



Splashtop Enterprise

Administratoren-Handbuch

03. November 2022

Inhaltsverzeichnis

| | |
|---|----|
| Änderungsprotokoll – ab der letzten Version vom 04/20/2022..... | 4 |
| 1. Bereitstellung | 5 |
| Wie aktualisiere ich Splashtop Streamer? | 9 |
| Präferenzrichtlinien..... | 10 |
| 2. Zusätzliche Anforderungen für MacOS..... | 11 |
| 3. Einmal-Login / Single Sign-On (SSO) | 12 |
| 4. Benutzer einladen | 13 |
| Teamrollen | 13 |
| 5. Gruppierung | 15 |
| Hinzufügen von Benutzern oder Computern zu einer Gruppe | 16 |
| 6. Zugriffsberechtigungen | 17 |
| 7. Geplanter Zugriff | 19 |
| Konfiguration des geplanten Zugriffs..... | 19 |
| Ressourcen & Zeitpläne verwalten | 24 |
| Wenn ein Gruppenadministrator entfernt wird, was passiert mit den Ressourcen/Zeitplänen, die ihm gehören? | 25 |
| 8. Team-Einstellungen..... | 26 |
| Übersicht der Team-Einstellungen..... | 26 |
| 9. Granulare Steuerung | 29 |
| 10. Remote-Computerverwaltung (Techniker)..... | 31 |
| Windows-Ereignisprotokolle..... | 31 |
| Computerbestand - System, Hardware, Software | 31 |
| Endpunkt-Sicherheit | 32 |
| Windows Updates..... | 32 |
| 1-to-many-Aktionen und -Zeitpläne | 33 |
| Konfigurierbare Warnmeldungen..... | 33 |
| Befehle aus der Ferne | 34 |
| 11. Beaufsichtigter Zugang – SOS (Techniker)..... | 35 |
| Detaillierte Einstellungen..... | 35 |

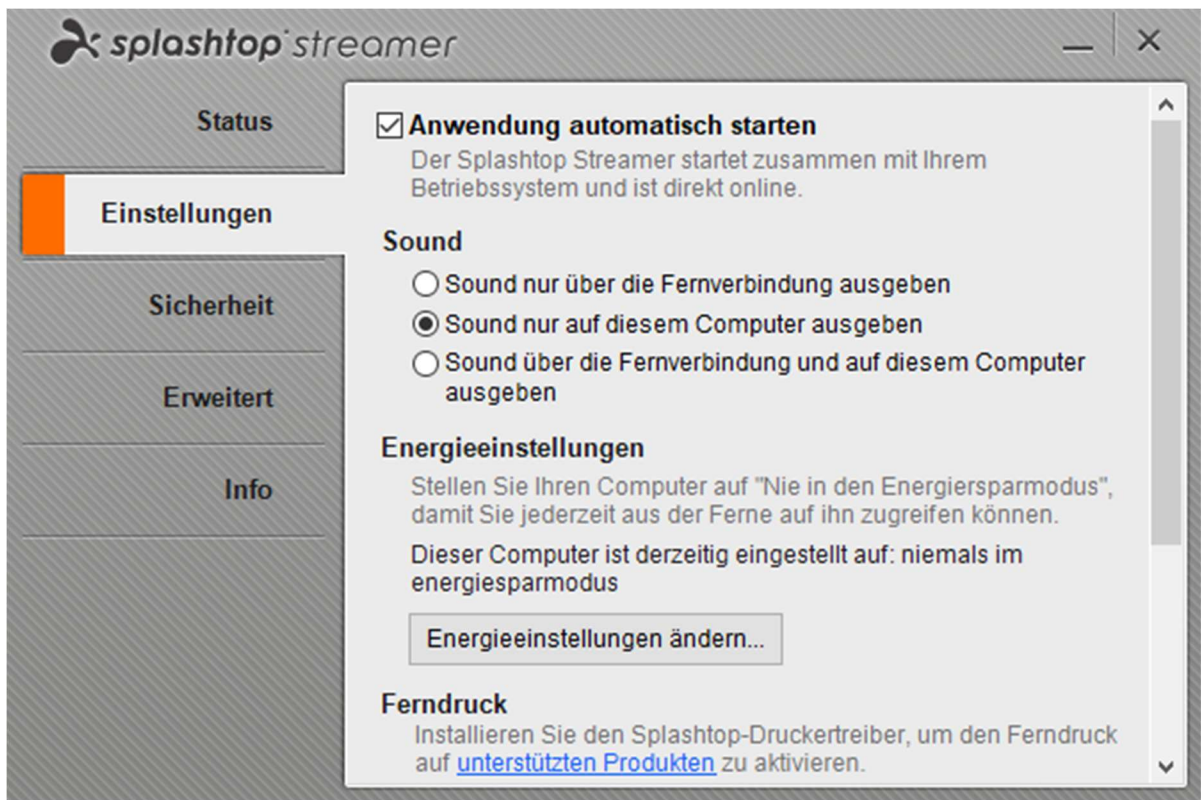
| | | |
|-----|----------------------------------|----|
| 12. | SOS-Anpassung (Techniker) | 36 |
| 13. | Service Desk (Techniker) | 37 |
| 14. | VERZEICHNISSE | 38 |
| 15. | Zusätzliche Eigenschaften: | 39 |
| | IP-Beschränkung | 39 |
| | SIEM-Protokollierung | 39 |
| | SPLASHTOP CONNECTOR | 40 |
| | Splashtop AR | 41 |

Änderungsprotokoll – ab der letzten Version vom 04/20/2022

- Bereitstellung, Abschnitt 1
 - Einstellungsrichtlinien hinzugefügt, um Streamer- und Sitzungseinstellungen über die Webkonsole zu verwalten
- Einladen von Benutzern, Abschnitt 4
 - Überarbeitet und Informationen zu Super Admins hinzugefügt
- Granulare Kontrollen, Abschnitt 9
 - 1-to-Many zur Liste der unterstützten granularen Steuerelemente hinzugefügt
- Remote-Computerverwaltung, Abschnitt 10
 - Informationen zum Inventar-Dashboard hinzugefügt
 - Informationen über 1-to-Many hinzugefügt - Skripte sind jetzt standardmäßig in der Technikerlizenz enthalten.
- Service Desk (Techniker), Abschnitt 13
 - Erwähnung für 6-stelligen PIN-Code hinzufügen

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.com ein und klicken Sie auf **Management -> Deployment**.



