Splashtop On-Prem

La solution d'accès et d'assistance à distance sur site, auto-hébergée.

Accès à distance hautement sécurisé et performant aux bureaux physiques et virtuels. Vous permet, ainsi qu'à votre équipe, d'accéder à des machines virtuelles et de contrôler à distance des bureaux physiques. Permet également au service informatique de prendre en charge à distance les appareils surveillés et non surveillés.

La solution la plus simple et plus rapide pour un accès et une assistance à distance hébergé sur site

Exploitez la puissance de la technologie sécurisée de Splashtop pour non seulement donner aux employés un accès à distance à leurs appareils, mais aussi pour permettre aux service informatique d'accéder à distance aux appareils et de les prendre en charge.

Principales caractéristiques et avantages

- **Haute performance** - Consultez le site Streaming 4K à 40fps et iMac Pro Retina 5K en streaming à faible latence. L'utilisation réduite du processeur offre une plus grande marge de manœuvre pour le traitement des demandes. Les réglages peuvent être affinés pour obtenir des performances optimales. Le moteur d'encodage et de décodage optimisé tire parti des dernières accélérations matérielles d'Intel, NVIDIA, AMD.
- **Prise en charge de plusieurs moniteurs** - Télécommande sur plusieurs moniteurs connectés à vos postes de travail.
- **Large support de dispositif** - Vous pouvez accéder à distance à votre ordinateur Mac, Windows ou Linux depuis n'importe quel appareil Mac, Windows, iOS, Android ou Chromebook.
- **Intégration d'Active Directory** - Pour faciliter le déploiement et la gestion informatique, Splashtop On-Prem vous permet d'utiliser Active Directory pour approvisionner facilement les comptes des utilisateurs et authentifier/autoriser chaque demande de session utilisateur.
- **Connexions sécurisées** - Obtenir une infrastructure sécurisée, une protection contre les intrusions, un cryptage SSL/AES 256 bits et autres des fonctions de sécurité avancées.
- **Support à distance autonome pour les Android/ appareils IOT robustes** - Splashtop On-Prem fournit un accès et une assistance à distance à tout appareil Android depuis n'importe quel ordinateur ou appareil mobile, même sans la présence d'un utilisateur final. Les appareils Android comprennent les téléphones intelligents, les tablettes, les terminaux de point de vente, les kiosques, les décodeurs et bien d'autres encore.
- **Console d'administration centralisée** - Les administrateurs informatiques peuvent facilement déployer et gérer l'accès à distance des employés aux ordinateurs à partir d'une console centralisée. Ils peuvent également fournir une assistance aux employés, avec ou sans surveillance, en se connectant à distance à leurs appareils.

Qui en bénéficie?

Les organisations qui cherchent à donner à leurs employés un accès à distance à leurs appareils ainsi qu'à fournir une assistance à distance facile et sécurisée pour les appareils.

- Les cadres peuvent rester au courant des affaires en accédant à distance et en analysant des données sensibles en toute sécurité, où qu'ils se trouvent.
- Les agents de terrain du gouvernement peuvent accéder aux applications sans avoir à télécharger des informations confidentielles.
- Les professionnels de la santé peuvent accéder en toute sécurité aux dossiers des patients tout en préservant la confidentialité.
- Les employés travaillant à distance peuvent accéder à leur ordinateur avec tous leurs fichiers et applications au bout des doigts.
- Les services informatiques peuvent accéder à distance et prendre en charge des appareils sans surveillance, ainsi que prendre en charge des ordinateurs non gérés sur demande.

Utiliser des commandes personnalisées pour la CAM/CAD 3D sur iPad

Exigences du système

Configuration requise pour le serveur de Splashtop

Systèmes d'exploitation supportés (version 32/64 bits)

- Windows Server 2008 R2 (Standard, Enterprise, DataCenter et Web Edition)
- Windows Server 2012, Windows Server 2012 R2
- Windows Server 2016 ou Windows Server 2019
- Windows 8 ou Windows 10

Exigences en matière de logiciels

- Exécuter avec le privilège d'administrateur

Configuration matérielle requise
Moins de 100 sessions simultanées

- Processeur : 4 cœurs 2,4 GHz ou plus
- Mémoire : 8 Go ou plus
- Disque dur : 60 Go ou plus sur le lecteur installé

Plus de 100 sessions simultanées

- Processeur : 8cores, 2,4 GHz ou plus
- Mémoire : 1 Go ou plus
- Espace disponible : 80 Go ou plus sur le disque installé

Exigences du client (dispositif client)

Installez l'application Splashtop On-Prem :

- iPad ou iPhone - iOS version 12.x ou supérieure
- Android - Version 4.0 ou supérieure
- ARM 32/64, processeur X86 ou Nvidia Tegra
- Windows - XP, Vista, 7, 8 ou 10
- Mac - macOS 10.8 ou supérieur

Exigences en matière de streaming (ordinateur hôte)

- Windows 10, Windows 8/8.1, Windows 7, Windows Vista*, Windows XP*, Server 2016, 2012, 2008, 2003* (le noyau du serveur n'est pas pris en charge)
- Windows Server 2008 R2 ou supérieur
- Mac OS 10.8 ou supérieur
- Android 4.0 ou supérieur
- iOS 12.x ou supérieur (pour SOS on-prem)
- Linux Ubuntu desktop 16.04, 18.04, et 20.04, CentOS 7 et 8, Red Hat Enterprise Linux (RHEL) 7.3-8.1, Fedora 29-31

Exigences en matière de matériel

- Processeur : 1,6 GHz ou plus rapide, double cœur
- Mémoire : 2 Go ou plus
- Connexion au réseau

Exigences du réseau

- Une adresse IP et un nom de domaine : si vous avez besoin d'une session à distance de pare-feu croisé, veuillez préparer une adresse IP publique pour la passerelle Splashtop ou paramétrer le transfert de port de l'adresse IP publique vers l'adresse IP privée dans votre pare-feu.
- Un port :
  Passerelle Splashtop et port relais : 443 (par défaut).
  Veuillez vous assurer que le port 443 n'est pas bloqué par votre pare-feu.

030121

Remote Support

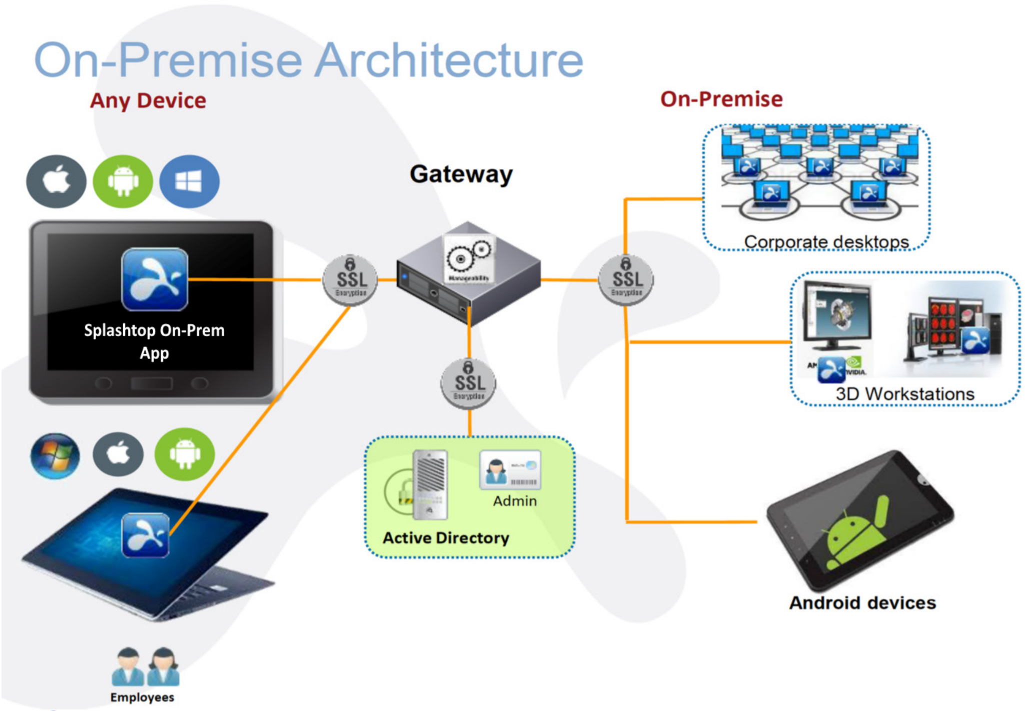
Les équipes informatiques peuvent fournir un support rapide et attentif aux appareils Windows, Mac, iOS et Android sans installation préalable, en utilisant un code de session à 9 chiffres. Elles peuvent également se connecter à distance sur des ordinateurs gérés sans la présence d'un utilisateur final pour fournir une télé-assistance ou s'assurer que les ordinateurs sont à jour.

Prix

Chaque utilisateur ou administrateur peut accéder, contrôler et prendre en charge des ordinateurs physiques, des ordinateurs virtuels, des bureaux virtuels et des appareils Android à partir de tous leurs appareils mobiles et ordinateurs.

Les prix sont basés sur le nombre d'utilisateurs et d'ordinateurs. Contactez-nous pour les prix.

Économisez 50 % ou plus par rapport aux autres solutions d'accès et d'assistance à distance.



La session de contrôle à distance avec un appareil Zebra vous permet de transférer des fichiers, d'enregistrer des sessions et plus encore ! Vous pouvez lancer une session à distance à partir de votre appareil mobile ou de votre ordinateur.

Splashtop On-Prem Features

Key Features	Flexible licensing – Choose named end-user licenses and/or concurrent technician licenses	
	End-user License	Technician License
HD quality, fast connections in real-time, frame rates up to 60 fps, minimized latency, performance indicator, quality settings and more	✓	✓
Remotely access computers and servers running Windows XP/7/8/10, Windows Server 2003/2008/2012/2016, macOS / Mac OSX 10.8+, Linux Ubuntu Desktop 16.04, 18.04, and 20.04, CentOS 7 and 8, RHEL 7.3-8.1, Fedora 29-31	✓	✓
Unattended support (Windows, Mac, Android)	✓	✓
Remotely access mobile device - remote view (iOS, Android 5.0 or later), remote control (Android 5.0 or later with supported add-on, Android 8.0 or later for all IoT/Rugged devices)	✓	✓
Remote from Windows, Mac, iOS, and Android	✓	✓
View computer status, inactive time, streamer version, logged-in user	✓	✓
Multi-monitor support – (multi-to-one & multi-to-multi)	✓	✓
Lock remote screen	✓	✓
Blank remote screen in session	✓	✓
Lock remote keyboard and mouse in session	✓	✓
File transfer (including drag-and-drop file transfer and Windows copy/paste file transfer)	✓	✓
File transfer outside of a remote access session	✓	✓
Remote print	✓	✓
Chat (in-session & outside session)	✓	✓
Session recording	✓	✓
Remote wake (Wake on LAN)	✓	✓
Remote reboot (normal reboot & safe mode reboot)	✓	✓
Audio	✓	✓
Remote command	✓	✓
Two technicians can remote into one machine	✓	✓
View-only Mode - Select “View Only” in the session toolbar during a remote access session to only view activity and annotate the remote computer screen, not remotely control it	✓	✓
Schedule remote computer access for end-users	✓	✓
Microphone Passthrough - Transmit input via your local microphone to the remote computer as the microphone input (Windows only)	✓	✓
USB Device Redirection - Redirect a USB device (smart card reader, security key, stylus/HID device, or printer) on your local computer to the remote computer. The redirected device works on the remote computer as if it's plugged in directly at that computer (Windows only)	✓	✓
Apps available in English, French, German, Spanish, Italian, Portuguese, Japanese, and Simplified Chinese	✓	✓

Manageability		
Web console for computer and user management	✓	✓
Group permission	✓	✓
User management	✓	✓
Logging of connections, file transfers and management activity	✓	✓
Active Directory integration	✓	✓
Computer and user grouping	✓	✓
Enable Admin to enforce session recording and upload to a target folder	✓	✓
Splashtop Connector (RDP)	✓	✓
Restrict access to Gateway based on user IP	✓	✓
Export log data to a syslog server for SIEM system to retrieve and analyze	✓	✓
Security		
On-premise deployment	✓	✓
SSL certificate import	✓	✓
256-bit AES encryption	✓	✓
Two-step verification	✓	✓
Require Windows or Mac password	✓	✓
Request permission upon connection	✓	✓
Customize watermark content	✓	✓
Set browser timeout	✓	✓
Enhanced Android and IoT Management		
1-to-Many actions for apk push-install, remote reboot and file dispatch	✓	✓
Hardware and software system inventory and reporting	✓	✓
Attended Remote Support		
Attended/quick support for on-demand access to unmanaged Windows, Mac, Android, and iOS with a 9-digit access code		✓
Reboot and reconnect during attended support session		✓
Connect as Admin option to fully interact with UAC and perform privileged operations during attended support session		✓
Launch a remote session from within your Freshservice ticket		✓
Create a custom branded SOS app for Windows and Mac with your logo, text, colors		✓

splashtop®

Splashtop On-Prem Admin Guide

December 2021

Table of Contents

Company Information

Headquartered in San Jose, California and founded in 2006, Splashtop Inc. delivers the best-in-class remote access, remote support, cross-screen productivity and collaboration experience – bridging smartphones, tablets, computers, TVs, and clouds.

More than **30 million** users have downloaded Splashtop from app stores, and manufacturing partners including HP, Lenovo, Dell, Acer, Sony, Asus, Toshiba, Intel and others have shipped Splashtop software on more than **100 million** devices.

Splashtop Inc.
1054 S. De Anza Blvd., Suite 200
San Jose, CA 95129, U.S.A.

Introduction

Splashtop On-Prem is an On-premise solution that can be totally self-hosted inside enterprise network. With a centralized database and management console, the IT admin could conveniently tackle the system security while providing easy and smooth remote control experience to the users.

The Team Owner is able to customize a deployment package, which will exempt the end users from tedious installation and configuration steps.

Remote controlling becomes extremely easy and comfortable with **Splashtop On-Prem** applications. You can basically work on a remote computer as if you were sitting in front of it, without worrying about the slow and sluggish connection over VPN.

Features of Splashtop On-Prem

You can also enjoy the variety of features that are built into our **Splashtop On-Prem** solution. Click on individual name of the features to explore more.

HD quality remote performance: Splashtop On-Prem for Remote Access and Support uses the same high-performance engine that powers our award-winning consumer and mid-market products used by millions. HD quality, fast connections in real-time, and multiple concurrent sessions.

Multi-to-multi monitor: View multiple remote screens from multi-monitor systems at the same time, including multi-to-one and multi-to-multi. Even multi-monitor for Mac!

File transfer: Transfer files quickly thanks to our fast and secure connections. You can drag-and-drop files between computers and also transfer files without starting a remote session!

Chat: Chat with the user at the remote computer while in a session or outside a session.

Remote reboot: Reboot the remote computer from your Splashtop app or web console. Choose Normal or Safe Mode reboot.

Remote wake: Remotely wake up your computer. The target computer must support Wake-on-LAN (WoL) and be connected by an Ethernet cable. And another computer on the same network must be powered on.

Remote print: Print files on a remote computer to a local printer. No need to transfer files, and no need to fax printed documents. Just select the file you need from your remote computer and print it on your local printer instantly.

Session recording: Record remote access sessions. Use the Screen Recording button in your remote access window to start and stop recording. All recordings are saved to your local computer.

AD integration: Microsoft Active Directory (AD) is now integrated with Splashtop On-Prem for Team Owner to easily manage permissions and access to computers and devices. Microsoft Windows Server 2012, 2016 and 2019 supported.

2-step verification: 2-step verification, also known as multi-factor authentication (mfa), elevates the security of user's account by deploying a second device which issues a time-dependent dynamic password to verify the credential. Your account is safer now with 2-step verification!

and more...

Usage scenarios

Splashtop On-Prem is designed to fit into different usage scenarios. Generally, Splashtop On-Prem can be deployed in one of the three modes: remote access, unattended support or attended support

Remote access

REMOTE ACCESS provides individuals and teams with convenient remote access to Windows PCs and Macs from a computer, smartphone or tablet anywhere anytime - just like the user is sitting in front of the computer. If you are looking for an alternative to LogMeIn Pro or GoToMyPC, choose Splashtop On-Prem remote access.

Unattended support

UNATTENDED SUPPORT works best for the scenario where an IT personnel is managing a bunch of dispersed computers and devices, and remote access to these computers and devices from one single computer would undoubtedly boost his productivity tremendously.

What needs to be done is to install and pre-configure an agent (the Streamer) in each of the remote devices, and they'll be always ready to connect.

Attended support (SOS)

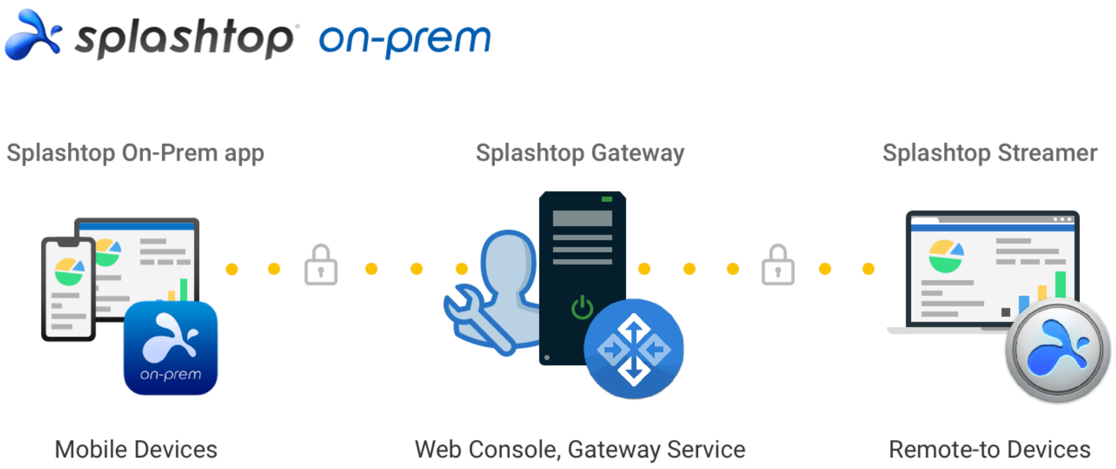
ATTENDED SUPPORT is a perfect solution for Service Desks and MSPs, and it provides the most convenient way for a technician to establish an ad-hoc remote session, without needing the end user to install any software or plug-in in the computer. Instead, the end user just downloads and launches a standalone application named **SOS** and provides the displayed code to the technician.

It is also the most cost-effective solution. With one single license, a technician can connect to unlimited number of computers to make sure every support request is well entertained.

If you are looking for an alternative to TeamViewer, LogMeIn Rescue or GoToAssist, choose Splashtop On-Prem attended support.

Installation

Key Components



- **Splashtop Gateway:** Performs Gateway, Relay, User, and Device management functions. This is the central server that authenticates, secures, and connects users and devices. It provides a Web Console to configure (and report of) users and devices. It is designed to install on a Windows server.
- **Splashtop On-Prem app:** Application makes it possible to establish remote sessions between local device and the target remote device running Splashtop Streamer.
- **Splashtop Streamer:** Software needs to be installed and running on the remote device you would like to access to. It streams audio and video to the On-Prem app device.

Download Installation Package

As an On-premise hosting solution, most components are packaged into the **Splashtop Gateway** installation package, with varies platforms support. Users should be able to download and install **Splashtop Streamer** and **Splashtop On-Prem app** after the success of **Gateway** initial setup.

- *For **Splashtop Gateway** installation package,* please refer to Splashtop Gateway publish announcement page
- *For **Splashtop Streamer** installer*, please refer to this article on how to get the right Splashtop Streamer installer
- *For **Splashtop On-Prem** app installer*, please refer to this article on how to get the right Splashtop On-Prem app

In addition to regular Splashtop Gateway releases with the packaged components, Splashtop will release **Splashtop Streamer** and **Splashtop On-Prem app** for patches, such components will be released as PKG files, that are only available for Team Owner to import into Gateway, before they are ready for users to download from Gateway, please refer to Software section in System Configuration on how to download and import new components into Splashtop Gateway.

System Requirements

Requirements for Splashtop Gateway Server

- **Operating System** (32/64-bit version)
  - Windows Server 2008 R2 (Standard, Enterprise, DataCenter, and Web Edition)
  - Windows Server 2012, Windows Server 2012 R2
  - Windows Server 2016
  - Windows Server 2019
  - Windows 8
  - Windows 10
- **Software**
  - Run with Administrator privilege
- **Minimum Hardware Spec (less than 100 concurrent sessions)**
  - Processor: Intel Core i5 2.0 GHz or above
  - Memory: 8 GB or above
  - HDD: 30 GB or above on installed drive

- Recommended Hardware Spec (more than 100 concurrent sessions)
  - Processor: 4 cores, 2.4 GHz or above
  - Memory: 16 GB or above
  - HDD: 60 GB or above on installed drive

Requirements for On-Prem app Devices

- **iPad or iPhone**
  - iOS 12.x or higher
- **Android**
  - Android 4.0 or higher
  - ARM 32/64, X86 processor or nVidia Tegra
- **Windows**
  - Windows XP, Vista, 7, 8, or 10
- **Mac**
  - macOS 10.8 or higher

Requirements for Streamer Devices

- **Operating System**
  - Windows XP, Vista, 7, 8, or 10, Windows Server 2008 R2 or higher
  - Mac OS 10.8 or higher
  - Android 5.0 or higher
  - iOS 12.x or higher (for SOS on-prem)
- **Hardware**
  - Processor: 1.6 GHz or faster dual-core CPU
  - Memory: 2 GB or above
  - Network connection

Requirements for Network

Internet-based Remote Session

Splashtop On-Prem is an On-premise solution and can be completely self-hosted on your office LAN network. But there are times that you need access your office computer from home or somewhere else, and connections must be established through the Internet.

To enable Internet-based remote session in Splashtop On-Prem, you can set up the system with a couple of options:

- Deploy the Splashtop Gateway Server in a DMZ network
- Assign a public IP address to the Splashtop Gateway Server
- Set port forwarding from a public IP to the private IP assigned to Splashtop Gateway Server
- Host the Splashtop Gateway Server on cloud
- Install VPN application in client devices

Firewall Port

By default port 443 is used by Splashtop Gateway to communicate with the Streamers and client devices, therefore it is important to make sure port 443 is not blocked by your network firewall or OS firewall, nor occupied by other applications.

The following Ports should not be occupied and blocked by your firewall:

- port number: **443**
- Port number: **9080**
- Port number: **5432**
- Port number: **7080**
- Port number: **7081**

Quick Installation Guide

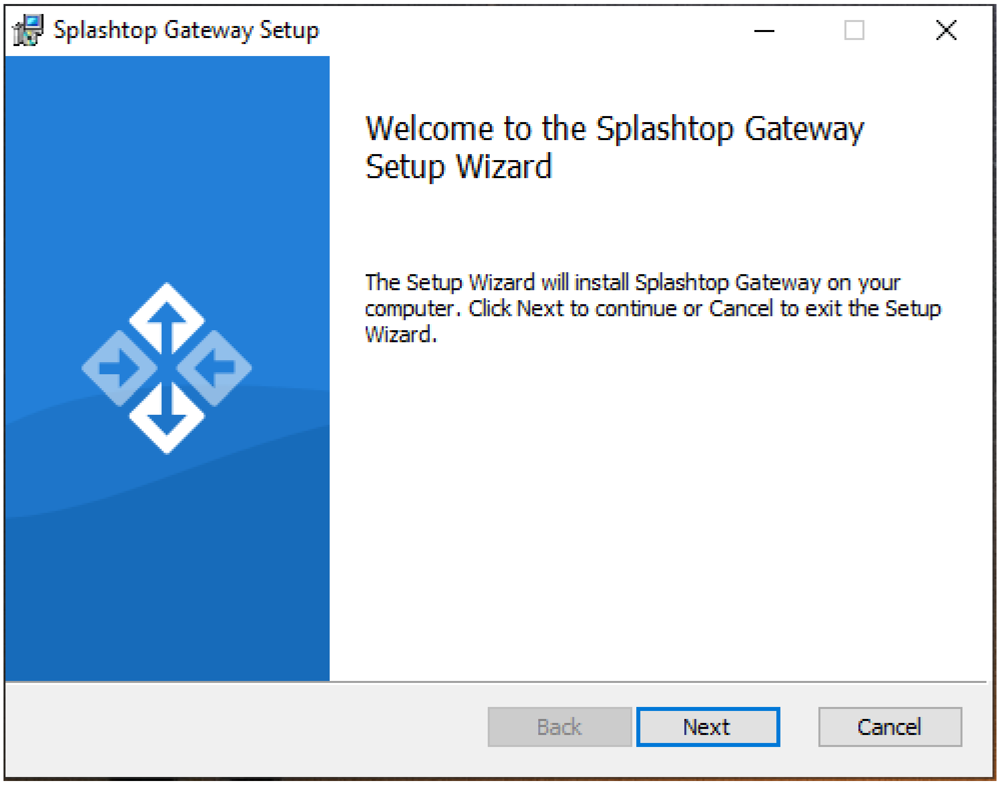
The basic steps to get Splashtop software up and running will typically look like the followings. The first five steps should be done by you, the Team Owner or Admin, and the remaining two will be done by the users

1. Team Owner sets up Splashtop Gateway on the company network.
2. Team Owner groups the computers as desired, and sets permissions accordingly.
3. Team Owner creates user accounts
4. Team Owner notifies users that they have been added to Splashtop Gateway, and provides specific credentials to them such as activation code and password.
5. Team Owner or Admin deploys the Streamers and install them on all the target computers available for users to remote access.
6. User downloads the Splashtop On-Prem client app via Splashtop Gateway web console to his/her device and install.
7. User launches Splashtop On-Prem client app and enter Gateway IP address, account name and password given by Team Owner or Admin. User can then establish a secured remote session with a computer in work environment.

Splashtop Gateway and Splashtop Steamer can be installed on the same Windows server. In fact, it is a good practice since remote access to that server can be provided in case Team Owner needs to configure Splashtop Gateway settings or restart the Splashtop Gateway service.

1. Install Splashtop Gateway

a) Download your program and double click the MSI file to begin installing by going through Windows Install Wizard.

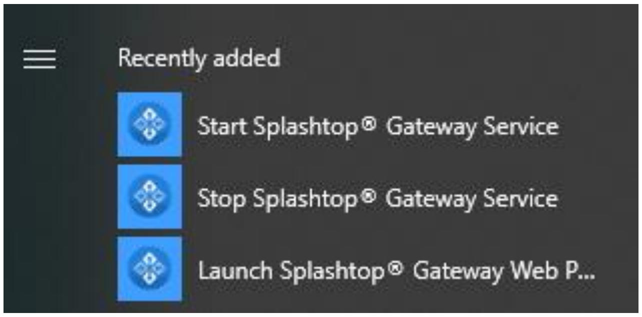


Splashtop Gateway Setup

Welcome to the Splashtop Gateway Setup Wizard

The Setup Wizard will install Splashtop Gateway on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

b) After the installation finished, go to Windows Startup menu in which 3 startup shortcuts just created. Click Launch Splashtop Gateway web portal to start gateway web console in your default browser.

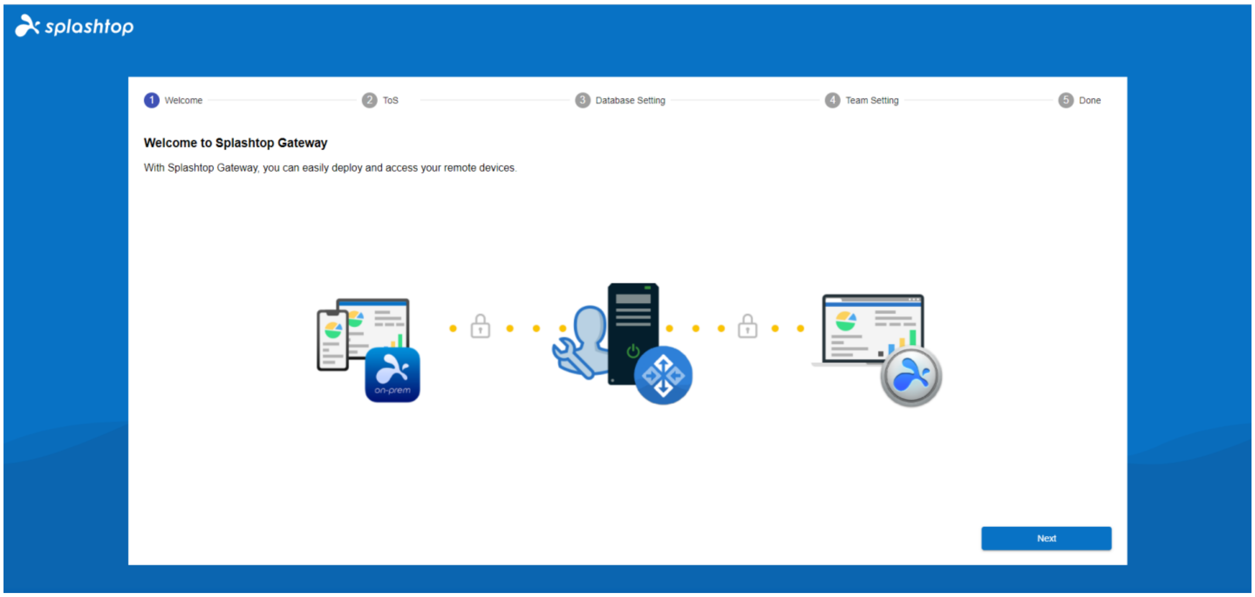


Recently added
Start Splashtop® Gateway Service
Stop Splashtop® Gateway Service
Launch Splashtop® Gateway Web P...

Note: We highly recommend using **Google Chrome** to navigate Splashtop Gateway web console.

2. Splashtop Gateway OOBE Setup

a) Once launched the web console from browser for the first time, an OOBE setup procedure containing Terms of Service will show up. Click next to continue.

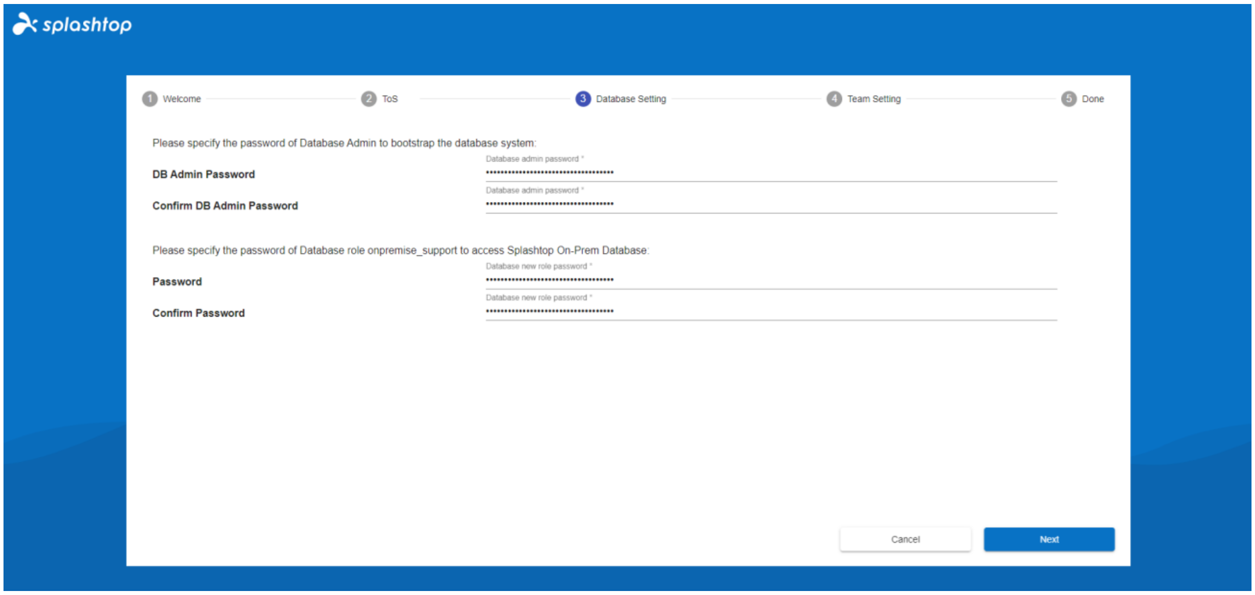


Welcome to Splashtop Gateway

With Splashtop Gateway, you can easily deploy and access your remote devices.

b) Set up your Splashtop Gateway Database management and access passwords. Please allow 30 seconds for Database initializing at this step.

Note: Please write down your Database passwords and saved in a secured place since there will be no way to change DB passwords later on.



Please specify the password of Database Admin to bootstrap the database system:

DB Admin Password — Database admin password * ••••••••••••••••••••••••••••••••

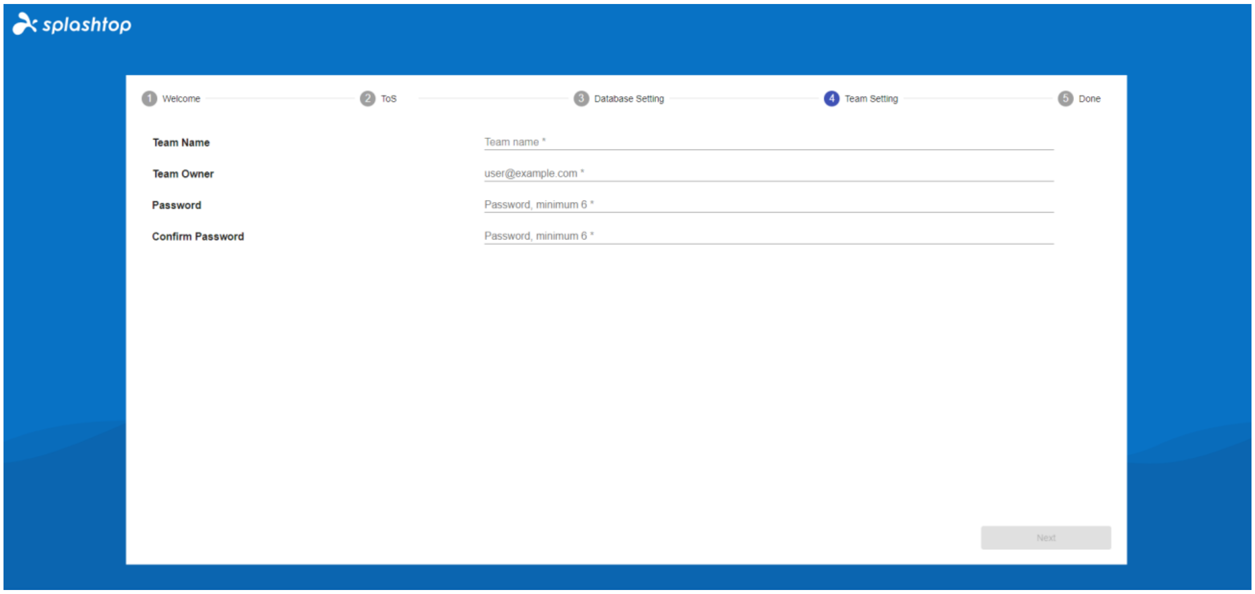
Confirm DB Admin Password — Database admin password * ••••••••••••••••••••••••••••••••

Please specify the password of Database role onpremise_support to access Splashtop On-Prem Database:

Password — Database new role password * ••••••••••••••••••••••••••••••••

Confirm Password — Database new role password * ••••••••••••••••••••••••••••••••

c) Establish your first team and owner by entering E-mail account and credentials to finish the OOBE setups.



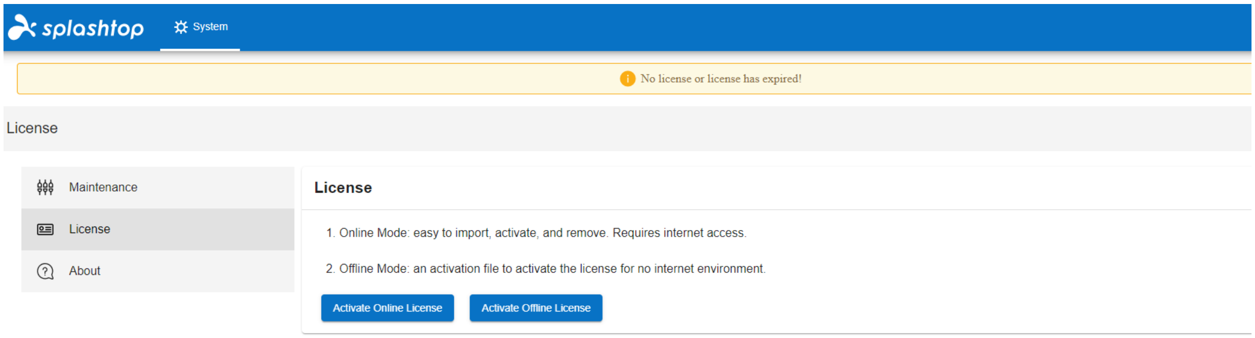
Team Name — Team name *

Team Owner — user@example.com *

Password — Password, minimum 6 *

Confirm Password — Password, minimum 6 *

d) Once OOBE setup completed, log in to web console with the credentials just created. You will need to activate online or offline license based on license mode tailored for you. (See Section 3)



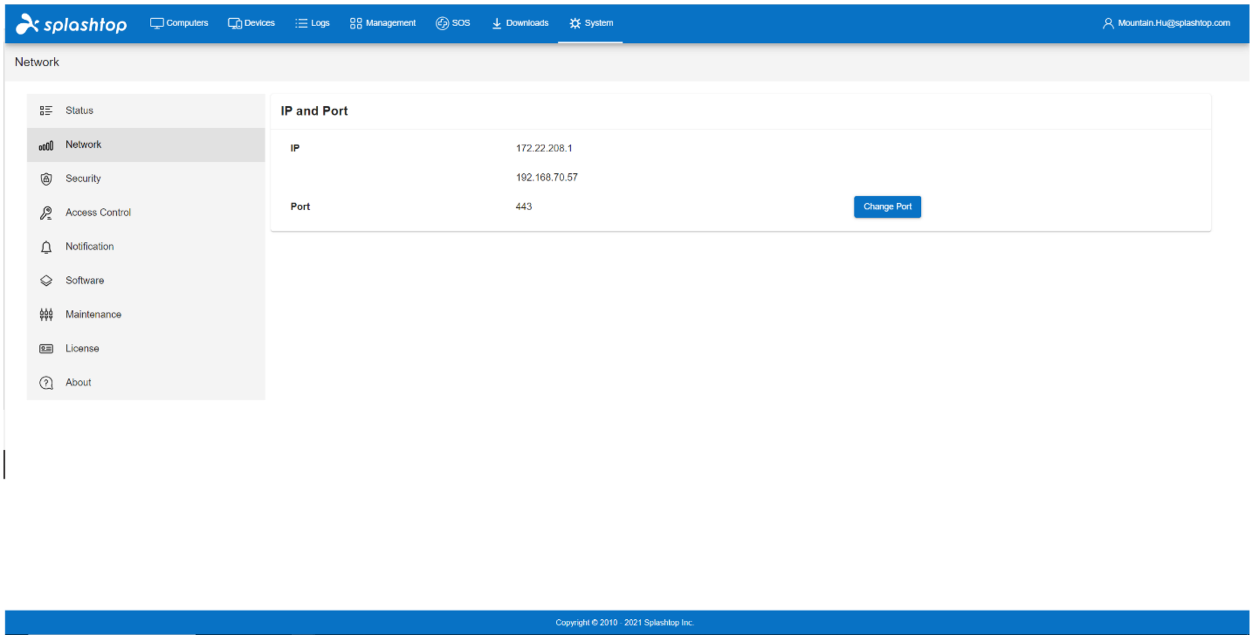
No license or license has expired!

License

1. Online Mode: easy to import, activate, and remove. Requires internet access.

2. Offline Mode: an activation file to activate the license for no internet environment.

e) When Splashtop On-Prem activated, you can log in to Splashtop Gateway – System – Network to see your Ethernet/ Wireless IP addresses and port number as shown in below screenshot. The IP address displayed in this page is the **Gateway IP address** which will be filled up along with your **port number** (**443** by default) when sign in **On-Prem Client Application** as well as **Splashtop Streamer**.



IP and Port

IP	172.22.208.1 192.168.70.57
Port	443

Copyright © 2010 - 2021 Splashtop Inc.

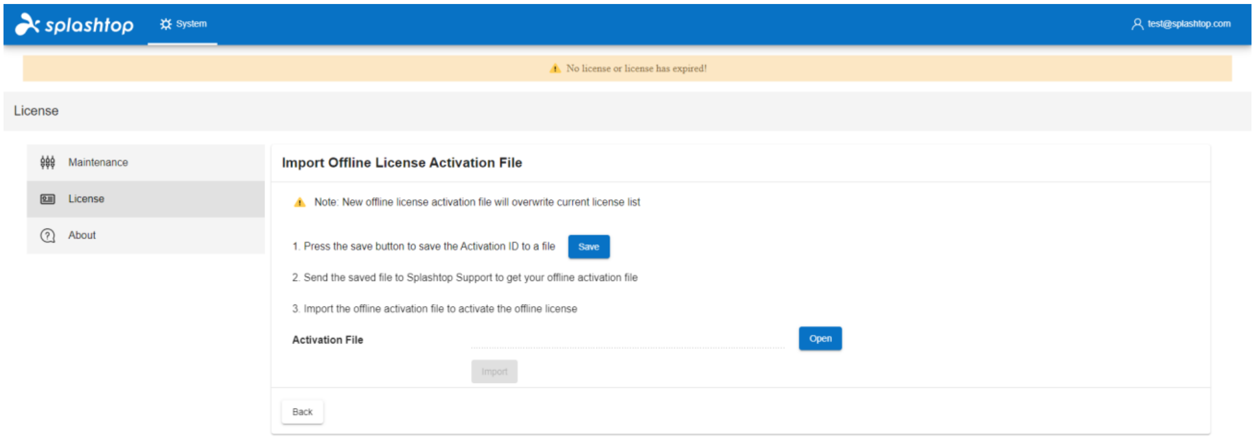
3. Activate Splashtop Gateway via License

Splashtop Gateway **must** be activated by a valid license to use.

Login into https://{gatewayaddress} with System Owner, navigate to **System** > **License** page to import a license to activate.

Splashtop Gateway provides both **Online** and **Offline** license activation.

- **Online activation:** Internet access is required to activate online license, once the Gateway is activated, it can be moved to offline environment.
- **Offline activation**: Click **Save** to download your activation ID and send it to our support. An activation file shortly will be sent back to proceed activation. Please follow the instructions on the web console. (See below)



No license or license has expired!

Import Offline License Activation File

Note: New offline license activation file will overwrite current license list

1. Press the save button to save the Activation ID to a file
2. Send the saved file to Splashtop Support to get your offline activation file
3. Import the offline activation file to activate the offline license

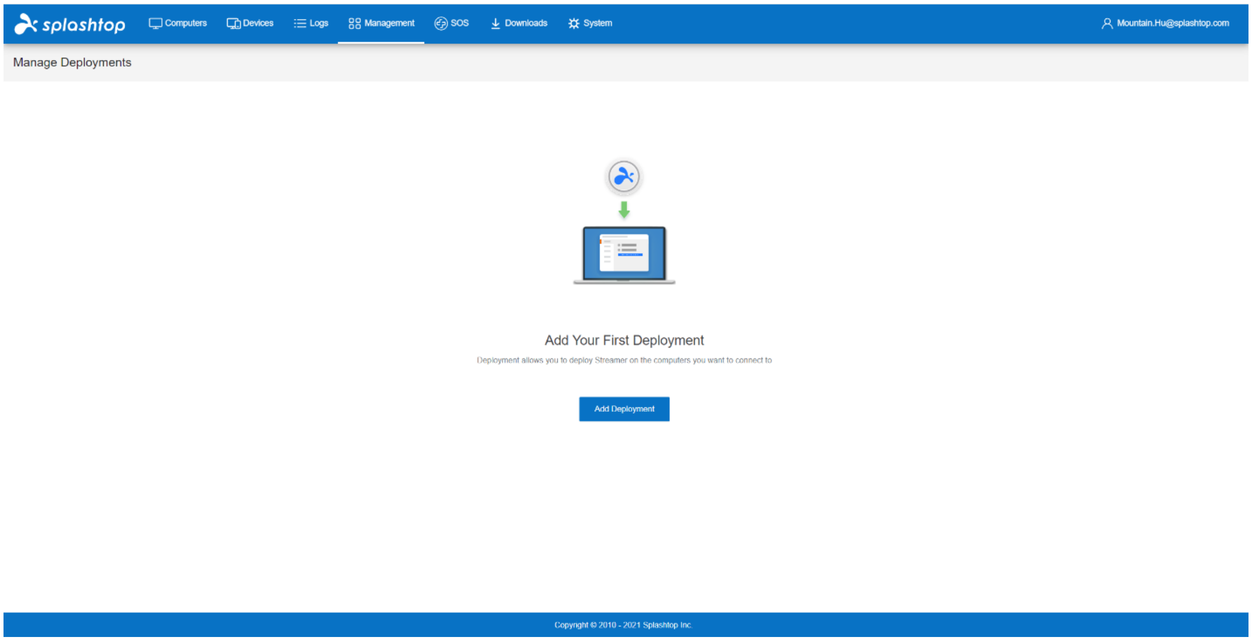
Activation File

4. Deploy Splashtop Streamer

Below instruction taking deploy Splashtop Streamer on Windows as an example, for more deploy info please refers to Deployment related support articles.

On the computers that you'd like to connect to, the Splashtop Streamer must be installed. This can be done in 3 easy steps.

1. **Go to** Splashtop Gateway Web Console > *Management* > *Deployment.* Click ***+Add Deployment*** button to create a new deployment package. A deployment package consists of a deployment streamer and a unique 12-digit deployment code.

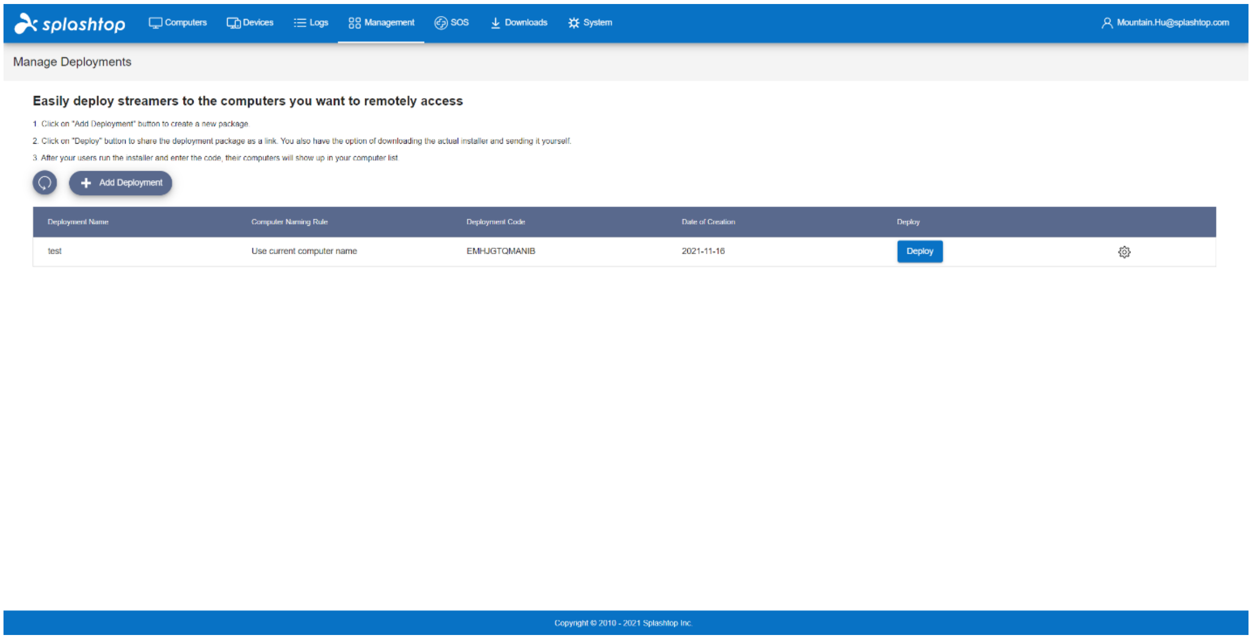


Manage Deployments

Add Your First Deployment

Deployment allows you to deploy Streamer on the computers you want to connect to

2. Select ***Deploy*** for the package that was just created.



Manage Deployments

Easily deploy streamers to the computers you want to remotely access

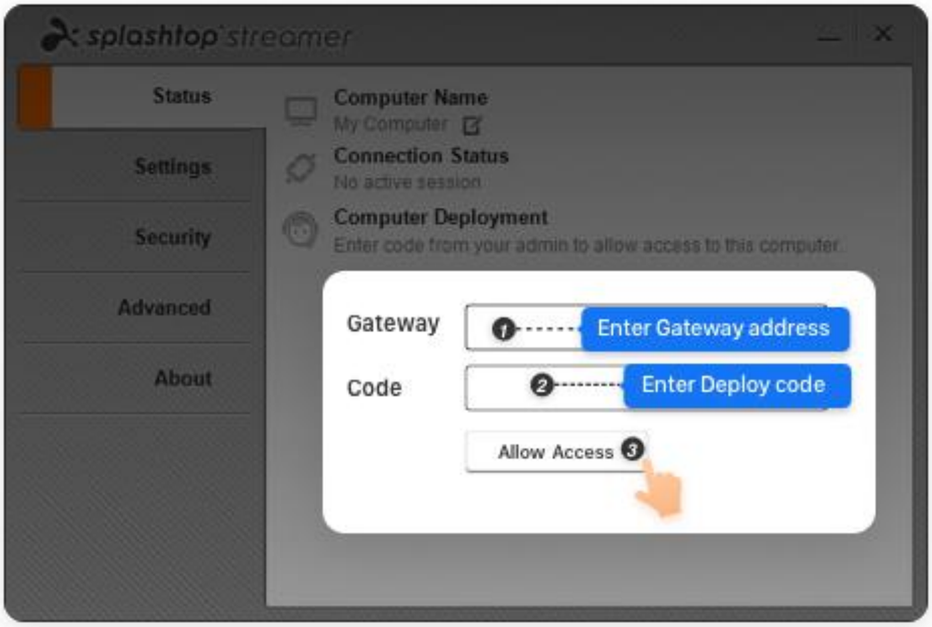
1. Click on "Add Deployment" button to create a new package
2. Click on "Deploy" button to share the deployment package as a link. You also have the option of downloading the actual installer and sending it yourself.
3. After your users run the installer and enter the code, their computers will show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

Deployment Name	Computer Naming Rule	Deployment Code	Date of Creation	Deploy	
test	Use current computer name	EMHJGTQMANIB	2021-11-16	Deploy	⚙

3. **Have your users install the streamer.** You can send the deployment package link to your users. By clicking the link, your users can download the streamer installer and run the file. You

can also send the streamer installer file and its associated deployment code directly to your users (via Dropbox, email, etc.).

