



Splashtop Enterprise

Administrator Guide

November 3, 2023

Table of Contents

Change Log - from last 11/03/2022 version	4
1. Deployment.....	5
How do I update Splashtop Streamer?	8
Preference Policies.....	9
2. MacOS Additional Requirements.....	11
3. Single Sign-On (SSO).....	12
4. Inviting Users.....	13
Team Roles.....	13
5. Grouping	14
Connection Pool.....	14
Adding Users or Computers to a Group.....	15
6. Access Permissions.....	16
7. Scheduled Access	17
Scheduled Access Configuration	17
Managing Resources & Schedules	21
If a Group Admin is removed, what happens to their owned Resource/Schedules?	22
8. Team Settings	23
Overview of Team Settings	23
Feature Configuration	23
User Configuration	25
Security	25
9. Granular Controls.....	26
10. Endpoint Management (Technicians)	28
Windows Event Logs	28
Computer Inventory – System, Hardware, Software.....	28
Endpoint Security.....	29
Windows Updates.....	29
1-to-Many Actions & Schedules.....	30
Configurable Alerts & Smart Actions	31
Remote Command	31
System Tools (Background Actions).....	32
11. Attended Access - SOS (Technicians)	33

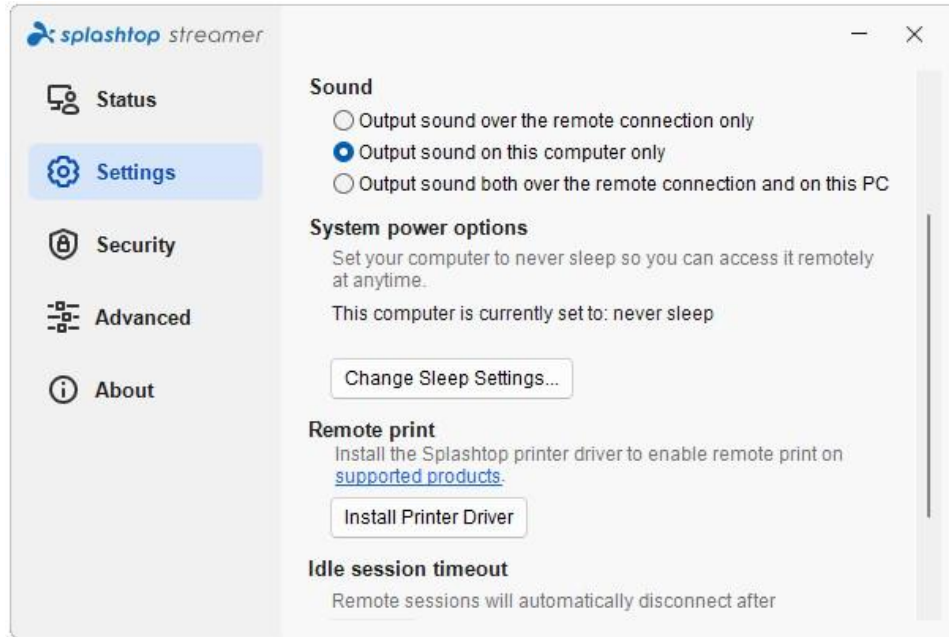
Granular Settings	33	
12.SOS Customization (Technicians)		34
13.Service Desk (Technicians)		35
.....	35	
Channel Management.....	36	
Creating Support Sessions	36	
Invitation Link or 6-digit PIN Code	36	
SOS Call	37	
Web Support Form.....	38	
14. Logs	41	
15. Open APIs.....	42	
16. Additional Features	43	
IP Restriction	43	
SIEM Logging.....	43	
Splashtop Connector.....	44	
Splashtop AR	44	

Change Log - from last 11/03/2022 version

- Deployment, Section 1
 - Add guide for PDQ, Kaseya deployment
- Single Sign-On (SSO), Section 3
 - Super Admins can also manage SSO
- Grouping, Section 5
 - Add Connection Pool section
- Scheduled Access, Section 7
 - Super Admins can configure scheduled timezone
- Team Settings, Section 8
 - Update new UI and settings
- Granular Controls, Section 9
 - Add granular controls for remote control, remote command prompt
- Endpoint Management, Section 10
 - Rename section from Remote Computer Management
 - Add Smart Actions, System Tools – Registry Editor, Service Manager, Device Manager, Task Manager
- Service Desk (Technicians), section 13
 - Add SOS Call, Web support forms
- Open APIs, Section 15
 - New section for Splashtop RESTful APIs

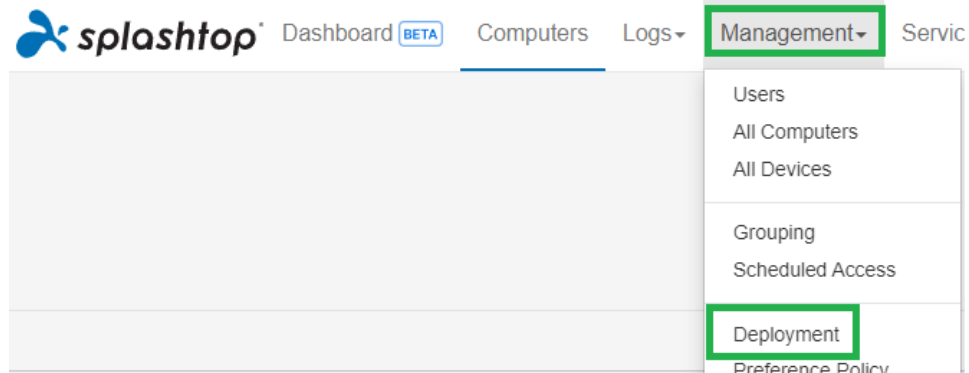
1. Deployment

Install Splashtop Streamer on computers to make them remotely accessible. You can create a deployment package to [customize the default Streamer settings for deployment](#). This way, you don't have to manually configure the settings after installation.



[Overview of the different streamer settings](#)

1. Log into my.splashtop.com and click **Management -> Deployment**.



- Click **Create Deployment Package** and select your desired Streamer settings. When creating the deployment package, you have the option of specifying default settings, including computer naming rule, security settings, sound re-direction, etc.

General Settings

Auto-launch streamer

Automatically launch Splashtop Streamer every time the computer starts.

Idle session timeout

Remote sessions will automatically disconnect after minutes of no activity (0 means no timeout).

Hide streamer tray icon

Hide streamer icon on Windows system tray or Mac menu bar. Check this option to reduce the chance of users tampering with the streamer.

Enable direct connection

When on the same network, use direct connection for better performance. Based on your organization's security policy, you may want to disable this option.

Security

Require Windows or Mac login

Require entering the computer's user name and password when

Note: If using Single Sign-On (SSO), do not select "Lock streamer settings using Splashtop admin credentials" - SSO accounts cannot unlock the streamer.

- After saving the package, you can see the newly created package and unique 12-digit deployment code. Click **Deploy** to view deployment options.

Deployment Package Name	Computer Naming Rule	Code	Date of Creation	Deploy
Animation	Use current computer name	PY42WJK2WPXS	2020/07/08 10:00	 <input type="button" value="Deploy"/>

- You will find two options for distributing the deployment package:

Option 1: Share Link

Send this link to allow a user to download and install the streamer for you.

Shareable Link

Option 1: Share Link

- Send the link above to your users. The link will take them to a web page where they can download the installer and follow simple instructions to set up.
- After your users run the installer, their computers will become accessible by you.

Users who follow the link will see instructions to download and install the streamer.

Welcome to Splashtop Remote Support

Install Splashtop Streamer on your computer to allow the organization below to remotely access your computer at any time (unless otherwise configured).

's team (owner: @splashtop.com)

I trust the organization above and want to allow remote access to my computer.

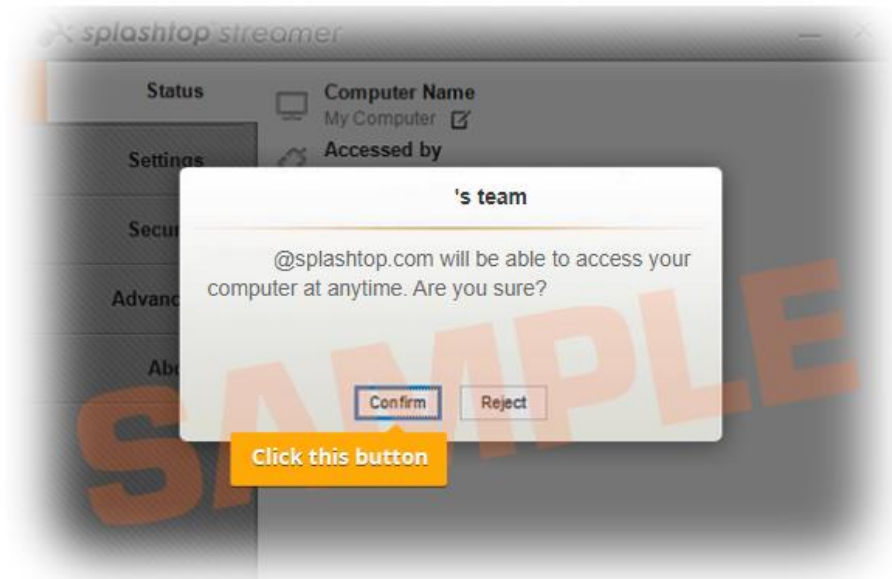
Step 1 : Download the streamer



Also available for  Mac,  Android

Step 2 : Run the installer and allow access






After the installation is complete, open the Splashtop streamer app, and click "Confirm" to allow access.



