



BeyondTrust

Privilegierter Remote-Zugriff Android-Zugriffskonsole 2.2.7

Inhaltsverzeichnis

Handbuch für die BeyondTrust Android-Zugriffskonsole	3
Installation der Zugriffskonsole auf Android	4
Anmelden in der Zugriffskonsole für Android	5
Ändern der Einstellungen in der Android-Zugriffskonsole	8
Verwenden von Jump-Elementen zum Zugriff auf Endpunkte über die Android-Zugriffskonsole	9
Autorisierung durch Endbenutzer oder Drittpartei	9
Daten zur automatischen Anmeldung	11
Anmelden an Endpunkten mit Anmeldedaten-Einfügung in der Android-Zugriffskonsole	12
Installation und Konfiguration des Endpunkt-Anmeldedaten-Managers	12
Installation und Konfiguration des Plugins	14
Konfiguration einer Verbindung zu Ihrem Anmeldedaten-Speicher	15
Verwendung der Anmeldedaten-Einfügung zum Zugriff auf Endpunkte	16
Team-Chat zum Chatten mit anderen Benutzern in der Android-Zugriffskonsole verwenden	18
Zugriffssitzungen in der Android-Zugriffskonsole anzeigen	19
Bildschirmfreigabe mit dem Endpunkt über die Android-Zugriffskonsole	20
Freigabe einer Sitzung für andere Benutzer über die Android-Zugriffskonsole	22
Einladen externer Support-Techniker zur Teilnahme an einer Sitzung über die Android-Konsole des Support-Technikers	23
Über die Android-Zugriffskonsole ein Mitglied aus der Sitzung entfernen	25
Öffnet die Befehlsshell an einem Remote-Endpunkt mithilfe der Android-Zugriffskonsole	26
Endpunkt-Systeminformationen über die Android-Zugriffskonsole anzeigen	28
Über die Android-Zugriffskonsole eine Zusammenfassung der Zugriffssitzung anzeigen und Notizen hinzufügen	29
Über die Android-Zugriffskonsole eine Sitzung schließen	30

Handbuch für die BeyondTrust Android-Zugriffskonsole

Dieser Leitfaden soll Ihnen helfen, BeyondTrust auf Ihrem Android-Gerät zu installieren und die Funktionen der Android-access console zu verstehen. BeyondTrust ermöglicht Ihnen den Fernzugriff auf Endpunkte, indem Sie sich über den support_button mit ihnen verbinden.

Beachten Sie: Obwohl Screenshots eines Android-Smartphones in diesem Handbuch verwendet werden, gelten die gleichen Schritte bei der Verwendung eines Android-Tablets.

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.

Installation der Zugriffskonsole auf Android

Die BeyondTrust access console für Android steht kostenlos bei Google Play zum Download zur Verfügung. Suchen Sie über Ihr Android-Gerät in Google Play nach „BeyondTrust Access Console“ und installieren Sie dann die App.

Um die BeyondTrust access console auf Ihrem Gerät auszuführen, muss auf Ihrem B Series Appliance Softwareversion 15.2 oder höher ausgeführt werden. Die BeyondTrust access console wird auf Android-Smartphones mit Version 2.3 und höher unterstützt, sowie auf Android-Tablets mit Version 3.0 und höher.



Hinweis: Nur die BeyondTrust access console kann mit einer Privilegierter Remote-Zugriff (PRA) verwendet werden. Die BeyondTrust-Konsole des Support-Technikers kann nicht für die Verbindung mit einer Privilegierter Remote-Zugriff-Website verwendet werden. Ferner kann die BeyondTrust access console nicht für die Verbindung mit einer BeyondTrust Remote-Support-Website verwendet werden.



WICHTIG!

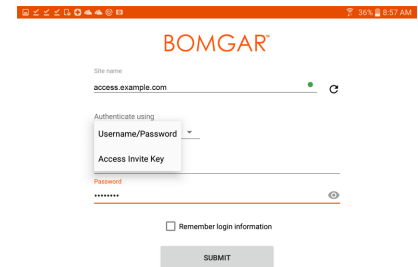
Ihr B Series Appliance muss über ein von einer Zertifizierungsstelle signiertes SSL-Zertifikat verfügen. BeyondTrust unterstützt keine selbstsignierten Zertifikate für die Android-access console.¹ Sobald Sie ein von einer Zertifizierungsstelle signiertes SSL-Zertifikat auf Ihrem B Series Appliance übernommen 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 access console auf Ihrem Gerät ausführen, um von fast überall auf Ihre Endpunkte zuzugreifen.

¹Bei Android-Geräten mit einem Betriebssystem, das älter ist als 4.0, können möglicherweise Zertifikatfehler auftreten, wenn Sie eine Verbindung mit Ihrer BeyondTrust-Website herzustellen zu versuchen. Dieses Problem tritt wegen eines fehlenden Root-SSL-Zertifikats im Zertifikatspeicher des Android-Gerätes auf. Dieses Problem tritt nur aufgrund des Android-Betriebssystems auf und steht nicht mit der BeyondTrust-Software in Zusammenhang. Um dieses Problem zu lösen, aktualisieren Sie entweder das Android-Gerät oder kontaktieren Sie die Zertifizierungsstelle zur Anforderung eines weiteren Root-SSL-Zertifikats, das mit dem Android-Gerät kompatibel ist.

Anmelden in der Zugriffskonsole für Android

Geben Sie auf dem Anmeldebildschirm den Hostnamen Ihrer BeyondTrust-Website ein, wie etwa `access.example.com`. Geben Sie dann den mit Ihrem BeyondTrust-Benutzerkonto verknüpften Benutzernamen und das dazugehörige Kennwort ein. Sie können wählen, dass die BeyondTrust-access console Ihre Anmeldedaten speichert. Tippen Sie dann auf **Anmelden**.

Berechtigte Benutzer oder Anbieter, welche die access console verwenden, können die Authentifizierungsmethode durch Tippen auf die **Benutzername-/Kennwort**-Beschriftung ändern. Wählen Sie **Zugriffseinladungsschlüssel** aus dem Dropdown-Menü, um den Schlüssel einzugeben, den Sie erhalten haben.



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

Anmeldung an der Android-Zugriffskonsole mit SAML for Mobile

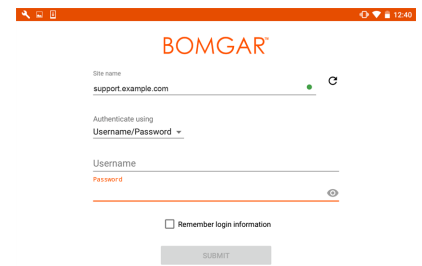
Mit SAML for Mobile können Sie sich leicht und sicher an der Android-access console anmelden. Um mehr über die SAML-Einzelanmeldung zu erfahren, lesen Sie weiter unter [Security Assertion Markup Language](https://en.wikipedia.org/wiki/Security_Assertion_Markup_Language) unter https://en.wikipedia.org/wiki/Security_Assertion_Markup_Language. Folgen Sie den unten beschriebenen Schritten, um mit SAML auf die Android-access console zuzugreifen.