4. When the **Splashtop Streamer** App has finished installing, the user can input the **Splashtop Gateway server's IP address** with default **port number 443** in conjunction with the deploy code obtained from Team Owner or Admin to log in. Users who don't have this information will need to ask the IT department for it.

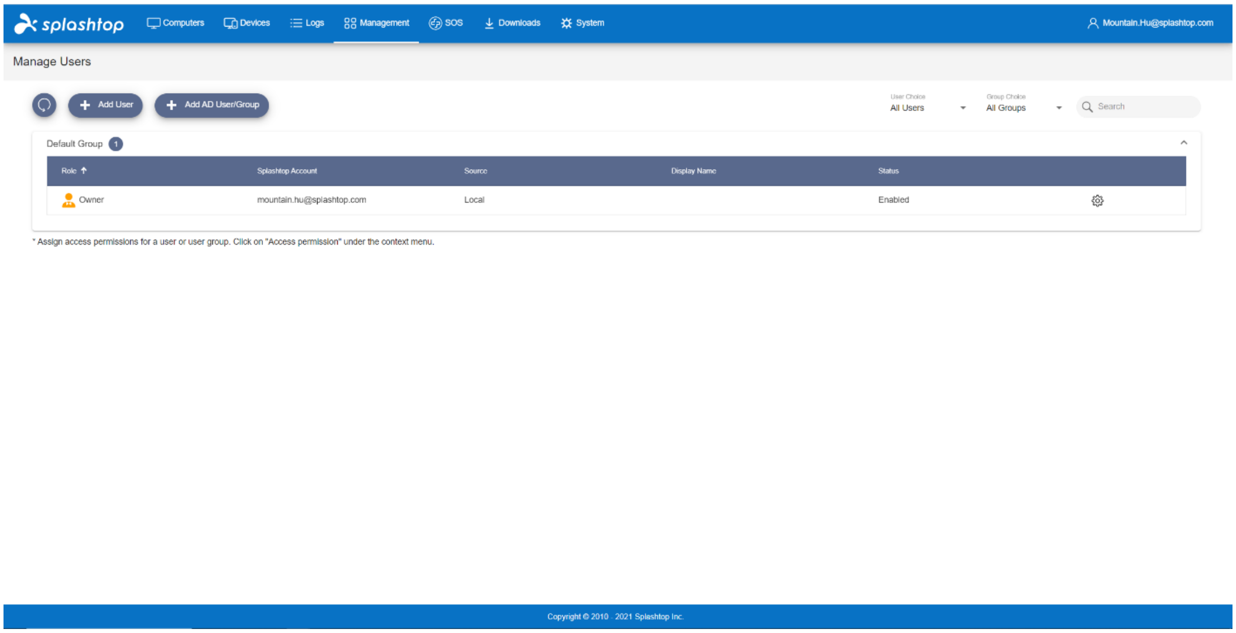


5. Create user accounts

Create Remote Support / Remote Access users

System Owner or Team Admin can create user allowing centralized user management in Splashtop Gateway.

1. Go to Splashtop Gateway Web Console > Management > Users. Press +***Add User button*** to create a new user.



Manage Users

User Choice: All Users

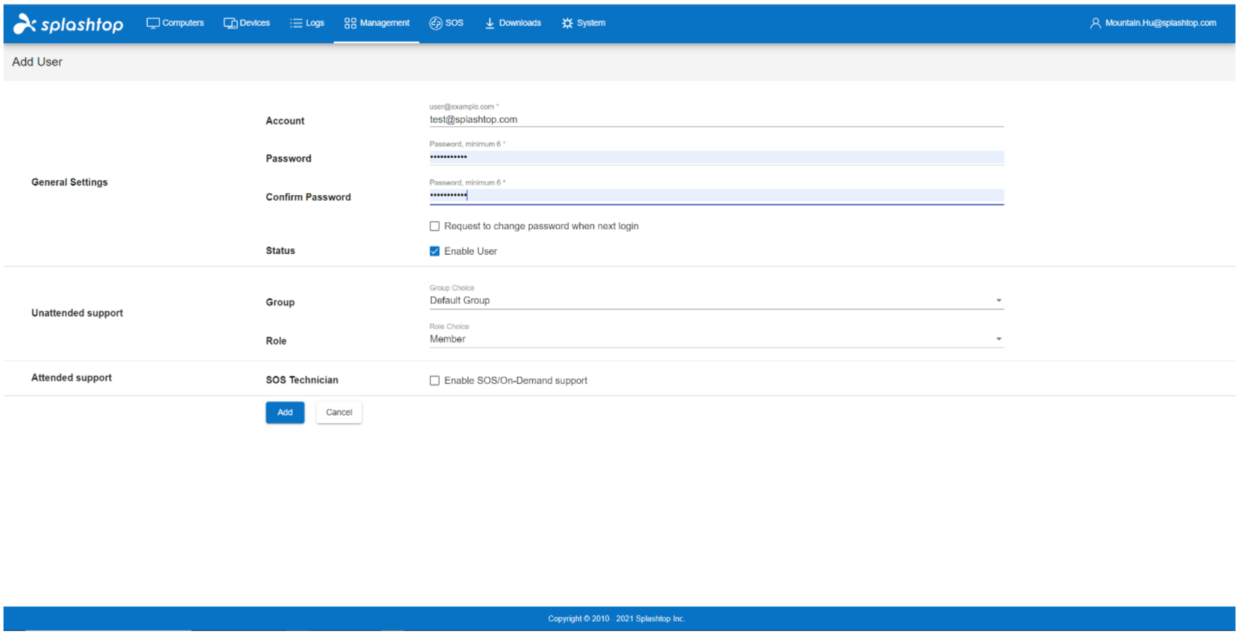
Group Choice: All Groups

Default Group 1

Role ↑	Splashtop Account	Source	Display Name	Status
Owner	mountain.hu@splashtop.com	Local		Enabled

* Assign access permissions for a user or user group. Click on "Access permission" under the context menu.

2. Team Owner or Team Admin sets the user role and group type during user creation process.



Add User

General Settings

Account: user@example.com * test@splashtop.com

Password: Password, minimum 6 * •••••••••••

Confirm Password: Password, minimum 6 * •••••••••••

☐ Request to change password when next login

Status: ☑ Enable User

Unattended support

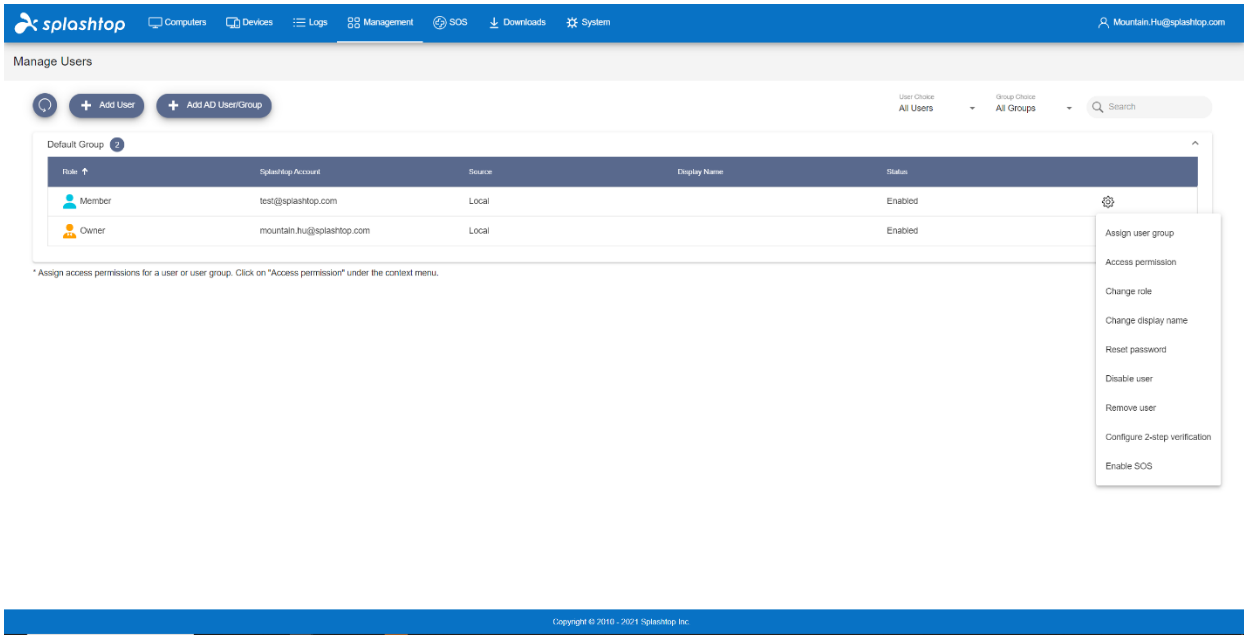
Group: Group Choice Default Group

Role: Role Choice Member

Attended support

SOS Technician: ☐ Enable SOS/On-Demand support

3. Team Owner or Team Admin can assign user access permission to specific devices or groups by clicking Access Permission from context drop-down menu (Gear Button).



Manage Users

User Choice: All Users
Group Choice: All Groups

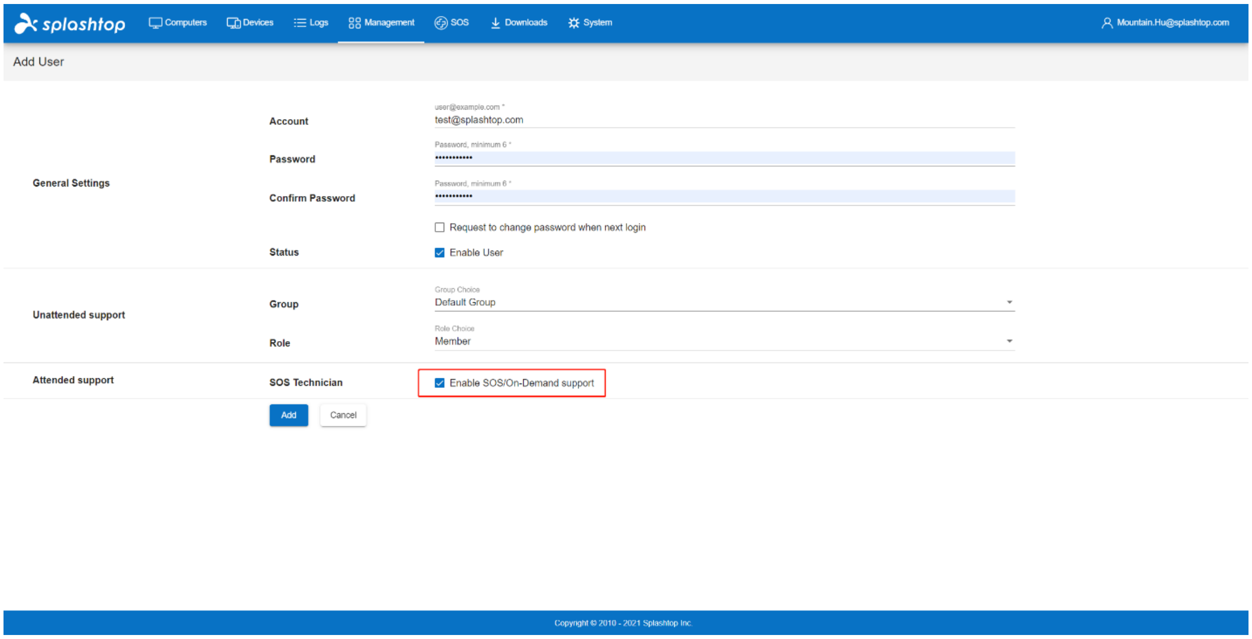
Default Group 2

Role ↑	Splashtop Account	Source	Display Name	Status
Member	test@splashtop.com	Local		Enabled
Owner	mountain.hu@splashtop.com	Local		Enabled

* Assign access permissions for a user or user group. Click on "Access permission" under the context menu.

Create users with additional On-Demand Support/SOS capability

a) Team owner or admin can enable a user's SOS capability either from user creation page or user's property drop-down.



Add User

General Settings

Account: user@example.com * test@splashtop.com

Password: Password, minimum 6 * •••••••••••

Confirm Password: Password, minimum 6 * •••••••••••

□ Request to change password when next login

Status: ☑ Enable User

Unattended support

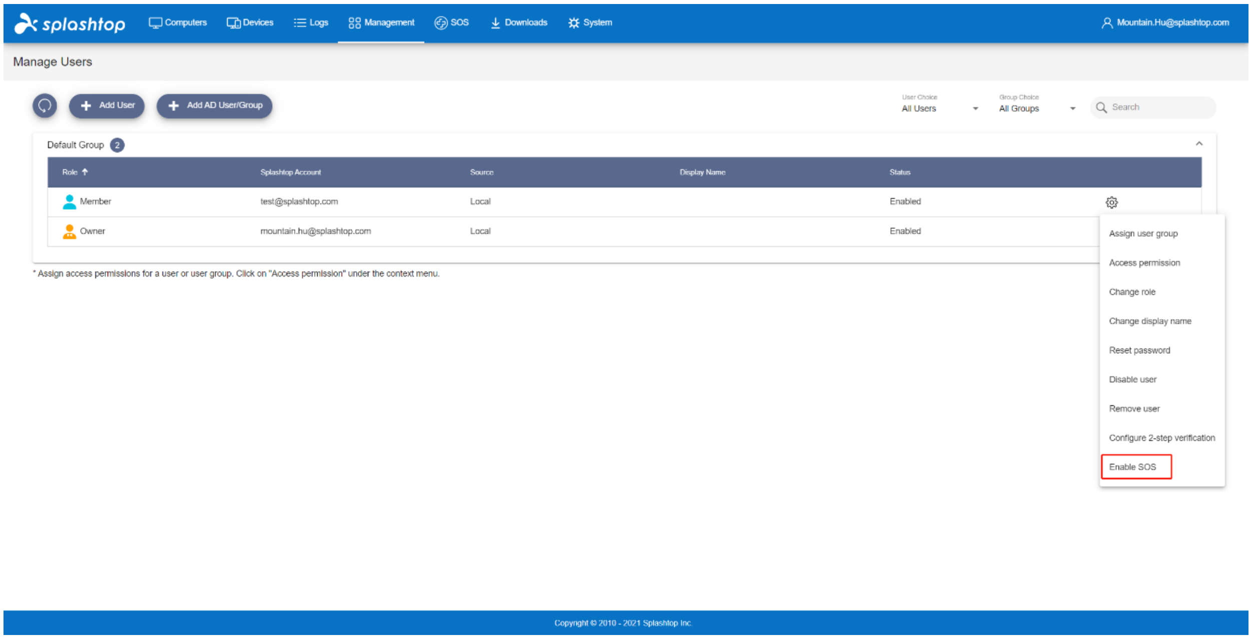
Group: Group Choice Default Group

Role: Role Choice Member

Attended support

SOS Technician: ☑ Enable SOS/On-Demand support

b) Created remote support user can be granted SOS feature via user property drop-down.



Manage Users

User Choice: All Users

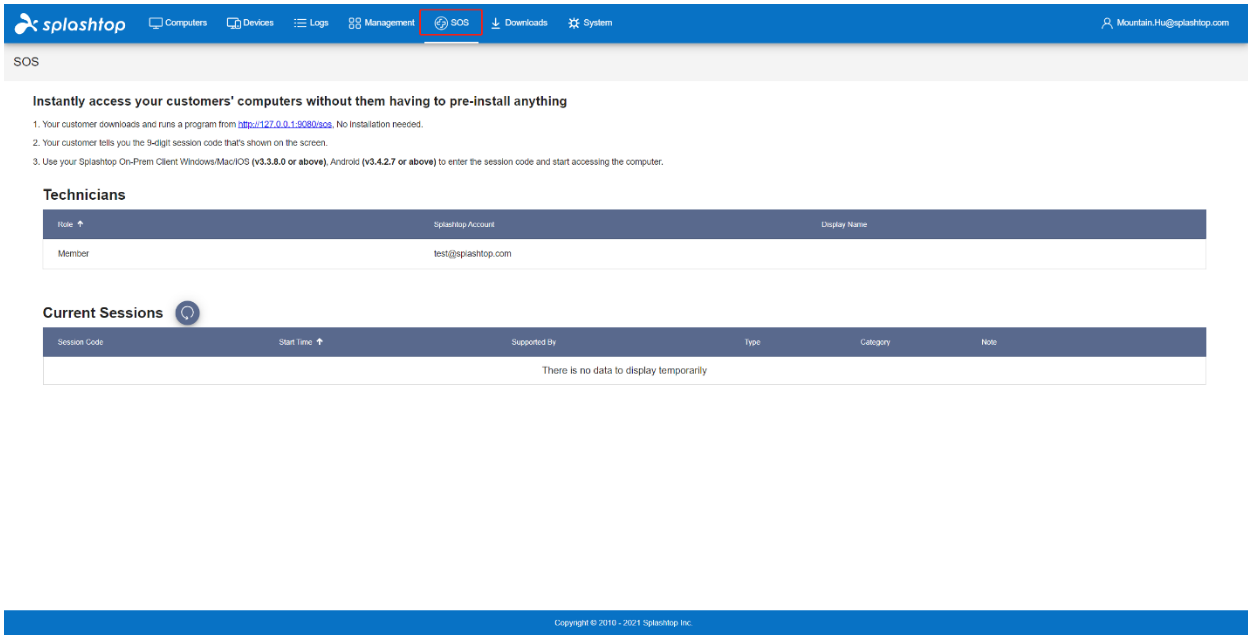
Group Choice: All Groups

Default Group 2

Role ↑	Splashtop Account	Source	Display Name	Status
Member	test@splashtop.com	Local		Enabled
Owner	mountain.hu@splashtop.com	Local		Enabled

* Assign access permissions for a user or user group. Click on "Access permission" under the context menu.

c) Users with SOS capability can be found in the SOS page on web portal.


splashtop
Computers
Devices
Logs
Management
SOS
Downloads
System
Mountain.Hu@splashtop.com
Copyright © 2010 - 2021 Splashtop Inc.

SOS

Instantly access your customers' computers without them having to pre-install anything

1. Your customer downloads and runs a program from http://127.0.0.1:9080/sos. No installation needed.
2. Your customer tells you the 9-digit session code that's shown on the screen.
3. Use your Splashtop On-Prem Client Windows/Mac/iOS **(v3.3.8.0 or above)**, Android **(v3.4.2.7 or above)** to enter the session code and start accessing the computer.

Technicians

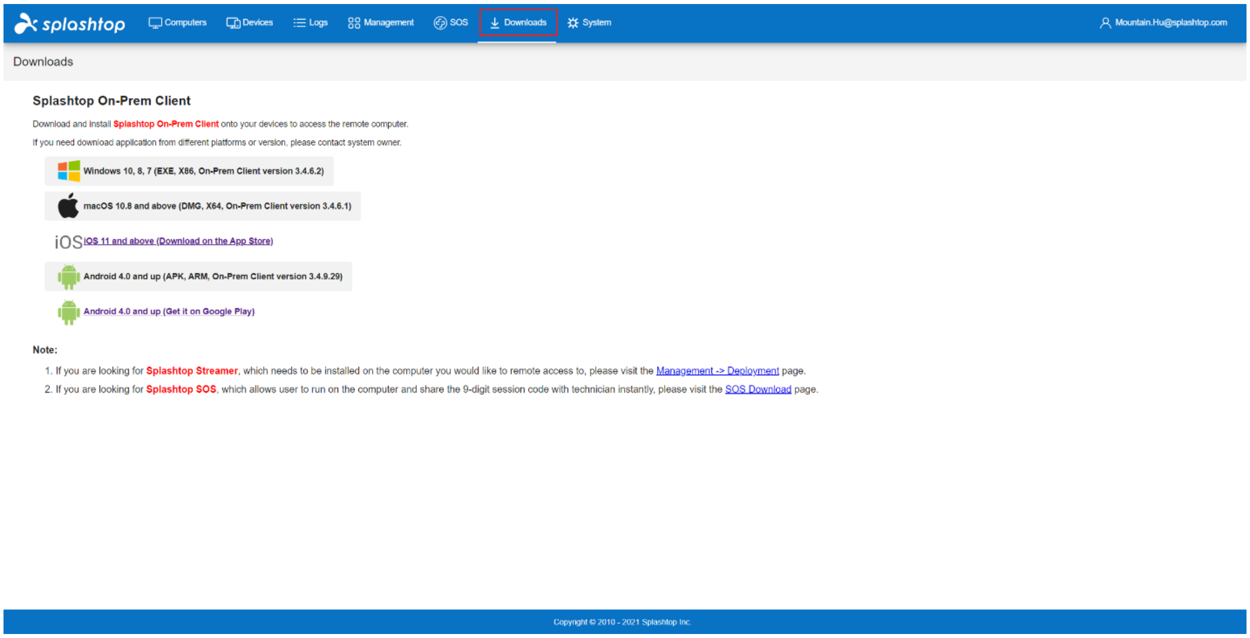
Role ↑	Splashtop Account	Display Name
Member	test@splashtop.com	

Current Sessions

Session Code	Start Time ↑	Supported By	Type	Category	Note
There is no data to display temporarily					

6. Install client app and access

1. Users assigned as a Member can only browser limited content when log in to Splashtop Gateway web console compared to Team Owner or Team Admin as shown in below screenshot. Member can log in Splashtop Gateway Web Console and download the latest Splashtop On-Prem Client via Downloads menu tab and Install desired client applications.



Downloads

Splashtop On-Prem Client

Download and install Splashtop On-Prem Client onto your devices to access the remote computer.

If you need download application from different platforms or version, please contact system owner.

Windows 10, 8, 7 (EXE, X86, On-Prem Client version 3.4.6.2)

macOS 10.8 and above (DMG, X64, On-Prem Client version 3.4.6.1)

iOS iOS 11 and above (Download on the App Store)

Android 4.0 and up (APK, ARM, On-Prem Client version 3.4.9.29)

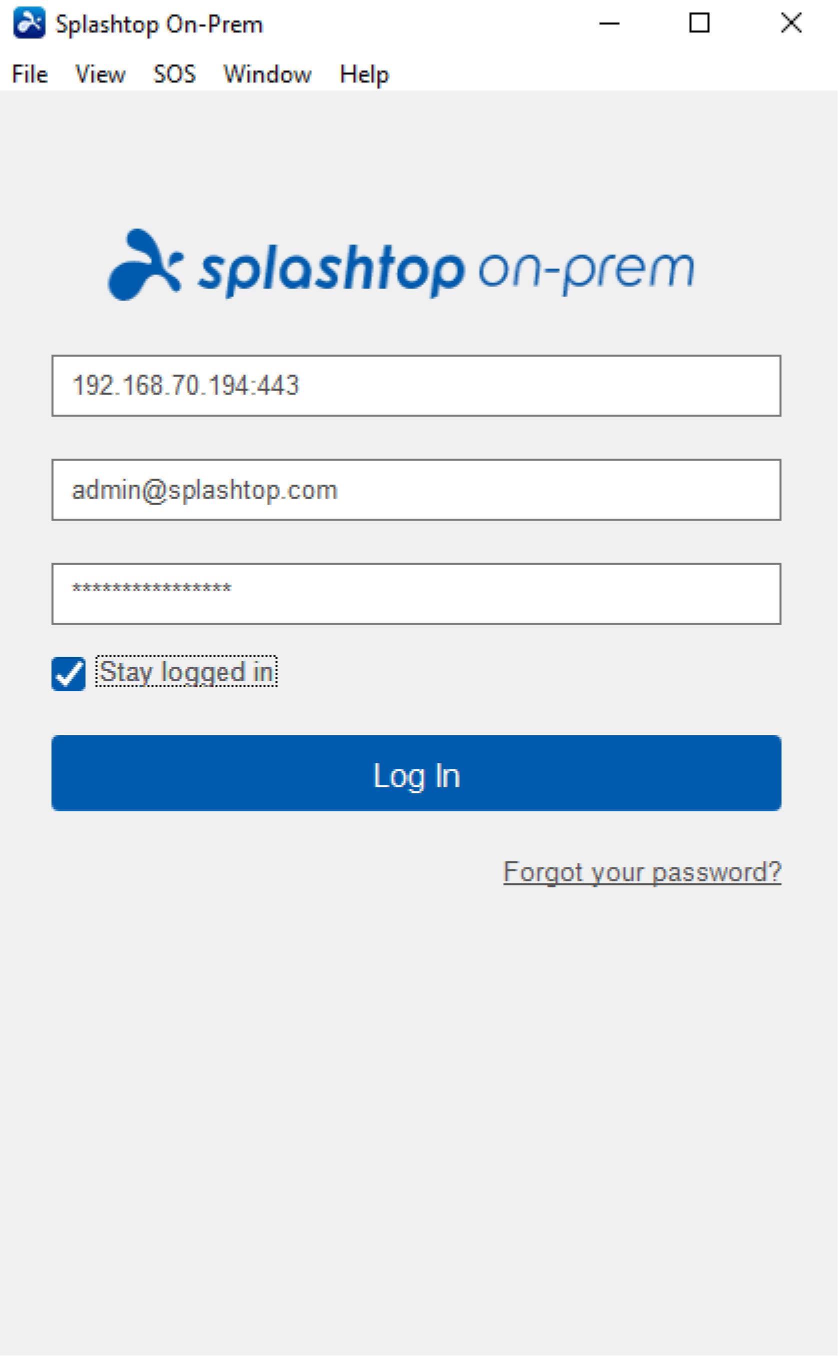
Android 4.0 and up (Get it on Google Play)

Note:

1. If you are looking for Splashtop Streamer, which needs to be installed on the computer you would like to remote access to, please visit the Management -> Deployment page.
2. If you are looking for Splashtop SOS, which allows user to run on the computer and share the 9-digit session code with technician instantly, please visit the SOS Download page.

Copyright © 2010 - 2021 Splashtop Inc.

2. When **Splashtop On-Prem client app** installed, user simply inputs the Splashtop **Gateway server's IP address or FQDN** with default port number **443**, the account name and password obtained from Team Owner or Admin to log in. Users with no such information will need to consult Team owner or Admin.



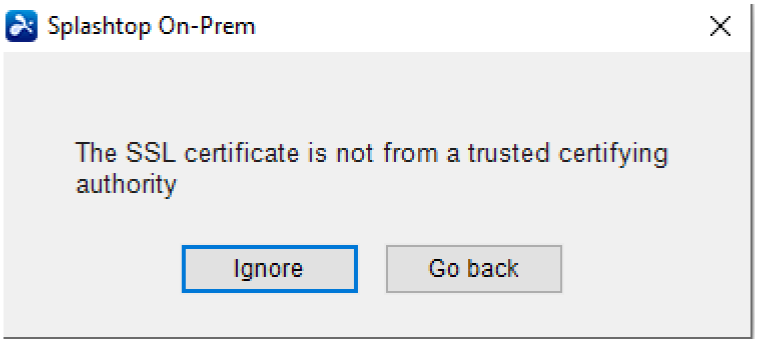
192.168.70.194:443

admin@splashtop.com

****

☑ Stay logged in

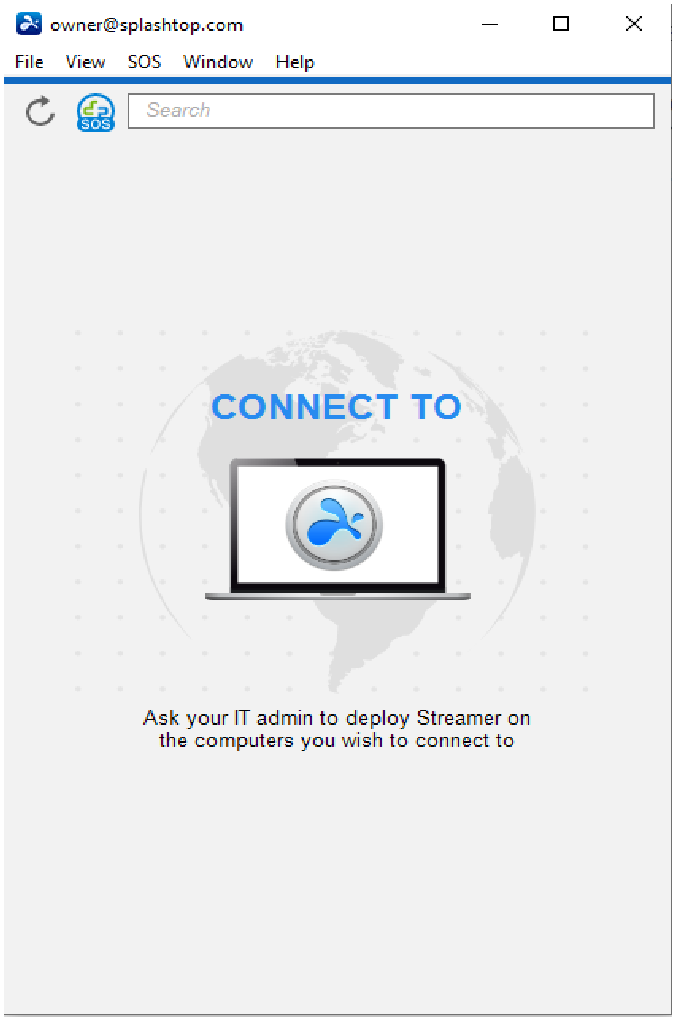
3. If a warning message pops up when you tap **Log In**, stating the SSL certificate is not from a trusted certifying authority, it is likely that the SSL certificate is self-generated, and you can choose to ignore it. However, we recommend that users who have encountered this message popping up should consult their IT department for the proper guidelines to be complied.



Splashtop On-Prem

The SSL certificate is not from a trusted certifying authority

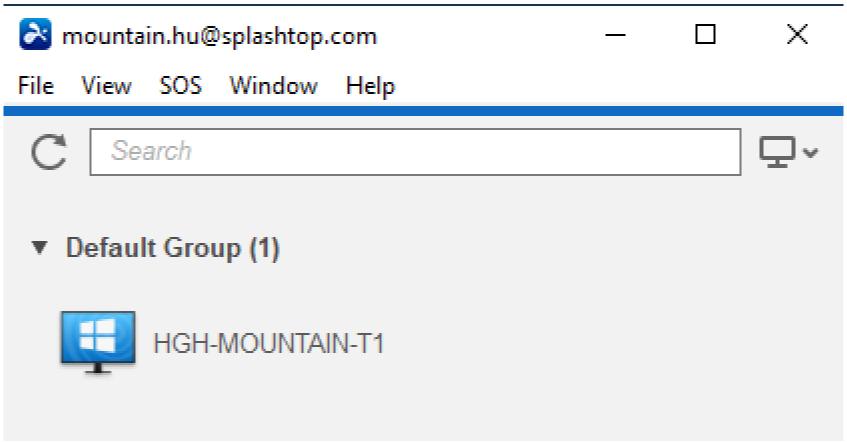
4. When you logged in to On-Prem app, either a list of remote devices ready to be connected will display or you may just engage a screen does not list any specific computer as shown below. In this case please consult your Team Owner or Admin.



owner@splashtop.com

Ask your IT admin to deploy Streamer on the computers you wish to connect to

5. Below Screenshot reveals one specific Windows PC has been successfully deployed so that the user is able to remote access to this device by clicking **connect** button to the right or double clicking the blueish field.

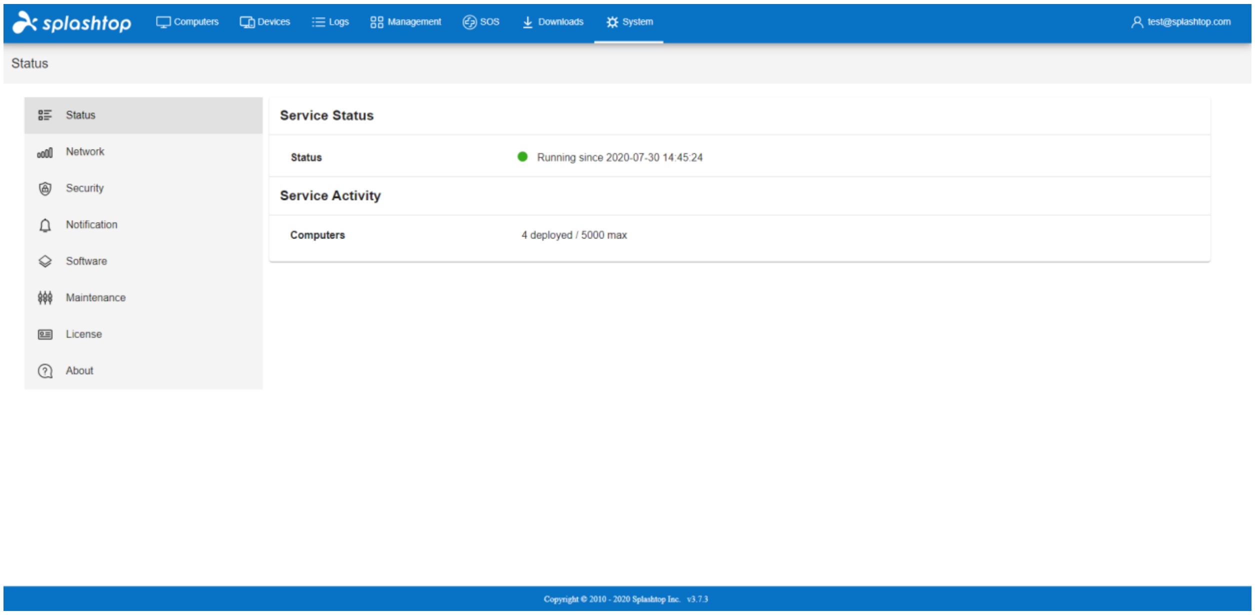


System Configuration

Introduction

System page of **Splashtop Gateway** provides the capability for **Team Owner** to configure system settings.

Log in as Team Owner, you will see **System tab** on the top menu bar, click it to enter system settings.



Service Status

Status	● Running since 2020-07-30 14:45:24

Service Activity

Computers	4 deployed / 5000 max

Copyright © 2010 - 2020 Splashtop Inc. v3.7.3

- **Status** shows the current status of the Splashtop Gateway
- **Network** shows the network configuration of the Splashtop Gateway
- **Security** allows Team Owner to configure security related settings, such as SSL Certificate, TLS settings
- **Access Control** allows Team Owner to configure access policy, such as web console, Splashtop On-Prem Client
- **Notification** allows Team Owner to set notification to notify users, such as scheduled system maintenance

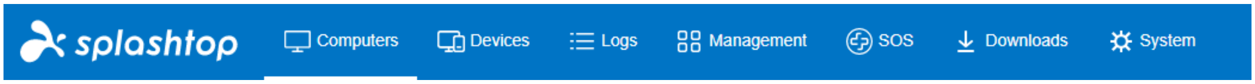
- **Software** allows Team Owner to configure software components, such as enable/disable particular version of Splashtop Streamer and Splashtop On-Prem, uploading new version of components
- **Maintenance** allows Team Owner to do system maintenance, such as backup and restore
- **License** allows Team Owner to configure license, such as import/update licenses
- **About** shows the version, copyright, Terms of Service, Privacy, and Acknowledgements

Access Gateway Portal

Splashtop Gateway web portal is a web-based console to configure and manage Splashtop On-Prem system. It can be accessed from a web-browser, preferably Chromium based browser such as Google Chrome.

Every registered user in Splashtop On-Prem system is granted access to the Gateway web portal, but the menu display varies depending on the assigned role of the user.

Menu available for a team/Team Owner.



Gateway web portal can be easily accessed by opening a web browser and entering the address of the Gateway Server.

The format of the address is defined as follow:

https://(IP address of Server):(Port number)

An example of such address: https://192.168.1.100:443

This example address points to a Gateway Server with IP address of 192.168.1.100 and the server uses the default port 443.

Note: You should always use **https** instead of **http** here as this is a secured **http** connection with SSL encryption.

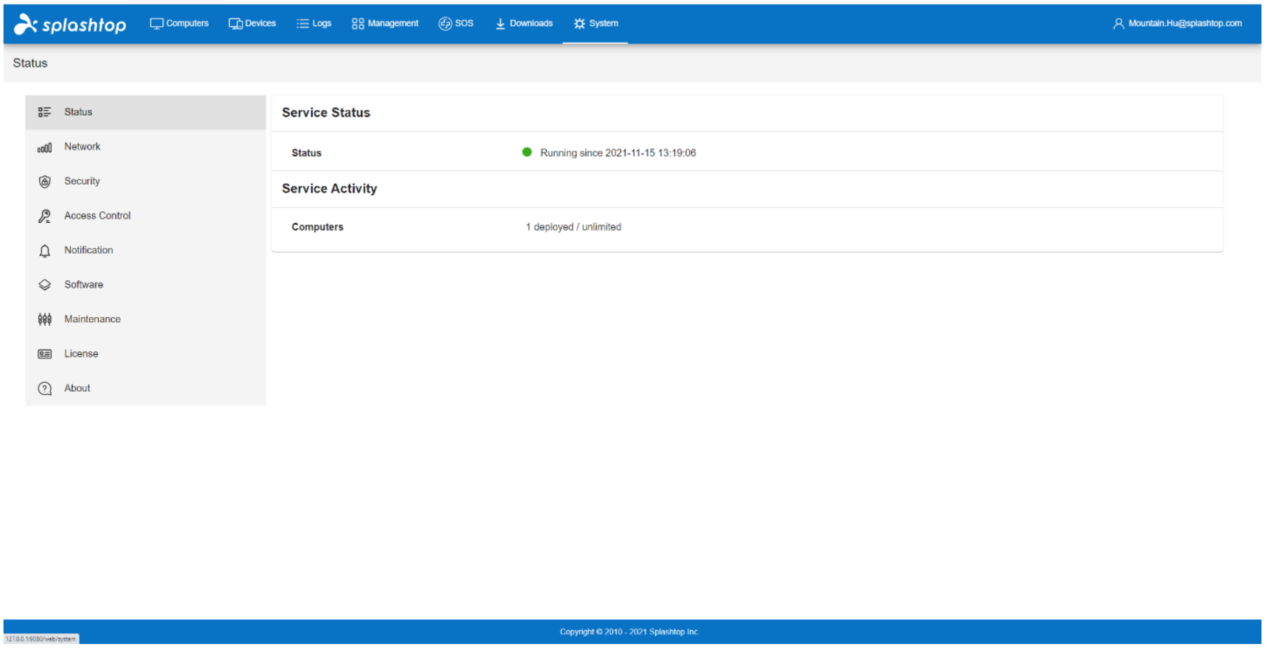
IP Address of Server

This is the IP address of the server machine where Splashtop Gateway is installed. It can be a local IP address if you are connecting from a computer sitting in the same LAN network, or it can be a public IP address if you are connecting via the Internet. If the server machine has multiple network cards, you can use any of the IP addresses to access the Gateway web portal. With this feature, you can safely deploy the Gateway server machine in a DMZ network.

Port Number

By default, Splashtop On-Prem makes use of Port number 443, but you can change the port number following instructions in the article below:

Status



Service Status

Status ● Running since 2021-11-15 13:19:06

Service Activity

Computers 1 deployed / unlimited

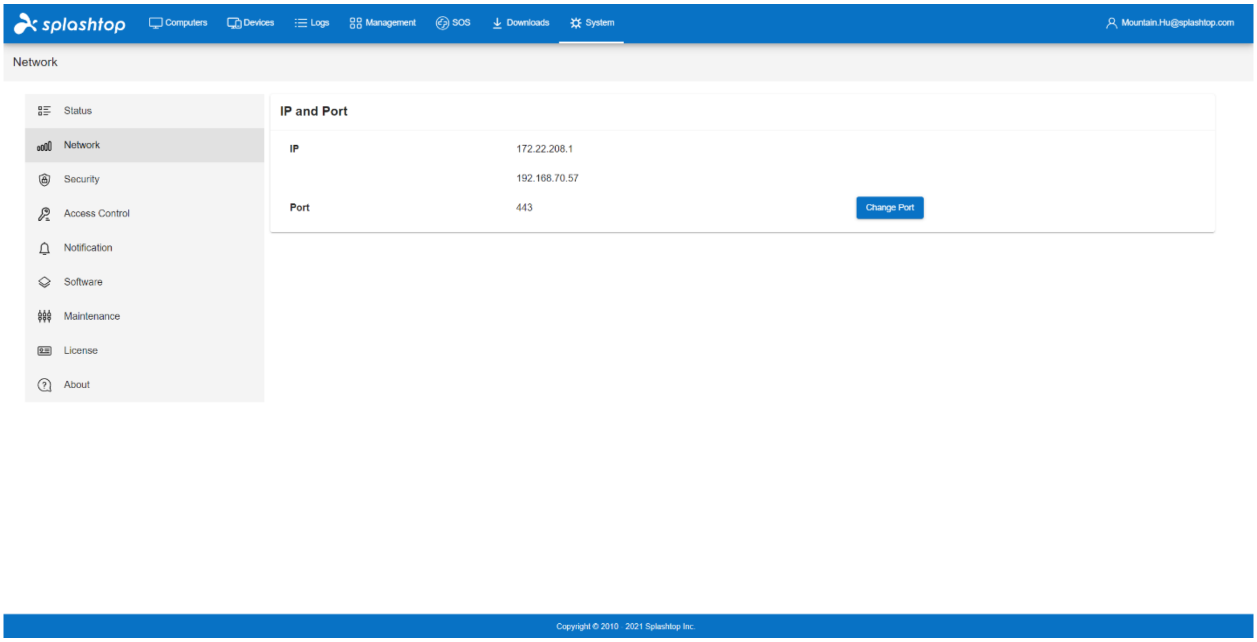
The status page is a summary of the Splashtop Gateway service. It shows:

- **Service Status**: the current status of the service (green indicates healthy) and the timestamp of last service launch.
- **Service Activity**: number of deployed computers (Streamers) in the system and the maximum allowed number of computers for remote access (unattended) sessions.

Network

Change Network Port

Log in to Gateway's management console with the Team Owner, go to **System** > **Network**, the **Port** section shows the port that Gateway is currently serving, click **Change Port** will allow user to input a new port and apply.



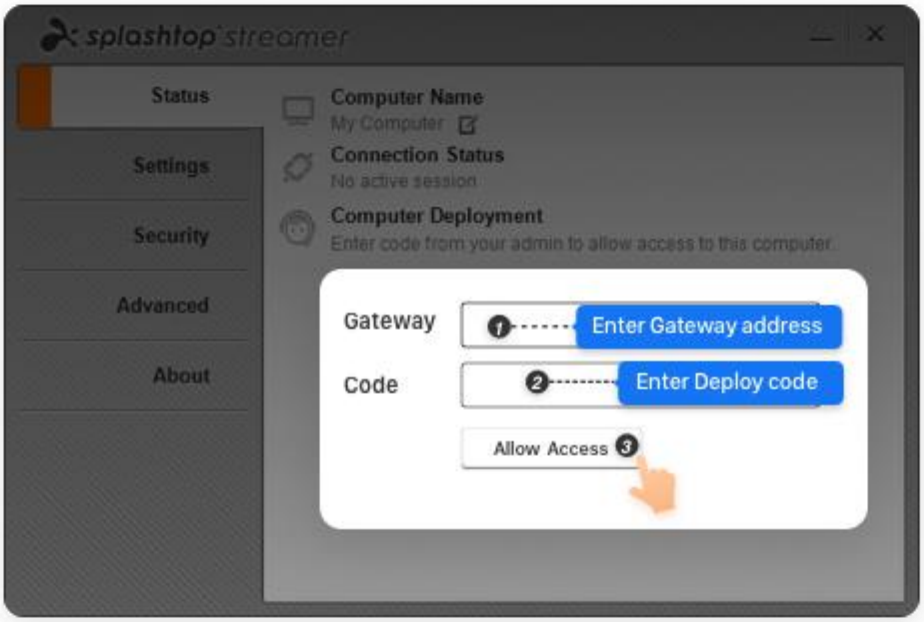
IP and Port

IP	172.22.208.1 192.168.70.57
Port	443

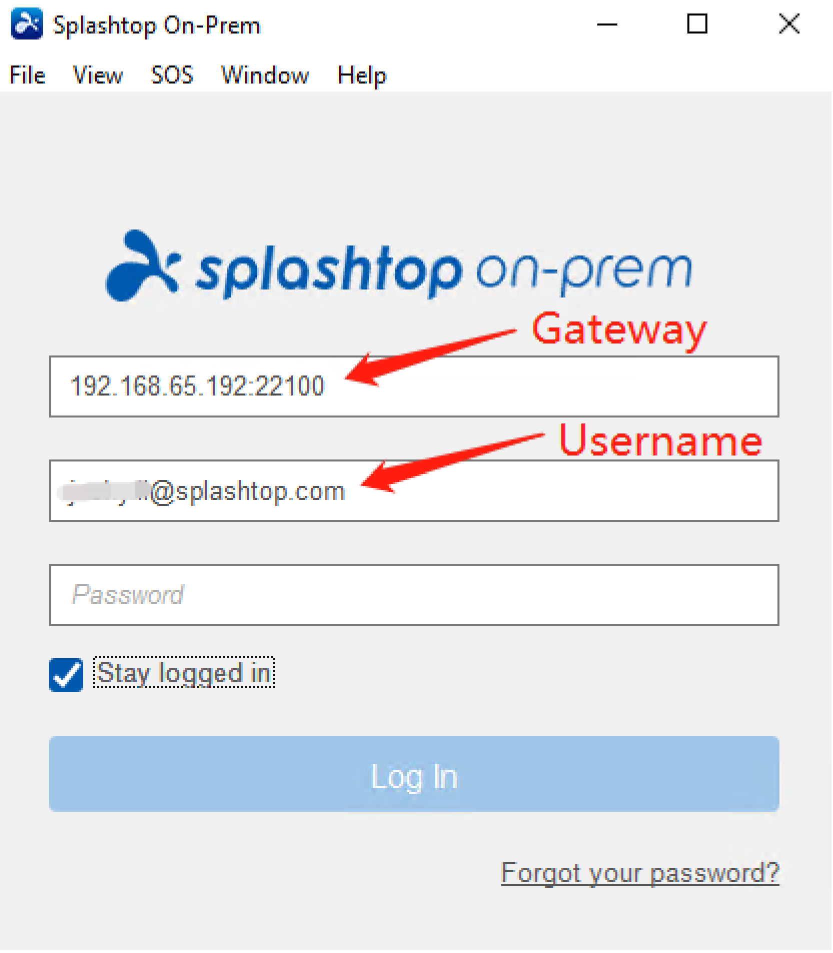
Notice:

1. Changing port will automatically restart Gateway service, it needs approximately 30 seconds to be ready again.

2. If you already have Streamer deployed or On-Prem app logged in, these Streamers and On-Prem apps will be logged off, due to the port change, you need to specify the correct *IP:Port* in the Streamer and On-Prem app side to log into the Gateway again. 443 is the default port, which can be ignored when typing.



