BeyondTrust

Remote Support 21.1
Handbuch für Support-Techniker

TC:4/22/2021

Table of Contents

BeyondTrust Konsole d. Support-Technikers

Dieser Leitfaden soll Ihnen helfen, die BeyondTrust Konsole d. Support-Technikers auf Ihrem Computer zu installieren und die Funktionen zu verstehen. BeyondTrust ermöglicht Ihnen die Unterstützung Ihrer Kunden per Remote-Zugriff, indem Sie sich über den Secure Remote Access Appliance mit ihnen verbinden.

Konsole des Support-Technikers installieren

Wechseln Sie in einem beliebigen Webbrowser zur URL Ihres Secure Remote Access Appliance, gefolgt von **/login** und dem Benutzernamen sowie dem von Ihrem Administrator festgelegten Kennwort. Bei der ersten Anmeldung werden Sie unter Umständen aufgefordert, das Kennwort zu ändern.

Auf der Seite **Mein Konto** können Sie die BeyondTrust Konsole d. Support-Technikers herunterladen und installieren. Es wird standardmäßig das jeweilige Installationsprogramm für Ihr Betriebssystem verwendet.

> ***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.*

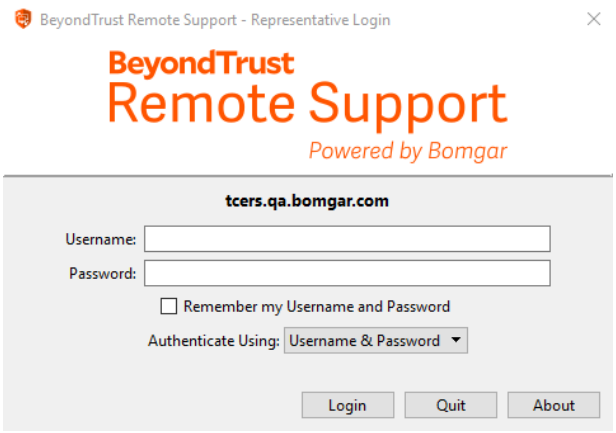
Befolgen Sie zur Installation der Software die Anweisungen im angezeigten Installationsassistenten. Nach Installation der Konsole d. Support-Technikers können Sie **Konsole d. Support-Technikers jetzt ausführen** und **Beim Start ausführen** wählen. Klicken Sie dann auf **Fertigstellen**.

> ***Hinweis:*** *Wenn Sie während der Installation* ***Konsole d. Support-Technikers jetzt ausführen*** *wählen, erscheint auf dem Bildschirm eine Anmeldeaufforderung.*

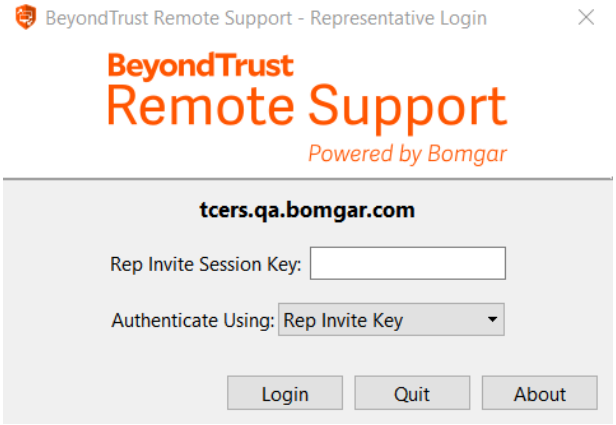
Anmelden in der Konsole des Support-Technikers

Starten Sie nach dem Installieren der BeyondTrust Konsole d. Support-Technikers die Konsole aus dem Ordner, den Sie während der Installation angegeben haben.

> ***Hinweis:*** *Standardmäßig können Sie in Windows über* ***Startmenü > Alle Programme > BeyondTrust > support.beispiel.com*** *auf die Konsole zugreifen, wobei* ***support.beispiel.com*** *der Hostname der Website ist, von der Sie die Konsole heruntergeladen haben.*

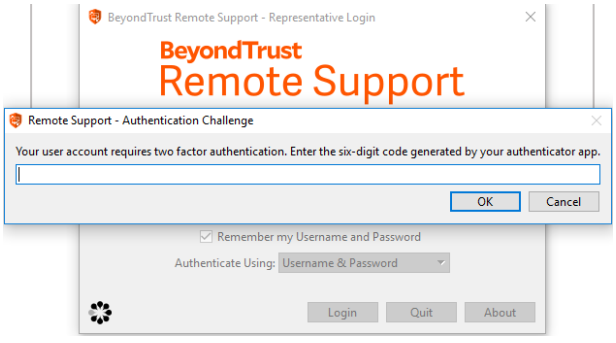


Geben Sie bei der Eingabeaufforderung Ihren Benutzernamen und Ihr Kennwort ein.

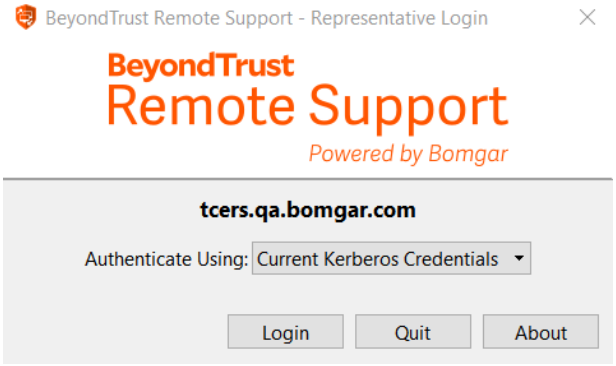


Wenn die Zwei-Faktor-Authentifizierung für Ihr Konto aktiviert wurde, geben Sie den Code der Authentifikator-App ein.

> ***Hinweis:*** *Benutzer, die zuvor E-Mail-Codes zur Anmeldung erhielten, werden automatisch auf Zwei-Faktor-Authentifizierung (2FA) aufgestuft. Sie können jedoch weiterhin E-Mail-Codes nutzen, bis sie eine App registrieren. Nach der erstmaligen Verwendung von 2FA wird die E-Mail-Code-Option dauerhaft deaktiviert.*



Alternativ kann Ihr Administrator einen Kerberos-Server konfiguriert haben, um die Einzelanmeldung zu ermöglichen. Sie können sich dann ohne Eingabe Ihrer Anmeldedaten in der Konsole anmelden. Die Konsole d. Support-Technikers merkt sich den zuletzt verwendeten Anmeldemechanismus – seien es lokale Anmeldedaten, Kerberos oder ein anderer Sicherheitsanbieter.



Eingeladene Benutzer können auch einen Sitzungsschlüssel eingeben, um einmalig einer freigegebenen Sitzung beizutreten.

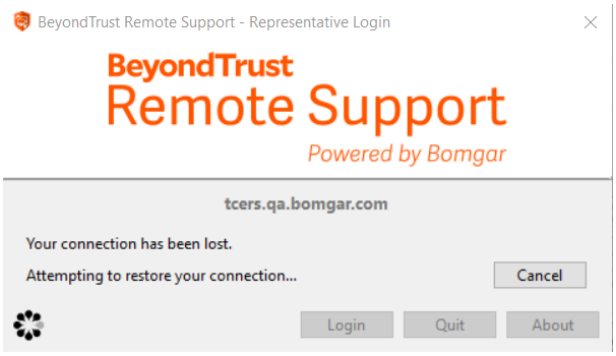
Aktivieren Sie **Meine Anmeldeinformationen speichern**, damit die Konsole Ihren Benutzernamen und Ihr Kennwort speichert. Diese Option kann über **/login > Verwaltung > Sicherheit** aktiviert bzw. deaktiviert werden.

Wenn Sie für Ihre Seite mehrere Sprachen aktiviert haben, wählen Sie die gewünschte Sprache aus der Dropdown-Liste neben dem Weltkugel-Symbol. Wenn Sie die gewählte Sprache nach der Anmeldung ändern möchten, müssen Sie sich erneut abmelden, um eine andere Sprache zu wählen.

Nach der Anmeldung öffnet sich die Konsole, und ein BeyondTrust-Symbol erscheint im Infobereich Ihres Computers. Wenn Sie die Konsole schließen, sich aber nicht abmelden, können Sie das Fenster durch Doppelklicken auf das Symbol im Infobereich oder durch Klicken mit der rechten Maustaste auf das Symbol und Auswählen von **Fenster anzeigen** wieder öffnen.

Hinweis: *Ihr Administrator kann von Ihnen fordern, sich mit Netzwerk mit uneingeschränktem Zugriff zu verbinden, um sich an der Konsole anmelden zu können. Diese Netzwerkeinschränkung gilt möglicherweise nur für die erste Anmeldung oder aber jedes Mal. Diese Einschränkung gilt nicht für Support-Techniker-Einladungen.*

Sollte die Verbindung abbrechen, versucht die Konsole d. Support-Technikers 60 Sekunden lang, die Verbindung wieder aufzubauen. Wenn Ihre Verbindung innerhalb dieser Zeit wieder aufgebaut ist, wird die Konsole d. Support-Technikers erneut geöffnet und alle Ihre offenen Sitzungen werden wiederhergestellt. Wenn die Verbindung nicht innerhalb dieser Zeit wiederhergestellt werden kann, fallen Ihre Sitzungen entsprechend der unter **/login > Konfiguration > Optionen** festgelegten Regeln zurück und Sie werden aufgefordert, sich erneut anzumelden oder die Konsole zu beenden.



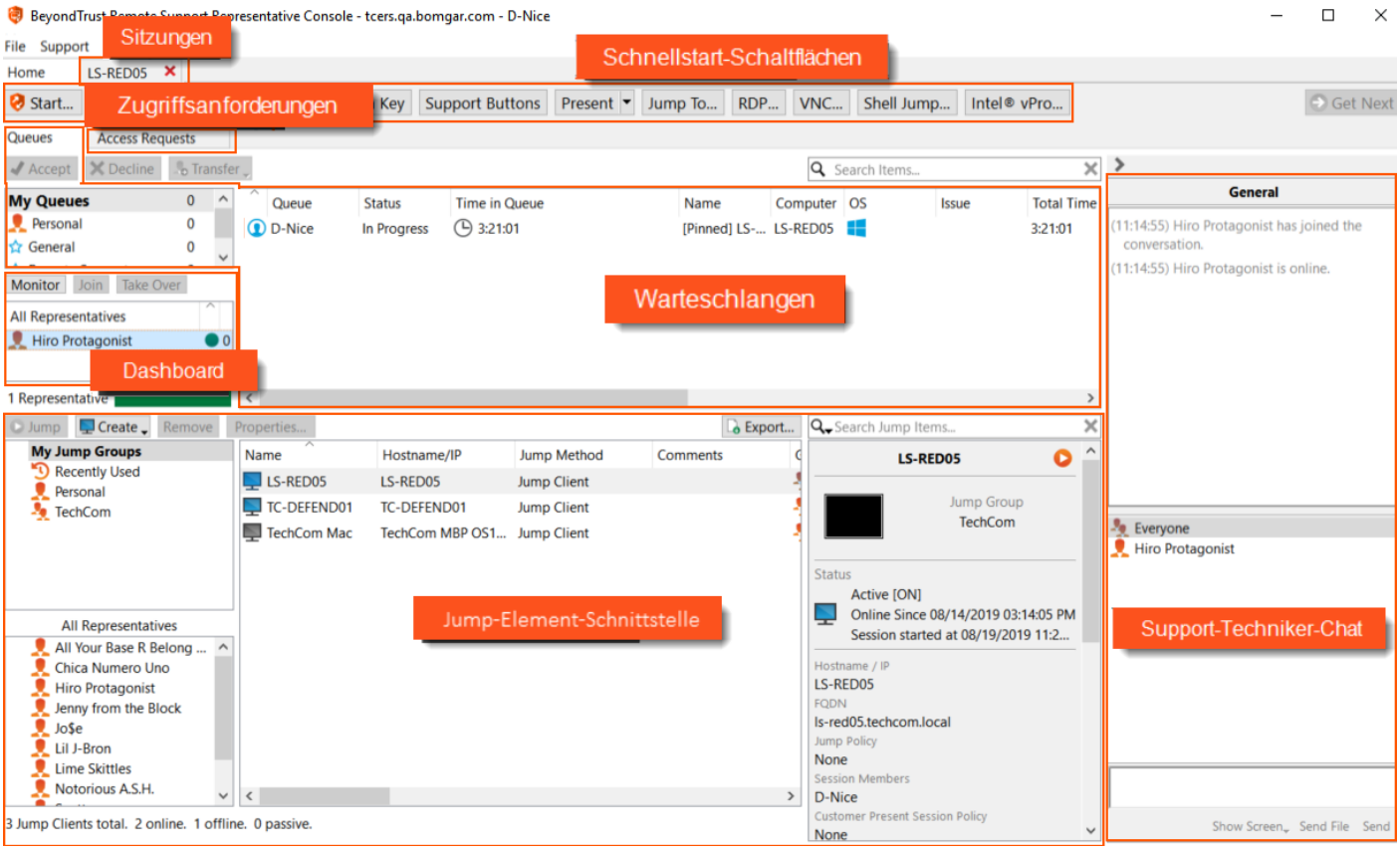
Wenn Sie an einem Ort an der Konsole d. Support-Technikers angemeldet sind und sich dann einem anderen Ort anmelden, werden offene Sitzungen beibehalten.

Hinweis: *Um sich mit einem bereits verwendeten Konto anzumelden und die Verbindung auf dem anderen System zu schließen, muss die Einstellung* ***Sitzung abbrechen, wenn Konto verwendet wird*** *auf der Seite* ***/login > Verwaltung > Sicherheit*** *aktiviert werden.*

Nach einem Upgrade oder bei der ersten Inbetriebnahme der Desktop-Konsole d. Support-Technikers wird bei allen nicht eingeladenen Support-Technikern nach der Anmeldung automatisch das Dialogfenster **Was ist neu?** angezeigt. Dieses Dialogfenster kann jederzeit über **Hilfe > Was ist neu?** aufgerufen werden und enthält Informationen zu aktuellen und vergangenen Versionen. Hierbei handelt es sich um eine kontoabhängige Roaming-Präferenz; daher wird das Dialogfenster ungeachtet dessen, von wo aus sich ein Support-Techniker anmeldet, nur ein einziges Mal angezeigt.

Weitere Informationen zu eingeladenen Benutzern finden Sie in Einladung für Support-Techniker: Erstellen Sie Profile, um externe Support-Techniker zu Sitzungen einzuladen unter https://www.beyondtrust.com/docs/remote-support/getting-started/admin/rep-invite.htm.

Benutzerschnittstelle der Konsole des Support-Technikers



Sitzungen: Verwalten Sie mehrere Remote-Sitzungen gleichzeitig.

> ***Hinweis:*** *Sitzungsreiter können verschoben und neu geordnet werden, damit Sie Ihr Arbeitspensum organisieren und priorisieren können. Ziehen Sie einfach einen Sitzungsreiter in eine neue Position. Sitzungsreiter können zudem vom Konsole d. Support-Technikers-Hauptfenster gelöst werden.*

Schnellstart-Schaltflächen: Leicht auf häufig benötigte Werkzeuge zugreifen. Schnellstart-Schaltflächen können über **Datei > Einstellungen** aktiviert oder deaktiviert werden.

- **Start**: Öffnen Sie einen Dialog, um die Kurzanleitung über das Starten einer Sitzung einzusehen.
- **Sitzungsschlüssel**: Sitzungen mit zufällig generierten, einmal verwendbaren Sitzungsschlüsseln beginnen.
- **Support Buttons**: Details und Nutzungsstatistiken für bereitgestellte Support Buttons anzeigen.
- **Präsentation**: Ihren Bildschirm für einen oder mehr Remote-Teilnehmer freigeben. Sie können eine Präsentation sofort starten oder für ein späteres Datum einplanen.
- **Jump zu**: Durchführen eines Jumps zu einem Computer in einem Remote-Netzwerk über Jumpoint oder in Ihrem lokalen Netzwerk. Die Jump-Technologie von BeyondTrust ermöglicht berechtigten Support-Technikern, eine Verbindung mit einem unüberwachten Remote-Computer herzustellen und eine Sitzung zu beginnen, ohne dass der Endbenutzer dabei mithilft.
- **RDP**: Starten Sie eine Remote-Desktop-Protokoll-Sitzung mit einem Remote-Windows-System.

- **VNC**: Starten Sie eine VNC-Sitzung mit einem Remote-Windows-System.
- **Shell Jump**: Stellen Sie über einen bereitgestellten Jumpoint schnell eine Verbindung mit SSH- und Telnet-fähigen Netzwerkgeräten her.
- **Intel® vPro**: Mithilfe der Intel®Active Management-Technologie können Sie vollständig bereitgestellte Intel®vPro-Windows-Systeme unterhalb der Betriebssystemebene unterstützen.

Warteschlangen: In der Warteschlange werden Kunden angezeigt, die entweder auf Support warten oder die sich in einer Sitzung befinden. In diesem Abschnitt werden Details zum Remote-System angezeigt, das unterstützt wird.

Dashboard: Mit dem Dashboard können berechtigte Benutzer laufende Sitzungen und Teammitglieder einer niedrigeren Rolle anzeigen und überwachen, wodurch sie eine administrative Aufsichtsfunktion einnehmen und Personal besser unterstützen können. Statusindikatoren zeigen, ob Support-Techniker verfügbar, inaktiv oder beschäftigt sind oder die automatische Zuweisung ausgeschaltet haben. Eine Leiste unten am Dashboard zeigt den Prozentsatz der Support-Techniker mit jedem Status.

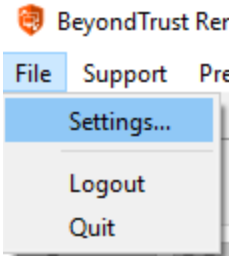
Zugriffsanforderungen: Ist ein Support-Techniker ein Sponsor in einer oder mehreren Zugriffssponsorengruppen, wird er die Registerkarte Zugriffsanforderungen in der Konsole d. Support-Technikers sehen. Erstellt ein Support-Techniker eine Anforderung, sehen alle Sponsoren in der ausgewählten Zugriffssponsorengruppe eine neue Anforderung auf der Registerkarte Zugriffsanforderungen der Konsole d. Support-Technikers.

Jump-Element-Schnittstelle: Installierte Jump-Clients und symbolische Jump-Links erscheinen hier, gruppiert nach Zugriff.

Support-Techniker-Chat: Chatten Sie mit anderen angemeldeten Benutzern. Sie können außerdem Ihren Bildschirm für ein Teammitglied freigeben, ohne dass eine Sitzung notwendig ist.

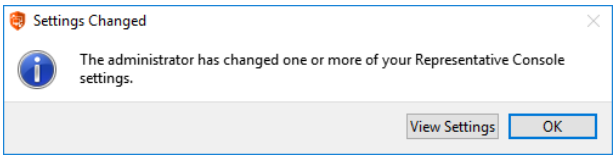
Einstellungen und Voreinstellungen in der Konsole des Support-Technikers ändern

Klicken Sie auf **Datei > Einstellungen** oben links in der Konsole, um Ihre Präferenzen festzulegen.



Allgemein können Sie die Einstellungen für die Konsole ensprechend Ihren Wünschen konfigurieren. Ihr BeyondTrust-Administrator kann jedoch entscheiden, die Verwaltung Ihrer Einstellungen zu übernehmen und diese verwalteten Einstellungen falls erwünscht zu erzwingen.

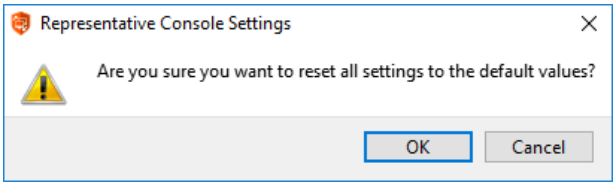
Wenn Ihr BeyondTrust-Administrator die Standardeinstellungen geändert und übernommen hat, erscheint eine Alarmmeldung, dass **Einstellungen geändert** wurden, wenn Sie sich das nächste Mal in der Konsole anmelden. Klicken Sie auf **Einstellungen anzeigen**, um Ihr Einstellungsfenster zur Anzeige der Änderungen zu öffnen, oder klicken Sie einfach auf **OK**, um die Änderungen zu akzeptieren.



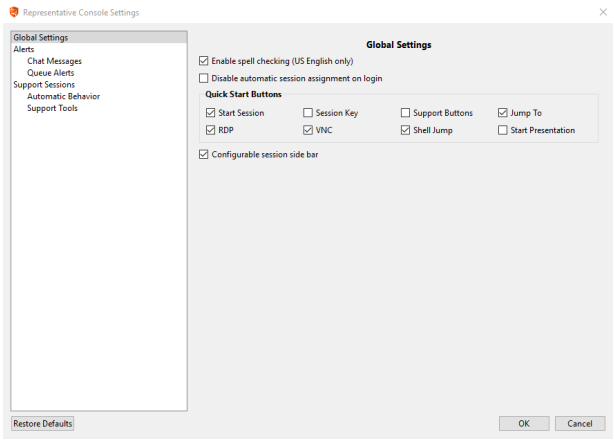
Einstellungen ändern

> ***Hinweis:*** *Diese Anweisungen gehen davon aus, dass Sie berechtigt sind, die für Ihre Konsole verwendeten Einstellungen zu wählen. Die von Ihrem Administrator erzwungenen Einstellungen erscheinen grau und mit Sternchen markiert. Diese sind nicht lokal konfigurierbar. Wenden Sie sich an Ihren Administrator oder lesen Sie den Abschnitt Einstellungen der Konsole d. Support-Technikers im Benutzerhandbuch für Administratoren für weitere Informationen.*

Jedes Fenster für die Einstellungen der Konsole umfasst untenl inks eine Schaltfläche **Auf Standardeinstellungen zurücksetzen**. Wenn Sie auf die Schaltfläche klickne, werden all Ihre Einstellungen auf die BeyondTrust-Standardeinstellungen oder die von Ihrem Administrator festgelegten Standardeinstellungen (falls zutreffend) zurückgesetzt. Ein Warndialog bittet Sie um Bestätigung, dass Sie zurück zu den Standardeinstellungen wechseln möchten. Klicken Sie auf **Abbrechen**, wenn Sie zu Ihren lokal gespeicherten Einstellungen zurückkehren möchten.



> ***Hinweis:*** *Bei Erzwingung von Standardeinstellungen durch Ihren Administrator ist keine Konfiguration möglich.*



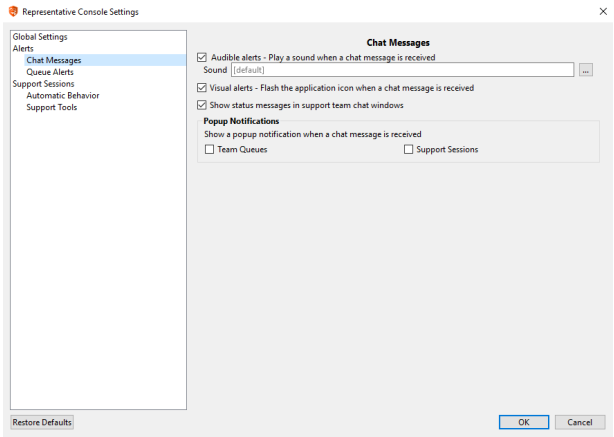
Im Abschnitt **Globale Einstellungen** können Sie die Rechtschreibprüfung für Chat und Sitzungsnotizen aktivieren oder deaktivieren. Derzeit steht die Rechtschreibprüfung nur für US-Englisch zur Verfügung.

Wird die automatische Sitzungszuweisung bei der Anmeldung deaktiviert, werden Ihnen erst automatisch Sitzungen zugewiesen, wenn Sie dem Opt-In zustimmen.

Wenn Sie unter **Schnellstartschaltflächen** die Option **Sitzungsstart** auswählen, wird oberhalb der Konsole d. Support-Technikers eine Schaltfläche **Start** angezeigt. Durch Klicken auf diese Schaltfläche können Sie die verschiedenen Möglichkeiten einsehen, mit denen Ihr Kunde eine Support-Sitzung Tech starten kann. Sie können auch **Sitzungsschlüssel** auswählen, um eine den Sitzungsschlüssel generierende Schaltfläche anzuzeigen. Wählen Sie **Support Buttonn**, um eine Schaltfläche zum Starten der Support Button-Verwaltungsschnittstelle anzuzeigen. Wählen Sie **Jump zu**, **RDP**, **VNC**, **Shell Jump** und **Intel® vPro**, um Schaltflächen zum Starten dieser Jump-Verbindungen anzuzeigen. **Präsentation starten** ermöglicht es Ihnen, leicht eine neue Präsentation zu starten.

Wählen Sie, ob das Sitzungsmenü-Symbol angezeigt werden soll, ob die Seitenleiste gelöst werden kann und ob die Widgets der Sitzungs-Seitenleiste neu angeordnet und in der Größe verändert werden können.

Ist die Echtzeit-Chatübersetzung für Ihre Website aktiviert, wählen Sie Ihre bevorzugte Chatsprache aus dem Dropdown-Menü. Damit weiß die Konsole des Support-Technikers, in welcher Sprache Sie tippen, sodass Chatnachrichten in die gewählte Sprache des Kunden übersetzt werden können und umgekehrt.

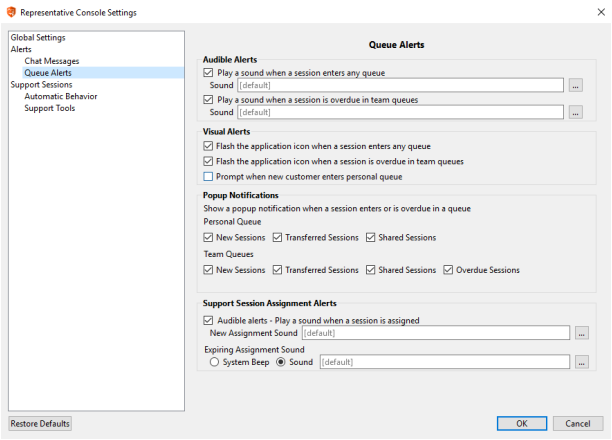


Wählen Sie Ihre Warneinstellungen für Chat-Nachrichten. Beim Erhalt einer Chat-Nachricht können Sie wählen, ob ein Sound ertönen und das Anwendungssymbol aufblinken soll.

Wenn Sie eine benutzerdefinierte Sounddatei für Chat-Nachrichten hochladen möchten, klicken Sie auf die Schaltfläche **[...]** und wählen Sie eine WAV-Datei auf Ihrem Computer aus. Die Datei darf nicht größer als 1 MB sein.

Wählen Sie, ob der Team-Chat Statusnachrichten wie die An- und Abmeldung von Benutzern enthalten soll oder nur zwischen Teammitgliedern gesendete Chatnachrichten.

Legen Sie fest, ob Sie Popup-Benachrichtigungen für in einem Team-Chat und/oder in einem Sitzungs-Chat erhaltene Nachrichten erhalten möchten.



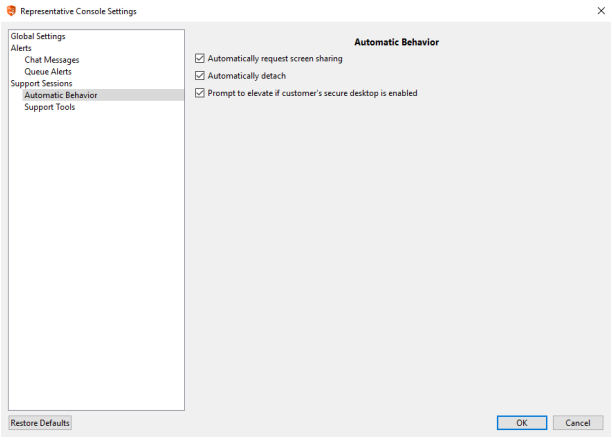
Legen Sie fest, ob Sie einen hörbaren Alarmton hören möchten, wenn ein Kunde einer Ihrer Warteschlangen hinzugefügt wurde und/oder wenn eine wartende Sitzung als überfällig markiert wurde. Wenn Sie einen benutzerdefinierten Sound für diese Alarme hochladen möchten, klicken Sie auf die Schaltfläche **[...]** und wählen Sie eine WAV-Datei auf Ihrem Computer aus. Die Datei darf nicht größer als 1 MB sein.

Sie können auch festlegen, ob das Anwendungssymbol blinken soll, wenn ein Kunde einer Ihrer Warteschlangen hinzugefügt wurde und/oder wenn eine wartende Sitzung als überfällig markiert wurde. Wird ein Kunde in Ihre persönliche Warteschlange eingereiht, indem er beispielsweise auf Ihren Namen klickt oder auf der öffentlichen Website einen Sitzungsschlüssel eingibt, kann die Sitzung sofort beginnen oder zunächst ein Auswahldialog für Sie angezeigt werden.

Sie können auch Popup-Hinweise für gewisse Ereignisse erhalten. Diese Benachrichtigungen erscheinen unabhängig von der Konsole und vor anderen Fenstern. Stellen Sie ein, wo und wie lange diese Popups angezeigt werden sollen.

Legen Sie fest, ob Sie einen Alarm hören möchten, wenn Ihnen eine Support-Sitzung Tech automatisch zugewiesen wird. Sie können einen benutzerdefinierten Sound für Sitzungszuweisungen festlegen.

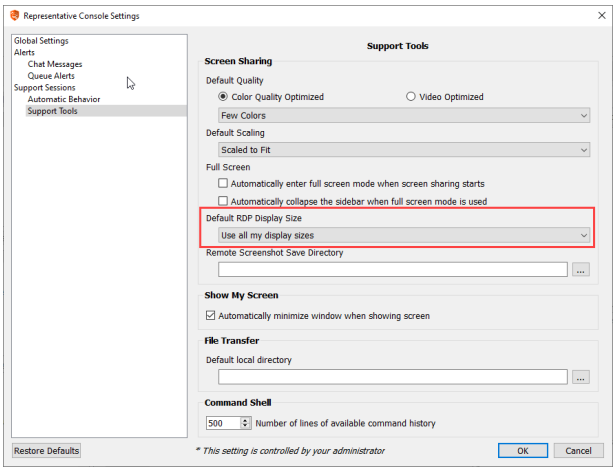
Darüber hinaus können Sie sich benachrichtigen lassen, wenn eine automatisch zugewiesene Sitzungseinladung in Kürze abläuft. Sie können einen benutzerdefinierten Sound oder **Systemton** wählen, wodurch der standardmäßige Systemsound abgespielt wird.



Wählen Sie, ob Sie Sitzungen nur im Chat starten oder sofort die Bildschirmfreigabe anfordern möchten.

Sie können Sitzungen entweder als Registerkarten in der Konsole oder aber automatisch als neue Fenster öffnen lassen.

Wenn Probleme auftreten, weil der sichere Desktop eines Kunden aktiviert ist, können Sie bei Beginn der Sitzung aufgefordert werden, auf die Ausführung mit Administratorrechten heraufzusetzen.



Legen Sie die Standardqualität und -größe für eine Bildschirmfreigabe-Sitzung fest. Wenn die Bildschirmfreigabe beginnt, können Sie automatisch den Vollbildmodus aktivieren, wodurch die Chat-Leiste wiederum automatisch ausgeblendet werden kann.

Zu Beginn der Bildschirmfreigabe kann das Remote-System auch automatisch die Anzeige, Maus- und Tastatureingabe einschränken und bewahrt so die Privatsphäre.

Wählen Sie die Standard-RDP-Anzeigegröße für alle RDP-Sitzungen aus. 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.

Legen Sie für einen einfacheren Zugriff auf Bildschirmaufnahmen, die Sie aus der Konsole machen, das Standardverzeichnis fest, in dem Ihre Remote-Screenshots aus der Konsole gespeichert werden.

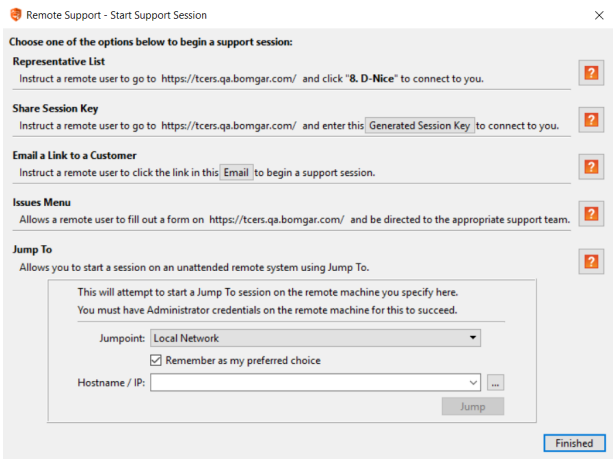
Für eine einfachere Dateiübertragung legen Sie das Standardverzeichnis fest, von dem aus Ihr lokales Dateisystem durchsucht werden soll.

Legen Sie die Anzahl der Zeilen fest, die im Befehlsshellverlauf gespeichert werden sollen.

Benutzer unterstützen

Optionen für den Start von Support-Sitzungen Tech

Klicken Sie oberhalb Ihrer Konsole d. Support-Technikers auf **Start**, um eine Kurzreferenz zu den Optionen für den Sitzungsstart anzuzeigen. Bitte beachten Sie, dass die verfügbaren Optionen je nach Website-Konfiguration und Kontoberechtigungen variieren.



Von Kunden initiierte Sitzungen

Kunden können auf mehreren Wegen eine Remote-Support-Sitzung Tech mit einem Support-Techniker initiieren.

E-Mail

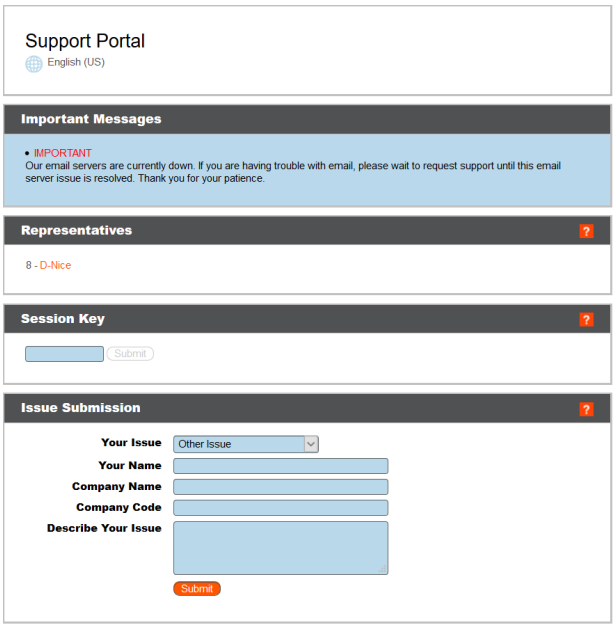
Support-Techniker können eine E-Mail-Nachricht erstellen, die einen Hyperlink erstellt. Um Support zu erhalten, klickt der Empfänger der E-Mail auf den Link, was den Download des Kunden-Client auf das System auslöst. Damit wird eine sichere Verbindung zum Support-Techniker aufgebaut, der die Einladung ausgestellt hat.

URL

Support-Techniker können eine Hyperlink-URL für den Remote-Benutzer über mehrere Methoden erstellen, wie etwa Textchat.

BeyondTrust-Web-Portal

Mit BeyondTrust können Sie Web-Support-Portale oder auch öffentliche Websites für Ihr Secure Remote Access Appliance erstellen. Diese Portale ermöglichen es Ihren Kunden, mithilfe der Remote-Support-Software von BeyondTrust Support anzufordern. Jedes Support-Portal kann an das Branding und die Support-Prozesse Ihres Unternehmens angepasst werden. Dazu gehört die Anpassung von Logos und das Starten von BeyondTrust-Sitzungen per Click-to-Chat.



Mehr über Support-Portale erfahren Sie in So passen Sie Support-Portale an unter https://www.beyondtrust.com/docs/remote-support/how-to/customize-portals/index.htm.

- **Support-Techniker**: Sie können eine Liste angemeldeter Support-Techniker anzeigen, sodass Kunden auf den Namen eines Technikers klicken können, um den Download des Kunden-Client zu starten. Wenn der Download abgeschlossen ist, wird eine Sitzung mit dem Support-Techniker gestartet.
- **Sitzungsschlüssel**: Ein Support-Techniker kann einen alphanumerischen Sitzungsschlüssel erstellen und ihn an den Kunden übermitteln. Dann kann der Kunde das Support-Portal besuchen und den Sitzungsschlüssel in ein Eingabefeld eingeben. Damit wird der Download des Kunden-Client ausgelöst und eine sichere Verbindung zum Support-Techniker, der die Einladung ausgestellt hat, wird aufgebaut.
- **Einreichen von Problemen**: Das Support-Portal kann darauf konfiguriert werden, eine Auswahl von Problemen anzuzeigen, aus denen der Kunde beim Anfordern von Support wählen kann. Kunden können ein Problem aus dem Dropdown-Menü auswählen, um den Download des Kunden-Client auszulösen. Diese Aktion erstellt eine Anforderung in der Teamwarteschlange für das jeweilige Problem. Wenn der Benutzer beispielsweise **E-Mail-Probleme** auswählt, wird die Anforderung an ein Team von Support-Technikern geleitet, die für die Unterstützung von E-Mail-Systemen besonders ausgebildet sind.

Support Button

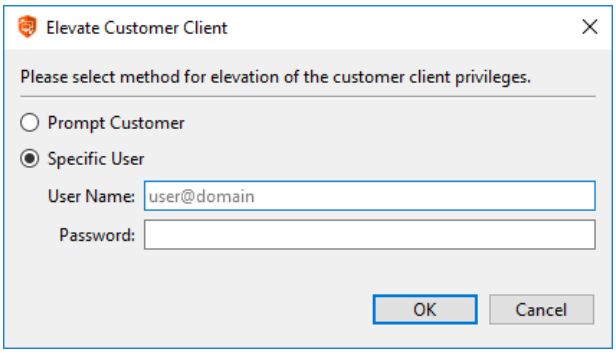
Der Support Button ist eine Desktop-Verknüpfung, die zuvor auf der Workstation eines Kunden installiert wird, um den Kunden-Client auszulösen. Wenn der Benutzer auf den Support Button klickt, wird er aufgefordert, einen Sitzungsschlüssel einzugeben oder sein Problem zu beschreiben. Darüber hinaus kann der Benutzer möglicherweise direkt zur für den Support Button konfigurierten Warteschlange hinzugefügt werden. Diese Sitzungsinitiierungsmethode kann auf ein Standard-Image vorinstalliert werden und erfordert keinen Download des Kunden-Client.

***Hinweis:** Ein Support Button kann nicht aus einer Sitzung bereitgestellt werden, die von einem SAML-authentifizierten öffentlichen Portal gestartet wurde, und ein Support Button kann nicht verwendet werden, um eine Sitzung mit einem öffentlichen Portal zu starten, das SAML-Authentifizierung erfordert.*

Weitere Informationen über Support Buttons finden Sie in Support Button: Schnell Support anfordern unter https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/support-button.htm.

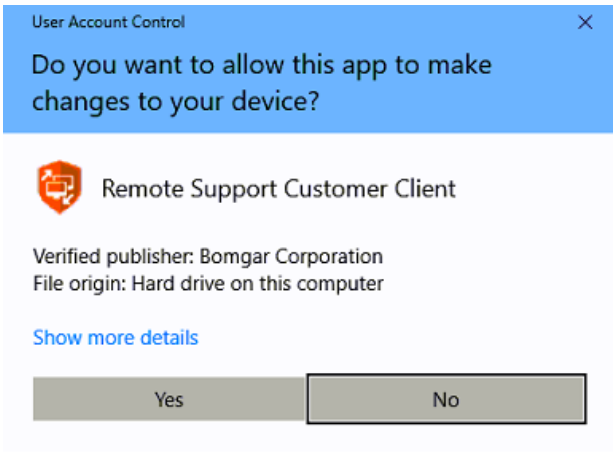
Heraufsetzung

Für jede vom Kunden initiierte Sitzungsstartmethode wird der Kunden-Client im Kontext des angemeldeten Benutzers ausgeführt. Daher entstehen beim Bereitstellen von Support im Zusammenhang mit der Windows-Benutzerzugriffssteuerung (User Access Control (UAC)) Herausforderungen. Um in diesen Situationen Support zu ermöglichen, bietet BeyondTrust die Fähigkeit, den Kunden-Client heraufzusetzen. Das bedeutet, dass der Kunden-Client, der als angemeldeter Benutzer ausgeführt wird, zu einem Systemdienst heraufgesetzt werden kann, indem Administratorbenutzerdaten angegeben werden.



Dieser Prozess erzeugt eine UAC-Aufforderung, die bei der Bildschirmfreigabe nicht sichtbar ist und vom Kunden beantwortet werden muss. Diese Aufforderung erfordert keine Endbenutzeranmeldedaten. Der Benutzer muss lediglich auf **Ja** klicken.

Nach dem Abschluss wird der Kunden-Client als Systemdienst ausgeführt. Daher sind alle nachfolgenden UAC-Aufforderungen auch bei der Bildschirmfreigabe sichtbar.



Vom Support-Techniker initiierte Sitzung

BeyondTrust Jump-Client (vorinstallierter ausgeführter Agent)

Der BeyondTrust Jump-Client ist ein ausführbarer Dienst, mit dem der Support-Techniker eine Support-Sitzung Tech für ein bestimmtes Remote-System über die Konsole des Support-Technikers initiieren kann. Dies kann zur Initiierung von Sitzungen für unüberwachte Systeme, bei denen kein Benutzer anwesend ist, und als Standardmethode für die Bereitstellung von Support verwendet werden. Obwohl die Sitzung vom Support-Techniker initiiert wird, bieten die Berechtigungen in BeyondTrust Flexibilität hinsichtlich dessen, ob Support-Techniker eine Zugriffsgenehmigung anfordern müssen, und es kann sogar auf die Präsenz eines angemeldeten Benutzers geprüft werden. Darüber hinaus kann der Zugriff auf einzelne Jump-Clients in BeyondTrustindividuell oder nach Gruppenmitgliedschaft gesteuert werden. Dabei können unterschiedliche Gruppen unterschiedliche Berechtigungen besitzen.

> *Weitere Informationen zu Jump-Clients finden Sie in Remote SupportHandbuch für Jump-Clients: Unüberwachter Zugriff auf Systeme in einem beliebigen Netzwerk unter https://www.beyondtrust.com/docs/remote-support/how-to/jump-clients/index.htm.*

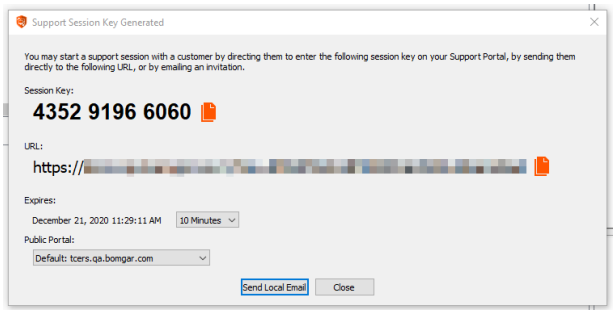
Jump zu (ad-hoc)

Die zweite vom Support-Techniker initiierte Methode zum Starten einer Support-Sitzung Tech ist die BeyondTrust-Funktion „Jump zu“. Mit „Jump zu“ können Support-Techniker die Konsole des Support-Technikers verwenden, um den Kunden-Client auf eine Remote-Workstation zu pushen und eine Support-Sitzung Tech zu initiieren. Wie auch beim Download des Client von einer Portalseite handelt es sich hier um eine Ad-hoc-Sitzung, bei der nichts vorinstalliert wird und sämtliche Dateien nach dem Ende der Sitzung entfernt werden. Im Unterschied zu den meisten anderen Methoden bestehen bei dieser Sitzungsinitiierungsmethode mehrere Einschränkungen. Zunächst einmal ist sie nur auf Windows nutzbar. Zweitens ist die Ausführung von mehreren Windows-Diensten abhängig, und mehrere Remote-TCP-Ports müssen am Remote-System offen sein. Aus diesem Grund bietet BeyondTrust eine Technologie namens Jumpoints, die die Initiierung von Sitzungen auf einem Remote-Netzwerk vereinfacht.

> *Besuchen Sie für weitere Informationen über Jumpoints bitte Remote Support Handbuch zu Jumpoints: Unüberwachter Zugriff auf Computer in einem Netzwerk unter https://www.beyondtrust.com/docs/remote-support/how-to/jumpoint/index.htm.*

Sitzungsschlüssel zum Starten einer Support-Sitzung Tech. erstellen

Je nach Ihren Kontoberechtigungen besteht eine Methode zum Starten einer Support-Sitzung Tech. darin, einmalige, zufällig generierte Sitzungsschlüssel zu verwenden. Sitzungsschlüssel werden nicht zur Authentifizierung verwenden. Sie leiten den Kunden einfach zum passenden Team oder Support-Techniker und gelten für begrenzte Zeit. Die Methoden, mit denen das Secure Remote Access Appliance Sitzungsschlüssel generiert, unterliegen dem Urheberrecht. Wenn Ihr Kunde mit einer Support-Anforderung anruft, können Sie einen neuen Sitzungsschlüssel mittels folgender Optionen erstellen:



- Das **Support**-Menü der Konsole des Konsole d. Support-Technikers
- über die Schaltfläche **Start** oben in der Konsole d. Support-Technikers
- über die Schaltfläche **Sitzungsschlüssel** oben in der Konsole d. Support-Technikers
- mit Druck auf **Strg + F4** oder **Cmd + F4**

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.

