



Splashtop Enterprise

Administrator Guide

November 3, 2022

Table of Contents

Change Log - from last 04/20/2022 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
Adding Users or Computers to a Group	14
6. Access Permissions.....	15
7. Scheduled Access	16
Scheduled Access Configuration.....	16
Managing Resources & Schedules	20
If a Group Admin is removed, what happens to their owned Resource/Schedules?	21
8. Team Settings.....	22
Overview of Team Settings	22
9. Granular Controls	24
10. Remote Computer Management (Technicians)	26
Windows Event Logs	26
Computer Inventory – System, Hardware, Software	26
Endpoint Security.....	27
Windows Updates.....	27
1-to-Many Actions & Schedules	28
Configurable Alerts	29
Remote Command	29
11. Attended Access - SOS (Technicians)	30
Granular Settings	30
12. SOS Customization (Technicians).....	31
13. Service Desk (Technicians).....	32

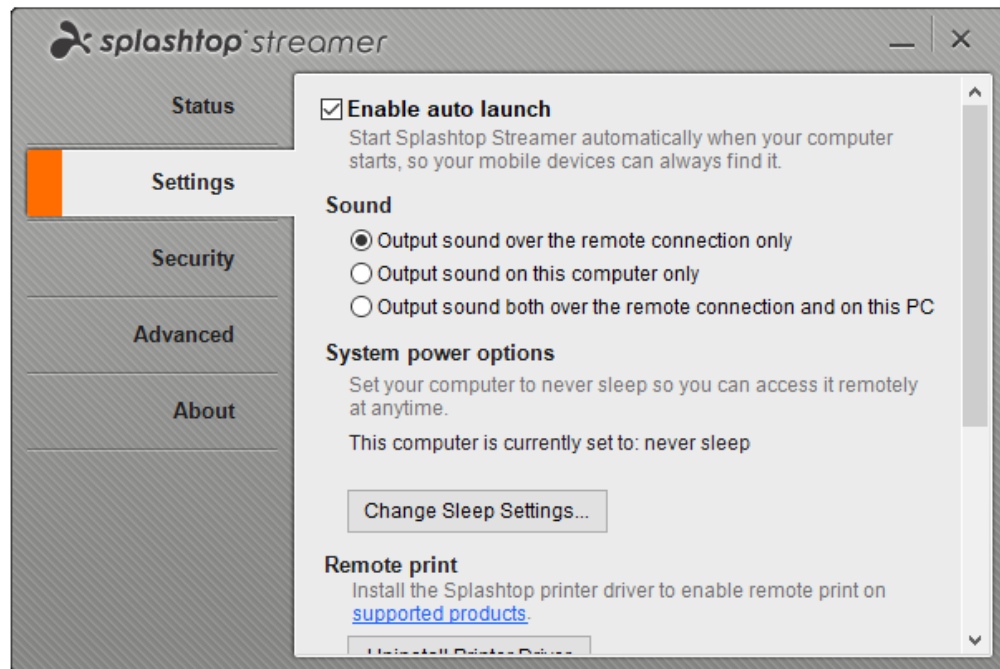
14.	Logs	34
15.	Additional Features	35
	IP Restriction	35
	SIEM Logging	35
	Splashtop Connector	36
	Splashtop AR	36

Change Log - from last 04/20/2022 version

- Deployment, section 1
 - Added Preference Policies, for managing streamer and session settings from the web console
- Inviting Users, Section 4
 - Revised and added information on Super Admins
- Granular Controls, Section 9
 - Added 1-to-many to list of supported granular controls
- Remote Computer Management, Section 10
 - Added information on Inventory dashboard
 - Edit information for 1-to-many. Scripting is now included by default in Technician license
- Service Desk (Technicians), section 13
 - Add mention for 6-digit pin code

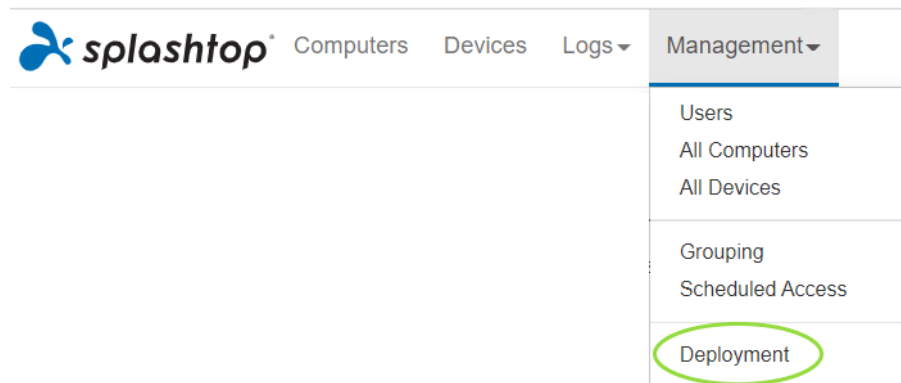
1. Deployment

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**.



2. 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.

3. 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	 Deploy

4. 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

https://my.splashtop.com/team_deployment/download/PY42WJK2WPXS

Try Link

Option 1: Share Link

- 1 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.
- 2 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.