- 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, Klangerleitung usw.

Allgemeine Einstellungen

Automatischer Start des Streamer

Starten Sie Splashtop Streamer bei jedem Start des Computers automatisch.

Timeout der Leerlaufsitzung

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.


Sicherheit

Verlangen Sie eine Anmeldung unter Windows oder Mac

Bei einer Remote-Verbindung muss der Benutzername und das

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 **Deploy**, um die Bereitstellungsoptionen anzuzeigen.

| Name des Bereitstellungspakets | Regel für die Benennung von Computern | Code | Erstellungsdatum | Bereitstellen |
|--------------------------------|---|----------------------|---|--|
| Animatiion | Verwenden Sie den aktuellen Computernamen | <input type="text"/> | 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.

Teilbarer Link

https://my.splashtop.com/team_deployment/download/PY42WJK2WPXS

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.

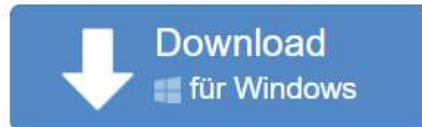
Willkommen bei Splashtop Remote Support

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

team (owner @splashtop.com)

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

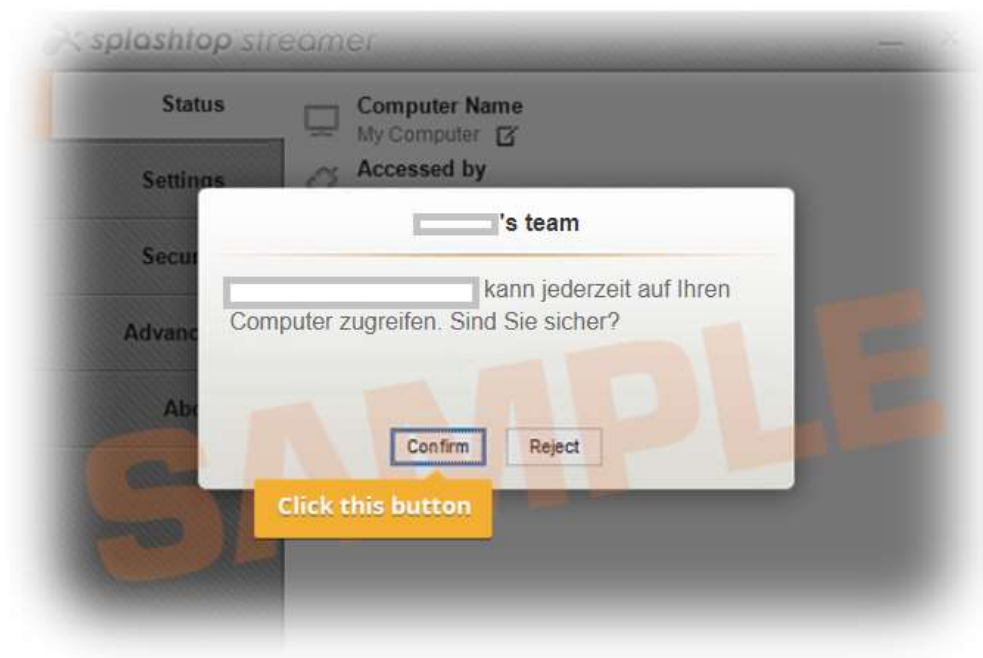
Schritt 1: Laden Sie den Streamer herunter.



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   

Windows (EXE, version 3.4.6.0) (Einfache Bereit: 

[Herunterladen](#)



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](#)
- Die Einstellungen des Bereitstellungspakets gelten für den Streamer nur bei der Installation. Um die Einstellungen eines Streamers nach der Bereitstellung zu aktualisieren, können Sie ihn mit einem neuen Paket erneut bereitstellen oder die Einstellungen direkt im Streamer manuell ändern.
- 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
- 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. Weisen Sie der Richtlinie Computer zu.
Hinweis: Nur Streamer ab Version 3.5.2.2 werden im Menü angezeigt.
4. Zugewiesene Computer werden durch ein neues Symbol gekennzeichnet, das angibt, dass sie Teil einer Richtlinie sind.
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.](#)

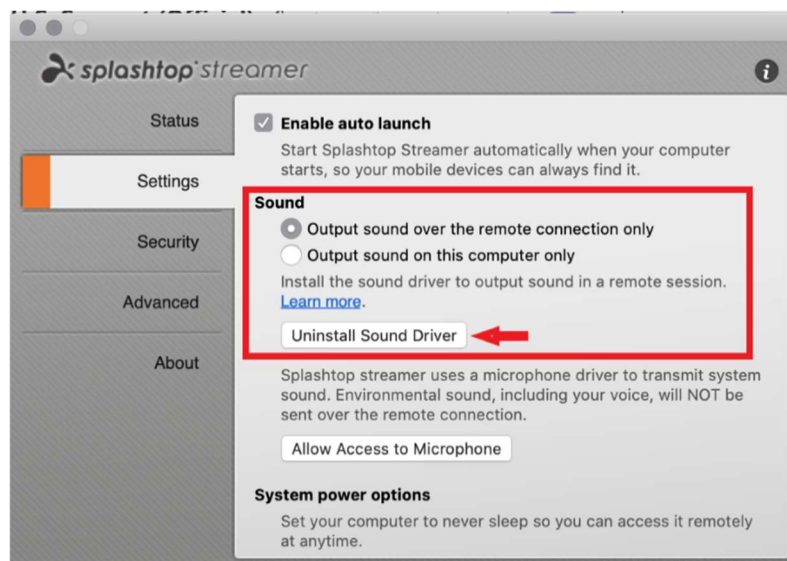
2. Zusätzliche Anforderungen für MacOS

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

- **Sicherheits- und Datenschutzberechtigungen** für macOS [10.14 Mojave](#), [10.15 Catalina/11 Big Sur](#) und neuer:



- **Audio:** Um das Audio-Streaming über die Remoteverbindung zu aktivieren, [installieren Sie den Splashtop Sound Driver](#) und erlauben Sie die Mikrofon-Berechtigung für Mojave/Catalina/Big Sur. Wenn Apps auf Mac-Computern Soundtreiber von Drittanbietern wie Avid Pro Tools oder Adobe Premiere verwenden, sind möglicherweise [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, beachten Sie, dass Sie die [Geräteauthentifizierung](#) für Benutzer, die mit dieser Methode verbunden sind, ausschalten können. So müssen die Benutzer nicht auf zusätzliche E-Mail-Links klicken, um ihre Geräte zu authentifizieren. Deaktivieren Sie einfach die Geräteauthentifizierung für die SSO-Methode unter **Verwaltung -> Einstellungen (nur Team-Eigentümer)**.

| Standardmäßig (zurücksetzen) | Status | SSO- Name | IDP Type | Protokoll | Geräteauthentifizierung | die Einstellungen |
|---------------------------------|-------------------------------------|----------------------|-------------|-----------|--------------------------|---|
| <input type="radio"/> | <input checked="" type="checkbox"/> | <input type="text"/> | ADFS | SAML 2.0 | <input type="checkbox"/> |  |

4. Benutzer einladen

Laden Sie Benutzer ein, indem Sie auf **Verwaltung -> Benutzer -> Benutzer 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 X

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

:

Teamrollen

- **Besitzer:** Der Besitzer 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 Besitzer, und der Status kann nicht zwischen Benutzerkonten übertragen werden.

- **Administrator:** 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.
 - [Gruppenadministrator](#) : Gruppenadministrator 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 & Gruppen-Admins haben Zugriff auf die Remote Management-Funktionen (Remote Command, Systeminventar, etc.), wenn Sie **Technikerlizenzen** von Splashtop Enterprise erworben haben. Die Möglichkeit, bestimmten Benutzern Zugriff auf diese Funktionen zu gewähren (unabhängig von der Teamrolle), wird in Kürze verfügbar sein.

- **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

Wenn Sie mehrere Gruppen eingeben, trennen Sie diese einfach durch Kommas oder geben Sie sie jeweils in einer neuen Zeile ein.

Der Name darf keines der folgenden Zeichen enthalten <> ; : " * + = \ | ?

- Benutzergruppe
- Computergruppe

Gruppe erstellen

Abbrechen

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.

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.

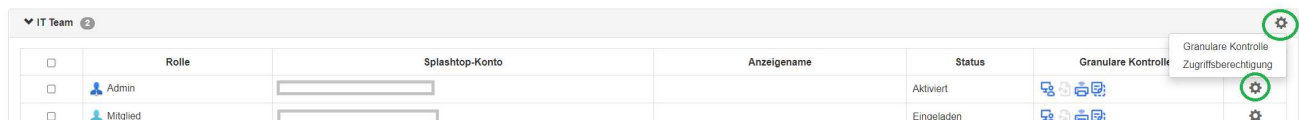
6. Zugriffsberechtigungen








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.



| | Rolle | Splashtop-Konto | Anzeigename | Status | Granulare Kontrolle |
|--------------------------|----------|-----------------|-------------|------------|---|
| <input type="checkbox"/> | Admin | | | Aktiviert |     |
| <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

Speichern

Abbrechen

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

Alle Gruppen

Wählen Sie Alle / Alles löschen Alle erweitern / Alles einklappen

Nur ausgewählte Anzeigen

7 Computer ausgewählt

Site A 3

Site B 2

| | Computername  |
|-------------------------------------|---|
| <input checked="" type="checkbox"/> |  Computer E |
| <input type="checkbox"/> |  Computer F |

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.

Ressource Erstellen



1 Allgemein — 2 Computer

Ressourcenname

Buchhaltungscomputer

Beschreibung (optional)

Ressource für eine Reihe von Computern, die von den Buchhaltern unseres Unternehmens verwendet werden.

[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.
Nur Windows Streamer v3.4.6.0
- Unterstützt exklusiven (Remote- oder lokalen) Zugriff 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** 
- Leerer Bildschirm und Sperren von Tastatur/Maus während einer Sitzung.
- Melden Sie sich nach dem normalen Trennen automatisch ab: **Sofort** 
- Sperrbildschirm vor der automatischen Abmeldung für unbeabsichtigtes Trennen: **1 minute** 

Für "Benutzer bei einer Trennung abmelden" und "Bildschirm vor Benutzerabmeldung sperren ..." ist Splashtop Streamer v3.4.4.0 oder höher erforderlich.


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

Ressource Bearbeiten


1 — 2 — 3
Allgemein **Computer&gruppenadministration**

Computer

Computer Auswählen

Wählen Sie Alle / Alles löschen Alle erweitern / Alles einklappen Nur ausgewählte AnzeigenAlle Gruppen 

4 Computer ausgewählt

| | | Computername  |
|-------------------------------------|--------------------------|--|
| <input checked="" type="checkbox"/> | <input type="checkbox"/> | Computer E |
| <input type="checkbox"/> | <input type="checkbox"/> | Computer E |

- (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 Bearbeiten



Gruppenadministrator zuweisen (optional)

Wählen Sie Gruppenadministrator

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

Verwaltung / Geplanter Zugriff

Geplanter Zugriff

- Erstellen Sie eine Ressource, um eine Reihe von C
- Berechtigungen für Geplanten Zugriff werden zus
- Berechtigungen für Geplanten Zugriff überschreit

Ressource Erstellen

Ressourcename

Buchhaltungscomputer
Ressource für eine Reihe von Computern, die von

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**

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

Terminplan Erstellen

Terminplanname

Wochenendrückblick

Beschreibung (optional)

Der Buchhalter greift jeden Montag auf den Computer zu, um die Ausgaben der letzten Woche zu überprüfen.

