



BeyondTrust

Remote Support 23.2

Web-Konsole des Support-Technikers

Inhaltsverzeichnis

Handbuch für die Web-Konsole des Support-Technikers	4
Anforderungen für die Web-Konsole des Support-Technikers	5
Web-Konsole des Support-Technikers starten	6
Starten der Web-Konsole des Support-Technikers mit /console	6
Starten der Web-Konsole des Support-Technikers mit /login	6
Web-Konsole des Support-Technikers-Einstellungen	8
Direkte Anmeldung in der Web-Konsole des Support-Technikers über SAML	8
Authentifizierung an der Web-Konsole des Support-Technikers über die Client-Skripting-API	10
Beitreten einer Sitzung als externer Support-Techniker über die Web-Konsole des Support-Technikers	11
Desktop-Konsole des Support-Technikers über die Web-Konsole des Support-Technikers herunterladen	12
Über die Web-Konsole des Support-Technikers die in der Warteschlange befindlichen Support-Sitzungen Tech anzeigen	13
Starten einer neuen Sitzung mit einem Sitzungsschlüssel in der Web-Konsole des Support-Technikers	14
Verwenden von Jump-Elementen zum Bereitstellen von Support für Systeme in der Web-Konsole des Support-Technikers	15
Jump-Client-Upgrade	17
Erstellen und verwenden Sie symbolische Remote-Jump-Links	18
Erstellen und verwenden Sie symbolische Remote-RDP-Links	21
Erstellen und Verwenden von symbolischen VNC-Links (Remote)	25
Erstellen und Verwenden symbolischer Shell Jump-Links	28
Anmelden im System mithilfe der Anmeldedaten-Einfügung über die Web-Konsole des Support-Technikers	31
Verwalten mehrerer Support-Sitzungen in der Web-Konsole des Support-Technikers ..	36
Support-Sitzungs-Aktionen in der Web-Konsole des Support-Technikers	37
Support-Sitzungs-Aktionen	37
Steuern des Remote-Systems mit der Bildschirmfreigabe in der Web-Konsole des Support-Technikers	39
Bildschirmfreigabe-Werkzeuge	40
Zugriff auf die Befehlsshell am Remote-System über die Web-Konsole des Support-Technikers	42

Befehlsshell-Tools	43
Verwenden der Web-Konsole des Support-Technikers zur Übertragung von Dateien zu und von Remote-Systemen	44
Werkzeuge für den Dateitransfer	46
RDP-Dateitransfer	47
Anzeige von Systeminformationen am Remote-Endpunkt	48
Werkzeuge für Systeminformationen	48
Fügen Sie über die Web-Konsole des Support-Technikers einen Support-Button hinzu	49
Einen Jump-Client über die Web-Konsole des Support-Technikers fixieren	50
Sitzung in der Web-Konsole des Support-Technikers heraufsetzen	51
Über die Web-Konsole des Support-Technikers eine Sitzung auf einen anderen Support-Techniker oder ein Team übertragen	52
Freigabe einer Sitzung für Teammitglieder oder externe Benutzer mithilfe der Web-Konsole des Support-Technikers	53
Team-Mitglieder einladen	53
Externe Benutzer einladen	54
Ein Mitglied aus einer Sitzung der Web-Konsole des Support-Technikers entfernen	57
Über die Web-Konsole des Support-Technikers mit dem Remote-Benutzer chatten	58
Sitzung in der Web-Konsole des Support-Technikers schließen	59

Handbuch für die Web-Konsole des Support-Technikers

Mit der BeyondTrust Web-Konsole des Support-Technikers kann Support für Kunden und Remote-Systeme bereitgestellt werden, auch wenn diese Support-Techniker keine Software innerhalb ihrer eigenen Desktop-Umgebungen installieren können. Stattdessen können Kunden und Remote-Systeme über die web-basierte Konsole d. Support-Technikers unterstützt werden.

In diesem Leitfaden besprechen wir, wie die browserbasierte Web-Konsole des Support-Technikers Kunden unterstützt und andere nötige Funktionen ausführt, während stets ein Höchstmaß an Sicherheit gewährleistet wird.



Hinweis: Verwenden Sie dieses Handbuch erst, wenn die anfängliche Einrichtung und Konfiguration des B Series Appliance durch einen Administrator abgeschlossen wurde, entsprechend der Beschreibung im [BeyondTrust Appliance B Series Installationshandbuch für Hardware](https://www.beyondtrust.com/docs/remote-support/getting-started/deployment/hardware-sra/index.htm) unter <https://www.beyondtrust.com/docs/remote-support/getting-started/deployment/hardware-sra/index.htm>. Sollten Sie Hilfe benötigen, wenden Sie sich bitte an [BeyondTrust Technical Support](https://www.beyondtrust.com/docs/index.htm#support) unter www.beyondtrust.com/docs/index.htm#support.

Anforderungen für die Web-Konsole des Support-Technikers

Damit die Web-Konsole des Support-Technikers auf Ihrem System ausgeführt werden kann, muss das BeyondTrust Appliance B Series mit Software-Version 16.2 oder höher ausgeführt werden. Auf der Seite **/login > Verwaltung > Sicherheit** muss die Berechtigung **Verbindung der mobilen Konsole des Support-Technikers und der Web-Konsole des Support-Technikers zulassen** aktiviert sein. Die Web-Konsole des Support-Technikers wird auf den folgenden Plattformen und Browsern unterstützt:

Plattformen

- Windows
- Mac
- Linux

Browser

- Chrome 46+
- Firefox 42+
- Internet Explorer 11+
- Safari 8+
- Windows Edge



WICHTIG!

Ihr BeyondTrust Appliance B Series muss mit einem von einer Zertifizierungsstelle signierten SSL-Zertifikat ausgestattet sein. Sobald Sie ein von einer Zertifizierungsstelle signiertes SSL-Zertifikat auf Ihrem B Series Appliance übernommen haben, wenden Sie sich an den BeyondTrust Technical Support. Ihr Support-Techniker wird einen neuen Software-Build erstellen, der Ihr SSL-Zertifikat integriert. Mit diesem aktualisierten, auf Ihrem B Series Appliance installierten Build können Sie die BeyondTrust Konsole d. Support-Technikers auf Ihrem Gerät ausführen, um von fast überall auf Ihre Endpunkte zuzugreifen.

Web-Konsole des Support-Technikers starten

Mit der Web-Konsole des Support-Technikers können Sie eine webbasierte Konsole d. Support-Technikers verwenden, um sicheren Support für Kunden bereitzustellen und auf Remote-Systeme zuzugreifen, indem Sie sich per Fernzugriff über das B Series Appliance mit ihnen verbinden. Um die <MadCap:variable name="ProductNames.WebConsole" />zur Unterstützung von Kunden zu verwenden, folgen Sie den unten beschriebenen Schritten.

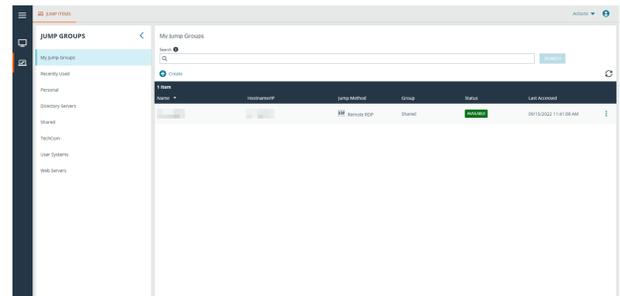


Hinweis: Support-Techniker, die ein Chrome OS-Gerät für den Support von Kunden nutzen, müssen die Web-Konsole des Support-Technikers verwenden.

Starten der Web-Konsole des Support-Technikers mit /console

Dies ist der schnellste Weg, um auf die Webkonsole zuzugreifen.

1. Geben Sie in die Adressleiste Ihres Browsers den BeyondTrust-Hostnamen Ihrer Website, gefolgt von **/console** ein, zum Beispiel **access.example.com/console**.
2. Geben Sie dann den mit Ihrem BeyondTrust Benutzerkonto verknüpften Benutzernamen und das dazugehörige Passwort ein.
3. Klicken Sie auf **Anmelden**, um Ihre webbasierte Konsole d. Support-Technikers-Sitzung zu starten.



FIDO2-zertifizierte Authentifizierer können für die sichere Anmeldung ohne Eingabe Ihres Passworts auf der Desktop-Konsole d. Support-Technikers (nur Windows), Web-Konsole des Support-Technikers und der Verwaltungsschnittstelle /login verwendet werden. Sie können bis zu 10 Authentifizierer registrieren.

Wenn die passwortlose Anmeldung aktiviert wurde, kann **Authentifizierung über** auf **Passwortlos FIDO2** voreingestellt werden oder es kann ausgewählt werden. Der genaue Ablauf der passwortlosen Anmeldung hängt von der Art des Geräts und dem Hersteller ab.

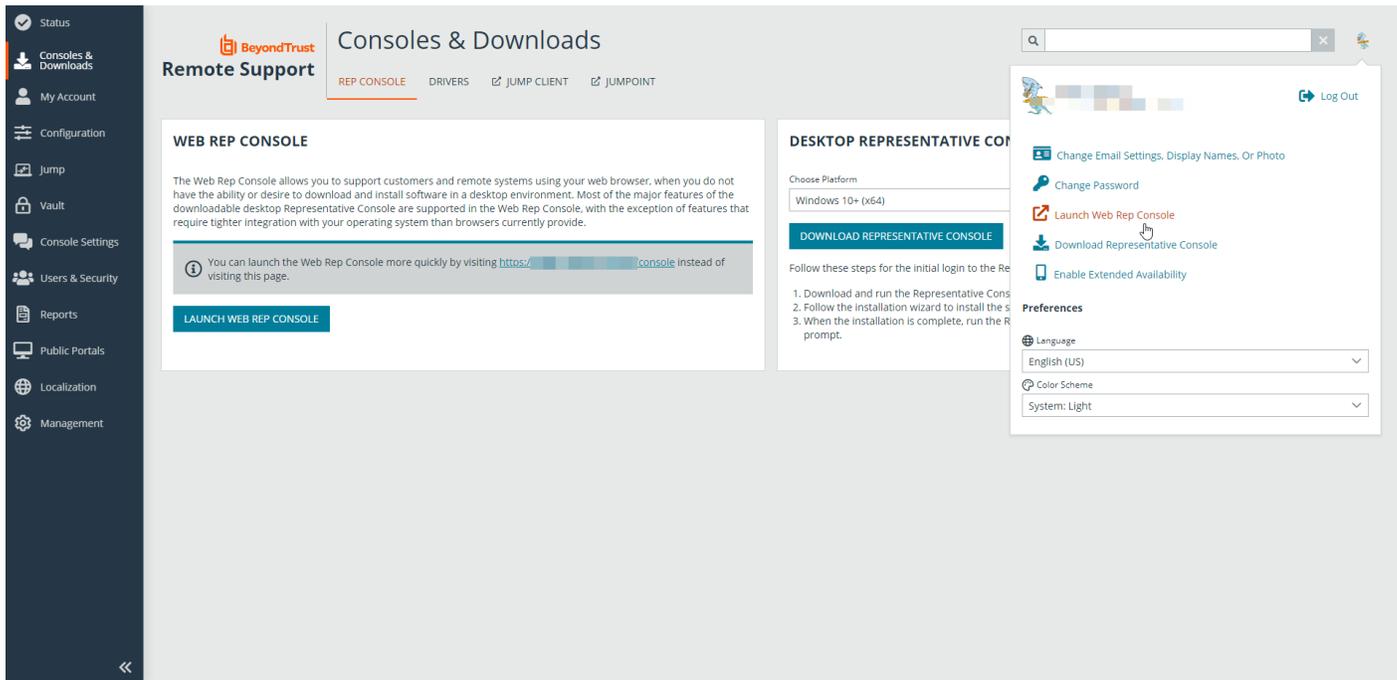
Sie können die passwortlose Anmeldung aktivieren und die Standardauthentifizierung festlegen, indem Sie sich bei der Verwaltungsschnittstelle /login anmelden, zu **Verwaltung > Sicherheit** navigieren und dann die passwortlosen Authentifizierer unter **Mein Konto > Sicherheit** registrieren.

Starten der Web-Konsole des Support-Technikers mit /login



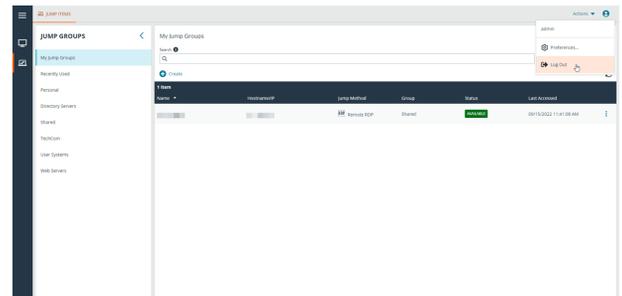
Hinweis: Standardmäßig ist diese Option nicht verfügbar. Um die Webkonsole über die Verwaltungsschnittstelle /login zu starten, müssen Sie zu **Verwaltung > Sicherheit** navigieren und **Mobiler Konsole d. Support-Technikers und Web-Konsole des Support-Technikers Verbindung gestatten** aktivieren.

1. Geben Sie in die Adressleiste Ihres Browsers den Hostnamen Ihrer BeyondTrust Website gefolgt von **/login** ein, zum Beispiel **access.example.com/login**.
2. Geben Sie dann den mit Ihrem BeyondTrust Benutzerkonto verbundenen Benutzernamen und das dazugehörige Passwort ein und klicken Sie auf **Anmelden**, oder melden Sie sich mit passwortloser Authentifizierung an.
3. Klicken Sie im linken Menü auf **Konsolen & Downloads** oder auf das Benutzersymbol in der oberen rechten Ecke des Bildschirms. In der folgenden Abbildung sind beide Optionen ausgewählt.



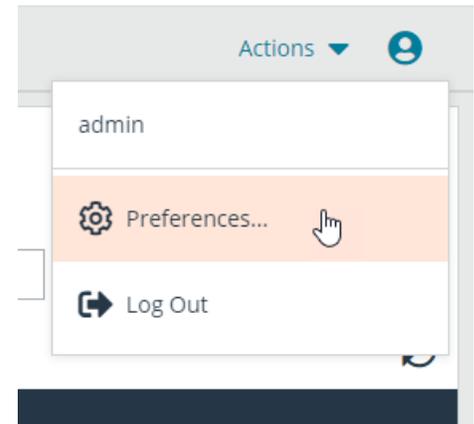
4. Klicken Sie auf **Web-Konsole des Support-Technikers starten** auf dem Bildschirm **Konsolen & Downloads** oder im Fenster mit den Benutzeroptionen.
5. Die Web-Konsole des Support-Technikers wird in einer neuen Registerkarte geöffnet und Sie können mit der Arbeit auf Endpunkten beginnen.

Um sich von der Web-Konsole des Support-Technikers abzumelden, klicken Sie auf das Benutzersymbol in der oberen rechten Ecke des Bildschirms und dann auf **Abmelden**. Hierdurch werden Sie nicht von der Verwaltungsschnittstelle /login abgemeldet. Um sich von der Verwaltungsschnittstelle /login abzumelden, klicken Sie auf das Benutzersymbol in der oberen rechten Ecke dieses Bildschirms und dann auf **Abmelden**.



Web-Konsole des Support-Technikers-Einstellungen

Die Sprach- und Farbschemaoptionen, die beim Klicken auf das Benutzersymbol in der Verwaltungsschnittstelle /login sichtbar sind, betreffen nur diese Schnittstelle. Um die Einstellungen in Web-Konsole des Support-Technikers festzulegen, klicken Sie auf das Benutzersymbol in der oberen rechten Ecke des Web-Konsole des Support-Technikers und dann auf **Einstellungen**. Wählen Sie im Pop-up-Fenster Ihre Einstellungen aus.



Wählen Sie Ihr bevorzugtes Farbschema aus. Sie können zwischen den Modi **Hell** und **Dunkel** oder **System** wechseln, bei dem der für Ihr System ausgewählte Modus verwendet wird.

Wählen Sie eine der automatischen Optionen, die Sie verwenden möchten:

- Minimiert automatisch das Bedienfeld **Sitzungswarteschlangen**, wenn eine Sitzung ausgewählt wurde.
- Minimiert automatisch das Bedienfeld **Jump-Gruppen**, wenn ein Jump Item ausgewählt wurde.
- Chat-Seitenleiste in neuen Sitzungen automatisch öffnen.
- Die in neuen Sitzungen geöffnete Chat-Seitenleiste automatisch sperren.
- Minimiert automatisch das Bedienfeld **Volumen**, wenn eine Datei in der Ansicht **Dateitransfer** ausgewählt wurde.

PREFERENCES

Color Scheme

System (Currently: Light)

Light

Dark

Automatically collapse the Session Queues panel when a session is selected.

Automatically collapse the Jump Groups panel when a Jump Item is selected.

Automatically open the chat sidebar in new sessions.

Automatically lock the chat sidebar open in new sessions.

Automatically collapse the Volumes panel when a file is selected in the File Transfer view.

CLOSE

Direkte Anmeldung in der Web-Konsole des Support-Technikers über SAML

Es ist möglich, eine Anwendung oder Kachel in einem SAML-Identitätsanbieter (IdP) zu konfigurieren (wie die für die Anmeldung in Okta und ähnlichen Anwendungen verwendeten Kacheln), der Sie direkt zur Web-Konsole des Support-Technikers anstelle zu /login leitet.

So konfigurieren Sie dies:

- Einrichten der Anwendung im IdP wie bei /login
- Ändern Sie den Parameter **RelayState** zum Wort *Konsole* (kleingeschrieben, ohne / usw.)

Die SAML-Konfiguration umfasst zwei Teile: den IdP und den Serviceanbieter (SP). In dieser Instanz sind Sie der SP, und der SAML-Service ist der IdP (OneLogin, Okta und ähnlich). Derzeit können Sie unter /login (im Abschnitt „Serviceanbieter“) Metadaten aus dem

SAML-Sicherheitsanbieter exportieren, die Sie dann in den IdP importieren können, um die Konfiguration der SAML-Seite zu unterstützen. Wenn Sie im Rahmen dieser Konfiguration den Parameter **RelayState** auf **console** setzen, werden Sie bei jeder vom IdP initiierten Anmeldung (z. B. durch Klicken auf die Kachel in Okta) zum Web-Konsole des Support-Technikers und nicht zu /login geleitet.

Authentifizierung an der Web-Konsole des Support-Technikers über die Client-Skripting-API

Mit dieser Funktion können sich Benutzer an der Web-Konsole des Support-Technikers anmelden und mithilfe der [Remote Support Client-Skripting-API](https://www.beyondtrust.com/docs/remote-support/how-to/integrations/api/client-script/index.htm) (<https://www.beyondtrust.com/docs/remote-support/how-to/integrations/api/client-script/index.htm>) einen Jump zu einem Endpunkt durchführen.

Die Client-Skripting-API-URL folgt dem Format **https://support.beispiel.com/api/client_script**, wobei support.beispiel.com der Hostname Ihres B Series Appliance ist.

