BeyondTrust

Privilegierter Remote-Zugriff
iOS Zugriffskonsole 2.2.4

TC:7/22/2021

Inhaltsverzeichnis

Handbuch für die iOS-Zugriffskonsole

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

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

Installation der Zugriffskonsole auf iOS

Die BeyondTrust access console für iOS steht kostenlos im Apple App Store zum Download zur Verfügung. Suchen Sie über Ihr iOS-Gerät im App Store nach „BeyondTrust Access Console“ und installieren Sie dann die App.

Wenn Ihr Unternehmen einen Unternehmens-App-Store zum Verteilen von Apps verwendet, kontaktieren Sie den technischen Support von BeyondTrust, um die App für die BeyondTrust access console über Ihren Unternehmens-App-Store verfügbar zu machen.

Um die BeyondTrust access console auf Ihrem Gerät auszuführen, benötigen Sie BeyondTrust in der Software-Version 15.2 oder höher, während auf dem iOS-Gerät iOS 7 oder neuer ausgeführt werden muss.

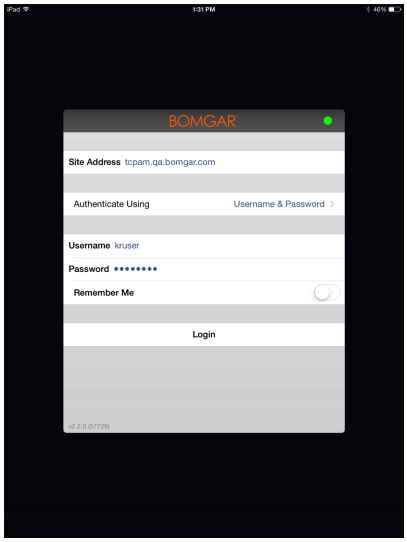
Hinweis: *Nur die BeyondTrust access console kann mit einer Privilegierter Remote-Zugriff (PRA) verwendet werden. Die BeyondTrust-Konsole des Support-Technikers kann nicht für die Verbindung mit einer PRA-Website verwendet werden. Ferner kann die BeyondTrust access console nicht für die Verbindung mit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

WICHTIG!

Ihr B Series Appliance muss mit einem von einer Zertifizierungsstelle signierten SSL-Zertifikat ausgestattet sein. BeyondTrust unterstützt keine selbstsignierten Zertifikate für die iOS-access console. Sobald Sie ein von einer Zertifizierungsstelle signiertes SSL-Zertifikat auf Ihrem B Series Appliance übernommen haben, wenden Sie sich an den technischen BeyondTrust-Support. Ihr Support-Techniker wird einen neuen Software-Build erstellen, der Ihr SSL-Zertifikat integriert. Mit dieser aktualisierten, auf Ihrem B Series Appliance installierten Build können Sie die BeyondTrust access console auf Ihrem Gerät ausführen, um von fast überall auf Endpunkte zuzugreifen.

Anmelden an der iOS-Zugriffskonsole

Geben Sie auf dem Anmeldungsbildschirm 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 die Schaltfläche **Anmelden**.



> ***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.*

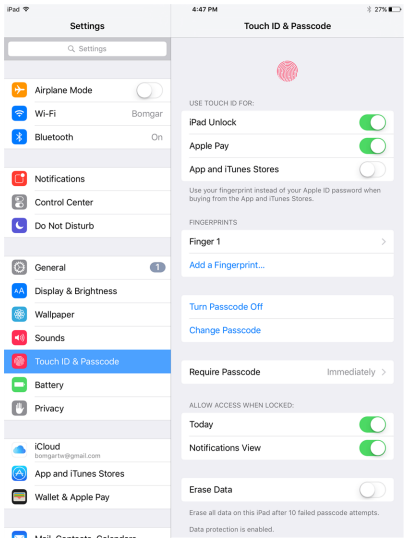
Alternativ, falls Sie von einem anderen Benutzer einmalig zur Teilnahme an einer Sitzung eingeladen wurden, tippen Sie auf **Authentifizierung über** und wählen Sie **Zugriffseinladungs-Schlüssel**.

Geben Sie den in Ihrer Einladung aufgeführten Schlüssel für die Einladung ein und tippen Sie auf **Anmelden**.

Melden Sie sich mit Touch ID bei der BeyondTrust Privilegierter Remote-Zugriff Konsole für iOS an

Touch ID ist der Fingerabdruck-Identifizierungssensor in folgenden iOS-Geräten:

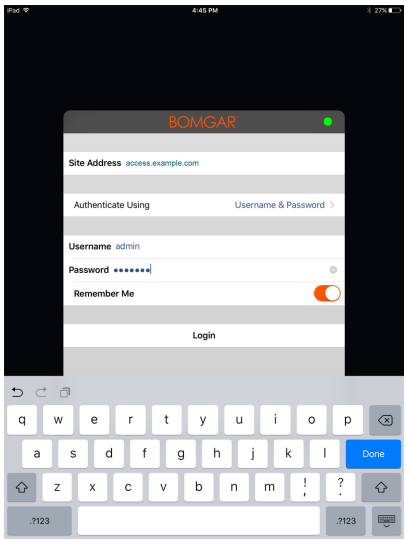
- **iPhone 5s und neuer**
- **iPad Pro**
- **iPad Air 2**
- **iPad Mini 3 und neuer**



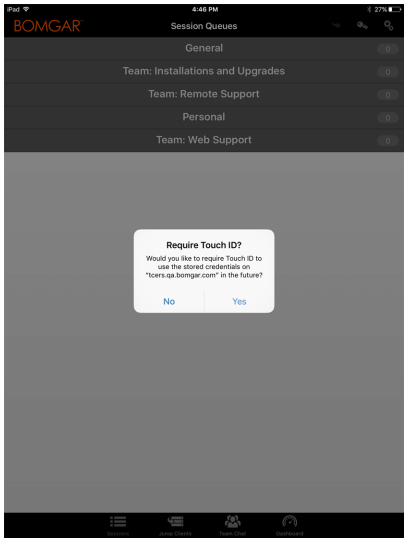
Mit diesem Feature können Sie Ihr Gerät entsperren oder andere Aktionen über Ihr iPhone und iPad autorisieren und dabei Ihren Fingerabdruck als Passcode verwenden. Mehr über Touch ID und darüber, wie Sie es auf Ihrem Gerät aktivieren, erfahren Sie unter Über Touch ID-Sicherheit auf iPhone und iPad unter https://support.apple.com/en-us/HT204587 und Verwenden von Touch ID auf iPhone und iPad unter https://support.apple.com/en-us/HT201371.

Ab BeyondTrust Privilegierter Remote-Zugriff 16.1 können Sie Touch ID zur Anmeldung in der mobilen access console für iOS verwenden. Die gleiche Fingerabdruckauthentifizierung, die Sie zur Entsperrung Ihres Gerätes verwenden, kann auch verwendet werden, um Zugriff auf Ihre access console zu erhalten. Folgen Sie den unten beschriebenen Schritten, um die ID-Authentifizierung für Ihre mobile access console zu aktivieren.

1. Öffnen Sie die BeyondTrust mobile access console Anwendung.
2. Geben Sie den Hostnamen Ihrer BeyondTrust-Website ein, wie etwa access.example.com, sowie Ihre Anmeldedaten.
3. Überprüfen Sie, ob die Option **Anmeldedaten speichern** aktiviert ist. Klicken Sie auf **Anmelden**.



4. Tippen Sie in der Touch ID-Eingabeaufforderung, die nach der Anmeldung erscheint, auf **Ja**.
5. Melden Sie sich von der access console ab.



6. Tippen Sie auf die Option **Anmelden mit Touch ID**, die auf dem Anmeldungsbildschirm erscheint.

7. Platzieren Sie Ihren Finger auf der **Home**-Taste ihres Geräts, um die Anmeldung in der Konsole des Support-Technikers abzuschließen.

> ***Hinweis:*** *Sie können sich jederzeit mit Ihrem Benutzernamen und Kennwort anmelden, indem Sie auf die Option* ***Zurück zur Anmeldung*** *tippen.*

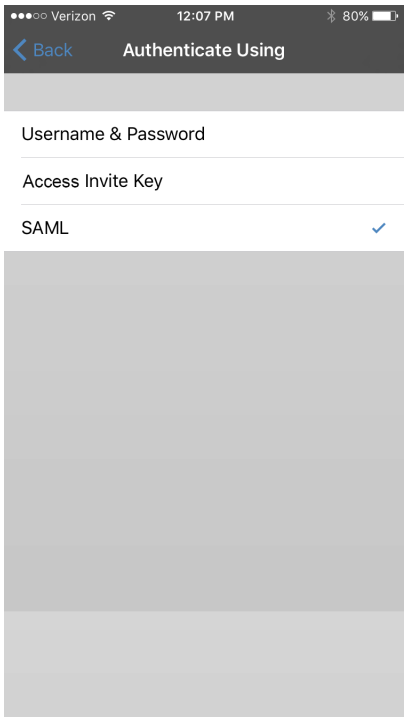
Anmeldung an der iOS-Zugriffskonsole mit SAML for Mobile

SAML for Mobile ist eine einfache und sichere Methode, um sich an der iOS-access console anzumelden. Um mehr über die SAML-Einzelanmeldung zu erfahren, lesen Sie weiter unter 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 mobile access console zuzugreifen.

