BeyondTrust

Privilegierter Remote-Zugriff 21.1
Benutzerhandbuch für die Zugriffskonsole

TC:7/22/2021

Inhaltsverzeichnis

BeyondTrust-Zugriffskonsole

Dieser Leitfaden soll Ihnen helfen, die BeyondTrust access console auf Ihrem Computer zu installieren und die Funktionen zu verstehen. BeyondTrust Privilegierter Remote-Zugriff ermöglicht Ihnen den Fernzugriff auf Endpunkte, indem Sie sich über den BeyondTrust Appliance B Series mit ihnen verbinden.

Verwenden Sie dieses Handbuch erst, wenn die anfängliche Einrichtung und Konfiguration des B Series Appliance durch einen Administrator abgeschlossen wurde, entsprechend der Beschreibung im BeyondTrust Appliance B Series Installationshandbuch für Hardware. Ist BeyondTrust korrekt installiert, können Sie sofort mit dem Zugriff auf Ihre Endpunkte beginnen. Sollten Sie Hilfe benötigen, wenden Sie sich bitte an BeyondTrust Technical Support unter www.beyondtrust.com/support.

Installieren Sie die Zugriffskonsole

Wechseln Sie in einem beliebigen Webbrowser zur URL Ihres B Series 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 access console herunterladen und installieren. Es wird standardmäßig das jeweilige Installationsprogramm für Ihr Betriebssystem verwendet.

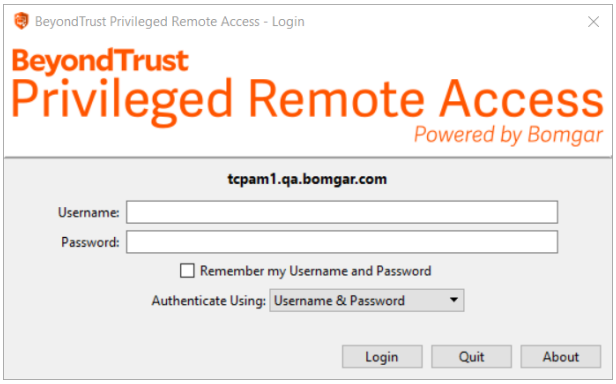
> ***Hinweis:*** *Auf einem Linux-System müssen Sie die Datei auf Ihrem Computer speichern und nach dem Herunterladen am Speicherort öffnen. Verwenden Sie nicht den Link* ***Öffnen****, der nach dem Herunterladen der Datei bei einigen Browsern angezeigt wird.*

Befolgen Sie zur Installation der Software die Anweisungen im angezeigten Installationsassistenten. Nach Installation der access console können Sie **BeyondTrust Access Console jetzt ausführen** und/oder **Beim Start ausführen** wählen. Klicken Sie dann auf **Fertig stellen**.

> ***Hinweis:*** *Wenn Sie während der Installation* ***BeyondTrust Access Console jetzt ausführen*** *wählen, erscheint auf dem Bildschirm eine Anmeldeaufforderung.*

Anmeldung an der PRA-Zugriffskonsole

Starten Sie nach dem Installieren der BeyondTrust-Konsole die access console aus dem Ordner, den Sie während der Installation angegeben haben.



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

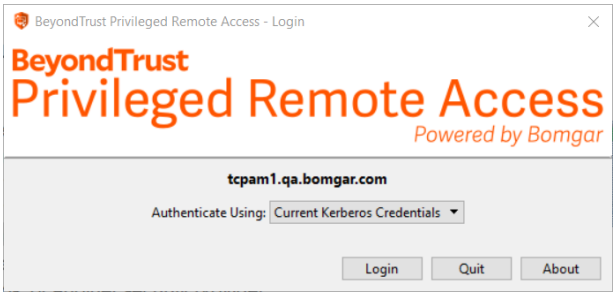
Wenn die **Anmeldungsvereinbarung** aktiviert wurde, müssen Sie auf **Akzeptieren** klicken, um fortzufahren.

> *Weitere Informationen zum Einrichten der Anmeldungsvereinbarung finden Sie unter Website-Konfiguration: HTTP-Ports festlegen, Erforderliche Anmeldungsvereinbarung aktivieren unter https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/site-configuration.htm.*

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 E-Mail-Codes zur Anmeldung erhalten, werden automatisch auf die 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 access console merkt sich den zuletzt verwendeten Anmeldemechanismus – seien es lokale Anmeldedaten, Kerberos oder ein anderer Sicherheitsanbieter.

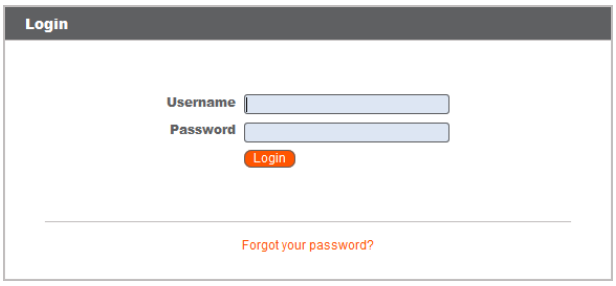
Eingeladene Benutzer können auch einen Sitzungsschlüssel eingeben, um einmalig einer freigegebenen Sitzung beizutreten.

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.

Nach der Anmeldung öffnet sich die Konsole, und ein BeyondTrust-Symbol erscheint im Infobereich Ihres Computers.

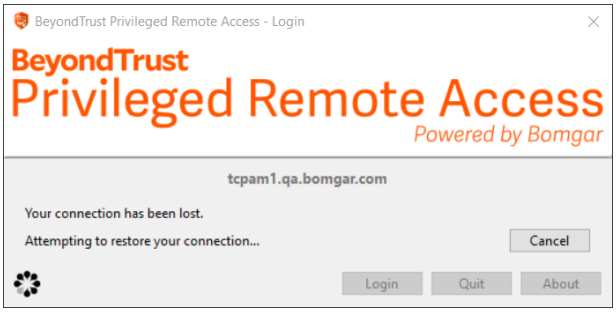
> ***Hinweis:*** *Ihr Administrator kann von Ihnen fordern, sich mit einem zugelassenen Netzwerk zu verbinden, um sich in der Konsole anmelden zu können. Diese Netzwerkeinschränkung gilt möglicherweise nur für die erste Anmeldung oder aber jedes Mal.*

> ***Hinweis:*** *Wenn Sie Ihr Kennwort vergessen haben, navigieren Sie zu* ***/login*** *und klicken Sie auf den Link* ***Kennwort vergessen?****. Dies ist eine Option, die von Ihrem Administrator festgelegt wird. Wenn Sie diese Option nicht sehen, kontaktieren Sie bitte Ihren Administrator.*



Sollte die Verbindung abbrechen, versucht die access console 60 Sekunden lang, die Verbindung wieder aufzubauen. Wenn Ihre Verbindung innerhalb dieser Zeit wieder aufgebaut ist, wird die access console erneut geöffnet und alle Ihre offenen Sitzungen werden wiederhergestellt. Wenn die Verbindung innerhalb dieser Zeit nicht wiederhergestellt werden kann, werden Sie aufgefordert, sich erneut anzumelden oder die Konsole zu beenden.

Wenn Sie an einem Ort an der access console angemeldet sind und sich dann einem anderen Ort anmelden, werden offene Sitzungen beibehalten.



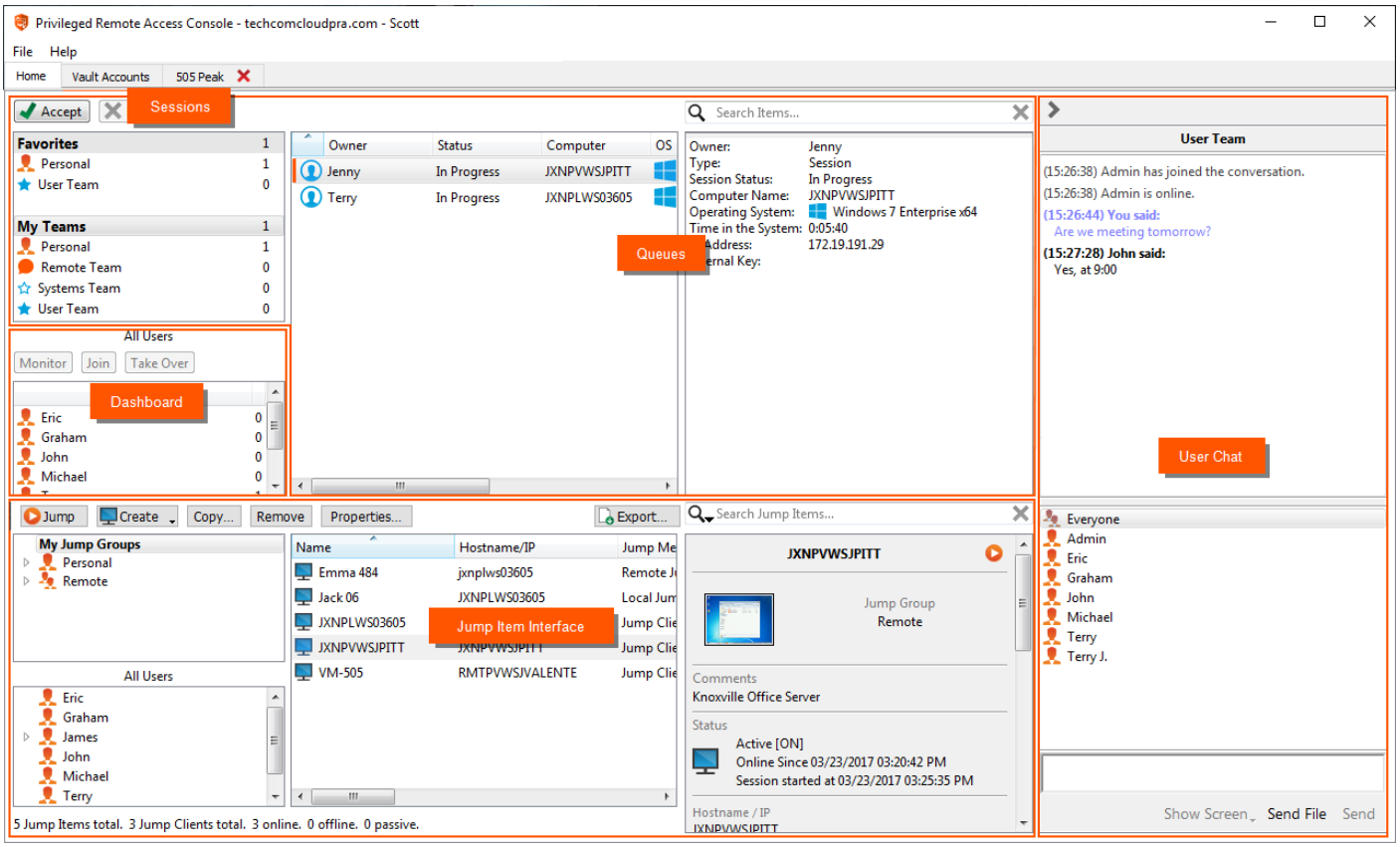
> ***Hinweis:*** *Um sich mit einem bereits verwendeten Konto anzumelden und die Verbindung auf dem anderen System zu schließen, muss die Einstellung* ***Sitzung abbrechen, wenn Konto verwendet wird*** *auf der Seite* ***/login > Verwaltung > Sicherheit*** *aktiviert werden.*

Nach einem Upgrade oder bei der ersten Inbetriebnahme der Desktop-access console wird bei allen nicht eingeladenen Support-Technikern nach der Anmeldung automatisch das Dialogfenster **Was ist neu?** angezeigt. Dieses Dialogfenster kann jederzeit über das **Hilfe**menü (**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 Benutzer anmeldet, nur ein einziges Mal angezeigt.

Weitere Informationen finden Sie hier:

- *Wie Sie die Anmeldungsvereinbarung einrichten, aktivieren oder deaktivieren können, erfahren Sie unter Website-Konfiguration: HTTP-Ports festlegen, Erforderliche Anmeldungsvereinbarung aktivieren unter https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/site-configuration.htm*
- *Für eingeladene Benutzer, Einladen eines externen Benutzers zur Teilnahme an einer Zugriffssitzung unter https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/access-invite.htm*

contiAccess-Benutzerschnittstelle der Konsole



Sitzungen: Verwalten Sie mehrere Remote-Sitzungen gleichzeitig.

Warteschlangen: Warteschlangen listen aktuell ausgeführte Sitzungen sowie Anforderungen zur Sitzungsfreigabe für Teammitglieder auf. In diesem Abschnitt werden Details zum Remote-System angezeigt.

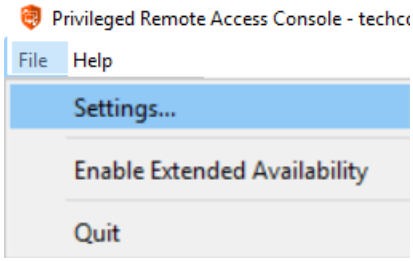
Dashboard: Mit dem Dashboard können berechtigte Benutzer laufende Sitzungen und Teammitglieder einer niedrigeren Rolle anzeigen und überwachen, wodurch sie eine administrative Aufsichtsfunktion einnehmen und Personal besser unterstützen können.

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

Benutzer-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 Zugriffskonsole ändern

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



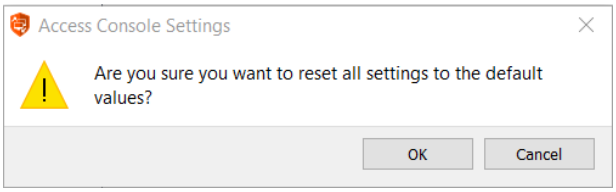
Allgemein können Sie die Einstellungen für die Konsole ensprechend Ihren Wünschen konfigurieren. Ihr BeyondTrust-Administrator kann jedoch entscheiden, die Verwaltung Ihrer Einstellungen zu übernehmen und diese verwalteten Einstellungen falls erwünscht zu erzwingen.

Wenn Ihr BeyondTrust-Administrator die Standardeinstellungen geändert und übernommen hat, erhalten Sie eine Benachrichtigung, 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 auf **OK**, um die Änderungen zu akzeptieren.

Einstellungen ändern

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 bitte an Ihren Administrator oder lesen Sie den Abschnitt Einstellungen der access console im Benutzerhandbuch für Administratoren für weitere Informationen.

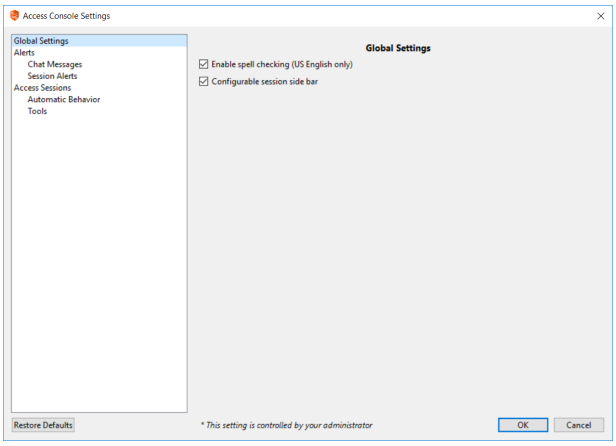
Das Fenster für die **Access Console Einstellungen** umfasst eine Schaltfläche **Auf Standardeinstellungen zurücksetzen**, mit der all Ihre Einstellungen auf die BeyondTrust-Standardeinstellungen oder die von Ihrem Administrator festgelegten Standardeinstellungen (falls zutreffend) zurückgesetzt werden. 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 Rechtschreibkorrektur für den Chat aktivieren oder deaktivieren. Derzeit steht die Rechtschreibprüfung nur für US-Englisch zur Verfügung.

Wählen Sie, ob das Sitzungsmenüsymbol 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.

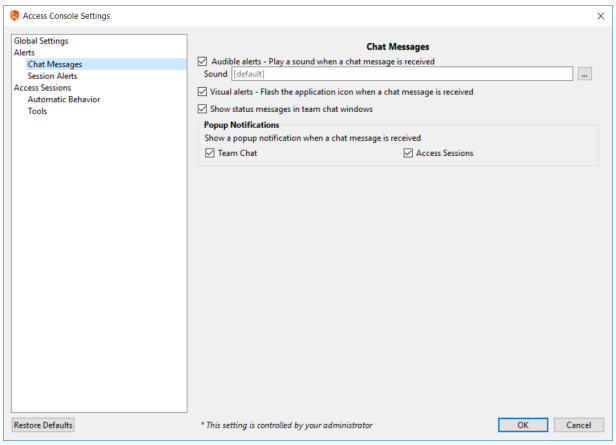


Wählen Sie Ihre Warneinstellungen für Chat-Nachrichten. Beim Erhalt einer Chat-Nachricht können Sie wählen, ob ein Sound ertönen und das Anwendungssymbol aufblinken soll.

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.

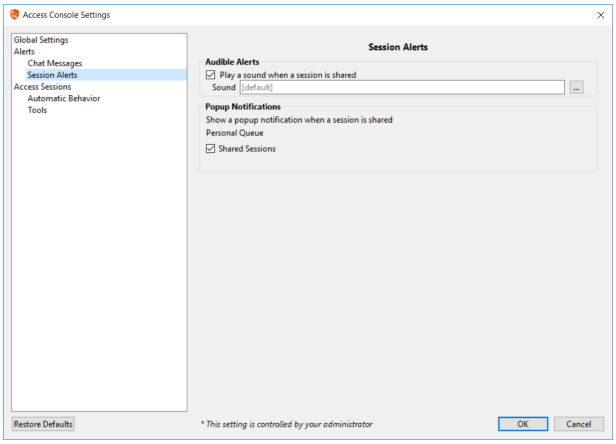
Wählen Sie, ob der Team-Chat Statusnachrichten wie die An- und Abmeldung von Benutzern enthalten soll oder nur zwischen Teammitgliedern gesendete Chatnachrichten.

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



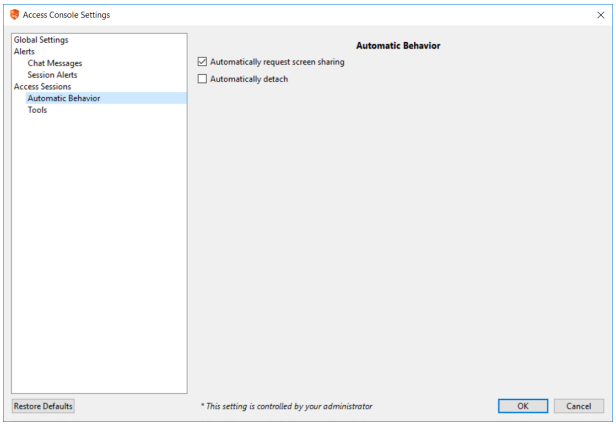
Wählen, Sie ob Sie einen hörbaren Alarm wünschen, wenn ein anderer Benutzer die Freigabe einer Sitzung mit Ihnen anfordert. Wenn Sie eine benutzerdefinierte Sounddatei für freigegebene Sitzungen hochladen möchten, klicken Sie auf die Schaltfläche **[...]** und wählen Sie eine WAV-Datei auf Ihrem Computer aus. Die Datei darf nicht größer als 1 MB sein.

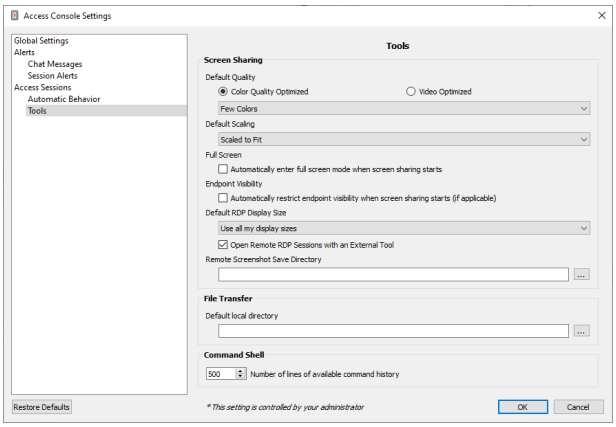
Sie können auch Popup-Hinweise für gewisse Ereignisse erhalten. Diese Hinweise werden unabhängig von Ihrer Konsole und im Vordergrund vor anderen Fenstern angezeigt. Stellen Sie ein, wo und wie lange diese Popups angezeigt werden sollen.



Wählen Sie, ob Sie zu Beginn einer Sitzung automatisch mit der Bildschirmfreigabe beginnen möchten.

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





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 PRA-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.

Wenn Sie Ihr eigenes RDP-Werkzeug verwenden möchten, aktivieren Sie **Öffnen von Remote-RDP-Sitzungen mit einem externen Tool**.

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.

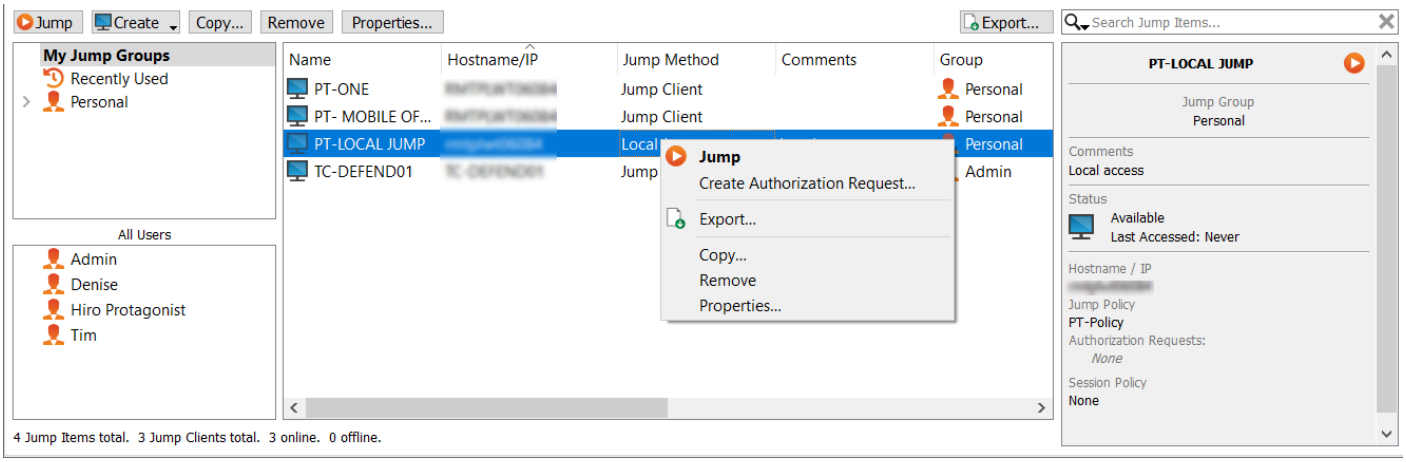
Legen Sie die Anzahl der Zeilen fest, die im Befehlsshellverlauf gespeichert werden sollen.