Die API akzeptiert einen Client-Typ (**web_console**), eine auszuführende Operation (**execute**) und einen Befehl (**start_jump_item_session**). Keine anderen Befehle werden für den Client-Typ **web_console** unterstützt.

Wenn der Benutzer in der Desktop-Konsole d. Support-Technikers angemeldet ist, wenn die Client-Skripting-API-URL mit **type=web_console** genutzt wird, wird der Benutzer in der Web-Konsole des Support-Technikers angemeldet und von der Desktop-Konsole d. Support-Technikers getrennt. Wird dieses Verhalten nicht gewünscht, muss der Benutzer eine Client-Skripting-API-URL mit **type=rep** statt **type=web_console** verwenden.

Ähnlich gilt: Wenn der Benutzer in der Web-Konsole des Support-Technikers angemeldet ist und die API **type=rep** aufruft, wird der Benutzer in der Desktop-Konsole d. Support-Technikers angemeldet und von der Web-Konsole des Support-Technikers getrennt.

Hier ein Beispiel einer gültigen Client-Skripting-API-Anforderung:

```
https://support.beispiel.com/api/client_script?type=web_console&operation=execute&action=start_jump_item_session&search_string=ABCDEF02
```

Ist der Benutzer bereits in der Web-Konsole des Support-Technikers angemeldet, führt die obige Anforderung den Befehl in der Browser-Registerkarte aus, in der die Web-Konsole des Support-Technikers ausgeführt wird. In diesem Fall startet der Befehl eine Sitzung mit dem Jump-Client, dessen Hostname, Kommentare, öffentliche IP oder private IP mit dem Suchbegriff „ABCDEF02“ übereinstimmen.

Ist der Benutzer nicht bereits in der Web-Konsole des Support-Technikers angemeldet, öffnet die obige Anforderung eine neue Browser-Registerkarte und leitet den Benutzer zur Authentifizierung zu /login weiter (dieser Schritt wird übersprungen, wenn der Benutzer bereits in /login angemeldet ist). Der Benutzer wird dann zur Web-Konsole des Support-Technikers weitergeleitet, und der Befehl startet eine Sitzung mit dem Jump-Client, dessen Hostname, Kommentare, öffentliche IP oder private IP mit dem Suchbegriff „ABCDEF02“ übereinstimmen.

In beiden Fällen gilt: Erfüllt mehr als ein Jump-Element die Suchkriterien, muss der Benutzer das richtige Jump-Element aus einer Liste wählen. Wenn keine Jump-Elemente die Suchkriterien erfüllen, zeigt die Web-Konsole des Support-Technikers dem Benutzer einen Fehler an.

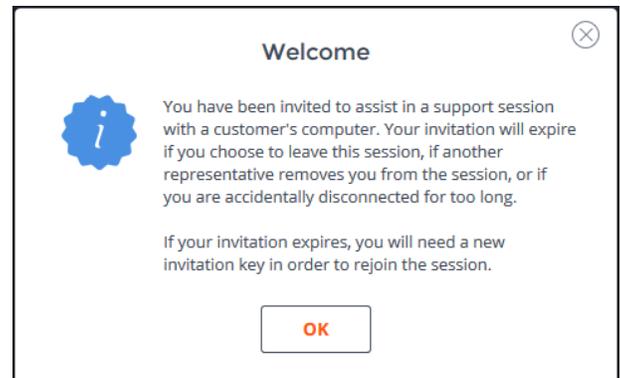
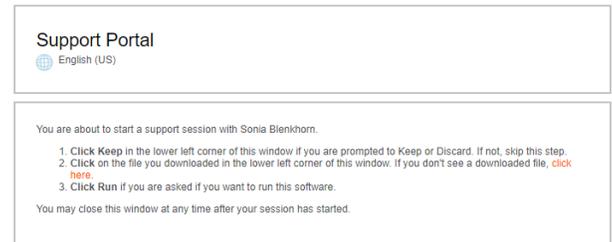
Alle der Suchkriterien für den Befehl **start_jump_item_session** werden mit **type=web_console** unterstützt, darunter:

- jump.method
- search_string
- client.hostname
- client.comments
- client.tag
- client.public_ip
- client.private_ip
- session.custom.<attribute code name>

Beitreten einer Sitzung als externer Support-Techniker über die Web-Konsole des Support-Technikers

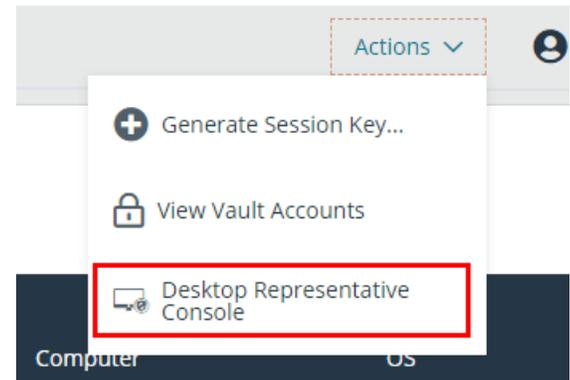
Über die native Konsole d. Support-Technikers kann ein Support-Techniker einen externen Benutzer einladen, einmalig an einer Sitzung teilzunehmen. Wenn der externe Support-Techniker auf die URL zur Einladung klickt, hat er die Option, der Sitzung mithilfe der Web-Konsole des Support-Technikers beizutreten, oder die Desktop-Konsole d. Support-Technikers herunterzuladen und zu installieren. Sobald er die Web-Konsole des Support-Technikers gewählt oder die Desktop-Konsole d. Support-Technikers installiert hat, kann er der Sitzung beitreten.

Wenn der externe Support-Techniker einer Sitzung beitrifft, wird er mit einer Willkommensnachricht begrüßt. Er hat nur Zugriff auf die Sitzung, zu die er eingeladen wurde, und verfügt über einen beschränkten Berechtigungssatz. Der eingeladene Benutzer kann nie der Eigentümer der Sitzung sein. Wenn der einladende Support-Techniker die Sitzung verlässt, ohne dass ein anderer Sitzungseigentümer anwesend ist, wird der externe Support-Techniker abgemeldet.



Desktop-Konsole des Support-Technikers über die Web-Konsole des Support-Technikers herunterladen

Bei der Arbeit in der Web-Konsole des Support-Technikers können Sie jederzeit die native Desktop-Konsole d. Support-Technikers auf Ihren Computer herunterladen. Klicken Sie auf den Menüpunkt **Desktop-Konsole des Support-Technikers** im Menü **Aktionen** oben rechts auf dem Bildschirm.



Hinweis: Support-Techniker mit Chrome OS-Geräten können die Desktop-Konsole des Support-Technikers nicht herunterladen und verwenden.

Wenn Sie die Desktop-Konsole d. Support-Technikers bereits installiert haben, führen Sie das Skript für die BeyondTrust Konsole d. Support-Technikers aus und melden Sie sich an der Konsole d. Support-Technikers an. Jegliche in der Web-Konsole des Support-Technikers aktive Sitzungen werden in der Desktop-Konsole d. Support-Technikers geöffnet. Sie werden automatisch von der Web-Konsole des Support-Technikers abgemeldet.

Wenn Sie die Desktop-Konsole d. Support-Technikers nicht bereits installiert haben, müssen Sie zunächst dem Link zur Seite **Mein Konto** folgen, um die Desktop-Konsole d. Support-Technikers herunterzuladen und zu installieren. Dann können Sie die BRCS-Datei ausführen.



Hinweis: Auf einem Linux-System müssen Sie die Datei auf Ihrem Computer speichern und nach dem Herunterladen am Speicherort öffnen. Verwenden Sie nicht den Link **Öffnen**, der nach dem Herunterladen der Datei bei einigen Browsern angezeigt wird.

RUN REPRESENTATIVE CONSOLE

1. If you have not already, download & install the Representative Console for your platform from your [My Account](#) page.
2. A file with a ".brcs-techcomm_ers" extension should download in your browser momentarily. [If not, click here.](#)
3. Open the ".brcs-techcomm_ers" file to launch the desktop Representative Console.

DISMISS

Über die Web-Konsole des Support-Technikers die in der Warteschlange befindlichen Support-Sitzungen Tech anzeigen

Warteschlangen

Sitzungswarteschlangen enthalten Informationen über bzw. Zugriff auf Kunden, die auf Support warten. Die Warteschlange **Persönlich** enthält Kunden, denen Sie zurzeit helfen oder die speziell auf eine Sitzung mit Ihnen warten. Eine wartende Sitzung erscheint in Ihrer persönlichen Warteschlange, wenn Sie Ihnen übertragen wurde, oder vom Kunden durch Eingabe eines von Ihnen erstellten Sitzungsschlüssels, durch Auswahl Ihres Namens auf der öffentlichen Website bzw. durch Anklicken eines mit Ihnen verknüpften Support-Buttons gestartet wurde. Die Warteschlange enthält auch Einladungen zum Beitritt einer freigegebenen Sitzung.

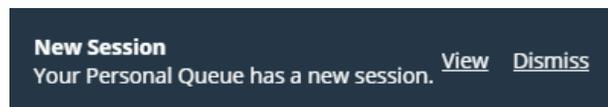


Sie haben auch Warteschlangen für Teams, denen Sie angehören. Leitet ein Kunde eine Sitzung durch Auswählen eines Problemtyps aus einem Kontaktformular für Problemfälle ein, wird dieser Kunde dem Problem gemäß in eine spezifische, einem Team zugehörige Warteschlange eingereiht. Ein Kunde wird auch in eine Teamwarteschlange eingereiht, wenn er auf einen mit einem Team verknüpften **Support-Button** klickt. Eine Sitzung kann auch in eine Warteschlange eingereiht werden, wenn sie absichtlich weitergeleitet wurde, aufgrund von Regeln für wartende Sitzungen, oder wenn die Verbindung mit dem Support-Techniker während einer Sitzung unterbrochen wird. Diese Warteschlangen enthalten auch Einladungen an alle Support-Techniker eines Teams, einer freigegebenen Sitzung beizutreten.

Klicken Sie auf den Stern links neben einem Teamnamen, um diese Warteschlange als Favorit zu markieren. Wenn eine Team-Chatnachricht gesandt wird, erscheint eine orange Chatblase statt des Sterns.

Kunden können ebenfalls direkt Hilfestellung über eine Website anfordern, die einen Hilfe-Link enthält. Damit wird eine Browserfreigabe-Sitzung eingeleitet, die es einem Support-Techniker ermöglicht, mit einem Kunden zu chatten und seine Website anzuzeigen. Administratoren können benutzerdefinierte Links generieren, um Browser-Sitzungen an die richtige Support-Techniker- bzw. Team-Warteschlange weiterzuleiten. In der Warteschlange werden Browserfreigabe-Sitzungen durch das Präfix **[Browser]** neben dem Kundennamen gekennzeichnet.

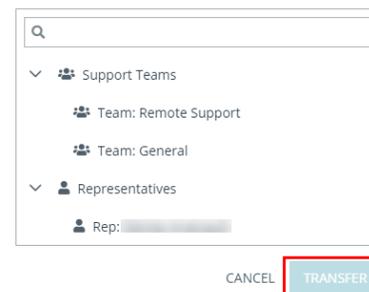
Wenn eine neue Sitzung in eine Ihrer Warteschlangen eingereiht wird, erscheint außerdem eine Popup-Benachrichtigung in der linken unteren Ecke Ihres Bildschirms. Sie können auf die Schaltfläche **Anzeigen** klicken, um die Details der Sitzungen in der Warteschlange anzuzeigen.



Klicken Sie auf einen Warteschlangennamen, um deren Sitzungen anzuzeigen. Klicken Sie auf einen Sitzungseintrag, um Details zur Support-Anfrage anzuzeigen. Um mit dem Support für die gewünschte Sitzung zu beginnen, klicken Sie auf die Schaltfläche **Akzeptieren**. Wenn Sie eine Sitzung akzeptieren, wechselt Ihre Ansicht zur Sitzungsansicht. Sie können mehrere Sitzungen gleichzeitig ausführen.

Alternativ können Sie eine Sitzung in eine andere Warteschlange übertragen. Klicken Sie auf die Schaltfläche **Übertragen**. Wählen Sie **Support-Teams** oder **Support-Techniker**. Wählen Sie die Warteschlange, in die Sie die Sitzung verschieben möchten, und klicken Sie auf die orange Schaltfläche **ÜBERTRAGEN**.

TRANSFER SESSION



Starten einer neuen Sitzung mit einem Sitzungsschlüssel in der Web-Konsole des Support-Technikers

Eine Methode zum Starten einer Support-Sitzung Tech besteht darin, Ihrem Kunden einen einmaligen, zufällig generierten Sitzungsschlüssel auf Ihrer öffentlichen Website zur Verfügung zu stellen. Abhängig von Ihren Kontoberechtigungen können Sie Sitzungsschlüssel zu diesem Zweck generieren. Klicken Sie auf die Schaltfläche **Sitzungsschlüssel erstellen** oben rechts auf dem Bildschirm. Damit wird ein Menü geöffnet, über das Sie die Einzelheiten zum Sitzungsschlüssel bearbeiten können.

 **Generate Session Key...**

Legen Sie fest, wie lange dieser Sitzungsschlüssel gültig sein soll. Die Ablaufzeit gilt nur für die Zeit, die der Schlüssel zum Starten einer Sitzung verwendet werden kann, und wirkt sich nicht auf die Länge der Sitzung selbst aus.

Sie können auch das öffentliche Portal auswählen, durch das Ihr Kunde der Sitzung beitreten kann.

Weisen Sie Ihren Kunden an, entweder zur eindeutigen URL zu wechseln oder den Sitzungsschlüssel auf Ihrer öffentlichen Website einzugeben. Klicken Sie auf den Sitzungsschlüssel oder die URL, um sie in Ihre Zwischenablage zu kopieren.

Außerdem können Sie Ihrem Kunden eine E-Mail-Einladung senden, die eine einzigartige URL enthält.

Nachdem der Kunden-Client ausgeführt wurde, wird Ihr Kunde in Ihrer persönlichen Warteschlange angezeigt.

SUPPORT SESSION KEY

You may start a support session with a customer by directing them to enter the following session key on your Support Portal, by sending them directly to the following URL, or by emailing an invitation.

Session Key

URL

Expires in

 
August 26, 2021, 10:00:03 AM

Public Portal

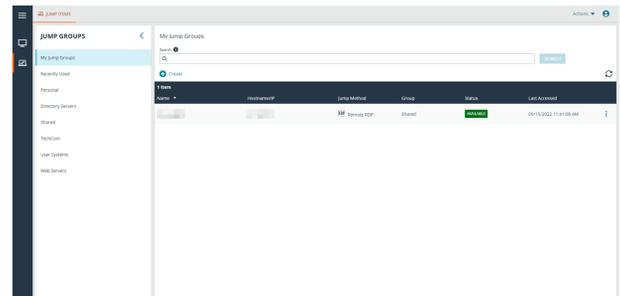
 

[CLOSE](#) [SEND LOCAL EMAIL](#)

Verwenden von Jump-Elementen zum Bereitstellen von Support für Systeme in der Web-Konsole des Support-Technikers

Die Jump-Technologie von BeyondTrust ermöglicht berechtigten Benutzern, eine Verbindung mit einem unüberwachten Remote-System herzustellen und eine Sitzung zu beginnen, ohne dass der Endbenutzer dabei mithilft.

Jump-Items können über die Seite **Jump-Clients** der /login-Schnittstelle oder über die Konsole d. Support-Technikers installiert werden. Einige Typen von Jump-Items können in Web-Konsole des Support-Technikers erstellt werden. Um ein Jump Item in Web-Konsole des Support-Technikers zu erstellen, klicken Sie auf **Erstellen** oben in der Jump-Schnittstelle. Die vollständigen Einzelheiten, wie man verschiedene Jump-Items erstellt, finden Sie weiter hinten in diesem Handbuch.



Hinweis: Ihre Kontoeinstellungen bestimmen, welche Jump-Element-Berechtigungen Sie haben, darunter auch, auf welche Jump-Gruppen Sie zugreifen können und welche Arten von Jump-Elementen Sie nutzen können.

Jump-Elemente werden in Jump-Gruppen aufgeführt. Wenn Sie einer oder mehr Jump-Gruppen zugewiesen werden, können Sie auf die Jump-Elemente in diesen Gruppen zuweisen, wobei die Berechtigungen von Ihrem Administrator festgelegt werden.

Ihre persönliche Liste von Jump-Elementen ist hauptsächlich zu Ihrer persönlichen Verwendung gedacht, obwohl Ihre Teamleiter, Team-Manager und zur Ansicht aller Jump-Elemente berechnete Benutzer ebenfalls auf Ihre persönliche Liste von Jump-Elementen zugreifen können. Wenn Sie ein Team-Manager oder -leiter mit den geeigneten Berechtigungen sind, können Sie entsprechend die persönlichen Listen von Jump-Elementen Ihrer Teammitglieder sehen. Außerdem sind Sie möglicherweise berechtigt, auf Jump-Elementen in Jump-Gruppen zuzugreifen, denen Sie nicht angehören, und auf persönliche Jump-Elemente von Personen, die keine Teammitglieder sind.

Um mehr Einzelheiten über ein Jump Item anzuzeigen oder um ein Jump-Item zu kopieren oder zu bearbeiten, klicken Sie auf die vertikale Ellipse am rechten Ende der Zeile des Jump-Items. Klicken Sie auf die **Jump**-Startfläche rechts neben dem Jump-Element-Eintrag, um eine Sitzung mit dem Jump-Element zu starten.



Hinweis: Die Liste **Häufig verwendete Jump-Elemente** zeigt alle Jump-Elemente an, auf die Sie regelmäßig zugreifen. Um eine Sitzung mit einem häufig verwendeten System zu starten, fahren Sie mit der Maus über das Element und klicken Sie auf **Sitzung starten**.



Hinweis: Die Liste der Jump-Items kann nur maximal 50 Jump-Items anzeigen.

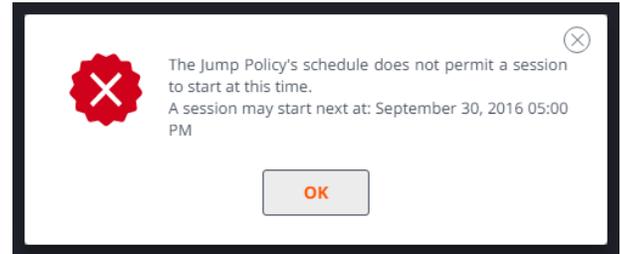


Hinweis: Falls Sie auf Jump-Elemente zugreifen müssen, wenn kein Benutzer verfügbar ist, müssen Sie gewährleisten, dass die Sitzungsberechtigungen entweder so festgelegt sind, dass die Aufforderung deaktiviert wird, oder die Standardeinstellung für unüberwachte Sitzungen **Zulassen** lautet.