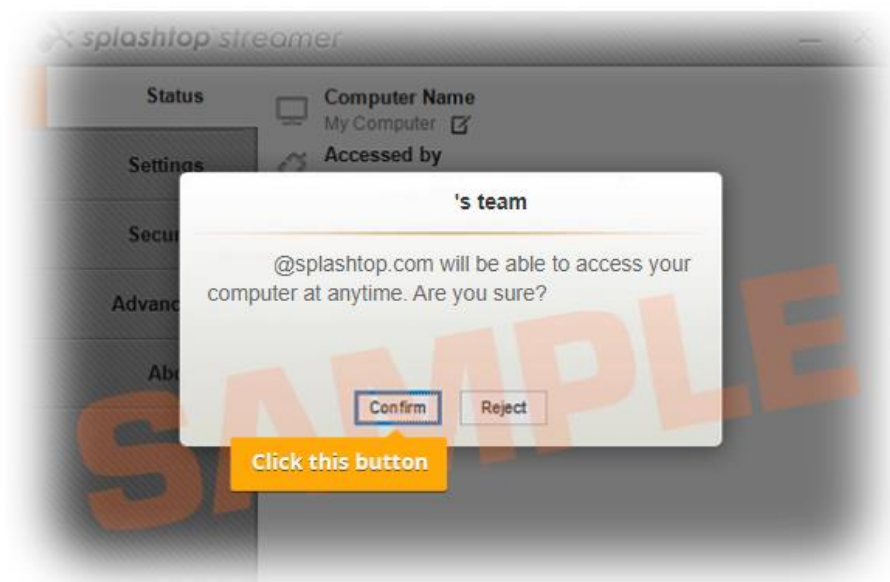
Step 1 : Download the streamer



Also available for  Mac,  Android

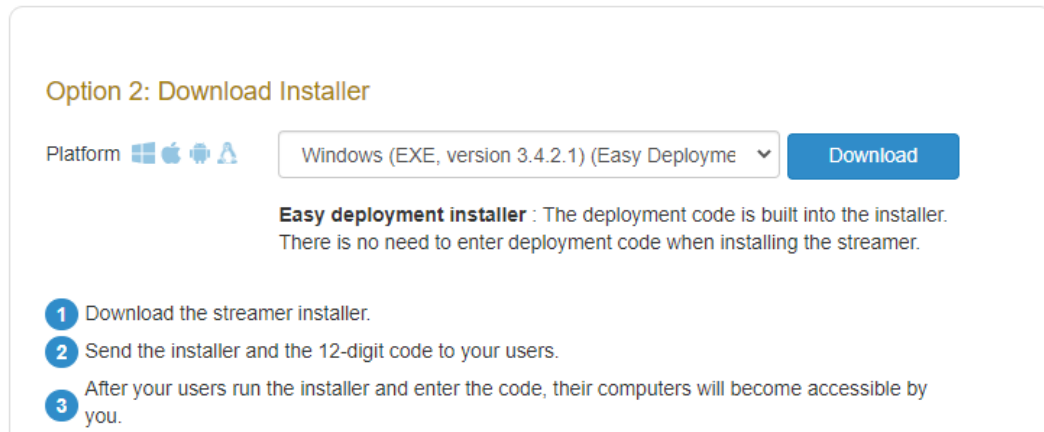
Step 2 : Run the installer and allow access

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.



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](#)
- 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 or manually change the settings directly in the Streamer.
- 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:

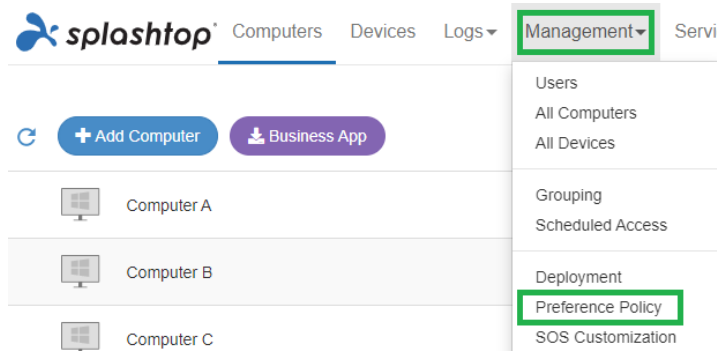
- Manually Update from the web console
- Manually Update from the Streamer -> About -> Check for Updates tab
- Manually Update by running the latest streamer installer
- Silently update using the .EXE, .MSI or .PKG