Zeit

Die Zeitzone ist in GMT +00:00 (UTC).

2021-06-01

08:00

12:30

Wiederholen

Wöchentlich

So

Mo

Di

Mi

Do

Fr

Sa

Die Wiederholung endet am (optional)

Wählen Sie Enddatum

In-Session-Einstellungen

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

Benachrichtigen Sie Benutzer, bevor die Sitzung

endet: 5 minuten

Erweiterte Einstellungen

Verbindungseinstellungen

- Legen Sie diesen Terminplan als Connection Pool fest.

Benutzergruppen Zuordnen (max: 250)

Bitte geben Sie die Gruppennamen ein

Wähle die Gruppe

Benutzer Zuordnen (max: 1000)

Bitte geben Sie die E-Mail-Adressen Ihrer Benutzer ein

Nutzer Hinzufügen

- 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 aus dem Betriebssystem des Computers abgemeldet.
- Klicken Sie auf Erweiterte Einstellungen, um die Verbindungspool- und Exklusivzugriffseinstellungen zu verwalten, falls diese in der Ressource aktiviert sind.

Ressourcen & Zeitpläne verwalten

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

The screenshot shows a resource card for 'Buchhaltungscomputer' under the category 'Computer'. The card includes a description: 'Ressource für eine Reihe von Computern, die von den Buchhaltern unseres Unt...'. A 'Hinzufügen' button is visible. To the right of the card is a management menu with three options: 'Terminplan Verwalten', 'Bearbeiten', and 'Löschen'. A green circle highlights the three-dot menu icon.

- **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.

The screenshot displays a calendar interface for 'Buchhaltungscomputer' for the month of June 2021. A 'Terminplan Erstellen' button is at the top left. The calendar shows a weekly overview with dates from Monday to Sunday. A detailed view for Monday, 7. Juni, is shown on the right, featuring an event titled 'Wochenendrückblick' from 08:00 to 12:30. The event description reads: 'Der Buchhalter greift jeden Montag auf den Computer zu, um die Ausgaben der letzten Woche zu überprüfen.' Below the description, it shows the time '08:00 - 12:30 7. Juni 2021' and a note: 'Erzwingen Sie die Trennung der Sitzung, wenn der Terminplan endet, und benachrichtigen Sie den Benutzer 5 Minuten im Voraus.' There are dropdown menus for 'Gruppen' (0) and 'Benutzer' (1). At the bottom of the event card, there are buttons for 'Bearbeiten', 'Löschen', and a three-dot menu. A secondary menu is open below the three-dot menu, showing options 'Klonen' and '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 | Gruppenadministrator |
|---|------------|----------------------|
| Inaktiv Buchhaltungscomputer Ressource für eine Reihe von Computern, die von den Buchhaltern unseres Unt... | Hinzufügen | Keinen |

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

| Ressourcenname | Computer | Gruppenadministrator |
|---|------------|----------------------|
| Inaktiv Buchhaltungscomputer Ressource für eine Reihe von Computern, die von den Buchhaltern unseres Unt... | Hinzufügen | Keinen |

Terminplan Verwalten
Bearbeiten
Löschen

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

Ressource Bearbeiten

Ressourcen status: **Inaktiv** ?

1 Allgemein — 2 Computergruppenadministration — 3

Ressourcenname

Buchhaltungscomputer

Beschreibung (optional)

Ressource für eine Reihe von Computern, die von den Buchhaltern unseres Unternehmens verwendet werden.

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. Diese Seite ist nur für den **Team-Eigentümer** zugänglich.

Übersicht der Team-Einstellungen

Einstellungen

| |
|------------------------|
| Kontoübersicht |
| Team |
| Abonnements |
| Zahlung und Abrechnung |
| Zahlungshistorie |
| Code einlösen |

| | |
|--|--|
| Splashtop Enterprise Einstellungen - 5 gleichzeitige Techniker und 20 Benutzer | |
| Teamname | <input type="text" value="s team"/> (ändern) |
| Computer | 16 von 1200 Computern bereitgestellt (ändern) |
| Verwaltung | <ul style="list-style-type: none"><input checked="" type="checkbox"/> Dateübertragung aktivieren<input checked="" type="checkbox"/> Remotedruck aktivieren<input checked="" type="checkbox"/> Aktivieren Sie die Geräteumleitung (detaillierte Einrichtung)<input checked="" type="checkbox"/> Aktivieren Sie den Umleitungsmikrofoneingang<input checked="" type="checkbox"/> Aktivieren Sie das Kopieren und Einfügen von Text<input checked="" type="checkbox"/> Remoteaktivierung aktivieren<input checked="" type="checkbox"/> Remoteneustart aktivieren<input checked="" type="checkbox"/> Chat aktivieren (vor der Sitzung).<input checked="" type="checkbox"/> Aktivieren Sie die Sitzungsaufzeichnung (unbetreuter zugriff) (detaillierte Einrichtung)<input checked="" type="checkbox"/> Aktivieren Sie die Sitzungsaufzeichnung (betreuter zugriff) (detaillierte Einrichtung)<input checked="" type="checkbox"/> Aktivieren Sie die Freigabe meines Desktops (unbetreuter zugriff)<input checked="" type="checkbox"/> Aktivieren Sie die Freigabe meines Desktops (betreuter zugriff)<input checked="" type="checkbox"/> Gleichzeitige Remote-Sitzungen aktivieren (unbetreuter zugriff)<input checked="" type="checkbox"/> Gleichzeitige Remote-Sitzungen aktivieren (betreuter zugriff)<input checked="" type="checkbox"/> Remotebefehl aktivieren<input checked="" type="checkbox"/> Aktivieren Sie 1-to-Many-Scripting für <input type="text" value="nur Teambesitzer"/><input checked="" type="checkbox"/> Gruppenspezifische Adminrolle aktivieren (weitere infos)<input checked="" type="checkbox"/> Aktivieren Sie die Anzeige des aktuell angemeldeten Benutzers<input type="checkbox"/> Erlauben Sie Mitgliedern den Zugriff auf die Registerkarte Management.<input type="checkbox"/> Erlauben Sie Mitgliedern, Gruppen zu sehen<input checked="" type="checkbox"/> Benutzern erlauben, Windows/Mac-Anmeldedaten zu speichern (diese werden beim Starten einer Sitzung eingegeben)<input checked="" type="checkbox"/> Benutzern erlauben, Sicherheitscode zu speichern (dieser wird beim Starten einer Sitzung eingegeben)<input type="checkbox"/> Mitgliedern erlauben, auf Computer mit laufenden Sitzungen zuzugreifen.<input type="checkbox"/> Ermöglichen Sie Mitgliedern, gleichzeitige Sitzungen einzurichten<input type="checkbox"/> Ermöglichen Sie Mitgliedern, die Sitzungen anderer zu trennen<input type="checkbox"/> Ermöglichen Sie Mitgliedern, Computer neu zu starten und Streamer neu zu starten. |