Wenn eine Jump-Richtlinie einen Zeitplan für dieses Jump-Element erzwingt, verhindert ein Versuch, außerhalb des gestatteten Zeitplans auf das Jump-Element zuzugreifen den Jump. Eine Aufforderung informiert Sie über die Richtlinieneinschränkungen und gibt Datum und Uhrzeit an, wann wieder auf dieses Jump-Element zugegriffen werden kann.

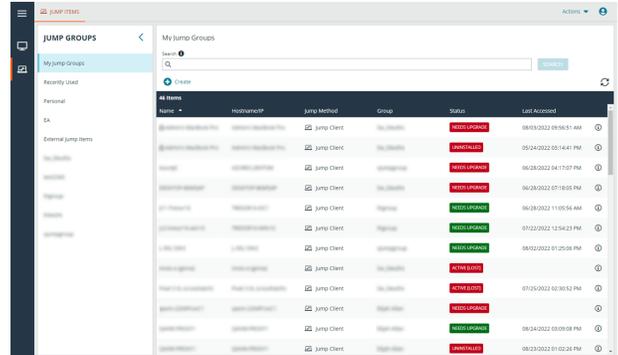


Hinweis: Wenn Sie zur Änderung von Jump-Richtlinien berechtigt sind, gibt Ihnen die Eingabeaufforderung die Option, den Zeitplan außer Kraft zu setzen und dennoch eine Sitzung zu starten.



Jump-Client-Upgrade

Sie können die Jump-Clients in Web-Konsole des Support-Technikers aktualisieren. Ein **Benötigt Upgrade**-Banner wird unter **Status** angezeigt, grün, wenn der Jump-Client online ist, rot, wenn er offline ist. Sie können nur Jump-Clients aktualisieren, die online sind. Um einen bestimmten Jump-Client zu aktualisieren, klicken Sie auf das grüne Banner.



Name	hostnameIP	Jump Method	Group	Status	Last Account
...	...	Jump Client	...	NEEDS UPGRADE	08/03/2022 08:56:51 AM
...	...	Jump Client	...	NEEDS UPGRADE	05/24/2022 03:14:41 PM
...	...	Jump Client	...	NEEDS UPGRADE	06/28/2022 04:17:07 PM
...	...	Jump Client	...	NEEDS UPGRADE	06/28/2022 07:18:05 PM
...	...	Jump Client	...	NEEDS UPGRADE	06/28/2022 11:05:58 AM
...	...	Jump Client	...	NEEDS UPGRADE	07/22/2022 12:54:23 PM
...	...	Jump Client	...	NEEDS UPGRADE	08/03/2022 01:25:08 PM
...	...	Jump Client	...	NEEDS UPGRADE	07/25/2022 02:30:52 PM
...	...	Jump Client	...	NEEDS UPGRADE	08/24/2022 03:09:08 PM
...	...	Jump Client	...	NEEDS UPGRADE	08/23/2022 01:02:28 PM

Um Jump-Clients via Web-Konsole des Support-Technikers aktualisieren zu können, müssen Sie zunächst sicherstellen, dass **Automatische Jump-Client-Upgrades** in /login deaktiviert ist. Um dies zu tun, gehen Sie zu **/login > Jump > Jump-Clients > Upgrades** und deaktivieren Sie **Automatische Jump-Client-Upgrades**. Wenn das automatische Aktualisieren nicht deaktiviert ist, zeigen Jump-Clients, die aktualisiert werden müssen, stattdessen ein **Upgrade ausstehend**-Banner an.



UPGRADE

Maximum bandwidth of concurrent jump client upgrades: 10 MB/s

Maximum number of concurrent jump client upgrades: 50

Automatic Jump Client Upgrades

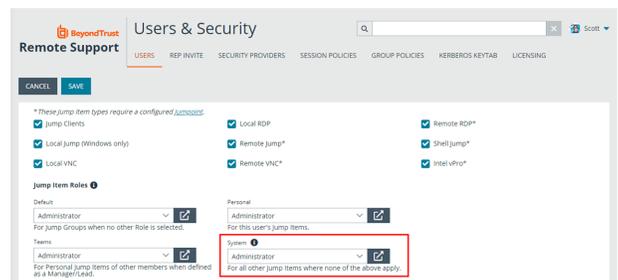
Disabled

Enabled for this version only

Enabled always

SAVE

Der Support-Techniker muss auch das Recht haben, das Update auszuführen. Dies kann in **/login > Benutzer & Sicherheit > Benutzer > Zugriffsberechtigungen > Jump-Item-Rollen** eingestellt werden. Stellen Sie sicher, dass **System** auch auf **Administrator** eingestellt ist.



Jump Item Roles

Default: Administrator

For Jump Groups when no other Role is selected: Administrator

For Personal jump items where none of the above apply: **System**

For all other jump items where none of the above apply: Administrator

Erstellen und verwenden Sie symbolische Remote-Jump-Links

Remote-Jump ermöglicht es einem berechtigten Benutzer, sich mit einem unüberwachten Remote-Computer in einem Netzwerk außerhalb des eigenen Netzwerkes zu verbinden. Remote-Jump ist von einem Jumpoint abhängig.

Ein Jumpoint agiert als Leitstelle für den Zugriff auf Computer in einem bekannten Remote-Netzwerk. Ein einziger auf einem Computer in einem LAN installierter Jumpoint wird zum Zugriff auf mehrere Systeme verwendet. So ist es nicht mehr notwendig, Software auf jedem Computer vorzuinstallieren, auf den Sie möglicherweise zugreifen müssen.



Hinweis: Remote- und lokale Jumps sind nur für Windows-Systeme verfügbar. Jump-Clients sind notwendig, um Remote-Zugriff auf Mac-Computer zu ermöglichen. Um ohne Jump-Client einen Jump auf einen Windows-Computer durchzuführen, muss auf diesem Computer der Remote-Registrierungsdienst aktiviert sein (standardmäßig in Vista deaktiviert) und auf eine Domäne gerichtet sein.

Symbolischen Jump-Link (Remote) erstellen

Um einen symbolischen Jump-Link (Remote) zu erstellen, klicken Sie auf die Schaltfläche **Erstellen** in der Jump-Schnittstelle. Wählen Sie aus der Dropdown-Liste **Remote-Jump**. Symbolische Jump-Links (Remote) erscheinen in der Jump-Schnittstelle zusammen mit Jump-Clients und anderen Arten von symbolischen Jump Item-Links.

Organisieren und verwalten Sie bestehende Jump-Elemente, indem Sie einen oder mehrere Jump-Clients auswählen und auf **Eigenschaften** klicken.



Hinweis: Um die Eigenschaften mehrerer Jump-Items anzuzeigen, müssen die ausgewählten Elemente vom gleichen Typ sein (z. B. alle Jump-Clients, alle Remote-Jumps usw.). Um Eigenschaften anderer Arten von Jump-Elementen zu überprüfen, schlagen Sie bitte im jeweiligen Abschnitt in diesem Handbuch nach.

Geben Sie einen **Namen** für das Jump-Element ein. Dieser Name kennzeichnet das Element in den Sitzungsregisterkarten. Diese Zeichenkette kann maximal 128 Zeichen lang sein.

Wählen Sie im Dropdown-Menü **Jumpoint** das Netzwerk aus, in dem sich der Computer befindet, auf den Sie zugreifen möchten. Die Konsole d. Support-Technikers merkt sich Ihre Jumpoint-Auswahl für das nächste Mal, wenn Sie diese Art von Jump-Element erstellen. Geben Sie den **Hostnamen / die IP** des Systems ein, auf das Sie zugreifen möchten.

Verschieben Sie Jump-Elemente von einer Jump-Gruppe in eine andere mithilfe des Dropdown-Menüs **Jump-Gruppe**. Die Fähigkeit, Jump-Elemente in oder aus unterschiedlichen Jump-Gruppen zu verschieben ist von Ihren Kontoberechtigungen abhängig.

Organisieren Sie Jump-Elemente eingehender, indem Sie den Namen eines neuen oder bestehenden **Tags** eingeben. Obwohl die ausgewählten Jump-Elemente unter dem Tag zusammengefasst sind, werden sie weiterhin in der Jump-Gruppe aufgeführt, in der sie fixiert wurden. Um ein Jump-Element wieder in die oberste Jump-Gruppe zu verschieben, lassen Sie dieses Feld leer.

Wählen Sie als nächstes das **Öffentliche Portal**, über das sich das Jump-Element verbinden soll. Wenn diesem öffentlichen Portal eine Sitzungsrichtlinie zugewiesen ist, kann sich diese Richtlinie auf die Berechtigungen auswirken, die für über dieses Jump-Element gestartete Sitzungen erlaubt sind. Die Möglichkeit zur Festlegung des öffentlichen Portals ist von Ihren Kontoberechtigungen abhängig.

Jump-Elemente umfassen auch ein **Kommentare**-Feld für einen Namen oder eine Beschreibung, wodurch die Sortierung, Suche und Identifizierung von Jump Clients schneller und einfacher wird.

Um festzulegen, wann es Benutzern gestattet werden soll, auf dieses Jump-Element zuzugreifen, legen Sie eine **Jump-Richtlinie** fest. Diese Richtlinien werden von Ihrem Administrator über die **/login**-Schnittstelle festgelegt.

Wählen Sie eine **Sitzungsrichtlinie**, die diesem Jump-Element zugewiesen werden soll. Die diesem Jump-Element zugewiesene Richtlinie hat die höchste Priorität bei der Festlegung von Sitzungsberechtigungen. Die Möglichkeit zur Festlegung einer Sitzungsrichtlinie ist von Ihren Kontoberechtigungen abhängig.

Wählen Sie Sitzungsrichtlinien, die diesem Jump-Element zugewiesen werden sollen. Diesem Jump-Element zugewiesene Sitzungsrichtlinien haben die höchste Priorität bei der Festlegung von Sitzungsberechtigungen. Die **Sitzungsrichtlinie für präsenste Kunden** gilt, wenn der Endbenutzer als präsent gilt. Ansonsten gilt die **Sitzungsrichtlinie für nicht präsenste Kunden**.

Die Art, wie die Kundenpräsenz bestimmt wird, wird von der Jump-Element-Einstellung **Bildschirmstatus verwenden, um Kundenpräsenz zu erkennen** in der **/login**-Schnittstelle festgelegt. Falls aktiviert, gilt ein Kunde nur als präsent, wenn ein Benutzer angemeldet ist, das System nicht gesperrt ist und kein Bildschirmschoner läuft. Falls deaktiviert, gilt ein Kunde als präsent, wenn ein Benutzer angemeldet ist, unabhängig vom Bildschirmstatus. Die Kundenpräsenz wird bestimmt, wenn die Jump-Element-Sitzung gestartet wird. Die für die Sitzung verwendete Sitzungsrichtlinie ändert sich nicht im Verlaufe der Sitzung, unabhängig von Änderungen an der Kundenpräsenz im Verlaufe der Sitzung. Die Möglichkeit zur Festlegung einer Sitzungsrichtlinie ist von Ihren Kontoberechtigungen abhängig.

CREATE NEW REMOTE JUMP SHORTCUT ×

Please configure a new Remote Jump Shortcut.

• *Required field*

Name •

Jumpoint

No Remote Jump Jumpoints Available.
▼

Hostname / IP •

Jump Group

Personal
▼

Tag

Public Portal

C
▼

Comments

Jump Policy

None
▼

Customer Present Session Policy

None
▼

Customer Not Present Session Policy

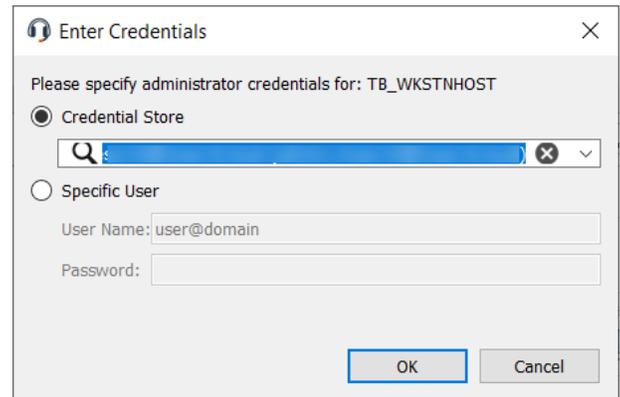
None
▼

CANCEL
OK

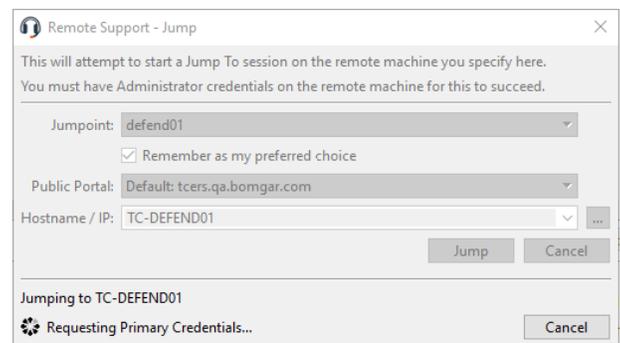
Symbolischen Jump-Link verwenden

Um einen symbolische Jump-Link zum Starten einer Sitzung zu verwenden, wählen Sie den symbolischen Link einfach aus der Jump-Schnittstelle und klicken Sie auf die Schaltfläche **Jump**.

Sie müssen Administrator-Anmeldedaten für den Remote-Computer eingeben, um den Jump abzuschließen. Die Administratorrechte müssen entweder denen eines lokalen Administrators am Remote-System oder eines Domänenadministrators entsprechen.



Die Client-Dateien werden auf das Remote-System hochgeladen und es wird versucht, eine Sitzung zu starten. Abhängig von den Sitzungsberechtigungen kann der Endbenutzer aufgefordert werden, die Sitzung zu akzeptieren oder abzulehnen. Trifft innerhalb eines definierten Zeitraums keine Antwort ein, wird die Sitzung entweder gestartet oder abgebrochen, je nach den Sitzungsberechtigungen.




Hinweis: Falls Sie über einen Jumpoint auf Systeme zugreifen müssen, wenn kein Benutzer verfügbar ist, müssen Sie gewährleisten, dass die Berechtigungen des öffentlichen Portals und Ihre Kontoberechtigungen entweder so festgelegt sind, dass die Aufforderung deaktiviert wird, oder die Standardeinstellung **Zulassen** lautet.



Hinweis: Jump-Elemente können ebenfalls eingestellt werden, um den gleichzeitigen Zugriff auf das gleiche Jump-Element durch mehrere Benutzer zu gestatten. Wenn **Bestehender Sitzung beitreten** gewählt wurde, können andere Benutzer einer bereits laufenden Sitzung beitreten. Der ursprüngliche Sitzungseigentümer wird benachrichtigt, dass ein anderer Benutzer der Sitzung beigetreten ist, darf den Zugriff aber nicht ablehnen. Weitere Informationen zu gleichzeitigen Jumps finden Sie in [Jump-Element-Einstellungen](http://www.beyondtrust.com/docs/remote-support/getting-started/admin/jump-items.htm) unter www.beyondtrust.com/docs/remote-support/getting-started/admin/jump-items.htm.

Erstellen und verwenden Sie symbolische Remote-RDP-Links

Verwenden Sie BeyondTrust, um eine Remote-Desktop-Protokoll (RDP)-Sitzung mit einem Remote-Windows- oder -Linux-System zu starten. Da RDP-Sitzungen in BeyondTrust-Sitzungen umgewandelt werden, können Benutzer Sitzungen freigeben oder übertragen, und diese können automatisch geprüft und aufgezeichnet werden, je nach Festlegung durch den Administrator.

Um RDP (Remote) über BeyondTrust nutzen zu können, benötigen Sie Zugriff auf einen Jumpoint und müssen die Benutzerberechtigung **Gestattete Jump-Methoden: RDP (Remote)** besitzen.

Symbolischen RDP-Link (Remote) erstellen

Um einen symbolischen Microsoft RDP Link (Remote) zu erstellen, klicken Sie in der Jump-Schnittstelle auf die Schaltfläche **Erstellen**. Wählen Sie aus der Dropdown-Liste **Remote-RDP**. Symbolische RDP-Links erscheinen in der Jump-Schnittstelle zusammen mit Jump-Clients und anderen Arten von symbolischen Jump-Item-Links.

Organisieren und verwalten Sie bestehende Jump-Elemente, indem Sie einen oder mehrere Jump-Clients auswählen und auf **Eigenschaften** klicken.



Hinweis: Um die Eigenschaften mehrerer Jump-Items anzuzeigen, müssen die ausgewählten Elemente vom gleichen Typ sein (z. B. alle Jump-Clients, alle Remote-Jumps usw.). Um Eigenschaften anderer Arten von Jump-Elementen zu überprüfen, schlagen Sie bitte im jeweiligen Abschnitt in diesem Handbuch nach.

Geben Sie einen **Namen** für das Jump-Element ein. Dieser Name kennzeichnet das Element in den Sitzungsregisterkarten. Diese Zeichenkette kann maximal 128 Zeichen lang sein.

Wählen Sie im Dropdown-Menü **Jumpoint** das Netzwerk aus, in dem sich der Computer befindet, auf den Sie zugreifen möchten. Die Konsole d. Support-Technikers merkt sich Ihre Jumpoint-Auswahl für das nächste Mal, wenn Sie diese Art von Jump-Element erstellen. Geben Sie den **Hostnamen / die IP** des Systems ein, auf das Sie zugreifen möchten.



Hinweis: Standardmäßig verwendet der RDP-Server den Port 3389, der daher der standardmäßige Port ist, über den BeyondTrust die Verbindung aufzubauen versucht. Wenn der Remote-RDP-Server zur Verwendung eines anderen Ports konfiguriert ist, fügen Sie diesen an den Hostnamen oder die IP-Adresse in der Form **<hostname>:<port>** oder **<ipaddress>:<port>** (zum Beispiel 10.10.24.127:40000).

Geben Sie den **Benutzernamen** ein, über den Sie sich anmelden möchten, zusammen mit der **Domäne**.

Wählen Sie die **Qualität** aus, in welcher der Remote-Bildschirm angezeigt werden soll. Diese kann nicht während der RDP-Sitzung geändert werden. Wählen Sie den Farboptimierungsmodus zur Anzeige des Remote-Bildschirms aus. Wenn Sie hauptsächlich Video freigeben, wählen Sie **Videooptimiert**; wählen Sie sonst zwischen **Schwarzweiß** (weniger Bandbreite), **Wenige Farben**, **Mehr Farben** und **Volle Farben** (verwendet mehr Bandbreite). Sowohl der videooptimierte sowie der Vollfarbmodus ermöglichen die Anzeige des Desktop-Hintergrundbilds.

Um eine neue Konsolensitzung statt einer neuen Sitzung zu starten, markieren Sie das Kontrollkästchen **Konsolensitzung**.

Wenn das Serverzertifikat nicht verifiziert werden kann, erhalten Sie eine Zertifikatswarnung. Durch Aktivieren von **Nicht vertrauenswürdiges Zertifikat ignorieren** können Sie eine Verbindung zum Remote-System aufbauen, ohne dass diese Meldung angezeigt wird.