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

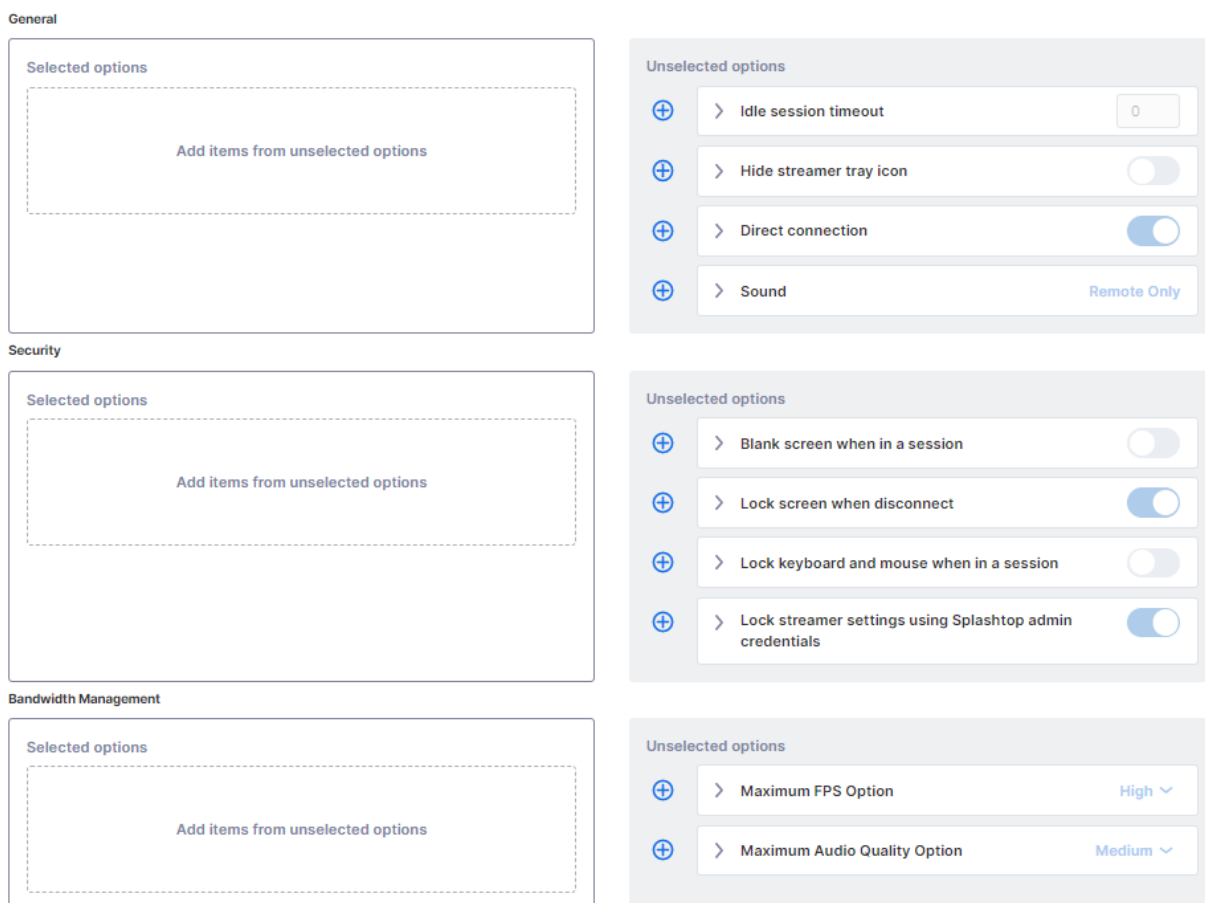
Preference Policies

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 ▾ ≡ 🔍

✓	Computer Name ↑	Streamer Version ⓘ	Group Name	Applied Policy
✓	Windows 11	3.5.2.2	Windows	

4. Assigned computers will be marked by a new icon that indicates that they are part of a policy.

+ Add Computer Business App Computer View ▾ All Groups ▾

Computer Name ⓘ	Group	Streamer Version	IP Address	Notes	Last Online	Last Session	Status	Updates	Alerts	
Windows 11	Windows	3.5.2.2	211.23.144.132		Online	2022-10-18 14:03	✓	✓	0	

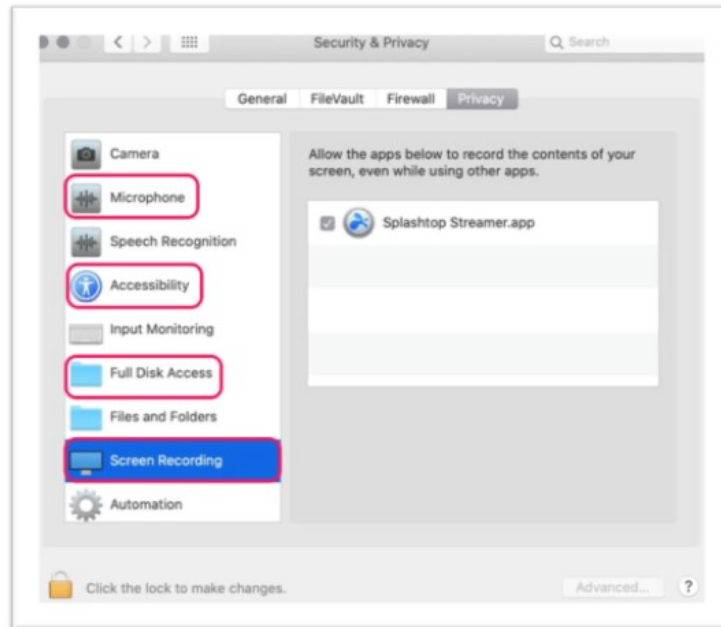
5. When a user connects to a computer that is part of your preference policy, the configured settings or restrictions will apply to the remote session. The user will not be able to reconfigure the policy settings from the Business App or Streamer menus.

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

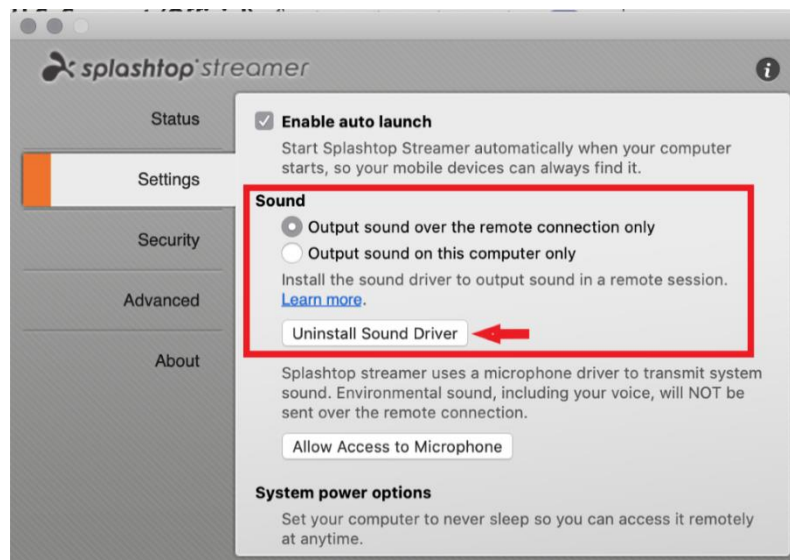
2. MacOS Additional Requirements

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

- **Security & Privacy permissions** for macOS [10.14 Mojave](#) , [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 Mojave/Catalina/Big Sur. 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 onboards 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 only)**.

Single Sign On					
Status	SSO Name	IDP Type	Protocol	Device Authentication	Settings
<input checked="" type="checkbox"/>	ST OKTA	Okta	SAML 2.0	<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/>	Splashtop ADFS	ADFS	SAML 2.0	<input checked="" type="checkbox"/>	

[Apply for new SSO method](#) [\(View instructions\)](#)

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

Email

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

Role : AdminGroup : Default Group

☐ 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

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

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

- ☒ user group
- ☒ computer group

Create Group

Cancel

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.

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.

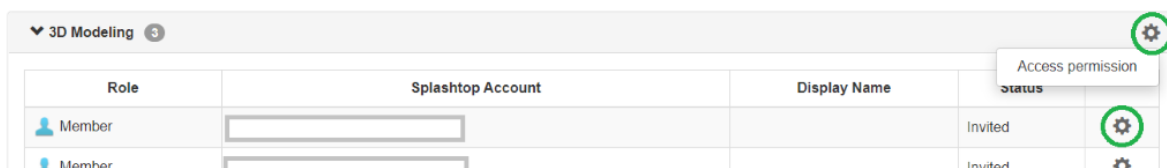
6. Access Permissions

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”.