Jump-Schnittstelle: Verwenden von Jump-Elementen zum Zugriff auf Remote-Systeme

Die Jump-Schnittstelle erscheint in der unteren Hälfte der access console und listet die Ihnen zur Verfügung stehenden Jump-Elemente auf. Die Liste kann sowohl aktive als auch passive Jump Clients sowie Jump-Verknüpfungen für Remote-Jumps, lokale Jumps, RDP-Sitzungen, VNC-Sitzungen, Protokoll-Tunnel-Jumps, Shell Jumps und Web Jumps enthalten.

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



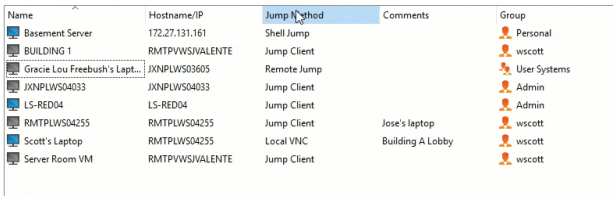
Jump-Elemente kopieren

Jump-Items können kopiert werden und können zu mehreren Jump-Gruppen gehören. Dies umfasst Jump-Client-Elemente und bietet Administratoren die Möglichkeit, separate Richtlinien und Gruppenberechtigungen festzulegen, ohne dass eine zusätzliche Jump-Client-Installation auf dem Ziel-Endpunkt erforderlich ist. Benutzer mit den entsprechenden Berechtigungen sehen die Option zum **Kopieren** von Jump-Items im Access Console, indem sie mit der rechten Maustaste auf das Item klicken. Benutzer können diese Funktion auch für mehrere Jump-Items ausführen.

Diese Funktion ermöglicht es Administratoren und Benutzern, verschiedene Richtlinien für Jump-Items und Jump-Clients effektiv zu verwalten, ohne ein neues Jump-Item erstellen zu müssen. Diese Funktion ermöglicht es Benutzern, die Anzahl der Clients zu begrenzen, die zum Aktivieren von Jump-Client-Sitzungen erforderlich sind, und begrenzt die manuellen Verwaltungsaufgaben beim Definieren von Zugriffspfaden für Benutzer.

Jump zu einem Jump-Element durchführen

Durchsuchen Sie Gruppen nach dem Computer, auf den Sie zugreifen möchten. Um das Durchsuchen der Liste der Jump-Elemente zu erleichtern, können Sie die Spalten in jeder beliebigen Reihenfolge verschieben und eine Spalte dann durch Anklicken der Spaltenüberschrift sortieren. Die access console merkt sich die Reihenfolge der Spalten und die Sortierreihenfolge für das nächste Mal, wenn die access console gestartet wird.



Neben dem Suchen nach Jump-Elementen können Sie auch basierend auf mehreren Feldern suchen. Geben Sie eine Zeichenfolge in das Suchfeld ein und drücken Sie 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.

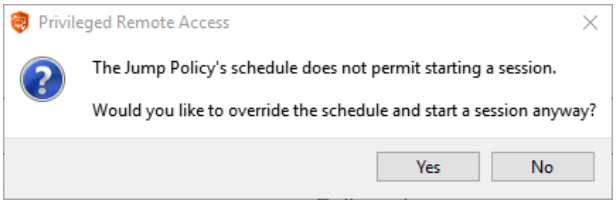
Eine Programm-Verbindung zum Jump-Element kann direkt vom Verwaltungs- oder Ticket-Tool Ihres Systems aus hergestellt werden. Wenn Ihre Suchanfrage nur ein Jump-Element aufweist, wird die Sitzung sofort gestartet. Wenn die Suchanfrage mehrere Jump-Elemente aufweist, können Sie ein Jump-Element aus der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

> ***Hinweis:*** *Einzelheiten zu Skripting finden Sie unter Access ConsoleSkripting für Zugriffskonsole und Client-Skripting-API unter www.beyondtrust.com/docs/privileged-remote-access/how-to/integrations/api/client-script.*

Wird eine Jump-Richtlinie auf das Jump-Element angewandt, beeinflusst diese Richtlinie, wie und/oder wann auf ein Jump-Element zugegriffen werden kann.

Planen

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



Benachrichtigung

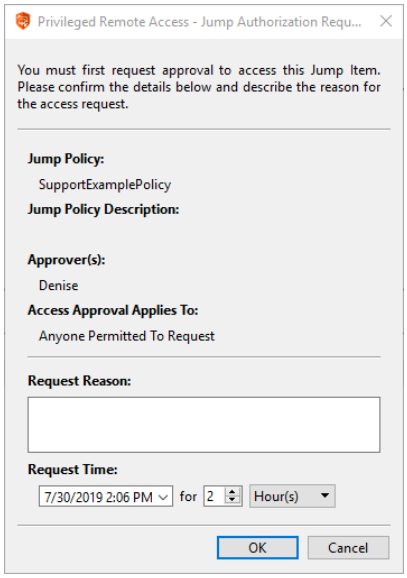
Ist eine Jump-Richtlinie darauf konfiguriert, beim Sitzungsstart oder -ende eine Benachrichtigung zu senden, unterrichtet Sie der Zugriff auf ein Jump-Element darüber, dass eine E-Mail gesendet wird. Sie können mit dem Jump fortfahren und eine Benachrichtigung senden lassen, oder den Jump abbrechen.

Ticket-ID

Wenn eine Jump-Richtlinie die Eingabe einer Ticket-ID Ihres externen ITSM oder Ticket-ID-Systems benötigt, bevor der Jump durchgeführt werden kann, wird ein Dialogfenster geöffnet. Geben Sie im Dialogfeld die benötigte Ticket-ID ein, die Sie zum Zugriff auf dieses Jump-Element autorisiert.

Autorisierung

Wenn eine Jump-Richtlinie vor Durchführung eines Jumps eine Autorisierung erfordert, wird ein Dialogfenster geöffnet. Geben Sie im Dialogfeld den Grund für den Zugriff auf das Jump-Element ein. Geben Sie dann Datum und Uhrzeit für den Beginn der Autorisierung ein und wie lange Sie den Zugriff auf das Jump-Element erfordern. Sowohl der Anforderungsgrund als auch der Anforderungszeitpunkt sind für den Genehmiger sichtbar und helfen bei der Entscheidung, den Zugriff zu genehmigen oder abzulehnen.



Wenn Sie auf **OK** klicken, wird eine E-Mail an die Adressen gesandt, die als Genehmiger für diese Richtlinie definiert wurden. Diese E-Mail enthält eine URL, bei der ein Genehmiger die Anfrage sehen, Kommentare hinzufügen und die Anfrage entweder genehmigen oder ablehnen kann.

Wenn eine Anfrage von einer Person genehmigt wurde, kann eine andere Person auf die URL zugreifen, um die Genehmigung zurückzunehmen und die Anfrage abzulehnen. Wenn die Anfrage abgelehnt wurde, können andere darauf zugreifende Genehmiger die Details einsehen, die Ablehnung jedoch nicht aufheben. Wenn ein Benutzer bereits einer genehmigten Sitzung beigetreten ist, kann dieser Zugriff nicht entzogen werden. Obwohl andere Genehmiger die E-Mail-Adresse der genehmigenden oder ablehnenden Person sehen können, kann der Anforderer dies nicht. Basierend auf den Einstellungen der Jump-Richtlinie gewährt eine genehmigte Anforderung den Zugriff entweder jedem Benutzer, der diesen Jump Client sehen und den Zugriff anfordern kann, oder nur dem Benutzer, der den Zugriff angefordert hat.

In der Jump-Schnittstelle zeigt das Fenster „Details“ des Jump-Elements den Status von Autorisierungsanforderungen entweder als ausstehend, genehmigt, nur genehmigt für einen anderen Benutzer, oder abgelehnt an. Wenn ein Genehmiger auf eine Anfrage antwortet, erscheint eine Popup-Meldung auf dem Bildschirm des Anfordernden und benachrichtigt diesen über die Genehmigung oder Ablehnung des Zugriffs. Wenn der Anfordernde eine konfigurierte E-Mail-Adresse besitzt, wird ebenfalls eine E-Mail-Benachrichtigung an den Anfordernden gesandt.

Wenn ein Benutzer einen Jump zu einem Jump-Element durchgeführt, das zum Zugriff genehmigt wurde, benachrichtigt eine Meldung den Benutzer über vom Genehmiger hinterlassene Kommentare.

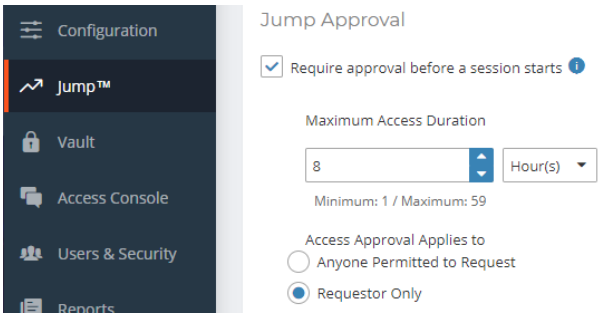
Wenn die Genehmigung für ein Jump-Element gewährt wurde, wird das Jump-Element entweder für jeden Benutzer verfügbar, der dieses Jump-Element sehen und den Zugriff anfordern kann, oder nur für den Benutzer, der den Zugriff angefordert hat. Dies wird durch die Jump-Richtlinie bestimmt.

> ***Hinweis:*** *Es können mehrere Anfragen zu unterschiedlichen Zeiten gesendet werden, aber die angeforderten Zugriffszeiten dürfen sich nicht überschneiden. Wird eine Anfrage abgelehnt, kann für die gleiche Zeit eine weitere Anfrage gesendet werden.*

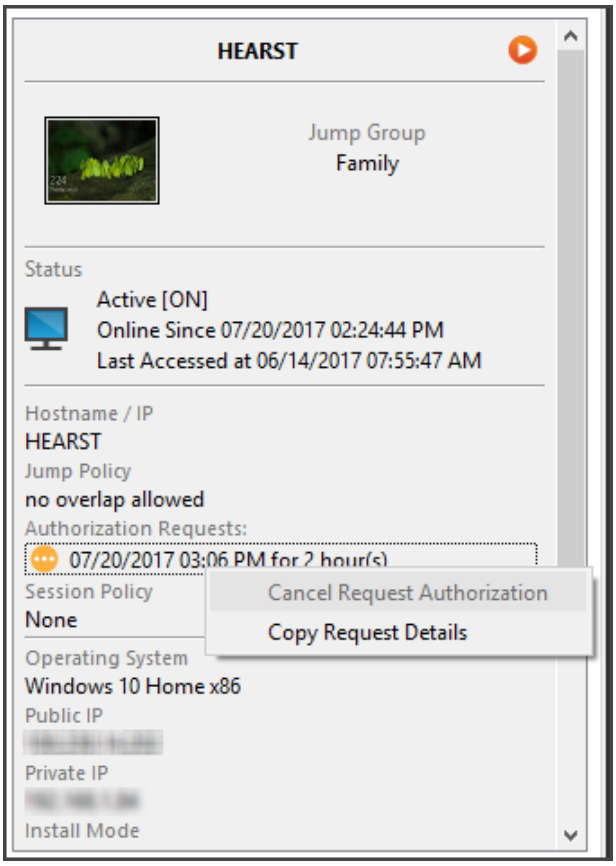
Widerruf einer Zugriffs-Genehmigungsanfrage

Die Berechtigung, genehmigte Zugriffsanforderungen zu widerrufen, wird durch die Jump-Richtlinie geregelt. Gehen Sie in der Web-Verwaltungsschnittstelle **/login** auf **Jump > Jump-Richtlinien**. Unter **Jump-Genehmigung** haben Sie zwei Optionen:

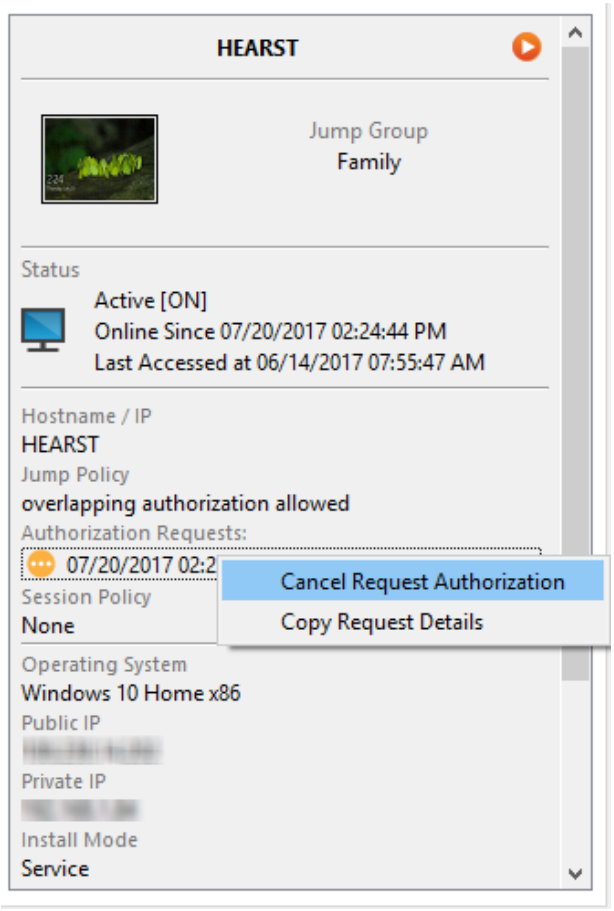
- **Jeden, der anfordern darf**
- **Nur Anforderer**



Wenn die Jump-Richtlinie auf **Nur Anforderer** eingestellt ist und eine Zugriffsanforderung derzeit für Benutzer A genehmigt ist, wird Benutzer B aufgefordert, eine neue Zugriffsanforderung zu erstellen, wenn er versucht, einen Jump zu dem Jump-Item durchzuführen, da diese Anforderung nicht für ihn gilt. Wenn Benutzer B außerdem versucht, die Zugriffs-Genehmigungsanforderung zu stornieren, wird die Option ausgegraut. Der einzige Benutzer, der die genehmigte Anforderung stornieren kann, ist Benutzer A, da er der genehmigte Benutzer für die Anforderung ist.



Wenn die Jump-Richtlinie jedoch auf **Jeder mit Anforderungsberechtigung** eingestellt ist und eine Zugriffsanforderung derzeit für Benutzer A genehmigt ist, ist Benutzer B berechtigt, eine neue Sitzung mit dem Jump-Item zu starten, wenn er versucht, einen Jump zu ihm durchzuführen. Außerdem kann jeder, der eine Zugriffsberechtigung auf das Jump-Item hat, die Anforderung abbrechen/widerrufen.



Verwenden von Jump Clients zum Zugriff auf Remote-Endpunkte

Um auf einen einzelnen Windows-, Mac- oder Linux-Computer zuzugreifen, der sich nicht in einem zugänglichen Netzwerk befindet, installieren Sie einen Jump-Client auf diesem System über die Seite **/login > Jump > Jump-Clients**. Jump Clients erscheinen in der Jump-Schnittstelle zusammen mit anderen symbolischen Jump-Element-Links.

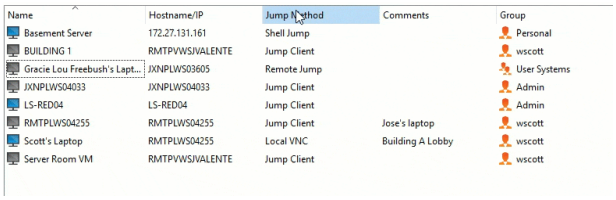
Verwenden eines Jump Clients

Um einen Jump-Client zum Start einer Sitzung zu verwenden, wählen Sie den Jump-Client aus der Jump-Schnittstelle und klicken Sie auf die Schaltfläche **Jump**.

> ***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/privileged-remote-access/getting-started/admin/jump-items.htm.*

Sortieren von Jump-Clients

Durchsuchen Sie Gruppen nach dem Computer, auf den Sie zugreifen möchten. Um das Durchsuchen der Liste der Jump-Elemente zu erleichtern, können Sie die Spalten in jeder beliebigen Reihenfolge verschieben und eine Spalte dann durch Anklicken der Spaltenüberschrift sortieren. Die access console merkt sich die Reihenfolge der Spalten und die Sortierreihenfolge für das nächste Mal, wenn die access console gestartet wird.



Suche eines Jump-Clients

Neben dem Suchen nach Jump-Elementen können Sie auch basierend auf mehreren Feldern suchen. Geben Sie eine Zeichenfolge in das Suchfeld ein und drücken Sie 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 B Series 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 erscheint 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)

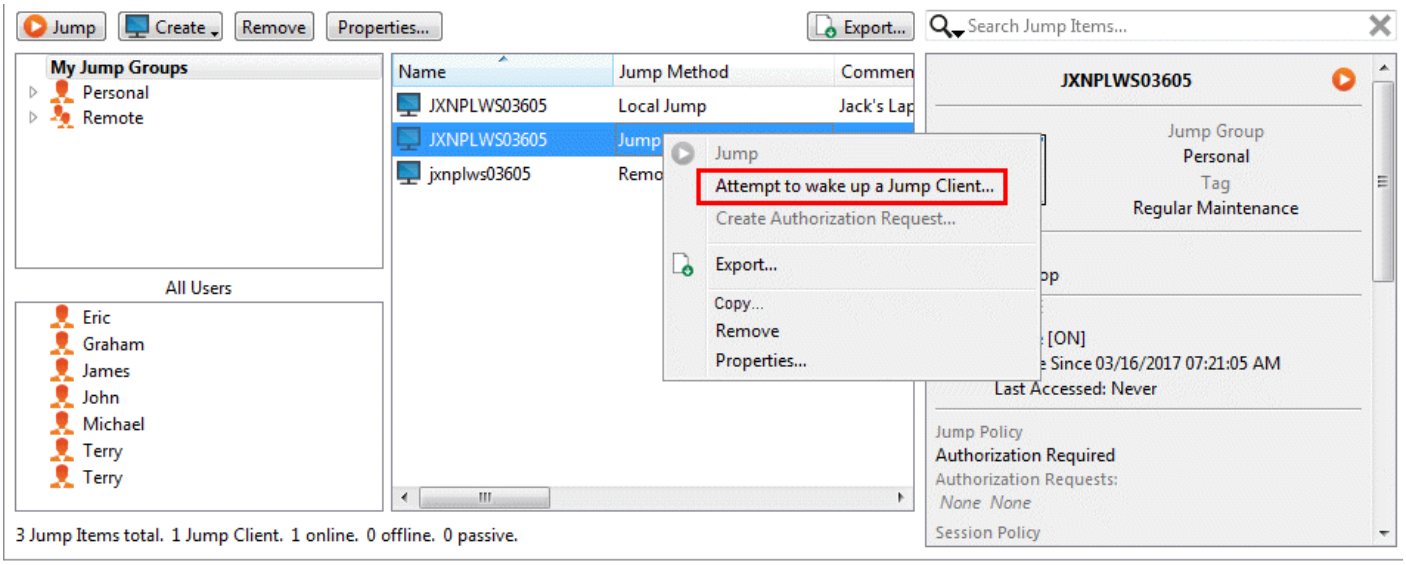
Wake-on-Lan (WOL) ermöglicht es Ihnen, für WOL konfigurierte Systeme über BeyondTrust per Remote-Zugriff einzuschalten oder aufzuwecken. In einer konfigurierten Umgebung können Kunden ihre Systeme ausschalten, aber gegebenenfalls noch immer BeyondTrust-Support erhalten.

> ***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 des Support-Technikers unterstützen WOL nicht.

Um einen aktiven Jump-Client mit WOL aufzuwecken, rechtsklicken Sie in der Konsole des 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 B Series Appliance. Das B Series Appliance 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 des Support-Technikers online geht.

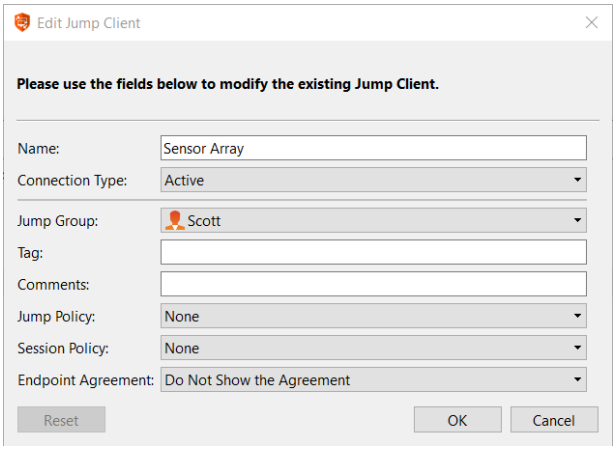
Jump-Elemente kopieren

Jump-Items können kopiert werden und können zu mehreren Jump-Gruppen gehören. Dies umfasst Jump-Client-Elemente und bietet Administratoren die Möglichkeit, separate Richtlinien und Gruppenberechtigungen festzulegen, ohne dass eine zusätzliche Jump-Client-Installation auf dem Ziel-Endpunkt erforderlich ist. Benutzer mit den entsprechenden Berechtigungen sehen die Option zum **Kopieren** von Jump-Items im Access Console, indem sie mit der rechten Maustaste auf das Item klicken. Benutzer können diese Funktion auch für mehrere Jump-Items ausführen.

