Splashtop On-Prem Admin Guide

Apr. 2024

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.

For further details and to trial Splashtop products, visit www.splashtop.com.

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!

Microphone passthrough: With microphone passthrough, you can redirect your microphone input on your local computer to the remote computer as if you were sitting directly at the remote computer. This enables you to join calls over Skype, Teams, Zoom, VoIP, etc. and also use voice dictation or recording software over the remote session.

USB device redirection: With device redirection, you can redirect a USB device 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.

and more...

Refer to online support site to learn more about new product features.

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)

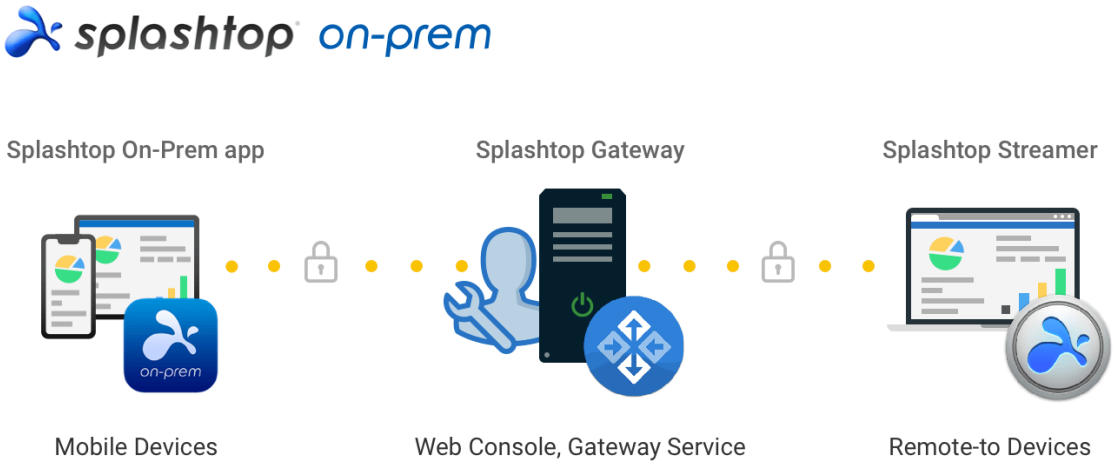
ATTENDED SUPPORT is a perfect solution for Service Desks and MSPs, and it provides the most convenient way for a technician to establish an ad-hoc remote session, without needing the end user to install any software or plug-in in the computer. Instead, the end user just downloads and launches a standalone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

Please always refer to Annoucements & Downloads to get the latest version of the system.

System Requirements

Requirements for Splashtop Gateway Server

- **Operating System** (64-bit version)
  - Windows Server 2022
  - Windows Server 2019
  - Windows Server 2016
  - Windows 11
  - Windows 10
- **Software**
  - Run with Administrator privilege.
- **Minimum Hardware Spec (less than 100 concurrent sessions without centralized session recording)**

  - Processor: 8 Cores or above
  - Memory: 16GB or above
  - SSD or HDD: 60GB or above on installed drive (Gateway installed on a Solid-state drive is recommended)
- Minimum **Hardware Spec (more than 100 concurrent sessions + centralized session recording)**
  - Processor: 16 cores or above
  - Memory: 64GB or above
  - SSD: 80GB or above on installed drive

Requirements for Browser type

  - Google Chrome
  - Safari
  - Edge
  - Firefox

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
  - Chromebook
- **Windows**
  - Windows XP*, Vista*, 7, 8, 10, or 11
- **Mac**
  - macOS 10.10 or higher

*Windows XP/Vista, Windows Server 2003, and Android 4.0 are not supported if TLS 1.0 and 1.1 are disabled (TLS 1.2 only) from Gateway Security tab.

Requirements for Streamer Devices

- Operating System
    - Windows 11
    - Windows 10
    - Windows 8/8.1
    - Windows 7
    - Windows Server 2022
    - Windows Server 2019
    - Windows Server 2016
    - Windows Server 2012
    - Mac OS 10.10 or higher
    - Android 5.0 or higher
    - iOS 12.x or higher (for SOS on-prem)
    - Linux
        - Ubuntu desktop 16.04 and 18.04
        - CentOS 7 and 8
        - Red Hat Enterprise Linux (RHEL) 7.3-8.1
        - Fedora 29-31

    - iOS 12.x or higher (for SOS on-prem)
    - Linux
        - Ubuntu desktop 16.04 and 18.04
        - CentOS 7 and 8
        - Red Hat Enterpr
        - Fedora 29-31
- **Hardware**
    - Processor: 1.6 GHz or faster dual-core CPU
    - Memory: 2 GB or above
    - Network connection

*Windows XP/Vista, Windows Server 2003, and Android 4.0 are not supported if TLS 1.0 and 1.1 are disabled (TLS 1.2 only) from Gateway Security tab.

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.

In addition, the following Ports should not be occupied as they are used by Gateway on the local machine.

- 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

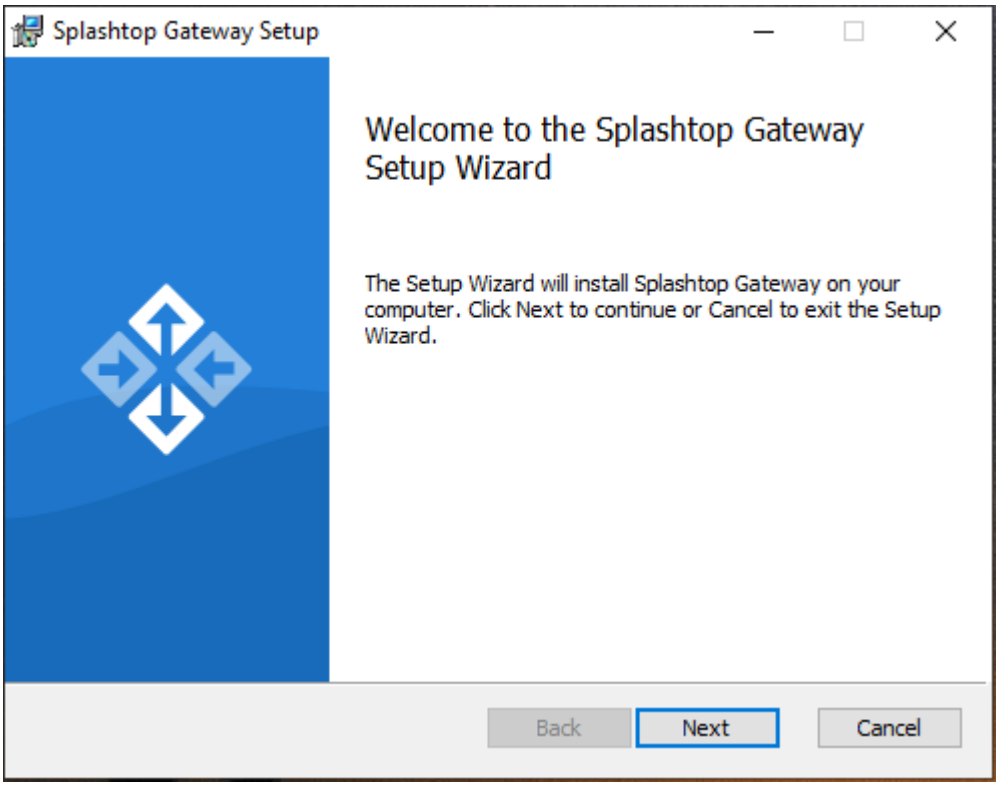
1. Team Owner sets up Splashtop Gateway on the company network.

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.

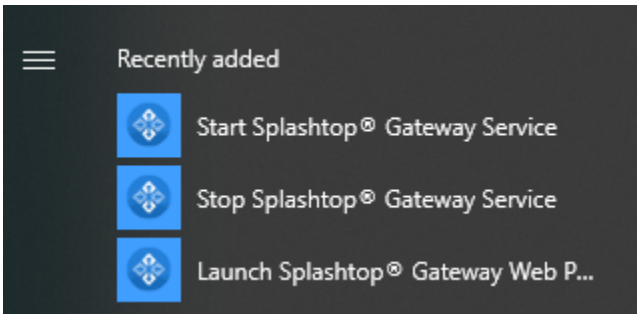
Splashtop Gateway and Splashtop Steamer can be installed on the same Windows server. In fact, it is a good practice since remote access to that server can be provided in case Team Owner needs to configure Splashtop Gateway settings or restart the Splashtop Gateway service.

1. Install Splashtop Gateway

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



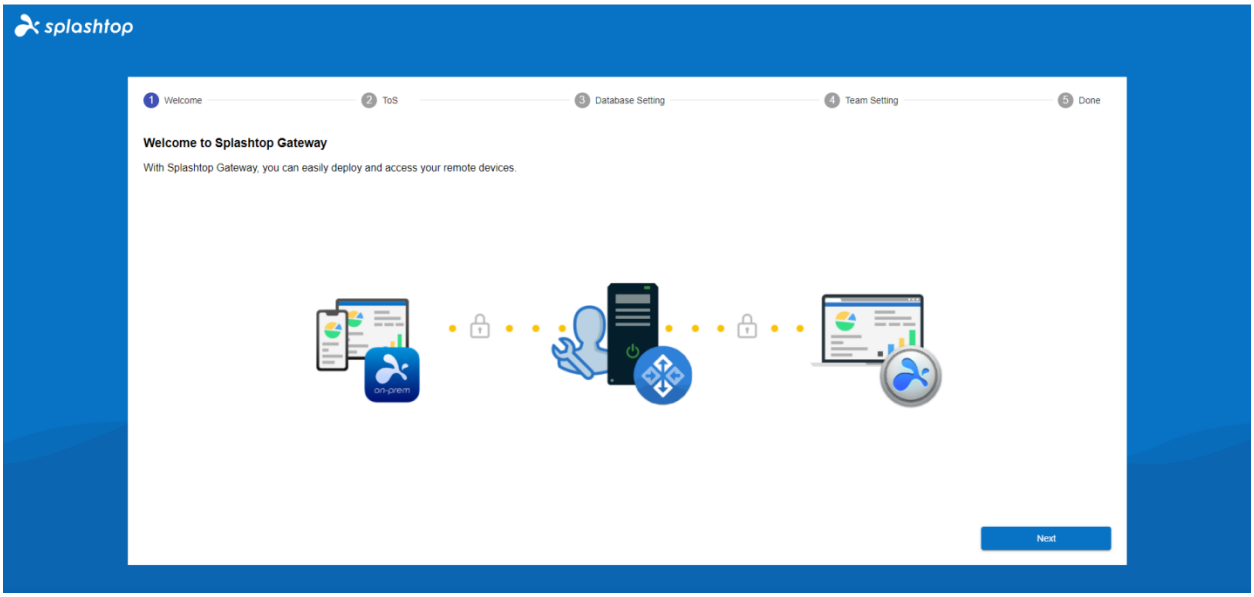
b) After the installation finished, go to Windows Startup menu in which 3 startup shortcuts just created. Click Launch Splashtop Gateway web portal to start gateway web console in your default browser.



Note: We highly recommend using **modern browsers (Google Chrome, new Microsoft Edge, Safari, Firefox, etc)** to navigate Splashtop Gateway web console.

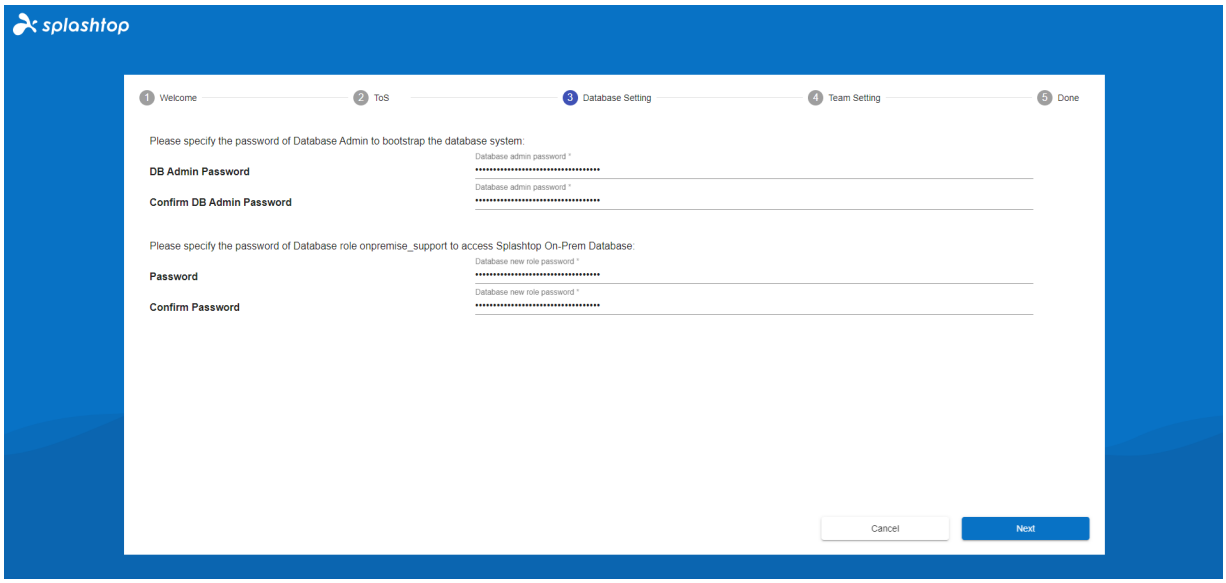
2. Splashtop Gateway OOBE Setup

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.

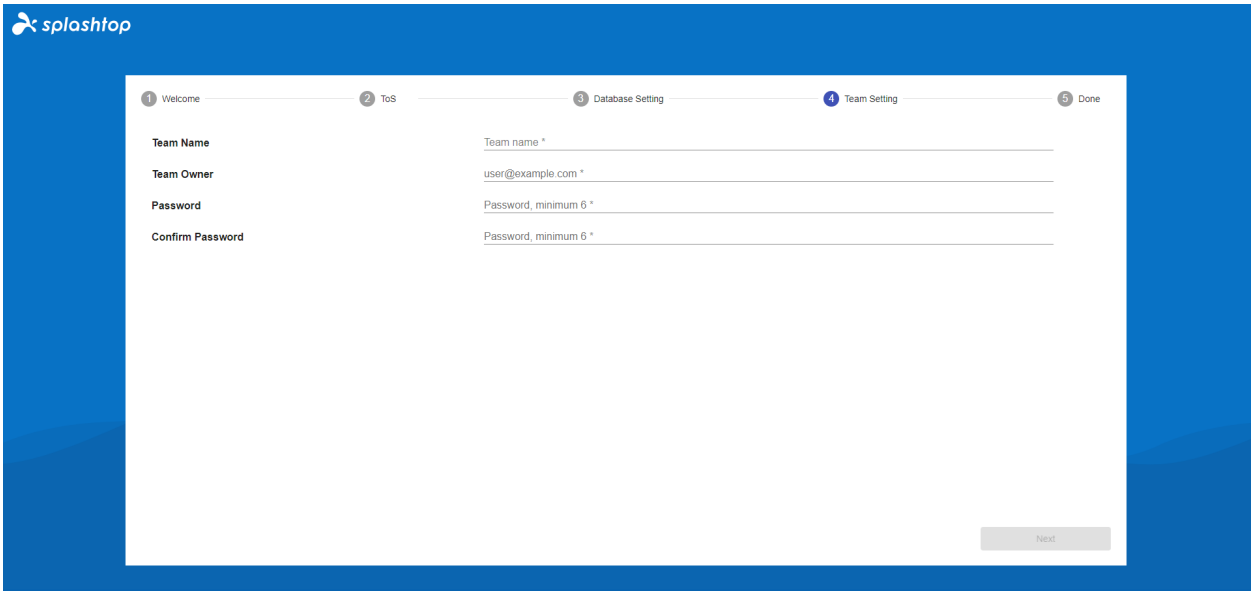


b) Set up your Splashtop Gateway Database management and access passwords. Please allow 30 seconds for Database initializing at this step.

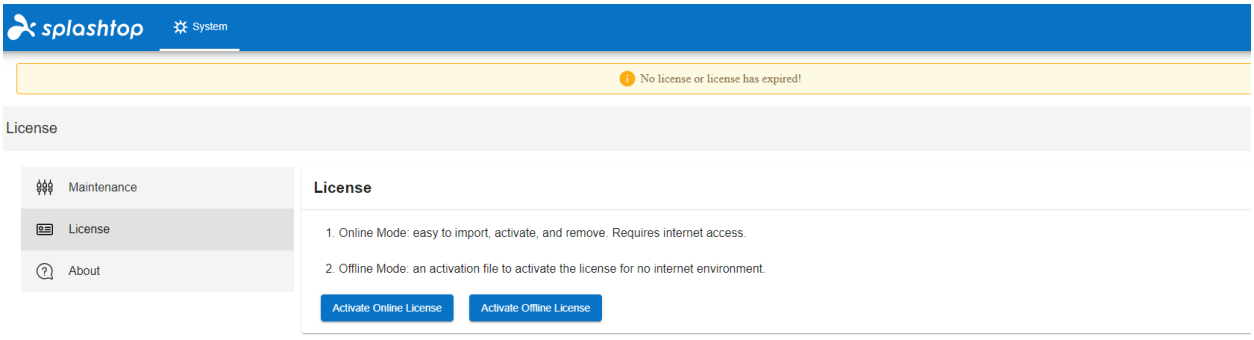
Note: Please write down your Database passwords and saved in a secured place since there will be no way to change DB passwords later on.



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

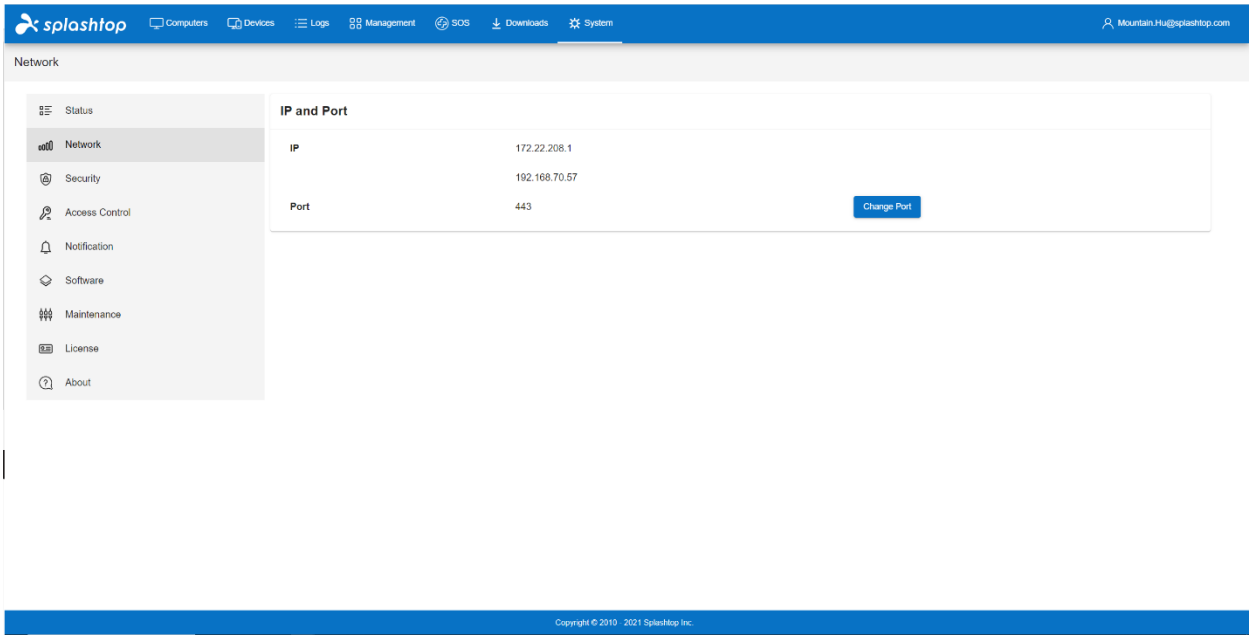


d) Once OOBE setup completed, log in to web console with the credentials just created. You will need to activate online or offline license based on license mode tailored for you. (See Section 3)



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**.



3. Activate Splashtop Gateway via License

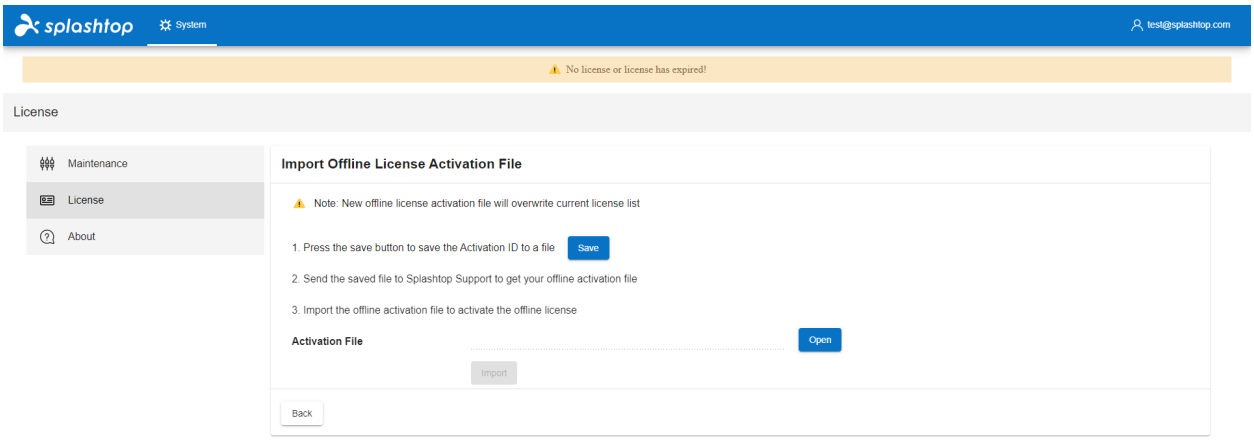
Splashtop Gateway **must** be activated by a valid license to use.

> **Note:** Please reach out to Splashtop Sales or Splashtop Support to request for trial license or obtain purchased license.

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)

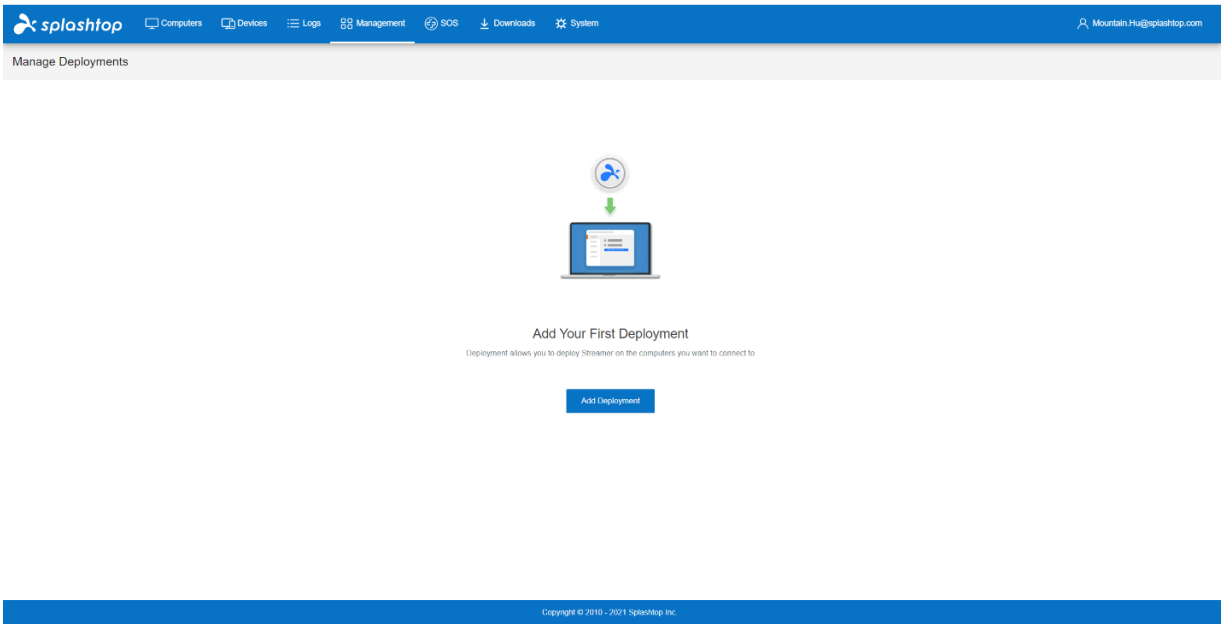


4. Deploy Splashtop Streamer

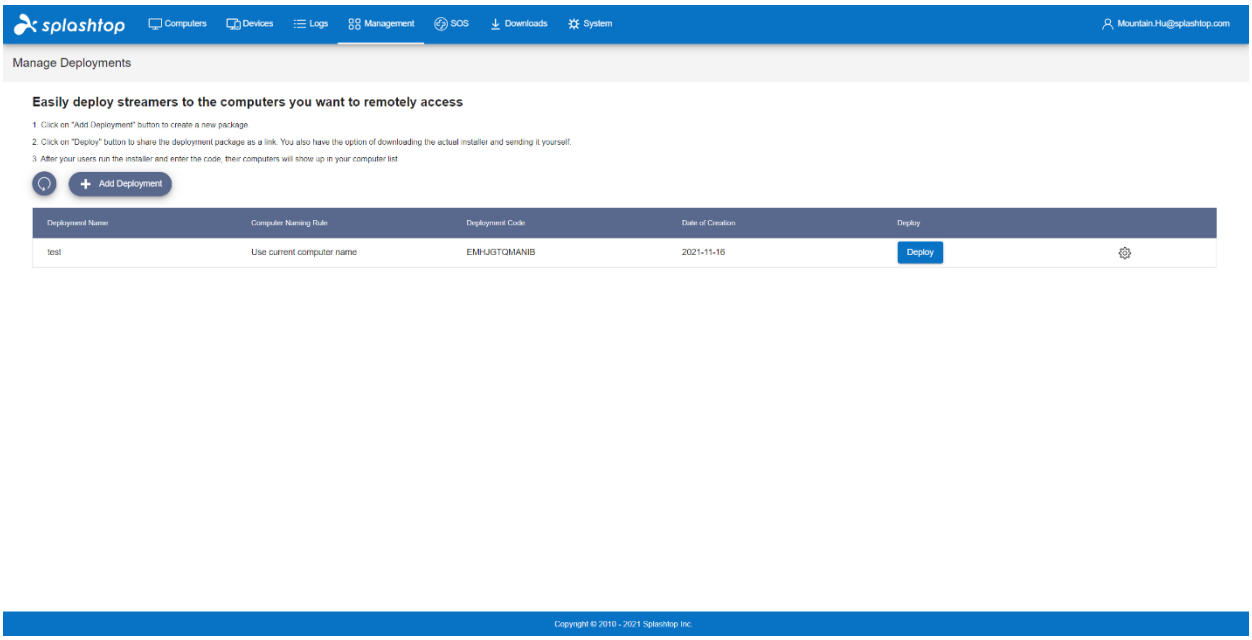
Below instruction taking deploy Splashtop Streamer on Windows as an example, for more deploy info please refers to Deployment related support articles.

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.

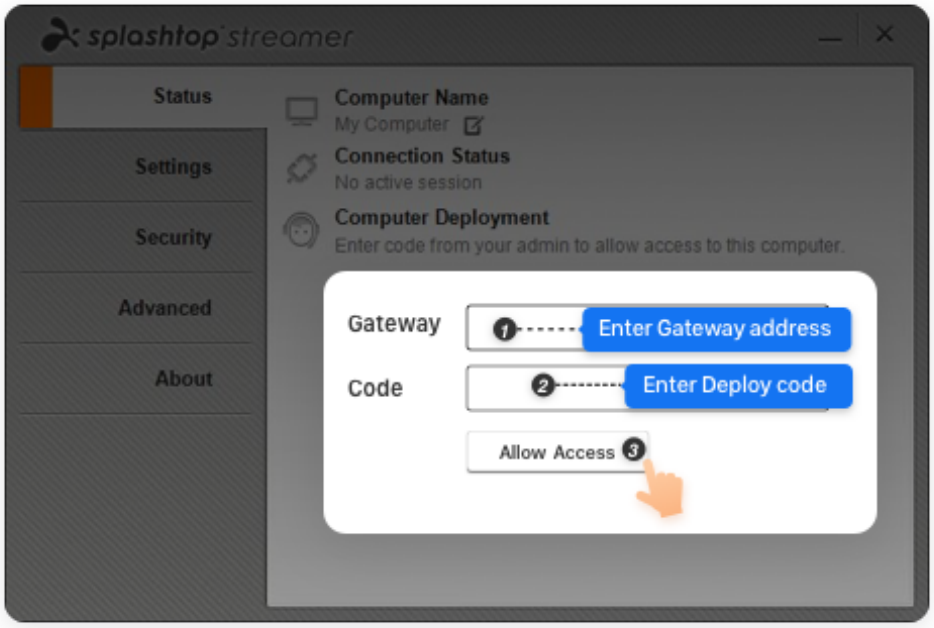


2. Select ***Deploy*** for the package that was just created.



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.

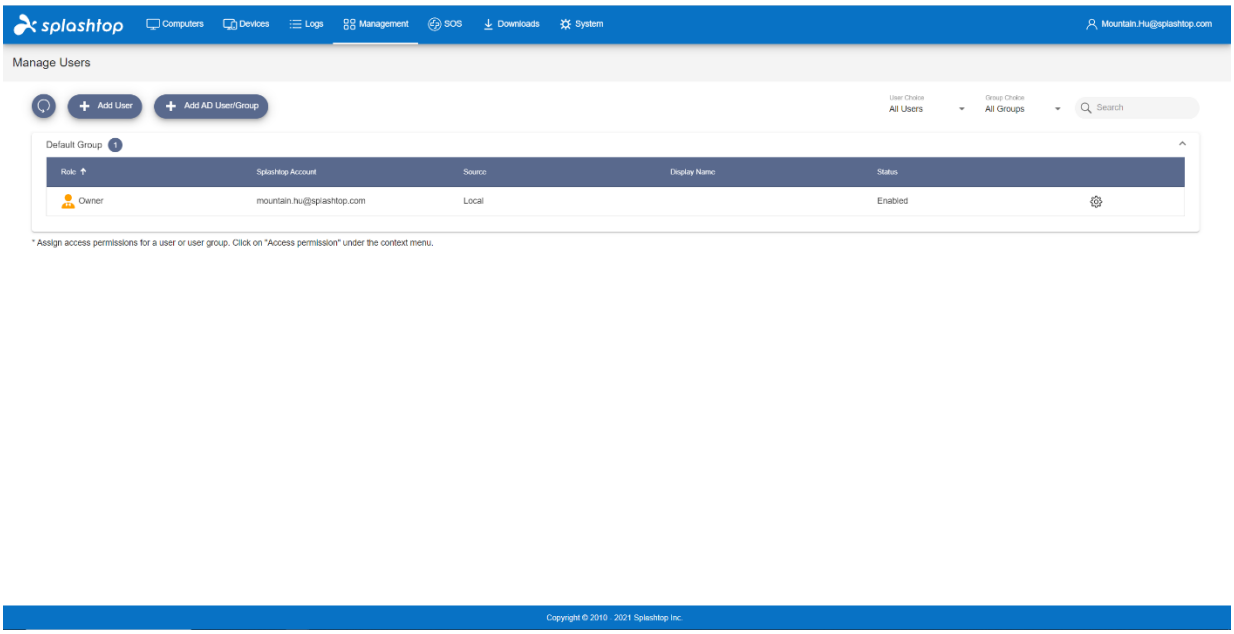


5. Create user accounts

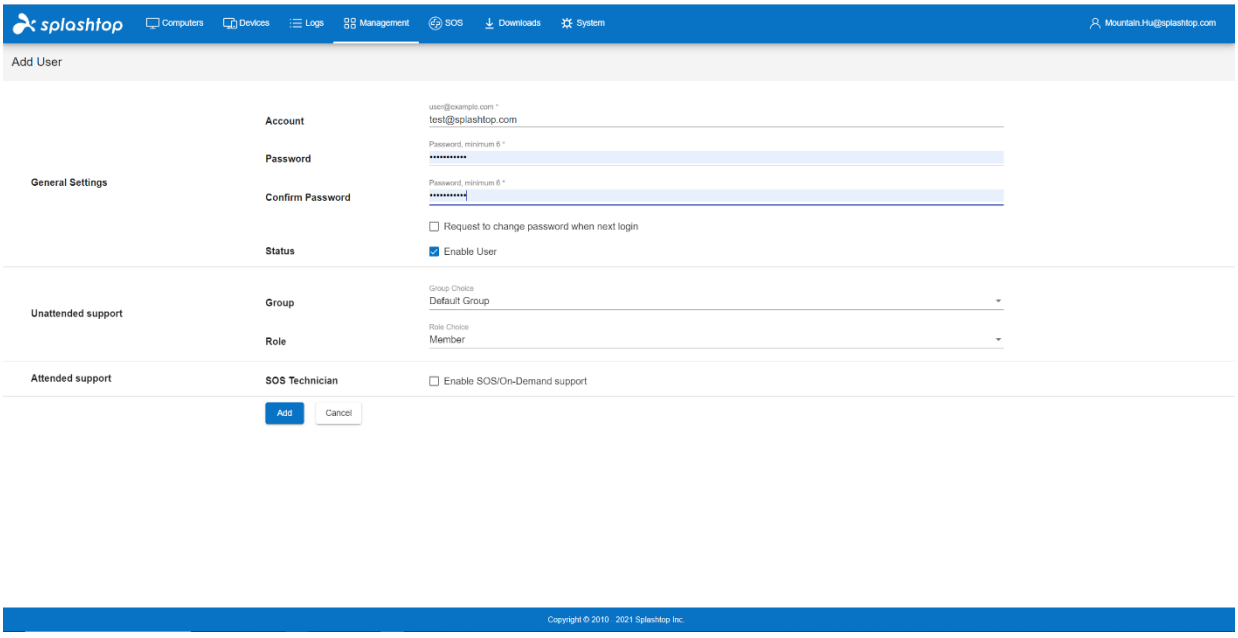
Create Remote Support / Remote Access users

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

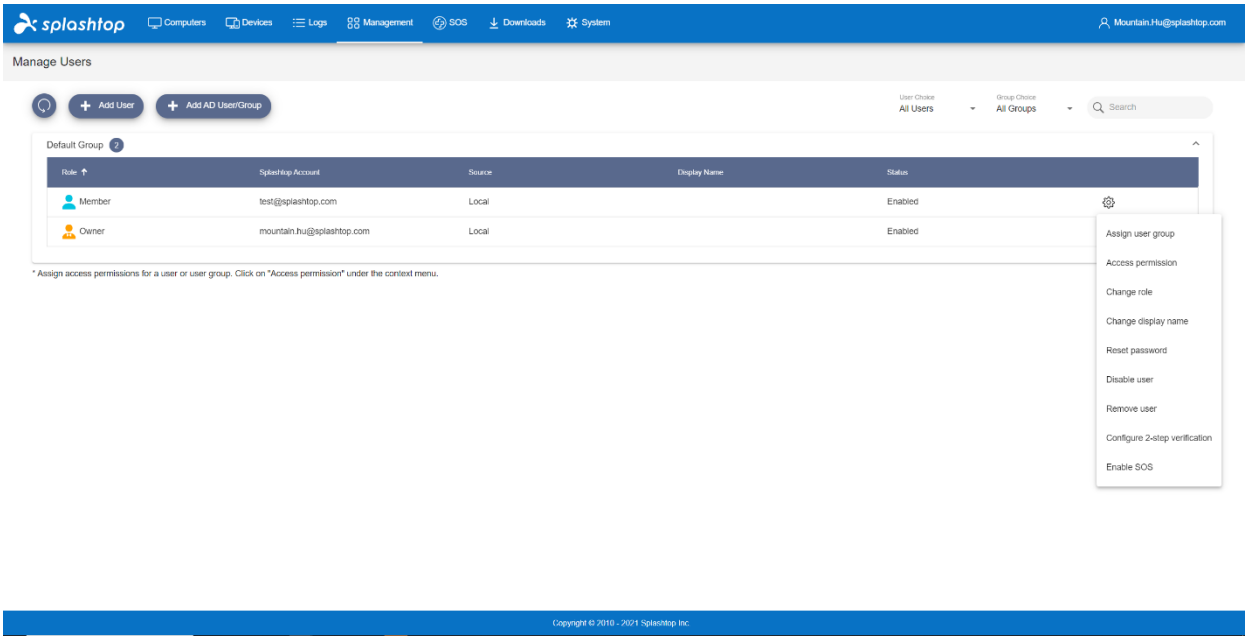
1. Go to Splashtop Gateway Web Console > Management > Users. Press +***Add User button*** to create a new user.



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

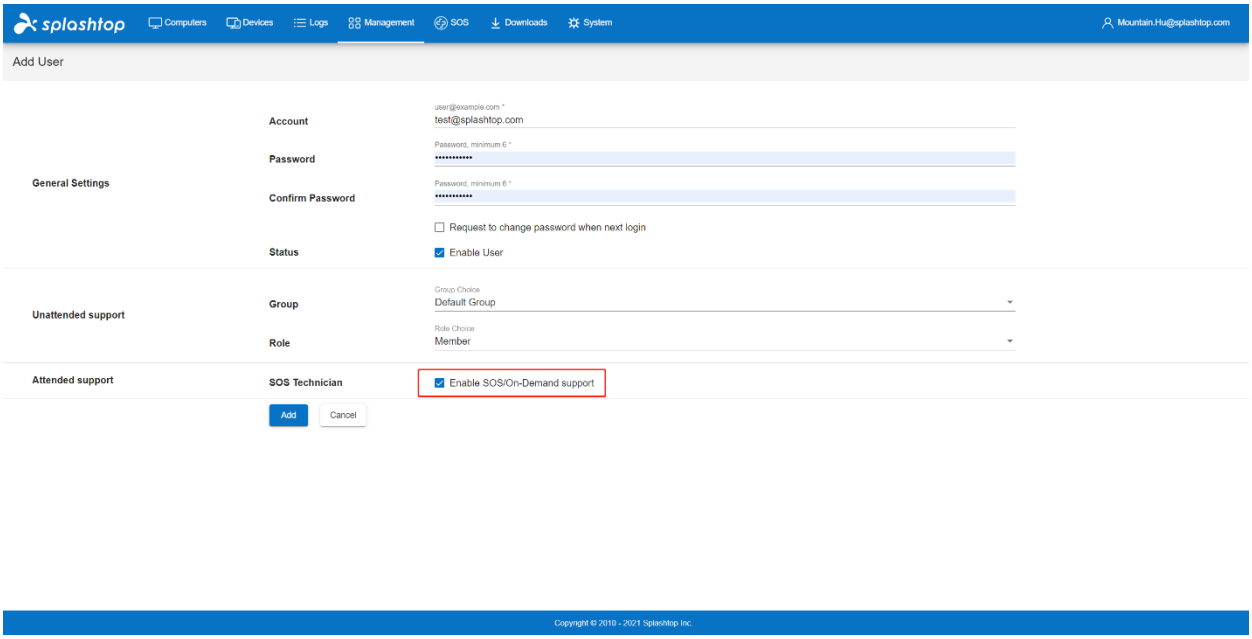


3. Team Owner or Team Admin can assign user access permission to specific devices or groups by clicking Access Permission from context drop-down menu (Gear Button).

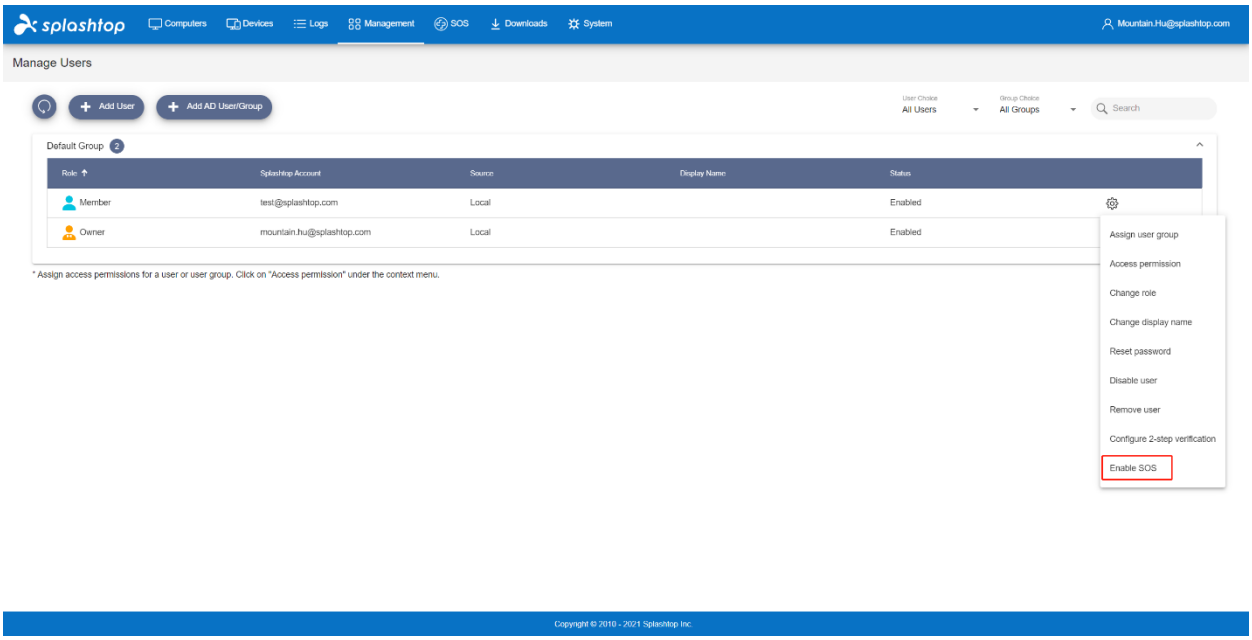


Create users with additional On-Demand Support/SOS capability

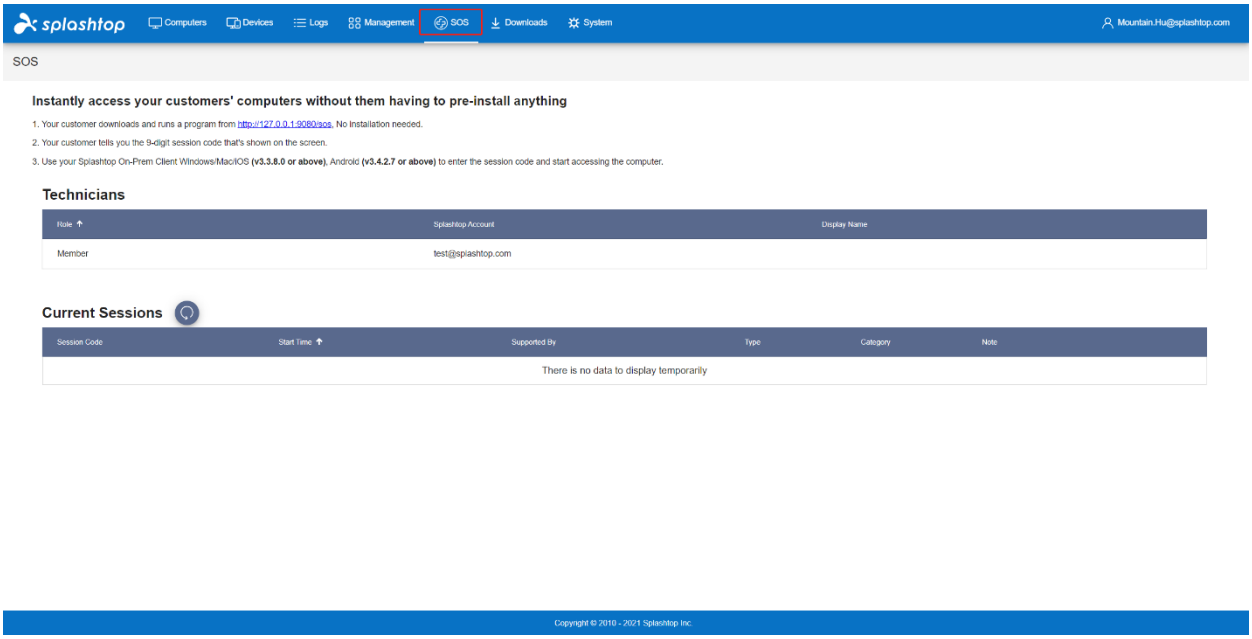
a) Team owner or admin can enable a user's SOS capability either from user creation page or user's property drop-down.



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

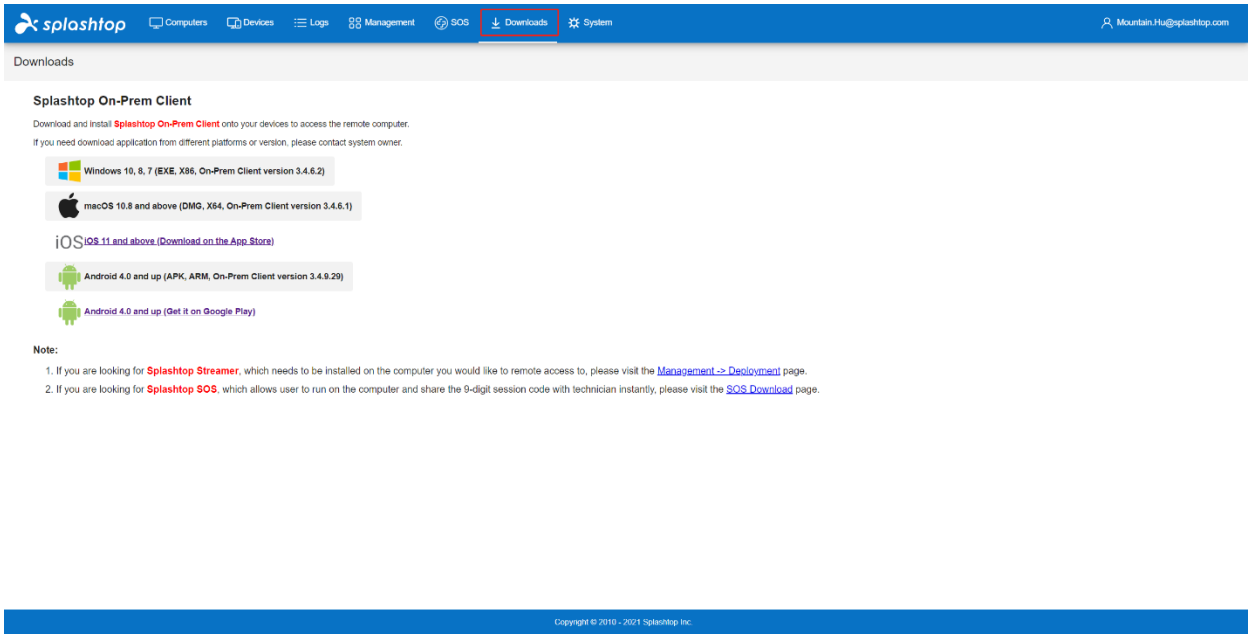


c) Users with SOS capability can be found in the SOS page on web portal.

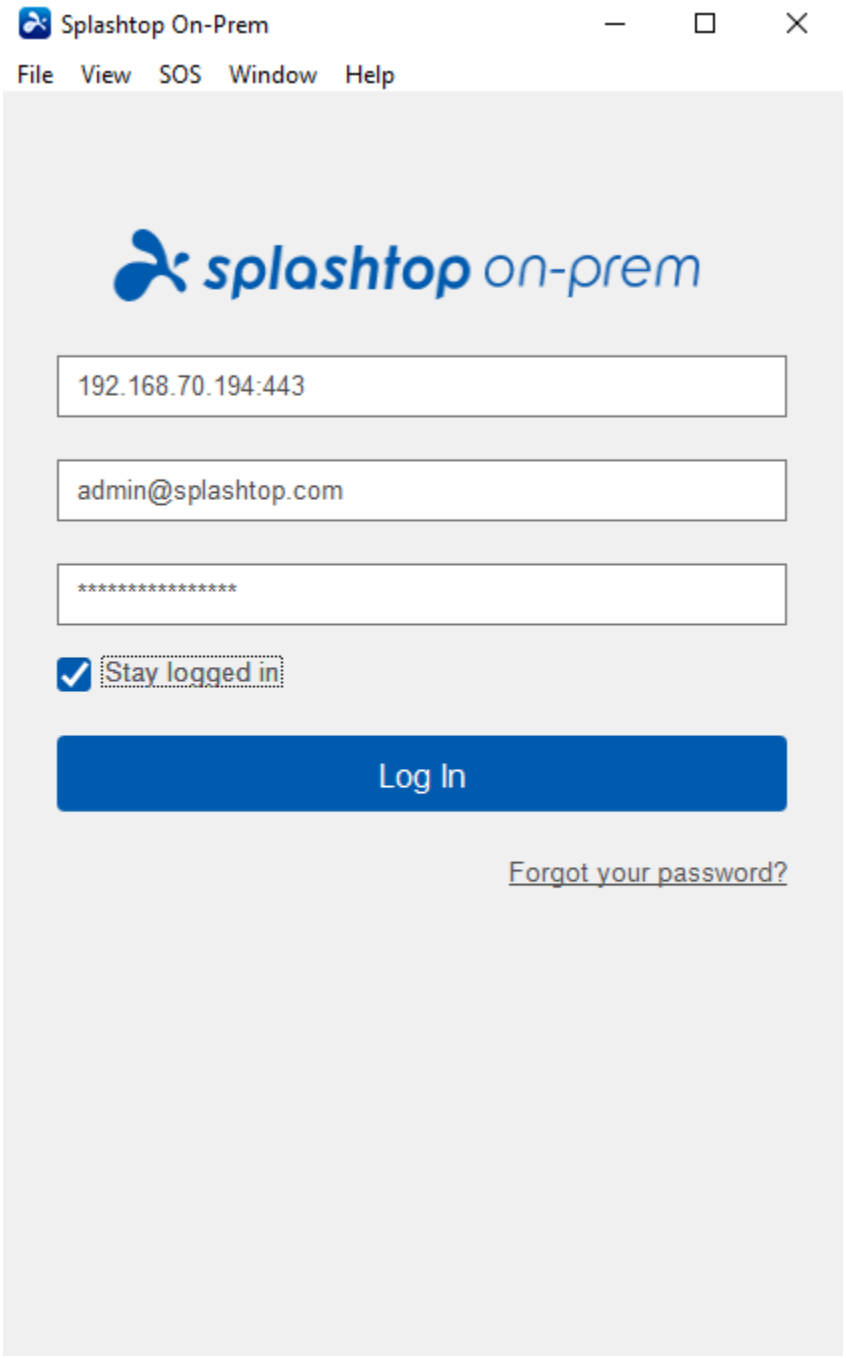


6. Install client app and access

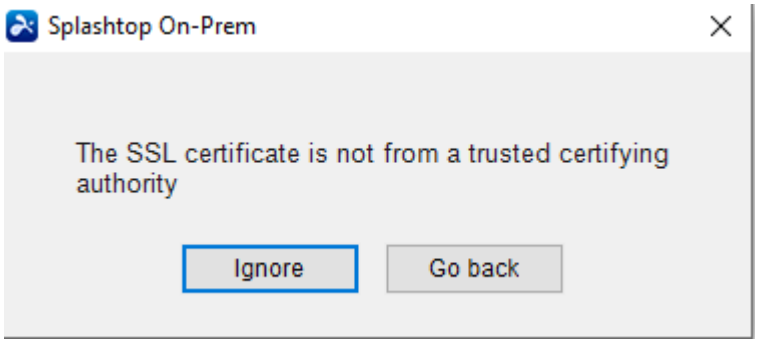
1. Users assigned as a Member can only browser limited content when log in to Splashtop Gateway web console compared to Team Owner or Team Admin as shown in below screenshot. Member can log in Splashtop Gateway Web Console and download the latest Splashtop On-Prem Client via Downloads menu tab and Install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



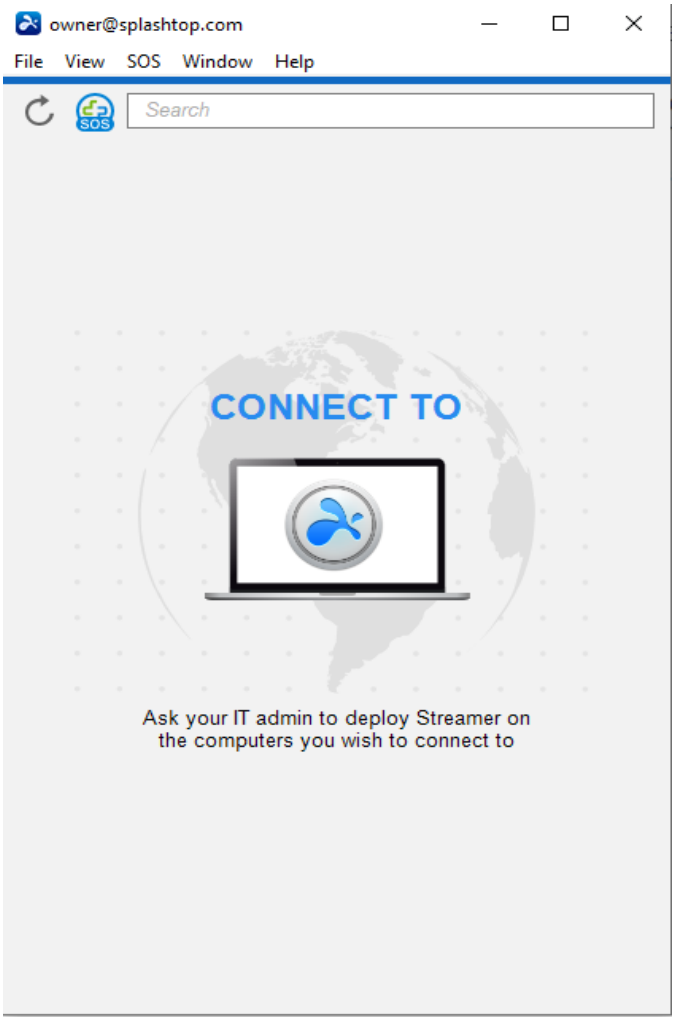
2. When **Splashtop On-Prem client app** installed, user simply inputs the Splashtop **Gateway server's IP address or FQDN** with default port number **443**, the account name and password obtained from Team Owner or Admin to log in. Users with no such information will need to consult Team owner or Admin.



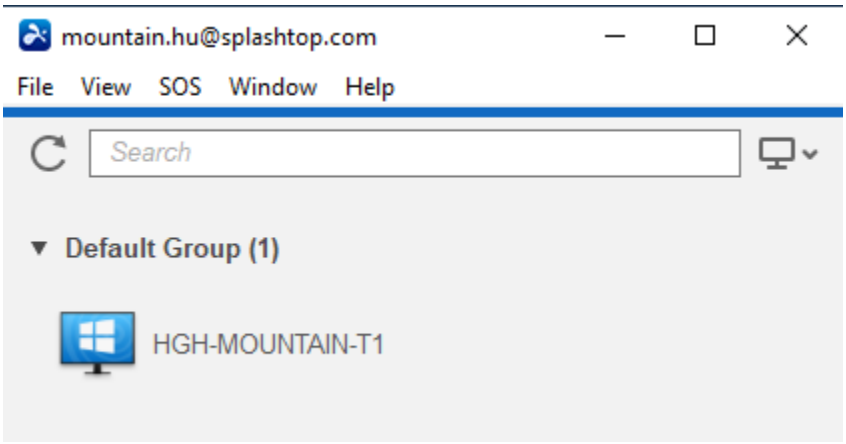
3. If a warning message pops up when you tap **Log In**, stating the SSL certificate is not from a trusted certifying authority, it is likely that the SSL certificate is self-generated, and you can choose to ignore it. However, we recommend that users who have encountered this message popping up should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



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.



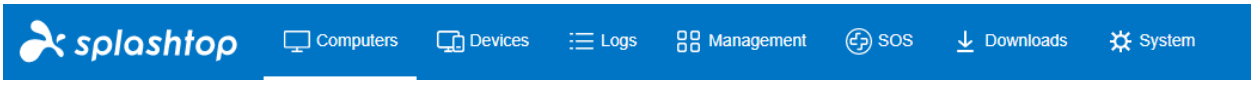
5. Below Screenshot reveals one specific Windows PC has been successfully deployed so that the user is able to remote access to this device by clicking **connect** button to the right or double clicking the blueish field.



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.



Entry	Team Owner	Team Admin	Member
Computers	✓	✓	✓
Devices	✓	✓	✓
Logs	✓	✓	✓ (1)
Management	✓	✓	
SOS	✓	✓	✓ (2)
Downloads	✓	✓	✓
System	✓		
User profile	✓	✓	✓

Note:
(1) For members, only its own logs is visible
(2) SOS page is visible to a user when SOS feature is enabled on it

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 or FQDN):(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

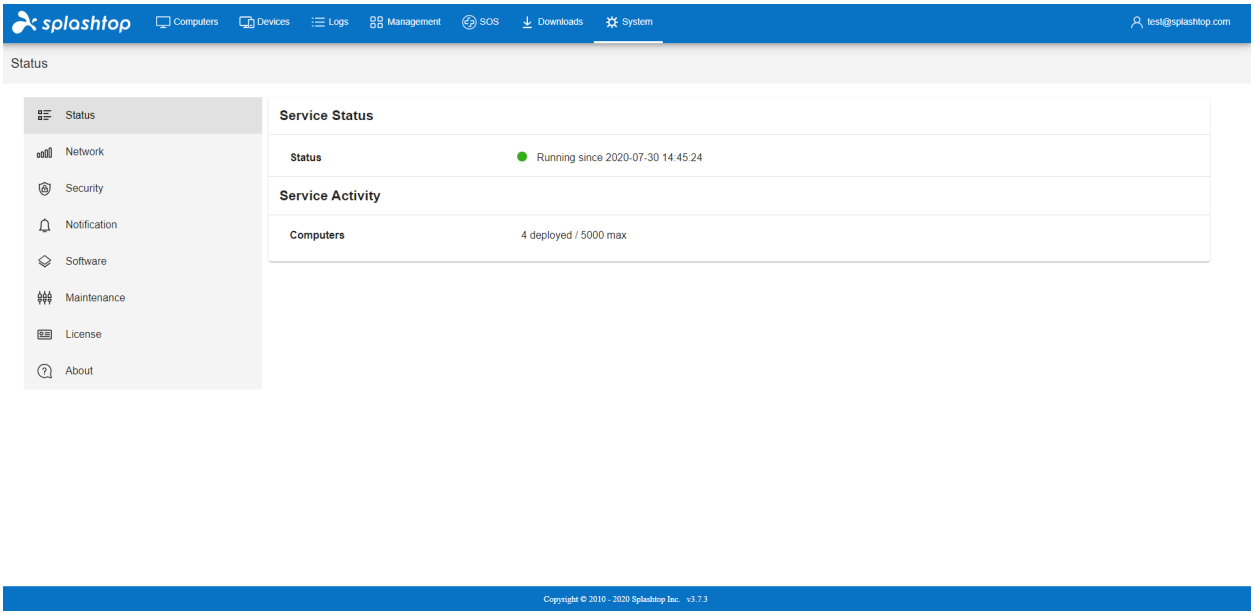
By default, Splashtop On-Prem makes use of Port number 443, but you can change the port number following instructions in the article below:

System Configuration

Introduction

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

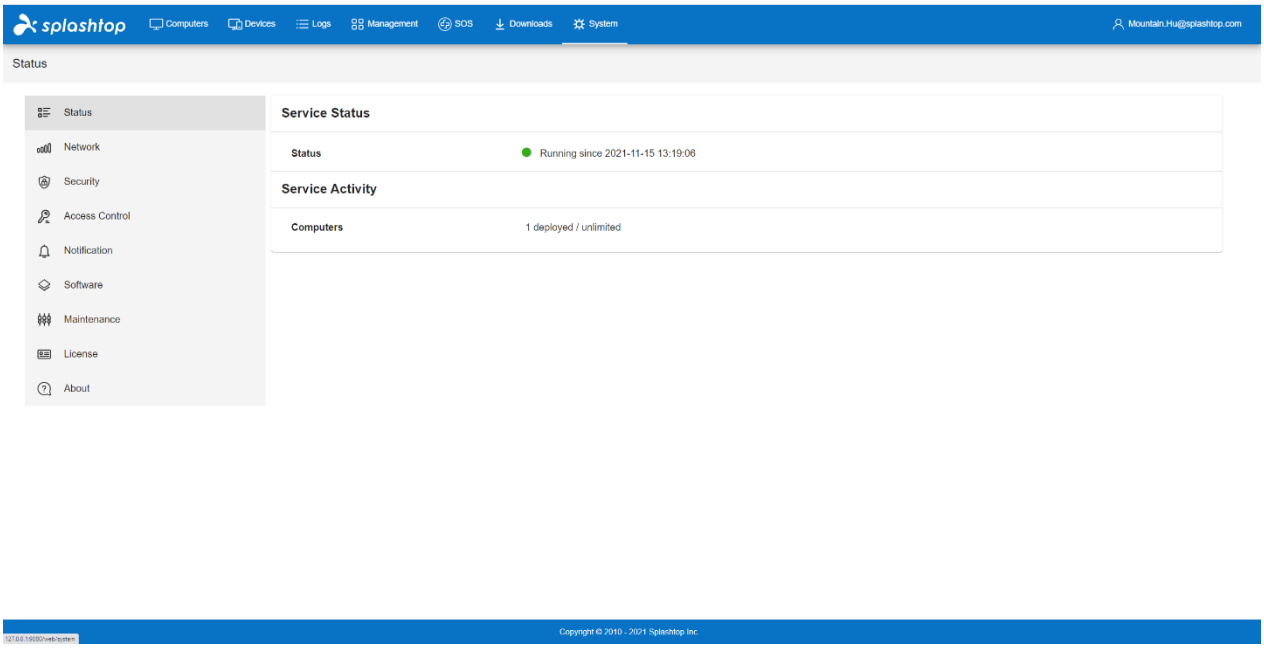
Log in as Team Owner, you will see **System tab** on the top menu bar, click it to enter system settings.