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.

Verwaltung: Diese Kontrollkästchen steuern die Funktionsfähigkeiten, Sichtbarkeitsoptionen und Sicherheitsprotokolle des Teams. Die meisten Einstellungen gelten global - sie werden für alle Benutzer des Teams aktiviert/deaktiviert, unabhängig von der Rolle. Einige Einstellungen sind rollenbasiert, einschließlich:

- Erlauben Sie gleichzeitige Remote-Sitzungen (zwei Benutzer an einem Computer)
 - Erlauben Sie Mitgliedern, sich mit Computern in einer aktiven Verbindung zu verbinden
- Erlauben Sie Mitgliedern den Zugriff auf die Registerkarte "Verwaltung"

- Erlauben Sie Mitgliedern, Gruppen zu sehen (nur Gruppennamen von Computern, auf die sie Zugriff haben)
- Erlauben Sie Mitgliedern, gleichzeitige Sitzungen einzurichten (Verbindung zu mehreren Computern)
- Erlauben Sie Mitgliedern, die Verbindung zu anderen Sitzungen zu trennen
- Aktivieren Sie den Fernneustart (normaler Neustart, Neustart des Streamers, Neustart im sicheren Modus)
 - Erlauben Sie Mitgliedern, Computer neu zu starten und Streamer neu zu starten

Geplanter Zugriff (GMT-08:00) Pacific Time (US & Canada) (ändern)

Benachrichtigung [Benachrichtigungs-E-Mails einrichten](#)

Zweistufige Verifizierung [Vertrauenswürdige Geräte verwalten](#)
 Erlauben Sie Benutzern, Geräten zu vertrauen
 Verlangen Sie von den Administratoren, eine zweistufige Verifizierung zu verwenden.
 Verlangen Sie von den Mitgliedern, eine zweistufige Verifizierung zu verwenden.

Geräteauthentifizierung Senden Sie den Geräte-Authentifizierungs-Link per E-Mail an

Browser-Authentifizierung Senden Sie den Geräte-Authentifizierungs-Link per E-Mail an

Endpunktsicherheit Benachrichtigen Sie Computerbedrohungen per E-Mail an

Browser-Timeout Melden Sie Benutzer im Leerlauf von der Webkonsole ab ⓘ

Integration von Drittanbietern [Richten Sie API-Schlüssel ein](#)

Single Sign On

| Standardmäßig (zurücksetzen) | Status | SSO-Name | IDP Type | Protokoll | Geräteauthentifizierung | die Einstellungen | CSV-Import (Weitere Infos) |
|----------------------------------|-------------------------------------|----------------------|----------|-----------|--------------------------|-------------------|----------------------------|
| <input checked="" type="radio"/> | <input checked="" type="checkbox"/> | <input type="text"/> | ADFS | SAML 2.0 | <input type="checkbox"/> | | |

[Beantragen Sie eine neue SSO-Methode](#) ([Anweisungen anzeigen](#))

SCIM-Bereitstellungstoken ([Richten Sie ein API-Token ein](#))

Zugriff auf den Zeitplan: Stellen Sie die Zeitzone für das Zeitplanungsmodul ein.

Sitzungsindikator: Konfigurieren Sie ein [permanentes Banner](#), das während Remote-Sitzungen angezeigt wird, um Endbenutzer darüber zu informieren, dass auf den Computer zugegriffen wird.

Benachrichtigung: Richten Sie E-Mail-Benachrichtigungen für bestimmte Aktionen im Team ein, z. B. wenn ein Computer hinzugefügt wird, wenn eine Verbindung initiiert wird, wenn ein Benutzer die Team-Einladung annimmt usw.

Zwei-Schritt-Verifizierung: Zwingen Sie Administratoren und/oder Mitglieder zur Verwendung der [Zwei-Schritt-Verifizierung](#) (2FA).

Geräte-/Browserauthentifizierung: Legen Sie fest, wer [Geräteauthentifizierung](#)-Links für neue Business-App- oder Webkonsolen-Anmeldungen erhält. Die E-Mail-Authentifizierung kann deaktiviert werden, wenn ein Benutzer die 2FA bereits aktiviert hat.

Integration von Drittanbietern: Wenn Sie über Technikerlizenzen für Splashtop SOS verfügen, können Sie [API-Schlüssel einrichten](#) , um Splashtop SOS mit Ihrer bestehenden ServiceNow-, Zendesk-, Freshservice-, Freshdesk- und/oder Jira-Helpdesk-Lösung zu integrieren.

Single Sign-On: Hier können Sie SSO-Methoden anwenden und verwalten.