Option 2: Download Installer

Download the installer to install directly on your computer, share via Dropbox, email, etc., or prepare for deployment with a 3rd party tool.

Option 2: Download Installer

Platform     Windows (EXE, version 3.4.2.1) (Easy Deployment)  [Download](#)

Easy deployment installer : The deployment code is built into the installer.
There is no need to enter deployment code when installing the streamer.

- 1 Download the streamer installer.
- 2 Send the installer and the 12-digit code to your users.
- 3 After your users run the installer and enter the code, their computers will become accessible by you.

Multiple installer options are offered for Windows, Mac, Android, and Linux.

- View this article for [Silent install parameters](#)
- Deployment guides are also available for:
 - [Group Policy \(GPO\)](#)
 - [Jamf Pro](#)
 - [Microsoft Intune](#)
 - [PDQ](#)
 - [Kaseya \(For Mac\)](#)
- Deployment package settings only apply to the Streamer upon installation. To update a Streamer's settings after deployment, you can re-deploy with a new package, manually change the settings directly in the Streamer, or use Preference Policies (mentioned next) to remotely manage settings.
- Deleting a deployment package does not affect any already-deployed computers – it prevents any new deployments with this package code.

How do I update Splashtop Streamer?

There are multiple ways to update the streamer, including:

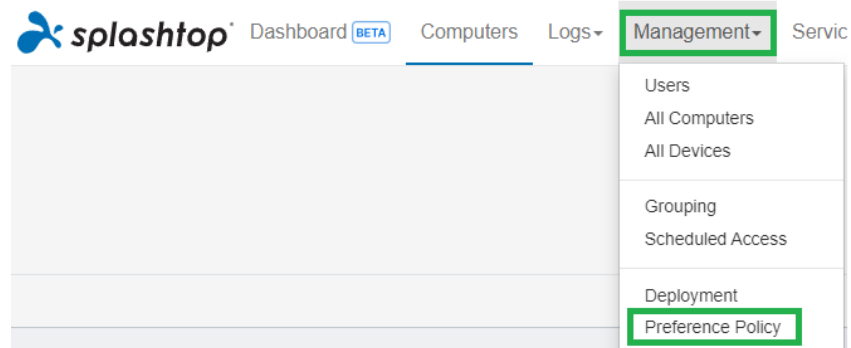
- Manually Update from the web console
- Manually Update from the Streamer -> About -> Check for Updates tab
- Manually Update by running the latest streamer installer
- Manually Update from within the Business App
- Silently update using the .EXE, .MSI or .PKG

For more info, see this article on [Splashtop Streamer Updates](#).

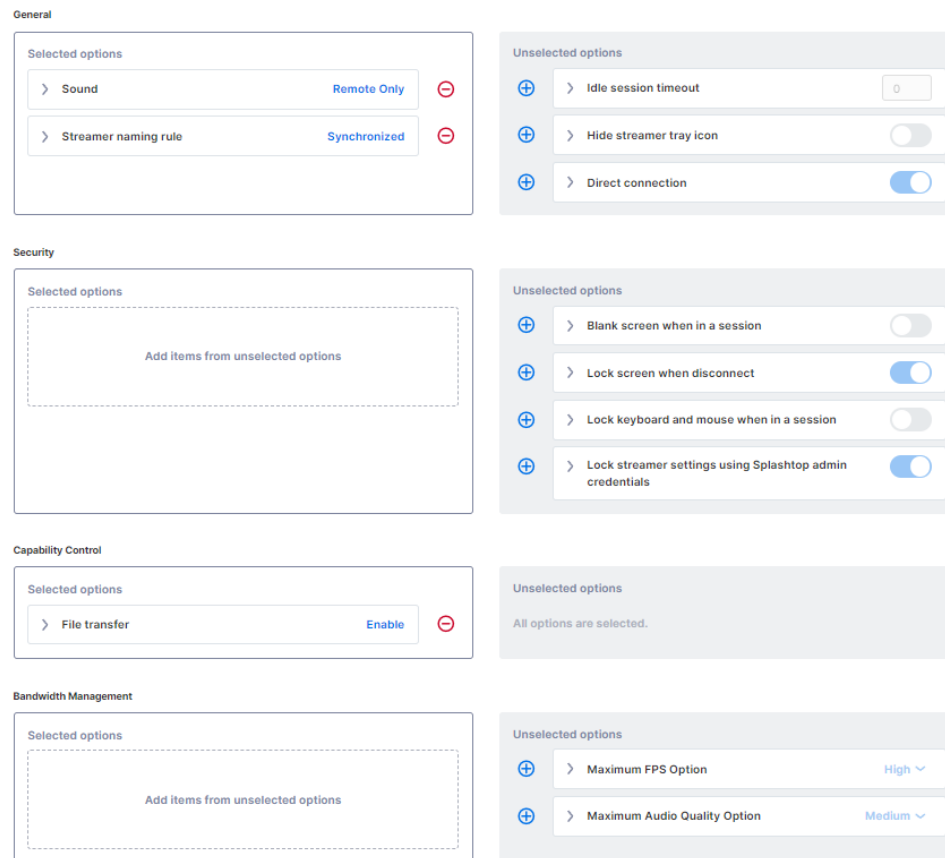
Preference Policies

Starting with Splashtop Streamer v3.5.2.2, you can manage certain streamer and in-session settings from the web console through Preference Policies. By assigning endpoints to your policy, you can configure and overwrite existing Streamer settings without having to redeploy the Streamer or manually change the settings locally at the endpoint.

1. To create a new policy, log into my.splashtop.com and click **Management -> Preference Policy**.



2. Add or remove different settings from the policy, including general in-session settings, security, and bandwidth options.




3. Assign computers to the policy.
Note: Only streamers v3.5.2.2+ will be shown in the menu.

Edit Computer

Updating to the latest streamer version is recommended to make sure the computer can comply to all policy settings.

1 computer selected All Groups ▾ ☰ 🔍

<input checked="" type="checkbox"/>	Computer Name ↑	Streamer Version ⓘ	Group Name	Applied Policy
<input checked="" type="checkbox"/>	 Windows 11	3.5.2.2	Windows	


4. Under Management -> All Computers, you can check which policy is assigned to each computer.

Management / All Computers

All Computers

Demo Team / 40 of 1600 computers deployed Latest s

Add Bulk Actions ▾ ↻ 0 selected

<input type="checkbox"/>	Name ↑	Group	Streamer Ver.	Preference Policy
<input type="checkbox"/>	 Windows 11	Data	3.6.0.1	Test Policy

5. When a user connects to a computer that is part of your preference policy, the configured settings or restrictions will apply to the remote session. The user will not be able to reconfigure the policy settings from the Business App or Streamer menus.

[View this article for more details on behavior and instructions.](#)

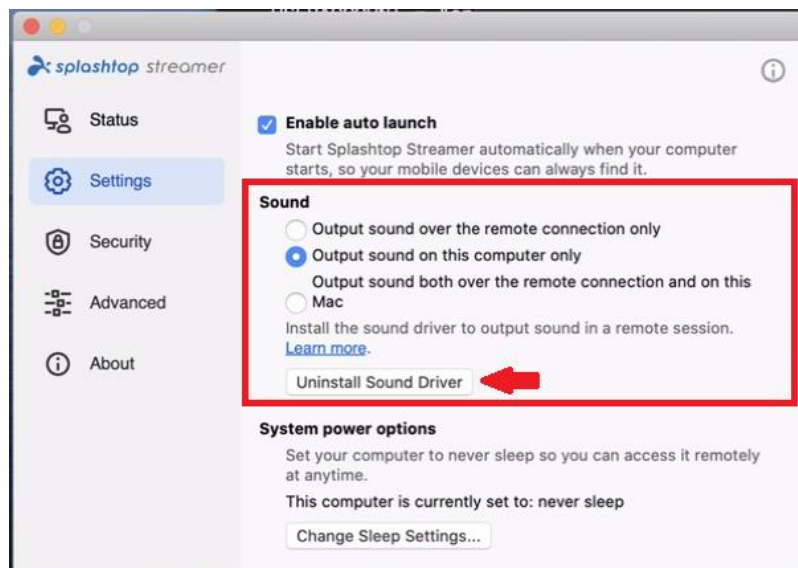
2. MacOS Additional Requirements

If deploying to Mac computers, note these additional requirements and setup instructions:

- **Security & Privacy permissions** for macOS [10.15 Catalina/11 Big Sur](#) and newer:



- **Audio:** To enable audio streaming over the remote connection, [install the Splashtop Sound Driver](#) and allow microphone permission for macOS 10.14+. If any apps on the Mac computers use 3rd party sound drivers, such as Avid Pro Tools or Adobe Premiere, some [additional configurations](#) may be required.



3. Single Sign-On (SSO)

Splashtop supports logging into <https://my.splashtop.com> and the Splashtop Business app using the credentials created from your SAML 2.0 identity providers.

If you would like users to use Single Sign-On (SSO), please complete two steps:

1. Create an SSO method for your IDP service in the Splashtop web console:
[How to apply for a new SSO method?](#)
 - a. Detailed instructions on certain IDP services, such as Azure AD, OKTA, ADFS, JumpCloud, OneLogin, can be found here:
[Single Sign-On \(SSO\)](#)
2. Our validation team will reach out to you with instructions to verify your domain access and activate your SSO method.
3. *(Recommended)* Set up **SCIM provisioning** (For [AzureAD](#), [Okta](#), and [JumpCloud](#)) to automatically provision and sync users and groups. This skips the invitation email process (*Section 4, Inviting Users*).
4. *(Recommended)* [Import SSO users by CSV file](#) if you are unable to use SCIM provisioning, to automatically onboard users into specified user groups. This also skips the invitation email process.