Verschieben Sie Jump-Elemente von einer Jump-Gruppe in eine andere mithilfe des Dropdown-Menüs **Jump-Gruppe**. Die Fähigkeit, Jump-Elemente in oder aus unterschiedlichen Jump-Gruppen zu verschieben ist von Ihren Kontoberechtigungen abhängig.

Organisieren Sie Jump-Elemente eingehender, indem Sie den Namen eines neuen oder bestehenden **Tags** eingeben. Obwohl die ausgewählten Jump-Elemente unter dem Tag zusammengefasst sind, werden sie weiterhin in der Jump-Gruppe aufgeführt, in der sie fixiert wurden. Um ein Jump-Element wieder in die oberste Jump-Gruppe zu verschieben, lassen Sie dieses Feld leer.

Wählen Sie als nächstes das **Öffentliche Portal**, über das sich das Jump-Element verbinden soll. Wenn diesem öffentlichen Portal eine Sitzungsrichtlinie zugewiesen ist, kann sich diese Richtlinie auf die Berechtigungen auswirken, die für über dieses Jump-Element gestartete Sitzungen erlaubt sind. Die Möglichkeit zur Festlegung des öffentlichen Portals ist von Ihren Kontoberechtigungen abhängig.

CREATE NEW REMOTE RDP JUMP SHORTCUT x

Please configure a new Remote RDP Jump Shortcut.

• Required field

Name •

Jumpoint

Hostname / IP •

Username

Domain

Quality

Console Session

Ignore Untrusted Certificate

Jump Group

Tag

Public Portal

Comments

Jump Policy

Session Policy

Jump-Elemente umfassen auch ein **Kommentare**-Feld für einen Namen oder eine Beschreibung, wodurch die Sortierung, Suche und Identifizierung von Jump Clients schneller und einfacher wird.

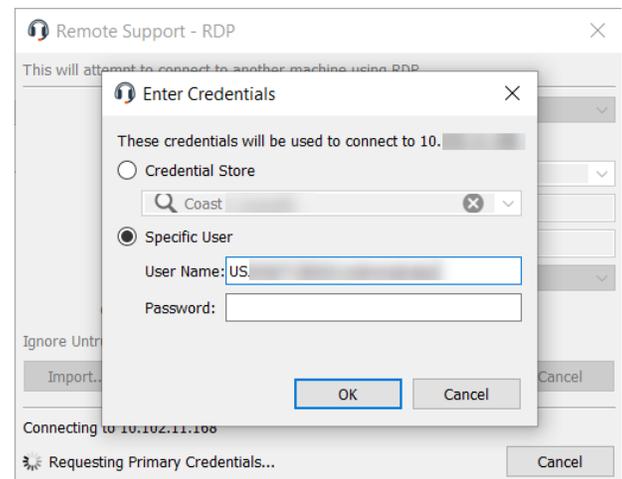
Um festzulegen, wann es Benutzern gestattet werden soll, auf dieses Jump-Element zuzugreifen, legen Sie eine **Jump-Richtlinie** fest. Diese Richtlinien werden von Ihrem Administrator über die **/login**-Schnittstelle festgelegt.

Wählen Sie eine **Sitzungsrichtlinie**, die diesem Jump-Element zugewiesen werden soll. Die diesem Jump-Element zugewiesene Richtlinie hat die höchste Priorität bei der Festlegung von Sitzungsberechtigungen. Die Möglichkeit zur Festlegung einer Sitzungsrichtlinie ist von Ihren Kontoberechtigungen abhängig.

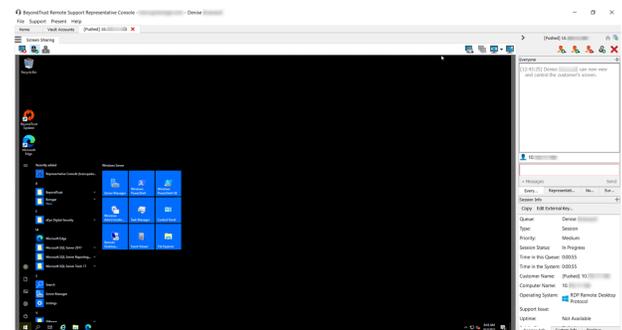
Symbolischen RDP-Link verwenden

Um einen symbolische Jump-Link zum Starten einer Sitzung zu verwenden, wählen Sie den symbolischen Link einfach aus der Jump-Schnittstelle und klicken Sie auf die Schaltfläche **Jump**.

Sie werden aufgefordert, das Passwort für den zuvor angegebenen Benutzernamen einzugeben.



Jetzt beginnt Ihre RDP-Sitzung. Beginnen Sie mit der Bildschirfreigabe, um den Remote-Desktop anzuzeigen. Sie können den Befehl **Strg+Alt+Entf** senden, eine Bildschirmaufnahme des Remote-Desktops machen und Inhalte der Zwischenablage freigeben. Sie können auch die RDP-Sitzung für andere angemeldete BeyondTrust-Benutzer freigeben oder an diese übertragen, sofern Sie die regulären Regeln Ihrer Benutzerkontoeinstellungen beachten.



Multi-Monitor-Support

Mit einer Option können Sie eine über alle Monitore des Client-Computers erweiterte Remote Support-Verbindung öffnen, unabhängig von der Konfiguration des Client-Monitors. Mit dieser Funktion können Sie alle an den Client-Computer angeschlossenen Monitore voll ausnutzen und somit die Bildschirmgröße und -skalierung während einer RDP-Sitzung über mehrere Monitore hinweg anpassen.



Hinweis: Wenn Sie während der Verwendung dieser Funktion die Vollbildschirm-Ansicht verwenden, wird das Remote-System auf allen Ihren Monitoren angezeigt.



Hinweis: Jump-Elemente können ebenfalls eingestellt werden, um den gleichzeitigen Zugriff auf das gleiche Jump-Element durch mehrere Benutzer zu gestatten. Falls auf **Neue Sitzung starten** eingestellt, wird eine neue unabhängige Sitzung für jeden Benutzer gestartet, die einen Jump zu einem bestimmten RDP-Jump-Element durchführt. Die RDP-Konfiguration am Endpunkt steuert das weitere Verhalten bezüglich gleichzeitiger RDP-Verbindungen.



Weitere Informationen zu gleichzeitigen Jumps finden Sie in [Jump-Element-Einstellungen](https://www.beyondtrust.com/docs/remote-support/getting-started/admin/jump-items.htm) unter www.beyondtrust.com/docs/remote-support/getting-started/admin/jump-items.htm.

Erstellen und Verwenden von symbolischen VNC-Links (Remote)

Verwenden Sie BeyondTrust, um eine VNC-Sitzung mit einem Remote-System zu starten. Da VNC-Sitzungen in BeyondTrust-Sitzungen umgewandelt werden, können Benutzer Sitzungen freigeben oder übertragen, und diese können automatisch geprüft und aufgezeichnet werden, je nach Festlegung durch den Administrator.

Um Remote-VNC über BeyondTrust nutzen zu können, benötigen Sie Zugriff auf einen Jumpoint sowie die Benutzerkontoberechtigung **Gestattete Jump-Methoden: Remote-VNC**.

Symbolischen VNC-Link (Remote) erstellen

Um einen symbolischen VNC-Link (Remote) zu erstellen, klicken Sie auf die Schaltfläche **Erstellen** in der Jump-Schnittstelle. Wählen Sie aus der Dropdown-Liste **Remote-VNC**. Symbolische VNC-Links erscheinen in der Jump-Schnittstelle zusammen mit Jump-Clients und anderen Arten von symbolischen Jump-Element-Links.

Organisieren und verwalten Sie bestehende Jump-Elemente, indem Sie einen oder mehrere Jump-Clients auswählen und auf **Eigenschaften** klicken.



Hinweis: Um die Eigenschaften mehrerer Jump-Items anzuzeigen, müssen die ausgewählten Elemente vom gleichen Typ sein (z. B. alle Jump-Clients, alle Remote-Jumps usw.).

Geben Sie einen **Namen** für das Jump-Element ein. Dieser Name kennzeichnet das Element in den Sitzungsregisterkarten. Diese Zeichenkette kann maximal 128 Zeichen lang sein.

Wählen Sie im Dropdown-Menü **Jumpoint** das Netzwerk aus, in dem sich der Computer befindet, auf den Sie zugreifen möchten. Die Konsole d. Support-Technikers merkt sich Ihre Jumpoint-Auswahl für das nächste Mal, wenn Sie diese Art von Jump-Element erstellen. Geben Sie den **Hostnamen / die IP** des Systems ein, auf das Sie zugreifen möchten.

Standardmäßig verwendet der VNC-Server den Port 5900, der daher der standardmäßige Port ist, über den BeyondTrust die Verbindung aufzubauen versucht. Wenn der Remote-VNC-Server zur Verwendung eines anderen Ports konfiguriert ist, geben Sie ihn im Feld **Port** ein.

Verschieben Sie Jump-Elemente von einer Jump-Gruppe in eine andere mithilfe des Dropdown-Menüs **Jump-Gruppe**. Die Fähigkeit, Jump-Elemente in oder aus unterschiedlichen Jump-Gruppen zu verschieben ist von Ihren Kontoberechtigungen abhängig.

Organisieren Sie Jump-Elemente eingehender, indem Sie den Namen eines neuen oder bestehenden **Tags** eingeben. Obwohl die ausgewählten Jump-Elemente unter dem Tag zusammengefasst sind, werden sie weiterhin in der Jump-Gruppe aufgeführt, in der sie fixiert wurden. Um ein Jump-Element wieder in die oberste Jump-Gruppe zu verschieben, lassen Sie dieses Feld leer.

Wählen Sie als nächstes das **Öffentliche Portal**, über das sich das Jump-Element verbinden soll. Wenn diesem öffentlichen Portal eine Sitzungsrichtlinie zugewiesen ist, kann sich diese Richtlinie auf die Berechtigungen auswirken, die für über dieses Jump-Element gestartete Sitzungen erlaubt sind. Die Möglichkeit zur Festlegung des öffentlichen Portals ist von Ihren Kontoberechtigungen abhängig.

Jump-Elemente umfassen auch ein **Kommentare**-Feld für einen Namen oder eine Beschreibung, wodurch die Sortierung, Suche und Identifizierung von Jump Clients schneller und einfacher wird.

Um festzulegen, wann es Benutzern gestattet werden soll, auf dieses Jump-Element zuzugreifen, legen Sie eine **Jump-Richtlinie** fest. Diese Richtlinien werden von Ihrem Administrator über die **/login**-Schnittstelle festgelegt.

Wählen Sie eine **Sitzungsrichtlinie**, die diesem Jump-Element zugewiesen werden soll. Die diesem Jump-Element zugewiesene Richtlinie hat die höchste Priorität bei der Festlegung von Sitzungsberechtigungen. Die Möglichkeit zur Festlegung einer Sitzungsrichtlinie ist von Ihren Kontoberechtigungen abhängig.

Einen symbolischen VNC-Link verwenden

Um einen symbolische Jump-Link zum Starten einer Sitzung zu verwenden, wählen Sie den symbolischen Link einfach aus der Jump-Schnittstelle und klicken Sie auf die Schaltfläche **Jump**.

CREATE NEW REMOTE VNC JUMP SHORTCUT ✕

Please configure a new Remote VNC Jump Shortcut.

- *Required field*

Name •

Jumpoint
No Remote VNC Jumpoints Available. ▼

Hostname / IP •

Port •

Jump Group
Personal ▼

Tag

Public Portal

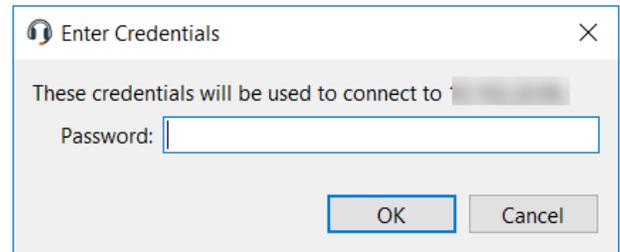
Comments

Jump Policy
None ▼

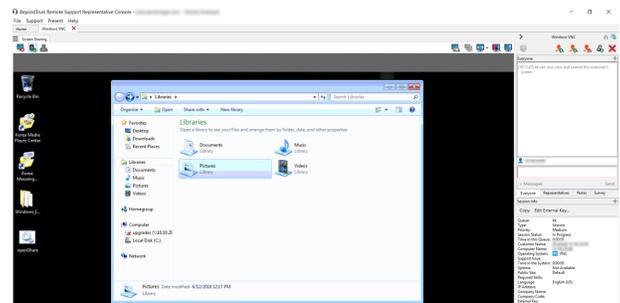
Session Policy
None ▼

CANCEL
OK

Beim Aufbau der Verbindung zum VNC-Server versucht das System, festzulegen, ob es zugehörige Anmeldedaten gibt. Falls ja, werden Sie zu deren Eingabe aufgefordert.



Ihre VNC-Sitzung beginnt. Beginnen Sie mit der Bildschirmfreigabe, um den Remote-Desktop anzuzeigen. Sie können den Befehl **Strg+Alt+Entf** senden, einen Screenshot des Remote-Desktops aufzunehmen und Textinhalte der Zwischenablage freigeben. Sie können auch die VNC-Sitzung freigeben, übertragen oder aufzeichnen, entsprechend der regulären Regeln Ihrer Benutzerkontoeinstellungen.



Hinweis: Jump-Elemente können ebenfalls eingestellt werden, um den gleichzeitigen Zugriff auf das gleiche Jump-Element durch mehrere Benutzer zu gestatten. Wenn **Bestehender Sitzung beitreten** gewählt wurde, können andere Benutzer einer bereits laufenden Sitzung beitreten. Der ursprüngliche Sitzungseigentümer wird benachrichtigt, dass ein anderer Benutzer der Sitzung beigetreten ist, darf den Zugriff aber nicht ablehnen.



Weitere Informationen zu gleichzeitigen Jumps finden Sie in [Jump-Element-Einstellungen](https://www.beyondtrust.com/docs/remote-support/getting-started/admin/jump-items.htm) unter www.beyondtrust.com/docs/remote-support/getting-started/admin/jump-items.htm.

Erstellen und Verwenden symbolischer Shell Jump-Links

Verbinden Sie sich mithilfe eines Shell Jump schnell mit einem SSH- oder Telnet-fähigen Netzwerkgerät, um die Befehlszeile auf diesem Remote-System verwenden zu können. Führen Sie beispielsweise ein standardisiertes Skript auf mehreren Systemen aus, um einen benötigten Patch zu installieren oder ein Netzwerkproblem zu beheben.

Erstellen eines symbolischen Shell Jump-Links

Um einen symbolischen Shell Jump-Link zu erstellen, klicken Sie auf die Schaltfläche **Erstellen** in der Jump-Schnittstelle. Wählen Sie aus der Dropdown-Liste **Shell Jump**. Symbolische Shell Jump-Links erscheinen in der Jump-Schnittstelle zusammen mit Jump-Clients und anderen Arten von symbolischen Jump-Element-Links.



Hinweis: Symbolische Shell Jump-Links werden nur aktiviert, wenn der Jump-Point für offenen oder eingeschränkten Shell Jump-Zugriff konfiguriert wurde.

Organisieren und verwalten Sie bestehende Jump-Elemente, indem Sie einen oder mehrere Jump-Clients auswählen und auf **Eigenschaften** klicken.



Hinweis: Um die Eigenschaften mehrerer Jump-Elemente anzuzeigen, müssen alle ausgewählten Elemente vom gleichen Typ sein (z. B. alle Jump-Clients, alle Remote-Jumps usw.). Um Eigenschaften anderer Arten von Jump-Elementen zu überprüfen, schlagen Sie bitte im jeweiligen Abschnitt in diesem Handbuch nach.

Geben Sie einen **Namen** für das Jump-Element ein. Dieser Name kennzeichnet das Element in den Sitzungsregisterkarten. Diese Zeichenkette kann maximal 128 Zeichen lang sein.

Wählen Sie im Dropdown-Menü **Jumpoint** das Netzwerk aus, in dem sich der Computer befindet, auf den Sie zugreifen möchten. Die Konsole d. Support-Technikers merkt sich Ihre Jumpoint-Auswahl für das nächste Mal, wenn Sie diese Art von Jump-Element erstellen. Geben Sie den **Hostnamen / die IP** des Systems ein, auf das Sie zugreifen möchten.

Wählen Sie das zu verwendende **Protokoll**, entweder **SSH** oder **Telnet**.

Port wechselt automatisch auf den Standard-Port für das ausgewählte Protokoll, kann aber Ihren Netzwerkeinstellungen entsprechend modifiziert werden.

Der **Benutzername**, mit dem die Anmeldung erfolgen soll.

Wählen Sie den **Terminaltyp**, entweder **xterm** oder **VT100**.

Sie können auch das **Senden von leeren Datenpaketen** aktivieren, damit inaktive Sitzungen nicht beendet werden. Geben Sie die Anzahl der Sekunden an, für die zwischen jeder Paketaussendung gewartet werden soll.

Verschieben Sie Jump-Elemente von einer Jump-Gruppe in eine andere mithilfe des Dropdown-Menüs **Jump-Gruppe**. Die Fähigkeit, Jump-Elemente in oder aus unterschiedlichen Jump-Gruppen zu verschieben ist von Ihren Kontoberechtigungen abhängig.

Organisieren Sie Jump-Elemente eingehender, indem Sie den Namen eines neuen oder bestehenden **Tags** eingeben. Obwohl die ausgewählten Jump-Elemente unter dem Tag zusammengefasst sind, werden sie weiterhin in der Jump-Gruppe aufgeführt, in der sie fixiert wurden. Um ein Jump-Element wieder in die oberste Jump-Gruppe zu verschieben, lassen Sie dieses Feld leer.

Wählen Sie als nächstes das **Öffentliche Portal**, über das sich das Jump-Element verbinden soll. Wenn diesem öffentlichen Portal eine Sitzungsrichtlinie zugewiesen ist, kann sich diese Richtlinie auf die Berechtigungen auswirken, die für über dieses Jump-Element gestartete Sitzungen erlaubt sind. Die Möglichkeit zur Festlegung des öffentlichen Portals ist von Ihren Kontoberechtigungen abhängig.

Jump-Elemente umfassen auch ein **Kommentare**-Feld für einen Namen oder eine Beschreibung, wodurch die Sortierung, Suche und Identifizierung von Jump Clients schneller und einfacher wird.

Um festzulegen, wann es Benutzern gestattet werden soll, auf dieses Jump-Element zuzugreifen, legen Sie eine **Jump-Richtlinie** fest. Diese Richtlinien werden von Ihrem Administrator über die **/login**-Schnittstelle festgelegt.

Wählen Sie eine **Sitzungsrichtlinie**, die diesem Jump-Element zugewiesen werden soll. Die diesem Jump-Element zugewiesene Richtlinie hat die höchste Priorität bei der Festlegung von Sitzungsberechtigungen. Die Möglichkeit zur Festlegung einer Sitzungsrichtlinie ist von Ihren Kontoberechtigungen abhängig.