Diese Funktion ermöglicht es Administratoren und Benutzern, verschiedene Richtlinien für Jump-Items und Jump-Clients effektiv zu verwalten, ohne ein neues Jump-Item erstellen zu müssen. Diese Funktion ermöglicht es Benutzern, die Anzahl der Clients zu begrenzen, die zum Aktivieren von Jump-Client-Sitzungen erforderlich sind, und begrenzt die manuellen Verwaltungsaufgaben beim Definieren von Zugriffspfaden für Benutzer.

Jump-Client-Eigenschaften

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 (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.

Ändern Sie den Modus eines Jump-Client über das Dropdown-Menü **Verbindungstyp**. Aktive Jump-Clients senden in definierten Zeitabständen Statistiken an das B Series Appliance. Passive Jump-Clients senden einmal täglich oder nach einem manuellen Check-in Statistiken an das B Series Appliance.

> ***Hinweis:*** *Diese Funktion ist nur für Kunden verfügbar, die ein B Series Appliance an ihrem Standort betreiben. BeyondTrust Cloud-Kunden haben keinen Zugriff auf diese Funktion.*

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.

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.

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 Benutzer auf dieses Jump-Element zugreifen können, ob eine Zugriffsbenachrichtigung gesendet werden sollte oder ob eine Berechtigung oder eine Ticket-ID Ihres externen Ticketsystems zur Verwendung dieses Jump-Elements notwendig ist, wählen Sie **Jump-Richtlinie**. Diese Richtlinien werden von Ihrem Administrator über die /login-Schnittstelle festgelegt.

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

Wählen Sie eine **Endpunkt-Vereinbarung**, die diesem Jump-Element zugewiesen werden soll. Abhängig von der Auswahl wird eine Endpunkt-Vereinbarung angezeigt. Gibt es keine Antwort, wird die Vereinbarung automatisch akzeptiert oder abgelehnt.

Wenn Sie den Zugriff auf ein Remote-System nicht länger benötigen, wählen Sie das Jump-Element und klicken Sie auf die Schaltfläche **Entfernen** oder rechtsklicken Sie auf das Jump-Element und wählen Sie **Entfernen** aus dem Menü. Sie können mehrere Jump-Elemente 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 access console entfernt. Wenn der Jump-Client das B Series Appliance zum Deinstallationszeitpunkt nicht kontaktieren kann, verbleibt das betroffene Element im Offline-Zustand. Diese Einstellung ist unter* ***/login > Jump > Jump-Clients*** *verfügbar. Wenn ein Jump Client offline geht und sich 180 Tage lang nicht erneut mit dem B Series Appliance verbindet, wird er automatisch vom Zielcomputer deinstalliert und aus der Jump-Schnittstelle entfernt.*

Verwenden von Remote-Jump für den unüberwachten Zugriff auf Computer in einem separaten Netzwerk

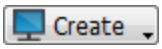
Remote-Jump ermöglicht es einem berechtigten Benutzer, sich mit einem unüberwachten Remote-Computer in einem Netzwerk außerhalb des eigenen Netzwerkes zu verbinden. Remote-Jump ist von einem Jumpoint abhängig.

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.

> ***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. Sie können keinen Jump auf ein mobiles Gerät durchführen, obwohl Jump-Technologie über mobile BeyondTrust-Konsolen verfügbar ist.*

Symbolischen Jump-Link (Remote) erstellen

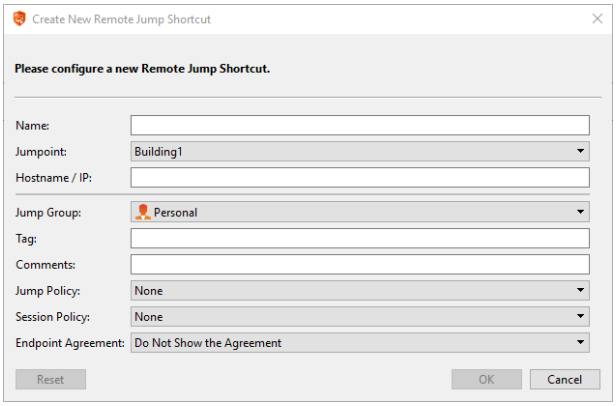
Um einen symbolischen Jump-Link (Remote) zu erstellen, klicken Sie auf die Schaltfläche **Erstellen** in der Jump-Schnittstelle. Wählen Sie aus der Dropdown-Liste **Remote-Jump**. Symbolische Jump-Links (Remote) erscheinen in der Jump-Schnittstelle zusammen mit Jump-Clients und anderen Arten von symbolischen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

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 Benutzer auf dieses Jump-Element zugreifen können, ob eine Zugriffsbenachrichtigung gesendet werden sollte oder ob eine Berechtigung oder eine Ticket-ID Ihres externen Ticketsystems zur Verwendung dieses Jump-Elements notwendig ist, wählen Sie **Jump-Richtlinie**. Diese Richtlinien werden von Ihrem Administrator über die /login-Schnittstelle festgelegt.

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

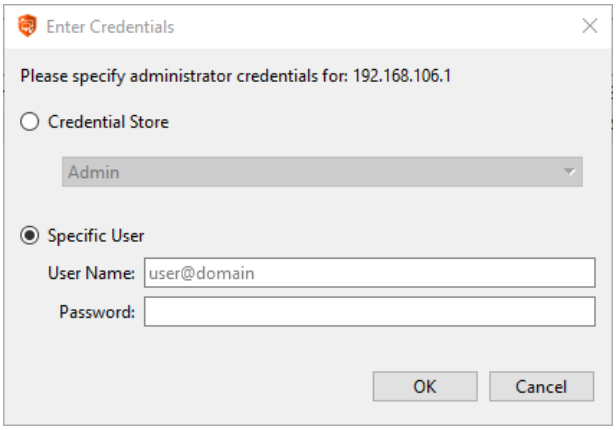
Wählen Sie eine **Endpunkt-Vereinbarung**, die diesem Jump-Element zugewiesen werden soll. Abhängig von der Auswahl wird eine Endpunkt-Vereinbarung angezeigt. Gibt es keine Antwort, wird die Vereinbarung automatisch akzeptiert oder abgelehnt.

Symbolischen Jump-Link (Remote) 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 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.



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/privileged-remote-access/getting-started/admin/jump-items.htm.*

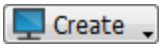
Verwenden Sie lokale Jumps für den unüberwachten Zugriff auf Computern in Ihrem lokalen Netzwerk

Lokaler Jump berechtigt einen Benutzer dazu, sich mit einem unüberwachten Remote-Computer im lokalen Netzwerk zu verbinden. Innerhalb des lokalen Netzwerks kann der Computer eines BeyondTrust-Benutzers eine Sitzung mit einem Windows-System direkt ohne Verwendung eines Jumpoint initiieren, falls die geeigneten Benutzerberechtigungen aktiviert wurden. Ein Jumpoint wird nur notwendig, wenn der Computer des BeyondTrust-Benutzers nicht direkt auf den Zielcomputer zugreifen kann.

> ***Hinweis:*** *Lokaler Jump ist 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.*

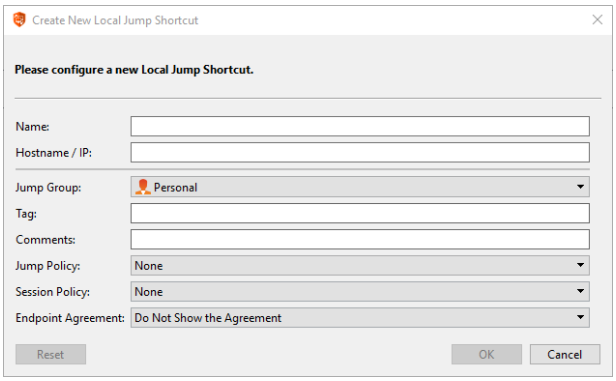
Symbolischen Jump-Link (lokal) erstellen

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 (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.

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 Benutzer auf dieses Jump-Element zugreifen können, ob eine Zugriffsbenachrichtigung gesendet werden sollte oder ob eine Berechtigung oder eine Ticket-ID Ihres externen Ticketsystems zur Verwendung dieses Jump-Elements notwendig ist, wählen Sie **Jump-Richtlinie**. Diese Richtlinien werden von Ihrem Administrator über die /login-Schnittstelle festgelegt.

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

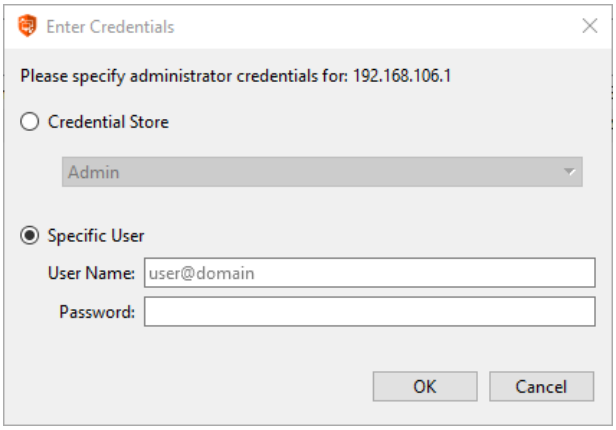
Wählen Sie eine **Endpunkt-Vereinbarung**, die diesem Jump-Element zugewiesen werden soll. Abhängig von der Auswahl wird eine Endpunkt-Vereinbarung angezeigt. Gibt es keine Antwort, wird die Vereinbarung automatisch akzeptiert oder abgelehnt.

Symbolischen Jump-Link (lokal) 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 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.



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/privileged-remote-access/getting-started/admin/jump-items.htm.*

RDP zum Zugriff auf einen Remote Windows-Endpunkt

Verwenden Sie BeyondTrust, um eine Remote-Desktop-Protokoll (RDP)-Sitzung mit Remote-Windows- und -Linux-Systemen zu starten. Da RDP-Sitzungen per Proxy durch einen Jumpoint geleitet und 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 über BeyondTrust nutzen zu können, benötigen Sie Zugriff auf einen Jumpoint sowie die Benutzerkontoberechtigung **Gestattete Jump-Methoden: RDP über einen Jumpoint**.

Sie können Ihr eigenes RDP-Werkzeug für Remote-RDP-Sitzungen verwenden. Weitere Informationen finden Sie in Einstellungen und Voreinstellungen in der Zugriffskonsole ändern unter https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/settings.htm.

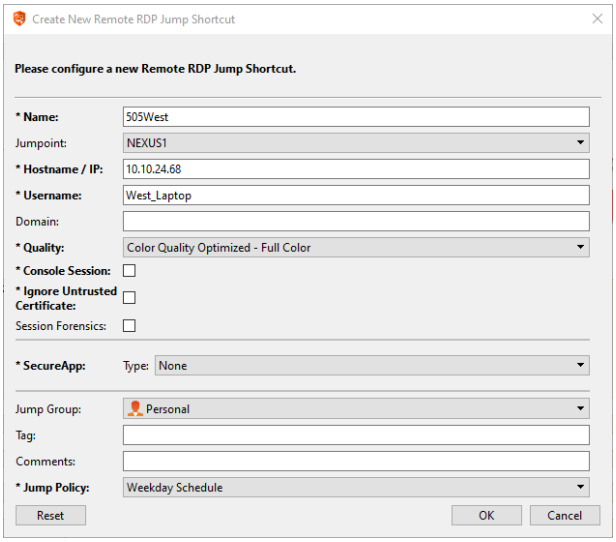
Symbolischen RDP-Link erstellen

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

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 Remote-Desktop-Protokoll (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 **Schwarzweiß** (weniger Bandbreite), **Wenige Farben**, **Mehr Farben** oder **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.

> ***Hinweis:*** *Wenn der Remote-App- oder Remote Desktop Agent von BeyondTrust im Bereich SecureApp gewählt wurde, wird das Kontrollkästchen* ***Konsolensitzung*** *deaktiviert. Remote-Anwendungen können nicht in einer Konsolensitzung auf einem RDP-Server ausgeführt werden.*

Ausführlichere Daten zur RDP-Sitzung finden Sie in **Sitzungsforensik**. Damit diese Funktion genutzt werden kann, müssen Sie für die Dauer der Verwendung des Jumpoints ein **RDP-Service-Konto** auswählen. Wenn Sie diese Einstellung aktivieren, wird folgende Erinnerung angezeigt:

Wird diese Funktion aktiviert, muss der RDP-Server so konfiguriert werden, dass er den Überwachungsagenten empfängt, und ein RDP-Servicekonto muss für diesen Jumpoint eingerichtet werden. Werden diese Voraussetzungen nicht erfüllt, schlagen alle Versuche, eine Sitzung zu starten, fehl.

Wenn **Sitzungsforensik** aktiviert ist, werden folgende zusätzliche Details aufgezeichnet:

- Fokussiertes Fensteränderungsereignis
- Mausklick-Ereignis
- Menüöffnungs-Ereignis
- Neues Fensteröffnungsereignis

Um eine Sitzung mit einer Remote-Anwendung zu starten, konfigurieren Sie den Bereich **SecureApp**. Die folgenden Dropdown-Optionen sind verfügbar:

- **Ohne:** Beim Zugriff auf ein Remote-RDP-Jump-Element wird keine Anwendung gestartet.
- **Remote-App:**Der Benutzer kann ein Anwendungsprofil oder Befehlsargument konfigurieren, das eine Anwendung auf einem Remote-Server startet. Wählen Sie zur Konfiguration die Option **Remote-App** und geben Sie die folgenden Informationen ein.
  - **Name der Remote-App:** Geben Sie den Namen der Anwendung ein, mit der Sie sich verbinden möchten.
  - **Parameter der Remote-App:** Geben Sie die Profildetails oder Befehlszeilenargumente ein, die für den Start der Anwendung erforderlich sind.
- **BeyondTrust Remote Desktop Agent:** Mit dieser Option können Parameter durch einen Agenten geleitet werden, um Anwendungen auf einem Remote-Host zu starten. Wählen Sie zur Konfiguration die Option **BeyondTrustRemote Desktop Agent** und geben Sie die folgenden Informationen ein:
  - **Ausführbarer Pfad:** Geben Sie den Pfad der Anwendung ein, mit dem der Agent sich verbinden wird.
  - **Parameter:** Geben Sie alle Parameter ein, die Sie normalerweise in einer Befehlszeile eingeben würden, wenn Sie die App im Remote-System starten.

> *Weitere Informationen zur Sitzungsforensik und zum RDP-Service-Konto finden Sie in Jumpoint: Einrichten des unüberwachten Zugriffs auf ein Netzwerk > RDP-Service-Konto unter https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/jumpoint.htm.*

Anmeldedaten einfügen

Die Option **Anmeldedaten einfügen** wird verfügbar, wenn der **BeyondTrustRemote Desktop Agent** ausgewählt wird. Mit dieser Option können Parameter sowie Anmeldedaten durch einen Agenten geleitet werden, um Anwendungen auf einem Remote-Host zu starten. Der erste Anmeldedaten-Satz befindet sich in der Jump-Definition. Dabei handelt es sich um die Anmeldedaten für das Benutzerkonto, das Sie für die Anmeldung im Remote-System verwenden werden. Es wird eine zweite Eingabeaufforderung für zusätzliche Anmeldedaten

angezeigt, die entweder manuell oder über einen Kennwort-Vault eingegeben werden müssen. Diese sekundären Anmeldedaten, die von Ihnen über die Makros %USERNAME% und %PASSWORD% definiert wurden (weitere Makros werden unten angezeigt), werden auf der Befehlszeile verfügbar gemacht. So können Sie zusätzliche Anmeldedaten an die von Ihnen gestartete Anwendung leiten (z. B. SQL Server Management Studio). Wählen Sie zur Konfiguration die Option **BeyondTrustRemote Desktop Agent** und geben Sie die folgenden Informationen ein:

- Geben Sie den **Ausführbaren Pfad** und die **Parameter** wie oben beschrieben ein.
- **Zielsystem:** Geben Sie den Namen des Systems ein, auf dem die Anwendung ausgeführt wird.
- **Art der Anmeldedaten:** Geben Sie den Anmeldedaten-Typ wie im Anmeldedaten-Verwaltungssystem definiert ein (z. B. SQL).

Name des Makros	Ergebnis
%USERNAME%	Benutzername
%USERPRINCIPLENAME%	nutzername@domäne
%DOWNLEVELLOGONNAME%	domain\username
%DOMAIN%	domäne
%PASSWORD%	kennwort
%PASSWORDRAW%	Kennwort (ohne Versuch, Sonderzeichen auszulassen)
%TARGETSYSTEM%	angegebener Zielsystemwert; im Fall von SQL Server wäre dies der SQL-Servername.
%APPLICATIONNAME%	optionaler Anwendungsname; im Fall von SQL Server kann dies auf „SQL Server“ oder ähnlich fest kodiert werden.

Hinweis: *Für die Option* ***BeyondTrust Remote Desktop Agent*** *muss ein* ***BeyondTrustRemote Desktop Agent*** *im Zielsystem vorkonfiguriert sein. Diesr Agent kann auf der Seite* ***Mein Konto*** *in der* ***/login****-Schnittstelle heruntergeladen weden. Der Agent ist weder versions- noch website-spezifisch, daher kann sein Name für so viele Anwendungen verwendet werden, wie der Administrator unterstützen möchte. Sobald der Agent installiert ist, können Sie mit BeyondTrustRDP-Jump-Elemente erstellen, die für die Nutzung der Option Remote Desktop Agent von BeyondTrust zum Starten einer beliebigen auf dem Remote-System installierten Anwendung konfiguriert sind.*

Hinweis: *SecureApp fußt auf der Veröffentlichung von Anwendungen mit Microsoft RDS RemoteApps. Bitte beziehen Sie sich auf die Microsoft-Dokumentation für die Veröffentlichung von Anwendungen.*

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.

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.

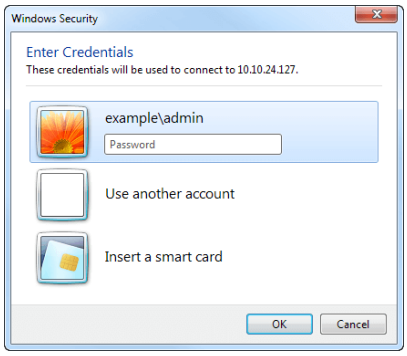
Um festzulegen, wann Benutzer auf dieses Jump-Element zugreifen können, ob eine Zugriffsbenachrichtigung gesendet werden sollte oder ob eine Berechtigung oder eine Ticket-ID Ihres externen Ticketsystems zur Verwendung dieses Jump-Elements notwendig ist, wählen Sie **Jump-Richtlinie**. Diese Richtlinien werden von Ihrem Administrator über die /login-Schnittstelle festgelegt.

Für weitere Informationen über enthaltene Datenbankbenutzer lesen Sie weiter unter Enthaltene Datenbankbenutzer - So machen Sie Ihre Datenbank portabel unter docs.microsoft.com/en-us/sql/relational-databases/security/contained-database-users-making-your-database-portable.

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 Remote-Desktop-Protokoll (RDP)-Sitzung.

***Hinweis:** Beim Starten einer RDP-Sitzung entspricht die RDP-Tastatur automatisch der in der Zugriffskonsole gewählten Sprache. Diese Funktion ist nur für Windows-basierte Zugriffskonsolen verfügbar.*

Beginnen Sie mit der Bildschirmfreigabe, um den Remote-Desktop anzuzeigen. Sie können den Befehl Strg+Alt+Entf senden, einen Screenshot des Remote-Desktops aufnehmen, Inhalte der Zwischenablage freigeben und eine Schlüsseleinfügung vornehmen. Außerdem können Sie die RDP-Sitzung für andere angemeldete BeyondTrust-Benutzer freigeben, wobei dies den normalen Regeln Ihrer Benutzerkontoeinstellungen unterliegt.

***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/privileged-remote-access/getting-started/admin/jump-items.htm.*

VNC zum Zugriff auf einen Remote Windows-Endpunkt

Verwenden Sie BeyondTrust, um eine VNC-Sitzung mit einem Remote-Windows-System zu starten. Da VNC-Sitzungen per Proxy durch einen Jumpoint geleitet und 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 VNC über BeyondTrust nutzen zu können, benötigen Sie Zugriff auf einen Jumpoint sowie die Benutzerkontoberechtigung **Gestattete Jump-Methoden: Remote-VNC über einen Jumpoint**.

Einen neuen symbolischen VNC-Link erstellen

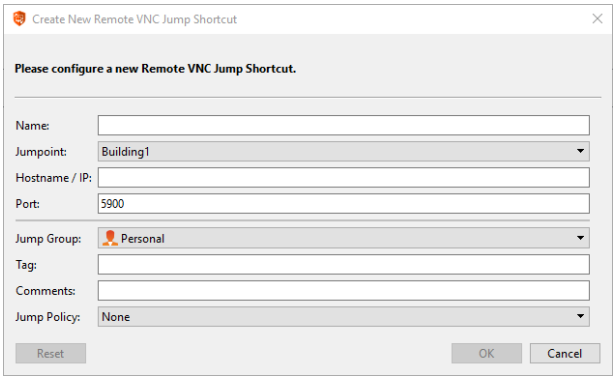
Um einen symbolischen VNC-Link zu erstellen, klicken Sie in der Jump-Schnittstelle auf die Schaltfläche **Erstellen**. Wählen Sie aus der Dropdown-Liste **Remote-VNC**. Symbolische VNC-Links erscheinen in der Jump-Schnittstelle zusammen mit Jump-Clients und anderen Arten von symbolischen Jump-Element-Links.