[View this article to read the limitations with SSO.](#)

Once your SSO method has been activated, note that you can turn off [Device Authentication](#) for users that are associated with this method. This way, users do not need to click additional email links to authenticate their devices. Simply, uncheck the Device Authentication checkbox for the SSO method under **Management -> Settings (Team owner and Super Admin only)**.

Single Sign On

[New SSO Method](#) [View instructions](#)

SSO Name	IDP Type	Protocol	Status	Device Authentication	
Default Okta	Okta	SAML 2.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	...
Splashtop ADFS	ADFS	SAML 2.0	<input type="checkbox"/>	<input checked="" type="checkbox"/>	...

4. Inviting Users

Invite users by going to **Management -> Users -> Invite Users**. Assign team roles, user groups, and SSO authentication methods during the invitation process or later. You can invite up to 500 email addresses in each invitation window.

Invite Users via Email X

Email

For multiple email addresses, just separate them by commas or enter each on a new line.

Role : Admin v Group : Default Group v

Set as group-specific admin instead of regular admin

*Admins can access all computers by default. Members can not access any computers by default. You can use "Allow Access" or "Assign Group" to change the access permission later.

Authentication method : test method v

Team Roles

- **Owner:** The Owner is the highest level of authority and can perform any functions in Splashtop, including (but not limited to) inviting users, changing roles, viewing anyone's connection history, managing computers, changing access permissions and changing team settings. The team Owner is the only user who has access to the team subscription/payment info.
 - There is only one Owner, and status cannot be transferred between user accounts.

- **Admin:** The Admin role has the same permissions as the Owner above, except they cannot access subscription/payment info, the Team Settings tab, and cannot change users' roles.
 - [Super Admin](#): The Super Admin is an elevated role above Admin, who can have the same permissions as the Owner above, including accessing the Team Settings tab and changing users' roles. They cannot access subscription/payment info.
 - [Group Admin](#): Group admin is a limited Admin role that gives a user admin privilege over specific user and/or computer groups. This allows them to add/remove users & computers only for the groups that are authorized.
 - Admins & Group Admins have access to use remote management features (Remote command, system inventory, etc.) if you have purchased **Technician licenses** of Splashtop Enterprise. The ability to delegate specific users access to these features (regardless of team role) is coming soon.

- **Member:** Members are general users who have been added to the team to allow remote access. They only have access to computers that they are granted permission for, and can check their own status, account info, team info, and logs. They can remove themselves ("quit") from a team in the Account Summary tab.

5. Grouping

With Splashtop, you can group your users and computers for easier management and access permission control. Each user or computer can only belong to one group. However, users can have access to multiple computer groups. Get started by going to **Management -> Grouping**.

Create Group

Group Name

You can separate multiple groups by adding each one on a new line.
The name cannot contain these special characters <>;"*+=\|?

user group

computer group

Set this group as connection pool

You can create 3 types of groups:

1. User-only group
2. Computer-only group
3. User & Computer group

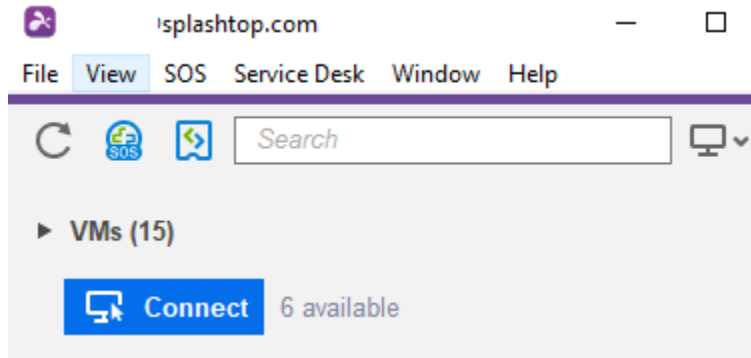
A **user-only group** can only consist of users. Grouping users is useful for setting access permissions for multiple users at a time. It is also useful for automatically applying access permissions to a new user.

A **computer-only group** can only consist of computers. Grouping computers helps to organize a large computer list for easier navigation. It can also make assigning access permissions easier – you can grant a user access to an entire group of computers.

A **user & computer group** is a shortcut for group-based access control. It can consist of both users and computers. By default, all users in this group can access all computers in this group.

Connection Pool

Set this group as a connection pool will enable the Connection Pool feature for the computer group. Users can click the “Connect” button to connect to any available computer in the group. This is useful for scenarios such as RDP pools, computer labs, and more where it doesn’t matter which computer the user connects to.



Connection Pools can also be enabled for specific sets of computers outside of computer group assignments. See Section 7, Scheduled Access.

Adding Users or Computers to a Group

From **Management -> Grouping**, use the gear icon to the right of the group to assign users or computers. Multiple users or computers can be added at a time. You can also assign a Group Admin.

From **Management -> All Computers**, use the gear icon to the right of each computer to assign that computer to a group.

From **Management -> Users**, use the gear icon to the right of each user to assign the user to a group. You can also select a user's group when sending an invitation.

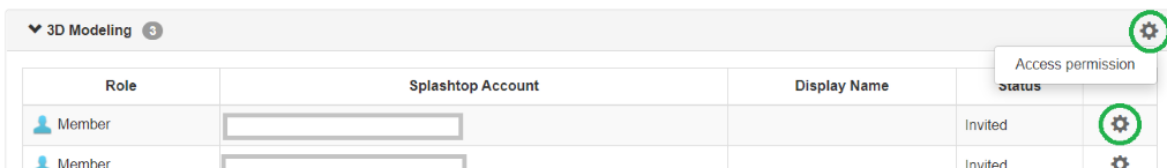
6. Access Permissions

Access permissions determine which computers a user will have access to. They can be configured by the team Owner or Admins under **Management -> Users**.

Note:

- Access permissions will grant a user persistent access to computers, regardless of time of day. To only grant access for a particular timeslot, see *Section 7, Scheduled Access*.

You can set access permissions for a single user or a group of users. Click on the gear icon to the right of a user or user group and choose **Access Permission**.



By default, when a user is invited,

- Admins have access to All Computers
- Members have access to No Computers if they are not invited into a group
- Members have access based on the group's permission when assigned or invited to a group

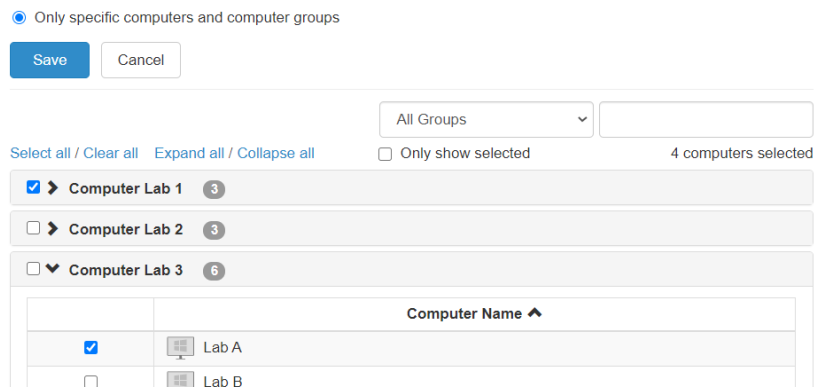
User access permission (@gmail.com)
Admins can grant users/user groups access to computers/computer groups.

All computers No computers

Only computers in its group Only computers based on group permissions

Only specific computers and computer groups

To give a user or user group access to multiple computers or computer groups, select “Only specific computers and computer groups”.



7. Scheduled Access

Scheduled Access allows admins to schedule users, groups, and computers for remote access on a time-slot basis. The team **Owner, Admins, and Group Admins** have access to the scheduling module.

Notes:

- Scheduled Access is granted in addition to existing user/group access permissions that are set under *Management -> Users* – they do NOT override existing user/group access permissions.
- For users who only need scheduled remote access, set their access permission under *Management -> Users* to “No Computers”.


Scheduled Access Configuration

1. Before creating any new schedules, go to **Management -> Settings** to configure the Scheduled Access time zone. **The time zone cannot be changed when a schedule is in place.** Only the team Owner or super admin has access to this setting.

Scheduled Access

Time zone setting (GMT-08:00) Pacific Time (US & Canada) ▾

2. Go to **Management -> Scheduled Access** and click on **Create Resource**.



Create your first Resource

Scheduled Access allow you to manage users' access within a certain time period.

[Create Resource](#)

3. Enter the Resource **Name** and **Description** (*optional*). The Resource contains the set of computers that will be scheduled for access.

Create Resource

1 — 2 — 3
General Computers Group Admin

Resource Name

Description (*optional*)

[Advanced Settings](#) ▾

4. Click **Advanced Settings** if you would like to enable [Connection Pool](#) or [Exclusive Access](#) on this Resource. This will be the default template for the settings on each schedule that you create.
 - Connection Pool allows your users to connect to any available computer in the resource. This is useful for cases where it doesn't matter which computer the user connects to.
 - Exclusive access prevents a remote user from accessing a computer if there is already an OS user logged into the computer. This is useful for scenarios where there may be users working locally at the computer. You can also enforce additional features such as blank screen, lock keyboard & mouse, and logout after disconnect for remote sessions that follow the schedule.