(Input *IP:Port* in the **Gateway** field when deploy)



192.168.65.192:22100

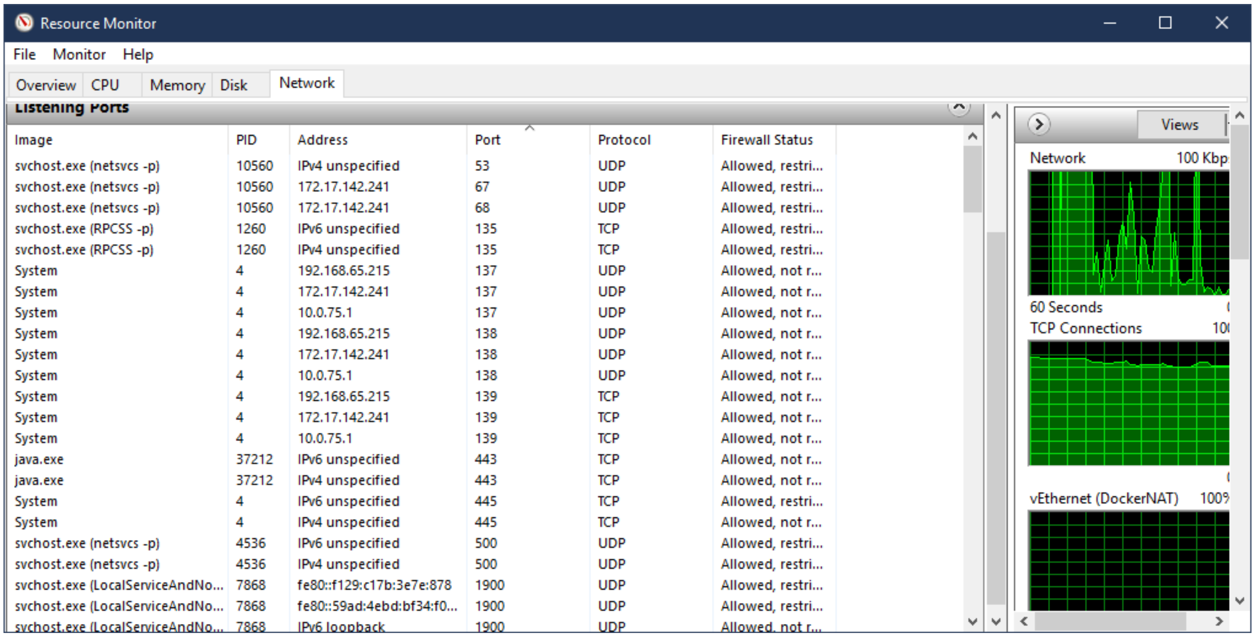
[redacted]@splashtop.com

Password

☑ Stay logged in

(Input *IP:Port* in the **Gateway** field to login)

3. As a general practice, we would suggest you, as the IT admin, need to make sure the port you would like to change to has **not been occupied**, you can use Windows built-in **resmon** utility to check. From Windows search, type *resmon*, run **resmon** tool, go to **Network**, expand **Listening Port**, and check there is no other software listening on the chosen port.



Listening Ports

Image	PID	Address	Port	Protocol	Firewall Status
svchost.exe (netsvcs -p)	10560	IPv4 unspecified	53	UDP	Allowed, restri...
svchost.exe (netsvcs -p)	10560	172.17.142.241	67	UDP	Allowed, restri...
svchost.exe (netsvcs -p)	10560	172.17.142.241	68	UDP	Allowed, restri...
svchost.exe (RPCSS -p)	1260	IPv6 unspecified	135	TCP	Allowed, restri...
svchost.exe (RPCSS -p)	1260	IPv4 unspecified	135	TCP	Allowed, restri...
System	4	192.168.65.215	137	UDP	Allowed, not r...
System	4	172.17.142.241	137	UDP	Allowed, not r...
System	4	10.0.75.1	137	UDP	Allowed, not r...
System	4	192.168.65.215	138	UDP	Allowed, not r...
System	4	172.17.142.241	138	UDP	Allowed, not r...
System	4	10.0.75.1	138	UDP	Allowed, not r...
System	4	192.168.65.215	139	TCP	Allowed, not r...
System	4	172.17.142.241	139	TCP	Allowed, not r...
System	4	10.0.75.1	139	TCP	Allowed, not r...
java.exe	37212	IPv6 unspecified	443	TCP	Allowed, not r...
java.exe	37212	IPv4 unspecified	443	TCP	Allowed, not r...
System	4	IPv6 unspecified	445	TCP	Allowed, restri...
System	4	IPv4 unspecified	445	TCP	Allowed, not r...
svchost.exe (netsvcs -p)	4536	IPv6 unspecified	500	UDP	Allowed, restri...
svchost.exe (netsvcs -p)	4536	IPv4 unspecified	500	UDP	Allowed, restri...
svchost.exe (LocalServiceAndNo...	7868	fe80::f129:c17b:3e7e:878	1900	UDP	Allowed, restri...
svchost.exe (LocalServiceAndNo...	7868	fe80::59ad:4ebd:bf34:f0...	1900	UDP	Allowed, restri...
svchost.exe (LocalServiceAndNo...	7868	IPv6 loopback	1900	UDP	Allowed, not r...

Authentication

Active Directory

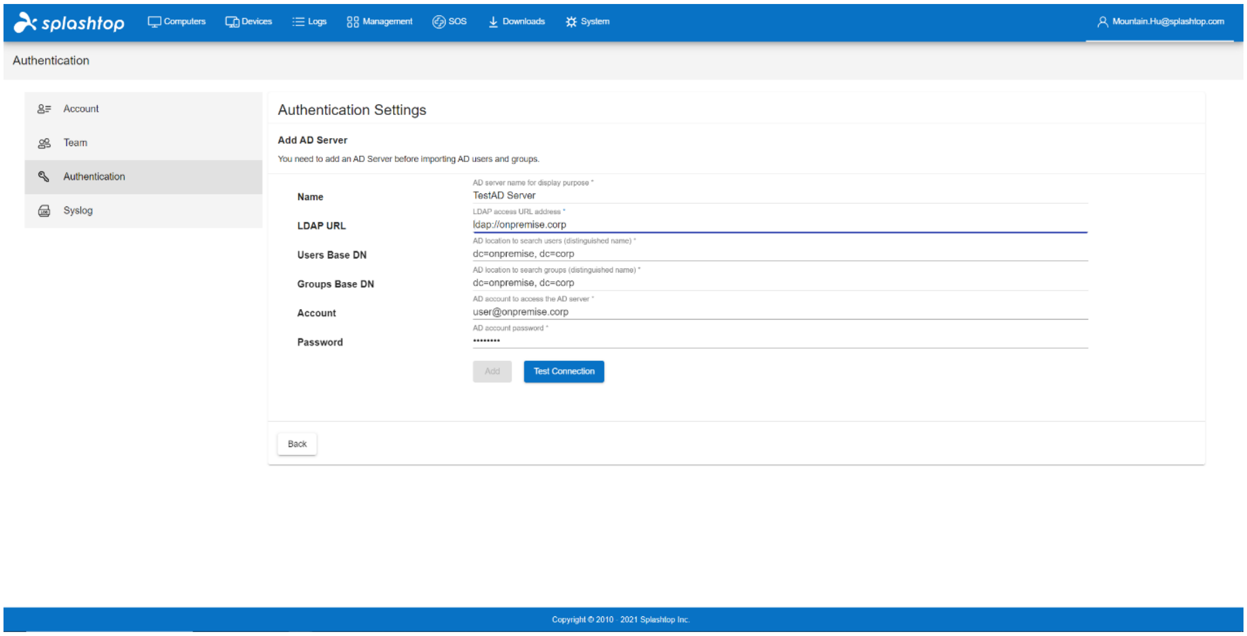
Splashtop On-Prem AD integration is compatible with Windows Server 2008 r2, 2012, 2016, 2019 Active Directory and Microsoft Azure AD. This allows Team Owner easily authenticates and manages AD accounts and start to use Splashtop remote service immediately.

To add an AD server, open the Active Directory page using team admin/owner account from **Management -> Settings > Authentication**

- **Name**: Fill up an AD Server name concatenated to the actual AD server of your organization.
- **LDAP URL Syntax**: The syntax here including **ldap scheme (ldap://) + implied address (of target AD server) +port number (if needed).** LDAPS is **supported** as well.
- **Users Base DN**: The active directory user's **Distinguished Name.** We use Users Base DN as user authentication checkpoint in AD hierarchy.

- **Groups Base DN:** The active directory group's **Distinguished Name**. We use Group Base DN as group authentication checkpoint in AD hierarchy.
- **Account**: User account from target AD server to bind. The user account syntax: **sAMaccountName@ADLocalDomainName**
- **Password**: The AD password of associated AD user account.
- **Test Connection**: Click this button to check the availability of target AD server for authentication.
- **Add**: Click this button to bind a validated AD server to Splashtop Gateway AD Server list.

Note: Avoid adding multiple AD Servers with overlapping scope. Please verify the uniqueness of Users Base DN and Groups Base DN so that each user and group only roots from one AD Server source. Overlapping scope may cause **authentication invalidity and unsolvable group members**.



Authentication

Authentication Settings

Add AD Server

You need to add an AD Server before importing AD users and groups.

Name	AD server name for display purpose * TestAD Server
LDAP URL	LDAP access URL address * ldap://onpremise.corp
Users Base DN	AD location to search users (distinguished name) * dc=onpremise, dc=corp
Groups Base DN	AD location to search groups (distinguished name) * dc=onpremise, dc=corp
Account	AD account to access the AD server * user@onpremise.corp
Password	AD account password * ••••••••

AD maintenance

This is a built-in tool to clean up unsolvable AD group members in the Splashtop On-Prem system. Unsolvable AD group members refer to the users that are missing from external AD servers but still in the internal database.

It is suggested to clean up the unsolvable AD group members to keep the user database neat and manageable. To perform an AD maintenance task, check the users that are to be removed from the Splashtop On-Prem system and simply click on the **Clean Up** button.

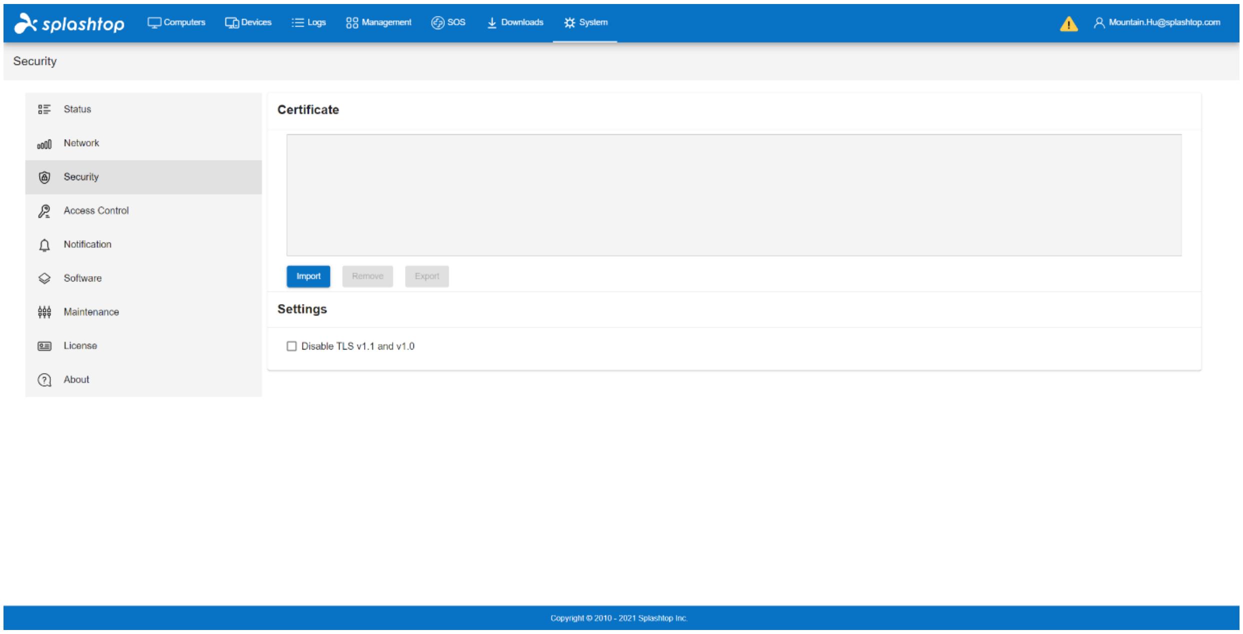
Security

Import SSL Certificate

Splashtop Gateway supports importing your own certificate, which can be self-signed certificate, or certificate issued by 3rd party authority.

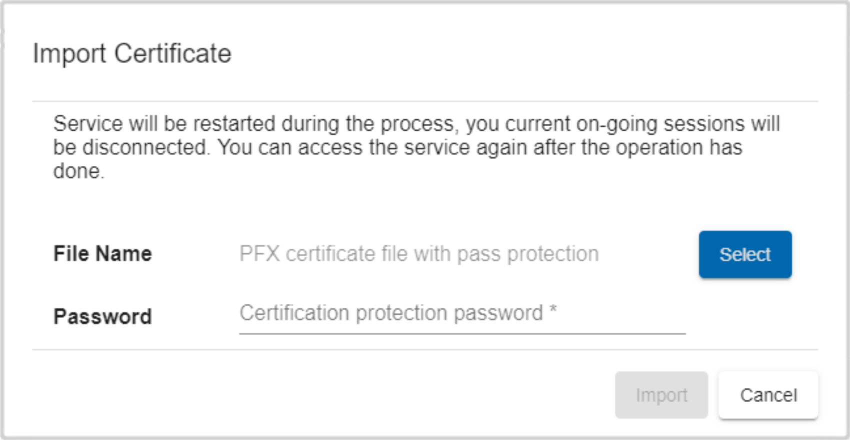
PKCS#12 (PFX) format certificate is supported by Gateway.

Step 1. To import new certificate, please login to Gateway's management console as Team Owner then go to **System** > **Security** page. It shows the current imported certificate information, if there is no certificate info shown; it means Gateway is using the Gateway bundled self-signed certificate.



□ Disable TLS v1.1 and v1.0

Step 2. Click **Import**, it will show the importing dialog, select the PFX file and also the password which is set when generating the certificate.



Import Certificate

Service will be restarted during the process, you current on-going sessions will be disconnected. You can access the service again after the operation has done.

File Name PFX certificate file with pass protection

Password Certification protection password *

Step 3. Click Import to finish importing, which will restart Gateway service to make the new certificate effective.

Convert SSL Cert to PFX format

On Windows:

1. Click **Start** followed by **Run**. Type **MMC.exe**, and then click **OK**. Click **File** and then **Add/Remove Snap-in**.

2. Click **Add**. Highlight the "certificates" and then click **Add** again.

3. Choose **Computer account** and then click **Next**. Select **Local Computer** followed by **OK**. Click **Close** and then **OK** to close the "Snap-in" window.

4. Open the **Certificates** (Local Computer) snap-in that you created. Go to **Personal** followed by **Certificates**.

5. Right-click on the server certificate you want to convert, and then select **All Tasks** followed by **Export**.

6. Click **Next** on the wizard that opens. If the wizard doesn't open, repeat Step 5. If it still doesn't open, restart your computer and go back to Step 4.

7. Choose **Private key** as your export, and then click **Next**.

8. Choose the Personal Information Exchange (PFX) file format to create a PFX file.

9. Click **Next** and choose a password for the file. Click **Next** again.

10. Choose the file name. Don't include an extension, as the wizard automatically adds the PFX extension.

11. Click **Next**, write down where the file is saved to, and then click **Finish**.

Alternately (using OpenSSL cmd line, and GoDaddy signed certificate as example):

http://support.godaddy.com/help/article/5343/generating-a-certificate-signing-request

We generate CSR via OpenSSL command prompt:
http://support.godaddy.com/help/article/5269/generating-a-certificate-signing-request-csr-apache-2x
>openssl req –new –newkey rsa:2048 –nodes –keyout yourdomain.key –out yourdomain.csr

Please refer to this site for command examples: http://www.sslshopper.com/article-most-common-openssl-commands.html

1. Convert private key, certificate and godaddy certificate bundle into .PEM file
2. Concatenate .PEM files of private key, certificate, godaddy certificates into one single .PEM file
3. Convert final .PEM file into .pfx file

REQUIREMENTS:

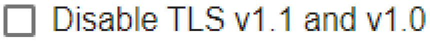
When creating PFX, the middle/intermediate layer CA cert must be included. If the PFX does not contain the direct issuer’s CA, issues may be seen from portable OS.

The openssl command line is:
openssl pkcs12 -export -out output.pfx -inkey private.key -in star-splashtop.com.crt -certfile int.cer
Openssl will prompt IT to input password to protect output PFX file.
Output.pfx: the output file name.
Private.key: the private key for certificate.
Star-splashtop.com.crt: the signature for our site, provided by 3rd CA
Int.cer: 3rd CA’s certificate

Disable TLS 1.1 and 1.0

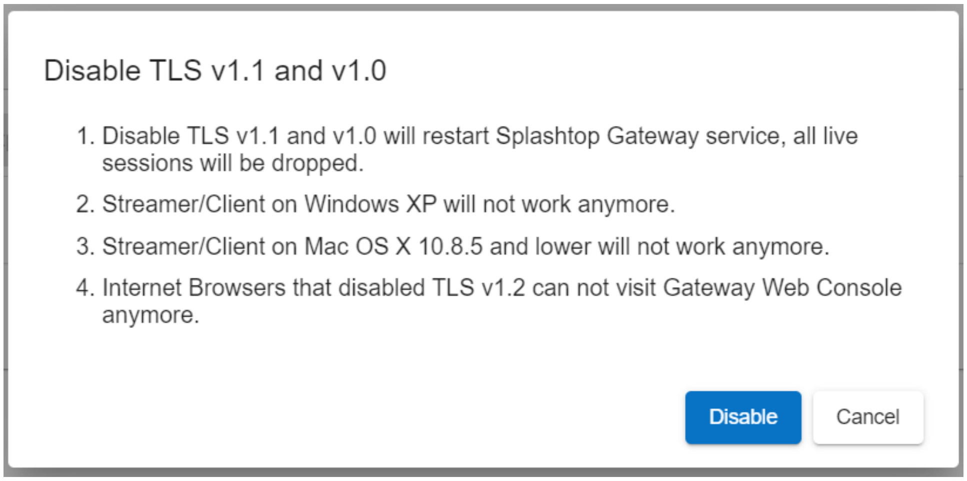
Team Owner can disable TLS 1.1 and 1.0 on Splashtop Gateway to enhance the security or be compliant to PCI compliance. Once disabled, Gateway will enforce all endpoints to run on TLS 1.2 only level.

Step 1: Log into Gateway's management console as Team Owner, go to **System** > **Security**, click the *Disable TLS v1.1 and 1.0* option



□ Disable TLS v1.1 and v1.0

Step 2: In the prompted dialog, Gateway will indicate the important information of disabling TLS 1.1 and 1.0, you will need to click **Disable** to proceed**.** Gateway will be started to enforce TLS 1.1 and 1.0 disabled.



Disable TLS v1.1 and v1.0

1. Disable TLS v1.1 and v1.0 will restart Splashtop Gateway service, all live sessions will be dropped.
2. Streamer/Client on Windows XP will not work anymore.
3. Streamer/Client on Mac OS X 10.8.5 and lower will not work anymore.
4. Internet Browsers that disabled TLS v1.2 can not visit Gateway Web Console anymore.

With TLS 1.1 and 1.0 disabled, you need to do some system tunes on Windows 7 and Server 2008, because the default setting for these OS versions is TLS 1.0. Here are the instructions:

1. Get Windows update to support TLS 1.2

Please refers to this article https://support.microsoft.com/en-us/help/3140245/ to get the update to support TLS 1.2.

2. Register TLS 1.2

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client]
"Enabled"=dword:ffffffff
"DisabledByDefault"=dword:00000000
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server]
"Enabled"=dword:ffffffff
"DisabledByDefault"=dword:00000000
```

3. Configure TLS 1.1 to be used for WinHTTP by default

For 32-bit Windows 7/Server 2008

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\WinHttp]
"DefaultSecureProtocols"=dword:00000200
```