> *Weitere Informationen finden Sie unter „Maximale Zeitüberschreitung des Sitzungsschlüssels“ in Sicherheit: Verwalten der Sicherheitseinstellungen unter https://www.beyondtrust.com/docs/remote-support/getting-started/admin/security-options.htm.*

Sie können auch das öffentliche Portal auswählen, über das Ihr Kunde die Sitzung betreten soll, und zwar aus den Portalen, die Ihnen Ihr Administrator zur Verfügung stellt. Die Konsole d. Support-Technikers merkt sich die Auswahl, wenn Sie das nächste Mal einen Sitzungsschlüssel erstellen.

Abhängig von den von Ihrem Administrator gewählten Optionen können Sie die Einladung über Ihren lokalen E-Mail-Client, serverseitig oder via SMS versenden.

Weisen Sie Ihren Kunden an, entweder zur eindeutigen URL zu wechseln oder den Sitzungsschlüssel auf Ihrer öffentlichen Website einzugeben. Nachdem der Kunden-Client ausgeführt wurde, wird Ihr Kunde in Ihrer persönlichen Warteschlange angezeigt.

Support-Sitzungen Tech. in der Warteschlange 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.

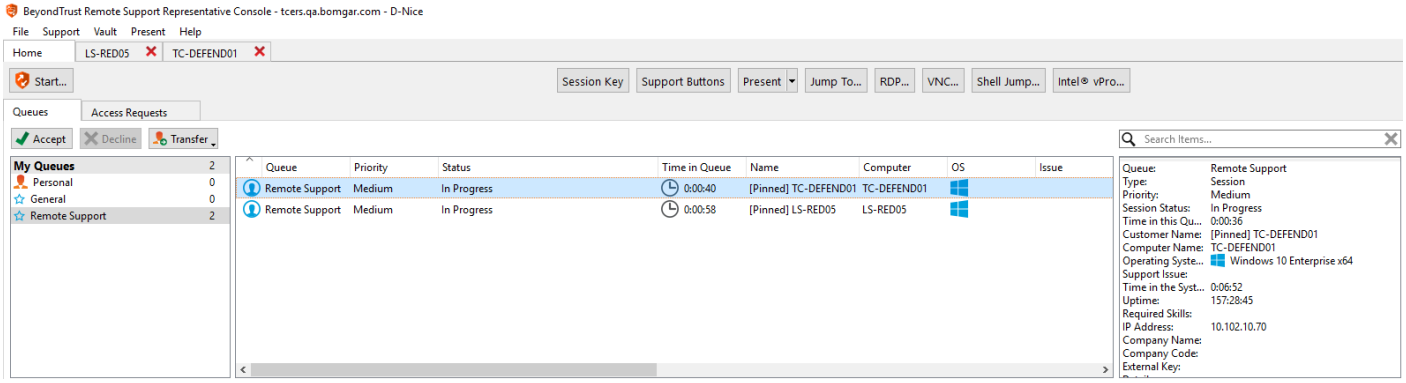
Klicken Sie auf den Stern links neben einem Teamnamen, um diese Warteschlange als Favorit zu markieren. Wenn eine Team-Chatnachricht gesandt wird, erscheint eine orange Chatblase statt des Sterns.

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.

Sortieren Sie Ihre Warteschlangen nach mehreren Kriterien wie z. B. wie lange der Kunde in der Warteschlange war, dem Namen des Kunden, der Problemkategorie usw. Je nach der Art und Weise, mit der der Kunde die Sitzung eingeleitet hat, sind unter Umständen nicht alle Kriterien verfügbar. Sie können auch nach einer aktiven Sitzung suchen. Klicken Sie auf ein Element in der Warteschlange, um Details anzuzeigen. Klicken Sie erneut darauf, um das Detailfenster zu schließen. Die Konsole d. Support-Technikers merkt sich die Sortierreihenfolge und die Sortierreihenfolge der Sitzungswarteschlange für das nächste Mal, wenn die Konsole d. Support-Technikers gestartet wird.

Befindet sich der Kunde in der Warteschlange, doppelklicken Sie auf den Kundeneintrag oder wählen Sie den Eintrag aus, und klicken Sie auf **Akzeptieren**. Durch Akzeptieren einer Sitzung wird oben in der Konsole d. Support-Technikers eine neue Registerkarte für diese Sitzung geöffnet. Sie können mehrere Sitzungen gleichzeitig ausführen. Für jede Sitzung wird eine neue Registerkarte erstellt.

Weitere Möglichkeiten der Annahme von Support-Anfragen finden Sie „Eine Sitzung zum Start des Supports akzeptieren“ auf Seite 23



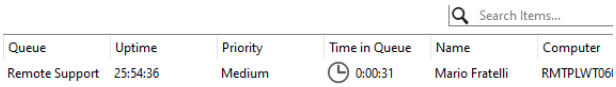
Eine Sitzung zum Start des Supports akzeptieren

Befindet sich der Kunde in der Warteschlange, gibt es mehrere Möglichkeiten, die Sitzung zu akzeptieren. Befindet sich die Sitzung in Ihrer persönlichen Warteschlange oder sind Sie berechtigt, Sitzungen aus einer Teamwarteschlange manuell zu akzeptieren, doppelklicken Sie auf den Kundeneintrag oder wählen Sie den Eintrag aus und klicken Sie auf **Akzeptieren**. Falls Sie diese Funktion verwenden dürfen, beginnen Sie mit dem Support der ältesten in die Warteschlange eingereihten Sitzung aller Ihrer Teamwarteschlangen. Dazu wählen Sie, die nächste Sitzung über folgende Optionen abzurufen:

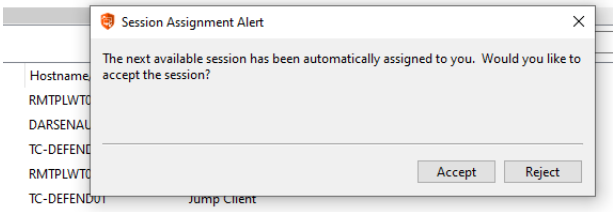
- Das **Support**-Menü der Konsole des Konsole d. Support-Technikers
- Die Schaltfläche **Nächste aufrufen** oberhalb der Konsole d. Support-Technikers

Sitzungszuweisungsregeln

Sie können auch mit Equilibrium zugewiesene Sitzungen akzeptieren. Wenn eine Sitzung in eine Warteschlange mit aktiviertem Equilibrium eingereiht wird, wird diese Sitzung automatisch dem am wenigsten beschäftigten und am besten qualifizierten Support-Techniker zugewiesen. Die Zuweisung basiert auf den passenden Qualifikationen, wie viele Sitzungen dieser Support-Techniker unterstützt und wie lange er bereits verfügbar ist.



Wenn Ihnen eine Sitzung zugewiesen wird, wird Ihnen eine Aufforderung zur Annahme oder Ablehnung der Sitzung angezeigt, zusammen mit einem hörbaren Alarm, falls aktiviert. Läuft die Einladung bald ab, werden Sie durch visuelle und Audioalarme darauf hingewiesen. Falls Sie die Einladung ablehnen oder der Zeitraum abläuft, wird die Sitzung dem nächsten am wenigsten beschäftigten und am besten qualifizierten Support-Techniker in der jeweiligen Warteschlange zugewiesen.

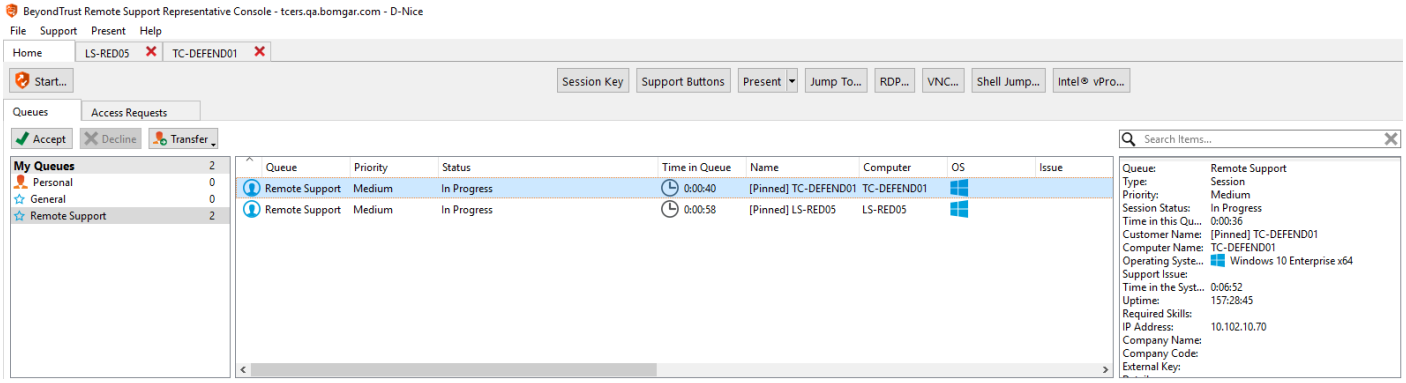


Eine abgelehnte Sitzung wird dem gleichen Support-Techniker nicht noch einmal zugewiesen, außer sie wird manuell in eine andere Warteschlange übertragen, für die dieser Support-Techniker verfügbar ist. Durchläuft eine Sitzung alle verfügbaren Support-Techniker für die Warteschlange und wird nicht akzeptiert, bleibt sie in der Warteschlange, bis jemand sie manuell akzeptiert oder überträgt.

Alternativ gibt die Sitzung, falls Ihr Administrator eine Regel für wartende Sitzungen für diese Warteschlange eingerichtet hat, einen hörbaren und sichtbaren Alarm aus, wenn die Sitzung überfällig ist, oder sie wird auf eine Überlaufwarteschlange übertragen. Wenn diese Überlaufwarteschlange über eine Regel für wartende Sitzungen verfügt, welche die Sitzung zurück auf die erste Warteschlange überträgt, kann die Sitzung möglicherweise zwischen den Warteschlangen hin- und herspringen, bis sie akzeptiert wird.

Eine Sitzung wird einem Support-Techniker nicht zugewiesen, wenn dieser nicht verfügbar ist. Wenn Sie Ihren Computer sperren oder zum Anmeldungsbildschirm wechseln, werden Sie als nicht verfügbar gekennzeichnet. Außerdem markieren Regeln in den Benutzerberechtigungen Sie als nicht verfügbar, wenn Sie an mehr als einer festgelegten Anzahl von Sitzungen teilnehmen oder länger als eine angegebene Zeit untätig waren. Wenn Sie berechtigt sind, sich per Opt-Out aus Sitzungszuweisungen auszuschließen, können Sie wählen, keine automatischen Sitzungszuweisungen zu erhalten. Automatische Zuweisung festlegen über:

- Das **Support**-Menü der Konsole des Konsole d. Support-Technikers
- Die Schaltfläche **Automatisch zuweisen** oberhalb der Konsole d. Support-Technikers
- das Rechtsklickmenü des Infobereich-Symbols



Durch Akzeptieren einer Sitzung wird oben in der Konsole d. Support-Technikers eine neue Registerkarte für diese Sitzung geöffnet. Sie können mehrere Sitzungen gleichzeitig ausführen. Für jede Sitzung wird eine neue Registerkarte erstellt.

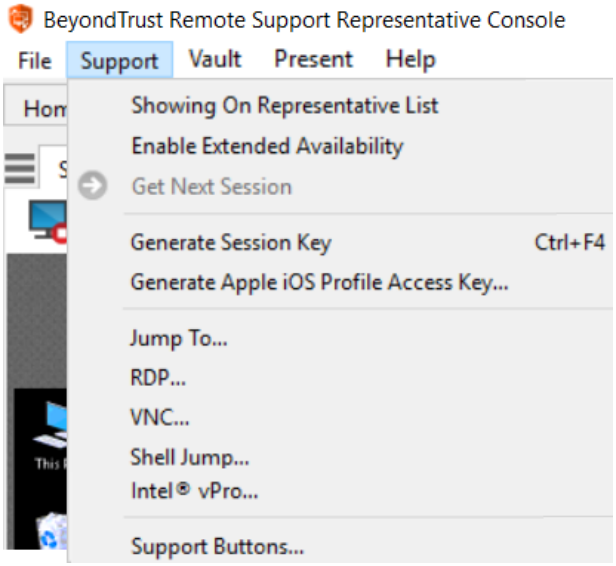
> ***Hinweis:*** *Sitzungsreiter können verschoben und neu geordnet werden, damit Sie Ihr Arbeitspensum organisieren und priorisieren können. Ziehen Sie einfach einen Sitzungsreiter in eine neue Position. Sitzungsreiter können zudem vom Konsole d. Support-Technikers-Hauptfenster gelöst werden.*

Generieren eines Apple iOS-Profilzugriffsschlüssels

Um Ihre BeyondTrust-fähigen öffentlichen und privaten Profile an Kunden mit Apple iOS-Geräten zu verteilen, generieren Sie einen Profil-Zugriffsschlüssel für Apple iOS über das Menü **Support** in der Konsole d. Support-Technikers.

Die Einstellung **iOS-Konfigurationsprofillink aktiviert** muss in **/login > Öffentliche Portale > iOS-Konfiguration** gewählt werden, damit diese Option verfügbar ist.

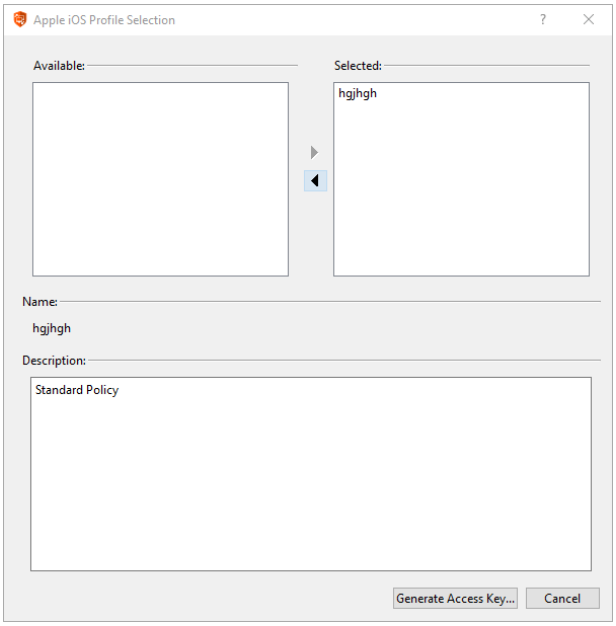
Klicken Sie auf **Apple iOS Profilzugriffsschlüssel generieren**, um die Schnittstelle **Apple iOS Profilauswahl** zu starten.



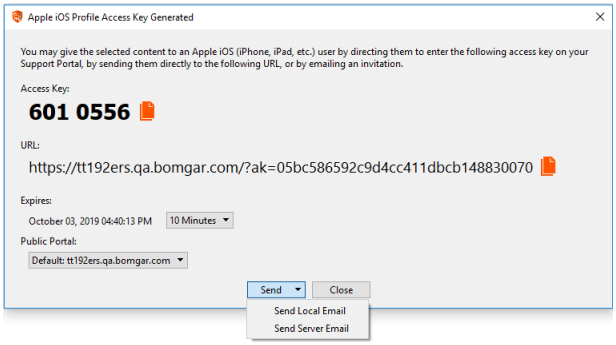
Die Schnittstelle **Apple iOS Profilauswahl** enthält verfügbare öffentliche oder private Profile, die vorab in der /login-Schnittstelle konfiguriert wurden.

Da eine öffentliche Website öffentliche iOS-Profile für jeden zugänglich macht, der die URL kennt, ist ein Zugriffsschlüssel die einzige Möglichkeit, einem Kunden Zugang zu einem privaten iOS-Profil zu gewähren.

Hier können Sie öffentliche und private Profile wählen, um sie an Ihre Kunden mit Apple iOS-Geräten über Ihr Support-Portal mit iOS-Unterstützung sicher zu verteilen. Klicken Sie auf die Schaltfläche **Zugriffsschlüssel erstellen**.



Wenn Sie auf die Schaltfläche **Zugriffsschlüssel erstellen** klicken, wird ein eigenständiger Bildschirm **Zugriffsschlüssel erstellt** geöffnet, der spezielle Optionen zum Senden einer E-Mail-Einladung an Kunden mit Apple iOS-Geräten enthält. Abhängig von den von Ihrem Administrator gewählten Optionen können Sie die Einladung über Ihren lokalen E-Mail-Client, serverseitig oder via SMS versenden.



Jump-Schnittstelle

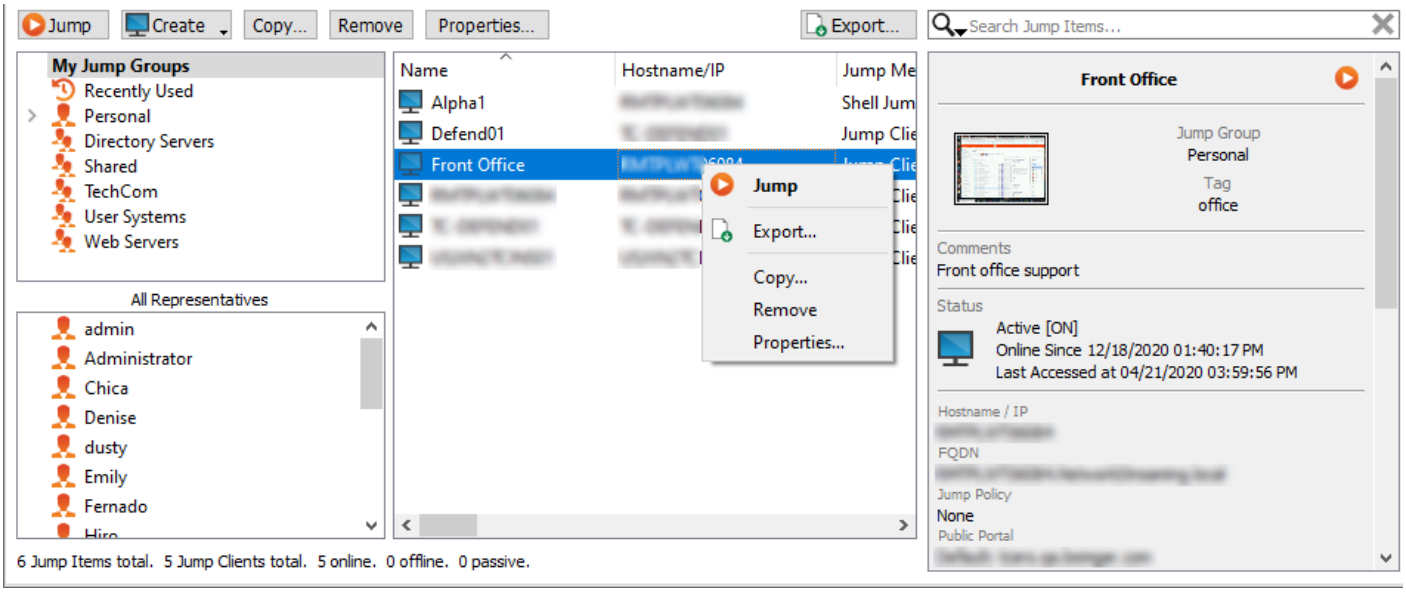
Verwenden von Jump-Elementen zum Bereitstellen von Support für Remote-Systeme

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. Ja nach Ihren Berechtigungen können Sie per Jump auf jeden beliebigen Computer in Ihrem LAN/VPN oder in einem Netzwerk mit Jumpoint-Agent wechseln. Sie können symbolische Jump-Links für häufig verwendete Systeme speichern. Um einen Jump zu einem Nicht-Windows-Computer oder einem System, das nicht mit einem Netzwerk verbunden ist, durchzuführen, können Sie einen Jump-Client installieren.

Die Jump-Schnittstelle erscheint in der unteren Hälfte der Konsole d. Support-Technikers. Die Liste kann sowohl aktive als auch passive Jump-Clients sowie Jump-Verknüpfungen für Remote-Jumps, lokale Jumps, Remote- und lokale RDP-Sitzungen, Remote- und lokale VNC-Sitzungen, Shell Jumps und Intel® vPro Jumps enthalten.

Jump-Elemente werde in Jump-Gruppen aufgeführt. Wenn Sie einer oder mehreren Jump-Gruppen zugewiesen werden, können Sie auf die Jump-Elemente in diesen Gruppen zugreifen, wobei die Berechtigungen von Ihrem Administrator festgelegt werden. Wenn Sie eine Jump-Gruppe auswählen und dann auf **Erstellen** klicken, wird die Jump-Gruppe im Jump-Element-Konfigurationsfenster automatisch ausgewählt.

Ihre persönliche Liste von Jump-Elementen ist hauptsächlich zu Ihrer persönlichen Verwendung gedacht, obwohl Ihre Teamleiter, Team-Manager und zur Ansicht aller Jump-Elemente berechtigte 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.



Jump zu einem Jump-Element durchführen

Durchsuchen Sie Gruppen oder suchen Sie dynamisch nach Computern.

Um das Durchsuchen der Liste der Jump-Clients zu erleichtern, können Sie die Spalten in jeder beliebigen Reihenfolge verschieben und eine Spalte dann durch Anklicken der Spaltenüberschrift sortieren. Die Konsole d. Support-Technikers merkt sich die Reihenfolge der Spalten und die Sortierreihenfolge für das nächste Mal, wenn die Konsole d. Support-Technikers gestartet wird.

Neben der Suche nach Jump-Clients können Sie auch anhand mehrerer Felder suchen. Geben Sie einen Suchbegriff im Suchfeld ein und drücken Sie dann die **Eingabetaste**. Um die durchsuchten Felder zu ändern, klicken Sie auf die Lupe und aktivieren oder deaktivieren Sie die verfügbaren Felder. Die durchsuchbaren Felder umfassen **Kommentare**, **Konsolenbenutzer**, **Domäne, FQDN, Gruppe**, **Hostname/IP**, **Jump-Methode**, **Letzter Zugriff**, **Name**, **Private IP**, **Öffentliche IP**, **Status**, **Tag** und **Arbeitsgruppe**.

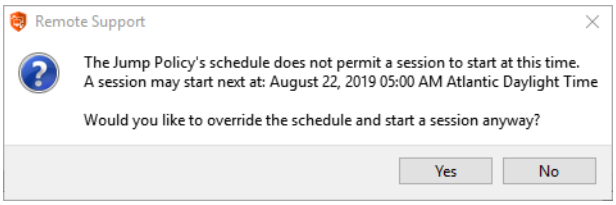
Wenn Sie den Computer gefunden haben, auf den Sie zugreifen möchten, doppelklicken Sie auf den Eintrag oder wählen Sie ihn aus und klicken Sie auf **Jump**. Dadurch wird versucht, eine Sitzung mit dem Remote-Computer zu starten.

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.*

Eine Programm-Verbindung zum Jump-Element kann direkt vom Verwaltungs- oder Ticket-Tool Ihres Systems aus hergestellt werden. Wenn Ihre Suchanfrage nur ein Jump-Element aufweist, wird die Sitzung sofort gestartet. Wenn die Suchanfrage mehrere Jump-Elemente aufweist, können Sie ein Jump-Element aus der Liste im Auswahlfenster auswählen und auf **OK** klicken.

Details zum Skripting finden Sie in Konsole d. Support-TechnikersSkripting der Konsole des Support-Technikers und Client-Skripting-API unter www.beyondtrust.com/docs/remote-support/how-to/integrations/api/client-script/index.htm.

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.*

Verwenden von Jump-Clients zum Zugriff auf unüberwachte Computer

Um auf einen einzelnen Computer ohne Endbenutzerunterstützung zuzugreifen, installieren Sie innerhalb einer Sitzung oder über die Seite **Jump-Clients** der Verwaltungsschnittstelle einen Jump-Client auf diesem System. 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.

Sortieren von Jump-Clients

Um das Durchsuchen der Liste der Jump-Clients zu erleichtern, können Sie die Spalten in jeder beliebigen Reihenfolge verschieben und eine Spalte dann durch Anklicken der Spaltenüberschrift sortieren. Die Konsole d. Support-Technikers merkt sich die Reihenfolge der Spalten und die Sortierreihenfolge für das nächste Mal, wenn die Konsole d. Support-Technikers gestartet wird.

Suche eines Jump-Clients

Neben der Suche nach Jump-Clients können Sie auch anhand mehrerer Felder suchen. Geben Sie einen Suchbegriff im Suchfeld ein und drücken Sie dann die **Eingabetaste**. Um die durchsuchten Felder zu ändern, klicken Sie auf die Lupe und aktivieren oder deaktivieren Sie die verfügbaren Felder. Die durchsuchbaren Felder umfassen **Kommentare**, **Konsolenbenutzer**, **Domäne, FQDN, Gruppe**, **Hostname/IP**, **Jump-Methode**, **Letzter Zugriff**, **Name**, **Private IP**, **Öffentliche IP**, **Status**, **Tag** und **Arbeitsgruppe**.

Detailfenster für Jump-Clients

Wenn Sie einen Jump-Client auswählen, wird ein Detailfenster rechts in der Jump-Schnittstelle angezeigt. Die hier angezeigten Details werden durch die Einstellung **Jump-Client-Statistik** in der /login-Schnittstelle sowie durch das Remote-Betriebssystem bestimmt.

Geht ein Jump-Client offline und verbindet sich nicht für die in der /login-Schnittstelle unter **Jump-Client-Einstellungen** angegebene Anzahl von Tagen erneut mit dem Secure Remote Access Appliance, gilt er als verloren. Es wird keine weitere Maßnahme bezüglich dieses Jump-Client ergriffen. Er wird nur zu Identifikationszwecken als verloren gekennzeichnet, sodass ein Administrator den Grund für die verlorene Verbindung bestimmen und Maßnahmen ergreifen kann, um das Problem zu lösen. Im Detailfenster sehen Sie das geplante Löschdatum, falls der Jump-Client nicht mehr online kommt.

Nach einer Softwareaktualisierung werden Jump-Clients automatisch aktualisiert. Die Anzahl gleichzeitiger Jump-Client-Upgrades wird durch die Einstellungen auf der Seite **/login > Jump > Jump-Clients** bestimmt. Falls ein Jump-Client noch nicht aktualisiert wurde, wird er als **Upgrade ausstehend** markiert und eine Versions- und Revisionsnummer erscheinen im Detailfenster. Sie können einen veralteten Jump-Client modifizieren, aber keinen Jump zu ihm durchführen. Der Versuch eines Jumps verschiebt diesen Jump-Client jedoch an die Spitze der Upgrade-Warteschlange.

Wake-on-Lan (WOL)

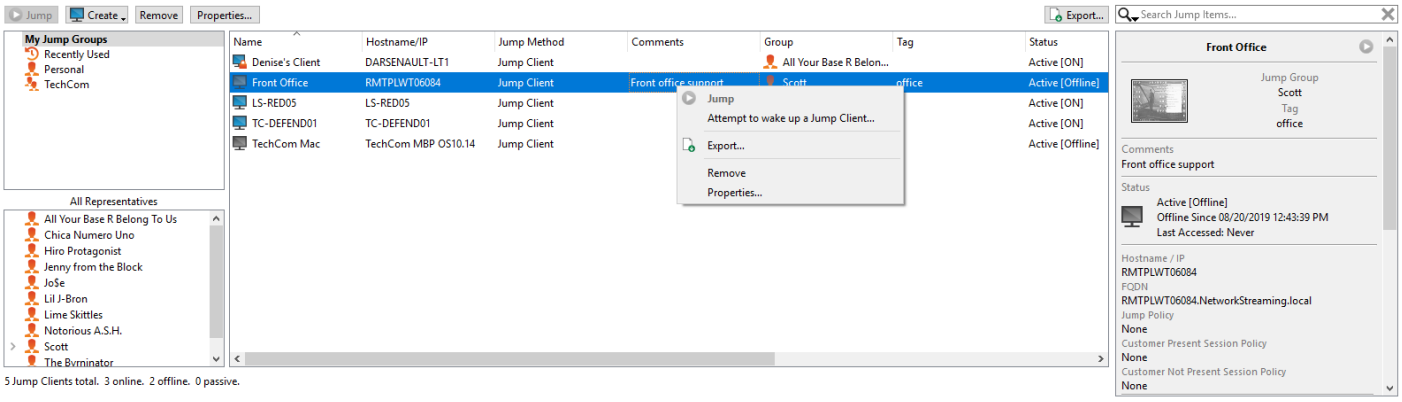
Wake-on-Lan (WOL) ermöglicht es Ihnen, für WOL konfigurierte Systeme über BeyondTrust per Remote-Zugriff einzuschalten oder aufzuwecken. In einer konfigurierten Umgebung können Kunden ihre Systeme ausschalten, aber gegebenenfalls noch immer BeyondTrust-Support erhalten.

> ***Hinweis:*** *WOL ist keine BeyondTrust-Technologie. Die BeyondTrust-Software ist mit bestehenden WOL-Systemen integrierbar. Um WOL mit BeyondTrust verwenden zu können, muss auf den System WOL aktiviert sein und das Netzwerk muss den Versand von WOL-Paketen gestatten.*

Um WOL-Unterstützung in BeyondTrust zu aktivieren, aktivieren Sie die WOL-Einstellung in der /login-Schnittstelle unter **Jump > Jump-Clients**. Beachten Sie bei Aktivierung der WOL-Option Folgendes:

- WOL funktioniert nicht bei Drahtlos-Clients. Eine kabelgebundene Verbindung ist erforderlich.
- WOL wird von der darunterliegenden Systemhardware unterstützt, die unabhängig vom installierten Betriebssystem ist.
- WOL wird nur von aktiven Jump-Clients unterstützt. Passive Jump-Clients, Jumpoints und lokale Jumps über die Konsole d. Support-Technikers unterstützen WOL nicht.

Um einen aktiven Jump-Client mit WOL aufzuwecken, rechtsklicken Sie in der Konsole d. Support-Technikers auf einen bestehenden Jump Client. Versuchen Sie, das System aufzuwecken, indem Sie auf die Option **Versuchen, einen Jump-Client aufzuwecken** klicken.



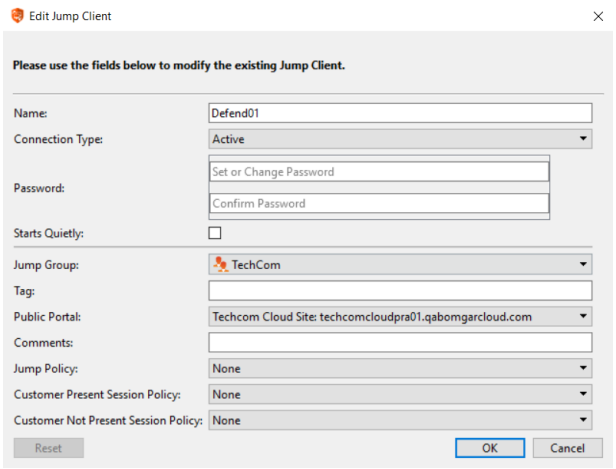
Die Aufweckoption ist nur bei Auswahl eines einzelnen Jump-Client verfügbar. Sie ist nicht verfügbar, wenn mehrere Jump-Clients ausgewählt werden.

WOL-Pakete werden von anderen Jump-Clients gesandt, die sich im gleichen Netzwerk befinden wie das Zielsystem. Wenn ein aktiver Jump-Client installiert ist oder sich eincheckt, registriert er seine Netzwerkinformationen beim Gerät. Das Gerät nutzt dann diese Informationen, um zu bestimmen, welche Jump-Clients sich im gleichen Netzwerk befinden.

Nachdem versucht wurde, einen gewählten Jump-Client aufzuwecken, wird die WOL-Option 30 Sekunden lang grau markiert, bevor eine weitere Aufweckanforderung versandt werden kann. Wenn keine anderen Jump-Clients im gleichen Netzwerk verfügbar sind, um WOL-Pakete an das Zielsystem zu senden, wird der Support-Techniker benachrichtigt, dass keine anderen Jump-Clients im Netzwerk verfügbar sind. Beim Senden eines WOL-Pakets verfügt der Support-Techniker über eine weitere Option zur Angabe eines Kennworts für WOL-Umgebungen, welche ein sicheres WOL-Kennwort erfordern. Ein WOL-Paket ist ein Ein-Weg-Paket. Der Support-Techniker erhält keine Bestätigung über die erfolgreiche Ausführung und sieht lediglich, wenn der Client in der Konsole d. Support-Technikers online geht.

Jump-Client-Eigenschaften

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



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.

Ändern Sie den Modus eines Jump-Client über das Dropdown-Menü **Verbindungstyp**. Aktive Jump-Clients senden in definierten Zeitabständen Statistiken an das Secure Remote Access Appliance. Passive Jump-Clients senden einmal täglich oder nach einem manuellen Check-in Statistiken an das Secure Remote Access Appliance. Je nach den von Ihrem Administrator festgelegten Optionen umfassen diese Statistiken die angemeldeten Konsolenbenutzer des Remote-Computers, das Betriebssystem, die Betriebszeit, die CPU, die Speicherplatzbelegung und eine Bildschirmaufnahme der letzten Aktualisierung.

Wurde für einen Jump-Client ein Kennwort festgelegt, zeigt sein Symbol, dass er gesperrt ist, und die Bildschirmaufnahme wird ebenfalls gesperrt. Um einen Jump auf einen gesperrten Jump-Client durchzuführen, müssen Sie sein Kennwort angeben. Sie müssen das Kennwort auch bereitstellen, um einen gesperrten Jump-Client über die Jump-Client-Schnittstelle zu entfernen. Das Kennwort muss nicht angegeben werden, um den Client in einer Sitzung zu lösen, da Sie das Kennwort zum Jump auf die Sitzung bereits eingegeben haben.

Ist **Lautlos starten** ausgewählt, wird der Kunden-Client nicht in den Vordergrund gebracht und verbleibt minimiert in der Taskleiste oder im Dock, wenn eine Sitzung gestartet 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 **Tag**s 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.

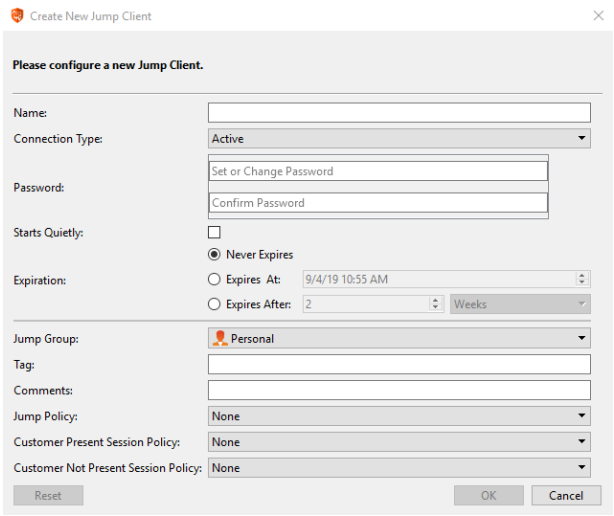
Jump-Elemente umfassen auch ein **Kommentare**-Feld für einen Namen oder eine Beschreibung, wodurch die Sortierung, Suche und Identifizierung von Jump-Clients schneller und einfacher wird.

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 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 präsente Kunden** gilt, wenn der Endbenutzer als präsent gilt. Ansonsten gilt die **Sitzungsrichtlinie für nicht präsente 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.

Beim Fixieren eines Jump-Client innerhalb einer Sitzung und Anpassen seiner Eigenschaften im Voraus haben Sie ebenfalls die Option, den Ablaufzeitpunkt für den Jump-Client festzulegen. Dies kann niemals, zu einer bestimmten Uhrzeit an einem bestimmten Tag oder nach einer bestimmten Dauer sein. Ein abgelaufener Jump-Client deinstalliert sich automatisch vom Remote-System und wird in der Jump-Client-Schnittstelle aus der Liste entfernt.



Wenn Sie den Zugriff auf ein Remote-System nicht länger benötigen, wählen Sie den Jump-Client und klicken Sie auf die Schaltfläche **Entfernen** oder rechtsklicken Sie auf den Jump-Client und wählen Sie **Entfernen** aus dem Menü. Sie können mehrere Jump-Clients auswählen, um sie gleichzeitig zu entfernen.

Hinweis: *Wenn der Remote-Benutzer einen Jump-Client manuell deinstalliert, wird das gelöschte Element entweder als deinstalliert gekennzeichnet oder komplett von der Liste der Jump-Elemente in der Konsole d. Support-Technikers entfernt. Diese Einstellung ist unter* ***/login > Jump > Jump-Clients*** *verfügbar. Wenn der Jump-Client das Secure Remote Access Appliance zum Deinstallationszeitpunkt nicht kontaktieren kann, verbleibt das betroffene Element im Offline-Zustand. Wenn ein Jump Client offline geht und sich 180 Tage lang nicht erneut mit dem Secure Remote Access Appliance verbindet, wird er automatisch vom Zielcomputer deinstalliert und aus der Jump-Schnittstelle entfernt.*

<table>
<tr><th colspan="2">Aktive und passive Jump-Clients</th></tr>
<tr><th>Aktiver Jump-Client</th><th>Passiver Jump-Client</th></tr>
<tr><td>Hält eine dauerhafte Verbindung mit dem Secure Remote Access Appliance aufrecht.</td><td>Achtet auf Remote-Zugriffsanforderungen vom Secure Remote Access Appliance.

Hinweis: Eine Konfiguration der Firewall ist möglicherweise erforderlich.</td></tr>
<tr><td>Sendet in regelmäßigen Zeitabständen Statistiken an das Secure Remote Access Appliance.</td><td>Sendet einmal täglich, nach manuellem Anmelden oder bei Anmeldung eines neuen Benutzers (sofern diese Funktion aktiviert ist), die Statistiken an das Secure Remote Access Appliance.</td></tr>
<tr><td>Ermöglicht den Fernzugriff auf jedes Desktop-Betriebssystem, das von BeyondTrust unterstützt wird.</td><td>Ermöglicht den Fernzugriff auf jedes Desktop-Betriebssystem, das von BeyondTrust unterstützt wird.</td></tr>
<tr><td>Die Anzahl der Clients, die installiert werden kann, ist abhängig vom Modell Ihres Secure Remote Access Appliance.

<table><tr><th>B200</th><th>B300</th><th>B400</th></tr><tr><td>Bis zu 1.000 aktive Jump-Clients</td><td>Bis zu 10.000 aktive Jump-Clients</td><td>Bis zu 25.000 aktive Jump-Clients</td></tr><tr><th>Virtuelles Gerät (S)</th><th>Virtuelles Gerät (M)</th><th>Virtuelles Gerät (L)</th></tr><tr><td>Bis zu 1.000 aktive Jump-Clients</td><td>Bis zu 10.000 aktive Jump-Clients</td><td>Bis zu 25.000 aktive Jump-Clients</td></tr></table></td><td>50.000 passive Jump-Clients, unterstützt auf allen Modellen des Secure Remote Access Appliance.

Wenn Sie mehr passive Jump-Clients benötigen, kontaktieren Sie den technischen Support unter www.beyondtrust.com/support.</td></tr>
</table>

Die maximale Anzahl an Jump-Clients, die einem RS Virtual Appliance zur Verfügung steht, basiert auf den zugewiesenen Ressourcen. Weitere Informationen finden Sie in den RS Virtual Appliance-Dimensionierungsrichtlinien unter www.beyondtrust.com/docs/remote-support/getting-started/deployment/virtual/sizing.htm.

Verwenden von Jump-Clients zum Zugriff auf unüberwachte Android-Geräte

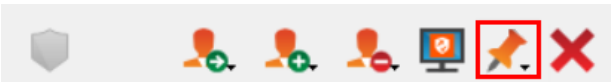
Eine dauerhafte Verbindung kann mit einem Samsung- oder Zebra-Android-Gerät aufgebaut werden, indem ein Jump-Client auf dem Gerät fixiert wird. Damit wird die Möglichkeit geboten, unüberwachte Support-Sitzungen Tech. durchzuführen. Sie können Jump-Clients über die unten angegebenen Methoden bereitstellen.

Hinweis: *Bandbreitenverbrauch und Akkulaufzeit werden durch den Aufbau einer dauerhaften Verbindung minimal beeinflusst.*

Dauerhafte Verbindungen mit einem unüberwachten Android-Gerät können nur erfolgen, wenn die Geräte sowohl die ***BeyondTrust Support-Client-App*** *als auch die* ***BeyondTrust Jump-Client-App*** *aus dem Google Play Store installiert*

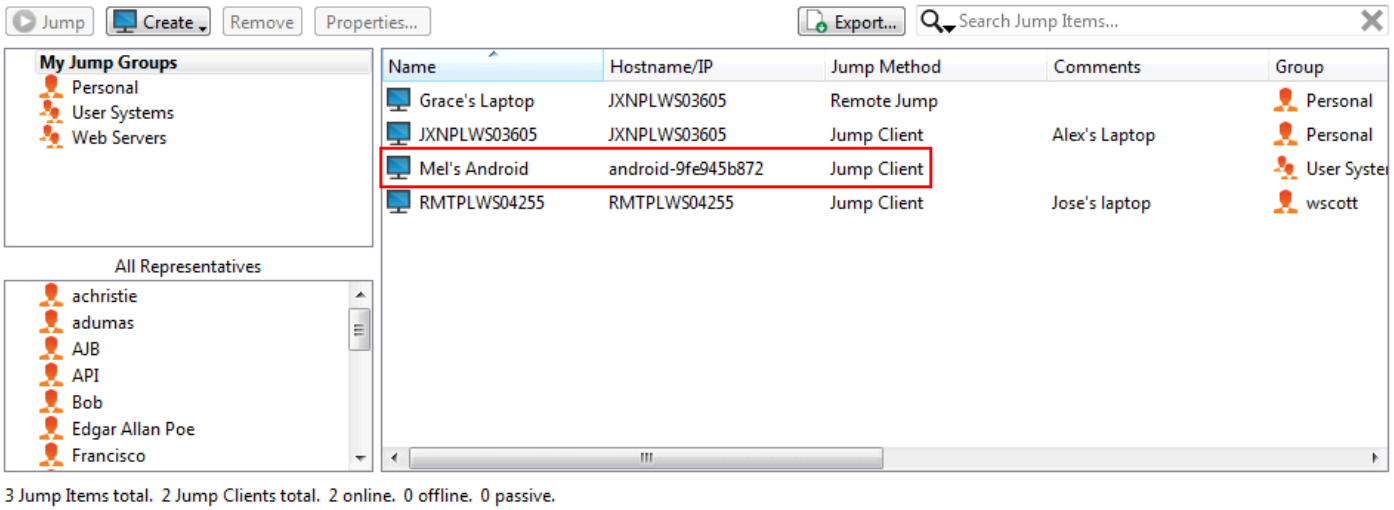
haben. Weitere Informationen finden Sie unter Die BeyondTrust Support-Client- und die BeyondTrust Jump-Client-App unter https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/android/android-download-app.htm herunterladen.

Einen Android Jump-Client über die Konsole d. Support-Technikers fixieren



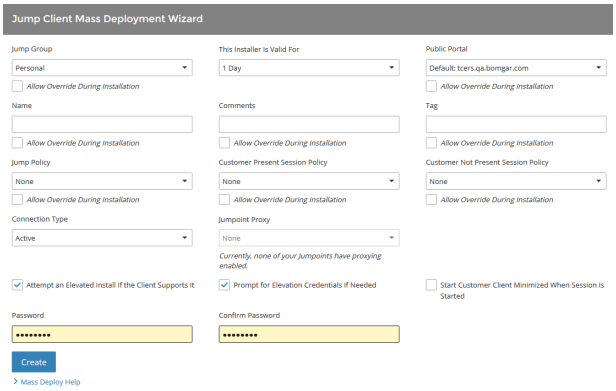
1. Klicken Sie in einer Support-Sitzung Tech. auf dem Android-Gerät auf das Symbol **Als Jump-Client fixieren**.
2. Klicken Sie nach dem Fixieren auf die Option **Aktualisieren** oberhalb der Jump-Element-Liste, und das Android-Gerät erscheint als Jump-Element in der Liste. Wenn das Symbol **Jump-Client fixieren** ausgegraut ist, wurde der Android Jump-Client nicht auf dem Android-Gerät installiert.
3. Gleichzeitig zeigt die BeyondTrust Jump-Client-App auf dem Gerät den Client mit Datum und Uhrzeitstempel als fixiert an.