CREATE NEW SHELL JUMP SHORTCUT ×

Please configure a new Shell Jump Shortcut.

- *Required field*

Name •

Jumpoint
No Shell Jump Jumpoints Available. ▼

Hostname / IP •

Protocol
SSH ▼

Port •

Username

Terminal Type
xterm ▼

Keep-Alive
 Send Keep-Alive Packets

Jump Group
Personal ▼

Tag

Public Portal
BeyondTrust.sqa.com/gar.com ▼

Comments

Jump Policy
None ▼

Session Policy
None ▼

CANCEL
OK

Symbolischen Shell Jump-Link verwenden

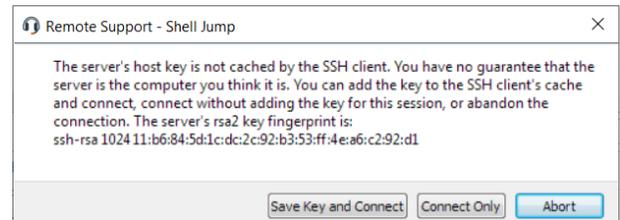
Um einen symbolische Jump-Link zum Starten einer Sitzung zu verwenden, wählen Sie den symbolischen Link einfach aus der Jump-Schnittstelle und klicken Sie auf die Schaltfläche **Jump**.

Wenn Sie versuchen, per Shell Jump auf ein SSH-Gerät ohne zwischengespeicherten Hostschlüssel zu wechseln, erhalten Sie eine Warnmeldung, dass der Hostschlüssel des Servers nicht zwischengespeichert ist und nicht garantiert wird, dass es sich bei dem Server um den von Ihnen vermuteten Computer handelt.

Wenn Sie **Schlüssel speichern und verbinden** wählen, wird der Schlüssel auf dem Hostsystem des Jumpoint zwischengespeichert, sodass zukünftige Versuche, per Shell Jump auf dieses System zuzugreifen, nicht wieder zur Anzeige dieser Eingabeaufforderung führen. **Nur verbinden** startet die Sitzung, ohne den Schlüssel zwischenzuspeichern, und **Abbrechen** beendet die Shell Jump-Sitzung.

Wenn Sie per Shell Jump auf ein SSH-Gerät aktivierter interaktiver MFA für die Tastatur wechseln, wird eine zweite Eingabeaufforderung angezeigt.

Wenn Sie per Shell Jump auf ein Remote-Gerät wechseln, beginnt sofort eine Befehlsshell-Sitzung mit diesem Gerät. Wenn Sie per Shell Jump auf ein bereitgestelltes SSH-Gerät mit unverschlüsseltem Schlüssel oder verschlüsseltem Schlüssel, dessen Passwort zwischengespeichert wurde, wechseln, werden Sie nicht aufgefordert, ein Passwort einzugeben. Ansonsten werden Sie zur Eingabe eines Passworts aufgefordert. Sie können dann Befehle an das Remote-System senden.



Anmelden im System mithilfe der Anmeldedaten-Einfügung über die Web-Konsole des Support-Technikers

Beim Zugriff auf ein Windows-basiertes Jump-Element über die Web-Konsole des Support-Technikers können Sie Anmeldedaten aus einem Anmeldedaten-Speicher verwenden, um sich am Endpunkt anzumelden oder Anwendungen als Administrator auszuführen.

Stellen Sie vor Verwendung der Anmeldedaten-Einfügung sicher, dass ein Anmeldedaten-Speicher oder ein Passwortspeicher zur Verfügung steht, um sich mit BeyondTrust Remote Support zu verbinden.

Installation und Konfiguration des Endpunkt-Anmeldedaten-Managers

Bevor Sie damit beginnen können, mithilfe der Anmeldedaten-Einfügung auf Jump-Elemente zuzugreifen, müssen Sie den BeyondTrust Endpunkt-Anmeldedaten-Manager (ECM) herunterladen, installieren und konfigurieren. Mit dem BeyondTrust ECM können Sie Ihre Verbindung zu einem Anmeldedaten-Speicher (wie einem Passwort-Vault) schnell konfigurieren.



Hinweis: Der ECM muss auf Ihrem System installiert werden, damit der BeyondTrust ECM-Dienst aktiviert und die Anmeldedateneinfügung in BeyondTrust Remote Support ermöglicht werden kann.

Systemanforderungen

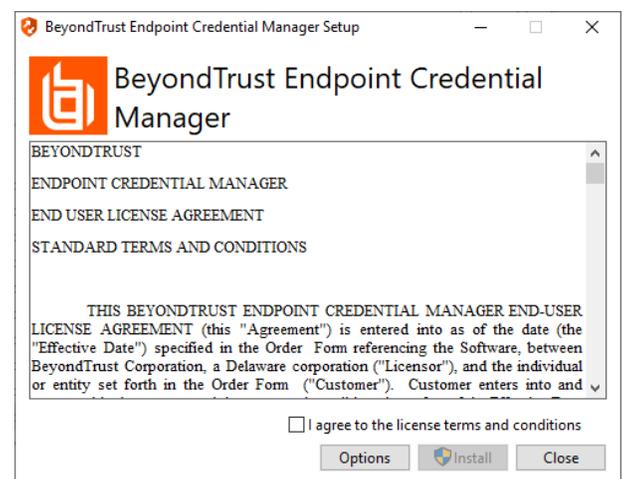
- Windows Vista oder neuer, nur 64 Bit
- .NET 4.5 oder neuer
- Prozessor: 2 GHz oder schneller
- Speicher: 2 GB oder mehr
- Verfügbarer Festplattenspeicherplatz: 80 GB oder mehr

1. Laden Sie zunächst den BeyondTrust Endpunkt-Anmeldedaten-Manager (ECM) von [BeyondTrust Support](https://www.beyondtrust.com/docs/index.htm#support) unter <https://www.beyondtrust.com/docs/index.htm#support> herunter. Öffnen Sie den BeyondTrust-Konfigurationsassistenten des Endpunkt-Anmeldedaten-Managers.
2. Stimmen Sie den Bedingungen der Endbenutzer-Lizenzvereinbarung zu. Aktivieren Sie das Kontrollkästchen zur Zustimmung und klicken Sie auf **Installieren**. Klicken Sie auf die Schaltfläche **Optionen**, um den Installationspfad anzupassen.

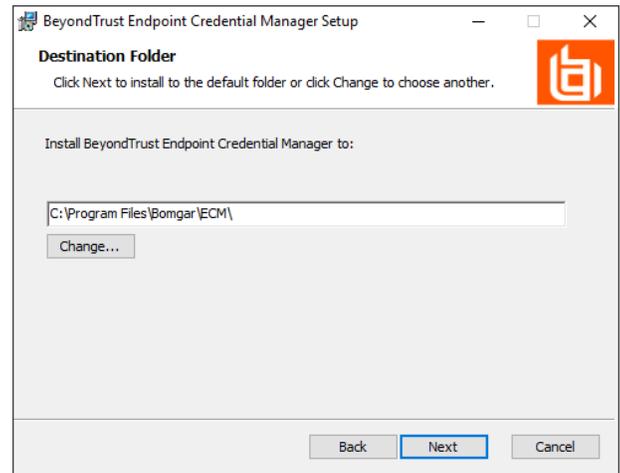


Hinweis: Sie können mit der Installation erst fortfahren, wenn Sie der Endbenutzer-Lizenzvereinbarung zustimmen.

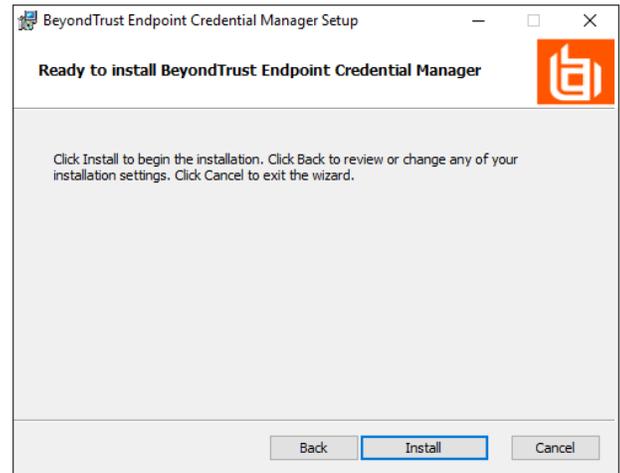
3. Klicken Sie auf **Installieren**.



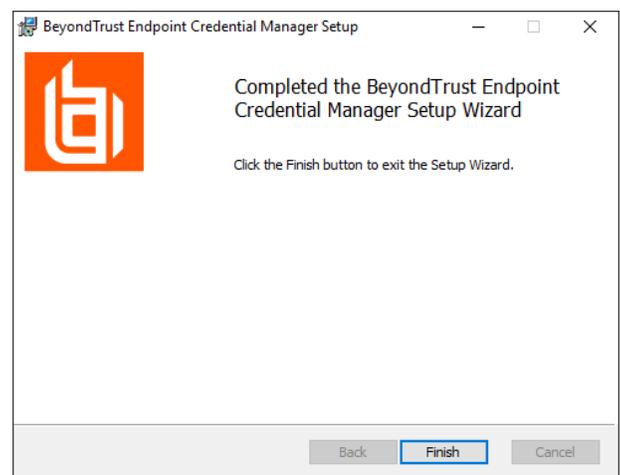
4. Wählen Sie den Installationsort für den Anmeldedaten-Manager und klicken Sie auf **Weiter**.
5. Auf dem nächsten Bildschirm können Sie mit der Installation beginnen oder vorherige Schritte überprüfen.



6. Klicken Sie auf **Installieren**, wenn Sie bereit sind.



7. Die Installation nimmt einige Zeit in Anspruch. Klicken Sie auf dem Bildschirm auf **Fertigstellen**.



Hinweis: Um einen ausfallfreien Betrieb zu gewährleisten, können Administratoren bis zu fünf ECMs auf unterschiedlichen Windows-Systemen installieren, um über das BeyondTrust Appliance B Series mit der gleichen Site zu kommunizieren. Eine Liste der mit der B Series Appliance-Site verbundenen ECMs finden Sie unter **/login > Status > Informationen > ECM-Clients**.

Hinweis: Wenn mehrere ECMs mit einer BeyondTrust-Website verbunden sind, leitet das B Series Appliance Anfragen an den ECM, der am längsten mit dem B Series Appliance verbunden ist.

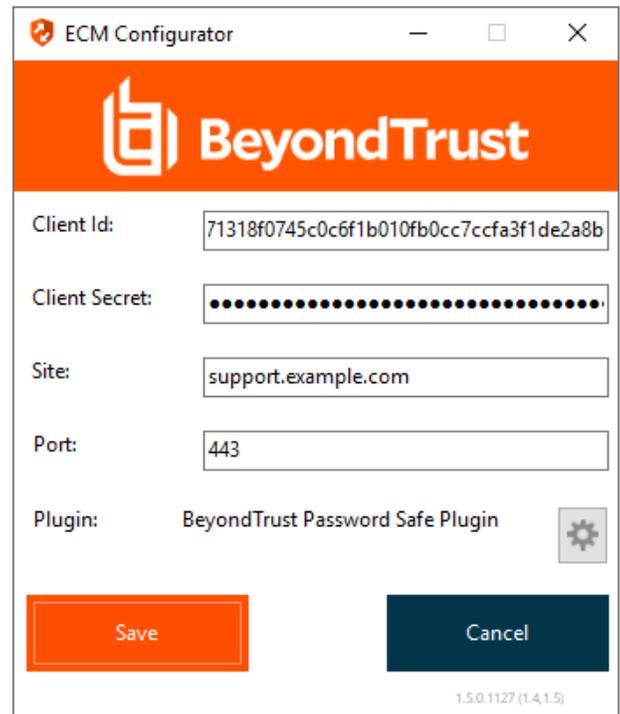
Hinweis: Sollte während der Installation ein Windows-Pluginfehler auftreten, suchen und entsperren Sie die Datei **BomgarVaultRestPlugin.dll**.

Konfiguration einer Verbindung zu Ihrem Anmeldedaten-Speicher

Mit dem Konfigurator des Anmeldedaten-Managers können Sie eine Verbindung zu Ihrem Anmeldedaten-Speicher aufbauen.

1. Machen Sie den soeben installierten BeyondTrust ECM-Konfiguratur über das Windows-Suchfeld oder durch Aufruf der Programmliste in Ihrem **Startmenü** ausfindig.
2. Führen Sie das Programm aus, um eine Verbindung aufzubauen.
3. Wenn der Konfigurator geöffnet wird, vervollständigen Sie die Felder. Alle Felder müssen ausgefüllt werden.

BeyondTrust-ECMConfigurator.exe	7/23/2019 2:35 PM	Application	317 KB
BeyondTrust-ECMConfigurator.exe.config	7/23/2019 2:35 PM	CONFIG File	1 KB
BeyondTrust-ECMService.exe	7/23/2019 2:35 PM	Application	26 KB
BeyondTrust-ECMService.exe.config	7/23/2019 2:35 PM	CONFIG File	2 KB
Configurator.log	11/14/2019 3:06 PM	Text Document	3 KB
ECM.dll	7/23/2019 2:35 PM	Application exten...	65 KB
ECM.log	11/14/2019 3:06 PM	Text Document	4 KB
ECSM.settings	7/23/2019 2:35 PM	SETTINGS File	1 KB
log4net.dll	7/23/2019 2:35 PM	Application exten...	294 KB
Newtonsoft.Json.dll	8/3/2014 9:33 PM	Application exten...	491 KB
Util.dll	7/23/2019 2:35 PM	Application exten...	31 KB



Geben Sie folgende Werte ein:

Feldbezeichnung	Wert
Client-ID	Die Admin-ID für Ihren Anmeldedatenspeicher.
Client-Secret	Der Admin-Geheimschlüssel für Ihren Anmeldedatenspeicher.
Website	Die URL für Ihre Anmeldedaten-Speicher-Instanz.
Port	Der Serverport, über den sich der Anmeldedaten-Manager mit Ihrer Website verbindet.
Plugin	Klicken Sie auf die Schaltfläche Plugin wählen... , um das Plugin ausfindig zu machen.

4. Wenn Sie auf die Schaltfläche **Plugin wählen...** klicken, wird der Speicherort für den Anmeldedaten-Speicher geöffnet.
5. Fügen Sie Ihre Plugin-Dateien in den Ordner ein.
6. Öffnen Sie die Plugin-Datei, um mit dem Ladevorgang zu beginnen.



Hinweis: Wenn Sie sich mit einem Passwort-Speicher verbinden, sind möglicherweise weitere Konfigurationsschritte auf Plugin-Ebene notwendig. Die Plugin-Anforderungen variieren basierend auf dem Anmeldedaten-Speicher, mit dem Sie eine Verbindung aufbauen.



WICHTIG!

Um die neuen Einstellungen in der Konfiguration zu übernehmen, starten Sie den Anmeldedaten-Manager-Dienst neu.

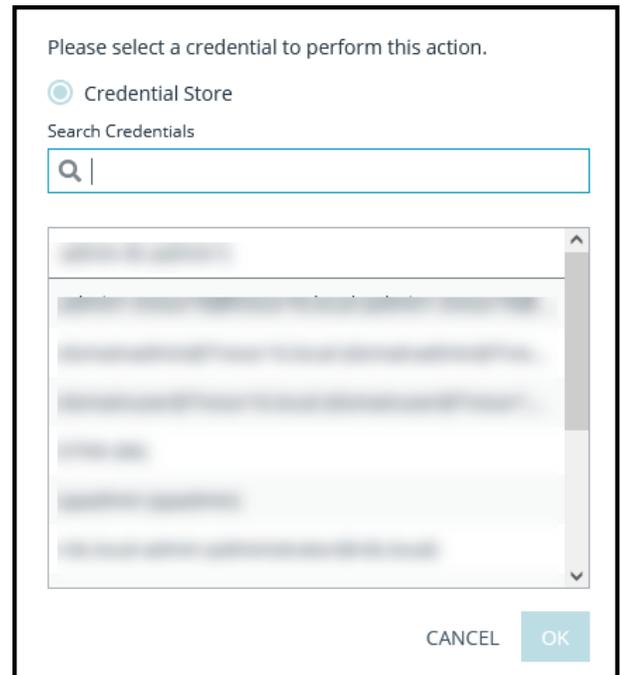
Verwendung der Anmeldedaten-Einfügung zum Zugriff auf Remote-Systeme

Nachdem der Anmeldedaten-Speicher konfiguriert und eine Verbindung aufgebaut wurde, kann die Web-Konsole des Support-Technikers mit der Verwendung von Anmeldedaten aus dem Anmeldedaten-Speicher zur Anmeldung in Remote-Systemen beginnen.

1. Melden Sie sich in der Web-Konsole des Support-Technikers an.
2. Führen Sie einen Jump zu einem Remote-System mit einem Jump-Element durch, das als heraufgesetzter Dienst auf einem Windows-System installiert wurde.
3. Klicken Sie auf die Schaltfläche **Wiedergabe**, um die Bildschirmfreigabe mit dem Remote-System zu beginnen. Wenn sich das Remote-System am Windows-Anmeldebildschirm befindet, wird die Schaltfläche **Anmeldedaten einfügen** hervorgehoben.
4. Klicken Sie auf die Schaltfläche **Anmeldedaten einfügen**. Ein Popup-Dialog zur Anmeldedatenauswahl erscheint und führt die Anmeldedaten auf, die über den Endpunkt-Anmeldedaten-Manager verfügbar sind.



5. Wählen Sie die geeigneten Anmeldedaten aus dem Endpunkt-Anmeldedaten-Manager, die verwendet werden sollen. Das System ruft die Anmeldedaten vom Endpunkt-Anmeldedaten-Manager ab und setzt sie auf dem Windows-Anmeldungs Bildschirm ein.
6. Der Support-Techniker wird am Remote-System angemeldet.



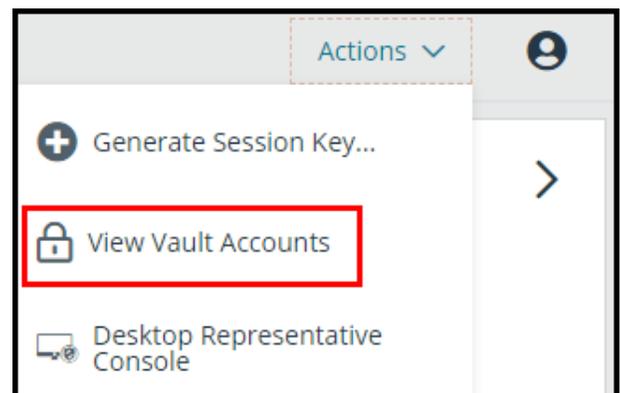
Hinweis: Wenn Sie BeyondTrust Vault verwenden, können im Dropdown-Menü maximal 2.000 Anmeldedaten angezeigt werden. Wird der ECM verwendet, sind höchstens 200 möglich.