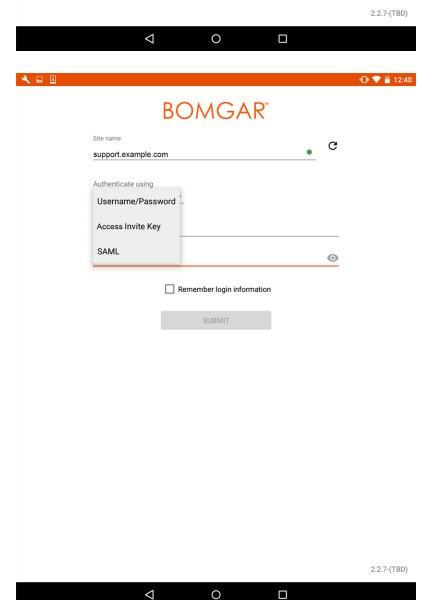
Hinweis: Stellen Sie vor der Anmeldung an der Android-access console mit SAML sicher, dass ein SAML-Anbieter für Ihre /login-Verwaltungsumgebung konfiguriert wurde, indem Sie zu **Benutzer und Sicherheit > Sicherheitsanbieter** navigieren. Wenn SAML nicht in /login konfiguriert ist, steht SAML nicht als Authentifizierungsmethode für die Android-access console zur Verfügung. Weitere Informationen zur Integration von SAML für die Einzelanmeldung in Ihrer BeyondTrust Privilegierter Remote-Zugriff-Umgebung finden Sie in [SAML-Sicherheitsanbieter erstellen und konfigurieren](http://www.beyondtrust.com/docs/privileged-remote-access/how-to/integrations/security-providers/saml/configure-settings.htm) unter www.beyondtrust.com/docs/privileged-remote-access/how-to/integrations/security-providers/saml/configure-settings.htm.

1. Tippen Sie auf die App access console auf Ihrem Android-Gerät.

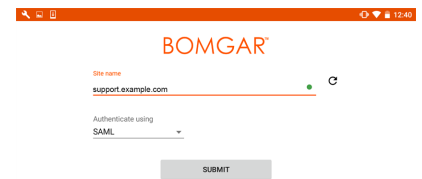
2. Tippen Sie auf dem Anmeldebildschirm auf **Benutzername und Kennwort**.



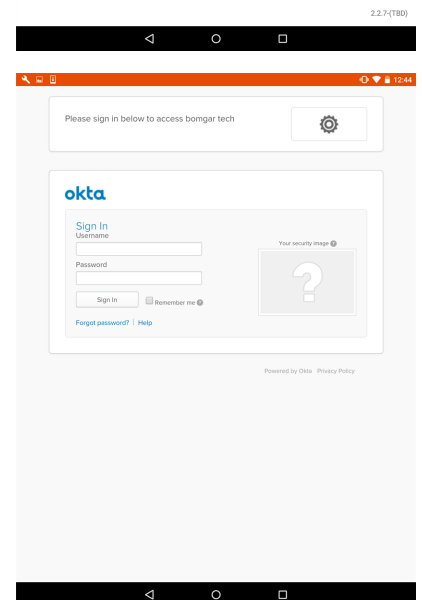
3. Wählen Sie **SAML**.



4. Tippen Sie auf **Senden**.



5. Geben Sie Ihre Anmeldedaten ein, nachdem Sie zur Seite Ihres SAML-Anbieters geleitet wurden.
6. Tippen Sie auf **Anmelden**, um auf die Konsole zuzugreifen.



Ändern der Einstellungen in der Android-Zugriffskonsole

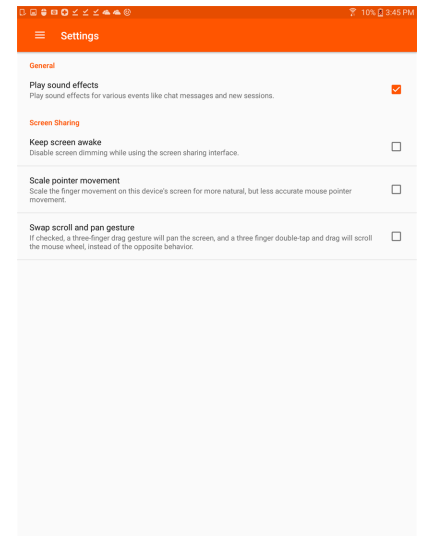
Um Ihre Einstellungen zu ändern, wählen Sie **Einstellungen** aus dem Menü.

Ist **Soundeffekte wiedergeben** aktiviert, spielt Ihr Gerät Audioalarme für bestimmte Ereignisse ab, die in der access console stattfinden.

Um zu verhindern, dass Ihr Bildschirm während der Bildschirmfreigabe verdunkelt wird, aktivieren Sie **Bildschirm aktiviert lassen**.

Ist die Option **Zeigerbewegung skalieren** aktiviert, entspricht der Remote-Zeiger den Bewegungen Ihres Fingers auf dem Bildschirm. Ist die Option deaktiviert, reagiert der Zeiger zwar verzögert, aber seine Position ist präziser.

Über **Scrollen und Schwenken tauschen** können Sie bestimmen, welche von zwei Gesten das Rad der Remote-Maus dreht und welche den Bildschirm schwenkt.



Verwenden von Jump-Elementen zum Zugriff auf Endpunkte über die Android-Zugriffskonsole

Um auf einen einzelnen Endpunkt ohne Endbenutzerunterstützung zuzugreifen, installieren Sie das Jump-Element über die Seite **Jump Clients** der /login-Verwaltungsschnittstelle auf diesem System. Zusätzlich werden die folgenden Jump-Elementtypen von der mobilen access console unterstützt:

- **Remote-Jump**
- **VNC (Remote)**
- **RDP**
- **Shell Jump**

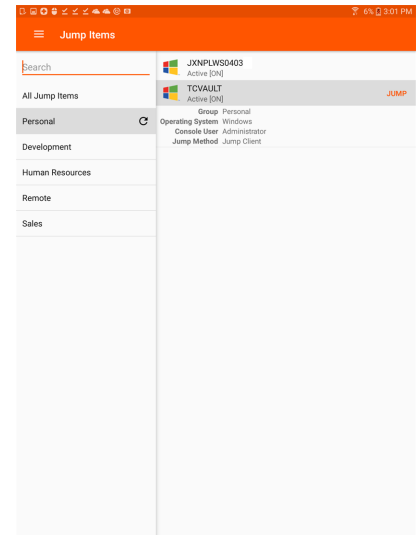
Jump-Elemente werden in Jump-Gruppen aufgeführt. Wenn Sie einer oder mehr Jump-Gruppen zugewiesen werden, können Sie auf die Jump-Elemente in diesen Gruppen zuweisen, wobei die Berechtigungen von Ihrem Administrator festgelegt werden.

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

Um ein Jump-Element zu lokalisieren, tippen Sie auf die Option **Jump-Elemente** aus dem Menü.

Wählen Sie einen Standort und tippen Sie auf die Schaltfläche **Aktualisieren**. Wenn Sie den Endpunkt gefunden haben, auf den Sie zugreifen möchten, wählen Sie den Eintrag aus, um Details anzuzeigen.

Tippen Sie auf die Schaltfläche **Jump**, um eine Sitzung zu starten.

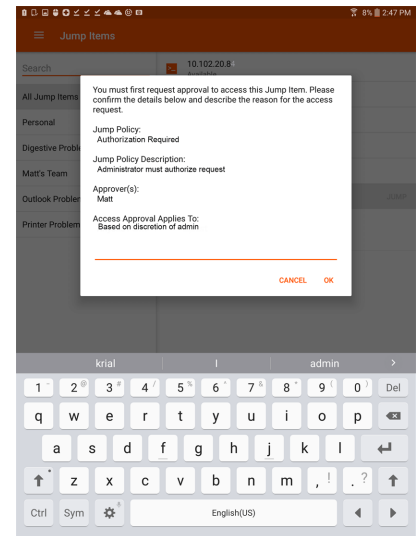


Autorisierung durch Endbenutzer oder Drittpartei

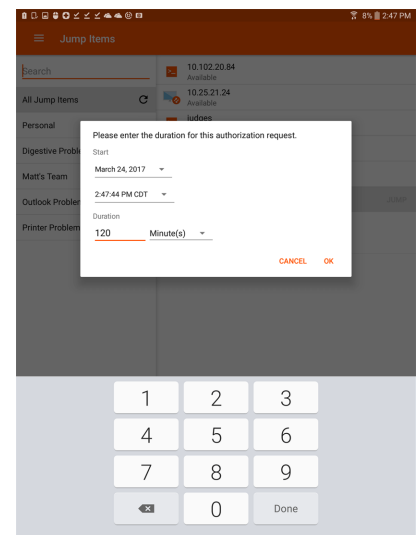
Abhängig von der Konfiguration von Jump-Elementen innerhalb der /login-Verwaltungsschnittstelle kann ein Jump-Element über eine zugeordnete Jump-Richtlinie verfügen. Die Richtlinie kann eine Autorisierungskomponente definieren, die Sie zwingt, eine Berechtigung von Dritten oder einem Administrator anzufordern,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

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

Nachdem Sie auf die Jump-Schaltfläche getippt und den Zugriff angefordert haben, erscheint eine Aufforderung und Sie müssen die Begründung für den Zugriff auf das System eingeben.