- **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

Status



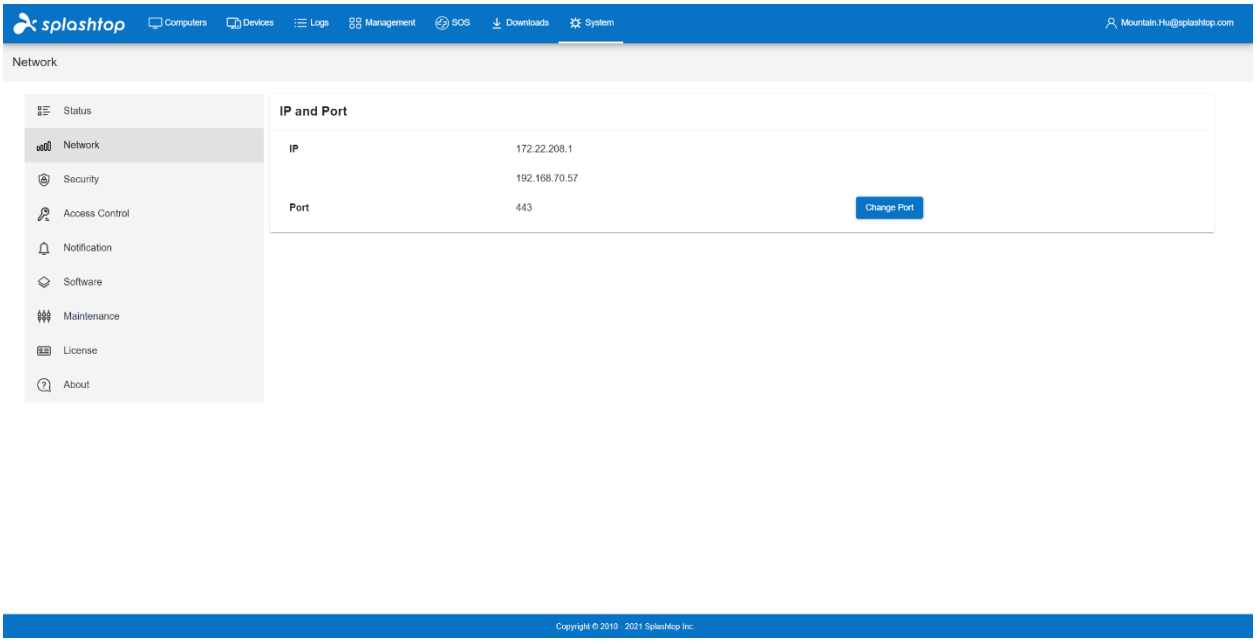
The status page is a summary of the Splashtop Gateway service. It shows:

- **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

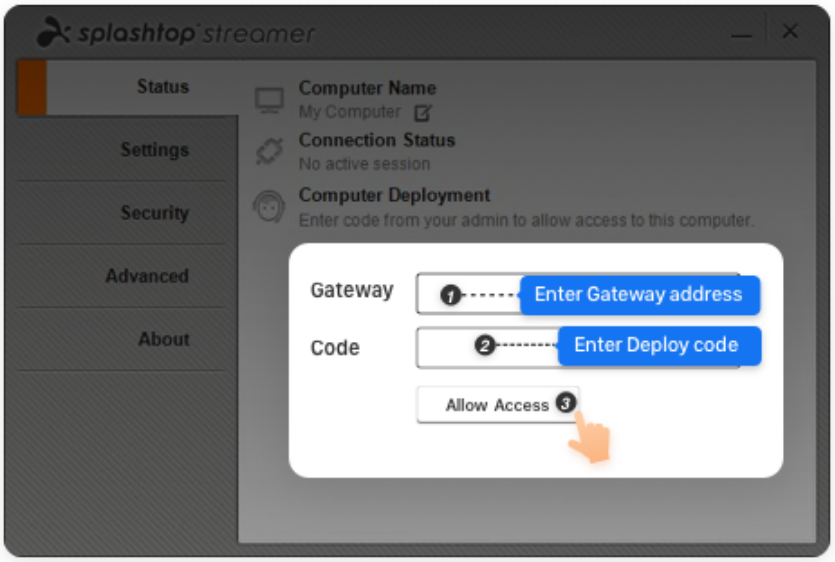
Log in to Gateway's management console with the Team Owner, go to **System** > **Network**, the **Port** section shows the port that Gateway is currently serving, click **Change Port** will allow user to input a new port and apply.



Notice:

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

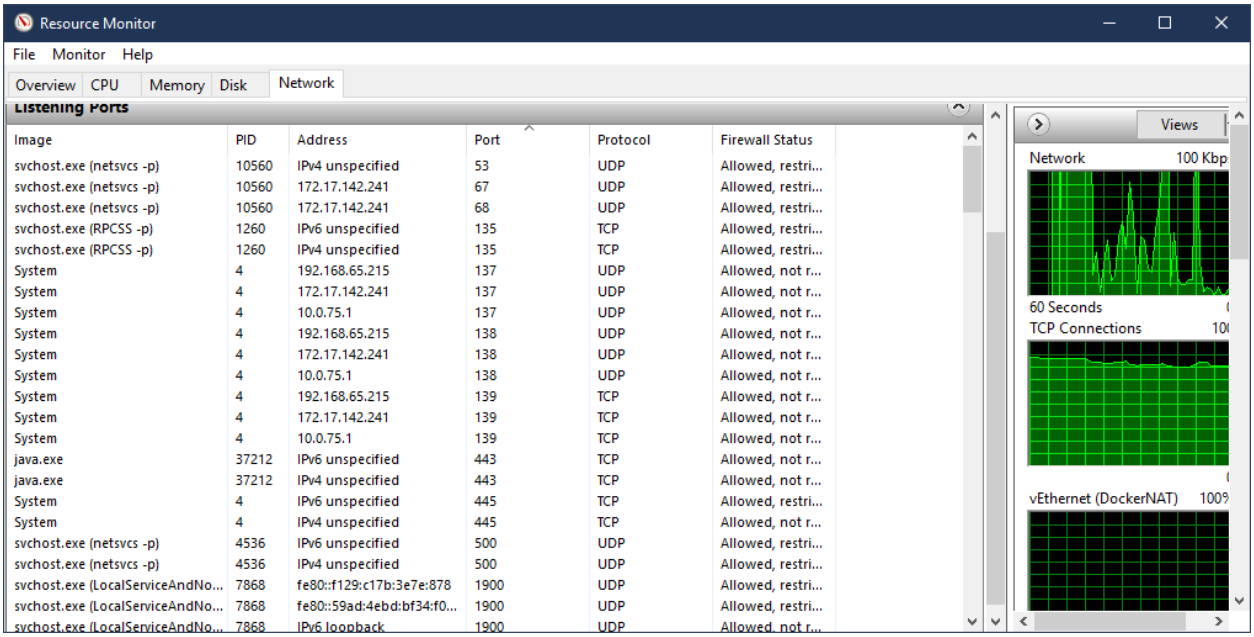
2. If you already have Streamer deployed or On-Prem app logged in, these Streamers and On-Prem apps will be logged off, due to the port change, you need to specify the correct *IP:Port* in the Streamer and On-Prem app side to log into the Gateway again. 443 is the default port, which can be ignored when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



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

(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.



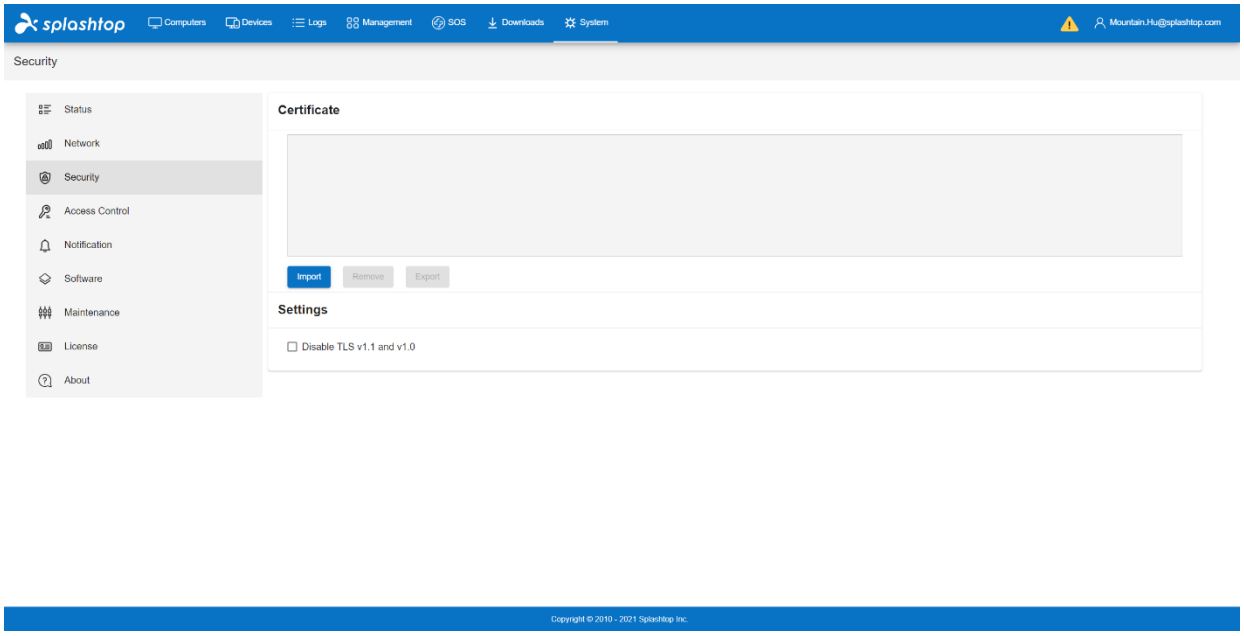
Security

Import SSL Certificate

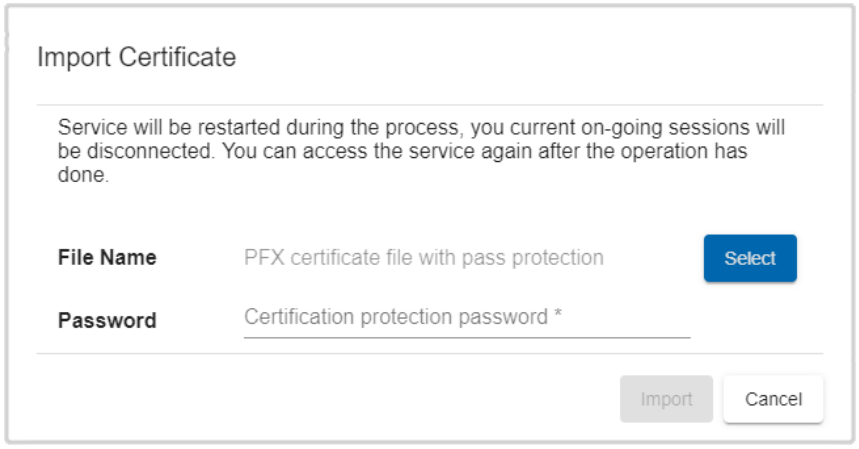
Splashtop Gateway supports importing your own certificate, which can be self-signed certificate, or certificate issued by 3rd party authority.

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.



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.



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:

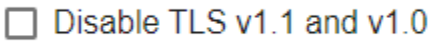
When creating PFX, the middle/intermediate layer CA cert must be included. If the PFX does not contain the direct issuer's CA, issues may be seen from portable OS.

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

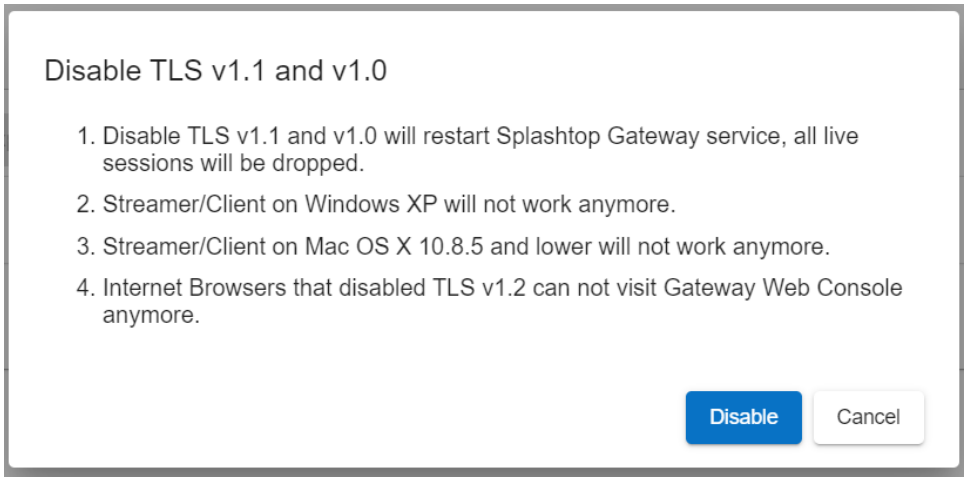
Disable TLS 1.1 and 1.0

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



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.



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:

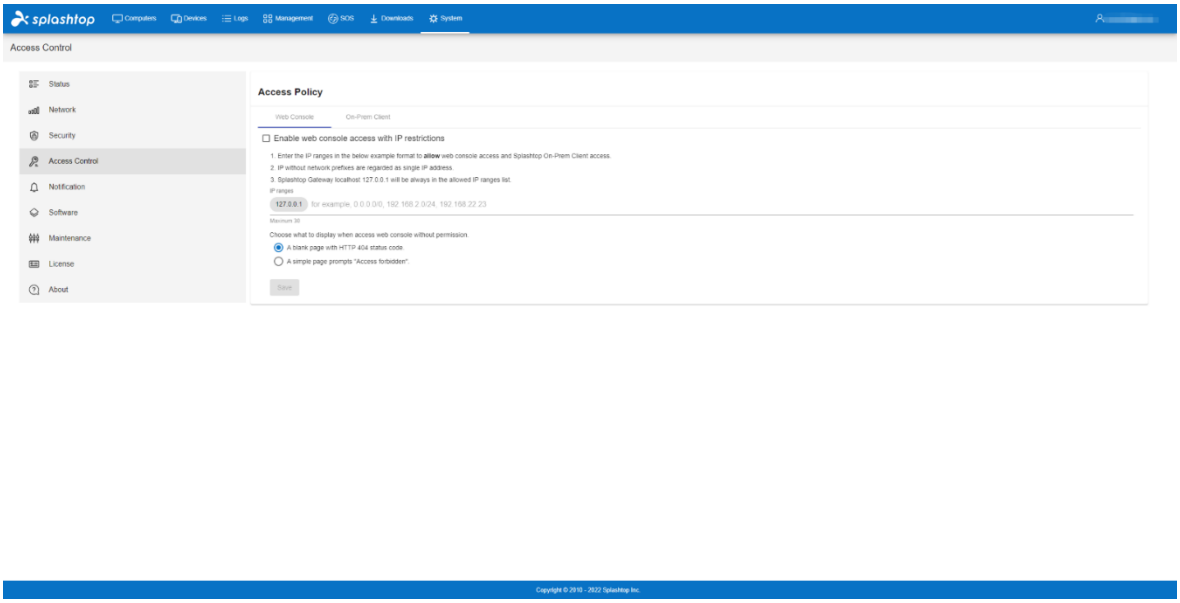
1. Windows XP uses SSL v3 by default for WinHTTP. Windows 8 or later uses TLS 1.1 for WinHTTP by default.

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

Reference Article: Microsoft Support

Access Control

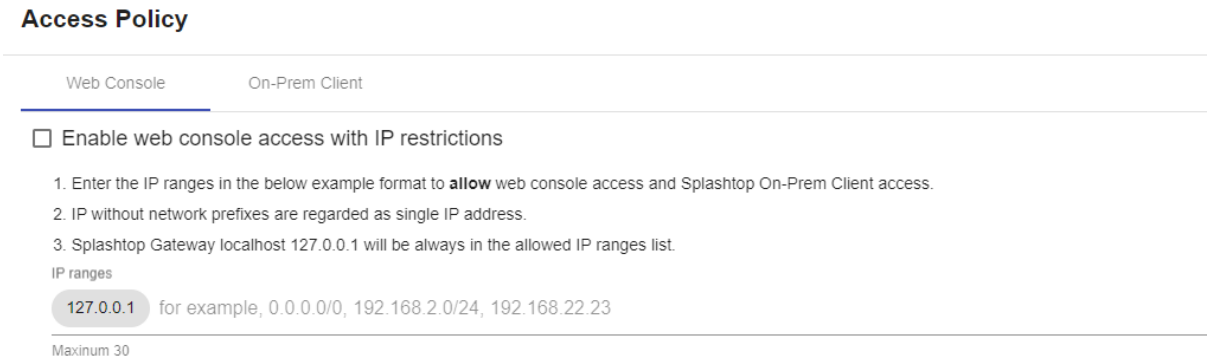
The access control page allows an Owner to manage the web console access and Splashtop On-Prem client access with IP restriction.



Step 1

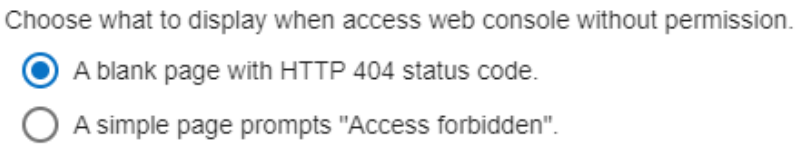
Log into Gateway's management console as Owner, go to System > Access Control. Splashtop currently supports IP restrction on the access to Gateway web console or On-Prem client app.

Filled up the allowed IP addresses into IP range list. The IP syntax should be in CIDR.



Step 2

In addition, owner can choose different display methods for web console access denied.



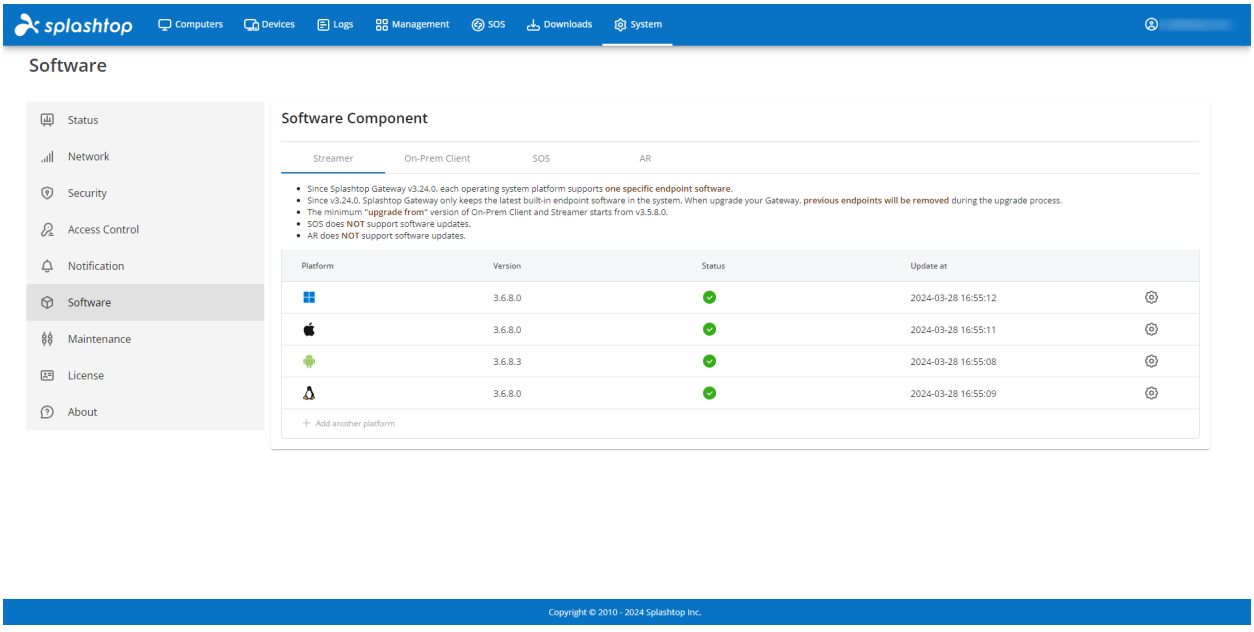
Step 3

Enable IP access restrictions for Splashtop On-Prem Client or Web Console so that access generated from IP sources excluded from the list will be blocked.

Click Save button to save the settings and turn on the feature.

Software

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



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.

Software Updates

1. Introduction

Splahtop Gateway (v3.24.0 or higher) server initiated update involves a built-in update repository loaded with the latest Splashtop endpoints software and also controls the distribution and deployment of software updates to your client devices (Windows, Mac and Linux) based on customized schedule. This architecture facilitates centralized management and deployment of updates, offering flexible control and better security to meet your special maintenance needs.

2. Requirements

- *Splashtop Gateway* **v3.24.0** or higher
- *Splashtop Streamer* and *On-Prem Client app* **v3.5.8.3** or higher.
    - v3.5.8.3 is the default version for Windows and Mac endpoints that packed into Gateway v3.24.0
    - v3.5.8.3 serves the first "upgrade from" version. Endpoints software version lower than v3.5.8.3 does **NOT** support upgrades.

Important: Upgrade Gateway behavior changes

1. After upgrade your Splahtop Gateway to v3.24.0, all previous client app/Streamer version **lower than v3.5.8.3 will be removed and replaced by v3.5.8.3**. The server will maintain only to the latest software suite at a given version.

For example, after an upgrade of Gateway from v3.20.x to v3.24.0, the v3.5.2.x packed in the Gateway v3.20.x will be replaced by v3.5.8.x in v3.24.0.

Below are the default endpoints version in the last 4 major releases of Splashtop Gateway.

Gateway v3.16.x -> Default Endpoints v3.4.8.x

Gateway v3.18.x -> Default Endpoints v3.5.0.x

Gateway v3.20.x -> Default Endpoints v3.5.2.x

Gateway v3.24.x -> Default Endpoints v3.5.8.x

Gateway v3.26.x -> Default Endpoints v3.5.8.x

Gateway v3.28.x -> Default Endpoints v3.6.8.x

2. When back up your Splashtop Gateway v3.24.0, the endpoints will **no longer** to be included in the backup file. As Splahtop continues to introduce new compatible platforms for the upmost cross-platform expericence, the maintenance process should not be comprised by the ever increasing package size.

3. Endpoints software feature scope

Splashtop On-Prem Client

Platform	Supported Since
Windows	v3.5.8.3 (Supports check for updates manually or automatically)
macOS	v3.5.8.3 (Supports check for updates manually or automatically)
Android	Not supported. (Get new apps from Google Play)
iOS	Not supported. (Get new apps from App Store)
Linux	Not supported.

Splashtop Streamer

Platform	Supported Since
Windows	v3.5.8.3 (Supports silent update and check for updates)
macOS	v3.5.8.3 (Supports silent update and check fo updates)

Android	Not supported. (Get new apps from Google Play)
Linux	v3.5.8.3 (Supports silent update and check fo updates)

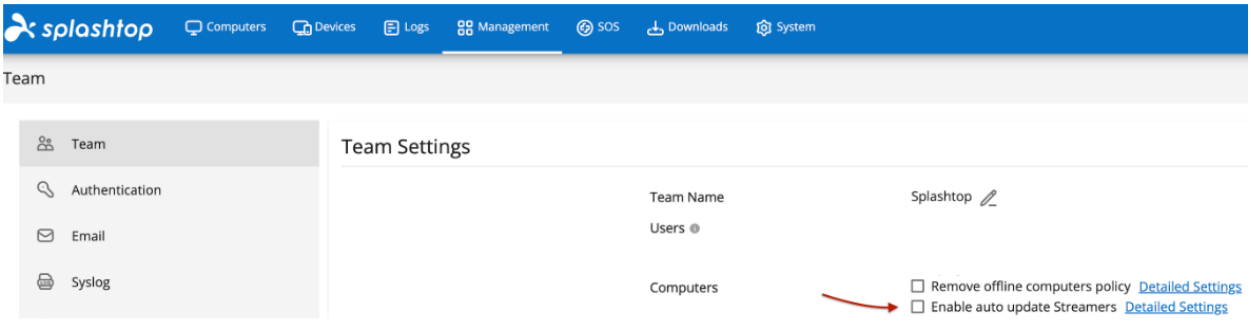
** Splashtop SOS and AR do NOT support updates from Splashtop Gateway.*

4. Update Management

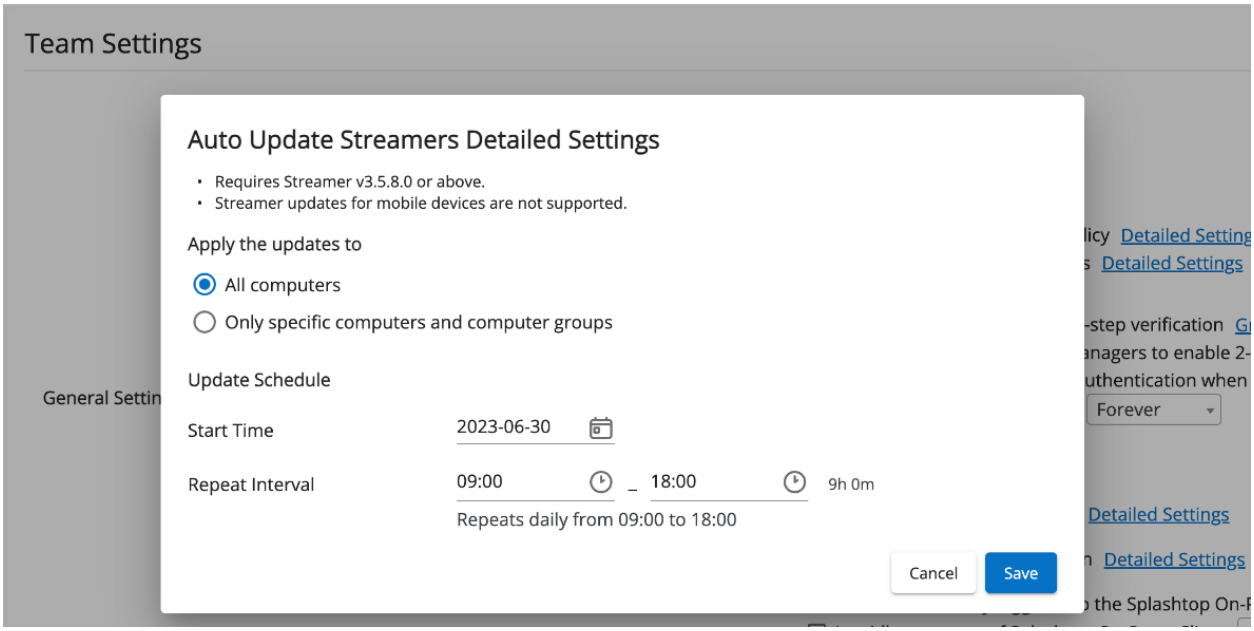
Auto Updates

In the unattended scenario, Streamer auto update can be managed from Splashtop Gateway web console.

1. Log in as Owner and navigate to Management > Team Settings



2. In Computers section, find Enable auto update Streamers, open Detailed Settings.



3. Staging and full-fledged updates

Apply the updates to - All computers

- Select this option if you plan to upgrade all of your deployed Streamers in one attempt.

Apply the updates to - Only specific computers and computer groups

- Select this option to validate the functionality of Streamer upgrades in your company environment by limit the upgrade scope to a selected group of computers.

We highly recommend all users start with partial updates first as a staging process before eventually apply the upgrades to all computers, especially in the scenario where large number of Streamers had been deployed.

4. Update Schedule

Start Time

- Schedule a proper date to start your update event. Note there is no end time, meaning the update event is always happening (if a lower version was detected) when enabled.

Repeat Interval

- Determines the update interval. There will be no update events out of the scheduled interval.

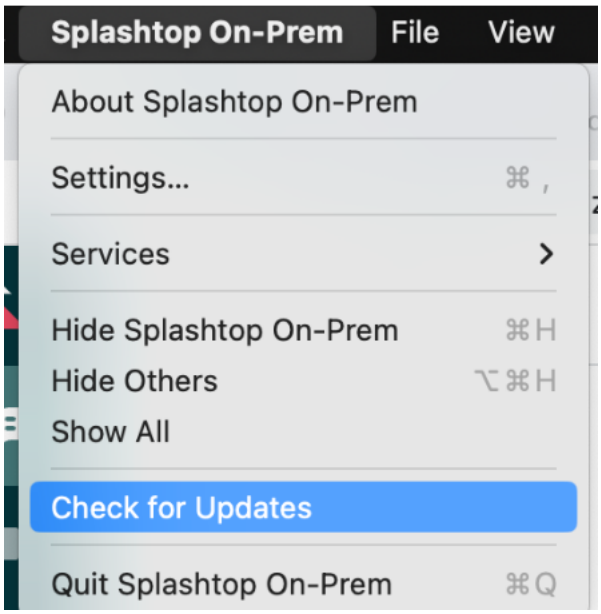
It is suggested to schedule the update interval during non-working hours.

Manual Updates

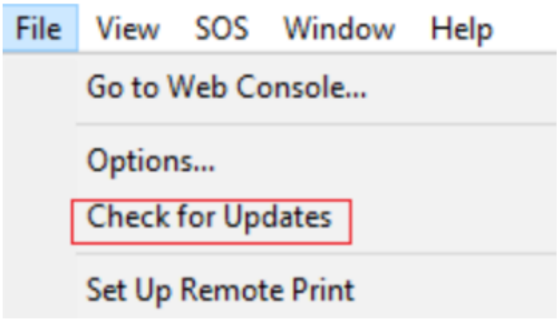
1. Splashtop On-Prem Client app

Log in to your Client app

Mac: Splahtop On-Prem > Check for Updates

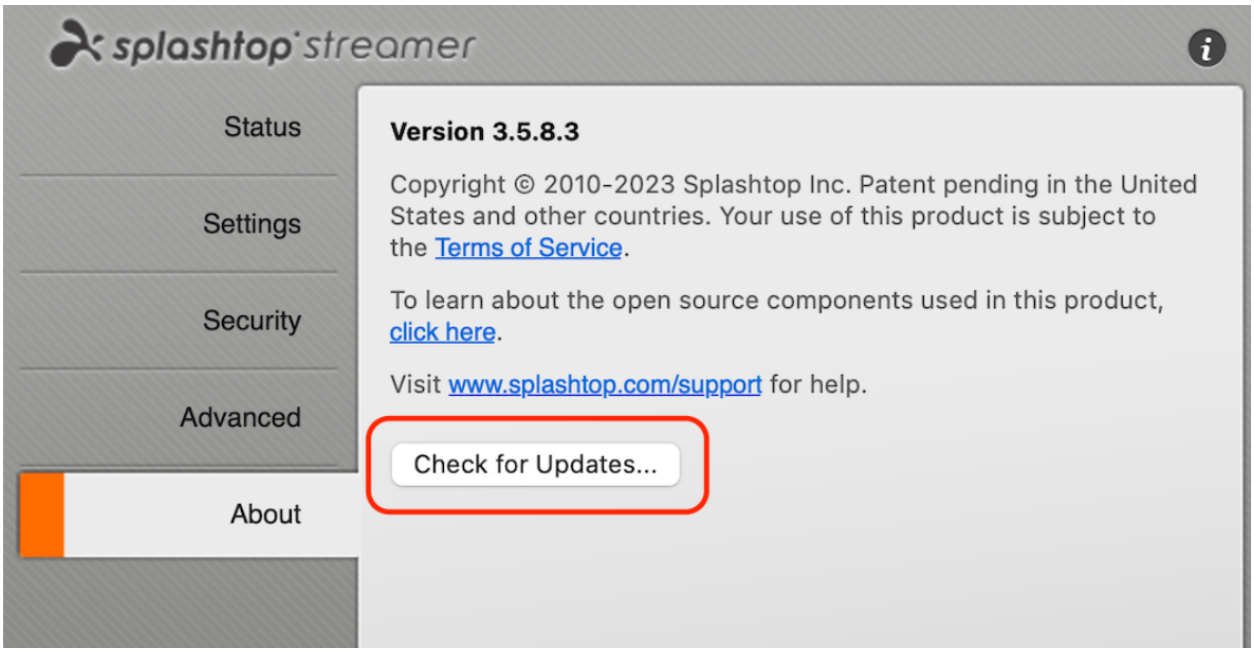


Windows: File > Check for Updates



Note: Client apps can only get updated manually by Check for Updates.

2. Splashtop Streamer: About > Check for Updates



Note: Streamer updates by clicking "Check for Updates" will need user interaction to complete the whole update process. This update event is irrelevant to "auto-update Streamer interval".

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

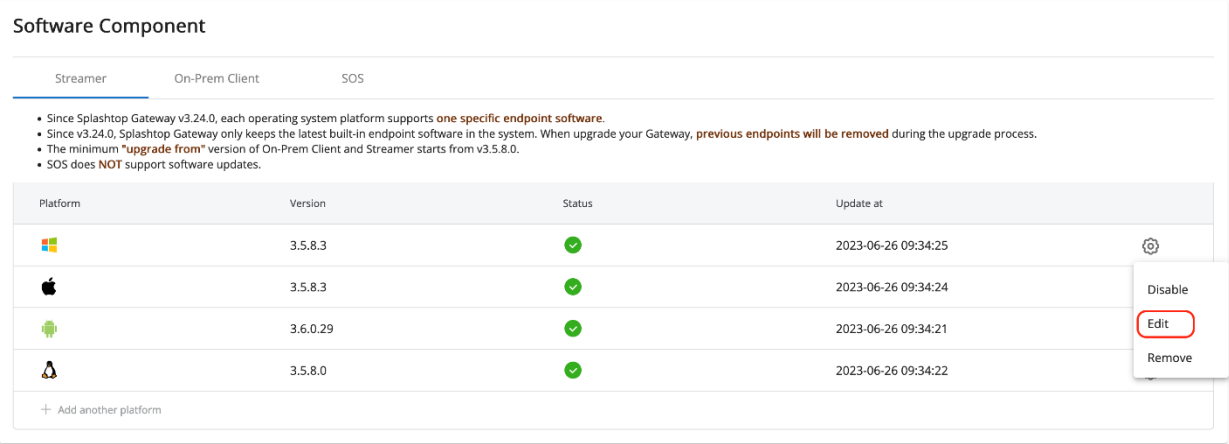
In the following new version announcement pages, you can get new versions of software components in PKG file format.

- **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

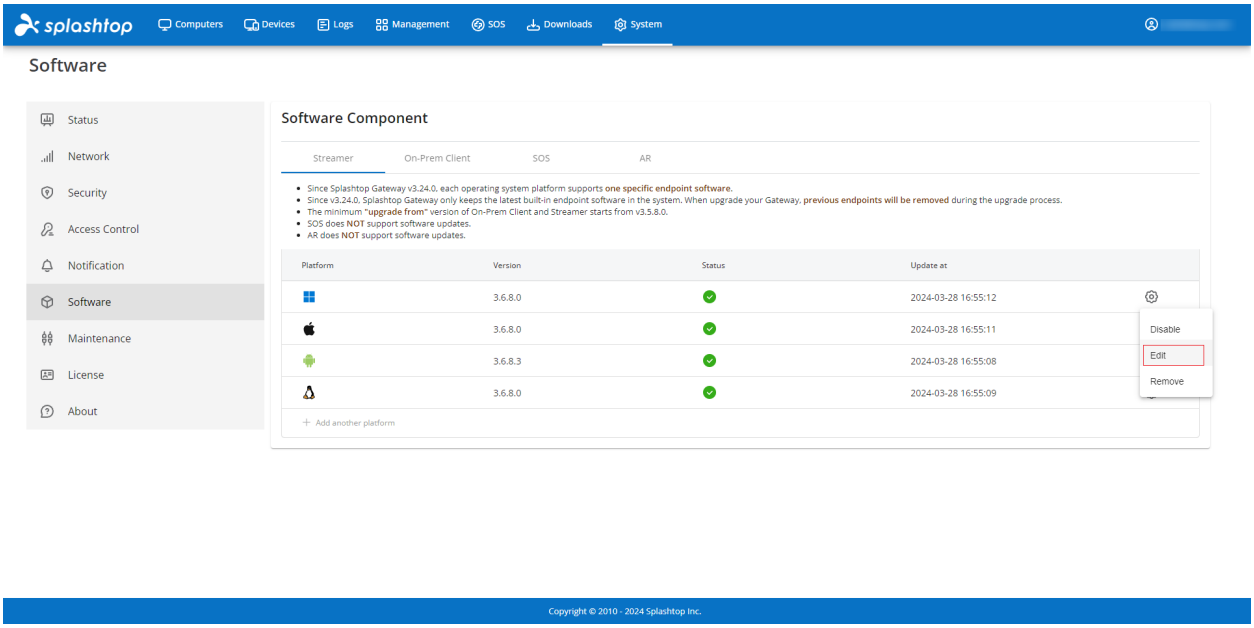
Import PKG file into Splashtop Gateway

Note: Since Gateway v3.24.0, upload PKG has been relocated to Software list -> Gear button -> Edit



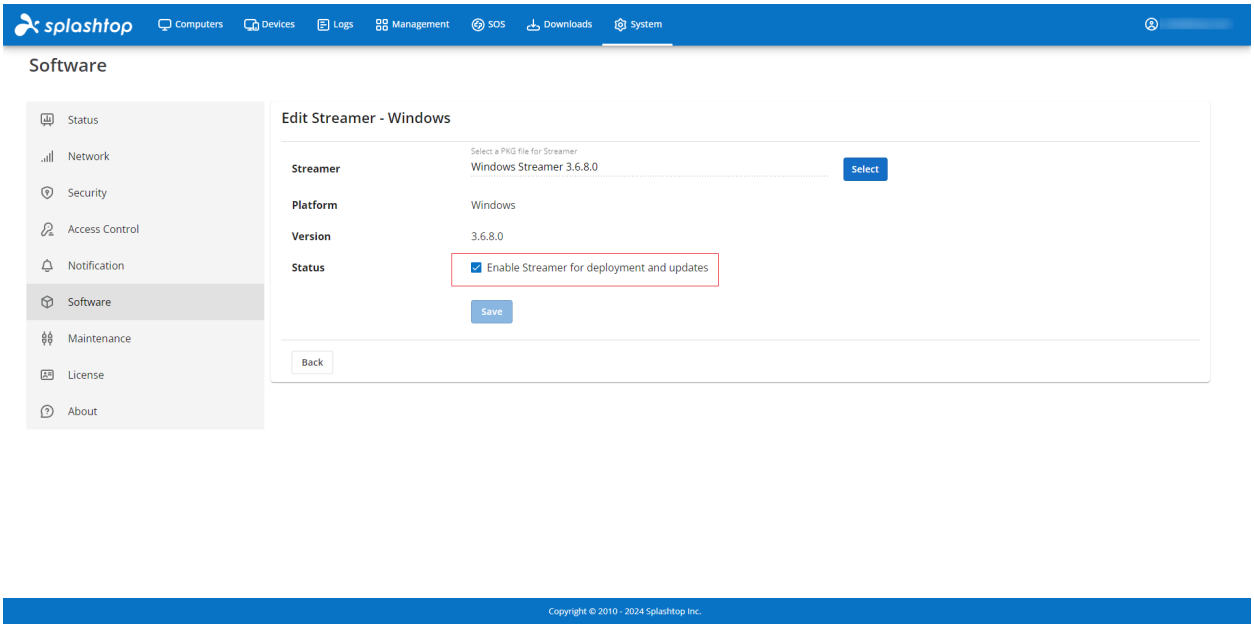
Import Streamer

1. Log in as Team Owner, go to Gateway's management console > *System* > *Software* > *Streamer*, select Streamer based on OS platform and click Edit as showing below.

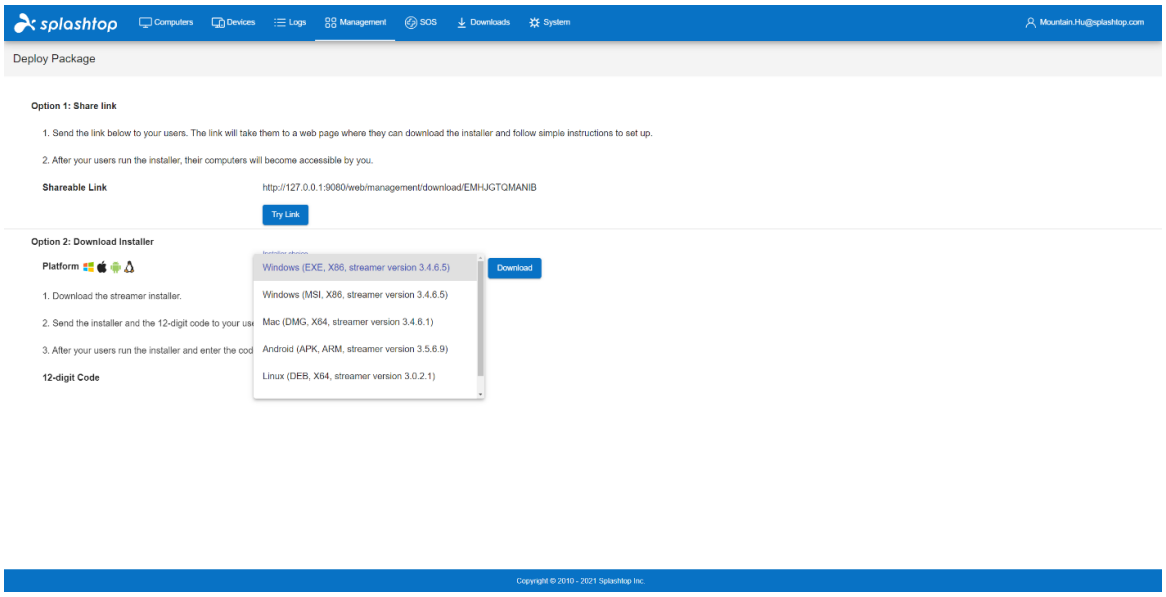


2. Select the PKG file, the system will verify if the PKG is packaged for Gateway correctly, and show the package info, like *platform* and *version*. Finally click **Save** to save the settings.

Enable the uploaded Streamer to make it available for deployment and updates.

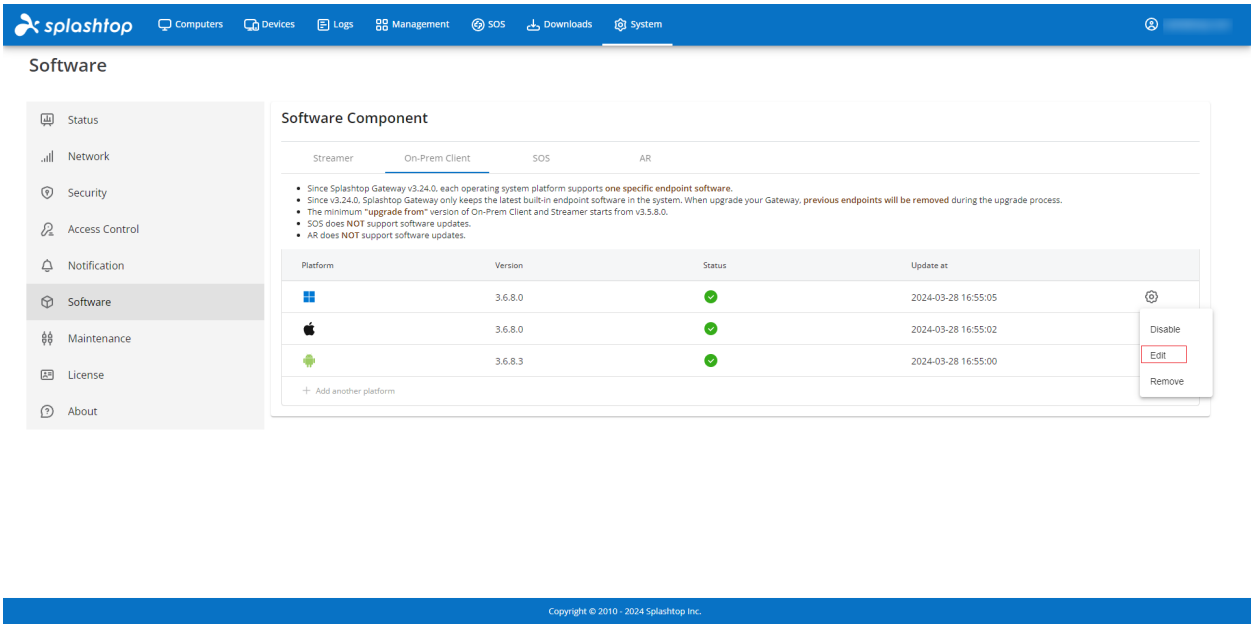


3. Once done, the newly uploaded software is now available for deployment and updates.



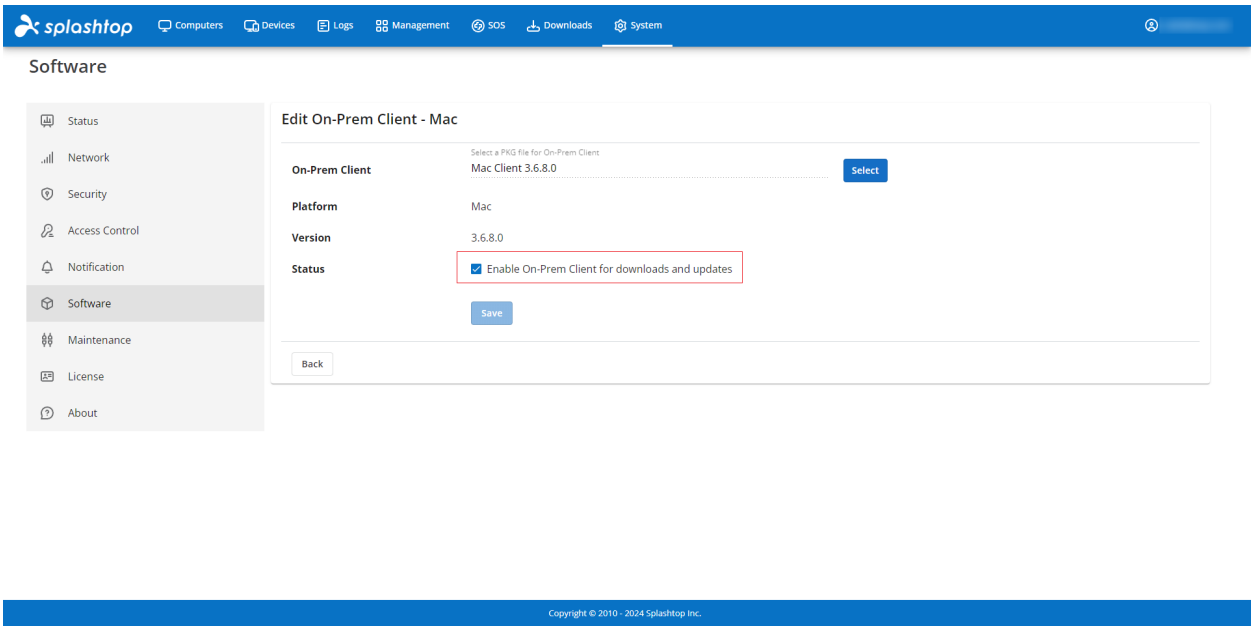
Import Splashtop On-Prem App

1. Log in as Team Owner, go to Gateway's management console > *System* > *Software* > *On-Prem Client*, select Client app based on OS platform and click Edit as showing below.

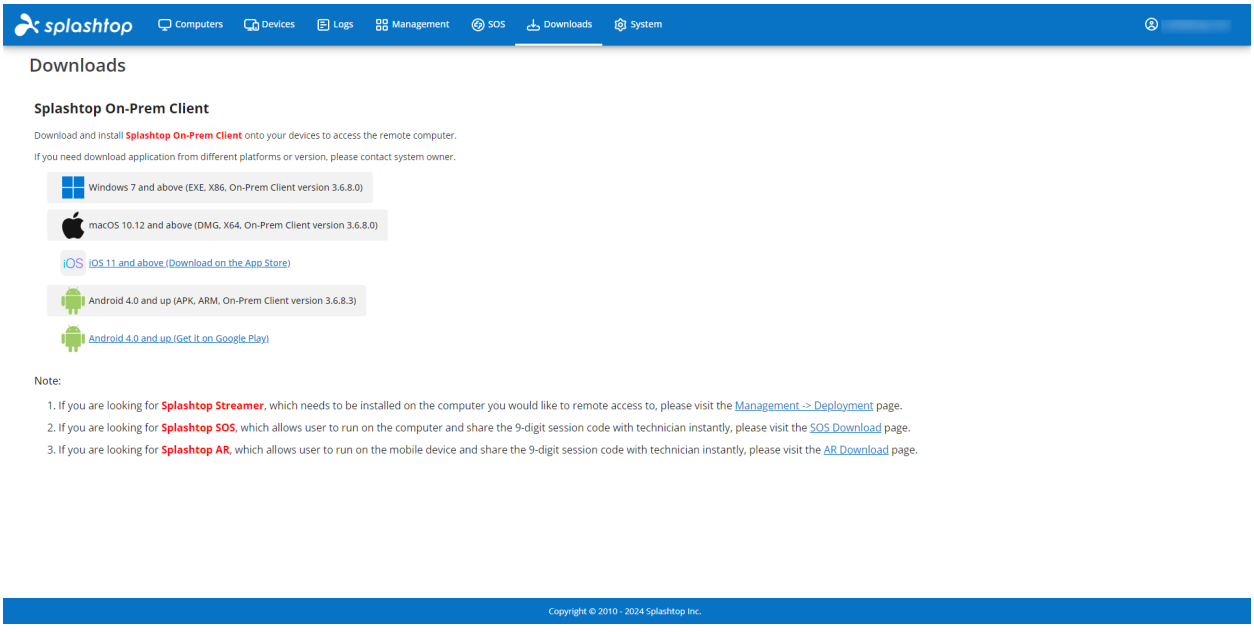


2. Select the PKG file, the system will verify if the PKG is packaged for Gateway correctly, and show the package info, like *platform* and *version*. Finally click **Save** to save the settings.

Enable the uploaded Streamer to make it available for deployment and updates.



3. Once done, the newly uploaded software is now available for deployment and updates.

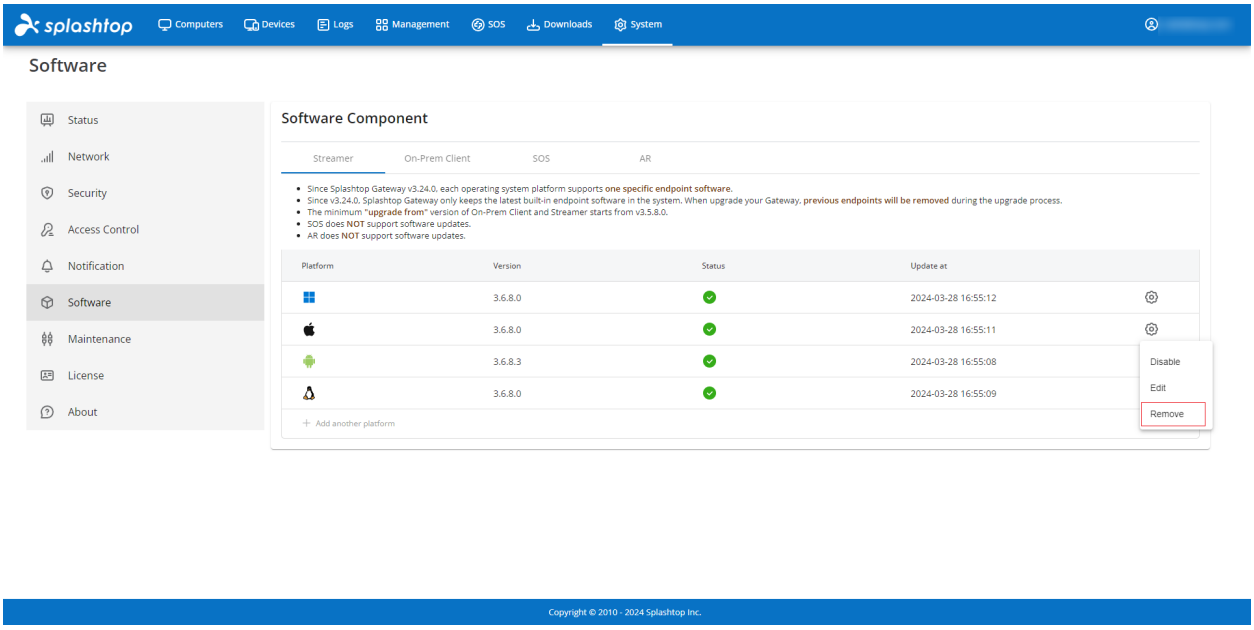


Remove software components

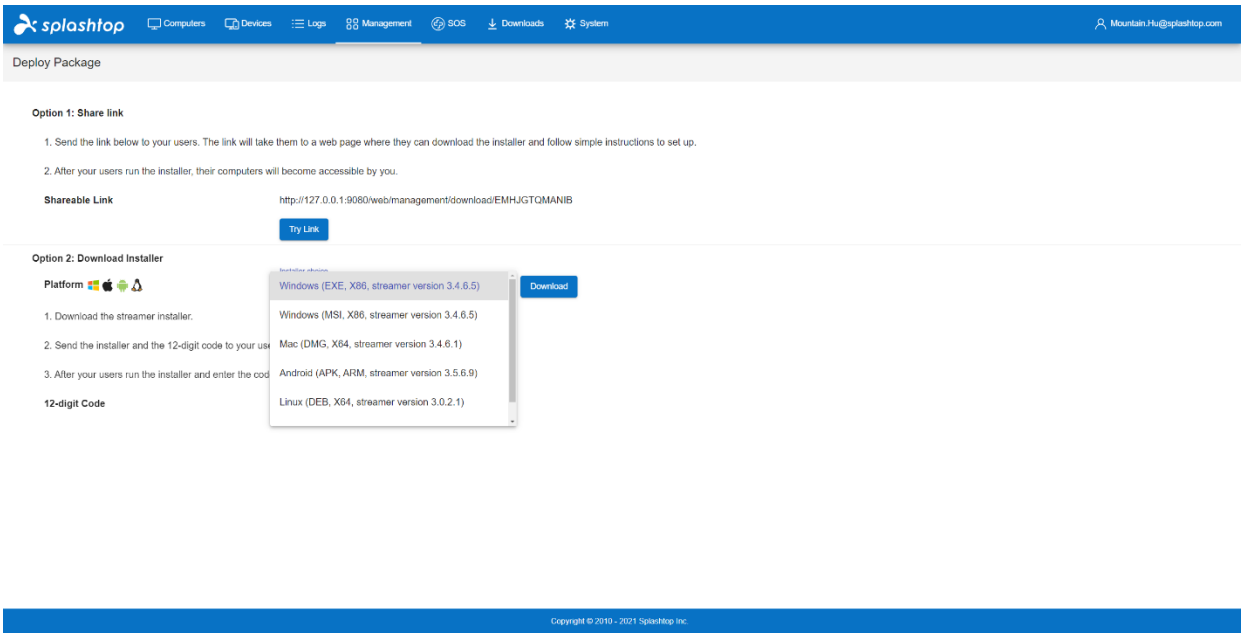
Team Owner can remove particular Streamer or On-Prem app from Splashtop Gateway, a removed component will not be able to be downloaded anymore, but it does not impact the existing installations.

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.

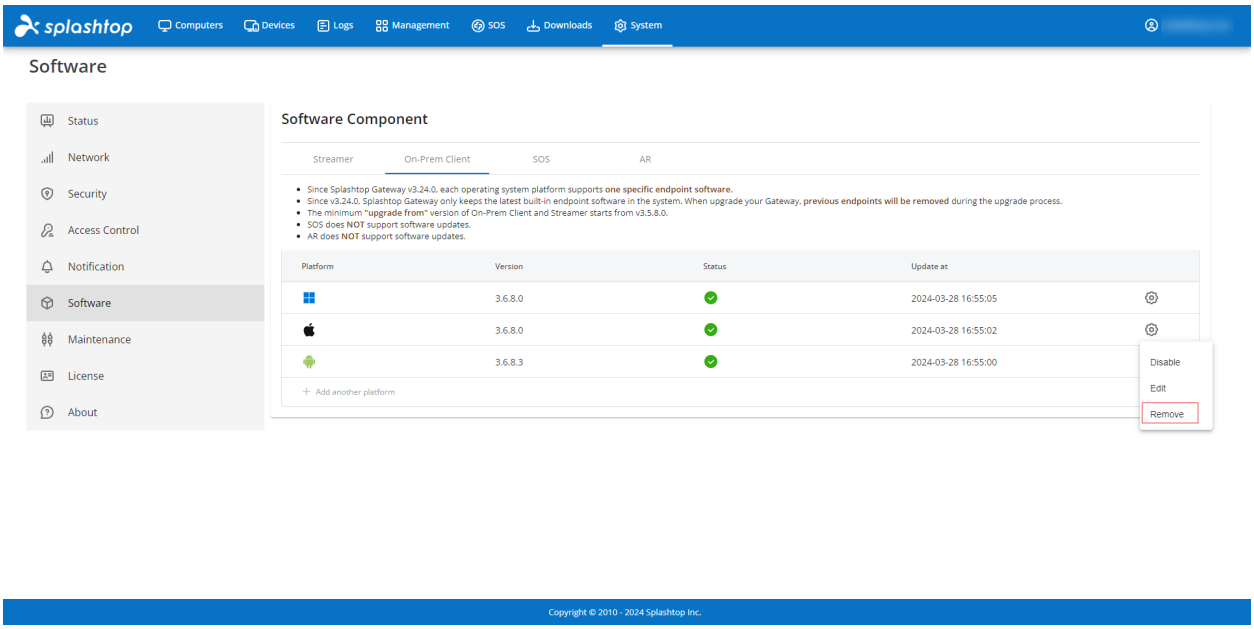


2. If a Streamer is removed, it will not be available in the **deployment** page.



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.



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

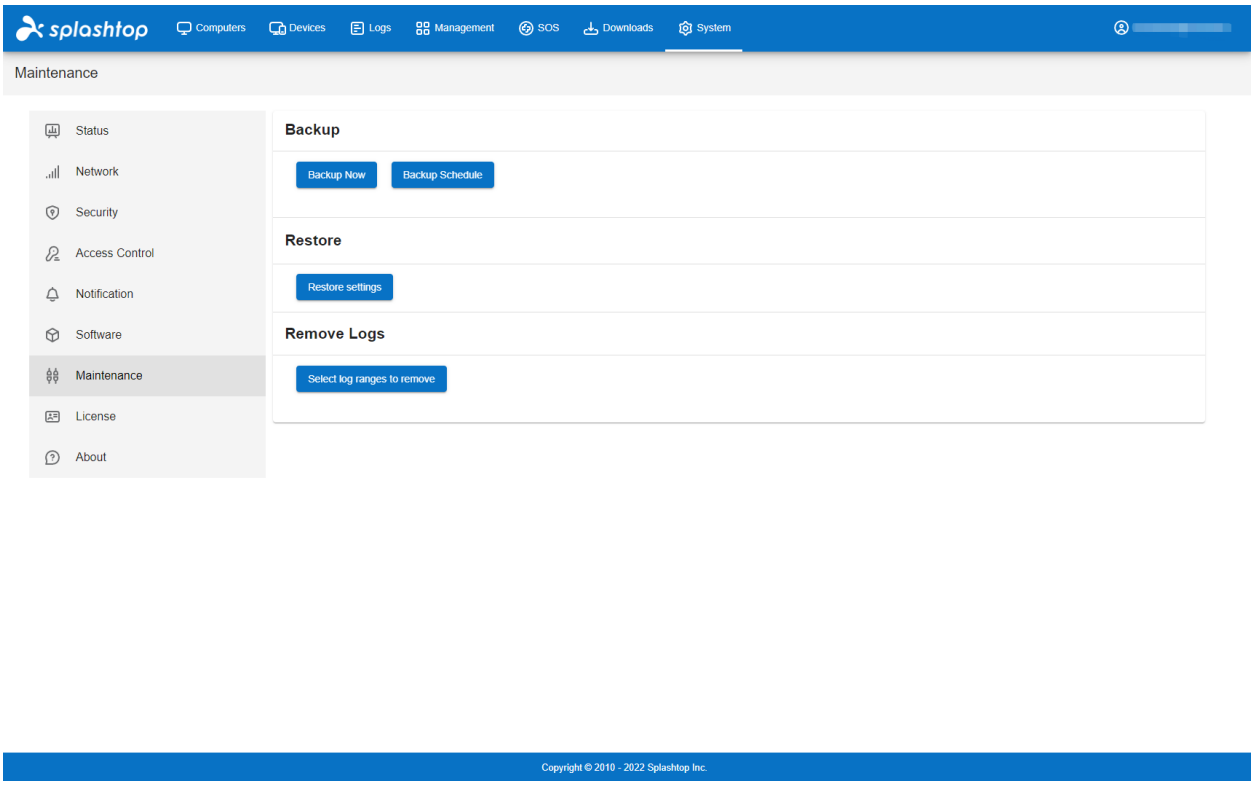
Maintenance

It is important to back up the 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.

