Splashtop Enterprise

Administratoren-Handbuch

3. November 2023

https://www.splashtop.com/enterprise

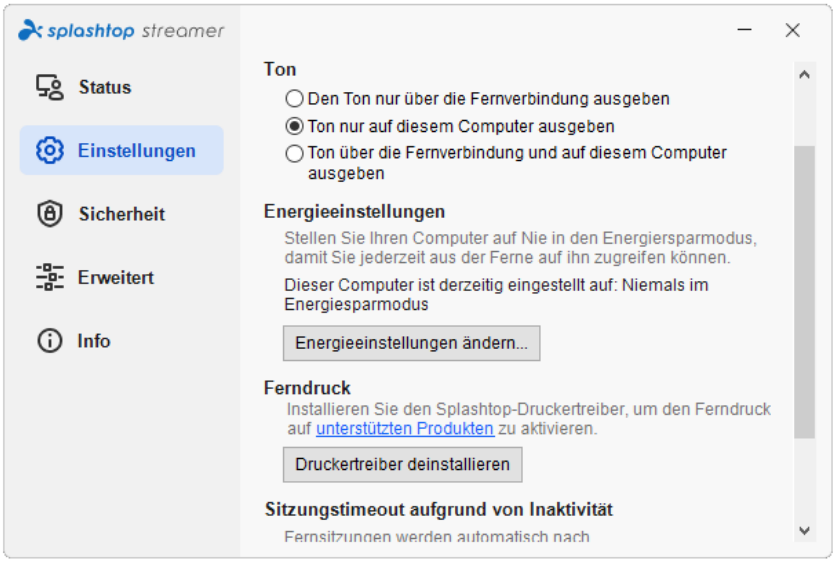
Inhaltsverzeichnis

Änderungsprotokoll – ab der letzten Version vom 03.11.2022

- Bereitstellung, Abschnitt 1
  - Leitfaden für PDQ- und Kaseya-Deployment hinzufügen
- Single Sign-On (SSO), Abschnitt 3
  - Super Admins können auch SSO verwalten
- Gruppierung, Abschnitt 5
  - Abschnitt „Verbindungspool“ hinzufügen
- Geplanter Zugriff, Abschnitt 7
  - Super Admins können geplante Zeitzonen konfigurieren
- Teameinstellungen, Abschnitt 8
  - Neue Benutzeroberfläche und Einstellungen aktualisieren
- Granulare Kontrollen, Abschnitt 9
  - Granulare Steuerungen für die Fernsteuerung und die Remote-Eingabeaufforderung hinzufügen
- Endpunktverwaltung, Abschnitt 10
  - Abschnitt von Fernverwaltung von Computern umbenennen
  - Smart Actions, Systemtools hinzufügen – Registry Editor, Service Manager, Device Manager, Task Manager
- Service Desk (Techniker), Abschnitt 13
  - SOS Call hinzufügen, Web-Support-Formulare
- Offene APIs, Abschnitt 15
  - Neuer Abschnitt für Splashtop RESTful APIs

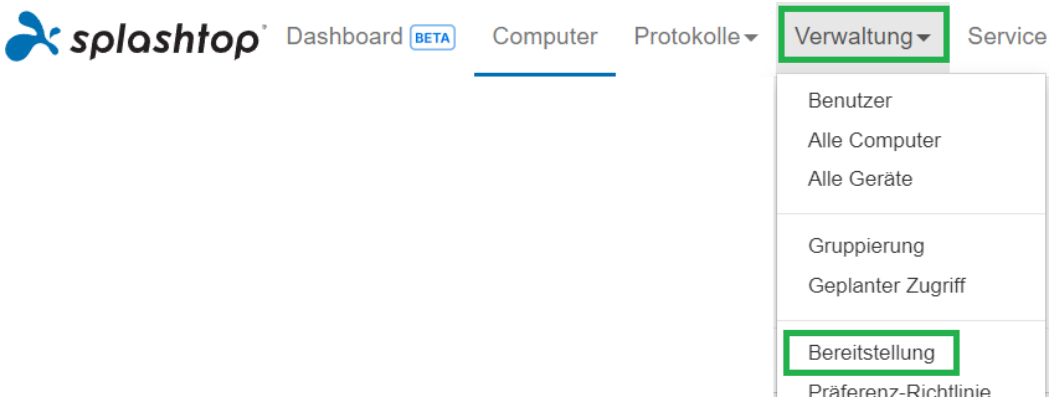
1. Bereitstellung

Installieren Sie Splashtop Streamer auf Computern, um diese aus der Ferne zugänglich zu machen. Sie können ein Bereitstellungspaket erstellen, um die Standardeinstellungen von Streamer für die Bereitstellung anzupassen . Auf diese Weise müssen Sie die Einstellungen nach der Installation nicht manuell konfigurieren.

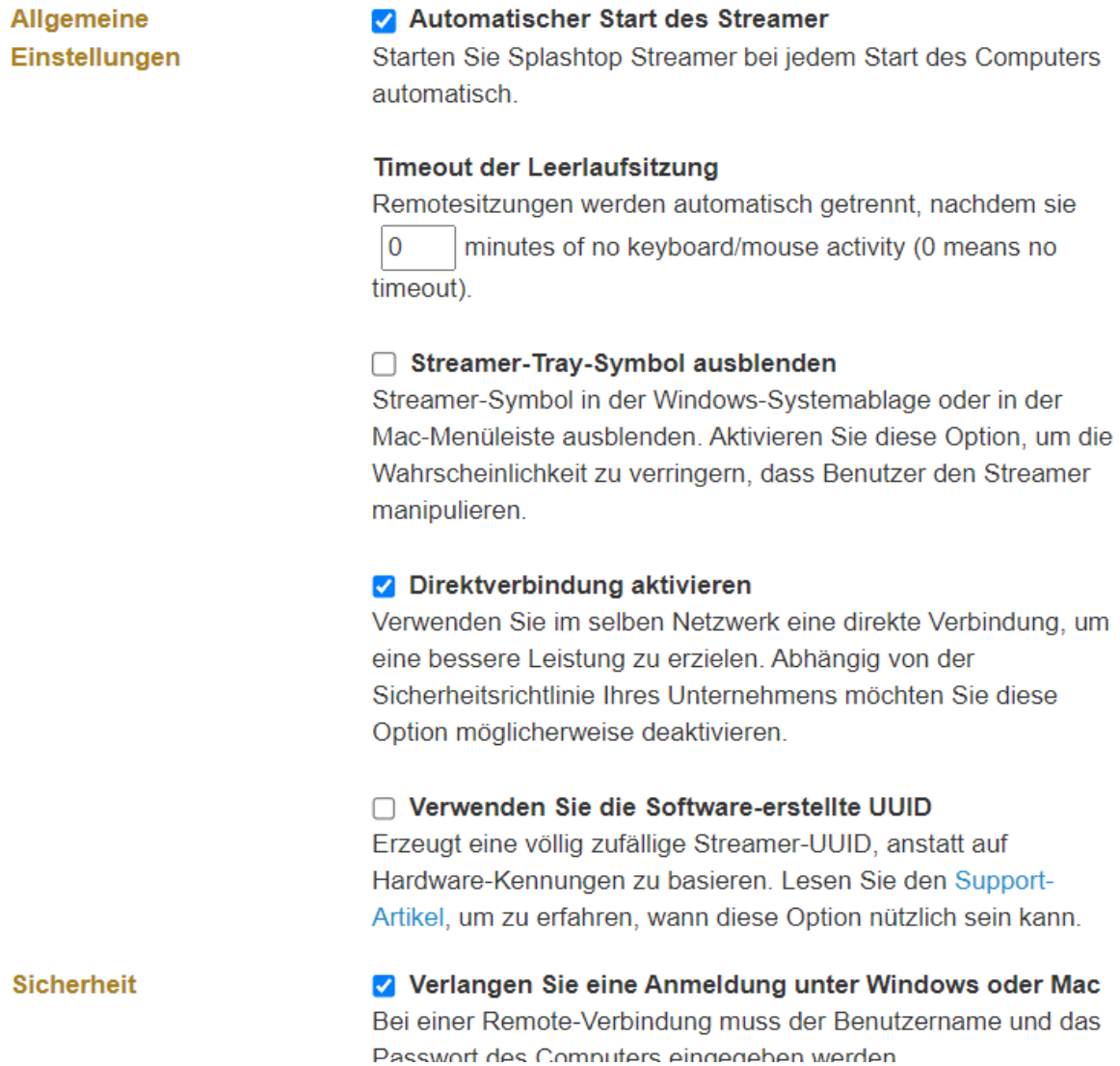


Übersicht der verschiedenen Streamer-Einstellungen

1. Loggen Sie sich auf my.splashtop.eu ein und klicken Sie auf ***Verwaltung -> Bereitstellung.***

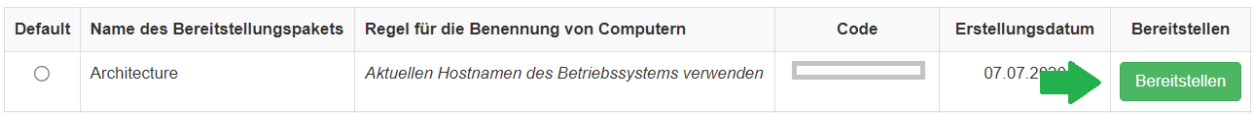


2. Klicken Sie auf ***Bereitstellungspaket erstellen*** und wählen Sie die gewünschten Streamer-Einstellungen. Beim Erstellen des Bereitstellungspakets haben Sie die Möglichkeit, die Standardeinstellungen festzulegen, einschließlich Computer-Benennungsregel, Sicherheitseinstellungen, Klangumleitung usw.



Hinweis: Wenn Sie das einmalige Anmelden/Single Sign-On (SSO) verwenden, wählenSie nicht "Streamer-Einstellungen mit Splashtop-Admin-Zugangsdaten sperren" aus - SSO-Konten können den Streamer nicht entsperren.

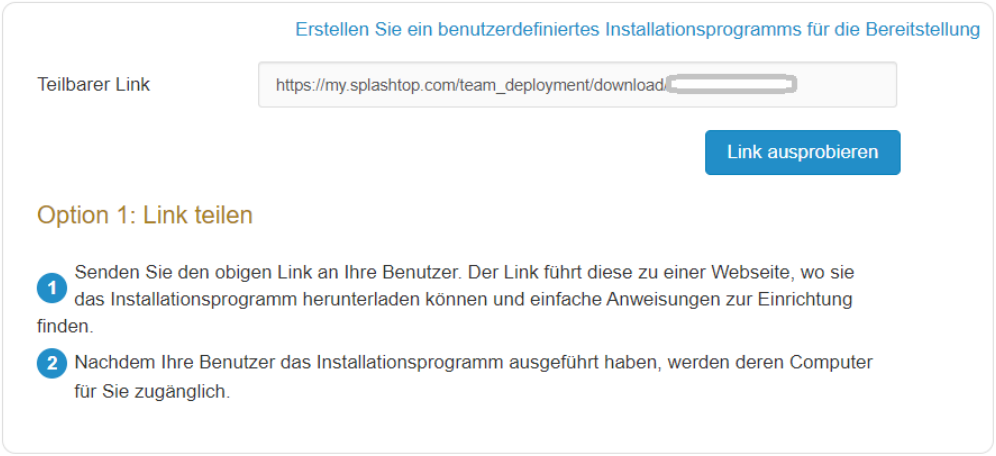
3. Wenn Sie das Paket gespeichert haben, sehen Sie das neu erstellte Paket und den eindeutigen 12-stelligen Bereitstellungscode. Klicken Sie auf **Bereitstellen** , um die Bereitstellungsoptionen anzuzeigen.



4. Hier finden zwei Möglichkeiten, das Bereitstellungspaket zu verteilen:

Option 1: Link teilen

Senden Sie diesen Link, damit ein Benutzer den Streamer für Sie herunterladen und installieren kann.



Benutzer, die auf den Link klicken, erhalten Anweisungen zum Herunterladen und Installieren des Streamers.

Willkommen bei Splashtop Remote Support

Installieren Sie Splashtop Streamer auf Ihrem Computer, damit das untenstehende Unternehmen jederzeit remote auf Ihren Computer zugreifen kann (sofern nicht anders konfiguriert).

Demo Team (owner: megan@splashtop.com)

☑ Ich vertraue der oben genannten Organisation und möchte den Remotezugriff auf meinen Computer zulassen.

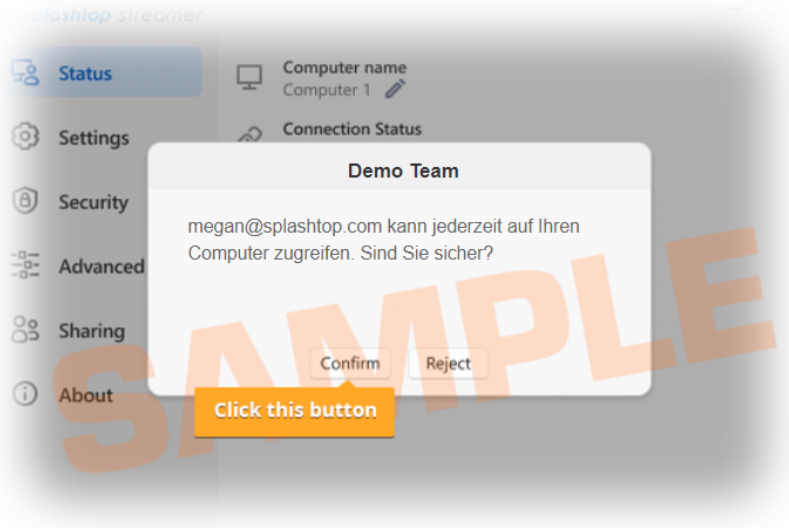
Schritt 1: Laden Sie den Streamer herunter.

Download
für Windows

Auch verfügbar für Mac, Android

Schritt 2: Starten Sie das Installationsprogramm und erlauben Sie den Zugriff.

Nachdem die Installation abgeschlossen ist, öffnen Sie die Splashtop Streamer-App und klicken Sie auf "Bestätigen", um den Zugriff zu ermöglichen.



Option 2: Installationsprogramm herunterladen

Laden Sie das Installationsprogramm herunter, um es direkt auf Ihrem Computer zu installieren, über Dropbox, E-Mail usw. freizugeben oder für die Bereitstellung mit einem Drittanbieter-Tool vorzubereiten.

Es werden mehrere Installationsoptionen für Windows, Mac, Android und Linux angeboten.

- Siehe diesen Artikel für Parameter für die stille Installation
- Es sind auch Leitfäden für den Einsatz verfügbar:
  - Gruppenrichtlinie (GPO)
  - Jamf Pro
  - Microsoft Intune
  - PDQ
  - Kaseya (für Mac)
- Die Einstellungen des Bereitstellungspakets gelten für den Streamer nur bei der Installation.Um die Einstellungen eines Streamers nach der Bereitstellung zu aktualisieren, können Sie die Bereitstellung mit einem neuen Paket erneut durchführen, die Einstellungen direkt im Streamer manuell ändern oder Präferenzrichtlinien (siehe unten) verwenden, um Einstellungen aus der Ferne zu verwalten.
- Das Löschen eines Bereitstellungspakets wirkt sich nicht auf bereits bereitgestellte Computer aus - es verhindert lediglich neue Bereitstellungen mit diesem Paketcode.