Als nächstes müssen Sie angeben, wann und für wie lange Sie auf das System zugreifen wollen.



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. 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.

Bomgar

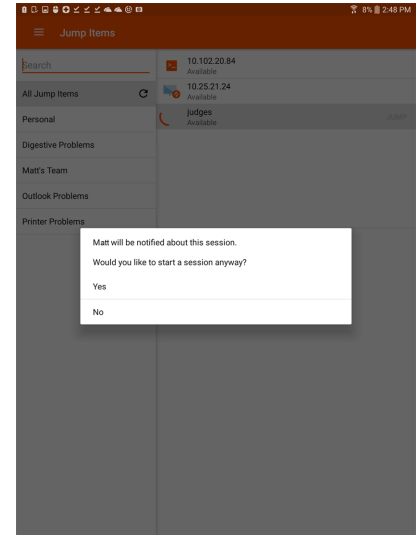
Your jump authorization request number 1 beginning at 05/31/49198 10:19:53 PM has been approved.

OK

Nach dem Tippen auf die Jump-Schaltfläche sehen Sie eine Meldung, die Sie fragt, ob Sie eine Zugriffssitzung beginnen möchten. Wenn Sie die Sitzung beginnen möchten, erscheinen die Kommentare der genehmigenden Partei und Sie können mit dem Zugriff auf das System beginnen.

Entscheidet sich der Benutzer für die Fortsetzung, erscheinen die Kommentare der genehmigenden Partei und der Benutzer kann die Arbeit mit dem System beginnen.

Weitere Informationen dazu, wie Jump-Elemente mit Jump-Zeitplänen, Ticket-ID-Workflow usw. funktionieren, finden Sie unter [Jump-Schnittstelle: Verwenden von Jump-Elementen zum Zugriff auf Remote-Systeme](#).



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 Anmeldedatenpeicher wählen oder manuell seine eigenen Anmeldedaten eingeben.

i 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.

Anmelden an Endpunkten mit Anmeldedaten-Einfügung in der Android-Zugriffskonsole

Beim Zugriff auf Windows-basierte Jump-Clients über die mobile access console können Sie Anmeldedaten aus einem Anmeldedaten-Speicher verwenden, um sich am Endpunkt anzumelden oder Anwendungen als Administrator auszuführen.

Stellen Sie vor Verwendung der Anmeldedaten-Einfügung sicher, dass ein Kennwortspeicher zur Verfügung steht, um sich mit BeyondTrust PRA zu verbinden, wie z. B. ein Passwort-Vault.

Installation und Konfiguration des Endpunkt-Anmeldedaten-Managers

Anforderungen:

- 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

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.



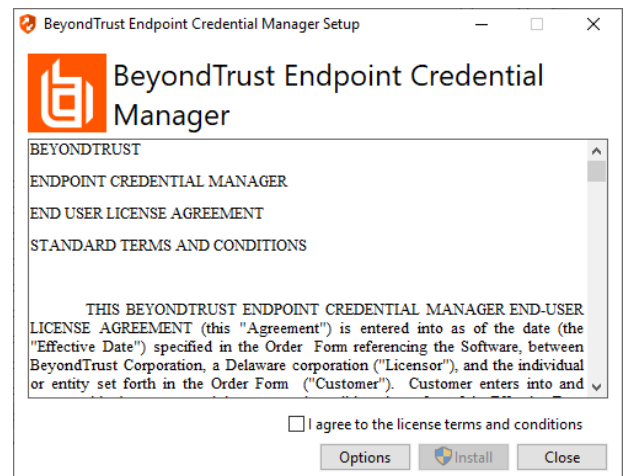
Hinweis: Der Endpunkt-Anmeldedaten-Manager muss in Ihrem Netzwerk installiert werden, damit der zugehörige BeyondTrust-Dienst aktiviert und die Anmeldedateneinfügung in BeyondTrust PRA ermöglicht werden kann.

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

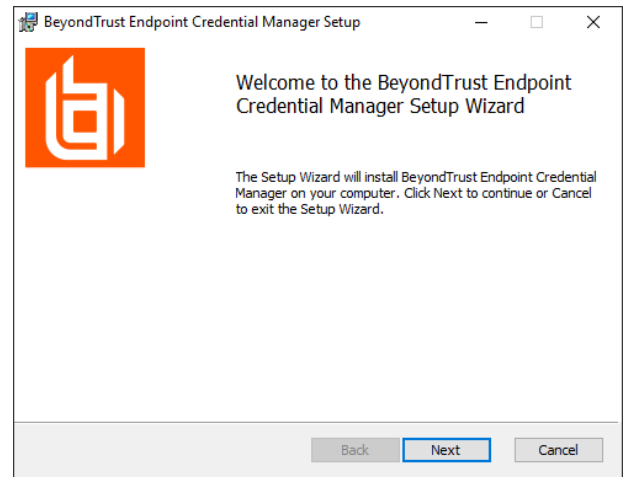
Wenn Sie den Installationspfad von ECM anpassen müssen, klicken Sie auf die Schaltfläche **Optionen**.



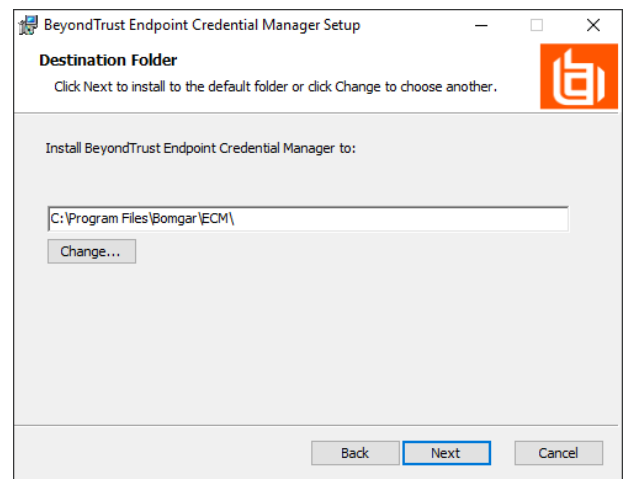
Hinweis: Sie können mit der Installation erst fortfahren, wenn Sie der Endbenutzer-Lizenzvereinbarung zustimmen.



