BeyondTrust

Privileged Remote Access 23.2
Zugriffskonsole für Privileged Web Access

TC:12/12/2023

Inhaltsverzeichnis

Handbuch zur Privileged Web-Zugriffskonsole

Mit BeyondTrust Zugriffskonsole für Privileged Web Access können Informations- und Cybersicherheits-Teams berechtigten Benutzern Secure Remote Access auf kritische Systeme gewähren, auch wenn diese Benutzer keine Software innerhalb ihrer eigenen Desktop-Umgebungen installieren können. Stattdessen greifen sie über die webbasierte zugriffskonsole auf Endpunkte zu. Damit wird sichergestellt, dass der notwendige Zugriff stets gewährt werden kann. So erfüllen Systemeigentümer Geschäftsanforderungen wie etwa bezüglich der Systemverfügbarkeit und anderer interner wie externer Vorschriften, ohne dass Verteidigungsmaßnahmen zum Schutz von schadhaften Angriffen außer Kraft gesetzt werden müssen.

In diesem Handbuch besprechen wir die Zugriffskonsole für Privileged Web Access und erläutern, wie diese browserbasierte zugriffskonsole unter Beibehaltung eines Höchstmaßes an Sicherheit auf Endpunkte zugreift und andere nötige Funktionen durchführt.

> ***Hinweis:*** *Verwenden Sie dieses Handbuch erst, wenn die anfängliche Einrichtung und Konfiguration des B Series Appliance durch einen Administrator abgeschlossen wurde, entsprechend der Beschreibung im BeyondTrust Appliance B Series Installationshandbuch für Hardware. Sollten Sie Hilfe benötigen, wenden Sie sich bitte an BeyondTrust Technical Support unter www.beyondtrust.com/support.*

Voraussetzungen für die Privileged Web-Zugriffskonsole

Damit die Zugriffskonsole für Privileged Web Access auf Ihrem System ausgeführt werden kann, muss das B Series Appliance mit Software-Version 15.3 oder höher ausgeführt werden. Die Zugriffskonsole für Privileged Web Access wird auf den folgenden Plattformen und Browsern unterstützt:

Plattformen

- Windows
- Macintosh
- Linux

Browser

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

WICHTIG!

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

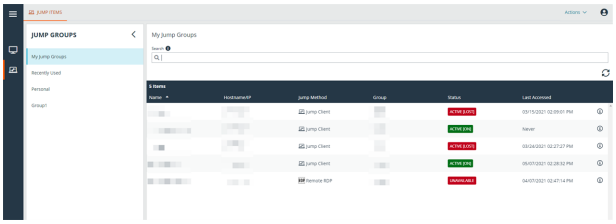
Starten der Web-Zugriffskonsole

Mit Zugriffskonsole für Privileged Web Access können Sie sicher Ihre Endpunkte hinzufügen, darauf zugreifen, sie bearbeiten und löschen, indem Sie über B Series Appliance eine Remote-Verbindung zu ihnen herstellen. Um die Zugriffskonsole für Privileged Web Access zum Zugriff auf Endpunkte zu verwenden, starten Sie die Konsole mithilfe der unten beschriebenen Schritte.

Starten der Web-Zugriffskonsole mit /console

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

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



FIDO2-zertifizierte Authentifizierer können für die sichere Anmeldung ohne Eingabe Ihres Passworts auf der Desktop-zugriffskonsole (nur Windows), Zugriffskonsole für Privileged Web Access und der Verwaltungsschnittstelle /login verwendet werden. Sie können bis zu 10 Authentifizierer registrieren.

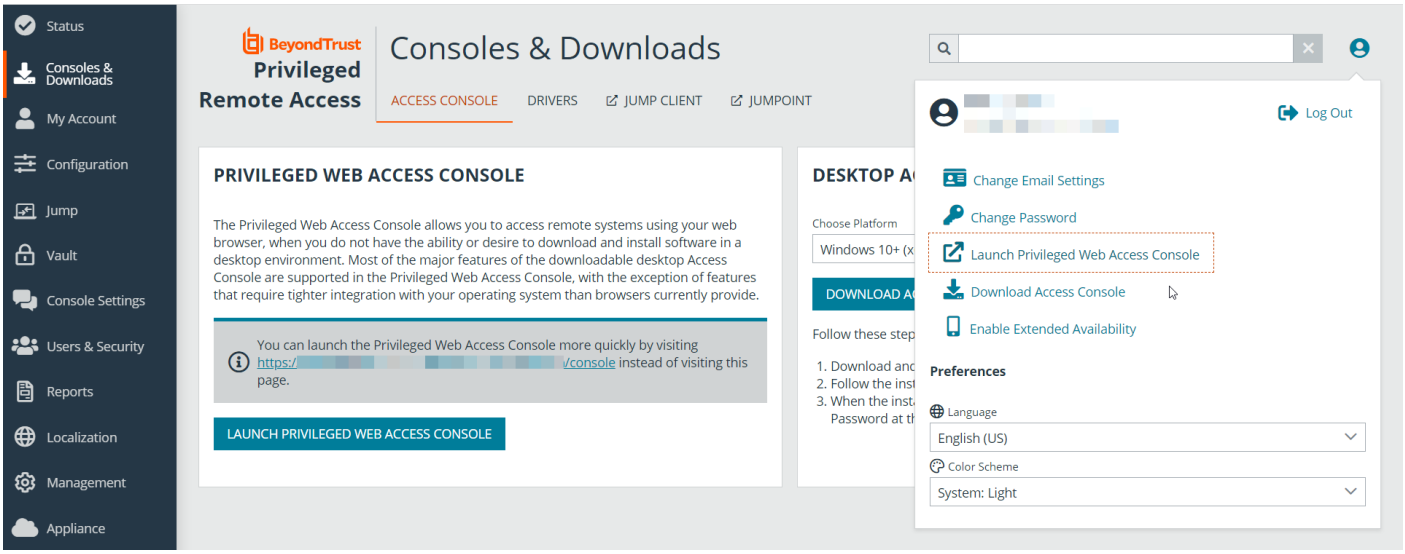
Wenn die passwortlose Anmeldung aktiviert wurde, kann **Authentifizierung über** auf **Passwortlos FIDO2** voreingestellt werden oder es kann ausgewählt werden. Der genaue Ablauf der passwortlosen Anmeldung hängt von der Art des Geräts und dem Hersteller ab.

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

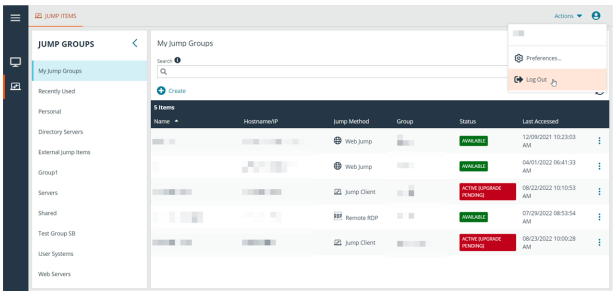
Starten der Web-Zugriffskonsole mit /login

> ***Hinweis:*** *Standardmäßig ist diese Option nicht verfügbar. Um die Webkonsole über die Verwaltungsschnittstelle /login zu starten, müssen Sie zu* ***Verwaltung > Sicherheit*** *navigieren und* ***Mobiler Zugriffskonsole und Zugriffskonsole für Privileged Web Access Verbindung gestatten*** *aktivieren.*

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



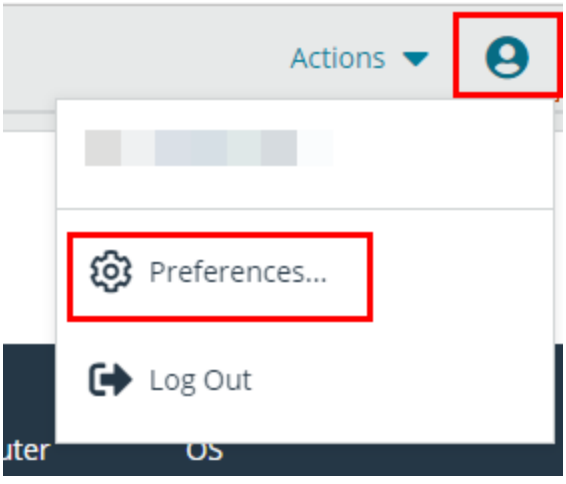
4. Klicken Sie auf **Zugriffskonsole für Privileged Web Access starten** auf dem Bildschirm **Konsolen & Downloads** oder im Fenster mit den Benutzeroptionen.
5. Die Zugriffskonsole für Privileged Web Access wird in einer neuen Registerkarte geöffnet und Sie können mit der Arbeit auf Endpunkten beginnen.



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

Zugriffskonsole für Privileged Web Access-Einstellungen

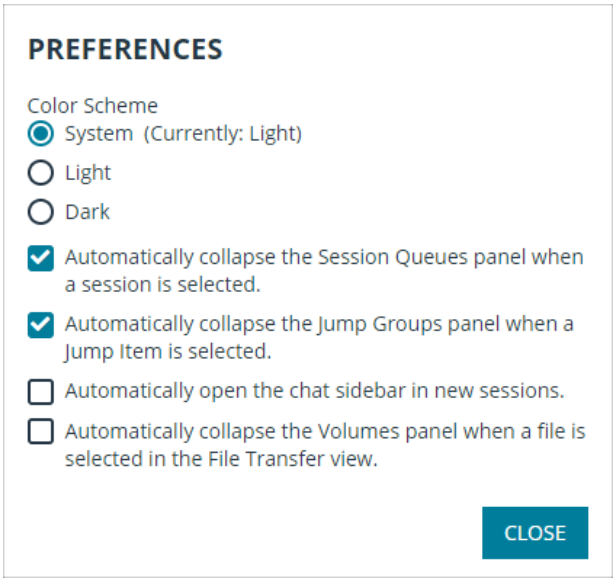
Die Sprach- und Farbschemaoptionen, die beim Klicken auf das Benutzersymbol in der Verwaltungsschnittstelle /login sichtbar sind, betreffen nur diese Schnittstelle. Um die Einstellungen im Web-zugriffskonsole festzulegen, klicken Sie auf das Benutzersymbol in der oberen rechten Ecke des Web-zugriffskonsole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



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

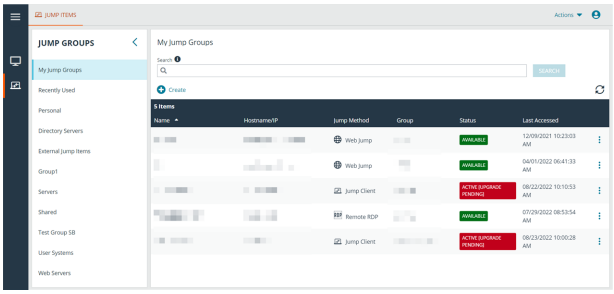
Wählen Sie eine der automatischen Optionen, die Sie verwenden möchten:

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



Verwenden von Jump-Elementen zum Zugriff auf Endpunkte in der Privileged Web-Zugriffskonsole

Um auf einen Endpunkt zuzugreifen, installieren Sie ein Jump Item. Um ein Jump Item zu installieren, tippen Sie auf **Erstellen** oben in der Jump-Schnittstelle. Die vollständigen Einzelheiten, wie man Jump-Items erstellt, finden Sie weiter hinten in diesem Handbuch. 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 genauso wie Jump-Item-Verknüpfungen.



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.

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.

Mit dem Zugriff auf Endpunkte können Sie über drei Wege beginnen:

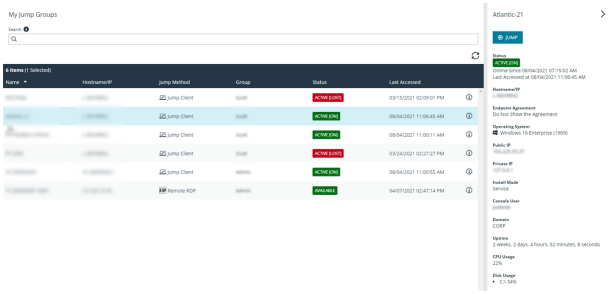
- Lokalisieren und wählen Sie einen Endpunkt aus der Liste **Meine Jump-Gruppen**.
- Wählen Sie eine Jump-Gruppe und dann einen Endpunkt aus der Liste der Endpunkte der Gruppe aus.
- Wählen Sie eine Sitzung aus der Liste **Häufig verwendete Jump-Elemente**.