Wie aktualisiere ich Splashtop Streamer?

Es gibt mehrere Möglichkeiten, den Streamer zu aktualisieren, darunter:

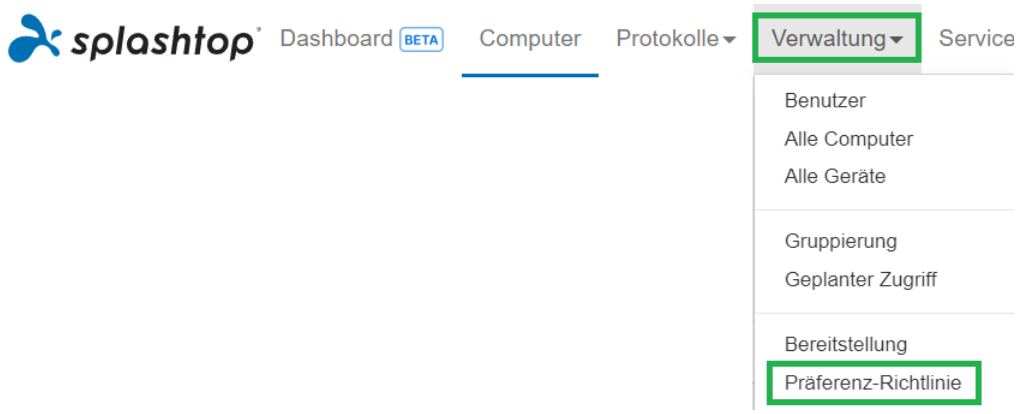
- Manuelles Update über die Webkonsole
- Manuelles Update über Registerkarte Streamer -> Info -> Nach Updates suchen
- Manuelles Update durchführen, indem Sie das neueste Streamer-Installationsprogramm ausführen
- Manuelles Update innerhalb der Business App
- Automatisches Aktualisieren mit .EXE, .MSI oder .PKG

Weitere Informationen finden Sie in diesem Artikel über Splashtop Streamer-Updates.

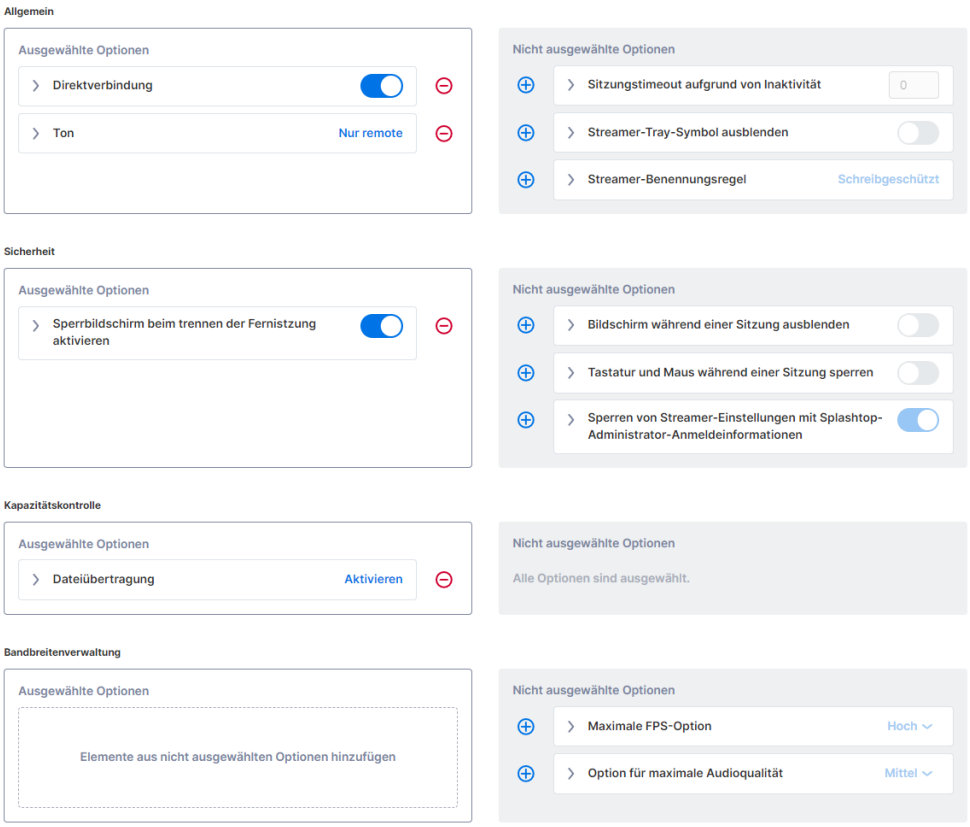
Präferenzrichtlinien

Ab Splashtop Streamer v3.5.2.2 können Sie bestimmte Streamer- und Sitzungseinstellungen über die Präferenzrichtlinien in der Webkonsole verwalten. Durch das Zuweisen von Endpunkten zu Ihrer Richtlinie können Sie vorhandene Streamer-Einstellungen konfigurieren und überschreiben, ohne den Streamer erneut bereitstellen oder die Einstellungen lokal am Endpunkt manuell ändern zu müssen.

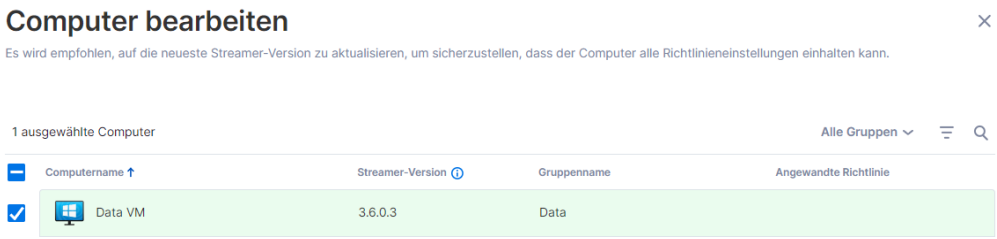
1. Um eine neue Richtlinie zu erstellen, melden Sie sich bei my.splashtop.com an und klicken Sie auf ***Verwaltung -> Präferenzrichtlinie.***



2. Fügen Sie der Richtlinie verschiedene Einstellungen hinzu oder entfernen Sie diese, einschließlich allgemeiner Sitzungseinstellungen, Sicherheits- und Bandbreitenoptionen.



3. Zuweisung von Computern zur Richtlinie.
   Hinweis: Nur Streamer v3.5.2.2+ werden im Menü angezeigt.



4. Unter Management -> Alle Computer können Sie überprüfen, welche Richtlinie jedem Computer zugewiesen ist.

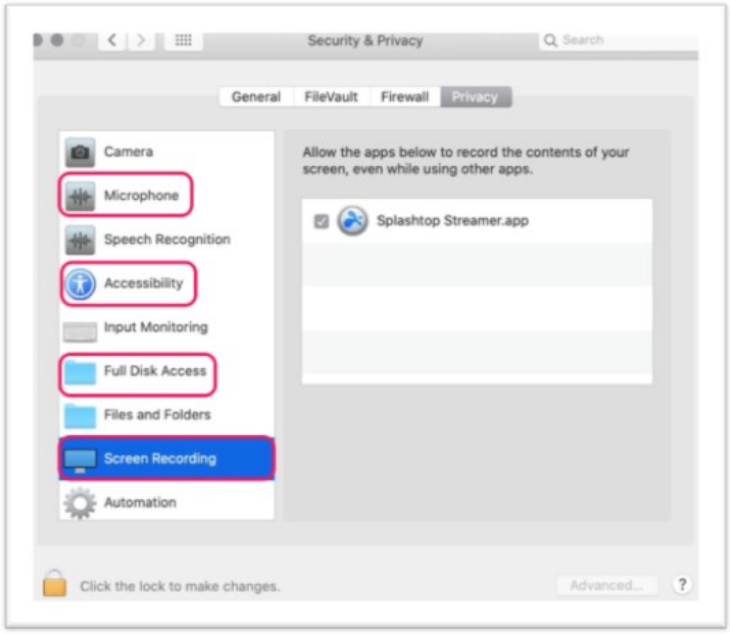
5. Wenn ein Benutzer eine Verbindung zu einem Computer herstellt, der Teil Ihrer bevorzugten Richtlinie ist, gelten die konfigurierten Einstellungen oder Einschränkungen für die Remote-Sitzung. Der Benutzer kann die Richtlinieneinstellungen nicht über die Business-App- oder Streamer-Menüs neu konfigurieren.

[In diesem Artikel finden Sie weitere Informationen zum Verhalten und Anweisungen.]

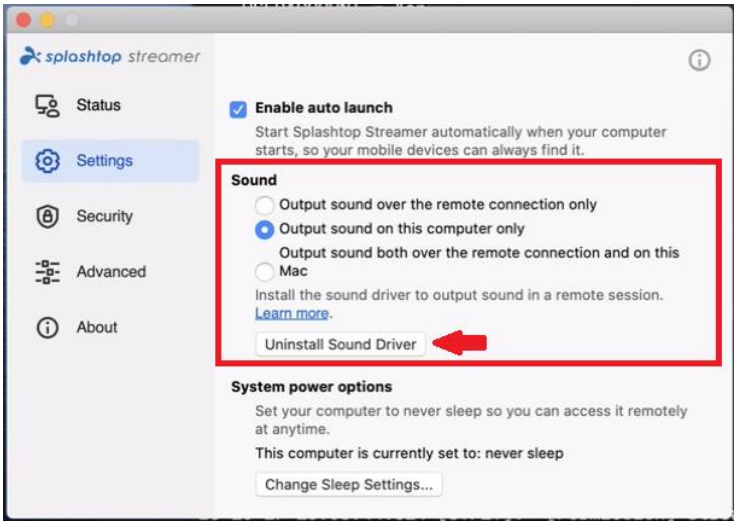
2. Zusätzliche Anforderungen für MacOS

Beachten Sie bei der Bereitstellung auf Mac-Computern diese zusätzlichen Anforderungen und Installationsanweisungen:

- **Sicherheit- und Datenschutzberechtigungen** für macOS 10.15 Catalina/11 Big Sur und neuer:



- **Audio**: Um das Audio-Streaming über die Fernverbindung zu aktivieren, installieren Sie den Splashtop Sound Driver und erlauben Sie die Mikrofonberechtigung für macOS 10.14+. Wenn irgendwelche Apps auf den Mac-Computern Soundtreiber von Drittanbietern verwenden, z. B. Avid Pro Tools oder Adobe Premiere, sind möglicherweise einige zusätzliche Konfigurationen erforderlich.



3. Einmal-Login / Single Sign-On (SSO)

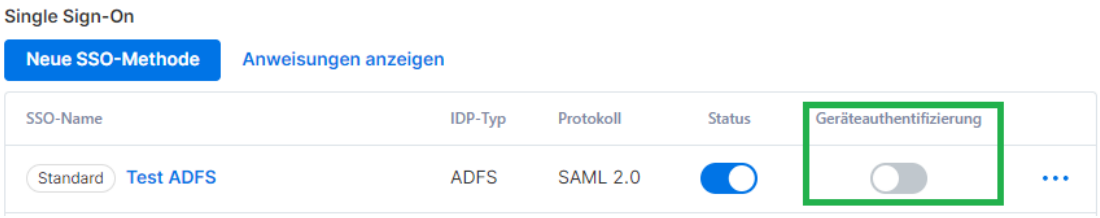
Splashtop unterstützt das Einloggen bei https://my.splashtop.com und die Splashtop Business-App unter Verwendung der von Ihren SAML 2.0-Identitätsanbietern erstellten Berechtigungsnachweisen.

Wenn Sie möchten, dass die Benutzer einmalige Anmelden/Single Sign-On (SSO) verwenden, führen Sie bitte zwei Schritte aus:

1. Erstellen Sie eine SSO-Methode für Ihren IDP-Dienst in der Splashtop-Webkonsole: Wie können Sie eine neue SSO Methode anwenden?
    a. Detaillierte Anweisungen zu bestimmten IDP-Diensten wie Azure AD, OKTA, ADFS, JumpCloud, OneLogin finden Sie hier: Single Sign-On (SSO)
2. Unser Validierungsteam wird sich mit Anweisungen zur Verifizierung Ihres Domain-Zugangs und zur Aktivierung Ihrer SSO-Methode bei Ihnen melden.
3. *(Empfohlen)* Richten Sie die **SCIM-Bereitstellung** (für AzureAD, Okta und JumpCloud) ein, um Benutzer und Gruppen automatisch bereitzustellen und zu synchronisieren. Dadurch wird der E-Mail-Einladungsprozess *(Abschnitt 4, Einladen von Benutzern)* übersprungen.
4. (*Empfohlen*) Importieren Sie SSO-Benutzer per CSV-Datei, wenn Sie die SCIM-Bereitstellung nicht verwenden können, um Benutzer automatisch in bestimmte Benutzergruppen einzufügen. Dadurch wird ebenfalls der E-Mail-Einladungsprozess übersprungen.

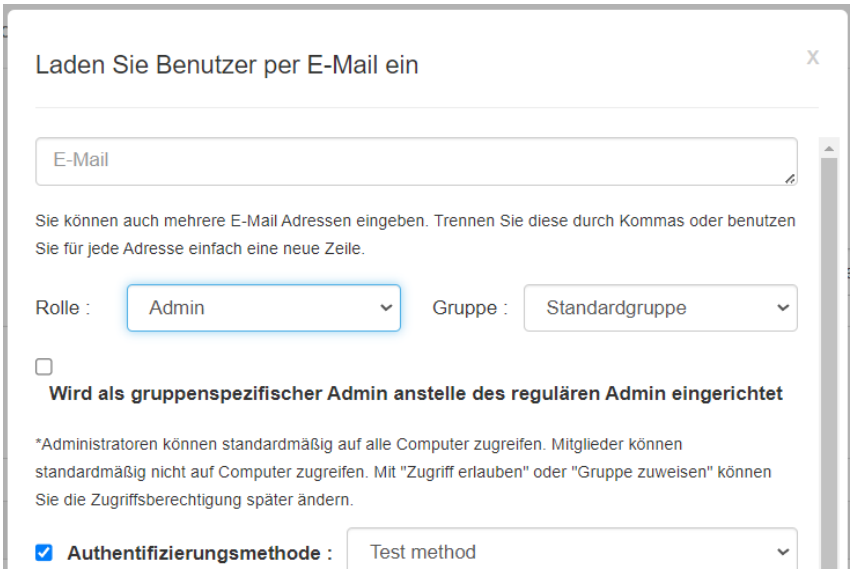
In diesem Artikel finden Sie die SSO-Einschränkungen.

Sobald Ihre SSO-Methode aktiviert ist, können Sie die Geräteauthentifizierung für Benutzer, die mit dieser Methode assoziiert sind, deaktivieren. So müssen Benutzer nicht auf zusätzliche E-Mail-Links klicken, um ihre Geräte zu authentifizieren. Deaktivieren Sie einfach das Kontrollkästchen für die Geräteauthentifizierung der SSO-Methode unter ***Verwaltung -> Einstellungen*** *(nur Team-Eigentümer und Super Admin)*.



