Glossary

This section explains the terms used in Getscreen.me. Terms are grouped into remote access entities, system components, features, and the account environment.

November 16, 2026

Table of contents

1. Glossary 6
1.1 About Software 6
1.2 Terms Categories 6
2. Remote Access Entities 7
2.1 Remote Device 7
2.2 Technician 7
2.3 Connection 7
3. System Components 8
3.1 Server 8
3.2 Account 8
3.3 SaaS Server 8
3.4 Self-Hosted Server 8
3.5 Agent Application 8
3.6 Web Dashboard 8
3.7 Dashboard Application 8
3.8 Dashboard Chrome Extension 9
3.9 Gateway Application 9
4. Connection 10
4.1 Connection Window 10
4.2 Connection Participant 10
4.3 Connection Mode 10
4.4 Screen Control 10
4.5 File Manager 11
4.6 Terminal Mode 12
4.7 Control Panel 13
4.8 Video Channel 13
4.9 WebRTC Channel 13
4.10 WebSocket Channel 13
4.11 Connection History 13
4.12 Video Record 13
5. Share Screen 14
5.1 Share Link 14
5.2 Share Code 15
6. Permanent Access 17
6.1 Device Card 19

6.2 Group 20
6.3 Group Manager 20
6.4 Group Policy 21
6.5 Agent App Settings 22
6.6 Concurrent Connection 23
6.7 Mass Deployment 24
7. Quick Support 26
7.1 Invitation 26
7.2 Invitation Link 27
7.3 Invitation Code 27
7.4 Widget 27
7.5 Widget Embed Code 28
7.6 Widget Application 28
8. Team 32
8.1 Team Owner 32
8.2 Technician Invitation 32
8.3 Technician Account 33
8.4 WorkSpace 34
8.5 Department 34
8.6 Team Settings 34
8.7 Identity Provider (IdP) 35
8.8 LDAP 35
8.9 SAML SSO 36
9. Access Right System 38
9.1 Public Link 38
9.2 Access Right 38
9.3 Permission 38
9.4 Role 41
9.4.1 System Role 42
9.4.2 Role Purpose 42
9.4.3 Role Manager 42
9.5 Team Access 42
9.6 Public Access 43
9.6.1 Password Access 44
9.6.2 OTP Access 44
9.7 One-Time Access 44
9.8 Cross-Team Access 45
9.9 Unregistered Technician 46

10. Settings 48
10.1 Team Settings 48
10.2 Video Capture Settings 48
10.3 Video Records Settings 49
10.4 Branding Settings 50
10.5 Gateway Settings 51
10.5.1 Authorization Token 51
10.6 Integrations 52
10.7 HTTP API 53
10.7.1 API Key 53
11. Security 54
11.1 Dashboard Session 54
11.2 Two-Factor Authentication (2FA) 54
11.3 Audit Logs 55
11.4 Black Screen Mode 56
11.5 Lock Input Mode 56
12. License 57
12.1 Limits 57
12.1.1 Team 57
12.1.2 Permanent Access 57
12.1.3 Quick Support 58
12.2 Premium Options 58
12.2.1 Concurrent Connections 58
12.2.2 Joint Connections 58
12.2.3 File Manager 58
12.2.4 Terminal Mode 58
12.2.5 Support Mobile Devices 58
12.2.6 Black Screen Mode 58
12.2.7 Video Recording 58
12.2.8 Reboot During Connection 58
12.2.9 In-Session Calls 59
12.2.10 Support RDP Protocol 59
12.2.11 Connection History 59
12.2.12 In-session Unattended Access Request 59
12.2.13 Custom Proxy for Media Data 59
12.2.14 Wake-on-LAN 59
12.2.15 Public Access for Device 59
12.2.16 Customization of Public Access Link 59

12.2.17 Share with Another Account 59
12.2.18 Proxy Settings for Agent App 59
12.2.19 Server Access Through Gateway 60
12.2.20 Team Access Rights System 60
12.2.21 Departments for Technicians 60
12.2.22 Audit Log 60
12.2.23 Import Technicians from Identity Provider (LDAP) 60
12.2.24 Branding Title, Icon and Subdomain 60
12.2.25 Custom Domain for Links 60
12.2.26 HTTP API Access 60

1. Glossary

This section provides explanations of commonly used terms in the context of Getscreen.me software.

1.1 About Software

Getscreen.me is remote desktop software that allows users to remotely access and control computers and mobile devices over the Internet or a local network. It is designed for corporate network administration, technical support, and personal use.

Getscreen.me is developed by Point B Ltd, a private limited liability company based in Limassol, Republic of Cyprus. The Getscreen.me trademark is protected under applicable intellectual property laws in the jurisdictions where it has been granted legal protection.

1.2 Terms Categories

For convenience, the terms are grouped into semantic categories. These categories correspond to the structure and terminology used across the main user interfaces of the software:

- **Remote Access Entities** — the main participants and entities involved in the remote access process.
- **System Components** — tools used to establish and manage connections to remote devices.
- **Connection** — the process of connecting to remote devices to view and control their screens and use remote access tools.
- **Share Screen** — an optional Agent App feature for one-time screen sharing with or without remote control via a generated link, without requiring additional software installation.
- **Permanent Access** — an account section for managing linked devices and establishing unattended remote connections at any time.
- **Quick Support** — an account section for establishing one-time remote connections through invitation links without configuring permanent access or entering connection codes.
- **Team** — an account section for managing a team of technicians, enabling collaboration and workload distribution for remote support and administration.
- **Access Right System** — a system for managing technician access to devices and device groups, including permissions for specific actions.
- **Settings** — an account section for configuring system elements and features related to remote access and its administration.
- **Security** — an account section covering features related to account security and remote connection protection.
- **License** — descriptions of the entities and components of the account licensing system.

2. Remote Access Entities

The main participants and entities involved in the remote access process.

2.1 Remote Device

Remote Device is a computer device that is controlled remotely using remote access technology over the Internet or a local network.

A remote device can be a physical or virtual server, desktop computer, laptop, IoT device, mobile phone, or tablet.

2.2 Technician

Technician is a user who controls a remote device while being physically located elsewhere.

A technician can be a corporate network administrator, a technical support specialist, or an individual user accessing their own devices remotely.

2.3 Connection

Connection is a network session established between a Technician and a Remote Device to exchange data between them.

During a connection, control commands are sent from the technician to the remote device, while screen data from the remote device is transmitted back to the technician.

3. System Components

Learn about the key components of the system, including servers, applications, interfaces, and other elements used to provide and manage remote access.

3.1 Server

Server — the central component of the system that establishes and manages connections between remote devices and technicians. It operates as a web server and uses web protocols to exchange data between remote access participants.

3.2 Account

Account — a technician's user account on the server. Remote devices, invitations, connection history, team members, and other remote access settings are associated with the account.

3.3 SaaS Server

SaaS Server — the cloud-hosted version of the server deployed on the `getscreen.me` domain and available for public use. It is administered and maintained by the Getscreen.me team.

3.4 Self-Hosted Server

Self-Hosted Server — a version of the server designed to be deployed, operated, and maintained within the customer's own infrastructure. Learn More

3.5 Agent Application

Agent Application — a desktop application installed on a remote device. It captures the device screen and transmits it to the technician, while also executing commands received from the technician on the remote device.

The application is available for Windows, Linux, macOS, and Android.

3.6 Web Dashboard

Web Dashboard — a web interface for accessing your account, managing remote access settings, and connecting to remote devices directly from a browser.

3.7 Dashboard Application

Dashboard Application — a desktop application for accessing your account that provides the same core functionality as the web version.

Remote connections are opened directly inside the application rather than in a browser, making it more convenient for extended work with remote devices.

The application is available for Windows, macOS, and Linux.

3.8 Dashboard Chrome Extension

Dashboard Chrome Extension — a Google Chrome extension that provides quick access to selected Dashboard features.

It is designed for fast access to remote devices and invitations while working with other websites and web-based systems. Remote connections are opened in the browser.

3.9 Gateway Application

Gateway Application — a lightweight background utility without a graphical user interface. It is installed within a local network and acts as a gateway between internal network resources and the server.

The application is available for Windows and Linux and can be used for the following purposes:

- Proxying connection traffic to improve data transfer performance
- Importing technician accounts from an Identity Provider using LDAP
- Waking up remote devices using Wake-on-LAN
- Providing server access for devices located in isolated or restricted networks

4. Connection

This is an ongoing process of connecting a technician to a remote device, during which the technician can view and control the device screen and use the available remote access tools.

4.1 Connection Window

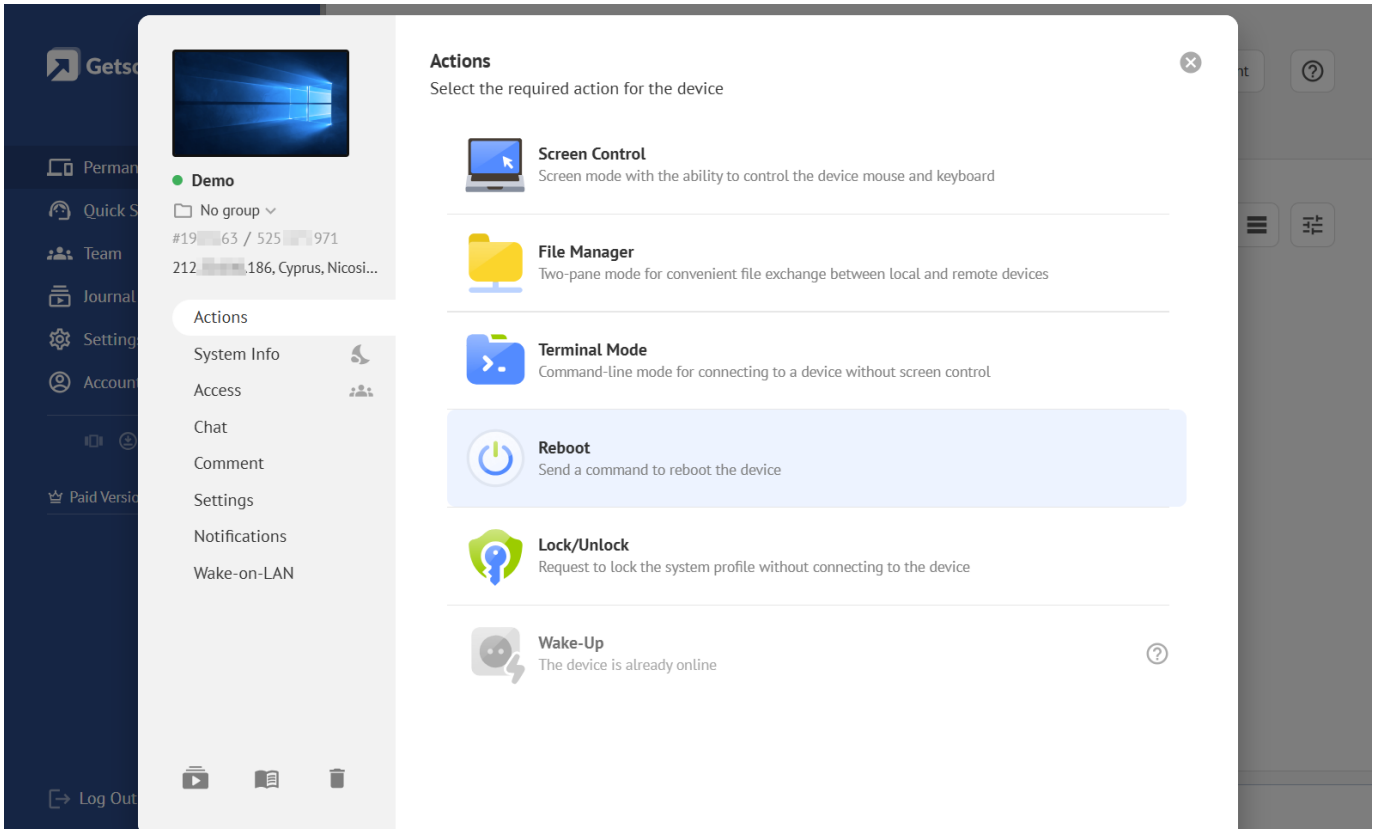
Connection Window — the graphical interface of the window or browser tab in which a connection to a remote device is established.

4.2 Connection Participant

Connection Participant — a participant in a connection acting as a technician. Multiple technicians can join the same connection simultaneously for collaborative work. Learn More

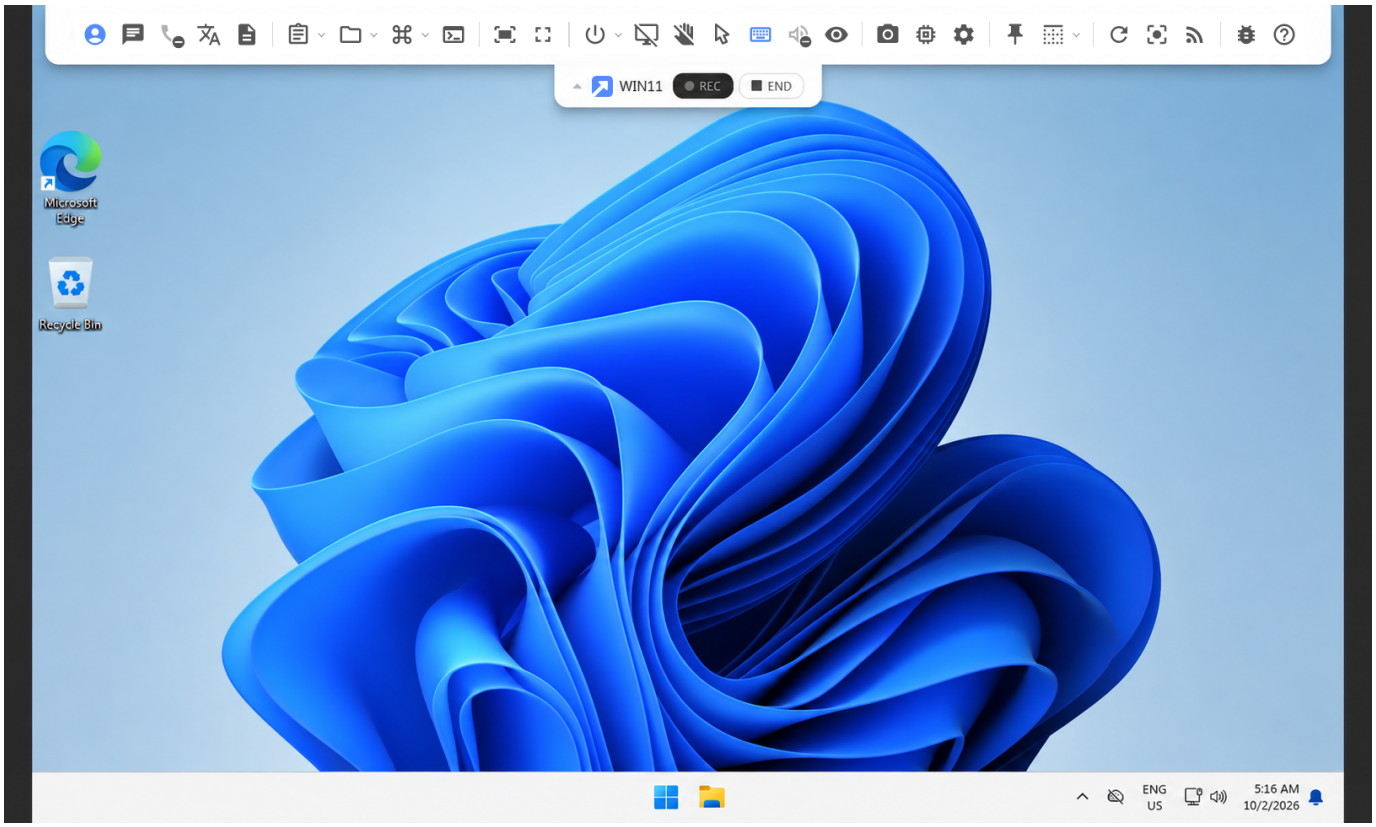
4.3 Connection Mode

Connection Mode — a mode for interacting with and managing a remote device. Mode selection is available for devices from Permanent Access or Quick Support invitations.



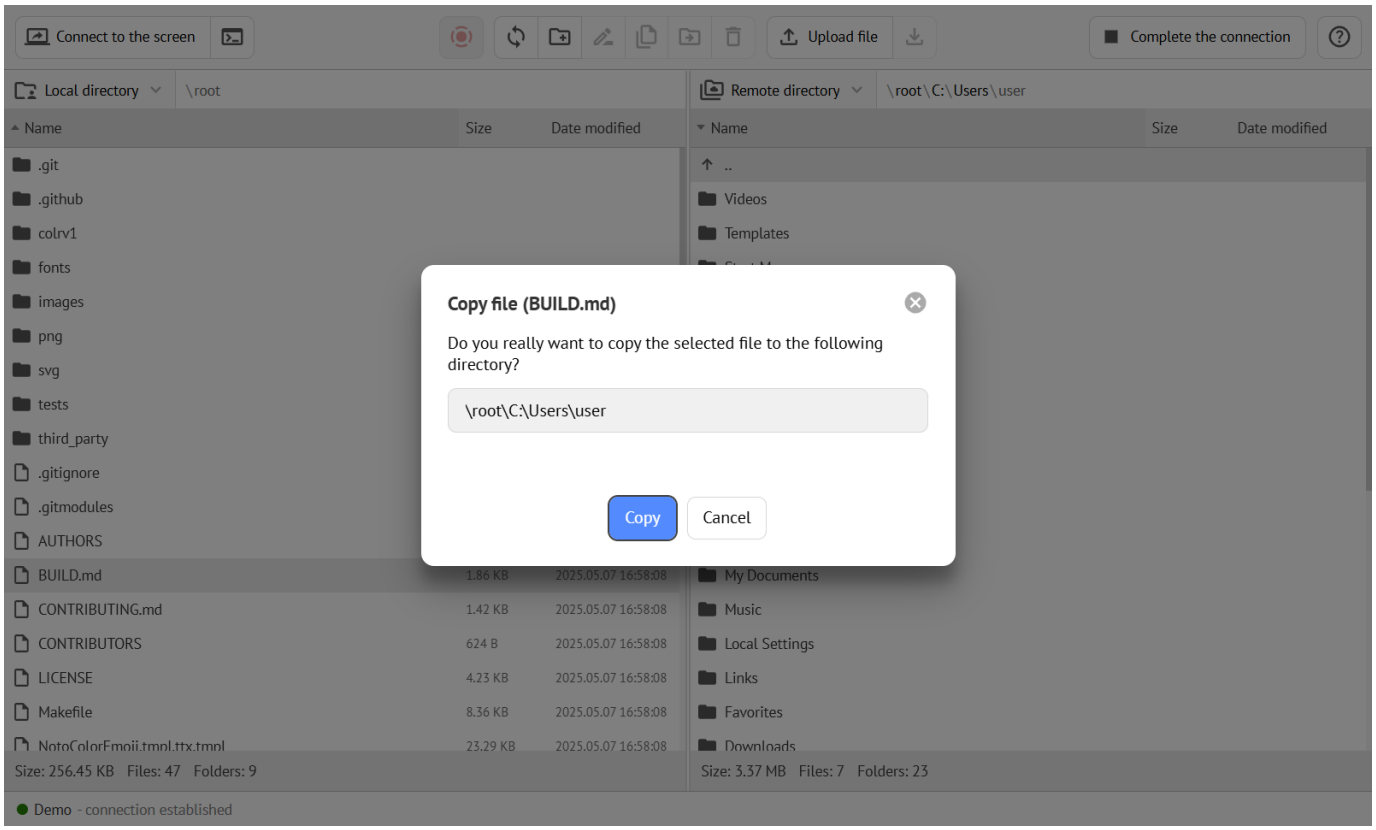
4.4 Screen Control

Screen Control — a mode for controlling the screen of a remote device using a mouse and keyboard. Learn More



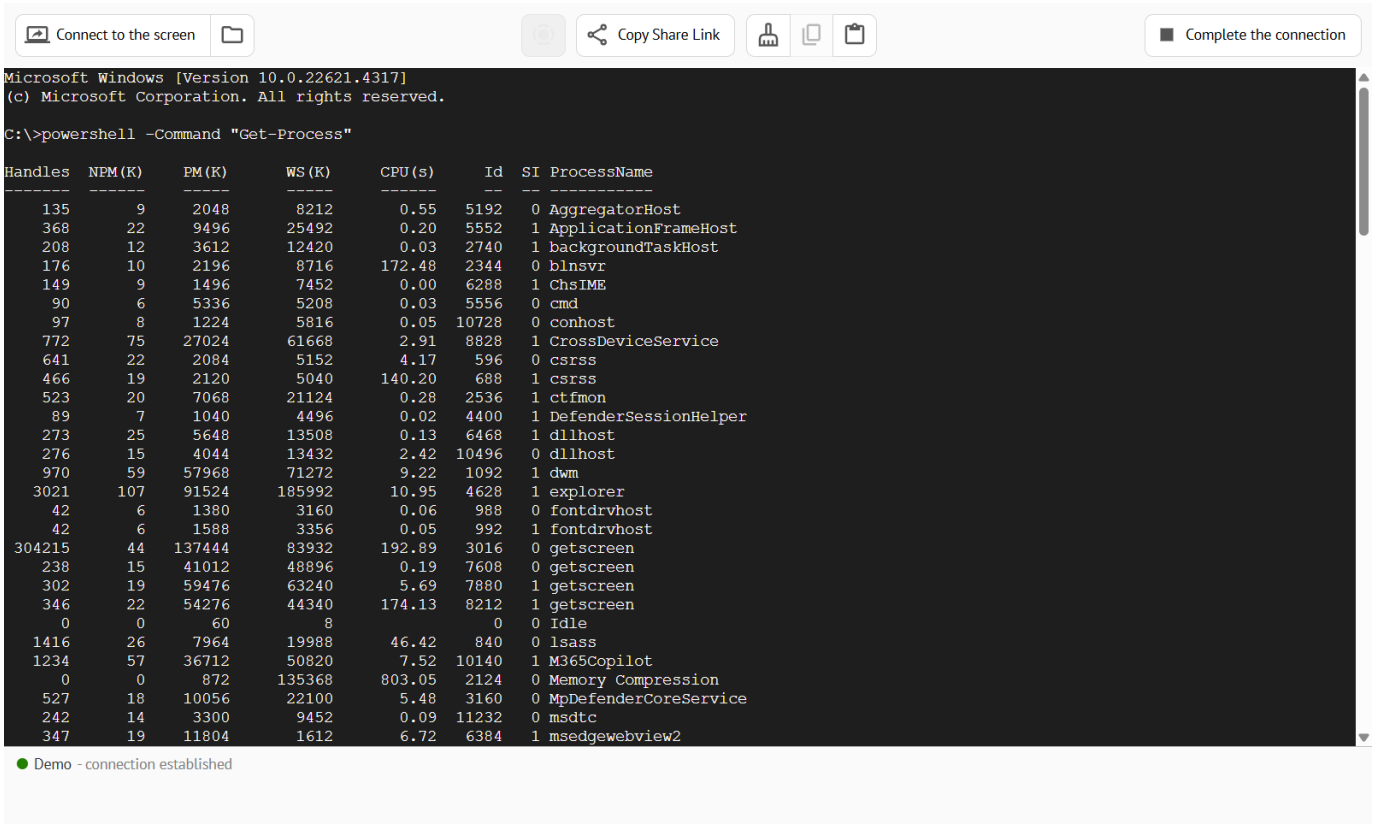
4.5 File Manager

File Manager — a mode for managing the file system of a remote device, including uploading, downloading, and managing files and folders. The mode uses a two-pane graphical interface for transferring files between the technician's device and the remote device. Learn More



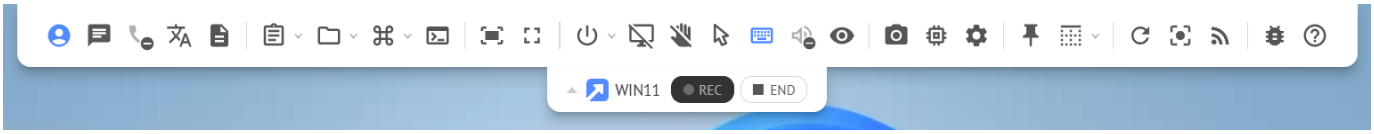
4.6 Terminal Mode

Terminal Mode — a mode for managing a remote device using the command line.