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

> ***Hinweis:*** *Um die Eigenschaften mehrerer Jump-Elemente anzuzeigen, müssen alle ausgewählten Elemente vom gleichen Typ sein (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 access console 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 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, fügen Sie diesen an den Hostnamen oder die IP-Adresse in der Form* ***<hostname>:<port>*** *oder* ***<ipaddress>:<port>*** *an (z.B.., 10.10.24.127:40000).*

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.

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 Benutzer auf dieses Jump-Element zugreifen können, ob eine Zugriffsbenachrichtigung gesendet werden sollte oder ob eine Berechtigung oder eine Ticket-ID Ihres externen Ticketsystems zur Verwendung dieses Jump-Elements notwendig ist, wählen Sie **Jump-Richtlinie**. 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, einen Screenshot des Remote-Desktops aufnehmen und Textinhalte der Zwischenablage freigeben. Ebenfalls können Sie die VNC-Sitzung freigeben, übertragen oder aufzeichnen, entsprechend der regulären Regeln Ihrer Benutzerkontoeinstellungen.

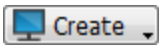
Hinweis: *Jump-Elemente können ebenfalls eingestellt werden, um den gleichzeitigen Zugriff auf das gleiche Jump-Element durch mehrere Benutzer zu gestatten. Wenn* ***Bestehender Sitzung beitreten*** *gewählt wurde, können andere Benutzer einer bereits laufenden Sitzung beitreten. Der ursprüngliche Sitzungseigentümer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

Verwenden Sie einen Protokoll-Tunnel-Jump, um eine TCP-Verbindung zu einem Remote-System aufzubauen

Verwenden Sie einen Protokoll-Tunnel-Jump, um eine TCP-Verbindung von Ihrem System zu einem Endpunkt an einem Remote-Netzwerk aufzubauen. Da die Verbindung über einen Jumpoint erfolgt, kann der Administrator steuern, welche Benutzer Zugriff haben, wann der Zugriff zur Verfügung stehen sollen, und ob Sitzungen aufgezeichnet werden sollen.

Erstellen eines symbolischen Protokoll-Tunnel-Jump-Links

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



> ***Hinweis:*** *Protokoll-Tunnel-Jump-Links werden nur aktiviert, wenn der Jumpoint auf der Seite* ***/login > Jump > Jumpoint*** *für die Protokoll-Tunnel-Jump-Methode konfiguriert wurde.*

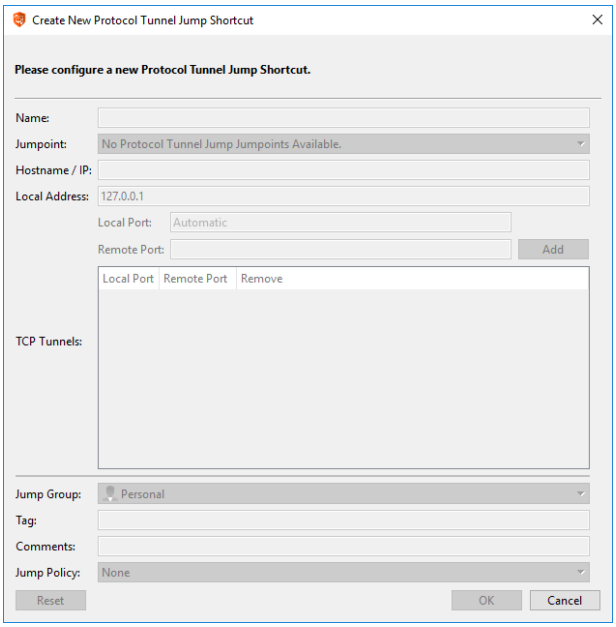
Geben Sie einen **Namen** für das Jump-Element ein. Dieser Name kennzeichnet das Element in den Sitzungsregisterkarten. Diese Zeichenkette kann maximal 128 Zeichen lang sein.

Wählen Sie im Dropdown-Menü **Jumpoint** das Netzwerk aus, in dem sich der Computer befindet, auf den Sie zugreifen möchten. Die access console 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.

Geben Sie eine **Lokale Adresse** an. Die Standardadresse lautet 127.0.0.1. Wenn Sie sich gleichzeitig mit mehreren Verbindungen am gleichen RemotePort verbinden müssen, können Sie diese Verbindung ermöglichen, indem Sie die Adresse jedes symbolischen Protokoll-Tunnel-Jump-Links zu einer anderen Adresse im Unterbereich 127.x.x.x ändern.

Geben Sie unter **Lokaler Port** den Port an, der auf dem lokalen System des Benutzers geprüft wird. Wird dies als „automatisch“ belassen, weist die access console einen freien Port zu.

Geben Sie unter **Remote-Port** den Port am Remote-System an, über den die Verbindung aufgebaut werden soll. Dies wird durch den Servertyp bestimmt, mit dem Sie sich verbinden.



Sie können mehrere Paare von **TCP-Tunneln** gemäß Ihrer Konfiguration definieren.

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.

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 Benutzer auf dieses Jump-Element zugreifen können, ob eine Zugriffsbenachrichtigung gesendet werden sollte oder ob eine Berechtigung oder eine Ticket-ID Ihres externen Ticketsystems zur Verwendung dieses Jump-Elements notwendig ist, wählen Sie **Jump-Richtlinie**. Diese Richtlinien werden von Ihrem Administrator über die /login-Schnittstelle festgelegt.

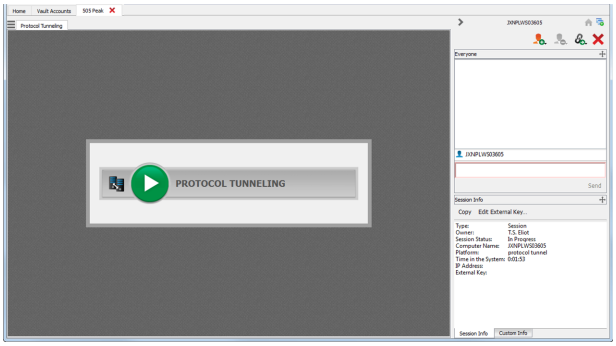
Organisieren und verwalten Sie bestehende Jump-Elemente, indem Sie einen oder mehrere Jump-Clients auswählen und auf **Eigenschaften** klicken.

> ***Hinweis:*** *Um die Eigenschaften mehrerer Jump-Elemente anzuzeigen, müssen alle ausgewählten Elemente vom gleichen Typ sein (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.*

Verwenden eines symbolischen Protokoll-Tunnel-Jump-Links

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

Eine Sitzung erscheint in Ihrer access console. Klicken Sie auf die Schaltfläche **Protokoll-Tunneling**, um die Verbindung aufzubauen.

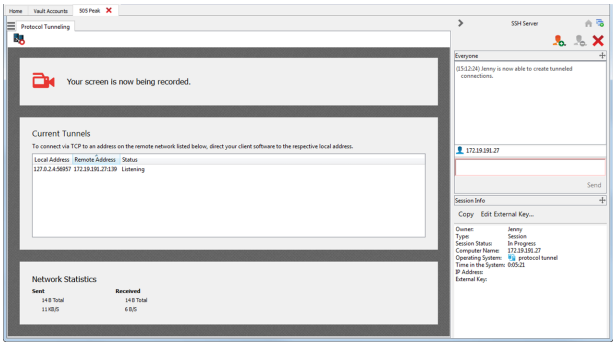


Wenn die Bildschirmaufzeichnung aktiviert ist, erscheint eine Eingabeaufforderung und informiert Sie, dass Ihr Desktop aufgezeichnet wird. Klicken Sie anschließend auf **OK**. Wenn Sie auf **Abbrechen** klicken, wird der Protokoll-Tunnel nicht erstellt.

Ist die Bildschirmaufzeichnung aktiviert, erscheint ein Indikator oberhalb Ihres Sitzungsbildschirms.

Der Bereich **Aktuelle Tunnel** zeigt die aktuellen Verbindungen und den dazugehörigen Status an. Ebenfalls können Sie sich zusammengefasste **Netzwerkstatistiken** ansehen.

Sie können jetzt einen Drittanbieter-Client öffnen, um Aufgaben am Remote-System durchzuführen. Verwenden Sie die angegebenen Ports, um sich mit dem Jumpoint zu verbinden.



Voraussetzungen zum fehlerfreien Betrieb

Die Protokoll-Tunneling-Funktion tunnelt Netzwerkverkehr so, dass die Kommunikation zwischen dem Benutzersystem und dem Endpunkt einigen Beschränkungen unterliegt.

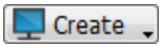
- Sämtlicher Verkehr muss auf TCP-Basis erfolgen.
- Nicht mehr als 256 gleichzeitige Verbindungen sind möglich.
- Alle TCP-Verbindungen müssen vom Endpunkt stammen und vom Benutzersystem akzeptiert werden. Das Anwendungsprotokoll darf nicht erfordern, dass das Benutzersystem eine separate Verbindung zurück zum Endpunkt aufbaut.
- Alle TCP-Verbindungen des Endpunkts zurück zum Benutzersystem müssen über bereits in den Eigenschaften des Protokoll-Tunnel-Jump-Elements definierten Tunneln erfolgen.
- Betriebssysteme gestatten es in der Regel nicht heraufgesetzten Prozessen nicht, Ports unter 1024 abzuhören. Daher muss der lokale Port größer als 1024 sein. Die Endpunkt-Software verbindet sich mit dem Server, indem Sie sich mit dem lokalen Port verbindet, den die access console (ein nicht heraufgesetzter Prozess) abhört.
- Die Endpunkt-Software kann keine Verbindungen zu anderen Systemen am Remote-Netzwerk aufbauen. Es ist nur eine Verbindung zu dem System möglich, das in den Eigenschaften des Protokoll-Tunnel-Jump-Elements angegeben wurde.
- Das Protokoll muss gegenüber dem Hostnamen, der vom Endpunkt zur Verbindung zum Server verwendet, agnostisch sein. Ansonsten müssen die Protokollanforderungen anderweitig erfüllt werden, etwa durch Zuweisung eines Hostnamens zu 127.0.0.1 in der Hosts-Datei oder durch Anwendung einer besonderen Konfiguration im Endpunkt-Client.
- Wenn die Tunnel-Definition einen lokalen Port aufweist, der sich vom Remote-Port unterscheidet (etwa, wenn der lokale Port größer als 1024 sein muss, weil der Serverport kleiner als 1024 ist), muss das Protokoll gegenüber dem Port, den der Endpunkt-Client zur Serververbindung nutzt, agnostisch sein.
- Für Protokolle, die über den Aufbau einer einzelnen TCP-Verbindung vom Endpunkt-Client zum Benutzersystem hinausgehen, ist das Verständnis des Administrators bezüglich des jeweiligen Protokolls und der obigen Voraussetzungen erforderlich.

Shell Jump zum Zugriff auf ein Remote-Netzwerkgerät verwenden

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. Administratoren können die Befehlsfilterung aktivieren, um zu verhindern, dass Benutzer an SSH-verbundenen Endpunkten versehentlich schädliche Befehle verwenden.

Erstellen eines symbolischen Shell Jump-Links

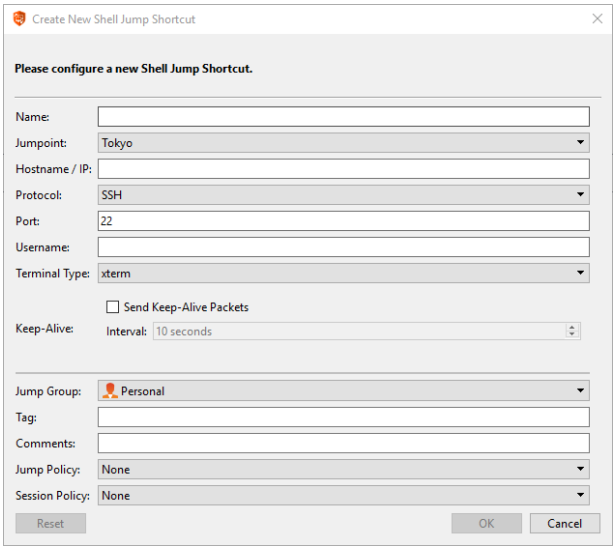
Um einen symbolischen Shell Jump-Link zu erstellen, klicken Sie auf die Schaltfläche **Erstellen** in der Jump-Schnittstelle. Wählen Sie aus der Dropdown-Liste **Shell Jump**. Symbolische Shell Jump-Links erscheinen in der Jump-Schnittstelle zusammen mit Jump-Clients und anderen Arten von symbolischen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

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 Benutzer auf dieses Jump-Element zugreifen können, ob eine Zugriffsbenachrichtigung gesendet werden sollte oder ob eine Berechtigung oder eine Ticket-ID Ihres externen Ticketsystems zur Verwendung dieses Jump-Elements notwendig ist, wählen Sie **Jump-Richtlinie**. 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 einen symbolischen Shell Jump-Link zum Start einer Sitzung zu verwenden, wählen Sie einfach den symbolischen Link aus der Jump-Schnittstelle und klicken Sie auf die Schaltfläche **Jump**.

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

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

Wenn Sie per Shell Jump auf ein 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.

Administratoren können die Befehlsfilterung an Shell Jump-Elementen verwenden, um manche Befehle zu blockieren und andere wiederum zu erlauben, damit der Benutzer nicht versehentlich einen Befehl verwendet, der zu unerwünschten Ergebnissen führt. Falls ein Benutzer versucht, einen Befehl zu verwenden, der einem unzulässigen Ausdruck entspricht, wird er entsprechend darauf hingewiesen und kann den Befehl nicht ausführen.

> *Der Befehlsfilter von BeyondTrust verwendet erweiterte reguläre Ausdrücke, die jedoch nicht mit egrep zu verwechseln sind. Weitere Informationen finden Sie in den Details unter docs.microsoft.com/en-us/cpp/standard-library/regular-expressions-cpp.*

Shellaufforderungsfilterung:

1. Melden Sie sich als Benutzer mit Berechtigungen zur Konfiguration von Jump-Elementen und Sitzungsrichtlinien in der /login-Schnittstelle an.
2. Navigieren Sie zu **Jump > Jump-Elemente** und schrollen Sie nach unten zum Bereich **Shell Jump-Filterung**.
3. Geben Sie in das Textfeld **Anerkannte Shell-Eingabeaufforderungen** reguläre Ausdrücke ein, die in Ihrem Endpunkt-Systemen zu finden sind, und zwar eine pro Zeile.

> ***Hinweis:** Zeilenumbrüche oder neue Zeilen sind innerhalb der eingegebenen Befehlsaufforderungsmuster nicht zulässig. Wenn ein Endpunkt-System eine mehrzeilige Aufforderung verwendet, geben Sie einen Ausdruck ein, der ausschließlich der letzten Zeile der Aufforderung im Textfeld entspricht.*

4. Klicken Sie auf **Speichern**.

> ***Hinweis:*** *Sobald Sie die gewünschten regulären Ausdrücke eingegeben haben, können Sie eine Shell-Eingabeaufforderung ausprobieren, um zu bestimmen, ob sie einem der regulären Ausdrücke auf der Liste entspricht. So können Sie Ihre regulären Ausdrücke prüfen, ohne eine Sitzung starten zu müssen. Geben Sie den Ausdruck in das Textfeld* ***Shell-Eingabeaufforderung*** *ein und klicken Sie auf die Schaltfläche* ***Prüfen****. Sie werden darauf hingewiesen, ob die von Ihnen eingegebene Shell-Eingabeaufforderung einem der regulären Ausdrücke auf der Liste entpsricht.*

Befehlsfilterung konfigurieren:

1. Navigieren Sie zu **Benutzer und Sicherheit > Sitzungsrichtlinien** und erstellen Sie entweder eine neue Richtlinie oder bearbeiten Sie eine vorhandene Richtlinie.

> ***Hinweis:*** *Sie können dies auch für Benutzer und/oder Gruppenrichtlinien konfigurieren.*

2. Machen Sie die Einstellungen **Befehlsshell** im Abschnitt „Berechtigungen“ ausfindig.
3. Da Sie die Befehlsfilterung mit Shell Jump-Elementen verwenden werden, wählen Sie über die Optionsschaltfläche **Zulassen** die Verwendung der Befehlsshell aus.
4. Wählen Sie zwischen **Alle Befehle zulassen**, **Nachstehende Befehlsmuster zulassen** und **Nachstehende Befehlsmuster ablehnen** und geben Sie im Textfeld an, welche Muster regulärer Ausdrücke Sie zulassen oder blockieren möchten.

> ***Hinweis:*** *Sobald Sie die Befehlsmuster eingegeben haben, die Sie zulassen oder blockieren möchten, können Sie Befehle im Textfeld* ***Befehlstester*** *prüfen. So können Sie Ihre Befehlsfilter prüfen, ohne eine Sitzung starten zu müssen. So können Sie Ihre Befehlsfilter prüfen, ohne eine Sitzung starten zu müssen. Sie erhalten einen Hinweis, in dem darauf hingewiesen wird, ob der eingegebene Befehl den auf der Liste stehenden regulären Ausdrücken zufolge im Remote-System zulässig wäre.*
>
> *Folgende Hinweise sind möglich:*
>
> - *Der eingegebene Shell-Befehl ist basierend auf Ihrer Auswahl zulässig.*
> - *Der eingegebene Shell-Befehl ist basierend auf der Auswahl nicht zulässig.*

Verwenden der Anmeldedaten-Einfügung mit SUDO an einem Linux-Endpunkt

Zur Verwendung der Anmeldedaten-Einfügung mit SUDO muss ein Administrator ein oder mehr funktionale Konten auf jedem Linux-Endpunkt erstellen, auf den per Shell Jump zugegriffen werden soll. Da der Prozess zur Konfiguration der sudoers-Datei komplex ist und von Plattform zu Plattform variiert, beziehen Sie sich bitte auf die Dokumentation Ihrer Plattform zu Einzelheiten für diesen Prozess. Jedes funktionale Konto muss:

- SSH-Authentifizierung zulassen (Kennwort oder SSH-Schlüssel)
- Die Konto-Anmeldedaten im Endpunkt-Anmeldedaten-Manager speichern lassen
- Einen oder mehrere Einträge in `/etc/sudoers` besitzen, welche dem funktionalen Konto Zugriff auf einen oder mehrere Befehle gewähren, die ohne Anforderung eines Kennworts als root ausgeführt werden können (`NOPASSWD`).

Ein Administrator muss ein Shell Jump-Element für den Endpunkt erstellen.

Als nächstes muss ein Administrator den Endpunkt-Anmeldedaten-Manager und/oder das Kennwort-Vault konfigurieren, um Benutzern Zugriff auf die jeweiligen funktionalen Konten für das Jump-Element zu gewähren.

Wenn ein Benutzer einen Jump zu dem Shell Jump-Element durchführt, kann er aus einer Liste funktionaler Konten für diesen Endpunkt wählen. Jedes funktionale Konto hat seine eigenen Befehle, die per SUDO ausgeführt werden können, abhängig von der Konfiguration

des Administrators am Endpunkt. Die Anmeldedaten für das Konto werden vom Endpunkt-Anmeldedaten-Manager an den Endpunkt weitergegeben.

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/privileged-remote-access/getting-started/admin/jump-items.htm.*

Verwenden von Web-Jump zum Zugriff auf Webdienste

Angesichts des Trends hin zu webbasierten Konfigurationsschnittstellen für Infrastrukturkomponenten stehen IT-Administratoren einer zusehends komplexeren Sicherheitsverwaltungssituation gegenüber. Der autorisierte Zugriff auf webbasierte Ressourcen ist schwierig zu kontrollieren und zu prüfen. Gleichermaßen ist eine ordnungsgemäße Authentifizierung ohne Beeinträchtigung der Geschäftsproduktivität eine Herausforderung. IT-Administratoren benötigen einen Weg, um über Webschnittstellen verwaltete Ressourcen effektiv zu kontrollieren und zu prüfen, darunter:

- Extern gehostete IaaS-Server (Infrastructure as a Service) wie Amazon AWS, Microsoft Azure, IBM SoftLayer und Rackspace
- Intern gehostete Server, die von Hypervisor-Software wie VMware vSphere, Citrix XenServer und Microsoft Hyper-V verwaltet werden
- Moderne Netzwerk-Kerninfrastruktur, die webbasierte Konfigurationsschnittstellen nutzt

Die Identitäts- und Zugriffsverwaltungsfunktionen variieren unter IaaS, Hypervisor-Anbietern und Kerninfrastruktursystemen stark. Viele bieten keine native Unterstützung für Multifaktor-Authentifizierung, wodurch es an einer zusätzlichen Sicherheitsebene mangelt. Diese systemübergreifenden Inkonsistenzen sind ein Nährboden für Unternehmensschwachstellen, wie etwa Konten- und Zugriffsmissbrauch, wodurch empfindliche Daten nach außen gelangen könnten. Bei BeyondTrust Web Jump handelt es sich um einen zusätzlichen Sicherheitslayer für die Authentifizierung in solchen Systemen.

WICHTIG!

Flash wird von Web Jump nicht unterstützt. Beachten Sie Ihre Hypervisor-Dokumentation und aktualisieren Sie sie auf eine Version, die HTML5 unterstützt.

***Hinweis:** Beim Web Jump-Element handelt es sich um ein Add-on für Privilegierter Remote-Zugriff und muss separat erworben werden.*

Erstellen eines symbolischen Web-Jump-Links

***Hinweis:** Stellen Sie vor der Erstellung von symbolischen Web-Jump-Links sicher, dass Ihr Benutzerkonto zum Zugriff auf Web-Jumps berechtigt ist, indem Sie zu **Benutzer und Sicherheit > Benutzereinstellungen > Jump-Technologie** navigieren.*

Um einen symbolischen Web-Jump-Link zu erstellen, klicken Sie in der Jump-Schnittstelle auf die Schaltfläche **Erstellen**. Wählen Sie aus der Dropdown-Liste **Web-Jump**. Symbolische Web-Jump-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 (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.