Einchecken und Auschecken von Vault-Anmeldedaten

Von der Web-Konsole des Support-Technikers aus können Sie über die Schnittstelle **/login** einfach auf den BeyondTrust-Vault zugreifen, um bei Bedarf Anmeldedaten auszuchecken und einzuchecken, entweder während einer Sitzung oder auf Ihrem lokalen Computer.

Um auf Vault zuzugreifen, klicken Sie oben rechts auf dem Bildschirm auf das Menüelement **Aktionen** und wählen Sie **Vault-Konten anzeigen**. Sie gelangen direkt auf die Seite **Vault > Konten** in der Schnittstelle **/login**, wenn Sie angemeldet sind.

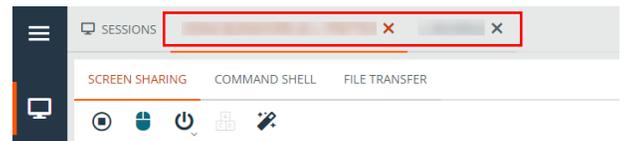
Sie können dann ein Vaultkonto auswählen und auschecken oder einchecken.



Verwalten mehrerer Support-Sitzungen in der Web-Konsole des Support-Technikers

Zur aktiven Sitzung zurückkehren

Wenn Sie über mehrere laufende Support-Sitzung Techs verfügen, können Sie jederzeit zu einer anderen Sitzung zurückkehren. Um zu einem System zurückzukehren, auf das Sie bereits in einer anderen Sitzung zugreifen, klicken Sie auf die gewünschte Support-Sitzung Tech am oberen Bildschirmrand.



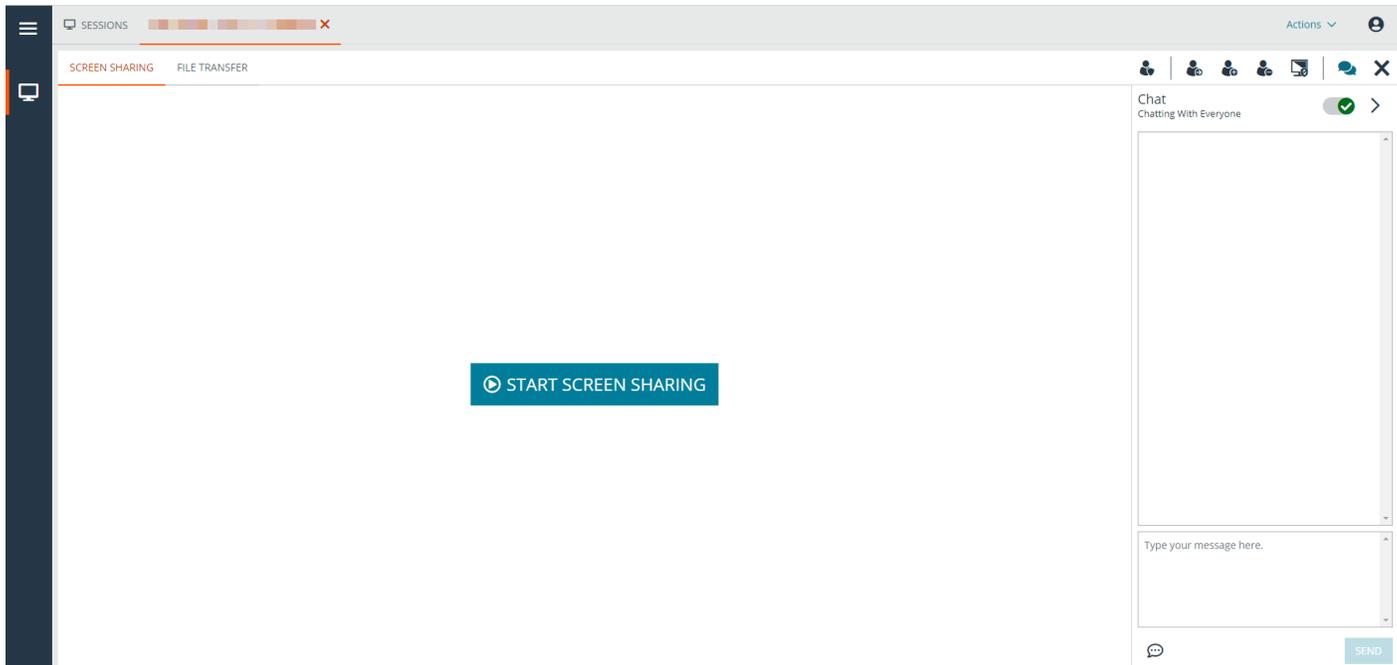
Wenn eine neue Sitzung in eine Ihrer Warteschlangen eingereicht wird, erscheint eine Popup-Benachrichtigung in der linken unteren Ecke Ihres Bildschirms. Sie können auf **Anzeigen** klicken, um die Details der Sitzungen in der Warteschlange anzuzeigen.



Hinweis: Bei Bereitstellung von Support für einen mobilen Client bietet die Web-Konsole des Support-Technikers „Nur Anzeigen“-Support.

Support-Sitzungs-Aktionen in der Web-Konsole des Support-Technikers

In einer Support-Sitzung Tech können Sie mit dem Kunden chatten, eine Bildschirmfreigabe-Sitzung oder eine Befehlshell-Sitzung starten. Die Schaltfläche oben links in der Sitzungsschnittstelle gewährt Zugriff auf das Remote-System, während die Schaltflächen oben rechts in der Sitzungsschnittstelle die Verwaltung der Sitzung als Ganzes ermöglichen.



Support-Sitzungs-Aktionen

	<p>Wird ein kompatibles iOS-Gerät erkannt, erscheint das Symbol Spezielle Aktionen und ermöglicht es dem Support-Techniker, iOS-Bildschirmfreigabeanweisungen auf das Gerät zu pushen.</p>
 	<p>Falls zulässig, installieren Sie einen Support-Button auf dem Remote-Desktop oder entfernen Sie einen zuvor installierten Support-Button. Der Kunde kann einen Support-Button schnell und einfach durch Klicken auf die Support-Sitzung Tech einleiten.</p>
 	<p>Falls zulässig, installieren Sie einen Jump-Client auf dem Remote-Computer, damit Sie oder Ihre Teammitglieder später ohne Einleitung durch den Endbenutzer wieder auf das System zugreifen können. Deinstallieren Sie den Client, wenn Sie keinen unüberwachten Zugriff auf dieses System mehr brauchen.</p>

	<p>Setzen Sie eine Click-to-Chat-Sitzung auf den vollständigen Kunden-Client herauf oder setzen Sie den Kunden-Client so herauf, dass er Administratorrechte aufweist, indem Sie auf die Schiltschaltfläche klicken. Wählen Sie Kunden auffordern, um die Admin-Anmeldedaten vom Remote-Benutzer anzufordern. Wenn Sie am Remote-Computer über Administratorrechte verfügen, wählen Sie Bestimmter Benutzer, um selbst einen Benutzernamen und ein Passwort mit Administratorrechten anzugeben.</p> <p>Die Heraufsetzung des Kunden-Clients ermöglicht den Wechsel von Benutzerkonten, die Bereitstellung von Jump-Clients im Dienstmodus und die Steuerung geschützter Fenster und UAC-Dialogfelder. Die Heraufsetzung verändert nicht den Benutzerkontext des aktiven Benutzers und gleicht nicht der Abmeldung als aktiver Benutzer und erneuter Anmeldung als Administrator.</p> <p>Die Heraufsetzung auf Admin-Rechte ist aktuell nur für Windows- und Mac-Computer verfügbar. Administratoren können den Kunden-Client darauf konfigurieren, die Heraufsetzung auf Windows-Systemen beim Starten der Sitzung automatisch anzufordern.</p>
	<p>Sollten Sie entscheiden, eine Sitzung besser von jemand anderem durchführen zu lassen, übertragen Sie die Kontrolle über diese Sitzung auf ein anderes Team oder einen anderen Benutzer. Bleiben Sie als Teilnehmer in der Sitzung oder schließen Sie Ihre Registerkarte, um die Sitzung mit dem neuen Eigentümer zu verlassen. Sobald Sie die Sitzung einem neuen Eigentümer übertragen haben, werden die Symbole Übertragen, Freigeben und Entfernen grau. Sie können diese Aktionen dann nicht länger durchführen, da Sie nicht mehr der Sitzungseigentümer sind. Die Sitzung wird weiter bestehen, bis der neue Eigentümer der Sitzung diese schließt.</p>
	<p>Laden Sie einen anderen Benutzer zur Teilnahme an einer freigegebenen Sitzung ein. Sie sind weiterhin Eigentümer der Sitzung, können aber Beiträge eines oder mehrerer Teammitglieder erhalten.</p>
	<p>Der Sitzungseigentümer kann einen anderen Benutzer aus einer freigegebenen Sitzung entfernen. Zusätzlich können Sie die Verbindung mit dem Kunden abbrechen, aber weiterhin in der Sitzungsregisterkarte bleiben.</p>
	<p>Aktiviert oder deaktiviert die Chatleiste.</p>
	<p>Fixiert oder löst die Chat-Leiste.</p>
	<p>Schließen Sie Ihre Sitzungsseite ganz. Falls Sie Eigentümer der Sitzung sind, können Sie den Kunden-Client entweder vom Remote-System deinstallieren oder die Sitzung in der Warteschlange belassen.</p>



Weitere Informationen zur Bildschirmfreigabe unter iOS finden Sie in [Bildschirmfreigabe mit dem iOS-Gerät auf https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/apple-ios/ios-screen-sharing.htm](https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/apple-ios/ios-screen-sharing.htm).

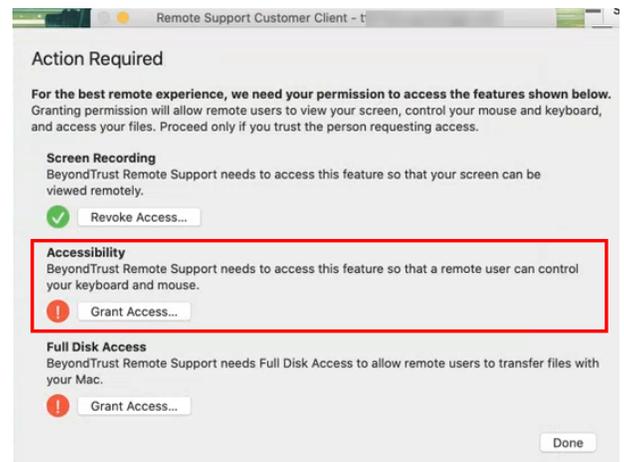
Steuern des Remote-Systems mit der Bildschirmfreigabe in der Web-Konsole des Support-Technikers

Um den Bildschirm eines Kunden anzuzeigen und zu steuern, können Sie die Bildschirmfreigabeaktion in einer Support-Sitzung Tech verwenden.

Klicken Sie im Sitzungsfenster auf **Bildschirmfreigabe starten**, um mit dem Zugriff auf das System zu beginnen.



Hinweis: Klicken Sie bei macOS Catalina (10.15)+-Systemen auf den Link oben auf der Seite **Bildschirmfreigabe**, wenn die Remote-Steuerung nicht aktiviert ist, um den Kunden nach Berechtigungen zu fragen. Der Kunde kann dann den Zugriff gewähren, wenn er im Kunden-Client dazu aufgefordert wird, und der Support-Techniker wird zu den richtigen Bereichen in den **Einstellungen** geleitet, um die Berechtigungen zu aktualisieren.

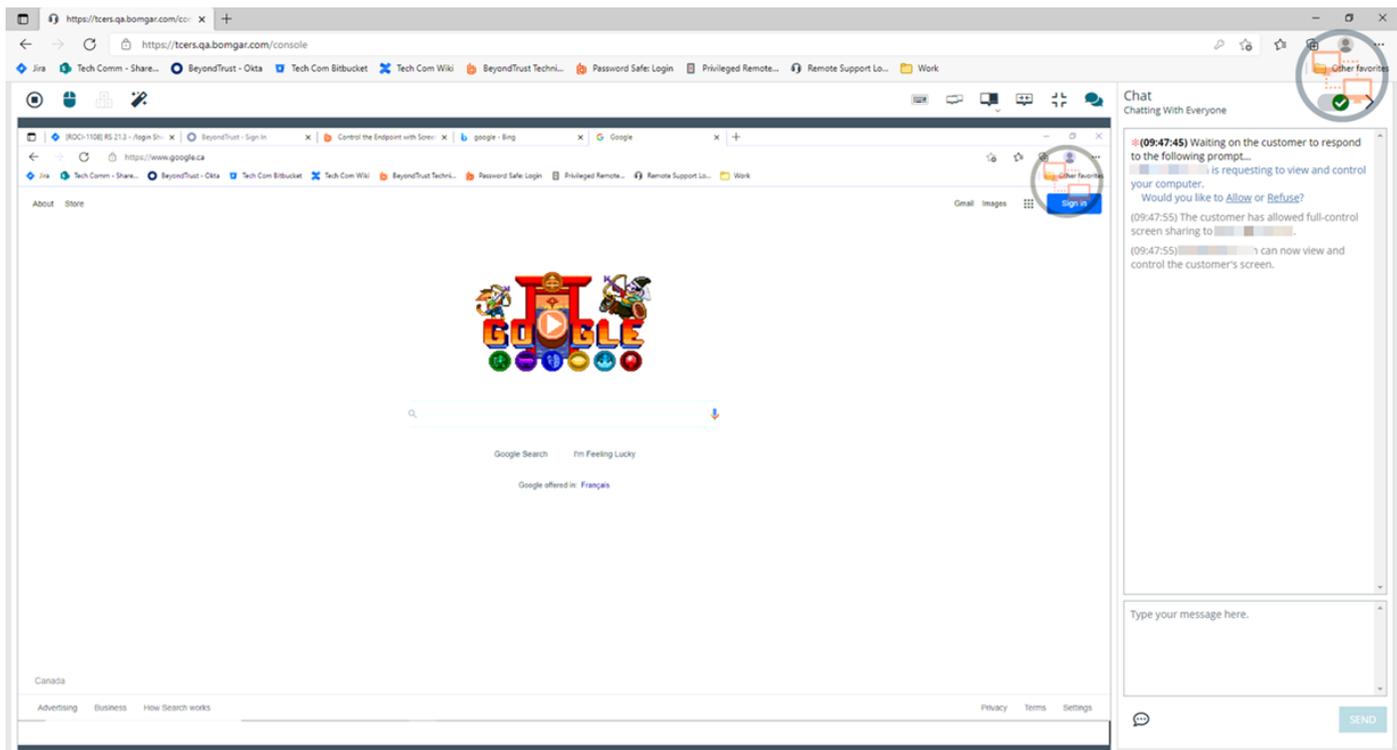


Verwenden Sie folgende Aktionen in einer Sitzung für unterschiedliche Funktionen:

Bildschirmfreigabe-Werkzeuge

	<p>Bildschirmfreigabe beenden.</p>
	<p>Bei Arbeiten auf dem Remote-Computer können Sie die Steuerung der Tastatur oder Maus anfordern bzw. beenden.</p> <p>Support-Techniker, die ein macOS-System verwenden, können Strg+Linke Maustaste über die verbundene Bildschirmfreigabebesitzung an das Remote-System senden, indem sie Strg+CMD+Linke Maustaste verwenden.</p>
	<p>Wenn Ihre Berechtigungen es zulassen, können Sie die Bildschirmansicht und die Maus- und Tastatureingabe des Remote-Benutzers deaktivieren. Die Kundenansicht des privaten Bildschirms erläutert dann, dass der Support-Techniker die Kundenansicht deaktiviert hat. Ihr Kunde kann durch Drücken von Strg-Alt-Entf stets wieder die Kontrolle übernehmen.</p> <p>Alternativ können Sie die Maus- und Tastatureingabe des Kunden deaktivieren, wobei er weiterhin den Bildschirm ansehen kann. Wenn die Eingabe eingeschränkt ist, erscheint ein orangener Rahmen auf den Monitoren des Kunden und eine Nachricht gibt an, dass der Support-Techniker die Maus- und Tastatursteuerung besitzt. Ihr Kunde kann durch Drücken von Strg-Alt-Entf stets wieder die Kontrolle übernehmen.</p> <p>Die eingeschränkte Kundeninteraktion ist nur bei der Unterstützung von macOS- Windows- Computern verfügbar. In Windows Vista und höher muss der Kunden-Client heraufgesetzt werden. In Windows 8 und höher ist der private Bildschirm nicht verfügbar, und der Support-Techniker kann nur Maus und Tastatur deaktivieren.</p>
	<p>Senden Sie einen Strg-Alt-Entf-Befehl an den Remote-Computer.</p>
	<p>Eine spezielle Aktion auf dem Remote-System durchführen. Je nach Betriebssystem und Konfiguration des Remote-Computers variieren die verfügbaren Aufgaben. Bei der Verwendung des heraufgesetzten Modus können einige Aktionen im Systemkontext ausgeführt werden. Alternativ können Sie die Anmeldedaten eines Administrators verwenden, um eine spezielle Aktion in diesem Benutzerkontext durchzuführen. Vordefinierte Skripte, die dem Benutzer zur Verfügung stehen, erscheinen in einem ausklappbaren Menü.</p>
	<p>Schalten Sie die virtuelle Tastatur ein oder aus.</p>
	<p>Nehmen Sie eine Bildschirmaufnahme auf. Sie können sie in einer Datei oder in der Zwischenablage speichern.</p>
	<p>Einen alternativen Remote-Bildschirm für die Anzeige auswählen. Der primäre Monitor wird mit einem P gekennzeichnet.</p>
	<p>Den Remote-Bildschirm in der tatsächlichen Größe oder skaliert anzeigen.</p>

	<p>Wählen Sie den Farboptimierungsmodus zur Anzeige des Remote-Bildschirms aus. Wenn Sie hauptsächlich Video freigeben, wählen Sie Videooptimiert; wählen Sie sonst zwischen Schwarzweiß (weniger Bandbreite), Wenige Farben, Mehr Farben und Volle Farben (verwendet mehr Bandbreite). Sowohl der videooptimierte wie auch der Vollfarbmodus ermöglichen die Anzeige des Desktop-Hintergrundbilds.</p>
 	<p>Zeigen Sie den Remote-Desktop im Vollbildmodus an oder kehren Sie zur Schnittstellenansicht zurück. Im Vollbildmodus werden besondere Tasten an das Remote-System weitergegeben. Dies umfasst, aber ist nicht beschränkt auf Modifikatortasten, Funktionstasten und die Windows Start-Taste. Beachten Sie, dass dies nicht für den Befehl Strg-Alt-Entf gilt.</p>



Zugriff auf die Befehlshell am Remote-System über die Web-Konsole des Support-Technikers

Mit der Remote-Befehlshell kann ein berechtigter Support-Techniker eine virtuelle Befehlszeilenschnittstelle für den Remote-Computer öffnen. Der Benutzer kann dann Befehle lokal eingeben, aber auf dem Remote-Computer ausführen lassen. Sie können mit mehreren Shells arbeiten.