4.7 Control Panel

Control Panel — a panel inside the connection window that provides various control functions and commands for the technician.



4.8 Video Channel

Video Channel — a channel for transmitting media data between the connection window on the technician's side and the Agent App on the remote device. Learn More

4.9 WebRTC Channel

WebRTC Channel — the primary data transmission channel that uses WebRTC technology to establish a direct P2P connection. Learn More

4.10 WebSocket Channel

WebSocket Channel — a fallback data transmission channel that uses WebSocket technology to establish a connection through a proxy server. Learn More

4.11 Connection History

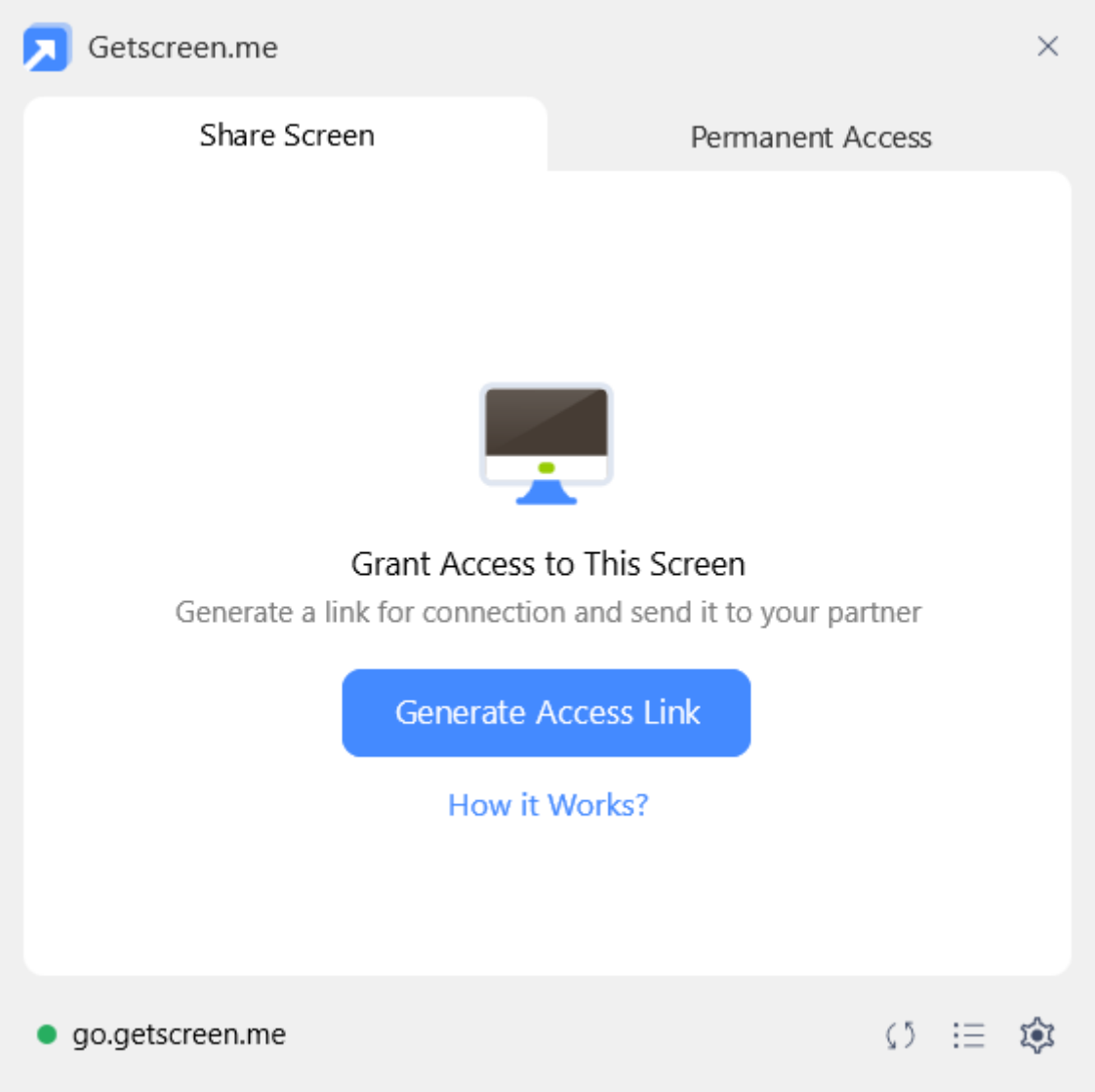
Connection History — a history of all connections made by all technicians in the team.

4.12 Video Record

Video Record — a video recording of a specific connection. Video recording is available for different connection modes. Learn More

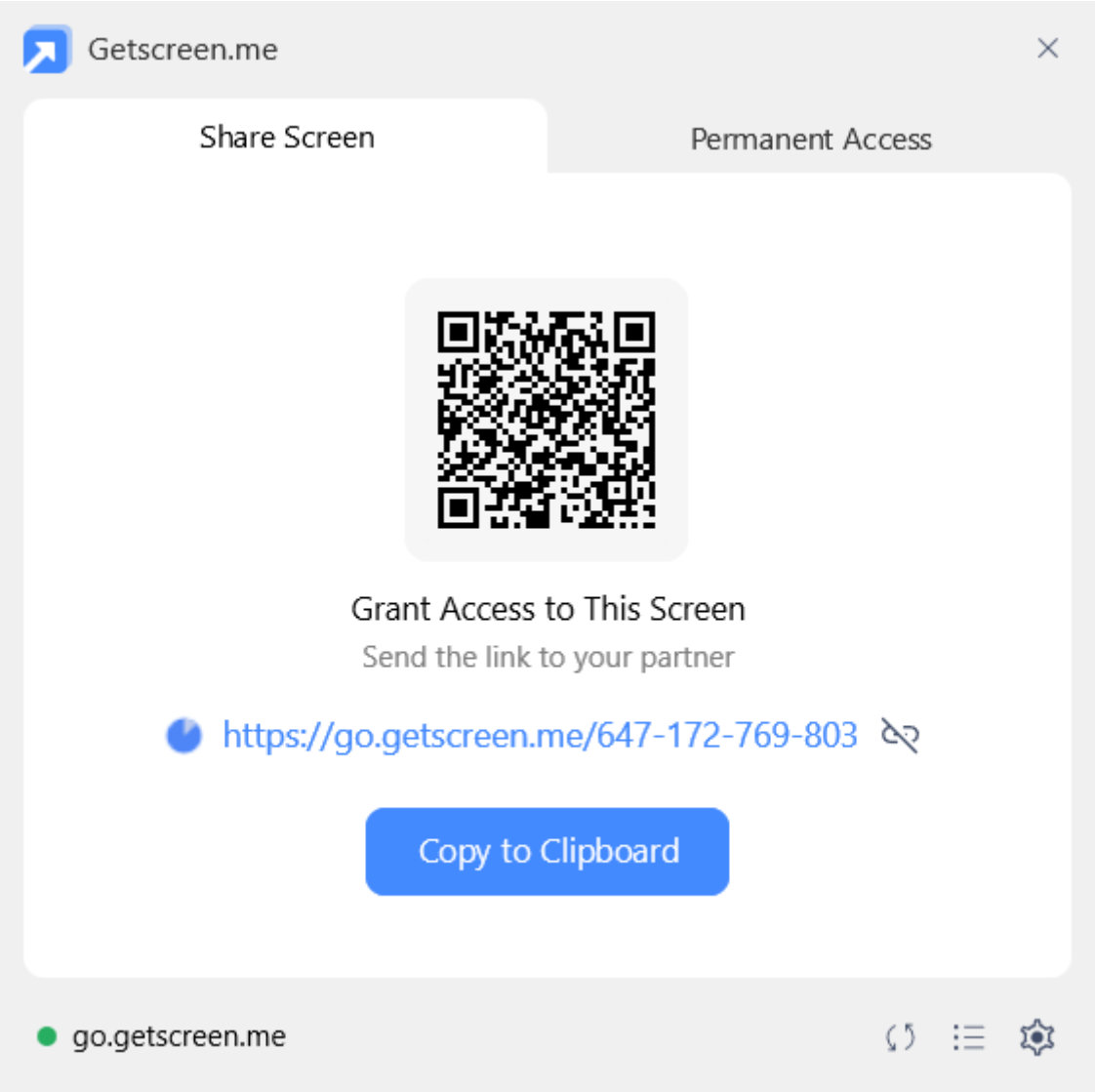
5. Share Screen

This is an optional Agent App feature intended for one-time screen sharing, with or without remote control. The workflow is very simple: the running Agent App generates a URL for connecting to the device. When the link is opened on another device, the connection is established automatically. No application installation is required.



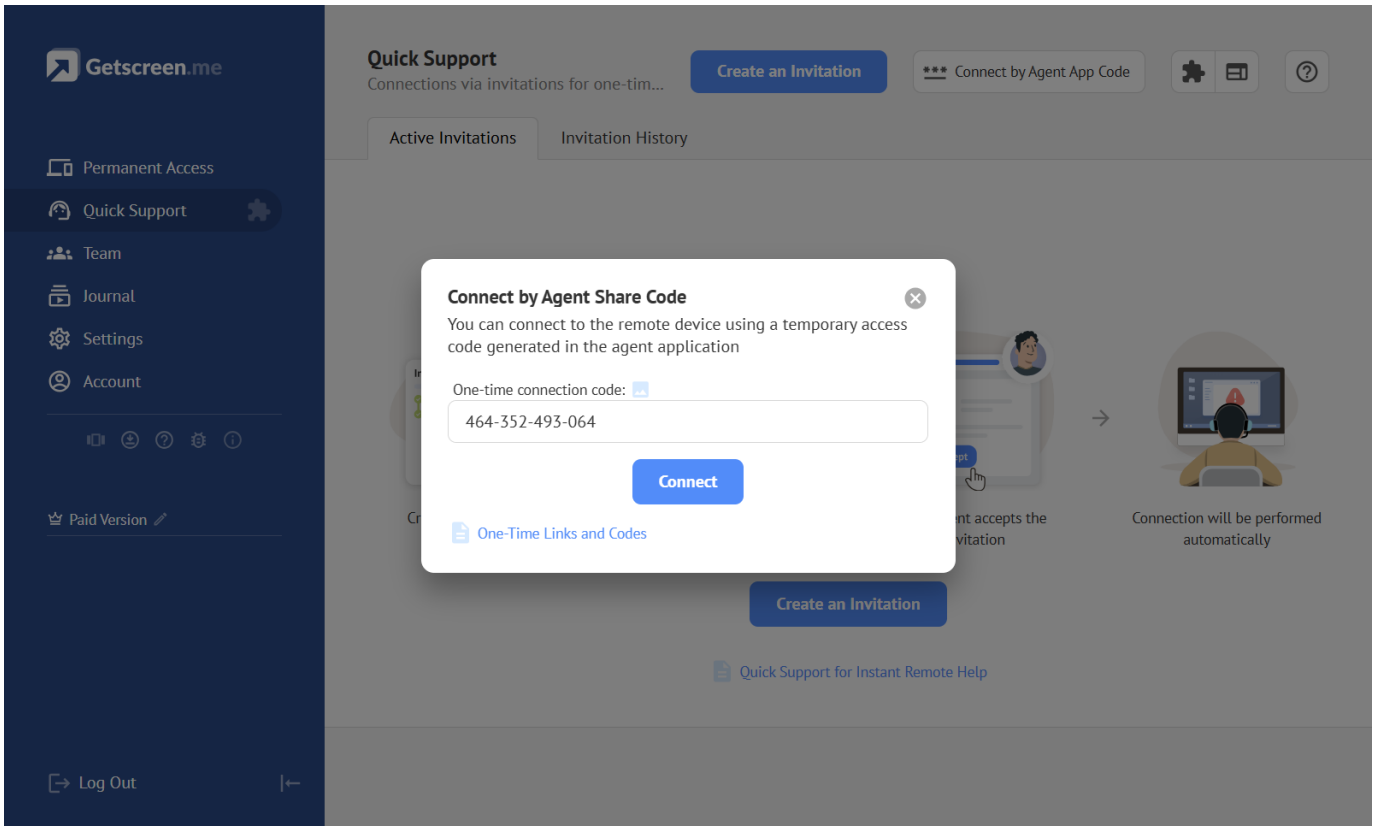
5.1 Share Link

Share Link — a one-time URL used to connect to a device. The link is generated automatically when the Agent App starts or manually using the generation button. The generated link is valid for a limited number of minutes, and its lifetime can be customized in the team settings.



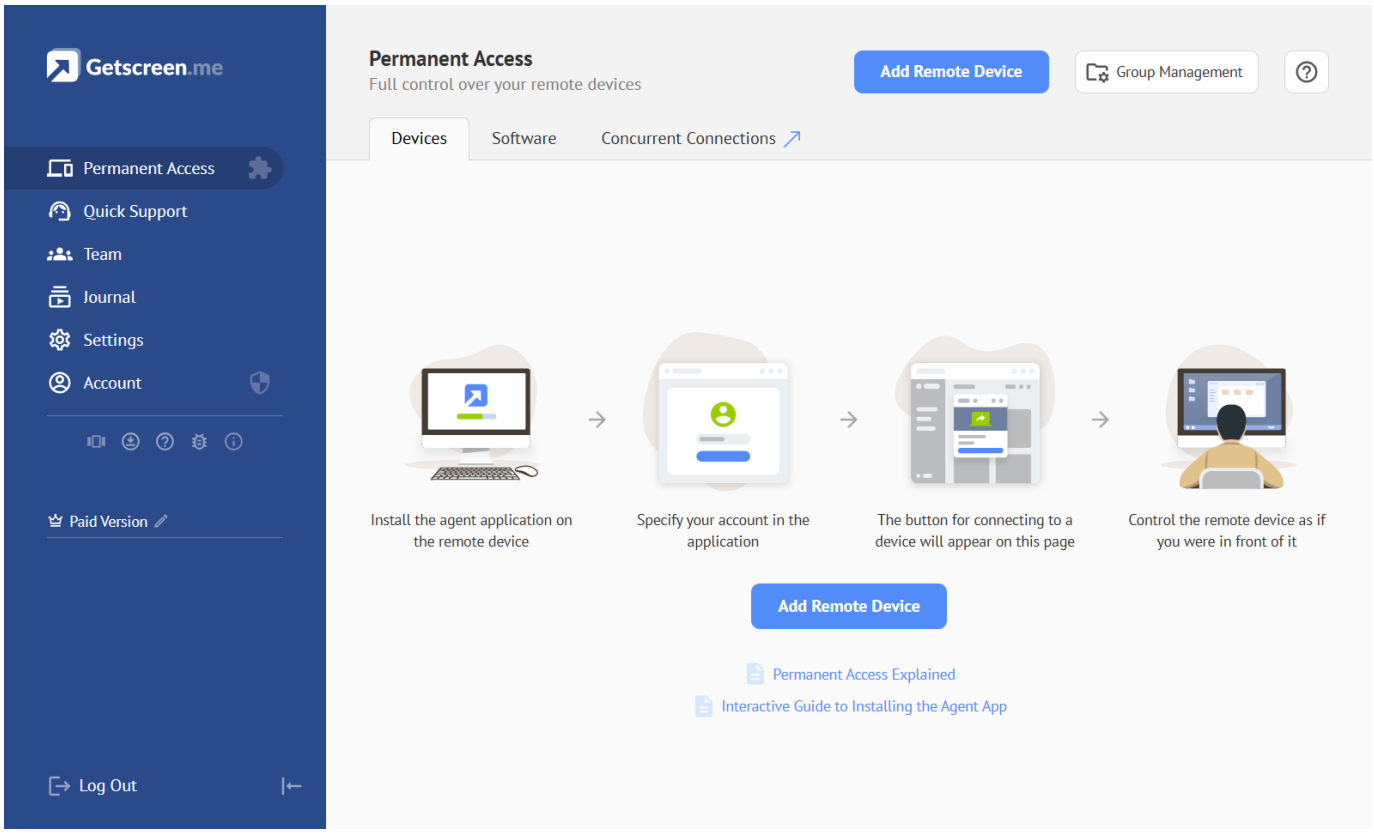
5.2 Share Code

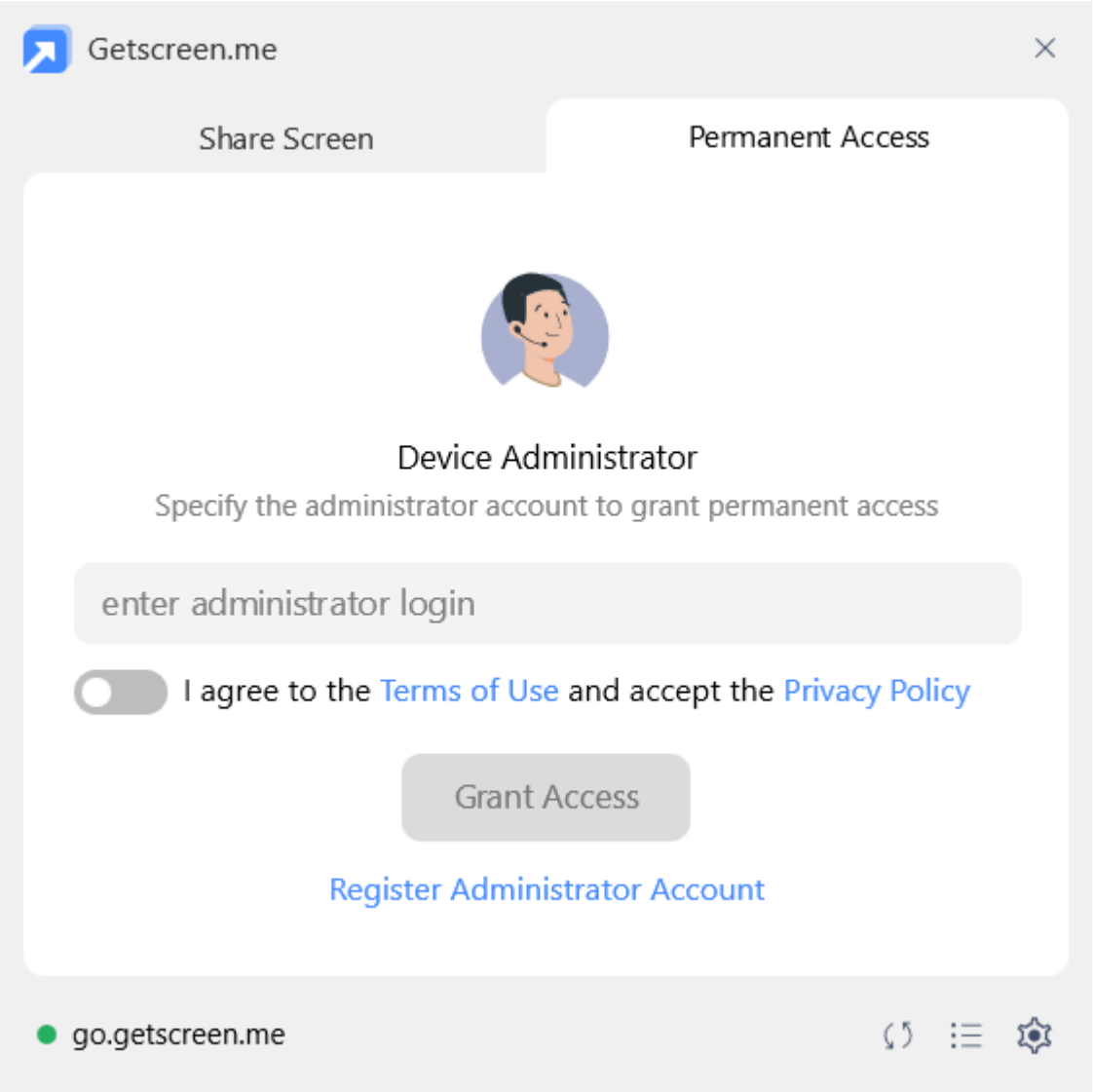
Share Code — the numeric part of the Share Link that identifies it. This code can be used when you want to share your screen with a technician registered in the system. The technician can use it as an invitation code in the Quick Support section.


Getscreen.me
Permanent Access
Quick Support
Team
Journal
Settings
Account
Paid Version
Log Out
Quick Support
Connections via invitations for one-tim...
Create an Invitation
Connect by Agent App Code
Active Invitations
Invitation History
Connect by Agent Share Code
You can connect to the remote device using a temporary access code generated in the agent application
One-time connection code:
464-352-493-064
Connect
One-Time Links and Codes
Connection will be performed automatically
Create an Invitation
Quick Support for Instant Remote Help

6. Permanent Access

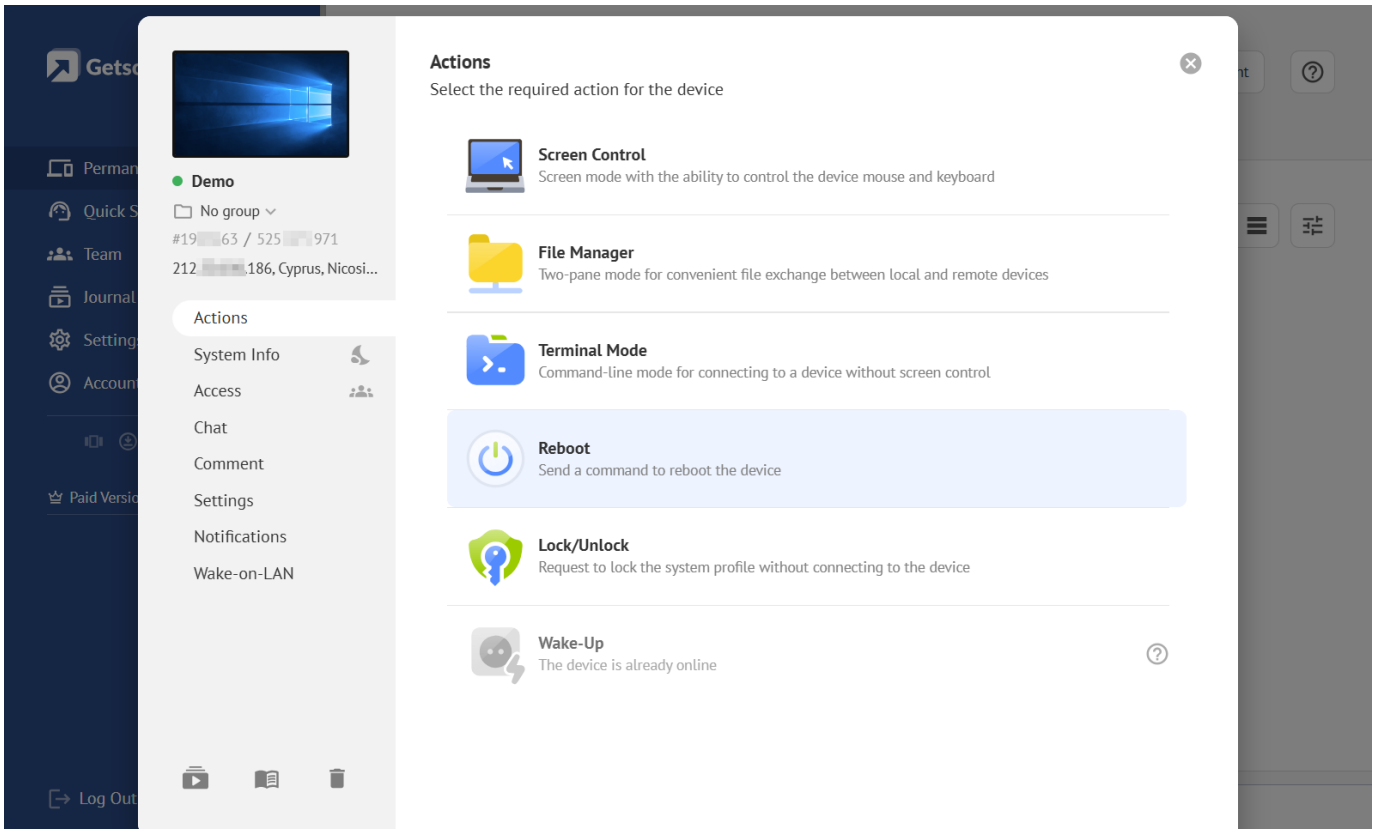
This is an account section and the corresponding device management mechanism for devices linked to a technician account and intended for permanent unattended access and connection at any time. Devices are linked using the technician's email address. Connections are started from the dashboard. It is intended for long-term administration of personal or corporate devices. Learn More


Getscreen.me
Permanent Access
Quick Support
Team
Journal
Settings
Account
Paid Version
Log Out
Permanent Access
Full control over your remote devices
Add Remote Device
Group Management
Devices
Software
Concurrent Connections
Install the agent application on the remote device
Specify your account in the application
The button for connecting to a device will appear on this page
Control the remote device as if you were in front of it
Add Remote Device
Permanent Access Explained
Interactive Guide to Installing the Agent App



6.1 Device Card

Device Card — the interface card for a device configured for permanent unattended access. It contains general device information, management functions, settings, and connection options.

