecting to and enable file transfer in agent settings.

To start file transferring, tap on the computer in your list and select File Transfer. You will see a list of local and remote folders. Tap marker icon (or long press on a file), mark files you want to transfer, select the folder to transfer them and click the transfer icon in the lower right corner. File transfer will start.

Cyber Protect Connect client for Android

Cyber Protect Connect client overview

Introduction

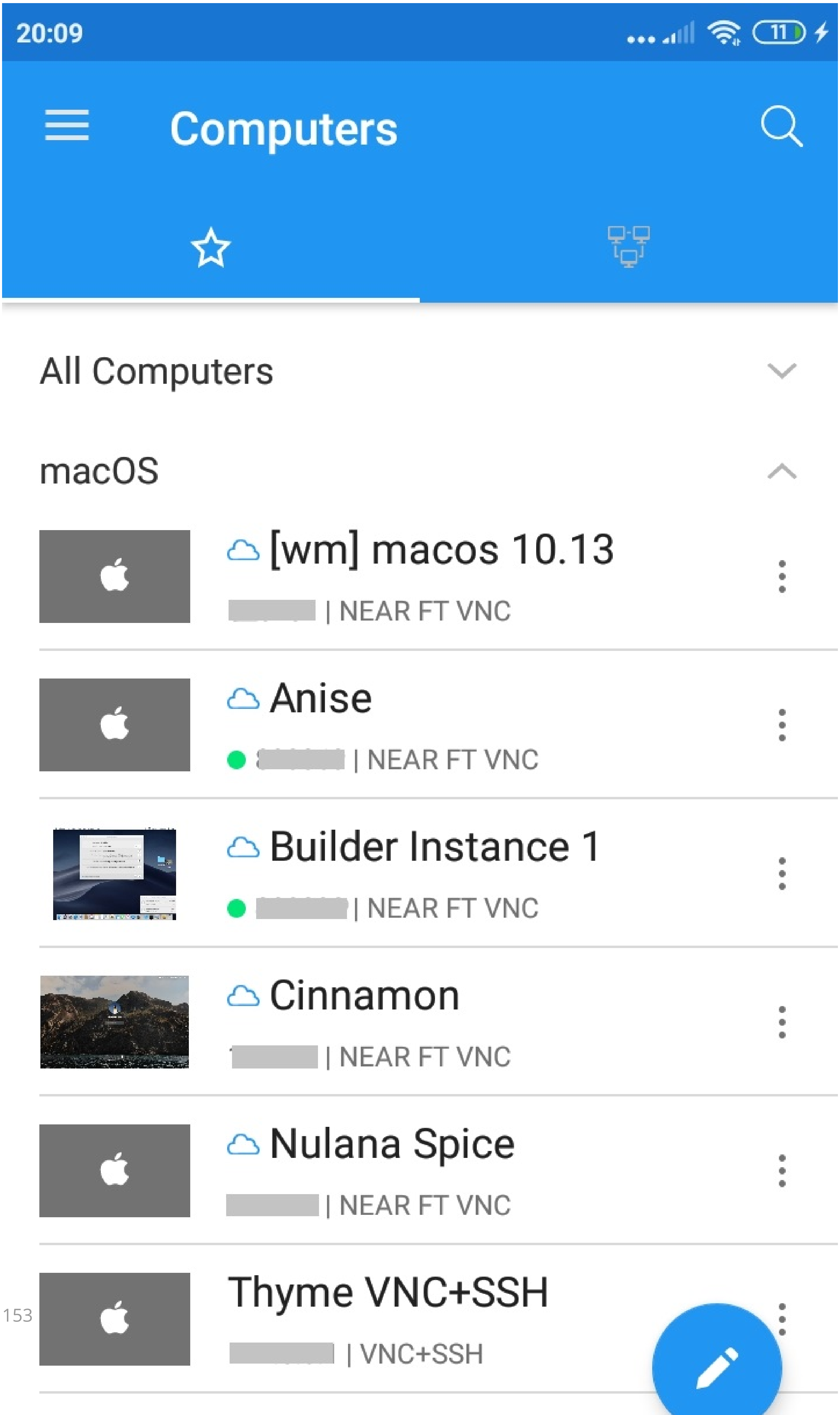
The Acronis Cyber Protect Connect client is a powerful yet simple client for remote access. You can connect to your computer from anywhere with almost zero lag via NEAR protocol.

The Cyber Protect Connect client supports:

- NEAR – the Cyber Protect Connect client's own low-latency protocol
- Remote Desktop Protocol (RDP)
- Apple Screen Sharing
- Virtual Network Computing (VNC)

It allows you to connect to any remote desktop running any operating system from your Android device.

Main Screen



All Computers

macOS

[wm] macos 10.13
[redacted] | NEAR FT VNC

Anise
● [redacted] | NEAR FT VNC

Builder Instance 1
● [redacted] | NEAR FT VNC

Cinnamon
[redacted] | NEAR FT VNC

Nulana Spice
[redacted] | NEAR FT VNC

Thyme VNC+SSH
[redacted] | VNC+SSH

Cyber Protect Connect Account

Register at connect.acronis.com to get an Acronis Cyber Protect Connect Cloud account and connect to remote computers using NEAR, and store and synchronize your remote connections and credentials across all devices.

When logged in, this pane displays your account information page and notifications from the Acronis Cyber Protect Connect console.

