BeyondTrust

Remote Support 23.2
Administratorhandbuch

TC:12/12/2023

Inhaltsverzeichnis

Remote Support Verwaltungsschnittstelle

Diese Anleitung bietet eine detaillierte Übersicht über die **/login**-Schnittstelle und soll Ihnen bei der Verwaltung Ihrer BeyondTrust-Software und von BeyondTrust-Benutzern helfen. Das BeyondTrust Appliance B Series dient als zentrale Administrations- und Verwaltungsstelle für Ihre BeyondTrust-Software und ermöglicht es Ihnen, sich von einem beliebigen Punkt mit Internetzugang aus anzumelden, um die Konsole d. Support-Technikers herunterzuladen.

Verwenden Sie dieses Handbuch erst, wenn die anfängliche Einrichtung und Konfiguration des B Series Appliances durch einen Administrator abgeschlossen wurde, entsprechend der Beschreibung im BeyondTrust Appliance B Series Installationshandbuch für Hardware auf www.beyondtrust.com/docs/remote-support/getting-started/deployment/hardware. Sobald BeyondTrust korrekt installiert ist, können Sie Kunden sofort unterstützen. Sollten Sie Hilfe benötigen, wenden Sie sich bitte an unter www.beyondtrust.com/support.

Anmeldung in der Verwaltungsschnittstelle

Anmelden

Mit der Benutzer-Verwaltungsschnittstelle können Administratoren Benutzerkonten erstellen und Software-Einstellungen konfigurieren. Melden Sie sich in der Benutzer-Verwaltungsschnittstelle an. Dazu wechseln Sie zur öffentlichen URL Ihres B Series Appliances, gefolgt von **/login**.

Obgleich es sich bei der URL Ihres B Series Appliance um jedes registrierte DNS handeln kann, ist sie wahrscheinlich eine Unterdomäne der Hauptdomäne Ihres Unternehmens, zum Beispiel **access.example.com/login**.

Standardbenutzername: **admin**

Standardpasswort: **password**

Weil BeyondTrust Remote Support von mehreren Benutzern gleichzeitig lizenziert wird, können Sie beliebig viele Konten mit jeweils eindeutigen Benutzernamen und Kennwörtern einrichten.

Hinweis: *Aus Sicherheitsgründen unterscheiden sich der Administrator-Benutzername und das für die Schnittstelle /appliance verwendete Passwort von den für die Schnittstelle /login verwendeten Anmeldedaten und müssen daher separat verwaltet werden.*

Wenn die Zwei-Faktor-Authentifizierung für Ihr Konto aktiviert wurde, geben Sie den Code der Authentifikator-App ein.

Hinweis: *Wenn mehr als eine Sprache für Ihre Website aktiviert ist, wählen Sie die gewünschte Sprache aus dem Dropdown-Menü. Sie können auch die Sprache Ihrer Wahl ändern, nachdem Sie sich auf der Verwaltungsseite angemeldet haben.*

Weitere Informationen zu 2FA finden Sie in So verwenden Sie Zwei-Faktor-Authentifizierung mit BeyondTrust Remote Support auf www.beyondtrust.com/docs/remote-support/how-to/2-factor-authentication/.

Passwortlose Anmeldung

FIDO2-zertifizierte Authentifizierer können für die sichere Anmeldung ohne Eingabe Ihres Passworts auf der Desktop-Konsole d. Support-Technikers (nur Windows), Web-Konsole des Support-Technikers und der Verwaltungsschnittstelle /login verwendet werden. Sie können bis zu 10 Authentifizierer registrieren.

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

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

Integrierte Browser-Authentifizierung verwenden

Wurde Kerberos korrekt für die Einzelanmeldung konfiguriert, können Sie auf den Link für die Verwendung der integrierten Browser-Authentifizierung klicken und dann direkt auf die Webschnittstelle zugreifen, ohne Ihre Anmeldedaten eingeben zu müssen.

Weitere Informationen finden Sie in Kerberos-Server für die Einzelanmeldung unter https://www.beyondtrust.com/docs/remote-support/how-to/integrations/security-providers/kerberos/index.htm.

Passwort vergessen?

Wenn auf der Seite **/login > Verwaltung > Sicherheit** die Passwortzurücksetzung aktiviert wurde und der SMTP-Server für Ihre Site eingerichtet wurde, wird dieser Link sichtbar sein. Um Ihr Passwort zurückzusetzen, klicken Sie auf den Link, geben Sie Ihre E-Mail-Adresse ein und klicken Sie dann auf **Senden**. Wenn mehr als ein Benutzer die gleiche E-Mail-Adresse besitzt, müssen Sie Ihren Benutzernamen bestätigen. Sie erhalten eine E-Mail mit einem Link, mit dem Sie zur Anmeldungsseite gelangen. Geben Sie auf dem Anmeldungsbildschirm Ihr neues Passwort ein und klicken Sie dann auf **Passwort ändern**.

Anmeldungsvereinbarung

Administratoren können den Zugriff auf den Anmeldebildschirm einschränken, indem sie eine erforderliche Anmeldungsvereinbarung aktivieren, die bestätigt werden muss, bevor der Anmeldebildschirm angezeigt wird. Auf der Seite **/login > Verwaltung > Website-Konfiguration** können Sie die Anmeldungsvereinbarung aktivieren und anpassen.

Suche /login Verwaltungsschnittstelle

Von jeder Seite innerhalb von Remote Support /login können Sie über die Suchleiste in der oberen rechten Ecke nach Einstellungen und Funktionen innerhalb der Verwaltungsschnittstelle suchen. Diese Funktion sucht nach statischem Text, einschließlich Titeln und Beschriftungen, innerhalb der Gesamtheit von /login. Die Suchergebnisse werden in einer Dropdown-Liste nach Seiten gruppiert aufgelistet. Sie können auf jedes Element in den aufgelisteten Suchergebnissen klicken, um direkt auf die Seite in /login zu gelangen. Die für Ihre Suche relevanten Titel und Bezeichnungen werden auf der Seite hervorgehoben.

Hinweis:

- *Die Suchergebnisse umfassen nur die Bereiche innerhalb von /login, für die Sie Berechtigungen haben.*
- *Von Benutzern eingegebene Elemente werden nicht durchsucht.*
- *Die Suche unterstützt alle von /login unterstützten Sprachen – alle Sprachen werden durchsucht und erfasst.*

Status

Informationen: Anzeigen von Details der BeyondTrust Remote Support-Software

Website-Status

Die Hauptseite der BeyondTrust Remote Support-/login-Schnittstelle bietet einen Überblick über die Statistik Ihres B Series Appliance. Wenn Sie den technischen BeyondTrust Technical Support-Support für Softwareaktualisierungen oder zur Problembehebung kontaktieren, werden Sie möglicherweise darum gebeten, eine Bildschirmaufnahme dieser Seite zur Verfügung zu stellen.

Zeitzone

Ein Administrator kann aus einer Dropdown-Liste die passende Zeitzone auswählen und so das korrekte Datum und die korrekte Uhrzeit des B Series Appliances für die ausgewählte Region festlegen.

Gesamtanzahl gestatteter Jump-Clients

Sehen Sie sich die Gesamtanzahl der aktiven und passiven Jump-Clients an, die auf Ihrem System gestattet sind. Wenn Sie mehr Jump-Clients benötigen, kontaktieren Sie BeyondTrust Technical Support.

Lizenzen für umfassenden Support

Sehen Sie sich die Anzahl der Lizenzen an, die auf Ihrem BeyondTrust Appliance B Series verfügbar sind. Wenn Sie mehr Lizenzen benötigen, kontaktieren Sie die BeyondTrust-Vertriebsabteilung.

Chat-Support-Lizenzen

Sehen Sie sich die Anzahl der Chat-Lizenzen an, die auf Ihrem BeyondTrust Appliance B Series verfügbar sind. Wenn Sie mehr Lizenzen benötigen, kontaktieren Sie die BeyondTrust-Vertriebsabteilung.

Lizenzpakete

Einmalig installierte Listen und wiederkehrende Lizenzpakete unter Angabe von deren Anzahl, aktivem Status, Anfangs- und Enddatum und wiederkehrendem Status. Kunden mit Lizenzen in Form eines Abonnements können mehrere einzelne Lizenzpakete hinzufügen, die entweder ablaufen (bersten) oder sich reaktivieren (saisonal).

Hinweis: *Aktive Lizenzpakete sind in der Anzahl der vollständigen Support-Lizenzen enthalten; sie können allerdings keinen Lizenzpools zugewiesen werden.*

Neustart der Remote Support-Software

Sie können die BeyondTrust-Software aus der Ferne neu starten. Starten Sie Ihre Software nur neu, wenn Sie der BeyondTrust Technical Support dazu auffordert.

Client-Software

Dies ist der Hostname, zu dem die BeyondTrust-Client-Software eine Verbindung herstellt. Wenn der von der Client-Software verwendete Hostname geändert werden muss, benachrichtigen Sie den BeyondTrust Technical Support über die benötigten Änderungen, damit der Support eine Softwareaktualisierung bereitstellen kann.

Verbundene Clients

Zeigen Sie die Anzahl und den Typ der BeyondTrust-Software-Clients an, die mit Ihrem BeyondTrust Appliance B Series verbunden sind.

ECM-Clients

Zeigen Sie die Anzahl der BeyondTrust Endpunkt-Anmeldedaten-Manager (ECM) an, die mit Ihrem BeyondTrust Appliance B Series verbunden sind. Sie können auch Informationen zum Ort und der Verbindungszeit jedes ECMs anzeigen.

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

Hinweis: *Wenn mehrere ECMs mit einer BeyondTrust-Website verbunden sind, leitet das B Series Appliance Anfragen an den ECM, der am längsten mit dem B Series Applianceverbunden ist.*

Support-Techniker: Anzeige angemeldeter Support-Techniker und Senden von Nachrichten

Status | SUPPORT-TECHNIKER

Angemeldete Support-Techniker

Zeigen Sie eine Liste der bei der Konsole d. Support-Technikers angemeldeten Support-Techniker an, sowie deren Anmeldezeit und ob sie Support- oder Präsentationssitzungen abhalten.

Sitzung beenden

Sie können die Verbindung eines Support-Technikers mit der Konsole d. Support-Technikers beenden.

Nachricht an Support-Techniker senden

Senden Sie über ein Pop-up-Fenster in der Konsole d. Support-Technikers eine Nachricht an alle angemeldeten Support-Techniker.

Support-Techniker mit erweiterter Verfügbarkeit

Sie können Support-Techniker anzeigen, für die der erweiterte Verfügbarkeitsmodus aktiviert wurde. Die Aktivierung des erweiterten Verfügbarkeitsmodus verbraucht eine Lizenz.

Erweiterte Verfügbarkeit deaktivieren

Sie können die erweiterte Verfügbarkeit eines Support-Technikers deaktivieren, um eine Lizenz freizugeben.

Neues: Siehe Softwareversionsdetails

Neues

Verschaffen Sie sich problemlos einen Überblick über die neuen BeyondTrust-Funktionen, die mit jeder Version verfügbar werden. Erfahren Sie mehr über die neuen Funktionen, sobald sie verfügbar werden, um das gesamte Potenzial Ihrer BeyondTrust-Bereitstellung zu nutzen.

Wenn Sie sich nach einem BeyondTrust-Software-Upgrade erstmals in der Verwaltungsschnittstelle anmelden, wird die Seite **Neues** angezeigt, um Sie auf neue Funktionen auf Ihrer Website hinzuweisen. Sie müssen ein Administrator sein, um diese Registerkarte anzuzeigen.

Die auf der Seite **Neues** angezeigten Informationen stehen über das Menü **Hilfe > Über** in der Konsole d. Support-Technikers auch Support-Technikern zur Verfügung.

> *Weitere Informationen finden Sie in Aktualisierungen und Feature-Listen unter https://www.beyondtrust.com/docs/remote-support/updates/index.htm.*

Benutzer-Menü

Das Benutzer-Dropdown-Menü in der oberen rechten Ecke des Bildschirms ermöglicht den Zugriff auf einige wichtige Funktionen von jeder Stelle der Verwaltungsseite aus. Klicken Sie auf das Benutzersymbol, um den angemeldeten Benutzernamen und die E-Mail-Adresse sowie die verfügbaren Links und Optionen anzuzeigen.

Abmelden: Klicken, um von der Verwaltungsschnittstelle /login abgemeldet zu werden. Hierdurch werden Sie nicht von Konsolen abgemeldet. Von diesen müssen Sie sich separat abmelden.

E-Mail-Einstellungen, Anzeigenamen oder Foto ändern: Dies ist ein Link zu **Mein Konto > Profil**.

Passwort ändern: Dies ist ein Link zu **Mein Konto > Sicherheit**.

Starten Web-Konsole des Support-Technikers: Damit haben Sie bequemen Zugriff auf die Web-Konsole des Support-Technikers von überall in /login.

Herunterladen Konsole d. Support-Technikers: Hier finden Sie einen schnellen Link zum Herunterladen der Web-Konsole des Support-Technikers.

Erweiterte Verfügbarkeit aktivieren: Klicken, um diese Funktion in Konsole d. Support-Technikers zu aktivieren. Sobald sie aktiviert ist, wechselt diese Option zu **Deaktivieren** und kann erneut angeklickt werden, um diese Funktion zu deaktivieren.

Sprache: Zeigt die aktuelle Sprache an. Wenn mehr als eine Sprache für Ihre Website aktiviert ist, wählen Sie die gewünschte Sprache aus dem Dropdown-Menü. Diese Sprache wird auch auf Web-Konsole des Support-Technikers angewendet.

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

Weitere Informationen zu diesen Funktionen finden Sie hier:

- *„Eigenes Konto: E-Mail- und Benutzereinstellungen ändern und den erweiterten Verfügbarkeitsmodus aktivieren“ auf Seite 17*
- *„Das Passwort ändern“ auf Seite 19*
- *Verwenden der erweiterten Verfügbarkeit, um auch nach der Abmeldung einen Zugriff zu ermöglichen unter https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/extended-availability.htm.*

Konsolen & Downloads: Starten Sie Web-Konsole des Support-Technikers und laden Sie die Desktop-Konsole d. Support-Technikers herunter

Konsolen & Downloads | KONSOLE DES SUPPORT-TECHNIKERS

Web-Konsole des Support-Technikers

Starten Sie die Web-Konsole des Support-Technikers, eine webbasierte Konsole d. Support-Technikers. Greifen Sie über Ihren Browser auf Remote-Systeme zu, ohne die volle Konsole d. Support-Technikers herunterladen und installieren zu müssen.

Konsole d. Support-Technikers

Plattform auswählen

Wählen Sie das Betriebssystem, auf dem Sie diese Software installieren möchten. Standardmäßig wird in diesem Dropdown-Menü das geeignete Installationsprogramm für Ihr Betriebssystem erkannt.

> *Weitere Informationen finden Sie im Web-Konsole des Support-Technikers-Handbuch auf https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/web/index.htm.*

Konsole d. Support-Technikers herunterladen

Laden Sie das Installationsprogramm für die BeyondTrust Konsole d. Support-Technikers herunter, um Remote-Support bereitzustellen.

Um die Konsole d. Support-Technikers ohne die Anzeige von Fenstern, Spinnern, Fehlern oder sichtbaren Benachrichtigungen zu installieren, fügen Sie **/S** an das Ende des EXE-Befehls an. Für die Stapelbereitstellung empfiehlt BeyondTrust jedoch die Verwendung des MSI-Installationsprogramms.

Der Microsoft Installer eignet sich für Systemadministratoren, die die Zugriffskonsole auf einer großen Anzahl von Systemen bereitstellen müssen, und kann zusammen mit dem Systemverwaltungs-Tool Ihrer Wahl verwendet werden. Wenn der Befehl zur Installation der Zugriffskonsole mithilfe eines MSI verfasst wird, wechseln Sie in das Verzeichnis, in das das MSI heruntergeladen wurde, und geben Sie den auf der Seite **Mein Konto** angegebenen Befehl ein.

Sie können für Ihre MSI-Installation auch optionale Parameter eingeben.

- **INSTALLDIR=** akzeptiert jeden gültigen Verzeichnispfad, in dem die Zugriffskonsole installiert werden soll.
- **RUNATSTARTUP=** akzeptiert **0** (Standard) oder **1**. Falls Sie 1 eingeben, wird die Konsole bei jedem Hochfahren des Computers ausgeführt.
- **ALLUSERS=** akzeptiert **“”** (Standard) oder **1**. **“”** ist der Standardwert. Dieses Attribut wird nur bei der Angabe von Einzelsysteminstallationen benötigt.

ALLUSERS=“” führt zu einer Einzelbenutzerinstallation. Dies zwingt die Konsole d. Support-Technikers dazu, im gleichen Kontext wie die Ausführung der MSI-Installation installiert zu werden. Dies ist nicht ideal, wenn das lokale System zur Ausführung der Installation verwendet wird, wie bei Stapelbereitstellungsassistenten häufig der Fall ist. Es ist nicht möglich, die Installation über MSI-Parameter an einen bestimmten Benutzer zu binden. Wenn Sie das MSI also über ein automatisches Bereitstellungssystem bereitstellen und dabei den Parameter für die Einzelbenutzerinstallation verwenden, muss das Bereitstellungssystem die MSI-Installation im Kontext des gleichen Benutzers ausführen, der sich später in der Konsole anmelden können soll.

- **SHOULDAUTOUPDATE=1** Wenn Sie nur für den aktuellen Benutzer installieren, können Sie die Konsole automatisch jedes Mal aktualisieren, wenn die Website aktualisiert wird. Geben Sie dazu den Wert **1** ein. Ein Wert von **0** (Standard) bedeutet, dass keine automatische Aktualisierung stattfindet und die Konsole manuell neu installiert werden muss, wenn die Website aktualisiert wird. Falls Sie die Konsole für alle Benutzer installieren, wird sie nicht automatisch aktualisiert.
- **/quiet** oder **/q** führt das Installationsprogramm aus, ohne dass Fenster, Spinner, Fehler oder andere sichtbare Warnungen angezeigt werden.

Hinweis: *Wenn Sie* ***ALLUSERS=1*** *mit* ***SHOULDAUTOUPDATE=1*** *verwenden, wird die Konsole d. Support-Technikers nicht automatisch aktualisiert. Wenn Sie* ***SHOULDAUTOUPDATE=1*** *ohne* ***ALLUSERS=1*** *verwenden, wird die Konsole d. Support-Technikers automatisch aktualisiert, ohne dass Sie andere Anmeldedaten als die des BeyondTrust- und aktiven Windows-Benutzers angeben müssen. Keine Administrator-Anmeldedaten sind nötig.*

WICHTIG!

Wird die Konsole d. Support-Technikers über MSI installiert, müssen noch immer einige Informationen von dem B Series Appliance abgerufen werden. Während der erstmaligen Anmeldung wird ein Token für die Konsole d. Support-Technikers bereitgestellt, das zur Anforderung von Software-Updates verwendet wird. Wenn sich vor dem Upgrade des B Series Appliances kein Benutzer in der Konsole d. Support-Technikers anmeldet oder wenn eine MSI einer vorherigen Version zur Installation der Konsole d. Support-Technikers verwendet wird, wird die Konsole nicht aktualisiert, da das nötige Token fehlt. In diesem Fall wird der folgende Fehler angezeigt:

„Kommunikationsfehler mit Server während der Softwareaktualisierung. Aktualisieren Sie die Software, indem Sie sie von der Website herunterladen. (1.1gws)“

Aus diesem Grunde gilt: Wenn die Konsole d. Support-Technikers per MSI stapelbereitgestellt wird, führen Sie die nötigen Schritte durch, um sicherzustellen, dass sich Benutzer mindestens einmal vor der Installation von Updates auf dem BeyondTrust Appliance B Series in der Konsole anmelden.

Weitere Informationen finden Sie hier:

- *BeyondTrust Konsole des Support-Technikers auf https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/index.htm*
- *Stapelbereitstellung der BeyondTrust-Software auf Macs auf https://www.beyondtrust.com/docs/remote-support/how-to/mass-deploy-mac/index.htm*

Konsolen & Downloads: Installationsprogramm für Virtual Smart-Card herunterladen

Konsolen & Downloads | TREIBER

Installationsprogramm für Virtual Smart-Card herunterladen

Eine virtuelle Smart-Card ermöglicht es Ihnen, sich an einem Remote-System mithilfe einer Smart-Card, die an Ihrem lokalen System angeschlossen ist, zu authentifizieren.

Windows-Architektur auswählen

Wählen Sie das Betriebssystem, auf dem Sie diese Software installieren möchten. Standardmäßig wird in diesem Dropdown-Menü das geeignete Installationsprogramm für Ihr Betriebssystem erkannt.

Wenn Sie eine lokale Smart-Card auf einem unterstützten Remote-System verwenden müssen, müssen Sie den BeyondTrust Remote Support Virtual Smart Card-Treiber sowohl im System des Support-Technikers als auch des Kunden installieren. Laden Sie den entsprechenden Virtual Smart Card-Treiber (VSC-Installationsprogramm für Support-Techniker) für Support-Techniker herunter und geben Sie ihn an alle Support-Techniker in Ihrem Support-Center weiter, die die Remote-Smart Card-Funktion benötigen. Der Treiber kann manuell oder mithilfe eines Software-Bereitstellungstools installiert werden. Sobald der Treiber installiert ist, erstellt er einen Dienst: Den Remote-Support-VSC-Dienst für Support-Techniker.

Eigenes Konto: E-Mail- und Benutzereinstellungen ändern und den erweiterten Verfügbarkeitsmodus aktivieren

Eigenes Konto | PROFIL

E-Mail-Einstellungen ändern

E-Mail-Adresse

Legen Sie die E-Mail-Adresse fest, an die E-Mail-Benachrichtigungen gesendet werden, wie etwa Passwortzurücksetzungen oder Alarme zum erweiterten Verfügbarkeitsmodus.

Bevorzugte E-Mail-Sprache

Wenn mehr als eine Sprache für die Website aktiviert ist, legen Sie die Sprache fest, in der E-Mails versandt werden sollen.

Passwort

Geben Sie das Passwort für Ihr /login-Konto, nicht Ihr E-Mail-Passwort, ein.

Ändern Sie Ihre Anzeigenamen

Privater Anzeigename

Ihr Name, wie er in allen internen Mitteilungen unter Support-Technikern, in Chat-Mitschrifts-Berichten, Teamaktvititätsberichten usw. angezeigt wird.

Öffentlicher Anzeigename

Ihr Name, wie er Kunden angezeigt wird.

> ***Hinweis:*** *Standardmäßig sind die beiden Felder synchronisiert. Alles, was Sie also in* ***Privater Anzeigename*** *eingeben, wird automatisch in das Feld* ***Öffentlicher Anzeigename*** *kopiert. Um Ihren öffentlichen Anzeigenamen zu ändern, geben Sie den Namen ein, den Ihre Kunden sehen sollen. Um die Felder wieder zu synchronisieren, gleichen Sie die Eingaben einfach wieder an.*

Ihr Foto ändern

Sie können das Ihrem Konto zugeordnete Foto ändern oder löschen. Dieses Foto wird im Chat-Fenster des Kunden-Client und in der **/login**-Verwaltungsschnittstelle angezeigt. Das Bild muss im .png- oder .jpeg-Format sein, nicht größer als 1 MB und mindestens 80x80

Pixel groß. Wählen Sie **Datei auswählen**, um ein Bild auszuwählen. Sobald der gewählte Dateiname angezeigt wird, klicken Sie auf **Hochladen**, um sie zu verwenden, oder auf **Abbrechen**, wenn Sie das gewählte Bild nicht behalten möchten. Wenn das gewählte Bild die richtige Größe hat, zeigt eine Meldung an, dass das Hochladen erfolgreich war.

Erweiterter Verfügbarkeitsmodus

Aktivieren oder Deaktivieren

Aktivieren oder deaktivieren Sie den erweiterten Verfügbarkeitsmodus, indem Sie auf die Schaltfläche **Aktivieren/Deaktivieren** klicken. Mit dem erweiterten Verfügbarkeitsmodus können Sie E-Mail-Einladungen von anderen Benutzern erhalten, die eine Sitzung freigeben möchten, wenn Sie nicht an der Konsole angemeldet sind.

Weitere Informationen finden Sie in Verwenden der erweiterten Verfügbarkeit, um auch nach der Abmeldung einen Zugriff zu ermöglichen unter https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/extended-availability.htm.

Weitere Informationen finden Sie in Kunden-Client: Support-Sitzung Tech-Schnittstelle auf https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/customer-support-interface.htm.

Eigenes Konto: Passworteinstellungen ändern und passwortlose Authentifizierung hinzufügen

Das Passwort ändern

BeyondTrust empfiehlt, dass Sie Ihr Passwort regelmäßig ändern.

Benutzername, aktuelles Passwort, neues Passwort

Stellen Sie sicher, dass Sie mit dem Konto angemeldet sind, dessen Passwort Sie ändern möchten, und geben Sie dann Ihr aktuelles Passwort ein. Erstellen und bestätigen Sie ein neues Passwort für Ihr Konto. Das Passwort kann nach eigenen Wünschen festgelegt werden, solange die Zeichenfolge die definierte Richtlinie erfüllt, die auf der Seite **/login > Verwaltung > Sicherheit** festgelegt wurde.

Passwortlose Authentifizierer

Diese Funktion ist nur verfügbar, wenn sie unter **Verwaltung > Sicherheit** aktiviert wurde. Hier wird auch die Standard-Authentifizierungsmethode ausgewählt. Bei der Anmeldung kann eine der beiden Authentifizierungsmethoden ausgewählt werden.

FIDO2-zertifizierte Authentifikatoren können für die sichere Anmeldung ohne Eingabe Ihres Passworts in Konsole d. Support-Technikers (nur Windows), Web-Konsole des Support-Technikers und /login verwendet werden. Sie können bis zu 10 Authentifizierer registrieren.

Nur FIDO2-zertifizierte Hardware-Authentifizierer, die die Benutzerverifizierung durchführen (Biometrik oder PIN), sind zulässig.

Es gibt zwei Arten von Authentifizierern:

Roaming

Roaming-Authentifizierer oder plattformübergreifende Sicherheitsschlüssel wie YubiKeys sind FIDO2-zertifizierte externe Geräte, die Biometrie oder eine PIN zur Benutzerverifizierung verwenden. Sie können bei der Anmeldung auf der Desktop-Konsole d. Support-Technikers (nur Windows), Web-Konsole des Support-Technikers und /login auf jedem Rechner verwendet werden und werden von jedem Betriebssystem unterstützt, das die Verwendung externer FIDO2-Authentifizierer zulässt.

Plattform

Plattform-Authentifizierer wie Windows Hello oder macOS Touch ID sind integrierte, FIDO2-zertifizierte biometrische Authentifizierer. Diese Authentifizierer sind an das Gerät gebunden, auf dem Sie den Authentifizierer registriert haben. Sie können bei der Anmeldung in Konsole d. Support-Technikers (nur Windows), Web-Konsole des Support-Technikers und /login anstelle Ihres Passworts verwendet werden. Unter macOS und Linux können Plattform-Authentifizierer nur in dem Browser verwendet werden, in dem sie registriert wurden. Inkognito-Fenster oder private Browser können nicht zur Authentifizierung verwendet werden.

Registrieren und Verwalten von Authentifizierern

Auf dem Bildschirm werden alle registrierten Authentifizierer mit Namen, Typ, Registrierungsdatum und -zeit sowie Datum und Uhrzeit der letzten Verwendung angezeigt. Registrierte Authentifizierer können bearbeitet oder gelöscht werden, indem Sie sie auswählen und auf das entsprechende Symbol klicken.

Um einen neuen Authentifizierer zu registrieren, klicken Sie auf **Registrieren**.

Wählen Sie **Roaming** oder **Plattform**, je nach Ihren Anforderungen.

Geben Sie einen **Authentifizierer-Namen** ein. Wählen Sie einen Namen, mit dem Sie diesen Authentifizierer identifizieren können, wenn Sie die registrierten Authentifizierer in einer Liste anzeigen.

Geben Sie Ihr BeyondTrust Remote Support **Kontopasswort** ein. Dies ist das Passwort, für die Anmeldung mit der Authentifizierung *Benutzername & Passwort*, nicht der PIN oder das Passwort des Authentifizierers. Es wird für die Verifizierung Ihrer Identität verwendet, ehe ein neuer Authentifizierer in Ihrem Konto registriert werden kann. Sie ist in keiner Weise mit dem Authentifizierer verbunden.

Klicken Sie auf **Fortsetzen**.

Die übrigen Schritte zur Registrierung Ihres Authentifizierers hängen vom Typ, vom Hersteller, vom Browser und vom Betriebssystem ab.

Tipp: *Browser oder Betriebssystem können die Authentifizierung verzögern, wenn es zu Verzögerungen bei der Beantwortung von Eingabeaufforderungen kommt.*

Legen Sie Authentifizierer (z. B. YubiKey oder Windows Hello) innerhalb des Betriebssystems fest, bevor Sie den Authentifizierer registrieren. Beachten Sie unbedingt die Anweisungen des Herstellers. Zum Beispiel erfordert YubiKey Bio bei der Einrichtung eine PIN, auch für die Authentifizierung mit Fingerabdruck.

Windows Hello kann mit einer PIN und einem Fingerabdruck eingerichtet werden. In diesem Fall kann jede Methode verwendet werden, unabhängig davon, wie sie registriert ist.

Das Registrieren eines Authentifizierers kann fehlschlagen, wenn die Kombination aus Browser und Betriebssystem die passwortlose Authentifizierung nicht unterstützt. Firefox 110 unterstützt zum Beispiel die passwortlose Authentifizierung für Linux und macOS nicht. In solchen Fällen wird normalerweise eine Warnmeldung ausgegeben.

Hinweis: *Authentifizierer registrieren in der Regel fehlgeschlagene Authentifizierungsversuche und können sich sperren. Daher müssen sie gemäß den Anweisungen des Herstellers zurückgesetzt werden. Eine gescheiterte Authentifizierung am Authentifizierungsgerät zählt nicht als gescheiterte Anmeldung bei der BeyondTrust-Website, da die falschen Informationen nicht an die Website übermittelt werden.*

Zwei-Faktor-Authentifizierung

Zwei-Faktor-Authentifizierung aktivieren

Aktivieren Sie die Zwei-Faktor-Authentifizierung (2FA), um das Sicherheitsniveau für Benutzer, die auf /login und BeyondTrust Konsole d. Support-Technikers zugreifen, zu erhöhen. Klicken Sie auf **Zwei-Faktor-Authentifizierung aktivieren** und scannen Sie den angezeigten QR-Code mit einer Authentifizierungs-App, z. B. Google Authenticator. Alternativ können Sie den alphanumerischen Code, der unter dem QR-Code angezeigt wird, manuell in Ihrer Authentifikator-App eingeben.

Die App registriert automatisch das Konto und stellt Ihnen Codes zur Verfügung. Geben Sie Ihr Passwort und den von der Authentifizierungs-App generierten Code ein. Klicken Sie dann auf **Aktivieren**. Bitte beachten Sie, dass jeder Code 60 Sekunden lang gültig ist. Danach wird ein neuer Code generiert. Sobald Sie sich angemeldet haben, haben Sie die Option, zu einer anderen Authentifikator-App zu wechseln oder 2FA zu deaktivieren.

Hinweis: *Wenn 2FA von Ihrem Administrator bereitgestellt wurde, können Sie es nicht deaktivieren.*

Weitere Informationen zu 2FA finden Sie in So verwenden Sie Zwei-Faktor-Authentifizierung mit BeyondTrust Remote Support auf www.beyondtrust.com/docs/remote-support/how-to/2-factor-authentication/.

Konfiguration

Optionen: Verwalten von Sitzungswarteschlangenoptionen, Aufzeichnen von Sitzungen, Einrichten von Textnachrichten

Konfiguration | OPTIONEN

Warteschlangenoptionen für Support-Sitzung Tech.

Sitzungsabschluss zum Abmelden oder Verlassen erforderlich

Wenn Sie **Sitzungsabschluss zum Abmelden oder Verlassen erforderlich** wählen, können sich Benutzer nicht von der Konsole abmelden, solange sie Sitzungsregisterkarten offen haben.

Regeln zum Sitzungsrückfall

Es gibt fünf Regeln dazu, wenn die Verbindung eines Support-Technikers mit einer Sitzung abgebrochen oder beendet wird: (1) Handelt es sich um eine freigegebene Sitzung, wird sie an den Support-Techniker weitergeleitet, der die Sitzung am längsten freigegeben hat. Ist sie nicht freigegeben, wird sie (2) an die letzte Warteschlange weitergeleitet, zu der sie gehört hat, (3) zur Warteschlange, in der sie eingegeben wurde oder (4) zu einer festgelegten Rückfall-Warteschlange. Der zweite Regelsatz kann für reguläre Sitzungen (überwacht), Jump-Sitzungen (unüberwacht) oder beides aktiviert bzw. deaktiviert werden. (5) Wenn kein Support-Techniker gefunden wird, wird die Sitzung schließlich beendet.

***Hinweis:** Befindet sich die Sitzung in einer dauerhaften Warteschlange, gilt die obige Logik nicht. Sie können dauerhafte Warteschlangen über die Seite **Konfiguration > Support-Teams** aktivieren.*

Regeln 2, 3 und 4 für normale Sitzungen und/oder Jump-Sitzungen aktivieren

Aktivieren Sie die mittleren drei Fallback-Regeln für von Kunden initiierte und/oder unüberwachte Sitzungen.

Weitere Informationen finden Sie unter In der Warteschlange befindliche Support-Sitzung Techanzeigen auf https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/queues.htm.

Equilibriumsoptionen

Sitzungsinformationen in allen Alarm-Dialogfeldern anzeigen

Der Support-Techniker erhält eine Nachricht, wenn eine Sitzung zugewiesen wird. Wenn **Sitzungsinformationen in allen Alarm-Dialogfenstern anzeigen** aktiviert ist, zeigen alle Sitzungszuweisungsalarme die Informationen für die Supportanfrage an.

Weitere Informationen finden Sie in Eine Sitzung zum Starten des Supports akzeptieren unter https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/accepting-a-session.htm.

Protokolloptionen für Support-Sitzung Tech.

Bildschirmfreigabe aktivieren / Eigene Bildschirmaufzeichnung anzeigen / Befehlsshell-Aufzeichnung

Wählen Sie, ob Bildschirmfreigabe-Sitzungen, „Eigenen Bildschirm anzeigen"-Sitzungen und/oder Befehlsshell-Sitzungen automatisch als Videos aufgezeichnet werden sollen.

Bildschirmfreigabe / Auflösung für Eigene Bildschirmaufzeichnung anzeigen / Auflösung für Befehlsshell-Aufzeichnung

Legen Sie die Auflösung fest, mit der die Wiedergabe der Sitzungsaufzeichnung angezeigt wird.

***Hinweis:** Alle Aufzeichnungen werden im Raw-Format gespeichert. Die Auflösungsgröße wirkt sich nur auf die Wiedergabe aus.*

Automatische Protokollierung von Systeminformationen aktivieren

Legen Sie fest, ob Systeminformationen automatisch zu Beginn der Sitzung vom Remote-System abgerufen werden und später in den Sitzungsberichtsdetails verfügbar sein sollen.

Protokollierung der Systeminformationen für mobile Plattformen

Wählen Sie, wenn mobile Plattformen unterstützt werden, **Standard** aus, um einen kleinen Datensatz abzurufen oder **Erweitert**, um alle verfügbaren Informationen abzurufen.

***Hinweis:** Diese seitenweit geltenden Einstellungen können durch Einstellungen für öffentliche Websites oder gemäß Kundenwunsch überschrieben werden, wie auf der Seite **Öffentliche Portale > Kunden-Client** konfiguriert.*

Präsentations-Protokolloptionen

Bildschirmfreigabe-Aufzeichnung aktivieren

Wählen Sie, ob Präsentationen automatisch als Videos aufgezeichnet werden sollen.

***Hinweis:** Wenn Sie eine Präsentation starten und darauf warten, dass Teilnehmer beitreten, beginnt die Aufzeichnung erst, nachdem der erste Teilnehmer der Präsentation beigetreten ist. Wenn niemand der Präsentation beitritt, wird keine Sitzungsaufzeichnung erstellt.*

Auflösung für Bildschirmfreigabe-Aufzeichnung

Legen Sie die Auflösung fest, mit der die Wiedergabe der Präsentationsaufzeichnung angezeigt wird.

Peer-to-Peer-Optionen

Die Aktivierung von Peer-to-Peer-Verbindungen für Support-Sitzungen verbessert die Leistung der Support-Werkzeuge Bildschirmfreigabe, Dateiübertragung und Befehlsshell. Unter Umständen ist eine zusätzliche Firewall-Konfiguration erforderlich, um Peer-to-Peer-Verbindungen erfolgreich herzustellen.

Deaktiviert

Deaktiviert Peer-to-Peer-Verbindungen. Um diese Funktion zu aktivieren, müssen Sie einen Server zur Aushandlung der Sitzung wählen. Wird eine Bildschirmfreigabe, ein Dateitransfer oder eine Remote-Shell erkannt, wird versucht, eine Peer-to-Peer-Verbindung aufzubauen. Falls erfolgreich, baut dies eine direkte Verbindung zwischen dem Support-Techniker und den Client-Systemen auf, während ein sekundärer Datenstrom zu Prüfungszwecken weiterhin an das B Series Appliance gesendet wird. Sollte eine Peer-to-Peer-Verbindung nicht hergestellt werden können, wird der Sitzungsdatenverkehr auf die vom B Series Appliance hergestellte Verbindung umgeleitet.

Den gehosteten Peer-to-Peer-Server von BeyondTrust verwenden

Dies ist die standardmäßige Einstellung. BeyondTrust-Clients versuchen, über den von BeyondTrust gehosteten Server eine Peer-to-Peer-Verbindung aufzubauen. Dies erfordert, dass Ihre BeyondTrust-Clients ausgehende Verbindungsanforderungen auf UDP 3478 zu stun.bt3ng.com vornehmen können. Diese Einstellung sollte in den meisten Situationen funktionieren.

Das B Series Appliance als Peer-to-Peer-Server verwenden

Sollte Ihr Unternehmen bestimmte Sicherheitseinstellungen für den Datenverkehr erfordern, können Sie das B Series Appliance als Peer-to-Peer-Server verwenden. Dies erfordert, dass Ihr B Series Appliance eingehende Verbindungsanforderungen auf UDP 3478 ausgehend von Ihren BeyondTrust-Clients annehmen kann. Sie müssen sicherstellen, dass jegliche Firewalls auf der Route zwischen den Clients und dem B Series Appliance den Port UDP 3478 passieren lassen.

> *Weitere Informationen siehe Geräteverwaltung: Konten, Netzwerke und Ports einschränken, Syslog einrichten, Anmeldevereinbarung aktivieren, Administratorkonto zurücksetzen unter https://www.beyondtrust.com/docs/remote-support/getting-started/deployment/web/security-appliance-administration.htm.*

Optionen für E-Mail-Einladungen

Aktivieren von client-seitigen E-Mails für Support- und Präsentations-Einladungen

Wenn aktiviert, können Support-Techniker Einladungs-E-Mails für Support- und Präsentations-Sitzungen über einen lokalen E-Mail-Client wie Outlook versenden. Diese E-Mails werden über das E-Mail-Konto des Support-Technikers versandt. Der Support-Techniker kann die E-Mail, falls gewünscht, anzeigen und ändern.

Serverseitige E-Mails für Support-Einladungen aktivieren

Falls aktiviert, können Support-Techniker Einladungs-E-Mails über das B Series Appliance statt ihren lokalen E-Mail-Client versenden. Ein Dialog fordert den Support-Techniker auf, den E-Mail-Empfänger anzugeben. Der Support-Techniker darf Betreff oder Inhalt der E-Mail nicht ändern. Die E-Mail-Adresse, von der serverseitige E-Mails gesendet werden, kann für jedes Portal über die Seite **Öffentliche Portale > Kunden-Client** angepasst werden, oder es kann die unter **Verwaltung > E-Mail-Konfiguration** konfigurierte Adresse verwendet werden.

> *Weitere Informationen finden Sie in Einen Sitzungsschlüssel zum Starten einer Support-Sitzung Tech generieren auf https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/session-keys.htm.*

SMS-Gateway

SMS-Gateway-URL

Geben Sie eine sichere SMS-Gateway-URL von Ihrem ISP oder einem externen Gateway-Anbieter ein, um Support-Technikern die Möglichkeit zu bieten, Support-Zugangsschlüssel per SMS zu versenden. Senden Sie Support-Mitteilungen per SMS von der Konsole d. Support-Technikers aus an ein mobiles Gerät. SMS, die auf diese Weise an andere Mobilgeräte gesendet werden, erhalten trotzdem einen Sitzungs-Link. Die SMS-Kommunikation wird nicht im B Series Appliance aufgezeichnet.

Probleme: Support-Probleme verwalten

Konfiguration | PROBLEME

Support-Probleme

Erstellen Sie Support-Problemfälle, um das Erlebnis Ihrer Kunden zu optimieren, wenn sie auf dem öffentlichen Portal Support anfordern. Erstellte Probleme können so konfiguriert werden, dass sie im Dropdown-Menü des Kontaktformulars für Problemfälle erscheinen; sie enthalten eine Liste der Support-Probleme, auf die Ihre Kunden wahrscheinlich gestoßen sind.

Da Support-Probleme an technische Support-Teams geleitet werden müssen, müssen Sie Teams erstellen, bevor Sie mit der Erstellung von Support-Problemfällen beginnen können.

Weitere Informationen finden Sie in Konfigurieren der Teameinstellungen unter https://www.beyondtrust.com/docs/remote-support/how-to/equilibrium/configure-team-settings.htm.

Weitere Informationen finden Sie in Problemen Qualifikationen zuweisen auf https://www.beyondtrust.com/docs/remote-support/how-to/equilibrium/assign-skills-issue.htm.

Neues Support-Problem hinzufügen, bearbeiten, löschen

Erstellen Sie ein neues Problem, bearbeiten Sie ein bestehendes Problem oder entfernen Sie ein bestehendes Problem.

Support-Problem hinzufügen oder bearbeiten

Beschreibung

Fügen Sie eine kurze Beschreibung eines Problems hinzu, das Sie als Support-Ticket erwarten. Wird das Kontaktformular für Problemfälle aktiviert, ist diese Beschreibung für Kunden sichtbar und kann Support-Technikern dabei helfen, schnell festzustellen, welches Problem dem Kunden widerfahren ist. Die Beschreibung kann ebenfalls für Support-Techniker sichtbar sein, die Hilfe aus einer Support-Sitzung Tech. heraus anfordern.

Codename

Legen Sie einen Codenamen zu Integrationszwecken fest. Wenn Sie keinen Codenamen festlegen, wird automatisch einer erstellt.

Weiterleiten an

Verwenden Sie das Dropdown-Menü **Weiterleiten an**, um dieses Problem an ein bestimmtes Team weiterzuleiten.

Priorität

Setzen Sie die Priorität des Problems auf **Hoch**, **Mittel** oder **Niedrig**, je nachdem, wie das Problem vom System gehandhabt werden soll. Die Standardeinstellung lautet **Mittel**.

Zulassen, dass Support-Techniker Hilfe für dieses Support-Problem anfordern

Aktivieren Sie als nächstes das Kontrollkästchen, wenn es Support-Technikern gestattet sein soll, während einer Sitzung Hilfe für dieses Support-Problem anzufordern. Falls aktiviert, wird das Problem im Flyout-Fenster **Hilfe anfordern** der Konsole d. Support-Technikers aufgeführt, wenn die Option **Sitzungsfreigabe** gewählt ist.

Erforderliche Qualifikationen

Probleme können mit den Qualifikationen verbunden werden, die erforderlich sind, um das Problem zu lösen. Qualifikationen können **Bevorzugter**, **Weniger bevorzugt** oder **Ignoriert** sein, je nach Wissenslevel, das zur Behebung eines bestimmten Problems erforderlich ist. Dadurch wird festgelegt, wie Support-Anfragen vom System weitergeleitet und gehandhabt werden.

Technische Support-Teams: Gruppieren von Support-Technikern in Teams

Verwalten von Support-Teams

Das Gruppieren von Support-Technikern in Teams sorgt für mehr Effizienz, indem die Führungsaufgaben innerhalb von Support-Techniker-Gruppen zugewiesen werden und Kunden einfacher zu dem Support-Techniker geleitet werden können, der am besten in der Lage ist, ein bestimmtes Problem zu beheben. In der Konsole d. Support-Technikers erscheint jedes Team als separate Warteschlange für wartende Support-Sitzung Tech.

Neues Team hinzufügen, bearbeiten, löschen

Erstellen Sie ein neues Team, bearbeiten Sie ein bestehendes Team oder entfernen Sie ein bestehendes Team. Durch das Löschen eines Teams werden nicht dessen Benutzerkonten gelöscht, sondern lediglich das Team, dem sie zugeordnet sind.

Hinzufügen oder Bearbeiten von Support-Teams

Teamname

Erstellen Sie einen eindeutigen Namen, um dieses Team leichter zu identifizieren.

Codename

Legen Sie einen Codenamen zu Integrationszwecken fest. Wenn Sie keinen Codenamen festlegen, wird automatisch einer erstellt.

Kommentare

Fügen Sie Kommentare hinzu, die den Zweck dieses Teams identifizieren.

Dauerhafte Warteschlange

Wenn diese Option aktiviert ist, verbleiben Support-Sitzung Techen in dieser Warteschlange, selbst wenn keine Support-Techniker zur Verfügung stehen. Eine Sitzung in dieser Warteschlange verbleibt für unbestimmte Zeit darin, bis ein Support-Techniker oder ein API-Vorgang die Sitzung übernimmt. Diese Option bietet zusätzliche Flexibilität für eine individuelle Sitzungsweiterleitung.

Gruppenrichtlinien

Berücksichtigen Sie jegliche Gruppenrichtlinien, die diesem Team Mitglieder zuweisen. Klicken Sie auf den Link, um zur Seite **Gruppenrichtlinie** zu gehen und Richtlinienmitglieder zu verifizieren oder zuzuweisen.

Portal-Zugriff

Support-Techniker können nur auf die Portale zugreifen, auf die ihrem Team Zugriff gewährt worden ist. Über die Portal-Zugriffsoptionen können Sie Mitgliedern eines Teams Zugriff auf alle oder bestimmte Portale gewähren.

Mitgliedern dieses Teams Zugriff auf alle Portale gewähren

Aktivieren Sie das Kontrollkästchen, um Mitgliedern des ausgewählten Teams Zugriff auf alle Portale zu gewähren.

Mitgliedern dieses Team Zugriff auf die folgenden Portale gewähren:

Diese Option wird nur dann angezeigt, wenn die obige Option nicht aktiviert ist. Aktivieren Sie das Kontrollkästchen für jedes Portal, auf das Mitglieder des ausgewählten Teams zugreifen können. Die Mitglieder eines Teams sollten stets Zugriff auf das Standardportal erhalten. Nicht aktivierte Portale werden nicht auf der Liste der Portal-Optionen angezeigt, wenn der Support-Techniker einen Sitzungsschlüssel generiert.

Teammitglieder

Suchen Sie nach Benutzern, die diesem Team hinzugefügt werden sollen. Sie können die Rolle jedes Mitglieds als **Teammitglied**, **Teamführer** oder **Team-Manager** festlegen. Diese Rollen spielen in der **Dashboard**-Funktion der Konsole d. Support-Technikers eine wichtige Rolle.

Zeigen Sie in der folgenden Tabelle bestehende Teammitglieder an. Sie können die Ansicht filtern, indem Sie eine Zeichenfolge in das Feld **Nach Namen filtern** eingeben. Sie können auch Mitgliedereinstellungen bearbeiten oder ein Mitglied aus dem Team löschen.

Um eine Benutzergruppe zu einem Team hinzuzufügen, navigieren Sie zu **Benutzer und Sicherheit > Gruppenrichtlinien** und weisen Sie diese Gruppe einer oder mehreren Teams in einer bestimmten Rolle zu.

> ***Hinweis:*** *Möglicherweise werden Benutzer angezeigt, für die die Optionen **Bearbeiten** und **Löschen** deaktiviert sind. Dies tritt auf, wenn ein Benutzer über eine Gruppenrichtlinie hinzugefügt wird.*
>
> *Sie können auf den Gruppenrichtlinien-Link klicken, um die Richtlinie als Ganzes zu modifizieren. Jegliche Änderungen an der Gruppenrichtlinie werden auf alle Mitglieder dieser Richtlinie angewandt.*
>
> *Sue können auch eine Person zu einem Team hinzufügen und andernorts definierte Einstellungen übersteuern.*

Equilibrium-Einstellungen

Verwalten Sie die automatische Sitzungsweiterleitung für dieses Team mit Equilibrium.

Weiterleitungsalgorithmus

Wird für diese Option **Am wenigsten beschäftigt** gewählt, wird eine Sitzung in dieser Warteschlange dem am wenigsten beschäftigten Support-Techniker zugewiesen, der zur Annahme von Sitzungen aus dieser Warteschlange verfügbar ist. Wird **Qualifikationen stimmen, am wenigsten beschäftigt** gewählt, wird, falls für eine Sitzung benötigte Qualifikationen markiert wurden und falls sich diese in dieser Warteschlange befindet, diese Sitzung dem Support-Techniker mit der besten Qualifikationsübereinstimmung zugewiesen, der zur Annahme von Sitzungen aus dieser Warteschlange verfügbar ist.

Alarm-Zeitüberschreitung

Der Support-Techniker hat so lange Zeit, wie hier festgelegt ist, um eine zugewiesene Sitzung anzunehmen oder abzulehnen. Lehnt der Support-Techniker die Sitzung ab oder kommt es vor seiner Reaktion zu einer Zeitüberschreitung, wird die Sitzung dem nächsten Support-Techniker mit den am besten übereinstimmenden Qualifikationen zugewiesen, der zur Annahme von Sitzungen aus dieser Warteschlange verfügbar ist.

Regel für wartende Sitzung

Sie können auch eine **Regel für wartende Sitzung** erstellen. Falls aktiviert, legen Sie damit fest, wie lange eine Sitzung in dieser Warteschlange verbleiben darf. Wählen Sie dann die Aktion, die durchgeführt werden soll, wenn die Sitzung über die festgelegte Zeit hinaus wartet. Sie können die Sitzung entweder auf eine Überlaufwarteschlange übertragen oder sie als überfällig markieren. Eine überfällige Sitzung spielt einen Audioalarm ab, blinkt in der Warteschlange, bringt die Warteschlange selbst zum Blinken und zeigt eine Popup-Meldung an. Diese Benachrichtigungen können in den Einstellungen für die Konsole d. Support-Technikers geändert werden.

Weitere Informationen finden Sie in Handbuch für die automatische Sitzungsweiterleitung mit Equilibrium at https://www.beyondtrust.com/docs/remote-support/how-to/equilibrium/index.htm.

Dashboard-Einstellungen

In einem Team kann ein Benutzer nur andere Benutzer mit Rollen überwachen, die seiner untergeordnet sind.

***Hinweis:** Es ist aber zu beachten, dass die Rollen strikt auf Teambasis gelten. Ein Benutzer kann also unter Umständen in der Lage sein, einen anderen Benutzer in einem Team zu verwalten, aber nicht den gleichen Benutzer in einem anderen Team.*

Überwachung von Teammitgliedern über Dashboard

Falls aktiviert, kann ein Teamführer oder Manager Teammitglieder über das Dashboard überwachen. Sie können wählen, ob Sie diese Einstellung **Deaktivieren**, auf **Nur Konsole d. Support-Technikers** beschränken oder einem Teamführer oder -Manager die Erlaubnis erteilen möchten, den **Gesamten Bildschirm** eines Teammitglieds zu überwachen. Die Überwachung betrifft Teamführer und Manager aller Teams.

Überwachungsanzeige aktivieren

Ist diese Option aktiviert, sieht ein Teammitglied, dessen Bildschirm überwacht wird, ein Überwachungssymbol auf seinem Bildschirm.

Sitzungstransfer und -übernahme in Dashboard aktivieren

Ist diese Option aktiviert, kann ein Teamführer die Sitzungen eines Teammitglieds übernehmen oder übertragen. Auf ähnliche Weise kann ein Team-Manager sowohl Teammitglieder als auch Teamführer verwalten. Der Teamleiter muss über den Startsitzungszugriff auf das Jump-Item verfügen, das zum Erstellen der Sitzung verwendet wurde, es sei denn, die unten stehende Option ist ebenfalls aktiviert.

