BOMGAR™

Privileged Access
Privileged Web

TC:4/26/2018

Inhaltsverzeichnis

Handbuch zur Privileged Web-Zugriffskonsole

Mit der Bomgar Privileged Web-Zugriffskonsole können Informations- und Cyber-Sicherheits-Teams berechtigten Benutzern sicheren Remote-Zugriff 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 Privileged Web-Zugriffskonsole 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 Bomgar-Geräts durch einen Administrator abgeschlossen wurde, entsprechend der Beschreibung im Bomgar Installationshandbuch für Gerätehardware. Sollten Sie Hilfe benötigen, wenden Sie sich an den technischen Bomgar-Support unter help.bomgar.com.*

Voraussetzungen für die Privileged Web-Zugriffskonsole

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

Plattformen

- Windows
- Macintosh
- Linux

Browser

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

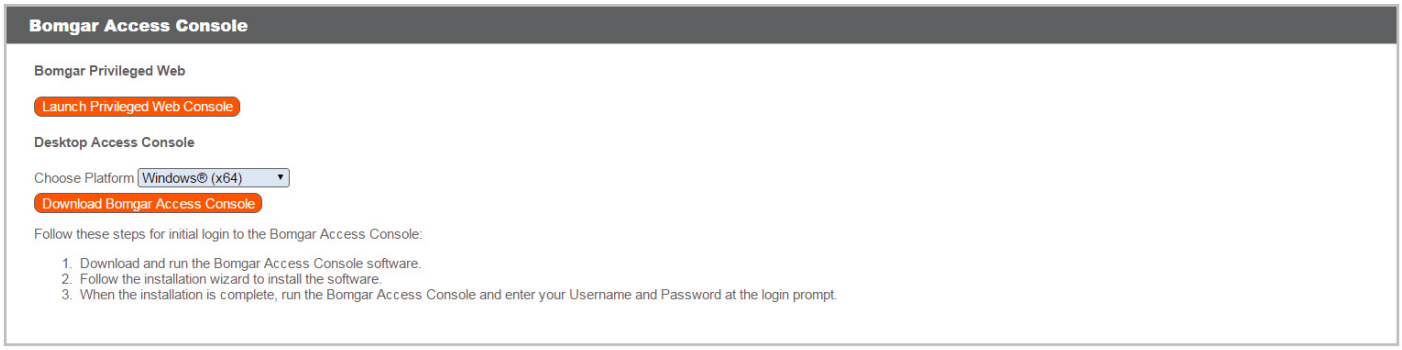
WICHTIG!

Ihr Bomgar-Gerät 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 Bomgar-Gerät übernommen haben, wenden Sie sich an den technischen Bomgar-Support. Ihr Support-Techniker wird einen neuen Software-Build erstellen, der Ihr SSL-Zertifikat integriert. Mit dieser aktualisierten, auf Ihrem Gerät installierten Build können Sie die Bomgar-Zugriffskonsole auf Ihrem Gerät ausführen, um von fast überall auf Ihre Endpunkte zuzugreifen.

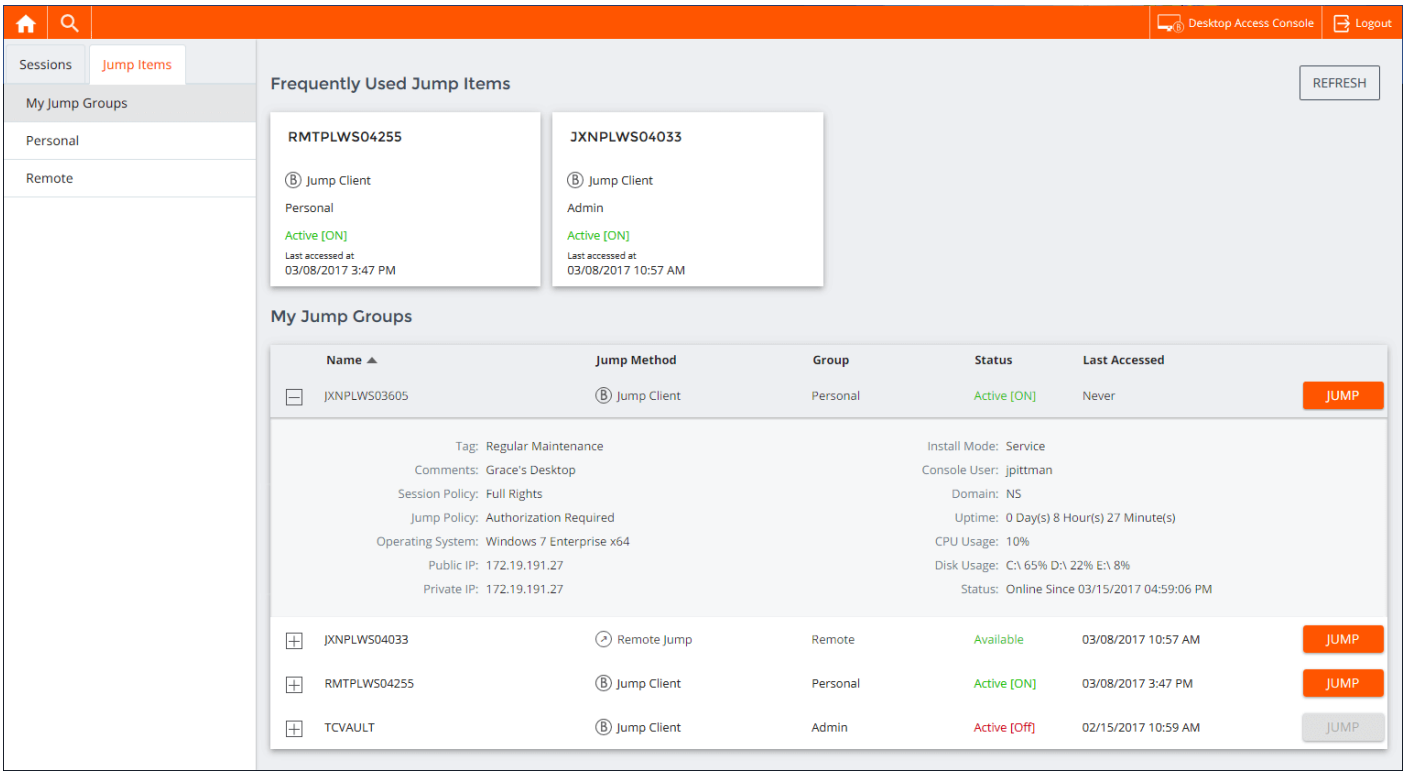
Starten der Privileged Web-Zugriffskonsole über /login