Stored Computers

The Cyber Protect Connect Stored Computers screen presents a list of stored connections available to open.

When you connect to a nearby computer for the first time, you need to choose authentication type. When you disconnect, this computer gets added to the Stored list. All settings that you've selected or changed on-the-fly, will be stored. A star icon to the right of the connection name indicates that you have this connection in the Stored list.

Connections that you have never visited before have a default "blank" thumbnail and no stored settings.

To add a connection manually

1. Go to the menu in the right bottom corner and press [+] button.
2. Select the type of a new connection.
3. Type in the address (Computer ID for NEAR, and hostname or IP for VNC or RDP).

   The other fields are optional.

   If you leave the **Port** field blank, the Cyber Protect Connect client will use the default value (5900 for VNC and 3389 for RDP).

When you finish, the new connection will appear in the Stored list with a blank thumbnail.

When you disconnect after a successful connection, the Cyber Protect Connect client saves the remote screen as a thumbnail to help you recognize it later. The thumbnail gets refreshed at the end of every session. To disable thumbnail saving, set "Store thumbnail" option to Off.

Nearby

The Cyber Protect Connect client uses Bonjour and LAN scanners to discover nearby computers available to connect.

- Bonjour: nearby servers on the local subnet that announce themselves using Bonjour technology.
- LAN: IP address/port scan of all computers available on the Wi-Fi interface.

Quick Connect

You may quickly connect to a remote computer running Cyber Protect Connect agent or Cyber Protect Connect Quick Assist using this pane.

- To establish a connection, enter the **Computer ID** and **Access Code** shown in the Cyber Protect Connect agent on the remote computer.

Application Settings

Color theme

Choose light or dark color theme. the Cyber Protect Connect client uses the system setting if possible.

Computer list settings

Sort mode Choose how to sort your stored connections: by name, address or online status.

Compact view Choose to show more servers in the same screen estate.

Connection settings

Auto Reconnect If set, the Cyber Protect Connect client will try to re-establish connection automatically when disconnected (for example. if you have answered a call on your device or switched to another app).

Show hidden files in file transfer Choose whether you want to see and transfer hidden and system files in the File Transfer dialog.

Offer saving credentials by default If set, the Cyber Protect Connect client will offer saving credentials by default.

Viewer options

Screen orientation Choose screen orientation for a remote connection: portrait, landscape or automatic. This can be changed on the fly.

Cursor scale Choose between available mouse cursor sizes: 1x, 2x, 3x.

Don'tdimscreen If set, the Cyber Protect Connect client will prevent your device's screen from dimming while connected to a remote computer.

Visualize clicks If set, the Cyber Protect Connect client will show a spot to let you know when a click is registered.

Invert Scroll If set, the direction of vertical scrolling will be inverted.

Scroll sensitivity Set the preferred sensitivity of screen scrolling.

Fullscreen type Allows to setup elements of user interface, which will be hidden in the full screen mode - only the Cyber Protect Connect client toolbar, only Android toolbar or both.

Alternative keyboard processing (Chrome on-screen keyboard) If you prefer Chrome on-screen keyboard, you can use it during remote session.

Remapsystemkey You can remap the modifier keys to use a Ctrl or Alt key as Win/Cmd.

Alwaysshowfunctionkeys Enable to display F1-F12 keys on Viewer toolbar. If disabled, they will be accessible from the extended keyboard.

Security

Curtain Mode on Mac Connections Turn on if you want the remote screen to be locked automatically each time you connect to a remote Mac with NEAR or Screen Sharing.

App security & privacy Select **Master Password*** if you want the Cyber Protect Connect client to require additional authentication each time you start the application and/or after some time of inactivity.

* Master Password/Biometric Login on Android devices, and Face ID/Touch ID on iOS devices.

Synchronization

Synchronize connections Enable to sync your non-Cloud connections and Cloud server settings across your devices.

Acronis Cloud Keychain Turn on to sync your stored connections credentials across your devices using Acronis Cyber Protect Connect Cloud.

Upload session info to Cloud If set, the Cyber Protect Connect client will upload session info (protocol, duration and direction) to the Cloud automatically.

Computer Settings

Each stored computer in the list has its own drop-down settings menu, including:

Common settings

Name Computer name determines the name of your computer in the Acronis Cyber Protect Connect console web interface and in the Acronis Cyber Protect Connect client. Type or change it here.

Groups Enter or select group to include this computer in. Group servers in any way you like: by company, location, hardware type, and even owner's age.

Store Thumbnail The Cyber Protect Connect client saves the remote screen as a thumbnail to help you recognize it later. The thumbnail gets refreshed at the end of every session. To disable thumbnail saving, set "Store thumbnail" option to Off.

Connection settings

NEAR Settings

Authentication Options

Ask if needed You will be asked about the authentication if it is required.

No authentication If Acronis Cyber Protect Connect agent allows, you will connect to the computer without authentication.

Access Code Authentication by the Access Code, as displayed in Cyber Protect Connect agent main window on the target computer.

System Logon Uses Windows or Mac OS X user credentials to authenticate. Note that you will only be able to log in into logon session or the existing session of the specified user.

NEAR connection options

Quality Select the quality depending on your current workflow.

Smooth is the best for games or video playback. It uses hardware-accelerated H.264 to encode the remote desktop. Sharp gives you the best quality picture at the sacrifice of frames per second. Balanced (the default) is optimized for the general use.

