2020

REMOTE LABS

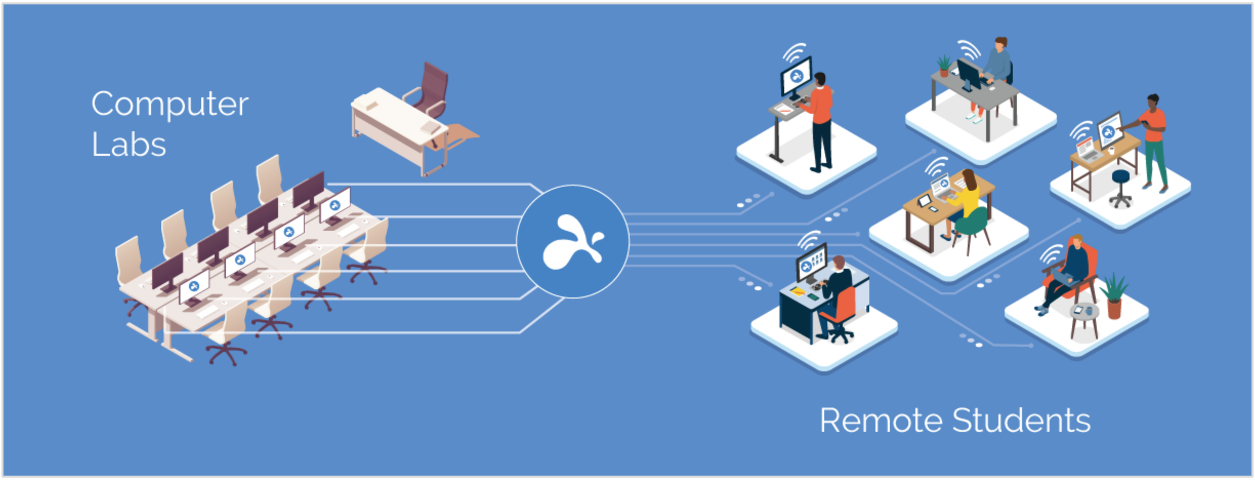
ADMINISTRATOR GUIDE

V1.1

SPLASHTOP INC. |

Table of Contents

1. Introduction



Splashtop remote desktop software lets users remotely access and take control of on-site computers from their own devices. Once connected, they will see the screen of the remote computer on their own device and be able to use any application or file as if they were sitting in front of it.

Educational institutions enhance distance learning by enabling students and faculty to remote into Windows and Mac computer labs from any computer or mobile device, including Chromebooks.

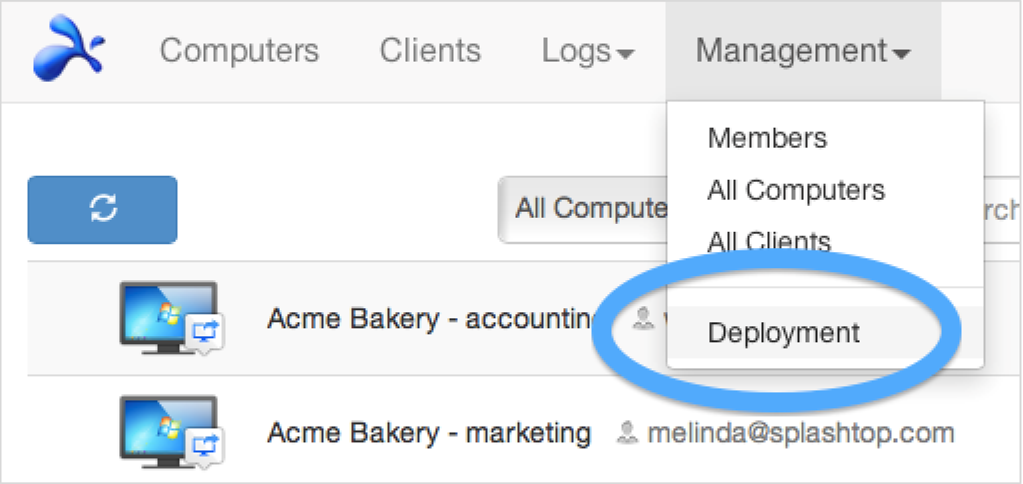
Splashtop for Remote Labs offers:

- Effective distance learning
- Remote into on-campus computers to access desktop software like Adobe and Autodesk apps.
- Remote work on computers with specialized hardware to create and edit videos, animations, models, designs, VFX, graphics in real-time.
- Use of personal devices like Chromebooks and iPads to leverage the processing and computing power of lab computers.

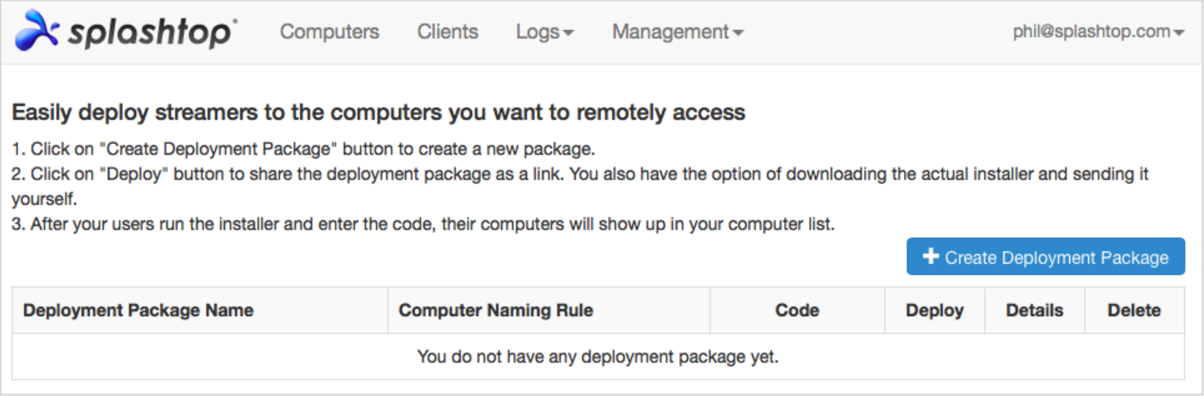
2. Deployment

IT admins can easily deploy and manage remote access to lab computers through a centralized console. Flexible grouping and access permissions allow admins to give students and instructors access only to the computers they need. Students can see which computers are in session and which are available to use. Splashtop's intuitive, easy-to-use features enable institutions to rapidly set up remote labs.

1. To deploy **lab computers**, log into my.splashtop.com and click on ***Management -> Deployment***.



2. Create deployment package.



Easily deploy streamers to the computers you want to remotely access

1. Click on "Create Deployment Package" button to create a new package.
2. Click on "Deploy" button to share the deployment package as a link. You also have the option of downloading the actual installer and sending it yourself.
3. After your users run the installer and enter the code, their computers will show up in your computer list.

Deployment Package Name	Computer Naming Rule	Code	Deploy	Details	Delete
You do not have any deployment package yet.					

When creating the deployment package, you have the option of specifying various default settings for the streamer, including computer name, security settings, sound re-direction, auto-launch behavior, etc.

Notes:

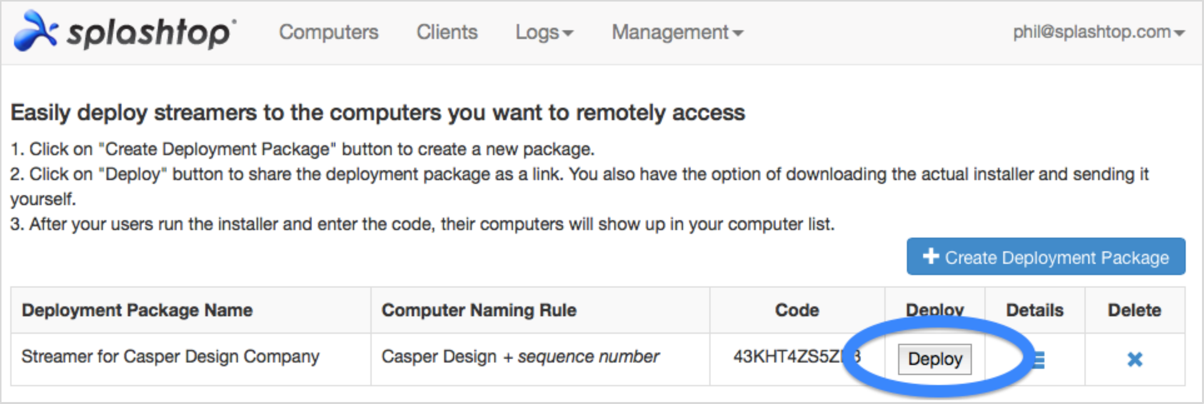
- If using Single Sign-On (SSO), do **not** select "Lock streamer settings using Splashtop admin credentials" - SSO accounts cannot unlock the streamer.

- “Lock screen when disconnect” locks the user account of the computer, but does not log out. To enable “force logout after session disconnect”, see additional instructions here.

Read more about customizing the default streamer settings using deployment packages and an overview of the different streamer settings.

3. Get the deployment package (either link or installer).

Click on the **Deploy** button.

