



Splashtop On-Prem Admin Guide

Aug. 2026

Company Information	6
Introduction.....	7
Features of Splashtop On-Prem.....	7
Usage scenarios	9
Installation	10
Key components	10
Download installation package	10
System requirements.....	11
Quick installation guide	14
Access Gateway portal	32
System Configuration.....	34
Introduction.....	34
Status.....	35
Network	39
Change network port.....	39
Security	41
Import SSL certificate	41
Convert SSL certificate to PFX format.....	43
TLS settings	44
Access control	48
Software.....	49
Software updates	51
Import new version of software components.....	57
Remove software components	62
Maintenance	64
Backup.....	64
Backup schedule	67
Restore	71
Remove Splashtop On-Prem logs.....	74
Notification	75
Splashtop On-Prem License	77
Understand your license and privileges	77
Activate license	81

About.....	83
Management Console.....	85
Introduction.....	85
Users.....	86
Create user accounts.....	86
Bulk import user accounts.....	91
Set access permission.....	96
Updating access permissions via CSV.....	100
Granular feature control.....	105
Set admin rights.....	109
Enable SOS for AD group members from user list.....	112
Export user list or access permission list.....	113
Super Admin.....	115
Grant/Revoke System Management.....	117
Computers.....	121
Manage a specific computer.....	122
Reboot computer.....	123
Delete computer.....	123
Rename computer.....	124
Assign computer group.....	124
Add note.....	124
See user list.....	125
See properties.....	125
Export and save a copy/record of the computer list.....	126
Computer Inventory.....	128
Devices.....	131
Export the device list.....	132
Grouping.....	134
Manage grouping.....	134
Connection pool.....	135
Group user limits.....	137
Scheduled access.....	139
Service Desk.....	147
Service Desk - Channel.....	147

Service Desk - Console and general usage.....	151
Service Desk - SOS Call	161
Service Desk - Transcripts.....	170
Deployment	172
Endpoints Management.....	190
System Reboot.....	195
Remote Command (Windows).....	196
Batch/Executable File (Windows)	198
Remote install MSI (Windows).....	200
Remote Install APK (Android).....	202
File Dispatch (Windows).....	204
File Dispatch (Android)	206
Shell Script (Mac)	209
Script/Executable File (Mac)	212
File Dispatch (Mac)	214
OS Patch (Computer View)	217
OS Patch (Patch View).....	225
Endpoint Policy.....	230
Single Sign-On (SSO)	239
How to apply for a new SSO method? (SAML 2.0)	239
Create SSO user.....	241
Bulk import SSO users.....	244
How to associate SSO method to existing team admin/member?.....	248
How can I log in using an SSO account?.....	250
How to generate the SCIM provisioning token?.....	255
Settings	256
Team Settings	256
Remove offline computers policy.....	272
How to set web access?	273
Setup two-step verification	276
Set up Two-Step Verification with Email.....	286
Local session recording on Gateway web console	292
Centralized session recording.....	294
Integrate Splashtop On-Prem with Freshservice	300

Device/Browser authentication	301
Splashtop On-Prem password policy	305
Account lockout policy	306
Getting notified when a computer goes online or offline	308
Session Transcript.....	311
Authentication	314
How to apply for a new SSO method? (SAML 2.0)	314
Active Directory.....	316
Email settings (SMTP server integration).....	319
Introduction.....	319
How to use Open API.....	322
Syslog	326
Splashtop Connector	328
Installation	330
Create RDP/RDS profile	331
Create VNC profile	334
Create SSH profile.....	336
How to create HTTP/S profiles?	341
How to create Port Forwarding profiles?	344
Support Resources	348

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.
10050 North Wolfe Road Suite SW2-S260,
Cupertino, CA 95014, 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)

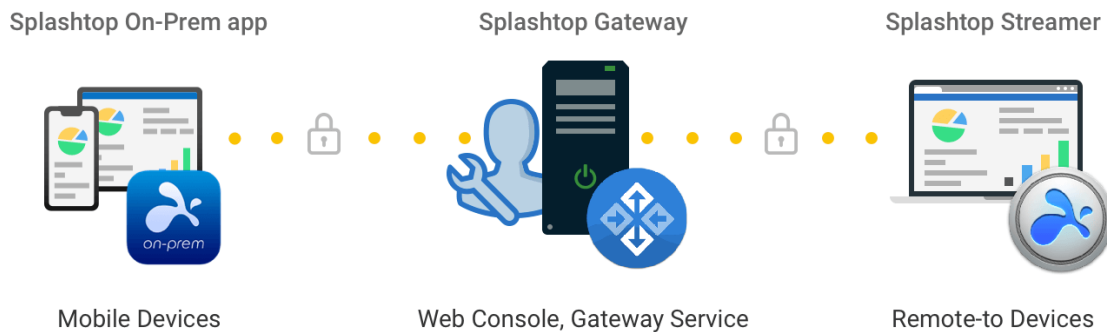
ATTENDED SUPPORT is a perfect solution for Service Desks and MSPs, and it provides the most convenient way for a technician to establish an ad-hoc remote session, without needing the end user to install any software or plug-in in the computer. Instead, the end user just downloads and launches a standalone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

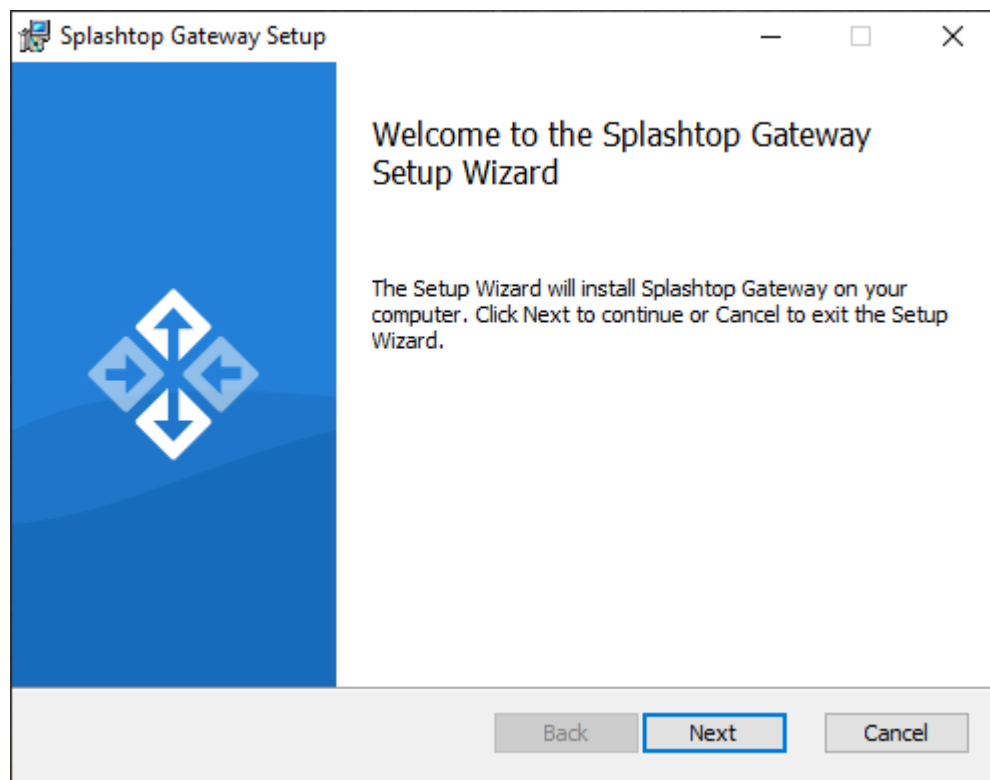
1. Team Owner sets up Splashtop Gateway on the company network.

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.

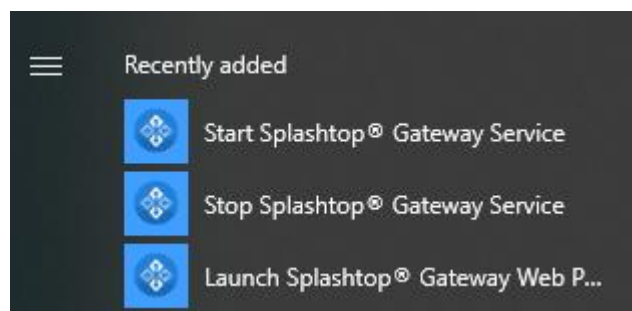
Splashtop Gateway and Splashtop Steamer can be installed on the same Windows server. In fact, it is a good practice since remote access to that server can be provided in case Team Owner needs to configure Splashtop Gateway settings or restart the Splashtop Gateway service.

1. Install Splashtop Gateway

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



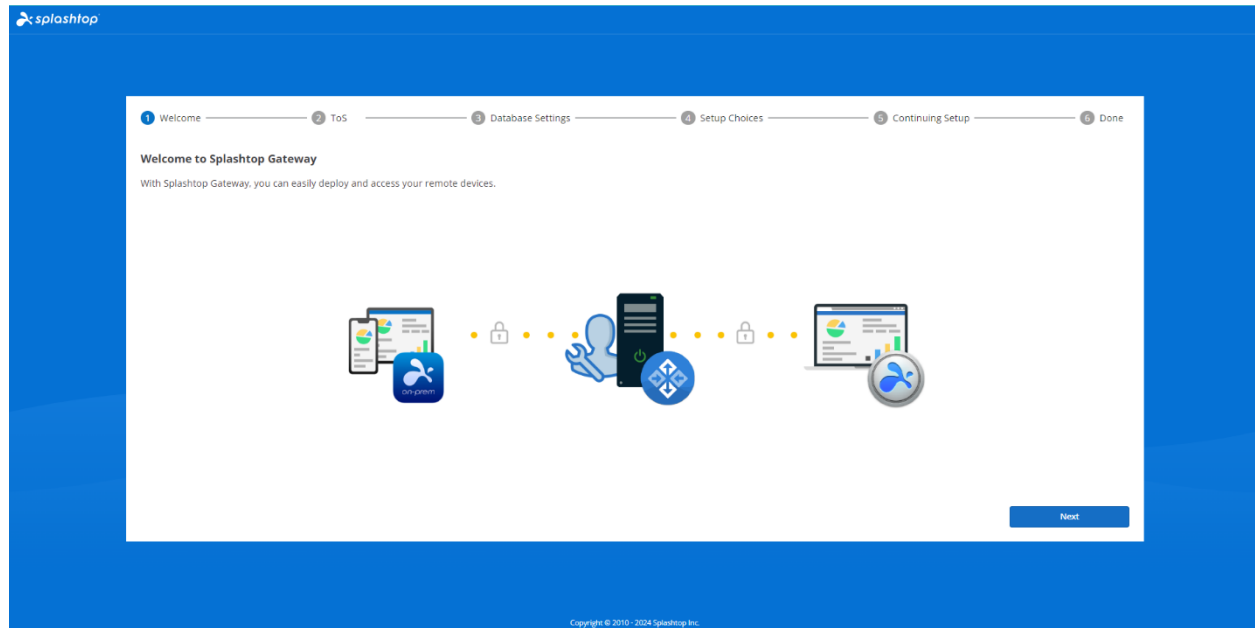
b) After the installation finished, go to Windows Startup menu in which 3 startup shortcuts just created. Click Launch Splashtop Gateway web portal to start gateway web console in your default browser.



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

2. Splashtop Gateway OOB Setup

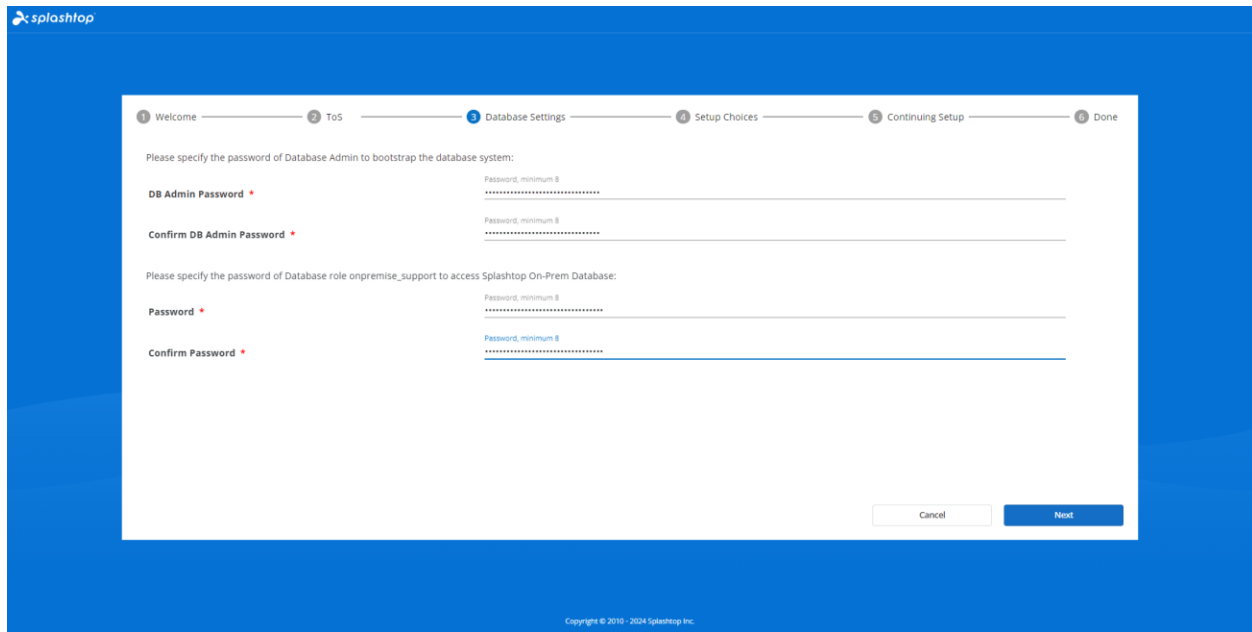
a) Once launched the web console from browser for the first time, an OOB setup procedure containing Terms of Service will show up. Click next to continue.



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

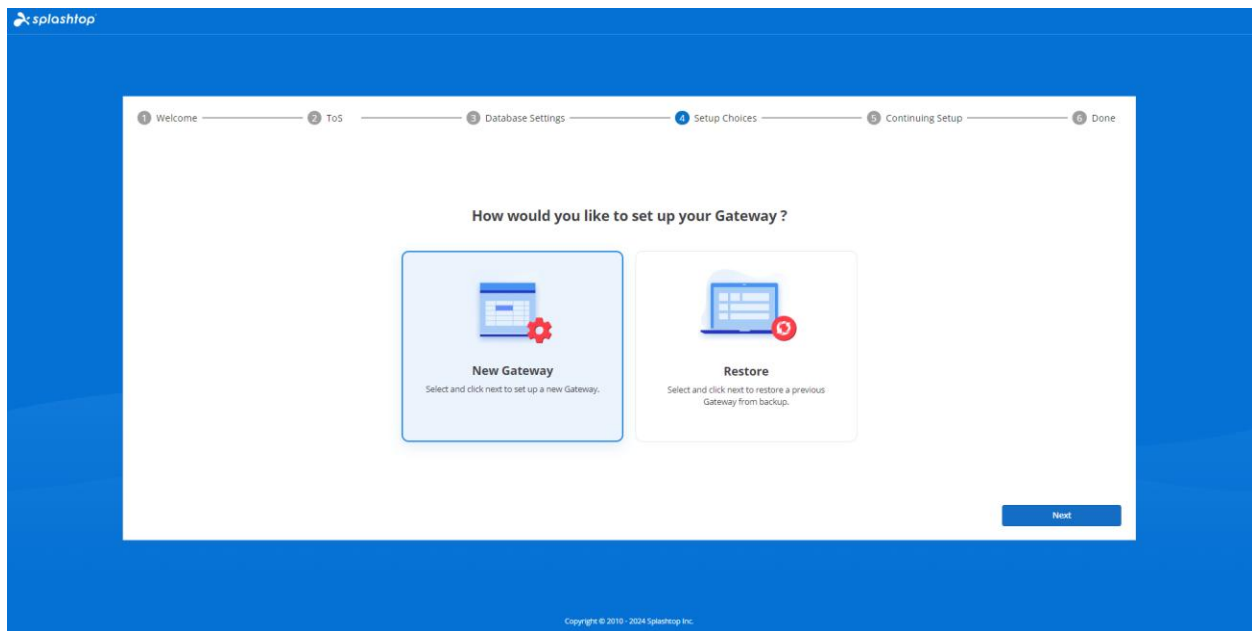


Note: Please write down your Database passwords and saved in a secured place since there will be no way to change DB passwords later on.



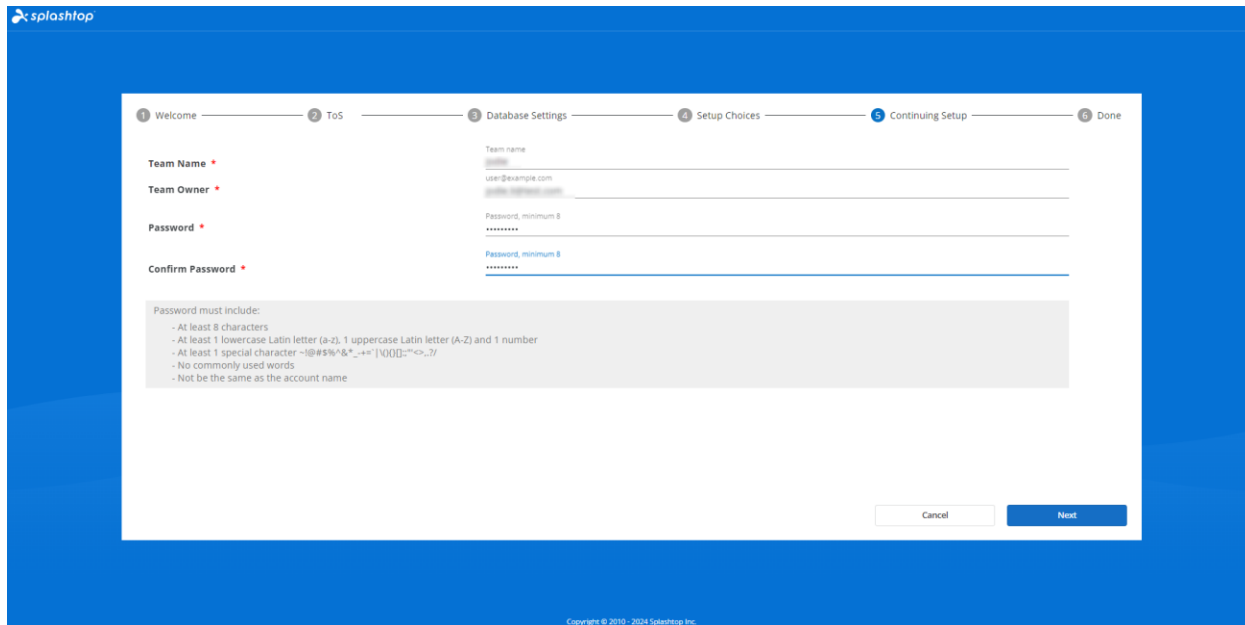
The screenshot shows the 'Database Settings' step of the Splashtop On-Prem Admin Setup Wizard. The progress bar at the top indicates the following steps: 1 Welcome, 2 ToS, 3 Database Settings (current), 4 Setup Choices, 5 Continuing Setup, and 6 Done. The main content area contains two password prompts. The first prompt asks for the 'DB Admin Password' to bootstrap the database system, with fields for 'DB Admin Password' and 'Confirm DB Admin Password'. The second prompt asks for the password of the Database role 'onpremise_support' to access the Splashtop On-Prem Database, with fields for 'Password' and 'Confirm Password'. Each password field has a 'Password, minimum 8' label and a masked input field. At the bottom right, there are 'Cancel' and 'Next' buttons. The footer contains the copyright notice: 'Copyright © 2010 - 2024 Splashtop Inc.'

c) Chose your Gateway setup preference.



The screenshot shows the 'Setup Choices' step of the Splashtop On-Prem Admin Setup Wizard. The progress bar at the top indicates the following steps: 1 Welcome, 2 ToS, 3 Database Settings, 4 Setup Choices (current), 5 Continuing Setup, and 6 Done. The main content area is titled 'How would you like to set up your Gateway ?' and contains two options: 'New Gateway' and 'Restore'. The 'New Gateway' option is highlighted with a blue border and a gear icon, with the text 'Select and click next to set up a new Gateway.' below it. The 'Restore' option is highlighted with a red border and a restore icon, with the text 'Select and click next to restore a previous Gateway from backup.' below it. At the bottom right, there is a 'Next' button. The footer contains the copyright notice: 'Copyright © 2010 - 2024 Splashtop Inc.'

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



1 Welcome 2 ToS 3 Database Settings 4 Setup Choices 5 Continuing Setup 6 Done

Team Name *

Team Owner *

Password *

Confirm Password *

Team name
user@example.com
password@domain.com

Password, minimum 8
Password, minimum 8

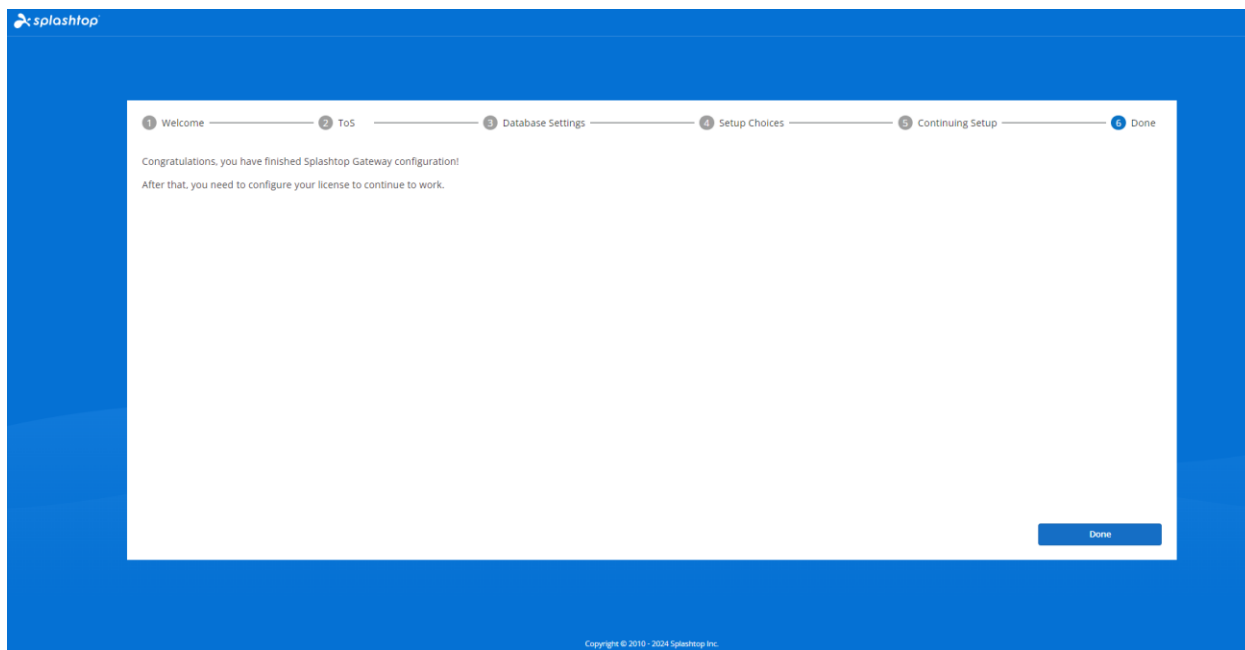
Password must include:

- At least 8 characters
- At least 1 lowercase Latin letter (a-z), 1 uppercase Latin letter (A-Z) and 1 number
- At least 1 special character ~!@#\$%^&*~+~"{}[];:'<>.,/?
- No commonly used words
- Not be the same as the account name

Cancel Next

Copyright © 2010 - 2024 Splashtop Inc.

e) Once OOB 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.



1 Welcome 2 ToS 3 Database Settings 4 Setup Choices 5 Continuing Setup 6 Done

Congratulations, you have finished Splashtop Gateway configuration!

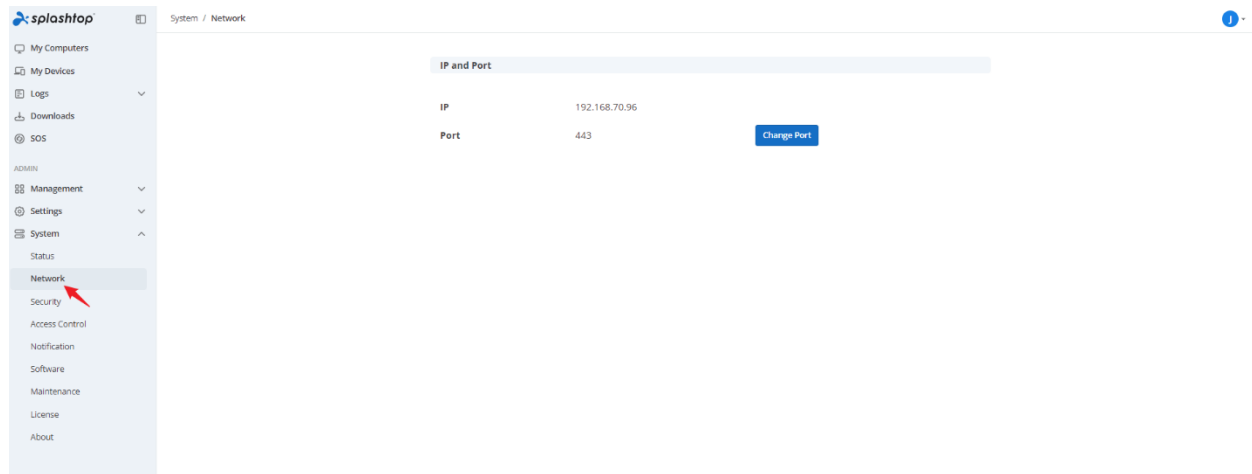
After that, you need to configure your license to continue to work.

Done

Copyright © 2010 - 2024 Splashtop Inc.

f) 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.

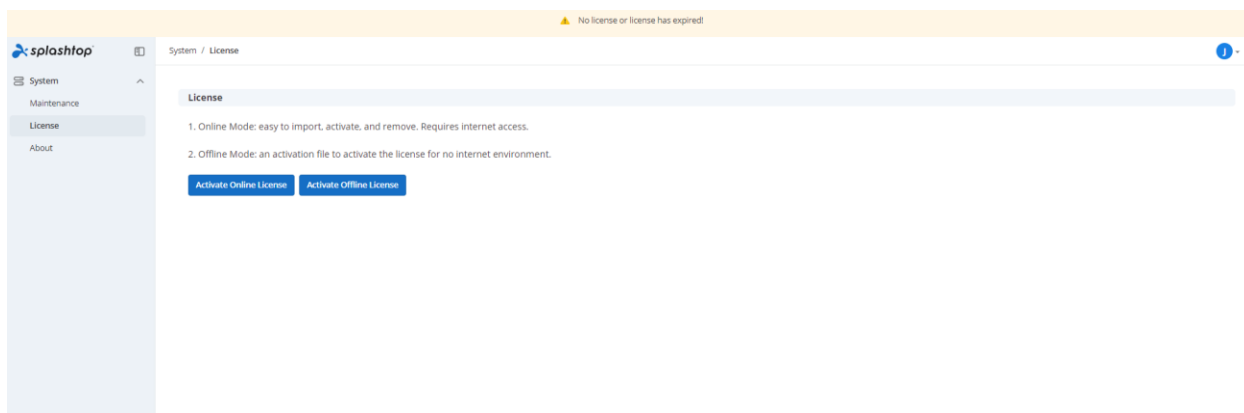


Note: Please reach out to Splashtop Sales or Splashtop Support to request for trial license or obtain purchased license.

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)



System / License

Import Offline License Activation File

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

1. Press the save button to save the Activation ID to a file

Save

2. Send the saved file to Splashtop Support to get your offline activation file

3. Import the offline activation file to activate the offline license

Activation File

Open

Import

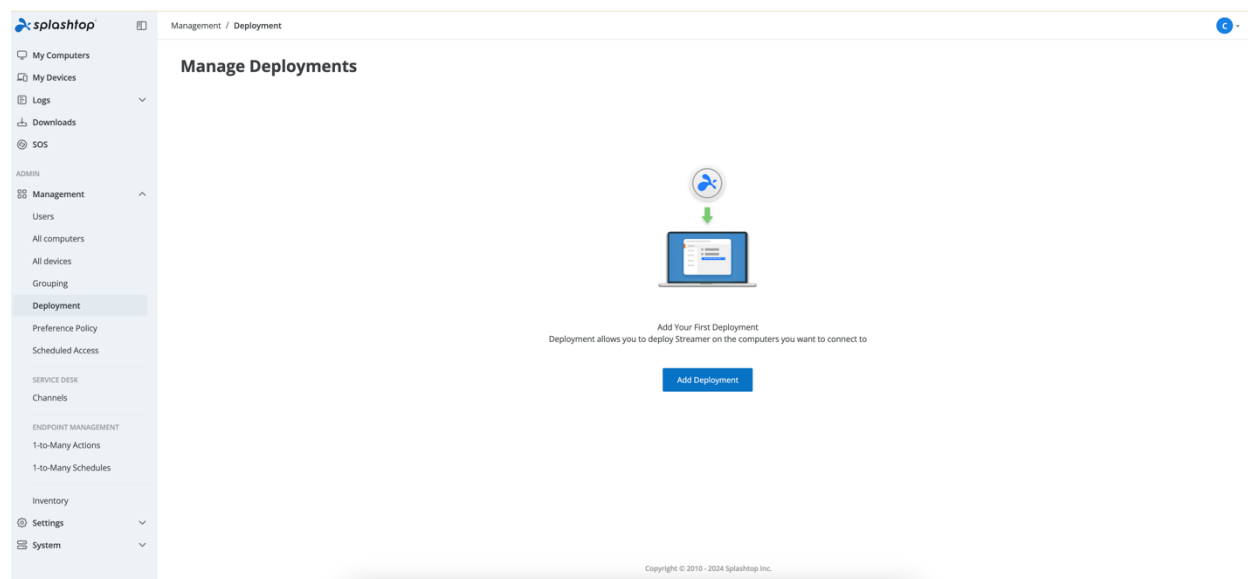
Back

4. Deploy Splashtop Streamer

Below instruction taking deploy Splashtop Streamer on Windows as an example.

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.



splashtop Management / Deployment / Add Deployment Package

Add Deployment Package

Package Name

Policy Name

Select a preference policy

[Create preference policy](#)

Computer Naming Rule
(Computers deployed using Splashtop Connector will always follow the Profile Name defined in the Connector settings.)

☒ Use current OS hostname
☐ Keep in sync with OS hostname ⓘ
☐ Use custom name + sequence number
 e.g. Acme Bakery (005)
☐ Use custom name + current OS hostname
 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 hostname.

Grouping

Group Choice

[Create or manage groups](#)

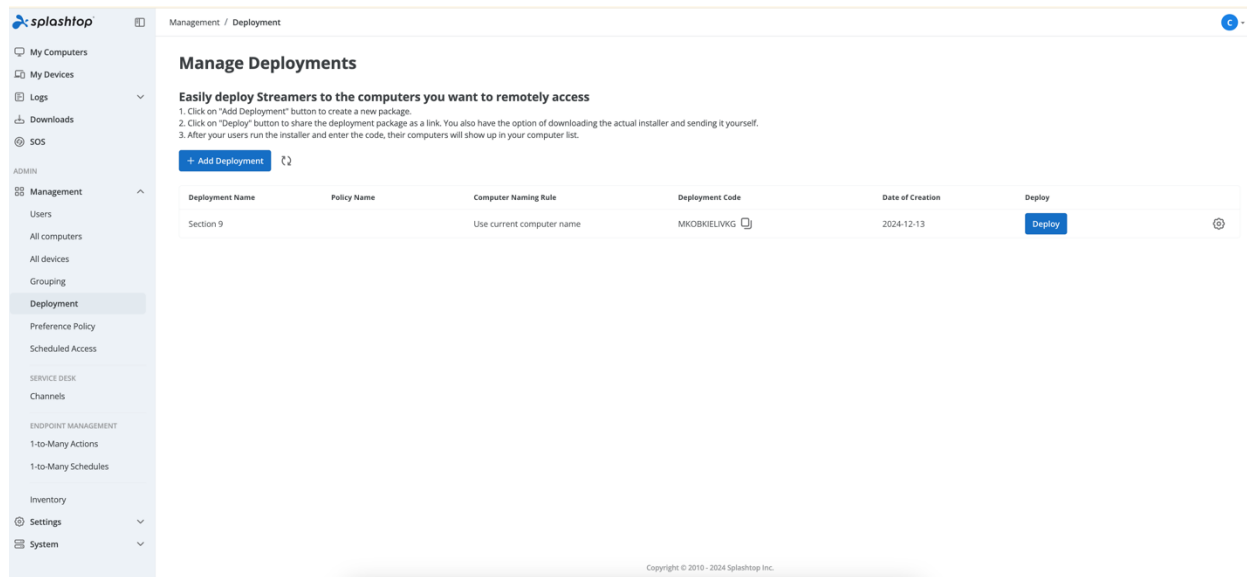
☒ **Auto-launch Streamer**
Automatically launch Splashtop Streamer every time the computer starts. (Not applicable to computers deployed using Splashtop Connector.)

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

General Settings

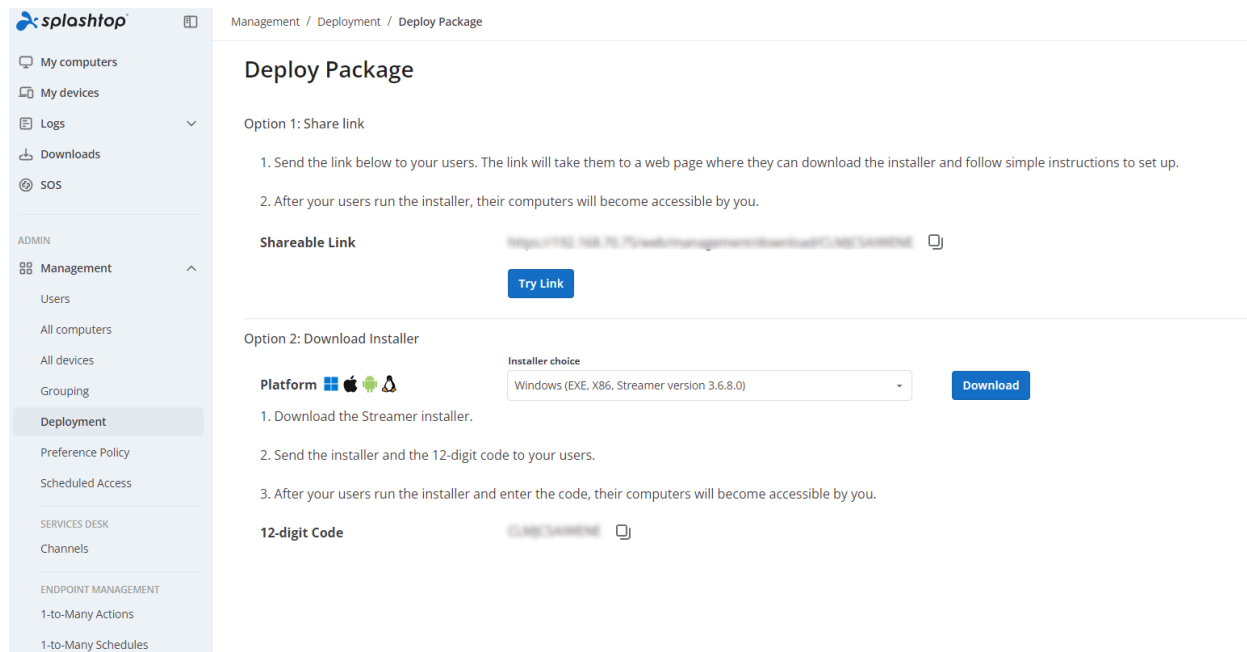
☐ **Hide Streamer tray icon**
Hide Streamer icon on Windows system tray or Mac menu bar. Check this option to reduce the chance of users tampering with the Streamer. (Not applicable to computers deployed using Splashtop Connector.)

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



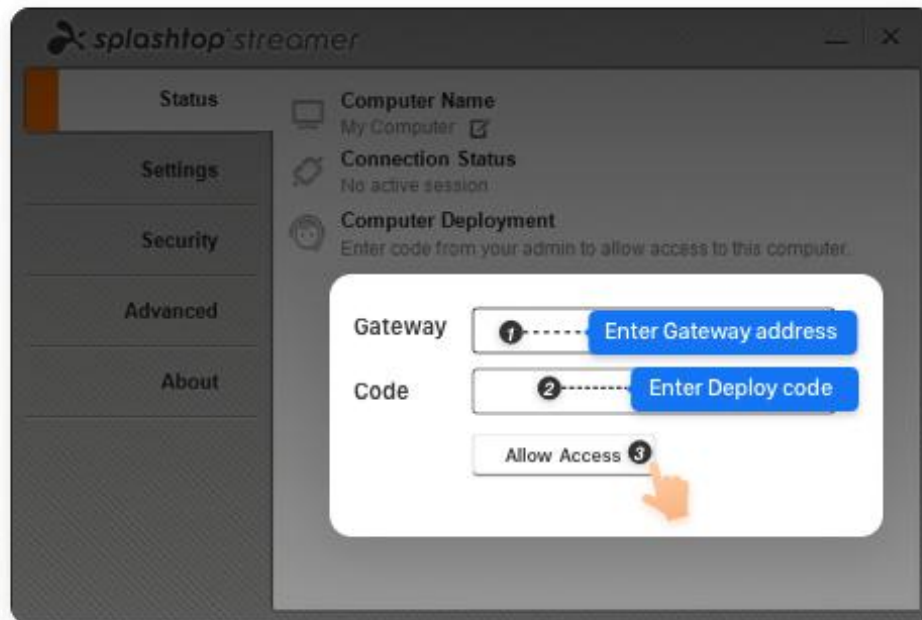
The screenshot shows the 'Manage Deployments' page in the Splashtop On-Prem Admin interface. The left sidebar contains navigation options: My Computers, My Devices, Logs, Downloads, SOS, ADMIN (Management, Users, All computers, All devices, Grouping, Deployment, Preference Policy, Scheduled Access), SERVICE DESK (Channels), ENDPOINT MANAGEMENT (1-to-Many Actions, 1-to-Many Schedules), Inventory, Settings, and System. The main content area is titled 'Manage Deployments' and includes instructions on how to deploy streamers. Below the instructions is a table with columns: Deployment Name, Policy Name, Computer Naming Rule, Deployment Code, Date of Creation, and Deploy. The table contains one entry for 'Section 9' with a deployment code 'MK0BKIELVWG' and a date of creation '2024-12-13'. A 'Deploy' button is visible next to the entry.

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.).



The screenshot shows the 'Deploy Package' page in the Splashtop On-Prem Admin interface. The left sidebar is identical to the previous screenshot. The main content area is titled 'Deploy Package' and includes instructions on how to deploy the package. Below the instructions are two options: 'Option 1: Share link' and 'Option 2: Download Installer'. Under 'Option 1: Share link', there is a 'Shareable Link' field with a copy icon and a 'Try Link' button. Under 'Option 2: Download Installer', there is a 'Platform' dropdown menu (Windows, macOS, Linux, Android, iOS) and an 'Installer choice' dropdown menu (Windows (EXE, X86, Streamer version 3.6.8.0)). A 'Download' button is visible next to the installer choice. Below the installer choice, there are instructions on how to download the installer and send it to users. At the bottom, there is a '12-digit Code' field with a copy icon.

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

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 button** to create a new user.

Users

Add
Bulk Actions
☐ Only show selected

Filters
Menu
Share
Search

Web Access
User SOS Status
More Filters

Role ↑	Source	Display Name	Group	Last Login	
Owner	Local		Default Group	2024-08-20 16:04:34	
Admin	AD Group Member (Member of...		Alpha Corp. Default Gr...	2024-07-15 11:09:25	
Admin	Local		Gamma Industries		
Admin	Local		Alpha Corp	2024-08-20 16:06:14	

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

Add User

* Account

* Password

* Confirm Password

☐ Request to change password when next login

Password must include:

- At least 8 characters
- At least 1 lowercase Latin letter (a-z), 1 uppercase Latin letter (A-Z) and 1 number
- At least 1 special character ~!@#%&*_{+~}|~\0{}[]:"'<>.,/?
- No match of the account name

Group

Role

Status

☒ Enable user

☒ Enable web access

SOS Technician

☐ Enable SOS/On-Demand support

Field	Meaning
Account	This is the user's login account, it's unique in the system.
Password	Complex password rule.
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.
Enable User and web access	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. Disable web access for specific account to restrict his/her web console access, the remote access (remote session) will not be affected.
Group	User can be grouped into different groups, grouping is efficient in users management / access permissions.
Role	There are two types of roles in the system:
SOS Technician*	If SOS service is included in your subscription, you can enable SOS capability when create a user to have on-demand support available.

3. 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.

- 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:** Chose Admin or Member to assign different access permission tailored to needs.
- ***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 AD User/Group

Type

AD User

AD Server

CBK (dc=belle, dc=epoque)

* Account

User account to login

Verify

Group

Default Group

Role

Member

Status

☒ Enable User

☒ Enable web access

SOS Technician

☐ Enable SOS/On-Demand support

Cancel

Add

@belle.epoque

@belle.epoque

@example.com

@test.com

@k.com

@m1.com

@outlook.com

4. Add AD group members

AD accounts can be determined by "Source" column from the user list. 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.

Users

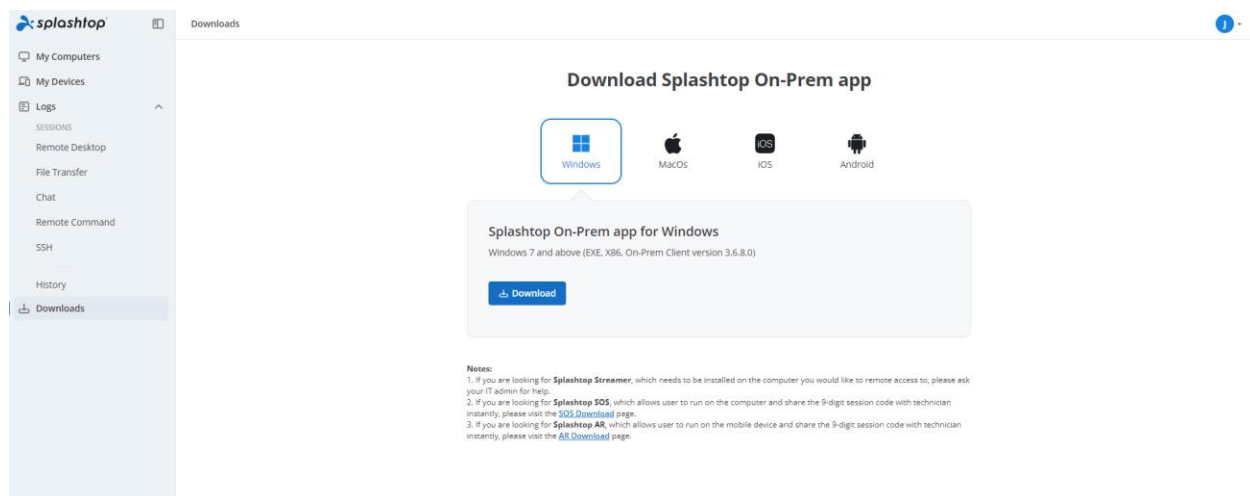
[Add](#)
[Bulk Actions](#)
☐ Only show selected

[Group](#)
[Role](#)
[Status](#)
[Web Access](#)
[User SOS Status](#)
[More Filters](#)

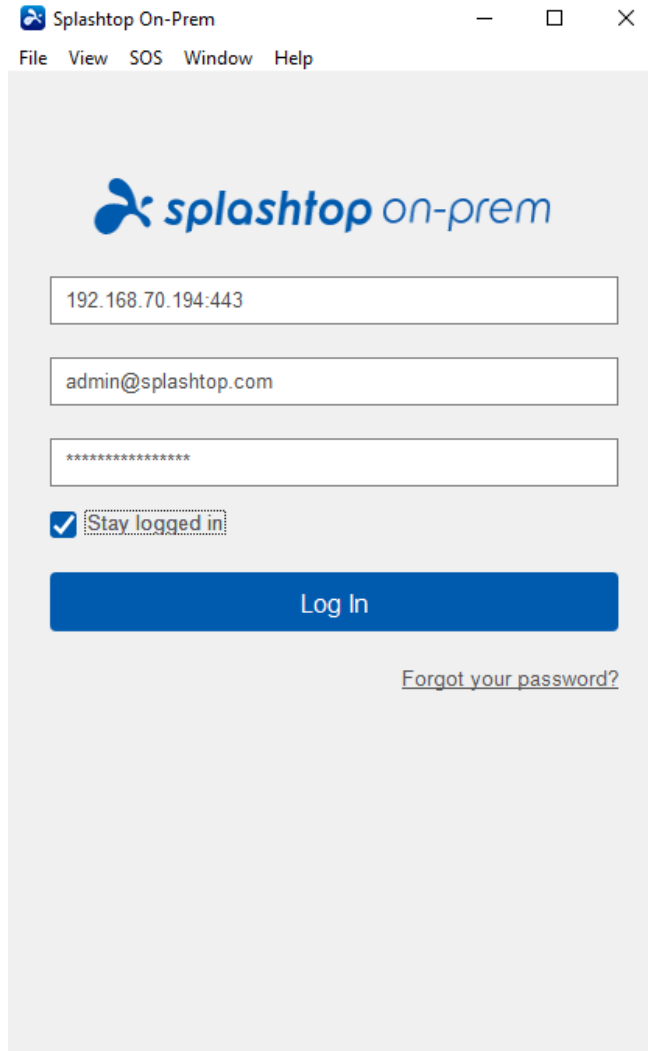
☐	Account	Role	Group	AD Group Member (Member of Remote Support / CBK)	Name	
☐	jack.doe@test.com	Member	Default Group	AD Group Member (Memb...		
☐	diane.xiong@k.com	Member	Default Group	AD Group Member (Memb...		

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.



Splashtop On-Prem

File View SOS Window Help



192.168.70.194:443

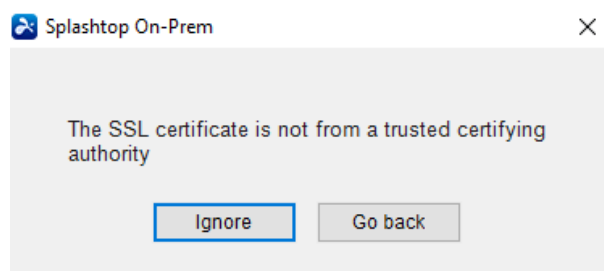
admin@splashtop.com

☒ Stay logged in

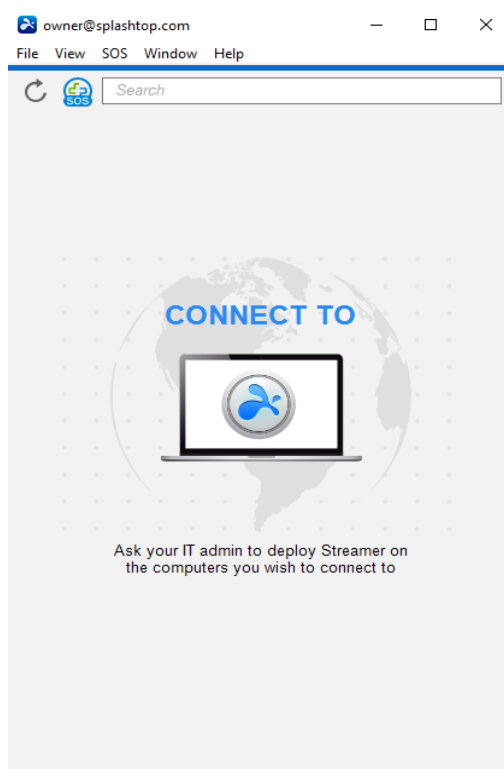
Log In

[Forgot your password?](#)

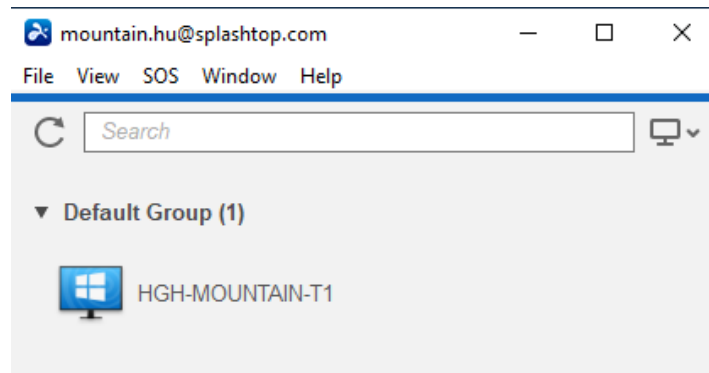
3. If a warning message pops up when you tap **Log In**, stating the SSL certificate is not from a trusted certifying authority, it is likely that the SSL certificate is self-generated, and you can choose to ignore it. However, we recommend that users who have encountered this message popping up should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

 Computers Devices Logs Management SOS Downloads System				
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://\(IP address or FQDN\):\(Port number\)](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

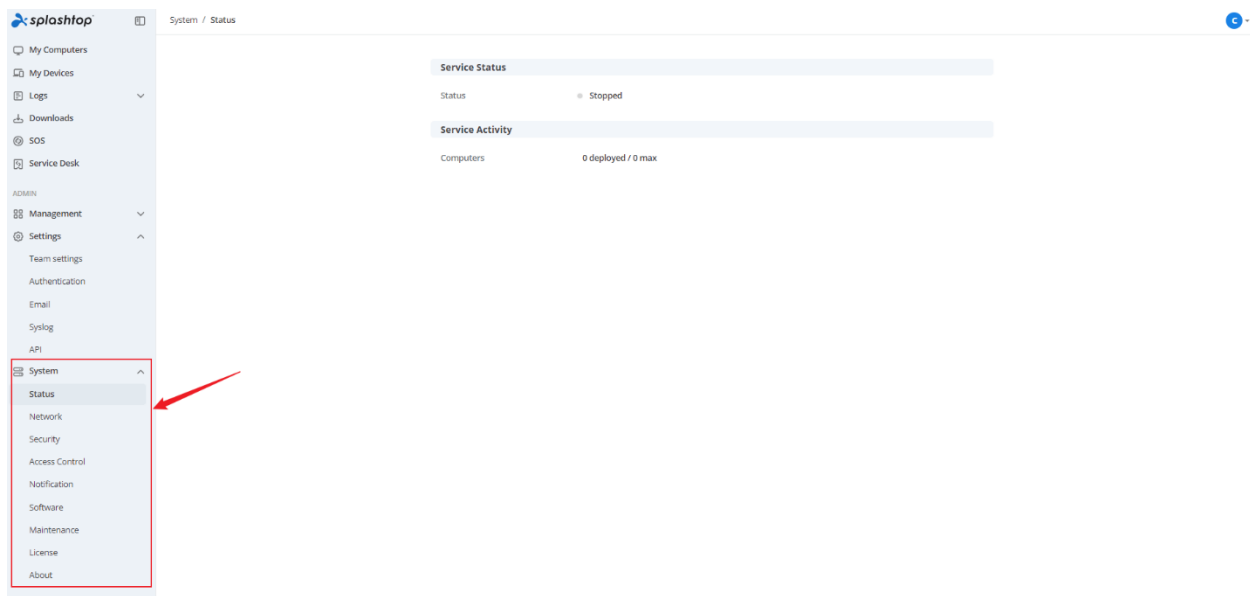
By default, Splashtop On-Prem makes use of Port number 443, but you can change the port number following instructions in the article below:

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

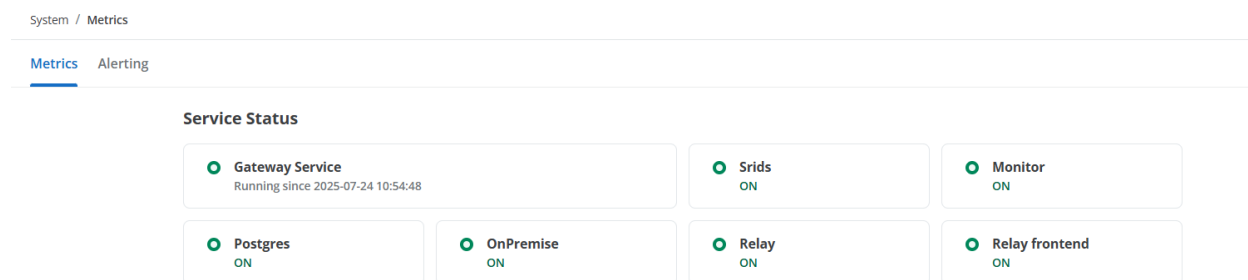
- **Software** allows Team Owner to configure [software components](#), such as enable/disable particular version of Splashtop Streamer and Splashtop On-Prem, uploading new version of components
- **Maintenance** allows Team Owner to do [system maintenance](#), such as backup and restore
- **License**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

Status

Metrics – Visibility into System Performance

Service Status

Monitor whether critical Gateway-related services are running as expected.



The following is a brief description of each service in the Splashtop On-Prem Gateway.

- **Gateway Service:** The main Windows service that hosts and manages all core Splashtop On-Prem components.
- **Postgre:** Provides the core database storing configuration and runtime data for all services.
- **OnPremise:** The API service that handles business logic, authentication requests, and communicates with the database.
- **Relay:** Handles secure data transmission during remote sessions.
- **Relay frontend:** Acts as the entry point for relay connections and dispatches traffic to backend relay instances.
- **Srlds:** Manages the unique identifiers for remote sessions, tracks session lifecycle and metadata, and facilitates session routing and auditing within the system.
- **Monitor:** Observes the health and performance of system components, collecting metrics such as CPU usage, memory consumption, disk space, and service status, and generates

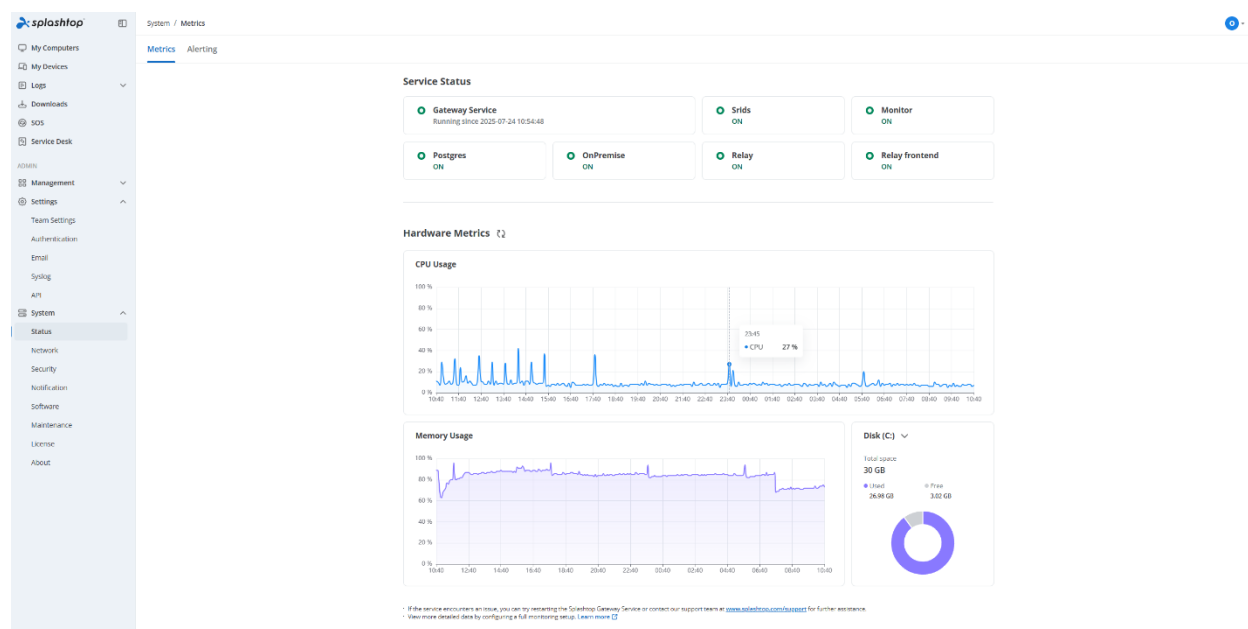
alerts for anomalies to ensure system reliability and timely issue resolution. Please complete the alerting configuration to activate this service.

Hardware Metrics

The Hardware Metrics section provides a visual overview of your system's current health status. It includes:

- **CPU Usage:** Track real-time CPU utilization across your system.
- **Memory Usage:** View memory consumption to detect potential bottlenecks.
- **Disk Space:** Monitor available disk space and usage trends.

All of these metrics are displayed using intuitive graphs and charts, giving you at-a-glance visibility into system performance over time.



Alerting – Stay Notified Before Issues Escalate

The Alerting feature helps you set up automatic notifications so you're always informed about critical system events.

SMTP Settings

Configure your SMTP server to enable email-based alert notifications.

SMTP Settings

The SMTP Settings will be used for sending alert notifications.

[Edit SMTP Settings](#)

☒ Sync Gateway SMTP Settings

* SMTP Server Enter an SMTP server address	* Port 1-65535	* Encryption Please select
* Sender Email Address All alerts will be sent from this address	* Recipient Enter a recipient email address	
☒ Enable SMTP Authentication		
* Username Enter a username	* Password Enter a password	

- **SMTP Server:** Enter the address of the SMTP server used to send emails.
- **Port:** Specify the port number used by the SMTP server (typically 25, 465, or 587).
- **Encryption:** Choose the encryption method for securing email transmission.
- **Sender Email Address:** The email address that will appear as the sender of alert messages.
- **Recipient:** The email address where alert notifications will be delivered.
- **Enable SMTP Authentication:** Check this box if the SMTP server requires login credentials to send emails.
 - **Username:** Enter a username for SMTP authentication.
 - **Password:** Enter a password for SMTP authentication.
- **Sync Gateway SMTP Settings:** Click to automatically import SMTP settings from the web/Management/Email in your Gateway.

Alert Settings

Define the specific conditions under which alerts should be triggered. You can configure alerts for:

- Service Status changes (e.g., a service stops unexpectedly)
- High CPU Usage
- High Memory Usage
- Low Disk Space

Alerts are sent instantly based on your configurations, helping you respond quickly and minimize downtime.

Alert settings

An alert will be triggered when the metric meets the configured threshold for the evaluation period.

[Edit Alert Settings](#)

Status	Metrics	Threshold	Evaluation Period ⓘ	Repeat Interval ⓘ
☒	Service	Stopped	0 h 5 m 0 s	1 h 0 m 0 s
☒	CPU	> 80 %	0 h 5 m 0 s	
☒	Memory	> 90 %	0 h 5 m 0 s	
☒	Disk: (C:)	< 10 GB	0 h 5 m 0 s	

Save

Cancel

- **Status:** Check this box if you want to enable specific alerts.
- **Metrics:** The specific monitoring items, such as CPU usage, memory usage, or disk space.
- **Threshold:** The specific value at which a metric triggers an alert (e.g., CPU usage > 90%).
- **Evaluation Period:** The time window over which the metric is evaluated to determine if it meets or exceeds the threshold.
- **Repeat Interval:** The minimum time between repeated alert notifications for the same condition.

System / Status

Service Status

Status ● Running since 2024-12-03 09:44:53

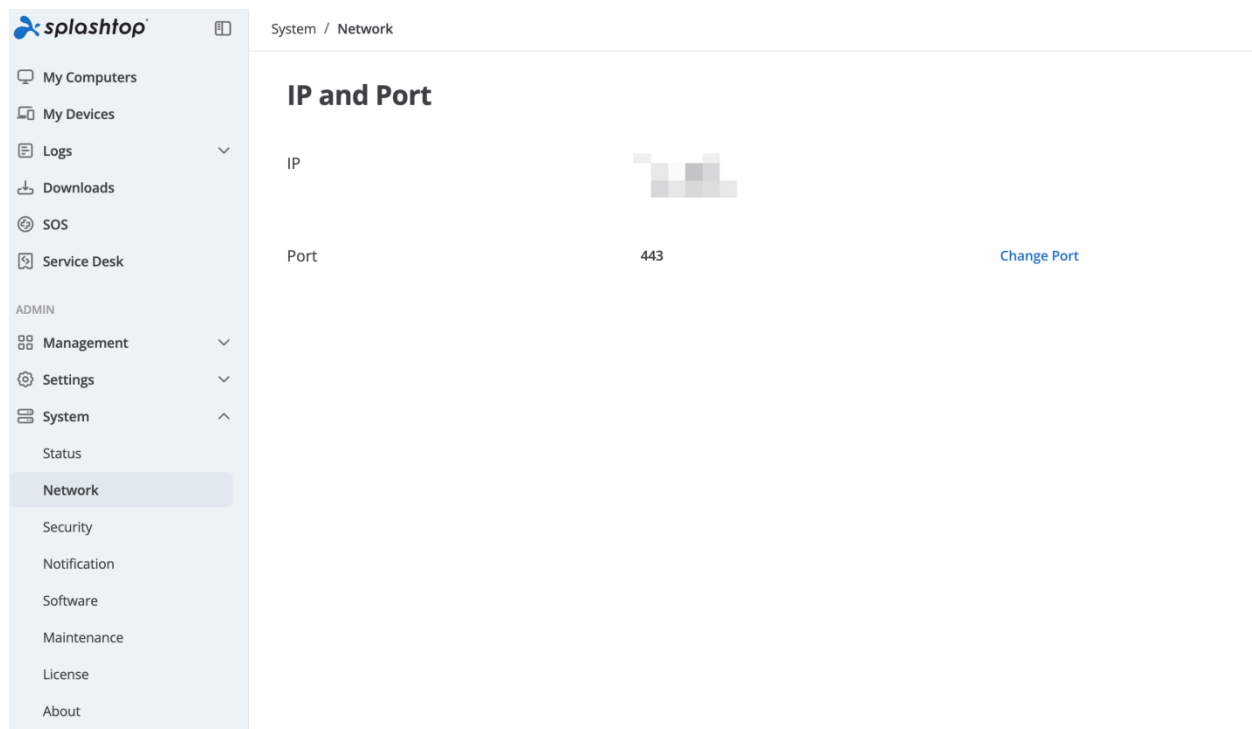
Service Activity

Computers 1 deployed / 60000 max

Network

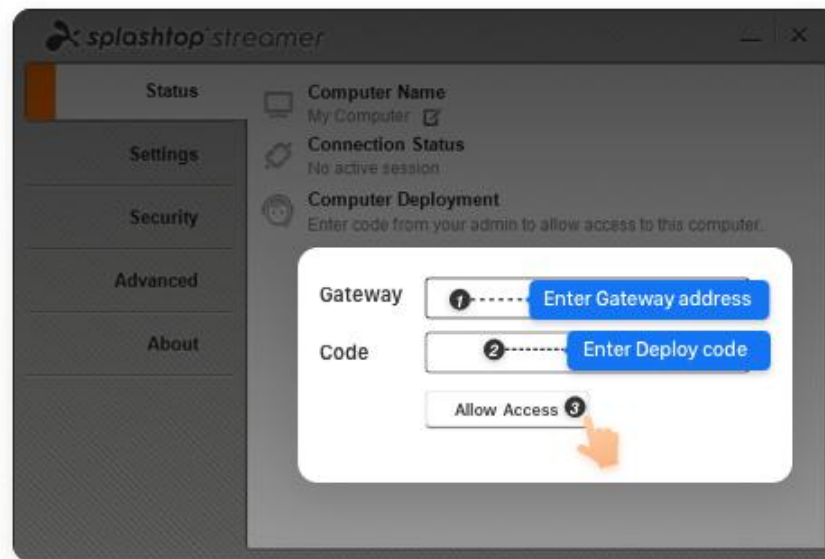
Change network port

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.

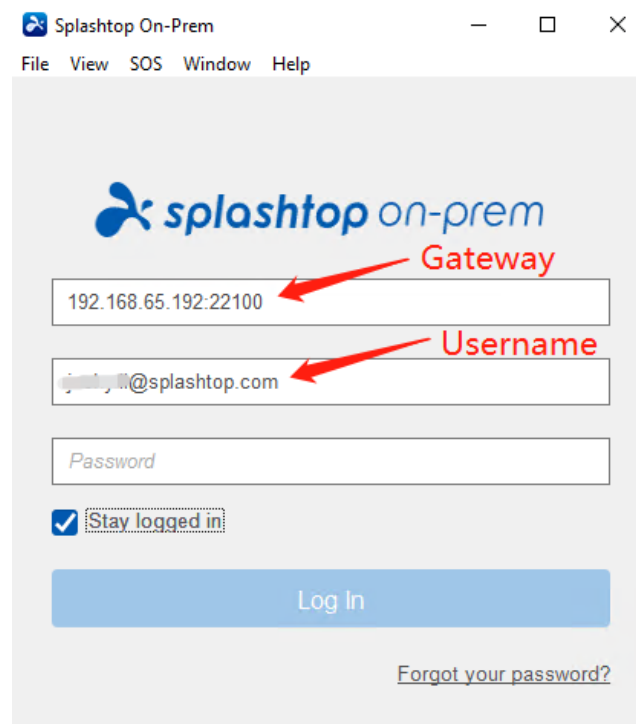


Notice:

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.
-

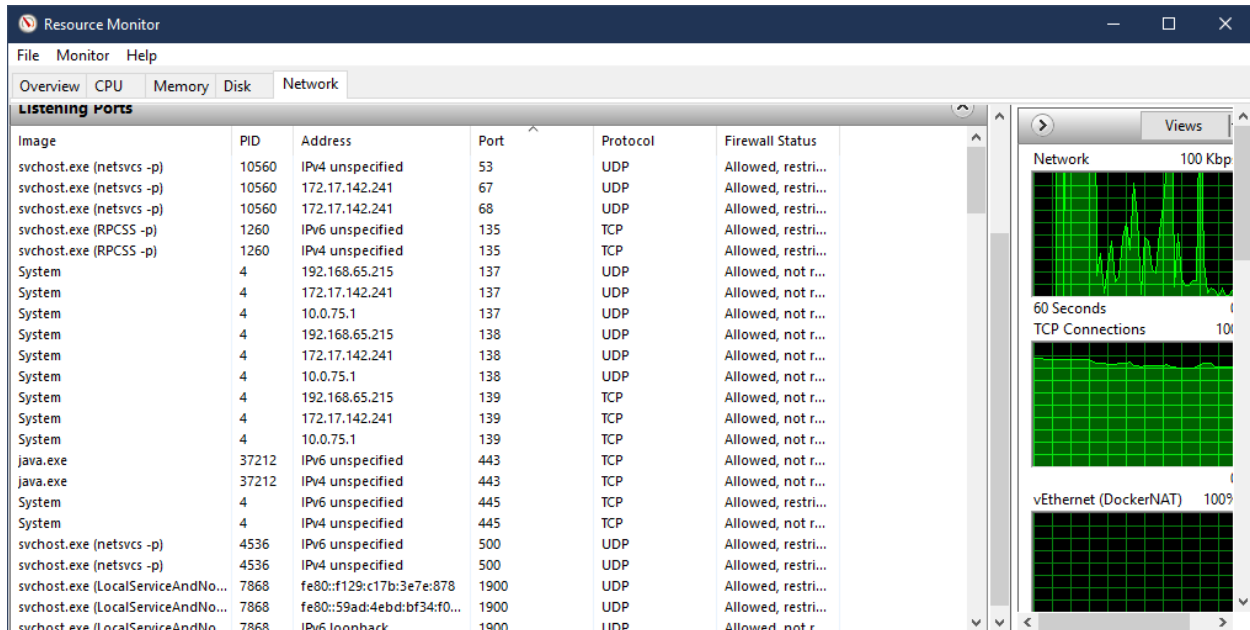


(Input *IP:Port* in the **Gateway** field when deploy)



(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.