Server Scale Enables or disables scaling of the remote desktop picture to optimize network bandwidth.

Redirect Sound Enables or disables the playback of the remote computer sound on your device.

Hide Local Cursor If the remote computer displays cursor as part of the remote screen you can disable the local cursor rendering.

VNC Settings

Options for Mac-based (Screen Sharing) servers

Keyboard through clipboard paste Having this option on you do not need to switch the keyboard layout on your server. You can type any national characters from keyboard layouts installed on your device. The only drawback of this method is that system clipboard and clipboard synchronization between your device and computer will not be available.

Quality Level To have the best experience over different network speed, the Cyber Protect Connect client allows selection of the quality level. You can choose between black & white, grayscale, medium, adaptive and full quality. The least bandwidth hungry is black and white. Adaptive quality codec provided by Apple Screen Sharing™ minimizes buffering and guarantees a fast start. It also provides a fast performance on average and slow connections, although it is rather CPU hungry.

Server Scaling You can further improve performance of the Cyber Protect Connect client on zoomed out view by setting up this option. On the connect stage the Cyber Protect Connect client sends a command to server to send back downscaled image. This will reduce required bandwidth and free your device resources.

Display Apple Screen Sharing only. If Mac you are connecting to have multiple displays, the Cyber Protect Connect client allows selection of the active monitor. Option include "Combined" to use all displays, or each display individually.

Options for other VNC servers

Operating system Selected server OS defines extended keyboard layout (OS-dependant modifiers) and Dock / taskbar icon for the corresponding gesture and ensures correct work of cut/copy/paste extended keyboard buttons.

Preferred Encodings You may choose the preferred graphical encodings used by the Cyber Protect Connect client for every server.

If all encodings are turned off, the raw encoding will be used (which does not perform any compression and needs the widest bandwidth).

Color Depth This option is only available if Adaptive codec is selected. You can adjust color depth of the Viewer screen. The higher the value - the greater the width of bandwidth used. You can get satisfying level of picture quality vs. performance adjusting this option, e.g. on GPRS connection or on older devices you need to set it on 8 or 16 bits.

SSH Tunneling

You may use a secured connection through SSH (SSH tunnel) to access your machine if you have SSH server available. To establish a secured connection, enable "Use SSH tunnel" option in the Cyber Protect Connect client connection preferences.
You will be asked to provide the following information:

SSH username This is the username that you will use to log in via SSH. Usually it is the same as your OS login on the remote computer.

To enable SSH connection on your Mac:

1. Go to System Preferences -> Sharing pane.
2. Enable Remote Login service.

Authentication type You may choose either interactive or public key-based way to authenticate. For interactive, you have to enter password associated with the SSH username. For public-key based authentication, you need to have a pair of keys. For detailed instructions, see section 10.

SSH password (or Private key passphrase)
You may fill it in advance, or leave blank if you want to be asked for this password on every connection attempt.

SSH host and **SSH port** determine the intermediary machine SSH connection goes through.

RDP Settings

Authentication Options

Domain Enter the Windows domain here if your computer is part of domain. If not, leave the field empty.

Username Enter the Windows username here.

Password Enter the Windows password here.

RDP Connection Options

Desktop Size Select the resolution of the remote session.

Autofit mode adapts RDP resolution to match your device. RDP resolution will be changed on rotations and entering/leaving fullscreen mode. Note: live resolution change only works for non-server Windows editions, starting from 8.1.

There are "Fullscreen (Portrait)" and "Fullscreen (Landscape)" options for the Cyber Protect Connect client to automatically calculate the resolution, so it fits the screen completely in Portrait or Landscape orientations correspondingly. Also, you can set up custom sizes if you select "Custom".

Desktop Scale Select the scale factor used for desktop elements. This is especially useful on high-resolution devices, like Surface Pro.

Performance options

Performance
Select the performance profile of the connection. In "Auto" mode, the Cyber Protect Connect client detects whether you are running on Wi-Fi or 3G and selects "3G" or "LAN" correspondingly. You can also select "Custom" profile and set up the details manually:

Wallpaper determines whether desktop background would be drawn

Full Window Drag if set, windows are moved with contents, otherwise only the outline will be displayed during drag

- **Menu Animations** determines whether menus would appear immediately or animated
- **Theming** if set, your Windows theme will be applied
- **Cursor Shadow** sets the cursor shadow drawing
- **Cursor Shadow** sets the cursor shadow drawing
- **Cursor Settings** disables cursor blinking
- **Font Smoothing** determines whether font smoothing will be in use
- **Desktop Composition** enables or disables desktop composition.

Compression Set to "On" if you want the Cyber Protect Connect client to compress all RDP traffic.
Note: this can be actually slower due to increased CPU requirements on Android device.

Color Depth Color depth determines the number of colors in the picture RDP would transfer. Higher value requires higher bandwidth.

Enhanced Graphics (H.264) Select to use hardware-accelerated H.264 encoding provides the best picture for work, video and games.

Audio Options

Audio Playback Selects audio mode.

- **None** no audio will be played or redirected
- **Play on Computer** audio will be played on the remote computer
- **Dynamic Quality** audio will be redirected to Android device and audio quality will be adapted automatically
- **Medium Quality** audio will be redirected to Android device with medium quality
- **High Quality** audio will be redirected to Android device with high quality

Audio Recording
Determines whether audio recoding (speaking to the microphone) will be transferred to the remote computer.