4. Benutzer einladen

Laden Sie Benutzer ein, indem Sie auf ***Verwaltung -> Benutzer -> Mitglieder einladen*** gehen. Weisen Sie Team-Rollen, Benutzergruppen und SSO-Authentifizierungsmethoden während des Einladungsprozesses oder später zu. Sie können in jedem Einladungsfenster bis zu 500 E-Mail-Adressen einladen.



Teamrollen

- **Eigentümer**: Der Eigentümer ist die höchste Autoritätsebene und kann alle Funktionen in Splashtop ausführen, einschließlich (aber nicht beschränkt auf) das Einladen von Benutzern, das Ändern von Rollen, das Einsehen der Verbindungshistorie von Benutzern, das Verwalten von Computern, das Ändern von Zugriffsberechtigungen und das Ändern von Teameinstellungen. Der Teambesitzer ist der einzige Benutzer, der Zugriff auf die Abonnement-/Zahlungsinformationen des Teams hat.
    - Es gibt nur einen Eigentümer, und der Status kann nicht zwischen Benutzerkonten übertragen werden.

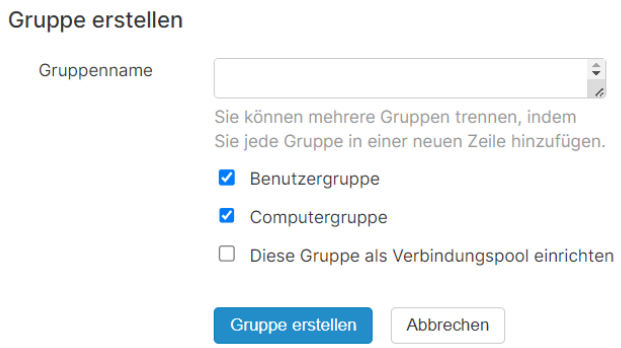
- **Admin**: Die Administrator-Rolle hat die gleichen Berechtigungen wie der obige Eigentümer, außer dass sie keinen Zugriff auf Abonnement-/Zahlungsinformationen und die Registerkarte "Team-Einstellungen" hat und die Rollen der Benutzer nicht ändern kann.
    - Super Admin: Der Super Admin liegt über dem Admin und hat die gleichen Rechte wie der Besitzer, einschließlich des Zugriffs auf die Registerkarte Teameinstellungen und der Änderung der Benutzerrollen. Er kann jedoch nicht auf Abonnement-/Zahlungsinformationen zugreifen.
    - gruppenspezifischer Admin : gruppenspezifischer Admin ist eine eingeschränkte Administrator-Rolle, die einem Benutzer Administrator-Rechte für bestimmte Benutzer-

und/oder Computergruppen verleiht. Dies ermöglicht ihm das Hinzufügen/Entfernen von Benutzern & Computern nur für die Gruppen, die berechtigt sind.
    - Admins und Group Admins haben Zugriff auf die Remote-Management-Funktionen (Remote Command, System Inventory usw.), wenn Sie ***Technikerlizenzen*** von Splashtop Enterprise erworben haben. Die Möglichkeit, bestimmten Benutzern Zugriff auf diese Funktionen zu gewähren (unabhängig von der Teamrolle), ist in Kürze verfügbar.

- **Mitglied**: Mitglieder sind allgemeine Benutzer, die dem Team hinzugefügt wurden, um ihnen den Fernzugriff zu ermöglichen. Sie haben nur Zugriff auf Computer, für die sie eine Berechtigung haben, und können ihren eigenen Status, Kontoinformationen, Team-Informationen und Protokolle überprüfen. Sie können sich auf der Registerkarte "Kontoübersicht" selbst aus einem Team entfernen ("verlassen").

5. Gruppierung

Mit Splashtop können Sie Ihre Benutzer und Computer gruppieren, um die Verwaltung und die Kontrolle der Zugriffsrechte zu vereinfachen. Jeder Benutzer oder Computer kann nur zu einer Gruppe gehören. Benutzer können jedoch Zugriff auf mehrere Computergruppen haben. Gehen Sie dazu auf ***Verwaltung -> Gruppierung*** .



Sie können 3 Arten von Gruppen erstellen:

1. Nur-Benutzer-Gruppe
2. Nur-Computer-Gruppe
3. Benutzer- und Computergruppe

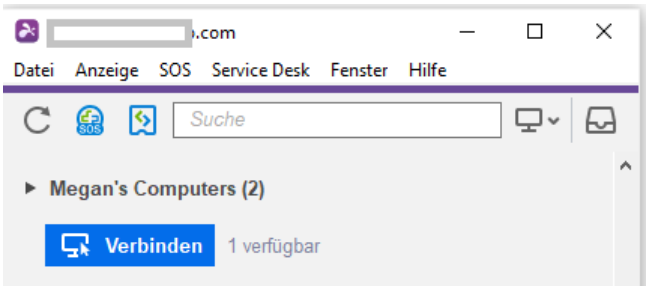
Eine **Nur-Benutzer-Gruppe** darf nur aus Benutzern bestehen. Die Gruppierung von Benutzern ermöglicht, Zugriffsberechtigungen für mehrere Benutzer gleichzeitig festzulegen. Sie ermöglicht außerdem, Zugriffsberechtigungen automatisch auf einen neuen Benutzer anzuwenden.

Eine **Nur-Computer-Gruppe** darf nur aus Computern bestehen. Die Gruppierung von Computern hilft, eine große Computerliste zu organisieren, um die Navigation zu erleichtern. Sie kann auch die Zuweisung von Zugriffsberechtigungen erleichtern. Sie können Benutzern den Zugriff auf eine ganze Gruppe von Computern gewähren.

Ein **Benutzer & Computergruppe** ist eine Abkürzung für eine gruppenbasierte Zugriffssteuerung. Sie kann sowohl aus Benutzern als auch aus Computern bestehen. Standardmäßig können alle Benutzer in dieser Gruppe auf alle Computer in dieser Gruppe zugreifen.

Verbindungspool

Diese Gruppe als Verbindungspool einrichten, um die Verbindungspool-Funktion für die Computergruppe zu aktivieren. Benutzer können auf die Schaltfläche „Verbinden“ klicken, um eine Verbindung mit einem beliebigen verfügbaren Computer in der Gruppe herzustellen. Dies ist nützlich für Szenarien wie RDP-Pools, Computerlabore und mehr, wo es keine Rolle spielt, mit welchem Computer der Benutzer eine Verbindung herstellt.



Verbindungspools können auch für bestimmte Computer außerhalb der Computer-Gruppenzuweisungen aktiviert werden. Siehe Abschnitt 7, Geplanter Zugriff.

Hinzufügen von Benutzern oder Computern zu einer Gruppe

Klicken Sie in ***Verwaltung -> Gruppierung*** auf das Zahnradsymbol rechts neben der Gruppe, um Benutzer oder Computer zuzuweisen. Es können mehrere Benutzer oder Computer auf einmal hinzugefügt werden. Sie können auch einen Gruppenadministrator zuweisen.

Klicken Sie in ***Verwaltung -> Alle Computer*** auf das Zahnradsymbol rechts neben jedem Computer, um diesen Computer einer Gruppe zuzuordnen.

Klicken Sie in ***Verwaltung -> Benutzer*** auf das Zahnradsymbol rechts neben jedem Benutzer, um den Benutzer einer Gruppe zuzuordnen. Sie können auch die Gruppe eines Benutzers auswählen, wenn Sie eine Einladung senden.

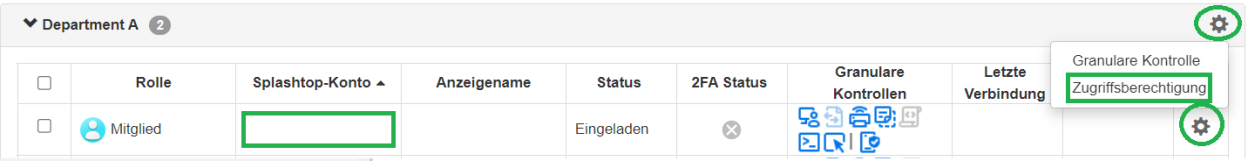
6. Zugriffsberechtigungen

Mit den Zugriffsberechtigungen werden bestimmt, auf welche Computer ein Benutzer Zugriff hat. Diese können vom Team-Eigentümer oder den Administratoren in ***Verwaltung -> Benutzer*** konfiguriert werden.

Anmerkung:

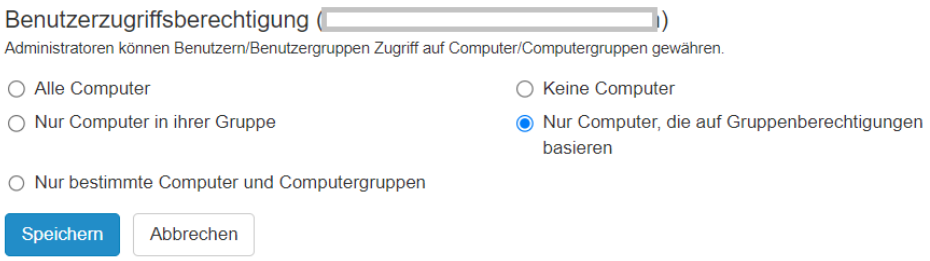
- Zugriffsberechtigungen gewähren einem Benutzer dauerhaften Zugriff auf Computer, unabhängig von der Tageszeit. Um den Zugriff nur für ein bestimmtes Zeitfenster zu gewähren, siehe *Abschnitt 7, Geplanter Zugriff*.

Sie können Zugriffsberechtigungen für einen einzelnen Benutzer oder eine Gruppe von Benutzern festlegen. Klicken Sie auf das Zahnradsymbol rechts neben einem Benutzer oder einer Benutzergruppe und wählen Sie „**Zugriffsberechtigung**“ aus.



Standardmäßig, wenn ein Benutzer eingeladen wird:

- Administratoren haben Zugriff auf alle Computer
- Mitglieder haben keinen Zugriff auf Computer, wenn sie nicht in eine Gruppe eingeladen sind
- Mitglieder haben Zugriff basierend auf der Berechtigung der Gruppe, der sie zugewiesen oder zu der sie eingeladen werden



Um einem Benutzer oder einer Benutzergruppe Zugriff auf mehrere Computer oder Computergruppen zu gewähren, wählen Sie „Nur bestimmte Computer und Computergruppen“ aus.


Nur bestimmte Computer und Computergruppen
Speichern
Abbrechen
Ausgewählte Computer
1 ausgewählt
Alle Gruppen
Name
Data 2
Computer A
Data VM

7. Geplanter Zugriff

Mit dem Modul "Geplanter Zugriff" können Administratoren für Benutzer, Gruppen und Computer den Fernzugriff basierend auf Zeitfenster planen. Der Team-**Eigentümer, Administratoren und Gruppenadministratoren**haben Zugriff auf das Planungsmodul.

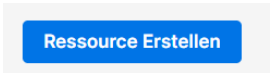
Anmerkungen:

- "Geplanter Zugriff" wird zusätzlich zu bestehenden Benutzer-/Gruppen-Zugriffsberechtigungen gewährt, die unter *Verwaltung -> Benutzer* festgelegt sind - sie setzen bestehende Benutzer-/Gruppen-Zugriffsberechtigungen NICHT außer Kraft.
- Für Benutzer, die nur einen geplanten Fernzugriff benötigen, können Sie deren Zugriffsberechtigung unter *Verwaltung -> Benutzer* auf "Keine Computer" setzen.

Konfiguration des geplanten Zugriffs

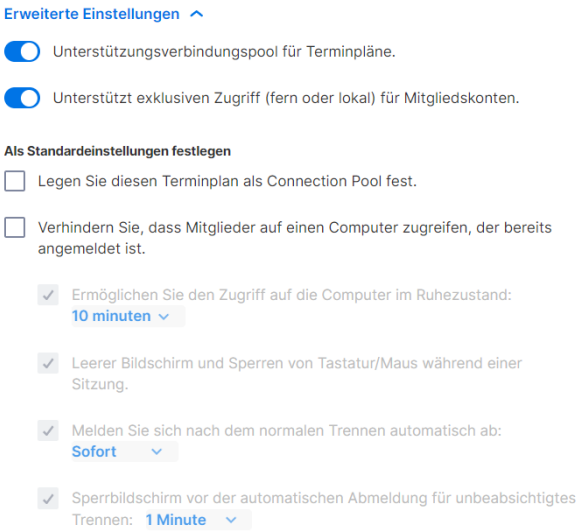
1. Bevor Sie neue Zeitpläne erstellen, gehen Sie zu ***Verwaltung -> Einstellungen***, um die Zeitzone für den geplanten Zugriff zu konfigurieren. Die Zeitzone kann nicht geändert werden, wenn ein Zeitplan eingerichtet ist. Nur der Team-Eigentümer hat Zugriff auf diese Einstellung.

2. Gehen Sie auf ***Verwaltung -> Geplanter Zugriff*** und klicken Sie auf **Ressource erstellen**.

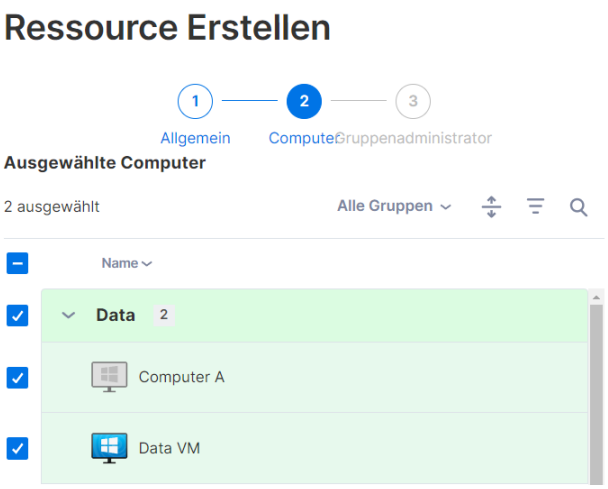


3. Eingabe der Ressource **Name** und **Beschreibung** *(optional)*. Die Ressource enthält die Menge der Computer, für die der Zugriff geplant wird.

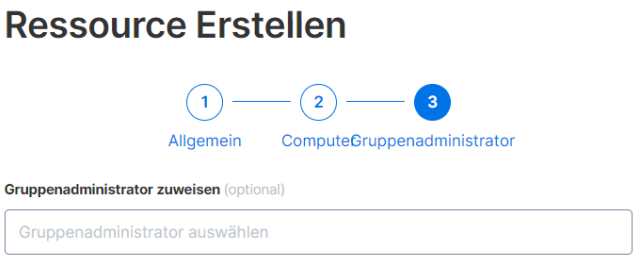
4. Klicken Sie auf **Erweiterte Einstellungen**, wenn Sie **Verbindungspool** oder **Exklusiver Zugriff** in dieser Ressource aktivieren möchten. Dies ist die Standardvorlage für die Einstellungen jedes von Ihnen erstellten Zeitplans.
    - Der Verbindungspool ermöglicht Ihren Benutzern, eine Verbindung zu jedem verfügbaren Computer in der Ressource herzustellen. Dies ist nützlich in Fällen, in denen es keine Rolle spielt, mit welchem Computer der Benutzer eine Verbindung herstellt.
    - Exklusiver Zugriff verhindert, dass ein Remote-Benutzer auf einen Computer zugreift, wenn in diesem Computer bereits ein Betriebssystembenutzer angemeldet ist. Dies ist nützlich für Szenarien, in denen Benutzer lokal am Computer arbeiten. Sie können auch zusätzliche Funktionen erzwingen, wie z. B. einen leeren Bildschirm, die Sperrung der Tastatur und Maus und die Abmeldung nach dem Trennen der Verbindung bei Remote-Sitzungen, die einem bestimmten Zeitplan folgen.