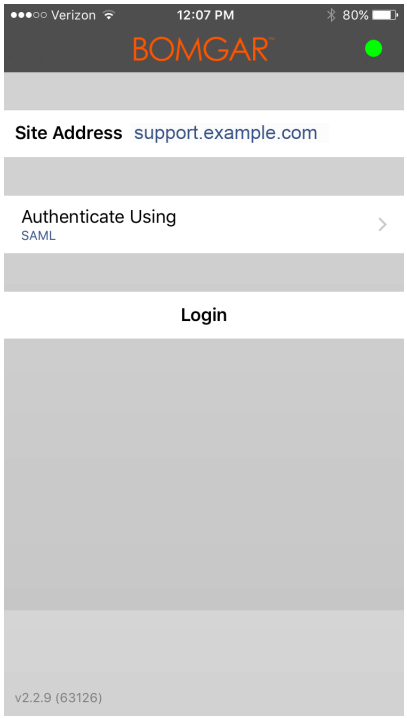
> ***Hinweis:*** *Bevor Sie versuchen, sich mit SAML an der iOS-access console anzumelden, stellen Sie sicher, dass für Ihre /login-Verwaltungsumgebung ein SAML-Anbieter konfiguriert wurde, indem Sie zu* ***Benutzer und Sicherheit > Sicherheitsanbieter*** *navigieren. Wenn SAML nicht in /login konfiguriert ist, steht SAML nicht als Authentifizierungsmethode für die iOS-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 unter www.beyondtrust.com/docs/privileged-remote-access/how-to/integrations/security-providers/saml/configure-settings.htm.*

1. Tippen Sie auf die access console App auf Ihrem iOS-Gerät.
2. Tippen Sie auf dem Anmeldungsbildschirm auf **Anmelden mit**.

3. Wählen Sie **SAML**.



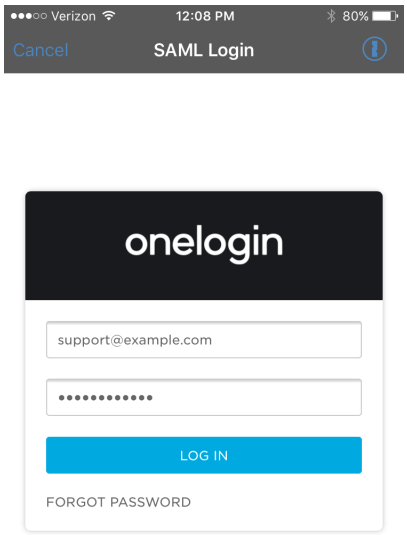
4. Tippen Sie auf **Anmelden**. Sie sehen dann die Seite Ihres SAML-Anbieters.



5. Geben Sie auf der Seite Ihres Anbieters Ihre Anmeldedaten ein.

> ***Hinweis:*** *Wenn für Ihr Gerät ein Kennwortspeicher konfiguriert wurde, können Sie auf das Schlosssymbol oben rechts tippen, um auf Ihren Kennwortspeicher und Ihre Anmeldedaten zuzugreifen.*

6. Tippen Sie auf **Anmelden**, um auf die Konsole zuzugreifen.

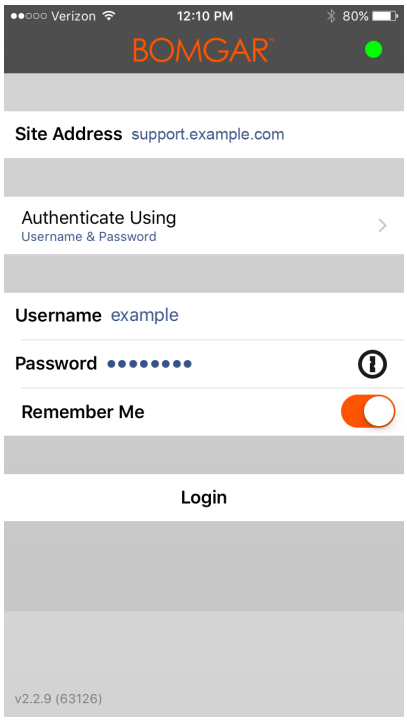


Anmeldung an der iOS-Zugriffskonsole mit einem Kennwortmanager

Kennwortmanager wie 1Password und LastPass sind ein einfacher Weg, um Ihre Kennwörter sicher und vertraulich zu halten. Um mehr über die proprietäre 1Password-Erweiterung zu erfahren, lesen Sie weiter unter Sicherheit ist nicht nur ein Feature. Sie ist unser Fundament. unter https://1password.com/security/. Folgen Sie den nachstehenden Schritten, um 1Password oder andere Kennwortmanager für den Zugriff auf die BeyondTrust iOS-Zugriffskonsole zu verwenden.

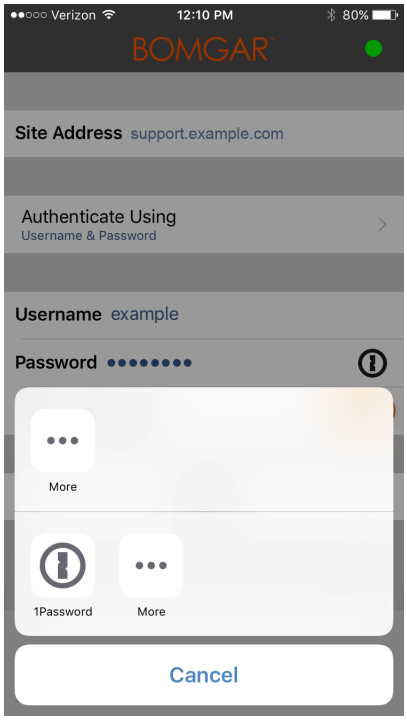
> ***Hinweis:*** *Bevor Sie einen Kennwortmanager mit der BeyondTrust iOS-Zugriffskonsole verwenden, stellen Sie sicher, dass Sie ein Konto im Kennwortmanager konfiguriert haben und dass die Anwendung mit Ihrem Gerät synchronisiert ist.*

1. Öffnen Sie die Zugriffskonsolen-App auf Ihrem iOS-Gerät.
2. Tippen Sie auf das Schlossssymbol im Feld **Kennwort**.

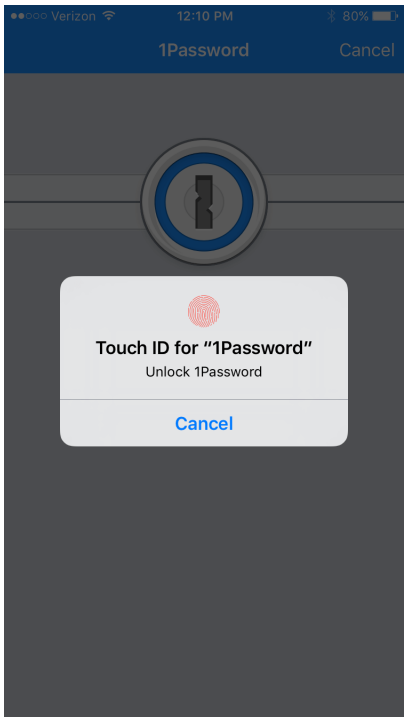


3. Wählen Sie an der Eingabeaufforderung auf den Kennwortmanager, den Sie nutzen möchten, und Sie sollten dann zur Anmeldungsseite des Kennwortmanagers geleitet werden.

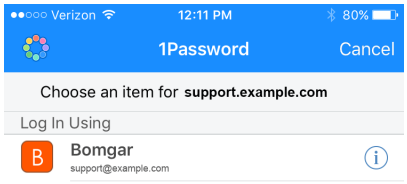
> ***Hinweis:*** *Wenn der Kennwortmanager nicht für das Gerät konfiguriert ist, ist das Schlosssymbol nicht sichtbar.*



4. Wenn Touch ID aktiviert ist, ermöglicht Ihnen Ihr Gerät die Nutzung Ihres Fingerabdrucks als Authentifizierung zum Öffnen der App. Wenn Touch ID nicht auf Ihrem Gerät aktiviert ist, müssen Sie Ihr Kennwort zur Authentifizierung eingeben.



5. Nach der Anmeldung führt der Kennwortmanager die Konten auf, die auf die Konsole zugreifen können. Tippen Sie auf das Konto, das Sie zum Zugriff auf die Konsole verwenden möchten.

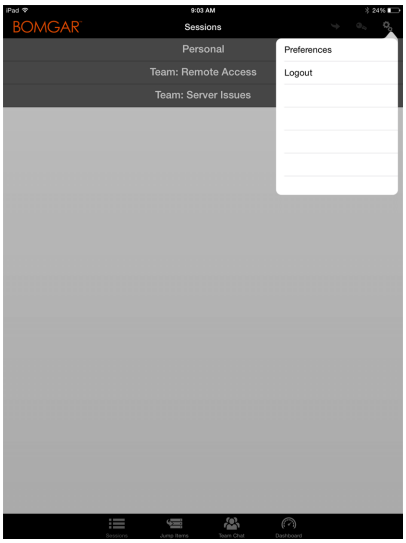


Einstellungen in der iOS-Zugriffskonsole ändern

Um Ihre Einstellungen auf einem iPad zu ändern, tippen Sie auf das **Zahnradsymbol** in der oberen rechten Ecke des Bildschirms.