Redirection

Access your Android files as a folder on the remote computer.

Keyboard

Keyboard Mode (Unicode or Keycode)

Keyboard Type (choose what keyboard you use: software or hardware)

Advanced Options

Console Session Set to on if you want to connect to the existing first session on RDP server (Windows Server 2003 only).

Startup Program Specify the path to the executable, which will be started on user logon (Windows Server only)

Working Directory Specify the working directory for the startup program. Only applies if startup program is set. (Windows Server only)

RD Gateway

If your company is using Remote Desktop Gateway to provide an access to your machines within your company network, specify the gateway parameters here.

SSH Tunneling

You may use a secured connection through SSH (SSH tunnel) to access your machine if you have SSH server available. To establish a secured connection, enable "Use SSH tunnel" option in the Cyber Protect Connect client connection preferences.

Supported servers and authentication modes

NEAR

You can install Acronis Cyber Protect Connect agent and Acronis Cyber Protect Connect Quick Assist with NEAR on the following operating systems:

- Windows 7 or later
- MacOS X 10.11 or later
- Generic Linux with X server

VNC servers

Acronis Cyber Protect Connect client supports the following servers and authentication modes:

- Mac OS X Screen Sharing™: Ask for observe, Ask for control, Mac OS X authentication (Mac OS X username + password), VNC password;
- UltraVNC: VNC password, MS Logon II authentication (Windows username + password);
- RealVNC (without encryption): VNC password;
- TightVNC: VNC password;
- TigerVNC: VNC password;
- TurboVNC: VNC password;
- x11vnc: VNC password.

You may also connect to any of supported servers over SSH.

RDP servers

The Acronis Cyber Protect Connect client RDP supports the connections to the following Windows versions:

- Windows XP SP1, SP2, SP3 (starting from Professional)
- Windows Server 2003
- Windows Vista (starting from Professional)
- Windows 7 (starting from Professional)
- Windows Server 2008/2008 R2
- Windows 8/8.1

- Windows Server 2012/2012 R2
- Windows 10

You may also connect to any of the supported servers over SSH.

How to set up a computer you are connecting to

NEAR

To install Acronis Cyber Protect Connect agent, follow the instructions in Acronis Cyber Protect Connect Cloud help.

VNC

You own a Mac

To enable Screen Sharing on your Mac

1. In **System Preferences**, open the **Sharing** pane.
2. Select the **Remote Management** service in the list and enable it.
3. Ensure that access is allowed for all users.
4. Click **Options...** and enable all options in the list.
5. Click **Computer settings...** and enable **Anyone may request permission to control screen**.

After you complete these steps, your Mac appears automatically under the **Bonjour** section in the Acronis Cyber Protect Connect client.

You own a PC

First select one VNC server. The most popular ones are Ultra VNC and Tight VNC.

After you complete these steps, perform rescan using **local network** or **NetBIOS** scanner to discover your computer.

RDP

Windows XP and Windows Server 2003

Do the following

1. In **Control Panel**, select **Switch to Classic View**.
2. Select **System**.
3. Click the **Remote** tab.
4. Enable **Allow users to connect remotely to this computer**.
5. Click **Remote Desktop Users** and select users on this computer who will be allowed to use RDP.

After you complete these steps, perform rescan on LAN or NetBIOS scanner and your computer will automatically appear under the corresponding section in the Cyber Protect Connect client with "RDP" label.

Windows 7 and Windows Server 2008

Do the following

1. In the **Control panel**, change the **view by** to **Large Icons**.
2. Click **System**.
3. In the left menu, select **Remote Settings**.
4. Select **Allow remote connections to this computer**.
5. Click **Select Users...**, and select the users on this computer who will be allowed to use RDP.

Windows 8

Do the following

1. From the Metro interface, click **Desktop** to get access to the desktop.
2. Move your mouse to the left-bottom corner and right-click it.
3. In the menu, select **Control Panel**.
4. In the **Control Panel**, change **view by** to **Large Icons**.
5. Click **System**.
6. In the left menu, select **Remote Settings**.
7. Select A**llow remote connections to this computer**.
8. Click Select Users..." and select users on this machine which will be allowed to use RDP.

After you complete these steps, perform rescan on LAN or NetBIOS scanner and your computer will automatically appear under corresponding section in the Cyber Protect Connect client with "RDP" label.

Windows 10

Do the following

1. Right click on the start menu.
2. Select System.
3. In the left menu, select Remote Settings.
4. Select Allow remote connections to this computer.
5. Click Select Users... and select users on this computer who will be allowed to use RDP.

After you complete these steps, perform rescan on LAN or NetBIOS scanner and your computer will automatically appear under corresponding section in the Cyber Protect Connect client with "RDP" label.

Make your computer accessible outside the local network

We recommend using Acronis Cyber Protect Connect Cloud, which makes your computer automatically accessible over internet without any additional router or port configuration.