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

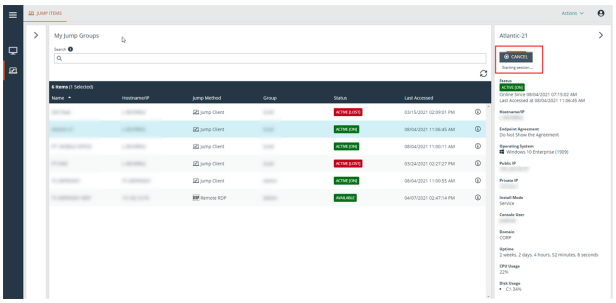
> ***Hinweis:*** *Die Liste der Jump-Items kann nur maximal 50 Jump-Items anzeigen.*

Um mit dem Zugriff auf Jump-Elemente zu beginnen, folgen Sie den unten beschriebenen Schritten:

1. Wählen Sie eine Jump-Gruppe und klicken Sie auf die Schaltfläche **Aktualisieren**.
2. Eine Liste aller Jump-Elemente wird angezeigt und Sie können die Details zum Jump-Element einsehen, einschließlich: **Name**, **Methode**, **Gruppe**, **Status** und **Letzter Zugriff**. Um mehr Einzelheiten über das Jump-Element anzuzeigen, klicken Sie auf das Plussymbol neben dem Namen des Jump-Elements.
3. Klicken Sie auf die Schaltfläche **JUMP**, um eine Sitzung mit dem Endpunkt zu starten.



4. Um eine Jump-Zugriffsanforderung zu stornieren, klicken Sie auf **Abbrechen**.

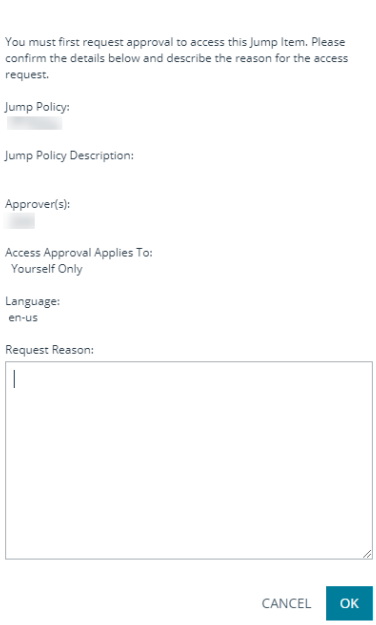


Autorisierung durch Endbenutzer oder Drittpartei

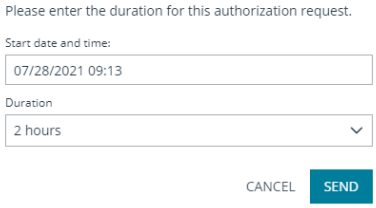
Abhängig von der Konfiguration von Jump-Elementen innerhalb der /login-Verwaltungsschnittstelle kann ein Jump-Element über eine zugeordnete Jump-Richtlinie verfügen. Die Richtlinie kann eine Autorisierungskomponente definieren, die Sie zwingt, eine Berechtigung von Dritten oder einem Administrator anzufordern, bevor eine Zugriffssitzung mit dem Jump-Element begonnen werden kann.

Weitere Informationen über die Konfiguration von Dritt- und Endbenutzerbenachrichtigungen und -genehmigungen finden Sie unter Jump-Richtlinien: Zeitpläne, Benachrichtigungen und Genehmigungen für Jump-Elemente festlegen unter https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/jump-policies.htm.

1. Nachdem auf die **JUMP**-Schaltfläche geklickt und der Zugriff angefordert wurde, erscheint eine Aufforderung und Sie müssen einen Grund für den Zugriff auf das System eingeben.



2. Als nächstes müssen Sie angeben, wann und für wie lange Sie auf das System zugreifen wollen.
3. Nach dem Absenden der Anfrage wird die Drittpartei oder Person, die für die Genehmigung von Zugriffsanforderungen verantwortlich ist, per E-Mail benachrichtigt und hat die Gelegenheit, die Anfrage zu akzeptieren oder abzulehnen. Obwohl andere Genehmiger die E-Mail-Adresse der genehmigenden oder ablehnenden Person sehen können, kann der Anforderer dies nicht.

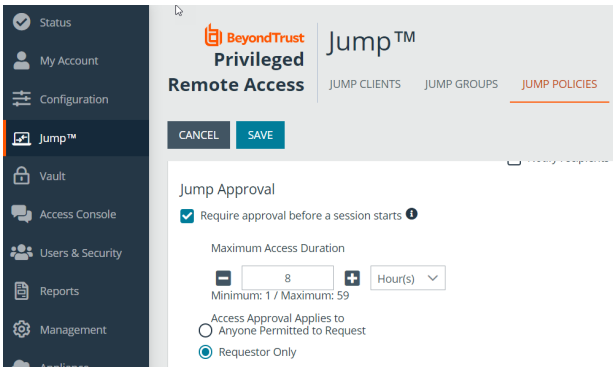


4. Nach Festlegen der Berechtigung erscheint eine Autorisierungsbenachrichtigung innerhalb der Jump-Element-Informationen und gibt entweder *Genehmigt* oder *Abgelehnt* an. Wird der Zugriff genehmigt, können Sie auf die Jump-Schaltfläche tippen, um mit dem Zugriff auf das System zu beginnen.
5. Dann sehen Sie eine Meldung, die Sie fragt, ob Sie eine Zugriffssitzung beginnen möchten.
6. Wenn Sie die Sitzung beginnen möchten, erscheinen die Kommentare der genehmigenden Partei und Sie können mit dem Zugriff auf das System beginnen.

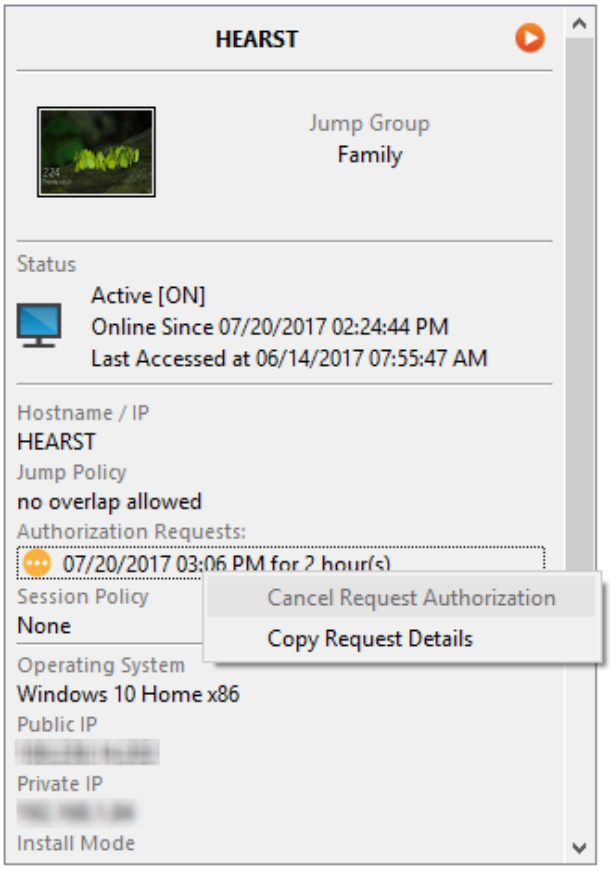
Widerruf einer Zugriffs-Genehmigungsanfrage

Die Berechtigung, genehmigte Zugriffsanforderungen zu widerrufen, wird durch die Jump-Richtlinie geregelt. Alle Benutzer, die Anfragen im Rahmen der Jump-Richtlinie genehmigen können, können abhängig von der Genehmigungsart Anfragen stornieren. Gehen Sie in der Web-Verwaltungsschnittstelle **/login** auf **Jump > Jump-Richtlinien**. Unter **Jump-Genehmigung** haben Sie zwei Optionen:

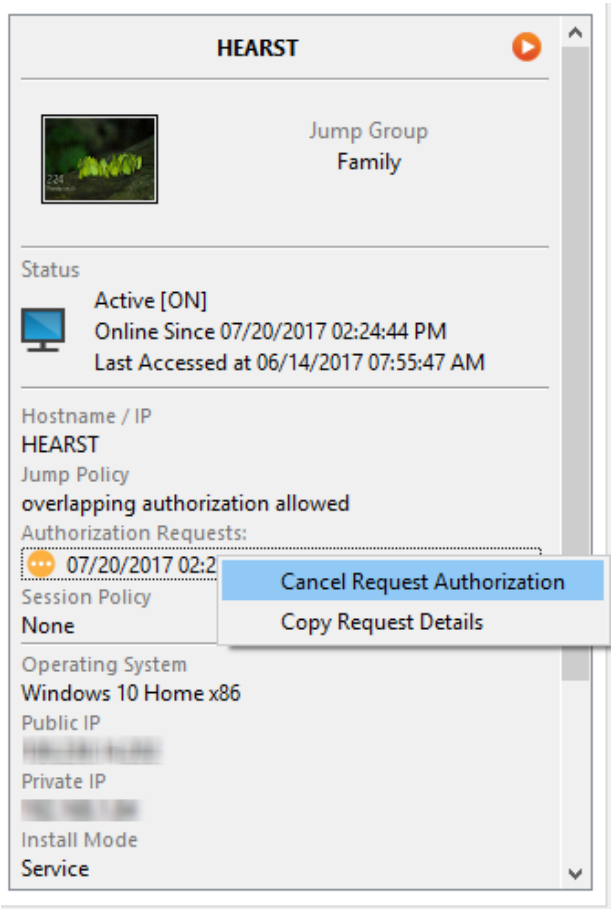
- **Jeden, der anfordern darf**
- **Nur Anforderer**



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.



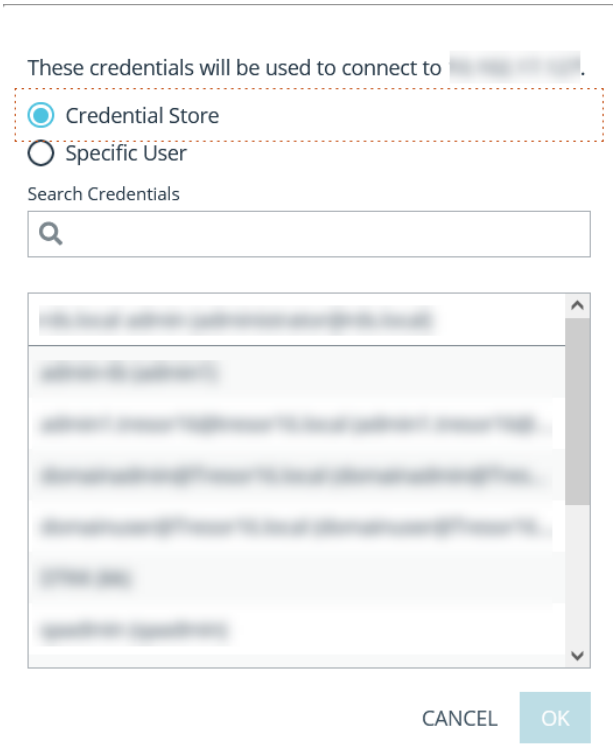
Wenn die Jump-Richtlinie jedoch auf **Jeder mit Anforderungsberechtigung** eingestellt ist und eine Zugriffsanforderung derzeit für Benutzer A genehmigt ist, ist Benutzer B berechtigt, eine neue Sitzung mit dem Jump-Item zu starten, wenn er versucht, einen Jump zu ihm durchzuführen. Außerdem kann jeder,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



Daten zur automatischen Anmeldung

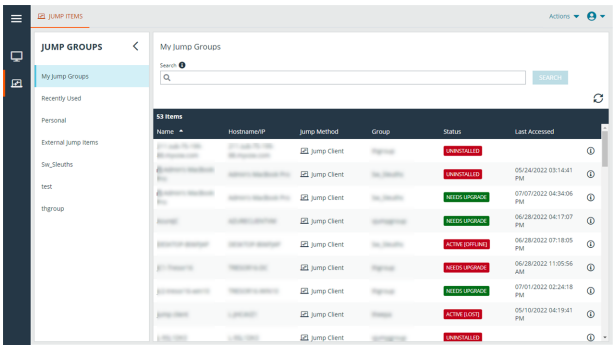
Anmeldedaten des **Endpunkt-Anmeldedatenmanagers** können für die RDP-Anmeldung und zur Durchführung von Remote-Jumps verwendet werden. Möchte ein Benutzer einen Jump zu einem Remote-Jump- oder Remote-RDP-Element durchführen und es stehen keine automatischen Anmeldedaten zur Verfügung, muss ein Benutzername und ein Passwort in die Aufforderung eingegeben werden, bevor die Zugriffssitzung mit dem Endpunkt beginnen kann. Wenn die /login-Verwaltungsschnittstelle für Anmeldedaten für die automatische Anmeldung konfiguriert wurde und nur ein Satz von Anmeldedaten für einen bestimmten Benutzer und ein Jump-Element als verfügbar zurückgegeben wird, wird die Anmeldedatenanforderung übersprungen und die Anmeldedaten werden zum Start der Sitzung verwendet. Ist mehr als ein Satz von Anmeldedaten in der /login-Verwaltungsschnittstelle konfiguriert wurden, kann der Benutzer entweder Anmeldedaten vom Anmeldedatenspeicher wählen oder manuell seine eigenen Anmeldedaten eingeben.