For 64-bit Windows 7/Server 2008

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\WinHttp]
"DefaultSecureProtocols"=dword:00000200
```

4. Configure TLS 1.2 to be used for WinHTTP by default

For 32-bit Windows 7/Server 2008

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\WinHttp]
"DefaultSecureProtocols"=dword:00000800

For 64-bit Windows 7/Server 2008

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\WinHttp]
"DefaultSecureProtocols"=dword:00000800

Note:

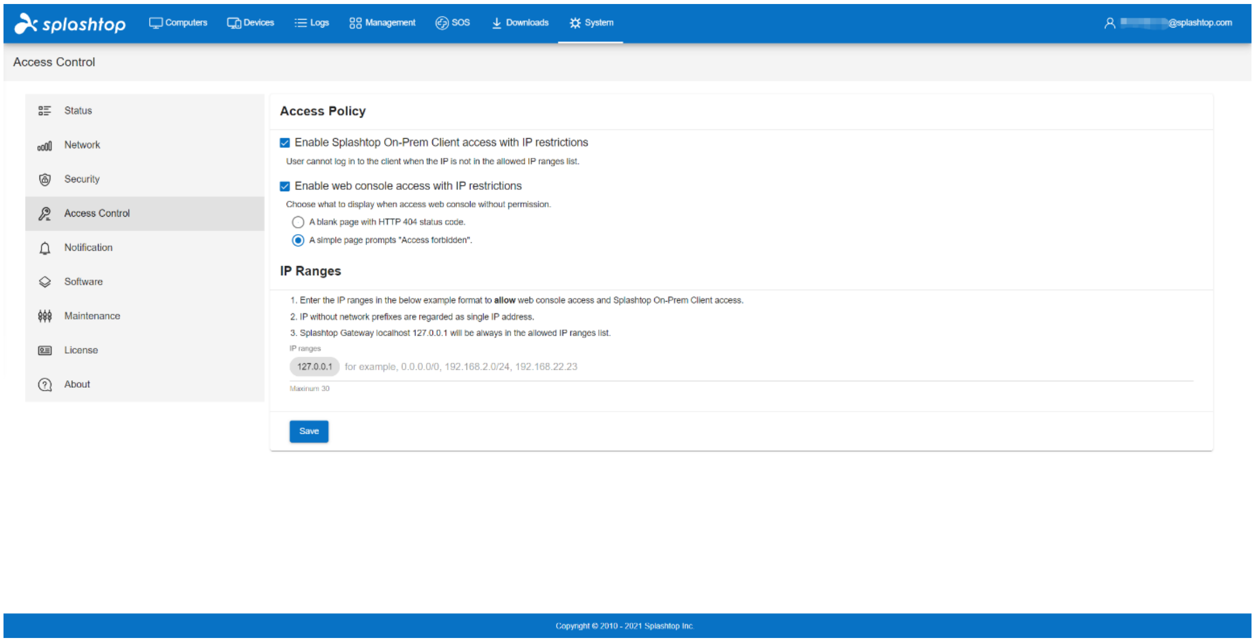
1. Windows XP uses SSL v3 by default for WinHTTP. Windows 8 or later uses TLS 1.1 for WinHTTP by default.

2. Please add key if there is none showing: TLS 1.2\Server, TLS 1.2\Client

Reference Article: Microsoft Support

Access Control

The access control page allows owners manage the web console access and Splashtop On-Prem client access with IP restriction.



Access Policy

☑ Enable Splashtop On-Prem Client access with IP restrictions

User cannot log in to the client when the IP is not in the allowed IP ranges list.

☑ Enable web console access with IP restrictions

Choose what to display when access web console without permission.

○ A blank page with HTTP 404 status code.

● A simple page prompts "Access forbidden".

IP Ranges

1. Enter the IP ranges in the below example format to **allow** web console access and Splashtop On-Prem Client access.
2. IP without network prefixes are regarded as single IP address.
3. Splashtop Gateway localhost 127.0.0.1 will be always in the allowed IP ranges list.

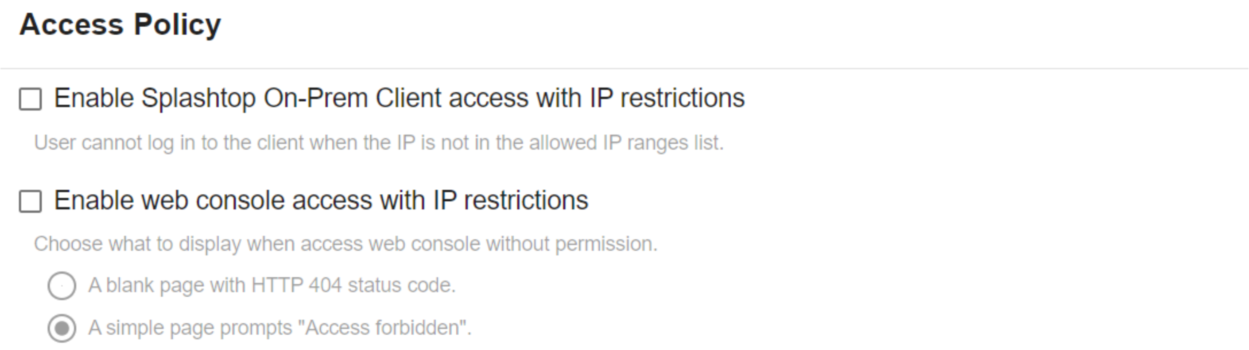
IP ranges

127.0.0.1 for example, 0.0.0.0/0, 192.168.2.0/24, 192.168.22.23

Maximum 30

Step 1

Log into Gateway's management console as Owner, go to *System* > *Access Control*, enable IP access restrictions for Splashtop On-Prem Client or web console. In addition, owner can choose different display methods for web console access denied.



Access Policy

☐ Enable Splashtop On-Prem Client access with IP restrictions

User cannot log in to the client when the IP is not in the allowed IP ranges list.

☐ Enable web console access with IP restrictions

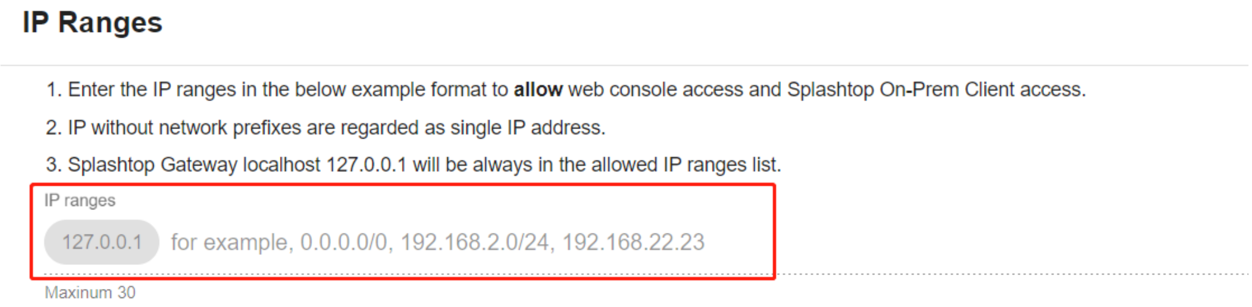
Choose what to display when access web console without permission.

○ A blank page with HTTP 404 status code.

● A simple page prompts "Access forbidden".

Step 2

Input allowed IP in IP ranges, user cannot log in to the client when the IP is not in the allowed IP ranges list.



IP Ranges

1. Enter the IP ranges in the below example format to **allow** web console access and Splashtop On-Prem Client access.
2. IP without network prefixes are regarded as single IP address.
3. Splashtop Gateway localhost 127.0.0.1 will be always in the allowed IP ranges list.

IP ranges

127.0.0.1 for example, 0.0.0.0/0, 192.168.2.0/24, 192.168.22.23

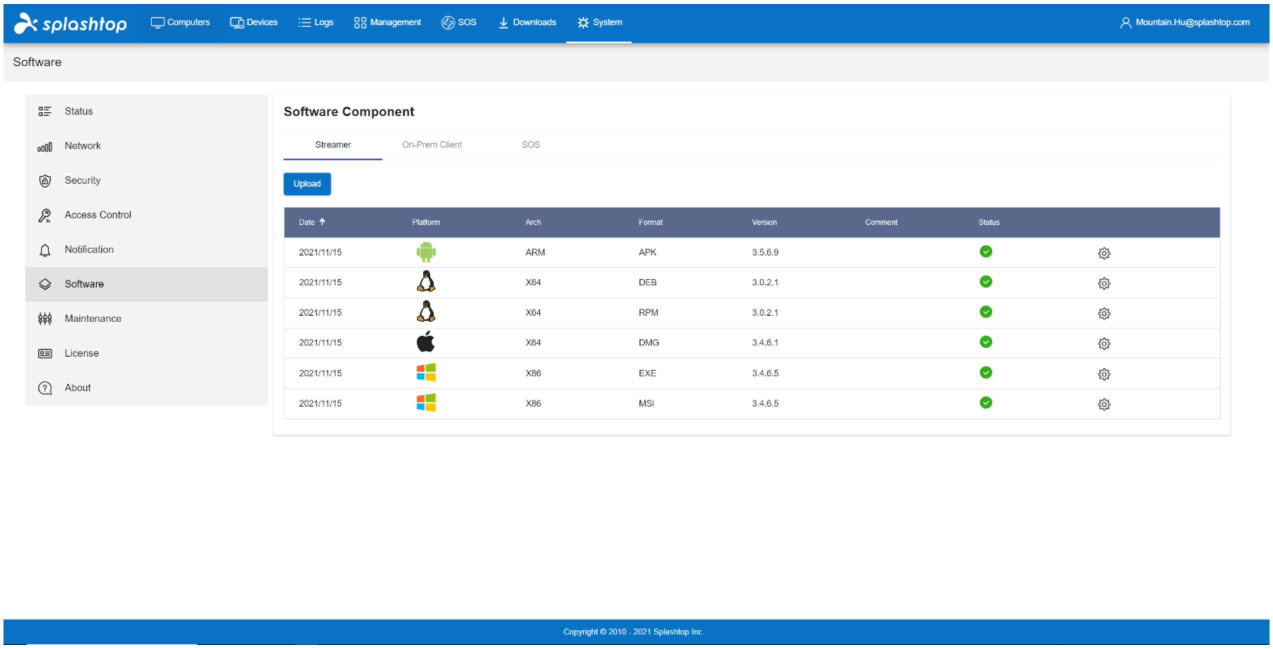
Maxinum 30

Step 3

Click Save button to save the settings.

Software

The *software component* page in Gateway's **System** page allows Team Owner to manage the software components.



Software Component

Date ↑	Platform	Arch	Format	Version	Comment	Status	
2021/11/15	🤖	ARM	APK	3.5.6.9		✓	⚙
2021/11/15	🐧	X64	DEB	3.0.2.1		✓	⚙
2021/11/15	🐧	X64	RPM	3.0.2.1		✓	⚙
2021/11/15		X64	DMG	3.4.6.1		✓	⚙
2021/11/15	⊞	X86	EXE	3.4.6.5		✓	⚙
2021/11/15	⊞	X86	MSI	3.4.6.5		✓	⚙

Team Owner can configure the following software components:

- **Splashtop Streamer:** Software needs to be installed and running on the remote device you would like to access to. It streams audio and video to the client device.

- **SOS**: The application running on the target device that user would like to have an on-demand support, it will show a 9-digit session code that allows technician to remote in for support.
- **Splashtop On-Prem Client App:** Application makes it possible to establish remote sessions between local device and the target remote device running Splashtop Streamer or Splashtop SOS.

Import new version of Software components

In addition to the embedded software components in Splashtop Gateway, Splashtop will release new components with new features, patches. You can import into your Gateway, and also you are recommended to do so to keep the system running healthy. This section explains how to import new version of software components into Splashtop Gateway.

Get PKG file

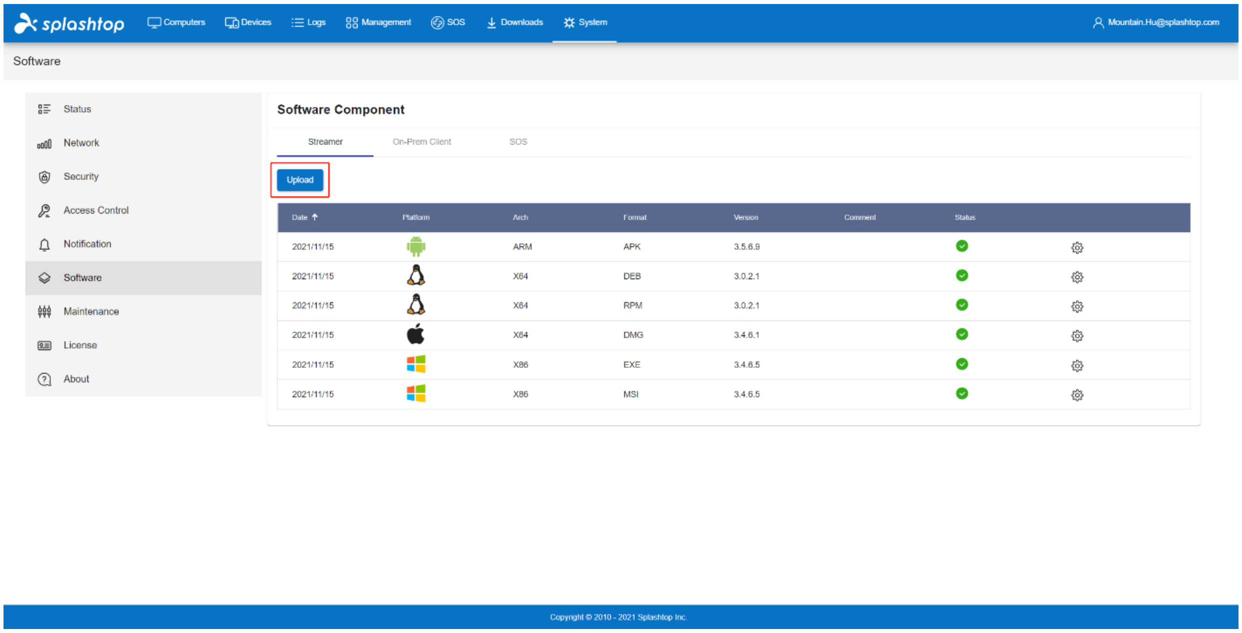
In the following new version announcement pages, you can get new versions of software components in PKG file format.

- **Splashtop Gateway -** new version announcements page
- **Splashtop Streamer -** new version announcements page
- **Splashtop On-Prem Client App -** new version announcements page

Notice: Please check the version compatibility info in the page

Import Streamer

1. Log in as Team Owner, go to Gateway's management console > *System* > *Software* > *Streamer*, click **Upload** to open upload page.

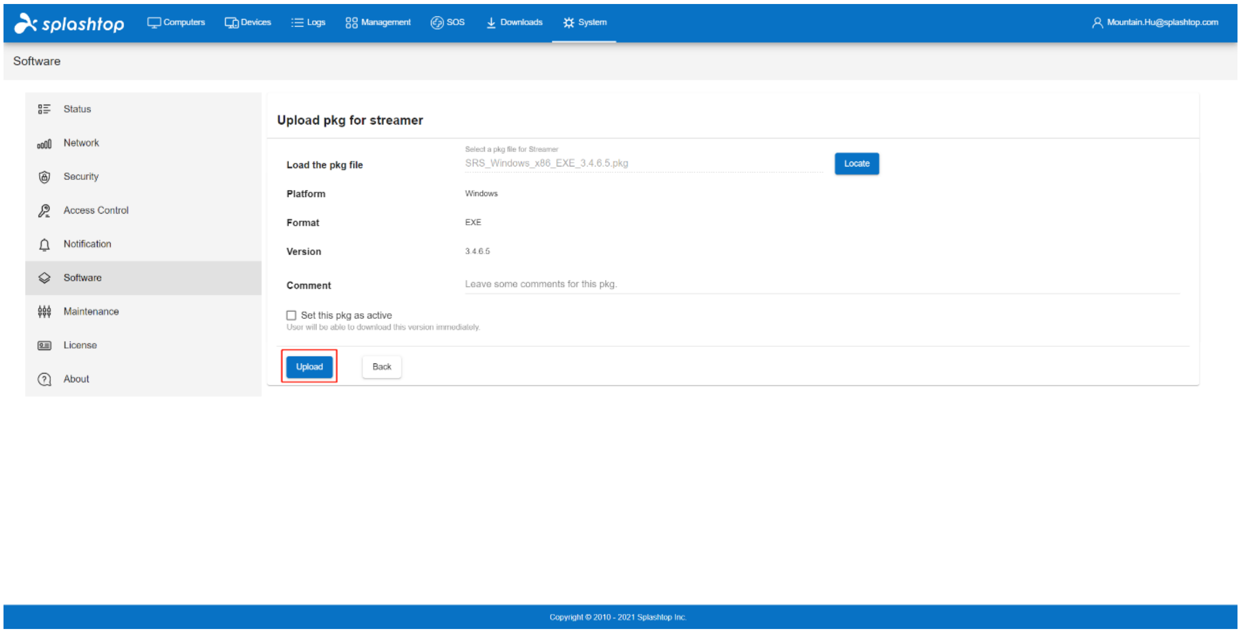


Software Component

Date ↑	Platform	Arch	Format	Version	Comment	Status	
2021/11/15	🤖	ARM	APK	3.5.6.9		✓	⚙
2021/11/15	🐧	X64	DEB	3.0.2.1		✓	⚙
2021/11/15	🐧	X64	RPM	3.0.2.1		✓	⚙
2021/11/15		X64	DMG	3.4.6.1		✓	⚙
2021/11/15	⊞	X86	EXE	3.4.6.5		✓	⚙
2021/11/15	⊞	X86	MSI	3.4.6.5		✓	⚙

2. Locate the PKG file, system will verify if the PKG is packaged for Gateway correctly, and show the package info, like *platform*, *format*, and *version*. Finally click **Upload** to upload the package.

Set it to *active* to make it able for deployment.

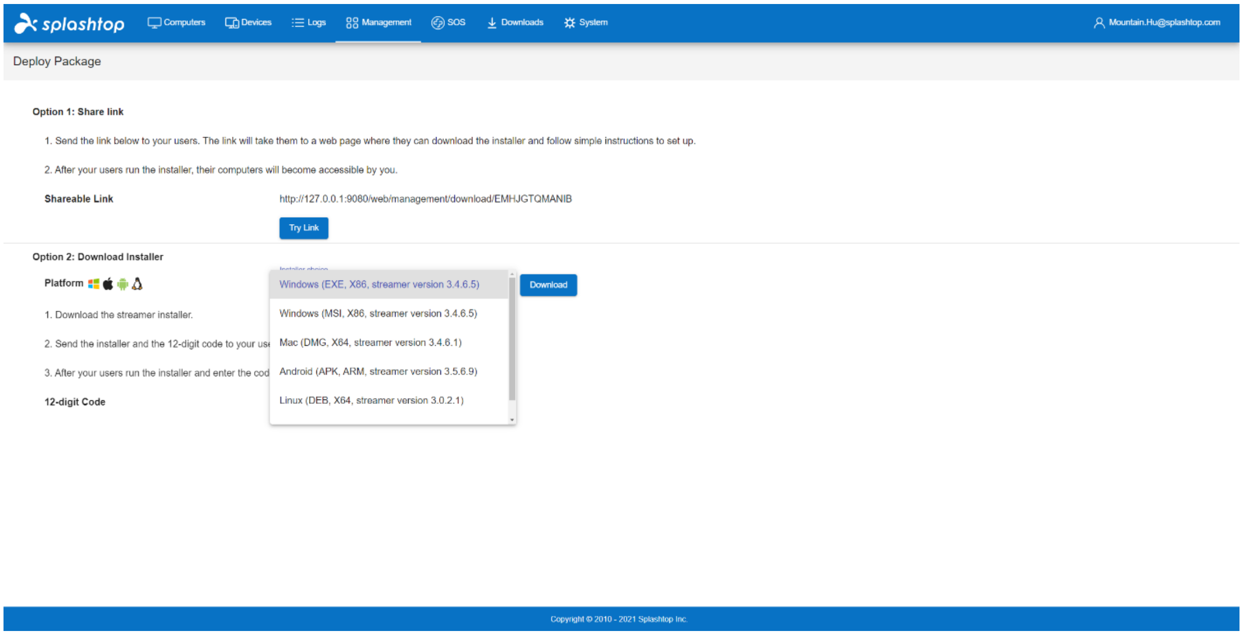


Upload pkg for streamer

Load the pkg file	Select a pkg file for Streamer SRS_Windows_x86_EXE_3.4.6.5.pkg
Platform	Windows
Format	EXE
Version	3.4.6.5
Comment	Leave some comments for this pkg.

□ Set this pkg as active
User will be able to download this version immediately.

3. Once finished uploading, and set as active, in the Streamer deployment page, the newly uploaded component is available for download.



Deploy Package

Option 1: Share 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. After your users run the installer, their computers will become accessible by you.

Shareable Link http://127.0.0.1:9080/web/management/download/EMHJGTQMANIB

Option 2: Download Installer

Platform

Installer choice

- Windows (EXE, X86, streamer version 3.4.6.5)
- Windows (MSI, X86, streamer version 3.4.6.5)
- Mac (DMG, X64, streamer version 3.4.6.1)
- Android (APK, ARM, streamer version 3.5.6.9)
- Linux (DEB, X64, streamer version 3.0.2.1)

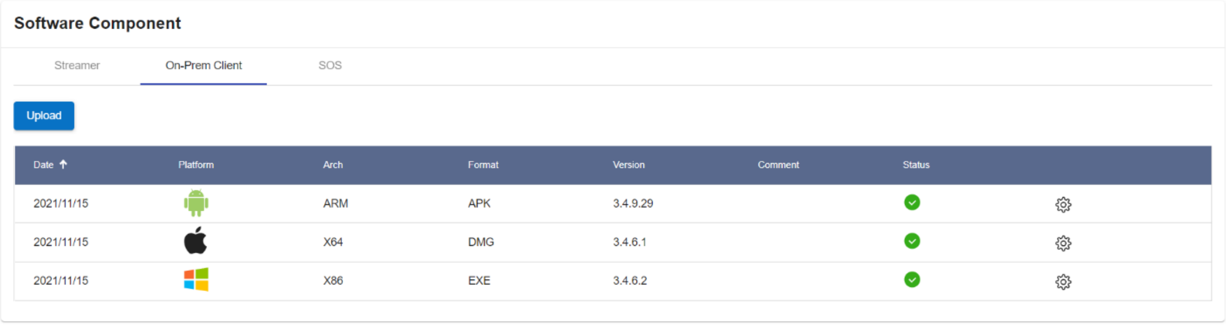
1. Download the streamer installer.
2. Send the installer and the 12-digit code to your use
3. After your users run the installer and enter the cod

12-digit Code

Copyright © 2010 - 2021 Splashtop Inc.

Import Splashtop On-Prem App

1. Log in as Team Owner, go to Gateway's management console > *System* > *Software* > *On-Prem app*, click **Upload** to open upload page.

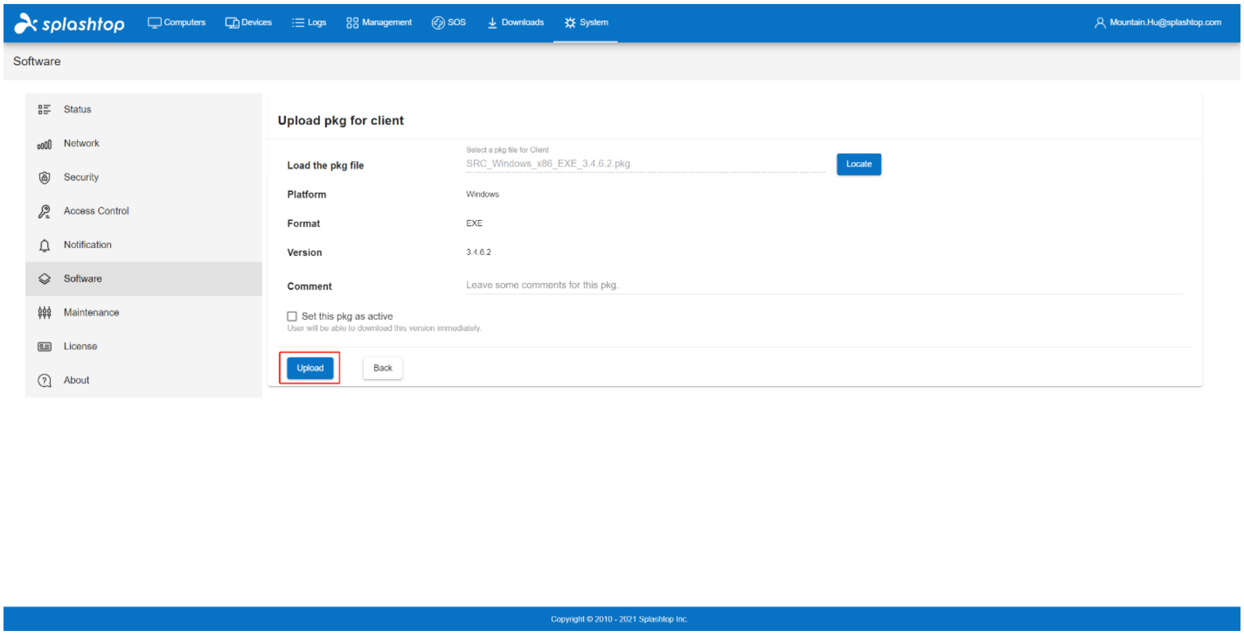


Software Component

Date ↑	Platform	Arch	Format	Version	Comment	Status	
2021/11/15	Android	ARM	APK	3.4.9.29		✓	⚙
2021/11/15	Mac	X64	DMG	3.4.6.1		✓	⚙
2021/11/15	Windows	X86	EXE	3.4.6.2		✓	⚙

2. Locate the PKG file, system will verify if the PKG is packaged for Gateway correctly, and show the package info, like *platform*, *format*, and *version*. Finally click **Upload** to upload the package.

Set it to *active* to make it able for download.



Software

Upload pkg for client

Load the pkg file Select a pkg file for Client SRC_Windows_x86_EXE_3.4.6.2.pkg

Platform Windows

Format EXE

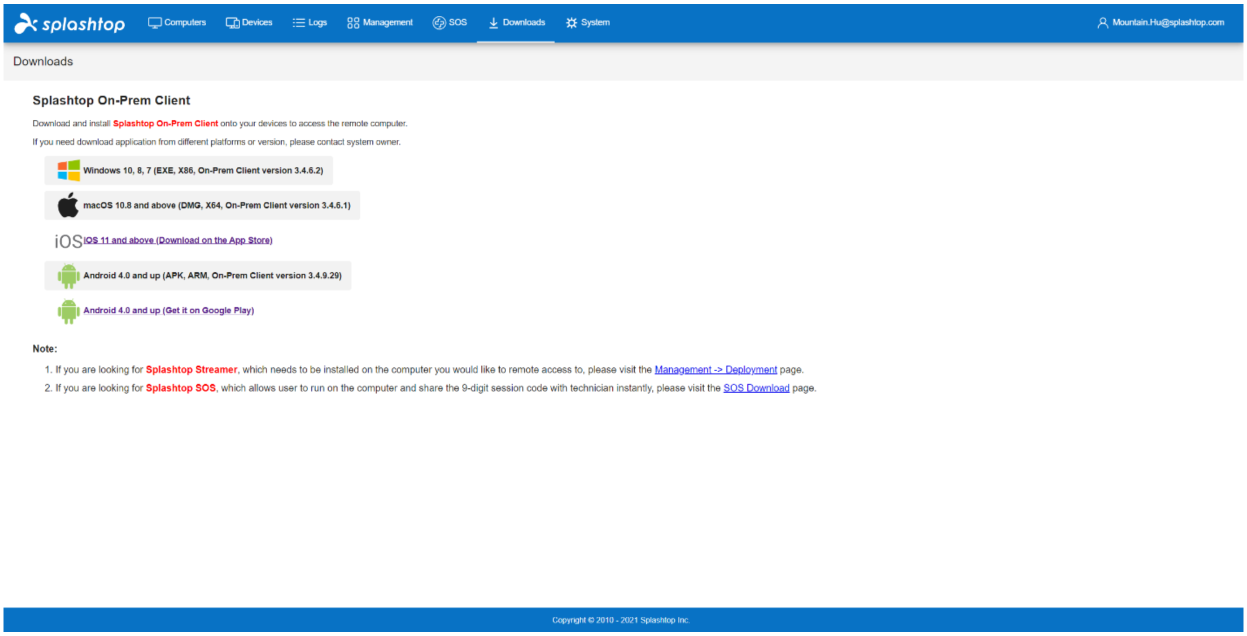
Version 3.4.6.2

Comment Leave some comments for this pkg.

□ Set this pkg as active
User will be able to download this version immediately.

Copyright © 2010 - 2021 Splashtop Inc.

3. Once finished uploading, and set as active, in the **Downloads** page, the newly uploaded component is available for download.



Downloads

Splashtop On-Prem Client

Download and install **Splashtop On-Prem Client** onto your devices to access the remote computer.

If you need download application from different platforms or version, please contact system owner.

- Windows 10, 8, 7 (EXE, X86, On-Prem Client version 3.4.6.2)
- macOS 10.8 and above (DMG, X64, On-Prem Client version 3.4.6.1)
- iOS iOS 11 and above (Download on the App Store)
- Android 4.0 and up (APK, ARM, On-Prem Client version 3.4.9.29)
- Android 4.0 and up (Get it on Google Play)

Note:

1. If you are looking for **Splashtop Streamer**, which needs to be installed on the computer you would like to remote access to, please visit the Management -> Deployment page.
2. If you are looking for **Splashtop SOS**, which allows user to run on the computer and share the 9-digit session code with technician instantly, please visit the SOS Download page.

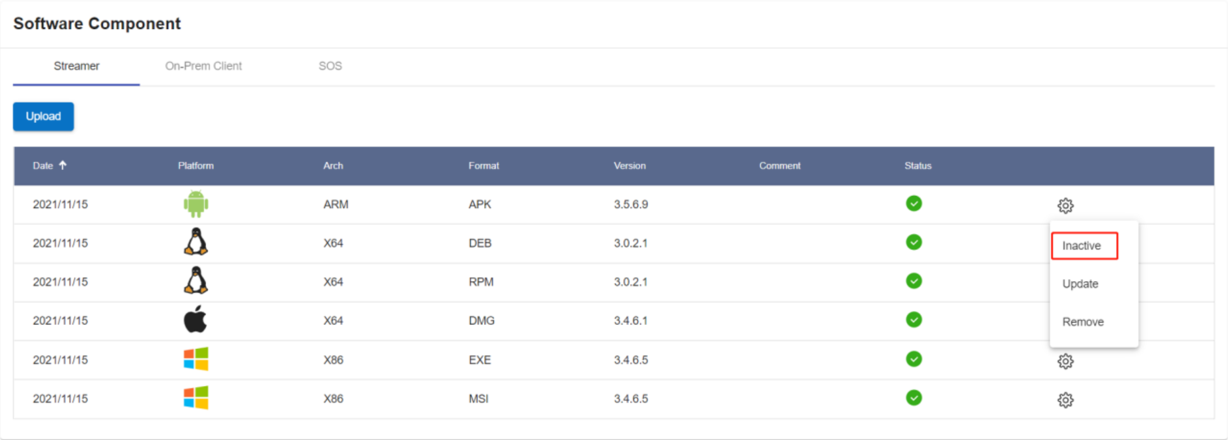
Copyright © 2010 - 2021 Splashtop Inc.

Set software components to active/inactive

Team Owner can set particular Streamer or On-Prem app to be active or inactive, an active component means available for user to download, and inactive component is not available for user to download.

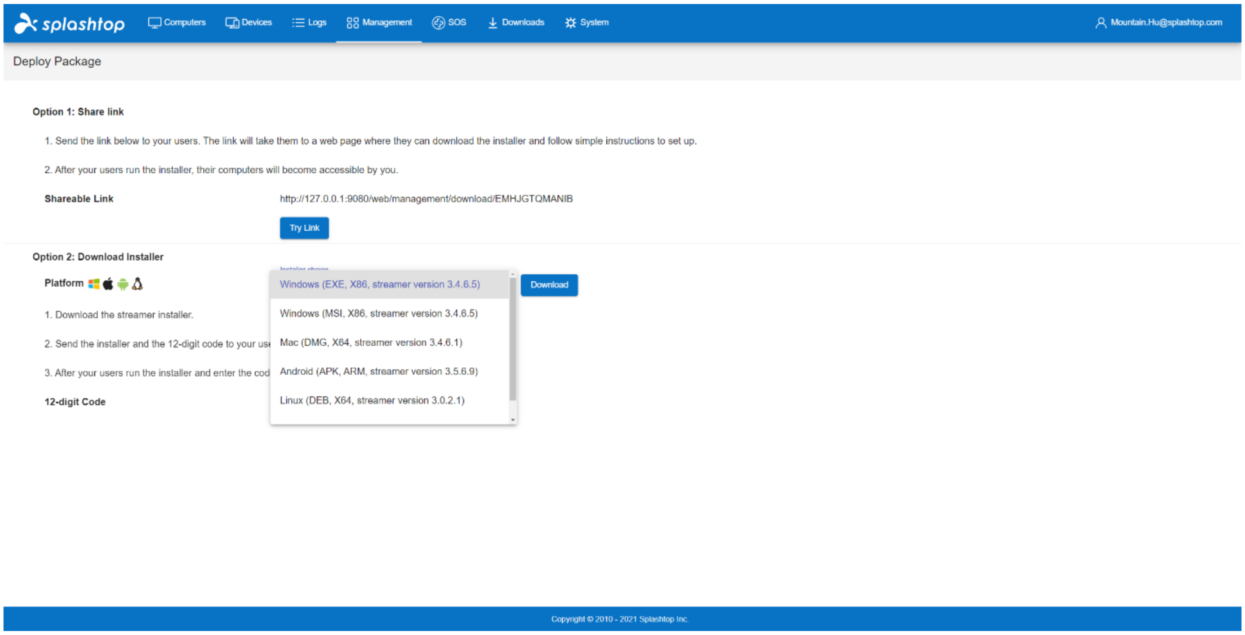
Set Streamer to be active/inactive

1. Log in as **Team Owner**, go to management console > *System* > *Software* > *Streamer*, in the gear button menu, click *inactive/active* to turn the Streamer to be inactive/active.



Date ↑	Platform	Arch	Format	Version	Comment	Status	
2021/11/15	🤖	ARM	APK	3.5.6.9		✓	⚙
2021/11/15	🐧	X64	DEB	3.0.2.1		✓	
2021/11/15	🐧	X64	RPM	3.0.2.1		✓	
2021/11/15		X64	DMG	3.4.6.1		✓	
2021/11/15	⊞	X86	EXE	3.4.6.5		✓	⚙
2021/11/15	⊞	X86	MSI	3.4.6.5		✓	⚙

2. If a Streamer is set to be inactive, it will not be available in the **deploy** page.



Deploy Package

Option 1: Share 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. After your users run the installer, their computers will become accessible by you.

Shareable Link http://127.0.0.1:9080/web/management/download/EMHJGTQMANIB

Option 2: Download Installer

Platform

Installer choice
Windows (EXE, X86, streamer version 3.4.6.5)
Windows (MSI, X86, streamer version 3.4.6.5)
Mac (DMG, X64, streamer version 3.4.6.1)
Android (APK, ARM, streamer version 3.5.6.9)
Linux (DEB, X64, streamer version 3.0.2.1)
Download

1. Download the streamer installer.

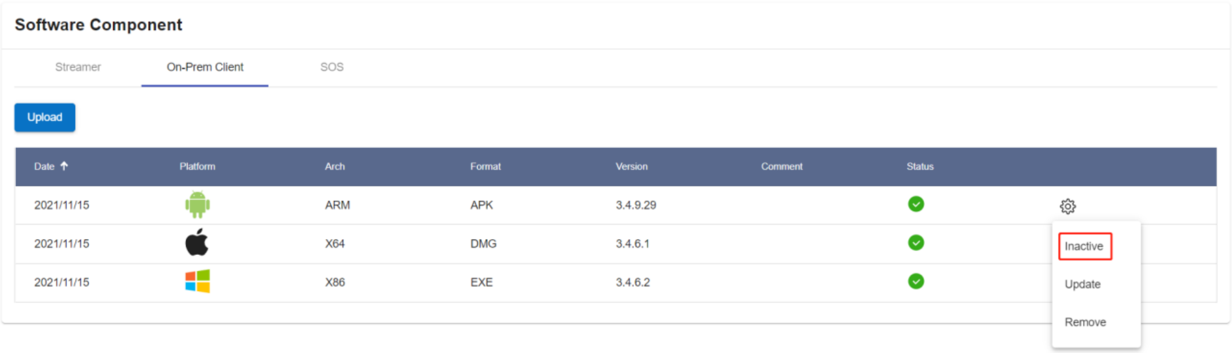
2. Send the installer and the 12-digit code to your use

3. After your users run the installer and enter the cod

12-digit Code

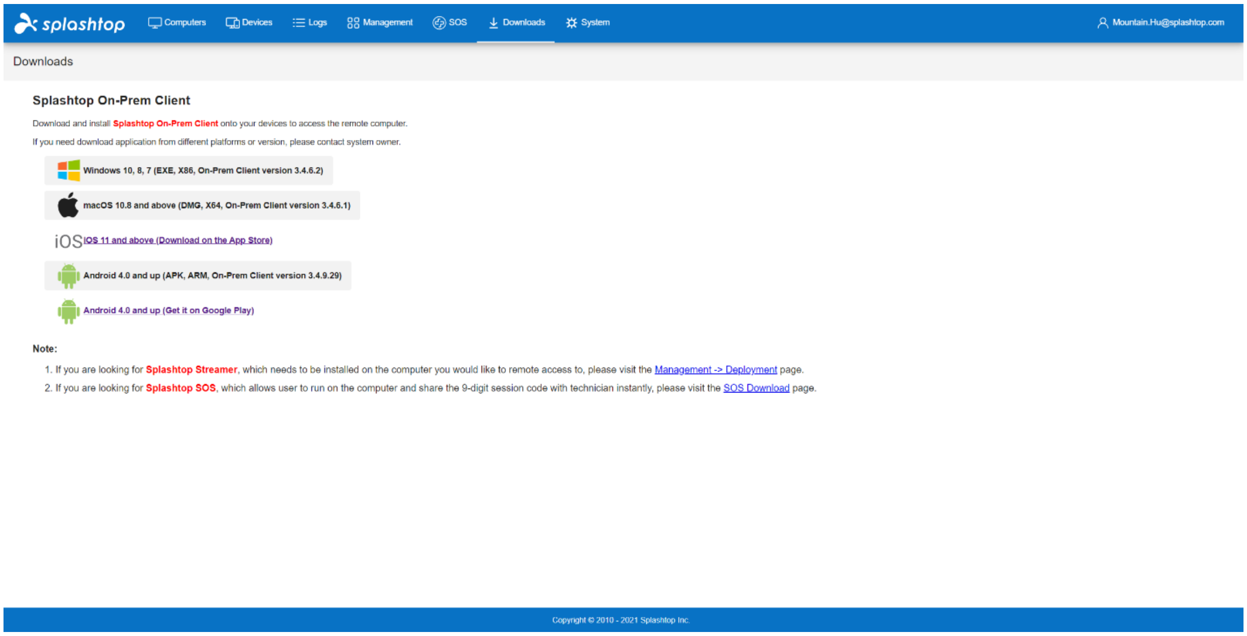
Set Splashtop On-Prem app to be active/inactive

1. Log in as **Team Owner**, go to management console > *System* > *Software* > *On-Prem App*, in the gear button menu, click *inactive/active* to turn the Streamer to be inactive/active.



Date ↑	Platform	Arch	Format	Version	Comment	Status	
2021/11/15		ARM	APK	3.4.9.29		✓	
2021/11/15		X64	DMG	3.4.6.1		✓	
2021/11/15		X86	EXE	3.4.6.2		✓	

2. If an On-Prem app is set to be inactive, it will not be available in the **Downloads** page.



Downloads

Splashtop On-Prem Client

Download and install **Splashtop On-Prem Client** onto your devices to access the remote computer.

If you need download application from different platforms or version, please contact system owner.

- Windows 10, 8, 7 (EXE, X86, On-Prem Client version 3.4.6.2)
- macOS 10.8 and above (DMG, X64, On-Prem Client version 3.4.6.1)
- iOS iOS 11 and above (Download on the App Store)
- Android 4.0 and up (APK, ARM, On-Prem Client version 3.4.9.29)
- Android 4.0 and up (Get it on Google Play)

Note:

1. If you are looking for **Splashtop Streamer**, which needs to be installed on the computer you would like to remote access to, please visit the Management -> Deployment page.
2. If you are looking for **Splashtop SOS**, which allows user to run on the computer and share the 9-digit session code with technician instantly, please visit the SOS Download page.

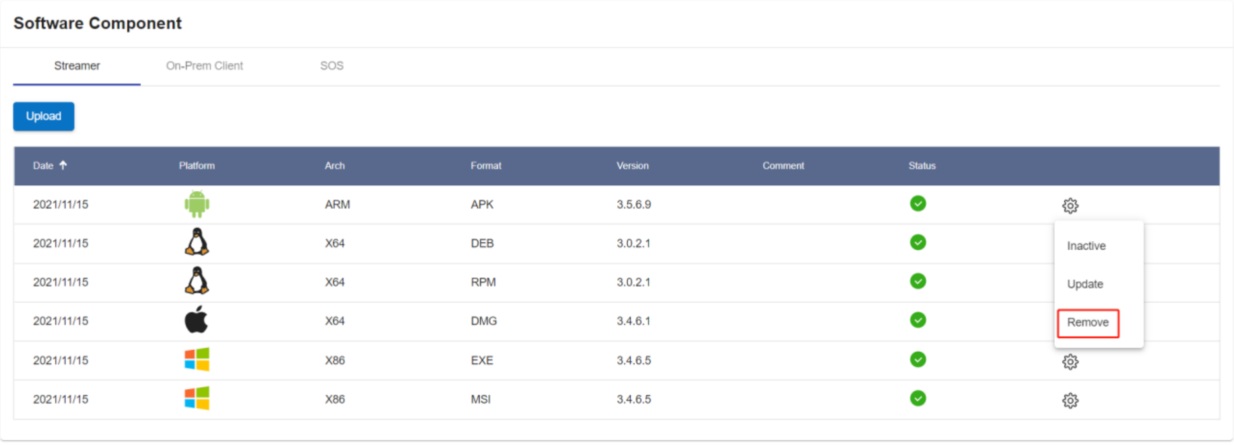
Copyright © 2010 - 2021 Splashtop Inc.

Remove software components

Team Owner can remove particular Streamer or On-Prem app from Splashtop Gateway, a removed component will not be able to be downloaded anymore, but it does not impact the existing installations.

Remove Streamer

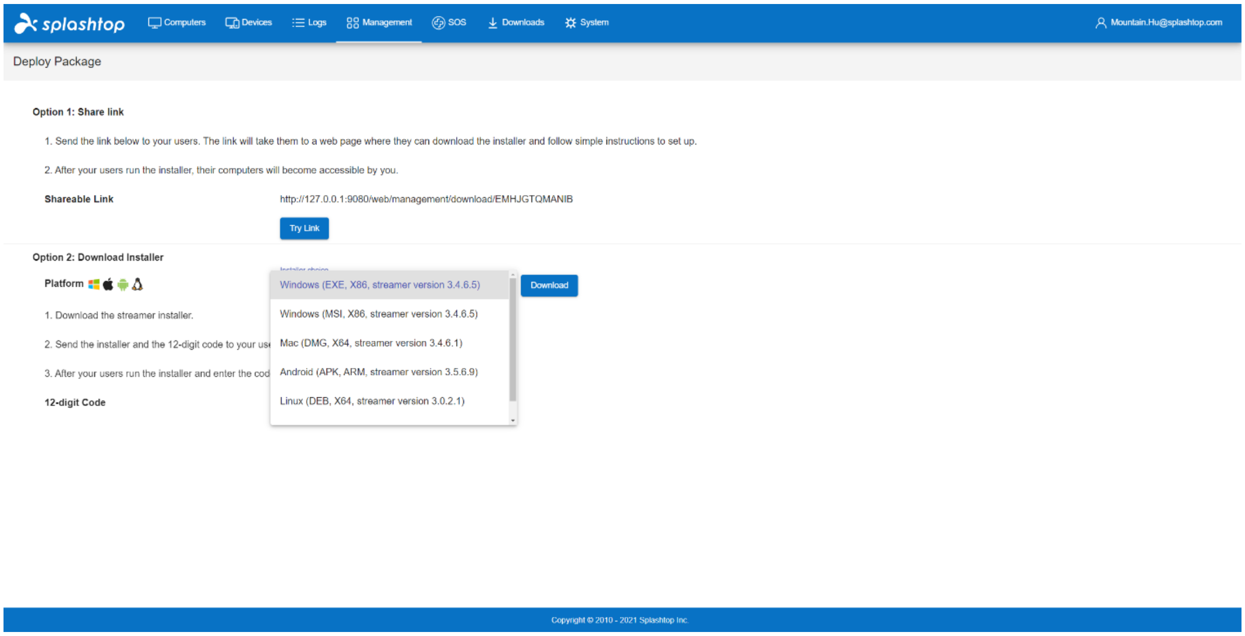
1. Log in as **Team Owner**, go to management console > *System* > *Software* > *Streamer*, in the gear button menu, click *remove* to remove the Streamer from Gateway.



Software Component

Date ↑	Platform	Arch	Format	Version	Comment	Status	
2021/11/15		ARM	APK	3.5.6.9		✓	⚙
2021/11/15		X64	DEB	3.0.2.1		✓	
2021/11/15		X64	RPM	3.0.2.1		✓	
2021/11/15		X64	DMG	3.4.6.1		✓	
2021/11/15		X86	EXE	3.4.6.5		✓	⚙
2021/11/15		X86	MSI	3.4.6.5		✓	⚙

2. If a Streamer is removed, it will not be available in the **deploy** page.



Deploy Package

Option 1: Share 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. After your users run the installer, their computers will become accessible by you.

Shareable Link http://127.0.0.1:9080/web/management/download/EMHJGTQMANIB

Option 2: Download Installer

Platform

1. Download the streamer installer.

2. Send the installer and the 12-digit code to your use

3. After your users run the installer and enter the cod

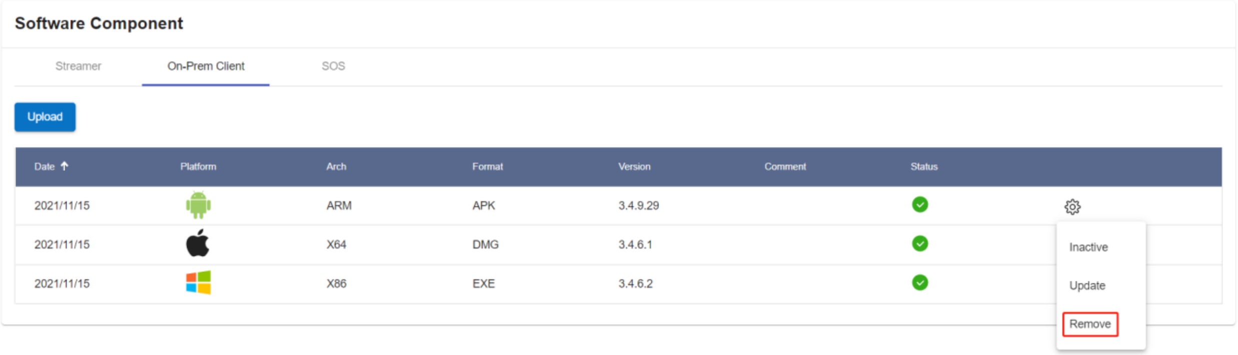
12-digit Code

Windows (EXE, X86, streamer version 3.4.6.5)
Windows (MSI, X86, streamer version 3.4.6.5)
Mac (DMG, X64, streamer version 3.4.6.1)
Android (APK, ARM, streamer version 3.5.6.9)
Linux (DEB, X64, streamer version 3.0.2.1)

Copyright © 2010 - 2021 Splashtop Inc.

Remove Splashtop On-Prem app

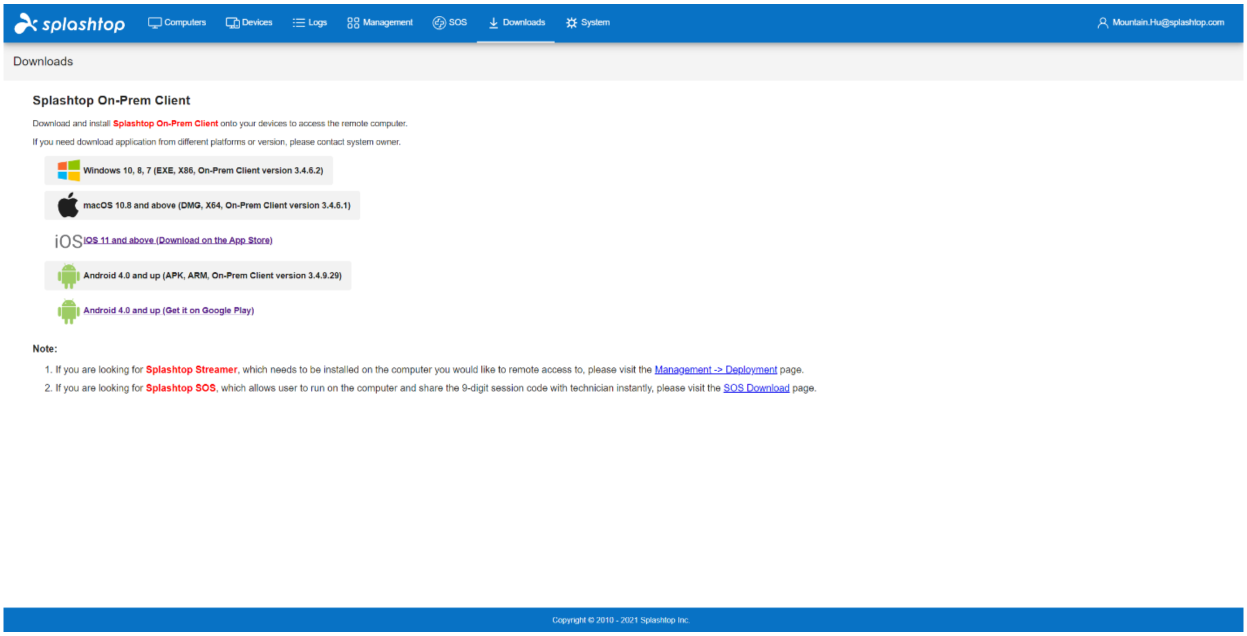
1. Log in as **Team Owner**, go to management console > *System* > *Software* > *On-Prem App*, in the gear button menu, click *Remove* to remove it from Gateway.



Software Component

Date ↑	Platform	Arch	Format	Version	Comment	Status	
2021/11/15	🤖	ARM	APK	3.4.9.29		✓	⚙
2021/11/15		X64	DMG	3.4.6.1		✓	
2021/11/15	⊞	X86	EXE	3.4.6.2		✓	

2. If an On-Prem app is removed, it will not be available in the **Downloads** page.



Downloads

Splashtop On-Prem Client

Download and install **Splashtop On-Prem Client** onto your devices to access the remote computer.

If you need download application from different platforms or version, please contact system owner.

- Windows 10, 8, 7 (EXE, X86, On-Prem Client version 3.4.6.2)
- macOS 10.8 and above (DMG, X64, On-Prem Client version 3.4.6.1)
- iOS 11 and above (Download on the App Store)
- Android 4.0 and up (APK, ARM, On-Prem Client version 3.4.9.29)
- Android 4.0 and up (Get it on Google Play)

Note:

1. If you are looking for **Splashtop Streamer**, which needs to be installed on the computer you would like to remote access to, please visit the Management -> Deployment page.
2. If you are looking for **Splashtop SOS**, which allows user to run on the computer and share the 9-digit session code with technician instantly, please visit the SOS Download page.

Copyright © 2010 - 2021 Splashtop Inc.

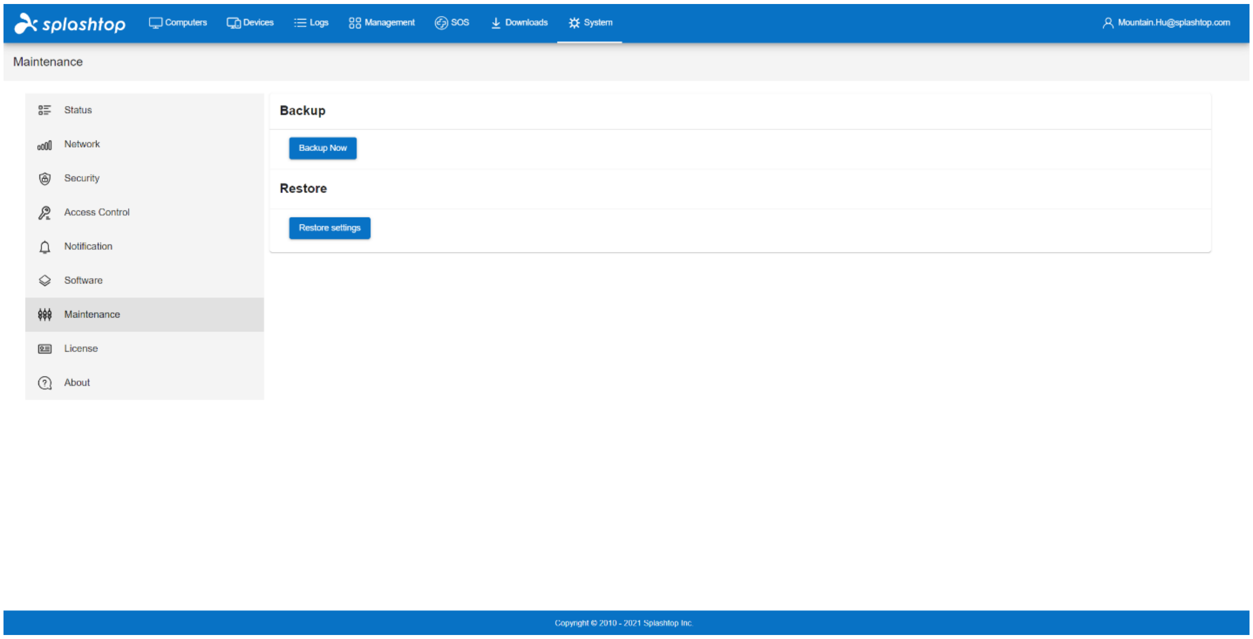
Maintenance

It is important to back up system regularly. It helps to recover Splashtop On-Prem system after unexpected hardware/software failure or accidental data deletion. System backups are essential for protection against data loss that can completely disrupt business operations.

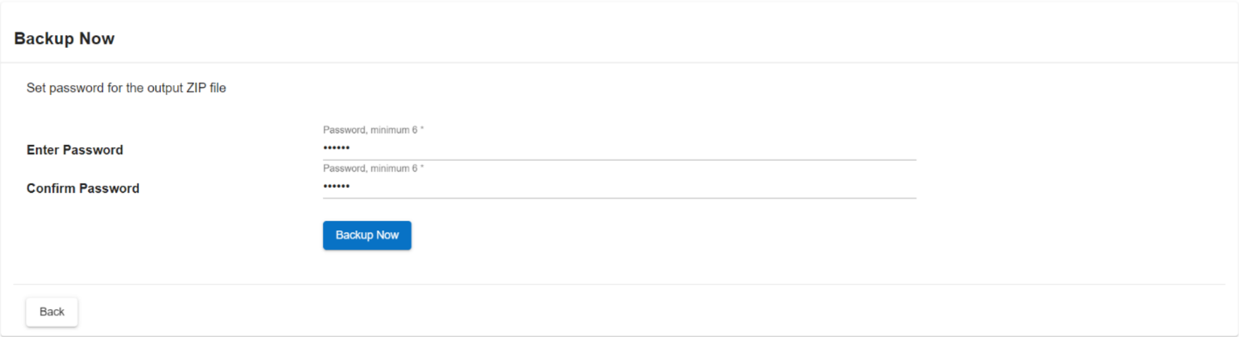
Backup

To start a system backup or restore task, you have to use the **system owner account** to log in to the **Splashtop Gateway web portal**. The system owner account is the email address used to activate the license of Splashtop On-Prem system.

After logging in to the Gateway web portal, go to the **System** menu bar, and then navigate to **Maintenance** page.



Click on **Backup Now** button. You are required to set a password for the ZIP file to be produced, before initiating the whole backup process.


Backup Now

Set password for the output ZIP file

Enter Password: Password, minimum 6 * ••••••

Confirm Password: Password, minimum 6 * ••••••