☒ Only specific computers and computer groups

All Groups

Select all / Clear all Expand all / Collapse all ☐ Only show selected 4 computers selected

☒ Computer Lab 1 3

☐ Computer Lab 2 3

☐ Computer Lab 3 6

	Computer Name
<input checked="" type="checkbox"/>	Lab A
<input type="checkbox"/>	Lab B

7. Scheduled Access

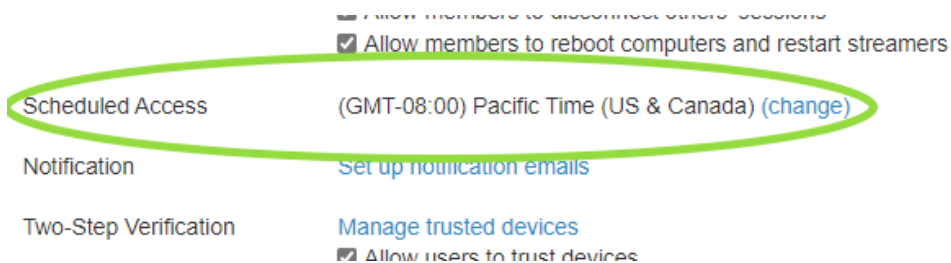
Scheduled Access allows admins to schedule users, groups, and computers for remote access on a time-slot basis. The team **Owner, Admins, and Group Admins** have access to the scheduling module.

Notes:

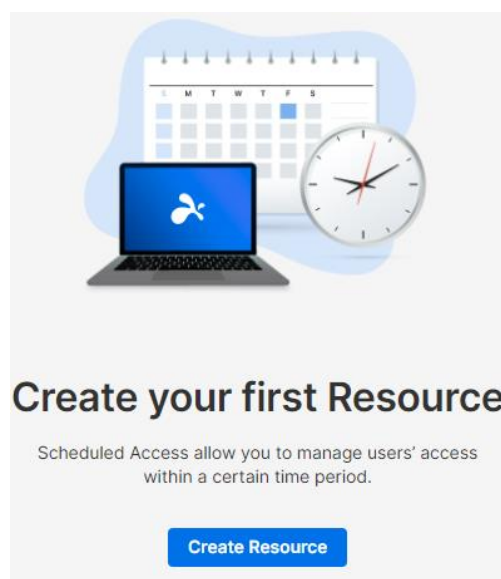
- Scheduled Access is granted in addition to existing user/group access permissions that are set under *Management -> Users* – they do NOT override existing user/group access permissions.
- For users who only need scheduled remote access, set their access permission under *Management -> Users* to “No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



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

GeneralComputersGroup Admin

Resource Name

Accounting Computers

Description (*optional*)

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

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

1

2

3

General

Computers

Group Admin

Computers

Select Computers

Select all / Clear all Expand all / Collapse all ☐ Only show selected

<input checked="" type="checkbox"/>	Computer Lab 1 3
<input type="checkbox"/>	Computer Lab 2 3
	Computer Name ^
<input checked="" type="checkbox"/>	Computer D
<input type="checkbox"/>	Computer E
<input type="checkbox"/>	Computer F

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

1

2

3

General

Computers

Group Admin

Assign group admin (optional)

Select Group Admin

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

Management / Scheduled Access

Scheduled Access

- Create Resource to select a set of computers, the
- Scheduled Access Permissions are granted in ad
- Scheduled Access Permissions do not override u

Create Resource

Resource Name

Accounting Computers

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

Finish with Schedule

You have successfully created resource. Now you could create schedule for users to access the associated computers and computer groups.

Later

Create Schedule

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))**.

2020-11-16

08:00 - 16:00

Repeat

Weekly

Sun Mon Tue Wed Thu Fri Sat

Repeat Ends (optional)

Choose End Date

Connections

☒ Force session to disconnect when Schedule ends.

Notify users before session ends:

5 minutes

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.

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	
			<div><div>Manage Schedule</div><div>Edit</div><div>Delete</div></div>

- **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 08:00 End of W...				20	21
22	23 08:00 End of W...				27	28
29	30 08:00 End of W...	Dec 01 04:00 Session 1	2		4	5

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 Resource for set of computers used by our company's Accountants.	4	None	...

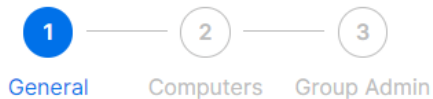
1. To re-activate a Resource, click the menu to the right of the **Resource** -> **Edit**.

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

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**.

Overview of Team Settings

Settings




Account Summary	Splashtop Enterprise Settings - 5 concurrent technician(s) and 10 end user(s)	
Team	Team name	Megan's team (change)
Subscriptions	Computers	29 of 1600 computers deployed (change)
Payment and Billing	Management	<ul style="list-style-type: none"><input checked="" type="checkbox"/> Enable file transfer<input checked="" type="checkbox"/> Enable remote print<input checked="" type="checkbox"/> Enable device redirection (detailed setup)<input checked="" type="checkbox"/> Enable redirect microphone input<input checked="" type="checkbox"/> Enable text copy-and-paste<input checked="" type="checkbox"/> Enable Paste Clipboard as Keystrokes<input checked="" type="checkbox"/> Enable remote wake<input checked="" type="checkbox"/> Enable remote reboot<input checked="" type="checkbox"/> Enable saving in-session chat transcript to session logs (learn more)<input checked="" type="checkbox"/> Enable chat (pre-session). Save chat transcript to session logs: Yes ▾ (learn more)<input checked="" type="checkbox"/> Enable in-session voice call (unattended access)<input checked="" type="checkbox"/> Enable in-session voice call (attended access)<input checked="" type="checkbox"/> Enable session recording (unattended access) (detailed setup)<input checked="" type="checkbox"/> Enable session recording (attended access) (detailed setup)<input checked="" type="checkbox"/> Enable share my desktop ⓘ (unattended access)<input checked="" type="checkbox"/> Enable share my desktop ⓘ (attended access)<input checked="" type="checkbox"/> Enable concurrent remote sessions (unattended access)<input checked="" type="checkbox"/> Enable concurrent remote sessions (attended access)<input checked="" type="checkbox"/> Enable remote command<input checked="" type="checkbox"/> Enable RDP computer<input checked="" type="checkbox"/> Enable 1-to-Many Scripting for team owner and all admins ▾<input checked="" type="checkbox"/> Enable group-specific admin role (learn more)<input checked="" type="checkbox"/> Enable showing currently logged-in Windows or Mac user (learn more)<input checked="" type="checkbox"/> Allow members to access the Management tab
Payment History		
Redeem Code		

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.