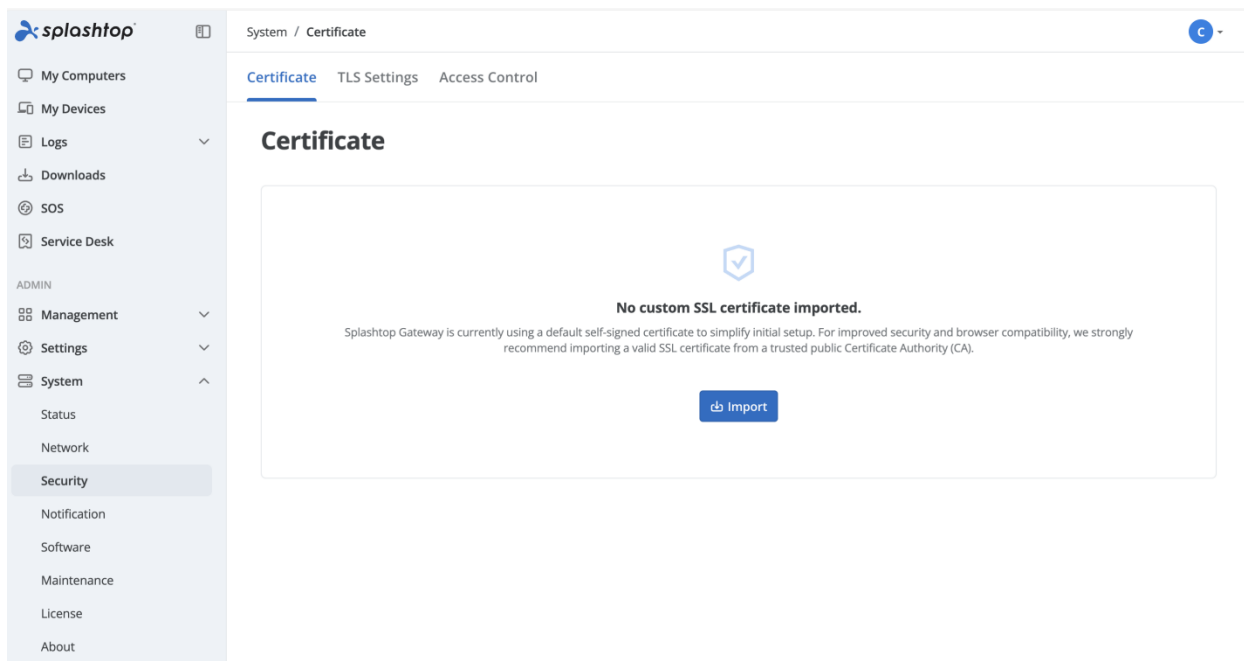
Security

Import SSL certificate

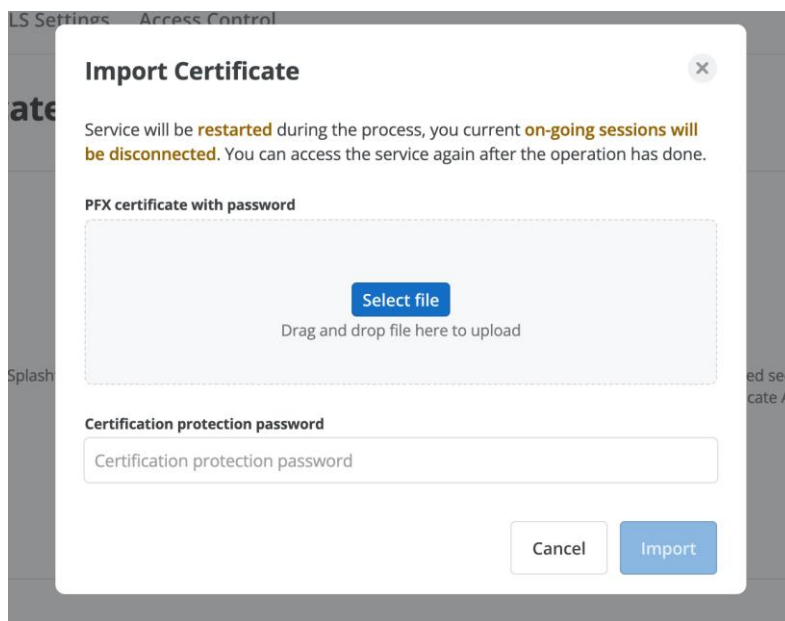
Splashtop Gateway supports importing your own certificate, which can be self-signed certificate, or certificate issued by 3rd party authority.

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 certificate 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.

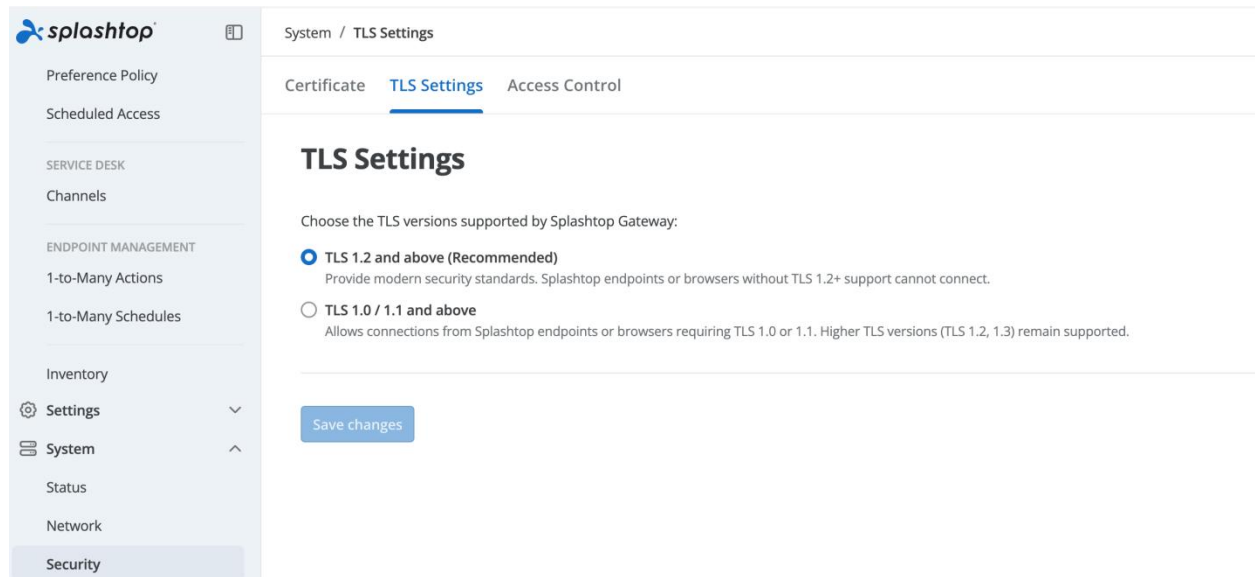
Star-splashtop.com.crt: the signature for our site, provided by 3rd CA

Int.cer: 3rd CA's certificate

TLS settings

Splashtop Gateway allows Team Owner to configure which TLS versions are supported for client and browser connections. You can choose between two options, depending on your security requirements and compatibility needs.

Log into Gateway's management console as Team Owner, go to **System > Security > TLS Settings**



Option 1: TLS 1.2 and above (Recommended)

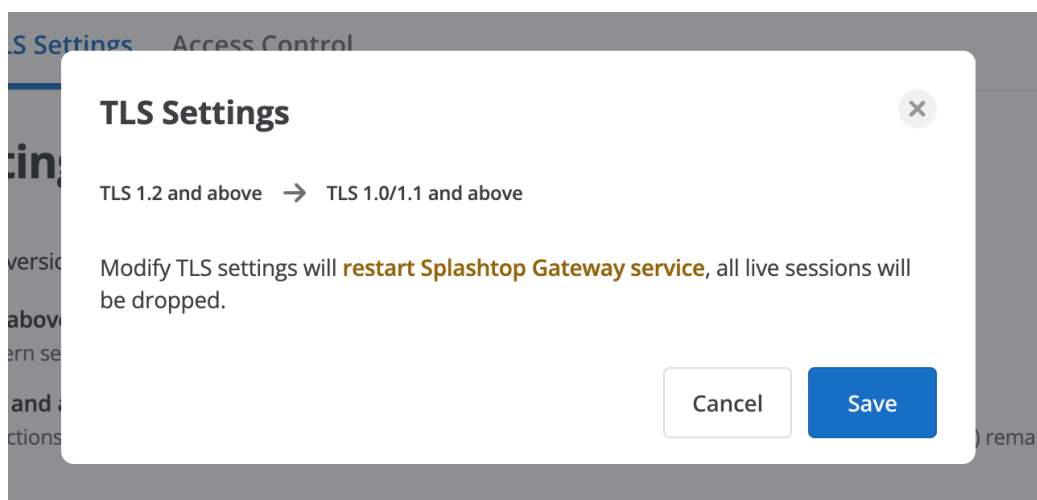
- Provides modern security standards.
- Ensures compliance with current industry and regulatory requirements.
- Only endpoints or browsers that support TLS 1.2 or higher can connect.
- Recommended for most deployments where security is the priority.

Option 2: TLS 1.0 / 1.1 and above

- Allows connections from older Splashtop endpoints or browsers that require TLS 1.0 or 1.1.
- Maintains backward compatibility with legacy environments.
- Higher TLS versions (1.2 and 1.3) remain supported, but this option is less secure than enforcing TLS 1.2+.

Applying Changes

- When you switch between these options and click **Save changes**, the Splashtop Gateway service will restart, and any active sessions will be disconnected.



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 refer 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:

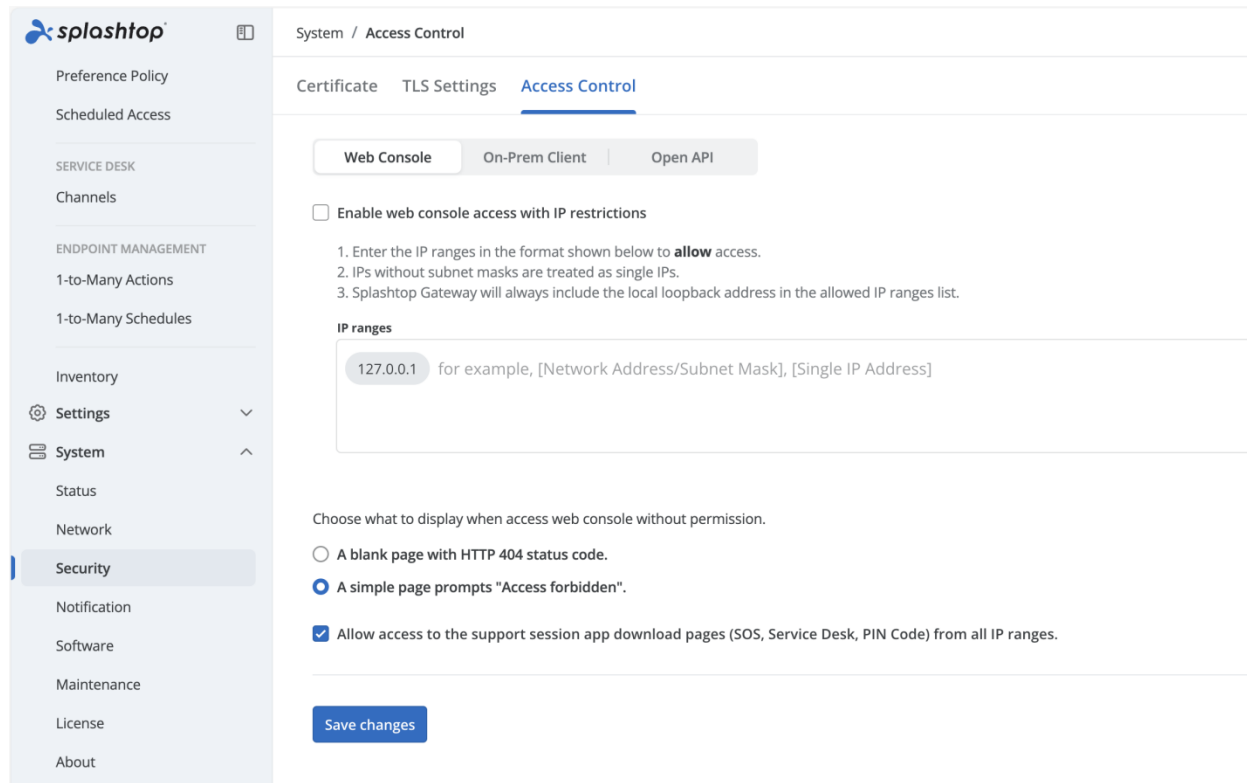
1. Windows XP uses SSL v3 by default for WinHTTP. Windows 8 or later uses TLS 1.1 for WinHTTP by default.

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 the team owner to manage the access of Gateway web console, On-Prem client app and Open API with IP restriction.



The screenshot shows the Splashtop Admin Console interface. On the left is a sidebar with navigation links: Preference Policy, Scheduled Access, SERVICE DESK (Channels), ENDPOINT MANAGEMENT (1-to-Many Actions, 1-to-Many Schedules), Inventory, Settings (with a dropdown arrow), System (with an up arrow), Status, Network, Security (highlighted with a blue bar), Notification, Software, Maintenance, License, and About. The main content area is titled 'System / Access Control' and has three tabs: Certificate, TLS Settings, and Access Control (which is active). Below the tabs are three sub-tabs: Web Console, On-Prem Client, and Open API. Under the 'Web Console' sub-tab, there is a checkbox labeled 'Enable web console access with IP restrictions'. Below this checkbox are three numbered instructions: 1. Enter the IP ranges in the format shown below to **allow** access. 2. IPs without subnet masks are treated as single IPs. 3. Splashtop Gateway will always include the local loopback address in the allowed IP ranges list. There is a text input field labeled 'IP ranges' containing the example '127.0.0.1 for example, [Network Address/Subnet Mask], [Single IP Address]'. Below the input field, there is a section titled 'Choose what to display when access web console without permission.' with three radio button options: 'A blank page with HTTP 404 status code.', 'A simple page prompts "Access forbidden".', and 'Allow access to the support session app download pages (SOS, Service Desk, PIN Code) from all IP ranges.' (which is selected with a blue circle). At the bottom of the main content area is a blue button labeled 'Save changes'.

Step 1

Log into Gateway's management console as Owner, go to System > Security > Access Control.

Splashtop currently supports IP restriction on the access to Gateway web console, On-Prem client app or Open API.

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

System / Access Control

Certificate TLS Settings **Access Control**

Web Console

On-Prem Client

Open API

☐ Enable Splashtop On-Prem Client access with IP restrictions

1. Enter the IP ranges in the format shown below to **allow** access.
2. IPs without subnet masks are treated as single IPs.
3. Splashtop Gateway will always include the local loopback address in the allowed IP ranges list.

IP ranges

127.0.0.1 for example, [Network Address/Subnet Mask], [Single IP Address]

Step 2

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

Choose what to display when access web console without permission.

- ☐ A blank page with HTTP 404 status code.
- ☒ A simple page prompts "Access forbidden".

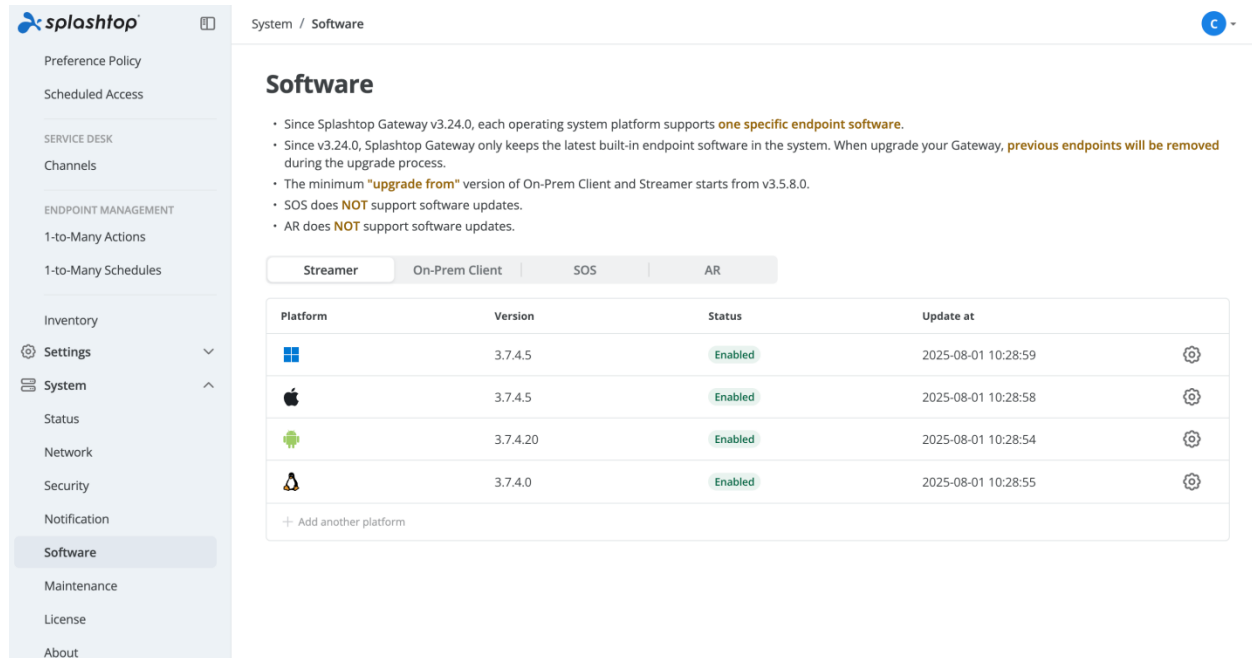
Step 3

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** > **Software** page allows Team Owner to manage the software components.



Software

- Since Splashtop Gateway v3.24.0, each operating system platform supports **one specific endpoint software**.
- Since v3.24.0, Splashtop Gateway only keeps the latest built-in endpoint software in the system. When upgrade your Gateway, **previous endpoints will be removed** during the upgrade process.
- The minimum **"upgrade from"** version of On-Prem Client and Streamer starts from v3.5.8.0.
- SOS does **NOT** support software updates.
- AR does **NOT** support software updates.

Platform	Version	Status	Update at
	3.7.4.5	Enabled	2025-08-01 10:28:59
	3.7.4.5	Enabled	2025-08-01 10:28:58
	3.7.4.20	Enabled	2025-08-01 10:28:54
	3.7.4.0	Enabled	2025-08-01 10:28:55

+ Add another platform

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.
- **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.
- **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.
- **AR: An innovative app that enables seamless augmented reality collaboration and support for remote teams.**

Team Owner can do the following operations in this page:

- Import new version of software components
- Set software components as enabled / disabled
- Remove software components
- Customize software components

Software updates

1. Introduction

Splashtop 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 Splashtop 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

Gateway v3.32.x -> Default Endpoints v3.7.2.x

2. When back up your Splashtop Gateway v3.24.0, the endpoints will **no longer** to be included in the backup file. As Splashtop continues to introduce new compatible platforms for the upmost cross-platform experience, 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

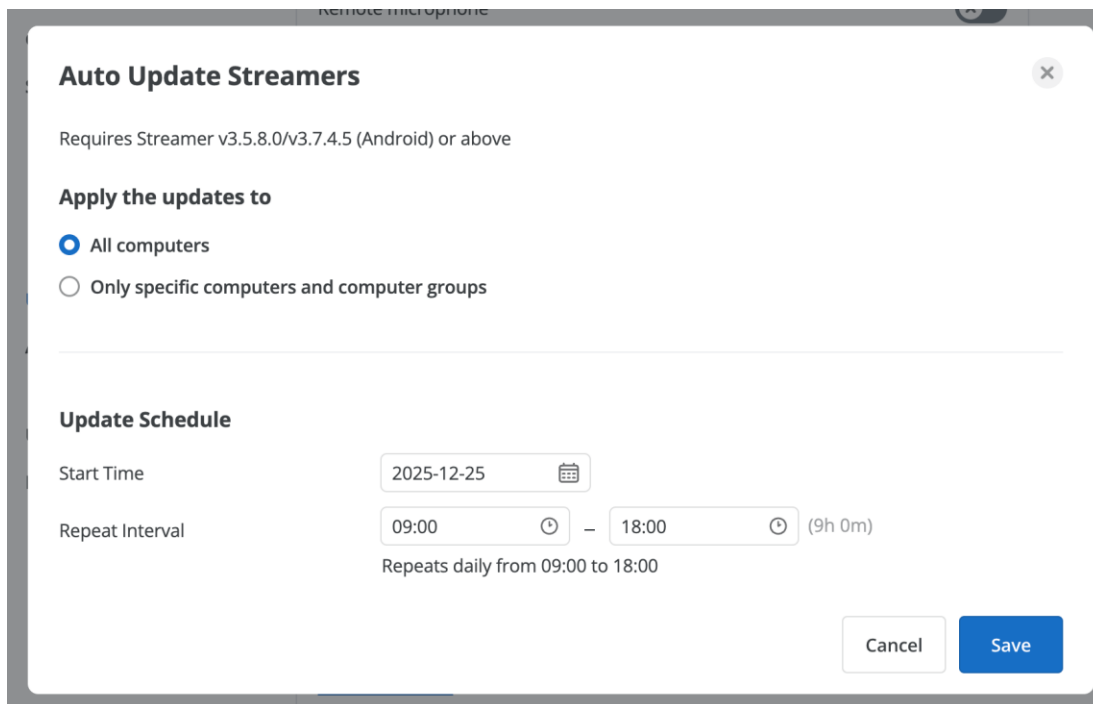
In the unattended scenario, Streamer auto update can be managed from Splashtop Gateway web console.

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

Settings / Team settings

General	SSH Computer			
Security	Web app ^① Learn more			
Two-step verification	System Tools for Owner only ^① 			
Device authentication	Offline computers policy Detailed settings			
Account policy	Auto update Streamers Detailed settings			
Session security	Scheduled access ^①	Asia/Shanghai (GMT +08:00) 		
Unattended access	Session Indicator ^①			
Attended access	Remote session Background actions ^①			
User Settings	Display type	Pop-up & Banner 		
	Allow user to close the banner			

2. In Unattended access section, find 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.

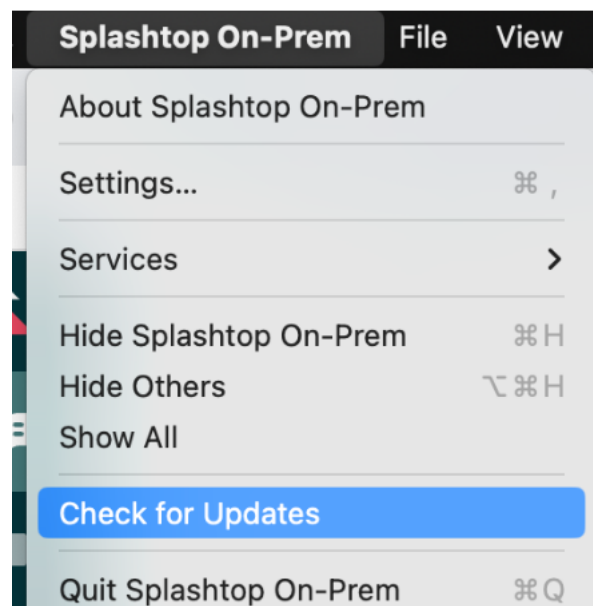
It is suggested to schedule the update interval during non-working hours.

Manual Updates

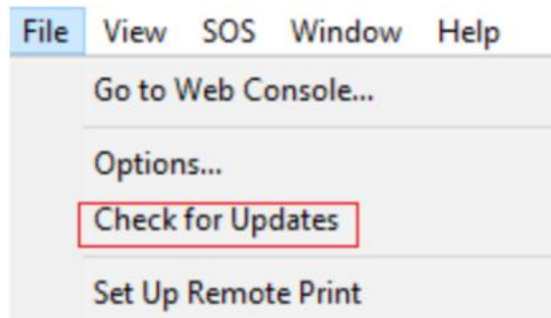
1. Splashtop On-Prem Client app

Log in to your Client app

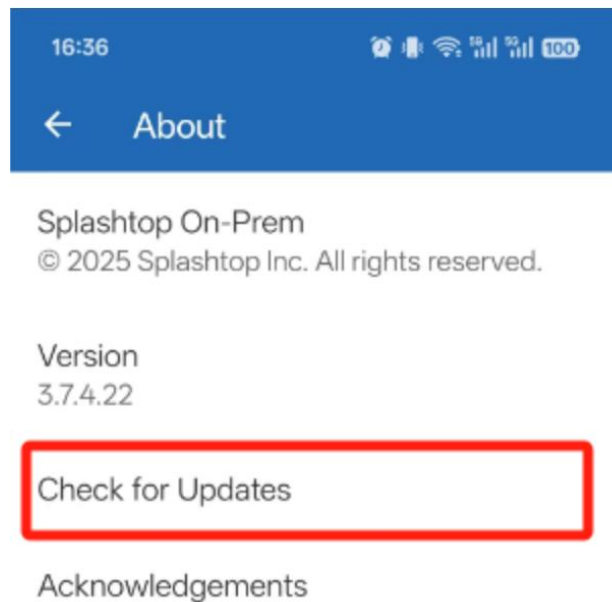
Mac: Splashtop On-Prem > Check for Updates



Windows: File > Check for Updates

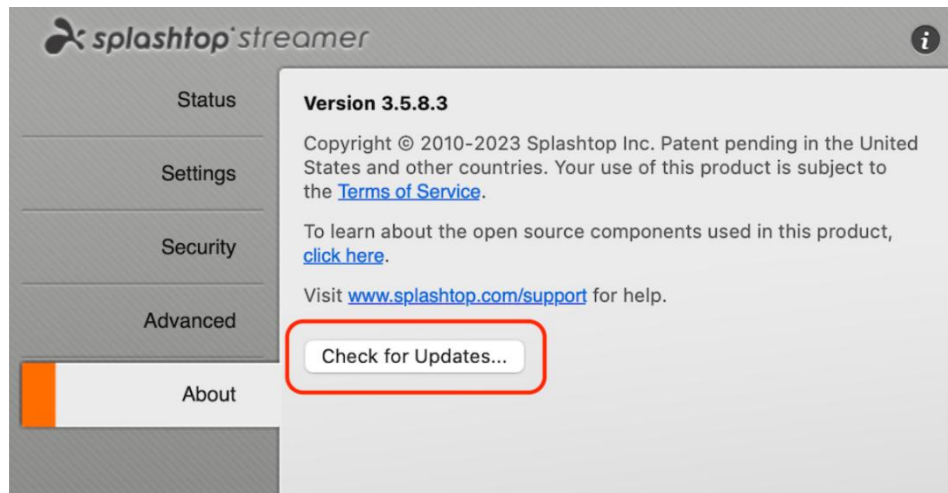


Windows: Settings > About > Check for Updates



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.

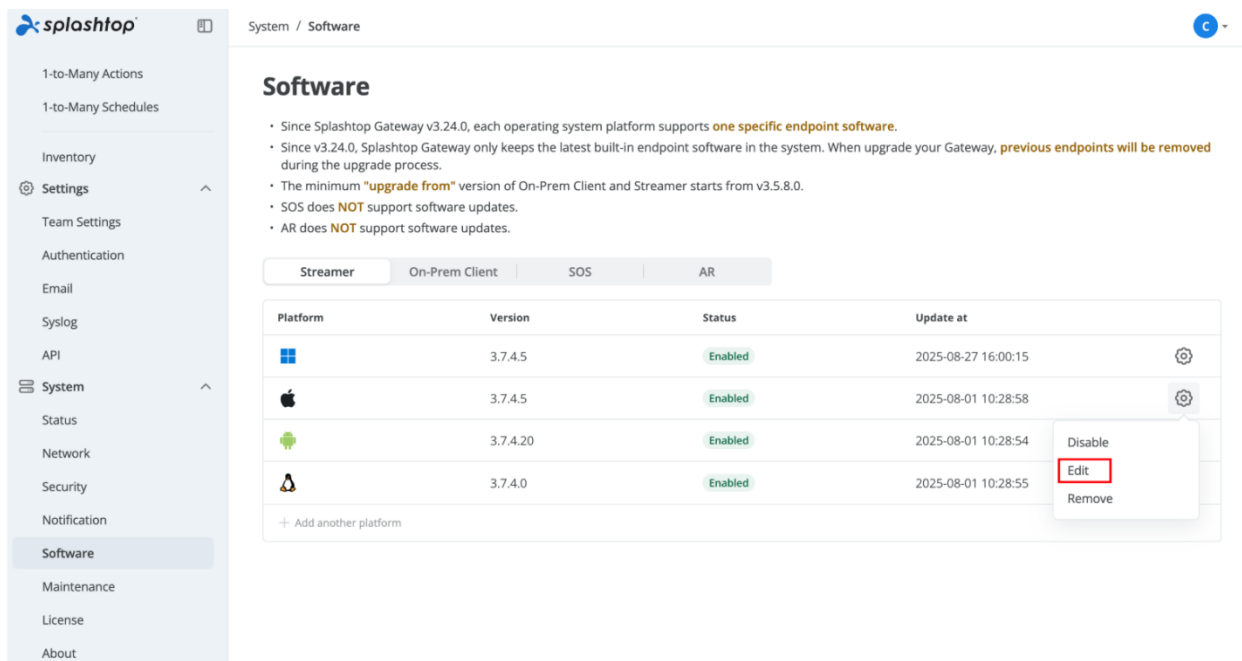
- **Splashtop Gateway** - [new version announcements page](#)
- **Splashtop Streamer** - [new version announcements page](#)
- **Splashtop On-Prem Client App** - [new version announcements page](#)



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

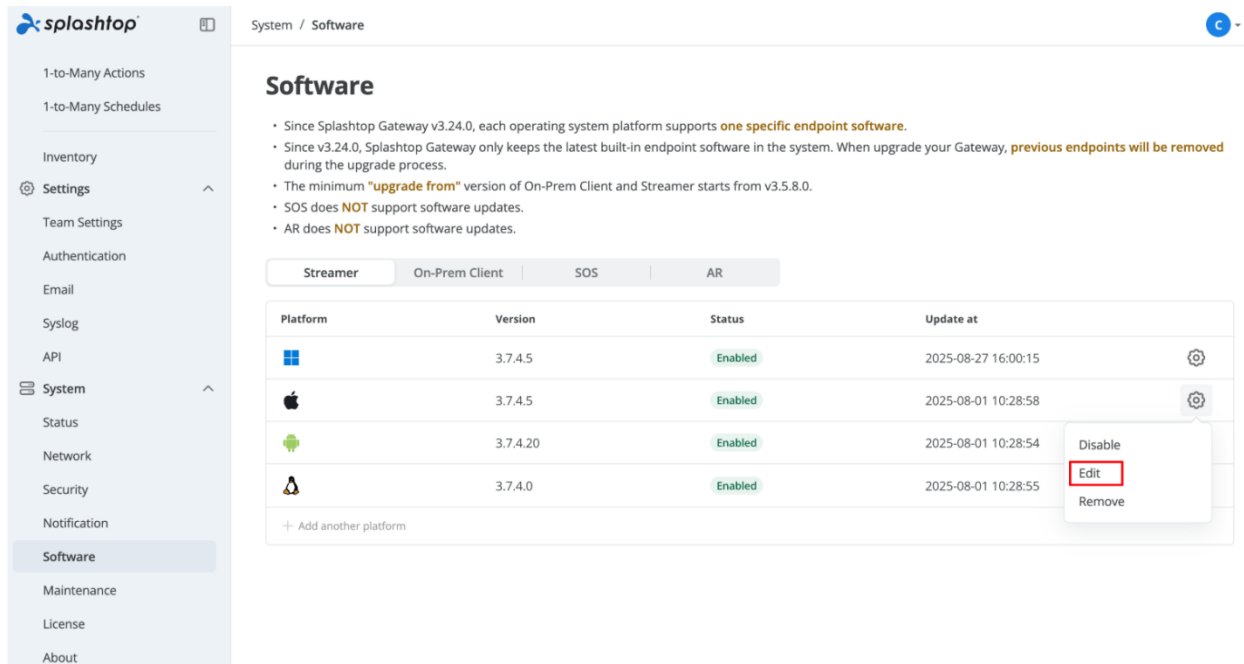


The screenshot shows the Splashtop Admin Console interface. On the left is a sidebar with navigation options: 1-to-Many Actions, 1-to-Many Schedules, Inventory, Settings (expanded), Team Settings, Authentication, Email, Syslog, API, System (expanded), Status, Network, Security, Notification, Software (selected), Maintenance, License, and About. The main content area is titled 'System / Software' and 'Software'. It contains a list of software endpoints for the 'Streamer' tab. The table has columns: Platform, Version, Status, and Update at. There are four entries, all with status 'Enabled'. A context menu is open over the third entry (Android), showing options: Disable, Edit (highlighted with a red box), and Remove. Below the table is a link '+ Add another platform'.

Platform	Version	Status	Update at
	3.7.4.5	Enabled	2025-08-27 16:00:15
	3.7.4.5	Enabled	2025-08-01 10:28:58
	3.7.4.20	Enabled	2025-08-01 10:28:54
	3.7.4.0	Enabled	2025-08-01 10:28:55

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.



Software

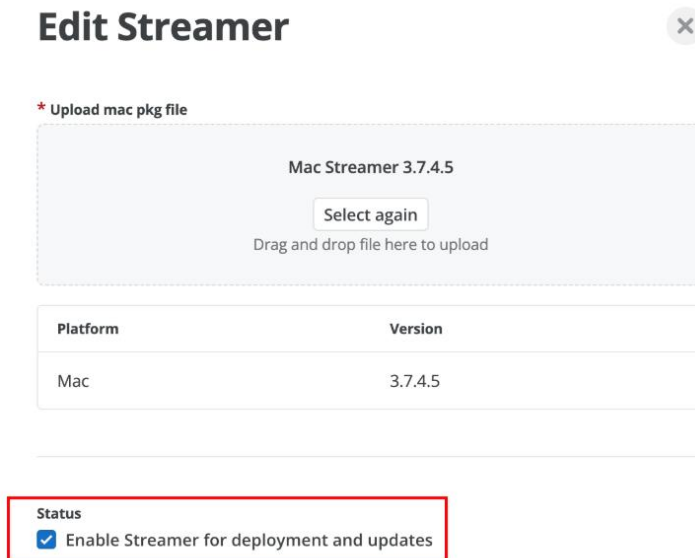
- Since Splashtop Gateway v3.24.0, each operating system platform supports **one specific endpoint software**.
- Since v3.24.0, Splashtop Gateway only keeps the latest built-in endpoint software in the system. When upgrade your Gateway, **previous endpoints will be removed** during the upgrade process.
- The minimum **"upgrade from"** version of On-Prem Client and Streamer starts from v3.5.8.0.
- SOS does **NOT** support software updates.
- AR does **NOT** support software updates.

Platform	Version	Status	Update at
Windows	3.7.4.5	Enabled	2025-08-27 16:00:15
macOS	3.7.4.5	Enabled	2025-08-01 10:28:58
Linux	3.7.4.20	Enabled	2025-08-01 10:28:54
Android	3.7.4.0	Enabled	2025-08-01 10:28:55

+ Add another platform

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.



Edit Streamer

* Upload mac pkg file

Mac Streamer 3.7.4.5

Select again

Drag and drop file here to upload

Platform	Version
Mac	3.7.4.5

Status

☒ Enable Streamer for deployment and updates

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

Deployment Options

Deploy with Link
Deploy with Installer

1 Download the Streamer installer.

Windows

macOS

Android

Linux

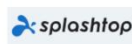
Splashtop Streamer app for Windows

Windows 7 and above (Streamer version 3.7.4.5)

EXE
MSI

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.


System / Software

Software

- Since Splashtop Gateway v3.24.0, each operating system platform supports **one specific endpoint software**.
- Since v3.24.0, Splashtop Gateway only keeps the latest built-in endpoint software in the system. When upgrade your Gateway, **previous endpoints will be removed** during the upgrade process.
- The minimum "**upgrade from**" version of On-Prem Client and Streamer starts from v3.5.8.0.
- SOS does **NOT** support software updates.
- AR does **NOT** support software updates.

Streamer
On-Prem Client
SOS
AR

Platform	Version	Status	Update at	
	3.7.4.6	Disabled	2025-08-27 16:01:30	
	3.7.4.5	Enabled	2025-08-01 10:28:47	Enable Edit Remove
	3.7.4.23	Enabled	2025-08-01 10:28:45	

+ Add another platform

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 Client app to make it available for downloads and updates.

Edit On-Prem Client ✕

* Upload windows pkg file

Windows Client 3.7.4.6
Select again
Drag and drop file here to upload

Platform	Version
Windows	3.7.4.6

Status

☒ Enable On-Prem Client for downloads and updates

3. Once done, the newly uploaded software is now available for downloads and updates from Gateway.

Downloads

Download Splashtop On-Prem app



Splashtop On-Prem app for Windows

Windows 7 and above (On-Prem Client version 3.7.4.6)



Notes:

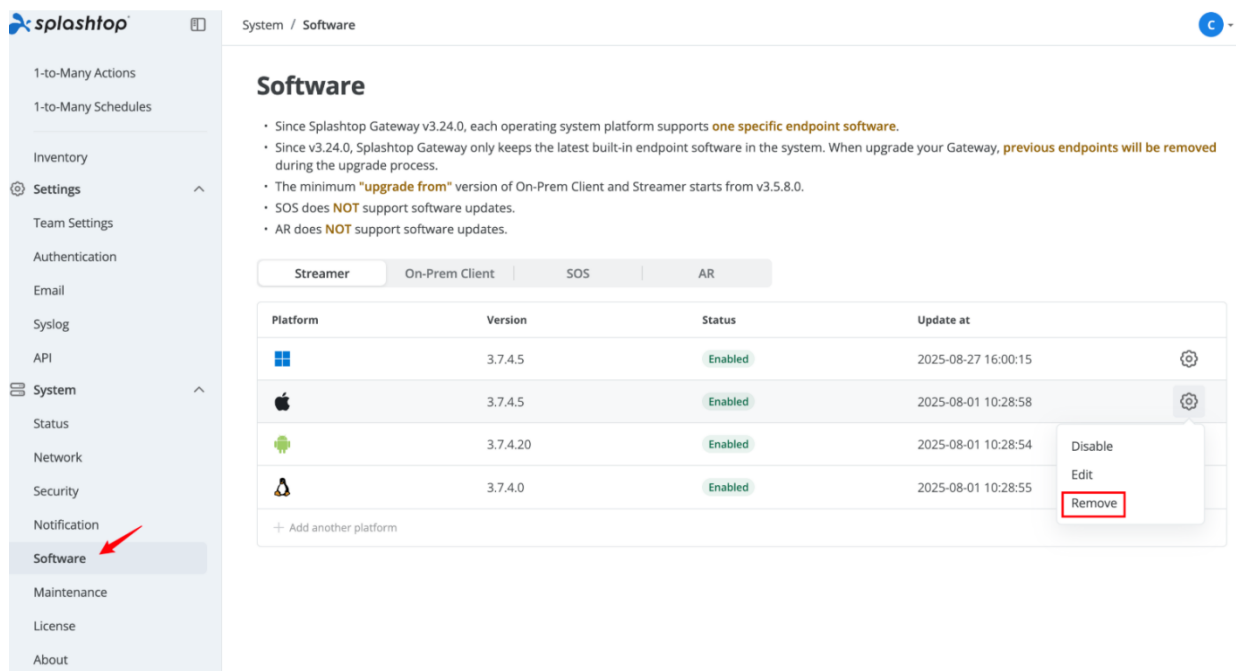
1. If you are looking for **Splashtop Streamer**, which needs to be installed on the computer you would like to remote access to, please visit the [Management > Deployment](#) page.
2. If you are looking for **Splashtop SOS**, which allows user to run on the computer and share the 9-digit session code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

Remove software components

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

Remove Streamer

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



Software

- Since Splashtop Gateway v3.24.0, each operating system platform supports **one specific endpoint software**.
- Since v3.24.0, Splashtop Gateway only keeps the latest built-in endpoint software in the system. When upgrade your Gateway, **previous endpoints will be removed** during the upgrade process.
- The minimum **"upgrade from"** version of On-Prem Client and Streamer starts from v3.5.8.0.
- SOS does **NOT** support software updates.
- AR does **NOT** support software updates.

Streamer | On-Prem Client | SOS | AR

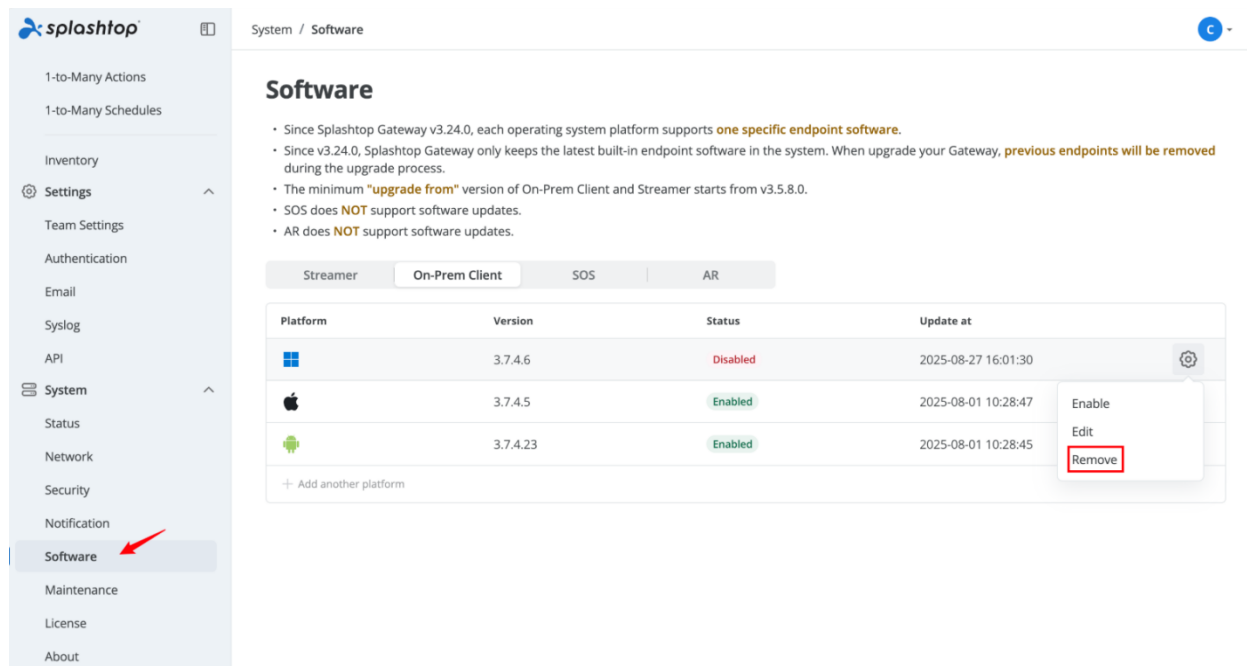
Platform	Version	Status	Update at	
	3.7.4.5	Enabled	2025-08-27 16:00:15	
	3.7.4.5	Enabled	2025-08-01 10:28:58	
	3.7.4.20	Enabled	2025-08-01 10:28:54	Disable Edit Remove
	3.7.4.0	Enabled	2025-08-01 10:28:55	

+ Add another platform

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 Client*, in the gear button menu, click *Remove* to remove it from Gateway.



System / Software

Software

- Since Splashtop Gateway v3.24.0, each operating system platform supports **one specific endpoint software**.
- Since v3.24.0, Splashtop Gateway only keeps the latest built-in endpoint software in the system. When upgrade your Gateway, **previous endpoints will be removed** during the upgrade process.
- The minimum **"upgrade from"** version of On-Prem Client and Streamer starts from v3.5.8.0.
- SOS does **NOT** support software updates.
- AR does **NOT** support software updates.

Platform	Version	Status	Update at
	3.7.4.6	Disabled	2025-08-27 16:01:30
	3.7.4.5	Enabled	2025-08-01 10:28:47
	3.7.4.23	Enabled	2025-08-01 10:28:45

+ Add another platform

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

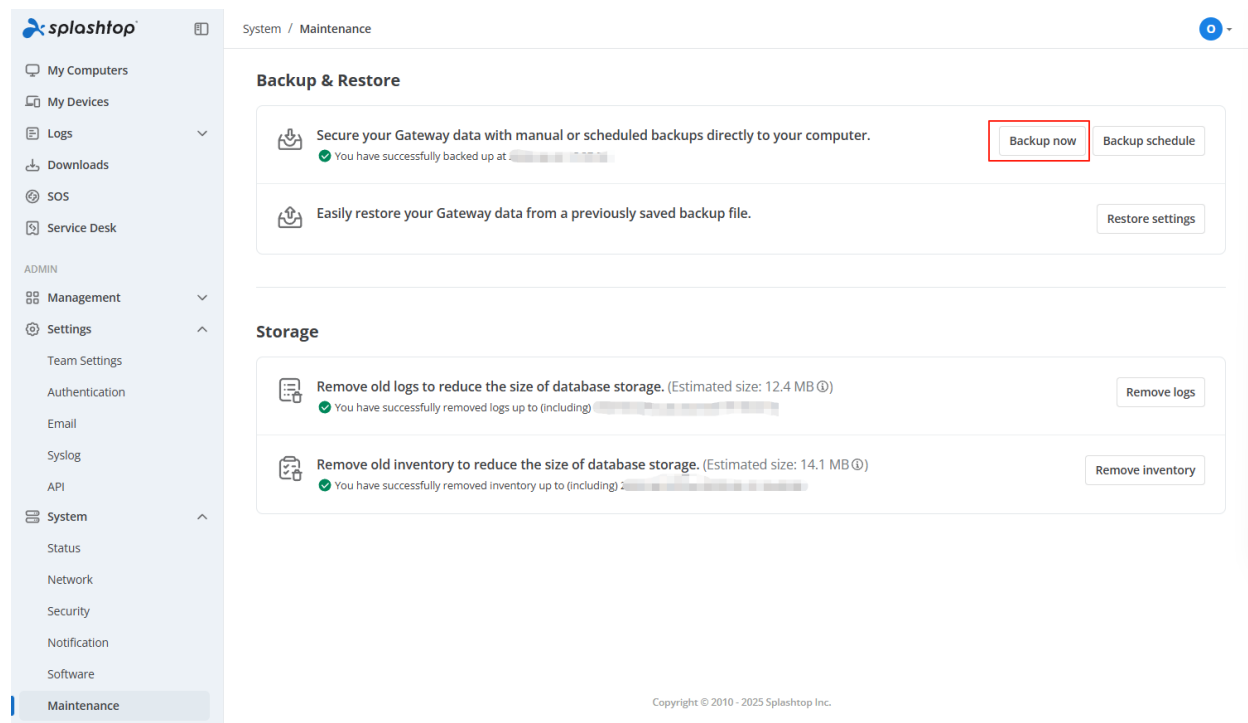
Maintenance

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.

Backup Now

Backup Choice

☒ Include Gateway logs in the backup
Estimated size: 6.0 MB ⓘ

☒ Include Computer Inventory in the backup
Estimated size: 2.8 MB ⓘ

Set password for the output ZIP file

*** Password**

Password, minimum 8

*** Confirm Password**

Password, minimum 8

These items will be included in the backup:

- ✓ Certificate
- ✓ Gateway settings and data
- ✓ Gateway logs
- ✓ Computer Inventory

These items will not be included in the backup:

- ✗ License
- ✗ Software Component (Streamer, On-Prem app, SOS)
- ✗ Centralized session recordings

Cancel

Backup Now

A confirmation dialog will appear, listing the size of backup items in the database included in this backup.

Start Backup Now

Are you sure you want to start the backup?

Backup item	Size
Gateway settings and data	51.5 MB
Gateway logs	12.4 MB
Computer Inventory	14.1 MB
Estimated backup size ⓘ	78.0 MB

CancelStart

When you click the **Start** 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 etc. However, license is not a part of the backup, hence the system requires license re-activation if restored from the SQL script.

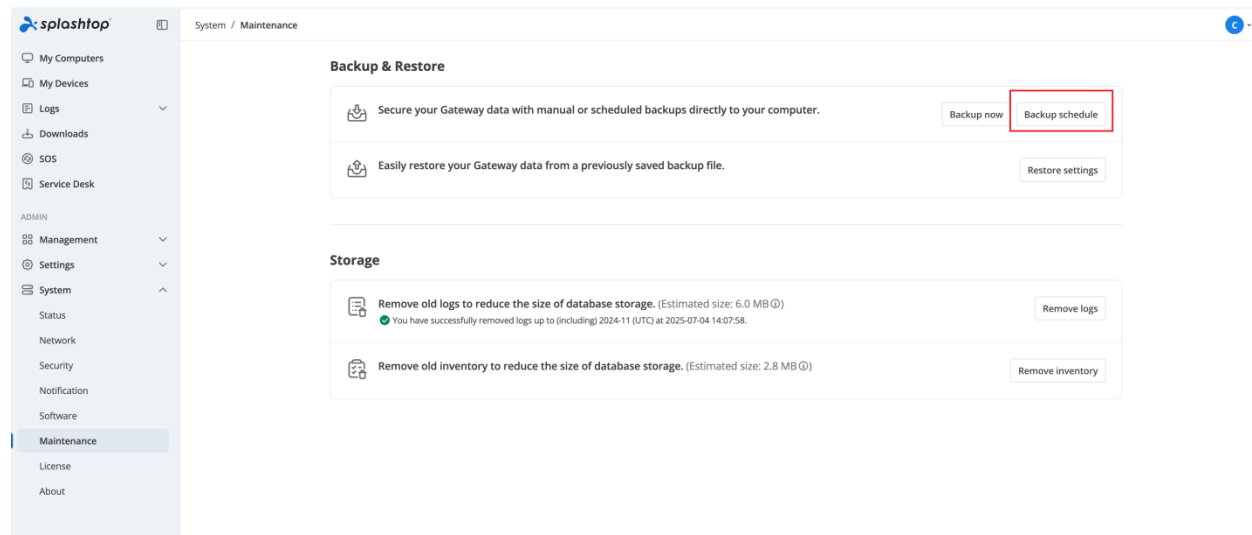
Backup schedule

Backup schedule is a useful way to ensure that backups are done in a consistent and timely manner. If 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.

Backup Schedule ✕

Status
☒ Enable Backup Schedule

Backup Folder
 C:\Program Files (x86)\Splashtop\Splashtop Remote\Splashtop Gateway\Backup Schedule

Backup Choice
☒ Include Gateway logs in the backup
☒ Include Computer Inventory in the backup

Set password for the output ZIP file

*** Password**

*** Confirm Password**

*** Backup Days**
☒ Sun ☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☒ Sat

Backup Time
 (UTC Time: 00:00)

Retention Rule
 Keep the number of backups

These items will be included in the backup:

- ✓ Certificate
- ✓ Gateway settings and data
- ✓ Gateway logs
- ✓ Computer Inventory

These items will not be included in the backup:

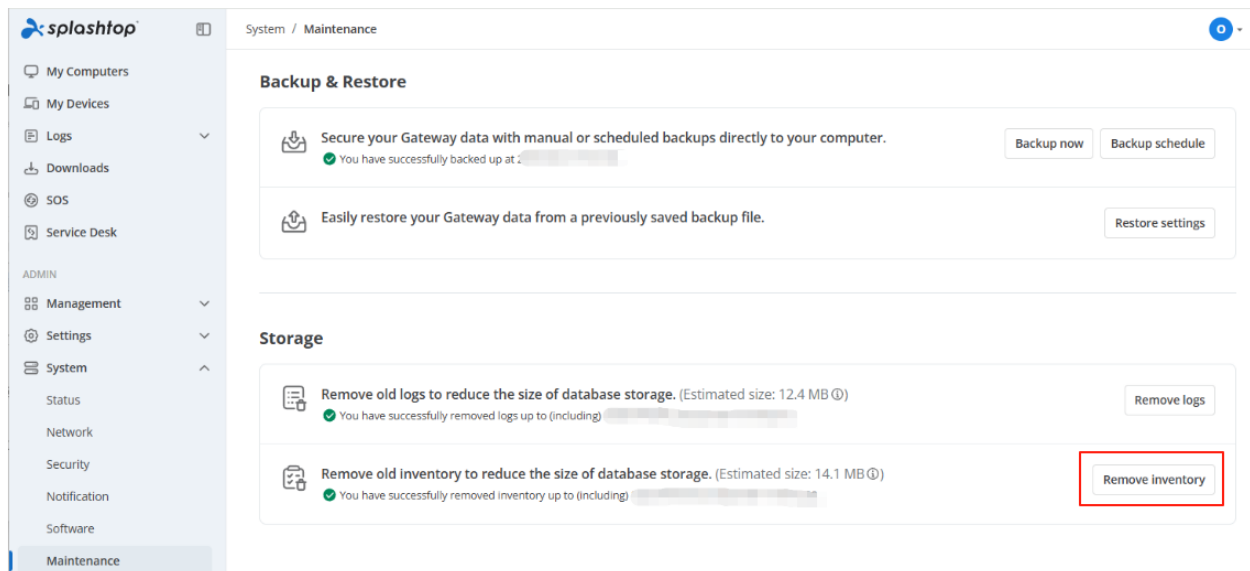
- ✗ License
- ✗ Software Component (Streamer, On-Prem app, SOS)
- ✗ Centralized session recordings

- **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 Computer inventory history 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

Starting from **Gateway v3.36.x**, the team owner can remove computer inventory for maintenance purpose.



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

Find "**Remove inventory**" and start to clear up your computer inventory to release the disk space.

Note:

1. Removed computer inventory 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 computer inventory.
2. Computer inventory is removed by month(s), and logs of the nearest 2 months cannot be removed.

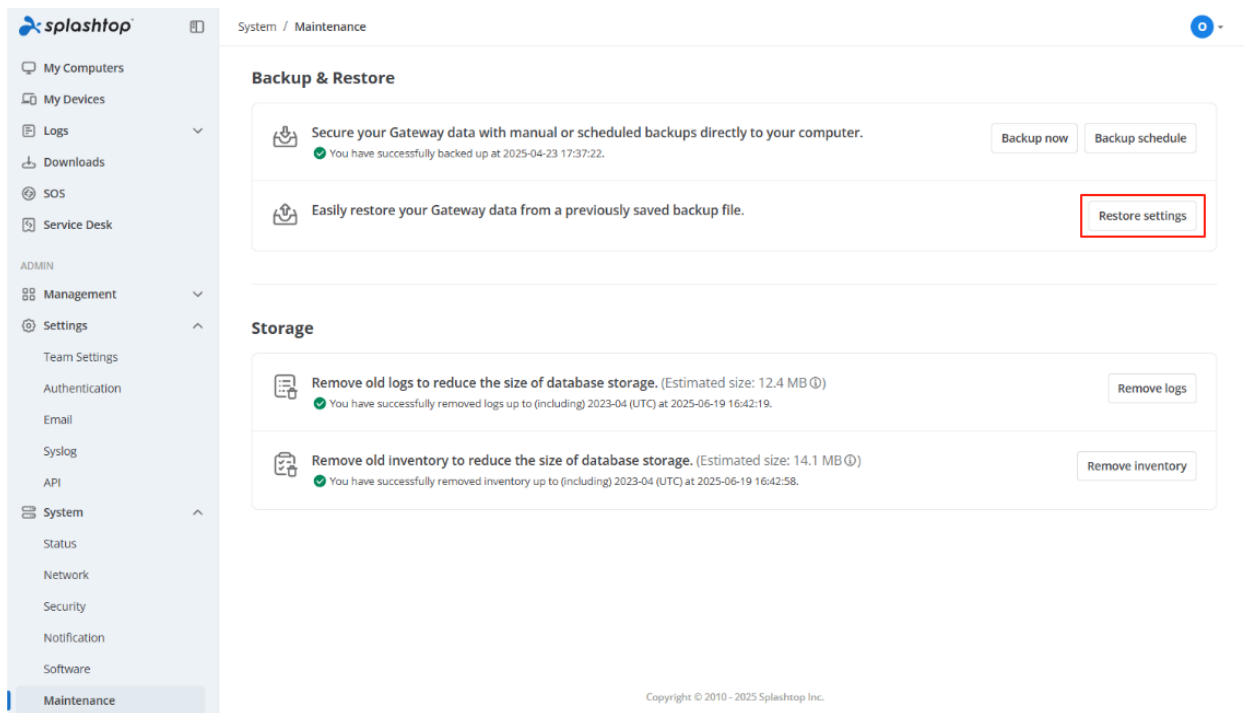
Restore

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.

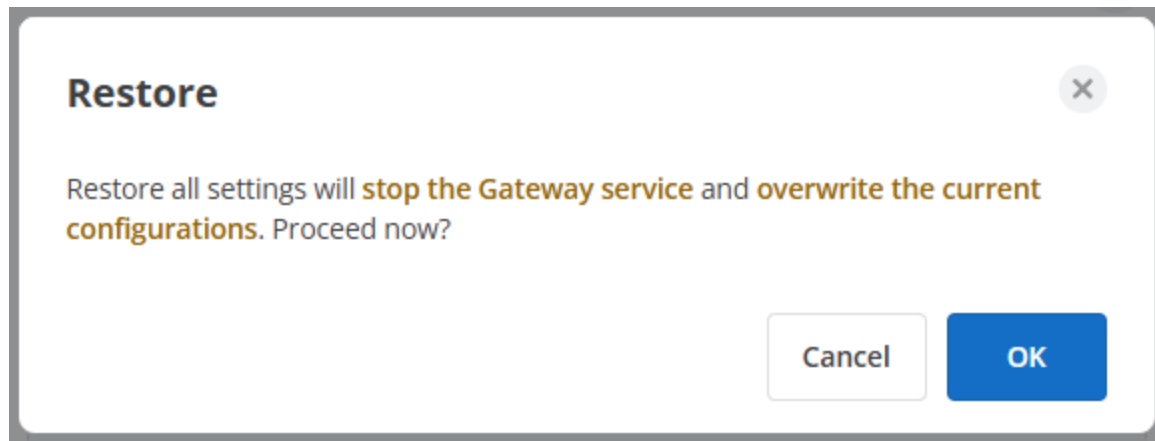
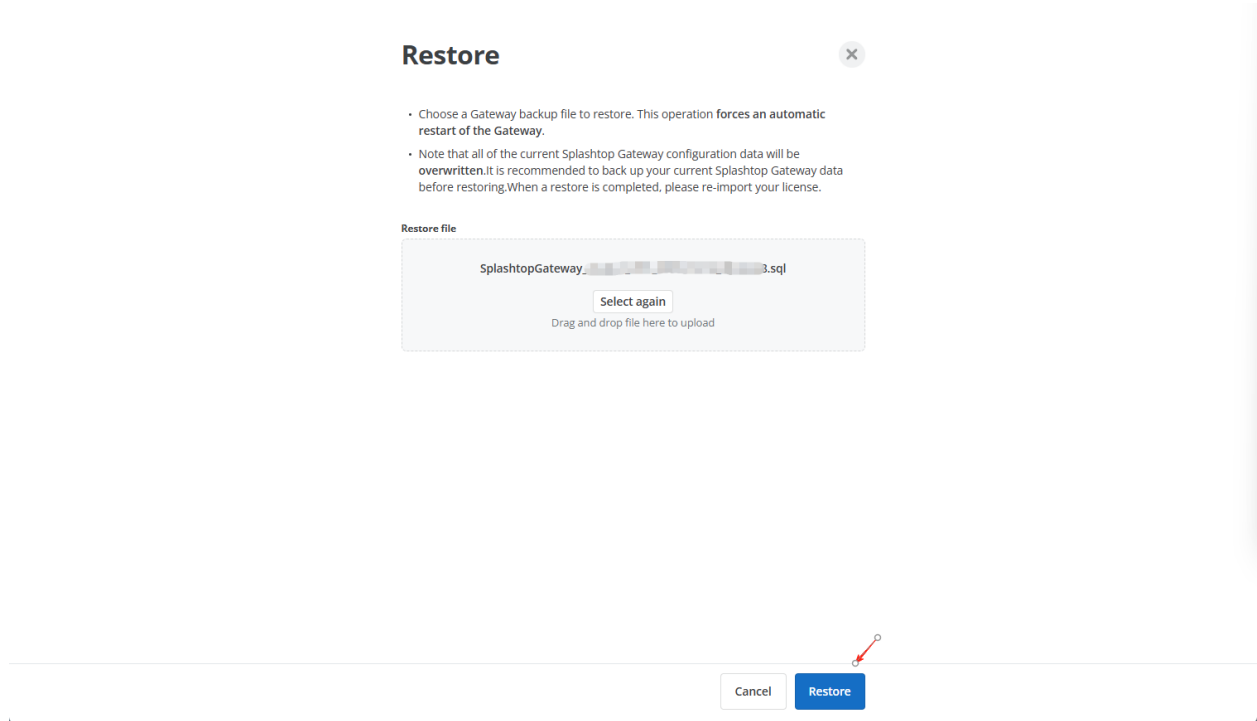
Same as **Backup**, you have to log in with the system owner account to the Splashtop Gateway web portal, click on System menu and navigate to the **Maintenance** page.

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

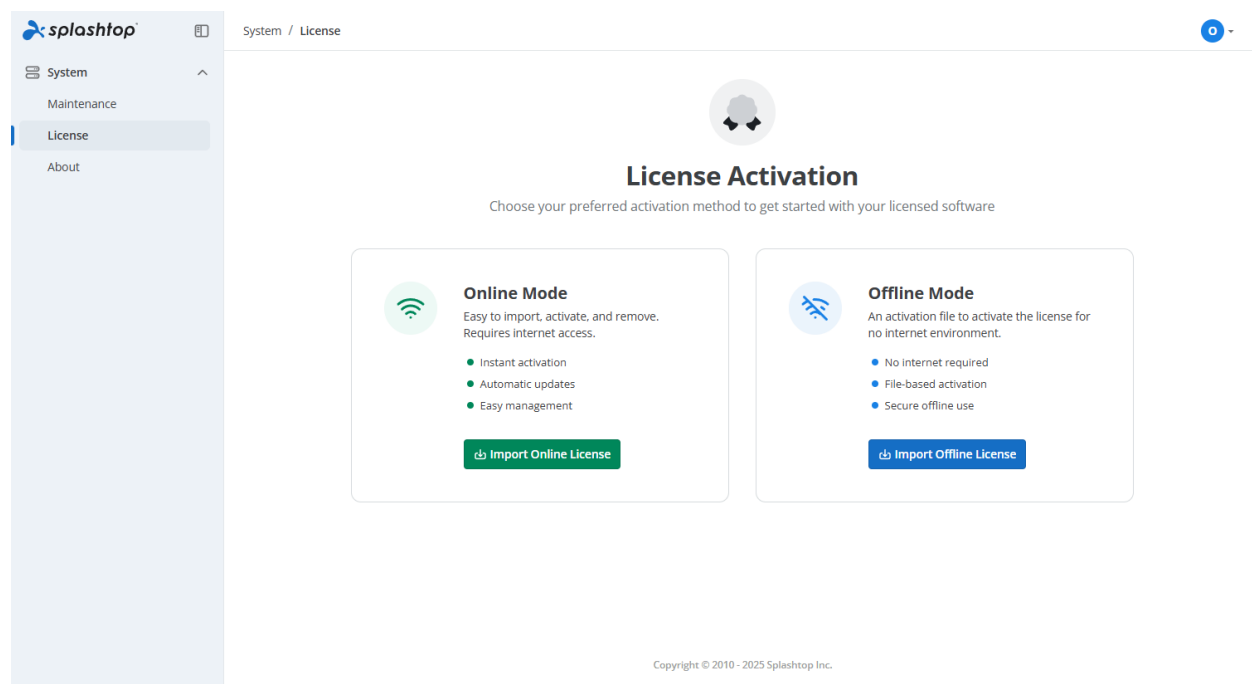


The screenshot displays the Splashtop On-Prem Admin Guide interface. On the left is a sidebar with a navigation menu including 'My Computers', 'My Devices', 'Logs', 'Downloads', 'SOS', 'Service Desk', 'ADMIN', 'Management', 'Settings', 'Team Settings', 'Authentication', 'Email', 'Syslog', 'API', 'System', and 'Maintenance' (which is currently selected). The main content area is titled 'System / Maintenance' and contains two sections: 'Backup & Restore' and 'Storage'. The 'Backup & Restore' section has a message about securing Gateway data with manual or scheduled backups, with a 'Backup now' button and a 'Backup schedule' button. Below this, it says 'Easily restore your Gateway data from a previously saved backup file.' with a 'Restore settings' button highlighted by a red rectangle. The 'Storage' section has two items: 'Remove old logs to reduce the size of database storage. (Estimated size: 12.4 MB)' with a 'Remove logs' button, and 'Remove old inventory to reduce the size of database storage. (Estimated size: 14.1 MB)' with a 'Remove inventory' button. At the bottom of the page, there is a copyright notice: 'Copyright © 2010 - 2025 Splashtop Inc.'

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.

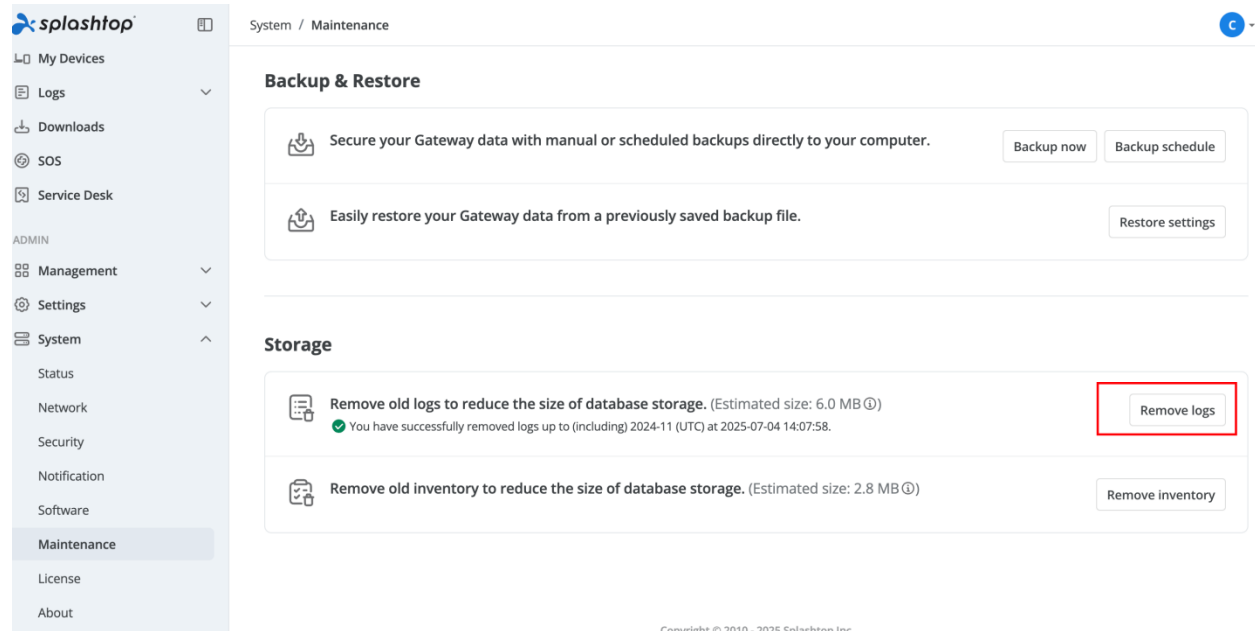


Activate the license through online or offline mode, depending on the type of license you acquired before.

Now you have done a successful system restoration.

Remove Splashtop On-Prem logs

System administrator can remove Gateway logs for maintenance purpose.



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

Find "Remove logs" 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 corresponding 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.

System / Notification

System Notification

☐ Enable

Input notification content, max 300 characters

End Time (UTC)

Select Date

2024-12-06



Select Time

16:52



Save

Below screenshot provides System notification as an example:

System Notification

☒ Enable

Input notification content, max 300 characters

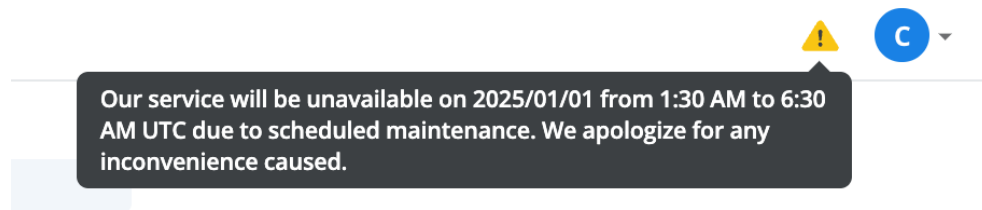
Our service will be unavailable on 2025/01/01 from 1:30 AM to 6:30 AM UTC due to scheduled maintenance. We apologize for any inconvenience caused.

End Time (UTC)

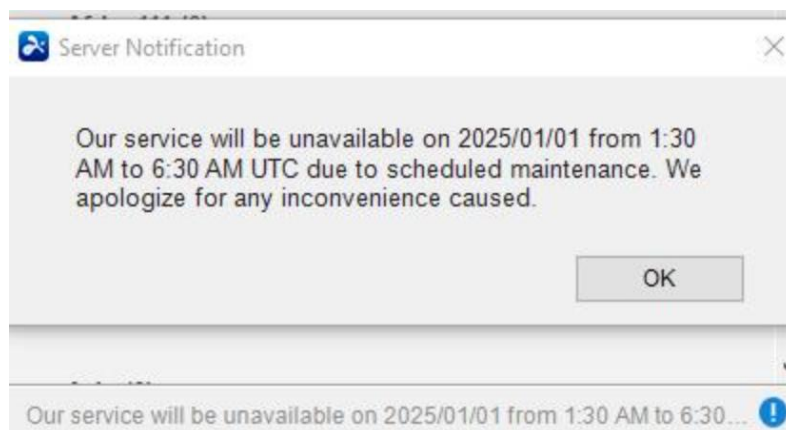
Select Date	Select Time
2025-01-01 	06:30 

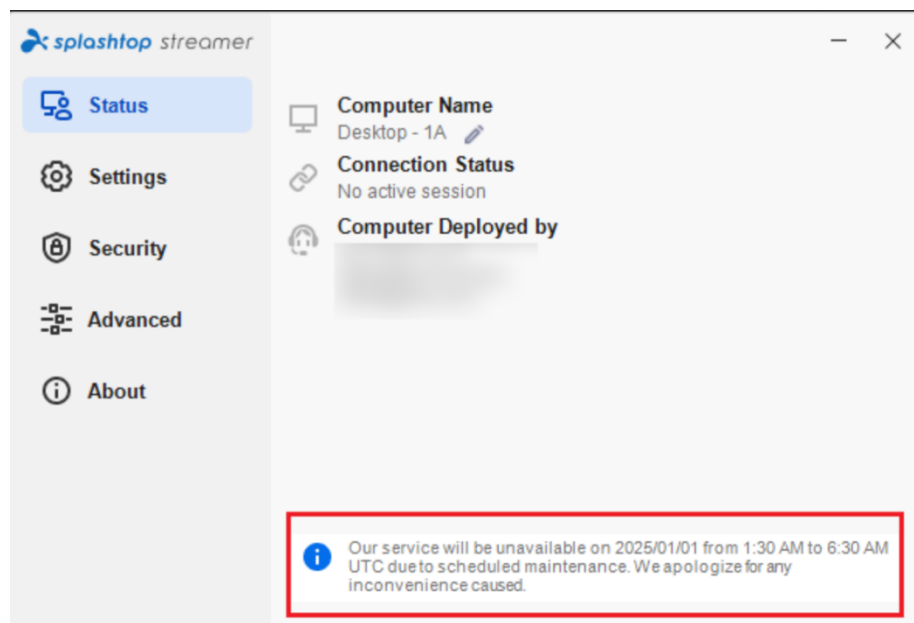
Save

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. 6:30 AM on 2025/01/01.