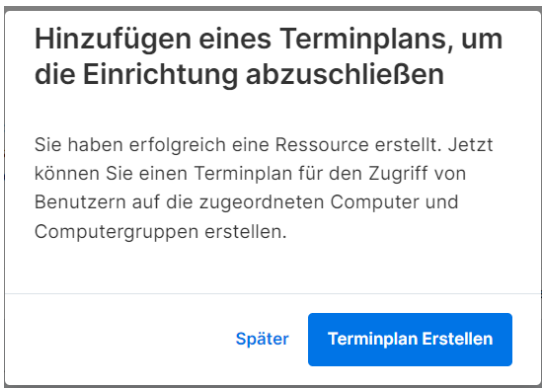
5. Wählen Sie die Computer und/oder Gruppen aus, die Sie in der Ressource verfügbar machen möchten.



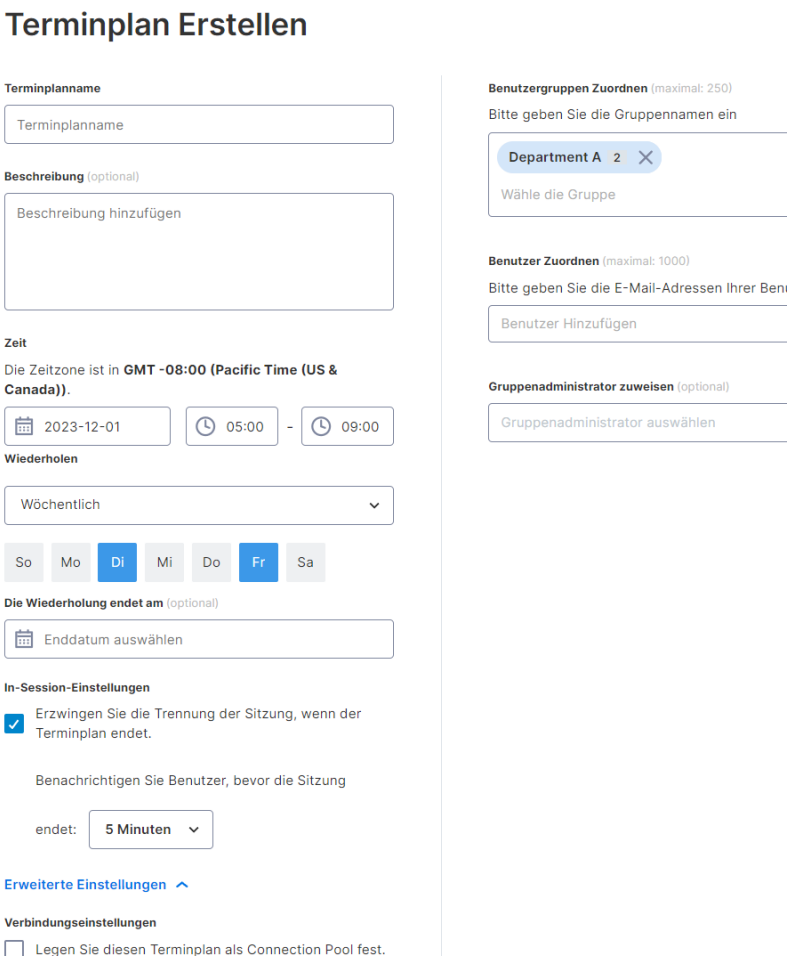
6. *(Optional)* Weisen Sie Gruppenadministratoren zu, um bei der Verwaltung von Zeitplänen für diese Ressource zu helfen. Gruppenadministratoren können jede Ressource einsehen, der sie zugewiesen sind, und können auch neue Ressourcen und Zeitpläne erstellen.



7. Fahren Sie mit **Terminplan Erstellen** fort, oder klicken Sie später auf den Ressourcennamen, um Zeitpläne zuzuweisen.



8. Erstellen Sie einen Zeitplan für die Ressource, indem Sie die Felder **Name**, **Startdatum** und **Wiederholung** ausfüllen.



- Wählen Sie Benutzergruppen und/oder bestimmte Benutzer für den Zugriff auf den Zeitplan aus.
  Sie können auch eine Liste von Benutzer-E-Mails in das Feld "Benutzer" kopieren/einfügen.

- Die Zeit-Dropdown-Auswahl zeigt 30-Minuten-Intervalle an, aber Sie können jeden Wert minutengenau eintippen.

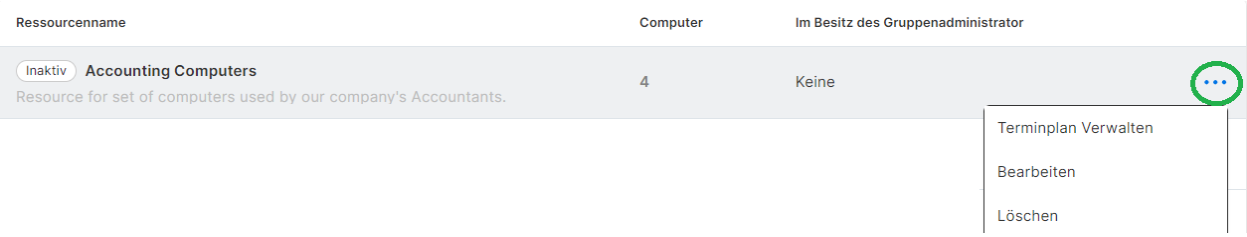
- Sie können mehrere Tage in einer wöchentlichen Wiederholung auswählen.

- Markieren Sie **Sitzungsunterbrechung am Ende jedes Zeitplans erzwingen**, wenn Sie möchten, dass die Sitzungen am Ende des Zeitfensters zwangsweise unterbrochen werden.
  Hinweis: Dadurch wird das Benutzerkonto nicht vom Betriebssystem des Computers abgemeldet.

- Klicken Sie auf **Erweiterte Einstellungen**, um den Verbindungspool und die exklusiven Zugriffseinstellungen zu verwalten, wenn sie in der Ressource aktiviert sind. Diese Optionen sind nur verfügbar, wenn sie innerhalb der Ressource aktiviert sind.

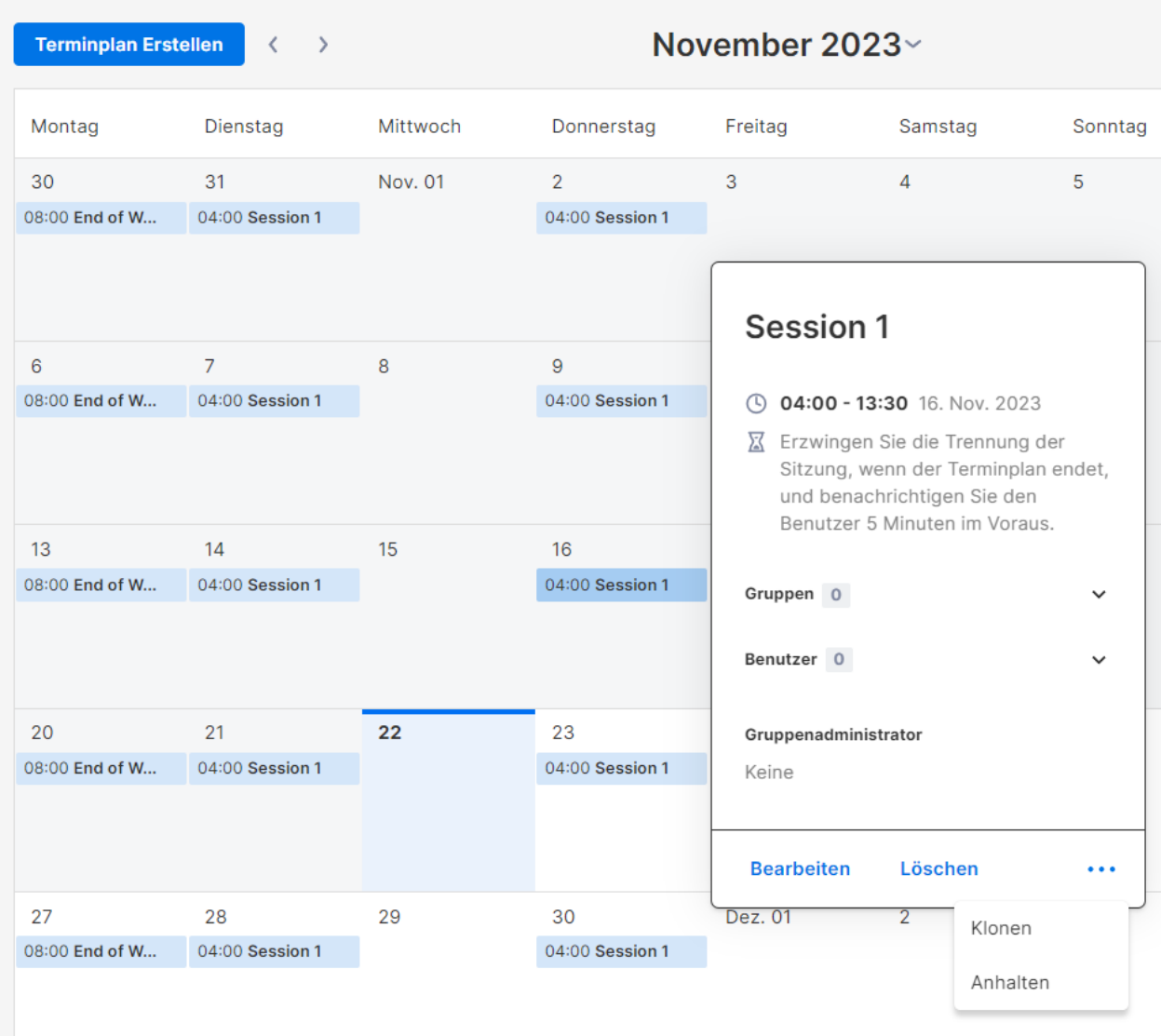
Ressourcen & Zeitpläne verwalten

Klicken Sie auf das Menü rechts neben jeder Ressource, um die Verwaltungsoptionen anzuzeigen.



- **Zeitplan verwalten**, um zur Kalenderansicht der Ressource zu gelangen.
- **Bearbeiten**, um die Konfigurationen der Ressource zu ändern.
- **Löschen** , um die Ressource zu entfernen.

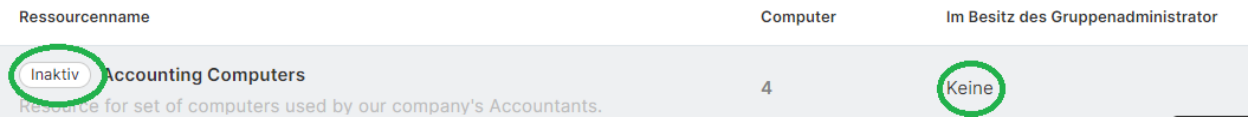
Klicken Sie auf einen Zeitplan in der Kalenderansicht, um die Zeitplanfunktionen zu verwalten.



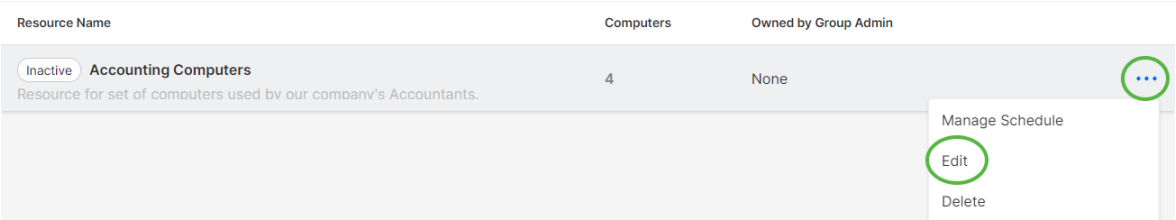
- **Bearbeiten** , um die Konfigurationen des Zeitplans zu ändern.
- **Löschen** , um alle Wiederholungen eines Zeitplans zu entfernen.
- **Klonen**, um ganz einfach einen neuen Zeitplan mit ähnlichen Konfigurationen zu erstellen.
- Die Wiederholung eines Zeitplans (Bsp.: Feiertage, Wartung) **pausieren/wiederaufnehmen**

Wenn ein Gruppenadministrator entfernt wird, was passiert mit den Ressourcen/Zeitplänen, die ihm gehören?

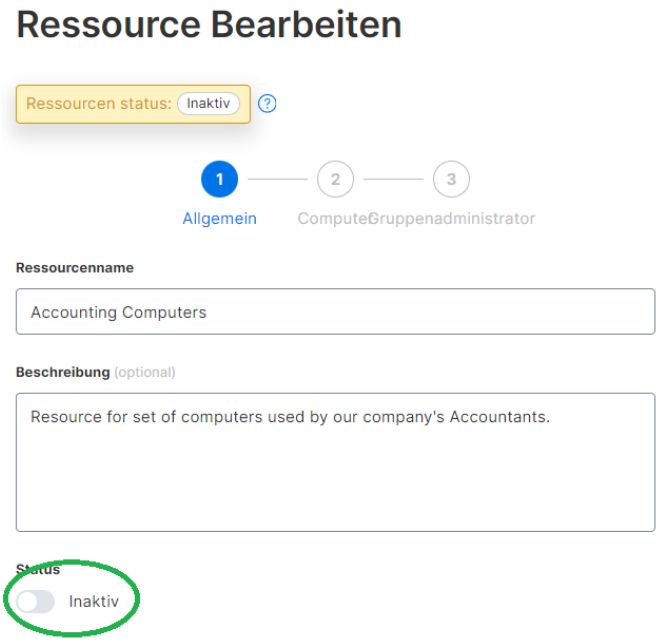
Wenn ein Gruppenadministrator aus dem Team entfernt wird oder ihm seine Administratorrechte entzogen werden, werden seine eigenen Ressourcen „inaktiv“.