Weitere Informationen zur Konfiguration und Verwaltung von Anmeldedaten finden Sie unter Sicherheit: Verwalten der Sicherheitseinstellungen unter www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/security.htm.

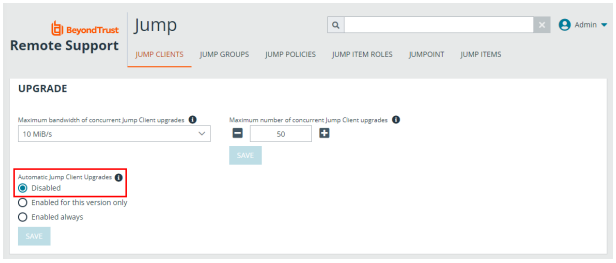


Jump-Client-Upgrade

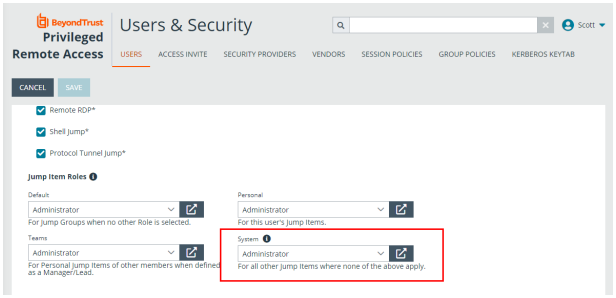
Sie können die Jump-Clients in Zugriffskonsole für Privileged Web Access aktualisieren. Ein **Benötigt Upgrade**-Banner wird unter **Status** angezeigt, grün, wenn der Jump-Client online ist, rot, wenn er offline ist. Sie können nur Jump-Clients aktualisieren, die online sind. Um einen bestimmten Jump-Client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



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



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



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-Item-Links.

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

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

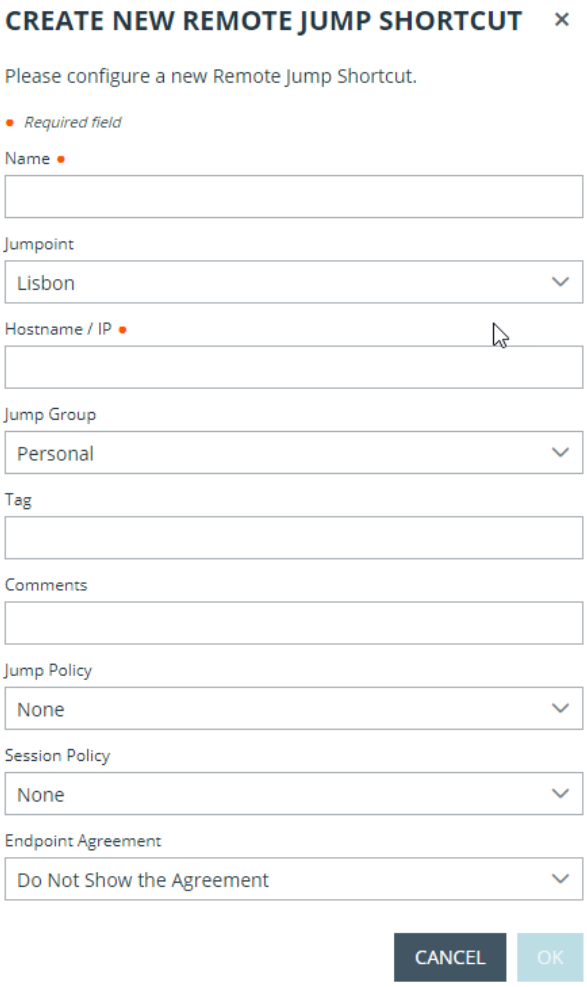
Verschieben Sie Jump-Elemente von einer Jump-Gruppe in eine andere mithilfe des Dropdown-Menüs **Jump-Gruppe**. Die Fähigkeit, Jump-Elemente in oder aus unterschiedlichen Jump-Gruppen zu verschieben ist von Ihren Kontoberechtigungen abhängig.

Organisieren Sie Jump-Elemente eingehender, indem Sie den Namen eines neuen oder bestehenden **Tag**s eingeben. Obwohl die ausgewählten Jump-Items 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 einen symbolische Jump-Link zum Starten einer Sitzung zu verwenden, wählen Sie den symbolischen Link einfach aus der Jump-Schnittstelle und klicken Sie auf die Schaltfläche **Jump**.

Es öffnet sich für Sie ein Dialogfeld, in dem Sie Administrator-Anmeldedaten für den Remote-Computer eingeben müssen, 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: *Da ein Remote Jump versucht, eine direkte Verbindung über das Gerät herzustellen, muss der Endcomputer ebenfalls mit dem Gerät kommunizieren können. Wenn dies nicht der Fall ist, können Sie die Funktion Jump Zone Proxy verwenden, um den Datenverkehr über den Jumpoint zu leiten.*

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**.

Hinweis: *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.*

WICHTIG!

Um Ihr eigenes Tool verwenden zu können, müssen Sie ***Protocol Tunnel Jump*** *in* ***/login > Benutzer & Sicherheit > Benutzer > Jump Technology > Protocol Tunnel Jump*** *aktivieren.*

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-Item-Links.

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

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

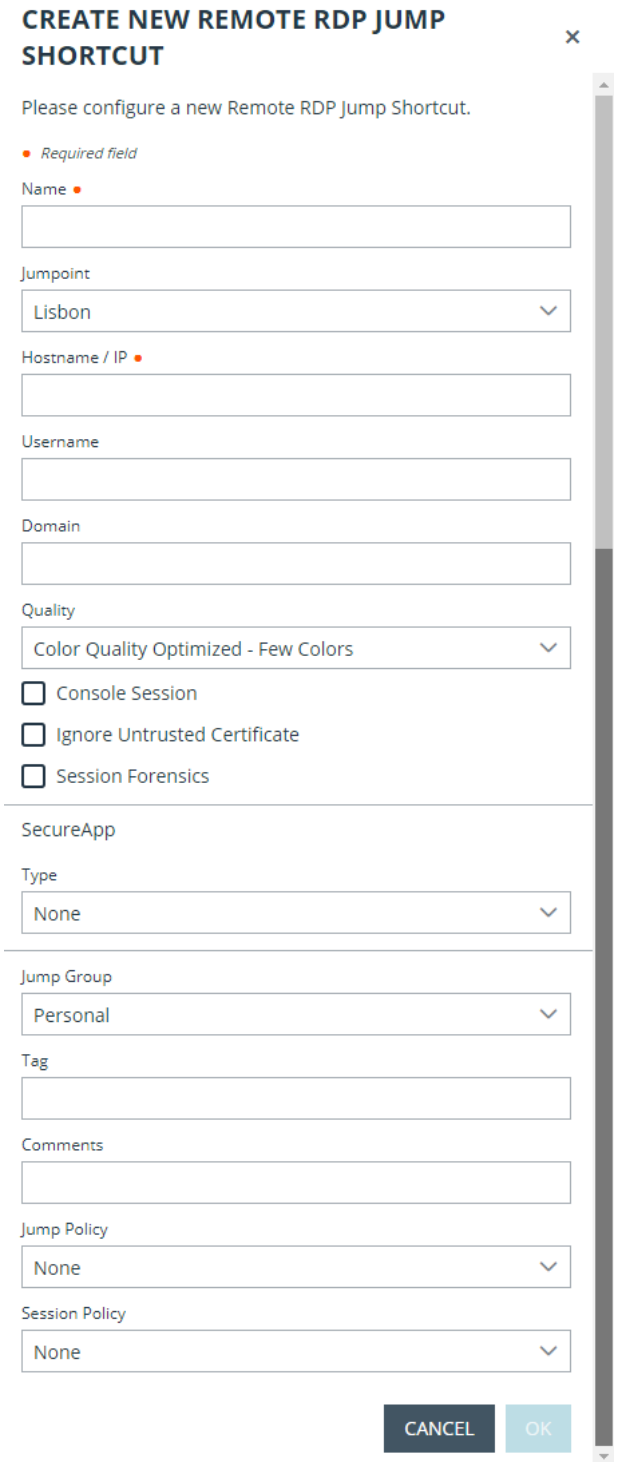
Wählen Sie im Dropdown-Menü **Jumpoint** das Netzwerk aus, in dem sich der Computer befindet, auf den Sie zugreifen möchten. Die zugriffskonsole merkt sich Ihre Jumpoint-Auswahl für das nächste Mal, wenn Sie diese Art von Jump-Element erstellen. Geben Sie den **Hostnamen / die IP** des Systems ein, auf 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* ***BeyondTrust Remote Desktop Agent*** *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 den verwendeten Jumpoint 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-Service-Konto muss für diesen Jumpoint eingerichtet werden. Werden diese Voraussetzungen nicht erfüllt, schlagen alle Versuche, eine Sitzung zu starten, fehl.

> ***Hinweis:*** *In üblichen Installationen benötigt das RDP-Service-Konto Berechtigungen, einschließlich des Zugriffs zum Erstellen und Steuern von Remote-Diensten und des Schreibzugriffs auf Remote-Dateisysteme. Wir empfehlen Ihnen, ein AD-Konto zu erstellen und die AD-Gruppenrichtlinieneinstellungen zu verwenden, um die Berechtigungen zu konfigurieren. Die genauen erforderlichen Berechtigungen hängen jedoch von Ihrer AD-Konfiguration ab.*

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** ist 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 Passwort-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%	passwort
%PASSWORDRAW%	Passwort (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-Items 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.

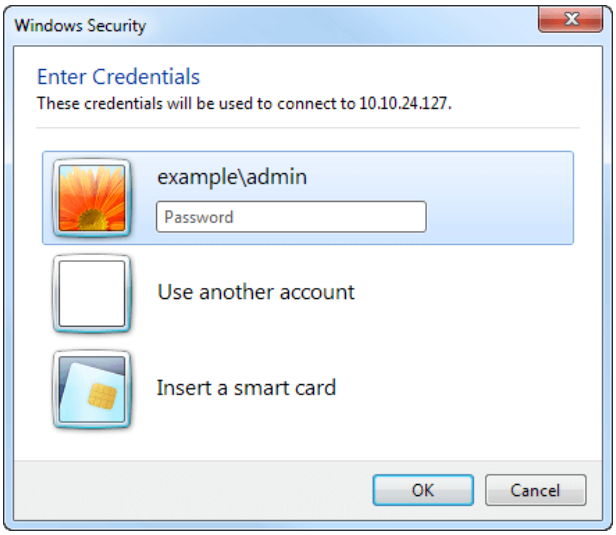
Um festzulegen, wann Benutzer auf dieses Jump-Element zugreifen können, ob eine Zugriffsbenachrichtigung gesendet werden sollte oder ob eine Berechtigung oder eine Ticket-ID Ihres externen Ticketsystems zur Verwendung dieses Jump-Elements notwendig ist, wählen Sie **Jump-Richtlinie**. Diese Richtlinien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

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



Jetzt beginnt Ihre RDP-Sitzung.

***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, die Befehle **Alt** und **Shift** verwenden 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- oder Linux-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.