One more click on **Backup Now** button, a password protected ZIP file will be automatically saved into your browser download folder. This ZIP file contains an SQL script with detailed system configuration, including the system settings, users and groups, deployed computers and client devices, logs and etc. However, license is not included in the backup file, hence the system will require license re-activation after being restored from the SQL script.

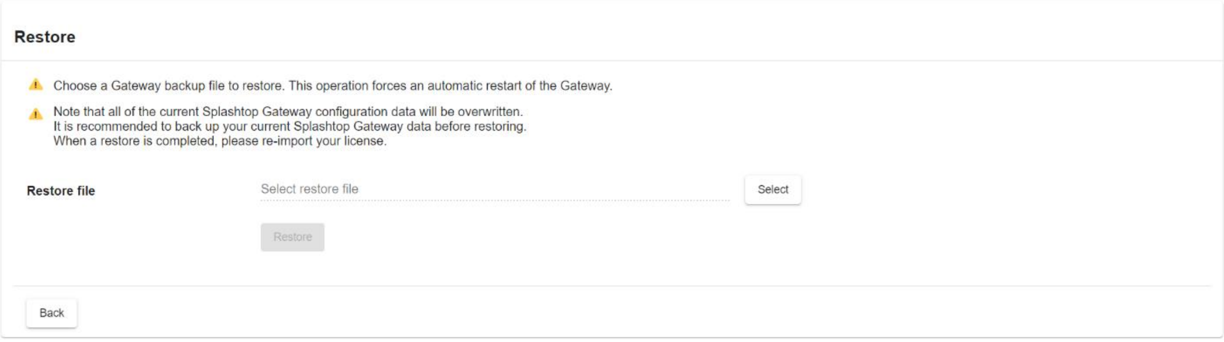
Restore

Before a restore task is performed, it is important to make sure:

- You have the license key for Splashtop On-Prem at hand. You will be asked to activate the license again after a system restoration.
- Get the restore file ready by unzipping the backup ZIP file and saving the SQL script into a local folder.
- Back up the current system as all existing configuration will be deleted permanently.

Same as **Backup**, you have to log in with the system owner account to the Splashtop Gateway web portal, click on System menu and navigate to the **Maintenance** page.

Click **Restore settings** button and click on **Select** button to browse the SQL script file.



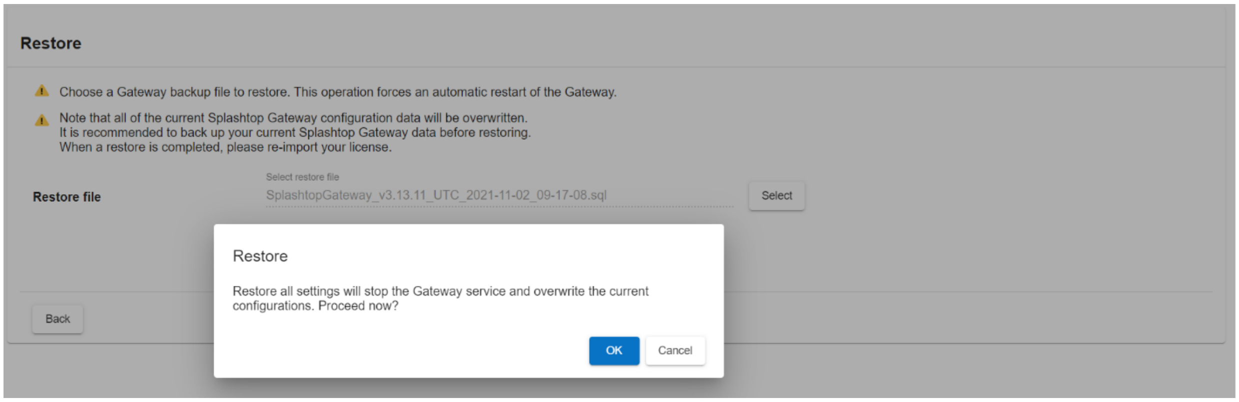
Restore

⚠ Choose a Gateway backup file to restore. This operation forces an automatic restart of the Gateway.

⚠ Note that all of the current Splashtop Gateway configuration data will be overwritten.
It is recommended to back up your current Splashtop Gateway data before restoring.
When a restore is completed, please re-import your license.

Restore file: Select restore file

Click on **Restore** button and confirm to restore the system.



Restore

⚠ Choose a Gateway backup file to restore. This operation forces an automatic restart of the Gateway.

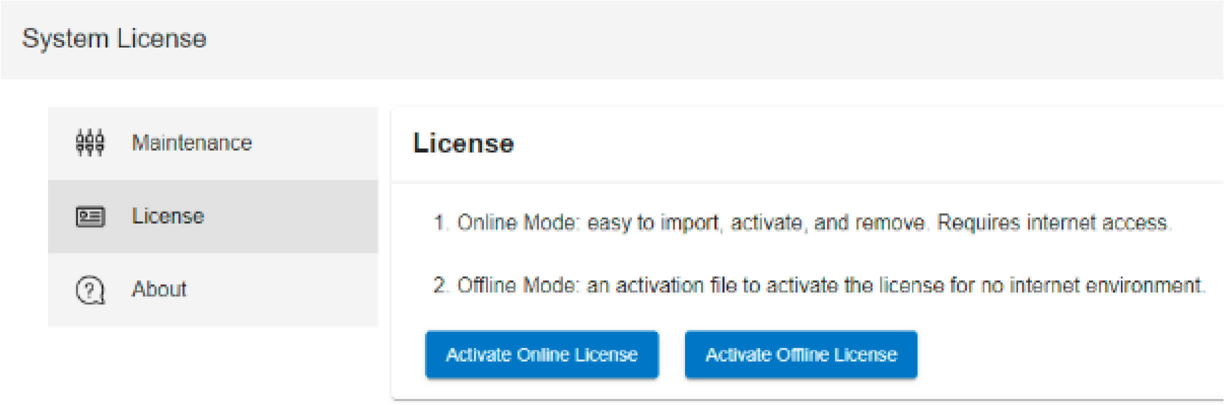
⚠ Note that all of the current Splashtop Gateway configuration data will be overwritten.
It is recommended to back up your current Splashtop Gateway data before restoring.
When a restore is completed, please re-import your license.

Restore file: Select restore file: SplashtopGateway_v3.13.11_UTC_2021-11-02_09-17-08.sql

Restore

Restore all settings will stop the Gateway service and overwrite the current configurations. Proceed now?

After the Splashtop On-Prem system is successfully restored, the page will automatically be redirected to **License** page.



License

1. Online Mode: easy to import, activate, and remove. Requires internet access.

2. Offline Mode: an activation file to activate the license for no internet environment.

Activate the license through online or offline mode, depending on the type of license you acquired before.

Now you have done a successful system restoration.

Notification

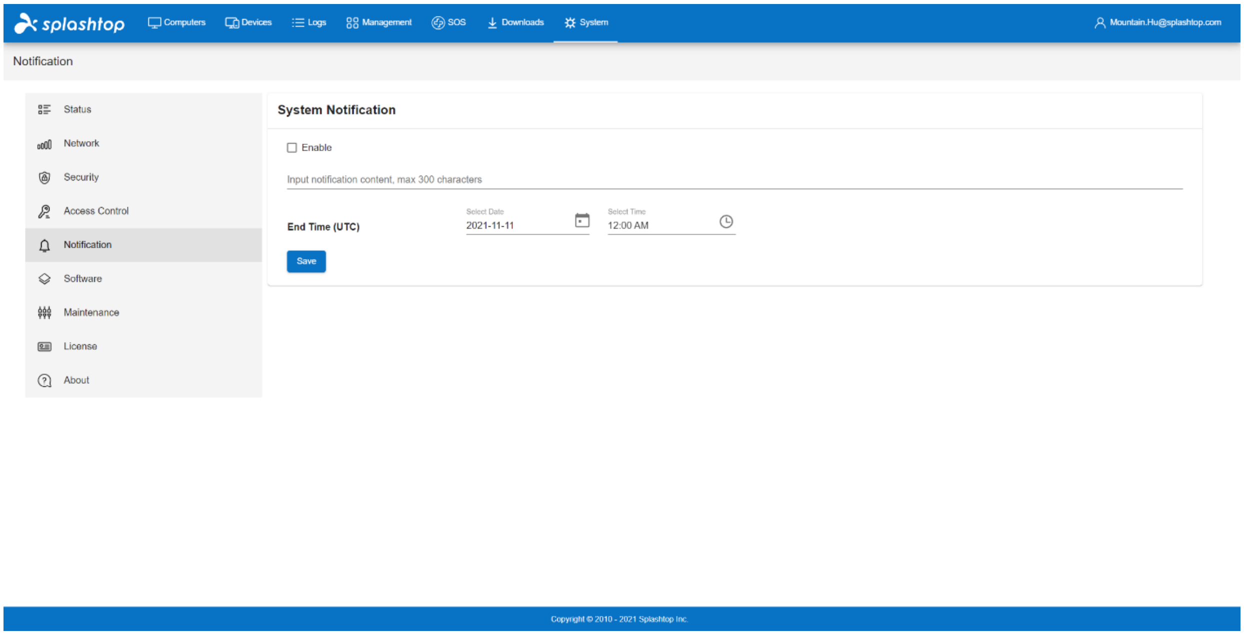
A Splashtop On-Prem Team Owner can publish a system notification from the **Notification** page, in order to notify the users if there is an expected downtime due to system maintenance, or if any update on the endpoints is available.

The Notification page is available for a Team Owner account at **Splashtop Gateway** > **System** > **Notification**

To publish a notification, firstly check the **Enable** box.

Type the notification content in the blank space below and set an End Time when the notification will stop being seen by the users.

Note: System Notification is **in UTC Time. Please calculate time difference before publish notification.**



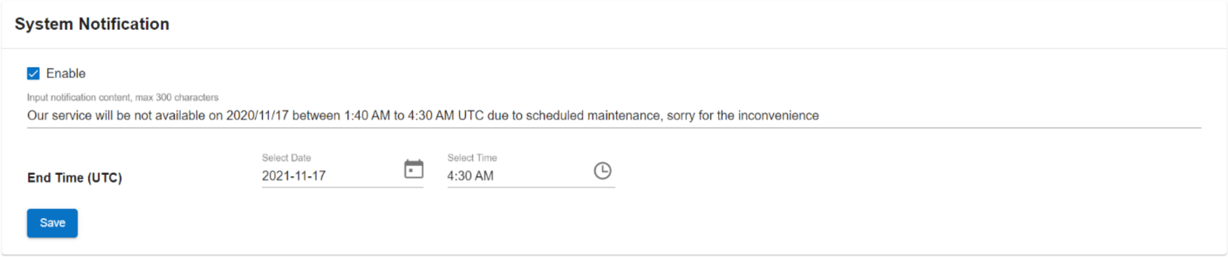
System Notification

□ Enable

Input notification content, max 300 characters

End Time (UTC) Select Date 2021-11-11 Select Time 12:00 AM

Take a notification as below for example:



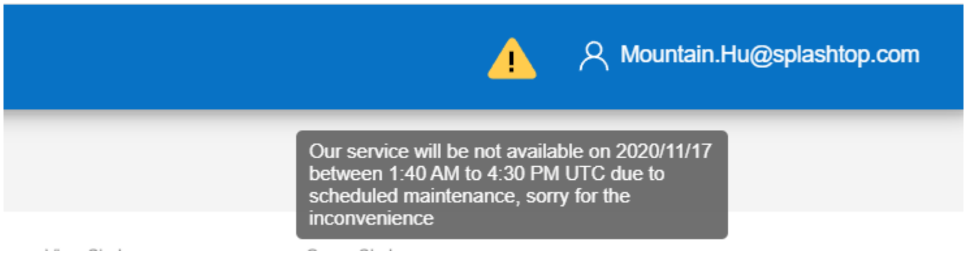
System Notification

☑ Enable

Input notification content, max 300 characters
Our service will be not available on 2020/11/17 between 1:40 AM to 4:30 AM UTC due to scheduled maintenance, sorry for the inconvenience

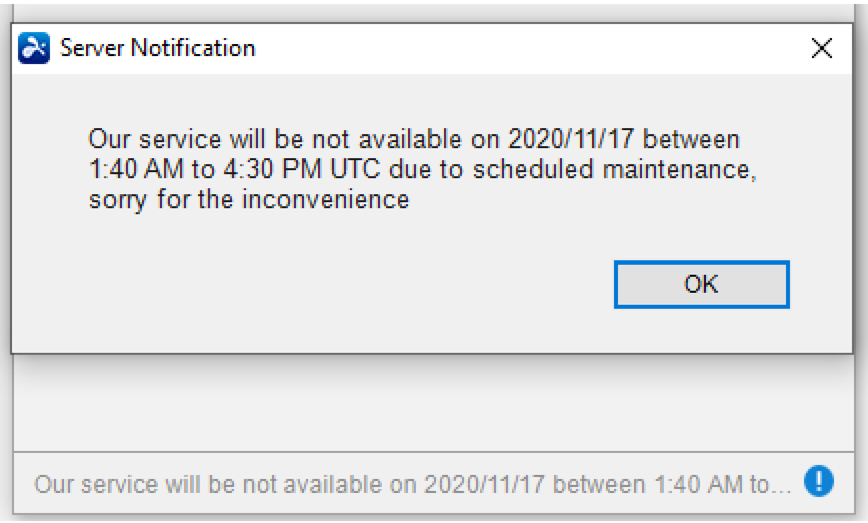
End Time (UTC) Select Date 2021-11-17 Select Time 4:30 AM

This notification will be displayed at the right top corner of the Gateway page with a yellow exclamation mark. Hovering over the mark, the notification will be displayed.



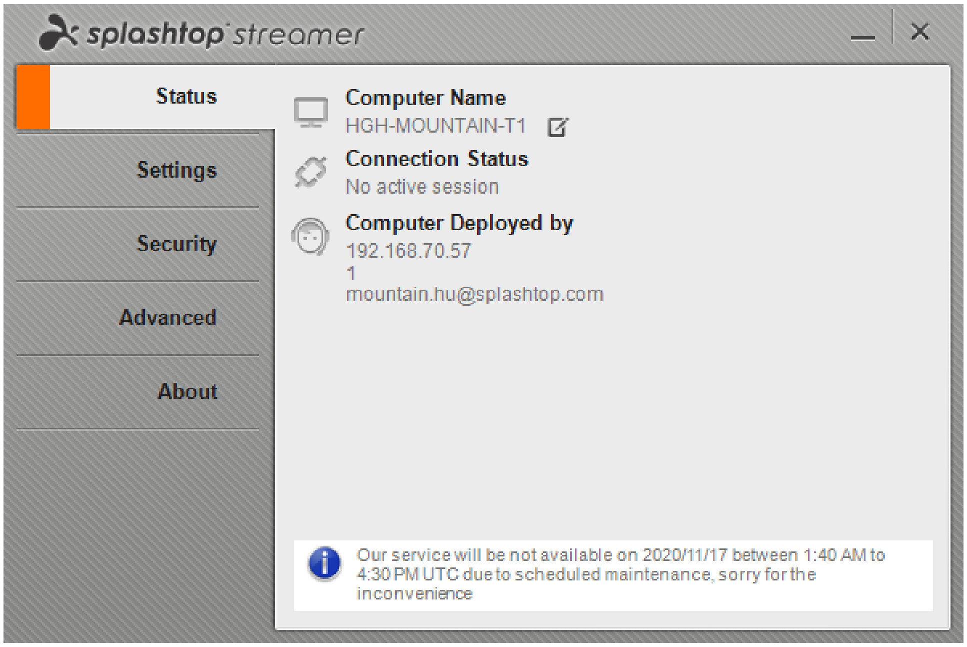
Our service will be not available on 2020/11/17 between 1:40 AM to 4:30 PM UTC due to scheduled maintenance, sorry for the inconvenience

This notification also can be seen at any active On-Prem app (click blue exclamation at bottom to see more) or Streamer from current enabled time to the End Time, i.e. 4:30 AM on the 24th Dec 2020.



Our service will be not available on 2020/11/17 between 1:40 AM to 4:30 PM UTC due to scheduled maintenance, sorry for the inconvenience

Our service will be not available on 2020/11/17 between 1:40 AM to...



Computer Name
HGH-MOUNTAIN-T1

Connection Status
No active session

Computer Deployed by
192.168.70.57
1
mountain.hu@splashtop.com

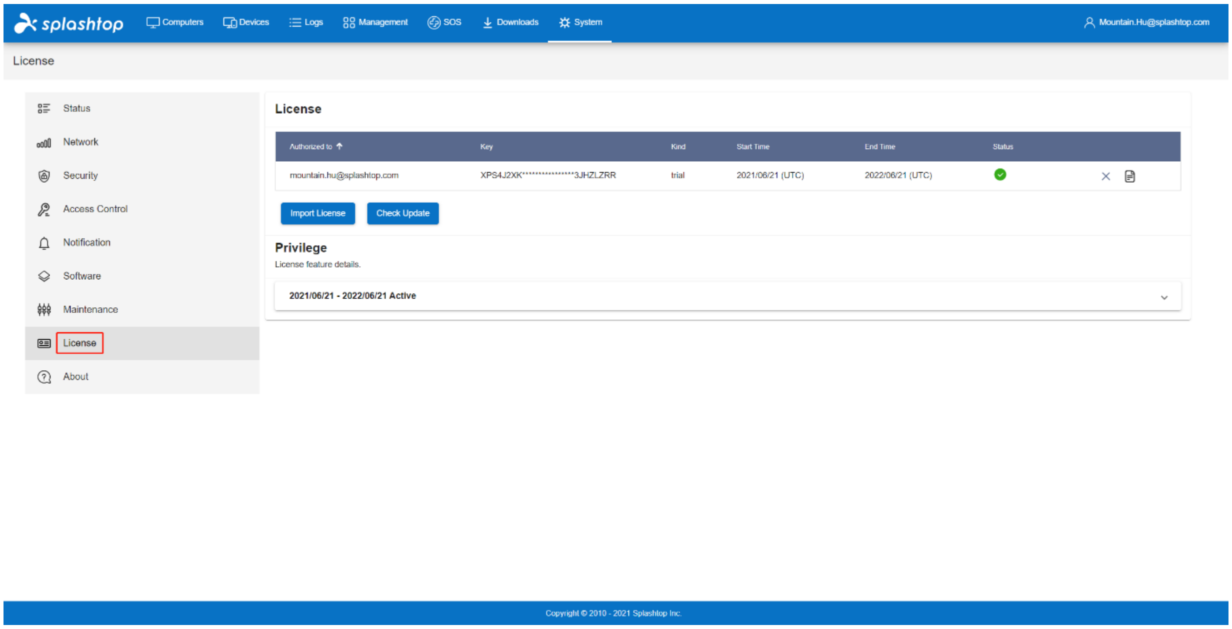
Our service will be not available on 2020/11/17 between 1:40 AM to 4:30 PM UTC due to scheduled maintenance, sorry for the inconvenience

On Prem License

Understand your license and privileges

Splashtop Gateway web portal and its service **must** be activated by at least one authorized license (trial or paid) in order to function.

To access the information of your license, open Splashtop Gateway in a browser using **Team Owner**'s account, and go to **System** > **License**.



License

Authorized to ↑	Key	Kind	Start Time	End Time	Status	
mountain.hu@splashtop.com	XPS4J2XK****************3JHZLZRR	trial	2021/06/21 (UTC)	2022/06/21 (UTC)	✓	×

Privilege

License feature details.

2021/06/21 - 2022/06/21 Active

Splashtop On-Prem supports **multi-licensing**, meaning you can apply two or more licenses with different periods of validity and privilege sets to the same system. On the License page, information including license owner, key number, validity and status is displayed for each license.

You can check the privileges coming with the specific license by clicking on the icon at end of the line, or go to the Privilege session and click on the license validity to show its license details.

A license is described in three parts: general, unattended feature, attended feature (also named SOS). An unattended session refers to a scenario where no acknowledgement is required from the remote computer to establish a remote connection, while an attended session needs help from someone at the remote computer to set up the connection. Refer to Usage scenarios for more info.

To understand what privileges your license is entitled to, please check the following table which explains the features associated to license items.

Validity	**Meaning**
Date range	The date range of the following privilege set
Max unattended user	Max number of unattended user accounts can be enabled
Max Unattended Concurrent User	Max number of unattended users can establish the sessions at the same time
Max Unattended Streamer	Max number of unattended Streamers can be deployed
Max Attended User	Max number of user accounts can be enabled with SOS feature
Max Attended Concurrent User	Max number of attended users can establish the SOS session at the same time
Unattended Feature	
Max Remote Session	Max number of unattended concurrent sessions on the entire system, even it's set to *unlimited*, the **Max Unattended Concurrent User** policy will still be enforced
Max concurrent remote session to one Streamer	Max number of users can be allowed to access to one Streamer at the same time
Max File Transfer (outside session)	Max number of outside session file transfer sessions can be established on the entire system
Max concurrent file transfer (outside session) to one Streamer	Max number of outside session file transfer allowed to one Streamer at the same time

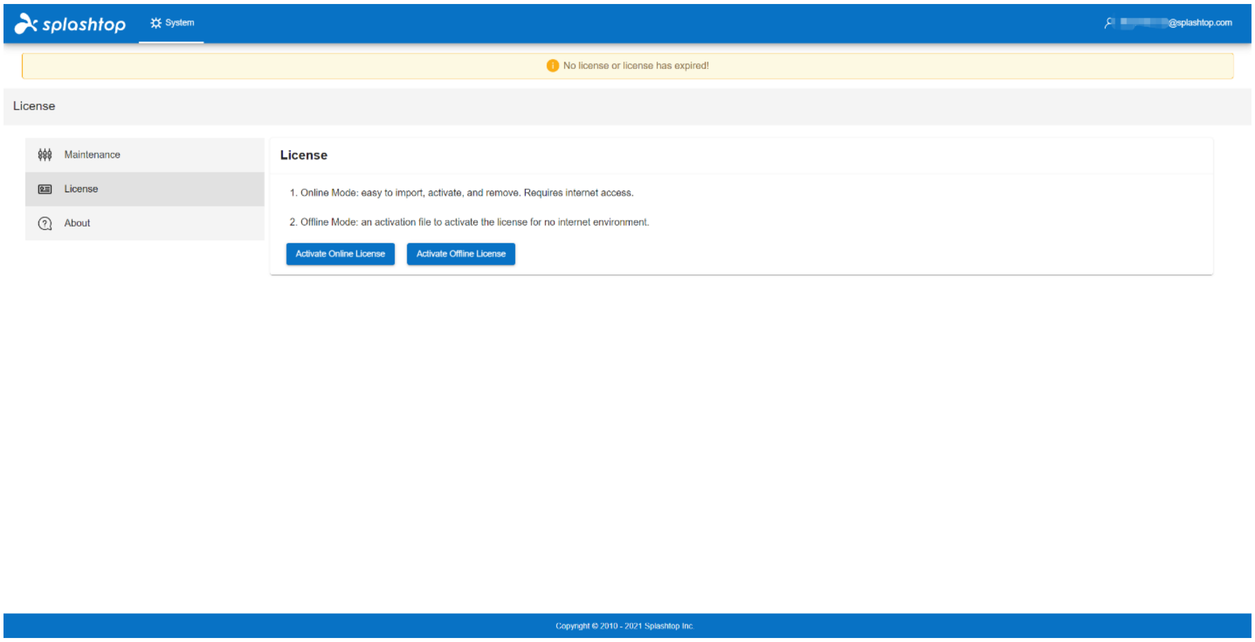
Max Chat (outside session)	Max number of outside session chat sessions on the entire system
Max concurrent chat (outside session) to one Streamer	Max number of outside session chat sessions can be established to one Streamer at the same time
Remote Print	Remote print feature is allowed or not
Remote Wakeup	Remote wakeup feature is allowed or not
Remote Reboot	Remote reboot feature is allowed or not
Remote Command	Remote command feature is allowed or not
Audio	Audio redirection feature is allowed or not
Computer Streamer	Computer Streamer is allowed or not, which means Windows, Mac, Linux (coming soon)
Mobile Streamer	Mobile Streamer is allowed or not, which means Android
Terminal Session	Access RDP terminal session is allowed or not
Multi-to-one Monitor	Multiple screen to one screen is allowed or not
Multi-to-multi Monitor	Multiple screen to multiple screen is allowed or not
Session Recording	Session recording is allowed or not
Attended feature	
Max Remote Session	Max number of attended sessions on the entire system,

	even it's set to *unlimited*, the **Max Attended Concurrent User** policy will still be enforced
Max concurrent remote session to one Streamer	Max number of users can be allowed to access to one Streamer at the same time
Computer Streamer	Computer Streamer is allowed or not, which means Windows, Mac, Linux (coming soon)
Mobile Streamer	Android Streamer is allowed or not
Multi-to-one Monitor	Multiple screen to one screen is allowed or not
Multi-to-multi Monitor	Multiple screen to multiple screen is allowed or not
Session Recording	Session recording is allowed or not

Activate license

Splashtop Gateway supports license activation in two modes, online activation and offline activation. You will be required to activate the license before you are able to use the system.

You need to login as Team Owner to activate the license, which is in Gateway's **System** > **License** page.



No license or license has expired!

License

License

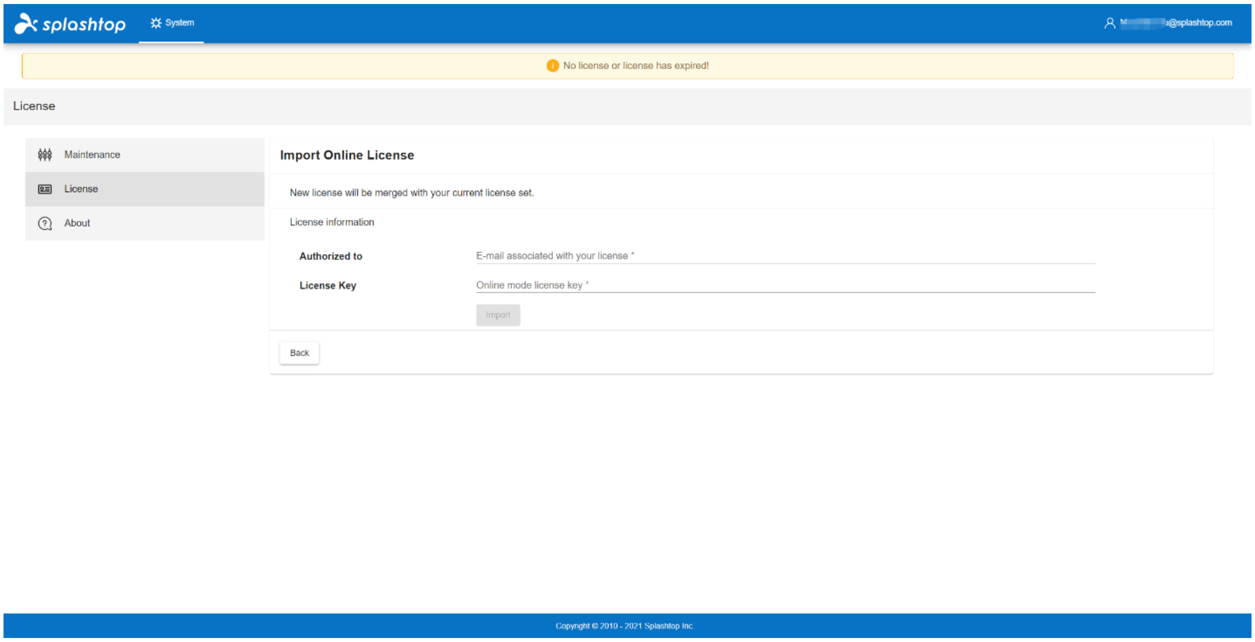
1. Online Mode: easy to import, activate, and remove. Requires internet access.

2. Offline Mode: an activation file to activate the license for no internet environment.

Online license activation

For online license activation, click Import Online License, input the Authorized to and License key which you obtain from Splashtop Sales.

Notice: Your Splashtop Gateway need to have Internet access, and the outbound **license.splashtop.com:443** should not be blocked by your firewall.



No license or license has expired!

License

Import Online License

New license will be merged with your current license set.

License information

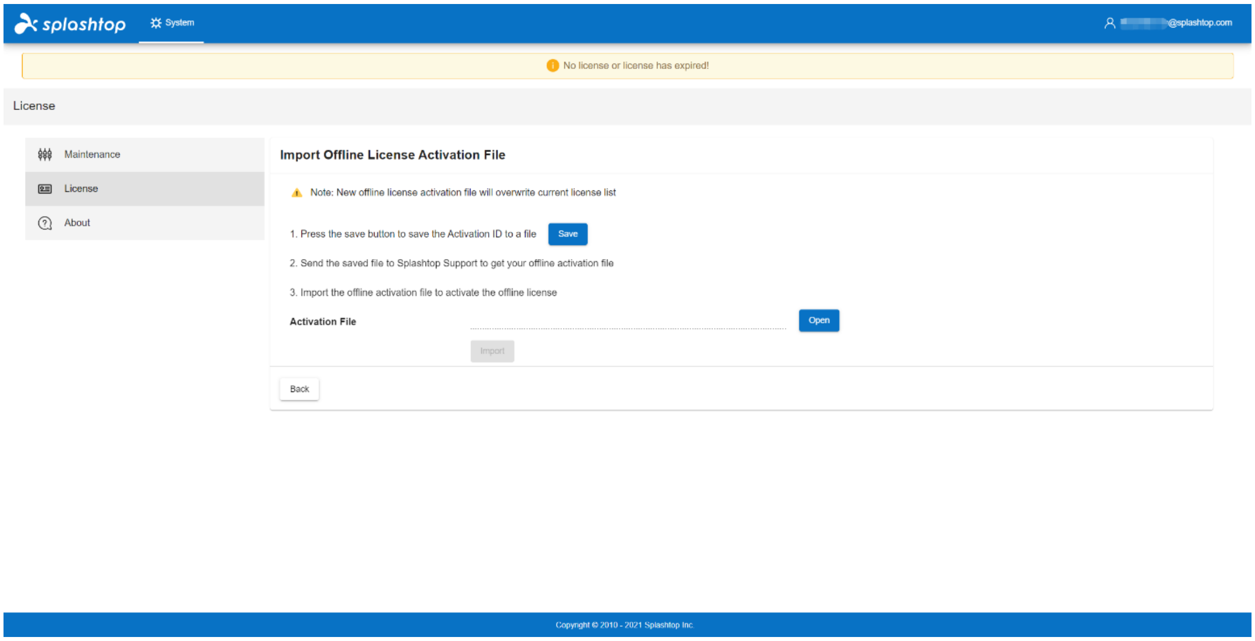
Authorized to E-mail associated with your license *

License Key Online mode license key *

Copyright © 2010 - 2021 Splashtop Inc.

Offline license activation

If your Splashtop Gateway has no Internet access, you can choose offline license activation.



No license or license has expired!

License

Import Offline License Activation File

Note: New offline license activation file will overwrite current license list

1. Press the save button to save the Activation ID to a file Save
2. Send the saved file to Splashtop Support to get your offline activation file
3. Import the offline activation file to activate the offline license

Activation File Open

Copyright © 2010 - 2021 Splashtop Inc.

1. Click **Import Offline License** on license page, click **Save** to download Activation ID.

2. Send the activation ID file to Splashtop Sales, Splashtop Sales will generate offline activation file and send back to you.

3. Click **Open** to upload the activation file and click **Import** to finish offline license activation

About

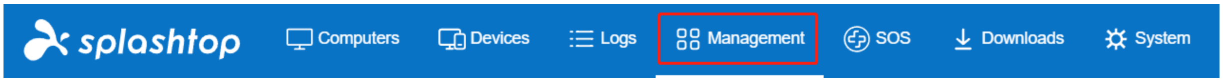
The About page provides relevant system information, includes:

- **Version**: version number of the Splashtop On-Prem followed by the build number
- **Build Date**: the date when this release was built
- **Valid to**: end date of license current privilege validity
- **Terms of Service**: terms and conditions of your use of Splashtop's Services between you and Splashtop
- **Privacy Policy**: documentation describing Splashtop's privacy policy for your peruse
- **Support site**: a link directing you to Splashtop support site. Please choose Splashtop On-Prem in the linked page if you are a Splashtop On-Prem user.

Management Console

Introduction

Management console is an important panel in Splashtop Gateway web portal for Team Administrator and Group Manager to manage system configurations, such as the users and groups, computers and end points, deployment package, security settings, and etc.



The menu available in management console varies depending on the role you are assigned to, whether a team administrator, a group manager or just an ordinary member.

Member user is not allowed to access the management console, so Management tab does not appear in the menu.

Team Admin can see 8 items in Management context menu: Users, All Computers, All Devices, Grouping, Deployment, 1-to-Many Actions, 1-to-Many Schedules and Reports.

The team Owner has 10 items in Management tab: Users, All Computers, All Devices, Grouping, Scheduled Access, Deployment, 1-to-Many Actions, 1-to-Many Schedules, Reports and Settings.

We will explain the functionality of each item in Management Console from the team owner's perspective.

- **Users**
- **All Computers**
- **All Device**
- **Grouping**
- **Scheduled Access**
- **Deployment**
- **1-to-Many Actions**
- **1-to-Many Schedules**
- **Reports**

- **Settings**

Users

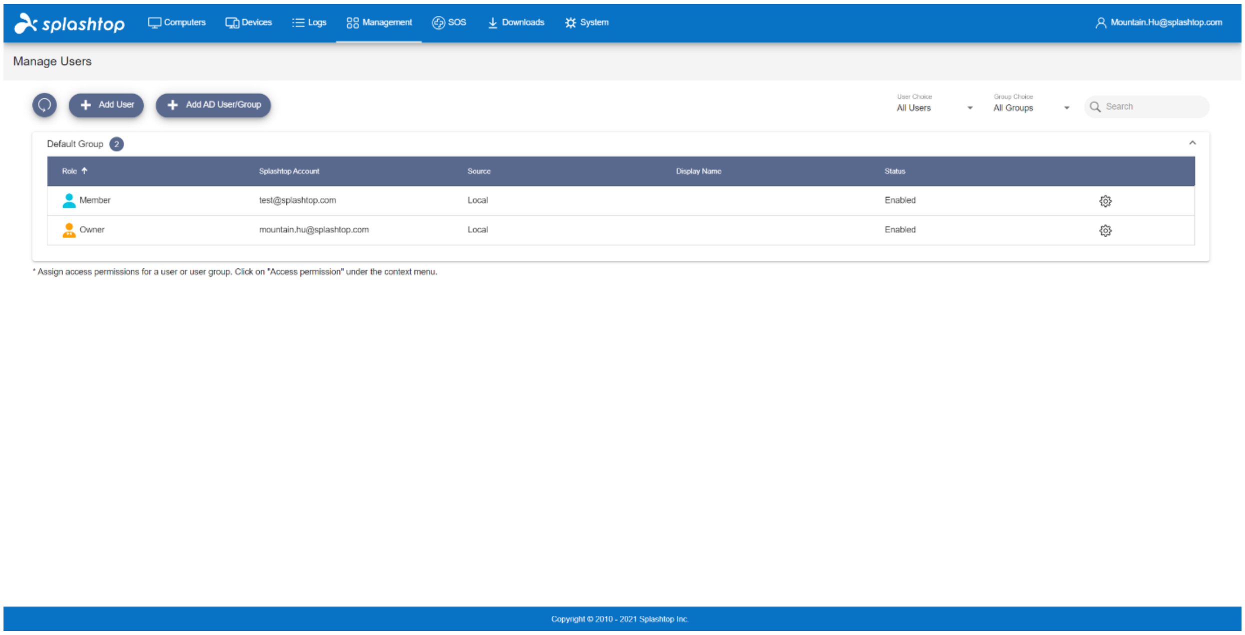
Team Owner/Admin can use this page to create a new user or modify attributes of existing users.

There are two types of user account in Splashtop On-Prem: local account and active directory (AD) account. To add an AD user, Team Owner should firstly configure the active directory server in **System** settings.

User attributes, including role, group, access permission, display name, password, 2-step verification, are available to configure in the Users page.

Create user accounts

Users management is in https://{gateway} > **Management** > **Users**.



Manage Users

User Choice: All Users
Group Choice: All Groups

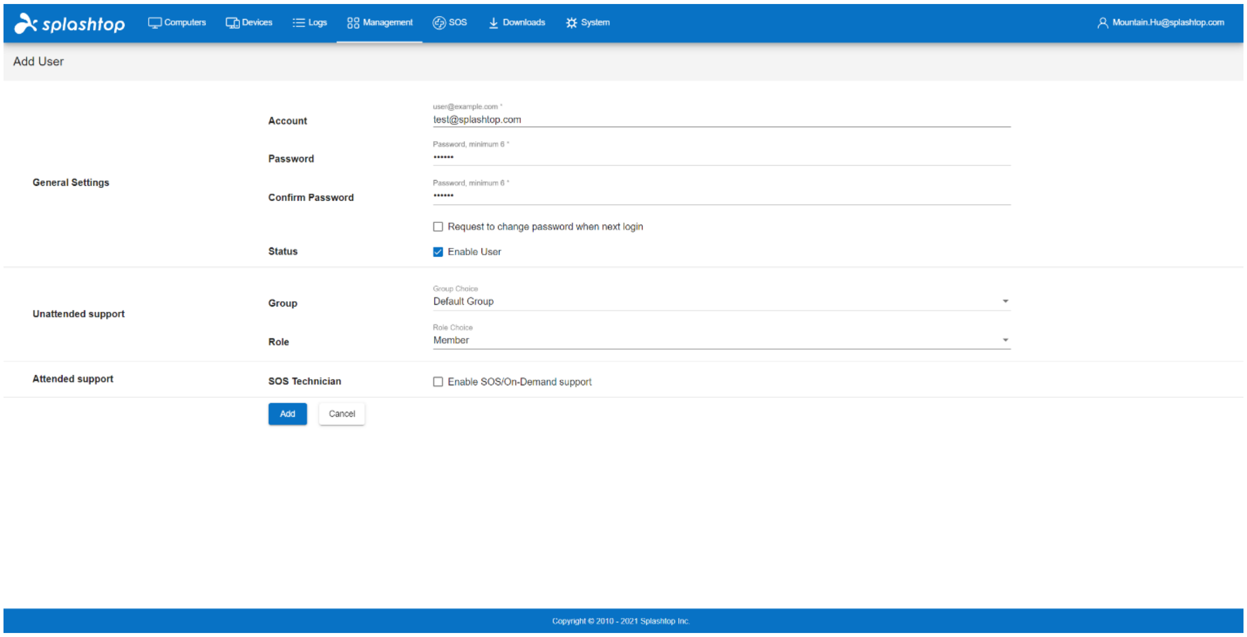
Default Group 2

Role ↑	Splashtop Account	Source	Display Name	Status
Member	test@splashtop.com	Local		Enabled
Owner	mountain.hu@splashtop.com	Local		Enabled

* Assign access permissions for a user or user group. Click on "Access permission" under the context menu.

Copyright © 2010 - 2021 Splashtop Inc.

Create local account



Add User

General Settings

Account: user@example.com * test@splashtop.com

Password: Password, minimum 6 * ••••••

Confirm Password: Password, minimum 6 * ••••••

□ Request to change password when next login

Status: ☑ Enable User

Unattended support

Group: Group Choice Default Group

Role: Role Choice Member

Attended support

SOS Technician: □ Enable SOS/On-Demand support

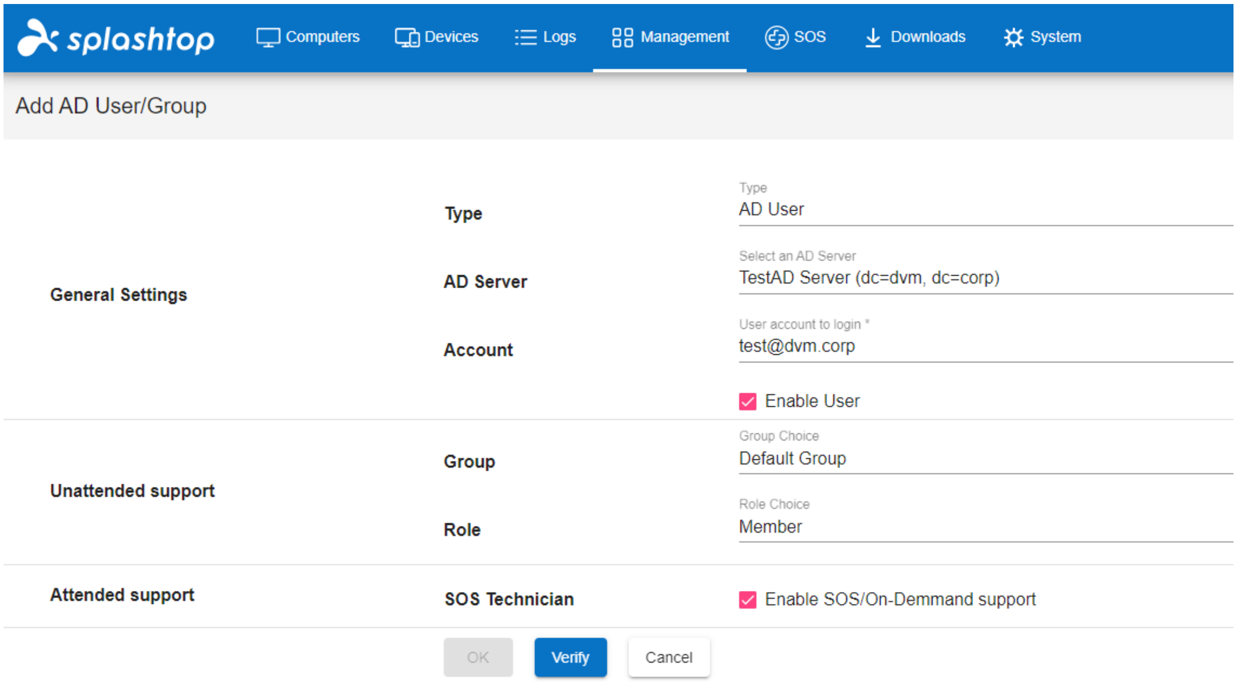
Copyright © 2010 - 2021 Splashtop Inc.

Field	***Meaning***
Account	This is the user's login account, it is unique in the system.
Password	Minimum 6 characters.
Generate Password	This helps to generate a more random password for secure reason.
Request change password when next login	With this option, when user log-in to the system, he/she will be required to change the password.
Group	User can be grouped into different groups, group is a great way to manage users / access permissions.

Role	There are two types of roles in the system: Admin: An admin can manage the users, computers, grant access permissions etc. Admins can have remote sessions too. Member: A member can only have remote sessions with the computers with access permission granted.
Enable	If an account is enabled, he/she can establish remote session, if the account is disabled, he/she can still access the web portal, but remote session is disabled.

Add AD account

Once an AD server has been successfully authenticated, it would appear to AD server list in System- Active Directory tab. Now navigate to **Management** tab – **Users**, click on **Add AD User** button on the top.



Add AD User/Group

General Settings	Type	Type: AD User
	AD Server	Select an AD Server: TestAD Server (dc=dvm, dc=corp)