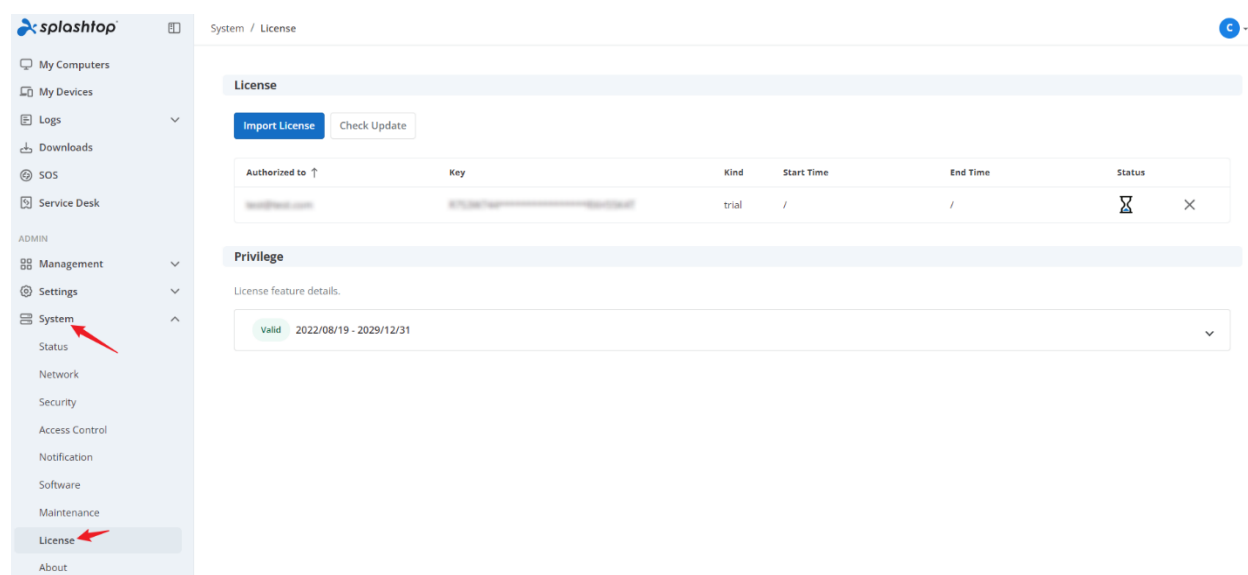


Splashtop On-Prem License

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

<i>Unattended Feature</i>	
Max Remote Session	Max number of unattended concurrent sessions on the entire system, even if it is set to <i>unlimited</i> , 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

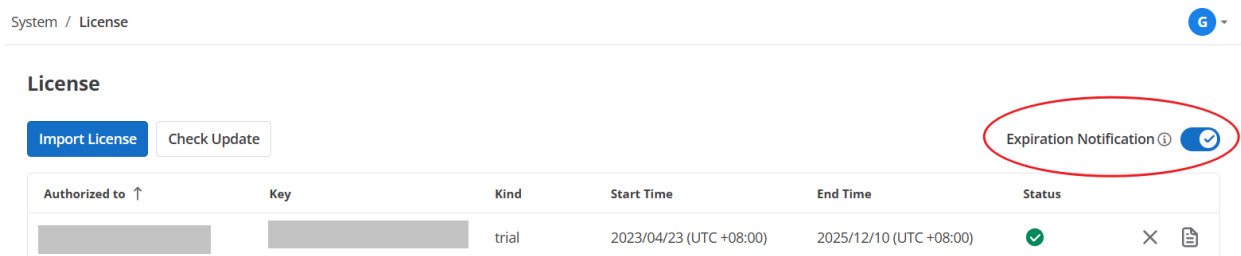
Computer Streamer	Computer Streamer is allowed or not, which means Windows, Mac, Linux (coming soon)
Mobile Streamer	Mobile Streamer is allowed or not, which means Android
Terminal Session	Access RDP terminal session is allowed or not
Multi-to-one Monitor	Multiple screen to one screen is allowed or not
Multi-to-multi Monitor	Multiple screen to multiple screen is allowed or not
Session Recording	Session recording is allowed or not
<i>Attended feature</i>	
Max Remote Session	Max number of attended sessions on the entire system, even it's set to <i>unlimited</i> , 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

License Expiration Reminder

Splashtop On-Prem provides automatic license expiration notifications to help administrators take timely action and avoid service disruptions.

Feature Details

- This feature is enabled by default, and no manual setup is required. You can find it under System -> License.

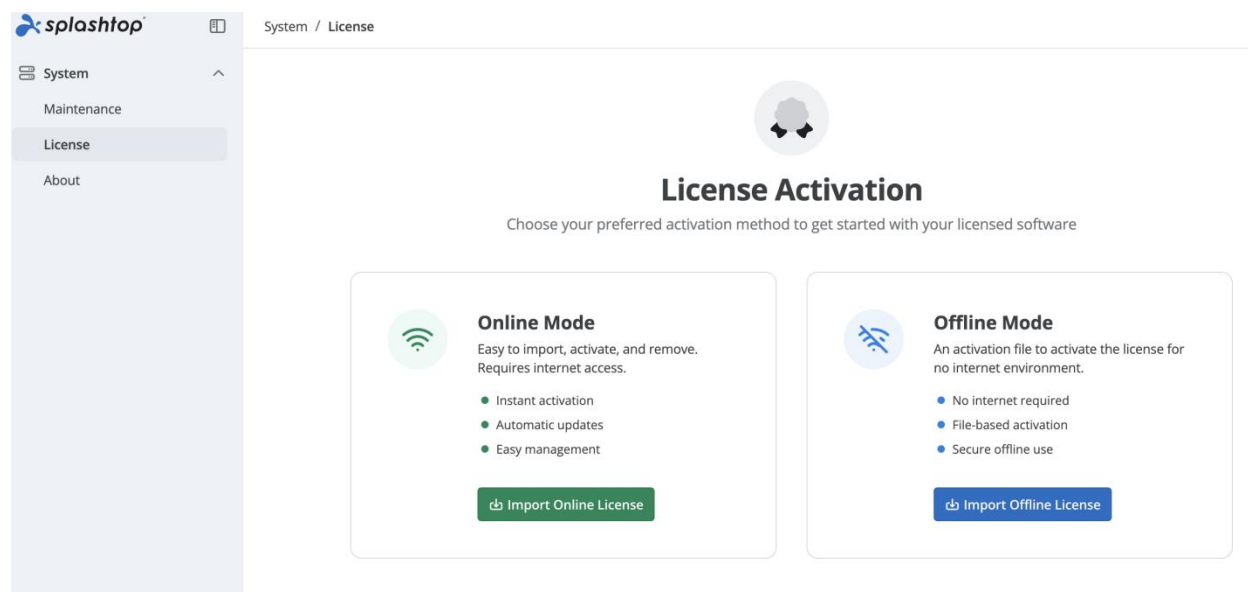


- Team Owner will receive email notifications 30, 7, and 1 day(s) before the license expires.
- This feature takes effect when the SMTP server is enabled.

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, enter the Authorized to and License key which you obtain from Splashtop Sales.

Import Online License

 New license will be merged with your current license set.

License information

Authorized to

E-mail associated with your license

License Key

Online mode license key



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.

Import Offline License ×

1 New offline license activation file will overwrite current license list

1 Press the save button to save the Activation ID to a file Save

2 Send the saved file to Splashtop Support to get your offline activation file

3 Import the offline activation file to activate the offline license

Select file

Drag and drop file here to upload

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 **Select** to upload the activation file and click **Import** to finish offline license activation.

About

The About page provides relevant system information, includes:

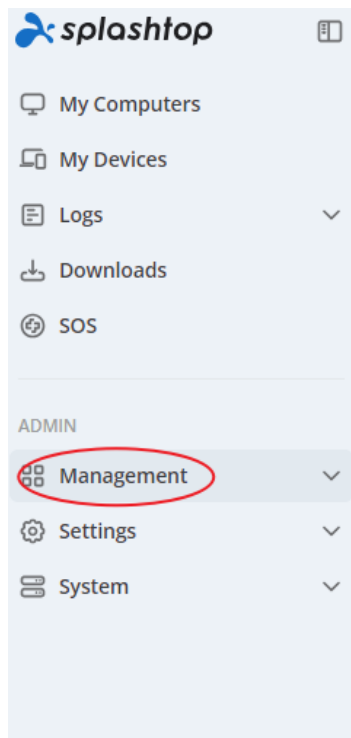
- **Version:** version number of the Splashtop On-Prem followed by the build number.
- **Build Time:** the date and time when this release was built.
- **What's new:** The new features and enhancements of this release.
- **Terms of Service:** terms and conditions of your use of Splashtop's Services between 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, 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 users are not allowed to access the management console, so Management and Settings tab will not appear in the menu.

In this example, team owner and admin can see below items in Management context menu: Users, All Computers, All Devices, Grouping, Deployment, Preference Policy, 1-to-Many Actions, 1-to-Many Schedules, Channels, and Inventory.

Team owner exclusive management scope including: Settings – Team settings, Authentication, Email, Syslog, and API.

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**
- **Preference Policy**
- **1-to-Many Actions**
- **1-to-Many Schedules**
- **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**.

Users

Add
Bulk Actions
Only show selected

Add
Local User
AD User/Group
SSO User
Import
Local Users
AD Users
SSO Users

Status
Web Access
User SOS Status
More Filters

Role ↑	Source	Display Name	Group	Last Login	
Owner	Local		Default Group	2024-08-20 16:04:34	
Admin	AD Group Member (Member of...		Alpha Corp, Default Gr...	2024-07-15 11:09:25	
Admin	Local		Gamma Industries		
Admin	Local		Alpha Corp	2024-08-20 16:06:14	

Create local account

Add User

* Account

user@example.com

* Password

Password, minimum 8

* Confirm Password

Password, minimum 8

☐ Request to change password when next login

Group

Default Group

Role

Member

Status

☒ Enable user

☒ Enable web access

SOS Technician

☐ Enable SOS/On-Demand support

Password must include:

- At least 8 characters
- At least 1 lowercase Latin letter (a-z), 1 uppercase Latin letter (A-Z) and 1 number
- At least 1 special character ~!@#\$%^&*_{+~|`~"~'~<~>~/\[]
- No match of the account name

Cancel

Add

<i>Field</i>	<i>Meaning</i>
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 user	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.
Enable web access	Disable this option will disable the web access for this account.
SOS Technician*	If SOS service is included in your subscription, you can enable SOS capability when create a user to have on-demand support available.

Add AD account

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

Add AD User/Group

Type

AD User

AD Server

CBK (dc=belle, dc=epoque)

* Account

User account to login

Verify

@belle.epoque

@belle.epoque ✓

@example.com

@test.com

@k.com

@m1.com

@outlook.com

Group

Default Group

Role

Member

Status

☒ Enable User

☒ Enable web access

SOS Technician

☐ Enable SOS/On-Demand support

Cancel

Add

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.
Add	Add a validated AD user or group to the target group.

Ad 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.

Users

☐ Only show selected

☐	Account	Role	Group	AD Group Member (Member of Remote Support / CBK)	Name	
☐	jack.doe@test.com	Member	Default Group	AD Group Member (Memb...		
☐	diane.xiong@k.com	Member	Default Group	AD Group Member (Memb...		

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.

Users

☐ Only show selected

Add

Local User

AD User/Group

SSO User

Import

Local Users

AD Users

SSO Users

	Role ↑	Source	Display Name
	Owner	Local	
	Member	Local	
	Member	Local	
	Member	Local	

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.

Import Users ✕

Upload CSV file

Download template

Select file

Drag and drop file here to upload

Group

Default Group

Email notification

☐ Enable email notification

Status

☒ Enable users

☒ Enable web access

SOS Technician

☐ Enable SOS/On-Demand support

You have successfully imported 1 users at 2024-07-23 17:11:59. Visit the [last imported report](#).

Cancel

Import

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.

Import AD Users ✕

Authentication

CBK (dc=belle, dc=epoque) ▼

*Upload CSV file

[Download template](#)

Select file

Drag and drop file here to upload

Group

Default Group ▼

Email notification

☐ Enable email notification

Status

☒ Enable users

☒ Enable web access

SOS Technician

☐ Enable SOS/On-Demand support

Cancel

Import

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.

Import Users Report



 Please download the imported report to get the **one-time password** for each imported users after the import is completed. The one-time password only can be used within 7 days.

Account ↑	Status
[REDACTED]	✓ Success
[REDACTED]	✓ Success
[REDACTED]	✓ Success
[REDACTED]	✓ Success
[REDACTED]	✓ Success
[REDACTED]	✓ Success

12 Completed 0 Failed

Close

Download 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

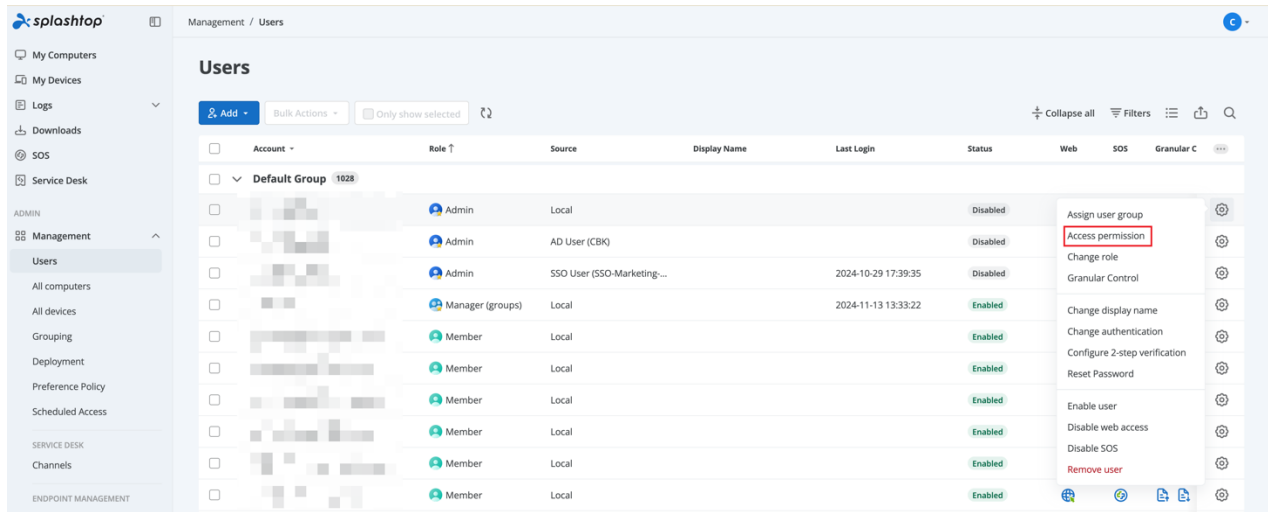
Where to configure access permissions

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).



Users

Account Role Source Display Name Last Login Status Web SOS Granular Control

Default Group 1628

Account	Role	Source	Display Name	Last Login	Status	Web	SOS	Granular Control
[Redacted]	Admin	Local			Disabled			
[Redacted]	Admin	AD User (CBK)			Disabled			
[Redacted]	Admin	SSO User (SSO-Marketing-...		2024-10-29 17:39:35	Disabled			
[Redacted]	Manager (groups)	Local		2024-11-13 13:33:22	Enabled			
[Redacted]	Member	Local			Enabled			
[Redacted]	Member	Local			Enabled			
[Redacted]	Member	Local			Enabled			
[Redacted]	Member	Local			Enabled			
[Redacted]	Member	Local			Enabled			
[Redacted]	Member	Local			Enabled			
[Redacted]	Member	Local			Enabled			

Context Menu Options:

- Assign user group
- Access permission
- Change role
- Granular Control
- Change display name
- Change authentication
- Configure 2-step verification
- Reset Password
- Enable user
- Disable web access
- Disable SOS
- Remove user

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)

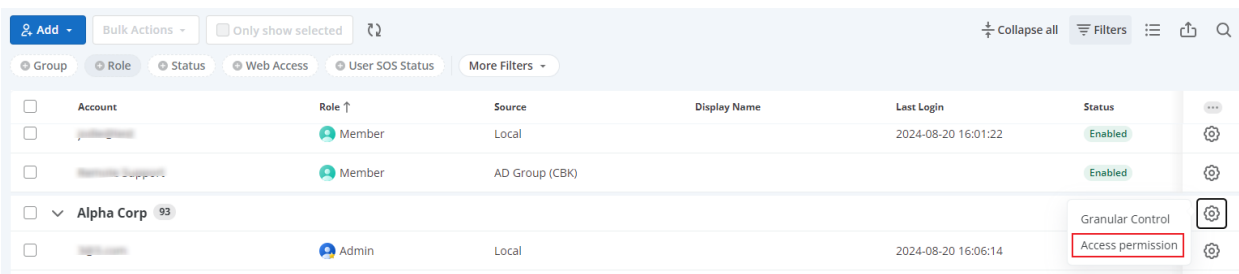
Option 5 - Only specific computers and computer groups

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.



Account	Role ↑	Source	Display Name	Last Login	Status	
☐ jsmith@alpha.com	Member	Local		2024-08-20 16:01:22	Enabled	
☐ jsmith@alpha.com	Member	AD Group (CBK)			Enabled	
☒ Alpha Corp 93						
☐ jsmith@alpha.com	Admin	Local		2024-08-20 16:06:14		Granular Control Access permission

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

Group Access Permission

Admins can grant users/user groups access to computers/computer groups. Users in this group **Accounting** who are configured to follow the group's access permissions can access:

- ☐ No computers
- ☒ Only computers in its group
- ☐ Only specific computers and computer groups

Updating access permissions via CSV

The CSV upload feature allows administrators to efficiently manage access permissions for users and groups by:

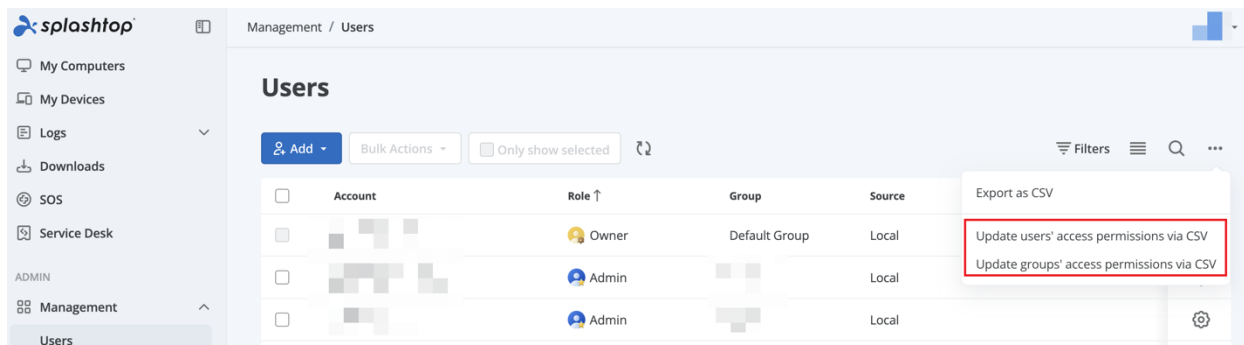
1. Exporting current permissions to a CSV file.
2. Editing the exported file to update access permissions.
3. Re-uploading the edited CSV file to apply changes.

This functionality supports bulk updates, validation, and detailed reporting to ensure accurate permission management.

Steps to Update Access Permissions

1. Access the CSV Update Feature

- Navigate to the **Management** section in the Splashtop web console.
- Select **Update Users' Access Permissions via CSV** or **Update Groups' Access Permissions via CSV**, depending on your needs.



2. Download the Preformatted CSV File

- In the **Preparations** step, download the relevant files:
 - **Users' Access Permissions CSV**
 - **All Computers CSV**
 - **All Groups CSV**
- Use these files to ensure proper formatting and references when editing permissions.

1 Preparations

- 1) Review the instructions before editing the access permission CSV file. [Instructions](#)
- 2) Export the pre-formatted Access Permissions list for modification. Use only the exported file to ensure proper formatting.

Export Users' access permissions
- 3) Download the Computer list to assign computers to users or groups by UUID. [Download All Computers CSV.](#)
- 4) Download the Group list to assign computer groups to users or groups by Group Name. [Download All Groups CSV.](#)

3. Edit the CSV File

- Open the downloaded CSV file using a spreadsheet editor.
- Update the following fields as needed:
 - **Access Permission:** Set values (1–5) based on the access type.
 - **Assigned Computer ID and Assigned Computer Group Name:** Specify unique identifiers for computers or groups (if Access Permission = 5).

Validation Rules:

- Ensure no conflicting permissions exist for the same account.
- Follow the predefined formats for each field.

30 # 3. Conflict Handling Rules:

31 # - If multiple rows for the same "Account" have conflicting "Access Permission" values, none of the rows for that account will be processed.

32 # - Example of conflicting permissions:

33 # - Row 1: john.doe@company.com, Access Permission = 1

34 # - Row 2: john.doe@company.com, Access Permission = 5

35 # - Result: Both rows are flagged as conflicts and rejected. Correct and re-upload.

36 # - Rows with duplicate "Assigned Computer ID" or "Assigned Computer Group Name" for the same "Account" are allowed but will be deduplicated automatically during processing.

37 #

38 # 4. Reference Fields (Non-Editable):

39 # - "Computer Name": Provides a readable name for each computer corresponding to "Assigned Computer ID".

40 # - "Host Name": Displays the OS-level host name or IP address of each computer corresponding to "Assigned Computer ID".

41 # - "User Group Name": Specifies the group or department to which the user belongs.

42 #

Splashtop Account	Access Permission	Assigned Computer ID	Assigned Computer Group Name	Assigned Computer Name	Host Name	User Group Name
user01@example.com	1					TestGroup
user02@example.com	2					TestGroup
user03@example.com	3					TestGroup
user04@example.com	4					TestGroup
user05@example.com	5					TestGroup
user05@example.com	5	6596309db2f9148c6548ec73c0e11de6				TestGroup
user06@example.com	5		TestGroup			TestGroup
user06@example.com	5	6596309db2f9148c6548ec73c0e11de6				TestGroup
user06@example.com	5	6c4cab88e453b7648584de9d16045				TestGroup
user06@example.com	5	9feffdea82e192b1f4ad7baa8f0ba19f				TestGroup
user07@example.com	5	9feffdea82e192b1f4ad7baa8f0ba19f				TestGroup

4. Upload the Edited CSV File

- Drag and drop the edited file into the upload area on the **Upload CSV File** page or use the file selector.
- The system will automatically validate the file and generate a pre-validation report.

2 Upload the edited CSV file

User-access-permission_2024-12-19_16-54-50.csv

Select again

Drag and drop file here to upload

✓ The uploaded CSV has been validated. A file with the Validation Result column is ready for download. Review and fix any issues before proceeding with the update. [Download validation results](#)

5. Review Validation Results

- Download the validation report to check for errors.
- Correct any issues highlighted in the report and re-upload the corrected file.

2 Upload the edited CSV file

User-access-permission_2024-12-19_16-54-50.csv

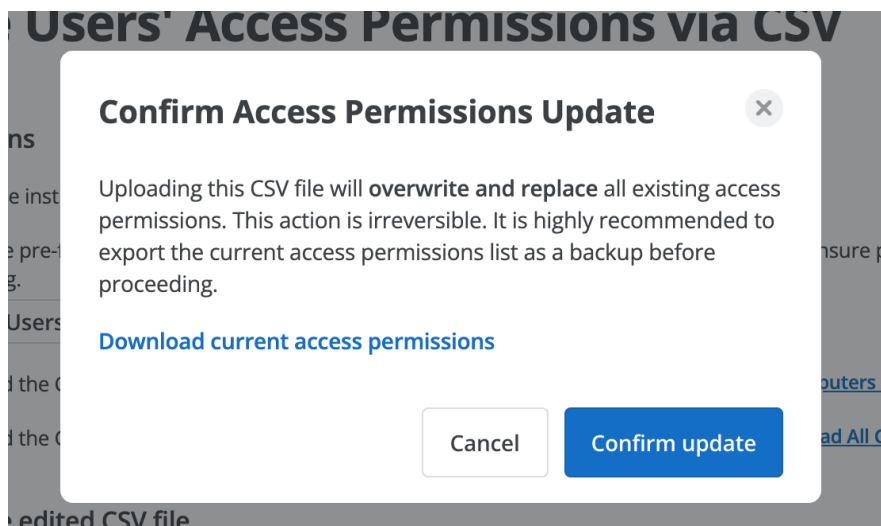
Select again

Drag and drop file here to upload

✓ The uploaded CSV has been validated. A file with the Validation Result column is ready for download. Review and fix any issues before proceeding with the update. [Download validation results](#)

6. Confirm and Apply Updates

- Once the file passes validation, click the **Update** button.
- A confirmation dialog will appear:
 - Review the summary of changes.
 - Confirm the update to proceed.



7. Review Update Summary

- After the update, the system will display a detailed summary of the operation:
 - Number of successful updates.
 - Errors encountered (if any).
- Download the update report for records.

Update Users' Access Permission Report

Row Number	Account	Status
44	user01@example.com	✓ Success
45	user02@example.com	✓ Success
46	user03@example.com	✓ Success
47	user04@example.com	✓ Success
48	user05@example.com	✓ Success
49	user05@example.com	✓ Success
50	user06@example.com	✓ Success
51	user06@example.com	✓ Success
52	user06@example.com	✓ Success
53	user06@example.com	✓ Success
54	user07@example.com	✓ Success

Success: 11, Failure: 0

[Close](#) [Download Report](#)

You have successfully updated 11 users' access permission at 2024-12-19 16:59:53. Visit the [last imported report](#).

Best Practices

- Always export and back up current permissions before making changes.
- Use the preformatted CSV file to minimize errors.
- Validate the file thoroughly before applying updates.

Troubleshooting Common Issues

1. File Validation Errors:

- Check for missing or improperly formatted columns.
- Ensure the file is UTF-8 encoded.

2. Conflicting Permissions:

- Resolve conflicts by ensuring each user/group has a single permission type per row.
3. **Exceeding File Size/Row Limits:**
- Split the file into smaller segments or use filters to reduce the dataset.

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 Settings → Team settings → 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.

Unattended access

		Default Granular Settings		
		Admin / Group manager	Member	Admin configurable ⓘ
File transfer 	Upload	☒	☒	Off ▾
	Download	☒	☒	Off ▾
Text copy and paste 	From local to remote	☒	☒	Off ▾
	From remote to local	☒	☒	Off ▾
Remote print 		☒	☒	Off ▾
Remote command 		☒	☒	Off ▾
Watermark protection Detailed settings 		☒	☒	Off ▾
Request permission to connect ⓘ		☐	☐	Off ▾
Centralized session recording Detailed settings 		☒	☒	Off ▾

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"**.

☐ ▾ Alpha Corp 93									
☐ [User Name]		Admin	Local	2024-08-20 16:06:14	Enabled				
☐ [User Name]		Admin	AD Group (CBK)		Enabled				

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

☐ [User Name]		Owner	Local	2024-08-21 15:57:25	Enabled				
☐ [User Name]		Member	Local	2024-08-08 17:55:50	Enabled				
☐ [User Name]		Member	Local		Enabled				
☐ [User Name]		Member	Local	2024-08-20 16:01:22	Enabled				
☐ [User Name]		Member	AD Group (CBK)		Enabled				
☐ ▾ Alpha Corp 93									

Granular Control

jane.doe@abc.com

Security

Name	Status	Admin configurable ⓘ
Remote control	Default ▾	Default ▾
Require 2-step verification	Default ▴	Default ▾

Unattended Access

Name	Status	Admin configurable ⓘ
File transfer	Default ▴	
Upload	Default ▾	Default ▾
Download	Default ▾	Default ▾
Copy and paste		
From local to remote	Default ▾	Default ▾
From remote to local	Default ▾	Default ▾
Remote print	Default ▾	Default ▾

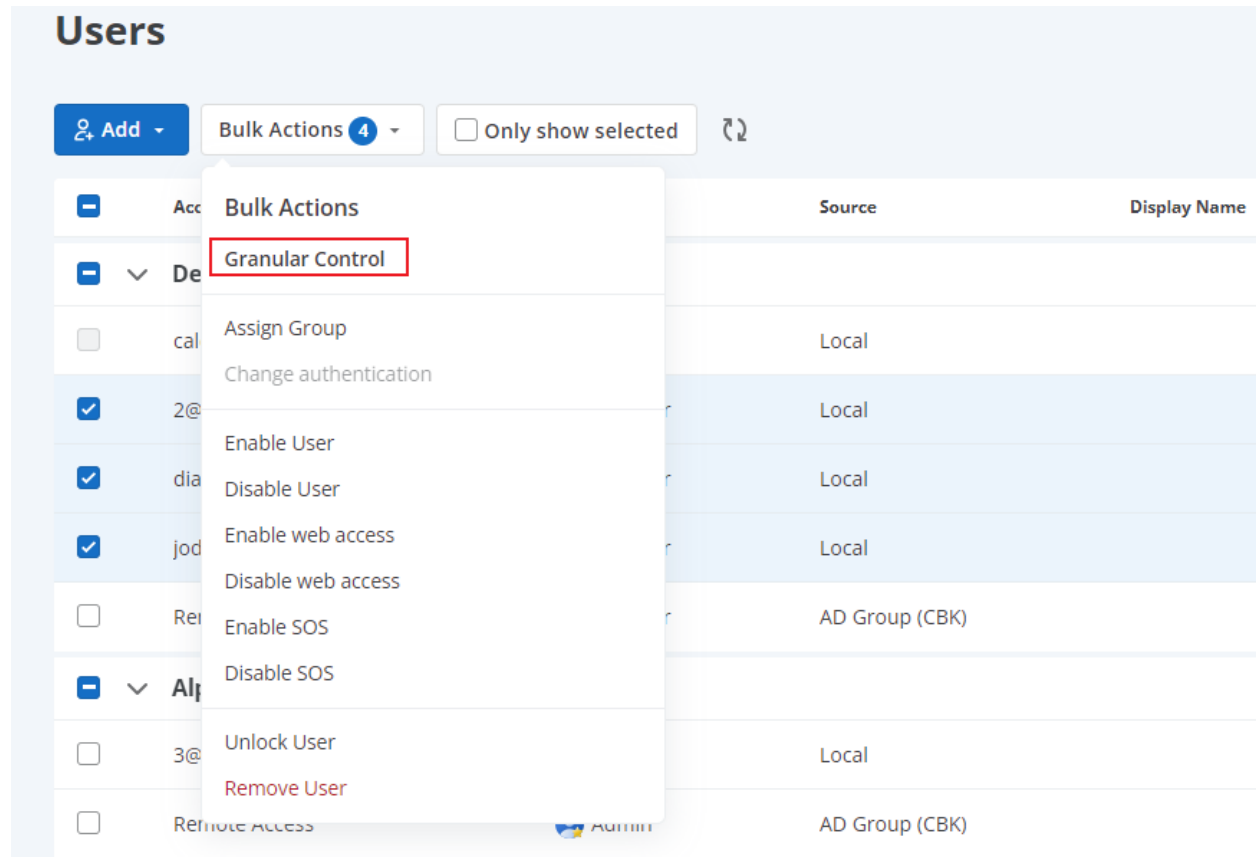
Cancel

Save

- **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 Settings → Team settings → Default Granular 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 Save button to save the settings.



The screenshot shows the 'Users' management page in the Splashtop On-Prem Admin Guide. At the top, there is a blue 'Add' button, a 'Bulk Actions' dropdown menu with a '4' indicator, and a checkbox for 'Only show selected'. Below these is a table with columns for 'Source' and 'Display Name'. A dropdown menu is open from the 'Bulk Actions' button, showing a list of actions: 'Bulk Actions', 'Granular Control' (highlighted with a red box), 'Assign Group', 'Change authentication', 'Enable User', 'Disable User', 'Enable web access', 'Disable web access', 'Enable SOS', 'Disable SOS', 'Unlock User', and 'Remove User' (in red text). The table below the dropdown shows several user entries with checkboxes in the first column and 'Local' or 'AD Group (CBK)' in the 'Source' column.

Granular Control

Security

Name	Status
Remote control	Please select
Require 2-step verification	Please select

Unattended Access

Name	Status
File transfer	
Upload	Please select
Download	Please select
Copy and paste	
From local to remote	Please select
From remote to local	Please select
Remote print	Please select
Remote command	Please select

Cancel

Save

Set admin rights

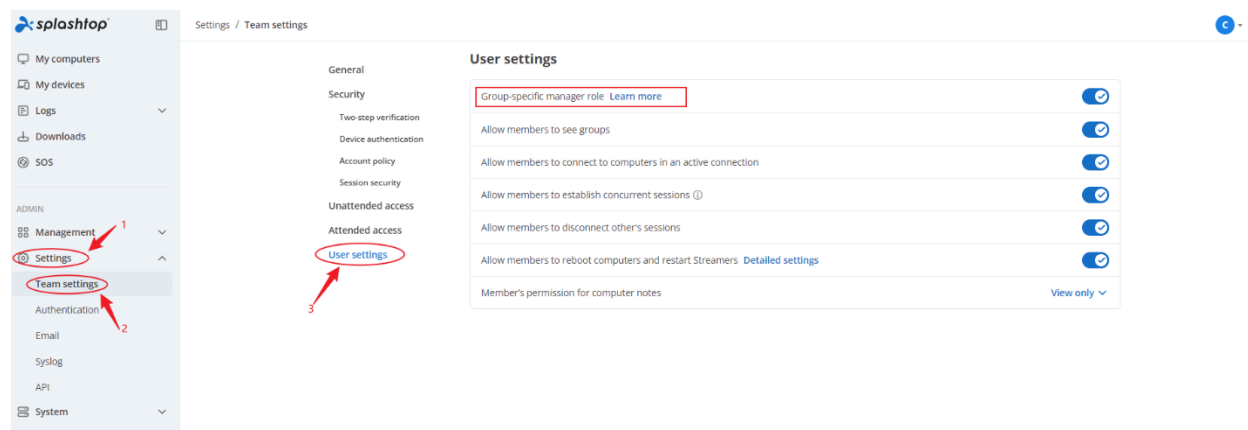
On Splashtop On-Prem, an Admin user can remotely access and **manage all computers by default**.

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 Settings> Team settings> User settings. 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."

☐	Account	Role ↑	Source	Display Name	Last Login	Status	Assign user group	...
☐	[redacted]	Member	Local		2024-08-20 16:01:22	Enabled	Access permission	⚙️
☐	[redacted]	Member	AD Group (CBK)			Enabled	Change role	⚙️
							Granular Control	⚙️

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

Change Role

jodie@test

Admin Member

☐ Set as group-specific manager instead of regular admin

User access permission to computers will not be altered by role change. You can fine tune the "Access permission" later to the new role.

Cancel Save

Another way to assign group-specific managers

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

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

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

Grouping

Group your users and computers for easier management. Use computer groups to better organize your computer list. Use user groups to easily control access permissions for multiple users. [Learn more](#) about grouping.

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

[+ Add Group](#)

Group ↑	Number of Group Managers	Number of Users	Number of Computers	Number of enabled user limits
Accounting	0	14	0	—
Africa111	0	0	0	—
Alpha Corp	2	93	0	—
Analysts	0	0	0	—

Edit group
Assign user
Assign group manager
Assign computer
Remove 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

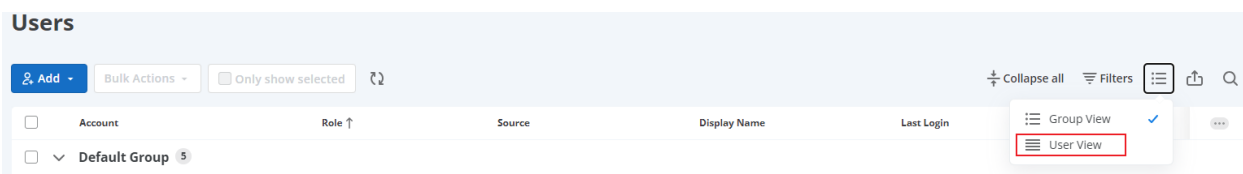
- Add/edit computer notes
- Add/delete computers, including create deployment packages
- Create/enable/disable/delete users
- Set access permissions
- Configure user's 2FA (aka. MFA) and trusted devices

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.

☐		Admin	AD Group Member (Memb...	2024-10-24 10:14:05	Enabled				
☐		Admin	AD User (123)	2024-10-23 18:41:52	Enabled				
☐		Admin	AD Group (123)		Enabled				
☐		Admin	AD User (123)		Enabled				
☐		Member	AD Group Member (Memb...	2024-10-24 10:50:11	Enabled				
☐		Member	AD Group (245555)		Enabled				
☐		Member	AD Group (245555)		Enabled				
☐		Member	AD User (245555)	2024-10-23 16:58:00	Enabled				

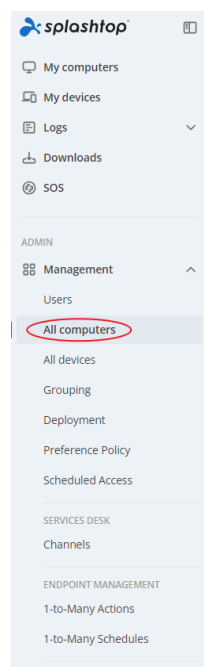
Note: Because a single AD group member can exist in different AD groups at the same time, the granular control settings for AD group member will be the merged results from those AD groups, it is not supported to configure these settings right from a single AD group member.

Export user list or access permission list

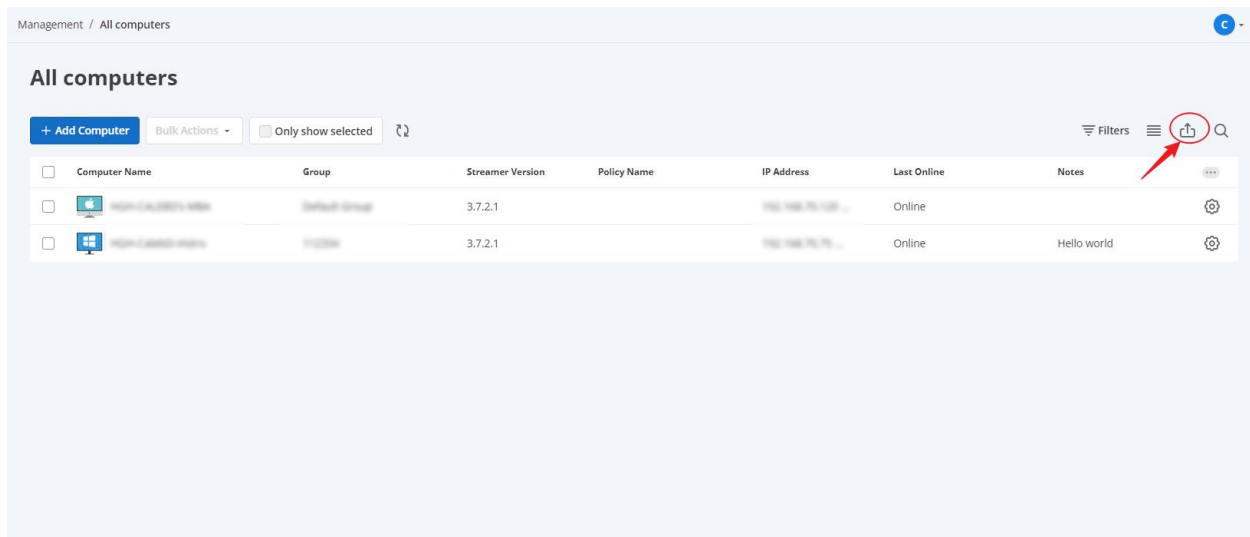
When you are managing several users on your team, you may want to export the user list or access permissions to maintain a record. The user list and access permissions can be exported as a CSV file.

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

Super Admin

Starting with Gateway version 3.40.0, we have introduced the Super Admin feature, which provides your organization with more flexible permission management and enhanced system control capabilities. This article will guide you through configuring Super Admin, understanding the differences in permissions, and following best practices.

How to Promote a User to Super Admin

1. Log in to your Gateway as the Team Owner.
2. Go to **Management > Users**.
3. Click the **Gear icon** of the user profile you would like to modify.
4. Select **Change role**.
5. Select **Super Admin** as the user's role from the dropdown menu, then select **at least one permission** to save the settings.

Change role ✕



Role

 Super Admin ▼

☒ Grant permission to have full control over all admins

☒ Grant permission to manage team policies and settings

Select at least one permission for the super admin to save the settings.

A Super Admin has all Admin permissions by default, along with the ability to configure additional privileges.

Cancel

Save

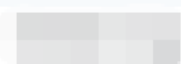
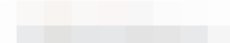
After completing the above configuration, you can see the user's role has been changed to Super Admin in the user list.

Users

 Add ▼

Bulk Actions ▼

☐ Only show selected 

☐	Account ▼	Role ↑
☐	 4	
☐		 Owner
☐		 Super Admin
☐		 Member
☐		 Member

What can a Super Admin do?

A Super Admin has all the permissions of a regular Admin, plus two additional configurable privileges:

1. Grant permission to have full control over all admins

This permission grants the Super Admin full authority to manage all administrative users across the organization, including both Admins and Group Managers.

When enabled, the Super Admin can:

- Change the role of existing Admins or Group Managers.
- Remove (delete) Admins or Group Managers from Gateway.
- Assign the Admin or Group Manager role to members.
- Reset passwords for any Admin or Group Manager.

2. Grant permission to manage team policies and settings

This permission allows the Super Admin to configure organization-wide policies and settings at the team level.

When enabled, the Super Admin can:

- Modify settings within the **Team Settings** interface.
- Configure the **Authentication** interface, including **Single Sign-On (SSO)** and **AD Authentication**.

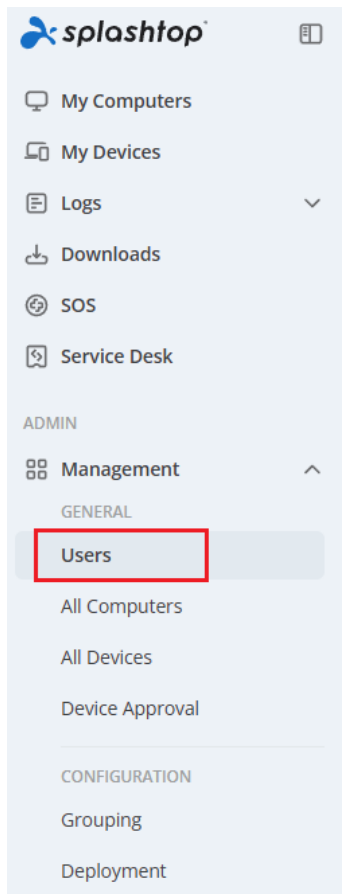
Grant/Revoke System Management

System Owner can grant or revoke system management permissions for other users. Users with system management permissions can view and configure system-level settings in the web portal.

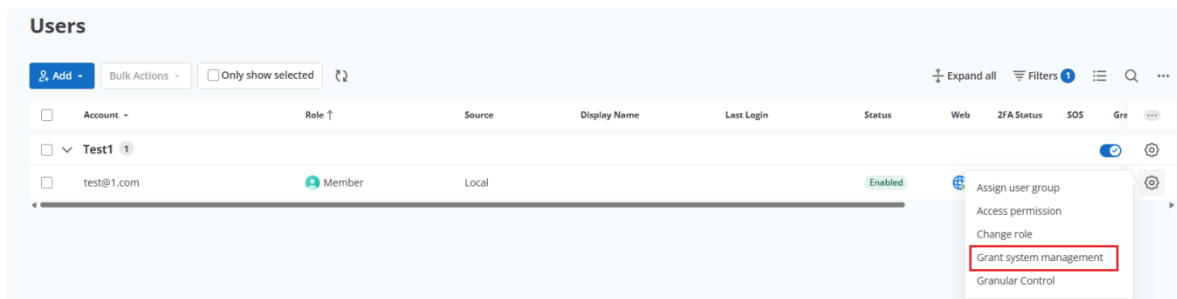
This article explains how to grant and revoke System Management permissions, what access changes for affected users, and security best practices.

How to grant system management

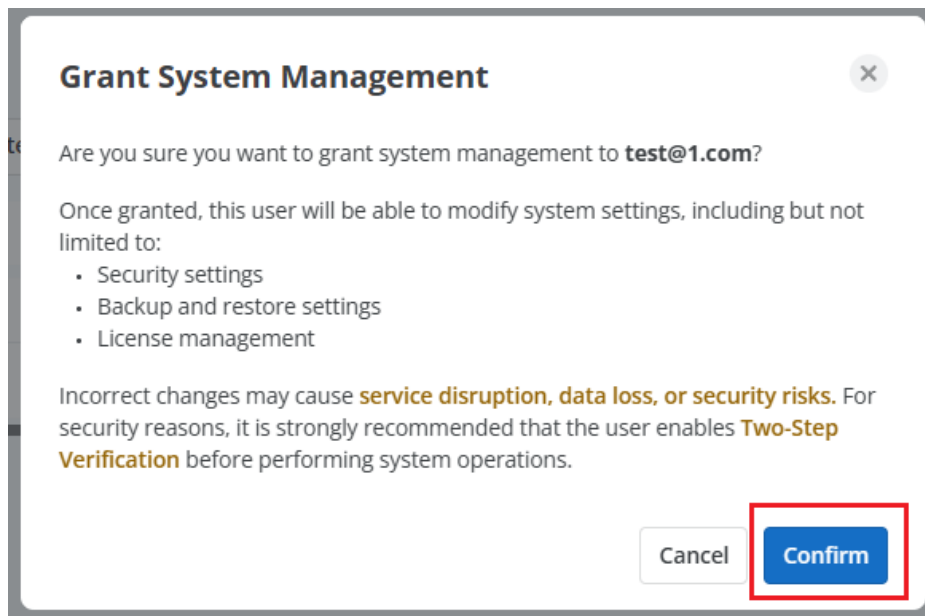
1. Log in to Gateway web console and navigate to **Management > Users**.



2. Locate the user you want to update.
3. Click the gear button and find the "Grant system management" option for that user.

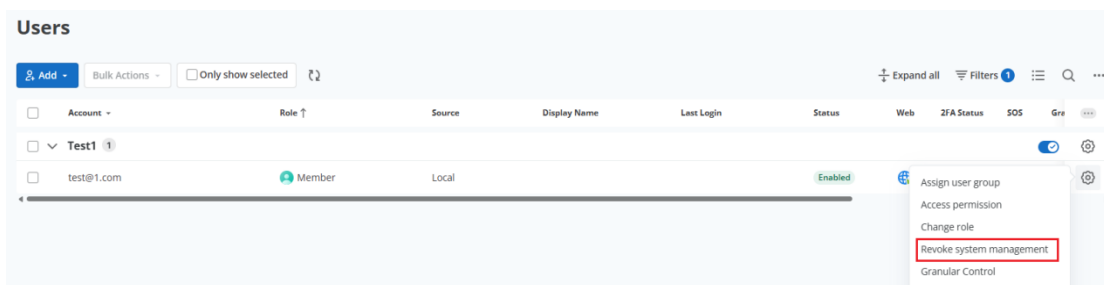


4. Click the option and confirm the change in the confirmation dialog.

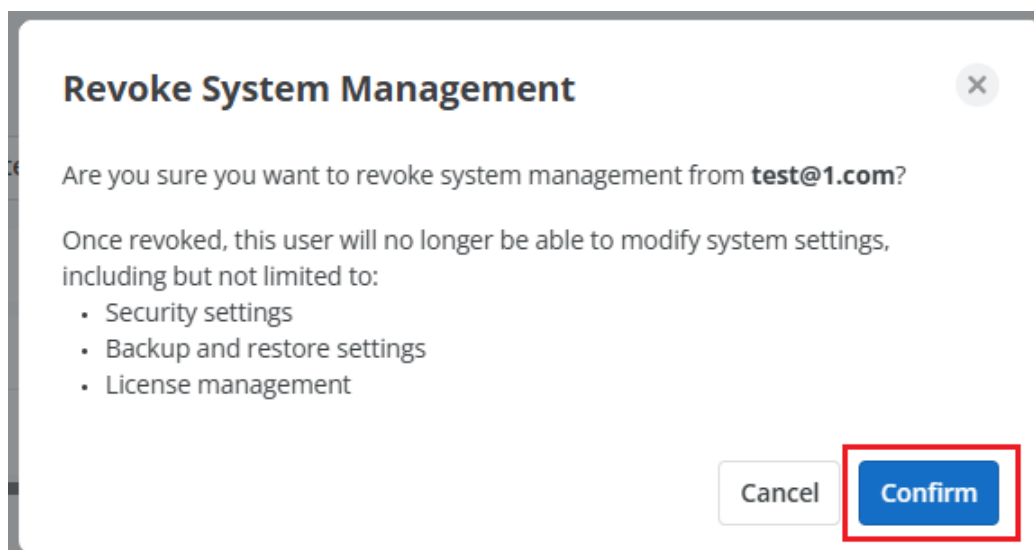


How to revoke system management

1. Log in to Gateway web console and navigate to **Management > Users**.
2. Locate the user who is granted system management.
3. Click the gear button and find the "Revoke system management" option for that user.



4. Click the option and confirm the change in the confirmation dialog.



What system management permissions include

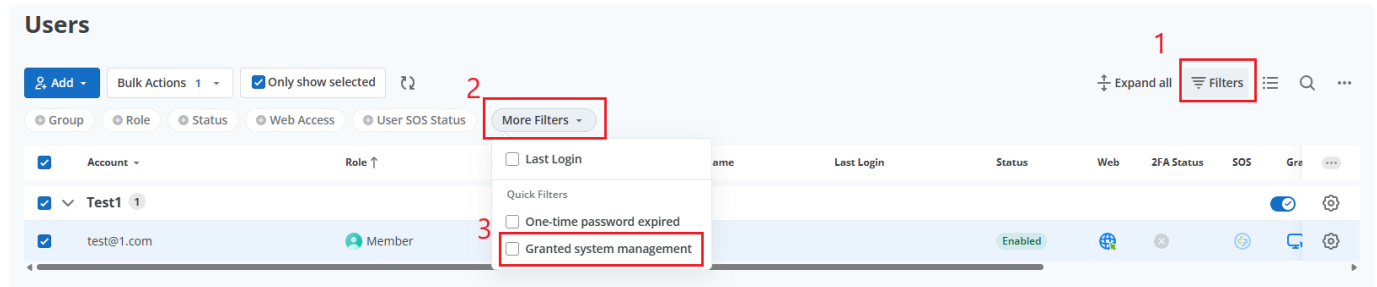
Once granted system management, a user can access system-related settings pages in the web portal and modify system-level configurations, including but not limited to:

- Security settings
- Backup and restore settings
- License management
- System monitoring
- Network settings
- SMTP settings
- Syslog settings, etc.

Users without system management will not see system-related pages or settings in the web portal.

Quick filter

The system owner can view the users who have been granted system management by filtering.



Security best practices

Because the system management grants access to critical system configurations, we strongly recommend the following for all users with this permission:

- **Enable 2FA:** Users with system management should have Two-Factor Authentication enabled on their accounts. This adds an extra layer of protection in case credentials are compromised.
- **Limit access:** Only grant system management to users who genuinely need it. Regularly review the **User Management** page to ensure permissions remain appropriate.
- **Revoke promptly:** If a user no longer requires system access (e.g., role change, offboarding), revoke the permission immediately.

Note: This feature is available from Gateway v3.40.1 and later.

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.

Management / All computers C

All computers

[+ Add Computer](#) [Bulk Actions](#) ☐ Only show selected [↻](#)

[Filters](#) [≡](#) [📄](#) [🔍](#)

☐	Computer Name	Group	Streamer Version	Policy Name	IP Address	Last Online	Notes	⋮
☐	 192.168.1.100	Default Group	3.7.2.1		192.168.1.100	Online		
☐	 192.168.1.101	112334	3.7.2.1		192.168.1.101	Online	Hello world	

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.

Management / All computers C

All computers

[+ Add Computer](#) [Bulk Actions](#) ☐ Only show selected [↻](#)

[Filters](#) [≡](#) [📄](#) [🔍](#)

☐	Computer Name	Group	Streamer Version	Policy Name	IP Address	Last Online	Notes	⋮
☐	 192.168.1.100	Default Group	3.7.2.1		192.168.1.100	Online		
☐	 192.168.1.101	112334	3.7.2.1		192.168.1.101	Online		

Reboot computer >

Rename computer

Assign computer group

System inventory

See user list

Add notes

Properties

Remove computer

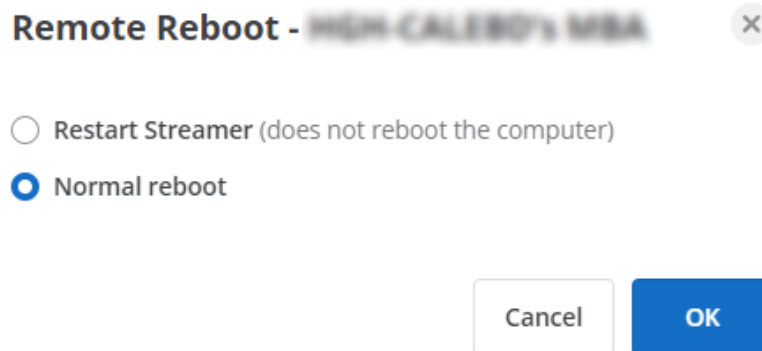
Functions include:

- Reboot computer
- Delete computer

- Rename computer
- Assign computer group
- Add notes
- System inventory
- See user list
- See properties

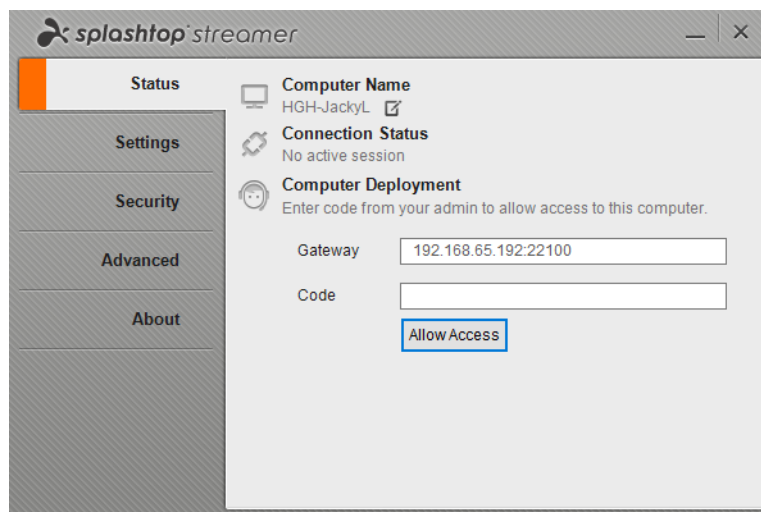
Reboot computer

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.

Rename Computer

This name will be displayed in the computer list. It will not change the OS hostname.

New Name

HGH-CALEBD's MBA 18/200

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

Cancel

Save

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.

User list



The users who have access to HGH-CALEBD's MBA

- AD/SSO group members will not be displayed.
- On [Users](#) page, you can change the access permission.

Role ↑	Account	User Group
 Admin	admin@hghlebd.com	Developers
 Manager (groups)	group@hghlebd.com	112334
 Member	hgh-admin	Developers
 Member	john@hghlebd.com	Default Group
 Member	Remote Support	Default Group
 Owner	calebd@hghlebd.com	Default Group

 6 Users

Close

See properties

This page displayed the properties of the computer.

Computer info

Computer Name
HGH-CalebD-Vistro 

Device Name
HGH-CalebD-Vistro

Streamer Version
3.7.2.1

OS Version
Windows 10 Pro 64-bit 22H2 (10.0.19045.5011)

WAN IP Address 


LAN IP Address


Status
Online since 2024-10-25 09:22
The computer has no user activity for 17 minutes

Last Session
From 2024-09-27 10:38:29 to 2024-09-27 10:40:24 by user caleb@sop.com from device Web Client

Group
112334 

[Update group](#)

Notes
Hello world 

[Update notes](#)

Remove computer

This will permanently remove "HGH-CalebD-Vistro" from this team, and the action cannot be undone.

[Remove this computer](#)

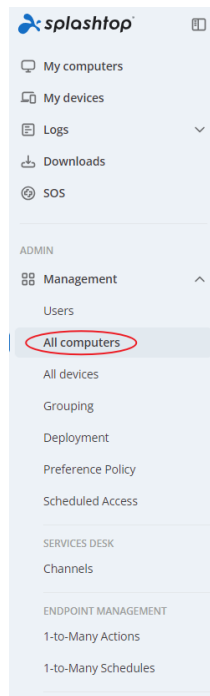
Copyright © 2010 - 2024 Splashtop Inc.

Export and save a copy/record of the computer list

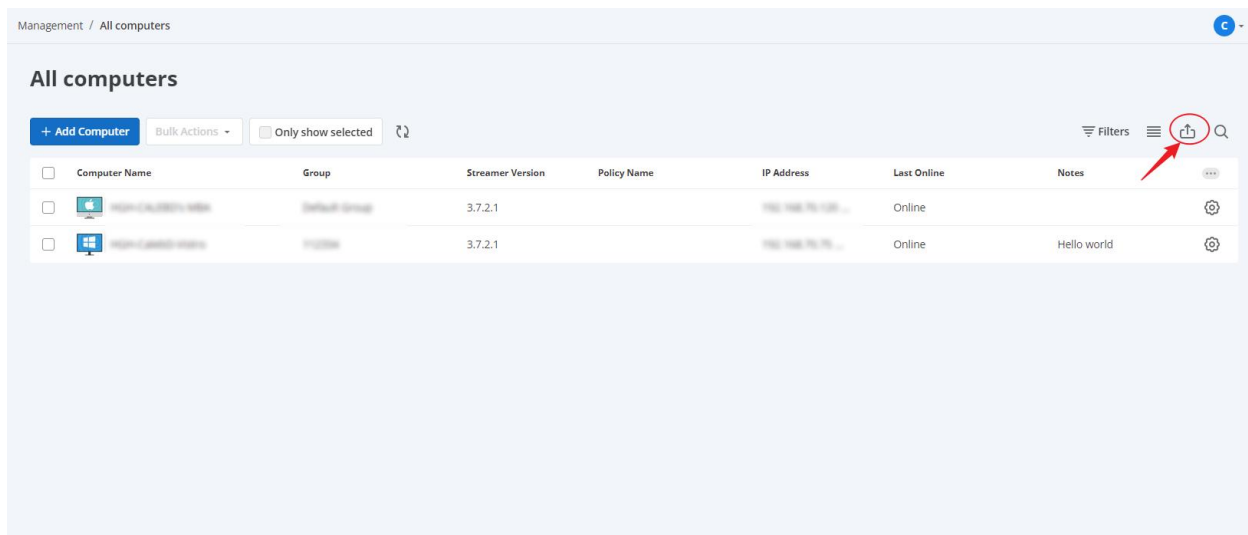
When you are managing several computers on your team, you may want to export the computer list to maintain a record. The computer list can be exported as a CSV file. The Computer List's CSV file includes Computer Name, Host Name, Group Name, OS, etc.

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.

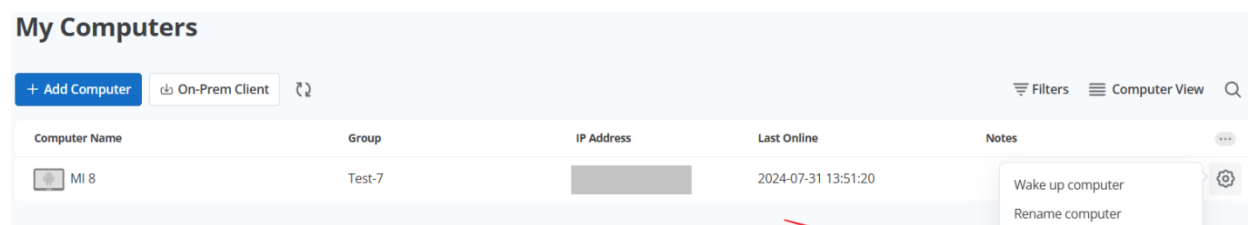
	A	B	C	D	E	F	G
1	Computer Name	Host Name	UUID	Type	Pool Size	Group Name	Operating System
2	rds - 2	rds - 2		RDP		Default Group	Microsoft Windows
3	rdp	rdp		RDP		Default Group	Microsoft Windows
4	rds - 1	rds - 1		RDP		Default Group	Microsoft Windows
5	rdspool	rdspool		RDS pool	2	Default Group	
6	Macmini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

Computer Inventory

System, Hardware, and Software Inventory can be viewed and exported from the web portal.

View Inventory for one computer

Step 1: Log in to Gateway web console and navigate to My Computers or Management -> All Computers. For the computer you want to check System Inventory for, click the gear icon and select System Inventory.



Step 2: Select the action type (View snapshot/Compare snapshot/View changelog) and date for the snapshot that you'd like to check, then click the "Fetch" button. In the right panel, you can also choose different reports for System Inventory: System, Hardware, and Software.

View snapshot:

My Computers / System Inventory

General **Inventory** User list

View the system inventory of [redacted]

Select action

View snapshot

Select snapshots date

2025-10-20

Last Report Time

2025-10-20 03:40:10 +0800

Fetch

System Hardware Software

Manufacturer	Apple Inc.
Model	MacBook Air (M1, 2020)
Serial Number	[redacted]
Motherboard	Chipset N/A Memory Slots 1 SMC Version N/A
Processor	Processor 1 Type Apple M1 Speed N/A Slot 1 Number of cores 8 Number of logical processors 8

Compare snapshot:

My Computers / System Inventory

General **Inventory** User list

View the system inventory of [redacted]

Select action

Compare snapshot

Select Date

2025-10-15 and 2025-10-20

Last Report Time

2025-10-20 03:40:10 +0800

Fetch

System Hardware Software

	2025-10-15	2025-10-20
Manufacturer	Manufacturer Apple Inc.	Manufacturer Apple Inc.
Model	Model MacBook Air (M1, 2020)	Model MacBook Air (M1, 2020)
Serial Number	Serial Number [redacted]	Serial Number [redacted]
Motherboard	Chipset N/A Memory Slots 1 SMC Version N/A	Chipset N/A Memory Slots 1 SMC Version N/A
Processor	Processor 1 Type Apple M1 Speed N/A Slot 1 Number of cores 8 Number of logical processors 8	Processor 1 Type Apple M1 Speed N/A Slot 1 Number of cores 8 Number of logical processors 8

View changelog:

My Computers / System Inventory C

General Inventory User list

View the system inventory of 

Select action
View changelog

Select Date
2025-10-15 and 2025-10-21

Last Report Time
2025-10-20 03:40:10 +0800

Fetch

	2025-10-15	2025-10-16
Drive	Drive 1 Partition 1 Mount Point /System/Volumes/Data Name Data File System APFS * Used Space 204.19 GB * Free Space 40.91 GB Capacity 245.11 GB Partition 2 Mount Point / Name Macintosh HD File System APFS * Used Space 204.19 GB * Free Space 40.91 GB Capacity 245.11 GB	Drive 1 Partition 1 Mount Point /System/Volumes/Data Name Data File System APFS * Used Space 204.07 GB * Free Space 41.04 GB Capacity 245.11 GB Partition 2 Mount Point / Name Macintosh HD File System APFS * Used Space 204.07 GB * Free Space 41.04 GB Capacity 245.11 GB
	2025-10-16	2025-10-17
Drive	Drive 1 Partition 1 Mount Point /System/Volumes/Data Name Data	Drive 1 Partition 1 Mount Point /System/Volumes/Data Name Data

View Inventory for all computers

- As an Owner/Admin/Group Manager, log in to Gateway web console and navigate to *Management -> Computer Inventory*. The list shows the latest computer inventory, which users can view and export.

 Management / Computer Inventory G

My Computers

My Devices

Logs

Downloads

SOS

Service Desk

ADMIN

Management

Users

All Computers

Computer Inventory

All Devices

Computer Inventory

Export

All Groups - Select Date

Computer Name	Group	Report Time	OS Version	Device Name	Manufacturer	Model/Product	
Test2-Mac	Test 5	2025-09-11 12:16:34 +0800	macOS Ventura		Apple Inc.	Mac mini (M1, 2020)	Apple
Test1-Windows	Default Group	2025-09-17 10:09:14 +0800	Windows 11 Enterprise		LENOVO	LNVB161216	AMD Rade

- Clicking on any computer will pop up a full report for that computer.
- Filters are available to help you view specific inventories, including group filter, time filter, column selector, and search.

Computer Inventory

Export 

All Groups ▾ 2025-09-17  

Computer Name	Group	Report Time	OS Version	Device Name	M
Test1-Windows	Default Group	2025-09-17 10:09:14 +0800	Windows 11 Enterprise		LE

Column settings

☒ Computer Name
☒ Report Time
☐ OS Build
☒ Device Name
☒ Model/Product
☒ CPU
☒ Total Free Space (GB)
☒ LAN IP Address
☒ Last Boot Time

☒ Group
☒ OS Version
☐ Architecture
☒ Manufacturer
☐ Serial Number
☒ Total RAM (GB)
☒ Total Storage (GB)
☐ Time Zone
☒ Last Boot Time

- Clicking the "Export" button will pop up a menu where you can export **System/Hardware Inventory** and **Software Inventory** to a CSV file.

Export as CSV

Select export type

- ☒ System / Hardware Inventory
- ☐ Filtered results only
- ☐ Software Inventory

Cancel

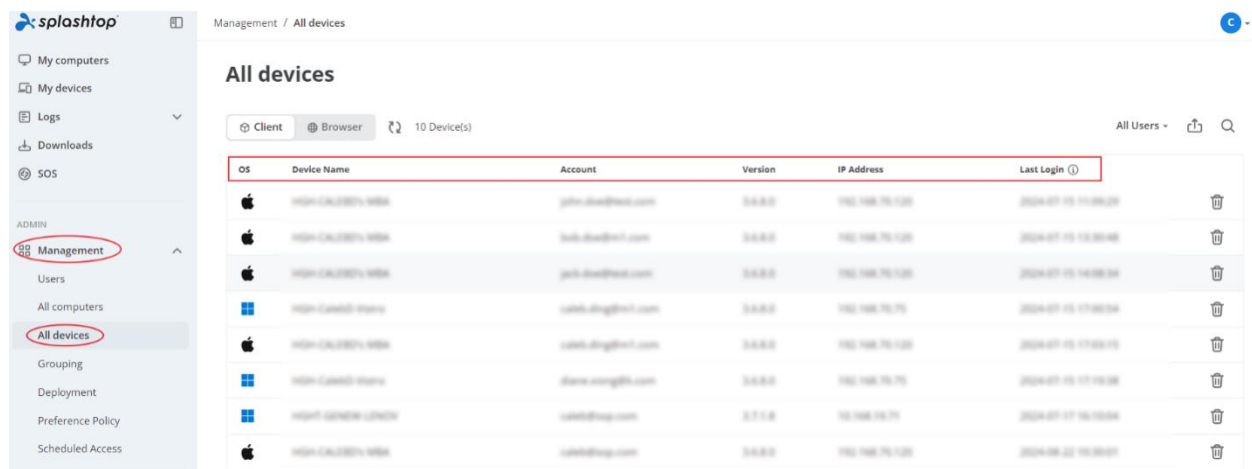
Export

Note: The column selector on the web console does affect the exported CSV file. The CSV file will include all hardware and software columns.

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.



Management / All devices

All devices

Client Browser 10 Device(s)

All Users +

OS	Device Name	Account	Version	IP Address	Last Login	
Apple	iPhone-CAL0001-1000	john.doe@corp.com	3.6.0.0	192.168.75.120	2024-07-15 11:00:20	
Apple	iPhone-CAL0001-1000	jane.doe@corp.com	3.6.0.0	192.168.75.120	2024-07-15 10:00:00	
Apple	iPhone-CAL0001-1000	jane.doe@corp.com	3.6.0.0	192.168.75.120	2024-07-15 10:00:00	
Windows	Win-CAL0001-1000	john.doe@corp.com	3.6.0.0	192.168.75.120	2024-07-15 11:00:20	
Apple	iPhone-CAL0001-1000	john.doe@corp.com	3.6.0.0	192.168.75.120	2024-07-15 11:00:20	
Windows	Win-CAL0001-1000	jane.doe@corp.com	3.6.0.0	192.168.75.120	2024-07-15 11:00:20	
Windows	Win-CAL0001-1000	john.doe@corp.com	3.6.0.0	192.168.75.120	2024-07-15 11:00:20	
Windows	Win-CAL0001-1000	john.doe@corp.com	3.6.0.0	192.168.75.120	2024-07-15 11:00:20	
Windows	Win-CAL0001-1000	john.doe@corp.com	3.6.0.0	192.168.75.120	2024-07-15 11:00:20	
Windows	Win-CAL0001-1000	john.doe@corp.com	3.6.0.0	192.168.75.120	2024-07-15 11:00:20	

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.