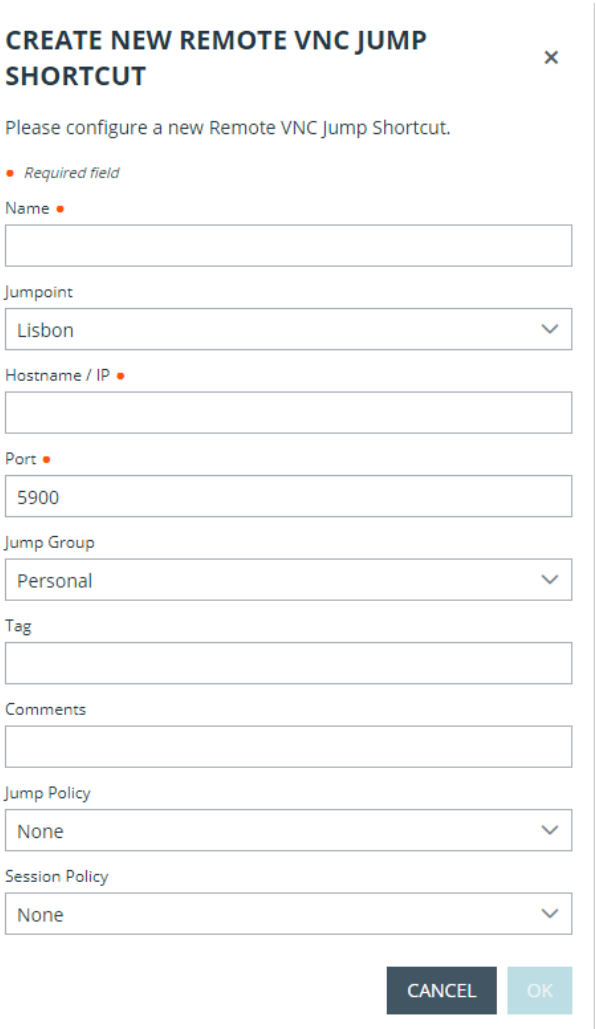
Organisieren und verwalten Sie bestehende Jump-Elemente, indem Sie einen oder mehrere Jump-Clients auswählen und auf **Eigenschaften** klicken.

> ***Hinweis:*** *Um die Eigenschaften mehrerer Jump-Items anzuzeigen, müssen die 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 zugriffskonsole 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-Items 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 einen symbolische Jump-Link zum Starten einer Sitzung zu verwenden, wählen Sie den symbolischen Link einfach aus der Jump-Schnittstelle und klicken Sie auf die Schaltfläche **Jump**.

Beim Aufbau der Verbindung zum VNC-Server versucht das System festzulegen, ob es verbundene 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.*

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 beispielsweise 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.

Hinweis: *Für das SSH-Protokoll können Sie Ihr eigenes SSH-Tool verwenden. Weitere Informationen finden Sie in* *„Einstellungen und Voreinstellungen in der Zugriffskonsole ändern“ auf Seite 1**.*

WICHTIG!

Um Ihr eigenes Tool verwenden zu können, müssen Sie ***Protocol Tunnel Jump*** *in* ***/login > Benutzer & Sicherheit > Benutzer > Jump Technology > Protocol Tunnel Jump*** *aktivieren.*

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 genauso wie Jump-Clients und anderen Arten von symbolischen Jump-Item-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-Items anzuzeigen, müssen die 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 zugriffskonsole 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**.

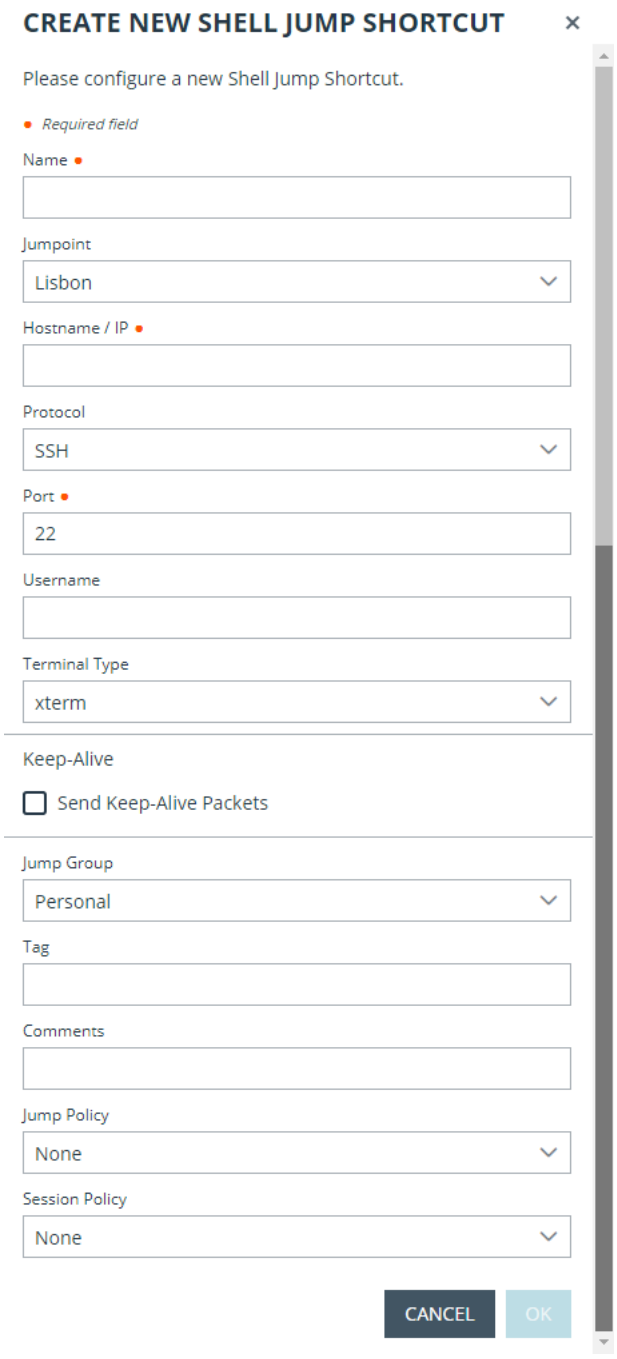
Sie können auch das **Senden von leeren Datenpaketen** aktivieren, damit inaktive Sitzungen nicht beendet werden. Geben Sie die Anzahl der Sekunden an, für die zwischen jeder Paketaussendung gewartet werden soll.

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

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

Administratoren können die Befehlsfilterung an Shell Jump Items 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.

> ***Hinweis:*** *Der Befehlsfilter von BeyondTrust verwendet erweiterte reguläre Ausdrücke, die jedoch nicht mit* ***egrep*** *zu verwechseln sind. Weitere Informationen finden Sie in Reguläre Ausdrücke (C++) 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-Items 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**. Es wird ein Hinweis angezeigt, ob die von Ihnen eingegebene Shell-Eingabeaufforderung einem der regulären Ausdrücke auf der Liste entspricht.*

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. Es wird ein Hinweis angezeigt, 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 (Passwort oder SSH-Schlüssel).
- Die Konto-Anmeldedaten im Endpunkt-Anmeldedaten-Manager (ECM) 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 Passworts als root ausgeführt werden können (**NOPASSWD**).

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

Als nächstes muss ein Administrator den ECM und/oder das Passwort-Vault konfigurieren, um Benutzern Zugriff auf die jeweiligen funktionalen Konten für das Jump Item 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 ECM 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!

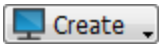
Flash wird von Web Jump nicht unterstützt. Beachten Sie Ihre Hypervisor-Dokumentation und aktualisieren Sie sie auf eine Version, die HTML5 unterstützt.

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

Erstellen eines symbolischen Web-Jump-Links

***Hinweis:** Stellen Sie vor der Erstellung von Web Jump-Verknüpfungen sicher, dass Ihr Benutzerkonto die Möglichkeit hat, auf Web Jumps zuzugreifen. Diese Berechtigung wird in Ihrem Benutzerkonto in der /login-Schnittstelle unter **Zugriffsberechtigungen > Jump Technology** festgelegt.*

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-Item-Links.



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

***Hinweis:** Um die Eigenschaften mehrerer Jump-Items anzuzeigen, müssen die ausgewählten Elemente vom gleichen Typ sein (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** den Windows- oder Linux-Jumpoint aus, der den Computer hostet, auf den Sie zugreifen möchten.

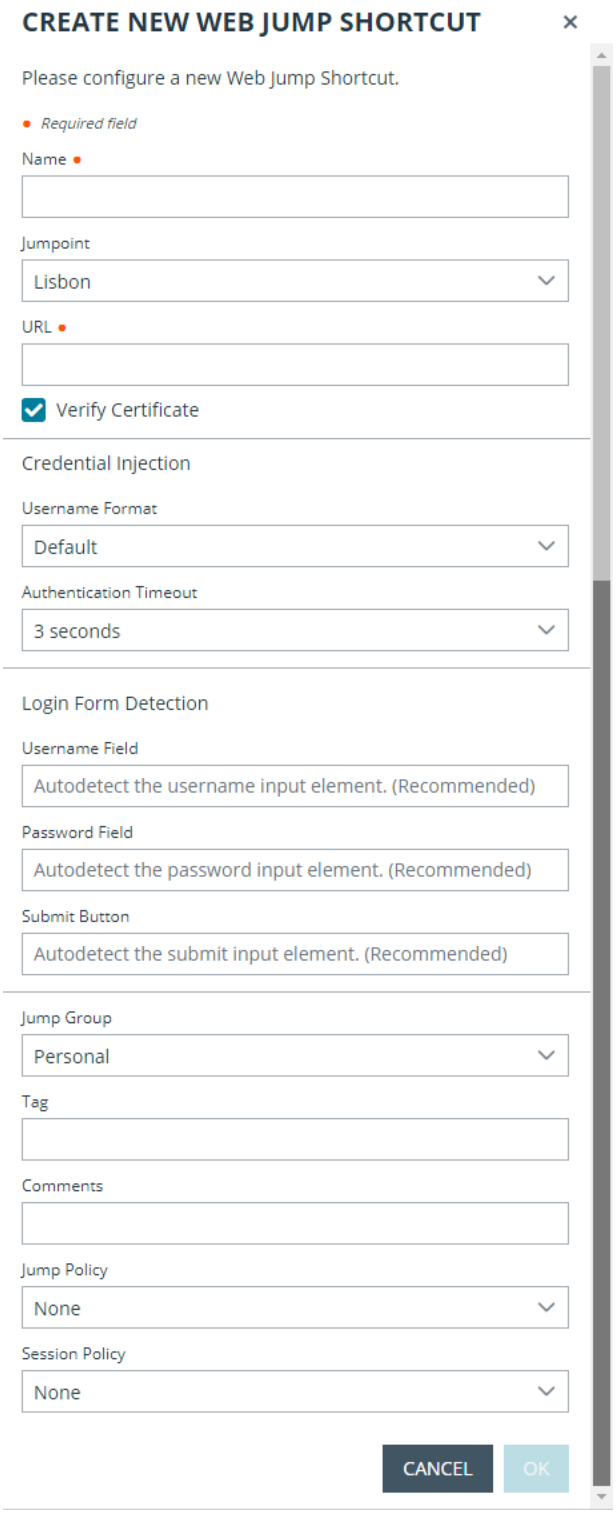
> ***Hinweis:*** *Die Funktion Kopieren/Einfügen wird für Linux-Jumpoints nicht unterstützt.*

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.

Unter **Erkennung des Anmeldeformulars** wird empfohlen, die drei Felder leer zu lassen und dem System zu erlauben, die bereits gespeicherten Informationen für die Anmeldung automatisch zu erkennen und zu verwenden. Wenn die automatische Erkennung fehlschlägt, scheitert die Eingabe und eine Meldung besagt, dass das Feld **Benutzername**, das Feld **Passwort** und/oder die Schaltfläche **Senden** nicht gefunden werden konnte.

Wenn Sie die Namen der Eingabeelemente eingeben, geben Sie die HTML-id, den HTML-Namen oder den CSS-Selektor für jedes Element auf der Anmeldeseite ein.

***Example:** Dies zeigt HTML-ids mit Eingabefeldern und einer Schaltfläche „Abschicken“, wie sie in der Codeansicht einer Anmeldeseite erscheinen könnten. Die HTML-ids lauten hier **user**, **pwd** und **button**.*

```
<form action="/action_page.php">
Benutzername: <input type="text" id="user"><br>
Passwort: <input type="password" id="pwd"><br>
<input type="submit" value="Submit" id="button">
</form>
```

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-Items 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.