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

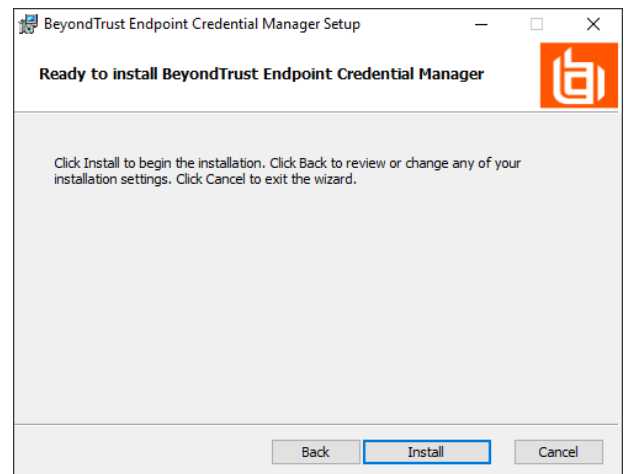


5. Wählen Sie den Installationsort für den Anmeldedaten-Manager und klicken Sie dann auf **Weiter**.

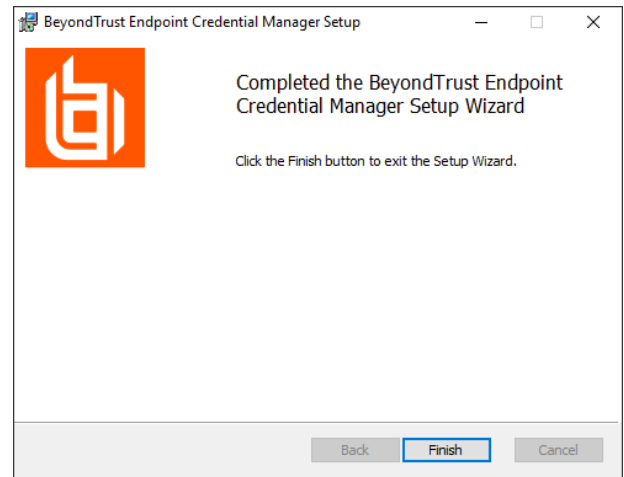


6. Auf dem nächsten Bildschirm können Sie mit der Installation beginnen oder vorherige Schritte überprüfen.

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



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



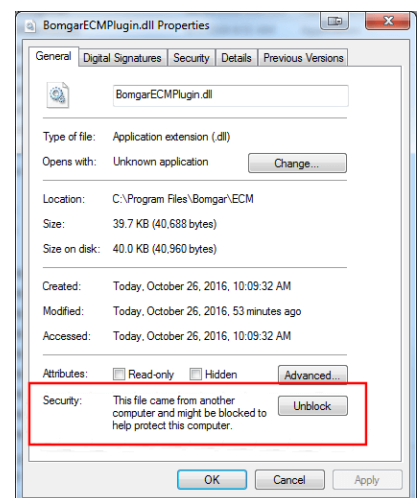
Hinweis: Um einen ausfallfreien Betrieb zu gewährleisten, können Administratoren bis zu drei ECMs auf unterschiedlichen Windows-Systemen installieren, um mit dem gleichen Anmeldedatenspeicher zu kommunizieren. Eine Liste der mit der Geräte-Site verbundenen ECMs finden Sie in **/login > Status > Informationen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



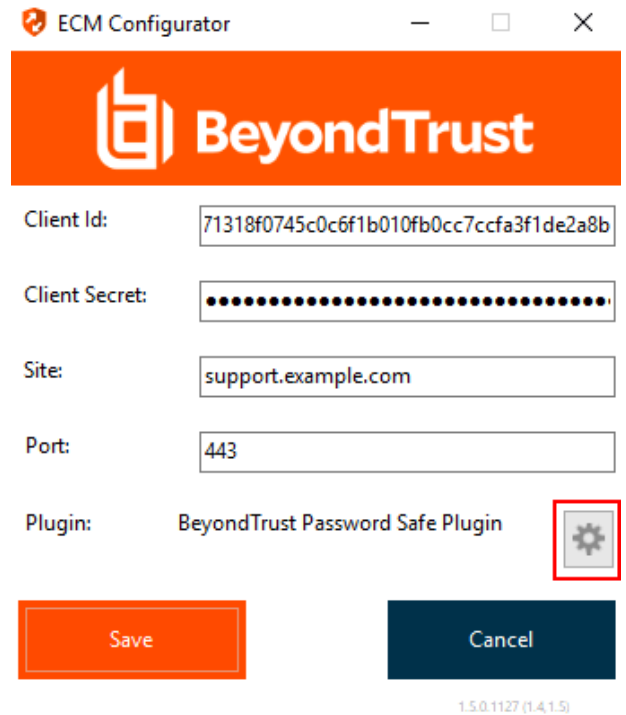
Hinweis: Wenn ECMs in einer Konfiguration mit hoher Verfügbarkeit verbunden sind, leitet das BeyondTrust Appliance B Series Anfragen an den ECM in die ECM-Gruppe, die am längsten mit dem Gerät verbunden ist.

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.



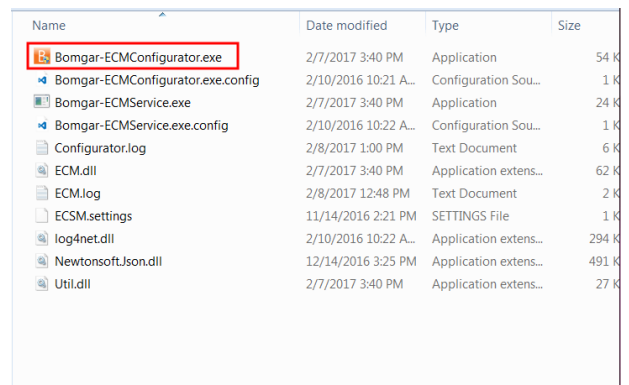
4. Klicken Sie auf das Zahnrad-Symbol im Fenster **Konfigurator**, um die Plugin-Einstellungen zu konfigurieren.



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 **Startmenü** ausfindig.
2. Führen Sie das Programm aus, um eine Verbindung aufzubauen.



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


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.

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

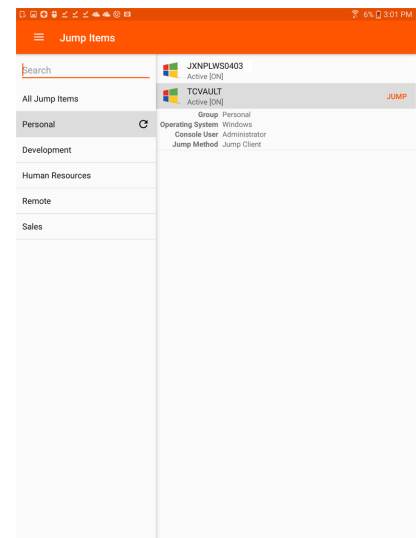
Name	Date modified	Type	Size
ECM.dll	2/7/2017 3:40 PM	Application extens...	62 KB
log4net.dll	2/10/2016 10:22 A...	Application extens...	294 KB
Newtonsoft.Json.dll	12/14/2016 3:25 PM	Application extens...	491 KB
Util.dll	2/7/2017 3:40 PM	Application extens...	27 KB

 **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.

Verwendung der Anmeldedaten-Einfügung zum Zugriff auf Endpunkte

Nachdem der Anmeldedaten-Speicher konfiguriert und eine Verbindung aufgebaut wurde, kann BeyondTrust PRA mit der Verwendung von Anmeldedaten des Anmeldedaten-Speichers zur Anmeldung an Endpunkten beginnen.

- Navigieren Sie zu Ihrer **Jump-Element-Liste**.
- Tippen Sie auf das Jump-Element, auf das Sie zugreifen möchten.
- Tippen Sie auf **Jump**.



- Die Aufforderung **Anmeldedaten eingeben** erscheint. Tippen Sie auf **Anmeldedaten-Speicher**.
- Tippen Sie auf die Anmeldedaten, die Sie zum Zugriff auf das System verwenden möchten.
- Tippen Sie auf **OK**.

Enter Credentials

These credentials will be used to connect to VAULT2.