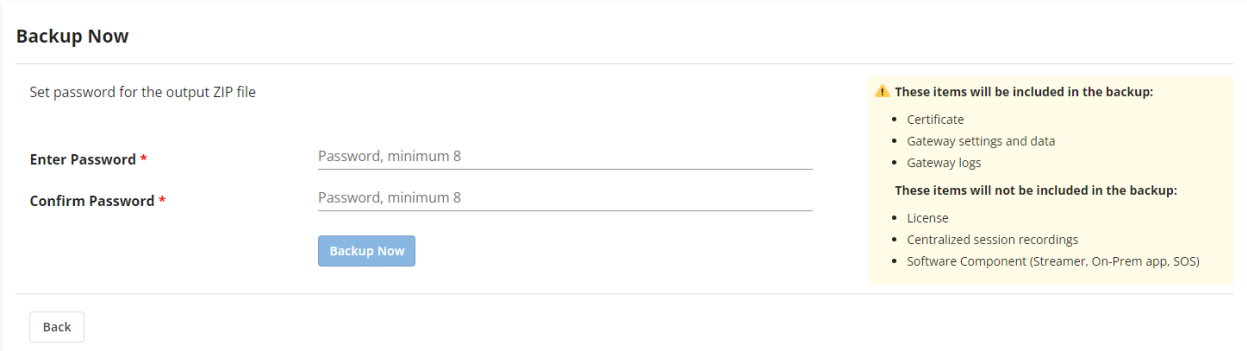
Backup

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.



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.

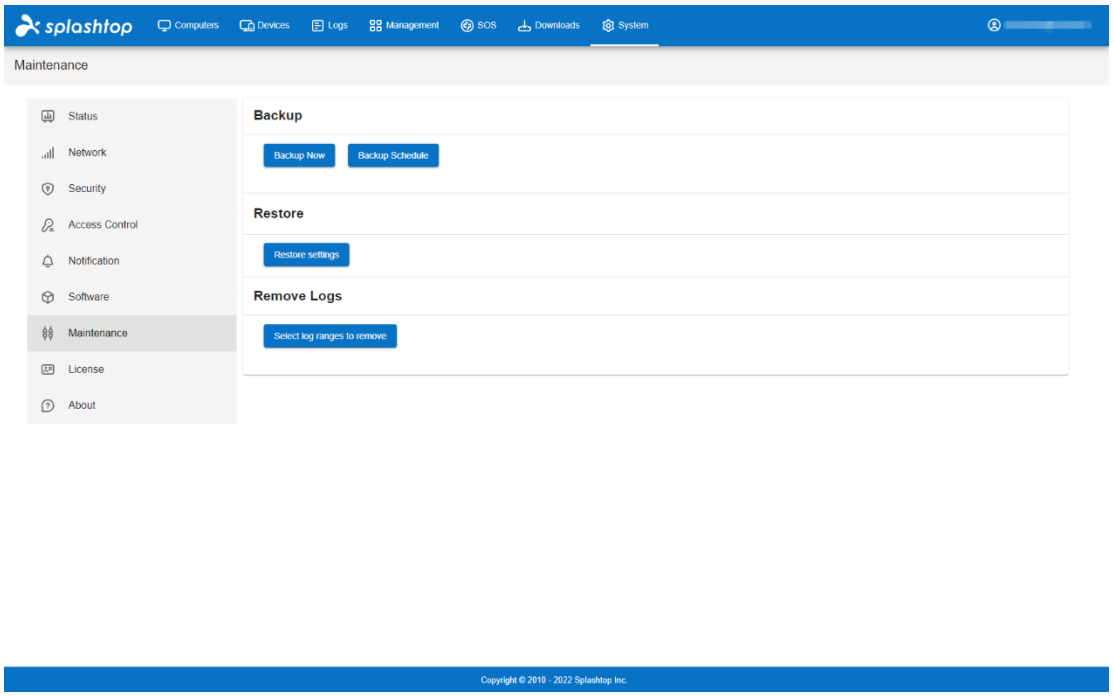
Backup Schedule

Backup schedule is a useful way to ensure that backupsfe are done in a consistent and timely manner. As long as the backup schedule is configured and enabled, the system can regularly perform a data backup in a proper schedule.

Where can you configure Backup Schedule?

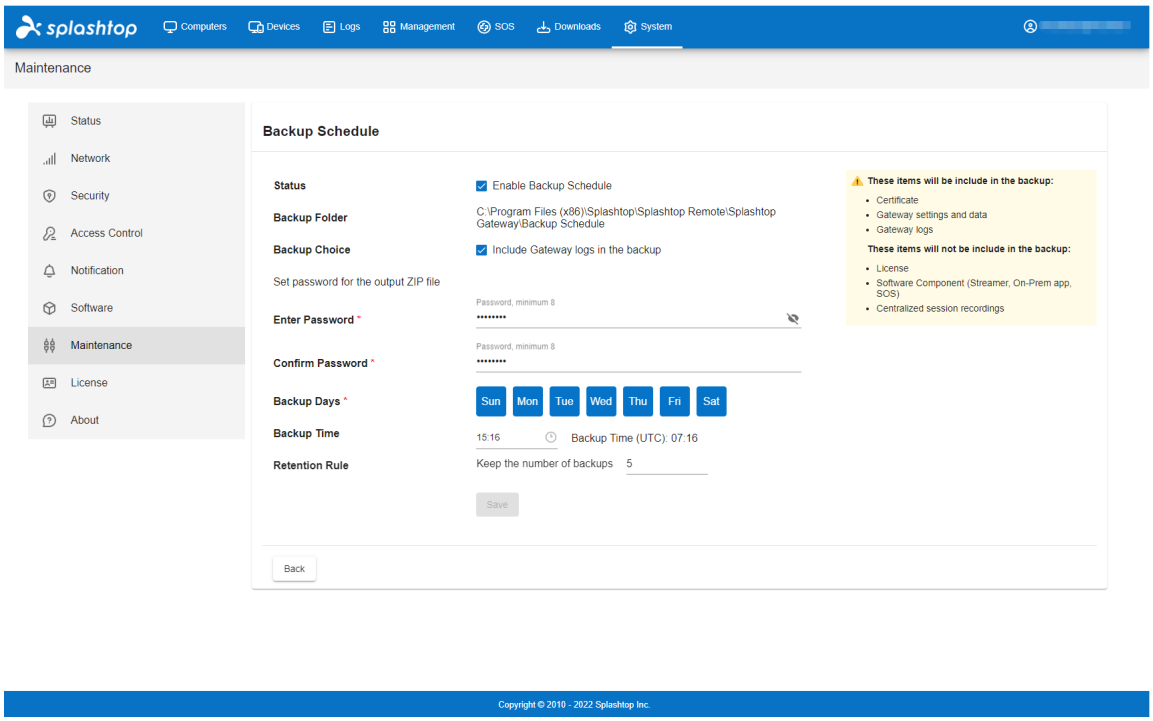
To configure Backup Schedule, you have to use the **Team Owner Account** to log in to the Splashtop Gateway web portal. Team owner account is the email address used to activate the license of Splashtop On-Prem system.

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



Backup Schedule Settings

Now you need to configure these items to create your backup schedule policy.



- **Status**, turn on this option to enable backup schedule. If this option is not enabled, the backup schedule will not run even if the configuration is saved.
- **Backup Folder**, show the path where the backup schedule file is stored.
- **Backup Choice**, choose whether to include Gateway logs in the backup schedule file and the right-hand area of the page will show the exact scope of the current backup according to the settings of backup choice.
- **Enter Password**, you are required to set a password for the ZIP file to be produced, before initiating the whole backup process.
- **Confirm Password**, you are required to set a password for the ZIP file to be produced, before initiating the whole backup process.
- **Backup Days**, choose the backup days for backup schedule.
- **Backup Time**, choose the backup time for backup schedule.
- **Retention Rule**, choose how many backups you need to keep in backup folder.

Note

- Only one backup can run at the same time.
- To ensure the efficiency of the backup schedule, the endpoints will not be included in the backup schedule file

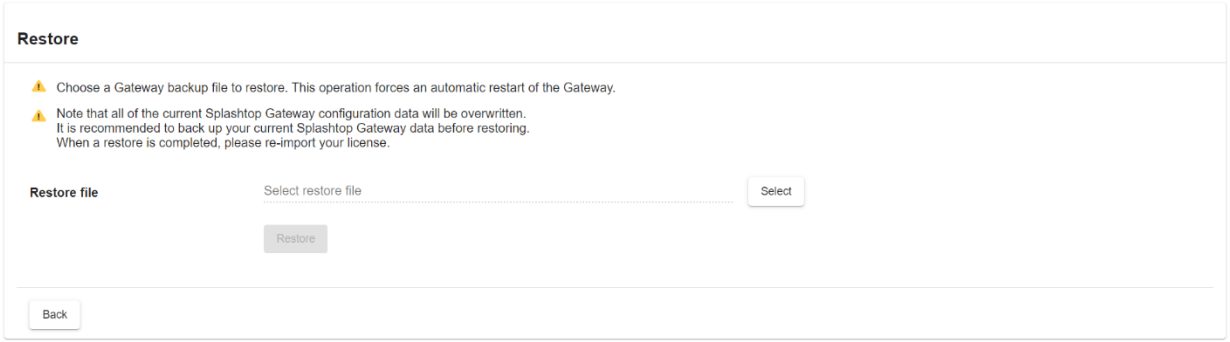
Restore

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

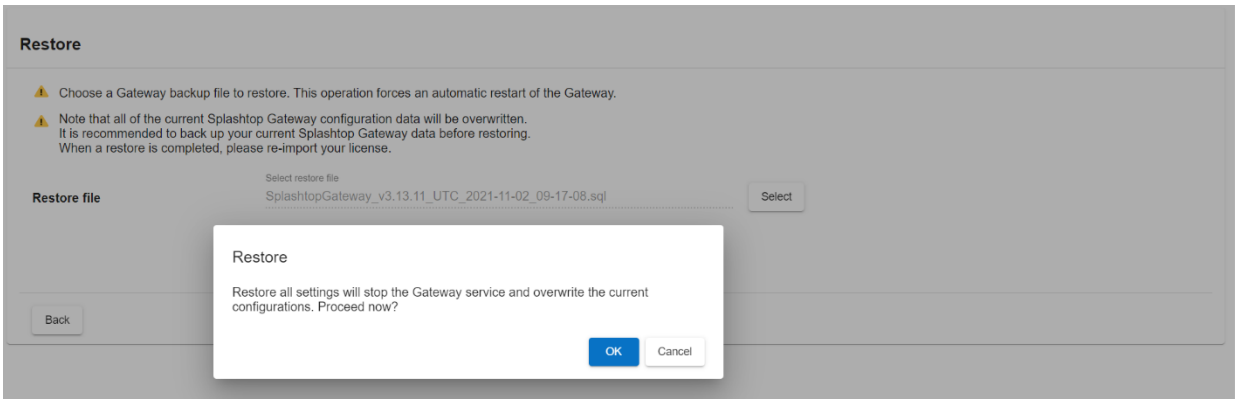
- You have the license key for Splashtop On-Prem at hand. You will be asked to activate the license again after a system restoration.
- Get the restore file ready by unzipping the backup ZIP file and saving the SQL script into a local folder.
- Back up the current system as all existing configurations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

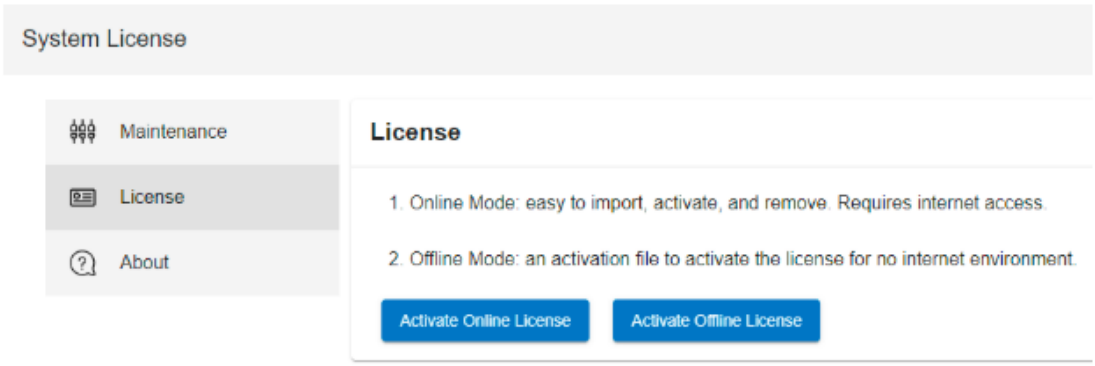
Click **Restore settings** button and click on **Select** button to browse the SQL script file.



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



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

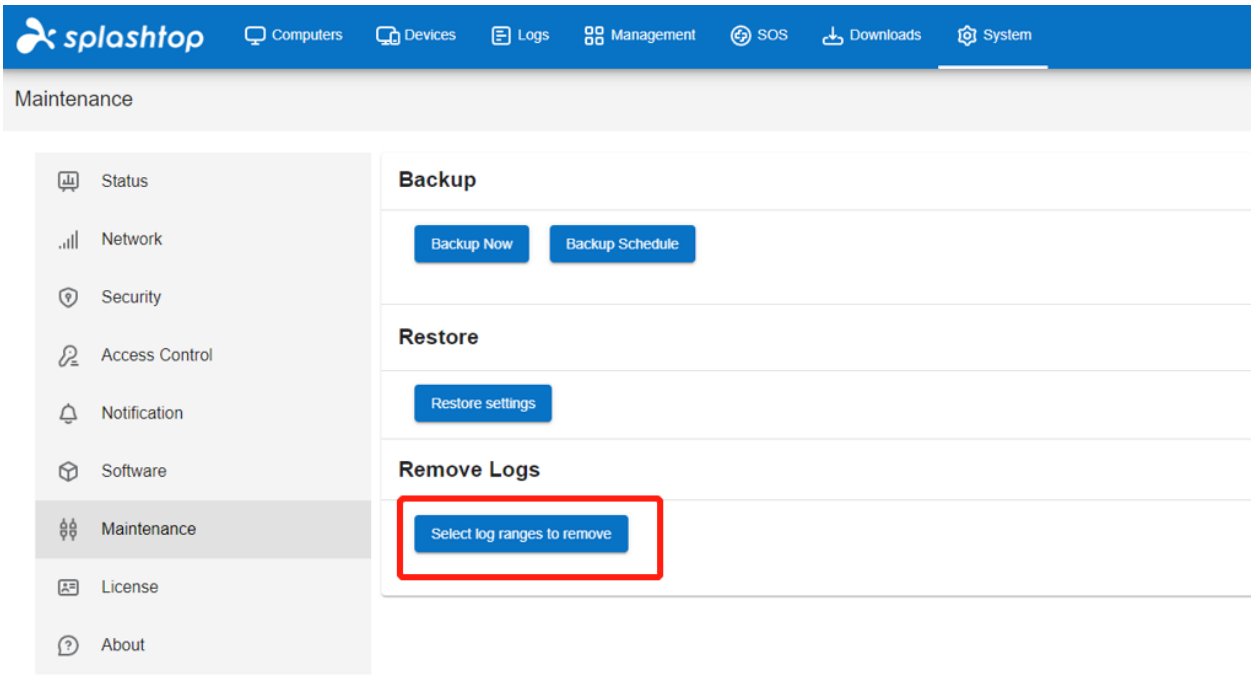


Activate the license through online or offline mode, depending on the type of license you acquired before.

Now you have done a successful system restoration.

Remove Splashtop On-Prem Logs

Starting from **Gateway v3.18.0**, system administrator can remove Gateway logs for maintenance
purpose.



Log in to Splashtop Gateway as Owner, go to web/system/maintenance

Find "Select log ranges to remove" and start to clear up your logs to release the disk space.

Notice:

1. Removed logs are gone for good and will not be possible to retrieve back. If regular auditing is serving as a routine in your organization, please consult before removing any logs.

2. Logs are removed by month(s), and logs of the nearest 2 months cannot be removed.

3. Neither removed logs can be visible in web/log/... nor export the correspoinding CSV.

Notification

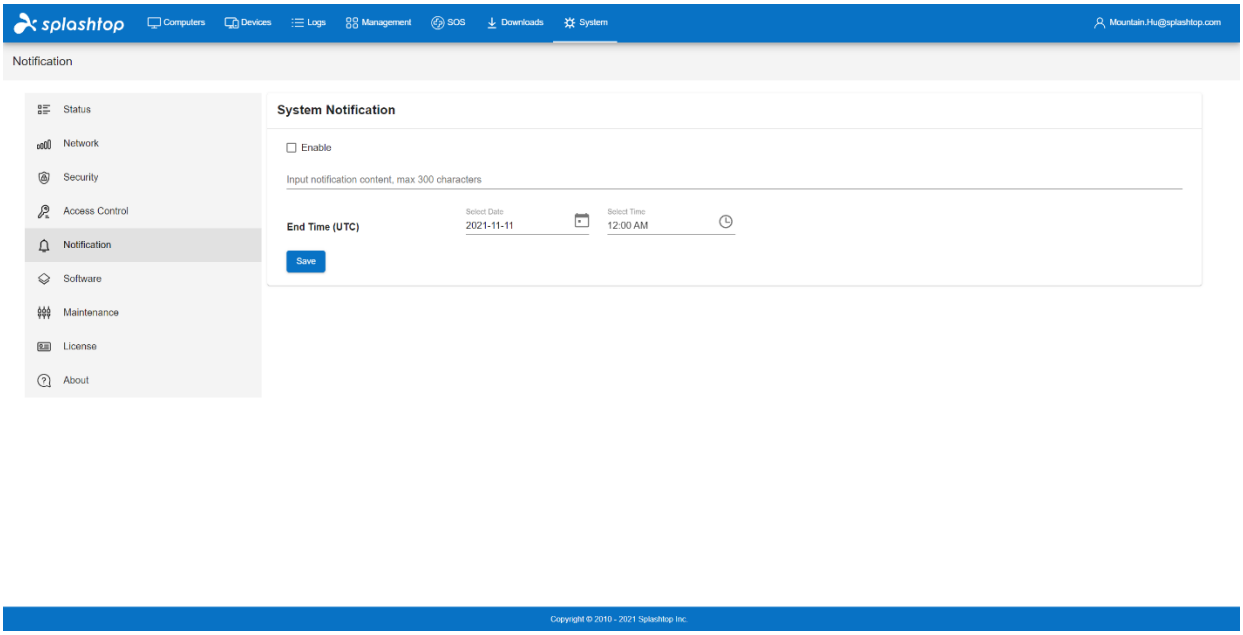
A Splashtop On-Prem Team Owner can publish a system notification from the **Notification** page, in order to notify the users if there is an expected downtime due to system maintenance, or if any update on the endpoints is available.

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

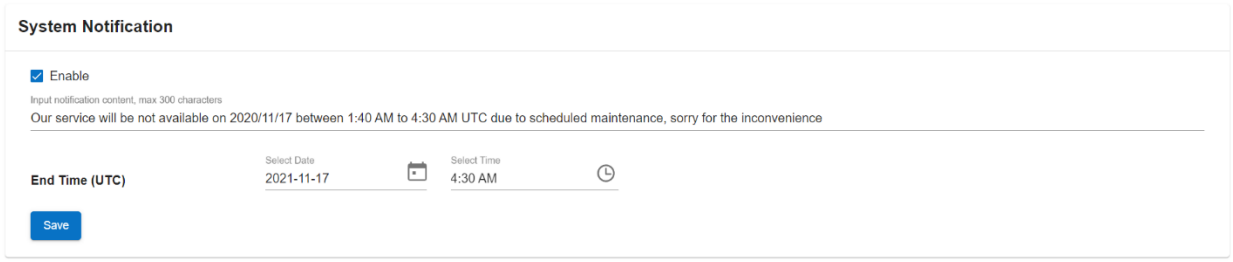
To publish a notification, firstly check the **Enable** box.

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

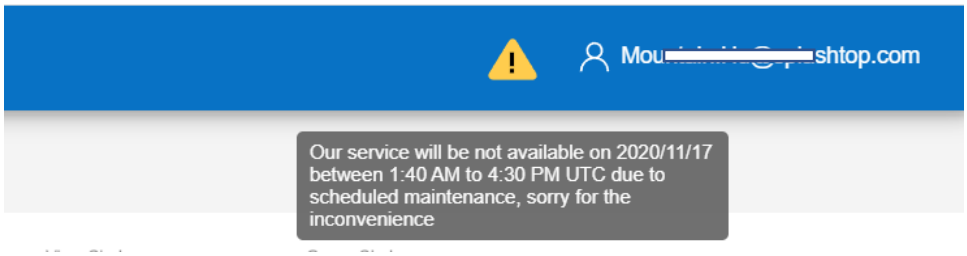
Note: System Notification is **in UTC Time. Please calculate time difference before publish notification.**



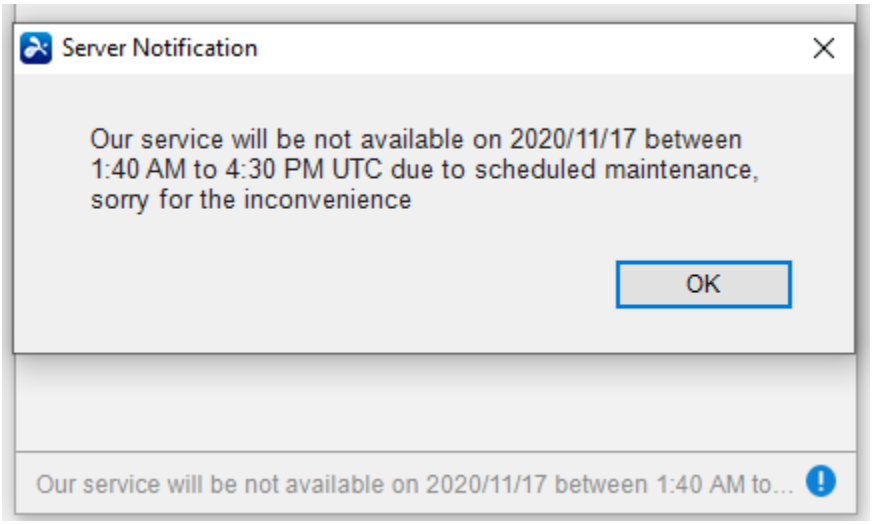
Below screenshot provides System notification as an example:

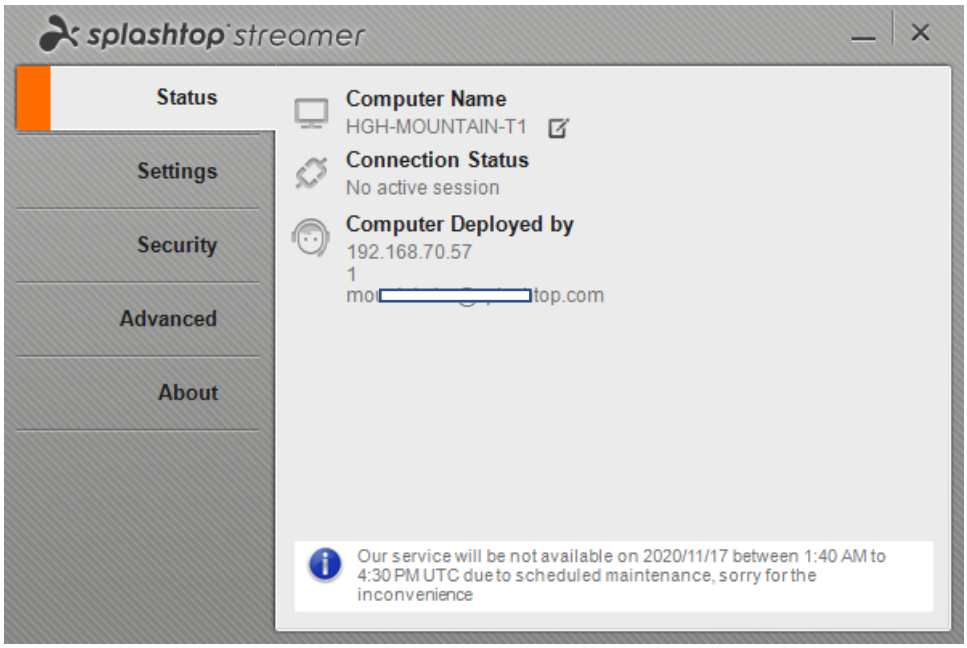


After being saved, System notification will be displayed at the top right corner of the Gateway page with a yellow exclamation mark. Hovering over the mark, the notification will be displayed to every logged in user.



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.



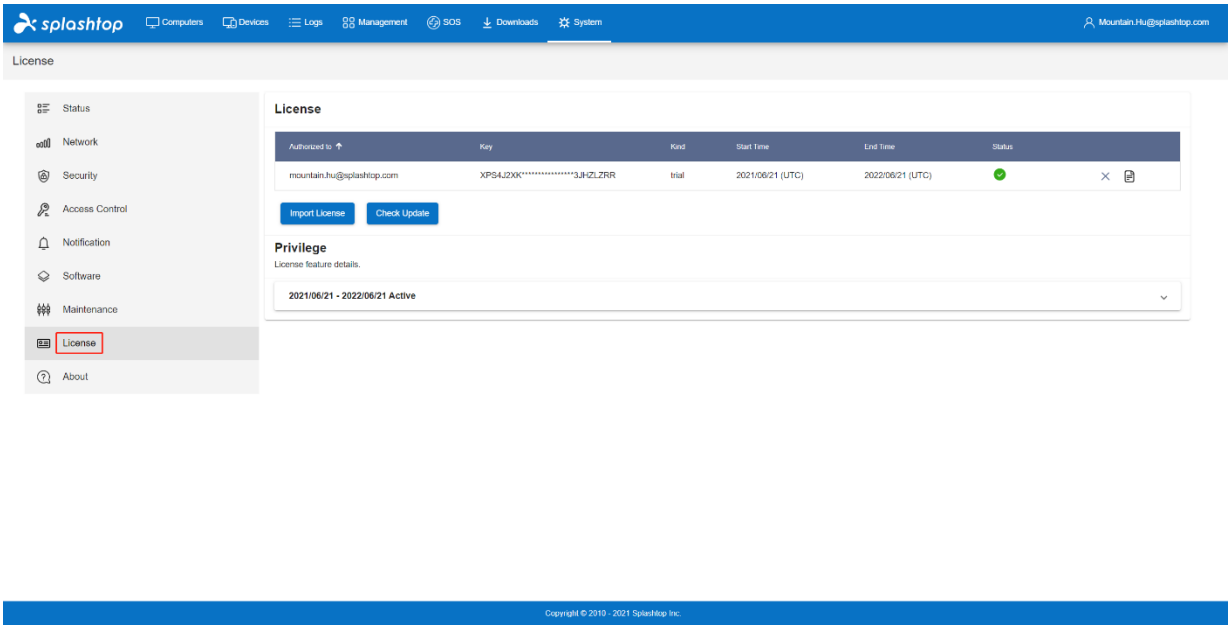


On Prem License

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**.



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 with 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 if it is 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

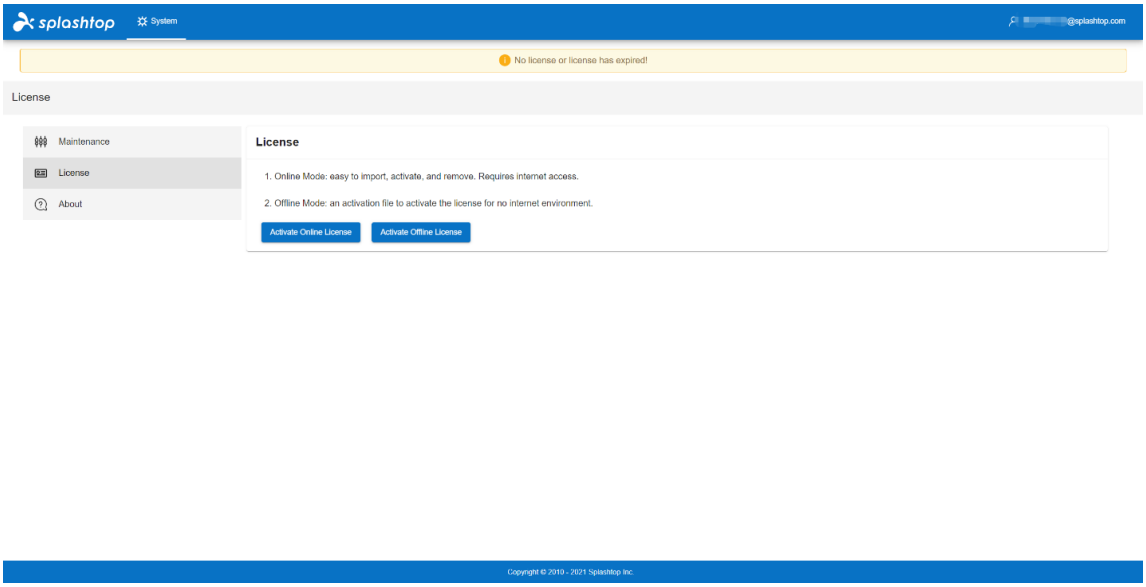
Max concurrent file transfer (outside session) to one Streamer	Max number of outside session file transfer allowed to one Streamer at the same time
Max Chat (outside session)	Max number of outside session chat sessions on the entire system
Max concurrent chat (outside session) to one Streamer	Max number 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.

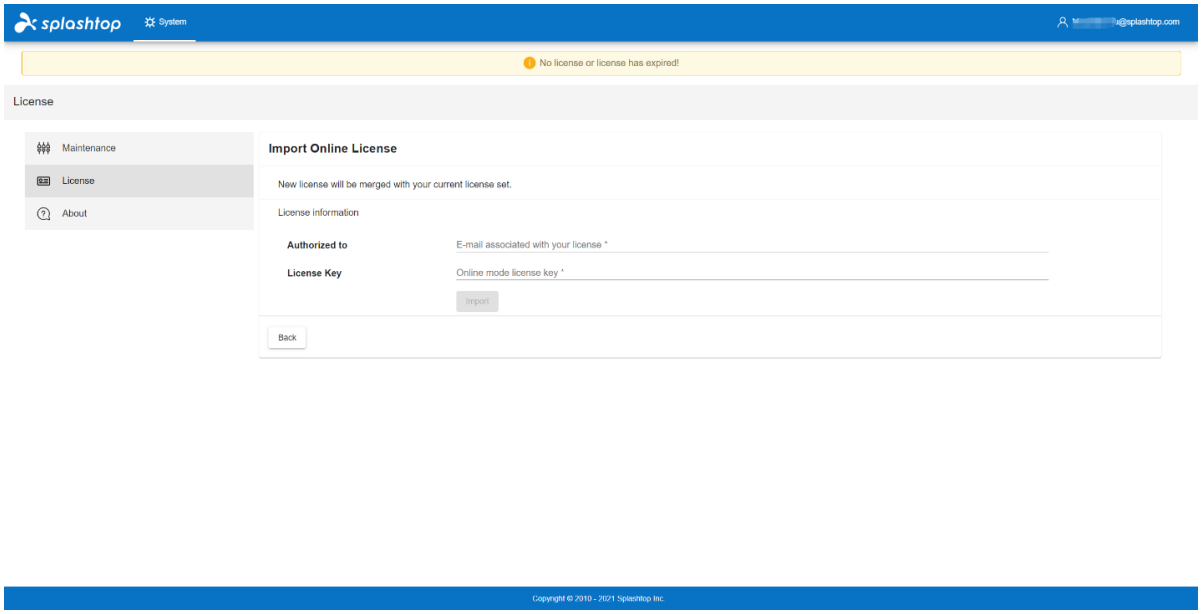
You need to login as Team Owner to activate the license, which is in Gateway's **System** > **License** page.



Online license activation

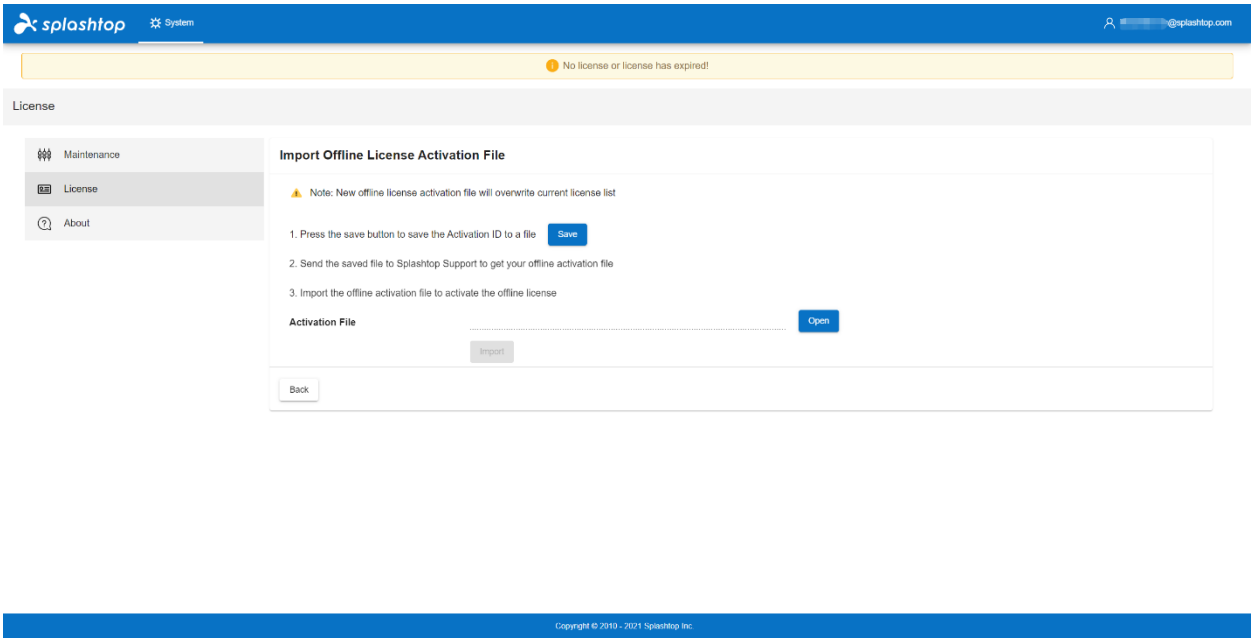
For online license activation, click Import Online License, input the Authorized to and License key which you obtain from Splashtop Sales.

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



Offline license activation

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



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

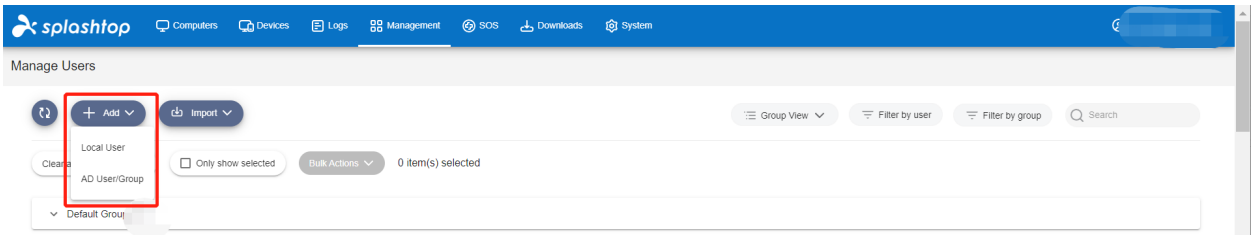
Team Owner/Admin can use this page to create a new user or modify attributes of existing users.

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.

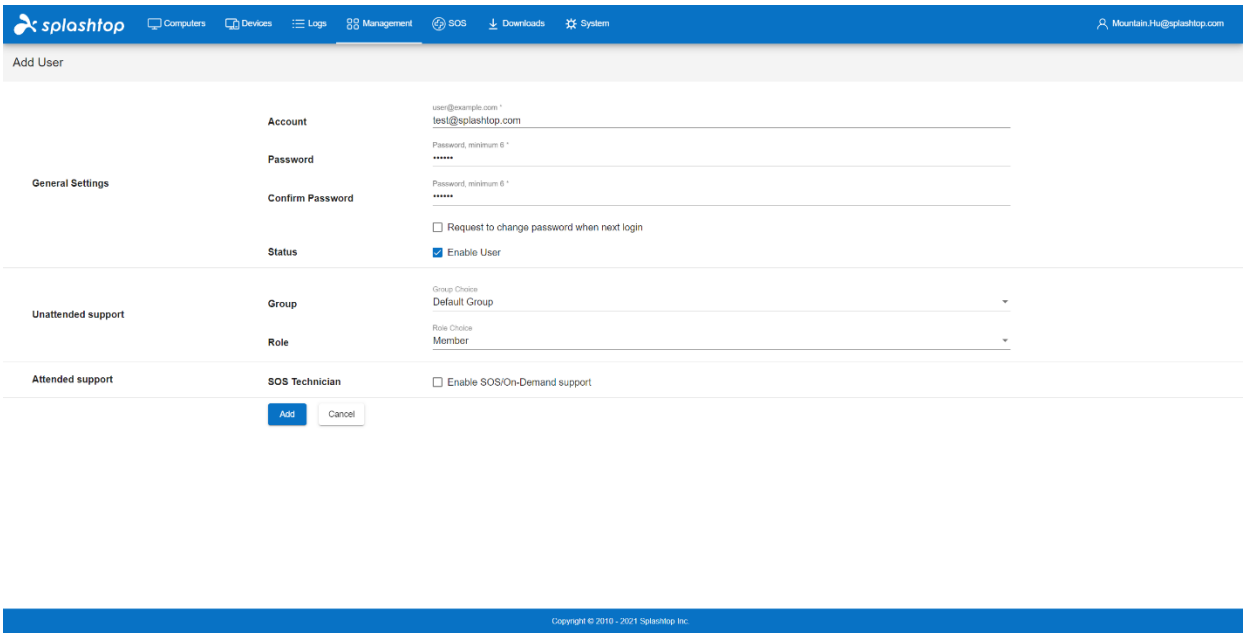
User attributes, including role, group, access permission, display name, password, 2-step verification, are available to configure in the Users page.

Create user accounts

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



Create local account

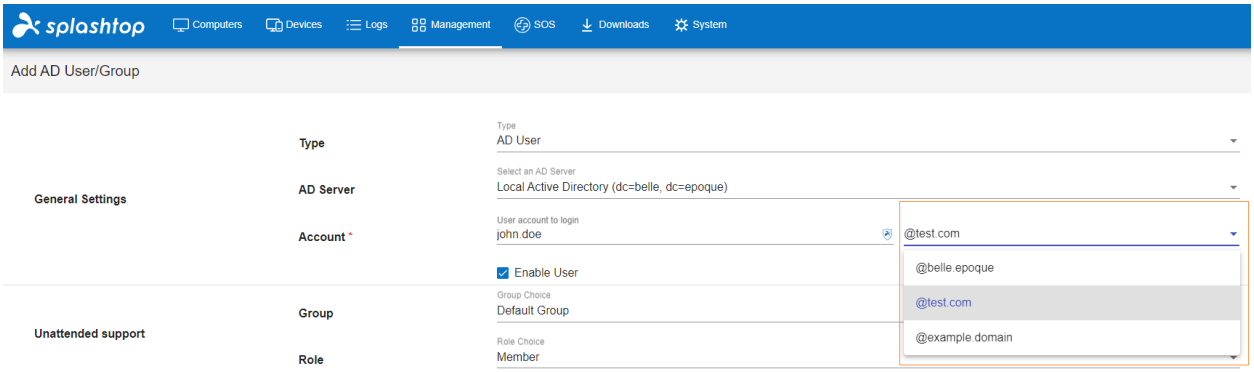


Field	*Meaning*
Account	This is the user's login account, it is unique in the system.
Password	Minimum 8 characters.
Generate Password	This helps to generate a more random password for secure reason.
Request change password when next login	With this option, when user log-in to the system, he/she will 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.



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)** or **User Principle Name (UPN)** 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.

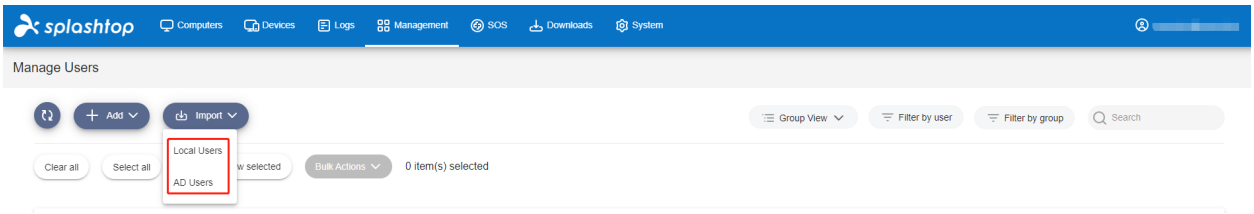
The AD users in AD Group Members will be showed up in **AD Group Members** after log into Gateway portal or client application with his/her AD account at **least once**. By contrast, an **AD individual user** added to Gateway will be displayed and modified property immediately.

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

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

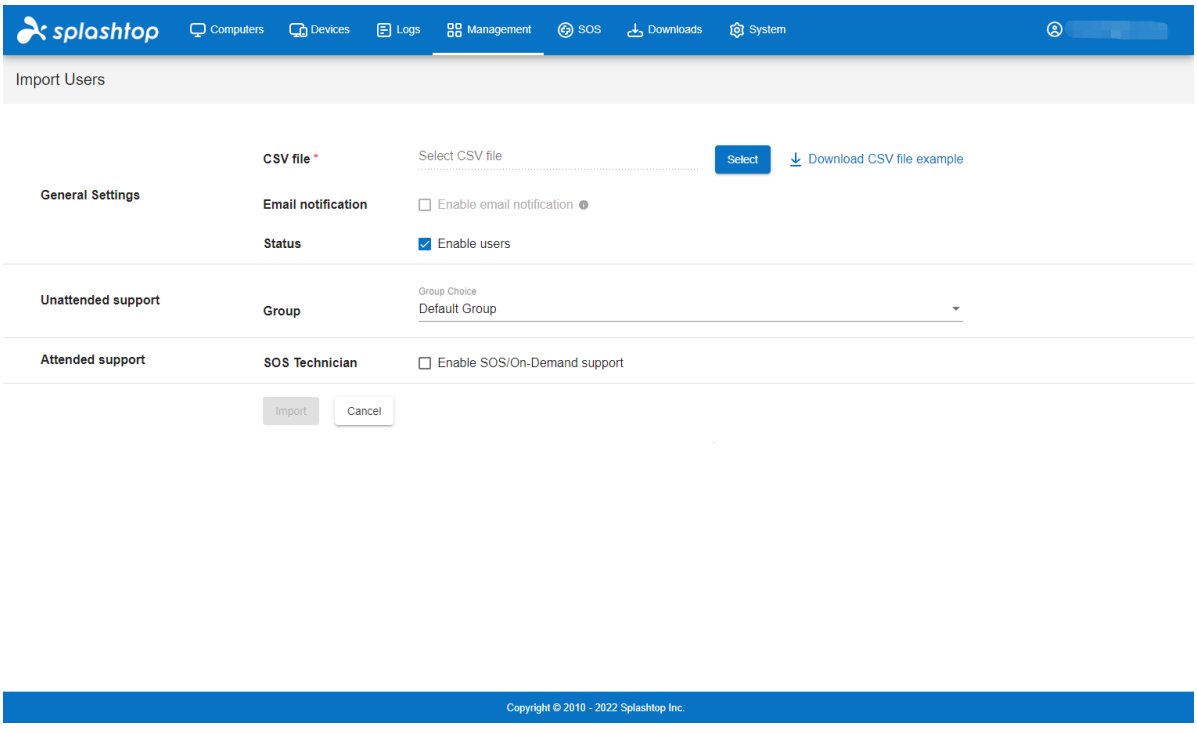
Bulk import user accounts

With **Bulk Import**, you can easily import a large number of local users or AD individual users into your Gateway instead of adding them one by one.



Import local user

When the users have been imported, the system will assign a one-time password which is valid for 7 days to each successfully imported local user account. These users will not be able to log in to the Gateway and Splashtop On-Prem app until the passwords for these users have been reset.



Download CSV file template: Import users using the CSV file template.

Select CSV file: Upload the CSV file with the user account list.

Enable email notification: if you are configured SMTP server, enable this checkbox, user can receive the account and one-time password by email.

Status: If an account is enabled, he/she can establish a remote session, if the account is disabled, he/she can still access the web portal, but the remote session is disabled.

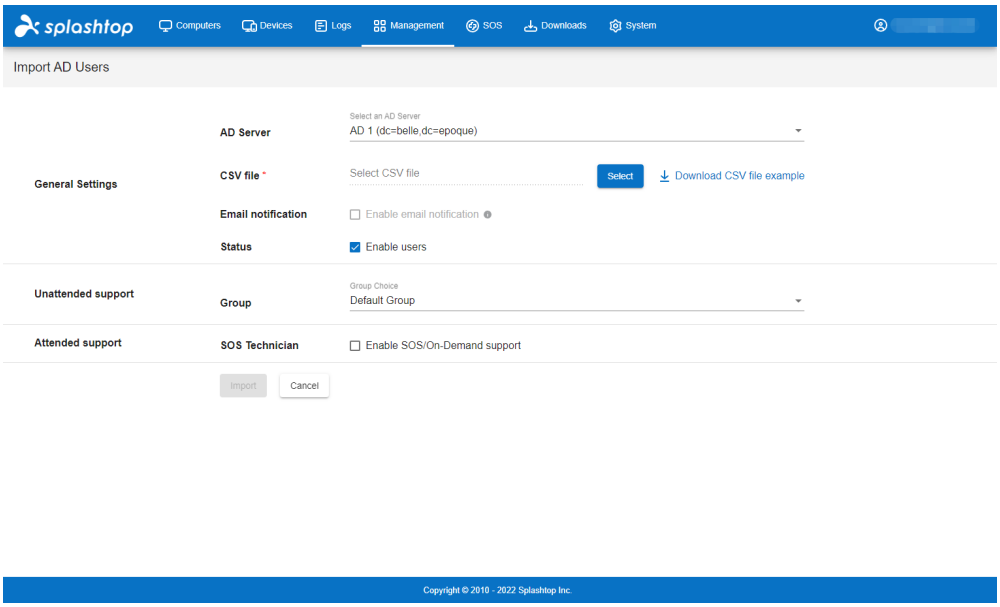
Group: Users can be grouped into different groups, grouping is efficient in users management/access permissions.

SOS Technician: Enable SOS On-Demand support capability.

Import: Import the local users in the CSV file to the target group.

Import AD users

Once an AD server has been successfully authenticated, it would appear in AD server list in System- Active Directory tab. Now navigate to Management tab – Users, click on Import button on the top, then select AD Users. All successfully authenticated AD users can log in On-Prem client application with their AD credentials and start to use Splashtop remote service.



AD Server: Select the AD server which contains the target AD user.

Download CSV file template: Import AD users using the CSV file template.

Select CSV file: **Upload** the CSV file with the AD user list.

Enable email notification: if you are configured SMTP server, enable this, user can receive the account and one-time password by email.

Status: 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.

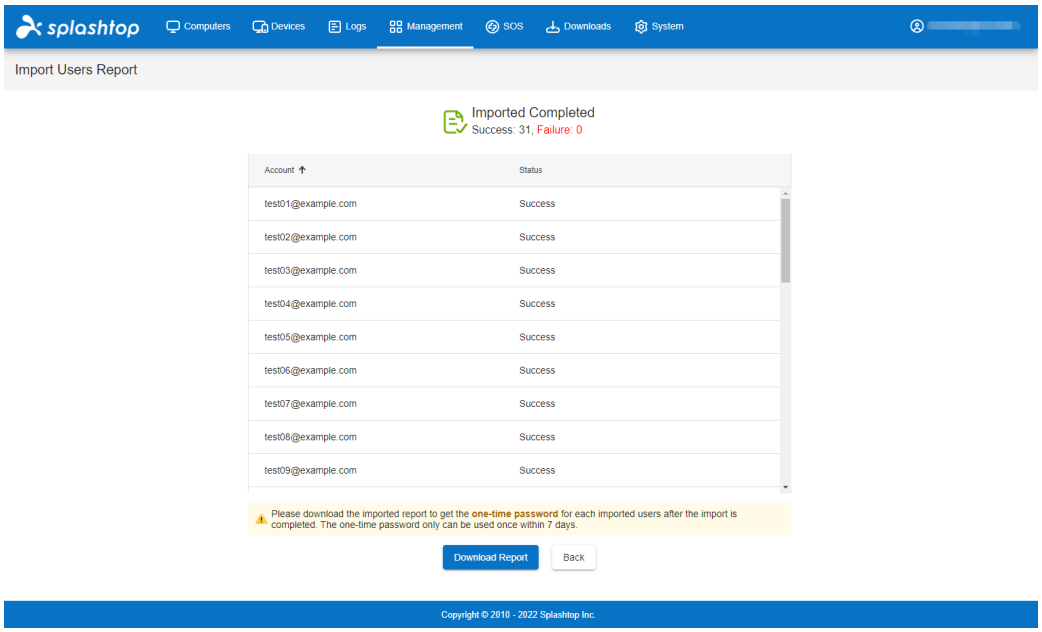
Group: Users can be grouped into different groups, grouping is efficient in users management / access permissions.

SOS Technician: Enable SOS-On Demand support capability.

Import: Import the AD users in CSV file to the target group.

Imported report

After the user import is completed, **Admin** or **Owner** can view the import results and download the imported report.



Important Notes

1. It is only CSV file format supported.
2. The data in the file has to follow the standard layout. You can download the example.csv below to check the layout/format.
3. You cannot start importing another CSV file until the current import has been completed.
4. All successfully imported users will be given the member role.

Set access permission

Access permissions

Access permissions determine which users have access to a certain computer.

Access permissions can be configured to be:

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

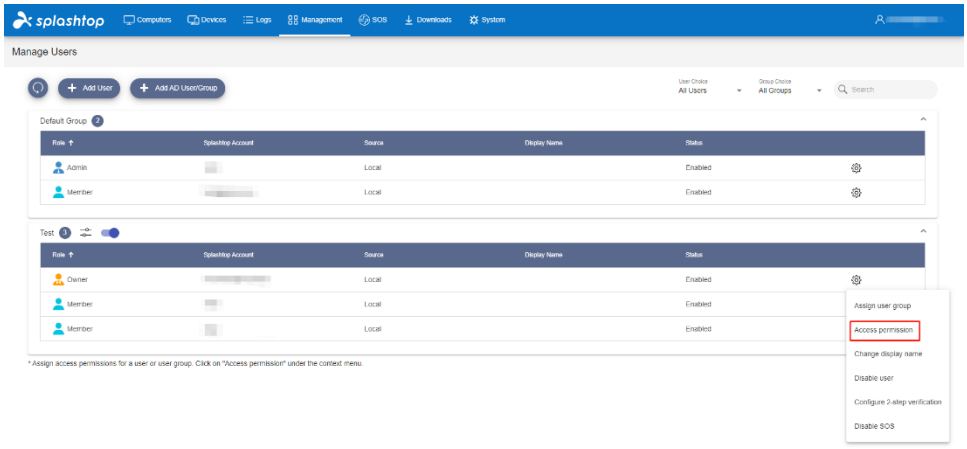
Where to configure access permissions

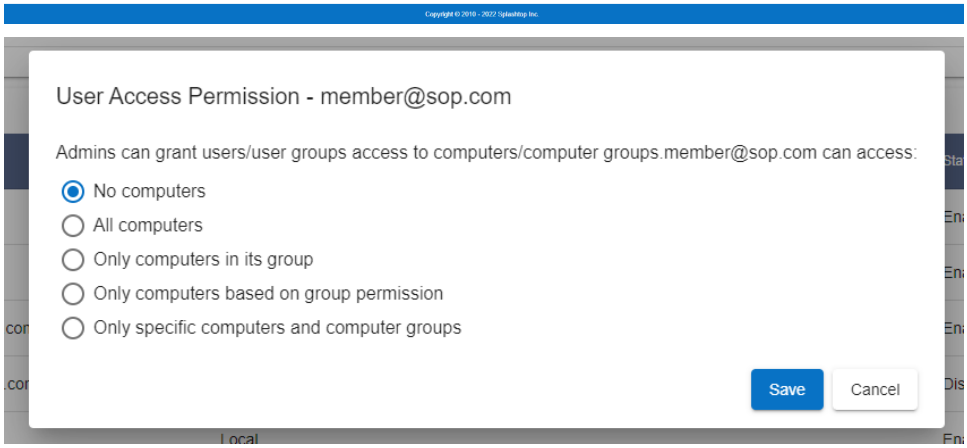
Log into your Gateway web console with the owner or admin account.

Navigate to web/management/users page, next to each user in the user list, click on the gear icon and choose Access permission. This is for setting the access permissions of this user.

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).





Access Permissions Options

Option 1 - No computers

The user will not be able to access any computers. This is the default option for a newly created user.

Option 2 - All computers

The user will be able to access all computers.

Option 3 - Only computers in its group

The user will be able to access computers assigned to the same group.

Option 4 - Only computers based on group access permission

Group access permission contains

- No Computers (within this group)
- Only computers in its group (within this group)
- Only Specific computers and computer groups (all groups)

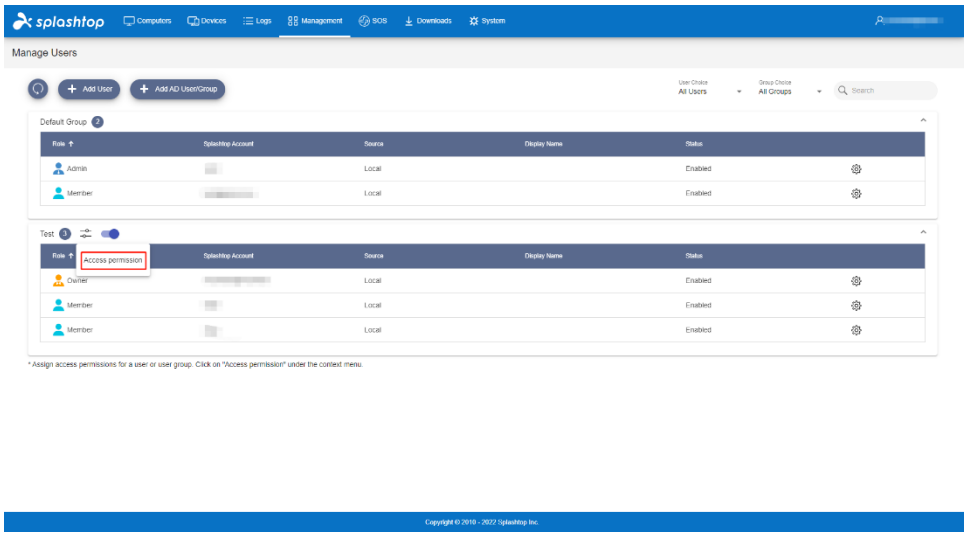
Option 5 - Only specific computers and computer groups

Splashtop is flexible enough to allow specific computers or a group of computers tied to specific users.

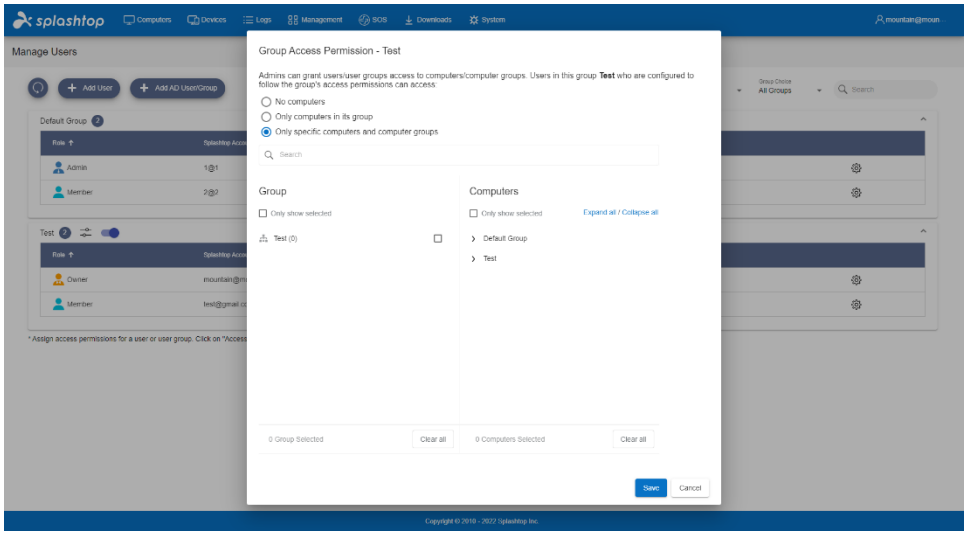
Meaning users can extend their access permission across all groups with more granular settings.

Group Access Permissions

If you want a group of 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.



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.



Granular feature control

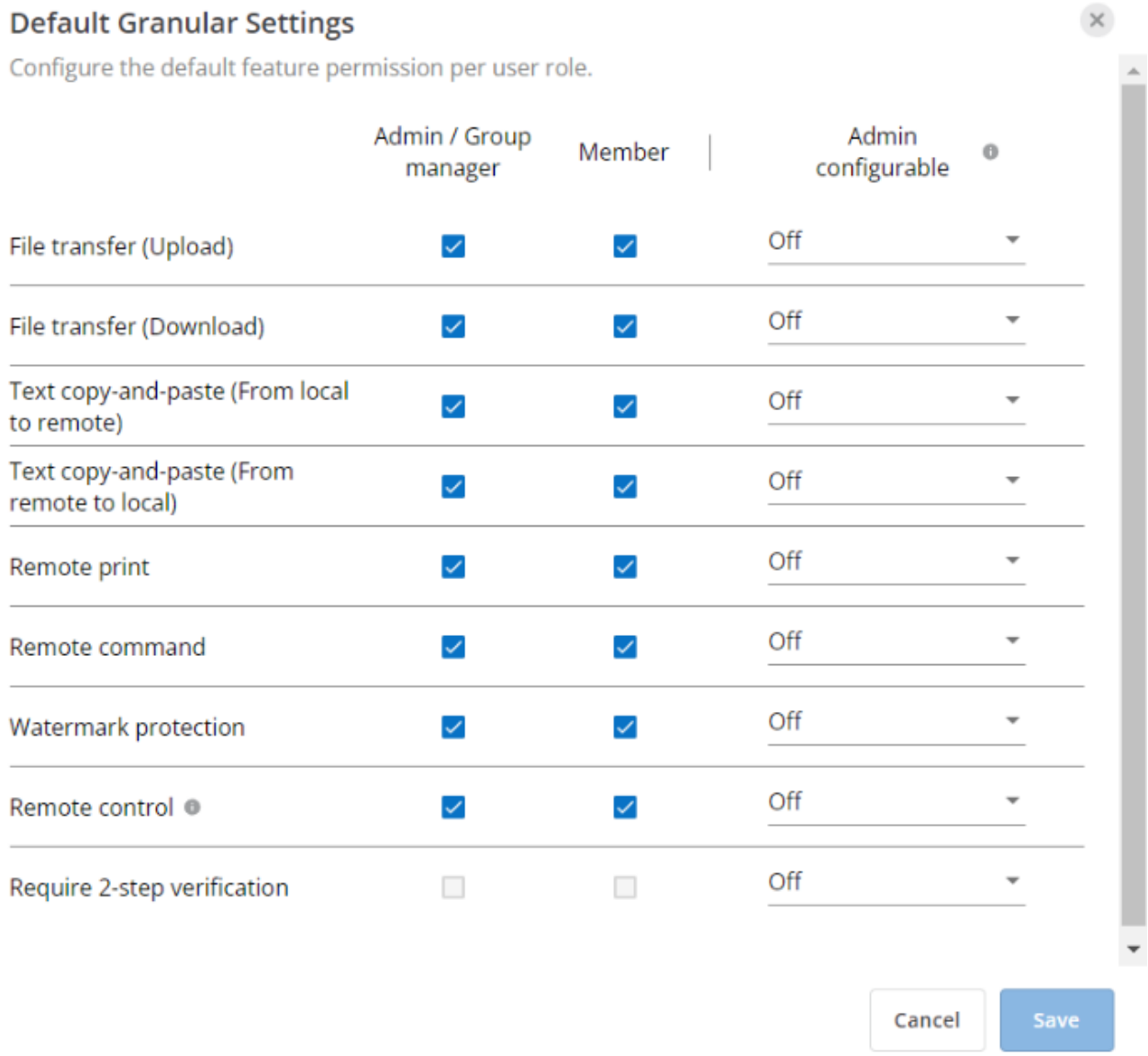
With Granular Control, you can take more control of the features on your team, and limit certain features to certain users or certain user groups.

Details:

- Splashtop On-Prem can now use our granular control features to specify which users on the team can use File transfer, Copy paste, Remote print, Remote command, Watermark protection, Remote control, and two-step verification.