Um Ihre Einstellungen auf einem iPhone zu ändern, tippen Sie auf das **Menüsymbol** in der oberen rechten Ecke des Bildschirms.

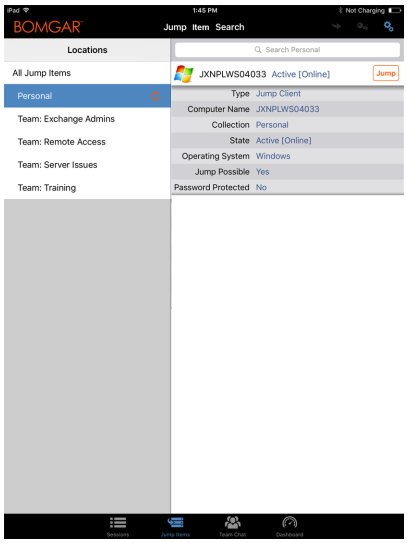
Tippen Sie auf **Einstellungen**.



Hörbare Alarme	iPad und iPhone	Falls aktiviert, spielt Ihr Gerät Audioalarme für bestimmte Ereignisse ab, die in der access console stattfinden.
Absoluter Mauszeiger	iPad und iPhone	Falls deaktiviert, müssen Sie Ihren Finger auf dem Mauszeiger platzieren und ihn ziehen, um die Maus zu bewegen. Tippen und halten Sie, um den Mauszeiger ausfindig zu machen, wenn die absolute Positionierung deaktiviert ist. Falls aktiviert, können Sie den Mauszeiger dort platzieren, wo Ihr Finger den Bildschirm berührt. Ist die Einstellung „Absolute Position“ aktiviert, tippen und halten Sie, um ein ausklappbares Menü zu öffnen, in dem Sie unterschiedliche Klickmethoden wählen können.
Gerät schütteln, um in der Sitzungsansicht die Hilfe aufzurufen	Nur iPad	Falls aktiviert, können Sie das Gerät schütteln, um in einer Zugriffssitzung die Hilfe für Bildschirmfreigabe-Gesten zu aktivieren.

Verwenden von Jump-Elementen zum Zugriff auf Endpunkte über die iOS-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. Die folgenden Jump-Elementtypen werden von der mobilen access console unterstützt:



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

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.

Um ein Jump-Element zu lokalisieren, tippen Sie auf die Registerkarte **Jump-Elemente** oben auf dem Bildschirm.

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.

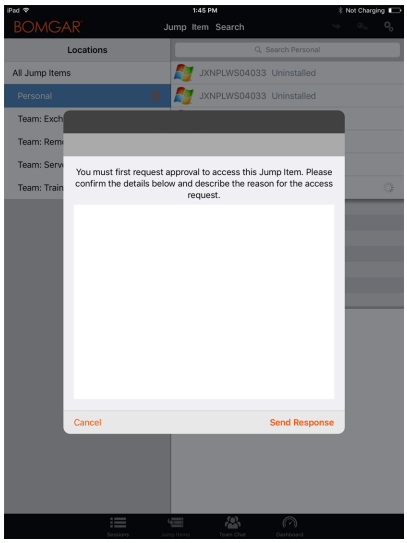
Abhängig von Ihren Konto-Berechtigungen, die Ihr Administrator für Ihr Konto festgelegt hat, kann ein Endbenutzer oder eine Drittpartei aufgefordert werden, die Sitzung zu akzeptieren oder abzulehnen. Trifft innerhalb eines definierten Zeitraums keine Antwort ein, wird die Sitzung entweder gestartet oder abgebrochen, je nachdem, wie Ihre Kontoberechtigungen lauten.

Autorisierung durch Endbenutzer oder Drittpartei

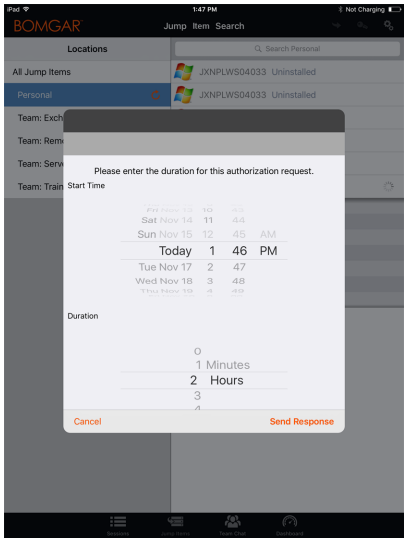
Abhängig von der Konfiguration von Jump-Elementen innerhalb der /login-Verwaltungsschnittstelle kann ein Jump-Element über eine zugeordnete Jump-Richtlinie verfügen. Die Richtlinie kann eine Autorisierungskomponente definieren, die Sie zwingt, eine Berechtigung von Dritten oder einem Administrator anzufordern,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

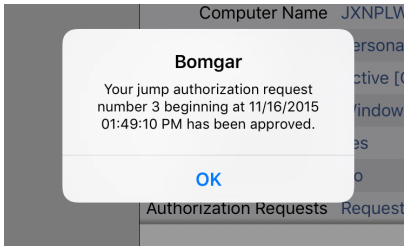
Nachdem Sie auf die Jump-Schaltfläche getippt und den Zugriff angefordert haben, erscheint eine Aufforderung und Sie müssen die Begründung für den Zugriff auf das System eingeben.



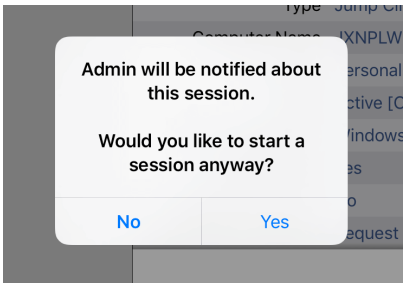
Als nächstes müssen Sie angeben, wann und für wie lange Sie auf das System zugreifen wollen.



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.



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.



Anmeldedaten zur automatischen Anmeldung für die mobile Zugriffskonsole

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.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/security.htm.*

Anmelden an Endpunkten mithilfe der Anmeldedaten-Einfügung über die iOS-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

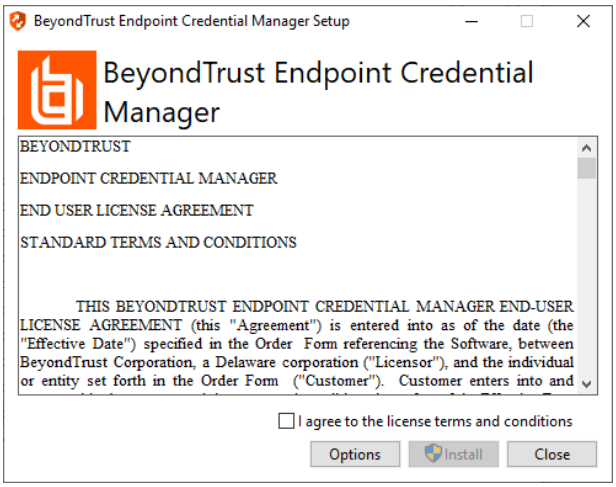
Bevor Sie damit beginnen können, mithilfe der Anmeldedaten-Einfügung auf Jump-Elemente zuzugreifen, müssen Sie den BeyondTrust Endpunkt-Anmeldedaten-Manager (ECM) herunterladen, installieren und konfigurieren.

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

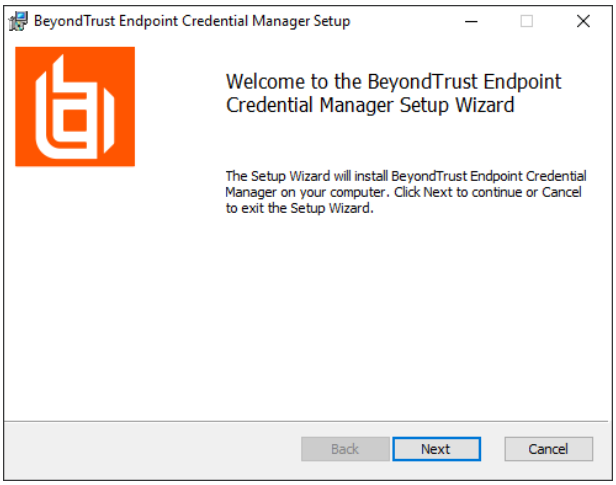
1. Laden Sie zunächst den BeyondTrust Endpunkt-Anmeldedaten-Manager (ECM) von BeyondTrust Support unter beyondtrustcorp.service-now.com/csm herunter.
2. Starten Sie den Installationsassistenten für den BeyondTrustEndpunkt-Anmeldedaten-Manager.
3. Stimmen Sie den Bedingungen der Endbenutzer-Lizenzvereinbarung 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**.