1. Um eine Ressource wieder zu aktivieren, klicken Sie auf das Menü rechts neben der ***Ressource -> Bearbeiten***.



2. Umschalten des **Status** der Ressource von **Inaktiv -> Aktiv**.



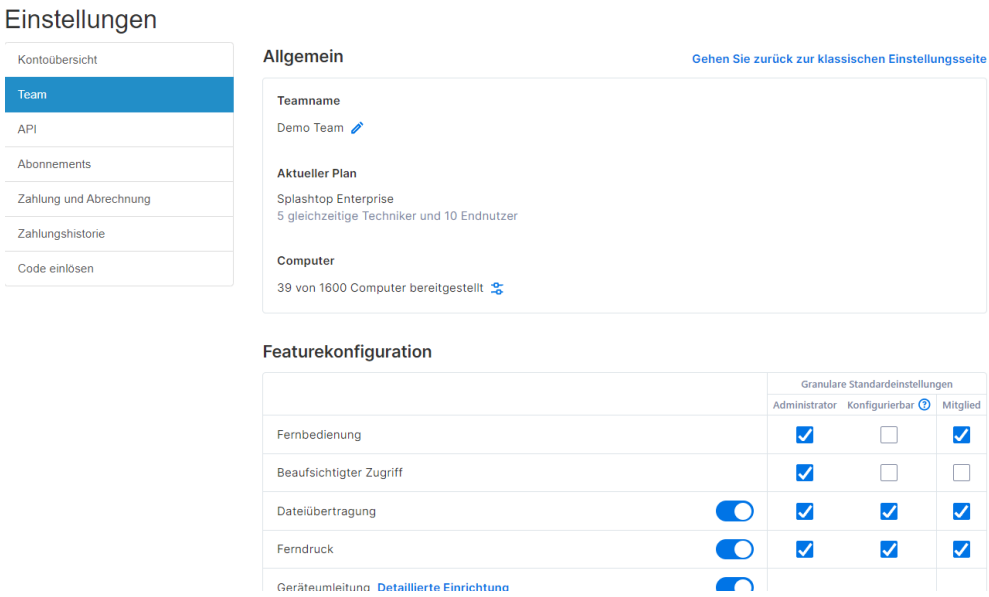
Wenn eine Ressource im Besitz mehrerer Gruppenadministratoren ist, wird die Ressource nur dann inaktiv, wenn alle Gruppenadministratoren entfernt werden.

8. Team-Einstellungen

Gehen Sie zu ***Verwaltung -> Einstellungen***, um die Team-Einstellungen zu überprüfen und zu konfigurieren. Die Team-Einstellungen steuern wichtige Richtlinien für Ihr Team, z. B. Funktionsfähigkeiten und Authentifizierung. Auf diese Seite kann nur der **Team-Eigentümer und Super Admin** zugreifen.

Übersicht der Team-Einstellungen

Ausführliche Informationen finden Sie in diesem Artikel.

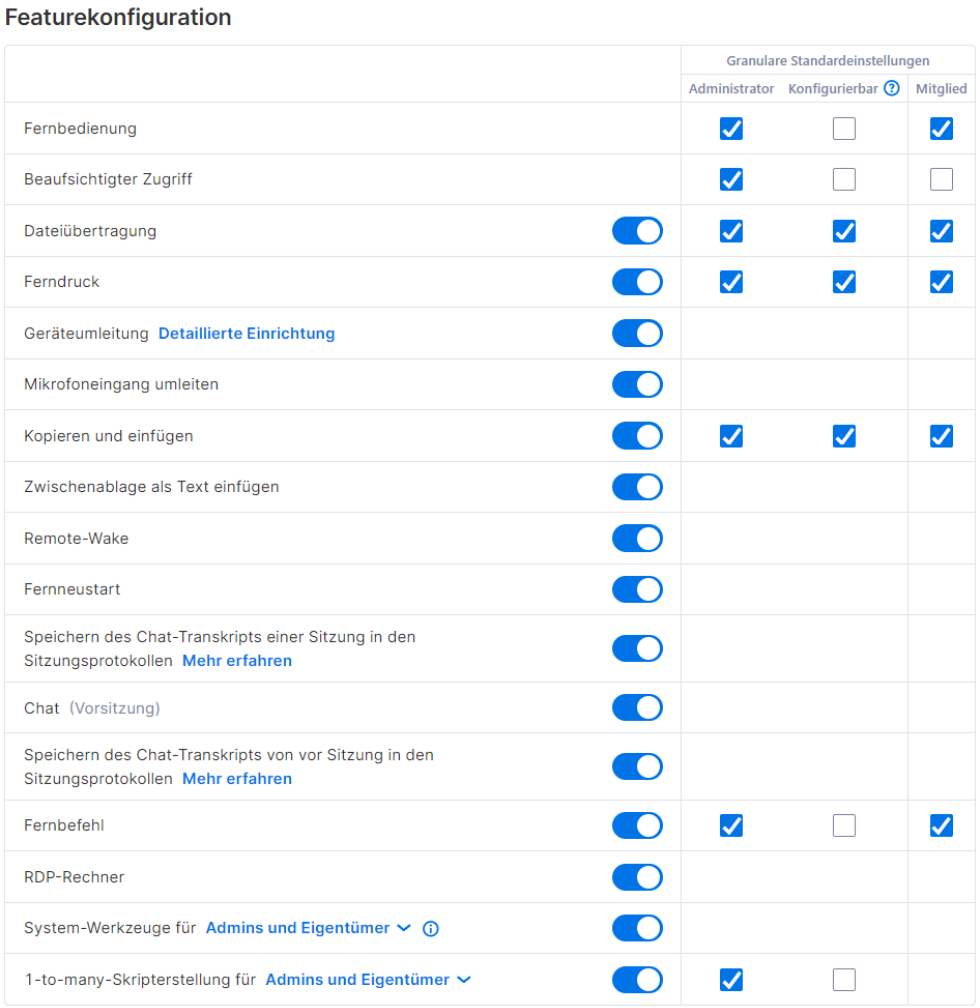


Team-Name: Dies ist der Name, den die Benutzer in ihrer Team-Einladung und ihren Kontoinformationen sehen. Der Team-Name wird auch auf der Registerkarte "Status" des eingesetzten Splashtop Streamers angezeigt.

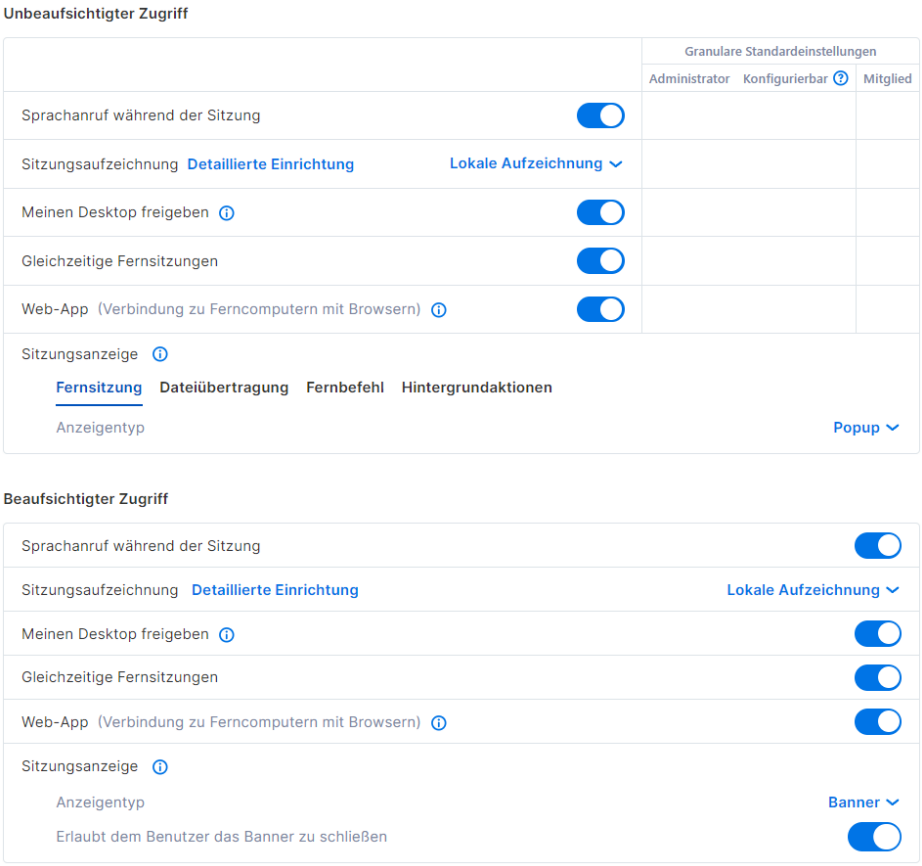
Computer: Die Anzahl der Streamer, die von der maximalen Gesamtzahl eingesetzt werden.

Feature-Konfiguration

Diese Kontrollkästchen steuern die Feature-Funktionen des Teams. Die meisten lassen sich global ein- und ausschalten, einige können nach Benutzer oder Benutzergruppe granular aktiviert werden (siehe Abschnitt 9, Granulare Steuerungen).

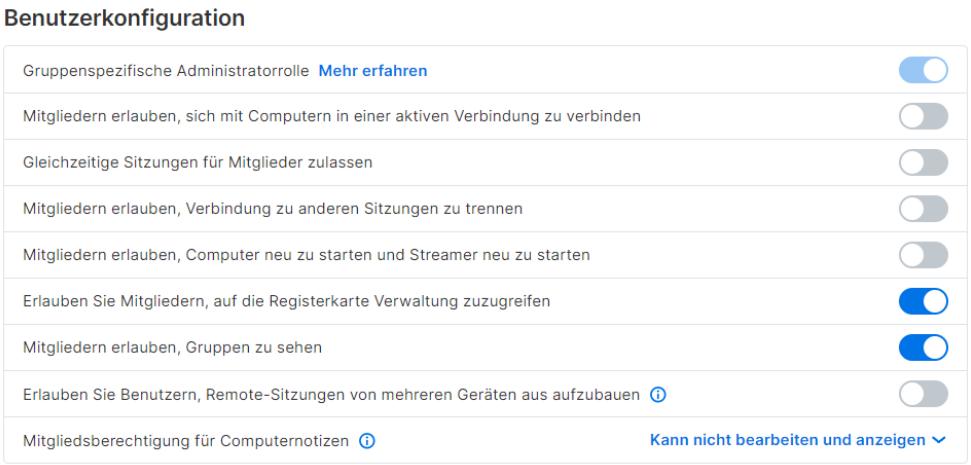


Darüber hinaus können einige Funktionen auch für unbeaufsichtigten und beaufsichtigten Zugriff (Technikerlizenz) eingestellt werden.



Benutzer-Konfiguration

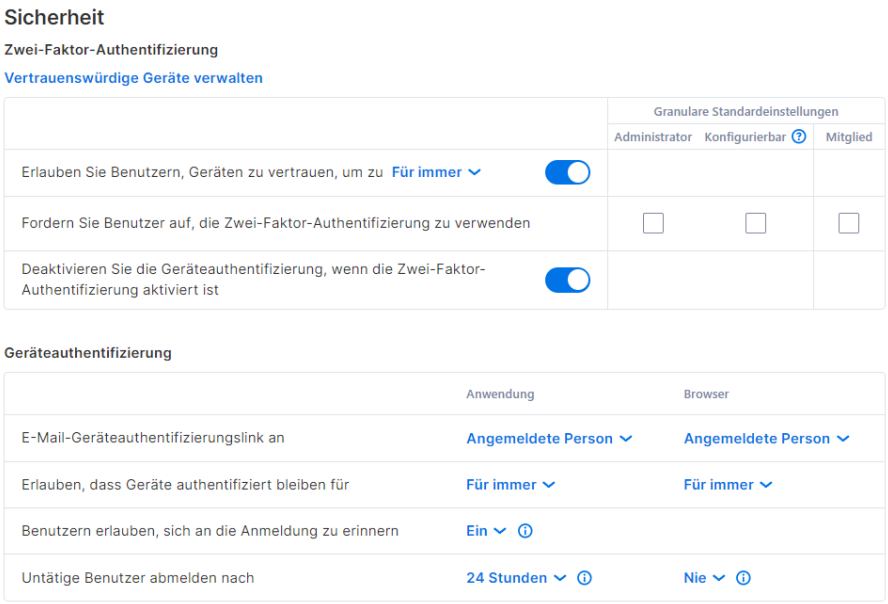
Diese Funktionen können hilfreich sein, um bestimmte Funktionen je nach Benutzerrolle einzuschränken.



- Mitgliedern erlauben, sich mit Computern in einer aktiven Verbindung zu verbinden (2 Benutzer auf 1 Computer)
- Mitgliedern den Aufbau gleichzeitiger Sitzungen erlauben (Verbindung zu mehr als einem Computer herstellen).
- Erlauben Sie Mitgliedern, die Verbindung zu anderen Sitzungen zu trennen
- Erlauben Sie Mitgliedern, Computer neu zu starten und Streamer neu zu starten
- Mitgliedern den Zugriff auf die Registerkarte „Verwaltung“ (schreibgeschützt) erlauben.
- Erlauben Sie Mitgliedern, Gruppen zu sehen (nur Gruppennamen von Computern, auf die sie Zugriff haben)
- Benutzern erlauben, von mehreren Geräten aus Fernsitzungen aufzubauen
- Mitgliedern erlauben, Computernotizen zu lesen/schreiben

Sicherheit

Verwalten Sie sicherheitsbezogene Einstellungen wie die zweistufige Überprüfung, Geräteauthentifizierung, SSO und vieles mehr.



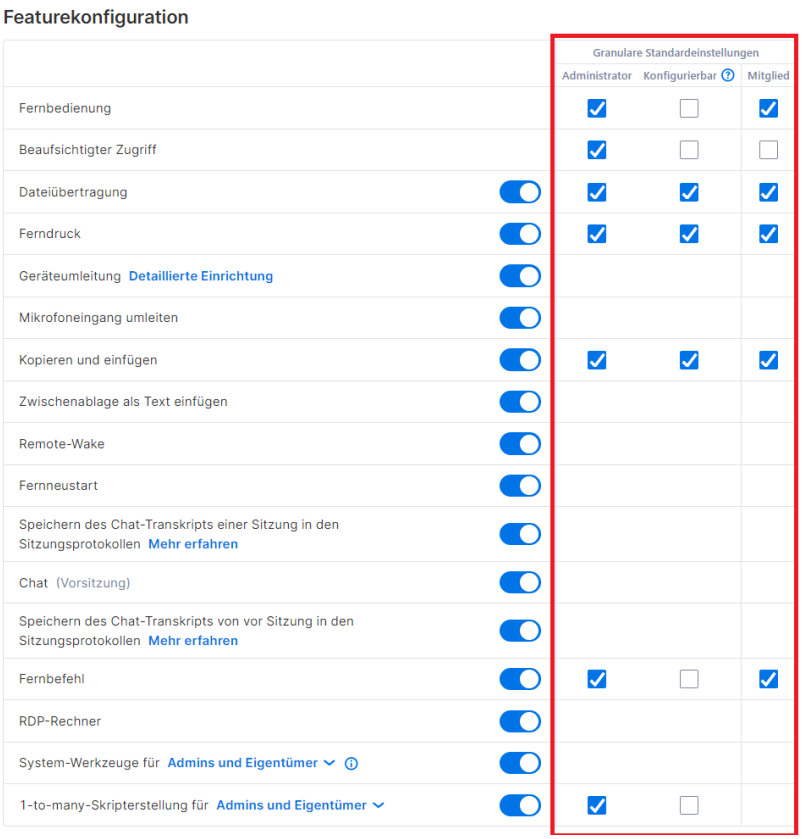
9. Granulare Steuerung

Mit granularen Steuerelementen können Sie bestimmte Funktionen für bestimmte Benutzer oder Gruppen aktivieren oder deaktivieren.