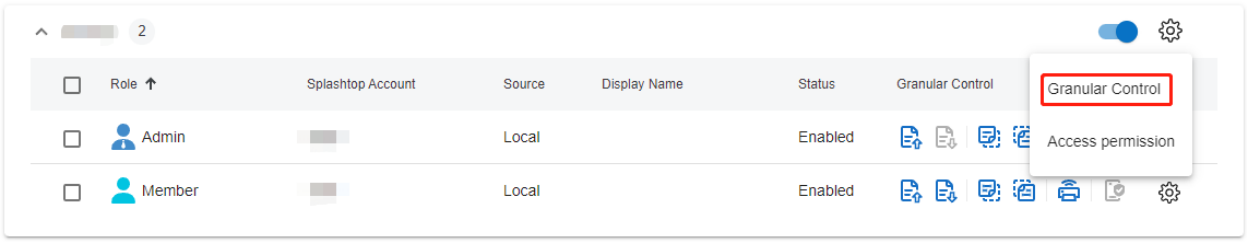
Default Granular Settings

- The Team Owner can configure the default feature permission per user role under **Management** → **Settings** under **Default Granular Settings**. This determines a user's default Attended Access permission when they are invited to the team (I.e., if Owner and Admin are checked under Default Granular Settings next to attended access, they will have attended access by default when first joining the team).
- **Configurable by Admin**: If this option is selected, this will grant Admins / Group managers the ability to configure Member's capability for the certain feature.

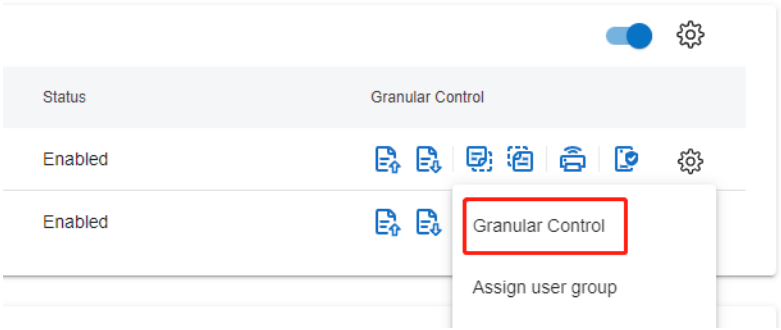


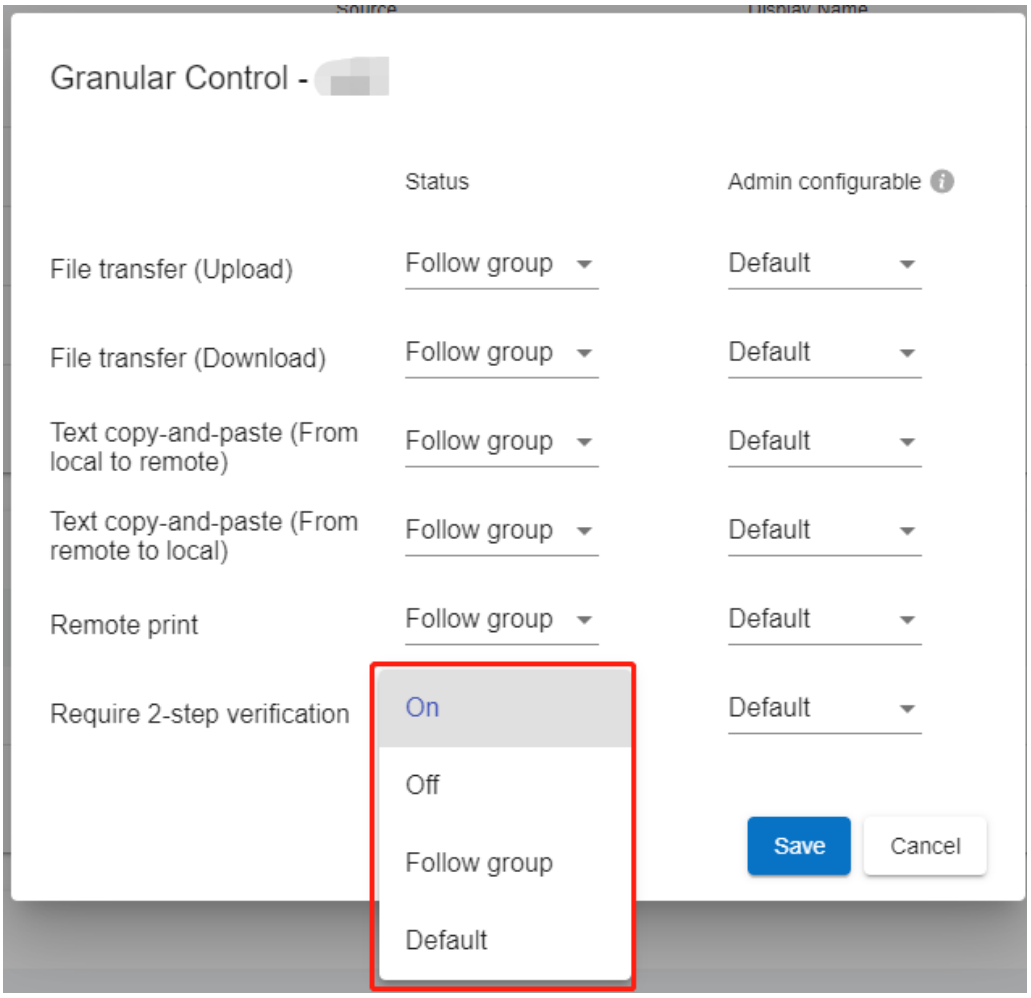
User Granular Settings

Under **Management** → **Users**, you can also configure Granular Control per group. Click the gear button to the right of the group's name and click "**Granular Control**".



To configure this per user, click the gear button next to the user's name and click "**Granular Control**".



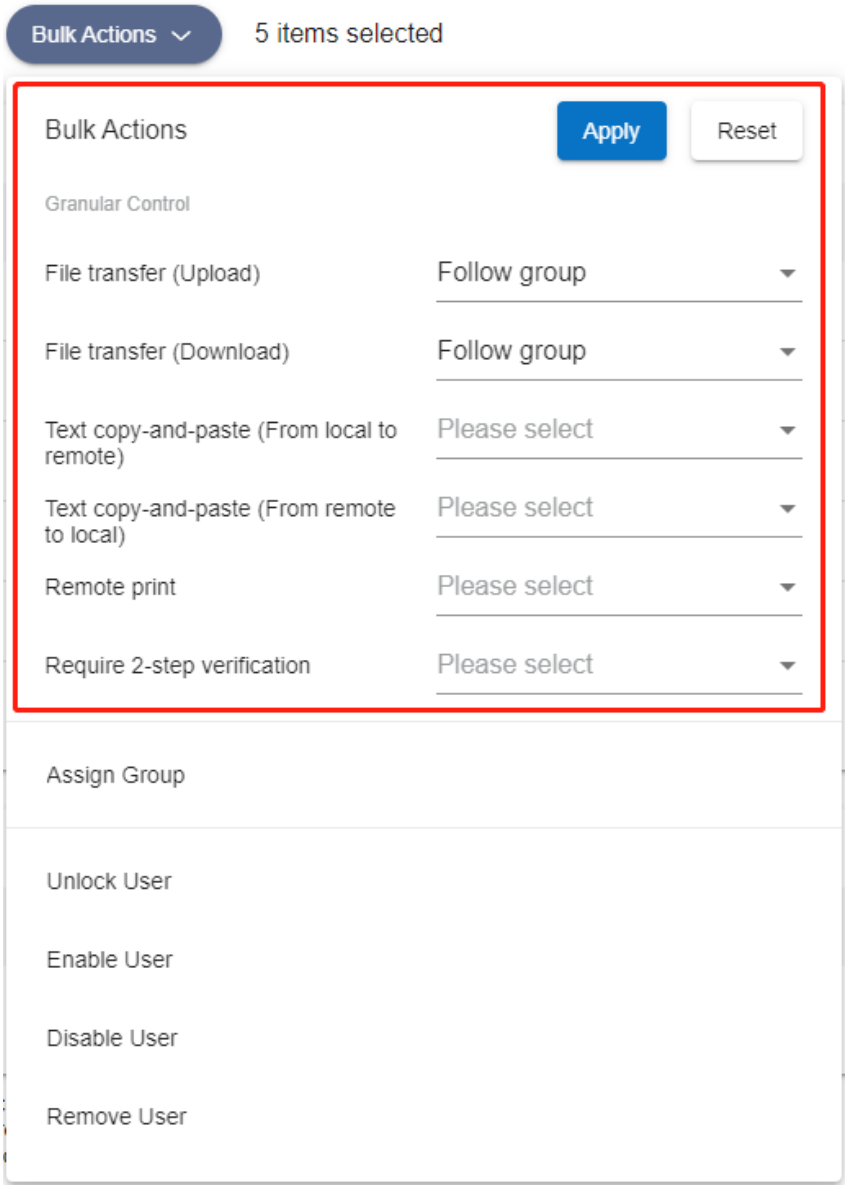


- **On**: This user will have access to the selected feature.
- **Off**: This user will NOT have access to the selected feature.

- **Follow Group**: Selecting this option will follow the group granular settings. To set the user group granular settings, click the gear button next to the Group name and select "**Granular Control**".
  - When adjusting the group setting, you can configure this option for the entire group to either On/Off or to follow the team default settings.
- **Default:** Selecting this option will follow the Default Granular Settings set under **Management** → **Settings**.

Bulk Actions

- Under **Management** → **Users**, you can also configure Granular Control by bulk actions.
- Select account by clicking on the checkboxes to the left of the account. Then click the Bulk Actions button to configure the granular control items for selected accounts.
- Click the Apply button to save the settings.



Set admin rights

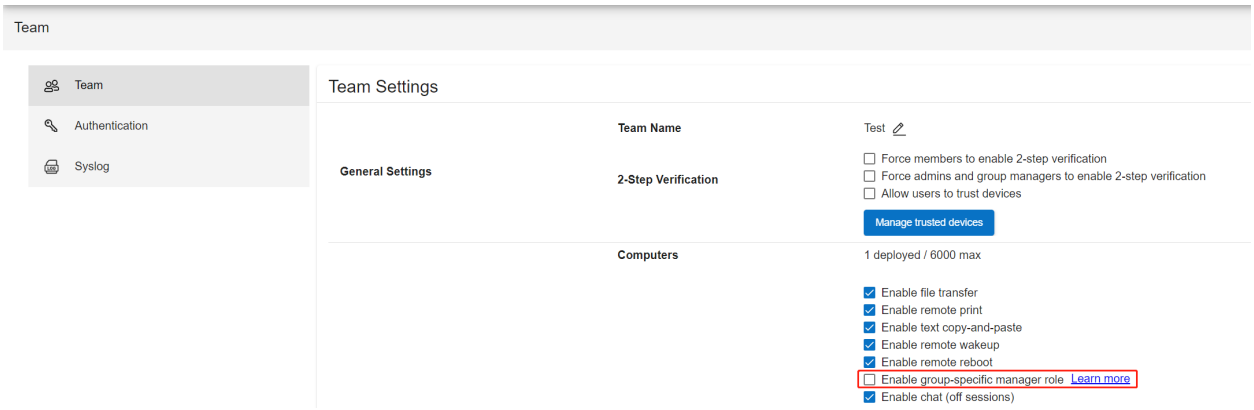
On Splashtop On-Prem, an Admin user can remotely access and **manage all computers by default**.

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

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

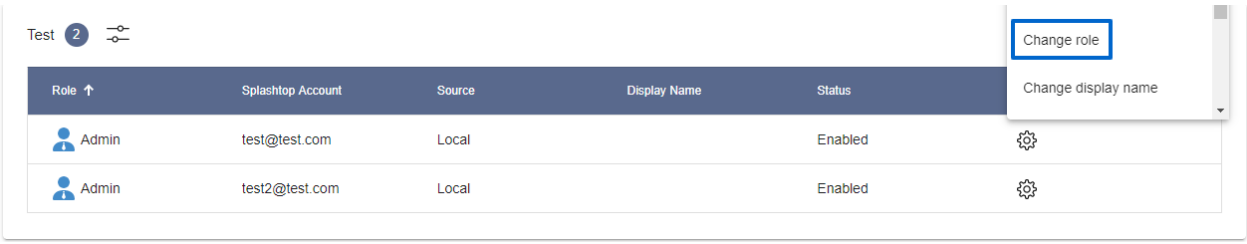
Enable group-specific manager feature

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



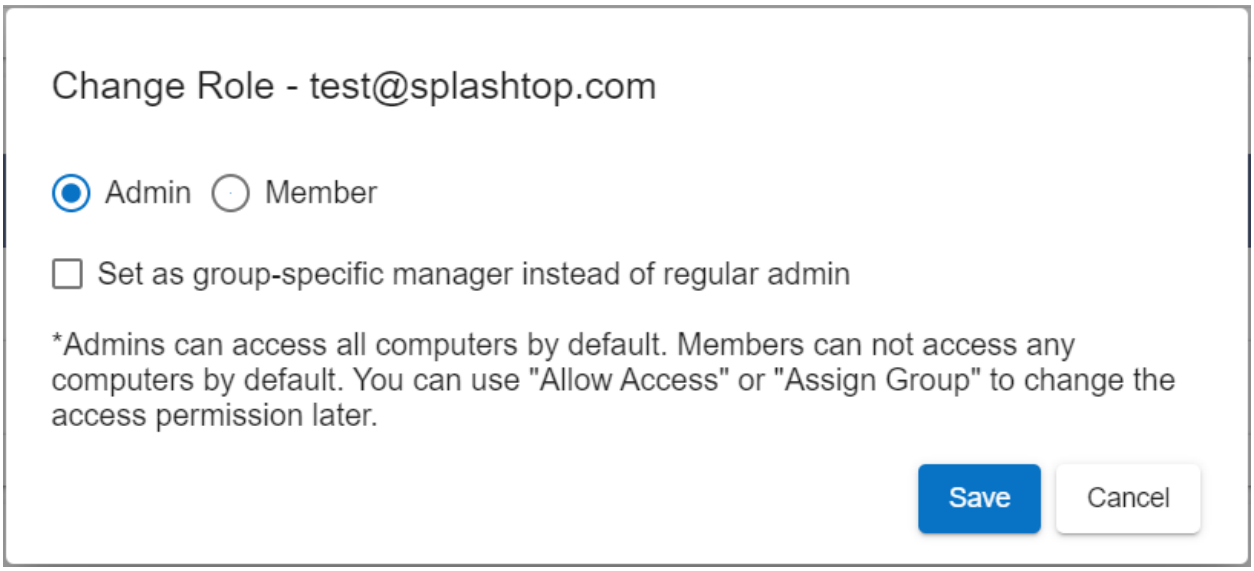
Set a user as a group-specific manager

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."



In the resulting dialog box:

1. Select the "Admin" radio button
2. Check the "Set as group-specific manager" checkbox
3. Select the checkboxes for whichever group(s) you want this user to manage

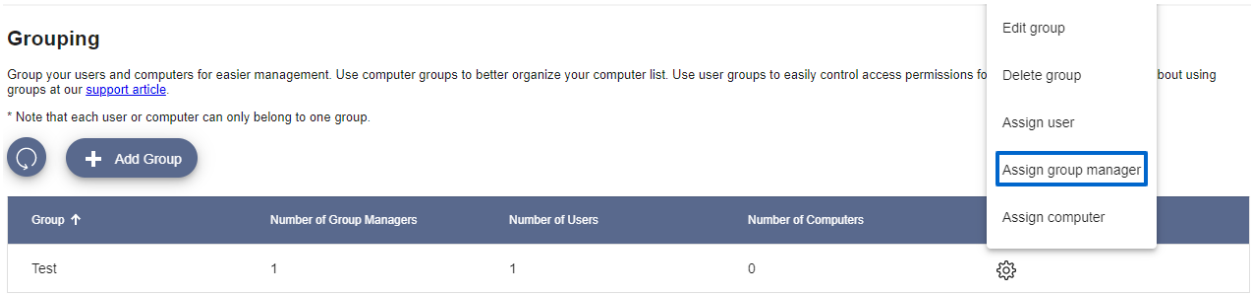


Another way to assign group-specific managers

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.



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.

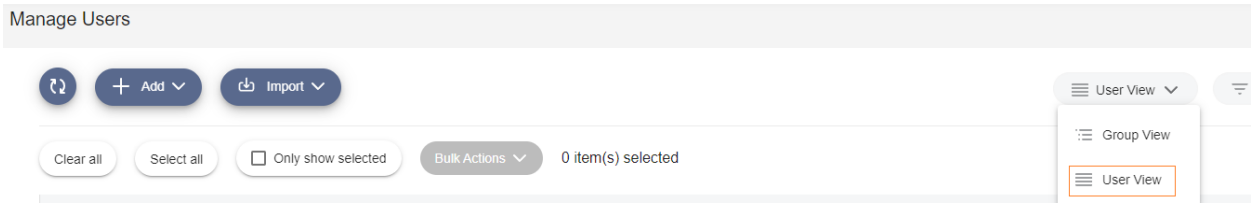
- Rename computer
- Add/edit computer notes
- Add/delete computers, including create deployment packages
- Create/enable/disable/delete users
- Set access permissions
- Configure user's 2FA (aka. MFA) and trusted devices

Notes

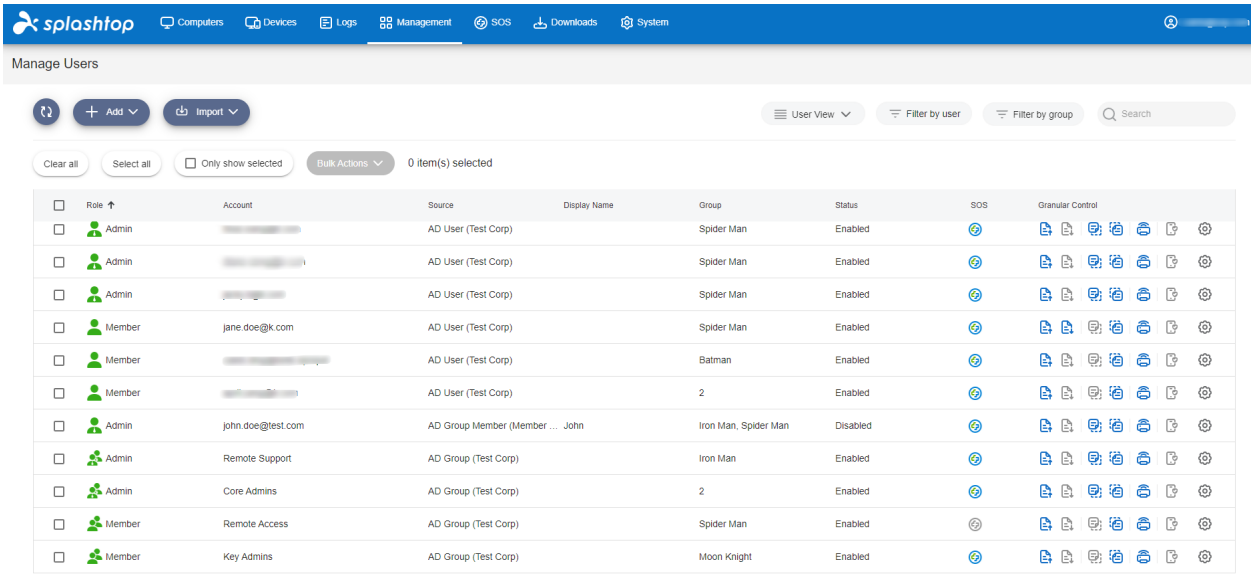
- When an admin is assigned to be a group-specific manager, the management scope is reduced from the whole team to only specific group(s).
- You can always see which users have been assigned group-specific manager rights by navigating **Management** > **Users**. The role for such users is labeled as "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.

Enable SOS for AD group members from user list

Since Gateway v3.20.0, the AD group members can be displayed all at once in user view.



Switching the view list from Group view to User view allows you to enable or disable SOS for AD group members.



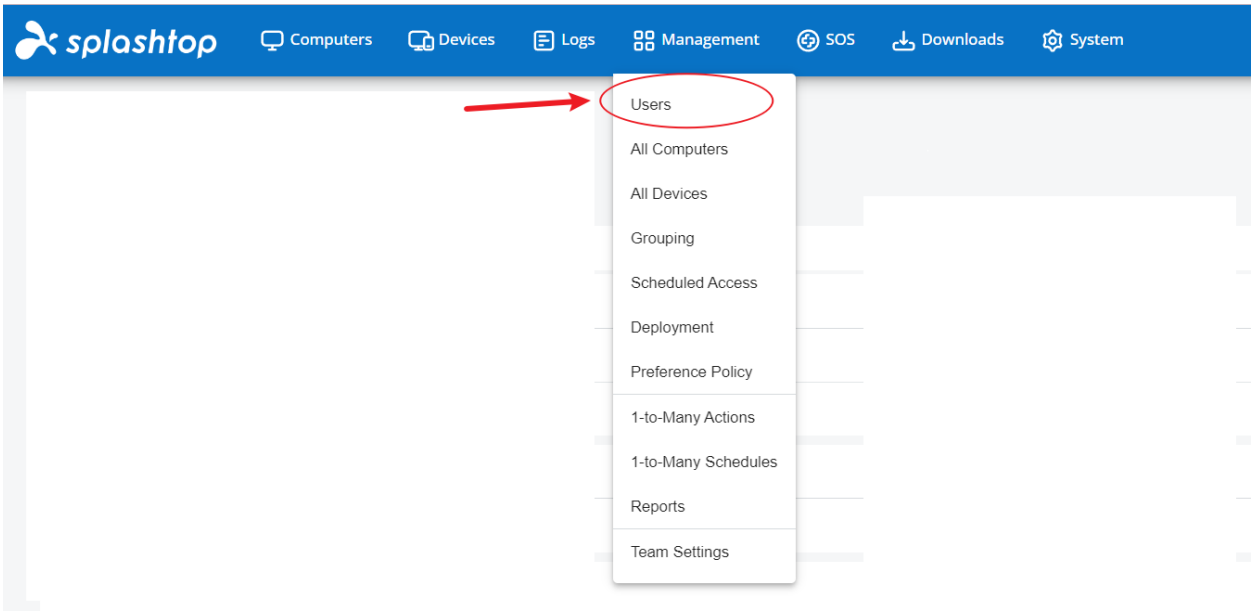
Note: Because a single AD group member can exist in different AD groups at the same time, the granular control settings for AD group member will be the merged results from those AD groups, it is not supported to configure these settings right from a single AD group member.

Export user list or access permission list

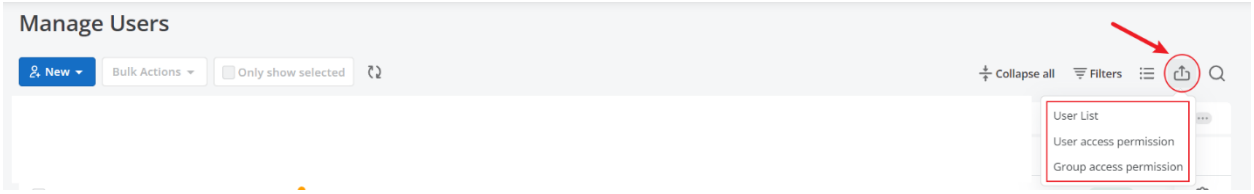
When you are managing several users on your team, you may want to export the user list or access permissions to maintain a record. The user list and access permissions can be exported as a CSV file.

Required Gateway version v3.28.2 or higher.

Login to Gateway web portal, then click the **Management tab**, then click the **Users** button.



If you click the Export icon**, and click the option in the droplist, you can download the user list, user access permission or group access permission as a CSV file.**



The User List's CSV file includes the Account, Group Name, Status, Role, etc.

	A	B	C	D	E	F
1	Splashtop Account	Group	Status (setting)	Status (result)	Source	Role
2		Default Group	enabled	enabled	Local	owner
3		a	enabled	enabled	Local	group_manager
4		c	enabled	enabled	Local	admin
5		Default Group	enabled	enabled	Local	member
6		b	enabled	enabled	Ad Group(	admin
7		Default Group	enabled	invalid	Ad Group	member

The User Access Permission's CSV file includes the Account, Role, Status, User Group Name, Access Permission, etc.

	A	B	C	D	E
1	Splashtop Account	Role	Status	User Group	Access Permission
2		admin	enabled	c	All computers
3		member	enabled	Default Group	No computers
4		admin	enabled	b	All computers
5		owner	enabled	Default Group	All computers
6		group_manager	enabled	a	All computers

The Group Access Permission's CSV file includes the Group Name, Access Permission, Computer Name, Computer Group, etc.

	A	B	C	D	E	F	G
1	Computer Name	Host Name	UUID	Type	Pool Size	Group Name	Operating System
2	rds - 2	rds - 2		RDP		Default Group	Microsoft Windows
3	rdp	rdp		RDP		Default Group	Microsoft Windows
4	rds - 1	rds - 1		RDP		Default Group	Microsoft Windows
5	rdspool	rdspool		RDS pool	2	Default Group	
6	Macmini	Macmini		Computer		Default Group	macOS Ventura 13.3.1

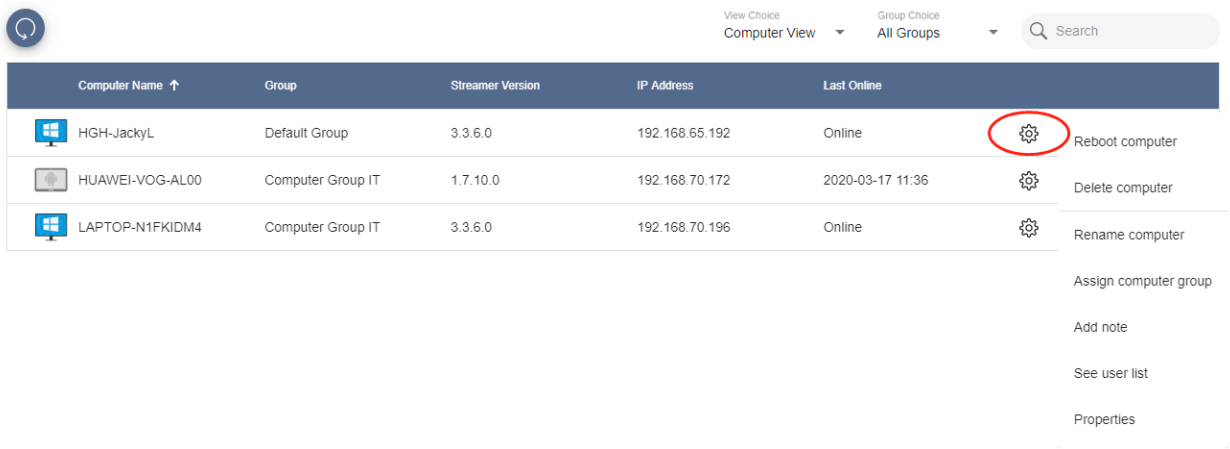
Computers

With **All Computers** page, an administrator can have an overview of the registered computers with the Splashtop Gateway. A computer is considered "registered" in the Gateway after applying a deployment package or manually installing Streamer and granting access.

You can choose to display the computers in list view or in group view and you can select to show a specific computer group only.

Manage a Specific Computer

An administrator can remotely manage a specific computer by clicking the gear icon at the end of its row.

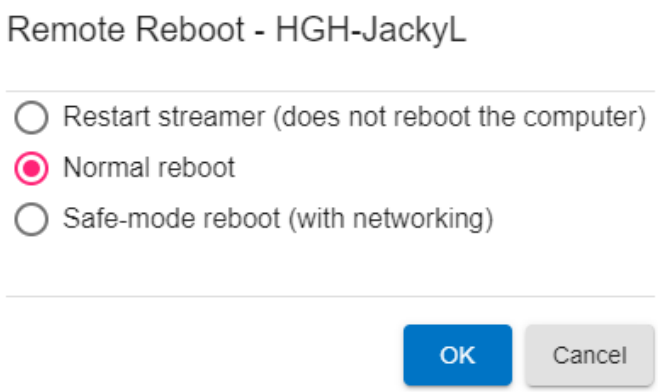


Functions include:

- Reboot computer
- Delete computer
- Rename computer
- Assign computer group
- Add note
- See user list
- See properties

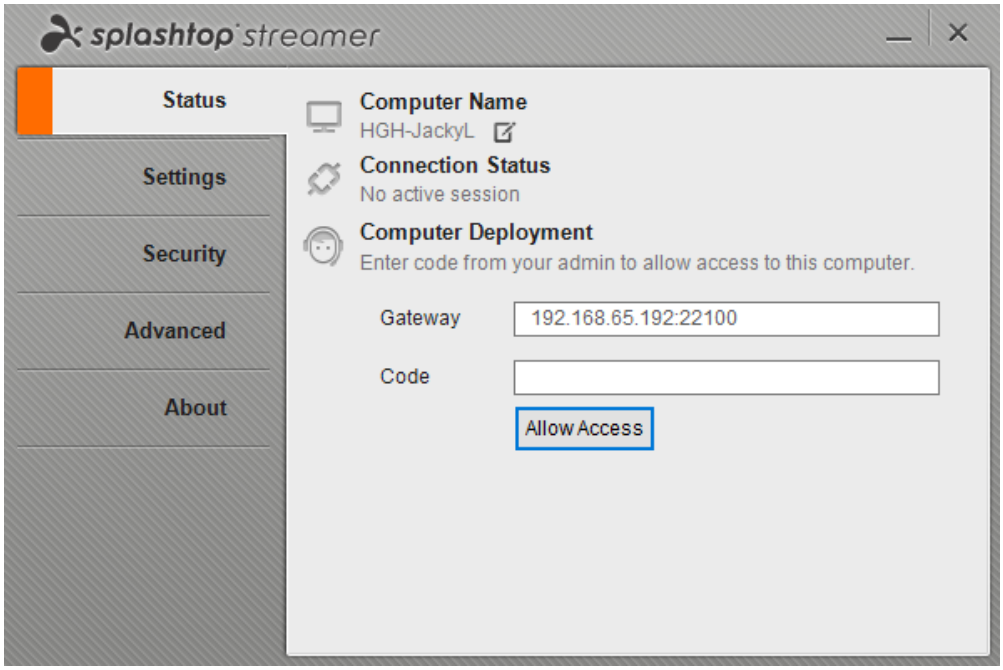
Reboot computer

Administrator can remotely restart the Streamer, and perform a normal computer reboot or a safe-mode reboot with networking.



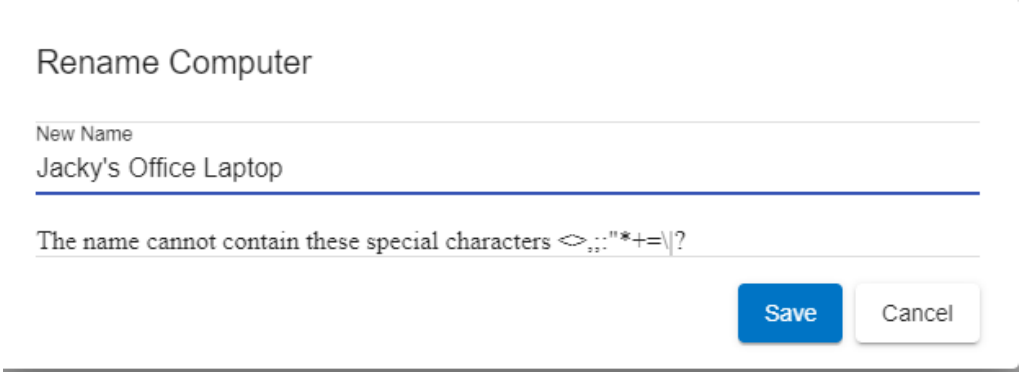
Delete computer

Administrator can remove the computer from the Gateway by logging out the Streamer. Once a computer is deleted, the Streamer of that computer must re-grant access using the deployment code in order to register again in the system.



Rename Computer

Administrator can assign a customized name for the computer.



Assign computer group

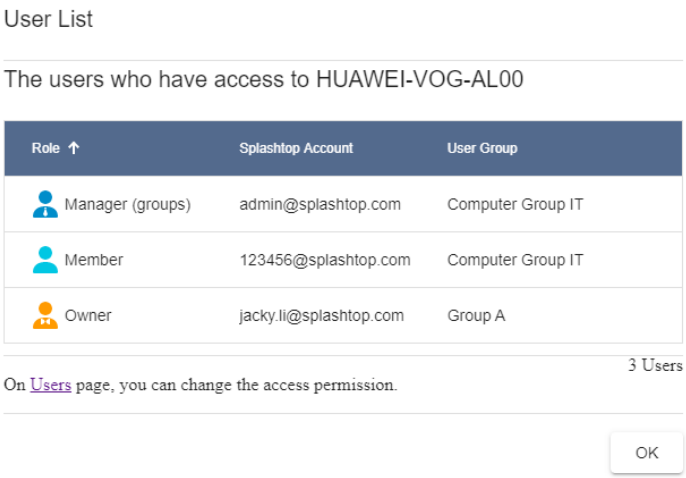
Administrators can assign the computer to a group to inherit the access permission of the group.

Add note

A note field available to add description to the computer.

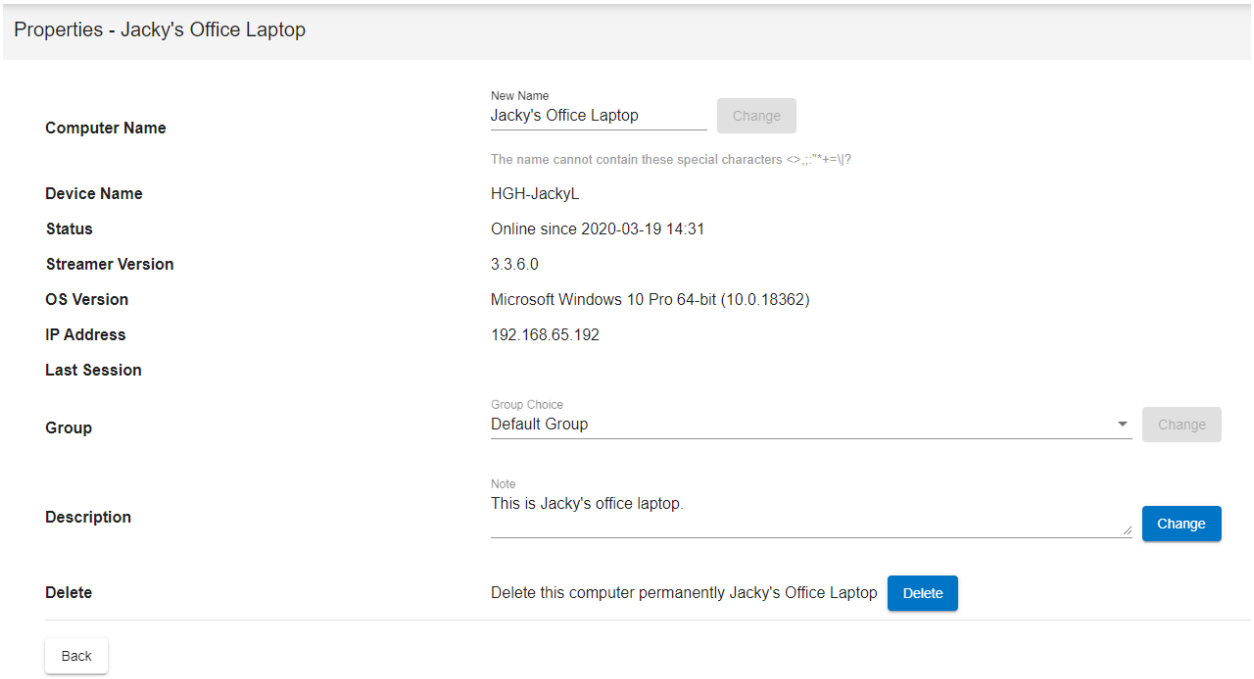
See user list

Administrators can check the list of users that have access permission to this computer.



See Properties

This page displayed the properties of the computer.

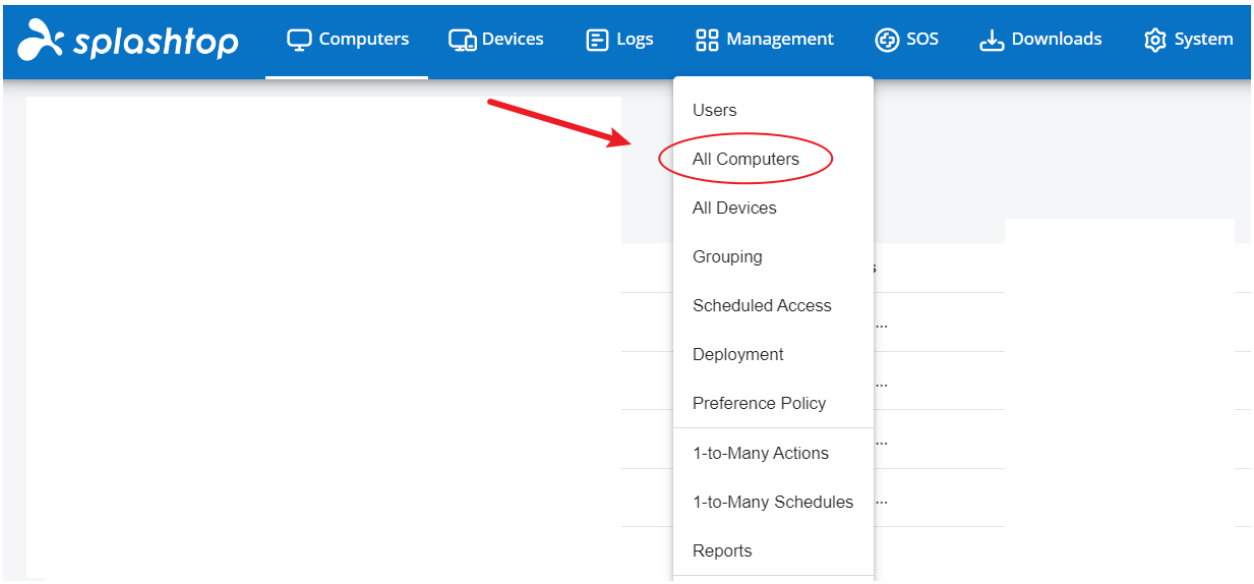


Export and save a copy/record of the computer list

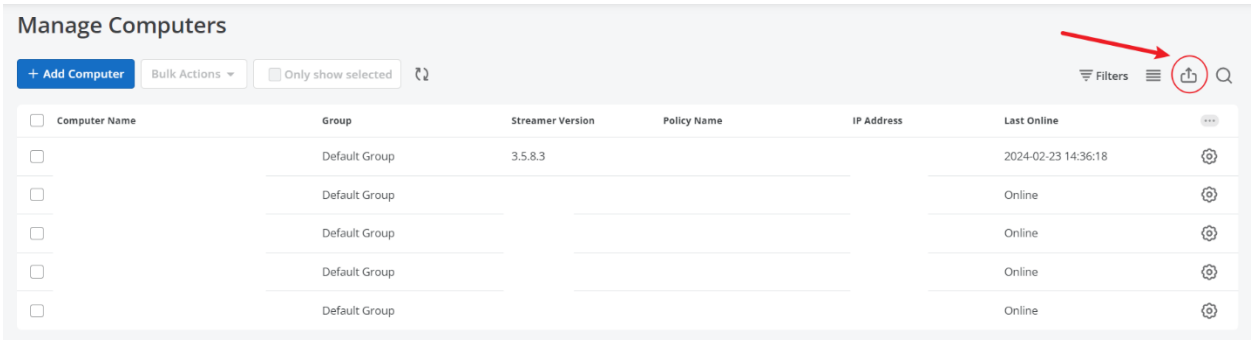
When you are managing several computers on your team, you may want to export the computer list to maintain a record. The computer list can be exported as a CSV file. The Computer List's CSV file includes Computer Name, Host Name, Group Name, OS, etc.

Required Gateway version v3.28.2 or higher.

Login to Gateway web portal, then click **Management** tab, then click the **All Computers** button.



If you click the **Export icon**, you can download the computer list as a CSV file.



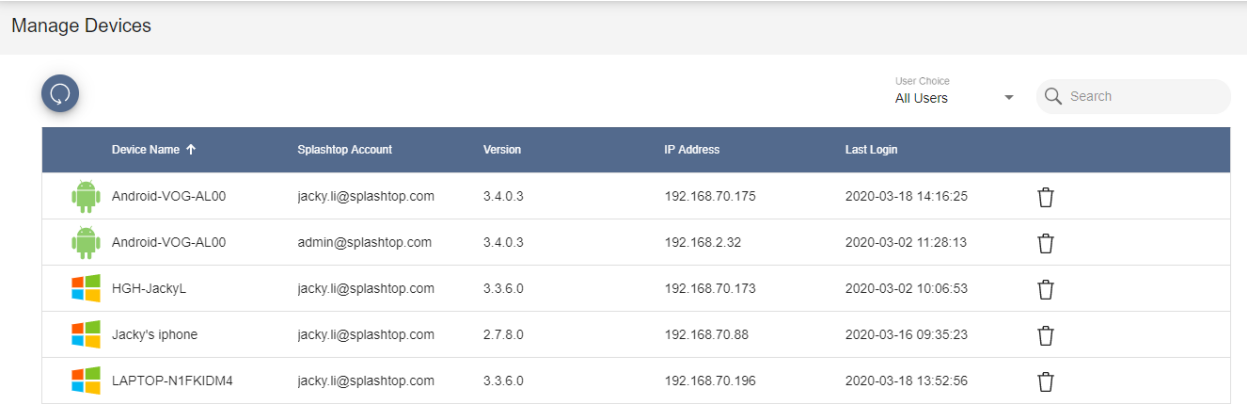
The CSV file includes Computer Name, Host Name, Group Name, OS, etc.

	A	B	C	D	E	F	G
1	Computer Name	Host Name	UUID	Type	Pool Size	Group Name	Operating System
2	rds - 2	rds - 2		RDP		Default Group	Microsoft Windows
3	rdp	rdp		RDP		Default Group	Microsoft Windows
4	rds - 1	rds - 1		RDP		Default Group	Microsoft Windows
5	rdspool	rdspool		RDS pool	2	Default Group	
6	Macmini	Macmini		Computer		Default Group	macOS Ventura 13.3.1

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.



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

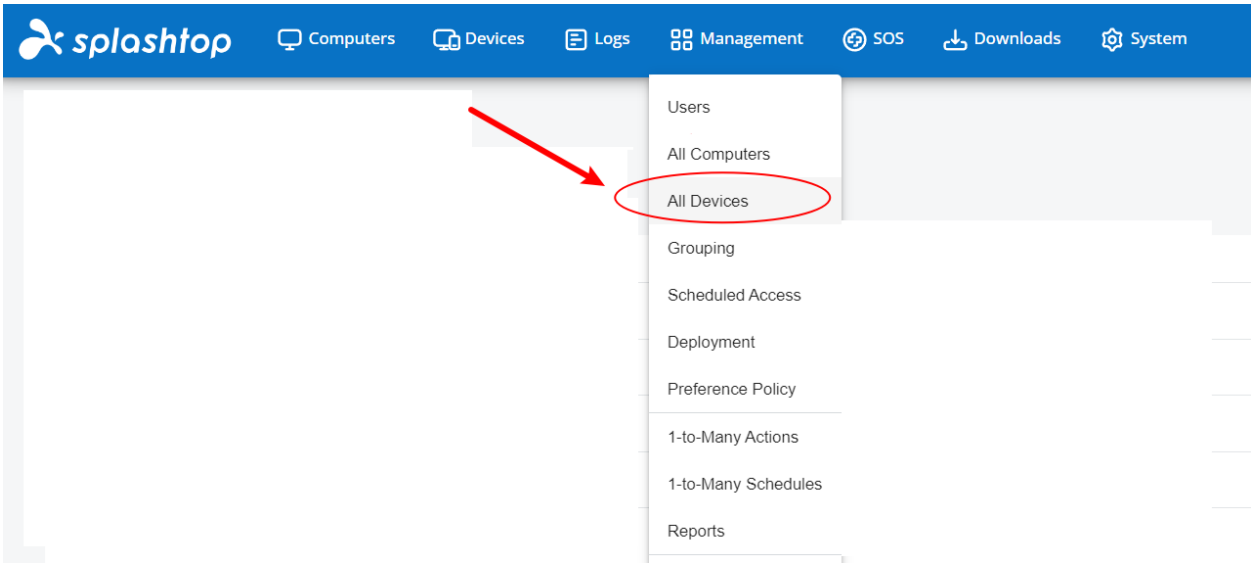
You can choose to delete a device by clicking on the Bin icon at the end of each row.

Export the device list

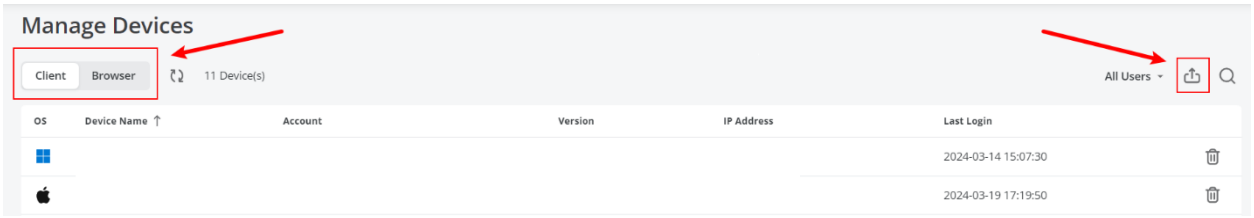
When you are managing several devices on your team, you may want to export the device list to maintain a record. The device list can be exported as a CSV file. The Device List's CSV file includes Device Name, Platform, Account, Version, etc.

Required Gateway version v3.28.2 or higher.

Login to Gateway web portal, then click **Management** tab, then click the **All Devices** button.



Firstly, you can choose the Client tab or the Browser tab, then click the Export icon. **You can download the client list or browser list as a CSV file.**



The CSV file includes Device Name, Platform, Account, Version, etc.

	A	B	C	D	E	F
1	Device Name	Platform	Account	Version	IP Address	Last Login
2		Browser		3.6.8.0		2/27/2024 11:13
3		Windows		3.6.8.0		3/14/2024 15:07
4		Browser		3.6.8.0		3/7/2024 17:51
5		Browser		3.6.8.0		3/4/2024 21:48
6		Browser		3.6.8.0		3/11/2024 14:28
7		MacOS		3.6.8.0		3/22/2024 17:32

Grouping

Manage 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 logging in 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 creating 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.

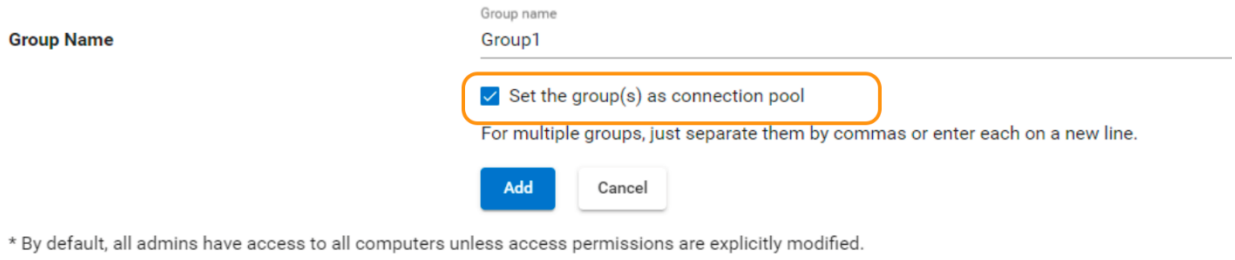
Connection pool

Connection pool allows user to connect to the remote computer by just clicking the Connect button under the group section, rather than expanding the group and select one particular computer to connect, which provides convenience when user don't need to care which computer it will connect to, like the following scenarios: When connecting to a RDS server through Splashtop Connector, Splashtop Connector will fork virtual computers per the profile's pool size definition.

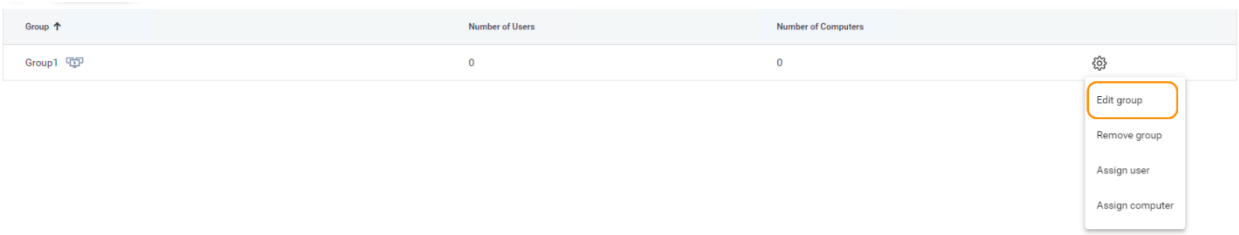
Connection pool works not only with RDS setup, but also physical computers setup, as long as the group is enabled as connection pool, Gateway will regard all the computers inside the group as the pool.

Steps to setup Connection pool:

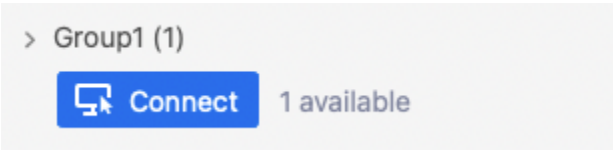
1. When you are creating a group in Management -> Grouping -> Add Group, you can check Set the group as connection pool option.



For existing group, you can click the gear button in the group list, choose "Edit group" and enable the option.



2. And then on user's On-Prem client app, there will be Connect button appear under the group, user can click Connect to connect a Gateway assigned computer

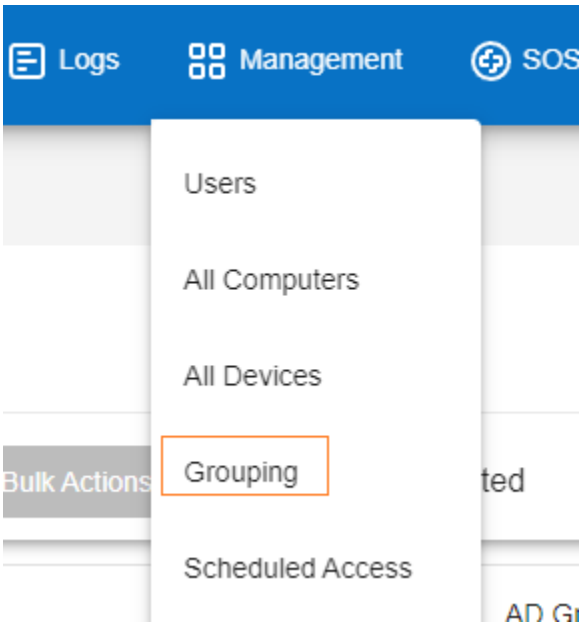


Notice: Please enable Allow members to see groups option in Team Settings to make sure user can see the group. (Management -> Team Settings)

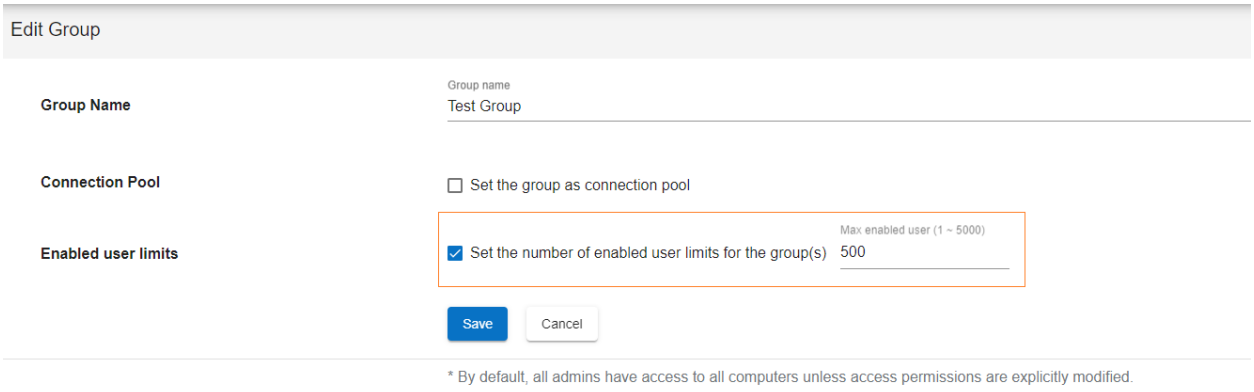
Group user limits

Define a max user number for groups could be useful if your Gateway groups are designed to be isolated from each other, and IT admin would like to have better control over license seat management.

1. Go to Management/grouping



2. Set a user limit number and apply to the group by enable the checkbox and save.



3. Below actions will be blocked when trying to break the limits.

- Adding new users to a group
- Moving users between groups
- Enabling users (in the 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.

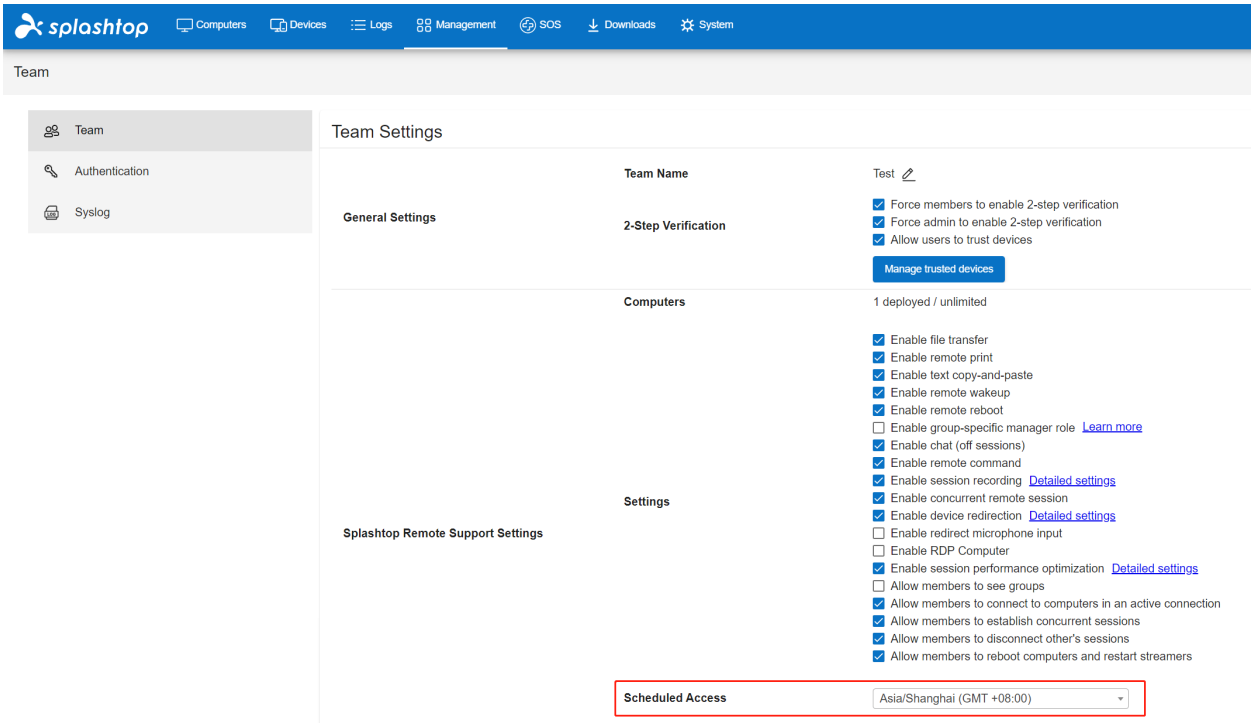
Notes and Best Practices

- 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.

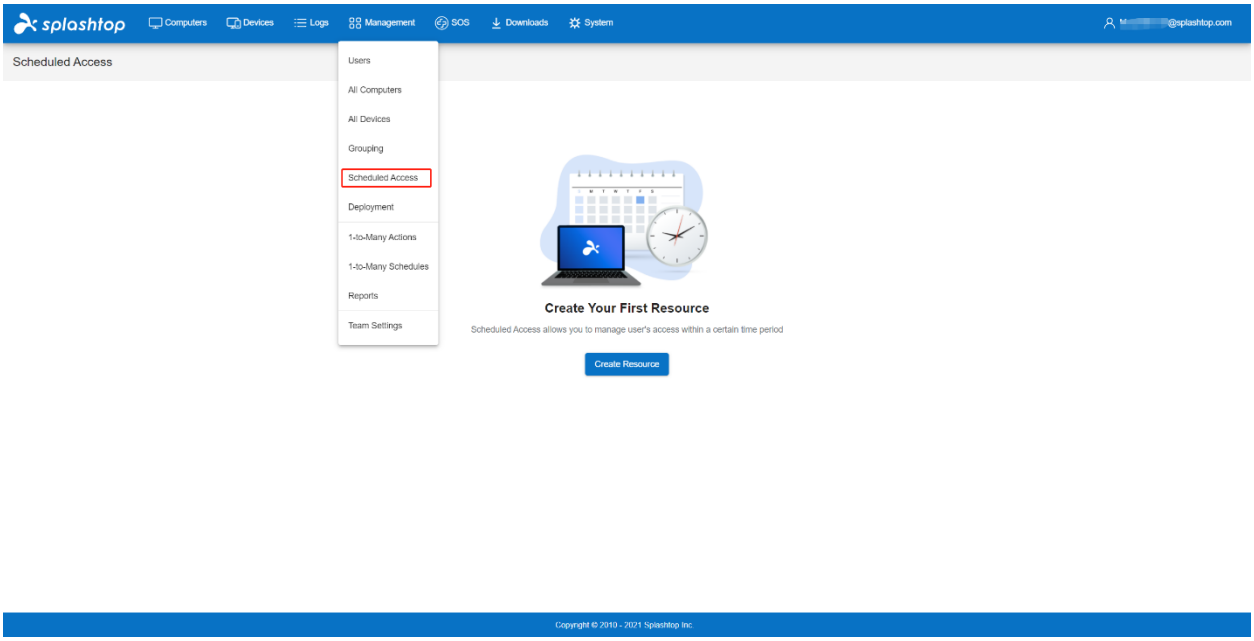
- The Team Owner and Admins can use the Scheduled Access feature.
- For open lab hours, create a separate schedule and configure a timeslot for it. For example, 0:00 – 9:00, include all groups of members. 17:00 – 23:59 another timeslot and include the group of members.
- To receive the proper disconnect warning messages, it 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

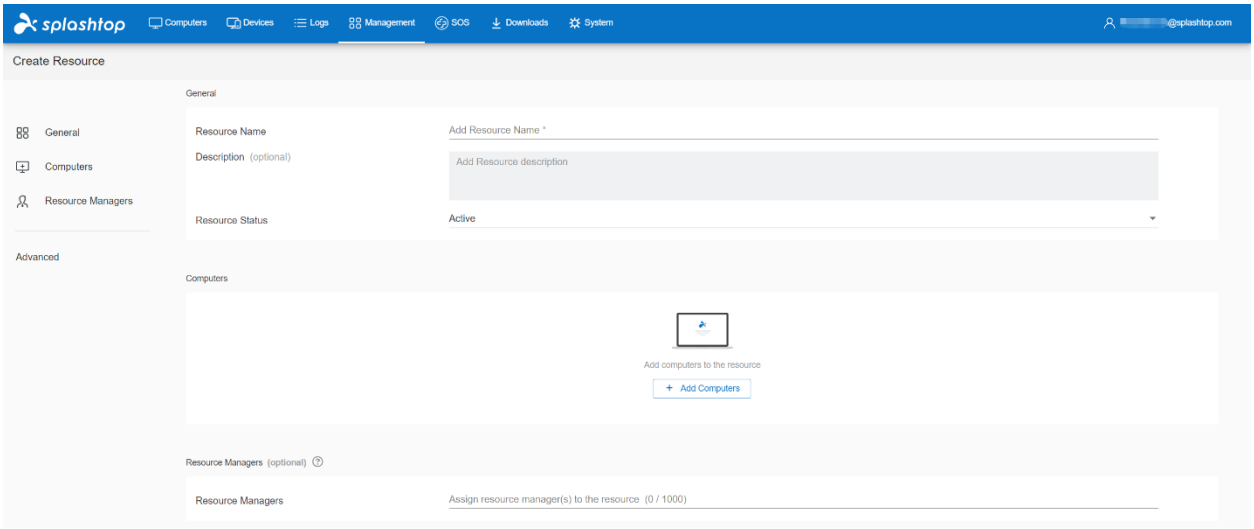
1. Before creating any new schedules, go to *https://{gatewayaddress} -> Management -> Settings* to configure the **Scheduled Access timezone**. Timezone cannot be changed when a schedule is in place. Only the team owner has access to this setting.