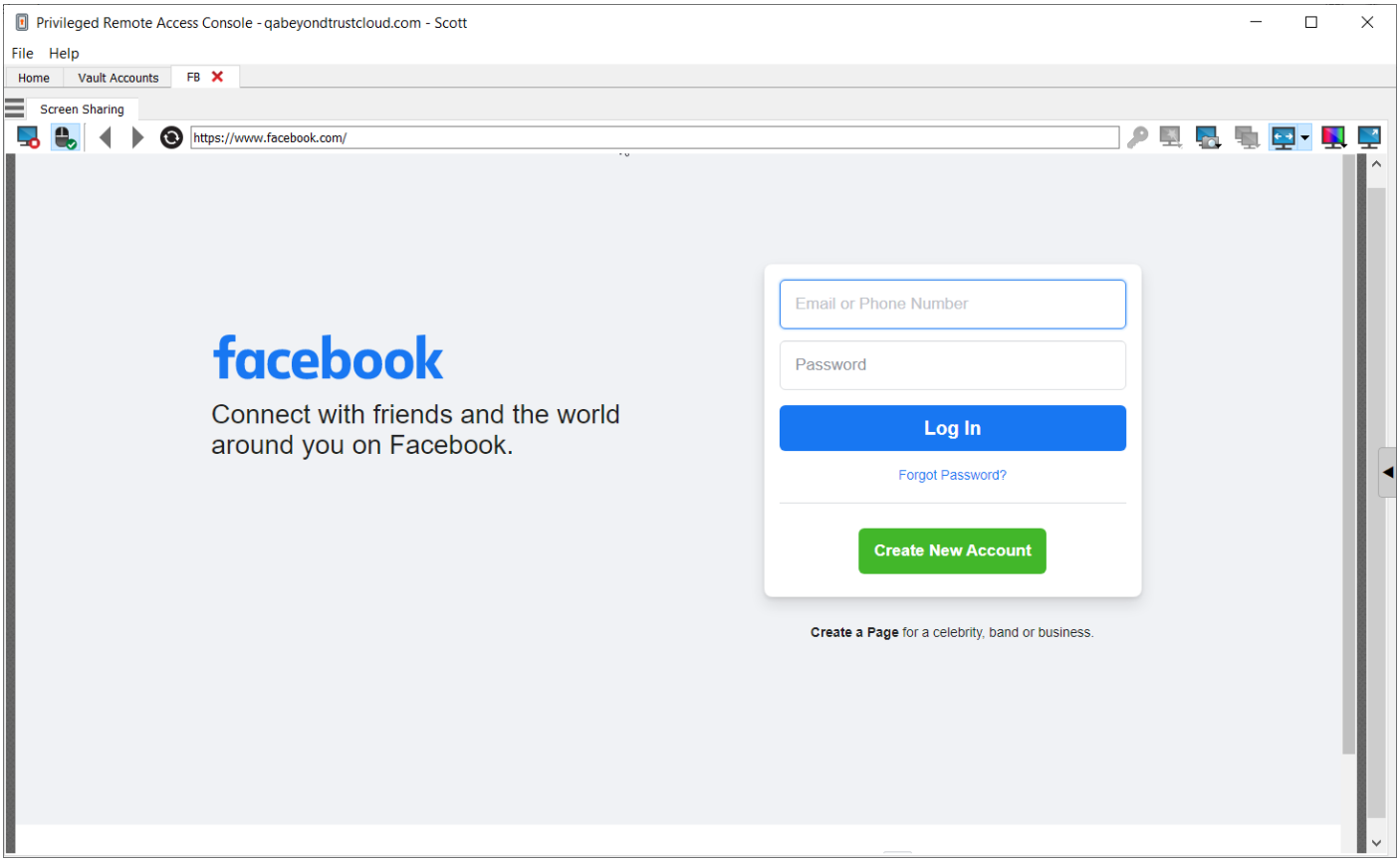
Wählen Sie eine **Sitzungsrichtlinie**, die diesem Jump-Element zugewiesen werden soll. Die diesem Jump-Element zugewiesene Richtlinie hat die höchste Priorität bei der Festlegung von Sitzungsberechtigungen. Die Möglichkeit zur Festlegung einer Sitzungsrichtlinie ist von Ihren Kontoberechtigungen abhängig.

Weitere Informationen zur Identifizierung von HTML-Formularfeldern finden Sie in Online-Ressourcen wie dieser Seite, die die Verwendung von CSS-Selektoren unter https://developer.mozilla.org/en-US/docs/Web/CSS/CSS_Selectors erläutert.

Symbolischen Web-Jump-Link verwenden

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

Sobald eine Verbindung zur Website aufgebaut ist, klicken Sie auf das Bildschirmfreigabe-Symbol. Die Anmeldungsschnittstelle der Webseite wird verfügbar.



Hinweis: *Wenn Sie unter Windows oder Linux eine neue Registerkarte öffnen möchten, halten Sie die Taste **CTRL** gedrückt und klicken Sie mit der Maustaste. Bei iOS halten Sie die Taste **Command** gedrückt und klicken mit der Maustaste.*

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

Hochladen und Herunterladen von Dateien mit einer Web-Jump-Verknüpfung

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: *Zugriffskonsole für Privileged Web Access unterstützt nicht das Hochladen von Dateien auf eine Webseite über einen Web-Jump. Das Hochladen von Dateien auf eine Webseite über Web-Jump wird nur von der Desktop-Anwendung zugriffskonsole unterstützt.*

Verwenden der Anmeldedaten-Einfügung

WICHTIG!

Anmeldedaten-Einfügung wird für nicht sichere Sites (nicht-HTTPS) nicht unterstützt.

Bei der Integration von BeyondTrust PRA mit einem Passwort-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 Passwort 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 zugriffskonsole 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 und installieren Sie das VMware-Client-Integrations-Plugin.*
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 zugriffskonsole 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.*

Weitere Informationen zum Herunterladen des entsprechenden VMware-Client-Integrations-Plugin finden Sie unter Upgrade des VMware-Client-Integrations-Plugins auf die neueste Version unter https://kb.vmware.com/s/article/2145066.

Anmelden an Endpunkten mit Anmeldedaten-Einfügung

Beim Zugriff auf ein Windows-basiertes Jump-Element über die Zugriffskonsole für Privileged Web Access können Sie Anmeldedaten aus einem Anmeldedaten-Speicher verwenden, um sich am Endpunkt anzumelden oder Anwendungen als Administrator auszuführen.

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

Installation und Konfiguration des Endpunkt-Anmeldedaten-Managers

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

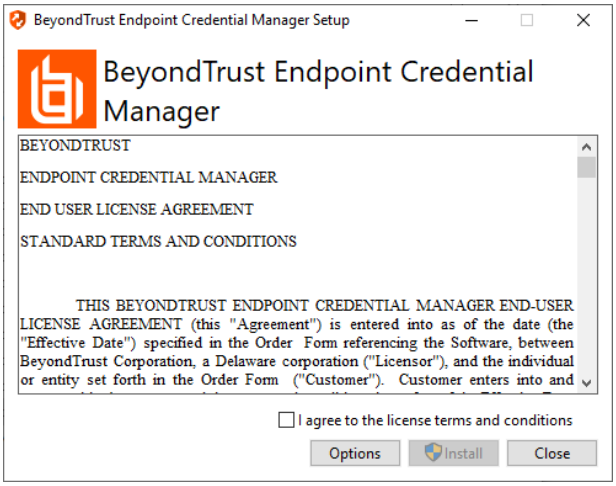
Hinweis: *Der ECM muss auf Ihrem System installiert werden, damit der BeyondTrust ECM-Dienst aktiviert und die Anmeldedateneinfügung in BeyondTrust Privileged Remote Access ermöglicht werden kann.*

Systemanforderungen

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

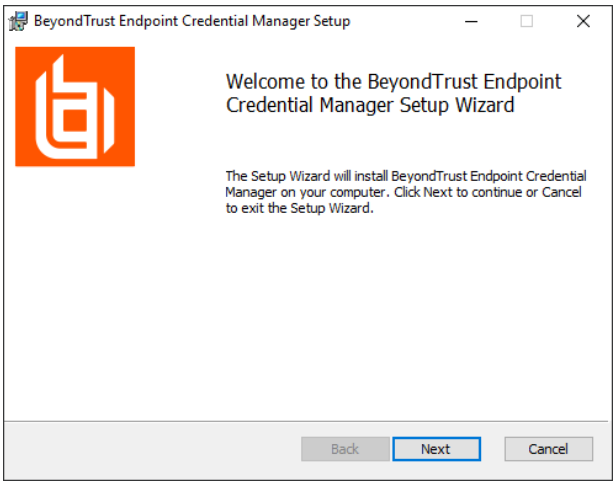
1. Laden Sie zunächst den BeyondTrust Endpunkt-Anmeldedaten-Manager (ECM) von BeyondTrust Support unter beyondtrustcorp.service-now.com/csm herunter.
2. Starten Sie den Installationsassistenten für den BeyondTrustEndpunkt-Anmeldedaten-Manager.
3. Stimmen Sie den Bedingungen der Endbenutzer-Lizenzvereinbarung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

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

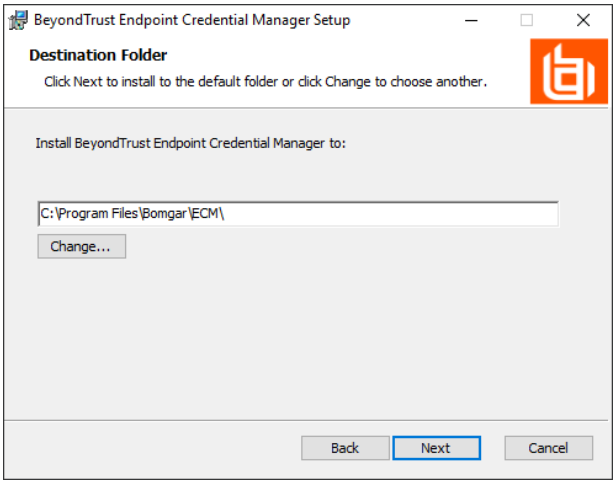


Hinweis: *Sie können mit der Installation erst fortfahren, wenn Sie der Endbenutzer-Lizenzvereinbarung zustimmen.*

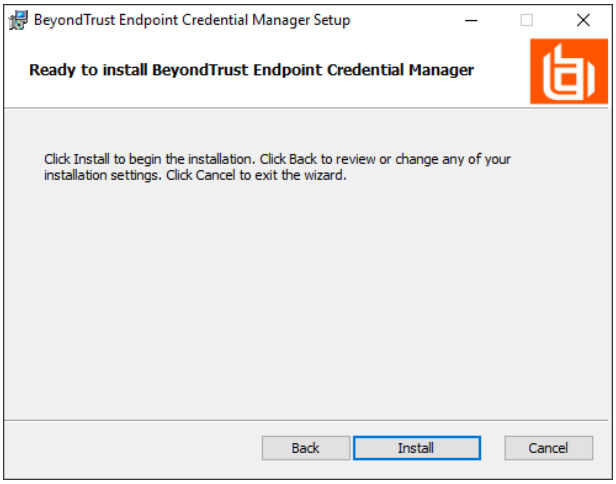
4. Klicken Sie auf dem Begrüßungsbildschirm auf **Weiter**.



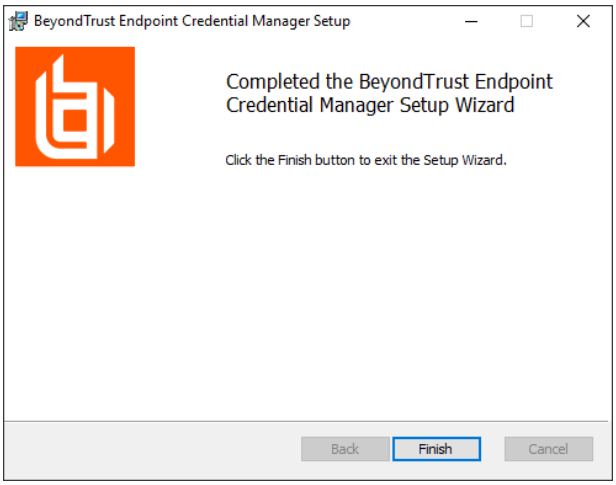
5. Wählen Sie den Installationsort für den Anmeldedaten-Manager und klicken Sie dann auf **Weiter**.
6. Auf dem nächsten Bildschirm können Sie mit der Installation beginnen oder vorherige Schritte überprüfen.