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
- Ferndruck
- Beaufsichtigter Zugang (Technikerlizenz)
- 1-to-Many (Technikerlizenz)

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 erlauben möchten, bei der Verwaltung der granularen Steuerelemente zu helfen.

| Granulare Standardeinstellungen | Admin | Mitglied | Konfigurierbar durch Admin |
|---------------------------------|-------------------------------------|-------------------------------------|----------------------------|
| Betreuer Zugriff | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Datei übertragung | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Remote print | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Kopieren einfügen | <input checked="" type="checkbox"/> | <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.

| | Rolle | Splash-Top-Konto | Anzeigenname | Status | Granulare Kontrolle | Granulare Kontrolle Zugriffsberechtigung |
|--------------------------|-------|------------------|--------------|-----------|---------------------|--|
| <input type="checkbox"/> | Admin | | | Aktiviert | | |

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.



Granulare Kontrolle

| | Status |
|-------------------|---------------|
| Betreuer Zugriff | Ein |
| Datei übertragung | Aus |
| Remote print | Standardmäßig |
| Kopieren einfügen | Ein |

- 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. Remote-Computerverwaltung (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.

Ereignisprotokolle anzeigen:

Ereignisebene: Critical Error Warning Information

Ereignistyp: System Application Security Setup

von : zu :

Fügen Sie detaillierte Informationen hinzu: Ja Nein

Ereignis-ID-Filter: ⓘ

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

Computerbestand - 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 das Inventar aller Computer exportieren, indem Sie unten auf der Seite **Verwaltung -> Alle Computer** auf die Option **Exportieren** klicken oder sich alle unter **Verwaltung -> Inventar** ansehen.

Zeigt das Systeminventar von an:

Schnappschüsse an für

Schnappschuss vergleichen und

Changelog anzeigen von zu

Der Schnappschuss für 2021-05-28 wurde am 2021-05-28 03:19:06 -0700 aktualisiert. (Aktualisieren des heutigen Inventars)

| | 2021-05-27 | 2021-05-28 |
|------------|---|---|
| Software 1 | Name: Adobe Acrobat Reader DC Vendor: Adobe Systems Incorporated | Name: Adobe Acrobat Reader DC Vendor: Adobe Systems Incorporated |

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

Endpunkt-Sicherheit

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

Actions Gruppenansicht Alle Gruppen

Megan's Computers 3

| Status | Computername | Software | Schutz | Letzte Scanzzeit | Bedrohungen | Details |
|--------------------------|--------------|---|-----------|---------------------|-------------|---------|
| <input type="checkbox"/> | [red X] | Bitdefender Endpoint Security Tools Antimalware | Aktiviert | 2021-05-22 07:00:00 | 54 | |

Scan-Aufgabe: N/A

[Alle Bedrohungen bestätigen](#)

| Name der Bedrohung | Erkannter Zeitstempel | Objektname | Aktion | Anerkannt |
|-----------------------------------|---------------------------|------------|---------|----------------------------|
| Gen.Illusion.ML.Skyline.B.2010101 | 2021-02-13 10:31:10 -0800 | [redacted] | REMOVED | Bestätigen |
| Gen.Illusion.ML.Skyline.B.2010101 | 2021-02-12 14:00:00 -0800 | [redacted] | | Bestätigen |

[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.

Actions Computeransicht

| Status aktualisieren | Computername | Gruppe | OS | Wichtig | Optional | Update-Richtlinie | Letzte Aktualisierung | Details |
|--------------------------|---------------------|-------------------------|--|---------|----------|--|----------------------------|---------|
| <input type="checkbox"/> | DESKTOP-P ODOP7U | [redacted] Computers | Microsoft Windows 10 Home 64-bit (10.0.19041) | 0 | 4 | Updates automatisch installieren | 2021-05-14 18:18:21 UTC | |
| <input type="checkbox"/> | laptop test | [redacted] Computers | Microsoft Windows 10 Home 64-bit (10.0.19042) | 1 | 3 | Updates automatisch installieren | 2021-05-26 06:50:54 UTC | |

Verfügbare Updates: 0 wichtig, 2 optional Nach Updates suchen Updates für andere Microsoft-Produkte einschließen
 (Letzte Überprüfung nach Updates: 2021-05-28 10:05:11 +0000)

| <input type="checkbox"/> | Code | Wichtig | Neustarten | Größe | Speichern |
|--------------------------|---------|---------|------------|-------|---|
| <input type="checkbox"/> | 4589211 | No | Yes | 3 MB | 2021-01 Update for Windows 10 Version 1909 for x64-based Systems (KB4589211) - 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 |

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.

↻

Alle Aktionen ▾

Aktionsname

🔍

+ Aktion erstellen ▾

| Name | Art der Aktion | Zugehörige Zeitpläne | Verwaltet von Gruppenadministrator |
|------|----------------|----------------------|--|
| | | | <div style="border: 1px solid #ccc; padding: 5px; background-color: #f0f0f0;"> <ul style="list-style-type: none"> Systemneustart Windows Updates Fern-Befehlszeile Batch/Ausführbare Datei Shell Script (Mac) Skript/ausführbare Datei (Mac) MSI-Datei </div> |

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.

Aktivieren Sie 1-to-Many-Scripting für nur Teambesitzer ▾

- nur Teambesitzer
- Teambesitzer und alle Administratoren

Zusätzlich können die Berechtigungen über Granulare Kontrollen konfiguriert werden.

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

Konfigurierbare Warnmeldungen

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

Name des Warnungsprofils (Aktiviert) - Warnung(en) hinzufügen

CPU-Auslastung (Aktiviert)

Name: Typ: CPU-Auslastung

Verwenden Sie diese Warnung, um die Prozessorauslastung zu überwachen. Ein Alarm wird ausgelöst, wenn die Nutzung über oder gleich dem angegebenen Wert für die angegebene Dauer liegt.

Warnt, wenn die durchschnittliche CPU-Auslastung größer oder gleich % für Minute(n) ist.