Management / Grouping / Add Group

Add Group

Group Name

Group name

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

Connection Pool

☐ Set the group(s) as connection pool

Enabled user limits

☐ Set the number of enabled user limits for the group(s)

Max enabled user (1 ~ 5000)

5000

* By default, all admins have access to all computers unless access permissions are explicitly modified.

Add

Cancel

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

Grouping

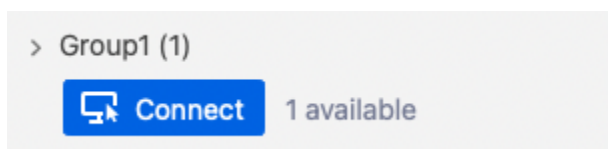
Group your users and computers for easier management. Use computer groups to better organize your computer list. Use user groups to easily control access permissions for multiple users. [Learn more](#) about grouping.

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

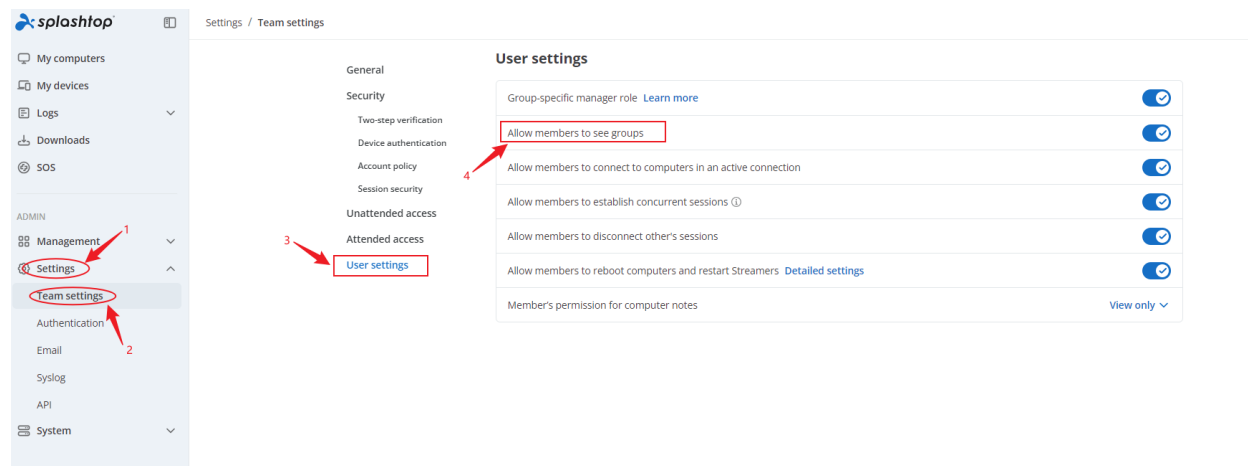
+ Add Group

Group ↑	Number of Group Managers	Number of Users	Number of Computers	Number of enabled user limits	
Accounting	0	100	0	-	Edit group Assign user Assign group manager Assign computer Remove group
HR/Finance	0	0	0	-	
Support Group	2	100	0	-	
Marketing	0	0	0	-	
HR	0	0	0	-	

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



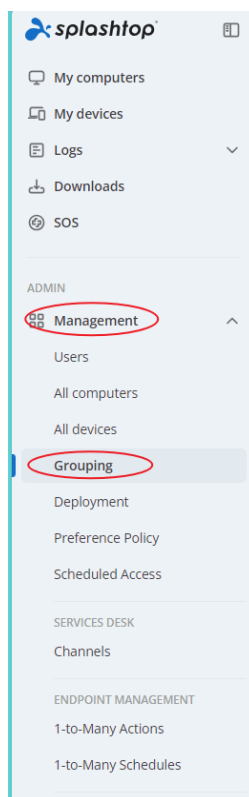
Notice: Please enable Allow members to see groups option in Team settings to make sure user can see the group. (Settings → Team settings → User settings)



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.

Management / Grouping / Edit Group

Edit Group

Group Name Group name
Accounting

Connection Pool ☐ Set the group as connection pool

Enabled user limits ☒ Set the number of enabled user limits for the group(s)
Max enabled user (1 ~ 5000)
5000

* By default, all admins have access to all computers unless access permissions are explicitly modified.

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.

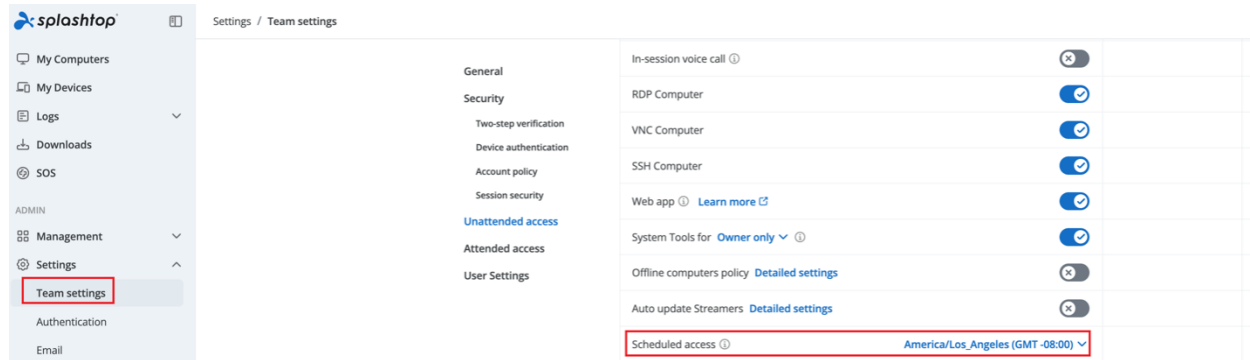
See this article for a few [example scheduling scenarios](#).

Notes and Best Practices

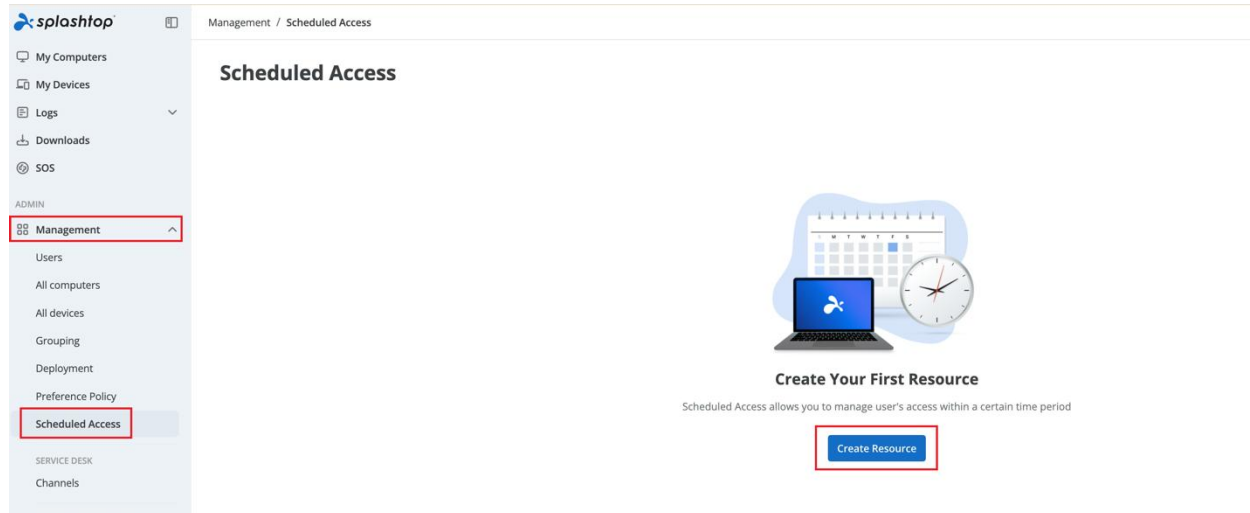
- Scheduled Access are granted in addition to existing user/group permissions that are set under *Management -> Users* - they do ***NOT*** override existing user/group permissions.
- If there are already existing permissions configured under *Management -> Users*, it is recommended to de-associate these 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 *Splashtop web console -> Settings -> Team settings -> Unattended access* 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.

Advanced ^

☒ Support connection pool for schedules ⓘ

☒ Support exclusive (remote or local) access for member accounts ⓘ

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

☐ Set the schedule as connection pool

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

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

☐ Blank screen and lock keyboard/mouse when in a session

☒ Log out user on a disconnect: 1 minute ▾

☒ Lock screen before user logout for unintentional disconnects: Immediately ▾

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

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

Create Resource

General

Resource Name * Add Resource Name

Description (optional) Add Resource description

Resource Status Active ▾

Computers

Add computers to the resource

+ Add Computers

Select Computer

Search

Groups

☐ Only show selected

Alpha Corp (0)

Beta Enterprises (0)

Gamma Industries (0)

Delta Systems (0)

Epsilon Holdings (0)

Zeta Solutions (0)

Eta Technologies (0)

Theta Innovations (0)

Iota Consulting (0)

Kappa Services (0)

Accounting (0)

HR (0)

IT (0)

Marketing (0)

Sales (0)

Customer Support (0)

Research & Development (0)

Computers

☐ Only show selected

> Developers

> Designers

> Analysts

> Technicians

> Support Staff

> Interns

> Meeting Rooms

> Office Equipment

> Vehicles

> Laptops

> Desktops

> Mobile Devices

> Software Licenses

> Network Resources

> Storage Solutions

> Printers

> Project Alpha

0 Group(s) Selected

Clear all

0 Computer(s) Selected

Clear all

Cancel

OK

- (Optional) Assign a [Group Manager](#) to help with managing schedules on the resource.
Group managers also have the capability to create resources and schedules.

Resource Managers (optional) ⓘ

Resource Managers

Assign resource manager(s) to the resource (0 / 1000)

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

© 2010-2026 Splashtop Inc. Splashtop and the logo are registered trademarks of Splashtop Inc. in the U.S. and elsewhere. All other trademarks, product and company names, and logos are the property of their respective owners.

Page 142 of 348

Scheduled Access

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

[+ Create Resource](#) 

Resource Name	Computer	Owned by Resource Manager	Created at	Updated at ↓	
Resource 1	Computer 1	Owner 1	2024-07-28 10:00:00	2024-08-10 10:00:00	Manage Schedule Edit Remove 
Resource 2	Computer 2	Owner 2	2024-07-28 10:00:00	2024-07-28 10:00:00	
Resource 3	Computer 3	Owner 3	2024-07-28 10:00:00	2024-07-28 10:00:00	

Management > Scheduled Access > Rt222

[Create Schedule](#) < > **August 2024**  

Month Week Day

Sun	Mon	Tue	Wed	Thu	Fri	Sat	Wednesday, Aug 28
28	29	30	31	1	2	3	
4	5	6	7	8	9	10	
11	12	13	14	15	16	17	
18	19 00:00 fewafew	20	21	22	23	24	
25	26	27	28	29	30	31	
1	2	3	4	5	6	7	

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

×

Schedule Name *

🕒

Select Date *

📅

00:00

🕒

-

23:59

🕒

Time zone

🔄

Never

▼

👥

Associate groups to the schedule (optional) (0 / 250) ⓘ

👤

Associate users to the schedule (optional) (0 / 1000) ⓘ

👤

Assign a Schedule Manager to the schedule (optional) ⓘ

🔗

Force session to disconnect when schedule ends ☒

Notify users before session ends:

3 minutes ▼

≡

Add Description

Cancel

Create

Repeat ×

Repeat on:

Sun

Mon

Tue

Wed

Thu

Fri

Sat

End Time:

☒ Never End

☐ To

Select Date

📅

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

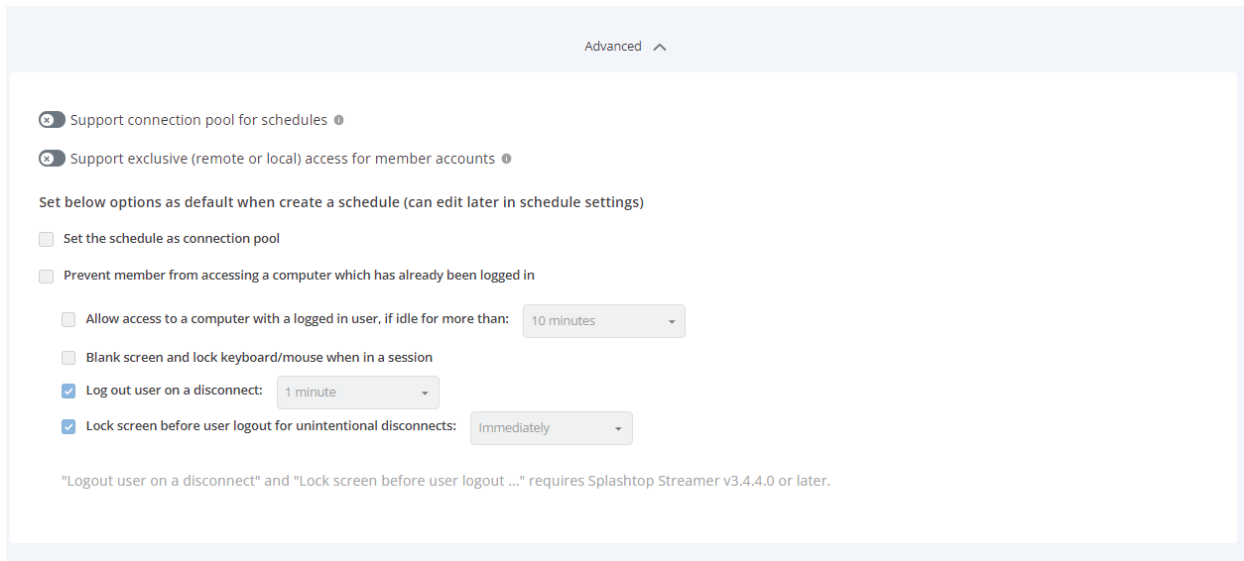
Cancel

Done

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

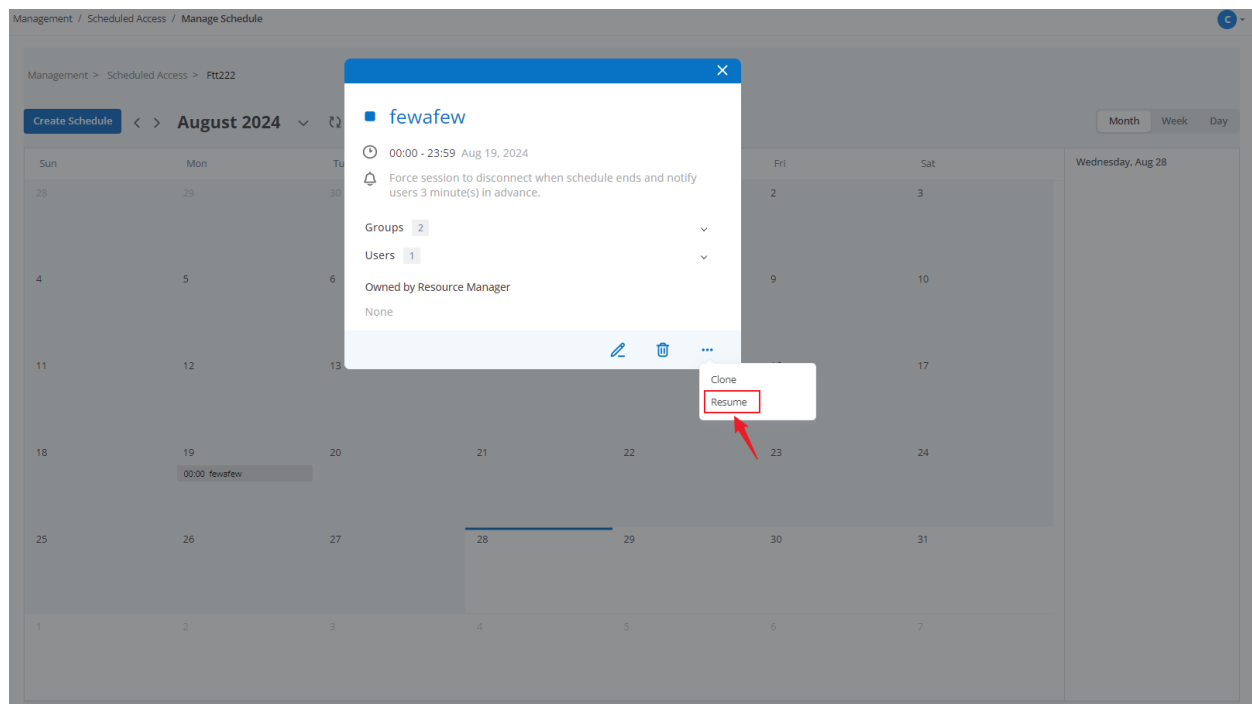
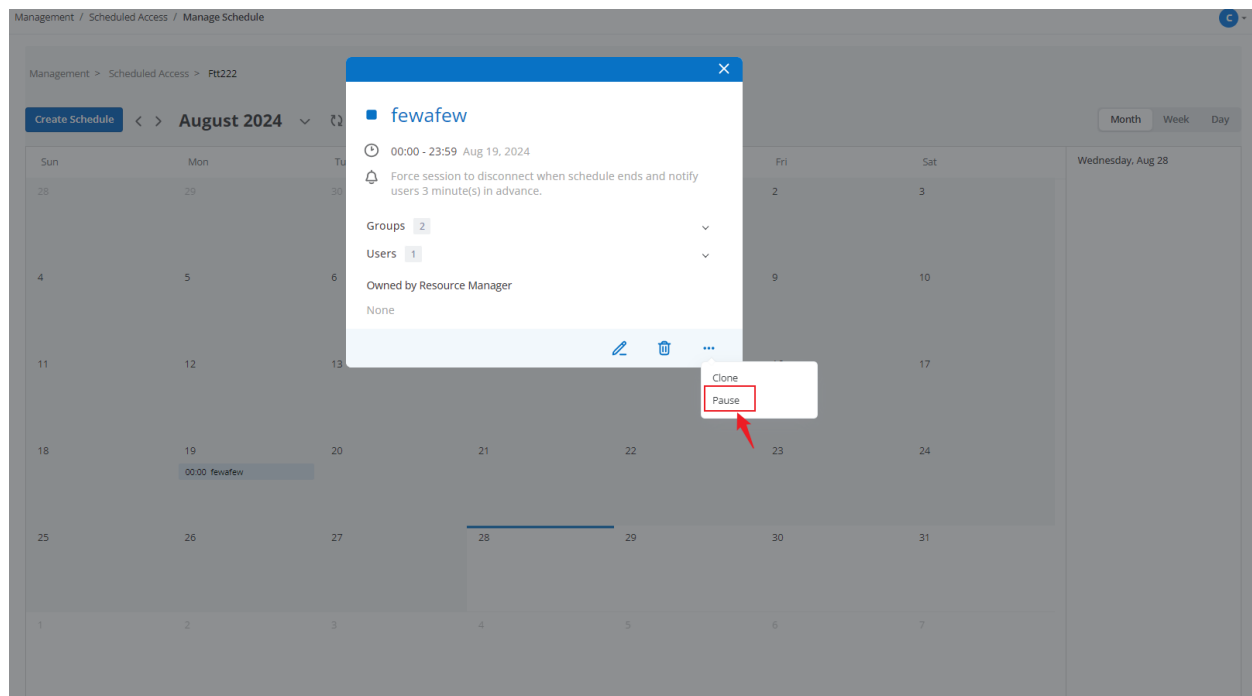


The screenshot shows the 'Advanced' settings tab in the Splashtop admin interface. It contains several toggle switches and dropdown menus for configuring session behavior. The 'Support exclusive (remote or local) access for member accounts' toggle is turned on. Below this, there are instructions to set default options when creating a schedule. The 'Set the schedule as connection pool' and 'Prevent member from accessing a computer which has already been logged in' toggles are turned off. The 'Allow access to a computer with a logged in user, if idle for more than:' dropdown is set to '10 minutes'. The 'Blank screen and lock keyboard/mouse when in a session' toggle is turned off. The 'Log out user on a disconnect:' dropdown is set to '1 minute' and is checked. The 'Lock screen before user logout for unintentional disconnects:' dropdown is set to 'Immediately' and is checked. A note at the bottom states: '"Logout user on a disconnect" and "Lock screen before user logout ..." requires Splashtop Streamer v3.4.4.0 or later.'

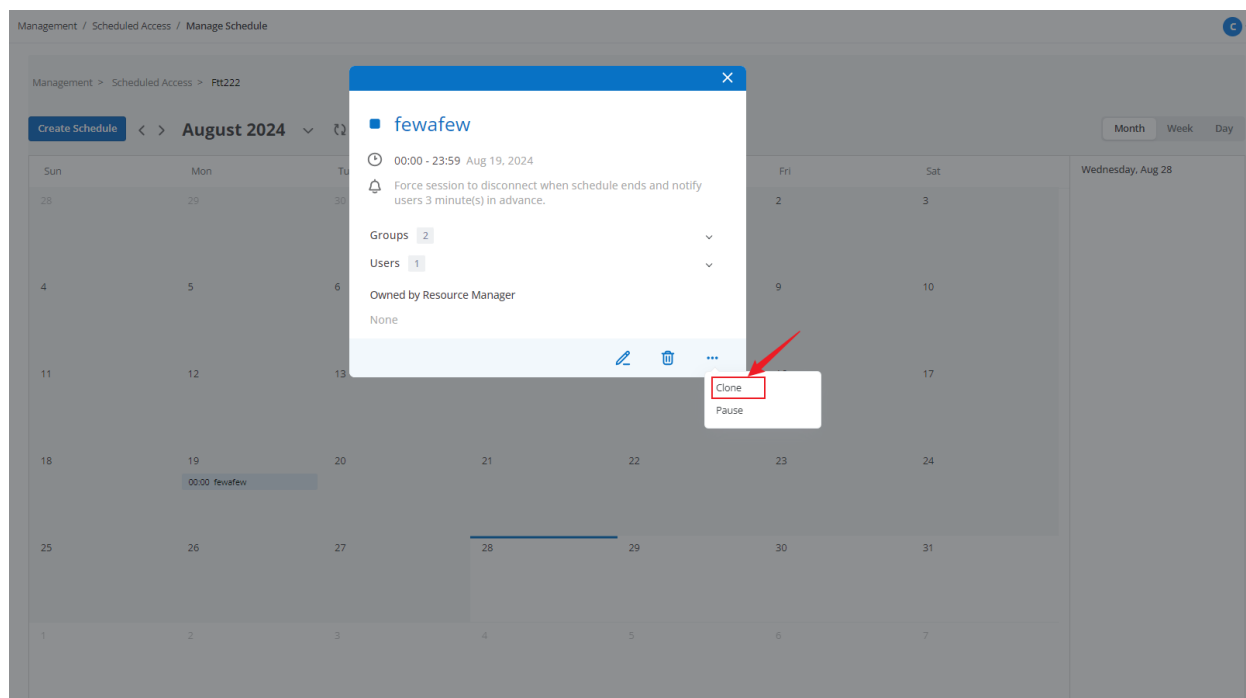
Allows computers that are part of this schedule to be accessed only if the computer is currently at the Windows/Mac Login screen, making the computer exclusive for the user that is currently logged in to the Operating system using the computer. Applies for users either present at the lab or remotely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

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

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



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



Service Desk

Service Desk - Channel

Overview

The Service Desk - Channel feature in Splashtop On-Prem simplifies IT support by organizing support sessions into manageable channels.

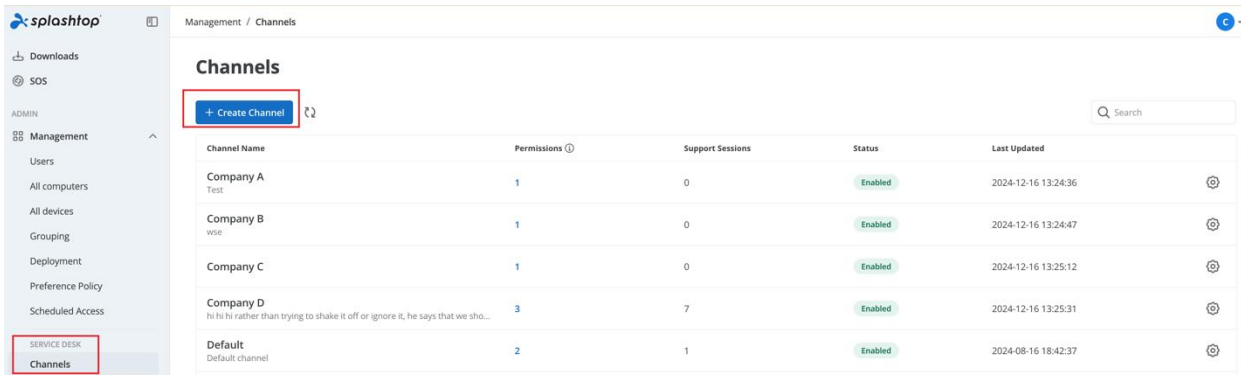
Features of Service Desk - Channel

1. Channel Management:
 - a. Create and edit channels for organized support.
 - b. Associate technicians and groups with channels.
 - c. Enable granular permissions for each channel.
2. Permissions and Roles:
 - a. Assign roles such as Channel Manager or Technician with distinct permissions.
 - b. Permissions include creating, transferring, and managing support sessions.

3. Support Sessions:
 - a. Each channel can manage up to 100 support sessions.
 - b. Sessions can be transferred, closed, or reassigned across channels.
4. Default Channel:
 - a. A system-created default channel ensures seamless transition for unassigned sessions.
5. Granular Control:
 - a. Fine-tuned permissions for tasks such as remote access, file transfers, and command execution.

How to Use Channels

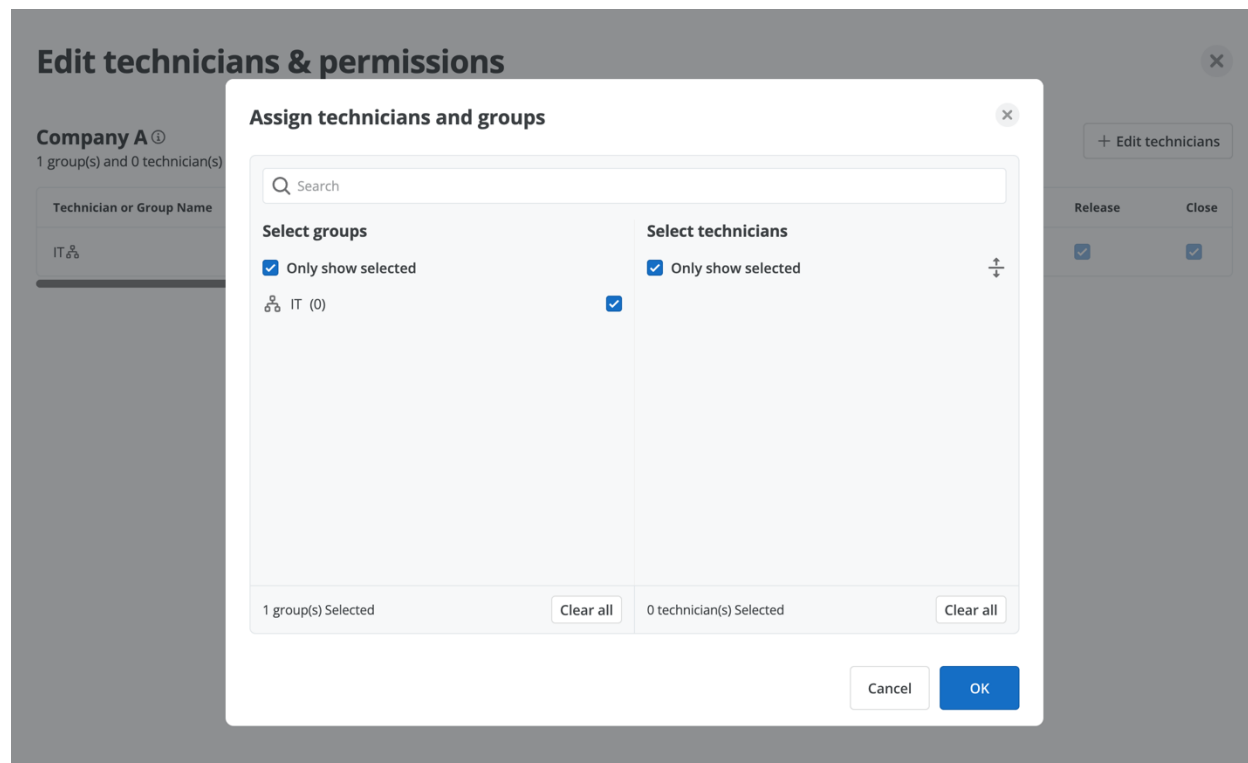
1. Creating a Channel
 - a. Navigate to Management > Service Desk > Channels.
 - b. Click on Create Channel.
 - c. Fill in the required fields:
 - i. Channel Name: Must be unique (up to 64 characters).
 - ii. Description: Optional but helpful for identification.
 - iii. Session Expiration: Define expiration (e.g., 30 mins, 1 day).



The screenshot displays the Splashtop On-Prem Admin interface. On the left, the navigation sidebar shows 'Channels' selected under the 'SERVICE DESK' section. The main area is titled 'Channels' and features a '+ Create Channel' button highlighted with a red box. Below this is a table listing existing channels:

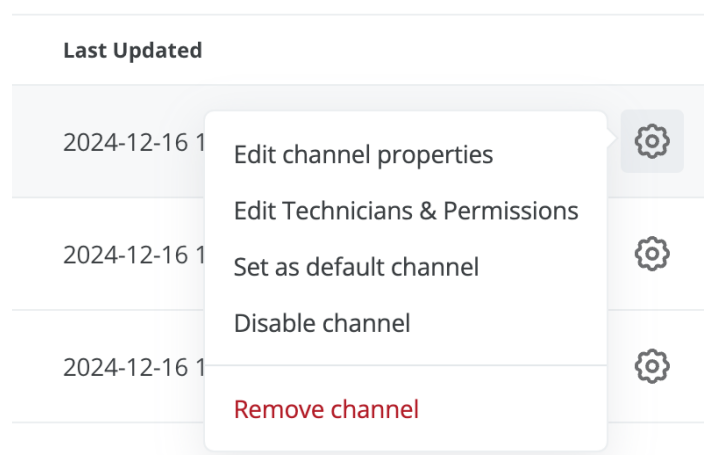
Channel Name	Permissions	Support Sessions	Status	Last Updated
Company A Test	1	0	Enabled	2024-12-16 13:24:36
Company B wise	1	0	Enabled	2024-12-16 13:24:47
Company C	1	0	Enabled	2024-12-16 13:25:12
Company D hi hi hi rather than trying to shake it off or ignore it, he says that we sho...	3	7	Enabled	2024-12-16 13:25:31
Default Default channel	2	1	Enabled	2024-08-16 18:42:37

2. Assigning Technicians and Groups
 - a. Use the Assign Technicians & Groups panel.
 - b. Select from available groups or technicians.
 - c. Note: Up to 1,000 technicians and 100 groups can be associated with a channel.



3. Editing or Deleting a Channel

- Access the gear menu next to the channel name.
- Select Edit Channel to modify properties or permissions.
- Choose Remove Channel to delete. Note that this action is irreversible.



Permission Matrix

Roles dictate the actions a user can perform. Below is a summary:

Role	Permissions
Owner	Full access to manage channels, permissions, and support sessions.
Team Admin	Similar to Owner, but cannot remove default channels.
Technician	Limited to managing assigned sessions.
Group Manager	Manages associated groups and permissions but cannot create channels.

Channel Behaviors

Default Channel

- A single default channel exists per team.
- Unassigned sessions from private channels are automatically moved here.
- Cannot be deleted or disabled.

Enabling/Disabling Channels

- Disabled channels are hidden from the Service Desk console but retain their data.
- Enabled channels appear in the console and allow session management.

Error Handling

- Duplicate names trigger an error prompt.
- Session limits: Exceeding 100 sessions or maximum active channels results in errors.

Best Practices

1. Organize Channels:
 - a. Use descriptive names and appropriate session expiration times to streamline management.
2. Utilize Default Channel:
 - a. Ensure proper handling of unassigned sessions by configuring the default channel correctly.
3. Leverage Granular Controls:
 - a. Assign permissions based on roles for precise control over session actions.

Logs and Reporting

- Channel logs include details of changes, session activities, and user actions.
- Export logs monthly or filter by date and channel for detailed reports.

Troubleshooting Common Issues

- Channel Not Visible: Check the channel status (enabled/disabled).
- Permission Errors: Verify role assignments and granular settings.
- Session Transfer Errors: Ensure technicians are assigned to both source and destination channels.

Service Desk - Console and general usage

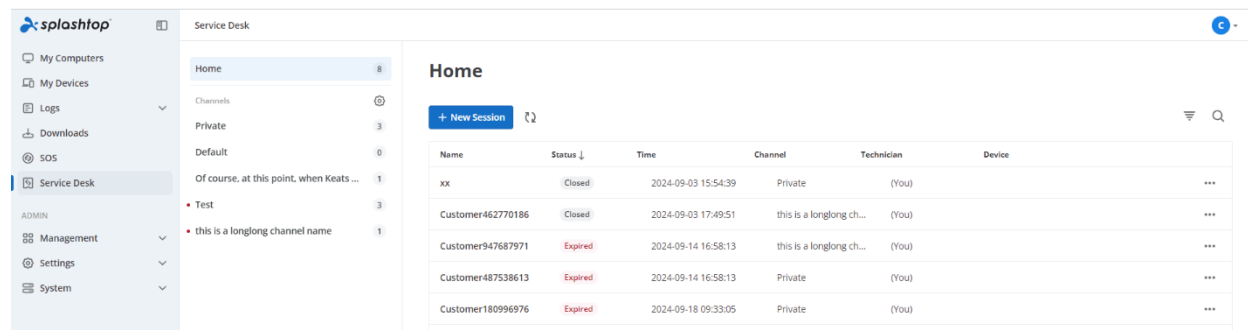
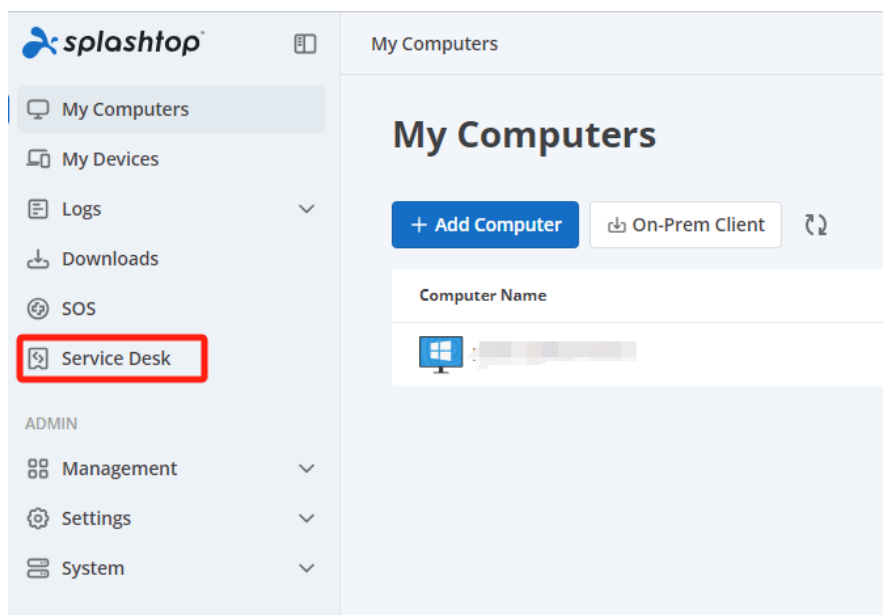
Service Desk provides not only a new interface for users to monitor and manage attended sessions but also an opportunity to enhance user's workflow. You don't need to wait for a new 9-digit code generated from the end users' side each time when starting an attended remote connection.

Requirements

- Both On-Prem app and SOS version v3.7.2.1 or newer
- For a user account to be able to use the feature:
 - The attended access feature (SOS) should be included in your license.
 - He/she must have the attended access feature available to him/her, being a technician role for example.

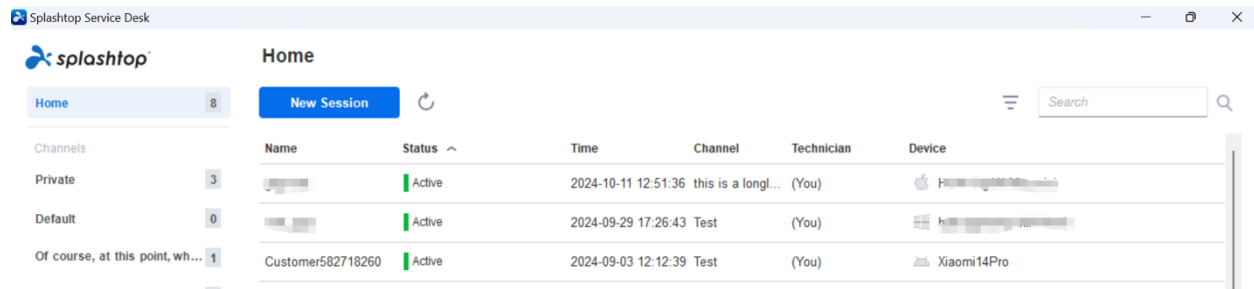
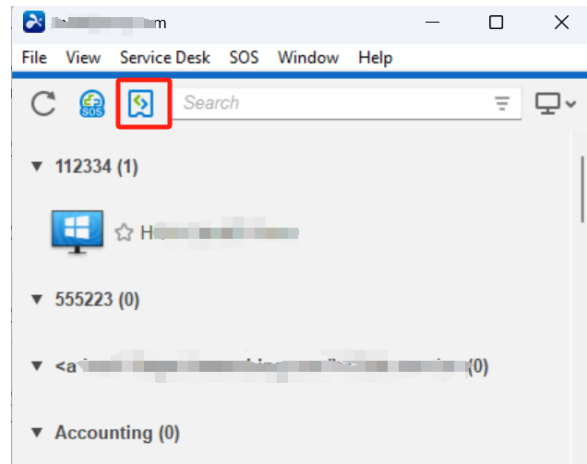
How to enter Service Desk console:

- You can enter Service Desk console from either the web console or the On-Prem client app.
- From Web console:

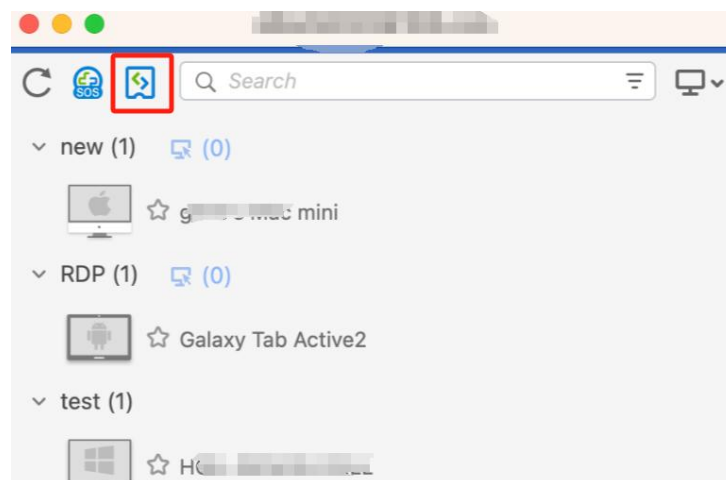


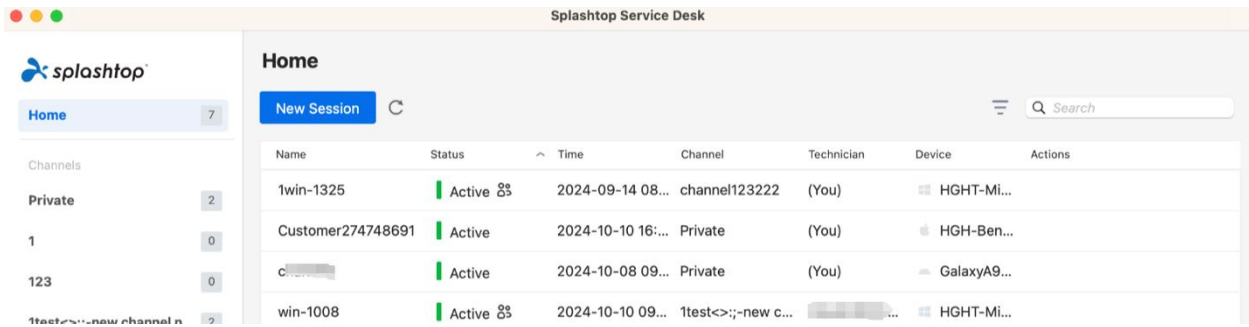
From On-Prem client app

- Windows users



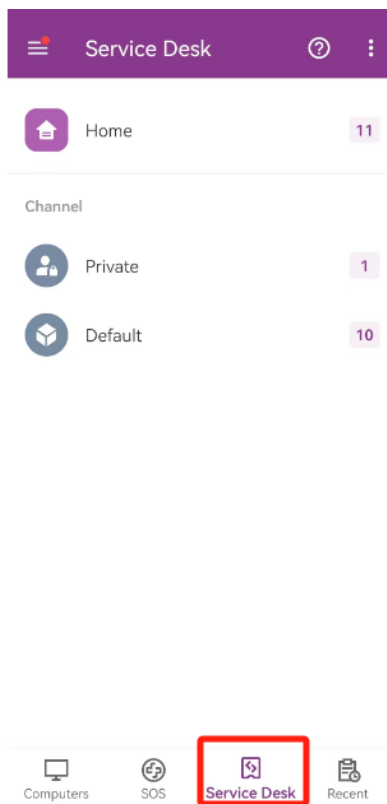
- Mac users





Name	Status	Time	Channel	Technician	Device	Actions
1win-1325	Active	2024-09-14 08...	channel123222	(You)	HGHT-Mi...	
Customer274748691	Active	2024-10-10 16:...	Private	(You)	HGH-Ben...	
...	Active	2024-10-08 09...	Private	(You)	GalaxyA9...	
win-1008	Active	2024-10-10 09...	1test<>:-new c...	...	HGHT-Mi...	

- Android users



Service Desk

Home 11

Channel

Private 1

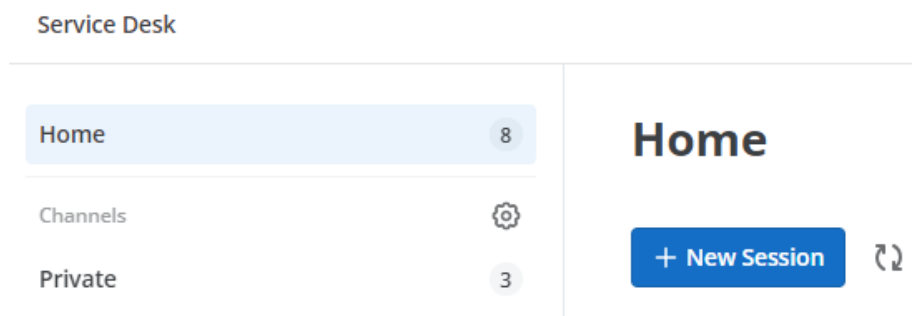
Default 10

Computers SOS **Service Desk** Recent

How to help your client via Service Desk

Channels: In Service Desk, “Channel” is like the concept of group of related sessions.

When you enter Service Desk, you will find Home and Channel there:

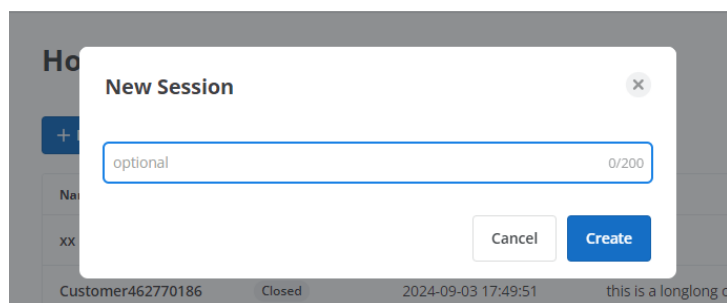


- Home: On Home, you can find all the attended sessions that are assigned to you.
- Private: Sessions in Private channel can only be seen by yourself.

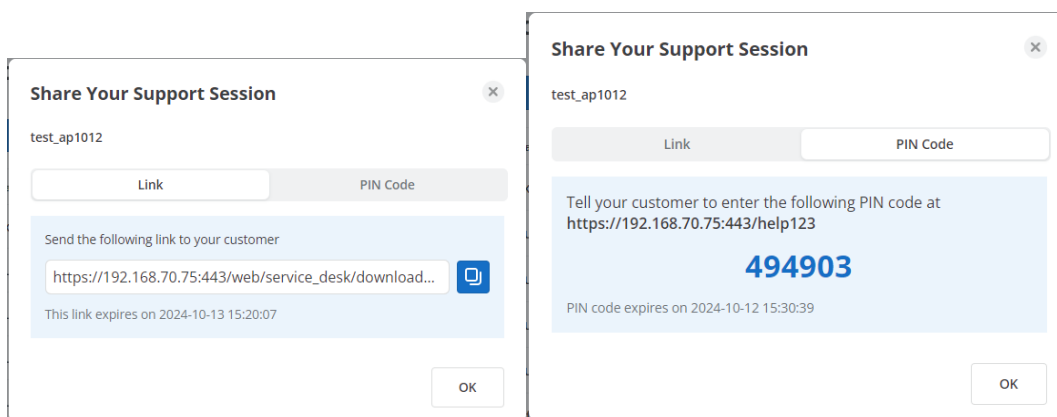
Create a new session and get it ready for support:

Step [1] <Technician side>:

Click the "New session" button on your chosen channel



Share this support session to you client via link or pin code:



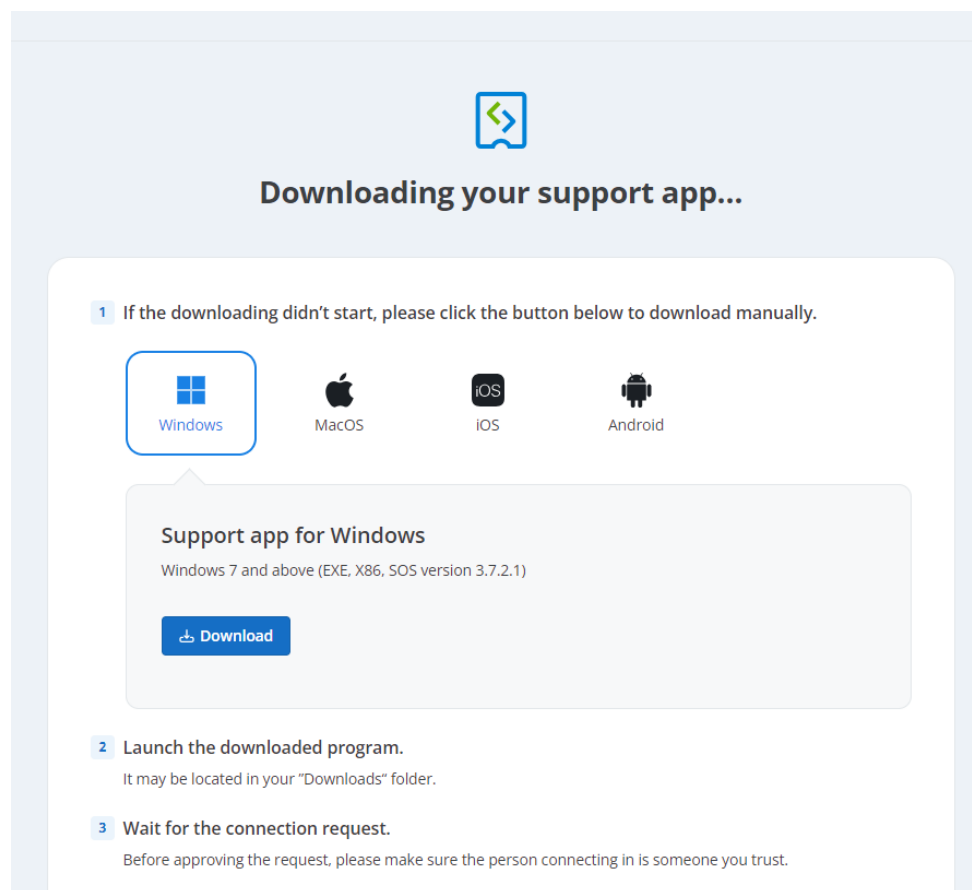
The status of the session will be "Waiting" by now:

test_ap1012	Waiting	2024-10-12 15:20:07	Private	(You)	  
-------------	---------	---------------------	---------	-------	---

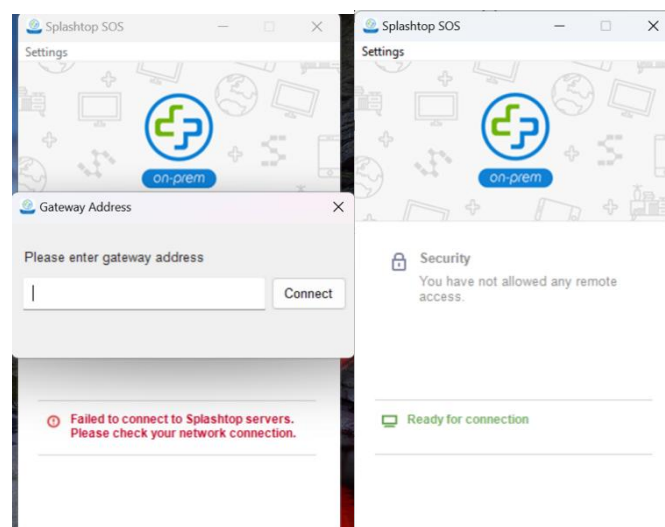
Step [2] <Client side>:

With the link or pin code, the client can download the app and launch it.

- Download:



- Launch the app: Input your team gateway address and get ready (If you want to skip this for your client, can contact us and get a SOS build with gateway address, then config it on your admin console)



Step [3] <Technician side>:

Request the access permission to the client's device

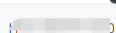
- Once the end user launches the support app, the status of the session will change from “Waiting” to “Active”

Name	Status ↑	Time	Channel	Technician	Device
test_ap1012	Active	2024-10-12 15:20:07	Private	(You)	    

- When the session is active, technician can request permission to connect by clicking “Start Remote Session”

Home

[+ New Session](#) 

Name	Status ↑	Time	Channel	Technician	Device	
test_ap1012	Active	2024-10-12 15:20:07	Private	(You)	    	Start Remote Session

Request Permission

Requesting permissions from test_ap1012 for the following actions:

Permissions

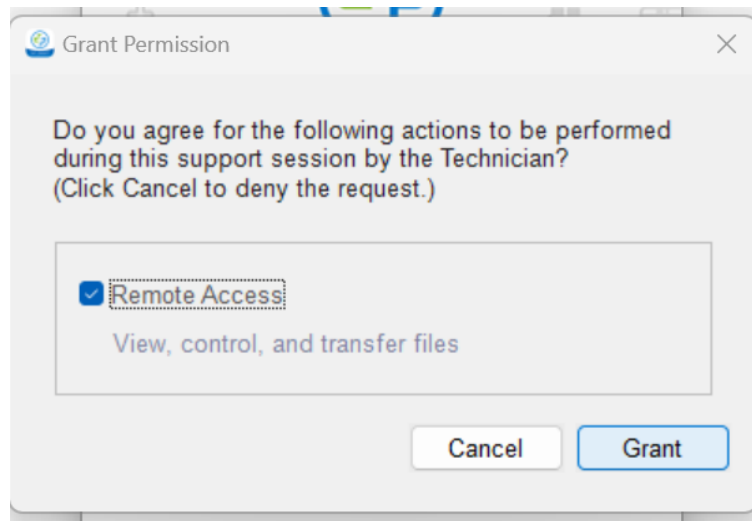
- ☒ Remote Access ⓘ
View, control, and transfer files

[Cancel](#) [Request](#)

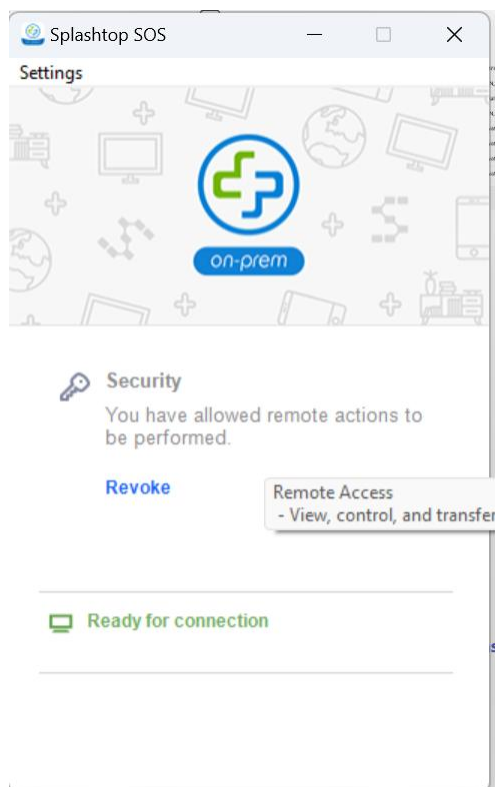
Step [4] <Client side>:

Handle the permission request from technician

- After the technician requests permission, the end user would see the prompt as follows to reject or grant permission.



- The following will show on the end user's side if he/she grants the permission:



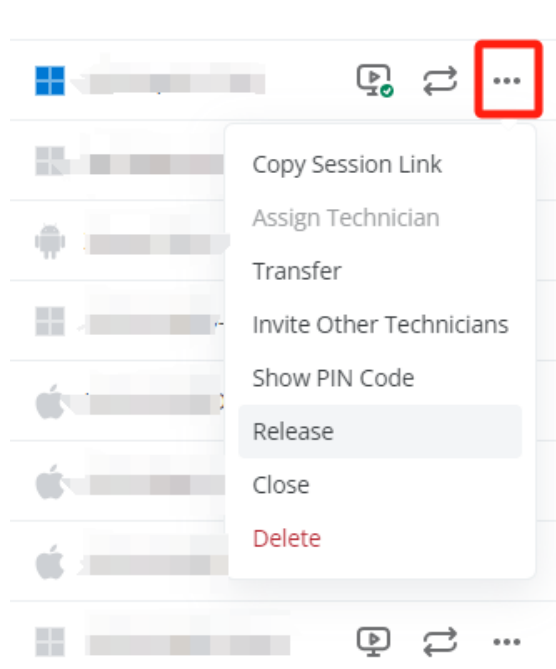
Step [5] <Technician side>: Access to the target device to support

- If the user grants the permission, the “Start Remote Session” icon will change from  to , which means the technician can connect to the user.
- Now, the technician can start to connect by clicking “Start Remote Session”

Name	Status ↑	Time	Channel	Technician	Device	Start Remote Session
test_ap1012	Active	2024-10-12 15:20:07	Private	(You)	    	  

Other actions supported on Service Desk console

In addition to “Start Remote Session”, you can also take the following actions.



- Assign Technician: assign or re-assign a technician to the support session.
- Transfer: transfer the session to another assignee or another channel
- To transfer to another assignee, permission for Release should be granted
- To transfer to another channel, access to another channel should be granted
- Invite Other Technicians: Invite up to 2 other technicians to the support session (max total 3 techs)

- Copy Session Link
- Show PIN Code
- Release: release the session from the assigned technician
- Close: close the session
- Delete: delete the session from the channel

Session status

Name	Status ↑	Time	Channel	Technician	Device	
test_ap1012	Active	2024-10-12 15:20:07	Default	(You)	 HGH-Aprily-T490	  
Customer998634503	Expired	2024-10-09 13:00:20	Test	(You)		
Customer005329358	Waiting	2024-10-09 11:55:38	Of course, at this po...	(You)		  
test_...:	In queue	2024-10-12 15:40:00	Default		 	  

- Waiting: The status will be “Waiting” for the user to download and run the Service Desk support app from the unique link right after a new session link has been generated.
- Active: The Service Desk support app has been started on the end user's computer; this session has a technician assigned, and the technician is ready to request permission to connect.
- In queue: The session has been released, and it is waiting for a technician to take the session.
- Expired: The session exceeded the Session Expiration time that was preset from the Channel settings.
- Closed: The technician has manually closed the session. No further connection is possible. To connect again, generating a new session is required.

Service Desk - SOS Call

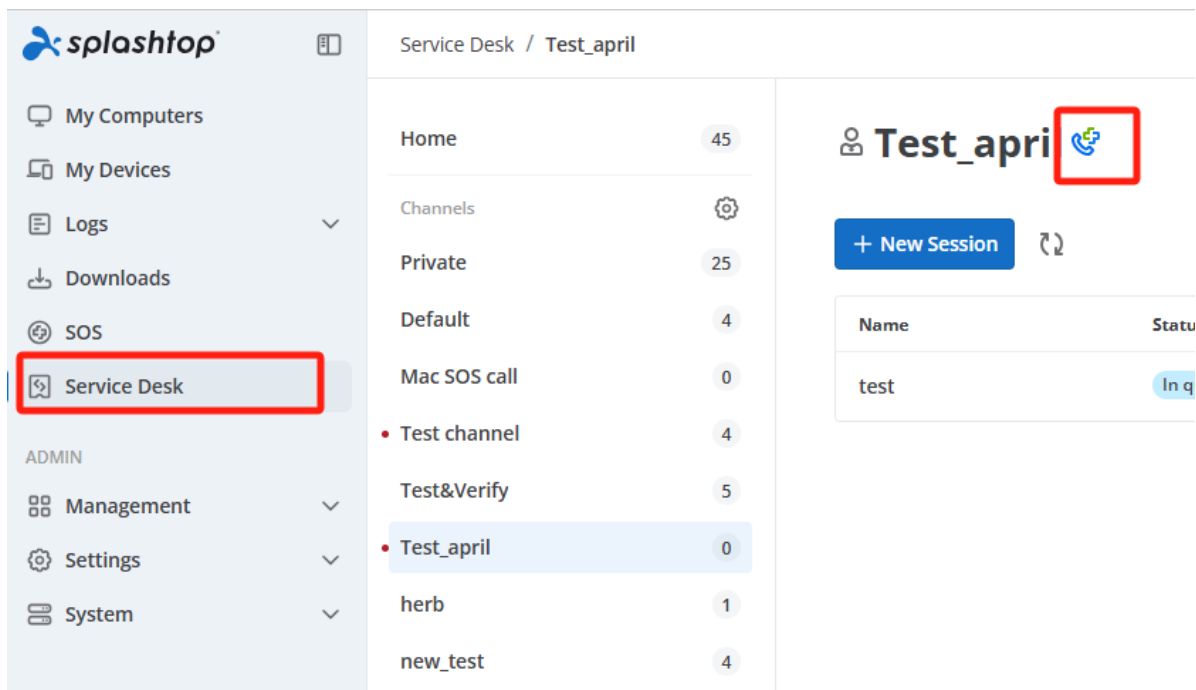
1. Requirements

- Both On-Prem app and SOS version v3.7.4.5 or newer.
- Gateway version v3.36.0 or newer.

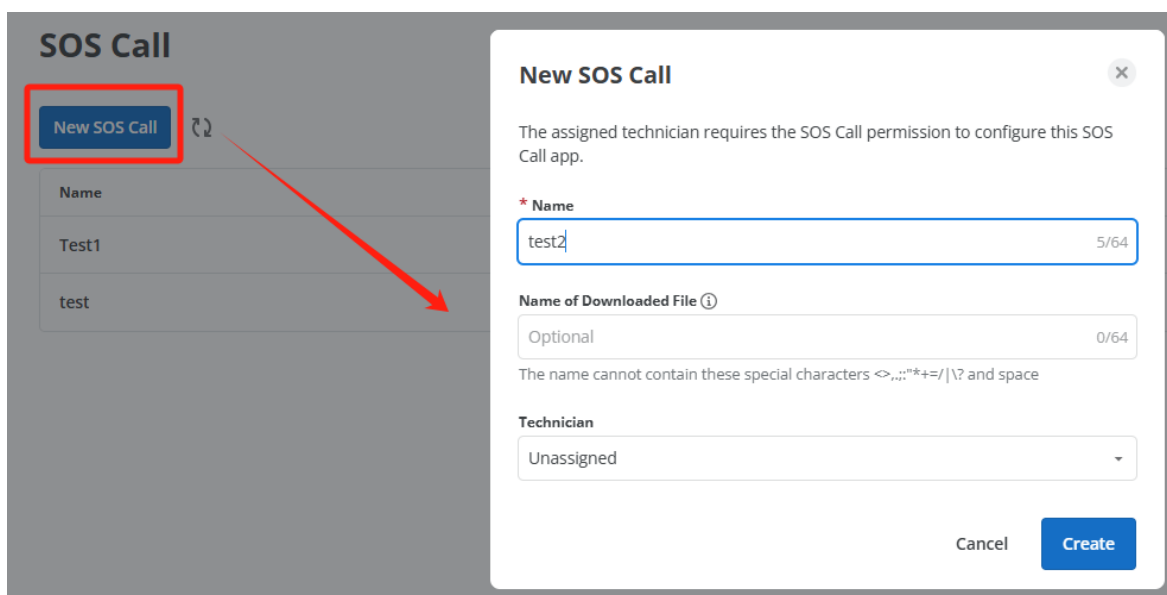
2. The main usage flow of SOS Call

Step[1]<Technician side>: Create the SOS Call

- Enter the SOS Call management:

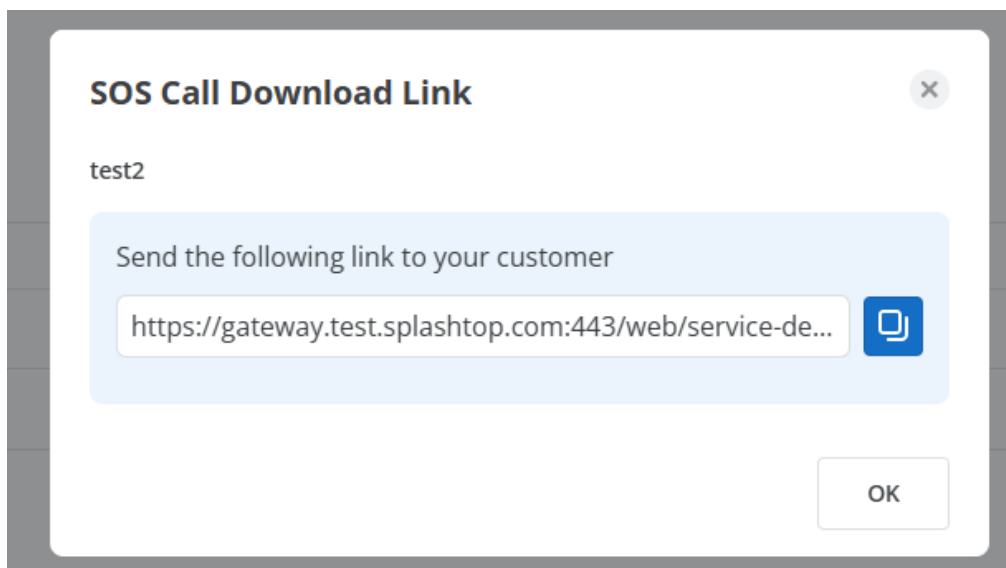


- Create a new SOS Call:



- Get the download link and send it to your supportee:

- Note: A single SOS Call link can be used by multiple users without the need to create a link for each user.



Step[2]<Supportee side>: Download and run the SOS app

- With the download link, get the SOS Call app based on your platform:



Downloading SOS Call app...

Request support right from your desktop

1 If the download didn't start, please click the button below to download manually.
For Android devices that need support, open this page on your Android device.


Windows


macOS


Android

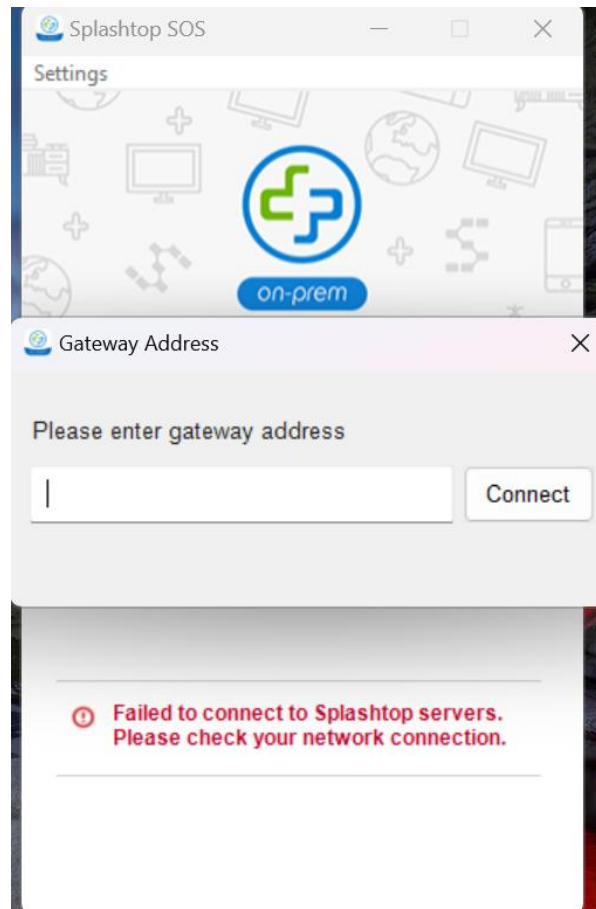
Support app for Windows

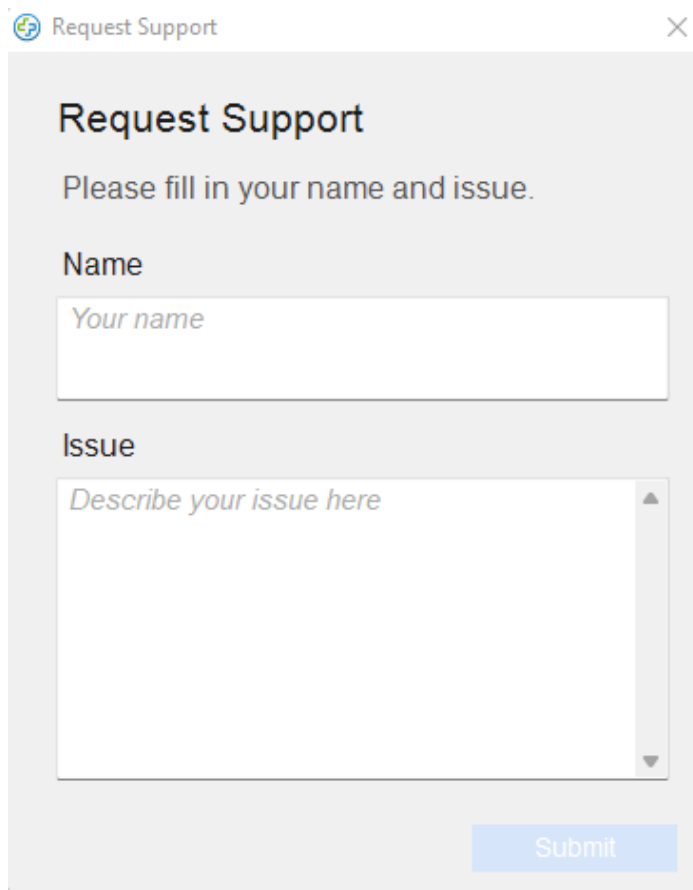
Windows 7 and above (EXE, X86, SOS version 3.7.3.55)

 EXE

- Once there's any issue need to be help with your technicians, launch the app:

- Input your gateway address if needed. And submit your name and issues.





A screenshot of a 'Request Support' dialog box. The dialog has a title bar with a close button (X) and a 'Request Support' icon. The main content area is titled 'Request Support' and contains the instruction 'Please fill in your name and issue.' Below this, there are two input fields: 'Name' with a placeholder 'Your name' and 'Issue' with a placeholder 'Describe your issue here'. A 'Submit' button is located at the bottom right of the dialog.

Step[3]<Technician side>: Find the request and offer support

- After the request has been submitted on the supporter side, technicians would then see a new entry in the Splashtop Service Desk console indicating the user has requested support.

Name	Status ↓	Time	Channel	Technician	Device
test	Active 	2025-06-09 15:29:50	Test_april	(You)	 HC  

- Additional information about name and issue details can be found by clicking on the newly-created entry:

test 





Session info

Device info

Comment

Transcript

Customer Name	test
Customer issue	123
Session ID	990421123
Channel	Test_april
Status	Active 
	2025-06-09 15:29:50
Technician	owner@stp.com (You)
Source	SOS Call

3. The management of SOS Call on the admin console

3.1 Enable SOS Call for new/existing Service Desk channels

- SOS Call is a setting item belonging to channel, it can be edited from the channel settings:

	Add	0	Enabled	2025-03-19 17:56:50	
	2	0	Enabled	2025-03-20 1	
	3	1	Enabled	2025-03-20 1	
Test 	5	1	Enabled	2025-06-09 1	

Edit channel properties
Edit Technicians & Permissions
Set as default channel
Disable channel
Remove channel

- Scroll down the channel edit page to find Enable SOS Call:

SOS Call

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

☒ **Enable SOS Call** ⓘ

⚠ One or more of your SOS versions in Splashtop Gateway are below 3.7.4.0 and do not support SOS Call. Please contact your team owner.

3.2 Manage and create SOS Call download links

- SOS Call applications should be dedicated to a whole group of end-users (E.g. A specific company, team of users, etc) since the generated link is reusable.
- After enabling SOS Call in 3.1, you can access the management section. The Manage SOS Call icon will be found on the channel you've enabled.