***Hinweis:** Optionen sind für die Deaktivierung des Jump-Clients verfügbar, wenn das Gerät mit Akkustrom betrieben oder zur Verbindung eine Datenverbindung verwendet wird.*

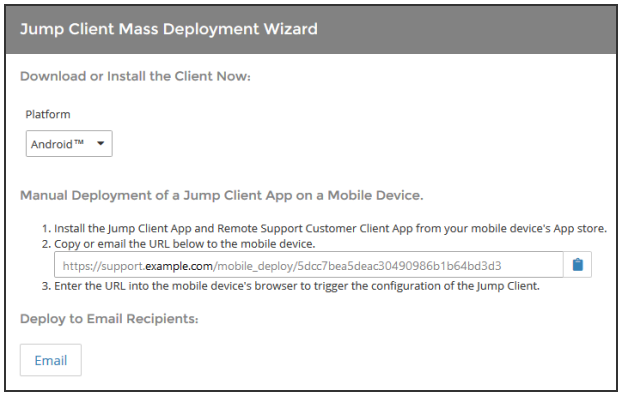


Einen Link über die /login-Schnittstelle zur Installation eines Android Jump-Client versenden

1. Navigieren Sie in der /login-Schnittstelle zu **Jump > Jump-Clients > Stapelbereitstellungsassistnet für Jump-Clients**.



2. Geben Sie die für Ihren Jump-Client nötigen Informationen an, wie **Jump-Gruppe**, **Öffentliches Portal** usw.
3. Klicken Sie auf **Erstellen**.
4. Wählen Sie im Bereich **Client jetzt herunterladen oder installieren** die Option **Android** als Plattform.
5. Stellen Sie sicher, dass die **BeyondTrustJump-Client**-App auf dem Android-Gerät installiert ist. Falls nicht, navigieren Sie zum Google Play App Store, um die App herunterzuladen.



6. Um den Jump-Client auf das Gerät herunterzuladen, öffnen Sie einen Browser auf dem Android-Gerät und navigieren Sie zur URL, die vom Stapelbereitstellungsassistenten angegeben wurde.

> ***Hinweis:*** *Außerdem können Sie die URL per E-Mail an das Android-Gerät senden, indem Sie auf den Link **E-Mail** im Abschnitt **Für E-Mail-Empfänger bereitstellen** klicken.*

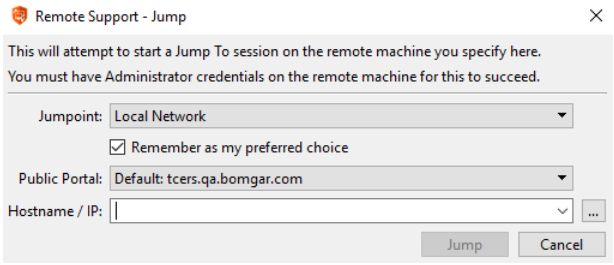
Erstellen und Verwenden von lokalen Jump-Links

Hinweis: *Jumpoint ist für Windows- und Linux-Systeme erhältlich. 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. Falls Sie auf Remote-Computer über einen Jumpoint zugreifen müssen, wenn kein Benutzer verfügbar ist, müssen Sie gewährleisten, dass Ihre Kontoberechtigungen entweder so festgelegt sind, dass die Aufforderung deaktiviert wird, oder die Standardeinstellung **Zulassen** lautet. Sie können keinen Jump auf ein mobiles Gerät durchführen, obwohl Jump-Technologie für mobile BeyondTrust-Konsolen verfügbar ist.*

Hinweis: *Linux-Jumpoints können nur für RDP- und SSH/Telnet-Sitzungen verwendet werden.*

Um ohne vorinstallierten Client per Jump zu wechseln, öffnen Sie das Dialogfeld **Jump zu…**:

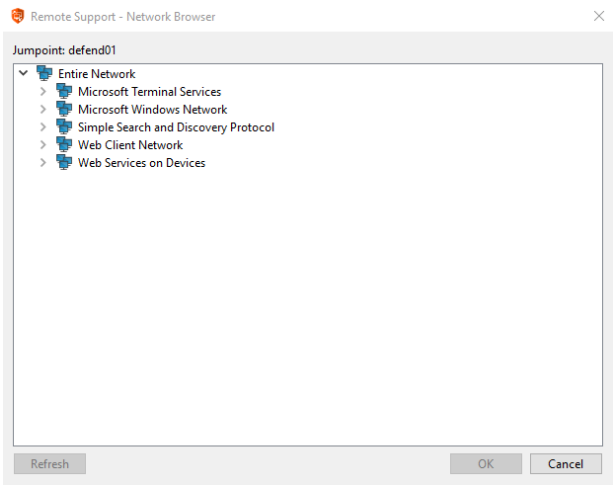
- Das **Support**-Menü der Konsole des Konsole d. Support-Technikers
- über die Schaltfläche **Start** oben in der Konsole d. Support-Technikers
- Die Schaltfläche **Jump zu** im oberen Bereich der Konsole d. Support-Technikers



Wählen Sie im Dropdown-Menü **Jumpoint** das Netzwerk aus, in dem sich der Computer befindet, auf den Sie zugreifen möchten. Abhängig von Ihren Kontoberechtigungen können Sie einen Jump zu einem System in Ihrem lokalen Netzwerk durchführen oder zu einem Netzwerk, in dem ein Jumpoint installiert wurde.

Wählen Sie das öffentliche Portal, das Sie mit Ihrer Sitzung verknüpfen möchten. Damit weiß das System, welches Kundenvereinbarungsverhalten erfolgen soll.

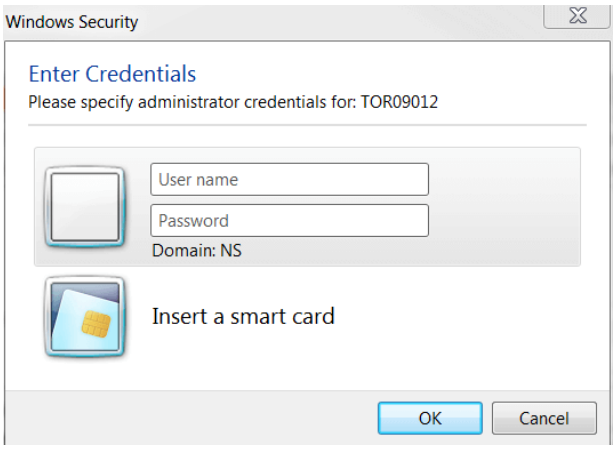
Weitere Informationen erhalten Sie unter Kunden-Client: Ändern der Einladungs-E-Mail, Anzeigeoptionen, Verbindungsoptionen unter https://www.beyondtrust.com/docs/remote-support/getting-started/admin/customer-client.htm.



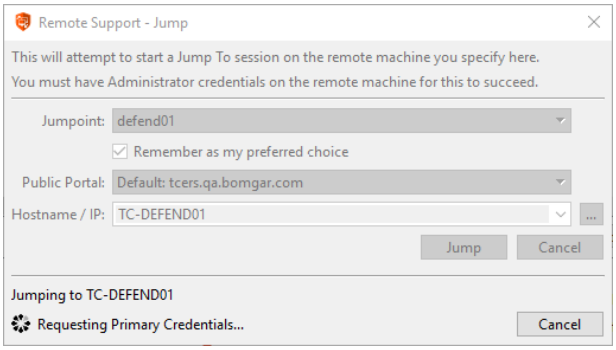
Geben Sie den Hostnamen oder die IP-Adresse des Systems ein, auf das Sie zugreifen wollen. Wenn die Netzwerksuche über die Seite **/login > Jump > Jumpoint** aktiviert wurde, können Sie auch auf die Schaltfläche **[...]** klicken, um den Verzeichnisbaum zu durchsuchen.

Wenn Sie den Computer gefunden haben, mit dem Sie eine Verbindung herstellen möchten, klicken Sie auf **Jump durchführen**.

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.*

Erstellen und Verwenden von Remote- und lokalen Jump-Elementen

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.

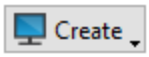
Ein Jumpoint agiert als Leitstelle für den unüberwachten Zugriff auf Windows- und Linux-Computer in einem bekannten Remote-Netzwerk. Ein einziger auf einem Computer in einem lokalen Netzwerk installierter Jumpoint wird zum Zugriff auf mehrere Systeme verwendet. So ist es nicht mehr notwendig, Software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

Lokaler Jump berechtigt einen Benutzer dazu, sich mit einem unüberwachten Remote-Computer im lokalen Netzwerk zu verbinden. Innerhalb des lokalen Netzwerks kann der BeyondTrust-Computerbenutzer eine Sitzung direkt ohne Verwendung eines Jumpoints mit einem Windows- oder Linux-System initiieren.

> ***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

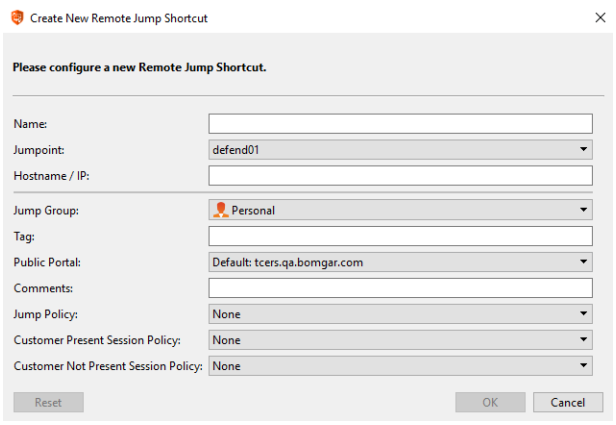
Um einen symbolischen Jump-Link (Remote) zu erstellen, klicken Sie auf die Schaltfläche **Erstellen** in der Jump-Schnittstelle. Wählen Sie aus der Dropdown-Liste **Remote-Jump**. Symbolische Jump-Links (Remote) erscheinen in der Jump-Schnittstelle zusammen mit Jump-Clients und anderen Arten von symbolischen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

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 **Tag**s 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.

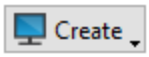
Um festzulegen, wann es Benutzern gestattet werden soll, auf dieses Jump-Element zuzugreifen, legen Sie eine **Jump-Richtlinie** fest. Diese Richtlinien werden von Ihrem Administrator über die **/login**-Schnittstelle festgelegt.

Wählen Sie 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 präsente Kunden** gilt, wenn der Endbenutzer als präsent gilt. Ansonsten gilt die **Sitzungsrichtlinie für nicht präsente 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.

Symbolischen Jump-Link (lokal) erstellen

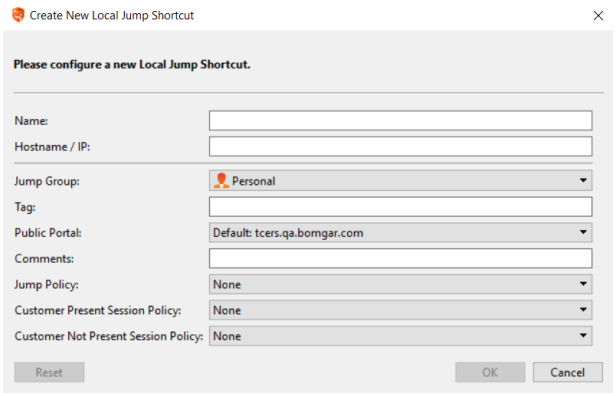
Um einen symbolischen Jump-Link (lokal) zu erstellen, klicken Sie in der Jump-Schnittstelle auf die Schaltfläche **Erstellen**. Wählen Sie in der Dropdown-Liste **Lokaler Jump**. Symbolische Jump-Links (lokal) erscheinen in der Jump-Schnittstelle zusammen mit Jump-Clients und anderen Arten von symbolischen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



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 **Tag**s 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.

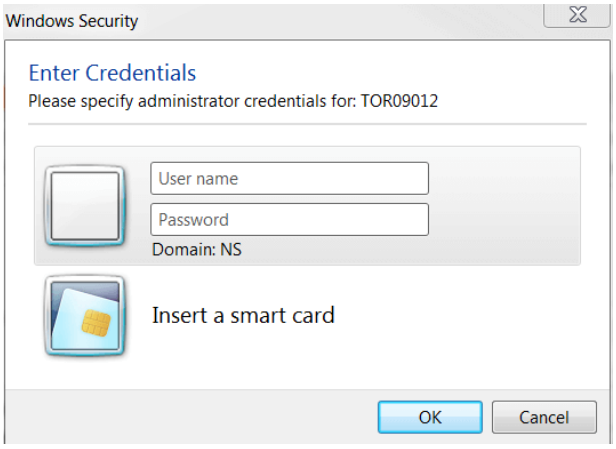
Wählen Sie Sitzungsrichtlinien, die diesem Jump-Element zugewiesen werden sollen. Diesem Jump-Element zugewiesene Sitzungsrichtlinien haben die höchste Priorität bei der Festlegung von Sitzungsberechtigungen. Die **Sitzungsrichtlinie für präsente Kunden** gilt, wenn der Endbenutzer als präsent gilt.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

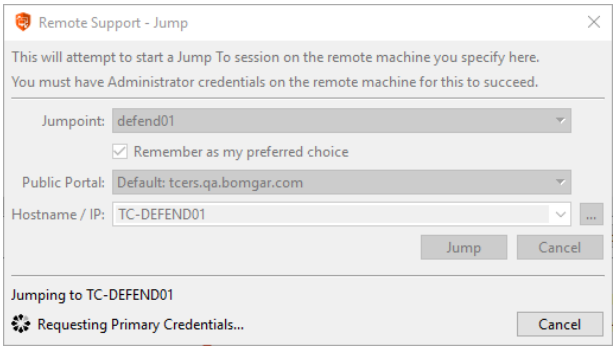
Verwenden eines symbolischen Remote-Jump oder lokalen Jump-Links

Um eine symbolische Jump-Verknüpfung zum Starten einer Sitzung zu verwenden, wählen Sie die Verknüpfung einfach aus der Jump-Schnittstelle und klicken Sie auf die Taste **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.*

RDP zu einem Remote-Windows- oder -Linux-System

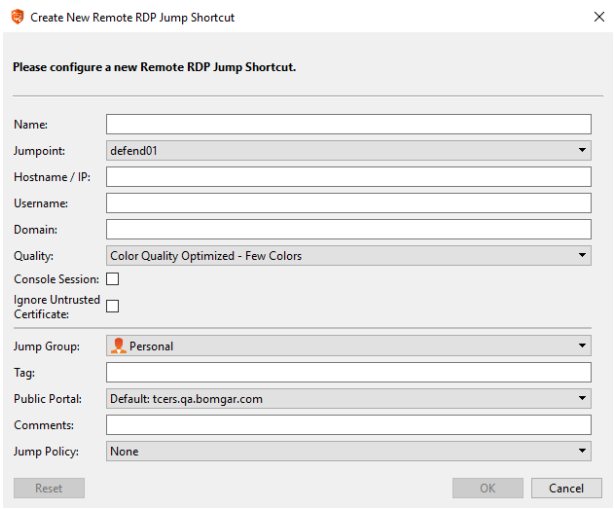
Verwenden Sie BeyondTrust, um eine Remote-Desktop-Protokoll (RDP)-Sitzung mit einem Remote-Windows- oder -Linux-System zu starten. Da RDP-Sitzungen in BeyondTrust-Sitzungen umgewandelt werden, können Benutzer Sitzungen freigeben oder übertragen, und diese können automatisch geprüft und aufgezeichnet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

Um RDP (lokal) über BeyondTrust nutzen zu können, müssen Sie sich im gleichen Netzwerksegment wie das Zielsystem befinden und die Benutzerberechtigung **Gestattete Jump-Methoden: RDP (lokal)** besitzen.

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

Um eine RDP-Sitzung zu starten, öffnen Sie das Dialogfeld **Remote-Desktop-Protokoll** über:

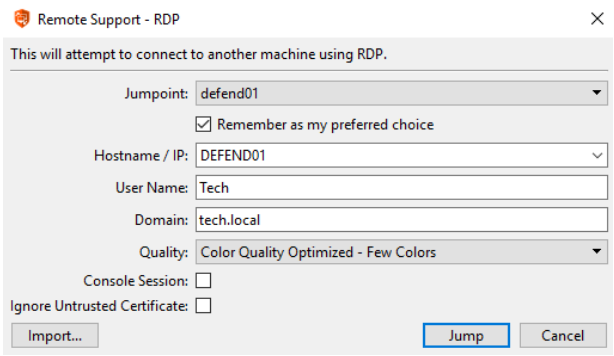
- Das **Support**-Menü der Konsole des Konsole d. Support-Technikers
- Die Schaltfläche **RDP zu** oben in der Konsole d. Support-Technikers



Wählen Sie im Dropdown-Menü **Jumpoint** das Netzwerk aus, in dem sich der Computer befindet, auf den Sie zugreifen möchten. Wenn Sie in der Regel auf den gleichen Jumpoint zugreifen, aktivieren Sie **Als bevorzugte Einstellung markieren**. Geben Sie den **Hostnamen / die IP** des Systems ein, auf das Sie zugreifen möchten.

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. Aktivieren Sie **Nicht vertrauenswürdiges Zertifikat ignorieren**, um eine Verbindung zum Remote-System aufzubauen, 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 **Tag**s 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.

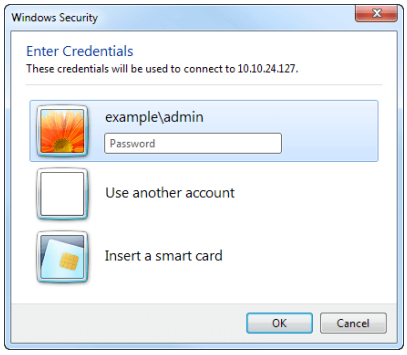
Jump-Elemente umfassen auch ein **Kommentare**-Feld für einen Namen oder eine Beschreibung, wodurch die Sortierung, Suche und Identifizierung von Jump-Clients schneller und einfacher wird.

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.

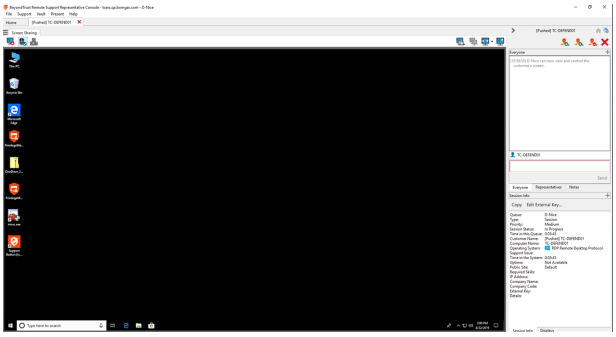
Um eine RDP-Datei zu importieren, klicken Sie auf die Schaltfläche **Importieren**. Damit werden einige der für die RDP-Verbindung erforderlichen Felder vorausgefüllt.

Um die RDP-Sitzung zu beginnen, klicken Sie auf **Jump**.

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



Jetzt beginnt Ihre RDP-Sitzung. Beginnen Sie mit der Bildschirmfreigabe, 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.*

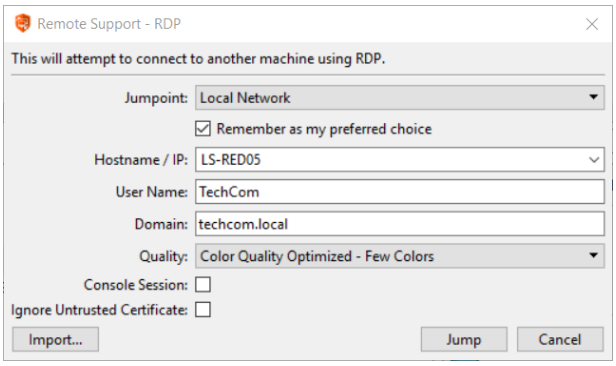
Hinweis: *Jump-Elemente können ebenfalls eingestellt werden, um den gleichzeitigen Zugriff auf das gleiche Jump-Element durch mehrere Benutzer zu gestatten. Falls auf* ***Neue Sitzung starten*** *eingestellt, wird eine neue unabhängige Sitzung für*

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.

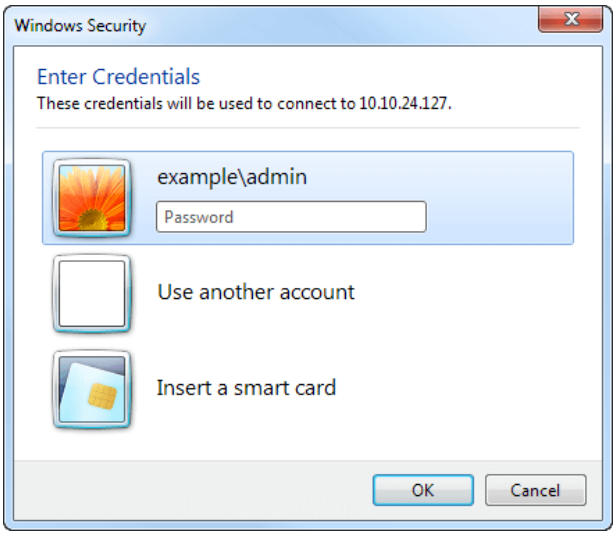
Weitere Informationen zu gleichzeitigen Jumps finden Sie in Jump-Element-Einstellungen unter www.beyondtrust.com/docs/remote-support/getting-started/admin/jump-items.htm.

RDP (lokal) für den Zugriff auf Windows- und Linux-Systeme verwenden

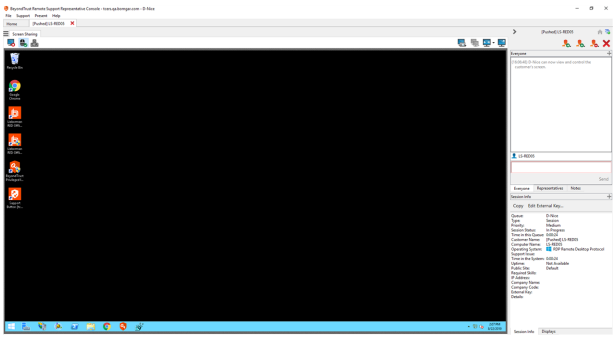
Verwenden Sie BeyondTrust, um eine lokale Remote-Desktop-Protokoll (RDP)-Sitzung mit Remote-Windows- und -Linux-Systemen zu starten. Anders als bei einer üblichen BeyondTrust RDP-Sitzung werden lokale RDP-Sitzungen nicht über einen Jumpoint geleitet. Das bedeutet, dass Benutzer Jumps nur zu Systemen innerhalb ihres lokalen Netzwerks durchführen können. Um RDP über BeyondTrust nutzen zu können, benötigen Sie die Benutzerkontoberechtigung **Gestattete Jump-Methoden: RDP (lokal) über das lokale Netzwerk**.



1. Um eine lokale RDP-Sitzung über die Konsole d. Support-Technikers zu starten, öffnen Sie den Dialog **Remote-Desktop-Protokoll** über das **Support**-Menü oder die Schaltfläche **RDP zu**.
2. Wählen Sie als Jumpoint-Option **Lokales Netzwerk**.
3. Geben Sie den Hostnamen oder die IP-Adresse des Computers ein, für den Sie Support bereitstellen möchten.
4. Geben Sie den Benutzernamen ein, über den Sie sich anmelden möchten.
5. Wählen Sie eine Domäne.
6. 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** wie auch der **Vollfarbmodus** ermöglichen die Anzeige des Desktop-Hintergrundbilds.
7. 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.
8. Um eine RDP-Datei zu importieren, klicken Sie auf die Schaltfläche **Importieren**. Damit werden einige der für die Remote-Desktop-Protokoll-Verbindung erforderlichen Felder vorausgefüllt.
9. Um die Remote-Desktop (RDP)-Sitzung zu beginnen, klicken Sie auf **Jump**.
10. Sie werden aufgefordert, das Kennwort für den zuvor angegebenen Benutzernamen einzugeben.



11. Jetzt beginnt Ihre Remote-Desktop-Protokoll (RDP)-Sitzung.



Erstellen und Nutzen von Jump-Elementen mit lokalem oder Remote-RDP

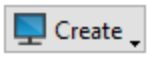
Verwenden Sie BeyondTrust, um eine Remote-Desktop-Protokoll (RDP)-Sitzung mit einem Remote-Windows- oder -Linux-System zu starten. Da RDP-Sitzungen in BeyondTrust-Sitzungen umgewandelt werden, können Benutzer Sitzungen freigeben oder übertragen, und diese können automatisch geprüft und aufgezeichnet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

Um RDP (lokal) über BeyondTrust nutzen zu können, müssen Sie sich im gleichen Netzwerksegment wie das Zielsystem befinden und die Benutzerberechtigung **Gestattete Jump-Methoden: RDP (lokal)** besitzen.

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

Erstellen eines symbolischen RDP-Links (lokal)

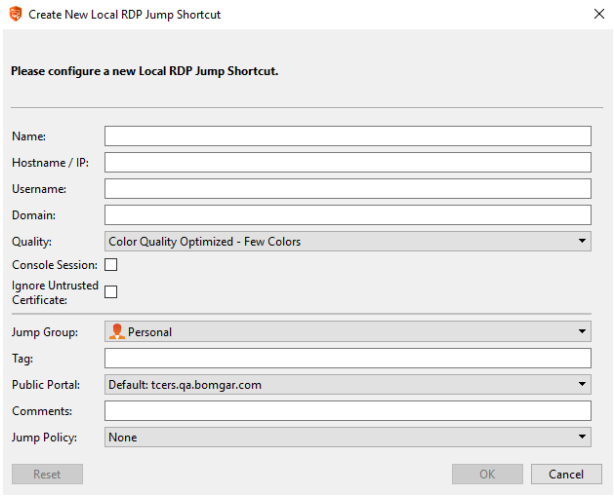
Um einen symbolischen Link für das Microsoft Remote Desktop Protocol zu erstellen, klicken Sie in der Jump-Schnittstelle auf die Schaltfläche **Erstellen**. Wählen Sie in der Dropdown-Liste **RDP (lokal)**. Symbolische RDP-Links erscheinen in der Jump-Schnittstelle zusammen mit Jump-Clients und anderen 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-Elemente anzuzeigen, müssen alle ausgewählten Elemente vom gleichen Typ sein (z. B. alle Jump-Clients, alle Remote-Jumps usw.). Um die Eigenschaften anderer Arten von Jump-Elementen anzusehen, beziehen Sie sich bitte auf den entsprechenden Abschnitt in diesem Handbuch.*

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.



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 **Tag**s 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.

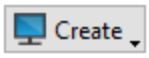
Wählen Sie als nächstes das **Öffentliche Portal**, über das sich das Jump-Element verbinden soll. Wenn diesem öffentlichen Portal eine Sitzungsrichtlinie zugewiesen ist, kann sich diese Richtlinie auf die Berechtigungen auswirken, die für über dieses Jump-Element gestartete Sitzungen erlaubt sind. Die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

Symbolischen RDP-Link (Remote) erstellen

Um einen symbolischen Remote Microsoft Remote Desktop Protocol-Link zu erstellen, klicken Sie in der Jump-Schnittstelle auf **Erstellen**. Wählen Sie im Dropdown-Menü **RDP (Remote)**. Symbolische RDP-Links erscheinen in der Jump-Schnittstelle zusammen mit Jump-Clients und anderen Arten von symbolischen Jump-Element-Links.

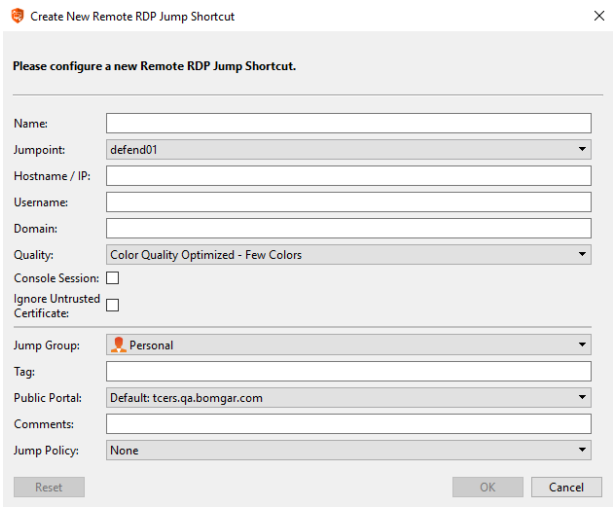


Organisieren und verwalten Sie bestehende Jump-Elemente, indem Sie einen oder mehrere Jump-Clients auswählen und auf **Eigenschaften** klicken.

> ***Hinweis:*** *Um die Eigenschaften mehrerer Jump-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.



> ***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 **Tag**s 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.

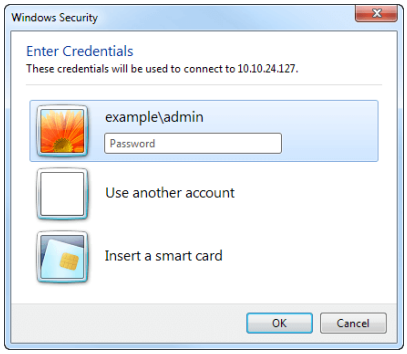
Jump-Elemente umfassen auch ein **Kommentare**-Feld für einen Namen oder eine Beschreibung, wodurch die Sortierung, Suche und Identifizierung von Jump-Clients schneller und einfacher wird.

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.

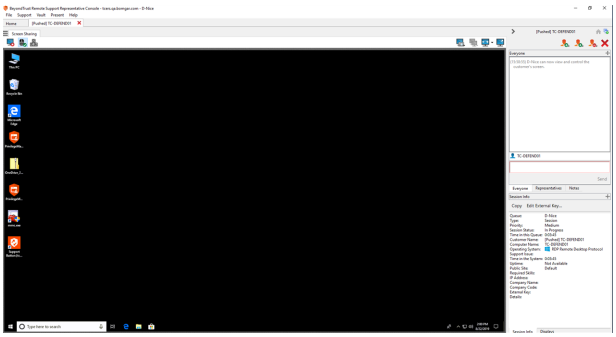
Symbolischen RDP-Link verwenden

Um eine symbolische Jump-Verknüpfung zum Starten einer Sitzung zu verwenden, wählen Sie die Verknüpfung einfach aus der Jump-Schnittstelle und klicken Sie auf die Taste **Jump**.

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



Jetzt beginnt Ihre RDP-Sitzung. Beginnen Sie mit der Bildschirmfreigabe, 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.



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 unter www.beyondtrust.com/docs/remote-support/getting-started/admin/jump-items.htm.

VNC zu einem Remote-System

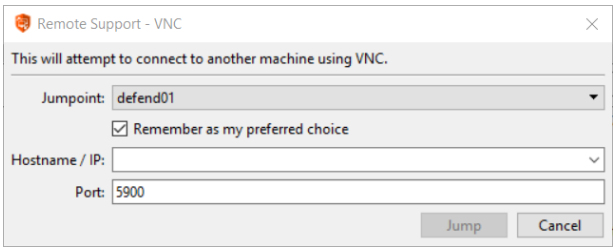
Verwenden Sie BeyondTrust, um eine VNC-Sitzung mit einem Remote-System zu starten. Da VNC-Sitzungen in BeyondTrust-Sitzungen umgewandelt werden, können Benutzer Sitzungen freigeben oder übertragen, und diese können automatisch geprüft und aufgezeichnet werden, je nach Festlegung durch den Administrator.

Um lokales VNC über BeyondTrust nutzen zu können, müssen Sie sich auf dem gleichen Netzwerksegment wie das Zielsystem befinden und die Benutzerkontoberechtigung **Gestattete Jump-Methoden: Lokales VNC** besitzen.

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

Um eine VNC-Sitzung zu starten, öffnen Sie das Dialogfeld **VNC**:

- Das **Support**-Menü der Konsole des Konsole d. Support-Technikers
- Über die Schaltfläche **VNC** oberhalb der Konsole d. Support-Technikers



Wählen Sie im Dropdown-Menü **Jumpoint** das Netzwerk aus, in dem sich der Computer befindet, auf den Sie zugreifen möchten. Wenn Sie in der Regel auf den gleichen Jumpoint zugreifen, aktivieren Sie **Als bevorzugte Einstellung markieren**. 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.

Um die VNC-Sitzung zu beginnen, klicken Sie auf **Jump**.

Erstellen und Verwenden von symbolischen VNC-Links

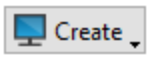
Verwenden Sie BeyondTrust, um eine VNC-Sitzung mit einem Remote-System zu starten. Da VNC-Sitzungen in BeyondTrust-Sitzungen umgewandelt werden, können Benutzer Sitzungen freigeben oder übertragen, und diese können automatisch geprüft und aufgezeichnet werden, je nach Festlegung durch den Administrator.

Um lokales VNC über BeyondTrust nutzen zu können, müssen Sie sich auf dem gleichen Netzwerksegment wie das Zielsystem befinden und die Benutzerkontoberechtigung **Gestattete Jump-Methoden: Lokales VNC** besitzen.

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 (lokal) erstellen

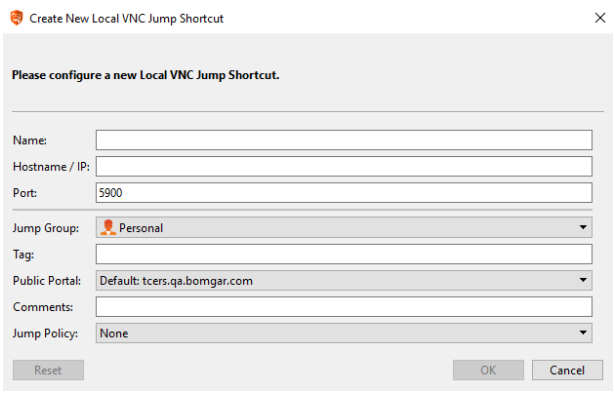
Um einen symbolischen VNC-Link (lokal) zu erstellen, klicken Sie in der Jump-Schnittstelle auf die Schaltfläche **Erstellen**. Wählen Sie in der Dropdown-Liste **Lokaler VNC**. Symbolische VNC-Links erscheinen in der Jump-Schnittstelle zusammen mit Jump-Clients und anderen Arten von symbolischen Jump-Element-Links.



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-Elemente anzuzeigen, müssen alle 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.



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 **Tag**s 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.

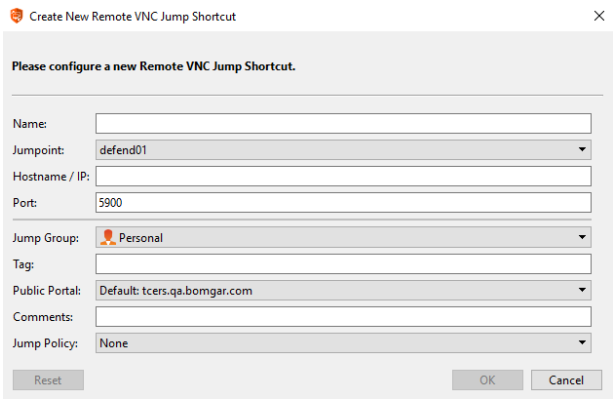
Symbolischen VNC-Link (Remote) erstellen

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** aus. 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-Elemente anzuzeigen, müssen alle 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 **Tag**s 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.

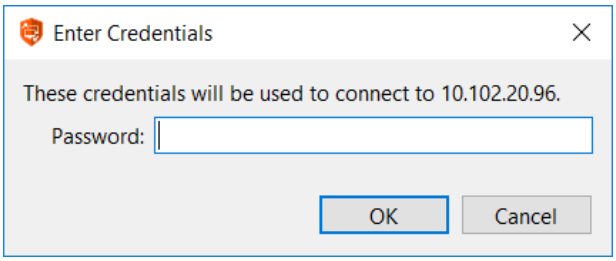
Jump-Elemente umfassen auch ein **Kommentare**-Feld für einen Namen oder eine Beschreibung, wodurch die Sortierung, Suche und Identifizierung von Jump-Clients schneller und einfacher wird.

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.

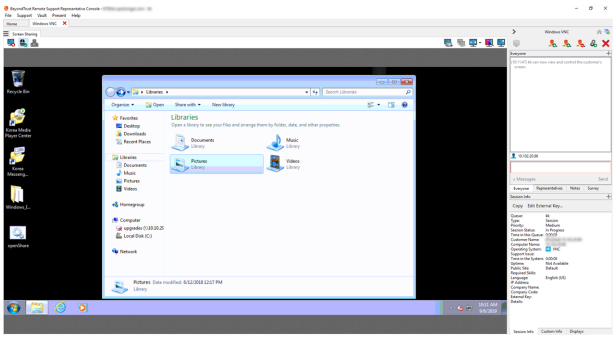
Einen symbolischen VNC-Link verwenden

Um eine symbolische Jump-Verknüpfung zum Starten einer Sitzung zu verwenden, wählen Sie die Verknüpfung einfach aus der Jump-Schnittstelle und klicken Sie auf die Taste **Jump**.

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, eine Bildschirmaufnahme des Remote-Desktops machen und Textinhalte der Zwischenablage freigeben. Sue 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 unter www.beyondtrust.com/docs/remote-support/getting-started/admin/jump-items.htm.

Shell Jump auf ein Remote-Netzwerkgerät

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 bespielsweise ein standardisiertes Skript auf mehreren Systemen aus, um einen benötigten Patch zu installieren oder ein Netzwerkproblem zu beheben.

Um über BeyondTrust einen Shell Jump durchzuführen, benötigen Sie Zugriff auf einen Jumpoint mit aktiviertem Shell Jump sowie die Benutzerkontoberechtigung **Gestattete Jump-Methoden: Shell Jump**.

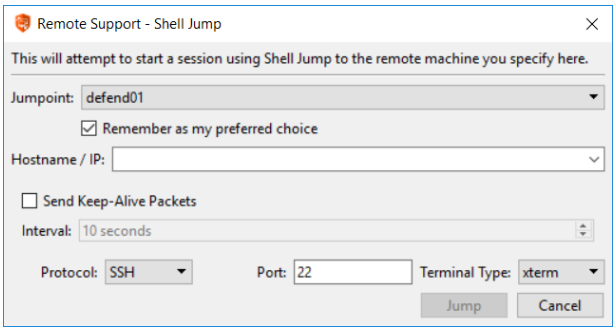
Um eine Shell Jump-Sitzung zu starten, öffnen Sie das Dialogfeld **Shell Jump**:

- Das **Support**-Menü der Konsole des Konsole d. Support-Technikers
- Über die Schaltfläche **Shell Jump** oberhalb der Konsole d. Support-Technikers

Ihr Jumpoint ist möglicherweise nur für bereitgestellten Shell Jump-Zugriff konfiguriert.

Wählen Sie im Dropdown-Menü **Jumpoint** das Netzwerk aus, in dem sich der Computer befindet, auf den Sie zugreifen möchten. Wenn Sie in der Regel auf den gleichen Jumpoint zugreifen, aktivieren Sie **Als bevorzugte Einstellung markieren**. Wählen Sie das bereitgestellte System, auf das Sie zugreifen möchten.

Alternativ kann Ihr Jumpoint für offenen Zugriff oder beschränkten Zugriff konfiguriert werden.



Wählen Sie im Dropdown-Menü **Jumpoint** das Netzwerk aus, in dem sich der Computer befindet, auf den Sie zugreifen möchten. Wenn Sie in der Regel auf den gleichen Jumpoint zugreifen, aktivieren Sie **Als bevorzugte Einstellung markieren**.

Um auf ein bereitgestelltes System zuzugreifen, aktivieren Sie **Verwendung bereitgestellt** und wählen Sie das System im Dropdown-Menü.

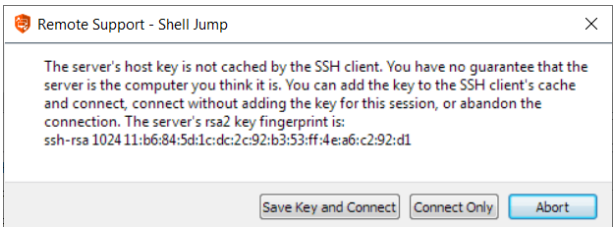
Alternativ können Sie den **Hostnamen / die IP** des Systems ein, auf das Sie zugreifen möchten. Wenn Ihr Jumpoint für eingeschränkten Zugriff konfiguriert ist, muss sich das Remote-System im angegebenen IP-Adressbereich befinden.

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.

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

Klicken Sie dann auf **Jump**.

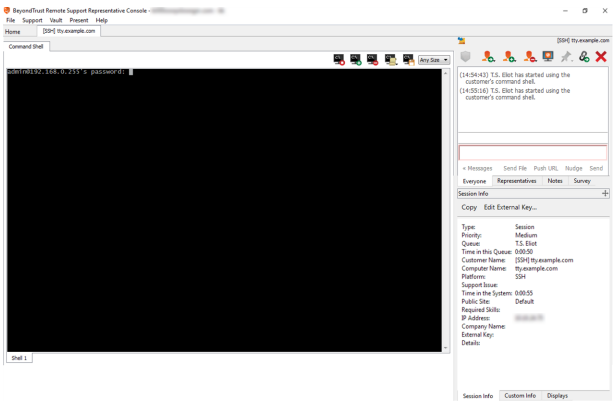
Wenn Sie versuchen, per Shell Jump auf ein SSH-Gerät ohne zwischengespeicherten Hostschlüssel zu wechseln, erhalten Sie eine Warnmeldung, dass der Hostschlüssel des Servers nicht zwischengespeichert ist und nicht garantiert wird, dass es sich bei dem Server um den von Ihnen vermuteten Computer handelt.



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 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 Kennwort zwischengespeichert wurde, wechseln, werden Sie nicht aufgefordert, ein Kennwort einzugeben. Ansonsten werden Sie zur Eingabe eines Passworts aufgefordert. Sie können dann Befehle an das Remote-System senden.

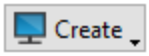


Erstellen und Verwenden symbolischer Shell Jump-Links

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 bespielsweise ein standardisiertes Skript auf mehreren Systemen aus, um einen benötigten Patch zu installieren oder ein Netzwerkproblem zu beheben.

Erstellen eines symbolischen Shell Jump-Links

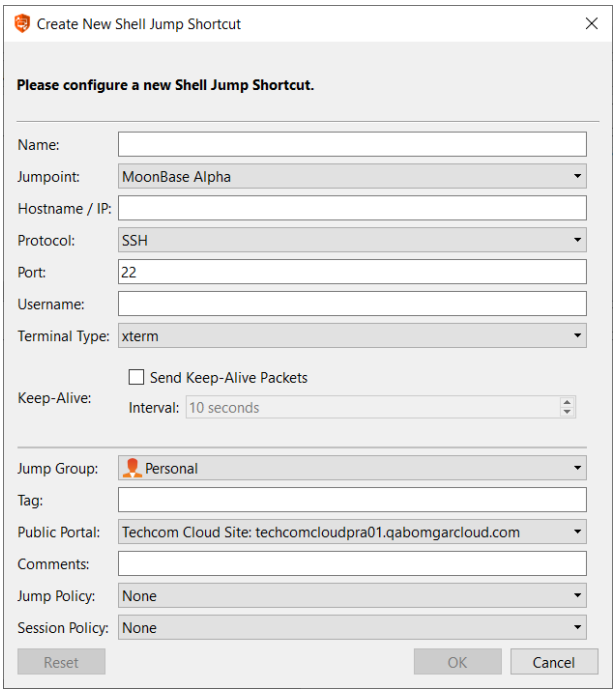
Um einen symbolischen Shell Jump-Link zu erstellen, klicken Sie auf die Schaltfläche **Erstellen** in der Jump-Schnittstelle. Wählen Sie aus der Dropdown-Liste **Shell Jump**. Symbolische Shell Jump-Links erscheinen in der Jump-Schnittstelle zusammen mit Jump-Clients und anderen Arten von symbolischen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



> ***Hinweis:*** *Symbolische Shell Jump-Links werden nur aktiviert, wenn der Jumpoint 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 **Tag**s 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.

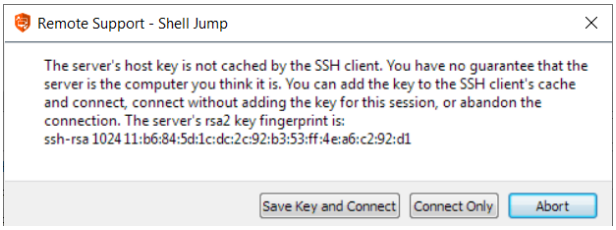
Um festzulegen, wann es Benutzern gestattet werden soll, auf dieses Jump-Element zuzugreifen, legen Sie eine **Jump-Richtlinie** fest. Diese Richtlinien werden von Ihrem Administrator über die **/login**-Schnittstelle festgelegt.

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.