Credential Store

qavault\vault

Specific User

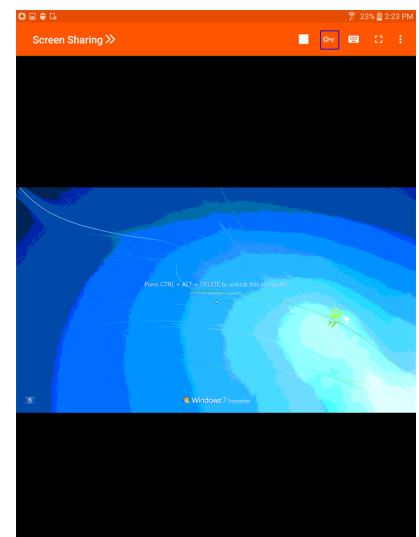
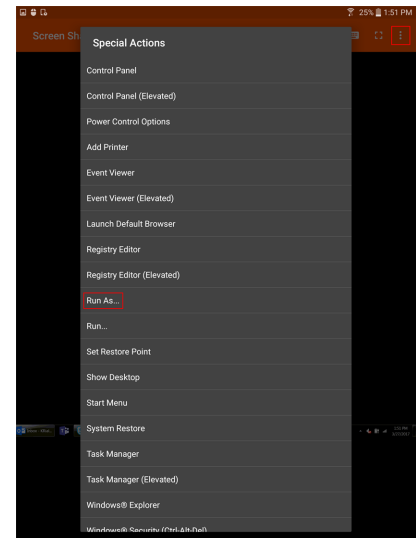
Username/Password

Username

Password

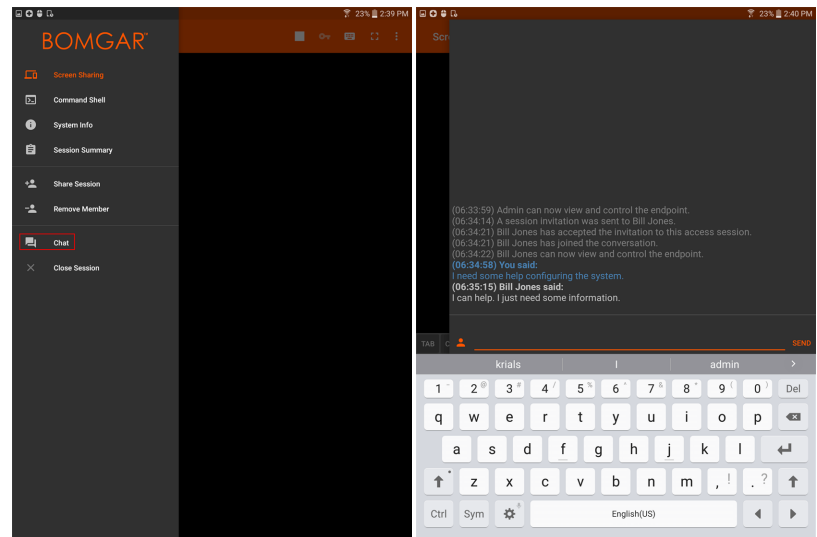
CANCEL OK

7. Tippen Sie in der Sitzung auf die Schaltfläche **Start**, um mit der Bildschirmfreigabe zu beginnen.
 8. Tippen Sie auf die Option **Spezielle Aktionen**. Tippen Sie auf **Ausführen als....**
 9. Tippen Sie auf **Windows Security (Strg-Alt-Entf)**.
-
10. Tippen Sie auf das **Schlüssel**-Symbol. Mit dem Schlüsselsymbol kann das System Ihre gespeicherten Anmeldedaten anzeigen, um sich Zugang zum Endpunkt zu verschaffen



Team-Chat zum Chatten mit anderen Benutzern in der Android-Zugriffskonsole verwenden

Mit Tipp auf die Option **Chat** können Sie mit anderen angemeldeten Teammitgliedern chatten. Sind Sie Mitglied eines oder mehrerer Teams, wählen Sie aus der Liste das Team, mit dem Sie chatten möchten. Sie können mit allen Mitgliedern dieses Teams chatten oder einen Namen aus der Mitgliederliste auswählen und nur mit diesem Benutzer chatten.

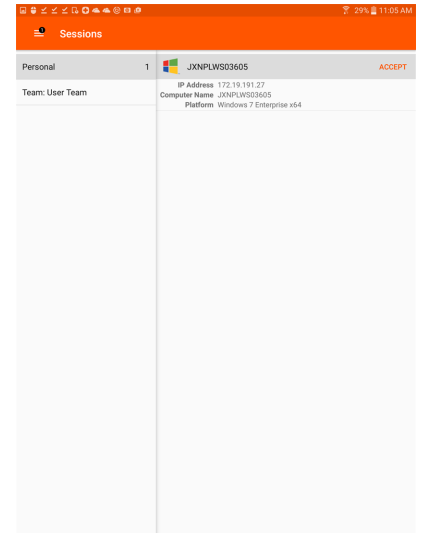


Zugriffssitzungen in der Android-Zugriffskonsole anzeigen

In der access console sind aktive Zugriffssitzungen in Team-Warteschlangen unterteilt. Wenn Sie auf die Option **Sitzungen** im Menü tippen, wird eine Liste aller konfigurierter Warteschlangen angezeigt. Diese Warteschlangen entsprechen den Teams, die in der /login-Verwaltungsschnittstelle eingerichtet wurden. Sobald ein Team definiert wurde, wird eine Warteschlange im Bereich **Sitzungen** der access console verfügbar.

Die **persönliche** Warteschlange enthält Sitzungen, die von einem anderen Teammitglied für Sie freigegeben wurden. Die verbleibenden Warteschlangen stehen für bestimmte Teams, denen Sie angehören.

Tippen Sie auf einen Team-Warteschlangennamen, um laufende Sitzungen anzuzeigen. Die Nummer neben der Sitzungsoption zeigt an, wie viele Sitzungen in dieser Warteschlange laufen.



Personal	1	JKNPLWS03605	ACCEPT
Team: User Team		IP Address 172.19.191.27 Computer Name JKNPLWS03605 Platform Windows 7 Enterprise x64	

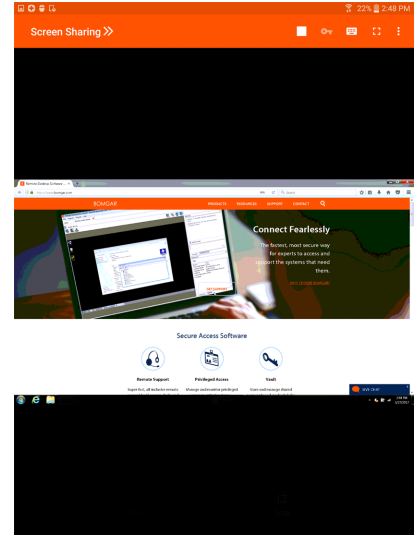


Hinweis: Wenn eine Sitzung für Sie freigegeben wurde, tippen Sie auf die Warteschlange, in der sich die Sitzung befindet. Tippen Sie dann auf die Sitzung. Wählen Sie **Akzeptieren**. Mit der Annahme einer Sitzung wird diese auf Ihrem Gerät geöffnet.






Bildschirmfreigabe mit dem Endpunkt über die Android-Zugriffskonsole


Wenn die Bildschirmfreigabe nicht automatisch startet, tippen Sie auf die **Wiedergabeschaltfläche** oben auf der Seite **Bildschirmfreigabe**, um die Anzeige und Steuerung des Remote-Systems anzufordern. Sie verfügen über die komplette Maus- und Tastatursteuerung des Remote-Systems, wodurch Sie so auf dem Remote-Computer arbeiten können, als ob Sie davor sitzen würden.

- Tippen Sie einmal, um linkszuklicken.
- Doppelklicken Sie, um zu doppelklicken.
- Platzieren Sie Ihren Finger auf dem Cursor und ziehen Sie ihn, um mit der Maus zu navigieren.
- Doppeltippen Sie auf ein Element und ziehen Sie es für Drag and Drop-Verhalten.
- Ziehen Sie zwei Finger zusammen, um den Remote-Bildschirm in einer skalierten Größe oder in voller Auflösung anzuzeigen. Ein Zoom erfolgt dort, wo die Finger platziert werden, unabhängig von der aktuellen Cursorposition.
- Tippen Sie mit zwei Fingern, um rechtszuklicken.
- Scrollen Sie mit dem Mousrad, indem Sie mit drei Fingern ziehen.
- Tippen Sie mit drei Fingern, um die Tastatur ein- oder auszublenden.
- Tippen und halten Sie, um den Cursor ausfindig zu machen.