Management: These checkboxes control the team's feature capabilities, visibility options, and security protocols. Most settings apply global – they will be enabled/disabled for all users of the team, regardless of role. Some settings are role-based, including:

- Enable concurrent remote sessions (Two users into one computer)
 - Allow members to connect to computers in an active connection
- Allow members to access the Management tab
- Allow members to see groups (Only group names of computers they have access to)
- Allow members to establish concurrent sessions (connecting to multiple computers)
- Allow members to disconnect others' sessions
- Enable remote reboot (normal reboot, restart streamer, safe-mode reboot)
 - Allow members to reboot computers and restart streamers

Scheduled Access	(GMT-08:00) Pacific Time (US & Canada) (change)														
Notification	Set up notification emails														
Two-Step Verification	Manage trusted devices <input checked="" type="checkbox"/> Allow users to trust devices <input type="checkbox"/> Require admins to use two-step verification <input type="checkbox"/> Require members to use two-step verification														
Device Authentication	Email device authentication link to user only ▼														
Browser Authentication	Email device authentication link to user only ▼														
Third-party integration	Set up API keys														
Single Sign On	<table> <thead> <tr> <th>Default (reset)</th> <th>Status</th> <th>SSO Name</th> <th>IDP Type</th> <th>Protocol</th> <th>Device Authentication</th> <th>Settings</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="radio"/></td> <td><input checked="" type="checkbox"/></td> <td>test method</td> <td>ADFS</td> <td>SAML 2.0</td> <td><input type="checkbox"/></td> <td></td> </tr> </tbody> </table> Apply for new SSO method (View instructions)	Default (reset)	Status	SSO Name	IDP Type	Protocol	Device Authentication	Settings	<input checked="" type="radio"/>	<input checked="" type="checkbox"/>	test method	ADFS	SAML 2.0	<input type="checkbox"/>	
Default (reset)	Status	SSO Name	IDP Type	Protocol	Device Authentication	Settings									
<input checked="" type="radio"/>	<input checked="" type="checkbox"/>	test method	ADFS	SAML 2.0	<input type="checkbox"/>										
SCIM Provisioning Token	(Set up an API token)														

Schedule Access: Set the time zone for the scheduling module.

Session Indicator: Configure a [persistent banner](#) to show during remote sessions to notify end users that the computer is being accessed.

Notification: Set up email notifications for certain actions in the team, such as when a computer is added, when a connection is initiated, when a user accepts the team invitation, etc.

Two-Step Verification: Force admins and/or members to use [Two-Step Verification](#) (2FA).

Device/Browser Authentication: Determine who receives [device authentication](#) links for new Business App or Web Console logins. Email authentication can be disabled if a user already has 2FA turned on.

Third-party integration: If you have technician licenses to use Splashtop SOS, you can [set up API keys](#) to integrate Splashtop SOS with your existing ServiceNow, Zendesk, Freshservice, Freshdesk, and/or Jira helpdesk solution.

Single Sign-On: Apply and manage SSO methods here.

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 Print
- Attended Access (Technician license)
- 1-to-Many (Technician License)

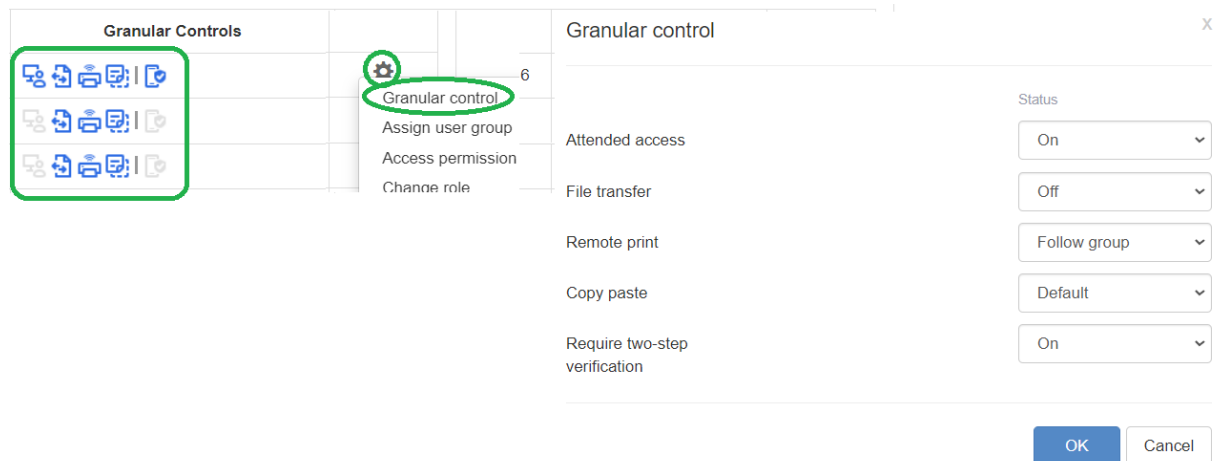
From **Management -> Settings**, you can set the **Default Granular Settings** of these features per user role. These default settings will be applied when a new user is invited to the team's default group or if a user/group's granular control setting is set to follow the default. The **Admin Configurable**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

Default Granular Settings	Admin	Member	Admin Configurable ?
Attended access	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
File transfer	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Remote print	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Copy paste	<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.

▼ Group 1 ⚙️					
<input type="checkbox"/>	Role	Splashtop Account	Display Name	Status	Granular control Access permission
<input type="checkbox"/>	 Admin	splashtop@splashtop.com		Enabled	    ⚙️

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



- 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. Remote Computer 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: 320.58 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 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.**

Actions

Buy Bitdefender

Computer View

All Groups

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

Scan task: N/A

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 14:00:00 -0800	C:\Users\ [redacted]		Acknowledge

[Acknowledge all threats](#)

[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.

