



Splashtop Enterprise

Administratoren-Handbuch

3. November 2023

Inhaltsverzeichnis

Änderungsprotokoll – ab der letzten Version vom 03.11.2022.....	4
1. Bereitstellung	5
Wie aktualisiere ich Splashtop Streamer?	9
Präferenzrichtlinien	10
2. Zusätzliche Anforderungen für MacOS.....	12
3. Einmal-Login / Single Sign-On (SSO)	13
4. Benutzer einladen	14
Teamrollen	14
5. Gruppierung	16
Verbindungspool.....	16
Hinzufügen von Benutzern oder Computern zu einer Gruppe	17
6. Zugriffsberechtigungen	18
7. Geplanter Zugriff	20
Konfiguration des geplanten Zugriffs.....	20
Ressourcen & Zeitpläne verwalten	24
Wenn ein Gruppenadministrator entfernt wird, was passiert mit den Ressourcen/Zeitplänen, die ihm gehören?	25
8. Team-Einstellungen.....	27
Übersicht der Team-Einstellungen.....	27
Feature-Konfiguration.....	28
Benutzer-Konfiguration.....	29
Sicherheit	30
9. Granulare Steuerung	31
10. Endpunktverwaltung (Techniker)	33
Windows-Ereignisprotokolle.....	33
Computerinventar - System, Hardware, Software	33
Endpunkt-Sicherheit	34
Windows Updates.....	34
1-to-many-Aktionen und -Zeitpläne	35
Konfigurierbare Warnungen und Smart Actions	36
Befehle aus der Ferne	36

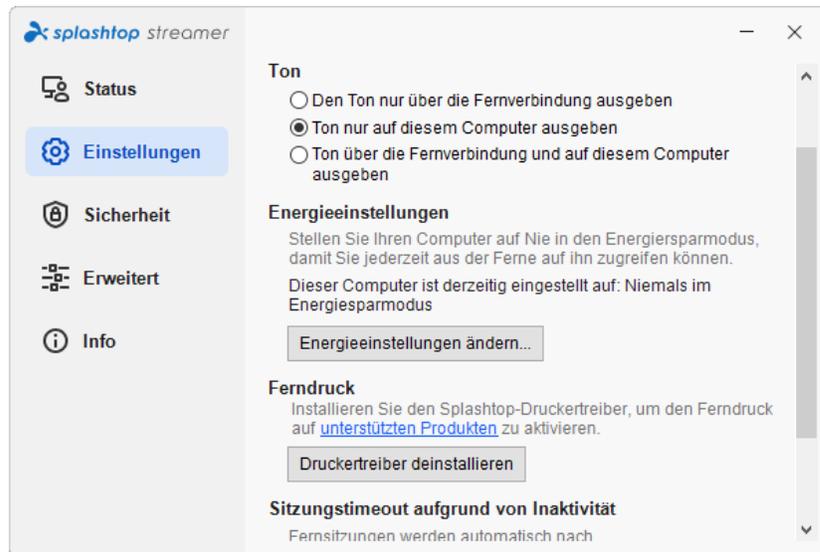
Systemtools (Hintergrundaktionen)	37
11. Beaufsichtigter Zugang – SOS (Techniker)	38
Detaillierte Einstellungen	38
12. SOS-Anpassung (Techniker)	39
13. Service Desk (Techniker)	40
Channel Management	40
Erstellen von Support-Sitzungen	41
Einladungslink oder 6-stelliger PIN-Code	41
SOS Call	41
Web-Support-Formular	43
14. VERZEICHNISSE	46
15. Offene APIs	47
16. Zusätzliche Eigenschaften:	48
IP-Beschränkung	48
SIEM-Protokollierung	48
SPLASHTOP CONNECTOR	49
Splashtop AR	49

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 Zeitzone 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

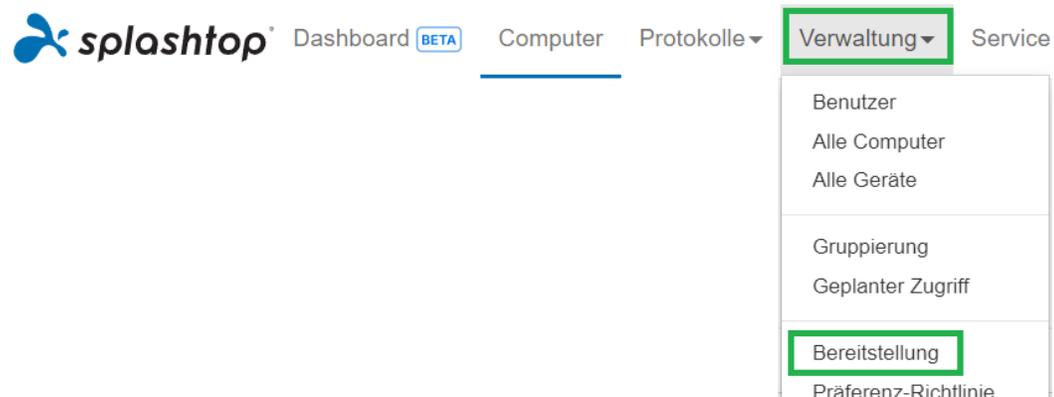
1. Bereitstellung

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**.



- 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.

**Allgemeine
Einstellungen**

Automatischer Start des Streamer

Starten Sie Splashtop Streamer bei jedem Start des Computers automatisch.

Timeout der Leerlaufsituation

Remotesitzungen werden automatisch getrennt, nachdem sie

minutes of no keyboard/mouse activity (0 means no timeout).

Streamer-Tray-Symbol ausblenden

Streamer-Symbol in der Windows-Systemablage oder in der Mac-Menüleiste ausblenden. Aktivieren Sie diese Option, um die Wahrscheinlichkeit zu verringern, dass Benutzer den Streamer manipulieren.

Direktverbindung aktivieren

Verwenden Sie im selben Netzwerk eine direkte Verbindung, um eine bessere Leistung zu erzielen. Abhängig von der Sicherheitsrichtlinie Ihres Unternehmens möchten Sie diese Option möglicherweise deaktivieren.

Verwenden Sie die Software-erstellte UUID

Erzeugt eine völlig zufällige Streamer-UUID, anstatt auf Hardware-Kennungen zu basieren. Lesen Sie den [Support-Artikel](#), um zu erfahren, wann diese Option nützlich sein kann.

Sicherheit

Verlangen Sie eine Anmeldung unter Windows oder Mac

Bei einer Remote-Verbindung muss der Benutzername und das Passwort des Computers eingegeben werden

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

- 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.

Default	Name des Bereitstellungspakets	Regel für die Benennung von Computern	Code	Erstellungsdatum	Bereitstellen
<input type="radio"/>	Architecture	Aktuellen Hostnamen des Betriebssystems verwenden	<input type="text"/>	07.07.2020 	<input type="button" value="Bereitstellen"/>

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.