Team-Managern/-Leitern erlauben, „Übertragen“, „Übernehmen“ und „Sitzung beitreten“ für Sitzungen zu verwenden, die von Jump-Items gestartet werden, auf die sie nicht den Zugriff „Sitzung starten“ haben

Wenn diese Option aktiviert ist, kann der Teamführer Sitzungen eines Teammitglieds beitreten oder sie übernehmen, selbst wenn er nicht über Zugriff auf die Startsitzung für das Jump-Item verfügt, mit dem die Sitzung erstellt wurde.

> *Weitere Informationen finden Sie in Teammitglieder im Dashboard überwachen auf https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/dashboard.htm.*

Team-Chat-Verlauf

Wiederholung des Team-Chatverlaufs aktivieren

Wenn diese Option aktiviert ist, bleiben Chat-Nachrichten an alle im Bereich **Team-Chat** der Konsole d. Support-Technikers zwischen den Anmeldungen an der Konsole d. Support-Technikers bestehen.

Dies verhindert den Verlust des Chatverlaufs, wenn die Verbindung unterbrochen wird. Dies hat keine Auswirkungen auf den Chat innerhalb einer Sitzung oder auf private Chats.

Stunden des Team-Chatverlaufs zum Wiederholen

Standardmäßig werden 8 Stunden des Verlaufs gespeichert. Dieser Wert kann mit den Symbolen **+** und **-** oder durch Eingabe des gewünschten Wertes von mindestens 1 bis maximal 24 geändert werden. Die Zeit wird in Schritten von einer Stunde eingestellt. Klicken Sie auf **Speichern**, nachdem Sie die Uhrzeit geändert haben.

> ***Hinweis:** Es werden maximal 1000 Chatnachrichten wiedergegeben. Diese Grenze gilt unabhängig von der Anzahl der gewählten Stunden.*

Support-Techniker-Status

Konfigurieren Sie bis zu 10 Statuscodes. Erlauben Sie Support-Technikern, ihren Status anzugeben, wenn sie die automatische Sitzungszuweisung ablehnen. Wenn Support-Techniker ihren Status ändern, wird der neue Status im Dashboard Konsole d. Support-Technikers für alle Teammanager angezeigt. Support-Techniker-Statusänderungen werden außerdem im Teamaktivitätsbericht aufgezeichnet.

Neuer Support-Techniker-Statuscode, bearbeiten, löschen

Erstellen Sie einen neue Support-Techniker-Statuscode, ändern oder entfernen Sie einen vorhandenen Support-Techniker-Statuscode. Es gibt 3 vordefinierte Statuscodes: **Verfügbar**, **Abwesend** und **Beschäftigt**. Der Statuscode **Verfügbar** kann nicht geändert oder gelöscht werden. Die Statuscodes **Abwesend** und **Beschäftigt** können geändert, aber nicht gelöscht werden.

Anzeigename

Erstellen Sie einen eindeutigen Namen, um diesen Support-Techniker-Statuscode leichter zu identifizieren.

Codename

Legen Sie einen Codenamen zu Integrationszwecken fest. Wenn Sie keinen Codenamen festlegen, wird automatisch einer erstellt.

Anzeigen als

Wählen Sie die Option **Abwesend** oder **Beschäftigt**. Dies sehen Teammitglieder zu jedem Support-Techniker-Status in der **Dashboard**-Funktion in Konsole d. Support-Technikers, wenn der Support-Techniker diesen Statuscode verwendet.

Auto-Status-Optionen

Wählen Sie Standard-Status zur Anzeige im Konsole d. Support-Technikers-Dashboard aus, wenn ein Support-Techniker inaktiv oder beschäftigt ist und seinen Status nicht manuell geändert hat.

Support-Techniker – Status „Inaktiv“

Geben Sie einen Status an, der automatisch gesetzt werden soll, wenn der Support-Techniker inaktiv ist.

Support-Techniker – Status „Beschäftigt“

Geben Sie einen Status an, der automatisch gesetzt werden soll, wenn der Support-Techniker beschäftigt ist.

Qualifikationen: Probleme an Support-Techniker weiterleiten

Qualifikationen

Qualifikationen sind die Kompetenzbereiche, die Ihr Support-Techniker abdeckt. Als Administrator müssen Sie eine Liste dieser Qualifikationen erstellen, die entsprechend ihrer Bedeutung in Kategorien eingestuft werden. Diesen Grundqualifikationen können eine Reihe von Unterqualifikationen zugewiesen werden. Beispielsweise kann die Grundqualifikation „Antivirus“ eine Liste gängiger Antivirus-Programme mit jeweils einer bestimmten Unterqualifikation enthalten, die erforderlich ist, um ein Kunden-Support-Problem im Zusammenhang mit Antivirus-Problemen zu lösen.

Support-Techniker, die mit einer bestimmten Qualifikation assoziiert sind, werden rechts aufgelistet. Wenn kein Support-Techniker mit einer Qualifikation verbunden ist, klicken Sie auf **Benutzer und Sicherheit > Benutzer**, wählen Sie einen Benutzer aus, der bearbeitet werden soll, und klicken Sie auf **Verfügbarkeitseinstellungen**, um Qualifikationen zu konfigurieren.

Hinweis: *Um Qualifikationen erstellen und bearbeiten zu können, muss diese Berechtigung vom Benutzer eingestellt werden. Gehen Sie zu* ***Benutzer und Sicherheit > Benutzer****, scrollen Sie nach unten zum Abschnitt* ***Berechtigungen*** *und stellen Sie sicher, dass die Berechtigung* ***Berechtigt, Qualifikationen zu bearbeiten*** *markiert ist. Administratoren wird diese Berechtigung automatisch gewährt.*

Um Qualifikationen zu erstellen oder zu bearbeiten gehen Sie zu **Konfiguration > Qualifikationen**.

Neue Grundqualifikation

Um zu beginnen, müssen Sie eine Liste von Grundqualifikationen als allgemeine Kategorien erstellen.

Neue Qualifikation

Fügen Sie nun Qualifikationen unter der neuen Grundqualifikation hinzu.

Bearbeiten, löschen

Bearbeiten oder entfernen Sie ein bestehendes Objekt.

Priorität ändern

Wenn Sie die Priorität einer Grundqualifikation ändern müssen, klicken Sie auf **Priorität ändern**. Sie können nun Qualifikationen an ihre neuen Positionen ziehen und dort ablegen.

Qualifikationen

Die neuen Grundqualifikationen und ihre Unterkategorien werden in der Baumstruktur **Qualifikationen** angezeigt. Sie können die einzelnen Abschnitte mithilfe der orangefarbenen Pfeile erweitern oder reduzieren.

Grundqualifikationen werden sequenziell von kritischer zu weniger kritisch eingestuft. Wenn Equilibrium aktiviert ist, versucht das System zuerst, alle Grundqualifikationen zuzuordnen. Wenn dies nicht möglich ist, beginnt das System, nach und nach die Qualifikationen der unteren Prioritäten zu entfernen, bis eine Übereinstimmung gefunden wird.

Anzeigename

Erstellen Sie einen eindeutigen Namen, um diese Qualifikation leichter zu identifizieren.

Codename

Legen Sie einen Codenamen zu Integrationszwecken fest. Wenn Sie keinen Codenamen festlegen, wird automatisch einer erstellt.

> *Weitere Informationen finden Sie in Qualifikationen zur Weiterleitung von Problemen an Support-Techniker konfigurieren unter https://www.beyondtrust.com/docs/remote-support/how-to/equilibrium/configure-skills.htm.*

Benutzerqualifikationen importieren

Nachdem Qualifikationen erstellt wurden, können Sie auf der Seite **Benutzer und Sicherheit > Benutzer** Support-Technikern zugewiesen werden.

Wenn eine große Anzahl von Support-Technikern und/oder Qualifikationen vorhanden ist, kann es leichter sein, die Qualifikationen mit der Massenimport-Funktion den Support-Technikern zuzuweisen. Verwenden Sie die Funktion **Datei wählen**, um eine CSV-Datei mit den Benutzernamen und zugehörigen Qualifikationen hochzuladen. Die CSV-Datei sollte das folgende Format aufweisen:

```
"username1", "skill_code_name"
"username1", "skill_code_name2"
"username2", "skill_code_name"
```

Bitte beachten Sie, dass die für einen bestimmten Support-Techniker in der Importdatei aufgeführten Qualifikationen alle Qualifikationen überschreibt, die diesem Benutzer bereits zugeordnet sind. Wenn Sie alle einem bestimmten Benutzer zugeordneten Qualifikationen entfernen müssen, lassen Sie den Codenamen der Qualifikation leer („Benutzername3“, „“).

> *Weitere Informationen finden Sie in Qualifikationen zur Weiterleitung von Problemen an Support-Techniker konfigurieren unter https://www.beyondtrust.com/docs/remote-support/how-to/equilibrium/configure-skills.htm.*

> *Weitere Informationen finden Sie in Qualifikationen Support-Technikern zuweisen unter https://www.beyondtrust.com/docs/remote-support/how-to/equilibrium/assign-skills-rep.htm.*

> *Weitere Informationen finden Sie in Qualifikationszuweisungsalgorithmen unter https://www.beyondtrust.com/docs/remote-support/how-to/equilibrium/skills-routing-algorithms.htm.*

Zugriffssponsoren: Gruppen von berechtigten Benutzern erstellen

Konfiguration | ZUGRIFFSSPONSOREN

Zugriffssponsorengruppen

Erstellen Sie Zugriffssponsorengruppen, damit ein Support-Techniker mit beschränkten Berechtigungen einen Support-Techniker mit mehr Berechtigungen auffordern kann, bestimmte Aktionen in seinem Namen durchzuführen, z. B. einen Kunden-Client auf Administratorrechte heraufzusetzen oder Anmeldedaten für ein Remote-System einzugeben.

Neue Zugriffssponsorengruppe hinzufügen, bearbeiten, löschen

Erstellen Sie eine neue Gruppe, bearbeiten Sie eine bestehende Gruppe oder entfernen Sie eine bestehende Gruppe.

Zugriffssponsorengruppe hinzufügen oder bearbeiten

Name

Erstellen Sie einen eindeutigen Namen, um diese Gruppe leichter zu identifizieren. Dieser Name sollte Support-Technikern dabei helfen, die korrekte Zugriffssponsorengruppe zu bestimmen, von der die Unterstützung angefordert werden soll.

Beschreibung

Fügen Sie eine kurze Beschreibung hinzu, um den Zweck dieser Gruppe zusammenzufassen.

Gruppenmitglieder

Fügen Sie Support-Techniker mit geringerem Berechtigungsumfang als Anfordernde und Support-Techniker mit mehr Berechtigungen als Sponsoren zu dieser Gruppe hinzu.

> *Weitere Informationen finden Sie in Eine Zugriffsanforderung zum Anbieten von Heraufsetzungshilfe annehmen auf https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/access-requests.htm.*

Support-Buttons: Bereitstellen von Support-Button für den schnellen Sitzungsstart

Konfiguration | SUPPORT-BUTTONS

Support-Button-Stapelbereitstellungsassistent

Durch Bereitstellung eines Support-Buttons auf dem Computer Ihres Kunden wird ein Kunden-Client auf dessen Rechner installiert, der eine schnelle, nahtlose Methode für das Starten von Support-Sitzungen Tech. bietet. Der Support-Button hält KEINE Verbindung mit dem B Series Appliance aufrecht, sondern bietet eine vom Kunden eingeleitete Methode zum Anfordern von Support. Abhängig von der Konfiguration der Support-Button und der Support-Site verbindet der Support-Button den Kunden mit einem zuvor festgelegten Support-Techniker oder Team, fordert den Kunden zur Eingabe eines Sitzungsschlüssels auf oder ermöglicht es dem Kunden, ein Kontaktformular für Problemfälle abzusenden. Support-Buttons können auf Computern mit Windows, Mac oder Linux installiert werden.

Weitere Informationen finden Sie in Support-Buttonn verwalten auf https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/support-schaltfläche-management-interface.htm.

Weitere Informationen finden Sie in Support-Button: Schnell Support anfordern auf https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/support-schaltfläche.htm.

Beschreibung

Erstellen Sie einen eindeutigen Namen, um diesen Support-Button leichter zu identifizieren. Dieser Name kann bei der Verwaltung bereitgestellter Support-Buttons hilfreich sein.

Öffentliches Portal

Wählen Sie das öffentliche Portal, über das sich dieses Element für eine Support-Sitzung Tech verbinden soll. Wenn diesem öffentlichen Portal eine Sitzungsrichtlinie zugewiesen ist, kann sich diese Richtlinie auf die Berechtigungen auswirken, die für über dieses Element gestartete Sitzungen erlaubt sind.

Sprache

Ist auf dieser Website mehr als eine Sprache aktiviert, stellen Sie die Sprache ein, die in diesem Support-Button verwendet werden soll. Support-Buttons erkennen die örtliche Sprache bei der Ausführung nicht. Sie verwenden nur die bei der Bereitstellung zugewiesene Standardsprache.

Team

Geben Sie an, ob mit dem Starten einer Sitzung über diesen Support-Button der Kunde in Ihre persönliche Warteschlange oder eine Team-Warteschlange aufgenommen werden soll.

Bereitgestellte Support-Buttons sind gültig für

Stellen Sie die Lebensdauer des Buttons ein. Der Kunde kann mit diesem Button nur so lange Sitzungen starten, wie hier angegeben. Klickt der Kunde auf den Button, nachdem dieser abgelaufen ist, wird eine Meldung angezeigt, dass der Sitzungsschlüssel ungültig ist, und der Browser auf Ihr Support-Portal aktualisiert. Diese Zeit wirkt sich NICHT darauf aus, wie lange das Installationsprogramm aktiv ist oder wie lange eine Sitzung dauern kann.

Installationsmodus

Legen Sie fest, ob der Support-Button für einen einzelnen Benutzer installiert werden soll oder für alle Benutzer des Remote-Systems. Die Bereitstellung eines Support-Buttons für alle Benutzer ist nur auf Windows-Plattformen verfügbar. Wenn Sie Änderungen an dem Profil eines Support-Buttons vornehmen, wird ein für einen einzelnen Benutzer bereitgestellter Support-Button diese Änderungen beim nächsten Verbindungsaufbau übernehmen, während ein für alle Benutzer bereitgestellter Support-Button erneut bereitgestellt werden muss, um diese Änderungen zu empfangen. Zum Erzielen der besten Ergebnisse sollten Sie Support-Buttons für alle Benutzer jedes Mal erneut bereitstellen, wenn Sie Ihre BeyondTrust-Software aktualisieren. Beachten Sie, dass für alle Benutzer bereitgestellte Support-Buttons nicht über die Konsole d. Support-Technikers entfernt werden können. Sie müssen direkt über den Zielcomputer deinstalliert werden.

Profil

Wählen Sie aus dem Dropdown-Menü ein Profil zum Verwenden aus.

Erstellen

Durch Anklicken können Sie den Support-Button erstellen.

Jetzt herunterladen

Plattform

Wählen Sie das Betriebssystem, auf dem Sie diese Software installieren möchten. Standardmäßig wird in diesem Dropdown-Menü das geeignete Installationsprogramm für Ihr Betriebssystem erkannt.

Die MSI-Option eignet sich für Systemadministratoren, die das Support-Buttons-Installationsprogramm auf einer großen Anzahl von Systemen bereitstellen müssen, und kann zusammen mit dem Systemverwaltungs-Tool Ihrer Wahl verwendet werden. Wenn der Befehl zur Installation des Support-Buttons mithilfe eines MSI verfasst wird, wechseln Sie in das Verzeichnis, in das das MSI heruntergeladen wurde, und geben Sie den auf der Seite **Support-Button** angegebenen Befehl ein.

> ***Hinweis:*** *Im Gegensatz zur Konsole d. Support-Technikers führen über MSI installierte Support-Buttons automatische Aktualisierungen durch.*

Bei der Installation einer ausführbaren Support-Button-Datei auf Remote-Windows-Systemen können Sie darüber hinaus einen gültigen benutzerdefinierten Installationspfad angeben, unter dem der Support-Button installiert werden soll. Sollte das angegebene Installationsverzeichnis nicht existieren, wird es erstellt, solange die Installation die notwendigen Berechtigungen am lokalen System besitzt. Sie können das Installationsverzeichnis entweder über das MSI-Installationspaket oder das EXE-Installationspaket angeben. Die Installation in benutzerdefinierten Pfaden wird auf Mac- und Linuxsystemen nicht unterstützt.

Die Syntax für die EXE-Installation lautet:

```
bomgar-scc-w07dc30w8ff8h51116g785zgh151hdfe8y6z7jgc408c90 --cb-install-dir „C:\Support-Button"
```

wobei `bomgar-scc-w07dc30w8ff8h51116g785zgh151hdfe8y6z7jgc408c90` der Dateiname Ihres ausführbaren Installations-Client ist und `„C:\Support-Button"` der Pfad, der für die Installation verwendet werden soll.

Die Syntax für die MSI-Installation lautet

```
msiexec /i bomgar-scc-win64.msi KEY_INFO=w0hdc301hd18wxj8xjfd8z6jzyefz7wzd1gwwd6c408c90
INSTALLDIR="C:\Support-Button"
```

Dabei ist `bomgar-scc-win64.msi` der Name Ihres MSI-Installationspakets, `w0hdc301hd18wxj8xjfd8z6jzyefz7wzd1gwwd6c408c90` der Schlüssel Ihres Installationspakets und `„C:\Support-Button"` der Pfad, der für die Installation verwendet werden soll.

Um einen Support-Button ohne die Anzeige von Fenstern, Spinnern, Fehlern oder sichtbaren Benachrichtigungen zu installieren, fügen Sie **--silent** an das Ende des EXE-Befehls oder **/quiet** an das Ende des MSI-Befehls an.

Herunterladen

Sie können das Installationsprogramm sofort herunterladen, wenn Sie vorhaben, dieses über ein Systemverwaltungs-Tool zu verteilen, oder wenn Sie sich am Computer befinden, auf den Sie später zugreifen müssen.

> ***Hinweis:*** *Weil bei einigen Browsern das Installationsprogramm gespeichert werden muss, bevor es ausgeführt werden kann, kann es manchmal unklar sein, wann der Support-Button vollständig installiert ist. Die heruntergeladene Datei bomgar-scc-{uid}.exe ist nicht der Button selbst, sondern lediglich das Installationsprogramm für den Button. Diese ausführbare Datei muss ausgeführt werden, um die Installation abzuschließen.*

Für E-Mail-Empfänger bereitstellen

E-Mail

Sie können das Installationsprogramm auch per E-Mail an einen oder mehrere Remote-Benutzer senden. Mehrere Empfänger können den Client über den gleichen Link installieren. Klicken Sie auf den **Direkter Download-Link**, um den Link zu kopieren.

Support-Button-Profile – Hinzufügen

Erstellen Sie ein neues Profil, bearbeiten Sie ein bestehendes Profil oder entfernen Sie ein bestehendes Profil. Sie können das standardmäßige Support-Button-Profil zwar bearbeiten, aber nicht löschen.

Name

Erstellen Sie einen eindeutigen Namen, um dieses Profil leichter zu identifizieren. Dieser Name soll Support-Technikern dabei helfen, zu entscheiden, welches Profil einem Support-Button zugeordnet werden soll.

Symbol

Laden Sie die Datei mit dem personalisierten Schaltflächen-Symbol hoch. Die Datei muss vom Typ PNG sein und eine maximale Größe von 150 KB sowie eine Mindesthöhe und -breite von 128 Pixeln haben. Höhe und Breite müssen gleich sein.

Titel

Dieser Titel wird als Titel des Desktopsymbols verwendet.

Kurzbezeichnung

Der Kurztitel wird verwendet, wenn das Betriebssystem des Kunden die Titellänge beschränkt.

Bereitstellungsorte

Legen Sie nun fest, ob der Support-Button auf dem Desktop oder im Menü bereitgestellt werden soll. Die Menüoption wird nur von Windows-, Mac- und Linux-Systemen unterstützt.

Direkten Zugriff auf die Warteschlange zulassen

Legen Sie fest, ob der Kunde den Support-Button verwenden kann, um direkt mit einer bestimmten Warteschlange verbunden zu werden (die Warteschlange wird durch die Dropdown-Liste **Team** im Support-Buttonn-Stapelbereitstellungsassistenten angegeben).

Registrierungsdatei-Generator für eingebetteten Support-Button

Verwenden Sie den **Registrierungsdatei-Generator für eingebettete Support-Buttons**, um Registrierungsdateien zu erstellen, die den Support-Button in der Titelleiste einer Anwendung einbetten. Mit einem eingebetteten Support-Button können Support-Dienstleister den Supportweg für bestimmte Anwendungen vereinfachen. Wenn Ihr technisches Support-Team beispielsweise oft Probleme mit Microsoft Outlook bearbeitet, können Sie einen Support-Button in Outlook einbetten. Sie können diesen eingebetteten Support-Button so konfigurieren, dass sie auf ein bestimmtes Problem hinweist, damit per Klick auf die Schaltfläche sofort eine Sitzung mit dem Team gestartet wird, das am besten auf die Outlook-Problembehandlung vorbereitet ist. Eingebettete Support-Buttons sind nur unter Windows verfügbar.

Zur Erstellung eines eingebetteten Support-Buttons muss zunächst ein Support-Button im Remote-System bereitgestellt werden. Sie können das Support-Button-Profil so festlegen, dass weder die Desktop-Verknüpfung noch der Eintrag im Startmenü erstellt werden.

Installationsmodus

Legen Sie fest, ob die Installation für alle Benutzer eines Systems oder einen einzelnen Benutzer durchgeführt werden soll.

Name der ausführbaren Datei

Geben Sie den Namen des Programms ein, in dem ein Support-Button eingebettet werden soll. Geben Sie dabei nicht den Dateipfad an.

Problem

Wählen Sie optional ein Problem, das mit über diesen eingebetteten Support-Button gestarteten Sitzungen verbunden werden soll. Alternativ können Sie auch **Kein Problem zugewiesen** wählen.

Frontend-Umfrage anzeigen

Wenn Sie **Frontend-Umfrage anzeigen** aktivieren, wird der Kunde aufgefordert, sein Problem zu beschreiben, bevor eine Sitzung gestartet wird. Wenn Sie diese Option nicht markieren, wird die Sitzung sofort und ohne weitere Angaben des Kunden gestartet.

Externer Schlüssel

Sie können Sitzungen, die über diese eingebetteten Support-Buttons gestartet wurden, einen externen Schlüssel zuweisen.

Löschen

Entfernt eine bestehende Anwendung aus dieser Registrierungsdatei.

Neue Zeile hinzufügen

Um mehrere Anwendungen zu einer Registrierungsdatei hinzuzufügen, klicken Sie auf **Neue Zeile hinzufügen** und geben Sie die Informationen für eine andere Anwendung ein.

Registrierungsdatei importieren

Um die Funktionalität eines eingebetteten Support-Buttons zu bearbeiten, können Sie die Registrierungsdatei importieren und ihre Einträge bearbeiten. Wenn Sie fertig sind, klicken Sie auf **Registrierungsdatei erstellen**. Mit dem Ausführen der Registrierungsdatei werden die bestehenden Registrierungseinträge überschrieben.

Registrierungsdatei erstellen

Wenn Sie alle ausführbaren Dateien hinzugefügt haben, in denen Support-Buttons eingebettet werden sollen, klicken Sie auf **Registrierungsdatei erstellen**. Damit werden Sie aufgefordert, eine Registrierungsdatei auf Ihrem System zu speichern. Mit Active Directory oder einem Bereitstellungs-Tool können Sie die Registrierungsdatei auf allen Remote-Systemen bereitstellen, welche die eingebetteten Support-Buttons verwenden sollen. Nach Ausführen der Registrierungsdatei muss sich der Remote-Benutzer ab- und wieder anmelden, damit der Registrierungseintrag für den Support-Button erstellt wird.

> ***Hinweis:*** *Es wird empfohlen, eine Kopie jeglicher generierten Registrierungsdateien zu speichern. Die Informationen zu den Registrierungsdateien werden nicht auf dem BeyondTrust Appliance B Series gespeichert.*

Wenn nun eine der gewählten Anwendungen ausgeführt wird, wird ein Support-Button in der oberen rechten Ecke neben der Minimieren-Schaltfläche angezeigt. Per Klick auf diesen eingebettete Support-Button wird eine Sitzung entsprechend ihrer Profil- und Registrierungsdateieinstellungen gestartet.

> ***Hinweis:*** *Mit dem Ausführen einer Support-Button-Registrierungsdatei auf einem System, das bereits über Support-Button-Registrierungseinträge verfügt, werden die ursprünglichen Registrierungseinträge überschrieben. Wenn Sie also einen Support-Button in einer Anwendung eingebettet haben und sie in einer weiteren Anwendung einbetten möchten, muss die neue Registrierungsdatei die Namen beider ausführbaren Dateien enthalten. Wenn die neue Registrierungsdatei nur den Namen der neuen ausführbaren Datei enthält, wird der eingebettete Support-Button nur in der neuen Anwendung, nicht aber in der vorherigen Anwendung angezeigt.*

Um einen eingebetteten Support-Button aus einer bestimmten Anwendung zu entfernen, ohne ihn zu einer anderen Anwendung hinzuzufügen, müssen Sie die Registrierung bearbeiten. Öffnen Sie die anfangs bereitgestellte Registrierungsdatei mit Notepad oder einem ähnlichen Bearbeitungsprogramm und fügen Sie vor jedem Registrierungsschlüssel, den Sie löschen möchten, einen Bindestrich ein. Speichern Sie die Registrierungsdatei und stellen Sie sie erneut bereit, um den Registrierungseintrag zu entfernen. Im Folgenden ist ein Beispiel für einen zur Löschung markierten Registrierungseintrag angegeben.

```
[-HKEY_LOCAL_MACHINE\Software\Test]
```

Besuchen Sie für weitere Informationen zu Registrierungseinträgen bitte https://support.microsoft.com/kb/310516.

***Hinweis:** Mit dem Deinstallieren des Support-Buttons wird er aus allen Programmen entfernt, in denen er eingebettet wurde. Die Registrierungseinträge werden damit allerdings nicht gelöscht. Wenn also für die gleiche Website ein anderer Support-Button installiert wird, übernimmt dieser die vorherigen Registrierungseinträge und wird in denselben Programmen eingebettet.*

Weitere Informationen finden Sie in Support-Buttonn verwalten auf https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/support-schaltfläche-management-interface.htm.

Benutzerdefinierte Felder: Erstellen und Modifizieren von Feldern für Problemeinreichungen über das öffentliche Portal

Konfiguration | BENUTZERDEFINIERTE FELDER

Benutzerdefinierte Felder

Sie können bis zu 30 benutzerdefinierte Felder konfigurieren. Benutzerdefinierte Felder können für individuelle Support-Sitzungen Tech. mit der Konfiguration für die Problemeinreichung über das öffentliche Portal sowie über bestimmte API-Vorgänge erstellt und konfiguriert werden. Sie werden in der BeyondTrust Konsole d. Support-Technikers angezeigt.

Neues Feld erstellen, bearbeiten, löschen

Erstellen, modifizieren oder löschen Sie ein benutzerdefiniertes Feld. Gelöschte benutzerdefinierte Felder werden nicht mehr in der Konsole d. Support-Technikers oder in den Sitzungsberichten angezeigt.

Benutzerdefinierte Felder hinzufügen oder bearbeiten

Anzeigename

Erstellen Sie einen eindeutigen Namen, um dieses Feld leichter zu identifizieren.

Codename

Legen Sie einen Codenamen zu Integrationszwecken fest. Wenn Sie keinen Codenamen festlegen, wird automatisch einer erstellt.

In der Konsole des Support-Technikers anzeigen

Aktivieren Sie dieses Kontrollkästchen, wenn Sie möchten, dass dieses Feld in der Konsole d. Support-Technikers angezeigt wird.

> ***Hinweis:*** *Um im öffentlichen Portal anzuzeigende Probleme sowie die Reihenfolge, in der diese angezeigt werden sollen, auszuwählen, gehen Sie zu* ***Öffentliche Portale > Umfrage zum Einreichen von Problemen verwenden****. Fügen Sie eine öffentliche Website hinzu oder bearbeiten Sie sie und klicken Sie auf* ***Umfrage zum Einreichen von Problemen verwenden****. Wählen Sie unter den verfügbaren Feldern die Felder aus, die angezeigt werden sollen.*

MS Teams: Aktivieren und Anpassen der Microsoft Teams-Integration

Konfiguration | MS TEAMS

Integration von Microsoft Teams

Wird diese Funktion aktiviert, können Sie damit Ihre Support-Kapazitäten innerhalb von Microsoft Teams erweitern. MS Teams unterstützt mehrere Remote Support-Teams und nutzt die Integration (bei Wunsch auf unterschiedliche Art und Weise) für alle verschiedenen Portal-Websites. Administratoren können eigene Begrüßungen erstellen und eigene BeyondTrustRemote Support-Bots für ihr Unternehmen bereitstellen, so dass ihre Benutzer mit Support-Technikern chatten und im Chat in Microsoft Teams Sitzungseinladungen anklicken können.

Folgen Sie den Anweisungen auf dem Bildschirm, um die Integration vorzunehmen.

> ***Hinweis:*** *Sie müssen* ***Microsoft Teams-Integration aktivieren*** *aktivieren, um die Anweisungen anzuzeigen.*

Ein Portal auswählen

Wenn Sie über mehrere öffentliche Portale verfügen, wählen Sie das Portal für die Integration aus dem Dropdown-Menü **Öffentliche Website zum Bearbeiten auswählen** aus. Um die Teams-Integration für mehrere Portale einzurichten, wiederholen Sie den Prozess bei jedem Portal.

Microsoft Teams-Integration aktivieren

Aktivieren Sie diese Option, um Integration in MS Teams zu aktivieren und zeigen Sie die **Konfigurationsanleitung** und Konfigurationsoptionen an.

Basis-Konfiguration

Befolgen Sie die Anweisungen auf dem Bildschirm, Schritt 1, Punkte 1 bis 7, um einen eigenen Bot für Ihren Azure-Mandanten bereitzustellen und die Informationen für das Ausfüllen der Felder **Basis-Konfiguration** zu erhalten. Dafür müssen Sie in Ihrem Azure-Portal arbeiten.

Bot-Konfiguration

Folgen Sie den Anweisungen auf dem Bildschirm, Schritt 1, Punkt 8, um das Bot-Profil einzurichten.

Stellen Sie den Bot dem Microsoft-Teams-Mandanten bereit

Klicken Sie gemäß Anweisung auf dem Bildschirm, Schritt 2, Punkte 1 bis 4, auf **Teams Manifest-Paket herunterladen**, wenn die Konfiguration abgeschlossen ist, und laden Sie die Datei in das Microsoft Teams-Verwaltungszentrum hoch.

Jump

Jump-Clients: Verwalten von Einstellungen und Installieren von Jump-Clients für unüberwachten Zugriff

Jump | JUMP-CLIENTS

Jump-Client-Installationsprogrammliste

Die Liste zeigt alle vorher installierten aktiven Jump-Client-Installationsprogramme an. Administratoren und berechtigte Benutzer können Jump-Client-Installationsprogramme anzeigen, herunterladen, löschen oder erweitern.

Stapelbereitstellungsassistent für Jump-Clients

Um Zugriff auf den Jump-Client-Stapelbereitstellungsassistenten zu erhalten, klicken Sie oben in der Jump-Client-Installationsprogrammlsite auf **Hinzufügen**.

Mit dem Stapelbereitstellungsassistenten können Administratoren und berechtigte Benutzer Jump-Clients für einen oder mehrere Remote-Computer für den späteren unüberwachten Zugriff bereitstellen.

> *Weitere Informationen finden Sie im Remote Support-Handbuch für Jump-Clients: Unüberwachter Zugriff auf Systeme in einem beliebigen Netzwerk unter https://www.beyondtrust.com/docs/remote-support/how-to/jump-clients/index.htm.*

Jump-Gruppe

Wählen Sie aus der Dropdown-Liste **Jump-Gruppe**, ob Sie den Jump-Client in Ihrer persönlichen Liste von Jump-Elementen oder in einer von anderen Benutzern freigegebenen Jump-Gruppe fixieren möchten. Durch Fixieren in Ihrer persönlichen Liste von Jump-Elementen können nur Sie (und höher gestellte Rollen in Ihrem Team, wie beispielsweise der Teamführer und Team-Manager, wenn Sie ein Teammitglied sind, und der Team-Manager, wenn Sie Teamführer sind) über diesen Jump-Client auf diesen Remote-Computer zugreifen. Wird der Jump-Client in einer freigegebenen Jump-Gruppe fixiert, wird er für alle Mitglieder dieser Jump-Gruppe verfügbar.

Überschreiben während der Installation gestatten

Einige Einstellungen des Stapelbereitstellungsassistenten ermöglichen die Überschreibung, wodurch Sie die Befehlszeile verwenden können, um bereitstellungsspezifische Parameter vor der Installation festzulegen.

Dieses Installationsprogramm gilt für

Das Installationsprogramm ist nur so lange verwendbar, wie in der Dropdown-Option **Dieses Installationsprogramm ist gültig für** angegeben. Lassen Sie ausreichend Zeit zur Installation. Sollte jemand versuchen, das Jump-Client-Installationsprogramm nach Ablauf dieser Zeit auszuführen, schlägt die Installation fehl, und ein neues Jump-Client-Installationsprogramm muss erstellt werden. Darüber hinaus gilt: Wenn das Installationsprogramm innerhalb des gewährten Zeitraums ausgeführt wird, der Jump-Client aber keine Verbindung

zum B Series Appliance aufbauen kann, wird der Jump-Client deinstalliert und ein neues Installationsprogramm muss bereitgestellt werden. Der Gültigkeitszeitraum kann auf einen beliebigen Wert von 10 Minuten bis 1 Jahr festgelegt werden. Diese Zeitangabe hat KEINE Auswirkungen darauf, wie lange der Jump-Client aktiv ist.

Nach der Installation eines Jump-Client verbleibt er online und aktiv, bis er entweder von einem angemeldeten Administrator mit den erforderlichen Berechtigungen, einem Nutzer über die Jump-Schnittstelle oder durch ein Deinstallationsskript vom lokalen System deinstalliert wird. Er kann auch von der Jump-Client-Installationsprogramm-Liste deinstalliert oder erweitert werden. Ein Benutzer kann einen Jump-Client erst entfernen, wenn er die geeigneten Berechtigungen über die /login-Schnittstelle durch den Administrator zugeteilt bekommen hat.

Öffentliches Portal

Wählen Sie das öffentliche Portal, über das sich dieses Element für eine Support-Sitzung Tech verbinden soll. Wenn diesem öffentlichen Portal eine Sitzungsrichtlinie zugewiesen ist, kann sich diese Richtlinie auf die Berechtigungen auswirken, die für über dieses Element gestartete Sitzungen erlaubt sind.

Name

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

Kommentare

Fügen Sie **Kommentare** hinzu, die bei der Suche nach und Identifizierung von Remote-Computern nützlich sein können. Beachten Sie, dass alle über dieses Installationsprogramm bereitgestellte Jump-Clients anfänglich über die gleichen Kommentare verfügen werden, es sei denn, Sie aktivieren **Überschreibung während der Installation zulassen** und verwenden die verfügbaren Parameter, um das Installationsprogramm für individuelle Installationen anzupassen.

Tag

Das Hinzufügen eines **Tags** hilft bei der Anordnung von Jump-Clients in Kategorien innerhalb der Konsole d. Support-Technikers.

Jump-Richtlinie

Sie können auf diesen Jump-Client eine **Jump-Richtlinie** anwenden. Jump-Richtlinien werden auf der Seite **Jump > Jump-Richtlinien** konfiguriert und bestimmen die Zeiten, während denen ein Benutzer Zugriff auf diesen Jump-Client hat. Wird keine Jump-Richtlinie angewendet, kann jederzeit auf diesen Jump-Client zugegriffen werden.

Sitzungsrichtlinie für präsente Kunden und Sitzungsrichtlinie für nicht präsente Kunden

Wählen Sie Richtlinien, die diesem Jump-Client zugewiesen werden sollen. Diesem Jump-Client zugewiesene Richtlinien haben die höchste Priorität bei der Festlegung von Sitzungsberechtigungen. Die **Sitzungsrichtlinie für präsente Kunden** gilt, wenn der Endbenutzer als präsent gilt. Ansonsten gilt die **Sitzungsrichtlinie für nicht präsente Kunden**. Die Art, wie die Kundenpräsenz bestimmt wird, wird von der Jump-Client-Einstellung **Bildschirmstatus verwenden, um Kundenpräsenz zu erkennen** festgelegt. Die Kundenpräsenz wird erkannt, wenn die Jump-Client-Sitzung gestartet wird. Die für die Sitzung verwendete Sitzungsrichtlinie ändert sich nicht im Verlaufe der Sitzung, unabhängig von Änderungen an der Kundenpräsenz im Verlaufe der Sitzung.

Verbindungstyp

Stellen Sie den **Verbindungstyp** für die bereitgestellten Jump-Clients auf **Aktiv** oder **Passiv**.

Jumpoint-Proxy

Falls Sie einen oder mehrere Jumpoints als Proxys eingerichtet haben, können Sie einen Jumpoint auswählen, um diese Jump-Client-Verbindungen per Proxy aufzurufen. Wenn diese Jump-Clients auf Computern ohne eigene Internetverbindungen installiert werden, können sie so den Jumpoint benutzen, um wieder eine Verbindung mit Ihrem B Series Appliance herzustellen. Die Jump-Clients müssen im gleichen Netzwerk installiert sein wie der für den Proxy-Aufruf der Verbindungen ausgewählte Jumpoint.

Maximale Offline-Minuten vor der Löschung

Sie können die **Maximalen Offline-Minuten vor der Löschung** eines Jump-Client aus dem System festlegen. Diese Einstellung überschreibt die globale Einstellung, sofern diese angegeben ist.

Eine heraufgesetzte Installation versuchen, wenn der Client dies unterstützt

Ist die Option **Eine heraufgesetzte Installation versuchen, wenn der Client dies unterstützt** aktiviert, versucht das Installationsprogramm eine Ausführung mit Administratorrechten und installiert den Jump-Client als Systemdienst. Wenn der Versuch der heraufgesetzten Installation nicht erfolgreich ist oder wenn diese Option deaktiviert wird, wird das Installationsprogramm mit Benutzerrechten ausgeführt und installiert den Jump-Client als Anwendung. Diese Option gilt nur für Windows- und Mac-Betriebssysteme.

> ***Hinweis:*** *Ein im Benutzermodus fixierter Jump-Client ist nur verfügbar, wenn dieser Benutzer angemeldet ist. Im Gegensatz dazu gestattet ein im Dienstmodus fixierter Jump-Client mit heraufgesetzten Rechten es dem System, stets verfügbar zu sein, unabhängig davon, welcher Benutzer angemeldet ist.*

Bei Bedarf zur Eingabe von Heraufsetzungs-Anmeldedaten auffordern

Ist **Bei Bedarf zur Eingabe von Heraufsetzungs-Anmeldedaten auffordern** aktiviert, fordert das Installationsprogramm den Benutzer zur Eingabe von Administrator-Anmeldedaten auf, wenn das System verlangt, dass diese Anmeldedaten unabhängig bereitgestellt werden. Ansonsten wird der Jump-Client mit Benutzerrechten installiert. Dies gilt nur, wenn versucht wird, eine heraufgesetzte Installation auszuführen.

Kunden-Client minimiert starten, wenn die Sitzung gestartet wird

Durch die Wahl von **Kunden-Client beim Start der Sitzung minimiert starten** wird der Fokus nicht auf den Kunden-Client gelenkt, und dieser bleibt minimiert in der Taskbar oder im Dock, wenn eine Sitzung über einen dieser Jump-Clients gestartet wird.

Hilfe zur Stapelbereitstellung

Die ausführbare Datei für Windows, Mac oder Linux oder die Windows MSI-Datei eignet sich für Systemadministratoren, die das Jump Client-Installationsprogramm auf einer großen Anzahl an Systemen bereitstellen müssen und kann mit dem Systemverwaltungstool Ihrer Wahl verwendet werden. Sie können einen gültigen benutzerdefinierten Installationspfad angeben, in dem der Jump-Client installiert werden soll.

Sie können außerdem bestimmte Installationsparameter entsprechend Ihrer eigenen Anforderungen überschreiben. Diese Parameter können sowohl für die MSI und EXE mit einem Systemadministrationswerkzeug oder der Befehlszeile angegeben werden. Wenn Sie bestimmte Installationsoptionen während der Installation zur Überschreibung markieren, können Sie die folgenden optionalen Parameter

zur Modifizierung des Jump-Client-Installationsprogramms in individuellen Fällen nutzen. Beachten Sie: Wenn ein Parameter auf der Befehlszeile weitergegeben wird, aber nicht in der /login-Verwaltungsschnittstelle zur Überschreibung markiert wurde, schlägt die Installation fehl. Wenn die Installation fehlschlägt, überprüfen Sie das Ereignisprotokoll des Betriebssystems auf Installationsfehler.

> ***Hinweis:*** *Es kommt häufig vor, dass Sie während der Installation eine Fehlermeldung erhalten, die ein Problem mit dem Layout oder der Darstellung betrifft. Diese kann vernachlässigt werden.*

Befehlszeilenparameter	Wert	Beschreibung
--install-dir	<directory_path>	Gibt ein neues beschreibbares Verzeichnis an, in dem der Jump-Client installiert werden soll. Dies wird nur unter Windows und Linux unterstützt. Stellen Sie bei der Definition eines eigenen Installationsordners sicher, dass der Ordner, den Sie erstellen, nicht bereits existiert und beschreibbar ist.
--jc-name	<name...>	Wenn die Überschreibung gestattet ist, legt dieser Befehlszeilenparameter den Namen des Jump-Clients fest.
--jc-jump-group	Benutzer:<benutzername> Jump-Gruppe:<jumpgroup-code-name>	Wenn die Überschreibung gestattet ist, überschreibt dieser Befehlszeilenparameter die im Stapelbereitstellungsassistent angegebene Jump-Gruppe.
--jc-public-site-address	<public-site-address-hostname>	Wenn die Überschreibung gestattet ist, verknüpft dieser Befehlszeilenparameter den Jump-Client mit dem öffentlichen Portal, das den angegebenen Hostnamen als Site-Adresse besitzt. Wenn kein öffentliches Portal den angegebenen Hostnamen als Site-Adresse besitzt, verwendet der Jump-Client die standardmäßige öffentliche Website.
--jc-session-policy-present	<session-policy-code-name>	Wenn die Überschreibung gestattet ist, legt dieser Befehlszeilenparameter die Sitzungsrichtlinie des Jump-Client fest, welche die Berechtigungsrichtlinie während einer Support-Sitzung Tech steuert, falls der Kunde an der Konsole präsent ist.
--jc-session-policy-not-present	<session-policy-code-name>	Wenn die Überschreibung gestattet ist, legt dieser Befehlszeilenparameter die Sitzungsrichtlinie des Jump-Client fest, welche die Berechtigungsrichtlinie während einer Support-Sitzung Tech steuert, falls der Kunde nicht an der Konsole präsent ist.
--jc-jump-policy	<jump-policy-code-name>	Wenn die Überschreibung gestattet ist, legt dieser Befehlszeilenparameter die Jump-Richtlinie fest, die steuert, wie Benutzer einen Jump zum Jump-Client durchführen dürfen.
--jc-max-offline-minutes	<minutes>	Die maximale Anzahl an Minuten, die ein Jump-Client offline ist, ehe er vom System gelöscht wird. Diese Einstellung überschreibt die globale Einstellung, sofern diese angegeben ist.
--jc-ephemeral		Legt die maximale Anzahl an Minuten, die ein Jump-Client offline ist, ehe er vom System gelöscht wird, auf 5 Minuten fest. Dies ist eine praktische Option, die den Jump-Client als temporär festlegt und funktionell der Angabe von **--jc-max-offline-minutes 5** entspricht.

--jc-tag	<tag-name>	Wenn die Überschreibung gestattet ist, legt dieser Befehlszeilenparameter den Tag des Jump Client fest.
--jc-comments	<comments ... >	Wenn die Überschreibung gestattet ist, legt dieser Befehlszeilenparameter die Kommentare des Jump-Client fest.
--silent		Falls angegeben, zeigt das Installationsprogramm keine Fenster, Spinner, Fehler oder andere sichtbaren Benachrichtigungen an.

Hinweis: *Bei Bereitstellung eines MSI-Installationsprogramms auf Windows über den msiexec-Befehl können die obigen Parameter wie folgt angegeben werden:*

1. *Entfernen der vorangehenden Bindestriche (--)*
2. *Umwandlung der verbleibenden Bindestriche in Unterstriche (_)*
3. *Zuweisung eines Wertes über ein Gleichheitszeichen (=)*

MSI-Beispiel:

```
msiexec /i bomgar-scc-win32.msi KEY_INFO=w0dc3056g7ff8d1j68ee6wi6dhwzfefggyezh7c40jc90
jc_jump_group=jumpgroup:server_support jc_tag=servers
```

Bei Bereitstellung eines EXE-Installationsprogramms können die obigen Parameter wie folgt angegeben werden:

- *Hinzufügen von Bindestrichen*
- *Fügen Sie anstelle eines Gleichzeichens ein Leerzeichen zwischen dem Parameter und dem Wert hinzu*

EXE-Beispiel:

```
bomgar-scc-[unique id].exe --jc-jump-group jumpgroup:servers --jc-tag servers
```

Andere zu berücksichtigende Regeln:

- ***installdir*** *verfügt über einen Bindestrich in der EXE-Version, nicht aber in der MSI-Version.*
- ***/quiet*** *wird in der MSI-Version anstelle von* ***--silent*** *der EXE-Version verwendet.*

Weitere Informationen finden Sie in Stapelbereitstellung von BeyondTrust-Software auf Macs auf https://www.beyondtrust.com/docs/remote-support/how-to/mass-deploy-mac/index.htm/docs//how-to/mass-deploy-mac/index.htm.

Client jetzt herunterladen oder installieren

Plattform

Wählen Sie das Betriebssystem, auf dem Sie diese Software installieren möchten. Standardmäßig wird in diesem Dropdown-Menü das geeignete Installationsprogramm für Ihr Betriebssystem erkannt.

> ***Hinweis:*** *Im Gegensatz zur Konsole d. Support-Technikers führen über MSI installierte Jump-Clients automatische Aktualisierungen durch.*

> ***Hinweis:*** *Um einen Jump-Client im Servicemodus auf einem Linux-System zu installieren, muss das Jump-Client-Installationsprogramm vom Root ausgeführt werden, der Jump-Client-Service sollte jedoch nicht im Root-Benutzerkontext ausgeführt werden. Ein Jump-Client im Servicemodus ermöglicht es dem Benutzer, auch dann eine Sitzung zu starten, wenn kein Benutzer angemeldet ist. Außerdem kann er den aktuellen Benutzer abmelden und sich mit anderen Anmeldedaten anmelden. Ein im Benutzermodus auf Linux installierter Jump-Client kann nicht innerhalb einer Sitzung heraufgesetzt werden.*

Verwenden Sie folgende Syntax, um der Datei ausführbare Berechtigungen hinzuzufügen. Dabei ist **{uid}** eine eindeutige Kennung, die aus Buchstaben und Zahlen besteht:

1. Fügen Sie der Datei ausführbare Berechtigungen hinzu:

   ```
   sudo chmod +x ./Downloads/bomgar-scc-[uid].desktop
   ```

2. Führen Sie das Installationsprogramm mit dem Befehl **sudo** als Root-Benutzer aus:

   ```
   sudo sh ./Downloads/bomgar-scc-[uid].desktop
   ```

Herunterladen/Installieren

Sie können das Installationsprogramm sofort herunterladen, wenn Sie vorhaben, dieses über ein Systemverwaltungs-Tool zu verteilen, oder wenn Sie sich am Computer befinden, auf den Sie später zugreifen müssen.

> ***Hinweis:*** *Sobald das Installationsprogramm ausgeführt wurde, versucht der Jump-Client, sich mit dem B Series Appliance zu verbinden. Falls erfolgreich, erscheint der Jump-Client in der Jump-Schnittstelle der Konsole d. Support-Technikers. Wenn der Jump-Client das B Series Appliance nicht sofort erreichen kann, wird der Verbindungsaufbau erneut versucht, bis dieser erfolgreich ist. Wenn der Verbindungsaufbau innerhalb der unter* ***Dieses Installationsprogramm gilt für*** *festgelegten Zeit nicht erfolgreich ist, wird der Jump-Client vom Remote-System deinstalliert und muss erneut bereitgestellt werden.*

Für E-Mail-Empfänger bereitstellen

E-Mail

Sie können das Installationsprogramm auch per E-Mail an einen oder mehrere Remote-Benutzer senden. Mehrere Empfänger können den Client über den gleichen Link installieren. Klicken Sie auf den **Direkter Download-Link**, um den Link zu kopieren.

> *Weitere Informationen zum Stapelbereitstellungsassistenten finden Sie in Bereitstellen von Jump-Clients während einer Support-Sitzung Tech. oder vor dem Support unter https://www.beyondtrust.com/docs/remote-support/how-to/jump-clients/deploying.htm.*

Jump-Client-Statistiken

Ein Administrator kann auf Website-Basis wählen, welche Statistiken für alle Jump-Clients angezeigt werden. Diese Statistiken werden in der Konsole d. Support-Technikers angezeigt und umfassen Angaben zu CPU, Konsolenbenutzer, Festplattennutzung, Betriebssystem, eine Miniaturansicht des Remote-Systems und die Betriebszeit.

Aktualisierungsintervall für die Statistiken des aktiven Jump-Client

Das **Statistikaktualisierungsintervall für den aktiven Jump-Client** legt fest, wie oft diese Statistiken aktualisiert werden. Indem Sie festlegen, welche Statistiken wie oft angezeigt werden, können Sie die verbrauchte Bandbreite beeinflussen. Je mehr aktive Jump-Clients Sie bereitgestellt haben, desto weniger Statistiken liegen vor und desto länger muss das Intervall unter Umständen sein.

Upgrade

Maximale Bandbreite für gleichzeitige Upgrades für Jump-Clients

Sie können die Bandbreitennutzung steuern, indem Sie die Option **Maximale Bandbreite für gleichzeitige Jump-Client-Aktualisierungen** festlegen. Die maximale Upgrade-Bandbreite beträgt 100 MiB/s.

> ***Hinweis:*** *Diese Einstellung hat keine Auswirkung auf Konsole d. Support-Technikers-Upgrades oder Support-Button-Bereitstellungen.*

Maximale Anzahl an gleichzeitigen Upgrades für Jump-Clients

Legen Sie die maximale Anzahl der Jump Clients fest, die gleichzeitig aktualisiert werden sollen. Bitte beachten: Wenn Sie viele Jump Clients bereitgestellt haben, müssen Sie diese Zahl unter Umständen begrenzen, um die verbrauchte Bandbreite zu steuern. Die maximal zulässige Anzahl ist 500.

> ***Hinweis:*** *Diese Einstellung hat keine Auswirkung auf Konsole d. Support-Technikers-Upgrades oder Support-Button-Bereitstellungen.*

Automatische Jump-Client-Upgrades

Verwenden Sie die folgenden Auswahlknöpfe, um automatische Upgrades für Jump-Client zu steuern. Sie können:

- Jump-Client-Upgrades dauerhaft deaktivieren.
- Jump-Client-Upgrades für den aktuellen Upgrade-Zyklus temporär aktivieren.
- Jump-Client-Upgrades dauerhaft aktivieren.

> ***Hinweis:*** *Um Jump-Clients in Web-Konsole des Support-Technikers manuell aktualisieren zu können, müssen Sie zunächst die automatischen Jump Client-Aktualisierungen deaktivieren.*

Wartung

Anzahl der Tage, bevor Jump-Clients, die sich nicht verbunden haben, automatisch gelöscht werden

Geht ein Jump-Client offline und verbindet sich für die unter **Anzahl der Tage, bevor Jump-Clients, die sich nicht verbunden haben, automatisch gelöscht werden** angegebene Anzahl von Tagen nicht mit dem B Series Appliance, wird er automatisch vom Zielcomputer deinstalliert und von der Jump-Schnittstelle der Konsole d. Support-Technikers entfernt.

Hinweis: *Diese Einstellung wird im normalen Betrieb an den Jump-Client selbst weitergegeben, sodass dieser sich selbst bei keiner Kommunikation mit der Seite nach der konfigurierten Zeit deinstalliert. Wird diese Einstellung geändert, nachdem der Jump-Client die Verbindung zum B Series Appliance trennt, deinstalliert er sich zum vorher konfigurierten Zeitpunkt.*

Hinweis: *Die Einstellung muss für 15 Tage oder länger konfiguriert sein.*

Anzahl der Tage, bevor Jump-Clients, die sich nicht verbunden haben, als verloren gelten

Geht ein Jump Client offline und verbindet er sich für die unter **Anzahl der Tage, bevor Jump Clients, die sich nicht verbunden haben, als verloren gelten** angegebene Anzahl von Tagen nicht mit dem B Series Appliance, wird er in der Konsole d. Support-Technikers als verloren markiert. Es wird keine weitere Maßnahme bezüglich des Jump-Clients ergriffen. Er wird nur zu Identifikationszwecken als verloren gekennzeichnet, sodass ein Administrator den Grund für die verlorene Verbindung bestimmen und Maßnahmen ergreifen kann, um das Problem zu lösen.