 **Test_april** 

+ New Session 

Name	Status ↓	Time
test	Active 	2025-06-

- Besides the creation, the existing SOS Call apps can be managed as follows:
- Edit : To assign a new technician or to change the name of the application

Edit SOS Call



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

*** Name**

4/64

Name of Downloaded File ⓘ

0/64

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

Technician

Cancel

Save

- **Suspend:** Would temporarily make this SOS Call application link invalid for any new downloads, as well as for existing downloaded applications. Resuming an application won't generate a new link, the link would remain unchanged.
- **Remove:** Would invalidate any existing link or downloaded applications.

test	owner@stp.com	2025-06-09 14:16:40	 
			Edit Suspend Remove

3.3 SOS Call permissions

- To edit permissions, go to Management > Channels > Edit technicians & permissions

Edit technicians & permissions



Test_april ①

4 group(s) and 1 technician(s)

+ Edit technicians

Technician or Group Name	Channel Manager	Invite	SOS Call	Release	Close	Delete	Remote Access ①
[Redacted] m	☐		☒	☒	☒	☒	☒
G [Redacted] o	☒		☒	☒	☒	☒	☒
[Redacted] Group	☒		☒	☒	☒	☒	☒
[Redacted]	☒		☒	☒	☒	☒	☒
[Redacted]	☒		☒	☒	☒	☒	☒

- All technicians will be able to see new SOS Call applications if the default assignee is "Unassigned"
- Technicians with SOS Call permission can create/manage SOS Call applications whose default assignee is themselves.
- Technicians w/o SOS Call permission cannot create/manage any existing SOS Call applications.

Service Desk - Transcripts

Overview

Splashtop Service Desk now supports session transcripts, providing a full record of key session activities for auditing, troubleshooting, and compliance purposes. These transcripts include chat interactions, remote controls, and system tool operations performed during a system tool background session.

What Is Recorded in a Transcript?

Session Metadata

- Session start and end time
- Session ID and host machine details
- Session transition records.
- Session comments.

Chat Messages

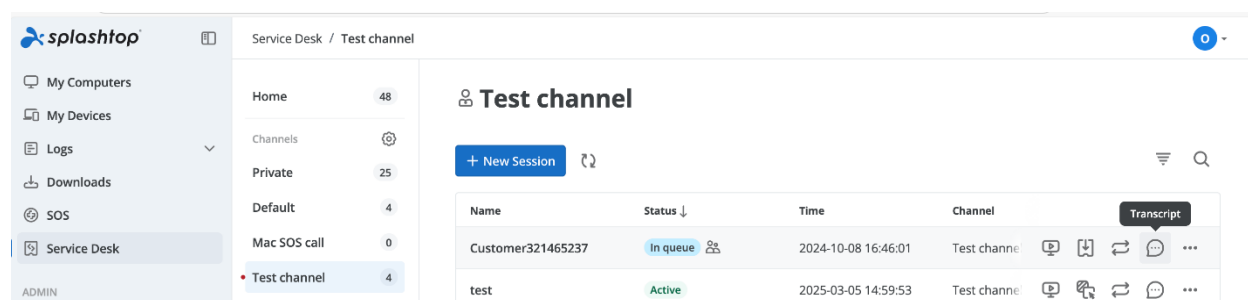
- All text messages exchanged during the session

System Tool Usage (if applicable)

How to View Transcripts

For Active Sessions

1. Open the Service Desk console.
2. Navigate to the Support Session list.
3. Select the session you are currently in.
4. Click the Transcript tab to view real-time logs.

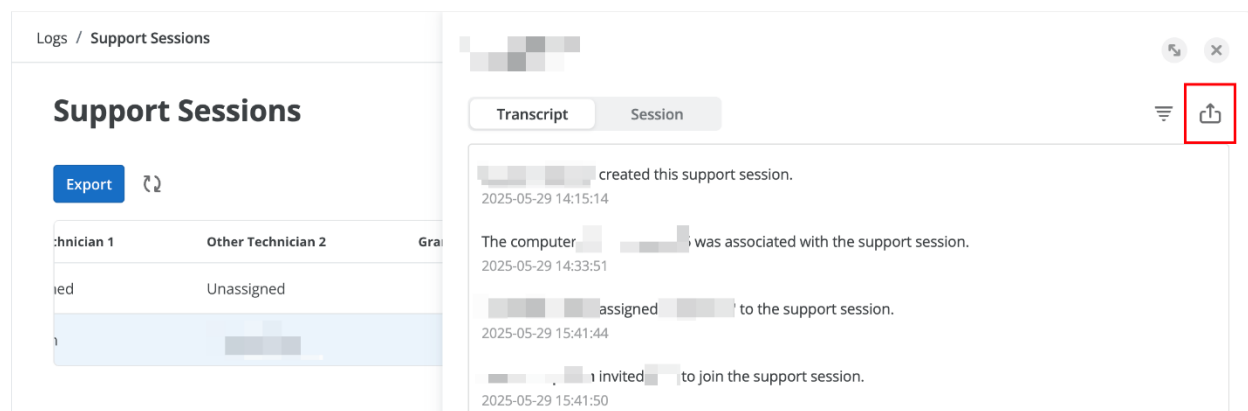


For Past Sessions

1. Go to Logs → Service Desk → Support Sessions
2. Select the completed session you want to review.
3. Click the session record to display the recorded logs.

Exporting Transcripts

- **Export Formats:** Transcripts can be exported in CSV format for record-keeping.
- **How to Export:**
 - Open the desired session's transcript from logs.
 - Click Export and the file will download to your local system.



Use Cases

- **Compliance & Audit** – Ensure your support sessions meet internal IT or industry compliance requirements.
- **Troubleshooting** – Review exactly what commands and file transfers occurred during problem resolution.
- **Training & Quality Control** – Use transcripts to review team performance and provide targeted coaching.

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.



- My computers
- My devices
- Logs
- Downloads
- SOS

ADMIN

- Management
- Users
- All computers
- All devices
- Grouping
- Deployment
- Preference Policy
- Scheduled Access

SERVICES DESK

- Channels

Management / Deployment



Manage Deployments

Easily deploy Streamers to the computers you want to remotely access

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

[+ Add Deployment](#)

Deployment Name	Policy Name	Computer Naming Rule	Deployment Code	Date of Creation	Deploy
10		Use current computer name	10ABCD1234567890	2024-08-05	Deploy
10		Use current computer name	10ABCD1234567890	2024-08-05	Deploy
10		Use current computer name	10ABCD1234567890	2024-08-05	Deploy
100		Use current computer name	100ABCD1234567890	2024-08-05	Deploy
10000		Use current computer name	10000ABCD1234567890	2024-08-05	Deploy
107		Use current computer name	107ABCD1234567890	2024-08-05	Deploy
10000		Use current computer name	10000ABCD1234567890	2024-07-23	Deploy
10		Use current computer name	10ABCD1234567890	2024-07-23	Deploy



- My computers
- My devices
- Logs
- Downloads
- SOS

ADMIN

- Management
- Users
- All computers
- All devices
- Grouping
- Deployment
- Preference Policy
- Scheduled Access

SERVICES DESK

- Channels

Management / Deployment / Add Deployment Package



Add Deployment Package

Package Name

Policy Name

[Create preference policy](#)

Computer Naming Rule
(Computers deployed using Splashtop Connector will always follow the Profile Name defined in the Connector settings.)

☒ Use current OS hostname
☐ Keep in sync with OS hostname
☐ Use custom name + sequence number
e.g., Acme Bakery (005)
☐ Use custom name + current OS hostname
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 hostname.

Grouping
Group Choice
[Create or manage groups](#)

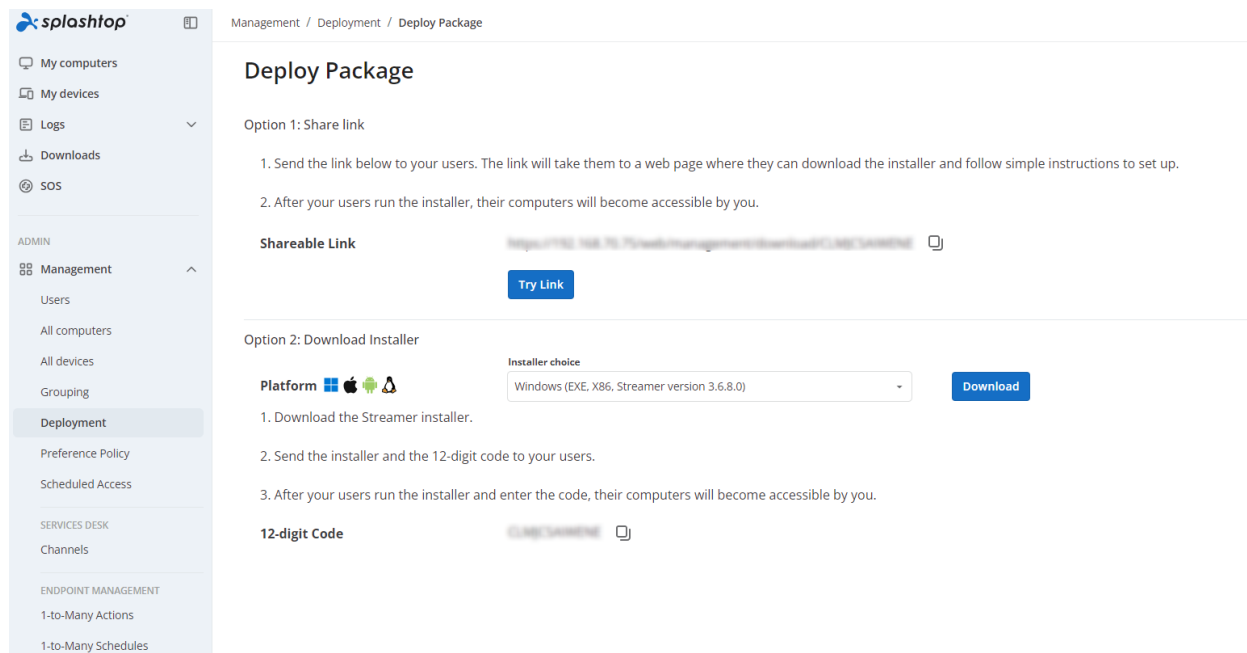
☒ **Auto-launch Streamer**
Automatically launch Splashtop Streamer every time the computer starts. (Not applicable to computers deployed using Splashtop Connector.)

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

General Settings
☐ **Hide Streamer tray icon**
Hide Streamer icon on Windows system tray or Mac menu bar. Check this option to reduce the chance of users tampering with the Streamer. (Not applicable to computers deployed using Splashtop Connector.)

2. Select  for the package that was just created.

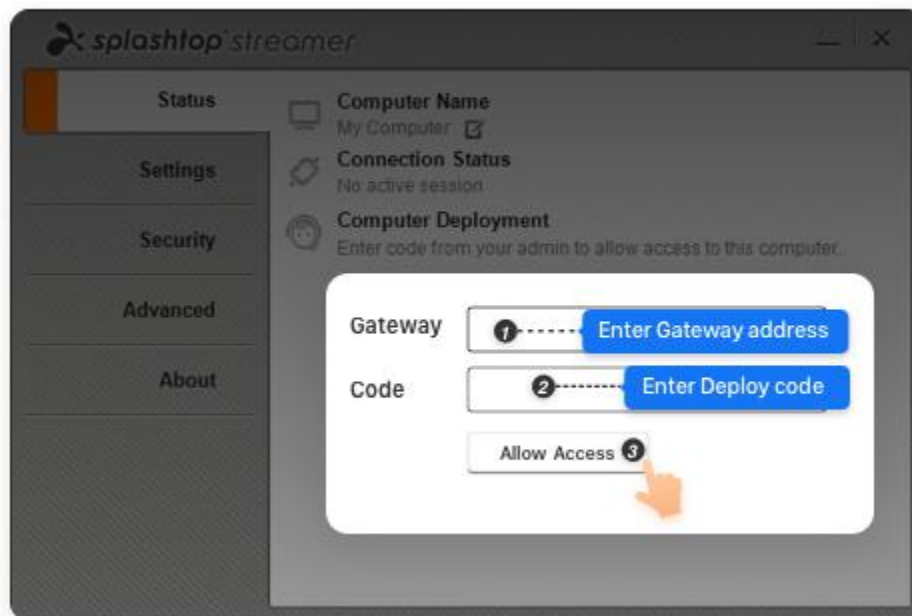
3. **Have your users install the streamer.** You can send the deployment package link to your users. By following the link, your users can download the streamer installer and run the file. You can also send the streamer installer file directly to your users (via Dropbox, email, etc.).



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
Policy Name	Select a preference policy None Create preference policy
Computer Naming Rule (Computers deployed using Splashtop Connector will always follow the Profile Name defined in the Connector settings.)	☒ Use current OS hostname ☐ Keep in sync with OS hostname ⓘ ☐ Use custom name + sequence number e.g. Acme Bakery (005) ☐ Use custom name + current OS hostname 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 hostname.
Grouping	Group Choice Default Group Create or manage groups
General Settings	☒ Auto-launch Streamer Automatically launch Splashtop Streamer every time the computer starts. (Not applicable to computers deployed using Splashtop Connector.) Idle session timeout Remote sessions will automatically disconnect after 0 minutes of no activity (0 means no timeout). idle session timeout ☐ Hide Streamer tray icon Hide Streamer icon on Windows system tray or Mac menu bar. Check this option to reduce the chance of users tampering with the Streamer. (Not applicable to computers deployed using Splashtop Connector.) ☒ Enable direct connection When on the same network, use direct connection for better performance. Based on your organization's security policy, you may want to disable this option. ☒ Enable direct connection When on the same network, use direct connection for better performance. Based on your organization's security policy, you may want to disable this option. ☒ Require Windows or Mac login Require entering the computer's user name and password when connecting remotely. Request permission to connect Prompt for user's permission at the computer when connecting remotely. ☐ Reject connection after request expires (At login screen, reject automatically) ☐ Reject connection after request expires (At login screen, allow automatically) ☐ Allow connection after request expires ☒ Off
Security (Not applicable to computers deployed using Splashtop Connector.)	☐ Blank screen when in a session Prevent others from seeing what is on the remote screen while you are remotely controlling this computer. ☐ Lock screen when disconnect Prevent others from seeing what is on the remote screen while you are remotely controlling this computer. ☐ Lock keyboard and mouse when in a session When your device connects to the computer, lock the computer's keyboard and mouse. ☐ Lock Streamer settings using Splashtop admin credentials By default, Streamer settings can be modified by anyone with Windows or Mac admin account. By checking this option, Streamer settings will be locked and can only be unlocked by admins on your Splashtop Gateway team.
Sound (Not applicable to computers deployed using Splashtop Connector.)	☒ Output sound over the remote connection only ☐ Output sound on the local computer only ☐ Output sound both over the remote connection and on the local computer (Windows Streamer only)
	Add Cancel

Option	Description	Notes
Package Name	Enter a unique name to identify the deployment package.	Helps distinguish between different deployment packages.
Policy Name	Select a preference policy or create a new one.	Determines session settings, quality, and security options.
Computer Naming Rule	- Use current OS hostname: Keeps the computer name synced with the OS hostname. - Use custom name + sequence number: Customize computer names with an incremental number (e.g., 'Acme Bakery-001'). - Use custom name or current hostname: Allows a custom name but defaults to the OS hostname if unspecified.	Organizes computers with identifiable names in the Splashtop management console.
Grouping	Assign the computer to a specific group (e.g., 'Default Group').	Use the 'Create or manage groups' link to add/edit groups.
Auto-launch Streamer	Automatically starts the Streamer when the computer boots up.	Not applicable to Splashtop Connector deployments.
Idle Session Timeout	Automatically disconnects sessions after a specified period of inactivity.	Set to '0' for no timeout.

Hide Streamer Tray Icon	Removes the Streamer icon from the system tray/menu bar to prevent user tampering.	Not applicable to Splashtop Connector deployments.
Enable Direct Connection	Allows direct connections for better performance when on the same local network.	
Require Windows or Mac Login	Options for requiring login credentials for remote access: - Prompt for user permission. - Reject if no permission is granted (auto-reject). - Allow connection automatically if no action is taken (auto-allow). - Turn off the feature entirely.	Helps enforce security and control over remote access.
Blank Screen	Hides the content on the remote screen during sessions for privacy.	
Lock Screen on Disconnect	Automatically locks the remote computer's screen after a session ends.	
Lock Keyboard and Mouse	Prevents local users from interacting with the computer during a session.	
Lock Streamer Settings	Restricts changes to Streamer settings to administrators.	

Sound	Options for sound output: - Remote connection only. - Local computer only. - Both remote and local computers (Windows Streamer only).	Let you configure audio routing during sessions.
--------------	---	--

Features marked as 'Not applicable to computers deployed via Splashtop Connector' may not function as expected, as the connector bypasses certain standard deployment features by providing a direct deployment mechanism.

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

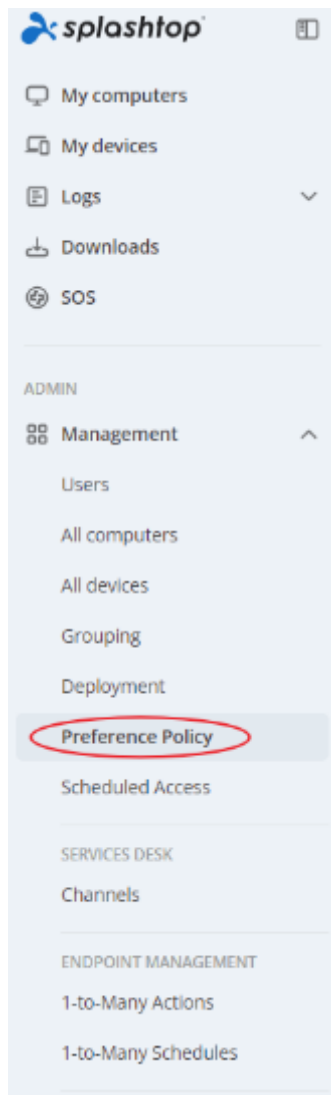
At the current time, only **Windows** and **Mac** Streamers (version **3.5.2.5** and higher) can be added to a Preference Policy.

Usage

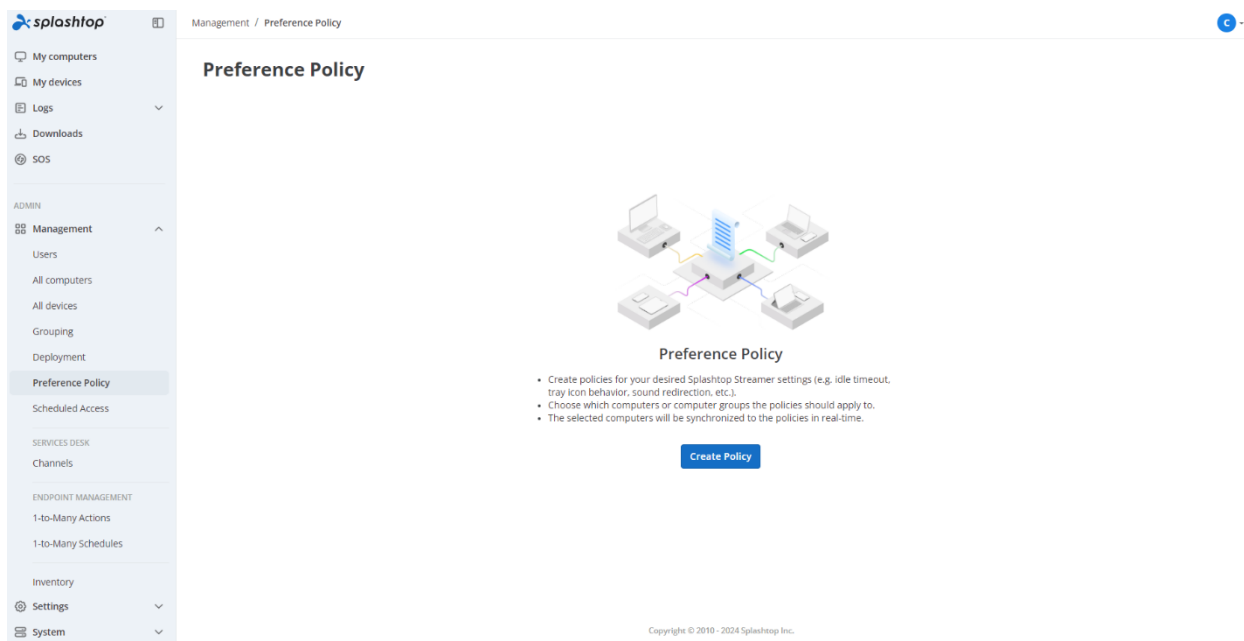
Create Policy

- Overview

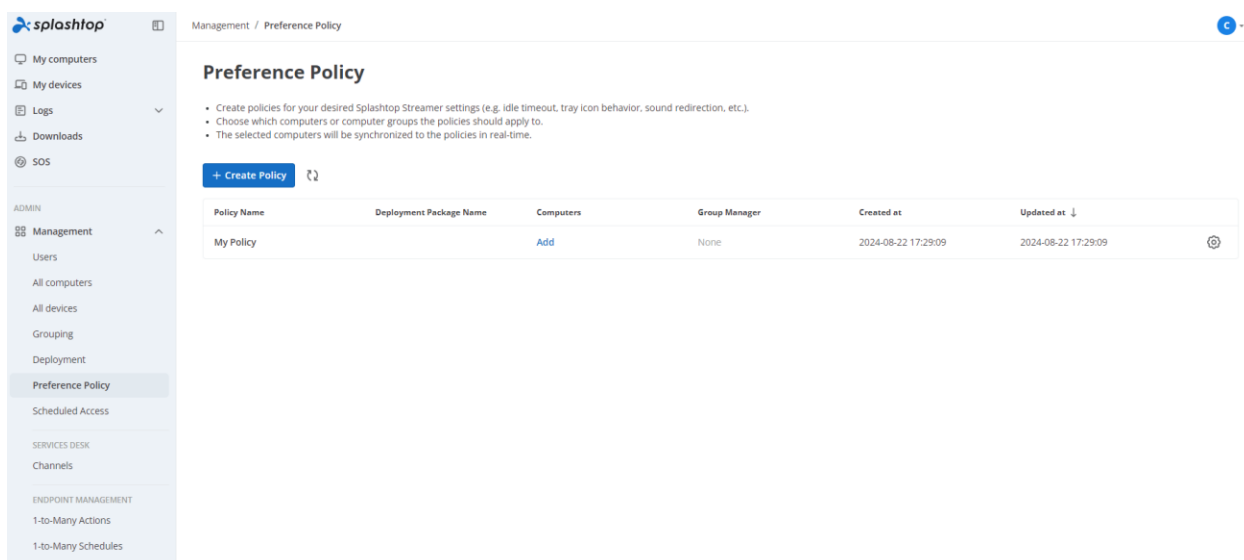
To create a new policy, log into your Splashtop Gateway web console, hover over **Management**, and click on **Preference Policy** in the drop-down menu. Then, click on **Create Policy**.



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**.

Policy Properties

Policy Name *

Add Policy Name

Description (optional)

Policy description

Group Manager

None

Streamer settings

General

Add items from unselected options

The selected options will be applied to the added computers

Unselected options

+ > Idle Session Timeout 0

+ > Hide Streamer tray icon

+ > Enable direct connection

+ > Sound Remote Only

+ > Lock streamer name

+ > Sync with OS hostname

Security

Add items from unselected options

The selected options will be applied to the added computers

Unselected options

+ > Blank screen when in a session

+ > Lock screen when disconnected

+ > Lock keyboard and mouse when in a session

+ > Lock Streamer settings using Splashtop admin credentials

Bandwidth Management

Add items from unselected options

The selected options will be applied to the added computers

Unselected options

+ > Maximum FPS Option High

+ > Maximum Audio Quality Option High

Cancel

Create

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.

© 2010-2026 Splashtop Inc. Splashtop and the logo are registered trademarks of Splashtop Inc. in the U.S. and elsewhere. All other trademarks, product and company names, and logos are the property of their respective owners.

Page 182 of 348

Policy Properties

Policy Name *	Add Policy Name
Description (optional)	Policy description
Group Manager	None

- 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.

Streamer settings

General

Selected options > Idle Session Timeout 0	Unselected options + > Hide Streamer tray icon + > Enable direct connection + > Sound Remote Only + > Lock streamer name + > Sync with OS hostname
--	---

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.

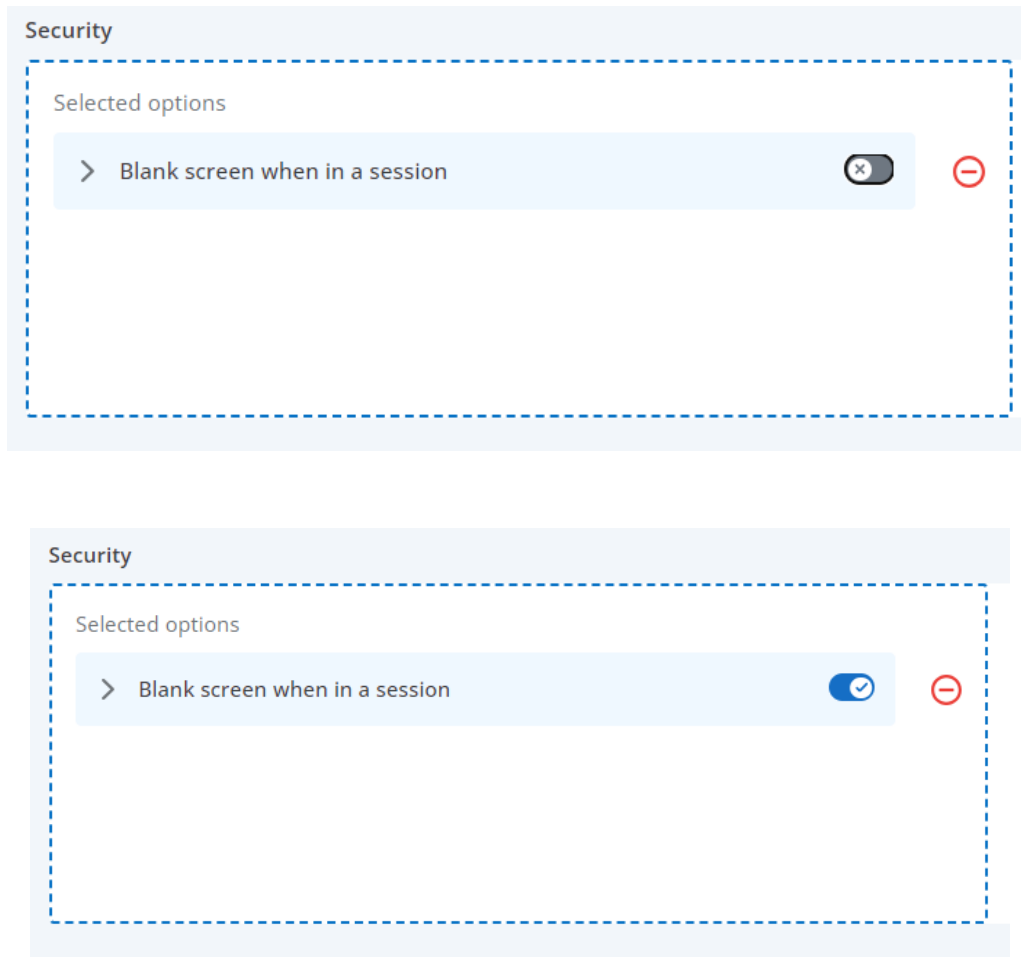
Streamer settings

General

Selected options > Idle Session Timeout 0	Unselected options + > Hide Streamer tray icon + > Enable direct connection + > Sound Remote Only + > Lock streamer name + > Sync with OS hostname
--	---

- Configure the value of an added item

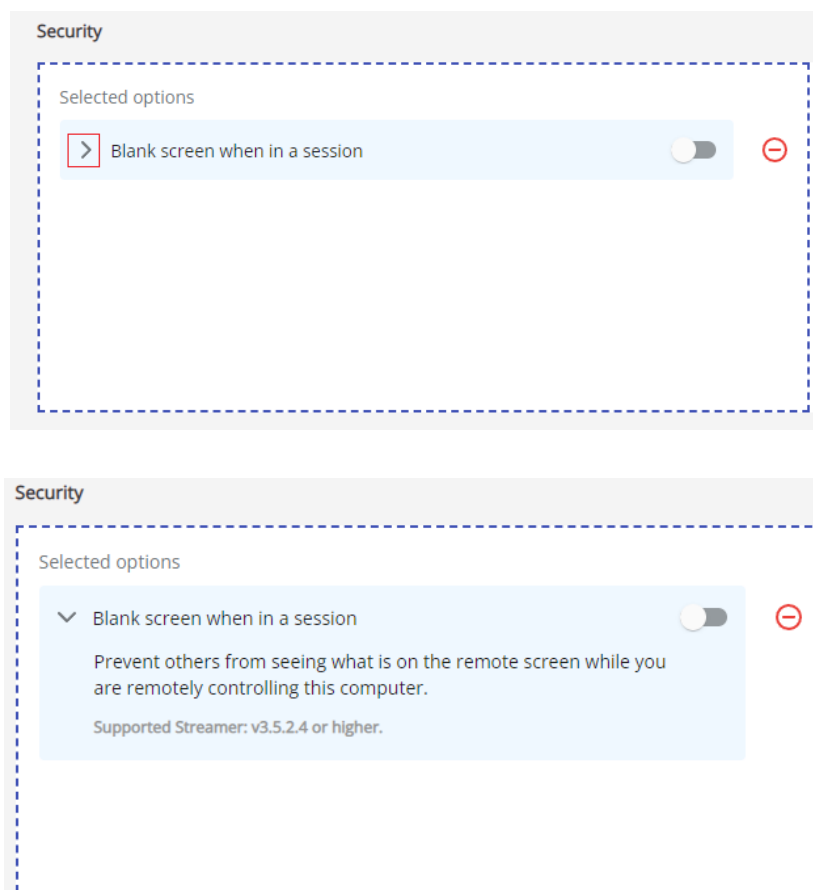
After you have added an item to your policy, you can configure its value. Most of the items have binary values that you can toggle on or off. If the switch is greyed out, the value is set to off. Conversely, if the switch is blue, the value is set to on.



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

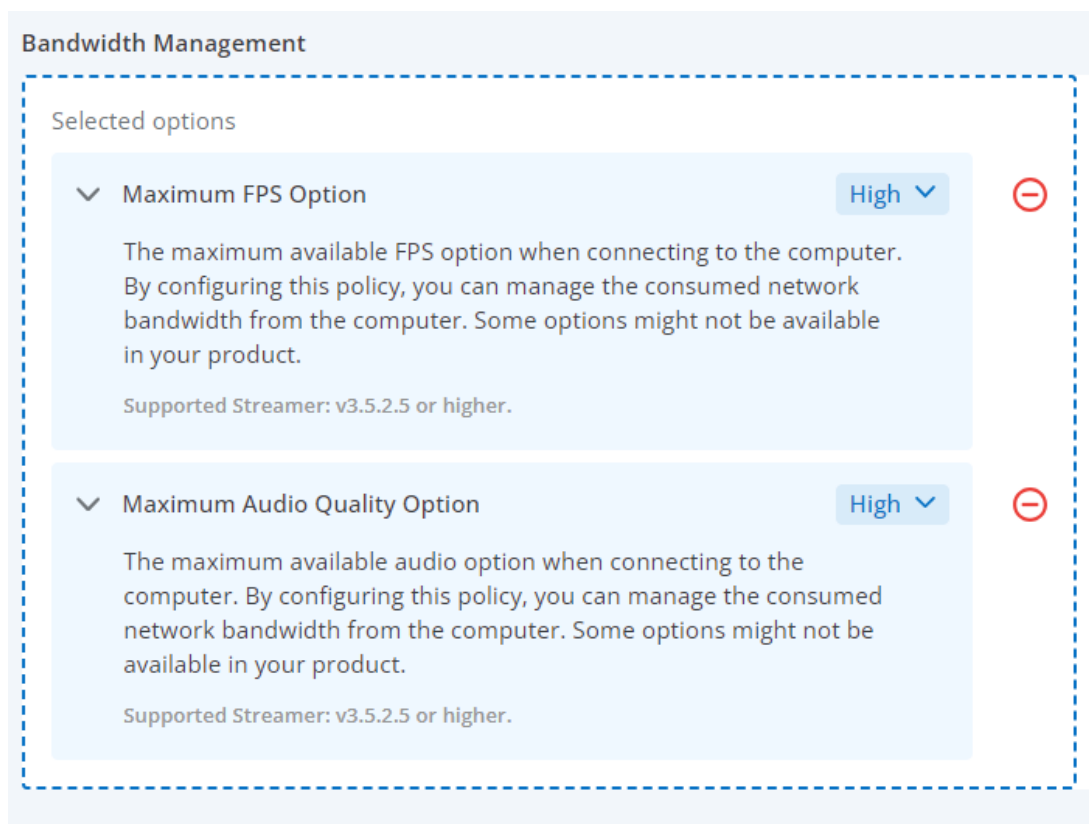
If you are not sure about the function of an item, you can click on the angle bracket icon to display a concise description.



- Bandwidth Management

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

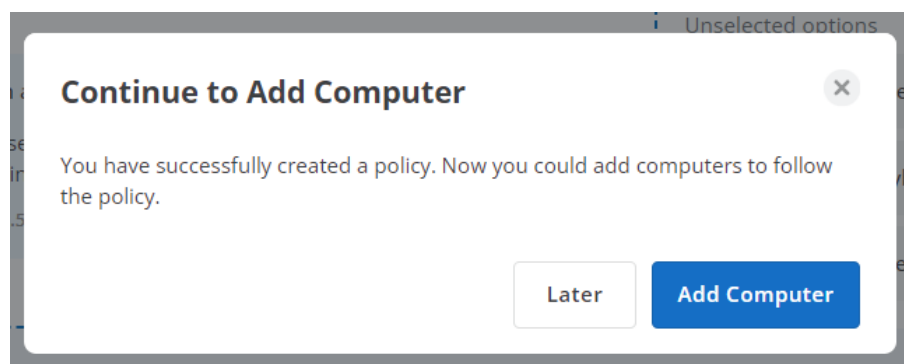
As for the items **Maximum FPS Option** and **Maximum Audio Quality Option**, if you select the highest value (Maximum FPS Option: "Ultra High", Maximum Audio Quality Option: Ultra High - 384k"), it will have the same effect as not adding these items to your policy at all: no bandwidth restrictions for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

Preference Policy

- Create policies for your desired Splashtop Streamer settings (e.g. idle timeout, tray icon behavior, sound redirection, etc.).
- Choose which computers or computer groups the policies should apply to.
- The selected computers will be synchronized to the policies in real-time.

[+ Create Policy](#) 

Policy Name	Deployment Package Name	Computers	Group Manager	Created at	Updated at ↓	
111		Add	None	2024-08-22 17:41:54	2024-08-22 17:41:54	
My Policy		Add	None	2024-08-22 17:29:09	2024-08-22 17:29:09	

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.

Management / Preference Policy / Add Computer



Add Computer



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

[Clear all](#) [Select all](#) ☐ Only show selected 0 item(s) selected

Filter by group

☐	Status	Computer Name ↑	Streamer Version ⓘ	Group	Applied Policy
☐		192.168.1.100	3.7.2.1	Default Group	
☐		192.168.1.101	3.7.2.1	112334	

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

Management / All computers



All computers

[+ Add Computer](#) [Bulk Actions](#) ☐ Only show selected 

Filters   

☐	Computer Name	Group	Streamer Version	Policy Name	IP Address	Last Online	Notes	
☐		Default Group	3.7.2.1	My Policy	192.168.1.100	Online		
☐		112334	3.7.2.1	My Policy	192.168.1.101	Online	Hello world	

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?](#)

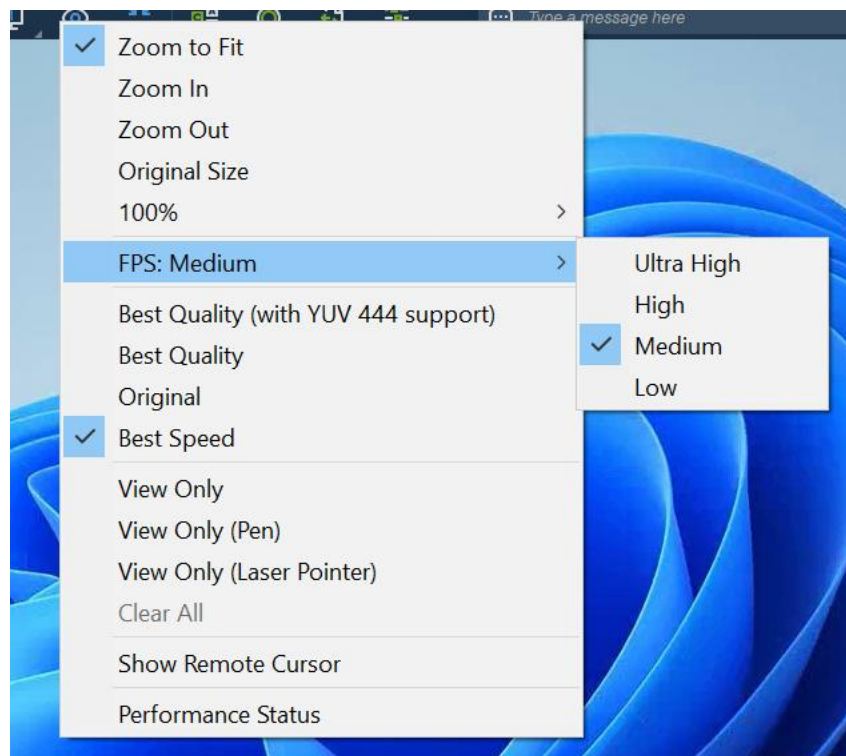
Add Deployment Package

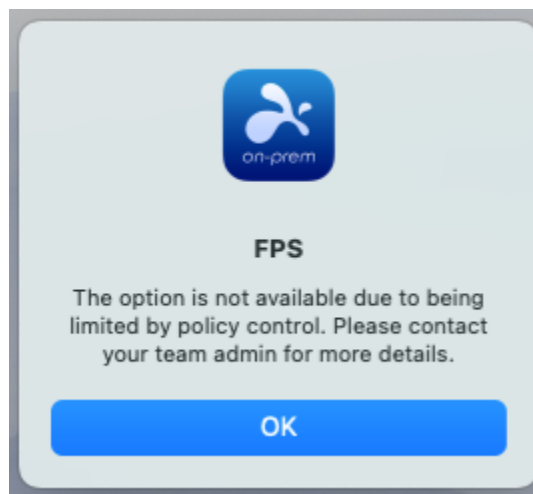
Package Name	Package name
Policy Name	Select a preference policy None Create preference policy

Behavior

- In-Session

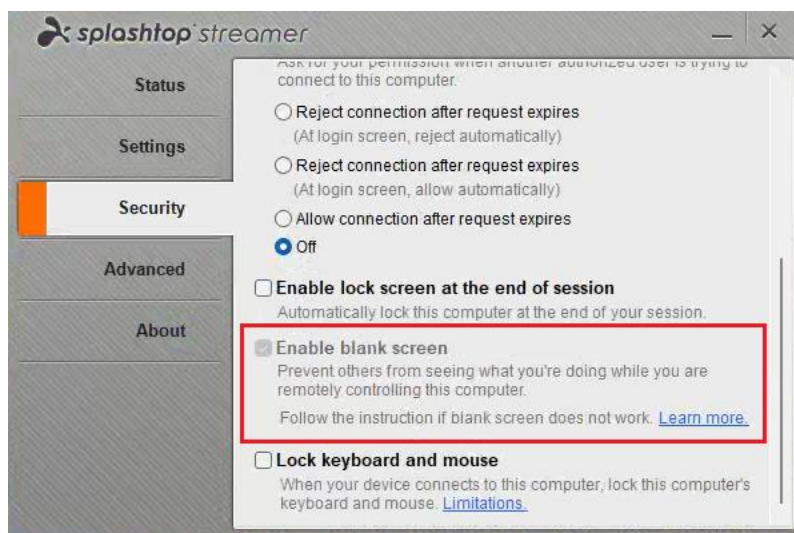
When a user remotes to a computer that associated to a preference policy, the configured settings or restrictions apply to the remote session. For example, if your policy restricts the FPS to High and the user tries to set it to Ultra High, an error message will pop-up.





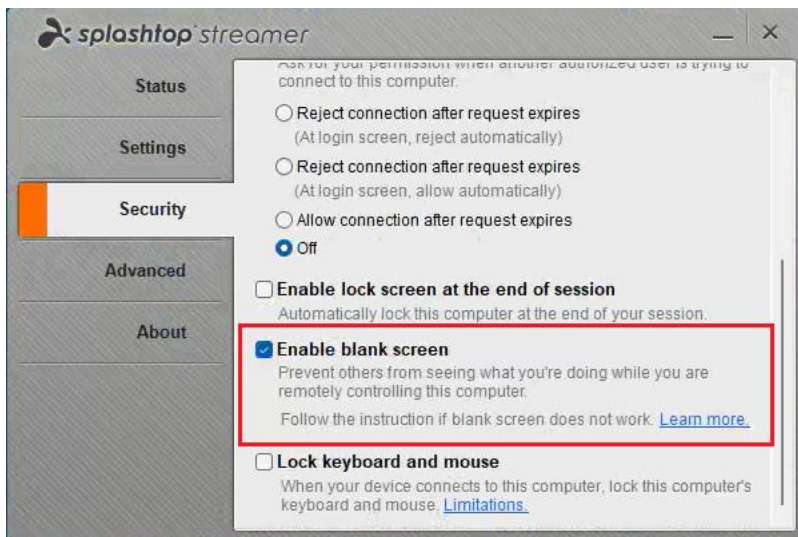
- Streamer

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.



Endpoints Management

Introduction to 1-to-Many Actions (Windows and Android)

1-to-many actions is a premium feature included with Splashtop On-Prem Gateway. Simplify endpoint management by instantly executing or scheduling tasks to multiple endpoints simultaneously. 1-to-many allows you to use the web console to select one of the below action types, set up an instant or scheduled action, and select which computers you would like to perform that action on.

Note: If you were using 1-to-Many features (e.g., Android APK install, File Dispatch). When you upgrade Gateway to v3.38.x or later, please follow the steps below to ensure these features continue functioning after the upgrade.

For online license users:

Go to System → License → Check Update to reactivate the feature.

For offline license users:

Please contact your sales representative to update your license file.

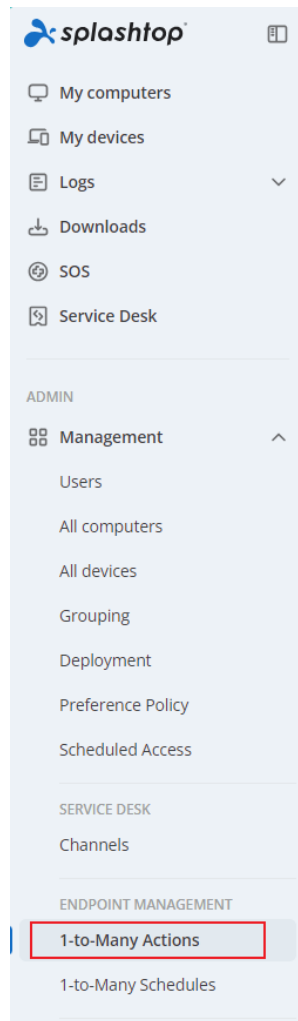
Security Requirements

1-to-Many Actions can take effect directly on deployed computers. To mitigate security risks, users must meet the following two requirements to use this feature

- You need to configure Two-Factor Authentication (2FA) and will be required to enter the 2FA code for the high-risk operations.
- Ensure your Streamers are deployed using the trusted SSL certificate.

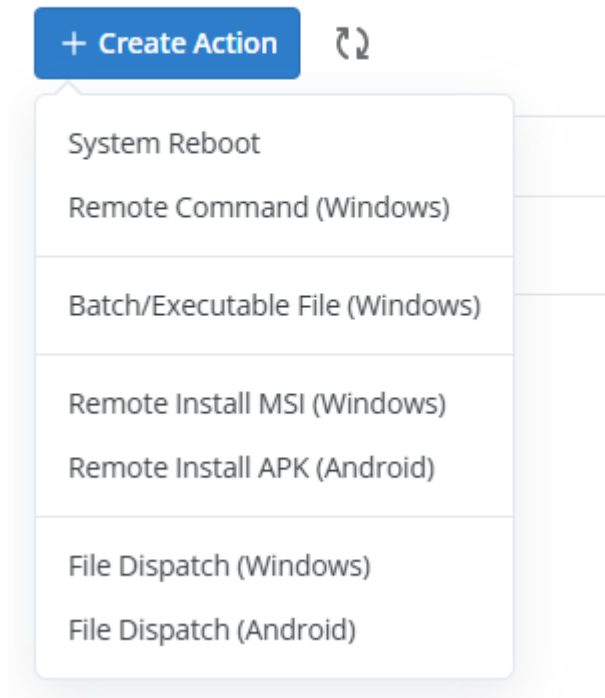
Working Flow

1. Log in to Gateway web console and select *Management > 1-to-Many Actions*.



2. Select Create Action and select which action you'd like to set up.

1-to-Many Actions



3. Set the Action Name and the Action Settings. Each 1-to-Many Action has different Action Settings to review.

File Dispatch (Windows)

 Actions will be executed across multiple computers. Confirm details before proceeding.

* Action Name

Test Action

Action Settings

* Default file path

C:\Documents

{filename}

☒ Create path if not already exists

☒ Overwrite identical files in destination path

* Upload files

 openAPI.yaml



 Customize file path

+ Add file

Allow up to 10 files to dispatch at a time.

Notes

Add your notes here

0/200

* Requires Streamer version 3.7.4.8 or higher.

Cancel

Save

Save and Schedule

Save and Run

4. Click Save and Run to set up for executing the action now. Click Save and Schedule to set up executing the action at a later time.

Cancel

Save

Save and Schedule

Save and Run

5. Select which computers you want to run the action on and select Enter Credentials and Run.
6. Enter Admin credentials for the computers. Verify the credentials on the computer by selecting the computer, clicking on Manage Credentials > Edit Credentials.

Manage Credentials ✕

Set up credentials to execute the action on each computer. The action will only be executed on computers with verified credentials.

Manage Credentials 1
☐ Only show no credentials yet

All Groups ▾ ⌵ 🔍

	Computer Name	Credentials	Status
▾	Default Group 2		
☒	 [blurred]	[blurred] 	✓ Verification success
☐	 [blurred]	[blurred] 	✗ No credentials or verification failed

System Reboot

Description

- This allows you to schedule a full system reboot for your computers.

Action Setup

- Action Name
 - Name this action instance.
- Action Settings
 - Notify remote computer XX minutes after reboot
- You have the option to send a notification to that computer 2-5 minutes before the action reboots the computer.
- Notes
 - If you would like to add any custom notes for this action.

System Reboot



 Actions will be executed across multiple computers. Confirm details before proceeding.

*** Action Name**

Test

Action Settings

Notify remote computer minutes before reboot

Notes

Add your notes here

0/200

* Requires Streamer version 3.3.6.0 or higher.

Cancel

Save

Save and Schedule

Save and Run

Remote Command (Windows)

Description

- This allows you to send a Command Prompt or PowerShell command to your computers.

Requirements

- Requires Windows Streamer version 3.7.4.8 or higher.
 - Action Setup
- Action Name
 - Name this action instance.
- Action Settings
 - Language
 - CMD
 - Powershell
 - Command
 - Note: Only use silent commands without user Interaction
 - Notes

Remote Command (Windows) ✕

 Actions will be executed across multiple computers. Confirm details before proceeding.

*** Action Name**

Test

Action Settings

Language

CMD

*** Command**

test commands

Only use silent commands without user interaction.

Notes

Add your notes here

0/200

* Requires Streamer version 3.7.4.8 or higher.

Cancel

Save

Save and Schedule

Save and Run

Batch/Executable File (Windows)

Description

- This allows you to deploy and install new software to your computers silently.

Requirements

- Requires Windows Streamer version 3.7.4.8 or higher.

Action Setup

- Action Name
 - Name this action instance.
- Action Settings
 - Upload File
 - NOTE: Must be .BAT, .CMD, .EXE format file
 - Size limit: 200 MB
 - Parameters
 - Command line parameters for silent install
 - Note: Uploaded file must execute in silent mode without user interaction.
 - Log source
 - Standard output and standard error
 - Custom log file
 - Notes

Batch/Executable File (Windows)



 Actions will be executed across multiple computers. Confirm details before proceeding.

* Action Name

Test

Action Settings

*Upload files

Select again



test.bat



Parameters

Uploaded file must execute in silent mode without user interaction.

Log source

☒ Standard output and standard error

☐ Custom log file

Notes

Add your notes here

0/200

* Requires Streamer version 3.7.4.8 or higher.

Cancel

Save

Save and Schedule

Save and Run

Remote install MSI (Windows)

Description

- This allows you to deploy and install/uninstall software via .MSI files to your computers silently.

Requirements

- Requires Windows Streamer version 3.7.4.8 or higher.

Action Setup

- Action Name
 - Name this action instance.
- Action Settings
 - Upload File
 - NOTE: Must be .MSI format file
 - Size limit: 1 GB
 - Parameters
 - Command line parameters for silent install
 - Note: *Uploaded file must execute in silent mode without user interaction.
 - Log source
 - Standard output and standard error
 - Custom log file
 - Notes

Remote Install MSI (Windows)



 Actions will be executed across multiple computers. Confirm details before proceeding.

* Action Name

Test

Action Settings

*Upload files

Select again

 test.msi 

Parameters

Uploaded file must execute in silent mode without user interaction.

☒ Install ☐ Uninstall

Log source

☒ Standard output and standard error

☐ Custom log file

Full Command

Msiexec.exe /i "test.msi" /q /! *v output.log

Notes

Add your notes here

0/200

Cancel

Save

Save and Schedule

Save and Run

Remote Install APK (Android)

Requirements

- Android Streamer v3.2.0 or higher.
- Remote control must be enabled for the Android devices.
- File dispatch only supports Android 10 and lower for now.

1. log in to Splashtop Gateway web console and select *Management > 1-to-Many Actions -> Create Action -> Remote Install APK (Android)*.

2. Action Settings

- Android APK File - Select a APK file
- Uninstall to clear storage data then fresh install - Select this option when there are old apps installed and you think there are insufficient space on your Android devices that may lead to installation failure. Only the target intall app will be affected.

3. Notes

- If you would like to add any custom notes for this action.

4 . Click Save and Run to set up for executing the action now. Click Save and Schedule to set up executing the action at a later time.

5. Select which Android Devices you want to run the action on and Run.

Remote Install APK (Android) ✕

 Actions will be executed across multiple computers. Confirm details before proceeding.

* Action Name

Test

Action Settings

*Upload files

Select again



☐ Uninstall to clear storage data then fresh install

Notes

Add your notes here

0/200

* Requires Android Streamer version 3.2.0 or higher.

Cancel

Save

Save and Schedule

Save and Run

File Dispatch (Windows)

Description

- This allows you to dispatch the files to your computers silently.

Requirements

- Requires Windows Streamer version 3.7.4.8 or higher.

Action Setup

- Action Name
 - Name this action instance.
- Action Settings
 - Default file path
 - Enter the default file path for your file dispatch.
 - Create path if not already exists - Determines whether new locations can be created on the target Android devices for the storage of dispatched files.
 - Overwrite identical files destination path - Determines whether to overwrite identical files on the target Android devices when dispatching files.
 - Upload files
 - Customize file path
 - Configure the specific file path for each file.
 - Allow up to 10 files to dispatch at a time.
 - Size limit: 1 GB
 - Notes

File Dispatch (Windows) ✕

 Actions will be executed across multiple computers. Confirm details before proceeding.

* Action Name

Test

Action Settings

* Default file path

C:\Documents

\{filename}

- ☒ Create path if not already exists
- ☒ Overwrite identical files in destination path

* Upload files

 test.txt 

 Customize file path

 Add file

Allow up to 10 files to dispatch at a time.

Notes

Add your notes here

Cancel

Save

Save and Schedule

Save and Run

File Dispatch (Android)

Requirements

- Android Streamer v3.2.0 or higher.

- Remote control must be enabled for the Android devices.
- File dispatch only supports Android 10 and lower for now.

1. log in to Splashtop Gateway web console and select *Management > 1-to-Many Actions -> Create Action -> File Dispatch (Android)*.

2. Up to 10 files can be added to in 1 action. The Destination path will be under Android primary external storage directory /sdcard/.

3. Action Settings

- Overwrite identical files destination path - Determines whether to overwrite identical files on the target Android devices when dispatching files.
- Create path if not already exists - Determines whether new locations can be created on the target Android devices for the storage of dispatched files.

4. Notes

- If you would like to add any custom notes for this action.

5. Click Save and Run to set up for executing the action now. Click Save and Schedule to set up executing the action at a later time.

6. Select which Android Devices you want to run the action on and Run.

File Dispatch (Android)



 Actions will be executed across multiple computers. Confirm details before proceeding.

* Action Name

Test

Action Settings

Default file path

/sdcard/

{filename}

- ☒ Create path if not already exists
- ☒ Overwrite identical files in destination path

* Upload files



Customize file path

+ Add file

Allow up to 10 files to dispatch at a time.

Notes

Add your notes here

0/200

Cancel

Save

Save and Schedule

Save and Run

Introduction to 1-to-Many Actions (Mac)

Starting from Gateway v3.40.3, MAC-based 1-to-many actions are supported. These actions require Mac Streamer version 3.8.0.7 or higher.

Security Requirements

1-to-Many Actions can take effect directly on deployed computers. To mitigate security risks, users must meet the following two requirements to use this feature:

- You need to configure Two-Factor Authentication (2FA) and will be required to enter the 2FA code for the high-risk operations.
- Ensure your Streamers are deployed using the trusted SSL certificate.

Shell Script (Mac)

Description

- This allows you to send a shell script to your Mac computers.

Requirements

- Requires Windows Streamer version 3.8.0.7 or higher.

Action Setup

- Action Name
 - Name this action instance.
- Assign Group Admin
 - If you would like to assign this action to a specific group admin to make them the action owner.
- Action Settings
 - Shell Script:
 - NOTE: Only use silent commands without user interaction.

- Notes
 - Add your notes here.

Shell Script (Mac)



 Actions will be executed across multiple computers. Confirm details before proceeding.

*** Action Name**

Shell Script (Mac)

Assign Group Manager

None

Action Settings

*** Shell Script**

Only use silent commands without user interaction.

Only use silent commands without user interaction.

Notes

Add your notes here



0/200

* Requires Streamer version 3.8.0.7 or higher.

Cancel

Save

Save and Schedule

Save and Run

Script/Executable File (Mac)

Description

- This allows you to deploy new software or scripts to your Mac computers silently.

Requirements

- Requires Windows Streamer version 3.8.0.7 or higher.

Action Setup

- Action Name
 - Name this action instance.
- Assign Group Admin
 - If you would like to assign this action to a specific group admin to make them the action owner.
- Action Settings
 - Upload File
 - NOTE: Must be .pkg, .py or Shell script format file.
 - Log source
 - Standard output and standard error
 - Custom log file
- Notes
 - Add your notes here.

Script/Executable File (Mac)



 Actions will be executed across multiple computers. Confirm details before proceeding.

*** Action Name**

Action Name

Assign Group Manager

None

Action Settings

***Upload files**

+ Add file

pkg, .py or Shell script.

Parameters

Uploaded file must execute in silent mode without user interaction.

Log source

☒ Standard output and standard error

☐ Custom log file

Notes

Add your notes here

0/200

* Requires Streamer version 3.8.0.7 or higher.

Cancel

Save

Save and Schedule

Save and Run

File Dispatch (Mac)

Description

- This allows you to dispatch the files to your computers silently.

Requirements

- Requires Windows Streamer version 3.8.0.7 or higher.

Action Setup

- Action Name
 - Name this action instance.
- Action Settings
 - Default file path
 - Enter the default file path for your file dispatch.
 - Create path if not already exists
 - Automatically generates any missing folders in the destination path to ensure the file can be placed correctly.
 - Overwrite identical files destination path
 - Replaces any file at the target location with the same name, even if the content is identical.
 - Change ownership
 - Modifies the file's user ownership to a specified owner account on the system.
 - Change group
 - Assigns a specific group to the file, determining access permissions for members of that group.
 - Change permission

- Sets specific read, write, and execute access rights for the owner, group, and others.
- Upload files
 - Customize file path
 - Configure the specific file path for each file.
 - Allow up to 10 files to dispatch at a time.
 - Size limit: 1 GB
- Notes
 - Add your notes here.

File Dispatch (Mac)



 Actions will be executed across multiple computers. Confirm details before proceeding.

*** Action Name**

Action Name

Assign Group Manager

None

Action Settings

*** Default file path**

/System/Library/

{filename}

- ☒ Create path if not already exists
- ☒ Overwrite identical files in destination path
- ☐ Change ownership
- ☐ Change group
- ☐ Change permission

*** Upload files**

+ Add file

Allow up to 10 files to dispatch at a time.

Notes

Add your notes here

0/200

* Requires Streamer version 3.8.0.7 or higher.

Cancel

Save

Save and Schedule

Save and Run

OS Patch (Computer View)

Introduction

The **OS Patch (Computer View)** page allows you to manage operating system updates for Windows devices directly from the computer view. For a broader overview of patch status across your team, see [Patch View](#).

We currently support **Critical, Important, Optional, and Feature** updates as well as full system upgrades.

Requirements

Platform	Streamer Version	Supported OS Versions	Notes
Windows	v3.8.0.7 and up	Windows 7 and newer	Windows 10+ cannot use the Windows API to set update policies. Only Professional or higher editions can modify Group Policy for update control.

Instructions

Default schedule

- Log in to Gateway web portal and navigate to **Settings > Team Settings > Endpoint management**.

Endpoint management

Computer Inventory	
OS patch Detailed settings	

- Configure the default scan schedule by selecting a Daily, Weekly, or Monthly frequency, along with your preferred day and time. The Streamer will then perform scans accordingly.
- Configure the default install schedule by selecting a Daily, Weekly, or Monthly frequency, along with your preferred day and time. The Streamer will automatically install approved patches accordingly.

OS patch default schedule

- Requires Streamer version 3.8.0.7 or above.
- Randomize the scan/install time within 30 minutes after the scheduled time.

Scan Schedule

Set the default scan schedule to your preferred time so the Streamer can report patch information.

Mode	Time
Daily	02:00 

(Local computer time)

Install Schedule

Set the default install schedule to your preferred time so the Streamer can install **approved** patches.

Mode	Day Choice	Time
Weekly	Saturday, Sunday 2	02:00 

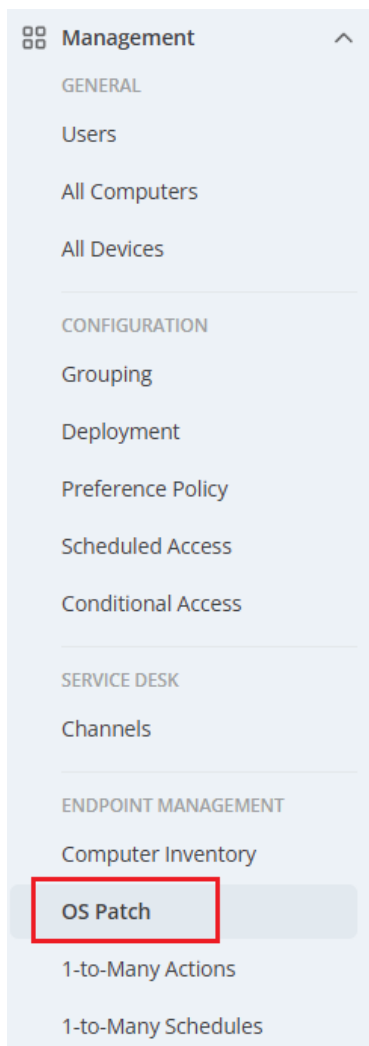
(Local computer time)

Cancel

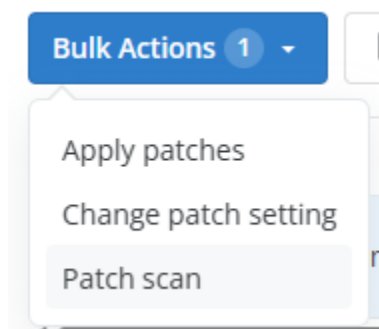
Save

Scan and apply OS patches

- Log in to Gateway web console and navigate to **Management > OS Patch > Computers**.



- Select the computers you would like to check, or select all, then click **Bulk Actions > Patch scan**.



- Click **OK** to continue.
- After scanning, select the computers and click **Bulk Actions > Apply patches** to apply patches.
- On the page that appears, select the patches you would like to apply, and click **Next** to continue.

Apply Patches

Apply 3 selected patch(es) for 1 computer(s).

 Search

☒	Patch	KB	Important	Category	Reboot	Computer
☒	MS16-016	1,024 KB	High	Security	Yes	Computer 1
☒	MS16-017	1,024 KB	High	Security	Yes	Computer 1
☒	MS16-018	1,024 KB	High	Security	Yes	Computer 1

- You will see the options below:

Apply Patches

*Processing time varies based on online computers and system workload.

Apply **3** selected patch(es) for **1** computer(s).

Install Patches

☒ Immediately after the patches have been downloaded

☐ Attempt to install between -

Reboot Computer (if required)

☒ Immediately after patches are installed

☐ At the computer's local time:

☐ On the date:

Notify User

Warn logged-on user before restart computer:

- **Install Patches:**
 - Choose to install the patches immediately after the patches have downloaded, or during a specific date range.
- **Reboot Computer:**
 - Choose to reboot the computer immediately after the patch is installed, or at a certain time after the patch is installed.
- **Notify User:**
 - **Warn logged-on user before restart computer:** You have the option to send a notification to that computer 3-120 minutes before the patch reboots the computer if a user is logged in.

Change patch setting

Enhanced Update Control

For **Windows** streamer version 3.8.0.7 and higher, ticking Enhanced Update Control will ensure correct control of Windows updates on Windows 10 and 11 by utilizing GPO (Group Policy).

Supported Editions for Windows update on Windows 10 and 11 by utilizing GPO (Group Policy):

- Windows Pro Edition
- Windows Enterprise and Education Editions
- Windows Server Editions

Change Patch Setting ✕

Processing time varies based on online computers and system workload.

☐ **Enhanced Windows Update Control**

Enable this option to utilize GPO (Group Policy Object), which ensures correct control of Windows update behavior on Windows 10 and 11.

Patch Setting

Let OS install patches automatically ▼

Restart the computer when a patch requires a reboot to take effect: **Monday** ▼ **00:00** ▼

☐ **Include patches for other Microsoft products**

Selected Computers



Patch Setting

There are 3 patch settings you can pick from:

1. Let OS install patches automatically
2. Download patches but let me choose whether to install them
3. Scan patches but let me choose whether to download and install them

If you select "**Let OS install patches automatically**", you can choose **one day/every day** and what hour to reboot the computer to install pending patches.

Patch Setting

Download patches but let me choose whether to install them

Let OS install patches automatically

Download patches but let me choose whether to install them ✓

Scan patches but let me choose whether to download and install them

For Windows devices, there is also an option to include patches for other Microsoft Products supported by Windows Updates.

Patch Setting

Download patches but let me choose whether to install them

☒ Include patches for other Microsoft products

Filtering and searching

Filters: Sort patches by:

- **Group:** All Groups, Default Group.
- **Patch Status:** Up to Date, Important Patches Pending, Optional Patches Pending, Patching in Progress, Reboot Required, Never Scan for Patches, and Scanning.

Search:

You can search for computers by computer name, group name, patch setting, and OS information.

Computer property

- Log in to Gateway web console and navigate to **Management > All Computers > Gear button > Properties > Patches**. From here, you can manage the patches by viewing details, scanning, and applying patches.

Management / [All Computers](#) / OS Patch

General **Patches** Inventory User list

OS Version Windows 11 Enterprise 64-bit 24H2 (10.0.26100.7840)
Last Patched 2026-02-27 09:37:54 [Patch history](#)
Status Ready
Patch Setting Let OS install patches automatically

Patch [Patch scan](#) (Last Scan Time: 2026-02-26 11:07:42)
☒ Include patches for other Microsoft products

[Apply Patches](#)

☐	Patch	KB	Important	Category	Reboot	Size
☐	KB2026-02-27 09:37:54					
☐	KB2026-02-27 09:37:54					
☐	KB2026-02-27 09:37:54					

OS patch logs

Log in to Gateway web console and navigate to **Logs > OS Patch**. You can view the patch install requests and click the **Details** icon to view the specific results.

Logs / OS Patch

9

OS Patch

[Refresh](#) Last 7 Days

Computer Name	Group	Requested by	Requested at	Status	Success	Failure	Details
qa	Default Group			Waiting for installation	0	0	
qa	Default Group			Complete	2	0	
qa	Default Group			Complete	2	0	
qa	Default Group			Waiting for installation	0	0	
qa	Default Group			Waiting for installation	0	0	
qa	Default Group			Waiting for installation	0	0	
qa	Default Group			Waiting for installation	0	0	
qa	Default Group			Waiting for installation	0	0	
qa	Default Group			Complete	0	0	
qa	Default Group			Complete	1	0	

Patch history for qa

The patches on 2026-02-27 (4 success, 0 failure)

Status

Complete

Requested by

Requested by [redacted] at 2026-02-27 11:11:53 (UTC +08:00)

Success: 4, Failure: 0

Patch	KB	Important	Category	Result
[redacted]	[redacted]	[redacted]	[redacted]	Success
[redacted]	[redacted]	[redacted]	[redacted]	Success
[redacted]	[redacted]	[redacted]	[redacted]	Success
[redacted]	[redacted]	[redacted]	[redacted]	Success

OK

Note: This feature is available from Gateway v3.40.1 and later.

OS Patch (Patch View)

Introduction

The **OS Patch (Patch View)** page provides a centralized interface for managing operating system updates for Windows devices. Unlike the [Computer View](#), which focuses on individual device updates, the Patch View allows for bulk management, enabling administrators to oversee patches across multiple devices efficiently.

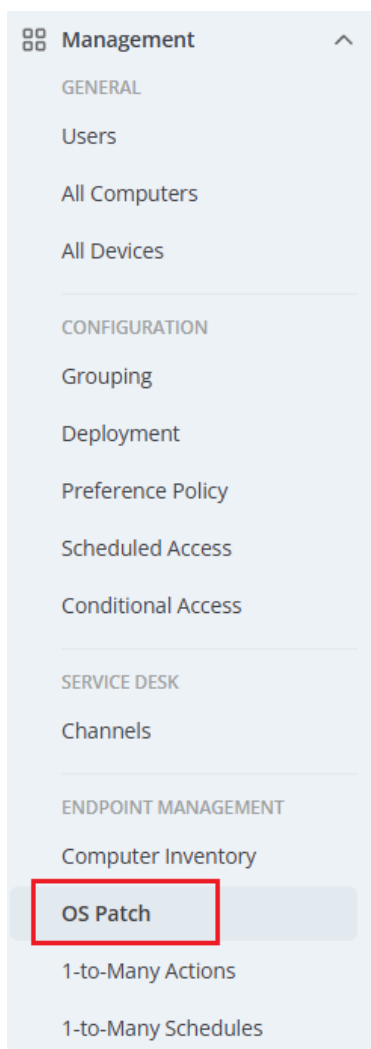
Requirements

Platform	Streamer Version	Supported OS Versions	Notes
Windows	v3.8.0.7 and up	Windows 7 and newer	Windows 10+ cannot use the Windows API to set update policies. Only Professional or higher editions can modify Group Policy for update control.

Instructions

Accessing OS patch (Patch View)

- Log in to Gateway web console and navigate to **Management > OS Patch > Patches**.



- The page will display lists of updates under various statuses: Pending, Approved, Failed, Installed, Ignored, and Expired.

Management / OS Patch (Patches) 6

Patches Computers

OS Patch   1

Approve and monitor patches here. [How to setup](#)

Pending 3 Approved 0 Failed 0 Installed 0 Ignored 0 Expired 0

Bulk Actions ☐ Only show selected Filters Q

☐	Patch	KB	Important	Category	Reboot	Release Date	Size	Computers
☐	Microsoft Windows 10 KB4013218	1.5 MB		Windows 10		10/10/2018	1.5 MB	1
☐	Microsoft Windows 10 KB4013218	1.5 MB		Windows 10		10/10/2018	1.5 MB	1
☐	Microsoft Windows 10 KB4013218	1.5 MB		Windows 10		10/10/2018	1.5 MB	1

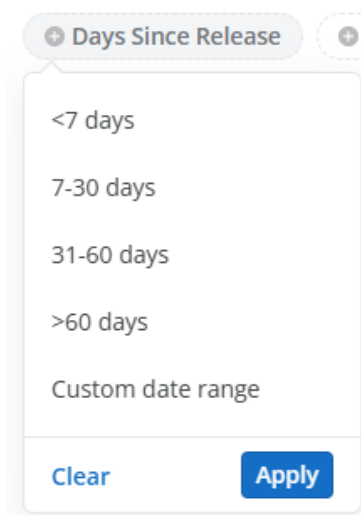
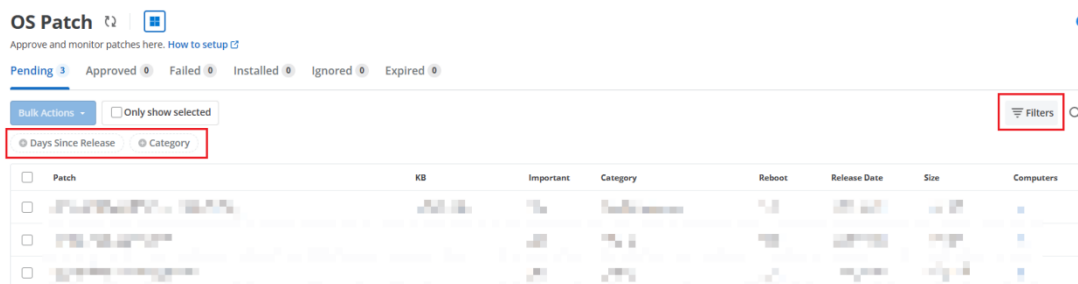
Managing patches

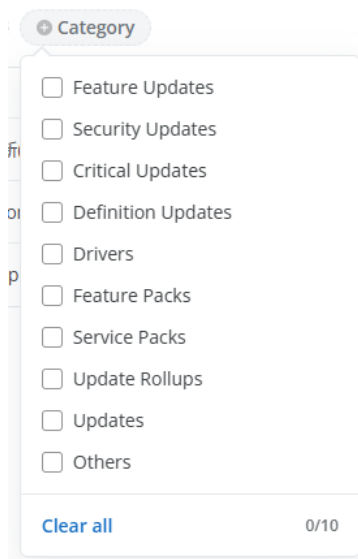
The available actions vary depending on the tab. No actions are available in the **Installed** tab and **Expired** tab.