Symbolischen Shell Jump-Link verwenden

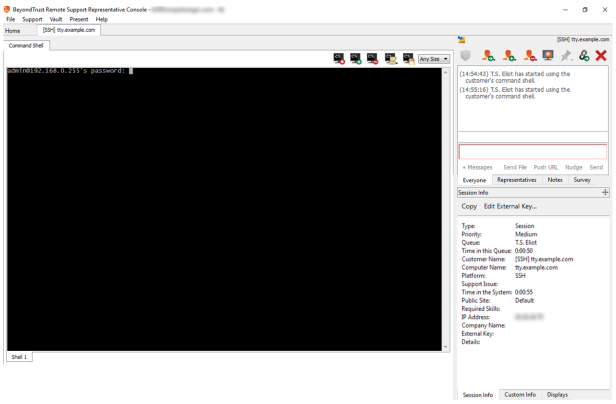
Um eine symbolische Jump-Verknüpfung zum Starten einer Sitzung zu verwenden, wählen Sie die Verknüpfung einfach aus der Jump-Schnittstelle und klicken Sie auf die Taste **Jump**.

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 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 Kennwort zwischengespeichert wurde, wechseln, werden Sie nicht aufgefordert, ein Kennwort einzugeben. Ansonsten werden Sie zur Eingabe eines Passworts aufgefordert. Sie können dann Befehle an das Remote-System senden.



Support für Intel® vPro Windows-Systeme bereitstellen

Mithilfe der Intel® Active Management-Technologie können berechtigte Benutzer Support für vollständig bereitgestellte Intel® vPro-Windows-Systeme unterhalb der Betriebssystemebene zur Verfügung stellen, unabhängig vom Status bzw. Stromversorgungsstatus dieser Remote-Systeme. Um Intel® vPro-Support nutzen zu können, müssen Sie Zugriff auf einen Jumpoint mit aktiviertem Intel® vPro haben und in Ihrem Benutzerkonto über die Berechtigung **Erlaubte Jump-Methoden: Intel® vPro** verfügen.

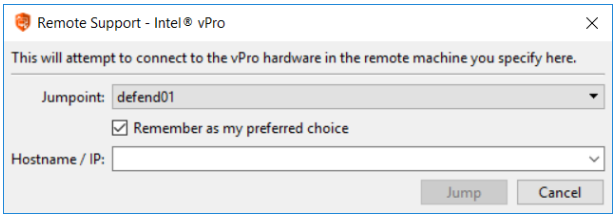
Hinweis: *Remote-Systeme, die vPro mit AMT-Version 5 oder höher verwenden, können mit BeyondTrust unterstützt werden.*

Hinweis: *Während vPro von geclusterten Jumpoints unterstützt wird, sind Konfigurationsoptionen nur bei Standalone-Jumpoints verfügbar. Geclusterte Jumpoints haben keine Konfigurationsoptionen für Intel® vPro.*

Um eine Sitzung mit einem Intel® vPro-System zu starten, öffnen Sie das **Intel® vPro** Dialogfenster über:

- Das **Support**-Menü der Konsole des Konsole d. Support-Technikers
- Die Schaltfläche **Intel® vPro** oberhalb der Konsole d. Support-Technikers

Wählen Sie im Dropdown-Menü **Jumpoint** das Netzwerk aus, in dem sich der Computer befindet, auf den Sie zugreifen möchten. Wenn Sie in der Regel auf den gleichen Jumpoint zugreifen, aktivieren Sie **Als bevorzugte Einstellung markieren**. Geben Sie den **Hostnamen / die IP** des Systems ein, auf das Sie zugreifen möchten.

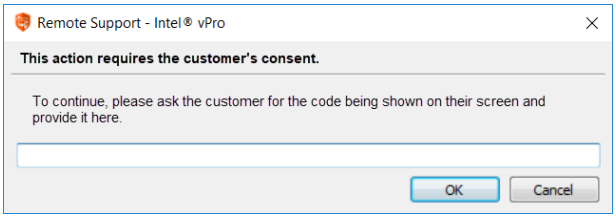


Klicken Sie auf **Jump**.

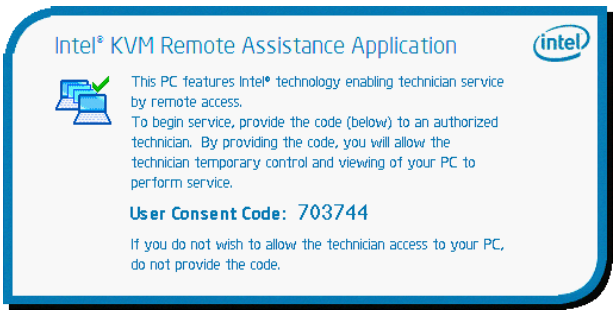
Abhängig von Ihrer Jumpoint-Konfiguration werden Sie möglicherweise zur Eingabe von Benutzernamen und Kennwort aufgefordert.

Der Jumpoint erkennt die bereitgestellte vPro-Hardware. Wenn die während der Konfiguration des Jumpoints bzw. dem Jump-Versuch angegebenen Anmeldedaten den Anmeldedaten auf dem über vPro bereitgestellten System entsprechen, wird die Verbindung eingeleitet.

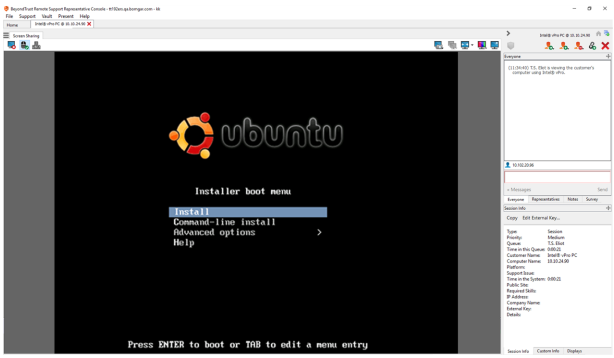
Abhängig davon, wie der vPro-Computer bereitgestellt ist, werden Sie möglicherweise dazu aufgefordert, vor der Durchführung bestimmter Aktionen einen Benutzer-Zustimmungscode einzugeben.



Sollte ein Zustimmungscode erforderlich sein, erscheint auf dem Remote-Bildschirm ein Popup. Der Endbenutzer muss Ihnen diesen Code zur Verfügung stellen, damit Sie Zugriff auf die Hardware erhalten.



Sobald die Verbindung hergestellt ist, haben Sie Zugriff auf die Remote-vPro-Hardware. Sie können dann die vPro-Sitzungswerkzeuge verwenden, um am Remote-System zu arbeiten.

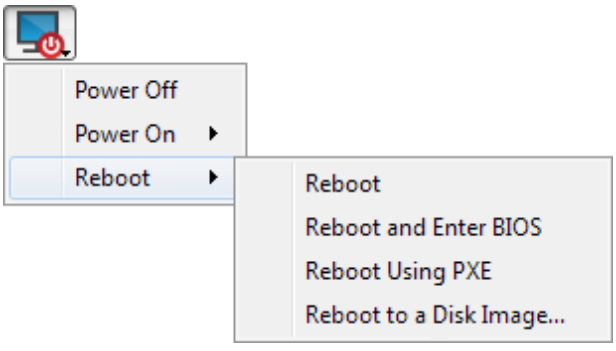


vPro Sitzungswerkzeuge

	vPro-Verbindung zurücksetzen.
	Fahren Sie die Host-Maschine herunter bzw. hoch. Sie können die Host-Maschine auch normal, in BIOS, in PXE oder in einem ausgewählten Festplattenabbild neu starten.
	Wählen Sie eine ISO- oder IMG-Datei, die auf dem Remote-System erstellt werden soll. Der Dateispeicherort wird während der Jumpoint-Konfiguration festgelegt.
	Starten bzw. beenden Sie mithilfe von KVM die Bildschirmanzeige des Remote-Systems.
	Senden Sie **Strg-Alt-Entf** an den Remote-Computer.
	Während der Bildschirmfreigabe können Sie eine Bildschirmaufnahme des Remote-Bildschirms bzw. der Remote-Bildschirme mit voller Auflösung im PNG-Format aufnehmen. Speichern Sie die Bilddatei in Ihrem lokalen System oder in der Zwischenablage. Die Aufzeichnungs-Aktion wird im Chat-Protokoll mit einem Link zum lokal gespeicherten Bild aufgezeichnet. Der Link bleibt aktiv, selbst wenn der Kunde die Sitzung verlassen hat, wird aber nicht im BeyondTrust-Sitzungsbericht gespeichert. Sie können das Zielverzeichnis für Bildschirmaufnahmen im Menü **Datei > Einstellungen > Support-Tools** in der Konsole d. Support-Technikers ändern. Dies funktioniert auf Mac, Windows und Linux.
	Einen alternativen Remote-Bildschirm für die Anzeige auswählen. Der primäre Monitor wird mit einem **P** gekennzeichnet.
	Den Remote-Bildschirm in der tatsächlichen Größe oder skaliert anzeigen.
	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.
	Zeigen Sie den Remote-Desktop im Vollbildmodus an oder kehren Sie zur Schnittstellenansicht zurück.

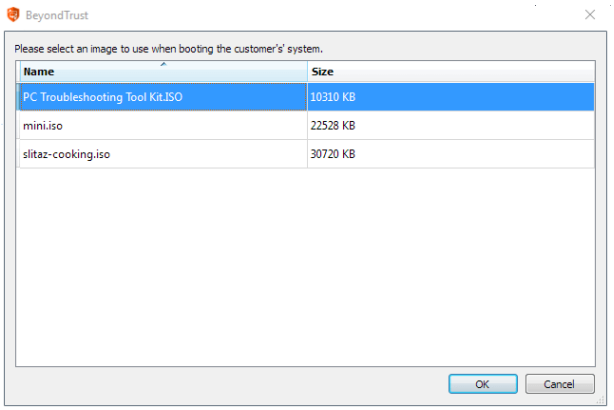
Wählen Sie im Menü **Neustart** die Option **Neu starten und BIOS öffnen**, um den BIOS-Bootprozess auf dem Remote-vPro-System zu starten. Sie haben dann zur Fehlersuche Zugang zum BIOS.

Wählen Sie **Mithilfe von PXE neu starten**, um das Remote-System mithilfe einer von den Datenspeichergeräten bzw. installierten Betriebssystemen unabhängigen Netzwerkschnittstelle zu booten.



Mit Laufwerksabbild neu starten verwendet IDE-R, um das Remote-System mit einer angegebenen ISO- oder IMG-Datei zu booten.

Beachten Sie, dass das Remote-System den Bildschirm genau so anzeigt, wie Sie ihn sehen, selbst wenn Sie mit einem anderen Abbild booten.

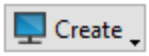


Symbolischen Intel vPro Jump-Links erstellen und verwenden

Mithilfe der Intel® Active Management-Technologie können berechtigte Benutzer Support für vollständig bereitgestellte Intel® vPro-Windows-Systeme unterhalb der Betriebssystemebene zur Verfügung stellen, unabhängig vom Status bzw. Stromversorgungsstatus dieser Remote-Systeme.

Erstellen eines symbolischen Intel® vPro-Links

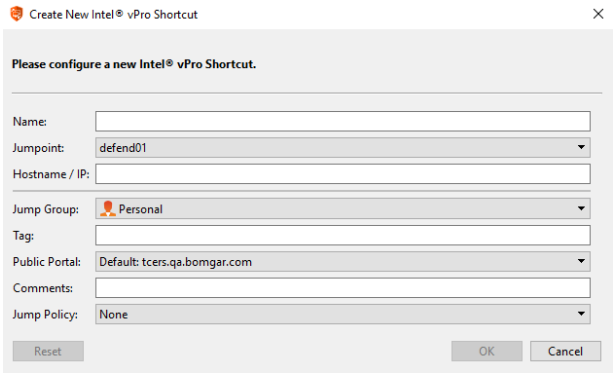
Um einen symbolischen Intel® vPro-Link zu erstellen, klicken Sie auf die Schaltfläche **Erstellen** in der Jump-Schnittstelle. Wählen Sie in der Dropdown-Liste **Intel® vPro**. Symbolische Intel® vPro-Links erscheinen in der Jump-Schnittstelle zusammen mit Jump-Clients und anderen Arten von symbolischen 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-Elemente anzuzeigen, müssen alle 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.

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 **Tag**s 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.

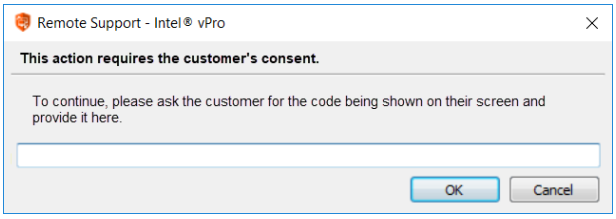
Um festzulegen, wann es Benutzern gestattet werden soll, auf dieses Jump-Element zuzugreifen, legen Sie eine **Jump-Richtlinie** fest. Diese Richtlinien werden von Ihrem Administrator über die **/login**-Schnittstelle festgelegt.

Verwenden eines symbolischern Intel® vPro-Links

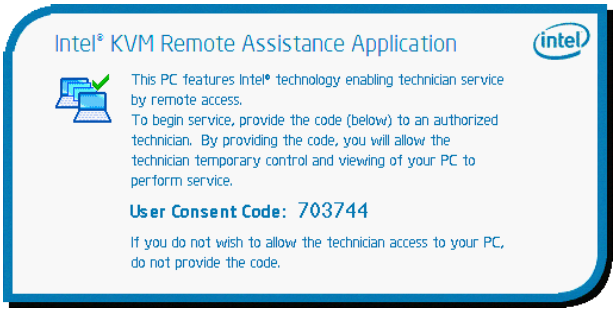
Abhängig von Ihrer Jumpoint-Konfiguration werden Sie möglicherweise zur Eingabe von Benutzernamen und Kennwort aufgefordert.

Der Jumpoint erkennt die bereitgestellte vPro-Hardware. Wenn die während der Konfiguration des Jumpoints bzw. dem Jump-Versuch angegebenen Anmeldedaten den Anmeldedaten auf dem über vPro bereitgestellten System entsprechen, wird die Verbindung eingeleitet.

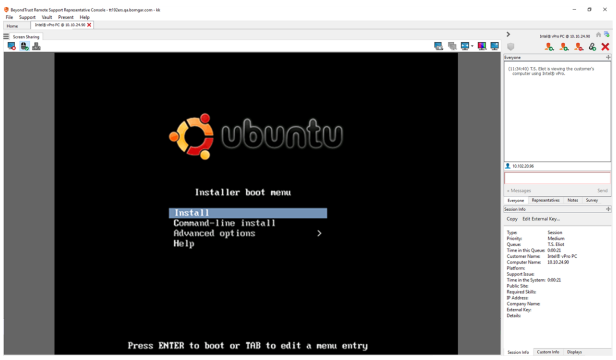
Abhängig davon, wie der vPro-Computer bereitgestellt ist, werden Sie möglicherweise dazu aufgefordert, vor der Durchführung bestimmter Aktionen einen Benutzer-Zustimmungscode einzugeben.



Sollte ein Zustimmungscode erforderlich sein, erscheint auf dem Remote-Bildschirm ein Popup. Der Endbenutzer muss Ihnen diesen Code zur Verfügung stellen, damit Sie Zugriff auf die Hardware erhalten.



Sobald die Verbindung hergestellt ist, haben Sie Zugriff auf die Remote-vPro-Hardware. Sie können dann die vPro-Sitzungswerkzeuge verwenden, um am Remote-System zu arbeiten.

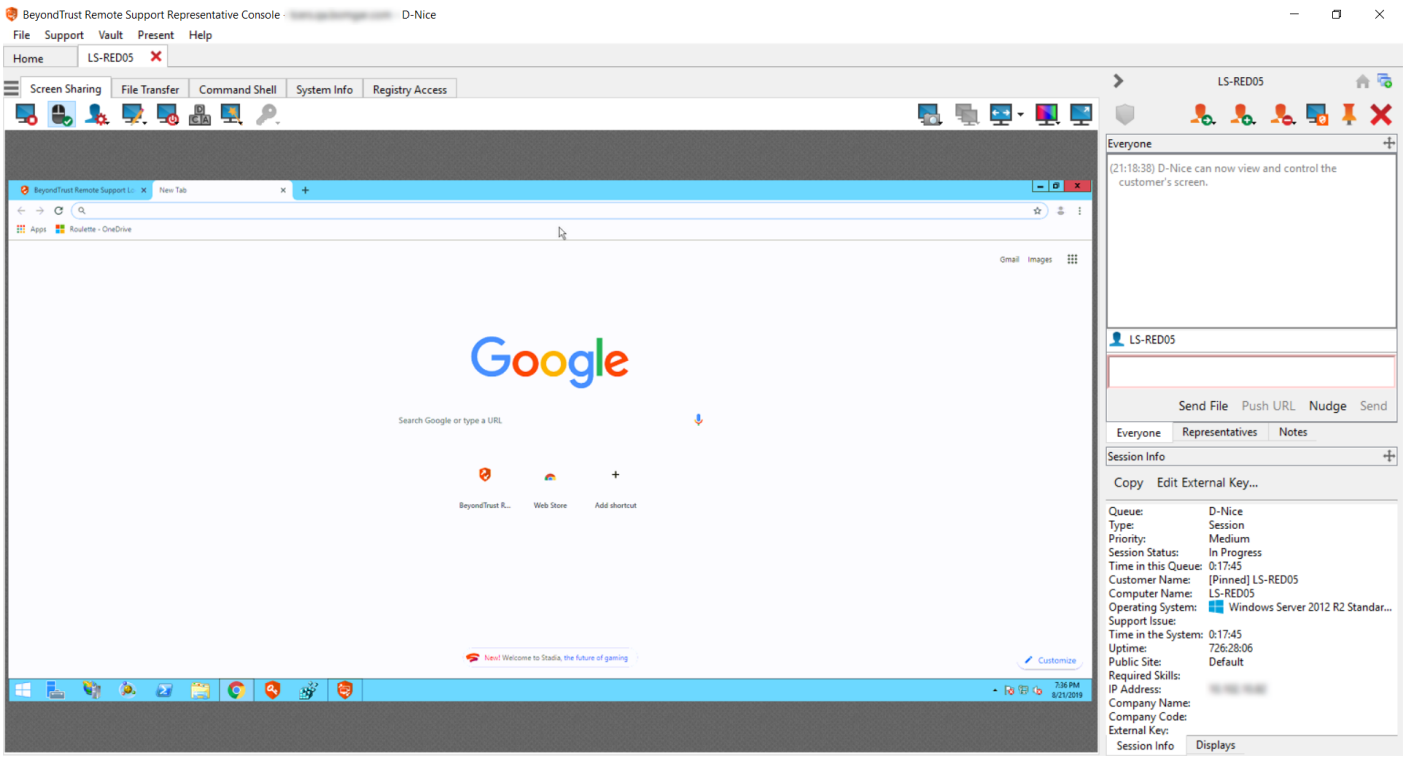


Hinweis: *Jump-Elemente können ebenfalls eingestellt werden, um den gleichzeitigen Zugriff auf das gleiche Jump-Element durch mehrere Benutzer zu gestatten. Wenn* ***Bestehender Sitzung beitreten*** *gewählt wurde, können andere Benutzer einer bereits laufenden Sitzung beitreten. Der ursprüngliche Sitzungseigentümer 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 unter www.beyondtrust.com/docs/remote-support/getting-started/admin/jump-items.htm.

Werkzeuge

Überblick über Support-Sitzungen Tech. und Tools



Sitzungswerkzeuge

	Klicken Sie auf das Symbol oben links im Sitzungsfenster, um auf die Sitzungssteuerelemente für Ihre Support-Sitzung Tech. zuzugreifen. Sie können auch auf die Sitzungsregisterkarte rechtsklicken, um auf die Sitzungssteuerelemente zuzugreifen. Mehrere dieser Steuerungen haben eigene Symbole an anderer Stelle auf der Oberfläche und sind unten beschrieben (**Übertragen**, **Einladen**, **Teilnehmer entfernen**, **Heraufsetzen**, **Support Button bereitstellen**, **Jump-Client bereitstellen**, **Benutzerdefinierte Links**, **Schließen**). Wählen Sie aus dem Menü **Sitzungsregisterkarte lösen**, um die Sitzung aus der Konsole zu lösen, oder klicken Sie auf die Sitzungsregisterkarte und ziehen Sie diese vom Hauptfenster weg. Das Menüsymbol verbleibt in der Sitzung, auch wenn Sie die Sitzungsregisterkarte lösen. So können Sie die Sitzungsregisterkarte beliebig positionieren, etwa auf einem anderen Monitor, und haben weiterhin Zugriff auf die Sitzungs-Tools. Sie können die Sitzung mit der Option **Sitzungsregisterkarte anheften** wieder anheften, oder indem Sie auf das X klicken, um das gelöste Fenster zu schließen. Darüber hinaus können Sie aus dem Menü **Seitenleiste lokalisieren** wählen, um die Seitenleiste für die Sitzung zu finden. Dies hilft, wenn Sie über mehrere gelöste Sitzungsseitenleisten (siehe unten) verfügen, die auf Ihrem Bildschirm verteilt sind. Sie können die Sitzung auch umbenennen oder den Namen auf den Standardwert zurücksetzen.
 	Klappen Sie die Seitenleiste ein, um Ihren Sitzungs-Arbeitsbereich zu maximieren. Um die Seitenleiste wieder zu fixieren, fahren Sie über den Pfeil der eingeklappten Seitenleiste und klicken Sie auf das Symbol **Seitenleiste fixieren**.
 	Klicken Sie auf dieses Symbol, um die Seitenleiste zu lösen. Nach dem Lösen kann die Seitenleiste beliebig auf Ihrem Desktop oder auf einem separaten Monitor positioniert werden. Die Seitenleiste kann auch entsprechend Ihrer Bedürfnisse in der Größe angepasst werden. Alternativ können Sie auch das Fenster in der Seitenleiste in der Größe verändern, um mehr Platz zu erhalten. Klicken Sie auf das Symbol **Seitenleiste anheften**, um die Seitenleiste wieder anzuheften. Wenn die Seitenleiste angeheftet ist, wird das Symbol **Start** aktiviert (siehe unten).
	Das Symbol **Start** ist aktiviert, wann immer die Seitenleiste gelöst wird. In Fällen, bei denen gleichzeitig mehrere Sitzungen ausgeführt werden und sich mehrere gelöste Seitenleisten auf Ihrem Bildschirm befinden, können Sie auf das **Start**-Symbol einer Seitenleiste klicken, um die dazugehörige Sitzung in den Vordergrund zu bringen. So ersparen Sie sich Zeit und Verwirrung beim Versuch, jede Seitenleiste der entsprechenden Sitzung zuzuordnen.
 	Es ist möglich, die unterschiedlichen Widget-Sektionen der Seitenleiste, wie etwa das Chat-Fenster, das Sitzungsinformationen-Fenster usw. neu zu positionieren. Wenn Sie über die Titelleiste einer Sektion fahren, verwandelt sich der Mauszeiger in eine geschlossene Hand. So können Sie diese Sektion auf der Seitenleiste ziehen und neu positionieren.

 	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 Schildschaltfläche 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 Kennwort mit Administratorrechten anzugeben. 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. 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.
	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.
	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 oder eines externen Benutzers erhalten. Sie können zudem einen Zugriffssponsor beantragen, der bestimmte Handlungen für Sie durchführen kann.
	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, um Notizen hinzuzufügen oder die zuletzt abgerufenen Systeminformationen anzuzeigen.
 	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.
 	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. Um Details festzulegen, darunter Kennwort, Kommentare, Gruppe usw., wählen Sie **Anpassen**.
	Öffnen Sie einen Webbrowser auf Ihrem Computer und geben Sie eine von Ihrem Administrator vorgegebene Website ein. Diese Schaltfläche kann darauf konfiguriert werden, detaillierte Informationen zur Sitzung, zum Endkunden und/oder dem BeyondTrust-Benutzer, der den benutzerdefinierten Link öffnet, zu beinhalten. Wenn z. B. der externe Schlüssel mit der einzigartigen Kennung eines in Ihrem Verwaltungssystem für Kundenbeziehungen vorhandenen Falls übereinstimmt, können Sie durch das Anklicken dieser Schaltfläche den dazugehörigen Fall im externen System aufrufen.

	Wird ein kompatibles iOS-Gerät erkannt, erscheint das Symbol **Spezielle Aktionen** und ermöglicht es dem Support-Techniker, iOS-Bildschirmfreigabeanweisungen auf das Gerät zu pushen. Weitere Informationen zur Bildschirmfreigabe unter iOS finden Sie in Bildschirmfreigabe mit dem iOS-Gerät unter https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/apple-ios/ios-screen-sharing.htm.
	Sitzungsregisterkarte ganz schließen. Falls Sie Eigentümer der Sitzung sind, können Sie den Kunden-Client entweder vom Remote-Rechner deinstallieren oder den Kunden in der Warteschlange lassen, damit ein anderer Support-Techniker die Sitzung fortsetzt. Sie können die Sitzung von der Seitenleiste, dem Sitzungsmenü oder der Sitzungsregisterkarte aus schließen.

Unten rechts im Sitzungsfenster werden Informationen zum Remote-System angezeigt, zusammen mit jeglichen anderen Informationen, die der Kunde womöglich im Kontaktformular für Problemfälle angegeben hat. Dies kann Folgendes umfassen:

- **Typ**: Den Sitzungstyp.
- **Priorität**: Die Prioritätsstufe (Niedrig, Mittel (Standard) oder Hoch) der Anforderung, abhängig von den vom BeyondTrust-Administrator definierten Support-Problemen.
- **Warteschlange**: Die persönliche Warteschlange des Support-Technikers, der Eigentümer der Sitzung ist.
- **Sitzungsstatus**: Warten (kein Support-Techniker beigetreten), Läuft (Support-Techniker und Kunde beigetreten) oder Kunde abwesend (Support-Techniker beigetreten, aber Kunde hat Sitzung verlassen).
- **Name des Kunden**: Dies ist entweder der zum Sitzungsbeginn vom Kunden eingegebene Name, der Benutzername des angemeldeten Benutzers, der Hostname des Kundensystems (für gepushte und fixierte Sitzungen) oder des Dienstes (für heraufgesetzte Sitzungen).
- **Name des Computers**: Den Hostnamen des Kundensystems, wie in den Systemeinstellungen aufgeführt.
- **Plattform**: Das Betriebssystem des Kunden.
- **Support-Problem**: Falls ein Problem ausgewählt wurde, zeigt dies den Namen des Problems an, das der Kunde ausgewählt hat.
- **Zeit im System**: Dies verfolgt die verstrichene Zeit, sobald die Sitzung in die erste Warteschlange gestellt wurde.
- **Öffentliche Website**: In der Regel wird dies standardmäßig aufgeführt. Wenn jedoch nicht standardmäßige Websites vorhanden sind, können diese ebenfalls aufgeführt sein.
- **Erforderliche Qualifikationen**: Qualifikationen, die mit dem vom Kunden gewählten Problem verknüpft sind. Der BeyondTrust-Administrator erstellt über die BeyondTrust /login-Schnittstelle Qualifikationen und weist diese Problemen zu.
- **IP-Adresse**: Die öffentliche und/oder private IP-Adresse des lokalen Kundensystems.

Hat Ihr Administrator die XML API aktiviert, können Sie einen externen Schlüssel für die Verwendung in Sitzungsberichten festlegen. Jegliche von Ihrem Administrator aktivierten benutzerdefinierten Sitzungsattribute erscheinen in einer Registerkarte **Benutzerdefinierte Informationen**. Klicken Sie auf **Kopieren**, um alle Informationen in die Zwischenablage zu kopieren.

Eine weitere Option, die Ihr Administrator aktivieren kann, ist die Möglichkeit, den Windows-Benutzer automatisch abzumelden oder den Remote-Computer beim Schließen der Sitzung zu sperren. Falls Sie z. B. auf einem unüberwachten System gearbeitet haben, wird das Sperren des Computers empfohlen, um zu verhindern, dass nicht autorisierte Benutzer vertrauliche Informationen einsehen können. Wählen Sie die vorzunehmende Aktion aus dem Dropdown-Menü unten am Fenster.

Anmelden in Remote-Systemen mithilfe der Anmeldedaten-Einfügung über die Konsole d. Support-Technikers

Beim Zugriff auf ein Windows-basiertes Jump-Element in der Konsole d. 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 Kennwortspeicher 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.

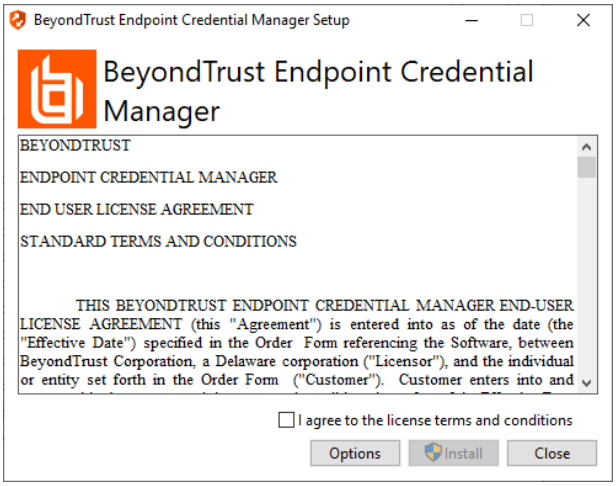
> ***Hinweis:*** *Der ECM muss auf Ihrem System installiert werden, damit der BeyondTrust ECM-Dienst aktiviert und die Anmeldedateneinfügung in BeyondTrust Remote Support ermöglicht werden kann.*

Systemanforderungen

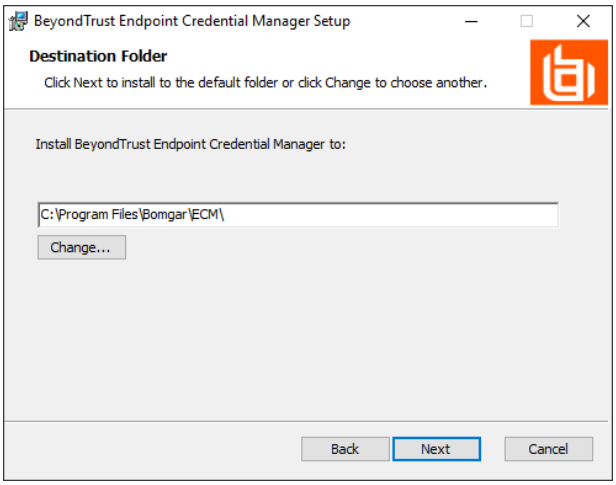
- Windows Vista oder neuer, nur 64 Bit
- .NET 4.5 oder neuer
- Prozessor: 2 GHz oder schneller
- Speicher: 2 GB oder mehr
- Verfügbarer Festplattenspeicherplatz: 80 GB oder mehr

1. Laden Sie zunächst den BeyondTrust Endpunkt-Anmeldedaten-Manager (ECM) von BeyondTrust Support unter https://www.beyondtrust.com/docs/index.htm#support herunter. Starten Sie den Installationsassistenten für den BeyondTrustEndpunkt-Anmeldedaten-Manager.
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.

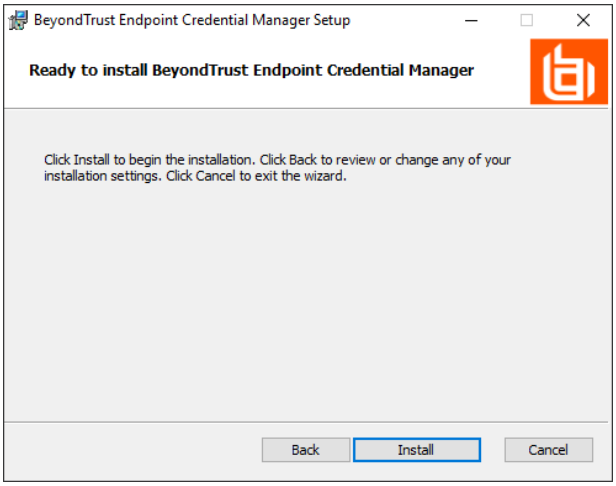
> ***Hinweis:*** *Sie können mit der Installation erst fortfahren, wenn Sie der Endbenutzer-Lizenzvereinbarung zustimmen.*



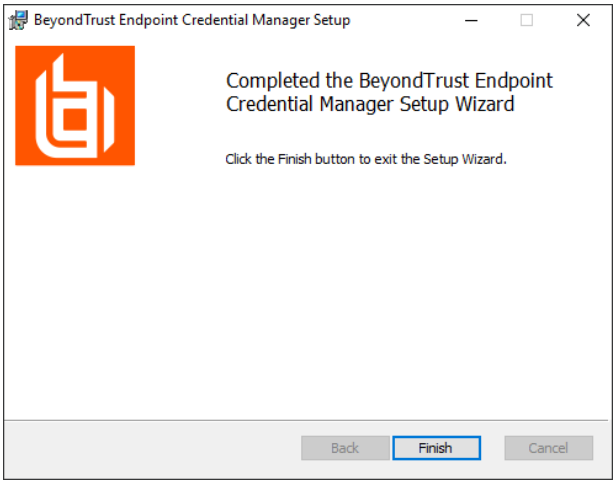
3. Wählen Sie den Installationsort für den Anmeldedaten-Manager und klicken Sie auf **Weiter**.
4. Auf dem nächsten Bildschirm können Sie mit der Installation beginnen oder vorherige Schritte überprüfen.



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



6. 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 Secure Remote Access Appliance mit der gleichen Site zu kommunizieren. Eine Liste der mit der Geräte-Site verbundenen ECMs finden Sie in* ***/login > Status > Informationen > ECM-Clients****.*

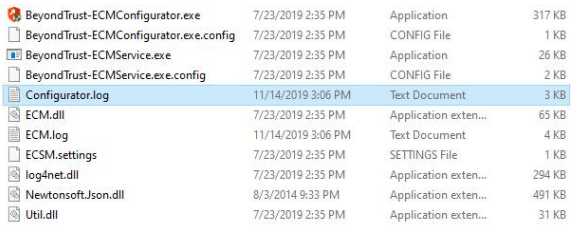
> ***Hinweis:*** *Wenn mehrere ECMs mit einer BeyondTrust-Site verbunden sind, leitet das Secure Remote Access Appliance Anfragen an den ECM weiter, der am längsten mit dem Gerät verbunden ist.*

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

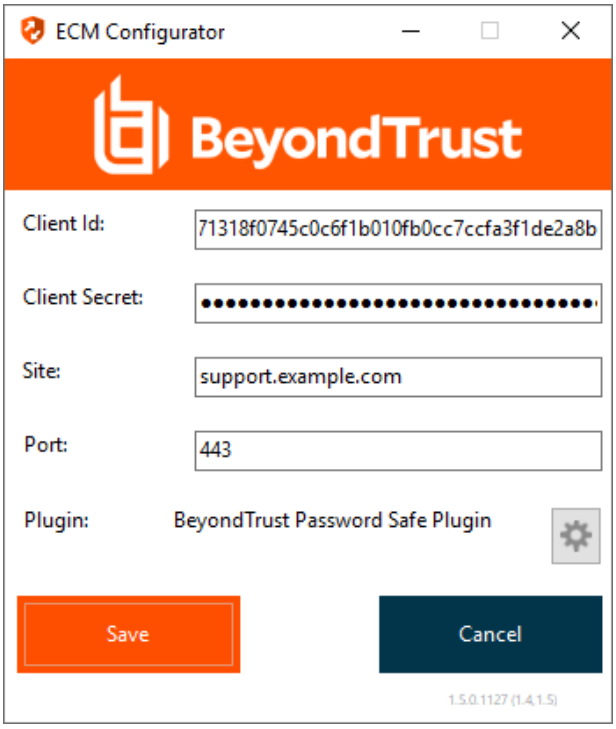
Konfiguration einer Verbindung zu Ihrem Anmeldedaten-Speicher

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 **Start**menü 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.



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.

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

***Hinweis:** Wenn Sie sich mit einem Kennwort-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!

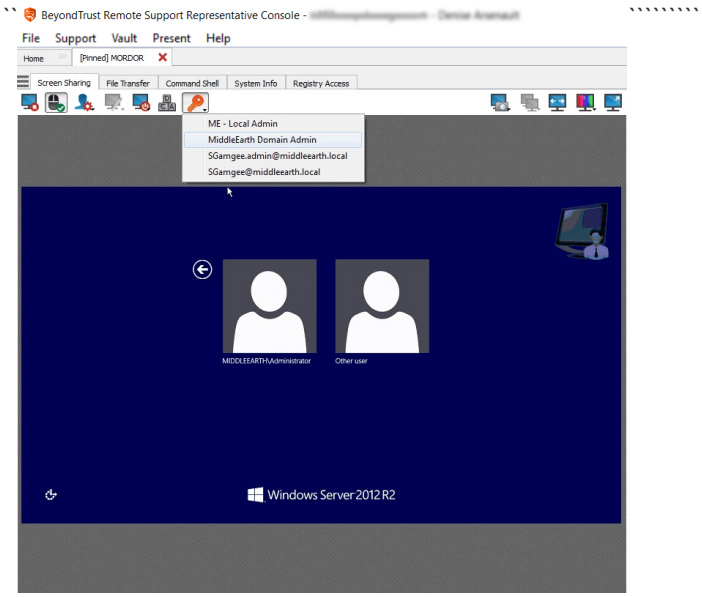
Um die neuen Einstellungen in der Konfiguration zu übernehmen, starten Sie den Anmeldedaten-Manager-Dienst neu.

Verwendung der Anmeldedaten-Einfügung zum Zugriff auf Remote-Systeme

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

1. Melden Sie sich in der Konsole d. 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-Anmeldungsbildschirm ein.
6. Der Support-Techniker wird am Remote-System angemeldet.



Aus bevorzugten Anmeldedaten zur Einfügung wählen

Nachdem sich ein Support-Techniker mit Anmeldedaten an einem Endpunkt angemeldet hat, speichert das System die bevorzugten Anmeldedaten des Benutzers für den Endpunkt sowie den Kontext, in dem sie benutzt worden sind (um sich anzumelden, um eine Sonderaktion auszuführen, für eine Heraufsetzung oder zum Pushen), in der Gerätedatenbank. Wenn der Benutzer beim nächsten Mal Anmeldedaten für den Zugriff auf denselben Endpunkt benutzen möchte, empfiehlt das Anmeldedaten-Einfügungsmenü, welche Anmeldedaten verwendet werden sollen. Die Anmeldedaten werden auf der Anmeldedaten-Liste ganz oben angezeigt, gefolgt von verbleibenden Anmeldedaten. Ist zu einem Endpunkt kein Anmeldedaten-Verlauf vorhanden, zeigt das Gerät einfach alle möglichen Anmeldedaten an.

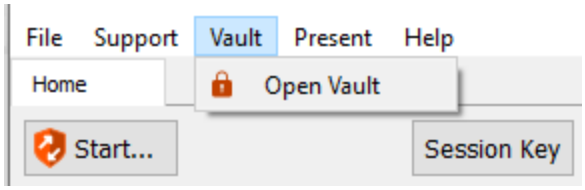
Die Anmeldedaten-Liste empfiehlt höchstens fünf Anmeldedaten.

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

Auschecken und Einchecken von Vault-Anmeldedaten

Von der Konsole d. 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 außerhalb einer Sitzung direkt am Konsole d. Support-Technikers.

Um auf den Vault zuzugreifen, wählen Sie das Menüelement **Vault > Vault öffnen**. Sie gelangen direkt auf die Seite **Vault > Konten** in der Schnittstelle **/login**, wenn Sie angemeldet sind.

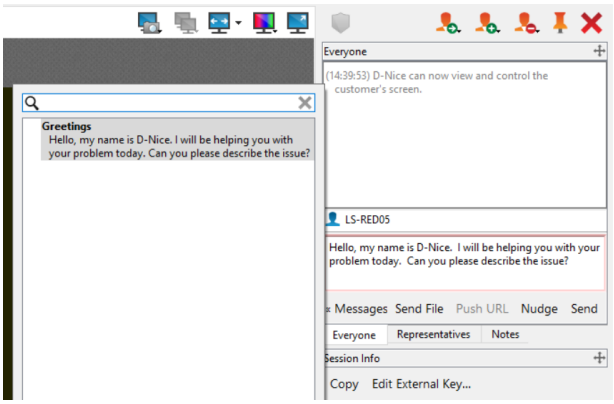


> ***Hinweis:*** *Wenn Sie nicht angemeldet sind, werden Sie aufgefordert, Ihre Anmeldedaten einzugeben. Sie gelangen dann auf die Seite Vaultkonten. Wenn Sie bereits in einem Browser-Fenster angemeldet sind, werden Sie nicht nach Ihren Anmeldedaten gefragt und gelangen direkt auf die Vault-Seite.*

Sie können dann ein Vaultkonto auswählen und auschecken oder einchecken.

Während einer Sitzung mit dem Kunden chatten

Während der gesamten Support-Sitzung Tech können Sie mit Ihrem Remote-Kunden chatten. Sie benötigen keine Erlaubnis für eine Bildschirmfreigabe, bevor Sie die Chat-Sitzung starten. Falls in den Einstellungen der Konsole d. Support-Technikers aktiviert, erhalten Sie Popup-Benachrichtigungen, wenn Sie Chatnachrichten erhalten. Wenn Sie Ihr Foto oder ein Avatarbild hochgeladen haben, wird es nach dem Beginn des Chat im Chatfenster des Kunden angezeigt.



Klicken Sie auf das Pfeilsymbol oben links in der Seitenleiste, um die Schiebe-Seitenleiste einzuklappen. Ist die Schiebe-Seitenleiste eingeklappt, fahren Sie über den Pfeil neben dem verborgenen Fenster, um es anzuzeigen. Klicken Sie auf das Fixierungssymbol, das das Pfeilsymbol oben links in der Seitenleiste ersetzt hat, um die Schiebe-Seitenleiste erneut zu fixieren.

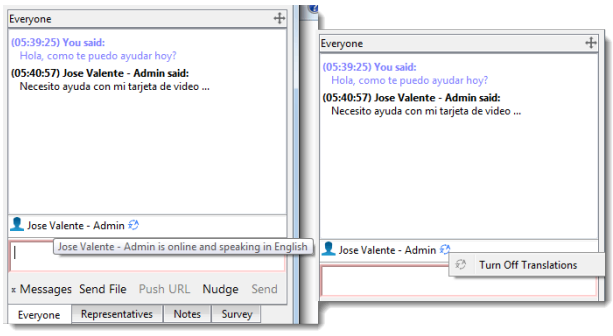
Wenn Sie Englisch schreiben, werden Rechtschreibfehler rot unterstrichen. Rechtsklicken Sie zur Anzeige von Rechtschreibungsvorschlägen, oder um diese Schreibweise für die aktuelle Konsolensitzung zu ignorieren.

Ist die Echtzeit-Chatübersetzung aktiviert, können Kunden in ihrer eigenen Sprache mit einem Support-Techniker chatten. So kann beispielsweise ein englischsprachiger Kunde mit einem Support-Techniker chatten, der nur Niederländisch spricht, wobei der Chatverkehr in Echtzeit übersetzt wird.

> *Weitere Informationen zur Konfiguration von Chat-Übersetzungen in Echtzeit finden Sie in Echtzeit-Chatübersetzung unter https://www.beyondtrust.com/docs/remote-support/videos/real-time-chat-translation.htm.*

> *Weitere Informationen zur Konfiguration der Chat-Übersetzung in Echtzeit finden Sie in Echtzeit-Chat: Übersetzen von Chatnachrichten zwischen Support-Techniker und Kunde unter https://www.beyondtrust.com/docs/remote-support/getting-started/admin/real-time-chat.htm.*

Wenn Sie mit dem Mauszeiger über den Namen des Support-Technikers fahren, wird angezeigt, welche Sprache zur Übersetzung der an den Kunden gesandten Nachrichten verwendet wird. Im gezeigten Beispiel wird der Support-Techniker als „online und englischsprachig“ angezeigt, obwohl der Support-Techniker seinen Text auf Spanisch eingibt.



Sie können Übersetzungen deaktivieren, indem Sie einen Rechtsklick auf das Übersetzungssymbol ausführen und dann auf **Übersetzungen deaktivieren** klicken. Um Übersetzungen wieder zu aktivieren, führen Sie einen Rechtsklick auf das Symbol aus und wählen Sie **Übersetzungen aktivieren**. Es ist für den Kunden nicht möglich, den Übersetzungsprozess auf seiner Seite zu deaktivieren.

Wenn Ihr Administrator vordefinierte Meldungen konfiguriert hat, können Sie auf die Schaltfläche **Meldungen** im unteren linken Bereich der Chat-Eingabe klicken, um zuvor geschriebene Nachrichten in den Chat einzugeben. Klicken Sie auf den Pfeil links neben einem

Kategorienamen, um die Meldungen und Unterkategorien einzusehen. Geben Sie Begriffe in das Suchfeld ein, um nach einer bestimmten Meldung zu suchen.