Mit der Privileged Web-Zugriffskonsole können Sie sicher auf Ihre Endpunkte zugreifen, indem Sie über eine webbasierte Zugriffskonsole und eine Remote-Verbindung durch das Bomgar-Gerät auf sie zugreifen. Um die Privileged Web-Zugriffskonsole zum Zugriff auf Endpunkte zu verwenden, folgen Sie den unten beschriebenen Schritten:

Hinweis: *Standardmäßig ist die Schaltfläche* ***„Privileged Web-Zugriffskonsole starten“*** *nicht verfügbar. Sie müssen zu* ***Verwaltung > Sicherheit*** *navigieren und* ***Mobiler Bomgar-Zugriffskonsole und Bomgar Privileged Web-Zugriffskonsole Verbindung gestatten*** *aktivieren, um die Konsole zu aktivieren.*



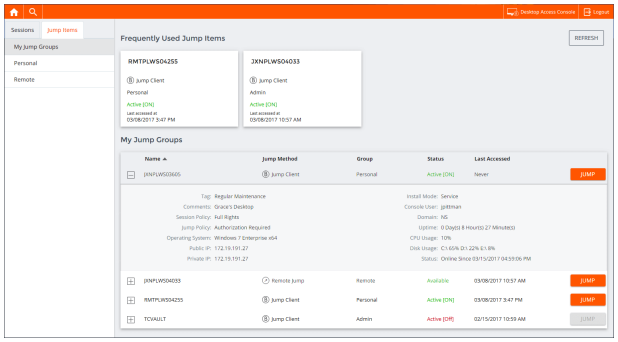
1. Geben Sie in der Adressleiste Ihres Browsers den Hostnamen Ihrer Bomgar-Site gefolgt von /login ein, etwa access.example.com/login.
2. Geben Sie dann den mit Ihrem Bomgar-Benutzerkonto verknüpften Benutzernamen und das dazugehörige Kennwort ein.
3. Klicken Sie auf **Anmelden**.
4. Klicken Sie nach der Anmeldung in der /login-Verwaltungsschnittstelle auf die Registerkarte **Mein Konto**.
5. Klicken Sie auf die Schaltfläche **Privileged Web-Zugriffskonsole starten**, die sich im Abschnitt **Bomgar-Zugriffskonsole** befindet.
6. Die Privileged Web-Zugriffskonsole wird in einer neuen Registerkarte geöffnet und Sie können mit dem Zugriff auf Endpunkte beginnen.



Um sich von der Zugriffskonsole abzumelden, tippen Sie auf das **Abmelden**-Symbol in der oberen rechten Ecke des Bildschirms.

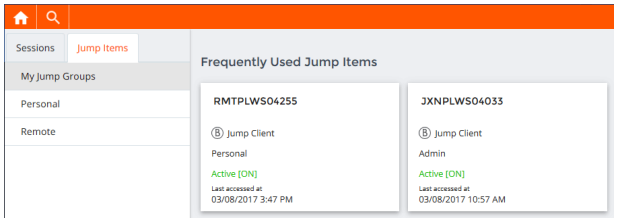
Verwenden von Jump-Elementen zum Zugriff auf Endpunkte in der Privileged Web-Zugriffskonsole

Um auf einen Endpunkt zuzugreifen, installieren Sie über die Seite **Jump Clients** der /login-Verwaltungsschnittstelle ein Jump-Element auf diesem System.



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. Ebenfalls 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.

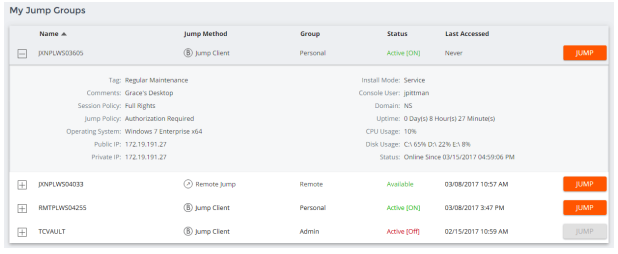


Mit dem Zugriff auf Endpunkte können Sie über drei Wege beginnen:

- Lokalisieren und wählen Sie einen Endpunkt aus der Liste **Meine Jump-Gruppen**.
- Wählen Sie eine Jump-Gruppe und wählen Sie einen Endpunkt aus der Liste der Endpunkte der Gruppe.
- 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****.*

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

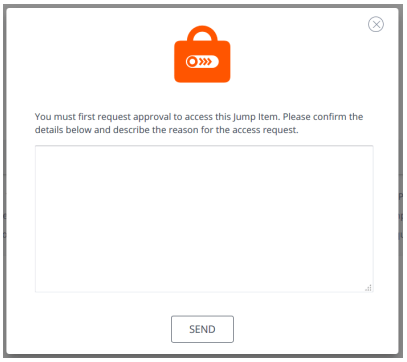


1. Wählen Sie einen Ort und klicken Sie auf die Schaltfläche **Alle aktualisieren**.
2. Eine Liste aller Jump-Elemente wird angezeigt und Sie können die Details zum Jump-Element einsehen, einschließlich: **Name**, **Methode**, **Gruppe**, **Status** und **Letzter Zugriff**. Um mehr Einzelheiten über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

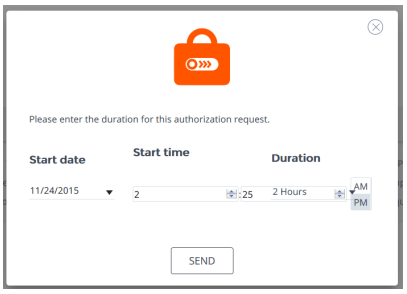
Autorisierung durch Endbenutzer oder Drittpartei

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. Um mehr über die Konfiguration von Dritt- und Endbenutzerbenachrichtigungen und -genehmigungen zu erfahren, lesen Sie weiter unter Jump-Richtlinien: Zeitpläne, Benachrichtigungen und Genehmigungen für Jump-Elemente festlegen unter https://www.bomgar.com/docs/privileged-access/getting-started/admin/jump-policies.htm.