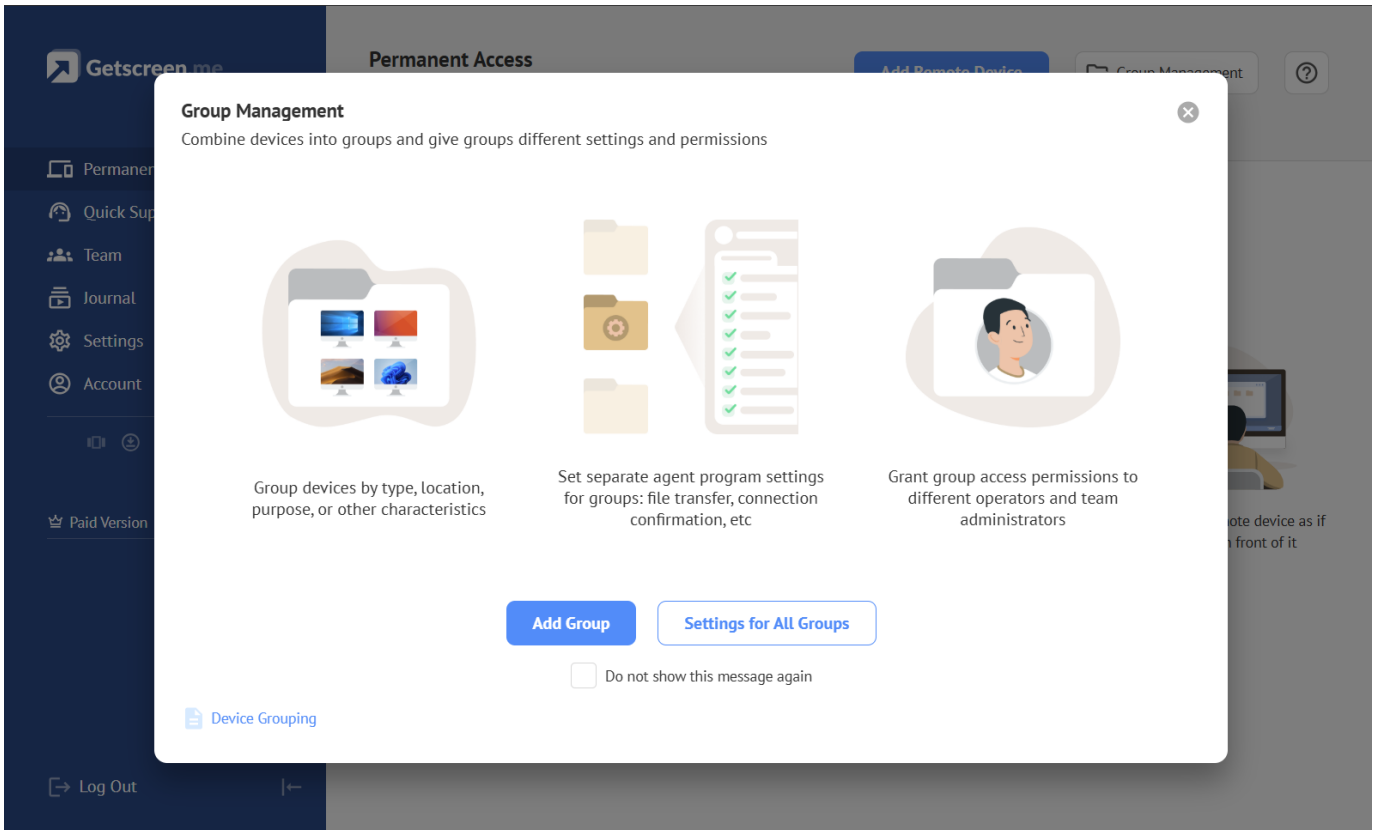


6.2 Group

Group — an internal system entity used to group devices from Permanent Access for managing access permissions and Agent App settings. Learn More

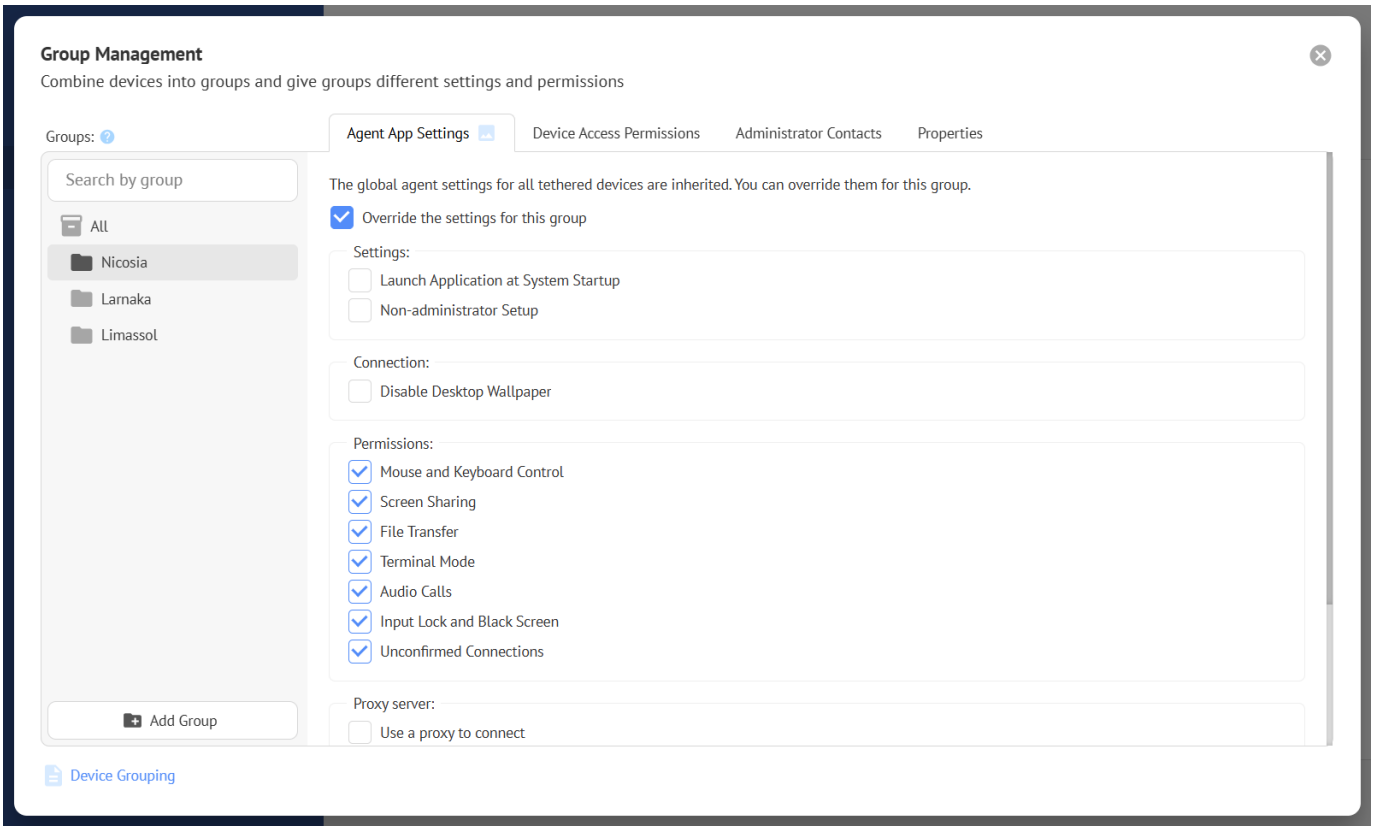
6.3 Group Manager

Group Manager — a tool for creating, deleting, and editing device groups.



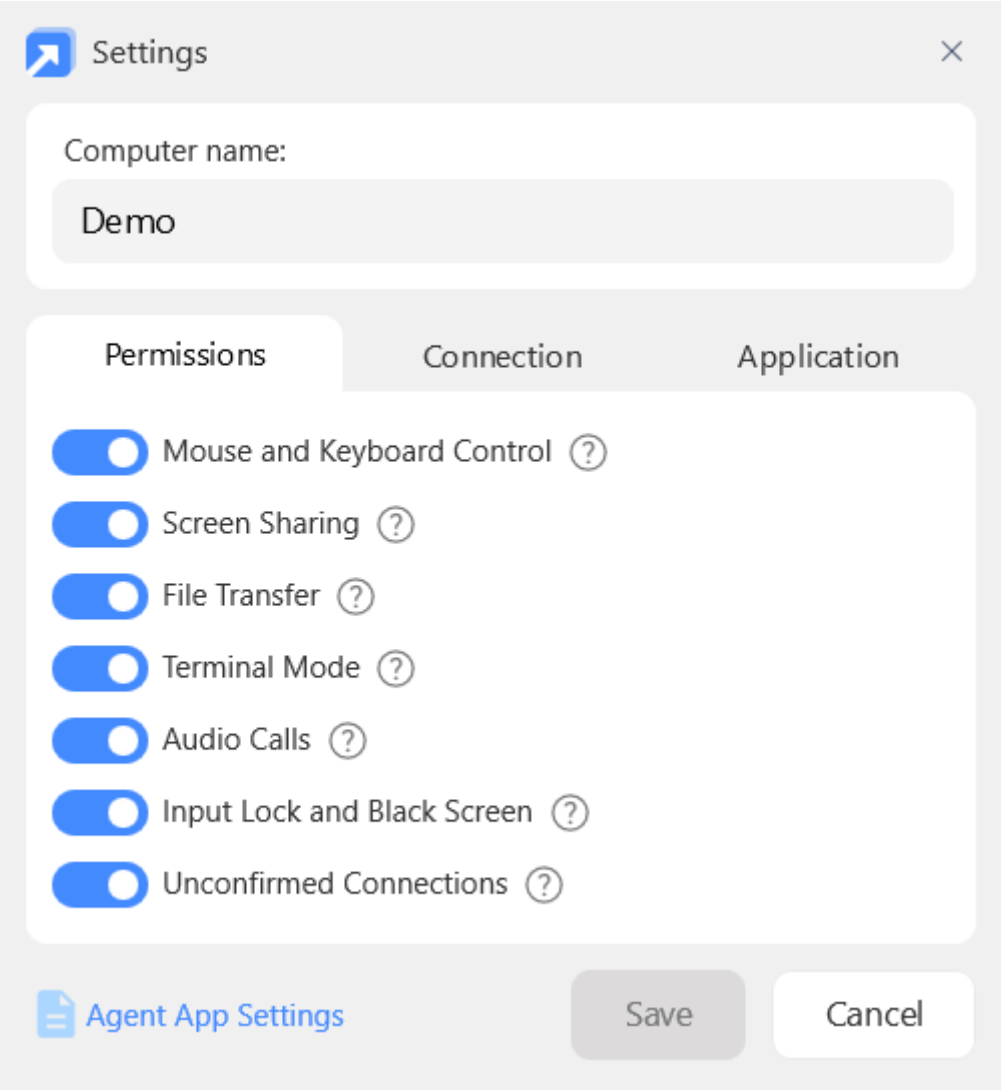
6.4 Group Policy

Group Policy — a set of group policies used to apply the same Agent App settings to a group of devices configured for permanent unattended access. Settings applied through Group Policies take priority over settings configured through the app interface and cannot be changed from the Agent App interface.



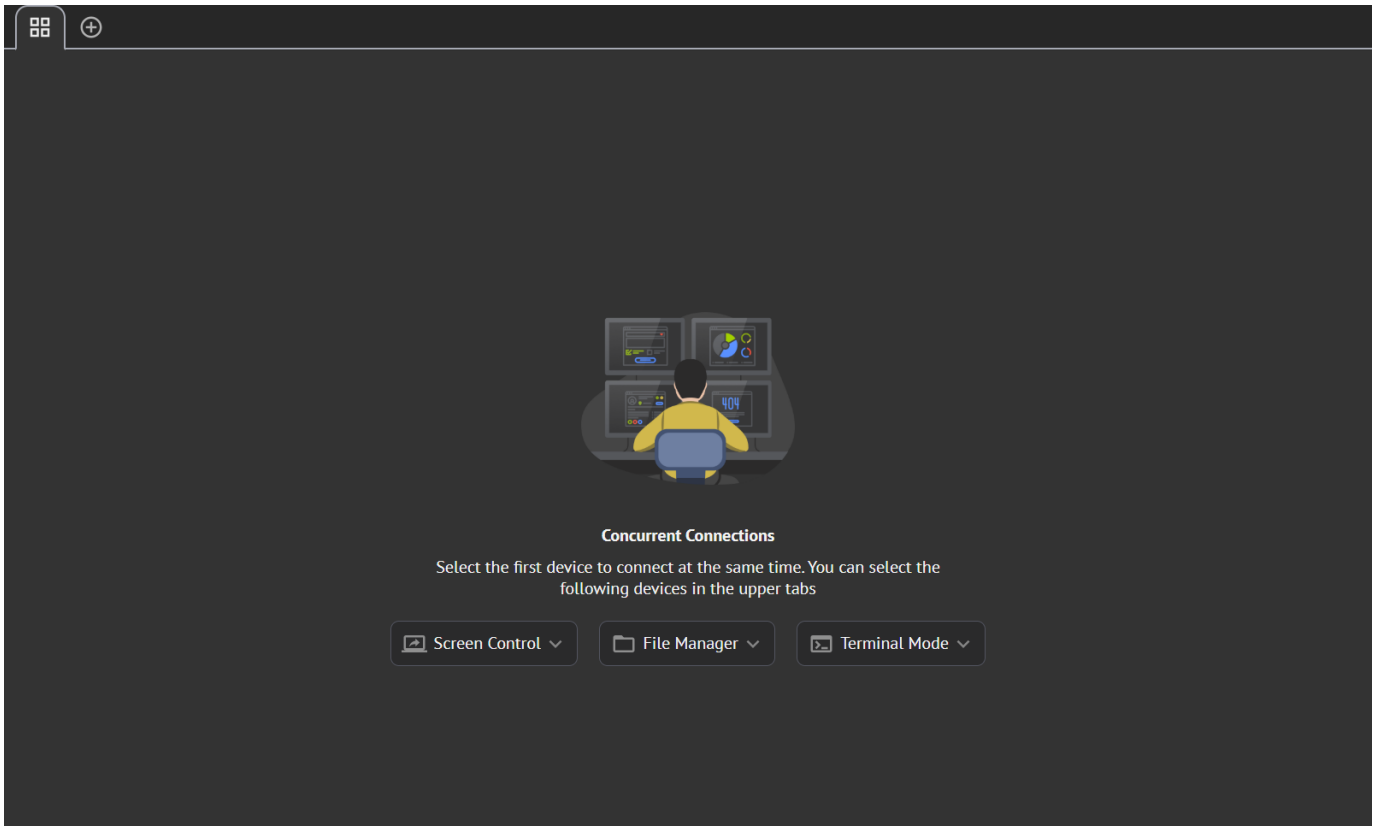
6.5 Agent App Settings

Agent App Settings — a set of Agent App settings that control which device access functions are allowed, such as the available connection modes. Settings can be configured individually on each device through the app interface. They can also be applied through Group Policies. Learn More



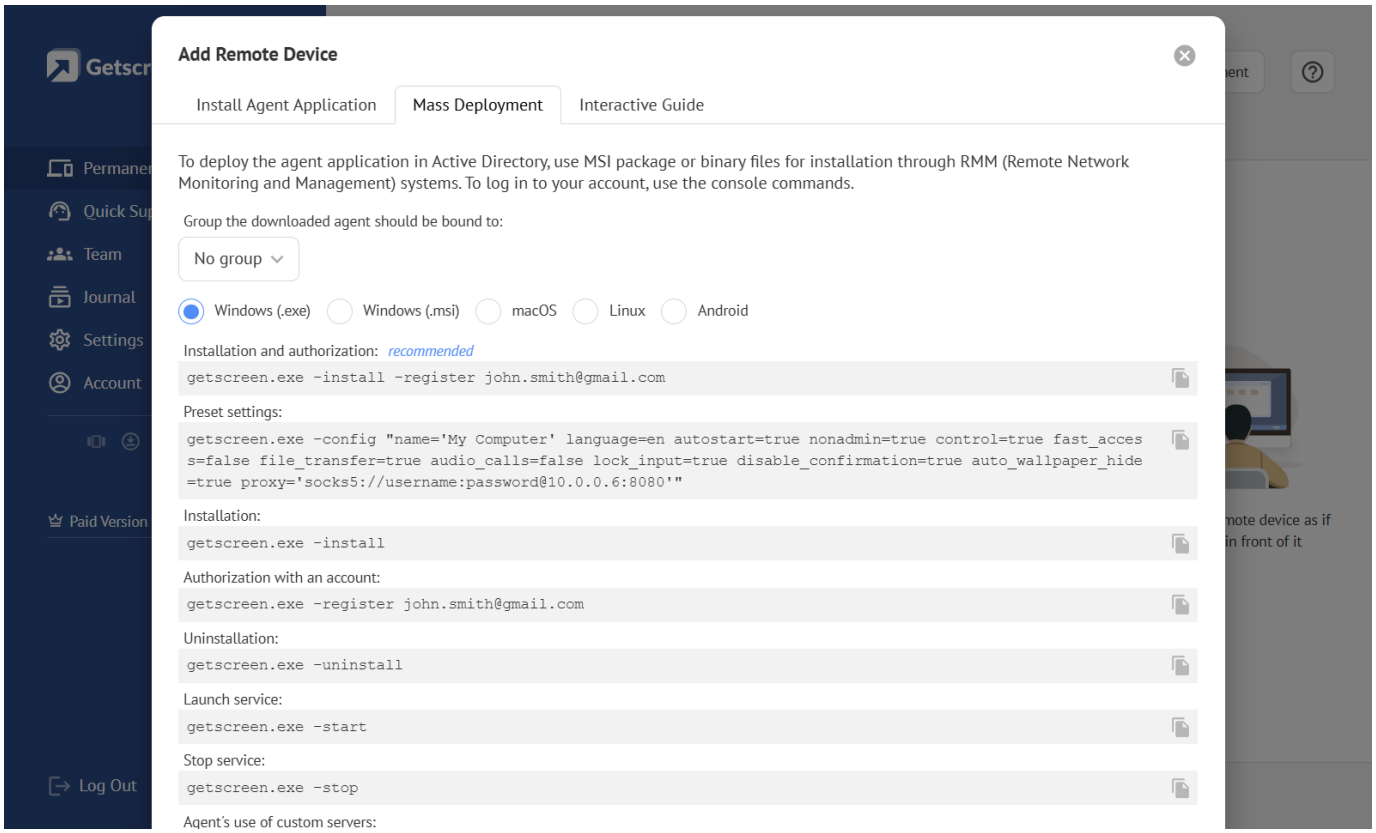
6.6 Concurrent Connection

Concurrent Connection — the ability for one technician to connect to multiple devices at the same time. It is available only for devices configured for Permanent Access. Learn More



6.7 Mass Deployment

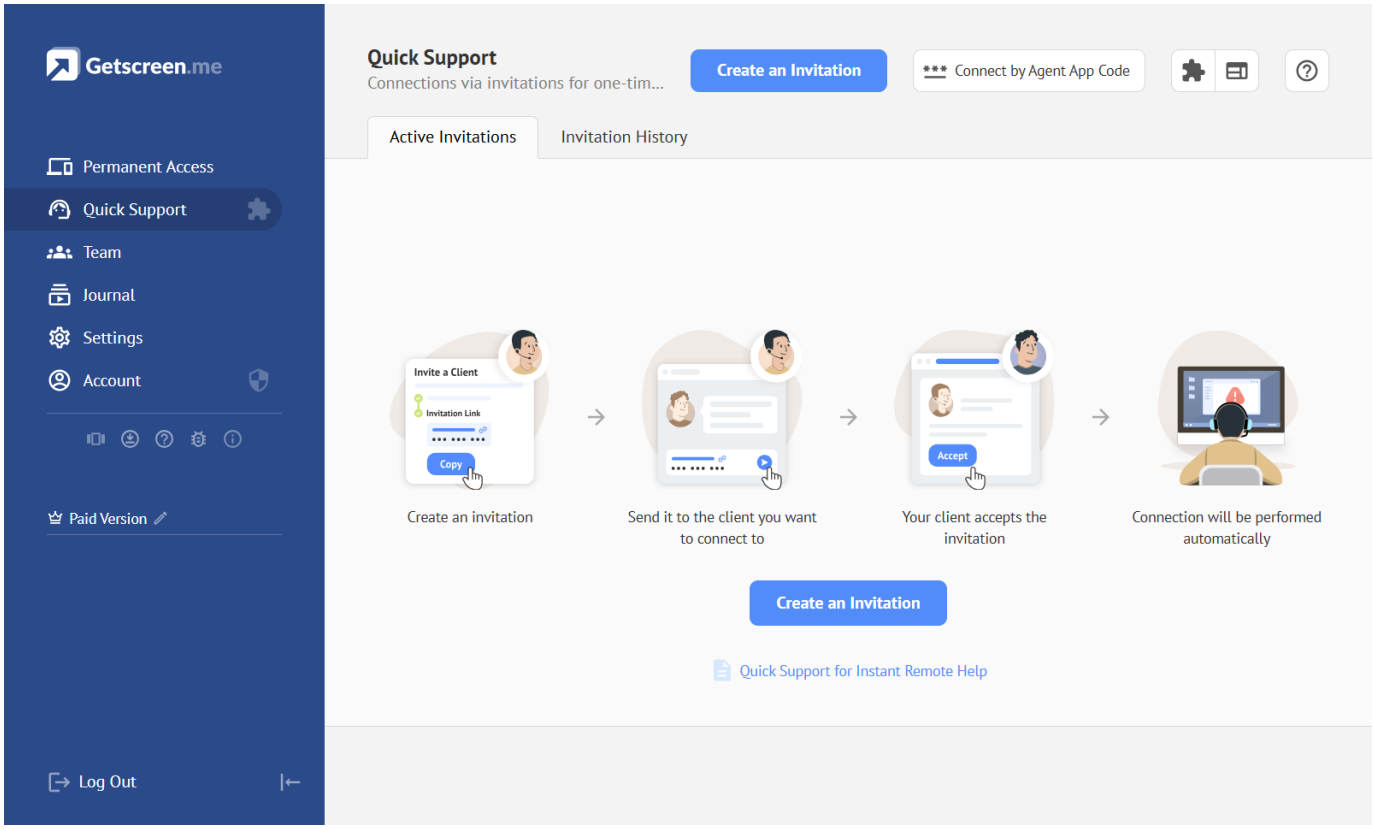
Mass Deployment — the process of deploying the Agent App to multiple devices across a corporate local network. It uses command-line options available in the Agent App together with specialized software deployment systems. Learn More