[Advanced Settings](#) ▲

- Support connection pool for schedules.
Windows Streamer v3.4.6.0 only
- Support exclusive (remote or local) access for member accounts.

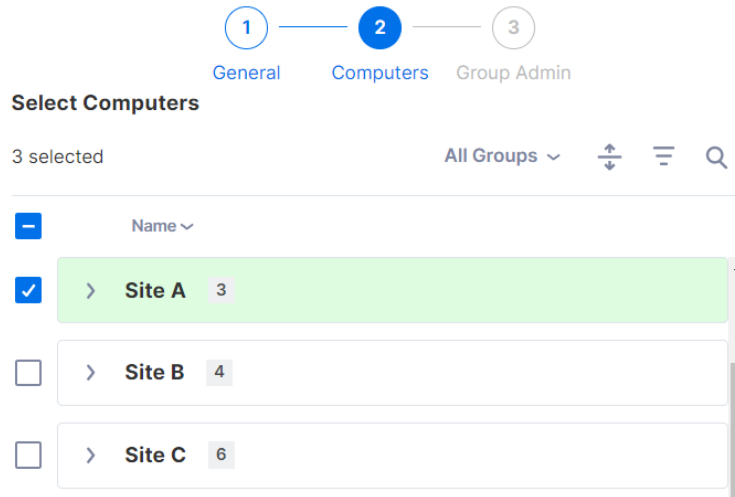
Set as Default for Schedules

- Set the schedule as connection pool.
- Prevent member from accessing a computer which has already been logged in.
- Allow access to a computer with a logged in user, if idle for more than: **10 minutes** ▾
- Blank screen and lock keyboard/mouse when in a session.
- Log out user on a disconnect: **Immediately** ▾
- Lock screen before user logout for unintentional disconnects: **1 minute** ▾

"Log out user on a disconnect" and "Lock screen before user logout..." requires Splashtop Streamer v3.4.4.0 or later.

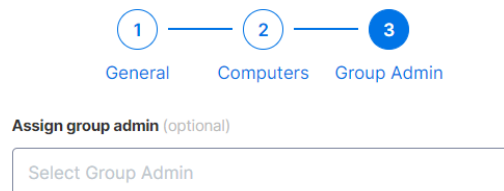
5. Select the computers and/or groups that you would like to make available in the Resource.

Create Resource

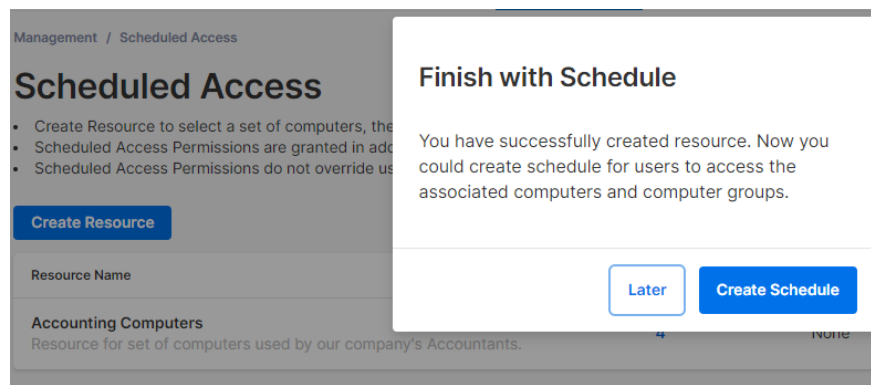


6. (Optional) Assign [Group Admin](#)(s) to help with managing schedules on this Resource. Group Admins can view any Resource that they are assigned to, and can also create new Resources and Schedules.

Create Resource



7. Continue to **Create Schedule**, or later click on the Resource name to assign schedules.



8. Create a Schedule for the Resource by filling in the **Name**, **Starting Date**, and **Recurrence**.

Edit Schedule

Schedule Name

Description (optional)

Accountant accesses computer to review the past week's expenses every Monday

Time

The time zone is in **GMT -08:00 (Pacific Time (US & Canada))**.

-

Repeat

Weekly

Sun **Mon** Tue Wed Thu Fri Sat

Repeat Ends (optional)

Connections

Force session to disconnect when Schedule ends.

Notify users before session ends:

[Advanced Settings](#)

Exclusive access (remote and local) management

Prevent member from accessing a computer which has already been logged in.

Allow access to a computer with a logged in user,

Associate User Groups (max: 250)

Accounting 1 X

Select Group

Associate Users (max: 1000)

Please fill in your users' email addresses

@splashtop.com X

Add User


Assign group admin (optional)

Select Group Admin

- Select user groups and/or specific users to access the Schedule. You may also copy/paste a list of user emails into the Users box.
- The time drop-down selection is in 30-minute intervals, but you can type in any value granular to a minute.
- You can select multiple days in a weekly recurrence.
- Check **Force session to disconnect when Schedule ends** if you would like sessions to forcefully disconnect at the end of the timeslot.
Note: This does not automatically log out of the computer's OS user account.
- Click **Advanced Settings** to manage the Connection Pool and Exclusive access settings if they are enabled in the Resource. These options are only available if they are enabled within the Resource.

Managing Resources & Schedules

Click on the menu to the right of each Resource to view management options.

Resource Name	Computers	Owned by Group Admin	
Accounting Computers Resource for set of computers used by our company's Accountants.	4	None	

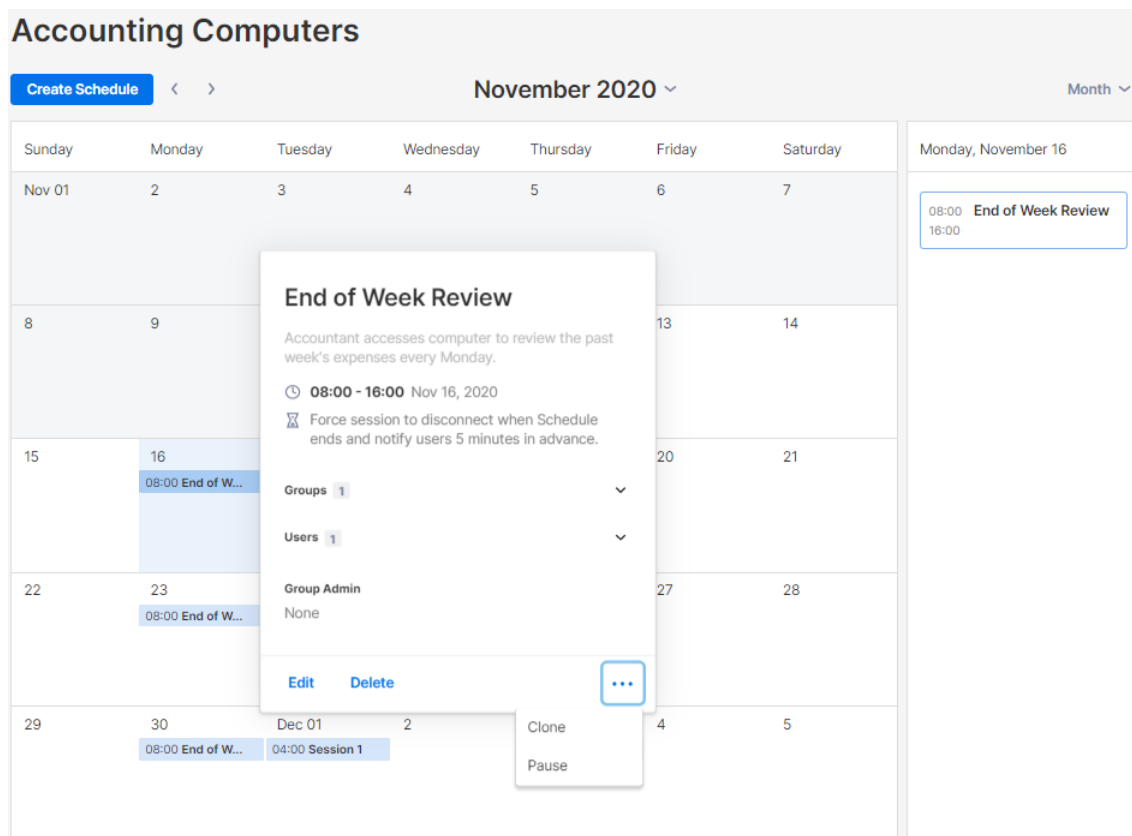
Manage Schedule

Edit

Delete

- **Manage Schedule** to get to the Resource's calendar view.
- **Edit** to change configurations of the Resource.
- **Delete** to remove the Resource.

Click on a Schedule in the calendar view to manage schedule functions.



Accounting Computers

Create Schedule < > November 2020 Month

Sunday Monday Tuesday Wednesday Thursday Friday Saturday

Nov 01 2 3 4 5 6 7

8 9 13 14

15 16 20 21

22 23 27 28

29 30 Dec 01 2 4 5

Monday, November 16

08:00 End of Week Review
16:00

End of Week Review

Accountant accesses computer to review the past week's expenses every Monday.

🕒 08:00 - 16:00 Nov 16, 2020

⚠ Force session to disconnect when Schedule ends and notify users 5 minutes in advance.

Groups 1

Users 1

Group Admin
None

Edit Delete

⋮

Clone

Pause

- **Edit** to change configurations of the schedule.
- **Delete** to remove all recurrences of a schedule.
- **Clone** to easily create a new schedule with similar configurations.
- **Pause/Resume** the recurrence of a Schedule. (ex: holidays, maintenance)

If a Group Admin is removed, what happens to their owned Resource/Schedules?