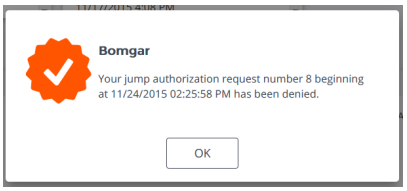
1. Nachdem auf die **JUMP**-Schaltfläche geklickt und der Zugriff angefordert wurde, erscheint eine Aufforderung und Sie müssen einen Grund für den Zugriff auf das System eingeben.



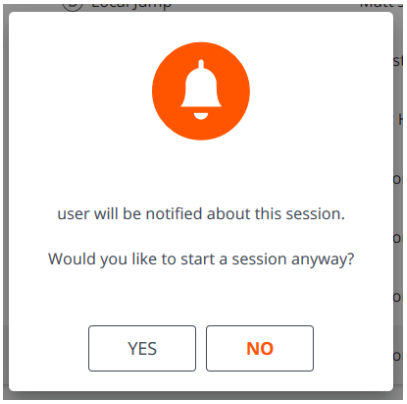
2. Als nächstes müssen Sie angeben, wann und für wie lange Sie auf das System zugreifen wollen.
3. Nach dem Absenden der Anfrage wird die Drittpartei oder Person, die für die Genehmigung von Zugriffsanforderungen verantwortlich ist, per E-Mail benachrichtigt und hat die Gelegenheit, die Anfrage zu akzeptieren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



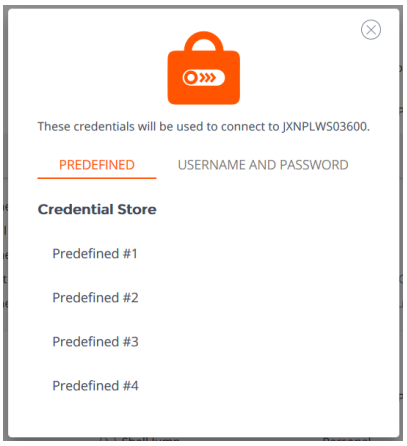
4. Nach Festlegen der Berechtigung erscheint eine Autorisierungsbenachrichtigung innerhalb der Jump-Element-Informationen und gibt entweder „Genehmigt“ oder „Abgelehnt“ an. Wird der Zugriff genehmigt, können Sie auf die Jump-Schaltfläche tippen, um mit dem Zugriff auf das System zu beginnen.



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.



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 Kennwort 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.bomgar.com/docs/privileged-access/getting-started/admin/security.htm.

Anmelden an Endpunkten mit Anmeldedaten-Einfügung

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

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

***Hinweis:** Haben Sie keinen Kennwort-Speicher? Erfahren Sie mehr über **Bomgar Vault** unter https://www.bomgar.com/vault.*

Installation und Konfiguration des Endpunkt-Anmeldedaten-Managers

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

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

Systemanforderungen

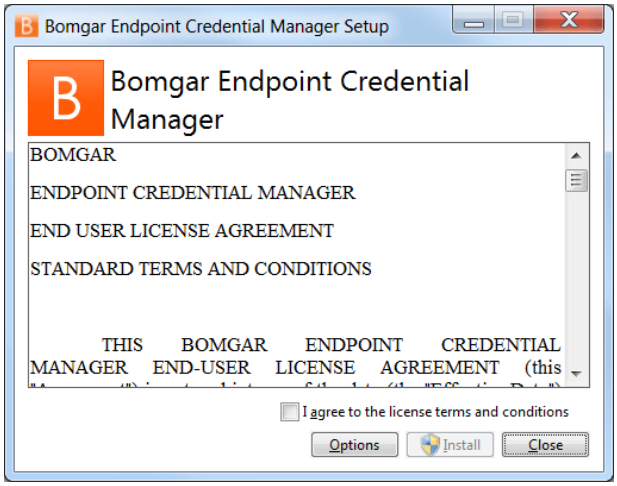
- **Windows Vista oder neuer, nur 64 Bit**
- **.NET 4.5 oder neuer**

***Hinweis:** Bei der Installation des Endpunkt-Anmeldedaten-Managers zur Nutzung mit dem Bomgar Vault empfehlen wir die Installation auf einem System mit statischer IP-Adresse, um mögliche Probleme mit dem IP-Whitelisting des Vault für die API zu vermeiden.*

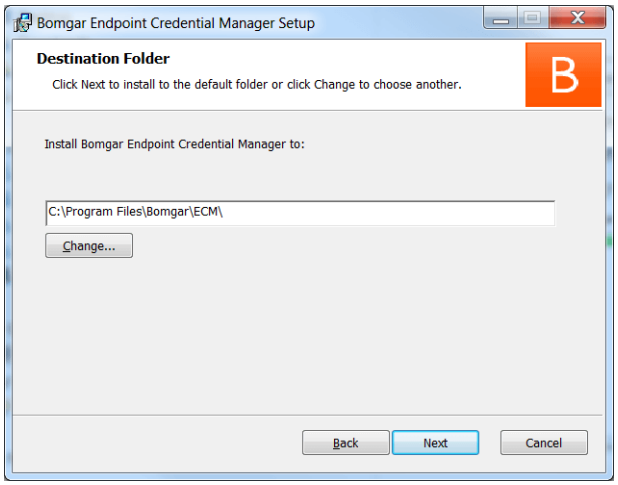
1. Um zu beginnen, laden Sie den Bomgar Endpunkt-Anmeldedaten-Manager (ECM) unter Bomgar-Support auf ssc.bomgar.com herunter. Starten Sie den Installationsassistenten für den Bomgar Endpunkt-Anmeldedaten-Manager.
2. Stimmen Sie den Bedingungen der Endbenutzer-Lizenzvereinbarung zu. Aktivieren Sie das Kontrollkästchen zur Zustimmung und klicken Sie auf **Installieren**.