Add Remote Device
Install Agent Application
Mass Deployment
Interactive Guide
To deploy the agent application in Active Directory, use MSI package or binary files for installation through RMM (Remote Network Monitoring and Management) systems. To log in to your account, use the console commands.
Group the downloaded agent should be bound to:
No group
Windows (.exe)
Windows (.msi)
macOS
Linux
Android
Installation and authorization: recommended
getscreen.exe -install -register john.smith@gmail.com
Preset settings:
getscreen.exe -config "name='My Computer' language=en autostart=true nonadmin=true control=true fast_access=false file_transfer=true audio_calls=false lock_input=true disable_confirmation=true auto_wallpaper_hide=true proxy='socks5://username:password@10.0.0.6:8080'"
Installation:
getscreen.exe -install
Authorization with an account:
getscreen.exe -register john.smith@gmail.com
Uninstallation:
getscreen.exe -uninstall
Launch service:
getscreen.exe -start
Stop service:
getscreen.exe -stop
Agent's use of custom servers:
Permanent
Quick Support
Team
Journal
Settings
Account
Paid Version
Log Out

7. Quick Support

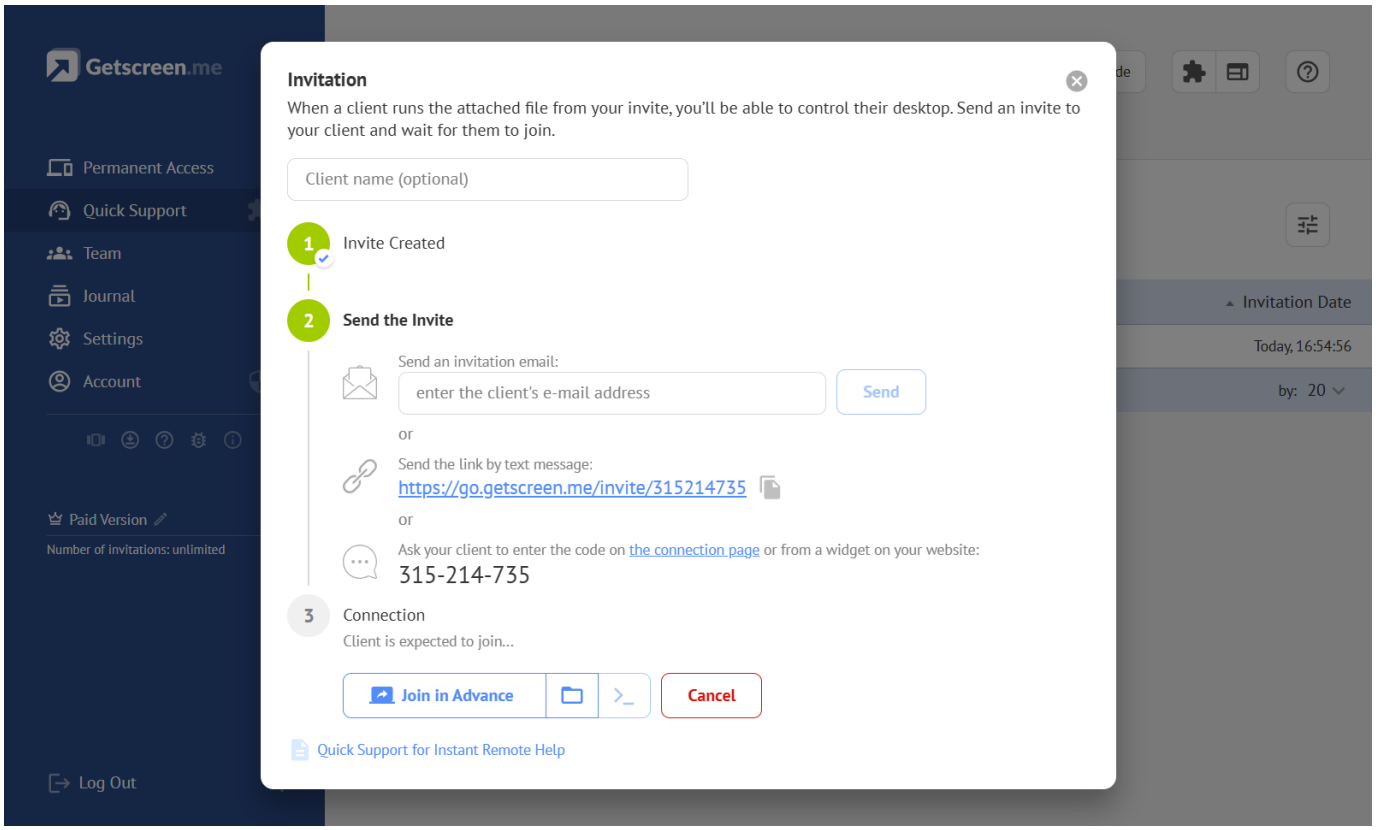
This account section is used for one-time connections to remote devices without setting up permanent unattended access. Connections are created through invitations, each containing a link to a one-time Agent App.

When the user launches the Agent App, the connection starts automatically — no connection codes or other identifiers are required. The Agent App has a simplified interface designed specifically for quick technical support. Learn More



7.1 Invitation

Invitation — an entry in the Quick Support section used to invite a specific client to establish a connection. An invitation can have a waiting-for-client status or an active-connection status.



7.2 Invitation Link

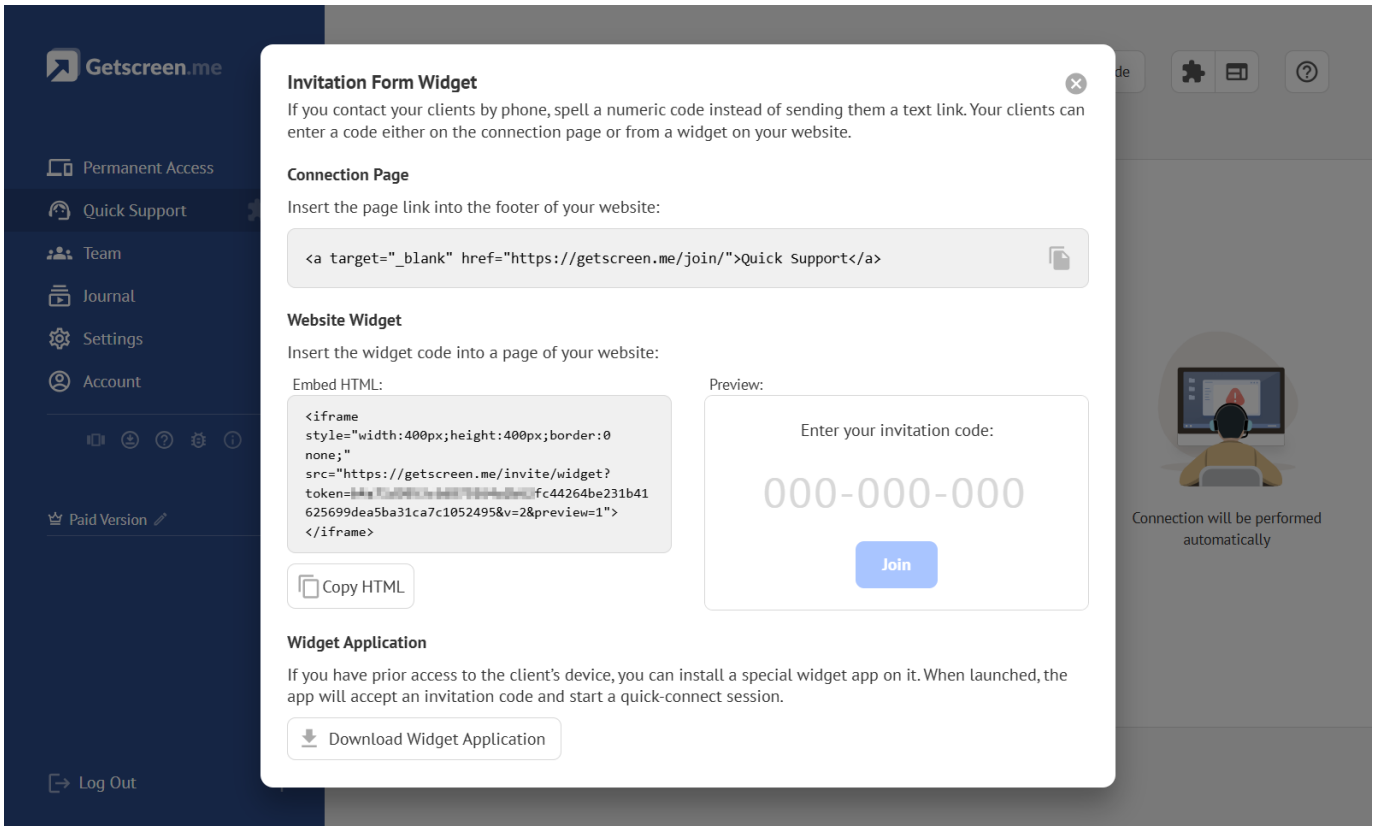
Invitation Link — a unique URL of the invitation page intended for sharing the invitation through text-based communication channels, such as email or messaging apps.

7.3 Invitation Code

Invitation Code — a unique invitation identifier intended for sharing the invitation through voice communication. To open the invitation page, the user can enter the invitation code into a dedicated public form or a preconfigured widget.

7.4 Widget

Widget — a form for entering an invitation code that can be embedded into any public website, such as the website of a company providing technical support.



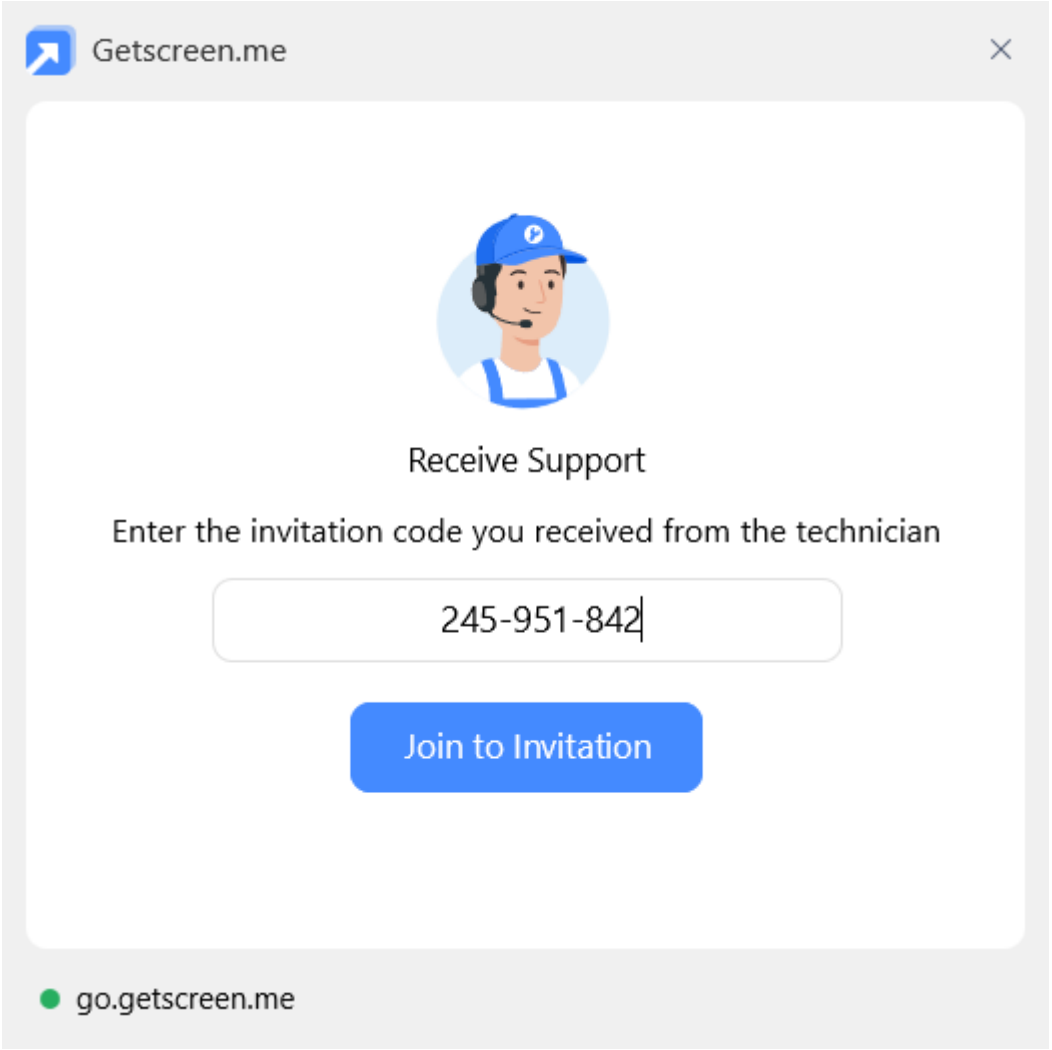
7.5 Widget Embed Code

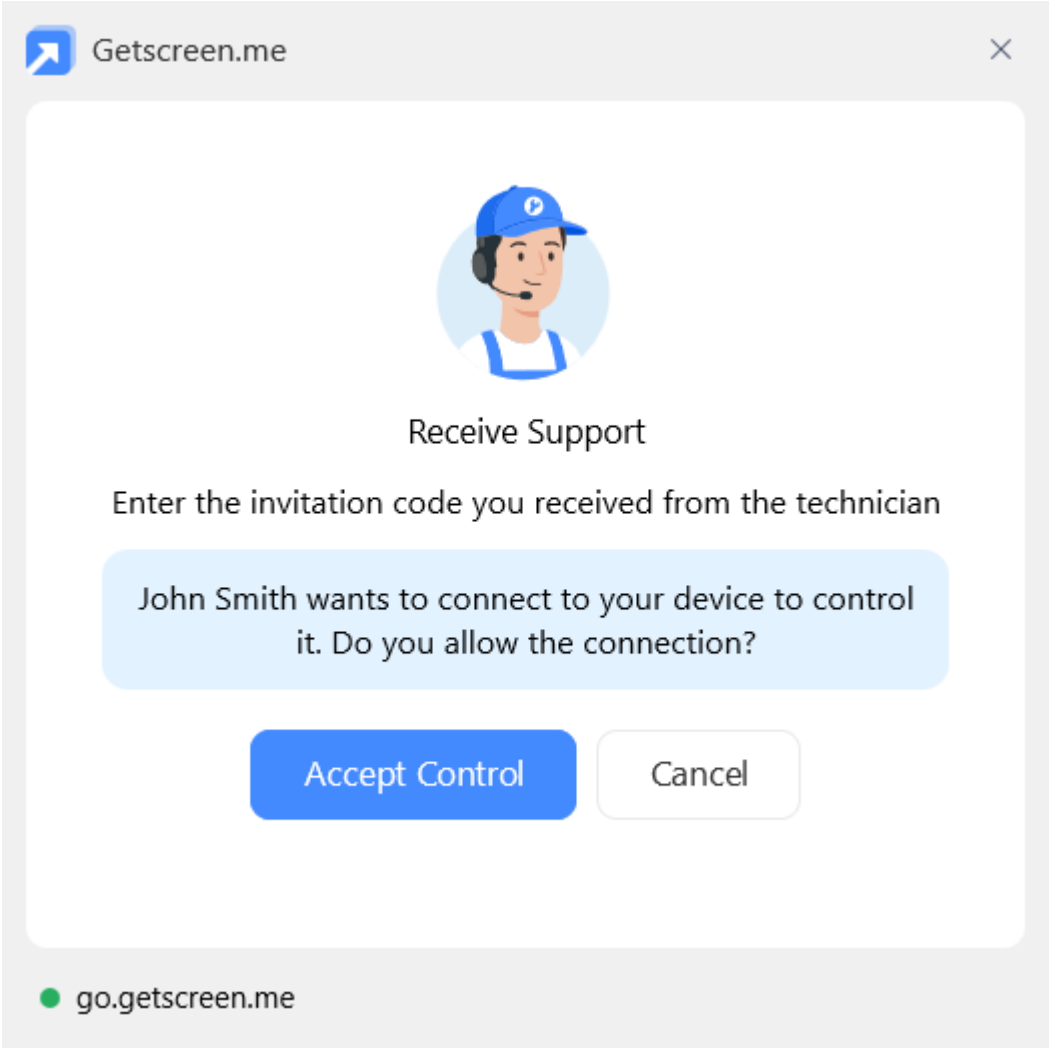
Widget Embed Code — a fragment of HTML code used to embed the widget into a web page.

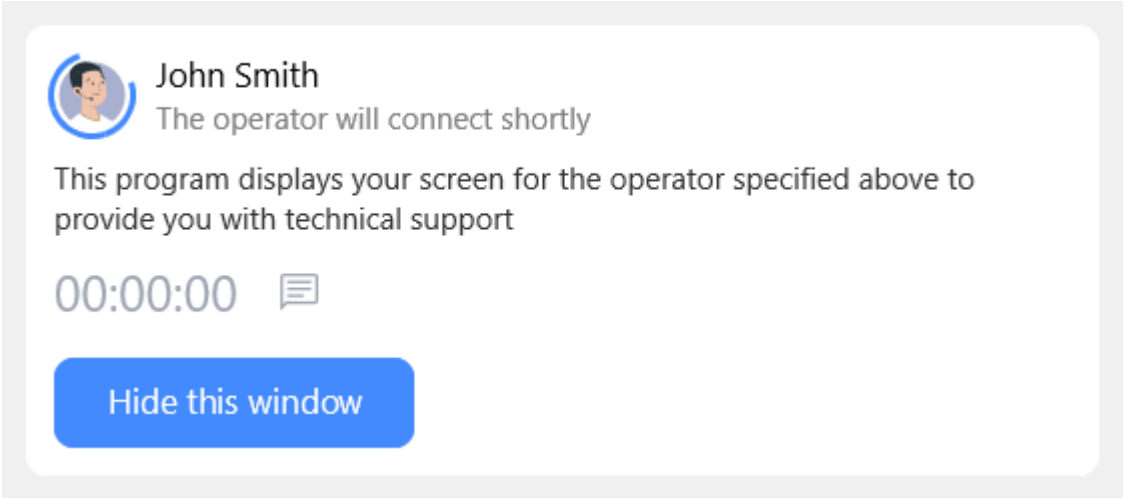
7.6 Widget Application

Widget Application — a special version of the Agent App that lets users enter an invitation code. It is used for Quick Support connections to regular clients or devices without setting up permanent unattended access.

After the invitation code is entered, the application shows the invitation details and an acceptance button. Once accepted, it switches to Agent mode, starts screen sharing, and allows the remote technician to control the device.

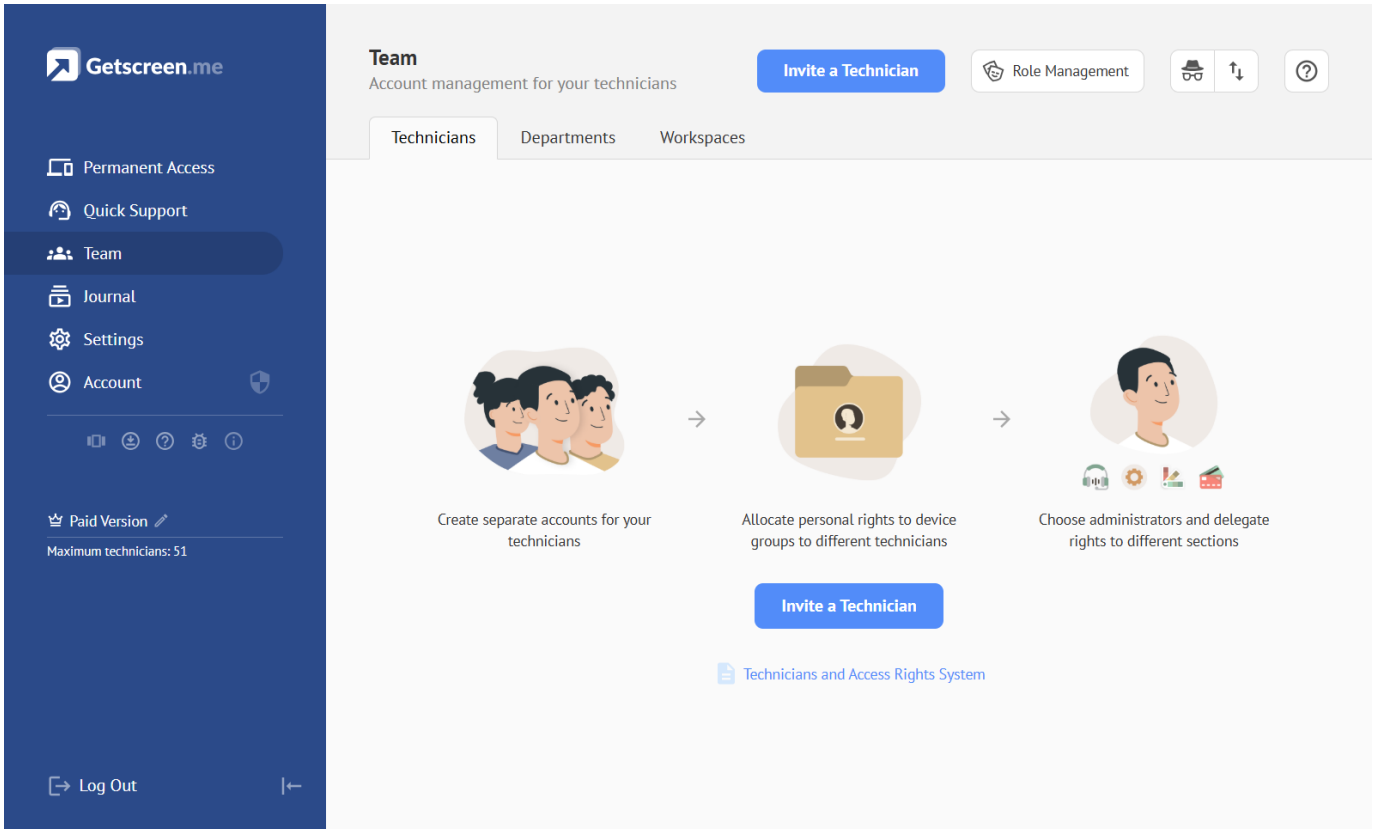

Getscreen.me
Receive Support
Enter the invitation code you received from the technician
245-951-842
Join to Invitation
go.getscreen.me


Getscreen.me
Receive Support
Enter the invitation code you received from the technician
John Smith wants to connect to your device to control it. Do you allow the connection?
Accept Control
Cancel
go.getscreen.me


John Smith
The operator will connect shortly
This program displays your screen for the operator specified above to provide you with technical support
00:00:00
Hide this window

8. Team

This is an account section for managing your own team of subordinate technicians. A team is used for collaboration and workload distribution when working with remote devices. It is intended for company or product technical support departments and for corporate network administration.