↺

Actions

Computer View

All Groups

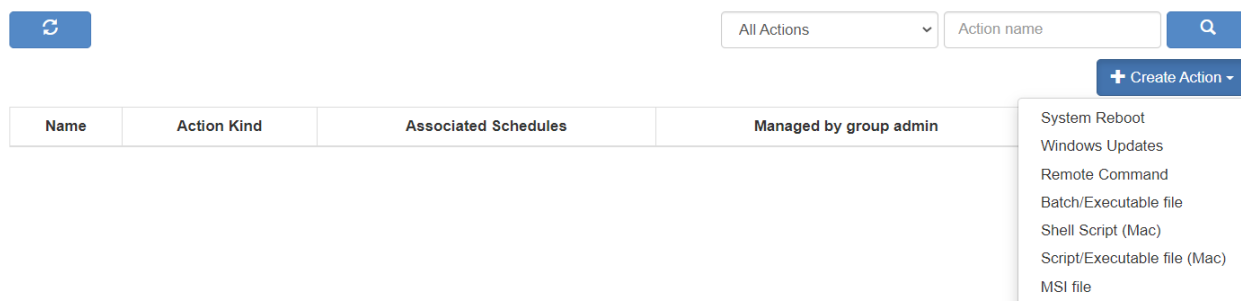
	Update Status	Computer Name	Group	OS	Important	Optional	Updates Policy	Last Update Time	Details
<input type="checkbox"/>	<div><div></div><div></div></div>	<div><div></div><div>Test</div></div>	Megan's Computers	Microsoft Windows 10 Pro 64-bit (10.0.18363)	0	0	Install updates automatically	2020-11-11 03:43:02 UTC	<div><div></div><div></div></div>
<input type="checkbox"/>	<div><div></div><div></div></div>	<div><div></div><div>Lab F</div></div>	Computer Lab 3	Microsoft Windows 10 Pro 64-bit (10.0.17134)	0	2	Install updates automatically		<div><div></div><div></div></div>

Available updates: 1 important, 9 optional [Check for updates](#) ☐ Include updates for other Microsoft products (Last checked for updates: 2020-11-11 00:30:10 -0800)

Code	Important	Reboot	Size	Update
<input type="checkbox"/> 2267602	Yes	No	789 MB	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.327.723.0) - Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.
<input type="checkbox"/>	No	Yes	45 MB	Intel - System - 9/19/2017 12:00:00 AM - 11.7.0.1000 - Intel System driver update released in September 2017

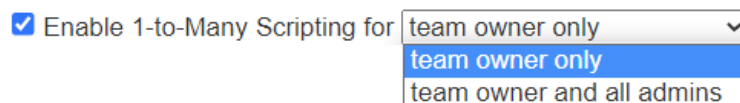
1-to-Many Actions & Schedules

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**.

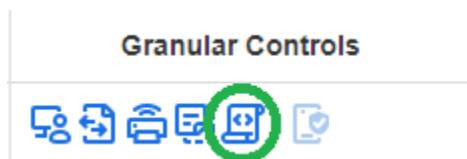


Actions that are set to run immediately can only be run on Online computers. If a computer is offline when a Schedule Action is attempted, there is currently no retry mechanism.

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

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.

Alert Profile Name (Enabled)

CPU Utilization (Enabled)

Name: Type: CPU Utilization

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.

Alert when the average CPU utilization is greater than or equal to % for

Also notify via email for ☐ alert ☐ acknowledgement ☐ recovery ☒ Also attach the connection link in the email.

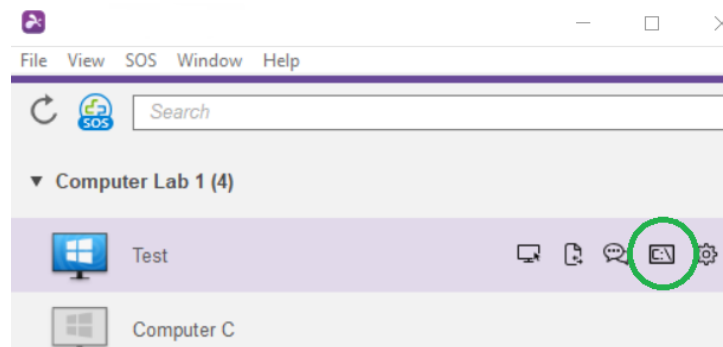
▼ Add Alert(s)

- CPU Utilization
- Memory Usage
- Disk Space
- Computer Online
- Computer Offline
- Software Installed
- Software Uninstalled
- Windows Update
- Available Updates
- 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.

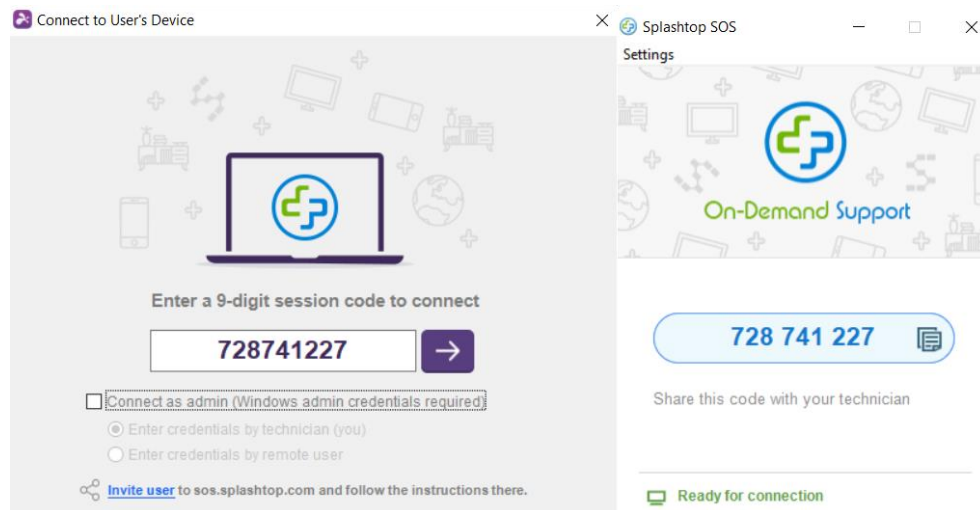


This feature is available for all users of the team if enabled, and requires the user to enter admin credentials of the remote computer to access.