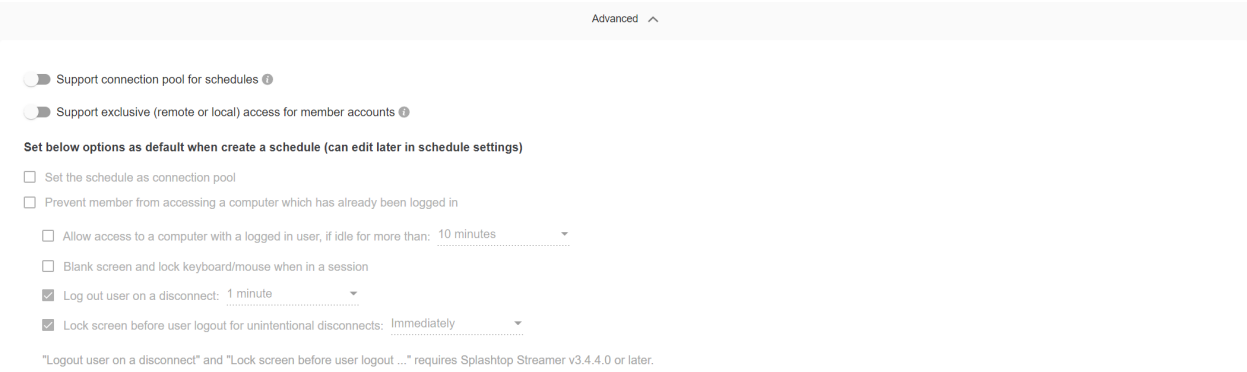
2. Go to *https://{gatewayaddress} -> Management -> Scheduled Access*



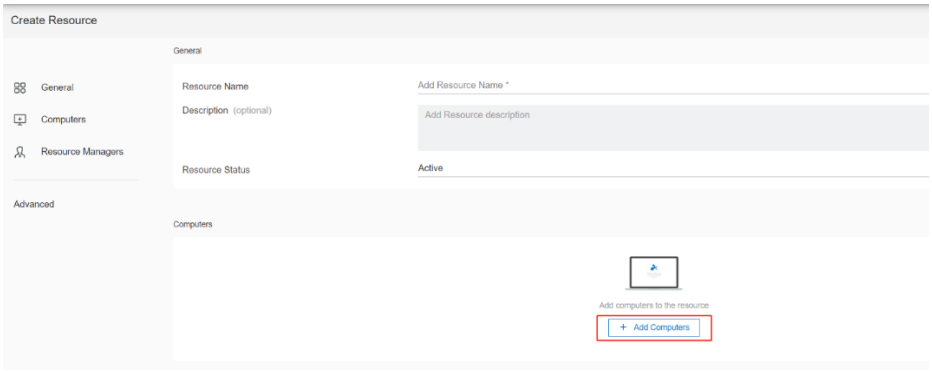
3. Click "Create Resource" and fill in the fields. The resource will contain what set of computers will be scheduled for access, such as a specific computer lab.

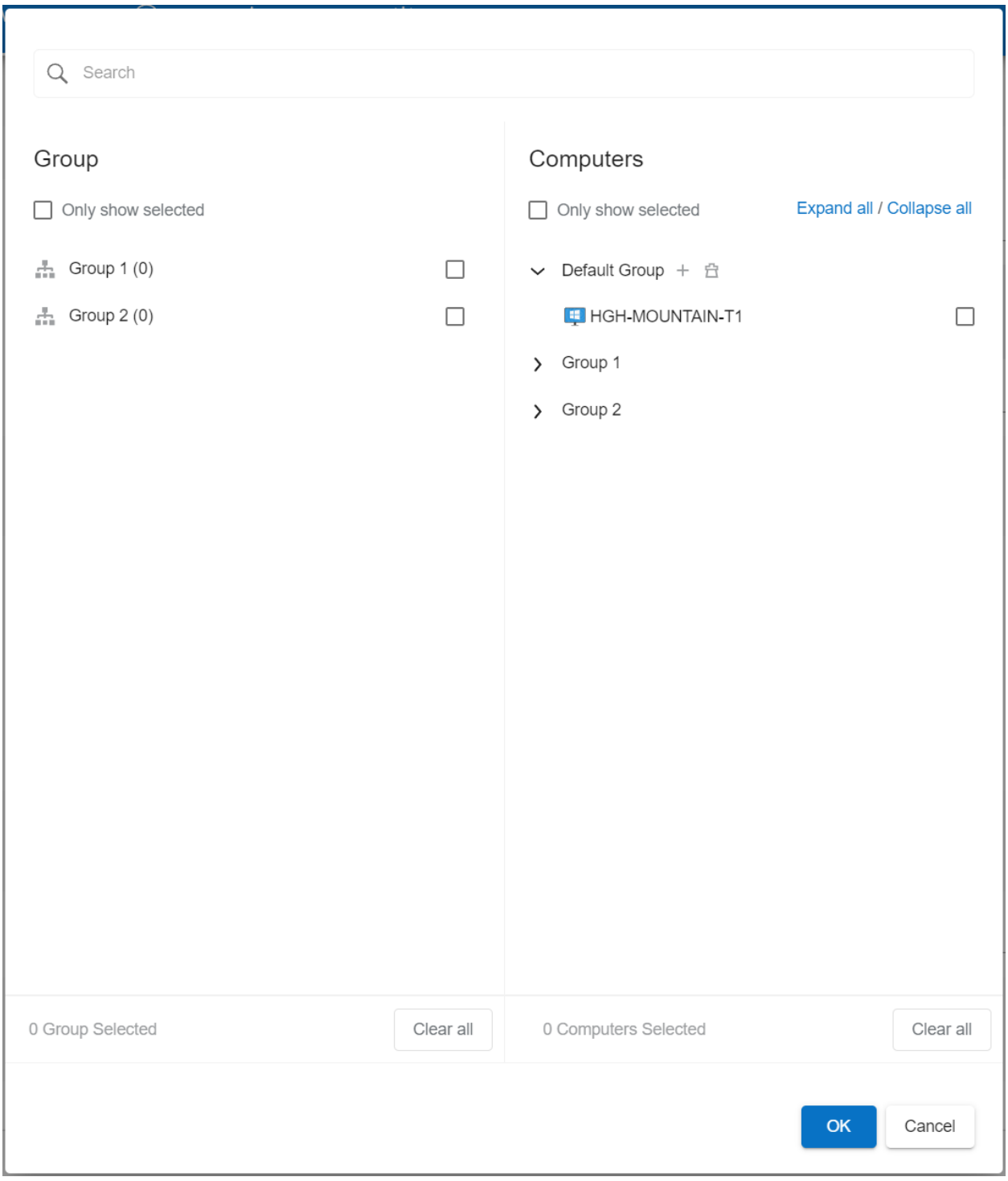


4. Click "Advanced Settings" to enable support for Exclusive Mode. This setting prevents a remote user from accessing a computer if there is a user logged into the operating system. This helps with preventing users from connecting to a computer that is in local use. The logout and lock screen settings also help for cases where students forget to log out of their OS accounts.

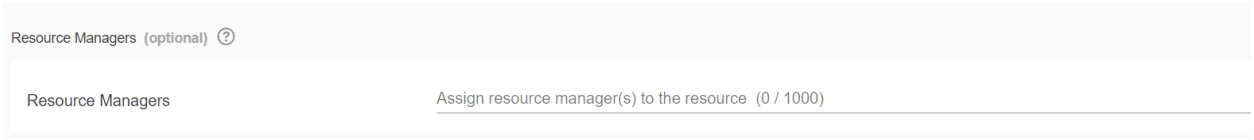


5. Select the computers or computer groups that you would like to make available in the resource.

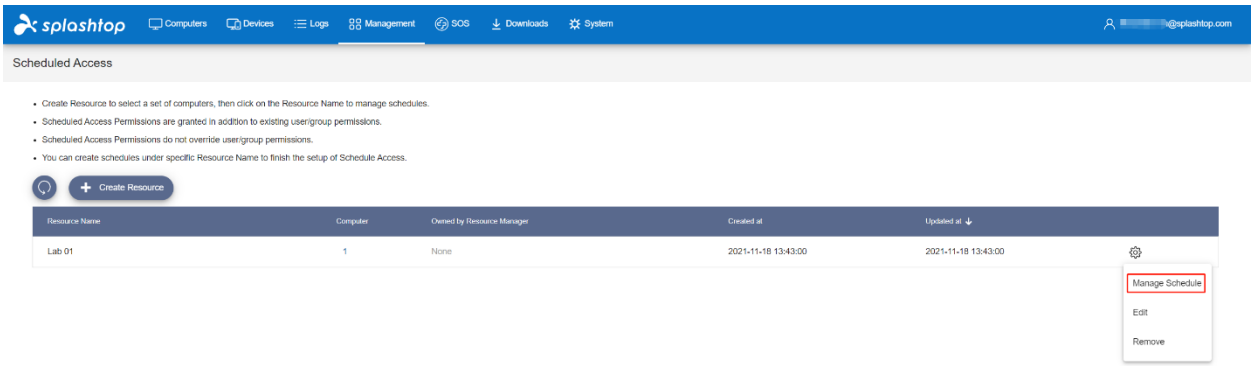


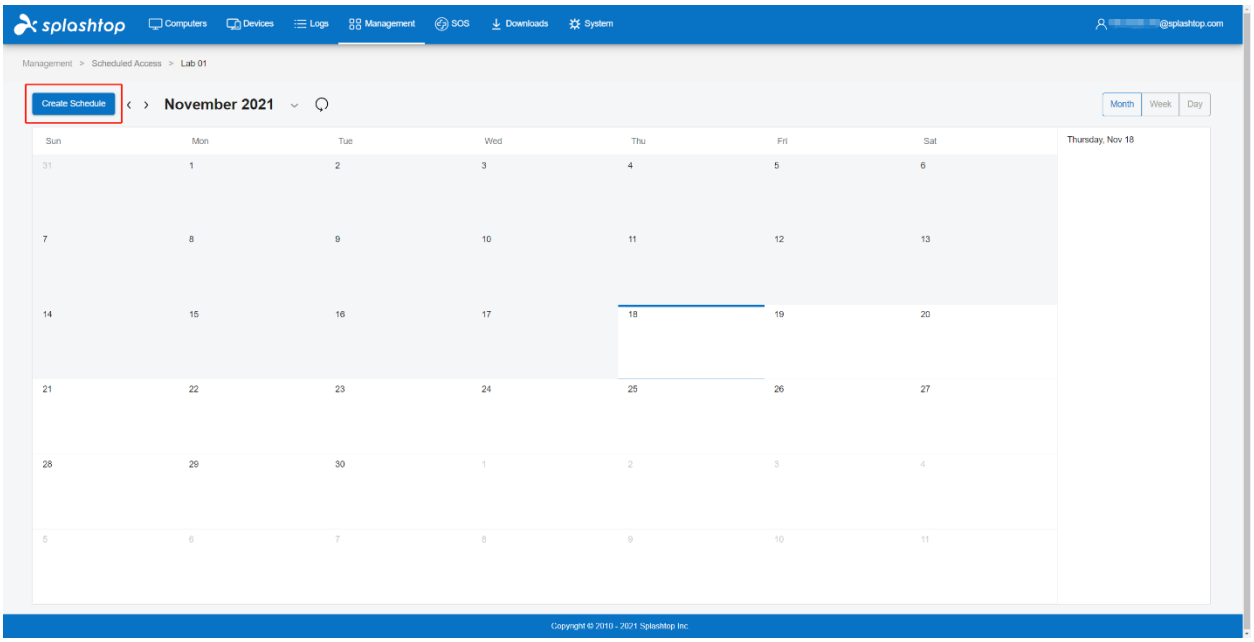


6. (Optional) Assign a Group Admin to help with managing schedules on the resource. Group admins also have the capability to create resources and schedules.

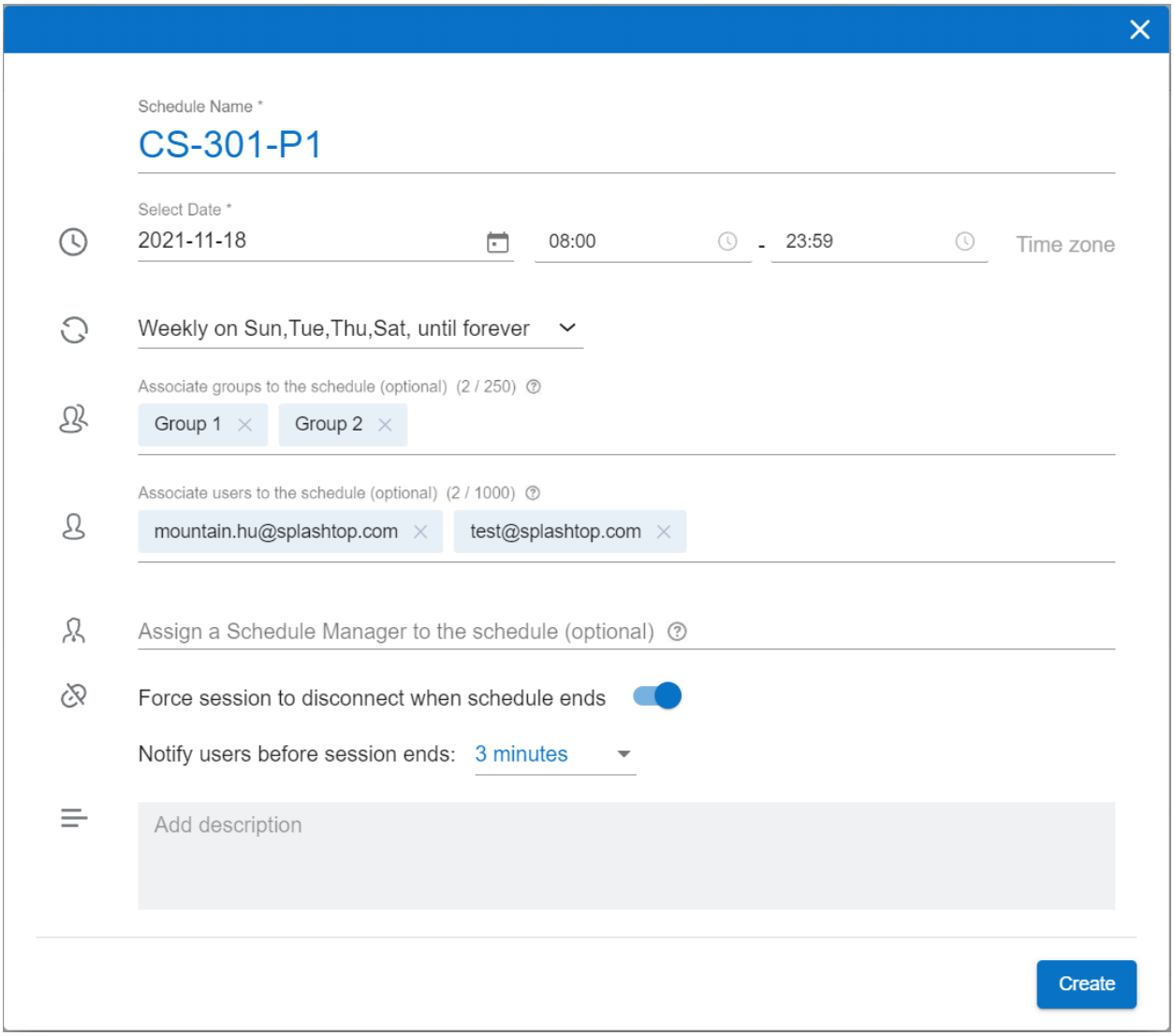


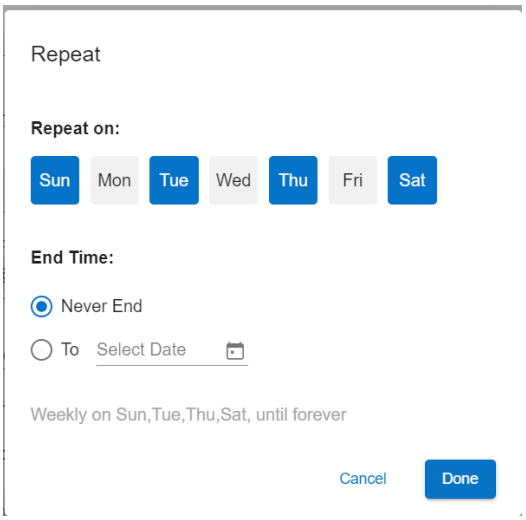
7. Click Manage Schedule from context drop-down menu (Gear Button) to assign Schedules to the resource.





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.

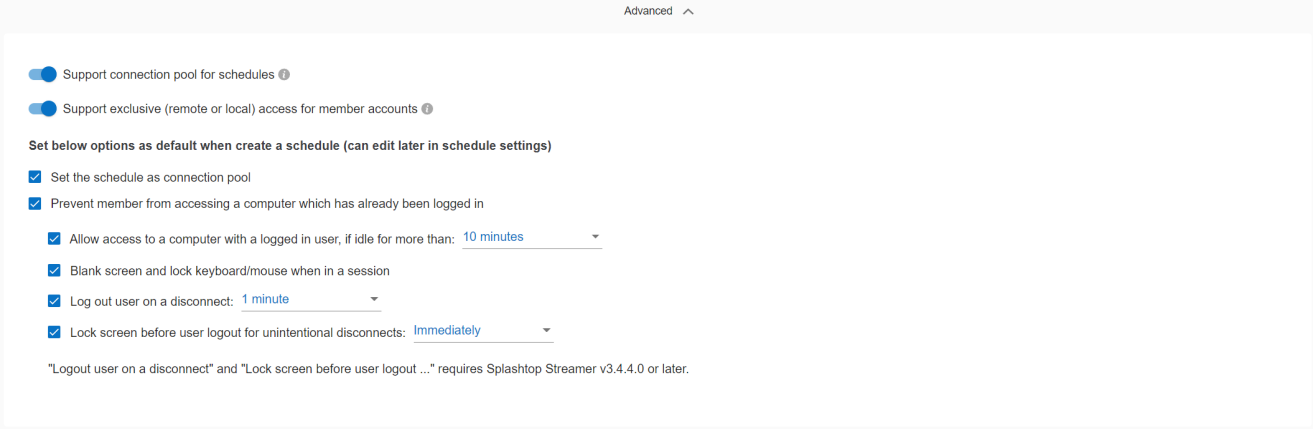




Check "Force session to disconnect when schedule ends" if you would like sessions to forcefully disconnect at the end of the timeslot. Note: This does not log out of the remote computer's user account.

Exclusive mode:

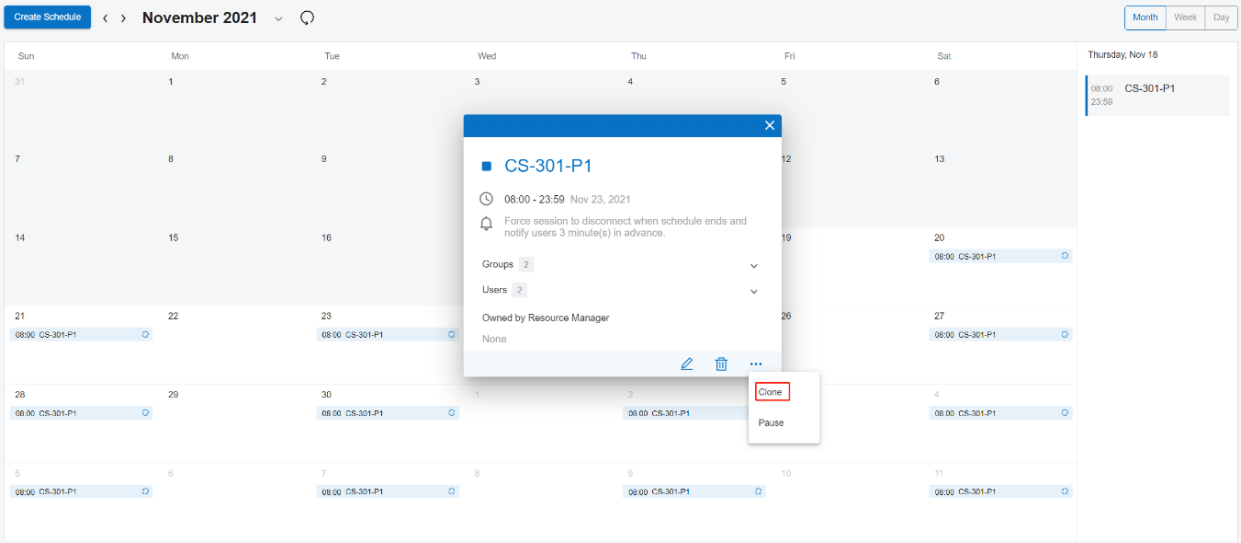
Click "Advanced Settings" to turn on/off exclusive access



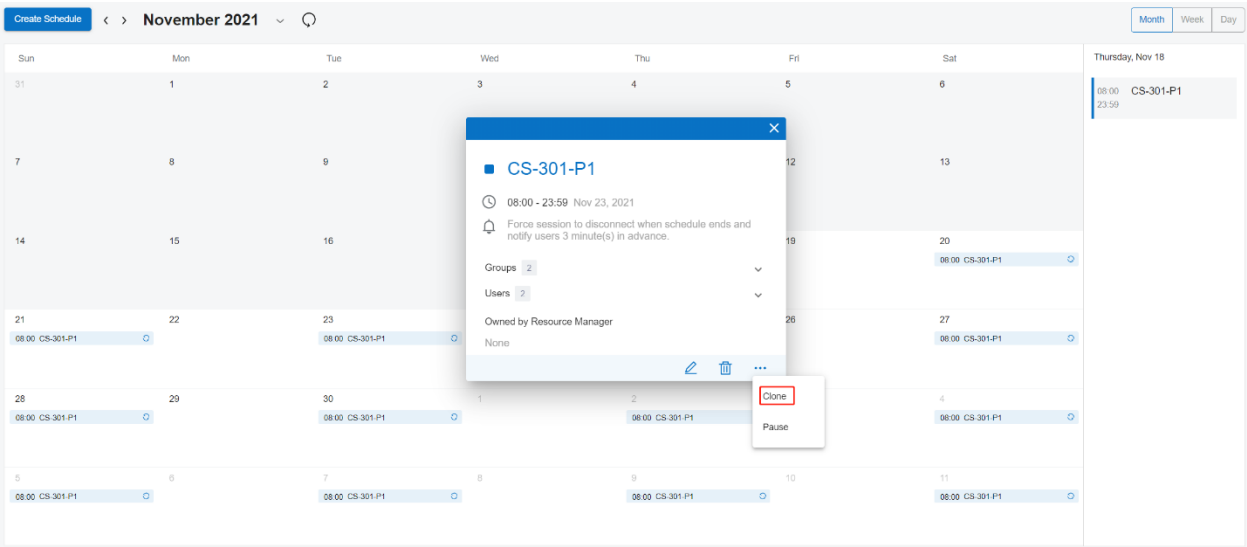
Allows computers that are part of this schedule to be accessed only if the computer is currently at the Windows/Mac Login screen, making the computer exclusive for the user that is currently logged in to the Operating system using the computer. Applies for users either present at the lab or remotely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



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

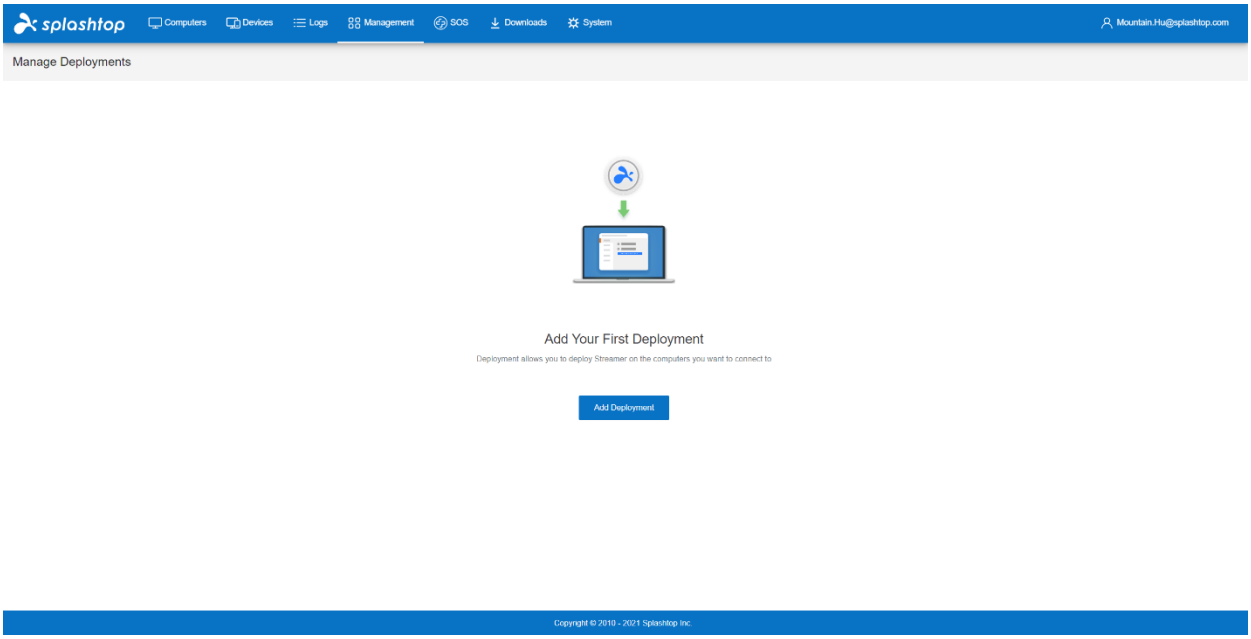


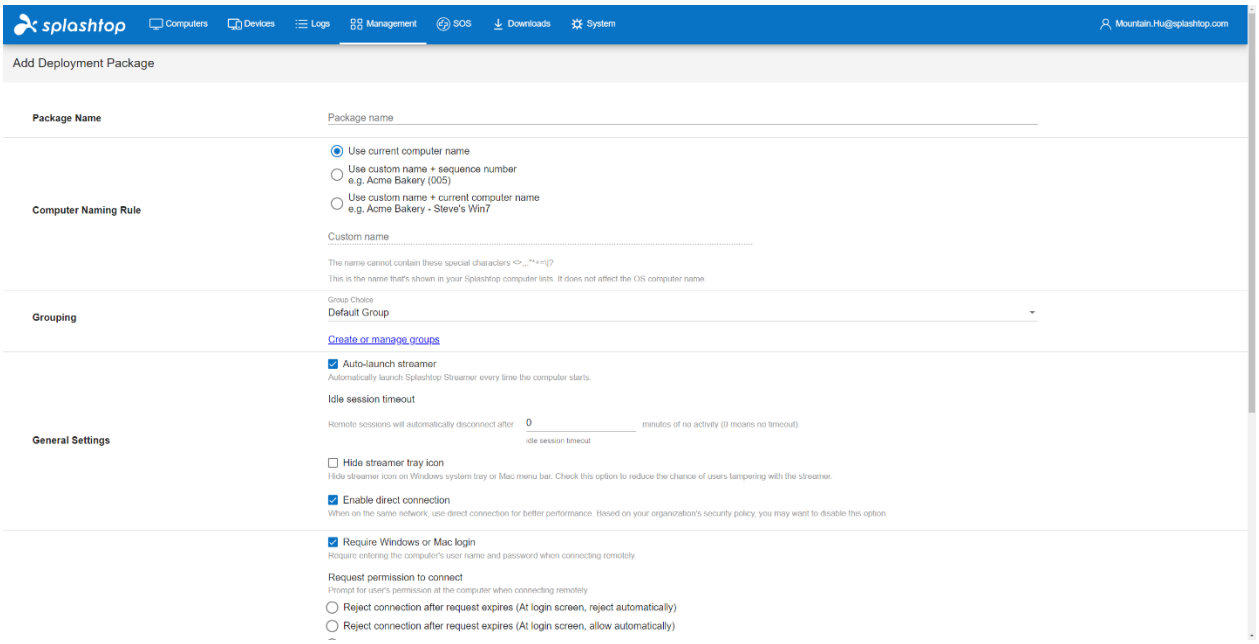
Deployment

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

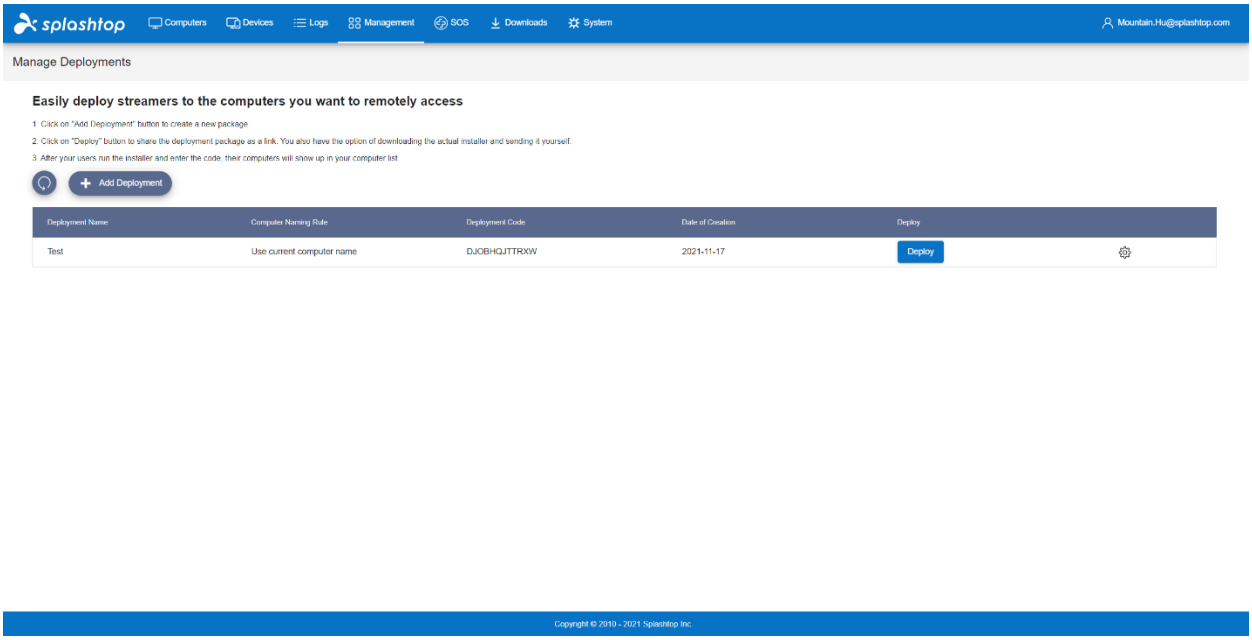
On the computers that you'd like to connect to, the Splashtop Streamer must be installed. This can be done in 4 simple steps.

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

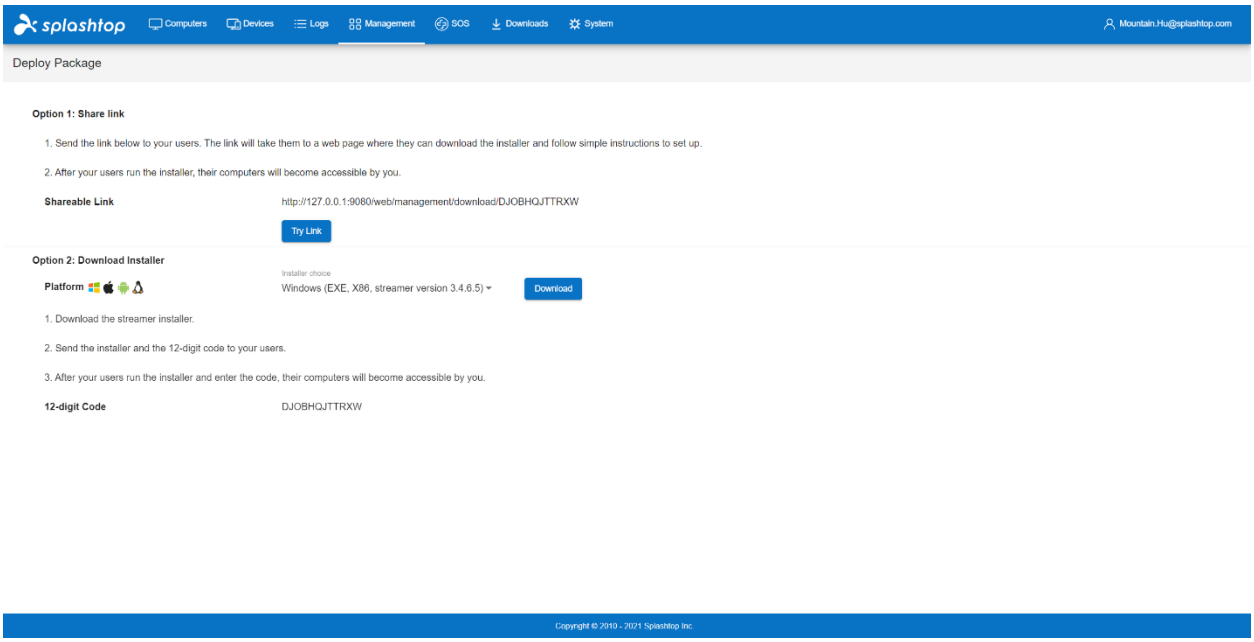




2. **Select**  **for the package that was just created.**



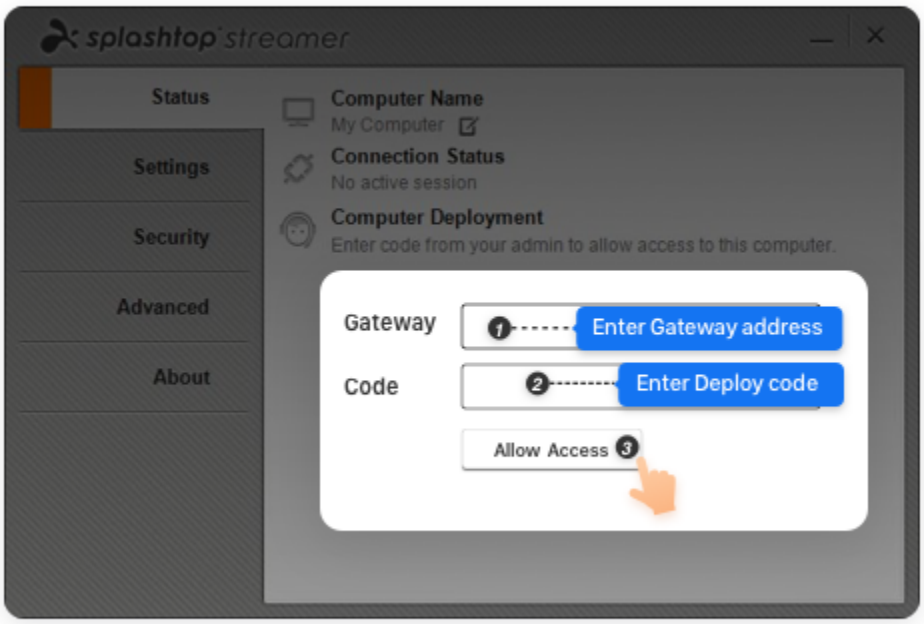
3. **Have your users install the streamer.** You can send the deployment package link to your users. By following the link, your users can download the streamer installer and run the file. You can also send the streamer installer file directly to your users (via Dropbox, email, etc.).



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 mass deploy computers with the help of 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 it when entering the Gateway address.



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)

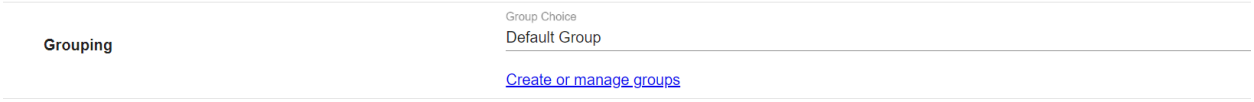
- Use current computer name
- Use custom name + sequence number
  e.g. Acme Bakery (005)
- Use custom name + current computer name
  e.g. Acme Bakery - Steve's Win7

Custom name

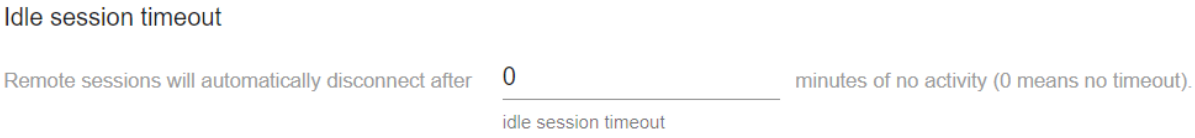
The name cannot contain these special characters <>,;:"*+=\|?

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.

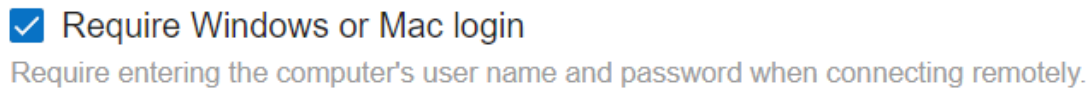


Specify which group the computer should be belong to, **Group** provides a way to organize the computers and grant access permissions in convenience.

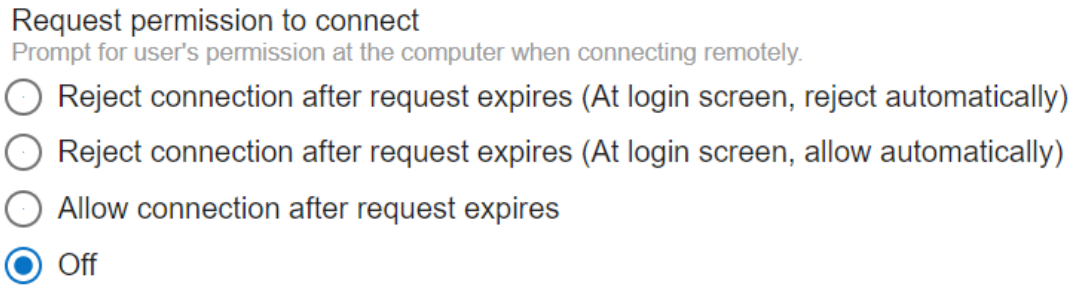


Specify the session idle time to disconnect.

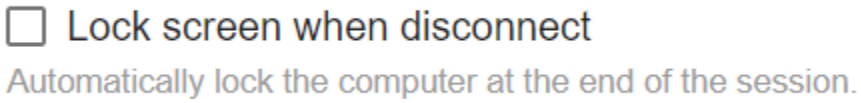
Specify if the Streamer tray icon should be hidden from user's system tray (Windows/Mac).



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

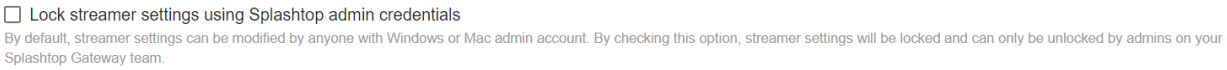


Specify the user's rule on permission when connection comes in.

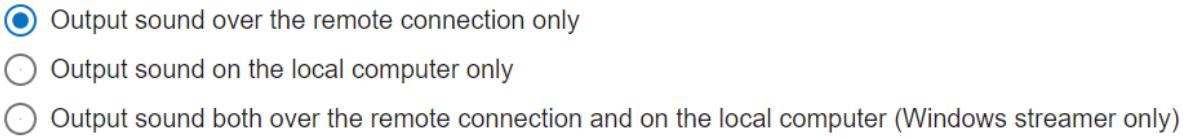


Specify if the screen should be locked when disconnected.

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



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.



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

Preference Policy

Introduction

Preference Policy is a tool to remotely configure the Streamer settings of your deployed Streamers and is accessible from the Splashtop Gateway web console. By assigning Streamers to your policy, you can configure and overwrite existing Streamer settings without having to redeploy the Streamer or manually change the settings locally at the endpoint.

Required Gateway version: **v3.24.0 or higher**

Platforms

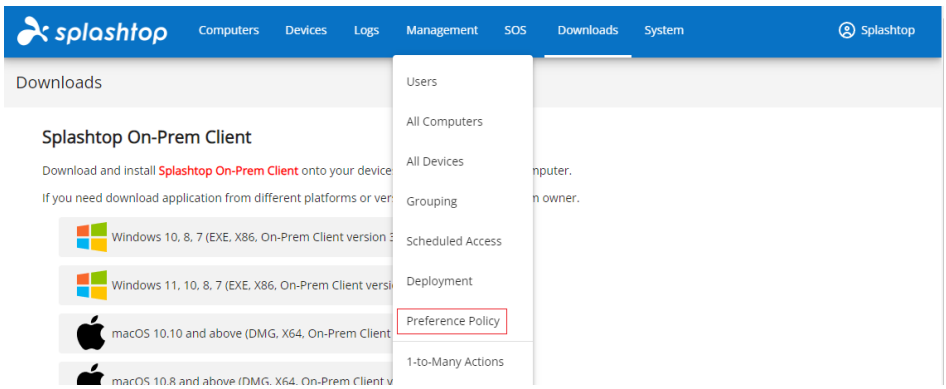
At the current time, only **Windows** and **Mac** Streamers (version **3.5.2.5** and higher) can be added to a Preference Policy.

Usage

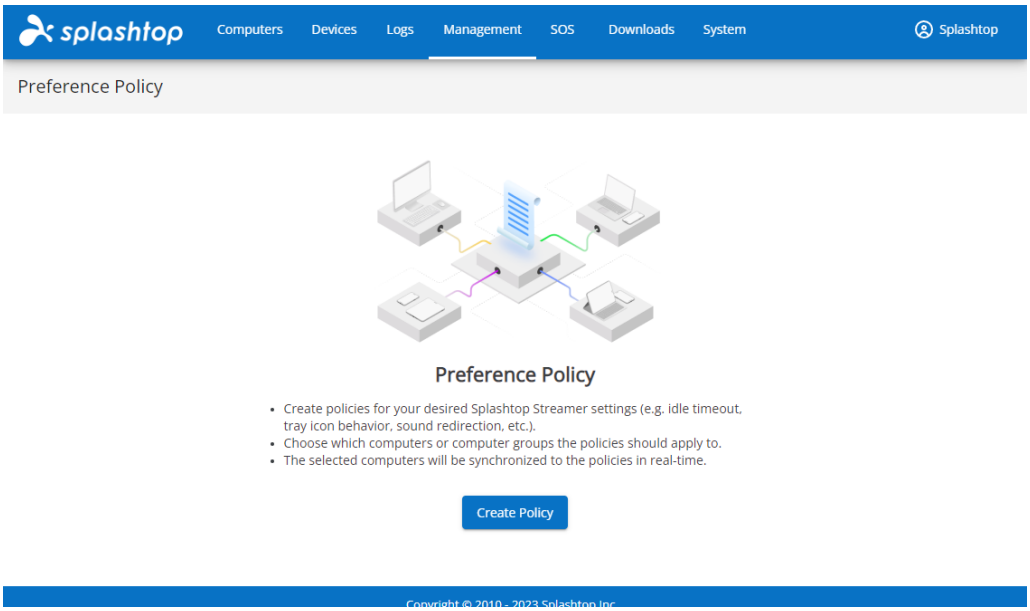
Create Policy

- Overview

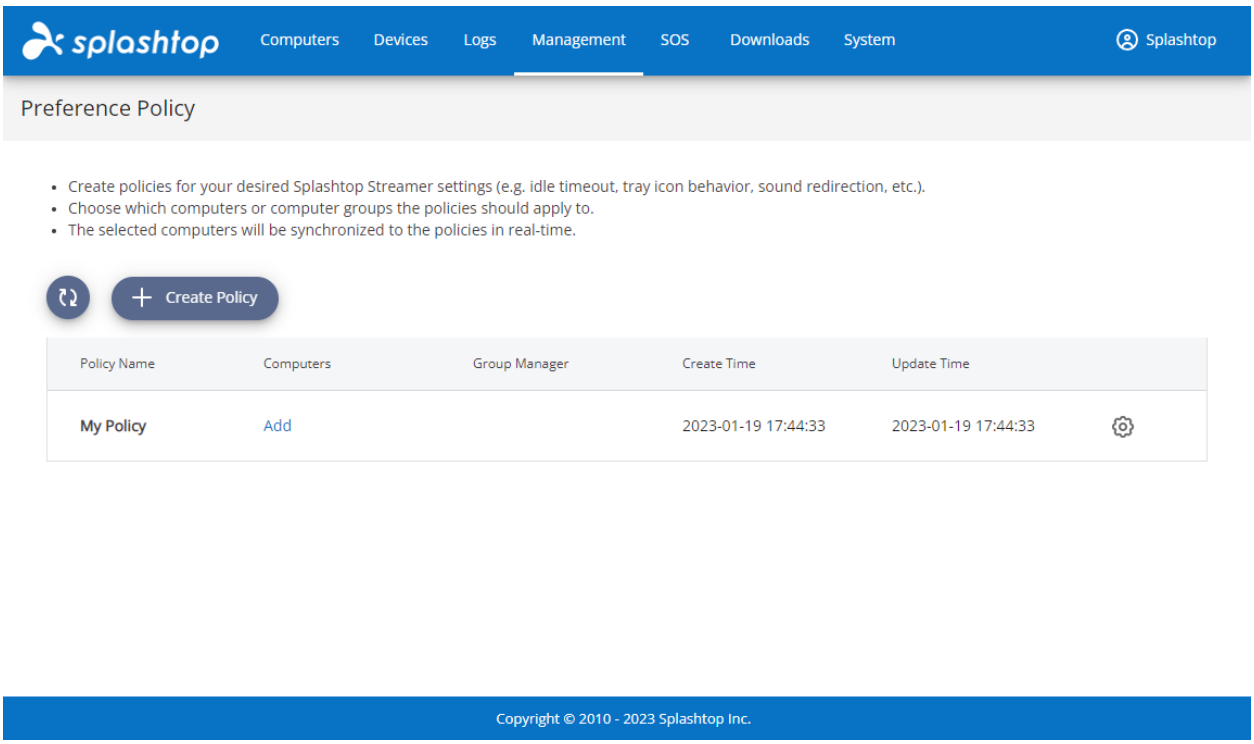
To create a new policy, log into your Splashtop Gateway web console, hover over **Management**, and click on **Preference Policy** in the drop-down menu. Then, click on **Create Policy**.



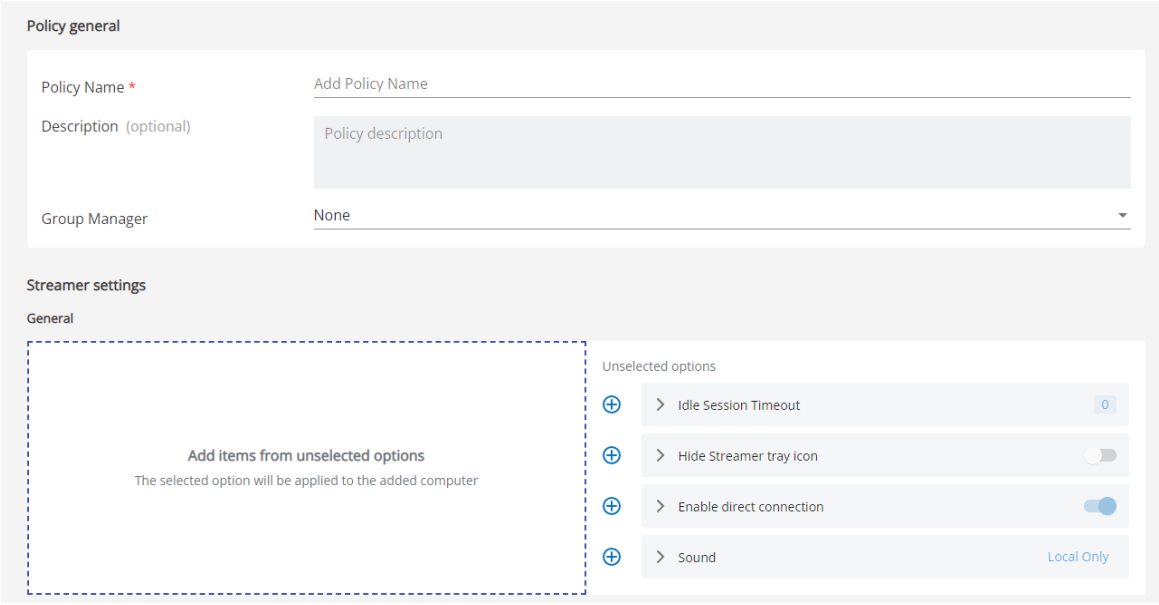
You will see the following screen if you have not created any policy yet.

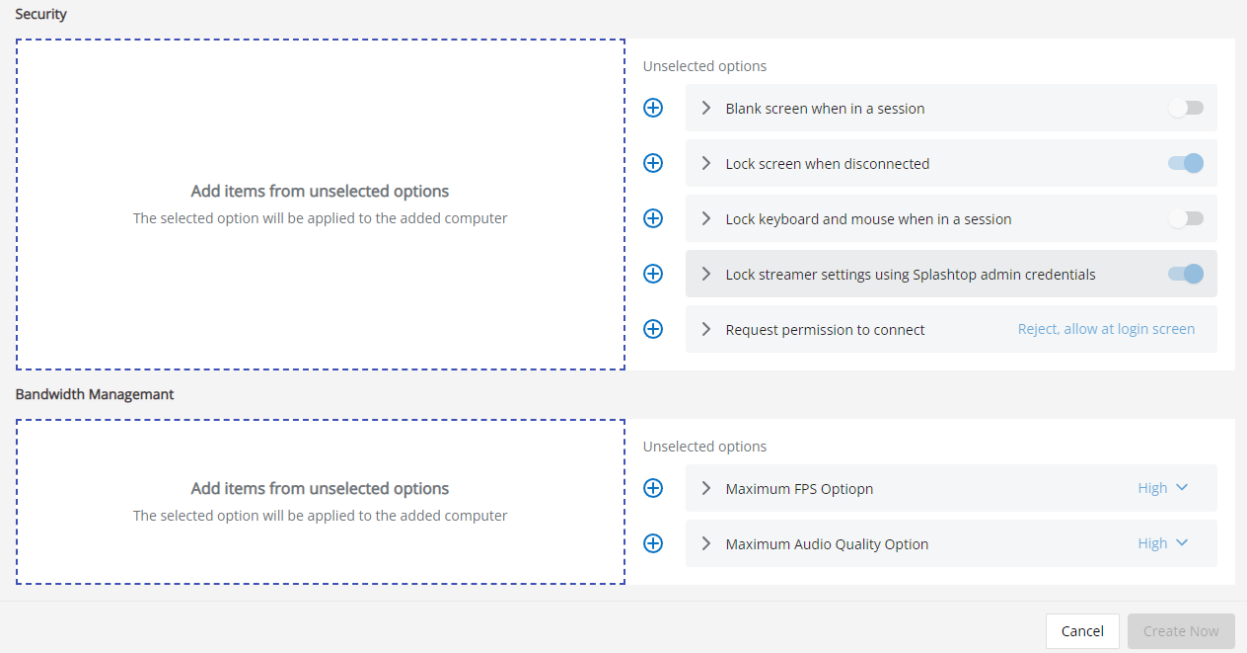


If you have already created a policy, you will see the following screen instead.



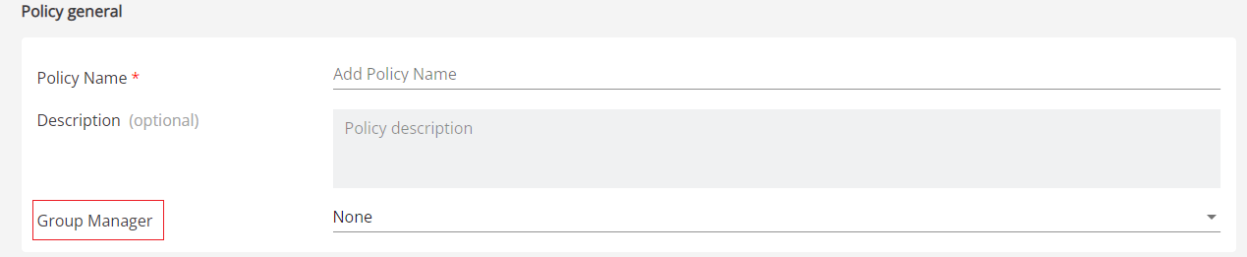
Beside **Name** and **Description**, there are three major categories: **General**, **Security**, and **Bandwidth Management**.





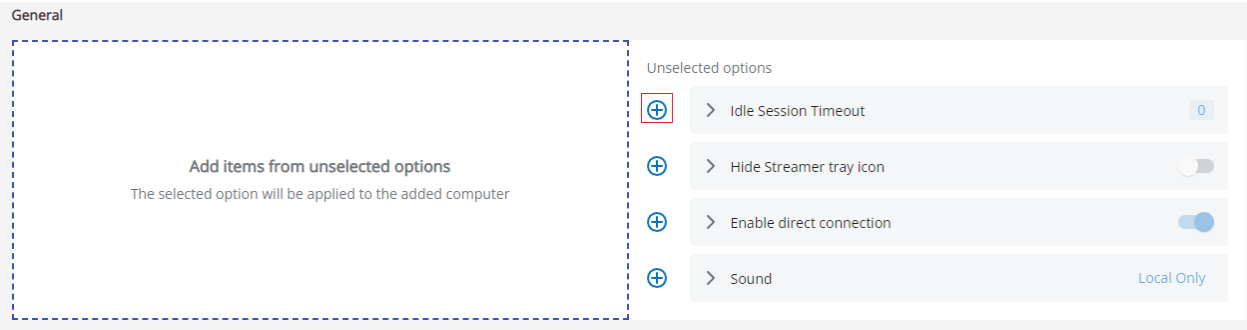
Each of the three categories divide up into two boxes. The left box (Selected Options) contains the settings that you have added to your policy. The right box (Unselected Options) contains the settings that you can choose from to add to your policy.

You can also assign a **group manager** to your policy.

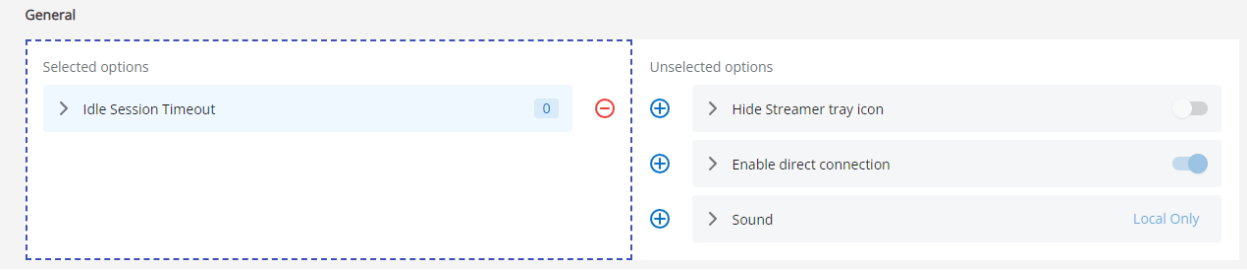


- Add and remove items to your policy

To add an item to your policy, click on the blue plus button. The selected item will be moved to the left box of selected options.

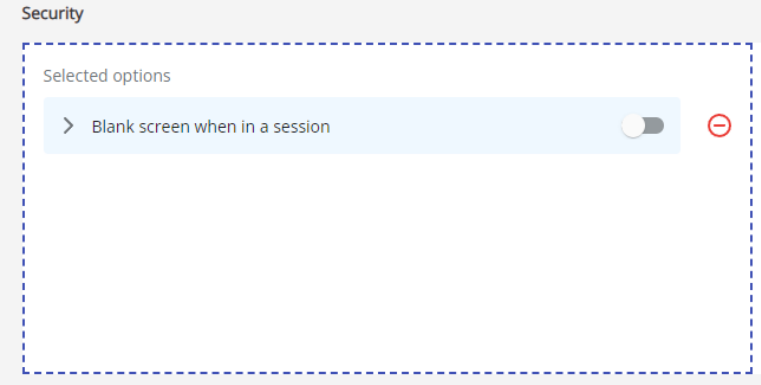


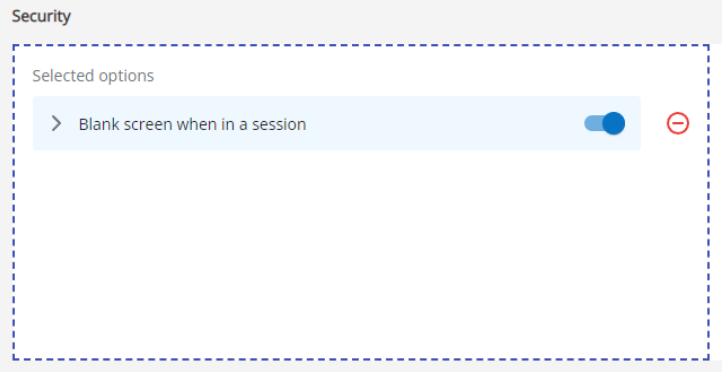
Instead, if you want to remove an item from your policy, click on the red minus button. The selected item will be moved to the right box of unselected options.



- Configure the value of an added item

After you have added an item to your policy, you can configure its value. Most of the items have binary values that you can toggle on or off. If the switch is greyed out, the value is set to off. Conversely, if the switch is blue, the value is set to on.

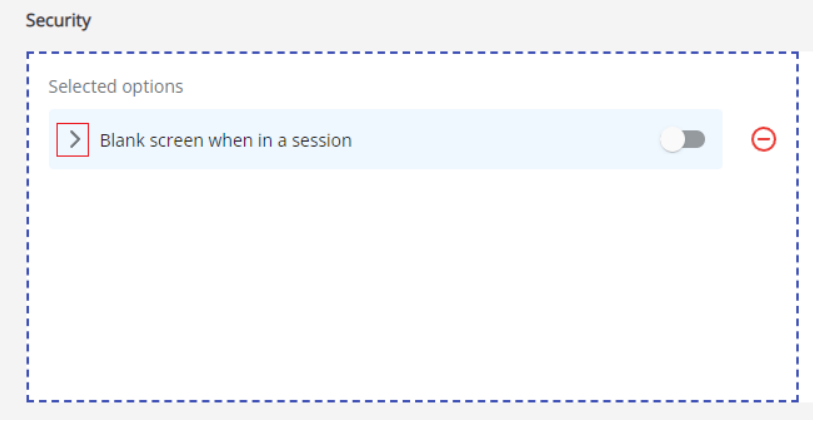


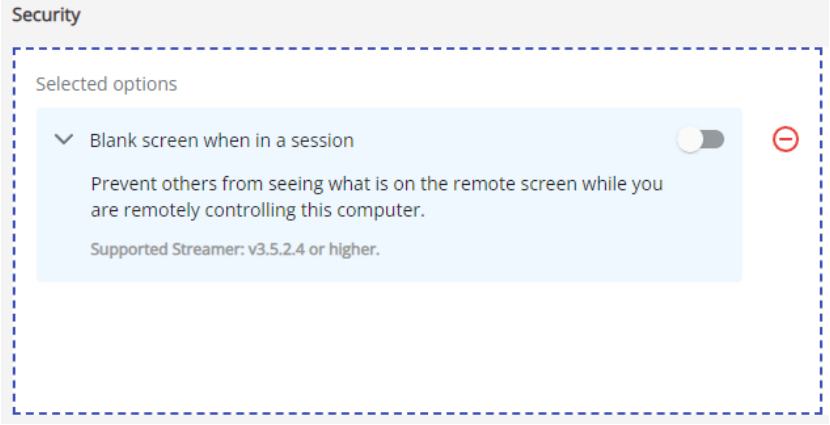


Initially, the item values are set to their default value. For example, the blank screen setting above is by default turned off.

- Know your item

If you are not sure about the function of an item, you can click on the angle bracket icon to display a concise description.

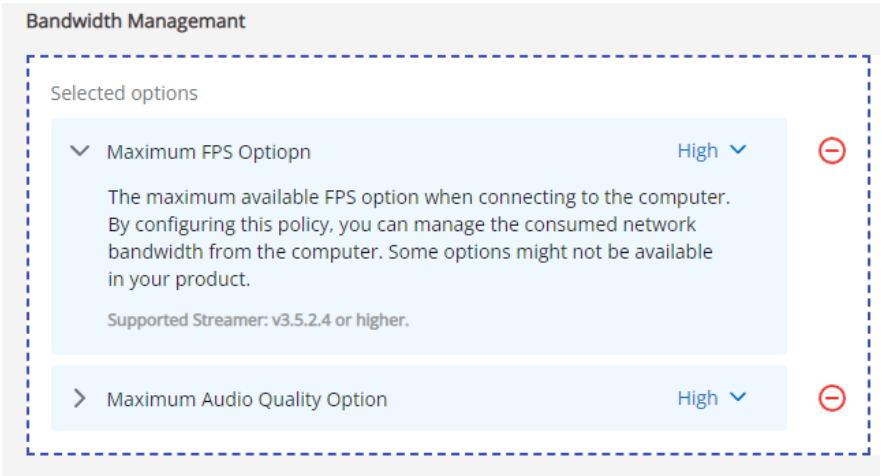




- Bandwidth Management

Bandwidth Management is a brand new tool that allows you to control bandwidth in terms of the parameters FPS and audio quality.

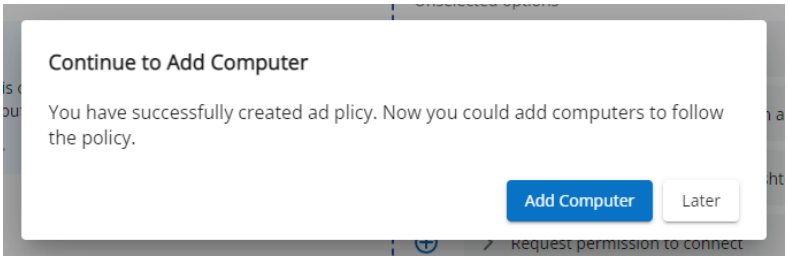
As for the items **Maximum FPS Option** and **Maximum Audio Quality Option**, if you select the highest value (Maximum FPS Option: "Ultra High", Maximum Audio Quality Option: Ultra High - 384k"), it will have the same effect as not adding these items to your policy at all: no bandwidth restrictions for your users.