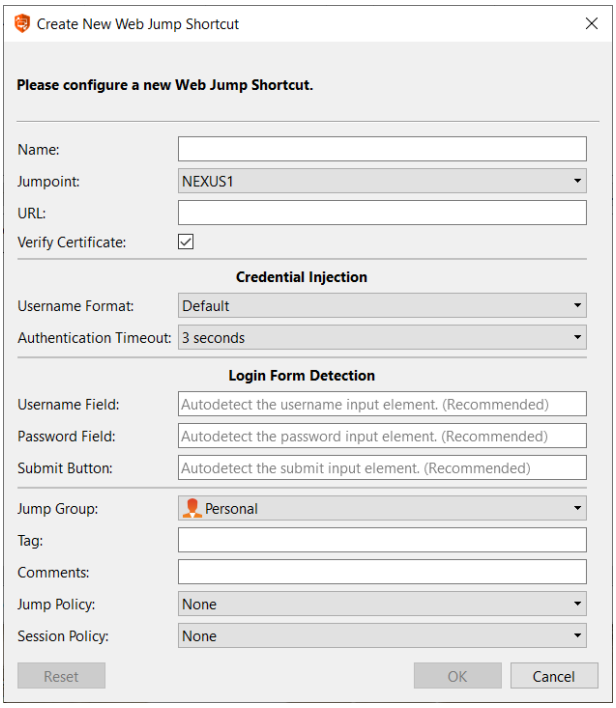
Wählen Sie im Dropdown-Menü **Jumpoint** das Netzwerk aus, in dem sich der Computer befindet, auf den Sie zugreifen möchten.

Geben Sie die **URL** für die Website ein, auf die Sie zugreifen möchten.

Aktivieren Sie **Zertifikat verifizieren**, wenn das Seitenzertifikat vor dem Verbindungsaufbau validiert werden soll. Ist diese Option aktiviert und es werden Probleme mit dem Zertifikat festgestellt, wird die Sitzung nicht gestartet.

WICHTIG!

*Deaktivieren Sie **Zertifikat verifizieren** nur, wenn Sie einen Jump zu einer Site durchführen, der Sie vertrauen, die aber ein selbstsigniertes Zertifikat verwendet.*



Wenn Sie das Einfügen von Anmeldedaten verwenden möchten, wählen Sie zunächst das **Benutzernamenformat**:

- **Standard**: Dies ist der Standardwert für neue und bestehende Web-Jump-Elemente. Der Benutzername wird vor dem Einfügen in die Webseite nicht verändert und wird im gespeicherten Format verwendet. Für den Endpunkt-Anmeldeverwalter (ECM) können die Anmeldedaten entweder im UPN- oder DLLN-Format vorliegen. Für Vault ist der Benutzername immer im UPN-Format.
- **Nur Benutzername**: Unabhängig vom Format, das entweder im Vault oder im ECM gespeichert ist **(benutzername@domäne** oder **domäne\benutzername**), wird die Domäne entfernt und nur der Benutzername verwendet.

Geben Sie unter **Erkennung des Anmeldeformulars** je nach Bedarf Informationen zu den drei Optionen an:

- **Benutzername-Feld**: Diese Einstellung gibt den Hinweis für das Benutzername-Feld auf der Anmeldeseite an. Wenn kein Feld für den Benutzernamen gefunden wird, schlägt die Eingabe fehl. Dem Benutzer wird eine Fehlermeldung angezeigt, die besagt, dass das Feld Benutzername nicht gefunden werden konnte.
- **Kennwortfeld**: Diese Einstellung gibt den Hinweis für das Kennwortfeld auf der Anmeldeseite an. Wenn kein Kennwortfeld gefunden wird, schlägt die Eingabe fehl. Dem Benutzer wird eine Fehlermeldung angezeigt, die besagt, dass das Kennwortfeld nicht gefunden werden konnte.
- **Schaltfläche "Abschicken"**: Diese Einstellung gibt den Hinweis für die Schaltfläche "Abschicken" auf der Anmeldeseite an. Wenn keine solche Schaltfläche gefunden wird, schlägt die Eingabe fehl. Dem Benutzer wird eine Fehlermeldung angezeigt, die besagt, dass die Schaltfläche nicht gefunden werden konnte.

***Hinweis:** Wenn diese drei Felder leer gelassen werden, erkennt das System automatisch die notwendigen Informationen, die bereits für die Anmeldung gespeichert sind, und verwendet sie.*

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.

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.

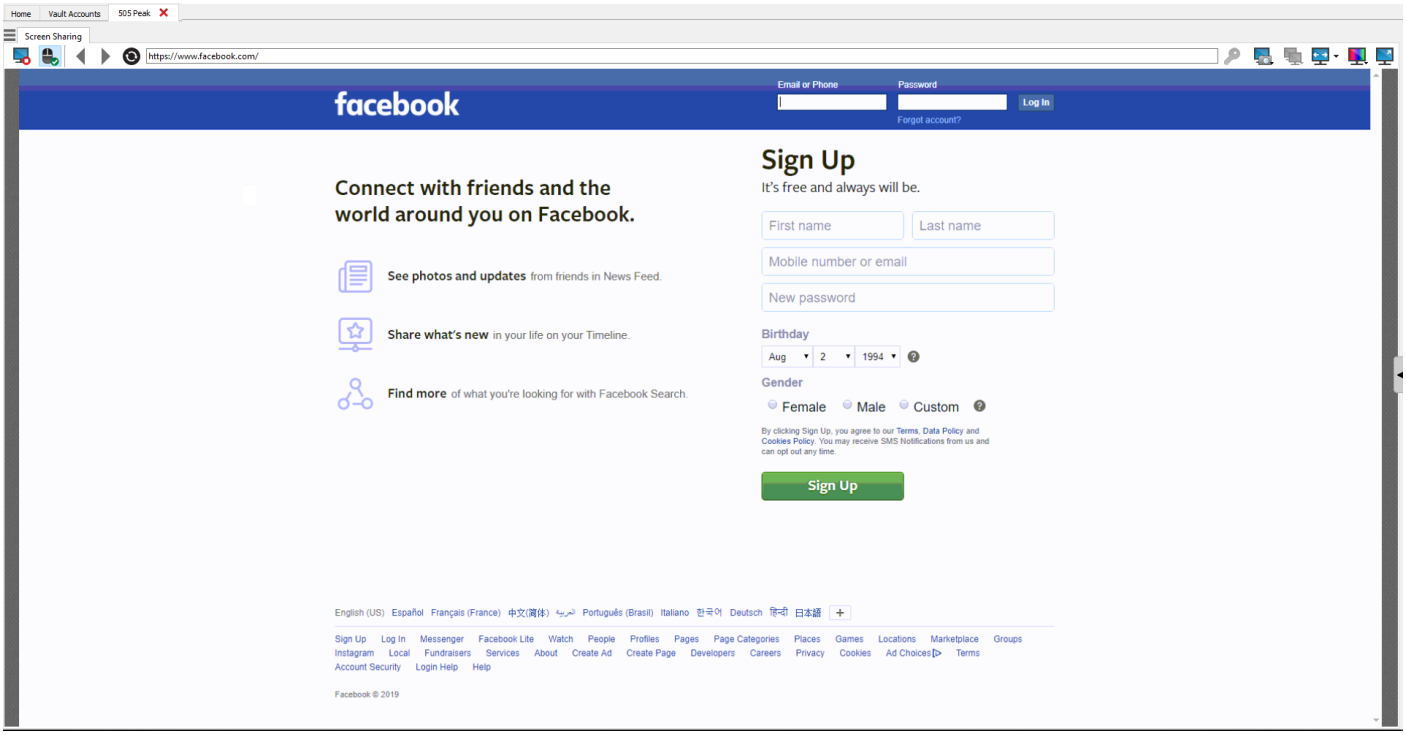
Um festzulegen, wann Benutzer auf dieses Jump-Element zugreifen können, ob eine Zugriffsbenachrichtigung gesendet werden sollte oder ob eine Berechtigung oder eine Ticket-ID Ihres externen Ticketsystems zur Verwendung dieses Jump-Elements notwendig ist, wählen Sie **Jump-Richtlinie**. Diese Richtlinien 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 Web-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**.

Sobald eine Verbindung zur Website aufgebaut ist, klicken Sie auf das Bildschirmfreigabe-Symbol. Die Anmeldungsschnittstelle der Webseite wird verfügbar. Wenn Sie auf einen Link klicken, um eine Datei von der Website herunterzuladen, erscheint eine Aufforderung in Ihrem Chatfenster, die Sie bittet, den Download zu akzeptieren oder abzulehnen. Wenn Sie ihn akzeptieren, öffnet sich ein Fenster auf Ihrem Computer und gestattet es Ihnen, einen Download-Ort zu wählen. Das Hochladen von Dateien auf die Webseite funktioniert auf ähnliche Art und Weise und öffnet ein Fenster, bei dem Sie die hochzuladenden Dateien wählen können.



Hinweis: *Wenn die Webseite eine neue Registerkarte erfordert, öffnet sich eine neue Registerkarte. Sie können neue Registerkarten nicht willkürlich öffnen.*

Tipp: *Sie können Text in die und aus der Webseite kopieren und einfügen, indem Sie die Kopieren/Einfügen-Steuerung Ihres Betriebssystems verwenden.*

Verwenden der Anmeldedaten-Einfügung

Bei der Integration von BeyondTrust PRA mit einem Kennwort-Speicher (Vault) können Sie mit der Anmeldedaten-Einfügung nahtlos auf Ihre Website-Konten zugreifen, ohne den Anmeldebildschirm sehen oder Anmeldedaten eingeben zu müssen.

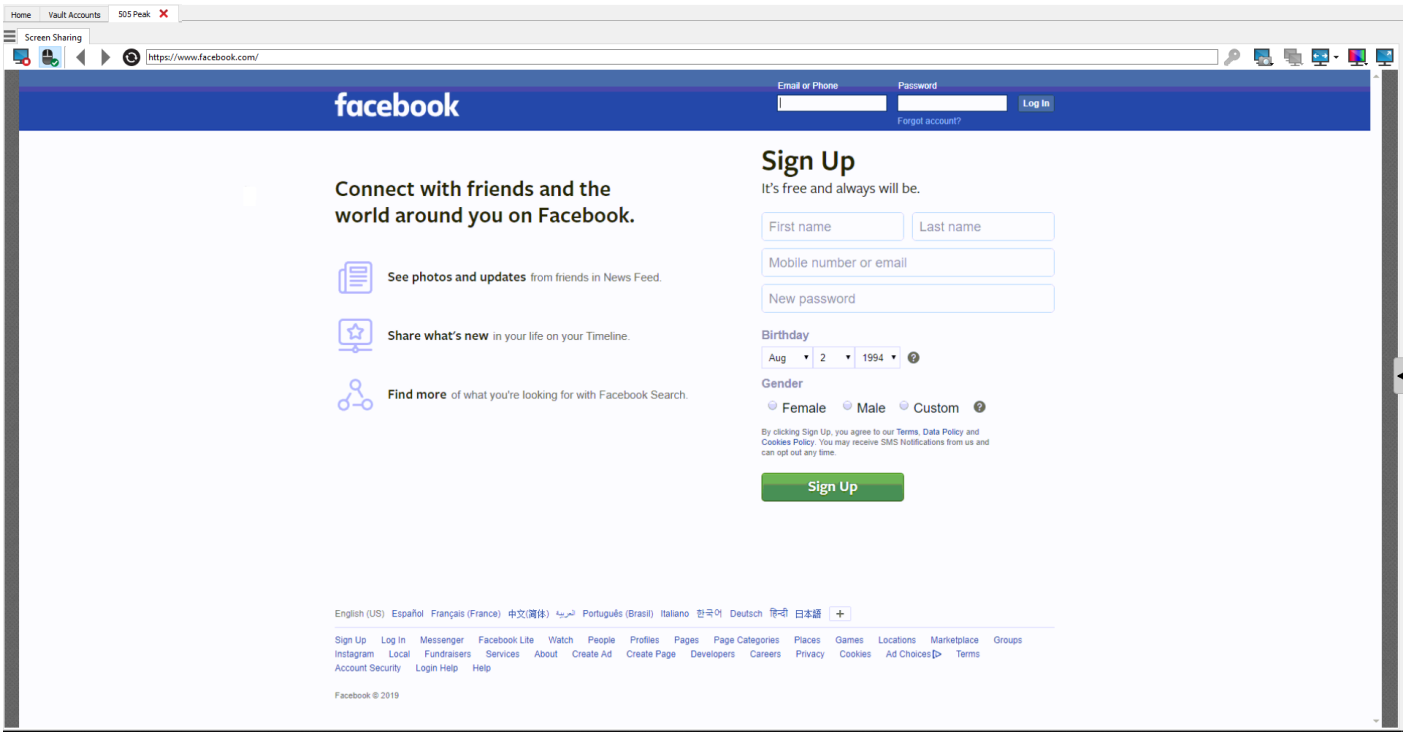
Hinweis: *Web Jump unterstützt die Authentifizierung in mehreren Schritten, bei denen Benutzername und Kennwort nicht auf ein und derselben Browserseite erforderlich sind. Web Jump unterstützt darüber hinaus Szenarien, in denen sich ein Benutzer mit einem nicht authentifizierten Teil einer Website verbindet, aber dann versucht, mit einfacher Authentifizierung einen Bereich aufzurufen. Darüber hinaus unterstützt Web-Jump Websites, die CAPTCHAs enthalten, indem sie Benutzern die Möglichkeit geben, das CAPTCHA durchzuführen, ohne dass der Vorgang der Anmeldedaten-Einfügung beendet wird. Sobald die Interaktion mit einem CAPTCHA abgeschlossen ist, klickt der Benutzer auf das Schlüsselsymbol in der access console und schließt die Anmeldedaten-Einfügung ab.*

Hinweis: *Für nahtlose Anmeldedaten-Einfügung auf einer VMware-Konsole sind bestimmte Konfigurationsaufgaben erforderlich.*

1. *Gehen Sie zum Computer, der den Jumpoint hostet.*
2. *Laden Sie das Client-Integrations-Plugin von der oben angegebenen VMware-URL herunter und installieren Sie es.*
3. *Öffnen Sie mithilfe der Admin-Berechtigungen die Windows-Dienste (**services.msc**) auf dem Jumpoint-Host.*
4. *Rechtsklicken Sie auf den BeyondTrust-Jumpoint und wählen Sie **Eigenschaften**.*
5. *Aktivieren Sie auf der Registerkarte **Anmeldung** unter **Lokales Systemkonto** die Option **Dienst die Interaktion mit Desktop gestatten**.*
6. *Klicken Sie auf **OK**.*
7. *Starten Sie auf dem lokalen Benutzersystem, wo die access console installiert wurde, einen Web-Jump mit der obigen VMware-URL.*
8. *Wählen Sie **Windows-Anmeldedaten verwenden**.*
9. *Damit wird eine Aufforderung auf dem Jumpoint-Host-System gestartet, mit der Dienste mit einem externen Programm interagieren können. Gewähren Sie dem Dienst die Berechtigung.*
10. *Eine Aufforderung für die VMware-Anmeldedateneinfügung wird angezeigt. Deaktivieren Sie die Option, die fragt, ob die Aufforderung bei jedem Programmaufruf angezeigt werden soll. Wählen Sie **Akzeptieren**.*
11. *Sie können jetzt Web-Jumps zur VMware-Konsole mit Windows-Anmeldedaten durchführen, ohne, dass eine Aufforderung erscheint.*

Zugriffs-Toolset

Überblick über Zugriffssitzungen 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. 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 über das Menü auch die Sitzung 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.
	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.
	Der Sitzungseigentümer kann einen anderen Benutzer aus einer freigegebenen Sitzung entfernen.
	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 Endpunkt 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.
	Sitzungsregisterkarte ganz schließen. Sie können die Sitzung von der Seitenleiste, dem Sitzungsmenü oder der Sitzungsregisterkarte aus schließen.

Unten rechts im Sitzungsfenster werden Informationen zum Remote-System angezeigt. 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 Access Console

Beim Zugriff auf ein Windows-basiertes Jump-Element über die access console 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 Privilegierter Remote-Zugriff zu verbinden.

> ***Hinweis:*** *Anmeldedaten-Einfügung ist nicht für Mac Jump-Clients verfügbar.*

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.

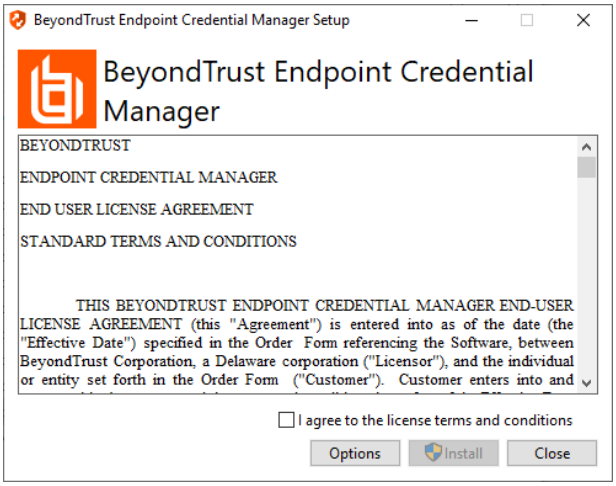
> ***Hinweis:*** *Der ECM muss auf Ihrem System installiert werden, damit der BeyondTrust ECM-Dienst aktiviert und die Anmeldedateneinfügung in BeyondTrust Privilegierter Remote-Zugriff ermöglicht werden kann.*

Systemanforderungen

- **Windows Vista oder neuer, nur 64 Bit**
- **.NET 4.5 oder neuer**

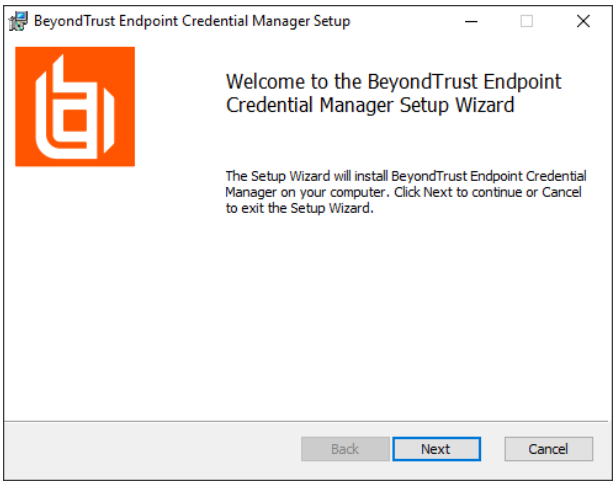
1. Laden Sie zunächst den BeyondTrust Endpunkt-Anmeldedaten-Manager (ECM) von BeyondTrust Support unter beyondtrustcorp.service-now.com/csm herunter.
2. Starten Sie den Installationsassistenten für den BeyondTrustEndpunkt-Anmeldedaten-Manager.
3. Stimmen Sie den Bedingungen der Endbenutzer-Lizenzvereinbarung zu. Aktivieren Sie das Kontrollkästchen zur Zustimmung und klicken Sie dann auf **Installieren**.

   Wenn Sie den Installationspfad von ECM anpassen müssen, klicken Sie auf die Schaltfläche **Optionen**.

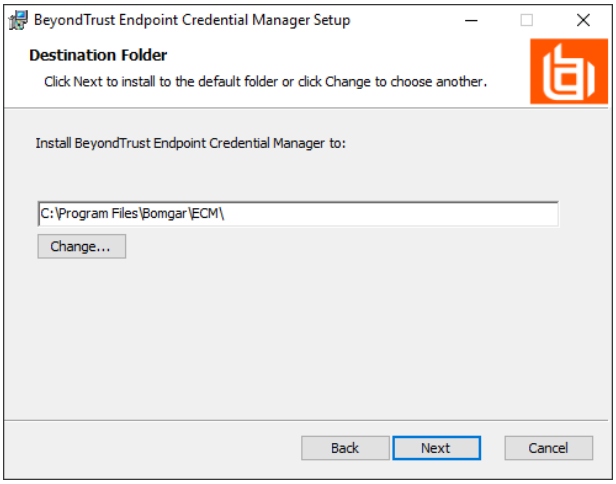


> ***Hinweis:*** *Sie können mit der Installation erst fortfahren, wenn Sie der Endbenutzer-Lizenzvereinbarung zustimmen.*

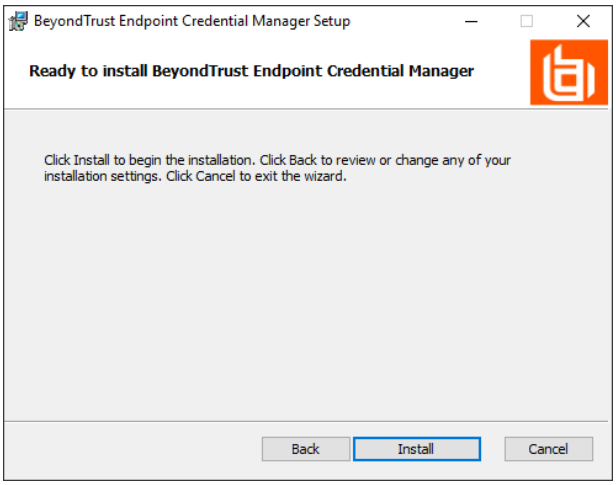
4. Klicken Sie auf dem Begrüßungsbildschirm auf **Weiter**.