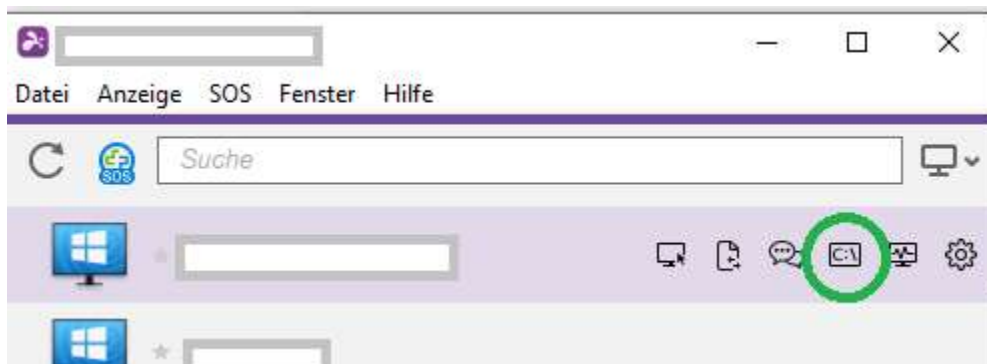
Benachrichtigen Sie auch per E-Mail für Warnung Bestätigung Wiederherstellung Hängen Sie auch den Verbindungslink in der E-Mail an.

- CPU-Auslastung
- Speicherauslastung
- Festplattenspeicher
- Computer Online
- Computer Offline
- Software installiert
- Software deinstalliert
- Windows Update
- Verfügbare Updates
- Windows-Ereignisprotokoll

[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.

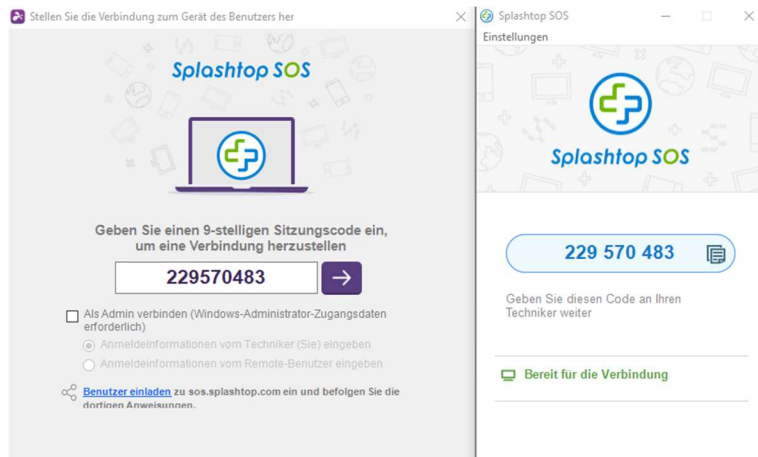


Diese Funktion ist für alle Benutzer des Teams verfügbar, wenn sie aktiviert ist, und erfordert die Eingabe der Administrator-Anmeldedaten des Remote-Computers, um darauf zuzugreifen.

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

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 granularen Einstellungen, wer den beaufsichtigten Zugang verwenden kann. Der Team-Verantwortliche kann die Standardberechtigung für den beaufsichtigten Zugang pro Benutzerrolle unter **Verwaltung -> Einstellungen** konfigurieren. Dies bestimmt die Standardberechtigung eines Benutzers für den beaufsichtigten Zugang, wenn er in das Team eingeladen wird.

| Granulare Standardeinstellungen | Admin | Mitglied | Konfigurierbar durch Admin ? |
|---------------------------------|-------------------------------------|--------------------------|------------------------------|
| Betreuer Zugriff | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

Unter **Verwaltung -> Benutzer** können Sie auch die Berechtigung Beaufsichtigter Zugang für einzelne Benutzer oder Benutzergruppen konfigurieren.

| IT Team | Rolle | Splashtop-Konto | Anzeigenname | Status | Granulare Kontrolle |
|--------------------------|-------|-----------------|--------------|-----------|---------------------|
| <input type="checkbox"/> | Admin | | | Aktiviert | |

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**.

SOS-Personalisierung

Personalisieren Sie das Aussehen und die Einstellungen der SOS-App.

[+ SOS-App erstellen](#)

| Name | Erstellungsdatum | | |
|------------------|----------------------|---------------------------|-----|
| Test | 10.06.2021, 16:39:50 | Freigeben | ... |
| Test 2 | 15.12.2021, 18:16:12 | Freigeben | ... |
| ר'ס Test Package | 24.03.2022, 00:49:38 | Freigeben | ... |

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.

Design

[SOS-Design](#) [Service Desk-Design](#)

Symbol (nur Windows, Max. Bildgröße 2 MB, Format: ICO)

[Hochladen](#)

Titel (maximal 20 Zeichen)

Splashtop SOS

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

[Hochladen](#)

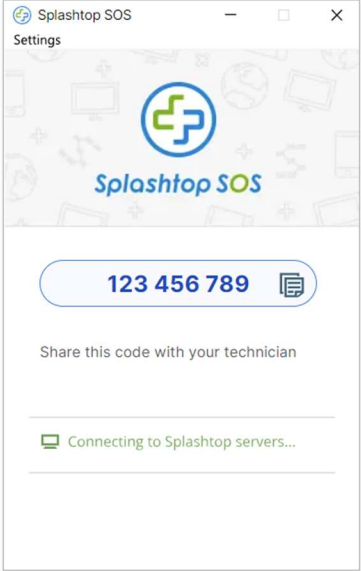
Hintergrundfarbe

9-stelliger Abschnitt

123 456 789

Anweisung Text (maximal 80 Zeichen)

Share this code with your technician



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.com](#) oder auf das Symbol in der Business-App.