	Account	User account to login *: test@dvm.corp
		☑ Enable User
Unattended support	Group	Group Choice: Default Group
	Role	Role Choice: Member
Attended support	SOS Technician	☑ Enable SOS/On-Demmand support

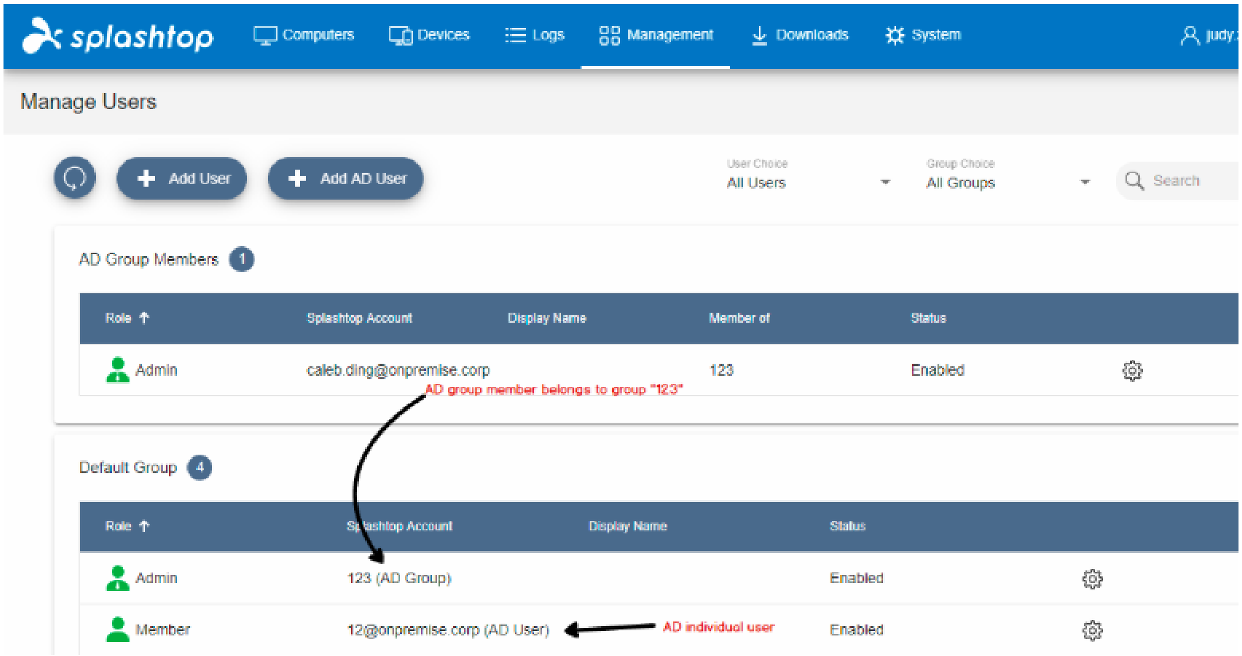
Field	*Meaning*
Type	By selecting AD user, an AD individual user will be authenticated and added to Splashtop Gateway. Selecting AD group allows **bulk authentication** of its AD group members. (Group members will have to login to Gateway Web portal first then displayed in the user list)
AD Server	Select the AD server which contains the target AD user or group.
Account	Fill up the **sAMaccountName@ADDomainName (local AD domain name)** of target AD user or group.
Group	Chose the initial Splashtop group an AD user or AD group will fall into once added.
Role	User can be grouped into different groups, group is a great way to manage users / access permissions.
SOS Technician	Enable SOS on demand support capability. (Based on subscription plan)
Verify	Check the availability of an AD user or group for authentication.
OK	Add a validated AD user or group to the target group.

Add Group Members

Green user icon represents AD users or AD groups as shown in the below screenshot below. If an AD group has been added to Splashtop Gateway, meaning its associated AD members have already been authenticated and able to log into Splashtop Gateway as well as On-Prem client application.

The AD users in AD Group Members will be showed up in **AD Group Members** after log into Gateway portal or client application with his/her AD account at **least once**. By contrast, an **AD individual user** added to Gateway will be displayed and modified property immediately.

Note: An AD account authenticated via its parent AD Group would inherit the user role and access permission of that group.



Manage Users

AD Group Members 1

Role ↑	Splashtop Account	Display Name	Member of	Status
Admin	caleb.ding@onpremise.corp		123	Enabled

AD group member belongs to group "123"

Default Group 4

Role ↑	Splashtop Account	Display Name	Status
Admin	123 (AD Group)		Enabled
Member	12@onpremise.corp (AD User)		Enabled

AD individual user

All successfully authenticated AD users can login On-Prem client application with their AD credentials and start to use Splashtop remote service.

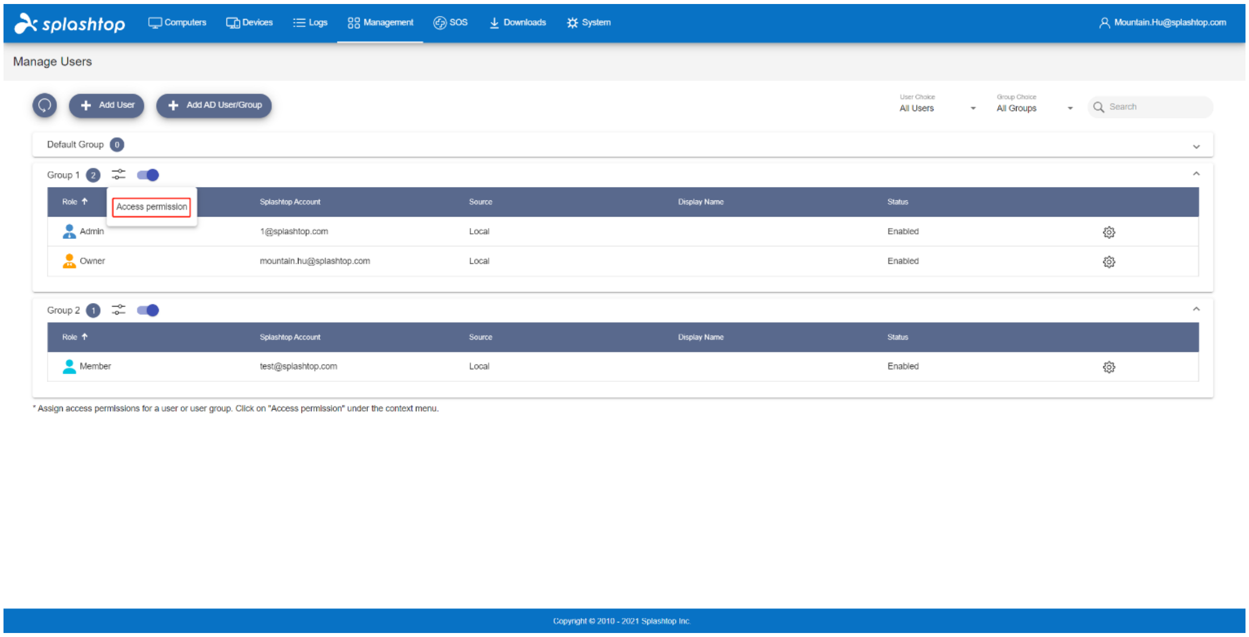
Set access permission

Access permissions determine which computers a user will have access to.

All access permission settings are configured through the https://{gateway} web console by the team's Owner or Admins.

Group Access Permissions

If you want several users to follow the same access permissions, you can create a group, add all the users to that group, and set the access permissions for that group.



Manage Users

User Choice: All Users
Group Choice: All Groups

Default Group 0

Group 1 2

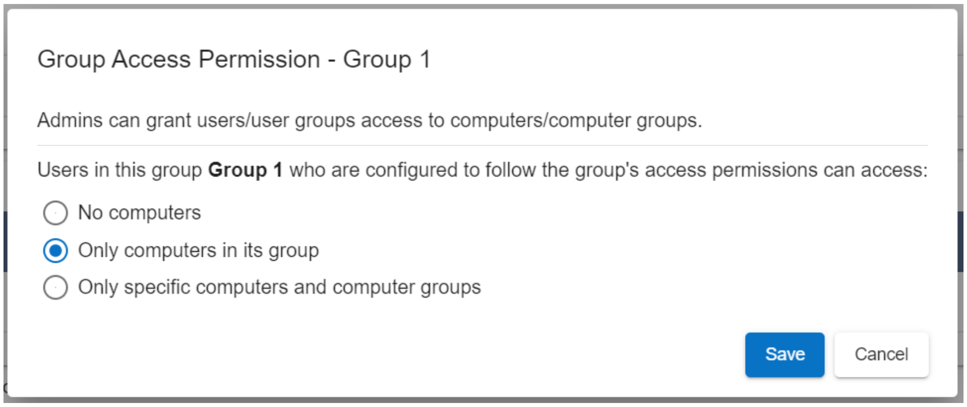
Role ↑	Splashtop Account	Source	Display Name	Status
Admin	1@splashtop.com	Local		Enabled
Owner	mountain.hu@splashtop.com	Local		Enabled

Group 2 1

Role ↑	Splashtop Account	Source	Display Name	Status
Member	test@splashtop.com	Local		Enabled

* Assign access permissions for a user or user group. Click on "Access permission" under the context menu.

By default, the users will have access to only the computers in the same group. You can set "Only specific..." to choose multiple groups of computers or specific computers only.



Group Access Permission - Group 1

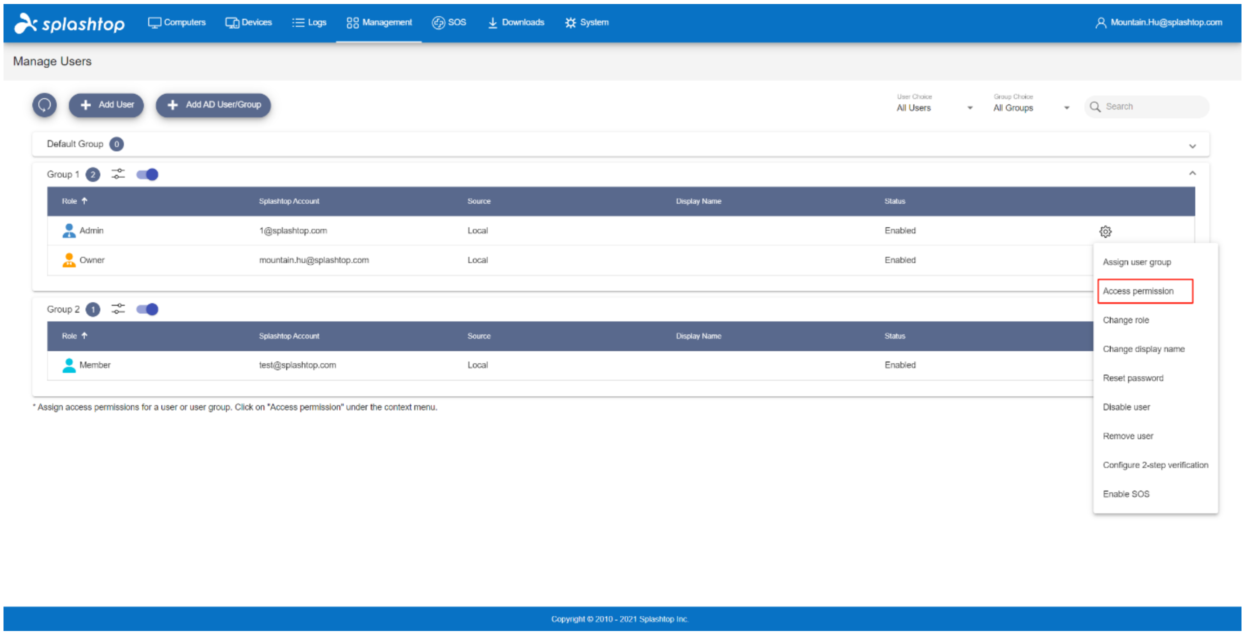
Admins can grant users/user groups access to computers/computer groups.

Users in this group **Group 1** who are configured to follow the group's access permissions can access:

○ No computers
● Only computers in its group
○ Only specific computers and computer groups

User Access Permissions

Additionally, you can choose a specific user account and set the access permissions for the specific account. This will override any group permissions settings even if you change the group permission settings, unless you change the settings back to follow the group access settings. This is useful if you want to give each end-user only access to their own computer(s).



Manage Users

User Choice: All Users
Group Choice: All Groups

Default Group 0

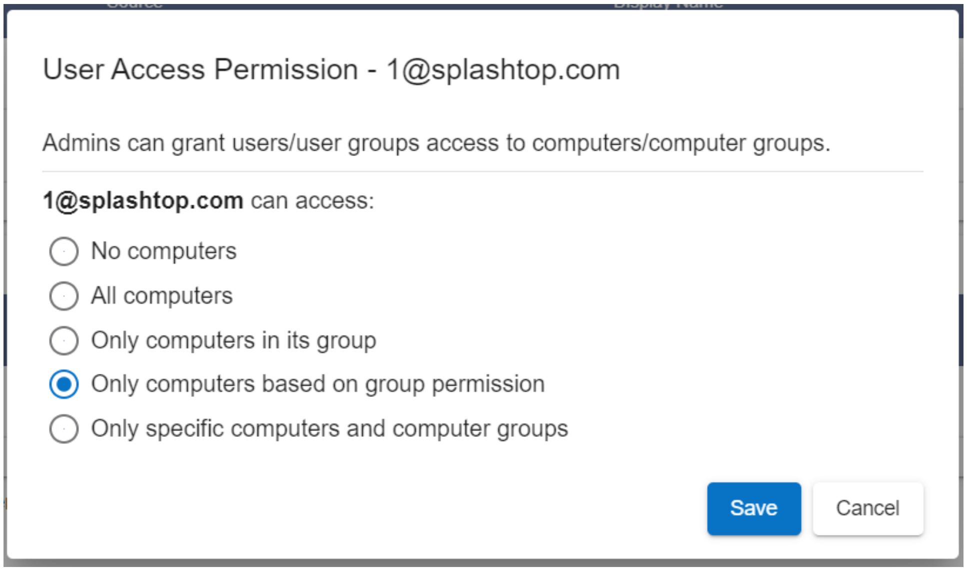
Group 1 2

Role ↑	Splashtop Account	Source	Display Name	Status
Admin	1@splashtop.com	Local		Enabled
Owner	mountain.hu@splashtop.com	Local		Enabled

Group 2 1

Role ↑	Splashtop Account	Source	Display Name	Status
Member	test@splashtop.com	Local		Enabled

* Assign access permissions for a user or user group. Click on "Access permission" under the context menu.



User Access Permission - 1@splashtop.com

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

1@splashtop.com can access:

○ No computers
○ All computers
○ Only computers in its group
● Only computers based on group permission
○ Only specific computers and computer groups

Set admin rights

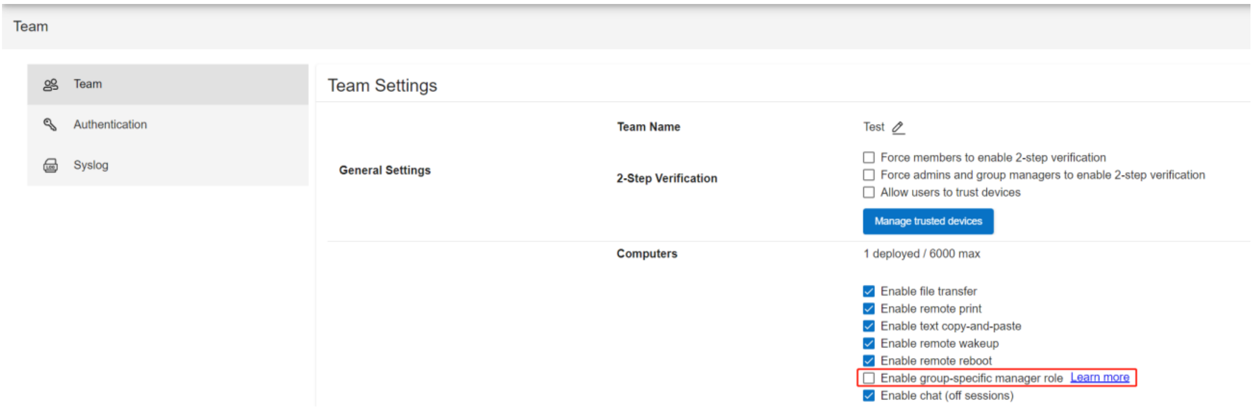
On Splashtop On-Prem, an Admin user can remotely access and **manage all computers by default**.

Sometimes you may want a client to have admin role, but limit their access to only a subset of computers. This allows the client to do things like add computer, remove computer, create user, etc., but **only for the groups that you authorized**.

Please see instructions below to enable and to use the feature.

Enable group-specific manager feature

Log into Splashtop Gateway as Team Owner. Navigate to **Management** > **Settings**. Check the box "Enable group-specific manager role."



Team

- Team
- Authentication
- Syslog

Team Settings

General Settings

Team Name: Test

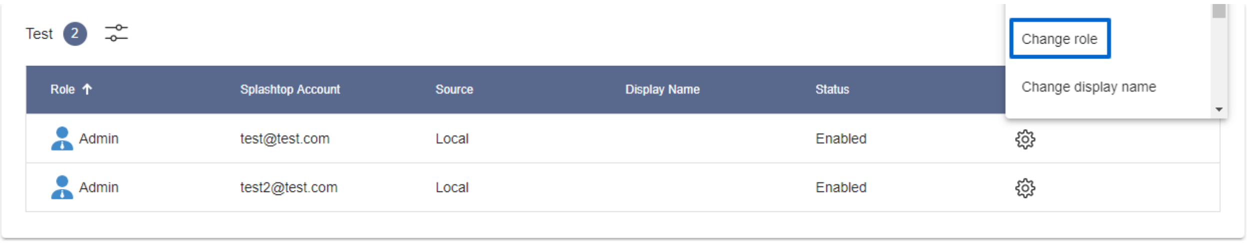
2-Step Verification:
□ Force members to enable 2-step verification
□ Force admins and group managers to enable 2-step verification
□ Allow users to trust devices

Computers: 1 deployed / 6000 max

☑ Enable file transfer
☑ Enable remote print
☑ Enable text copy-and-paste
☑ Enable remote wakeup
☑ Enable remote reboot
□ Enable group-specific manager role Learn more
☑ Enable chat (off sessions)

Set a user as a group-specific manager

Navigate to **Management** > **Users**. Click on the gear icon next to the user whom you want to set as a group-specific manager. Click on "Change role."



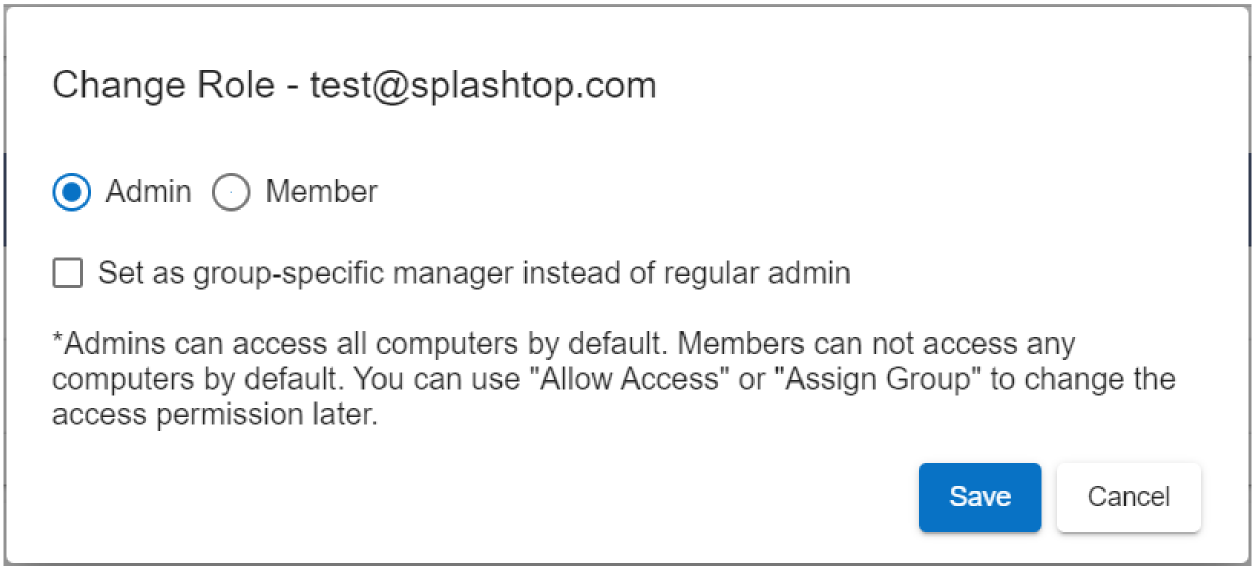
Test 2

Role ↑	Splashtop Account	Source	Display Name	Status	
Admin	test@test.com	Local		Enabled	⚙
Admin	test2@test.com	Local		Enabled	⚙

In the resulting dialog box:

1. Select the "Admin" radio button
2. Check the "Set as group-specific manager" checkbox

3. Select the check-boxes for whichever group(s) you want this user to manage



Change Role - test@splashtop.com

● Admin ○ Member

□ Set as group-specific manager instead of regular admin

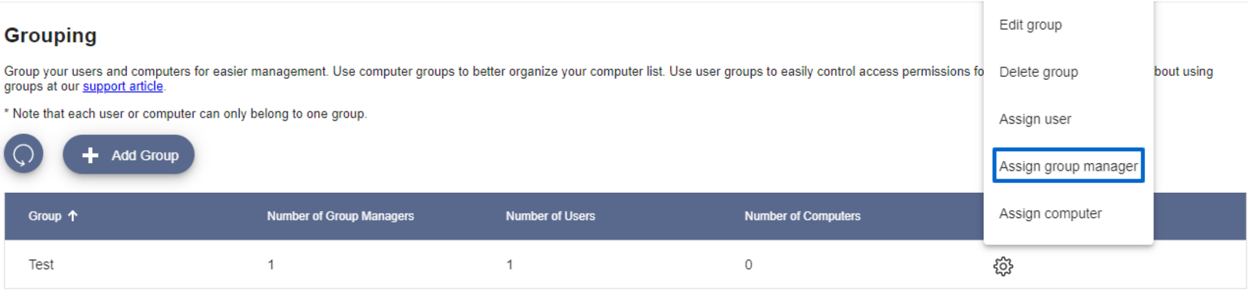
*Admins can access all computers by default. Members can not access any computers by default. You can use "Allow Access" or "Assign Group" to change the access permission later.

Another way to assign group-specific managers

Group-specific managers can also be assigned from the **Grouping** page.

Navigate to **Management** > **Grouping**. Click on the gear icon next to the group that you want to set a group manager for. Click on "Assign group manager."

In the resulting dialog box, you can choose which user(s) can manage this group.



Grouping

Group your users and computers for easier management. Use computer groups to better organize your computer list. Use user groups to easily control access permissions fo bout using groups at our support article.

* Note that each user or computer can only belong to one group.

Group ↑	Number of Group Managers	Number of Users	Number of Computers
Test	1	1	0

What a group-specific manager can do

The group-specific manager can perform these functions **only on the users and computers in the groups managed by him or her**. The group-specific manager will **not** be able to see the group names, users, and computers in other groups.

- Rename computer
- Add/edit computer notes
- Add/delete computers, including create deployment packages
- Create/enable/disable/delete users
- Set access permissions
- Configure user's 2FA (aka. MFA) and trusted devices

Notes

- When an admin is assigned to be a group-specific manager, the management scope is reduced from the whole team to only specific group(s).
- You can always see which users have been assigned group-specific manager rights by navigating **Management** > **Users**. The role for such users is labeled as "Manager (groups)." Mouse over the label to see the list of groups managed by the user.
- The role of group-specific manager will be changed to **Member** when the relevant group is deleted from Gateway web portal.

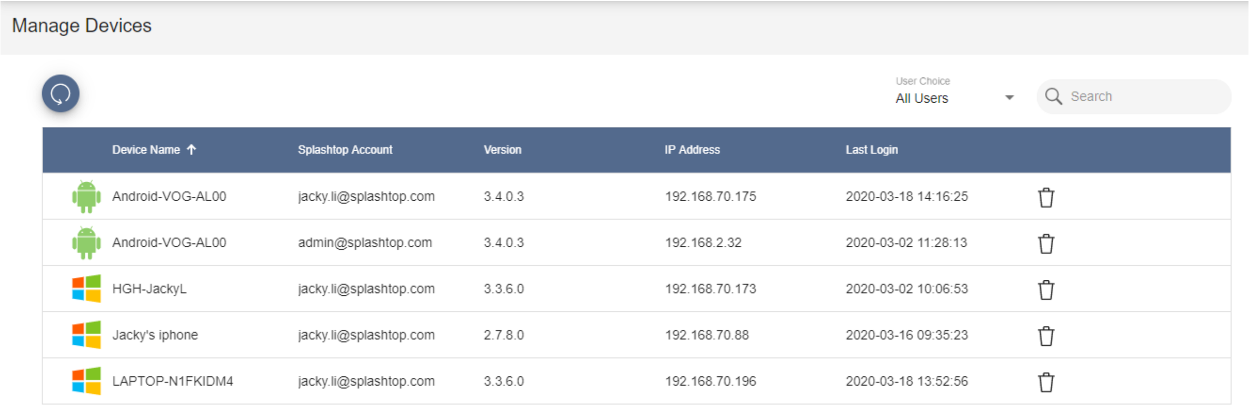
Computers

This page helps user/admin overview and manages the computers registered in Splashtop On-Prem system. A computer can be renamed, assigned to a group, assigned permissions for users and etc.

Devices

Administrator can manage the devices from **All Devices** in the **Management** console. A device refers to a client endpoint which the user uses to access the remote computer. It can be a computer, a smart phone device or a tablet.

Clicking on **All devices** from **Management** tab, you can see the list of enrolled devices.



Device Name ↑	Splashtop Account	Version	IP Address	Last Login	
Android-VOG-AL00	jacky.li@splashtop.com	3.4.0.3	192.168.70.175	2020-03-18 14:16:25	🗑
Android-VOG-AL00	admin@splashtop.com	3.4.0.3	192.168.2.32	2020-03-02 11:28:13	🗑
HGH-JackyL	jacky.li@splashtop.com	3.3.6.0	192.168.70.173	2020-03-02 10:06:53	🗑
Jacky's iphone	jacky.li@splashtop.com	2.7.8.0	192.168.70.88	2020-03-16 09:35:23	🗑
LAPTOP-N1FKIDM4	jacky.li@splashtop.com	3.3.6.0	192.168.70.196	2020-03-18 13:52:56	🗑

This table includes information such as the device name, IP address, version of client app, logged Splashtop account and time of last login.

You can choose to delete a device by clicking on the Bin icon at the end of each row.

Grouping

Now Splashtop On-Prem allows the administrator to create groups that contain specific computer(s) and user(s). It is easy to manage access permission based on groups.

Group your users and computers for easier management. Assign access permissions by user or by user group.

Get started by login to your Gateway Web Portal – Management, and clicking on **Grouping**.

Notes:

- Each user or computer can only belong to one group.
- Supported since Gateway v1.1.9

General

Group the computers for easier management. Your computers will then be organized by groups on your Splashtop On-Prem 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 login to your **Gateway Web Portal** >**Management** > **Grouping**.

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 create a user, you can optionally choose a user group. When done, 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 add users and computers to the group.

Set access permissions

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

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."

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

Scheduled access

Introduction

Scheduled Access is a new feature that will allow admins to schedule users, groups and computers for remote access on a time-slot basis.

See this article for a few example scheduling scenarios.

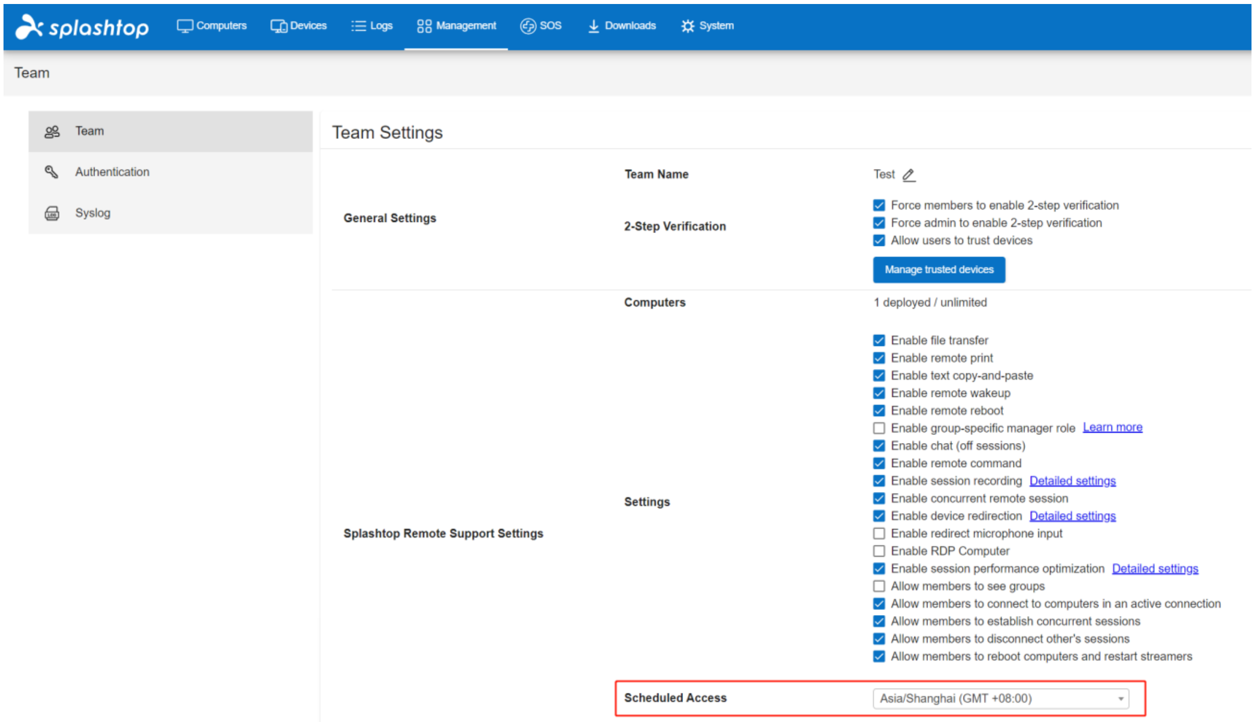
Notes and Best Practices

- Scheduled Access are granted in addition to existing user/group permissions that are set under *Management -> Users* - they do *NOT* override existing user/group permissions.
- If there are already existing permissions configured under *Management -> Users*, it is recommended to de-associate these existing permissions and “migrate” to use the Scheduled Access feature for users who only need scheduled remote access.
- The Team Owner and Admins can use the Scheduled Access feature.
- For open lab hours, create a separate schedule and configure a timeslot for it. For example, 0:00 – 9:00, include all groups of members. 17:00 – 23:59 another timeslot and include the group of members.
- To receive proper disconnect warning messages, requires Splashtop On-Prem app v3.4.4.0.
- The select computer page may not work well on IE11. If you see issues with IE11, please try another browser or upgrade IE.

Scheduled Access Configuration

1. Before creating any new schedules, go to *https://{gatewayaddress}* *-> Management ->*

Settings to configure the **Scheduled Access timezone**. Timezone cannot be changed when a schedule is in place. Only the team owner has access to this setting.



Team Settings

General Settings

Team Name Test

2-Step Verification
☑ Force members to enable 2-step verification
☑ Force admin to enable 2-step verification
☑ Allow users to trust devices

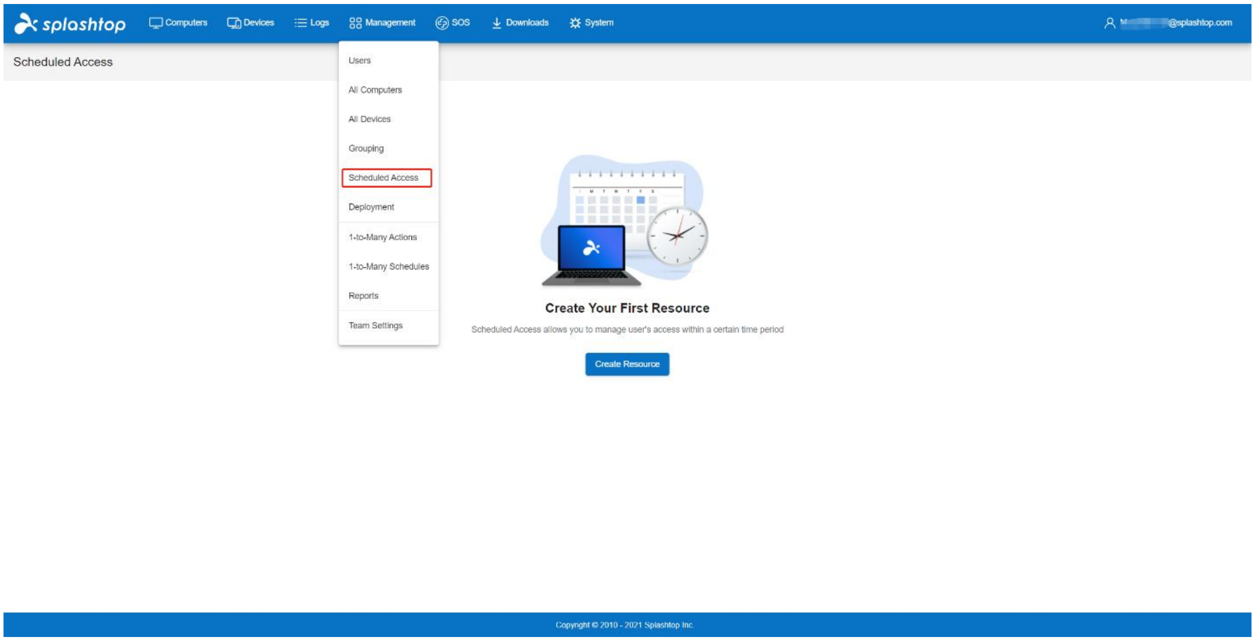
Splashtop Remote Support Settings

Computers 1 deployed / unlimited

Settings
☑ Enable file transfer
☑ Enable remote print
☑ Enable text copy-and-paste
☑ Enable remote wakeup
☑ Enable remote reboot
□ Enable group-specific manager role Learn more
☑ Enable chat (off sessions)
☑ Enable remote command
☑ Enable session recording Detailed settings
☑ Enable concurrent remote session
☑ Enable device redirection Detailed settings
□ Enable redirect microphone input
□ Enable RDP Computer
☑ Enable session performance optimization Detailed settings
□ Allow members to see groups
☑ Allow members to connect to computers in an active connection
☑ Allow members to establish concurrent sessions
☑ Allow members to disconnect other's sessions
☑ Allow members to reboot computers and restart streamers

Scheduled Access Asia/Shanghai (GMT +08:00)

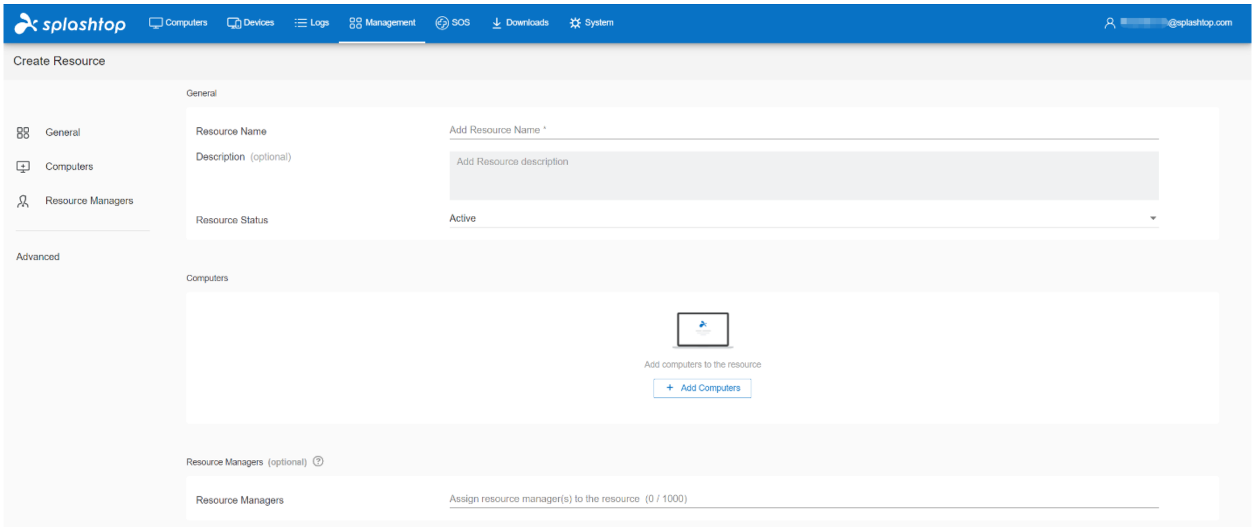
2. Go to *https://{gatewayaddress} -> Management -> Scheduled Access*



Create Your First Resource

Scheduled Access allows you to manage user's access within a certain time period

3. Click "Create Resource" and fill in the fields. The resource will contain what set of computers will be scheduled for access, such as a specific computer lab.



Create Resource

General

Resource Name: Add Resource Name *

Description (optional): Add Resource description

Resource Status: Active

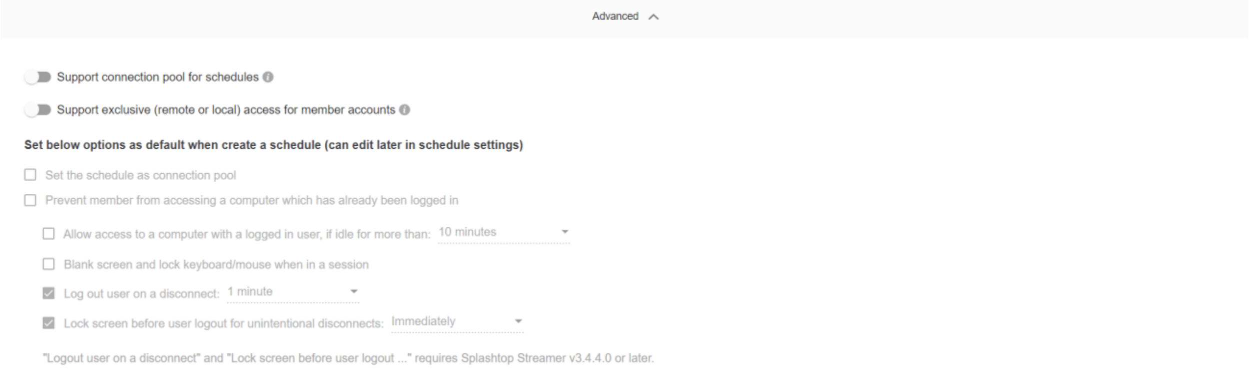
Computers

Add computers to the resource

Resource Managers (optional)

Resource Managers: Assign resource manager(s) to the resource (0 / 1000)

4. Click "Advanced Settings" to enable support for Exclusive Mode. 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. The logout and lock screen settings also help for cases where students forget to log out of their OS accounts.



Advanced

Support connection pool for schedules

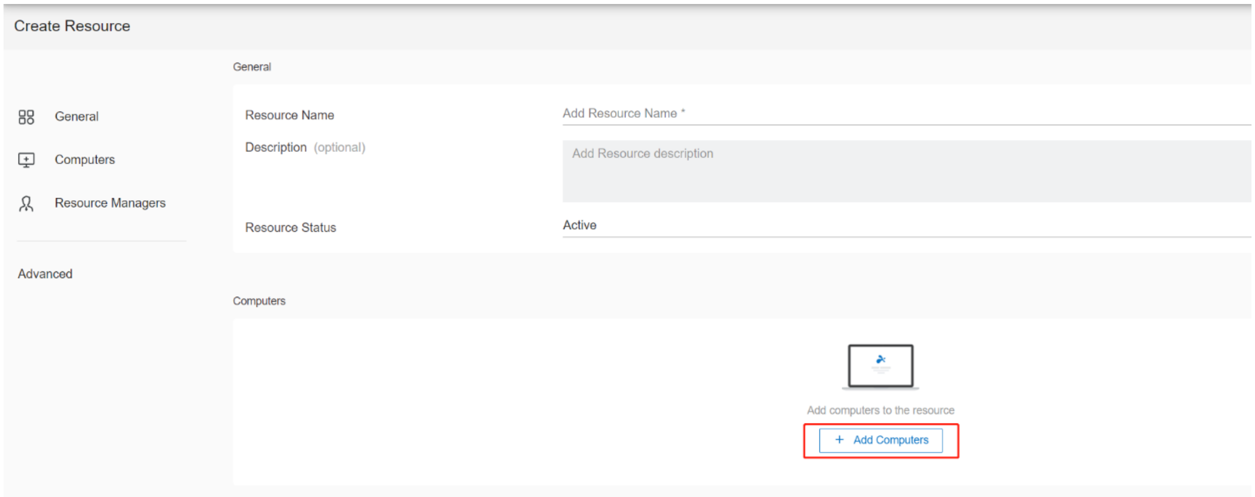
Support exclusive (remote or local) access for member accounts

Set below options as default when create a schedule (can edit later in schedule settings)

- ☐ 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: 1 minute
  - ☑ Lock screen before user logout for unintentional disconnects: Immediately

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

5. Select the computers or computer groups that you would like to make available in the resource.



Create Resource

General

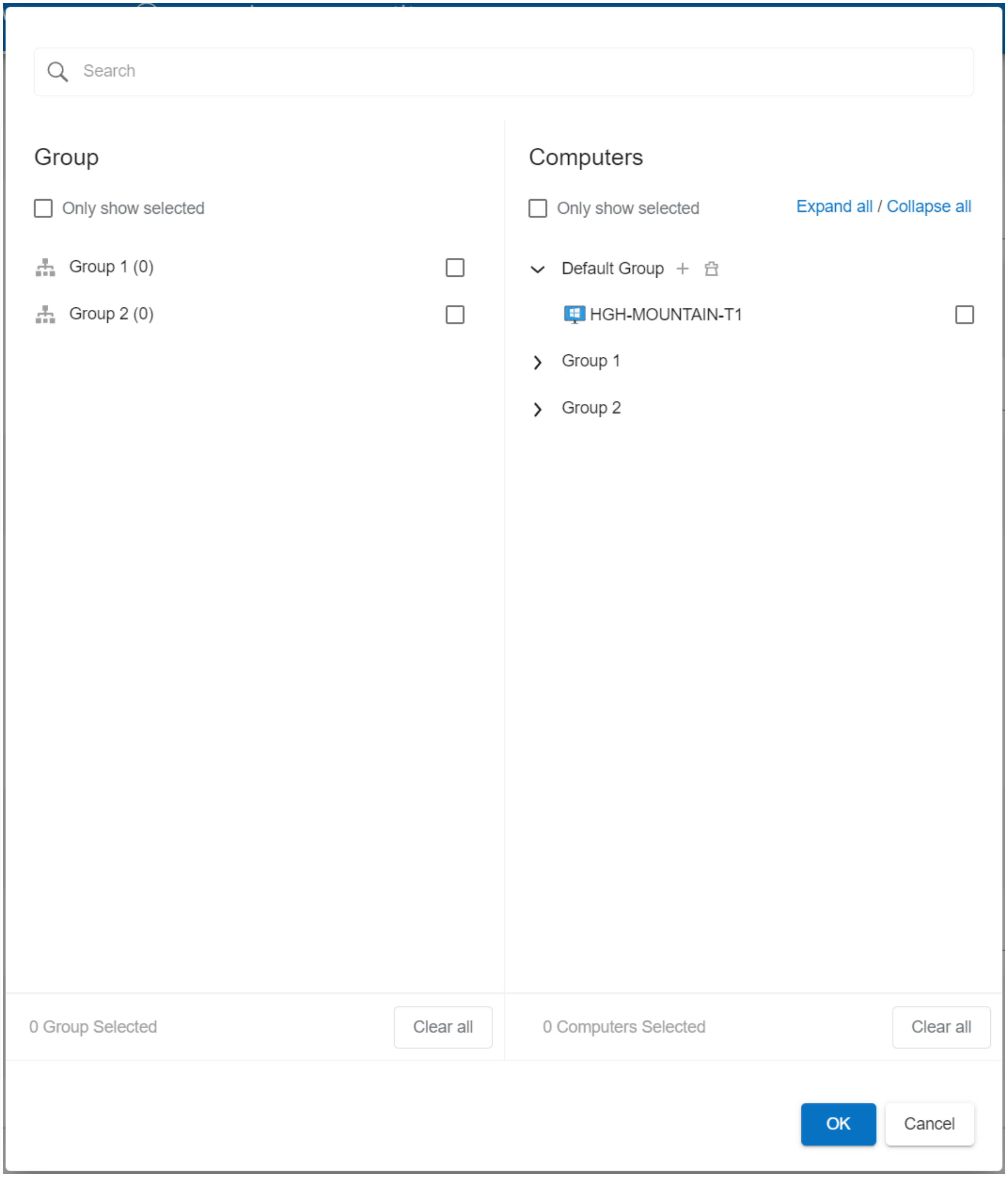
Resource Name: Add Resource Name *

Description (optional): Add Resource description

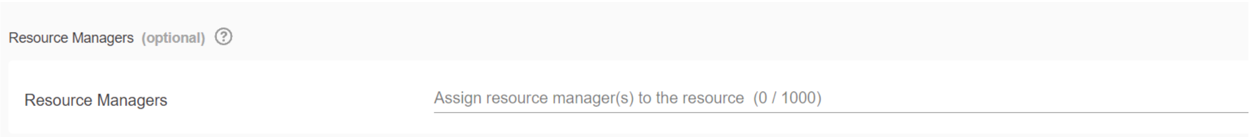
Resource Status: Active

Computers

Add computers to the resource



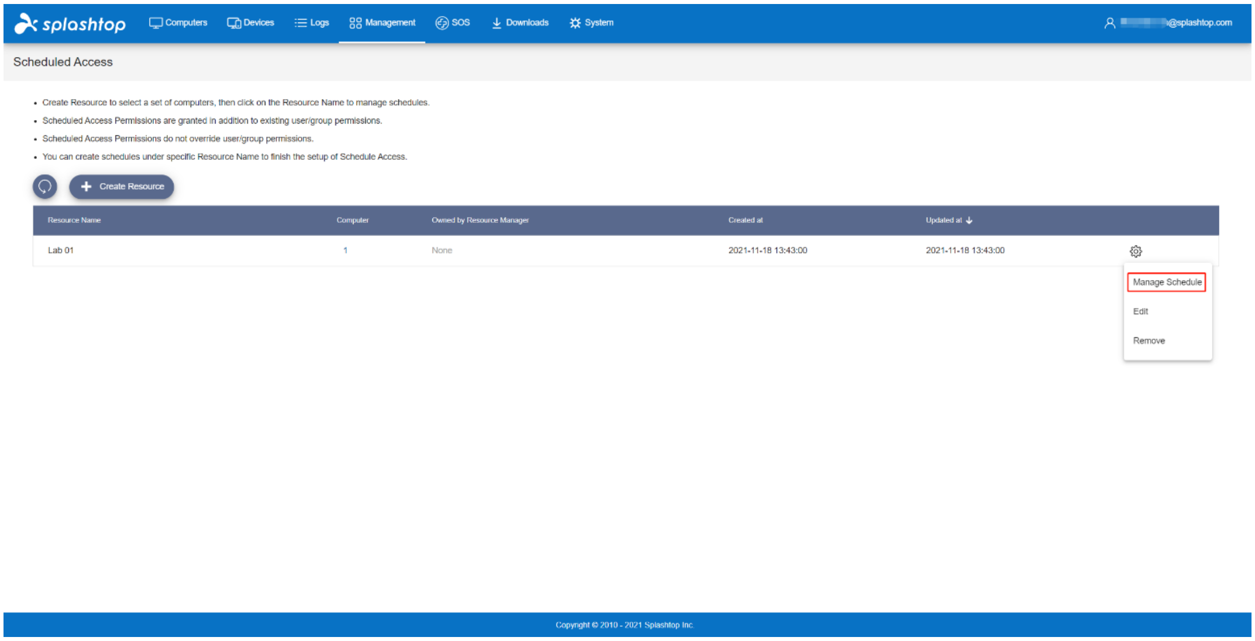
6. (Optional) Assign a Group Admin to help with managing schedules on the resource. Group admins also have the capability to create resources and schedules.



Resource Managers (optional) ?

Resource Managers — Assign resource manager(s) to the resource (0 / 1000)

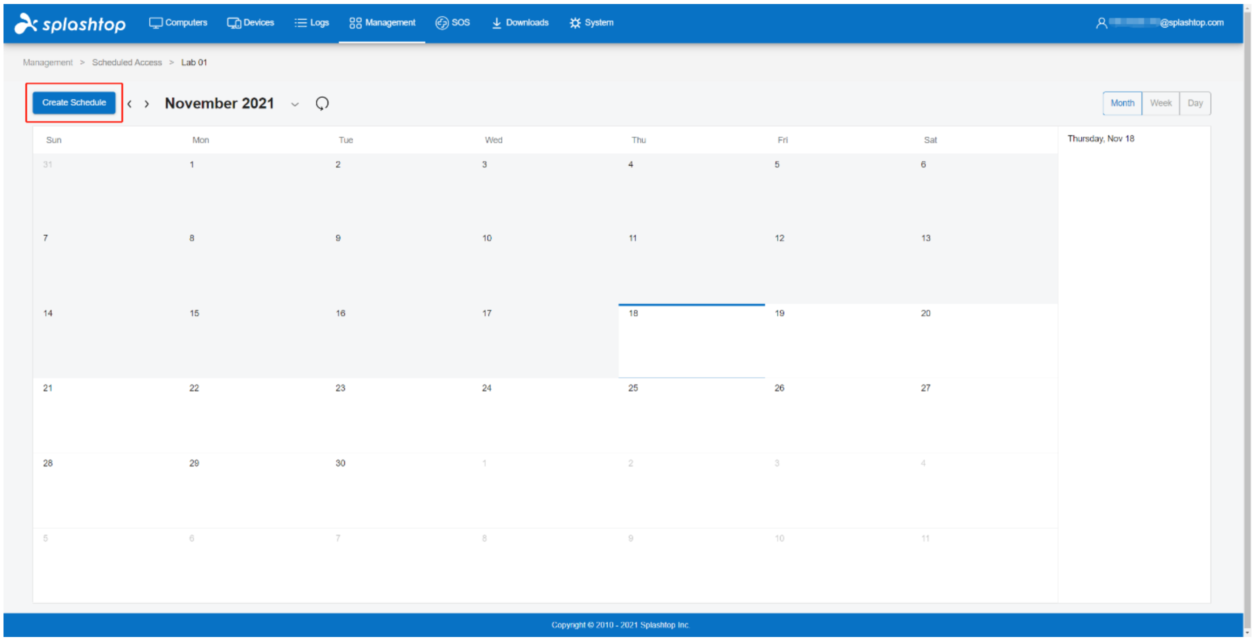
7. Click Manage Schedule from context drop-down menu (Gear Button) to assign Schedules to the resource.



Scheduled 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.