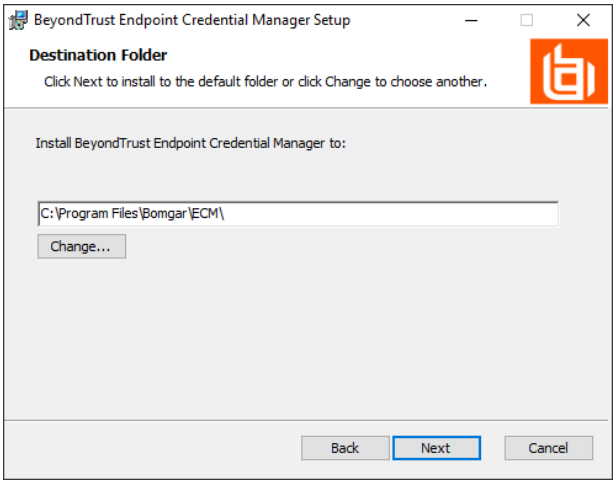
> ***Hinweis:*** *Sie können mit der Installation erst fortfahren, wenn Sie der Endbenutzer-Lizenzvereinbarung zustimmen.*



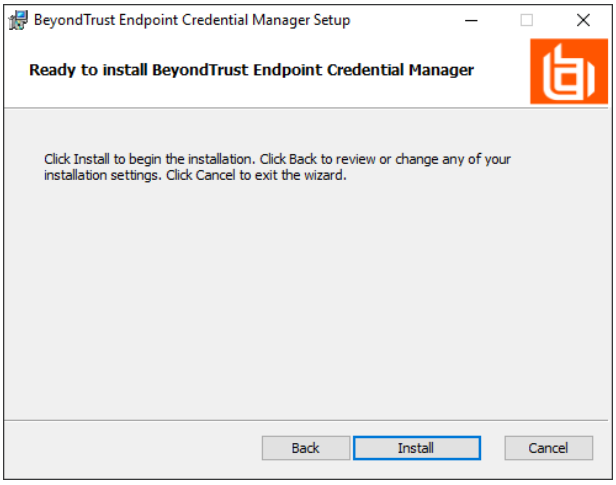
4. Klicken Sie auf dem Begrüßungsbildschirm auf **Weiter**.



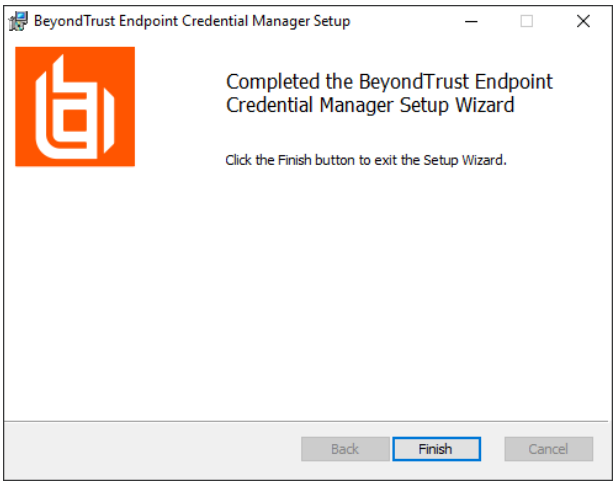
5. Wählen Sie den Installationsort für den Anmeldedaten-Manager und klicken Sie dann auf **Weiter**.



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 auf **Fertigstellen**.

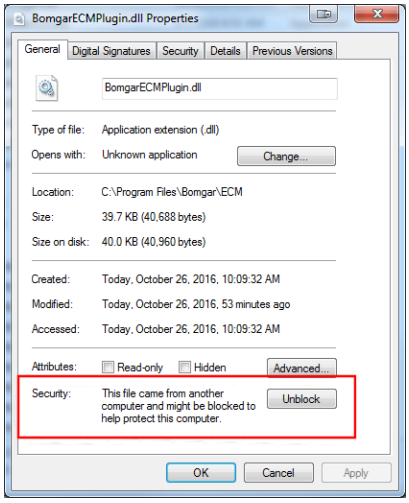


> ***Hinweis:*** *Um einen ausfallfreien Betrieb zu gewährleisten, können Administratoren bis zu drei ECMs auf unterschiedlichen Windows-Systemen installieren, um mit dem gleichen Anmeldedatenspeicher zu kommunizieren. Eine Liste der mit der Geräte-Site verbundenen ECMs finden Sie in* ***/login > Status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

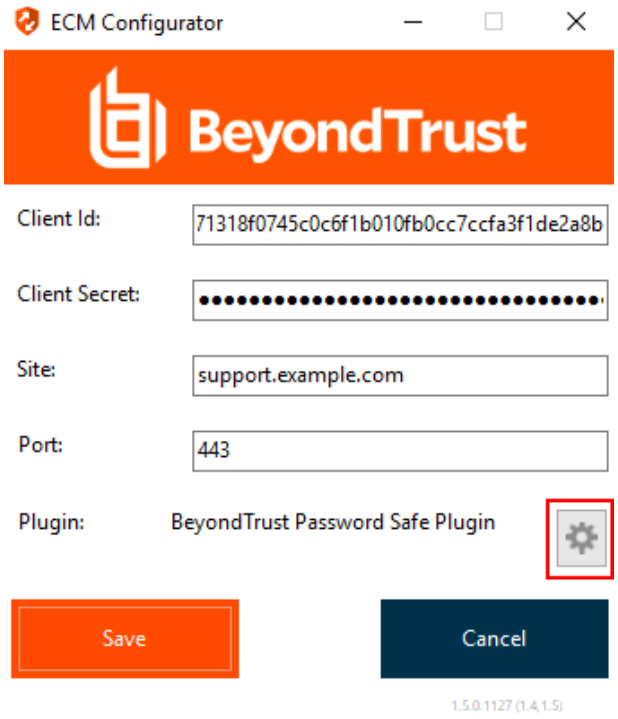
> ***Hinweis:*** *Wenn ECMs in einer Konfiguration mit hoher Verfügbarkeit verbunden sind, leitet das BeyondTrust Appliance B Series Anfragen an den ECM in die ECM-Gruppe, die am längsten mit dem Gerät verbunden ist.*

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.



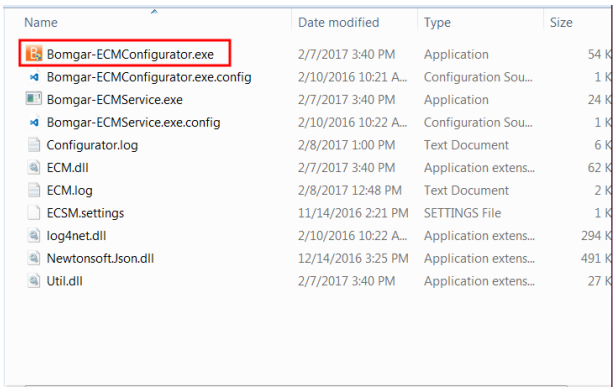
4. Klicken Sie auf das Zahnrad-Symbol im Fenster **Konfigurator**, um die Plugin-Einstellungen zu konfigurieren.



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.



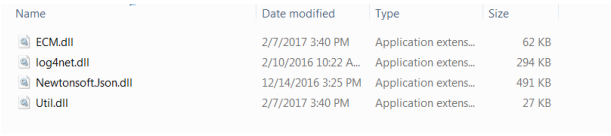
3. Wenn der Konfigurator geöffnet wird, vervollständigen Sie die Felder. Alle Felder müssen ausgefüllt werden.

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.

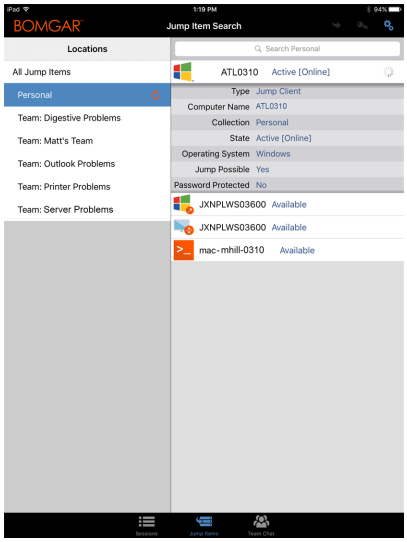


Hinweis: *Wenn Sie sich mit einem Kennwort-Speicher verbinden, sind möglicherweise weitere Konfigurationsschritte auf Plugin-Ebene notwendig. Die Plugin-Anforderungen variieren basierend auf dem Anmeldedaten-Speicher, mit dem Sie eine Verbindung aufbauen.*

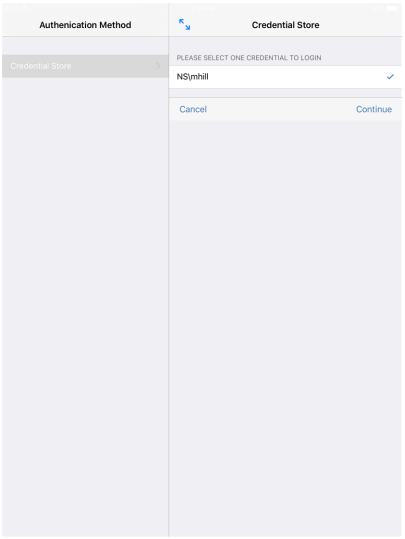
Verwendung der Anmeldedaten-Einfügung zum Zugriff auf Endpunkte

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.