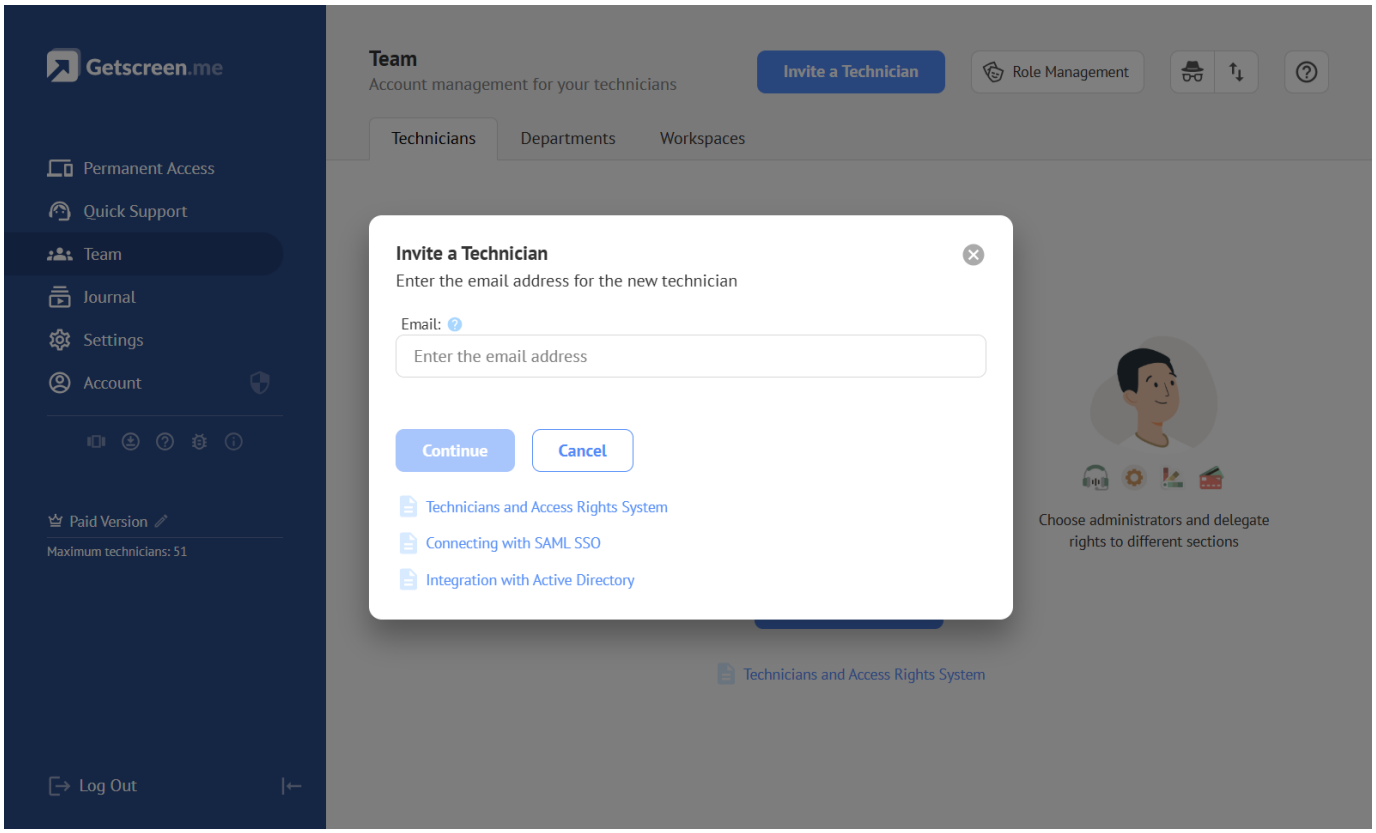


8.1 Team Owner

Team Owner — the account of the team owner. All team settings and devices are associated with this account, including devices added through subordinate technician accounts. The entire team uses the owner's licensing limits and options.

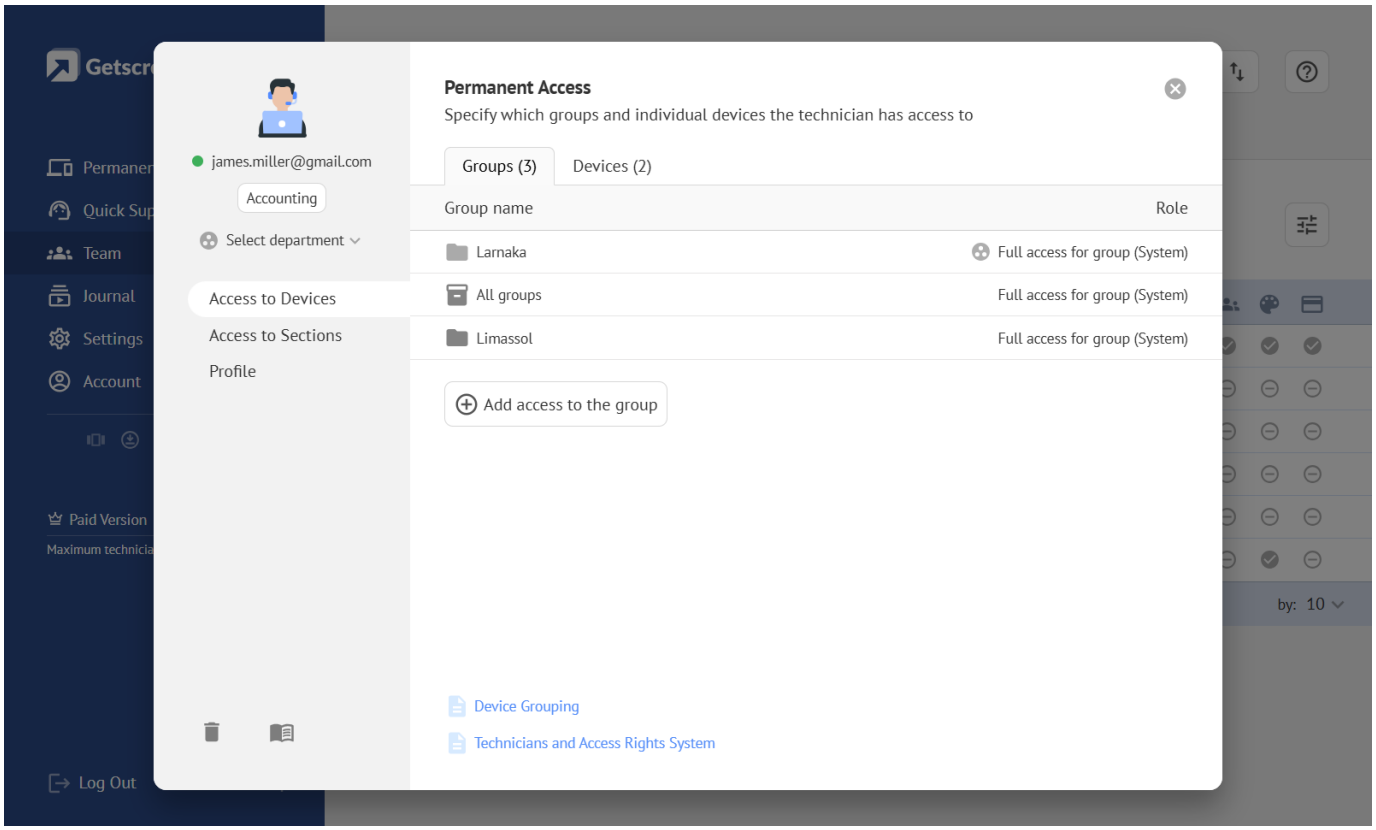
8.2 Technician Invitation

Technician Invitation — an invitation for a technician to join a team. The invitation is created by the team owner or another technician with team administration permissions and sent by email.



8.3 Technician Account

Technician Account — a separate account for a subordinate technician that is associated with a team and has its own login credentials. It is created when a technician accepts an invitation or can be created manually in the Self-Hosted version of the server. Technician accounts are managed by the team owner or a team administrator.



8.4 WorkSpace

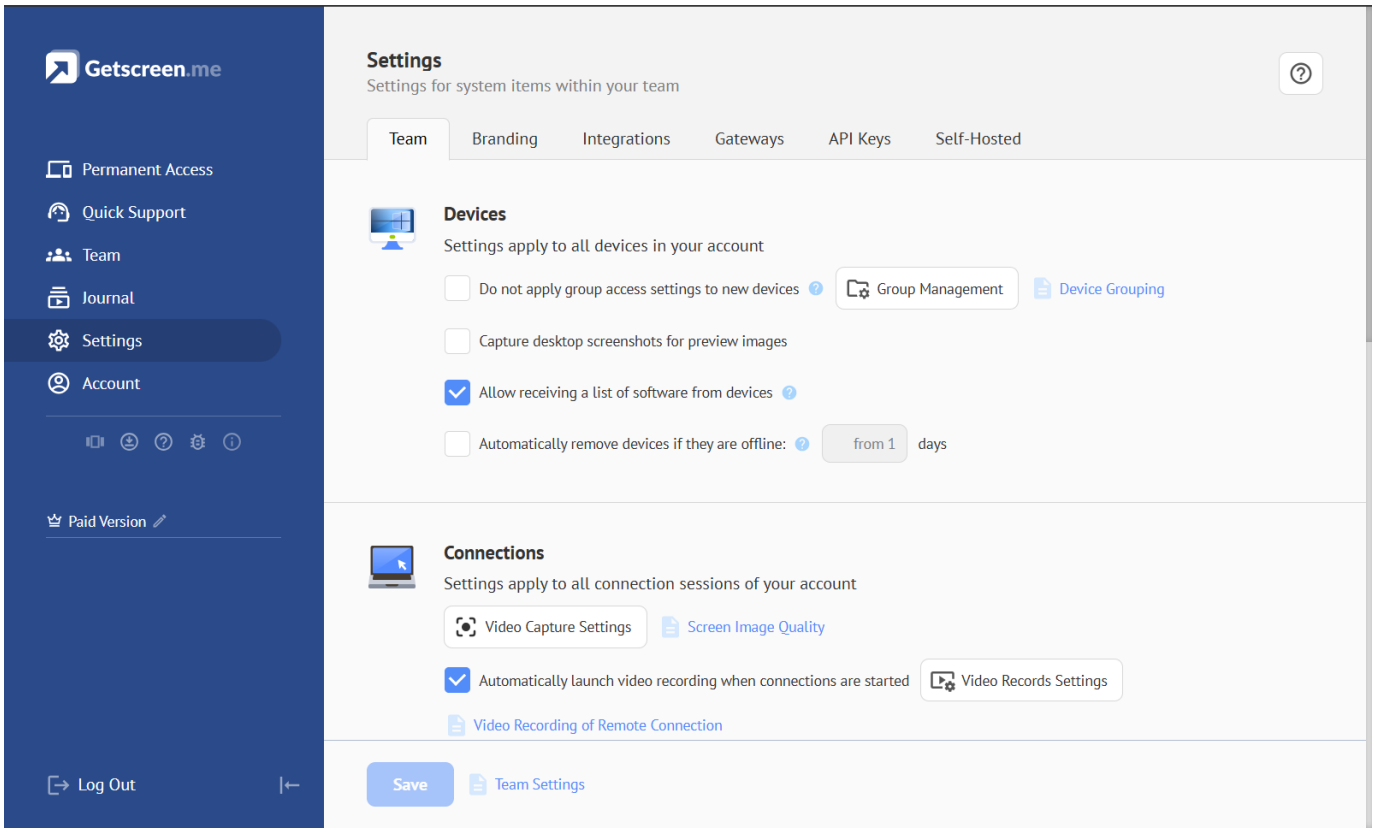
WorkSpace — a special restricted account designed for organizing remote workplaces. Unlike a technician account, a WorkSpace account can only be granted access to specific devices, with a maximum of 5 devices. Access to device groups cannot be granted.

8.5 Department

Department — a unit used to group technician accounts. A department can be created either for technicians or for WorkSpace accounts with the same restrictions. Department accounts can be synchronized with an Identity Provider using the LDAP protocol.

8.6 Team Settings

Team Settings — remote access settings that apply within a team to all system elements, including technicians, devices, and connections. Team settings can be managed by the team owner or by a technician with team administration permissions. Learn More

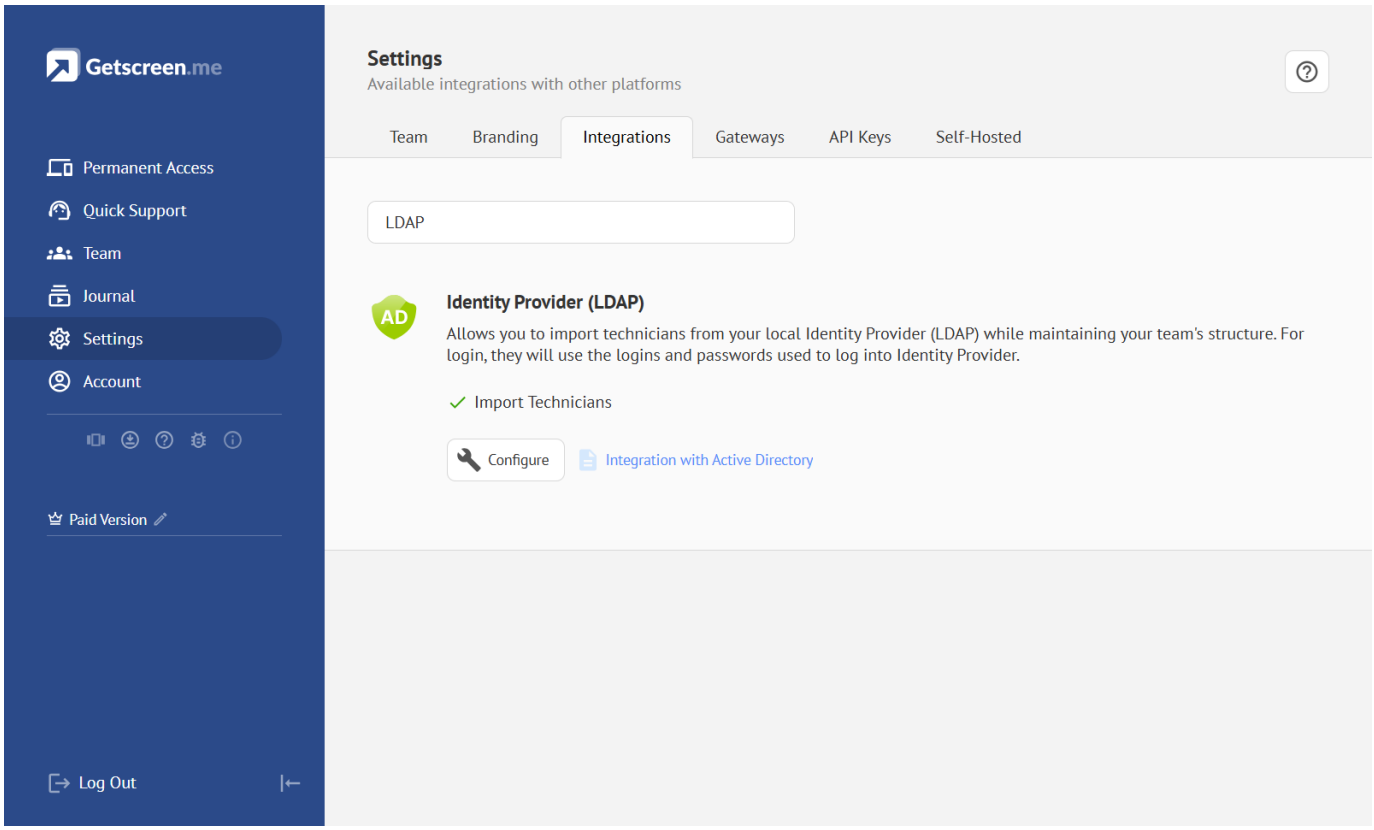


8.7 Identity Provider (IdP)

Identity Provider (IdP) — a system that manages users' digital identities, stores or verifies their credentials, and confirms their identity during authentication. It allows other applications and services to trust the authentication result and grant users access without storing their credentials separately.

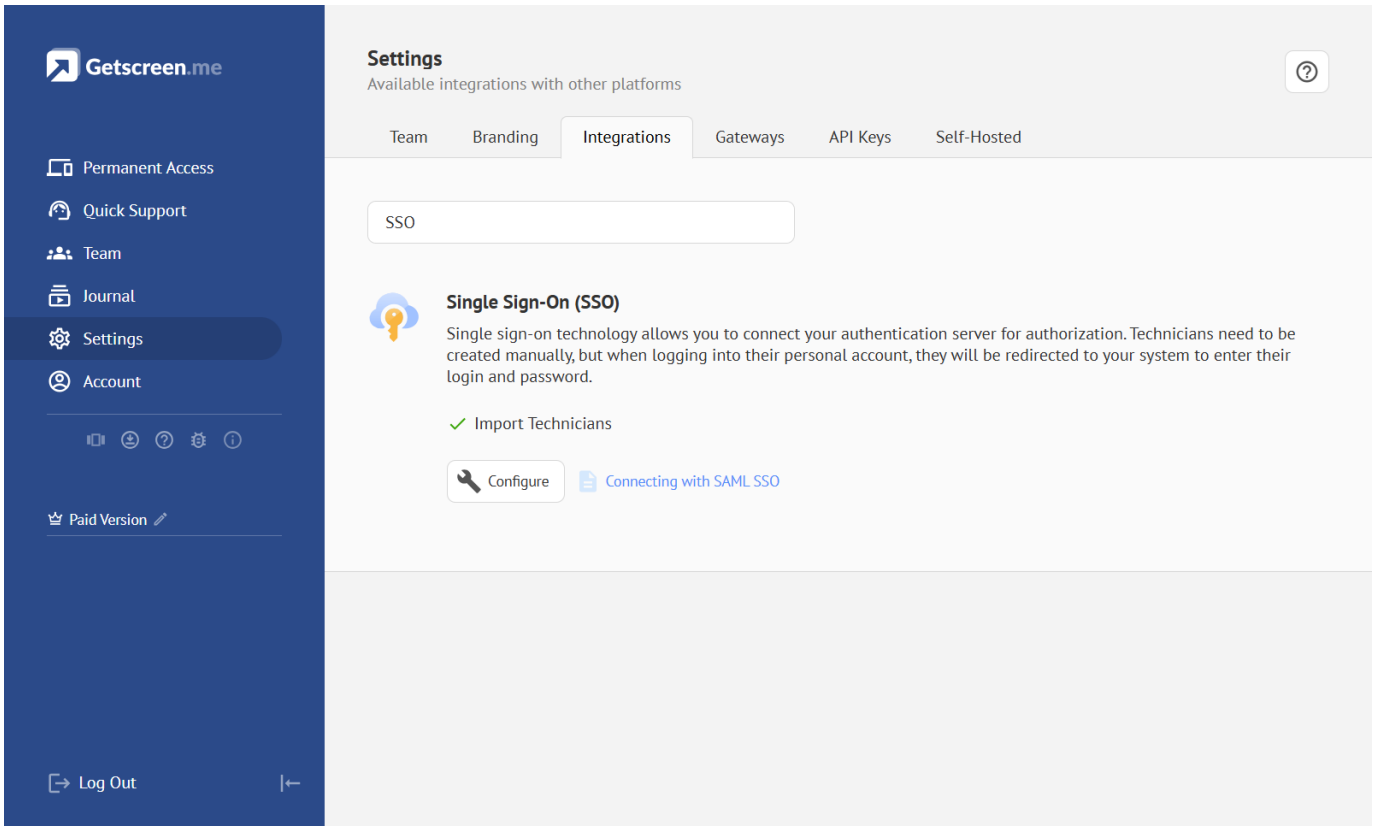
8.8 LDAP

LDAP (Lightweight Directory Access Protocol) — a protocol for accessing centralized directories of users, groups, devices, and other objects. It allows applications to find and retrieve directory data and use it for authentication, authorization, and access management.



8.9 SAML SSO

SAML SSO (Security Assertion Markup Language Single Sign-On) — a single sign-on technology in which users authenticate with a trusted Identity Provider and then access connected applications without entering their credentials again. The SAML standard is used to exchange authentication and user information between systems.


Getscreen.me
Permanent Access
Quick Support
Team
Journal
Settings
Account
Paid Version
Log Out
Settings
Available integrations with other platforms
Team
Branding
Integrations
Gateways
API Keys
Self-Hosted
SSO
Single Sign-On (SSO)
Single sign-on technology allows you to connect your authentication server for authorization. Technicians need to be created manually, but when logging into their personal account, they will be redirected to your system to enter their login and password.
Import Technicians
Configure
Connecting with SAML SSO

9. Access Right System

A system that allows you to assign access rights to individual devices or device groups for specific technicians, departments, or workplaces. It defines not only the subject and object of an access right, but also the list of actions that the subject is allowed to perform on the object.

9.1 Public Link

Public Link — a permanent public link used to connect to a device from the Permanent Access section. The link can be customized if necessary. Having the link itself does not grant access. Access rights are checked when the link is opened using several access control mechanisms.

9.2 Access Right

Access Right — a record in the Access Right System that defines the subject and object of the access right. The subject can be a technician, department, or workplace, while the object can be an individual device, a device group, or a specific system function.

9.3 Permission

Permission — an allowed action that applies to a remote device, a device group, or a specific system function.

The table below lists all available permissions for each purpose.