Hinweis: *Damit Sie verlorene Jump-Clients identifizieren können, bevor sie automatisch gelöscht werden, stellen Sie dieses Feld auf eine kleinere Zahl als das obige Löschfeld.*

Hinweis: *Die Einstellung muss für 15 Tage oder länger konfiguriert sein.*

Tipp: *Sie können Jump-Clients über den Bereich **Jump > Jump-Elemente > Jump-Einstellungen** darauf konfigurieren, gleichzeitige Jumps zuzulassen oder abzulehnen. Die Zulassung bietet eine Möglichkeit, mit der mehrere Benutzer gleichzeitig auf den gleichen Jump-Client zugreifen können, ohne von einem anderen Benutzer zur Teilnahme an einer aktiven Sitzung eingeladen werden zu müssen. Wird dies nicht zugelassen, kann nur ein Benutzer gleichzeitig einen Jump zu einem Jump-Client durchführen. Nur eine Einladung durch den Benutzer, der die Sitzung erstellt hat, ermöglicht es einem weiteren Benutzer, auf die Sitzung zuzugreifen.*

Weitere Informationen finden Sie in Jump-Client-Einstellungen verwalten auf https://www.beyondtrust.com/docs/remote-support/how-to/jump-clients/settings.htm.

Verhalten des deinstallierten Jump-Client

Verhalten des deinstallierten Jump-Client legt fest, wie ein von einem Endbenutzer gelöschter Jump-Client von der Konsole d. Support-Technikers behandelt wird. Abhängig von der gewählten Dropdown-Option kann das gelöschte Element entweder als deinstalliert markiert und in der Liste beibehalten oder vollständig von der Liste der Jump-Elemente in der Konsole d. Support-Technikers gelöscht werden. Wenn der Jump-Client das B Series Appliance zum Deinstallationszeitpunkt nicht kontaktieren kann, verbleibt das betroffene Element im Offline-Zustand.

Lokale Deinstallation/Deaktivierung von Jump-Clients einschränken

Lokale Deinstallation/Deaktivierung von Jump-Clients beschränken beschränkt die Fähigkeit des Remote-Benutzers, über das Rechtsklick-Kontextmenü Jump-Clients zu deinstallieren oder zu deaktivieren, wodurch Jump-Clients, die nicht deinstalliert werden sollten, nicht so oft neu installiert werden müssen. Ist diese Option aktiviert, können nur Benutzer mit den jeweiligen Berechtigungen auf dem Zielsystem den Jump-Client über die *Programmdeinstallation* des Hostsystems deinstallieren.

Sonstiges

Standardverbindungstyp für Jump-Client

Mit **Standardverbindungstyp für Jump-Client** können Sie festlegen, ob während einer vom Kunden initiierten Sitzung fixierte Jump-Clients standardmäßig aktiv oder passiv sein sollen.

Port für passive Jump-Clients

Der **Port für passive Jump-Clients** gibt an, welcher Port von einem Jump-Client verwendet wird, um einen *Aufweck*-Befehl vom B Series Appliance zu erhalten. Der Standard-Port ist 5832. Stellen Sie sicher, dass die Firewall-Einstellungen für Ihre Hosts eingehenden Verkehr für passive Jump-Clients auf diesem Port gestatten. Sobald Sie aufgeweckt wurden, verbinden sich Jump-Clients stets mit dem B Series Appliance auf Port 80 oder 443 (ausgehend).

Support-Technikern gestatten, das Aufwecken von Jump-Clients zu versuchen

Support-Technikern gestatten, das Aufwecken von Jump-Clients zu versuchen ermöglicht es, einen ausgewählten Jump-Client durch die Übertragung von Wake-on-LAN-Paketen (WOL) über einen anderen Jump-Client desselben Netzwerks aufzuwecken. Wenn ein WOL versucht wird, bleibt die Option 30 Sekunden lang nicht verfügbar, bis ein weiterer Versuch durchgeführt werden kann. WOL muss auf dem Zielcomputer und seinem Netzwerk aktiviert sein, damit dies funktioniert. Die Standard-Gateway-Informationen des Jump-Client werden verwendet, um zu bestimmen, ob sich andere Jump-Clients im gleichen Netzwerk befinden. Beim Senden eines WOL-Pakets verfügt der Benutzer über eine weitere Option zur Angabe eines Passworts für WOL-Umgebungen, welche ein sicheres WOL-Passwort erfordern.

Bildschirmstatus verwenden, um Kundenpräsenz zu erkennen

Bildschirmstatus verwenden, um Kundenpräsenz zu erkennen legt fest, wie die Kundenpräsenz bestimmt wird. Die Kundenpräsenz wird verwendet, um zu bestimmen, ob die Sitzungsrichtlinie für präsente Kunden oder die Sitzungsrichtlinie für nicht präsente Kunden verwendet wird. Falls aktiviert, gilt ein Kunde nur als präsent, wenn ein Benutzer angemeldet ist, das System nicht gesperrt ist und kein Bildschirmschoner läuft. Falls deaktiviert, gilt ein Kunde als präsent, wenn ein Benutzer angemeldet ist, unabhängig vom Bildschirmstatus.

Globale Verbindungsrate für Jump-Clients

Die globale Verbindungsrate für Jump-Clients bestimmt die maximale Rate pro Sekunde, mit der sich Jump-Clients während eines Upgrades oder nach einem größeren Netzwerkausfall zur gleichen Zeit mit dem B Series Appliance verbinden können. Die Standardeinstellung ist 50 Verbindungen; maximal zulässig sind 300.

Starten von Ad-hoc-Sitzungen auf bestehenden Jump-Clients erlauben

Wenn diese Option ausgewählt ist und bereits ein Jump-Client auf dem System des Benutzers installiert ist, wird eine heraufgesetzte Sitzung vom bestehenden Jump-Client gestartet. Dies trifft sowohl auf die Portal- als auch auf die Sitzungserstellungs-API zu.

Hinweis: *Damit die heraufgesetzte Sitzung startet, muss eine ähnliche Berechtigung für jedes öffentliche Portal gewährt werden. Siehe auch* *„Es wurde versucht, Sitzungen von installierten Jump-Clients zu starten“ auf Seite 195**.*

Jump-Gruppen: Konfiguration, welche Support-Techniker auf welche Jump-Elemente zugreifen können

Jump-Gruppen

Eine Jump-Gruppe ist ein Weg, Jump-Elemente zu organisieren und Mitgliedern unterschiedliche Zugriffsstufen für diese Elemente zu gewähren. Benutzer werden über diese Seite oder über **Benutzer und Sicherheit > Gruppenrichtlinien** zu Jump-Gruppen zugewiesen.

Neue Jump-Gruppe hinzufügen, bearbeiten, löschen

Erstellen Sie eine neue Gruppe, bearbeiten Sie eine bestehende Gruppe oder entfernen Sie eine bestehende Gruppe.

Jump-Gruppen durchsuchen

Um schnell eine vorhandene Gruppe in der Liste der **Jump-Gruppen** zu suchen, geben Sie den Namen ganz oder teilweise oder einen Begriff aus den Kommentaren ein. Auf der Liste werden alle Gruppen mit einem Namen oder Kommentar gefiltert, die den eingegebenen Suchbegriff enthalten. Die Liste wird so lange mit gefilterten Einträgen angezeigt, bis der Suchbegriff entfernt wird, selbst wenn der Benutzer andere Seiten aufruft oder sich abmeldet. Um den Suchbegriff zu entfernen, klicken Sie auf das **X** zur Rechten des Suchfeldes.

Hinzufügen oder bearbeiten einer Gruppe

Name

Erstellen Sie einen eindeutigen Namen, um diese Gruppe leichter zu identifizieren. Dieser Name hilft beim Hinzufügen von Jump-Elementen zu einer Gruppe und beim Bestimmen, welche Benutzer, und Gruppenrichtlinien Mitglieder einer Jump-Gruppe sind.

Codename

Legen Sie einen Codenamen zu Integrationszwecken fest. Wenn Sie keinen Codenamen festlegen, wird automatisch einer erstellt.

Kommentare

Fügen Sie eine kurze Beschreibung hinzu, um den Zweck dieser Jump-Gruppe zusammenzufassen.

Gruppenrichtlinien

Dies zeigt eine Liste der Gruppenrichtlinien an, die Benutzer dieser Jump-Gruppe zuweisen.

Zugelassene Benutzer

Suchen Sie nach Benutzern, die dieser Jump-Gruppe hinzugefügt werden sollen. Sie können die **Neue Mitgliedsrolle** jedes Benutzers festlegen, um seine Berechtigungen für Jump-Elemente in dieser Jump-Gruppe festzulegen. Alternativ können Sie die standardmäßigen Jump-Element-Rollen des Benutzers oder die auf der Seite **Benutzer und Sicherheit > Gruppenrichtlinien** oder **Benutzer und Sicherheit > Benutzer** festgelegten standardmäßigen Jump-Element-Rollen verwenden. Eine Jump-Element-Rolle ist ein vordefinierter Berechtigungssatz zur Verwaltung und Nutzung von Jump-Elementen.

Bestehende Jump-Gruppen-Benutzer werden in einer Tabelle angezeigt, zusammen mit der ihnen zugewiesenen Rolle und den Informationen, wie diese Rolle gewährt wurde. Sie können die Ansicht filtern, indem Sie eine Zeichenfolge in das Feld **Nach Namen filtern** eingeben. Außerdem können Sie die Einstellungen eines Benutzers bearbeiten oder den Benutzer aus der Jump-Gruppe entfernen.

Um Benutzergruppen zu einer Jump-Gruppe hinzuzufügen, navigieren Sie zu **Benutzer und Sicherheit > Gruppenrichtlinien** und weisen Sie diese Gruppe einer oder mehreren Jump-Gruppen zu.

Hinweis: *Die Bearbeitungs- und Löschfunktion kann für einige Benutzer deaktiviert sein. Diese geschieht entweder, wenn ein Benutzer über eine Gruppenrichtlinie hinzugefügt wird oder wenn die Jump-Element-Rolle eines Systembenutzers auf eine andere Option als* ***Kein Zugriff*** *eingestellt ist.*

Sie können auf den Gruppenrichtlinien-Link klicken, um die Richtlinie als Ganzes zu modifizieren. Jegliche Änderungen an der Gruppenrichtlinie werden auf alle Mitglieder dieser Gruppenrichtlinie angewandt.

Sie können auf den Benutzerlink klicken, um die Jump-Element-Rolle dieses Systembenutzers zu modifizieren. Jegliche Änderungen an der Jump-Element-Rolle des Systembenutzers werden auf alle anderen Jump-Gruppen angewandt, in denen der Benutzer ein nicht zugewiesenes Mitglied ist.

Ebenfalls können Sie die Person zur Gruppe hinzufügen und die andernorts definierten Einstellungen übersteuern.

Weitere Informationen finden Sie in Verwenden von Jump-Gruppen, um festzulegen, welche Benutzer auf welche Jump-Elemente zugreifen können unter https://www.beyondtrust.com/docs/remote-support/how-to/jumpoint/jump-groups.htm.

Jump-Richtlinien: Einrichten von Zeitplänen für Jump-Clients

Jump | JUMP-RICHTLINIEN

Jump-Richtlinien

Jump-Richtlinien werden verwendet, um mithilfe von Zeitplänen zu steuern, wann auf bestimmte Jump Elemente zugegriffen werden kann.

Weitere Informationen zum Erstellen und Verwenden von Jump-Richtlinien finden Sie unter Erstellen von Jump-Richtlinien für Jump-Elemente auf https://www.beyondtrust.com/docs/remote-support/how-to/jumpoint/policies.htm.

Hinzufügen, Bearbeiten, Löschen

Erstellen Sie eine neue Richtlinie, bearbeiten Sie eine bestehende Richtlinie oder entfernen Sie eine bestehende Richtlinie.

Richtlinie hinzufügen oder bearbeiten

Anzeigename

Erstellen Sie einen eindeutigen Namen, um diese Richtlinie leichter zu identifizieren. Dieser Name sollte Benutzern dabei helfen, diese Richtlinie bei der Zuweisung an Jump-Clients zu identifizieren.

Codename

Legen Sie einen Codenamen zu Integrationszwecken fest. Wenn Sie keinen Codenamen festlegen, wird automatisch einer erstellt.

Beschreibung

Fügen Sie eine kurze Beschreibung hinzu, um den Zweck dieser Richtlinie zusammenzufassen.

Jump-Zeitplan: Aktiviert

Legen Sie einen Zeitplan fest, der definiert, wann auf Jump-Elemente unter dieser Richtlinie zugegriffen werden kann. Legen Sie die Zeitzone fest, die für diesen Zeitplan verwendet werden soll, und fügen Sie dann einen oder mehrere Zeitplaneinträge hinzu. Geben Sie für jeden Eintrag das Startdatum und die Startuhrzeit an sowie das Enddatum und die Enduhrzeit.

Wenn die Zeit beispielsweise auf 8 Uhr (Start) und 17 Uhr (Ende) festgelegt wird, kann ein Support-Techniker jederzeit innerhalb dieses Zeitfensters eine Sitzung über ein Jump-Element starten und auch nach dem festgelegten Endzeitpunkt weiterarbeiten. Wenn jedoch nach 17 Uhr versucht wird, auf dieses Jump-Element zuzugreifen, erscheint eine Meldung, dass der Zeitplan einen Sitzungsstart verhindert. Falls nötig, kann der Benutzer die Zeitplaneinschränkung übergehen und die Sitzung dennoch starten.

Sitzungsende erzwingen, wenn der Zeitplan keinen Zugriff gestattet

Wenn eine strengere Zugriffskontrolle erforderlich ist, aktivieren Sie **Sitzungsende erzwingen, wenn der Zeitplan keinen Zugriff gestattet**. Damit wird die Sitzung gezwungen, zum geplanten Endzeitpunkt die Verbindung zu trennen. Iin diesem Fall erhält der Benutzer 15 Minuten vor der Trennung der Verbindung wiederholte Benachrichtigungen.

Jump-Element-Rollen: Konfigurieren von Berechtigungssätzen für Jump-Elemente

Jump | JUMP-ELEMENT-ROLLEN

Jump-Element-Rollen

Eine Jump-Element-Rolle ist ein vordefinierter Berechtigungssatz zur Verwaltung und Nutzung von Jump-Elementen. Jump-Element-Rollen werden auf Benutzer entweder über die Seite **Jump > Jump-Element-Rollen** oder über die Seite **Benutzer und Sicherheit > Gruppenrichtlinien** angewandt.

Wenn einem Benutzer mehr als eine Rolle zugewiesen ist, wird stets die spezifischste Rolle für einen Benutzer verwendet. Die Spezifizitätsreihenfolge für Jump-Element-Rollen in absteigender Reihenfolge lautet:

- Die auf der Seite **Jump > Jump-Element-Rollen** einer Beziehung zwischen einem Benutzer und einer Jump-Gruppe zugeordnete Rolle
- Die auf der Seite **Benutzer und Sicherheit > Gruppenrichtlinien** einer Beziehung zwischen einem Benutzer und einer Jump-Gruppe zugeordnete Rolle
- Die für einen Benutzer auf der Seite **Benutzer und Sicherheit > Benutzer** oder **Benutzer und Sicherheit > Gruppenrichtlinien** konfigurierten **Jump-Element-Rollen**

> ***Hinweis:*** *Eine neue **Jump-Item-Rolle** mit dem Namen **Auditor** wird automatisch bei neuen Standortinstallationen erstellt. Bei bestehenden Installationen muss sie erstellt werden. Bei dieser Rolle ist nur eine einzige Berechtigung **Berichte anzeigen** aktiviert, sodass Administratoren einem Benutzer nur die Berechtigung zum Ausführen von Jump-Item-Berichten erteilen können, ohne eine andere Berechtigung erteilen zu müssen.*

Neue Jump-Element-Rolle hinzufügen, bearbeiten, löschen

Erstellen Sie eine neue Rolle, bearbeiten Sie eine bestehende Rolle oder entfernen Sie eine bestehende Rolle.

Jump-Element-Rolle hinzufügen oder bearbeiten

Name

Erstellen Sie einen eindeutigen Namen, um diese Rolle einfacher zu identifizieren. Dieser Name hilft bei der Verknüpfung einer Jump-Element-Rolle mit einem Benutzer oder einer Gruppe von Benutzern in einer Jump-Gruppe.

Beschreibung

Fügen Sie eine kurze Beschreibung hinzu, um den Zweck dieser Rolle zusammenzufassen.

Berechtigungen

Jump-Gruppe oder persönliche Jump-Elemente

Neue Jump-Elemente erstellen und bereitstellen

Ermöglicht es dem Benutzer, Jump-Elemente zu erstellen und sie auf Remote-Systemen zu installieren.

Jump-Elemente verschieben und kopieren

Ermöglicht dem Benutzer das Verschieben oder Kopieren von Jump-Elementen von einer Jump-Gruppe in eine andere. Diese Berechtigung muss in beiden Jump-Gruppen aktiviert werden. Kopierte Jump-Elemente können bearbeitet werden.

> *Weitere Informationen dazu, wie Jump-Elemente kopiert werden, finden Sie in Jump-Elemente: Verwenden von Jump-Elementen zum Bereitstellen von Support für Remote-Systeme auf https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/jump-interface.htm.*

Bestehende Jump-Elemente entfernen

Ermöglicht es dem Benutzer, Jump-Elemente zu löschen.

Jump-Item

Sitzungen starten

Ermöglicht es dem Benutzer, Jumps zu Remote-Systemen durchzuführen.

Tag bearbeiten

Ermöglicht es dem Benutzer, das Tag-Feld eines Jump-Elements zu bearbeiten.

Kommentare bearbeiten

Ermöglicht es dem Benutzer, das Kommentarfeld eines Jump-Elements zu bearbeiten.

Öffentliches Portal bearbeiten

Ermöglicht es dem Benutzer, das öffentliche Portal festzulegen, dem ein Jump-Element zugeordnet ist.

Jump-Richtlinie bearbeiten

Ermöglicht es dem Benutzer, festzulegen, welche Jump-Richtlinie auf ein Jump-Element angewandt wird.

Sitzungsrichtlinie bearbeiten

Ermöglicht es dem Benutzer, festzulegen, welche Sitzungsrichtlinie ein Jump-Element verwenden soll. Das Ändern der Sitzungsrichtlinie kann sich auf die in der Sitzung gestatteten Berechtigungen auswirken.

Konnektivität und Authentifizierung bearbeiten

Ermöglicht es dem Benutzer, die Verbindungs- und Authentifizierungsinformationen eines Jump-Elements zu modifizieren. Dazu gehören u. a. Felder wie Hostname, Jumpoint, Port und Benutzername.

Verhalten und Erfahrung bearbeiten

Ermöglicht es dem Benutzer, das Verhalten von Jump-Elementen zu modifizieren. Dazu gehören u. a. Felder wie Verbindungstyp, Anzeigegröße und Terminaltyp.

Nur Jump-Clients

Kennwörter festlegen

Damit kann der Benutzer Jump-Clients durch Kennwörter schützen.

Kennwörter umgehen

Damit kann der Benutzer auf passwortgeschützte Jump-Clients zugreifen, ohne das Passwort kennen zu müssen.

> *Weitere Informationen finden Sie unter Verwenden von Jump-Element-Rollen, um Berechtigungen für Jump-Elemente zu erstellen auf https://www.beyondtrust.com/docs/remote-support/how-to/jumpoint/jump-item-roles.htm.*

Jumpoint: Einrichten des unüberwachten Zugriffs auf ein Netzwerk

Jump | JUMPOINT

Jumpoint-Verwaltung

Die Jump-Technologie von BeyondTrust ermöglicht es einem Benutzer, auf Computer in einem Remote-Netzwerk zuzugreifen, ohne auf jedem System Software vorinstallieren zu müssen. Installieren Sie einfach einen Jumpoint-Agent an einem beliebigen Punkt im Netzwerk, um unüberwachten Zugriff auf jeden PC in diesem Netzwerk zu erhalten.

Neuen Jumpoint hinzufügen, bearbeiten, löschen

Erstellen Sie einen neuen Jumpoint, bearbeiten Sie einen bestehenden Jumpoint oder entfernen Sie einen bestehenden Jumpoint.

Erneut bereitstellen

Deinstallieren Sie einen bestehenden Jumpoint und laden Sie ein Installationsprogramm herunter, um den bestehenden Jumpoint durch einen neuen zu ersetzen. Symbolische Jump-Links, die mit dem bestehenden Jumpoint verknüpft sind, verwenden nach der Installation den neuen Jumpoint.

> ***Hinweis:*** *Wenn ein bestehender Jumpoint ersetzt wird, wird seine Konfiguration nicht gespeichert. Der neue Jumpoint muss erneut konfiguriert werden.*

Netzwerksuche aktivieren

Am unteren Ende der **Jumpoint**-Seite befindet sich die Option **Netzwerksuche aktivieren**. Falls aktiviert, können berechtigte Benutzer Systeme aus der Verzeichnisstruktur des Netzwerks anzeigen und auswählen. Falls deaktiviert, können Benutzer nur dann über Jumpoint auf ein System zugreifen, wenn sie den Hostnamen oder die IP-Adresse des Systems eingeben. In beiden Fällen muss der Benutzer die gültigen Anmeldedaten für das Remote-System eingeben, bevor er Zugriff erhält.

Jumpoints hinzufügen oder bearbeiten

Name

Erstellen Sie einen eindeutigen Namen, um diesen Jumpoint leichter zu identifizieren. Dieser Name sollte Benutzern beim Auffinden dieses Jumpoints helfen, wenn sie eine Sitzung mit einem Computer am gleichen Netzwerk starten müssen.

Codename

Legen Sie einen Codenamen zu Integrationszwecken fest. Wenn Sie keinen Codenamen festlegen, wird automatisch einer erstellt.

Kommentare

Fügen Sie Kommentare hinzu, die den Zweck dieses Jumpoint identifizieren.

Deaktiviert

Falls aktiviert, steht dieser Jumpoint nicht für Jump-Verbindungen zur Verfügung.

Geclustert

Falls aktiviert, können Sie mehrere redundante Knoten des gleichen Jumpoints auf unterschiedlichen Host-Systemen hinzufügen. Damit wird sichergestellt, dass der Jumpoint verfügbar ist, solange mindestens ein Knoten online bleibt.

Shell Jump-Methode aktivieren

Wenn Benutzer in der Lage sein sollen, sich über diesen Jumpoint mit SSH- und Telnet-fähigen Netzwerkgeräten zu verbinden, wählen Sie **Shell Jump-Methode aktivieren**.

Gruppenrichtlinien

Dies zeigt eine Liste der Gruppenrichtlinien an, die Benutzern Zugriff auf diesen Jumpoint gewähren.

Zugelassene Benutzer

Neuer Mitgliedsname

Suchen Sie nach Benutzern, die diesem Jumpoint hinzugefügt werden sollen. Benutzer, die diesen Jumpoint benutzen dürfen, können darüber Sitzungen mit Jump-Elementen starten und/oder Jump-Elemente erstellen, wenn sie die entsprechenden Berechtigungen besitzen.

In der untenstehenden Tabelle können Sie bestehende Jumpoint-Benutzer anzeigen. Sie können die Ansicht filtern, indem Sie eine Zeichenfolge in das Feld **Nach Namen filtern** eingeben. Außerdem können Sie einen Benutzer vom Jumpoint entfernen.

Um Benutzergruppen zu einem Jumpoint hinzuzufügen, navigieren Sie zu **Benutzer und Sicherheit > Gruppenrichtlinien** und weisen Sie diese Gruppe einem oder mehreren Jumpoints zu.

Hinweis: *Möglicherweise sehen Sie einige Benutzer, für die die Option **Löschen** deaktiviert ist. Dies tritt auf, wenn ein Benutzer über eine Gruppenrichtlinie hinzugefügt wird.*

Sie können auf den Gruppenrichtlinien-Link klicken, um die Richtlinie als Ganzes zu modifizieren. Jegliche Änderungen an der Gruppenrichtlinie werden auf alle Mitglieder dieser Richtlinie angewandt.

Ebenfalls können Sie den Benutzer zum Jumpoint hinzufügen und die andernorts definierten Einstellungen übersteuern.

Weitere Informationen finden Sie in Konfigurieren und Installieren eines Jumpoints auf https://www.beyondtrust.com/docs/remote-support/how-to/jumpoint/installation-windows.htm.

Jump-Elemente: Importieren von symbolischen Links zu Jump-Elementen

Jump | JUMP-ITEMS

Massenimportassistent für symbolische Jump-Links

Erstellen Sie symbolische Jump-Links zum Starten von Standard-Support-Sitzungen, zum Starten von Remote-Desktop-Protokoll-Sitzungen oder VNC-Sitzungen, für Shell Jumps zu SSH- oder Telnet-fähigen Netzwerkgeräten oder zum Starten von Intel® vPro-Sitzungen.

Hinweis: *Linux-Jumpoints können nur für RDP-, SSH/Telnet- und VNC-Sitzungen verwendet werden und ermöglichen die Anmeldedaten-Einfügung vom Benutzer oder Vault, sowie RemoteApp-Funktionalität und Shell Jump-Filterung. Geclusterte Jumpoints können nur neue Knoten des gleichen Betriebssystems hinzufügen. Windows- und Linux-Knoten können nicht kombiniert werden.*

Bei der Erstellung einer großen Anzahl an Jump-Verknüpfungen ist es möglicherweise einfacher, diese über ein Spreadsheet zu importieren, statt sie einzeln in der Konsole d. Support-Technikers hinzuzufügen.

Weitere Informationen finden Sie in Verwenden von symbolischen Jump-Links zu Remote-Systemen unter https://www.beyondtrust.com/docs/remote-support/how-to/jumpoint/jump-shortcuts.htm.

Laden Sie eine Vorlage für den Import symbolischer Jump-Links herunter

Wählen Sie aus der Dropdown-Liste im **Massenimportassistent für symbolische Jump-Links** die Art von Jump-Element, das Sie hinzufügen möchten und klicken Sie dann auf **Vorlage herunterladen**. Verwenden Sie den Text in der CSV-Vorlage als Spaltenkopfzeilen und fügen Sie die Informationen für jeden symbolischen Jump-Link hinzu, den Sie importieren möchten. Optionale Felder können ausgefüllt oder leer gelassen werden.

Laden Sie eine Massenimportvorlage für symbolische Jump-Links hoch

Import von symbolischen Jump-Links

Wenn Sie mit dem Ausfüllen der Vorlage fertig sind, verwenden Sie **Symbolische Jump-Links importieren**, um die CSV-Datei mit den Jump-Element-Informationen hochzuladen. Die maximale Dateigröße pro Upload ist 5 MB. Nur ein Typ von Jump-Element kann in jeder CSV-Datei enthalten sein.

Symbolischer Jump-Link (lokal) – Hilfe

Parameter	Beschreibung
Hostname	Der Hostname des Endpunktes, auf den dieses Jump-Element zugreifen soll. Diese Zeichenkette kann

Parameter	Beschreibung
	maximal 128 Zeichen lang sein.
Name	Geben Sie einen **Namen** für das Jump-Element ein. Dieser Name kennzeichnet das Element in den Sitzungsregisterkarten. Diese Zeichenkette kann maximal 128 Zeichen lang sein.
Jump-Gruppe	Der Codename der Jump-Gruppe, die diesem Jump-Element zugeordnet werden sollte. ***Hinweis:*** *Mit der Importmethode kann ein Jump-Element nicht einer persönlichen Liste von Jump-Elementen zugeordnet werden.*
Tag (optional)	Sie können Ihre Jump-Elemente durch Hinzufügen eines Tags in Kategorien organisieren. Diese Zeichenkette kann maximal 1024 Zeichen lang sein.
Kommentare (optional)	Sie können Kommentare zu Ihren Jump-Elementen hinzufügen. Diese Zeichenkette kann maximal 1024 Zeichen lang sein.
Jump-Richtlinie (optional)	Der Codename einer Jump-Richtlinie. Sie können eine Jump-Richtlinie angeben, um den Zugriff auf dieses Jump-Element zu verwalten.
Öffentliches Portal (optional)	Das öffentliche Portal, über das sich dieses Jump-Element verbinden soll.
Sitzungsrichtlinie für anwesende Kunden (optional)	Der Codename einer Sitzungsrichtlinie. Sie können eine Sitzungsrichtlinie angeben, um die für dieses Jump-Element verfügbaren Berechtigungen zu verwalten, wenn ein Kunde anwesend ist.
Sitzungsrichtlinie für nicht anwesende Kunden (optional)	Der Codename einer Sitzungsrichtlinie. Sie können eine Sitzungsrichtlinie angeben, um die für dieses Jump-Element verfügbaren Berechtigungen zu verwalten, wenn der Kunde nicht anwesend ist.

Symbolischer Jump-Link (remote) – Hilfe

Parameter	Beschreibung
Hostname	Der Hostname des Endpunktes, auf den dieses Jump-Element zugreifen soll. Diese Zeichenkette kann maximal 128 Zeichen lang sein.
Jumpoint	Der Codename des Jumpoint, über den auf den Endpunkt zugegriffen wird.
Name	Geben Sie einen **Namen** für das Jump-Element ein. Dieser Name kennzeichnet das Element in den Sitzungsregisterkarten. Diese Zeichenkette kann maximal 128 Zeichen lang sein.
Jump-Gruppe	Der Codename der Jump-Gruppe, die diesem Jump-Element zugeordnet werden sollte. ***Hinweis:*** *Mit der Importmethode kann ein Jump-Element nicht einer persönlichen Liste von Jump-Elementen zugeordnet werden.*
Tag (optional)	Sie können Ihre Jump-Elemente durch Hinzufügen eines Tags in Kategorien organisieren. Diese Zeichenkette kann maximal 1024 Zeichen lang sein.

Parameter	Beschreibung
Kommentare (optional)	Sie können Kommentare zu Ihren Jump-Elementen hinzufügen. Diese Zeichenkette kann maximal 1024 Zeichen lang sein.
Jump-Richtlinie (optional)	Der Codename einer Jump-Richtlinie. Sie können eine Jump-Richtlinie angeben, um den Zugriff auf dieses Jump-Element zu verwalten.
Öffentliches Portal (optional)	Das öffentliche Portal, über das sich dieses Jump-Element verbinden soll.
Sitzungsrichtlinie für anwesende Kunden (optional)	Der Codename einer Sitzungsrichtlinie. Sie können eine Sitzungsrichtlinie angeben, um die für dieses Jump-Element verfügbaren Berechtigungen zu verwalten, wenn ein Kunde anwesend ist.
Sitzungsrichtlinie für nicht anwesende Kunden (optional)	Der Codename einer Sitzungsrichtlinie. Sie können eine Sitzungsrichtlinie angeben, um die für dieses Jump-Element verfügbaren Berechtigungen zu verwalten, wenn der Kunde nicht anwesend ist.

Symbolischer VNC-Jump-Link (lokal) – Hilfe

Parameter	Beschreibung
Hostname	Der Hostname des Endpunktes, auf den dieses Jump-Element zugreifen soll. Diese Zeichenkette kann maximal 128 Zeichen lang sein.
Port (optional)	Eine gültige Portnummer von **100** bis **65535**. Standardwert: **5900**.
Name	Geben Sie einen **Namen** für das Jump-Element ein. Dieser Name kennzeichnet das Element in den Sitzungsregisterkarten. Diese Zeichenkette kann maximal 128 Zeichen lang sein.
Jump-Gruppe	Der Codename der Jump-Gruppe, die diesem Jump-Element zugeordnet werden sollte. ***Hinweis:*** *Mit der Importmethode kann ein Jump-Element nicht einer persönlichen Liste von Jump-Elementen zugeordnet werden.*
Tag (optional)	Sie können Ihre Jump-Elemente durch Hinzufügen eines Tags in Kategorien organisieren. Diese Zeichenkette kann maximal 1024 Zeichen lang sein.
Kommentare (optional)	Sie können Kommentare zu Ihren Jump-Elementen hinzufügen. Diese Zeichenkette kann maximal 1024 Zeichen lang sein.
Jump-Richtlinie (optional)	Der Codename einer Jump-Richtlinie. Sie können eine Jump-Richtlinie angeben, um den Zugriff auf dieses Jump-Element zu verwalten.
Öffentliches Portal (optional)	Das öffentliche Portal, über das sich dieses Jump-Element verbinden soll.
Sitzungsrichtlinie (optional)	Der Codename einer Sitzungsrichtlinie. Sie können eine Sitzungsrichtlinie angeben, um die für dieses Jump-Element verfügbaren Berechtigungen zu verwalten.

Symbolischer VNC-Jump-Link (remote) – Hilfe

Parameter	Beschreibung
Hostname	Der Hostname des Endpunktes, auf den dieses Jump-Element zugreifen soll. Diese Zeichenkette kann maximal 128 Zeichen lang sein.
Jumpoint	Der Codename des Jumpoint, über den auf den Endpunkt zugegriffen wird.
Port (optional)	Eine gültige Portnummer von **100** bis **65535**. Standardwert: **5900**.
Name	Geben Sie einen **Namen** für das Jump-Element ein. Dieser Name kennzeichnet das Element in den Sitzungsregisterkarten. Diese Zeichenkette kann maximal 128 Zeichen lang sein.
Jump-Gruppe	Der Codename der Jump-Gruppe, die diesem Jump-Element zugeordnet werden sollte. ***Hinweis:*** *Mit der Importmethode kann ein Jump-Element nicht einer persönlichen Liste von Jump-Elementen zugeordnet werden.*
Tag (optional)	Sie können Ihre Jump-Elemente durch Hinzufügen eines Tags in Kategorien organisieren. Diese Zeichenkette kann maximal 1024 Zeichen lang sein.
Kommentare (optional)	Sie können Kommentare zu Ihren Jump-Elementen hinzufügen. Diese Zeichenkette kann maximal 1024 Zeichen lang sein.
Jump-Richtlinie (optional)	Der Codename einer Jump-Richtlinie. Sie können eine Jump-Richtlinie angeben, um den Zugriff auf dieses Jump-Element zu verwalten.
Öffentliches Portal (optional)	Das öffentliche Portal, über das sich dieses Jump-Element verbinden soll.
Sitzungsrichtlinie (optional)	Der Codename einer Sitzungsrichtlinie. Sie können eine Sitzungsrichtlinie angeben, um die für dieses Jump-Element verfügbaren Berechtigungen zu verwalten.

Symbolischer RDP-Jump-Link (remote) – Hilfe

Parameter	Beschreibung
Hostname	Der Hostname des Endpunktes, auf den dieses Jump-Element zugreifen soll. Diese Zeichenkette kann maximal 128 Zeichen lang sein.
Jumpoint	Der Codename des Jumpoint, über den auf den Endpunkt zugegriffen wird.
Benutzername (optional)	Der Benutzername, mit dem die Anmeldung erfolgen soll.
Domäne (optional)	Die Domäne, auf der sich der Endpunkt befindet.
Qualität (optional)	Die Qualität, in der das Remote-System angezeigt werden soll. Mögliche Optionen: **Niedrig** (2-Bit-Grauskala für den niedrigsten Bandbreitenverbrauch), **best_perf** (8-Bit-Farben für schnelle Leistung), **perf_and_qual** (16-Bit-Farben für mittlere Bildqualität und Leistung), **best_qual** (32-Bit für die höchste Bildauflösung) oder **video_opt** (VP9-Codec für flüssigeres Video). Diese kann nicht während der Remote-Desktop-Protokoll (RDP)-Sitzung geändert werden.

Parameter	Beschreibung
Konsolensitzung (optional)	**1**: Startet eine Konsolensitzung. **0**: Startet eine neue Sitzung (Standard).
Nicht vertrauenswürdiges Zertifikat ignorieren (optional)	**1**: Ignoriert Zertifikatwarnungen. **0**: Zeigt eine Warnung, wenn das Serverzertifikat nicht verifiziert werden kann.
Name	Geben Sie einen **Namen** für das Jump-Element ein. Dieser Name kennzeichnet das Element in den Sitzungsregisterkarten. Diese Zeichenkette kann maximal 128 Zeichen lang sein.
Jump-Gruppe	Der Codename der Jump-Gruppe, die diesem Jump-Element zugeordnet werden sollte. ***Hinweis:*** *Mit der Importmethode kann ein Jump-Element nicht einer persönlichen Liste von Jump-Elementen zugeordnet werden.*
Tag (optional)	Sie können Ihre Jump-Elemente durch Hinzufügen eines Tags in Kategorien organisieren. Diese Zeichenkette kann maximal 1024 Zeichen lang sein.
Kommentare (optional)	Sie können Kommentare zu Ihren Jump-Elementen hinzufügen. Diese Zeichenkette kann maximal 1024 Zeichen lang sein.
Jump-Richtlinie (optional)	Der Codename einer Jump-Richtlinie. Sie können eine Jump-Richtlinie angeben, um den Zugriff auf dieses Jump-Element zu verwalten.
Öffentliches Portal (optional)	Das öffentliche Portal, über das sich dieses Jump-Element verbinden soll.
Sitzungsrichtlinie (optional)	Der Codename einer Sitzungsrichtlinie. Sie können eine Sitzungsrichtlinie angeben, um die für dieses Jump-Element verfügbaren Berechtigungen zu verwalten.

Symbolischer RDP-Jump-Link (lokal) – Hilfe

Parameter	Beschreibung
Hostname	Der Hostname des Endpunktes, auf den dieses Jump-Element zugreifen soll. Diese Zeichenkette kann maximal 128 Zeichen lang sein.
Benutzername (optional)	Der Benutzername, mit dem die Anmeldung erfolgen soll.
Domäne (optional)	Die Domäne, auf der sich der Endpunkt befindet.
Qualität (optional)	Die Qualität, in der das Remote-System angezeigt werden soll. Mögliche Optionen: **Niedrig** (2-Bit-Grauskala für den niedrigsten Bandbreitenverbrauch), **best_perf** (8-Bit-Farben für schnelle Leistung), **perf_and_qual** (16-Bit-Farben für mittlere Bildqualität und Leistung), **best_qual** (32-Bit für die höchste Bildauflösung) oder **video_opt** (VP9-Codec für flüssigeres Video). Diese kann nicht während der Remote-Desktop-Protokoll (RDP)-Sitzung geändert werden.
Konsolensitzung (optional)	**1**: Startet eine Konsolensitzung. **0**: Startet eine neue Sitzung (Standard).

Parameter	Beschreibung
Nicht vertrauenswürdiges Zertifikat ignorieren (optional)	**1**: Ignoriert Zertifikatwarnungen. **0**: Zeigt eine Warnung, wenn das Serverzertifikat nicht verifiziert werden kann.
Name	Geben Sie einen **Namen** für das Jump-Element ein. Dieser Name kennzeichnet das Element in den Sitzungsregisterkarten. Diese Zeichenkette kann maximal 128 Zeichen lang sein.
Jump-Gruppe	Der Codename der Jump-Gruppe, die diesem Jump-Element zugeordnet werden sollte. ***Hinweis:*** *Mit der Importmethode kann ein Jump-Element nicht einer persönlichen Liste von Jump-Elementen zugeordnet werden.*
Tag (optional)	Sie können Ihre Jump-Elemente durch Hinzufügen eines Tags in Kategorien organisieren. Diese Zeichenkette kann maximal 1024 Zeichen lang sein.
Kommentare (optional)	Sie können Kommentare zu Ihren Jump-Elementen hinzufügen. Diese Zeichenkette kann maximal 1024 Zeichen lang sein.
Jump-Richtlinie (optional)	Der Codename einer Jump-Richtlinie. Sie können eine Jump-Richtlinie angeben, um den Zugriff auf dieses Jump-Element zu verwalten.
Öffentliches Portal (optional)	Das öffentliche Portal, über das sich dieses Jump-Element verbinden soll.
Sitzungsrichtlinie (optional)	Der Codename einer Sitzungsrichtlinie. Sie können eine Sitzungsrichtlinie angeben, um die für dieses Jump-Element verfügbaren Berechtigungen zu verwalten.

Symbolischer Shell Jump-Link – Hilfe

Parameter	Beschreibung
Hostname	Der Hostname des Endpunktes, auf den dieses Jump-Element zugreifen soll. Diese Zeichenkette kann maximal 128 Zeichen lang sein.
Jumpoint	Der Codename des Jumpoint, über den auf den Endpunkt zugegriffen wird.
Benutzername (optional)	Der Benutzername, mit dem die Anmeldung erfolgen soll.
Protokoll	Entweder **SSH** oder **Telnet**.
Port (optional)	Eine gültige Portnummer von **1** bis **65535**. Standardwert ist **22** für das Protokoll **ssh** oder **23** für das Protokoll **telnet**.
Terminaltyp (optional)	Kann entweder **xterm** (Standard) oder **VT100** sein.
Keep-Alive (optional)	Die Anzahl der Sekunden zwischen jedem gesendeten Paket, um den Abbruch einer inaktiven Sitzung zu verhindern. Kann eine Zahl von **0** bis **300** sein. **0** deaktiviert die Funktion (standardmäßig eingestellt).
Name	Geben Sie einen **Namen** für das Jump-Element ein. Dieser Name kennzeichnet das Element in den Sitzungsregisterkarten. Diese Zeichenkette kann maximal 128 Zeichen lang sein.

Parameter	Beschreibung
Jump-Gruppe	Der Codename der Jump-Gruppe, die diesem Jump-Element zugeordnet werden sollte. ***Hinweis:*** *Mit der Importmethode kann ein Jump-Element nicht einer persönlichen Liste von Jump-Elementen zugeordnet werden.*
Tag (optional)	Sie können Ihre Jump-Elemente durch Hinzufügen eines Tags in Kategorien organisieren. Diese Zeichenkette kann maximal 1024 Zeichen lang sein.
Kommentare (optional)	Sie können Kommentare zu Ihren Jump-Elementen hinzufügen. Diese Zeichenkette kann maximal 1024 Zeichen lang sein.
Jump-Richtlinie (optional)	Der Codename einer Jump-Richtlinie. Sie können eine Jump-Richtlinie angeben, um den Zugriff auf dieses Jump-Element zu verwalten.
Sitzungsrichtlinie (optional)	Der Codename einer Sitzungsrichtlinie. Sie können eine Sitzungsrichtlinie angeben, um die für dieses Jump-Element verfügbaren Berechtigungen zu verwalten.
Öffentliches Portal (optional)	Das öffentliche Portal, über das sich dieses Jump-Element verbinden soll.

Symbolische Intel vPro-Links – Hilfe

Parameter	Beschreibung
Hostname	Der Hostname des Endpunktes, auf den dieses Jump-Element zugreifen soll. Diese Zeichenkette kann maximal 128 Zeichen lang sein.
Jumpoint	Der Codename des Jumpoint, über den auf den Endpunkt zugegriffen wird.
Name	Geben Sie einen **Namen** für das Jump-Element ein. Dieser Name kennzeichnet das Element in den Sitzungsregisterkarten. Diese Zeichenkette kann maximal 128 Zeichen lang sein.
Jump-Gruppe	Der Codename der Jump-Gruppe, die diesem Jump-Element zugeordnet werden sollte. ***Hinweis:*** *Mit der Importmethode kann ein Jump-Element nicht einer persönlichen Liste von Jump-Elementen zugeordnet werden.*
Tag (optional)	Sie können Ihre Jump-Elemente durch Hinzufügen eines Tags in Kategorien organisieren. Diese Zeichenkette kann maximal 1024 Zeichen lang sein.
Kommentare (optional)	Sie können Kommentare zu Ihren Jump-Elementen hinzufügen. Diese Zeichenkette kann maximal 1024 Zeichen lang sein.
Jump-Richtlinie (optional)	Der Codename einer Jump-Richtlinie. Sie können eine Jump-Richtlinie angeben, um den Zugriff auf dieses Jump-Element zu verwalten.
Öffentliches Portal (optional)	Das öffentliche Portal, über das sich dieses Jump-Element verbinden soll.

> *Weitere Informationen finden Sie in Verwenden von symbolischen Jump-Links zu Remote-Systemen unter https://www.beyondtrust.com/docs/remote-support/how-to/jumpoint/jump-shortcuts.htm.*

Jump-Element-Einstellungen

Gleichzeitige Jumps

Für Jump-Client, lokaler Jump, Remote-Jump, lokaler VNC, Remote VNC und Intel® vPro

Setzen Sie **Gleichzeitige Jumps** auf **Bestehender Sitzung beitreten**, wenn mehrere Benutzer gleichzeitig auf das gleiche Jump-Element zugreifen können sollen, ohne von einem anderen Benutzer zur Teilnahme an einer aktiven Sitzung eingeladen werden zu müssen. Der erste Benutzer, der auf das Jump-Element zugreift, wird Eigentümer der Sitzung. Benutzer in einer freigegebenen Jump-Sitzung sehen sich und können miteinander chatten.

Wählen Sie hier **Jump verbieten**, um sicherzustellen, dass nur ein Benutzer gleichzeitig einen Jump zu einem Jump-Element durchführen kann. Nur eine Einladung durch den Benutzer, der die Sitzung erstellt hat, ermöglicht es einem weiteren Benutzer, auf die Sitzung zuzugreifen.

Diese Einstellung gilt für die folgenden Jump-Element-Typen:

- Jump-Client
- Lokaler Jump
- Remote-Jump
- Lokales VNC
- VNC (Remote)
- Shell Jump
- Intel® vPro

Für Remote-RDP, Lokal-RDP

Setzen Sie **Gleichzeitige Jumps** auf **Neue Sitzung starten**, wenn mehrere Benutzer gleichzeitig auf das gleichen Jump-Element zugreifen können sollen, ohne von einem anderen Benutzer zur Teilnahme an einer aktiven Sitzung eingeladen werden zu müssen. Bei RDP können mehrere Benutzer auf ein Jump-Element zugreifen, aber jeder Zugriff startet eine unabhängige Sitzung.

Legen Sie hier **Jump verbieten** fest, um sicherzustellen, dass nur ein Benutzer gleichzeitig einen Jump zu einem Jump-Element durchführen kann. Nur eine Einladung durch den Benutzer, der die Sitzung erstellt hat, ermöglicht es einem weiteren Benutzer, auf die Sitzung zuzugreifen.

Diese Einstellung gilt nur für Jump-Elementtypen mit lokalem und Remote-RDP.

Vault für Remote Support

Discovery: Konten, Endpunkte und Dienste in einer Domain erfassen

Vault | DISCOVERY

BeyondTrust Vault ist ein auf dem B Series Appliance integrierter Anmeldedaten-Speicher, der das Erkennen und den Zugriff auf privilegierte Anmeldedaten ermöglicht. Sie können privilegierte Anmeldedaten manuell hinzufügen oder das integrierte Discovery-Tool verwenden, um Active Directory- und lokale Konten in BeyondTrust Vault einzuscannen und zu importieren.

Weitere Informationen finden Sie in Vault Guide auf https://www.beyondtrust.com/docs/remote-support/how-to/vault/index.htm.

Discovery: Windows-Domäne

Mit dem BeyondTrust Vault-Add-on können Sie Active Directory-Konten, lokale Konten, Windows-Dienstkonten und Endpunkte erfassen. Jumpoints werden verwendet, um Endpunkte einzuscannen und die mit diesen Endpunkten assoziierten Konten zu erfassen.

Klicken Sie auf **Neuer Discovery-Auftrag**, um eine neue Discovery zu initiieren. Die Optionen sind:

- **Windows-Domäne**: Ermitteln von Endpunkten, Domänenkonten und lokalen Konten, die über einen Jumpoint auf einer Windows-Domäne zugänglich sind.
- **Lokale Windows-Konten auf Jump-Clients**: Ermitteln lokaler Windows-Konten auf Rechnern, auf denen derzeit ein aktiver Jump-Client im Servicemodus online ist.

***Hinweis:** Die Option **Lokale Windows-Konten auf Jump-Clients** wird nur angezeigt, wenn Sie über die Berechtigung **Jump Clients** verfügen, die sich unter **Benutzer & Sicherheit > Benutzer > Support-Techniker-Berechtigungen > Jump-Technologie** befindet. Wenden Sie sich bei Problemen an Ihren Website-Administrator.*

Klicken Sie auf **Fortsetzen**, um den Discovery-Prozess zu starten.

Wenn Sie **Windows-Domäne** ausgewählt haben, führen Sie die Schritte im Abschnitt **Domäne hinzufügen** aus. Wenn Sie **Lokale Windows-Konten auf Jump-Clients** ausgewählt haben, führen Sie die Schritte im Abschnitt **Discovery: Jump-Client-Suchkriterien** aus.

Weitere Informationen zu Jumpoints finden Sie im BeyondTrustRemote Support Jumpoint-Handbuch unter https://www.beyondtrust.com/docs/remote-support/how-to/jumpoint/index.htm.

Domäne hinzufügen

DNS-Name der Domäne

Geben Sie den DNS-Namen Ihrer Umgebung ein.

Jumpoint

Wählen Sie einen vorhandenen Jumpoint in der Umgebung, in der Sie Konten erfassen möchten.

Verwaltungskonto

Wählen Sie das für den Start des Discovery-Auftrags erforderliche Verwaltungskonto aus. Wählen Sie die Verwendung eines neuen Kontos aus. Dafür müssen **Benutzername**, **Passwort** und **Passwortbestätigung** eingegeben werden. Andernfalls können Sie auch ein in einem vorangehenden Auftrag erfasstes oder ein im Abschnitt **Konten** manuell hinzugefügtes Konto auswählen.

Benutzername

Geben Sie einen gültigen Benutzernamen ein, der für die Discovery verwendet werden soll (nutzername@domäne).

Passwort

Geben Sie ein gültiges Passwort ein, das für die Discovery verwendet werden soll.

Passwort bestätigen

Geben Sie das Passwort zur Bestätigung erneut ein.

> ***Hinweis:*** *Sie können definieren, welche Teile einer Domäne einen* ***Discovery-/Import****-Auftrag ausführen sollen. Sobald Sie die erforderlichen Felder für einen* ***Discovery-Auftrag*** *ausgewählt haben, können Sie die Suche verfeinern, indem Sie angeben, auf welche OUs die Suche abzielen soll, oder indem Sie LDAP-Abfragen eingeben.*

Discovery-Bereich

Wählen Sie die Objekte aus, die Vault erkennen soll:

- **Domänenkonten**
- **Endpunkte**
- **Lokale Konten**
- **Dienste**

Sie können einen **Suchpfad** eingeben oder ihn leer lassen, um alle OEs und Container zu durchsuchen. Sie können auch eine **LDAP-Abfrage** verwenden, um den Umfang der gesuchten Benutzerkonten und Endpunkte einzuschränken.

Discovery: Jump-Client-Suchkriterien

Geben Sie ein oder mehrere Suchkriterien ein, um aktive Jump-Clients zu finden, die Sie zur Ermittlung lokaler Windows-Kontenverwenden möchten. Alle Textfeldsuchen sind partiell und unterscheiden nicht zwischen Groß- und Kleinschreibung. Jump-Clients, die allen Suchkriterien entsprechen, werden auf der nächsten Seite zur Auswahl vor Beginn der Discovery angezeigt.

> ***Hinweis:*** *Die folgenden Arten von Jump-Clients können nicht für die lokale Konto-Discovery verwendet werden und werden nicht in den Suchergebnissen angezeigt:*

- *Jump-Clients, die derzeit offline oder deaktiviert sind*
- *Jump-Clients, die nicht als ein erweiterter Dienst laufen*
- *Jump-Clients, die in einem Domänen-Controller installiert sind*
- *Passive Jump-Clients*

Jump-Gruppen

Administratoren können über ihre Jump-Gruppen und deren Attribute nach Jump-Clients suchen. Wenn der Benutzer kein Mitglied einer Jump-Gruppe ist, ist der Auswahlabschnitt **Jump-Gruppen** ausgegraut und es wird entweder ein Tooltip oder ein Hinweis eingeblendet, der darauf hinweist, dass der Benutzer Mitglied in mindestens einer Jump-Gruppe sein muss, um mit dem Jump-Client Discovery-Prozess fortzufahren. Dies ist vergleichbar mit der Domänen-Discovery, wenn ein Benutzer während der Discovery kein Mitglied eines Jumpoint oder beim Importieren eines Endpunkts kein Mitglied einer Jump-Gruppe ist.

Sie können **Alle von Ihnen freigegebenen Jump-Gruppen** oder **Bestimmte Jump-Gruppen** durchsuchen.