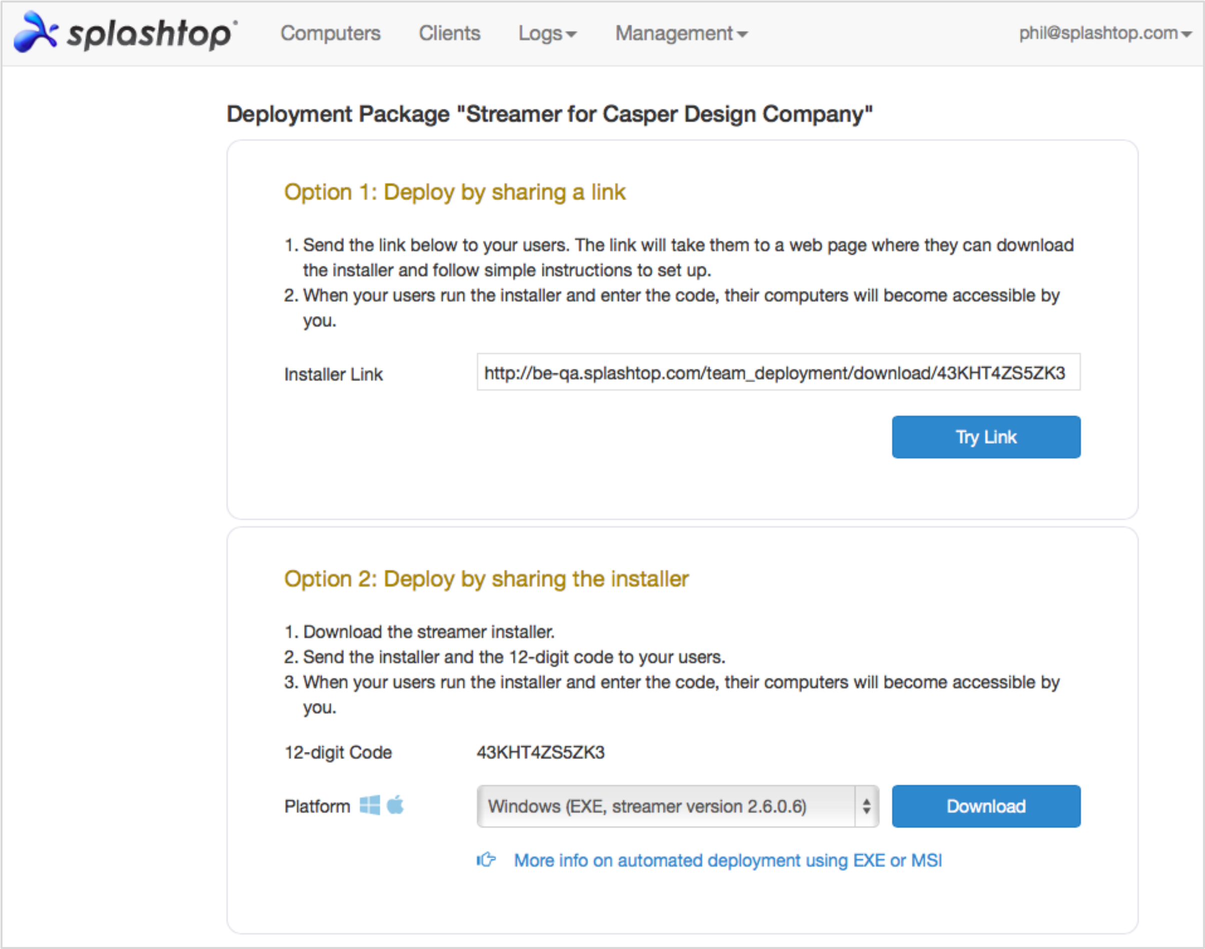


Easily deploy streamers to the computers you want to remotely access

1. Click on "Create Deployment Package" button to create a new package.
2. Click on "Deploy" button to share the deployment package as a link. You also have the option of downloading the actual installer and sending it yourself.
3. After your users run the installer and enter the code, their computers will show up in your computer list.

Deployment Package Name	Computer Naming Rule	Code	Deploy	Details	Delete
Streamer for Casper Design Company	Casper Design + *sequence number*	43KHT4ZS5Z[illegible]3	Deploy	≡	✖

You will find two options for distributing the deployment package: (1) share a link or (2) download the streamer installer for sharing via Dropbox, email, etc.



Deployment Package "Streamer for Casper Design Company"

Option 1: Deploy by sharing a link

1. Send the link below 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. When your users run the installer and enter the code, their computers will become accessible by you.

Installer Link http://be-qa.splashtop.com/team_deployment/download/43KHT4ZS5ZK3

Option 2: Deploy by sharing the installer

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

12-digit Code 43KHT4ZS5ZK3

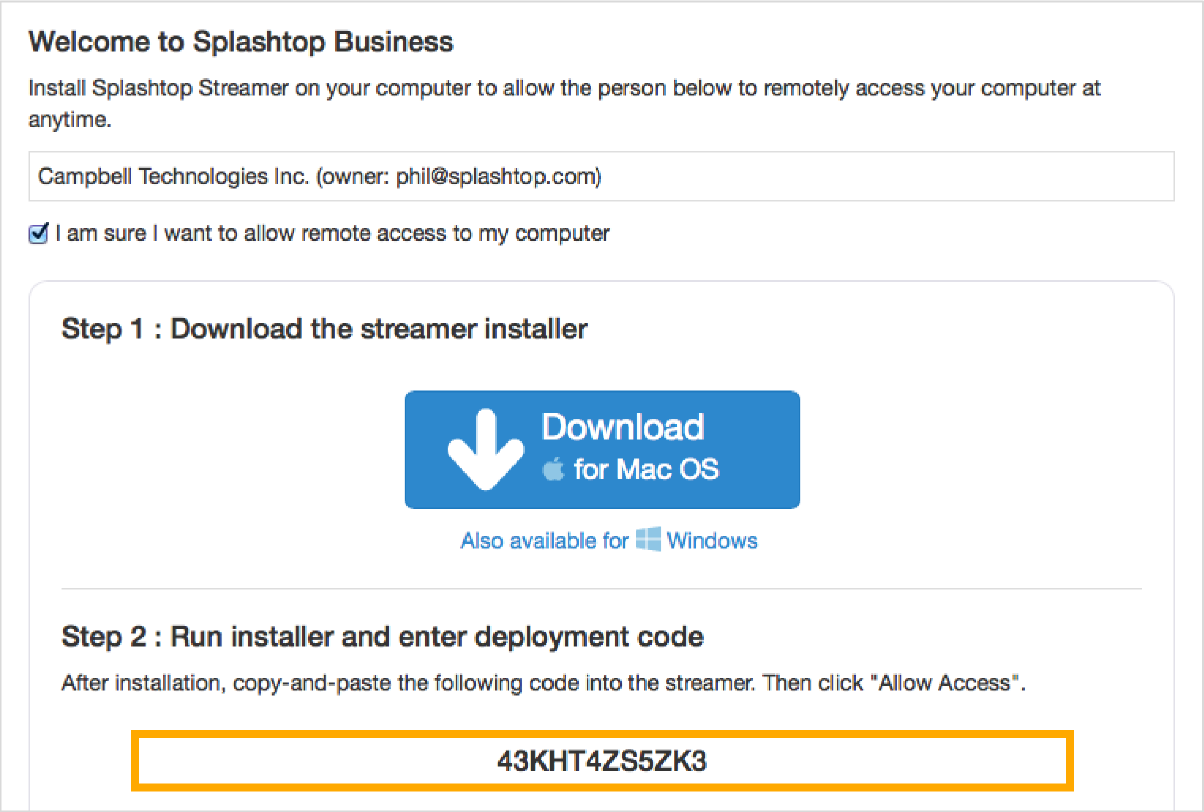
Platform Windows (EXE, streamer version 2.6.0.6)

More info on automated deployment using EXE or MSI

4. Send either the link or the streamer installer (and the 12-digit code) to your users, for them to set up their computers.

If you share a link, your users who follow the link will see a web page as follows.

From this web page, they can download the streamer installer and follow the instructions for entering your 12-digit code.



Welcome to Splashtop Business

Install Splashtop Streamer on your computer to allow the person below to remotely access your computer at anytime.

Campbell Technologies Inc. (owner: phil@splashtop.com)

☑ I am sure I want to allow remote access to my computer

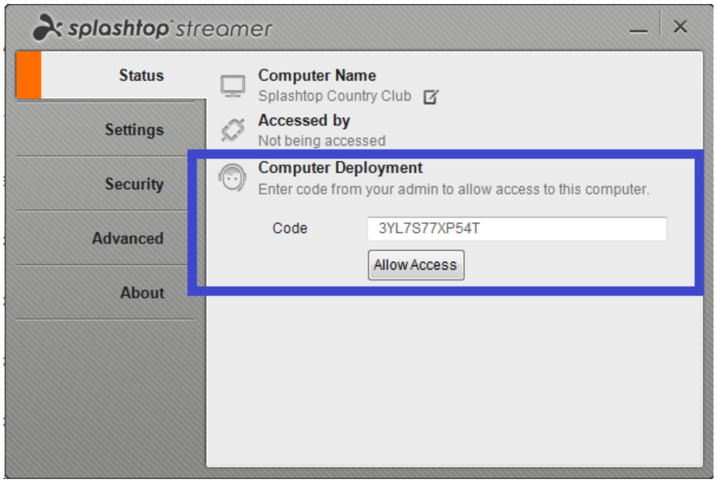
Step 1 : Download the streamer installer

Step 2 : Run installer and enter deployment code

After installation, copy-and-paste the following code into the streamer. Then click "Allow Access".