Erstellen Sie ein benutzerdefiniertes Installationsprogramms für die Bereitstellung

Teilbarer Link

[Link ausprobieren](#)

Option 1: Link teilen

- 1 Senden Sie den obigen Link an Ihre Benutzer. Der Link führt diese zu einer Webseite, wo sie das Installationsprogramm herunterladen können und einfache Anweisungen zur Einrichtung finden.
- 2 Nachdem Ihre Benutzer das Installationsprogramm ausgeführt haben, werden deren Computer für Sie zugänglich.

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.

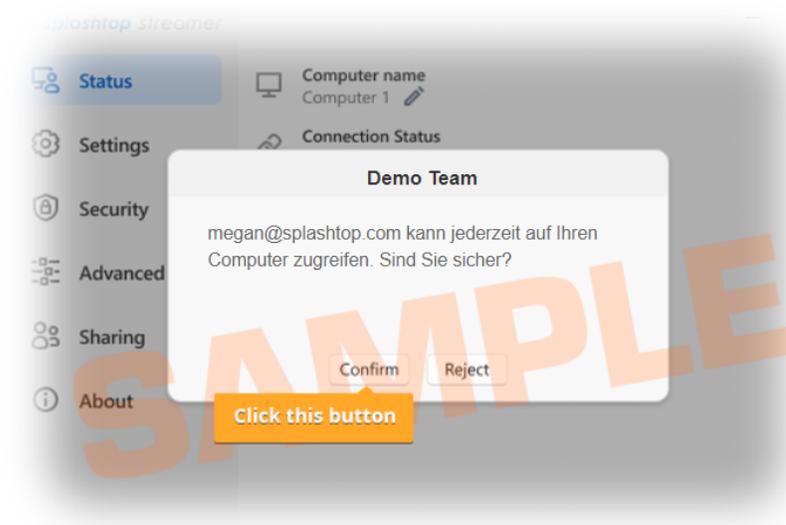
Schritt 1: Laden Sie den Streamer herunter.



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.

Option 2: Installer herunterladen

Plattform   



Easy Deployment Installer: Der Bereitstellungscode ist in das Installationsprogramm integriert. Bei der Installation des Streamers ist es nicht erforderlich, einen Bereitstellungscode einzugeben.

- 1 Laden Sie das Streamer-Installationsprogramm herunter.
- 2 Senden Sie das Installationsprogramm und den 12-stelligen Code an Ihre Benutzer.
- 3 Nachdem Ihre Benutzer das Installationsprogramm ausgeführt und den Code eingegeben haben, werden deren Computer für Sie zugänglich.

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:

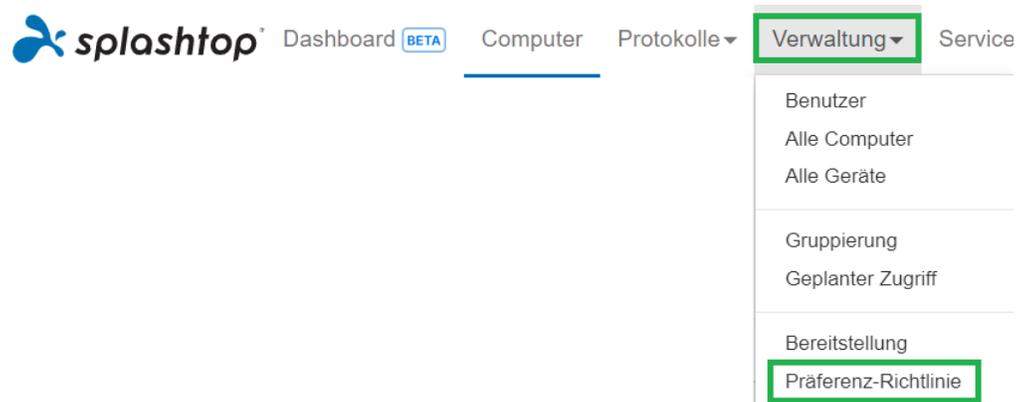
- Manuelles Update über die Webkonsole
- Manuelles Update über Registerkarte Streamer -> Info -> Nach Updates suchen
- Manuelles Update durchführen, indem Sie das neueste Streamer-Installationsprogramm ausführen
- Manuelles Update innerhalb der Business App
- Automatisches Aktualisieren mit .EXE, .MSI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

Weitere Informationen finden Sie in diesem Artikel über [Splashtop Streamer-Updates](#).

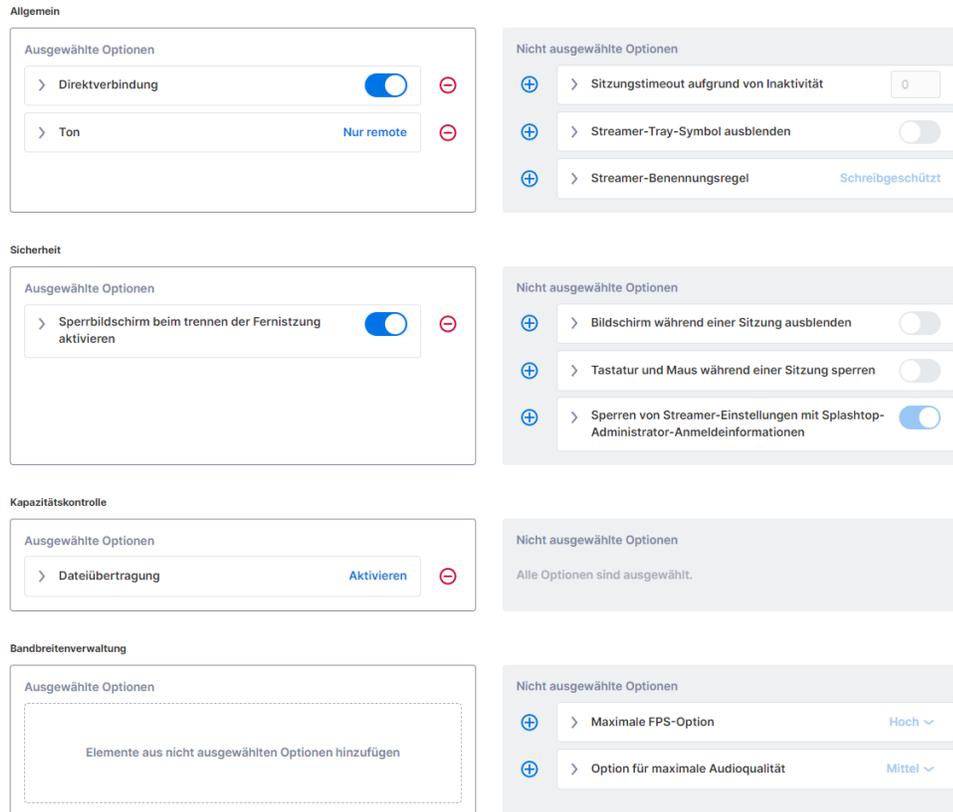
Präferenzrichtlinien

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.