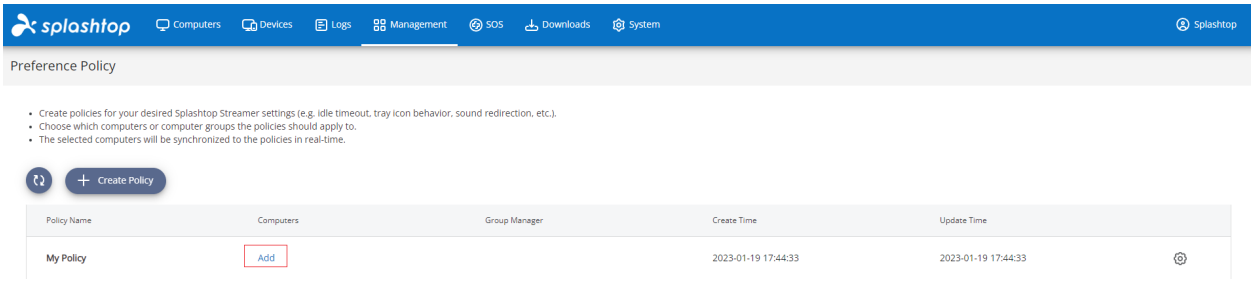
- Add computers

After you have created the policy, you can then add computers to it.

Directly click on **Add Computer** in the pop-up.

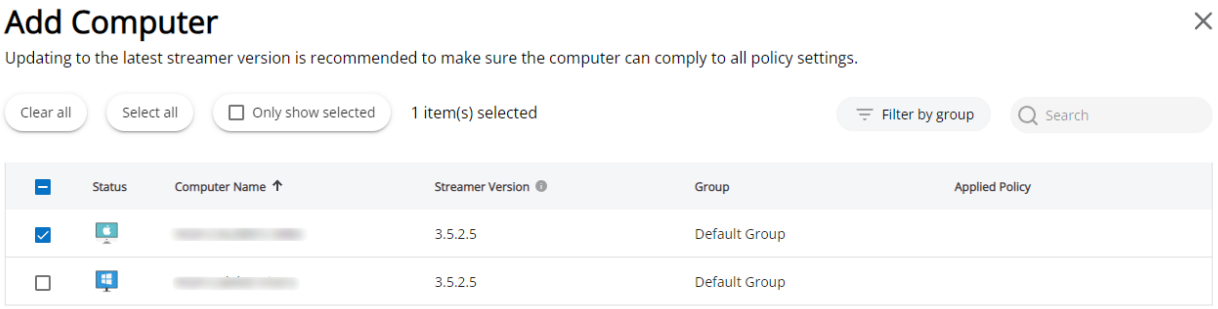


Alternatively, click on **Add** in the Preference Policy dashboard.

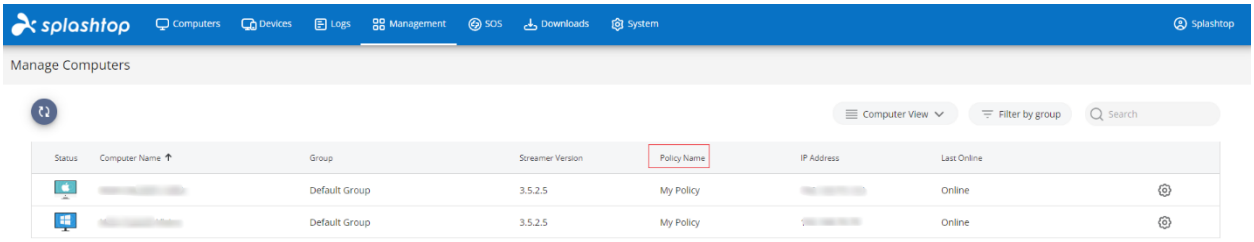


Select the computer or computer group you want to apply your policy to, and click on Save. Please also make sure that the Splashtop Streamer is updated to the latest version.

Please note that only Streamers v3.5.2.5 or higher will be displayed in the list of computers that you can add to your policy.

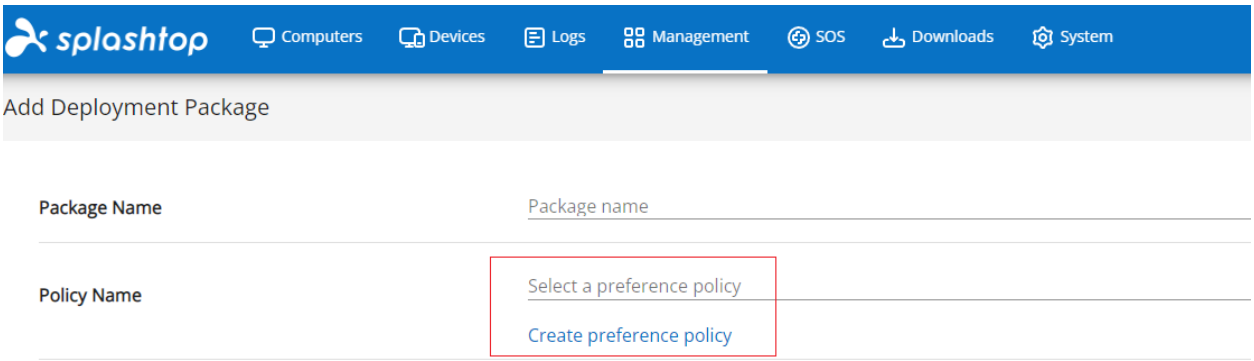


The associated policies will be displayed in a new column "Policy Name" at Management - all computers page.



Assign Preference Policy to Deployment Package

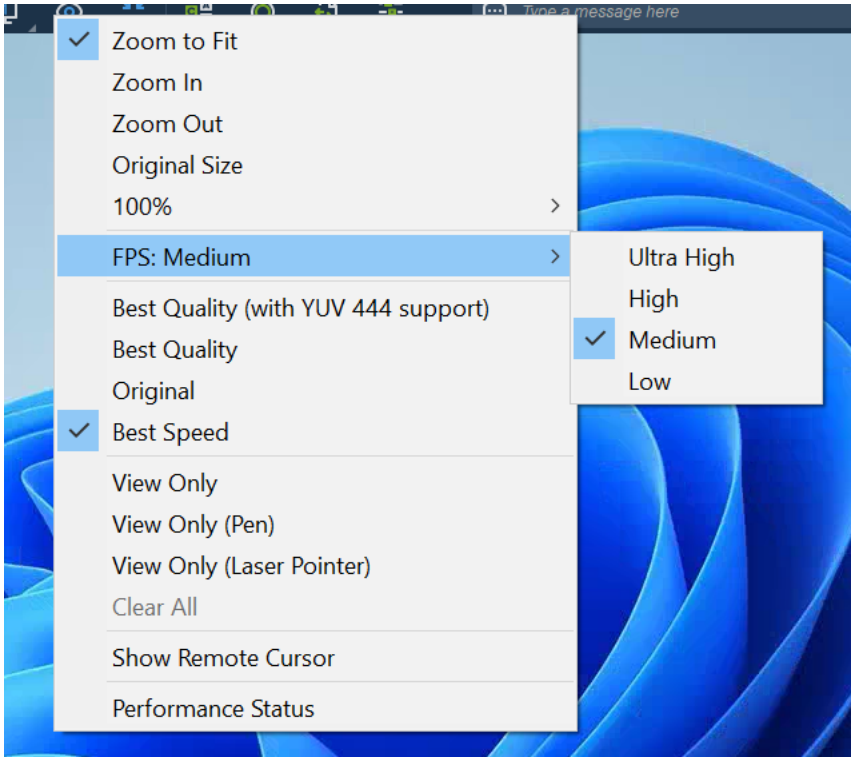
Since Splashtop On-Prem Gateway v3.24.0, you can have your Streamers to follow a specific preference policy the moment they get deployed. Select a created preference policy from the dropdown shown in the below screenshot when creating a new deployment package from the Deployment page. Please refer to this article for more information on how to create a new deployment package: [How do I set up the computers that I want to access remotely?]

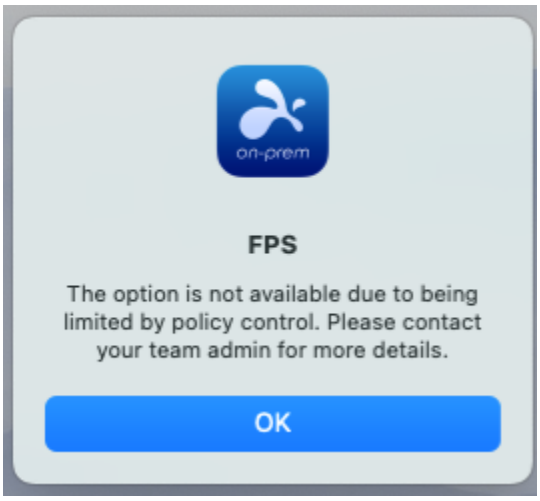


Behavior

- In-Session

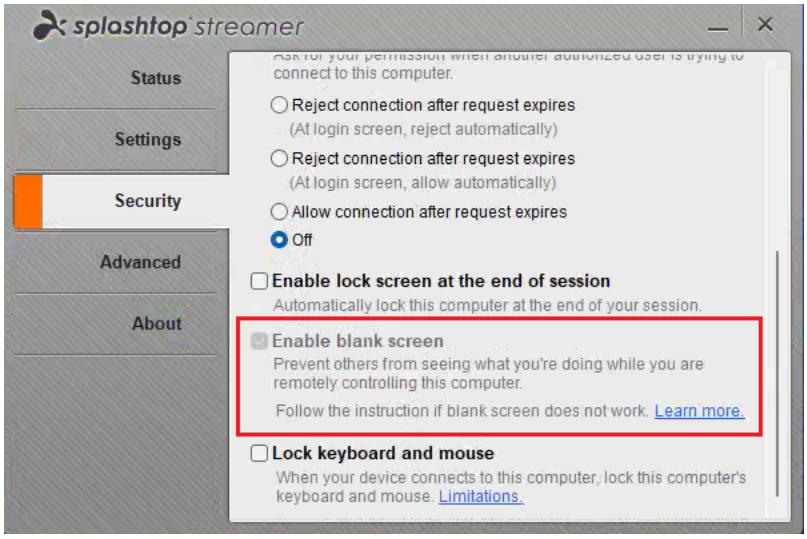
When a user remotes to a computer that associated to a preference policy, the configured settings or restrictions apply to the remote session. For example, if your policy restricts the FPS to High and the user tries to set it to Ultra High, an error message will pop-up.



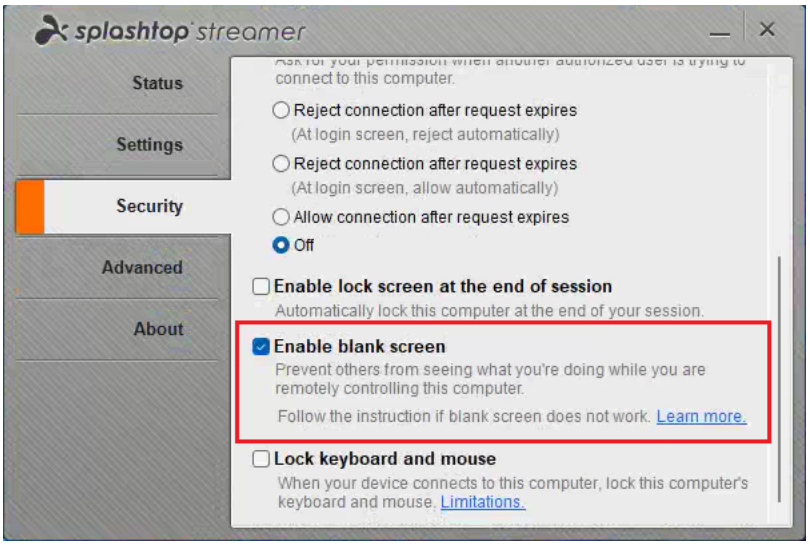


- Streamer

Many of the items that you can configure within Preference Policy can also be configured from within the Streamer UI. If a setting that you have configured in your policy is also part of the Streamer settings, the respective setting will be greyed out and cannot be configured from within the Streamer UI until detached from the policy. For example, since the blank screen setting has been enabled in the preference policy, this option is locked in the Streamer UI for all computers that this policy has been applied to.



If you remove the computer from the policy, or if you remove the item (in this case Blank Screen) from your policy, the setting can be configured from the Streamer UI again. However, its value will not automatically switch back to the default value (remember Blank Screen is turned off by default) but will keep the value it had been given to before.



Single Sign-On (SSO)

How to apply for a new SSO method? (SAML 2.0)

Splashtop now supports logging in to your Gateway and *Splashtop On-Prem app* using the credentials created by your SAML 2.0 identity providers. Please follow the below instructions to apply for an SSO method for your team.

Requirements

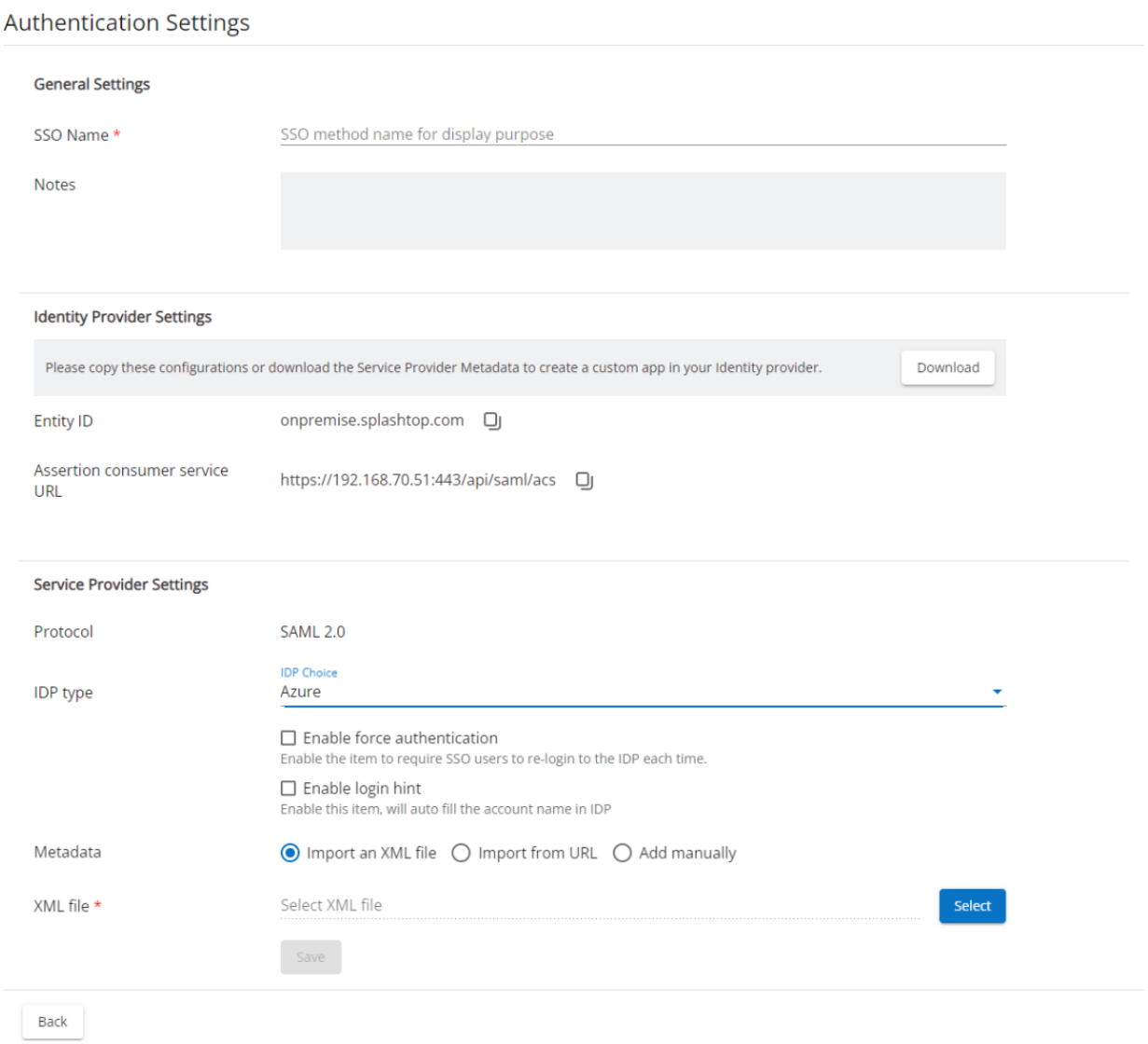
- **Splashtop Gateway v3.24.0** or higher

Insert the IDP/X.509 cert info

1. Log in to your Gateway with the owner account, then go to Management/Settings/Authentication/Single Sign-On.

2. Click "Add" to add Gateway URL. Please fill in the correct Gateway URL to ensure the connection between Gateway and IDP.

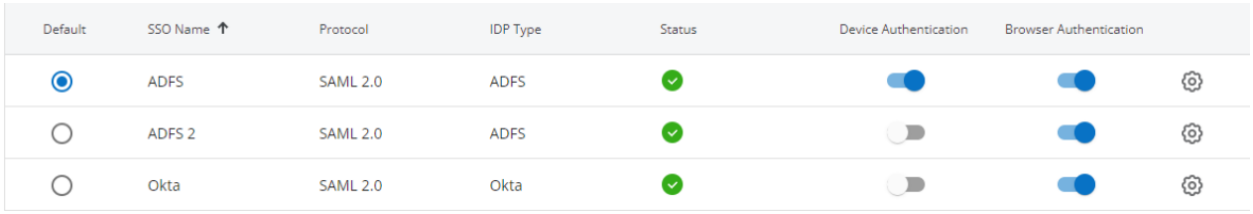
3. Click "Add SSO Method", then insert the required information and save the settings for your SSO method.



- **General Settings**
  - **SSO Name**: Insert a name for your SSO method.
  - **Notes**: Insert the notes for your SSO method.
- **Identity Provider Settings**
  - **Entity ID**: Please copy Entity ID and Assertion consumer service URL from Gateway, then paste it to your IDP.
  - **Assertion consumer service URL**: Please copy Entity ID and Assertion consumer service URL from Gateway, then paste it to your IDP.
  - **Download service provider metadata**: In addition, we also provide a metadata download for you to import SP's metadata in IDP.

- **Service Provider Settings**
  - **Protocol**: Fixed to **SAML 2.0**.
  - **IDP Type**: Choose IDP Type.
- **Metadata** (Insert the **IDP SSO Login URL**, **IDP Issuer,** and **X.509 Certificate** info from your IDP: Okta, Azure AD, JumpCloud, OneLogin or ADFS, or Other IdPs)
  - Use the metadata import to automatically populate the settings
    - **Upload an XML** or **Import from URL**
  - OR **Add manually**
    - For X.509, you need to copy the contents from IdP and then paste it to the field below.
    - Be careful on **http** versus **https** addresses

4. After clicking "Save", the SSO method will be enabled.



- You can enable/disable/remove the SSO method in the gear button.
- You have the option to disable device authentication for each SSO method - just uncheck the appropriate SSO method under the "Device Authentication" column.
- You have the option to disable browser authentication for each SSO method - just uncheck the appropriate SSO method under the "Browser Authentication" column.
- You can also set the default SSO method. Click the radio button for the appropriate SSO method under the "Default" column.

Note:

- SSO login is supported on **Gateway (v3.24.0 or higher)** and **Splashtop On-Prem app (v3.5.8.0 or higher)**.

Create SSO user

After you set up an SSO method on your Gateway, now you can add the SSO user.

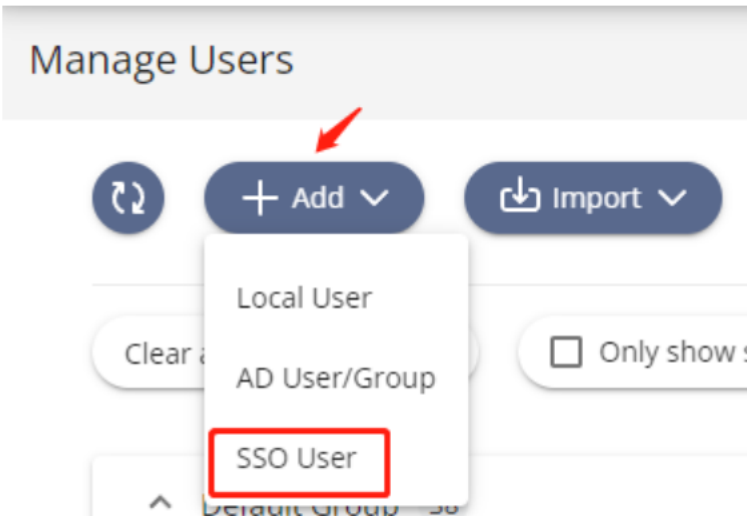
Requirements

- **Splashtop Gateway v3.24.0** or higher

Add SSO user

1. Follow the instructions to apply for SSO methods.

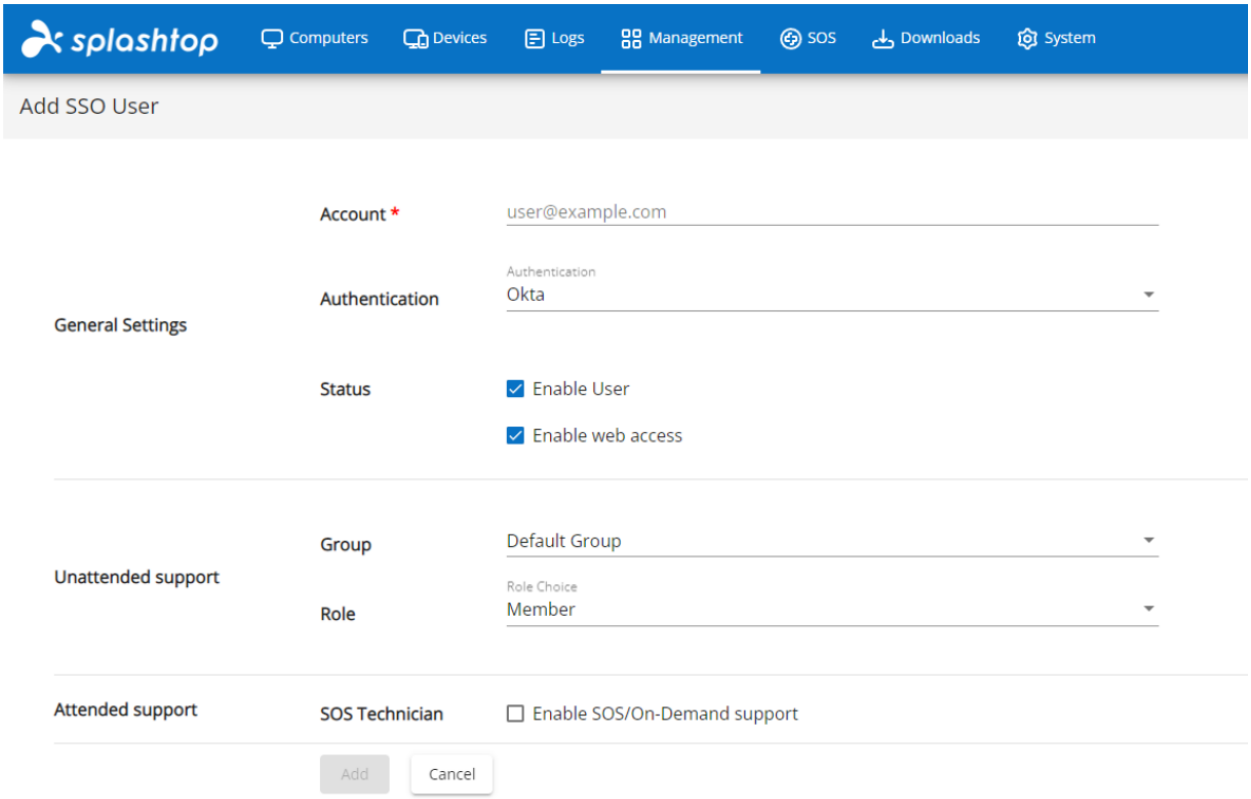
2. Go to **Management** tab – **Users**, click on **Import** button on the top, then select **SSO Users**.



3. Insert the required information of the SSO user, then click **Add**.

- **Account:** This is the SSO user's login account, it's unique in Gateway.
- **Authentication:** Select the SSO method you would like to associate.
- **Enable users:** If this item is enabled, users can establish a remote session. Otherwise, the remote session is disabled.
- **Enable web access:** If this item is enabled, users can access the web portal. Otherwise, web access will be denied.
- **Group:** Users can be grouped into different groups, grouping is efficient in users management/ 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.
- **SOS Technician:** Enable SOS-On Demand support capability.
- **Add:** Add the SSO user to the target group.



Add SSO Groups/SSO Group members

SSO groups/SSO group members cannot be added manually, these items can only be created through SCIM provisioning.

Note: An SSO group member would inherit the user role and access permission of its parent SSO Group.

Bulk import SSO users

After you set up an SSO method on your Gateway and confirm that you can log in successfully, now you can import your users using a CSV file.

Requirements

Splashtop Gateway v3.24.0 or higher

Working Flow

1. Set up your SSO method. (Instruction)

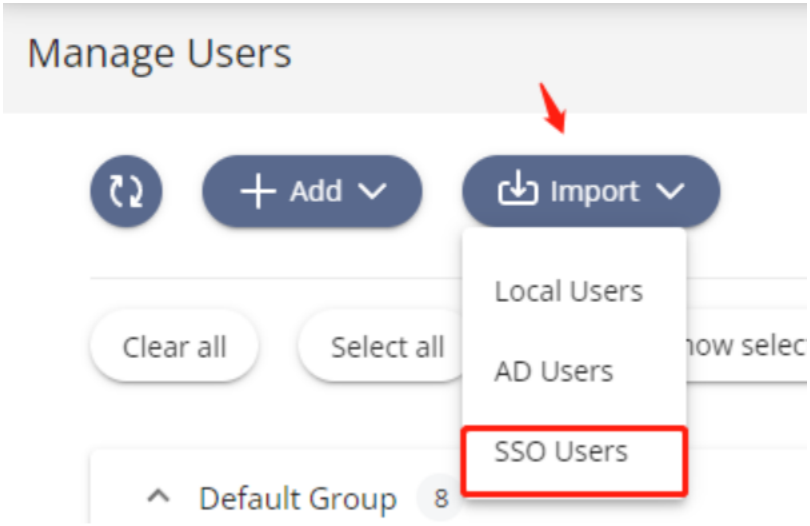
2. Create a user with the created SSO method (Instruction) or associate an existing user with the created SSO method (Instruction).

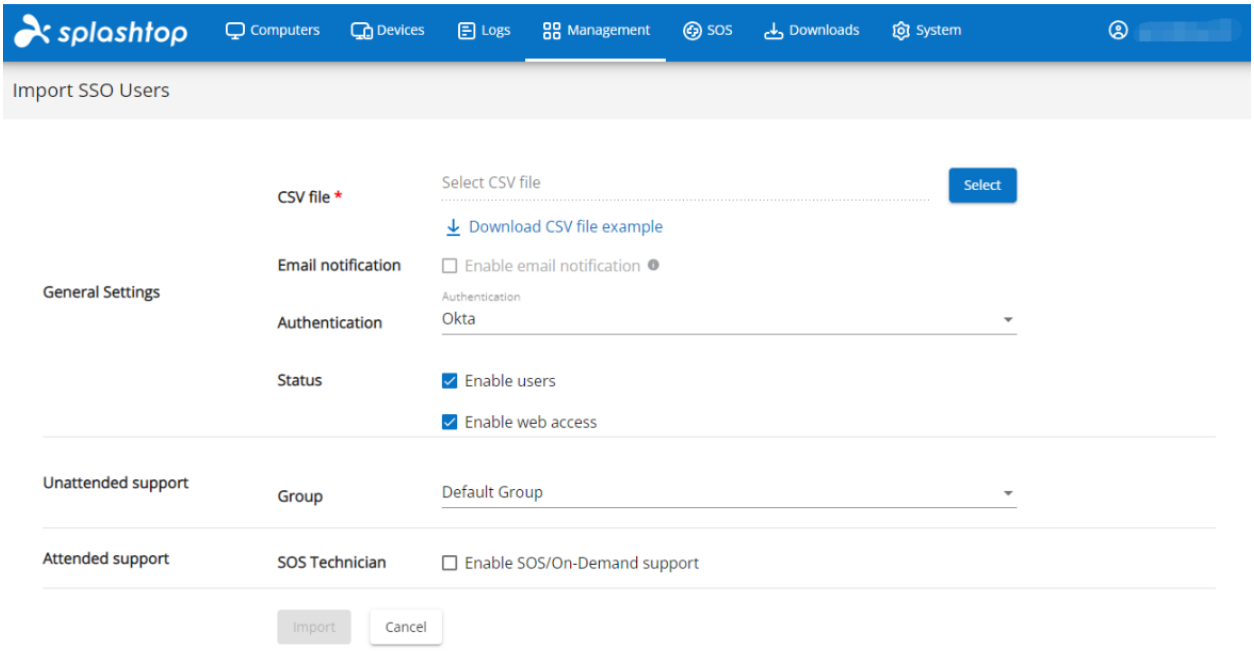
3. Test login using the above user.

4. For your created SSO method, start to import users using a CSV file.

Import SSO users

Go to **Management** tab – **Users**, click on **Import** button on the top, then select **SSO Users**.

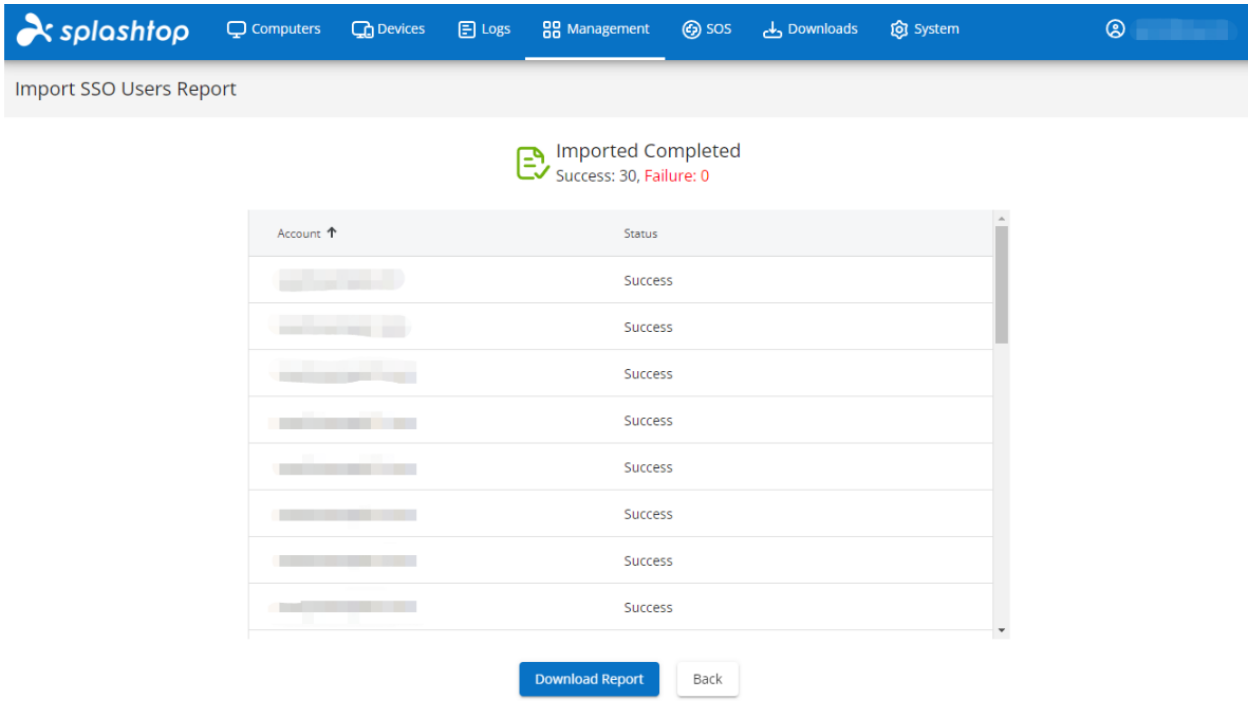




- **Select CSV file:** Upload the CSV file with the AD user list.
- **Download CSV file template:** Import AD users using the CSV file template.
- **Enable email notification:** if you are configured an SMTP server. Enable this item, then users can receive the notification email.
- **Authentication:** Select the SSO method you would like to associate.
- **Enable users:** If this item is enabled, users can establish a remote session. Otherwise, the remote session is disabled.
- **Enable web access:** If this item is enabled, users can access the web portal. Otherwise, web access will be denied.
- **Group:** Users can be grouped into different groups, grouping is efficient in users management/ access permissions.
- **SOS Technician:** Enable SOS-On Demand support capability.
- **Import:** Import the SSO users in a CSV file to the target group.

Imported report

After the user import is completed, **Admin** or **Owner** can view the import results and download the imported report.



Notes

1. It is only CSV file format supported.
2. The data in the file has to follow the standard layout. You can download the example.csv below to check the layout/format.
3. You cannot start importing another CSV file until the current import has been completed.
4. All successfully imported users will be given the member role.

How to associate SSO method to existing team admin/member?

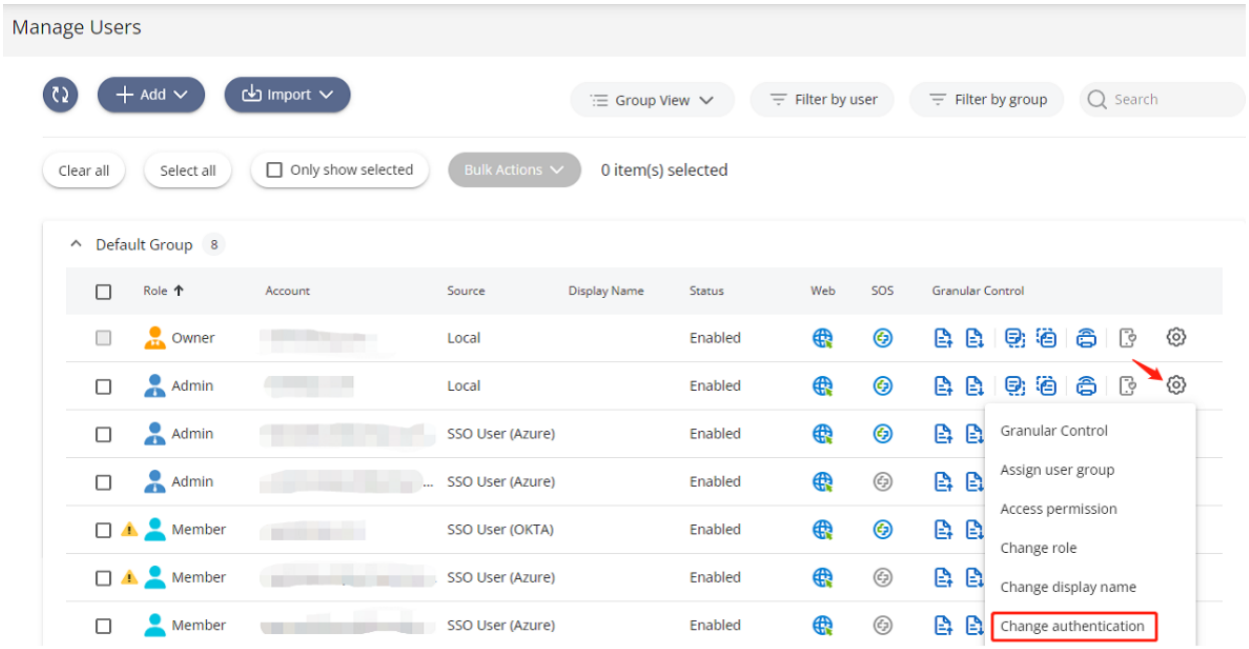
Requirements

- **Splashtop Gateway v3.24.0** or higher

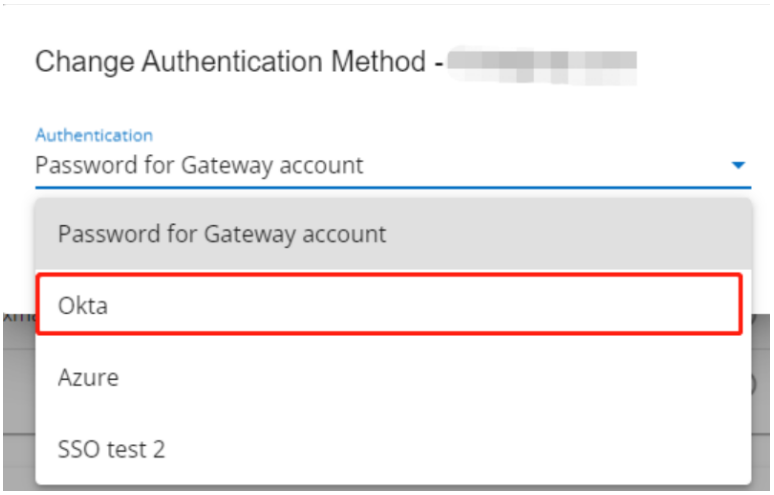
Working Flow

1. Follow the instructions to apply for SSO methods.

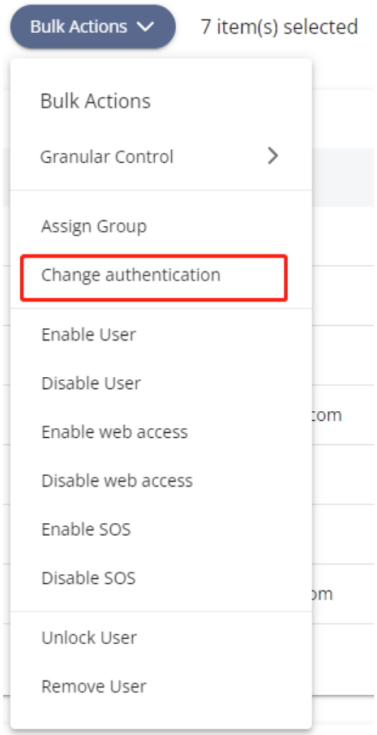
2. Log in to your Gateway → Management → Users, click the gear icon of the user profile you would like to modify and select **Change authentication**.

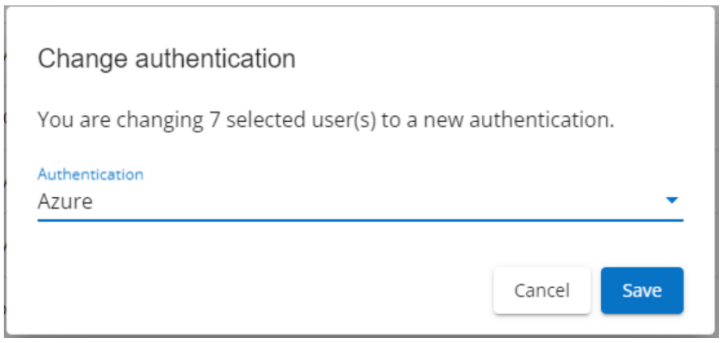


3. Select the SSO method you would like to associate with.



4. Additionally, you can change authentication by bulk actions. Select the account by clicking on the checkboxes to the left of the account. Then click the Bulk Actions button to configure the **Change authentication** items for selected accounts.





Notes

- For security concerns, only Owner can change Authentication Method.
- Owner's authentication can not be changed.
- AD user/AD group/AD group member's authentication can not be changed.
- When the authentication of the user has been changed, the ongoing web session and remote/SOS session will be interrupted and the user need to log in again based on their new authentication.

How can I log in using an SSO account?

You can use an SSO account to log in to your Splashtop Gateway and the Splashtop On-Prem app (v3.5.8.0 and newer).

Please follow the instructions below to log in using an SSO account.

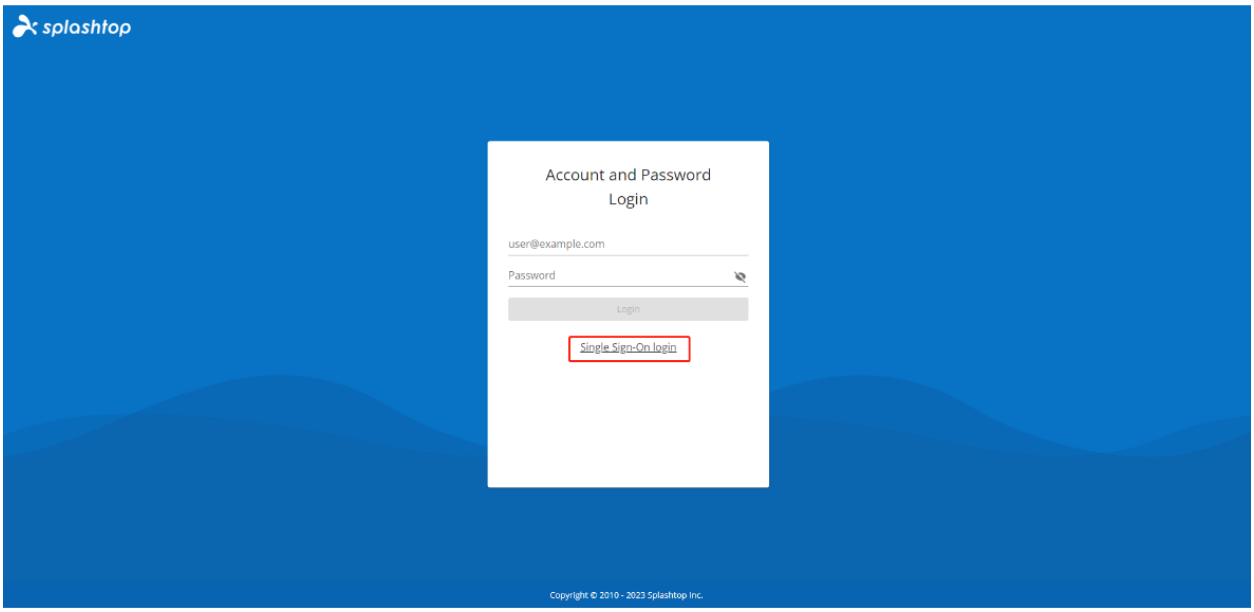
Requirements

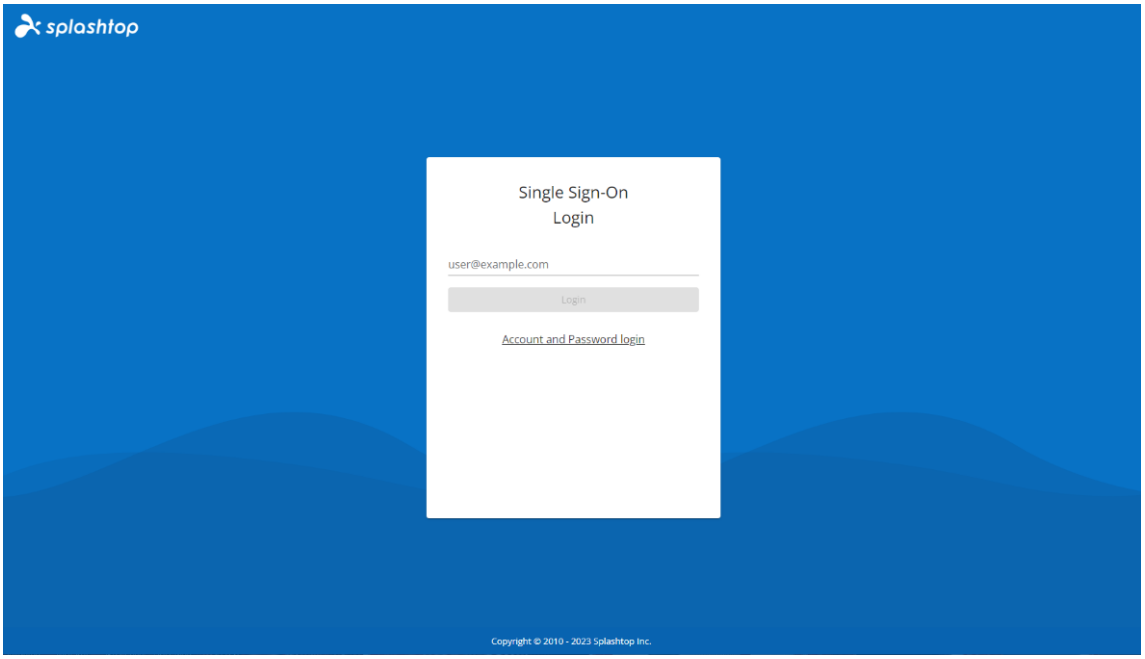
- **Splashtop Gateway v3.24.0** or higher
- **On-Prem Client app version 3.5.8.0** or higher

From Gateway

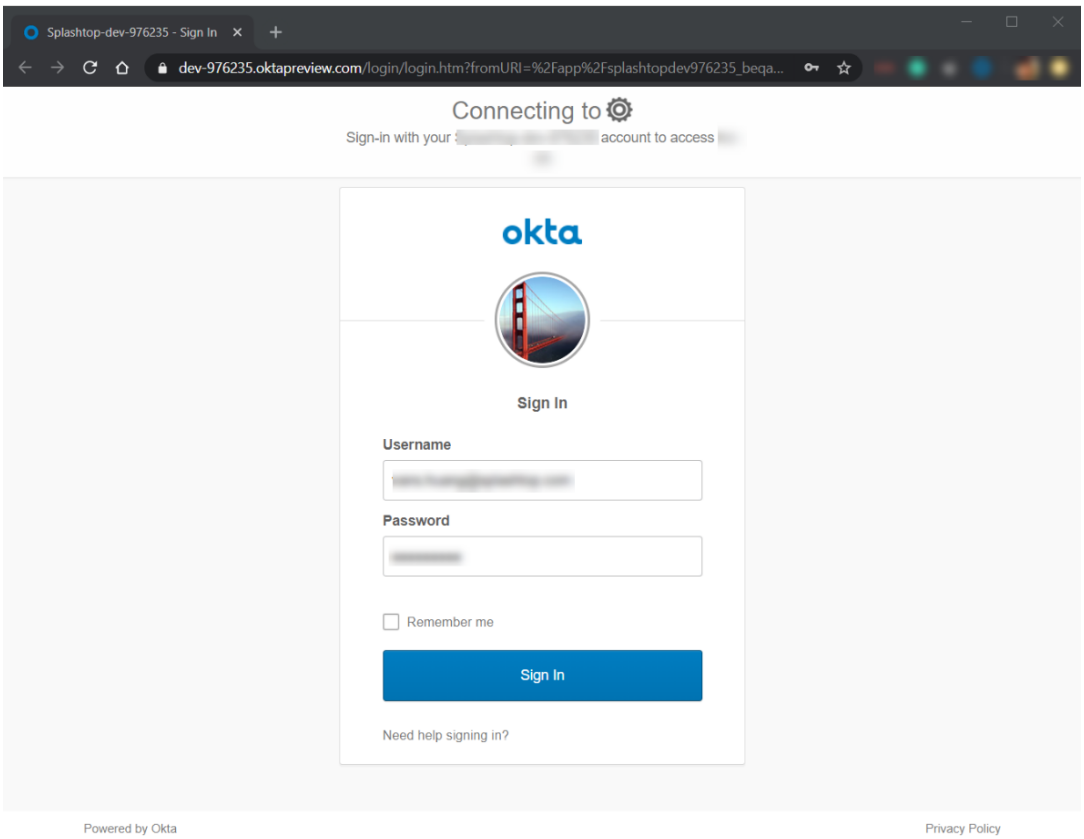
1. Enter your Gateway address and visit SSO login page

2. Insert your SSO account then log in.

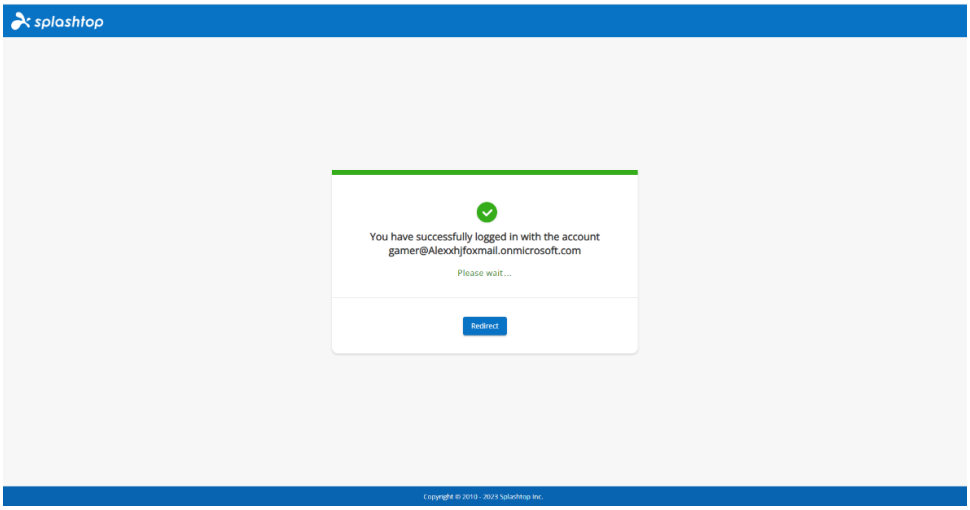




3. Click Single Sign On button, it will lead you to the identity provider portal. E.g., Okta portal.



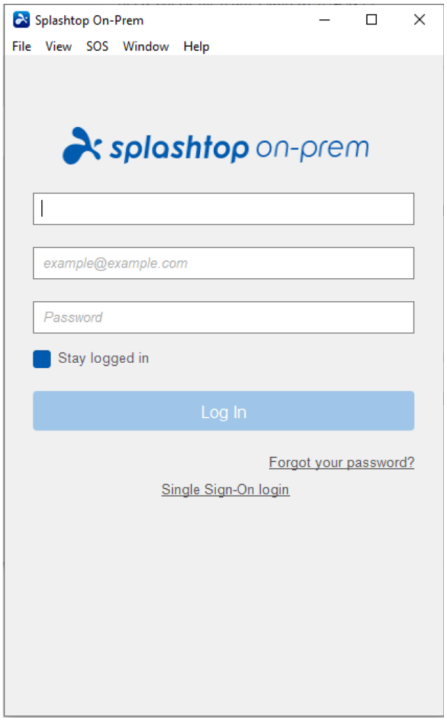
4. Log in to the identity provider portal then, it will log in to your Gateway.



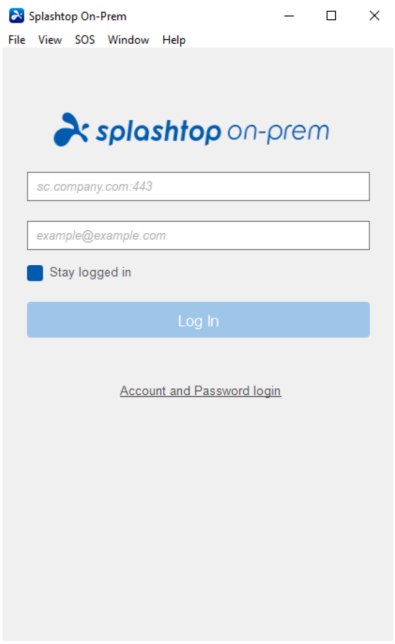
From Splashtop On-Prem app

Please make sure you are using v3.5.8.0+ Splashtop On-Prem app.

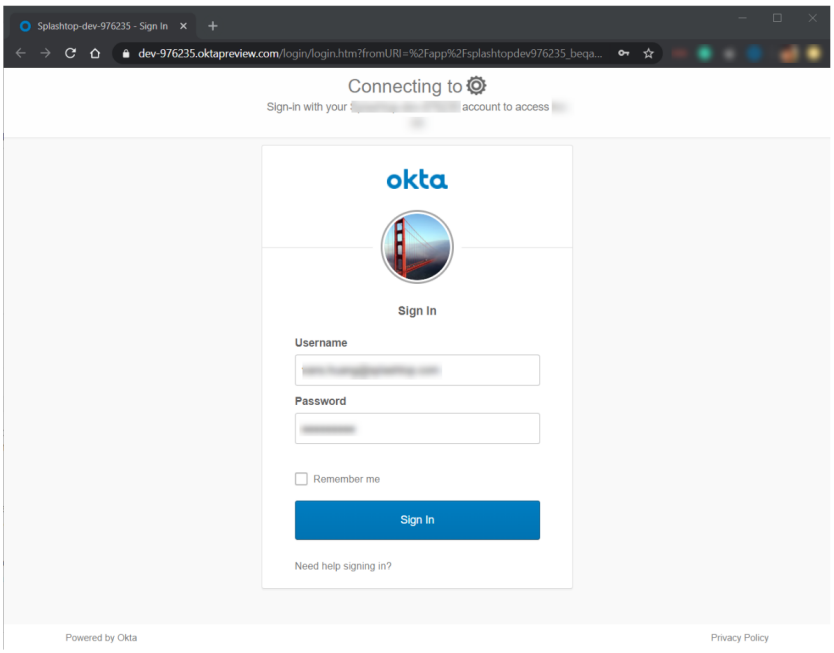
1. On Splashtop On-Prem app, click **Single Sign-On login** link.



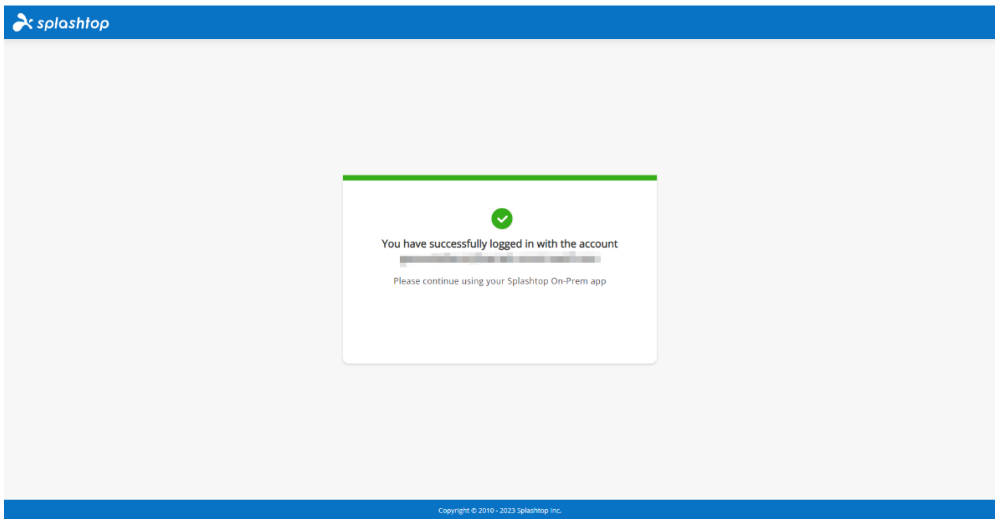
2. On the Single sign-on login page, insert your Gateway address and SSO account then click Log In.



3. Clicking the Log In will bring up your web browser and go to the identity provider portal. E.g., Okta portal.



4. Log in to the identity provider portal then, your app will log in.

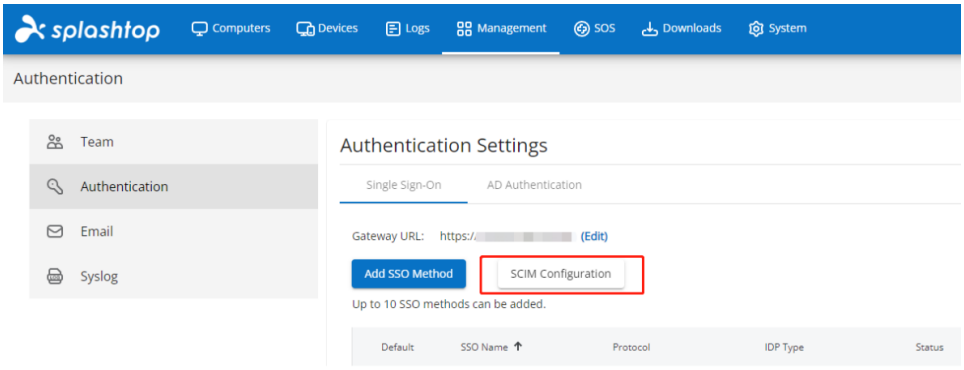


How to generate the SCIM provisioning token?

A secret token is required to be configured on your IDP portal so the SCIM provisioning can work. You can log on your Gateway to generate your secret token for SCIM Provisioning.

How to generate

1. On your Gateway, go to *Management/team settings/authentication/single sign-on*. Add your Gateway URL, then click **SCIM Configuration**.



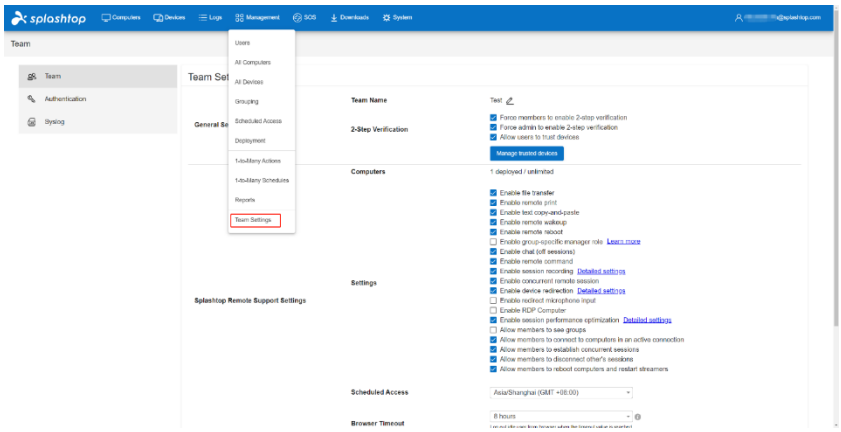
2. Click the copy icon to copy the Base URL and API Token.

3. Click generate icon to generate a new API Token.

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 can access and manage the Team Settings in the Management Console.

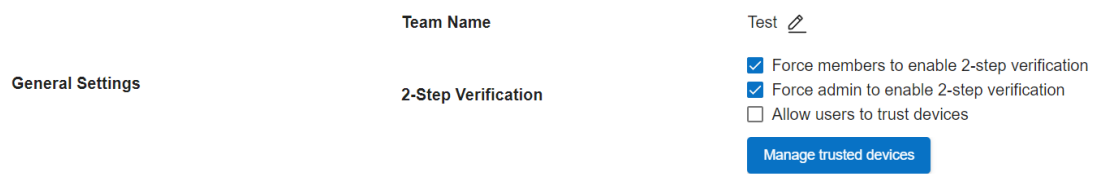
Team Settings



There are three sections in the page:

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

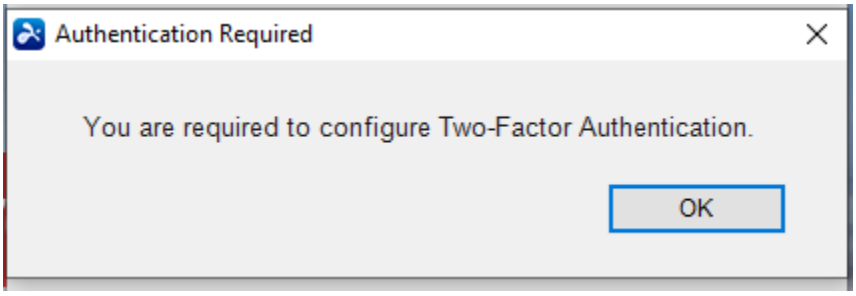
General Settings



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

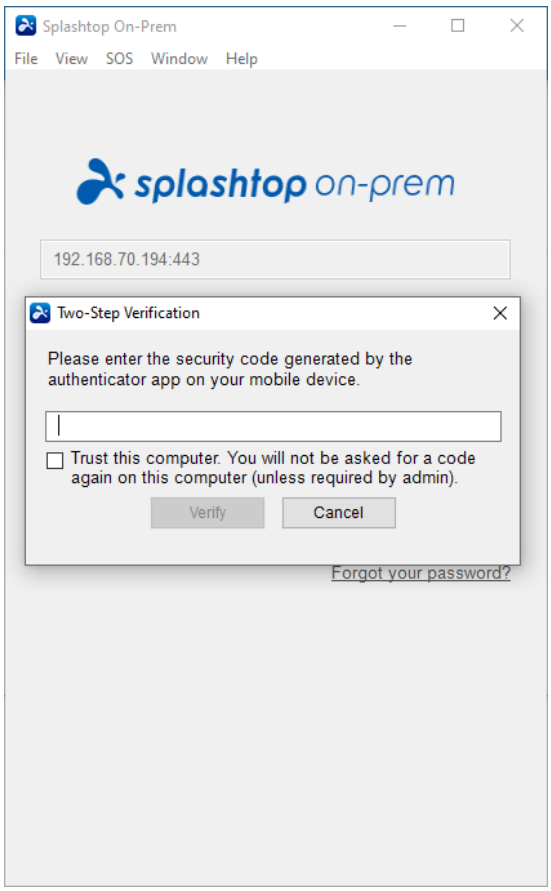
2-Step Verification: 2-Step Verification adds another layer of security by time-based OTP verification provided by prevalent authenticator APPs in mobile phones. An On-Prem client must input a 6-digit OTP code to log in to the device.

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.

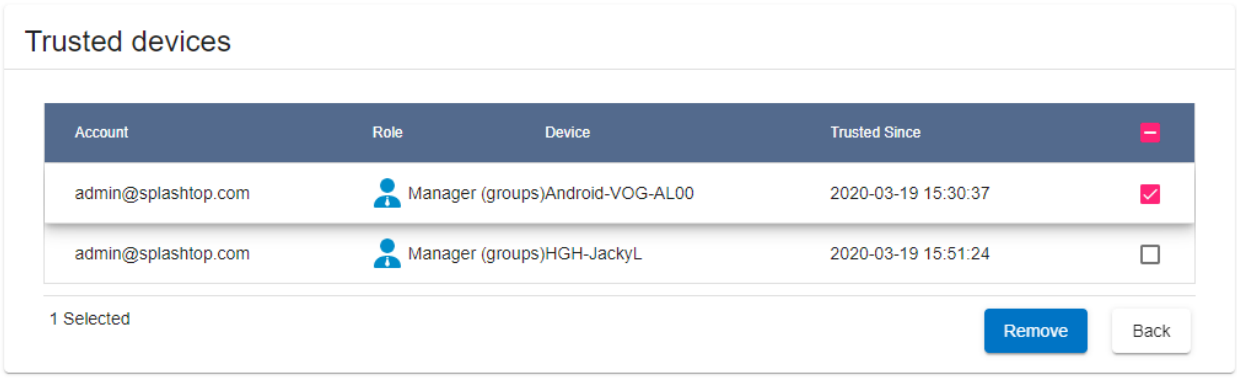


Force admin to enable 2-step verification: if this open is checked, an admin user is required to set up a 2-step verification device when he tries to log in to On-Prem client for the first time.