- **Tabs Representing Different Status:**
 - **Pending:** Lists available patches awaiting action.
 - **Approved:** Patches approved for installation at the scheduled time.
 - **Failed:** Patches that failed during installation and can be retried.
 - **Installed:** Patches that have been successfully installed.
 - **Ignored:** Patches that have been excluded from installation.
 - **Expired:** Patches that can't be installed because they're no longer available.
- **Available Actions:**
 - **Approve/Approve Again:** Select patches and click **Approve** to move them to the **Approved** tab. These patches will be installed at the scheduled time.
 - **Ignore:** Exclude specific patches from installation by clicking **Ignore**.
 - **Apply Patches:** Install selected patches.
- **Actions by Tab:**
 - **Pending tab:** You can **Approve**, **Ignore**, or **Apply Patches** for the pending patches.
 - **Approved tab:** You can **Ignore**, or **Apply Patches** for the approved patches.
 - **Failed tab:** You can **Approve again**, or **Apply Patches** for the failed patches.
 - **Ignored tab:** You can **Approve**, or **Apply Patches** for the Ignored patches.

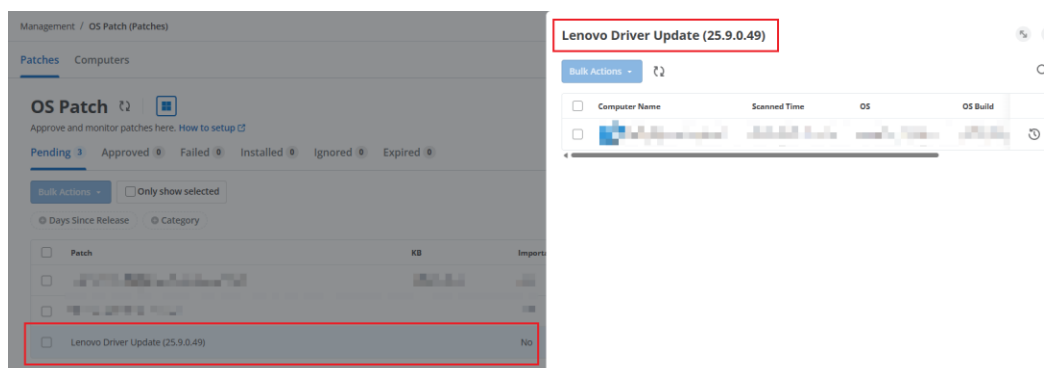
Filtering, searching, and viewing patches

- **Filters:** Sort updates by:
 - **Days since Release:** <7 days, 7-30 days, 31-60 days, >60 days, and custom date range.
 - **Category:** All, Feature Updates, Security Updates, Critical Updates, Definition Updates, Drivers, Feature Packs, Service Packs, Update Rollups, Updates, Others.





- **Search:**
 - You can search for patches by patch name, KB number, and category.
- **Viewing Patches:**
 - Click any patch to view affected computers. From the details drawer, you can perform bulk actions for that specific patch.



Limitation

OS patch records older than 3 months will be deleted. You can scan your computer again to obtain the latest patches.

Note: This feature is available from Gateway v3.40.1 and later.

Endpoint Policy

To meet the growing demand for comprehensive endpoint management, Endpoint Policies will streamline the process to manage settings for a large number of computers with centralized policy control and cover various configurations to apply seamlessly across endpoints.

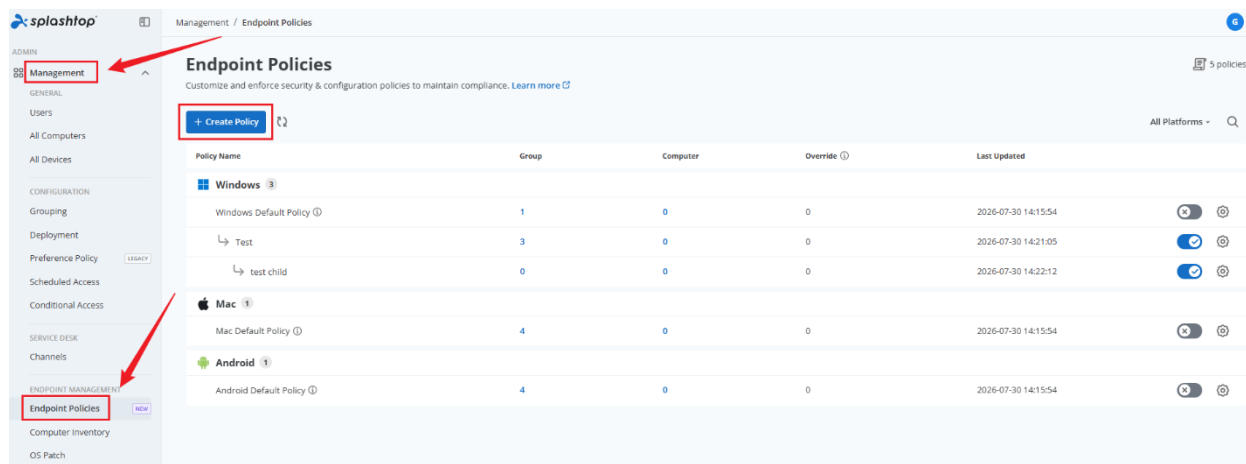
Policies are classified by platform and can be applied per computer or per group. Each team will have a default policy with all feature categories disabled and no pre-configured settings.

Instructions

Creating and editing policies

Creating policies

Log in to Gateway web portal and navigate to **Management > Endpoint Policies**.

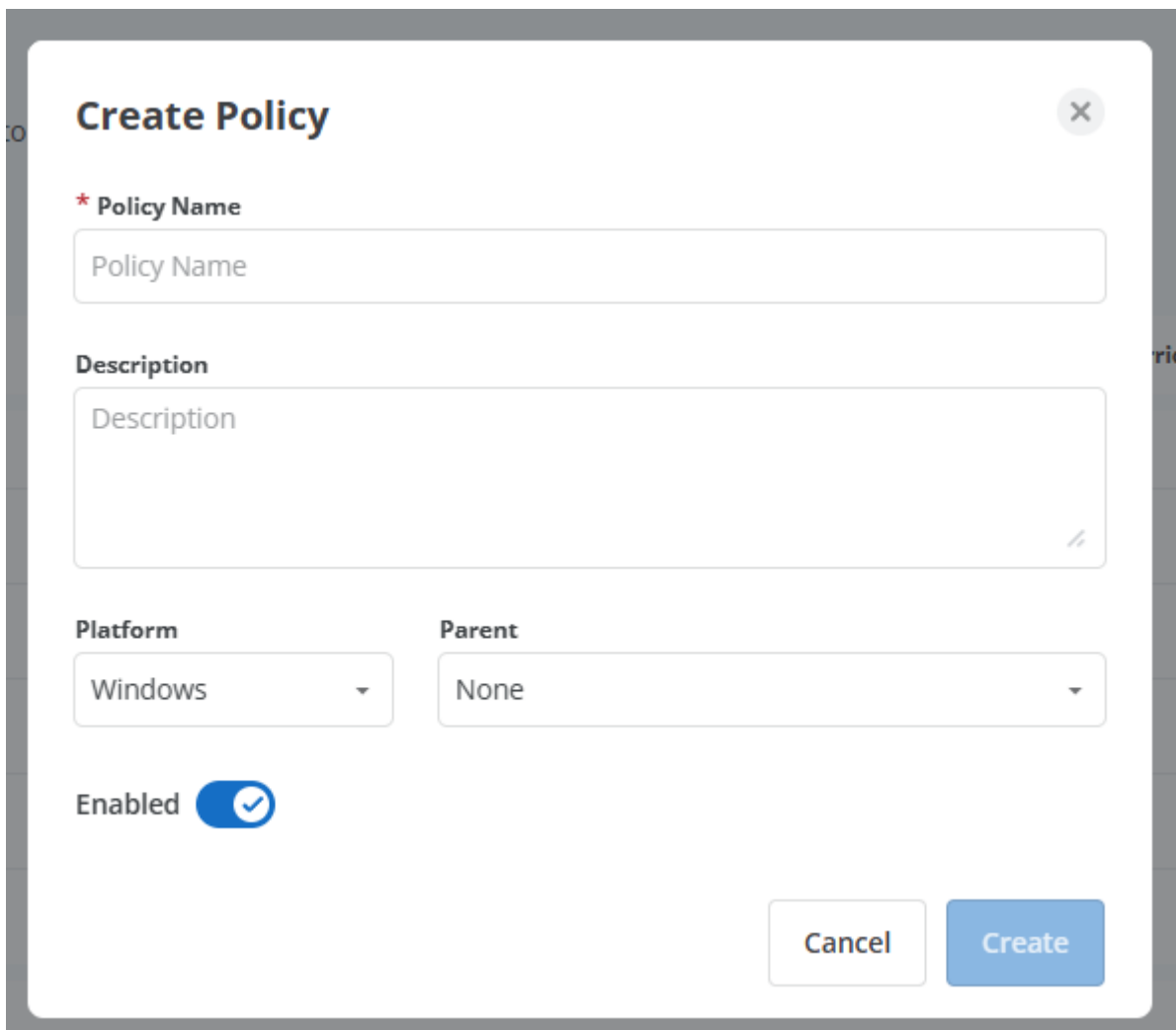


The screenshot shows the Splashtop Management interface. On the left, the 'Management' menu item is selected, and 'Endpoint Policies' is highlighted under the 'Endpoint Management' section. The main area displays the 'Endpoint Policies' page, which includes a '+ Create Policy' button and a table of existing policies.

Policy Name	Group	Computer	Override	Last Updated	
Windows					
Windows Default Policy	1	0	0	2026-07-30 14:15:54	
↳ Test	3	0	0	2026-07-30 14:21:05	
↳ test child	0	0	0	2026-07-30 14:22:12	
Mac					
Mac Default Policy	4	0	0	2026-07-30 14:15:54	
Android					
Android Default Policy	4	0	0	2026-07-30 14:15:54	

Click **Create Policy**, edit the policy name (up to 64 characters) and description (up to 256 characters), select a **Platform**, and choose a **Parent**. Policies can be created as enabled or disabled.

Click on **Create**.



Create Policy ✕

*** Policy Name**

Policy Name

Description

Description

Platform **Parent**

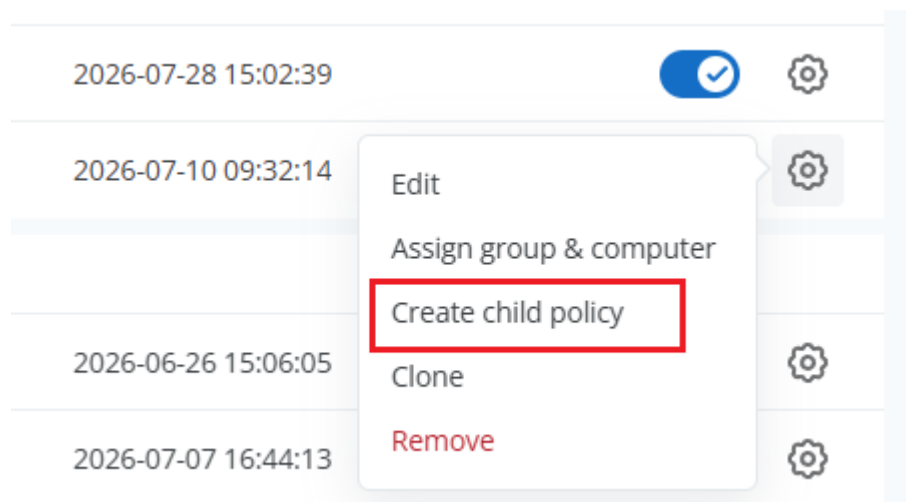
Windows None

Enabled ☒

Cancel Create

Creating child policies

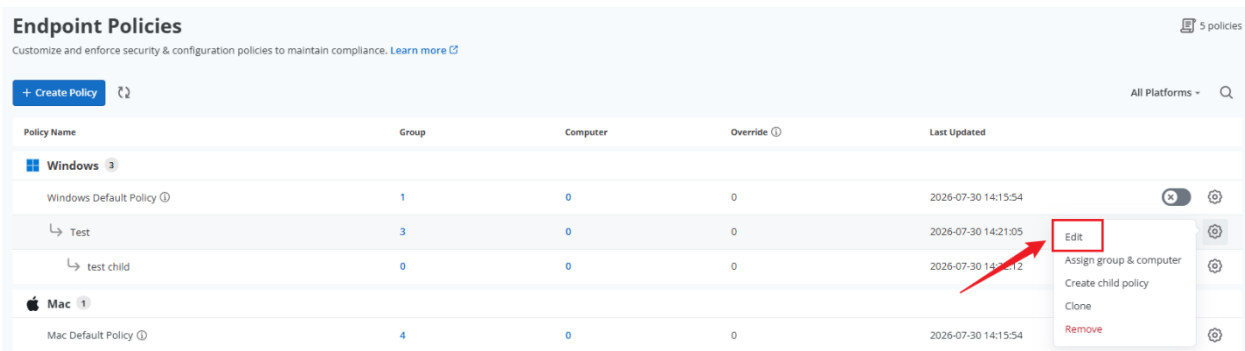
To create a child policy, choose a **Parent Policy** when creating a new policy, or select the parent policy and, in the right-side options, select **Create child policy**.



A policy tree can contain up to 5 levels.

Editing policies

To edit existing policies, select **Edit**.



For new and existing policies, select the features you would like to add to the policy. By default, features are disabled. Manually enable them as required.

Windows

PM-test



Streamer Settings

- Requires Streamer version 3.8.4.7 or above.
- Streamer settings configured here will take priority over the legacy Preference Policy. [Learn more](#) 

General

☒ **Idle session timeout**

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

0

☐ **Hide Streamer tray icon**

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

Disabled

☒ **Direct connection**

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

Enabled

Enabled

Disabled

☐ **Sound**

☒ Output sound over the remote connection only.

☐ Output sound over the local computer only.

☐ Output sound both over the remote connection and on the local computer.

Policy Inheritance

Policies support inheritance, allowing you to create a parent policy with standard settings and child policies that inherit these settings.

If you need to modify a basic setting for the entire group, update the parent policy. All child policies will automatically receive these updates from the main policy.

Policy override

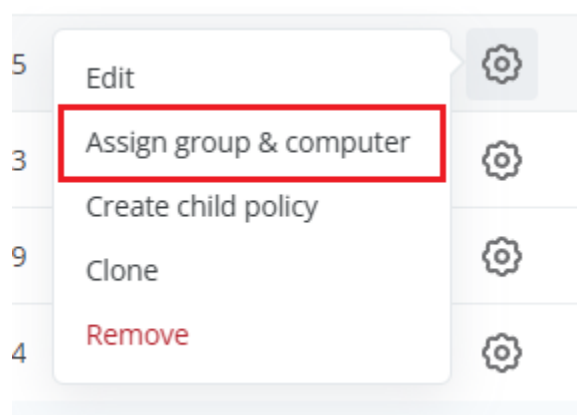
When you need different settings for just a few computers within a group, you can create a child policy and override specific settings. An override changes the configuration only for the selected computers, while all other computers in the group continue to follow the original policy. This gives you precise control over individual endpoints without disrupting the overall policy structure.

When creating child policies, if a setting from the parent policy is changed in the child policy, the setting in the child policy will be marked as **overridden**.

Additionally, each setting can be overridden at a computer level under the **Properties** page.

Assigning policies

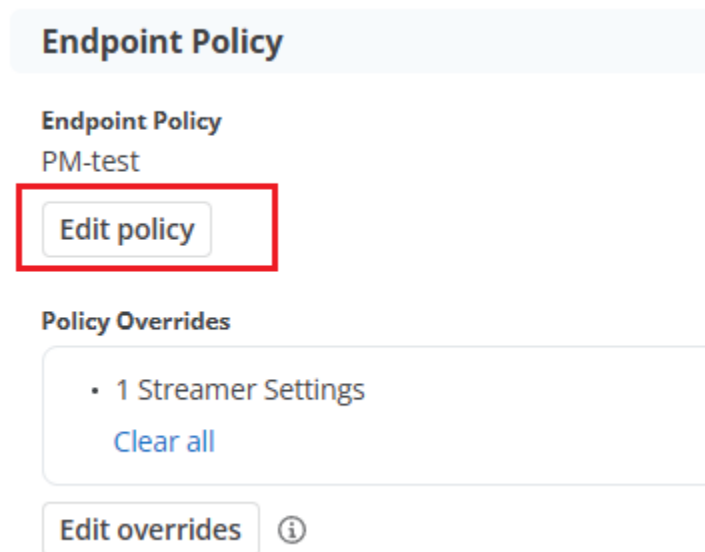
There are different ways to assign policies to computers and groups. First, from the **Endpoint Policies** page, click on the policy and select **Assign group and computer**. Select the group or computer, and click on **Assign**.



Assign a policy to a computer

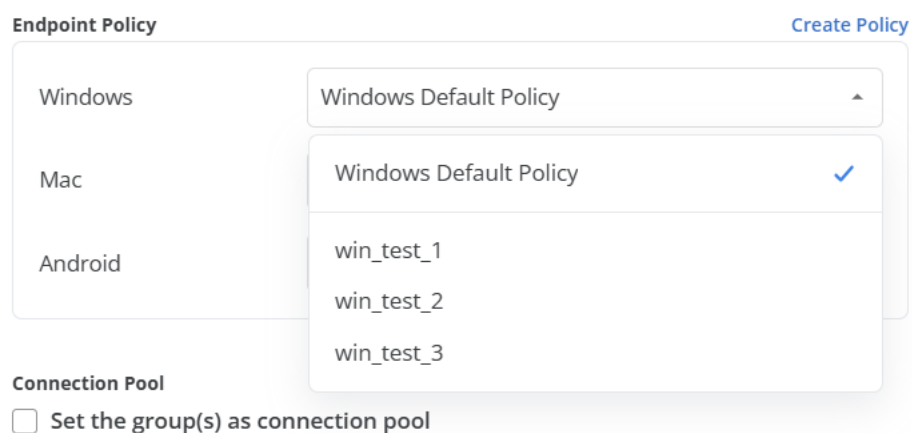
The default setting of each computer is to "Follow Group".

Individual computer policies can be edited/overridden. To do this, go to the **Computers** tab, and on the device you want to assign a policy to, click on **Properties**. In the **Endpoint Policy** section, click on **Edit policy** and select a policy.



Assign a policy to a group

To assign a policy to a group, go to **Management** → **Grouping**. Create or edit a group and select the policy.



Cloning policies

To quickly create a new policy based on an existing one, select a policy and choose **Clone**. The cloned policy keeps the same platform as the original (this cannot be changed) and copies over its settings. You can adjust the name, description, and parent. Once you click **Clone**, the new policy is created successfully.

Removing policies

When removing a policy, the associated group's policy will roll back to the platform default policy and its associated computers will fall back to "Follow Group".

All overrides on Computers will be deleted.

NOTE: Parent policies with child policies cannot be deleted.

Streamer settings

You can edit the following configurations in an Endpoint Policy. There is a new configuration - File transfer. This acts as the final gate for file transfer during a remote session—when disabled, it turns file transfer off even if the user's granular control allows it.

General

☒ **Idle session timeout**

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

0

☐ **Hide Streamer tray icon**

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

Disabled

☐ **Direct connection**

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

Enabled

☒ **Sound**

Remote Only

☒ Output sound over the remote connection only.

☐ Output sound over the local computer only.

☐ Output sound both over the remote connection and on the local computer.

☐ **Lock Streamer name**

Streamer name will be locked across the On-Prem app and the web console.

☐ **Sync with OS hostname**

Streamer name will be synchronized with the OS hostname.

Disabled

Security

☐ Blank screen when in a session Prevent others from seeing what is on the remote screen while you are remotely controlling this computer.	Disabled ▾
☐ Lock screen when disconnected Automatically lock the computer at the end of the session.	Enabled ▾
☐ Lock keyboard and mouse when in a session When your device connects to the computer, lock the computer's keyboard and mouse.	Disabled ▾
☒ Lock Streamer settings using Splashtop admin credentials By default, Streamer settings can be modified by anyone with Windows or Mac admin account. By checking this option, Streamer settings will be locked and can only be unlocked by admins on your Splashtop team.	Disabled ▾

Capability Control

☒ File transfer Manage file transfer capability between local and remote devices. If you have enabled file transfer from Team settings or user granular control, this can override the setting when connecting to computers assigned to this policy.	Disabled ▾
--	------------

Bandwidth Management

☐ Maximum FPS Option The maximum available FPS option when connecting to the computer. By configuring this policy, you can manage the consumed network bandwidth from the computer.	High ▾
☐ Maximum Audio Quality Option The maximum available audio option when connecting to the computer. By configuring this policy, you can manage the consumed network bandwidth from the computer.	Medium ▾

Note:

- This feature is available from Gateway v3.42.0 and later.
- This feature requires Streamer v3.8.4.7 for Windows, Mac, and Android platforms.
- **Endpoint Policies** takes priority over the legacy Preference Policy and is where all new controls will be added, so configure each setting there rather than in both.

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.

Settings / Authentication

[Single Sign-On](#) AD Authentication

General Settings

SSO Name * SSO method name for display purpose

Notes

Identity Provider Settings

Please copy these configurations or download the Service Provider Metadata to create a custom app in your Identity Provider. [Download](#)

Entity ID onpremise.splashtop.com

Assertion consumer service URL https://test.gatewayaddr.com:443/api/saml/acs

Service Provider Settings

Protocol SAML 2.0

IDP type ADFS

☐ Enable force authentication
Enable this item to require SSO users to re-login to the IDP each time.

☐ Enable login hint
Enable this item to pre-fill the SSO user name in IDP.

Metadata ☒ Import an XML file ☐ Import from URL ☐ Add manually

XML file * Select XML file. [Select](#)

[Save](#)

[Back](#)

- **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.

Default	SSO Name ↑	Protocol	IDP Type	Status	Device Authentication	Browser Authentication	
☒	ADFS	SAML 2.0	ADFS	✓	☒	☒	⚙️
☐	ADFS 2	SAML 2.0	ADFS	✓	☐	☒	⚙️
☐	Okta	SAML 2.0	Okta	✓	☐	☒	⚙️

- 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.

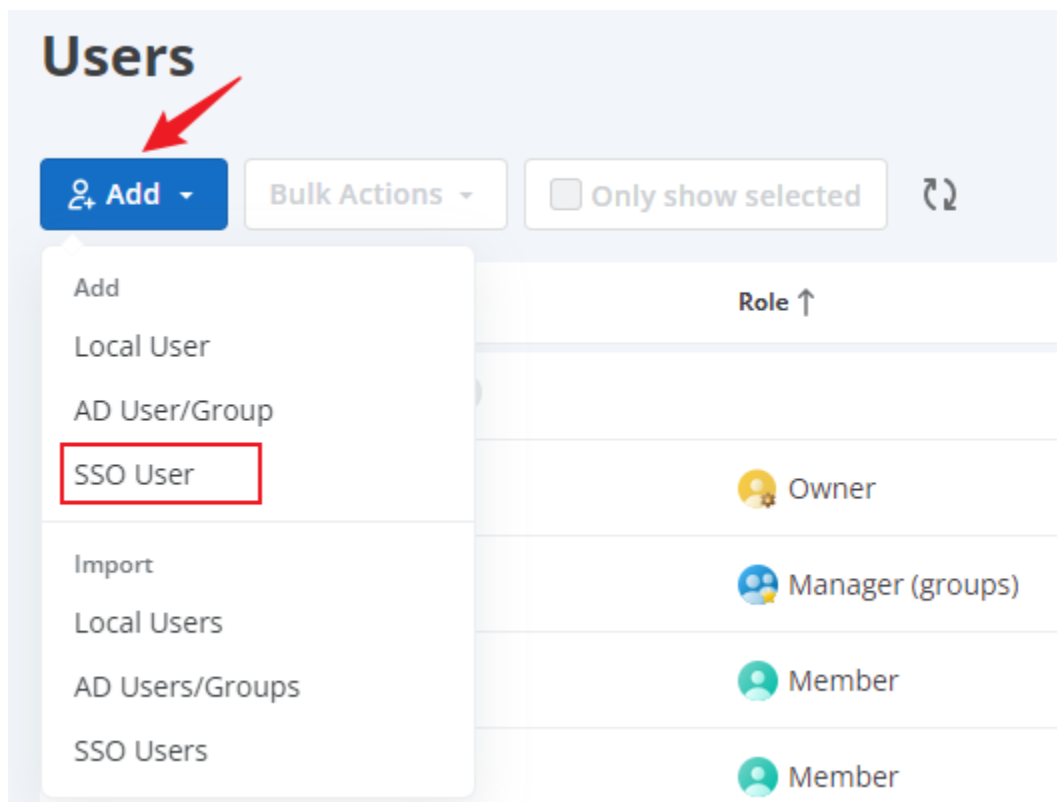
Requirements

- **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 **Add** 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 User

* Account

user@example.com

Authentication

SSO-Marketing-EU

Group

Default Group

Role

Member

Status

☒ Enable user

☒ Enable web access

SOS Technician

☐ Enable SOS

Cancel

Add

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**.

Users

 **Add** **Bulk Actions** ☐ Only show selected 

- Add
- Local User
- AD User/Group
- SSO User
- Import
- Local Users
- AD Users/Groups
- SSO Users**

	Role ↑	Source
 Owner		Local
 Manager (groups)		Local
 Member		Local
 Member		Local

Import SSO Users ✕

*** Upload CSV file** [Download example](#)

Select file

Drag and drop file here to upload

Authentication

SSO-Marketing-EU

Group

Default Group

Email notification

☐ Enable email notification

Status

☒ Enable users ☒ Enable web access

SOS Technician

☐ Enable SOS

You have successfully imported 1 users at 2024-10-31 15:25:26. Visit the [last imported report](#).

- **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.

Import SSO Users Report ×

Account ↑	Status
admin@domain.com	✓ Success
admin@domain.com	✓ Success
admin@domain.com	✓ Success
admin@domain.com	✓ Success
admin@domain.com	✓ Success
admin@domain.com	✓ Success

Success: 6, Failure: 0

CloseDownload 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.

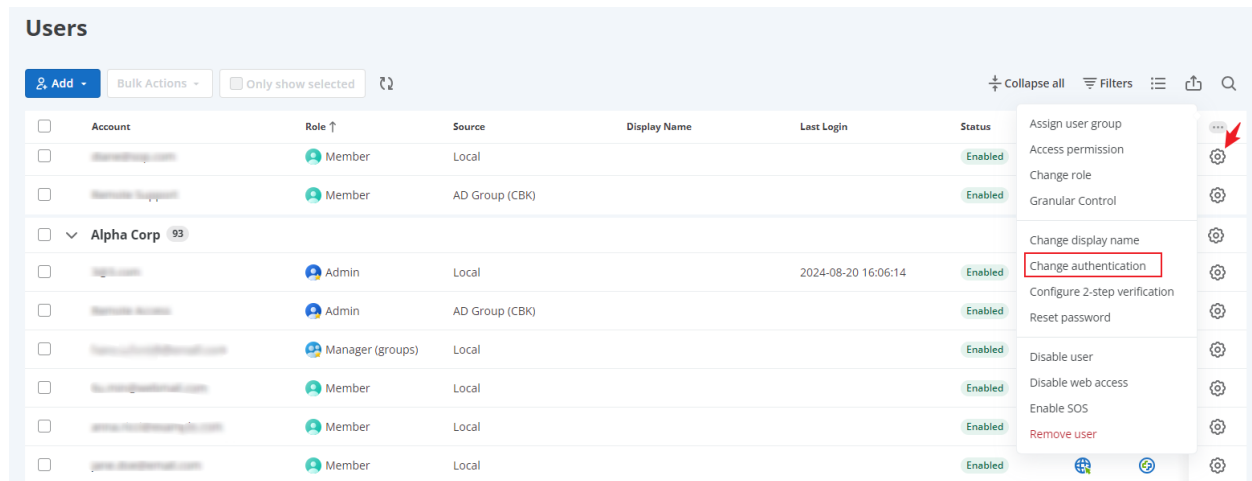
How to associate SSO method to existing team admin/member?

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**.



Users

Buttons: Add, Bulk Actions, Only show selected

Table Headers: Account, Role, Source, Display Name, Last Login, Status

Account	Role	Source	Display Name	Last Login	Status	Actions
...	Member	Local			Enabled	Assign user group, Access permission, Change role, Granular Control
...	Member	AD Group (CBK)			Enabled	
Alpha Corp (93)						Change display name, Change authentication , Configure 2-step verification, Reset password
...	Admin	Local		2024-08-20 16:06:14	Enabled	Disable user, Disable web access, Enable SSO, Remove user
...	Admin	AD Group (CBK)			Enabled	
...	Manager (groups)	Local			Enabled	
...	Member	Local			Enabled	
...	Member	Local			Enabled	
...	Member	Local			Enabled	

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

Change Authentication Method

Authentication

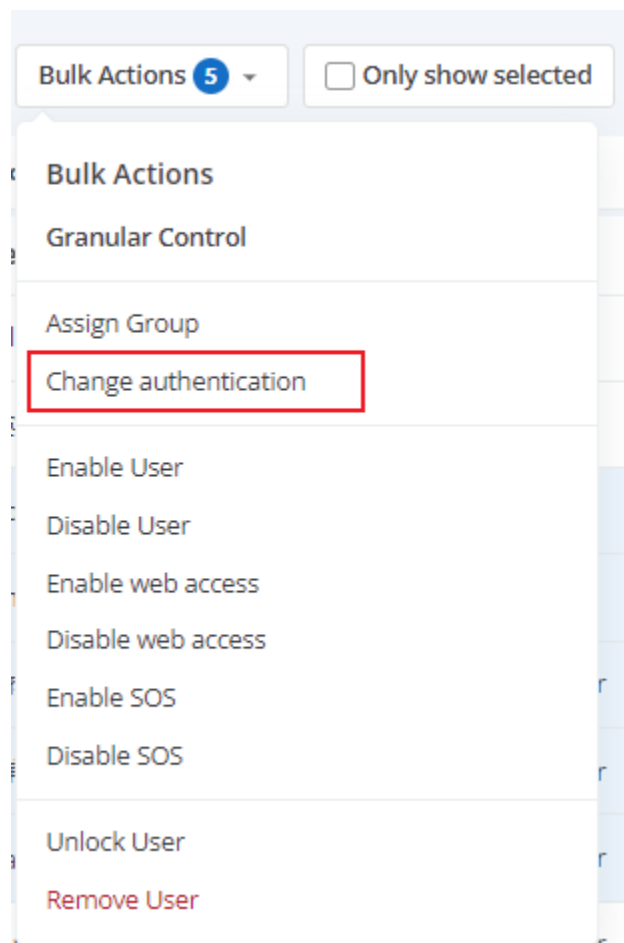
SSO-Marketing-EU

Password for Gateway account

SSO-Marketing-EU



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.



Change Authentication Method ✕

You are changing **5** selected user(s) to a new authentication.

Authentication

SSO-Marketing-EU ▼

[Create or manage SSO methods](#)

Cancel

Save

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.

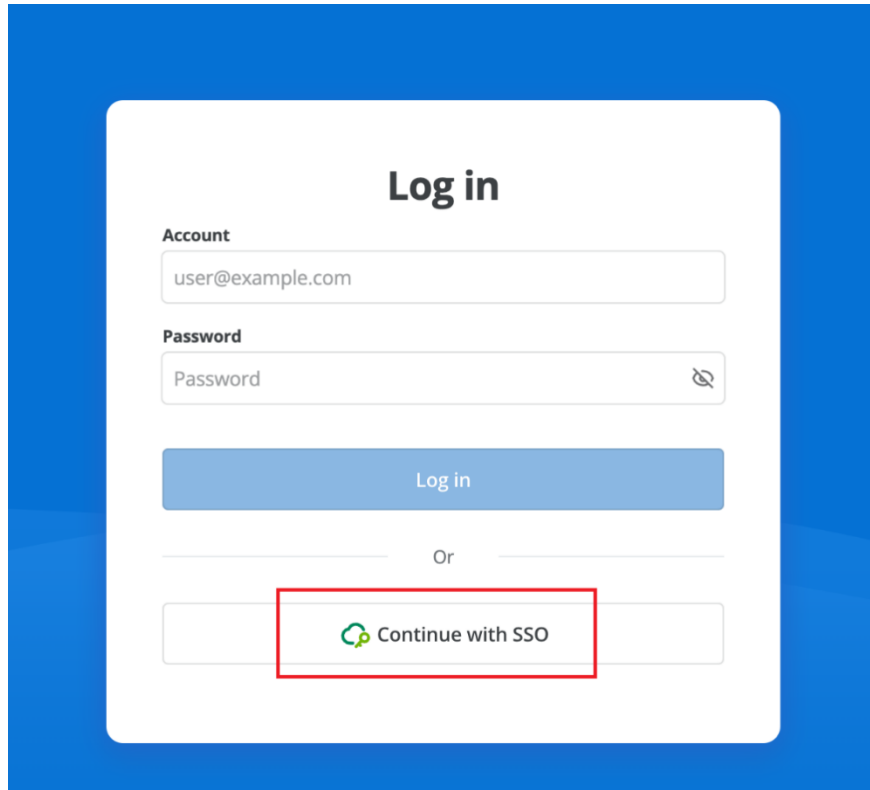
Requirements

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

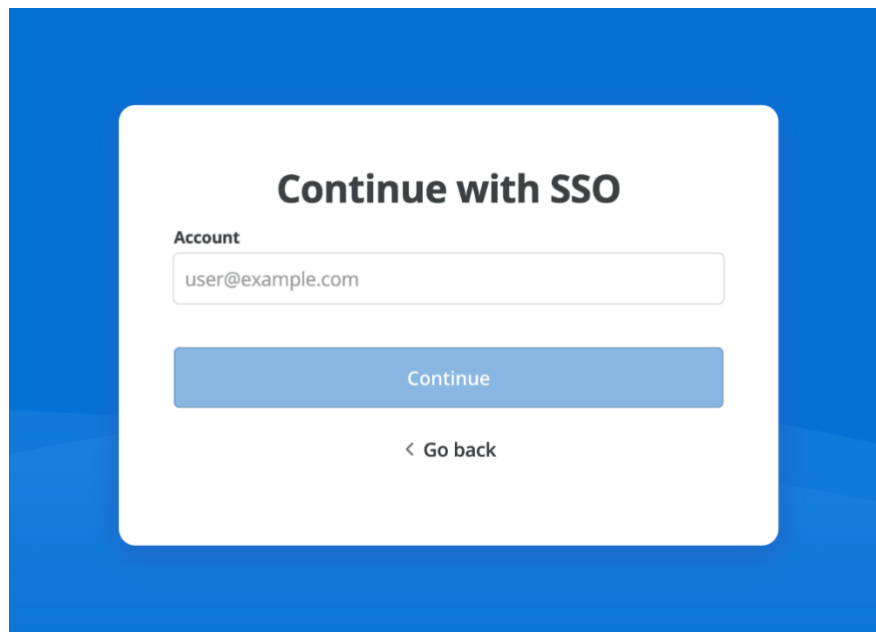
From Gateway

1. Enter your Gateway address and visit SSO login page

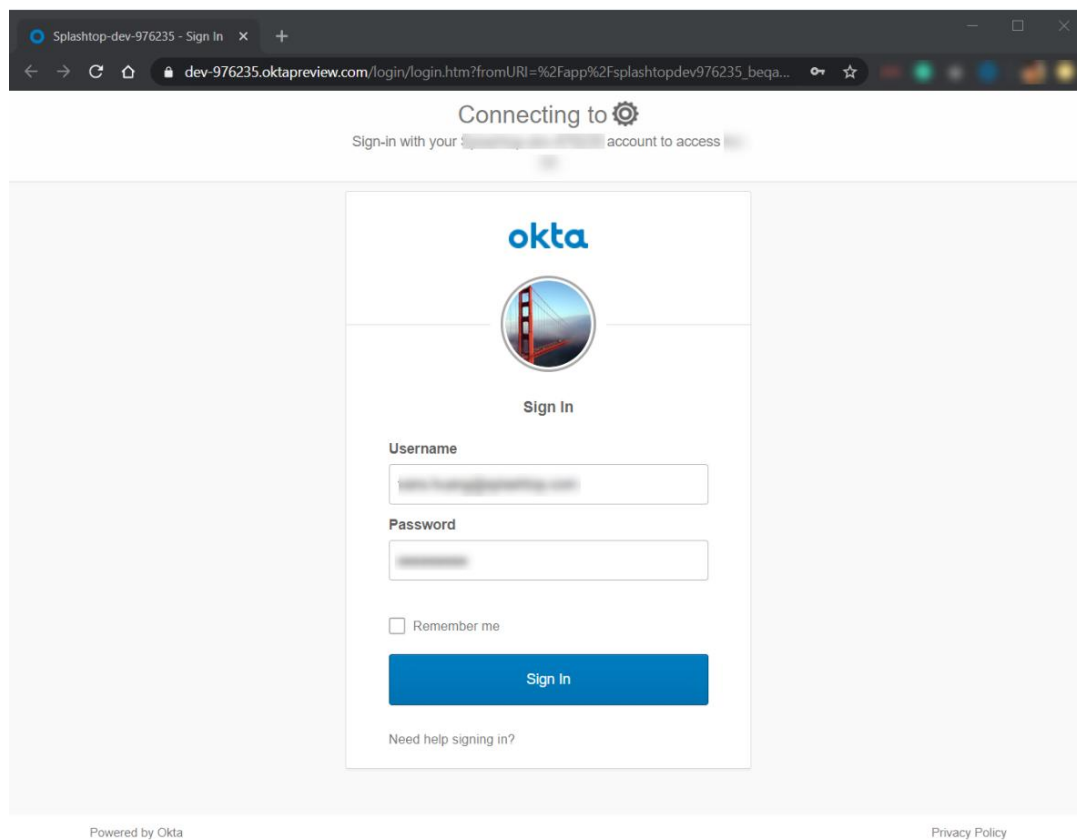
2. Insert your SSO account then log in.



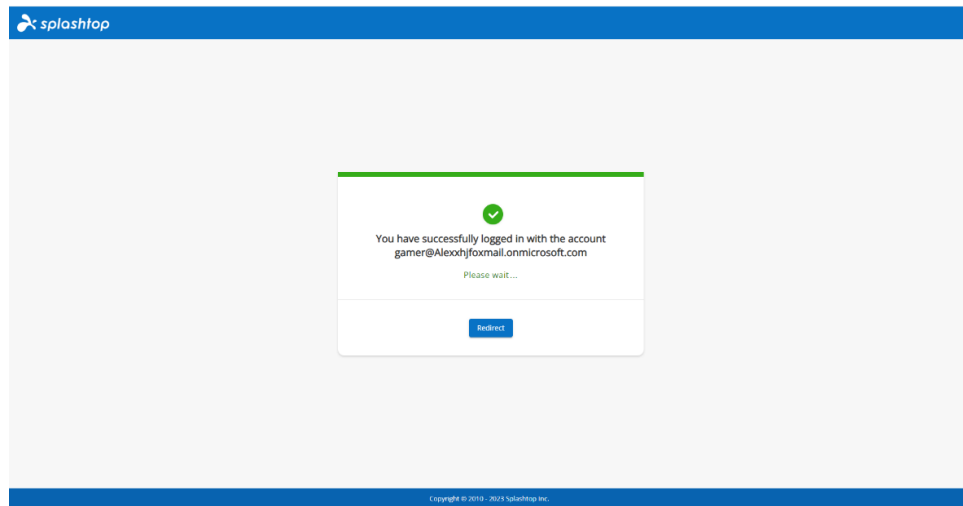
The image shows a login interface for Splashtop. It features a blue background with a white login card in the center. The card has the title "Log in" at the top. Below the title are two input fields: "Account" with the placeholder text "user@example.com" and "Password" with a placeholder text "Password" and a toggle icon. A blue "Log in" button is positioned below the password field. Below the button is a horizontal line with the word "Or" in the center. At the bottom of the card is a button labeled "Continue with SSO" with a red rectangular box highlighting it. The button has a small icon to its left.



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



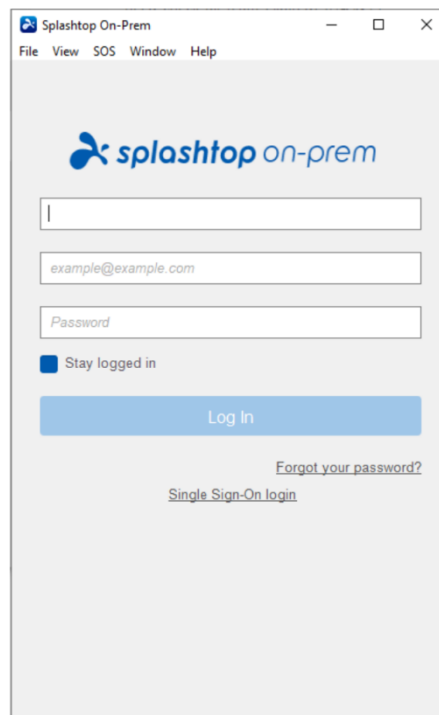
4. Log in to the identity provider portal then, it will log in to your Gateway.



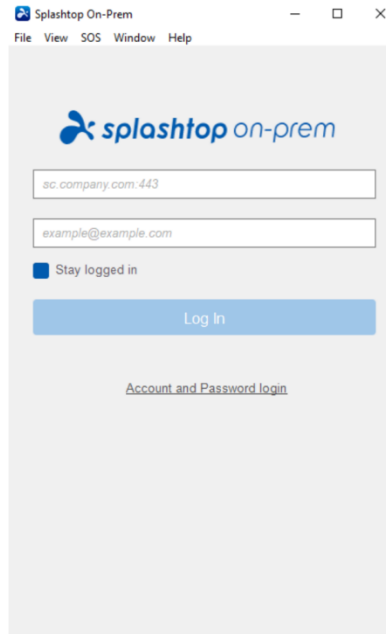
From Splashtop On-Prem app

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

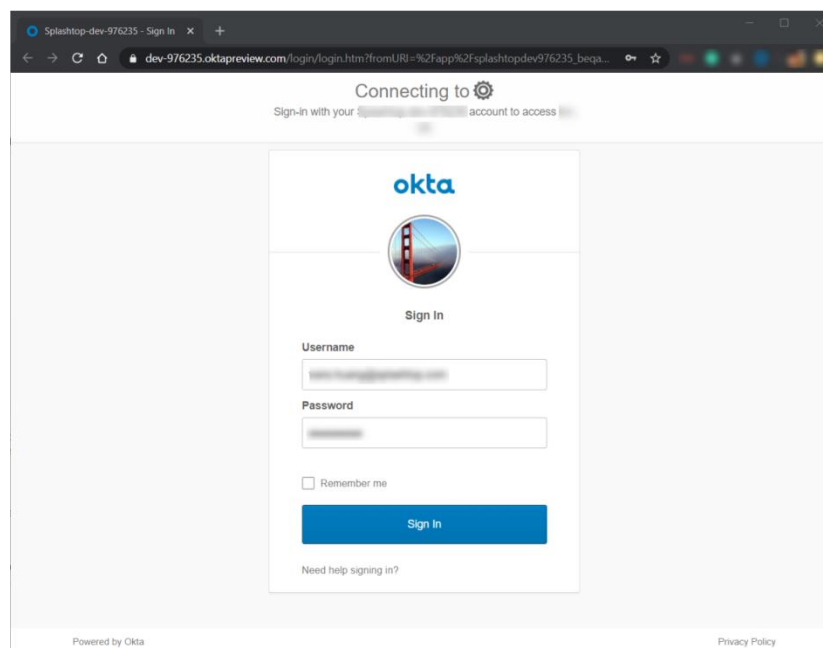
1. On Splashtop On-Prem app, click **Single Sign-On login** link.



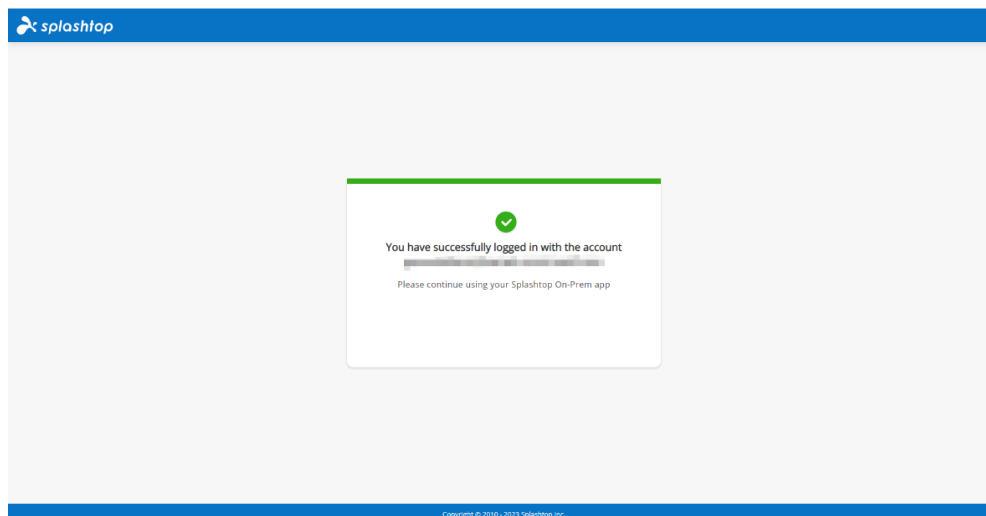
2. On the Single sign-on login page, insert your Gateway address and SSO account then click Log In.



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.

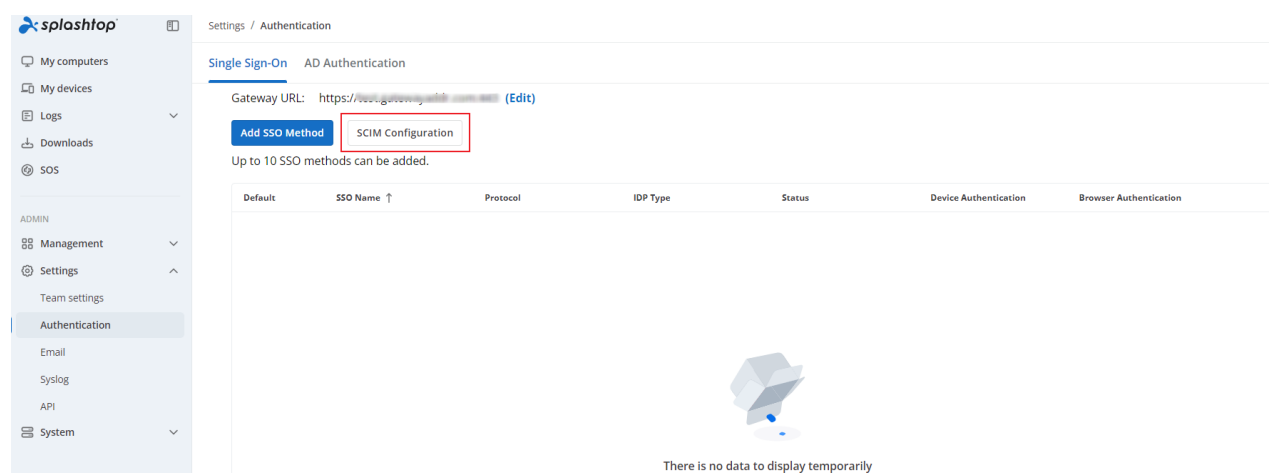


How to generate the SCIM provisioning token?

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.

SCIM Configuration

Base URL `https://[redacted]gatewayadmin.com:443/api/scim/v1`

API Token

`eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJ0aWQiOiJEsImtleSI6IiBJS3h3ektEY09WVUVRaGpmdlIOSUxETkl6c2d5QnVYIiwiaXNzIjoieU3BsYXNodG9wRW50ZXJwcmVzZSJ9.P3gpGeqELC2PulheDk3rOhOjCgQWtYV4IH9W8fMkl6dxr-DiKveLUCSsO0XY-Zu6sKVSPt5Kp_brobkXvJE-OhmlQStlFrKdGN7rNr0LVORNCYA0BZKLCO6SIA004P_-m_SLf2oaU242JFtrat2YI55QZfajaujLxuRm41_hzF0b0ggsOFzeZFCUZEtYKZNhk5PYCTENP4jvBMMyCFR9L-4Z5KJMP9IgVSng74AO9eRbosO3rylrHslN8fWYSFBR6NLCogjbOCh2LwBr4OUPz99jG8ZOXVqiZT1WbNve4VWGC08o81Y9oW0CiPQxNUeq81sBF0Ss59V_p_s7_EERHQ`

OK

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

SCIM Configuration

Base URL `https://[redacted]gatewayadmin.com:443/api/scim/v1`

API Token

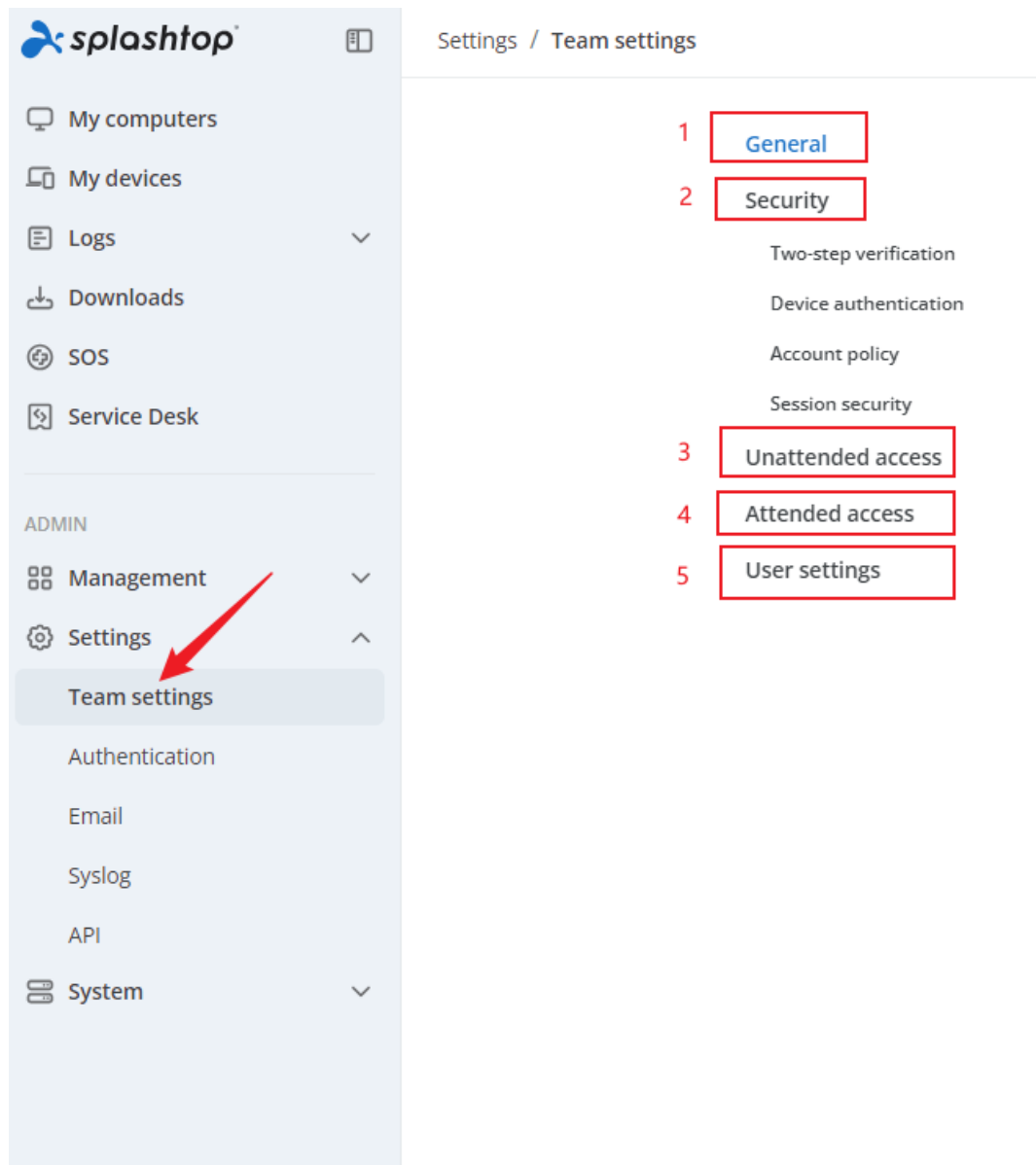
`eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJ0aWQiOiJEsImtleSI6IiBJS3h3ektEY09WVUVRaGpmdlIOSUxETkl6c2d5QnVYIiwiaXNzIjoieU3BsYXNodG9wRW50ZXJwcmVzZSJ9.P3gpGeqELC2PulheDk3rOhOjCgQWtYV4IH9W8fMkl6dxr-DiKveLUCSsO0XY-Zu6sKVSPt5Kp_brobkXvJE-OhmlQStlFrKdGN7rNr0LVORNCYA0BZKLCO6SIA004P_-m_SLf2oaU242JFtrat2YI55QZfajaujLxuRm41_hzF0b0ggsOFzeZFCUZEtYKZNhk5PYCTENP4jvBMMyCFR9L-4Z5KJMP9IgVSng74AO9eRbosO3rylrHslN8fWYSFBR6NLCogjbOCh2LwBr4OUPz99jG8ZOXVqiZT1WbNve4VWGC08o81Y9oW0CiPQxNUeq81sBF0Ss59V_p_s7_EERHQ`

OK

Settings

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.



There are 5 sections in the team settings page:

- **General**
- **Security**
- **Unattended access**
- **Attended access**
- **User settings**

General

General

Team name ABC 1234 	Gateway URL https://192.168.10.10:443 
User seats 1000 available / 1000 used 	SOS seats 1000 available / 1000 used
Computers 1 deployed / 1000 used	

- Team Name: you can customize the Team Name here. The Team Name will reflect in account information of all Streamer and client devices.
- User Seats: it shows the maximum count of the team's available user seats and the count of the enabled user seats.
- Computers: it shows the maximum count of the team's deployable computers and the count of the deployed computers.
- Gateway URL: This parameter serves as the external domain name for accessing the Splashtop Gateway service.
- SOS Seats: it shows the maximum count of the team's available SOS seats and the count of the enabled SOS seats.

Security

Security

Two-step verification

[Manage trusted devices](#)

	Default Granular Settings		
	Admin / Group manager	Member	Admin configurable ⓘ
Require users to enable two-step verification	☐	☒	Off ▾
Allow users to trust devices Forever ▾	☒		
Disable device and browser authentication when two-step verification is enabled	☒		

Device authentication

Device authentication Detailed settings	☒
Browser authentication Detailed settings	☒
Device MAC address restrictions Detailed settings	☒
Device timeout 24 hours ▾ ⓘ	☒
Browser timeout ⓘ	8 hours ▾

Account policy

Remember app login ⓘ	☒
Complex password Detailed settings	☒
Account lockout Detailed settings	☒

Session security

	Default Granular Settings		
	Admin / Group manager	Member	Admin configurable ⓘ
Remote control ⓘ	☒	☒	Off ▾
Save security code (Entered when starting a session)	☒		
Save Windows / Mac credential (Entered when starting a session)	☒		

Two-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 TOTP code to log in to the device.

Two-step verification

Manage trusted devices

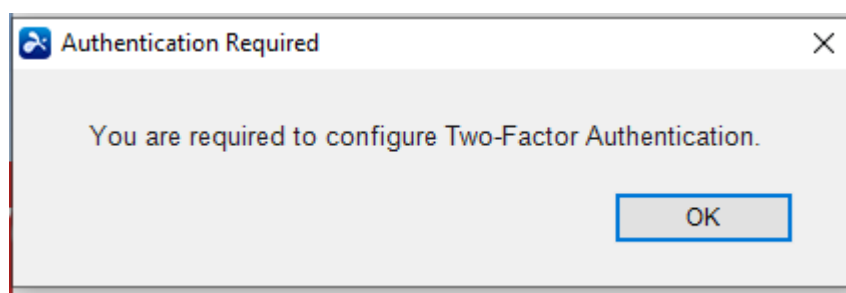
	Default Granular Settings		
	Admin / Group manager	Member	Admin configurable ⓘ
Require users to enable two-step verification	☒	☒	Off ▾
Allow users to trust devices Forever ▾	☒	☒	☒
Disable device and browser authentication when two-step verification is enabled	☒	☒	☒

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

Require users to enable two-step verification: **Here are two checkboxes in the Default Granular Settings column, one is for Admin/Group manager and the other is for Member.**

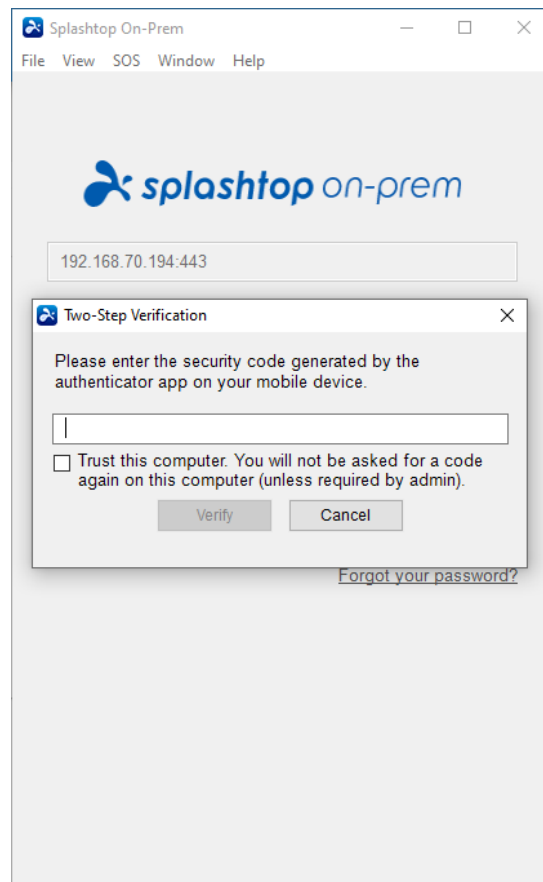
If the first checkbox is checked, an admin user/group manager is required to set up a 2-step verification device when trying to log in to On-Prem client for the first time.

If the second checkbox is checked, a member user is required to set up a 2-step verification device when trying to log in to On-Prem client for the first time.



In addition to the two checkboxes, there's a separate column named Admin configurable with a down arrow. If you want to allow admin and group manager to configure granular settings for others, you can click the down arrow and select ON.

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 TOTP code for future login. And you can click the down arrow to set a valid period (Forever, 1 days, 7 days, and 30 days) for the trusted devices.



Disable device and browser authentication when two-step verification is enabled: enabling this option means that device and browser authentication is disabled if you've enabled two-step verification (which provides even greater security).

Device authentication: if this option is checked, device authentication is required before a remote session can be initiated. You can click Detailed settings for more granular settings.

Device authentication

Device authentication Detailed settings	
Browser authentication Detailed settings	
MAC address restrictions for On-Prem app Detailed settings	
Log out idle users from On-Prem app 24 hours  	
Log out idle users from browser 	8 hours 

Browser authentication: if this option is checked, browser-based authentication is required before a remote session can be initiated. You can click [Detailed settings](#) for more granular settings.

MAC address restrictions for On-Prem app: because MAC-based addresses are unique to each device, using MAC addresses for authentication might seem more secure. If you check this option, you need to complete more detailed settings to ignore specific MAC addresses. You can input MAC addresses to ignore one by one, or directly import an existing .csv formatted file (which can also be exported).

Log out idle users from On-Prem app: if this option is checked, users will be force logged out from on-prem app when idle time reaches 15 minutes /1 hour /8 hours /24 hours.

Log out idle users from browser: this setting lets you log out users from the browser when they are idle for a certain amount of time (5 minutes /15 minutes /30 minutes /1 hour /4 hours /8 hours)

Account policy:

Account policy

Remember app login ⓘ	
Complex password Detailed settings	
Account logout Detailed settings	

Remember app login: if this option is checked, users don't need to enter their credentials every time they log in their account.

Complex password: by checking this option, you can finely tune the complex password policy, including password minimum length, enable password expiration period, and enforce password policy at next login.

Account logout: by checking this option, you can set the account logout threshold and choose how to lock the account out.

Session security:

Session security

	Default Granular Settings		
	Admin / Group manager	Member	Admin configurable ⓘ
Remote control ⓘ			Off 
Save security code (Entered when starting a session) 			
Save Windows / Mac credential (Entered when starting a session) 			

Remote control: this option is designed to disable to restrict remote control from Admin / Group manager and/or Member in a remote session. If you want to allow admin and group manager to configure granular settings for others, you can click the down arrow from the separate column of Admin configurable and select ON.

Save security code: if this option is checked, the security code will be saved while establishing a remote session.

Save Windows / Mac credential: if this option is checked, the Windows / Mac credential will be saved while establishing a remote session.

Unattended access

Splashtop Remote Support or Splashtop Business Access can enable remote support and control with the endpoint installing corresponding software. And initiating a remote session doesn't need anyone being present.

In this section, some features are supported to be finely tuned from the Default Granular Settings column.

Unattended access

		Default Granular Settings		
		Admin / Group manager	Member	Admin configurable ⓘ
File transfer				
	Upload	☒	☒	Off ▼
	Download	☒	☒	Off ▼
Text copy and paste				
	From local to remote	☒	☒	Off ▼
	From remote to local	☒	☒	Off ▼
Remote print		☒	☒	Off ▼
Remote command		☒	☒	Off ▼
Watermark protection Detailed settings	☒	☒	☒	Off ▼
Request permission to connect ⓘ		☐	☐	Off ▼
Centralized session recording Detailed settings	☒	☒	☒	Off ▼

File transfer: enable file transfer (upload and/or download) between the local and remote computer (Windows and Mac only).

Text copy and paste: enable text copy and paste from local to remote computer and/or from remote to local computer.

Remote print: enable document printing from a Streamer computer to a printer connected to the client computer.

Remote command: enable sending command to a Streamer computer from a client computer.

Watermark protection: by checking this option, users can customize the watermark text and layout to display during remote session, including font size, font color, font opacity, outline color, outline opacity, etc.

Request permission to connect: it provides the user 3 options on how to accept the remote connection prompt, namely reject connection after request expires(at login screen, reject automatically), request expires(at login screen, allow automatically), and allow connection after request expires.

Centralized session recording: by checking this option, recorded remote sessions will be automatically recorded to a centralized cloud location. Users can further select who can playback/download/remove recordings from Detailed settings.

Local session recording Detailed settings	☒		
Concurrent remote session ⓘ	☒		
Paste clipboard as keystrokes	☒		
Remote wake	☒		
Remote reboot	☒		
Off-session chat	☒		
Device redirection Detailed settings	☒		
Wacom Bridge ⓘ Learn more	☒		
Remote microphone	☒		
In-session voice call ⓘ	☐		
RDP Computer	☒		
VNC Computer	☒		
SSH Computer	☒		
Web app ⓘ Learn more	☒		
System Tools for Owner only ▼ ⓘ	☐		
Offline computers policy Detailed settings	☐		
Auto update Streamers Detailed settings	☐		
Scheduled access ⓘ Asia/Shanghai (GMT +08:00) ▼			
Session Indicator ⓘ Remote session Background actions ⓘ Display type Pop-up & Banner ▼ ☒ Allow user to close the banner ☒			

Local session recording: enable local session recording to assign auto recording, path and size limit to storage folder for SOS app by Windows or OS platforms.

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

Paste clipboard as keystrokes: a special way to paste, you can enable it to paste the content in local clipboard to remote computer as key strokes.

Remote wake: enable waking up a Streamer computer from a client device.

Remote reboot: enable rebooting a Streamer computer from a client device.

Off-session chat: enable off-session chat function.

Device redirection: enable it to select the USB class to user for device redirection.

Wacom Bridge: enable this function to seamless use Wacom's pen technology on local.

Remote microphone: enable this function to transmit a local microphone input to a remote computer.

In-session voice call: enable this function to initiate a voice call to the end-user during the remote access session.

RDP computer: enable connecting to an RDP computer from a client device.

VNC computer: enable connecting to a VNC computer from a client device.

SSH computer: enable connecting to an SSH computer from a client device.

Web app: enable this function to allow users to connect to remote computers with browsers.

System tools for: By entering computer's admin username and password, to designate who can access system tools.

Offline computers policy: Enabling this option to set how many days offline computers will be automatically removed.

Auto update Streamers: enable this to apply the Streamer updates to all computers or only specific computers and computer groups.

Scheduled access: enable this to schedule times for when users can remotely access.

Session indicator: from here you can choose display type and if you allow user to close the banner for remote session and background actions.

Attended access

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.

Attended access

	Default Granular Settings		
	Admin / Group manager	Member	Admin configurable ⓘ
Centralized session recording Detailed settings	☒	☒	Off ▾
Apply granular control settings as unattended access ⓘ	☒		
In-session file transfer Both upload and download ▾ ⓘ	☒		
Text copy and paste Both local and remote ▾ ⓘ	☒		
Watermark protection Detailed settings	☐		
Local session recording Detailed settings	☐		
Concurrent remote session ⓘ	☒		
Paste clipboard as keystrokes	☒		
In-session voice call ⓘ	☒		
Web app ⓘ Learn more	☒		
Third Party Integration	Set up API Key		
Session Indicator			
Display type ⓘ	Banner ▾		
Allow user to close the banner	☒		

Centralized session recording: by enabling this option, recorded remote sessions will be automatically recorded to a centralized cloud location. Users can further select who can playback/download/remove recordings from Detailed settings.

Apply granular control settings as unattended access: if this option is unchecked, e2-step verification and remote control would always follow granular control settings as the user level.

In-session file transfer: enable file transfer (upload and/or download) between the local and remote computer during the remote session.

Text copy and paste: enable text copy and paste from local to remote computer and/or from remote to local computer.

Watermark protection: by enabling this option, users can customize the watermark text and layout to display during remote session, including font size, font colour, font opacity, outline colour, outline opacity, etc.

Local session recording: enable session recording for SOS remote support session.

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

Paste clipboard as keystrokes: a special way to paste, you can enable it to paste the content in local clipboard to remote computer as key strokes.

In-session voice call: enable this function to initiate a voice call to the end-user during the remote access session.

Web app: enable this function to allow users to connect to remote computers with browsers.

Third Party Integration: from here users can integrate with a third party by clicking Set up API Keys.

Session indicator: from here users can choose display type and if allow user to close the banner.

User Settings

User settings

Group-specific manager role Learn more	
Allow members to see groups	
Allow members to connect to computers in an active connection	
Allow members to establish concurrent sessions ⓘ	
Allow members to disconnect other's sessions	
Allow members to reboot computers and restart Streamers Detailed settings	
Member's permission for computer notes	View only ▼

Group-specific manager role: enable group manager role who manages a group.

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

Allow members to connect to computers in an active connection: allow member users to establish remote sessions to the computers that have already been connected.

Allow members to establish concurrent sessions: allow member users to remote into multiple computers concurrently.

Allow members to disconnect from other's sessions: allow member users to end others' remote connections.

Allow members to reboot computers and restart Streamers: select actions that member users can perform on the computers, including restart Streamer, normal reboot, and safe-mote reboot.

Member's permission for computer notes: manage member users' permission for computer notes, including cannot view and edit, view only, and view and edit.

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.