Meldungen werden als einfacher Text im Chat-Eingabebereich angezeigt. Sie können in einer Meldung BBCode-Tags hinzufügen oder bearbeiten, um Text zu formatieren. Die Formatierung wird beim Senden der Nachricht angewendet.

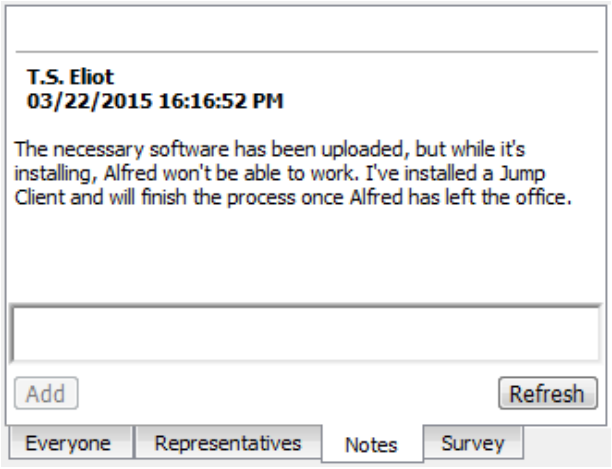
Um eine Datei über die Chat-Schnittstelle zu pushen, klicken Sie auf **Datei senden**. Wenn Sie eine URL über die Chat-Schnittstelle pushen, wird automatisch auf dem Remote-System ein Browser geöffnet und zur jeweiligen Website geleitet. Um eine URL zu pushen, muss die Internetadresse der einzige Text im Feld sein.

Klicken Sie auf **Anstupsen**, um die Aufmerksamkeit Ihres Kunden auf sich zu lenken. Dadurch wird der Fokus auf den Kunden-Client gelenkt, dieser gerüttelt und auf dem Remote-System ein Alarmton wiedergegeben. Der Stups wird im Chat-Verlauf protokolliert. Nachdem Sie einen Stups abgeschickt haben, müssen Sie ein paar Sekunden warten, bevor Sie einen weiteren Stups senden können.

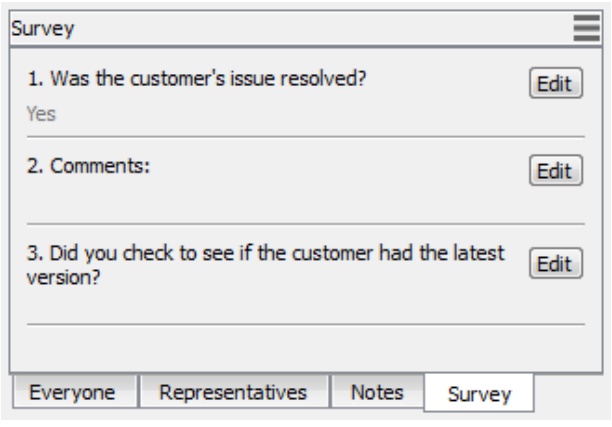
Das Chat-Fenster zeichnet nicht nur die Nachrichten und die Zeit des Sendens auf, sondern dient auch als laufendes Protokoll aller Aktivitäten während der Sendung, inklusive übertragener Dateien und erteilter Berechtigungen.

Falls ein oder mehrere Support-Techniker die Sitzung freigeben, können Sie mit allen Teilnehmern chatten oder aber nur privat mit den anderen Support-Technikern. Wenn ein weiterer Benutzer einer freigegebenen Sitzung beitritt, kann er den Chat-Verlauf der letzten Minuten einsehen.

Sie können auch Notizen zur Sitzung hinzufügen. Wird die Sitzung freigegeben oder übertragen, können diese Notizen von einem Support-Techniker übertragen und von einem anderen abgerufen werden, um die Situation schnell und vertraulich zu beurteilen. Diese Notizen stehen auch im Sitzungsbericht zur Verfügung. Notizen können sowohl während der Sitzung als auch nach Beendigung der Remote-Verbindung hinzugefügt werden.



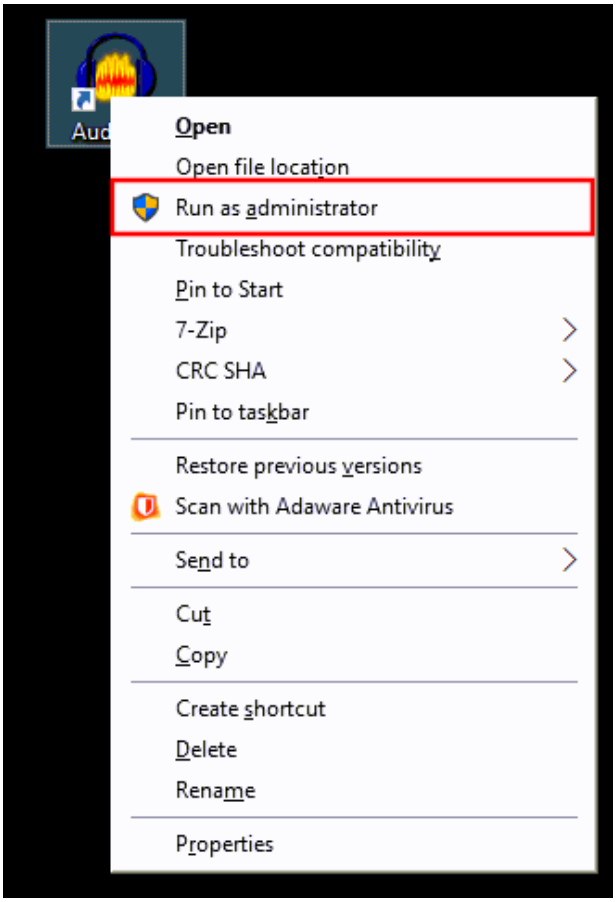
Ihr Administrator ermöglicht es Ihnen unter Umständen ebenfalls, während der Sitzung auf die Support-Techniker-Umfrage zuzugreifen. In diesem Szenario kann die Umfrage als Arbeitsablaufvorlage verwendet werden und ermöglicht es Ihrem Administrator, eine Reihe von Fragen und/oder Kontrollpunkten aufzustellen sowie bestimmte Links, die Sie in Ihrer Support-Sitzung Tech brauchen könnten.



> ***Hinweis:*** *Es ist möglich, die unterschiedlichen Widget-Sektionen der Seitenleiste, wie etwa das Chat-Fenster, das Sitzungsinformationen-Fenster usw. neu zu positionieren. Wenn Sie über die Titelleiste einer Sektion fahren, verwandelt sich der Mauszeiger in eine geschlossene Hand. So können Sie diese Sektion auf der Seitenleiste ziehen und neu positionieren.*

Den Client heraufsetzen

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. Sobald Sie eine Sitzung heraufgesetzt haben, können Sie sich mit dem bestehenden Benutzerkonto ab- und mit einem Administratorkonto anmelden, oder **Als Administrator ausführen** wählen, um Befehle oder Programme im Kontext eines Administrators auszuführen.

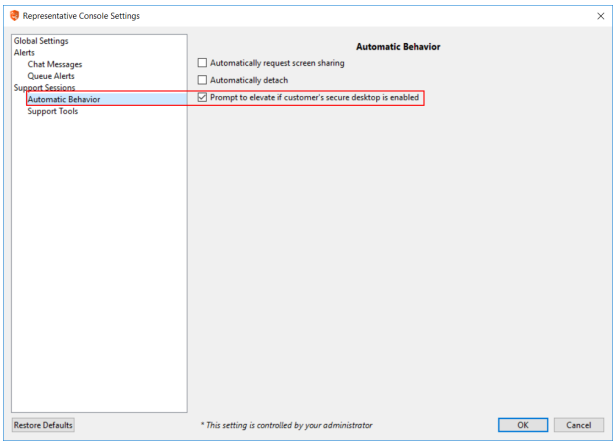


Heraufsetzung

Um den Kunden-Client auf Administratorrechte heraufzusetzen, klicken Sie auf die Schaltfläche **Heraufsetzen** oben im Sitzungsfenster.

Eine Eingabeaufforderung für Anmeldedaten erscheint. Eine Aufforderung zur Heruafsetzung erscheint auch, wenn der Support-Techniker versucht, eine Aktion auszuführen, welche Administratorrechte in einer nicht heraufgesetzten Sitzung erfordert.

Sie können auch Einstellungen in der Konsole d. Support-Technikers konfigurieren, sodass der Benutzer am Remote-Gerät automatisch aufgefordert wird, wenn der sichere Desktop aktiviert ist. Diese Einstellung finden Sie unter **Datei > Einstellungen > Support-Sitzungen > Automatisches Verhalten**. Diese Einstellung kann auch global in der /login-Schnittstelle auf der Seite **Konsole des Support-Technikers**



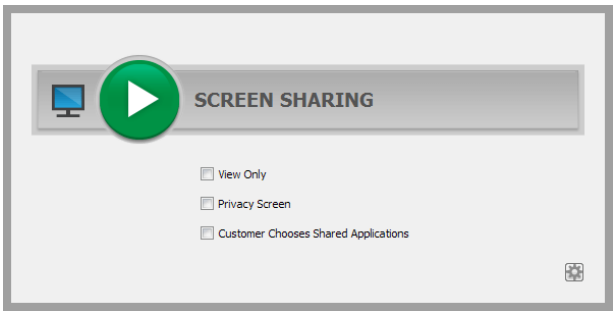
> Einstellungen der Konsole des Support-Technikers unter **Einstellungen für Konsole des Support-Technikers verwalten** konfiguriert werden.

Weitere Informationen zur Heraufsetzung finden Sie in folgenden Artikeln:

- *Sitzung in der Web-Konsole des Support-Technikers heraufsetzen unter https://www.beyondtrust.com/docs/remote-support/getting-started/rep-web/elevate.htm*
- *Rechte im Kunden-Client über die Android-Konsole des Support-Technikers heraufsetzen unter https://www.beyondtrust.com/docs/remote-support/getting-started/rep-android/elevate.htm*
- *Rechte im Kunden-Client über die iOS-Konsole des Support-Technikers heraufsetzen unter https://www.beyondtrust.com/docs/remote-support/getting-started/rep-ios/elevate.htm*
- *Einen Jump-Client, Jumpoint oder Heraufsetzungsservice für den heraufgesetzten Sitzungsstart installieren unter https://www.beyondtrust.com/docs/remote-support/how-to/smart-card/jump-client-installation.htm*

Bildschirmfreigabe bei Remote-Kunde für Anzeige und Steuerung

Klicken Sie im Sitzungsfenster auf **Bildschirmfreigabe**, um die Steuerung des Remote-Computers anzufordern. Abhängig von Ihren Kontoeinstellungen können unterhalb der Schaltfläche weitere Optionen zur Verfügung stehen. Klicken Sie auf die Zahnrad-Schaltfläche, um die Optionen anzuzeigen.



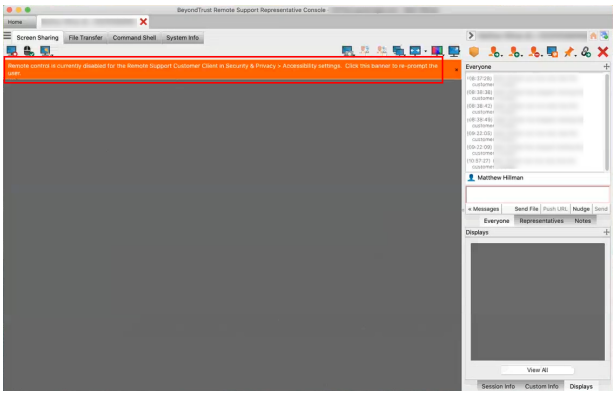
Optionen zur Bildschirmfreigabe

- Verbleiben alle Optionen deaktiviert, wird die vollständige Bildschirmfreigabe angefordert, welche die Ansicht oder Steuerung des gesamten Desktops des Remote-Systems und aller Anwendungen gewährt.
- Wenn Sie **Vollen Zugriff** aktivieren (verfügbar nur in einer kundenseitig initiierten Sitzung), fordern Sie sowohl die Bildschirmfreigabe- sowie alle anderen Berechtigungen gleichzeitig an.
- Wenn Sie **Nur Anzeigen** auswählen, können Sie den Remote-Bildschirm sehen, aber nicht steuern.
- **Privater Bildschirm** (nur bei Jumps verfügbar), startet die Sitzung mit deaktivierter Ansicht und Steuerung des Remote-Kunden. Der private Bildschirm ist nicht verfügbar, wenn Support für Windows 8 bereitgestellt wird.
- Mit **Kunde wählt die freigegebenen Anwendungen** (nur bei Support eines Windows- oder Mac-Computers verfügbar) kann der Kunde wählen, welche Anwendungen freigegeben werden sollen.

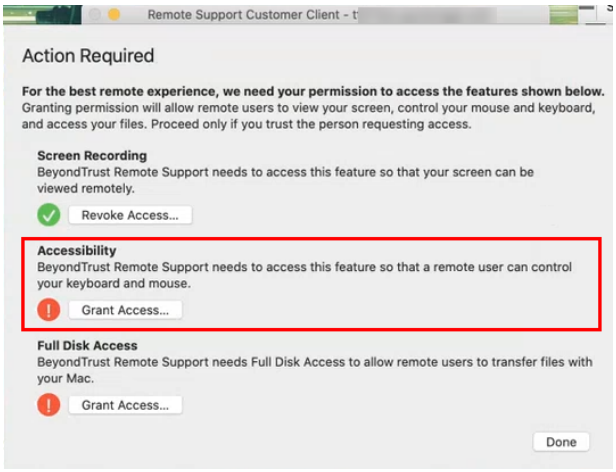
Hat Ihr Administrator Ihr Konto so eingerichtet, dass der Kunde auswählen muss, welche Anwendungen freigegeben werden, ist für Sie nur die beschränkte Bildschirmfreigabe zulässig. Alternativ dazu dürfen Sie evtl. nur eine Anforderung zur vollständigen Bildschirmfreigabe anfordern, oder Sie dürfen auswählen, welche Zugriffsebene Sie anfordern können.

> ***Hinweis:*** *Eine website-weite Einstellung kann Ihrem Kunden, unabhängig von der angeforderten Zugriffsebene, die Beschränkung von Anwendungen ermöglichen, nachdem die Bildschirmfreigabe gestartet wird.*

Klicken Sie bei macOS Catalina (10.15)+-Systemen auf das Banner oben auf der Registerkarte **Bildschirmfreigabe**, wenn die Remote-Steuerung nicht aktiviert ist, um den Benutzer nach Berechtigungen zu fragen.

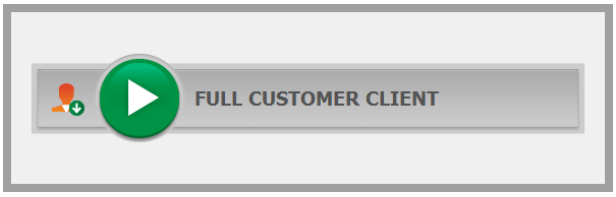


Der Kunde kann dann den Zugriff gewähren, wenn er im Kunden-Client dazu aufgefordert wird, und der Support-Techniker wird zu den richtigen Bereichen in den **Einstellungen** geleitet, um die Berechtigungen zu aktualisieren.

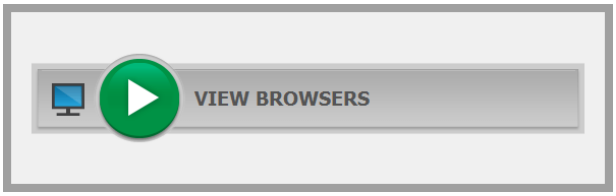


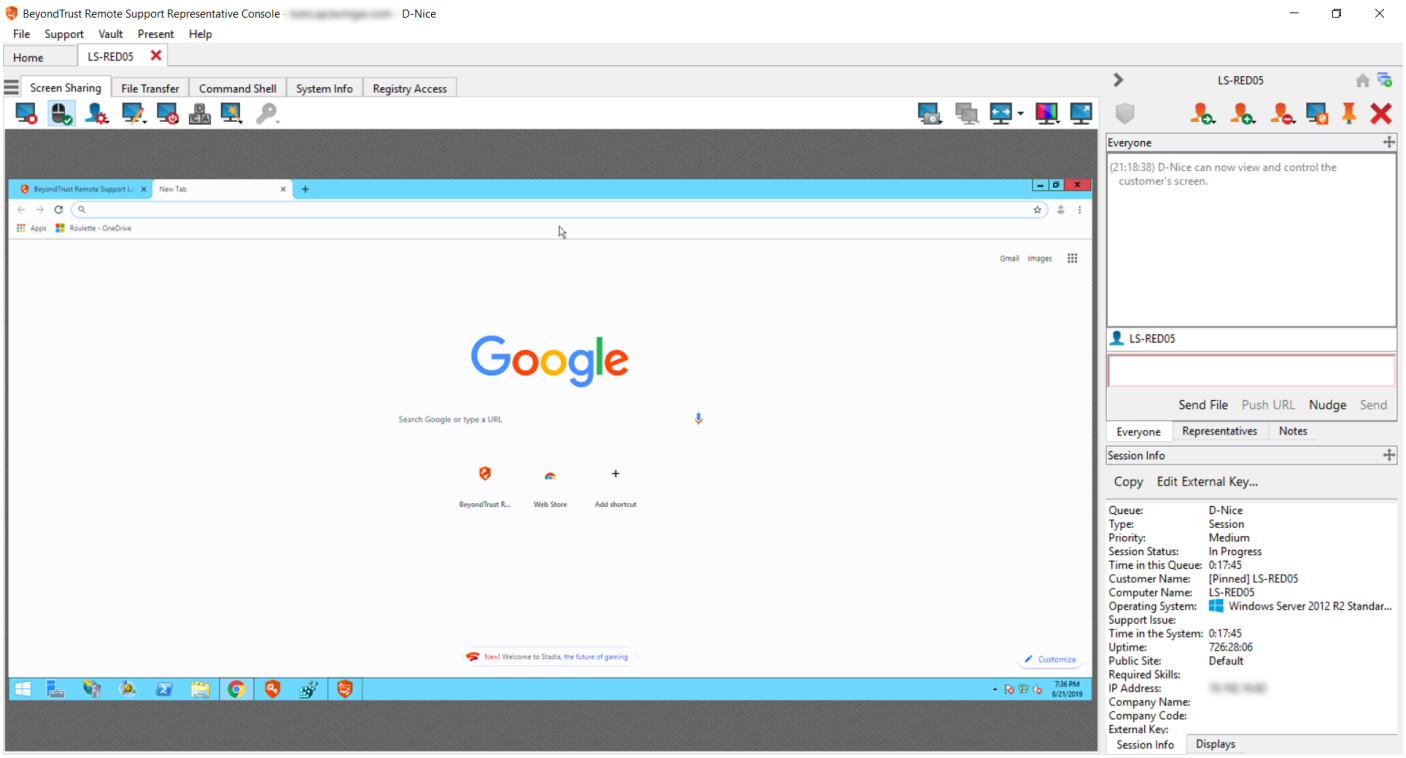
Hat der Kunde die Berechtigung erteilt, werden die aktivierten Anwendungen des Remote-Desktops in Ihrem Fenster angezeigt. Ihr Kunde kann Ihnen schreibgeschützten Zugriff erteilen, oder, falls Ihre Berechtigungen das zulassen, völlige Maus- und Tastatursteuerung, wodurch Sie so auf dem Remote-Computer arbeiten können, als ob Sie davor sitzen würden. Sie können jederzeit während der Sitzung anfordern, Ihre Berechtigungsstufe zu erhöhen.

In einer Click-to-Chat-Sitzung können Sie nur mit dem Kunden chatten und grundlegende Details zur Sitzung einsehen. Wenn Sie umfassenderen Support zur Verfügung stellen müssen, fordern Sie die Heraufsetzung der Sitzung zum vollen Kunden-Client an.



Bei Browserfreigabe-Sitzungen ist die Bildschirmfreigabe nur in einem eingeschränkten Modus verfügbar, da nur die Remote-Browser angezeigt werden können. Support-Techniker können weiterhin Anmerkungen verwenden, um auf dem Bildschirm des Kunden zu zeichnen und können ebenfalls den virtuellen Zeiger verwenden. Bei der Browserfreigabe sind die Registerkarten **Dateitransfer**, **Befehlsshell** und **Systeminfo** nicht verfügbar. Wird die Aufzeichnung der Bildschirmfreigabe aktiviert, werden Browserfreigabe-Sitzungen aufgezeichnet.





Bildschirmfreigabe-Werkzeuge

	Bildschirmfreigabe beenden.
	Bei Arbeiten auf dem Remote-Computer können Sie die Steuerung der Tastatur oder Maus anfordern bzw. beenden.
	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. 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. 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.
	Anmerkungswerkzeuge ermöglichen es Ihnen, Kunden durch komplexere Aufgaben zu führen und dezentral arbeitende Mitarbeiter anzuleiten, wodurch die Anzahl der Rückrufe und damit die Schulungskosten gesenkt werden. Eine Reihe von Werkzeugen steht zur Verfügung, darunter Formen und freies Zeichnen. BeyondTrust InSight ermöglicht Anmerkungen auf einem Live-Kamera-Feed eines Android- oder iOS-Geräts. Beachten Sie, dass Anmerkungen bei bestimmten mobilen Plattformen besondere Anforderungen haben. Um mehr über BeyondTrust InSight zu erfahren, lesen Sie weiter unter BeyondTrust InSight für iOS oder BeyondTrust InSight für Android.
	Starten Sie das Remote-System entweder im normalen oder im abgesicherten Modus mit Netzwerk-Funktion neu, oder fahren Sie das Remote-System herunter. Sie können den Endbenutzer auch auffordern, gültige Anmeldedaten einzugeben, damit der Support-Techniker nach einem Neustart wieder mit den angegebenen Anmeldedaten angemeldet werden kann, ohne dass der Kunde anwesend sein muss. Weitere Details finden Sie in „Daten zur automatischen Anmeldung: Neustart und Neuverbindung“ auf Seite 129.
	Senden Sie einen **Strg-Alt-Entf**-Befehl an den Remote-Computer.
	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 Skripts, die für den Benutzer verfügbar sind, erscheinen in einem erweiterbaren Menü.
	Greifen Sie auf eine Dropdown-Liste verfügbarer Smart-Card-Lesegeräte auf Ihrem lokalen System zu. Verwenden Sie die virtuelle Smart-Card, um administrative Aktionen durchzuführen, Programme in einem anderen Benutzerkontext auszuführen oder, um sich als ein anderer Benutzer anzumelden. Um die Smart-Card-Berechtigungen auf einem Remote-System nutzen zu können, müssen Sie die Sitzung über einen heraufgesetzten Jump-Client, einen Jumpoint oder einen lokalen Netzwerk-Jump starten. Die richtigen Treiber für die virtuelle Smart-Card müssen sowohl auf Ihrem lokalen System als auch auf dem Remote-System installiert werden, während die Dienste laufen.

	Beginnen Sie mit der iOS-Bildschirmfreigabe. Einzelheiten finden Sie in Support für Apple iOS-Geräte auf www.beyondtrust.com/docs/remote-support/getting-started/customer-client/apple-ios/index.htm. Bei der Bereitstellung von Support für ein System mit Apple OS X 10.10 oder höher, an dem ein Mobilgerät mit Apple iOS 8.0.1 oder höher angeschlossen ist, klicken Sie auf diese Schaltfläche, um auf dem angeschlossenen iOS-Gerät die Nur-Anzeige-Bildschirmfreigabe zu beginnen oder zu beenden. Beachten Sie, dass diese Schaltfläche erst bei einer standardmäßigen Bildschirmfreigabe-Support-Sitzung Tech mit einem Apple OS X Yosemite-System sichtbar wird. Die Schaltfläche wird erst aktiviert, wenn ein Gerät mit Apple iOS 8.0.1 oder höher mit dem OS X Yosemite-System verbunden wird.
	Während der Bildschirmfreigabe können Sie eine Bildschirmaufnahme des Remote-Bildschirms bzw. der Remote-Bildschirme mit voller Auflösung im PNG-Format aufnehmen. Speichern Sie die Bilddatei in Ihrem lokalen System oder in der Zwischenablage. Die Aufzeichnungs-Aktion wird im Chat-Protokoll mit einem Link zum lokal gespeicherten Bild aufgezeichnet. Der Link bleibt aktiv, selbst wenn der Kunde die Sitzung verlassen hat, wird aber nicht im BeyondTrust-Sitzungsbericht gespeichert. Sie können das Zielverzeichnis für Bildschirmaufnahmen im Menü **Datei > Einstellungen > Support-Tools** in der Konsole d. Support-Technikers ändern. Dies funktioniert auf Mac, Windows und Linux.
	Sie können die Inhalte Ihrer Zwischenablage manuell an den Remote-Computer senden. Dieses Werkzeugsymbol wird nicht angezeigt, wenn Sie die Berechtigung zum automatischen Senden der Inhalte Ihrer Zwischenablage haben, oder wenn Sie nicht die Berechtigung zum Senden der Zwischenablage an das Remote-System haben.
	Sie können die Inhalte der Zwischenablage manuell vom Remote-Computer empfangen. Dieses Werkzeugsymbol wird nicht angezeigt, wenn Sie die Berechtigung zum automatischen Abrufen der Inhalte der Zwischenablage haben, oder wenn Sie nicht die Berechtigung zum Abrufen der Zwischenablage des Remote-Systems haben.
	Einen alternativen Remote-Bildschirm für die Anzeige auswählen. Der primäre Monitor wird mit einem **P** gekennzeichnet.
	Den Remote-Bildschirm in der tatsächlichen Größe oder skaliert anzeigen.
	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.
	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.

Verwenden Sie Anmerkungen, um auf dem Bildschirm des Remote-Benutzers zu zeichnen

Nutzen Sie Anmerkungswerkzeuge, um Kunden durch komplexere Aufgaben zu führen und dezentral arbeitende Mitarbeiter anzuleiten, wodurch die Anzahl der Rückrufe und damit die Schulungskosten gesenkt werden. Den Support-Technikern wird eine interaktivere Art des Umgangs mit Kunden ermöglicht, wodurch mögliche frustrierende Situationen vermieden und die Kundenzufriedenheit gesteigert wird.

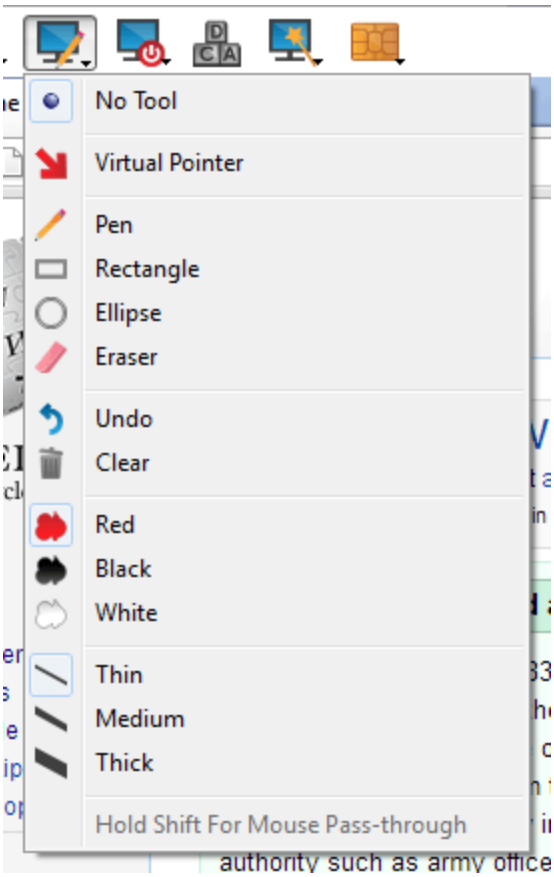
Während Sie sich im Anmerkungsmodus befinden, können Sie trotzdem Ihre Maus bewegen oder Objekte auf dem Desktop des Kunden steuern. Durch Gedrückthalten der **Umschalt**-Taste wird der Anmerkungsmodus vorübergehend unterbrochen.

Anmerkungen aktivieren

Um mit der Verwendung von **Anmerkungen** zu beginnen, klicken Sie auf das Anmerkungssymbol.

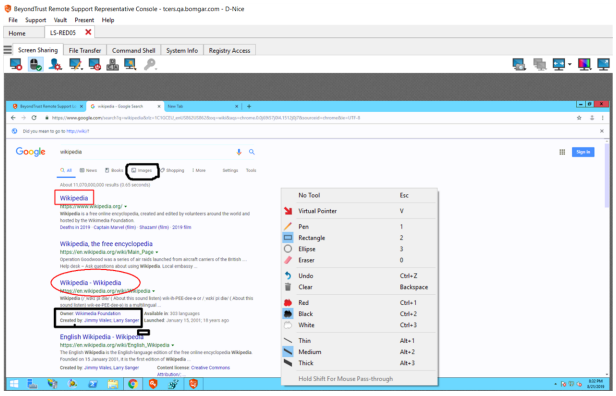
Durch Klicken auf eine beliebige Dropdown-Menüoption wird der **Anmerkungsmodus** eingeschaltet. Sie können aus einer Reihe von Werkzeugen auswählen, mit denen Sie einen Kunden durch eine Reihe von Schritten leiten oder eine Schulungssitzung verbessern können. Die folgenden Werkzeuge und Funktionen stehen zur Verfügung:

- Virtueller Zeiger
- Stift
- Rechteck-Zeichenwerkzeug
- Ellipse-Zeichenwerkzeug
- Radiergummi
- Rückgängig
- Löschen
- Rote, schwarze oder weiße Farbe
- Dünne, mitteldicke oder dicke Linie



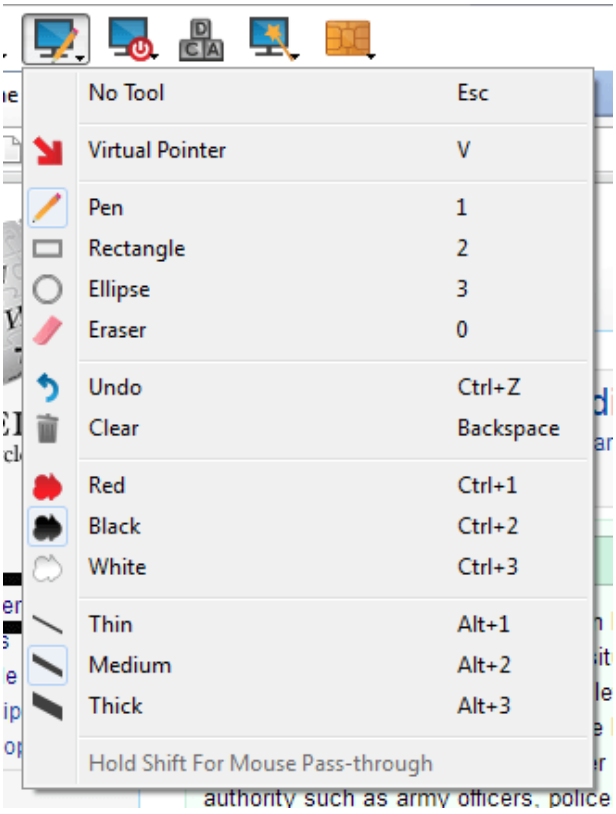
Sie können Ihr Werkzeug aus dem Dropdown-Menü **Anmerkungen** oder durch Rechtsklicken im Remote-Bildschirmbereich auswählen. Wenn Sie in den Bereichen außerhalb des Remote-Bildschirms klicken, wird das Dropdown-Menü nicht angezeigt.

Anmerkungen erscheinen auf dem Remote-Bildschirm, um bei Bedarf die Aufmerksamkeit auf bestimmte wichtige Punkte zu lenken oder Bereiche hervorzuheben.



Um **Anmerkungen** auszuschalten, wählen Sie **Kein Werkzeug** im Dropdown-Menü, oder klicken Sie auf **Esc.**

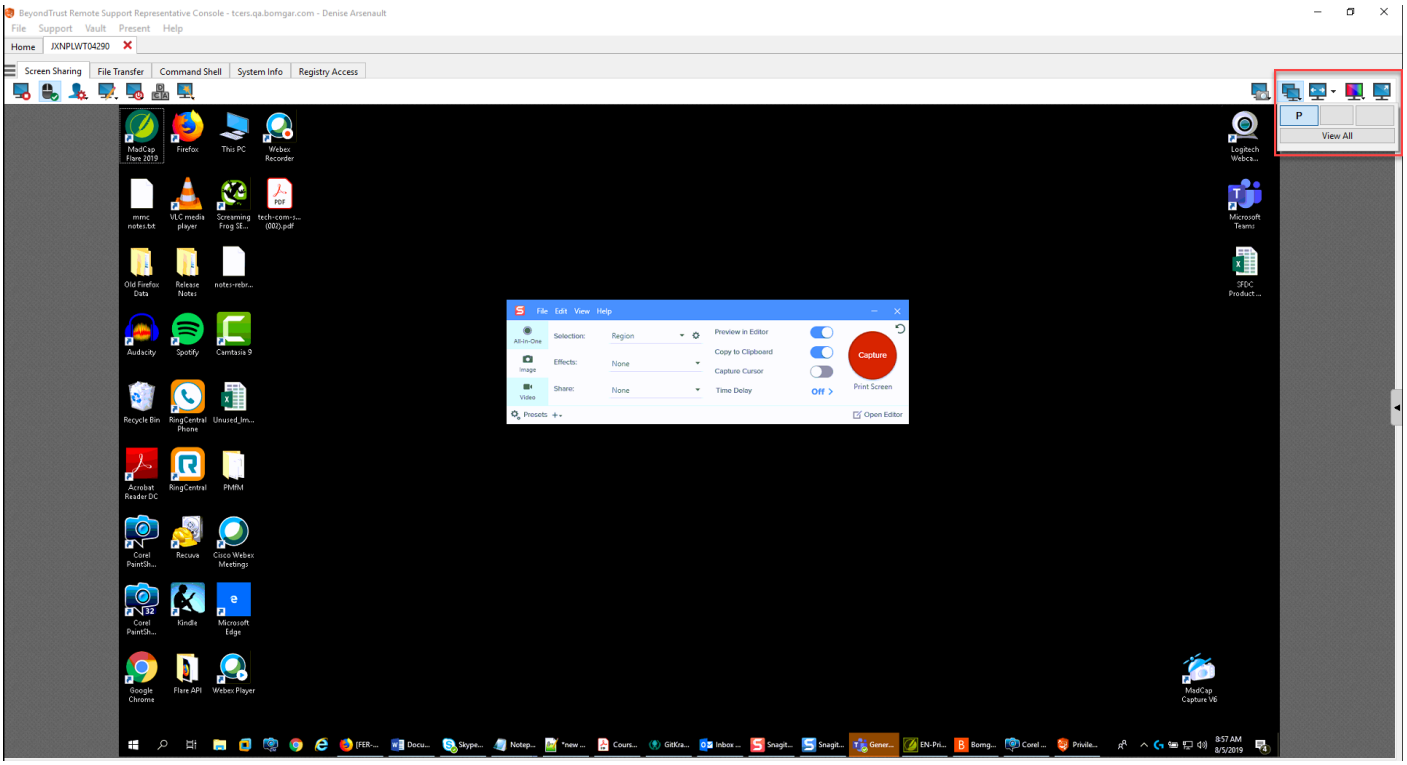
Alle Anmerkungen werden vom Kundenbildschirm gelöscht, wenn die Sitzung beendet ist.



Anmerkungen können auch während Präsentationen verfügbar sein. Weitere Informationen finden Sie unter „Eine Präsentation für Remote-Teilnehmer abhalten“ auf Seite 100.

Anzeige mehrerer Monitore am Remote-System

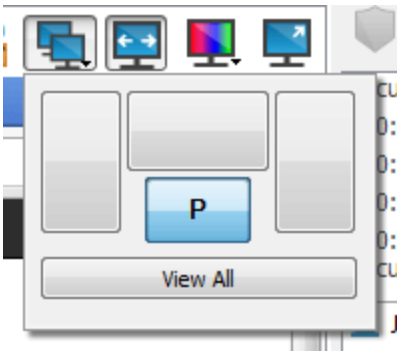
BeyondTrust unterstützt Remote-Desktops, die so konfiguriert sind, dass mehrere Monitore verwendet werden können. Wenn Sie sich mit einem Remote-Desktop verbinden, sehen Sie den Primär-Monitor in der Registerkarte **Bildschirmfreigabe**. Wenn zusätzliche Monitore konfiguriert werden, wird das Symbol **Monitor** in der Symbolleiste **Bildschirmfreigabe** aktiviert und eine Registerkarte **Monitore** erscheint in der unteren rechten Ecke der Konsole.



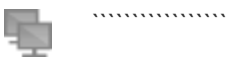
Das Monitor-Symbol verwenden

Klicken Sie das **Monitor**-Symbol an, um alle Monitore anzuzeigen, die mit dem Remote-Computer verbunden sind. In dieser Ansicht werden die Remote-Monitore durch Rechtecke anstatt Miniaturansichten dargestellt. Die Position jedes Rechtecks stimmt überein mit der Position eines jeden Monitors am Remote-Desktop.

Der Primär-Monitor erscheint standardmäßig im Fenster **Bildschirmfreigabe**. Um die Ansicht zu ändern, klicken Sie das Rechteck an, das den Monitor darstellt, den Sie anzeigen möchten. Sie können auch **Alle anzeigen** auswählen, um alle Monitore im Fenster **Bildschirmfreigabe** anzuzeigen, die mit dem Remote-Computer verbunden sind.

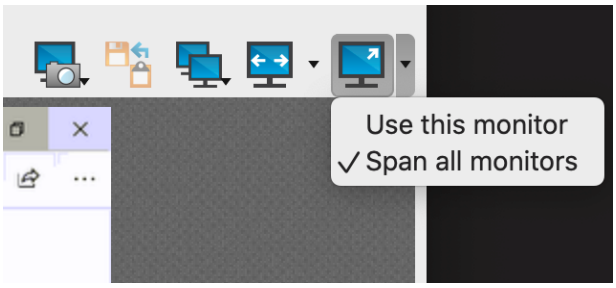


Wenn an den Remote-Computer keine weiteren Monitore angeschlossen sind, ist das Symbol **Monitor** nicht aktiv.



Multi-Monitor-Support für RDP-Sitzungen

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.

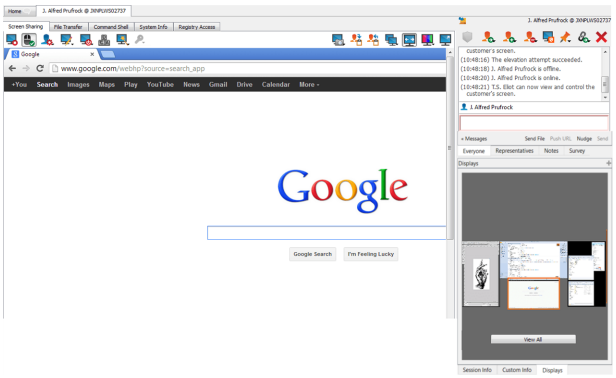


> ***Hinweis:*** *Wenn Sie während der Verwendung dieser Funktion die Vollbildschirm-Ansicht verwenden, wird das Remote-System auf allen Ihren Monitoren angezeigt.*

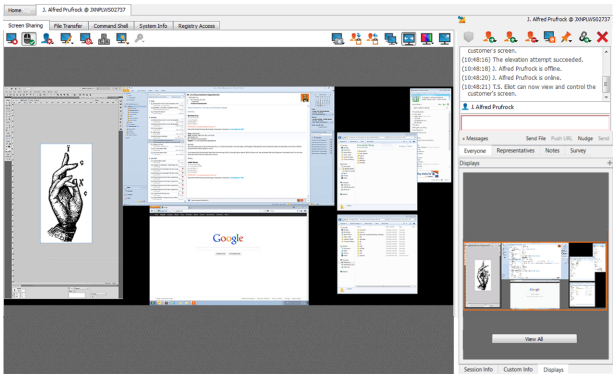
Die Registerkarte „Monitore“ verwenden

Klicken Sie auf die Registerkarte **Monitore**, um die Miniaturansichten all jener Monitore anzuzeigen, die mit dem Remote-Computer verbunden sind. Die Position jeder Miniaturansicht stimmt überein mit der Position eines jeden Monitors am Remote-Desktop.

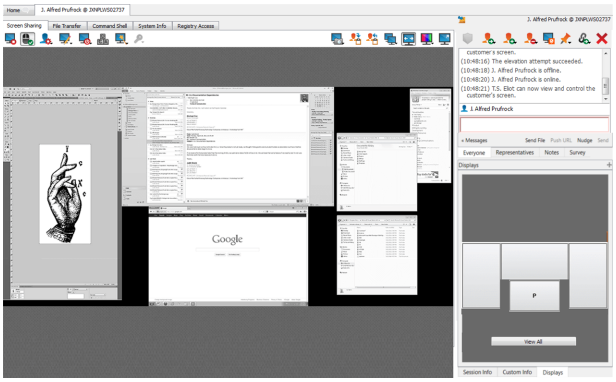
Der Monitor, der zurzeit auf der Registerkarte **Bildschirmfreigabe** angezeigt wird, ist hervorgehoben.



Der Primär-Monitor erscheint standardmäßig im Fenster **Bildschirmfreigabe**. Um die Ansicht zu ändern, klicken Sie die Miniaturansicht des Monitors an, den Sie anzeigen möchten. Sie können auch **Alle anzeigen** auswählen, um alle Monitore im Fenster **Bildschirmfreigabe** anzuzeigen, die mit dem Remote-Computer verbunden sind.



Wenn die Sitzung im Graustufenmodus stattfindet, werden die Remote-Monitore durch Rechtecke anstatt Miniaturansichten dargestellt. Die Position jedes Rechtecks stimmt überein mit der Position eines jeden Monitors am Remote-Desktop.



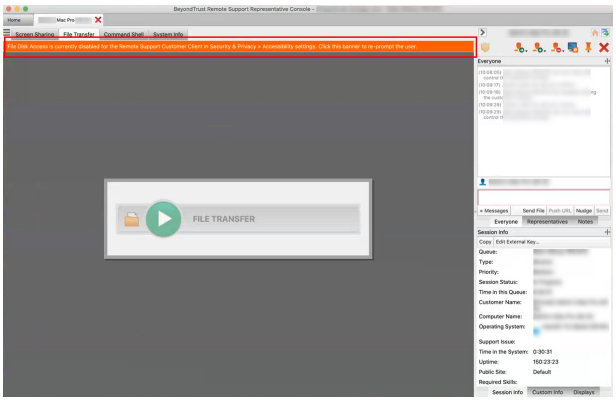
Hinweis: *Der Aktualisierungszyklus der Miniaturansicht dauert unter idealen Umständen ca. drei Sekunden, kann aber, je nach Internetgeschwindigkeit und Datentransfer, länger dauern.*

Dateitransfer zum und vom Remote-System

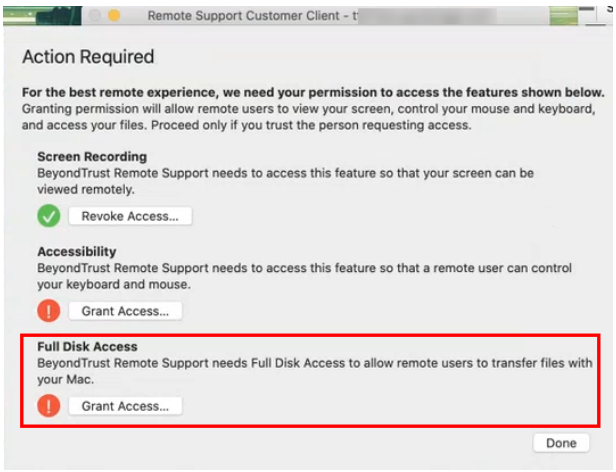
Berechtigte Benutzer können während einer Sitzung Dateien und sogar ganze Verzeichnisse sowohl auf den Remote-Computer als auch vom Remote-Computer oder von dem Remote-Gerät auf die SD-Karte oder umgekehrt übertragen, löschen oder umbenennen. Sie müssen nicht die vollständige Kontrolle über den Remote-Computer haben, um Dateien übertragen zu können.

Je nach den Berechtigungen, die Ihr Administrator für Ihr Konto festgelegt haben, 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 durchgesetzt wird, dass Uploads oder Downloads nur in bestimmten Verzeichnissen erfolgen.