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

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.

Default Granular Settings

	Owner	Admin	Member	Configurable by Admin ?
Attended Access	<input checked="" type="checkbox"/>	<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.

Role	Splashtop Account	Display Name	Status	Configuration
Admin			Enabled	
Member			Invited	

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**.

Management / SOS Customization

SOS Customization

Customize the SOS app's appearance and settings.

+ Create SOS App

Name	Date of Creation		
Test	2021-06-10 16:39:50	Share	...
Test 2	2021-12-15 18:16:12	Share	...
Company ABC	2022-03-24 00:49:38	Share	...

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)

Upload

Caption (max 20 characters)

This is a custom app

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

Upload

Edit



Background Color



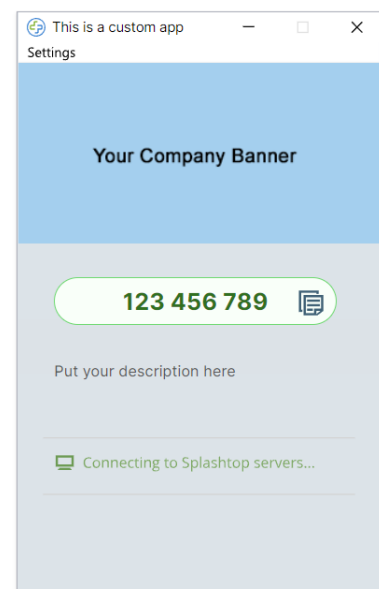
9-digit Section

123 456 789



Instruction Text (max 80 characters)

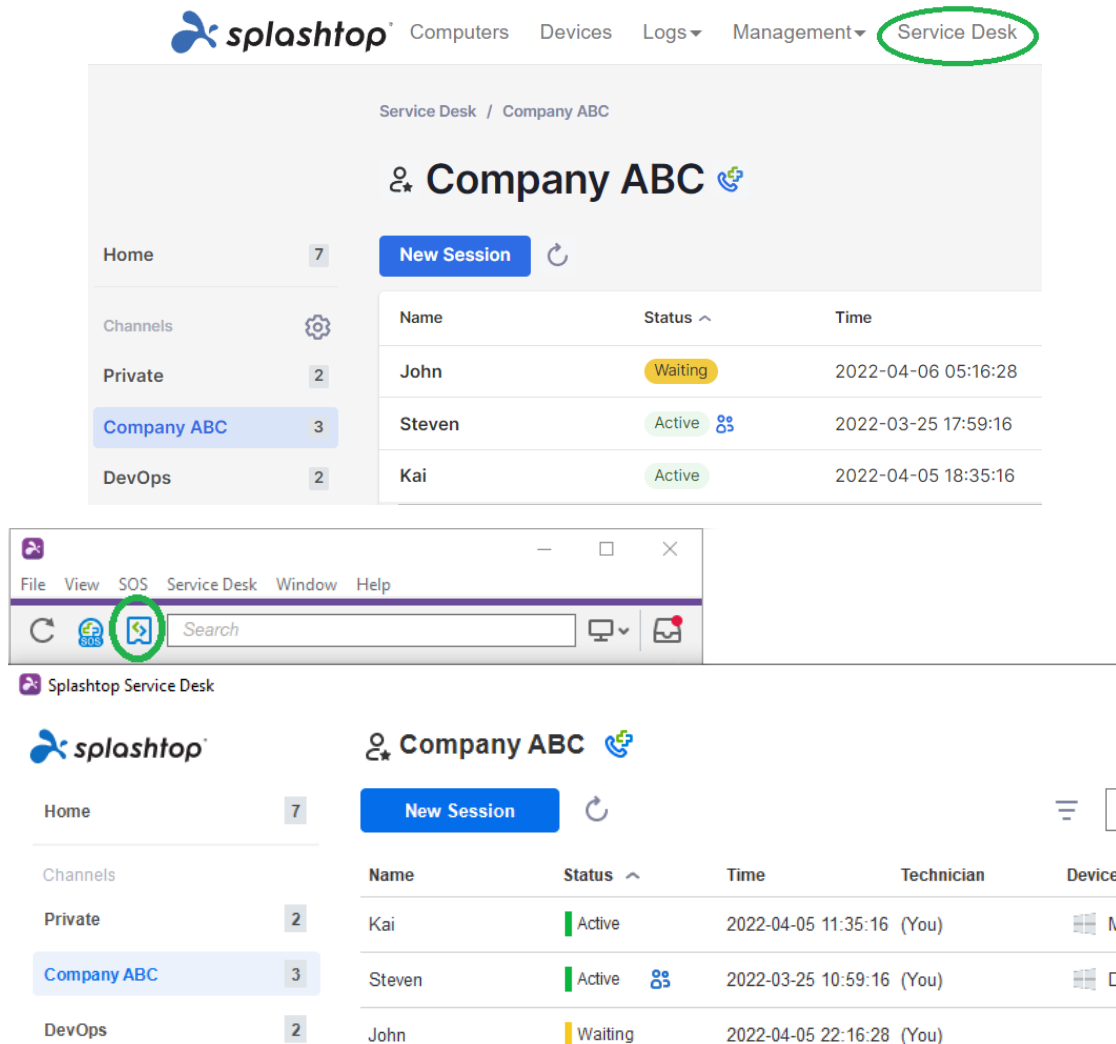
Put your description here



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 displays the Splashtop Service Desk interface. At the top, the navigation bar includes 'Computers', 'Devices', 'Logs', 'Management', and 'Service Desk' (highlighted with a green circle). Below the navigation bar, the page title is 'Service Desk / Company ABC'. The main content area shows a list of sessions for 'Company ABC'. The sessions are listed in a table with columns: Name, Status, Time, Technician, and Device. The sessions are:

Name	Status	Time	Technician	Device
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 sessions list, there is a 'New Session' button and a 'Search' bar. The 'Search' bar is highlighted with a green circle. The bottom of the screenshot shows the 'Splashtop Service Desk' logo and the 'Company ABC' logo.