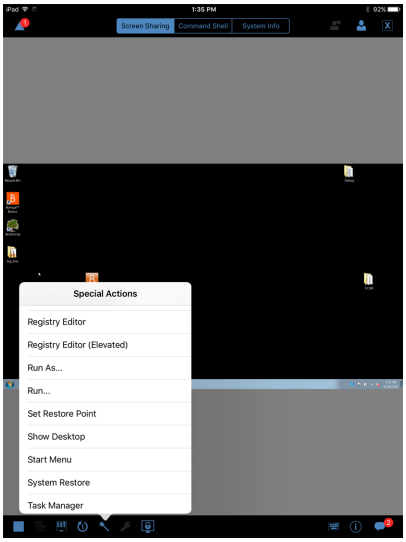
1. Navigieren Sie zu Ihrer **Jump-Element-Liste**.
2. Tippen Sie auf das Jump-Element, auf das Sie zugreifen möchten.
3. Tippen Sie auf **Jump**.



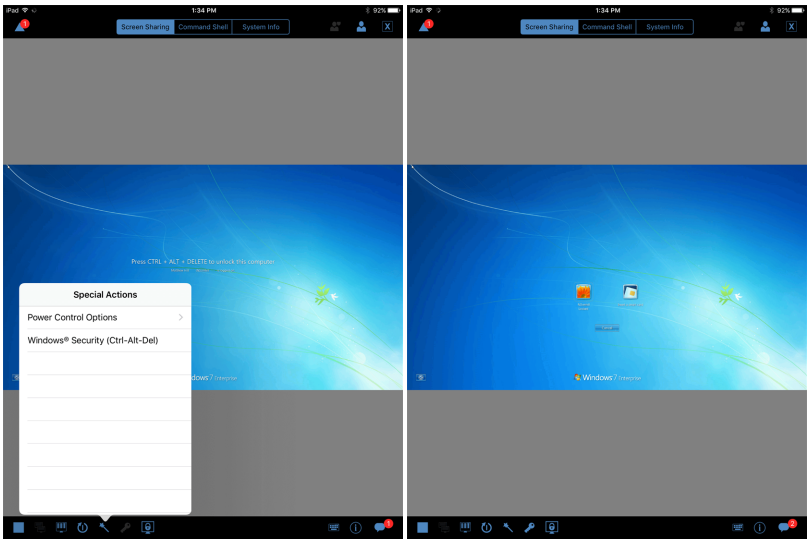
4. Tippen Sie auf **Anmeldedaten-Speicher**.
5. Tippen Sie auf die Anmeldedaten, die Sie zum Zugriff auf das System verwenden möchten.
6. Tippen Sie auf **Fortfahren**.



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...**.



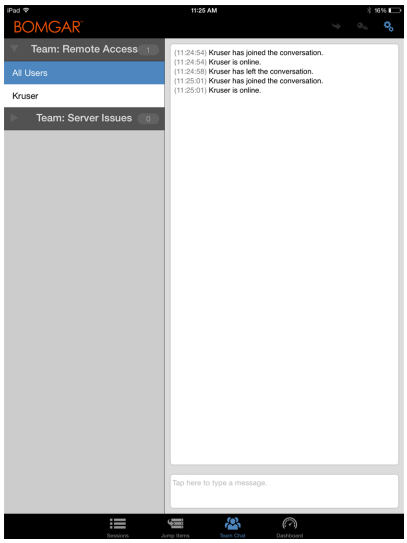
9. Tippen Sie auf **Windows Security (Strg-Alt-Entf)**.

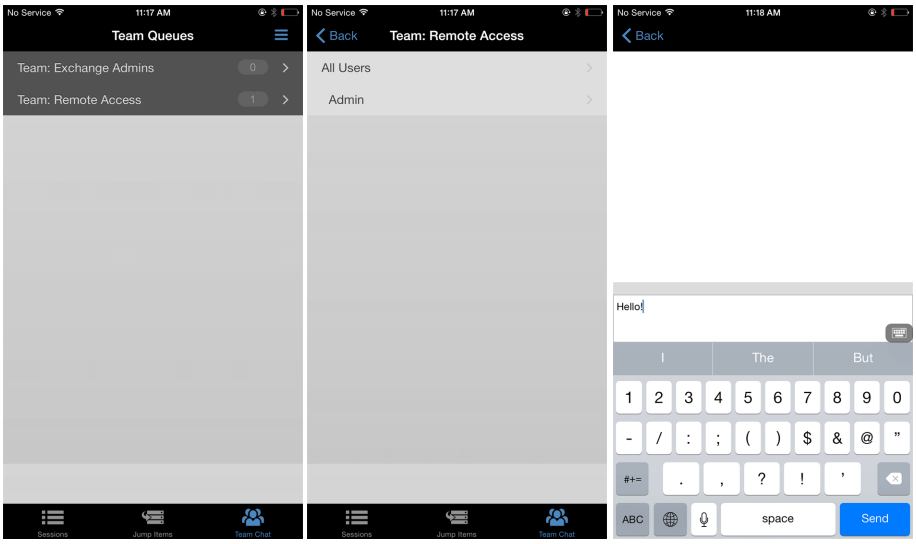


10. Tippen Sie auf das **Schlüssel**-Symbol. Mit dem Schlüsselsymbol kann das System Ihre gespeicherten Anmeldedaten anzeigen, um sich Zugang zum Endpunkt zu verschaffen.

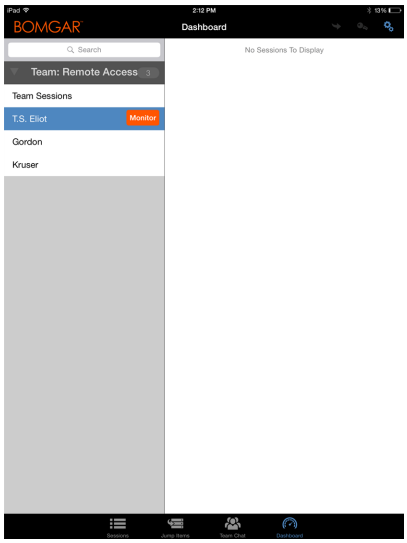
In der iOS-Zugriffskonsole mit anderen Benutzern chatten

Über das Symbol **Team-Chat** unten auf dem Bildschirm 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 wählen, um nur mit diesem Mitglied zu chatten.





Verwalten von Teammitgliedern über das Dashboard (nur iPad)



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

Ist ein Benutzer Team-Manager oder Teamführer eines oder mehrerer Teams, erscheint das Dashboard-Symbol unten auf dem Bildschirm. Auf dem Dashboard werden nur angemeldete Teammitglieder einer niedrigeren Rolle für das ausgewählte Team angezeigt.

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

Wählen Sie den Benutzer, dessen Bildschirm Sie anzeigen möchten, und tippen Sie dann auf die Schaltfläche **Überwachen**. Dadurch wird in Ihrer access console eine neue Seite geöffnet, auf der, abhängig von den Einstellungen des Administrators, entweder der gesamte Computerbildschirm des Benutzers oder nur die access console angezeigt wird.

Innerhalb eines Teams kann ein Benutzer nur Benutzer mit einer niedrigeren Rolle verwalten. Beachten Sie jedoch, dass die Rollen strikt auf Teambasis gelten. So kann ein Benutzer einen anderen Benutzer in einem Team überwachen, dies aber möglicherweise nicht in einem anderen Team tun.

3D Touch für mobilen Zugriff verwenden

3D Touch ist eine druckempfindliche Funktion, die beim iPhone 6s und neuer verfügbar ist.

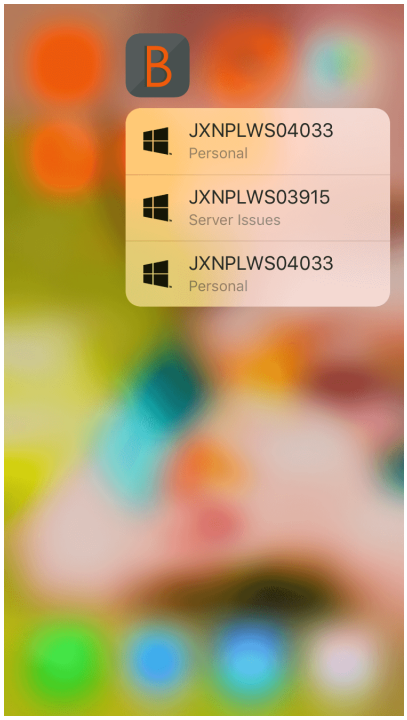
Mit dieser Funktion können Sie Druck in unterschiedlicher Stärke auf den Bildschirm ausüben, um die Funktionen „Peek“ und „Pop“ zu verwenden. Mit diesen Aktionen können Sie über Ihr iPhone 6s/6s Plus-Gerät Inhaltsvorschauen anzeigen und Befehle ausführen, ohne eine Anwendung ganz öffnen zu müssen. Mehr Informationen yu 3D Touch, Peek und Pop finden Sie unter Nutzen Sie 3D Touch unter https://developer.apple.com/ios/3d-touch/.