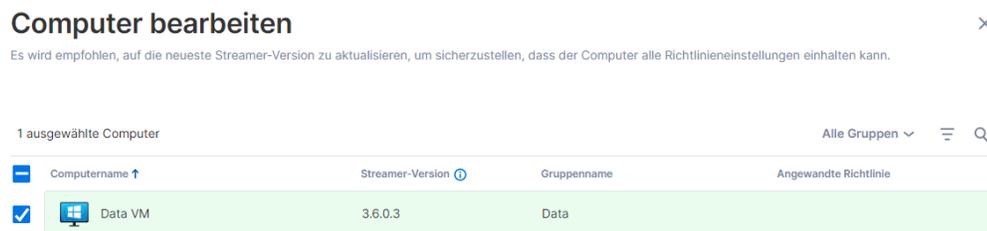
1. Um eine neue Richtlinie zu erstellen, melden Sie sich bei my.splashtop.com an und klicken Sie auf **Verwaltung** -> **Präferenzrichtlinie**.



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.

<input type="checkbox"/>	Name ↑	Gruppe	Streamer Ver.	Präferenz-Richtlinie
<input type="checkbox"/>	 Data VM	Data	3.6.0.3	ABC

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.](#)

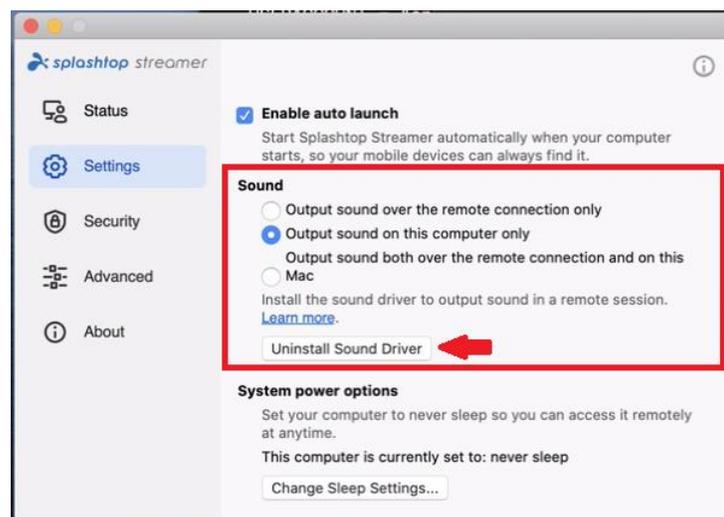
2. Zusätzliche Anforderungen für MacOS

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 Mikrophonberechtigung 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).

Single Sign-On

[Neue SSO-Methode](#) [Anweisungen anzeigen](#)

SSO-Name	IDP-Typ	Protokoll	Status	Geräteauthentifizierung	
Standard Test ADFS	ADFS	SAML 2.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	...

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.

Laden Sie Benutzer per E-Mail ein

E-Mail

Sie können auch mehrere E-Mail Adressen eingeben. Trennen Sie diese durch Kommas oder benutzen Sie für jede Adresse einfach eine neue Zeile.

Rolle : Admin Gruppe : Standardgruppe

Wird als gruppenspezifischer Admin anstelle des regulären Admin eingerichtet

*Administratoren können standardmäßig auf alle Computer zugreifen. Mitglieder können standardmäßig nicht auf Computer zugreifen. Mit "Zugriff erlauben" oder "Gruppe zuweisen" können Sie die Zugriffsberechtigung später ändern.

Authentifizierungsmethode : Test method

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**.

Gruppe erstellen

Gruppenname

Sie können mehrere Gruppen trennen, indem Sie jede Gruppe in einer neuen Zeile hinzufügen.

Benutzergruppe

Computergruppe

Diese Gruppe als Verbindungspool einrichten

Sie können 3 Arten von Gruppen erstellen:

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

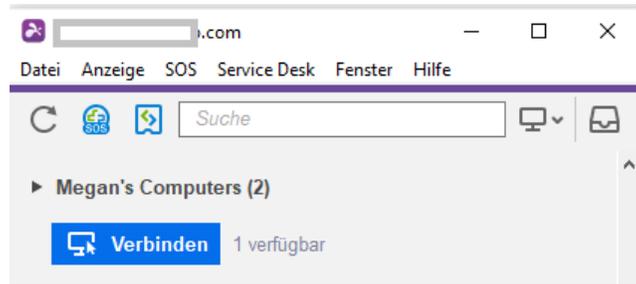
Eine **Nur-Benutzer-Gruppe** darf nur aus Benutzern bestehen. Die Gruppierung von Benutzern ermöglicht, Zugriffsberechtigungen für mehrere Benutzer gleichzeitig festzulegen. Sie ermöglicht außerdem, Zugriffsberechtigungen automatisch auf einen neuen Benutzer anzuwenden.

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.



<input type="checkbox"/>	Rolle	Splashtop-Konto	Anzeigenname	Status	2FA Status	Granulare Kontrollen	Letzte Verbindung	Granulare Kontrolle Zugriffsberechtigung
<input type="checkbox"/>	Mitglied			Eingeladen	⊗			

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

Benutzerzugriffsberechtigung ()

Administratoren können Benutzern/Benutzergruppen Zugriff auf Computer/Computergruppen gewähren.

Alle Computer

Nur Computer in ihrer Gruppe

Nur bestimmte Computer und Computergruppen

Keine Computer

Nur Computer, die auf Gruppenberechtigungen basieren

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

Ausgewählte Computer

1 ausgewählt

Alle Gruppen

<input type="checkbox"/>	Name <input type="button" value="v"/>
<input type="checkbox"/>	<input type="button" value="v"/> Data 2
<input type="checkbox"/>	<input type="button" value="🖥️"/> Computer A
<input checked="" type="checkbox"/>	<input type="button" value="🖥️"/> 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.

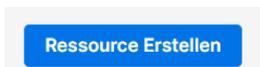
Konfiguration des geplanten Zugriffs

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.

Geplanter Zugriff

Zeitzoneneinstellungen (GMT-08:00) Pacific Time (US & Canada) ▼

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.

Ressource Erstellen



Ressourcenname

Name der Ressource

Beschreibung (optional)

Beschreibung hinzufügen

Erweiterte Einstellungen ▼

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.

Erweiterte Einstellungen [^](#)

Unterstützungsverbindungspool für Terminpläne.

Unterstützt exklusiven Zugriff (fern oder lokal) für Mitgliedskonten.

Als Standardeinstellungen festlegen

Legen Sie diesen Terminplan als Connection Pool fest.

Verhindern Sie, dass Mitglieder auf einen Computer zugreifen, der bereits angemeldet ist.

Ermöglichen Sie den Zugriff auf die Computer im Ruhezustand:
10 minuten [v](#)

Leerer Bildschirm und Sperren von Tastatur/Maus während einer Sitzung.

Melden Sie sich nach dem normalen Trennen automatisch ab:
Sofort [v](#)

Sperrbildschirm vor der automatischen Abmeldung für unbeabsichtigtes Trennen:
Trennen: 1 Minute [v](#)

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

Ressource Erstellen

1 —
 2 —
 3

Allgemein **Computergruppenadministrator**

Ausgewählte Computer

2 ausgewählt Alle Gruppen [v](#) [+](#) [-](#) [Q](#)

	Name v
<input checked="" type="checkbox"/>	v Data 2
<input checked="" type="checkbox"/>	<input type="checkbox"/> Computer A
<input checked="" type="checkbox"/>	<input type="checkbox"/> Data VM

- (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.