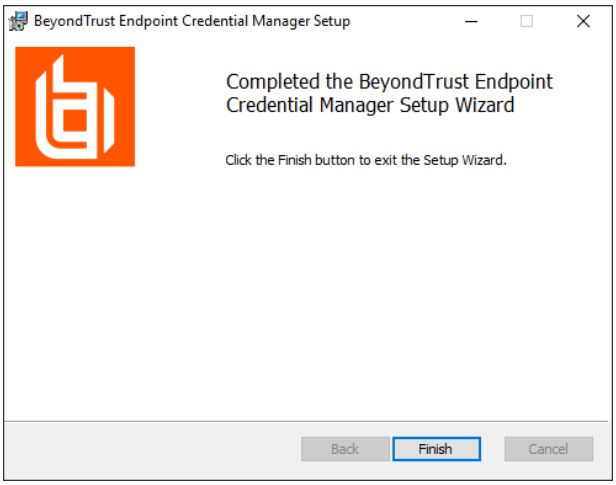
5. Wählen Sie den Installationsort für den Anmeldedaten-Manager und klicken Sie dann auf **Weiter**.



6. Auf dem nächsten Bildschirm können Sie mit der Installation beginnen oder vorherige Schritte überprüfen.
7. Klicken Sie auf **Installieren**, wenn Sie bereit sind.



8. 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 drei ECMs auf unterschiedlichen Windows-Systemen installieren, um mit dem gleichen Anmeldedatenspeicher zu kommunizieren. Eine Liste der mit der Geräte-Site verbundenen ECMs finden Sie in* ***/login > Status > Informationen > ECM-Clients****.*

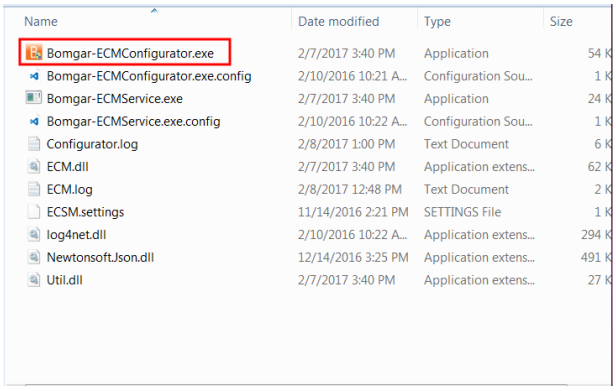
Hinweis: *Wenn ECMs in einer Konfiguration mit hoher Verfügbarkeit verbunden sind, leitet das BeyondTrust Appliance B Series Anfragen an den ECM in die ECM-Gruppe, die am längsten mit dem Gerät verbunden ist.*

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

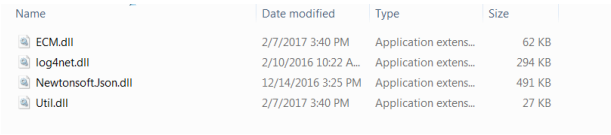


3. Wenn der Konfigurator geöffnet wird, vervollständigen Sie die Felder. Alle Felder müssen ausgefüllt werden.

Geben Sie folgende Werte ein:

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

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



Hinweis: *Wenn Sie sich mit einem 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.*

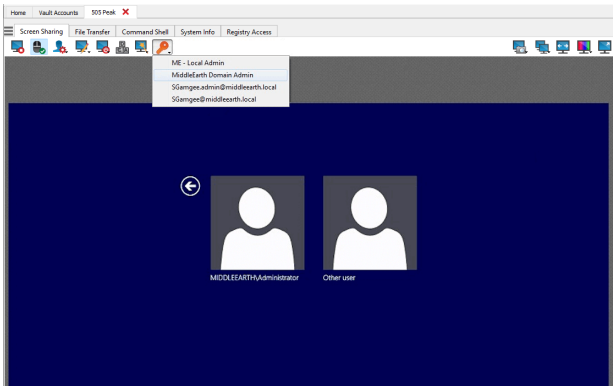
WICHTIG!

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 access console mit der Verwendung von Anmeldedaten aus dem Anmeldedaten-Speicher zur Anmeldung in Remote-Systemen beginnen.

1. Melden Sie sich in der access console 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 im Remote-System angemeldet.



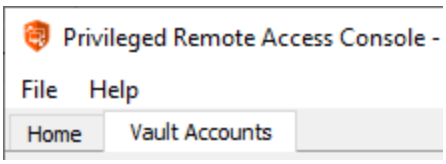
Aus bevorzugten Anmeldedaten zur Einfügung wählen

Nachdem Sie sich mit Anmeldedaten an einem Endpunkt angemeldet haben, speichert das System Ihre bevorzugten Anmeldedaten 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 B Series Appliance-Datenbank. Wenn Sie beim nächsten Mal Anmeldedaten für den Zugriff auf den selben Endpunkt benutzen, empfiehlt das 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 B Series Appliance einfach alle möglichen Anmeldedaten an.

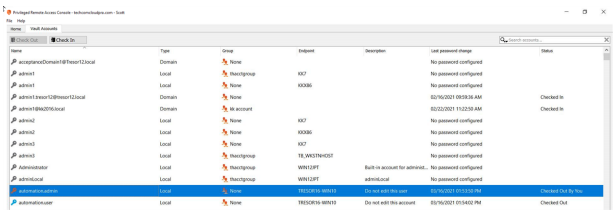
Die Anmeldedaten-Liste empfiehlt höchstens fünf Anmeldedaten.

Auschecken und Einchecken von Vault-Anmeldedaten

Sie können auf den Privilegierter Remote-Zugriff-Vault einfach über den access console zugreifen. Dadurch können Sie bei Bedarf Anmeldedaten auschecken und einchecken, entweder während einer Sitzung oder auf Ihrem lokalen Computer.

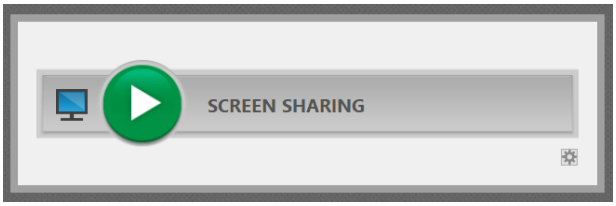


Wählen Sie die Registerkarte **Vaultkonten**, um eine Liste der verfügbaren Anmeldedaten und zugehörigen Informationen anzuzeigen.



Steuern des Remote-Endpunkts mit der Bildschirmfreigabe

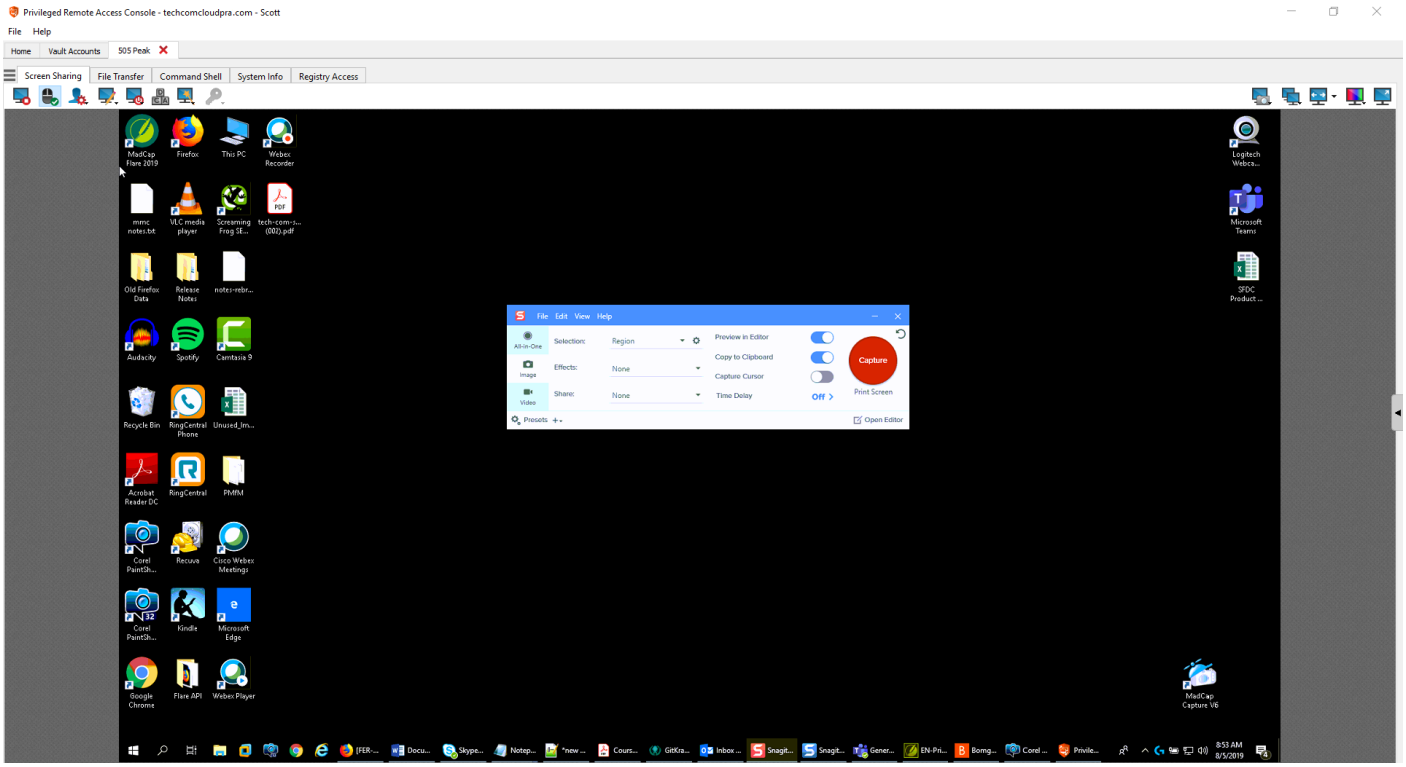
Klicken Sie im Sitzungsfenster auf **Bildschirmfreigabe**, um die Steuerung des Remote-Computers anzufordern, falls die Bildschirmfreigabe nicht automatisch startet. Abhängig von Ihren Kontoeinstellungen können unterhalb der Schaltfläche weitere Optionen zur Verfügung stehen. Klicken Sie auf die Zahnrad-Schaltfläche,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



Wenn Sie eine Sitzung gestartet haben, beginnt die Zugriffskonsole sofort mit der Bildschirmfreigabe mit dem Endpunkt. Abhängig vom System haben Sie möglicherweise die volle Kontrolle oder nur Anzeigeberechtigungen bei der Bildschirmfreigabe mit dem System.

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 **Nur Anzeigen** auswählen, können Sie den Remote-Bildschirm sehen, aber nicht steuern.
- **Privater Bildschirm** startet die Sitzung mit deaktivierter Ansicht und Steuerung des Remote-Endpunktes. Der private Bildschirm ist nicht verfügbar, wenn Support für Windows 8 bereitgestellt wird.



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 Endbenutzeransicht des privaten Bildschirms erläutert dann, dass der BeyondTrust-Benutzer die Kundenansicht deaktiviert hat. Der Endbenutzer kann durch Drücken von **Strg-Alt-Entf** stets wieder die Kontrolle übernehmen. Deaktivieren Sie alternativ die Maus- und Tastatureingabe des Endbenutzers und gestatten Sie weiterhin die Ansicht des Bildschirms. Wenn die Eingabe eingeschränkt ist, erscheint ein orangener Rahmen auf den Monitoren des Endbenutzers und eine Nachricht gibt an, dass der BeyondTrust-Benutzer die Maus- und Tastatursteuerung besitzt. Der Endbenutzer kann durch Drücken von **Strg-Alt-Entf** stets wieder die Kontrolle übernehmen. Die eingeschränkte Endpunktinteraktion ist nur beim Zugriff auf macOS- oder Windows-Computer verfügbar. Die eingeschränkte Kundeninteraktion ist nur bei der Unterstützung von Windows-Computern verfügbar. In Windows Vista und höher muss der endpoint client heraufgesetzt werden. In Windows 8 ist dieses Feature auf die Deaktivierung von Maus und Tastatur beschränkt.
	Anmerkungswerkzeuge ermöglichen eine einfachere Zusammenarbeit in freigegebenen Sitzungen. Eine Reihe von Werkzeugen steht zur Verfügung, darunter Formen und freies Zeichnen.
	Starten Sie das Remote-System entweder im normalen oder im abgesicherten Modus mit Netzwerk-Funktion neu, oder fahren Sie das Remote-System herunter.
	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. Vordefinierte Skripts, die für den Benutzer verfügbar sind, erscheinen in einem erweiterbaren Menü. Auf einem Windows®-System können Sie mit der besonderen Aktion „Ausführen als“ auch Anmeldedaten aus einem Endpunkt-Anmeldedaten-Manager auswählen. Die Verwendung des Endpunkt-Anmeldedaten-Managers erfordert eine separate Dienstleistungsvereinbarung mit BeyondTrust. Nach Abschluss einer Dienstleistungsvereinbarung können Sie die erforderliche Middleware vom BeyondTrust Support-Portal herunterladen.
	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. 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.
	Zum Neustart der Bildschirmfreigabe mit einem iOS-Gerät. Einzelheiten finden Sie in Support für Apple iOS-Geräte auf www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/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-access session 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.

	Melden Sie sich am Endpunkt mit Anmeldedaten an, die von einem externen Anmeldedatenspeicher zur Verfügung gestellt werden. Die Verwendung des Endpunkt-Anmeldedaten-Managers erfordert eine separate Dienstleistungsvereinbarung mit BeyondTrust. Nach Abschluss einer Dienstleistungsvereinbarung können Sie die erforderliche Middleware vom BeyondTrust Support-Portal herunterladen. Vor 15.2 war diese Funktion nur in Sitzungen verfügbar, die auf Windows® über einen heraufgesetzten Jump-Client gestartet wurden. Ab 15.2 können Sie auch den Endpoint Credential Manager in Remote-Jump-Sitzungen, Microsoft® Remote Desktop Protocol-Sitzungen, VNC-Sitzungen und Shell Jump-Sitzungen verwenden.
	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 Screenshots im Menü **Datei > Einstellungen > Extras** in der access console 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 sowie 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 Remote-Bildschirm des Endpunktes zu zeichnen

Verwenden Sie Anmerkungswerkzeuge, um in freigegebenen Sitzungen mit anderen Benutzern zusammenzuarbeiten. Anmerkungen sind ein interaktiver Weg zur visuellen Kommunikation, mit dem möglicherweise frustrierende Situationen reduziert und Prozesse beschleunigt werden.

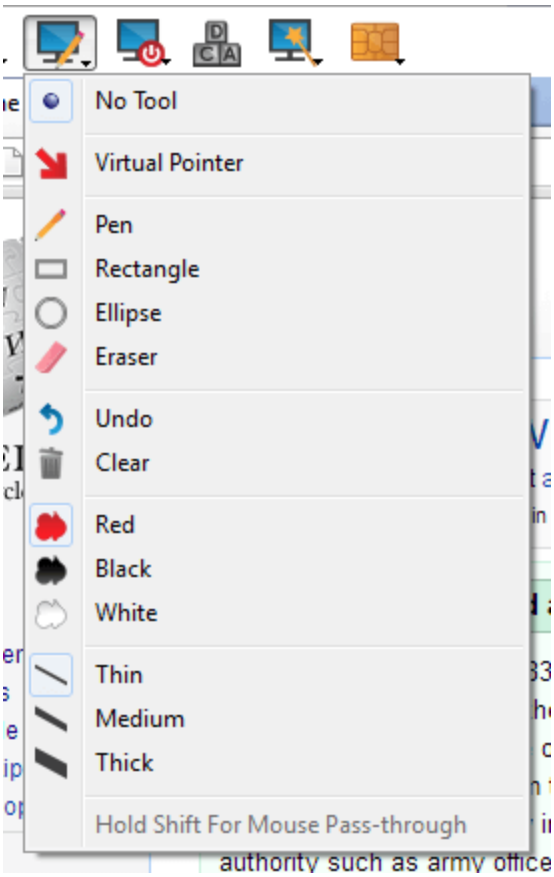
Während Sie sich im Anmerkungsmodus befinden, können Sie trotzdem Ihre Maus bewegen oder Objekte auf dem Desktop des Kunden steuern. Durch Gedrückthalten der **Umschalt**-Taste wird der Anmerkungsmodus vorübergehend unterbrochen.

Anmerkungen aktivieren

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

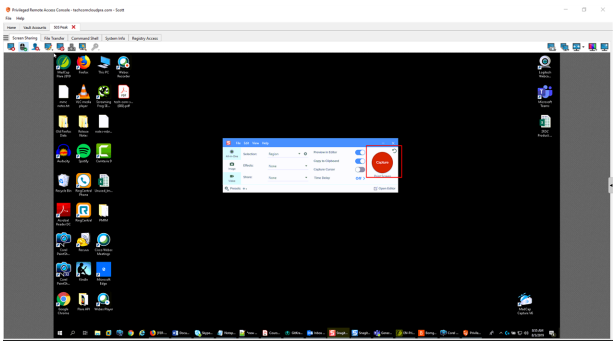
Durch Klicken auf eine beliebige Dropdown-Menüoption wird der **Anmerkungsmodus** eingeschaltet. Die folgenden Werkzeuge und Funktionen stehen zur Verfügung:

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



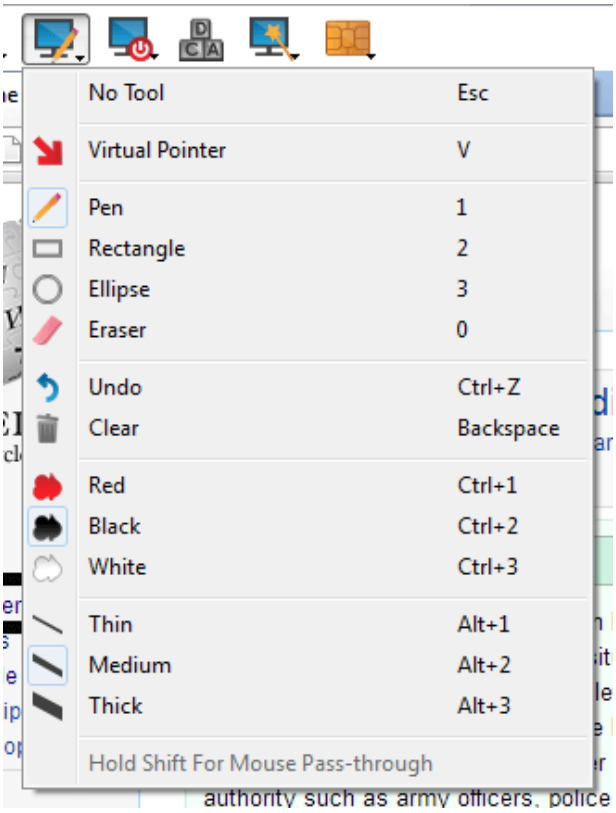
Sie können Ihr Werkzeug aus dem Dropdown-Menü **Anmerkungen** oder durch Rechtsklicken im Remote-Bildschirmbereich auswählen. Wenn Sie in den Bereichen außerhalb des Remote-Bildschirms klicken, wird das Dropdown-Menü nicht angezeigt.

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



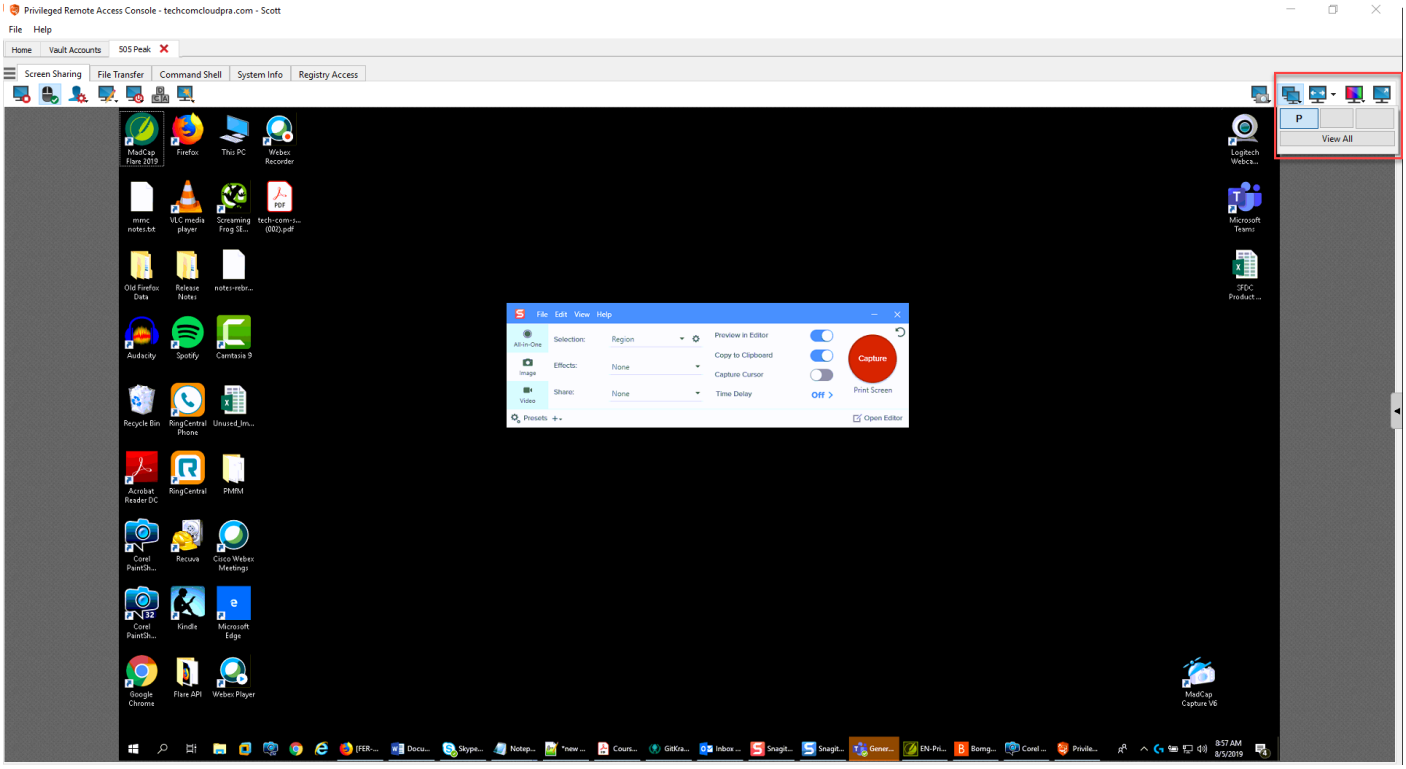
Um **Anmerkungen** auszuschalten, wählen Sie **Kein Werkzeug** im Dropdown-Menü, oder klicken Sie auf **Esc.**

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



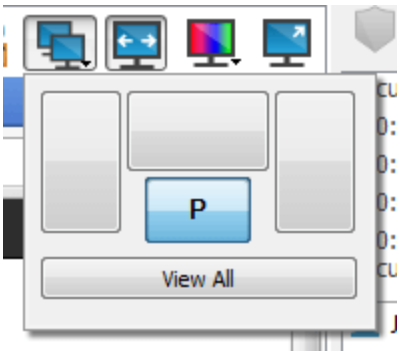
Zeigen Sie mehrere Monitore am Remote-Endpunkt an

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.