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



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

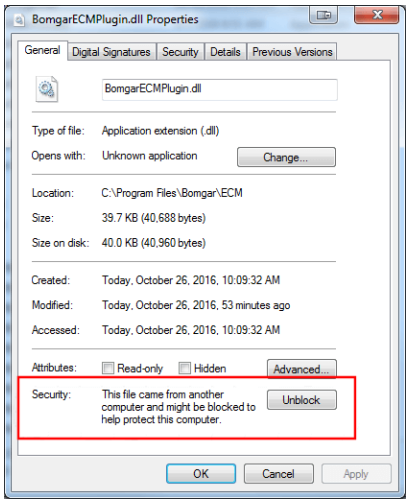


Hinweis: *Um einen ausfallfreien Betrieb zu gewährleisten, können Administratoren bis zu drei ECMs auf unterschiedlichen Windows-Systemen installieren, um mit dem gleichen Anmeldedatenspeicher zu kommunizieren. Eine Liste der mit der Geräte-Site verbundenen ECMs finden Sie in* ***/login > Status > Informationen > ECM-Clients****.*

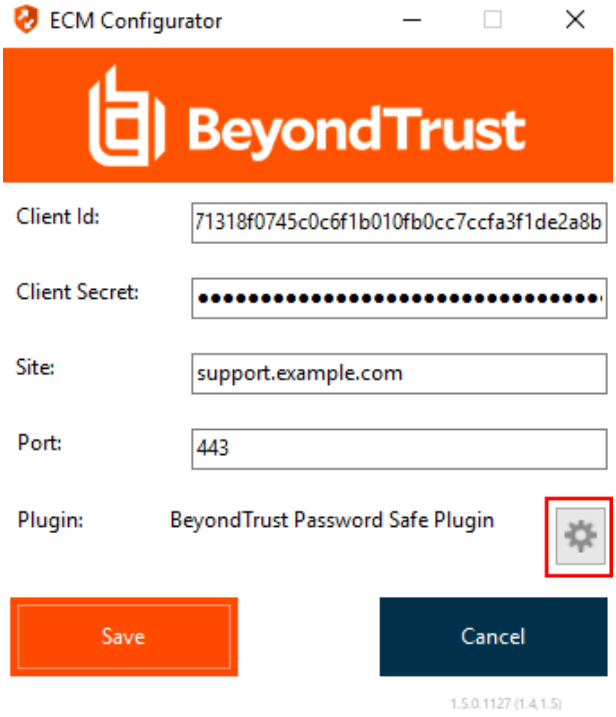
Hinweis: *Wenn ECMs in einer Konfiguration mit hoher Verfügbarkeit verbunden sind, leitet das BeyondTrust Appliance B Series Anfragen an den ECM in die ECM-Gruppe, die am längsten mit dem Gerät verbunden ist.*

Installation und Konfiguration des Plugins

1. Extrahieren und kopieren Sie die Plugin-Dateien nach der Installation des BeyondTrust-ECM in das Installationsverzeichnis (typischerweise **C:\Program Files\Bomgar\ECM**).
2. Starten Sie den **ECM-Konfigurator**, um das Plugin zu installieren.
3. Der Konfigurator sollte das Plugin automatisch erkennen und laden. Wenn ja, fahren Sie mit Schritt 4 fort. Befolgen Sie diese Schritte:
    - Stellen Sie zunächst sicher, dass die DLL nicht blockiert wird. Rechtsklicken Sie auf die DLL und wählen Sie **Eigenschaften**.
    - Sehen Sie sich auf der Registerkarte **Allgemein** den unteren Teil des Fensters an. Wenn es einen Abschnitt **Sicherheit** mit einer Schaltfläche **Entsperren** gibt, klicken Sie auf die Schaltfläche.
    - Wiederholen Sie diese Schritte für alle anderen mit dem Plugin verpackten DLLs.
    - Klicken Sie im Konfigurator auf die Schaltfläche **Plugin auswählen** und navigieren Sie zum Speicherort der Plugin-DLL.



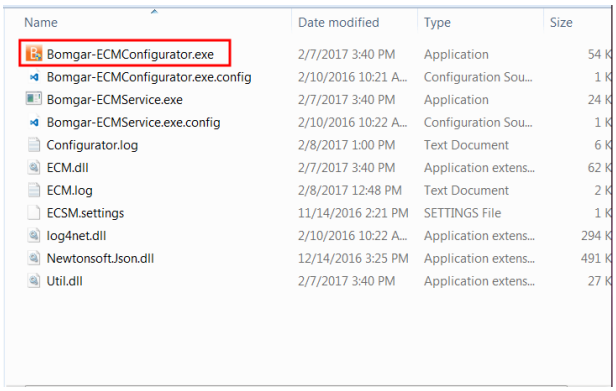
4. Klicken Sie auf das Zahnrad-Symbol im Fenster **Konfigurator**, um die Plugin-Einstellungen zu konfigurieren.



Konfiguration einer Verbindung zu Ihrem Anmeldedaten-Speicher

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

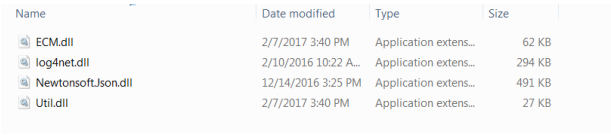
1. Machen Sie den soeben installierten BeyondTrust ECM-Konfiguratur über das Windows-Suchfeld oder durch Aufruf der Programmliste in Ihrem **Start**menü ausfindig.
2. Führen Sie das Programm aus, um eine Verbindung aufzubauen.
3. Wenn der Konfigurator geöffnet wird, vervollständigen Sie die Felder. Alle 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 Passwort-Speicher verbinden, sind möglicherweise weitere Konfigurationsschritte auf Plugin-Ebene notwendig. Die Plugin-Anforderungen variieren basierend auf dem Anmeldedaten-Speicher, mit dem Sie eine Verbindung aufbauen.*

WICHTIG!

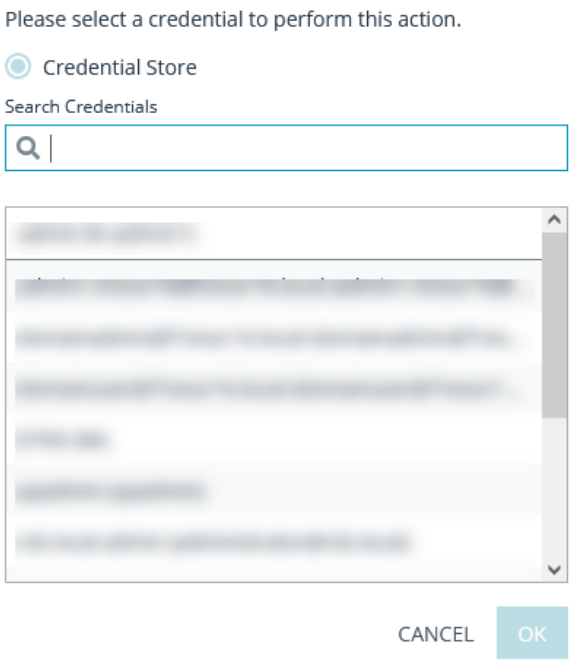
Um die neuen Einstellungen in der Konfiguration zu übernehmen, starten Sie den Anmeldedaten-Manager-Dienst neu.

Verwendung der Anmeldedaten-Einfügung zum Zugriff auf Endpunkte

Nachdem der Anmeldedaten-Speicher konfiguriert und eine Verbindung aufgebaut wurde, kann die Zugriffskonsole für Privileged Web Access mit der Verwendung von Anmeldedaten des Anmeldedaten-Speichers zur Anmeldung an Endpunkten beginnen.

1. Melden Sie sich in der Zugriffskonsole für Privileged Web Access an.
2. Führen Sie einen Jump zu einem Endpunkt 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 Endpunkt zu beginnen. Wenn sich der Endpunkt 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.

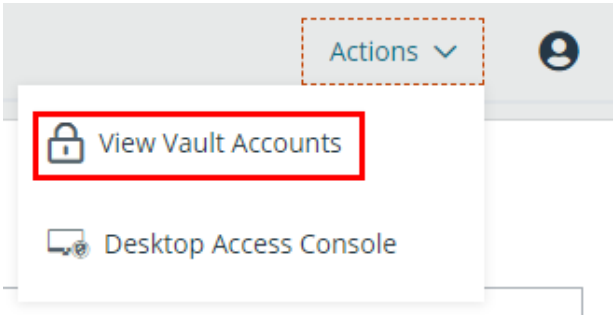
5. Wählen Sie die geeigneten Anmeldedaten aus dem Endpunkt-Anmeldedaten-Manager, die verwendet werden sollen. Das System ruft die Anmeldedaten vom Endpunkt-Anmeldedaten-Manager ab und setzt sie auf dem Windows-Anmeldungsbildschirm ein.
6. Der Benutzer wird am Endpunkt angemeldet.



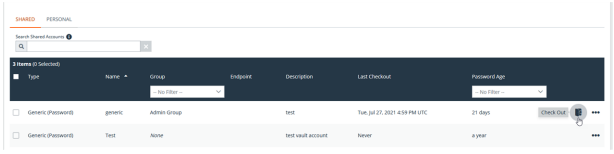
Einchecken und Auschecken von Vault-Anmeldedaten

Von der Web-Zugriffskonsole aus können Sie über die Schnittstelle /login einfach auf den Privileged Remote Access-Vault zugreifen, um bei Bedarf Anmeldedaten auszuchecken und einzuchecken, entweder während einer Sitzung oder auf Ihrem lokalen Computer.

Um auf den Vault zuzugreifen, klicken Sie in der oberen Navigationsleiste auf das Dropdown-Menü **Aktionen** und wählen Sie **Vault-Konten anzeigen**. Sie gelangen direkt auf die Seite **Vault > Konten** in der Schnittstelle **/login**, wenn Sie angemeldet sind.



Sie können dann ein Vaultkonto auswählen und auschecken oder einchecken.



Authentifizierung über die Client-Skripting-API

Mit dieser Funktion können sich Benutzer an der Zugriffskonsole für Privileged Web Access anmelden und mithilfe der PRA Client-Skripting-API (https://www.beyondtrust.com/docs/privileged-remote-access/how-to/integrations/api/client-script/index.htm#client-scripting-api) einen Jump zu einem Endpunkt durchführen.

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

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

Wenn der Benutzer in der Desktop-zugriffskonsole angemeldet ist, wenn die Client-Skripting-API-URL mit **type=web_console** genutzt wird, wird der Benutzer in der Zugriffskonsole für Privileged Web Access angemeldet und von der Desktop-zugriffskonsole getrennt. Wird dieses Verhalten nicht gewünscht, muss der Benutzer eine Client-Skripting-API-URL mit **type=rep** statt **type=web_console** verwenden.

Ähnlich gilt: Wenn der Benutzer in der Zugriffskonsole für Privileged Web Access angemeldet ist und die API **type=rep** aufruft, wird der Benutzer in der Desktop-zugriffskonsole angemeldet und von der Zugriffskonsole für Privileged Web Access getrennt.

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

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

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

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

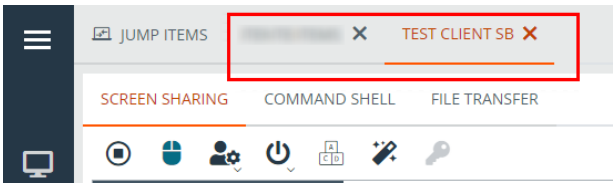
In beiden Fällen gilt: Erfüllt mehr als ein Jump-Element die Suchkriterien, muss der Benutzer das richtige Jump-Element aus einer Liste wählen. Wenn keine Jump-Elemente die Suchkriterien erfüllen, zeigt die Zugriffskonsole für Privileged Web Access dem Benutzer einen Fehler an.

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

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

Zu einer aktiven Sitzung in der Privileged Web-Zugriffskonsole zurückkehren

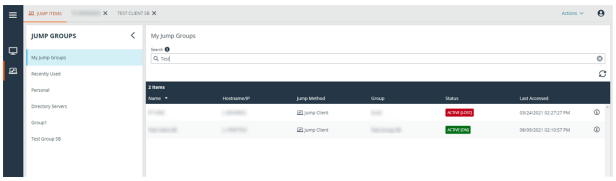
Wenn Sie über mehrere laufende Zugriffssitzungen verfügen, können Sie jederzeit zu einer dieser Sitzungen zurückkehren. Um zu einem Endpunkt zurückzukehren, auf den bereits in einer anderen Sitzung zugegriffen wurde, klicken Sie auf die Sitzung am oberen Bildschirmrand.



Suchen nach Endpunkten

Bei der Verwendung von Zugriffskonsole für Privileged Web Access können Sie in einer Zugriffssitzung nach bestimmten Endpunkten suchen. Innerhalb der Suchergebnisse können Sie auch auf die Schaltfläche **Start** klicken, um eine Sitzung mit diesem Endpunkt zu beginnen.