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

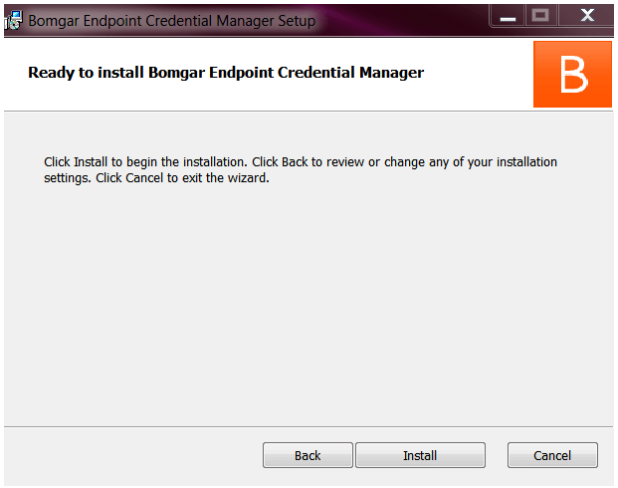
   Klicken Sie auf die Schaltfläche **Optionen**, um den Installationspfad von ECM anzupassen.
3. Klicken Sie auf **Installieren**.



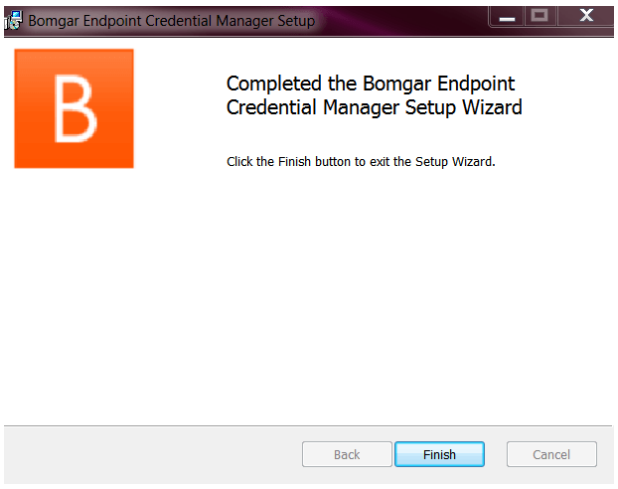
4. Wählen Sie den Installationsort für den Anmeldedaten-Manager und klicken Sie auf **Weiter**.
5. Auf dem nächsten Bildschirm können Sie mit der Installation beginnen oder vorherige Schritte überprüfen.



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



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



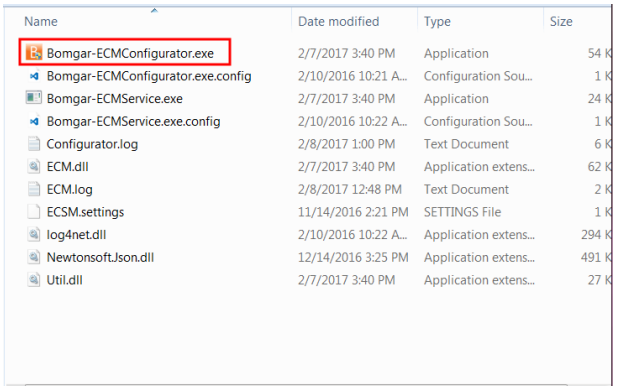
Hinweis: *Um einen ausfallfreien Betrieb zu gewährleisten, können Administratoren bis zu fünf ECMs auf unterschiedlichen Windows-Systemen installieren, um über das Bomgar-Gerät mit der gleichen Site zu kommunizieren. Eine Liste der mit der Geräte-Site verbundenen ECMs finden Sie unter* ***/login > Status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

Hinweis: *Wenn mehrere ECMs mit einer Bomgar-Site verbunden sind, leitet das Bomgar-Gerät Anfragen an den ECM, der am längsten mit dem Gerät verbunden ist.*

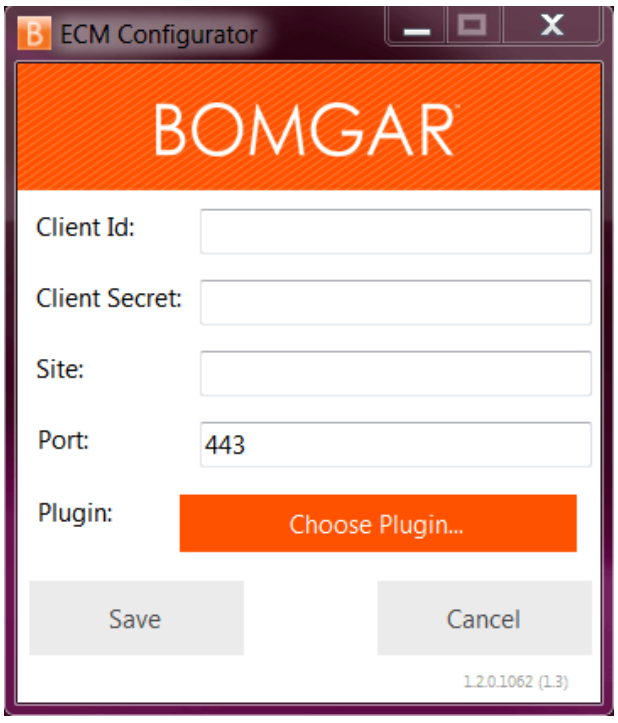
Konfiguration einer Verbindung zu Ihrem Anmeldedaten-Speicher

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

1. Machen Sie den soeben installierten Bomgar ECM-Konfigurator über das Windows-Suchfeld oder durch Aufruf Ihrer **Start**-Programmliste ausfindig.
2. Führen Sie das Programm aus, um eine Verbindung aufzubauen.



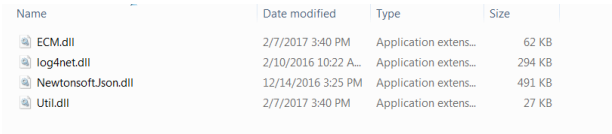
3. Wenn der Konfigurator geöffnet wird, vervollständigen Sie die Felder. Alle Felder müssen ausgefüllt werden.