Jump-Client-Attribute

Sie können eine oder mehrere freigegebene Jump-Gruppen auswählen. Private Jump-Gruppen werden nicht unterstützt.

Es können ein oder mehrere Jump-Client-Attribute eingegeben werden. Wenn mehr als ein Suchkriterium eingegeben wird, werden nur Jump-Clients, die alle Kriterien erfüllen, für die Discovery verwendet.

Die folgenden Attribute können als Suchkriterien verwendet werden:

- **Name**: Der Name des Jump-Clients, wie er in der Spalte **Name** in der Konsole d. Support-Technikers erscheint.
- **Hostname:** Der Hostname des Jump-Clients, wie er in der Spalte **Hostname/IP** der Konsole d. Support-Technikers erscheint.
- **FQDN**: Der vollqualifizierte Domänenname des Jump-Clients, wie er unter dem **FQDN**-Label des Detailbereichs Jump-Client in der Konsole d. Support-Technikers angegeben ist.
- **Tag:** Das Tag des Jump-Clients, wie es in der Spalte **Tag** der Konsole des Support-Technikers erscheint.
- **Öffentliche/Private IP**: Die öffentlichen und privaten IP-Adressen des Jump-Clients, wie sie unter dem Label **Öffentliche IP** des Detailbereichs Jump-Client in der Konsole d. Support-Technikers angegeben sind. Jump-Clients, deren IP-Adresse mit dem angegebenen Suchwert beginnt, werden gefunden.

Klicken Sie auf **Fortsetzen**, um den Discovery-Prozess zu initiieren.

Discovery: Jump-Clients wählen

In diesem Bildschirm werden die Jump-Clients angezeigt, die bei der Discovery verwendet werden sollen. Wählen Sie einen oder mehrere aus und klicken Sie auf **Discovery starten**.

Discovery-Ergebnisse

Die Ergebnisse zeigen eine Liste der ermittelten **Endpunkte** und **lokalen Konten** an. Wählen Sie einen oder mehrere aus und klicken Sie auf **Auswahl importieren**.

Gefundene Elemente importieren

Eine Liste der von Ihnen getroffenen Auswahlen wird angezeigt.

Kontogruppe

Wählen Sie aus, aus welcher Kontengruppe Sie importieren möchten, und klicken Sie dann auf **Import starten**. Es wird eine Warnung angezeigt, die darauf hinweist, dass dieser Prozess nicht gestoppt werden kann, wenn er einmal gestartet ist. Klicken Sie auf **Ja**, um fortzufahren, oder auf **Nein**, um abzubrechen.

Importieren

Eine Meldung zeigt an, dass der Import erfolgreich abgeschlossen wurde. Eine Liste der **Endpunkte** und **lokalen Konten** wird angezeigt.

Konten

Nach Freigegebenen/Persönlichen Konten suchen

Wenn Sie eine umfangreiche Liste ermittelter Konten erhalten, verwenden Sie das Feld **Suchen**, um Konten nach **Name**, **Endpunkt** oder **Beschreibung** zu suchen (nach **Name** und **Beschreibung** nur für persönliche Konten).

Schalten Sie zwischen **freigegebenen** und **persönlichen** Konten um. Wählen Sie ein oder mehrere Konten. Klicken Sie auf **...**, um das **Passwort zu rotieren**, das Konto zu **bearbeiten** oder zu **löschen**. Sie können auch oben auf der Seite auf **Rotieren** klicken, um das Passwort für die ausgewählten Konten zu rotieren.

Discovery-Aufträge

Zeigen Sie Discovery-Aufträge an, die derzeit für eine spezifische Domäne ausgeführt werden, oder prüfen Sie die Ergebnisse erfolgreicher oder fehlgeschlagener Discovery-Aufträge.

Ergebnisse anzeigen

Klicken Sie bei einem Discovery-Auftrag auf **Ergebnisse anzeigen**, um die **Discovery-Ergebnisse** anzuzeigen. Dazu gehören erfasste Endpunkte, erfasste lokale Konten, erfasste Domänen-Konten sowie Services, die in der Domäne gefunden werden.

Anhand des Filterfelds über dem Raster können Sie die Liste der Elemente nach Attributen filtern. Klicken Sie in jedem Reiter auf das **i** neben dem Filterfeld, um anzuzeigen, nach welchen Attributen gesucht werden kann.

Sie können festlegen, welche Endpunkte, Konten und Services in Ihre BeyondTrust Vault-Instanz importiert und gespeichert werden sollen. Markieren Sie für jedes Listenelement, das Sie importieren möchten, das danebenstehende Kontrollkästchen und klicken Sie auf **Ausgewählte importieren**.

> *Weitere Informationen finden Sie in Domänen, Endpunkte und Konten mit BeyondTrust Vault erfassen auf https://www.beyondtrust.com/docs/remote-support/how-to/vault/discovery.htm/docs//how-to/vault/discovery.htm.*

Konten: Vault-Konten verwalten

Vault | KONTEN

Zeigen Sie Informationen zu allen erfassten und manuell hinzugefügten Konten an und verwalten Sie sie.

Hinweis: *Vault kann bis zu 60.000 Konten importieren, rotieren und verwalten.*

Zu den verfügbaren Informationen zu geteilten Konten gehören:

- **Typ**: Der Kontotyp, insbesondere, ob es sich um ein Domänenkonto oder ein lokales Konto oder ein generisches Passwort-Konto handelt.
- **Name**: Der Name des Kontos.
- **Benutzername**: Der mit dem Konto verknüpfte Benutzername.
- **Gruppe:** Der Name der Kontogruppe, der das Konto angehört.
- **Endpunkt**: Der Endpunkt, mit dem das Konto verknüpft ist.
- **Beschreibung**: Kurzbeschreibung zum Konto.
- **Letzter Checkout**: Das letzte Mal, an dem das Konto ausgecheckt worden ist.
- **Passwortalter**: Das Alter des Passworts.
- **Status**: Der Status des Kontos. In dieser Spalte werden z. B. Warnungen, Fehler und ob man vom Konto abgemeldet ist, angezeigt. Diese Spalte wird automatisch ausgeblendet, wenn es für keine Konten einen Status anzugeben gibt. Mehrere Statusangaben werden gestapelt und in verschiedenen Farben angezeigt. Sie können mit dem Mauszeiger über einen bestimmten Status fahren, um weitere Details zu diesem anzuzeigen.

Tipp: *Sie können die Liste der geteilten Konten, die angezeigt werden, anhand der Filter für* ***Gruppe*** *und* ***Passwortalter*** *filtern.*

Anhand dieser Informationen können Sie verschiedene Aktionen ausführen, wie beispielsweise Aus-/Einchecken von Anmeldedaten und die Anmeldedaten-Rotation.

Zu den verfügbaren Informationen über persönliche Konten gehören:

- **Typ**: Der Kontotyp, insbesondere, ob es sich um ein Domänenkonto oder ein lokales Konto oder ein generisches Passwort-Konto handelt.
- **Name**: Der Name des Kontos.
- **Eigentümer**: Der Name der Person, die das Konto erstellt hat und besitzt.
- **Beschreibung**: Kurzbeschreibung zum Konto.
- **Passwortalter**: Das Alter des Passworts.

Tipp: *Sie können die Liste der geteilten Konten, die angezeigt werden, anhand der Filter für* ***Eigentümer*** *und* ***Passwortalter*** *filtern.*

Konten

Konto hinzufügen

Klicken Sie auf **Hinzufügen**, um manuell ein geteiltes oder persönliches generisches Konto zu BeyondTrust Vault hinzuzufügen.

Freigegebene Konten durchsuchen

Suchen Sie anhand von **Name**, **Endpunkt-Name** oder **Beschreibung** nach einem bestimmten freigegebenen Konto oder einer Gruppe von Konten.

Sichtbare Spalten auswählen

Klicken Sie auf die Schaltfläche **Sichtbare Spalten auswählen** (Spaltensymbol) über dem Raster **Konten** und wählen Sie die Spalten, die im Raster angezeigt werden sollen.

Auschecken und Einchecken eines geteilten Kontos

Klicken Sie auf **Auschecken**, um die Anmeldedaten anzuzeigen und zu verwenden. Nach der entsprechenden Auswahl wird die Eingabeaufforderung **Konto-Passwort** angezeigt, und der Anmeldedaten-Satz wird für 60 Sekunden angezeigt, damit Sie das Passwort kopieren können. Sobald die Eingabeaufforderung geschlossen ist, wird die Option **Einchecken** verfügbar. Wenn Sie mit der Nutzung des Kontos fertig sind, klicken Sie auf **Einchecken**, um das Passwort wieder im System einzuchecken.

> *Weitere Informationen finden Sie in Anmeldedaten von der /login-Schnittstelle auschecken unter https://www.beyondtrust.com/docs/remote-support/how-to/vault/check-out.htm.*

Ellipsis-Menü für geteilte Konten

Klicken Sie auf **...**, um weitere Aktionen anzuzeigen, wie **Passwort rotieren**, **Bearbeiten** und **Löschen**. Wenn **Passwort rotieren** ausgewählt ist, rotiert oder ändert das System das Passwort automatisch. Wenn **Bearbeiten** ausgewählt ist, können Sie die Informationen des Kontos ändern. Über die Option **Löschen** entfernen Sie das Konto aus der Liste **Konten**.

> *Weitere Informationen finden Sie in Privilegierte Anmeldedaten mit BeyondTrust Vault rotieren auf https://www.beyondtrust.com/docs/remote-support/how-to/vault/rotation.htm.*

Persönliche Konten durchsuchen

Suchen Sie anhand von **Name** und **Beschreibung** nach einem bestimmten persönlichen Konto oder einer Gruppe von Konten.

Passwort für persönliche Konten anzeigen

Klicken Sie auf **Passwort anzeigen**, um die Anmeldedaten anzuzeigen und zu verwenden. Nach der entsprechenden Auswahl wird die Eingabeaufforderung **Konto-Passwort** angezeigt, und der Anmeldedaten-Satz wird für 60 Sekunden angezeigt, damit Sie das Passwort kopieren können.

Persönliches Konto bearbeiten

Klicken Sie auf **Konto bearbeiten**, um die Kontoinformationen zu ändern, insbesondere **Name**, **Beschreibung**, **Benutzername** und **Passwort**.

Geteiltes Konto hinzufügen

Anhand der Option **Hinzufügen > Geteiltes generisches Konto** können Sie Konten hinzufügen, ohne einen Discovery-Auftrag ausführen zu müssen. Stattdessen können Sie manuell Informationen zum Konto eingeben. Diese Option ist in Situationen nützlich, in denen ein geteiltes Konto oder eine Kombination aus Benutzername und Passwort verwendet werden kann, um auf viele verschiedene Systeme zuzugreifen.

Name

Geben Sie einen Namen für das Konto ein.

Beschreibung

Geben Sie eine knappe, aber prägnante Beschreibung für das Konto ein.

Benutzername

Geben Sie den Benutzernamen für das Konto an.

Authentifizierung

Wählen Sie die Authentifizierungsmethode für das Konto aus: **Kennwort**, **privater SSH-Schlüssel** oder **privater SSH-Schlüssel mit Zertifikat**.

> ***Hinweis:*** *Wenn Sie einen privaten SSH-Schlüssel zur Authentifizierung verwenden, müssen Sie einen privaten Schlüssel für das Konto im OpenSSH-Format angeben. Optional können Sie die mit dem privaten Schlüssel verknüpfte Passphrase eingeben.*

Passwort und Bestätigung des Passworts

Wird zur Authentifizierung **Passwort** ausgewählt, müssen Sie das Passwort für das Konto eingeben und das Passwort dann bestätigen.

Privater SSH-Schlüssel

Wird zur Authentifizierung **Privater SSH-Schlüssel** ausgewählt, müssen Sie den privaten SSH-Schlüssel für das Konto eingeben.

Privater SSH-Schlüssel mit Zertifikat

Wird zur Authentifizierung **Privater SSH-Schlüssel mit Zertifikat** ausgewählt, müssen Sie den privaten SSH-Schlüssel für das Konto eingeben, sowie gegebenenfalls die SSH-Schlüssel-Passphrase. Sie müssen auch das öffentliche SSH-Zertifikat für das Konto angeben.

SSH-Schlüssel-Passphrase

Geben Sie ggf. die Passphrase des privaten SSH-Schlüssels ein.

Kontorichtlinie

Wählen Sie eine bestimmte Richtlinie für das Konto aus oder belassen Sie **Konto-Richtlinie** auf dem Standardwert **Richtlinieneinstellungen übernehmen**. In diesem Fall übernimmt das Konto die Richtlinieneinstellungen der Kontogruppe. Wenn für das Konto keine Kontogruppe ausgewählt wird, übernimmt das Konto die Richtlinieneinstellungen, die für die globale Standardkontorichtlinie auf der Seite **Vault > Optionen** festgelegt wurden.

Kontogruppe

Wählen Sie eine Gruppe aus der Liste aus, die dem geteilten Konto einer Kontogruppe hinzugefügt werden soll. Wenn keine Gruppe ausgewählt ist, wird das Konto der **Standardgruppe** hinzugefügt.

Gruppenrichtlinien

Wenn die Kontengruppe zu Gruppenrichtlinien hinzugefügt wurde, werden sie hier zusammen mit ihren Vault-Kontorollen aufgeführt.

Kontobenutzer

Neuer Benutzername

Legen Sie fest, welche Benutzer auf dieses Konto zugreifen können, sowie ihre Vault-Kontorolle, und klicken Sie dann auf **Hinzufügen**.

Neue Mitgliedsrolle

Wählen Sie die Vault-Kontorolle für den neuen Benutzer aus und klicken Sie dann auf **Hinzufügen**. Benutzern kann eine von zwei Rollen zugewiesen werden:

- **Einfügen** (Standardwert): Benutzer mit dieser Rolle können dieses Konto in Remote Support-Sitzungen verwenden.
- **Einfügen und auschecken**: Benutzer mit dieser Rolle können dieses Konto in Remote Support-Sitzungen verwenden und das Konto auf **/login** auschecken. Die Berechtigung **Auschecken** hat keinen Einfluss auf generische SSH-Konten.

***Hinweis:** Die **Vault-Konto-Rolle** ist in der Liste der dem Vault-Konto hinzugefügten Benutzer sichtbar.*

***Hinweis:** Bei der Aktualisierung auf eine BeyondTrust Remote Support-Installation mit der Funktion Konfigurierbarer Vault-Checkout haben alle bestehenden **Vault-Konto-Mitgliedschaften**, die vor der Aktualisierung in den Gruppenrichtlinien konfiguriert wurden, ihre **Vault-Konto-Rolle** nach der Aktualisierung standardmäßig auf **Eingeben und Auschecken** eingestellt.*

WICHTIG!

***Priorität der Vault-Konto-Rolle**: Vault-Konto-Rollen können sowohl Benutzern als auch Gruppenrichtlinien zugewiesen werden. Das bedeutet, dass ein und derselbe Benutzer verschiedene Rollen für ein einziges Vault-Konto haben könnte. Eine Rolle könnte durch die Gruppenrichtlinien des Benutzers zugewiesen werden, während eine andere Rolle durch den expliziten Zugriff des Benutzers auf das Vault-Konto zugewiesen werden könnte. In solchen Fällen verwendet das System die spezifischste Rolle für diesen Benutzer. Daher lässt das System die auf der Seite **Vault-Konto bearbeiten** zugewiesene Rolle die in der Gruppenrichtlinie des Benutzers zugewiesene Rolle überschreiben. Wenn die Rolle auf diese Weise überschrieben wird, erscheint das Wort überschrieben auf der Seite **Vault-Konto bearbeiten** für die Gruppenrichtlinien-Mitgliedschaft des Benutzers. Dieses Verhalten entspricht der Rangfolge der Jump-Element-Rollen.*

***Hinweis:** Benutzerkonten mit der Berechtigung **Kann Vault verwalten** ist es ausdrücklich gestattet, auf jedes Vault-Konto zuzugreifen.*

Jump-Item-Verknüpfungen

Wählen Sie den Typ der **Jump-Item-Verknüpfungen** für das Konto. Die Einstellung **Jump-Item-Verknüpfungen** legt fest, mit welchen Jump-Items das Konto verknüpft ist, sodass das Konto nur für die entsprechenden Zielcomputer in der Konsole d. Support-Technikers bei Anmeldedaten-Eingabeversuchen verfügbar ist. Wählen Sie eine der folgenden Verknüpfungsmethoden:

- **Von der Kontogruppe übernommen**: Die Verknüpfungen für dieses Konto werden durch die in der **Kontogruppe** dieses Kontos definierten Verknüpfungen bestimmt.
- **Beliebige Jump-Items**: Dieses Konto kann in jede Sitzung injiziert werden, die von einem Jump-Item aus gestartet wird, in dem das Konto anwendbar ist.
- **Keine Jump-Items**: Dieses Konto kann nicht in eine Sitzung eingefügt werden, die über ein Jump-Item gestartet wird.
- **Abgleichkriterien für Jump-Items**: Dieses Konto kann nur in Sitzungen eingefügt werden, die von Jump-Items gestartet werden, die den von Ihnen definierten Kriterien entsprechen, in denen das Konto anwendbar ist.
    - Sie können direkte Verknüpfungen zwischen Vault-Konten und bestimmten Jump-Items definieren, indem Sie die Jump-Items in der Liste auswählen und dann auf **Jump-Item hinzufügen** klicken.
    - Sie können die Verknüpfungen zwischen Vault-Konten und Jump-Items weiter definieren, indem Sie Abgleichkriterien auf der Grundlage der folgenden Jump-Item-Attribute angeben. Wenn das Konto konfiguriert ist, steht es für die Injektion für alle Jump-Items zur Verfügung, die den angegebenen Attributkriterien entsprechen, zusätzlich zu den spezifischen Jump-Items, die Sie als Übereinstimmungskriterien hinzugefügt haben.
        - **Freigegebene Jump-Gruppen**: Wählen Sie eine Jump-Gruppe aus der Liste aus.
        - **Name**: Dieser Filter wird mit dem Wert abgeglichen, der in der Spalte **Name** des Jump-Items in der Konsole d. Support-Technikers erscheint.
        - **Hostname/IP**: Dieser Filter wird mit dem Wert abgeglichen, der in der Spalte **Hostname/IP** des Jump-Items in der Konsole d. Support-Technikers erscheint.
        - **Tag:** Dieser Filter wird mit dem Wert abgeglichen, der in der Spalte **Tag** des Jump-Items in der Konsole d. Support-Technikers erscheint.
        - **Kommentare**: Dieser Filter wird mit dem Wert abgeglichen, der in der Spalte **Kommentare** des Jump-Items in der Konsole d. Support-Technikers erscheint.

*Tipp: Klicken Sie für jede Option und jedes Attribut auf das Symbol **i**, um genauere Informationen darüber zu erhalten.*

Hinweis: Lokale Konten sind für die Injektion innerhalb der Endpunkte verfügbar, auf denen sie entdeckt wurden.

Persönliches Konto hinzufügen

Name

Geben Sie einen Namen für das Konto ein.

Beschreibung

Geben Sie eine knappe, aber prägnante Beschreibung für das Konto ein.

Benutzername

Geben Sie den Benutzernamen für das Konto an.

Authentifizierung

Wählen Sie die Authentifizierungsmethode für das Konto aus: **Kennwort**, **privater SSH-Schlüssel** oder **privater SSH-Schlüssel mit Zertifikat**.

Hinweis: Wenn Sie einen privaten SSH-Schlüssel zur Authentifizierung auswählen, müssen Sie einen privaten Schlüssel für das Konto im OpenSSH-Format angeben. Optional können Sie die mit dem privaten Schlüssel verknüpfte Passphrase eingeben.

Passwort und Bestätigung des Passworts

Wird zur Authentifizierung **Passwort** ausgewählt, müssen Sie das Passwort für das Konto eingeben und das Passwort dann bestätigen.

Privater SSH-Schlüssel

Wird zur Authentifizierung **Privater SSH-Schlüssel** ausgewählt, müssen Sie den privaten SSH-Schlüssel für das Konto eingeben.

Privater SSH-Schlüssel mit Zertifikat

Wird zur Authentifizierung **Privater SSH-Schlüssel mit Zertifikat** ausgewählt, müssen Sie den privaten SSH-Schlüssel für das Konto eingeben, sowie gegebenenfalls die SSH-Schlüssel-Passphrase. Sie müssen auch das öffentliche SSH-Zertifikat für das Konto angeben.

SSH-Schlüssel-Passphrase

Geben Sie ggf. die Passphrase des privaten SSH-Schlüssels ein.

Lokales Konto bearbeiten

Name

Zeigen Sie den für das Konto verwendeten Namen an oder bearbeiten Sie ihn.

Beschreibung

Zeigen Sie die Beschreibung des Kontos an oder bearbeiten Sie sie.

Benutzername

Zeigen Sie den mit dem Konto verknüpften Benutzernamen an.

Passwort und Bestätigung des Passworts

Geben Sie ein neues Passwort für das Konto an oder lassen Sie das Feld leer, um das vorhandene Passwort zu behalten. Bestätigen Sie das eingegebene Passwort.

Passwortalter

Zeigen Sie das Alter des vorhandenen Passworts an.

Kontorichtlinie

Wählen Sie eine bestimmte Richtlinie für das Konto aus oder belassen Sie **Konto-Richtlinie** auf dem Standardwert **Richtlinieneinstellungen übernehmen**. In diesem Fall übernimmt das Konto die Richtlinieneinstellungen der Kontogruppe. Wenn für das Konto keine Kontogruppe ausgewählt wird, übernimmt das Konto die Richtlinieneinstellungen, die für die globale Standardkontorichtlinie auf der Seite **Vault > Optionen** festgelegt wurden.

Simultanes Auschecken gestatten

Wenn das Konto ausgecheckt und von mehreren Benutzern oder Sitzungen gleichzeitig verwendet werden kann, wählen Sie diese Option.

Kontogruppe

Wählen Sie eine Gruppe aus der Liste aus, die dem geteilten Konto einer Kontogruppe hinzugefügt werden soll. Wird eine Gruppe nicht ausgewählt, wird das Konto der Systemgruppe **Keine** hinzugefügt.

Name des Endpunkts

Zeigen Sie an, welcher Endpunkt bzw. welche Endpunkte mit dem Konto verknüpft sind.

Hostname des Endpunkts

Zeigen Sie den Hostnamen der verknüpften Endpunkte an.

Kontobenutzer

Legen Sie fest, welche Benutzer auf dieses Konto zugreifen können, sowie ihre Vault-Kontorolle, und klicken Sie dann auf **Hinzufügen**.

> ***Hinweis:*** *Benutzerkonten mit der Berechtigung* ***Kann Vault verwalten*** *ist es ausdrücklich gestattet, auf jedes Vault-Konto zuzugreifen.*

Jump-Item-Verknüpfungen

Wählen Sie den Typ der **Jump-Item-Verknüpfungen** für das Konto. Die Einstellung **Jump-Item-Verknüpfungen** legt fest, mit welchen Jump-Items das Konto verknüpft ist, sodass das Konto nur für die entsprechenden Zielcomputer in der Konsole d. Support-Technikers bei Anmeldedaten-Eingabeversuchen verfügbar ist. Wählen Sie eine der folgenden Verknüpfungsmethoden:

- **Von der Kontogruppe übernommen**: Die Verknüpfungen für dieses Konto werden durch die in der **Kontogruppe** dieses Kontos definierten Verknüpfungen bestimmt.
- **Beliebige Jump-Items**: Dieses Konto kann in jede Sitzung injiziert werden, die von einem Jump-Item aus gestartet wird, in dem das Konto anwendbar ist.
- **Keine Jump-Items**: Dieses Konto kann nicht in eine Sitzung eingefügt werden, die über ein Jump-Item gestartet wird.
- **Abgleichkriterien für Jump-Items**: Dieses Konto kann nur in Sitzungen eingefügt werden, die von Jump-Items gestartet werden, die den von Ihnen definierten Kriterien entsprechen, in denen das Konto anwendbar ist.
    - Sie können direkte Verknüpfungen zwischen Vault-Konten und bestimmten Jump-Items definieren, indem Sie die Jump-Items in der Liste auswählen und dann auf **Jump-Item hinzufügen** klicken.
    - Sie können die Verknüpfungen zwischen Vault-Konten und Jump-Items weiter definieren, indem Sie Abgleichkriterien auf der Grundlage der folgenden Jump-Item-Attribute angeben. Wenn das Konto konfiguriert ist, steht es für die Injektion für alle Jump-Items zur Verfügung, die den angegebenen Attributkriterien entsprechen, zusätzlich zu den spezifischen Jump-Items, die Sie als Übereinstimmungskriterien hinzugefügt haben.
        - **Freigegebene Jump-Gruppen**: Wählen Sie eine Jump-Gruppe aus der Liste aus.
        - **Name**: Dieser Filter wird mit dem Wert abgeglichen, der in der Spalte **Name** des Jump-Items in der Konsole d. Support-Technikers erscheint.
        - **Hostname/IP**: Dieser Filter wird mit dem Wert abgeglichen, der in der Spalte **Hostname/IP** des Jump-Items in der Konsole d. Support-Technikers erscheint.
        - **Tag:** Dieser Filter wird mit dem Wert abgeglichen, der in der Spalte **Tag** des Jump-Items in der Konsole d. Support-Technikers erscheint.
        - **Kommentare**: Dieser Filter wird mit dem Wert abgeglichen, der in der Spalte **Kommentare** des Jump-Items in der Konsole d. Support-Technikers erscheint.

Domänenkonto bearbeiten

Name

Zeigen Sie den für das Konto verwendeten Namen an oder bearbeiten Sie ihn.

Beschreibung

Zeigen Sie die Beschreibung des Kontos an oder bearbeiten Sie sie.

Benutzername

Zeigen Sie den mit dem Konto verknüpften Benutzernamen an.

Passwort und Bestätigung des Passworts

Geben Sie ein neues Passwort für das Konto an oder lassen Sie das Feld leer, um das vorhandene Passwort zu behalten. Bestätigen Sie das eingegebene Passwort.

Passwortverlauf anzeigen

Zeigen Sie die Daten und Uhrzeiten von Passwort-Änderungen an. Klicken Sie auf **Einblenden**, um das Passwort vorübergehend anzuzeigen. Klicken Sie auf **Benutzen**, um das Passwort dieses Kontos auf dieses Passwort einzustellen.

Passwortalter

Zeigen Sie das Alter des vorhandenen Passworts an.

Kontorichtlinie

Wählen Sie eine bestimmte Richtlinie für das Konto aus oder belassen Sie **Konto-Richtlinie** auf dem Standardwert **Richtlinieneinstellungen übernehmen**. In diesem Fall übernimmt das Konto die Richtlinieneinstellungen der Kontogruppe. Wenn für das Konto keine Kontogruppe ausgewählt wird, übernimmt das Konto die Richtlinieneinstellungen, die für die globale Standardkontorichtlinie auf der Seite **Vault > Optionen** festgelegt wurden.

Eindeutiger Name

Zeigen Sie den eindeutigen Namen des Kontos an.

Kontogruppe

Wählen Sie eine Gruppe aus der Liste aus, die dem geteilten Konto einer Kontogruppe hinzugefügt werden soll. Wenn keine Gruppe ausgewählt ist, wird das Konto der **Standardgruppe** hinzugefügt.

Kontobenutzer

Legen Sie fest, welche Benutzer auf dieses Konto zugreifen können, sowie ihre Vault-Kontorolle, und klicken Sie dann auf **Hinzufügen**.

> ***Hinweis:*** *Benutzerkonten mit der Berechtigung* ***Kann Vault verwalten*** *ist es ausdrücklich gestattet, auf jedes Vault-Konto zuzugreifen.*

Jump-Item-Verknüpfungen

Wählen Sie den Typ der **Jump-Item-Verknüpfungen** für das Konto. Die Einstellung **Jump-Item-Verknüpfungen** legt fest, mit welchen Jump-Items das Konto verknüpft ist, sodass das Konto nur für die entsprechenden Zielcomputer in der Konsole d. Support-Technikers bei Anmeldedaten-Eingabeversuchen verfügbar ist. Wählen Sie eine der folgenden Verknüpfungsmethoden:

- **Von der Kontogruppe übernommen**: Die Verknüpfungen für dieses Konto werden durch die in der **Kontogruppe** dieses Kontos definierten Verknüpfungen bestimmt.
- **Beliebige Jump-Items**: Dieses Konto kann in jede Sitzung injiziert werden, die von einem Jump-Item aus gestartet wird, in dem das Konto anwendbar ist.
- **Keine Jump-Items**: Dieses Konto kann nicht in eine Sitzung eingefügt werden, die über ein Jump-Item gestartet wird.
- **Abgleichkriterien für Jump-Items**: Dieses Konto kann nur in Sitzungen eingefügt werden, die von Jump-Items gestartet werden, die den von Ihnen definierten Kriterien entsprechen, in denen das Konto anwendbar ist.
    - Sie können direkte Verknüpfungen zwischen Vault-Konten und bestimmten Jump-Items definieren, indem Sie die Jump-Items in der Liste auswählen und dann auf **Jump-Item hinzufügen** klicken.
    - Sie können die Verknüpfungen zwischen Vault-Konten und Jump-Items weiter definieren, indem Sie Abgleichkriterien auf der Grundlage der folgenden Jump-Item-Attribute angeben. Wenn das Konto konfiguriert ist, steht es für die Injektion für alle Jump-Items zur Verfügung, die den angegebenen Attributkriterien entsprechen, zusätzlich zu den spezifischen Jump-Items, die Sie als Übereinstimmungskriterien hinzugefügt haben.
        - **Freigegebene Jump-Gruppen**: Wählen Sie eine Jump-Gruppe aus der Liste aus.
        - **Name**: Dieser Filter wird mit dem Wert abgeglichen, der in der Spalte **Name** des Jump-Items in der Konsole d. Support-Technikers erscheint.
        - **Hostname/IP**: Dieser Filter wird mit dem Wert abgeglichen, der in der Spalte **Hostname/IP** des Jump-Items in der Konsole d. Support-Technikers erscheint.
        - **Tag:** Dieser Filter wird mit dem Wert abgeglichen, der in der Spalte **Tag** des Jump-Items in der Konsole d. Support-Technikers erscheint.
        - **Kommentare**: Dieser Filter wird mit dem Wert abgeglichen, der in der Spalte **Kommentare** des Jump-Items in der Konsole d. Support-Technikers erscheint.

Persönliches generisches (Passwort) Konto bearbeiten

Name

Zeigen Sie den für das Konto verwendeten Namen an oder bearbeiten Sie ihn.

Beschreibung

Zeigen Sie die Beschreibung des Kontos an oder bearbeiten Sie sie.

Benutzername

Zeigen Sie den mit dem Konto verknüpften Benutzernamen an.

Passwort und Bestätigung des Passworts

Geben Sie ein neues Passwort für das Konto an oder lassen Sie das Feld leer, um das vorhandene Passwort zu behalten. Bestätigen Sie das eingegebene Passwort.

Vault-Kontogruppen: Kontogruppen hinzufügen und verwalten

Vault | KONTOGRUPPEN

Freigegebene Vault-Konten können zu einer Kontogruppe hinzugefügt werden, damit Vault-Administratoren Benutzern den Zugriff auf mehrere freigegebene Vault-Konten effizienter gewähren können. Kontogruppen können auch verwendet werden, um eine Gruppe von freigegebenen Vault-Konten mit einer Gruppenrichtlinie zu verknüpfen.

***Hinweis:** Ein freigegebenes Vault-Konto kann immer nur zu einer Gruppe gehören und persönliche Vault-Konten können nicht zu einer Kontogruppe hinzugefügt werden.*

Kontogruppen

Kontogruppen hinzufügen, anzeigen und verwalten.

Kontogruppe hinzufügen

Klicken Sie auf **Hinzufügen**, um eine Kontogruppe hinzuzufügen, Vault-Konten zu der Gruppe hinzuzufügen und Benutzern Zugriff auf die Gruppe der freigegebenen Vault-Konten zu gewähren.

Kontogruppen durchsuchen

Suchen Sie anhand von **Name** oder **Beschreibung** nach einer bestimmten Kontogruppe.

Kontogruppe hinzufügen

Mit der Option **Kontogruppe hinzufügen** können Sie Kontogruppen hinzufügen, um Benutzern gleichzeitig Zugriff auf mehrere Vault-Konten zu gewähren.

Name

Geben Sie einen Namen für die Kontogruppe ein.

Beschreibung

Geben Sie eine knappe, aber prägnante Beschreibung der Kontogruppe ein.

Kontorichtlinie

Wählen Sie eine bestimmte Richtlinie für die Kontogruppe oder belassen Sie **Konto-Richtlinie** auf dem Standardwert **Richtlinieneinstellungen übernehmen**. In diesem Fall übernehmen die Konten in dieser Kontogruppe die Richtlinieneinstellungen, die für die globale Standard-Konto-Richtlinie auf der Seite **Vault** > **Optionen** festgelegt wurden.

Gruppenrichtlinien

Wenn die Kontengruppe zu Gruppenrichtlinien hinzugefügt wurde, werden sie hier zusammen mit ihren Vault-Kontorollen aufgeführt.

Konten

Quellkontogruppe

Filtern Sie die Liste der Konten, die zum Hinzufügen zur Gruppe verfügbar sind, indem Sie eine Gruppe aus der Liste **Quellkontogruppe** auswählen.

Ausgewählte Kontogruppen durchsuchen

Filtern Sie die Liste der Konten, die zum Hinzufügen zur Gruppe verfügbar sind, indem Sie nach einer Kontogruppe suchen. Sie können nach **Name**, **Endpunkt** und **Beschreibung** suchen.

Konten in der Gruppe „Standardgruppe“

Liste der Vault-Konten, die zum Hinzufügen zur Kontengruppe verfügbar sind.

Hinzufügen

Wählen Sie Konten aus der Liste der verfügbaren Gruppen aus und klicken Sie dann auf **Hinzufügen**, um sie der Liste **Konten in dieser Gruppe** hinzuzufügen.

Entfernen

Wählen Sie Konten aus der Liste der **Konten in dieser Gruppe** und klicken Sie dann auf **Entfernen**, um sie aus der Kontengruppe zu entfernen.

Diese Kontogruppe durchsuchen

Filtern Sie die Liste der **Konten in dieser Gruppe**, indem Sie nach einer Kontogruppe anhand von **Name**, **Endpunkt** und **Beschreibung** suchen.

Konten in dieser Gruppe

Liste der Vault-Konten, die in dieser Kontogruppe vorhanden sind.

Zugelassene Benutzer

Neuer Benutzername

Legen Sie fest, welche Benutzer auf dieses Konto zugreifen können.

Neue Mitgliedsrolle

Wählen Sie die Vault-Kontorolle für den neuen Benutzer aus und klicken Sie dann auf **Hinzufügen**. Benutzern kann eine von zwei Rollen zugewiesen werden:

- **Einfügen** (Standardwert): Benutzer mit dieser Rolle können dieses Konto in Remote Support-Sitzungen verwenden.
- **Einfügen und auschecken**: Benutzer mit dieser Rolle können dieses Konto in Remote Support-Sitzungen verwenden und das Konto auf **/login** auschecken. Die Berechtigung **Auschecken** hat keinen Einfluss auf generische SSH-Konten.

***Hinweis:** Die **Vault-Konto-Rolle** ist in der Liste der dem Vault-Konto hinzugefügten Benutzer sichtbar.*

Jump-Item-Verknüpfungen

Wählen Sie die Art der **Jump-Item-Verknüpfungen** für die Kontogruppe. Die Einstellung **Jump-Item-Verknüpfungen** legt fest, mit welchen Jump-Items die Konten in dieser Kontogruppe verbunden sind, sodass nur die Konten, die für den Zielcomputer relevant sind, bei Anmeldedaten-Einfügungs-Versuchen in der Konsole d. Support-Technikers verfügbar sind. Wählen Sie eine der folgenden Verknüpfungsmethoden:

- **Beliebige Jump-Items**: Konten in dieser Gruppe können in jede Jump-Item-Sitzung eingefügt werden, in der die Konten anwendbar sind.
- **Keine Jump-Items**: Konten in dieser Gruppe können nicht in eine Jump-Item-Sitzung eingefügt werden.
- **Abgleichkriterien für Jump-Items**: Konten in dieser Gruppe können nur in Jump-Item-Sitzungen eingefügt werden, die den von Ihnen definierten Kriterien entsprechen, in denen die Konten anwendbar sind.
    - Sie können eine direkte Verknüpfung zwischen anwendbaren Konten in dieser Kontogruppe und bestimmten Jump-Items definieren, indem Sie die Jump-Items in der Liste auswählen und dann auf **Jump-Item hinzufügen** klicken.
    - Sie können die Verknüpfung zwischen anwendbaren Konten in dieser Kontogruppe und Jump-Items weiter definieren, indem Sie Abgleichskriterien auf der Grundlage der folgenden Jump-Item-Attribute angeben. Wenn konfiguriert, stehen Konten in dieser Kontogruppe für die Injektion für alle Jump-Items zur Verfügung, die den angegebenen Attributkriterien entsprechen, zusätzlich zu den spezifischen Jump-Items, die Sie als Abgleichskriterien hinzugefügt haben.
        - **Freigegebene Jump-Gruppen**: Wählen Sie eine Jump-Gruppe aus der Liste aus.
        - **Name**: Dieser Filter wird mit dem Wert abgeglichen, der in der Spalte **Name** des Jump-Items in der Konsole d. Support-Technikers erscheint.
        - **Hostname/IP**: Dieser Filter wird mit dem Wert abgeglichen, der in der Spalte **Hostname/IP** des Jump-Items in der Konsole d. Support-Technikers erscheint.
        - **Tag:** Dieser Filter wird mit dem Wert abgeglichen, der in der Spalte **Tag** des Jump-Items in der Konsole d. Support-Technikers erscheint.
        - **Kommentare**: Dieser Filter wird mit dem Wert abgeglichen, der in der Spalte **Kommentare** des Jump-Items in der Konsole d. Support-Technikers erscheint.

***Tipp:** Klicken Sie für jede Option und jedes Attribut auf das Symbol **i**, um genauere Informationen darüber zu erhalten.*

***Hinweis:** Lokale Konten sind für die Injektion innerhalb der Endpunkte verfügbar, auf denen sie entdeckt wurden.*

Kontenrichtlinien: Kontogruppen hinzufügen und verwalten

Vault | KONTENRICHTLINIEN

Vault-Kontorichtlinien bieten eine Methode zur Definition von Kontoeinstellungen mit Bezug auf die Rotation von Passwörtern und das Auschecken von Anmeldedaten, und wenden diese Einstellungen gleichzeitig auf mehrere Konten an.

Mehrere, einem einzigen Vault-Konto zugewiesene Kontorichtlinien werden in der folgenden Reihenfolge angewandt, von oben nach unten:

- Die mit dem Vault-Konto verbundene Kontorichtlinie
- Die mit der Kontogruppe des Vaults verbundene Kontorichtlinie.
- Die globalen Standard-Kontorichtlinieneinstellungen

Wenn mehrere Kontorichtlinien eine Einstellung definieren, wird der Wert der ersten angewandten Richtlinie verwendet.

Kontenrichtlinien

Hinzufügen, Anzeigen und Verwalten von Kontorichtlinien.

Kontorichtlinie hinzufügen

Klicken Sie auf **Hinzufügen**, um eine Kontorichtlinie hinzuzufügen.

Kontorichtlinie kopieren

Klicken Sie auf **Kopieren**, um eine bestehende Kontorichtlinie zu kopieren.

Kontorichtlinie bearbeiten

Klicken Sie auf **Bearbeiten**, um eine bestehende Kontorichtlinie zu ändern.

Kontorichtlinie hinzufügen

Fügen Sie eine neue Kontorichtlinie hinzu.

Anzeigename

Geben Sie einen Namen für die Kontorichtlinie ein.

Codename

Legen Sie einen Codenamen zu Integrationszwecken fest. Wenn Sie keinen Codenamen festlegen, erstellt Remote Support automatisch einen.

Beschreibung

Geben Sie eine kurze und einprägsame Beschreibung der Kontorichtlinie ein.

Berechtigungen

Automatische Passwortverwaltung

Regeln für die geplante Passwortrotation

- Wählen Sie **Zulassen**, um Passwörter für Vault-Konten so zu planen, dass sie automatisch rotieren, wenn das Passwort ein bestimmtes Höchstalter erreicht.
- Wählen Sie **Ablehnen**, um die geplante Passwortrotation für Vault-Konten zu deaktivieren.

Maximales Passwortalter

Wenn die geplante Passwortrotation aktiviert ist, geben Sie die maximale Anzahl von Tagen an, die ein Passwort für Vault-Konten gültig sein kann, bevor es automatisch rotiert wird.

Kontoeinstellungen

Regel für automatisches Rotieren der Anmeldedaten nach Einchecken

- Wählen Sie **Zulassen**, um Passwörter automatisch zu rotieren, nachdem ein Anmelde-Datensatz eingecheckt wurde.
- Wählen Sie **Deaktivieren**, um die automatische Rotation von Passwörtern nach dem Einchecken eines Anmelde-Datensatzes zu deaktivieren.

Regeln für das Zulassen des simultanen Auscheckens

- Wählen Sie **Zulassen**, um das gleichzeitige Auschecken von Vault-Anmeldedaten zu ermöglichen.
- Wählen Sie **Ablehnen**, um die Möglichkeit des gleichzeitigen Auscheckens von Vault-Anmeldedaten zu deaktivieren.

Hinweis: *Wenn eine Einstellung in einer Kontorichtlinie nicht definiert ist, übernimmt sie die Einstellungen von der globalen Standardkontorichtlinie, die auf der Seite* ***Vault*** *>* ***Optionen*** *in /login konfiguriert wird.*

Endpunkte: Entdeckte Endpunkte verwalten

Vault | ENDPUNKTE

Endpunkte

Zeigen Sie Informationen zu allen erfassten Endpunkten an, wie Name und Hostname, Betriebssystem, Domain und Bezeichnung des Systems sowie Informationen zu den mit diesen Systemen verbundenen Konten.

Endpunkte durchsuchen

Suchen Sie anhand von **Namen**, **Hostnamen**, **Beschreibung** oder **Domain-Namen** nach einem bestimmten Endpunkt oder einer Gruppe an Endpunkten.

Sichtbare Spalten auswählen

Klicken Sie auf die Schaltfläche **Sichtbare Spalten auswählen** (Spaltensymbol) über dem Raster **Endpunkte** und wählen Sie die Spalten, die im Raster angezeigt werden sollen.

Konten

Zeigen Sie die Anzahl der Konten an, die mit jedem Endpunkt verbunden sind. Kicken Sie auf den Link **Konten**, um die mit dem System verknüpften Konten anzuzeigen.

Jump-Items

Zeigen Sie die Anzahl der Jump-Items an, die mit jedem Endpunkt verbunden sind. Kicken Sie auf den Link **Jump-Items**, um die mit dem System verknüpften Jump-Items anzuzeigen.

Dienste

Zeigen Sie die Anzahl der Windows-Dienste an, die mit jedem Endpunkt verbunden sind. Klicken Sie auf den Link **Dienste**, um die mit dem System verknüpften Dienste anzuzeigen.

Bearbeiten

Ändern Sie die Informationen zu den Endpunkten, insbesondere **Name**, **Beschreibung** und **Hostname**.

> ***Hinweis:*** *Wenn Windows-Dienste erkannt und in den Vault importiert wurden, wird jeder vom Endpunkt verwendete Dienst aufgelistet und das Benutzerkonto, das den Dienst ausführt, angegeben.*

Löschen

Löschen Sie den Endpunkt aus der Liste der **Endpunkte**.

Dienste: Erkannte Dienste anzeigen und verwalten

Vault | DIENSTE

Dienste

Zeigen Sie die Liste der bei der Erkennung gefundenen Dienste sowie die Endpunkte und Konten an, denen sie zugeordnet sind, sowie den letzten Status jedes Dienstes. Sie haben außerdem die Option, den Dienst nach der Rotation des Service-Kontos neu zu starten.

Kontogruppen durchsuchen

Suche nach bestimmten Diensten oder einer Gruppe von Diensten anhand von **Kurzname**, **Beschreibung**, **Endpunkt (Hostname)** oder **Benutzername**.

Neu starten

Aktivieren Sie das Kontrollkästchen **Neu starten** beim Dienst, damit der Dienst neu startet, wenn der das Konto ausführende Dienst rotiert wird.

Löschen

Löschen Sie den Dienst aus der Liste **Dienste**.

Domänen: Hinzufügen und Verwalten von Domänen

Vault | DOMÄNEN

Fügen Sie Informationen zu Ihren Domänen hinzu, zeigen Sie sie an und verwalten Sie sie.

Domänen

Domäne hinzufügen

Klicken Sie auf **Hinzufügen**, um manuell eine neue Domäne zur Liste **Domänen** hinzuzufügen.

Name der Domäne

Zeigen Sie den Namen der Domäne an.

Jumpoint

Zeigen Sie den für die Erfassung von Konten und Endpunkten in der Domäne verwendeten Jumpoint an.

Verwaltungskonto

Zeigen Sie das mit dem Jumpoint und der Domäne verknüpfte Verwaltungskonto an.

Entdecken

Klicken Sie auf **Erfassen**, um den Jumpoint zu initiieren und nach Endpunkten und Konten in der Domäne zu scannen.

Bearbeiten

Klicken Sie auf **Bearbeiten**, um die Angaben zur Domäne zu bearbeiten.

Löschen

Klicken Sie auf **Löschen**, um diese Domäne aus der Liste der **Domänen** zu löschen.

Hinzufügen oder Bearbeiten einer Domäne

DNS-Name

Geben Sie den **DNS-Namen** der Domäne ein.

Jumpoint

Wählen Sie einen vorhandenen Jumpoint in der Umgebung, in der Sie Konten erfassen möchten.

Verwaltungskonto

Wählen Sie das erforderliche Verwaltungskonto aus, um einen Discovery-Auftrag zu dieser Domäne zu initiieren. Wählen Sie die Verwendung eines neuen Kontos aus. Dafür müssen **Benutzername**, **Passwort** und **Passwortbestätigung** eingegeben werden. Andernfalls können Sie auch ein in einem vorangehenden Auftrag erfasstes oder ein im Abschnitt **Konten** manuell hinzugefügtes Konto auswählen.

Geplante Domänen-Discovery

Aktivieren und konfigurieren Sie die Domain-Erkennung so, dass sie nach einem bestimmten Zeitplan abläuft.

Geplante Discovery aktivieren

Aktivieren Sie das Kontrollkästchen, um die Optionen **Erkennungszeitplan** zu aktivieren.

Discovery-Zeitplan

Wählen Sie die Wochentage und die Uhrzeit aus, zu denen der Erkennungsauftrag ausgeführt werden soll.

Discovery-Bereich

Wählen Sie die Objekte aus, die Vault erkennen soll:

- **Domänenkonten**
- **Endpunkte**
- **Lokale Konten**
- **Dienste**

Sie können einen **Suchpfad** eingeben oder ihn leer lassen, um alle OEs und Container zu durchsuchen. Sie können auch eine **LDAP-Abfrage** verwenden, um den Umfang der gesuchten Benutzerkonten und Endpunkte einzuschränken.

Optionen: Konfigurieren der globalen Standard-Kontorichtlinieneinstellungen und der Passwortlänge für die Kontorotation

Vault | OPTIONEN

Globale Optionen

Konfigurieren Sie die Einstellungen für die globale Standard-Kontorichtlinie.

Die globale Standard-Kontorichtlinie muss für jede Einstellung eine Option definieren. Wenn für ein Konto keine Einstellung mit einer bestimmten Richtlinie definiert ist, erbt es die Richtlinie von der Kontengruppe. Wenn für die Kontogruppe keine Einstellung mit einer bestimmten Richtlinie definiert ist, erbt sie die Richtlinie von der globalen Standard-Kontorichtlinie.

Automatische Passwortverwaltung

Regeln für die geplante Passwortrotation

- Wählen Sie **Zulassen**, um Passwörter für Vault-Konten so zu planen, dass sie automatisch rotieren, wenn das Passwort ein bestimmtes Höchstalter erreicht.
- Wählen Sie **Ablehnen**, um die geplante Passwortrotation für Vault-Konten zu deaktivieren.

Maximales Passwortalter

Wenn die geplante Passwortrotation aktiviert ist, geben Sie die maximale Anzahl von Tagen an, die ein Passwort für Vault-Konten gültig sein kann, bevor es automatisch rotiert wird.

Kontoeinstellungen

Regel für automatisches Rotieren der Anmeldedaten nach Einchecken

- Wählen Sie **Zulassen**, um Passwörter automatisch zu rotieren, nachdem ein Anmelde-Datensatz eingecheckt wurde.
- Wählen Sie **Deaktivieren**, um die automatische Rotation von Passwörtern nach dem Einchecken eines Anmelde-Datensatzes zu deaktivieren.

Regeln für das Zulassen des simultanen Auscheckens

- Wählen Sie **Zulassen**, um das gleichzeitige Auschecken von Vault-Anmeldedaten zu ermöglichen.
- Wählen Sie **Ablehnen**, um die Möglichkeit des gleichzeitigen Auscheckens von Vault-Anmeldedaten zu deaktivieren.

Generierte Passwörter für die Kontorotation

Legen Sie die Länge der während der Kontorotation generierten Passwörter für Domänen und lokale Konten fest. Sie können eine Mindestlänge von **20** Zeichen und eine maximale Länge von **256** Zeichen einstellen.

> ***Hinweis:*** *Die Länge der Passwörter gilt nicht für SSH- und persönliche Konten.*

Passwortlänge

Legen Sie die minimale und maximale Anzahl von Zeichen für das Passwort fest, das während der manuellen, automatischen und geplanten Passwortrotation für Konten generiert wird, die über die Windows-API rotiert werden (Nicht-Azure-Konten).

Passwortlänge von AADDS-Konten

Legen Sie die minimale und maximale Anzahl von Zeichen fest, die für das Passwort zulässig sind, das während der Passwortrotation von Azure Active Directory Domain Services (AADDS)-Konten über MS Graph API generiert wird.

Konsole des Support-Technikers

Einstellungen für Konsole des Support-Technikers: Standardmäßige Einstellungen für die Konsole des Support-Technikers verwalten

Verwalten der Konsole d. Support-Technikers-Einstellungen

Sie können die Standardeinstellungen der Konsole d. Support-Technikers für Ihre gesamte Benutzerbasis konfigurieren, ein durchgängiges Benutzererlebnis mit der Konsole d. Support-Technikers umsetzen und so die Teameffizienz erhöhen. Sie können Einstellungen erzwingen, Einstellungen vom Benutzer überschreiben lassen oder die Einstellungen unverwaltet belassen. Wenn Sie **Nicht verwaltet** wählen, wird die BeyondTrust-Standardeinstellung als Vorschlag daneben angezeigt.

Die jeweiligen Einstellungen **Aktivieren** und **Deaktivieren** lassen sich über ein Administrator-Kontrollkästchen auch erzwingen. Erzwungene Einstellungen werden ab der nächsten Anmeldung des Benutzers wirksam und lassen sich nicht über die Konsole konfigurieren. Nicht erzwungene Einstellungen können von einem Benutzer mithilfe des Einstellungsfensters in der Konsole d. Support-Technikers überschrieben werden.

> *Weitere Informationen finden Sie in Einstellungen und Voreinstellungen in der Konsole des Support-Technikers ändern unter https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/settings.htm.*

Eine erzwungene Einstellung kann nicht überschrieben werden, es sei denn, ein Administrator deaktiviert das Kontrollkästchen **Erzwungen** in der **/login**-Verwaltungsschnittstelle.

Wählen Sie die Einstellungen, die Sie für Ihre Benutzer als Standard festlegen möchten und klicken Sie auf die Schaltfläche **Speichern** unten auf der Seite.

Beachten Sie, dass gespeicherte Einstellungen erst mit der Anmeldung in der Konsole wirksam werden. Selbst wenn Sie die Änderungen speichern und durch Klick auf die Schaltfläche **Jetzt übernehmen** oben auf der Seite übernehmen, kann der Benutzer die neuen Einstellungen erst ab der nächsten Anmeldung verwenden.

Wenn Sie beispielsweise Standardeinstellungen für neue Benutzer konfigurieren möchten, aber die Einstellungen bestehender Benutzer unberührt lassen wollen, speichern Sie Ihre verwalteten Einstellungen, aber übernehmen Sie sie nicht. Damit beginnen alle Anmeldungen in der Konsole d. Support-Technikers mit Ihren verwalteten Standardeinstellungen. Für bestehende Benutzer werden bei der nächsten Anmeldung erzwungene Einstellungen übernommen, alle anderen Einstellungen bleiben jedoch unberührt.