Ressource Erstellen

1 Allgemein — 2 ComputeGruppenadministrator — 3 Gruppenadministrator zuweisen (optional)

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

Hinzufügen eines Terminplans, um die Einrichtung abzuschließen

Sie haben erfolgreich eine Ressource erstellt. Jetzt können Sie einen Terminplan für den Zugriff von Benutzern auf die zugeordneten Computer und Computergruppen erstellen.

[Später](#) [Terminplan Erstellen](#)

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

Terminplan Erstellen

Terminplanname

Beschreibung (optional)

Zeit

Die Zeitzone ist in **GMT -08:00 (Pacific Time (US & Canada))**.

-

Wiederholen

So Mo **Di** Mi Do **Fr** Sa

Die Wiederholung endet am (optional)

In-Session-Einstellungen

Erzwingen Sie die Trennung der Sitzung, wenn der Terminplan endet.

Benachrichtigen Sie Benutzer, bevor die Sitzung endet:

endet:

[Erweiterte Einstellungen](#) ^

Verbindungseinstellungen

Legen Sie diesen Terminplan als Connection Pool fest.

Benutzergruppen Zuordnen (maximal: 250)

Bitte geben Sie die Gruppennamen ein

Wähle die Gruppe

Benutzer Zuordnen (maximal: 1000)

Bitte geben Sie die E-Mail-Adressen Ihrer Benutzer

Gruppenadministrator zuweisen (optional)

- 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.

Ressourcenname	Computer	Im Besitz des Gruppenadministrators	
Inaktiv Accounting Computers Resource for set of computers used by our company's Accountants.	4	Keine	 Terminplan Verwalten Bearbeiten Löschen

- **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.

Terminplan Erstellen < > November 2023

Montag	Dienstag	Mittwoch	Donnerstag	Freitag	Samstag	Sonntag
30 08:00 End of W...	31 04:00 Session 1	Nov. 01	2 04:00 Session 1	3	4	5
6 08:00 End of W...	7 04:00 Session 1	8	9 04:00 Session 1			
13 08:00 End of W...	14 04:00 Session 1	15	16 04:00 Session 1			
20 08:00 End of W...	21 04:00 Session 1	22	23 04:00 Session 1			
27 08:00 End of W...	28 04:00 Session 1	29	30 04:00 Session 1	Dez. 01	2	

Session 1

🕒 04:00 - 13:30 16. Nov. 2023

⌚ Erzwingen Sie die Trennung der Sitzung, wenn der Terminplan endet, und benachrichtigen Sie den Benutzer 5 Minuten im Voraus.

Gruppen 0

Benutzer 0

Gruppenadministrator
Keine

Bearbeiten Löschen ...

- Klonen
- Anhalten

- **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“.

Ressourcenname	Computer	Im Besitz des Gruppenadministrators
Inaktiv Accounting Computers <small>Resource for set of computers used by our company's Accountants.</small>	4	Keine

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

Resource Name	Computers	Owned by Group Admin
Inactive Accounting Computers Resource for set of computers used by our company's Accountants.	4	None

⋮

- Manage Schedule
- Edit**
- Delete

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

Ressource Bearbeiten

Ressourcen status: Inaktiv ?

1 — 2 — 3
Allgemein — ComputeGruppenadministrator

Ressourcenname

Beschreibung (optional)

Status

Inaktiv

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.](#)

Einstellungen

- Kontoubersicht
- Team**
- API
- Abonnements
- Zahlung und Abrechnung
- Zahlungshistorie
- Code einlösen

Allgemein

[Gehen Sie zurück zur klassischen Einstellungsseite](#)

Teamname
Demo Team

Aktueller Plan
Splashtop Enterprise
5 gleichzeitige Techniker und 10 Endnutzer

Computer
39 von 1600 Computer bereitgestellt

Featurekonfiguration

	Granulare Standardeinstellungen		
	Administrator	Konfigurierbar	Mitglied
Fernbedienung	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Beaufsichtigter Zugriff	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Dateiübertragung	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Ferndruck	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Geräteumleitung Detaillierte Einrichtung			

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).

Featurekonfiguration

		Granulare Standardeinstellungen		
		Administrator	Konfigurierbar ⓘ	Mitglied
Fernbedienung		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Beaufsichtigter Zugriff		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Dateiübertragung	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Ferndruck	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Geräteumleitung Detaillierte Einrichtung	<input checked="" type="checkbox"/>			
Mikrofoneingang umleiten	<input checked="" type="checkbox"/>			
Kopieren und einfügen	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Zwischenablage als Text einfügen	<input checked="" type="checkbox"/>			
Remote-Wake	<input checked="" type="checkbox"/>			
Ferneustart	<input checked="" type="checkbox"/>			
Speichern des Chat-Transkripts einer Sitzung in den Sitzungsprotokollen Mehr erfahren	<input checked="" type="checkbox"/>			
Chat (Vorsitzung)	<input checked="" type="checkbox"/>			
Speichern des Chat-Transkripts von vor Sitzung in den Sitzungsprotokollen Mehr erfahren	<input checked="" type="checkbox"/>			
Fernbefehl	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
RDP-Rechner	<input checked="" type="checkbox"/>			
System-Werkzeuge für Admins und Eigentümer ⓘ	<input checked="" type="checkbox"/>			
1-to-many-Skripterstellung für Admins und Eigentümer ⓘ	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

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

Unbeaufsichtigter Zugriff

	Granulare Standardeinstellungen		
	Administrator	Konfigurierbar	Mitglied
Sprachanruf während der Sitzung			
Sitzungsaufzeichnung Detaillierte Einrichtung Lokale Aufzeichnung			
Meinen Desktop freigeben			
Gleichzeitige Fernsitzungen			
Web-App (Verbindung zu Ferncomputern mit Browsern)			
Sitzungsanzeige	Fernsitzung Dateiübertragung Fernbefehl Hintergrundaktionen		
Anzeigentyp			Popup

Beaufsichtigter Zugriff

Sprachanruf während der Sitzung	
Sitzungsaufzeichnung Detaillierte Einrichtung Lokale Aufzeichnung	
Meinen Desktop freigeben	
Gleichzeitige Fernsitzungen	
Web-App (Verbindung zu Ferncomputern mit Browsern)	
Sitzungsanzeige	
Anzeigentyp	Banner
Erlaubt dem Benutzer das Banner zu schließen	

Benutzer-Konfiguration

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

Benutzerkonfiguration

Gruppenspezifische Administratorrolle Mehr erfahren	
Mitgliedern erlauben, sich mit Computern in einer aktiven Verbindung zu verbinden	
Gleichzeitige Sitzungen für Mitglieder zulassen	
Mitgliedern erlauben, Verbindung zu anderen Sitzungen zu trennen	
Mitgliedern erlauben, Computer neu zu starten und Streamer neu zu starten	
Erlauben Sie Mitgliedern, auf die Registerkarte Verwaltung zuzugreifen	
Mitgliedern erlauben, Gruppen zu sehen	
Erlauben Sie Benutzern, Remote-Sitzungen von mehreren Geräten aus aufzubauen	
Mitgliedsberechtigung für Computernotizen	Kann nicht bearbeiten und anzeigen

- 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.