43KHT4ZS5ZK3

5. Users install the streamer and enter the 12-digit code.



Computer Name
Splashtop Country Club

Accessed by
Not being accessed

Computer Deployment
Enter code from your admin to allow access to this computer.

Code 3YL7S77XP54T

Notes:

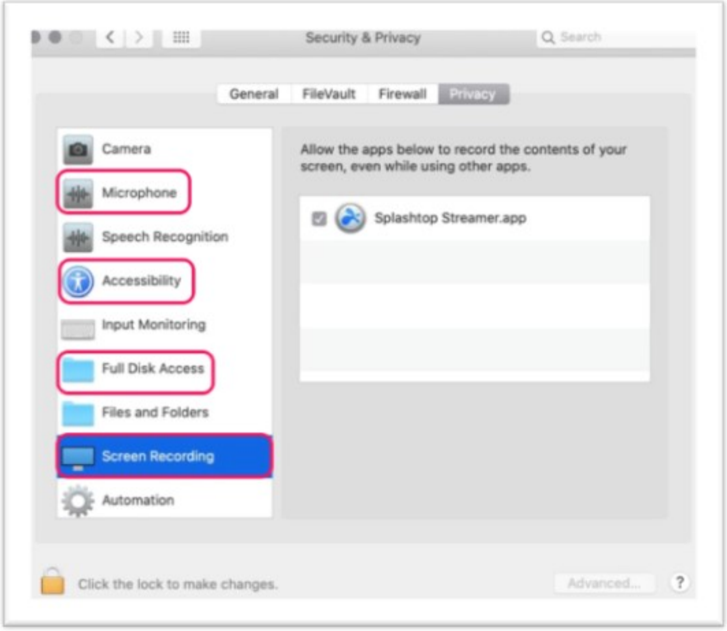
- Admins can configure the access permissions via my.splashtop.com.
- The streamer can be installed silently via command line.
- Deployment guides are also available for:

    - Group Policy (GPO)
    - Jamf Pro
    - Microsoft Intune
- Deleting a deployment package does not affect already deployed computers - only prevents new deployments with this code.

3. MacOS Additional Requirements

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

- **Security & Privacy permissions** for macOS 10.14 Mojave and macOS 10.15 Catalina.

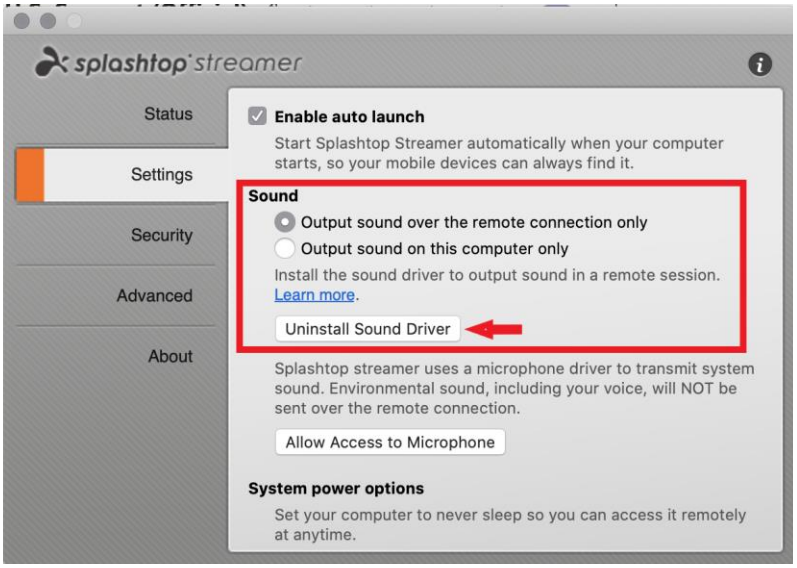


Allow the apps below to record the contents of your screen, even while using other apps.

☑ Splashtop Streamer.app

Click the lock to make changes.

- **Audio**: To enable audio streaming over the remote connection, install the Splashtop Sound Driver and allow microphone permission for Mojave/Catalina. 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.



☑ **Enable auto launch**

Start Splashtop Streamer automatically when your computer starts, so your mobile devices can always find it.

Sound

● Output sound over the remote connection only

○ Output sound on this computer only

Install the sound driver to output sound in a remote session. Learn more.

Splashtop streamer uses a microphone driver to transmit system sound. Environmental sound, including your voice, will NOT be sent over the remote connection.

System power options

Set your computer to never sleep so you can access it remotely at anytime.

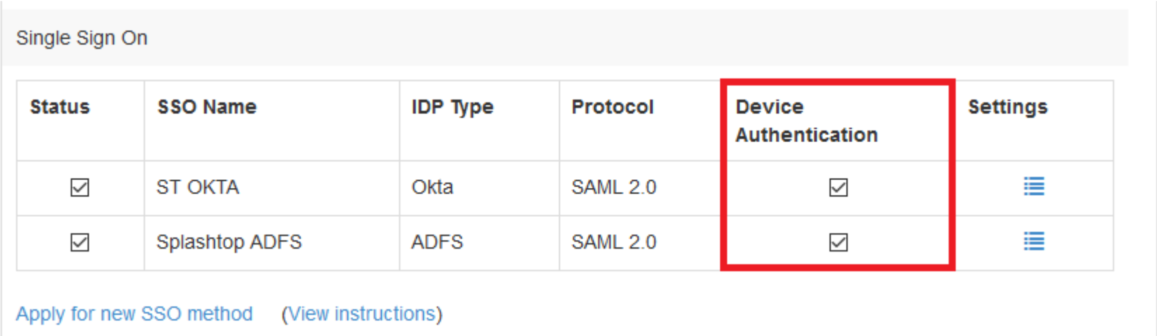
4. Single Sign-On (SSO)

Splashtop supports logging in https://my.splashtop.com and the *Splashtop Business app* using the credential created from your SAML 2.0 identity providers.

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

1. Create a DNS TXT record for all your domains that users will be using. A Splashtop rep will tell you the host and value to configure.
2. Create an SSO method for your IDP service in the Splashtop web console: How to apply for a new SSO method?
    a. Detailed instructions for certain IDP services, such as AzureAD, OKTA, ADFS, JumpCloud, OneLogin, can be found here: Single Sign-On (SSO)
3. *(Optional)* Set up **SCIM provisioning** (if you use AzureAD or Okta) to automatically provision and sync users and groups. This skips the invitation email process.
4. (Optional) Import SSO users by CSV fie if you are unable to use SCIM provisioning.

Once configured, you may want to disable device authentication emails for SSO configured accounts. This way, users that are associated with your SSO method do not need to click additional email links to authenticate their devices. Simply, uncheck the Device Authentication checkbox for the SSO method on your SSO table, under the owner account at ***Management -> Settings***.



Single Sign On

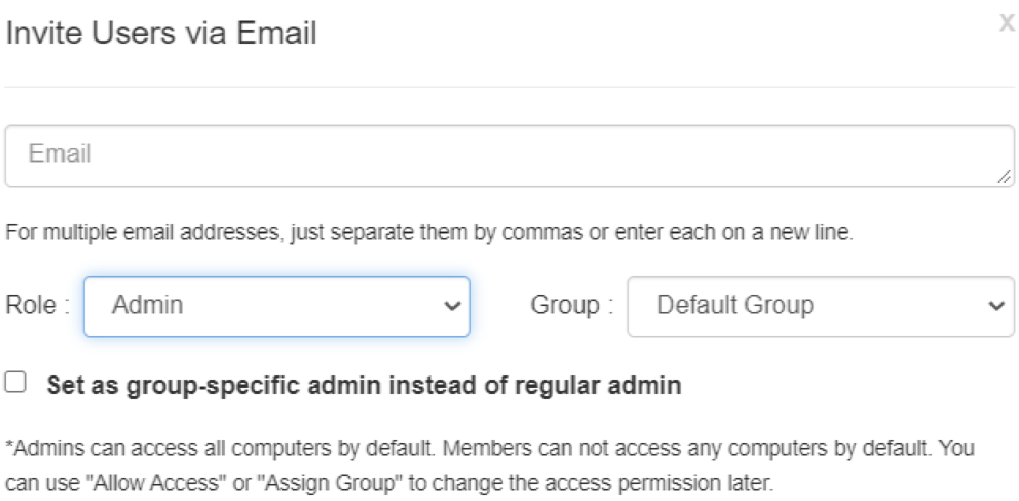
Status	SSO Name	IDP Type	Protocol	Device Authentication	Settings
☑	ST OKTA	Okta	SAML 2.0	☑	☰
☑	Splashtop ADFS	ADFS	SAML 2.0	☑	☰

Apply for new SSO method (View instructions)

5. Inviting Users

Inviting users by going to ***Management -> Users -> Invite Users***.