Ab BeyondTrust Privilegierter Remote-Zugriff 16.1 können Sie 3D Touch verwenden, um einfach auf Jump-Elemente zuzugreifen. Lesen Sie die folgenden Abschnitte, um mehr darüber zu erfahren, wie 3D Touch Ihnen beim schnellen Zugriff auf Ihre kritischen Systeme helfen kann.

Zugriff auf häufig genutzte Jump-Elemente mithilfe von 3D Touch

Mit 3D Touch können Sie leicht über den Startbildschirm Ihres iPhone auf bis zu drei Ihrer am häufigsten genutzten Jump-Elemente zugreifen. Folgen Sie den unten beschriebenen Schritten.

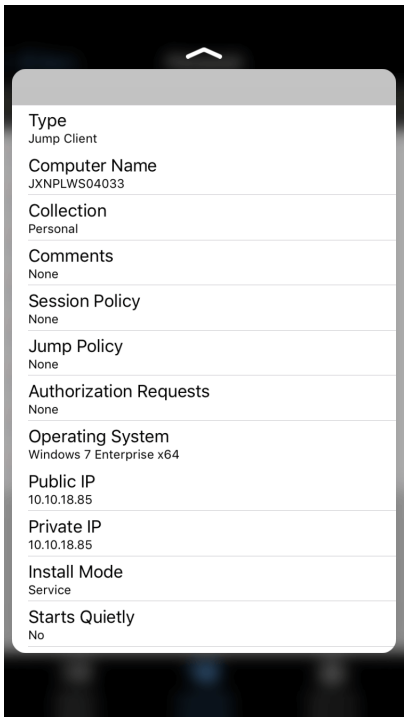
1. Tippen Sie auf das access console-App-Symbol im mobilen iOS und eine Liste Ihrer am häufigsten genutzten Jump-Elemente wird angezeigt. Beachten Sie, dass Sie zusätzlichen Druck auf den Bildschirm ausüben müssen, damit die Jump-Element-Optionen angezeigt werden.
2. Tippen Sie in der Liste auf das Jump-Element, auf das Sie zugreifen möchten.
3. Geben Sie Ihre Anmeldedaten ein.
4. Eine Sitzung mit diesem Jump-Element wird initiiert.



Vorschau von Informationen zu Jump-Elementen

Um Informationen zu Jump-Elementen anzuzeigen, bevor Sie eine Sitzung starten, können Sie die „Peek“- und „Pop“-Aktionen von 3D Touch verwenden. Folgen Sie den unten beschriebenen Schritten, um eine Vorschau für eine Sitzung anzuzeigen.

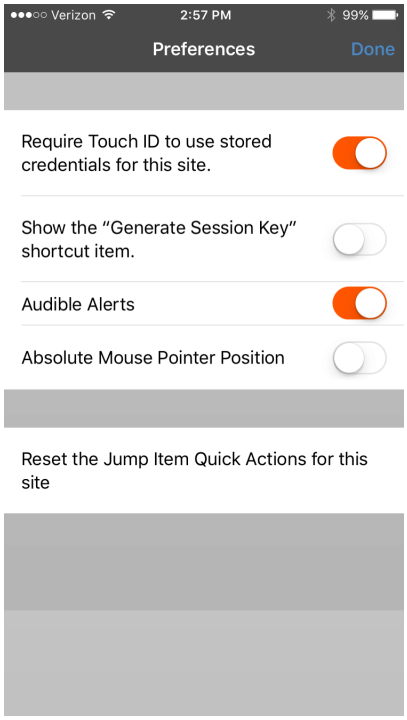
1. Wählen Sie auf der Seite **Jump-Elemente** die Warteschlange, in der sich das Jump-Element befindet.
2. Nachdem Sie auf die Warteschlange getippt haben, erscheint eine Liste der Jump-Elemente. Tippen Sie leicht auf Ihre Auswahl, bis die Informationen des Jump-Elements angezeigt werden.
3. Drücken Sie weiterhin auf den Bildschirm und wischen Sie nach oben, um die **Jump**-Aktion zu sehen. Klicken Sie auf „Jump“, um eine Sitzung zu initiieren.



> ***Hinweis:*** *Wenn Sie nicht stark oder lange genug drücken, wird die Vorschau nicht angezeigt. Stattdessen wird die Seite* ***Sitzungsinformationen*** *angezeigt.*

Festlegen der Einstellungen für 3D Touch

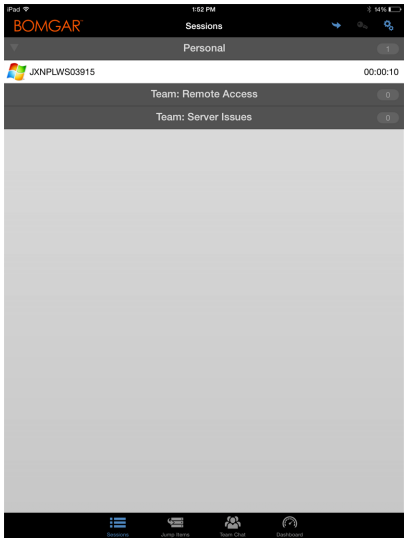
In der mobilen iOS-Zugriffskonsole können Sie auf das Menü Einstellungen zugreifen, indem Sie auf das Hamburgersymbol in der oberen rechten Ecke des Bildschirms tippen und die **Einstellungen** auswählen. In den Einstellungen ist **Zurücksetzen der Jump-Element-Schnellaktionen für diese Site** spezifisch für 3D Touch. Diese Einstellung ermöglicht es Ihnen, die Liste häufig genutzter Jump-Elemente zu löschen, die aufgerufen wird, wenn Sie auf das access console-App-Symbol im mobilen iOS tippen und es gedrückt halten.



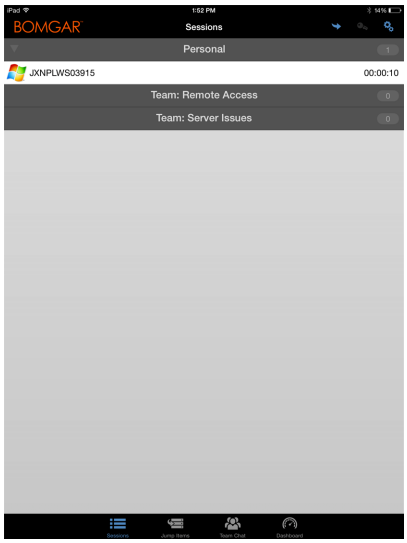
Über die iOS-Zugriffskonsole Zugriffssitzungen anzeigen

In der access console sind aktive Zugriffssitzungen in Team-Warteschlangen unterteilt. Wenn Sie auf das Symbol **Sitzungen** unten auf dem Bildschirm tippen, wird eine Liste aller konfigurierter Warteschlangen angezeigt. Diese Warteschlangen basieren auf den Teams, die Sie in der /login-Verwaltungsschnittstelle eingerichtet haben. Sobald ein Team definiert wurde, wird eine Warteschlange im Bereich **Sitzungen** der access console verfügbar. Diese Warteschlange wird immer angezeigt, solange mindestens ein Teammitglied in der access console angemeldet ist.

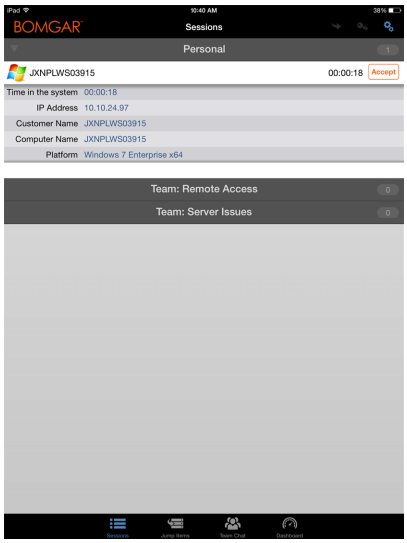
Die Warteschlange **Persönlich** enthält Sitzungen, die aktuell laufen, oder Sitzungen, die von einem anderen Mitglied für Sie freigegeben wurden. Die verbleibenden Warteschlangen sind für bestimmte Teams, denen Sie angehören.



Tippen Sie auf den Warteschlangennamen, um laufende Sitzungen anzuzeigen. Tippen Sie auf einen Sitzungseintrag, um Einzelheiten zum System oder zur Sitzung anzuzeigen. Um zu einer Sitzung zu navigieren, tippen Sie auf die Option **Zurückkehren**.