Geben Sie folgende Werte ein:

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

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



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

WICHTIG

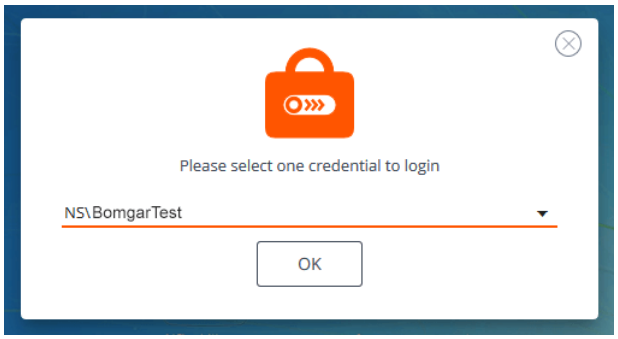
Um die neuen Einstellungen in der Konfiguration zu übernehmen, starten Sie den Anmeldedaten-Manager-Service neu.

Verwendung der Anmeldedaten-Einfügung zum Zugriff auf Endpunkte

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

1. Melden Sie sich in der Privileged Web-Zugriffskonsole 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.



Authentifizierung über die Client-Skripting-API

Mit dieser Funktion können sich Benutzer an der Privileged Web-Zugriffskonsole anmelden und mithilfe der PA Client Skripting-API (https://www.bomgar.com/docs/privileged-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 Geräts 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 Privileged Web-Zugriffskonsole 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 Privileged Web-Zugriffskonsole angemeldet ist und die API **type=rep** aufruft, wird der Benutzer in der Desktop-Zugriffskonsole angemeldet und wird von der Privileged Web-Zugriffskonsole 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 Privileged Web-Zugriffskonsole angemeldet, führt die obige Anforderung den Befehl in der Browser-Registerkarte aus, auf der die Privileged Web-Zugriffskonsole 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 Privileged Web-Zugriffskonsole 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 Privileged Web-Zugriffskonsole 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 Privileged Web-Zugriffskonsole 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 davon zurückkehren. Um zu einem Endpunkt zurückzukehren, auf den Sie bereits in einer anderen Sitzung zugreifen, folgen Sie den folgenden Schritten:

1. Klicken Sie auf das Dropdown-Menü **Sitzungen**.

> ***Hinweis:*** *Die im Dropdown-Menü* ***Sitzungen*** *aufgeführte Nummer gibt an, auf wie viele Sitzungen Sie gleichzeitig zugreifen.*

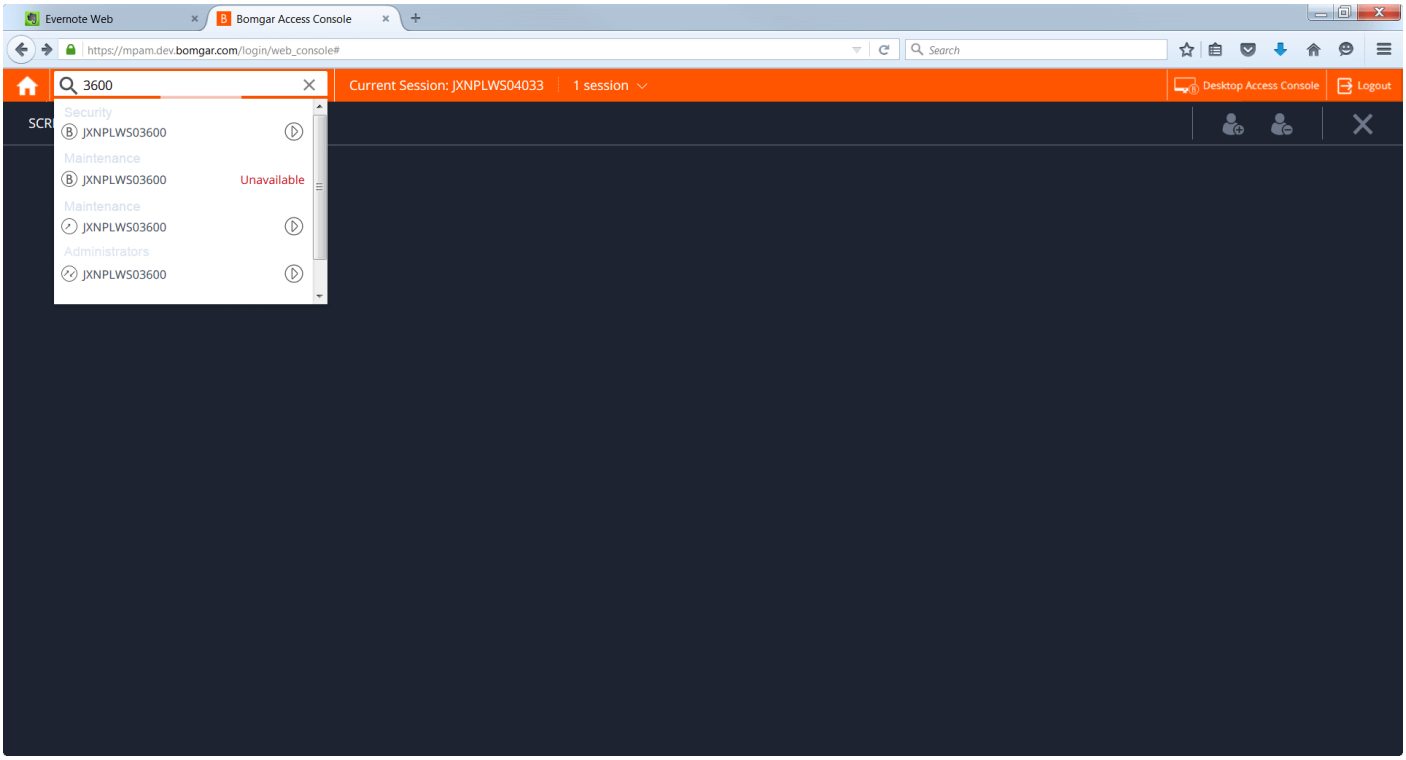
2. Wählen Sie einen Endpunkt aus der Liste.

3. Dann gelangen Sie zur Sitzung dieses Endpunktes.

Suchen nach Endpunkten

Bei der Verwendung der Privileged Web-Zugriffskonsole 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.

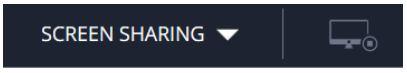
1. Klicken Sie auf das Symbol **Suchen** oben links auf dem Bildschirm.
2. Geben Sie in der Suchleiste den Namen des Endpunktes ein.
3. Wählen Sie aus den Suchergebnissen den Endpunkt, mit dem Sie eine Sitzung starten möchten und klicken Sie auf die Schaltfläche **Start**, um eine Sitzung zu beginnen.