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.

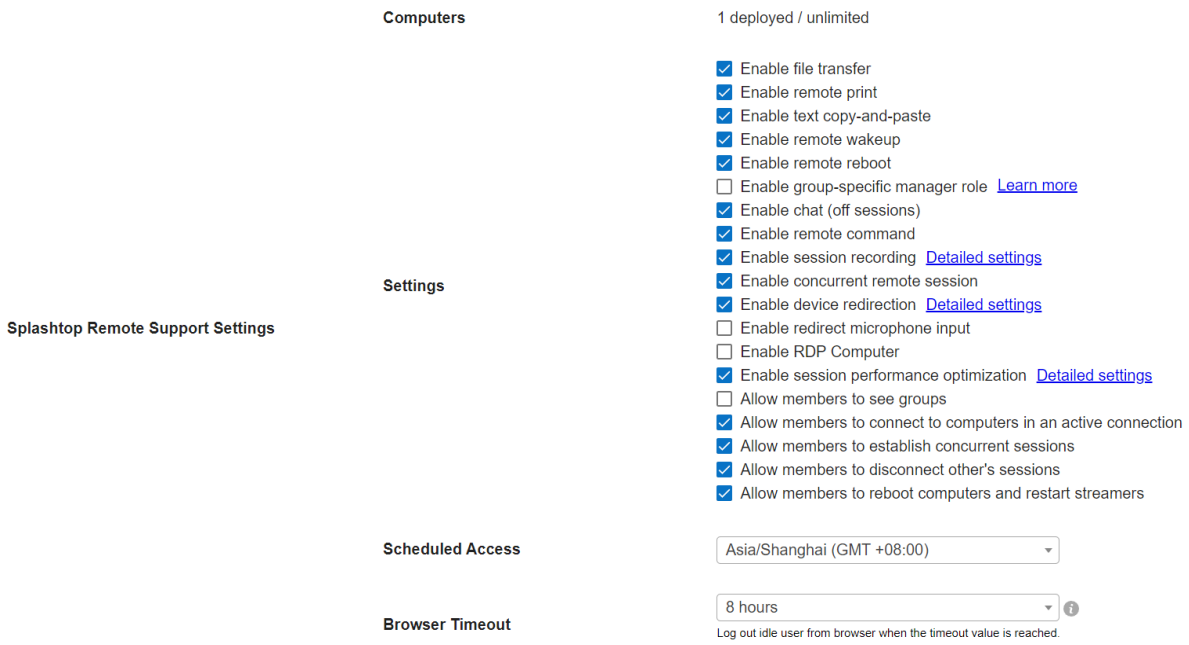


Manage trusted devices: Team administrator is able to overview the trusted devices and remove them if necessary.



Device authentication: Team admin can set the team to

Splashtop Remote Support Settings



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.

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.

Remove offline computers policy

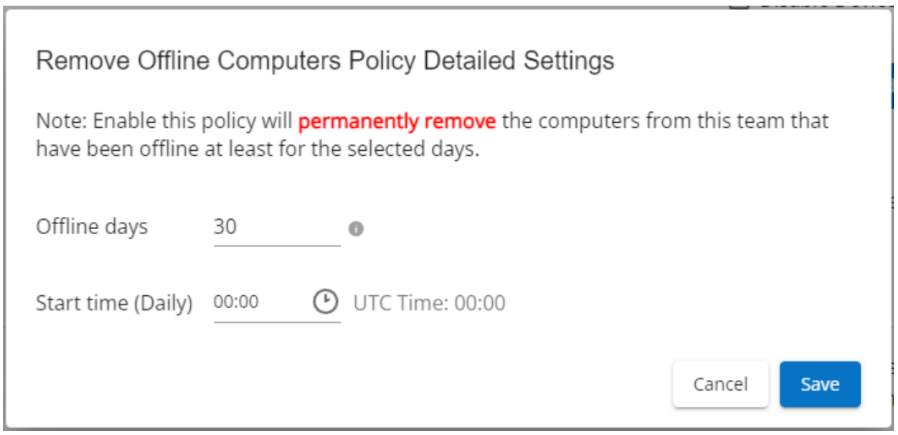
The Remove offline computers policy determines how many days offline computers will be automatically removed. This feature allows Team Owner to set policy parameters to clean the obsolete computers automatically.

How to set Remove offline computers policy?

1. Log in to Gateway's management console as Owner, go to *Management > Team Settings > General Settings > Computer.* Click the **Remove offline computers policy**.

2. Configure **Offline Days** and **Start time** in **Detailed Settings**. Then click **Save** button to save the settings and turn on the feature.

- **Offline days:** Set the offline days, the computers that meet the offline days will be removed.
- **Start time:** Set this policy's start time, which will repeat every day.



3. Click Save to save the settings。

4. This policy is disabled by default. Enabling the option when auto-remove computers will help in your scenario.

How to set web access?

What is web access

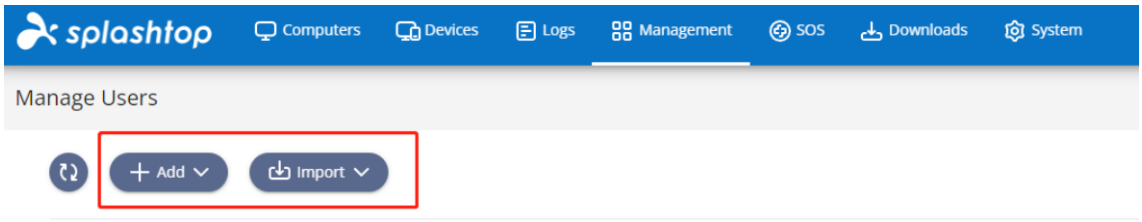
Web access determines whether or not can a user access Splashtop Gateway web portal. When web access is disabled, a login attempt will be blocked by browser, although this option does not affect the user's remote access capability from native Client apps.

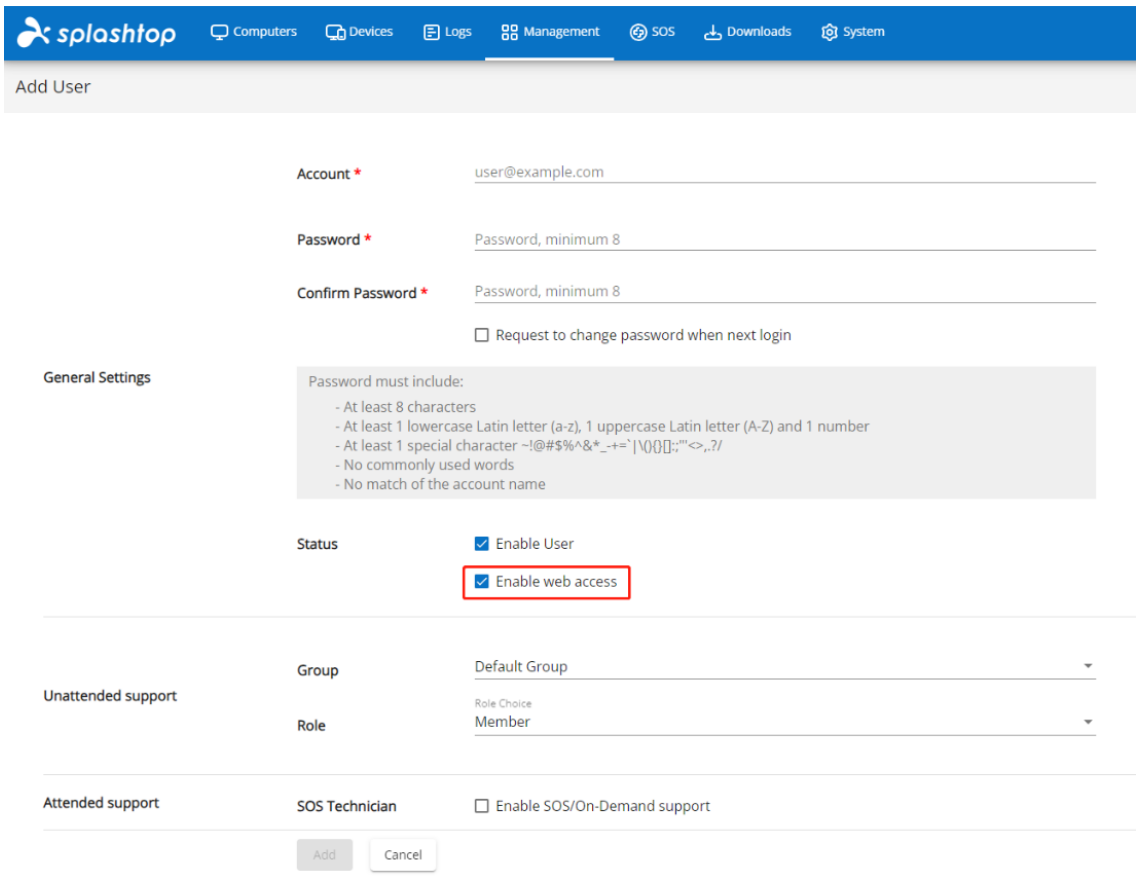
Where to configure web access

Log in to your Gateway web console with the owner or admin account.

Create User

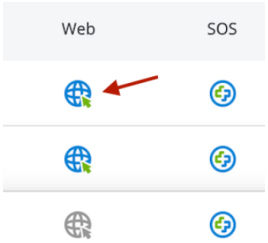
You can set the web access when creating new users. Navigate to *web/management/users* page, click on **Add** or **Import**.



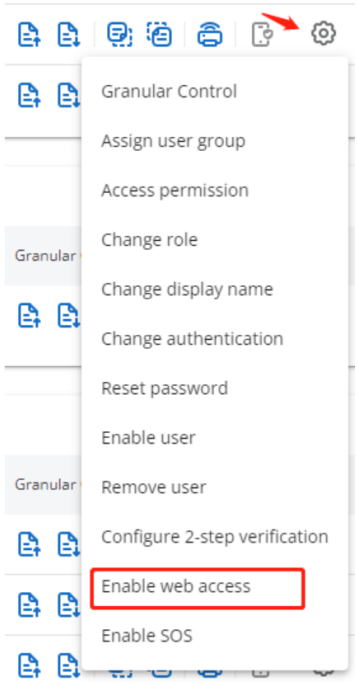


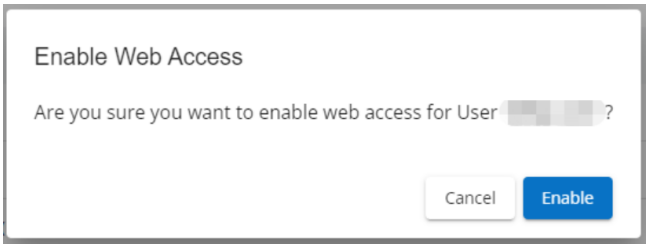
Edit User

Enable/Disable Web access from /management/users tables.



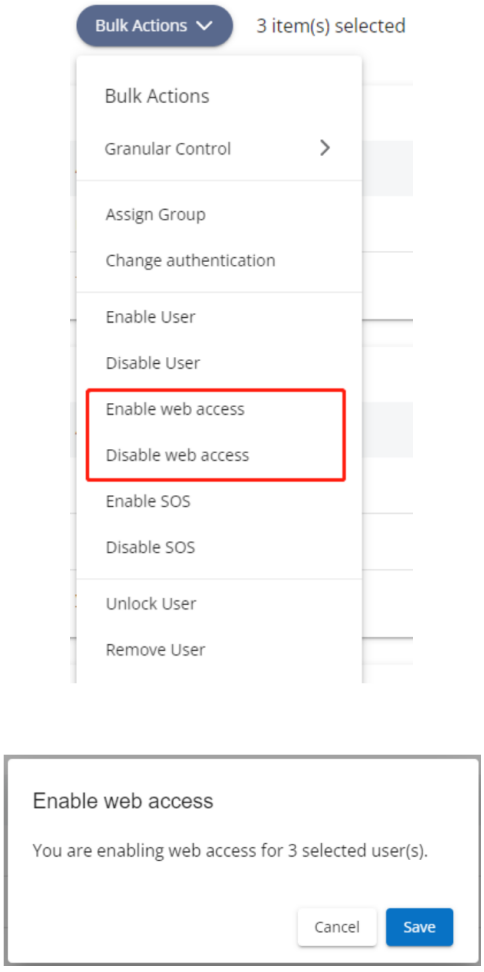
You can choose a specific user account and set the web access for the specific account. Navigate to *web/management/users* page, next to each user in the user list, click on the gear icon and choose **Web access**.





Bulk actions

You also can set the web access for multiple accounts via bulk actions. Navigate to *web/management/users* page, click on the gear icon and choose **Web access**.



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.

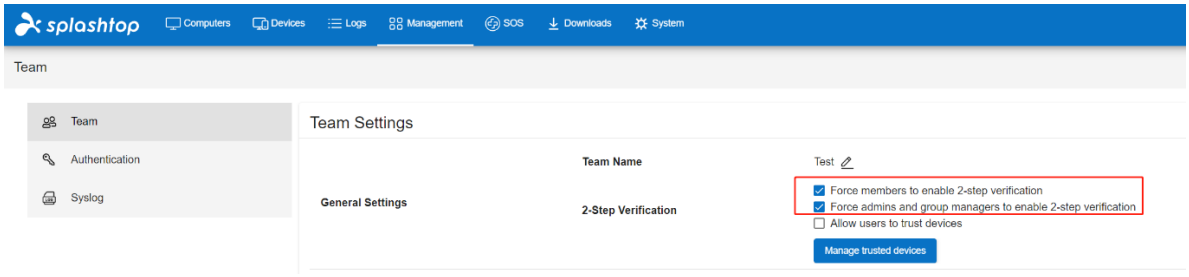
Splashtop On-Prem support TOTP (Time-based One-Time Password algorithm) based 2 step verification, and verified with the following authenticator apps:

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

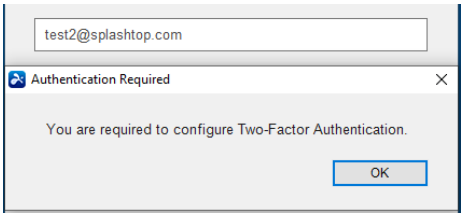
Setup Guide

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.

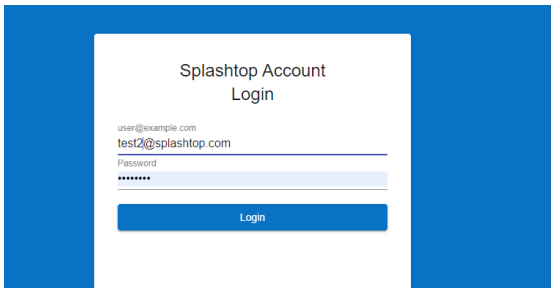


If an account has been enforced to enable 2-step verification, he/she will be required to pass through the 2-step verification setup guide to continue using the service, or it will pop up the following window when they try to log in to the client app.

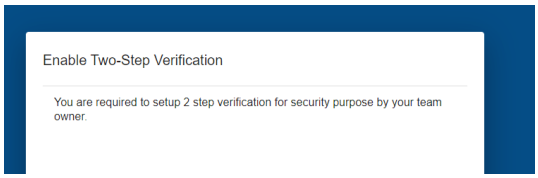


Step 2

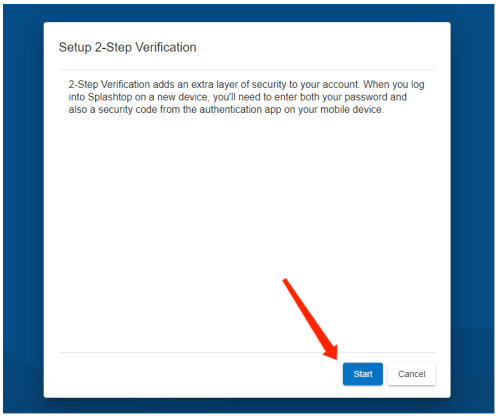
To set up the 2-step verification account for the first time, the user is required to log in to the **Gateway** using his/her own account.



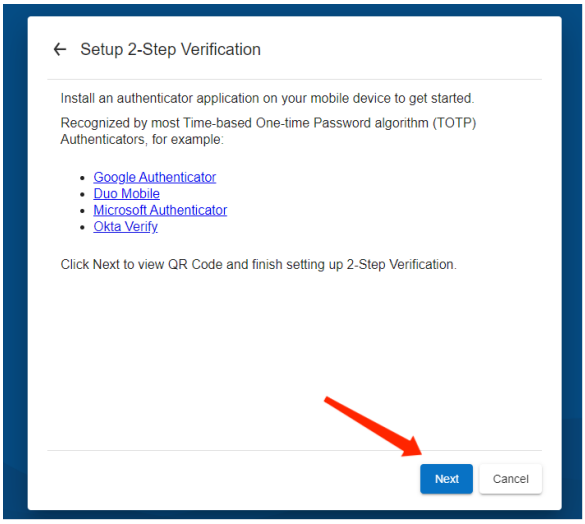
Follow the instructions to complete the setup.



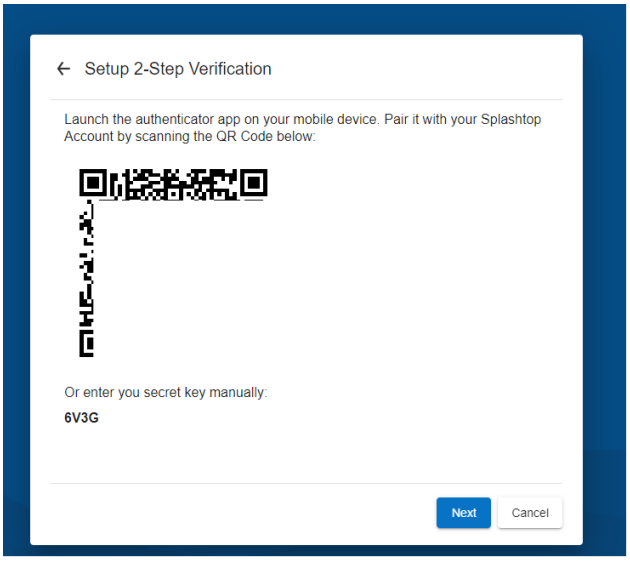
Click **Start.**



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

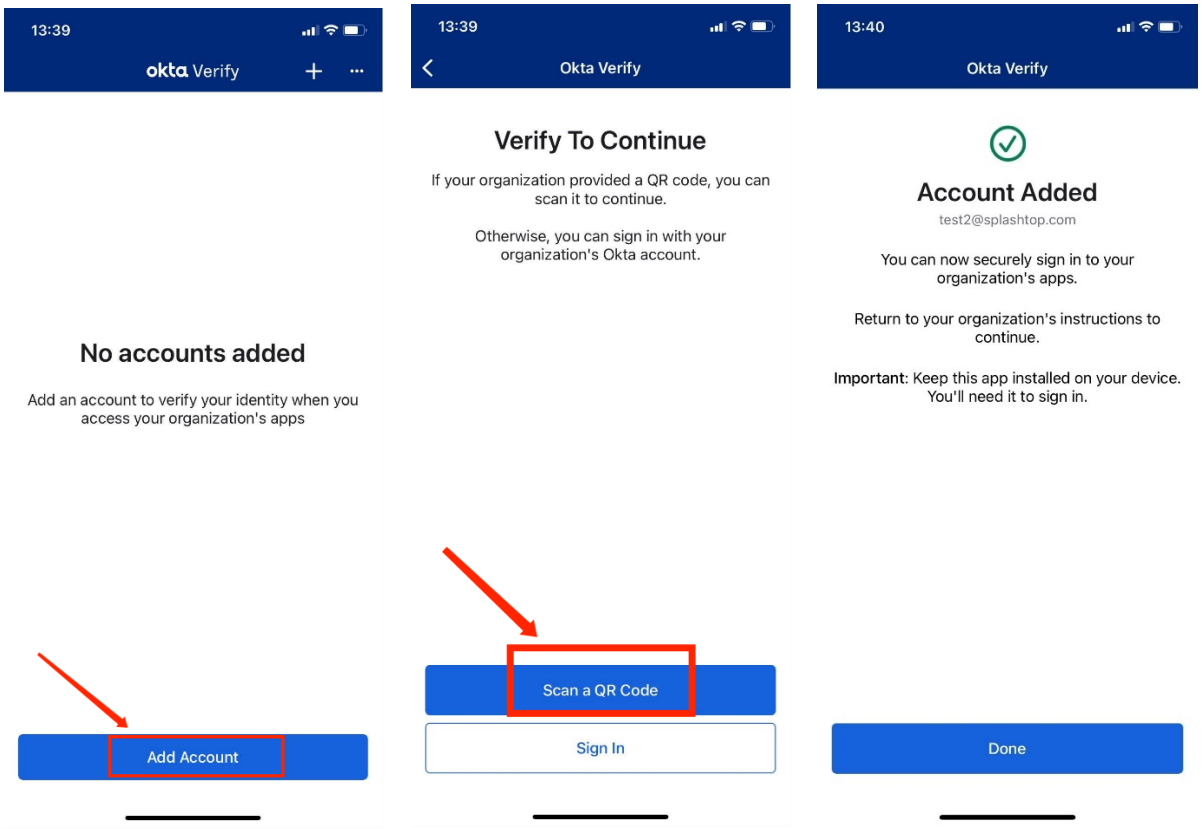


It would generate a **QR code**, users need to launch the **authenticator app** to scan it.

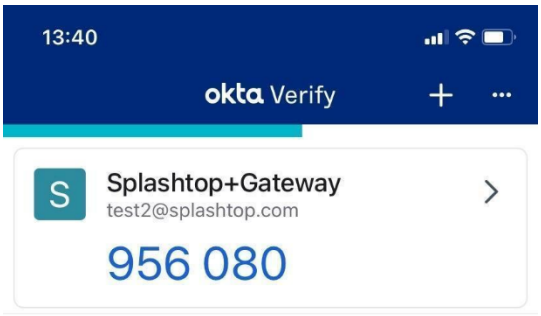


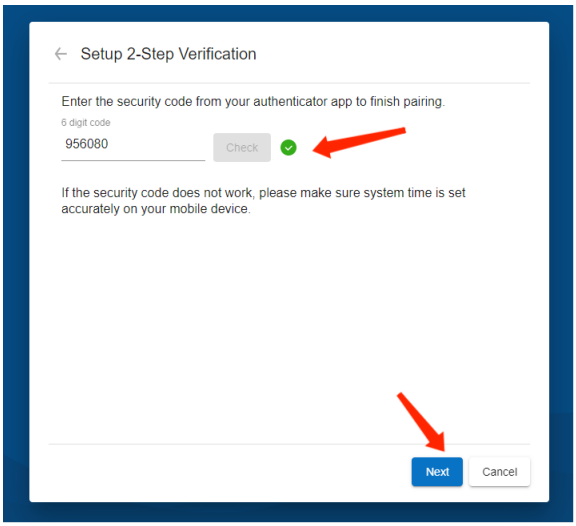
Launch the **okta Verify** and complete the following steps.

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

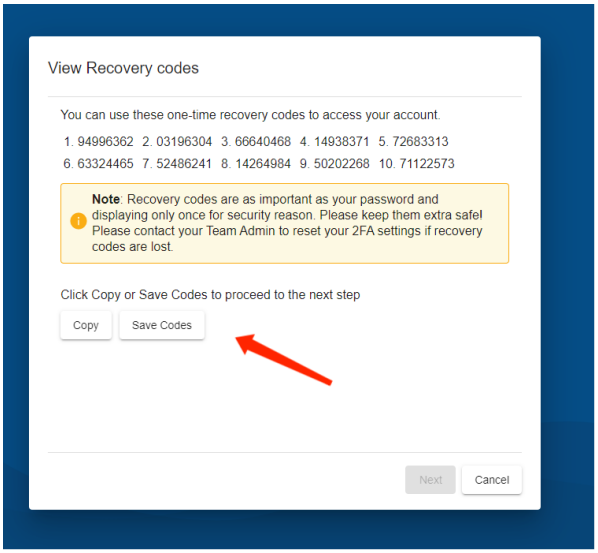


It will generate the **security code** on your app. Enter the security code from your authenticator app to finish pairing.

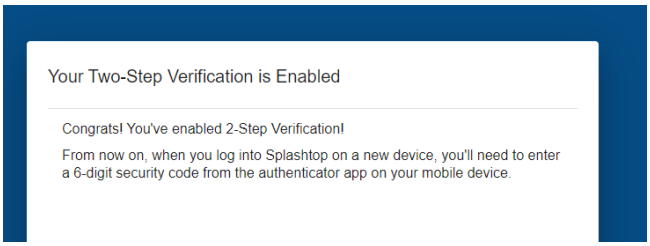




Click **Copy or Save codes** to proceed to the next step.



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



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.

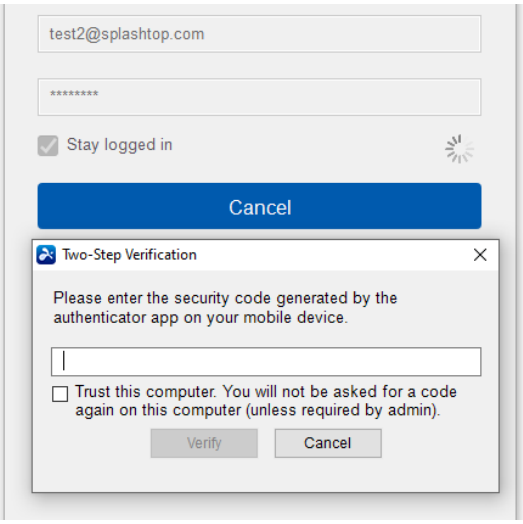


Figure. 2-sv passcode input dialog on On-Prem app

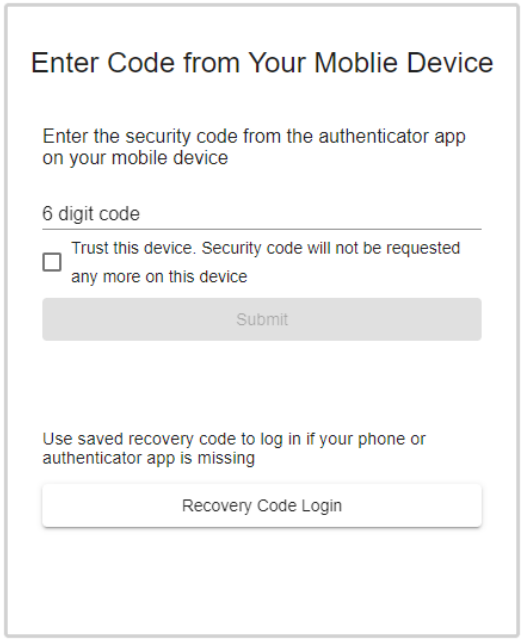


Figure. 2-sv passcode input dialog on web console

Q&A

1.Why do I always get errors with 2-sv passcode?

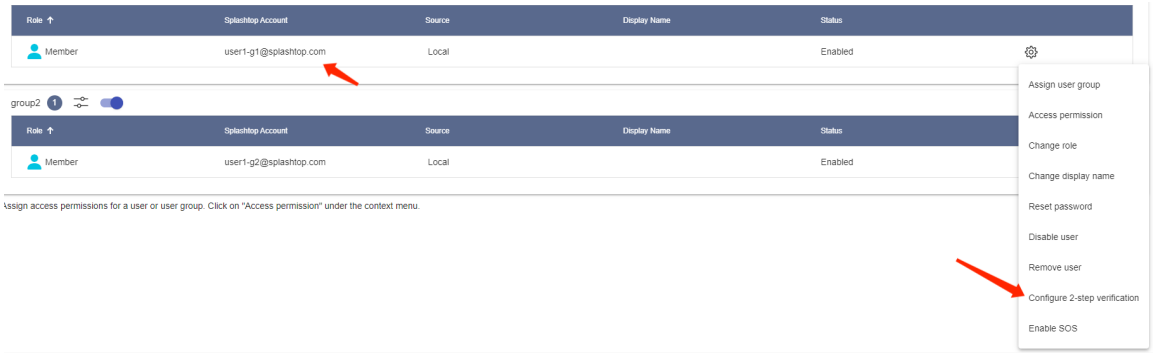
TOTP is working as a time and clock-based authentication, when there are obvious system clock differences, like more than 30 seconds, you may encounter error to pass 2-sv passcode. Please make sure the system time of Gateway server and your authentication keep in synchronized.

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

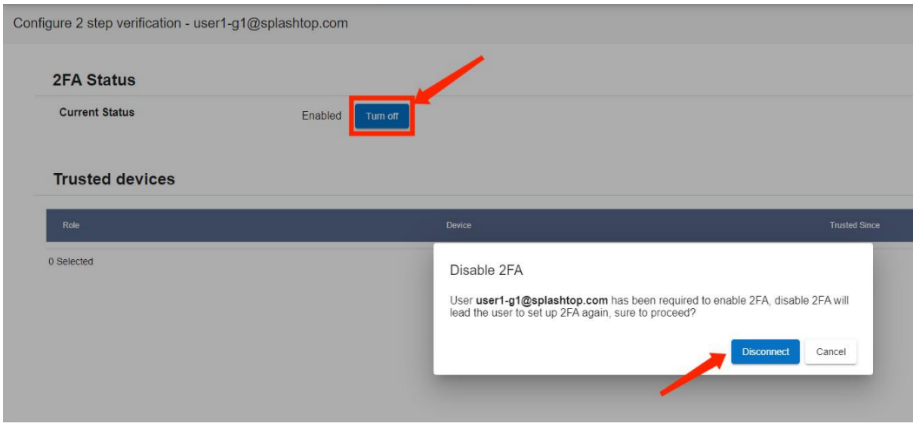
Please contact your **Team Admin** to reset your 2FA settings if recovery codes are lost.

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



3. Disable 2FA

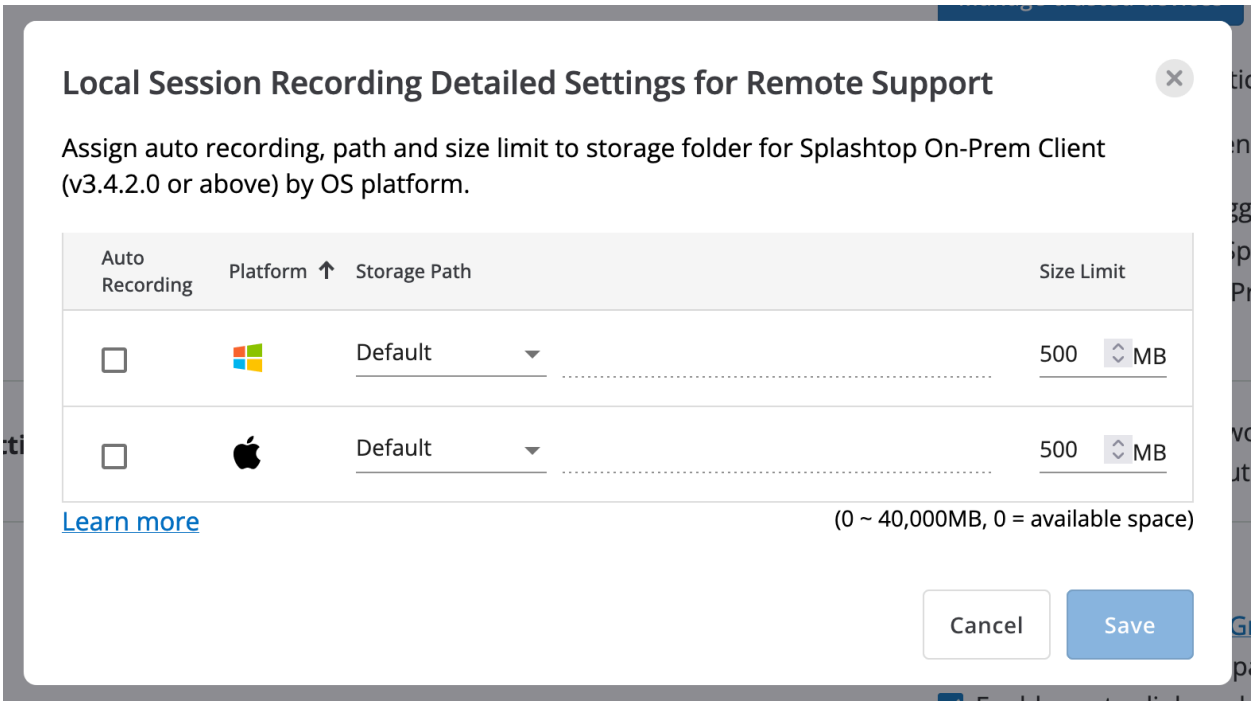


4. User could set up 2FA again.

Notice: TOTP is working as a time and clock-based authentication, when there are obvious system clock differences, like more than 30 seconds, you may encounter error to pass 2-sv passcode. Please make sure the system time of Gateway server and your authentication keep in synchronized.

Local Session Recording on Gateway Web Console

Local Session Recording Detailed Settings



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

Centralized Session Recording

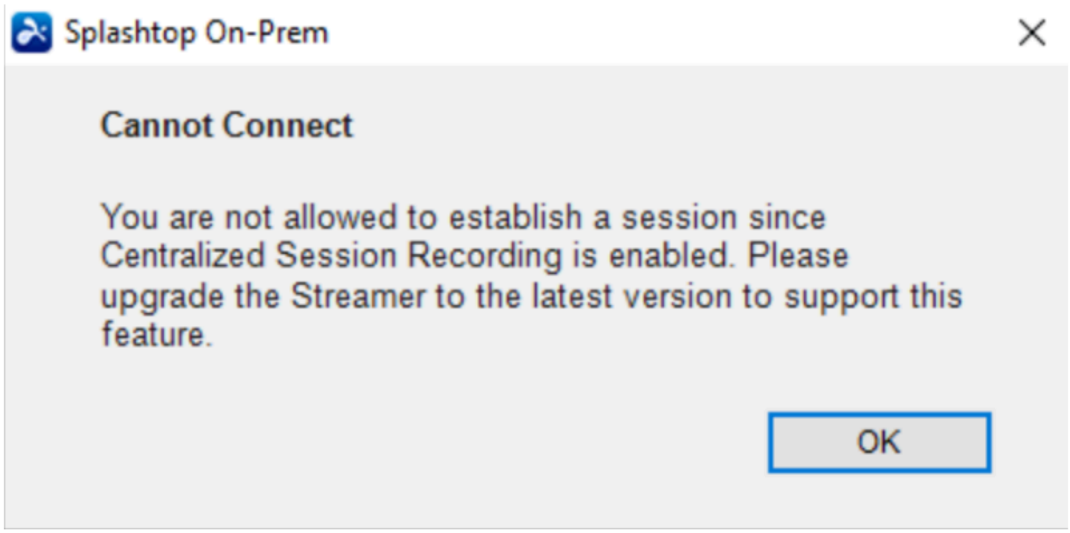
BETA TESTING - We are currently in beta testing phase of this new recording feature. Please contact Splashtop sales if you would like to give it a shot.

With centralized session recording, IT admin can enforce the recording of all Splashtop remote desktop sessions. All sessions are recorded by Splashtop Gateway server, and once this feature enabed the technicians do not need to manually start or stop recording from client app side.

The session recording videos can be played back or downloaded via the Splashtop web console, for training as well as auditing purposes.

Requirements

- **Local Computer** (technician side): Windows and Mac only; Client app v3.5.2.2 or higher.
- **Remote Computer** (endpoint/end user side): Windows, Mac, iOS, and Android; Streamer v3.5.2.2 or higher. If the streamer does not meet the version requirement, the session will be blocked with the following error message.

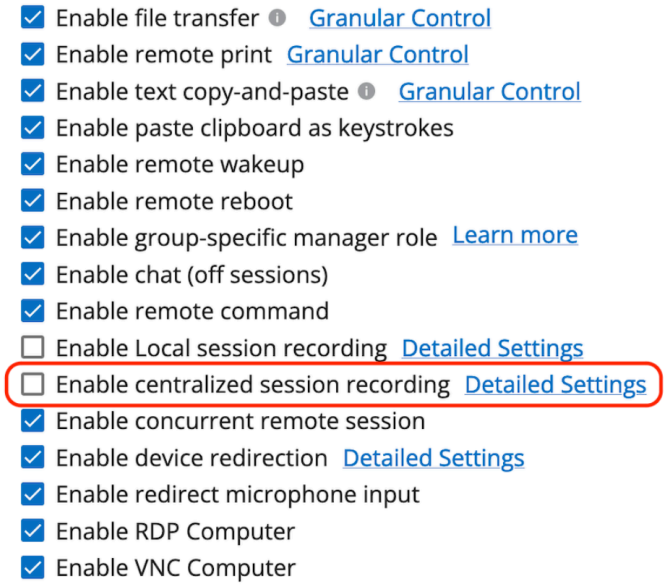


Enable Centralized Session Recording on the Web Console

Please contatct Splahtop sales representative to activate the add-on feature for your license.

Centralized session recording is disabled by default and can be enabled via the Splashtop web console.
(Gateway web console-> Management ->Team Settings -> Remote support / SOS settings)

Settings

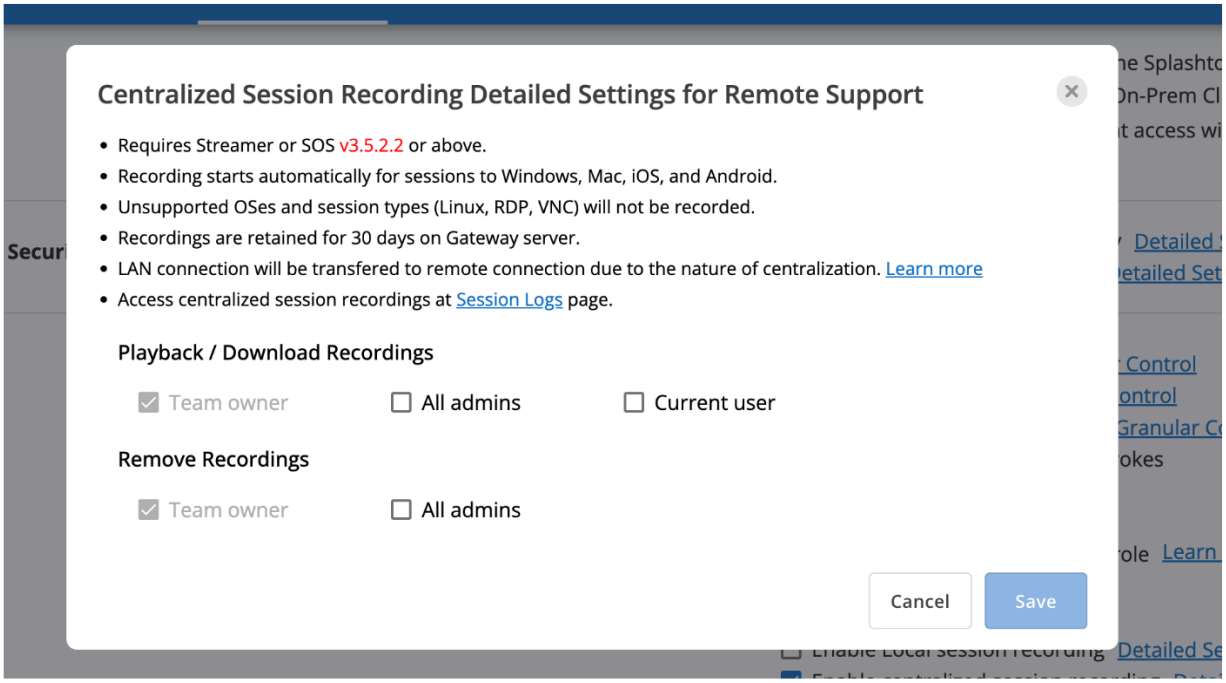


Detailed Settings

The ability to playback / download or remove recordings can be granted based on user role. Team owner is granted all permissions by default.

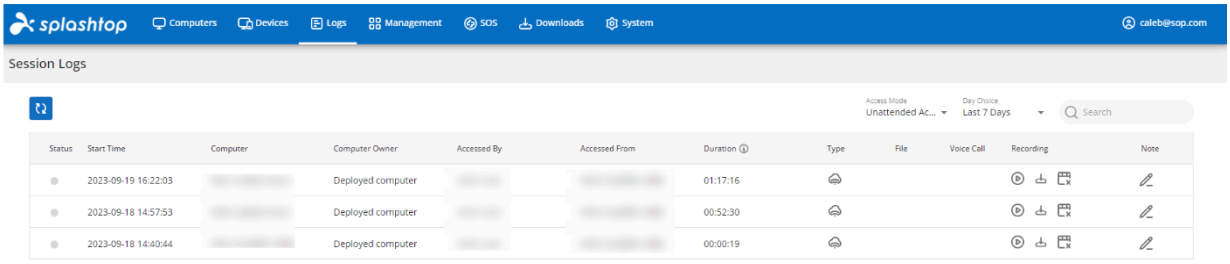
For utmost security in handling the recording files, the encrypted streaming data must be stored in your Splashtop Gateway to make sure file integrity. As a result, the LAN connection between Splahtop client app and Streamer will be redirected to your Gateway server.

The recording files are retained for 30 days on your Gateway server. Make sure to download all the files needed in time for future use.



Playback and Download

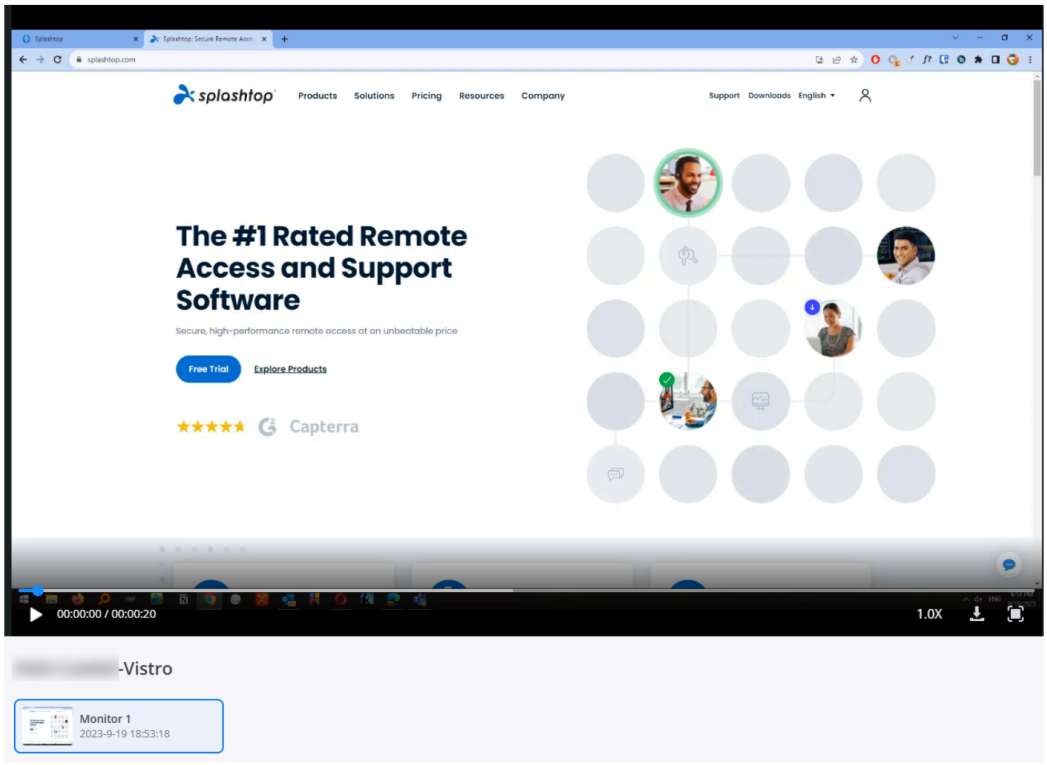
Recordings can be accessed from sessions log page in Splashtop web console. (Gateway web console -> Logs -> Sessions)



The Recording column on Session logs displays the access methods of a specific session.

Click on the recording icon next to a session to see the recording(s) for that session.

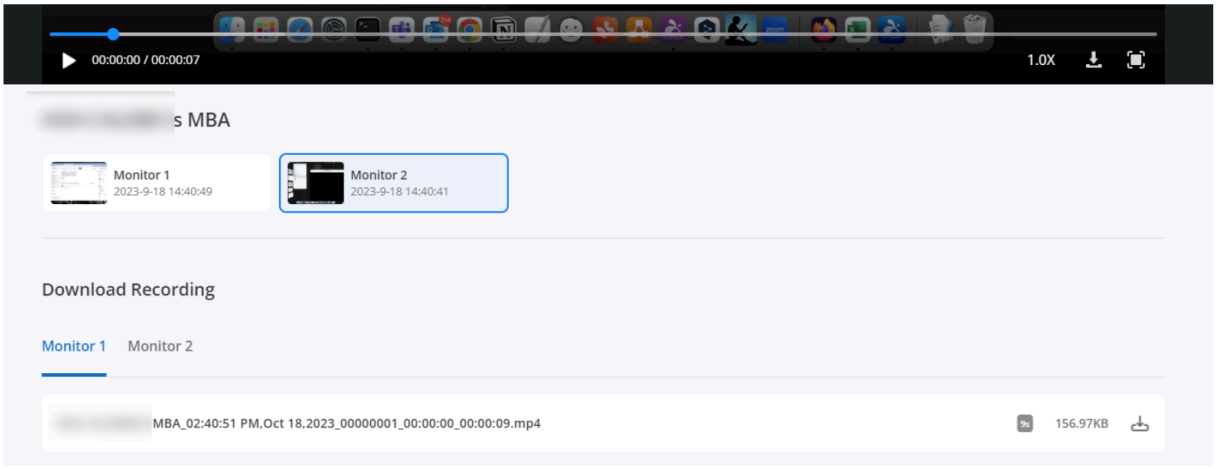
Playback



The recording will be split into multiple files when:

- File size reaches 512 MB (e.g. if total recording size is 3GB, it will consist of six files).
- Technician switches the view to a different monitor.
- Technician changes the frame rate.
- End user's device switches orientation between portrait and landscape.

Download your recordings



Click the download button either from Session logs web page or Player toolbar to enter the download interface and chose the .mp4 to download.

Notes

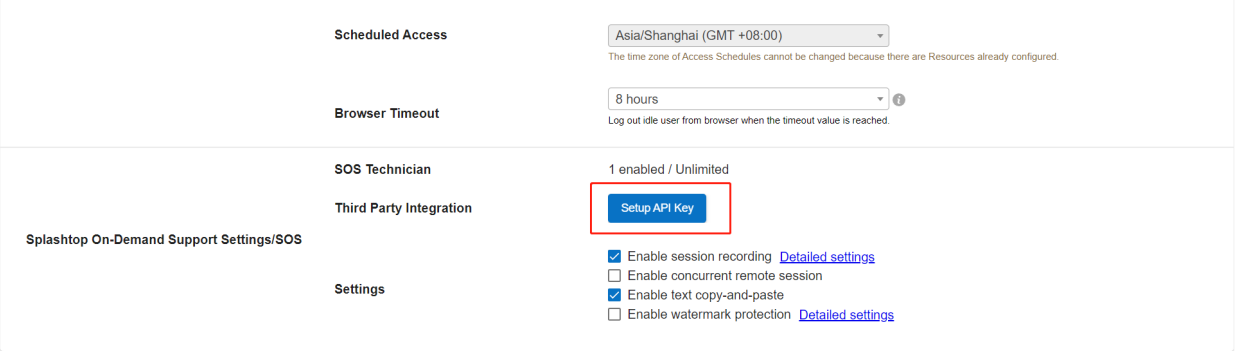
- Recording is performed by Splashtop Gateway as the sessions passing through the server. All sessions will be proxied through Splashtop Gateway so that no other parties can touch the recordings.
- Timestamps of recordings are based on the time zone of the session logs.
- Mouse cursor and audio are not part of the recording.
- If a session has multiple recording files (e.g. if technician switched the monitor view), the files are organized by monitor and by timestamp in the file name (see screenshot above).

Set Up API Keys for Third-party Integration

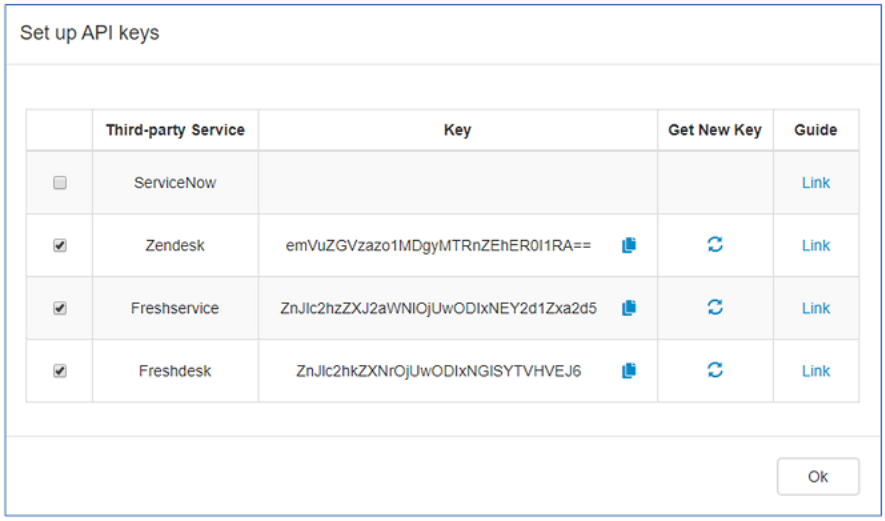
An API key is generated in Splashtop Gateway and passed to a third-party ticketing system, which is used by the ticketing system to authenticate access to the back-end of Splashtop On-Prem system. The API key is basically the linkage between the ticketing system and Splashtop On-Prem back-end. A ticketing 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



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.



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

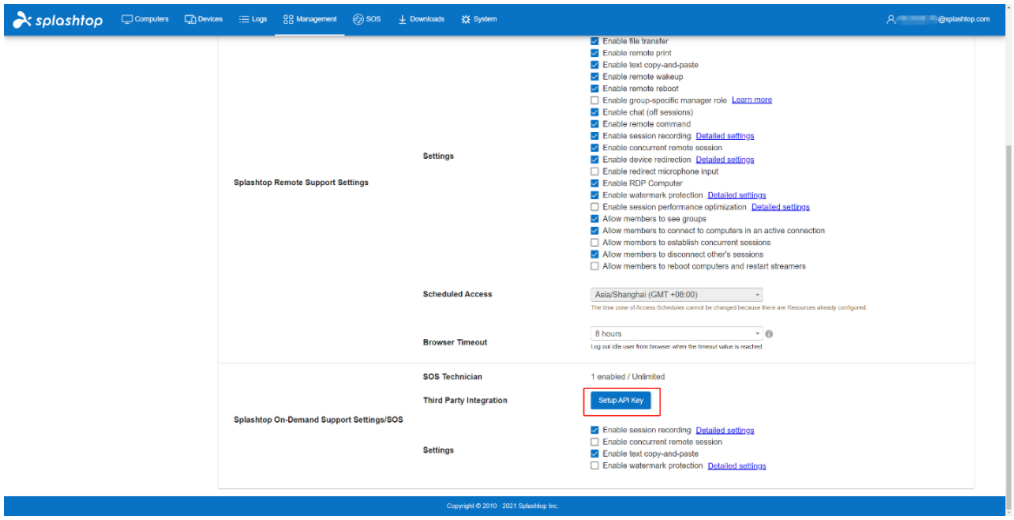
The setup of Splashtop On-Prem - Freshservice Integration is a one-time effort to connect the two systems using an API key. You'll need an administrator account for both Splashtop On-Prem and Freshservice to carry out the task.

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**.



SMTP Server Integration

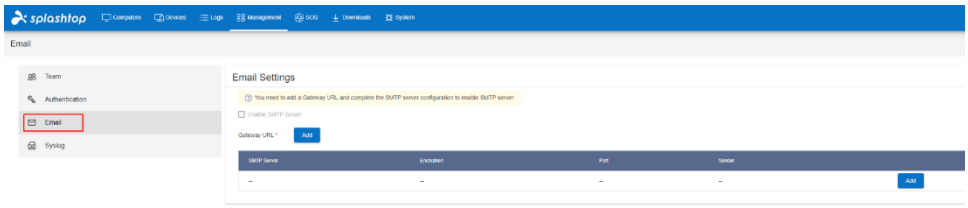
Introduction

SMTP Server is a feature that allows you to integrate a Smtp server to Splashtop On-Prem Gateway in the team settings. When SMTP server is successfully configured, devices can be authenticated by email.

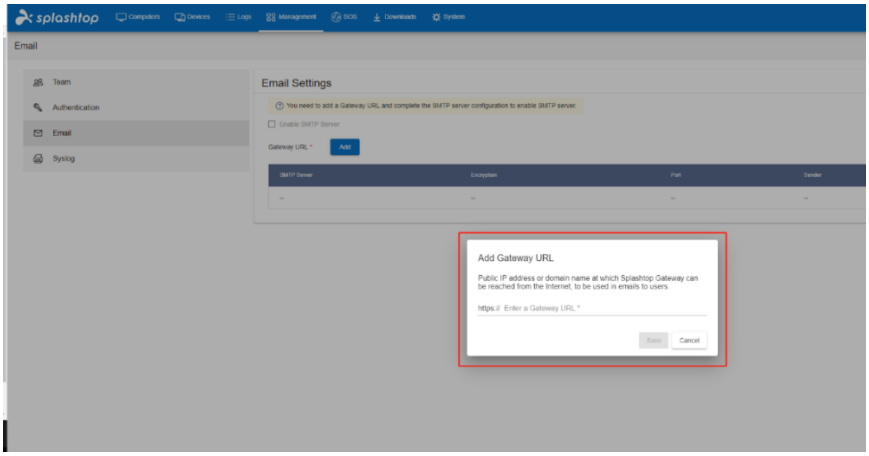
SMTP Server Configuration

- First, go to *https://{gatewayaddress} -> Management -> Team Settings -> Email* to configure the **SMTP server**. The SMTP server can only be enabled if all required

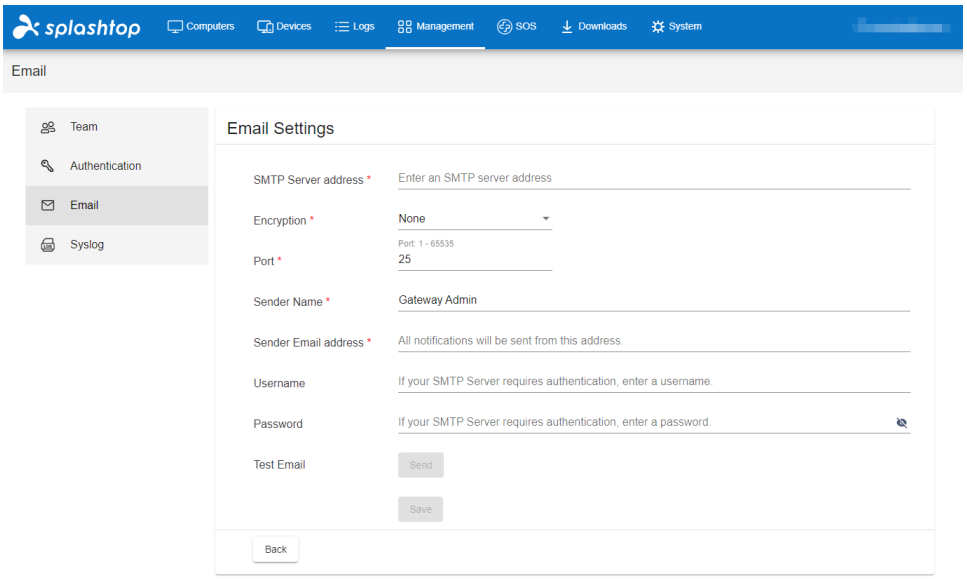
information has been successfully saved



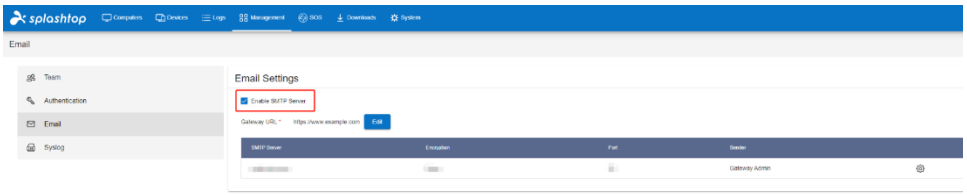
- Click "Add" to embed the Gateway URL in your Email. In the scenario that Gateway server is behind layers of firewall, Splashtop Gateway itself has limited capability to acquire its public address, thus requests origin from user's Email client would fail to reach Gateway and result in failure of some events. For instance, device authentication is done by clicking the authentication link in the email, which will be handled by your Gateway system. A correct Gateway URL insert is needed in this case to ensure every auth requests can reach the Gateway server.



- Click "Add" for SMTP server and fill in the fields of SMTP server. To ensure that SMTP server is configured correctly, the SMTP server needs to be verified before saving.

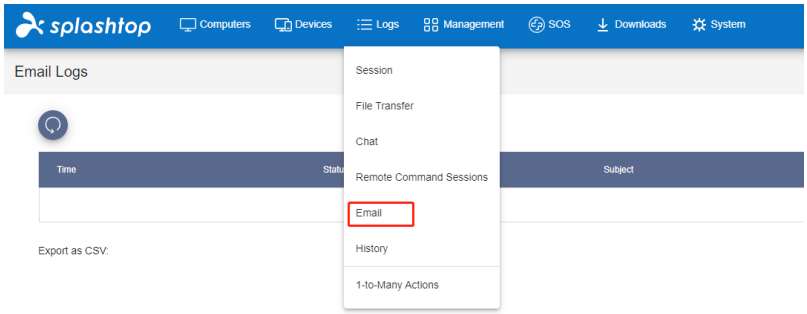


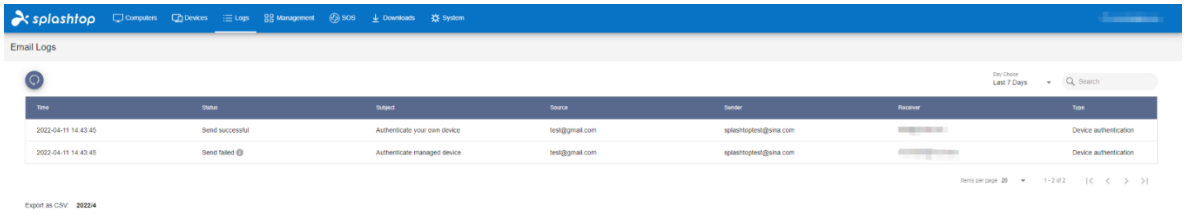
- When Gateway URL and SMTP server settings are successfully saved, click the check box to enable SMTP server.



Email Logs

- Go to *https://{gatewayaddress}* -> *Logs* -> *Email* to check the email log. Team owner/Admin can check the status of emails sent in the email log and detect problems in time.





Notes

- If SMTP server has changed, please modify the settings in Gateway in time. Otherwise, it may cause mail sending failure.
- In the email log, the status only indicates whether the mail was successfully sent to the SMTP server or not. Please fill in the correct email address to get the email.

Device/Browser Authentication

For better security, all devices where you run the Splashtop On-Prem app and log in with your Splashtop Account now need to be authenticated via email or web console.

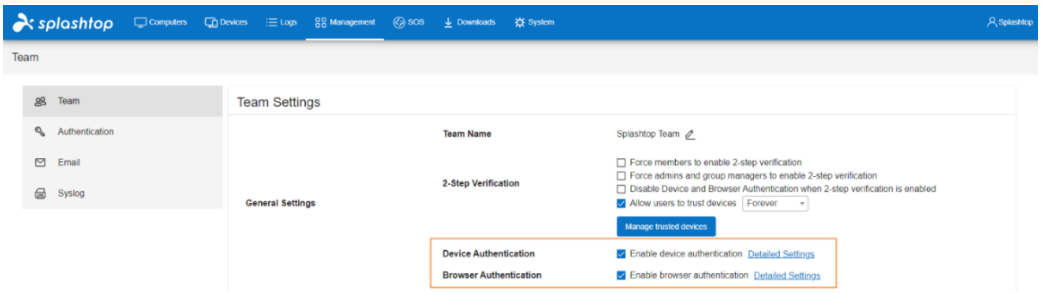
The emails should only trigger once per application/browser per computer. Meaning logging into the On-Prem app for the first time will trigger the email once and logging into the website in a new browser should trigger it once.