Globale Einstellungen

Rechtschreibprüfung aktiviert

Im Abschnitt **Globale Einstellungen** können Sie die Rechtschreibprüfung für Chat und Sitzungsnotizen aktivieren oder deaktivieren. Derzeit steht die Rechtschreibprüfung nur für US-Englisch zur Verfügung.

Automatische Sitzungszuweisung beim Anmelden deaktivieren

Wird die automatische Sitzungszuweisung bei der Anmeldung deaktiviert, werden dem Benutzer erst automatisch Sitzungen zugewiesen, wenn er dem Opt-In zustimmt.

Konfigurierbare Sitzungs-Seitenleiste

Wählen Sie, ob das Sitzungsmenüsymbol angezeigt werden soll, ob die Seitenleiste gelöst werden kann und ob die Widgets der Sitzungs-Seitenleiste neu angeordnet und in der Größe verändert werden können.

Schnellstart-Schaltflächen

Weitere Informationen finden Sie in Konsole d. Support-Technikers-Benutzerschnittstelle auf https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/representative-console-overview.htm.

***Hinweis:** Mit der Option **Erzwungen** können Sie verhindern, dass Support-Techniker die verwalteten Einstellungen überschreiben*

Sitzung starten

Zeigt die Schaltfläche **Start** oberhalb der Konsole d. Support-Technikers an. Durch Klicken auf diese Schaltfläche kann der Benutzer die verschiedenen Möglichkeiten einsehen, mit denen Ihr Kunde eine Support-Sitzung Tech starten kann.

Sitzungsschlüssel

Die Schaltfläche zur Sitzungsschlüsselgenerierung oberhalb der Konsole d. Support-Technikers anzeigen.

Support-Sitzung Techs

Eine Schaltfläche zum Starten der Support-Button-Verwaltungsoberfläche oben in der Konsole d. Support-Technikers anzeigen.

Shell Jump

Eine Schaltfläche zum Starten einer Shell Jump-Sitzung oben in der Konsole d. Support-Technikers anzeigen.

Jump zu

Eine Schaltfläche zum Starten einer lokalen oder Remote-Jump-Sitzung oben in der Konsole d. Support-Technikers anzeigen.

Intel® vPro

Eine Schaltfläche zum Zugriff auf einen bereitgestellten vPro Jumpoint oben in der Konsole d. Support-Technikers anzeigen.

RDP

Eine Schaltfläche zum Starten einer RDP-Sitzung oben in der Konsole d. Support-Technikers anzeigen.

VNC

Eine Schaltfläche zum Starten einer VNC-Sitzung oben in der Konsole d. Support-Technikers anzeigen.

Präsentation starten

Die Schaltfläche zum Planen oder sofortigen Starten einer neuen Präsentation oben in der Konsole d. Support-Technikers anzeigen.

Alarme

Hörbare Alarme - einen Ton wiedergeben, wenn eine Chatnachricht erhalten wird

Legen Sie fest, ob ein Klang abgespielt werden soll, wenn der Benutzer eine Chatnachricht erhält. Falls nicht verwaltet oder falls aktiviert und nicht erzwungen, kann der Benutzer einen benutzerdefinierten Klang im WAV-Format festlegen, der nicht größer als 1 MB ist.

Visuelle Alarme - Anwendungssymbol aufblinken lassen, wenn eine Chatnachricht erhalten wird

Wählen Sie, das Anwendungssymbol blinken soll, wenn der Benutzer eine Chatnachricht erhält.

Statusnachrichten in Chat-Fenstern des Support-Teams anzeigen

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

Popup-Benachrichtigungen

Team-Warteschlangen

Legen Sie fest, ob ein Benutzer eine Popup-Benachrichtigung für in einem Support-Team-Chat erhaltene Chatnachrichten erhalten soll.

Support-Sitzung Techs

Legen Sie fest, ob ein Benutzer eine Popup-Benachrichtigung für in einer Support-Sitzung Tech erhaltene Chatnachrichten erhalten soll.

Hörbare Alarme - einen Ton wiedergeben, wenn eine Sitzung in eine Warteschlange eingereiht wird

Wählen Sie, ob ein Klang abgespielt werden soll, wenn eine Sitzung in die Warteschlange eines Benutzers aufgenommen wird.

Hörbare Alarme - einen Ton wiedergeben, wenn eine Sitzung in den Teamwarteschlangen überfällig ist

Legen Sie fest, ob ein Klang abgespielt werden soll, wenn eine Sitzung in einer Teamwarteschlange überfällig ist.

Visuelle Alarme - Anwendungssymbol aufblinken lassen, wenn eine Sitzung in eine Warteschlange eingereiht wird

Legen Sie fest, ob das Anwendungssymbol aufblinken soll, wenn eine Sitzung in die Warteschlange eines Benutzers aufgenommen wird.

Visuelle Alarme - Anwendungssymbol aufblinken lassen, wenn eine Sitzung in den Teamwarteschlangen überfällig ist

Legen Sie fest, ob das Anwendungssymbol blinken soll, wenn eine Sitzung in einer Teamwarteschlange überfällig ist.

Eingabeaufforderung, wenn neuer Kunde einer persönlichen Warteschlange beitritt

Legen Sie fest, ob für den Benutzer eine Aufforderung angezeigt werden soll, wenn eine Sitzung in seine persönliche Warteschlange aufgenommen wird.

Popup-Benachrichtigungen

Popup-Benachrichtigungen erscheinen unabhängig von der Konsole d. Support-Technikers und im Vordergrund vor anderen Fenstern. Wenn der Popup-Hinweis aktiviert und nicht erzwungen oder unverwaltet ist, kann der Benutzer wählen, wie er die Popup-Hinweise erhalten möchte.

Persönliche Warteschlange - Neue Sitzungen, übertragene Sitzungen, freigegebene Sitzungen

Legen Sie fest, ob ein Benutzer eine Popup-Benachrichtigung für neue Sitzungen, übertragene Sitzungen und/oder freigegebene Sitzungen in dieser Warteschlange erhalten soll.

Team-Warteschlangen - Neue Sitzungen, übertragene Sitzungen, freigegebene Sitzungen, überfällige Sitzungen

Legen Sie fest, ob ein Benutzer eine Popup-Benachrichtigung für neue Sitzungen, übertragene Sitzungen, freigegebene Sitzungen und/oder überfällige Sitzungen in dieser Warteschlange erhalten soll.

Popup-Verhalten – Position und Dauer

Legen Sie die Standardposition und Dauer für Popup-Benachrichtigungen fest.

Sitzungszuweisungs-Alarme für Support-Sitzung Tech

Hörbare Alarme - einen Ton wiedergeben, wenn eine Sitzung zugewiesen wird

Legen Sie fest, ob ein Klang abgespielt werden soll, wenn eine Sitzung automatisch einem Benutzer zugewiesen wird.

Ton bei abgelaufener Zuweisung

Legen Sie fest, ob ein Klang abgespielt werden soll, wenn die Einladung zu einer automatisch zugewiesenen Sitzung vor dem Ablauf steht. Dieser Alarm kann entweder eine Audiodatei oder der Systemton sein. Falls nicht verwaltet oder falls aktiviert und nicht erzwungen, kann der Benutzer einen benutzerdefinierten Klang im WAV-Format festlegen, der nicht größer als 1 MB ist.

Support-Sitzung Techs

Automatisch Bildschirmfreigabe anfordern

Legen Sie fest, ob die Sitzungen Ihrer Benutzer nur mit dem Chat beginnen sollen, oder ob sofort eine Bildschirmfreigabe angefordert werden soll.

Automatisch lösen

Sitzungen können entweder als Registerkarten in der Konsole d. Support-Technikers oder aber automatisch als neue Fenster geöffnet werden.

Zum Heraufsetzen auffordern, wenn sicherer Desktop des Kunden aktiviert ist

In Situationen, in denen aufgrund des aktivierten sicheren Desktops Support-Probleme auftreten, können Sie es Ihren Benutzern gestatten, bei Beginn der Sitzung auf die Ausführung mit Administratorrechten heraufzusetzen.

Standardqualität

Legen Sie die Standardqualität für Bildschirmfreigabe-Sitzungen fest.

Standardskalierung

Legen Sie die Standardgröße für Bildschirmfreigabe-Sitzungen fest.

Automatisch auf Vollbildschirmmodus umschalten, wenn die Bildschirmfreigabe beginnt

Zu Beginn der Bildschirmfreigabe kann der Benutzer automatisch in den Vollbildschirmmodus wechseln.

Automatisch die Seitenleiste ausblenden, wenn der Vollbildschirmmodus verwendet wird

Wenn die Bildschirmfreigabe-Sitzung in den Vollbildschirmmodus wechselt, kann die Chat-Leiste automatisch ausgeblendet werden.

Eigenen Bildschirm anzeigen

Fenster bei Bildschirmanzeige automatisch minimieren

Wenn ein Benutzer während einer Sitzung einem Kunden seinen Bildschirm anzeigt, kann die Konsole d. Support-Technikers entweder offen belassen oder in die Task-Leiste des Benutzers minimiert werden.

Befehlsshell

Anzahl Zeilen des verfügbaren Befehlsverlaufs

Sie können die Anzahl der Zeilen festlegen, die im Befehlsshell-Verlauf gespeichert werden sollen. Als Standardwert sind 500 Zeilen festgelegt.

Speichern

Klicken Sie auf **Speichern**, um alle konfigurierten Profileinstellungen zu speichern. Oben auf der Seite wird die Bestätigungsnachricht **Einstellungsprofil erfolgreich bearbeitet** angezeigt. Alle Benutzer, die sich nach dem Speichern des neuen Profils in der Konsole d. Support-Technikers anmelden, erhalten die neuen Einstellungen als Standardeinstellungen.

Übernehmen von Konsole d. Support-Technikers-Einstellungen

Jetzt anwenden

Wenn Sie die Standardeinstellungen auf Ihre gesamte Nutzerbasis pushen möchten, klicken Sie auf **Jetzt übernehmen**. Oben auf der Seite wird die Bestätigungsnachricht **Einstellungsprofil wurde erfolgreich übernommen** angezeigt.

Nachdem die Einstellungen für Ihre Benutzerbasis übernommen wurden, erhalten die Benutzer eine Aufforderung zur Bestätigung, wenn sie sich nach der Übernahme der Einstellungen zum ersten Mal wieder in der Konsole d. Support-Technikers anmelden. Im Dialogfenster werden sie darüber informiert, dass die Einstellungen geändert wurden, und haben die Option, das Dialogfenster einfach zu schließen oder ihr Einstellungsfenster in der Konsole d. Support-Technikers zu öffnen, um die Änderungen zu prüfen.

Benutzerdefinierte Links: Hinzufügen von URL-Verknüpfungen zur Konsole d. Support-Technikers

Benutzerdefinierte Links

Erstellen Sie Links zu Websites, auf die Ihre Benutzer während Sitzungen zugreifen können. Dies können beispielsweise Links zu durchsuchbaren Wissensdatenbanken sein, wodurch Benutzer die Chance erhalten, eine Lösung für das Kundenproblem zu finden, oder ein Customer-Relationship-Management-System (CRM) mit Heraufsetzungsfunktionen. In diesem Fall könnte der Link das CRM-System auf einer Seite öffnen, auf der der Benutzer ein Heraufsetzungsformular für ein Team ausfüllen kann, das BeyondTrust nicht verwendet.

Hier erstellte Links werden über die Schaltfläche **Links** auf der Konsole d. Support-Technikers verfügbar.

Hinzufügen, Bearbeiten, Löschen

Erstellen Sie einen neuen Link, bearbeiten Sie einen bestehenden Link oder entfernen Sie einen bestehenden Link.

Benutzerdefinierten Link hinzufügen oder bearbeiten

Name

Erstellen Sie einen eindeutigen Namen, um diesen Link leichter zu identifizieren.

URL

Fügen Sie die URL hinzu, auf die dieser benutzerdefinierte Link verweisen soll. Verwenden Sie eines der unten auf der /login-Seite aufgeführten Makros, um den Text für Ihre Zwecke anzupassen.

> *Weitere Informationen finden Sie in Überblick über Support-Sitzungen Tech. und Tools unter https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/support-session-overview.htm.*

Vordefinierte Meldungen: Nachrichten für Chat erstellen

Konsole des Support-Technikers | VORDEFINIERTE MELDUNGEN

Für weitere Informationen siehe Während einer Sitzung mit dem Kunden chatten unter https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/chat.htm.

Vordefinierte Meldungen

Erstellen Sie vordefinierte Meldungen, die in Chat-Sitzungen verwendet werden. Mit vordefinierten Meldungen können Sie Ihre Reaktionszeit verringern und die Kommunikation zwischen Support-Technikern und Kunden standardisieren. Sie können die Ansicht filtern, indem Sie eine Kategorie oder ein Team aus der Dropdown-Liste oben auf der Seite wählen.

Hinzufügen, Bearbeiten, Löschen

Erstellen Sie eine neue Nachricht, bearbeiten Sie eine bestehende Nachricht oder entfernen Sie eine bestehende Nachricht.

Vordefinierte Meldungen hinzufügen oder bearbeiten

Titel

Erstellen Sie einen eindeutigen Namen, um diese Meldung leichter zu identifizieren.Dieser Name sollte Support-Technikern dabei helfen, die gewünschte Meldung zu lokalisieren.

Nachricht

Erstellen Sie den Text, der im Kunden-Chat angezeigt wird. Sie können BBCode verwenden, um geringfügige Formatierungsaufgaben wie Hinzufügen von Fettschrift, Farben oder Hyperlinks durchzuführen. Durch Klicken auf **Unterstützte BBCode-Formatierung** wird eine Liste der Codes und der sich daraus ergebenden Anwendungen angezeigt.

***Tipp:** Die Nachrichten sollten relativ kurz sein, damit sie ohne viel Bildlauf in den Fenstern des Kunden-Clients angezeigt werden können. Dies gilt für den nativen Client und die Click-to-Chat-Modi.*

Kategorie

Wählen Sie die Kategorie aus, unter der dieses Element aufgeführt werden soll.

Teamverfügbarkeit

Wählen Sie, welche Support-Teams dieses Element nutzen können sollen.

Kategorien vordefinierter Meldungen

Hinzufügen, Bearbeiten, Löschen

Erstellen Sie eine neue Kategorie, ändern Sie eine bestehende Kategorie oder entfernen Sie eine bestehende Kategorie.

Kategorie hinzufügen oder bearbeiten

Name

Erstellen Sie einen eindeutigen Namen, um diese Kategorie leichter zu identifizieren.Dieser Name sollte Support-Technikern dabei helfen, die gewünschte Meldung zu lokalisieren.

Übergeordnete Kategorie

Wählen Sie optional eine übergeordnete Kategorie zum Verschachteln von Kategorien aus.

Untergeordnete Kategorien

Zeigen Sie Namen von und Links zu untergeordneten Kategorien an.

Meldungen

Zeigen Sie Links zu Meldungen in dieser Kategorie an.

Vordefinierte Skripts: Skripte für Bildschirmfreigabe- oder Befehlsshell-Sitzungen erstellen

Vordefinierte Skripts

Erstellen Sie benutzerdefinierte Skripts, die in Bildschirmfreigabe- und Befehlsshell-Sitzungen verwendet werden. Das Skript wird während der Ausführung auf der Bildschirmfreigabe- oder Befehlsshell-Schnittstelle angezeigt. Das Ausführen eines Skriptes in der Bildschirmfreigabe-Schnittstelle zeigt das ausgeführte Skript auf dem Remote-Bildschirm an. Das Skript wird im Kontext des angemeldeten Benutzers ausgeführt, wenn die Sitzung nicht heraufgesetzt wurde, und wird als lokales System ausgeführt, wenn die Sitzung heraufgesetzt wurde. Sie können die Ansicht filtern, indem Sie eine Kategorie oder ein Team aus der Dropdown-Liste oben auf der Seite wählen.

Weitere Informationen finden Sie in Überblick über Support-Sitzungen Tech. und Tools unter https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/support-session-overview.htm.

Weitere Informationen finden Sie in Zugriff auf den Remote-Befehlsshell unter https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/command-shell.htm.

Hinzufügen, Bearbeiten, Löschen

Erstellen Sie ein neues Skript, bearbeiten Sie ein bestehendes Skript oder entfernen Sie ein bestehendes Skript.

Vordefinierte Skripts bearbeiten oder hinzufügen

Skriptname

Erstellen Sie einen eindeutigen Namen, um dieses Skript leichter zu identifizieren. Dieser Name sollte Benutzern dabei helfen, das gewünschte Skript ausfindig zu machen.

Beschreibung

Fügen Sie eine kurze Beschreibung hinzu, um den Zweck dieses Skripts zusammenzufassen. Die Beschreibung wird an der Eingabeaufforderung angezeigt, um zu bestätigen, dass der Benutzer das ausgewählte Skript ausführen möchte.

Befehlsreihenfolge

Schreiben Sie die Befehlsreihenfolge. Skripts müssen im Befehlszeilenformat verfasst werden, ähnlich wie beim Schreiben einer Stapeldatei oder eines Shellskripts. Bitte beachten: Nur die letzte Zeile des Skripts kann interaktiv sein. Sie können das Skript nicht pausieren, und eine Eingabeaufforderung kann sich nicht in der Mitte des Skripts befinden.

Verweisen Sie im Skript mit **"%RESOURCE_FILE%"** auf eine zugeordnete Ressourcendatei. Sie müssen dabei unbedingt die Anführungszeichen mit eingeben. Bitte achten Sie bei der Befehlsreihenfolge auf Groß- und Kleinschreibung.

Auf das temporäre Verzeichnis der Ressourcendatei greifen Sie über **%RESOURCE_DIR%** zu. Wenn Sie ein Skript mit einer zugeordneten Ressourcendatei ausführen, wird diese Datei temporär auf den Computer des Kunden hochgeladen.

Teamverfügbarkeit

Wählen Sie, welche Support-Teams dieses Element nutzen können sollen.

Kategorien

Wählen Sie die Kategorien aus, unter denen dieses Element aufgeführt werden soll.

Ressourcendatei

Sie können eine Ressourcendatei auswählen, die diesem Skript zugeordnet ist.

Heraufsetzungsmodus

Wählen Sie aus, ob das Skript nur zur Ausführung im heraufgesetzten Modus, im nicht heraufgesetzten Modus oder in beiden Modi verfügbar sein soll.

Verfügbar in der Bildschirmfreigabe im Nur-Ansicht-Modus als Sondervorgang

Wird diese Option aktiviert, kann dieses Skript auch dann ausgeführt werden, wenn der Benutzer den Remote-Computer nur anzeigen, aber nicht steuern darf. Beachten Sie: Wenn sich der Benutzer in der Nur-Anzeige-Bildschirmfreigabe befindet, erhält der Kunde eine Aufforderung zur Ausführung des Skripts.

> ***Hinweis:*** *Wenn dem Benutzer die Verwendung von vordefinierten Skripten gestattet ist, sind alle vordefinierten Skripte bei der Bildschirmfreigabe mit vollständiger Steuerung verfügbar, egal, ob diese Option aktiviert ist oder nicht.*

> *Weitere Informationen finden Sie in Bildschirmfreigabe bei Remote-Kunde für Anzeige und Steuerung unter https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/screen-sharing.htm.*

Kategorien

Kategorie hinzufügen, löschen

Erstellen Sie eine neue Kategorie oder entfernen Sie eine bestehende Kategorie.

Ressourcen

Ressource auswählen und hochladen

Fügen Sie alle Ressourcendateien hinzu, auf die Sie von Ihren Skripts aus zugreifen möchten. Die maximal zulässige Dateigröße ist 250 MB. Der maximale Speicherplatz für Ressourcen beträgt 1 GB.

Wenn Sie eine Ressourcendatei mit demselben Namen wie eine bestehende Ressourcendatei hochladen, erscheint eine Aufforderung, das Ersetzen der Datei zu bestätigen.

- Wenn Sie auf **JA** klicken, wird die aktualisierte Ressourcendatei hochgeladen und für alle anwendbaren vordefinierten Skripte verwendet.
- Wenn Sie auf **NEIN** klicken, wird die Datei nicht hochgeladen.

Löschen

Entfernen Sie eine bestehende Ressourcendatei.

Spezielle Aktionen: Erstellen von benutzerdefinierten speziellen Aktionen

Konsole des Support-Technikers | SPEZIELLE AKTIONEN

Weitere Informationen finden Sie in Bildschirmfreigabe bei Remote-Kunde für Anzeige und Steuerung unter https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/screen-sharing.htm.

Spezielle Aktionen

Erstellen Sie benutzerdefinierte spezielle Aktionen, um Ihre Prozesse zu beschleunigen. Benutzerdefinierte spezielle Aktionen können für Windows-, Mac- und Linux-Systeme erstellt werden.

Hinzufügen, Bearbeiten, Löschen

Erstellen Sie eine neue Aktion, bearbeiten Sie eine bestehende Aktion oder entfernen Sie eine bestehende Aktion.

Spezielle Aktion hinzufügen oder bearbeiten

Name des Vorgangs

Erstellen Sie einen eindeutigen Namen, um diese Aktion leichter zu identifizieren. In einer Sitzung kann ein Benutzer diesen Namen im Dropdown-Menü der speziellen Aktionen sehen.

Befehl

Geben Sie im Feld **Befehl** den vollen Pfad zur Anwendung an, die ausgeführt werden soll. Verwenden Sie keine Anführungszeichen. Diese werden bei Bedarf hinzugefügt. Windows-Systeme können die bereitgestellten Makros verwenden. Wenn der Befehl nicht auf dem Remote-System gefunden werden kann, erscheint diese benutzerdefinierte spezielle Aktion nicht in der Liste der speziellen Aktionen des Benutzers.

Argumente

Wenn der angegebene Befehl Befehlszeilenargumente akzeptiert, können Sie diese Argumente als nächstes eingeben. Argumente können bei Bedarf in Anführungszeichen stehen, und Argumente für Windows-Systeme können die bereitgestellten Makros verwenden.

Suchen Sie für weitere Informationen zu Windows-Argumenten mit dem Begriff „Befehlszeilenparameter" auf docs.microsoft.com/en-us/.

Bestätigen

Wenn Sie das Kontrollkästchen **Bestätigen** aktivieren, werden Benutzer dazu aufgefordert, die Ausführung der speziellen Aktion zu bestätigen, bevor diese ausgeführt wird. Ansonsten wird die benutzerdefinierte spezielle Aktion durch ihre Wahl aus dem Menü während einer Sitzung sofort ausgeführt.

Heraufgesetzt ausführen

Mit dem Aktivieren dieser Option erscheint diese spezielle Aktion nur, wenn der Kunden-Client im heraufgesetzten Modus ausgeführt wird. Wenn Sie eine benutzerdefinierte Aktion im heraufgesetzten Modus ausführen, werden Sie dazu aufgefordert, sie entweder als Systembenutzer auszuführen oder die Anmeldedaten für ein anderes gültiges Konto am Remote-System einzugeben.

Einstellungen für spezielle Aktionen

Integrierte Sondervorgänge anzeigen

Wenn Sie die von BeyondTrust bereitgestellten standardmäßigen speziellen Aktionen aktivieren möchten, aktivieren Sie das Kontrollkästchen **Integrierte spezielle Aktionen anzeigen**. Wählen Sie diese Option ansonsten ab, um nur Ihre benutzerdefinierten speziellen Aktionen zu aktivieren.

> ***Hinweis:*** *Die speziellen Aktionen* ***Windows-Sicherheit (Strg-Alt-Entf)*** *und* ***Betriebssteuerungsoptionen*** *können nicht deaktiviert werden. Außerdem führt das Deaktivieren der integrierten speziellen Aktionen nicht zur Deaktivierung der standardmäßigen speziellen Aktionen für Mobilgeräte.*

Benutzer und Sicherheit

Benutzer: Benutzerberechtigungen für einen Support-Techniker oder Admin hinzufügen

Benutzerkonten

Zeigen Sie Informationen über alle Benutzer an, die Zugriff auf Ihr B Series Appliance haben, einschließlich der lokalen Benutzer und aller Benutzer, die über die Integration des Sicherheitsanbieters Zugriff haben.

Hinzufügen, Bearbeiten, Löschen

Erstellen Sie ein neues Konto, bearbeiten Sie ein bestehendes Konto oder entfernen Sie ein bestehendes Konto. Ihr eigenes Konto können Sie nicht löschen.

Nach Benutzern suchen

Suchen Sie nach einem bestimmten Benutzer basierend auf **Zuletzt authentifiziert als**, **Öffentlicher Anzeigename**, **Privater Anzeigename** und **E-Mail-Adresse**.

Sicherheitsanbieter

Wählen Sie den Sicherheitsanbieter, den Sie durchsuchen wollen.

Synchronisieren

Synchronisieren Sie die Benutzer und Gruppen, die einem externen Sicherheitsanbieter zugewiesen wurden. Die Synchronisierung erfolgt automatisch einmal pro Tag. Mit Klick auf diese Schaltfläche erzwingen Sie eine manuelle Synchronisierung.

Sichtbare Spalten auswählen

Verwenden Sie das Dropdown-Menü, um auszuwählen, welche Spalten angezeigt werden sollen.

Benutzerkontenbericht

Exportieren Sie detaillierte Informationen über Ihre Benutzer zu Audit-Zwecken. Sammeln Sie detaillierte Informationen über alle Benutzer, Benutzer eines bestimmten Sicherheitsanbieters oder nur lokale Benutzer. Zu gesammelten Informationen gehören die unter der Schaltfläche „Details einblenden“ angezeigten Daten sowie Gruppenrichtlinien- und Team-Mitgliedschaften und Berechtigungen.

Hinzufügen oder Bearbeiten eines Nutzers

Klicken Sie nach der Bearbeitung auf **Speichern**, um Ihre Änderungen für diesen Benutzer zu speichern.

Benutzername

Eindeutige Kennung, die zur Anmeldung verwendet wird.

Anzeigename

Der Name des Benutzers, wie er auf der öffentlichen Website, in Chats usw. angezeigt wird. Benutzer können einen öffentlichen Anzeigenamen für den Kundenkontakt und einen privaten Anzeigenamen für die interne Kommunikation verwenden.

Anzeigenummer

Geben Sie eine eindeutige ID ein, oder lassen Sie dieses Feld leer, um die nächste verfügbare Nummer automatisch auszuwählen. Diese Nummer wirkt sich auf die Reihenfolge aus, in der Benutzer auf der öffentlichen Website aufgeführt werden.

Foto

Laden Sie das als Avatar des Support-Technikers zu verwendende Foto hoch, das im Chatfenster des Kunden-Client und in der **/login**-Verwaltungsschnittstelle angezeigt wird. Das Bild muss im .png- oder .jpeg-Format sein, nicht größer als 1 MB und mindestens 80x80 Pixel groß. Wählen Sie **Foto einstellen**, um ein Bild auszuwählen. Stellen Sie die Bildabmessungen mit dem Schieberegler und den Schaltflächen **An Fenster anpassen** und **Gesamtes Fenster ausfüllen** ein. Wenn Sie zufrieden sind, klicken Sie auf **Zuschneiden**, um es zu verwenden, oder auf **Abbrechen**, wenn Sie das gewählte Bild nicht behalten möchten. Klicken Sie auf **Foto ändern**, um ein neues Foto auszuwählen, oder auf **Foto löschen**, um den Avatar dieses Benutzers zu entfernen.

Das Foto kann auch über die Seite **/login > Mein Konto** geändert oder gelöscht werden.

Weitere Informationen finden Sie in Kunden-Client: Support-Sitzung Tech-Schnittstelle auf https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/customer-support-interface.htm.

E-Mail-Adresse

Legen Sie die E-Mail-Adresse fest, an die E-Mail-Benachrichtigungen gesendet werden, wie etwa Passwortzurücksetzungen oder Alarme zum erweiterten Verfügbarkeitsmodus.

Bevorzugte E-Mail-Sprache

Wenn mehr als eine Sprache für die Website aktiviert ist, legen Sie die Sprache fest, in der E-Mails versandt werden sollen.

Passwort

Passwort, das zusammen mit dem Benutzernamen zur Anmeldung verwendet wird. Das Passwort kann nach eigenen Wünschen festgelegt werden, solange die Zeichenfolge die definierte Richtlinie erfüllt, die auf der Seite **/login > Verwaltung > Sicherheit** festgelegt wurde.

Muss Passwort bei der nächsten Anmeldung zurücksetzen

Wenn diese Option ausgewählt wird, muss der Benutzer sein Passwort bei der nächsten Anmeldung zurücksetzen.

Passwort läuft niemals ab

Ist bei dieser Option ein Haken gesetzt, läuft das Passwort nie ab.

Passwort-Ablaufdatum

Führt dazu, dass das Passwort an einem bestimmten Datum abläuft.

Kontoeinstellungen

Zwei-Faktor-Authentifizierung: Anmelden mit einer Authentifikator-App:

Legen Sie fest, ob sich der Benutzer über eine Authentifizierungs-App anmelden muss oder ob dies optional ist (Standardeinstellung). Ist **Erforderlich** ausgewählt, wird, wenn sich dieser Benutzer das nächste Mal an der Verwaltungsschnittstelle oder der Konsole d. Support-Technikers anmeldet, ein Bildschirm angezeigt, dass die Zwei-Faktor-Authentifizierung aktiviert werden muss.

> *Weitere Informationen zu 2FA finden Sie in So verwenden Sie Zwei-Faktor-Authentifizierung mit BeyondTrust Remote Support auf www.beyondtrust.com/docs/remote-support/how-to/2-factor-authentication/.*

Das Konto läuft niemals ab

Ist bei dieser Option ein Haken gesetzt, läuft das Konto nie ab.

Konto-Ablaufdatum

Führt dazu, dass das Konto an einem bestimmten Datum abläuft.

Konto deaktiviert

Dadurch wird das Konto deaktiviert, sodass der Benutzer sich nicht anmelden kann. Durch das Deaktivieren wird das Konto NICHT gelöscht.

Berechtigt, ihre Anzeigenamen zu ändern

Ermöglicht es dem Benutzer, seinen Anzeigenamen zu ändern.

Berechtigt, ihr Bild zu ändern

Ermöglicht es Benutzern, ihre Avatarfotos zu ändern, die in der **/login**-Verwaltungsschnittstelle und im Chatfenster des Kunden-Client angezeigt werden.

Berechtigt, auf der öffentlichen Website anzuzeigen

Zeigt den Namen des Benutzers auf allen öffentlichen Websites an, auf denen die Support-Techniker-Liste aktiviert ist.

Kommentare

Fügen Sie Kommentare hinzu, die den Zweck dieses Kontos identifizieren.

Allgemeine Berechtigungen

Verwaltung

Administrator

Erteilt dem Benutzer volle Administratorrechte.

Zur Verwaltung von Vault berechtigt

Ermöglicht dem Benutzer die Verwaltung aller Aspekte des BeyondTrust Vault-Add-ons.

Berechtigt, Kennwörter festzulegen

Ermöglicht es dem Benutzer, für nicht-administrative lokale Benutzer Kennwörter festzulegen und Benutzerkonten freizuschalten.

Berechtigt, Jumpoints zu bearbeiten

Ermöglicht es dem Benutzer, Jumpoints zu erstellen oder zu bearbeiten. Diese Option wirkt sich nicht darauf aus, ob der Benutzer auf Remote-Computer über Jumpoints zugreifen kann, die einzeln oder über Gruppenrichtlinien konfiguriert werden.

Berechtigt, die öffentliche Website zu bearbeiten

Damit kann der Benutzer öffentliche Website-Konfigurationen erstellen und ändern, HTML-Vorlagen bearbeiten, die Übersetzungsschnittstelle anzeigen usw.

Berechtigt, Kundenhinweise zu bearbeiten

Gibt dem Benutzer die Möglichkeit, Meldungen zu erstellen und zu bearbeiten, mit denen Kunden beim Anfordern von Support über breitenwirksame IT-Ausfälle informiert werden.

Berechtigt, den Dateispeicher zu bearbeiten

Damit kann der Benutzer Dateien aus dem Dateispeicher entfernen oder Dateien hinzufügen.

Berechtigt, vordefinierte Meldungen zu bearbeiten

Ermöglicht es dem Benutzer, vordefinierte Chat-Nachrichten zu erstellen oder zu bearbeiten.

Berechtigt zum Bearbeiten technischer Support-Teams

Ermöglicht es dem Benutzer, Support-Teams zu erstellen oder zu bearbeiten.

Berechtigt, Jump-Gruppen zu bearbeiten

Ermöglicht es dem Benutzer, Jump-Gruppen zu erstellen oder zu bearbeiten.

Berechtigt, Probleme zu bearbeiten

Damit kann der Benutzer Probleme erstellen und bearbeiten.

Berechtigt, Qualifikationen zu bearbeiten

Damit kann der Benutzer Qualifikationen erstellen und bearbeiten.

Berechtigt, Support-Button-Profile zu bearbeiten

Ermöglicht es dem Benutzer, Support-Button-Profile anzupassen.

Berechtigt, vordefinierte Skripts zu bearbeiten

Damit kann der Benutzer vordefinierte Skripts für die Verwendung in Bildschirmfreigabe- oder Befehlsshell-Sitzungen erstellen oder bearbeiten.

Berechtigt, benutzerdefinierte Support-Techniker-Links zu bearbeiten

Ermöglicht es dem Benutzer, benutzerdefinierte Links zu erstellen oder zu bearbeiten.

Berechtigt, Zugriffssponsoren zu bearbeiten

Damit kann der Benutzer Zugriffssponsorenteams erstellen oder bearbeiten.

Berechtigt, iOS-Profile zu bearbeiten

Ermöglicht es dem Benutzer, Apple iOS-Profilinhalte zur Verteilung an Benutzer mit iOS-Geräten zu erstellen, zu bearbeiten und hochzuladen.

Bericht wird erstellt

Berechtigt, Support-Sitzung Tech-Berichte anzuzeigen

Ermöglicht dem Benutzer, Berichte zur Support-Sitzung Tech-Aktivität auszuführen, nur Sitzungen anzuzeigen, bei denen er der primäre Support-Techniker war, nur Sitzungen anzuzeigen, bei denen eines seiner Teams das primäre Team oder eines seiner Teammitglieder der primäre Support-Techniker war, oder alle Sitzungen anzuzeigen.

Berechtigt, Support-Sitzung Tech-Aufzeichnungen anzuzeigen

Damit kann der Benutzer Videoaufzeichnungen der Bildschirmfreigabe-, „Eigenen Bildschirm anzeigen“- und Befehlsshell-Sitzungen anzeigen.

Berechtigt, Lizenznutzungsberichte anzuzeigen

Damit kann der Benutzer Berichte zur BeyondTrust-Lizenznutzung erstellen.

Berechtigt, Vault-Berichte anzuzeigen

Ermöglicht dem Benutzer, Berichte zu Vault-Aktivitäten zu erstellen und dabei alle Ereignisdaten oder nur eigene Ereignisdaten anzuzeigen.

Berechtigt, Berichte zu Präsentationssitzungen anzuzeigen

Ermöglicht dem Benutzer, Berichte zur Präsentationsaktivität auszuführen, nur Präsentationen anzuzeigen, bei denen er der Moderator war, nur Sitzungen anzuzeigen, bei denen eines seiner Teammitglieder der Moderator war, oder alle Präsentationen anzuzeigen.

Berechtigt, Aufzeichnungen für Support-Sitzungen Tech. anzuzeigen

Damit kann der Benutzer Aufzeichnungen der Bildschirmfreigabe und Befehlsshell-Sitzungen anzeigen. Dies hat keine Auswirkung auf Aufzeichnungen von Präsentationen.

Berechtigt, Lizenznutzungsberichte anzuzeigen

Berechtigt den Benutzer, den Lizenzbericht für Support-Techniker anzuzeigen.

Berechtigt, Syslog-Berichte anzuzeigen

Ermöglicht dem Benutzer, eine ZIP-Datei mit allen auf dem Gerät vorhandenen Syslog-Dateien herunterzuladen. Administratoren müssen automatisch über Berechtigungen für den Zugriff auf diesen Bericht verfügen. Nicht-Administratorbenutzer müssen zum Anzeigen dieses Berichts den Zugriff anfordern.

Support-Technikerberechtigungen

Berechtigt, Remote-Support bereitzustellen

Damit kann der Benutzer die Konsole d. Support-Technikers verwenden, um Support-Sitzung Techen durchzuführen. Wenn Support aktiviert ist, sind auch Optionen für Remote-Support verfügbar. Deaktivieren Sie diese Einstellung für Nur-Präsentations-Benutzer.

Sitzungsverwaltung

Berechtigt, Sitzungsschlüssel für Support-Sitzung Tech innerhalb der Konsole d. Support-Technikers zu erstellen

Ermöglicht es dem Benutzer, Sitzungsschlüssel zu generieren, damit Kunden direkt Sitzungen mit ihm einleiten können.

> *Weitere Informationen finden Sie unter Einen Sitzungsschlüssel zum Starten einer Support-Sitzung generieren auf https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/session-keys.htm.*

Berechtigt, Zugriffsschlüssel zum Senden von iOS-Profilen zu erstellen

Ermöglicht es dem Benutzer, Zugriffsschlüssel zum Anbieten von iOS-Inhalten für Benutzer mit iOS-Geräten zu erstellen.

> *Weitere Informationen finden Sie in Einen Apple iOS-Profilzugriffsschlüssel generieren auf https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/apple-ios-access-key-management-interface.htm.*

Es können manuell Sitzungen aus einer Team-Warteschlange angenommen werden

Damit kann der Benutzer Sitzungen in einer seiner Teamwarteschlangen auswählen und starten.

> *Weitere Informationen finden Sie in Eine Sitzung zum Starten des Supports akzeptieren unter https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/accepting-a-session.htm.*

Berechtigt, Sitzungen an Teams zu übertragen, denen sie nicht angehören

Damit kann der Benutzer Sitzungen an andere Teams als seine eigenen übertragen. Bei Deaktivierung ist die Interaktion des Benutzers ausschließlich auf die ihm zugewiesenen Teams beschränkt.

> *Weitere Informationen finden Sie in Überblick über Support-Sitzungen Tech. und Tools unter https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/support-session-overview.htm.*

Berechtigt, Sitzungen für Teams freizugeben, denen sie nicht angehören

Ermöglicht es dem Benutzer, eine weniger stark beschränkte Gruppe von Benutzern zur Freigabe von Sitzungen einzuladen; nicht nur ihre Team-Mitglieder. In Kombination mit der Berechtigung Erweiterte Verfügbarkeit werden die Möglichkeiten zur Freigabe von Sitzungen durch diese Berechtigung ausgedehnt.

Weitere Informationen finden Sie in Überblick über Support-Sitzungen Tech. und Tools unter https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/support-session-overview.htm.

Berechtigt, externe Support-Techniker einzuladen

Damit kann der Benutzer Drittbenutzer dazu einladen, einmalig an einer Support-Sitzung Tech teilzunehmen.

Für weitere Informationen siehe Einladen eines externen Benutzers zur Teilnahme an einer Sitzung unter https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/rep-invite.htm.

Berechtigt zur Verwendung der Funktion „Nächste Sitzung aufrufen“

Damit kann der Benutzer durch einfachen Schaltflächenklick mit dem Support der ältesten Sitzung in der Warteschlange für seine Teams beginnen.

Weitere Informationen finden Sie in Eine Sitzung zum Starten des Supports akzeptieren unter https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/accepting-a-session.htm.

Aktivierung des erweiterten Verfügbarkeitsmodus zulassen

Ermöglicht es dem Benutzer, E-Mail-Einladungen von anderen Benutzern zu erhalten, die die Freigabe einer Sitzung anfordern, auch wenn sie nicht in der Konsole d. Support-Technikers angemeldet sind.

Weitere Informationen finden Sie in Verwenden der erweiterten Verfügbarkeit, um auch nach der Abmeldung einen Zugriff zu ermöglichen unter https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/extended-availability.htm.

Berechtigt, externen Schlüssel zu bearbeiten

Ermöglicht es dem Benutzer, den externen Schlüssel aus dem Fenster Sitzungsinformationen einer Sitzung innerhalb der Konsole d. Support-Technikers zu ändern.

Weitere Informationen finden Sie in Überblick über Support-Sitzungen Tech. und Tools unter https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/support-session-overview.htm.

Equilibrium

> *Weitere Informationen finden Sie in Handbuch für die automatische Sitzungsweiterleitung mit Equilibrium at https://www.beyondtrust.com/docs/remote-support/how-to/equilibrium/index.htm.*

Berechtigt zum Deaktivieren der Option zu Sitzungszuweisungen

Damit kann der Support-Techniker sich selbst als für Sitzungen nicht verfügbar markieren, die mit Equilibrium zugewiesen werden.

Keine Sitzungen zuweisen, wenn der Support-Techniker teilnimmt an mindestens

Damit wird die Mindestanzahl an Sitzungen festgelegt, die der Support-Techniker unterstützen muss, bevor Sitzungen nicht mehr automatisch mit Equilibrium zugewiesen werden.

Keine Sitzungen zuweisen, wenn der Support-Techniker untätig war für mindestens

Damit wird die Mindestzeit festgelegt, die der Support-Techniker untätig gewesen sein muss, bevor Sitzungen nicht mehr automatisch mit Equilibrium zugewiesen werden.

Techniker-zu-Techniker-Bildschirmfreigabe

> *Weitere Informationen finden Sie in Ihren Bildschirm für einen anderen Support-Techniker freigeben auf https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/representative-screensharing.htm.*

Berechtigt, anderen Support-Technikern den Bildschirm zu zeigen

Ermöglicht es dem Benutzer, seinen Bildschirm für einen anderen Benutzer freizugeben, ohne dass der empfangende Benutzer einer Sitzung beitreten muss. Diese Option ist auch dann verfügbar, wenn sich der Benutzer nicht in einer Sitzung befindet.

Berechtigt, die Steuerung zu gewähren, wenn anderen Support-Technikern der Bildschirm gezeigt wird

Ermöglicht es dem Benutzer, der seinen Bildschirm freigibt, die Steuerung von Tastatur und Maus dem Benutzer zu überlassen, der seinen Bildschirm anzeigt.

Support-Sitzung Techs

> *Weitere Informationen finden Sie in Überblick über Support-Sitzungen Tech. und Tools unter https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/support-session-overview.htm.*

Berechtigt zur Bereitstellung von Support-Buttonn in persönlicher Warteschlange

Ermöglicht es dem Benutzer, persönliche Support-Buttonn bereitzustellen und zu verwalten. Diese Einstellung wirkt sich auf die Bereitstellung von Support-Buttonn sowohl über die Webschnittstelle als auch die Konsole d. Support-Technikers aus. Um eine Support-Button innerhalb einer Sitzung bereitzustellen, muss die Sitzungsberechtigung **Bereitstellung vonSupport-Button** ebenfalls gewährt sein.

Team-Support-Buttons können verwaltet werden

Ermöglicht es dem Benutzer, die für seine eigenen Teams bereitgestellten Support-Buttonn zu ändern. Wenn der Benutzer Teamleiter oder -manager ist, kann er auch die persönlichen Support-Buttonn aller anderen Teammitglieder ändern.

> *Weitere Informationen finden Sie in Support-Buttone verwalten auf https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/support-schaltfläche-management-interface.htm.*

Berechtigt zur Änderung des dem Support-Button zugewiesenen öffentlichen Portals

Ermöglicht dem Benutzer, das öffentliche Portal festzulegen, über das sich eine Support-Button verbinden soll. Da Sitzungsrichtlinien auf öffentliche Portale angewandt werden können, kann sich die Änderung des Portals auf die in der Sitzung gestatteten Berechtigungen auswirken.

Team-Support-Buttonn können bereitgestellt werden

Ermöglicht es dem Benutzer, Team-Support-Buttonn für seine eigenen Teams bereitzustellen. Diese Einstellung wirkt sich auf die Bereitstellung von Support-Buttonn sowohl über die Webschnittstelle als auch die Konsole d. Support-Technikers aus. Um eine Support-Button innerhalb einer Sitzung bereitzustellen, muss die Sitzungsberechtigung **Support-ButtonBereitstellung von Support-Schaltflächen** ebenfalls gewährt sein.

Jump-Technologie

Gestattete Jump-Methoden

Ermöglicht es dem Benutzer, mit **Jump-Clients**, **lokalen Jumps**, **lokalen VNCs**, **RDP (lokal)**, **Remote-Jumps**, **Remote VNCs**, **RDP (Remote)**, **Shell Jumps**, und/oder **Intel vPro**-Jumps zu Computern durchzuführen.

Jump-Element-Rollen

Eine Jump-Element-Rolle ist ein vordefinierter Berechtigungssatz zur Verwaltung und Nutzung von Jump-Elementen. Klicken Sie für jede Option auf die Schaltfläche **Bearbeiten**, um die Jump-Element-Rolle in einer neuen Registerkarte zu öffnen.

Die **Standard**-Rolle wird nur verwendet, wenn **Benutzerstandard verwenden** für diesen Benutzer in einer Jump-Gruppe festgelegt wurde.

Die Rolle **Persönlich** gilt nur für Jump-Elemente, die auf der persönlichen Benutzerliste von Jump-Elementen fixiert wurden.

Die **Teams**-Rolle gilt für Jump-Elemente, die auf der persönlichen Liste von Jump-Elementen eines Teammitglieds mit niedrigerer Rolle fixiert wurden. Ein Team-Manager kann zum Beispiel die persönlichen Jump-Elemente von Teamleitern und Teammitgliedern anzeigen, während ein Teamleiter die persönlichen Jump-Elemente von Teammitgliedern anzeigen kann.

Die **System**-Rolle gilt für alle anderen Jump-Elemente im System. Für die meisten Benutzer sollte hier **Kein Zugriff** gewählt werden. Bei Wahl einer anderen Option wird der Benutzer zu Jump-Gruppen hinzugefügt, denen er normalerweise nicht zugeordnet werden würde. In der Konsole d. Support-Technikers kann dieser dann die persönlichen Listen von Jump-Elementen von Benutzern sehen, die keine Teammitglieder sind.

> *Weitere Informationen finden Sie in Verwenden von Jump-Element-Rollen, um Berechtigungssätze für Jump-Clients zu erstellen unter https://www.beyondtrust.com/docs/remote-support/how-to/jump-clients/jump-item-roles.htm.*

Präsentation

Berechtigt, Präsentationen zu leiten

Damit kann der Support-Techniker für einen oder mehrere Teilnehmer Präsentationen leiten.

> *Weitere Informationen finden Sie in Eine Präsentation für Remote-Teilnehmer abhalten unter https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/presentation.htm.*

Berechtigt, einem Präsentationsteilnehmer die Steuerung zu gewähren

Damit kann der Support-Techniker einem Teilnehmer während einer Präsentation die Steuerung über seinen Computer gewähren. Diese Einstellung wirkt sich nur auf Präsentationen und nicht auf die Funktion „Eigenen Bildschirm anzeigen“ einer Support-Sitzung Tech aus. Es kann nur jeweils ein Teilnehmer gleichzeitig die Steuerung übernehmen. Der Support-Techniker kann dies stets übersteuern.

> *Weitere Informationen siehe Präsentationsteilnehmer-Client: Einer Präsentation beitreten unter https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/customer-presentation-interface.htm.*

Konsole d. Support-Technikers

Zeitüberschreitung nach Inaktivität

Legt fest, wie lange der Support-Techniker inaktiv sein kann, bevor er von der Konsole d. Support-Technikers abgemeldet wird. Diese Berechtigung kann die seitenweit geltende Einstellung verwenden oder aber diese überschreiben.

Berechtigungen für überwachte und unüberwachte Sitzungen

Sitzungsrichtlinie

Legen Sie die Aufforderungs- und Berechtigungsregeln fest, die für die Sitzungen dieses Benutzers gelten sollen. Wählen Sie eine bestehende Sitzungsrichtlinie oder definieren Sie Ihre eigenen Berechtigungen für diesen Benutzer. Falls **Nicht definiert** gewählt wurde, wird die globale Standardrichtlinie verwendet. Diese Berechtigungen können von einer Richtlinie mit höherer Priorität überschrieben

werden.

Die gleichen Berechtigungen für unüberwachte Sitzungen verwenden

Um die gleichen Berechtigungen für sowohl überwachte wie auch unüberwachte Sitzungen zu verwenden, aktivieren Sie **Die gleichen Berechtigungen für unüberwachte Sitzungen verwenden**. Deaktivieren Sie dieses Kontrollkästchen, um Berechtigungen für überwachte und unüberwachte Sitzungen separat zu definieren. Sie können auch die Berechtigungen aus einer Kategorie in die andere kopieren.

Beschreibung

Zeigen Sie die Beschreibung einer vordefinierten Berechtigungsrichtlinie an.

Eingabeaufforderungen Support-Tool

> *Weitere Informationen erhalten Sie unter Kunden-Client: Schnittstelle für Support-Sitzungen Tech. unter https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/customer-support-interface.htm.*

Aufforderungsregeln

Wählen Sie, ob der Kunde bei Verwendung der untenstehenden Support-Funktionen um Genehmigung gebeten werden soll. Wählen Sie **Keine Aufforderung**, um niemals aufzufordern, **Immer auffordern**, um immer aufzufordern oder **Bei einigen Tools auffordern**, um zu wählen, für welche Berechtigungen aufgefordert werden soll. Wenn **Bei einigen Tools auffordern** gewählt wird, erscheint die Option **Kunde auffordern** neben jedem Tool, mit den Optionen **niemals** oder **immer** aufzufordern. Falls **Nicht definiert** gewählt wurde, wird diese Option durch die Richtlinie der nächstniedrigeren Priorität bestimmt. Diese Einstellung kann von einer Richtlinie mit höherer Priorität überschrieben werden.

Berechtigt, einmal aufzufordern

Wenn **Bildschirmfreigabe** auf **Anzeigen und steuern** festgelegt wurde und die Aufforderung aktiviert wurde, wird diese Option angezeigt. Aktivieren Sie das Kontrollkästchen, damit die Aufforderung zur Bildschirmfreigabe den Zugang zu allen Tools während der Sitzung anfordert, ohne weitere Aufforderungen.

Aufforderungsoptionen

Legen Sie fest, wie lange auf eine Antwort auf eine Aufforderung gewartet werden soll, bevor die Standardantwort **Ablehnen** oder **Zulassen** gewählt wird. Falls **Nicht definiert** gewählt wurde, wird diese Option durch die Richtlinie der nächstniedrigeren Priorität bestimmt. Diese Einstellung kann von einer Richtlinie mit höherer Priorität überschrieben werden.

Bildschirmfreigabe

Bildschirmfreigabe-Regeln

Ermöglicht es dem Benutzer, den Remote-Bildschirm anzuzeigen oder zu steuern. Falls **Nicht definiert** gewählt wurde, wird diese Option durch die Richtlinie der nächstniedrigeren Priorität bestimmt. Diese Einstellung kann von einer Richtlinie mit höherer Priorität

überschrieben werden.

> *Weitere Informationen finden Sie in Bildschirmfreigabe bei Remote-Kunde für Anzeige und Steuerung unter https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/screen-sharing.htm.*

Berechtigt, dem Kunden den eigenen Bildschirm anzuzeigen

Damit kann der Benutzer während einer Support-Sitzung Tech seinen Bildschirm für den Kunden freigeben. Diese Option ist verfügbar, wenn **Nur anzeigen** oder **Ansicht oder Steuerung** ausgewählt ist.

> *Weitere Informationen siehe Eigenen Bildschirm anzeigen: Umgekehrte Bildschirmfreigabe unter https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/show-my-screen.htm.*

Gestattete Kundeneinschränkungen

Legen Sie fest, ob der Support-Techniker Maus und Tastatur des Remote-Systems vorübergehend deaktivieren kann. Der Benutzer kann den Remote-Desktop auch daran hindern, angezeigt zu werden. Diese Option ist verfügbar, wenn **Anzeigen und steuern** ausgewählt ist. Wenn **Bildschirm, Maus und Tastatur** die ausgewählte Kundeneinschränkung ist, steht ein Kontrollkästchen zur Verfügung: **Bei Sitzungsbeginn automatisch einen privaten Bildschirm anfordern**. Der Bildschirm „Privatsphäre“ ist nur für Sitzungen verfügbar, die über einen Jump-Client, ein Remote Jump-Item oder ein lokales Jump-Item gestartet wurden. Wir empfehlen die Verwendung eines „Privatsphäre“-Bildschirms für unbeaufsichtigte Sitzungen. Das Remote-System muss den „Privatsphäre“-Bildschirm unterstützen.

> *Weitere Informationen siehe Eingeschränkte Kundeninteraktion: Privater Bildschirm, Remote-Eingaben deaktivieren unter https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/privacy-screen.htm.*

Aufforderungsverhalten bei Anwendungsfreigabe

Legen Sie fest, ob eine Anforderung zur Bildschirmfreigabe den Kunden immer oder nie dazu auffordern soll, die freizugebenden Anwendungen auszuwählen, oder ob der Benutzer wählen kann, ob eine Anwendungsfreigabe-Aufforderung erscheint oder nicht. Mit der Auswahl von **Immer** oder **Support-Techniker entscheidet** können Sie außerdem Anwendungsfreigabebeschränkungen vordefinieren.