If a Group Admin is removed from the team or has their admin privileges revoked, their owned Resources will become "Inactive".

Resource Name	Computers	Owned by Group Admin
Inactive Accounting Computers <small>Resource for set of computers used by our company's Accountants.</small>	4	None

1. To re-activate a Resource, click the menu to the right of the **Resource** -> **Edit**.

Resource Name	Computers	Owned by Group Admin
Inactive Accounting Computers <small>Resource for set of computers used by our company's Accountants.</small>	4	None

Manage Schedule
Edit
Delete

2. Toggle the **Status** of the Resource from **Inactive** -> **Active**.

Edit Resource

Resource status: Inactive ?



Resource Name

Accounting Computers

Description (optional)

Resource for set of computers used by our company's Accountants.

Status

Inactive

If a Resource is owned by multiple Group Admins, the Resource will not become inactive unless all Group Admins are removed.

8. Team Settings

Go to **Management -> Settings** to review and configure Team Settings. Team Settings control important policies for your team, such as feature capabilities and authentication. This page is only accessible by the **Team Owner and Super Admin**.

Overview of Team Settings

[You can view full details in this article.](#)

Settings

- Account Summary
- Team**
- API
- Subscriptions
- Payment and Billing
- Payment History
- Redeem Code

General [Go back to classic settings page](#)

Team Name
Demo Team

Current plan
Splashtop Enterprise
5 concurrent technician(s) and 10 end user(s)

Computers
40 of 1600 computers deployed

Feature Configuration

	Default Granular Settings		
	Admin	Configurable	Member
Remote control	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Attended Access	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
File transfer	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Remote print	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Team Name: This is the name users will see in their team invitation and account info. The team name is also displayed on the Status tab of deployed Splashtop Streamers.

Computers: The number of Streamers deployed of the max total.

Feature Configuration

These checkboxes control the team's feature capabilities. Most have a global on/off toggle, and some can be granularly enabled by user or user group (See Section 9, Granular Controls).

Feature Configuration

		Default Granular Settings		
		Admin	Configurable	Member
Remote control		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Attended Access		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
File transfer	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Remote print	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Device redirection Detailed setup	<input checked="" type="checkbox"/>			
Redirect microphone input	<input checked="" type="checkbox"/>			
Copy & paste	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Paste clipboard as keystrokes	<input checked="" type="checkbox"/>			
Remote wake	<input checked="" type="checkbox"/>			
Remote reboot	<input checked="" type="checkbox"/>			
Saving in-session chat transcript to session logs Learn more	<input checked="" type="checkbox"/>			
Chat (pre-session)	<input checked="" type="checkbox"/>			
Saving pre-session chat transcript to session logs Learn more	<input checked="" type="checkbox"/>			
Remote command	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
RDP computer	<input checked="" type="checkbox"/>			
Background Actions For Admins and owner	<input checked="" type="checkbox"/>			
1-to-Many Scripting for Admins and owner	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

Additionally, some features can also be set between unattended and attended access (technician license).

Unattended Access

		Default Granular Settings		
		Admin	Configurable	Member
In-session voice call	<input checked="" type="checkbox"/>			
Session recording Detailed setup	<input checked="" type="checkbox"/> Local recording			
Share my desktop	<input checked="" type="checkbox"/>			
Concurrent remote sessions	<input checked="" type="checkbox"/>			
Web App (Connect to remote computers with browsers)	<input checked="" type="checkbox"/>			
Session indicator	Remote session File transfer Remote command Background Actions			
Display type				<input type="checkbox"/> Pop-up

Attended Access

In-session voice call	<input checked="" type="checkbox"/>
Session recording Detailed setup	<input checked="" type="checkbox"/> Local recording
Share my desktop	<input checked="" type="checkbox"/>
Concurrent remote sessions	<input checked="" type="checkbox"/>
Web App (Connect to remote computers with browsers)	<input checked="" type="checkbox"/>
Session indicator	
Display type	<input type="checkbox"/> Banner
Allow user to close the banner	<input checked="" type="checkbox"/>

User Configuration

These features can be helpful for limiting certain functionality by user role.

User Configuration	
Group-specific admin role Learn more	<input checked="" type="checkbox"/>
Allow members to connect to computers in an active connection	<input type="checkbox"/>
Allow members to establish concurrent sessions	<input type="checkbox"/>
Allow members to disconnect others' sessions	<input type="checkbox"/>
Allow members to reboot computers and restart streamers	<input type="checkbox"/>
Allow members to access the Management tab	<input checked="" type="checkbox"/>
Allow members to see groups	<input checked="" type="checkbox"/>
Allow users to establish remote sessions from multiple devices ?	<input type="checkbox"/>
Member's permission for Computer Notes ?	Cannot edit and view v

- Allow members to connect to computers in an active connection (2 users to 1 computer)
- Allow members to establish concurrent sessions (connect to more than 1 computer)
- Allow members to disconnect others' sessions
- Allow members to reboot computers and restart streamers
- Allow members to access the Management tab (view-only)
- Allow members to see groups (Only group names of computers they have access to)
- Allow users to establish remote sessions from multiple devices
- Allow members to read/write computer notes

Security

Manage security-related settings such as two-step verification, device authentication, SSO, and more.

Security	Default Granular Settings		
	Admin	Configurable ?	Member
Two-Step Verification			
Manage trusted devices			
Allow users to trust devices for Forever v	<input checked="" type="checkbox"/>		
Require users to use two-step verification	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Disable device authentication when two-step verification is turned on	<input checked="" type="checkbox"/>		
Device Authentication			
	Application	Browser	
Email device authentication link to	Person logging in v	Person logging in v	
Allow devices to stay authenticated for	Forever v	Forever v	
Allow users to remember login	On v ?		
Log out idle users after	24 hours v ?	Never v ?	

9. Granular Controls




With Granular Controls, you can enable or disable certain features for specific users or groups.

Granular Controls are currently available for:

- File Transfer
- Copy & Paste
- Two-step Verification
- Remote Control
- Remote Print
- Attended Access (Technician license)
- 1-to-Many Scripting (Technician License)
- Remote Command Prompt

From **Management -> Settings**, you can set the **Default Granular Settings** of these features per user role. These default settings will be applied when a new user is invited to the team's default group or if a user/group's granular control setting is set to follow the default. The **Admin Configurable** setting can be checked if you would also like to allow Admins to help with configuring the granular controls.

Feature Configuration

		Default Granular Settings		
		Admin	Configurable 	Member
Remote control		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Attended Access		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
File transfer	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Remote print	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Device redirection Detailed setup	<input checked="" type="checkbox"/>			
Redirect microphone input	<input checked="" type="checkbox"/>			
Copy & paste	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Paste clipboard as keystrokes	<input checked="" type="checkbox"/>			
Remote wake	<input checked="" type="checkbox"/>			
Remote reboot	<input checked="" type="checkbox"/>			
Saving in-session chat transcript to session logs Learn more	<input checked="" type="checkbox"/>			
Chat (pre-session)	<input checked="" type="checkbox"/>			
Saving pre-session chat transcript to session logs Learn more	<input checked="" type="checkbox"/>			
Remote command	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
RDP computer	<input checked="" type="checkbox"/>			
Background Actions For Admins and owner 	<input checked="" type="checkbox"/>			
1-to-Many Scripting for Admins and owner 	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

Under **Management -> Users**, you can configure the granular control per user or user group. To configure the granular -> control settings for a user group, click the group's gear icon -> Granular Control.

Role	Splashtop Account	Display Name	Status	2FA Status	Granular Controls	Last Session
Member	email@splashtop.com	Example User	Enabled	⊗	⚙️	

To configure per individual user, click on each feature icon to enable/disable or click the user's gear icon -> Granular Control.

Granular Controls	Last Session	Last Login
⚙️		

Granular control X

Status

Attended access On ▾

File transfer Off ▾

Remote print Default ▾

Copy paste Default ▾

Require two-step verification On ▾

Command Prompt Default ▾

Remote Control Default ▾

- On: Enable this feature for the user.
- Off: Disable this feature for the user.
- Follow Group: Apply the user group's setting for the user.
- Default: Apply the team's default setting per the user's role from the Team's Default Granular Settings.

10. Endpoint Management (Technicians)

Technician licenses include features to remotely manage computers with the ability to view Windows event logs, system/hardware/software inventory, endpoint security, and manage Windows Updates and configurable alerts. You can also send commands to an unattended remote computer's command prompt in the background. All features described are available for the **Team Owner and Admins** unless otherwise specified.

Windows Event Logs

View an online computer's Windows Event Logs from within the Splashtop web console. You can filter by event level, type, date range, and ID.

View event logs:

Event level: Critical Error Warning Information

Event type: System Application Security Setup

From: 2020-11-11 00 : 00 to 2020-11-11 23 : 59

Include detailed information: Yes No

Event ID filter:

[Retrieve](#)

[View this article for more details and instructions.](#)

Computer Inventory – System, Hardware, Software

View and compare snapshots of a computer's System, Hardware, or Software inventory. This view is available per individual computer. You can also export the inventory of all computers by clicking the **Export** option at the bottom of the **Management -> All Computers** page, or view all at **Management -> Inventory**.