Create channels within the Service Desk console and assign technicians. Technicians can create support sessions for customers via an invitation link or 6-digit code, or provide an [SOS Call](#) app for customers to launch when they need support. Once a support session is created, technicians can re-assign, transfer, or invite other technicians to the session.

Share Your Support Session

Link

PIN Code

Send the following link to your customer.

https://my.splashtop.com/service_desk

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

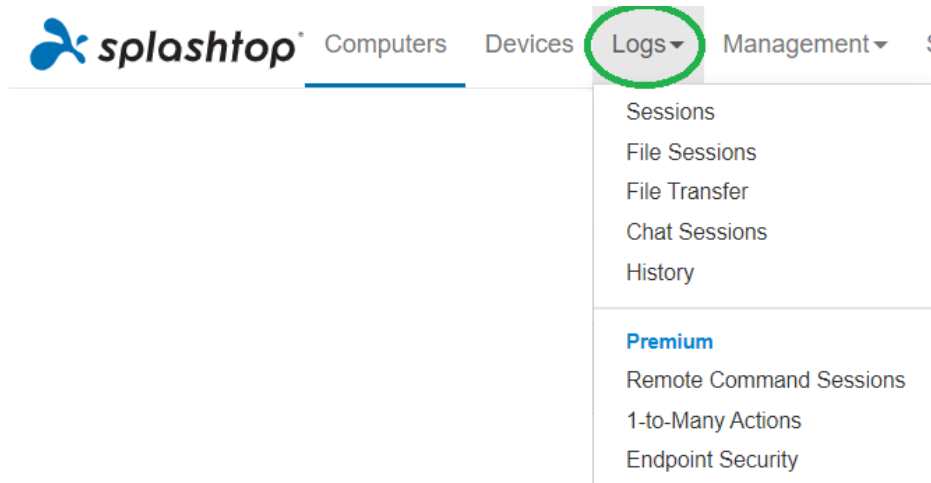
PIN code expires on 2022-09-01 17:54:54

Close

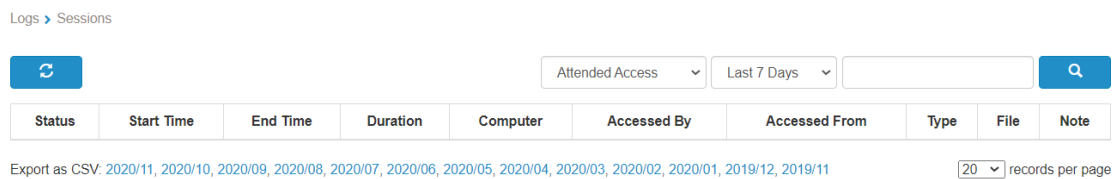
14. Logs

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. Additional Features

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

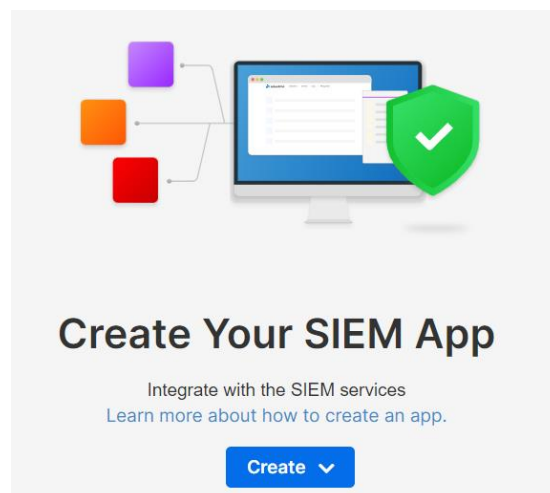
e.g. 168.168.168.168, 168.168.168.0/24



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

SIEM Logging

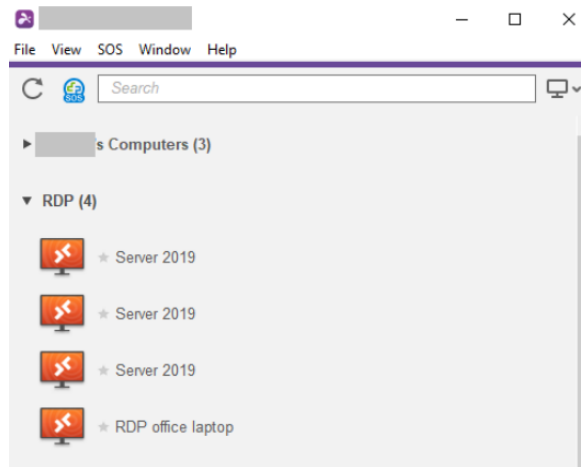
Export Splashtop session and history logs to a SIEM (Security information and event management) software for further analysis.



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

Splashtop Connector

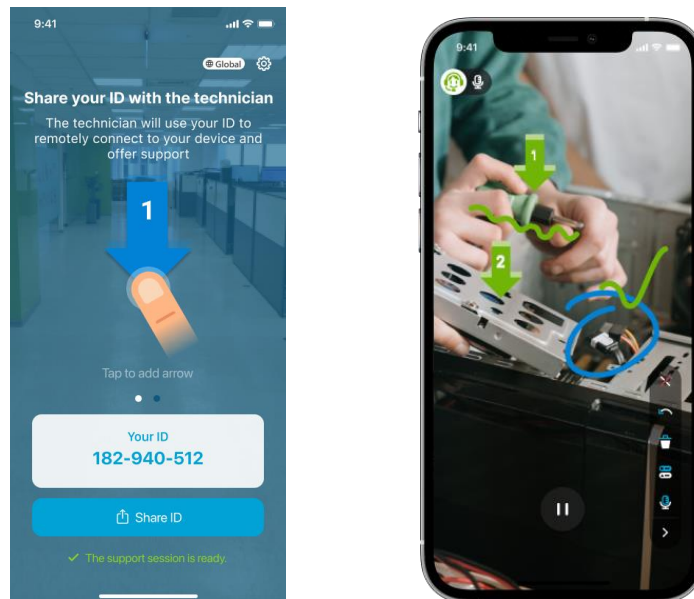
Securely bridge RDP connections to Windows computers and servers through Splashtop without using VPN or having to install software on each computer.



[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.](#)