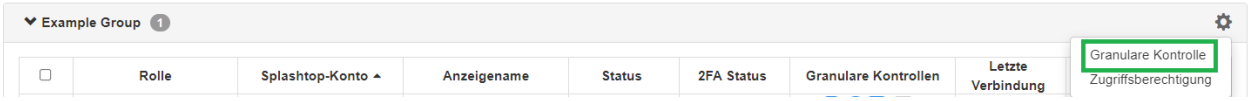
Granulare Steuerelemente sind derzeit verfügbar für:

- Dateiübertragung
- Copy-and-paste
- Zwei-Faktor-Authentifizierung
- Remote Control
- Ferndruck
- Beaufsichtigter Zugang (Technikerlizenz)
- 1-to-Many Scripting (Technikerlizenz)
- Ferngesteuerte Eingabeaufforderung

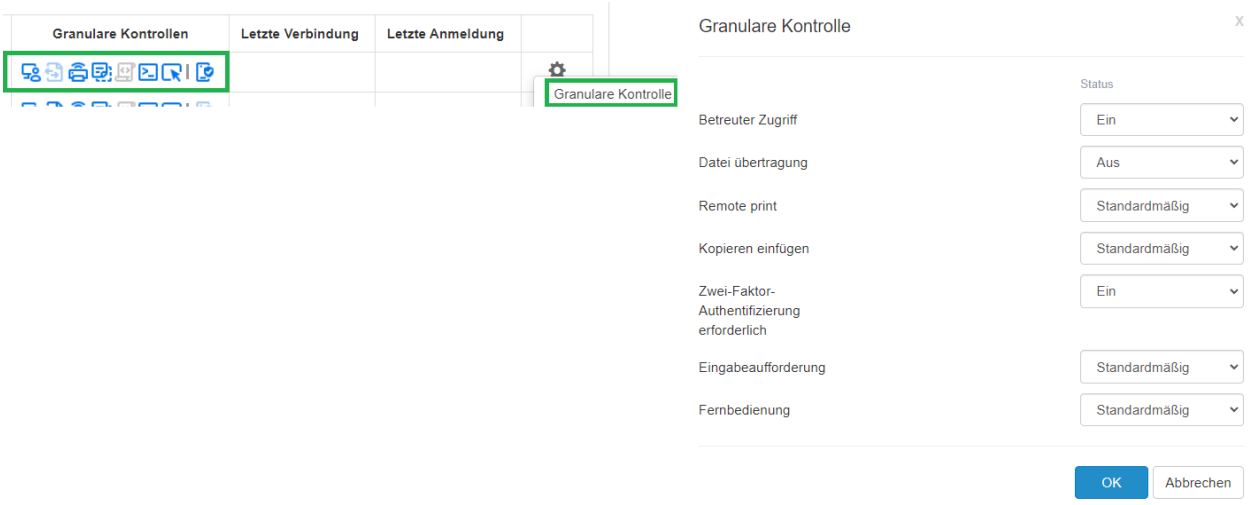
Unter ***Verwaltung -> Einstellungen*** können Sie die **granularen Standardeinstellungen** für diese Funktionen pro Benutzerrolle festlegen. Diese Standardeinstellungen werden angewendet, wenn ein neuer Benutzer in die Standardgruppe des Teams eingeladen wird oder wenn die granulare Steuerungseinstellung eines Benutzers/einer Gruppe so eingestellt ist, dass sie der Standardeinstellung folgt. Die Einstellung **Admin Configurable** kann geprüft werden, wenn Sie auch Admins die Verwaltung der granularen Steuerungen erlauben möchten.



Unter ***Verwaltung -> Benutzer*** können Sie die granulare Steuerung pro Benutzer oder Benutzergruppe konfigurieren. Um die granularen Steuerungseinstellungen für eine Benutzergruppe zu konfigurieren, klicken Sie auf das Zahnradsymbol der Gruppe -> Granulare Steuerung.



Um die Konfiguration für jeden einzelnen Benutzer vorzunehmen, klicken Sie auf jedes Funktionssymbol, um es zu aktivieren/zu deaktivieren, oder klicken Sie auf das Zahnradsymbol des Benutzers -> Granulare Steuerung.



- Ein: Aktivieren Sie diese Funktion für den Benutzer.
- Aus: Deaktivieren Sie diese Funktion für den Benutzer.
- Gruppe folgen: Wenden Sie die Benutzergruppeneinstellung für den Benutzer an.
- Standard: Wenden Sie aus den granularen Standardeinstellungen des Teams die Team-Standardeinstellung gemäß der Benutzerrolle an.

10. Endpunktverwaltung (Techniker)

Technikerlizenzen umfassen Funktionen zur Remote-Verwaltung von Computern mit der Möglichkeit, Windows-Ereignisprotokolle, System-/Hardware-/Softwareinventar oder die Endgerätesicherheit anzuzeigen und Windows-Updates und konfigurierbare Warnungen zu verwalten. Sie können Befehle auch an die Eingabeaufforderung eines unbeaufsichtigten Remote-Computers im Hintergrund senden. Alle beschriebenen Funktionen sind für den **Team-Verantwortlichen und die Team-Admins** verfügbar, sofern nichts anders angegeben wurde.

Windows-Ereignisprotokolle

Betrachten Sie die Windows-Ereignisprotokolle eines Online-Computers von der Splashtop-Webkonsole aus. Sie können nach Ereignisebene, Typ, Datumsbereich und ID filtern.

[In diesem Artikel finden Sie weitere Details und Anweisungen.]

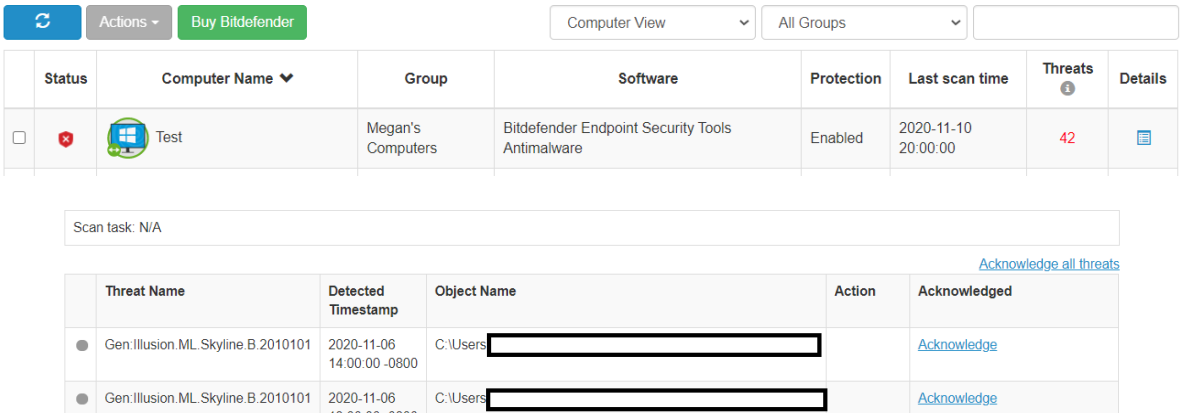
Computerinventar - System, Hardware, Software

Sehen Sie Schnappschüsse des System-, Hardware- oder Softwareinventars eines Computers ein und vergleichen Sie sie. Diese Ansicht ist für jeden einzelnen Computer verfügbar. Sie können auch den Bestand aller Computer exportieren, indem Sie auf die Option **Export** unten auf der Seite ***Verwaltung -> Alle Computer*** klicken oder sich alle anzeigen lassen unter ***Verwaltung -> Inventar***.

[In diesem Artikel finden Sie weitere Details und Anweisungen.]

Endpunkt-Sicherheit

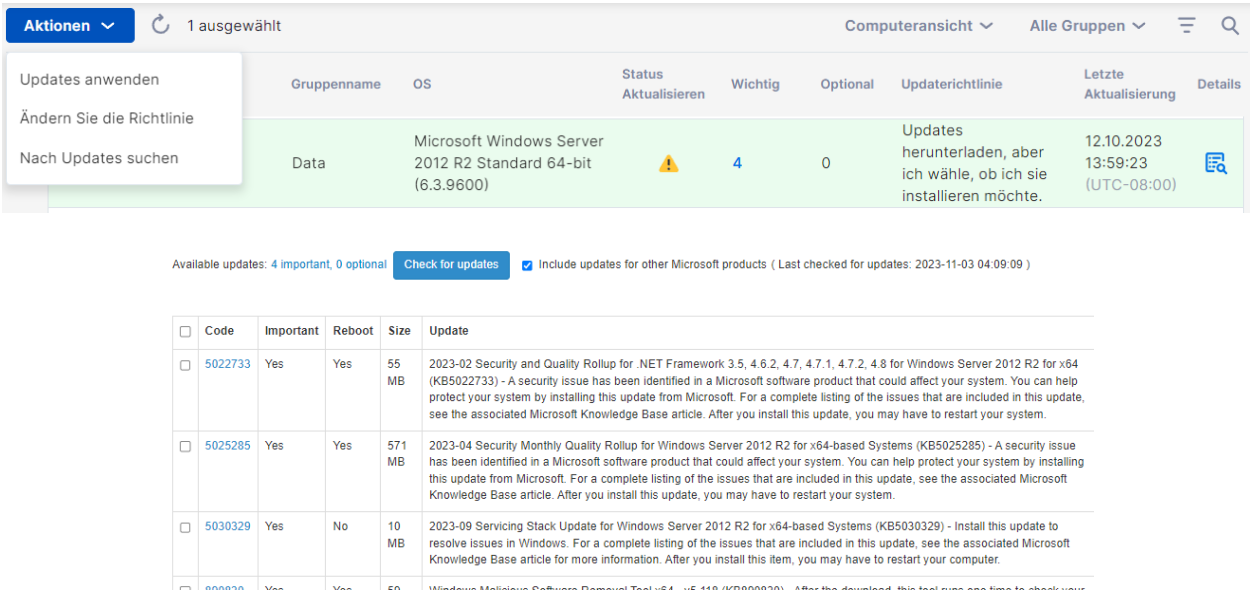
Sehen Sie sich den Status der Endpunktsicherheit für Windows-Computer unter ***Verwaltung -> Endpunktsicherheit*** an, um sicherzustellen, dass alle Computer geschützt sind. Sie können auch zusätzliche Lizenzen für [Splashtop Antivirus powered by Bitdefender] erwerben, um die Installation und das Scannen direkt über die Splashtop-Webkonsole zu ermöglichen. **Das Dashboard für Endpunktsicherheit ist für Team-Eigentümer, Admins und Group Admins verfügbar.**



[In diesem Artikel finden Sie weitere Details und Anweisungen zu Bitdefender.]

Windows Updates

Überprüfen Sie den Status der Windows Updates eines Computers unter ***Verwaltung -> Windows Updates***. Klicken Sie auf **Details** , um verfügbare Updates sofort oder zu einem geplanten Zeitpunkt für einen bestimmten Computer zu suchen, anzuzeigen und zu pushen.



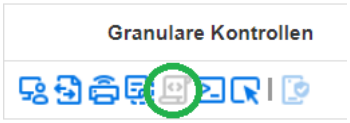
1-to-many-Aktionen und -Zeitpläne

Erstellen Sie eine 1-to-Many-Aktion, mit der Sie eine Aufgabe sofort ausführen oder für mehrere Computer oder Computergruppen planen können. Konfigurieren Sie einen Systemneustart, ein Windows-Update oder stellen Sie .EXE-, .MSI-, .PKG-Dateien und mehr automatisch bereit. Dies kann unter ***Management -> 1-to-Many-Aktionen*** oder ***1-to-Many-Zeitpläne*** konfiguriert werden.

Aktionen, die zur sofortigen Ausführung festgelegt sind, können nur auf Online-Computern ausgeführt werden. Wenn ein Computer offline ist und eine geplante Aktion durchgeführt werden soll, gibt es derzeit keinen Wiederholungsmechanismus.

1-to-Many kann je nachdem, welche Option unter ***Verwaltung -> Einstellungen*** ausgewählt wurde, nur für den Teambesitzer oder für den Teambesitzer und Administratoren verfügbar sein.

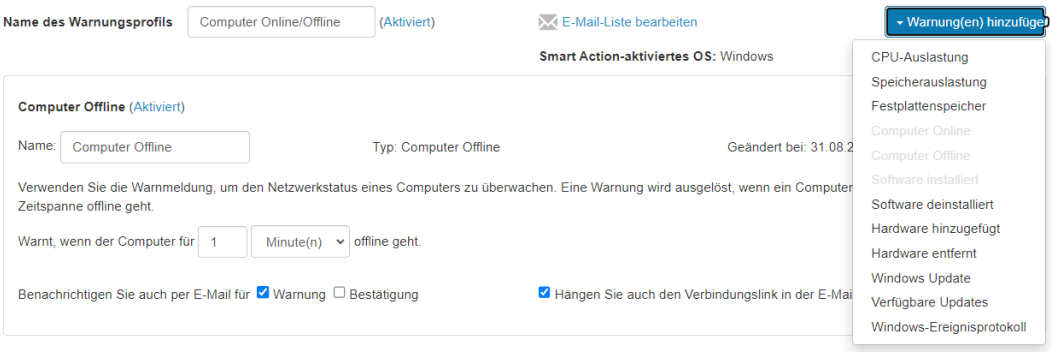
Zusätzlich können die Berechtigungen über Granulare Kontrollen konfiguriert werden.



In diesem Artikel finden Sie weitere Details und Anweisungen.

Konfigurierbare Warnungen und Smart Actions

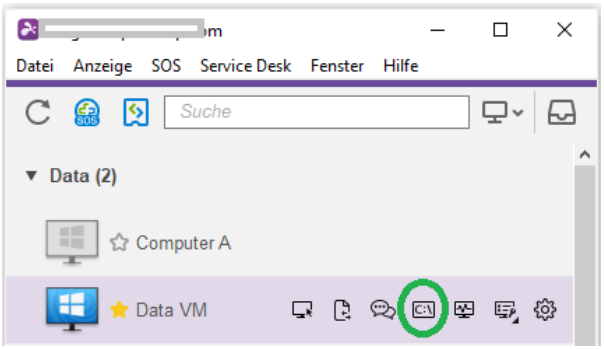
Richten Sie unter ***Verwaltung -> Warnungsprofile*** konfigurierbare Warnungen ein, um beim Auftreten bestimmter Aktionen benachrichtigt zu werden. Die Aktionen reichen von installierter/deinstallierter Software über CPU-/Festplattenauslastung bis hin zu Computer online/offline und mehr.



In diesem Artikel finden Sie weitere Details und Anweisungen.

Befehle aus der Ferne

Klicken Sie in der Business App auf das Symbol "Fernbefehl" eines Computers, um im Hintergrund Befehlszeilen- oder Terminalbefehle an einen entfernten Windows- oder Mac-Computer zu senden.