View the system inventory of Test:

View the snapshots for 2020-11-11

Compare snapshots 2020-11-01 and 2020-11-11

View changelog from to

The snapshot for 2020-11-11 was uploaded on 2020-11-11 03:29:11 -0800. ([Refresh today's inventory](#))

[Apply](#)

Software

	2020-11-01	2020-11-11
Software 1	Name: Adobe Acrobat Reader DC Vendor: Adobe Systems Incorporated * Version: 20.012.20048 * Size: 320.68 MB	Name: Adobe Acrobat Reader DC Vendor: Adobe Systems Incorporated * Version: 20.013.20064 * Size: 320.62 MB

[View this article for more details and instructions.](#)

Endpoint Security

View the endpoint security status for Windows computers at **Management -> Endpoint Security** to make sure all machines are protected. You can also purchase additional licensing for [Splashtop Antivirus powered Bitdefender](#) to enable installing and scanning directly from the Splashtop web console. **The Endpoint Security dashboard is available to the Team Owner, Admins, and Group Admins.**

Computer View
All Groups

Status	Computer Name	Group	Software	Protection	Last scan time	Threats	Details
<input type="checkbox"/>	Test	Megan's Computers	Bitdefender Endpoint Security Tools Antimalware	Enabled	2020-11-10 20:00:00	42	

Scan task: N/A

[Acknowledge all threats](#)

Threat Name	Detected Timestamp	Object Name	Action	Acknowledged
Gen:Illusion.ML.Skyline.B.2010101	2020-11-06 14:00:00 -0800	C:\Users\ [REDACTED]		Acknowledge
Gen:Illusion.ML.Skyline.B.2010101	2020-11-06	C:\Users\ [REDACTED]		Acknowledge

[View this article for more details and instructions on Bitdefender.](#)

Windows Updates

Check a computer's Windows Updates status at **Management -> Windows Updates**. Click **Details** to check for, view, and push available updates immediately or at a scheduled time for a specific computer.

1 selected
Computer View
All Groups

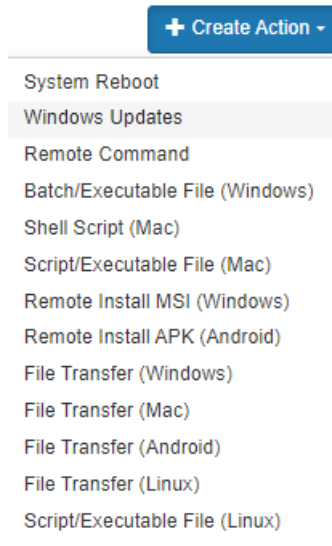
Group Name	OS	Update Status	Important	Optional	Update Policy	Last Update Time	Details
Data	Microsoft Windows Server 2012 R2 Standard 64-bit (6.3.9600)		4	0	Download updates but let me choose whether to install them	2023-10-12 14:59:23 (UTC-07:00)	

Available updates: 4 important, 0 optional Include updates for other Microsoft products (Last checked for updates: 2023-11-03 04:09:09)

Code	Important	Reboot	Size	Update
<input type="checkbox"/> 5022733	Yes	Yes	55 MB	2023-02 Security and Quality Rollup for .NET Framework 3.5, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows Server 2012 R2 for x64 (KB5022733) - A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.
<input type="checkbox"/> 5025285	Yes	Yes	571 MB	2023-04 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems (KB5025285) - A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.
<input type="checkbox"/> 5030329	Yes	No	10 MB	2023-09 Servicing Stack Update for Windows Server 2012 R2 for x64-based Systems (KB5030329) - Install this update to resolve issues in Windows. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article for more information. After you install this item, you may have to restart your computer.
<input type="checkbox"/> 5000000	Yes	Yes	50 MB	Windows Malicious Software Removal Tool x64 - x64 (KB5000000) - After the download, this tool runs on your time to check your

1-to-Many Actions & Schedules

Create a 1-to-Many Action that allows you to immediately run or schedule a task to multiple computers or computer groups. Configure a system reboot, Windows update, or silently deploy .EXE,.MSI,.PKG files and more. This can be configured under **Management -> 1-to-Many Actions** or **1-to-Many Schedules**.

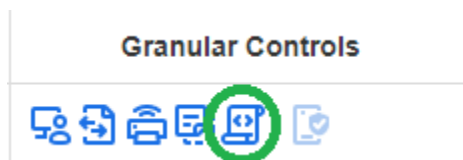


Actions that are set to run immediately can only be run on Online computers. If a computer is offline when a Schedule Action is attempted, there is currently no retry mechanism.

1-to-many can be available for only the Team Owner, or Team Owner and Admins, depending on the option selected under **Management -> Settings**.



Additionally, permission can be configured via Granular controls.



[View this article for more details and instructions.](#)

Configurable Alerts & Smart Actions

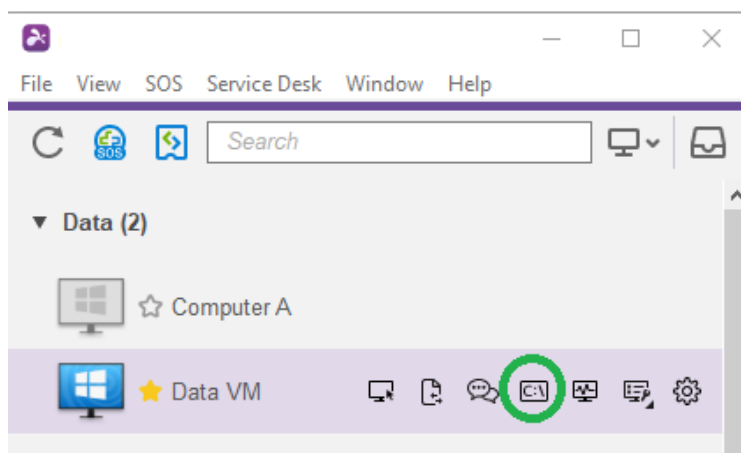
Set up configurable alerts under **Management -> Alert Profiles** to get notified when certain actions occur. Actions vary from software installed/uninstalled, CPU/disk utilization, computer online/offline, and more. Configure a smart action to execute once an alert is triggered.

The screenshot shows the configuration page for an alert profile named "Computer Online/Offline" (Enabled). The "Smart Action Enabled OS" is set to "Windows". The selected alert is "CPU Utilization (Enabled)". The name is "CPU Utilization" and the type is "CPU Utilization". The description states: "Use this alert to monitor processor utilization. An alert is triggered when the usage is over or equal to the threshold for the specified duration." The configuration is set to alert when the average CPU utilization is greater than or equal to 80% for 10 minutes. The "Also notify via email" section has "alert" checked, and "Also attach the connection link in the email" is also checked. The "Action kind" is "System Reboot" and the "Select action" is "Reboot". A dropdown menu on the right lists various alert types: CPU Utilization, Memory Usage, Disk Space, Computer Online, Computer Offline, Software Installed, Software Uninstalled, Hardware Added, Hardware Removed, Windows Update, Available Updates, and Windows Event Log.

[View this article for more details and instructions.](#)

Remote Command

From the [Business App](#), click on a computer's Remote Command icon to send command line or terminal commands to a remote Windows or Mac computer in the background.

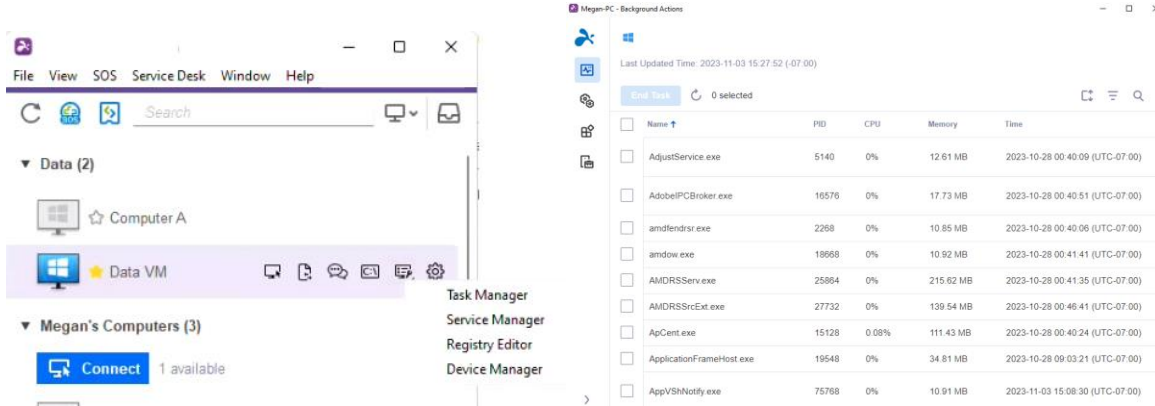


This feature is available for all users of the team if enabled, and requires the user to enter admin credentials of the remote computer to access.