The screenshot shows the Splashtop Service Desk interface. The top navigation bar includes 'Computers', 'Devices', 'Logs', 'Management', and 'Service Desk' (circled in green). The main content area displays 'Service Desk / Company ABC' and 'Company ABC' with a 'New Session' button. A table lists sessions:

| Name | Status | Time |
|--------|---------|---------------------|
| John | Waiting | 2022-04-06 05:16:28 |
| Steven | Active | 2022-03-25 17:59:16 |
| Kai | Active | 2022-04-05 18:35:16 |

A second screenshot shows the mobile app interface with the 'SOS' icon circled in green. The main content area displays 'Company ABC' and a table of sessions:

| Name | Status | Time | Technician | Device |
|--------|---------|---------------------|------------|--------|
| Kai | Active | 2022-04-05 11:35:16 | (You) | M |
| Steven | Active | 2022-03-25 10:59:16 | (You) | D |
| John | Waiting | 2022-04-05 22:16:28 | (You) | |

Erstellen Sie Kanäle innerhalb der Service-Desk-Konsole und weisen Sie Techniker zu. Techniker können Support-Sitzungen für Kunden über einen Einladungslink oder 6-stelligen Code erstellen oder eine [SOS Call](#)-App für Kunden bereitstellen, wenn sie Support benötigen. Sobald eine Supportsession erstellt wurde, können Techniker andere Techniker der Sitzung neu zuweisen, andere Techniker transferieren oder zur Sitzung einladen.

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.

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

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

15. Zusätzliche Eigenschaften:

Diese zusätzlichen erweiterten Funktionen sind für Splashtop Enterprise verfügbar.
[Kontaktieren Sie Splashtop Sales](#) für weitere Informationen.

IP-Beschränkung

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

Business App IP/Netzwerk Whitelist

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

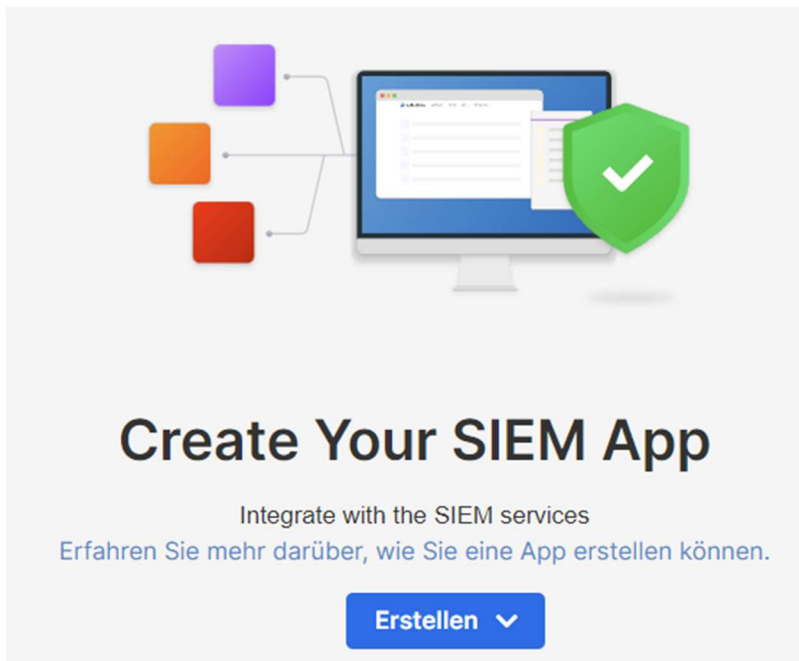
z. B. 168.168.168.168, 168.168.168.0/24



[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 graphic features a central computer monitor displaying a dashboard with various charts and data points. To the left of the monitor are three colored squares (purple, orange, and red) connected to the screen by thin lines. To the right of the monitor is a green shield with a white checkmark inside. Below the monitor, the text "Create Your SIEM App" is written in a large, bold, black font. Underneath this, in a smaller font, it says "Integrate with the SIEM services" and "Erfahren Sie mehr darüber, wie Sie eine App erstellen können." At the bottom center, there is a blue button with the text "Erstellen" and a small downward-pointing arrow.

Create Your SIEM App

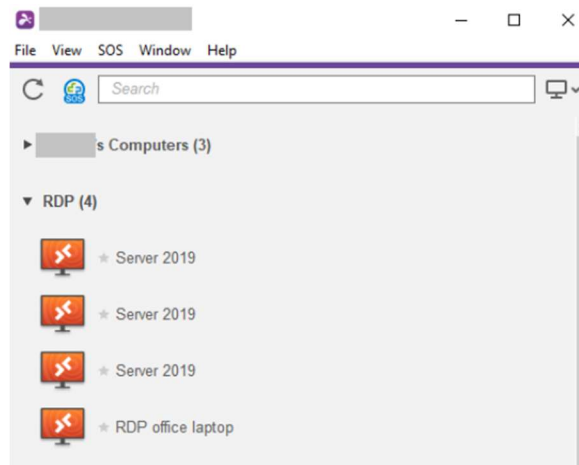
Integrate with the SIEM services
Erfahren Sie mehr darüber, wie Sie eine App erstellen können.

Erstellen ▾

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

SPLASHTOP CONNECTOR

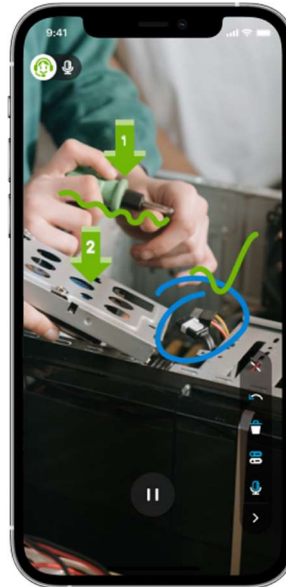
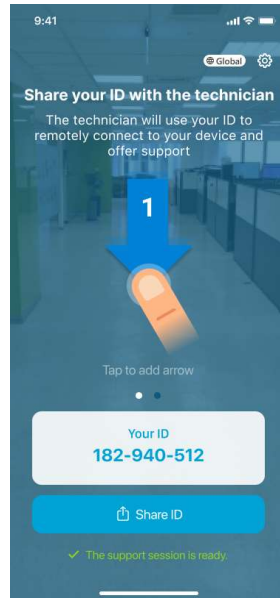
Überbrücken Sie RDP-Verbindungen zu Windows-Computern und -Servern sicher über Splashtop, ohne VPN zu verwenden oder Software auf jedem Computer installieren zu müssen.



[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.](#)