Sicherheit

Zwei-Faktor-Authentifizierung

[Vertrauenswürdige Geräte verwalten](#)

	Granulare Standardeinstellungen		
	Administrator	Konfigurierbar ⓘ	Mitglied
Erlauben Sie Benutzern, Geräten zu vertrauen, um zu Für immer ▼ 			
Fordern Sie Benutzer auf, die Zwei-Faktor-Authentifizierung zu verwenden	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Deaktivieren Sie die Geräteauthentifizierung, wenn die Zwei-Faktor-Authentifizierung aktiviert ist 			

Geräteauthentifizierung

	Anwendung	Browser
E-Mail-Geräteauthentifizierungslink an	Angemeldete Person ▼	Angemeldete Person ▼
Erlauben, dass Geräte authentifiziert bleiben für	Für immer ▼	Für immer ▼
Benutzern erlauben, sich an die Anmeldung zu erinnern	Ein ▼ ⓘ	
Untätige Benutzer abmelden nach	24 Stunden ▼ ⓘ	Nie ▼ ⓘ

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 Zugriff (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.

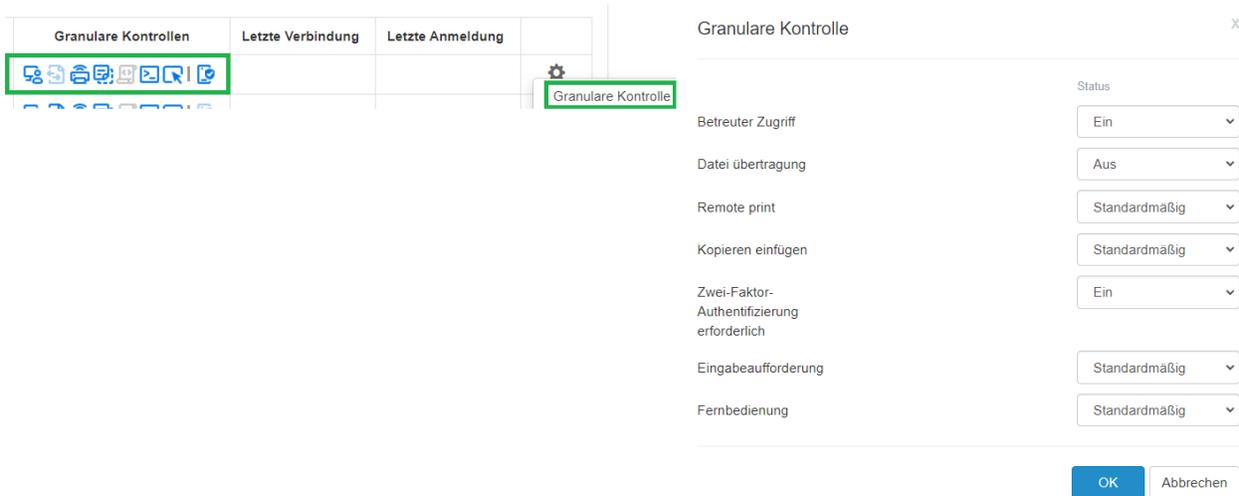
Featurekonfiguration

	Granulare Standardeinstellungen		
	Administrator	Konfigurierbar 	Mitglied
Fernbedienung	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Beaufsichtigter Zugriff	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Dateiübertragung 	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Ferndruck 	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Geräteumleitung Detaillierte Einrichtung 			
Mikrofoneingang umleiten 			
Kopieren und einfügen 	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Zwischenablage als Text einfügen 			
Remote-Wake 			
Ferneustart 			
Speichern des Chat-Transkripts einer Sitzung in den Sitzungsprotokollen Mehr erfahren 			
Chat (Vorsitzung) 			
Speichern des Chat-Transkripts von vor Sitzung in den Sitzungsprotokollen Mehr erfahren 			
Fernbefehl 	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
RDP-Rechner 			
System-Werkzeuge für Admins und Eigentümer  			
1-to-many-Skripterstellung für Admins und Eigentümer 	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

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-Standard-einstellung 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.

The screenshot shows a navigation bar with tabs: Allgemein, Aktualisierungen, Virenschutz, Warnungen, Ereignisprotokolle (selected), Inventar, Zeitpläne, and Benutzerliste. Below the tabs, the text 'Ereignisprotokolle anzeigen:' is followed by filter options. 'Ereignisebene:' has checkboxes for Critical (checked), Error (checked), Warning (checked), and Information (unchecked). 'Ereignistyp:' has checkboxes for System (checked), Application (checked), Security (checked), and Setup (checked). A date range filter is set from '2023-11-22 00:00' to '2023-11-22 23:59'. There is an 'Ereignis-ID-Filter:' input field with a search icon. A 'Zurückholen' button is at the bottom left. A checkbox 'Fügen Sie detaillierte Informationen hinzu:' is set to 'Nein'.

[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**.

The screenshot shows the 'Zeigt das Systeminventar von [Computername] an:' section. There are three radio button options: 'Schnappschüsse an für' (selected) with a date input '2023-11-22'; 'Schnappschuss vergleichen' with date inputs '2023-11-21' and '2023-11-22'; and 'Changelog anzeigen von' with two empty date inputs. Below the options, a message states: 'Der Schnappschuss für 2023-11-22 wurde am 2023-11-22 02:22:23 -0800 aktualisiert. (Aktualisieren des heutigen Inventars)'. An 'Anwenden' button is present. At the bottom, there is a dropdown menu currently showing 'Software'.

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

Endpoint-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.**

Status	Computer Name	Group	Software	Protection	Last scan time	Threats	Details
<input type="checkbox"/>	Test	Megan's Computers	Bitdefender Endpoint Security Tools Antimalware	Enabled	2020-11-10 20:00:00	42	

Scan task: N/A

[Acknowledge all threats](#)

Threat Name	Detected Timestamp	Object Name	Action	Acknowledged
Gen:Illusion.ML.Skyline.B.2010101	2020-11-06 14:00:00 -0800	C:\Users\ [REDACTED]		Acknowledge
Gen:Illusion.ML.Skyline.B.2010101	2020-11-06 14:00:00 -0800	C:\Users\ [REDACTED]		Acknowledge

[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.

Aktionen	Gruppenname	OS	Status Aktualisieren	Wichtig	Optional	Updaterrichtlinie	Letzte Aktualisierung	Details
<ul style="list-style-type: none"> Updates anwenden Ändern Sie die Richtlinie Nach Updates suchen 	Data	Microsoft Windows Server 2012 R2 Standard 64-bit (6.3.9600)		4	0	Updates heruntergeladen, aber ich wähle, ob ich sie installieren möchte.	12.10.2023 13:59:23 (UTC-08:00)	

Available updates: 4 important, 0 optional [Check for updates](#) Include updates for other Microsoft products (Last checked for updates: 2023-11-03 04:09:09)

<input type="checkbox"/>	Code	Important	Reboot	Size	Update
<input type="checkbox"/>	5022733	Yes	Yes	55 MB	2023-02 Security and Quality Rollup for .NET Framework 3.5, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows Server 2012 R2 for x64 (KB5022733) - A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.
<input type="checkbox"/>	5025285	Yes	Yes	571 MB	2023-04 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems (KB5025285) - A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.
<input type="checkbox"/>	5030329	Yes	No	10 MB	2023-09 Servicing Stack Update for Windows Server 2012 R2 for x64-based Systems (KB5030329) - Install this update to resolve issues in Windows. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article for more information. After you install this item, you may have to restart your computer.
<input type="checkbox"/>	5000000	Yes	Yes	50 MB	Windows Malicious Software Removal Tool (MSRT) v5.49 (KB5000000) - After the download, this tool runs one time to check your

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.