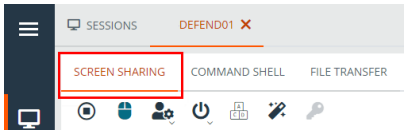
1. Klicken Sie auf das Symbol **Suchen** oben links auf dem Bildschirm.
2. Geben Sie in der Suchleiste den Namen des Endpunktes ein.
3. Wählen Sie aus den Suchergebnissen den Endpunkt, mit dem Sie eine Sitzung starten möchten und klicken Sie auf die Schaltfläche **Start**, um eine Sitzung zu beginnen.



Steuern des Remote-Endpunkts mit der Bildschirmfreigabe über Privileged Web

Um Remote-Systeme anzuzeigen und zu steuern, wählen Sie die Aktion Bildschirmfreigabe in einer Zugriffssitzung.

1. Klicken Sie im Sitzungsfenster auf die Registerkarte **Bildschirmfreigabe** am oberen Rand des Bildschirms. Alternativ können Sie auf das Symbol **Bildschirmfreigabe beginnen** klicken, um mit dem Zugriff auf den Endpunkt zu beginnen, falls die Bildschirmfreigabe nicht automatisch beginnt.
2. Verwenden Sie folgende Aktionen in einer Sitzung für unterschiedliche Funktionen:



Bildschirmfreigabe-Werkzeuge

	Bildschirmfreigabe beenden.
	Bei Arbeiten auf dem Remote-Computer können Sie die Steuerung der Tastatur oder Maus anfordern bzw. beenden. Support-Techniker, die ein macOS-System verwenden, können **Strg+Linke Maustaste** über die verbundene Bildschirmfreigabesitzung an das Remote-System senden, indem sie **Strg+CMD+Linke Maustaste** verwenden.
	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 Endpunkt-Client heraufgesetzt werden. In Windows 8 ist dieses Feature auf die Deaktivierung von Maus und Tastatur beschränkt.
	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.
	Schaltet die Zwischenablage ein oder aus.
	Schalten Sie die virtuelle Tastatur ein oder aus.
	Nehmen Sie eine Bildschirmaufnahme auf. Sie können sie in einer Datei oder in der Zwischenablage speichern.
	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.

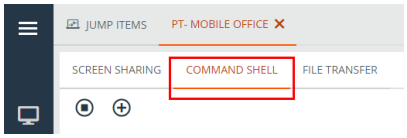
Öffnen der Befehlsshell am Remote-Endpunkt mit der Privileged Web-Konsole

Mit der Remote-Befehlsshell kann ein berechtigter Benutzer eine virtuelle Befehlszeilenschnittstelle für ein Remote-System 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.

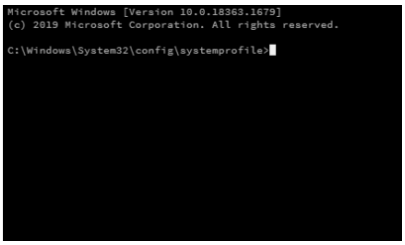
> ***Hinweis:*** *Je nach Sitzungsrichtlinie und Art des Jumps ist* ***Command Shell*** *möglicherweise nicht verfügbar.*

1. Um in einer Zugriffssitzung auf die **Command Shell** zuzugreifen, klicken Sie auf die Registerkarte **Command Shell** am oberen Bildschirmrand.



2. Wenn Sie nicht automatisch zur Command Shell geleitet werden, klicken Sie auf die Schaltfläche **Start des Command Shell**.

3. Die Befehlsoptionen und die Eingabeaufforderung werden angezeigt.

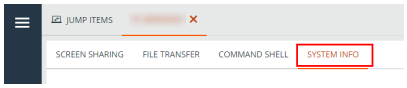


Befehlsshell-Tools

	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.

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.



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

Werkzeuge für Systeminformationen

	Systeminformationen aktualisieren.
	In Zwischenablage kopieren.
	In Datei speichern.

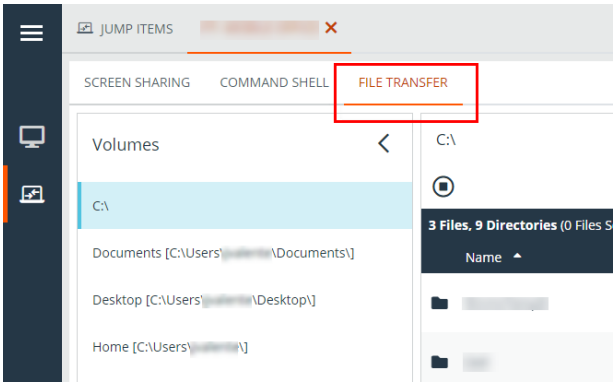
Nutzen der Privileged Web-Konsole zur Übertragung von Dateien an und von Remote-Systemen

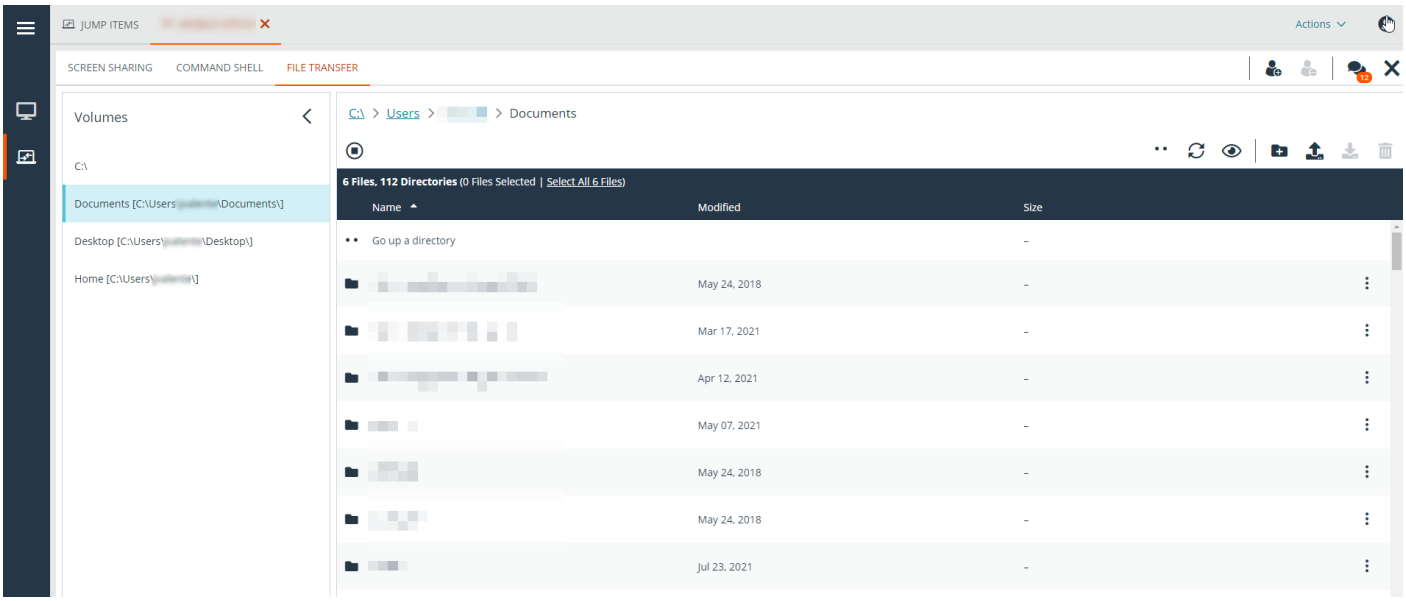
Berechtigte Benutzer können während einer Sitzung Dateien und sogar ganze Verzeichnisse sowohl auf den Remote-Computer als auch vom Remote-Computer oder vom Remote-Gerät auf die SD-Karte oder umgekehrt übertragen, löschen oder umbenennen. Sie müssen nicht die vollständige Kontrolle über den Remote-Computer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

Je nach den Berechtigungen, die Ihr Administrator für Ihr Konto festgelegt haben, können Sie womöglich nur Dateien auf das Remote-System hoch- oder Dateien auf Ihren lokalen Computer herunterladen. Der Dateisystemzugriff kann ebenfalls auf bestimmte Pfade auf dem Remote- oder lokalen System beschränkt sein, wodurch Uploads oder Downloads nur auf bestimmte Verzeichnisse beschränkt sind. Übertragen Sie Dateien mithilfe der Upload- oder Download-Schaltflächen. Überprüfen Sie den Übertragungs- und Löschfortschritt über das Plussymbol unten auf dem Bildschirm. Über das Symbol **Mehr Optionen** können Sie Dateien herunterladen, umbenennen oder löschen.

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

Wählen Sie ein Verzeichnis, um von der Spalte **Laufwerke** ausgehend zu suchen. Die Breadcrumbs oben zeigen Ihren momentanen Standort an. Doppelklicken Sie auf den Ordner, um ihn zu öffnen.





Wenn ein ICAP-Server aktiviert ist, werden alle per FTP übertragenen Dateien auf Malware gescannt. Wird in der Datei Malware entdeckt, wird sie nicht übertragen. Einzelheiten zu einer fehlgeschlagenen Dateiübertragung können auf dem

Bildschirm für die Dateiübertragung angezeigt werden und sind in Sitzungs- oder Teamberichten verfügbar. Um einen ICAP-Server zu aktivieren, siehe Sicherheit unter https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/security.htm.

Werkzeuge für den Dateitransfer

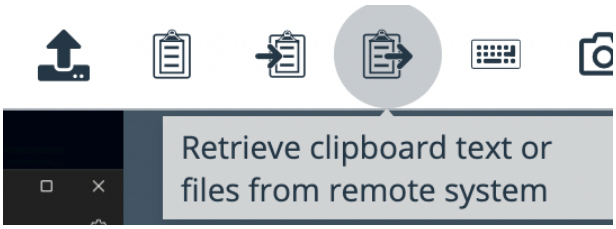
	Stoppen Sie den Zugriff auf das Dateisystem des Remote-Geräts.
	Ein Verzeichnis im ausgewählten Dateisystem nach oben wechseln.
	Ihre Ansicht des ausgewählten Dateisystems aktualisieren.
	Ausgeblendete Dateien anzeigen.
	Ein neues Verzeichnis erstellen.
	Hochladen einer Datei in ein Verzeichnis / Freigeben von Dateien mit der RDP-Zwischenablage.
	Laden Sie ausgewählte Dateien aus einem Verzeichnis herunter.
	Modifikatortasten umschalten.
	Text in der Zwischenablage an Remote-System senden.
	Text aus der Zwischenablage vom Remote-System abrufen / Text oder Dateien aus der Zwischenablage vom Remote-System (RDP) abrufen.

	Löschen Sie ausgewählte Dateien aus einem Verzeichnis.
	Ein Verzeichnis oder eine Datei herunterladen, umbenennen oder löschen.  ***Hinweis:*** *Die Löschung einer Datei oder eines Verzeichnisses ist nicht widerrufbar. Die Datei bzw. der Ordner wird nicht in den Papierkorb geworfen.*

RDP-Dateitransfer

Dateien herunterladen

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

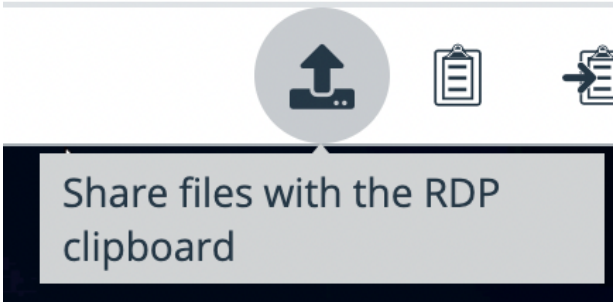


Das Kopieren von Dateien oder Verzeichnissen auf dem entfernten Endpunkt löst einen Dateidownload in Ihrem Browser aus. Die ausgewählte Datei wird in den Ordner heruntergeladen, den Sie auf Ihrem Computer angegeben haben. Je nach den Einstellungen Ihres Browsers werden Sie möglicherweise aufgefordert,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

Dateien hochladen

Das Hochladen von Dateien in die Zugriffskonsole für Privileged Web Access ist ein zweistufiger Prozess:

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



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

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

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

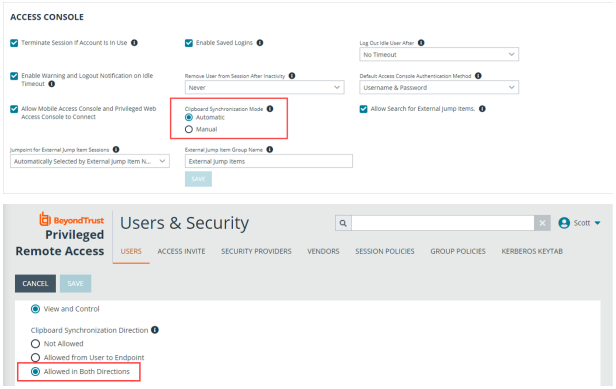
Nach dem Einfügen am Endpunkt zeigt Windows den Fortschritt der Übertragung in einem Dialogfeld am Endpunkt an und bietet eine Schaltfläche zum Abbrechen.