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.

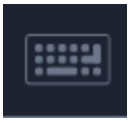
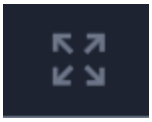
1. Klicken Sie im Sitzungsfenster auf das Dropdown-Menü **Sitzungsfreigabe** und wählen Sie die Option **Bildschirmfreigabe**. Alternativ können Sie auf das Symbol **Bildschirmfreigabe beginnen** klicken, um mit dem Zugriff auf den Endpunkt zu beginnen, falls die Bildschirmfreigabe nicht automatisch 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.
	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 Bomgar-Benutzer die Kundenansicht deaktiviert hat. Der Endbenutzer kann durch Drücken von **Strg-Alt-Entf** stets wieder die Kontrolle übernehmen. 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 und höher 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 Endpoint Credential Managers erfordert eine separate Dienstleistungsvereinbarung mit Bomgar. Nach Abschluss einer Dienstleistungsvereinbarung können Sie die erforderliche Middleware vom Bomgar Self-Service Center herunterladen.

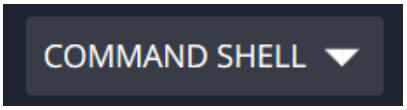
	Schalten Sie die virtuelle Tastatur ein oder aus.
	Schaltet die Zwischenablage ein oder aus.
	Einen alternativen Remote-Bildschirm für die Anzeige auswählen. Der primäre Monitor wird mit einem **P** gekennzeichnet.
	Den Remote-Bildschirm in der tatsächlichen Größe oder skaliert anzeigen.
	Wählen Sie 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.

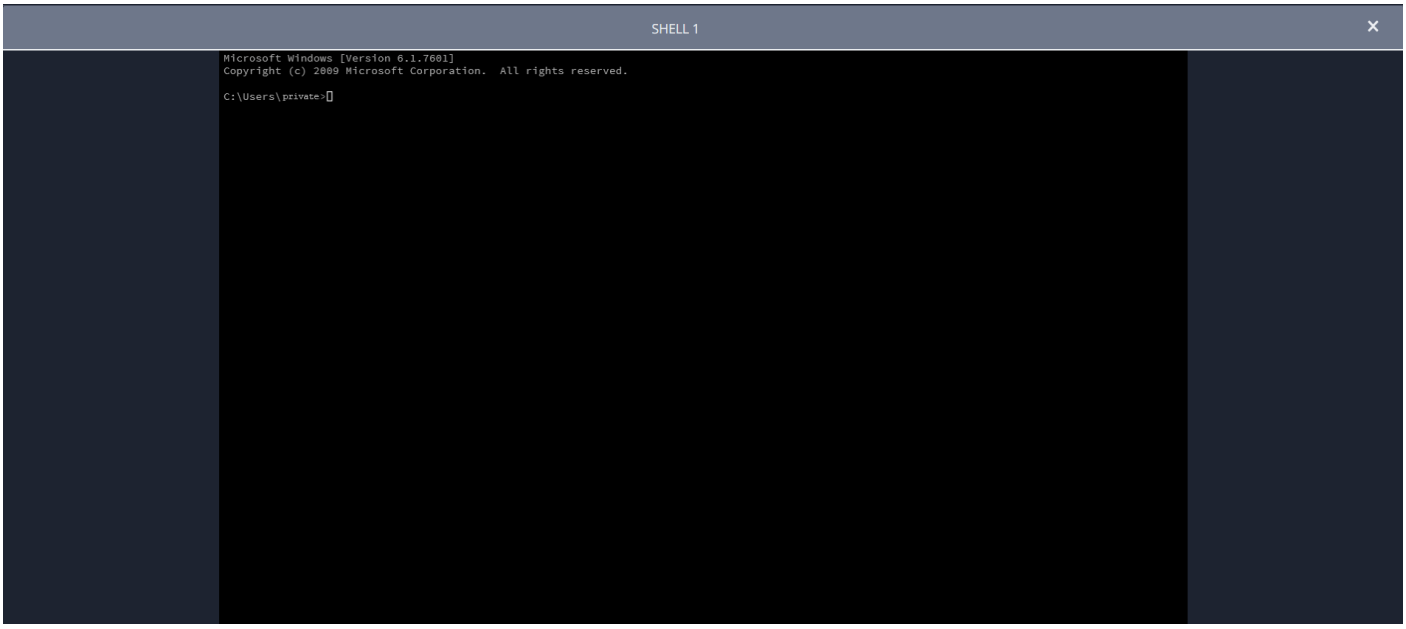
Öffnen der Befehlsshell am Remote-Endpunkt mit der Privileged Web-Konsole

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.

1. Um in einer Zugriffssitzung auf die **Befehlsshell** zuzugreifen, klicken Sie auf das Dropdown-Menü **Bildschirmfreigabe** oben rechts auf dem Bildschirm.
2. Wählen Sie die Option **Befehlsshell**.
3. Nach Wahl der Option **Befehlsshell** erscheinen die Befehlsoptionen und die Eingabeaufforderung.