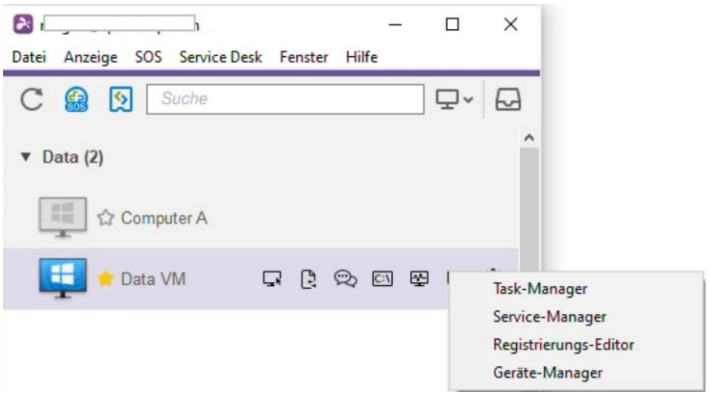


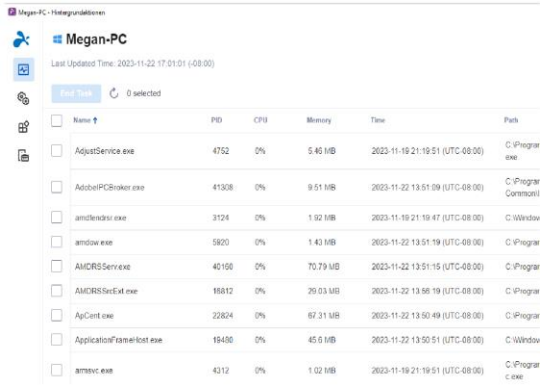
Diese Funktion ist für alle Benutzer des Teamsverfügbar, wenn sie aktiviert ist, und erfordert die Eingabe der Administrator-Anmeldedaten des Remote-Computers, um darauf zuzugreifen.

In diesem Artikel finden Sie weitere Details und Anweisungen.

Systemtools (Hintergrundaktionen)

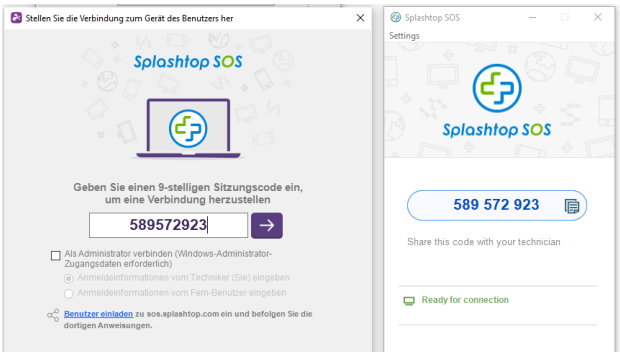
Greifen Sie auf Systemtools wie Registry Editor, Device Manager, Service Manager und Task Manager zu, ohne eine Fernsitzung starten zu müssen.





11. Beaufsichtigter Zugang – SOS (Techniker)

Techniker-Lizenzen ermöglichen den beaufsichtigten Zugang mit Splashtop SOS. Verwenden Sie Splashtop SOS, um mit einem 9-stelligen Sitzungscode auf Windows-, Mac-, iOS-, Android- und Chromebook-Geräte zuzugreifen.



Um eine Verbindung herzustellen, geben Sie den 9-stelligen Sitzungscode ein, den der Endbenutzer, der die Splashtop-SOS-App ausführt, generiert hat. Die Anleitung finden Sie hier .

Zusätzliche Eigenschaften:

- Verbinden mit Adminstratorrechten
- Wechseln von OS-Benutzern
- Neustart und Verbindung wiederherstellen
- SOS mit benutzerdefiniertem Branding
- ITSM/Helpdesk-Integrationen (ServiceNow, Freshservice, Freshdesk, Zendesk, Jira und weitere folgen in Kürze)

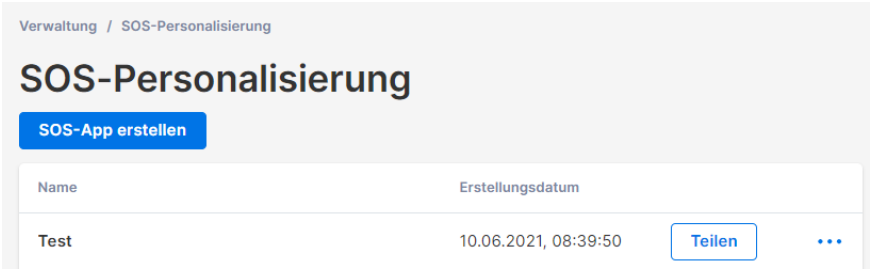
Detaillierte Einstellungen

Konfigurieren Sie mit den Detaillierten Einstellungen, wer den Beaufsichtigten Zugriff verwenden kann. Der Team-Eigentümer kann die Standardberechtigung „Beaufsichtigter Zugriff“ pro Benutzerrolle unter ***Verwaltung -> Einstellungen*** konfigurieren. Dies bestimmt die Standardberechtigung für den Beaufsichtigten Zugriff eines Benutzers, wenn er zum Team eingeladen wird.

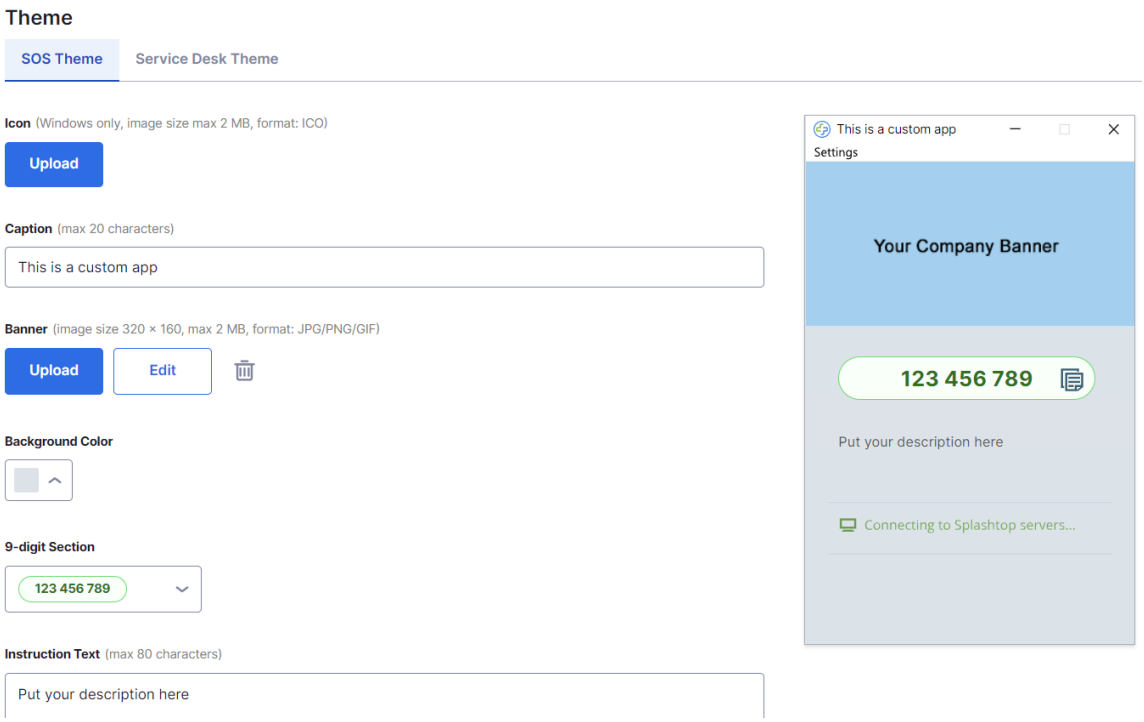
Unter ***Verwaltung -> Benutzer***, können Sie die Berechtigung „Beaufsichtigter Zugriff“ auch für einzelne Benutzer oder Benutzergruppen konfigurieren.

12. SOS-Anpassung (Techniker)

Individuelles Branding ist für die Splashtop SOS-App verfügbar. Um eine benutzerdefinierte App zu erstellen, gehen Sie zu ***Management -> SOS personalisieren -> SOS-App erstellen.***



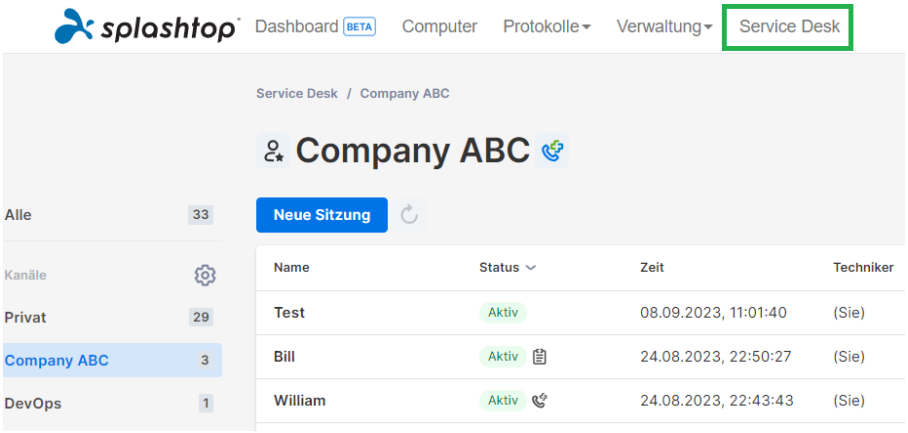
Passen Sie verschiedene Bereiche wie App-Name, Farben und Beschreibungen an. Sie können auch einen Haftungsausschluss erstellen und zusätzliche Einstellungen wie Audio und Proxy konfigurieren.

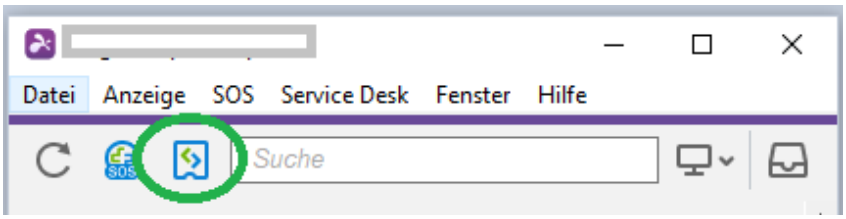


13. Service Desk (Techniker)

Service Desk bietet eine Schnittstelle für Techniker, um eine Warteschlange von beaufsichtigten Sitzungen zu verwalten und den Workflow ihrer Teams zu verbessern. Anstatt darauf zu warten, dass der Endbenutzer den 9-stelligen POS-Code bereitstellt, können Techniker einen benutzerdefinierten App-Link senden und ihn zu einer Warteschlange hinzufügen. **Erfordert eine Technikerlizenz.**

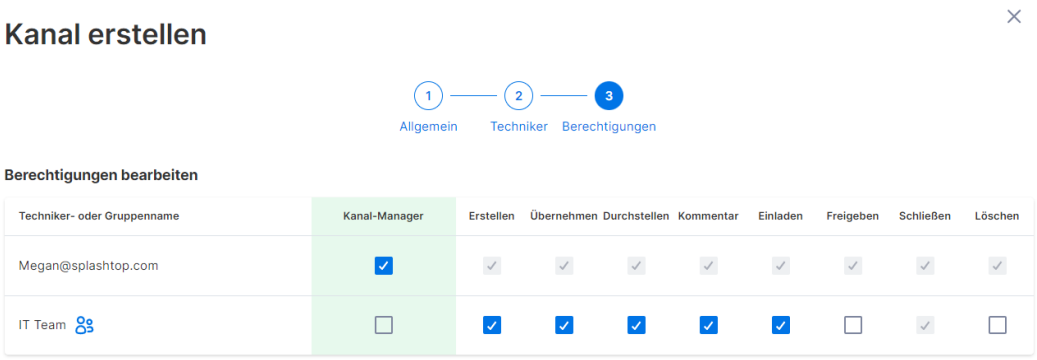
Um Service Desk aufzurufen, klicken Sie auf das Service Desk in my.splashtop.eu oder auf das Symbol in der Business-App.





Channel Management

Gehen Sie zu ***Verwaltung -> Kanäle***, um Servicedesk-Kanäle zu verwalten. Hier können Sie eine benutzerdefinierte SOS-App, Techniker und Berechtigungen zuweisen und zusätzliche Funktionen wie SOS Call aktivieren.



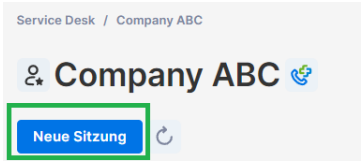
Erstellen von Support-Sitzungen

Es gibt mehrere Möglichkeiten, eine Service Desk-Supportsitzung zu starten:

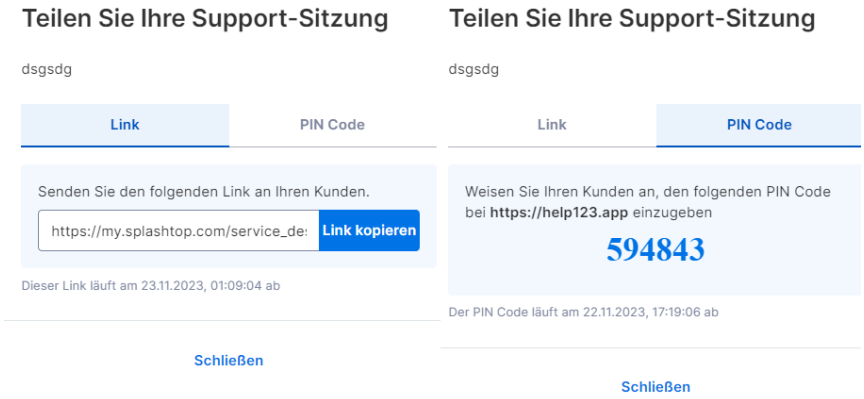
Einladungslink oder 6-stelliger PIN-Code

Techniker können eine Support-Sitzung initiieren, indem sie einen Sitzungseinladungslink oder einen 6-stelligen PIN-Code erstellen.

1. Klicken Sie in der Service Desk-Konsole auf **Neue Sitzung.**



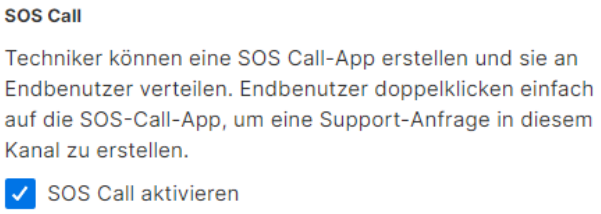
2. Sobald die Sitzung erstellt ist, teilen Sie den Einladungslink mit dem Endbenutzer oder weisen Sie den Benutzer an, help123.app aufzurufen und den 6-stelligen Code einzugeben.



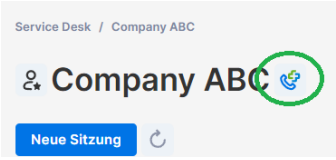
SOS Call

Erstellen Sie eine SOS Call-App und stellen Sie diese vorab den Endbenutzern zur Verfügung. Wann immer sie Unterstützung benötigen, können sie die SOS Call-App starten und eine Anfrage erstellen.