> *Weitere Informationen siehe Anwendungsfreigabe: Einschränkung der für den Support-Techniker sichtbaren Elemente unter https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/application-sharing.htm.*

Synchronisierungsrichtung für Zwischenablage

Diese Option ist verfügbar, wenn **Anzeigen und steuern** ausgewählt ist. Wählen Sie, wie der Inhalt der Zwischenablage zwischen Support-Technikern und Endbenutzern ausgetauscht wird. Die Optionen sind:

- **Nicht berechtigt**: Der Support-Techniker darf die Zwischenablage nicht verwenden, es werden keine Zwischenablage-Symbole im Konsole d. Support-Technikers angezeigt, und die Befehle zum Ausschneiden und Einfügen funktionieren nicht.
- **Zulässig vom Support-Techniker zum Kunden:** Der Support-Techniker kann den Inhalt der Zwischenablage an den Kunden weiterleiten, kann aber nicht aus der Zwischenablage des Endbenutzers einfügen. Nur das Zwischenablage-Symbol Senden wird im Konsole d. Support-Technikers angezeigt.

- **Zulässig in beide Richtungen:** Der Inhalt der Zwischenablage kann in beide Richtungen übertragen werden. Beide Symbole Zwischenablage senden und abrufen werden im Konsole d. Support-Technikers angezeigt.

> *Weitere Informationen über den Zwischenablage-Synchronisationsmodus finden Sie unter „Sicherheit: Verwalten der Sicherheitseinstellungen“ auf Seite 236.*

Browserfreigabe

Browserfreigabe-Regeln

Damit kann der Benutzer die gleiche Website anzeigen, die der Kunde sieht, ohne die Kontrolle zu besitzen oder andere Anwendungen zu sehen. Falls **Nicht definiert** gewählt wurde, wird diese Option durch die Richtlinie der nächstniedrigeren Priorität bestimmt. Diese Einstellung kann von einer Richtlinie mit höherer Priorität überschrieben werden.

> *Weitere Informationen finden Sie in Bildschirmfreigabe bei Remote-Kunde für Anzeige und Steuerung unter https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/screen-sharing.htm.*

Anmerkungen

Anmerkungsregeln

Gibt dem Benutzer die Möglichkeit, Anmerkungswerkzeuge zu verwenden, um auf dem Bildschirm des Remote-Benutzers zu zeichnen. Falls **Nicht definiert** gewählt wurde, wird diese Option durch die Richtlinie der nächstniedrigeren Priorität bestimmt. Diese Einstellung kann von einer Richtlinie mit höherer Priorität überschrieben werden.

> *Weitere Informationen finden Sie in Verwenden von Anmerkungen, um auf dem Remote-Bildschirm zu zeichnen auf https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/annotations.htm.*

Dateitransfer

Dateitransfer-Regeln

Ermöglicht es dem Benutzer, Dateien auf das Remote-System hochzuladen, Dateien vom Remote-System herunterzuladen oder beides. Falls **Nicht definiert** gewählt wurde, wird diese Option durch die Richtlinie der nächstniedrigeren Priorität bestimmt. Diese Einstellung kann von einer Richtlinie mit höherer Priorität überschrieben werden.

Zugängliche Pfade im Dateisystem des Kunden

Gestattet es Benutzern, Dateien direkt zu oder von jeglichen oder nur von bestimmten Verzeichnissen auf dem Remote-System zu übertragen.

Zugängliche Pfade im Dateisystem des Support-Technikers

Gestattet es Benutzern, Dateien direkt zu oder von jeglichen oder nur von bestimmten Verzeichnissen auf seinem lokalen System zu übertragen.

> *Weitere Informationen finden Sie in Dateitransfer zum und vom Remote-System unter https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/file-transfer.htm.*

Befehlsshell

Befehlsshell-Regeln hier eingeben

Damit kann der Benutzer über eine virtuelle Befehlszeilen-Schnittstelle Befehle auf dem Remote-Computer ausgeben. Falls **Nicht definiert** gewählt wurde, wird diese Option durch die Richtlinie der nächstniedrigeren Priorität bestimmt. Diese Einstellung kann von einer Richtlinie mit höherer Priorität überschrieben werden.

> ***Hinweis:** Der Zugriff auf Befehlsshells kann in Shell Jump-Sitzungen nicht eingeschränkt werden.*

> *Weitere Informationen finden Sie in Zugriff auf den Remote-Befehlsshell unter https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/command-shell.htm.*

Systeminformationen

Regeln für Systeminformationen

Ermöglicht es dem Benutzer, Systeminformationen zum Remote-Computer anzuzeigen. Falls **Nicht definiert** gewählt wurde, wird diese Option durch die Richtlinie der nächstniedrigeren Priorität bestimmt. Diese Einstellung kann von einer Richtlinie mit höherer Priorität überschrieben werden.

Berechtigt, Aktionen zu Systeminformationen zu verwenden

Ermöglicht es dem Benutzer, mit Prozessen und Programmen auf dem Remote-System zu interagieren, ohne dass eine Bildschirmfreigabe erforderlich ist. Es können Prozesse beendet, Dienste gestartet, gestoppt, pausiert, fortgesetzt und neugestartet und Programme deinstalliert werden.

> *Weitere Informationen finden Sie in Anzeige von Systeminformationen unter https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/system-info.htm.*

Zugriff auf Registrierung

Verzeichniszugriff-Regeln

Ermöglicht es dem Benutzer, mit der Registrierung auf dem Remote-Windows-System zu interagieren, ohne dass eine Bildschirmfreigabe erforderlich ist. Schlüssel können angezeigt, hinzugefügt, gelöscht und bearbeitet, durchsucht und importiert werden.

> *Weitere Informationen finden Sie in Zugriff auf den Registrierungseditor am Remote-Endpunkt unter https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/registry-editor.htm.*

Vordefinierte Skripts

Regeln für vordefinierte Skripts

Damit kann der Benutzer vordefinierte Skripts ausführen, die für seine Teams erstellt wurden. Beachten Sie: Wenn sich der Benutzer in der Nur-Anzeige-Bildschirmfreigabe befindet, erhält der Kunde eine Aufforderung zur Ausführung des Skripts.Falls **Nicht definiert** gewählt wurde, wird diese Option durch die Richtlinie der nächstniedrigeren Priorität bestimmt. Diese Einstellung kann von einer Richtlinie mit höherer Priorität überschrieben werden.

> *Weitere Informationen finden Sie in Zugriff auf den Remote-Befehlsshell unter https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/command-shell.htm.*

Heraufsetzung

Heraufsetzungsregeln

Gibt dem Benutzer die Möglichkeit zu versuchen, den Kunden-Client so heraufzusetzen, dass er mit administrativen Rechten auf dem Remote-System ausgeführt wird. Falls **Nicht definiert** gewählt wurde, wird diese Option durch die Richtlinie der nächstniedrigeren Priorität bestimmt. Diese Einstellung kann von einer Richtlinie mit höherer Priorität überschrieben werden.

> *Weitere Informationen finden Sie in Den Client heraufsetzen auf https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/elevation.htm.*

Support-Button Bereitstellung

Support-Button Bereitstellungsregeln

Ermöglicht es dem Benutzer, während einer Sitzung eine Support-Button bereitzustellen oder zu entfernen. Die für die Bereitstellung verfügbaren Orte sind von den obigen Support-Button-Einstellungen abhängig. Falls **Nicht definiert** gewählt wurde, wird diese Option durch die Richtlinie der nächstniedrigeren Priorität bestimmt. Diese Einstellung kann von einer Richtlinie mit höherer Priorität überschrieben werden.

> *Weitere Informationen finden Sie in Überblick über Support-Sitzungen Tech. und Tools unter https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/support-session-overview.htm.*

Fixieren/Lösen von Jump-Clients

Regeln zum Fixieren/Lösen von Jump-Clients

Ermöglicht es dem Benutzer, während einer Sitzung einen Jump-Client zu fixieren oder zu lösen. Die für die Bereitstellung verfügbaren Orte sind von den obigen Jump-Client-Einstellungen abhängig. Falls **Nicht definiert** gewählt wurde, wird diese Option durch die Richtlinie der nächstniedrigeren Priorität bestimmt. Diese Einstellung kann von einer Richtlinie mit höherer Priorität überschrieben werden.

> *Weitere Informationen finden Sie in Überblick über Support-Sitzungen Tech. und Tools unter https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/support-session-overview.htm.*

Chat

> *Für weitere Informationen siehe Während einer Sitzung mit dem Kunden chatten unter https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/chat.htm.*

Chat-Regeln

Damit kann der Benutzer mit dem Remote-Kunden chatten. Falls **Nicht definiert** gewählt wurde, wird diese Option durch die Richtlinie der nächstniedrigeren Priorität bestimmt. Diese Einstellung kann von einer Richtlinie mit höherer Priorität überschrieben werden.

Berechtigt, URLs zum Webbrowser des Kunden zu pushen

Damit kann der Benutzer eine URL im Chat-Bereich eingeben und dann auf **URL pushen** klicken, um automatisch einen Webbrowser mit dieser Adresse auf dem Remote-Computer zu öffnen.

Berechtigt, Dateien mithilfe der Chat-Schnittstelle zu senden

Damit kann der Benutzer Dateien über die Chat-Schnittstelle senden.

> *Weitere Informationen erhalten Sie unter Kunden-Client: Schnittstelle für Support-Sitzungen Tech. unter https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/customer-support-interface.htm.*

Verhalten beim Beenden der Sitzung

Wenn die Verbindung innerhalb der unter **Neuverbindungs-Zeitüberschreitung** festgelegten Zeit nicht wiederhergestellt werden kann, legen Sie hier fest, wie verfahren werden soll. Um zu verhindern, dass ein Endbenutzer nach einer heraufgesetzten Sitzung auf unautorisierte Berechtigungen zugreift, stellen Sie den Client so ein, dass der Endbenutzer am Ende der Sitzung automatisch vom

Remote-Windows-Computer abgemeldet wird, dass der Remote-Computer gesperrt wird, oder dass nichts getan wird. Diese Regeln gelten nicht für Browser-Freigabesitzungen.

Benutzer berechtigen, diese Einstellung sitzungsweise außer Kraft zu setzen

Sie können einem Benutzer die Übersteuerung der Sitzungsbeendigungseinstellung über die Registerkarte **Zusammenfassung** in der Konsole während einer Sitzung gestatten.

Verfügbarkeitseinstellungen

Pool für Lizenzen für umfassenden Support

Wählen Sie den Lizenzpool, zu dem dieser Support-Techniker gehören soll. Wenn sich dieser Support-Techniker an der Konsole d. Support-Technikers anmeldet, wird eine Lizenz aus dem zugewiesenen Lizenzpool verbraucht. Wird **Keine** ausgewählt, kann sich der Support-Techniker nur an der Konsole d. Support-Technikers anmelden, wenn mindestens eine Lizenz aus den Lizenzpools noch nicht zugewiesen wurde und verfügbar ist.

Qualifikationen

Bezeichnet die diesem Benutzer zugewiesenen Qualifikationen. Wenn die Qualifikationsübereinstimmung für Equilibrium verwendet wird, werden Sitzungen dem Benutzer mit den besten Qualifikationen zur Handhabung dieses spezifischen Problems zugewiesen.

> *Weitere Informationen finden Sie in Qualifikationen Support-Technikern zuweisen unter https://www.beyondtrust.com/docs/remote-support/how-to/equilibrium/assign-skills-rep.htm.*

Anmeldungszeitplan

Zugang von Support-Technikern auf den folgenden Zeitplan beschränken

Legen Sie einen Zeitplan fest, der definiert, wann sich Benutzer an der Konsole d. Support-Technikers anmelden können. Legen Sie die Zeitzone fest, die für diesen Zeitplan verwendet werden soll, und fügen Sie dann einen oder mehrere Zeitplaneinträge hinzu. Geben Sie für jeden Eintrag das Startdatum und die Startuhrzeit an sowie das Enddatum und die Enduhrzeit.

Wenn die Zeit beispielsweise für 8 Uhr (Start) und 17 Uhr (Ende) festgelegt wird, kann sich ein Benutzer jederzeit innerhalb dieses Zeitfensters anmelden und auch nach dem festgelegten Endzeitpunkt weiterarbeiten. Er kann sich nach 17 Uhr allerdings nicht erneut anmelden.

Abmeldung erzwingen, wenn der Zeitplan die Anmeldung nicht gestattet

Wenn eine strengere Zugriffskontrolle erforderlich ist, aktivieren Sie diese Option. Damit wird der Benutzer gezwungen, sich zum geplanten Endzeitpunkt abzumelden. Iin diesem Fall erhält der Benutzer 15 Minuten vor der Trennung der Verbindung wiederholte Benachrichtigungen. Wenn der Benutzer abgemeldet wird, folgen jegliche ihm angehörenden Sitzungen den Regeln zum Sitzungsrückfall.

Benutzerkonten für Passwortrücksetzung: Support-Technikern gestatten, Benutzerkennwörter zu verwalten

Benutzerkonten

Administratoren können durch die Erteilung von Benutzerberechtigungen die Rücksetzung lokaler Benutzerkennwörter und gesperrter Benutzerkonten an berechtigte Benutzer delegieren, ohne diesen dabei den vollständigen Administratorzugang zu gewähren. Lokale Benutzer können ihre eigenen Kennwörter weiterhin zurücksetzen.

Wenn ein berechtigter Benutzer ohne Administratorrechte auf die Seite **Benutzer und Sicherheit > Benutzer** in der /login-Verwaltungsschnittstelle zugreift, wird er einen eingeschränkt sichtbaren **Benutzer**-Bildschirm sehen, welcher Links zur **Passwortänderung** für Benutzer ohne Administratorrechte enthält. Der berechtigte Benutzer kann Benutzerkonten nicht bearbeiten oder löschen. Berechtigten Benutzern ist es nicht gestattet, Administratorkennwörter oder die Kennwörter von Sicherheitsanbieter-Benutzern zurückzusetzen.

> ***Hinweis:*** *Administratoren mit der Berechtigung* ***Berechtigt, Kennwörter festzulegen*** *werden keinen Unterschied in der Benutzeroberfläche erkennen.*

Nach Benutzern suchen

Suchen Sie nach einem bestimmten Benutzer basierend auf **Zuletzt authentifiziert als**, **Öffentlicher Anzeigename**, **Privater Anzeigename** und **E-Mail-Adresse**.

Sichtbare Spalten auswählen

Verwenden Sie das Dropdown-Menü, um auszuwählen, welche Spalten angezeigt werden sollen.

Zurücksetzen

Wenn ein Benutzer einen oder mehr fehlgeschlagene Anmeldungsversuche aufweist, klicken Sie auf die Schaltfläche **Zurücksetzen** neben seinem Namen, um den Zähler zurück auf 0 zu setzen.

Passwort ändern

Ändern Sie das Passwort für einen nichtadministrativen Benutzer.

Passwort ändern

Benutzername

Eindeutige Kennung, die zur Anmeldung verwendet wird.Dieses Feld kann nicht bearbeitet werden.

Anzeigename

Der Name des Benutzers, wie er auf der öffentlichen Website, in Chats usw. angezeigt wird. Benutzer können einen öffentlichen Anzeigenamen für den Kundenkontakt und einen privaten Anzeigenamen für die interne Kommunikation verwenden.Dieses Feld kann nicht bearbeitet werden.

E-Mail-Adresse

Die E-Mail-Adresse, an die E-Mail-Benachrichtigungen, wie etwa Passwortrücksetzungen oder Alarme zum erweiterten Verfügbarkeitsmodus, gesendet werden. Dieses Feld kann nicht bearbeitet werden.

Kommentare

Kommentare zum Konto. Dieses Feld kann nicht bearbeitet werden.

Passwort

Das neue Passwort, das diesem Benutzerkonto zugewiesen werden soll. Das Passwort kann nach eigenen Wünschen festgelegt werden, solange die Zeichenfolge die definierte Richtlinie erfüllt, die auf der Seite **/login > Verwaltung > Sicherheit** festgelegt wurde.

Passwortrücksetzungslink per E-Mail an Benutzer senden

Senden Sie eine E-Mail an den Benutzer, die einen Link zum Zurücksetzen des Passworts für sein Konto enthält. Diese Funktion erfordert eine gültige SMTP-Konfiguration für Ihr B Series Appliance, die auf der Seite **/login > Verwaltung > E-Mail-Konfiguration** eingerichtet wird.

Muss Passwort bei der nächsten Anmeldung zurücksetzen

Wenn diese Option ausgewählt wird, muss der Benutzer sein Passwort bei der nächsten Anmeldung zurücksetzen.

Support-Techniker-Einladung: Erstellen Sie Profile, um externe Support-Techniker zu Sitzungen einzuladen

E-Mail-Einladung für Support-Techniker

Mit der Support-Techniker-Einladung kann ein berechtigter Benutzer einen externen Benutzer zur einmaligen Teilnahme an einer Sitzung einladen. Die Einladungs-E-Mail wird gesendet, wenn Sie den externen Support-Techniker zur Sitzung einladen.

Wählen Sie eine öffentliche Website zum Bearbeiten aus

Wählen Sie im Dropdown-Menü oben auf der Seite die öffentliche Website aus, für die Sie die Support-Techniker-E-Mail-Einladung bearbeiten möchten.

Betreff

Passen Sie den Betreff dieser E-Mail an. Sie können diesen Text für jegliche aktivierten Sprachen lokalisieren.

Text

Passen Sie den Text dieser E-Mail an. Verwenden Sie eines der unten auf der /login-Seite aufgeführten Makros, um den Text für Ihre Zwecke anzupassen.Sie können diesen Text für jegliche aktivierten Sprachen lokalisieren.

Für weitere Informationen siehe Einladen eines externen Benutzers zur Teilnahme an einer Sitzung unter https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/rep-invite.htm.

Sicherheitsanbieter: Aktivieren Sie LDAP, Active Directory, RADIUS, Kerberos, SAML für Support-Techniker und SAML für öffentliche Portale

Sicherheitsanbieter

Sie können Ihr BeyondTrust Appliance B Series für die Authentifizierung von Benutzern anhand bestehender LDAP-, RADIUS-, Kerberos- oder SAML-Server konfigurieren und Berechtigungen anhand der bereits vorhandenen Hierarchie und Gruppeneinstellungen zuweisen, die bereits auf Ihren Servern angegeben wurden. Kerberos ermöglicht die Einzelanmeldung, während RSA und andere Zwei-Faktor-Authentifizierungsmechanismen über RADIUS eine zusätzliche Sicherheitsstufe bieten.

Hinzufügen

Erstellen Sie eine neue Sicherheitsanbieter-Konfiguration. Wählen Sie aus dem Dropdown-Menü LDAP, Active Directory, RADIUS, Kerberos, SAML für Support-Techniker oder SAML für öffentliche Portale.

Reihenfolge ändern

Klicken Sie auf diese Schaltfläche, um die Priorität von Sicherheitsanbietern per Drag and Drop festzulegen. Verschieben Sie Server innerhalb eines Clusters. Cluster können auch als Ganzes durch Ziehen verschoben werden. Klicken Sie auf **Reihenfolge speichern**. Dadurch treten die Priorisierungsänderungen in Kraft.

Synchronisieren

Synchronisieren Sie die Benutzer und Gruppen, die einem externen Sicherheitsanbieter zugewiesen wurden. Die Synchronisierung erfolgt automatisch einmal pro Tag. Mit Klick auf diese Schaltfläche erzwingen Sie eine manuelle Synchronisierung.

Deaktivieren

Diese Sicherheitsanbieter-Verbindung deaktivieren. Dies ist für Routinewartungen hilfreich, bei denen ein Server offline genommen, aber nicht gelöscht werden soll.

Protokoll anzeigen

Sehen Sie sich den Statusverlauf für die Verbindung zu einem Sicherheitsanbieter an.

Bearbeiten, löschen

Bearbeiten Sie einen bestehenden Anbieter oder entfernen Sie einen bestehenden Anbieter.

> ***Hinweis:*** *Wenn Sie den lokalen Sicherheitsanbieter bearbeiten und eine Standardrichtlinie auswählen, die nicht über Administratorberechtigungen verfügt, wird eine Warnmeldung angezeigt. Vergewissern Sie sich, dass andere Benutzer über Administratorrechte verfügen, ehe Sie fortfahren.*

Knoten duplizieren

Erstellen Sie eine Kopie einer bestehenden, in einem Cluster befindlichen Sicherheitsanbieter-Konfiguration. Diese wird als neuer Knoten im gleichen Cluster hinzugefügt.

Auf Cluster upgraden

Stufen Sie einen Sicherheitsanbieter auf einen Sicherheitsanbieter-Cluster auf. Um diesem Cluster mehr Sicherheitsanbieter hinzuzufügen, kopieren Sie einen bestehenden Knoten.

Kopieren

Erstellen Sie eine Kopie einer bestehenden Sicherheitsanbieter-Konfiguration. Diese wird als Sicherheitsanbieter auf oberster Ebene und nicht als Teil eines Clusters hinzugefügt.

Sicherheitsanbieter hinzufügen oder bearbeiten: LDAP

Name

Erstellen Sie einen eindeutigen Namen, um diesen Anbieter leichter zu identifizieren.

Aktiviert

Falls aktiviert, kann Ihr BeyondTrust Appliance B Series diesen Sicherheitsanbieter durchsuchen, wenn ein Benutzer versucht, sich in der Konsole d. Support-Technikers oder in **/login** anzumelden. Falls nicht aktiviert, wird dieser Sicherheitsanbieter nicht durchsucht.

Benutzerauthentifizierung

Dadurch kann dieser Anbieter zur Authentifizierung von Benutzern verwendet werden. Wenn diese Option deaktiviert ist, kann dieser Anbieter nur zum Abrufen von Gruppen für Benutzerberechtigungen verwendet werden.

Benutzerinformationen mit LDAP-Server synchronisiert lassen

Die Anzeigenamen werden entsprechend der unten definierten **Benutzerschemaeinstellungen** festgelegt. Wenn Sie das Fotoattribut eines Benutzers synchronisieren möchten, muss diese Option aktiviert sein.

Autorisierungseinstellungen

Synchronisierung: LDAP-Objektzwischenspeicher aktivieren

Falls aktiviert, werden für das B Series Appliance sichtbare LDAP-Objekte nächtlich oder ggf. manuell synchronisiert. Bei der Verwendung dieser Option werden weniger Verbindungen zum LDAP-Server zu Verwaltungszwecken vorgenommen, was Geschwindigkeit und Effizienz zu Gute kommt.

Falls nicht aktiviert, sind Änderungen am LDAP-Server sofort verfügbar. Es ist keine Synchronisierung notwendig. Wenn Sie jedoch über die Verwaltungsschnittstelle Änderungen an Benutzerrichtlinien vornehmen, kann es zu kurzen LDAP-Verbindungen kommen.

Für Anbieter, die die Synchronisierungseinstellung zuvor aktiviert hatten, führt das Deaktivieren der Synchronisierungsoption zur Löschung aller zwischengespeicherter Einträge, die aktuell nicht verwendet werden.

Gruppen suchen

Wählen Sie, ob Sie diesen Sicherheitsanbieter nur für die Benutzerauthentifizierung, nur für Gruppensuchen oder für beides verwenden möchten. Die **Benutzerauthentifizierung** muss ausgewählt werden, wenn Sie die Gruppensuche deaktivieren möchten.

Standardmäßige Gruppenrichtlinie *(Nur sichtbar, wenn die Benutzerauthentifizierung gestattet wurde)*

Jeder Benutzer, der sich an einem externen Server authentifiziert, muss Mitglied mindestens einer Gruppenrichtlinie sein, damit er sich an Ihrem B Series Appliance authentifizieren, sich an der /login-Schnittstelle oder in der Konsole d. Support-Technikers anmelden kann. Sie können eine standardmäßige Gruppenrichtlinie wählen, die für alle Benutzer gelten soll, die sich am konfigurierten Server authentifizieren können.

> ***Hinweis:*** *Wird eine Standardrichtlinie definiert, hat potenziell jeder gestattete Benutzer, der sich an diesem Server authentifiziert, auf der Ebene dieser Standardrichtlinie Zugriff. Daher wird empfohlen, als Standardrichtlinie eine Richtlinie mit minimalen Berechtigungen festzulegen, damit Benutzer nicht Berechtigungen erhalten, die sie nicht besitzen sollen.*

> ***Hinweis:*** *Wenn sich ein Benutzer in einer standardmäßigen Gruppenrichtlinie befindet und dann zu einer anderen, spezifischen Gruppenrichtlinie hinzugefügt wird, gelten die Einstellungen für die spezifische Gruppenrichtlinie stets vor den Einstellungen der standardmäßigen Gruppenrichtlinie, auch dann, wenn die spezifische Richtlinie eine geringere Priorität hat als die standardmäßige Richtlinie und auch wenn die Einstellungen der standardmäßigen Gruppenrichtlinie kein Überschreiben von Einstellungen gestatten.*

Verbindungseinstellungen *(Nicht sichtbar für Cluster)*

Hostname

Geben Sie den Hostnamen des Servers ein, der Ihren externen Verzeichnisspeicher beinhaltet.

> ***Hinweis:*** *Wenn Sie **LDAPS** oder **LDAP mit TLS** verwenden, muss der Hostname mit dem Hostnamen im Betreffnamen des öffentlichen SSL-Zertifikats, das Ihr LDAP-Server verwendet, übereinstimmen, oder mit der DNS-Komponente des alternativen Betreffnamens.*

Port

Geben Sie den Port für Ihren LDAP-Server an. Dabei handelt es sich in der Regel um Port **389** für LDAP oder Port **636** für LDAPS. BeyondTrust unterstützt zudem Global Catalog über Port **3268** für LDAP oder **3269** für LDAPS.

Verschlüsselung

Wählen Sie den Verschlüsselungstyp zur Kommunikation mit dem LDAP-Server aus. Aus Sicherheitsgründen wird **LDAPS** oder **LDAP mit TLS** empfohlen.

> ***Hinweis:*** *Reguläres LDAP sendet und empfängt Daten in Klartext zum und vom LDAP-Server. Damit werden möglicherweise empfindliche Benutzerkontoinformationen gegenüber Packet-Sniffern anfällig. Sowohl LDAPS und LDAP mit TLS verschlüsseln Benutzerdaten bei der Übertragung. Diese Methoden werden daher anstelle des regulären LDAP empfohlen. LDAP mit TLS verwendet die StartTLS-Funktion, um eine Verbindung über Klartext-LDAP zu initiieren, setzt diese Verbindung dann jedoch zu einer verschlüsselten Verbindung herauf. LDAPS initiiert die Verbindung verschlüsselt und sendet keinerlei Daten in Klartext.*

Wenn Sie **LDAPS** oder **LDAP mit TLS** wählen, müssen Sie das oberste SSL-Zertifikat hochladen, das von Ihrem LDAP-Server verwendet wird. Dies ist nötig, um die Gültigkeit des Servers und die Sicherheit der Daten sicherzustellen. Das oberste Zertifikat muss im PEM-Format vorliegen.

> ***Hinweis:*** *Wenn der Betreffname oder die DNS-Komponente des alternativen Betreffnamens des öffentlichen SSL-Zertifikats für den LDAP-Server nicht mit dem Wert im Feld **Hostname** übereinstimmt, wird der Anbieter als unerreichbar behandelt. Sie können jedoch ein Wildcard-Zertifikat verwenden, um mehrere Subdomänen der gleichen Site zu zertifizieren. Zum Beispiel zertifiziert ein Zertifikat für ***.example.com** sowohl **support.beispiel.com** und **remote.example.com**.*

Anmeldedaten binden

Geben Sie einen Benutzernamen und ein Passwort an, das Ihr B Series Appliance an den LDAP-Verzeichnisspeicher binden kann, um diesen zu durchsuchen.

Wenn Ihr Server anonyme Bindungen gestattet, können Sie die Bindung auch ohne Angabe von Benutzername und Passwort durchführen. Anonyme Bindungen gelten als unsicher und sind standardmäßig an den meisten LDAP-Servern deaktiviert.

Verbindungsmethode

Wenn Sie einen externen Verzeichnisspeicher im gleichen lokalen Netzwerk wie Ihr BeyondTrust Appliance B Series verwenden, können die beiden Systeme möglicherweise direkt kommunizieren. In diesem Fall können Sie die Option **Proxy vom Gerät über den Connection Agent** deaktiviert lassen und mit der Einrichtung fortfahren.

Wenn die beiden Systeme nicht direkt miteinander kommunizieren können, z. B. wenn sich Ihr externer Verzeichnisserver hinter einer Firewall befindet, müssen Sie einen Connection Agent verwenden. Mit dem Herunterladen des Win32 Connection Agent ermöglichen Sie

Ihrem Verzeichnisserver und Ihrem B Series Appliance, über eine SSL-verschlüsselte, ausgehende Verbindung auch ohne Firewall-Konfiguration zu kommunizieren. Der Connection Agent kann entweder auf den Verzeichnisserver oder einen separaten Server im Netzwerk (empfohlen) heruntergeladen werden.

Aktivieren Sie im obigen Fall **Proxy vom Gerät über den Connection Agent**. Erstellen Sie ein **Passwort für Connection Agent** zur Verwendung im Installationsprozess für den Connection Agent. Klicken Sie dann auf **Connection Agent herunterladen**, führen Sie das Installationsprogramm aus und folgen Sie dem Installationsassistenten. Während der Installation werden Sie aufgefordert, den Namen des Sicherheitsanbieters und das Passwort für den Connection Agent einzugeben, das Sie oben erstellt haben.

Verzeichnistyp *(Nicht sichtbar für Cluster)*

Um die Konfiguration der Netzwerkverbindung zwischen Ihrem B Series Appliance und Ihrem Sicherheitsanbieter zu vereinfachen, können Sie einen Verzeichnistyp als Vorlage auswählen. Damit werden die untenstehenden Konfigurationsfelder mit Standarddaten vorausgefüllt. Diese müssen jedoch angepasst werden, um der spezifischen Konfiguration Ihres Sicherheitsanbieters zu entsprechen. Active Directory LDAP ist der am weitesten verbreitete Servertyp, aber Sie können BeyondTrust auch auf die Kommunikation mit den meisten Sicherheitsanbietern konfigurieren.

Cluster-Einstellungen *(nur für Cluster sichtbar)*

Mitgliederauswahl-Algorithmus

Wählen Sie die Methode zum Suchen der Knoten in diesem Cluster.

Von oben nach unten versucht zunächst, eine Verbindung zum Server mit der höchsten Priorität im Cluster herzustellen. Wenn dieser Server nicht verfügbar ist oder das Konto nicht gefunden wird, wird die Verbindung zum Server mit der nächsthöheren Priorität aufgebaut. So läuft die Suche durch die Liste der Cluster-Server, bis das Konto entweder gefunden oder festgestellt wird, dass das Konto auf keinem der angegebenen und verfügbaren Server existiert.

Round-Robin ist darauf ausgelegt, die Arbeitslast zwischen mehreren Servern auszugleichen. Der Algorithmus wählt zufällig einen ersten Server zum Verbindungsaufbau aus. Ist dieser Server nicht verfügbar oder das Konto wird nicht gefunden, wird auf Zufallsbasis ein anderer Server ausgewählt. Die Suche wird so durch die weiteren Server im Cluster zufällig fortgesetzt, bis das Konto entweder gefunden oder festgestellt wird, dass das Konto auf keinem der angegebenen und verfügbaren Server existiert.

Verzögerung Wiederholter Versuch

Legen Sie fest, wie lange mit dem nächsten Versuch gewartet werden soll, nachdem ein Cluster-Mitglied nicht mehr verfügbar ist.

Benutzerschema-Einstellungen

Cluster-Werte überschreiben *(nur für Cluster-Knoten sichtbar)*

Wenn diese Option deaktiviert bleibt, verwendet dieser Cluster-Knoten die gleichen Schemaeinstellungen wie der Cluster. Wird die Option aktiviert, können Sie die untenstehenden Schemaeinstellungen ändern.

Basis-DN suchen

Legen Sie die Ebene in Ihrer Verzeichnishierarchie fest (angegeben durch einen repräsentativen Namen), auf der das B Series Appliance mit der Benutzersuche beginnen soll. Abhängig von der Größe Ihres Verzeichnisspeichers und der Benutzer, die BeyondTrust-Konten erfordern, können Sie die Leistung verbessern, indem Sie die genaue Geschäftseinheit innerhalb Ihres Verzeichnisspeichers angeben,

die den Zugriff erfordert. Wenn Sie sich nicht sicher sind oder wenn Benutzer mehrere Geschäftseinheiten umspannen, können Sie auch den obersten repräsentativen Namen Ihres Verzeichnisspeichers angeben.

Benutzerabfrage

Geben Sie die Abfrageinformationen an, welche das B Series Appliance verwenden soll, um einen LDAP-Benutzer ausfindig zu machen, wenn dieser Benutzer versucht sich anzumelden. Das Feld **Benutzerabfrage** akzeptiert eine standardmäßige LDAP-Abfrage (RFC 2254 – „String Representation of LDAP Search Filters“). Sie können die Abfrage-Zeichenfolge ändern und so bestimmen, wie sich Ihre Benutzer anmelden und welche Arten von Benutzernamen akzeptiert werden. Um den Wert innerhalb der Zeichenfolge anzugeben, der als Benutzername dienen soll, ersetzen Sie diesen Wert mit *****.

Navigationsanfrage

Beim Durchsuchen über Gruppenrichtlinien beeinflusst die Durchsuchen-Abfrage, wie Ergebnisse angezeigt werden. Damit werden Ergebnisse so gefiltert, dass nur bestimmte Ergebnisse im Dropdown-Menü der Mitgliedsauswahl angezeigt werden, wenn Sie Mitglieder zu einer Gruppenrichtlinie hinzufügen.

Objektklassen

Geben Sie gültige Objektklassen für einen Benutzer in Ihrem Verzeichnisspeicher an. Nur Benutzern mit mindestens einer dieser Objektklassen ist die Authentifizierung gestattet. Diese Objektklassen werden auch mit den untenstehenden Attributnamen verwendet, um für Ihr B Series Appliance das Schema zu kennzeichnen, das der LDAP-Server zur Identifizierung von Benutzern verwendet. Sie können mehrere Objektklassen eingeben, eine pro Zeile.

Attributnamen

Geben Sie an, welche Felder für die eindeutige ID und den Anzeigenamen eines Benutzers verwendet werden sollen.

Eindeutige ID

Dieses Feld benötigt eine eindeutige Kennung für das Objekt. Auch wenn der repräsentative Name als diese ID dienen kann, kann sich der repräsentative Name eines Benutzers im Laufe der Zeit häufig ändern, etwa aufgrund von Namens- oder Standortänderungen oder durch die Umbenennung des LDAP-Speichers. Daher verwenden die meisten LDAP-Server ein Feld, das pro Objekt einzigartig ist und sich für die gesamte Lebenszeit des Benutzers nicht ändert. Wenn Sie den repräsentativen Namen als einzigartige ID verwenden und sich der repräsentative Name eines Benutzers ändert, wird dieser Benutzer als neuer Benutzer angesehen und jegliche Änderungen, die am BeyondTrust-Benutzerkonto dieser Person vorgenommen werden, werden nicht auf den neuen Benutzer übernommen. Wenn Ihr LDAP-Server keine einzigartige Kennung verwendet, verwenden Sie ein Feld, das nicht zu einem identischen Eintrag bei einem anderen Benutzer führen wird.

E-Mail

Das E-Mail-Attribut synchronisiert die Benutzer-E-Mail-Adresse über LDAP. Bitte beachten Sie, dass die Sonderzeichen **?** und **!** nicht verwendet werden können.

Foto

Dieses Feld ermöglicht Ihnen die Konfiguration von LDAP-Anbietern zur Synchronisierung von Support-Techniker-Fotos über LDAP. Standardmäßig verwenden die Einstellungsvorlagen für Active Directory, Novell eDirectory und OpenLDAP alle das Attribut ***:jpegPhoto**. Administratoren können das Attribut bei Bedarf ändern. Wird kein Attribut angegeben, werden keine Fotos von LDAP abgerufen.

Fotos in LDAP müssen als JPEG-Bilder gespeichert werden, entweder als Rohbinär- oder Base64-enkodierte Daten. BeyondTrust Remote Support erkennt das Format der Verschlüsselung automatisch und entschlüsselt die Fotos nach Bedarf.

Verwenden des gleichen Attributs für öffentliche und private Anzeigenamen

Ist diese Option aktiviert, können Sie separate Werte für die privaten und öffentlichen Anzeigenamen des Benutzers angeben.

Anzeigename

Diese Felder legen fest, welche Felder als die privaten und öffentlichen Anzeigenamen des Benutzers verwendet werden.

Gruppenschemaeinstellungen *(Nur bei der Durchführung von Gruppensuchen sichtbar)*

Basis-DN suchen

Legen Sie die Ebene in Ihrer Verzeichnishierarchie fest (angegeben durch einen repräsentativen Namen), auf der das B Series Appliance mit der Gruppensuche beginnen soll. Abhängig von der Größe Ihres Verzeichnisspeichers und der Gruppen, welche Zugriff auf das B Series Appliance erfordern, können Sie die Leistung verbessern, indem Sie die genaue Geschäftseinheit innerhalb Ihres Verzeichnisspeichers angeben, welche den Zugriff erfordert. Wenn Sie sich nicht sicher sind oder wenn Gruppen mehrere Geschäftseinheiten beinhalten, können Sie auch den obersten repräsentativen Namen Ihres Verzeichnisspeichers angeben.

Navigationsanfrage

Beim Durchsuchen über Gruppenrichtlinien beeinflusst die Durchsuchen-Abfrage, wie Ergebnisse angezeigt werden. Damit werden Ergebnisse so gefiltert, dass nur bestimmte Ergebnisse im Dropdown-Menü der Mitgliedsauswahl angezeigt werden, wenn Sie Mitglieder zu einer Gruppenrichtlinie hinzufügen.

Objektklassen

Geben Sie gültige Objektklassen für eine Gruppe innerhalb Ihres Verzeichnisspeichers an. Nur Gruppen mit mindestens einer dieser Objektklassen werden zurückgegeben. Diese Objektklassen werden auch mit den untenstehenden Attributnamen verwendet, um für Ihr B Series Appliance zu kennzeichnen, welches Schema der LDAP-Server zum Identifizieren von Gruppen verwendet. Sie können mehrere Gruppenobjektklassen eingeben, eine pro Zeile.

Attributnamen

Geben Sie an, welche Felder für die eindeutige ID und den Anzeigenamen einer Gruppe verwendet werden sollten.

Eindeutige ID

Dieses Feld benötigt eine eindeutige Kennung für das Objekt. Auch wenn der repräsentative Name als diese ID dienen kann, kann sich der repräsentative Name einer Gruppe im Laufe der Zeit häufig ändern, etwa aufgrund von Standorträderungen oder durch die Umbenennung des LDAP-Speichers. Daher verwenden die meisten LDAP-Server ein Feld, das pro Objekt einzigartig ist und sich für die gesamte Lebenszeit der Gruppe nicht ändert. Wenn Sie den repräsentativen Namen als einzigartige ID verwenden und sich der repräsentative Name eine Gruppe ändert, wird diese Gruppe als neue Gruppe angesehen und jegliche Gruppenrichtlinien, die für diese Gruppe definiert wurden, werden nicht für die neue Gruppe übernommen. Wenn Ihr LDAP-Server keine einzigartige Kennung verwendet, verwenden Sie ein Feld, das nicht zu einem identischen Eintrag bei einer anderen Gruppe führen wird.

Anzeigename

Dieser Wert legt fest, welches Feld als Anzeigename der Gruppe verwendet werden soll.

Benutzer-zu-Gruppen-Beziehungen

Beziehungen

Dieses Feld fordert eine Abfrage an, um festzustellen, welche Benutzer welchen Gruppen zugehören oder welche Gruppen welche Benutzer enthalten.

Rekursive Gruppensuche durchführen

Sie können eine rekursive Suche für Gruppen durchführen. Damit wird eine Abfrage für einen Benutzer durchgeführt; daraufhin werden alle Gruppen abgefragt, zu denen dieser Benutzer gehört; daraufhin werden alle Gruppen abgefragt, zu denen diese Gruppen gehören und so weiter, bis alle möglichen mit diesem Benutzer assoziierten Gruppen gefunden wurden.

Die Ausführung einer rekursiven Suche kann sich beträchtlich auf die Leistung auswirken, da der Server weiter Abfragen durchführt, bis Informationen zu allen Gruppen gefunden wurden. Dauert dies zu lange, können sich Benutzer möglicherweise nicht anmelden.

Eine nichtrekursive Suche führt nur eine Abfrage pro Benutzer durch. Wenn Ihr LDAP-Server ein spezielles Feld besitzt, das alle Gruppen enthält, zu denen der Benutzer gehört, ist die rekursive Suche nicht nötig. Die rekursive Suche ist ebenfalls nicht nötig, wenn Ihr Verzeichnis-Design Gruppenmitglieder von Gruppen nicht berücksichtigt.

Einstellungen testen

Benutzername und Passwort

Geben Sie einen Benutzernamen und ein Passwort für ein Konto ein, das auf dem zu testenden Server existiert. Dieses Konto muss die in der obigen Konfiguration angegebenen Anmeldungskriterien erfüllen.

Es wird versucht, Benutzerattribute und Gruppenmitgliedschaften abzurufen, wenn die Anmeldedaten angenommen werden.

Wird diese Option aktiviert, versucht der erfolgreiche Anmeldedatentest auch, die Benutzerattribute und Gruppensuche zu prüfen.

> ***Hinweis:*** *Für den erfolgreichen Test dieser Funktionen müssen diese in Ihrem Sicherheitsanbieter unterstützt und konfiguriert sein.*

Testen

Wenn Ihr Server ordnungsgemäß konfiguriert ist und Sie einen gültigen Benutzernamen und ein Passwort zum Testen eingegeben haben, erhalten Sie eine positive Meldung. Andernfalls sehen Sie eine Fehlermeldung und ein Protokoll, das bei der Fehlerbehebung helfen kann.

Weitere Informationen finden Sie in LDAP-Sicherheitsanbieter erstellen und konfigurieren unter https://www.beyondtrust.com/docs/remote-support/how-to/integrations/security-providers/ldap-users/configure-settings.htm.

Sicherheitsanbieter hinzufügen oder bearbeiten: RADIUS

Name

Erstellen Sie einen eindeutigen Namen, um diesen Anbieter leichter zu identifizieren.

Aktiviert

Falls aktiviert, kann Ihr BeyondTrust Appliance B Series diesen Sicherheitsanbieter durchsuchen, wenn ein Benutzer versucht, sich in der Konsole d. Support-Technikers oder in **/login** anzumelden. Falls nicht aktiviert, wird dieser Sicherheitsanbieter nicht durchsucht.

Anzeigenamen mit Remote-System synchronisiert lassen

Diese Felder legen fest, welche Felder als die privaten und öffentlichen Anzeigenamen des Benutzers verwendet werden.

Autorisierungseinstellungen

Nur die folgenden Benutzer zulassen

Sie können den Zugriff nur bestimmten Benutzern auf Ihrem RADIUS-Server gewähren. Jeder Benutzername sollte dabei durch einen Zeilenumbruch getrennt werden. Nach der Eingabe stehen diese Benutzer über das Dialogfeld **Richtlinienmitglied hinzufügen** bei der Bearbeitung von Gruppenrichtlinien auf der Seite **/login > Benutzer und Sicherheit > Gruppenrichtlinien** zur Verfügung.

Wenn Sie dieses Feld leer lassen, werden alle Benutzer zugelassen, die sich über Ihren RADIUS-Server authentifizieren. Wenn Sie alle Benutzer zulassen, müssen Sie außerdem eine standardmäßige Gruppenrichtlinie angeben.

Standardmäßige Gruppenrichtlinie

Jeder Benutzer, der sich an einem externen Server authentifiziert, muss Mitglied mindestens einer Gruppenrichtlinie sein, damit er sich an Ihrem B Series Appliance authentifizieren, sich an der /login-Schnittstelle oder in der Konsole d. Support-Technikers anmelden kann. Sie können eine standardmäßige Gruppenrichtlinie wählen, die für alle Benutzer gelten soll, die sich am konfigurierten Server authentifizieren können.

LDAP-Gruppensuche

Wenn Benutzer dieses Sicherheitsanbieters ihren Gruppen auf einem separaten LDAP-Server zugewiesen werden sollen, wählen Sie einen oder mehrere LDAP-Gruppenserver, die zur Gruppensuche verwendet werden sollen.

Verbindungseinstellungen

Hostname

Geben Sie den Hostnamen des Servers ein, der Ihren externen Verzeichnisspeicher beinhaltet.

Port

Geben Sie den Authentifizierungsport für Ihren RADIUS-Server an. Dies ist in der Regel **1812**.

Zeitüberschreitung (Sekunden)

Maximale Wartezeit, für die auf eine Antwort vom Server gewartet werden soll. Beachten Sie: Bei einer Antwort vom Typ **Response-Accept** oder **Response-Challenge** wird RADIUS den gesamten hier angegebenen Zeitraum über warten, bevor das Konto authentifiziert wird. Daher empfehlen wir, diesen Wert abhängig von Ihren Netzwerkeinstellungen so gering wie möglich zu halten. Ein idealer Wert ist 3-5 Sekunden, mit einem Maximalwert von drei Minuten.

Verbindungsmethode

Wenn Sie einen externen Verzeichnisspeicher im gleichen lokalen Netzwerk wie Ihr BeyondTrust Appliance B Series verwenden, können die beiden Systeme möglicherweise direkt kommunizieren. In diesem Fall können Sie die Option **Proxy vom Gerät über den Connection Agent** deaktiviert lassen und mit der Einrichtung fortfahren.

Wenn die beiden Systeme nicht direkt miteinander kommunizieren können, z. B. wenn sich Ihr externer Verzeichnisserver hinter einer Firewall befindet, müssen Sie einen Connection Agent verwenden. Mit dem Herunterladen des Win32 Connection Agent ermöglichen Sie Ihrem Verzeichnisserver und Ihrem B Series Appliance, über eine SSL-verschlüsselte, ausgehende Verbindung auch ohne Firewall-Konfiguration zu kommunizieren. Der Connection Agent kann entweder auf den Verzeichnisserver oder einen separaten Server im Netzwerk (empfohlen) heruntergeladen werden.

Aktivieren Sie im obigen Fall **Proxy vom Gerät über den Connection Agent**. Erstellen Sie ein **Passwort für Connection Agent** zur Verwendung im Installationsprozess für den Connection Agent. Klicken Sie dann auf **Connection Agent herunterladen**, führen Sie das Installationsprogramm aus und folgen Sie dem Installationsassistenten. Während der Installation werden Sie aufgefordert, den Namen des Sicherheitsanbieters und das Passwort für den Connection Agent einzugeben, das Sie oben erstellt haben.

Gemeinsamer geheimer Schlüssel

Geben Sie einen neuen gemeinsamen geheimen Schlüssel an, damit Ihr B Series Appliance mit Ihrem RADIUS-Server kommunizieren kann.

Cluster-Einstellungen *(nur für Cluster sichtbar)*

Mitgliederauswahl-Algorithmus

Wählen Sie die Methode zum Suchen der Knoten in diesem Cluster.

Von oben nach unten versucht zunächst, eine Verbindung zum Server mit der höchsten Priorität im Cluster herzustellen. Wenn dieser Server nicht verfügbar ist oder das Konto nicht gefunden wird, wird die Verbindung zum Server mit der nächsthöheren Priorität aufgebaut. So läuft die Suche durch die Liste der Cluster-Server, bis das Konto entweder gefunden oder festgestellt wird, dass das Konto auf keinem der angegebenen und verfügbaren Server existiert.

Round-Robin ist darauf ausgelegt, die Arbeitslast zwischen mehreren Servern auszugleichen. Der Algorithmus wählt zufällig einen ersten Server zum Verbindungsaufbau aus. Ist dieser Server nicht verfügbar oder das Konto wird nicht gefunden, wird auf Zufallsbasis ein anderer Server ausgewählt. Die Suche wird so durch die weiteren Server im Cluster zufällig fortgesetzt, bis das Konto entweder gefunden oder festgestellt wird, dass das Konto auf keinem der angegebenen und verfügbaren Server existiert.

Verzögerung Wiederholter Versuch

Legen Sie fest, wie lange mit dem nächsten Versuch gewartet werden soll, nachdem ein Cluster-Mitglied nicht mehr verfügbar ist.

Einstellungen testen

Benutzername und Passwort

Geben Sie einen Benutzernamen und ein Passwort für ein Konto ein, das auf dem zu testenden Server existiert. Dieses Konto muss die in der obigen Konfiguration angegebenen Anmeldungskriterien erfüllen.

Es wird versucht, Benutzerattribute und Gruppenmitgliedschaften abzurufen, wenn die Anmeldedaten angenommen werden.

Wird diese Option aktiviert, versucht der erfolgreiche Anmeldedatentest auch, die Benutzerattribute und Gruppensuche zu prüfen.

> ***Hinweis:*** *Für den erfolgreichen Test dieser Funktionen müssen diese in Ihrem Sicherheitsanbieter unterstützt und konfiguriert sein.*

Testen

Wenn Ihr Server ordnungsgemäß konfiguriert ist und Sie einen gültigen Benutzernamen und ein Passwort zum Testen eingegeben haben, erhalten Sie eine positive Meldung. Andernfalls sehen Sie eine Fehlermeldung und ein Protokoll, das bei der Fehlerbehebung helfen kann.

> *Weitere Informationen finden Sie in Erstellen und Konfigurieren des RADIUS-Sicherheitsanbieters unter https://www.beyondtrust.com/docs/remote-support/how-to/integrations/security-providers/radius/configure-settings.htm.*

Sicherheitsanbieter hinzufügen oder bearbeiten: Kerberos

Name

Erstellen Sie einen eindeutigen Namen, um diesen Anbieter leichter zu identifizieren.

Aktiviert

Falls aktiviert, kann Ihr BeyondTrust Appliance B Series diesen Sicherheitsanbieter durchsuchen, wenn ein Benutzer versucht, sich in der Konsole d. Support-Technikers oder in **/login** anzumelden. Falls nicht aktiviert, wird dieser Sicherheitsanbieter nicht durchsucht.

Anzeigenamen mit Remote-System synchronisiert lassen

Diese Felder legen fest, welche Felder als die privaten und öffentlichen Anzeigenamen des Benutzers verwendet werden.

Realm aus Principal-Namen entfernen

Wählen Sie diese Option, um den REALM-Teil aus dem Benutzer-Principal-Namen zu entfernen, wenn Sie den BeyondTrust-Benutzernamen erstellen.

Autorisierungseinstellungen

Benutzer-Bearbeitungsmodus

Wählen Sie, welche Benutzer sich an Ihrem BeyondTrust Appliance B Series authentifizieren können. **Alle Benutzer zulassen** gestattet es allen, die sich aktuell über Ihr Key Distribution Center (KDC) authentifizieren. **Nur in der Liste angegebene Benutzer-Principals zulassen** gestattet nur ausdrücklich angegebene Benutzer-Principals. **Nur Benutzer-Principals, die mit der Regex übereinstimmen, zulassen** gestattet nur Benutzer-Principals, die mit einem Perl-kompatiblen regulären Ausdruck (PCRE) übereinstimmen.

Standardmäßige Gruppenrichtlinie

Jeder Benutzer, der sich an einem externen Server authentifiziert, muss Mitglied mindestens einer Gruppenrichtlinie sein, damit er sich an Ihrem B Series Appliance authentifizieren, sich an der /login-Schnittstelle oder in der Konsole d. Support-Technikers anmelden kann. Sie können eine standardmäßige Gruppenrichtlinie wählen, die für alle Benutzer gelten soll, die sich am konfigurierten Server authentifizieren können.

SPN-Bearbeitungsmodus

Nur in der Liste angegebene SPNs zulassen

Falls deaktiviert, sind alle konfigurierten Service Principal Names (SPNs) für diesen Sicherheitsanbieter gestattet. Falls aktiviert, wählen Sie bestimmte SPNs aus einer Liste aktuell konfigurierter SPNs.

LDAP-Gruppensuche

Wenn Benutzer dieses Sicherheitsanbieters ihren Gruppen auf einem separaten LDAP-Server zugewiesen werden sollen, wählen Sie einen oder mehrere LDAP-Gruppenserver, die zur Gruppensuche verwendet werden sollen.