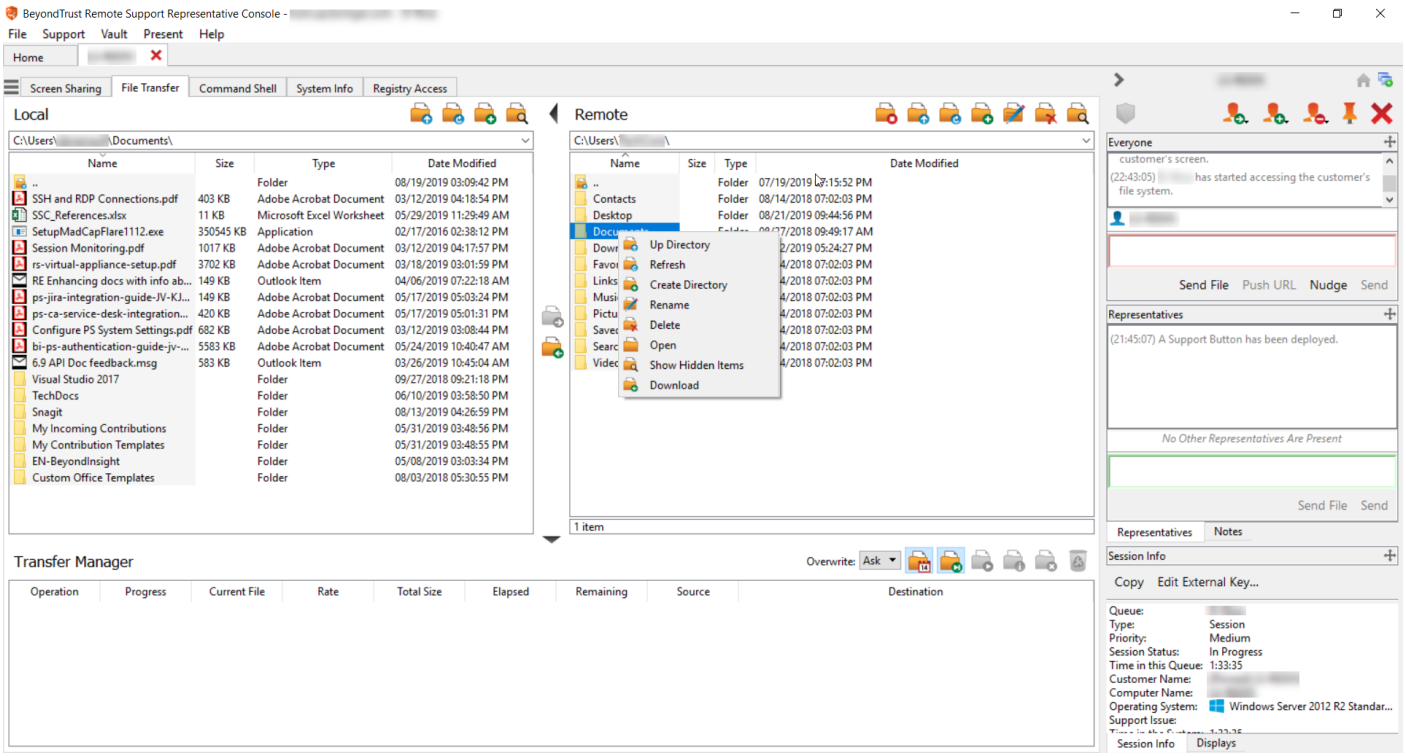
Ist die Bildschirmfreigabe in macOS Catalina (10.15) oder höher nicht aktiviert, klicken Sie auf das Banner über dem Reiter **Dateitransfer**, um den Kunden um die Berechtigung für den Transfer von Dateien zu bitten.



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.



Übertragen Sie Dateien mithilfe der Upload- oder Download-Schaltflächen oder durch Ziehen und Ablegen von Dateien. Mit einem Rechtsklick auf eine Datei wird ein kontextsensitives Menü aufgerufen, über das Sie unter anderem einen neuen Ordner erstellen, die Datei umbenennen, öffnen oder löschen oder direkt auf Ihr System herunterladen können.



Werkzeuge für den Dateitransfer

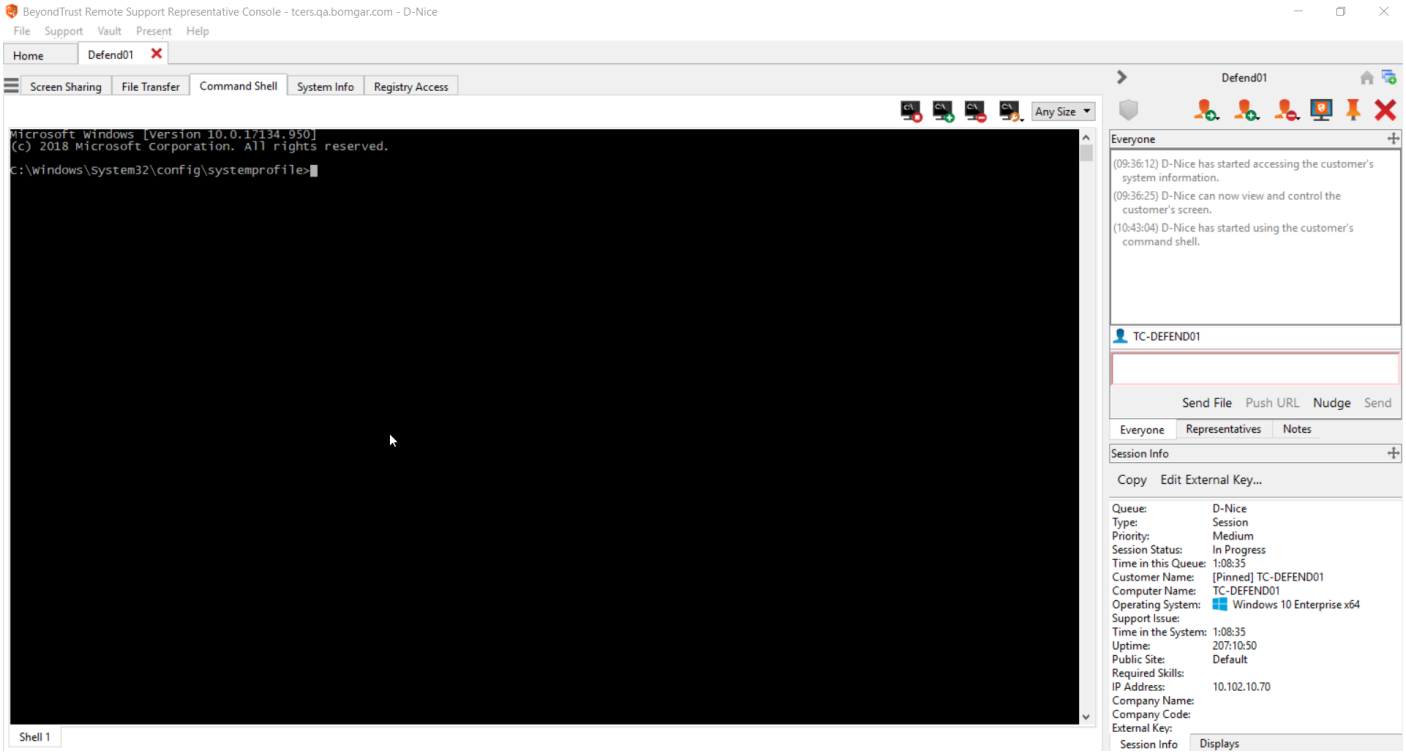
	Zugriff auf das Dateisystem des Remote-Geräts stoppen, wenn es nicht mehr benötigt wird.
	Ein Verzeichnis im ausgewählten Dateisystem nach oben wechseln.
	Ihre Ansicht des ausgewählten Dateisystems aktualisieren.
	Ein neues Verzeichnis erstellen.
	Ein Ordner oder eine Datei umbenennen.
	Ein Verzeichnis oder eine Datei löschen. Beachten Sie, dass dies die Datei oder den Ordner unwiderruflich löscht. Die Datei bzw. der Ordner wird nicht in den Papierkorb geworfen.
	Ausgeblendete Dateien anzeigen.
 	Wählen Sie eine oder mehrere Dateien oder Verzeichnisse und klicken Sie auf die jeweilige Schaltfläche, um die Dateien auf das Remote-System hochzuladen bzw. auf Ihr lokales System herunterzuladen. Sie können Dateien auch durch Ziehen übertragen.
	Ist bereits eine Datei des gleichen Namens am Speicherort, an den eine Datei übertragen werden soll, vorhanden, wählen Sie, ob die vorhandene Datei automatisch überschrieben, der Transfer abgebrochen oder für jede Datei mit identischem Namen eine Aufforderung angezeigt werden soll. Beachten Sie, dass bei identischem Inhalt der Dateien der Upload-Vorgang übersprungen und eine Warnmeldung angezeigt wird.
	Durch Beibehalten der Dateiinformationen wird auch der Originalzeitstempel der Datei beibehalten. Ist diese Option deaktiviert, gibt der Zeitstempel der Datei Datum und Uhrzeit der Übertragung wieder.
	Ist der automatische Dateitransfer aktiviert, beginnt die Übertragung, sobald auf die Schaltfläche zum Hoch- bzw. Herunterladen geklickt oder eine Datei aus einem Dateisystem in ein anderes gezogen wird.
	Ist der automatische Dateitransfer nicht aktiviert, wählen Sie im Transfermanager die Dateien aus, die Sie übertragen möchten, und klicken Sie auf **Start**, um mit dem Transfer zu beginnen.
	Wählen Sie im Transfermanager eine Datei aus und klicken Sie auf **Details**, um Informationen wie Datum und Uhrzeit des Transfers, Ursprung und Ziel der Dateien sowie die Anzahl der übertragenen Byte anzuzeigen.
	Wählen Sie eine oder mehrere Dateien im Transfermanager aus und klicken Sie auf **Abbrechen**, um den Transfer abzubrechen.
	Alle Informationen im Transfer-Manager löschen.

Zugriff auf die Remote-Befehlsshell

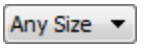
Mit der Remote-Befehlsshell kann ein berechtigter Benutzer eine virtuelle Befehlszeilenschnittstelle für den Remote-Computer öffnen. Der Benutzer kann dann Befehle lokal eingeben, aber auf dem Remote-Computer ausführen lassen. Sie können mit mehreren Shells arbeiten. Beachten Sie, dass die dem Benutzer zur Verfügung stehenden Skripte ebenfalls über die Bildschirmfreigabe-Schnittstelle auf dem Remote-Computer ausgeführt werden können.

Ihr Administrator kann auch die Remote-Shell-Aufzeichnung aktivieren, sodass ein Video jeder Shell später über den Sitzungsbericht angezeigt werden kann.

> ***Hinweis:*** *Die Lokalisierung ist für diese Funktion auf Zeichen der Größe von 1 Byte beschränkt. Die Verwendung von Zeichen der Größe von 2 Bytes (bestimmte Sprachpakete) können das Verhalten einiger Funktionen beeinflussen.*



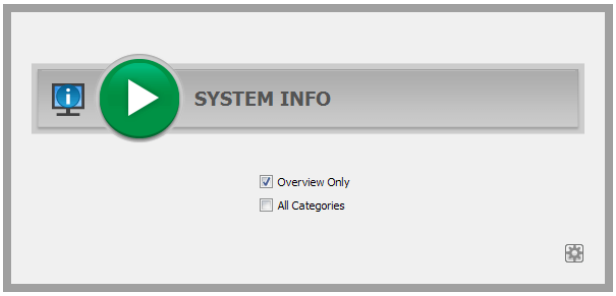
Befehlsshell-Tools

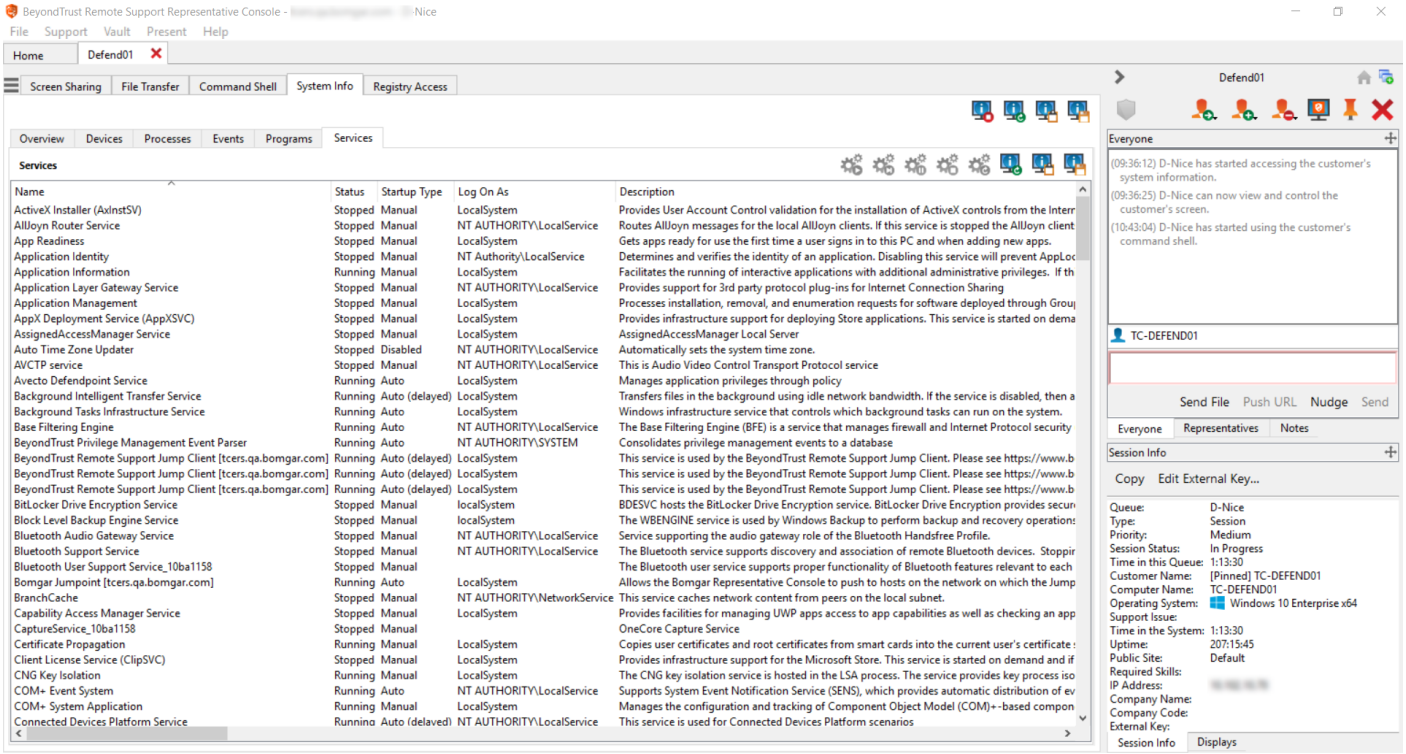
	Zugriff auf die Eingabeaufforderung stoppen, wenn er nicht mehr benötigt ist.
 	Öffnen Sie eine neue Shell, um mehrere Instanzen der Eingabeaufforderung auszuführen, oder schließen Sie einzelne Shells, ohne den Eingabeaufforderungs-Zugriff aufzugeben. Die einzelnen Instanzen werden als Registerkarten am unteren Bildschirmrand angezeigt.
	Greifen Sie auf eine Dropdown-Liste zuvor verfasster Skripts zu, falls dies zulässig ist. Wenn Sie ein Skript für die Ausführung auswählen, wird eine Eingabeaufforderung mit einer kurzen Beschreibung des Skripts angezeigt. Wenn Sie auf **Ja** klicken, wird das Skript in der aktiven Befehlsshell ausgeführt.
	Greifen Sie auf Tools für die Verwendung in der Befehlszeile zu. Fügen Sie den Inhalt Ihrer Zwischenablage ein, entweder über die Auswahl aus dem Menü oder durch Rechtsklick im Terminalfenster. Kopieren Sie ein Protokoll der aktuellen Shell in Ihre Zwischenablage oder speichern Sie es auf Ihrem Computer. Um einen Teil des Texts zu kopieren, wählen Sie ihn einfach aus. Löschen Sie jegliche aktuell nicht sichtbaren Zeilen oder löschen Sie alle Inhalte des Terminals. Sie können auch auf Tools zugreifen, indem Sie im Terminalfenster Strg gedrückt halten und rechtsklicken.
	Wählen Sie die Größe aus, in der die Anzeige erscheinen soll. Wählen Sie zwischen 80x50, 80x25 oder jeder beliebigen Größe.

Anzeige von Informationen zum Remote-System

Berechtigte 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. Benutzer mit den geeigneten Berechtigungen können ebenfalls Prozesse beenden, Dienste starten, stoppen, pausieren, fortsetzen und neu starten sowie Programme deinstallieren.

Weil der Abruf sehr großer Datenmengen zu langen Übertragungszeiten führen kann, können Sie sich entscheiden, Ihre Anzeige nur mit der Registerkarte **Übersicht** zu starten oder Daten für alle Registerkarten abzurufen. Wenn Sie mit **Nur Übersicht** beginnen, können Sie Daten von den anderen Registerkarten dadurch einholen, dass Sie zum jeweiligen Abschnitt wechseln, den Sie anzeigen müssen und oben in diesem Abschnitt auf **Aktualisieren** klicken.



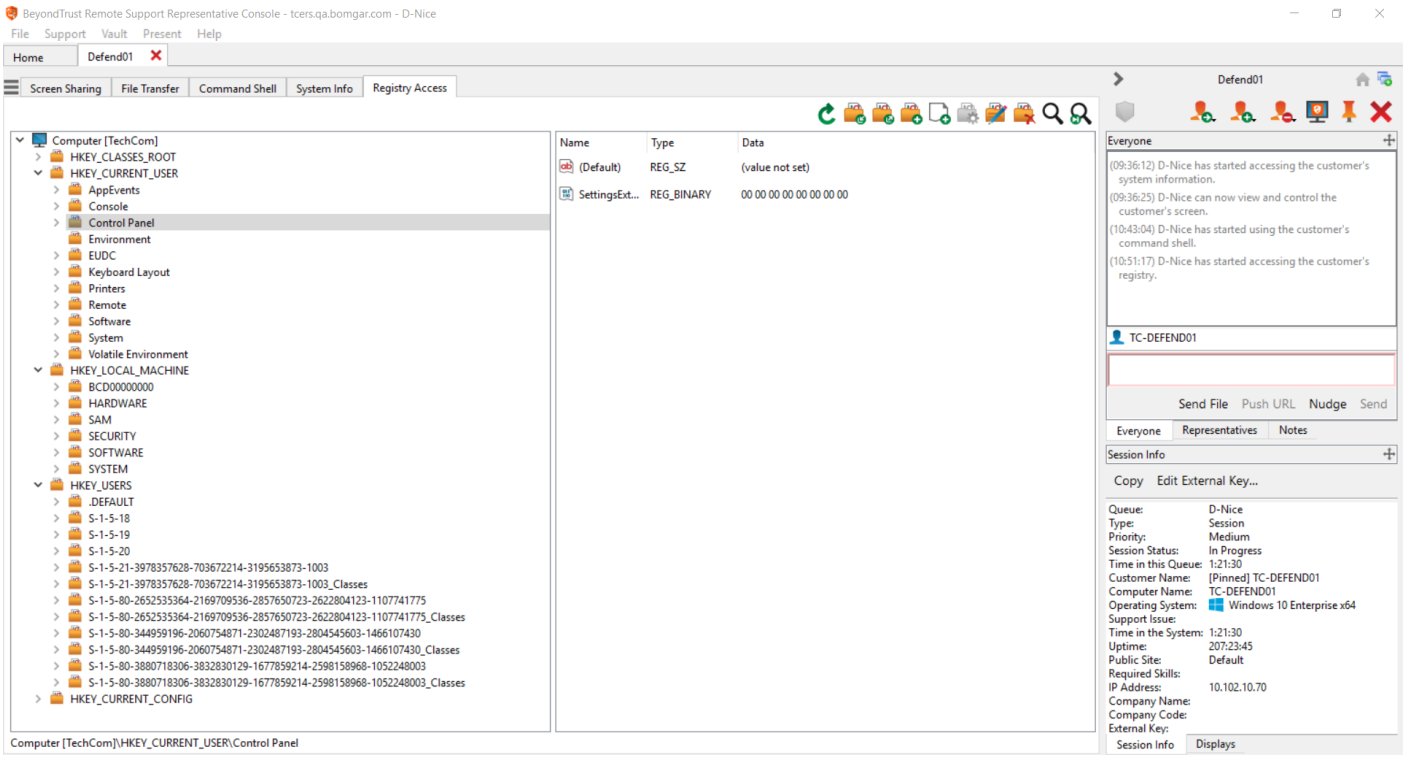


Werkzeuge für Systeminformationen

	Informationen über das Remote-System nicht länger abrufen. Beim Anhalten sind die zuletzt aktualisierten Informationen weiterhin zur Anzeige verfügbar, die aktuellen Daten werden jedoch nicht abgerufen.
	Ansicht der Systeminformationen aktualisieren oder Informationen für Registerkarten, auf die Sie anfänglich keinen Zugriff angefordert haben, abrufen. Die Aktualisierung ist für einzelne Bereiche oder alle Bereiche der ausgewählten Registerkarte möglich.
	Eine Kategorie von Systeminformationen automatisch aktualisieren.
	Informationen in die Zwischenablage kopieren. Kopieren Sie einzelne oder alle Bereiche der ausgewählten Registerkarte.
	Textdatei mit Systeminformationen auf Ihrem lokalen Computer speichern. Sie können einzelne oder alle Bereiche der ausgewählten Registerkarte speichern.
	Beendet einen laufenden Prozess auf dem Remote-System.
	Deinstalliert eine Anwendung auf dem Remote-System.
	Startet einen gestoppten Dienst auf dem Remote-System.
	Setzt einen pausierten Dienst auf dem Remote-System fort.
	Pausiert einen laufenden Dienst auf dem Remote-System.
	Stoppt einen laufenden Dienst auf dem Remote-System.
	Startet einen laufenden Dienst auf dem Remote-System neu.

Zugriff auf den Remote-Registrierungseditor

Greifen Sie auf eine Remote-Windows-Registrierung zu, ohne dass dabei eine Bildschirmfreigabe notwendig ist. Im virtuellen Registrierungseditor können Sie neue Schlüssel hinzufügen, löschen, bearbeiten, suchen und importieren oder exportieren. Die Verwendung des virtuellen Registrierungseditors ohne Bildschirmfreigabe führt zu weniger kundenseitigen Unterbrechungen und ermöglicht die schnellere Lösung von Problemen.



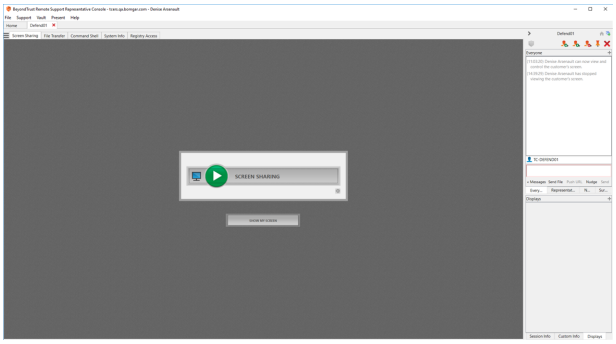
	Registrierung aktualisieren.
	Registrierungseinträge aus einer Datei importieren.
	Registrierungseinträge in eine Datei exportieren.
	Einen neuen Registrierungsschlüssel erstellen.
	Einen neuen Registrierungswert erstellen.
	Den ausgewählten Registrierungswert modifizieren.

	Den ausgewählten Registrierungseintrag umbenennen.
	Den ausgewählten Registrierungseintrag löschen.
	Die Registrierung durchsuchen.
	Nächste Fundstelle.

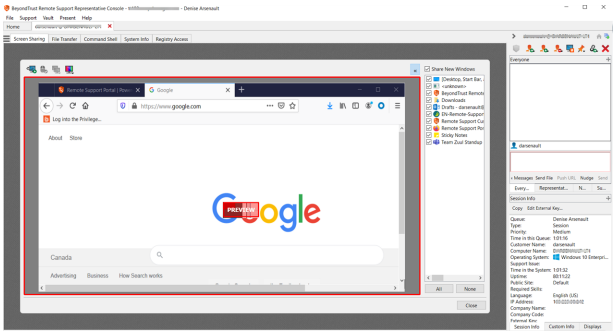
Dem Kunden meinen Bildschirm zeigen

Ein Support-Techniker mit entsprechenden Berechtigungen kann jederzeit seinen Bildschirm für einen Kunden freigeben und so die Effektivität von Support-Sitzungen Tech. oder Schulungsmaßnahmen steigern.

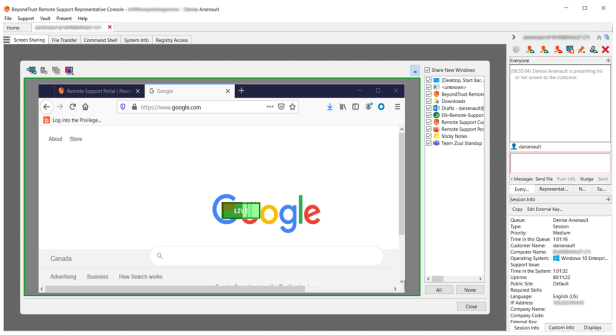
Für berechtigte Support-Techniker stehen die Optionen **Bildschirmfreigabe** und **Eigenen Bildschirm anzeigen** sofort zur Verfügung. Wenn Sie Ihren Bildschirm freigeben, müssen Sie dies wieder beenden, bevor Sie eine „Eigenen Bildschirm anzeigen“-Sitzung starten können.



Die Konsole d. Support-Technikers zeigt eine Vorschau davon an, wie Ihr Kunde den Bildschirm sehen wird, wenn Sie die Sitzung in den Live-Modus schalten. Wenn Sie Ihren Bildschirm während einer Support-Sitzung Tech. einem Kunden freigeben, kann Ihr Kunde entweder Ihren gesamten Desktop oder nur die Anwendungen sehen, die Sie anzeigen möchten. Außerdem können Sie wählen, neue Fenster automatisch freizugeben. Sie können den Anwendungsselektor anzeigen oder verbergen, indem Sie auf den Pfeil oben im Fenster **Eigenen Bildschirm anzeigen** klicken.



Klicken Sie auf das Symbol **Dem Kunden Ihren Bildschirm zeigen** oben links im Fenster, um Ihre „Eigenen Bildschirm anzeigen“-Sitzung im Live-Modus zu starten. Sie können während der gesamten Sitzung weiter mit Ihrem Kunden chatten.



> ***Hinweis:*** *Die „Eigenen Bildschirm anzeigen“-Aktivität wird zu Berichtszwecken aufgezeichnet, wenn dies unter* ***/login > Konfiguration > Optionen*** *konfiguriert wurde. Die Aufzeichnung steht Ihrem Kunde auf der Zielseite für das Sitzungsende nicht zur Verfügung.*

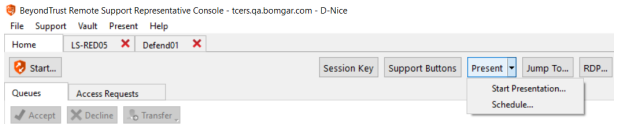
„Eigenen Bildschirm anzeigen“-Werkzeuge

 	Zeigen Sie den ganzen Bildschirm oder ausgewählte Anwendungen für den Remote-Benutzer an oder deaktivieren Sie die Anzeige Ihres Bildschirms.
	Bei der Anzeige Ihres Bildschirms können Sie dem Kunden den Zugriff auf Ihre Tastatur und Ihre Maus gewähren oder entziehen, genau wie bei der Schulung eines Kunden.  ***Hinweis:*** *Der Linux-Kunden-Client unterstützt nicht die Steuerung des Bildschirms des Support-Technikers.*
	Wählen Sie den Anzeigemonitor für Ihre „Eigenen Bildschirm anzeigen“-Sitzung. Der primäre Monitor wird mit einem **P** gekennzeichnet.

Eine Präsentation für Remote-Teilnehmer abhalten

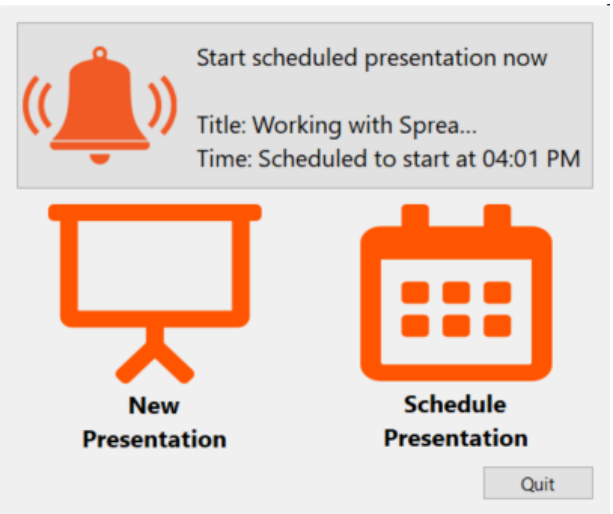
> ***Hinweis:*** *Die Präsentationsfunktion muss aktiviert sein, wenn Ihre Support-Website erstellt wird. Ist dies nicht der Fall, und Sie müssen Präsentationen durchführen, wenden Sie sich bitte an den Support oder Ihren Website-Administrator.*

Ein Support-Techniker mit Berechtigungen zum Abhalten von Präsentationen oder alternativ ein Support-Techniker, der nur über eine Berechtigung zum Abhalten von Präsentationen verfügt, kann seinen Bildschirm für einen oder mehrere Remote-Teilnehmer freigeben. Starten Sie eine Präsentation über:

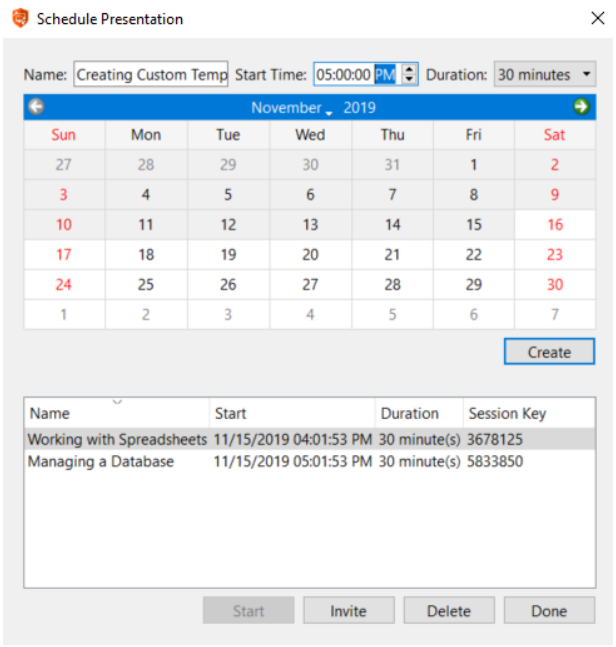


- Das Menü **Präsentation** der Konsole d. Support-Technikers
- Die Schnellstart-Schaltfläche **Präsentieren** oben in Ihrer Konsole d. Support-Technikers
- das Auswahlfenster der Nur-Präsentation-Schnittstelle (Support-Techniker ohne Berechtigung, Remote-Support zur Verfügung zu stellen)

Wenn Sie eine Präsentation sofort starten, indem Sie entweder auf die Schaltfläche **Präsentieren** klicken oder in der Konsole d. Support-Technikers die Option **Präsentation starten...** auswählen, wird die Präsentations-Schnittstelle von BeyondTrust geöffnet. Wenn Sie über Nur-Präsentations-Berechtigungen verfügen, können Sie eine Präsentation beginnen, indem Sie auf die Schaltfläche **Neue Präsentation** im Auswahlfenster der Nur-Präsentations-Schnittstelle klicken.



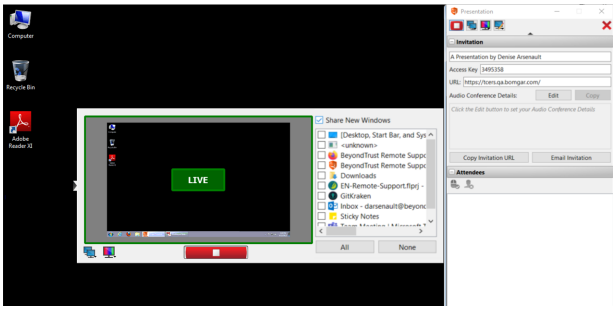
Sie können eine Präsentation auch für ein späteres Datum einplanen. Sie werden von einem Planer aufgefordert, einen Namen für Ihre Präsentation, eine Startzeit und ein Startdatum sowie die erwartete Dauer der Veranstaltung einzugeben. Wenn Sie diese Informationen eingegeben haben, klicken Sie auf **Erstellen**. Ihre Präsentation wird nun in einer Liste anstehender Präsentationen aufgeführt. Die Präsentationszeiten können sich nicht überlappen. Falls Sie eine Präsentation vor der geplanten Zeit löschen, werden alle gesendeten Einladungen ungültig und die Teilnehmer können keine Verbindung herstellen. Wenn Sie bereit sind, mit einer geplanten Präsentation zu beginnen, wählen Sie die Präsentation aus der Liste aus und klicken Sie auf **Start**, um die Präsentations-Schnittstelle zu öffnen.



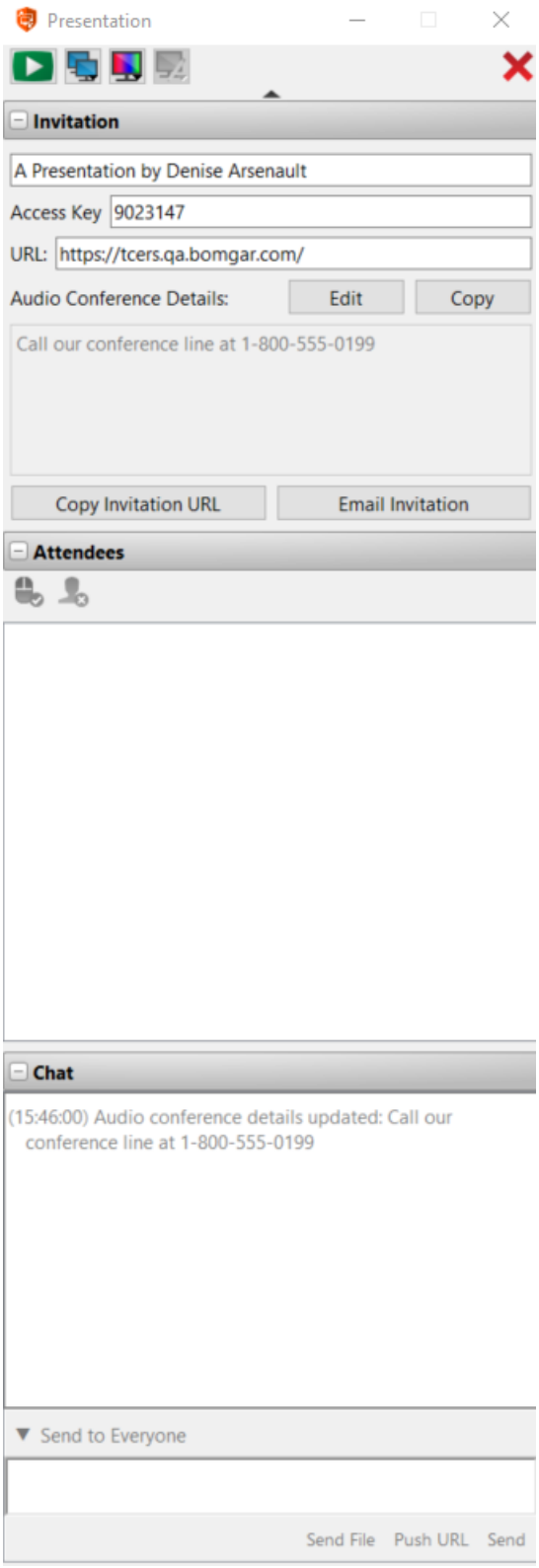
Über den Planer können Sie Teilnehmern eine E-Mail-Einladung senden, die eine eindeutige URL und jegliche Audiokonferenz-Details für Ihre Präsentation enthält. Sie können die Teilnehmer auch anweisen, Ihre öffentliche Website zu besuchen und den eindeutigen Sitzungsschlüssel einzugeben. Sie können über die Präsentations-Schnittstelle zudem eine E-Mail-Einladung senden.

Ist der Präsentationsstart in Kürze geplant, können Sie mit einer Schaltfläche oberhalb des Auswahlfensters der Nur-Präsentations-Schnittstelle die Präsentation direkt beginnen. Ebenfalls können Sie eine geplante Präsentation über das Planungsfenster starten.

Die Präsentations-Schnittstelle besteht aus einer unauffälligen vertikalen Seitenleiste mit drei einklappbaren Bereichen: **Einladung**, **Teilnehmer** und **Chat**. Ein horizontales Slide-Seitenfenster enthält ein Vorschaufenster, das einen Statusindikator anzeigt, der sich ändert, wenn Sie auf die Start-/Stopp-Schaltfläche klicken, um anzuzeigen, dass Sie eine Live-Präsentation abhalten. Ein Anwendungsselektor, ein Display-Selektor und ein Auflösungs-Selektor (unten beschrieben) stehen ebenfalls zur Verfügung.



Im Abschnitt **Einladung** können Sie, falls gewünscht, einen Namen für Ihre Präsentation angeben, oder aber den Standardeintrag verwenden, der den Namen des Support-Technikers enthält. Die aktivierten Felder für den **Zugriffsschlüssel** und die **URL** der Präsentation werden angezeigt, und Sie können auch die Audiokonferenz-Details eingeben und speichern, die über mehrere Präsentationen hinweg beibehalten und im Chat-Fenster protokolliert werden. Diese Informationen werden beim Verbindungsaufbau allen Teilnehmern zugesandt und jederzeit erneut veröffentlicht, wenn Sie die Informationen während einer Präsentation aktualisieren. Falls die Präsentationsliste auf Ihrer öffentlichen Website aktiviert ist, können Sie **Diese Präsentation auf der öffentlichen Liste anzeigen** auswählen, um einen Link anzuzeigen, über den Teilnehmer Ihrer Präsentation beitreten können. Mit bereitgestellten Schaltflächen ist es möglich, schnell und einfach die **Einladungs-URL zu kopieren** und die **Einladung als E-Mail zu senden**.



*Fehlt die Schaltfläche **Einladen** im Dialog für die Planung der Präsentation, vergewissern Sie sich, dass kundenseitige E-Mails in Ihrer Instanz konfiguriert und aktiviert worden sind. Weitere Informationen finden Sie in E-Mail-Konfiguration: Konfigurieren der Software für das Versenden von E-Mails unter https://www.beyondtrust.com/docs/remote-support/getting-started/admin/email-configuration.htm.*

Der Abschnitt **Teilnehmer** führt die Teilnehmer auf, die Ihrer Präsentation beigetreten sind. Falls zulässig, können Sie über eine Schaltfläche einem Teilnehmer die Steuerung Ihrer Maus und Tastatur gewähren. Sie können die Teilnehmer auch aus der Präsentation entfernen, indem Sie auf die Schaltfläche zur Entfernung von Teilnehmern klicken.

***Hinweis:** Wenn Ihr Teilnehmer die Steuerung Ihrer Maus und Ihrer Tastatur innehat, wird diesem Teilnehmer eine rote Leiste unterhalb des Teilnehmerfensters angezeigt. Wenn sich der Teilnehmer im Modus „Originalgröße“ oder „Vollbildschirm“ befindet, wird er diesen verlassen, wenn er die Steuerung von Ihnen übernimmt. Ein Teilnehmer mit einem mobilen Gerät kann nicht die Steuerung übernehmen.*

Der Abschnitt **Chat** in der Präsentations-Schnittstelle protokolliert Ihre Aktionen in der Schaltfläche sowie alle Nachrichten, die Sie an alle oder ausgewählte Teilnehmer senden. Ihre Teilnehmer können sich privat oder öffentlich mit Ihnen unterhalten.

Mit einem Klick auf den Pfeil über der Präsentations-Schnittstelle wird die Schnittstelle in den Minimodus minimiert, der nur die Bedienelemente der Präsentation enthält.

Bei der Vorschau der Präsentation oder während dem Abhalten der Präsentation können Sie das Fenster Vorschau/Live öffnen oder schließen, indem Sie auf den Schalter links daneben klicken. In diesem Fenster können Sie wählen, welche Anwendungen Sie freigeben wollen. Sie können festlegen, ob neue Fenster automatisch präsentiert werden sollen oder nicht.Wenn Sie mehr als einen Bildschirm für Ihren Computer verwenden, klicken Sie auf das Monitorsymbol, um festzulegen, welcher Monitor in der Präsentation verwendet werden soll. Der primäre Monitor wird mit einem **P** gekennzeichnet. Ebenfalls können Sie auch alle Bildschirme präsentieren.

Sie können auch die Farbtiefe der Präsentation auswählen - **niedrige Bandbreite**, **beste Leistung**, **Leistung und Qualität**, oder **beste Qualität**.

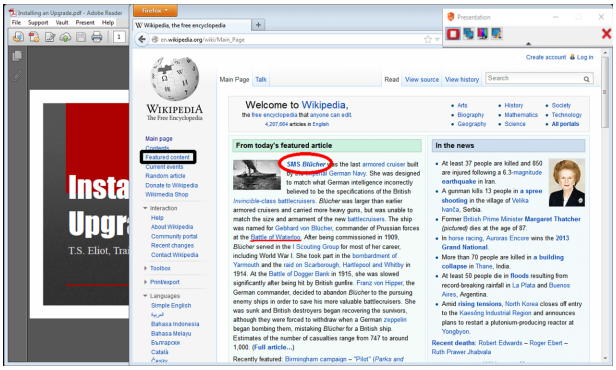
Die Schaltflächen „Start“, „Stopp“, Monitore und Farbtiefe sind auch dann verfügbar, wenn das Fenster „Vorschau“ oder „Live“ nicht geöffnet ist, und unabhängig davon, ob Sie die Präsentations-Schnittstelle von BeyondTrust minimiert haben (Minimodus). Die Anmerkungsschaltfläche ist ebenfalls während der Präsentation verfügbar.

Präsentationswerkzeuge

	Präsentation beginnen. Eine Live-Präsentation wird in der Präsentations-Schnittstelle durch einen durchscheinenden grünen **LIVE**-Indikator gekennzeichnet.
	Präsentation anhalten. Auf der Präsentations-Schnittstelle wird ein durchscheinender roter **VORSCHAU**-Indikator angezeigt.
	Wählen Sie den Monitor für Ihre Präsentationssitzung. Der primäre Monitor wird mit einem **P** gekennzeichnet.
	Zeigen Sie den Bildschirm in einer 2-Bit-Grauskala an, um möglichst wenig Bandbreite aufzuwenden, in 8-Bit-Farbe für schnelle Leistung, 16 Bit für eine mittlere Bildqualität und Leistung oder 32 Bit für die höchste Bildauflösung.
	Anmerkungen in Ihrer Live-Präsentation verwenden.
	Falls zulässig, einem Teilnehmer die Steuerung Ihrer Maus und Tastatur gewähren. Es kann nur jeweils ein Teilnehmer gleichzeitig die Steuerung über Ihren Computer übernehmen. Sie können dies stets übersteuern und die Steuerung durch den Teilnehmer jederzeit abbrechen. Ein Teilnehmer mit einem mobilen Gerät kann nicht die Steuerung übernehmen. Sie können eine Präsentation nicht an einen anderen Moderator übertragen.
	Teilnehmer aus Präsentation entfernen, ohne diese zu beenden.
	Präsentation ganz beenden und Präsentations-Schnittstelle schließen.

Anmerkungen

Wenn Sie Berechtigung zur Verwendung von Anmerkungen haben, ist dieses Werkzeug auch während Präsentationen verfügbar, sodass Sie Bereiche im Bildschirm hervorheben und die Aufmerksamkeit auf bestimmte Bereiche und Objekte lenken können.



Sobald Sie mit dem Verwenden von Anmerkungen begonnen haben, rechtsklicken Sie an eine beliebige Stelle auf Ihrer Präsentation, um aus den Anmerkungswerkzeugen auszuwählen. Um **Anmerkungen** auszuschalten, wählen Sie **Kein Werkzeug** im Dropdown-Menü, oder klicken Sie auf **Esc.**

Zu den verfügbaren Werkzeugen gehören freies Zeichnen, Rechteck- und Kreisformen, Radieren, Rückgängig machen, Löschen, Farbe (rot/schwarz/weiß) und Linienstärke (dünn/mittel/dick).