While you add new users, you can assign them different roles – Owner, Admin or Member. There is only one Owner. You can read more in detail about the authority associated with each of these roles. You can assign them to a user group, which can also be done at a later time. If using Single Sign-On, select an Authentication method to associate the user(s) to.



Invite Users via Email

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

Role : Admin

Group : 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.

In common practices, IT team members and staff who need control over all users and computers can be Admins. Faculty/Instructors who only need to administer specific user and/or computer groups can be group-specific Admins. Students and others who will only use granted remote access can be Members.

6. Grouping users/students and lab computers

With Splashtop you can group your users and computers for easier management and assign access permissions by user or by user group.

Get started by logging into my.splashtop.com and clicking on ***Management -> Grouping***.

Notes:

- Each user or computer can only belong to one group.

Group computers for **easier management**. Your computers will then be organized by groups on your Splashtop Business app and the web console.

Group users for **easier access permission control**. You can set access permissions for an entire group of users. New users added to the group can inherit that group's access permission settings.

Create a group

Create groups by logging into my.splashtop.com and clicking on **Grouping**.

You can create 3 types of groups:

1. User-only group
2. Computer-only group
3. User and computer group

A **user-only group** can only consist of users (students and instructors). 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 user access to a whole group of computers.

A **user and computer group** is a special group that is a shortcut for group-based access control. You can add both users and computers to this group. By default, all users in this group can access all computers in this group.

Best/common practices include:

- Grouping users by course or focus/major (ex: Architecture, Animation, Programming 101, etc)
- Grouping users by Students, Staff, IT, etc.
- Grouping computers by lab or site (ex: Room 101, Computer Lab A, etc)

Add users or computers to the group

From the grouping page, use the gear icon to the right of the group to add users or computers. Multiple users or computers can be added at a time.

From the computer list page, use the gear icon to the right of each computer to assign that computer to a group, one computer at a time.

When inviting a user, you can optionally choose a user group. Upon accepting the invitation, the user will automatically be placed in that group and inherit the group's access permissions.

Edit group

From the grouping page, use the gear icon to the right of the group to edit the group properties. You can rename the group. You can also change a user-only group or computer-only group to a "user and computer" group.

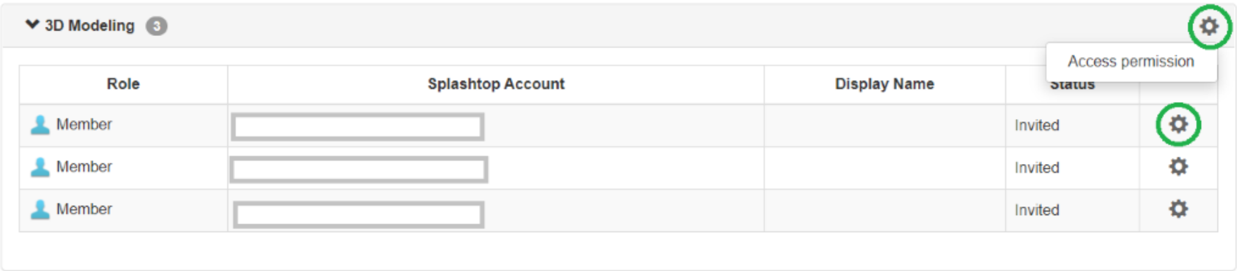
Set access permissions

Access permissions are set on the **Users** page, under ***Management -> Users***.

Notes:

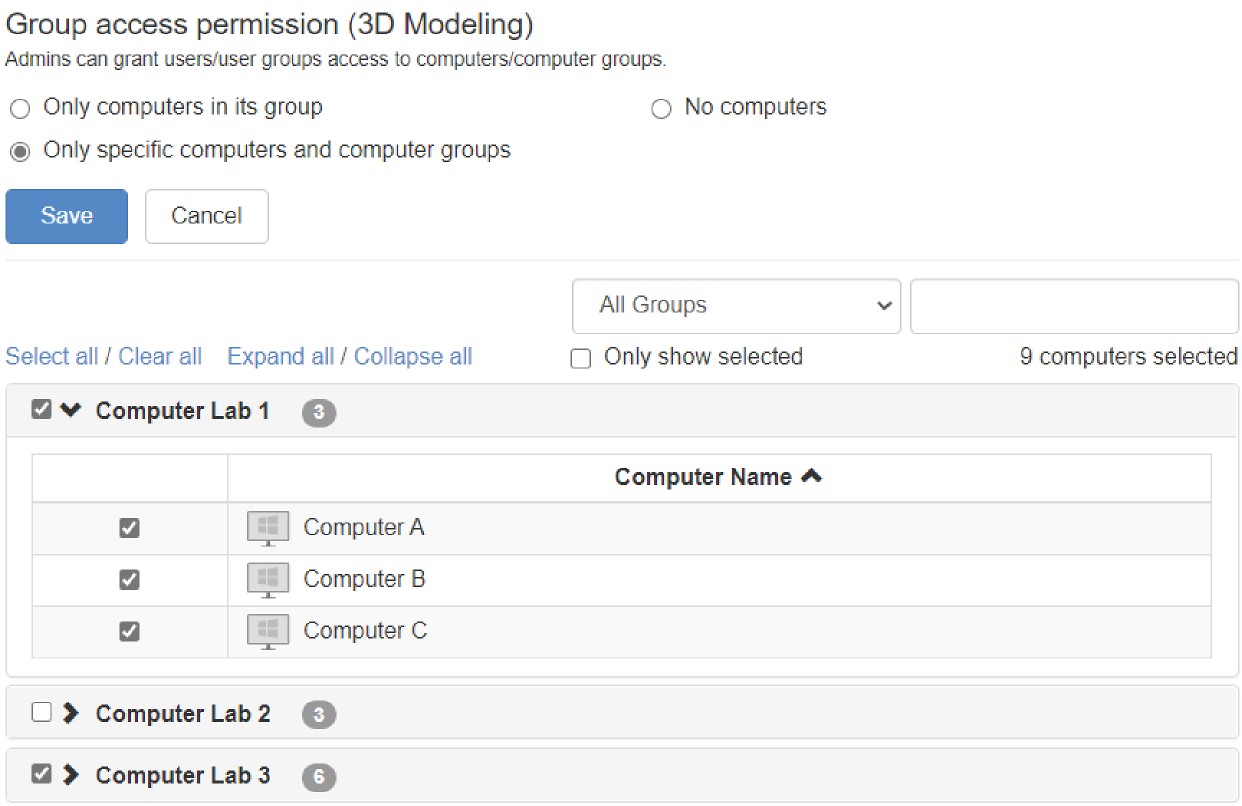
- Access permissions will grant a user access to computers, regardless of time of day. To only grant access for a particular timeslot, see the Access Schedule section below.

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."



Role	Splashtop Account	Display Name	Status	
Member			Invited	⚙
Member			Invited	⚙
Member			Invited	⚙

You can then select any combination of computers and computer groups to be accessible by that user or user group.



Group access permission (3D Modeling)

Admins can grant users/user groups access to computers/computer groups.

○ Only computers in its group ○ No computers

● Only specific computers and computer groups

□ Only show selected

9 computers selected

☑ Computer Lab 1 (3)

	Computer Name
☑	Computer A
☑	Computer B
☑	Computer C

□ Computer Lab 2 (3)

☑ Computer Lab 3 (6)

7. Access Schedule

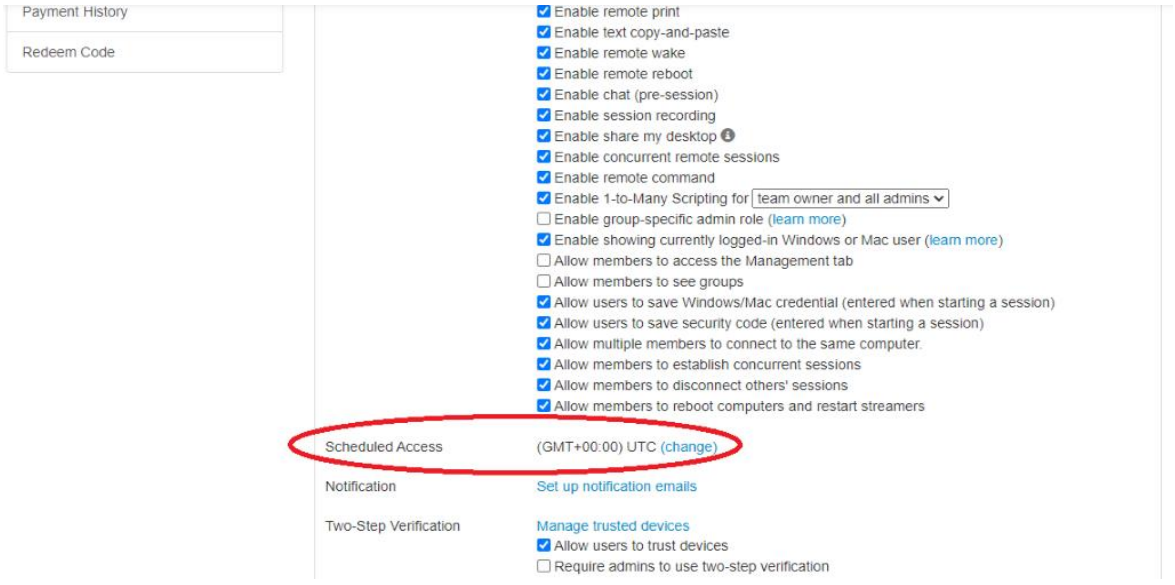
With Splashtop, admins can schedule access of individual users or group of users to specific computers or computer groups.