> *Weitere Informationen finden Sie in Das BeyondTrust Appliance B Series für die Kerberos-Authentifizierung konfigurieren auf https://www.beyondtrust.com/docs/remote-support/how-to/integrations/security-providers/kerberos-configuration/index.htm.*

Sicherheitsanbieter hinzufügen oder bearbeiten: SAML für Support-Techniker

Name

Geben Sie einen eindeutigen Namen ein, um Ihren Anbieter leichter zu identifizieren.

Aktiviert

Falls aktiviert, kann Ihr BeyondTrust Appliance B Series diesen Sicherheitsanbieter durchsuchen, wenn ein Benutzer versucht, sich in der Konsole d. Support-Technikers oder in **/login** anzumelden. Falls nicht aktiviert, wird dieser Sicherheitsanbieter nicht durchsucht.

Verknüpfte E-Mail-Domänen

Diese Einstellung ist nur dann gültig, wenn Sie über mehr als einen aktiven SAML-Anbieter verfügen und wird andernfalls ignoriert.

Fügen Sie alle E-Mail-Domänen hinzu, die mit diesem SAML-Anbieter verknüpft werden sollen, eine pro Zeile. Bei der Authentifizierung werden die Benutzer aufgefordert, ihre E-Mail-Adresse einzugeben. Die Domäne ihrer E-Mail-Adresse wird mit dieser Liste abgeglichen, und sie werden zur Authentifizierung an den entsprechenden Identitätsanbieter weitergeleitet.

Sind mehrere SAML-Anbieter konfiguriert, und die E-Mail-Adresse des Benutzers stimmt nicht mit einer der bei einem Anbieter verknüpften Domänen überein, kann die Authentifizierung nicht durchgeführt werden.

Identitätsanbieter-Einstellungen

Metadaten

Die Metadatendatei enthält alle Informationen, die für die anfängliche Einrichtung Ihres SAML-Anbieters erforderlich sind, und muss von Ihrem Identitätsanbieter heruntergeladen werden. Speichern Sie die XML-Datei und klicken Sie dann auf **Identitätsanbieter-Metadaten hochladen**, um die ausgewählte Datei auszuwählen und hochzuladen.

Entitäts-ID

Eindeutige Kennung für den verwendeten Identitätsanbieter.

Server-Zertifikat

Dieses Zertifikat wird verwendet, um die Signatur der Nachricht zu verifizieren, die vom Identitätsanbieter gesendet wurde.

> ***Hinweis:*** *Die Felder für* ***Entitäts-ID****,* ***Einzelanmeldungsdienst-URL*** *und* ***Zertifikat*** *werden automatisch über die Metadatendatei des Identitätsanbieters ausgefüllt. Wenn Sie keine Metadaten-Datei von Ihrem Anbieter erhalten, können diese Angaben auch manuell gemacht werden.*

Einzelanmeldungsdienst-URL

Wenn Sie sich mit SAML auf BeyondTrust anmelden möchten, werden Sie mit dieser URL automatisch weitergeleitet, damit Sie sich anmelden können.

SSO-URL-Protokoll-Bindung

Legt fest, ob ein Benutzer veröffentlicht oder zur Anmeldungs-URL weitergeleitet wird. Dies sollte standardmäßig auf „Weiterleiten“ belassen werden, soweit nicht anderweitig vom Identitätsanbieter gefordert.

Serviceanbieter-Einstellungen

Metadaten des Serviceanbieters herunterladen

Laden Sie die BeyondTrust-Metadaten herunter. Diese müssen dann bei Ihrem Identitätsanbieter hochgeladen werden.

Entitäts-ID

Dies ist Ihre BeyondTrust-URL. Sie identifiziert den Serviceanbieter eindeutig.

Privater Schlüssel

Falls nötig, können Sie vom Identitätsanbieter gesendete Nachrichten entschlüsseln, falls diese die Verschlüsselung unterstützen und erfordern. Klicken Sie auf **Datei wählen**, um den privaten Schlüssel hochzuladen, der für die Entschlüsselung der Nachrichten vom Identitätsanbieter erforderlich ist.

Benutzerattribut-Einstellungen

SAML-Attribute werden zur Bereitstellung von Benutzern in BeyondTrust verwendet. Die Standardwerte entsprechen von BeyondTrust zertifizierten Anwendungen mit verschiedenen Identitätsanbietern. Wenn Sie Ihren eigenen SAML-Connector erstellen, müssen Sie möglicherweise die Attribute an die Angaben Ihres Identitätsanbieters anpassen. Wenn Ihr Identitätsanbieter beim NameID-Attribut die Beachtung von Groß-/Kleinschreibung erfordert, wählen Sie **Vergleich für NameIDs ohne Beachtung von Groß-/Kleinschreibung verwenden**.

Autorisierungseinstellungen

Gruppen mit diesem Anbieter suchen

Die Aktivierung dieser Funktion ermöglicht eine schnellere Bereitstellung durch automatische Suche nach Gruppen für diesen Benutzer unter Verwendung von **Gruppensuche nach Attributname** und **Trennzeichen**.

Gruppensuche nach Attributname

Geben Sie den Namen des SAML-Attributs ein, das die Namen der Gruppen enthält, zu denen Benutzer gehören sollten. Wenn der Attributwert mehrere Gruppennamen enthält, geben Sie das **Trennzeichen** zur Trennung der Namen ein.

Falls leer gelassen, müssen SAML-Benutzer nach der ersten erfolgreichen Authentifizierung manuell zugewiesen werden.

Gruppensuch-Trennzeichen

Wenn das **Trennzeichen** leer gelassen wird, kann der Attributwert mehrere XML-Knoten mit jeweils unterschiedlichen Namen enthalten.

Verfügbare Gruppen

Hierbei handelt es sich um eine optionale Liste mit SAML-Gruppen, die immer für eine manuelle Zuweisung zu Gruppenrichtlinien verfügbar sind. Wird dieses Feld leer gelassen, wird eine SAML-Gruppe erst nach der ersten erfolgreichen Authentifizierung eines Benutzermitglieds einer solchen Gruppe verfügbar gemacht. Bitte geben Sie einen Gruppennamen pro Zeile ein.

Standardmäßige Gruppenrichtlinie

In der ausgewählten Gruppenrichtlinie werden die anfänglichen und standardmäßigen Berechtigungen, Mitgliedschaften und anderen Einstellungen für alle Benutzer definiert, die sich bei diesem Sicherheitsanbieter authentifizieren. Diese Einstellungen können individuell per Benutzer oder Benutzergruppe festgelegt werden, wenn die Benutzer anderen Gruppenrichtlinien angehören.

> *Weitere Informationen siehe SAML für die Einzelanmeldung unter https://www.beyondtrust.com/docs/remote-support/how-to/integrations/security-providers/saml/index.htm.*

Sicherheitsanbieter hinzufügen oder bearbeiten: SAML für öffentliche Portale

Name

Der Name Ihres SAML-Anbieters wird automatisch generiert und kann aktuell nicht bearbeitet werden.

Aktiviert

Falls aktiviert, kann Ihr BeyondTrust Appliance B Series diesen Sicherheitsanbieter durchsuchen, wenn ein Benutzer versucht, sich im öffentlichen Portal anzumelden. Falls nicht aktiviert, wird dieser Sicherheitsanbieter nicht durchsucht.

Identitätsanbieter-Einstellungen

Metadaten

Die Metadatendatei enthält alle Informationen, die für die anfängliche Einrichtung Ihres SAML-Anbieters erforderlich sind, und muss von Ihrem Identitätsanbieter heruntergeladen werden. Speichern Sie die XML-Datei und klicken Sie dann auf **Identitätsanbieter-Metadaten hochladen**, um die ausgewählte Datei auszuwählen und hochzuladen.

Entitäts-ID

Eindeutige Kennung für den verwendeten Identitätsanbieter.

Server-Zertifikat

Dieses Zertifikat wird verwendet, um die Signatur der Nachricht zu verifizieren, die vom Identitätsanbieter gesendet wurde.

> *Hinweis: Die Felder für **Entitäts-ID**, **Einzelanmeldungsdienst-URL** und **Zertifikat** werden automatisch über die Metadatendatei des Identitätsanbieters ausgefüllt. Wenn Sie keine Metadaten-Datei von Ihrem Anbieter erhalten, können diese Angaben auch manuell gemacht werden.*

Einzelanmeldungsdienst-URL

Wenn Sie sich mit SAML auf BeyondTrust anmelden möchten, werden Sie mit dieser URL automatisch weitergeleitet, damit Sie sich anmelden können.

SSO-URL-Protokoll-Bindung

Legt fest, ob ein Benutzer veröffentlicht oder zur Anmeldungs-URL weitergeleitet wird. Dies sollte standardmäßig auf „Weiterleiten“ belassen werden, soweit nicht anderweitig vom Identitätsanbieter gefordert.

Serviceanbieter-Einstellungen

Metadaten des Serviceanbieters herunterladen

Laden Sie die BeyondTrust-Metadaten herunter. Diese müssen dann bei Ihrem Identitätsanbieter hochgeladen werden.

Entitäts-ID

Dies ist Ihre BeyondTrust-URL. Sie identifiziert den Serviceanbieter eindeutig.

Privater Schlüssel

Falls nötig, können Sie vom Identitätsanbieter gesendete Nachrichten entschlüsseln, falls diese die Verschlüsselung unterstützen und erfordern. Klicken Sie auf **Datei wählen**, um den privaten Schlüssel hochzuladen, der für die Entschlüsselung der Nachrichten vom Identitätsanbieter erforderlich ist.

Benutzerattribut-Einstellungen

SAML-Attribute werden zur Bereitstellung von Benutzern in BeyondTrust verwendet. Die Standardwerte entsprechen von BeyondTrust zertifizierten Anwendungen mit verschiedenen Identitätsanbietern. Wenn Sie Ihren eigenen SAML-Connector erstellen, müssen Sie möglicherweise die Attribute an die Angaben Ihres Identitätsanbieters anpassen. Die SAML-Attribute können außerdem mit Sitzungen von Kunden verknüpft werden, indem auf der Seite **Benutzerdefinierte Felder** in **/login** benutzerdefinierte Felder mit entsprechenden Codenamen hinzugefügt werden.

> *Weitere Informationen siehe SAML für die Einzelanmeldung unter https://www.beyondtrust.com/docs/remote-support/how-to/integrations/security-providers/saml/index.htm.*

Sitzungsrichtlinien: Sitzungsberechtigungen und Aufforderungsregeln festlegen

Sitzungsrichtlinien

Mit Sitzungsrichtlinien können Sie die Sicherheitsberechtigungen für Sitzungen Tech. auf bestimmte Szenarien zuschneiden. Sitzungsrichtlinien können auf Benutzer, öffentliche Websites und alle Jump-Elemente angewendet werden.

> *Weitere Informationen finden Sie in So verwenden Sie Support-Sitzung Tech-Richtlinien auf www.beyondtrust.com/docs/remote-support/how-to/session-policies/.*

Der Abschnitt **Sitzungsrichtlinien** führt die verfügbaren Richtlinien auf. Klicken Sie auf den Pfeil neben einem Richtliniennamen, um schnell zu sehen, wo diese Richtlinie verwendet wird, für welche Benutzer, Support-Techniker-Einladungen und Jump-Clients sie verfügbar ist, welche Support-Tools konfiguriert wurden und welche Aufforderung konfiguriert wurde.

Hinzufügen, Bearbeiten, Löschen

Erstellen Sie eine neue Richtlinie, bearbeiten Sie eine bestehende Richtlinie oder entfernen Sie eine bestehende Richtlinie.

Kopieren

Um die Erstellung ähnlicher Gruppenrichtlinien zu beschleunigen, klicken Sie auf **Kopieren**, um eine neue Richtlinie mit identischen Einstellungen zu erstellen. Anschließend können Sie diese neue Richtlinie so bearbeiten, dass sie Ihre jeweiligen Anforderungen erfüllt.

Hinzufügen oder Bearbeiten der Sitzungsrichtlinie

Klicken Sie nach der Bearbeitung auf **Speichern**, um diese Richtlinie verfügbar zu machen.

Anzeigename

Erstellen Sie einen eindeutigen Namen, um diese Richtlinie leichter zu identifizieren. Dieser Name hilft bei der Zuweisung einer Sitzungsrichtlinie zu Benutzern, öffentlichen Portalen und Jump-Clients.

Codename

Legen Sie einen Codenamen zu Integrationszwecken fest. Wenn Sie keinen Codenamen festlegen, wird automatisch einer erstellt.

Beschreibung

Fügen Sie eine kurze Beschreibung hinzu, um den Zweck dieser Richtlinie zusammenzufassen. Die Beschreibung wird angezeigt, wenn eine Richtlinie auf Benutzerkonten, Gruppenrichtlinien und Support-Techniker-Einladungen angewandt wird.

Verfügbarkeit

Benutzer

Wählen Sie, ob diese Richtlinie zur Zuweisung an Benutzer (Benutzerkonten und Gruppenrichtlinien) zur Verfügung stehen soll.

Einladung für Support-Techniker

Legen Sie fest, ob diese Richtlinie zur Verwendung durch Benutzer zur Verfügung stehen soll, wenn ein externer Benutzer zu einer Sitzung eingeladen wird.

Jump-Items

Wählen Sie, ob diese Richtlinie zur Zuweisung an Jump-Elementen zur Verfügung stehen soll.

Abhängigkeiten

Wenn diese Sitzungsrichtlinie bereits verwendet wird, werden Sie die Anzahl von Benutzern, öffentlichen Portalen und Jump-Clients sehen, welche diese Richtlinie verwenden.

Berechtigungen

Für alle folgenden Berechtigungen können Sie die Berechtigung aktivieren oder deaktivieren, oder sie auf **Nicht definiert** setzen. Sitzungsrichtlinien werden auf hierarchische Art und Weise auf eine Sitzung angewandt, wobei Jump-Clients die höchste Priorität haben, gefolgt von Benutzern und schließlich dem globalen Standard. Wenn für eine Sitzung mehrere Richtlinien gelten, erhält die Richtlinie mit der höchsten Priorität Vorrang. Wenn beispielsweise die auf einen Jump-Client angewandte Richtlinie eine Berechtigung festlegt, dürfen keine anderen Richtlinien diese Berechtigung für die Sitzung ändern. Um eine Berechtigung durch eine Richtlinie mit niedrigerer Priorität definierbar zu machen, belassen Sie diese Berechtigung auf **Nicht definiert**.

> *Einzelheiten und Beispiele finden Sie in So verwenden Sie Support-Sitzung Tech-Richtlinien unter www.beyondtrust.com/docs/remote-support/how-to/session-policies/.*

Legen Sie fest, welche Tools mit dieser Richtlinie aktiviert oder deaktiviert werden sollen, und welche Tools den Kunden zur Gewährung der Berechtigung auffordern sollen.

Eingabeaufforderungen Support-Tool

> *Weitere Informationen erhalten Sie unter Kunden-Client: Schnittstelle für Support-Sitzungen Tech. unter https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/customer-support-interface.htm.*

Aufforderungsregeln

Wählen Sie, ob der Kunde bei Verwendung der untenstehenden Support-Funktionen um Genehmigung gebeten werden soll. Wählen Sie **Keine Aufforderung**, um niemals aufzufordern, **Immer auffordern**, um immer aufzufordern oder **Bei einigen Tools auffordern**, um zu

wählen, für welche Berechtigungen aufgefordert werden soll. Wenn **Bei einigen Tools auffordern** gewählt wird, erscheint die Option **Kunde auffordern** neben jedem Tool, mit den Optionen **niemals** oder **immer** aufzufordern. Falls **Nicht definiert** gewählt wurde, wird diese Option durch die Richtlinie der nächstniedrigeren Priorität bestimmt. Diese Einstellung kann von einer Richtlinie mit höherer Priorität überschrieben werden.

Berechtigt, einmal aufzufordern

Wenn **Bildschirmfreigabe** auf **Anzeigen und steuern** festgelegt wurde und die Aufforderung aktiviert wurde, wird diese Option angezeigt. Aktivieren Sie das Kontrollkästchen, damit die Aufforderung zur Bildschirmfreigabe den Zugang zu allen Tools während der Sitzung anfordert, ohne weitere Aufforderungen.

Aufforderungsoptionen

Legen Sie fest, wie lange auf eine Antwort auf eine Aufforderung gewartet werden soll, bevor die Standardantwort **Ablehnen** oder **Zulassen** gewählt wird. Falls **Nicht definiert** gewählt wurde, wird diese Option durch die Richtlinie der nächstniedrigeren Priorität bestimmt. Diese Einstellung kann von einer Richtlinie mit höherer Priorität überschrieben werden.

Bildschirmfreigabe

Bildschirmfreigabe-Regeln

Ermöglicht es dem Benutzer, den Remote-Bildschirm anzuzeigen oder zu steuern. Falls **Nicht definiert** gewählt wurde, wird diese Option durch die Richtlinie der nächstniedrigeren Priorität bestimmt. Diese Einstellung kann von einer Richtlinie mit höherer Priorität überschrieben werden.

> *Weitere Informationen finden Sie in Bildschirmfreigabe bei Remote-Kunde für Anzeige und Steuerung unter https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/screen-sharing.htm.*

Berechtigt, dem Kunden den eigenen Bildschirm anzuzeigen

Damit kann der Benutzer während einer Support-Sitzung Tech seinen Bildschirm für den Kunden freigeben. Diese Option ist verfügbar, wenn **Nur anzeigen** oder **Ansicht oder Steuerung** ausgewählt ist.

> *Weitere Informationen siehe Eigenen Bildschirm anzeigen: Umgekehrte Bildschirmfreigabe unter https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/show-my-screen.htm.*

Gestattete Kundeneinschränkungen

Legen Sie fest, ob der Support-Techniker Maus und Tastatur des Remote-Systems vorübergehend deaktivieren kann. Der Benutzer kann den Remote-Desktop auch daran hindern, angezeigt zu werden. Diese Option ist verfügbar, wenn **Anzeigen und steuern** ausgewählt ist. Wenn **Bildschirm, Maus und Tastatur** die ausgewählte Kundeneinschränkung ist, steht ein Kontrollkästchen zur Verfügung: **Bei Sitzungsbeginn automatisch einen privaten Bildschirm anfordern**. Der Bildschirm „Privatsphäre“ ist nur für Sitzungen verfügbar, die über einen Jump-Client, ein Remote Jump-Item oder ein lokales Jump-Item gestartet wurden. Wir empfehlen die Verwendung eines „Privatsphäre“-Bildschirms für unbeaufsichtigte Sitzungen. Das Remote-System muss den „Privatsphäre“-Bildschirm unterstützen.

> *Weitere Informationen siehe Eingeschränkte Kundeninteraktion: Privater Bildschirm, Remote-Eingaben deaktivieren unter https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/privacy-screen.htm.*

Aufforderungsverhalten bei Anwendungsfreigabe

Legen Sie fest, ob eine Anforderung zur Bildschirmfreigabe den Kunden immer oder nie dazu auffordern soll, die freizugebenden Anwendungen auszuwählen, oder ob der Benutzer wählen kann, ob eine Anwendungsfreigabe-Aufforderung erscheint oder nicht. Mit der Auswahl von **Immer** oder **Support-Techniker entscheidet** können Sie außerdem Anwendungsfreigabebeschränkungen vordefinieren.

> *Weitere Informationen siehe Anwendungsfreigabe: Einschränkung der für den Support-Techniker sichtbaren Elemente unter https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/application-sharing.htm.*

Synchronisierungsrichtung für Zwischenablage

Diese Option ist verfügbar, wenn **Anzeigen und steuern** ausgewählt ist. Wählen Sie, wie der Inhalt der Zwischenablage zwischen Support-Technikern und Endbenutzern ausgetauscht wird. Die Optionen sind:

- **Nicht berechtigt**: Der Support-Techniker darf die Zwischenablage nicht verwenden, es werden keine Zwischenablage-Symbole im Konsole d. Support-Technikers angezeigt, und die Befehle zum Ausschneiden und Einfügen funktionieren nicht.
- **Zulässig vom Support-Techniker zum Kunden:** Der Support-Techniker kann den Inhalt der Zwischenablage an den Kunden weiterleiten, kann aber nicht aus der Zwischenablage des Endbenutzers einfügen. Nur das Zwischenablage-Symbol Senden wird im Konsole d. Support-Technikers angezeigt.
- **Zulässig in beide Richtungen:** Der Inhalt der Zwischenablage kann in beide Richtungen übertragen werden. Beide Symbole Zwischenablage senden und abrufen werden im Konsole d. Support-Technikers angezeigt.

> *Weitere Informationen über den Zwischenablage-Synchronisationsmodus finden Sie unter „Sicherheit: Verwalten der Sicherheitseinstellungen“ auf Seite 236.*

Browserfreigabe

Browserfreigabe-Regeln

Damit kann der Benutzer die gleiche Website anzeigen, die der Kunde sieht, ohne die Kontrolle zu besitzen oder andere Anwendungen zu sehen. Falls **Nicht definiert** gewählt wurde, wird diese Option durch die Richtlinie der nächstniedrigeren Priorität bestimmt. Diese Einstellung kann von einer Richtlinie mit höherer Priorität überschrieben werden.

> *Weitere Informationen finden Sie in Bildschirmfreigabe bei Remote-Kunde für Anzeige und Steuerung unter https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/screen-sharing.htm.*

Anmerkungen

Anmerkungsregeln

Gibt dem Benutzer die Möglichkeit, Anmerkungswerkzeuge zu verwenden, um auf dem Bildschirm des Remote-Benutzers zu zeichnen. Falls **Nicht definiert** gewählt wurde, wird diese Option durch die Richtlinie der nächstniedrigeren Priorität bestimmt. Diese Einstellung kann von einer Richtlinie mit höherer Priorität überschrieben werden.

> *Weitere Informationen finden Sie in Verwenden von Anmerkungen, um auf dem Remote-Bildschirm zu zeichnen auf https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/annotations.htm.*

Dateitransfer

Dateitransfer-Regeln

Ermöglicht es dem Benutzer, Dateien auf das Remote-System hochzuladen, Dateien vom Remote-System herunterzuladen oder beides. Falls **Nicht definiert** gewählt wurde, wird diese Option durch die Richtlinie der nächstniedrigeren Priorität bestimmt. Diese Einstellung kann von einer Richtlinie mit höherer Priorität überschrieben werden.

Zugängliche Pfade im Dateisystem des Kunden

Gestattet es Benutzern, Dateien direkt zu oder von jeglichen oder nur von bestimmten Verzeichnissen auf dem Remote-System zu übertragen.

Zugängliche Pfade im Dateisystem des Support-Technikers

Gestattet es Benutzern, Dateien direkt zu oder von jeglichen oder nur von bestimmten Verzeichnissen auf seinem lokalen System zu übertragen.

> *Weitere Informationen finden Sie in Dateitransfer zum und vom Remote-System unter https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/file-transfer.htm.*

Befehlsshell

Befehlsshell-Regeln hier eingeben

Damit kann der Benutzer über eine virtuelle Befehlszeilen-Schnittstelle Befehle auf dem Remote-Computer ausgeben. Falls **Nicht definiert** gewählt wurde, wird diese Option durch die Richtlinie der nächstniedrigeren Priorität bestimmt. Diese Einstellung kann von einer Richtlinie mit höherer Priorität überschrieben werden.

> ***Hinweis:** Der Zugriff auf Befehlsshells kann in Shell Jump-Sitzungen nicht eingeschränkt werden.*

Weitere Informationen finden Sie in Zugriff auf den Remote-Befehlsshell unter https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/command-shell.htm.

Systeminformationen

Regeln für Systeminformationen

Ermöglicht es dem Benutzer, Systeminformationen zum Remote-Computer anzuzeigen. Falls **Nicht definiert** gewählt wurde, wird diese Option durch die Richtlinie der nächstniedrigeren Priorität bestimmt. Diese Einstellung kann von einer Richtlinie mit höherer Priorität überschrieben werden.

Berechtigt, Aktionen zu Systeminformationen zu verwenden

Ermöglicht es dem Benutzer, mit Prozessen und Programmen auf dem Remote-System zu interagieren, ohne dass eine Bildschirmfreigabe erforderlich ist. Es können Prozesse beendet, Dienste gestartet, gestoppt, pausiert, fortgesetzt und neugestartet und Programme deinstalliert werden.

Weitere Informationen finden Sie in Anzeige von Systeminformationen unter https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/system-info.htm.

Zugriff auf Registrierung

Verzeichniszugriff-Regeln

Ermöglicht es dem Benutzer, mit der Registrierung auf dem Remote-Windows-System zu interagieren, ohne dass eine Bildschirmfreigabe erforderlich ist. Schlüssel können angezeigt, hinzugefügt, gelöscht und bearbeitet, durchsucht und importiert werden.

Weitere Informationen finden Sie in Zugriff auf den Registrierungseditor am Remote-Endpunkt unter https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/registry-editor.htm.

Vordefinierte Skripts

Regeln für vordefinierte Skripts

Damit kann der Benutzer vordefinierte Skripts ausführen, die für seine Teams erstellt wurden. Beachten Sie: Wenn sich der Benutzer in der Nur-Anzeige-Bildschirmfreigabe befindet, erhält der Kunde eine Aufforderung zur Ausführung des Skripts.Falls **Nicht definiert** gewählt wurde, wird diese Option durch die Richtlinie der nächstniedrigeren Priorität bestimmt. Diese Einstellung kann von einer Richtlinie mit höherer Priorität überschrieben werden.

Weitere Informationen finden Sie in Zugriff auf den Remote-Befehlsshell unter https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/command-shell.htm.

Heraufsetzung

Heraufsetzungsregeln

Gibt dem Benutzer die Möglichkeit zu versuchen, den Kunden-Client so heraufzusetzen, dass er mit administrativen Rechten auf dem Remote-System ausgeführt wird. Falls **Nicht definiert** gewählt wurde, wird diese Option durch die Richtlinie der nächstniedrigeren Priorität bestimmt. Diese Einstellung kann von einer Richtlinie mit höherer Priorität überschrieben werden.

> *Weitere Informationen finden Sie in Den Client heraufsetzen auf https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/elevation.htm.*

Support-Button Bereitstellung

Support-Button Bereitstellungsregeln

Ermöglicht es dem Benutzer, während einer Sitzung eine Support-Button bereitzustellen oder zu entfernen. Die für die Bereitstellung verfügbaren Orte sind von den obigen Support-Button-Einstellungen abhängig. Falls **Nicht definiert** gewählt wurde, wird diese Option durch die Richtlinie der nächstniedrigeren Priorität bestimmt. Diese Einstellung kann von einer Richtlinie mit höherer Priorität überschrieben werden.

> *Weitere Informationen finden Sie in Überblick über Support-Sitzungen Tech. und Tools unter https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/support-session-overview.htm.*

Fixieren/Lösen von Jump-Clients

Regeln zum Fixieren/Lösen von Jump-Clients

Ermöglicht es dem Benutzer, während einer Sitzung einen Jump-Client zu fixieren oder zu lösen. Die für die Bereitstellung verfügbaren Orte sind von den obigen Jump-Client-Einstellungen abhängig. Falls **Nicht definiert** gewählt wurde, wird diese Option durch die Richtlinie der nächstniedrigeren Priorität bestimmt. Diese Einstellung kann von einer Richtlinie mit höherer Priorität überschrieben werden.

> *Weitere Informationen finden Sie in Überblick über Support-Sitzungen Tech. und Tools unter https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/support-session-overview.htm.*

Chat

> *Für weitere Informationen siehe Während einer Sitzung mit dem Kunden chatten unter https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/chat.htm.*

Chat-Regeln

Damit kann der Benutzer mit dem Remote-Kunden chatten. Falls **Nicht definiert** gewählt wurde, wird diese Option durch die Richtlinie der nächstniedrigeren Priorität bestimmt. Diese Einstellung kann von einer Richtlinie mit höherer Priorität überschrieben werden.

Berechtigt, URLs zum Webbrowser des Kunden zu pushen

Damit kann der Benutzer eine URL im Chat-Bereich eingeben und dann auf **URL pushen** klicken, um automatisch einen Webbrowser mit dieser Adresse auf dem Remote-Computer zu öffnen.

Berechtigt, Dateien mithilfe der Chat-Schnittstelle zu senden

Damit kann der Benutzer Dateien über die Chat-Schnittstelle senden.

> *Weitere Informationen erhalten Sie unter Kunden-Client: Schnittstelle für Support-Sitzungen Tech. unter https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/customer-support-interface.htm.*

Verhalten beim Beenden der Sitzung

Wenn die Verbindung innerhalb der unter **Neuverbindungs-Zeitüberschreitung** festgelegten Zeit nicht wiederhergestellt werden kann, legen Sie hier fest, wie verfahren werden soll. Um zu verhindern, dass ein Endbenutzer nach einer heraufgesetzten Sitzung auf unautorisierte Berechtigungen zugreift, stellen Sie den Client so ein, dass der Endbenutzer am Ende der Sitzung automatisch vom Remote-Windows-Computer abgemeldet wird, dass der Remote-Computer gesperrt wird, oder dass nichts getan wird. Diese Regeln gelten nicht für Browser-Freigabesitzungen.

Benutzer berechtigen, diese Einstellung sitzungsweise außer Kraft zu setzen

Sie können einem Benutzer die Übersteuerung der Sitzungsbeendigungseinstellung über die Registerkarte **Zusammenfassung** in der Konsole während einer Sitzung gestatten.

Richtlinie exportieren

Sie können eine Sitzungsrichtlinie von einer Site exportieren und diese Berechtigungen in eine Richtlinie auf einer anderen Site importieren. Bearbeiten Sie die Richtlinie, die Sie exportieren möchten, und rollen Sie zum Ende der Seite. Klicken Sie auf **Richtlinie exportieren** und speichern Sie die Datei.

Richtlinie importieren

Sie können diese Richtlinieneinstellungen in jede andere BeyondTrust-Website importieren, die den Import von Sitzungsrichtlinien unterstützt. Erstellen Sie eine neue Sitzungsrichtlinie und scrollen Sie zum Ende der Seite. Durchsuchen Sie die Richtliniendatei, und klicken Sie auf **Richtlinie importieren**. Nachdem die Richtliniendatei hochgeladen wurde, wird die Seite aktualisiert, sodass Sie Änderungen vornehmen können. Klicken Sie auf **Richtlinie speichern**, um die Richtlinie verfügbar zu machen.

Sitzungsrichtliniensimulator

Da die Schichtung von Richtlinien komplex sein kann, können Sie den **Sitzungsrichtliniensimulator** verwenden, um zu erfahren, welches Ergebnis Sie erhalten. Darüber hinaus können Sie den Simulator auch verwenden, um festzustellen, warum eine Berechtigung entgegen Ihren Erwartungen nicht verfügbar ist.

Support-Techniker

Beginnen Sie, indem Sie den Benutzer auswählen, der die Sitzung durchführt. Die Dropdown-Liste umfasst Benutzerkonten und Support-Techniker-Einladungs-Richtlinien.

Sitzungsstartmethode

Wählen Sie die Methode für den Sitzungsstart für diese Simulation.

Öffentliches Portal

Wenn Sie **Öffentliches Portal** gewählt haben, wählen Sie das für diese Simulation einer vom Kunden initiierten Sitzung zu verwendende öffentliche Portal.

Support-Button

Wenn Sie **Support-Button** gewählt haben, suchen Sie nach einer bereitgestellten Support-Button nach Profil, zugewiesenem öffentlichen Portal, zugewiesener Warteschlange, Computername oder Beschreibung. Das zugewiesene öffentliche Portal wird automatisch oben ausgewählt.

Jumpoint oder lokaler Jump

Da lokale Jumps und Jumpoints stets dem standardmäßigen öffentlichen Portal zugewiesen sind, müssen Sie keine weiteren Einstellungen festlegen.

Jump-Client, symbolischer Jump-Link (lokal), symbolischer Jump-Link (Remote), symbolischer VNC-Link (lokal), symbolischer VNC-Link (Remote), symbolischer RDP-Link (Remote), symbolischer RDP-Link (lokal), symbolischer Shell Jump-Link, symbolischer Intel® vPro-Link

Sie können nach einem fixierten Jump-Client oder symbolischen Jump-Link mithilfe von Name, Kommentaren, Jump-Gruppe, Tag oder zugehörigem öffentlichen Portal suchen. Das zugewiesene öffentliche Portal wird automatisch oben ausgewählt.

Kunde präsent

Wenn Sie **Jump-Client** gewählt haben, können Sie wählen, ob der Kunde als präsent angezeigt werden soll oder nicht.

Simulieren

Klicken Sie auf **Simulieren**. Im untenstehenden Bereich werden die nach Sitzungsrichtlinie konfigurierbaren Berechtigungen im schreibgeschützten Modus angezeigt. Sie können sehen, welche Berechtigungen als Ergebnis der kombinierten Richtlinien gewährt oder nicht gewährt wurden, und welche Richtlinie welche Berechtigung festgelegt hat.

Gruppenrichtlinien: Benutzerberechtigungen auf Benutzergruppen anwenden

Gruppenrichtlinien

Mit der Seite **Gruppenrichtlinien** können Sie Benutzergruppen mit gemeinsamen Berechtigungen einrichten.

Neue Richtlinie hinzufügen, bearbeiten, löschen

Erstellen Sie eine neue Richtlinie, bearbeiten Sie eine bestehende Richtlinie oder entfernen Sie eine bestehende Richtlinie.

> ***Hinweis:*** *Wenn Sie die als Standard für den lokalen Anbieter oder für lokale Administratorbenutzer eingerichtete Gruppenrichtlinie bearbeiten und Administratorrechte entfernen, wird eine Warnmeldung angezeigt. Vergewissern Sie sich, dass andere Benutzer über Administratorrechte verfügen, ehe Sie fortfahren.*

Reihenfolge ändern

Klicken Sie auf die Schaltfläche **Reihenfolge ändern**, um die Priorität von Gruppenrichtlinien per Drag and Drop festzulegen. Klicken Sie auf **Reihenfolge speichern**. Dadurch treten die Priorisierungsänderungen in Kraft. Finden auf einen bestimmten Benutzer mehrere Richtlinien Anwendung, gelten diese ab dem ersten Eintrag der Liste **Gruppenrichtlinien** und dann absteigend weiter. Steht eine Berechtigung in Widerspruch mit einer von einer Gruppenrichtlinie weiter oben in der Liste angewendeten Berechtigung, überschreibt die weiter unten stehende Berechtigung die weiter oben stehende, es sei denn, die höhere wurde als **Endgültig** eingestuft. Zusammengefasst: Gruppenrichtlinien weiter unten in der Liste haben eine höhere Priorität als weiter oben stehende Gruppenrichtlinien.

Gruppenrichtlinien durchsuchen

Um eine vorhandene Richtlinie in der Liste der **Gruppenrichtlinien** schnell zu finden, geben Sie den Namen oder einen Teil des Namens ein. Die Einträge der Liste werden nach allen Richtlinien mit einem Namen gefiltert, der den eingegebenen Suchbegriff enthält. Die Liste wird so lange mit gefilterten Einträgen angezeigt, bis der Suchbegriff entfernt wird, selbst wenn der Benutzer andere Seiten aufruft oder sich abmeldet. Um den Suchbegriff zu entfernen, klicken Sie auf das **X** zur Rechten des Suchfeldes.

Wenn Sie nach der Suche auf der Liste auf die Schaltfläche **Reihenfolge ändern** klicken, werden alle Gruppenrichtlinien angezeigt. Sie können die Gruppenrichtlinien ziehen und ablegen, um ihre Priorität festzulegen. Wenn Sie auf **Reihenfolge speichern** klicken, werden die Änderungen übernommen, und die Liste wird wieder mit Richtlinien mit einem Namen angezeigt, die den Suchbegriff enthalten.

Alle ausklappen/ Alle zuklappen

Um die Gruppenrichtlinien leichter suchen und durch diese navigieren zu können, klicken Sie auf den Link **Alle ausklappen** über dem Raster, um die Details aller aufgeführten Gruppenrichtlinien auszuklappen. Klicken Sie auf **Alle zuklappen**, um zur zugeklappten Liste der Gruppenrichtlinien zurückzukehren.

Kopieren

Um die Erstellung ähnlicher Gruppenrichtlinien zu beschleunigen, klicken Sie auf **Kopieren**, um eine neue Richtlinie mit identischen Einstellungen zu erstellen. Anschließend können Sie diese neue Richtlinie so bearbeiten, dass sie Ihre jeweiligen Anforderungen erfüllt.

Richtlinie hinzufügen oder bearbeiten

Nachdem Sie Ihre Änderungen vorgenommen haben, klicken Sie auf **Speichern**, um sie in dieser Gruppenrichtlinie zu speichern.

Richtlinienname

Erstellen Sie einen eindeutigen Namen, um diese Richtlinie leichter zu identifizieren.

Verfügbare Mitglieder und Richtlinienmitglieder

Um Mitglieder zuzuweisen, wählen Sie ein Mitglied aus der Liste **Verfügbare Mitglieder** und klicken Sie auf **Hinzufügen**, um es in das Feld **Richtlinienmitglieder** zu verschieben. Verwenden Sie das **Suchfeld**, um bestehende Mitglieder zu finden.

Sie können Benutzer Ihres lokalen Systems auswählen oder Benutzer oder gesamte Gruppen von konfigurierten Sicherheitsanbietern wählen. Um Benutzer oder Gruppen über einen externen Verzeichnisspeicher wie LDAP, RADIUS oder Kerberos hinzuzufügen, müssen Sie zunächst die Verbindung auf der Seite **/login > Benutzer und Sicherheit > Sicherheitsanbieter** konfigurieren. Ist der Versuch, einen Benutzer von einem konfigurierten Sicherheitsanbieter hinzuzufügen, ungültig, erscheint hier die Fehlermeldung des Synchronisierungsprotokolls (ebenfalls wird sie im Protokoll hinzugefügt).

Kontoeinstellungen

Welche Kontoeinstellungen soll diese Gruppenrichtlinie regeln?

Entscheiden Sie, ob eine Einstellung in dieser Richtlinie **Definiert** sein soll. Wenn dies der Fall ist, können Sie **Endgültig** auswählen, um zu verhindern, dass andere Richtlinien mit niedrigerer Priorität den mit dieser Richtlinie festgelegten Berechtigungswert aufheben. Wählen Sie **Alle**, um alle Einstellungen in diesem Abschnitt zu definieren.

Zwei-Faktor-Authentifizierung: Anmelden mit einer Authentifikator-App:

Legen Sie fest, ob sich der Benutzer über eine Authentifizierungs-App anmelden muss oder ob dies optional ist (Standardeinstellung). Ist **Erforderlich** ausgewählt, wird, wenn sich dieser Benutzer das nächste Mal an der Verwaltungsschnittstelle oder der Konsole d. Support-Technikers anmeldet, ein Bildschirm angezeigt, dass die Zwei-Faktor-Authentifizierung aktiviert werden muss.

> *Weitere Informationen zu 2FA finden Sie in So verwenden Sie Zwei-Faktor-Authentifizierung mit BeyondTrust Remote Support auf www.beyondtrust.com/docs/remote-support/how-to/2-factor-authentication/.*

Kontoablauf: Das Konto läuft niemals ab

Ist bei dieser Option ein Haken gesetzt, läuft das Konto nie ab.

Kontoablauf: Konto-Ablaufdatum

Führt dazu, dass das Konto an einem bestimmten Datum abläuft.

Kontoaktivierung: Konto deaktiviert

Dadurch wird das Konto deaktiviert, sodass der Benutzer sich nicht anmelden kann. Durch das Deaktivieren wird das Konto NICHT gelöscht.

Anzeigename-Bearbeitung: Berechtigt, ihre Anzeigenamen zu ändern

Ermöglicht es dem Benutzer, seinen Anzeigenamen zu ändern.

Fotobearbeitung: Berechtigt, ihr Bild zu ändern

Ermöglicht es Benutzern, ihre Avatarfotos zu ändern, die in der **/login**-Verwaltungsschnittstelle und im Chatfenster des Kunden-Client angezeigt werden.

Auf öffentlicher Website anzeigen: Berechtigt, auf der öffentlichen Website anzuzeigen

Zeigt den Namen des Benutzers auf allen öffentlichen Websites an, auf denen die Support-Techniker-Liste aktiviert ist.

Kommentare

Fügen Sie Kommentare hinzu, die den Zweck dieses Kontos identifizieren.

Allgemeine Berechtigungen

Welche allgemeinen Einstellungen soll diese Gruppenrichtlinie regeln?

Entscheiden Sie, ob eine Einstellung in dieser Richtlinie **Definiert** sein soll. Wenn dies der Fall ist, können Sie **Endgültig** auswählen, um zu verhindern, dass andere Richtlinien mit niedrigerer Priorität den mit dieser Richtlinie festgelegten Berechtigungswert aufheben. Wählen Sie **Alle**, um alle Einstellungen in diesem Abschnitt zu definieren.

Verwaltung

Administratorrechte: Administrator

Erteilt dem Benutzer volle Administratorrechte.

Vault-Administratorrechte: Zur Verwaltung von Vault berechtigt

Ermöglicht dem Benutzer die Verwaltung aller Aspekte des BeyondTrust Vault-Add-ons.

Passworteinstellung: Berechtigt, Kennwörter festzulegen

Ermöglicht es dem Benutzer, für nicht-administrative lokale Benutzer Kennwörter festzulegen und Benutzerkonten freizuschalten.

Bearbeiten des Jumpoint: Berechtigt, Jumpoints zu bearbeiten

Ermöglicht es dem Benutzer, Jumpoints zu erstellen oder zu bearbeiten. Diese Option wirkt sich nicht darauf aus, ob der Benutzer auf Remote-Computer über Jumpoints zugreifen kann, die einzeln oder über Gruppenrichtlinien konfiguriert werden.

Bearbeitung der öffentliche Website: Berechtigt, die öffentliche Website zu bearbeiten

Damit kann der Benutzer öffentliche Website-Konfigurationen erstellen und ändern, HTML-Vorlagen bearbeiten, die Übersetzungsschnittstelle anzeigen usw.

Bearbeitung von Kundenhinweisen: Berechtigt, Kundenhinweise zu bearbeiten

Gibt dem Benutzer die Möglichkeit, Meldungen zu erstellen und zu bearbeiten, mit denen Kunden beim Anfordern von Support über breitenwirksame IT-Ausfälle informiert werden.

Dateispeicher-Bearbeitung: Berechtigt, den Dateispeicher zu bearbeiten

Damit kann der Benutzer Dateien aus dem Dateispeicher entfernen oder Dateien hinzufügen.

Bearbeiten vordefinierter Meldungen: Berechtigt, vordefinierte Meldungen zu bearbeiten

Ermöglicht es dem Benutzer, vordefinierte Chat-Nachrichten zu erstellen oder zu bearbeiten.

Bearbeiten von Support-Teams: Berechtigt zum Bearbeiten technischer Support-Teams

Ermöglicht es dem Benutzer, Support-Teams zu erstellen oder zu bearbeiten.

Bearbeiten der Jump-Gruppe: Berechtigt, Jump-Gruppen zu bearbeiten

Ermöglicht es dem Benutzer, Jump-Gruppen zu erstellen oder zu bearbeiten.

Problembearbeitung: Berechtigt, Probleme zu bearbeiten

Damit kann der Benutzer Probleme erstellen und bearbeiten.

Bearbeiten von Qualifikationen: Berechtigt, Qualifikationen zu bearbeiten

Damit kann der Benutzer Qualifikationen erstellen und bearbeiten.

Support-Button Bearbeitung des Profils: Berechtigt, Support-Button-Profile zu bearbeiten

Ermöglicht es dem Benutzer, Support-Button-Profile anzupassen.

Bearbeitung vordefinierter Skripts: Berechtigt, vordefinierte Skripts zu bearbeiten

Damit kann der Benutzer vordefinierte Skripts für die Verwendung in Bildschirmfreigabe- oder Befehlsshell-Sitzungen erstellen oder bearbeiten.

Bearbeiten von benutzerdefinierten Support-Techniker-Links: Berechtigt, benutzerdefinierte Support-Techniker-Links zu bearbeiten

Ermöglicht es dem Benutzer, benutzerdefinierte Links zu erstellen oder zu bearbeiten.

Bearbeitung von Zugriffssponsoren: Berechtigt, Zugriffssponsoren zu bearbeiten

Damit kann der Benutzer Zugriffssponsorenteams erstellen oder bearbeiten.

Bearbeitung des iOS-Profils: Berechtigt, iOS-Profile zu bearbeiten

Ermöglicht es dem Benutzer, Apple iOS-Profilinhalte zur Verteilung an Benutzer mit iOS-Geräten zu erstellen, zu bearbeiten und hochzuladen.

Bericht wird erstellt

Zugriff auf Sitzungs- und Teamberichte: Berechtigt, Support-Sitzung Tech-Berichte anzuzeigen

Ermöglicht dem Benutzer, Berichte zur Support-Sitzung Tech-Aktivität auszuführen, nur Sitzungen anzuzeigen, bei denen er der primäre Support-Techniker war, nur Sitzungen anzuzeigen, bei denen eines seiner Teams das primäre Team oder eines seiner Teammitglieder der primäre Support-Techniker war, oder alle Sitzungen anzuzeigen.

Zugriff auf Sitzungs- und Teamberichte: Berechtigt, Support-Sitzung Tech-Aufzeichnungen anzuzeigen

Damit kann der Benutzer Videoaufzeichnungen der Bildschirmfreigabe-, „Eigenen Bildschirm anzeigen“- und Befehlsshell-Sitzungen anzeigen.

Zugriff auf den Lizenznutzungsbericht: Berechtigt, Lizenznutzungsberichte anzuzeigen

Damit kann der Benutzer Berichte zur BeyondTrust-Lizenznutzung erstellen.

Zugriff auf Vault-Berichte: Berechtigt, Vault-Berichte anzuzeigen

Ermöglicht dem Benutzer, Berichte zu Vault-Aktivitäten zu erstellen und dabei alle Ereignisdaten oder nur eigene Ereignisdaten anzuzeigen.

Zugriff auf Präsentationsberichte: Berechtigt, Berichte zu Präsentationssitzungen anzuzeigen

Ermöglicht dem Benutzer, Berichte zur Präsentationsaktivität auszuführen, nur Präsentationen anzuzeigen, bei denen er der Moderator war, nur Sitzungen anzuzeigen, bei denen eines seiner Teammitglieder der Moderator war, oder alle Präsentationen anzuzeigen.

Berechtigt, Aufzeichnungen für Support-Sitzungen Tech. anzuzeigen

Damit kann der Benutzer Aufzeichnungen der Bildschirmfreigabe und Befehlsshell-Sitzungen anzeigen. Dies hat keine Auswirkung auf Aufzeichnungen von Präsentationen.

Berechtigt, Lizenznutzungsberichte anzuzeigen

Berechtigt den Benutzer, den Lizenzbericht für Support-Techniker anzuzeigen.

Zugriff auf Syslog-Berichte: Berechtigt, Syslog-Berichte anzuzeigen

Ermöglicht dem Benutzer, eine ZIP-Datei mit allen auf dem Gerät vorhandenen Syslog-Dateien herunterzuladen. Administratoren müssen automatisch über Berechtigungen für den Zugriff auf diesen Bericht verfügen. Nicht-Administratorbenutzer müssen zum Anzeigen dieses Berichts den Zugriff anfordern.

Support-Technikerberechtigungen

Berechtigt, Remote-Support bereitzustellen

Damit kann der Benutzer die Konsole d. Support-Technikers verwenden, um Support-Sitzung Techen durchzuführen. Wenn Support aktiviert ist, sind auch Optionen für Remote-Support verfügbar. Deaktivieren Sie diese Einstellung für Nur-Präsentations-Benutzer.

Sitzungsverwaltung

Berechtigt, Sitzungsschlüssel für Support-Sitzung Tech innerhalb der Konsole d. Support-Technikers zu erstellen

Ermöglicht es dem Benutzer, Sitzungsschlüssel zu generieren, damit Kunden direkt Sitzungen mit ihm einleiten können.

> *Weitere Informationen finden Sie unter Einen Sitzungsschlüssel zum Starten einer Support-Sitzung generieren auf https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/session-keys.htm.*

Berechtigt, Zugriffsschlüssel zum Senden von iOS-Profilen zu erstellen

Ermöglicht es dem Benutzer, Zugriffsschlüssel zum Anbieten von iOS-Inhalten für Benutzer mit iOS-Geräten zu erstellen.

> *Weitere Informationen finden Sie in Einen Apple iOS-Profilzugriffsschlüssel generieren auf https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/apple-ios-access-key-management-interface.htm.*

Es können manuell Sitzungen aus einer Team-Warteschlange angenommen werden

Damit kann der Benutzer Sitzungen in einer seiner Teamwarteschlangen auswählen und starten.

> *Weitere Informationen finden Sie in Eine Sitzung zum Starten des Supports akzeptieren unter https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/accepting-a-session.htm.*

Berechtigt, Sitzungen an Teams zu übertragen, denen sie nicht angehören

Damit kann der Benutzer Sitzungen an andere Teams als seine eigenen übertragen. Bei Deaktivierung ist die Interaktion des Benutzers ausschließlich auf die ihm zugewiesenen Teams beschränkt.

> *Weitere Informationen finden Sie in Überblick über Support-Sitzungen Tech. und Tools unter https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/support-session-overview.htm.*

Berechtigt, Sitzungen für Teams freizugeben, denen sie nicht angehören

Ermöglicht es dem Benutzer, eine weniger stark beschränkte Gruppe von Benutzern zur Freigabe von Sitzungen einzuladen; nicht nur ihre Team-Mitglieder. In Kombination mit der Berechtigung Erweiterte Verfügbarkeit werden die Möglichkeiten zur Freigabe von Sitzungen durch diese Berechtigung ausgedehnt.

> *Weitere Informationen finden Sie in Überblick über Support-Sitzungen Tech. und Tools unter https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/support-session-overview.htm.*

Berechtigt, externe Support-Techniker einzuladen

Damit kann der Benutzer Drittbenutzer dazu einladen, einmalig an einer Support-Sitzung Tech teilzunehmen.

> *Für weitere Informationen siehe Einladen eines externen Benutzers zur Teilnahme an einer Sitzung unter https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/rep-invite.htm.*

Berechtigt zur Verwendung der Funktion „Nächste Sitzung aufrufen“

Damit kann der Benutzer durch einfachen Schaltflächenklick mit dem Support der ältesten Sitzung in der Warteschlange für seine Teams beginnen.

> *Weitere Informationen finden Sie in Eine Sitzung zum Starten des Supports akzeptieren unter https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/accepting-a-session.htm.*

Aktivierung des erweiterten Verfügbarkeitsmodus zulassen

Ermöglicht es dem Benutzer, E-Mail-Einladungen von anderen Benutzern zu erhalten, die die Freigabe einer Sitzung anfordern, auch wenn sie nicht in der Konsole d. Support-Technikers angemeldet sind.

> *Weitere Informationen finden Sie in Verwenden der erweiterten Verfügbarkeit, um auch nach der Abmeldung einen Zugriff zu ermöglichen unter https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/extended-availability.htm.*

Berechtigt, externen Schlüssel zu bearbeiten

Ermöglicht es dem Benutzer, den externen Schlüssel aus dem Fenster Sitzungsinformationen einer Sitzung innerhalb der Konsole d. Support-Technikers zu ändern.

> *Weitere Informationen finden Sie in Überblick über Support-Sitzungen Tech. und Tools unter https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/support-session-overview.htm.*

Equilibrium

> *Weitere Informationen finden Sie in Handbuch für die automatische Sitzungsweiterleitung mit Equilibrium at https://www.beyondtrust.com/docs/remote-support/how-to/equilibrium/index.htm.*

Berechtigt zum Deaktivieren der Option zu Sitzungszuweisungen

Damit kann der Support-Techniker sich selbst als für Sitzungen nicht verfügbar markieren, die mit Equilibrium zugewiesen werden.

Keine Sitzungen zuweisen, wenn der Support-Techniker teilnimmt an mindestens

Damit wird die Mindestanzahl an Sitzungen festgelegt, die der Support-Techniker unterstützen muss, bevor Sitzungen nicht mehr automatisch mit Equilibrium zugewiesen werden.

Keine Sitzungen zuweisen, wenn der Support-Techniker untätig war für mindestens

Damit wird die Mindestzeit festgelegt, die der Support-Techniker untätig gewesen sein muss, bevor Sitzungen nicht mehr automatisch mit Equilibrium zugewiesen werden.

Techniker-zu-Techniker-Bildschirmfreigabe

> *Weitere Informationen finden Sie in Ihren Bildschirm für einen anderen Support-Techniker freigeben auf https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/representative-screensharing.htm.*

Berechtigt, anderen Support-Technikern den Bildschirm zu zeigen

Ermöglicht es dem Benutzer, seinen Bildschirm für einen anderen Benutzer freizugeben, ohne dass der empfangende Benutzer einer Sitzung beitreten muss. Diese Option ist auch dann verfügbar, wenn sich der Benutzer nicht in einer Sitzung befindet.