Zusammenarbeit

Chatten mit anderen Support-Technikern

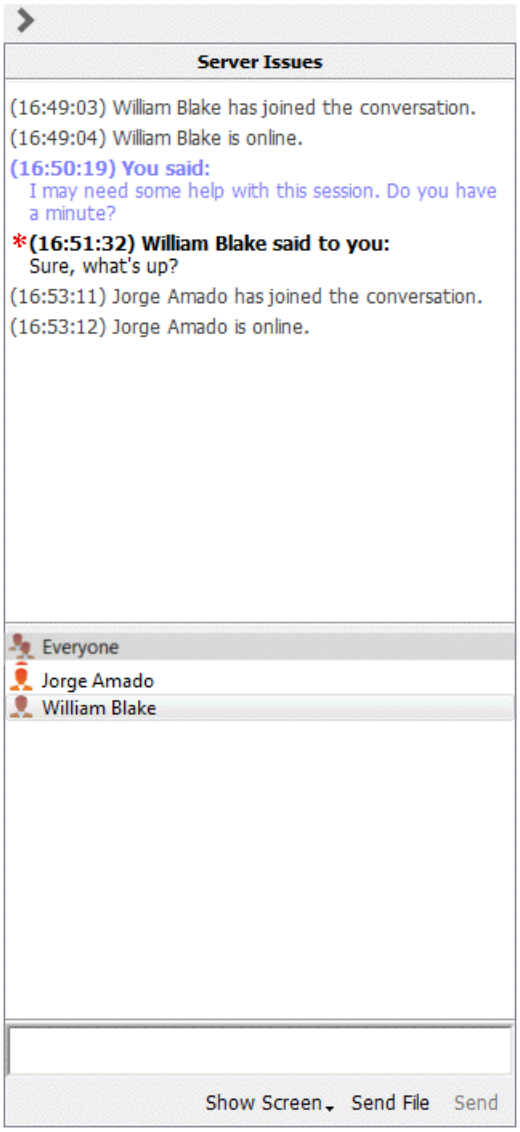
Über die Registerkarte **Startseite** der Konsole können Sie mit anderen angemeldeten Benutzern chatten. Sind Sie Mitglied eines oder mehrerer Teams, wählen Sie das Team, mit dem Sie chatten möchten, aus der Liste der Warteschlangen links neben der Registerkarte **Startseite**. Sie können mit allen Mitgliedern dieses Teams chatten oder nur mit dem gewünschten.

Wenn Sie zu Ihrer persönlichen Warteschlange zurückkehren oder **Alle Warteschlangen** wählen, verbleiben Sie für die gerade verlassene Warteschlange im Chat.

Klicken Sie auf das Pfeilsymbol oben links in der Seitenleiste, um die Schiebe-Seitenleiste einzuklappen. Ist die Schiebe-Seitenleiste eingeklappt, fahren Sie über den Pfeil neben dem verborgenen Fenster, um es anzuzeigen. Klicken Sie auf das Fixierungssymbol, das das Pfeilsymbol oben links in der Seitenleiste ersetzt hat, um die Schiebe-Seitenleiste erneut zu fixieren.

Wenn Sie Englisch schreiben, werden Rechtschreibfehler rot unterstrichen. Rechtsklicken Sie zur Anzeige von Rechtschreibungsvorschlägen, oder um diese Schreibweise für die aktuelle Konsolensitzung zu ignorieren.

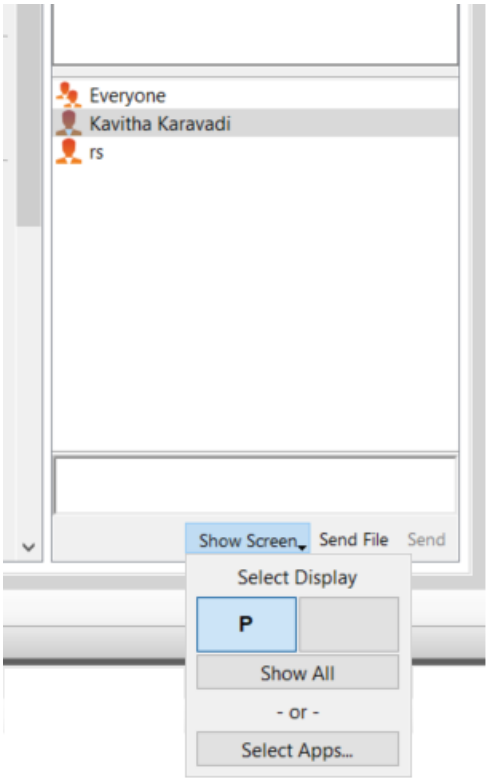
In den Einstellungen können Sie wählen, ob der Team-Chat Statusnachrichten wie die An- und Abmeldung von Benutzern enthalten soll oder nur zwischen Teammitgliedern gesendete Chatnachrichten.



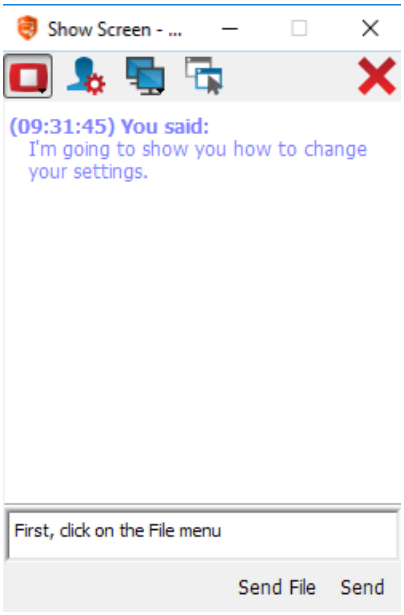
Bildschirm für anderen Support-Techniker freigeben

Wenn Ihr Administrator diese Berechtigung aktiviert hat, können Sie Ihren Bildschirm für einen anderen Benutzer freigeben, ohne dass der andere Benutzer einer Sitzung beitreten muss. Diese Option ist auch dann verfügbar, wenn Sie sich nicht in einer Sitzung befinden.

Wählen Sie aus einer Team-Warteschlange einen Benutzer und klicken Sie auf **Bildschirm anzeigen**. Wenn Sie mit mehr als einem Monitor arbeiten, können Sie auswählen, welchen Sie freigeben möchten oder welche Anwendungen für den anderen Benutzer sichtbar sein sollen. Sobald Sie Ihre Auswahl getroffen haben, erhält der andere Benutzer eine Benachrichtigung mit der Option, die Einladung anzunehmen oder abzulehnen.



Das Fenster **Bildschirm anzeigen** erscheint und zeigt den Namen des Benutzer an, der sich nun Ihren Bildschirm ansieht. Dieses Fenster enthält ein Chat-Kästchen und die Optionen, die Bildschirmfreigabe zu stoppen, dem empfangenden Benutzer die Steuerung zu überlassen und die Auswahl, welcher Monitor und welche Anwendungen freigegeben werden sollen. Sie können Ihre Bildschirmfreigabe stoppen, das Fenster aber offen lassen, oder die Freigabesitzung vollständig schließen. Wenn Sie das Fenster **Bildschirm anzeigen** offen lassen, können Sie die Bildschirmfreigabe wieder fortsetzen.



„Eigenen Bildschirm freigeben“-Werkzeuge

Freigebender Benutzer

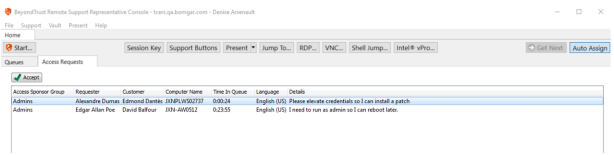
	Unterbricht vorübergehend die Freigabe Ihres Bildschirm für einen anderen Benutzer. Damit wird die Bildschirmfreigabe pausiert, das Fenster **Bildschirm anzeigen** aber nicht geschlossen, wodurch Sie die Bildschirmfreigabe wieder fortsetzen können.
	Bildschirmfreigabe (neu) starten.
	Überlässt dem Benutzer, der Ihren Bildschirm ansieht, die Steuerung von Maus und Tastatur.
	Wählen Sie den Monitor, der für den anderen Benutzer freigegeben werden soll. Der primäre Monitor wird mit einem **P** gekennzeichnet.
	Wählen Sie, welche Anwendungen für den anderen Benutzer freigegeben werden sollen.
	Bildschirmfreigabesitzung schließen. Damit wird die Oberfläche für die Bildschirmfreigabe mit einem anderen Benutzer geschlossen.

Anzeigender Benutzer

	Der Benutzer, der seinen Bildschirm für Sie freigibt, hat Ihnen die Steuerung von Tastatur und Maus überlassen.
	Schalten Sie einen virtuellen Cursor ein, der auf dem Bildschirm des freigebenden Benutzers sichtbar wird.
	Während der Bildschirmfreigabe können Sie eine Bildschirmaufnahme des Bildschirms des freigebenden Benutzers mit voller Auflösung aufnehmen.
	Den Remote-Bildschirm in der tatsächlichen Größe oder skaliert anzeigen.
	Zeigen Sie den Remote-Desktop im Vollbildmodus an oder kehren Sie zur Schnittstellenansicht zurück.
	Bildschirmfreigabesitzung schließen. Damit wird die Oberfläche für die Bildschirmfreigabe mit einem anderen Benutzer geschlossen.

Eine Zugriffsanforderung zum Anbieten von Heraufsetzungshilfe annehmen

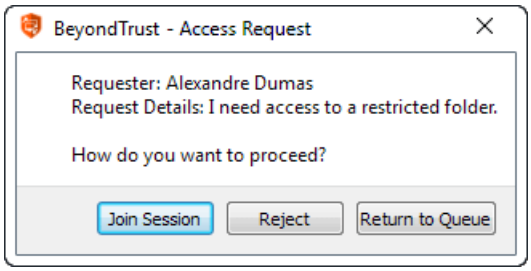
Ein Support-Techniker mit beschränkten Berechtigungen kann anhand von vordefinierten Zugriffssponsorengruppen einen Support-Techniker mit mehr Berechtigungen auffordern, bestimmte Aktionen in seinem Namen durchzuführen, z. B. einen Kunden-Client auf Administratorrechte heraufzusetzen oder Anmeldedaten für ein Remote-System einzugeben.



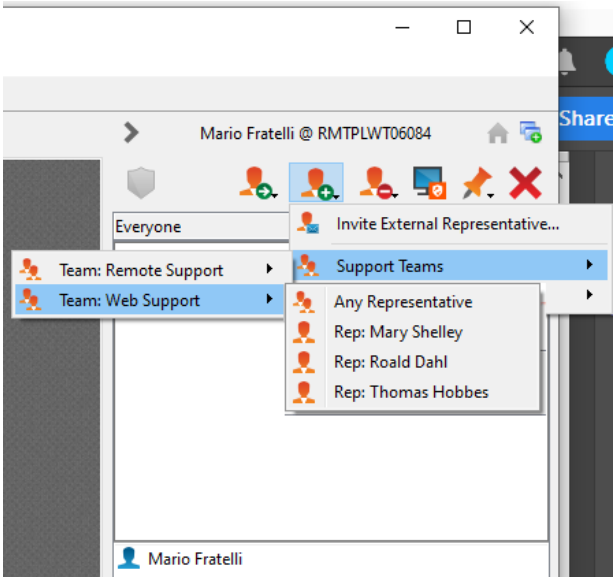
Ist ein Support-Techniker ein Sponsor in einer oder mehreren Zugriffssponsorengruppen, sieht er die Registerkarte **Zugriffsanforderungen** in der Konsole d. Support-Technikers.

Erstellt ein Support-Techniker eine Anforderung, sehen alle Sponsoren in der ausgewählten Zugriffssponsorengruppe eine neue Anforderung in der Registerkarte **Zugriffsanforderungen** der Konsole d. Support-Technikers.

Akzeptiert ein Sponsor die Anforderung, wird er aufgefordert, der Sitzung beizutreten, die Anforderung abzulehnen und einen Grund für die Ablehnung einzugeben oder die Anforderung wieder an die Warteschlange zu senden.



Freigabe einer Sitzung für andere Support-Techniker



Sie können einen Benutzer dazu einladen, einer Sitzung beizutreten, indem Sie in den Sitzungswerkzeugen auf die Schaltfläche **Freigeben** klicken. Standardmäßig werden nur Teams aufgelistet, denen Sie angehören.

Es gibt mehrere Wege, um einen Support-Techniker zur Teilnahme an einer Sitzung einzuladen. 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.

Sie können aus den angezeigten Teams einen Benutzer auswählen, um ihn oder sie zur Teilnahme an der Sitzung einzuladen.

Wenn Sie **Jeder Support-Techniker** wählen, wird die Einladung an die Teamwarteschlange gesandt, sodass jeder einzelne Support-Techniker im ausgewählten Team an der Sitzung teilnehmen kann. Sie können mehrere Einladungen versenden, wenn mehr Support-Techniker aus dem Team Ihrer Sitzung beitreten sollen.

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 Sie eine Einladung verschickt haben und diese noch aktiv ist, können Sie die Einladung zurückziehen, indem Sie sie im Menü **Einladung zurückziehen** auswählen. Einladungen können nur vom Sitzungseigentümer verschickt werden. Solange Sie Sitzungseigentümer bleiben, laufen Einladungen nicht ab. Für ein und denselben Benutzer können nicht mehrere aktive Einladungen für dieselbe Sitzung bestehen.

Eine Einladung wird dann inaktiv, wenn:

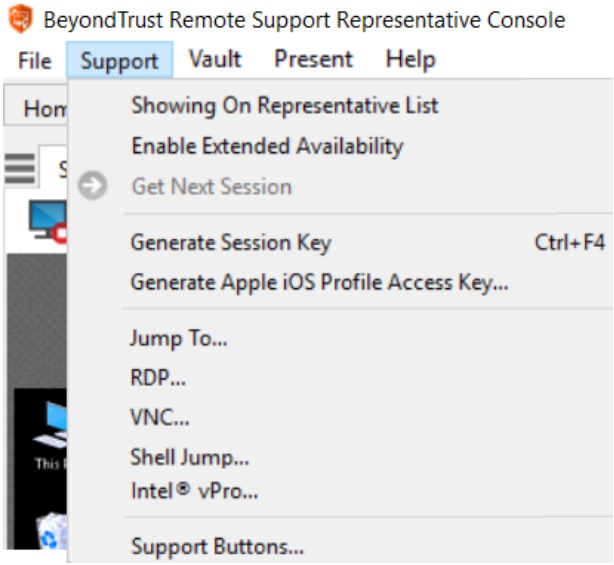
- Der einladende Benutzer zieht die Einladung zurück
- Der einladende Benutzer gibt das Eigentum der Sitzung ab bzw. weiter
- Die Sitzung endet
- Der eingeladene Benutzer nimmt die Einladung an
- Der eingeladene Benutzer lehnt die Einladung ab

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

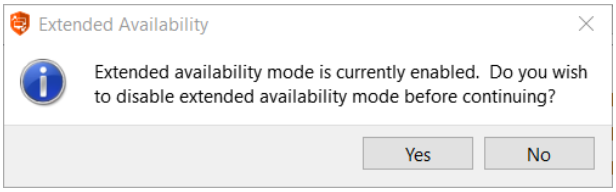
Verwenden der erweiterten Verfügbarkeit, um auch nach der Abmeldung einen Zugriff zu ermöglichen

Mit erweiterter Verfügbarkeit können berechtigte Benutzer E-Mail-Einladungen erhalten, um Sitzungen freizugeben, selbst wenn sie nicht in der Konsole angemeldet sind. Wenn Sie eine Einladung versenden, können Sie Teamkollegen einladen. Falls Sie dazu berechtigt sind, können Sie auch Benutzer aus Teams einladen, denen Sie nicht angehören. Durch die Möglichkeit, Sitzungen für Support-Techniker außerhalb Ihres Teams freizugeben und Sitzungseinladungen zu erhalten, wenn Sie sich von der Konsole des Support-Technikers abgemeldet haben, wird Ihre Verfügbarkeit als Support-Techniker erweitert.

Wenn Ihr Konto für eine erweiterte Verfügbarkeit konfiguriert ist, können Sie die Funktionalität im **Support**-Menü der Konsole d. Support-Technikers aktivieren bzw. deaktivieren.



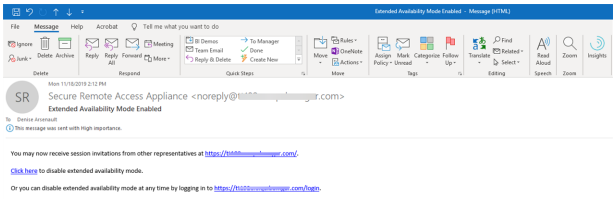
Wenn die erweiterte Verfügbarkeit aktiviert ist, wird eine Benachrichtigung angezeigt, wenn Sie sich in der Konsole anmelden. In diesem Dialogfeld können Sie die erweiterte Verfügbarkeit leicht deaktivieren, um Ablenkung zu vermeiden, wenn Sie sich beispielsweise gerade in einer Sitzung befinden.



Hinweis: *Wenn Sie die erweiterte Verfügbarkeit aktiviert lassen, wird ein Lizenz-Slot für Sie reserviert, bis die erweiterte Verfügbarkeit wieder deaktiviert wird. Damit wird sichergestellt, dass Ihnen im Falle einer Sitzungs-Einladung nicht aufgrund von Lizenznutzungsbeschränkungen die Anmeldung verweigert wird*

E-Mail-Benachrichtigung und -Einladung

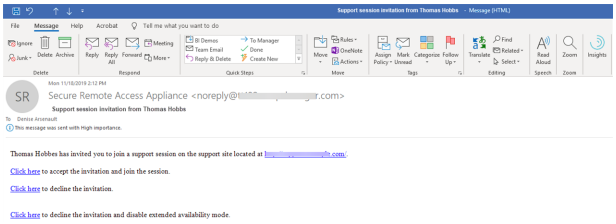
Immer wenn Sie den erweiterten Verfügbarkeitsmodus aktivieren, werden Sie vom Gerät über die in Ihrem Benutzerkonto hinterlegte E-Mail-Adresse in der angegebenen Sprache (falls verfügbar) darüber benachrichtigt.



> ***Hinweis:***
> *BeyondTrust ruft keine E-Mail-Adressen aus externen LDAP-Verzeichnisspeichern ab. Die E-Mail-Adresse muss in BeyondTrust auf eine von zwei Arten konfiguriert werden:*
>
> 1. *Ein Administrator kann eine E-Mail-Adresse einem Benutzerkonto hinzufügen, indem er zu **/login > Benutzer und Sicherheit > Benutzer** navigiert und das Konto bearbeitet.*
> 2. *Der Benutzer kann seine eigene E-Mail-Adresse festlegen, indem er zur Seite **/login > Mein Konto** navigiert.*

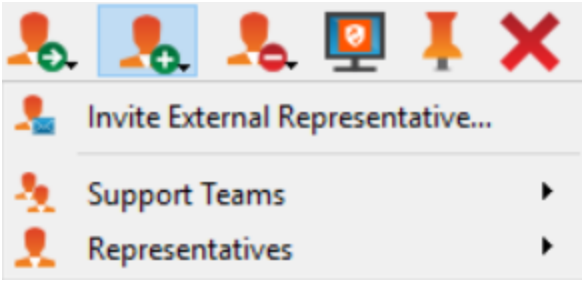
Die Benachrichtigung enthält die URL der Website sowie einen Link zur raschen Deaktivierung des erweiterten Verfügbarkeitsmodus.

Das Gerät verschickt darüber hinaus E-Mail-Benachrichtigungen, wenn Sie zu einer Sitzung eingeladen werden. So können Sie einer Sitzung beitreten, selbst wenn Sie aktuell nicht an der Konsole angemeldet sind. Die E-Mail-Benachrichtigung enthält Links zum Akzeptieren und Ablehnen der Einladung, sowie zur Ablehnung der Einladung während der erweiterte Verfügbarkeitsmodus deaktiviert wird.



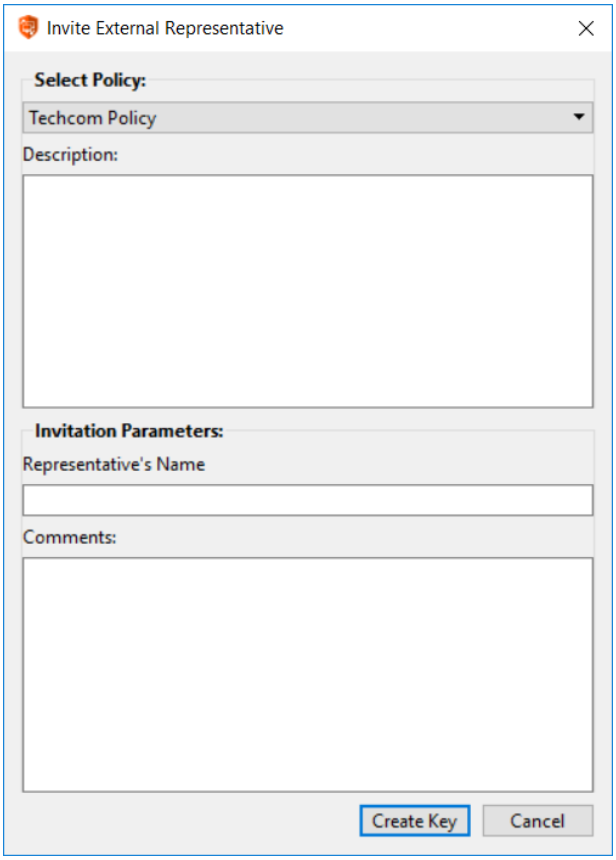
Einladen externer Support-Techniker zur Teilnahme an einer Sitzung

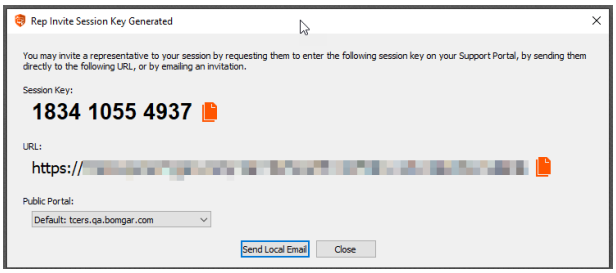
In einer Support-Sitzung Tech. kann ein Support-Techniker einen externen Support-Techniker auffordern, einmalig an einer Sitzung teilzunehmen. Der einladende Benutzer sollte auf die Schaltfläche **Sitzung freigeben** klicken und dann **Externen Support-Techniker einladen** wählen.



Der Benutzer wird in einem Dialogfeld aufgefordert, ein Sicherheitsprofil auszuwählen. Diese Profile werden in der Verwaltungsschnittstelle erstellt und bestimmen, welche Berechtigungen der externe Benutzer hat. Wenn Sie ein Profil auswählen, wird die vollständige Beschreibung darunter angezeigt.

Geben Sie den Namen des eingeladenen Benutzers ein. Dieser Name wird dem Kunden und in Berichten angezeigt. Geben Sie dann Kommentare dazu ein, warum dieser Benutzer eingeladen wurde. Klicken Sie auf **Schlüssel erstellen**. Es wird ein neues Dialogfeld mit dem Sitzungsschlüssel und der Direkt-URL angezeigt.





Klicken Sie auf die Schaltfläche **Senden**, um auszuwählen, wie der Sitzungsschlüssel an den externen Benutzer gesendet werden soll. Abhängig von den von Ihrem Administrator gewählten Optionen sind Sie möglicherweise in der Lage, die Einladung über Ihren lokalen E-Mail-Client oder serverseitig zu versenden. Sie können auch die direkte URL kopieren und einfügen und diese so dem externen Benutzer zukommen lassen. Der externe Benutzer muss das Installationsprogramm für die Konsole d. Support-Technikers herunterladen und ausführen. Dabei handelt es sich um einen abgekürzten Vorgang, im Gegensatz zur vollständigen Installation der Konsole d. Support-Technikers.

Der eingeladene Benutzer kann nur auf die Registerkarte der jeweiligen Sitzung zugreifen und weist einen beschränkten Berechtigungssatz auf. 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. Der Sitzungsschlüssel für den eingeladenen Benutzer ist zwei Stunden bzw. bis zum Ende der Sitzung gültig.

Sie können mehr als einen externen Benutzer zu einer Sitzung einladen. Achten Sie darauf, dass jeder externe Support-Techniker eine BeyondTrust-Lizenz zuordnet.

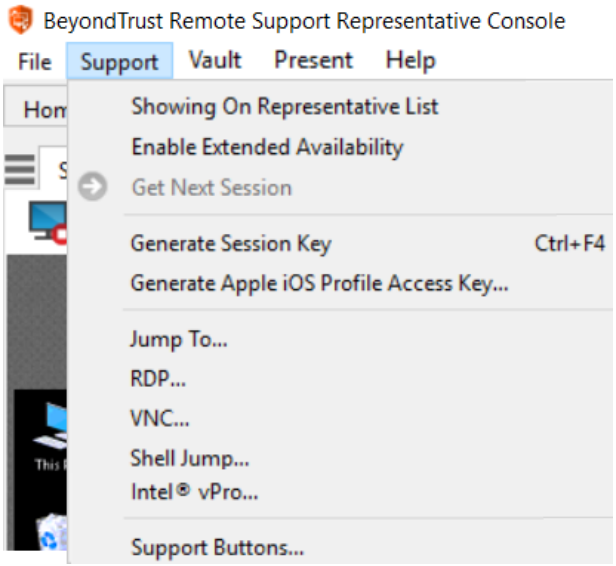
Verwaltung

Support Buttons verwalten

Support Buttons ermöglichen es Kunden, eine Support-Sitzung Tech. mit dem Ihnen zugewiesenen technischen Support-Team zu initiieren, einen Sitzungsschlüssel einzugeben oder ein Problem bei einer Support-Warteschlange einzureichen. Bereitgestellte Support Buttons können über die Support Button-Verwaltungsschnittstelle verwaltet werden. Beachten Sie, dass stapelweise bereitgestellte Support Buttons, die im systemweiten Modus installiert wurde, mithilfe von „Programme hinzufügen/entfernen“ bzw. Systemverwaltungstools entfernt werden muss.

Auf die Support Button-Verwaltungsschnittstelle können Sie wie folgt zugreifen:

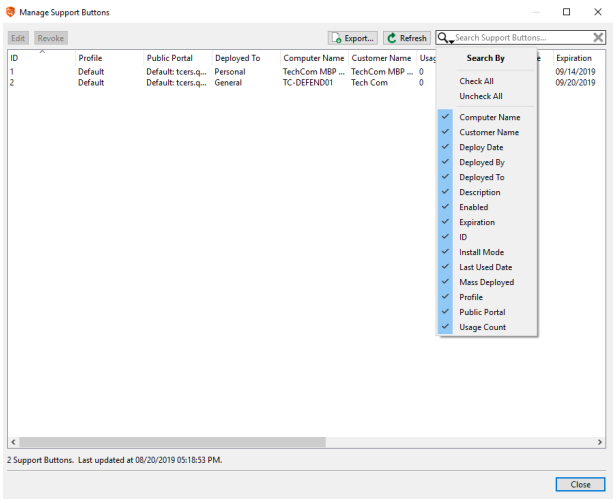
- Das **Support**-Menü der Konsole des Konsole d. Support-Technikers
- über die Schaltfläche **Support Buttons** oben in der Konsole d. Support-Technikers



Die Support Button-Verwaltungsschnittstelle zeigt eine Liste der bereitgestellten Support Buttons an, zusammen mit den Nutzungsstatistiken.

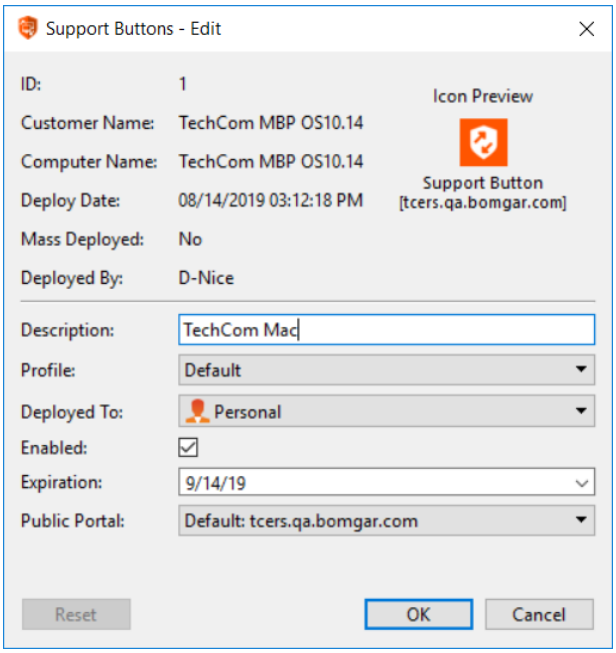
Administratoren sehen alle bereitgestellten Support Buttons, wohingegen berechtigte Benutzer die Schaltflächen sehen, die ihrer persönlichen Warteschlange und ihren Teamwarteschlangen zugeordnet sind.

Klicken Sie auf das Suchsymbol, um die zu durchsuchenden Felder auszuwählen. Geben Sie dann Text in das Eingabefeld ein und drücken Sie die Eingabetaste, um eine Suche durchzuführen. Zudem können Sie durch Klicken auf einen Spaltentitel die Datenreihen sortieren.



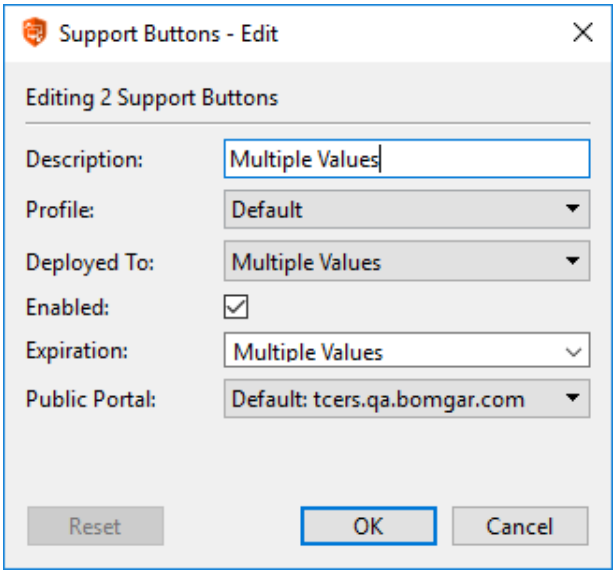
Die Support Button-Nutzungsstatistiken umfassen folgende Angaben:

- Statische Felder:
  - **ID**
  - **Name des Kunden**
  - **Name des Computers**
  - **Bereitstellungsdatum**
  - **Stapelbereitgestellt** (Ja/Nein)
  - **Bereitgestellt von** (Privater Anzeigename des Support-Technikers)
  - **Nutzungszähler**
  - **Datum der letzten Verwendung** (oder „Nie“, falls noch nicht verwendet)
  - **Installationsmodus** (Benutzer oder System)
  - **Symbolvorschau**
- Berechtigt, statische Felder zu bearbeiten:
  - **Beschreibung**
  - **Profil**
  - **Bereitgestellt an** (Warteschlange)
  - **Aktiviert** (Ja/Nein)
  - **Ablauf**
  - **Öffentliches Portal**

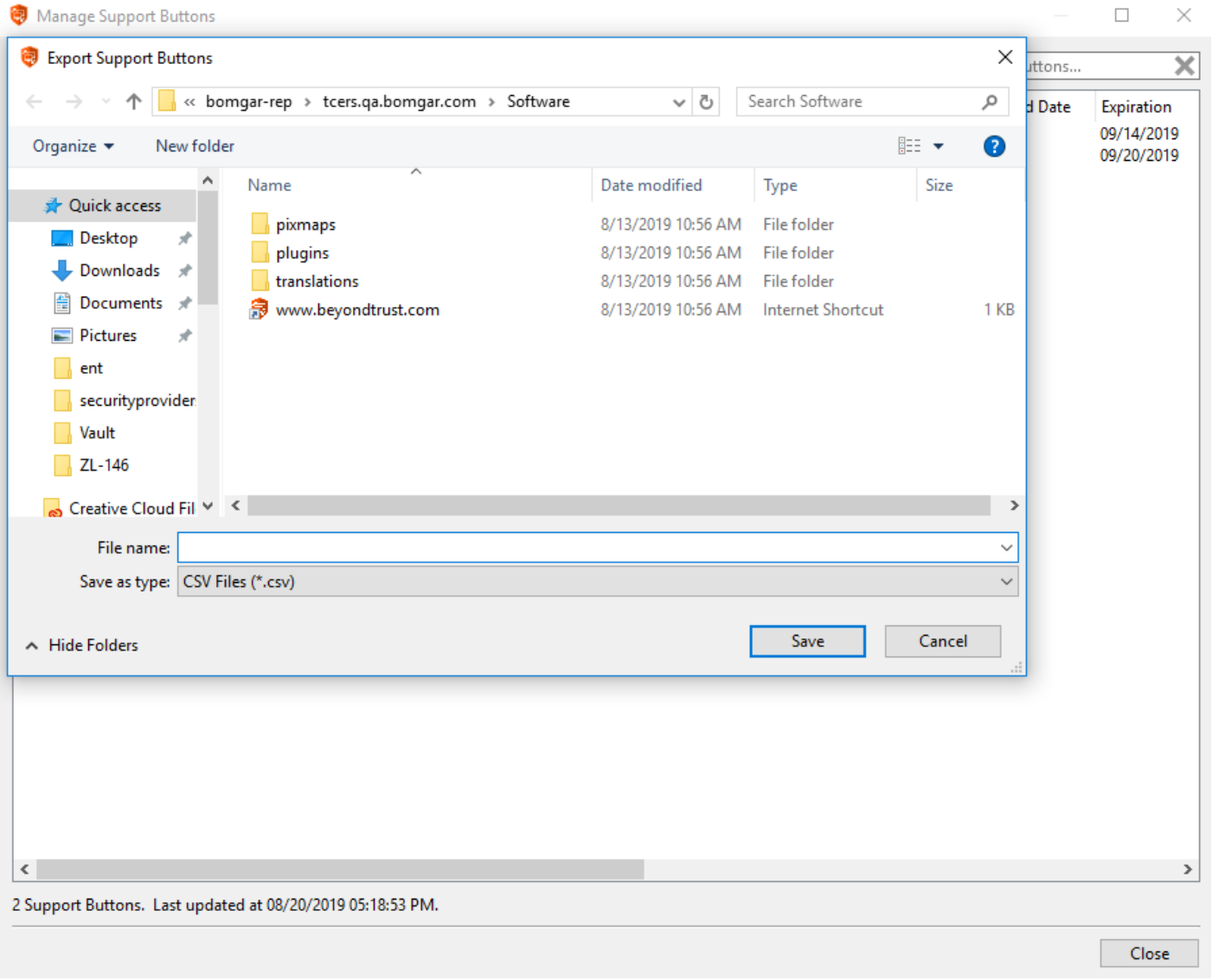


Sie können die dynamischen Felder auch **Bearbeiten**, einen Support Button **Widerrufen** oder die Nutzungsstatistiken für die Support Button in eine CSV-Datei **Exportieren**. Wenn Sie einen stapelweise bereitgestellten Support Button, der für alle Benutzer eines Systems installiert wurde, widerrufen, kann der Button nur mithilfe von „Programme hinzufügen/entfernen“ über die Systemsteuerung bzw. mit Systemverwaltungstools entfernt werden.

Wenn Sie in der **Support Button-Verwaltungsschnittstelle** den Eintrag **Bearbeiten** wählen, können Sie die dynamischen Felder bearbeiten. Wenn mehrere Support Buttons zur Bearbeitung ausgewählt sind, wird in allen dynamischen Feldern, die unterschiedliche Werte enthalten, **Mehrere Werte** angezeigt.



Wenn Sie die Nutzungsstatistiken **Exportieren** möchten, wird die Dateiauswahl angezeigt. Sie können den gewünschten Dateinamen und den Speicherort für die *.csv-Datei eingeben.



Überwachung von Teammitgliedern über das Dashboard

Mit dem Dashboard können berechtigte Benutzer laufende Sitzungen anzeigen und überwachen und die Administratoraufsicht aktivieren, um Personal besser anleiten zu können. Basierend auf den über die Seite **Technische Support-Teams** der Verwaltungsschnittstelle zugewiesenen Rollen können Teamführer Teammitglieder eines bestimmten Teams überwachen, und Team-Manager können Teamführer sowie die Mitglieder dieses Teams überwachen.

Ist ein Benutzer Team-Manager oder Teamführer eines oder mehrerer Teams, erscheint das Dashboard-Fenster unter dem Fenster der Warteschlangenauswahl auf der Registerkarte **Startseite** der Konsole. In diesem Bereich werden alle angemeldeten Teammitglieder einer niedrigeren Rolle für das ausgewählte Team angezeigt.

Statusindikatoren zeigen, ob Benutzer zur Annahme von Sitzungen verfügbar sind (grün), inaktiv sind (grau), beschäftigt sind (gelb) oder die automatische Zuweisung ausgeschaltet haben (rot). Wenn ein Benutzer über mehr als einen Status verfügt, zeigt die Statusfarbe die wichtigste Information an, und zwar in folgender Reihenfolge: Automatische Zuweisung ausgeschaltet, Beschäftigt, Inaktiv und Verfügbar. Fahren Sie mit dem Mauszeiger über den Namen des Benutzers, um die vollständigen Einzelheiten anzuzeigen. Eine Leiste unten am Dashboard zeigt den Prozentsatz der Benutzer mit jedem Status. Fahren Sie mit dem Mauszeiger über diese Leiste, um die Anzahl der Benutzer mit jedem Status anzuzeigen. Benutzer können die Anzeige ihres Status nicht manuell ändern.

Wählen Sie einen Benutzer aus dem Dashboard-Fenster aus, um jegliche Sitzungen anzuzeigen, die möglicherweise laufen. Ein Team-Manager oder Teamführer kann die Sitzung eines anderen Benutzers dieses Teams übernehmen, indem er die jeweilige Sitzung über die Warteschlange auswählt und auf **Übernehmen** klickt. Dadurch wird der Team-Manager oder Teamführer der Eigentümer dieser Sitzung. Der ursprüngliche Benutzer bleibt weiter Teilnehmer der Sitzung. Ein Team-Manager oder Teamführer kann das Eigentum einer Support-Sitzung Tech auch von einem Benutzer auf einen anderen oder auf ein Team übertragen.

Ebenfalls kann ein Team-Manager einer laufenden Sitzung beitreten, indem er auf die Schaltfläche **Beitreten** klickt. Dieser Vorgang ähnelt dem Beitritt einer Sitzung über eine Sitzungseinladung, es wird dabei jedoch keine Einladung benötigt.

Darüber hinaus kann ein Team-Manager oder Teamführer Teammitglieder einer niedrigeren Berechtigungsstufe bei entsprechender Konfiguration in der **/login**-Schnittstelle auch dann überwachen, wenn keine Sitzungen laufen, solange diese Benutzer in der Konsole angemeldet sind.

Ein Überwachungssymbol kann in der Ecke des Benutzer-Desktops angezeigt werden, um anzuzeigen, dass eine Überwachung stattfindet. Wenn der Benutzer seinen Cursor in die Nähe dieses Symbols bewegt, wird es in eine andere Ecke verschoben, um den Bildschirm nicht zu verdecken. Wählen Sie den Benutzer, dessen Bildschirm Sie anzeigen möchten, und klicken Sie auf **Überwachen**. Dadurch wird in Ihrer Konsole eine neue Registerkarte geöffnet, auf der, abhängig von den Einstellungen des Administrators, entweder der gesamte Computerbildschirm des Benutzers oder nur die Konsole angezeigt wird.

Um den Computer des Benutzers zu steuern, klicken Sie auf **Maus-/Tastatursteuerung aktivieren**.

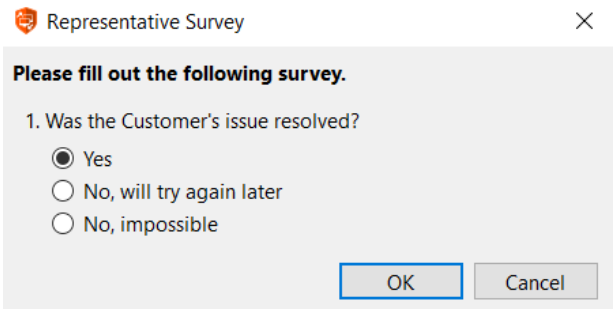
In einem Team kann ein Benutzer nur andere Benutzer mit Rollen überwachen, die seiner untergeordnet sind.

> ***Hinweis:*** *Die Rollen gelten strikt auf Teambasis; ein Benutzer kann also unter Umständen in der Lage sein, einen anderen Benutzer in einem Team zu verwalten, aber nicht denselben Benutzer in einem anderen Team.*

Support-Techniker-Umfrage

Am Ende der Sitzung können Sie aufgefordert werden, eine kurze Umfrage zur Sitzung auszufüllen. Ihr Administrator kann die Fragen über die Verwaltungsschnittstelle voll anpassen und die Ergebnisse aus den Sitzungsberichten beurteilen. Sind eine oder mehrere Fragen erforderlich, dürfen Sie die Sitzung erst schließen, wenn Sie diese Fragen beantwortet haben.

Ihr Administrator ermöglicht es Ihnen unter Umständen ebenfalls, während der Sitzung auf die Support-Techniker-Umfrage zuzugreifen. In diesem Szenario kann die Umfrage als Arbeitsablaufvorlage verwendet werden und ermöglicht es Ihrem Administrator, eine Reihe von Fragen und/oder Kontrollpunkten aufzustellen sowie bestimmte Links, die Sie in Ihrer Support-Sitzung Tech brauchen könnten.



Was Ihr Kunde sieht: Der BeyondTrust Kunden-Client

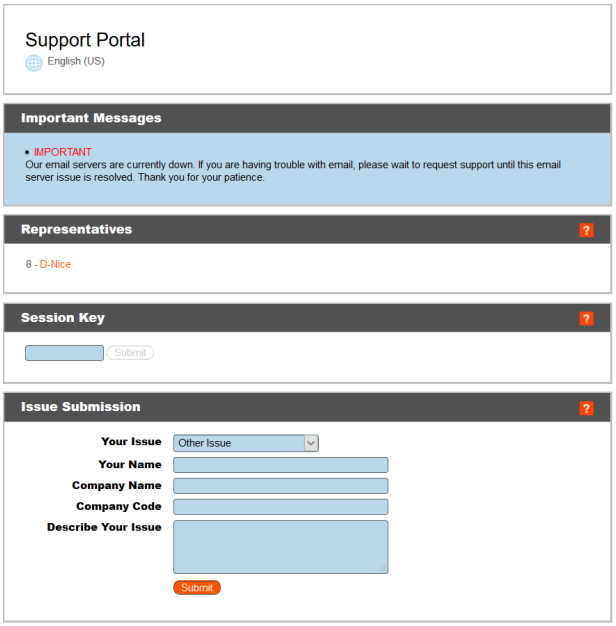
Kunden mit Remote-Desktops, Smartphones und anderen Geräten interagieren mit Support-Technikern vorwiegend über den BeyondTrust Kunden-Client mit Support-Technikern.

Sie können u.U. auch Anzeigen und Nachrichten auf der öffentlichen Website oder im Support-Portal lesen. In diesem Abschnitt werden die kundenseitigen Elemente einer BeyondTrust Remote-Support-Sitzung Tech. auf einem Desktop oder Laptop beschrieben.

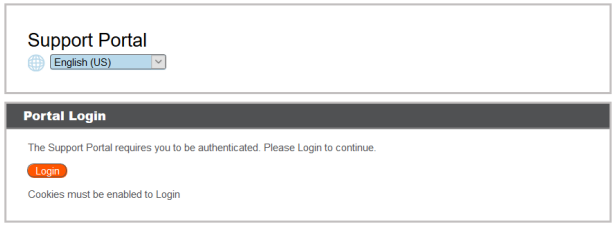
Weitere Informationen zur Unterstützung anderer Geräte, darunter Apple iOS und Android finden Sie auf https://www.beyondtrust.com/docs/remote-support/getting-started/index.htm.

Öffentliche Website: Support anfordern

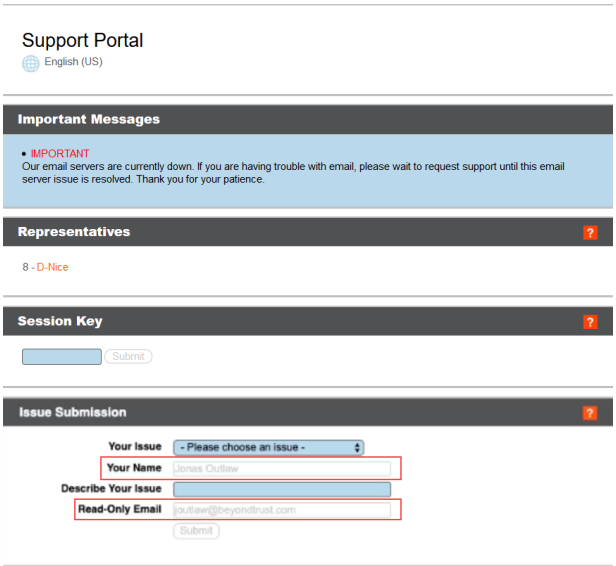
Die öffentliche Website ist das Support-Portal für Ihr Secure Remote Access Appliance. Ihre Kunden gehen hierhin, um eine Support-Sitzung Tech. anzufordern oder einer Präsentation beizutreten. Auf dieser Seite kann Ihr Kunde durch das Anklicken des Namens eines Support-Technikers, durch Einreichen eines Sitzungsschlüssels oder Ausfüllen eines Kontaktformulars für Problemfälle eine Sitzung einleiten. Kunden können auch jederzeit einer Präsentation beitreten, indem sie auf einen Präsentations-Link klicken oder einen Sitzungsschlüssel eingeben.