For manual setup, to your computer while not being in the same subnet

1. Ensure that your computer has a stable host name or IP address.
   If you do not have static IP or a host name, use a dynamic DNS service, such as dyndns.org.
2. Configure port forwarding on the network router to pass incoming connections from router to your server.
   You need to forward connections to the port of your computer (3389 for RDP, 5900 for VNC).
   Refer to your router documentation for detailed instructions on how to do this.
3. Configure firewall on your computer to accept incoming connections on the port.
   MacOS X enables this automatically when you turn on Screen Sharing or Remote Management.
   On Windows, you will need to add the RDP port to the exception list of the Windows Firewall.
4. As an alternative, you can use SSH tunnelling to access your local computer through the other computer with SSH running.

SSH tunnel using authentication key instead of password

The advantage of this method, is that you do not need different passwords to log on different servers. Once the public key is installed on the server, access will be granted with no password question. You can also authenticate via the personal private key on all servers, needing not to remember several passwords.

If target server running Windows, you can use SSH tunneling to perform secure connection from your device to intermediary computer (SSH host).

After you create two associated keys, the public key has to be stored on the remote computer host, and the private key should be stored on your device.

To generate a pair of keys on a Mac

1. Open Terminal.app.
2. Run the following command: ssh-keygen.
3. Enter passphrase that will be the password needed to use your private key. *(This could save you from unauthorized access under your username if the device with private key is stolen.)*
4. Repeat passphrase.
5. Open the folder where your pair of keys was saved. If you used default location, you may go there using this command: open ~/.ssh/

To install the public key on the server, add the contents of client's ~/.ssh/id_rsa.pub to the server's ~/.ssh/authorized_keys.
In most cases, this command will do the trick: cat ~/.ssh/id_rsa.pub >> ~/.ssh/authorized_keys

To generate a pair of keys in Windows

1. Download PuTTY.
2. Extract files.
3. Start PUTTYGEN.exe.
4. Select SSH-2 RSA.
5. Click "Generate".
6. Enter a passphrase that will be the password needed to use your private key. *(This could save you from unauthorized access under your username if the device with private key is stolen.)*
7. Save public and private keys to any directory with names you like.

To save your private key to the device:

Transfer private key file (usually named id_rsa) from you computer to the Cyber Protect Connect client documents with your Google Account or with a USB cable. For more information, see here.

To connect securely using this key

1. Go to Security preferences of your connection in Cyber Protect Connect client.
2. Select Public Key authentication type.
3. Select Private key file from the list of stored keys.
4. Enter key passphrase, if needed.
5. Save connection preferences.

Connection

Viewer

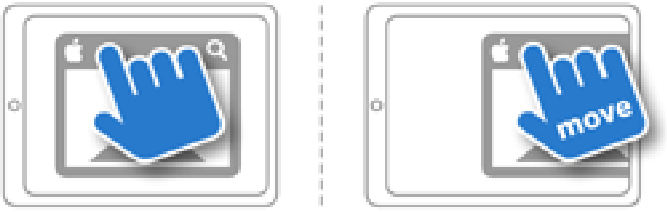
When you connect to a computer, the Acronis Cyber Protect Connect client Viewer screen shows the remote desktop.

NOTE: If you connect using "Ask for observe" option, the connection opens in the Observe mode so you cannot control or otherwise interact with the remote computer.

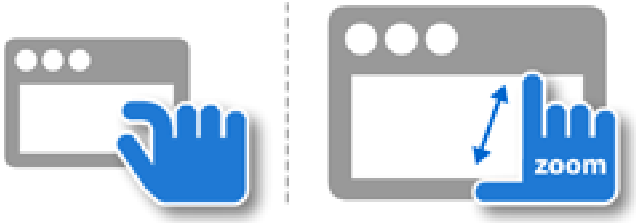
Gestures

The Acronis Cyber Protect Connect client supports multitouch gestures for the following actions:

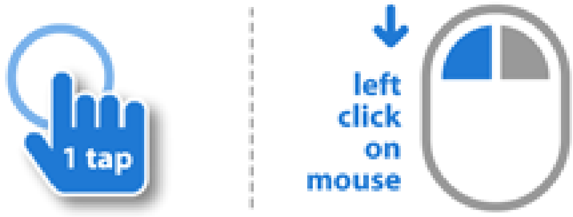
- **pan**



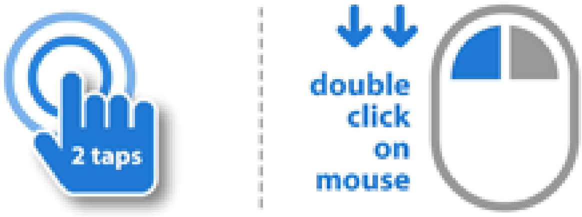
- **zoom**



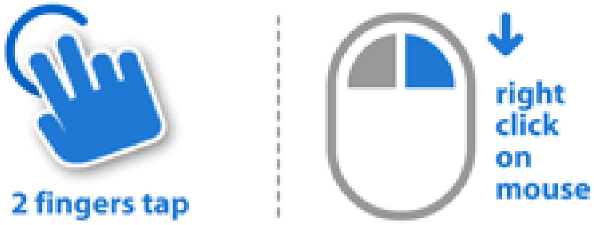
- **click**



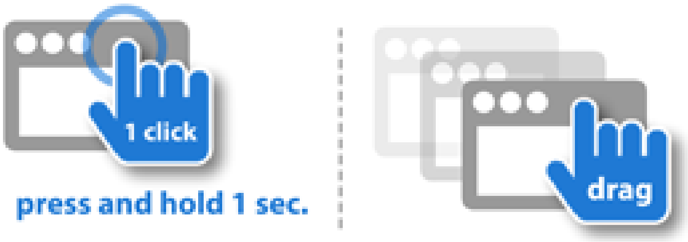
- **double click**



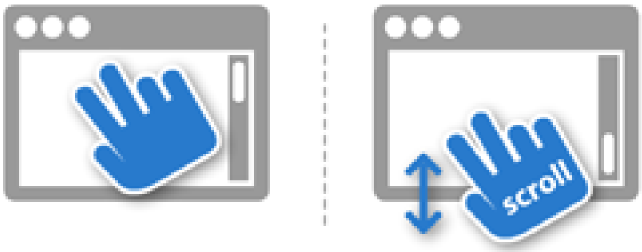
- **right click**



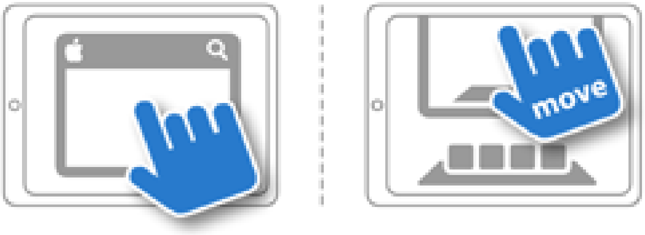
- **drag**



- **scroll**: move two fingers in the same direction to scroll. Vertical scroll is available on all kinds of connection. Horizontal scroll works on NEAR and Screen Sharing.



- **show the hiding Dock or taskbar**: pan the screen in the opposite direction.



Toolbar

The Cyber Protect Connect client toolbar contains the most useful buttons to manage your connection and to control the server.

Representation of options on the toolbar is depended of width of your screen in current device orientation. To see all use landscape orientation.

Keyboards The Cyber Protect Connect client allows you to use two keyboards: standard Android keyboard and extended one. Extended keyboard provides you with keys that you usually cannot access through standard Android keyboard, such as F1-F10, Escape and cursor keys. Special buttons for actions like "Cut", "Copy" and "Paste" are also included.

Right & middle click mode This button will imitate right mouse click or middle click instead of left one while it is selected. It won't be released until you do tap (for example, panning gesture will not cause it to release).

Touchpad mode Touchpad mode button (the hand) will switch the way you control the Cyber Protect Connect client viewer. In this mode, your finger movements would move the cursor over the screen and tapping on the screen would actually tap at the position of the cursor. You can continue to use gestures like two finger scroll to perform scrolling and two finger click to perform the right click.

Modifiers Modifier keys (^, ⌥, ⌘ / Ctrl, Alt, Win) are put on the toolbar. Once you press a modifier button, it stays pressed until released.
For example, to close a browser tab, first you press the modifier (⌘ or Ctrl), then 'T', then modifier again.
Note: if the width of your screen is insufficient, modifiers buttons can be hidden. In that case try another orientation of your device.

Cursor keys If width of your screen in current device orientation is enough - the cursor keys (← , ↓, ↑, →) are also present on the toolbar.

Settings menu

The options depend on the connection type.
Click the settings menu button to get access to full screen mode, zoom pixel to pixel or to change connection settings on the fly.

Disconnect Select Disconnect to end the connection to the current server.

Take Screenshot Takes the screenshot of the remote computer and allows you to share it.

Zoom 1:1 Zooms the current screen to pixel-to-pixel ratio.

Fullscreen Mode Hides the toolbar. To get access to toolbar press "Back" button.

Show Connection Info Displays HUD with connection information like rate, bandwidth and time connected.

Lock remote screen (Apple Screen Sharing only) Blacks out the physical screen on the computer you are connected to, preventing the others to see your actions on it.

Connection settings:

Display Resolution Select the resolution of the remote session.

Quality Select the quality depending on your current workflow. Smooth is the best for games or video playback. It uses hardware-accelerated H.264 to encode the remote desktop. Sharp gives you the best quality picture at the sacrifice of frames per second. Balanced (the default) is optimized for the general use.

Hide or **Always Show Local Cursor** If the remote computer displays cursor as part of the remote screen you can disable or always enable the local cursor rendering.

Synchronize Clipboard If set, Cyber Protect Connect client would perform automatic clipboard synchronization if server supports it. If you copy something into the pasteboard on device, the Cyber Protect Connect client sends it to the server. The opposite is also true - copying on server would automatically transfer clipboard contents to device. Supported types include text and images . If remote server does not support automatic clipboard synchronization (notable example is old version of Apple Screen Sharing server), you can use "Send clipboard" and "Get clipboard" actions, whose would appear in Settings menu to transfer pasteboard to and from server.

Keyboard settings:

Keyboard mode In some verions of Android you may need to set exact input type in connection settings. Set "Keyboard type" to "Hardware" for external keyboard.

Keyboard type (RDP only) Select unicode or keycode keyboard input mode.

Keyboard layot (Apple Screen Sharing only)

Options for VNC servers:

Preferred Encodings You may choose the preferred graphical encodings used by the Cyber Protect Connect client for every server. If all encodings are turned off, the raw encoding will be used (which does not perform any compression and needs the widest bandwidth).

Color Depth This option is only available if Adaptive codec is selected. You can adjust color depth of the Viewer screen. The higher the value - the greater the width of bandwidth used. You can get satisfying level of picture quality vs. performance adjusting this option, e.g. on GPRS connection or on older devices you need to set it on 8 or 16 bits.