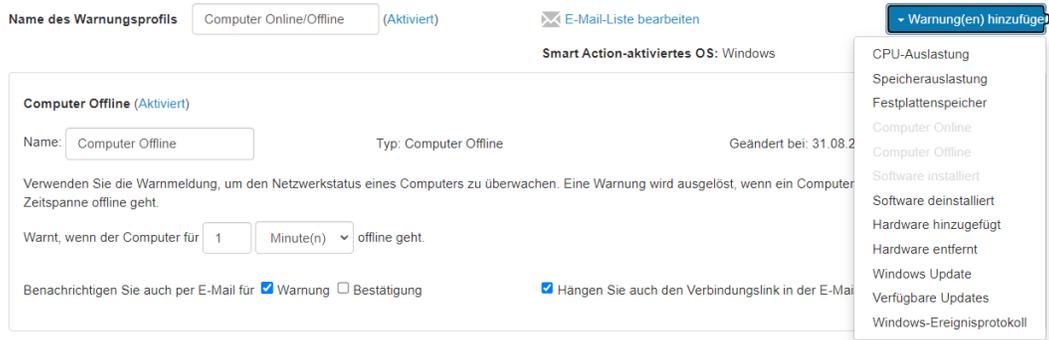
Zusätzlich können die Berechtigungen über Granulare Kontrollen konfiguriert werden.



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

Konfigurierbare Warnungen und Smart Actions

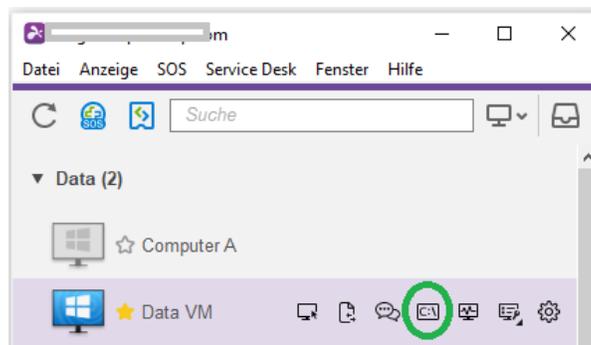
Richten Sie unter **Verwaltung -> Warnungsprofile** konfigurierbare Warnungen ein, um beim Auftreten bestimmter Aktionen benachrichtigt zu werden. Die Aktionen reichen von installierter/deinstallierter Software über CPU-/Festplattenauslastung bis hin zu Computer online/offline und mehr.



[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.

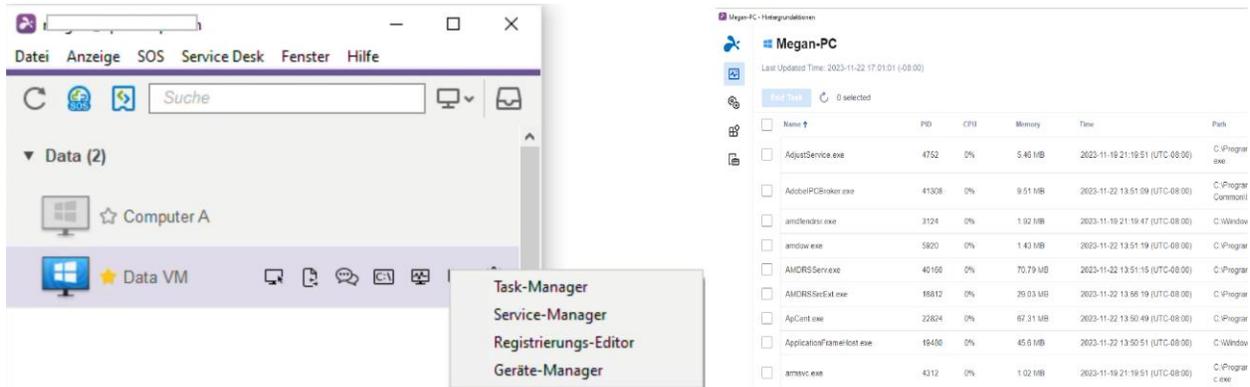


Diese Funktion ist für alle Benutzer des Teams verfügbar, wenn sie aktiviert ist, und erfordert die Eingabe der Administrator-Anmeldedaten des Remote-Computers, um darauf zuzugreifen.

[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.

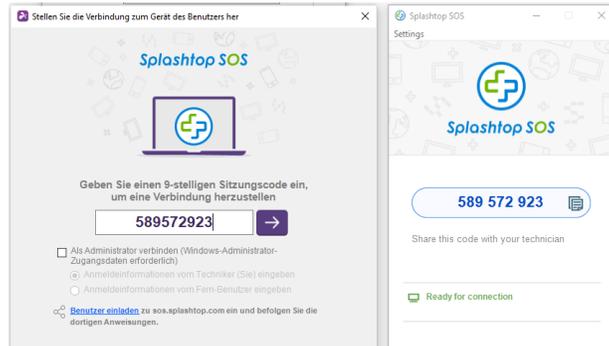


The image shows two screenshots from a Windows environment. The left screenshot displays a Windows File Explorer window with a search bar and a context menu open over the taskbar. The context menu lists the following system tools: Task-Manager, Service-Manager, Registrierungs-Editor, and Geräte-Manager. The right screenshot shows the Windows Task Manager window for a virtual machine named 'Megan-PC'. It displays a table of running processes with columns for Name, PID, CPU, Memory, Time, and Path.

Name	PID	CPU	Memory	Time	Path
AdjustService.exe	4752	0%	5.46 MB	2023-11-19 21:19:51 (UTC-08:00)	C:\Program.exe
AdobePCBroker.exe	41308	0%	9.51 MB	2023-11-22 13:51:09 (UTC-08:00)	C:\Program Gemeinl.exe
amdldrui.exe	3124	0%	1.92 MB	2023-11-19 21:19:47 (UTC-08:00)	C:\Window.exe
amdlow.exe	5820	0%	1.43 MB	2023-11-22 13:51:19 (UTC-08:00)	C:\Program.exe
AMDRSrv.exe	40168	0%	70.79 MB	2023-11-22 13:51:15 (UTC-08:00)	C:\Program.exe
AMDRSrvExt.exe	16812	0%	39.03 MB	2023-11-22 13:56:19 (UTC-08:00)	C:\Program.exe
ApCent.exe	22824	0%	67.31 MB	2023-11-22 13:50:49 (UTC-08:00)	C:\Program.exe
ApplicationFrameHost.exe	19406	0%	45.0 MB	2023-11-22 13:50:51 (UTC-08:00)	C:\Window.exe
amsvc.exe	4312	0%	1.92 MB	2023-11-19 21:19:51 (UTC-08:00)	C:\Program c.exe

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 Administratorrechten](#)
- [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.