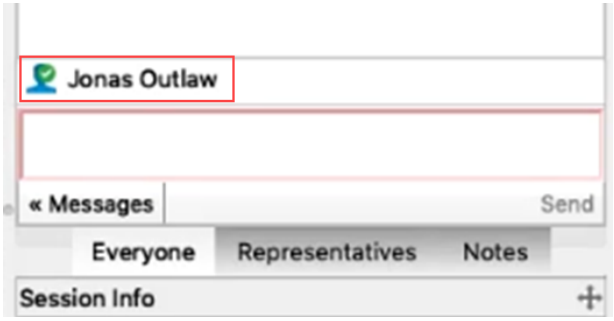
Ein Kunde kann auf das öffentliche Support-Portal zugreifen, indem er die von einem Support-Techniker bereitgestellte URL verwendet. Wenn die SAML-Authentifizierung für die öffentliche Website konfiguriert und aktiviert ist, wird dem Kunden das Fenster **Portalanmeldung** angezeigt. Der Kunde muss auf **Anmelden** klicken und dann seine Anmeldedaten angeben, um sich beim Identitätsanbieter zu authentifizieren.



Der Kunde wird dann auf die Seite des Support-Portals weitergeleitet, wo er seine Support-Anfrage stellen kann. Der Name des Kunden und alle konfigurierten benutzerdefinierten Felder, wie z. B. E-Mail, werden automatisch ausgefüllt und sind nicht editierbar.



> ***Tipp:*** *Ein grünes Häkchen wird neben dem Namen des Kunden im Konsole d. Support-Technikers Chat-Fenster angezeigt, um anzuzeigen, dass der Benutzer für das öffentliche Portal authentifiziert ist.*



> *Weitere Informationen siehe SAML für die Einzelanmeldung unter https://www.beyondtrust.com/docs/remote-support/how-to/integrations/security-providers/saml/index.htm.*

Ist die Echtzeit-Chatübersetzung aktiviert, können Kunden in ihrer eigenen Sprache mit einem Support-Techniker chatten. So kann beispielsweise ein englischsprachiger Kunde mit einem Support-Techniker chatten, der nur Niederländisch spricht, wobei der Chatverkehr in Echtzeit übersetzt wird.

> *Weitere Informationen zur Konfiguration von Chat-Übersetzungen in Echtzeit finden Sie in Echtzeit-Chatübersetzung unter https://www.beyondtrust.com/docs/remote-support/videos/real-time-chat-translation.htm.*

Ist die Problemeinreichungs-Umfrage aktiviert, wird Ihr Kunde aufgefordert, entweder den Namen eines Support-Technikers oder einen bestimmten Problemtyp zu wählen (je nach den von Ihrem Administrator festgelegten Einstellungen). Ihr Kunde kann auch seinen Namen, den Namen des Unternehmens und eine Beschreibung des Problems eingeben. Ihr Administrator kann optional das Feld **Unternehmenscode** vorgeben, damit Probleme besser verfolgt werden können.

Je nach der Methode der Sitzungseinleitung wird Ihr Kunde entweder in die Support-Warteschlange des ausgewählten Support-Technikers oder in die Support-Warteschlange für das dem ausgewählten Problem zugewiesene Team eingereiht bzw. tritt der angegebenen Präsentation bei.

Für Ihre Kunden mit Apple iOS-Geräten fungiert Ihr iOS-konfiguriertes Supportportal als geschützter Speicher für öffentliche und private Profile, die Sie in der **/login**-Schnittstelle hochgeladen haben. Private Profile sind nur dann zugänglich, wenn der Support-Techniker einen iOS-Zugangsschlüssel erstellt hat.

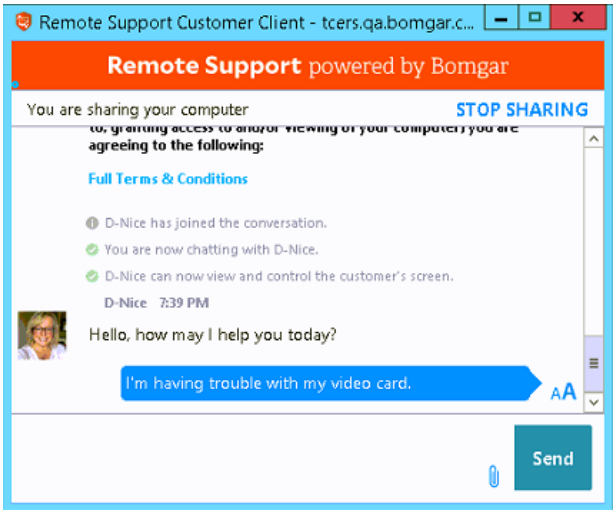
Wenn Kundenhinweise für diese Website aktiv sind, werden sie im Abschnitt **Wichtige Nachricht** angezeigt. Hinweise können Kunden auf breitenwirksame IT-Ausfälle aufmerksam machen, für die evtl. kein Support erforderlich ist; somit bleibt es dem Kunden erspart, unnötig einer Support-Sitzung Tech. beizutreten.

Wenn ein Zeitplan für diese öffentliche Website festgelegt wurde und die aktuelle Uhrzeit außerhalb der regulären Geschäftszeiten liegt, werden andere Sitzungsstartmethoden als Sitzungsschlüsel von der Website entfernt und eine Meldung erscheint, dass das Portal geschlossen ist.

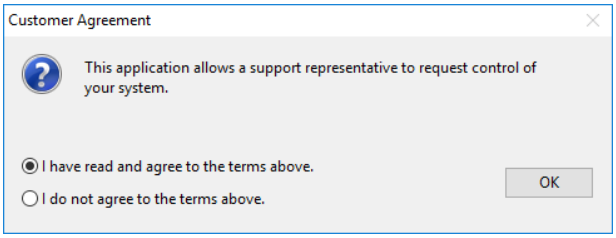
Kunden-Client: Schnittstelle für Support-Sitzungen Tech.

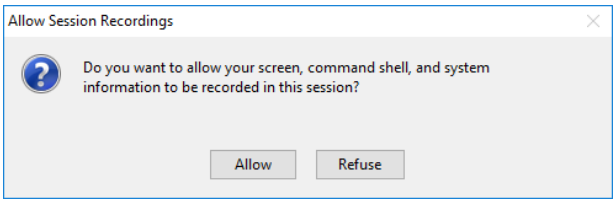
Wenn Ihr Kunde eine Support-Sitzung Tech. mit Ihnen startet, beginnt diese Sitzung entweder als web-basierter Chat oder mit dem vollständigen Download des Kunden-Clients, je nachdem welche Einstellungen für Ihre Website gelten. Wenn Sie einen Fotoavatar für Ihr Konto hochgeladen haben, wird das Foto im Chatfenster angezeigt. Beachten Sie, dass dies nur mit dem vollen Kunden-Client, nicht mit dem HTML-Client funktioniert.

Beim Start einer Sitzung als HTML5 web-basierter Chat wird Ihr Kunde gebeten, Benachrichtigungen und Pop-Up-Benachrichtigungen zu gestatten, damit die Kommunikation mit dem Kunden effizienter gestaltet werden kann.



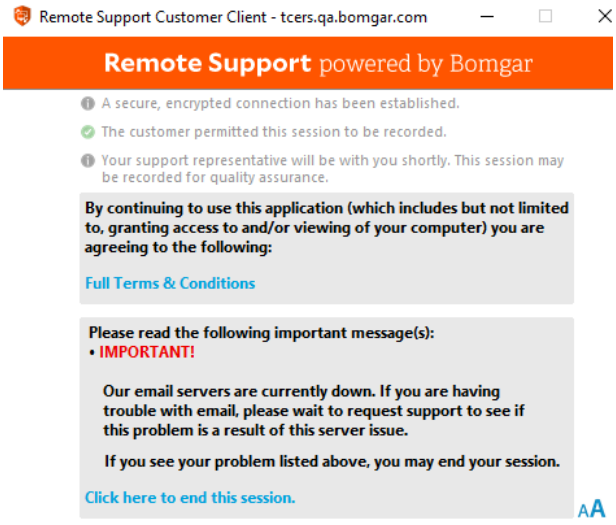
Ihr Administrator kann bestimmen, welche Nachrichten Ihr Kunde vor dem Beginn der Sitzung sieht. Zu den angezeigten Nachrichten gehören eine Kundenvereinbarung, mit der der Kunde die Bedingungen zur Teilnahme an einer Support-Sitzung Tech bestätigen muss, eine Aufforderung zum Zulassen oder Ablehnen von Sitzungsaufzeichnungen und eine Begrüßung, die die geschätzte Wartezeit und die Position des Kunden in der Warteschlange enthalten kann.



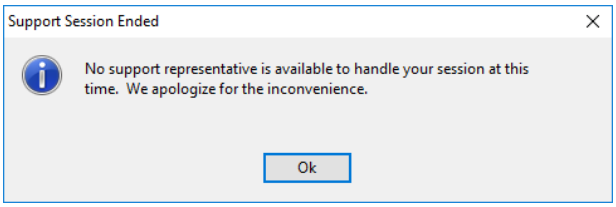


Wenn Kundenhinweise aktiv sind, können sie automatisch angezeigt oder manuell zum Kunden-Client gesendet werden. So erhalten die Kunden die Möglichkeit, die Sitzung zu verlassen, wenn sie auf ein im Hinweis beschriebenes, bekanntes Problem stoßen. Kunden, die die Sitzung auf diese Weise verlassen, gelangen nicht zur Seite **Austrittsumfrage**, da kein Service von Support-Technikern bereitgestellt wurde.

Evtl. wird regelmäßig eine Warteschleife-Nachricht angezeigt, die dem Kunden versichert, dass er sich noch in der Warteschlange befindet und bald bedient wird. Diese Nachricht kann die geschätzte Wartezeit und die Position des Kunden in der Warteschlange enthalten.



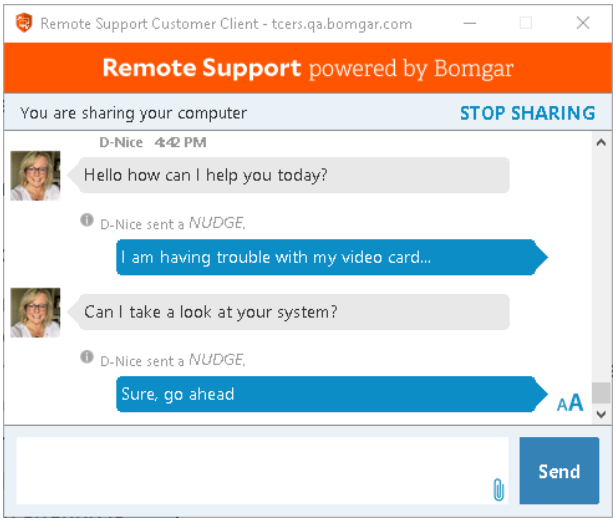
Steht kein Support-Techniker für die Sitzung zur Verfügung, kann eine Nachricht für eine verwaiste Sitzung angezeigt werden. Optional kann der Webbrowser des Kunden dann automatisch auf eine bestimmte URL, z. B. eine Wissensbank oder Kontaktseite geöffnet werden.



Während der Sitzung kann der Kunde mit Ihnen chatten und anfordern, Dateien an Ihren Computer zu senden. Ihr Kunde kann auch die Schriftgröße der Chat-Anzeige ändern.

Wenn Sie einen Stups senden, wird der Fokus auf den Kunden-Client gerichtet, dieser gerüttelt, und es ertönt ein Alarmton. In der Chat-Anzeige wird angezeigt, dass ein Stups gesendet wurde.

Um die Bildschirmfreigabe unmittelbar zu beenden und Berechtigungen des Support-Technikers zu deaktivieren, klicken Sie auf den Link **BILDSCHIRMFREIGABE BEENDEN** rechts neben dem Banner über dem Chat. Der Kunde kann die Sitzung auch gänzlich beenden, indem er das Chatfenster schließt. Dadurch wird die Software vom System deinstalliert.



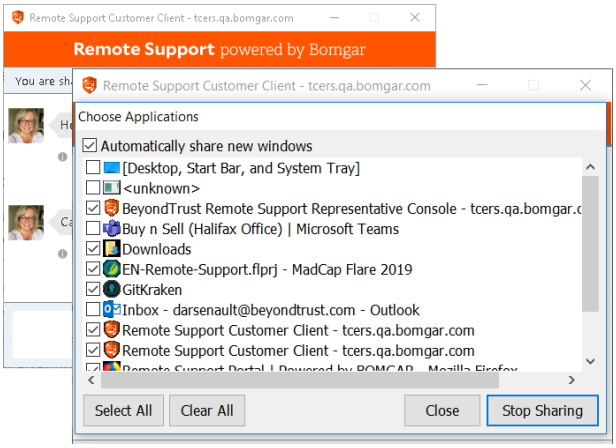
> ***Hinweis: BILDSCHIRMFREIGABE BEENDEN*** *erscheint, wenn die Bildschirmfreigabe ohne Einschränkungen erfolgt. Wenn Sie dem Kunden die Auswahl der Anwendungen gestatten, wird* ***FREIGABE ÄNDERN*** *angezeigt. Hier kann der Kunde die Freigabe von Anwendungen konfigurieren oder, falls gewünscht, die Freigabe vollständig beenden. In jedem Fall kann die Sitzung stets durch Schließen des Chatfensters beendet werden.*

Darüber hinaus kann auf dem Bildschirm Ihres Kunden abhängig von Ihren Site-Einstellungen während der Sitzung ein Wasserzeichen erscheinen. Dies gilt nur für Windows-Systeme.

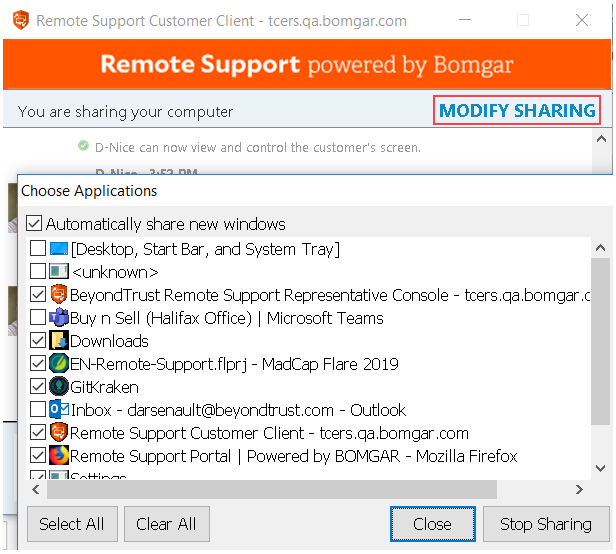
> ***Hinweis:*** *Kunden, die Linux ausführen, müssen die Kunden-Client-Download-Datei als ausführbare Datei markieren, bevor sie sie installieren können.*

Anwendungsfreigabe: Einschränkung der für den Support-Techniker sichtbaren Elemente

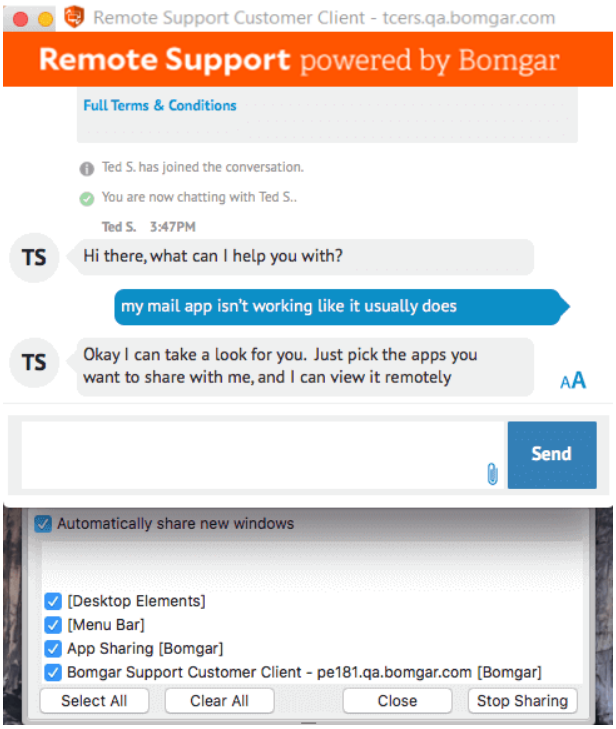
Wenn Sie eine beschränkte Bildschirmfreigabe anfordern, wird vor dem Kunden-Client-Chat-Fenster ein Auswahlfenster angezeigt.



Nachdem die Erlaubnis zur Bildschirmfreigabe erteilt wurde, können Sie über den Link **Bildschirmfreigabe modifizieren** auf das Anwendungsauswahlfenster zugreifen.

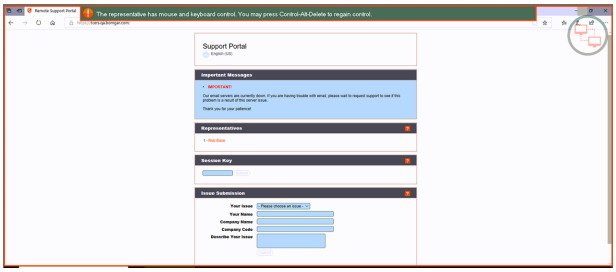


Je nach Ihren Website-Einstellungen kann Ihr Kunde unter Umständen stets Anwendungen über das Seitenmenü auswählen, auch wenn die beschränkte Bildschirmfreigabe nicht speziell angefordert wurde. Die Anwendungsfreigabe ist bei der Unterstützung von Windows oder Mac-Computern verfügbar. Sie verfügen möglicherweise über vordefinierte Anwendungsfreigabebeschränkungen, die vom Support-Team-Administrator festgelegt wurden und für Ihre Support-Sitzung Tech. gelten.



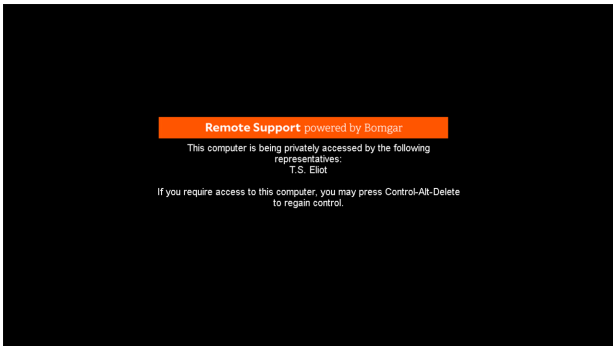
Beschränkte Kunden-Interaktion: Privater Bildschirm, Remote-Eingaben deaktivieren

Um den Support eines Remote-Computers zu beschleunigen, können Sie Beeinflussung durch den Kunden vermeiden, indem Sie die Eingabemöglichkeit über Maus und Tastatur des Kunden deaktivieren. Der Remote-Benutzer kann den aktiven Desktop trotzdem sehen. Während die Eingabemöglichkeit deaktiviert ist, wird auf jedem Remote-Bildschirm ein oranger Rahmen angezeigt.



Sollten Sie privat auf dem Remote-Computer arbeiten müssen, können Sie einen privaten Bildschirm aktivieren, sodass der Remote-Benutzer oder Passanten nicht sehen können, was Sie gerade machen. Stattdessen wird eine entsprechende Meldung angezeigt. Ihr Kunde kann durch Drücken von **Strg-Alt-Entf** stets wieder die Kontrolle übernehmen.

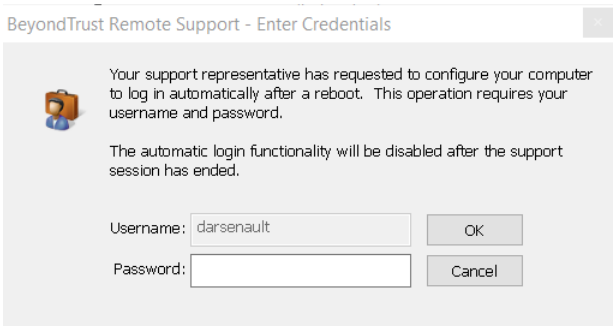
Die eingeschränkte Kundeninteraktion ist nur bei der Unterstützung von macOS- Windows-Computern verfügbar. In Windows Vista und höher muss der Kunden-Client heraufgesetzt werden. In Windows 8 und höher ist der private Bildschirm nicht verfügbar, und der Support-Techniker kann nur Maus und Tastatur deaktivieren.



*Diese Funktion wird über die Registerkarte **Bildschirmfreigabe** einer Support-Sitzung Tech. in der Konsole d. Support-Technikers aktiviert. Weitere Informationen finden Sie in „Bildschirmfreigabe bei Remote-Kunde für Anzeige und Steuerung“ auf Seite 79.*

Daten zur automatischen Anmeldung: Neustart und Neuverbindung

Sie können Ihren Kunden auffordern, einen gültigen Benutzernamen und ein Kennwort einzugeben, sodass Sie den Remote-Computer neu starten und sich automatisch wieder anmelden können, ohne die Anmeldedaten zu kennen oder zu erfordern, dass Ihr Kunde anwesend ist. Folgen Sie den untenstehenden Schritten, um die Funktion für die Daten zur automatischen Anmeldung zu verwenden:



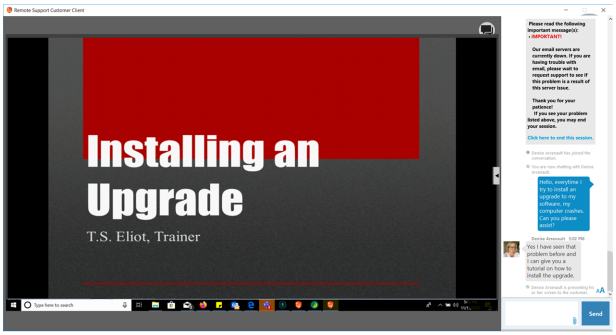
Hinweis: *Um diese Funktion auszuführen, muss Ihr Administrator die /login-Sicherheitsoption „Neustart mit zwischengespeicherten Anmeldedaten zulassen“ aktiviert haben.*

Tipp: *Bevor Sie diese Funktion verwenden können, müssen Sie die Support-Sitzung Tech. heraufsetzen und die Bildschirmfreigabe beginnen.*

Hinweis: *Die Anmeldedaten werden vom Betriebssystem und nicht von BeyondTrust gespeichert. Wir nutzen dafür eine Sicherheitsfunktion in Windows. Die Anmeldedaten werden niemals im Netzwerk offengelegt. Diese Funktion ist nur in Windows verfügbar und kann nicht auf Remote-Systemen mit Mac OS ausgeführt werden.*

1. Klicken Sie im Menü auf **Spezielle Betriebssteuerungsaktion**.
2. Wählen Sie **Anmeldedaten für automatische Anmeldung anfordern**.
3. Der Benutzer muss nun seine Anmeldedaten in die Aufforderung eingeben.
4. Danach ändert sich der Menütext von **Anmeldedaten für automatische Anmeldedaten anfordern** zu **Anmeldedaten für automatische Anmeldung löschen**.
5. Nach dem nächsten Neustart meldet sich das System mit den vom Benutzer eingegebenen Anmeldedaten an.

Eigenen Bildschirm anzeigen: Umgekehrte Bildschirmfreigabe



Wenn Sie Ihren Bildschirm während einer Support-Sitzung Tech. einem Kunden freigeben, kann Ihr Kunde entweder Ihren gesamten Desktop oder nur die Anwendungen sehen, die Sie anzeigen möchten. Sie können während des gesamten Vorgangs weiter mit Ihrem Kunden chatten.

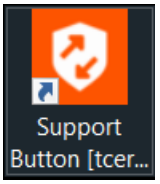
Um den Bildschirmanzeigebereich zu vergrößern, kann Ihr Kunde die Chat-Seitenleiste durch Klicken auf den Ein-/Ausblenden-Pfeil auf der Trennlinie zwischen der Chat-Leiste und dem Präsentationsfenster ausblenden. Erhält Ihr Kunde eine Nachricht, während die Chat-Leiste ausgeblendet ist, blinkt der Ein-/Ausblenden-Pfeil orange auf.

Ihr Kunde kann die Präsentationsanzeige weiter definieren, indem er wählt, Ihren Bildschirm in der tatsächlichen Größe oder im Client-Fenster skaliert anzuzeigen. Ihr Kunde kann Ihren Bildschirm auch bei 8 Bits (schneller), bei 16 Bits (mittlere Bildqualität und Leistung) oder 32 Bits (höchste Bildauflösung) anzeigen. Sie können die Maus- und Tastatursteuerung außerdem für Ihren Remote-Kunden freigeben.

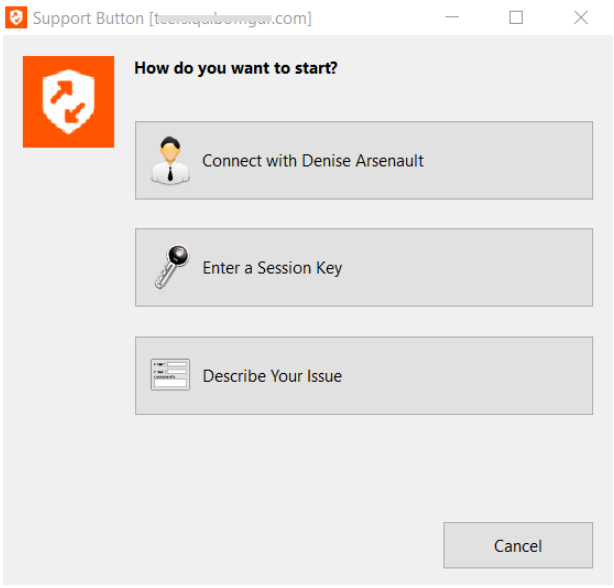
Hinweis: *Der Linux-Kunden-Client unterstützt nicht die Steuerung des Bildschirms des Support-Technikers.*

Support Button: Schnell Support anfordern

Falls Sie einen Support Button auf dem Computer Ihres Kunden installiert haben, wird dieser als Desktop-Verknüpfung oder Startmenü-Eintrag auf dessen Computer angezeigt. Wenn der Support Button angepasst wurde, wird er mit kundenspezifischem Bild und Titel auf dem Kundencomputer angezeigt.



Durch Klicken auf diese Schaltfläche wird ein Dialogfeld geöffnet, in dem Ihr Kunde dazu aufgefordert wird, eine Sitzung zu starten. Wurde diese Schaltfläche so vorkonfiguriert, dass eine Sitzung mit einem bestimmten Support-Techniker oder Team gestartet wird, kann Ihr Kunde die Sitzung durch einfaches Anklicken der Schaltfläche **Verbinden** starten.



Alternativ dazu können Ihre Kunden einen Sitzungsschlüssel eingeben oder ihr Problem beschreiben. Wenn Ihr Kunde einen Sitzungsschlüssel eingibt, wird er mit dem Support-Techniker verbunden, der den Schlüssel erstellt hat, unabhängig davon, ob der Support-Techniker diesem Support Button zugeordnet ist oder nicht.

> ***Hinweis:*** *Ein Support Button kann nicht aus einer Sitzung bereitgestellt werden, die von einem SAML-authentifizierten öffentlichen Portal gestartet wurde, und ein Support Button kann nicht verwendet werden, um eine Sitzung mit einem öffentlichen Portal zu starten, das SAML-Authentifizierung erfordert.*

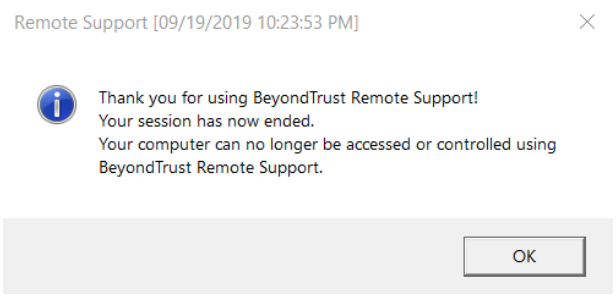
Wenn Kundenhinweise für die öffentliche Website aktiv sind, mit der dieser Support Button verbunden ist, werden diese Nachrichten oben angezeigt. Hinweise können Kunden auf IT-Komplettausfälle aufmerksam machen, für die evtl. kein Support erforderlich ist; somit bleibt es dem Kunden erspart, unnötig einer Support-Sitzung Tech. beizutreten.

Wenn ein Zeitplan für diese öffentliche Website festgelegt wurde und die aktuelle Uhrzeit außerhalb der regulären Geschäftszeiten liegt, werden andere Sitzungsstartmethoden als Sitzungsschlüsel vom Support Button entfernt und eine Meldung erscheint, dass das Portal geschlossen ist.

Wenn Sie einen Support Button in einer externen Anwendung eingebettet haben, wird dieser Support Button als Link in der Titelleiste der Anwendung angezeigt. Mit einem Klick auf diesen Link wird das Dialogfenster für alle Optionen für den Sitzungsstart oder die Umfrage zum Einreichen von Problemen mit vorausgewähltem Problem geöffnet, oder aber Ihr Kunde wird direkt mit einem vorausgewählten Problem in die Teamwarteschlange gesandt.

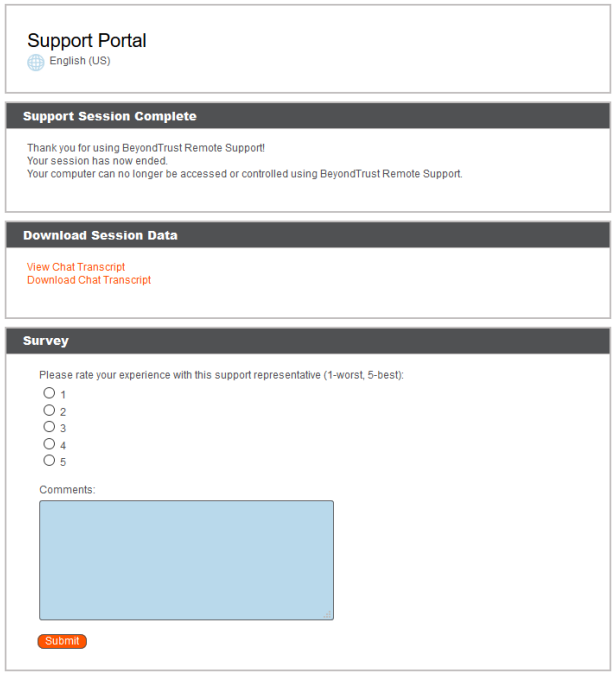
Kundenaustrittsumfrage: Feedback einreichen

Ist die Sitzung abgeschlossen und kein Jump-Client für den späteren Zugriff installiert, wird Ihr Kunde benachrichtigt, dass Sie seinen Computer nicht mehr sehen und auch nicht mehr darauf zugreifen können und BeyondTrust vollständig deinstalliert wurde.



Hat Ihr Administrator eine Austrittsumfrage aktiviert, wird Ihr Kunde an eine Umfrage weitergeleitet, in der er aufgefordert wird, seine Erfahrung mit der Sitzung zu beurteilen. Ihr Administrator kann diese Umfrage über die Verwaltungsschnittstelle völlig anpassen und die Antworten später anhand der Sitzungsberichte analysieren.

Alternativ kann Ihr Administrator eine URL für die Weiterleitung nach der Sitzung einrichten. Es wird dann ein Browser-Fenster auf dem Computer des Kunden geöffnet, und der Kunde wird zur jeweiligen Website weitergeleitet.



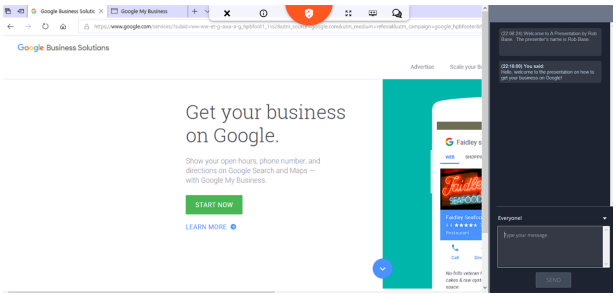
Präsentationsteilnehmer-Client: Beitreten zu einer Präsentation

> ***Hinweis:*** *Die Präsentationsfunktion muss aktiviert sein, wenn Ihre Support-Website erstellt wird. Ist dies nicht der Fall, und Sie müssen Präsentationen durchführen, wenden Sie sich bitte an den Support oder Ihren Website-Administrator.*

Um einer Präsentation von einem Computer aus beizutreten, verbindet sich Ihr Teilnehmer sofort und nahtlos über einen Browser mit HTML5. Ihr Teilnehmer kann einer Präsentation über mehrere Methoden beitreten.

Teilnehmer können einer Präsentation ebenfalls über ein iOS- oder Android-Gerät beitreten. Dafür muss er die BeyondTrust-Präsentations-App herunterladen. Einzelheiten zur Unterstützung des geeigneten Geräts finden Sie in der BeyondTrust-Dokumentation.

Ihr Administrator kann bestimmen, welche Nachrichten Ihr Teilnehmer vor dem Beginn der Präsentation sieht, falls gewünscht. Es können u. a. eine Teilnehmervereinbarung und eine Begrüßung angezeigt werden. Abhängig vom Präsentationsstatus wird Ihrem Teilnehmer die Meldung angezeigt, dass der Moderator die Präsentation angehalten hat oder dass die Präsentation beendet wurde und der Browser geschlossen werden kann. Ist niemand verfügbar, um die Präsentation abzuhalten, kann auch eine Meldung bezüglich einer verwaisten Präsentation angezeigt werden.

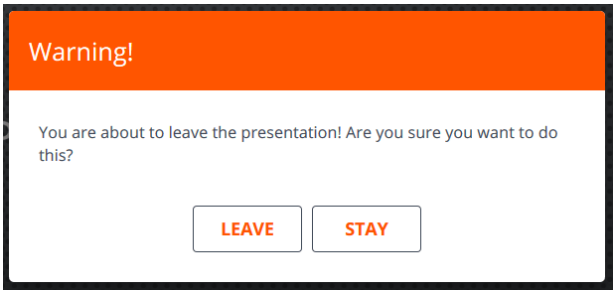


Während einer Präsentation können Teilnehmer Ihren Desktop oder ausgewählte Anwendungen einsehen und auch ausschließlich mit Ihnen oder mit Ihnen und anderen Teilnehmern gleichzeitig chatten.

Mit einem Klick auf das orange B-Symbol können Teilnehmer über die Symbolleiste Aktionen zur Ausführung wählen. Sie können die Sitzung verlassen, Präsentationsdetails anzeigen, in den Vollbildmodus wechseln, die Bildschirmgröße ändern und das Chatfenster ein- und ausblenden.

Sie können auch die Maus- und Tastatursteuerung für Teilnehmer freigeben. Die Symbolleiste und das Chatfenster werden fixiert, wenn der Teilnehmer die Steuerung übernimmt. Es kann nur jeweils ein Teilnehmer gleichzeitig die Steuerung über Ihren Computer übernehmen. Sie können die Steuerung des Teilnehmers jederzeit abbrechen.

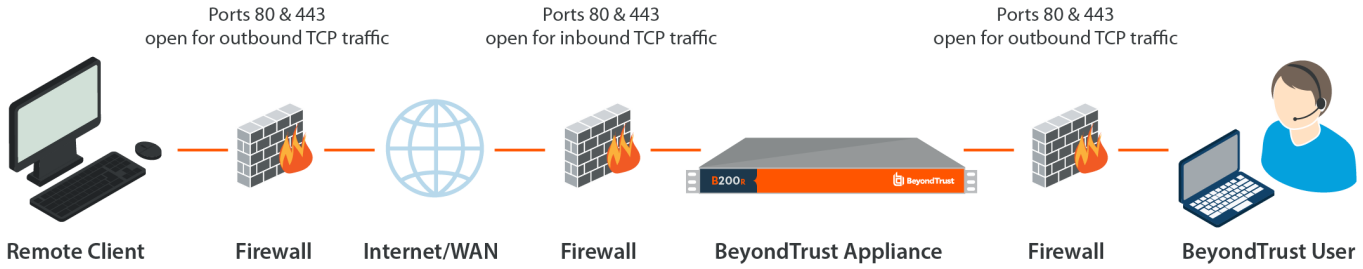
Am Ende der Präsentation erhalten Teilnehmer eine Meldung, die fragt, ob sie die Präsentation verlassen möchten.



Ports und Firewalls

BeyondTrust-Lösungen funktionieren transparent durch Firewalls, sodass eine Verbindung mit einem beliebigen Computer mit Internetkonnektivität weltweit hergestellt werden kann. Bei bestimmten, stark gesicherten Netzwerken sind aber unter Umständen einige Konfigurationsschritte erforderlich.

TYPICAL NETWORK SETUP



- Die Ports 80 und 443 müssen für ausgehenden TCP-Verkehr an der Firewall des Remote-Systems und an der des lokalen Benutzers offen sein. Mehr Ports stehen möglicherweise abhängig von Ihrer Konfiguration zur Verfügung. Das Diagramm zeigt eine typische Netzwerkkonfiguration. Weitere Informationen finden Sie in .
- Internetsicherheits-Software wie Software-Firewalls darf den Download von ausführbaren BeyondTrust-Dateien nicht blockieren. Einige Beispiele für Software-Firewalls sind McAfee Security, Norton Security und Zone Alarm. Falls Sie eine Software-Firewall verwenden, kann es zu Verbindungsproblemen kommen. Um diese zu vermeiden, konfigurieren Sie Ihre Firewall so, dass die folgenden ausführbaren Dateien zugelassen werden, wobei {uid} ein Platzhalter für eine eindeutige Kennung ist, die aus Buchstaben und Zahlen besteht:
    - bomgar-scc-{uid}.exe
    - bomgar-scc.exe
    - bomgar-pac-{uid}.exe
    - bomgar-pac.exe

  Unterstützung für die Konfiguration der Firewall erhalten Sie beim Hersteller der Firewall-Software.
- Beispiel-Firewall-Regeln basierend auf dem Gerätestandort finden Sie unter www.beyondtrust.com/docs/remote-support/getting-started/deployment/dmz/firewall-rules.htm.

Wenn weiterhin Probleme beim Herstellen einer Verbindung auftreten, wenden Sie sich an den BeyondTrust Technical Support unter www.beyondtrust.com/support.

Problembehebung für Verbindungen zur BeyondTrust-Konsole des Support-Technikers

1. Stellen Sie sicher, dass Sie an der Konsole d. Support-Technikers angemeldet sind.
2. Falls Sie die Support-Techniker-Liste gewählt haben, müssen Sie gewährleisten, dass Ihr Anzeigename auf Ihrer öffentlichen Website angezeigt wird. Sie können diesen Status über das Menü **Support** oder das Infobereich-Symbol ändern, indem Sie die Option**In Support-Techniker-Liste** anzeigen aktivieren bzw. deaktivieren.
3. Gehen Sie durch die ersten Schritte zum Starten einer BeyondTrust-Sitzung auf Ihrem eigenen Computer. Können Sie den Kunden-Client herunterladen?
4. Vergewissern Sie sich, dass der Remote-Kunde mit dem Internet verbunden ist. Kann Ihr Kunde Ihre öffentliche Website erreichen?
5. Führen Sie den Kunden durch die gleichen Schritte, die Sie in Schritt 3 dieses Fehlerbehebungsvorgangs zum Testen des Downloads des Kunden-Clients durchgeführt haben. Kann Ihr Kunde den Kunden-Client herunterladen?
6. Wird der Download nicht eingeleitet, wenn der Kunde auf Ihren Namen klickt, einen Sitzungsschlüssel oder eine Support-Anforderung eingibt, veranlassen Sie, dass der Kunde die Taste **Strg** gedrückt hält und gleichzeitig **F5** drückt. Dadurch sollte der Inhalt des Browser-Zwischenspeichers gelöscht werden, wodurch der Kunde nicht versucht, eine abgelaufene Version des Kunden-Client herunterzuladen.
7. Funktioniert das Löschen des Inhalts des Browser-Zwischenspeichers nicht und wird der Kunde nicht aufgefordert, eine Datei auszuführen, kann die Firewall, hinter der sich Ihr Kunde befindet, den Download blockieren. Wenden Sie sich für eine Umgehung an den BeyondTrust Technical Support unter www.beyondtrust.com/support.
8. Fordern Sie Ihren Remote-Kunden auf, den BeyondTrust-Client zu deinstallieren, den Computer neu zu starten und dann die ausführbare Datei erneut auszuführen.
9. Vergewissern Sie sich, dass Ihr Remote-Kunde alle Software-Firewalls deaktiviert hat, die ausgehende Verbindungen blockieren könnten. Einige Beispiele für Software-Firewalls sind McAfee Security, Norton Security und Zone Alarm. Diese Firewalls blockieren gelegentlich ausgehende Verbindungen auch nachdem sie deaktiviert wurden, sodass sie u. U. deinstalliert werden müssen.
10. Ihr Kunde kann auch aufgefordert worden sein, den Kunden-Client zuzulassen oder nicht zuzulassen/zu blockieren, als der heruntergeladene Client ausgeführt wurde. Hat der Kunde auf **Verweigern/Blockieren** geklickt, fordern Sie ihn auf, die Internetsicherheitssoftware auf seinem Computer zu öffnen und den Eintrag für **bomgar-scc.exe** auf **Zulassen/Genehmigen** zu ändern. Führen Sie Ihren Kunden noch einmal durch den Download-Vorgang und lassen Sie ihn auf **Speichern** statt **Ausführen** klicken. Anschließend muss er die ausführbare Datei erneut ausführen und auf **Zulassen/Genehmigen** klicken. Wenn weiterhin keine Verbindung zur Sitzung hergestellt werden kann, fordern Sie den Kunden auf, die gespeicherte ausführbare Datei noch einmal auszuführen – der Kunde sollte beim zweiten Mal nicht mehr zu einer Eingabe aufgefordert werden, und die Sitzungsverbindung sollte hergestellt werden.
11. Überprüfen Sie, ob der Kunde einen Proxy-Server eingerichtet hat. Vergewissern Sie sich, dass Ihr Kunde seine Anmeldedaten korrekt eingegeben hat, damit dem Kunden-Client gestattet wird, eine Verbindung mit Ihnen herzustellen.
12. Wenn Sie auch nach diesen Schritten keine Verbindung herstellen können, kontaktieren Sie den BeyondTrust Technical Support unter www.beyondtrust.com/support.

Haftungsausschlüsse, Lizenzierungsbeschränkungen und Technischer Support

Haftungsausschlüsse

Dieses Dokument dient ausschließlich Informationszwecken. BeyondTrust Corporation kann den Inhalt ohne Vorankündigung ändern. Es kann weder die Fehlerfreiheit dieses Dokuments garantiert werden, noch unterliegt das Dokument irgendwelchen Garantien oder Gewährleistungen, weder in mündlicher Form noch in konkludenter rechtlicher Form, einschließlich konkludenten Garantien und Gewährleistungen der Marktgängigkeit oder Eignung für einen bestimmten Zweck. Insbesondere lehnt BeyondTrust Corporation jedwede Haftung für den Inhalt des vorliegenden Dokuments ab, und durch dieses Dokument entstehen weder direkt noch indirekt irgendwelche vertraglichen Pflichten. Die hierin beschriebenen Technologien, Funktionen, Dienste und Prozesse können ohne Ankündigung geändert werden.

Alle Rechte vorbehalten. Andere Markenzeichen auf dieser Seite sind Eigentum der jeweiligen Inhaber. BeyondTrust ist keine gecharterte Bank oder Treuhandgesellschaft oder Hinterlegungsstelle. Sie ist nicht befugt, Geldeinlagen oder Treuhandkonten anzunehmen, und wird nicht von einem Staat oder einer Bundesbankbehörde lizensiert oder reguliert.

Lizenzierungsbeschränkungen

Mit einer BeyondTrust Remote Support-Lizenz kann jeweils ein Support-Techniker Probleme auf einer unbegrenzten Anzahl an Remote-Computern beheben. Dabei müssen die Benutzer nicht unbedingt am Computer sein. Obgleich mehrere Konten für die gleiche Lizenz eingerichtet sein können, sind zwei oder mehr Lizenzen (eine pro aktivem Support-Techniker) erforderlich, damit mehrere Support-Techniker gleichzeitig den Fehler beheben können.

Technischer Support

Wir bei BeyondTrust fühlen uns verpflichtet, Service von höchster Qualität zu bieten, indem wir gewährleisten, dass unsere Kunden alles haben, was sie für einen Betrieb bei maximaler Produktivität benötigen. Sollten Sie Hilfe benötigen, wenden Sie sich bitte an www.beyondtrust.com/support.

Technischen Support können Sie mit einem jährlichen Abonnement unseres Wartungsplans in Anspruch nehmen.