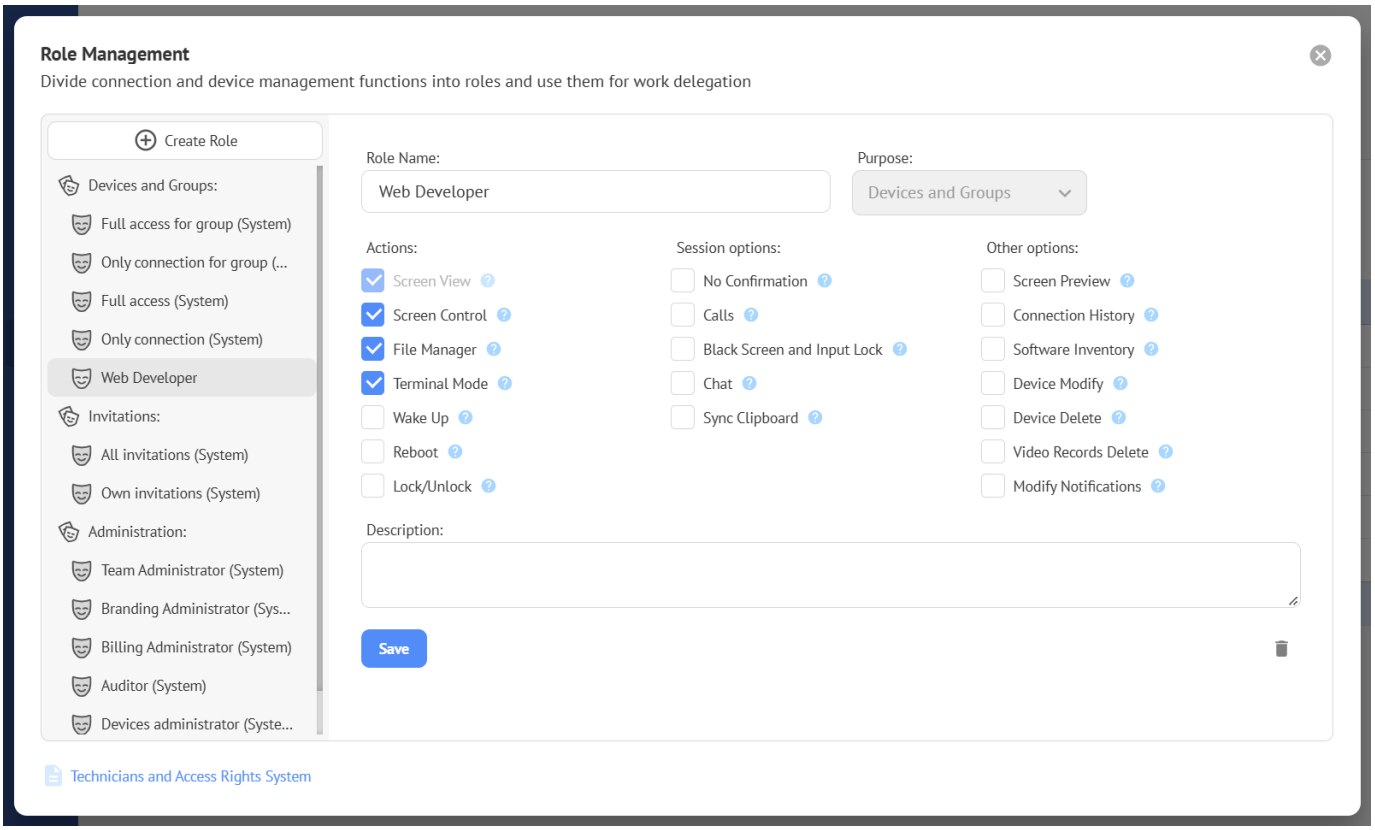
Name	Description
Actions	Available connection modes for the device
`Screen View`	Allows connecting to the device screen in view-only mode
`Screen Control`	Allows controlling the device screen using the mouse and keyboard
`File Manager`	Allows access to the device file system
`Terminal Mode`	Allows terminal-mode access to the device
`Wake Up`	Allows waking the device using Wake-on-LAN
`Reboot`	Allows rebooting the remote device
`Lock/Unlock`	Allows locking or unlocking the remote OS account
Session options	Features available during a remote session
`No Confirmation`	Allows connecting without requesting confirmation from the remote user
`Calls`	Allows making calls
`Black Screen and Input Lock`	Allows enabling Black Screen and blocking input devices
`Chat`	Allows sending text messages
`Sync Clipboard`	Allows synchronizing the clipboard
Other options	Other system functions applicable to devices
`Screen Preview`	Allows viewing a live screen preview in the device list
`Connection History`	Allows access to connection history
`Software Inventory`	Allows access to information about installed software
`Modify Notifications`	Allows managing notifications
`Video Recording Delete`	Allows deleting video recordings
`Device Modify`	Allows editing device properties
`Device Delete`	Allows deleting devices

Name	Description
Access to Invitations	Defines which invitations are accessible
`Own Invitations`	Allows access only to the technician's own invitations
`All Invitations`	Allows access to all team invitations
Actions	Available connection modes
`Screen View`	Allows connecting in screen view mode
`Screen Control`	Allows controlling the screen using the mouse and keyboard
`File Manager`	Allows access to the file system
`Terminal Mode`	Allows connecting in Terminal Mode
Session options	Features available during a connection
`Calls`	Allows making calls
`Chat`	Allows sending text messages
`Reboot`	Allows rebooting the device
`Installation Request`	Allows sending a request to install the agent application
`Sync Clipboard`	Allows synchronizing the clipboard
Other options	Other functions
`Screen Preview`	Allows viewing a live screen preview in the list
`Video Recording Delete`	Allows deleting session recordings

Name	Description
Administrator functions	Administration features
`Audit Log`	Allows access to team-wide audit logs
`Technicians and Team Settings`	Allows managing technicians and team settings
`Branding Settings`	Allows access to branding settings
`Billing Settings`	Allows managing billing settings
`API Settings`	Allows managing API keys
Other	Other features
`Permanent Access`	Grants access to the Permanent Access section. Normally, this section is available when the user has access rights to at least one device or device group. In some cases, however, the section may not be visible. This permission explicitly grants access to the section, for example, to add a new device.

9.4 Role

Role — a set of permissions used within an access right.



9.4.1 System Role

System Role — a built-in role that contains the minimum permissions required for the Access Right System to function and to maintain compatibility with previous versions. Permissions included in system roles cannot be modified.

9.4.2 Role Purpose

Role Purpose — a role property that defines what the role is intended for and limits the set of permissions that can be assigned to it. Three options are available:

1. **Devices and Groups** – for managing devices and device groups in Permanent Access.
2. **Invitations** – for working with Quick Support invitations.
3. **Administration** – for managing technicians and system administration functions.

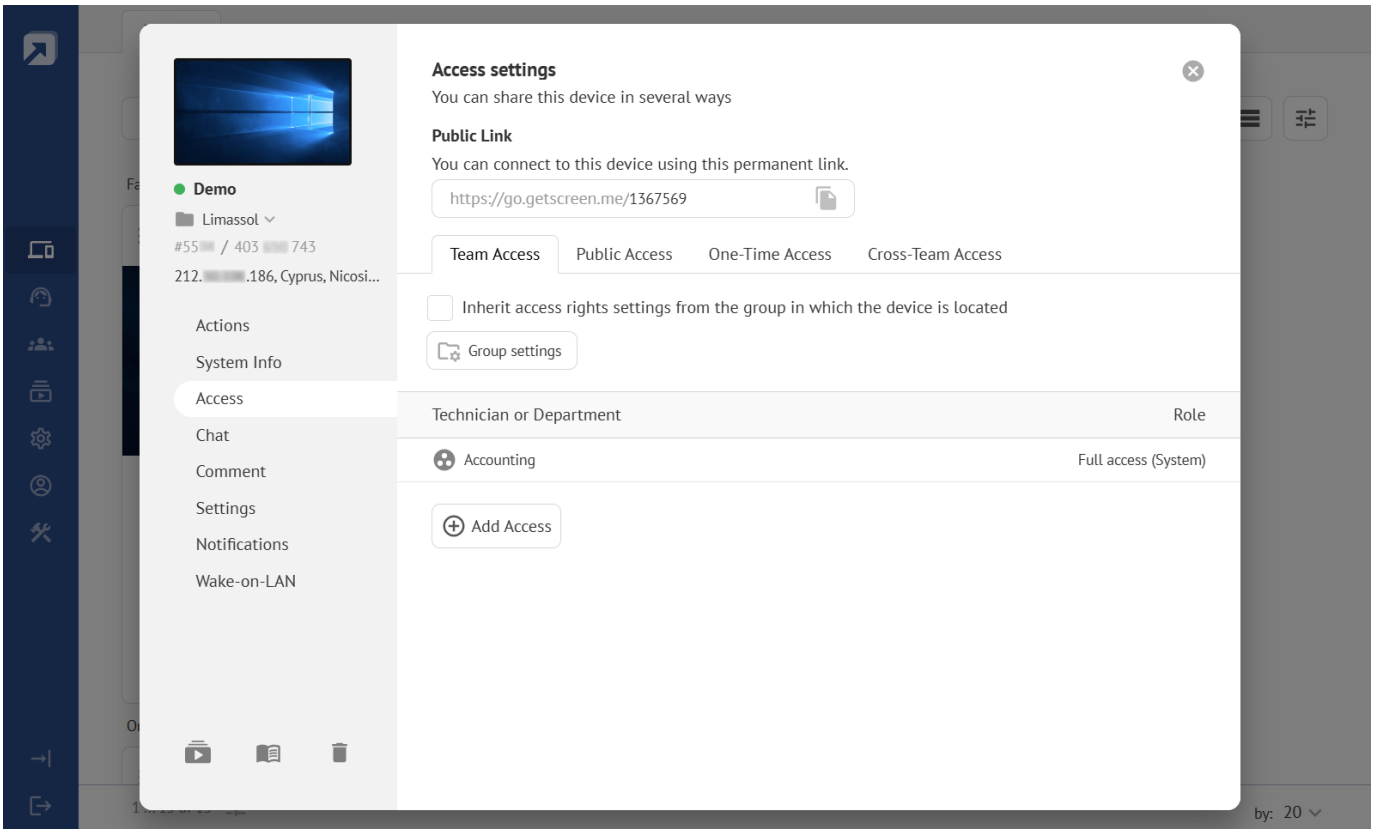
The purpose is selected when creating a new role. The purpose of an existing role cannot be changed.

9.4.3 Role Manager

Role Manager — the interface used to create, edit, and manage roles.

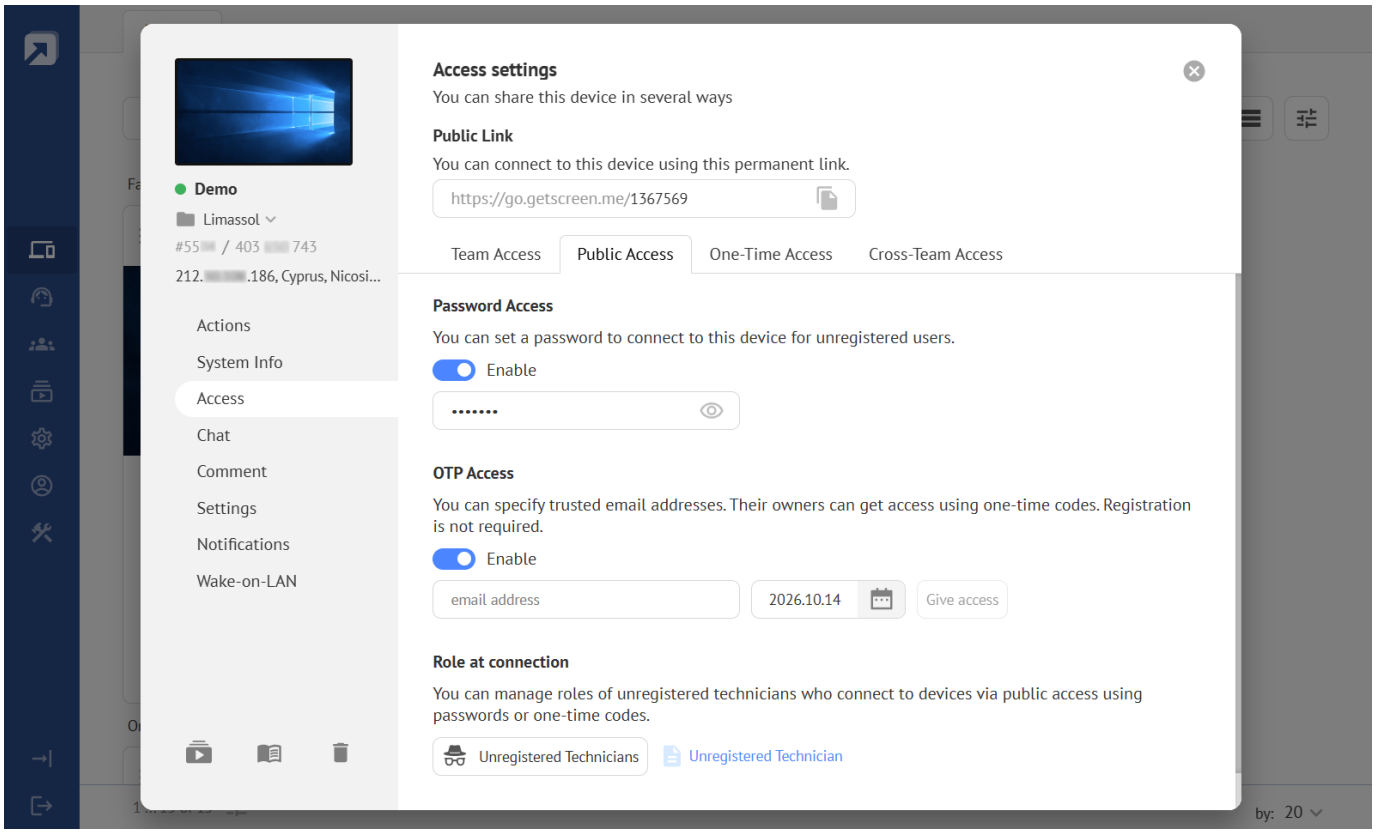
9.5 Team Access

Team Access — an access control subsystem designed for use within a team. It provides shared access to devices or device groups for specific technicians, departments, or workplaces.



9.6 Public Access

Public Access — an access control subsystem that allows unregistered technicians to access an individual device through its Public Link. A role for unregistered technicians can be assigned to individual devices or device groups.



9.6.1 Password Access

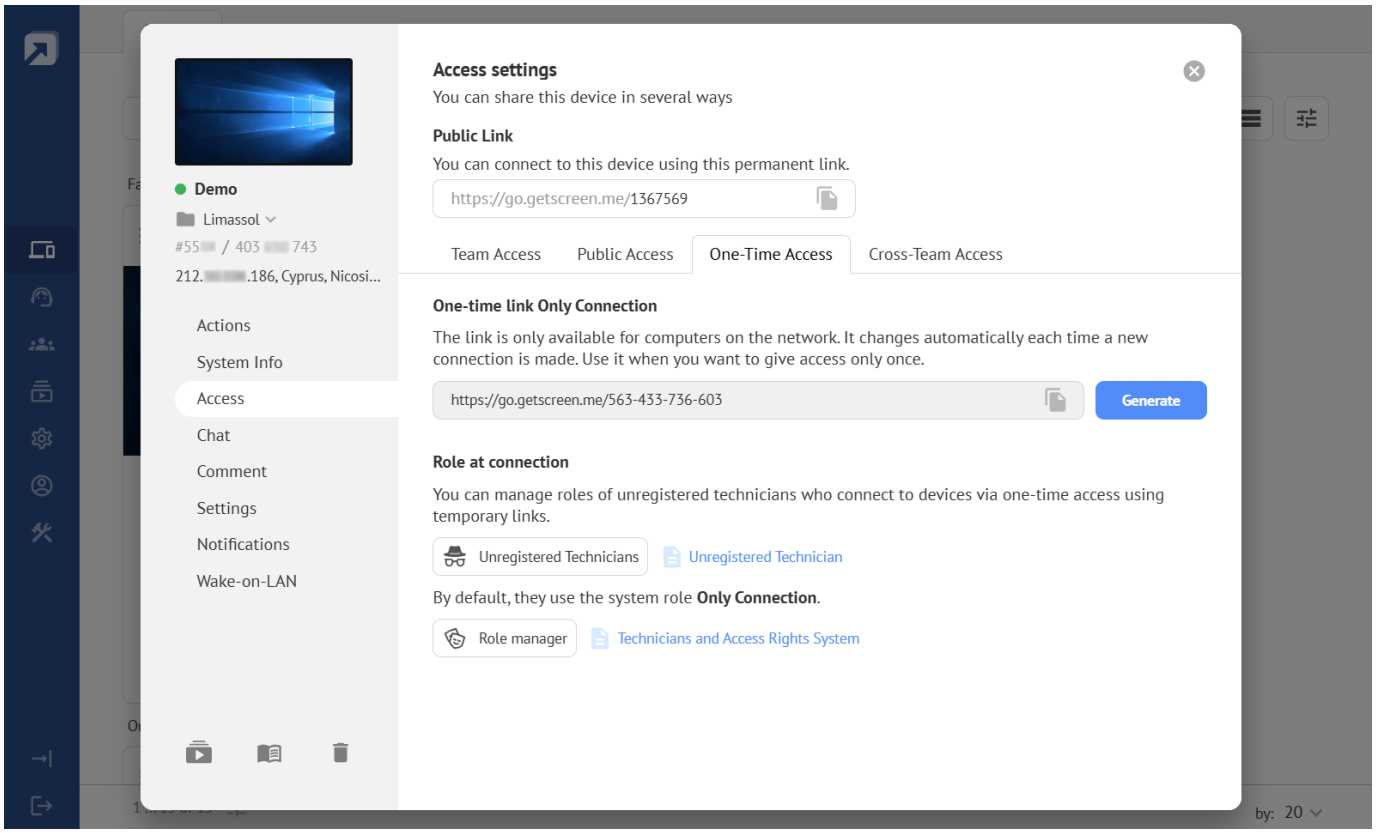
Password Access — access through a Public Link protected by a custom password. When an unregistered technician opens the link, they are prompted to enter the password. If the password is correct, the connection can proceed.

9.6.2 OTP Access

OTP Access — access through a Public Link using a one-time code sent by email. When OTP Access is enabled, a list of allowed email addresses is specified. When an unregistered technician opens the Public Link, they are prompted to enter their email address. If the address is allowed, a one-time code is sent to that address. If the code is entered correctly, the connection can proceed.

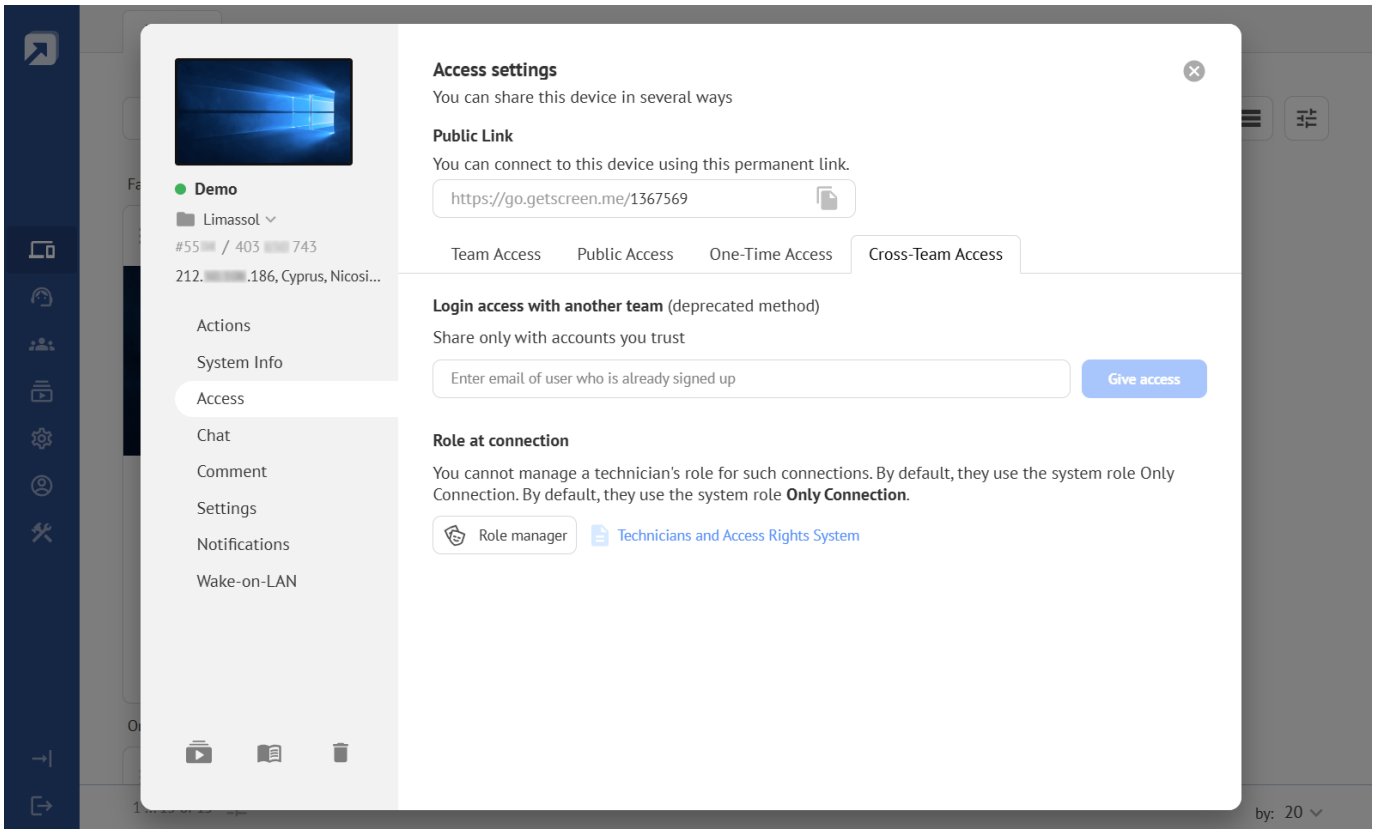
9.7 One-Time Access

One-Time Access — public access to an individual device for unregistered technicians using a one-time Share Link generated in the agent application on the remote device. A role for unregistered technicians can be assigned to individual devices or device groups.



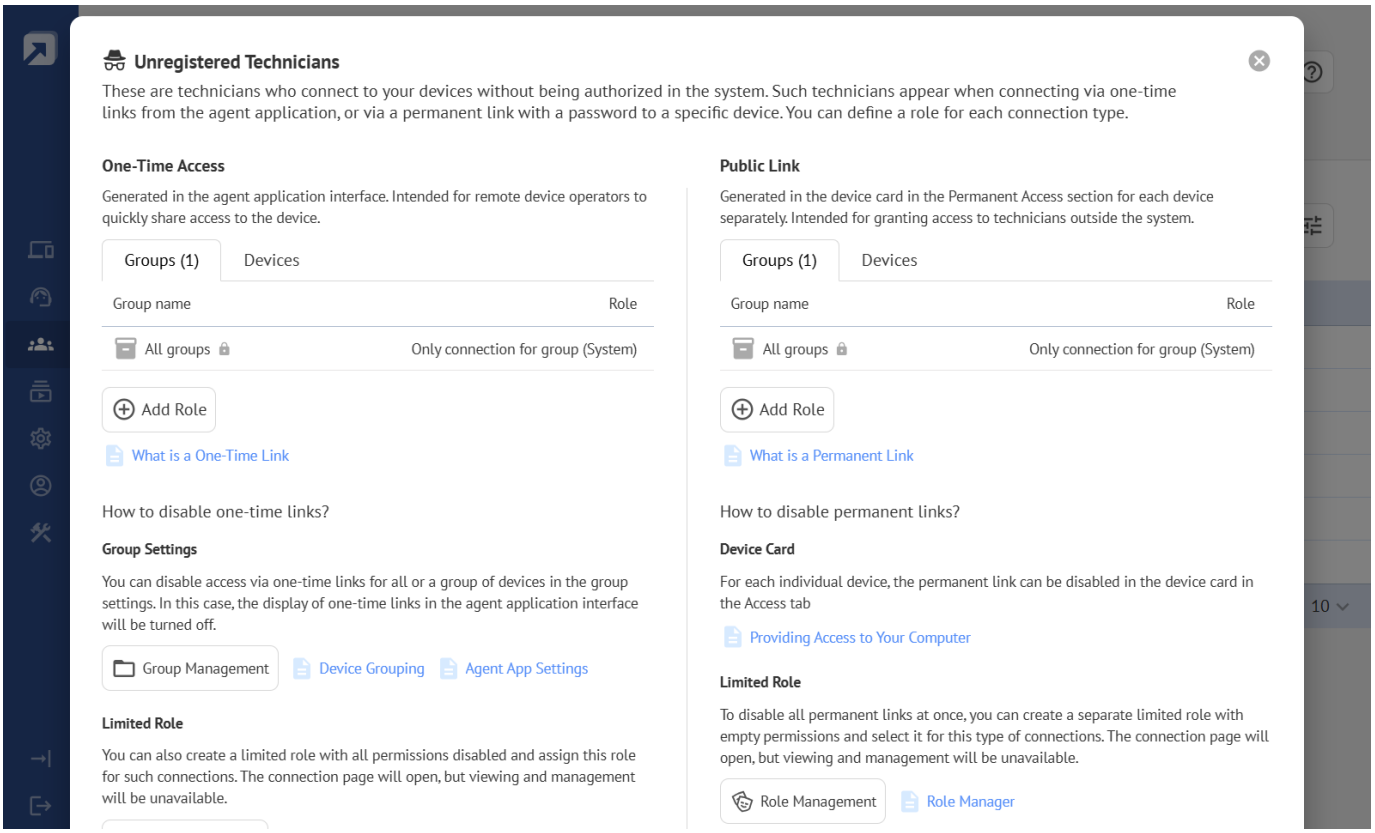
9.8 Cross-Team Access

Cross-Team Access — direct access to an individual device granted to a technician from another team. Access is granted using the technician's email address.



9.9 Unregistered Technician

Unregistered Technician — an operator who can access and control a device without having an account in the system. For public access methods, the role assigned to an unregistered technician can be predefined and restricted.