Notes:

- Scheduled Access Permissions are granted in addition to existing user/group access permissions – they do not override them.

Under ***Management -> Access Schedule*** section, admins can create schedules and associate the schedules with specific users and computers or groups of both.

1. **Before creating any new schedules, please go to *my.splashtop.com -> Management -> Settings* to configure the time zone. Time zone cannot be changed when a schedule is in place.**



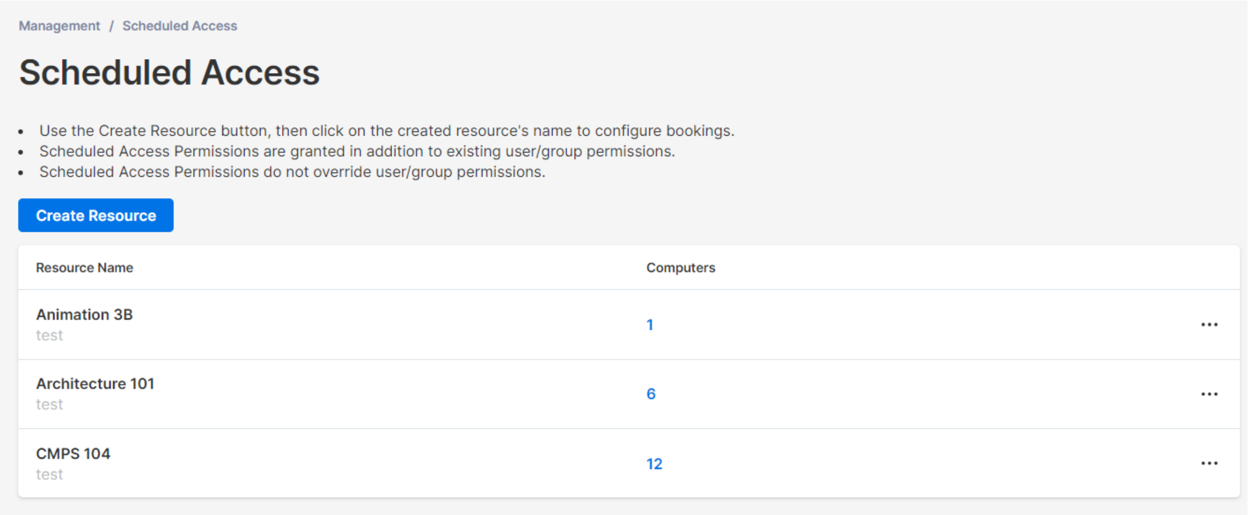
☑ Enable remote print
☑ Enable text copy-and-paste
☑ Enable remote wake
☑ Enable remote reboot
☑ Enable chat (pre-session)
☑ Enable session recording
☑ Enable share my desktop
☑ Enable concurrent remote sessions
☑ Enable remote command
☑ Enable 1-to-Many Scripting for team owner and all admins
□ Enable group-specific admin role (learn more)
☑ Enable showing currently logged-in Windows or Mac user (learn more)
□ Allow members to access the Management tab
□ Allow members to see groups
☑ Allow users to save Windows/Mac credential (entered when starting a session)
☑ Allow users to save security code (entered when starting a session)
☑ Allow multiple members to connect to the same computer
☑ Allow members to establish concurrent sessions
☑ Allow members to disconnect others' sessions
☑ Allow members to reboot computers and restart streamers

Scheduled Access (GMT+00:00) UTC (change)

Notification Set up notification emails

Two-Step Verification Manage trusted devices
☑ Allow users to trust devices
□ Require admins to use two-step verification

2. Go to ***Management -> Scheduled Access***. Click on "Create Resource".

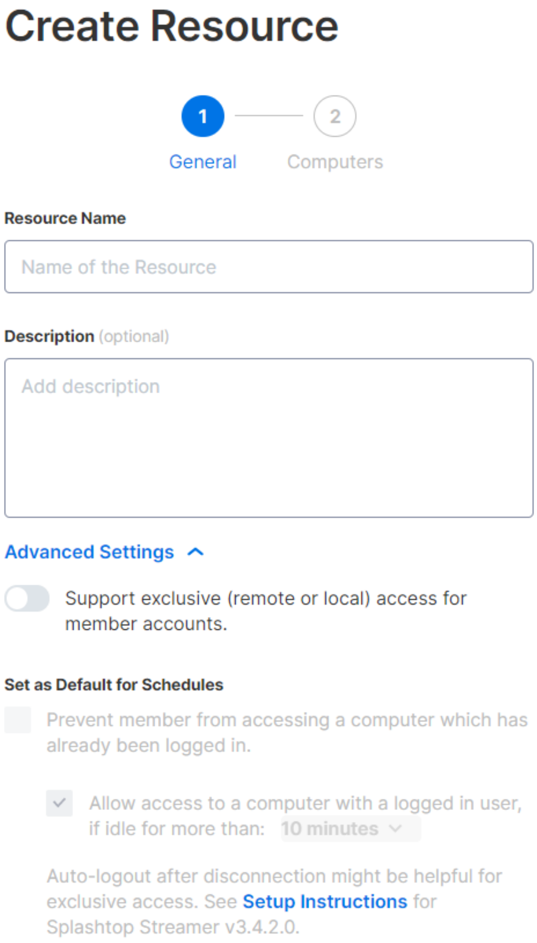

Management / Scheduled Access

Scheduled Access

- Use the Create Resource button, then click on the created resource's name to configure bookings.
- Scheduled Access Permissions are granted in addition to existing user/group permissions.
- Scheduled Access Permissions do not override user/group permissions.

Resource Name	Computers	
Animation 3B test	1	···
Architecture 101 test	6	···
CMPS 104 test	12	···

3. You can enter a resource name and description. The resource is a set of computers, such as a computer lab. Click "Advanced Settings" to enable support for exclusive access. This setting prevents a remote user from accessing a computer if there is a user logged into the operating system. This helps with preventing users from connecting into a computer that is in local use.



Create Resource

Resource Name

Name of the Resource

Description (optional)

Add description

Advanced Settings

○ Support exclusive (remote or local) access for member accounts.

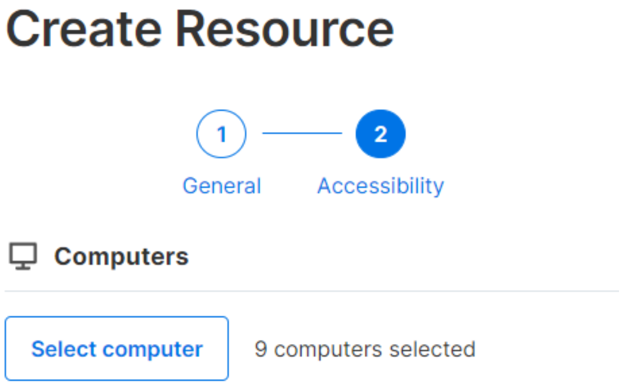
Set as Default for Schedules

□ 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

Auto-logout after disconnection might be helpful for exclusive access. See **Setup Instructions** for Splashtop Streamer v3.4.2.0.

4. On the second page, you can select the computers/computer groups that are associated with the resource.

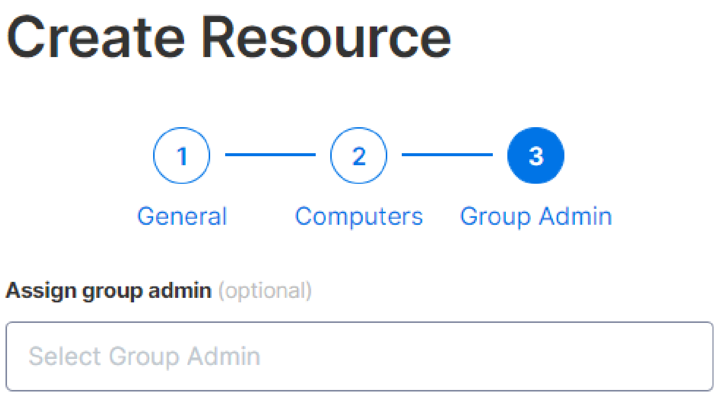


Create Resource

Computers

9 computers selected

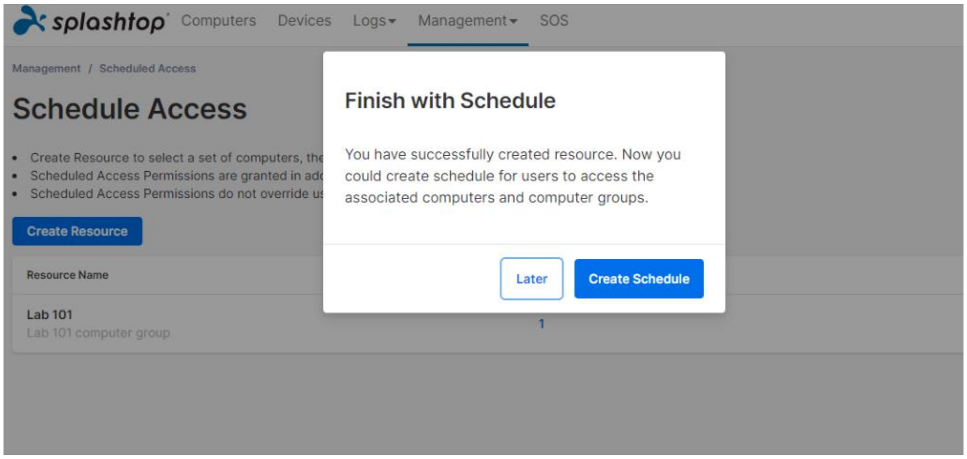
5. You can assign a Group Admin to help manage the resource and schedules. Group admins can only see resources that they create, or resources that they are assigned to.