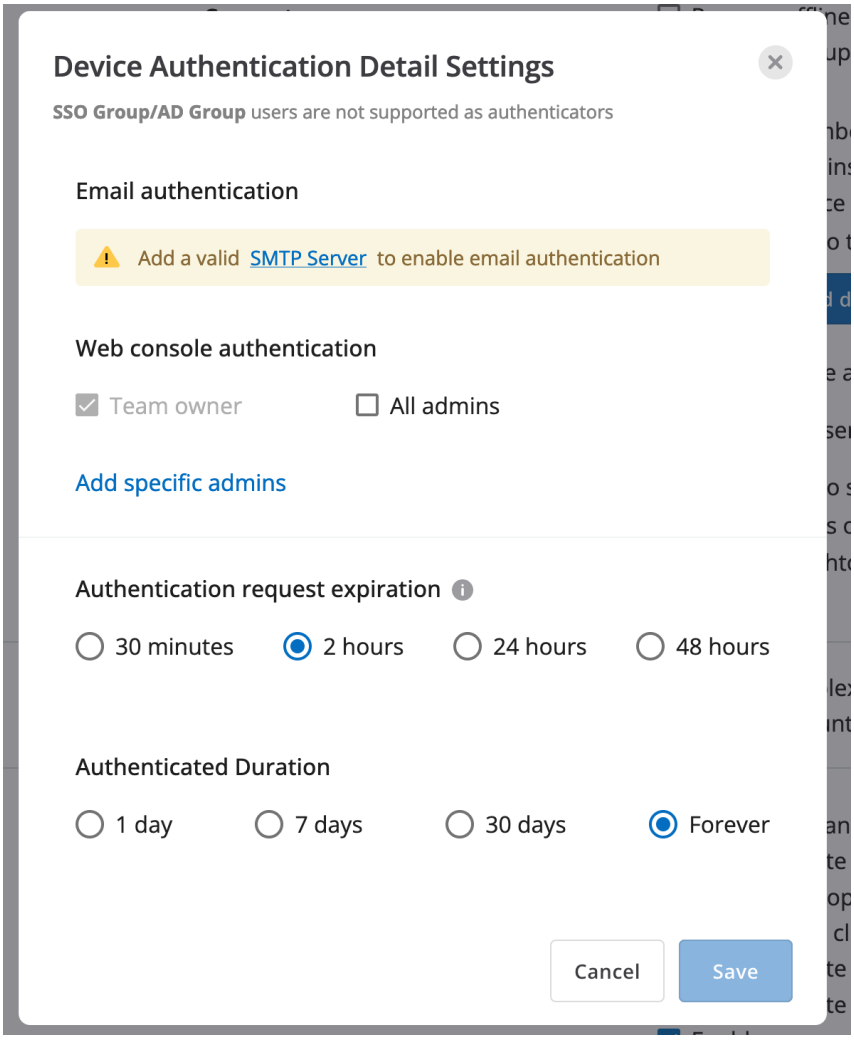
When you log into a new device for the first time, if your system administrator decided to use email authentication, we will email you an authentication link. You will need to click on the link before you can log in successfully and start using the Splashtop On-Prem app on that device. (Wait 5 minutes to try a login to get another email sent out).

System administrator can configure detail settings with the owner account by log in Splashtop Gateway web console top menu->Management -> Team Settings.

- Authenticator: Selected users can authenticate each log-in attempt generated from Splashtop On-Prem app or Splashtop web console by verification email or from web console.

- Authentication request expiration: If the authentication request is left pending for longer than the configured expiry time without anyone verifying it, end users need to resend the authentication request.
- Authentication duration: Once authenticated, the user won't have to authenticate the same device/browser within the configured duration.





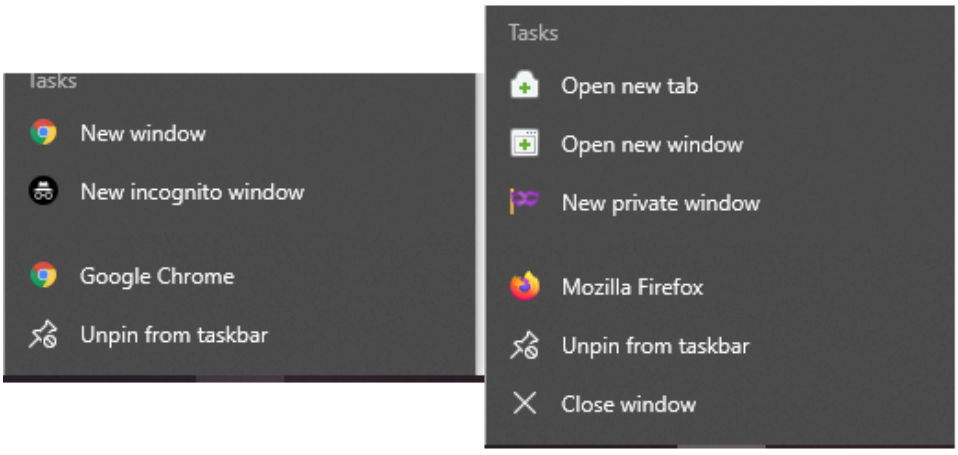
Why am I not getting verification emails?

If you are not seeing the emails, please check the following:

- Please check in a few minutes, mail routing may be delayed
- Please check your spam and junk folders
- Your email service (i.e outlook) has a black or whitelist and we are being blocked by that list/ yet to be approved.
    - In Outlook 2010/2013, click the **Junk** button on the ribbon and select **Junk E-Mail Options**. You'll find the whitelists on **Safe Senders** and **Safe Recipients** tabs. Blacklist is on **Blocked Senders** tab.
- Your network/domain has all emails from splashtop blocked and auto removed
    - Should this be the case please communicate with your local network/IT admin to allow splashtop emails through.

Clicking on the verification link doesn't work?

Sometimes you receive the verification email but clicking on the authentication link doesn't work. This can happen if the saved cookies on the browser are interfering sometimes. The easiest solution is to open a new private browser/incognito window.



Then from here fetch a fresh authentication email and go to your email to authentication all while using the incognito window/private window.

Notes

1. Please add a valid SMTP Server and test the function before using Email device/browser authentication.
2. If you no longer have access to the email address you used as the Splashtop ID, please change your Splashtop ID to a new email address and try to log in again. The authentication email will be sent to your new email address.
3. Changing your Splashtop ID will clear all previously authenticated devices.

Splashtop On-Prem Complex Password Policy

When create or update a password, it is important to choose one that meets the password complexity requirements.

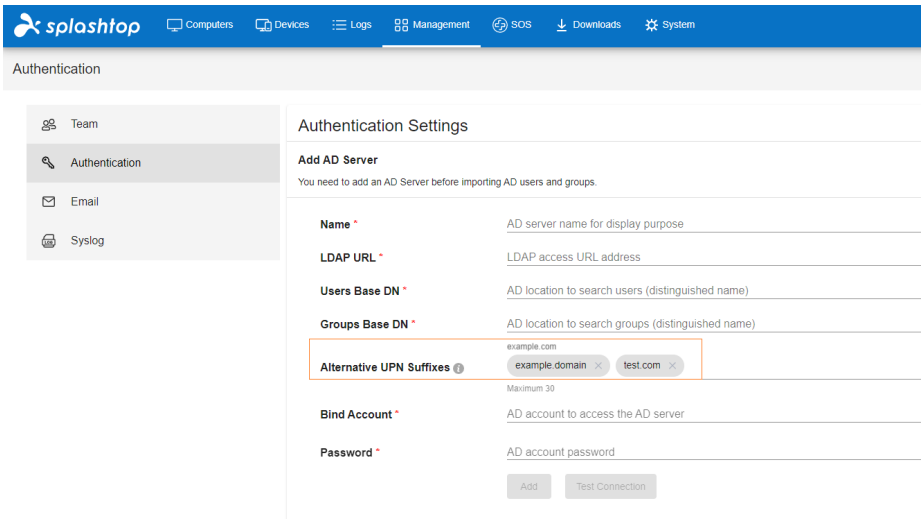
Complex Password Policy:

- 8 (minimum length is defined by your system administrator) or more characters
- At least 1 uppercase Latin letter (a-z), 1 lowercase Latin letter (A-Z), 1 number (0-9)
- At least 1 special char ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/
- No commonly used words
- No match of the account name or the last 5 passwords

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 -> Team 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.
- **Alternative UPN Suffixes:** This field allows you to add those UPN suffixes, when adding AD user in user management page, you can choose which domain suffix the user can use to login
- **Bind 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**.

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.

How to use Open API

Open API is a new feature that allows you to access data and manage your user accounts and computers. You can also use the Open API to develop apps that integrate Splashtop On-Prem functionality into your own corporate environment. Please follow the below instructions to apply for an Open API application for your team.

For more details, please refer to the API reference .

Requirements

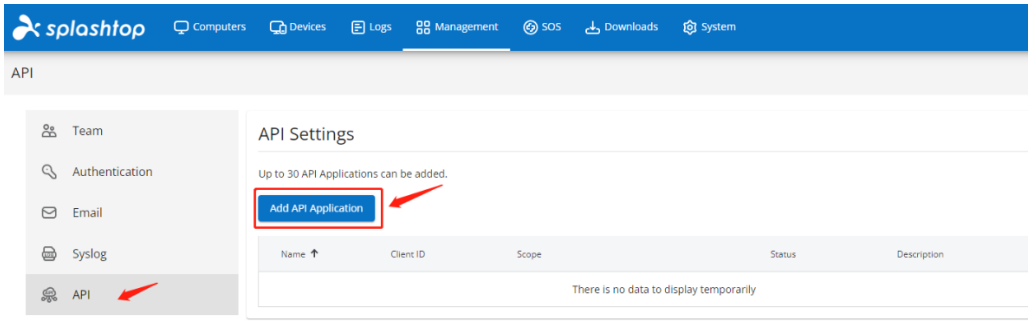
- **Splashtop Gateway v3.24.0** or higher.
- Open API is enabled in your license.

Configuration flow

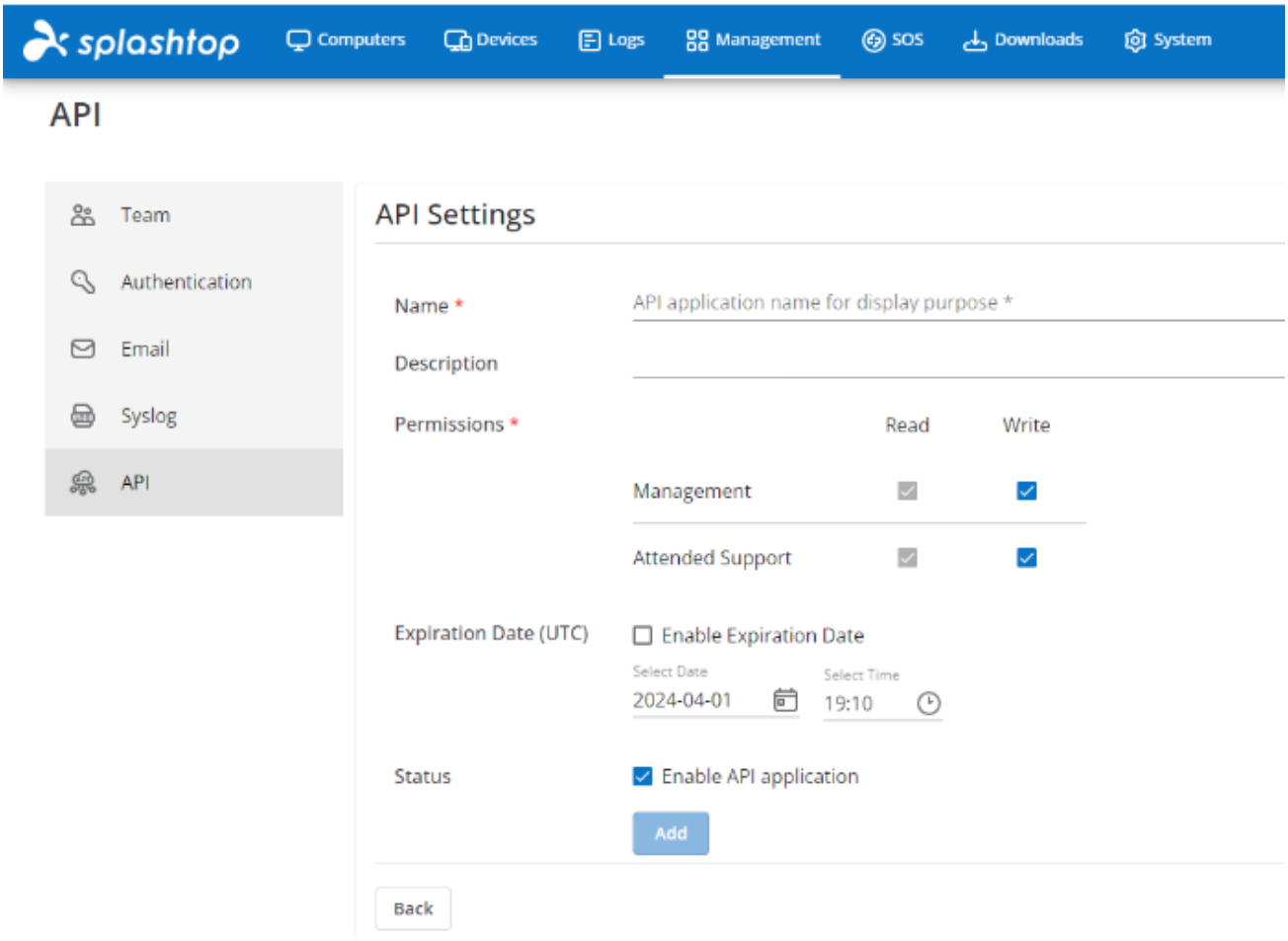
1. Make sure that Open API in your license is enabled. If you have any questions, please contact sales for more information.

2. Log in to your Gateway with the Team Owner's credential.

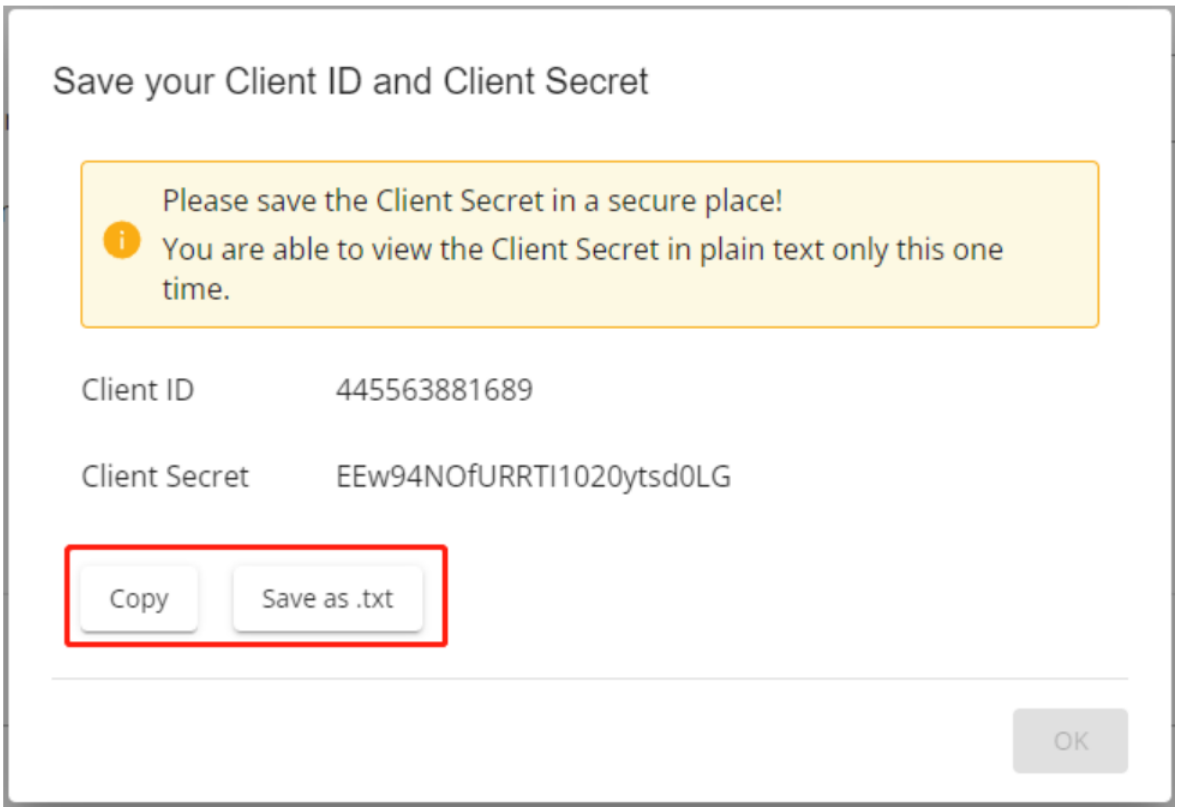
3. Go to **Management** > **Team Settings** > **API**, and Click **Add API application** button on **API Settings** page.



4. Enter API Application **Name** and configure the **API permission** (read or write), then click **Add** button.
    a. **Name**, API application name for display purposes.
    b. **Permission,** set the API permission for the API application.
        i. **Management**, when this item is enabled, allows you to **use user/access permission/computer/group/schedule/security**-related API
        ii. **Attended Support** (Requires Gateway v3.28.0), when this item is enabled, allows you to use **psa**-related API.
        iii. **Read**, when this item is enabled, allows you to use **GET** API.
        iv. Write, when this item is enabled, allows you to use **GET/PATCH/POST/PUT/DELETE** API.
    c. **Expiration Date** (Requires Gateway v3.28.0), set the expiration date for your API application. When the API application expires, APIs initiated from this API application will be blocked.
    d. **Status**, enable the API application to use Open API.



5. Click **Copy** or **Save as .txt** to save **Client ID** and **Client Secret** in a secure place, then click **OK**.



API functions

The API uses **OAuth 2.0** and **REST-based** for authentication and **JSON** for data communication.

API rate limit

Each API has a limit of 200 calls per minute.

API Documentation

API reference

Account Lockout Policy

The Account lockout policy setting **determines the number of failed logins attempts that will cause a user account to be locked**. A locked account can't be used until Admin or Owner reset it or until the number of minutes specified by the Account lockout duration policy setting expires.

Introduction

Account lockout threshold: The policy setting determines the number of failed login attempts that will cause a user account to be locked.

Account lockout duration: The policy setting determines the number of minutes that a locked-out account remains locked out before automatically becoming unlocked.

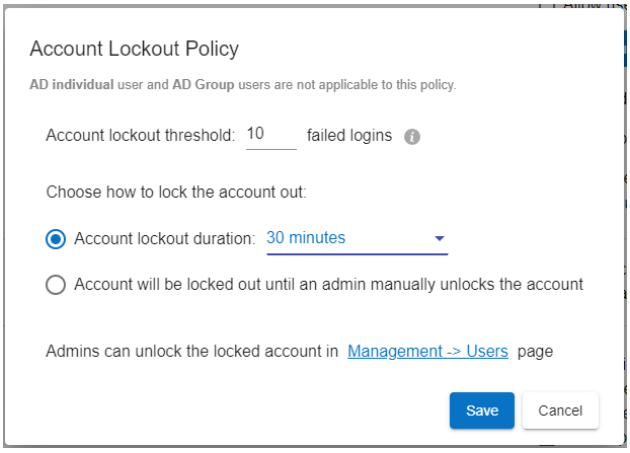
Manual unlocking: Admin or Owner can manually unlock the locked account in Management > Users page

How to set the account lockout policy?

1. Log into Gateway's management console as Owner, go to Management > Team Settings > Security Settings.

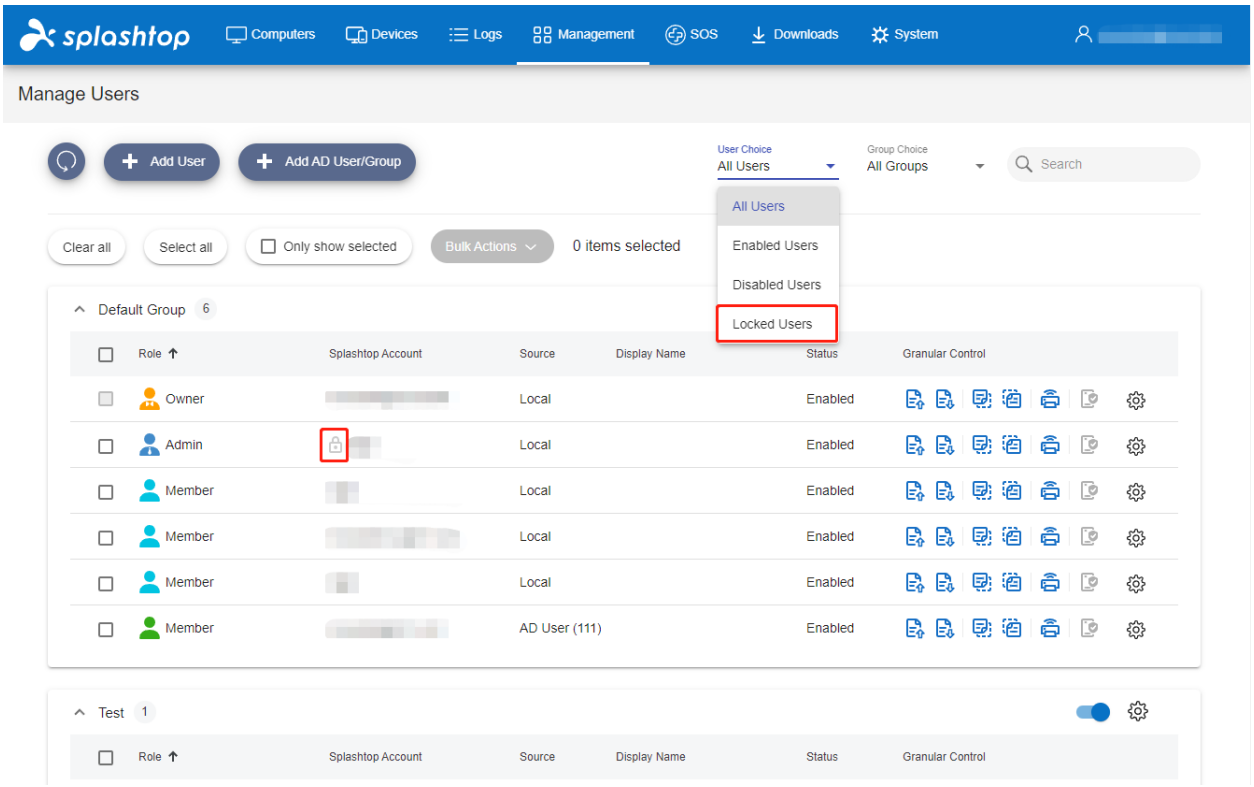
2. Then, Owner can configure the Account lockout threshold and Account lockout duration in detailed settings.

Click Save button to save the settings and turn on the feature.

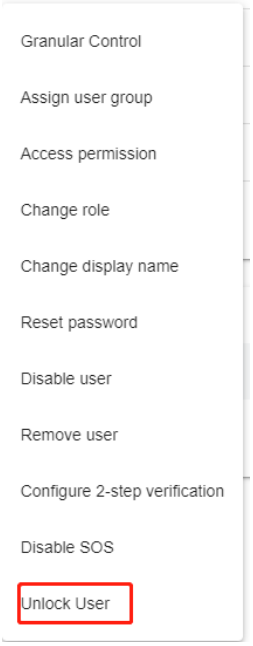


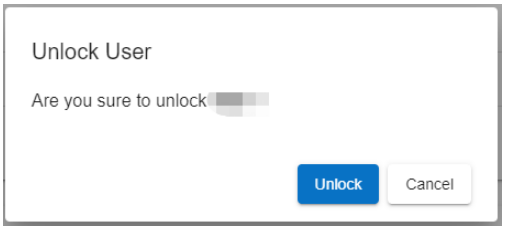
How to unlock the locked account by Admin?

1.Log into Gateway's management console as Admin or Owner, go to Management > Users page. Open the User Choice filter and select "Locked Users".



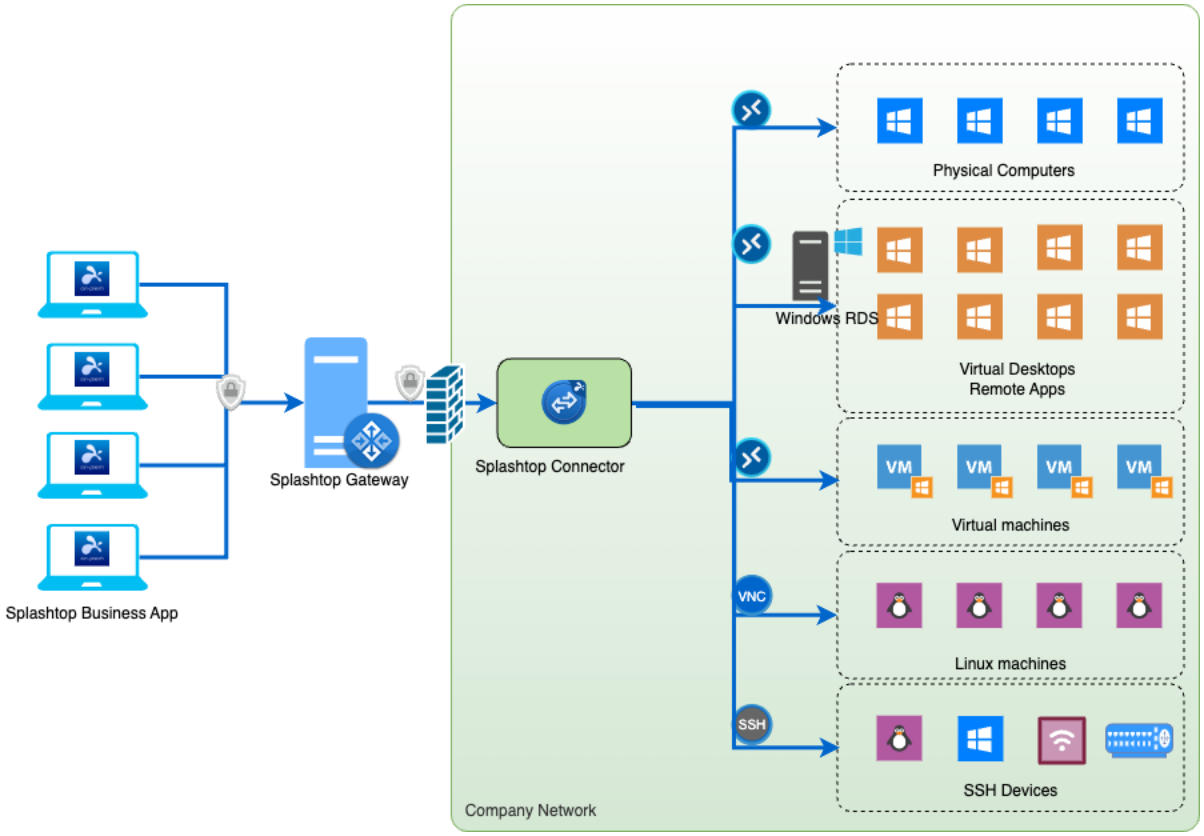
2.Find the locked account, click on the gear icon and choose Unlock user. The locked user will be unlocked after the confirmation.





Splashtop Connector

Splashtop Connector allow users to connect to computers and devices, it supports vary protocols, including RDP/RDS, VNC, SSH, user can directly connect to the computers and devices within Splashtop On-Prem client app, without using VPN or installing any remote access agent.



Capabilities

- Access RDP machines
- Access RDS server
- Access Remote App
- Allow accessing from Splashtop On-Prem client on Windows, Mac, iOS, Android
- File copy and paste (Windows only)
- Text copy and paste
- Session recording
- Remote print
- Multi-monitor
- IP Whitelist/Blacklisting
- Access VNC computers
- Access SSH computers and devices

Advantages

- **Ease of use**, IT admin can pre-configure RDP/VNC/SSH profiles in the Splashtop Connector management interface, and users can access the RDP/VNC/SSH resources as easy as accessing generic Windows machines with Splashtop Streamer installed.
- **Security**, Splashtop Connector will be deployed in the local network where it is routable to the RDP/VNC/SSH machines, so it's not necessary for IT admins to open the RDP/VNC/SSH port over the Internet to allow users to access. Splashtop Connector simulates the RDP/VNC/SSH resources and follows Splashtop's access permission system, so only users with proper access permissions will be able to connect to the RDP/VNC/SSH resource.
- **Auditing**, with Splashtop Connector, all RDP/VNC/SSH connections will have session logs recorded. Splashtop Connector also supports video session recording.

Best practices for deployment

1. Scalability

A single Splashtop Connector has its limitations of simultaneous RDP/VNC/SSH sessions, but you can deploy multiple Splashtop Connectors in your network to scale the capacity.

2. Network access

- The machine where Splashtop Connector is deployed should be able to access your Splashtop Gateway so that it can proxy the RDP/VNC/SSH protocol.
- The machine where Splashtop Connector is deployed should be able to access the RDP/VNC/SSH machines via RDP/VNC/SSH protocol. For better security, you can open the RDP/VNC/SSH protocol over local LAN access only.

3. Security

Grant access permission only to users that need to access these RDP/VNC/SSH machines.

Installation

Download Splashtop Connector software

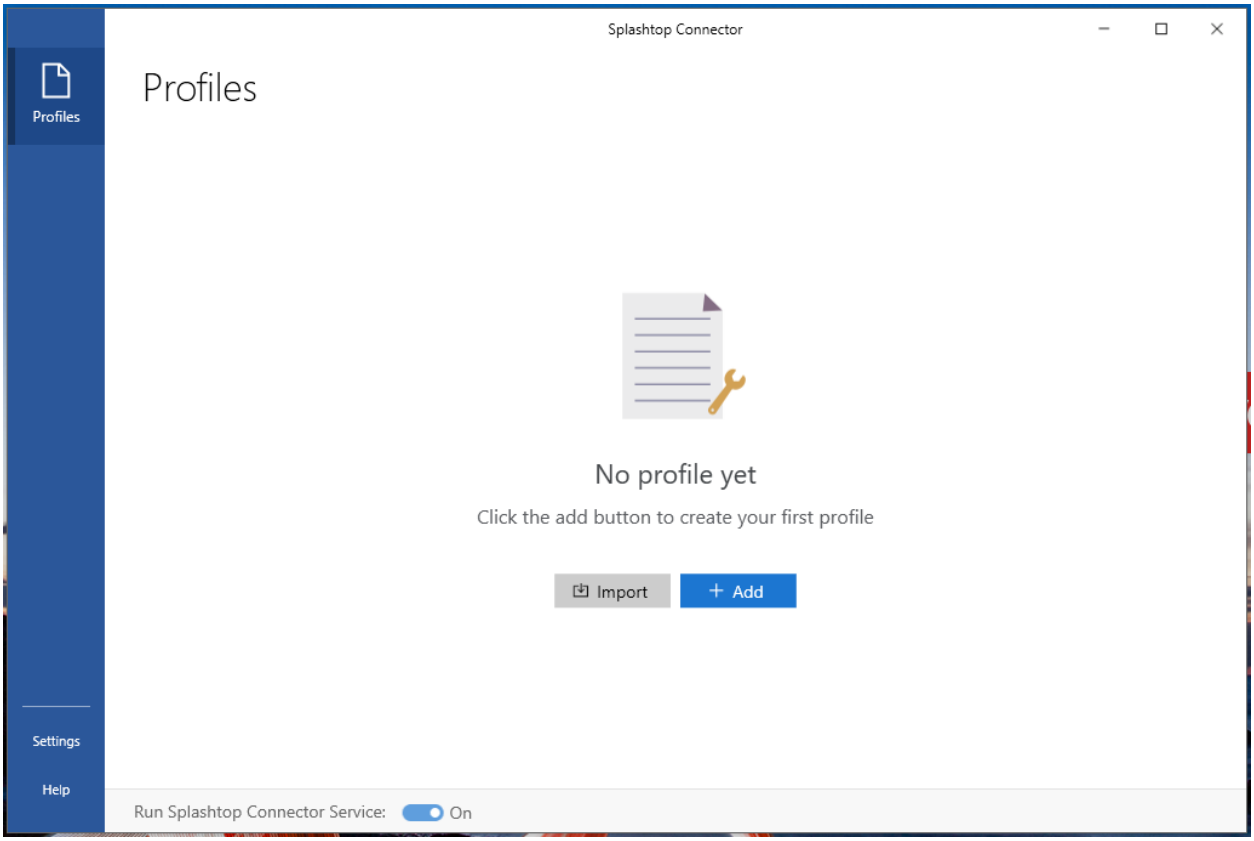
System requirements

- Windows 7, 8, 10, 11, Windows Server 2012, 2016, 2019 (with .Net 4 or up)
- RAM: 8G or up
- Storage: 50G or up
- Network
    - Routable to the RDP/VNC/SSH machines

Installation

Run the Splashtop Connector installer. Once installed, you should be able to see the Splashtop Connector management user interface, pictured below. Please make sure **Run Splashtop Connector Server** is turned **ON.**

Now you can create profiles to enable proxying to your RDP/RDS machines.

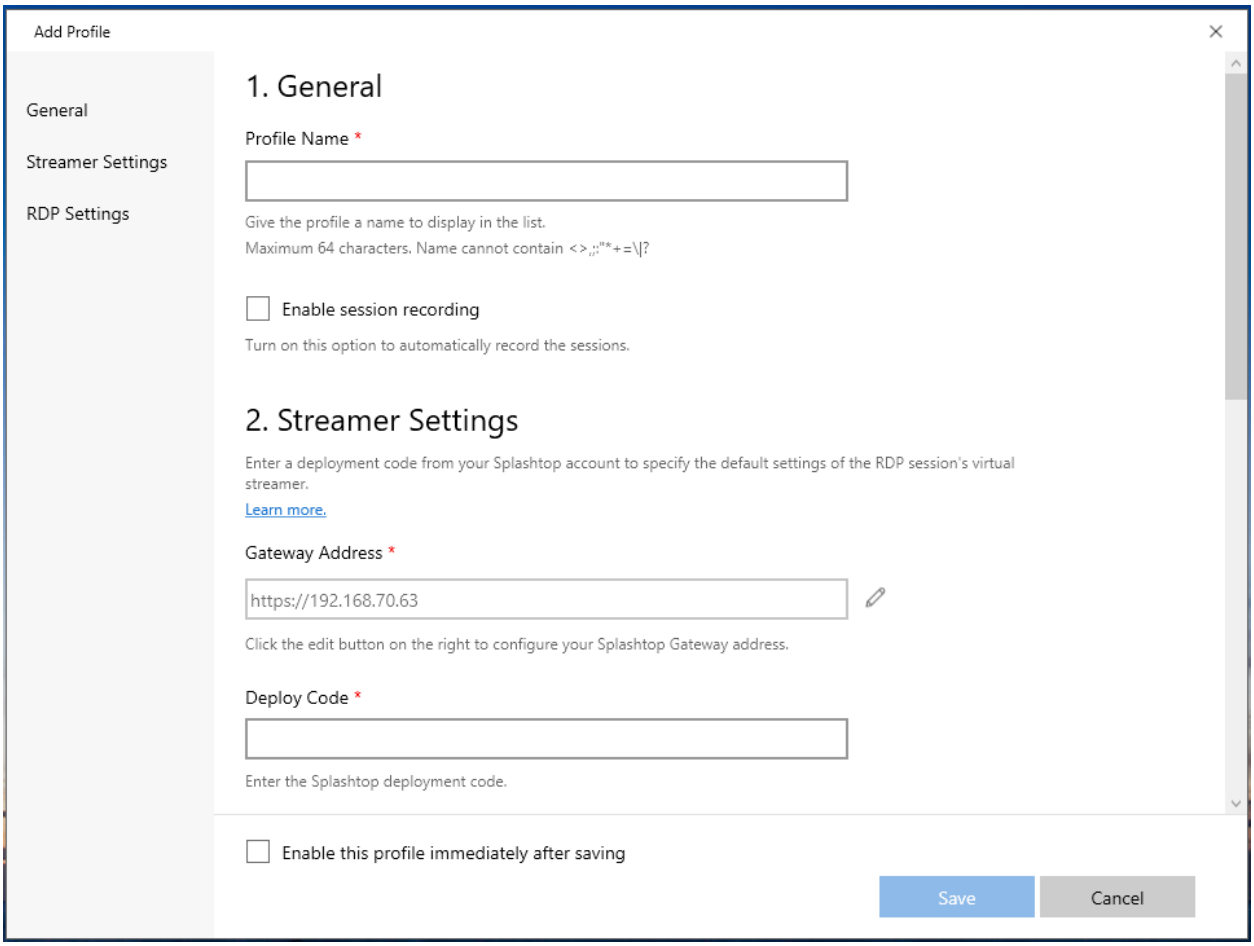


Create RDP/RDS Profile

In the Splashtop Connector, RDP resources will be available for the Splashtop On-Prem app to access by setting up Profiles. A profile setting consists of three sections: **General settings**, **Streamer settings**, and **RDP settings**.

You can create multiple Profiles in the Splashtop Connector. These RDP resources will contribute to the total computer number of your Splashtop team.

Enable the profile to make the RDP resource available for remote access.



General settings

- **Profile Name**, which will be shown in the Splashtop On-Prem client app. Give the Profile a meaningful name to let users know what the RDP machine is for.

- **Enable session recording**, turn on this option to automatically record the RDP sessions, which can be set on an individual Profile basis. The recordings are saved in the specified path on the Splashtop Connector machine.

Streamer settings

- **Gateway Address**, Splashtop Connector will be limited to **one** Gateway. User needs to configure the Gateway Address in Settings page. Only verified Gateway Address can be saved.
- **Deploy Code**, Splashtop uses deploy packages to determine the RDP resource's default computer group and access permissions. Please see this article on how to create deploy packages. Once created, enter the **Deploy Code** in this field.

RDP Settings

- **Mode**, Splashtop Connector supports both RDP for individual computers, and RDS as virtual desktops. RDS will require Windows Server and RDS licenses.
- **Pool Size**, if RDS is chosen, you can set the pool size, which means how many users can connect to RDS virtual desktops simultaneously. The pool size will contribute to the total number of computers in the Splashtop team.
- **Remote Computer**, you can pre-configure a remote computer's IP/DNS or ask the user to input this info when connecting to the machine.
    - **Ask user to specify which remote computer to connect to**, useful for ad-hoc support
    - **Fixed Remote computer with specified information**, for connecting to a specific machine
- **Login Credential**
    - **Ask user to login with Windows username and password**, user needs to input the remote computer's login credential to connect
    - **Fixed username and password**, user can connect to the remote computer with the pre-configured user name and password
- **Run in remote application mode**, if you have configured and published remote apps on your RDS server, you can let the session run in remote app mode. Turn on this option to set further settings for remote application
    - Remote App alias, or Remote App full path, depending on your choice

    - Optional remote application parameters, you need to enable remote application parameter support on RDS server.
- **Color depth**, choose the color depth.
- **Audio playback**, choose the audio playback option.
- **Keyboard layout**, choose the keyboard layout or add a new keyboard layout that is not in the pre-set list.

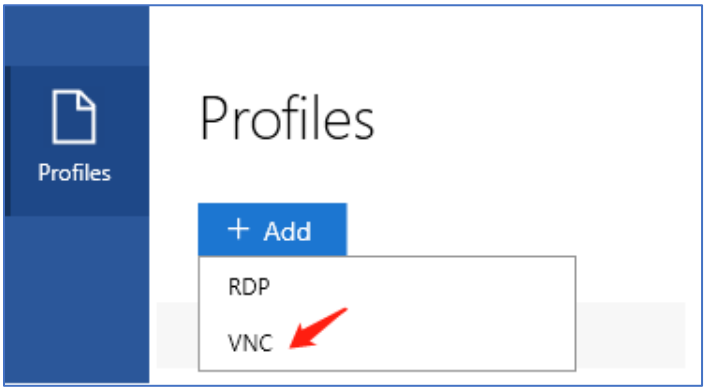
You can enable this profile immediately by turning on **Enable this profile immediately after saving**, or enable it in the main window.

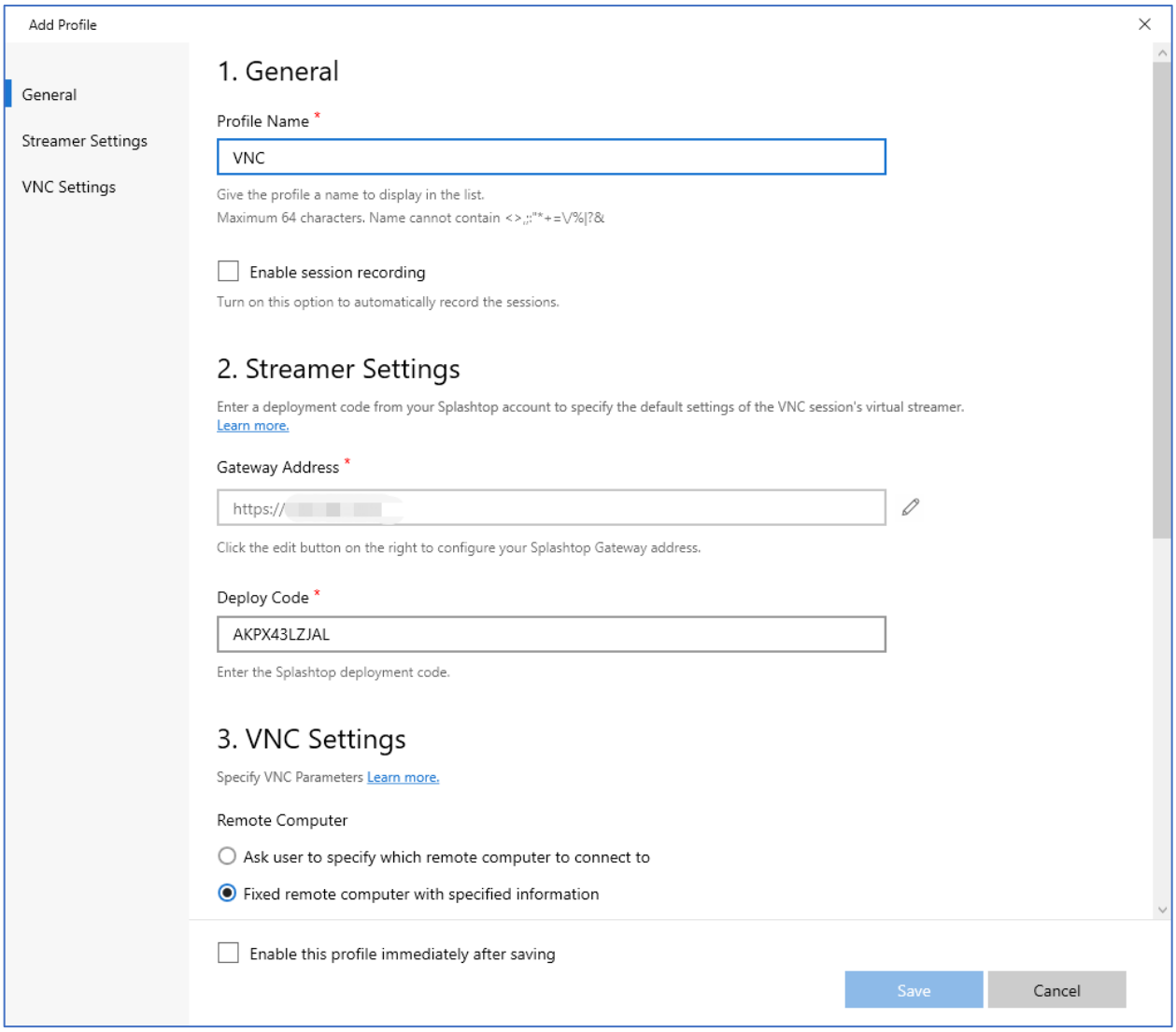
Create VNC Profile

In the Splashtop Connector, VNC resources will be available for the Splashtop On-Prem app to access by setting up Profiles. A profile setting consists of three sections: **General settings**, **Streamer settings**, and **VNC settings**.

You can create multiple Profiles in the Splashtop Connector. These VNC resources will contribute to the total number of computers on your Splashtop team.

Enable the profile to make the VNC resource available for remote access.





General settings

- **Profile Name**, which will be shown in the Splashtop On-Prem client app. Give the Profile a meaningful name to let users know what the VNC machine is for.
- **Enable session recording**, Turn this on to automatically record sessions for this resource. Recordings are saved in the specified path on the Splashtop Connector machine *(See Settings -> General)*

Streamer settings

- **Deploy code**, Enter a Splashtop deployment package code to determine the VNC resource's default computer group and access permissions. Please see this article on how to create deploy packages. Once created, enter the deployment code in this field.

VNC Settings

- **Remote Computer**, you can pre-configure a remote computer's IP/DNS or ask the user to input this info when connecting to the machine.
    - **Ask user to specify the remote computer to connect to** requires users to enter the VNC machine's IP/hostname upon connecting. This may be useful for ad-hoc support.
        - **Enable IP restriction configuration**, you can specify the whitelist/blacklist of the target VNC computers
    - **Fixed computer with specified information**, allows IT admins to preconfigure the VNC machine's specific IP/hostname and port.
- **Login Credential**
    - **Ask user to login when connect to the session**, user needs to input the remote computer's VNC password to connect
    - **Fixed password**, user can connect to the remote computer with the pre-configured VNC password

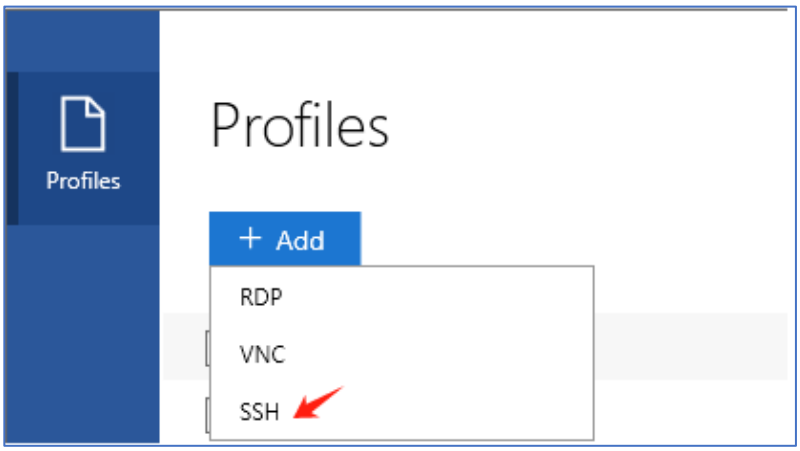
You can enable this profile immediately by turning on **Enable this profile immediately after saving**, or enable it in the main window.

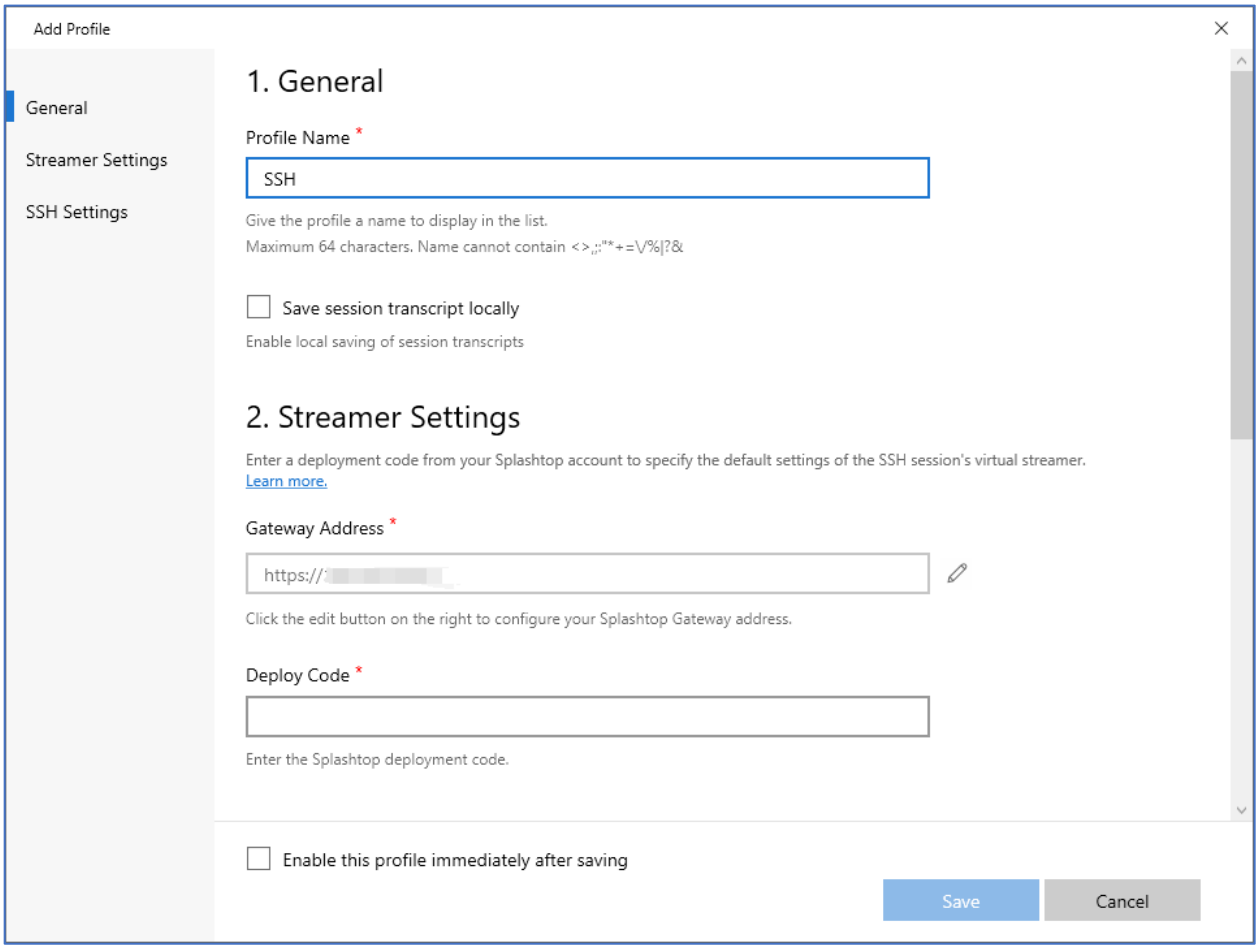
Create SSH Profile

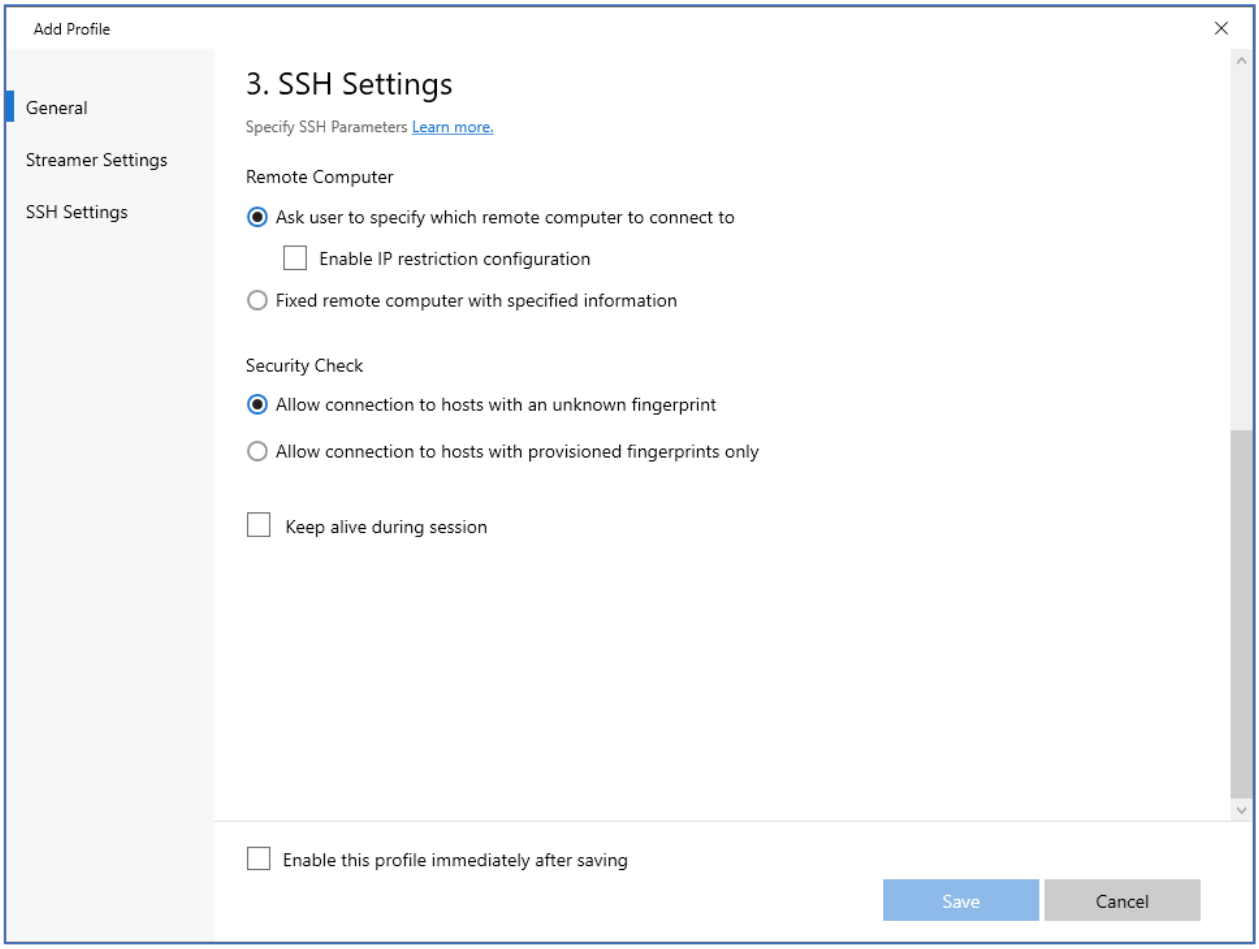
Since Splashtop Connector v1.1.8.4, SSH resources will be available for the Splashtop On-Prem app to access by setting up Profiles. A profile setting consists of three sections: **General settings**, **Streamer settings**, and **SSH settings**.

You can create multiple Profiles in the Splashtop Connector. These SSH resources will contribute to the total number of computers on your Splashtop team.

Enable the profile to make the SSH resource available for SSH access.







General Settings

- **Profile Name**, which will be shown in the Splashtop On-Prem client app. Give the Profile a meaningful name to let users know what the SSH machine is for.
- **Save session transcript locally**, Turn this on to automatically save session transcripts for this
  resource, which can be set on an individual Profile basis. The recordings are saved in the specified path on the Splashtop Connector machine.

Streamer Settings

- **Deploy code**, Enter a Splashtop deployment package code to determine the SSH resource's default computer group and access permissions. Please see this

article on how to create deploy packages. Once created, enter the deployment code in this field.

SSH Settings

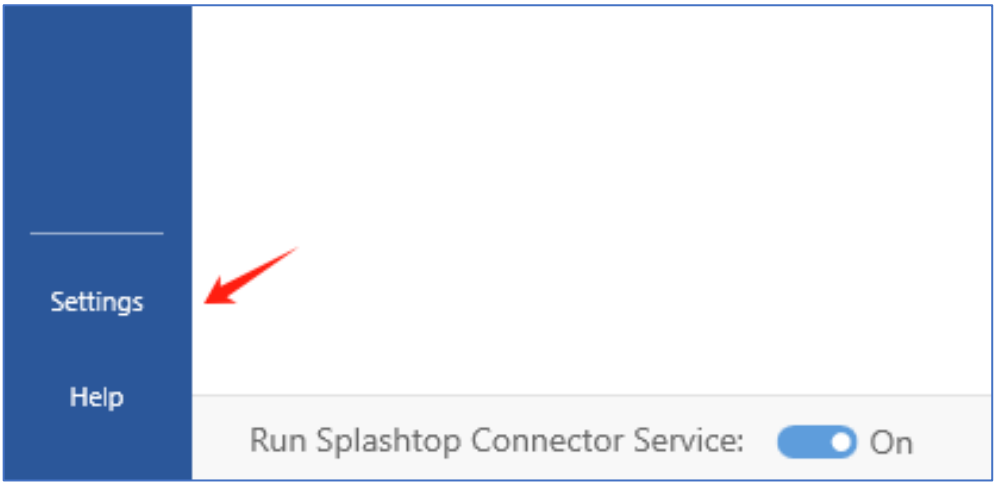
- **Remote Computer**, you can pre-configure a remote computer's IP/DNS or ask the user to input this info when connecting to the machine.
    - **Ask user to specify the remote computer to connect to** require users to enter the SSH machine's IP/hostname upon connecting. This may be useful for ad-hoc support.
        - **Enable IP restriction configuration**, you can specify the whitelist/blacklist of the target SSH computers.
    - **Fixed computer with specified information**, allow IT admins to preconfigure the SSH machine's specific IP/hostname and port.
        - **Use preset public key authentication**, Instead of password authentication, you can turn on public key authentication and select the preconfigured private key.
- **Security Check**

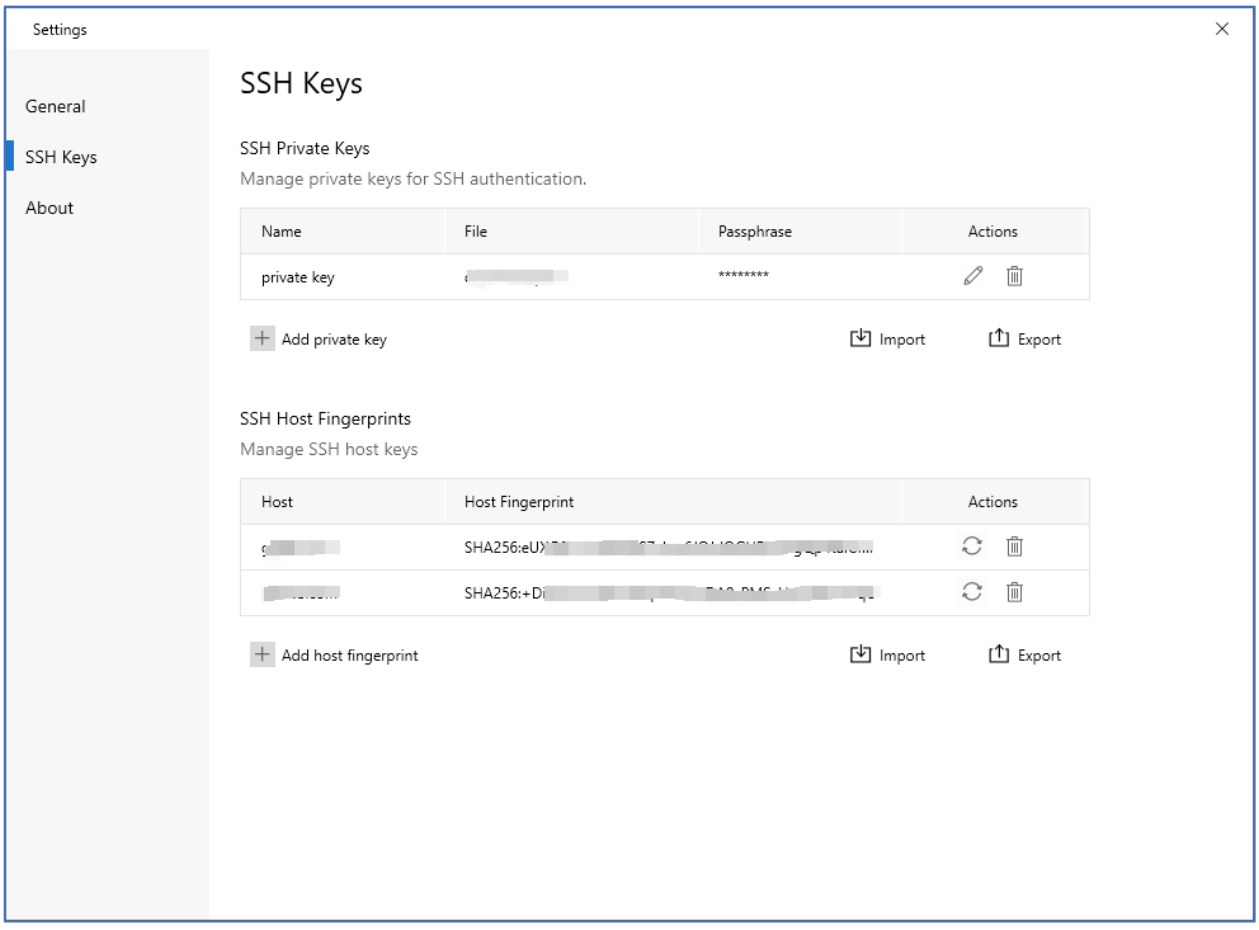
    - **Allow connection to hosts with an unknown fingerprint**, user can connect to the SSH computer with unknown SSH Host Fingerprints. When you successfully connect to the SSH server, the fingerprint will be automatically added to the SSH Host Fingerprints in SSH keys.
    - **Allow connection to hosts with a provisioned fingerprint**, user can only connect to the SSH computer with the pre-configured SSH Host Fingerprints in SSH Keys.

You can enable this profile immediately by turning on **Enable this profile immediately after saving** or enabling it in the main window.

SSH Keys

Additionally, you can go to *Settings -> SSH Keys* to manage your **private keys** and **SSH Host Fingerprints** in the Splashtop Connector.





- **SSH Private Keys**, allow IT admins to configure the private keys for SSH authentication by manually adding or importing.

- **SSH Host Fingerprints**, allow IT admins to configure the SSH host fingerprints by manually adding or importing.

You can find more helpful resources by accessing the online support portal.

Support Resources

About this document

This document is provided for information purposes 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-premises solution that can be self-hosted inside an enterprise network. With a centralized database and management console, the IT admin could conveniently tackle 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 providing the best technical support to our customers. Looking for more support resources?

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