Attended Access	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
-----------------	-------------------------------------	--------------------------	--------------------------

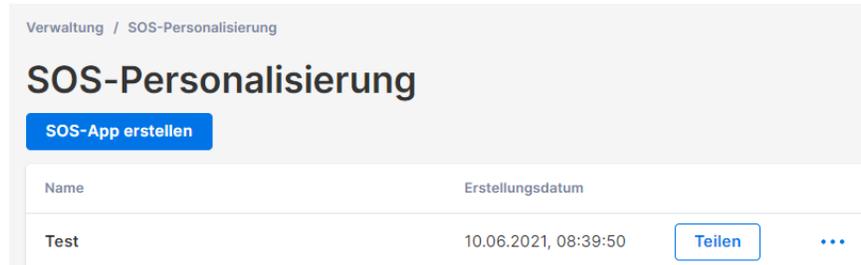
Unter **Verwaltung -> Benutzer**, können Sie die Berechtigung „Beaufsichtigter Zugriff“ auch für einzelne Benutzer oder Benutzergruppen konfigurieren.

Granulare Kontrollen	Letzte Verbindung	Letzte Anmeldung
            		
            		



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.

Theme

SOS Theme Service Desk Theme

Icon (Windows only, image size max 2 MB, format: ICO)

Upload

Caption (max 20 characters)

This is a custom app

Banner (image size 320 x 160, max 2 MB, format: JPG/PNG/GIF)

Upload

Edit



Background Color

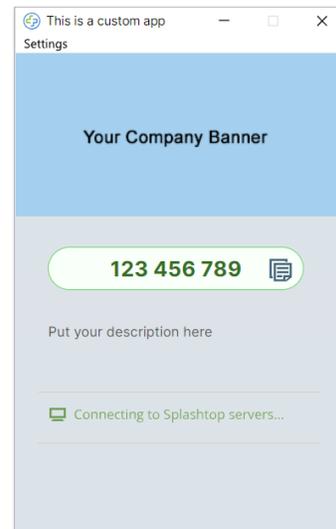


9-digit Section

123 456 789

Instruction Text (max 80 characters)

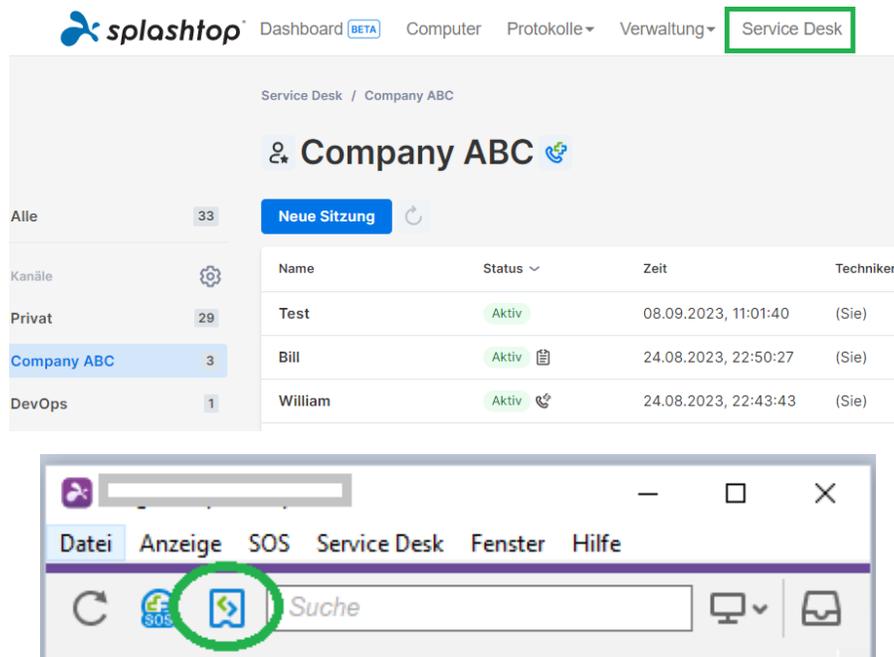
Put your description here



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.

Kanal erstellen



Berechtigungen bearbeiten

Techniker- oder Gruppenname	Kanal-Manager	Erstellen	Übernehmen	Durchstellen	Kommentar	Einladen	Freigeben	Schließen	Löschen
Megan@splashtop.com	<input checked="" type="checkbox"/>								
IT Team	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Erstellen von Support-Sitzungen

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

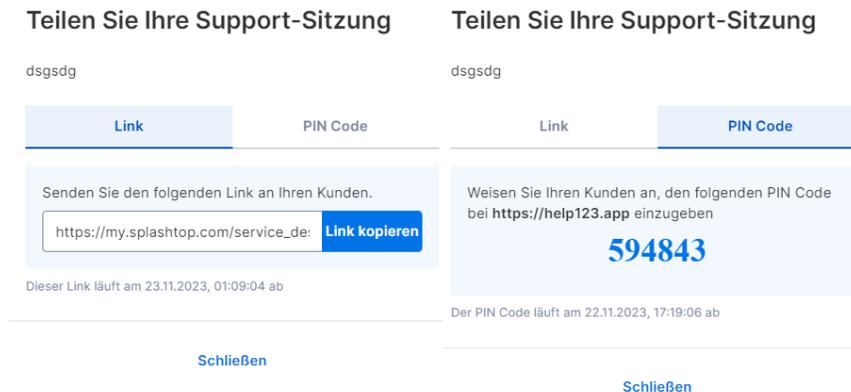
Einladungslink oder 6-stelliger PIN-Code

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.

SOS Call

Techniker können eine SOS Call-App erstellen und sie an Endbenutzer verteilen. Endbenutzer doppelklicken einfach auf die SOS-Call-App, um eine Support-Anfrage in diesem Kanal zu erstellen.

SOS Call aktivieren

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



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

Neuer SOS Call

Der beauftragte Techniker benötigt die SOS Call-Berechtigung, um diese SOS Call-App zu konfigurieren.

Name

Name der heruntergeladenen Datei ⓘ

Der Name darf nicht <>.,;: "*/+ =/|\? und keine Leerzeichen enthalten.

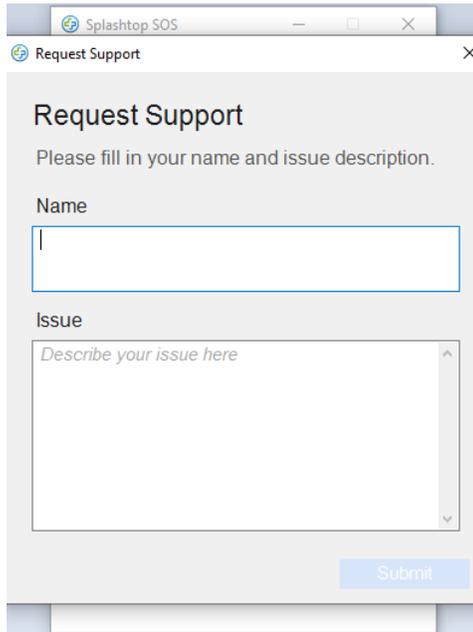
Techniker

[Abbrechen](#) [Erstellen](#)

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

Name	Name der heruntergeladenen Datei	Techniker	Erstelldatum
3600 SOS Call	CompanyABC_SOS	Nicht zugewiesen	24.08.2023, 12:28:26

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.