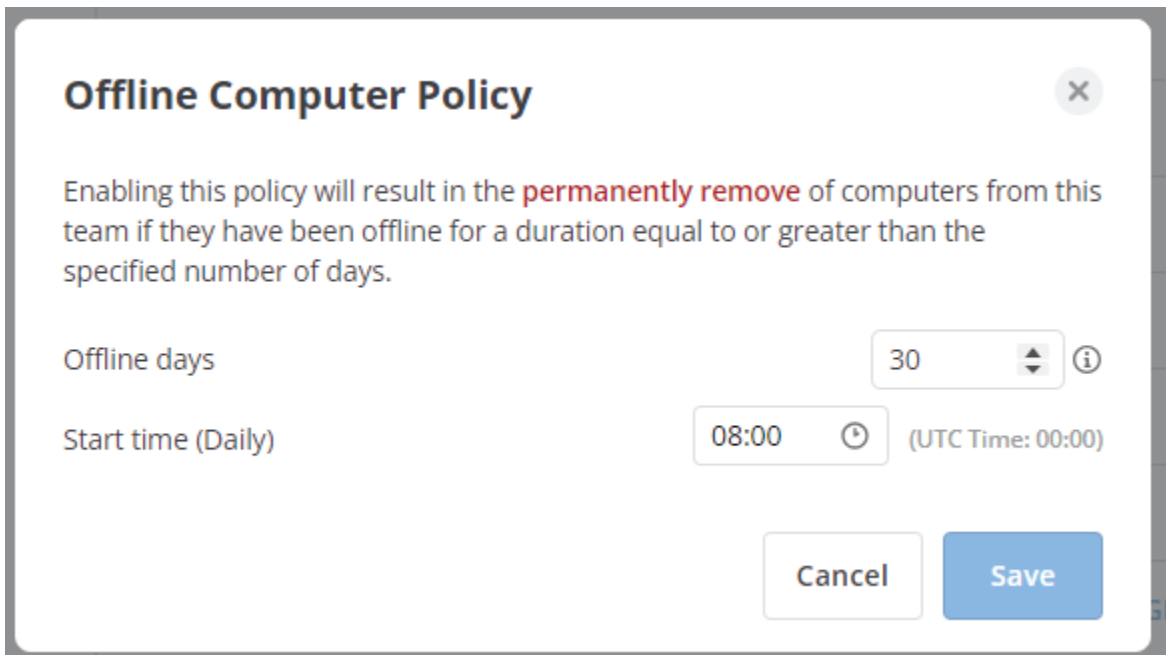
How to set Remove offline computers policy?

1. Log in to Gateway's management console as Owner, go to *Settings > Team Settings > Unattended access*. Check the **Offline computers policy**.

General	VNC Computer	☒		
Security	SSH Computer	☒		
Two-step verification	Web app ⓘ Learn more	☒		
Device authentication				
Account policy	System Tools for Owner only ▼ ⓘ	☐		
Session security	Offline computers policy Detailed settings	☐		
Unattended access				
Attended access	Auto update Streamers Detailed settings	☐		
User settings	Scheduled access ⓘ		Asia/Shanghai (GMT +08:00) ▼	
	Session Indicator ⓘ			

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 a user can 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**.

Users

+ Add
Bulk Actions
Only show selected
⌵
⌵ Collapse all
⌵ Filters
⌵
⌵
⌵

Role ↑	Source	Display Name	Last Login	Status	⋮
Owner	Local		2024-08-20 16:04:34	Enabled	⚙️
Member	Local		2024-08-08 17:55:50	Enabled	⚙️
Member	Local			Enabled	⚙️
Member	Local		2024-08-20 16:01:22	Enabled	⚙️

Add
Local User
AD User/Group
SSO User
Import
Local Users
AD Users
SSO Users

Add User

* Account

* Password

* Confirm Password

☐ Request to change password when next login

Group

Role

Status
☒ Enable user
☒ Enable web access

SOS Technician
☐ Enable SOS/On-Demand support

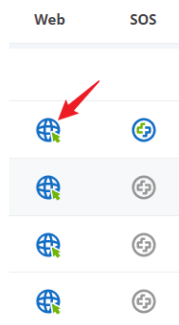
Password must include:

- At least 8 characters
- At least 1 lowercase Latin letter (a-z), 1 uppercase Latin letter (A-Z) and 1 number
- At least 1 special character ~!@#%&*_{+~`|~\~^~&~'~"~<~>~/?
- No match of the account name

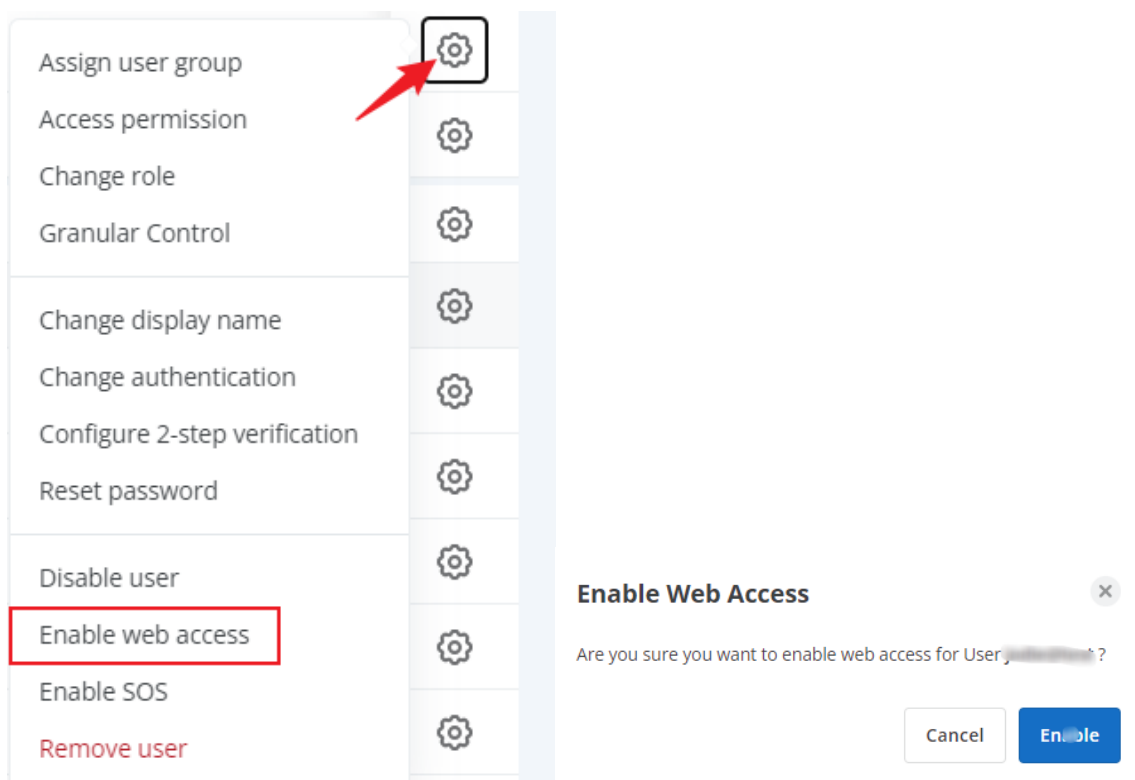
Cancel Add

Edit User

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

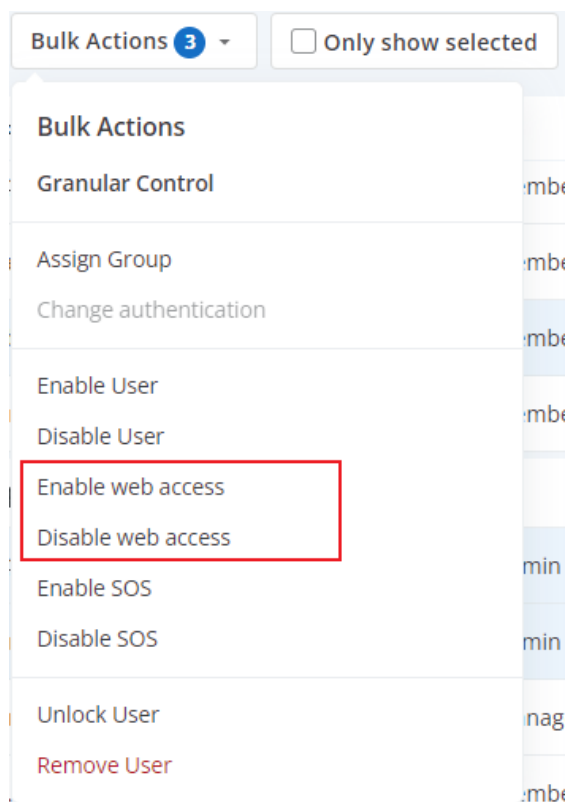


You can choose a specific user account and set the web access for the specific account. Navigate to *web/management/users* page, next to each user in the user list, click on the gear icon and choose **Web access**.



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**.



Enable web access

You are enabling web access for 3 selected user(s).

Cancel

Save

Setup two-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 **Settings** > **Team Settings**, you can specify how and whom the 2-step verification should be enforced.

Settings / Team settings

General
Security
Two-step verification
Device authentication
Account policy
Session security
Unattended access
Attended access
User Settings

Security

Two-step verification

[Manage trusted devices](#)

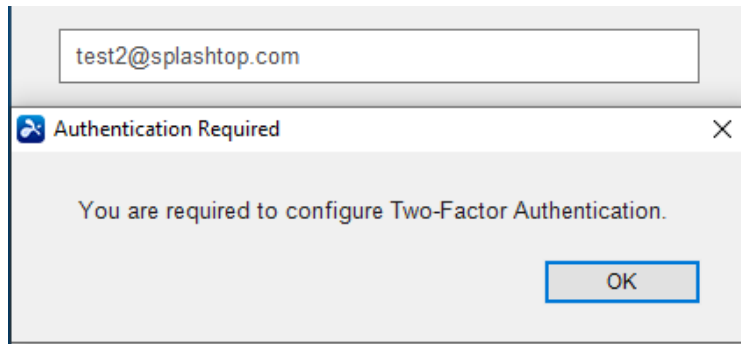
	Default Granular Settings		
	Admin / Group manager	Member	Admin configurable ⓘ
Require users to enable two-step verification	☐	☐	Off ▾
Allow users to trust devices Forever ▾	☒		
Disable device and browser authentication when two-step verification is enabled	☒		

Device authentication

Device authentication [Detailed settings](#) ☒

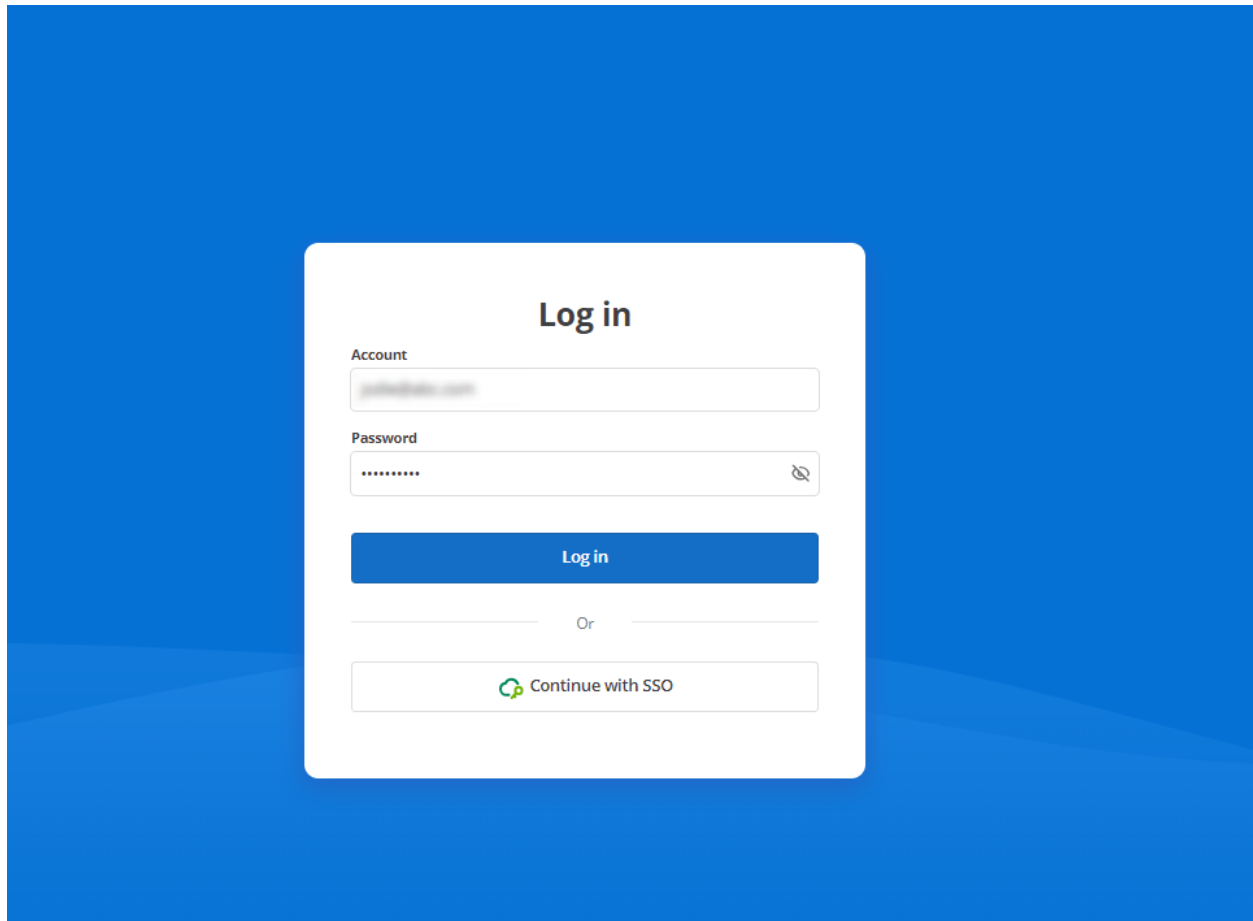
Browser authentication [Detailed settings](#) ☒

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.

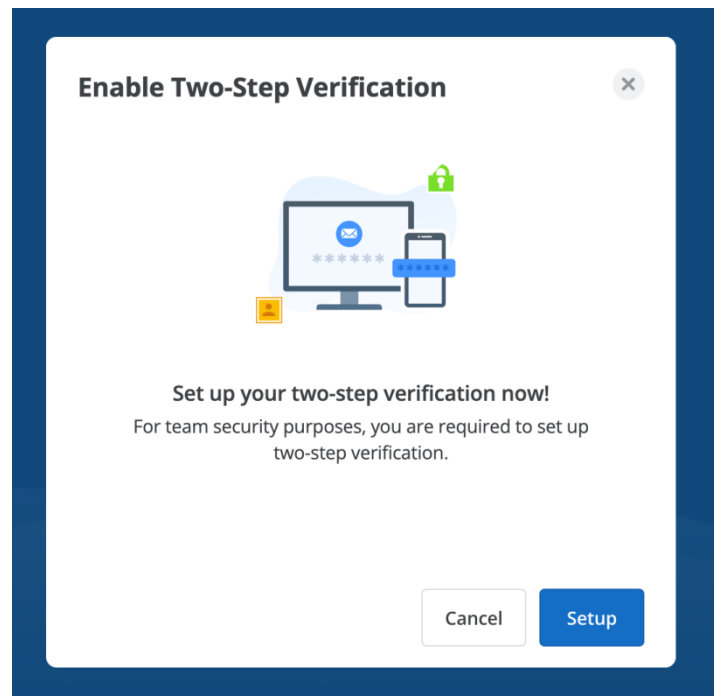


Step 2

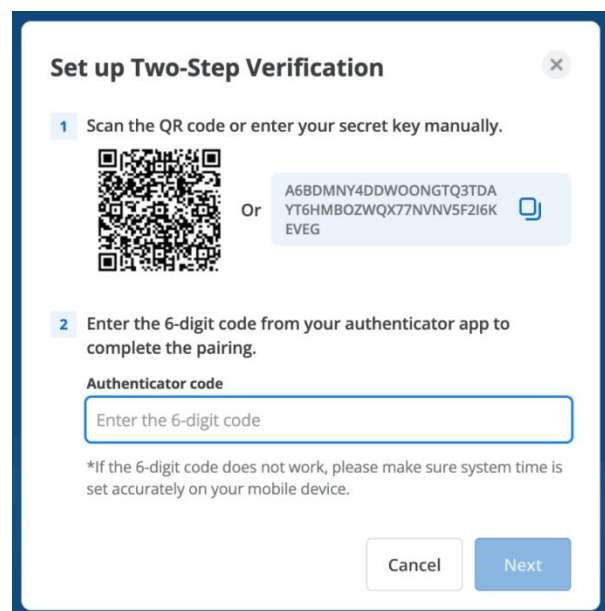
To set up the 2-step verification account for the first time, the user is required to log in to the **Gateway** using his/her own account.



Follow the instructions to complete the setup.

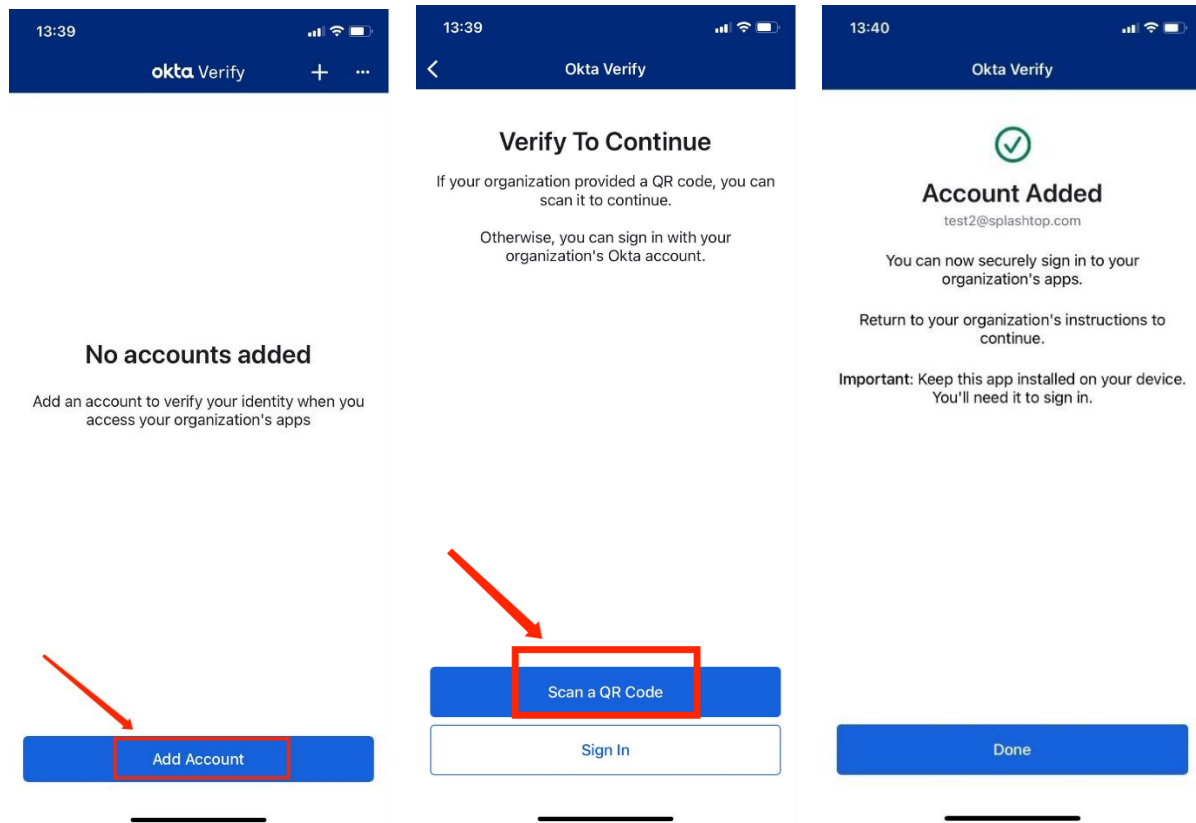


Click **Setup**, It would generate a QR code, users need to launch the authenticator app to scan it.

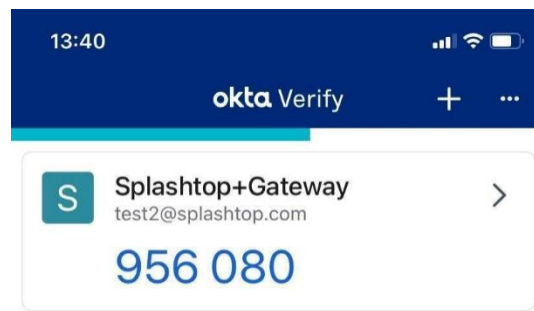


Launch the authenticator, take **okta Verify** as an example, and complete the following steps.

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.

Save Recovery Code ×

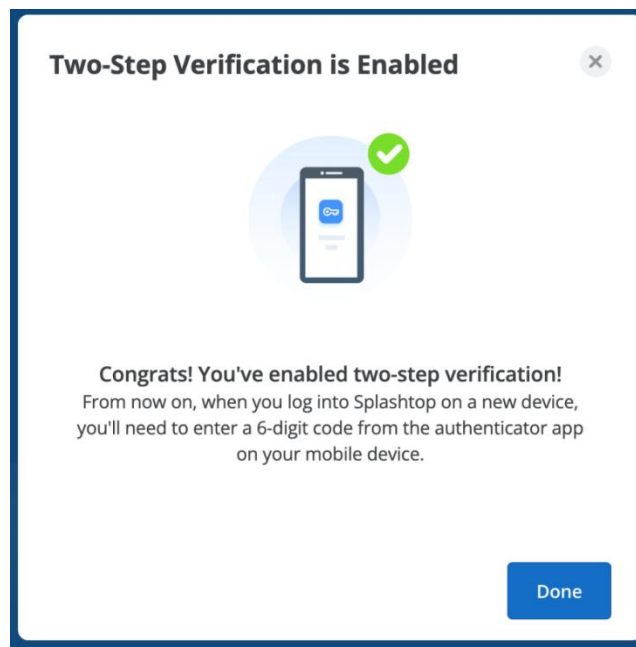
Recovery codes are as important as your password and are **shown only once** for security, which you can use these one-time codes to access your account if needed.

30253030	47963886
03772248	71163585
70256236	10195447
02536832	16150398
01989073	11974209

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

Copy codesSave codesProceed

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 two-step verification 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 for convenience.

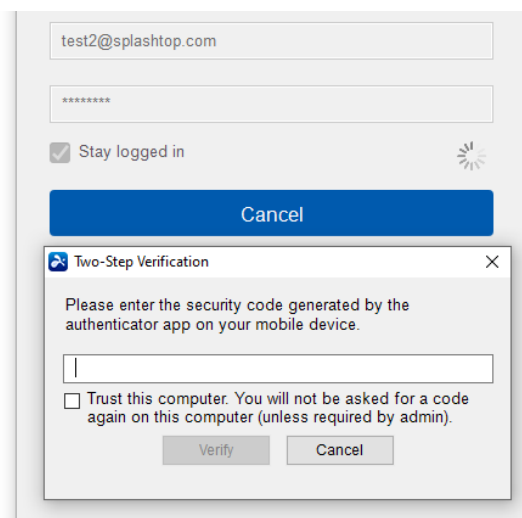
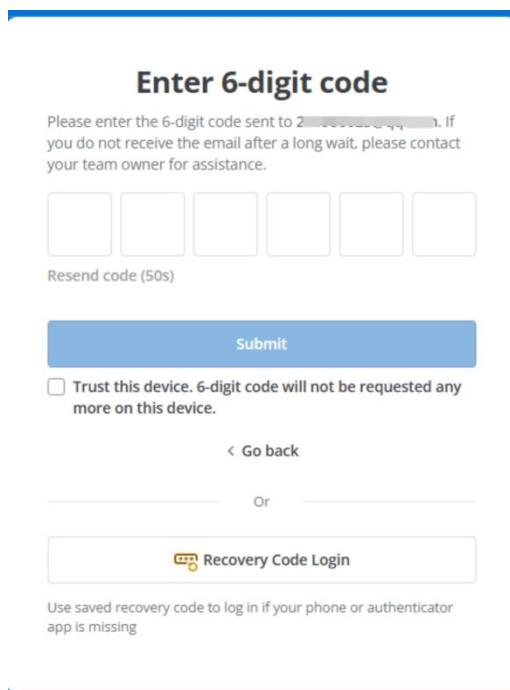


Figure. 2-sv passcode input dialog on On-Prem app



Enter 6-digit code

Please enter the 6-digit code sent to 2100000000000000. If you do not receive the email after a long wait, please contact your team owner for assistance.

[Resend code \(50s\)](#)

Submit

☐ Trust this device. 6-digit code will not be requested any more on this device.

[< Go back](#)

Or

 **Recovery Code Login**

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

Figure. 2-sv passcode input dialog on web console

Q&A

1. Why 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.

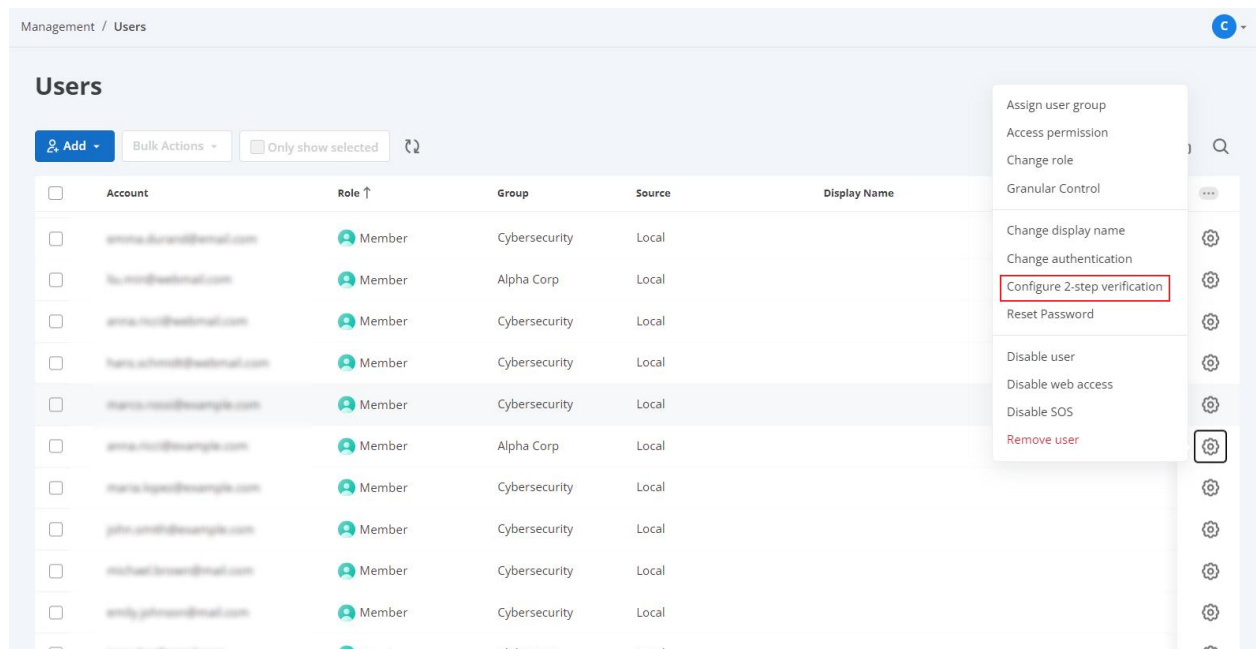
2. What if I lost my cell phone and forget my recovery code?

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

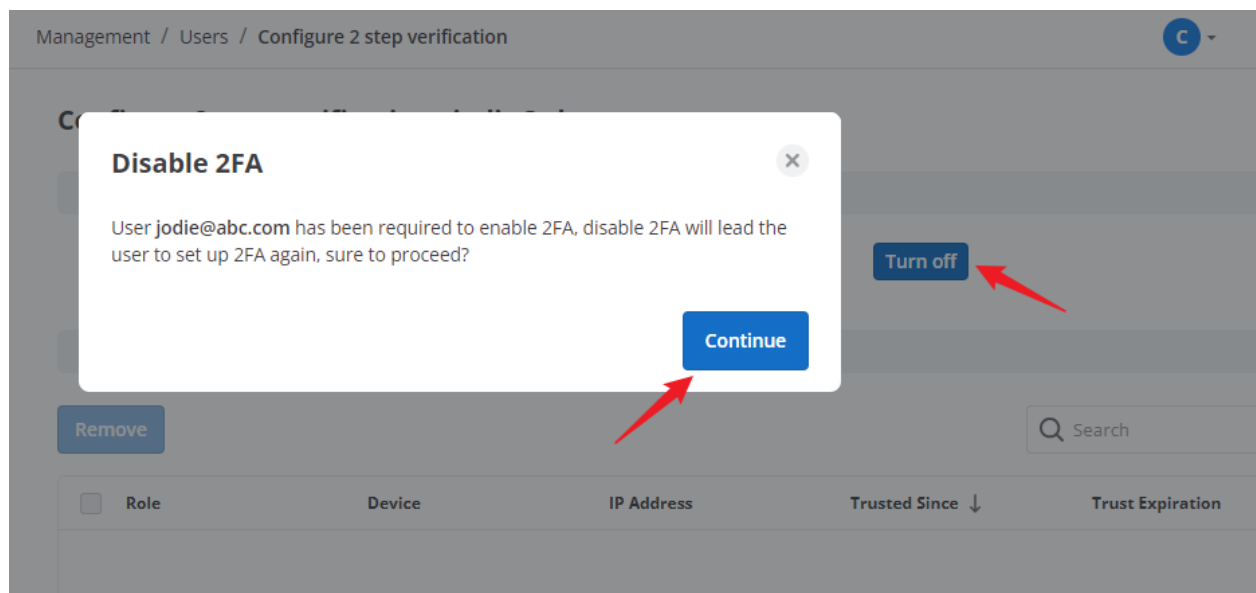
The following is the procedure of resetting 2FA for administrator:

1. Login to gateway as administrator

2. Go to Management ->Users -> Gear button -> Configure 2-step verification



3. Disable 2FA



4. User could set up 2FA again.



Note: 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.

Set up Two-Step Verification with Email

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 sent to your email.

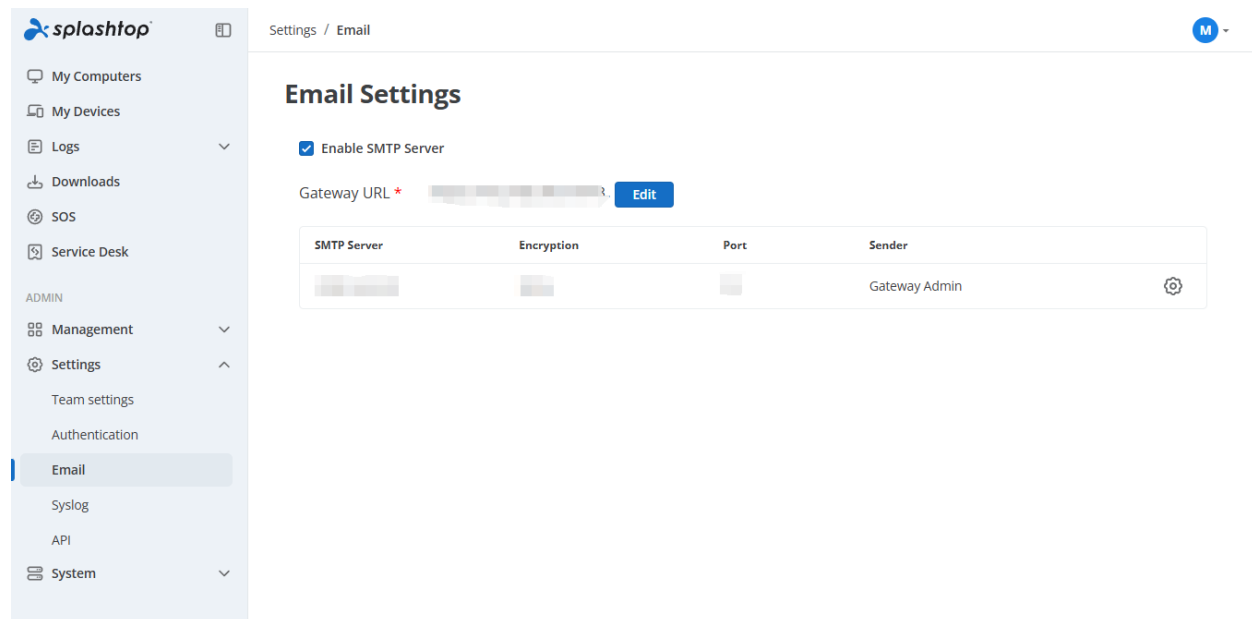
This means, even if someone has guessed or stolen your On-Prem account ID and password, he or she will not be able to log into your account and access your computers.

From Gateway v3.36.0, Splashtop On-Prem supports email OTP (One-Time Password) based two-step verification.

Enable SMTP server in Gateway

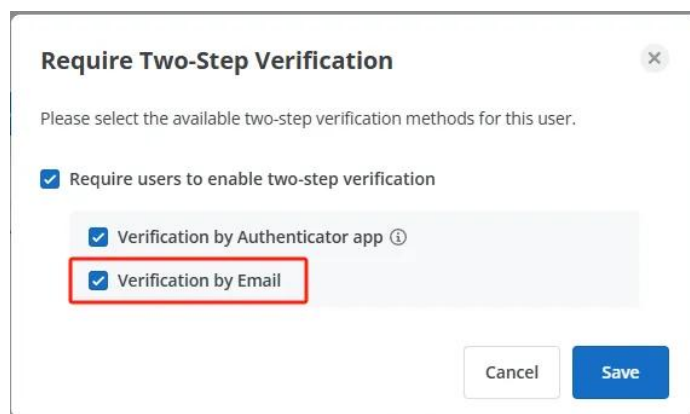
Since two-step verification relies on email, please ensure the SMTP server is correctly configured and enabled. Additionally, verify that users' email addresses are accurate. Otherwise, they will not receive the one-time password to complete the two-step verification process.

Log in to the web console as **Team Owner**, go to **Settings > Email**, then you need to configure and enable your SMTP server.



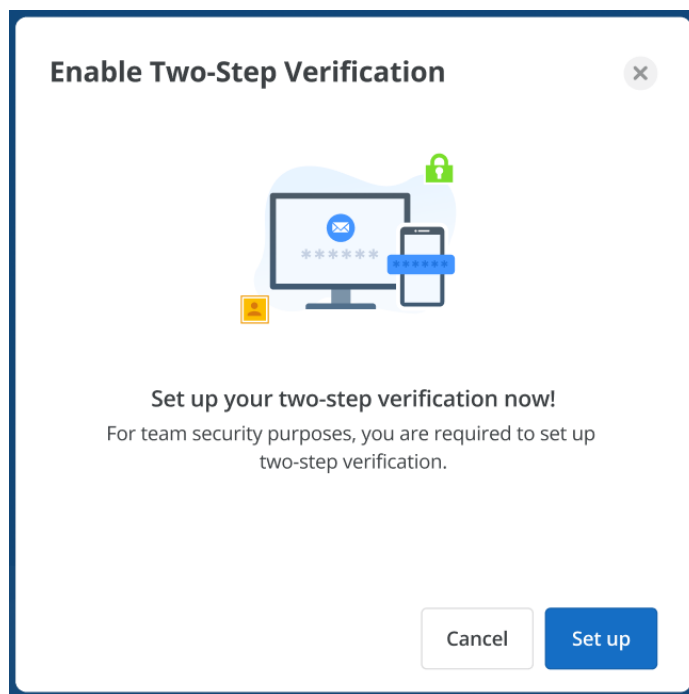
Enable and select the method for two-step verification

Log in to the web console as **Team Admin**. Go to **Management > User**, enable two-step verification for users and select **Verification by Email** as the two-step verification method.

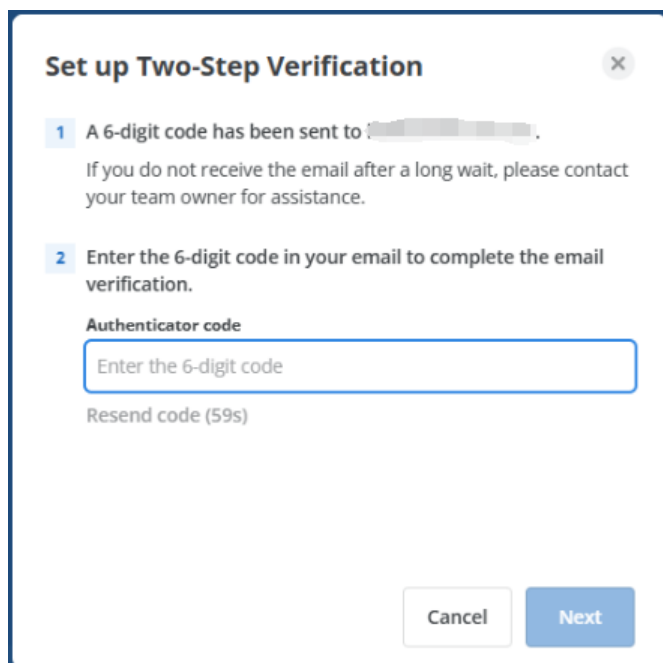


Set up two-step verification

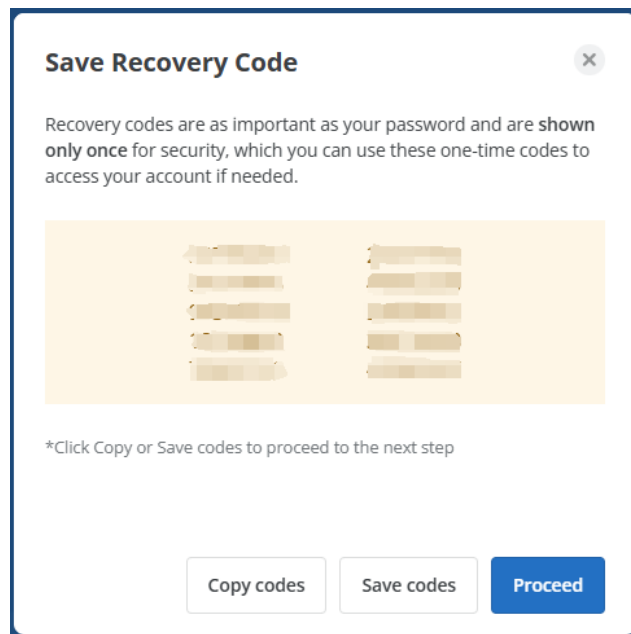
Please follow the instructions to complete the two-step setup flow. First of all, Click **Set up** to proceed to the next step.



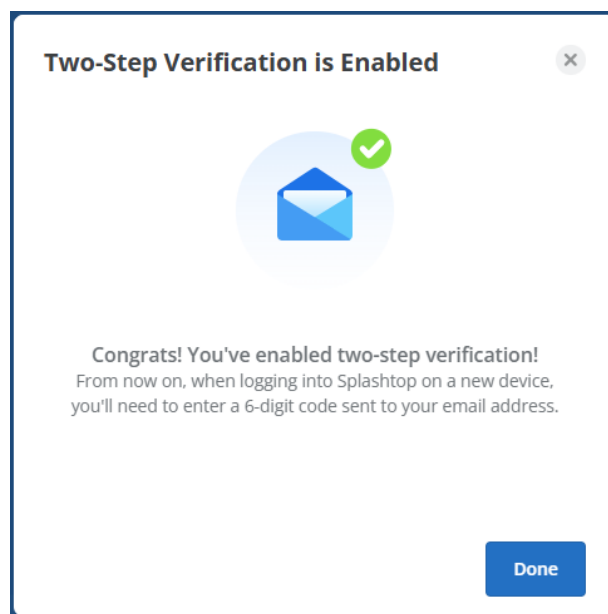
Then, the 6-digit code will be sent to your email. Enter the 6 code and click **Next** to finish pairing.



Click **Copy codes** or **Save codes** to save your recovery code. Please note that this code will only be displayed once, save it in a secure place. Then, click **Proceed** to go to the next step.



Finally, you've successfully enabled two-step verification.



Log in to Web Console or Splashtop On-Prem app with email

If an account has been enforced to enable two-step verification, after the user enters the account and password, he needs to fill in the one-time 6-digit code received in his mailbox to complete the login process.

Otherwise, if Team Owner has **allowed trust device**, users can check trust this device for convenience.

Enter 6-digit code

Please enter the 6-digit code sent to 201-555-1234. If you do not receive the email after a long wait, please contact your team owner for assistance.

Resend code (50s)

Submit

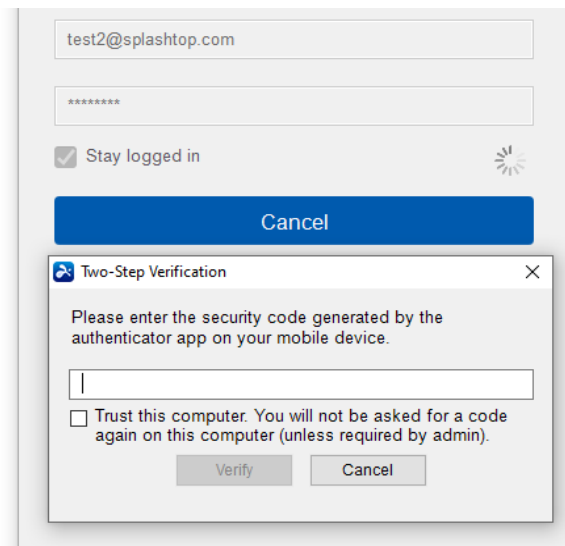
☐ Trust this device. 6-digit code will not be requested any more on this device.

< Go back

Or

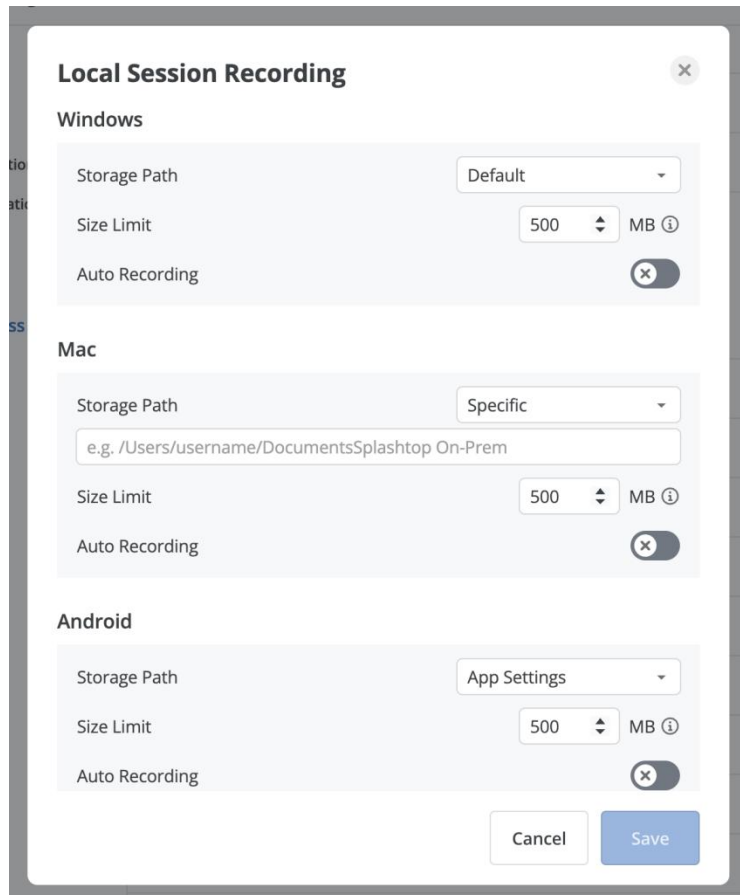
 Recovery Code Login

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



Local session recording on Gateway web console

Local Session Recording Detailed Settings



Local Session Recording

Windows

Storage Path: Default

Size Limit: 500 MB

Auto Recording: ☒

Mac

Storage Path: Specific
e.g. /Users/username/DocumentsSplashtop On-Prem

Size Limit: 500 MB

Auto Recording: ☒

Android

Storage Path: App Settings

Size Limit: 500 MB

Auto Recording: ☒

Cancel Save

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

- Windows
- macOS
- Android (Requires Gateway v3.36.0 or later and Android app 3.7.4.0 or later)

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*
 3. Android - *%device_album_path%/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

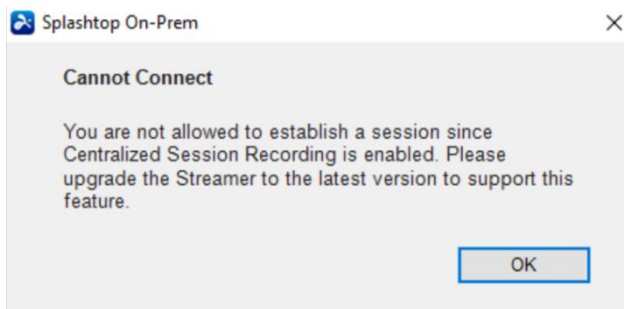
Centralized session recording

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 enabled 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 contact Splashtop 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-> Settings -> Team Settings -> Unattended Access / Attended Access)

	Watermark protection Detailed settings	☒	☒	Off v
General				
Security	Request permission to connect ^①	☐	☐	Off v
Two-step verification	Centralized session recording Detailed settings	☒	☒	Off v
Device authentication	Local session recording Detailed settings	☒		
Account policy	Concurrent remote session ^①	☒		
Session security	Paste clipboard as keystrokes	☒		
Unattended Access	Remote wake	☒		
Attended Access	Remote reboot	☒		
User Settings	Off-session chat	☒		
	Device redirection Detailed settings	☒		
	Wacom Bridge ^①	☒		
	Remote microphone	☒		

General

Security

Two-step verification

Device authentication

Account policy

Session security

Unattended Access

Attended Access

User Settings

Attended Access

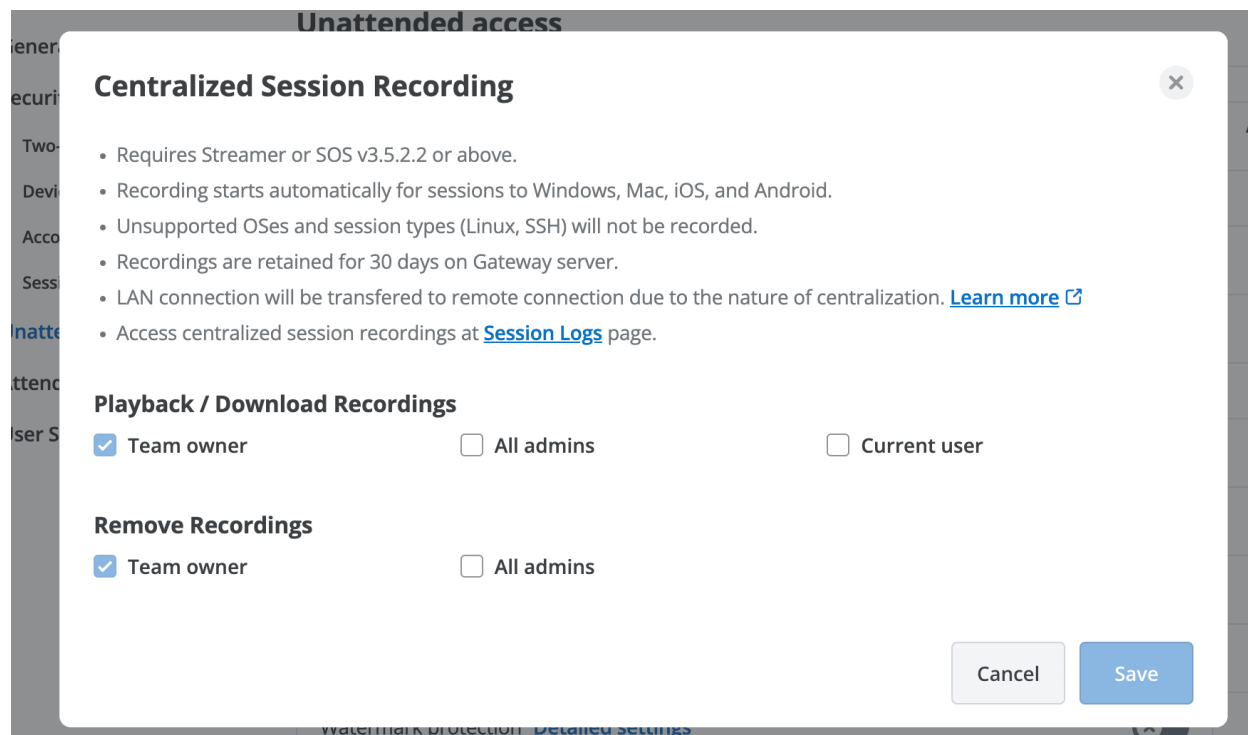
	Default Granular Settings		
	Admin / Group manager	Member	Admin configurable
Centralized session recording Detailed settings	☒	☒	Off
Apply granular control settings as unattended access	☒		
In-session file transfer Both upload and download	☒		
Text copy and paste Both local and remote	☒		
Watermark protection Detailed settings	☐		
Local session recording Detailed settings	☐		
Concurrent remote session	☒		
Paste clipboard as keystrokes	☒		

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.

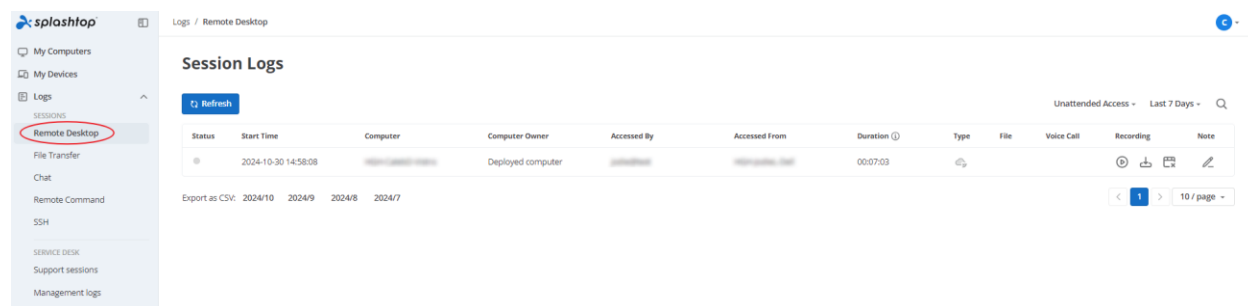
For utmost security in handling the recording files, the encrypted streaming data must be stored in your Splashtop Gateway to make sure file integrity. As a result, the LAN connection between Splashtop client app and Streamer will be redirected to your Gateway server.

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

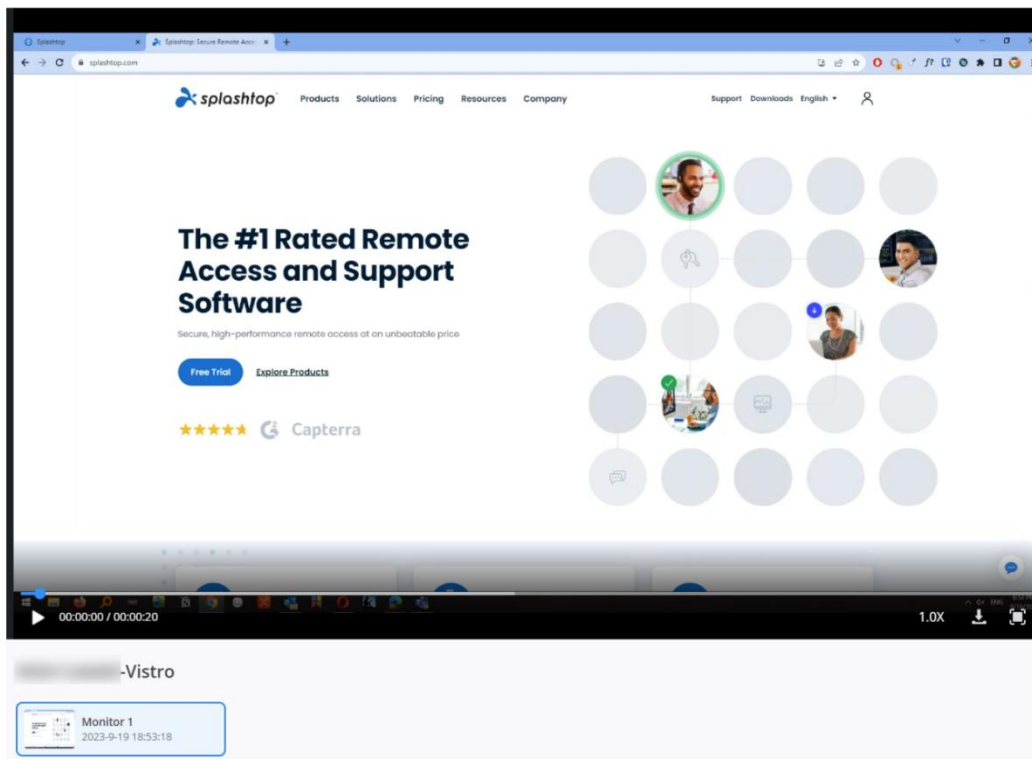
Recordings can be accessed from sessions log page in Splashtop web console.
(Gateway web console -> Logs -> Sessions)



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.

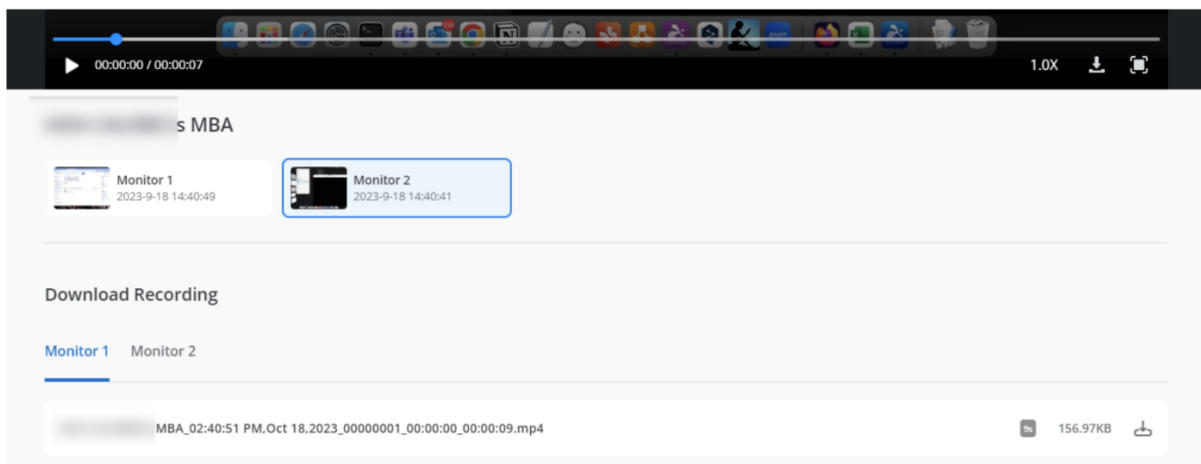
Playback



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 choose the .mp4 to download.

Storage configuration

With Gateway v3.40.3, you can configure the recording storage path and retention period by navigating to **System > Maintenance > Storage > Configuration**. Splashtop Gateway service **needs to restart** to apply the changes.

Centralized session recording

Storage Path

Local absolute paths only. Make sure the directory exists and has enough available space.

☒ **Default**

C:\Program Files (x86)\Splashtop\Splashtop Remote\Splashtop Gateway\sessionrecording

☐ **Specific**

Retention Period

☒ **30 days**

☐ 90 days

☐ 180 days

☐ 365 days

☐ Custom

If the centralized session recording storage path could not be found after restoration. Both the path and retention period will be reset to the default values.

Notes

- Recording is performed by Splashtop Gateway as the sessions pass 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).
- This feature provides [granular control](#) at the account level. (Requires Streamer or SOS v3.7.2.1 or above.)
- For the Clustering Gateway, additional configuration is required to enable centralized session recording.

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

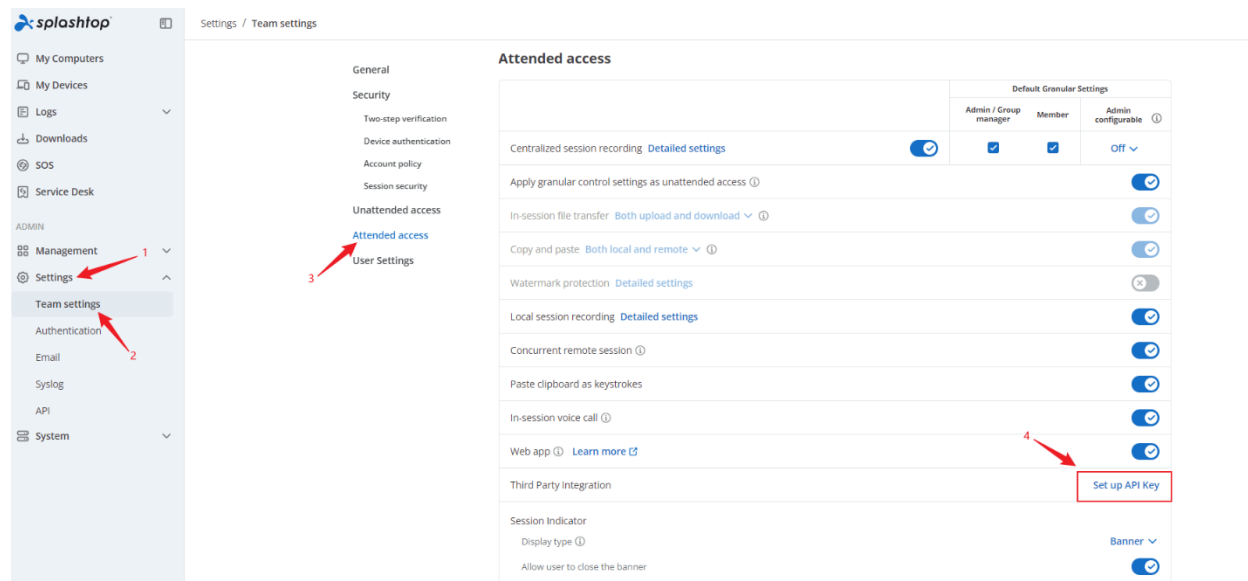
The setup of Splashtop On-Prem - Freshservice Integration is a one-time effort to connect the two systems using an API key. You'll need an administrator account for both Splashtop On-Prem and Freshservice to carry out the task.

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 **Settings > Team Settings > Attended access > Third Party Integration**.

Click on the button [Setup API Key](#).



In the pop-up window, check the checkbox at the beginning of the Freshservice row. This would generate an API key in the Key field.

Set up API Keys



The API key can be replaced with a new one by clicking on **Get New Key** button. The previous key will then be nullified.

Device/Browser authentication

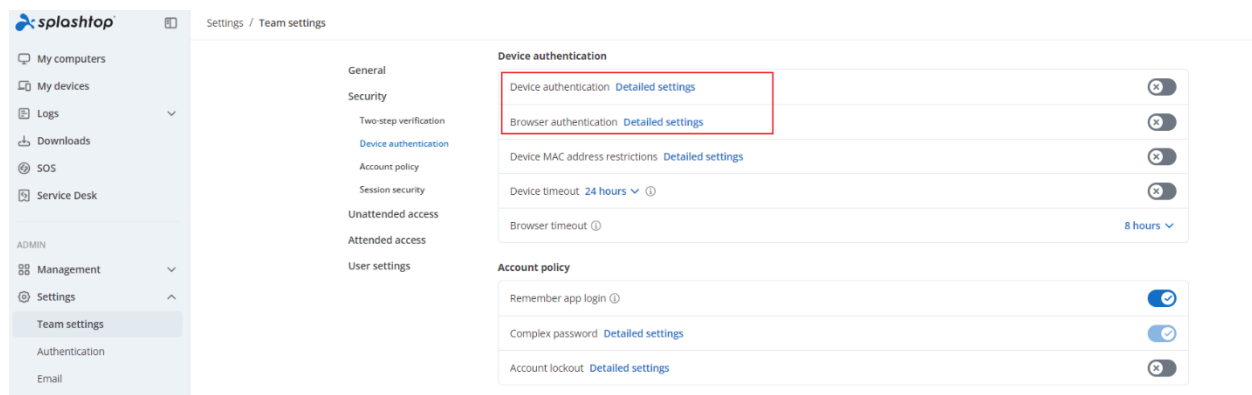
For better security, all devices where you run the Splashtop On-Prem app and log in with your Splashtop Account now need to be authenticated via email or web console.

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-> Settings -> 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.



splashtop Settings / Team settings

General
Security
Two-step verification
Device authentication
Account policy
Session security
Unattended access
Attended access
User settings

Device authentication

- Device authentication [Detailed settings](#) 
- Browser authentication [Detailed settings](#) 
- Device MAC address restrictions [Detailed settings](#) 
- Device timeout 24 hours 
- Browser timeout  8 hours

Account policy

- Remember app login 
- Complex password [Detailed settings](#) 
- Account lockout [Detailed settings](#) 

Device Authentication

SSO Group/AD Group users are not supported as authenticators

Email authentication

 Add a valid [SMTP Server](#) to enable email authentication

Web console authentication

Manage authentication at Management > Authentication Requests when feature enabled

☒ Team owner ☐ All admins

[Add specific admins](#)

Authentication request expiration

☐ 30 minutes ☐ 2 hours ☐ 24 hours ☒ 48 hours

Authenticated Duration

☐ 1 day ☐ 7 days ☐ 30 days ☒ Forever

Cancel

Save

Browser Authentication ✕

SSO Group/AD Group users are not supported as authenticators

Email authentication

 Add a valid [SMTP Server](#) to enable email authentication

Web console authentication

Manage authentication at [Management > Authentication Requests](#) when feature enabled

☒ Team owner ☐ All admins

[Add specific admins](#)

Authentication request expiration ⓘ

☐ 30 minutes ☒ 2 hours ☐ 24 hours ☐ 48 hours

Authenticated Duration

☐ 1 day ☐ 7 days ☐ 30 days ☒ Forever

Cancel

Save

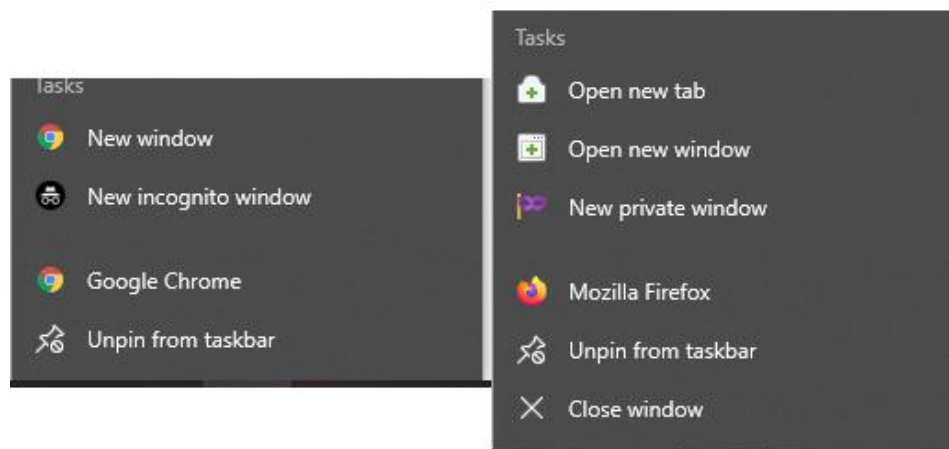
Why am I not getting verification emails?

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 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

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

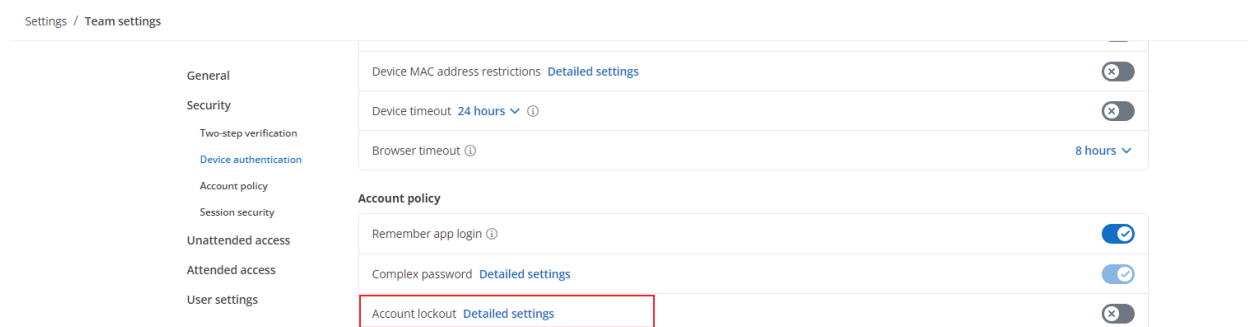
Account lockout threshold: The policy setting determines the number of failed login attempts that will cause a user account to be locked.

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

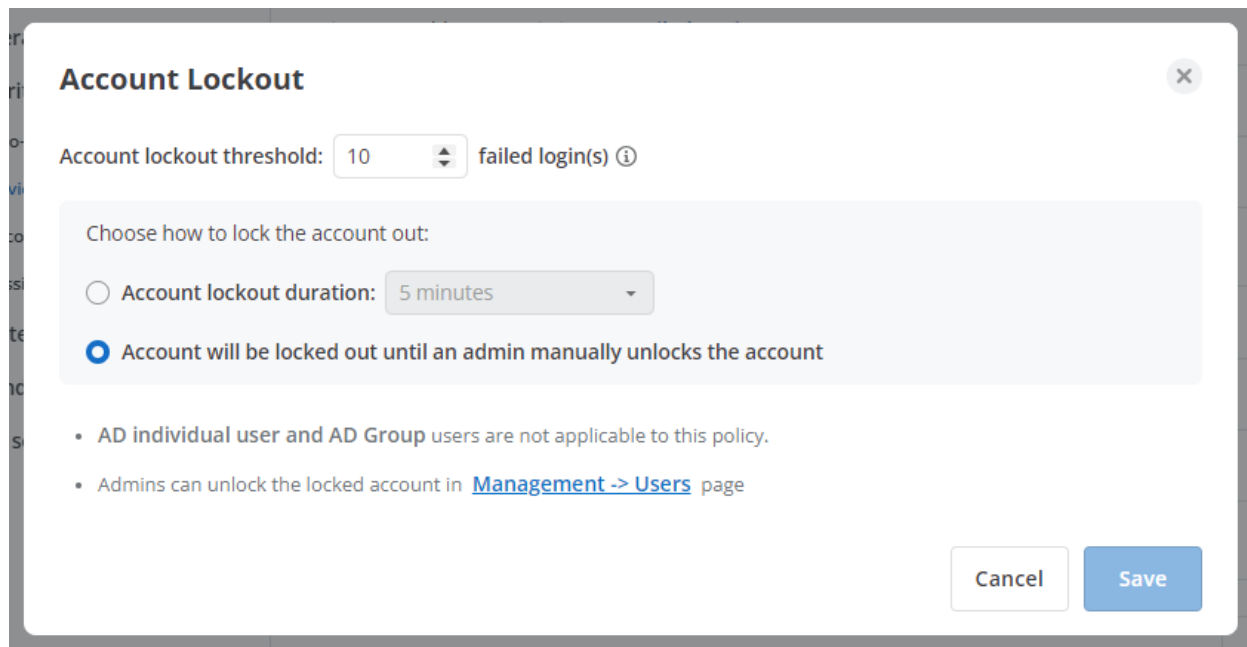
How to set the account lockout policy?

1. Log into Gateway's management console as Owner, go to Settings > Team Settings > Account policy > Account lockout.



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.



Account Lockout [X]

Account lockout threshold: failed login(s) ⓘ

Choose how to lock the account out:

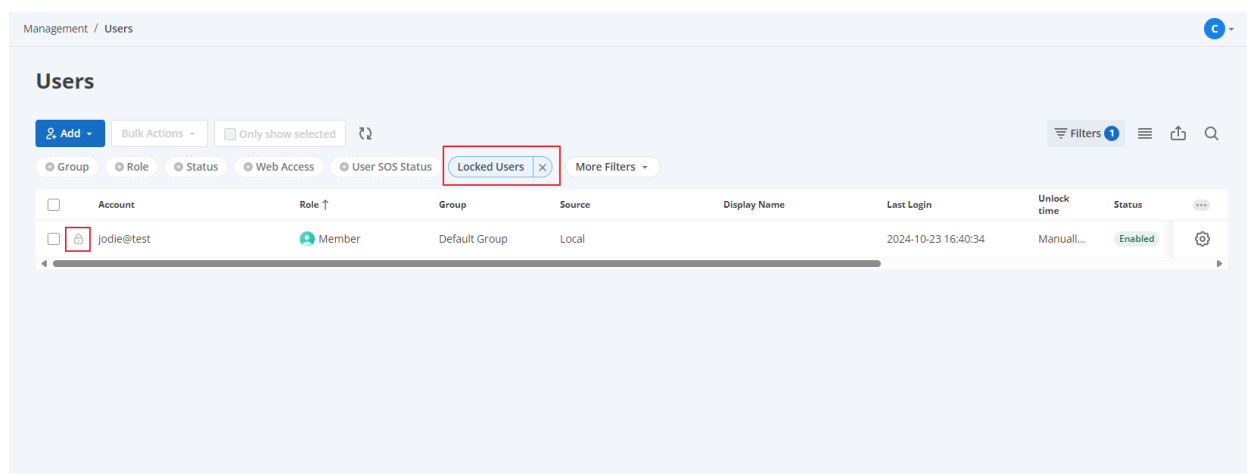
☐ Account lockout duration:

☒ Account will be locked out until an admin manually unlocks the account

- AD individual user and AD Group users are not applicable to this policy.
- Admins can unlock the locked account in [Management -> Users](#) page

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".