Bildschirmfreigabe-Werkzeuge

 	Bildschirmfreigabe anfordern oder beenden.
Bildschirmfreigabe	
	Sehen Sie sich zusätzliche Aktionen an, die bei der Bildschirmfreigabe verfügbar sind.
Hilfe	
	Greifen Sie auf die Tastatur zu, um auf dem Remote-Bildschirm zu tippen.
Tastatur	
	Wählen Sie aus zusätzlichen Bildschirmfreigabe-Aktionen und -Werkzeugen.
Optionen	

	Zeigen Sie den Remote-Desktop im Vollbildmodus an.
Vollbildschirm	

Zusätzliche Bildschirmfreigabe-Aktionen und -Werkzeuge

Spezielle Aktionen - Führen Sie eine spezielle Aktion auf dem Remote-System aus. Je nach Betriebssystem und Konfiguration des Remote-Computers variieren die verfügbaren Aufgaben.

In Zwischenablage einfügen - Fügt Elemente in die Zwischenablage Ihres Geräts ein.

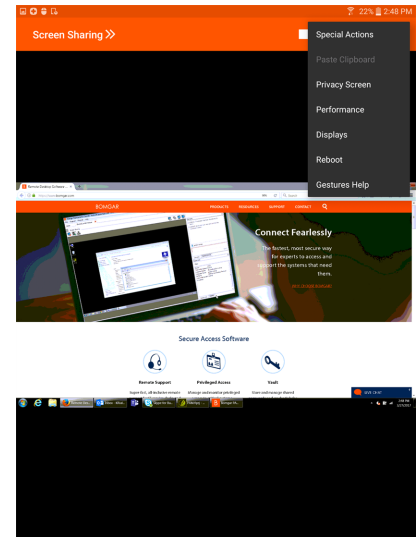
Privater Bildschirm - Deaktiviert die Bildschirmanzeige sowie die Maus- und Tastatureingabe des Remote-Benutzers. Die eingeschränkte Endpunktinteraktion ist nur beim Zugriff auf macOS- oder Windows-Computer verfügbar. Die eingeschränkte Kundeninteraktion ist nur bei der Unterstützung von Windows-Computern verfügbar. In Windows Vista und höher muss der endpoint client heraufgesetzt werden. In Windows 8 ist dieses Feature auf die Deaktivierung von Maus und Tastatur beschränkt.

Leistung - 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.

Displays - Wählen Sie einen alternativen Remote-Monitor zur Anzeige. Der primäre Monitor wird hervorgehoben.

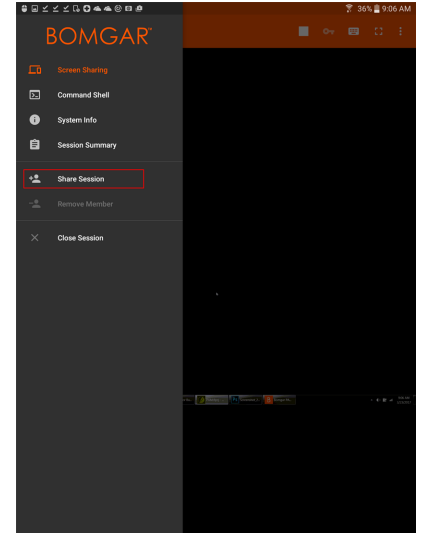
Neustart - Tippen Sie darauf, um das Remote-System neu zu starten.

Gestenhilfe - Tippen Sie darauf, um Tipps zur Navigation in der mobilen Zugriffskontrolle zu erhalten.



Freigabe einer Sitzung für andere Benutzer über die Android-Zugriffskonsole

Um eine Sitzung für ein anderes Teammitglied freizugeben, tippen Sie auf die Option **Sitzung freigeben** im Menü.

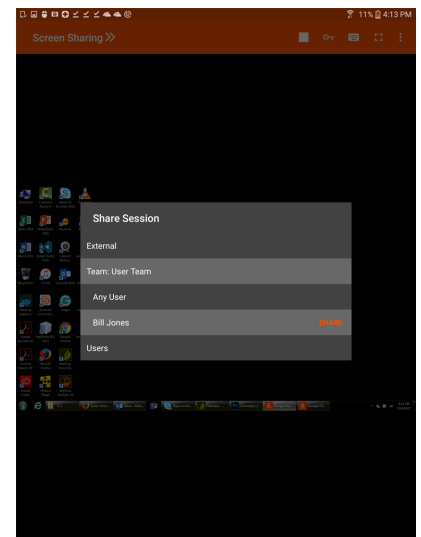


Sie können aus den angezeigten Teams einen Benutzer auswählen, um ihn oder sie zur Teilnahme an der Sitzung einzuladen. Sie können mehrere Einladungen versenden, wenn mehr Mitglieder aus dem Team Ihrer Sitzung beitreten sollen. Benutzer werden nur dann hier aufgelistet, wenn sie in der access console 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 access console angemeldetes Mitglied enthalten oder wenn sie die erweiterte Verfügbarkeit aktiviert haben.

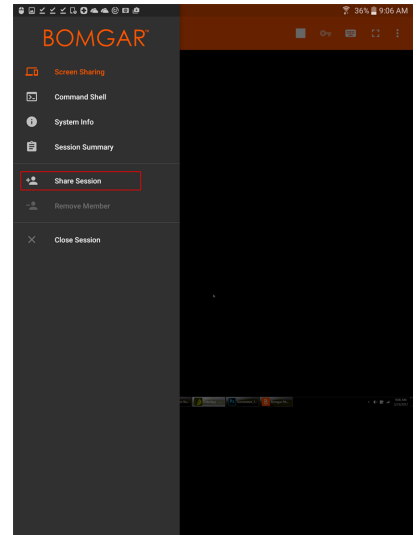
Einladungen können nur vom Sitzungseigentümer verschickt werden. Solange Sie Sitzungseigentümer bleiben, laufen Einladungen nicht ab. Für ein und denselben Benutzer können nicht mehrere aktive Einladungen für dieselbe Sitzung bestehen. Die Einladung verschwindet, falls:

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

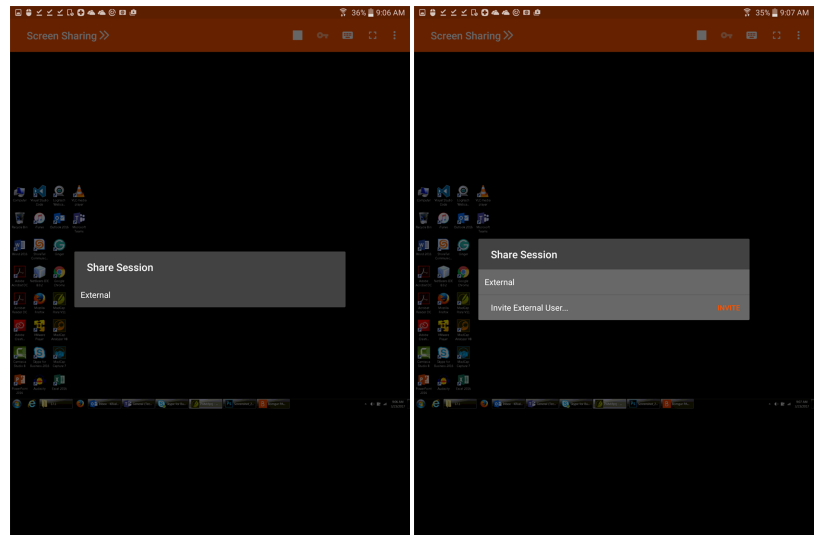


Einladen externer Support-Techniker zur Teilnahme an einer Sitzung über die Android-Konsole des Support-Technikers

In einer Support-Sitzung Tech. kann ein Support-Techniker einen externen Support-Techniker auffordern, einmalig an einer Sitzung teilzunehmen. Der einladende Benutzer sollte auf das Flyout-Menü tippen und das Menü **Sitzung freigeben** wählen.