Create Resource

Assign group admin (optional)

6. Continue to "Create Schedule", or later click the Resource name (or Manage Schedule) to assign Schedules to the resource.



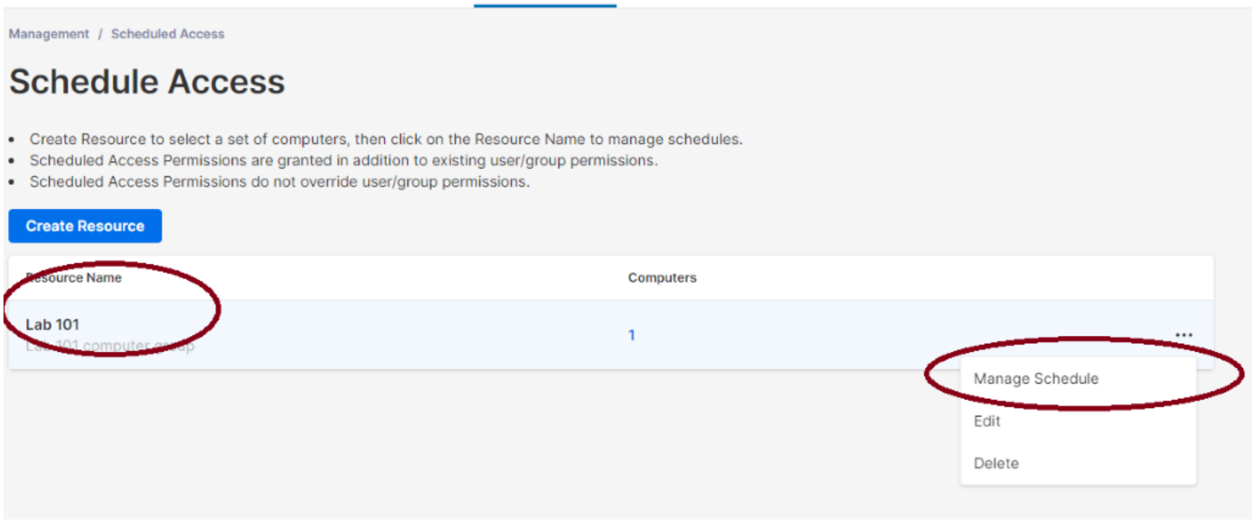
Schedule Access

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

Resource Name	
Lab 101 Lab 101 computer group	1

Finish with Schedule

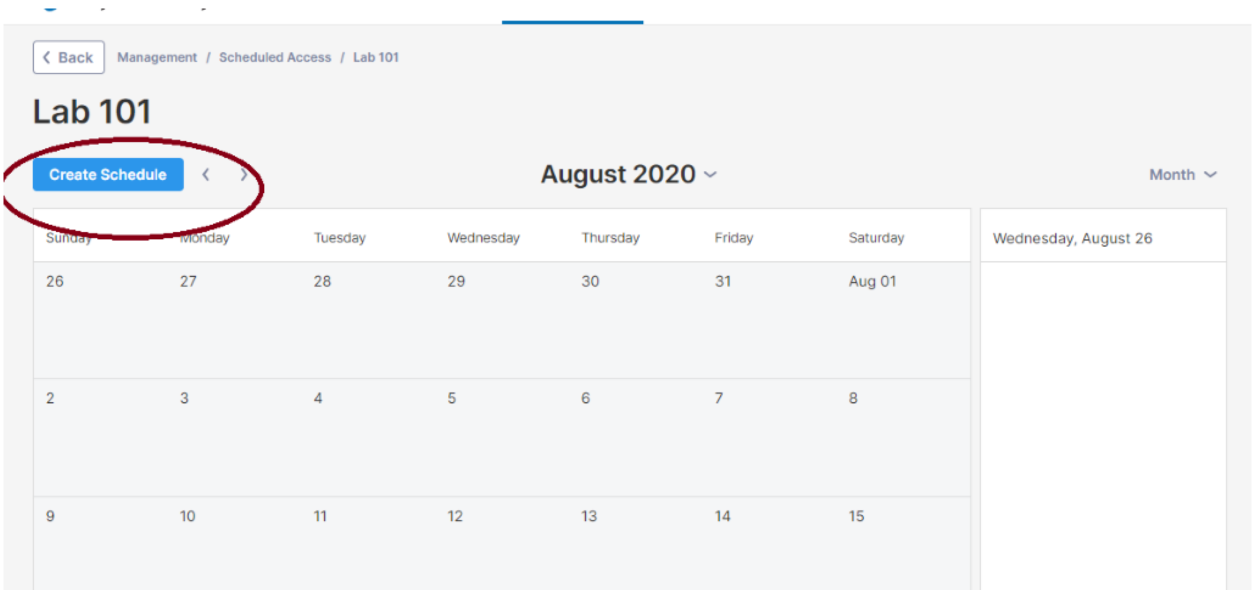
You have successfully created resource. Now you could create schedule for users to access the associated computers and computer groups.



Schedule Access

- Create Resource to select a set of computers, then click on the Resource Name to manage schedules.
- Scheduled Access Permissions are granted in addition to existing user/group permissions.
- Scheduled Access Permissions do not override user/group permissions.

Resource Name	Computers
Lab 101 Lab 101 computer group	1

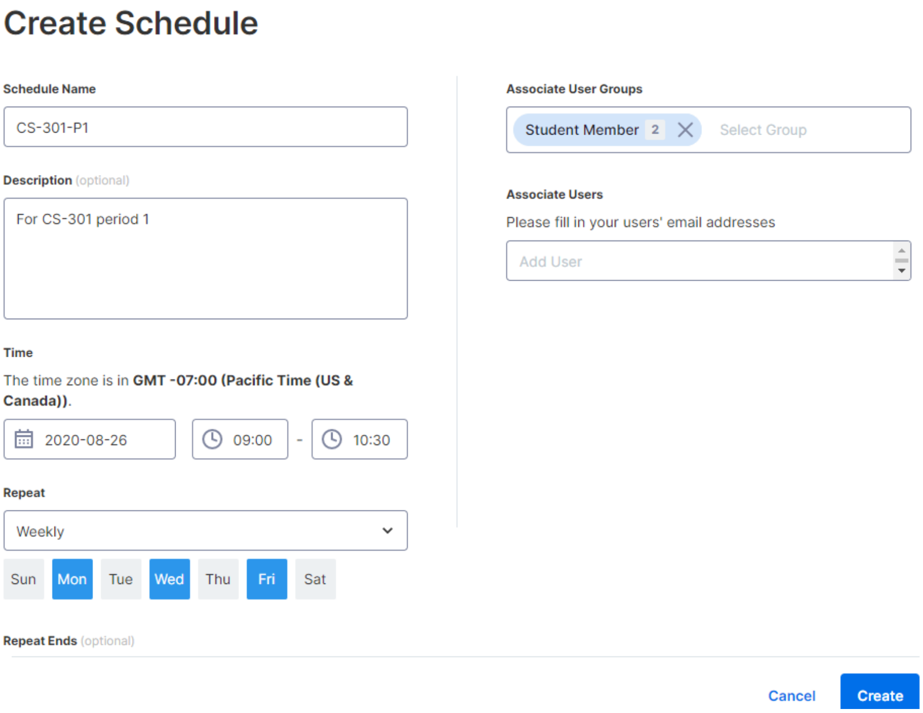


Lab 101

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
26	27	28	29	30	31	Aug 01
2	3	4	5	6	7	8
9	10	11	12	13	14	15

Wednesday, August 26

7. Create the Schedule for the resource by filling in the Name, Starting Date, and Recurrence. Select user groups or individual users to associate with the schedule. Note: The time drop-down selection is a 30-minute interval, but you can manually type in a value granular to a minute. You can also paste a list of users/emails, like from a class roster.



Create Schedule

Schedule Name: CS-301-P1

Description (optional): For CS-301 period 1

Time

The time zone is in **GMT -07:00 (Pacific Time (US & Canada))**.