Server Scaling You can further improve performance of Cyber Protect Connect client on zoomed out view by setting up this option. On the connect stage Cyber Protect Connect client sends a command to server to send back downscaled image. This will reduce required bandwidth and free your device resources.

External Keyboard

The Cyber Protect Connect client fully supports the external keyboard, including all modifier keys, such as Shift, Command and Windows button.

In some versions of Android, you may need to set exact input type in connection settings. Set "Keyboard type" to "Hardware" for external keyboard.

Tips and Tricks (ScreenSharing)

Dual-screen setup: you can choose whether you want to work with only one display of your multimonitor setup, or with all of them together, by choosing needed display in connection preferences on-the-fly.

Spaces navigation: to move between spaces on a Mac, use the Ctrl+Arrow keys shortcut (unless you have disabled it on your Mac).

File Transfer

You can use the Cyber Protect Connect client file transfer feature to move files from any of your computers to the mobile device and back. File transfer is part of NEAR protocol, so you need to install Acronis Cyber Protect Connect agent on the computer you will be connecting to and enable file transfer in agent settings.

To start file transferring, tap on the computer in your list and select File Transfer. You'll see a list of local and remote folders. Tap marker icon (or long press on a file), mark files you want to transfer, select the folder to transfer them and click the transfer icon in the lower right corner. File transfer will begin.

Index

(

(or other Linux that has no graphical desktop environment installed) 70

3

3.8. RD Gateway 141

3.9. SSH Tunneling 141

A

About authentication types 106

About URL syntax and *.vncloc files 100

ACCESS PERMISSIONS 30

Accessibility Permission 13

Account settings 46

Acquiring Permissions for Remote Access on Mac with macOS 10.15 Catalina 27

Acquiring permissions for remote access on macOS 12

Acronis Cyber Protect Connect 7

Actions 44, 130

Adaptive Codec 7

Add a remote computer by Computer ID 96

Add a remote computer by IP address 96

Adding a custom agent configuration 56

Adding a remote computer by IP address 92

Adding computers to the team 56

Adding credentials 93

Adding users to an access group 55

Adjusting quality for slow connections 111

Advanced Options 140, 160

Application Settings 135, 155

Assigning credentials for automatic authentication to a workload 93

Audio codec 71

Audio Options 118, 140, 160

Authentication Options 136, 139, 157, 159

Automatic distribution of custom agent configuration updates 57

B

Bluetooth mouse settings 149

C

Capturing a remote desktop screen to a file 119

Change Your Mind 17

Changing computer ID 41

Changing the access code 39

Chat 45

Checking dependencies on Linux 71

Color theme 155

Common tasks 35

Computer list settings 135, 155

Computer settings 136

Computer Settings 156

Configure the firewall to accept incoming connections 124

Configure the network router to accept incoming connections 124

Configuring email-based two-factor authentication for a team 54

Configuring permissions for remote access on macOS 10.14 Mojave 23, 32

Configuring remote sound 39

Configuring Single sign-on (SSO) access 49

Configuring user permissions 55

Connect using Acronis Cyber Protect Connect Cloud 95

Connect using Acronis Cyber Protect Connect Quick Assist 95

Connect using Back to My Mac 97

Connecting to a headless Linux 71

Connecting to a remote workload using saved credentials 94

Connecting to Mac using SSH authentication key 105

Connecting to remote computers 91

Connecting to remote workloads using Acronis Cyber Protect Connect Quick Assist 108