Befehlsshell-Werkzeuge

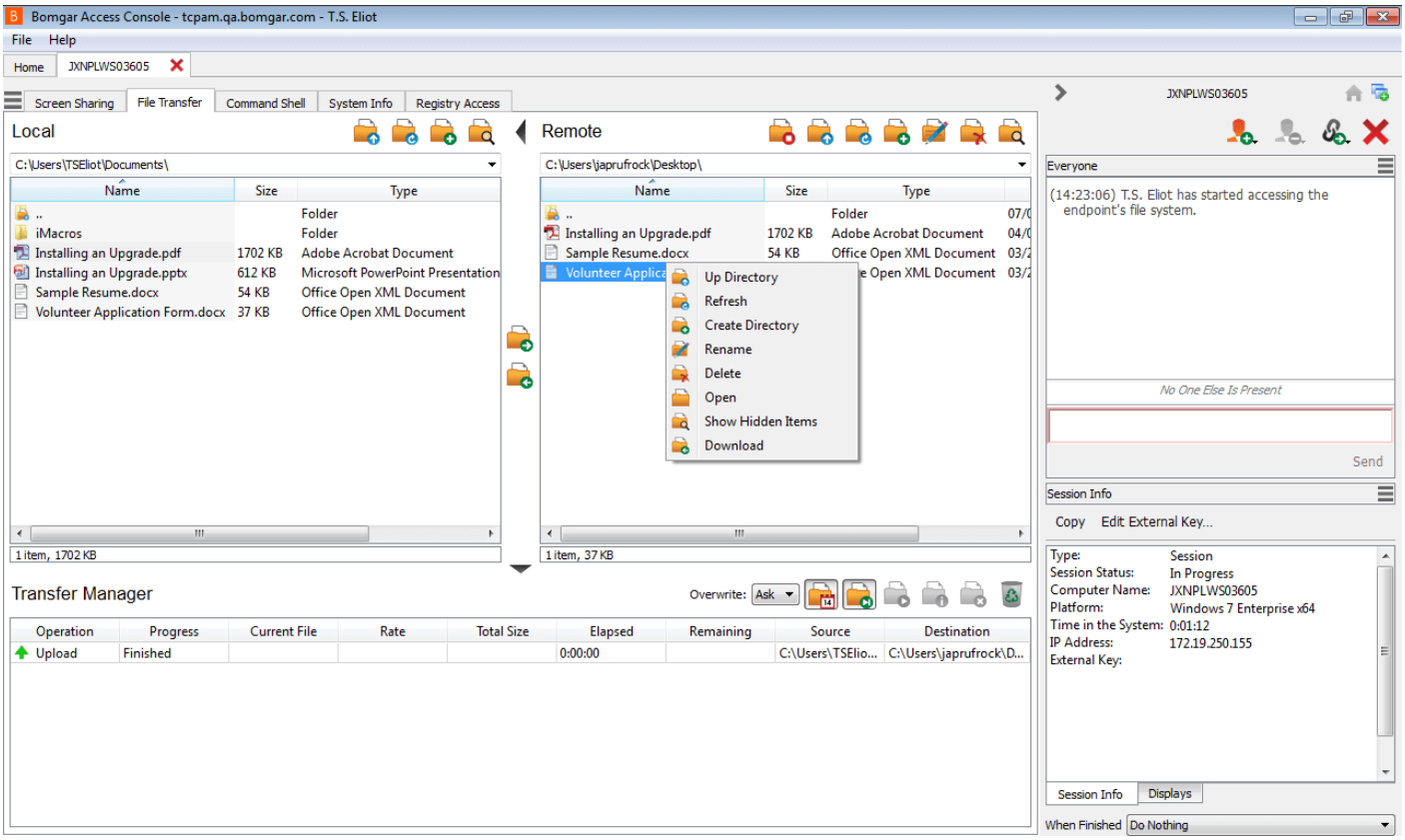
	Zugriff auf die Eingabeaufforderung stoppen, wenn er nicht mehr benötigt ist.
	Öffnen Sie eine neue Shell, um mehrere Instanzen der Eingabeaufforderung auszuführen, oder schließen Sie einzelne Shells, ohne den Eingabeaufforderungs-Zugriff aufzugeben. Die einzelnen Instanzen werden als Registerkarten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

Dateitransfer zum und vom Remote-Endpunkt

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

Je nach den Berechtigungen, die Ihr Administrator für Ihr Konto festgelegt haben, können Sie nur Dateien auf das Remote-System hochladen oder auch Dateien auf Ihren lokalen Computer herunterladen. Der Dateisystemzugriff kann ebenfalls auf bestimmte Pfade auf dem Remote- oder lokalen System beschränkt sein, wodurch durchgesetzt wird, dass Uploads oder Downloads nur in bestimmten Verzeichnissen erfolgen.

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



Werkzeuge für den Dateitransfer

	Zugriff auf das Dateisystem des Remote-Geräts stoppen, wenn es nicht mehr benötigt wird.
	Ein Verzeichnis im ausgewählten Dateisystem nach oben wechseln.

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

Freigabe einer Sitzung für andere Benutzer über die Privileged Web-Zugriffskonsole

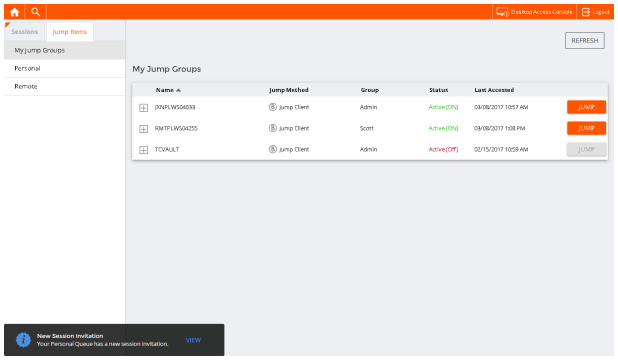
Innerhalb einer Sitzung können Sie ein Teammitglied auffordern, an einer Zugriffssitzung teilzunehmen. Folgen Sie zur Freigabe einer Sitzung diesen Schritten:

1. Klicken Sie auf das Symbol **Sitzung freigeben**.

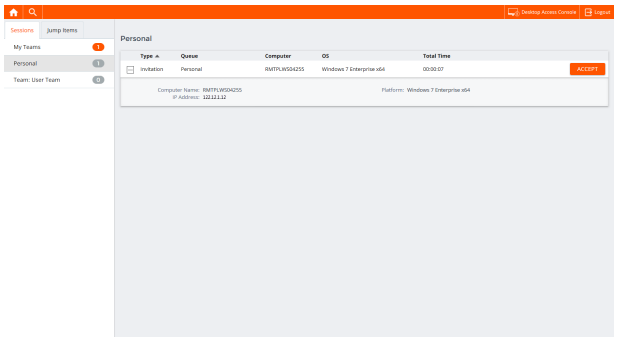
2. Wählen Sie das Team, dem der Benutzer angehört, aus dem Menü.