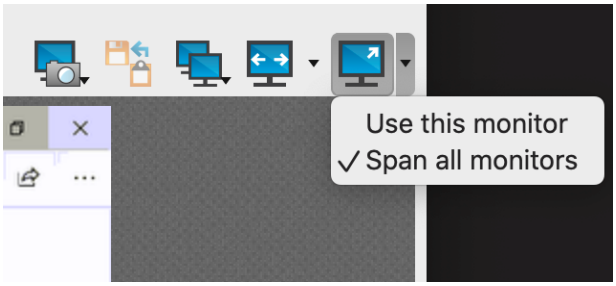


Der Primär-Monitor erscheint standardmäßig im Fenster **Bildschirmfreigabe**. Um die Ansicht zu ändern, klicken Sie das Rechteck an, das den Monitor darstellt, den Sie anzeigen möchten. Sie können auch **Alle anzeigen** auswählen, um alle Monitore im Fenster **Bildschirmfreigabe** anzuzeigen, die mit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

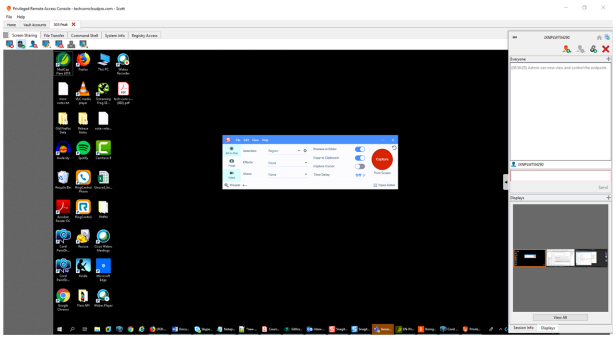
Mit einer Option können Sie eine über alle Monitore des Client-Computers erweiterte PRA-Verbindung öffnen, unabhängig von der Konfiguration des Client-Monitors. Mit dieser Funktion können Sie alle an den Client-Computer angeschlossenen Monitore voll ausnutzen und somit die Bildschirmgröße und -skalierung 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.*

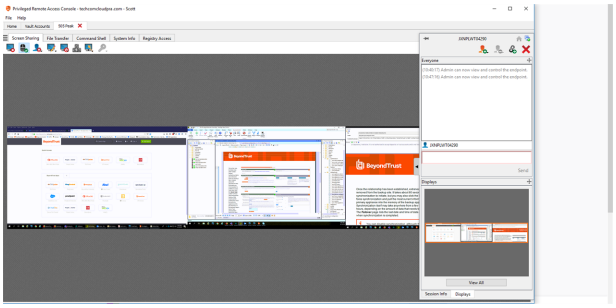
Die Registerkarte „Monitore“ verwenden

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.

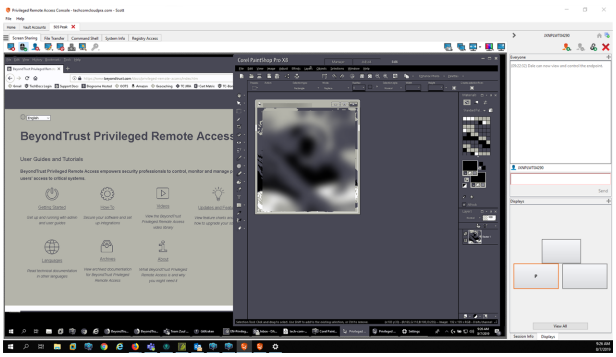


Der Monitor, der zurzeit auf der Registerkarte **Bildschirmfreigabe** angezeigt wird, ist hervorgehoben.

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.



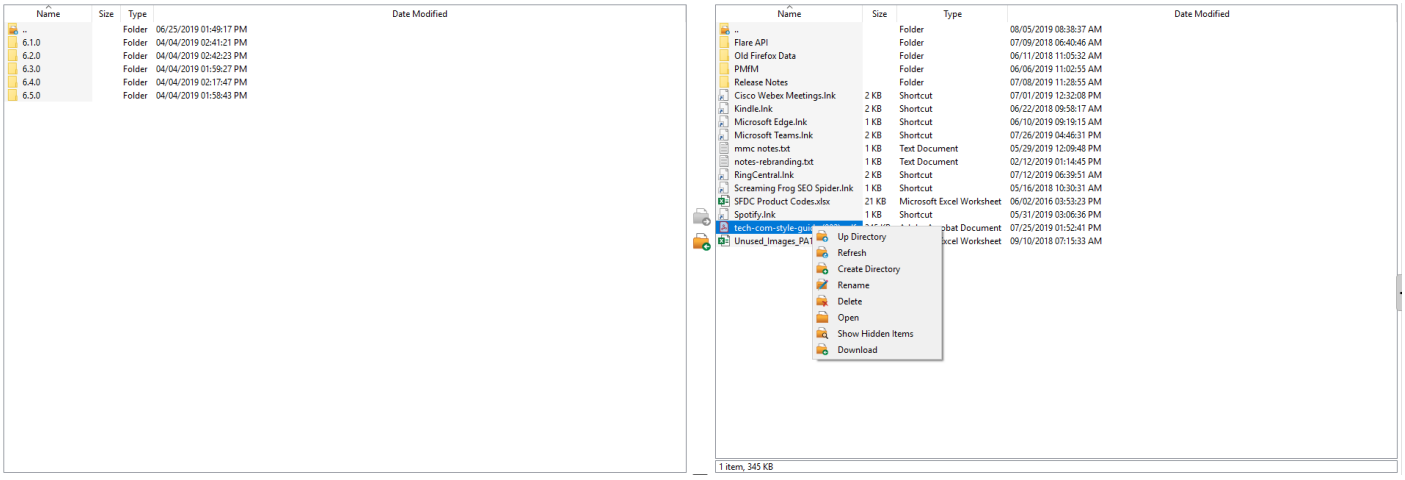
> ***Hinweis:*** *Der Aktualisierungszyklus der Miniaturansicht dauert unter idealen Umständen ca. drei Sekunden, kann aber, je nach Internetgeschwindigkeit und Datentransfer, länger dauern.*

Dateitransfer zum und vom Remote-Endpunkt

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.

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

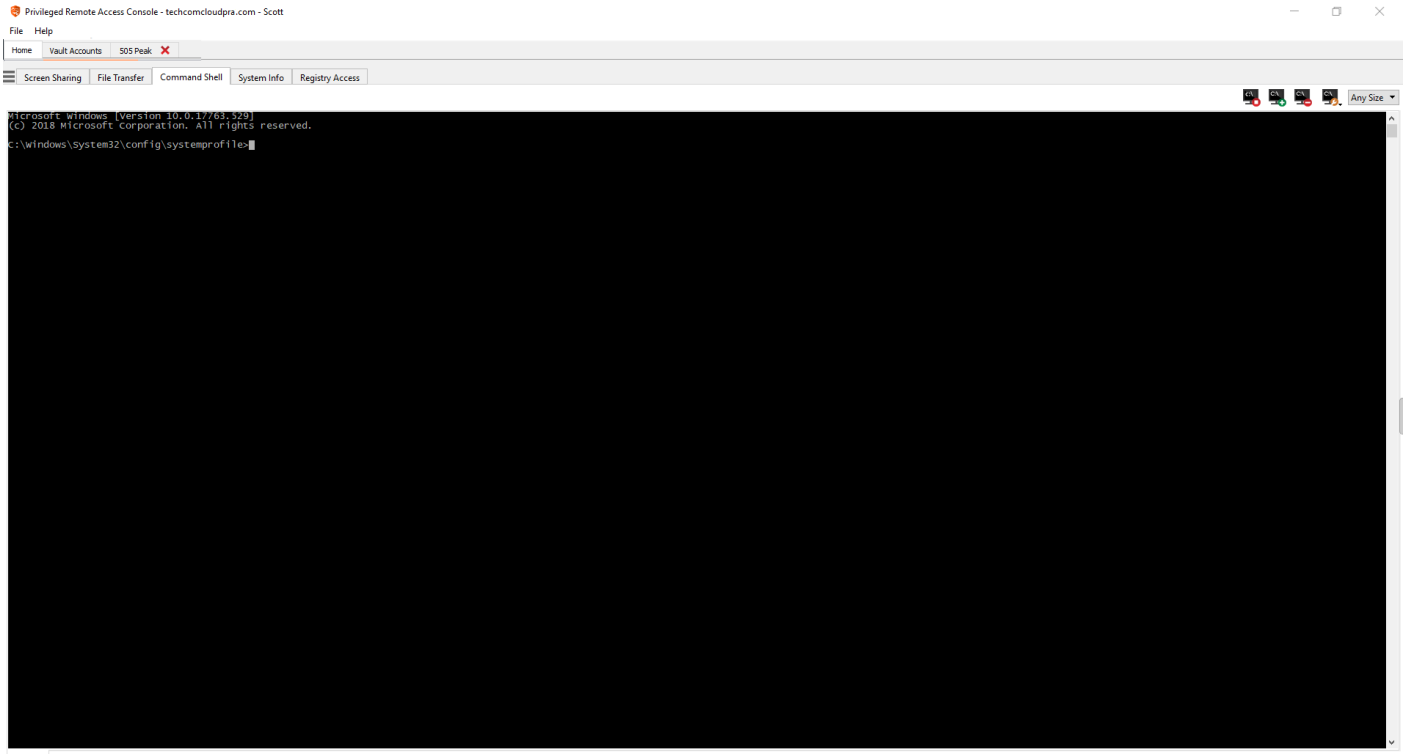
	Zugriff auf das Dateisystem des Remote-Geräts stoppen, wenn es nicht mehr benötigt wird.
	Ein Verzeichnis im ausgewählten Dateisystem nach oben wechseln.
	Ihre Ansicht des ausgewählten Dateisystems aktualisieren.
	Ein neues Verzeichnis erstellen.
	Ein Ordner oder eine Datei umbenennen.
	Ein Verzeichnis 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.

Öffnen Sie die Befehlsshell am Remote-Endpunkt mithilfe der Zugriffskonsole

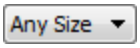
Mit der Remote-Befehlsshell kann ein berechtigter Benutzer eine virtuelle Befehlszeilenschnittstelle für den Remote-Computer öffnen. Der Benutzer kann dann Befehle lokal eingeben, aber diese auf dem Remote-Computer ausführen lassen. Sie können mit mehreren Shells arbeiten. Beachten Sie, dass die dem 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. Wenn Befehlsshell-Aufzeichnung aktiviert ist, ist ebenfalls eine Abschrift der Befehlsshell verfügbar.



Befehlsshell-Tools

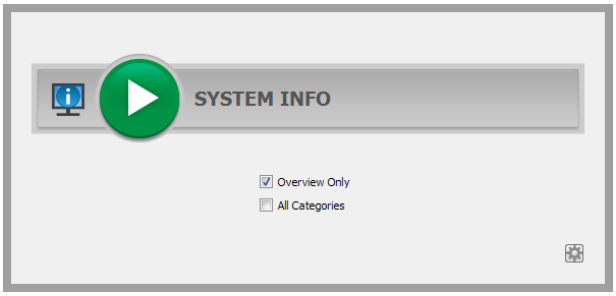
	Zugriff auf die Eingabeaufforderung stoppen, wenn er nicht mehr benötigt ist.
 	Öffnen Sie eine neue Shell, um mehrere Instanzen der Eingabeaufforderung auszuführen, oder schließen Sie einzelne Shells, ohne den Eingabeaufforderungs-Zugriff aufzugeben. Die einzelnen Instanzen werden als Registerkarten 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.

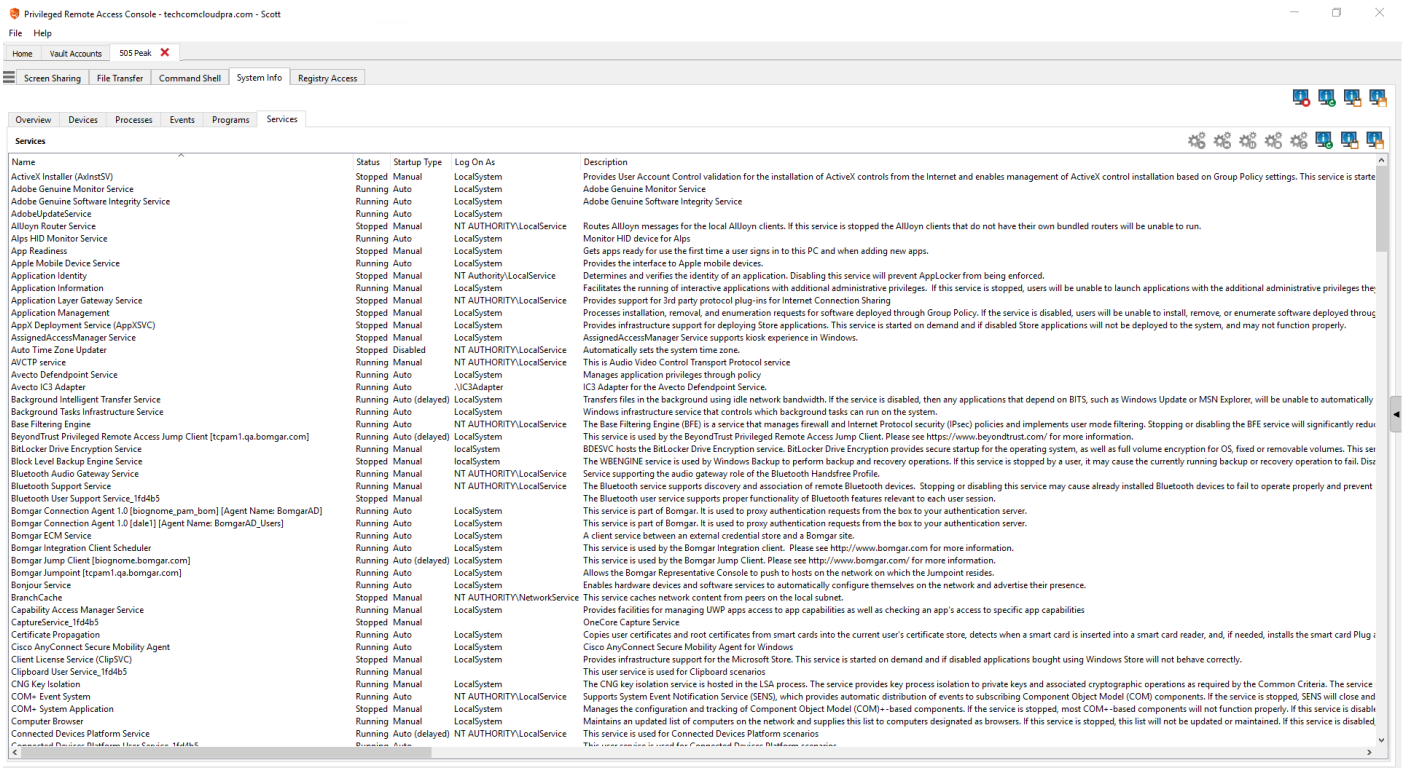
	Greifen Sie auf Tools für die Verwendung in der Befehlszeile zu. Fügen Sie den Inhalt Ihrer Zwischenablage ein, entweder über die Auswahl aus dem Menü oder durch Rechtsklick im Terminalfenster. Kopieren Sie ein Protokoll der aktuellen Shell in Ihre Zwischenablage oder speichern Sie es auf Ihrem Computer. Um einen Teil des Texts zu kopieren, wählen Sie ihn 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 Systeminformationen am Remote-Endpunkt

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.



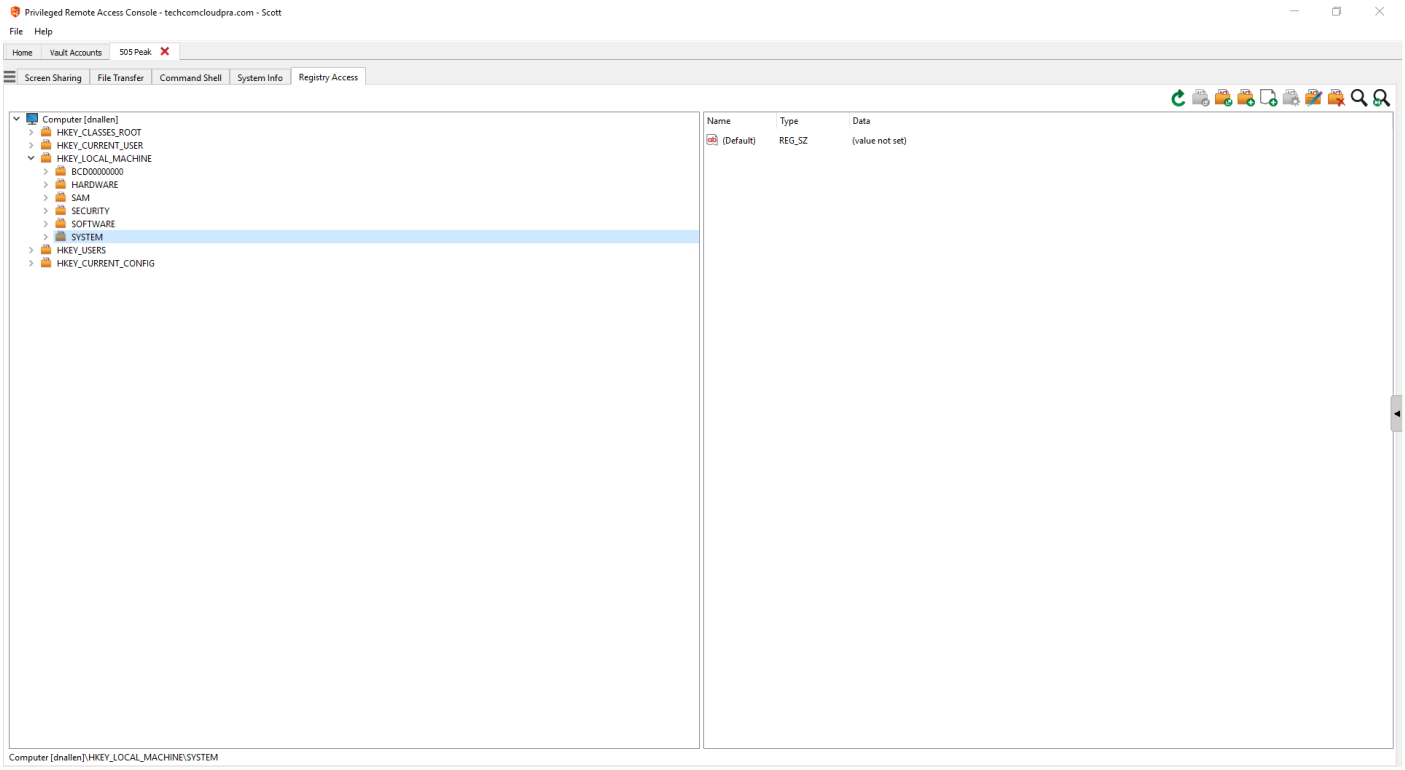


Werkzeuge für Systeminformationen

	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 Registrierungseditor am Remote-Endpunkt

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.



Registrierungseditor-Tools

	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.

Sitzungsverwaltung und Team-Zusammenarbeit

Aktive Zugriffssitzungen anzeigen

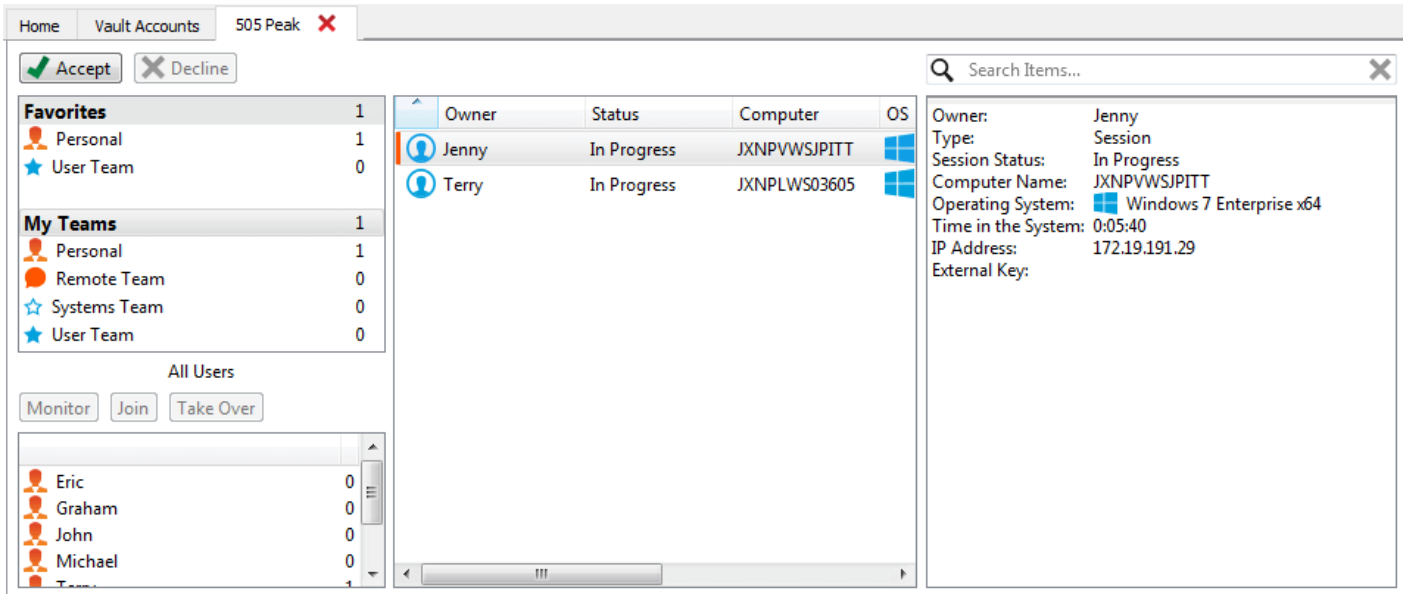
Sitzungswarteschlangen enthalten Informationen über bzw. Zugriff auf aktuell ausgeführte Sitzungen. Die **persönliche** Warteschlange enthält Sitzungen, die Sie aktuell ausführen, sowie Einladungen zum Beitritt einer freigegebenen Sitzung.