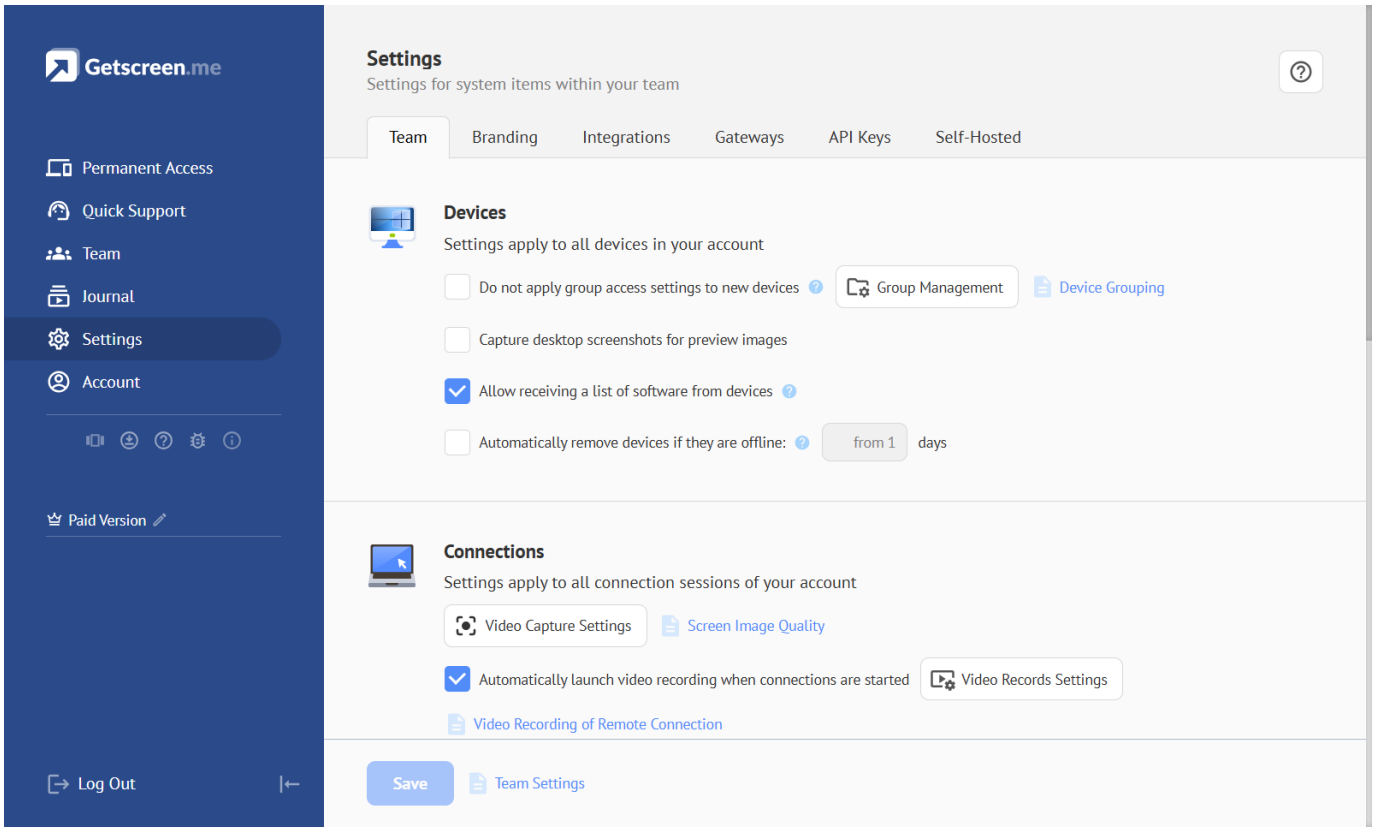

Unregistered Technicians
These are technicians who connect to your devices without being authorized in the system. Such technicians appear when connecting via one-time links from the agent application, or via a permanent link with a password to a specific device. You can define a role for each connection type.
One-Time Access
Generated in the agent application interface. Intended for remote device operators to quickly share access to the device.
Groups (1)
Devices
Group name
Role
All groups
Only connection for group (System)
Add Role
What is a One-Time Link
How to disable one-time links?
Group Settings
You can disable access via one-time links for all or a group of devices in the group settings. In this case, the display of one-time links in the agent application interface will be turned off.
Group Management
Device Grouping
Agent App Settings
Limited Role
You can also create a limited role with all permissions disabled and assign this role for such connections. The connection page will open, but viewing and management will be unavailable.
Public Link
Generated in the device card in the Permanent Access section for each device separately. Intended for granting access to technicians outside the system.
Groups (1)
Devices
Group name
Role
All groups
Only connection for group (System)
Add Role
What is a Permanent Link
How to disable permanent links?
Device Card
For each individual device, the permanent link can be disabled in the device card in the Access tab
Providing Access to Your Computer
Limited Role
To disable all permanent links at once, you can create a separate limited role with empty permissions and select it for this type of connections. The connection page will open, but viewing and management will be unavailable.
Role Management
Role Manager
10

10. Settings

This account section brings together all available settings for system elements and features used during remote access and its administration.

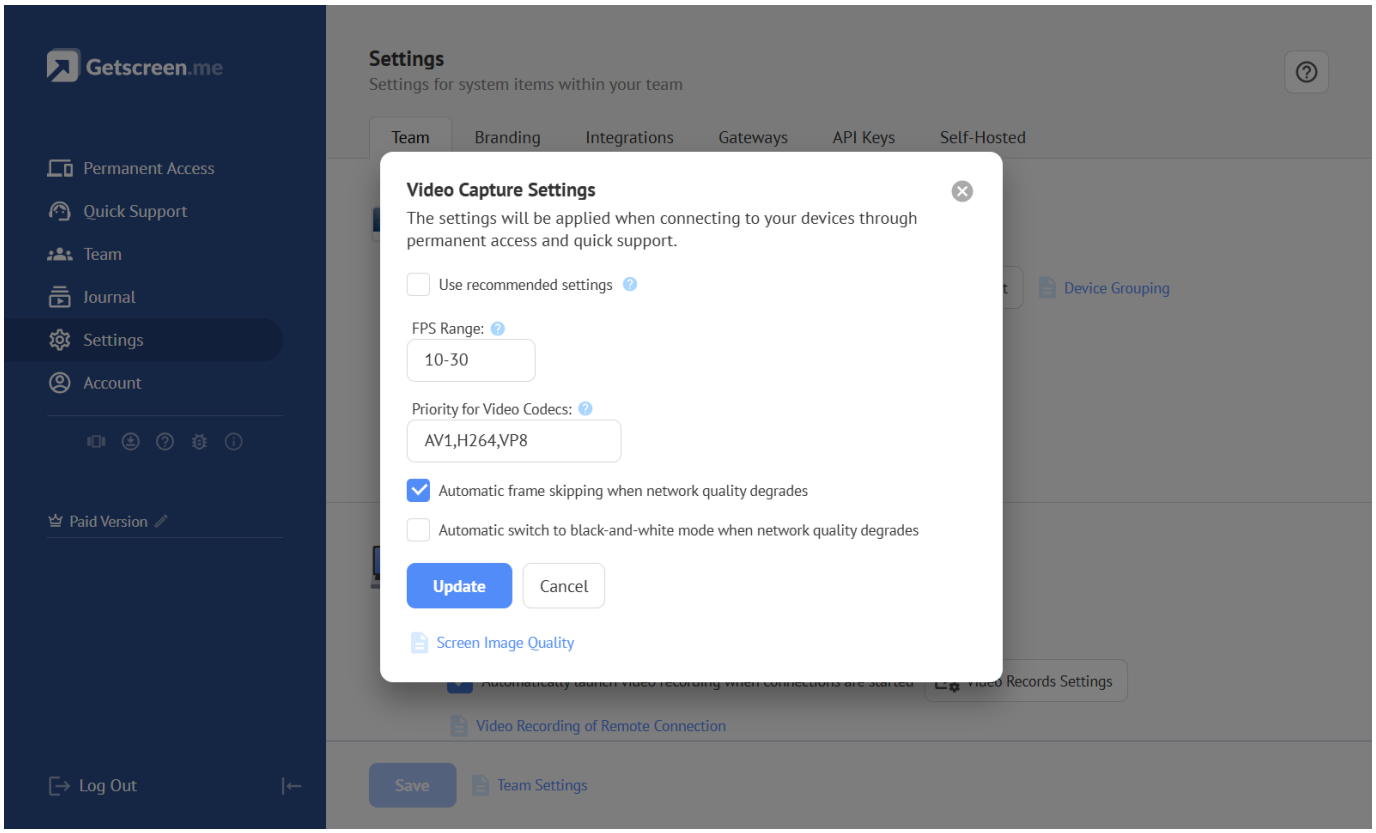
10.1 Team Settings

Team Settings — remote access settings that apply within a team to all system elements, including technicians, devices, and connections. Team settings can be managed by the team owner or by a technician with team administration permissions. Learn More



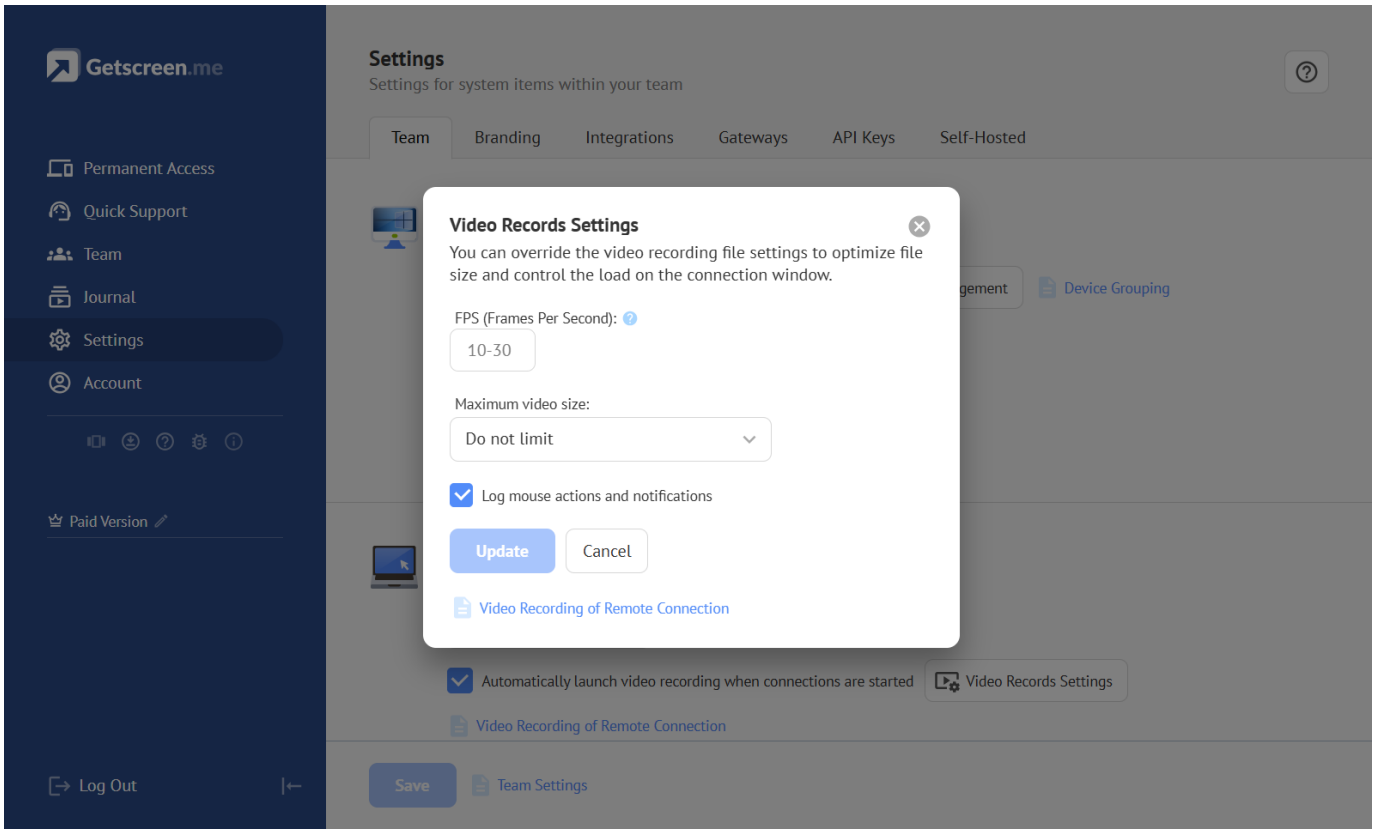
10.2 Video Capture Settings

Video Capture Settings — settings used to configure encoding of the video stream that transfers the remote device screen image. These settings are intended to optimize image quality and the amount of transmitted data. Learn More



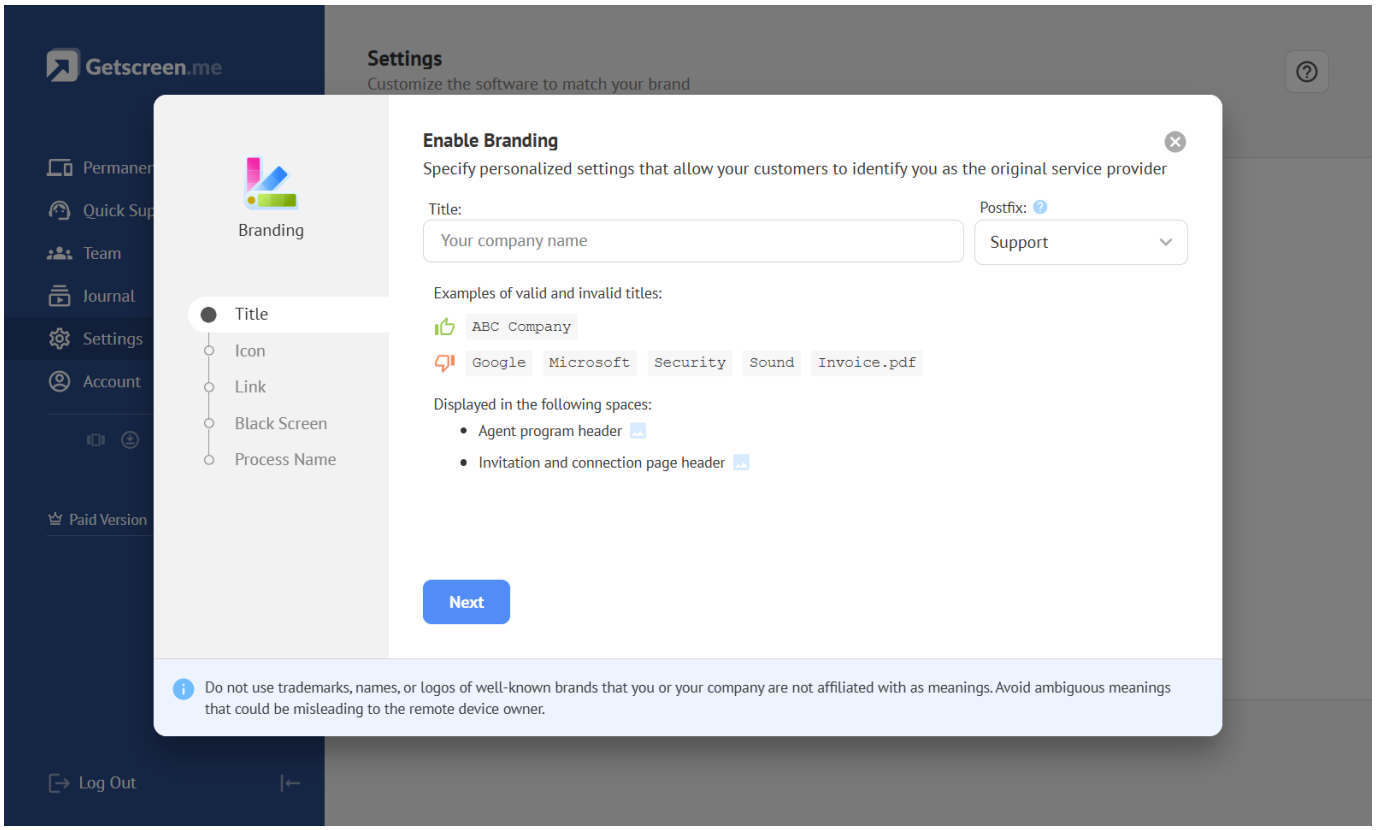
10.3 Video Records Settings

Video Records Settings — settings used to configure video recording of remote connection sessions. Video recording is a resource-intensive process performed on the technician's device during a connection. These settings help optimize resource usage on the technician's device. Learn More



10.4 Branding Settings

Branding Settings — settings used to customize the system interfaces that remote device users interact with. Branding can be applied to connection links, elements of the agent application, and Quick Support invitation pages. Learn More

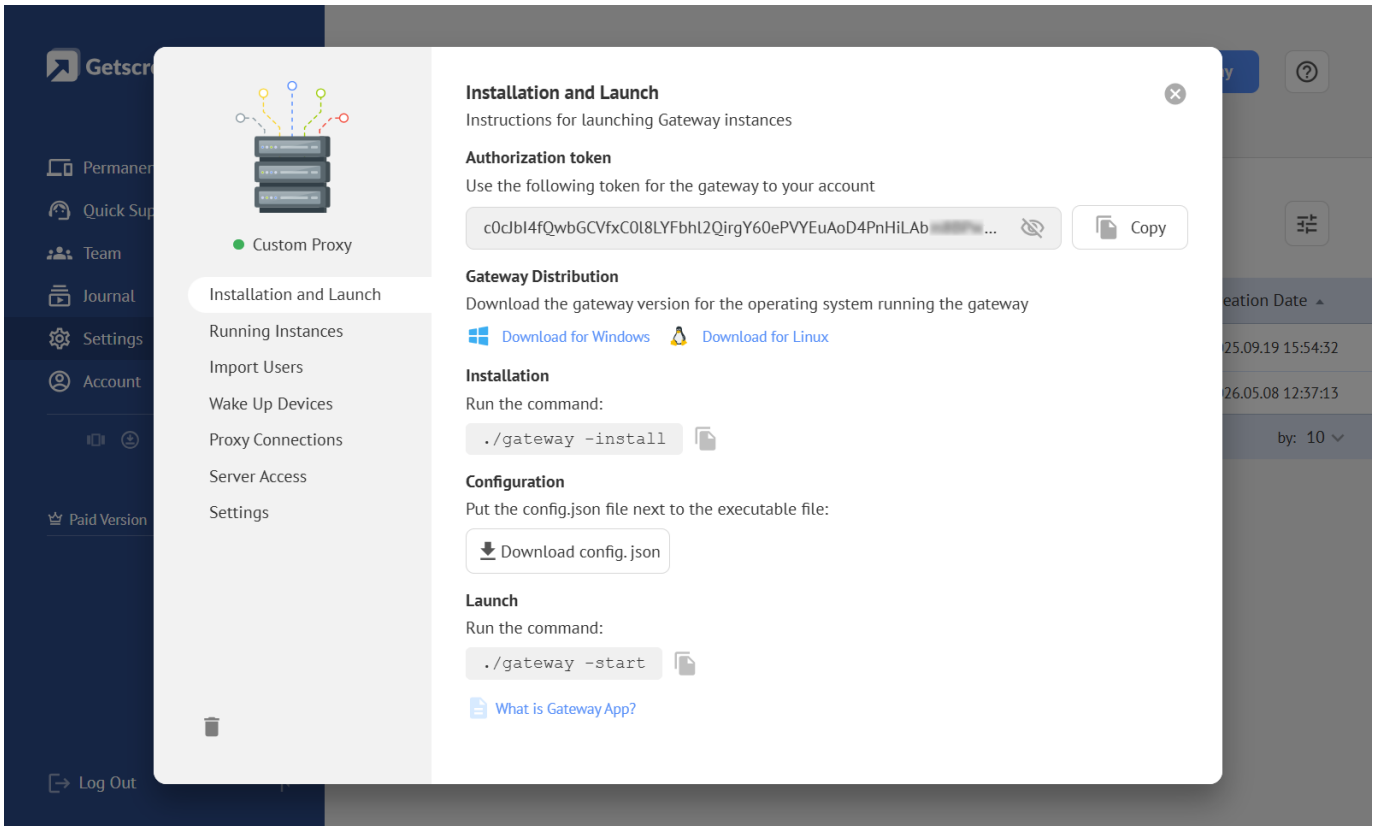


10.5 Gateway Settings

Gateway Settings — settings for gateway applications used to integrate with other systems or extend account functionality. Learn More

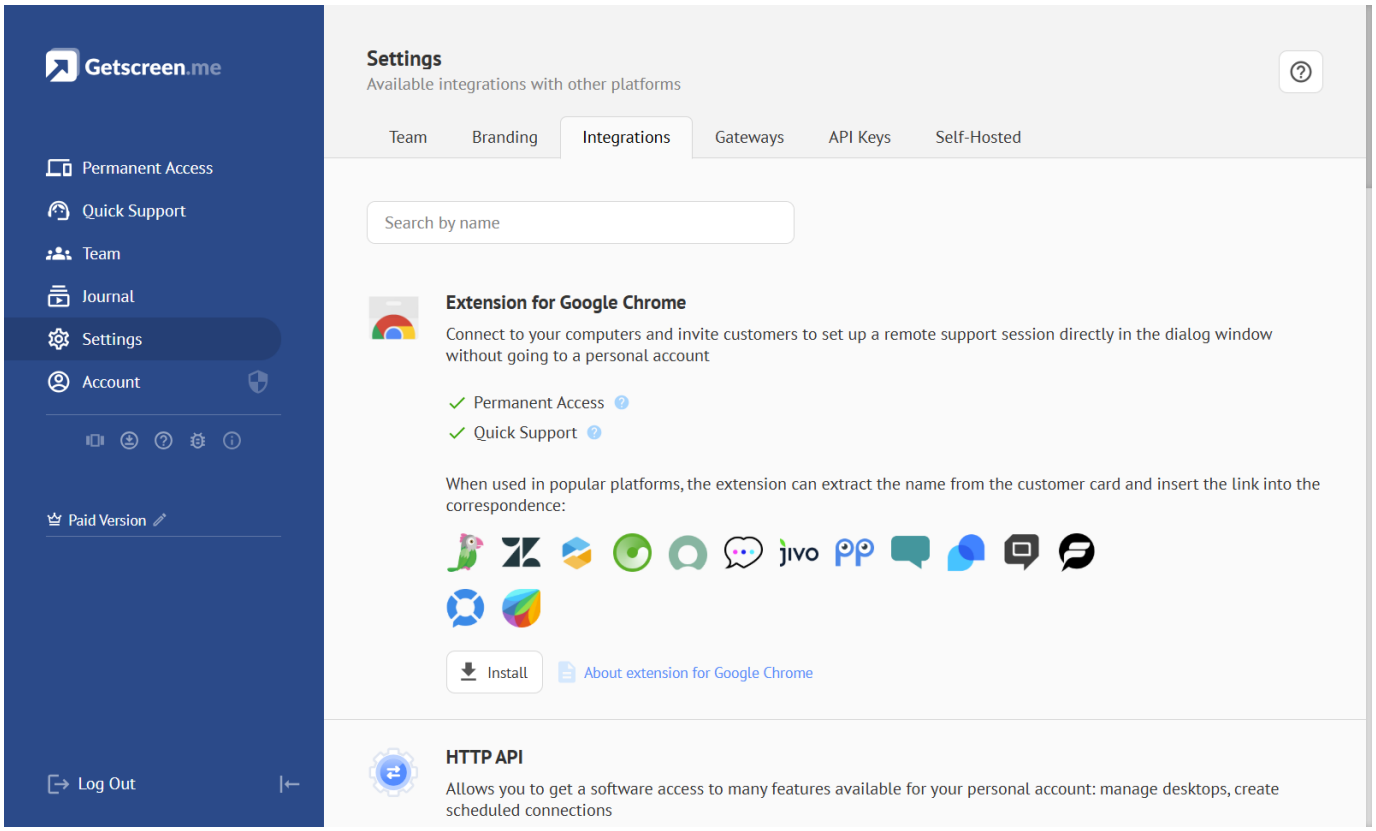
10.5.1 Authorization Token

Authorization Token — a token used to authorize a gateway application on the server.