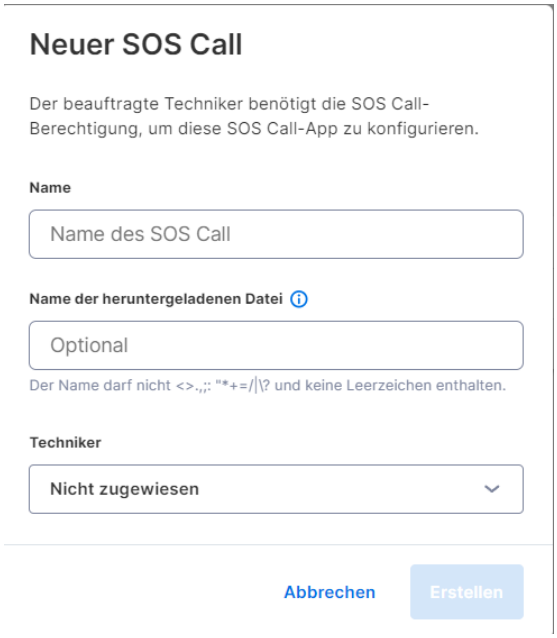
1. Stellen Sie sicher, dass in den Kanaleinstellungen SOS Call aktiviert ist.



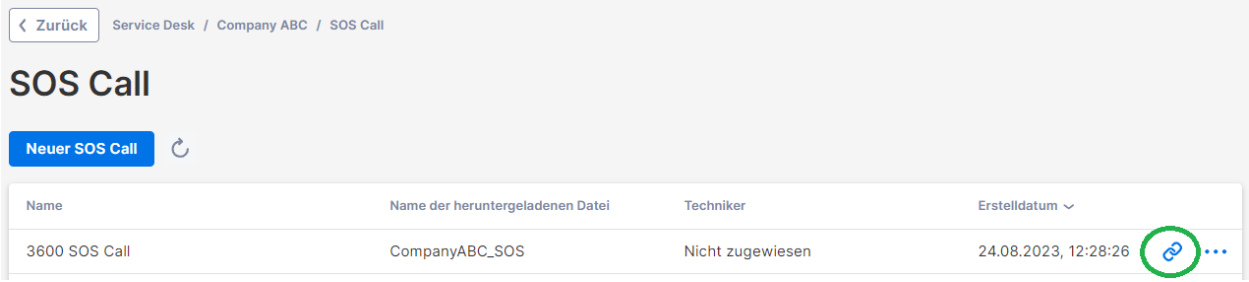
2. Um SOS Call-Apps zu erstellen und zu verwalten, klicken Sie auf das Symbol neben dem Kanalnamen:



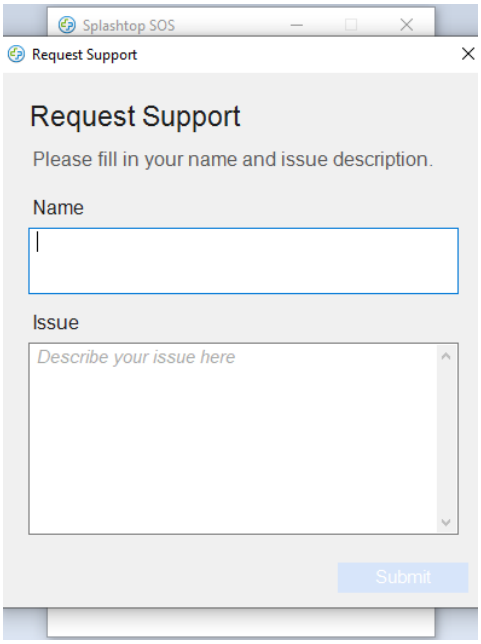
3. Erstellen Sie eine SOS Call-App. Sie können den Namen der heruntergeladenen Datei konfigurieren und den erstellten Sitzungen auch einen Techniker vorab zuweisen.



4. Kopieren Sie den Download-Link und senden Sie ihn an Ihren Endbenutzer. Endbenutzer können den Link zur späteren Verwendung auf ihrem Desktop speichern.



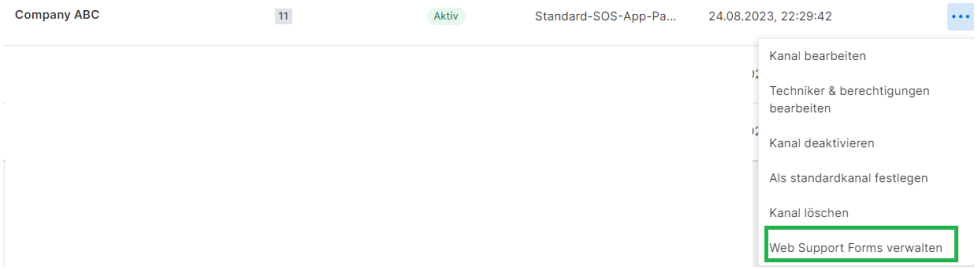
5. Wenn ein Endbenutzer bereit ist, eine Support-Sitzung zu starten, kann er die SOS Call-App herunterladen und ausführen, um seine Anfrage zu stellen.



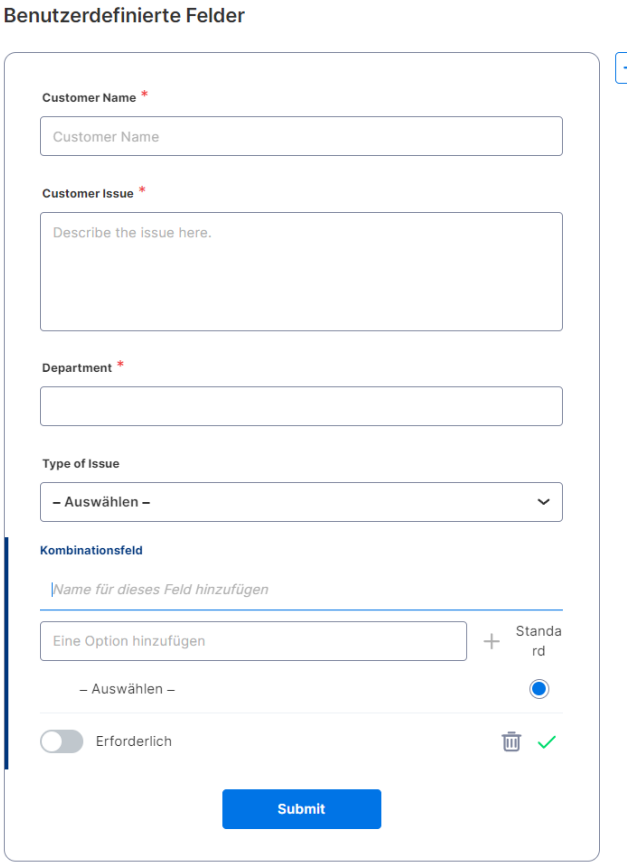
Web-Support-Formular

Erstellen Sie ein benutzerdefiniertes Webformular und betten Sie es in Ihre Support-Website ein. Endbenutzer können nach dem Absenden des Formulars eine Support-Sitzung starten.

1. Klicken Sie unter ***Verwaltung -> Kanäle*** auf **Web-Support-Form verwalten** für den jeweiligen Kanal.

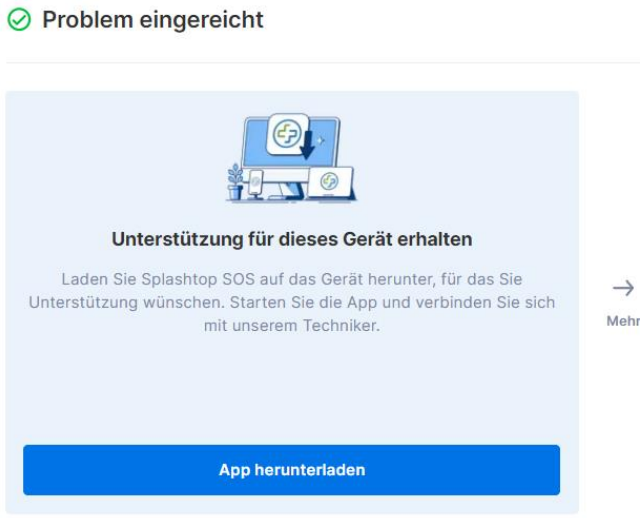


2. Erstellen Sie benutzerdefinierte Felder für das Webformular. Die Felder „Kundenname“ und „Vorfall“ sind erforderlich.



3. Betten Sie das Code-Snippet auf Ihrer Website ein.

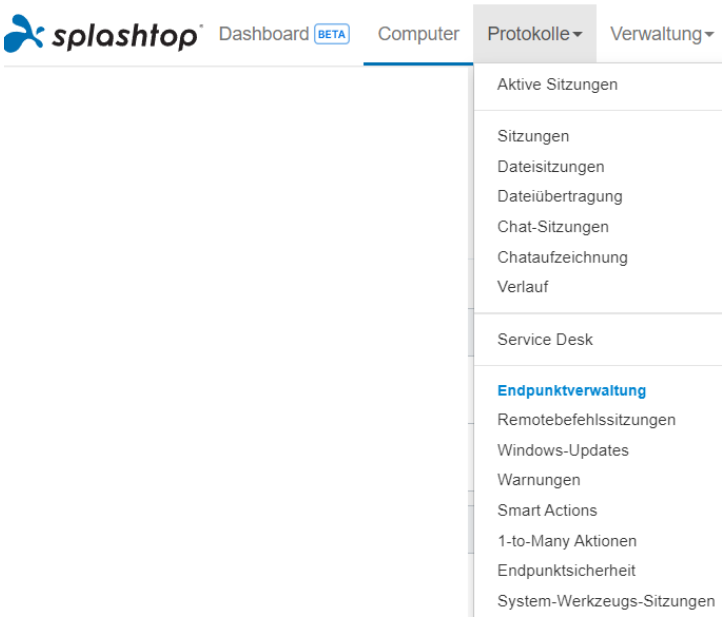
4. Endbenutzer werden aufgefordert, die SOS-App herunterzuladen und auszuführen, sobald sie das Formular eingereicht haben. Eine neue Sitzung wird in der Service Desk-Warteschlange erstellt.



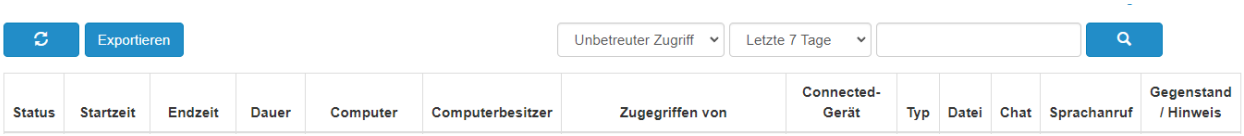
14. VERZEICHNISSE

Splashtop unterhält Protokolle zur Selbstkontrolle. Der Team-Eigentümer und die Administratoren können die Protokolle aller Mitglieder des Teams einsehen. Die Mitglieder sehen nur ihre eigenen Protokolle.

Um Protokolle anzusehen, gehen Sie zu ***my.splashtop.com -> Protokolle*** .



Die Protokolle umfassen die letzten 7, 30 oder 60 Tage. Wenn Ihr Dienst sowohl unbeaufsichtigten als auch beaufsichtigten Zugriff umfasst, können Sie auswählen, welche Protokolle angezeigt werden soll. Scrollen Sie zum unteren Ende der Seite zu **Als CSV exportieren**, um bis zu einem Jahr vergangener Protokolle herunterzuladen.



[In diesem Artikel finden Sie eine Übersicht über Protokolle.]

15. Offene APIs

RESTful APIs sind für alle Splashtop Enterprise-Teams verfügbar. APIs helfen dabei, manuelle Workflows zu optimieren und ermöglichen außerdem die Integration von Splashtop mit anderen Drittanbieter-Tools und -Plattformen.

Klicken Sie hier, um unsere API-Referenz anzuzeigen.

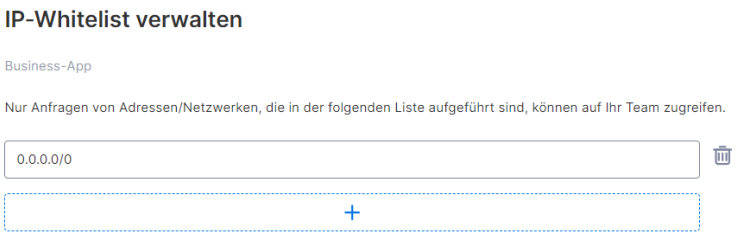
Der Team-Eigentümer oder Super Admin kann ein API-Token unter ***Verwaltung -> Einstellungen -> API*** erstellen.

16. Zusätzliche Eigenschaften:

Diese zusätzlichen erweiterten Funktionen sind für Splashtop Enterprise verfügbar. Kontaktieren Sie Splashtop Sales oder Customer Success, um weitere Informationen zu erhalten.

IP-Beschränkung

Beschränken Sie den Zugriff auf die Webkonsole https://my.splashtop.com oder auf die Splashtop Business App – basierend auf der IP-Adresse.



In diesem Artikel finden Sie weitere Details und Anweisungen.

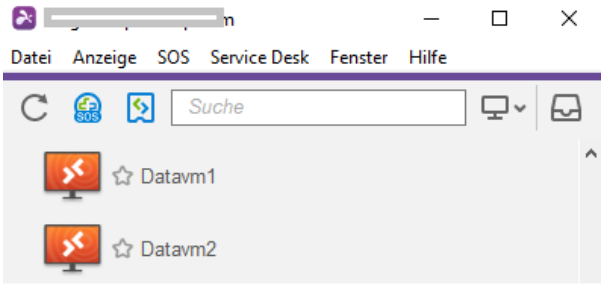
SIEM-Protokollierung

Exportieren Sie Splashtop-Sitzungs- und Verlaufsprotokolle zur weiteren Analyse in eine SIEM-Software (Security Information and Event Management).

In diesem Artikel finden Sie weitere Details und Anweisungen.

SPLASHTOP CONNECTOR

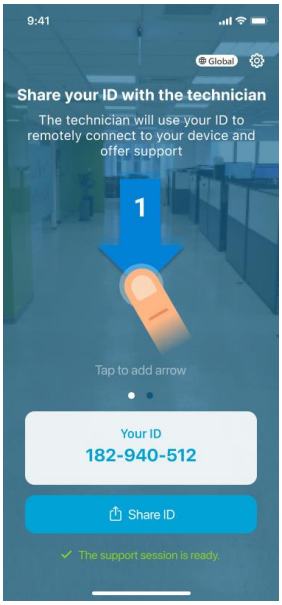
Überbrücken Sie RDP- und VNC-Verbindungen zu Windows-, Mac- und Linux-Computern sicher über Splashtop, ohne VPN zu verwenden oder Software auf jedem Computer installieren zu müssen.



In diesem Artikel finden Sie weitere Details und Anweisungen.

Splashtop AR

Stellen Sie eine Verbindung zu externen Standorten her und lösen Sie Probleme live mit Kamerafreigabe und AR-Anmerkungen.



In diesem Artikel finden Sie weitere Details und Anweisungen.