[View this article for more details and instructions.](#)

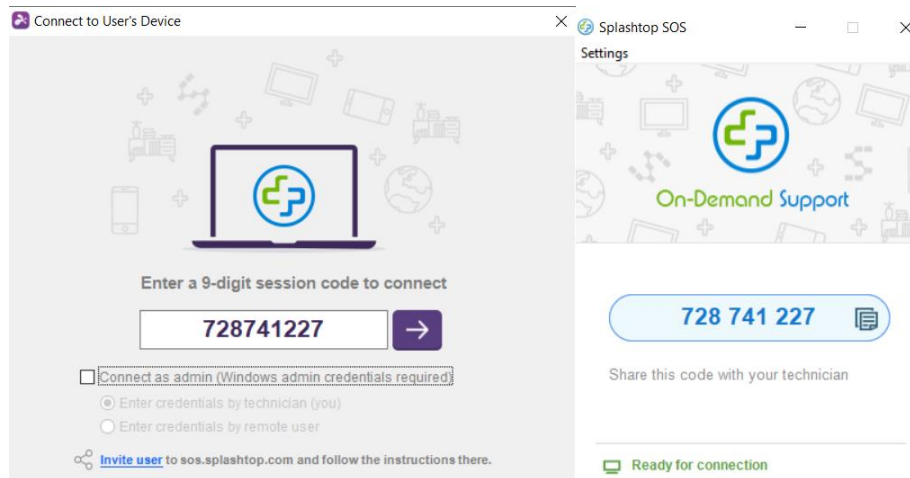
System Tools (Background Actions)

Access system tools such as Registry Editor, Device Manager, Service Manager, and Task Manager without having to start a remote session to the computer.



11. Attended Access - SOS (Technicians)

Technician licenses enable Attended Access with Splashtop SOS. Use Splashtop SOS to access Windows, Mac, iOS, Android, and Chromebook devices with a 9-digit session code.



To connect, enter the 9-digit session code generated by the end user who runs the Splashtop SOS app. [See the tutorial here.](#)

Additional Features:

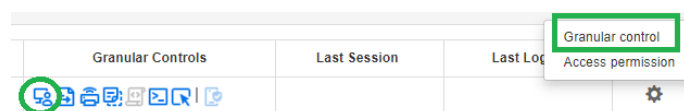
- [Connecting with Admin privileges](#)
- [Switching OS Users](#)
- [Reboot-and-Reconnect](#)
- [Custom Brand SOS](#)
- [ITSM/Helpdesk Integrations](#) (ServiceNow, Freshservice, Freshdesk, Zendesk, Jira, and more coming soon)

Granular Settings

Configure who can use Attended Access with Granular Settings. The Team Owner can configure the default Attended Access permission per user role under **Management -> Settings**. This determines a user's default Attended Access permission when they are invited to the team.

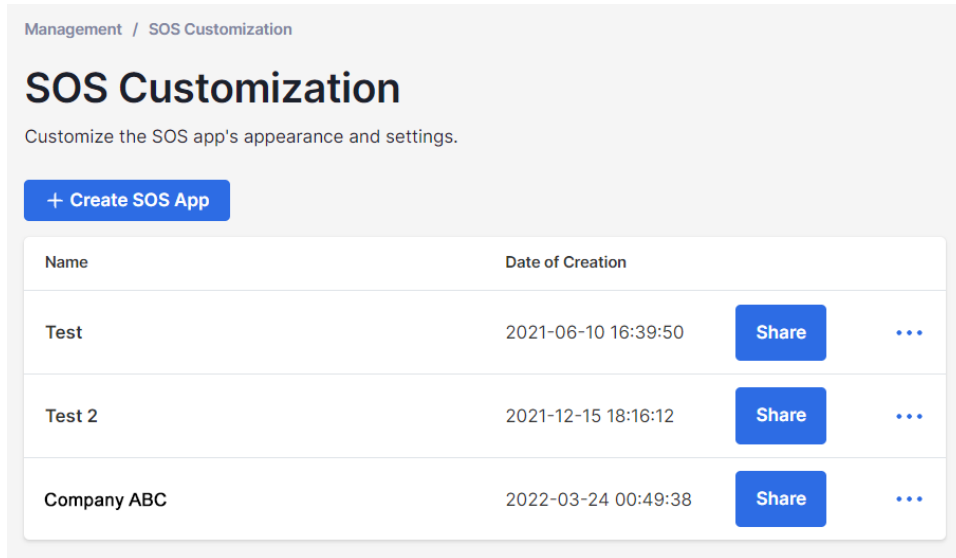
Attended Access	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
-----------------	-------------------------------------	--------------------------	--------------------------

Under **Management -> Users**, you can also configure the Attended Access permission per individual user or user group.



12. SOS Customization (Technicians)

[Custom branding](#) is available for the Splashtop SOS app. To create a custom app, go to **Management -> SOS Customization -> Create SOS App**.



Customize different areas such as the app name, colors and descriptions. You can also create a disclaimer and configure additional settings such as audio and proxy.

Theme

SOS Theme | Service Desk Theme

Icon (Windows only, image size max 2 MB, format: ICO)

Caption (max 20 characters)

Banner (image size 320 x 160, max 2 MB, format: JPG/PNG/GIF)

Background Color

9-digit Section

Instruction Text (max 80 characters)

The preview shows a window titled 'This is a custom app' with a 'Settings' header. It features a blue banner with the text 'Your Company Banner', a green rounded box containing the number '123 456 789' and a copy icon, a description field with the placeholder 'Put your description here', and a status bar at the bottom that says 'Connecting to Splashtop servers...'.

13. Service Desk (Technicians)

[Service Desk](#) provides an interface for technicians to manage a queue of attended sessions and enhance their team's workflow. Instead of waiting for the end user to provide the 9-digit SOS code, technicians can send a customized app link and add them to a queue. **Requires Technician license.**

To enter Service Desk, click the Service Desk in my.splashtop.com or the icon in the Business App.

The screenshot shows the Splashtop Service Desk interface for Company ABC. The top navigation bar includes 'Computers', 'Devices', 'Logs', 'Management', and 'Service Desk' (circled in green). The main content area displays a 'New Session' button and a table of sessions. The table has columns for Name, Status, and Time. The sessions listed are:

Name	Status	Time
John	Waiting	2022-04-06 05:16:28
Steven	Active	2022-03-25 17:59:16
Kai	Active	2022-04-05 18:35:16

Below the main interface, a separate window titled 'Splashtop Service Desk' is shown. It features a menu bar with 'File', 'View', 'SOS', 'Service Desk', 'Window', and 'Help'. The 'SOS' icon is circled in green. The main content area of this window shows the same 'New Session' button and a table with columns for Name, Status, Time, Technician, and Device. The sessions listed are:

Name	Status	Time	Technician	Device
Kai	Active	2022-04-05 11:35:16	(You)	M
Steven	Active	2022-03-25 10:59:16	(You)	D
John	Waiting	2022-04-05 22:16:28	(You)	

Channel Management

Go to **Management -> Channels** to manage Service Desk channels. Here, you can assign a custom SOS app, technicians, assign permissions, and enable additional features such as SOS call.

Create Channel

×



Edit Permissions

Technician or Group Name	Channel Manager	Create	Take	Transfer	Comment	Invite	Release	Close	Delete
Megan@splashtop.com	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
IT Team	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

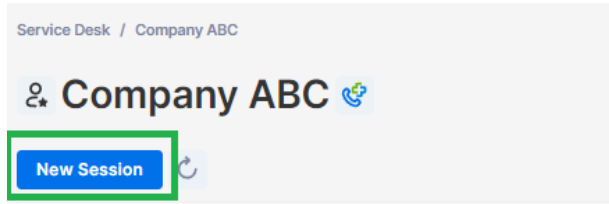
Creating Support Sessions

There are multiple ways to start a Service Desk support session:

Invitation Link or 6-digit PIN Code

Technicians can initiate a support session by creating a session invitation link or 6 digit PIN code.

1. From within the Service Desk console, click **Create Session**.



2. Once the session is created, share the invitation link to the end user, or instruct the user to go to help123.app and enter the 6-digit code.

Share Your Support Session

Link PIN Code

Send the following link to your customer.

Copy Link

This link expires on 2022-08-05 06:53:27

Close

Share Your Support Session

Link PIN Code

Tell your customer to enter the following PIN code at <https://help123.app>

569167

PIN code expires on 2022-09-01 17:54:54

Close

SOS Call

Create an SOS Call app and provide this to end users in advance. Whenever they need support, they can launch the SOS Call app and create a request.

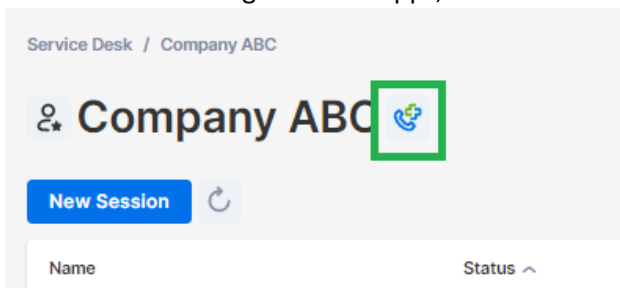
1. In the Channel's settings, make sure SOS Call is enabled.

SOS Call

Technicians can create a SOS Call app and deploy it to end users. End users simply double click on the SOS Call app to create a support request in this channel.

Enable SOS Call

2. To create and manage SOS Call apps, click the icon next to the channel name:



3. Create an SOS Call app. You can configure the name of the downloaded file and also pre-assign a technician to the created sessions.

New SOS Call

The assigned technician requires the SOS Call permission to configure this SOS Call app.

Name

Name of Downloaded File ⓘ

The name cannot contain <>,:;''*+=/|? and space.

Technician

[Cancel](#) [Create](#)

- Copy the download link and send it to your end user. End users can save the link onto their desktop for future use.

Name	Name of Downloaded File	Technician	Date Created
3600 SOS Call	CompanyABC_SOS	Unassigned	2023-08-24 13:28:26
general		Unassigned	2022-05-17 13:47:59

- When an end user is ready to start a support session, they can download and run the SOS Call app to make their request.

Web Support Form

Create a customized webform and embed it onto your support website. End users can start a support session after submitting the form.