> ***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****. Durch das Akzeptieren einer Sitzung wird diese auf Ihrem Bildschirm angezeigt.*



Bildschirmfreigabe mit Endpunkt über die iOS-Zugriffskonsole

Tippen Sie auf der Seite **Bildschirmfreigabe** auf die Schaltfläche **Wiedergabe**, um die Anzeige und Steuerung des Endpunkts anzufordern, falls die Bildschirmfreigabe automatisch beginnt. Wenn Sie auf den Endpunkt zugegriffen haben, erscheint er auf Ihrem Display. Sie verfügen über die komplette Maus- und Tastatursteuerung des Endpunktes, 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, **ODER** - wenn die absolute Mauszeigerposition in den Einstellungen aktiviert ist - platzieren Sie den Mauszeiger dort, wo Ihr Finger den Bildschirm berührt.
- 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 Mausrad, 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, **ODER** - wenn die absolute Mauszeigerposition in den Einstellungen aktiviert ist - tippen und halten Sie, um ein ausklappbares Menü zu öffnen, in dem Sie Linksklick, Rechtsklick oder Doppelklick wählen können.

> ***Hinweis:*** *Auf dem iPad können Sie (sofern dies in den Einstellungen aktiviert wurde) Ihr Gerät schütteln, um eine Schnellreferenz zu Bildschirmfreigabe-Gesten anzuzeigen.*

Auf einem iPad stehen alle Bildschirmfreigabeaktionen unten auf dem Bildschirm zur Verfügung. Um auf einem iPhone auf mehr Bildschirmfreigabe-Tools zuzugreifen, tippen Sie auf die Schaltfläche **Menü** in der oberen rechten Bildschirmecke. Tippen Sie auf **Gestenhilfe anzeigen**, um eine Schnellreferenz zu Bildschirmfreigabegesten anzuzeigen.

Bildschirmfreigabeaktionen

	Beginnt die Bildschirmfreigabe.
	Bildschirmfreigabe beenden.
	Einen alternativen Remote-Bildschirm für die Anzeige auswählen. Der primäre Monitor wird mit einem **P** gekennzeichnet.
	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.
	Eine spezielle Aktion auf dem Remote-System durchführen. Je nach Betriebssystem und Konfiguration des Remote-Computers variieren die verfügbaren Aufgaben. Bei der Verwendung des heraufgesetzten Modus können einige Aktionen im Systemkontext ausgeführt werden. Alternativ können Sie die Anmeldedaten eines Administrators verwenden, um eine spezielle Aktion in diesem Benutzerkontext durchzuführen.

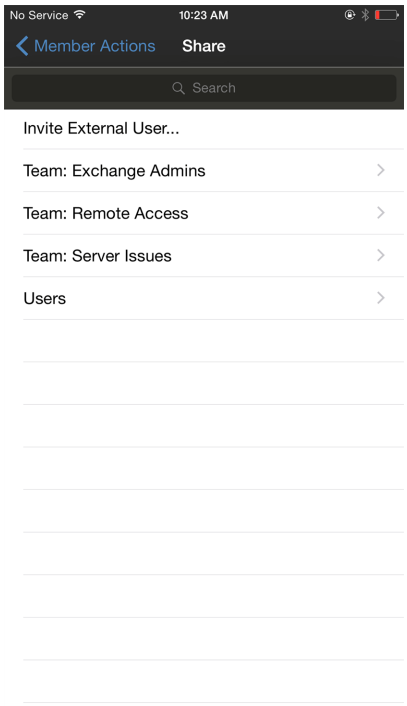
	Starten Sie das Remote-System neu, ohne Ihre Verbindung zur Zugriffssitzung zu verlieren.
	Unterbindet die Bildschirmanzeige und Maus- und Tastatureingabe für den Remote-Benutzer. Die eingeschränkte Endpunktinteraktion ist nur beim Zugriff auf macOS- oder Windows-Computer verfügbar. Die eingeschränkte 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.
	Greifen Sie auf die Tastatur zu, um auf dem Remote-Bildschirm zu tippen.

Freigabe einer Sitzung für andere Mitglieder über die iOS-Zugriffskonsole

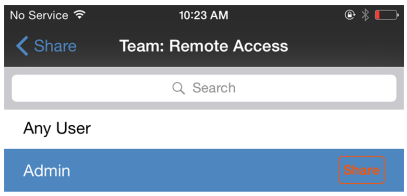
Um eine Sitzung für ein anderes Teammitglied über ein iPad freizugeben, tippen Sie auf das Personensymbol in der oberen rechten Ecke des Bildschirms. Tippen Sie bei der Verwendung eines iPhone auf das Symbol **Aktion** unten auf dem Bildschirm. Tippen Sie auf **Mitgliederaktionen**.

Wählen Sie im Menü **Sitzung freigeben**.

Lokalisieren Sie als nächstes den Benutzer, für den diese Sitzung freigegeben werden soll, indem Sie erst ein Team auswählen, dem der Benutzer angehört. Wählen Sie einen Teamnamen, um dessen Mitglieder anzuzeigen.



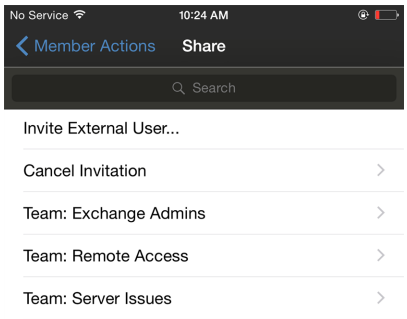
Sie können aus den angezeigten Teams einen Benutzer auswählen, um ihn oder sie zur Teilnahme an der Sitzung einzuladen. Sie können mehrere Einladungen versenden, wenn mehr Mitglieder aus dem Team Ihrer Sitzung beitreten sollen. Benutzer werden nur dann hier aufgelistet, wenn sie in der access console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

Wenn Sie eine Einladung verschickt haben und diese noch aktiv ist, können Sie die Einladung zurückziehen, indem Sie sie im Menü **Einladung zurückziehen** auswählen. Tippen Sie als nächstes auf die Schaltfläche **Absagen**. 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.



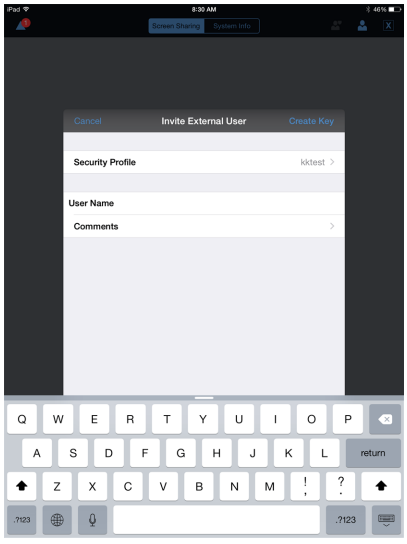
Einladen externer Benutzer zur Teilnahme an einer Sitzung über die iOS-Zugriffskonsole

Alternativ können Sie eine Sitzung für einen Benutzer freigeben, der nicht über ein Konto auf Ihrem B Series Appliance verfügt. Um einen externen Benutzer zum einmaligen Beitritt zu einer Sitzung einzuladen, tippen Sie auf die Schaltfläche **Mitgliederaktionen**. Um auf einem iPhone auf diese Schaltfläche zuzugreifen, tippen Sie zunächst auf die Schaltfläche **Aktionen**.

Wählen Sie im Menü **Sitzung freigeben**.

Tippen Sie auf **Externen Benutzer einladen**.

Ein Menü wird geöffnet, in dem Sie die Einladung anpassen und einen Sitzungsschlüssel für den Benutzer erstellen können.

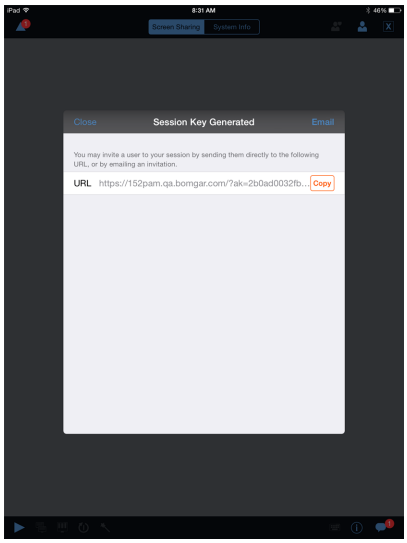


Tippen Sie auf **Sicherheitsprofil**, um auf eine Liste von verfügbaren Benutzerprofilen zuzugreifen. Diese Profile werden in der Verwaltungsschnittstelle erstellt und bestimmen, welche Berechtigungen der externe Benutzer hat. Wenn Sie ein Profil auswählen, wird die Liste geschlossen.

Tippen Sie als nächstes auf die Option **Schlüssel erstellen** in der oberen rechten Ecke des Bildschirms.

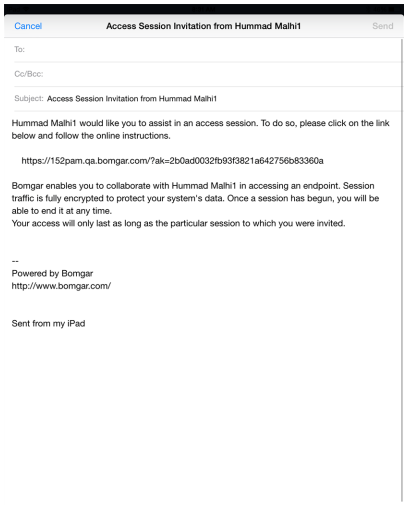
Nach dem Tippen darauf wird der Bereich **Sitzungsschlüssel wurde erstellt** ausgefüllt.