Ihr Administrator kann auch die Remote-Shell-Aufzeichnung aktivieren, sodass ein Video jeder Shell später über den Sitzungsbericht angezeigt werden kann. Wenn Befehlshell-Aufzeichnung aktiviert ist, ist ebenfalls eine Abschrift der Befehlshell verfügbar.

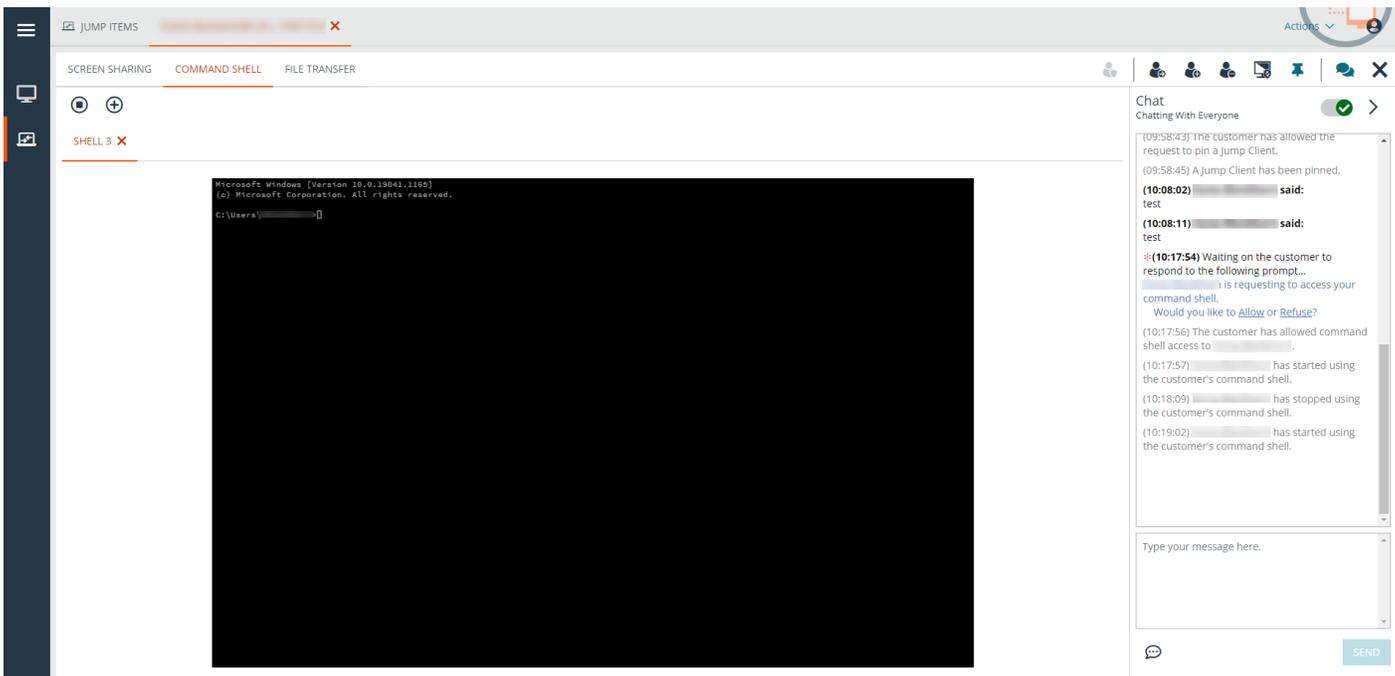
Um in einer Support-Sitzung auf die Befehlshell zuzugreifen, klicken Sie auf die Registerkarte **Befehlshell** am oberen Bildschirmrand.

Nach dem Anklicken von **Befehlshell** werden die Befehlsoptionen und die Eingabeaufforderung angezeigt.



Befehlshell-Tools

		<p>Zugriff auf die Eingabeaufforderung starten oder stoppen.</p>
		<p>Öffnen Sie eine neue Shell, um mehrere Instanzen der Eingabeaufforderung auszuführen. Die einzelnen Shells werden als Registerkarten am oberen Bildschirmrand angezeigt.</p>

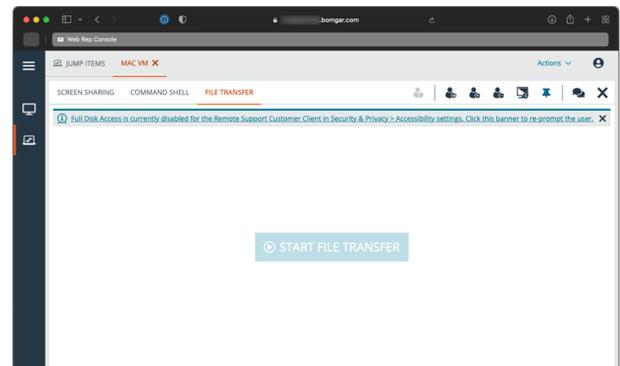


Verwenden der Web-Konsole des Support-Technikers zur Übertragung von Dateien zu und von Remote-Systemen

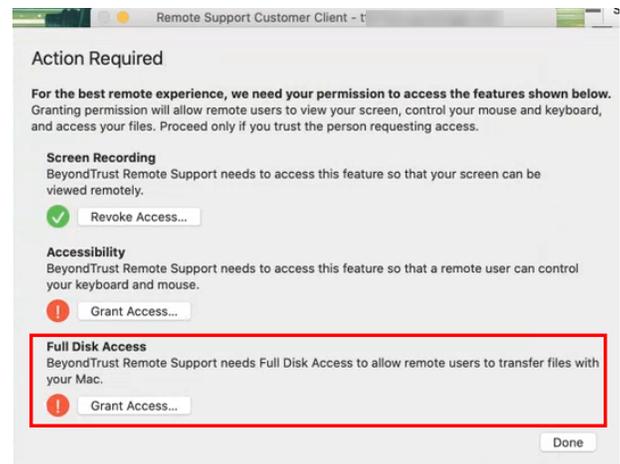
Während einer Sitzung können Support-Techniker Dateien und Verzeichnisse sowohl zu und vom Remote-System übertragen und diese löschen und umbenennen. Sie müssen nicht die vollständige Kontrolle über den Remote-Computer haben, um Dateien übertragen zu können.

Je nach den Berechtigungen, die Ihr Administrator für Ihr Konto festgelegt hat, können Sie nur Dateien auf das Remote-System hochladen oder auch Dateien auf Ihren lokalen Computer herunterladen. Der Dateisystemzugriff kann ebenfalls auf bestimmte Pfade auf dem Remote- oder lokalen System beschränkt sein, wodurch Uploads oder Downloads nur auf bestimmte Verzeichnisse beschränkt sind.

Ist die Bildschirmfreigabe in macOS Catalina (10.15) oder höher nicht aktiviert, klicken Sie auf den Link über der Seite **Dateitransfer**, um den Benutzer um die Berechtigung für den Transfer von Dateien zu bitten.



Der Kunde kann nun den Zugriff gewähren, wenn er in Kunden-Client dazu aufgefordert wird, und der Support-Techniker wird zu den richtigen Bereichen in den **Einstellungen** geleitet, um die Berechtigungen zu aktualisieren.



Übertragen Sie Dateien mithilfe der Upload- oder Download-Schaltflächen. Überprüfen Sie den Übertragungs- und Löschfortschritt, indem Sie auf den Abwärtspfeil **Übertragungsfortschritt** am unteren Bildschirmrand klicken. Sie können Dateien herunterladen, umbenennen oder löschen, indem Sie auf das Symbol **Weitere Optionen** klicken.

Um mit der Übertragung von Dateien auf ein System zu beginnen, klicken Sie auf **Dateitransfer** am oberen Rand des Bildschirms.

Klicken Sie auf die Schaltfläche **Dateitransfer starten**, um die Dateiübertragung zu beginnen. Wählen Sie dann in der Spalte **Volumen** einen Ort, an dem Sie die Navigation beginnen möchten. Die Breadcrumbs oben zeigen Ihren momentanen Standort an. Doppelklicken Sie auf ein Verzeichnis, um es zu öffnen.



SESSIONS
×

SCREEN SHARING
FILE TRANSFER

Volumes <

C:\

Documents [C:\Users\... \Documents\]

Desktop [C:\Users\... \Desktop\]

Home [C:\Users\... \]

C:\ > Users > Desktop

⋮
↺
👁
⬆
⬇
🗑

3 Files, 2 Directories (1 File Selected | [Select All 3 Files](#))

Name	Modified	Size
•• Go up a directory	-	-
📁 Images	Jul 26, 2021	-
📁 PDFs	Aug 24, 2021	-
📄 Google Chrome.Ink	Jun 29, 2021	2.24 KB
📄 Microsoft Teams.Ink	Aug 31, 2021	2.34 KB
📄 pra-cloud-admin.pdf	Aug 24, 2021	1.78 MB



Hinweis: Wenn ein ICAP-Server aktiviert ist, werden alle per FTP übertragenen Dateien auf Malware gescannt. Wird in der Datei Malware entdeckt, wird sie nicht übertragen. Einzelheiten zu einer fehlgeschlagenen Dateiübertragung können auf dem Bildschirm für die Dateiübertragung angezeigt werden und sind in Sitzungs- oder Teamberichten verfügbar. Um einen ICAP-Server zu aktivieren, siehe Sicherheit unter <https://www.beyondtrust.com/docs/remote-support/getting-started/admin/security.htm>.

Werkzeuge für den Dateitransfer

	Stoppen Sie den Zugriff auf das Dateisystem des Remote-Geräts.
	Ein Verzeichnis im ausgewählten Dateisystem nach oben wechseln.
	Ihre Ansicht des ausgewählten Dateisystems aktualisieren.
	Ausgeblendete Dateien anzeigen.
	Ein neues Verzeichnis erstellen.
	Laden Sie eine Datei in ein Verzeichnis hoch.
	Laden Sie ausgewählte Dateien aus einem Verzeichnis herunter.
	Modifikatortasten umschalten.
	Text in der Zwischenablage an Remote-System senden.
	Text aus der Zwischenablage vom Remote-System abrufen / Text oder Dateien aus der Zwischenablage vom Remote-System (RDP) abrufen.
	Löschen Sie ausgewählte Dateien aus einem Verzeichnis.
	Fahren Sie mit der Maus über ein Element und klicken Sie, um mehr Optionen zu erhalten. So können Sie ein Verzeichnis oder eine Datei herunterladen, umbenennen oder löschen.



Hinweis: Die Löschung einer Datei oder eines Verzeichnisses ist nicht widerrufbar. Die Datei bzw. der Ordner wird nicht in den Papierkorb geworfen.

RDP-Dateitransfer

Dateien herunterladen

Sie können Dateien während RDP-Sitzungen übertragen, indem Sie **Strg+C** zum Kopieren in die Zwischenablage verwenden, mit der rechten Maustaste auf **Kopieren** in einem Kontextmenü klicken oder auf eine Kopierschaltfläche in der Explorer-Symbolleiste klicken. *Diese Dateien werden in die Zwischenablage des Endpunkts kopiert*

Das Kopieren von Dateien oder Verzeichnissen auf dem entfernten Endpunkt löst einen Dateidownload in Ihrem Browser aus. Die ausgewählte Datei wird in den Ordner heruntergeladen, den Sie auf Ihrem Computer angegeben haben. Je nach den Einstellungen Ihres Browsers werden Sie möglicherweise aufgefordert, einen Download-Ort anzugeben.



Dateien hochladen

Das Hochladen von Dateien in die Web-Konsole des Support-Technikers ist ein zweistufiger Prozess:

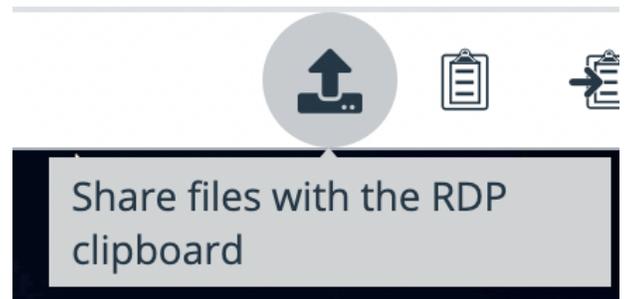
1. Teilen Sie dem Browser mit, welche Dateien Sie für die Remote-Zwischenablage freigeben möchten.
2. Führen Sie ein „Einfügen“ am Remote-Endpunkt durch.

Es gibt zwei Möglichkeiten, dem Browser mitzuteilen, welche Dateien freigegeben werden sollen:

1. Klicken Sie auf eine Schaltfläche in der Symbolleiste, die eine Standardauswahl für Systemdateien anzeigt, ähnlich wie beim Hochladen von Dateien auf der Registerkarte „Dateiübertragung“.
2. Ziehen Sie Dateien in die Ansicht für die Bildschirmfreigabe.

Nachdem Sie eine dieser Methoden ausgewählt haben, werden Sie durch eine Toast-Benachrichtigung am unteren Rand der Seite daran erinnert, die Daten auf dem Remote-Endpunkt einzufügen.

Nach dem Einfügen am Endpunkt zeigt Windows den Fortschritt der Übertragung in einem Dialogfeld am Endpunkt an und bietet eine Schaltfläche zum Abbrechen.

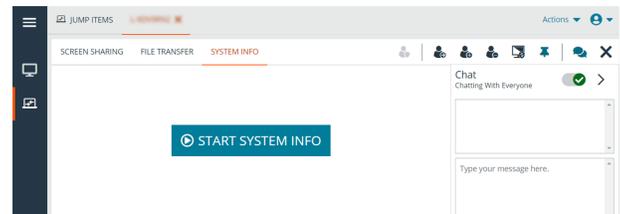


Hinweis: Wenn Sie mehr als eine Datei mit der Dateiauswahl oder durch Drag & Drop auswählen, bevor Sie die vorherige Dateiauswahl am Endpunkt einfügen, wird die zuerst ausgewählte Datei überschrieben.

Anzeige von Systeminformationen am Remote-Endpunkt

Remote Support-Benutzer können eine komplette Momentaufnahme der Systeminformationen des Remote-Geräts oder -Computers anzeigen, um die Diagnose und Problemlösung zu beschleunigen. Die verfügbaren Systeminformationen hängen vom Remote-Betriebssystem und der Konfiguration ab.

1. Klicken Sie im Sitzungsfenster auf die Registerkarte **Systeminfo** am oberen Rand des Bildschirms. Sie können auf die Schaltfläche **Systeminfo starten** klicken, wenn die Systeminformationen nicht automatisch geöffnet werden.
2. Verwenden Sie folgende Aktionen in einer Sitzung für unterschiedliche Funktionen:



Werkzeuge für Systeminformationen

	Systeminformationen aktualisieren.
	In Zwischenablage kopieren.
	In Datei speichern.

Fügen Sie über die Web-Konsole des Support-Technikers einen Support-Button hinzu

In einer Sitzung können Sie einen Support-Button am Remote-Computer bereitstellen. Dies ist eine schnelle Methode zum Anfordern von Support für Ihre Kunden. Um zu beginnen, klicken Sie auf die Schaltfläche **Support-Button bereitstellen**. Damit wird ein Menü geöffnet, in dem Sie die Support-Button-Details bearbeiten können.



Geben Sie eine Beschreibung ein, die Ihnen und anderen Support-Technikern angezeigt wird, die Zugriff auf diesen Support-Button haben.

Wählen Sie ein Profil, das auf diesen Support-Button angewandt werden soll. Profile werden unter **/login > Konfiguration > Support-Button** konfiguriert.

Wählen Sie die Warteschlange aus, mit der dieser Support-Button verknüpft werden soll. Sobald der Support-Button bereitgestellt wurde, kann Ihr Kunde diesen verwenden, um direkt in die angegebene Warteschlange aufgenommen zu werden.

Legen Sie fest, wie lange dieser Support-Button gültig sein soll. Der Kunde kann diesen Button nur innerhalb des angegebenen Zeitraums zum Starten von Sitzungen verwenden. Diese Zeit wirkt sich NICHT darauf aus, wie lange das Installationsprogramm aktiv ist oder wie lange eine Sitzung dauern kann.

Nachdem Sie die Details für diesen Support-Button festgelegt haben, klicken Sie auf **Bereitstellen**. Damit wird ein Support-Button auf dem System des Remote-Benutzers erstellt. Ihr Kunde kann den Support-Button nun verwenden, um schnell Support anzufordern.

Sie können auch den Support-Button vom Remote-System löschen, indem Sie auf die Schaltfläche **Support-Button entfernen** klicken. Wenn Sie aufgefordert werden, die Entfernung des Support-Buttons auf dem Kunden-Computer zu bestätigen, klicken Sie auf **Ja**.

ADD SUPPORT BUTTON

Select the options for deploying the Support Button to the customer.

Description	<input type="text" value="End User @ Windows® (x64)"/>	Icon Preview  Support Button [bomgar.com]
Profile	<input type="text" value="Default"/>	
Queue	<input type="text" value="Personal"/>	
Expiration	<input type="text" value="1 Month"/>	
October 20, 2021, 8:44:19 AM		
		<input type="button" value="CANCEL"/> <input type="button" value="DEPLOY"/>



Einen Jump-Client über die Web-Konsole des Support-Technikers fixieren

In einer Sitzung können Sie einen Jump-Client am Remote-Computer fixieren und somit später unüberwacht darauf zugreifen. Klicken Sie zum Beginnen auf die Schaltfläche **Den Jump-Client fixieren**. Damit wird ein Menü zur Konfiguration des Jump-Client geöffnet. 

Wählen Sie aus der Liste der verfügbaren Jump-Gruppen die Gruppe, in der Sie den Jump-Client fixieren möchten. Durch Fixieren des Jump-Client in Ihrer persönlichen Liste von Jump-Elementen können nur Sie über den Jump-Client auf diesen Remote-Computer zugreifen. Sie können den Jump-Client auch an bestimmten Jump-Gruppen fixieren, damit nur Mitglieder dieser Gruppe darauf Zugriff haben.

Wenn Sie den Jump-Client ohne Festlegen eines Passworts fixieren möchten, klicken Sie jetzt auf **Sitzung fixieren**.

Alternativ können Sie ein Passwort für diesen Jump-Client festlegen. Damit müssen alle Benutzer, die auf den Jump-Client zugreifen möchten, das richtige Passwort eingeben, bevor sie Zugang zum Remote-System erhalten. Geben Sie das gewünschte Passwort ein und klicken Sie auf **Sitzung fixieren**.

PIN AS A JUMP CLIENT

Select the queue to pin this session to as a Jump Client.

Queue

Optional Password

Confirm Password

[CLOSE](#) [PIN SESSION](#)

Wenn Sie den unbeaufsichtigten Zugriff auf das Remote-System nicht mehr benötigen, entfernen Sie den Jump-Client mit der Schaltfläche **Fixierung von Jump-Client lösen**. Klicken Sie bei der Aufforderung, den Jump-Client zu deinstallieren, auf **Ja**. 