2020-08-26 09:00 - 10:30

Repeat: Weekly

Sun [✓ Mon] Tue [✓ Wed] Thu [✓ Fri] Sat

Repeat Ends (optional)

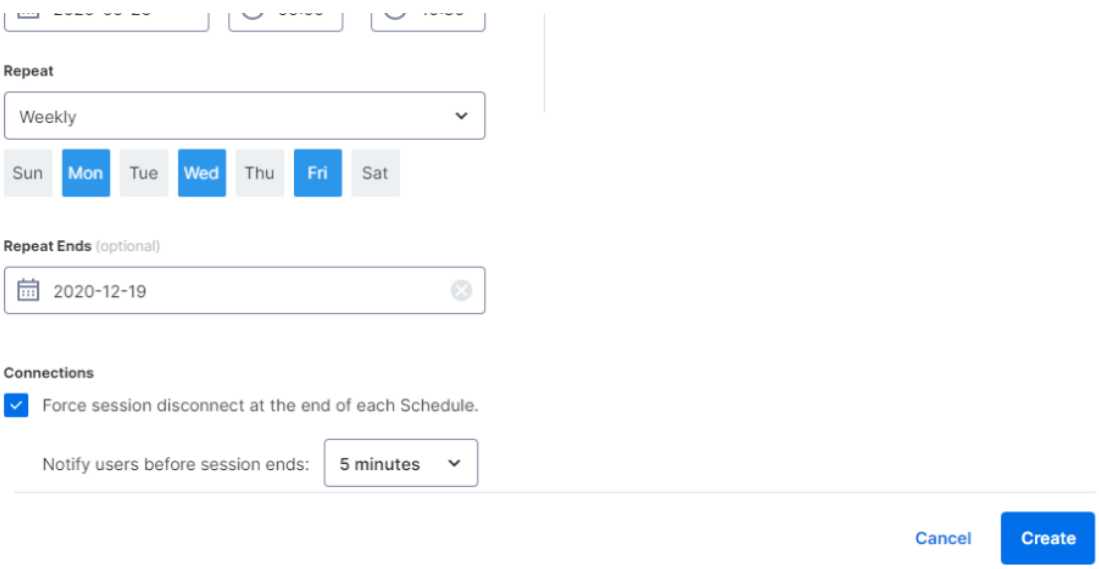
Associate User Groups: Student Member 2 ✕ Select Group

Associate Users

Please fill in your users' email addresses

Add User

8. Check "Force session disconnect at the end of each Schedule" if you would like sessions to forcefully disconnect at the end of the timeslot. Note: This does not log out of the remote computer's user account.



Repeat

Weekly

Sun ☐ Mon ☑ Tue ☐ Wed ☑ Thu ☐ Fri ☑ Sat ☐

Repeat Ends (optional)

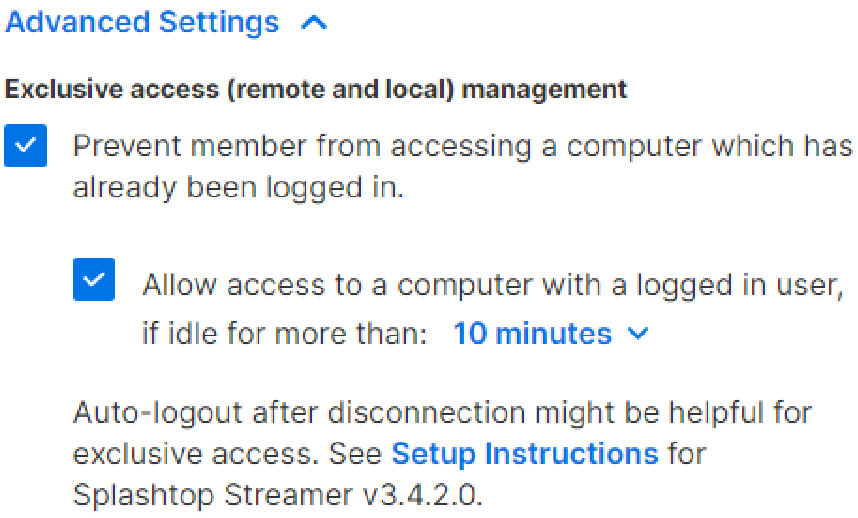
2020-12-19

Connections

☑ Force session disconnect at the end of each Schedule.

Notify users before session ends: 5 minutes

Click "Advanced Settings" to turn on/off exclusive access, which allows/disallows a remote user from connecting to a computer with a operating system user logged in.



Advanced Settings

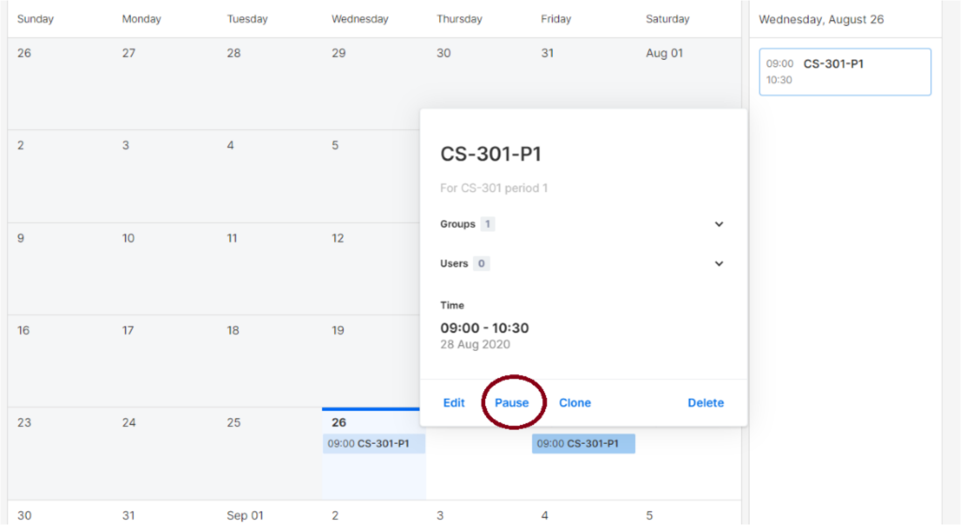
Exclusive access (remote and local) management

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

☑ Allow access to a computer with a logged in user, if idle for more than: 10 minutes

Auto-logout after disconnection might be helpful for exclusive access. See Setup Instructions for Splashtop Streamer v3.4.2.0.

9. To pause / resume a schedule, click on the schedule and then Pause / Resume button. To clone a booking, click the Clone button.