Tippen Sie auf die Option **E-Mail** in der oberen rechten Bildschirmecke.



Eine E-Mail wird erstellt. Nehmen Sie jegliche notwendigen Änderungen an der E-Mail vor.

Wenn Sie fertig sind, tippen Sie auf **Senden**.



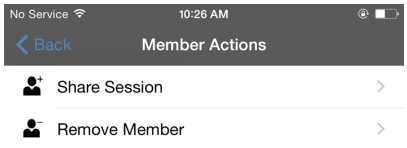
> ***Hinweis:*** *Ebenfalls haben Sie die Möglichkeit, die URL aus dem Bereich* ***Sitzungsschlüssel wurde erstellt*** *zu kopieren. Klicken Sie einfach auf die Option* ***Kopieren*** *neben der URL.*

Nachdem der externe Benutzer die E-Mail erhalten hat, muss er auf die **URL** in der E-Mail klicken. Er gelangt dann zum **Zugriffsportal**, wo er zum Herunterladen der access console aufgefordert wird.

Nach dem Herunterladen der Konsole erscheint die Anmeldungsseite zur access console mit bereits eingegebenem Zugriffssitzungsschlüssel. Dann muss der Benutzer auf **Anmelden** tippen, um auf die Konsole zuzugreifen.

Über die iOS-Zugriffskonsole ein Mitglied aus einer Sitzung entfernen

Sie können einen Benutzer aus einer freigegebenen Sitzung entfernen. Tippen Sie auf einem iPhone auf das Symbol **Aktionen** unten auf dem Bildschirm. Wählen Sie **Mitgliederaktionen**. Tippen Sie auf **Mitglied entfernen**.



Tippen Sie auf einem iPad auf das Personensymbol oben rechts auf dem Bildschirm. Wählen Sie im Menü **Mitglied entfernen**.

Wählen Sie den Benutzer, den Sie entfernen möchten. Tippen Sie dann auf die Option **Entfernen**.

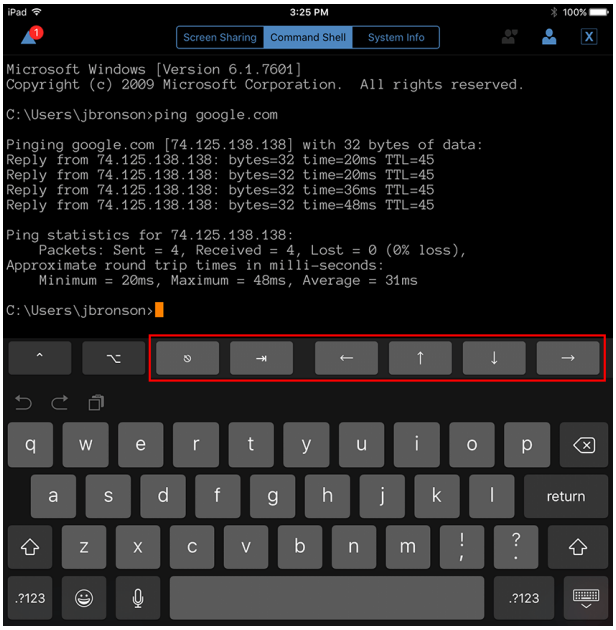
Öffnen Sie die Befehlsshell am Remote-Endpunkt mithilfe der Zugriffskonsole (Apple iOS)

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

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.

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

Wenn mehrere Befehlsshells geöffnet sind, können Sie den Shell-Bildschirm nach links und rechts wischen, um zwischen den offenen Shells zu wechseln.



Befehlsshell-Tools

	Öffnen Sie eine neue Shell, um mehrere Instanzen der Eingabeaufforderung auszuführen.
	Schließen Sie die aktuelle Befehlsshell. Andere offene Befehlsshells werden weiterhin ausgeführt.
	Schließen Sie alle offenen Befehlsshells.
	Zeigt eine Liste der aktuell geöffneten Befehlsshells. Tippen Sie auf ein Element in der Liste, um auf die zugehörige Befehlsshell zuzugreifen.

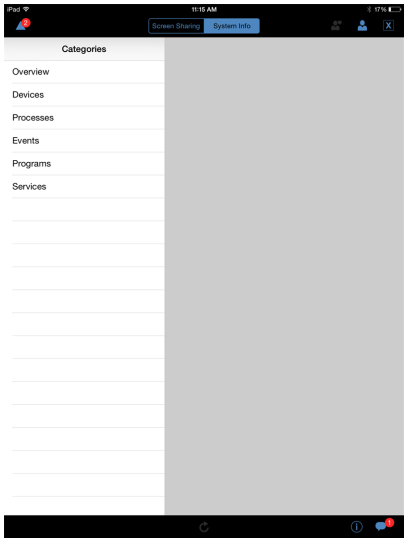
Remote-Systeminformationen über die iOS-Zugriffskonsole einsehen

Berechtigte Benutzer können eine komplette Momentaufnahme der Systeminformationen des Remote-Geräts anzeigen, um die Diagnose und Problemlösung zu beschleunigen. Die verfügbaren Systeminformationen hängen vom Remote-Betriebssystem und der Konfiguration ab.

Um Systeminformationen anzufordern, navigieren Sie zu **Systeminformationen**. Tippen Sie auf **Anfordern**.

Wählen Sie aufeinanderfolgende Kategorienamen, um auf die gewünschten Daten zuzugreifen. Um zur vorherigen Kategorie zurückzukehren, tippen Sie auf die Schaltfläche **Zurück**.

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



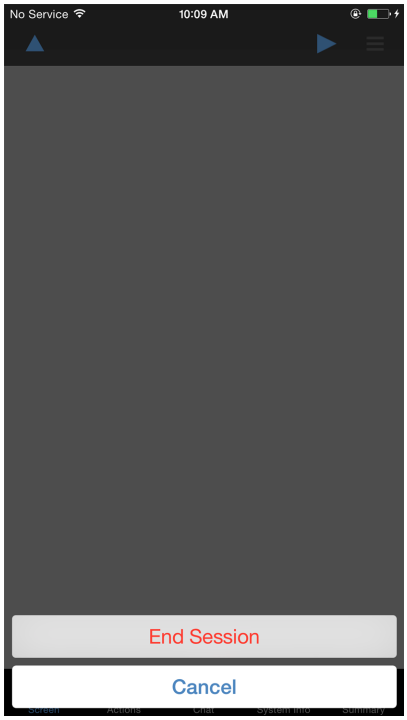
Zusammenfassung einer Zugriffssitzung ansehen

Die Seite **Zusammenfassung** bietet einen Überblick zum Remote-System, auf das zugegriffen wird. Die Seite **Zusammenfassung** gibt folgende Informationen zum Remote-System an:

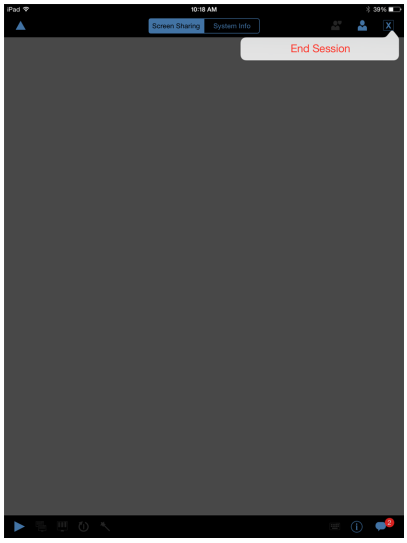
- **IP-Adresse**
- **Name des Kunden**
- **Name des Computers**
- **Plattform**

Schließen Sie eine Zugriffssitzung in der iOS-Zugriffskonsole

Um eine Sitzung auf einem iPhone zu verlassen, tippen Sie auf das Dreiecksymbol in der oberen linken Ecke des Bildschirms.



Um eine Sitzung auf einem iPad zu verlassen, tippen Sie auf das **X** in der oberen rechten Ecke des Bildschirms.



> ***Hinweis:*** *Es ist auch die Option* ***Sitzung beenden*** *verfügbar, indem Sie auf das Symbol* ***Aktionen*** *unten auf dem Bildschirm tippen.*

Wenn Sie der Sitzungseigentümer sind, schließt **Sitzung beenden** die Sitzungsseite in Ihrer access console und entfernt jegliche zusätzliche Benutzer, für welche die Sitzung möglicherweise freigegeben wurde. Ein installiertes Jump-Element wird jedoch nicht gelöscht.

Wenn Sie nicht der Sitzungseigentümer sind, werden Sie mit dem Tippen auf das **X**-Symbol und der Auswahl von **Sitzung verlassen** aus der Sitzung entfernt. Die Sitzung wird weiterhin durch den Sitzungseigentümer und andere Benutzer, für die die Sitzung freigegeben wurde, fortgesetzt.