Management / Users

Users

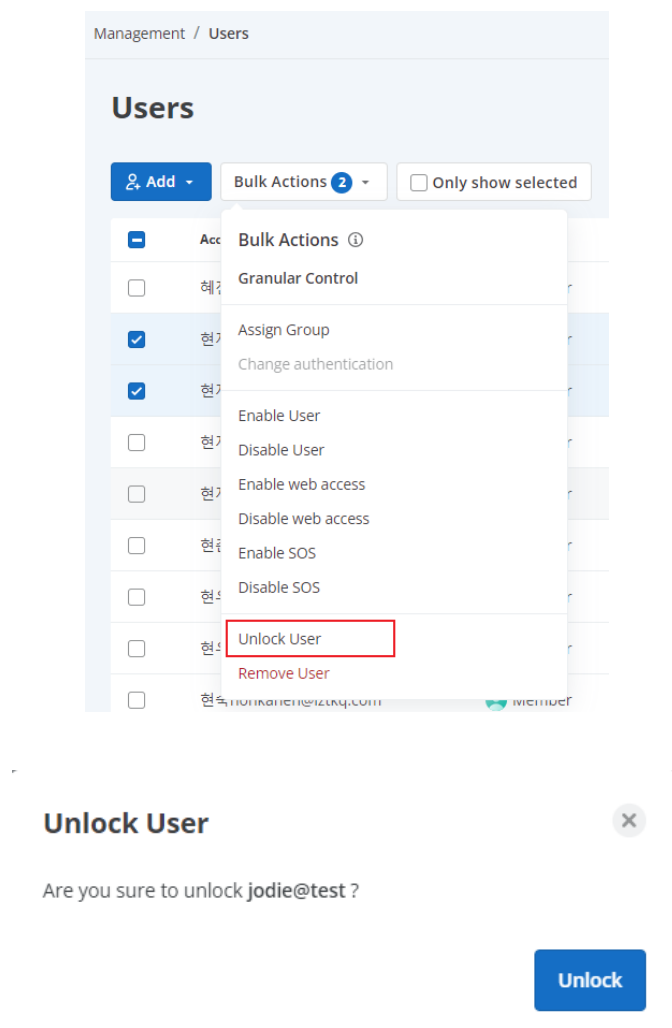
Bulk Actions Only show selected

Filters 1 [X] [Menu] [Share] [Search]

☒ Group ☐ Role ☐ Status ☐ Web Access ☐ User SOS Status ☒ Locked Users [X] More Filters

☐	Account	Role ↑	Group	Source	Display Name	Last Login	Unlock time	Status	...
☒	jodie@test	Member	Default Group	Local		2024-10-23 16:40:34	Manuall...	Enabled	[Settings]

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



Getting notified when a computer goes online or offline

Splashtop On-Prem supports notifications for computer online and offline status. These notifications can only be configured by the Owner.

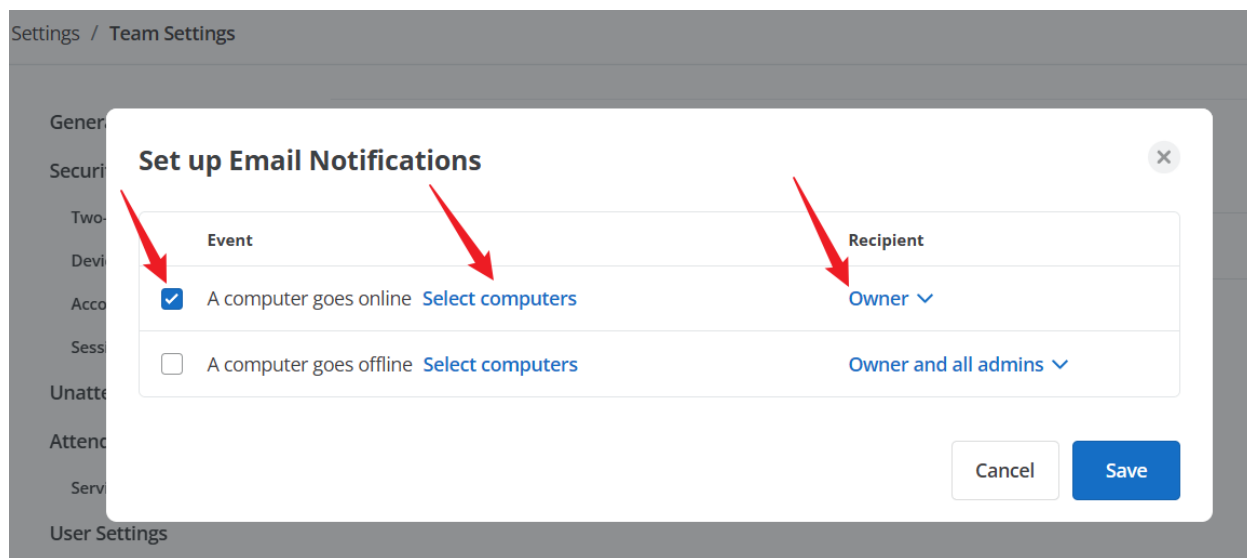
Getting started

Log in to the Gateway web console and navigate to *Settings -> Team Settings*.

Miscellaneous

Notification	Set up Email Notifications
--------------	--

Then click on the "Set up Email Notifications" link. You can enable/disable notifications and configure who receives them.



Settings / Team Settings

Set up Email Notifications

Event	Recipient
☒ A computer goes online Select computers	Owner ▼
☐ A computer goes offline Select computers	Owner and all admins ▼

Cancel Save

Choose the computers to monitor. Recipients will be notified when their status changes.

Select computers



Get notified when changes are made on the selected computers.

- ☐ All computers
- ☒ Only specific computers and computer groups

Select groups

☐ Only show selected

 Test - Connection Pool (0)

☐

 Test 1 (0)

☐

 Test 2 (0)

☐

 Test 3 (0)

☐

 Test 4 (0)

☐

 Test 5 (1)

☒

 Test 6 (0)

☐

 a (1)

☐

0 Group(s) Selected

Clear all

Select computers

☐ Only show selected

> Default Group

> Test - Connection Pool

> Test 1

> Test 2

> Test 3

> Test 4

> Test 5

> Test 6

1 Computer(s) Selected

Clear all

Cancel

OK

Notes

This feature takes effect when the SMTP server is enabled.

Session Transcript

Starting from version 3.36.0, Splashtop Gateway introduces support for **Session Transcripts**, enabling administrators and auditors to review textual records of user sessions for security and compliance purposes. This includes transcripts for:

Chat Transcript

Records all chat conversations between the technician and the remote user during a remote support session.

Remote Command Transcript

Captures all commands executed via the Remote Command feature.

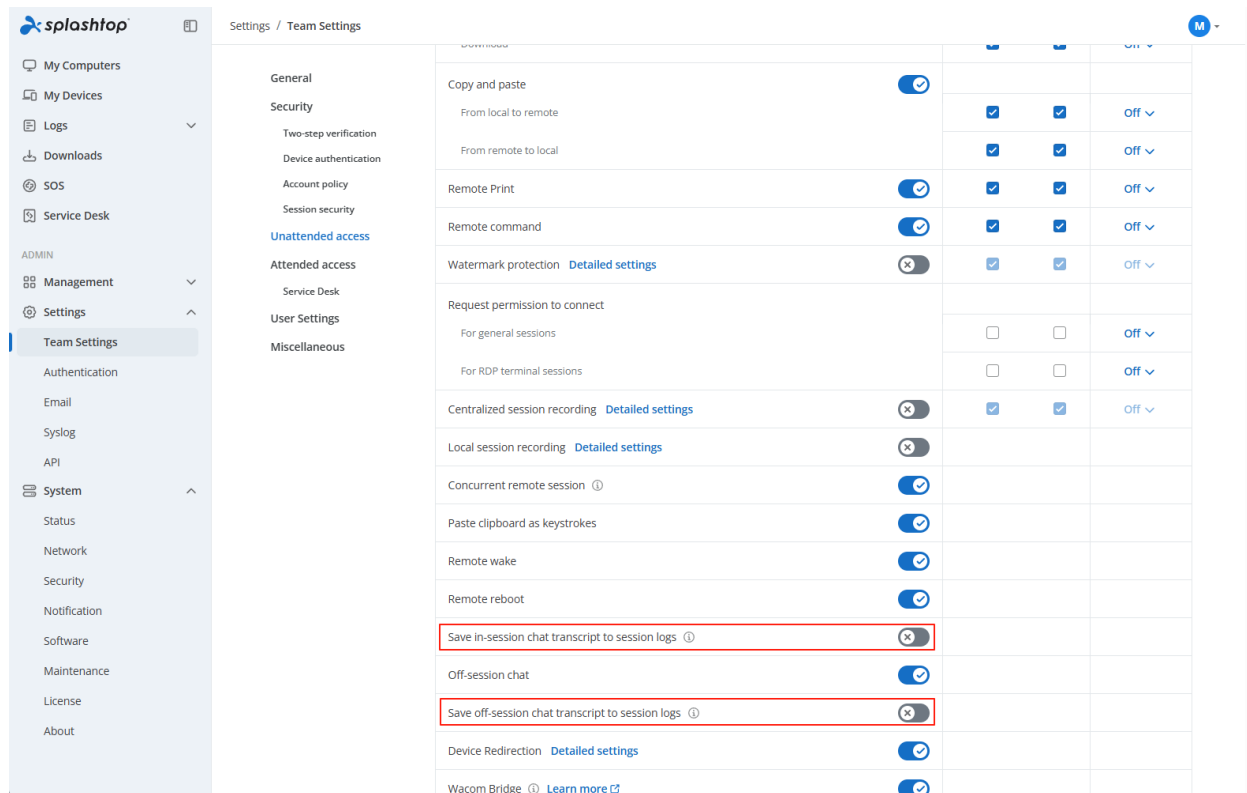
SSH Transcript

Records the terminal input/output of SSH sessions initiated through Splashtop.

How to enable chat transcripts?

Team Owner can either enable/disable the option to save in-session and off-session chat transcripts to session logs in Team Settings. (Requires On-Prem Streamer v3.7.4.5 or above).

For **Unattended access**, navigate to **[Settings] > [Team Settings] > [Unattended access]** in your Gateway.



Settings / Team Settings

General

Security

Two-step verification

Device authentication

Account policy

Session security

Unattended access

Attended access

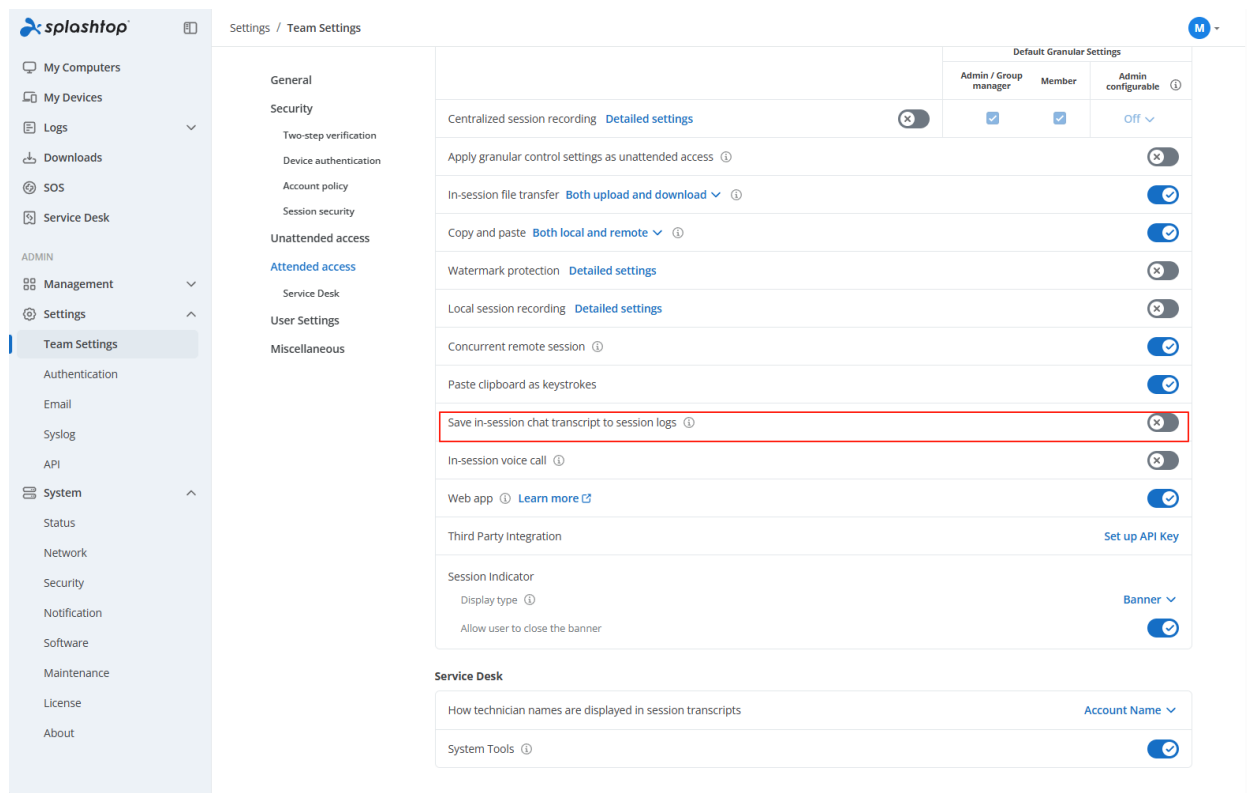
Service Desk

User Settings

Miscellaneous

Setting	Value	Value	Value
Copy and paste	On		
From local to remote	On	On	Off
From remote to local	On	On	Off
Remote Print	On	On	Off
Remote command	On	On	Off
Watermark protection Detailed settings	Off	On	Off
Request permission to connect			
For general sessions	Off	Off	Off
For RDP terminal sessions	Off	Off	Off
Centralized session recording Detailed settings	Off	On	Off
Local session recording Detailed settings	Off		
Concurrent remote session ⓘ	On		
Paste clipboard as keystrokes	On		
Remote wake	On		
Remote reboot	On		
Save in-session chat transcript to session logs ⓘ	Off		
Off-session chat	On		
Save off-session chat transcript to session logs ⓘ	Off		
Device Redirection Detailed settings	On		
Wacom Bridge ⓘ Learn more	On		

For **Attended access**, navigate to **[Settings] > [Team Settings] > [Attended access]** in your Gateway.



The screenshot displays the Splashtop On-Prem Admin interface. On the left is a navigation menu with categories like 'My Computers', 'My Devices', 'Logs', 'Downloads', 'SOS', 'Service Desk', 'ADMIN', 'Management', 'Settings', and 'Team Settings'. The 'Team Settings' page is active, showing a sidebar with 'General', 'Security', 'Unattended access', 'Attended access', 'Service Desk', 'User Settings', and 'Miscellaneous'. The main content area is titled 'Settings / Team Settings' and contains a table of settings. The 'Default Granular Settings' table has columns for 'Admin / Group manager', 'Member', and 'Admin configurable'. The 'Save in-session chat transcript to session logs' setting is highlighted with a red box and is currently disabled (toggle off). Other settings include 'Centralized session recording', 'Apply granular control settings as unattended access', 'In-session file transfer', 'Copy and paste', 'Watermark protection', 'Local session recording', 'Concurrent remote session', 'Paste clipboard as keystrokes', 'In-session voice call', 'Web app', 'Third Party Integration', 'Session Indicator', and 'Service Desk'.

How to view these transcripts?

If you have the chat saving option enabled, you can see the transcripts in your web console. Navigate to **[Logs] > [Chat]** to get the saved chat transcripts.

You can see the transcripts in your web console. Navigate to **[Logs] > [Remote Command]** to get the saved chat transcripts.

You can see the transcripts in your web console. Navigate to **[Logs] > [SSH]** to get the saved SSH transcripts.

Authentication

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.

Settings / Authentication

[Single Sign-On](#) [AD Authentication](#)

General Settings

SSO Name * SSO method name for display purpose

Notes

Identity Provider Settings

Please copy these configurations or download the Service Provider Metadata to create a custom app in your Identity Provider. [Download](#)

Entity ID onpremise.splashtop.com

Assertion consumer service URL https://test.gatewayaddr.com:443/api/saml/acs

Service Provider Settings

Protocol SAML 2.0

IDP type ADFS

☐ Enable force authentication
Enable this item to require SSO users to re-login to the IDP each time.

☐ Enable login hint
Enable this item to pre-fill the SSO user name in IDP.

Metadata ☒ Import an XML file ☐ Import from URL ☐ Add manually

XML file * Select XML file [Select](#)

[Save](#)

[Back](#)

- **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.

Default	SSO Name ↑	Protocol	IDP Type	Status	Device Authentication	Browser Authentication	
☒	ADFS	SAML 2.0	ADFS	✓	☒	☒	⚙️
☐	ADFS 2	SAML 2.0	ADFS	✓	☐	☒	⚙️
☐	Okta	SAML 2.0	Okta	✓	☐	☒	⚙️

- 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)**.

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 **Settings > Authentication > AD Authentication**

Add AD Server

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

Name *	AD server name for display purpose
LDAP URL *	LDAP access URL address
Users Base DN *	AD location to search users (distinguished name)
Groups Base DN *	AD location to search groups (distinguished name)
Alternative UPN Suffixes ⓘ	example.com Maximum 30
Bind Account *	AD account to access the AD server
Password *	AD account password

- **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 release user seats. 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 Remove button.

Settings / Authentication

Single Sign-On **AD Authentication**

[Add AD Server](#) [Remove Unsolvable AD Group Members](#)

Name ↑	LDAP URL	Users Base DN	Groups Base DN	Bind Account
CBK				

Authentication / Unsolvable AD group members

Unsolvable AD group members

Unsolvable AD group members - users not found in all the AD servers but still stored in Splashtop Gateway Database.
Remove the enabled unsolvable AD group members to release user seats.



☒ Group Member Account ↓	Display Name	Status
☒ bob.doe@m1.com		Invalid

1 Selected

[Remove](#) [Back](#)

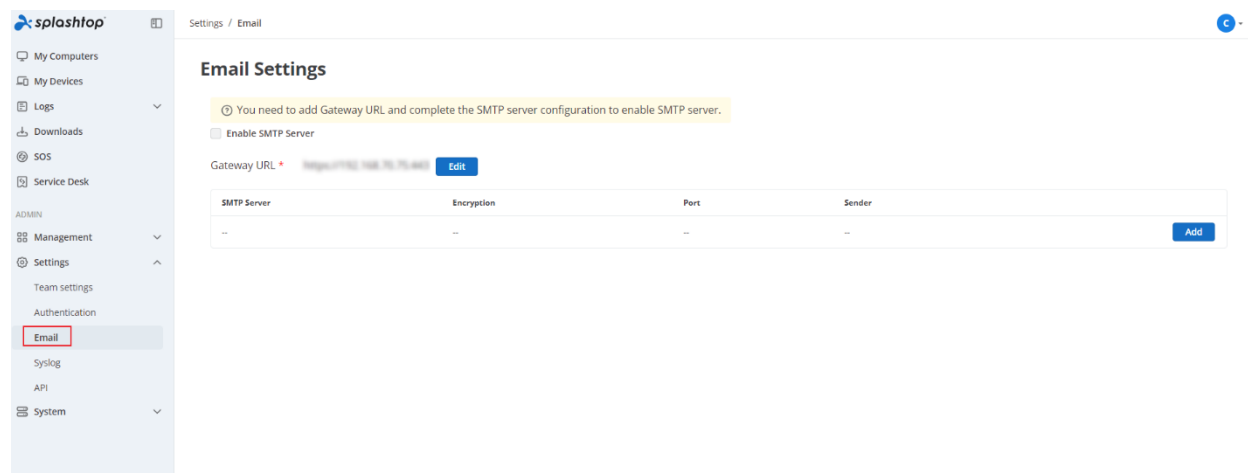
Email settings (SMTP server integration)

Introduction

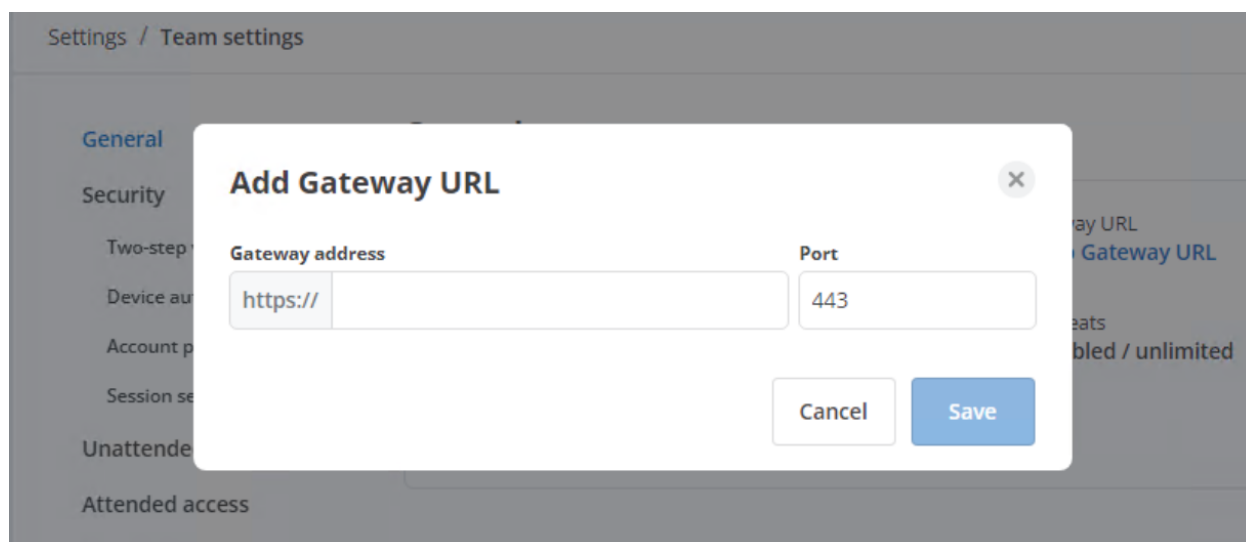
SMTP Server is a feature that allows you to integrate a Smtplib server to Splashtop On-Prem Gateway in the team settings. When SMTP server is successfully configured, devices can be authenticated by email.

SMTP Server Configuration

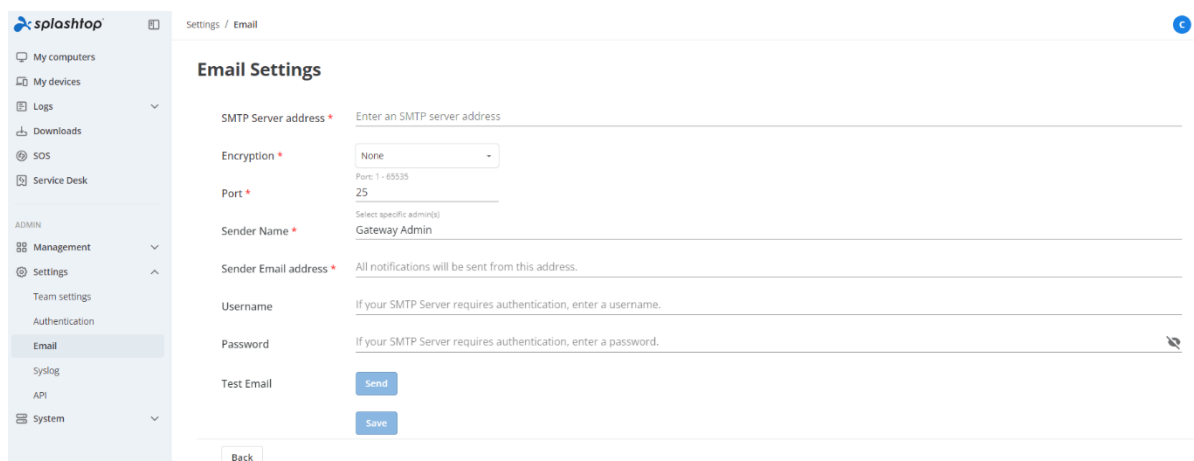
- First, go to <https://gatewayaddress> -> Settings -> Email to configure the **SMTP server**. The SMTP server can only be enabled if all required information has been successfully saved



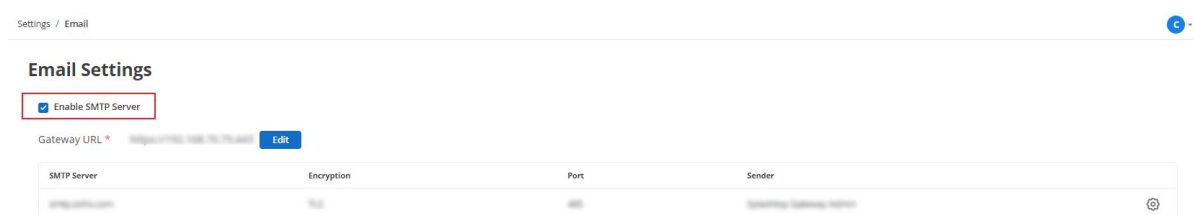
- Click "Add" to embed the Gateway URL in your Email. In the scenario that Gateway server is behind layers of firewall, Splashtop Gateway itself has limited capability to acquire its public address, thus requests origin from user's Email client would fail to reach Gateway and result in failure of some 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.

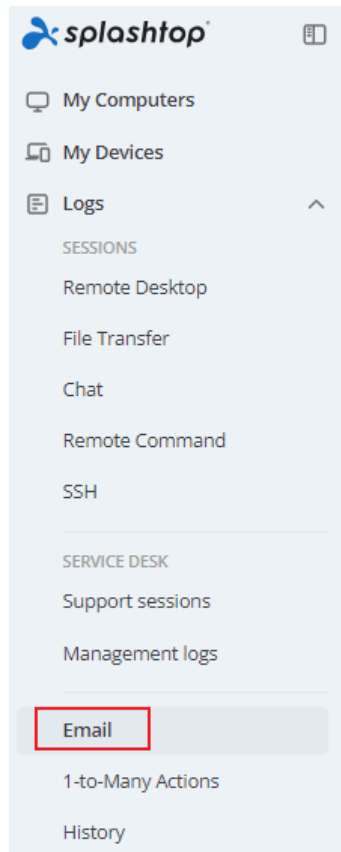


- When Gateway URL and SMTP server settings are successfully saved, click the check box to enable SMTP server.



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.



- In the email log, a separate log is generated for each mail sent. Each log consists of time, status, source, subject, sender, recipient and type.

Email Logs

 Refresh

Last 7 Days 

Time	Status	Subject	Source (i)	Sender	Recipient	Type
2024-10-31 16:39:55	Send successful	Splashtop On-Prem user authentication	xxxxxx@xxxxxx.com	xxxxxx@xxxxxx.com	xxxxxx@xxxxxx.com	Browser authentication

Export as CSV: 2024/10

< 1 > 10 / page

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.

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.

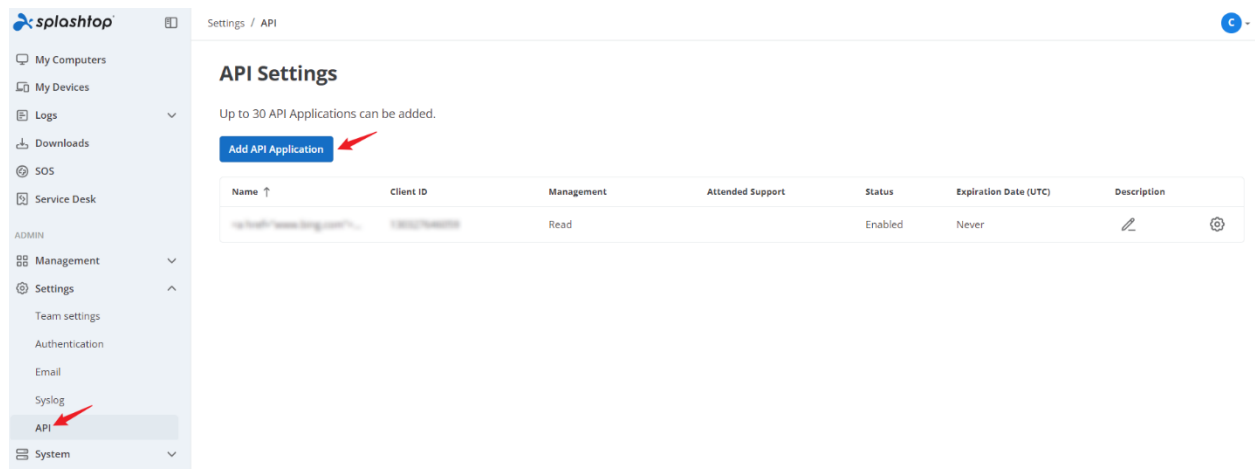
For more details, please refer to the [API reference](#).

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 **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.

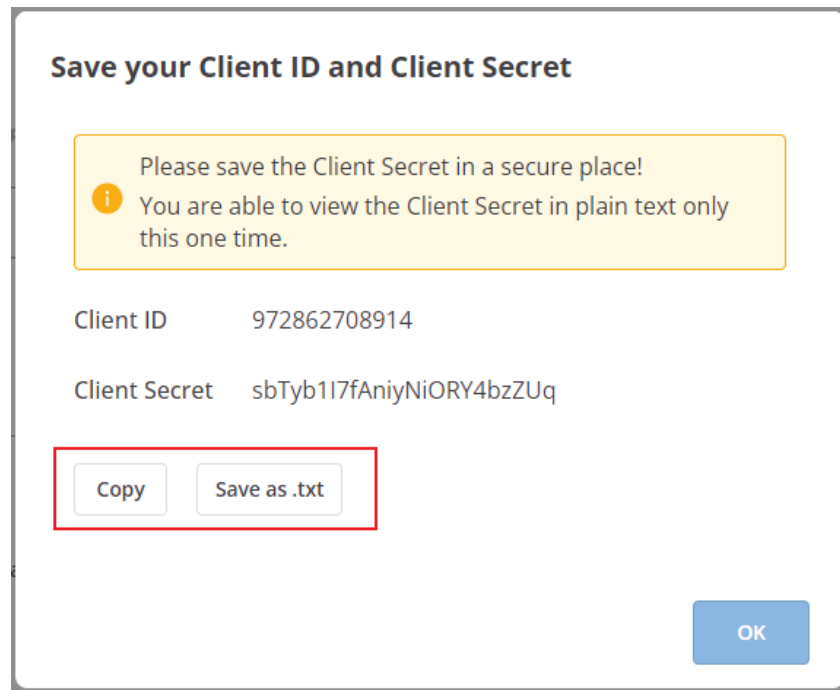
Settings / API

API Settings

Name *	API application name for display purpose *		
Description			
Permissions *	Read	Write	
Management	☐	☐	
Attended Support	☐	☐	
Expiration Date (UTC)	☐ Enable Expiration Date		
	Select Date	Select Time	
	2024-10-25 	14:25 	
Status	☒ Enable API application		
	<button>Add</button>		

[Back](#)

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](#)

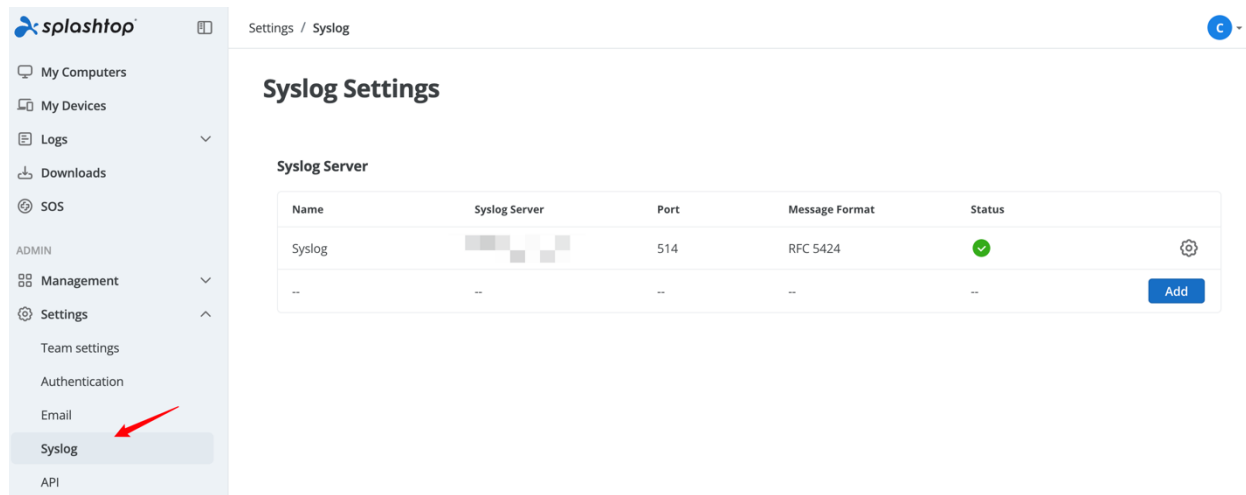
Syslog

In addition to accessing logs from web console, Splashtop log events can also be sent to a Syslog server or SIEM tool that support Syslog in your local environment. The auditing of Splashtop event logs can be accessed both from Gateway web console, download as CSV or Syslog collectors simultaneously.

1. Configuration

1. To configure Splashtop Gateway as Syslog source, log in web console as Team Owner, go to Settings → Syslog.

2. You can configure Gateway to send Syslog messages up to two Syslog servers.



The screenshot shows the Splashtop web console interface. On the left is a sidebar with a navigation menu. Under the 'Settings' section, 'Syslog' is highlighted with a red arrow. The main content area is titled 'Syslog Settings' and contains a table for 'Syslog Server' configuration.

Name	Syslog Server	Port	Message Format	Status
Syslog		514	RFC 5424	
--	--	--	--	--

An 'Add' button is located at the bottom right of the table.

3. Click add to configure your target Syslog server.

Add Syslog Server

Name *

Syslog Server address *

Port
System listen port: 1 ~ 65535

Syslog Protocol

Message Format

Facility

Severity

Status ☒ Enable Syslog Server

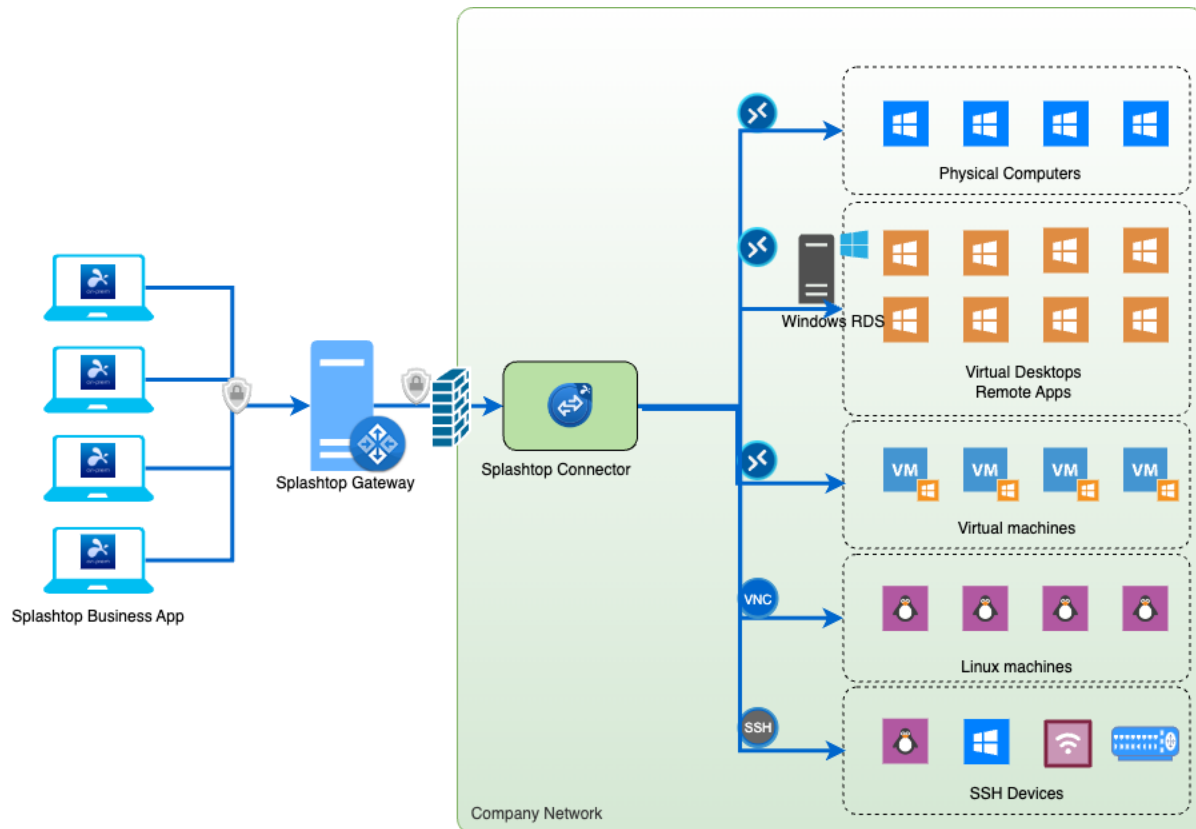
Test Message ⓘ

4. Syslog Settings

Name	Syslog host name in Splashtop Gateway.
Syslog Server address	Enter the hostname or IP address of the syslog server receiving log messages.
Port	Syslog over UDP defaults to use port 514. The defaults can be changed.
Syslog Protocol	Supports UDP or TCP.
Message Format	Supports RFC 5424 or RFC 3164 (BSD).
Facility	Choose proper facility from local0 - local7.
Severity	Choose the proper Syslog severity.
Status	Once enabled, Splashtop Gateway starts to send persistent syslog messages to your Syslog Server.
Test Message	Send a message to your Syslog Server to test the above settings.

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](#)

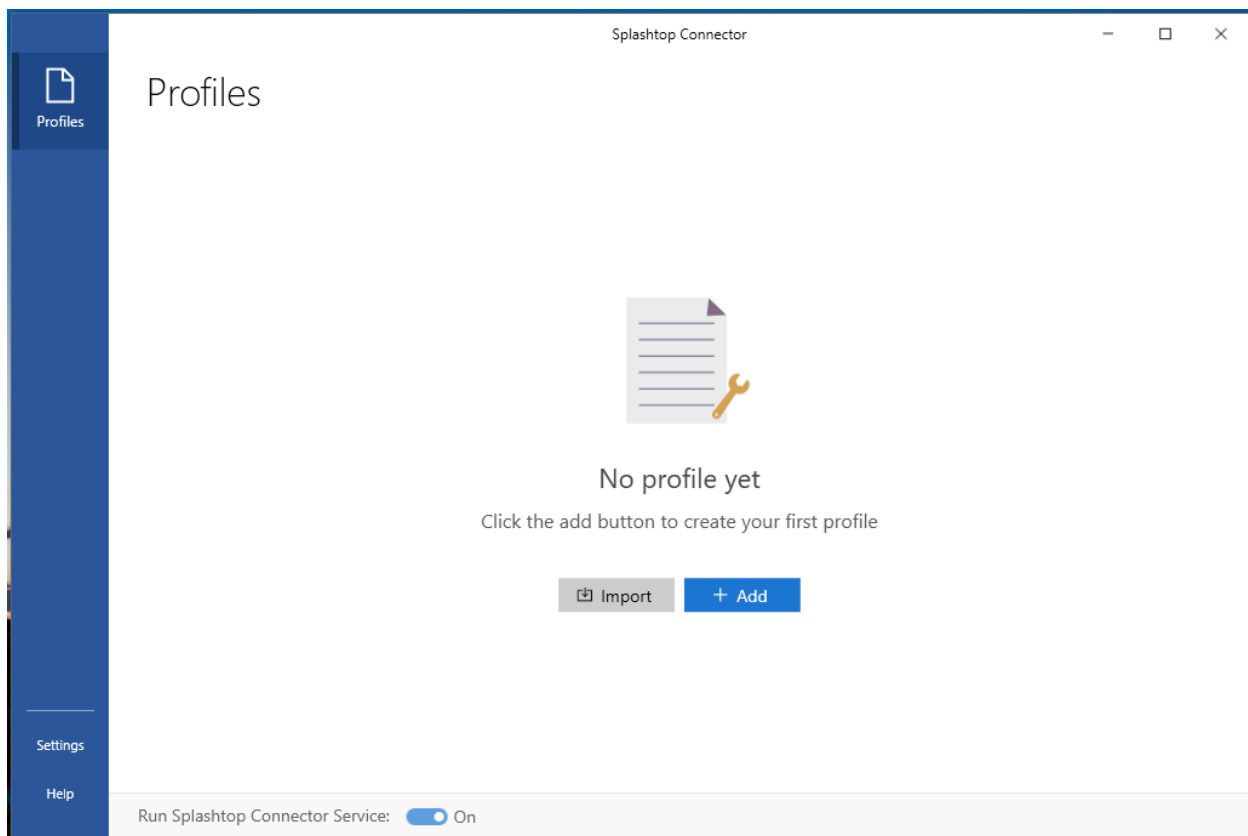
System requirements

- 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.

Add Profile

General

Streamer Settings

RDP Settings

1. General

Profile Name *

Give the profile a name to display in the list.
Maximum 64 characters. Name cannot contain <>,:\"

☐ Enable session recording

Turn on this option to automatically record the sessions.

2. Streamer Settings

Enter a deployment code from your Splashtop account to specify the default settings of the RDP session's virtual streamer.
[Learn more.](#)

Gateway Address *

Click the edit button on the right to configure your Splashtop Gateway address.

Deploy Code *

Enter the Splashtop deployment code.

☐ Enable this profile immediately after saving

Save Cancel

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.

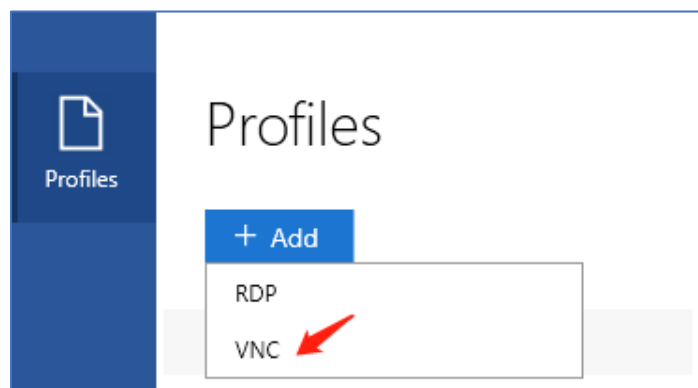
You can enable this profile immediately by turning on **Enable this profile immediately after saving**, or enable it in the main window.

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.



Add Profile

General

Streamer Settings

VNC Settings

1. General

Profile Name *

Give the profile a name to display in the list.
Maximum 64 characters. Name cannot contain <>,:;"*+=\%|?&

☐ Enable session recording
Turn on this option to automatically record the sessions.

2. Streamer Settings

Enter a deployment code from your Splashtop account to specify the default settings of the VNC session's virtual streamer.
[Learn more.](#)

Gateway Address *

Click the edit button on the right to configure your Splashtop Gateway address.

Deploy Code *

Enter the Splashtop deployment code.

3. VNC Settings

Specify VNC Parameters [Learn more.](#)

Remote Computer

☐ Ask user to specify which remote computer to connect to

☒ Fixed remote computer with specified information

☐ Enable this profile immediately after saving

SaveCancel

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

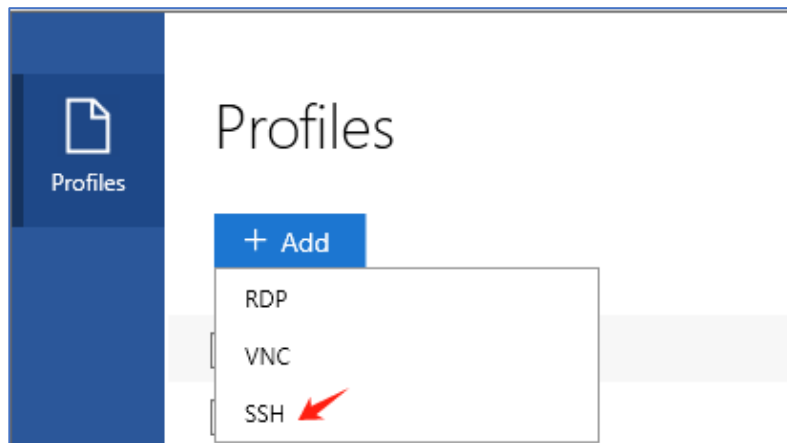
You can enable this profile immediately by turning on **Enable this profile immediately after saving**, or enable it in the main window.

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.



Add Profile

General

Streamer Settings

SSH Settings

1. General

Profile Name *

Give the profile a name to display in the list.
Maximum 64 characters. Name cannot contain <>,:;"*+=\%|?&

☐ Save session transcript locally
Enable local saving of session transcripts

2. Streamer Settings

Enter a deployment code from your Splashtop account to specify the default settings of the SSH session's virtual streamer.
[Learn more.](#)

Gateway Address *

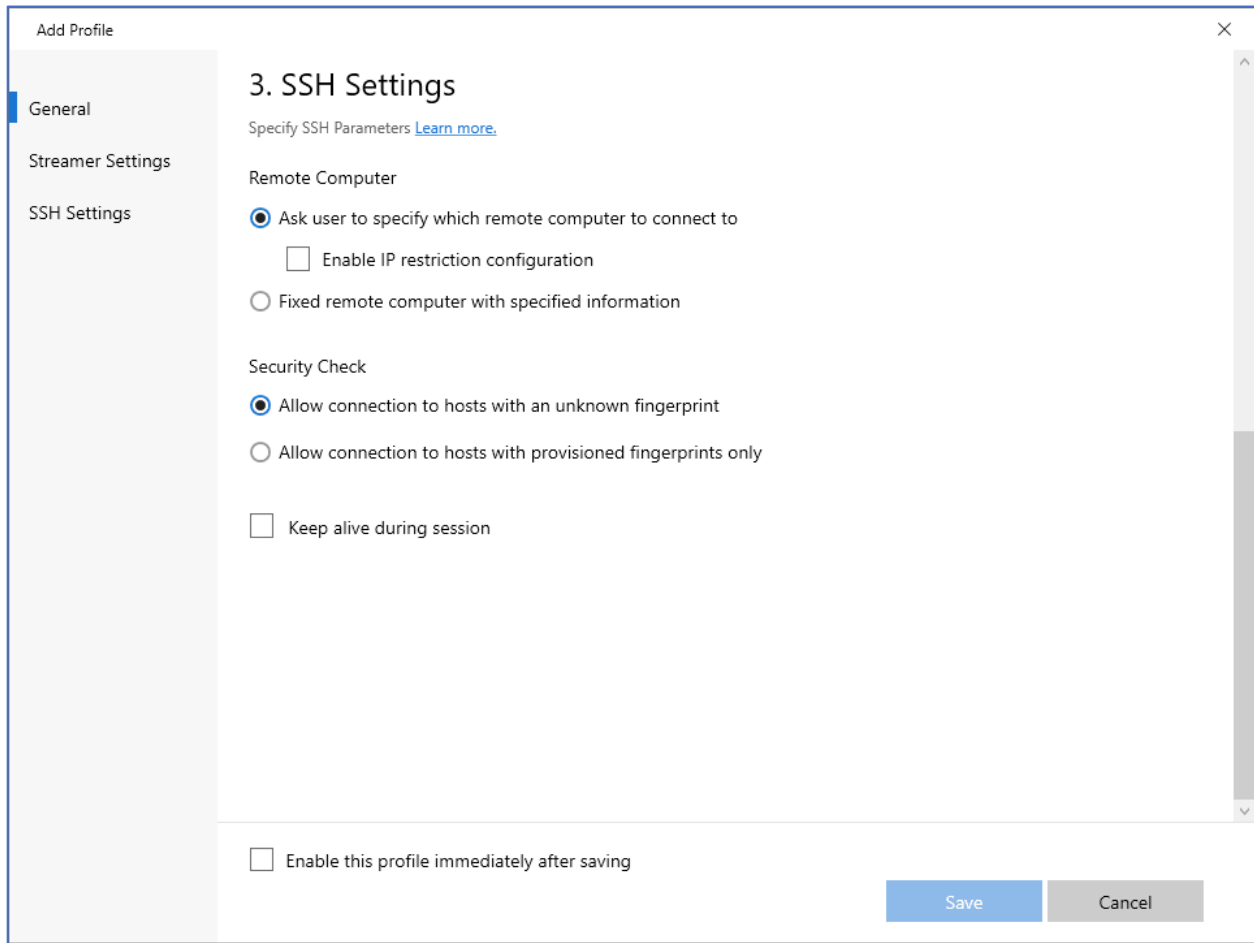
Click the edit button on the right to configure your Splashtop Gateway address.

Deploy Code *

Enter the Splashtop deployment code.

☐ Enable this profile immediately after saving

SaveCancel



Add Profile

General

Streamer Settings

SSH Settings

3. SSH Settings

Specify SSH Parameters [Learn more.](#)

Remote Computer

- ☒ Ask user to specify which remote computer to connect to
 - ☐ Enable IP restriction configuration
- ☐ Fixed remote computer with specified information

Security Check

- ☒ Allow connection to hosts with an unknown fingerprint
- ☐ Allow connection to hosts with provisioned fingerprints only

☐ Keep alive during session

☐ Enable this profile immediately after saving

Save Cancel

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.

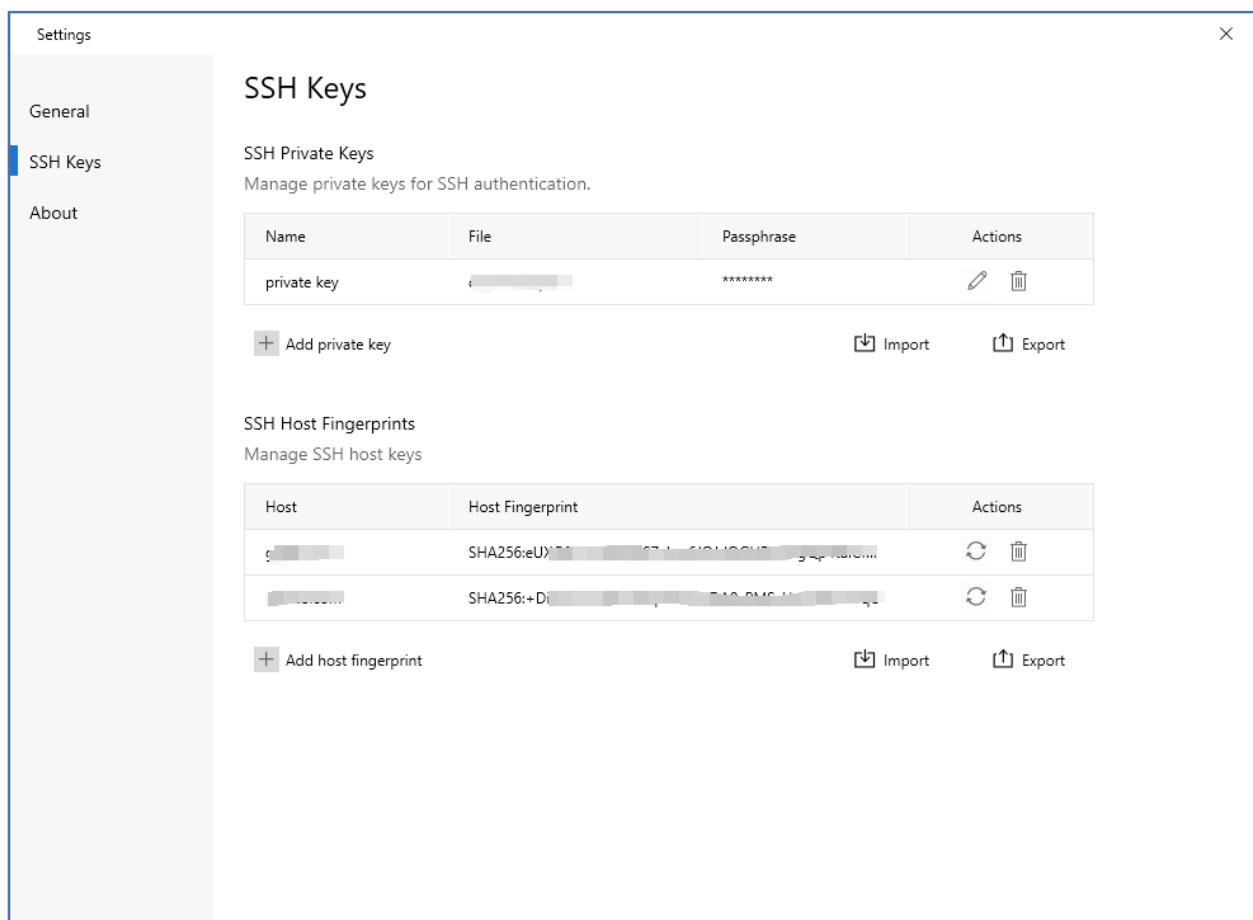
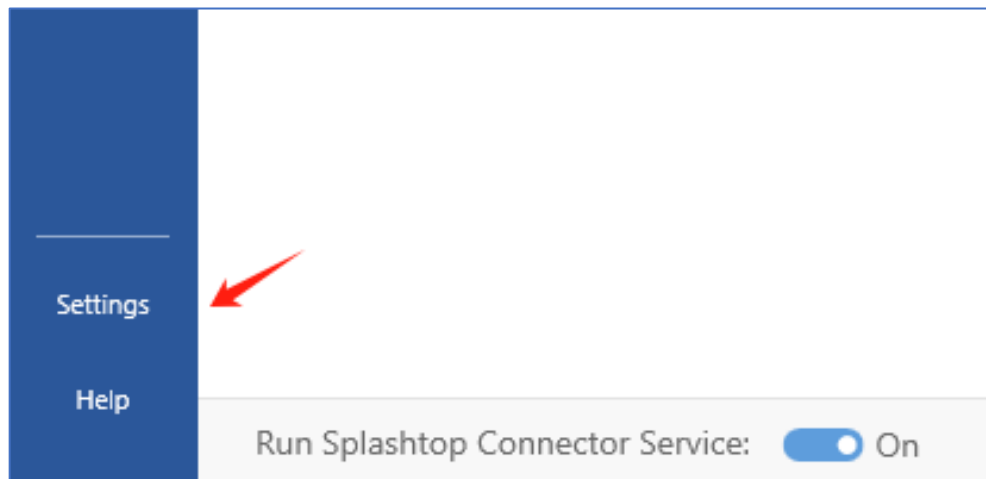
SSH Settings

- **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.



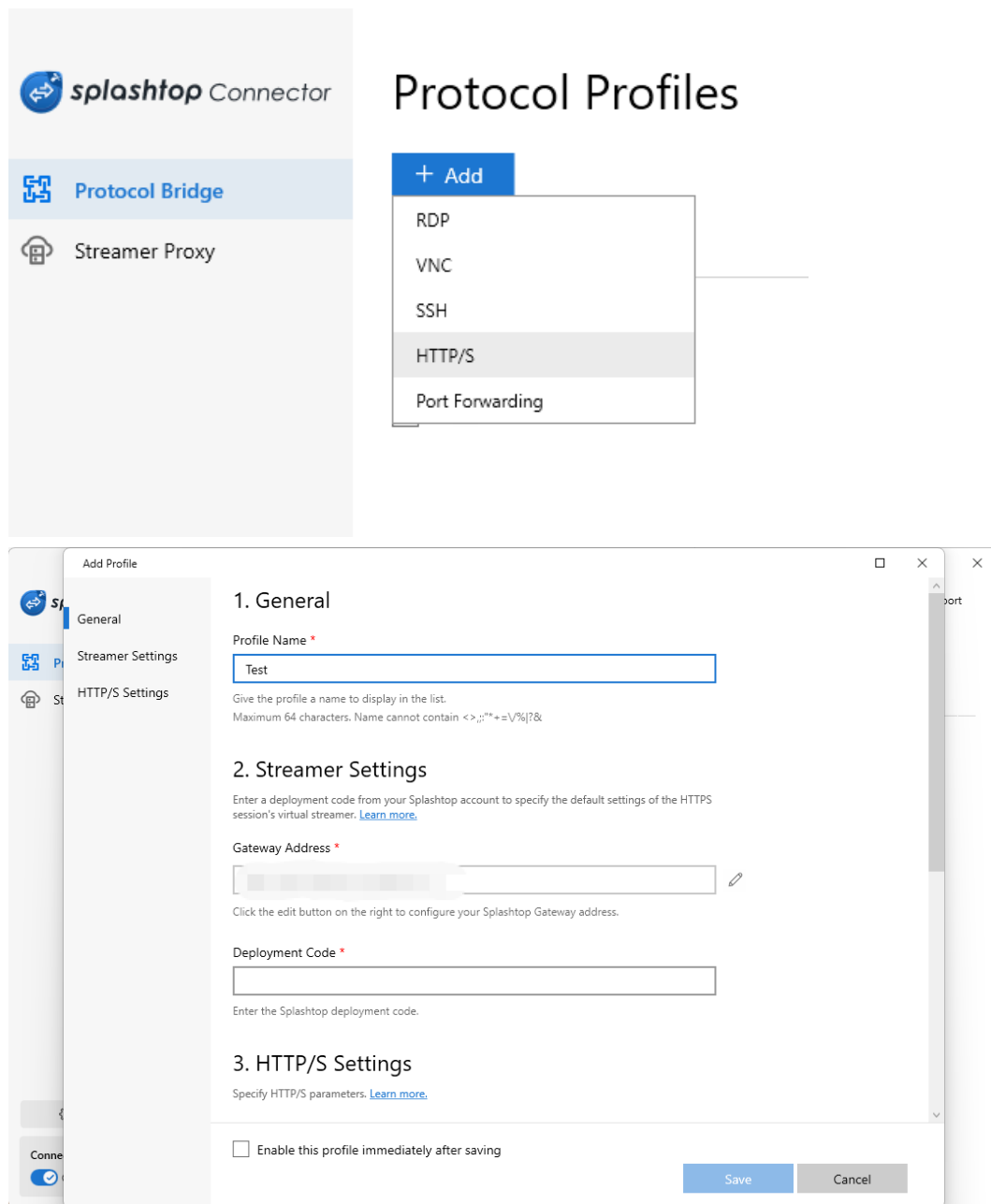
- **SSH Private Keys**, allow IT admins to configure the private keys for SSH authentication by manually adding or importing.

- **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](#).

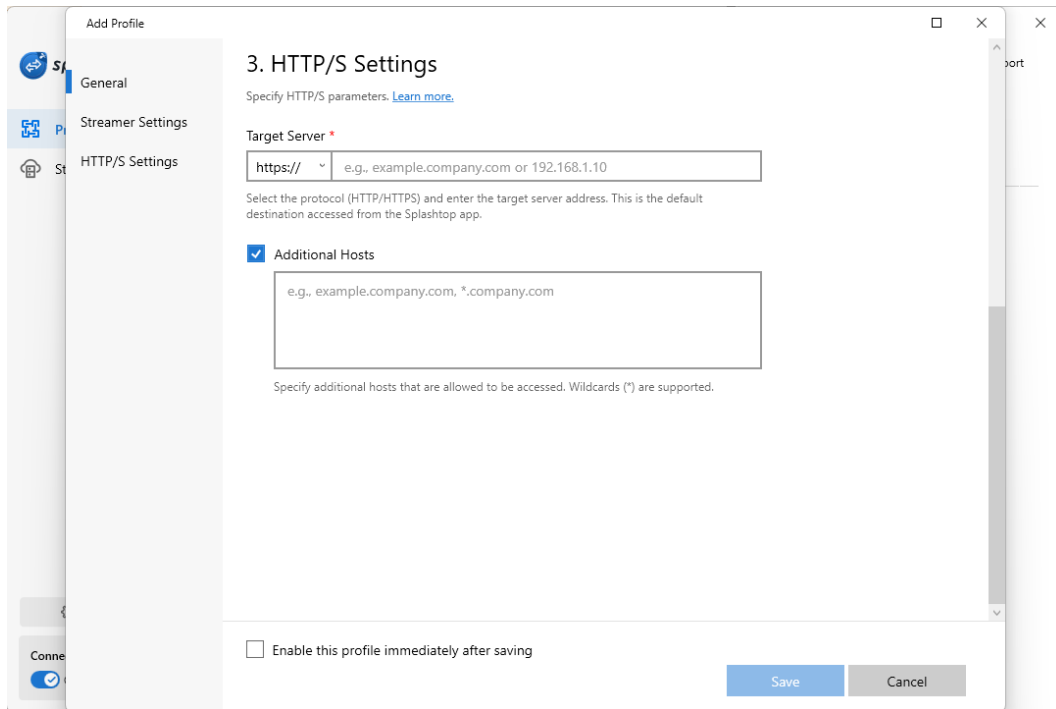
How to create HTTP/S profiles?

Since Splashtop Connector v1.3.0.0, HTTP/S 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 HTTP/S settings. You can create multiple Profiles in the Splashtop Connector. These HTTP/S resources will contribute to the total number of computers on your Splashtop team. Enable the profile to make the HTTP/S resource available for HTTP/S access.



The screenshot displays the Splashtop On-Prem Admin interface. On the left, a sidebar contains the Splashtop logo and the text "splashtop Connector". Below this, there are three menu items: "Protocol Bridge" (highlighted with a blue bar), "Streamer Proxy", and "Streamer Settings". The main content area is titled "Protocol Profiles". A blue "+ Add" button is visible, and a dropdown menu is open, showing the following options: "RDP", "VNC", "SSH", "HTTP/S" (which is highlighted), and "Port Forwarding".

Below the main content area, a "Add Profile" dialog box is open. The dialog has a sidebar with three tabs: "General", "Streamer Settings", and "HTTP/S Settings". The "General" tab is selected. The "General" section contains a "Profile Name" field with the value "Test". Below this, there is a note: "Give the profile a name to display in the list. Maximum 64 characters. Name cannot contain <>,:\";\"*+=\\%|?&". The "Streamer Settings" section contains a "Gateway Address" field with a masked value and an edit button, and a "Deployment Code" field. Below these, there is a note: "Enter the Splashtop deployment code." The "HTTP/S Settings" section contains a checkbox labeled "Enable this profile immediately after saving". At the bottom right of the dialog are "Save" and "Cancel" buttons.



Add Profile

General

Streamer Settings

HTTP/S Settings

3. HTTP/S Settings

Specify HTTP/S parameters. [Learn more.](#)

Target Server *

https:// e.g., example.company.com or 192.168.1.10

Select the protocol (HTTP/HTTPS) and enter the target server address. This is the default destination accessed from the Splashtop app.

☒ Additional Hosts

e.g., example.company.com, *.company.com

Specify additional hosts that are allowed to be accessed. Wildcards (*) are supported.

☐ Enable this profile immediately after saving

Save Cancel

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 HTTP/S machine is for.

Streamer Settings

- **Deployment Code**, Enter a Splashtop deployment package code to determine the HTTP/S 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.

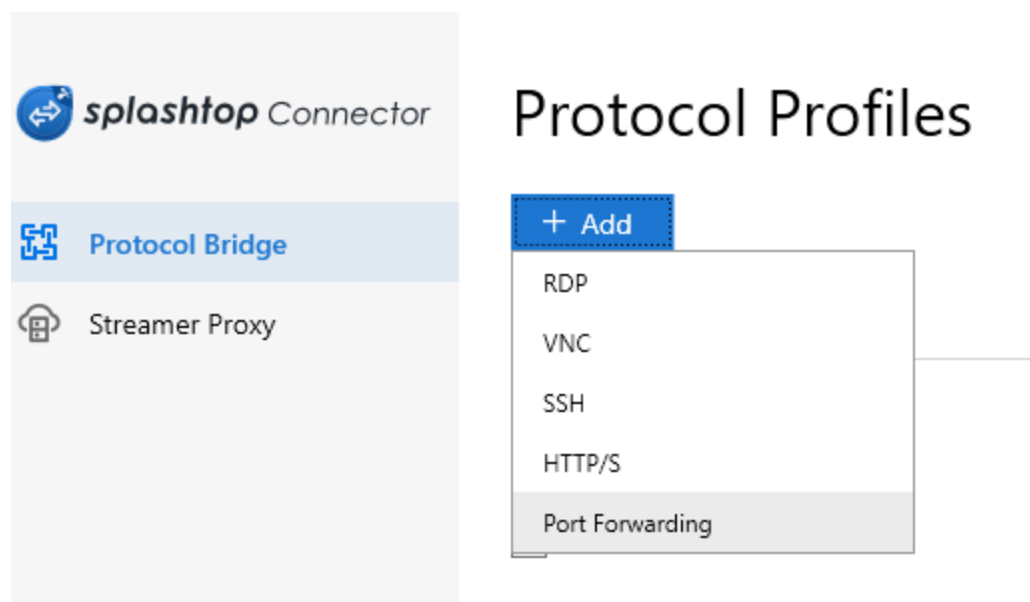
HTTP/S Settings

- **Target Server**, Select the protocol (HTTP/HTTPS) and enter the domain name or IP address of the target server. This is the default destination accessed from the Splashtop app.
- **Additional Hosts**, Optional. Specify any additional hosts that should be allowed for access alongside the Target Server.

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

How to create Port Forwarding profiles?

Since Splashtop Connector v1.3.0.0, Port Forwarding 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 Port Forwarding settings. You can create multiple Profiles in the Splashtop Connector. These Port Forwarding resources will contribute to the total number of computers on your Splashtop team. Enable the profile to make the Port Forwarding resource available for Port Forwarding access.



Add Profile

 Splashtop

General

 Port Forwarding

 Streamers

1. General

Profile Name *

Give the profile a name to display in the list.
Maximum 64 characters. Name cannot contain <>,:;"'*=\\%|?&

2. Streamer Settings

Enter a deployment code from your Splashtop account to specify the default settings of the PORT_FORWARDING session's virtual streamer. [Learn more.](#)

Gateway Address *

Click the edit button on the right to configure your Splashtop Gateway address.

Deployment Code *

Enter the Splashtop deployment code.

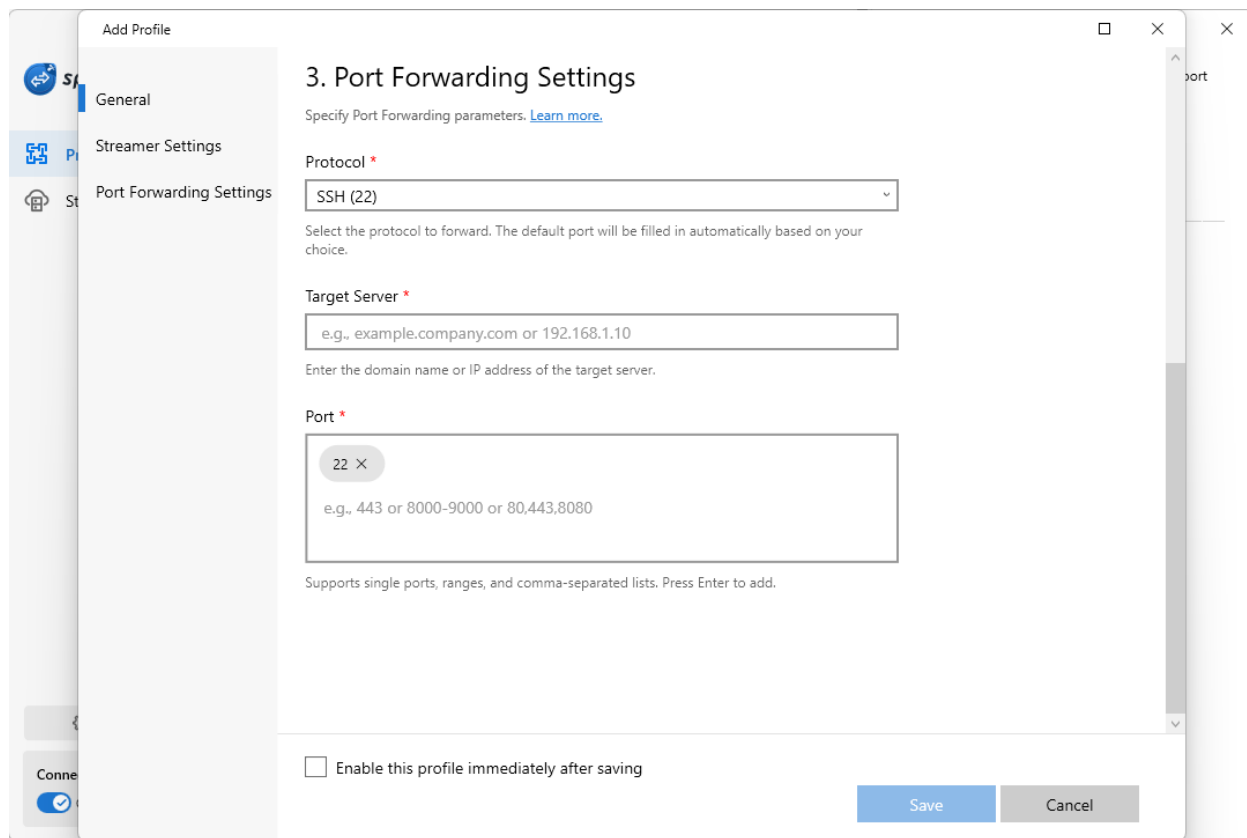
3. Port Forwarding Settings

Specify Port Forwarding parameters. [Learn more.](#)

☐ Enable this profile immediately after saving

Save

Cancel



Add Profile

3. Port Forwarding Settings

Specify Port Forwarding parameters. [Learn more.](#)

Protocol *

SSH (22)

Select the protocol to forward. The default port will be filled in automatically based on your choice.

Target Server *

e.g., example.company.com or 192.168.1.10

Enter the domain name or IP address of the target server.

Port *

22 X

e.g., 443 or 8000-9000 or 80,443,8080

Supports single ports, ranges, and comma-separated lists. Press Enter to add.

☐ Enable this profile immediately after saving

Save **Cancel**

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 Port Forwarding machine is for.

Streamer Settings

- **Deployment Code**, Enter a Splashtop deployment package code to determine the Port Forwarding 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.

Port Forwarding Settings

- **Protocol**, Select the protocol you want to forward (e.g., RDP, VNC, SSH). The default port for the selected protocol is filled in automatically, but you can still edit it in the Port field below.
- **Target Server**, Enter the domain name or IP address of the target server you want to forward traffic to. This must be reachable from the machine running the Connector.
- **Port**, Add one or more ports to forward. Supports a single port, a range, or a comma-separated list. Type a value and press **Enter** to add it as a tag; click the X on a tag to remove it.

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

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