Request Support

Please fill in your name and issue description.

Name

Issue

Describe your issue here

Submit

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.



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

Benutzerdefinierte Felder

The screenshot shows a web form editor interface with the following elements:

- Customer Name ***: A text input field with the placeholder text "Customer Name".
- Customer Issue ***: A text area with the placeholder text "Describe the issue here.".
- Department ***: A text input field.
- Type of Issue**: A dropdown menu with the selected option "- Auswählen -".
- Kombinationsfeld**: A section for configuring a combobox field. It includes a text input field with the placeholder "Name für dieses Feld hinzufügen", a "+ Standard" button, a dropdown menu with "- Auswählen -", a "Erforderlich" (Required) toggle switch, and a trash icon.
- Submit**: A blue button at the bottom of the form.

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



Erfolgreich erstellt!

The screenshot shows a code snippet generation tool with the following elements:

- Formularbreite**: A text input field with the value "552" and a "px" unit. Below it, the text "Maximal: 800 px, Minimale: 320 px" is displayed.
- Formularhöhe**: A text input field with the value "480" and a "px" unit. Below it, the text "Maximal: 720 px, Minimale: 480 px" is displayed.
- iframe**: A code block containing the following HTML snippet:

```
<iframe width="552" height="480" src="https://help123.app/w/form/ha  
bg2am" style="padding: 4px 0;border:1px solid #80859F;border-radius:  
12px;" sandbox="allow-scripts allow-same-origin allow-popups allow-d  
ownloads"></iframe>
```
- Codeausschnitte kopieren**: A blue button to copy the code snippet.

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.

✔ Problem eingereicht



Unterstützung für dieses Gerät erhalten

Laden Sie Splashtop SOS auf das Gerät herunter, für das Sie Unterstützung wünschen. Starten Sie die App und verbinden Sie sich mit unserem Techniker.

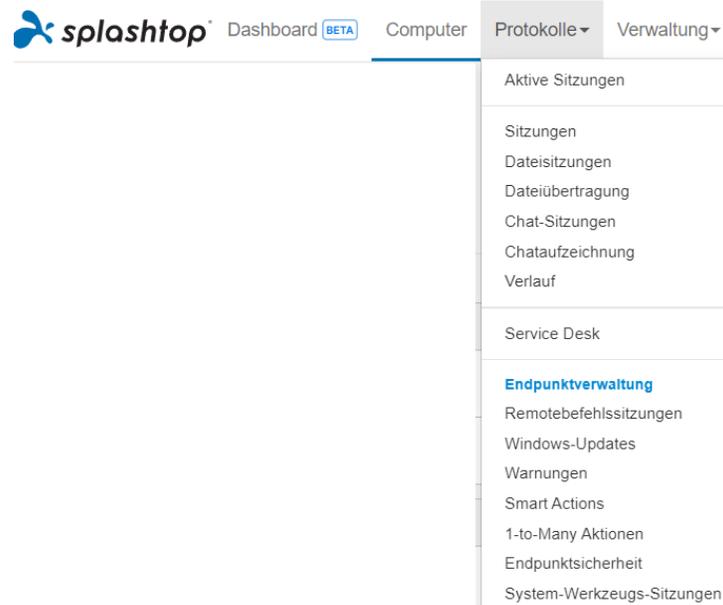
[App herunterladen](#)

→
Mehr

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.

	Exportieren	Unbetreuer Zugriff	Letzte 7 Tage	<input type="text"/>								
Status	Startzeit	Endzeit	Dauer	Computer	Computerbesitzer	Zugegriffen von	Connected-Gerät	Typ	Datei	Chat	Sprachanruf	Gegenstand / Hinweis

[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.

Einstellungen

- Kontoübersicht
- Team
- API**
- Abonnements
- Zahlung und Abrechnung
- Zahlungshistorie
- Code einlösen

API-Token

API-Token erstellen

Name	Beschreibung	Token	Status	Ablaufdatum	
New Test		1234640-xRid6WI... 	<input checked="" type="checkbox"/>	N/A	...
Test 3		1234649-U2GT73... 	<input checked="" type="checkbox"/>	N/A	...

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.

IP-Whitelist verwalten

Business-App

Nur Anfragen von Adressen/Netzwerken, die in der folgenden Liste aufgeführt sind, können auf Ihr Team zugreifen.

[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).

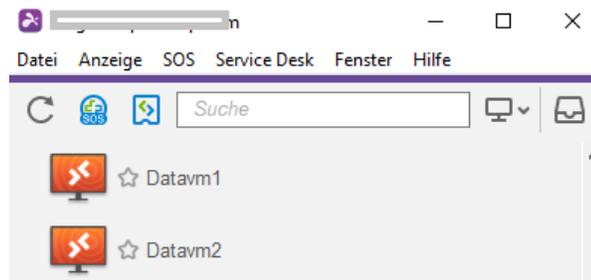


The banner features a central graphic of a computer monitor displaying a document, with three colored squares (purple, orange, red) to its left and a green shield with a white checkmark to its right. Below the graphic, the text reads: **Create Your SIEM App**, *Integrate with the SIEM services*, and *Erfahren Sie mehr darüber, wie Sie eine App erstellen können.* At the bottom center is a blue button with the text **Erstellen** and a downward arrow.

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

SPLASHTOP CONNECTOR

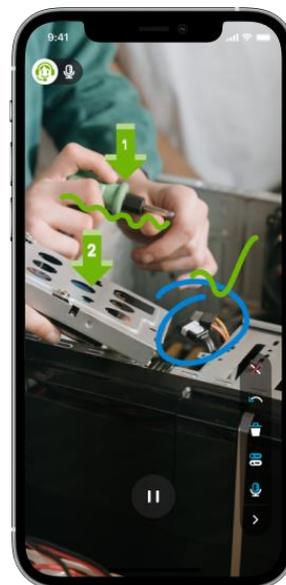
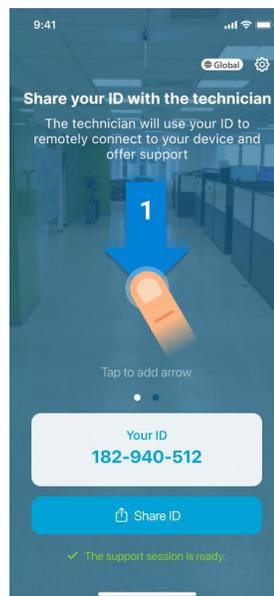
Überbrücken Sie RDP- und VNC-Verbindungen zu Windows-, Mac- und Linux-Computern sicher über Splashtop, ohne VPN zu verwenden oder Software auf jedem Computer installieren zu müssen.



[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.](#)