- You can create schedules under specific Resource Name to finish the setup of Schedule Access.

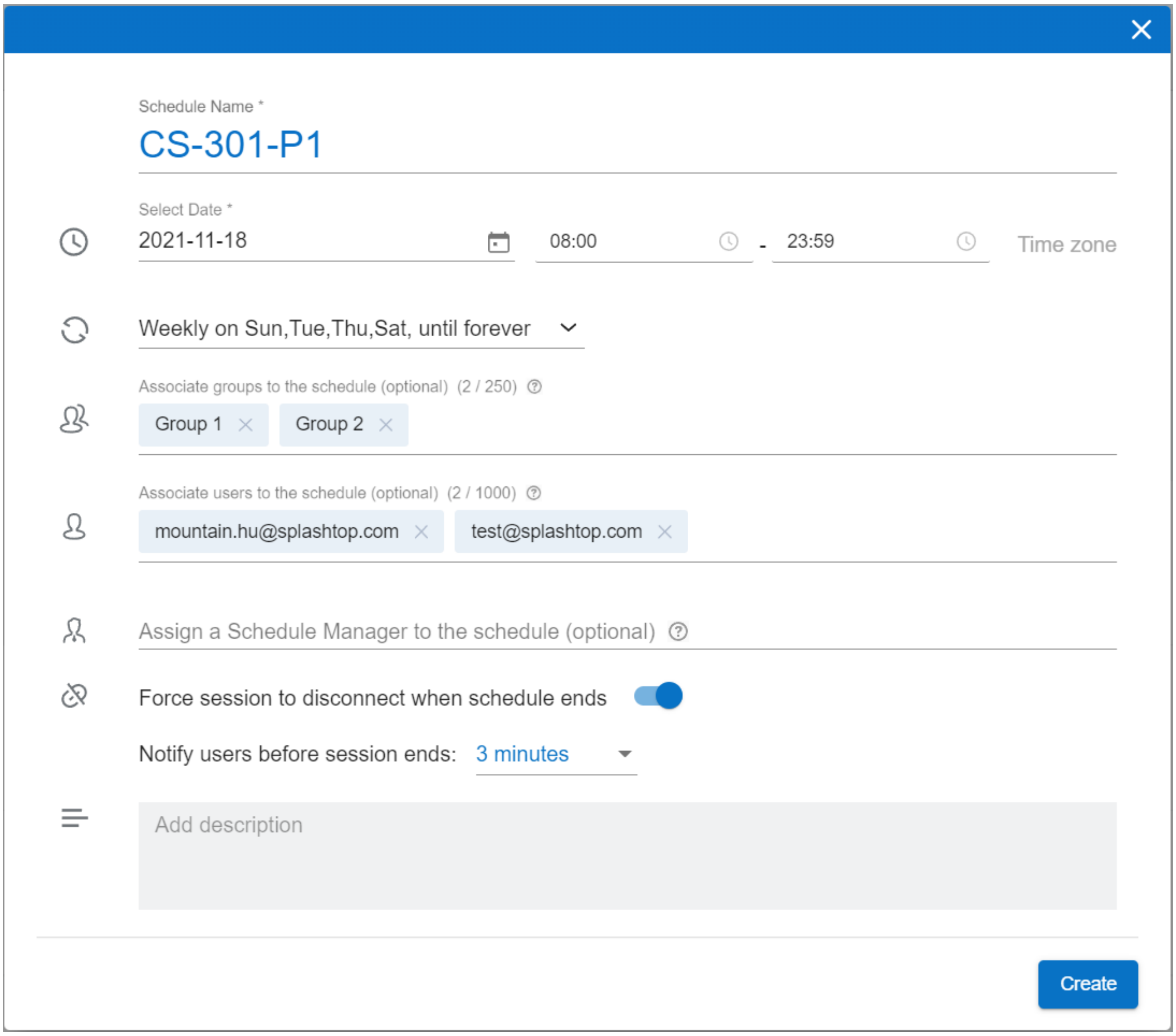
Resource Name	Computer	Owned by Resource Manager	Created at	Updated at ↓
Lab 01	1	None	2021-11-18 13:43:00	2021-11-18 13:43:00



Sun	Mon	Tue	Wed	Thu	Fri	Sat
31	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	1	2	3	4
5	6	7	8	9	10	11

8. 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. You may also paste a

list of user emails. Note: The time drop-down selection is a 30-minute interval, but you can manually type in a value granular to a minute.



Schedule Name *
CS-301-P1

Select Date *
2021-11-18
08:00 - 23:59

Weekly on Sun,Tue,Thu,Sat, until forever

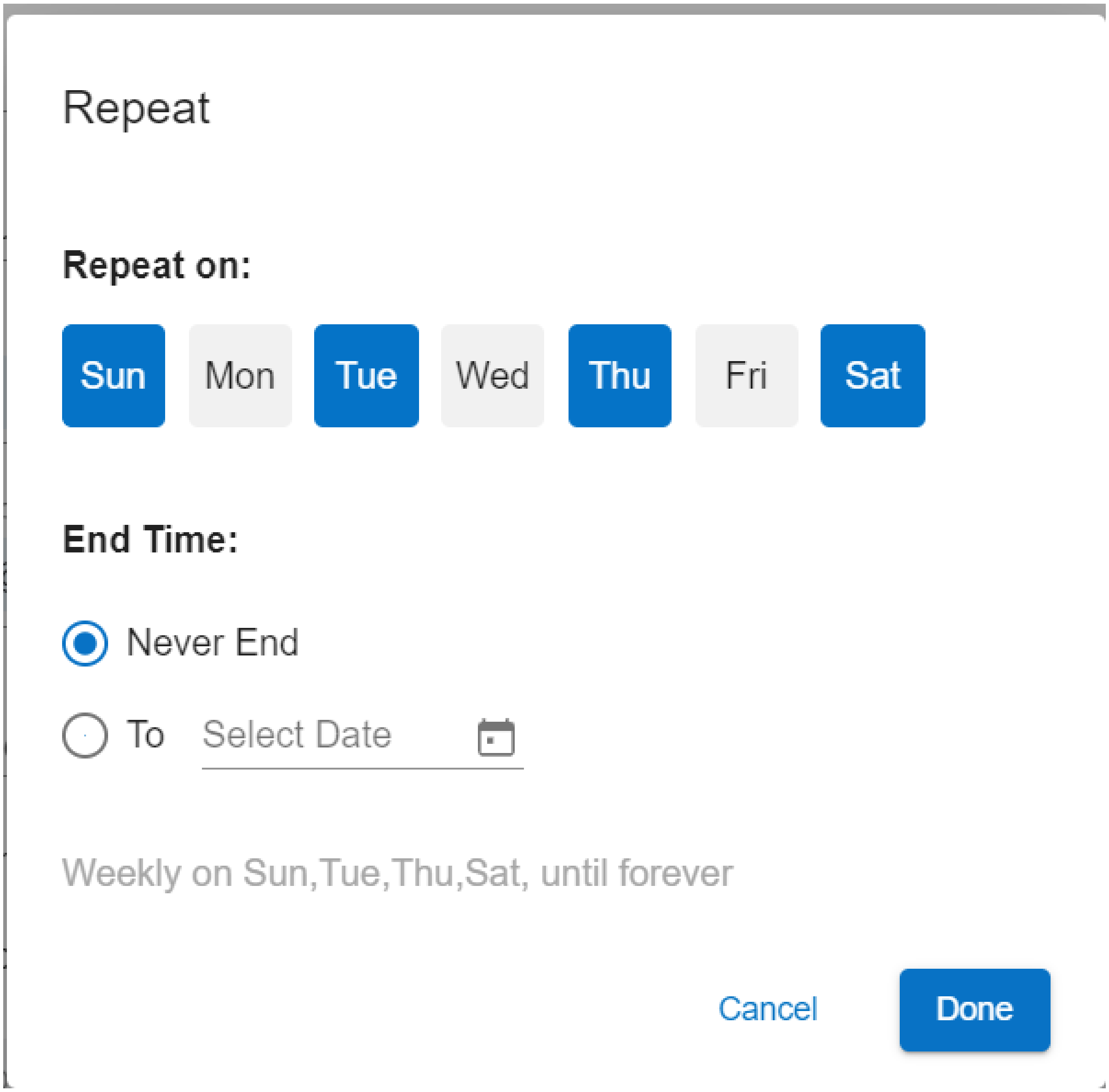
Associate groups to the schedule (optional) (2 / 250)
Group 1
Group 2

Associate users to the schedule (optional) (2 / 1000)
mountain.hu@splashtop.com
test@splashtop.com

Assign a Schedule Manager to the schedule (optional)

Force session to disconnect when schedule ends

Notify users before session ends: 3 minutes



Repeat

Repeat on:

End Time:

● Never End

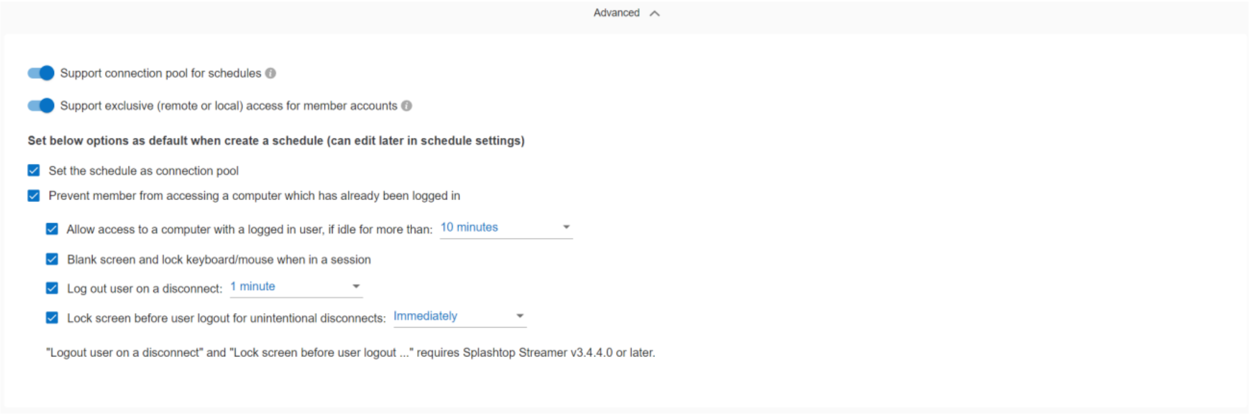
○ To Select Date

Weekly on Sun,Tue,Thu,Sat, until forever

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 log out of the remote computer's user account.

Exclusive mode:

Click "Advanced Settings" to turn on/off exclusive access



Advanced

● Support connection pool for schedules

● Support exclusive (remote or local) access for member accounts

Set below options as default when create a schedule (can edit later in schedule settings)

☑ Set the schedule as connection pool

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

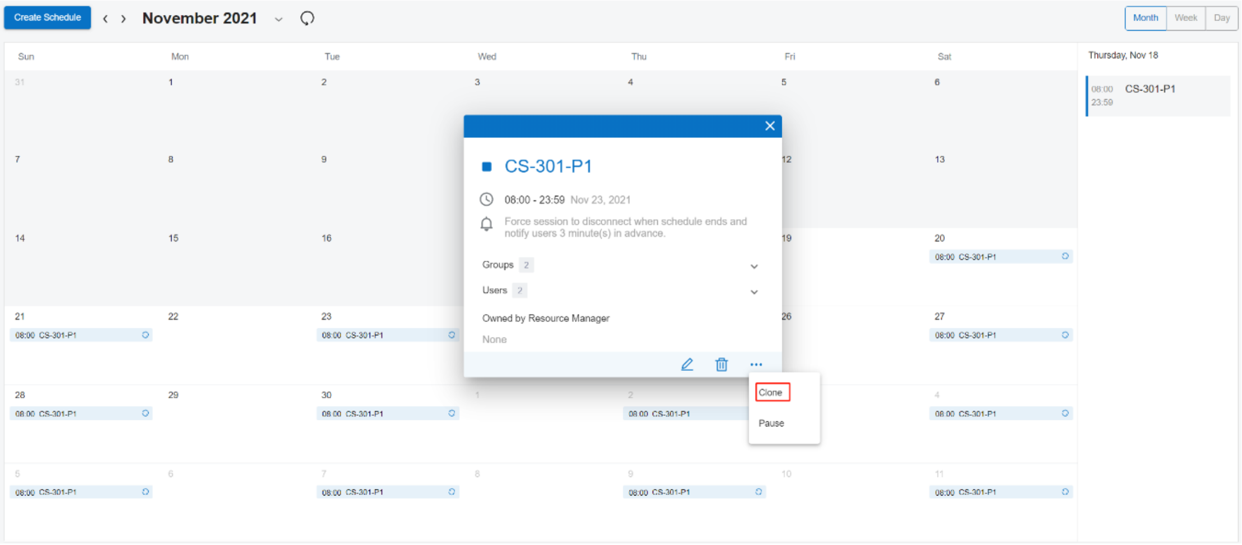
- ☑ Allow access to a computer with a logged in user, if idle for more than: 10 minutes
- ☑ Blank screen and lock keyboard/mouse when in a session
- ☑ Log out user on a disconnect: 1 minute
- ☑ Lock screen before user logout for unintentional disconnects: Immediately

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

Allows computers that are part of this schedule to be accessed only if the computer is currently at the Windows/Mac Login screen, making the computer exclusive for the user that is currently logged in to the Operating system using the computer. Applies for users either present at the lab or remotely connected through a Splashtop session.

Auto-logout after disconnection might be helpful for exclusive access. Make sure streamers are updated to v3.4.4.0 to use the checkbox option above.

9. To pause / resume a Schedule, click on the Schedule and then pause / resume button.



CS-301-P1

08:00 - 23:59 Nov 23, 2021

Force session to disconnect when schedule ends and notify users 3 minute(s) in advance.

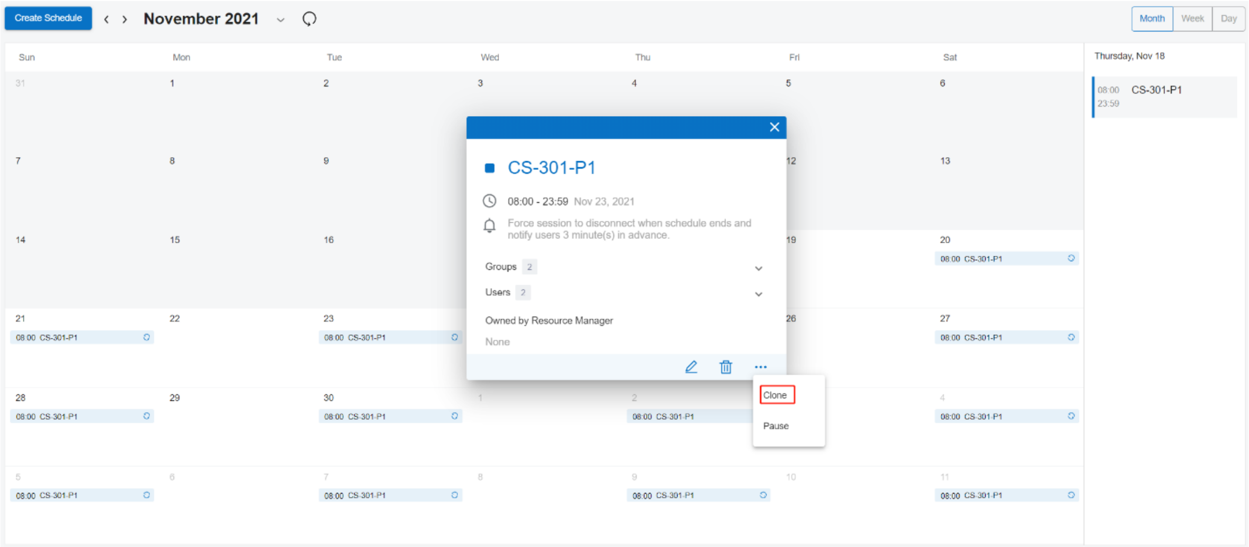
Groups 2

Users 2

Owned by Resource Manager

None

10. To clone a Schedule, use the Clone button.



CS-301-P1

08:00 - 23:59 Nov 23, 2021

Force session to disconnect when schedule ends and notify users 3 minute(s) in advance.

Groups 2

Users 2

Owned by Resource Manager

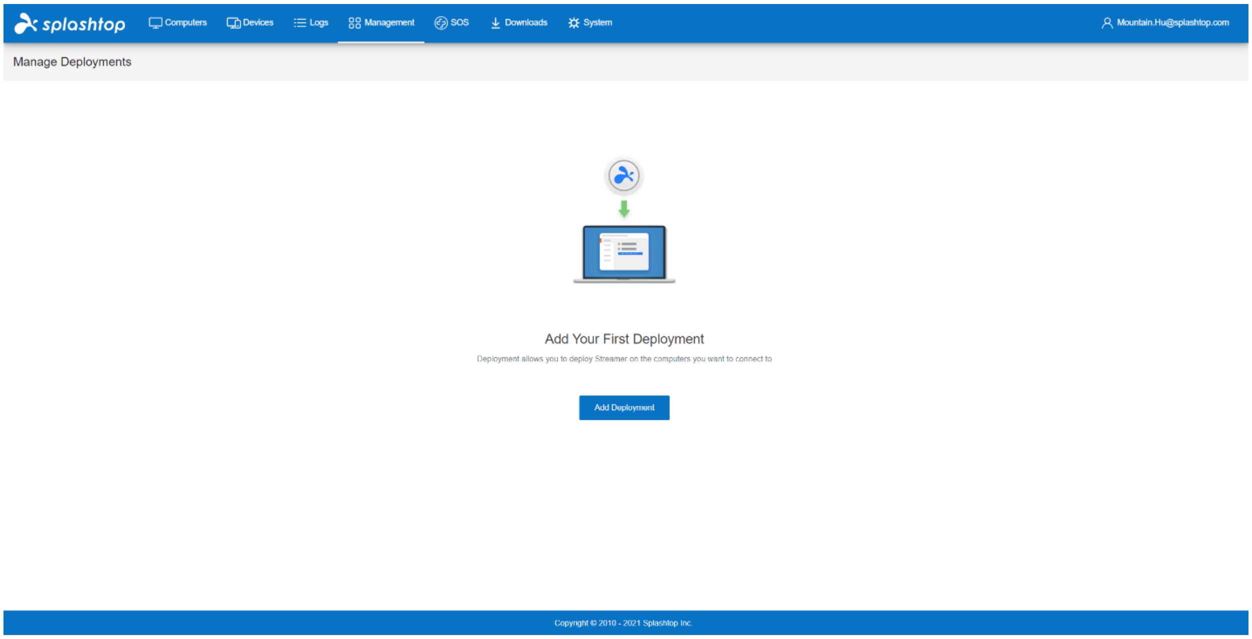
None

Deployment

Deployment package provides quick and easy way to install and configure Streamers in computers. Administrator can create different custom deployment packages based on company security policies.

On the computers that you'd like to connect to, the Splashtop Streamer must be installed. This can be done in 4 easy steps.

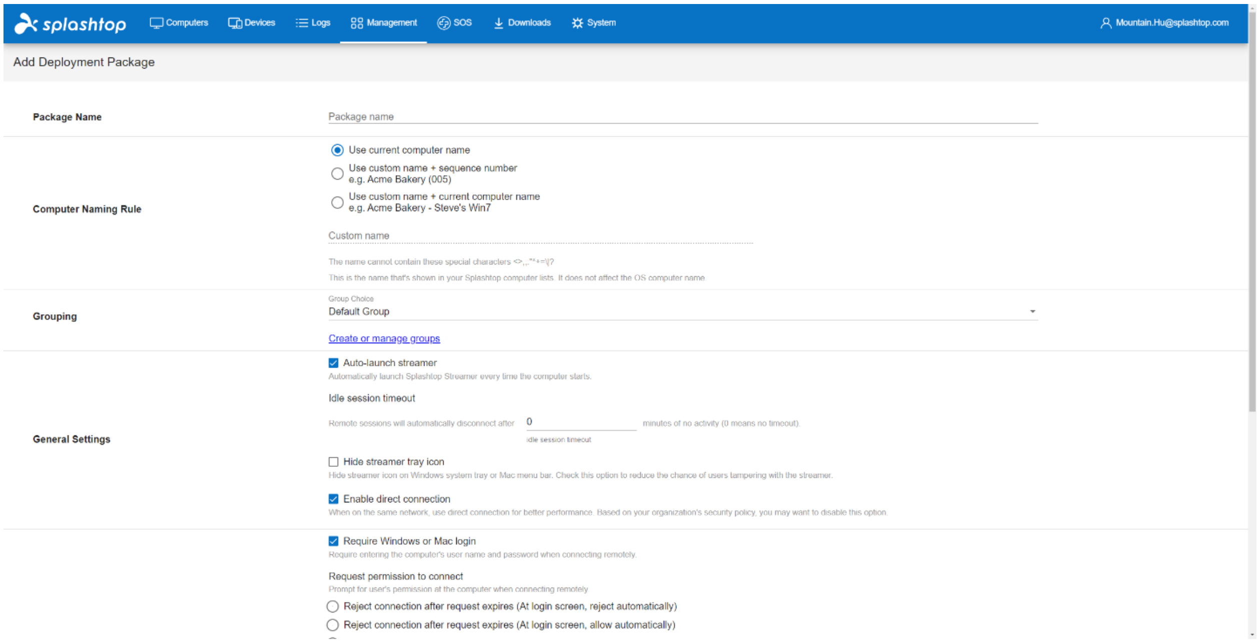
1. Create a deployment package on https://{gateway} > *Management* > *Deployment*. A deployment package consists of a deployment streamer and a unique 12-digit code.



Manage Deployments

Add Your First Deployment

Deployment allows you to deploy Streamer on the computers you want to connect to



Add Deployment Package

Package Name

Package name

Computer Naming Rule

● Use current computer name

○ Use custom name + sequence number
e.g. Acme Bakery (005)

○ Use custom name + current computer name
e.g. Acme Bakery - Steve's Win7

Custom name

The name cannot contain these special characters <>,;"*+=\|?

This is the name that's shown in your Splashtop computer lists. It does not affect the OS computer name

Grouping

Group Choice
Default Group

Create or manage groups

General Settings

☑ Auto-launch streamer
Automatically launch Splashtop Streamer every time the computer starts.

Idle session timeout

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

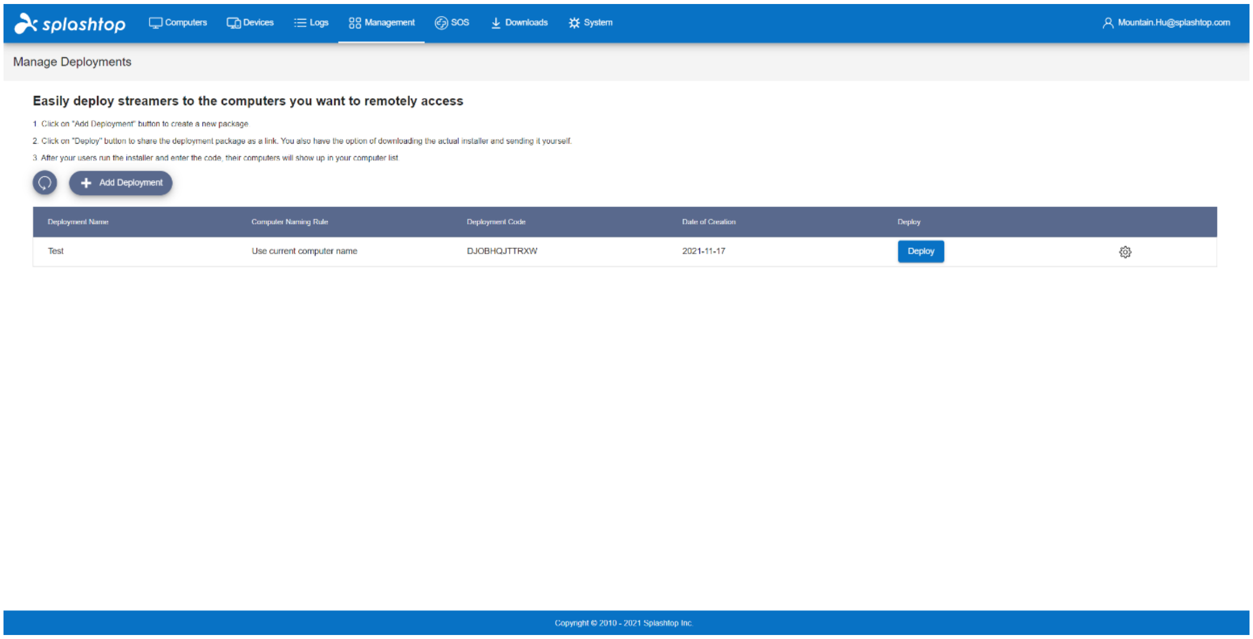
☑ Require Windows or Mac login
Require entering the computer's user name and password when connecting remotely.

Request permission to connect
Prompt for user's permission at the computer when connecting remotely

○ Reject connection after request expires (At login screen, reject automatically)

○ Reject connection after request expires (At login screen, allow automatically)

2. Select Deploy for the package that was just created.



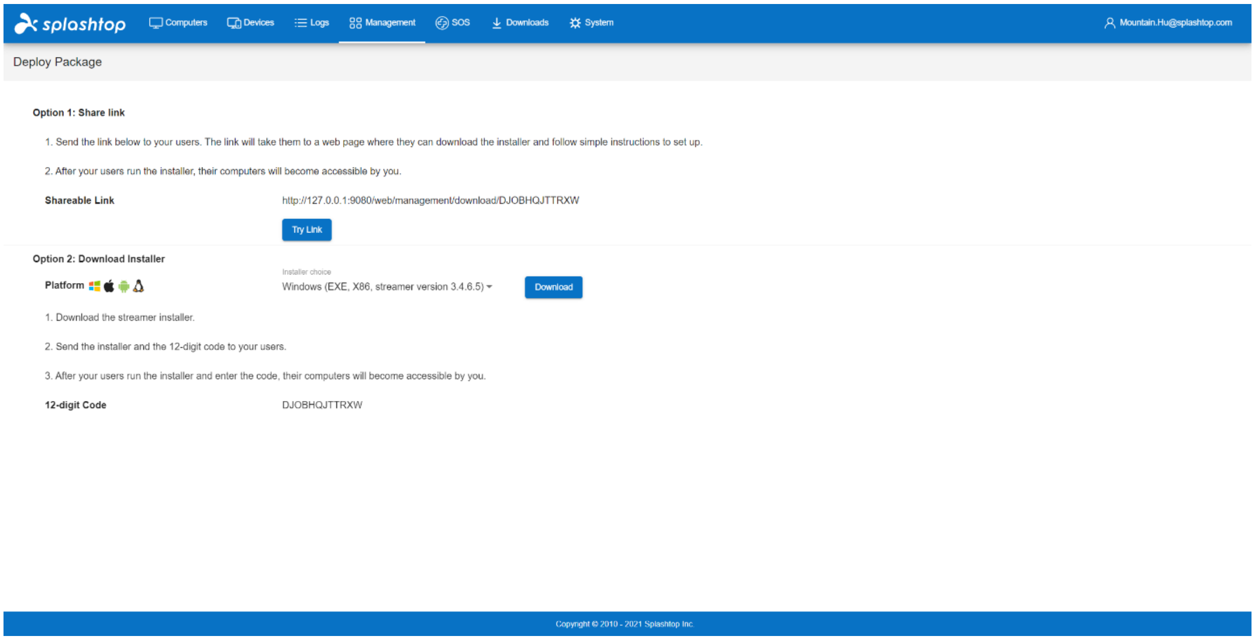
Manage Deployments

Easily deploy streamers to the computers you want to remotely access

1. Click on "Add Deployment" 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 Name	Computer Naming Rule	Deployment Code	Date of Creation	Deploy	
Test	Use current computer name	DJOBHQJTTRXW	2021-11-17	Deploy	⚙

3. **Have your users install the streamer.** You can send the deployment package link to your users. By following the link, your users can download the streamer installer and run the file. You can also send the streamer installer file directly to your users (via Dropbox, email, etc.).



Deploy Package

Option 1: Share 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. After your users run the installer, their computers will become accessible by you.

Shareable Link http://127.0.0.1:9080/web/management/download/DJOBHQJTTRXW

Option 2: Download Installer

Platform Installer choice: Windows (EXE, X86, streamer version 3.4.6.5)

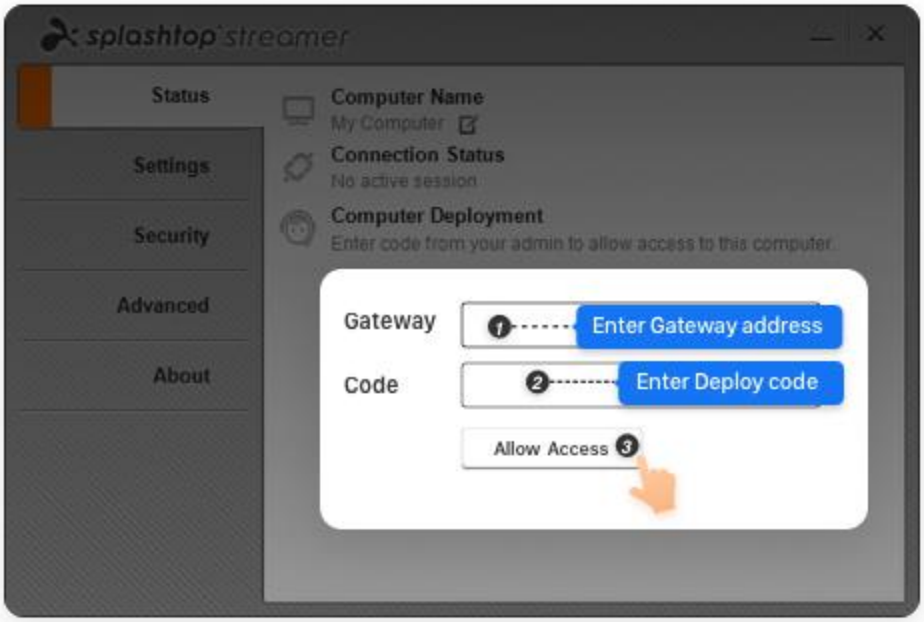
1. Download the streamer installer.
2. Send the installer and the 12-digit code to your users.
3. After your users run the installer and enter the code, their computers will become accessible by you.

12-digit Code DJOBHQJTTRXW

Or install the streamer yourself. Streamer installation on Windows or Mac computers can be done silently via command line executable or MSI. This is the easiest way to automatically deploy to a large number of computers if you have an RMM tool, Microsoft SCCM, or Microsoft Group Policy.

4. **Activate the Streamer with the deploy code.** Once the Streamer is installed, input the *{Gateway IP/FDQN:Port}* in the Gateway field and *Deploy code* in the Code field, and click **Allow Access** to activate.

Port 443 is default, so you can ignore when inputting the Gateway.



Computer Name
My Computer

Connection Status
No active session

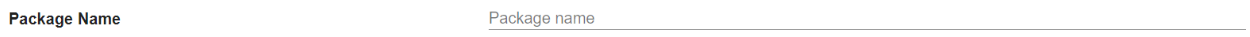
Computer Deployment
Enter code from your admin to allow access to this computer.

Gateway ①
Code ②
Allow Access ③

Team admin can further configure the Streamer's access permission on the management console.

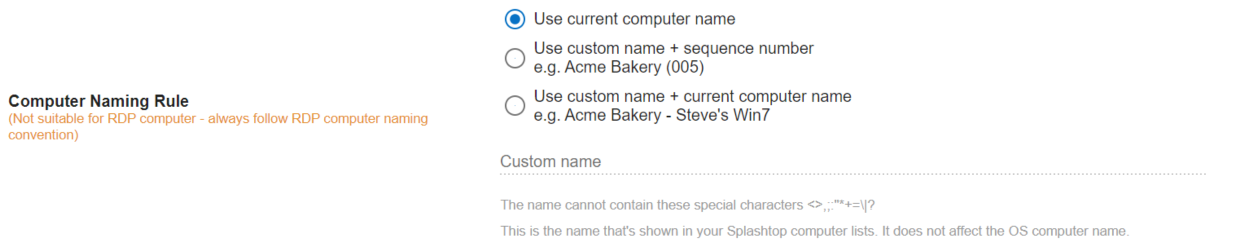
deploy options

You can specify deploy options when creating the deployment package. Here explains the meaning of these options.



Package Name Package name

Specify a friendly name for the deploy package for convenience.



Computer Naming Rule
(Not suitable for RDP computer - always follow RDP computer naming convention)

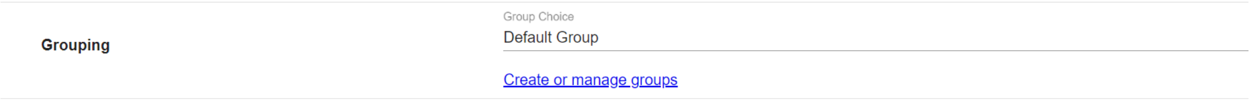
● Use current computer name
○ Use custom name + sequence number
e.g. Acme Bakery (005)
○ Use custom name + current computer name
e.g. Acme Bakery - Steve's Win7

Custom name

The name cannot contain these special characters <>,;:"*+=\|?

This is the name that's shown in your Splashtop computer lists. It does not affect the OS computer name.

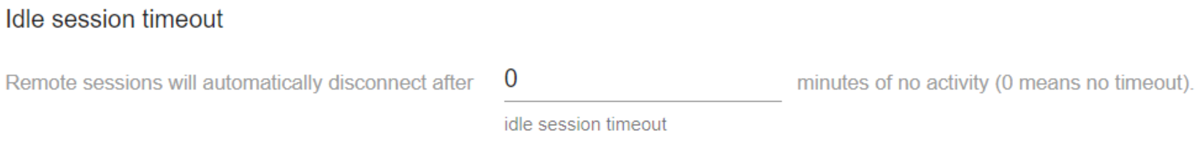
Specify how the computer will be named and displayed on the management console and also on the client app side.



Grouping Group Choice: Default Group

Create or manage groups

Specify which group the computer should be belong to, **Group** provides a way to organize the computers and grant access permissions in convenience.

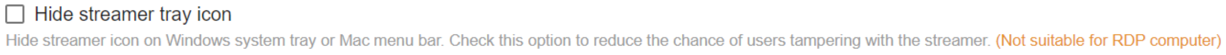


Idle session timeout

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

idle session timeout

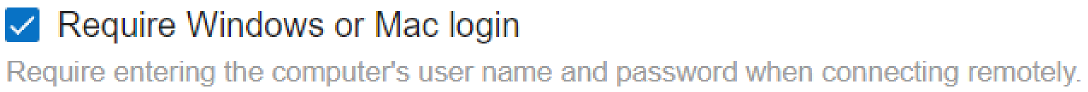
Specify the session idle time to disconnect.



□ 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. (Not suitable for RDP computer)

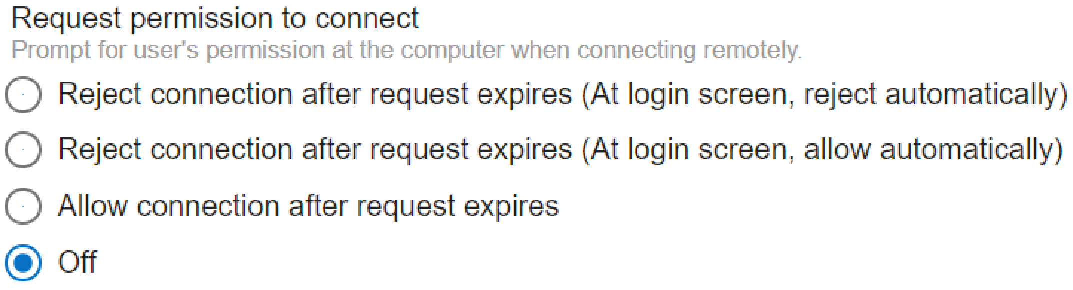
Specify if the Streamer tray icon should be hidden from user's system tray (Windows/Mac).



☑ Require Windows or Mac login

Require entering the computer's user name and password when connecting remotely.

Specify if user needs to input Windows/Mac login credential for the connection.



Request permission to connect

Prompt for user's permission at the computer when connecting remotely.

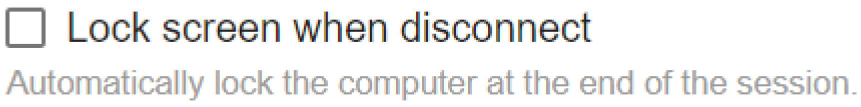
○ Reject connection after request expires (At login screen, reject automatically)

○ Reject connection after request expires (At login screen, allow automatically)

○ Allow connection after request expires

● Off

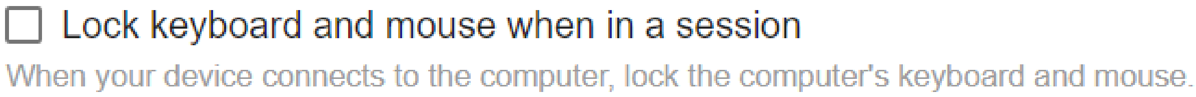
Specify the user's rule on permission when connection comes in.



□ Lock screen when disconnect

Automatically lock the computer at the end of the session.

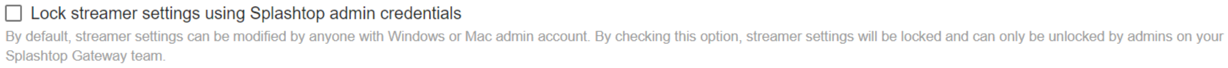
Specify if the screen should be locked when disconnect.



□ Lock keyboard and mouse when in a session

When your device connects to the computer, lock the computer's keyboard and mouse.

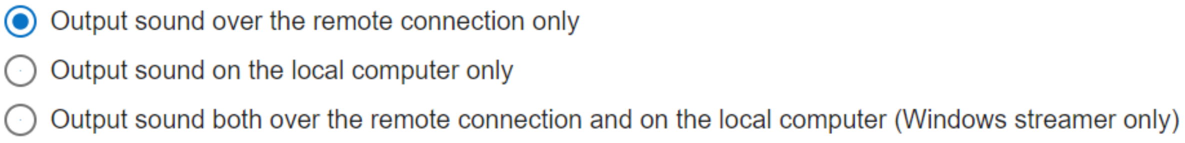
Specify if keyboard and mouse should be locked when in a remote session.



□ Lock streamer settings using Splashtop admin credentials

By default, streamer settings can be modified by anyone with Windows or Mac admin account. By checking this option, streamer settings will be locked and can only be unlocked by admins on your Splashtop Gateway team.

Specify if the Streamer settings page should be locked with Splashtop admin credential, it's the way to prevent user to change the setting by own.



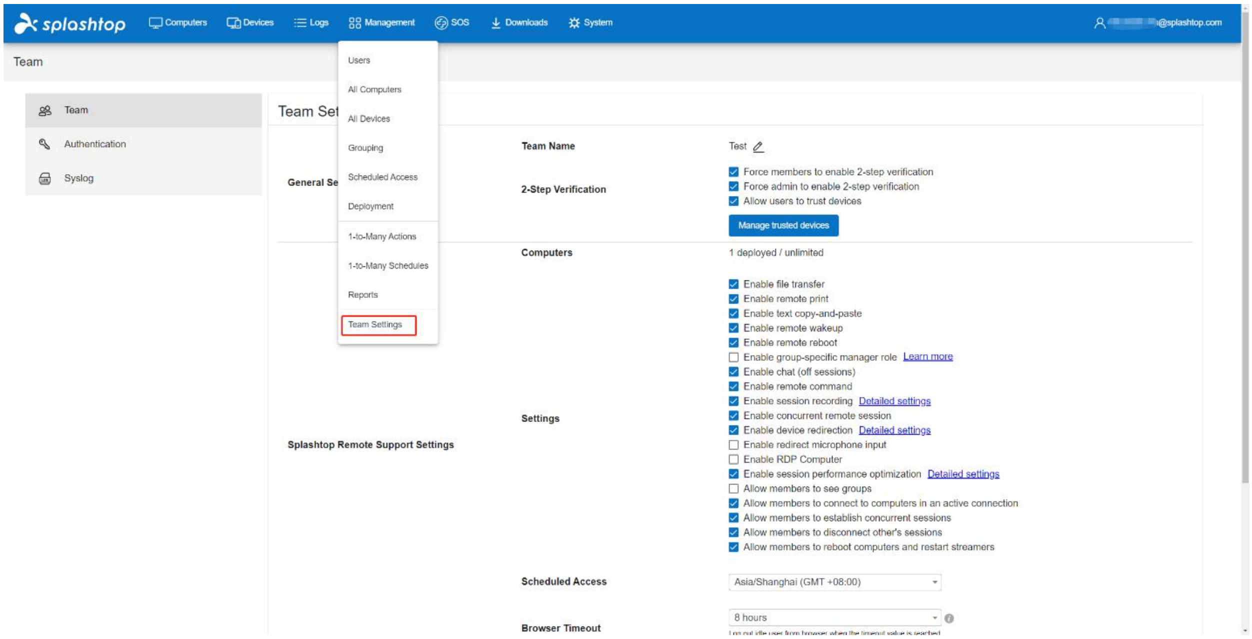
● Output sound over the remote connection only
○ Output sound on the local computer only
○ Output sound both over the remote connection and on the local computer (Windows streamer only)

Specify whether the audio should be redirected to the client side.

Team Settings

A team is a concept in multi-tenant Splashtop On-Prem system, where a tenant is regarded as a team. The Team Administrator is able to access and manage the Team Settings in the Management Console.

Team Settings



Splashtop Remote Support Settings

Team Name: Test

2-Step Verification
☑ Force members to enable 2-step verification
☑ Force admin to enable 2-step verification
☑ Allow users to trust devices

Computers: 1 deployed / unlimited

Settings
☑ Enable file transfer
☑ Enable remote print
☑ Enable text copy-and-paste
☑ Enable remote wakeup
☑ Enable remote reboot
☐ Enable group-specific manager role Learn more
☑ Enable chat (off sessions)
☑ Enable remote command
☑ Enable session recording Detailed settings
☑ Enable concurrent remote session
☑ Enable device redirection Detailed settings
☐ Enable redirect microphone input
☐ Enable RDP Computer
☑ Enable session performance optimization Detailed settings
☐ Allow members to see groups
☑ Allow members to connect to computers in an active connection
☑ Allow members to establish concurrent sessions
☑ Allow members to disconnect other's sessions
☑ Allow members to reboot computers and restart streamers

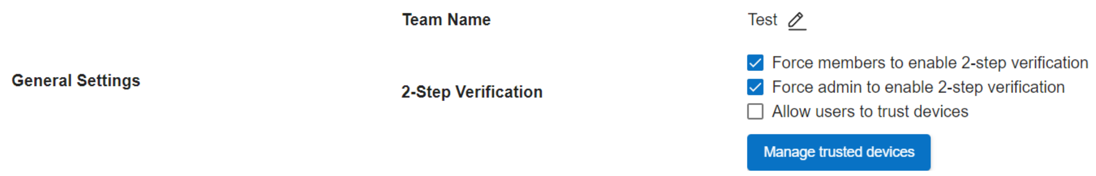
Scheduled Access: Asia/Shanghai (GMT +08:00)

Browser Timeout: 8 hours
Log out idle user from browser when the timeout value is reached

There are three sections in the page:

- **General Settings**
- **Splashtop Remote Support Settings**
- **Splashtop On-Demand Support Settings/SOS**

General Settings



General Settings

Team Name Test

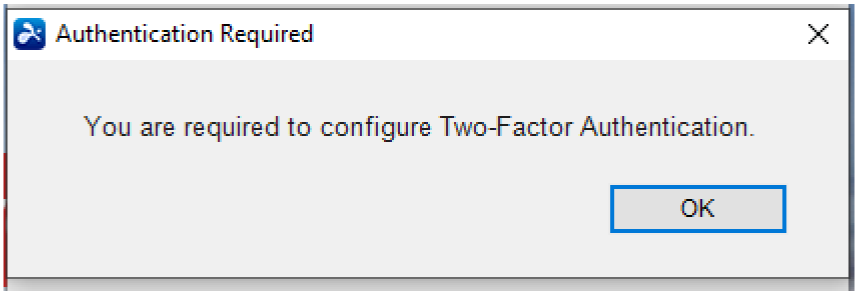
2-Step Verification

☑ Force members to enable 2-step verification
☑ Force admin to enable 2-step verification
□ Allow users to trust devices

Team Name: you can customize the Team Name here. The Team Name will reflect in account information of all Streamer and client devices.

2-Step Verification: 2-Step Verification adds another layer of security by time-based OTP verification provided by prevalent authenticator APPs in mobile phones. An On-Prem client must input a 6-digit OTP code to log in to the device.

Force members to enable 2-step verification: if this option is checked, a member user is required to set up a 2-step verification device when he tries to log in to On-Prem client for the first time.

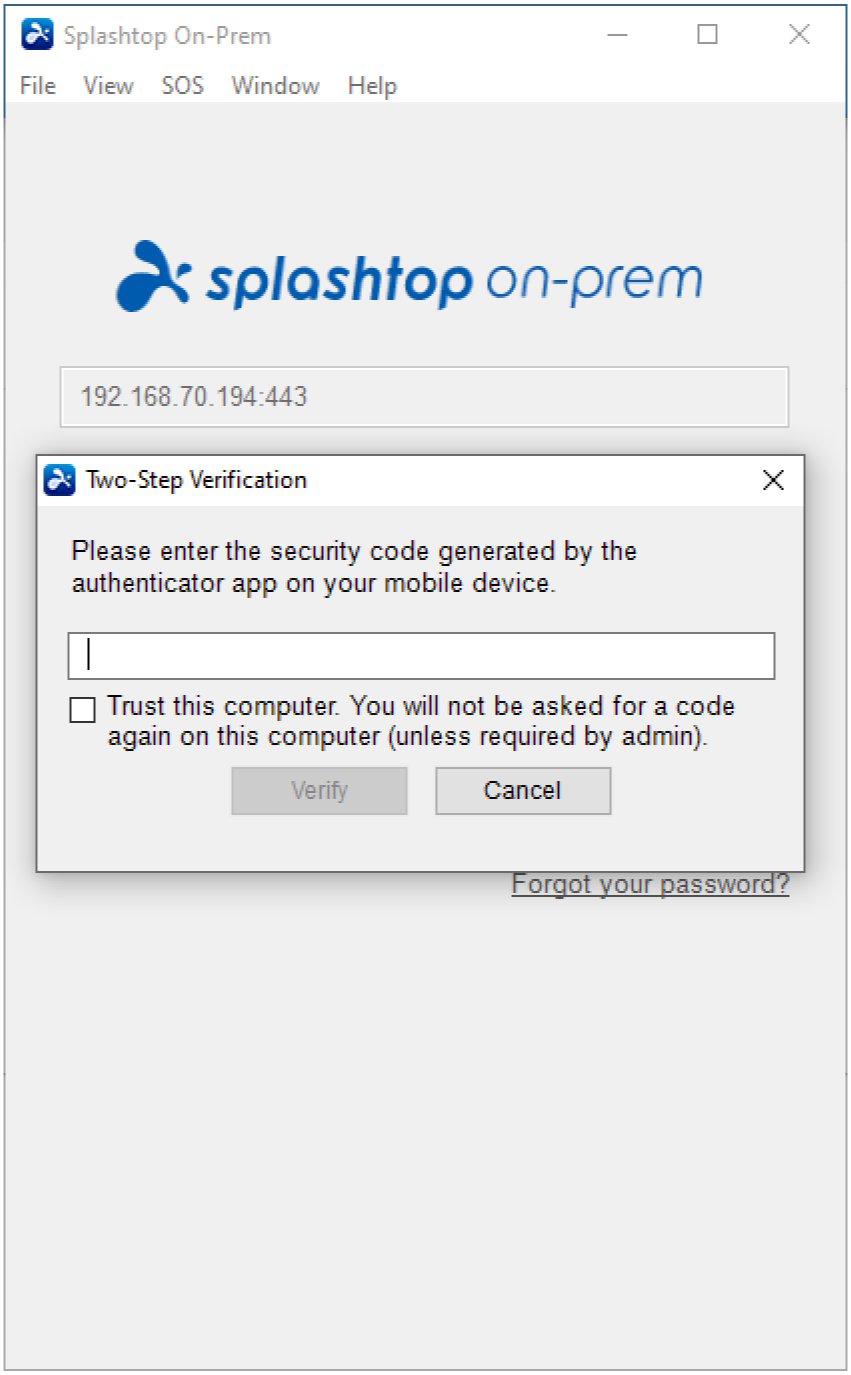


Authentication Required

You are required to configure Two-Factor Authentication.

Force admin to enable 2-step verification: if this open is checked, an admin user is required to set up a 2-step verification device when he tries to log in to On-Prem client for the first time.

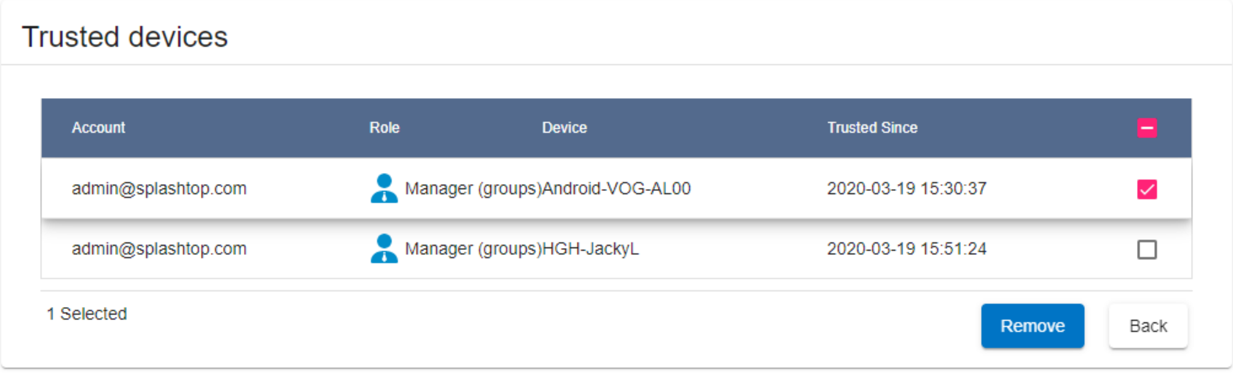
Allow users to trust devices: if this option is checked, a Splashtop On-Prem user can choose to trust a client device so that he is exempt from entering OTP code for future login.



Please enter the security code generated by the authenticator app on your mobile device.

□ Trust this computer. You will not be asked for a code again on this computer (unless required by admin).

Manage trusted devices: Team administrator is able to overview the trusted devices and remove them if necessary.

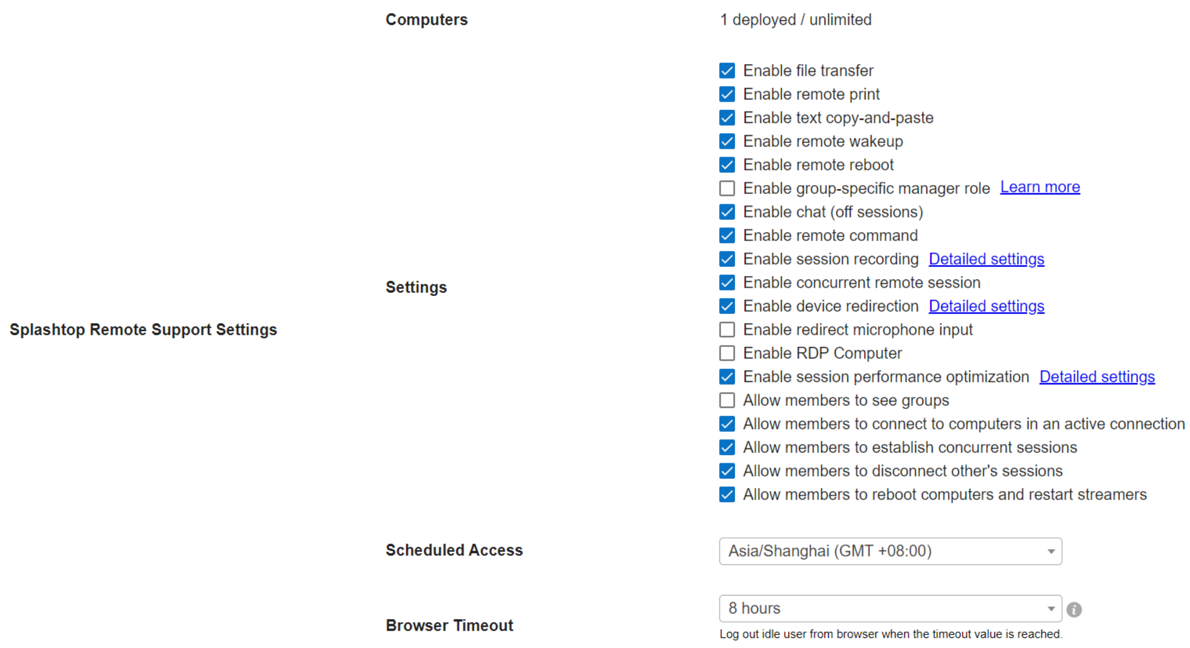


Trusted devices

Account	Role	Device	Trusted Since	⊟
admin@splashtop.com	Manager (groups)	Android-VOG-AL00	2020-03-19 15:30:37	☑
admin@splashtop.com	Manager (groups)	HGH-JackyL	2020-03-19 15:51:24	□

1 Selected

Splashtop Remote Support Settings



Splashtop Remote Support Settings	Computers	1 deployed / unlimited
	Settings	☑ Enable file transfer ☑ Enable remote print ☑ Enable text copy-and-paste ☑ Enable remote wakeup ☑ Enable remote reboot □ Enable group-specific manager role Learn more ☑ Enable chat (off sessions) ☑ Enable remote command ☑ Enable session recording Detailed settings ☑ Enable concurrent remote session ☑ Enable device redirection Detailed settings □ Enable redirect microphone input □ Enable RDP Computer ☑ Enable session performance optimization Detailed settings □ Allow members to see groups ☑ Allow members to connect to computers in an active connection ☑ Allow members to establish concurrent sessions ☑ Allow members to disconnect other's sessions ☑ Allow members to reboot computers and restart streamers
	Scheduled Access	Asia/Shanghai (GMT +08:00)
	Browser Timeout	8 hours Log out idle user from browser when the timeout value is reached.

Enable file transfer: Enable file transfer between the local and remote computer (Windows and Mac only).

Enable remote print: Enable document printing from a Streamer computer to a printer connected to the client computer.

Enable remote wake: Enable waking up a Streamer computer from a client device.

Enable remote reboot: Enable rebooting a Streamer computer from a client device.

Allow members to see groups: Allow member users to see computers in his group.

Enable group-specific manager role: Enable group manager role who manages a group.

Enable chat (off sessions): Enable off-session chat function.

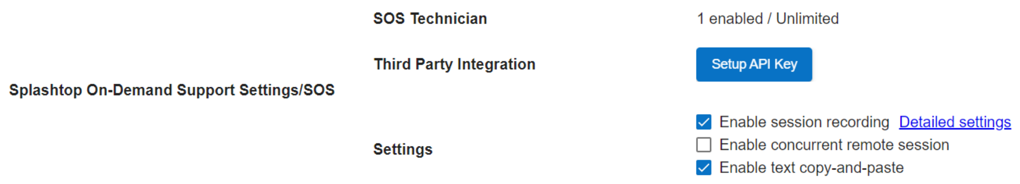
Enable remote command: Enable sending command to a Streamer computer from a client computer.

Enable session recording: Enable session recording and saved to a specific path on On Prem app computer.

Enable concurrent remote session: Enable concurrent remote session to a Streamer computer from multiple client devices.

Splashtop On-demand Support Settings/SOS

Splashtop On-demand support, A.K.A SOS, is a way of remote support without the endpoint installing any software. Instead, the endpoint downloads and launches a portable SOS app, to which a technician can connect with a Splashtop On-Prem client.