Sie haben auch Warteschlangen für Teams, denen Sie angehören. Wenn ein anderer Benutzer ein Mitglied eines Teams zum Beitritt zu einer Sitzung einlädt, erscheint diese Einladung in der Teamwarteschlange. Wenn kein bestimmtes Team ausgewählt ist, können Team-Manager und Teamleiter auch sehen, welche Teammitglieder an Sitzungen teilnehmen.

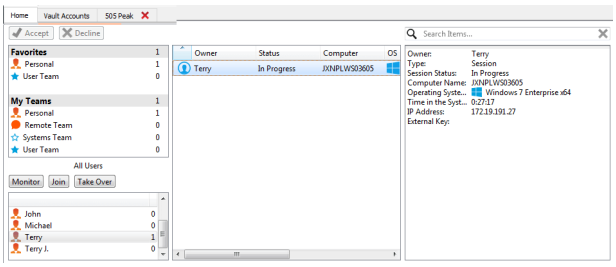
Klicken Sie auf den Stern links neben einem Teamnamen, um diese Warteschlange als Favorit zu markieren. Wenn eine Team-Chatnachricht gesandt wird, erscheint eine orange Chatblase statt des Sterns.

Sortieren Sie Ihre Warteschlangen nach mehreren Kriterien wie z. B. wie lange die Sitzung ausgeführt wird, den Namen des Computers, externer Schlüssel usw. 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 access console merkt sich die Sortierreihenfolge und die Sortierreihenfolge der Sitzungswarteschlange für das nächste Mal, wenn die access console gestartet wird.

Sie können mehrere Sitzungen gleichzeitig ausführen. Oberhalb der access console finden Sie eine Registerkarte für jede offene Sitzung.



Verwenden des Dashboards zur Verwaltung von Teammitgliedern



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 **Teams** der Verwaltungsschnittstelle zugewiesenen Rollen können Teamführer Teammitglieder eines bestimmten Teams überwachen, und Team-Manager können Teamführer sowie die Mitglieder dieses Teams überwachen.

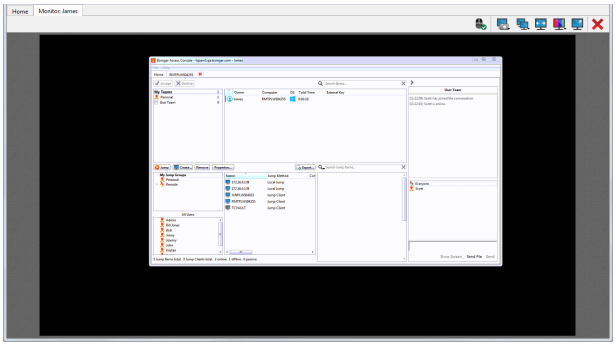
Ist ein Benutzer Team-Manager oder Teamführer eines oder mehrerer Teams, erscheint das Dashboard-Fenster unter dem Fenster der Warteschlangenauswahl auf der Registerkarte **Startseite** der Konsole, wenn eine der Warteschlangen ausgewählt wird. In diesem Fenster werden alle abgemeldeten Teammitglieder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

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.

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.

> ***Hinweis:*** *Der Teamführer kann der Sitzung eines Teammitglieds nur dann beitreten oder sie übernehmen, wenn er über Zugriff auf die Startsitzung für das Jump-Item verfügt, mit dem die Sitzung erstellt wurde, oder die Dashboard-Einstellung zum Beitreten oder Übernehmen ohne Zugriff auf die Startsitzung aktiviert ist.*

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



Ein Symbol wird in der Ecke des Benutzer-Desktops angezeigt, um anzugeben, dass eine Überwachung stattfindet. Wenn der Benutzer seinen Cursor in die Nähe dieses Symbols bewegt, verschiebt sich das Symbol in eine andere Ecke, um den Bildschirm nicht zu verdecken. Wählen Sie den Benutzer, dessen Bildschirm Sie anzeigen möchten, und klicken Sie auf **Überwachen**. Damit wird eine neue Registerkarte in Ihrer Konsole geöffnet, wo die Konsole des Benutzers 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 verwalten, die seiner untergeordnet sind. Es ist aber zu beachten, dass die Rollen strikt auf Teambasis gelten, ein Benutzer kann also unter

Umständen in der Lage sein, einen anderen Benutzer in einem Team zu verwalten, aber nicht den gleichen Benutzer in einem anderen Team.

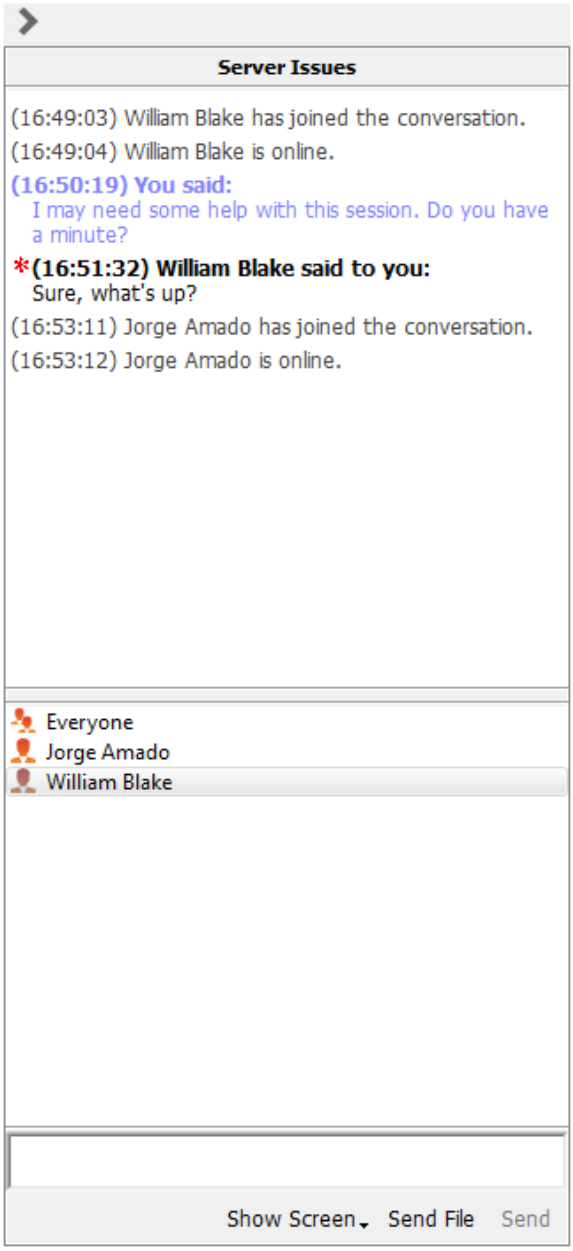
Mit anderen Benutzern chatten

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.

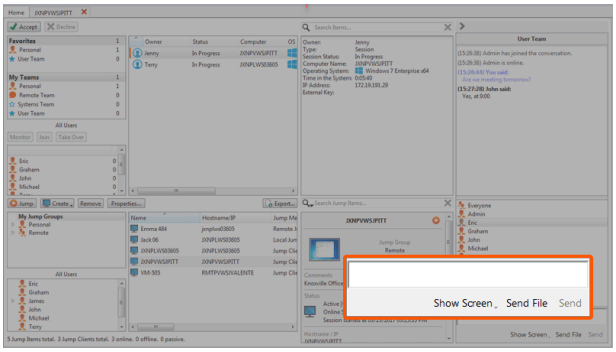
Klicken Sie auf das Pfeilsymbol oben links in der Seitenleiste, um die Schiebe-Seitenleiste einzuklappen. Ist die Schiebe-Seitenleiste eingeklappt, fahren Sie über den Pfeil neben dem verborgenen Fenster, um es anzuzeigen. Klicken Sie auf das Fixierungssymbol, das das Pfeilsymbol oben links in der Seitenleiste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

Beim Tippen werden falsch geschriebene Wörter 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.

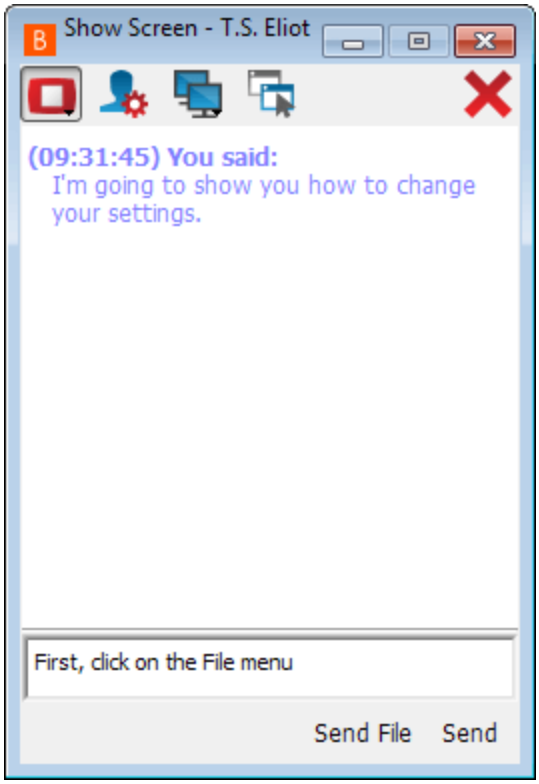


Bildschirm für anderen Benutzer freigeben



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.

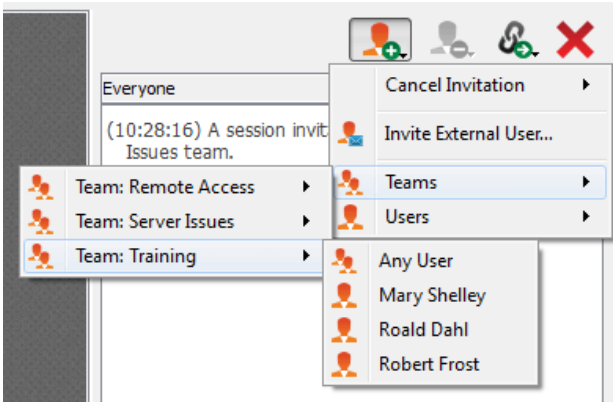
Eine Sitzung für andere Benutzer freigeben

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.

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

Wenn Sie **Jeder Benutzer** wählen, wird die Einladung an die Teamwarteschlange gesandt, sodass jeder einzelne Benutzer im ausgewählten Team an der Sitzung teilnehmen kann. Sie können mehrere Einladungen versenden, wenn mehr Benutzer 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
- 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.

Während einer freigegebenen Sitzung mit anderen Benutzern chatten

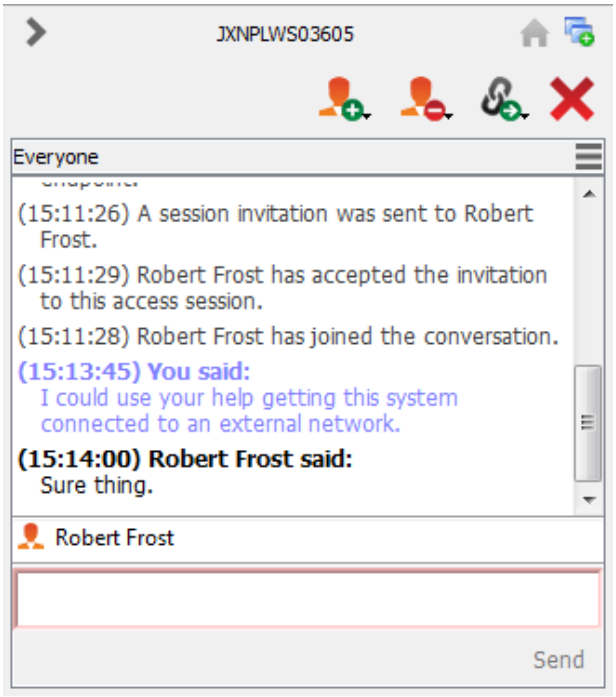
Das Chat-Fenster dient als laufendes Protokoll aller Aktivitäten während der Sitzung, inklusive übertragener Dateien und verwendeter Tools.

Falls ein oder mehrere Benutzer gemeinsam an der Sitzung teilnehmen, können Sie mit den anderen Benutzern chatten. Wenn ein weiterer Benutzer einer freigegebenen Sitzung beitritt, kann er den Chat-Verlauf der letzten Minuten einsehen.

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.

Beim Tippen werden falsch geschriebene Wörter rot unterstrichen. Rechtsklicken Sie zur Anzeige von Rechtschreibungsvorschlägen, oder um diese Schreibweise für die aktuelle Konsolensitzung zu ignorieren.

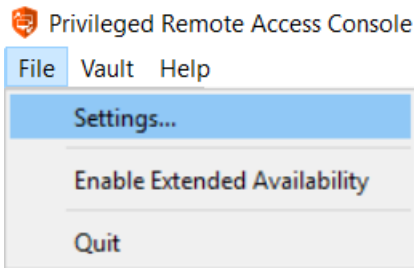
Meldungen werden als einfacher Text im Chat-Eingabebereich angezeigt. Sie können in einer Meldung BBCode-Tags hinzufügen oder bearbeiten, um Text zu formatieren. Die Formatierung wird angewandt, sobald die Nachricht gesendet wurde.



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.*

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.

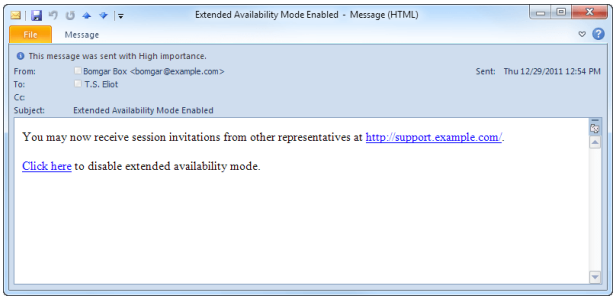


Wenn Ihr Konto für eine erweiterte Verfügbarkeit konfiguriert ist, können Sie die Funktionalität im **Datei**-Menü der access console aktivieren bzw. deaktivieren.

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.

E-Mail-Benachrichtigung und -Einladung

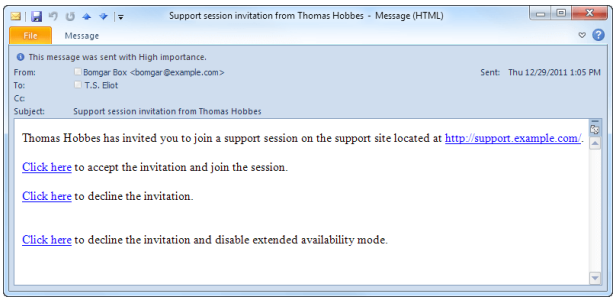
Immer wenn Sie den erweiterten Verfügbarkeitsmodus aktivieren, werden Sie vom B Series Appliance über die in Ihrem Benutzerkonto hinterlegte E-Mail-Adresse darüber benachrichtigt.



> ***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.*

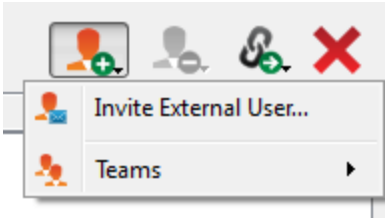
Die Benachrichtigung enthält die URL der Website sowie einen Link zur raschen Deaktivierung des erweiterten Verfügbarkeitsmodus.

Das B Series Appliance 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.



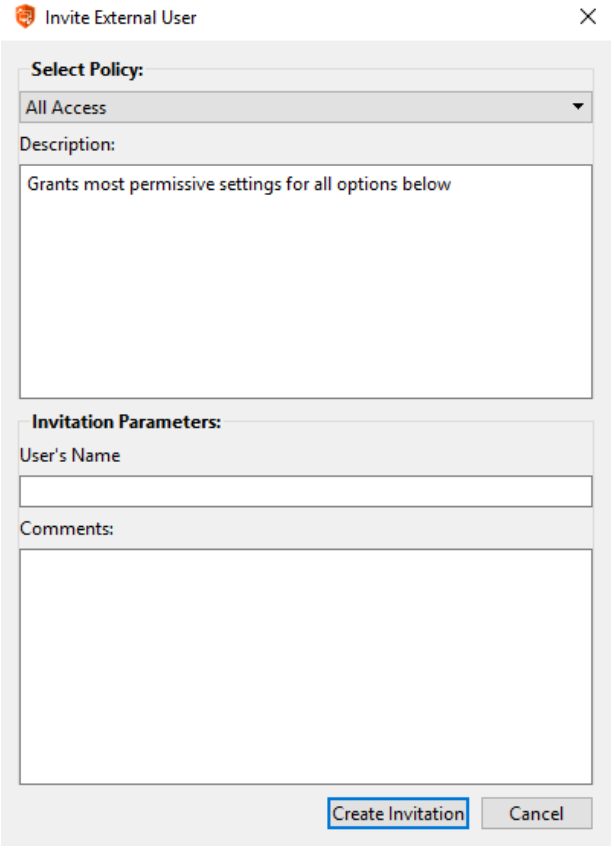
Einladen eines externen Benutzers zur Teilnahme an einer Zugriffssitzung

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 **Externe Benutzer einladen** wählen.

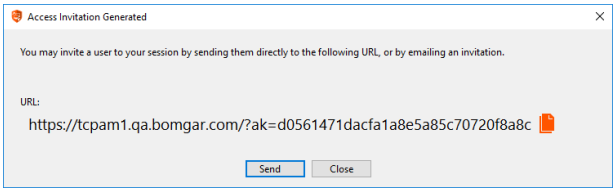


Der Benutzer wird in einem Dialogfeld aufgefordert, eine Sitzungsrichtlinie auszuwählen. Diese Profile werden in der Verwaltungsschnittstelle erstellt und bestimmen, welche Berechtigungen der externe Benutzer hat. Wenn Sie ein Profil auswählen, wird die vollständige Beschreibung darunter angezeigt.

Geben Sie den Namen des eingeladenen Benutzers ein. Dieser Name wird im Chatfenster und in Berichten angezeigt. Geben Sie dann Kommentare dazu ein, warum dieser Benutzer eingeladen wurde. Klicken Sie auf **Einladung erstellen**. Es wird ein neues Dialogfeld mit der Einladungs-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 access console herunterladen und ausführen. Dabei handelt es sich um einen abgekürzten Vorgang, im Gegensatz zur vollständigen Installation der access console.



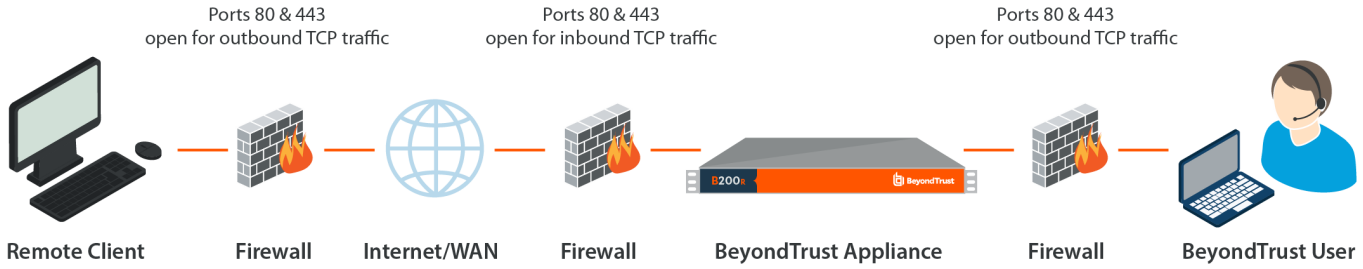
Der externe Benutzer kann nur auf die Registerkarte der jeweiligen Sitzung zugreifen und weist einen beschränkten Berechtigungssatz auf. Der externe Benutzer kann nie der Eigentümer der Sitzung sein. Wenn der einladende Benutzer die Sitzung verlässt, wird der externe Benutzer abgemeldet.

Sie können mehr als einen externen Benutzer zu einer Sitzung einladen.

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 im Installationshandbuch für BeyondTrust Appliance B Series-Hardware.
- 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
    - bomgar-pec-{uid}.exe
    - bomgar-pec.exe

    Unterstützung für die Konfiguration der Firewall erhalten Sie beim Hersteller der Firewall-Software.
- Beispiel-Firewall-Regeln basierend auf dem B Series Appliance-Standort finden Sie unter www.beyondtrust.com/docs/privileged-remote-access/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.