3. Wählen Sie aus der Teamliste den Benutzer, für den Sie die Sitzung freigeben möchten.

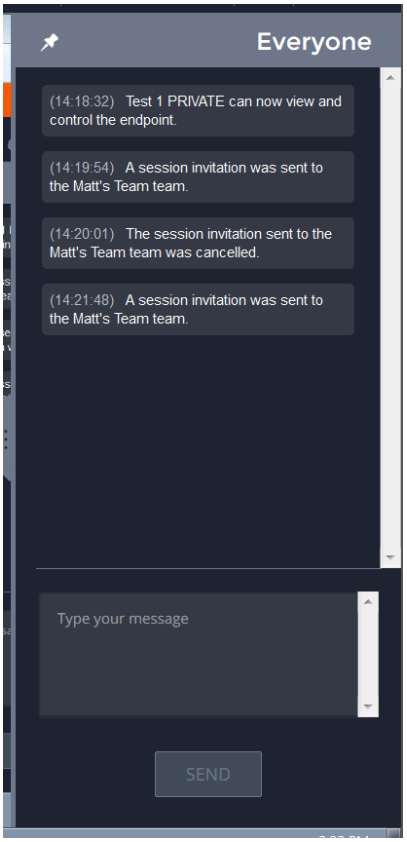
4. Der eingeladene Benutzer sieht eine Benachrichtigung in der unteren linken Ecke des Bildschirms, die auf eine neue Sitzungseinladung hinweist.



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, vorausgesetzt, dass diese zumindest ein Mitglied mit aktivierter erweiterter Verfügbarkeit enthalten.

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:

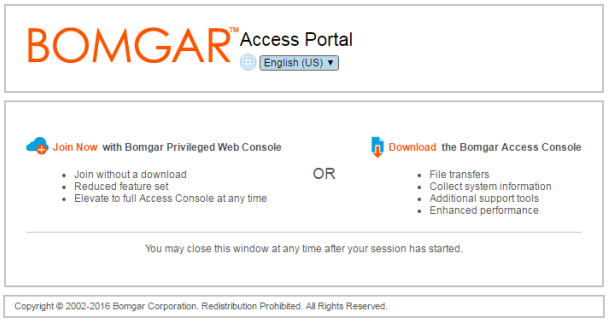
- Der einladende Benutzer die Einladung zurückzieht.
- Der einladende Benutzer die Sitzung verlässt.
- Die Sitzung endet.
- Der eingeladene Benutzer die Einladung annimmt.

Einladen eines externen Benutzers zur Teilnahme an einer Privileged Access-Sitzung

In einer Sitzung können Sie einen externen Benutzer dazu auffordern, einmalig an einer Sitzung teilzunehmen. Um einen externen Benutzer zu einer Sitzung einzuladen, folgen Sie diesen Schritten.

1. Klicken Sie während einer Sitzung auf die Schaltfläche **Sitzung freigeben**.
2. Wählen Sie im Menü **Externen Support-Techniker einladen**.
3. Wählen Sie eine Sicherheitsrichtlinie. Diese Richtlinien werden in der /login-Verwaltungsschnittstelle erstellt und bestimmen, welche Berechtigungen der externe Benutzer hat. Wenn Sie ein Profil auswählen, wird die vollständige Beschreibung darunter angezeigt.
4. Geben Sie den Namen des eingeladenen Benutzers ein. Dieser Name wird im Chatfenster und in Berichten angezeigt.
5. Geben Sie dann Kommentare dazu ein, warum dieser Benutzer eingeladen wurde.

6. Klicken Sie auf **Senden**. Es wird ein neues Dialogfeld mit der Einladungs-URL angezeigt.
7. Abhängig von den von Ihrem Administrator gewählten Optionen sind Sie möglicherweise in der Lage, die Einladung über Ihren lokalen E-Mail-Client oder serverseitig zu versenden. Sie können auch die direkte URL kopieren und einfügen und diese so dem Benutzer zukommen lassen.
8. Wenn der externe Benutzer auf die URL zur Zugriffseinladung klickt, hat er die Option, der Sitzung mithilfe der Privileged Web-Zugriffskonsole beizutreten, oder die Desktop-Zugriffskonsole herunterzuladen und zu installieren.
9. Sobald er die Privileged Web-Zugriffskonsole gewählt oder die Desktop-Zugriffskonsole installiert hat, kann er der Sitzung beitreten.



Hinweis: *Hier einige Tipps zur Einladung externer Benutzer:*

- *Ein Benutzer hat nur Zugriff auf die Sitzungsregisterkarte und verfügt über eingeschränkte Berechtigungen.*
- *Der externe Benutzer kann nie der Eigentümer der Sitzung sein.*
- *Wenn der einladende Benutzer die Sitzung verlässt, wird der externe Benutzer abgemeldet.*
- *Sie können mehr als einen externen Benutzer zu einer Sitzung einladen.*
- *Der externe Benutzer kann zur Desktop-Zugriffskonsole heraufsetzen. Wenn die Schaltfläche **Heraufsetzen** geklickt wird, öffnet sich eine neue Browser-Registerkarte, die den Benutzer zur Zugriffseinladungs-URL für die Desktop-Zugriffskonsole weiterleitet.*

Ein Mitglied aus einer Privileged Web-Zugriffskonsolen-Sitzung entfernen

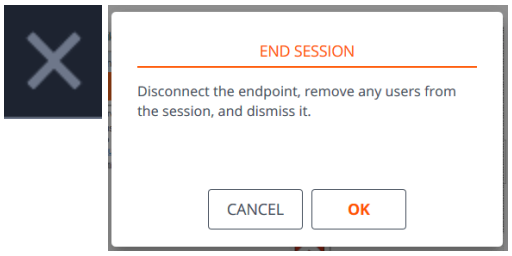
Falls erforderlich, können Sie einen anderen Benutzer aus einer freigegebenen Zugriffssitzung entfernen. Um einen Benutzer zu entfernen, klicken Sie auf das Symbol **Mitglied entfernen**.

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 der 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.

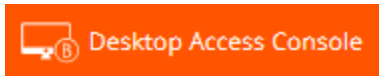


3. Wenn Sie auf **OK** klicken, wird die Sitzung beendet und Sie kehren zur Liste **Alle Jump-Elemente** zurück.

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

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

1. Um die native Desktop-Zugriffskonsole über die Privileged Web-Zugriffskonsole herunterzuladen, klicken Sie auf die Schaltfläche **Native Zugriffskonsole ausführen** oben rechts auf dem Bildschirm.



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.*