Splashtop On-Demand Support Settings/SOS	SOS Technician	1 enabled / Unlimited
	Third Party Integration	Setup API Key
	Settings	☑ Enable session recording Detailed settings □ Enable concurrent remote session ☑ Enable text copy-and-paste

Setup API Key: Enable API and get API Key for third-party service.

Enable concurrent remote session: Enable concurrent remote session for multiple Splashtop client to connect to the same SOS app.

Enable session recording: Enable session recording for SOS remote support session and saved to a specific path on On Prem app computer.

Enable text copy-and-paste: Enable text copy-and-paste for SOS remote support session.

Setup 2-step verification

Two-step verification, also known as 2-factor authentication or 2FA, or Multi-factor authentication (mfa) is an optional but highly recommended security feature.

Once enabled, logging into Splashtop will require an additional six-digit security code, in addition to your account's password. The security code will be generated by an authenticator app on your mobile device. (Text messaging is not supported.)

This means, even if someone has figured out or stolen your Splashtop On-Prem account ID and password, he or she will not be able to log into your account and access your computers.

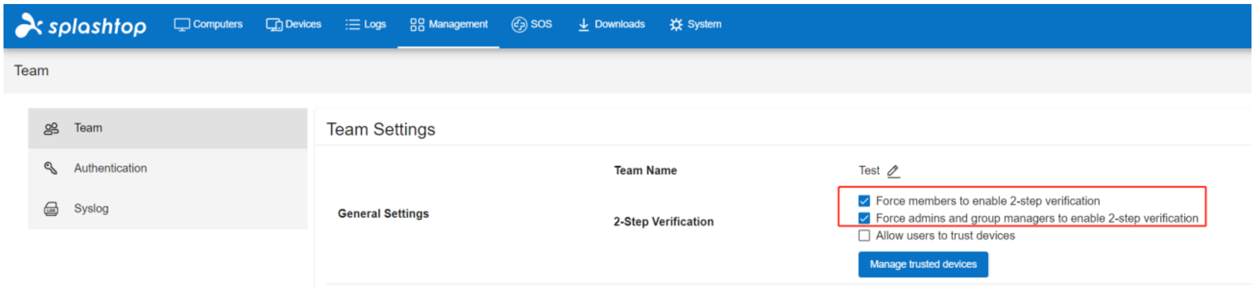
Splashtop On-Prem support TOTP (Time-based One-Time Password algorithm) based 2 step verification, and verified with the following authenticator apps:

- Google Authenticator (Android/iPhone/BlackBerry)
- Duo Mobile (Android/iPhone)
- Microsoft Authenticator (Android/iPhone/Windows Phone 7)
- Okta Verify (Android/iPhone)
- Other popular OTP apps

Setup Guide

Step 1

Login to management console as Team Owner, and go to **Management** > **Settings**, you can specify how and whom the 2-step verification should be enforced.



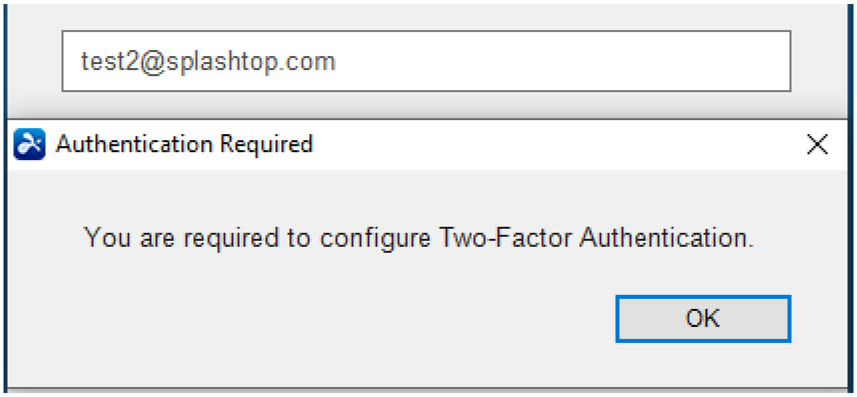
Team Settings

General Settings

Team Name: Test

2-Step Verification:
☑ Force members to enable 2-step verification
☑ Force admins and group managers to enable 2-step verification
□ Allow users to trust devices

If an account has been enforced to enable 2-step verification, he/she will be required to pass through the 2-step verification setup guide to continue using the service, or it will pop up the following window when they try to log in to the client app.



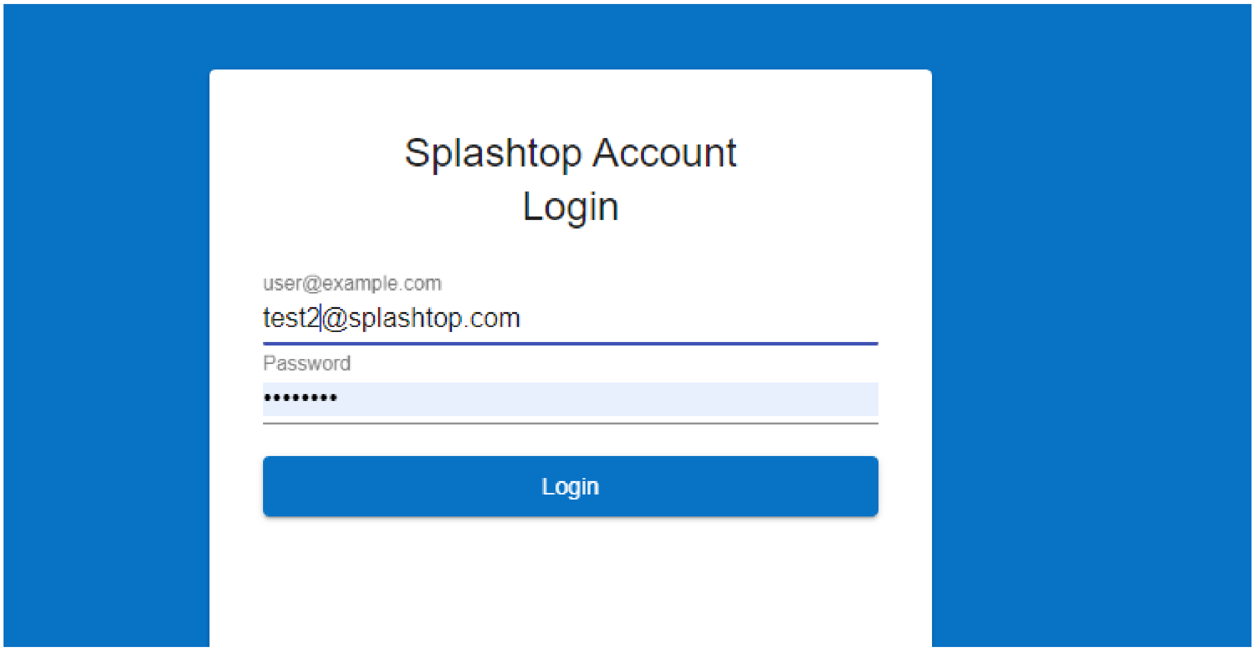
test2@splashtop.com

Authentication Required

You are required to configure Two-Factor Authentication.

Step 2

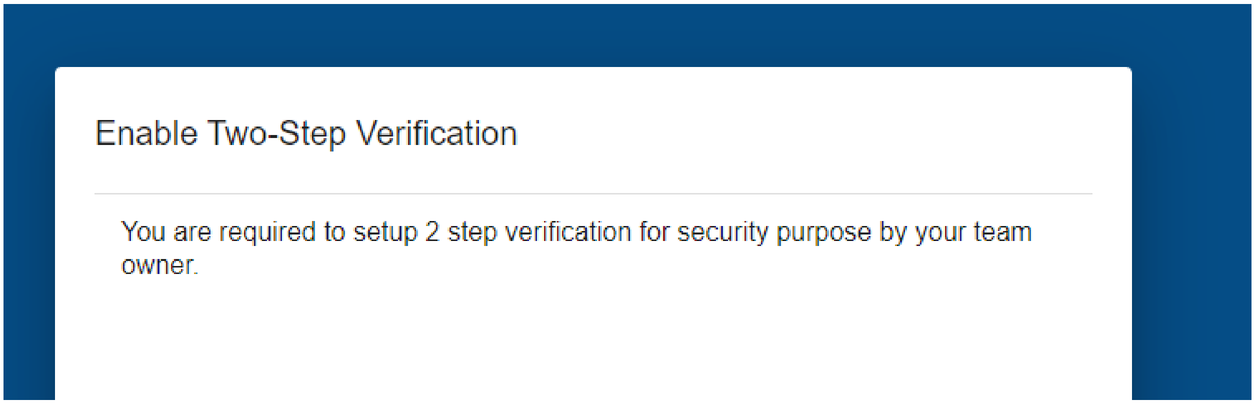
To set up the 2-step verification account for the first time, the user is required to log in to the **Gateway** using his/her own account.



Splashtop Account Login

user@example.com
test2@splashtop.com
Password
•••••••••

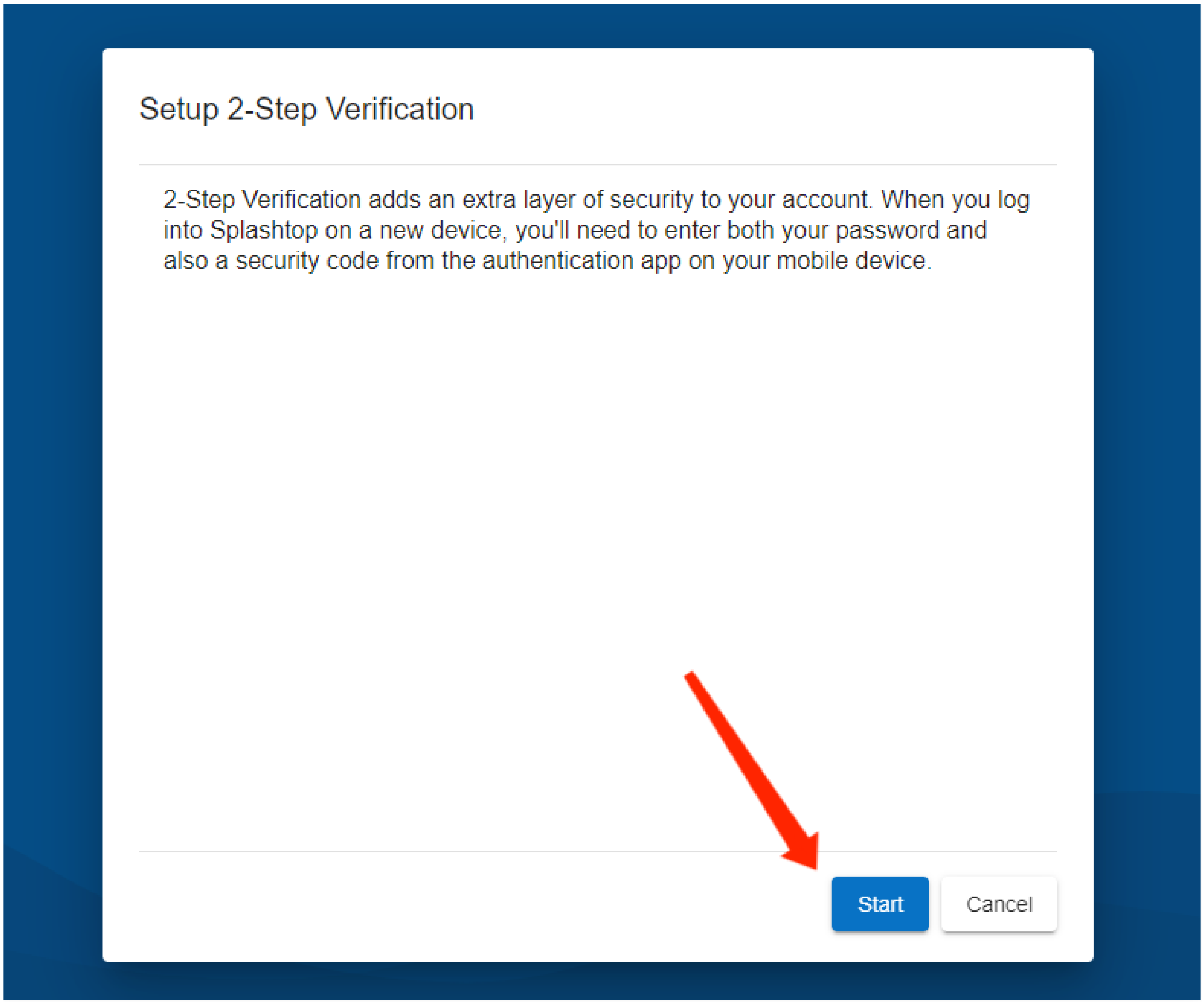
Follow the instructions to complete the setup.



Enable Two-Step Verification

You are required to setup 2 step verification for security purpose by your team owner.

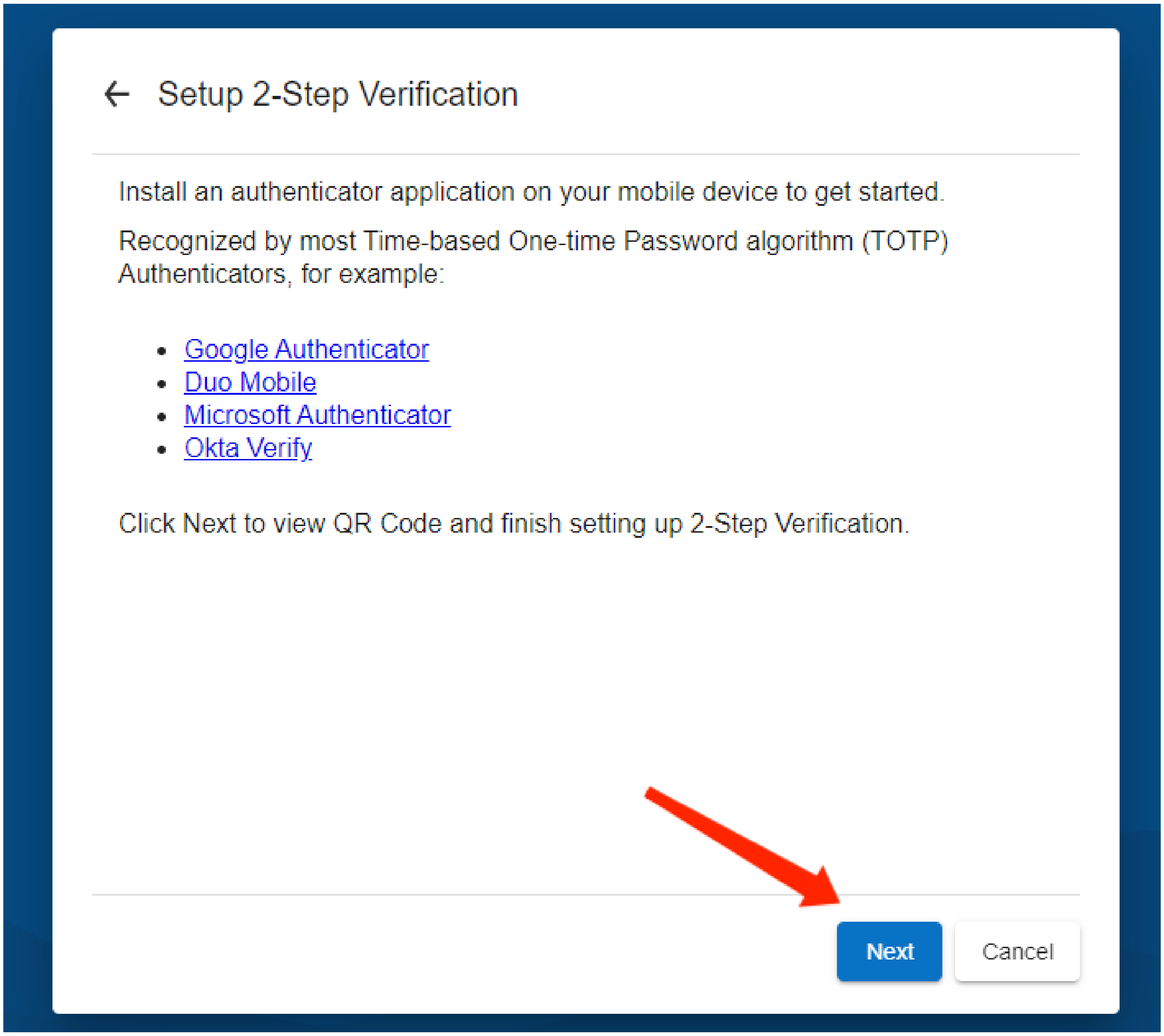
Click **Start.**



Setup 2-Step Verification

2-Step Verification adds an extra layer of security to your account. When you log into Splashtop on a new device, you'll need to enter both your password and also a security code from the authentication app on your mobile device.

Click **Next** and choose one **Authenticator app.** Take **Okta Verify** as an example.



Setup 2-Step Verification

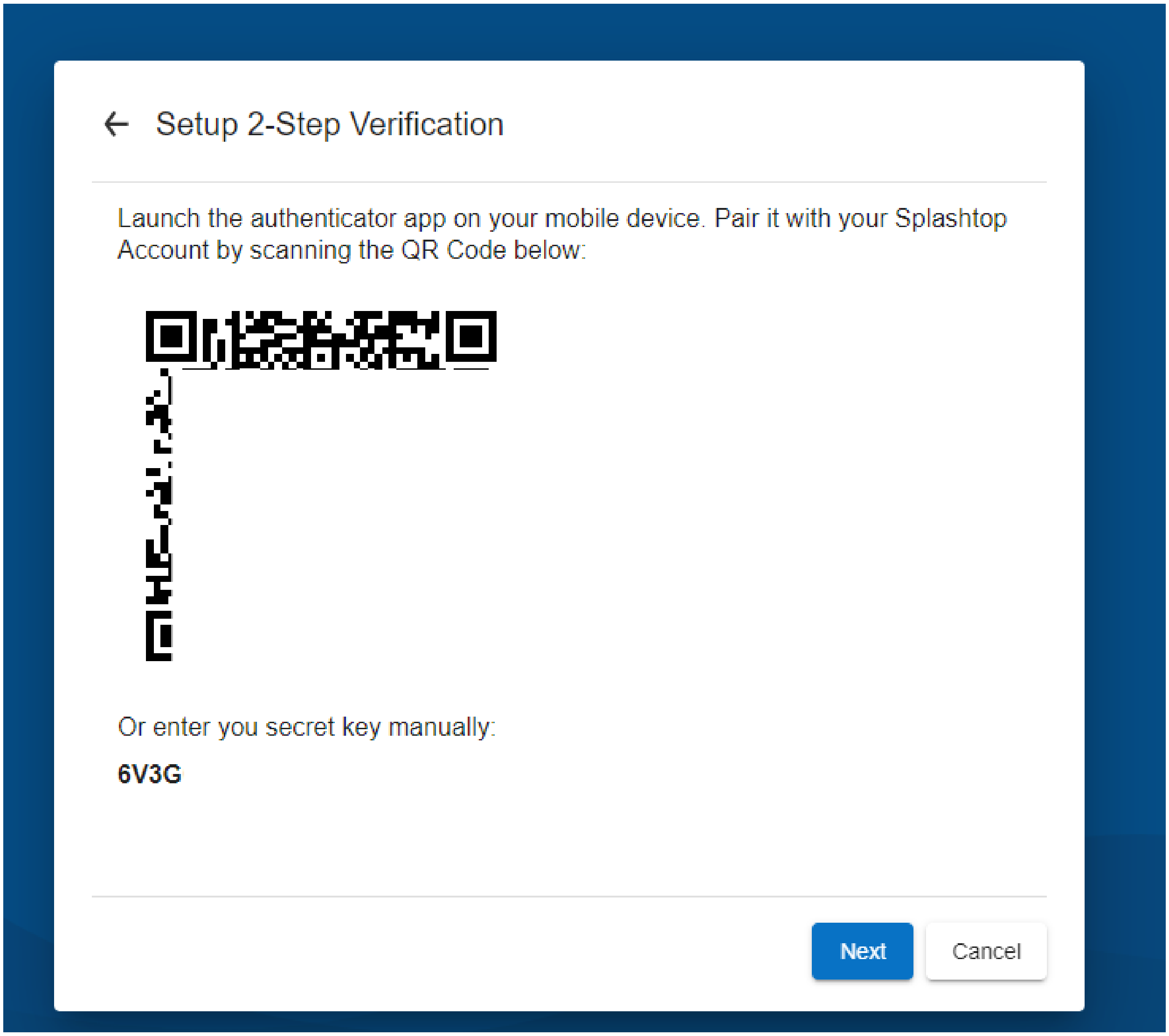
Install an authenticator application on your mobile device to get started.

Recognized by most Time-based One-time Password algorithm (TOTP) Authenticators, for example:

- Google Authenticator
- Duo Mobile
- Microsoft Authenticator
- Okta Verify

Click Next to view QR Code and finish setting up 2-Step Verification.

It would generate a **QR code**, users need to launch the **authenticator app** to scan it.



Setup 2-Step Verification

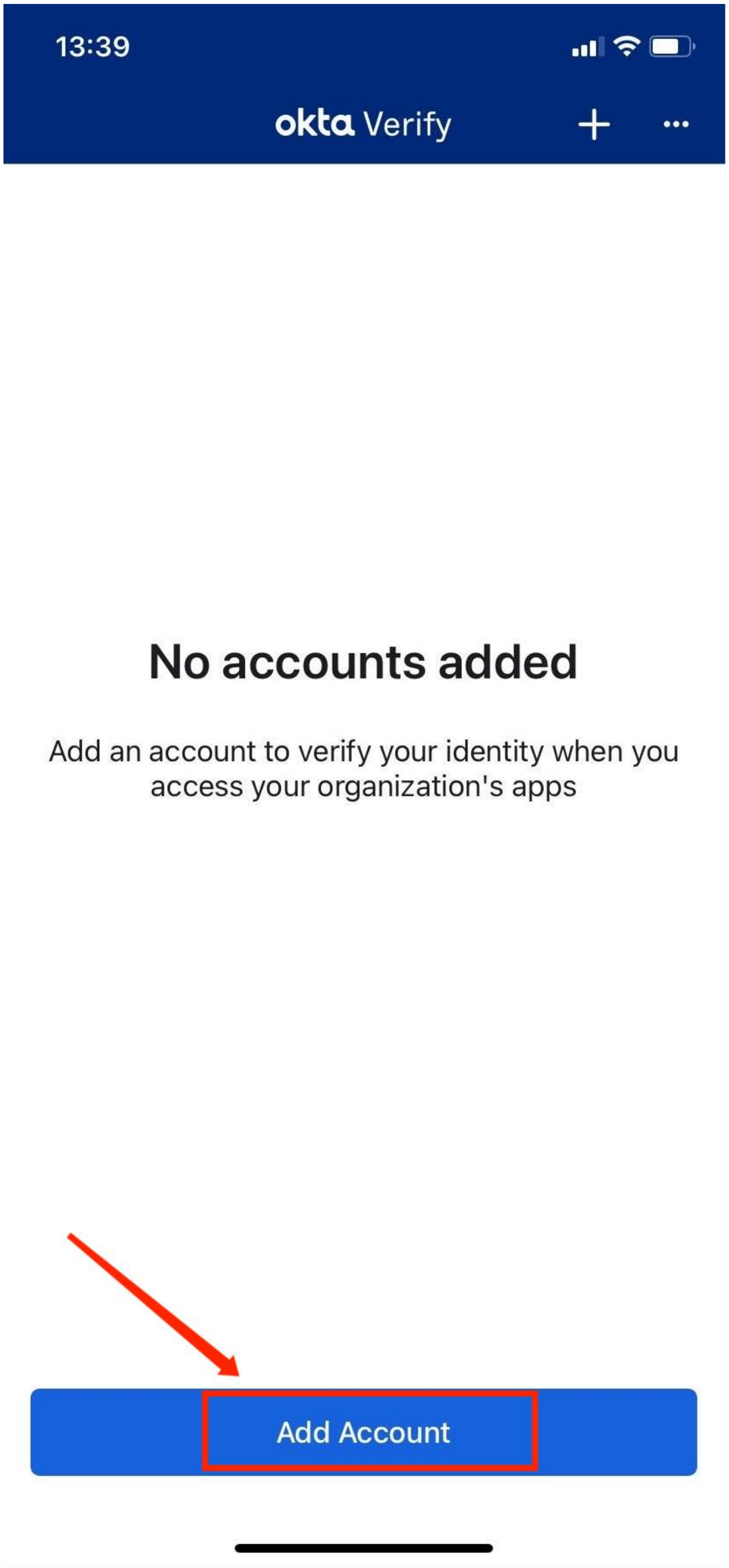
Launch the authenticator app on your mobile device. Pair it with your Splashtop Account by scanning the QR Code below:

Or enter you secret key manually:

6V3G

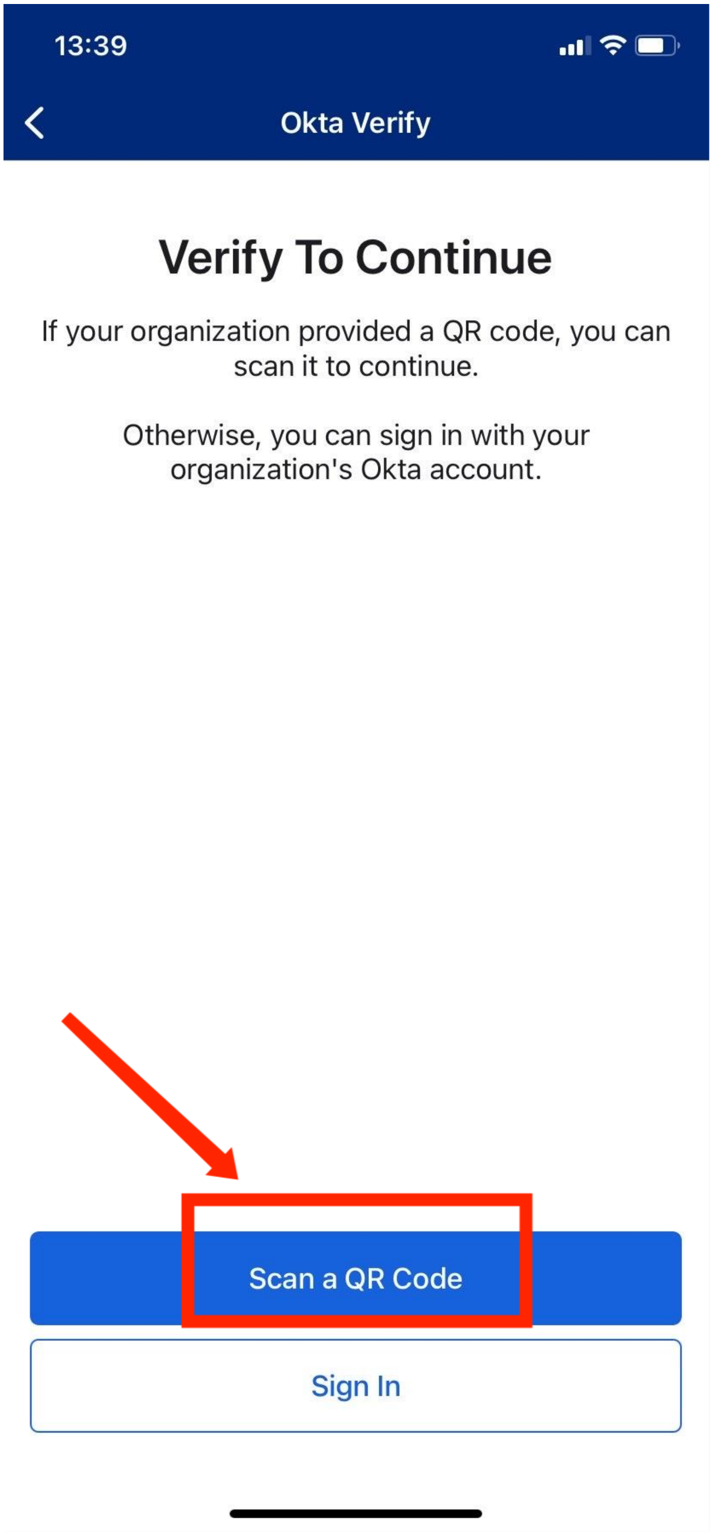
Launch the **okta Verify** and complete the following steps.

Add account -> Organization -> Scan a QR code -> Done.



No accounts added

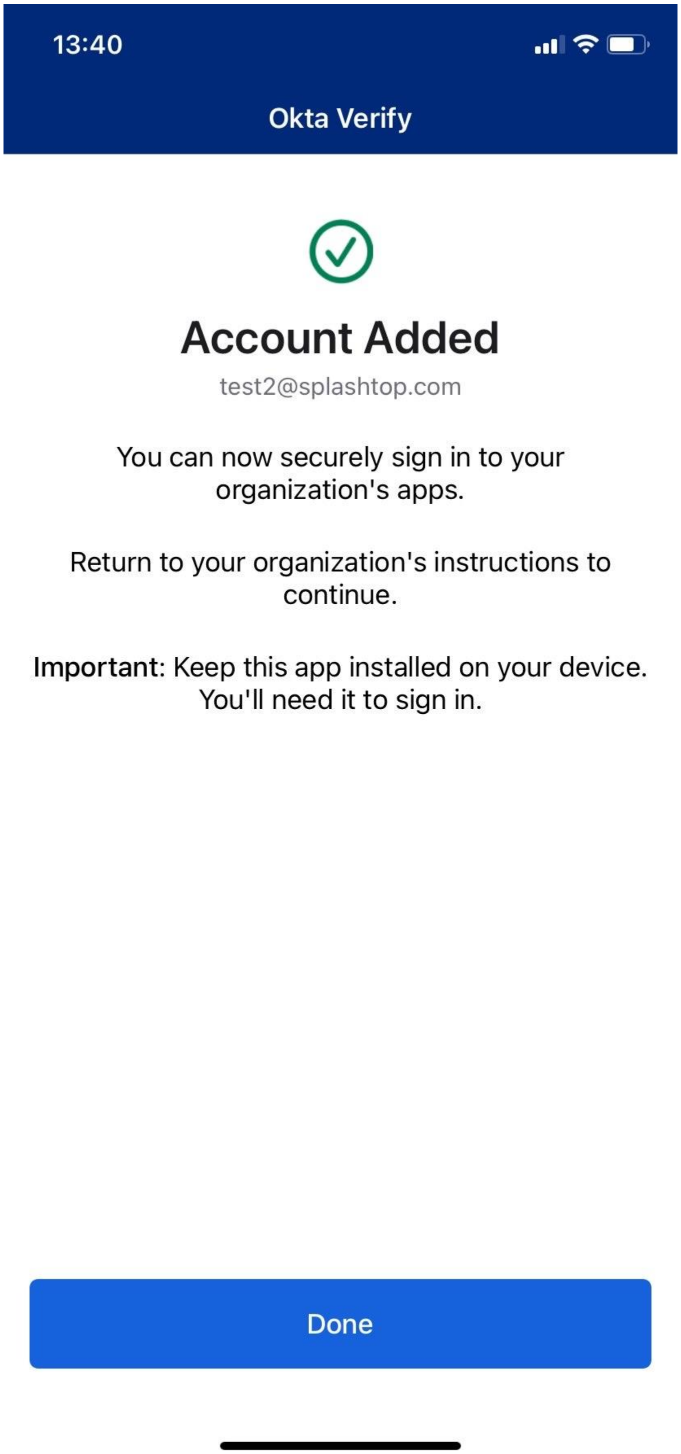
Add an account to verify your identity when you access your organization's apps



Verify To Continue

If your organization provided a QR code, you can scan it to continue.

Otherwise, you can sign in with your organization's Okta account.



Account Added

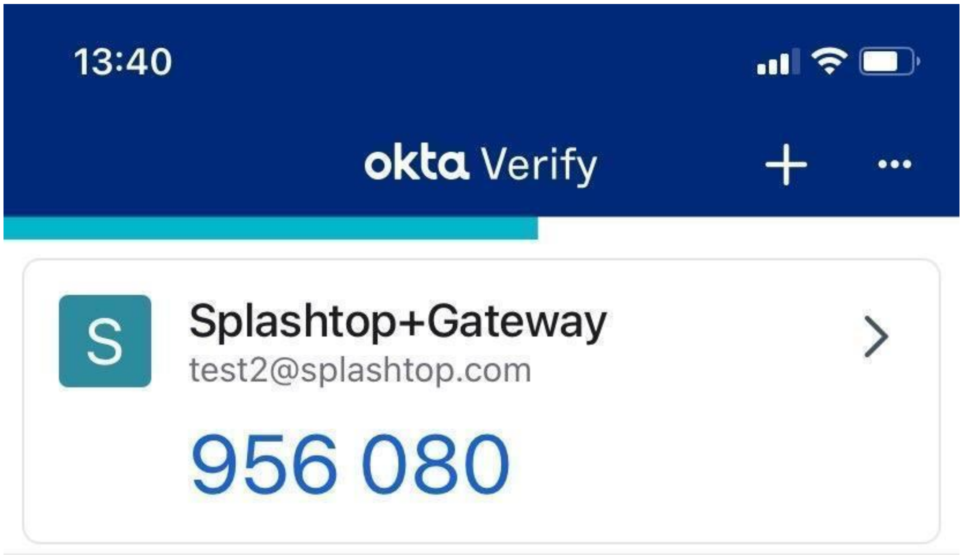
test2@splashtop.com

You can now securely sign in to your organization's apps.

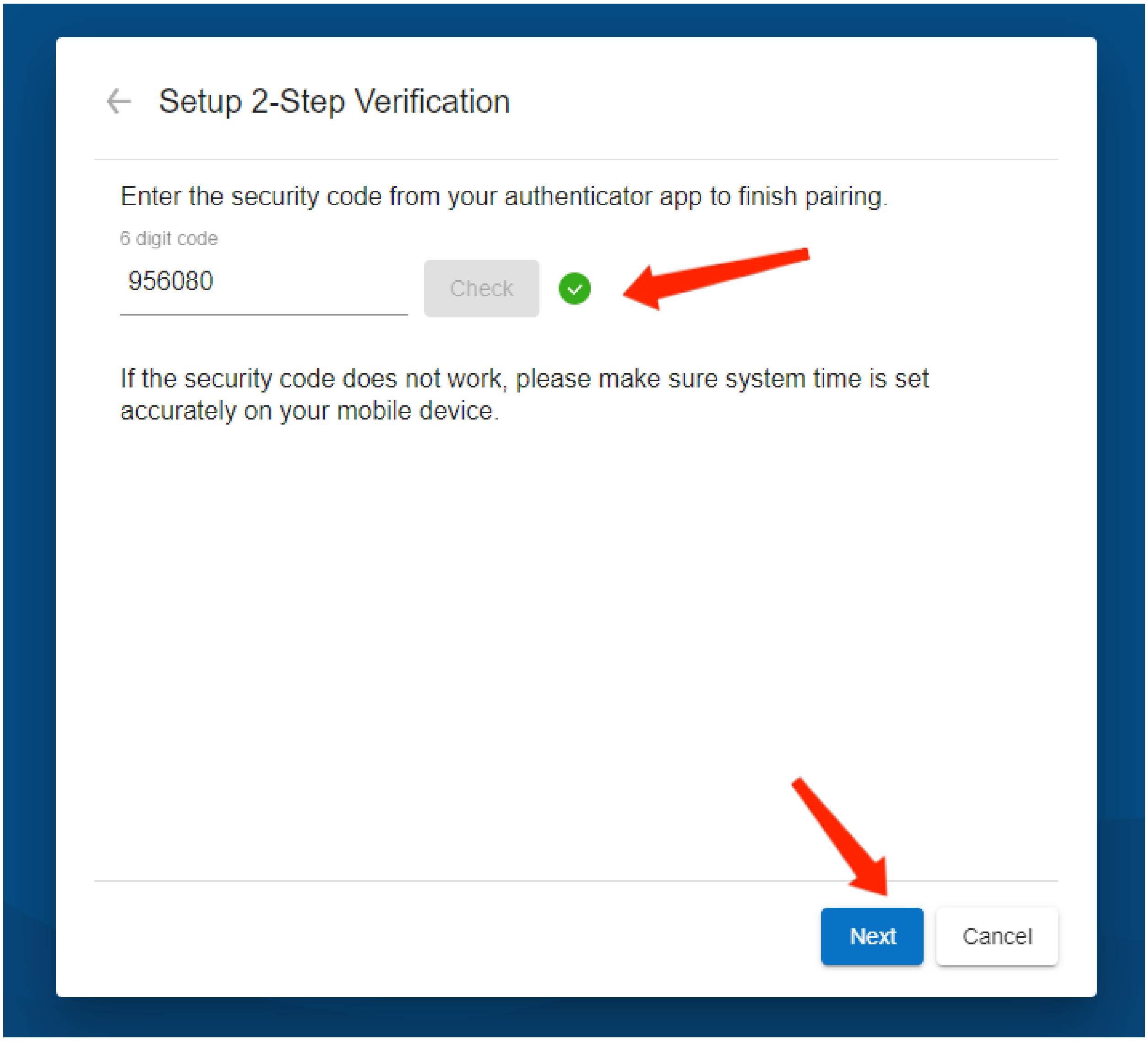
Return to your organization's instructions to continue.

Important: Keep this app installed on your device. You'll need it to sign in.

It will generate the **security code** on your app. Enter the security code from your authenticator app to finish pairing.



13:40
okta Verify
+
•••
S
Splashtop+Gateway
test2@splashtop.com
956 080
>



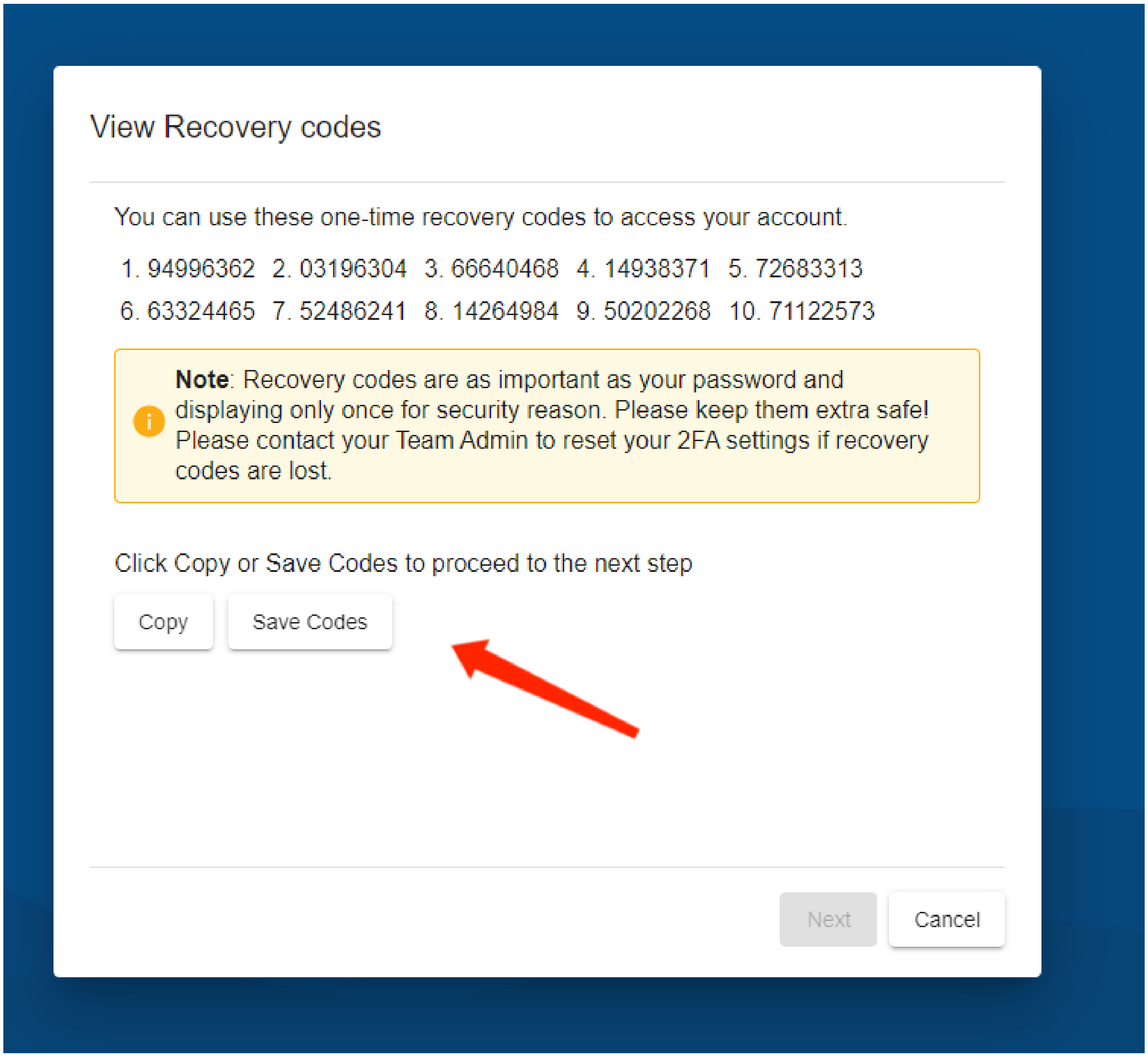
Setup 2-Step Verification

Enter the security code from your authenticator app to finish pairing.

6 digit code: 956080

If the security code does not work, please make sure system time is set accurately on your mobile device.

Click **Copy or Save codes** to proceed to the next step.



View Recovery codes

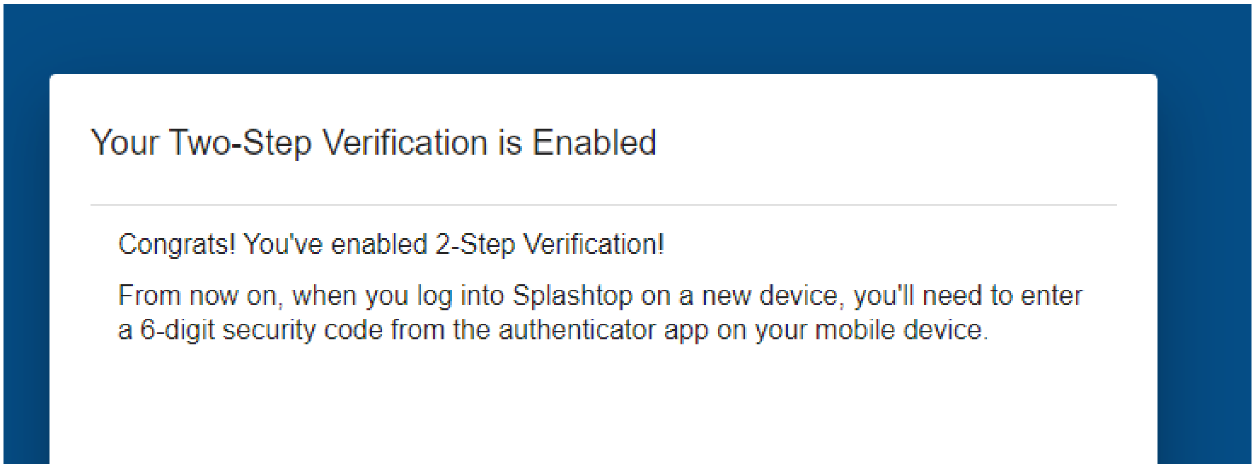
You can use these one-time recovery codes to access your account.

1. 94996362 2. 03196304 3. 66640468 4. 14938371 5. 72683313
6. 63324465 7. 52486241 8. 14264984 9. 50202268 10. 71122573

Note: Recovery codes are as important as your password and displaying only once for security reason. Please keep them extra safe! Please contact your Team Admin to reset your 2FA settings if recovery codes are lost.

Click Copy or Save Codes to proceed to the next step

Now, we have finished enabling two-step Verification. Users can login to Splashtop on a new device now!



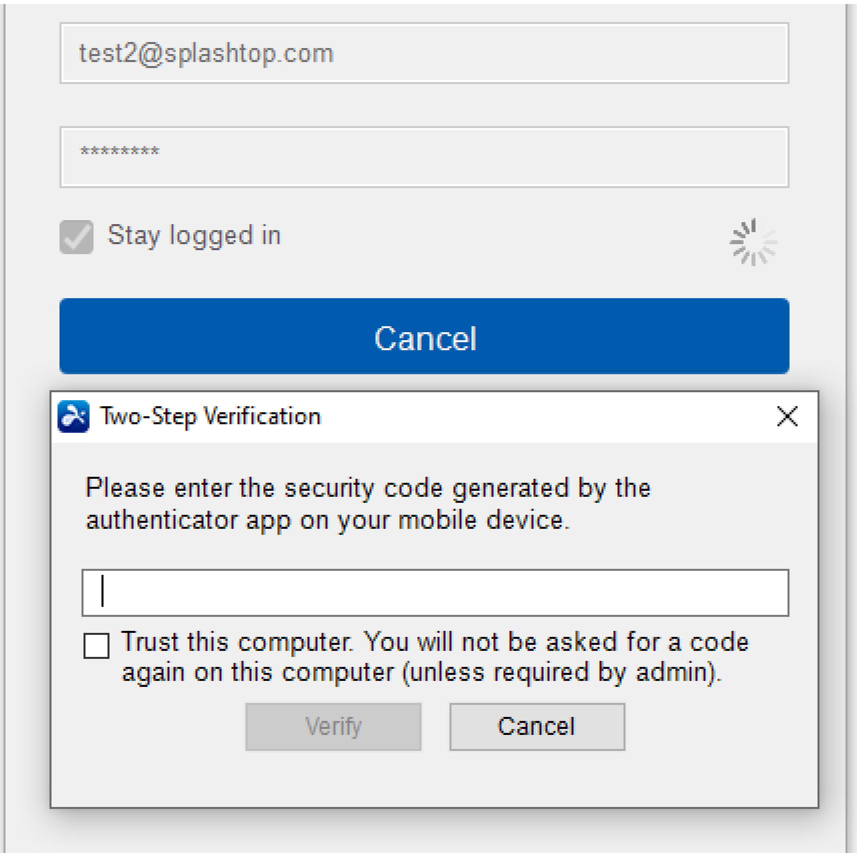
Your Two-Step Verification is Enabled

Congrats! You've enabled 2-Step Verification!

From now on, when you log into Splashtop on a new device, you'll need to enter a 6-digit security code from the authenticator app on your mobile device.

Step 3 Login console or On-Prem app with 2-sv enabled

Users will be required to enter the one-time passcode when 2-sv is enabled and setup. If Team Owner has **allowed trust device,** users can check trust this device as the convenience.



test2@splashtop.com

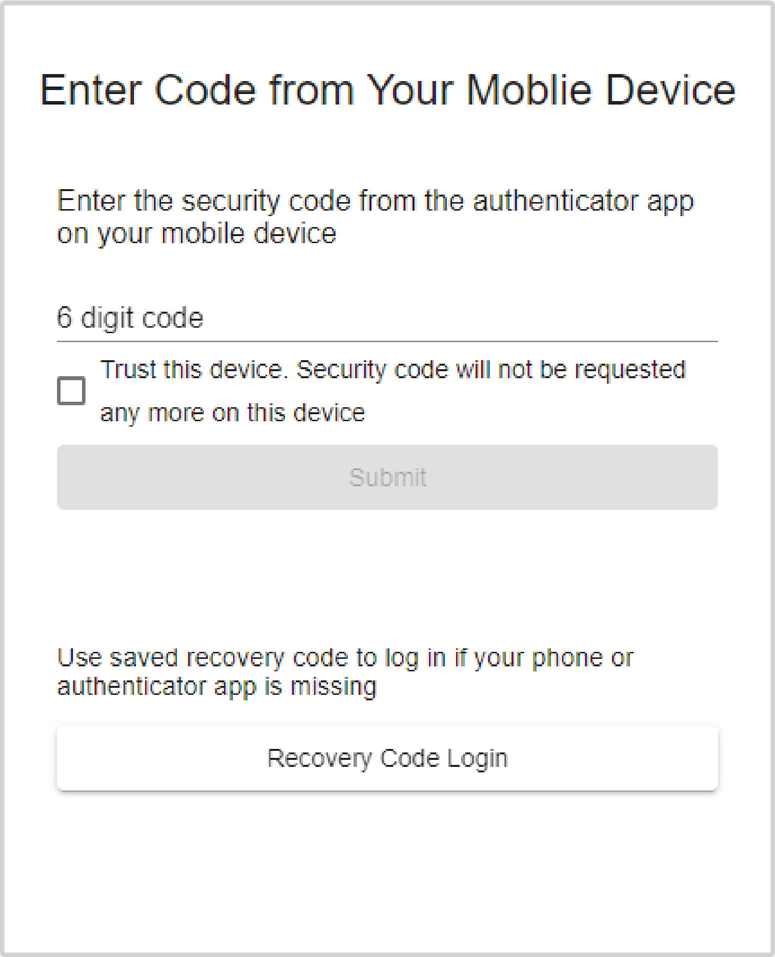
****

☑ Stay logged in

Please enter the security code generated by the authenticator app on your mobile device.

□ Trust this computer. You will not be asked for a code again on this computer (unless required by admin).

Figure. 2-sv passcode input dialog on On-Prem app



Enter Code from Your Moblie Device

Enter the security code from the authenticator app on your mobile device

6 digit code

□ Trust this device. Security code will not be requested any more on this device

Use saved recovery code to log in if your phone or authenticator app is missing

Figure. 2-sv passcode input dialog on web console

Q&A

1.Why I always can't pass 2-sv passcode?

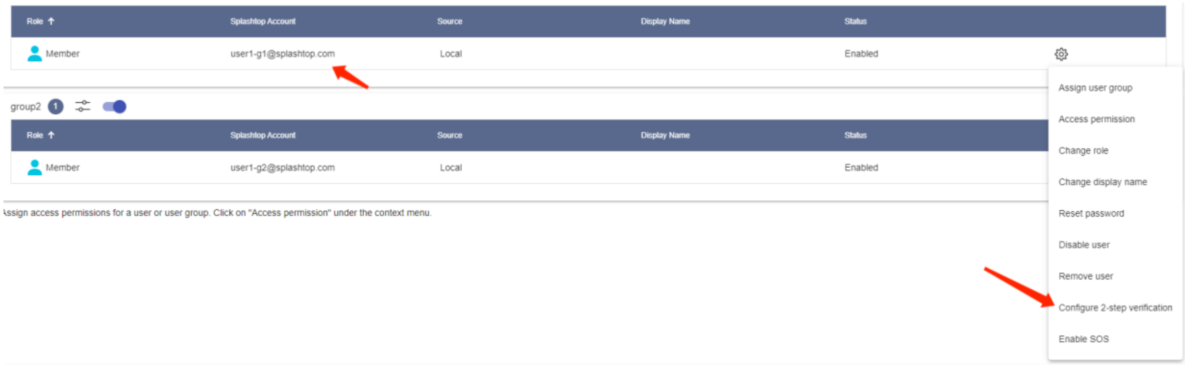
For TOTP is time and clock based authentication, if there are obvious system clock difference, like more than 30 seconds, you may encounter error to pass 2-sv passcode. please make sure your Gateway and authentication device has synchronized system time.

2.What if I lost my cell phone and forget my recovery code?

Please contact your **Team Admin** to reset your 2FA settings if recovery codes are lost.

The following is the procedure of resetting 2FA for administrator:

1. Login to gateway as administrator
2. Go to Management ->users -> Setting -> Configure 2-step verification



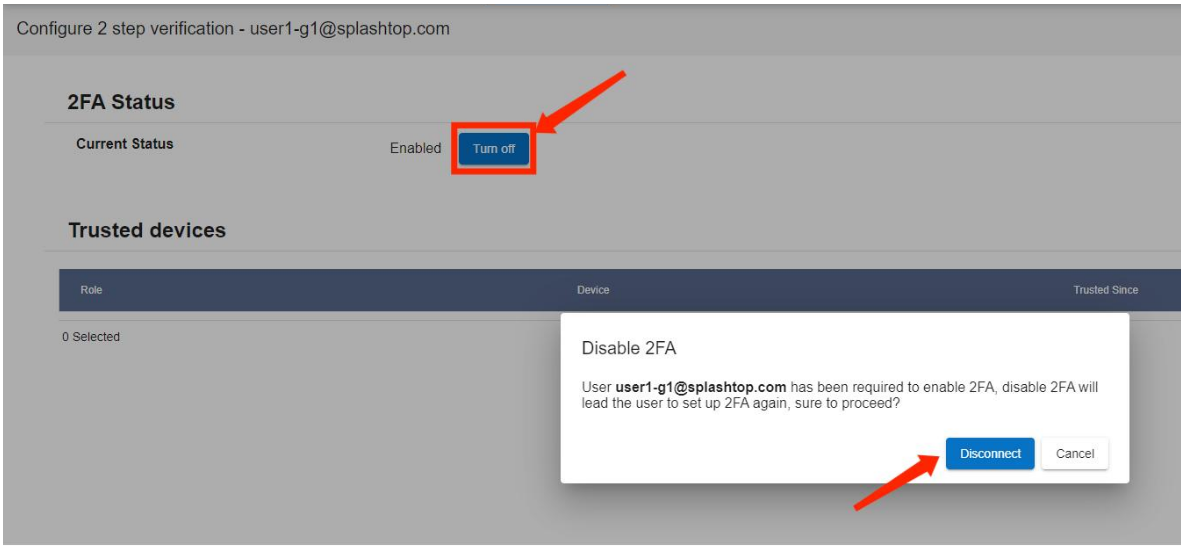
Role ↑	Splashtop Account	Source	Display Name	Status
Member	user1-g1@splashtop.com	Local		Enabled

group2 1

Role ↑	Splashtop Account	Source	Display Name	Status
Member	user1-g2@splashtop.com	Local		Enabled

ssign access permissions for a user or user group. Click on "Access permission" under the context menu.

3. Disable 2FA



Configure 2 step verification - user1-g1@splashtop.com

2FA Status

Current Status Enabled

Trusted devices

Role	Device	Trusted Since

0 Selected

Disable 2FA

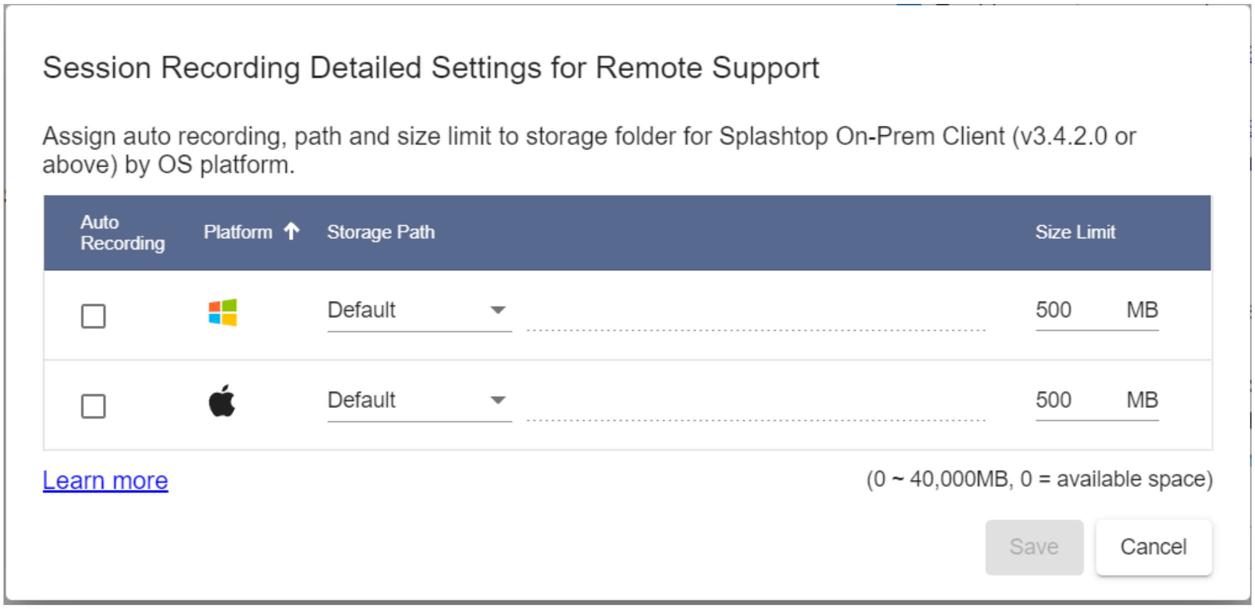
User **user1-g1@splashtop.com** has been required to enable 2FA, disable 2FA will lead the user to set up 2FA again, sure to proceed?

4. User could set up 2FA again.

Notice: For TOTP is time and clock-based authentication, if there are obvious system clock difference, like more than 30 seconds, you may encounter error to pass 2-sv passcode. please make sure your Gateway and authentication device has synchronized system time.

Session Recording on Gateway Web Console

Session Recording Detailed Settings



Session Recording Detailed Settings for Remote Support

Assign auto recording, path and size limit to storage folder for Splashtop On-Prem Client (v3.4.2.0 or above) by OS platform.

Auto Recording	Platform ↑	Storage Path		Size Limit
□	⊞	Default		500 MB
□		Default		500 MB

Learn more

(0 ~ 40,000MB, 0 = available space)

Auto Recording

- Keep Auto Recording checked would force Splashtop On-Prem app to automatically records each remote session when the session started.

- Settings from Splashtop Gateway Web Portal would overwrite On-Prem app settings by displaying "**Session recording is managed by team settings**" on **Options** > Advanced > Session Recording

Platform

- Currently only supports Windows and macOS.

Storage path

Recording files can be saved to different locations on On-Prem app computers or network drives by mapping UNC path to it.

- Default:

1. Windows - *C:\Users\username\Documents\Splashtop On-Prem*

2. macOS - */Users/username/Documents/Splashtop On-Prem*

- *Specific:*

1. *Manually input local folder path from On-Prem app computer.*
2. Manually input Windows UNC path: \\servername\path
3. Manually input macOS UNC path: //servername/path
4. Max path length: 256 characters.

- App Settings

Follows storage path based on **Splashtop On-Prem app settings**.

Size Limit

Recording files will be deleted automatically if the total recording file size exceeds the size limit.

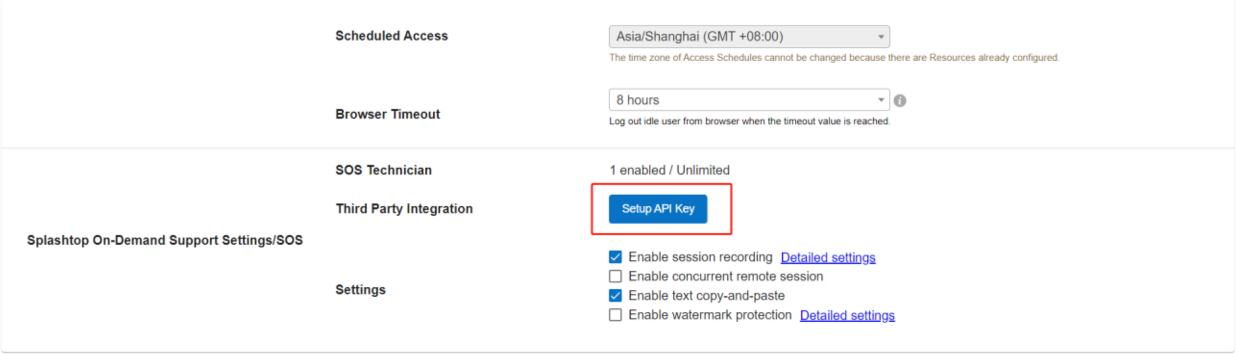
- Minimum: 0 MB (Unlimited, all available space on On-Prem app computer)
- Maximum: 40,000 MB

Set Up API Keys for Third-party Integration

An API key is generated in Splashtop Gateway and passed to a third-party ticketing system, which is used by the ticketing system to authenticate access to the back-end of Splashtop On-Prem system. The API key is basically the linkage between the ticketing system and Splashtop On-Prem back-end. A ticketing system hereby refers to a support portal, namely Freshservice, Freshdesk, Zendesk, Jira and ServiceNow.

To generate an API key, go to the Splashtop Gateway.

Open the **Management** page, and find **Third-party Integration** in the **Team** settings



Scheduled Access Asia/Shanghai (GMT +08:00)

The time zone of Access Schedules cannot be changed because there are Resources already configured.

Browser Timeout 8 hours

Log out idle user from browser when the timeout value is reached.

Splashtop On-Demand Support Settings/SOS

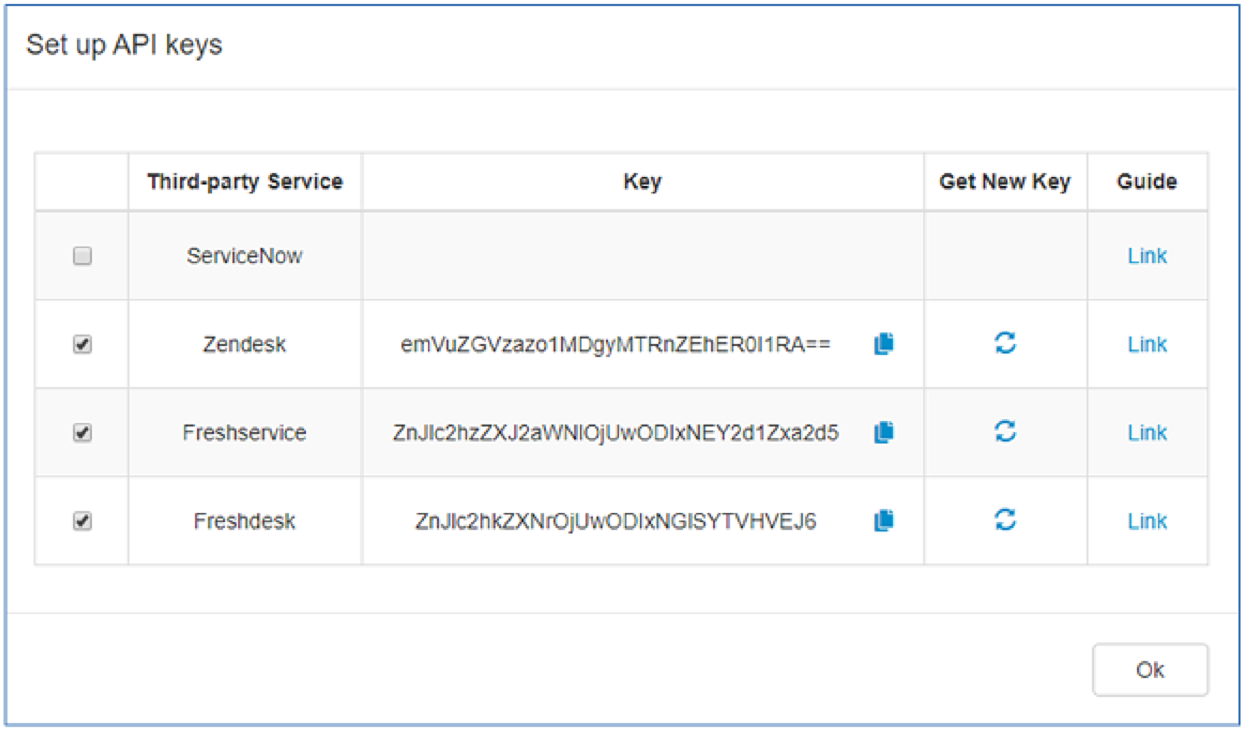
SOS Technician 1 enabled / Unlimited

Third Party Integration

Settings

- ☑ Enable session recording Detailed settings
- ☐ Enable concurrent remote session
- ☑ Enable text copy-and-paste
- ☐ Enable watermark protection Detailed settings

Once you click Set up API keys link, a pop-up window appears and it allows you to create an API key by simply checking the box on left of the ticketing system provider.



Set up API keys

	Third-party Service	Key	Get New Key	Guide
☐	ServiceNow			Link
☑	Zendesk	emVuZGVzazo1MDgyMTRnZEhER0I1RA==	↻	Link
☑	Freshservice	ZnJlc2hzZXJ2aWNlOjUwODIxNEY2d1Zxa2d5	↻	Link
☑	Freshdesk	ZnJlc2hkZXNrOjUwODIxNGISYTVHVEJ6	↻	Link

Copy the API key and paste it into appropriate field in the ticketing system app settings. If you need a new API key, one click on the refresh button and it will automatically generate a new key and retire the old key. In this case, do not forget to update the API key in the ticketing system, otherwise, Splashtop On-Prem back-end will fail the authentication.

Integrate Splashtop On-Prem with Freshservice

If you are using Freshservice to support customers or colleagues, it is now possible to remotely access the end user's computer to troubleshoot an issue easily, closely and efficiently, by launching the connection from the support ticket itself. Splashtop On-Prem, a top notch remote desktop solution with in-house deployment capability, is currently available to seamlessly integrate with your Freshservice account.

This article will guide you through the setup of the integration and how to use Splashtop to support your Freshservice end users.

Set Up Splashtop On-Prem - Freshservice Integration

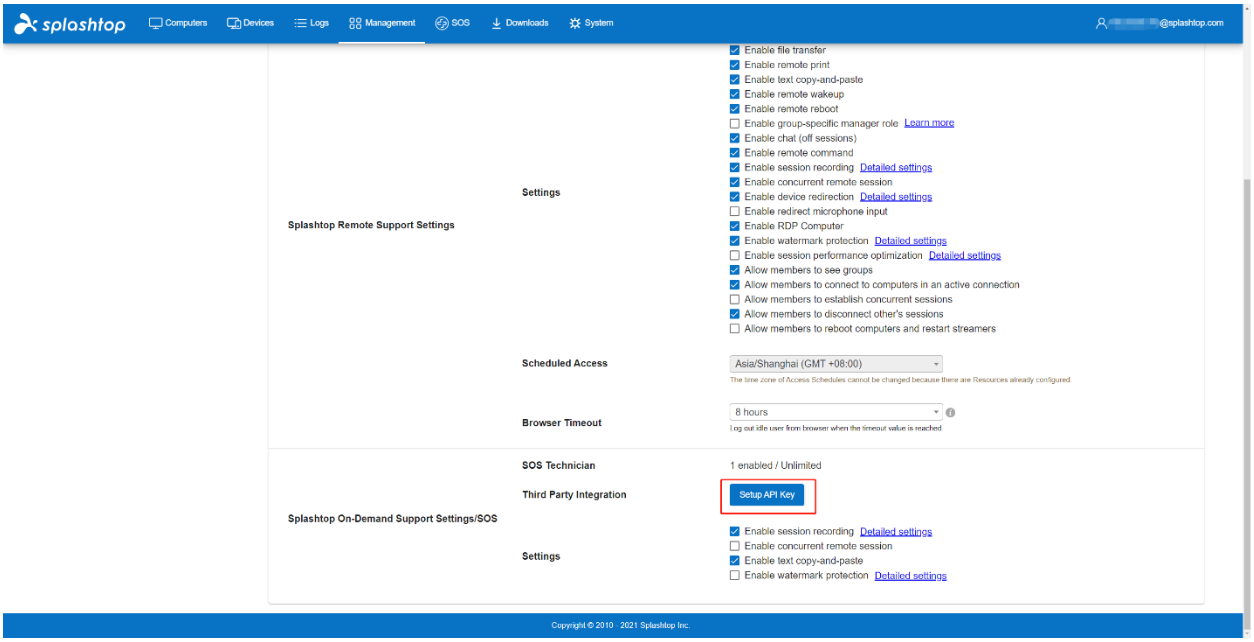
The setup of Splashtop On-Prem - Freshservice Integration is a one-time effort to connect the two systems using an API key. You'll need an administrator account for both Splashtop On-Prem and Freshservice to carry out the task.

Generate API key from Splashtop Gateway

Only a team owner is able to generate API keys from Splashtop Gateway.

Log in to Splashtop Gateway using team owner account, and browse to **Management** > **Team** > **Splashtop On-Demand Support Settings/SOS** > **Third Party Integration**.

Click on the button **Setup API Key**.



Splashtop Remote Support Settings

Settings

- ☑ Enable file transfer
- ☑ Enable remote print
- ☑ Enable text copy-and-paste
- ☑ Enable remote wakeup
- ☑ Enable remote reboot
- ☐ Enable group-specific manager role Learn more
- ☑ Enable chat (off sessions)
- ☑ Enable remote command
- ☑ Enable session recording Detailed settings
- ☑ Enable concurrent remote session
- ☑ Enable device redirection Detailed settings
- ☐ Enable redirect microphone input
- ☑ Enable RDP Computer
- ☑ Enable watermark protection Detailed settings
- ☐ Enable session performance optimization Detailed settings
- ☑ Allow members to see groups
- ☑ Allow members to connect to computers in an active connection
- ☐ Allow members to establish concurrent sessions
- ☑ Allow members to disconnect other's sessions
- ☐ Allow members to reboot computers and restart streamers

Scheduled Access: Asia/Shanghai (GMT +08:00)

The time zone of Access Schedules cannot be changed because there are Resources already configured.

Browser Timeout: 8 hours

Log out idle user from browser when the timeout value is reached

Splashtop On-Demand Support Settings/SOS

SOS Technician: 1 enabled / Unlimited

Third Party Integration: Setup API Key

Settings

- ☑ Enable session recording Detailed settings
- ☐ Enable concurrent remote session
- ☑ Enable text copy-and-paste
- ☐ Enable watermark protection Detailed settings

Copyright © 2010 - 2021 Splashtop Inc.

Support Resources

About this document

This document is provided for information purpose only. Splashtop Inc may change the contents hereof without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose.

About Splashtop On-Prem

Splashtop On-Prem is an on-premise solution that can be totally self-hosted inside enterprise network. With a centralized database and management console, the IT admin could conveniently tackle the system security while providing easy and smooth remote control experience to the users.

Product page: https://www.splashtop.com/on-prem

Technical Support

At Splashtop, we are committed to provide our best technical support to our customers. Looking for more support resources?

Help site: https://support-splashtoponprem.splashtop.com/
Contact us: support-onprem@splashtop.com