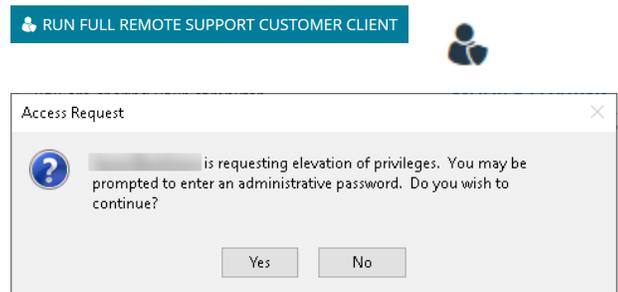
Sitzung in der Web-Konsole des Support-Technikers heraufsetzen

Wenn eine Sitzung im Click-to-Chat-Modus startet, steht nur der Chat zur Verfügung. Wenn Sie auf umfassendere Support-Features wie die Bildschirmfreigabe zugreifen möchten, müssen Sie den Kunden-Client heraufsetzen.

Wenn der heruntergeladene Kunden-Client im Benutzermodus ausgeführt wird, verfügen Sie ebenfalls möglicherweise nicht über die gewünschte Zugriffstiefe. Sie können den Kunden-Client zur Ausführung mit Administratorenrechten heraufsetzen. Damit wird er als Systemdienst ausgeführt. Die Heraufsetzung des Kunden-Clients ermöglicht den Wechsel von Benutzerkonten, die Bereitstellung von Jump-Clients im Dienstmodus und die Steuerung geschützter Fenster und UAC-Dialogfelder. Die Heraufsetzung verändert nicht den Benutzerkontext des aktiven Benutzers und gleicht nicht der Abmeldung als aktiver Benutzer und erneuter Anmeldung als Administrator.

Um von einer Click-to-Chat-Sitzung zum vollen Kunden-Client heraufzusetzen, klicken Sie auf die Schaltfläche **Vollständigen Remote-Support-Kunden-Client ausführen** in der Mitte des Bildschirms oder auf **Heraufsetzen** oben im Sitzungsfenster.

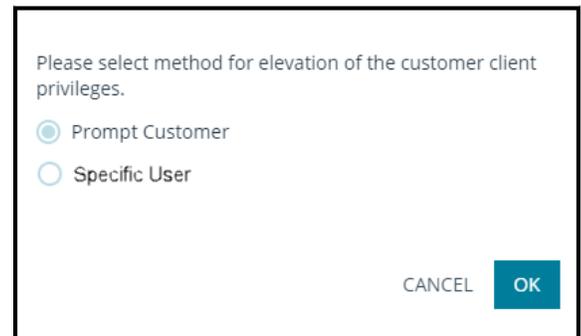
Der Kunde wird aufgefordert, den vollständigen Kunden-Client herunterzuladen und auszuführen.



Um den Kunden-Client auf Administratorrechte heraufzusetzen, klicken Sie auf die Schaltfläche **Heraufsetzen** oben im Sitzungsfenster. Eine Eingabeaufforderung für Anmeldedaten erscheint.

Um den Kunden aufzufordern, Administrator-Anmeldedaten für seinen Computer anzugeben, wählen Sie **Kunden-Eingabeaufforderung** und klicken Sie dann auf **OK**.

Wenn Sie am Remote-Computer über Administratorrechte verfügen, wählen Sie alternativ **Bestimmter Benutzer**, um selbst einen Benutzernamen und ein Passwort mit Administratorrechten anzugeben. Klicken Sie dann auf **OK**.



Über die Web-Konsole des Support-Technikers eine Sitzung auf einen anderen Support-Techniker oder ein Team übertragen

Wenn Sie der Sitzungsinhaber sind und die Steuerung der Sitzung einem anderen Team oder Support-Techniker übertragen möchten, klicken Sie auf die Schaltfläche **Übertragen**.



Wählen Sie entweder **Support-Teams** oder **Support-Techniker**. Durchsuchen Sie die Liste verfügbarer Teams oder Support-Techniker.

TRANSFER SESSION

▼ Support Teams
 Team: Remote Support
 Team: General
▼ Representatives
 Rep:

CANCEL **TRANSFER**

Wählen Sie den Ort, an den Sie die Sitzung übertragen möchten und klicken Sie auf **Übertragen**.

Wenn jemand die Sitzung akzeptiert, verbleiben Sie als Teilnehmer in der Sitzung, sind aber nicht länger der Sitzungsinhaber.

Freigabe einer Sitzung für Teammitglieder oder externe Benutzer mithilfe der Web-Konsole des Support-Technikers

Team-Mitglieder einladen

Innerhalb einer Sitzung können Sie ein Teammitglied auffordern, an einer Support-Sitzung Tech teilzunehmen. Klicken Sie zum Freigeben einer Sitzung auf das Symbol **Sitzung freigeben**.



Wählen Sie im Menü einen Teamnamen, die Option **Hilfe anfordern** oder die Option **Support-Techniker**.

SHARE SESSION

▼ Support Teams
 > Team: General
 > Team: Remote Support
 > Request Help
 > Representatives

CLOSE SHARE

Wählen Sie aus der Teamliste den Benutzer, für den Sie die Sitzung freigeben möchten oder wählen Sie **Jeder Support-Techniker**. Wenn Sie den Namen eines Support-Technikers wählen, wird die Einladung an die persönliche Warteschlange dieses Support-Technikers gesandt. Wenn Sie **Jeder Support-Techniker** wählen, wird die Einladung an die Teamwarteschlange gesandt, sodass jeder einzelne Support-Techniker in der ausgewählten Warteschlange an der Sitzung teilnehmen kann. Sie können mehrere Einladungen versenden, wenn mehr Support-Techniker aus dem Team Ihrer Sitzung beitreten sollen.

Sie können **Hilfe anfordern** verwenden, um Ihre Anfrage zur Behandlung eines bestimmten Support-Problems weiterzuleiten. Nur Probleme, für die das Anfordern von Hilfe gestattet wurde, werden in dieser Liste angezeigt.

Benutzer werden nur dann hier aufgelistet, wenn sie in der Konsole angemeldet sind oder die erweiterte Verfügbarkeit aktiviert haben.

Wenn Sie berechtigt sind, Sitzungen für Benutzer freizugeben, die nicht Ihrem Team angehören, werden zusätzliche Teams angezeigt, vorausgesetzt, dass diese zumindest ein Mitglied mit aktivierter erweiterter Verfügbarkeit enthalten.

Wenn Sie einen Benutzer mit aktivierter erweiterter Verfügbarkeit einladen, erhält er eine E-Mail-Benachrichtigung.

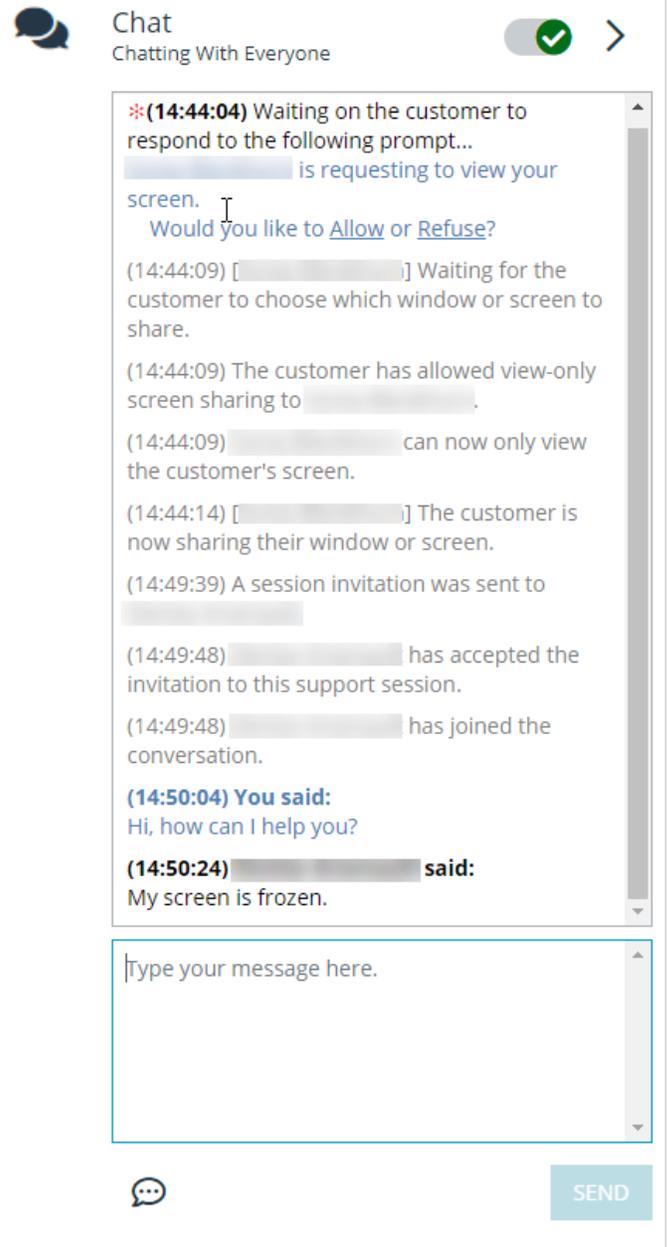
Wenn der Support-Techniker die Einladung angenommen und der Sitzung beigetreten ist, können Sie mit diesem chatten, indem Sie auf das Symbol **Chat** oben auf dem Bildschirm klicken.

Wenn Sie eine Einladung verschickt haben und diese noch aktiv ist, können Sie die Einladung zurückziehen, indem Sie sie im Menü **Einladung zurückziehen** finden und auf **Abbrechen** klicken.

Einladungen können nur vom Sitzungseigentümer verschickt werden. Solange Sie Sitzungseigentümer bleiben, laufen Einladungen nicht ab. Mehrere aktive Einladungen für den gleichen Support-Techniker zum Beitritt ein und der selben Sitzung sind nicht möglich. Die Einladung verschwindet, falls:

- Der einladende Benutzer zieht die Einladung zurück
- Der einladende Benutzer gibt das Eigentum der Sitzung ab bzw. weiter
- Die Sitzung endet
- Der eingeladene Benutzer nimmt die Einladung an
- Der eingeladene Benutzer lehnt die Einladung ab

Wenn ein weiterer Benutzer einer freigegebenen Sitzung beitrifft, kann er den Chat-Verlauf der letzten Minuten einsehen.



The screenshot shows a chat window titled "Chat" with a sub-header "Chatting With Everyone". The chat history includes:

- A system message at 14:44:04: "Waiting on the customer to respond to the following prompt... [redacted] is requesting to view your screen. Would you like to Allow or Refuse?"
- A message at 14:44:09: "[redacted] Waiting for the customer to choose which window or screen to share."
- A message at 14:44:09: "The customer has allowed view-only screen sharing to [redacted]."
- A message at 14:44:09: "[redacted] can now only view the customer's screen."
- A message at 14:44:14: "[redacted] The customer is now sharing their window or screen."
- A message at 14:49:39: "A session invitation was sent to [redacted]."
- A message at 14:49:48: "[redacted] has accepted the invitation to this support session."
- A message at 14:49:48: "[redacted] has joined the conversation."
- A message at 14:50:04: "You said: Hi, how can I help you?"
- A message at 14:50:24: "[redacted] said: My screen is frozen."

At the bottom, there is a text input field with the placeholder "Type your message here." and a "SEND" button.

Externe Benutzer einladen

Sie können einen externen Benutzer oder Anbieter zur Teilnahme an einer Zugriffssitzung einladen. Folgen Sie zur Freigabe einer Sitzung diesen Schritten:

1. Klicken Sie auf das Symbol **Andere Support-Techniker in diese Sitzung einladen**.
2. Klicken Sie auf **Externen Support-Techniker einladen....**

3. Wählen Sie ggf. eine Richtlinie aus und geben Sie eine kurze Beschreibung für die Art der Einladung ein.
4. Geben Sie im Bereich **Einladungsparameter** den Namen der einzuladenden Person und einige Kommentare ein, die mit der Einladung einhergehen sollen.
5. Klicken Sie auf **Schlüssel erstellen**.

SHARE SESSION

Invite External Representative...
> 👤 Support Teams

CLOSE

INVITE

INVITE EXTERNAL REPRESENTATIVE

• *Required field*

Select Policy

Allowed to Pin

Description

Invitation Parameters

Representative's Name •

George

Comments •

Need help with the new server

CANCEL

CREATE KEY

Sie können nun einen externen Benutzer einladen, indem Sie entweder auf das Symbol **In die Zwischenablage kopieren** klicken und dem Benutzer den Link zur Sitzungs-URL zur Verfügung stellen oder indem Sie eine E-Mail-Einladung senden.

REP INVITE SESSION KEY GENERATED

You may invite a representative to your session by requesting them to enter the following session key on your Support Portal, by sending them directly to the following URL, or by emailing an invitation.

Public Site

Default: 

Session Key

7213 6688 6687 

URL

https://ak=807b1d4bc9ab9c: 

CLOSE

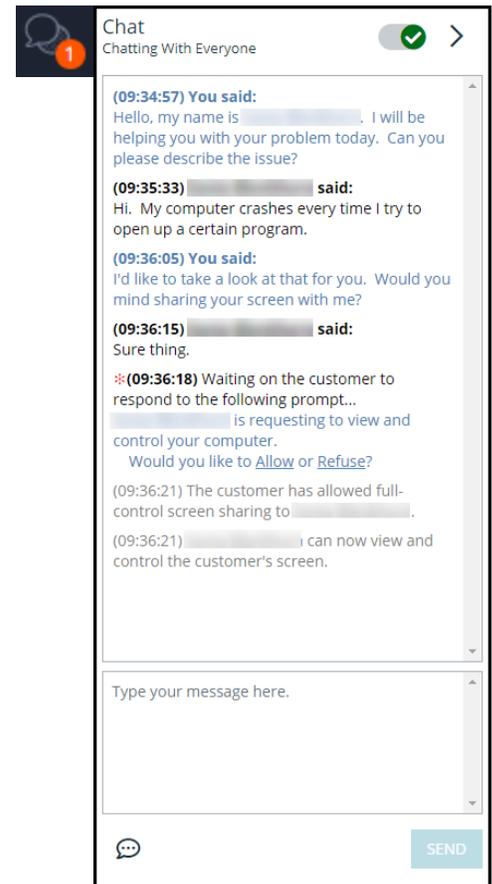
SEND LOCAL EMAIL

Über die Web-Konsole des Support-Technikers mit dem Remote-Benutzer chatten

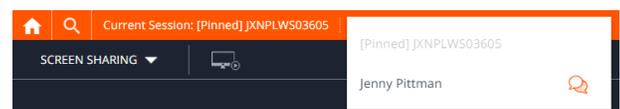
Während der gesamten Support-Sitzung Tech können Sie mit Ihrem Remote-Kunden chatten. Sie benötigen *keine* Erlaubnis für eine Bildschirmfreigabe, bevor Sie den Chat starten.

Wenn Sie eine Nachricht erhalten, während der Chat minimiert ist, zeigt das Chatsymbol die Anzahl der wartenden Nachrichten an. Klicken Sie auf die Schaltfläche **Chat**, um den Chatbereich zu öffnen oder zu schließen.

Sie können auch mit anderen Support-Technikern chatten, für die die Sitzung freigegeben wurde.



Wenn Sie sich in einer Sitzung befinden und eine Chatnachricht in einer anderen Sitzung erhalten, erscheint ein Chatsymbol im Dropdown-Menü der aktiven Sitzung oben auf dem Bildschirm. Wenn Sie das Dropdown-Menü öffnen, erscheint ein Chatsymbol rechts neben jeder Sitzung, in der eine Chatnachricht wartet.



Sitzung in der Web-Konsole des Support-Technikers schließen

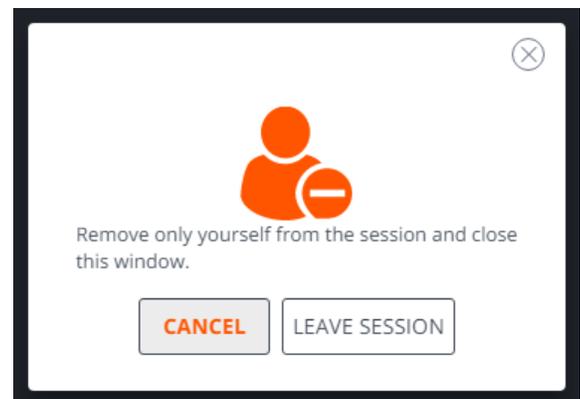
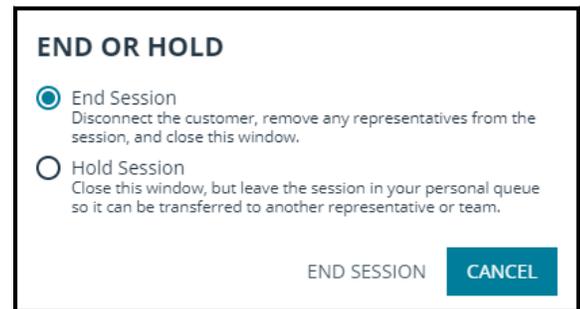
Um eine Sitzung zu verlassen, klicken Sie auf das **X**-Symbol oben rechts auf dem Bildschirm. Eine Bestätigungsaufforderung erscheint.



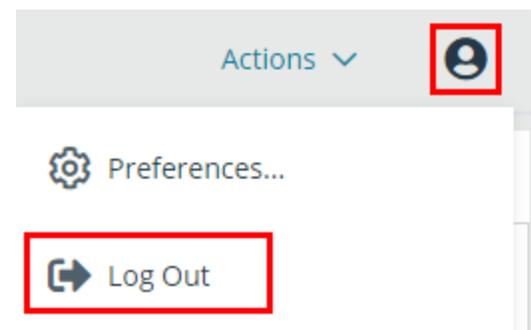
Wenn Sie der Sitzungseigentümer sind, schließt **Sitzung beenden** die Sitzung in der Konsole d. Support-Technikers und entfernt jegliche zusätzliche Support-Techniker, für welche die Sitzung möglicherweise freigegeben wird. Außerdem wird der Kunden-Client vom Remote-System deinstalliert. Ein installierter Jump-Client wird jedoch nicht gelöscht.

Wenn Sie **Sitzung pausieren** wählen, wird Ihre Sitzung in der Konsole d. Support-Technikers geschlossen, aber die Sitzung wird wieder in Ihre persönliche Warteschlange aufgenommen. Wenn die Sitzung für zusätzliche Support-Techniker freigegeben wurde, verbleiben diese in der Sitzung.

Wenn Sie nicht der Sitzungseigentümer sind, werden Sie mit **Sitzung verlassen** aus der Sitzung entfernt. Die Sitzung wird weiterhin durch den Sitzungseigentümer fortgesetzt.



Um sich vollständig von der Web-Konsole des Support-Technikers abzumelden, tippen Sie auf das Menüelement **Abmelden** im **Benutzermenü** in der oberen rechten Ecke des Bildschirms.



Sie werden sofort abgemeldet und eine Meldung erscheint, die diesen Status bestätigt.