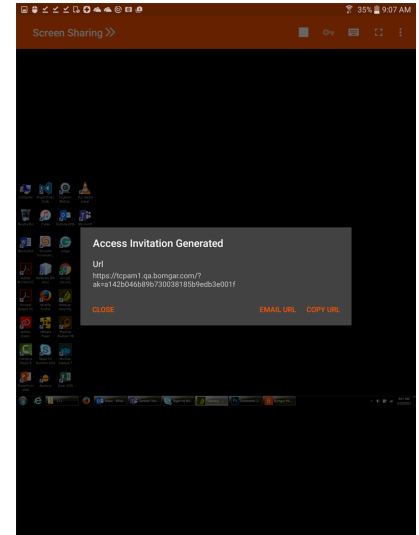


Wählen Sie als nächstes **Extern** und dann **Externen Benutzer einladen**. Tippen Sie zum Fortfahren auf die Schaltfläche **Einladen**.



Wählen Sie als nächstes eine Sicherheitsrichtlinie. Diese Richtlinien werden in der Verwaltungsschnittstelle erstellt und bestimmen, welche Berechtigungen der externe Benutzer hat. Wenn Sie ein Profil auswählen, wird die vollständige Beschreibung darunter angezeigt.

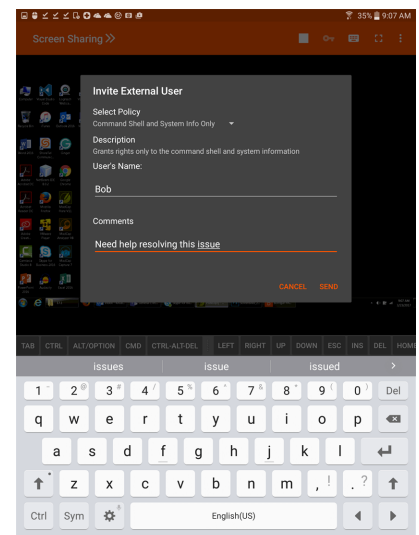
Geben Sie den Namen des externen Benutzers ein. Dieser Name wird im Chatfenster und in Berichten angezeigt. Geben Sie dann Kommentare dazu ein, warum dieser Benutzer eingeladen wurde. Klicken Sie auf **Senden**. Es wird ein neues Dialogfeld mit der Einladungs-URL angezeigt.



Abhängig von den von Ihrem Administrator gewählten Optionen sind Sie möglicherweise in der Lage, die Einladung über Ihren lokalen E-Mail-Client oder serverseitig zu versenden. Sie können auch die direkte URL kopieren und einfügen und diese so dem externen Benutzer zukommen lassen. Der externe Benutzer muss das Installationsprogramm für die access console herunterladen und ausführen. Dabei handelt es sich um einen abgekürzten Vorgang, im Gegensatz zur vollständigen Installation der access console.

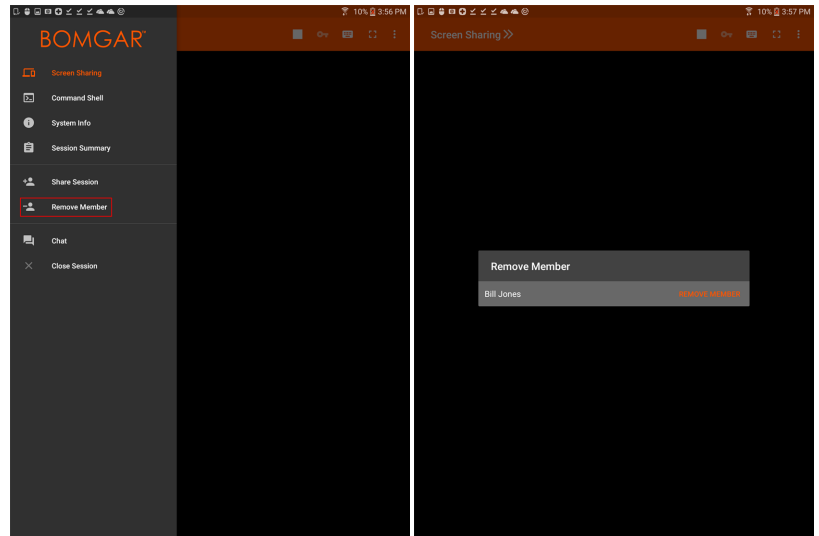
Ein Benutzer hat nur Zugriff auf die **Sitzungsregisterkarte** und verfügt über eingeschränkte Berechtigungen. Der externe Benutzer kann nie der Eigentümer der Sitzung sein. Wenn der einladende Benutzer die Sitzung verlässt, wird der externe Benutzer abgemeldet.

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

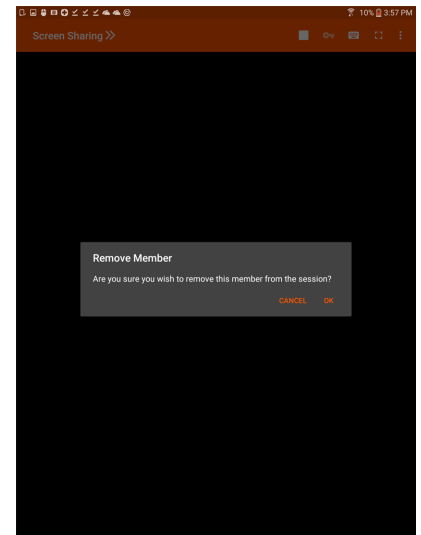


Über die Android-Zugriffskonsole ein Mitglied aus der Sitzung entfernen

Sie können einen anderen Benutzer aus einer freigegebenen Sitzung entfernen. Tippen Sie im Menü auf die Option **Mitglied entfernen**.



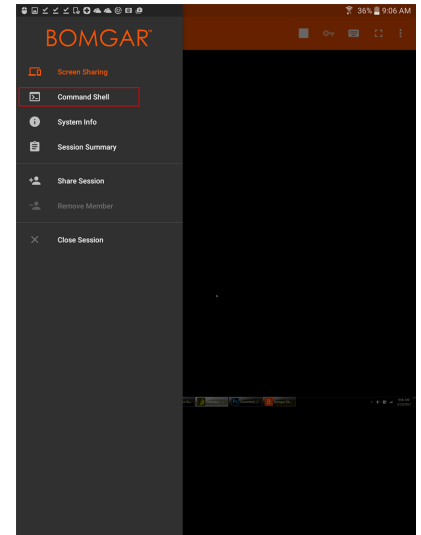
Wählen Sie den Teilnehmer, den Sie entfernen möchten. Tippen Sie dann auf **Entfernen**. Tippen Sie in der folgenden Aufforderung auf **OK**. Sie müssen Eigentümer der Sitzung sein, um ein anderes Mitglied entfernen zu können.



Öffnet die Befehlshell an einem Remote-Endpunkt mithilfe der Android-Zugriffskonsole

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

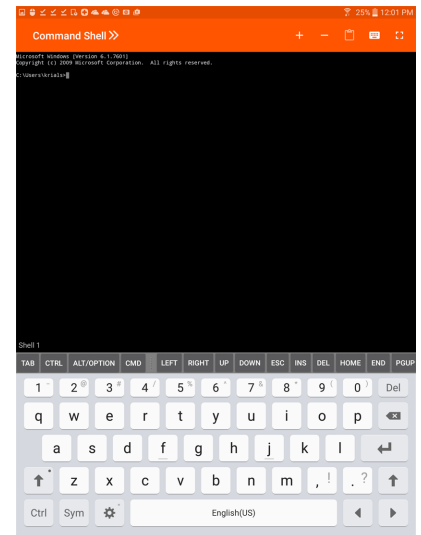
Um auf die Befehlshell zuzugreifen, wählen Sie **Befehlshell** im Menü. Tippen Sie auf das Symbol **+**, um eine neue Shell zu öffnen.