10.6 Integrations

Integrations — a list of systems and individual features available for integration with the account.

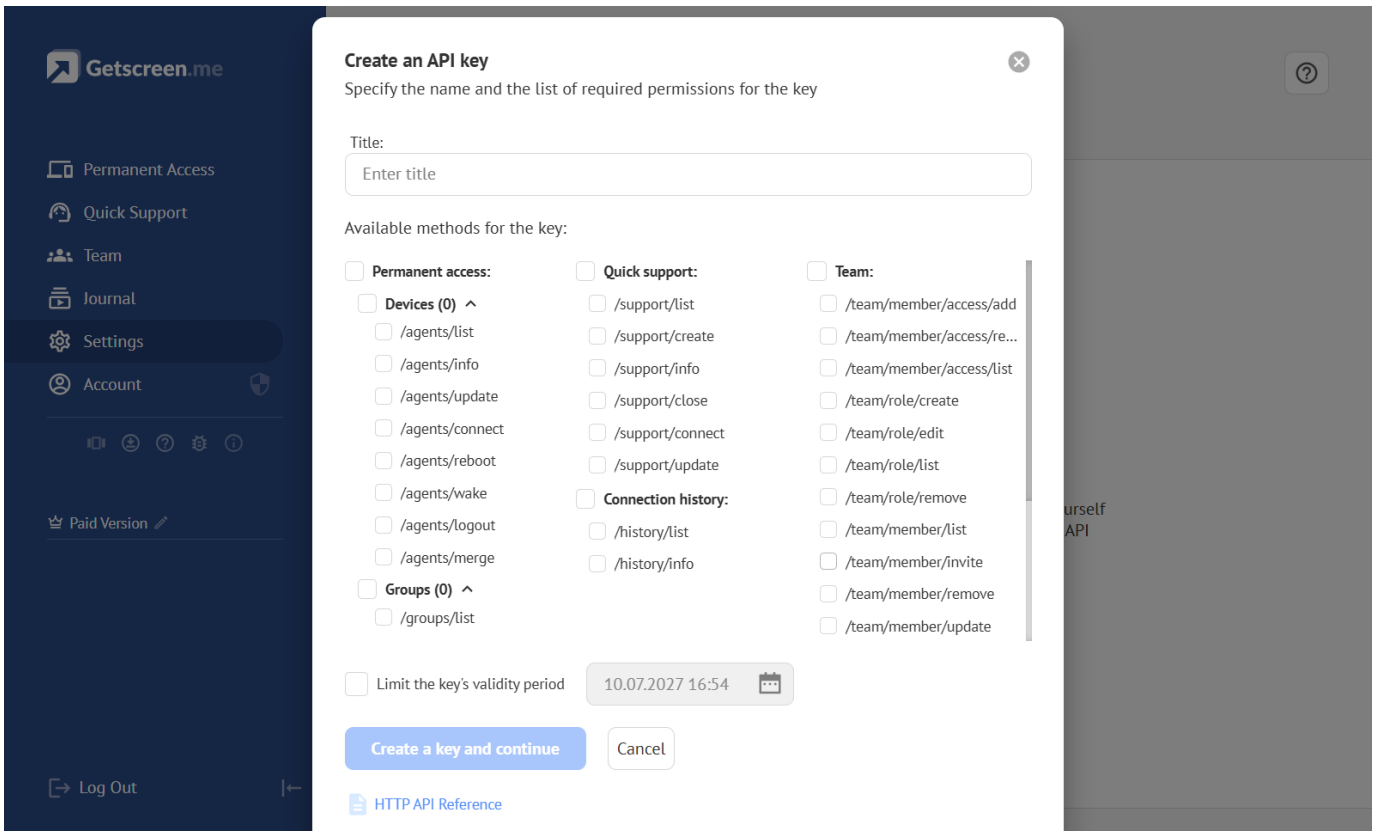


10.7 HTTP API

HTTP API — a public server interface for automated data exchange that provides methods for managing account elements and connecting to devices.

10.7.1 API Key

API Key — a key used to authorize requests sent to the server through the HTTP API. Each key has a defined set of allowed methods and an expiration date.

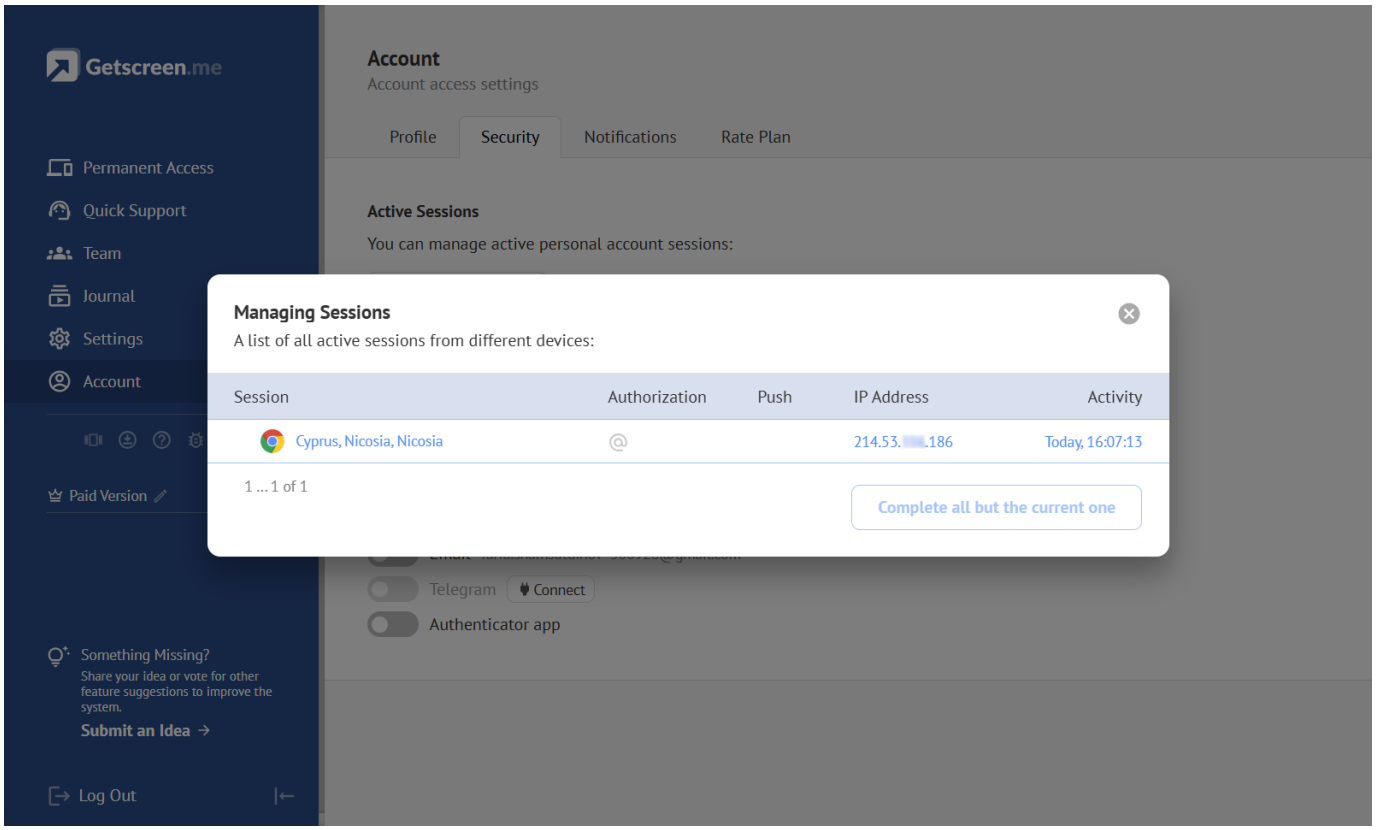


11. Security

This section lists features directly related to account security and the remote connection process.

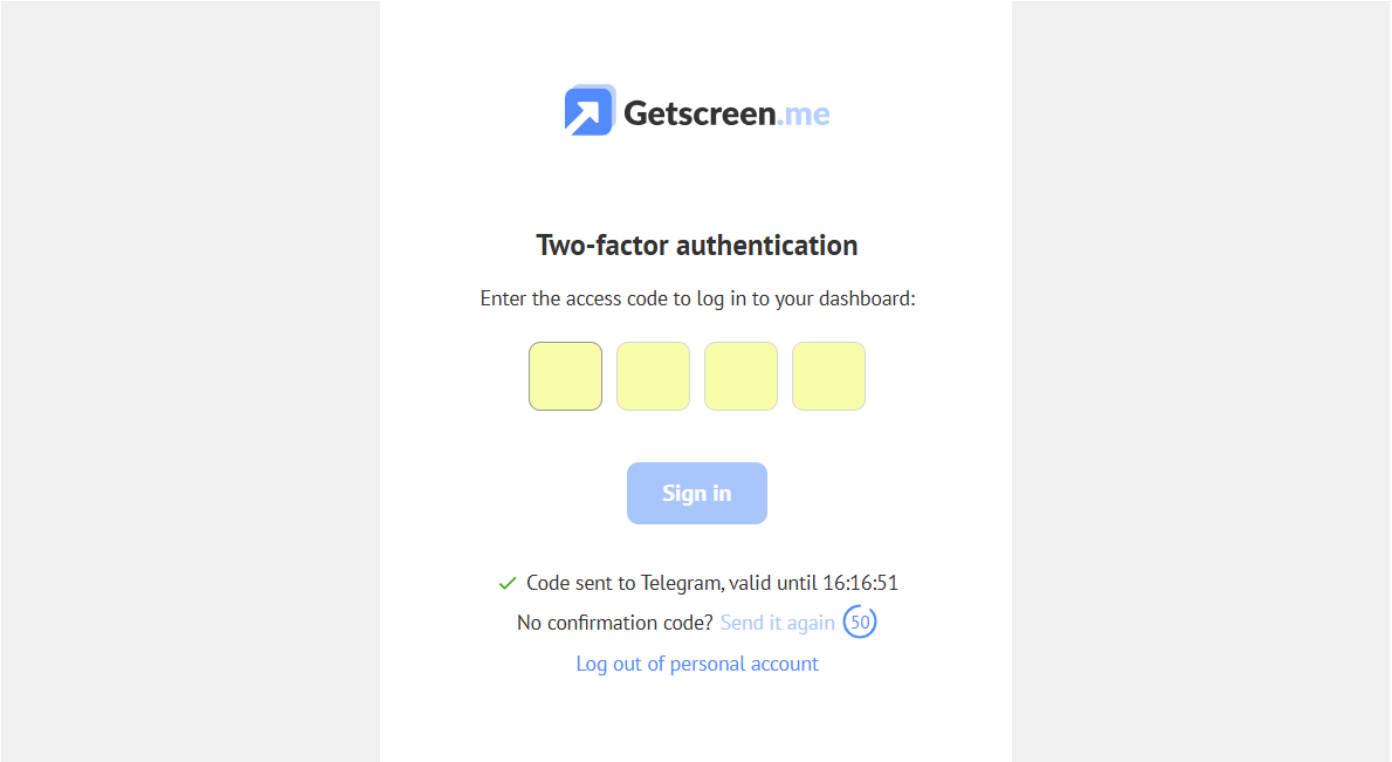
11.1 Dashboard Session

Dashboard Session — an active account login session established through the web dashboard or desktop dashboard application. When the account password is changed, all active sessions are terminated. The dashboard interface also allows you to view and manually terminate active sessions.



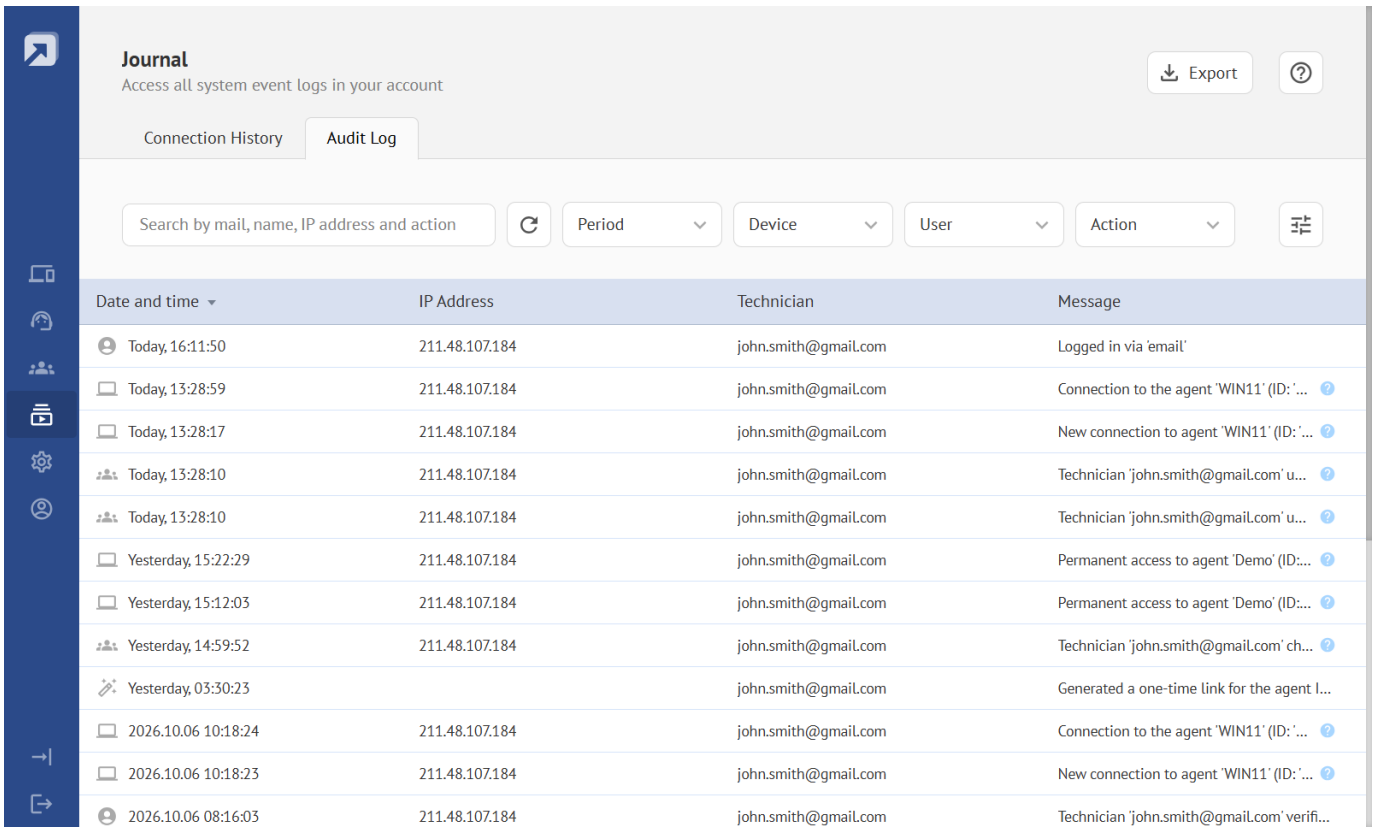
11.2 Two-Factor Authentication (2FA)

Two-Factor Authentication (2FA) — an additional account login security measure that verifies the account owner using one-time codes generated by another trusted system or application. Learn More



11.3 Audit Logs

Audit Logs — a system for collecting and displaying information about events related to the account and its associated devices. Learn More



11.4 Black Screen Mode

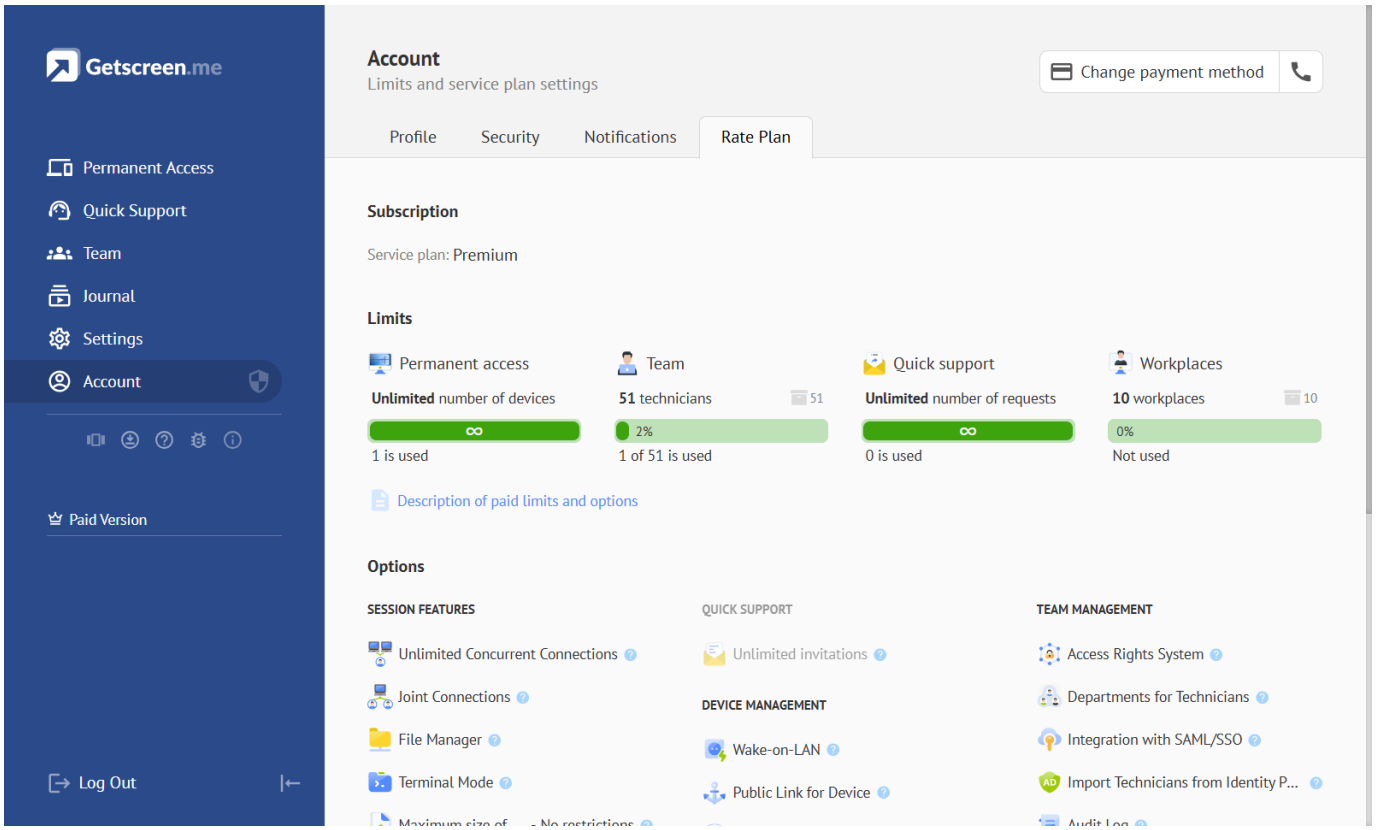
Black Screen Mode — a mode that disables the screen image on the monitor of the remote device while a connection is active. Learn More

11.5 Lock Input Mode

Lock Input Mode — a mode that disables input devices, including the keyboard, mouse, and touchscreen, on the remote device while a connection is active. Learn More

12. License

This section describes the entities used in the account licensing system.



Remote Access Pricing Plans Explained: Selecting the Best Fit

Learn more about the available pricing plans in the overview article on our blog.

12.1 Limits

Limits — licensing restrictions applied to measurable system resources. They define the allowed usage volume and directly affect the amount of system resources consumed.

12.1.1 Team

Team — a limit on the number of technician accounts within your team. Each technician has separate credentials for signing in to the dashboard. Learn More

12.1.2 Permanent Access

Permanent Access — a limit on the number of devices that can be added to Permanent Access and accessed by the account owner and team members at any time. Learn More

12.1.3 Quick Support

Quick Support — a limit on the number of active Quick Support invitations used for one-time connections to devices of external users or customers. Learn More

12.2 Premium Options

Premium Options — additional remote access features that improve technician workflow, simplify remote access management, and enhance the level of service provided to third-party customers.

12.2.1 Concurrent Connections

Concurrent Connections — Allows a technician to maintain open connections with multiple devices simultaneously, without any limit on the number of connections. Learn More

12.2.2 Joint Connections

Joint Connections — Allows a technician to connect to a device that is already being accessed by another technician. Learn More

12.2.3 File Manager

File Manager — Enables the exchange of batches of files, allowing multiple files and folders to be transferred at once. Learn More

12.2.4 Terminal Mode

Terminal Mode — Allows a technician to launch the command-line terminal without connecting to the device's screen. Learn More

12.2.5 Support Mobile Devices

Support Mobile Devices — Allows a technician to connect to mobile devices running the Android operating system. Learn More

12.2.6 Black Screen Mode

Black Screen Mode — Allows a technician to disable the screen or separately disable the keyboard and mouse on the remote device during a connection. Learn More

12.2.7 Video Recording

Video Recording — Allows saving video recordings of all connections. Learn More

12.2.8 Reboot During Connection

Reboot During Connection — Allows a technician to reboot a device with automatic reconnection. Learn More

12.2.9 In-Session Calls

In-Session Calls — Allows the technician and the remote device user to call each other during a connection session. Learn More

12.2.10 Support RDP Protocol

Support RDP Protocol — Allows a technician to use the RDP protocol to log into systems when connecting to servers. Learn More

12.2.11 Connection History

Connection History — Allows viewing the connection history. Learn More

12.2.12 In-session Unattended Access Request

In-session Unattended Access Request — Allows a technician to request permission from the remote device user to add the device for permanent access during a connection session. Learn More

12.2.13 Custom Proxy for Media Data

Custom Proxy for Media Data — Allows custom proxy servers to be used for transferring media data between the technician's device and the remote device. Learn More

12.2.14 Wake-on-LAN

Wake-on-LAN — Allows a technician to wake up powered-off devices configured for permanent access using the Wake-on-LAN command. Learn More

12.2.15 Public Access for Device

Public Access for Device — Allows a technician to assign a public link to a device from permanent access, enabling connections via the link. Learn More

12.2.16 Customization of Public Access Link

Customization of Public Access Link — Allows a technician to customize public links to devices. Learn More

12.2.17 Share with Another Account

Share with Another Account — Allows a technician to share a device with any system account using a login. Learn More

12.2.18 Proxy Settings for Agent App

Proxy Settings for Agent App — Allows a technician to predefine proxy settings for devices with permanent access. Learn More

12.2.19 Server Access Through Gateway

Server Access Through Gateway — Allows the Gateway application to be used as a proxy to establish a connection with the server when the agent application has no direct access to the server. Learn More

12.2.20 Team Access Rights System

Team Access Rights System — Allows configuring access rights to devices for team technicians.Learn More

12.2.21 Departments for Technicians

Departments for Technicians — Allows grouping team technicians into departments. Learn More

12.2.22 Audit Log

Audit Log — Allows viewing the system event log of all actions performed by all team technicians. Learn More

12.2.23 Import Technicians from Identity Provider (LDAP)

Import Technicians from Identity Provider (LDAP) — Allows importing technician accounts from Identity Provider by using LDAP protocol. Learn More

12.2.24 Branding Title, Icon and Subdomain

Branding Title, Icon and Subdomain — Allows customizing system elements displayed on the remote device. Learn More

12.2.25 Custom Domain for Links

Custom Domain for Links — Allows you to set your own domain for all connection links displayed on the remote device. Learn More

12.2.26 HTTP API Access

HTTP API Access — Allows accessing the system's API through HTTP API requests. Learn More