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

Einstellungen

Damit die Dateiübertragung wie beschrieben funktioniert, müssen Sie sicherstellen, dass die folgenden Einstellungen wie folgt sind:

- **Synchronisierungsmodus für Zwischenablage** ist auf **Automatisch** eingestellt (siehe **/login > Verwaltung > Sicherheit > Zugriffskonsole**)
- Die **Synchronisierungsrichtung für Zwischenablage** des Benutzers ist auf **In beiden Richtungen erlaubt** eingestellt (siehe **/login > Benutzer & Sicherheit > Benutzer > Sitzungsberechtigungen > Synchronisierungsrichtung der Zwischenablage**).



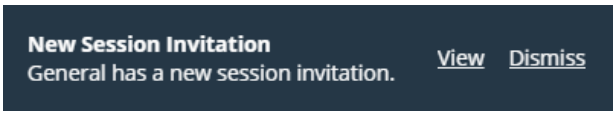
Freigabe einer Sitzung für Teammitglieder oder externe Benutzer mithilfe der Zugriffskonsole für Privileged Web Access

Team-Mitglieder einladen

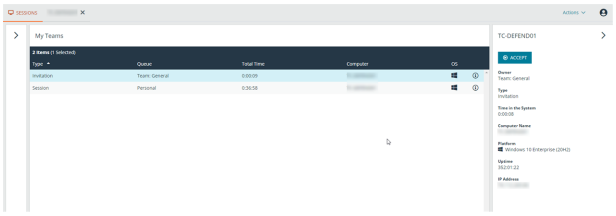
Innerhalb einer Sitzung können Sie ein Teammitglied auffordern, an einer Zugriffssitzung teilzunehmen. Folgen Sie zur Freigabe einer Sitzung diesen Schritten:

1. Klicken Sie auf die Schaltfläche **Andere Benutzer zu dieser Sitzung einladen**.
2. Wählen Sie das Team, dem der Benutzer angehört, aus dem Menü.
3. Wählen Sie aus der Teamliste den Benutzer, für den Sie die Sitzung freigeben möchten.

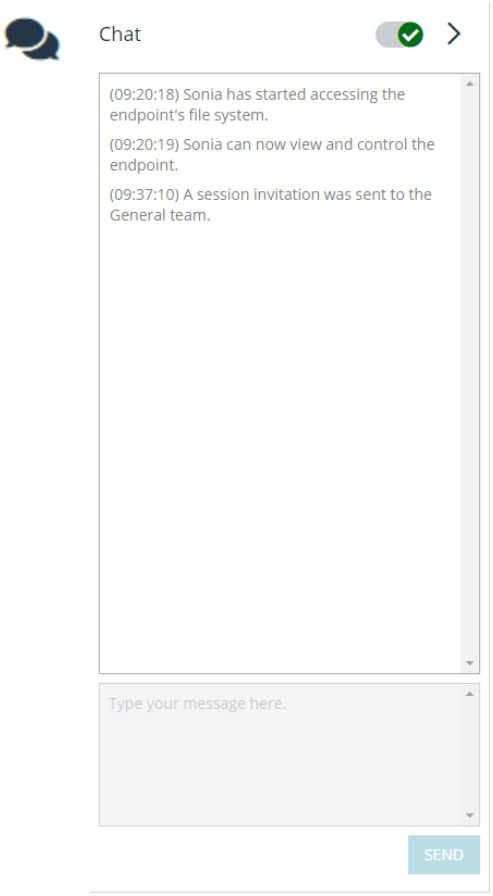
4. Der eingeladene Benutzer sieht eine Benachrichtigung in der unteren linken Ecke des Bildschirms, die auf eine neue Sitzungseinladung hinweist.



5. Wenn auf dem Benachrichtigungsbanner auf **ANZEIGEN** geklickt wird, werden Informationen zur Sitzung angezeigt. Der Benutzer kann dann auf **ANNEHMEN** klicken, um der Sitzung beizutreten.



6. Wenn der Benutzer der Sitzung beigetreten ist, können Sie mit diesem chatten, indem Sie auf das Symbol **Chat** oben auf dem Bildschirm klicken.



Sie können mehrere Einladungen versenden, wenn mehr Mitglieder aus dem Team Ihrer Sitzung beitreten sollen. Benutzer werden nur dann hier aufgelistet, wenn sie in der zugriffskonsole 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, sofern sie mindestens ein in der zugriffskonsole angemeldetes Mitglied enthalten oder wenn sie die erweiterte Verfügbarkeit aktiviert haben.

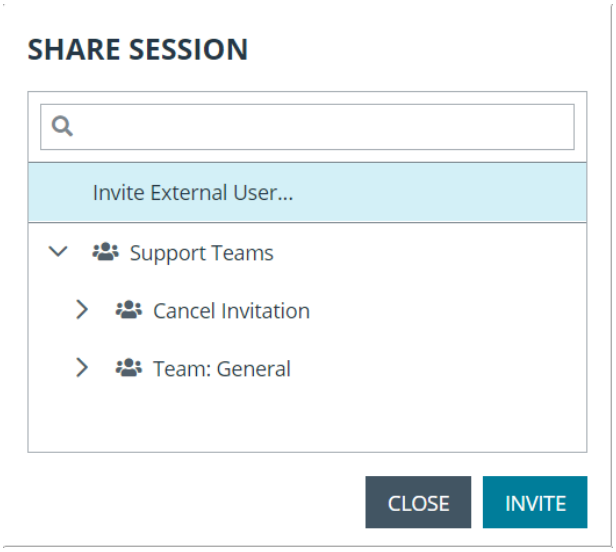
Einladungen können nur vom Sitzungseigentümer verschickt werden. Solange Sie Sitzungseigentümer bleiben, laufen Einladungen nicht ab. Für ein und denselben Benutzer können nicht mehrere aktive Einladungen für dieselbe Sitzung bestehen. Die Einladung verschwindet, falls:

- Der einladende Benutzer die Einladung zurückzieht.
- Der einladende Benutzer die Sitzung verlässt.
- Die Sitzung endet.
- Der eingeladene Benutzer die Einladung annimmt.

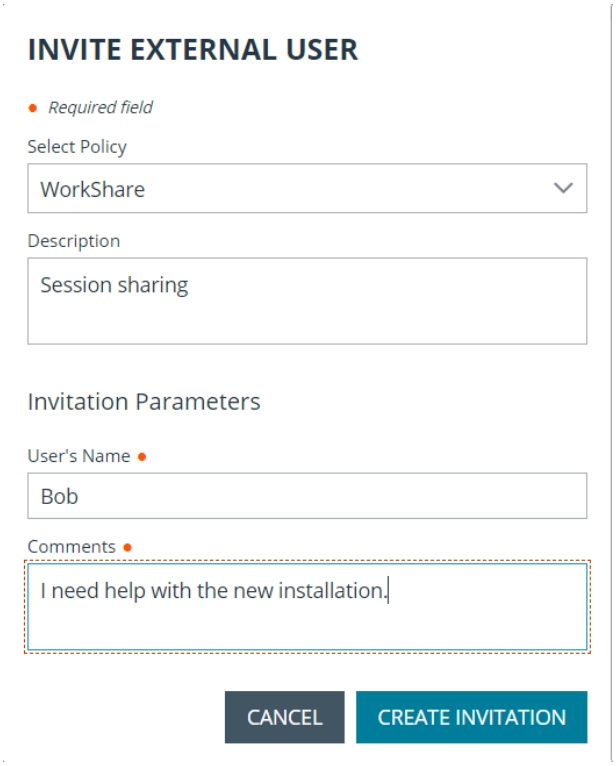
Externe Benutzer einladen

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

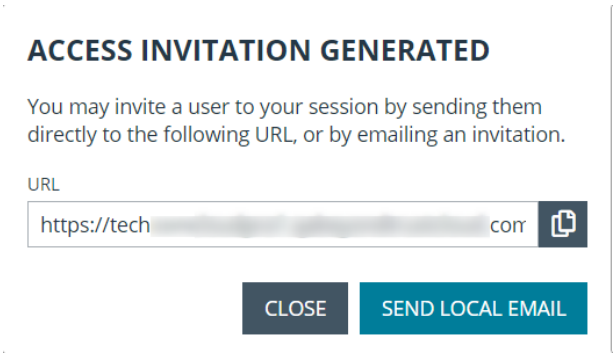
1. Klicken Sie auf die Schaltfläche **Andere Benutzer zu dieser Sitzung einladen**.
2. Wählen Sie **Externe Benutzer einladen ...**.



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



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



Ein Mitglied aus einer Privileged Web-Zugriffskonsolen-Sitzung entfernen

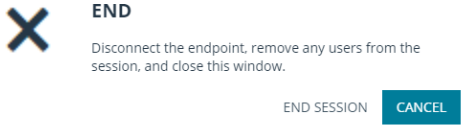
Falls erforderlich, können Sie einen anderen Benutzer aus einer freigegebenen Zugriffssitzung entfernen. Um einen Benutzer zu entfernen, klicken Sie auf das Symbol **Mitglied entfernen**.

Wählen Sie aus dem Menü den Teilnehmer, den Sie entfernen möchten. Klicken Sie auf **Mitglied entfernen**.

Hinweis: *Sie müssen Eigentümer der Sitzung sein, um ein anderes Mitglied entfernen zu können.*

Beenden der Privileged Web-Zugriffskonsolensitzung

1. Um eine Zugriffssitzung zu verlassen, klicken Sie auf das Symbol **X** in der oberen rechten Ecke des Bildschirms. Wenn Sie der Sitzungseigentümer sind, beachten Sie, dass **Sitzung beenden** die Sitzungsseite in Ihrer zugriffskonsole schließt und jegliche zusätzliche Mitglieder, für welche die Sitzung möglicherweise freigegeben wird, entfernt werden.

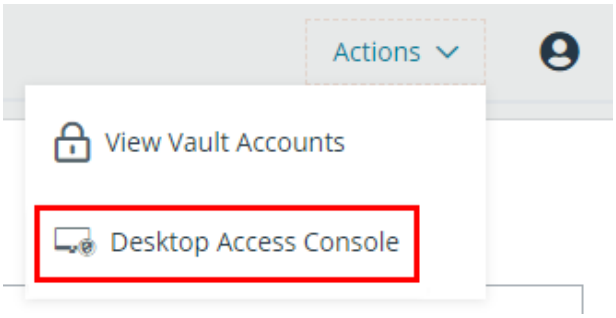


2. Als nächstes sehen Sie eine Eingabeaufforderung, die Sie fragt, ob Sie die Sitzung beenden möchten.
3. Wenn Sie auf **OK** klicken, wird die Sitzung beendet und Sie kehren zur Liste **Alle Jump-Elemente** zurück.

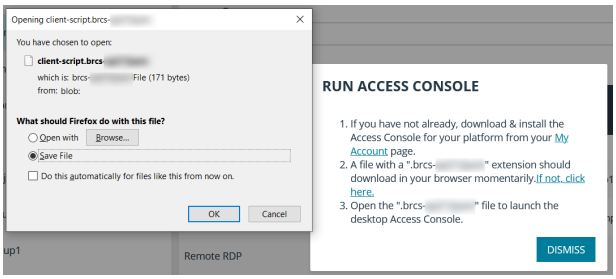
Herunterladen der nativen Desktop-Konsole über die Privileged Web-Zugriffskonsole

Bei der Arbeit in der Zugriffskonsole für Privileged Web Access können Sie jederzeit die native Desktop-zugriffskonsole auf Ihren Computer herunterladen.

1. Um die native Desktop-zugriffskonsole von Zugriffskonsole für Privileged Web Access herunterzuladen, wählen Sie **Desktop Zugriffskonsole**, das sich unter dem Menü **Aktiv** in der oberen rechten Ecke des Bildschirms befindet.



2. Befolgen Sie zur Installation der Software die Anweisungen im angezeigten Installationsassistenten.



> ***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.*