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

Zusätzliche Tastaturbefehle und Zeichen sind über der Standardtastatur verfügbar. Die zusätzlichen Tasten können nach links und rechts gewischt werden und geben dann mehr Optionen frei.

Wenn mehrere Befehlshells geöffnet sind, können Sie den Shell-Bildschirm nach links und rechts wischen, um zwischen den offenen Shells zu wechseln. Der Name der aktuellen Shell wird in der unteren linken Ecke des Shell-Bildschirms angezeigt.



Befehlshell-Tools



Öffnen Sie eine neue Shell, um mehrere Instanzen der Eingabeaufforderung auszuführen.



Schließen Sie die aktuelle Befehlshell. Andere offene Befehlshells werden weiterhin ausgeführt.



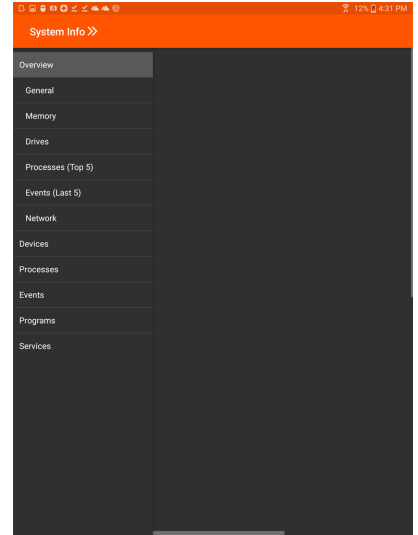
Greifen Sie auf die Tastatur zu, um Befehle in der Befehlshell zu tippen.



Greifen Sie auf das Befehlshell-Menü zu, um zusätzliche Aktionen durchzuführen, wie die Anzeige anderer Shell-Sitzungen und Wechsel in den Vollbildmodus.

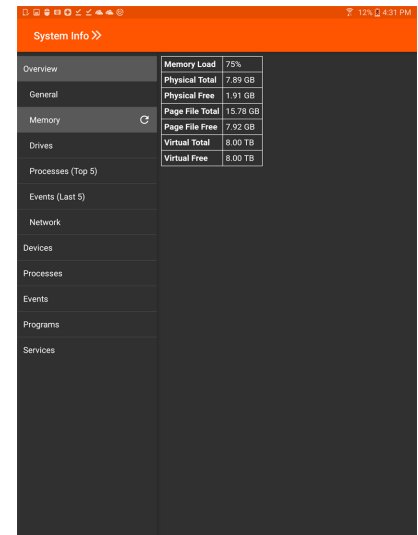
Endpunkt-Systeminformationen über die Android-Zugriffskonsole anzeigen

Benutzer können eine komplette Momentaufnahme der Systeminformationen des Endpunkts anzeigen, um die für Diagnose und Problemlösung benötigte Zeit zu verkürzen. Die verfügbaren Systeminformationen hängen vom Remote-Betriebssystem und der Konfiguration ab.



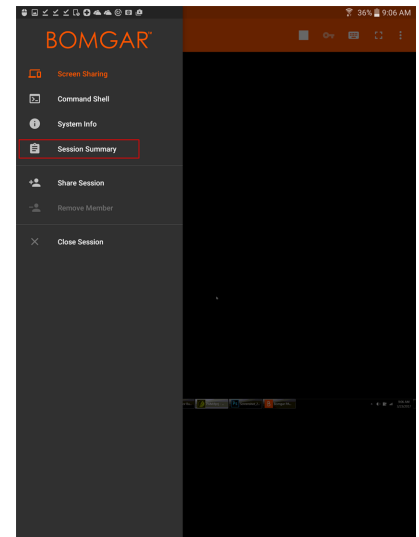
Wählen Sie aufeinanderfolgende Kategorienamen, um auf die gewünschten Daten zuzugreifen.

Sobald die Daten geladen wurden, können Sie auf die Schaltfläche **Aktualisieren** tippen, um die aktuellsten Daten abzurufen.

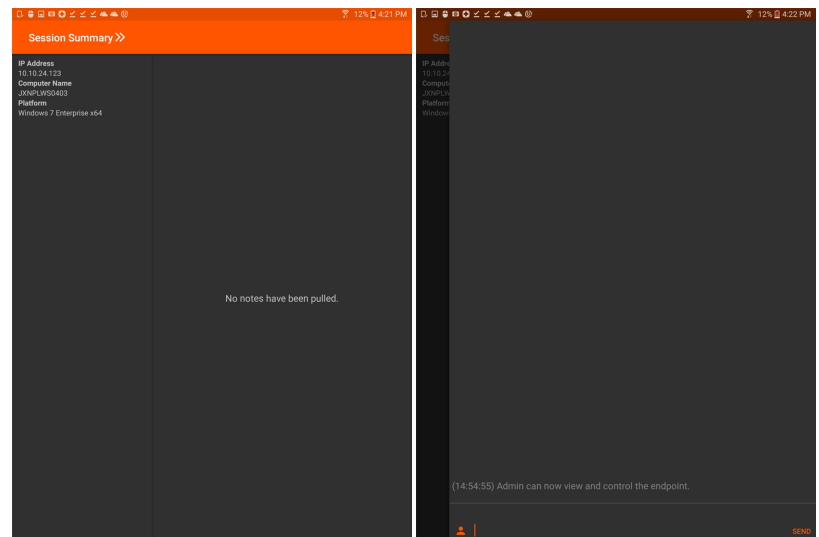


Über die Android-Zugriffskonsole eine Zusammenfassung der Zugriffssitzung anzeigen und Notizen hinzufügen

Die Seite **Zusammenfassung** bietet einen Überblick zum Remote-System, auf das zugegriffen wird.

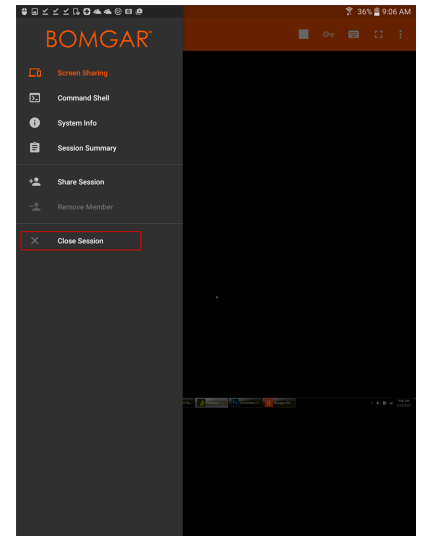


Sie können Notizen zur Sitzung hinzufügen, indem Sie nach links über den Bildschirm wischen. Notizen können von einem Benutzer hinzugefügt und von einem anderen Benutzer zur Einsicht abgerufen werden. Diese Notizen stehen auch im Sitzungsbericht zur Verfügung.



Über die Android-Zugriffskonsole eine Sitzung schließen

Tippen Sie zum Verlassen einer Sitzung auf **Sitzung schließen** über das Menü..



Wenn Sie der Sitzungseigentümer sind, schließt **Sitzung beenden** die Sitzungsseite in der access console und entfernt jegliche zusätzliche Mitglieder, für welche die Sitzung möglicherweise freigegeben wird.

Wenn Sie nicht der Sitzungseigentümer sind, werden Sie mit **Sitzung verlassen** einfach aus der Sitzung entfernt. Die Sitzung wird weiterhin durch den Sitzungseigentümer fortgesetzt. Wenn die Sitzung für zusätzliche Mitglieder freigegeben wurde, verbleiben diese in der Sitzung.