- Under **Management -> Channels**, click **Manage web support forms** for the specific channel.

Company ABC	5	Active	Default SOS app packa...	2023-08-24 23:29:42
	0	Active	Default SOS app packa...	2023-11-

2. Create custom fields for the webform. Customer Name and Issue are required.

Custom fields

The screenshot shows a webform configuration interface with three custom fields:

- Customer Name ***: A text input field with the placeholder text "Customer Name".
- Customer Issue ***: A text area with the placeholder text "Describe the issue here.".
- Combo Box**: A dropdown menu with the placeholder text "Add name for this field". Below it, there is an input field with "Add an option" and a "+ Default" button. The dropdown is currently set to "- Select -".

At the bottom of the configuration, there is a "Required" toggle switch (which is turned on), a trash icon, a checkmark icon, and a blue "Submit" button.

3. Embed the code snippet on your website.



Create Successfully!


The screenshot shows a code snippet generation interface with the following settings:

- Form Width**: Input field with "552" and "px" suffix. Below it, "Max: 800 px, Min: 320 px".
- Form Height**: Input field with "480" and "px" suffix. Below it, "Max: 720 px, Min: 480 px".
- iframe**: A text area containing the following code snippet:

```
<iframe width="552" height="480" src="https://help123.app/w/form/h72ek4i" style="padding: 4px 0;border:1px solid #80859F;border-radius:12px;" sandbox="allow-scripts allow-same-origin allow-popups allow-downloads"></iframe>
```
- A blue "Copy Code Snippet" button is located at the bottom.

4. End Users will be prompted to download and run the SOS app once they submit the form. A new session will be created in the Service Desk queue.

✔ **Issue submitted**



Get support on this device

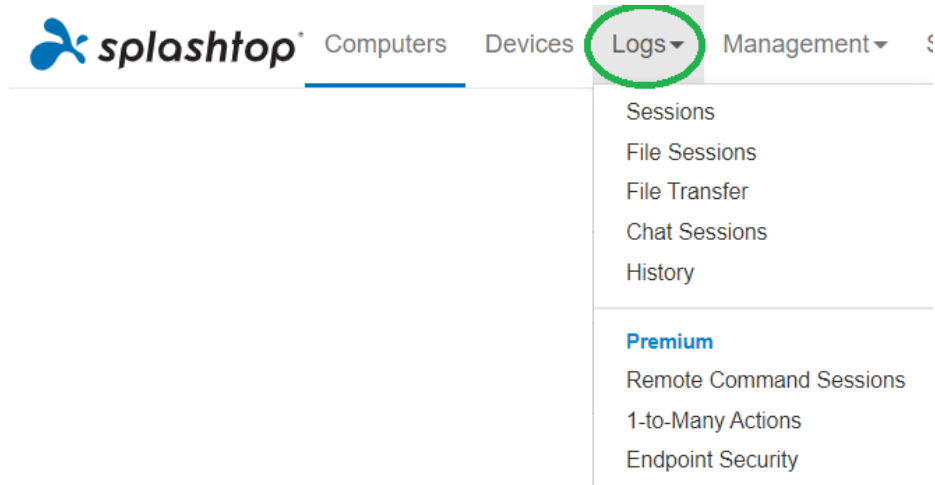
Download Splashtop SOS on the device you wish to be supported. Launch the app and connect with our technician.

[Get the App](#)

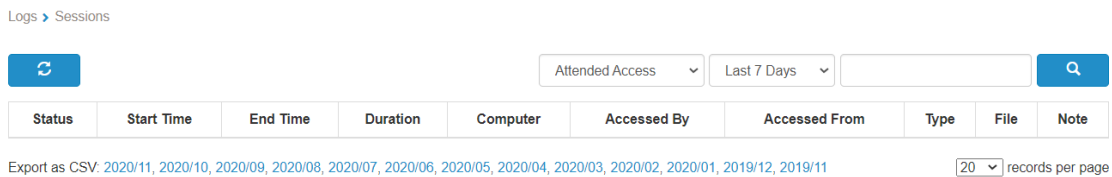
14. Logs

Splashtop maintains logs for self-auditing. The Team Owner and Admins can view logs of everyone in the team. Members will only see their own logs.

To view logs, go to **my.splashtop.com -> Logs**.



Logs include the last 7, 30, or 60 days. If your service includes both unattended and attended access, you can choose which to view. Scroll down to the bottom of the page to **Export to CSV** to download up to a year of past logs.



[View this article for an overview of logs.](#)

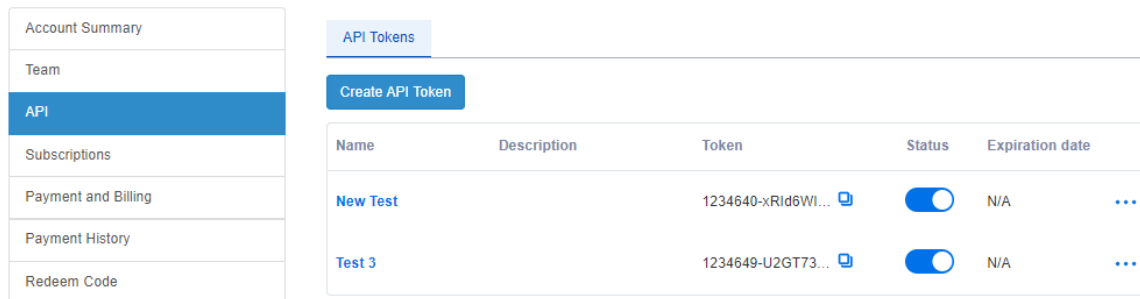
15. Open APIs

RESTful APIs are available for all Splashtop Enterprise teams. APIs help streamline manual workflows and also allow for integrating Splashtop with other 3rd party tools and platforms.



[Click here to view our API Reference.](#)

The Team Owner or Super Admin can create an API token at **Management -> Settings -> API**.

Settings



The screenshot shows the 'Settings' page with a sidebar on the left containing menu items: Account Summary, Team, API (highlighted), Subscriptions, Payment and Billing, Payment History, and Redeem Code. The main content area is titled 'API Tokens' and features a 'Create API Token' button. Below the button is a table with the following data:

Name	Description	Token	Status	Expiration date
New Test		1234640-xRld6WI... 	<input checked="" type="checkbox"/>	N/A
Test 3		1234649-U2GT73... 	<input checked="" type="checkbox"/>	N/A

16. Additional Features

These additional advanced features are available for Splashtop Enterprise.
[Contact Splashtop Sales or Customer Success](#) for additional information.

IP Restriction

Restrict access to the web console <https://my.splashtop.com> or to the Splashtop Business App based on IP address.

Business App IP/Network Whitelist

Only requests from address/network in the list below will be able to access your team.

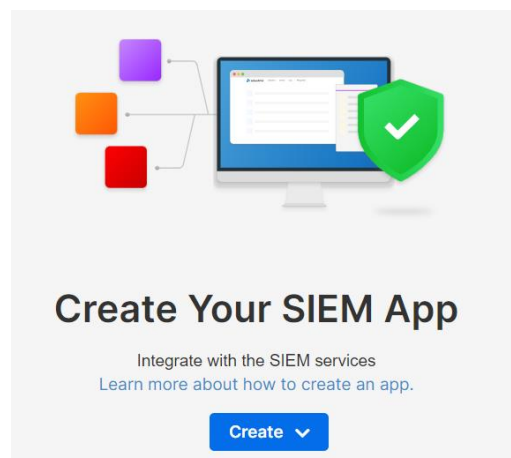
e.g. 168.168.168.168, 168.168.168.0/24



[View this article for more details and instructions.](#)

SIEM Logging

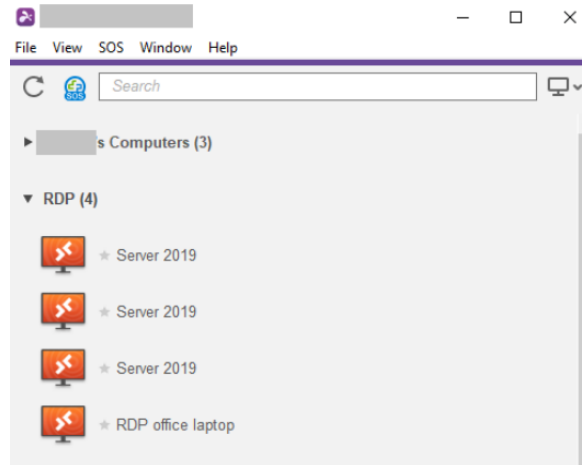
Export Splashtop session and history logs to a SIEM (Security information and event management) software for further analysis.



[View this article for more details and instructions.](#)

Splashtop Connector

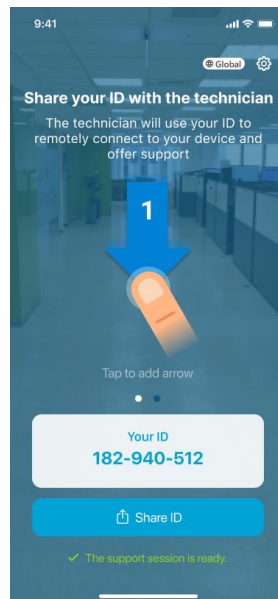
Securely bridge RDP and VNC connections to Windows, Mac, and Linux computers through Splashtop without using VPN or having to install software on each computer.



[View this article for more details and instructions.](#)

Splashtop AR

Connect to off-site locations and resolve issues live with camera sharing and AR annotations.



[View this article for more details and instructions.](#)