CS-301-P1

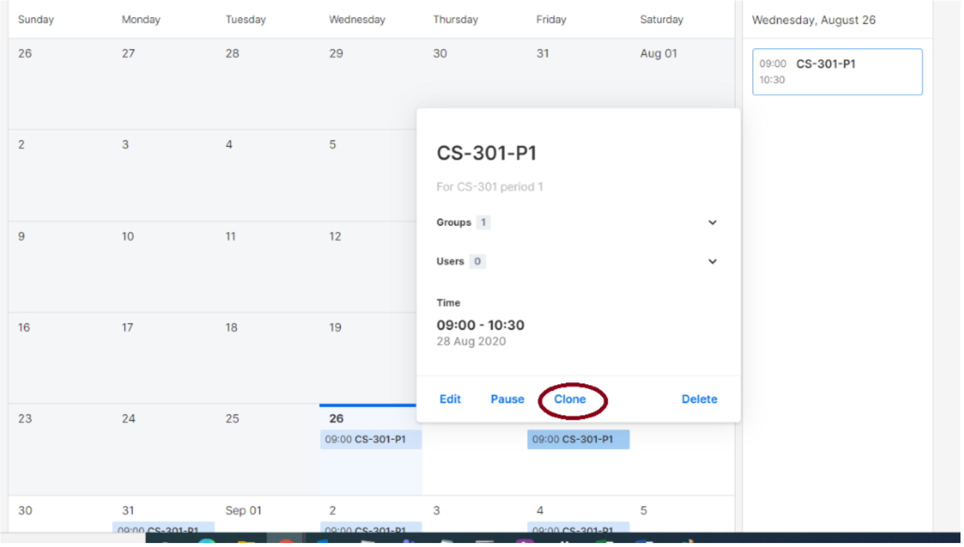
For CS-301 period 1

Groups 1

Users 0

Time

09:00 - 10:30
28 Aug 2020



CS-301-P1

For CS-301 period 1

Groups 1

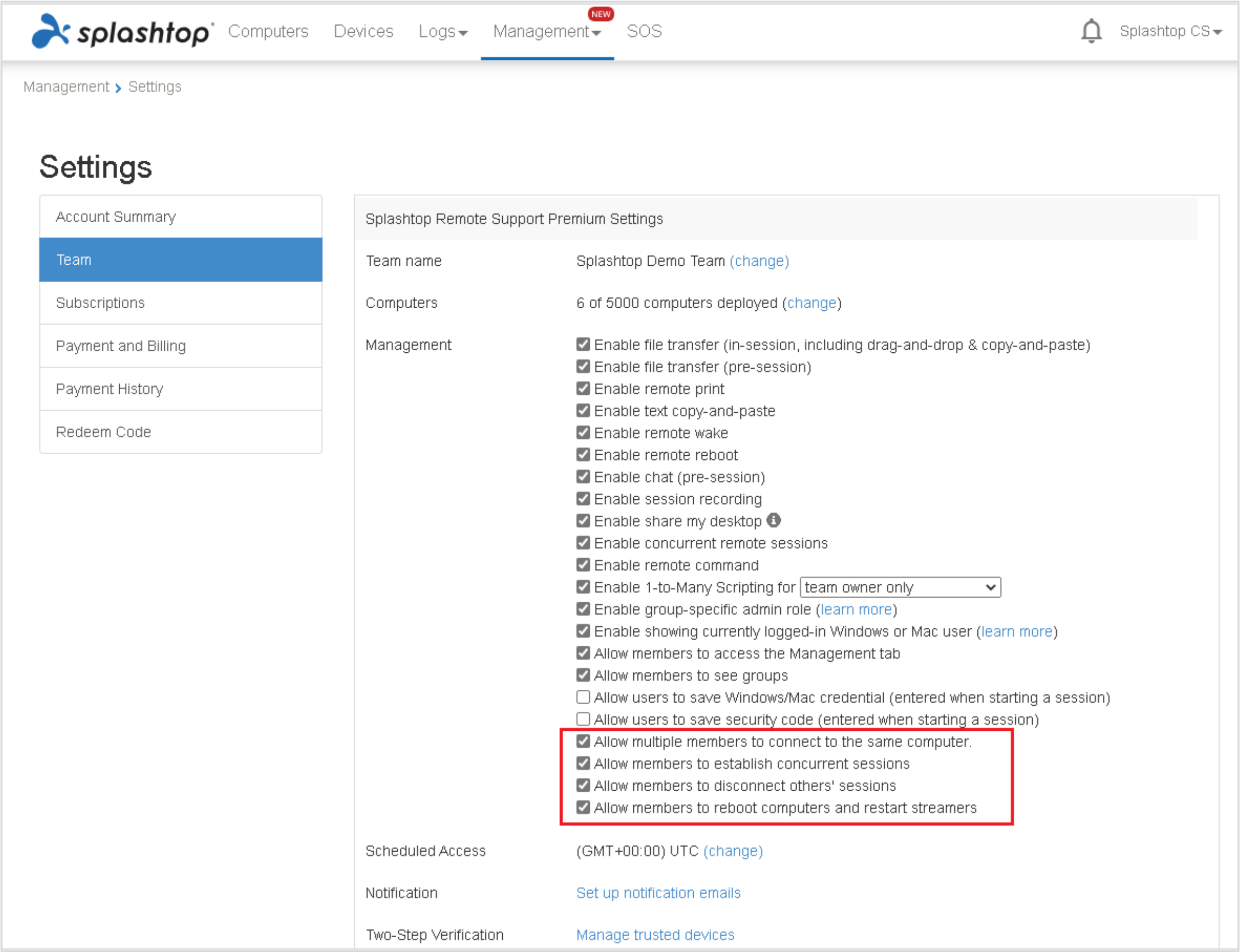
Users 0

Time

09:00 - 10:30
28 Aug 2020

8. Additional Features to limit student privileges on remote lab computers.

Splashtop Remote Labs comes with additional features to prevent certain actions by students on remote lab computers. These settings apply to members only (such as students) and not admins (such as instructors) and can be found at https://my.splashtop.com under Management > Settings > Team section.



Splashtop Remote Support Premium Settings

Team name Splashtop Demo Team (change)

Computers 6 of 5000 computers deployed (change)

Management
☑ Enable file transfer (in-session, including drag-and-drop & copy-and-paste)
☑ Enable file transfer (pre-session)
☑ Enable remote print
☑ Enable text copy-and-paste
☑ Enable remote wake
☑ Enable remote reboot
☑ Enable chat (pre-session)
☑ Enable session recording
☑ Enable share my desktop
☑ Enable concurrent remote sessions
☑ Enable remote command
☑ Enable 1-to-Many Scripting for team owner only
☑ Enable group-specific admin role (learn more)
☑ Enable showing currently logged-in Windows or Mac user (learn more)
☑ Allow members to access the Management tab
☑ Allow members to see groups
☐ Allow users to save Windows/Mac credential (entered when starting a session)
☐ Allow users to save security code (entered when starting a session)
☑ Allow multiple members to connect to the same computer.
☑ Allow members to establish concurrent sessions
☑ Allow members to disconnect others' sessions
☑ Allow members to reboot computers and restart streamers

Scheduled Access (GMT+00:00) UTC (change)

Notification Set up notification emails

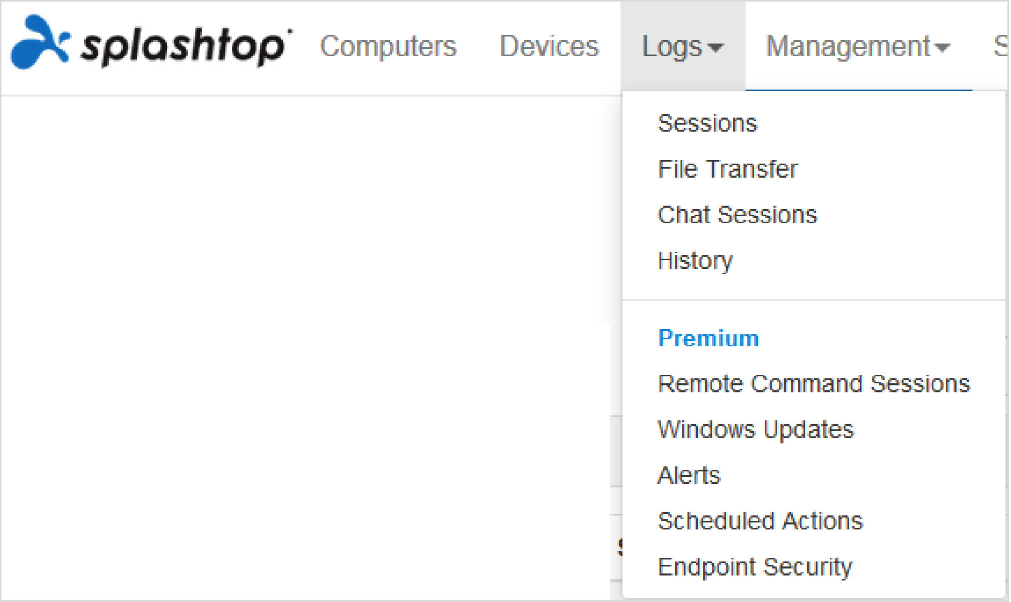
Two-Step Verification Manage trusted devices

By disabling the features highlighted in the screenshot above, you can prevent:

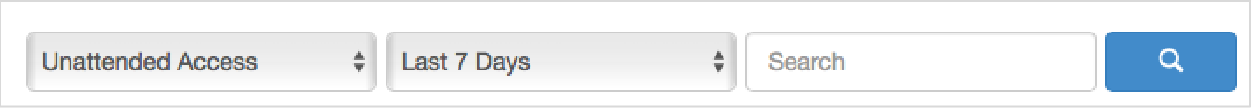
1. Multiple students from connecting to the same computer at the same time.
2. One student from remoting into multiple computers at the same time.
3. Students from disconnecting other students' connections.
4. Students from rebooting computers and restarting streamers.

9. Logs

Splashtop maintains logs for self auditing. Login to my.splashtop.com, then click on the "Logs" tab/menu. Team Owners and Admins will see the logs of everyone in the team. Members will only see their own logs.



Logs can show the last 7, 30, or 60 days of logs. If your service includes both unattended and attended access, you can choose which logs to view.

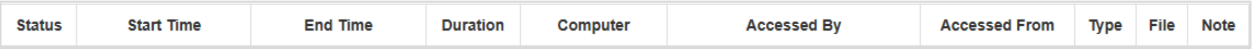

Unattended Access

Last 7 Days

If you scroll to the bottom of the page to "Export as CSV", you can download up to a year of logs.

Sessions

Session logs include all remote connections.

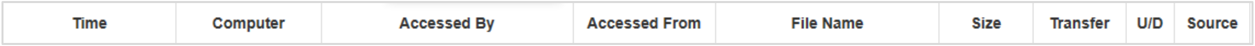


Status	Start Time	End Time	Duration	Computer	Accessed By	Accessed From	Type	File	Note

These logs include names and IP addresses of the 2 devices involved, time, user, and duration of the connections. It will also display the type of connection; Local or Remote. Local means both devices are on the same network and talk peer to peer. If there were any file transfers performed during the session, you can view the name of the file transferred.

File Transfer

Any in-session or off-session file transfers will be logged under this section.



Time	Computer	Accessed By	Accessed From	File Name	Size	Transfer	U/D	Source

These logs include the names and IP addresses of the 2 devices involved, time, user, filename, and size. It will also include whether the transfer was an upload or download. Upload means that the file was transferred from local to remote and Download means that the file was downloaded from remote to local. These logs do not include any contents of the files transferred.

Chat Sessions

Off-session chats will be logged in this section. The content of the chat session is not included.

History

These history logs show administrative actions, such as computers added/removed, group settings, permissions, etc. The logs note the time, account, IP address, and action.