Connecting using Remote Desktop Gateway 105

Connecting via Acronis Cloud 90

Connecting via Cyber Protect Connect account 91

Connection 135, 145, 165

Connection pane 84

Connection settings 136, 148, 155, 157, 168

Controlling or observing a single computer 108

Create a single connection 128

Create group 127

Creating a connection 91

Creating a connection knowing the target Computer ID 91

Creating a new team 49

Creating a new team user 55

Custom claims mapping 53

Cyber Protect Connect Account 135, 154

Cyber Protect Connect agent 9

Cyber Protect Connect agent for Linux 69

Cyber Protect Connect agent for Mac 61

Cyber Protect Connect agent for Windows 65

Cyber Protect Connect client 73

Cyber Protect Connect client for Android 151

Cyber Protect Connect client for iOS 131

Cyber Protect Connect client menu in the system menu 82

Cyber Protect Connect client overview 131, 151

Cyber Protect Connect client user interface 74

Cyber Protect Connect Cloud 90

Cyber Protect Connect console 9, 43, 63, 67

Cyber Protect Connect console main features 44

Cyber Protect Connect licensing 43

Cyber Protect Connect Quick Assist 58

Cyber Protect ConnectAccount 134

D

Delete a cloud computer 130

Delete a single connection 128

Delete computer's connection credentials 130

Delete computer's connection settings 130

Delete connection credentials 129

Deleting credentials 94

Displaying connection info panel 112

E

Editing credentials 94

Enable RDP access on Windows 122

Enable SSH on Mac 126

Enabling automatic reconnect to the remote computer 112

Enabling desktop sharing on Windows 21

Enabling synchronization with the Cloud 94

Establishing a secured connection 103

External Keyboard 149, 169

F

File Transfer 150, 169

Find a computer in the local area network 96

Finding remote computers 95

Folder & File Redirection 118

Full Disk Access Permission 15

G

General pane 83

Gestures 145, 165

Get a list of actions available for a given cloud computer 129

Get a list of configured connections for a given cloud computer 129

Get a list of groups 127

Get a list of items in the group 127

Get credentials of one of the connections of cloud computer 129

Get settings of a specific connection of the cloud computer 129

Get the list of the connections in NEARBY pane 127

Get the main settings of a cloud computer 129

H

H.264 7

Helping someone once 35

How to get remote sound from a Linux 39

How to get remote sound from a Mac 39

How to get remote sound from a PC 39

How to install Acronis Cyber Protect Connect agent on Linux 69

How to set up a computer you are connecting to 142, 162

How to set up a Tight VNC server 142

How to set up an Ultra VNC server 142

HTTP API for Cyber Protect Connect client 127

I

Initiate connect to a remote cloud computer 130

Initiate connect to an existing connection 130

Install VNC, RDP or Screen Sharing server 120

Installing Acronis Cyber Protect Connect agent to a Debian-Based Distribution 69

Installing Acronis Cyber Protect Connect agent to Azure SLES 70

Installing Acronis Cyber Protect Connect agent to Raspbian 70

Installing Acronis Cyber Protect Connect Quick Assist to an RPM-Based Distribution 70

Installing from a package 69

Installing from a repository 69

Interacting with remote computers 108

Introduction 131, 151

Inviting a user to the team 54

K

Keyboard 160

Keyboard Mode 140

Keyboard pane 85

Keyboard settings 168

L

Logging in with Single sign-on 49

Logon Methods 8

M

Main Screen 132, 152

Main window 61, 65

Main window reference 74

Make a server accessible 123

Make a VNC or RDP server accessible over the Internet 123

Make your computer accessible outside the local network 144, 164

Managing stored server lists 97

Managing team users 54

Map 45

Microphone Permission 14, 26, 34

Multi-viewer window reference 85

Multiuser Access on Mac 8

N

NEAR 141-142, 161-162

NEAR connection options 136, 157

NEAR protocol 7

NEAR Settings 136, 157

Nearby 134, 154

Network 85, 136

O

Observeing multiple servers 98

Optimizing image transmission for Retina displays 103

Options for Mac-based (Screen Sharing) servers 137, 157

Options for other VNC servers 138, 158

Options for VNC servers 149, 169

OTHER PERMISSIONS 31, 34

Overview 44

P

Perform silent installation 126

Performance 117

Performance options 139, 159

Player window reference 88

Preferences window reference 83

Prerequisites 49, 57, 59

Printer Redirection 118

Protect confidential data with master password 87

Q

Quick Connect 135, 155

R

RD Gateway 160

RD Gateways 85

RDP 142, 162

RDP Connection Options 139, 159

RDP performance options, file, sound and printer sharing 117

RDP servers 141, 161

RDP Settings 139, 159

Recording sessions 119

Redirection 140, 160

Remote connections 64, 68

Reports 45

S

Screen Recording Permission 12

SCREEN RECORDING PERMISSIONS 28

Screen sharing server scaling 115

Screen sharing virtual displays 114

Screenshot 46

Securing transmitted data 104

Security 8, 103, 135, 156

Security pane 83

Set a stable host name for the computer 123

Setting up a server for remote access 120

Setting up remote access 10

Setting up remote access on macOS 10

Setting up remote access on Windows 19

Setting up VNC, RDP and Screen Sharing server 120

Settings 64, 68

Settings menu 148, 168

Sharing aremote computer with colleagues 36

Sharing clipboards between the remote and local computers 115

Single sign-on providers 50

Sound Transfer 8

SSH tunnel using authentication key instead of password 144, 164

SSH Tunneling 138, 158, 161

SSH Tunnels 85

SSO protocols 50

Stored Computers 134, 154

Supported servers and authentication modes 141, 161

Synchronization 85, 156

T

Team activity log 56

Team user roles 48

Tips and Tricks (ScreenSharing) 149, 169

Toolbar 147, 167

Transferring data between client and server in NEAR connection mode using the clipboard 117

Transferring data between the remote and local computers in Screen Sharing mode 116

Troubleshooting 70

Trusted users 63, 67

Two-Factor Authentication 46

U

Unicode Input 8

Uninstalling Acronis Cyber Protect Connect agent 42

Update a cloud computer's main settings (name + groups it belongs to) 129

Update a connection's credentials 128

Update an existing connection 128

Update cloud computer connection 129

User account control on remote Windows workloads 59

Using common credentials 92

Using Cyber Protect Connect Quick Assist in Acronis Cloud 91

Using Teams functionality 48

V

Video codec 71

Viewer 145, 165

Viewer options 155

Viewer pane 84

Viewer settings 149

Viewer window reference 77

Viewing session history 57

Viewing the remote desktop 110

VNC 142, 162

VNC servers 141, 161

VNC Settings 137, 157

W

Windows 10 143, 163

Windows 7 and Windows Server 2008 143, 163

Windows 8 143, 163

Windows XP and Windows Server 2003 142, 162

Working with cloud computers 129

Working with connections 128

Working with groups 127

Working with licenses 43

Working with Teams as a User 57

Working with Teams as an Admin user 49

Y

You own a Mac 142, 162

You own a PC 142, 162

C

Common settings 136, 156