Berechtigt, die Steuerung zu gewähren, wenn anderen Support-Technikern der Bildschirm gezeigt wird

Ermöglicht es dem Benutzer, der seinen Bildschirm freigibt, die Steuerung von Tastatur und Maus dem Benutzer zu überlassen, der seinen Bildschirm anzeigt.

Support-Sitzung Techs

> *Weitere Informationen finden Sie in Überblick über Support-Sitzungen Tech. und Tools unter https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/support-session-overview.htm.*

Berechtigt zur Bereitstellung von Support-Buttonn in persönlicher Warteschlange

Ermöglicht es dem Benutzer, persönliche Support-Buttonn bereitzustellen und zu verwalten. Diese Einstellung wirkt sich auf die Bereitstellung von Support-Buttonn sowohl über die Webschnittstelle als auch die Konsole d. Support-Technikers aus. Um eine Support-Button innerhalb einer Sitzung bereitzustellen, muss die Sitzungsberechtigung **Bereitstellung vonSupport-Button** ebenfalls gewährt sein.

Team-Support-Buttons können verwaltet werden

Ermöglicht es dem Benutzer, die für seine eigenen Teams bereitgestellten Support-Buttonn zu ändern. Wenn der Benutzer Teamleiter oder -manager ist, kann er auch die persönlichen Support-Buttonn aller anderen Teammitglieder ändern.

> *Weitere Informationen finden Sie in Support-Buttone verwalten auf https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/support-schaltfläche-management-interface.htm.*

Berechtigt zur Änderung des dem Support-Button zugewiesenen öffentlichen Portals

Ermöglicht dem Benutzer, das öffentliche Portal festzulegen, über das sich eine Support-Button verbinden soll. Da Sitzungsrichtlinien auf öffentliche Portale angewandt werden können, kann sich die Änderung des Portals auf die in der Sitzung gestatteten Berechtigungen auswirken.

Team-Support-Buttonn können bereitgestellt werden

Ermöglicht es dem Benutzer, Team-Support-Buttonn für seine eigenen Teams bereitzustellen. Diese Einstellung wirkt sich auf die Bereitstellung von Support-Buttonn sowohl über die Webschnittstelle als auch die Konsole d. Support-Technikers aus. Um eine Support-Button innerhalb einer Sitzung bereitzustellen, muss die Sitzungsberechtigung **Support-ButtonBereitstellung von Support-Schaltflächen** ebenfalls gewährt sein.

Jump-Technologie

Gestattete Jump-Methoden

Ermöglicht es dem Benutzer, mit **Jump-Clients**, **lokalen Jumps**, **lokalen VNCs**, **RDP (lokal)**, **Remote-Jumps**, **Remote VNCs**, **RDP (Remote)**, **Shell Jumps**, und/oder **Intel vPro**-Jumps zu Computern durchzuführen.

Jump-Element-Rollen

Eine Jump-Element-Rolle ist ein vordefinierter Berechtigungssatz zur Verwaltung und Nutzung von Jump-Elementen. Klicken Sie für jede Option auf die Schaltfläche **Bearbeiten**, um die Jump-Element-Rolle in einer neuen Registerkarte zu öffnen.

Die **Standard**-Rolle wird nur verwendet, wenn **Benutzerstandard verwenden** für diesen Benutzer in einer Jump-Gruppe festgelegt wurde.

Die Rolle **Persönlich** gilt nur für Jump-Elemente, die auf der persönlichen Benutzerliste von Jump-Elementen fixiert wurden.

Die **Teams**-Rolle gilt für Jump-Elemente, die auf der persönlichen Liste von Jump-Elementen eines Teammitglieds mit niedrigerer Rolle fixiert wurden. Ein Team-Manager kann zum Beispiel die persönlichen Jump-Elemente von Teamleitern und Teammitgliedern anzeigen, während ein Teamleiter die persönlichen Jump-Elemente von Teammitgliedern anzeigen kann.

Die **System**-Rolle gilt für alle anderen Jump-Elemente im System. Für die meisten Benutzer sollte hier **Kein Zugriff** gewählt werden. Bei Wahl einer anderen Option wird der Benutzer zu Jump-Gruppen hinzugefügt, denen er normalerweise nicht zugeordnet werden würde. In der Konsole d. Support-Technikers kann dieser dann die persönlichen Listen von Jump-Elementen von Benutzern sehen, die keine Teammitglieder sind.

> *Weitere Informationen finden Sie in Verwenden von Jump-Element-Rollen, um Berechtigungssätze für Jump-Clients zu erstellen unter https://www.beyondtrust.com/docs/remote-support/how-to/jump-clients/jump-item-roles.htm.*

Präsentation

Berechtigt, Präsentationen zu leiten

Damit kann der Support-Techniker für einen oder mehrere Teilnehmer Präsentationen leiten.

> *Weitere Informationen finden Sie in Eine Präsentation für Remote-Teilnehmer abhalten unter https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/presentation.htm.*

Berechtigt, einem Präsentationsteilnehmer die Steuerung zu gewähren

Damit kann der Support-Techniker einem Teilnehmer während einer Präsentation die Steuerung über seinen Computer gewähren. Diese Einstellung wirkt sich nur auf Präsentationen und nicht auf die Funktion „Eigenen Bildschirm anzeigen“ einer Support-Sitzung Tech aus. Es kann nur jeweils ein Teilnehmer gleichzeitig die Steuerung übernehmen. Der Support-Techniker kann dies stets übersteuern.

> *Weitere Informationen siehe Präsentationsteilnehmer-Client: Einer Präsentation beitreten unter https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/customer-presentation-interface.htm.*

Konsole d. Support-Technikers

Zeitüberschreitung nach Inaktivität

Legt fest, wie lange der Support-Techniker inaktiv sein kann, bevor er von der Konsole d. Support-Technikers abgemeldet wird. Diese Berechtigung kann die seitenweit geltende Einstellung verwenden oder aber diese überschreiben.

Berechtigungen für überwachte und unüberwachte Sitzungen

Überwachte und unüberwachte Sitzungsrichtlinien

Sitzungsrichtlinie

Legen Sie die Aufforderungs- und Berechtigungsregeln fest, die für die Sitzungen dieses Benutzers gelten sollen. Wählen Sie eine bestehende Sitzungsrichtlinie oder definieren Sie Ihre eigenen Berechtigungen für diesen Benutzer. Falls **Nicht definiert** gewählt wurde, wird die globale Standardrichtlinie verwendet. Diese Berechtigungen können von einer Richtlinie mit höherer Priorität überschrieben werden.

Die gleichen Berechtigungen für unüberwachte Sitzungen verwenden

Um die gleichen Berechtigungen für sowohl überwachte wie auch unüberwachte Sitzungen zu verwenden, aktivieren Sie **Die gleichen Berechtigungen für unüberwachte Sitzungen verwenden**. Deaktivieren Sie dieses Kontrollkästchen, um Berechtigungen für überwachte und unüberwachte Sitzungen separat zu definieren. Sie können auch die Berechtigungen aus einer Kategorie in die andere kopieren.

Beschreibung

Zeigen Sie die Beschreibung einer vordefinierten Berechtigungsrichtlinie an.

Eingabeaufforderungen Support-Tool

> *Weitere Informationen erhalten Sie unter Kunden-Client: Schnittstelle für Support-Sitzungen Tech. unter https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/customer-support-interface.htm.*

Aufforderungsregeln

Wählen Sie, ob der Kunde bei Verwendung der untenstehenden Support-Funktionen um Genehmigung gebeten werden soll. Wählen Sie **Keine Aufforderung**, um niemals aufzufordern, **Immer auffordern**, um immer aufzufordern oder **Bei einigen Tools auffordern**, um zu wählen, für welche Berechtigungen aufgefordert werden soll. Wenn **Bei einigen Tools auffordern** gewählt wird, erscheint die Option **Kunde auffordern** neben jedem Tool, mit den Optionen **niemals** oder **immer** aufzufordern. Falls **Nicht definiert** gewählt wurde, wird diese Option durch die Richtlinie der nächstniedrigeren Priorität bestimmt. Diese Einstellung kann von einer Richtlinie mit höherer Priorität überschrieben werden.

Berechtigt, einmal aufzufordern

Wenn **Bildschirmfreigabe** auf **Anzeigen und steuern** festgelegt wurde und die Aufforderung aktiviert wurde, wird diese Option angezeigt. Aktivieren Sie das Kontrollkästchen, damit die Aufforderung zur Bildschirmfreigabe den Zugang zu allen Tools während der Sitzung anfordert, ohne weitere Aufforderungen.

Aufforderungsoptionen

Legen Sie fest, wie lange auf eine Antwort auf eine Aufforderung gewartet werden soll, bevor die Standardantwort **Ablehnen** oder **Zulassen** gewählt wird. Falls **Nicht definiert** gewählt wurde, wird diese Option durch die Richtlinie der nächstniedrigeren Priorität bestimmt. Diese Einstellung kann von einer Richtlinie mit höherer Priorität überschrieben werden.

Bildschirmfreigabe

Bildschirmfreigabe-Regeln

Ermöglicht es dem Benutzer, den Remote-Bildschirm anzuzeigen oder zu steuern. Falls **Nicht definiert** gewählt wurde, wird diese Option durch die Richtlinie der nächstniedrigeren Priorität bestimmt. Diese Einstellung kann von einer Richtlinie mit höherer Priorität überschrieben werden.

> *Weitere Informationen finden Sie in Bildschirmfreigabe bei Remote-Kunde für Anzeige und Steuerung unter https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/screen-sharing.htm.*

Berechtigt, dem Kunden den eigenen Bildschirm anzuzeigen

Damit kann der Benutzer während einer Support-Sitzung Tech seinen Bildschirm für den Kunden freigeben. Diese Option ist verfügbar, wenn **Nur anzeigen** oder **Ansicht oder Steuerung** ausgewählt ist.

> *Weitere Informationen siehe Eigenen Bildschirm anzeigen: Umgekehrte Bildschirmfreigabe unter https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/show-my-screen.htm.*

Gestattete Kundeneinschränkungen

Legen Sie fest, ob der Support-Techniker Maus und Tastatur des Remote-Systems vorübergehend deaktivieren kann. Der Benutzer kann den Remote-Desktop auch daran hindern, angezeigt zu werden. Diese Option ist verfügbar, wenn **Anzeigen und steuern** ausgewählt ist. Wenn **Bildschirm, Maus und Tastatur** die ausgewählte Kundeneinschränkung ist, steht ein Kontrollkästchen zur Verfügung: **Bei Sitzungsbeginn automatisch einen privaten Bildschirm anfordern**. Der Bildschirm „Privatsphäre“ ist nur für Sitzungen verfügbar, die über einen Jump-Client, ein Remote Jump-Item oder ein lokales Jump-Item gestartet wurden. Wir empfehlen die Verwendung eines „Privatsphäre“-Bildschirms für unbeaufsichtigte Sitzungen. Das Remote-System muss den „Privatsphäre“-Bildschirm unterstützen.

> *Weitere Informationen siehe Eingeschränkte Kundeninteraktion: Privater Bildschirm, Remote-Eingaben deaktivieren unter https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/privacy-screen.htm.*

Aufforderungsverhalten bei Anwendungsfreigabe

Legen Sie fest, ob eine Anforderung zur Bildschirmfreigabe den Kunden immer oder nie dazu auffordern soll, die freizugebenden Anwendungen auszuwählen, oder ob der Benutzer wählen kann, ob eine Anwendungsfreigabe-Aufforderung erscheint oder nicht. Mit der Auswahl von **Immer** oder **Support-Techniker entscheidet** können Sie außerdem Anwendungsfreigabebeschränkungen vordefinieren.

> *Weitere Informationen siehe Anwendungsfreigabe: Einschränkung der für den Support-Techniker sichtbaren Elemente unter https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/application-sharing.htm.*

Synchronisierungsrichtung für Zwischenablage

Diese Option ist verfügbar, wenn **Anzeigen und steuern** ausgewählt ist. Wählen Sie, wie der Inhalt der Zwischenablage zwischen Support-Technikern und Endbenutzern ausgetauscht wird. Die Optionen sind:

- **Nicht berechtigt**: Der Support-Techniker darf die Zwischenablage nicht verwenden, es werden keine Zwischenablage-Symbole im Konsole d. Support-Technikers angezeigt, und die Befehle zum Ausschneiden und Einfügen funktionieren nicht.
- **Zulässig vom Support-Techniker zum Kunden:** Der Support-Techniker kann den Inhalt der Zwischenablage an den Kunden weiterleiten, kann aber nicht aus der Zwischenablage des Endbenutzers einfügen. Nur das Zwischenablage-Symbol Senden wird im Konsole d. Support-Technikers angezeigt.
- **Zulässig in beide Richtungen:** Der Inhalt der Zwischenablage kann in beide Richtungen übertragen werden. Beide Symbole Zwischenablage senden und abrufen werden im Konsole d. Support-Technikers angezeigt.

> *Weitere Informationen über den Zwischenablage-Synchronisationsmodus finden Sie unter „Sicherheit: Verwalten der Sicherheitseinstellungen“ auf Seite 236.*

Browserfreigabe

Browserfreigabe-Regeln

Damit kann der Benutzer die gleiche Website anzeigen, die der Kunde sieht, ohne die Kontrolle zu besitzen oder andere Anwendungen zu sehen. Falls **Nicht definiert** gewählt wurde, wird diese Option durch die Richtlinie der nächstniedrigeren Priorität bestimmt. Diese Einstellung kann von einer Richtlinie mit höherer Priorität überschrieben werden.

> *Weitere Informationen finden Sie in Bildschirmfreigabe bei Remote-Kunde für Anzeige und Steuerung unter https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/screen-sharing.htm.*

Anmerkungen

Anmerkungsregeln

Gibt dem Benutzer die Möglichkeit, Anmerkungswerkzeuge zu verwenden, um auf dem Bildschirm des Remote-Benutzers zu zeichnen. Falls **Nicht definiert** gewählt wurde, wird diese Option durch die Richtlinie der nächstniedrigeren Priorität bestimmt. Diese Einstellung kann von einer Richtlinie mit höherer Priorität überschrieben werden.

Weitere Informationen finden Sie in Verwenden von Anmerkungen, um auf dem Remote-Bildschirm zu zeichnen auf https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/annotations.htm.

Dateitransfer

Dateitransfer-Regeln

Ermöglicht es dem Benutzer, Dateien auf das Remote-System hochzuladen, Dateien vom Remote-System herunterzuladen oder beides. Falls **Nicht definiert** gewählt wurde, wird diese Option durch die Richtlinie der nächstniedrigeren Priorität bestimmt. Diese Einstellung kann von einer Richtlinie mit höherer Priorität überschrieben werden.

Zugängliche Pfade im Dateisystem des Kunden

Gestattet es Benutzern, Dateien direkt zu oder von jeglichen oder nur von bestimmten Verzeichnissen auf dem Remote-System zu übertragen.

Zugängliche Pfade im Dateisystem des Support-Technikers

Gestattet es Benutzern, Dateien direkt zu oder von jeglichen oder nur von bestimmten Verzeichnissen auf seinem lokalen System zu übertragen.

Weitere Informationen finden Sie in Dateitransfer zum und vom Remote-System unter https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/file-transfer.htm.

Befehlsshell

Befehlsshell-Regeln hier eingeben

Damit kann der Benutzer über eine virtuelle Befehlszeilen-Schnittstelle Befehle auf dem Remote-Computer ausgeben. Falls **Nicht definiert** gewählt wurde, wird diese Option durch die Richtlinie der nächstniedrigeren Priorität bestimmt. Diese Einstellung kann von einer Richtlinie mit höherer Priorität überschrieben werden.

***Hinweis:** Der Zugriff auf Befehlsshells kann in Shell Jump-Sitzungen nicht eingeschränkt werden.*

Weitere Informationen finden Sie in Zugriff auf den Remote-Befehlsshell unter https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/command-shell.htm.

Systeminformationen

Regeln für Systeminformationen

Ermöglicht es dem Benutzer, Systeminformationen zum Remote-Computer anzuzeigen. Falls **Nicht definiert** gewählt wurde, wird diese Option durch die Richtlinie der nächstniedrigeren Priorität bestimmt. Diese Einstellung kann von einer Richtlinie mit höherer Priorität überschrieben werden.

Berechtigt, Aktionen zu Systeminformationen zu verwenden

Ermöglicht es dem Benutzer, mit Prozessen und Programmen auf dem Remote-System zu interagieren, ohne dass eine Bildschirmfreigabe erforderlich ist. Es können Prozesse beendet, Dienste gestartet, gestoppt, pausiert, fortgesetzt und neugestartet und Programme deinstalliert werden.

> *Weitere Informationen finden Sie in Anzeige von Systeminformationen unter https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/system-info.htm.*

Zugriff auf Registrierung

Verzeichniszugriff-Regeln

Ermöglicht es dem Benutzer, mit der Registrierung auf dem Remote-Windows-System zu interagieren, ohne dass eine Bildschirmfreigabe erforderlich ist. Schlüssel können angezeigt, hinzugefügt, gelöscht und bearbeitet, durchsucht und importiert werden.

> *Weitere Informationen finden Sie in Zugriff auf den Registrierungseditor am Remote-Endpunkt unter https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/registry-editor.htm.*

Vordefinierte Skripts

Regeln für vordefinierte Skripts

Damit kann der Benutzer vordefinierte Skripts ausführen, die für seine Teams erstellt wurden. Beachten Sie: Wenn sich der Benutzer in der Nur-Anzeige-Bildschirmfreigabe befindet, erhält der Kunde eine Aufforderung zur Ausführung des Skripts.Falls **Nicht definiert** gewählt wurde, wird diese Option durch die Richtlinie der nächstniedrigeren Priorität bestimmt. Diese Einstellung kann von einer Richtlinie mit höherer Priorität überschrieben werden.

> *Weitere Informationen finden Sie in Zugriff auf den Remote-Befehlsshell unter https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/command-shell.htm.*

Heraufsetzung

Heraufsetzungsregeln

Gibt dem Benutzer die Möglichkeit zu versuchen, den Kunden-Client so heraufzusetzen, dass er mit administrativen Rechten auf dem Remote-System ausgeführt wird. Falls **Nicht definiert** gewählt wurde, wird diese Option durch die Richtlinie der nächstniedrigeren Priorität bestimmt. Diese Einstellung kann von einer Richtlinie mit höherer Priorität überschrieben werden.

> *Weitere Informationen finden Sie in Den Client heraufsetzen auf https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/elevation.htm.*

Support-Button Bereitstellung

Support-Button Bereitstellungsregeln

Ermöglicht es dem Benutzer, während einer Sitzung eine Support-Button bereitzustellen oder zu entfernen. Die für die Bereitstellung verfügbaren Orte sind von den obigen Support-Button-Einstellungen abhängig. Falls **Nicht definiert** gewählt wurde, wird diese Option durch die Richtlinie der nächstniedrigeren Priorität bestimmt. Diese Einstellung kann von einer Richtlinie mit höherer Priorität überschrieben werden.

> *Weitere Informationen finden Sie in Überblick über Support-Sitzungen Tech. und Tools unter https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/support-session-overview.htm.*

Fixieren/Lösen von Jump-Clients

Regeln zum Fixieren/Lösen von Jump-Clients

Ermöglicht es dem Benutzer, während einer Sitzung einen Jump-Client zu fixieren oder zu lösen. Die für die Bereitstellung verfügbaren Orte sind von den obigen Jump-Client-Einstellungen abhängig. Falls **Nicht definiert** gewählt wurde, wird diese Option durch die Richtlinie der nächstniedrigeren Priorität bestimmt. Diese Einstellung kann von einer Richtlinie mit höherer Priorität überschrieben werden.

> *Weitere Informationen finden Sie in Überblick über Support-Sitzungen Tech. und Tools unter https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/support-session-overview.htm.*

Chat

> *Für weitere Informationen siehe Während einer Sitzung mit dem Kunden chatten unter https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/chat.htm.*

Chat-Regeln

Damit kann der Benutzer mit dem Remote-Kunden chatten. Falls **Nicht definiert** gewählt wurde, wird diese Option durch die Richtlinie der nächstniedrigeren Priorität bestimmt. Diese Einstellung kann von einer Richtlinie mit höherer Priorität überschrieben werden.

Berechtigt, URLs zum Webbrowser des Kunden zu pushen

Damit kann der Benutzer eine URL im Chat-Bereich eingeben und dann auf **URL pushen** klicken, um automatisch einen Webbrowser mit dieser Adresse auf dem Remote-Computer zu öffnen.

Berechtigt, Dateien mithilfe der Chat-Schnittstelle zu senden

Damit kann der Benutzer Dateien über die Chat-Schnittstelle senden.

> *Weitere Informationen erhalten Sie unter Kunden-Client: Schnittstelle für Support-Sitzungen Tech. unter https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/customer-support-interface.htm.*

Verhalten beim Beenden der Sitzung

Wenn die Verbindung innerhalb der unter **Neuverbindungs-Zeitüberschreitung** festgelegten Zeit nicht wiederhergestellt werden kann, legen Sie hier fest, wie verfahren werden soll. Um zu verhindern, dass ein Endbenutzer nach einer heraufgesetzten Sitzung auf unautorisierte Berechtigungen zugreift, stellen Sie den Client so ein, dass der Endbenutzer am Ende der Sitzung automatisch vom Remote-Windows-Computer abgemeldet wird, dass der Remote-Computer gesperrt wird, oder dass nichts getan wird. Diese Regeln gelten nicht für Browser-Freigabesitzungen.

Benutzer berechtigen, diese Einstellung sitzungsweise außer Kraft zu setzen

Sie können einem Benutzer die Übersteuerung der Sitzungsbeendigungseinstellung über die Registerkarte **Zusammenfassung** in der Konsole während einer Sitzung gestatten.

Verfügbarkeitseinstellungen

Welche Verfügbarkeitseinstellungen soll diese Gruppenrichtlinie kontrollieren?

Entscheiden Sie, ob eine Einstellung in dieser Richtlinie **Definiert** sein soll. Wenn dies der Fall ist, können Sie **Endgültig** auswählen, um zu verhindern, dass andere Richtlinien mit niedrigerer Priorität den mit dieser Richtlinie festgelegten Berechtigungswert aufheben. Wählen Sie **Alle**, um alle Einstellungen in diesem Abschnitt zu definieren.

Pool für Lizenzen für umfassenden Support

Wählen Sie den Lizenzpool, zu dem dieser Support-Techniker gehören soll. Wenn sich dieser Support-Techniker an der Konsole d. Support-Technikers anmeldet, wird eine Lizenz aus dem zugewiesenen Lizenzpool verbraucht. Wird **Keine** ausgewählt, kann sich der Support-Techniker nur an der Konsole d. Support-Technikers anmelden, wenn mindestens eine Lizenz aus den Lizenzpools noch nicht zugewiesen wurde und verfügbar ist.

Anmeldungszeitplan

Zugang von Support-Technikern auf den folgenden Zeitplan beschränken

Legen Sie einen Zeitplan fest, der definiert, wann sich Benutzer an der Konsole d. Support-Technikers anmelden können. Legen Sie die Zeitzone fest, die für diesen Zeitplan verwendet werden soll, und fügen Sie dann einen oder mehrere Zeitplaneinträge hinzu. Geben Sie für jeden Eintrag das Startdatum und die Startuhrzeit an sowie das Enddatum und die Enduhrzeit.

Wenn die Zeit beispielsweise für 8 Uhr (Start) und 17 Uhr (Ende) festgelegt wird, kann sich ein Benutzer jederzeit innerhalb dieses Zeitfensters anmelden und auch nach dem festgelegten Endzeitpunkt weiterarbeiten. Er kann sich nach 17 Uhr allerdings nicht erneut anmelden.

Abmeldung erzwingen, wenn der Zeitplan die Anmeldung nicht gestattet

Wenn eine strengere Zugriffskontrolle erforderlich ist, aktivieren Sie diese Option. Damit wird der Benutzer gezwungen, sich zum geplanten Endzeitpunkt abzumelden. Iin diesem Fall erhält der Benutzer 15 Minuten vor der Trennung der Verbindung wiederholte Benachrichtigungen. Wenn der Benutzer abgemeldet wird, folgen jegliche ihm angehörenden Sitzungen den Regeln zum Sitzungsrückfall.

Mitgliedschaften

Welche Mitgliedschaftseinstellungen soll diese Gruppenrichtlinie kontrollieren?

Entscheiden Sie, ob eine Einstellung in dieser Richtlinie **Definiert** sein soll. Wenn dies der Fall ist, können Sie **Endgültig** auswählen, um zu verhindern, dass andere Richtlinien mit niedrigerer Priorität den mit dieser Richtlinie festgelegten Berechtigungswert aufheben. Wählen Sie **Alle**, um alle Einstellungen in diesem Abschnitt zu definieren.

Mitgliedschaft in technischem Support-Team hinzufügen

Suchen Sie nach Teams, denen Mitglieder dieser Gruppenrichtlinie angehören sollen. Sie können die Rolle als **Teammitglied**, **Teamleiter** oder **Team-Manager** festlegen. Diese Rollen spielen in der **Dashboard**-Funktion der Konsole d. Support-Technikers eine wichtige Rolle. Klicken Sie auf **Hinzufügen**.

Hinzugefügte Teams werden in einer Tabelle angezeigt. Sie können die Rolle von Mitgliedern in einem Team bearbeiten oder das Team aus der Liste löschen.

Mitgliedschaft in technischem Support-Team entfernen

Suchen Sie nach Teams, aus denen Mitglieder dieser Gruppenrichtlinie entfernt werden sollen, und klicken Sie auf **Hinzufügen**. Entfernte Teams werden in einer Tabelle angezeigt. Sie können ein Team aus der Liste löschen.

Hinzufügen von Jumpoint-Mitgliedschaften

Suchen Sie nach Jumpoints, auf die Mitglieder dieser Gruppenrichtlinie Zugriff haben sollen, und klicken Sie dann auf **Hinzufügen**. Hinzugefügte Jumpoints werden in einer Tabelle angezeigt. Sie können einen Jumpoint aus der Liste löschen.

Jumpoint-Mitgliedschaften entfernen

Suchen Sie nach Jumpoints, von denen Mitglieder dieser Gruppenrichtlinie nicht entfernt werden sollen, und klicken Sie dann auf **Hinzufügen**. Entfernte Jumpoints werden in einer Tabelle angezeigt. Sie können einen Jumpoint aus der Liste löschen.

Hinzufügen von Jump-Gruppenmitgliedschaften

Suchen Sie nach Jump-Gruppen, denen Mitglieder dieser Gruppenrichtlinie angehören sollen. Sie können die Jump-Element-Rolle jedes Benutzers festlegen, um ihre Berechtigungen für Jump-Elemente in dieser Jump-Gruppe festzulegen. Alternativ können Sie die standardmäßigen Jump-Element-Rollen dieser Gruppenrichtlinie oder die auf der Seite **Benutzer und Sicherheit > Benutzer** konfigurierten Rollen verwenden. Eine Jump-Element-Rolle ist ein vordefinierter Berechtigungssatz zur Verwaltung und Nutzung von Jump-Elementen.

> *Weitere Informationen finden Sie in Jump-Element-Rollen: Konfigurieren von Berechtigungssätzen für Jump-Elemente unter www.beyondtrust.com/docs/remote-support/getting-started/admin/jump-item-roles.htm.*

Sie können auch eine Jump-Richtlinie anwenden, um den benutzerzugriff auf die Jump-Elemente dieser Jump-Gruppe zu verwalten.

Hinzugefügte Jump-Gruppen werden in einer Tabelle angezeigt. Sie können die Einstellungen einer Jump-Gruppe bearbeiten oder die Jump-Gruppe aus der Liste löschen.

Entfernen von Jump-Gruppenmitgliedschaften

Suchen Sie nach Jump-Gruppen, aus denen Mitglieder dieser Gruppenrichtlinie entfernt werden sollen, und klicken Sie auf **Hinzufügen**. Entfernte Jump-Gruppen werden in einer Tabelle angezeigt. Sie können eine Jump-Gruppe aus der Liste löschen.

Vault-Kontomitgliedschaften hinzufügen

Suchen Sie nach einem Konto, wählen Sie **Vault-Kontenrolle** und klicken Sie dann auf **Hinzufügen**, um Mitgliedern der Richtlinie Zugriff auf das ausgewählte Vault-Konto zu gewähren. Die Mitgliedschaften von Benutzern können von anderen Gruppenrichtlinien hinzugefügt werden. Rufen Sie **Vault > Konten** auf, um alle Mitglieder jeder Gruppe anzuzeigen. Benutzer können für die Nutzung des Vault-Kontos einer von zwei Rollen zugewiesen werden:

- **Einfügen** (Standardwert): Benutzer mit dieser Rolle können dieses Konto in Remote Support-Sitzungen verwenden.
- **Einfügen und auschecken**: Benutzer mit dieser Rolle können dieses Konto in Remote Support-Sitzungen verwenden und das Konto auf **/login** auschecken. Die Berechtigung **Auschecken** hat keinen Einfluss auf generische SSH-Konten.

> ***Hinweis:** Aktivieren Sie die Berechtigung **Vault-Kontomitgliedschaft hinzufügen**, um einem Vault-Konto in einer Gruppenrichtlinie eine **Vault-Konto-Rolle** hinzuzufügen. Die **Rolle des Rolle des Vault-Kontos** wird auf der Liste der der Gruppenrichtlinie hinzugefügten Konten angezeigt.*

Vault-Kontogruppenmitgliedschaften hinzufügen

Suchen Sie nach einer Kontogruppe, legen Sie die **Vault-Konto-Rolle** fest und klicken Sie dann auf **Hinzufügen**, um Mitgliedern der Richtlinie Zugriff auf die Gruppe der Vault-Konten zu gewähren. Die Mitgliedschaften von Benutzern können von anderen Gruppenrichtlinien hinzugefügt werden. Rufen Sie **Vault > Konten** auf, um alle Mitglieder jeder Gruppe anzuzeigen. Benutzern kann für die Verwendung der Gruppe der Vault-Konten eine von zwei Rollen zugewiesen werden:

- **Einfügen** (Standardwert): Benutzer mit dieser Rolle können dieses Konto in Remote Support-Sitzungen verwenden.
- **Einfügen und auschecken**: Benutzer mit dieser Rolle können dieses Konto in Remote Support-Sitzungen verwenden und das Konto auf **/login** auschecken. Die Berechtigung **Auschecken** hat keinen Einfluss auf generische SSH-Konten.

Hinweis: *Aktivieren Sie die Berechtigung* ***Vault-Kontogruppen hinzufügen****, um in einer Gruppenrichtlinie eine* ***Rolle des Vault-Kontos*** *hinzuzufügen. Die* ***Rolle des Rolle des Vault-Kontos*** *wird auf der Liste der der Gruppenrichtlinie hinzugefügten Kontengruppen angezeigt.*

Richtlinie exportieren

Sie können eine Gruppenrichtlinie von einer Website exportieren und diese Berechtigungen in eine Richtlinie auf einer anderen Website importieren. Bearbeiten Sie die Richtlinie, die Sie exportieren möchten, und rollen Sie zum Ende der Seite. Klicken Sie auf **Richtlinie exportieren** und speichern Sie die Datei.

Hinweis: *Wenn eine Gruppenrichtlinie exportiert wird, werden nur der Richtlinienname, die Kontoeinstellungen und die Berechtigungen exportiert. Richtlinienmitglieder, Support-Mitgliedschaften und Jumpoint-Mitgliedschaften sind nicht im Export enthalten.*

Richtlinie importieren

Sie können exportierte Gruppenrichtlinieneinstellungen auf jeder anderen BeyondTrust-Website importieren, die den Import von Gruppenrichtlinien unterstützt. Erstellen Sie eine neue Gruppenrichtlinie, oder bearbeiten Sie eine vorhandene Richtlinie, deren Berechtigungen Sie überschreiben möchten, und rollen Sie zum Ende der Seite. Durchsuchen Sie die Richtliniendatei und klicken Sie dann auf **Richtliniendatei auswählen**. Nachdem die Richtliniendatei hochgeladen wurde, wird die Seite aktualisiert, sodass Sie Änderungen vornehmen können. Klicken Sie auf **Speichern**, damit die Gruppenrichtlinie wirksam wird.

Hinweis: *Durch Importieren einer Richtliniendatei in eine bestehende Gruppenrichtlinie werden alle zuvor festgelegten Berechtigungen überschrieben; ausgenommen sind Richtlinienmitglieder, Teammitgliedschaften und Jumpoint-Mitgliedschaften.*

Kerberos-Keytab: Kerberos-Keytab verwalten

Kerberos-Keytab-Verwaltung

BeyondTrust unterstützt die Einzelanmeldungsfunktion mithilfe des Kerberos-Authentifizierungsprotokolls. Hierdurch können sich Benutzer beim B Series Appliance authentifizieren, ohne ihre Anmeldedaten eingeben zu müssen. Die Kerberos-Authentifizierung gilt sowohl für die Webschnittstelle /login als auch für die Konsole d. Support-Technikers.

Um Kerberos mit Ihrem B Series Appliance zu integrieren, müssen Sie eine Kerberos-Implementierung entweder derzeit bereitgestellt haben oder gerade dabei sein, sie bereitzustellen. Die spezifischen Anforderungen lauten wie folgt:

- Sie müssen ein funktionstüchtiges Key Distribution Center (KDC) implementiert haben.
- Die Uhrzeiten müssen über alle Clients, das KDC und das B Series Appliance hinweg synchronisiert werden. Die Verwendung eines Network Time Protocol-Servers (NTP) ist eine einfache Möglichkeit, dies zu gewährleisten.
- Sie müssen einen Service Principal Name (SPN) im KDC für Ihr B Series Appliance erstellt haben.

Konfigurierte Principals

Im Abschnitt **Konfigurierte Principals** werden alle verfügbaren SPNs für jede hochgeladene Keytab-Datei aufgeführt.

Wenn SPNs verfügbar sind, können Sie einen Kerberos-Sicherheitsanbieter auf der Seite **Sicherheitsanbieter** konfigurieren und definieren, welche Benutzer-Principals über Kerberos bei dem B Series Appliance authentifiziert werden können.

Keytab-Datei importieren

Datei wählen

Exportieren Sie die Keytab-Datei für den SPN aus Ihrem KDC und laden Sie sie zu B Series Appliance hoch.

> *Weitere Informationen finden Sie in Kerberos-Server für die Einzelanmeldung unter https://www.beyondtrust.com/docs/remote-support/how-to/integrations/security-providers/kerberos/index.htm.*

Lizensierung: Support-Techniker zu Lizenzpools zuordnen

Pools für Lizenzen für umfassenden Support

Sie können Pools konfigurieren, die die Struktur Ihres Support-Unternehmens widerspiegeln und sicherstellen, dass jeder Pool über die berechtigte Menge an Lizenzen verfügt. Die Tabelle zeigt die Anzahl reservierter Lizenzen und die maximale Anzahl von Lizenzen an, die für jeden Pool gestattet sind, zusammen mit der Anzahl an Benutzern, die diesem Pool zugewiesen sind. Beachten Sie, dass diese Anzahl nicht Benutzer berücksichtigt, die über eine Gruppenrichtlinie zugewiesen wurden, sowie eingeladene Support-Techniker.

Hinweis: *Aktive Lizenzpakete sind in der Anzahl der vollständigen Support-Lizenzen enthalten; sie können allerdings keinen Lizenzpools zugewiesen werden.*

Hinzufügen, Bearbeiten, Löschen

Erstellen Sie einen neuen Pool, bearbeiten Sie einen bestehenden Pool oder entfernen Sie einen bestehenden Pool.

Pool mit Lizenzen für umfassenden Support hinzufügen oder bearbeiten

Name

Erstellen Sie einen eindeutigen Namen, um diesen Pool leichter zu identifizieren. Dieser Name sollte Administratoren beim Zuweisen von Benutzern oder Gruppen zu einem Lizenzpool helfen.

Beschreibung

Fügen Sie eine kurze Beschreibung hinzu, um den Zweck dieses Pools zusammenzufassen.

Reservierte Lizenzen

Die Anzahl an Lizenzen, die für diesen Pool reserviert werden sollte. Wenn alle anderen Lizenzen verwendet werden und ein Support-Techniker, der nicht Teil dieses Pools ist, versucht, sich in der Konsole d. Support-Technikers anzumelden, wird ihm die Anmeldung verweigert. Die Anmerkung unten zeigt, wie viele nicht reservierte Lizenzen noch verfügbar sind und zugewiesen werden können.

Maximale Lizenzen

Die maximale Anzahl an Lizenzen, die von Benutzern dieses Pools verbraucht werden kann. Wenn die maximale Anzahl an Lizenzen bereits von Benutzern dieses Pools verwendet wird, wird einem Support-Techniker, der Teil des Pools ist und sich in der Konsole d. Support-Technikers anmelden möchte, die Anmeldung verweigert. Wenn Sie kein Maximum festlegen möchten, setzen Sie einen Haken bei **Unbegrenzt**.

Lizenzpool für eingeladene Support-Techniker

Identisch mit Einladung für Support-Techniker

Wenn ein Support-Techniker eine Support-Techniker-Einladung an einen externen Support-Techniker sendet, sollte der eingeladene Support-Techniker eine Lizenz aus dem gleichen Pool verbrauchen wie der Support-Techniker, der die Anforderung gesendet hat.

Verwenden des folgenden Pools für alle eingeladenen Support-Techniker

Wenn ein Support-Techniker eine Support-Techniker-Einladung an einen externen Support-Techniker sendet, sollte der eingeladene Support-Techniker eine Lizenz aus dem angegebenen Pool verbrauchen. Wird diese Option auf **Keine** festgelegt, wird die verwendete Lizenz aus den nicht reservierten Lizenzen bezogen.

Lizenznutzungsbenachrichtigung

Alarme für Lizenzschwellenwert aktivieren

E-Mail empfangen, wenn die Anzahl der verwendeten Lizenzen den unten angegebenen Schwellenwert erreicht.

Alarmoptionen für Lizenzschwellenwert

Legen Sie den Lizenzschwellenwert auf eine Gesamtanzahl oder einen Prozentsatz verwendeter Lizenzen fest. Legen Sie den Mindestzeitraum fest, der verstreichen muss, bevor eine weitere E-Mail gesendet werden kann.

Alarme für abgelehnte Anmeldung aktivieren

Falls aktiviert, wird ein E-Mail-Alarm gesendet, wann immer sich ein Support-Techniker aufgrund ungenügender Lizenzen, ungenügender reservierter Slots oder Erreichen des maximalen Lizenzlimits nicht anmelden kann.

Lizenzalarm-Kontakt

Geben Sie eine oder mehrere E-Mail-Adressen ein, an die E-Mails gesendet werden sollen. Trennen Sie Adressen mit einem Leerzeichen.Diese Funktion erfordert eine gültige SMTP-Konfiguration für Ihr B Series Appliance, die auf der Seite **/login > Verwaltung > E-Mail-Konfiguration** eingerichtet wird.

Berichte

Support: Berichte zu Sitzungsaktivitäten

Support-Berichte

Administratoren und berechtigte Benutzer können breitgefächerte, umfassende Berichte generieren und auch bestimmte Filterfunktionen aktivieren, um Informationen in diesen Berichten enthalten sind, auf Grundlage von ganz klaren Bedürfnissen anzupassen.

Berichtstyp

Generieren Sie einen Aktivitätsbericht gemäß vier unterschiedlichen Berichtstypen: **Sitzung**, **Zusammenfassung**, **Kundenaustrittsumfrage** und **Support-Techniker-Umfrage**.

Filter

Wenden Sie bei Bedarf Filteroptionen an, um mehr personalisierte Berichte aus den ggrundlegenden Berichttypen zu erhalten. Aktivieren Sie einen oder mehrere Filter, jedoch werden nur die Sitzungen angezeigt, die mit allen ausgewählten Filtern übereinstimmen.

Sitzungs-ID oder Sequenznummer

Bei dieser eindeutigen Kennung müssen Sie die ID (LSID) oder die Sequenznummer für die gesuchte Einzelsitzung angeben. Dies kann oft hilfreich sein, wenn Sie eine externe CRM-Integration oder ein externes Ticketing-System verwenden. Dieser Filter kann nicht mit anderen Filtern kombiniert werden.

Datumsbereich

Wählen Sie das Startdatum, für das Berichtsdaten abgerufen werden sollen. Wählen Sie dann entweder die Anzahl von Tagen, für die Ihr Bericht abgerufen werden soll, oder ein Enddatum.

Kunde

Filtern Sie Sitzungen nach Kundenname, Unternehmensname, Computername, öffentlicher IP oder privater IP.

Öffentliche Website

Sie können filtern, um Ihren Bericht auf eine bestimmte öffentliche Website zu beschränken.

Support-Techniker

Wählen Sie im Dropdown-Menü die Art der Support-Techniker-Teilnahme aus, die Sie hinzufügen möchten. Sie können Sitzungen wählen, denen beliebige Support-Techniker beigetreten sind, keine Support-Techniker beigetreten sind, ein bestimmter Support-Techniker beigetreten ist, oder an denen ein Support-Techniker eines Teams teilgenommen hat, einschließlich Sitzungen, die nie dem entsprechenden Team zugeordnet wurden.

Team

Wählen Sie im Dropdown-Menü die Art der Team-Teilnahme aus, die Sie hinzufügen möchten. Sie können Sitzungen wählen, die mindestens einem Team zugeordnet wurden, Sitzungen, die nie einem Team zugeordnet wurden, oder Sitzungen, die einem bestimmten Team zugeordnet wurden.

Externer Schlüssel

Sie können filtern, um Berichte zu Sitzungen zu erstellen, für die der gleiche spezifische externe Schlüssel verwendet wurde.

Umfasst nur beendete Sitzungen

Filtern Sie, um nur Sitzungen einzufügen, die abgeschlossen wurden. Davon sind noch laufende Sitzungen ausgeschlossen.

Gruppieren nach *(Nur sichtbar für Zusammenfassungsberichte)*

Wählen Sie, ob Zusammenfassungsberichtsdaten nach Support-Techniker, Team oder nach öffentlicher Website gruppiert werden sollen.

Support-Sitzung Tech – Berichten von Ergebnissen

Sie können alle Sitzungen anzeigen, die den auf der vorherigen Seite angegebenen Kriterien entsprechen. Sitzungsberichte umfassen grundlegende Sitzungsinformationen, zusammen mit Links zu Sitzungsdetails, Chat-Mitschriften und Videoaufzeichnungen von Bildschirmfreigabe-, „Eigenen Bildschirm anzeigen“- und Befehlsshell-Sitzungen. Klicken Sie auf **Sichtbare Spalten auswählen**, um festzulegen, welche Daten angezeigt werden sollen.

Support-Sitzung Tech-Detail

Sitzungsberichte enthalten eine detaillierte Abschrift des Chats, die Zahl der übertragenen Dateien (und Details zu fehlgeschlagenen Dateiübertragungen), sowie die angeforderten und erteilten Berechtigungen. Spezifische Befehlsinformationen, die für *Ausführen als*-Befehle relevant sind, einschließlich Anmeldedaten, werden ebenfalls bereitgestellt, aber diese Berichterstattung kann deaktiviert werden unter „Sicherheit: Verwalten der Sicherheitseinstellungen“ auf Seite 236. Andere Informationen betreffen unter anderem die öffentliche Website, über die die Sitzung stattfand, die Sitzungsdauer, die Namen und IP-Adressen der lokalen und Remote-Computer sowie Remote-Systeminformationen (falls aktiviert). Berichte können online angesehen oder auf Ihr lokales System heruntergeladen werden.

Ist die Sitzungsaufzeichnung aktiviert, können Sie ein Video einzelner Sitzungen anzeigen, einschließlich von Informationen, wer die Maus und die Tastatur zu einem bestimmten Zeitpunkt der Sitzung gesteuert hat. Dementsprechend können Sie bei aktivierter Aufzeichnung von „Eigenen Bildschirm anzeigen“ alle Videos des Systems eines Support-Technikers während einer „Eigenen Bildschirm anzeigen“-Sitzung anzeigen und herunterladen. Ist die Eingabeaufforderungsaufzeichnung aktiviert, können Sie auch die Aufzeichnung aller während der Sitzung ausgeführten Befehlsshells anzeigen. Alle Aufzeichnungen werden im Raw-Format auf dem B Series Appliance gespeichert und beim Anzeigen oder Herunterladen in ein komprimiertes Format konvertiert.

Zugriffszusammenfassungsbericht

Zusammenfassungsberichte bieten einen Überblick über die Aktivitäten in einem bestimmten Zeitraum und sind nach Support-Techniker, Team oder öffentlicher Website sortiert. Statistiken umfassen die Gesamtanzahl ausgeführter Sitzungen, die durchschnittliche Anzahl von Sitzungen nach Wochentag und die durchschnittliche Dauer der Sitzungen.

Kundenaustrittsumfrage oder Bericht zur Support-Techniker-Umfrage

Sehen Sie Berichte von Antworten auf Ihre benutzerdefinierten Umfragen, aufgeschlüsselt nach öffentlicher Website. Für jede Frage, die Sie in Ihre Umfragen aufnehmen, kommt eine Spalte hinzu, die dem im Feld **Berichtskopfzeile** angegebenen Namen entsprechend benannt wird. Bei Multiple-Choice-Fragen wird der **protokollierte Wert** als Antwort angezeigt. Wenn Support-Techniker während der Sitzung auch Zugang zur Support-Techniker-Umfrage erhalten und der Administrator diese zur Erstellung eines detaillierten Arbeitsablaufs verwendet hat, werden diese Fragen und/oder Felder zusammen mit den Antworten des Support-Technikers ebenfalls im Bericht angezeigt.

Teamaktivitätsbericht

Zeigen Sie alle Team-Aktivitäten an, die den auf der vorherigen Seite angegebenen Kriterien entsprechen. Team-Aktivitätsberichte umfassen Informationen zu Benutzern, die sich in der Konsole d. Support-Technikers an- oder abmelden, Chatnachrichten, die zwischen Teammitgliedern ausgetauscht werden, Änderungen am Status des Support-Technikers, Aktionen bei der Bildschirmfreigabe unter Benutzern, wie diese im Chat erscheinen, und freigegebene und heruntergeladene Dateien.

Datumsbereich

Wählen Sie das Startdatum, für das Berichtsdaten abgerufen werden sollen. Wählen Sie dann entweder die Anzahl von Tagen, für die Ihr Bericht abgerufen werden soll, oder ein Enddatum.

Team

Wählen Sie das Team, zu dem Sie Ergebnisse anzeigen möchten.

Hinweis: *Alle in den Remote Support-Berichten aufgeführten Elemente sind in der Reihenfolge vom neuesten bis zum ältesten Element geordnet.*

Präsentation: Berichte zu Präsentationsaktivitäten

Berichte | PRÄSENTATION

Präsentationen

Bereichsbeginn, Bereichsende

Wählen Sie das Startdatum, für das Berichtsdaten abgerufen werden sollen. Wählen Sie dann entweder die Anzahl von Tagen, für die Ihr Bericht abgerufen werden soll, oder ein Enddatum.

Präsentationsbericht-Ergebnisse

Sie können alle Präsentationen anzeigen, die den auf der vorherigen Seite angegebenen Kriterien entsprechen. Präsentationsberichte umfassen grundlegende Präsentationsinformationen zusammen mit Links zu Präsentationsdetails, Chat-Mitschriften und Videoaufzeichnungen. Klicken Sie auf **Sichtbare Spalten auswählen**, um festzulegen, welche Daten angezeigt werden sollen.

Lizensierung: Bericht zur Spitzen-Lizenznutzungszeit

Berichte | LIZENSIERUNG

Lizenzbericht für Support-Techniker

Datumsbereich

Wählen Sie das Startdatum, für das Berichtsdaten abgerufen werden sollen. Wählen Sie dann entweder die Anzahl von Tagen, für die Ihr Bericht abgerufen werden soll, oder ein Enddatum.

Gruppieren nach

Wählen Sie, ob Sie Berichtsdaten zur Spitzen-Lizenznutzungszeit nach Stunde, Tag oder Monat gruppieren möchten.

Lizenznutzungsbericht

Zeigen Sie Berichte zu den Spitzen-Lizenznutzungszeiten an. Zeigen Sie die Anzahl der angemeldeten Support-Techniker, die Anzahl der Support-Techniker im erweiterten Verfügbarkeitsmodus und die Gesamtanzahl verwendeter Lizenzen an.

Vault: Bericht zum Vault-Konto und zur Benutzeraktivität

Berichte | VAULT

Bericht zur Vault-Kontoaktivität

Datumsbereich

Wählen Sie das Startdatum, für das Berichtsdaten abgerufen werden sollen. Wählen Sie dann entweder die Anzahl von Tagen, für die Ihr Bericht abgerufen werden soll, oder ein Enddatum.

Konto

Um alle Ereignisse zu einem bestimmten in BeyondTrust Vault gespeicherten Konto anzuzeigen, geben Sie den Namen des Kontos ein oder wählen Sie das Konto aus der dynamischen Pop-up-Liste aus.

Durchgeführt von

Um alle Ereignisse anzuzeigen, die einen bestimmten Benutzer betreffen, geben Sie den Benutzernamen oder einen Teil davon ein und wählen dann den Benutzer aus der Liste aus. Um alle vom System ausgeführten Ereignisse zu sehen, klicken Sie in das Feld und wählen Sie dann **System** aus der Liste. Um alle Ereignisse anzuzeigen, die ein API-Konto betreffen, geben Sie **api** in das Feld ein und wählen Sie dann das API-Konto aus der Liste aus.

> ***Hinweis:*** *Wenn ein Benutzer aus Richtliniengründen anonymisiert worden ist, umfasst der Bericht zur* ***Vault-Kontoaktivität*** *womöglich Pseudonyme anstelle von Benutzerdaten, oder es wird darauf hingewiesen, dass diese Informationen gelöscht worden sind. Mehr über die Datenanonymisierung und -löschung aus Gründen der Richtlinieneinhaltung erfahren Sie unter Compliance: Anonymisierung von Daten zur Einhaltung von Richtlinien unter https://www.beyondtrust.com/docs/remote-support/getting-started/admin/compliance.htm.*

> *Weitere Informationen finden Sie in Vault Guide auf https://www.beyondtrust.com/docs/remote-support/how-to/vault/index.htm.*

Berichtsergebnisse zur Vault-Kontoaktivität

Da Benutzern getrennter Zugriff zum Verwenden und Auschecken von Konten gewährt werden kann, wird im **Vault-Kontoaktivitätsbericht** zwischen den beiden unterschieden. Dadurch können Administratoren den Unterschied zwischen einem Benutzer, der das Passwort des Kontos einsehen kann, und einem Benutzer, der nur Anmeldedaten in einer Sitzung eingeben kann, erkennen.

Im **Vault-Kontoaktivitätsbericht** zeigt die Spalte **Daten** mit dem Ereignis verbundene Informationen an. Das Ereignis **Anmeldedaten ausgecheckt** enthält einen Link **Details** in der neuen Spalte **Daten**, wenn Anmeldedaten während einer Sitzung ausgecheckt werden. Dieser Link führt zum **Detailbericht der Support-Sitzung**, in dem die Anmeldedaten verwendet wurden.

Hinweis: *Wenn die Anmeldedaten aus* ***/login*** *ausgecheckt werden, dann ist in der Spalte* ***Daten*** *kein Link* ***Details*** *vorhanden.*

Compliance: Daten anonymisieren zur Erfüllung von Compliance-Standards

Berichte | COMPLIANCE

WICHTIG!

*Standardmäßig ist die Registerkarte **Compliance** deaktiviert. Sollte Ihre Organisation diese Funktion benötigen, kontaktieren Sie bitte den BeyondTrust-Support unter https://www.beyondtrust.com/docs/index.htm#support.*

Support-Techniker-Anonymisierung

Informationen über Support-Techniker und die in Support-Sitzungen durchgeführten Maßnahmen können anonymisiert werden, um Datenschutzvorschriften und Compliance-Standards zu erfüllen.

Um Daten zu anonymisieren, wählen Sie einen Support-Techniker aus und klicken Sie dann auf **Support-Techniker-Aktivität durchsuchen**. Das System erstellt eine Liste der für den Support-Techniker gefundenen Informationen, zusammen mit einem zufällig generierten vorgeschlagenen Ersatzbegriff für die Informationen. Sie können auch auf **Benutzerdefiniert hinzufügen** klicken. Damit können Sie angepasste Informationen wie Kontonummern eingeben und suchen.

Um den Ersatztext zu ändern, klicken Sie auf die Schaltfläche **Bearbeiten**. Legen Sie in der Eingabeaufforderung **Ersatz bearbeiten** den gewünschten **Ersatz** fest. Wählen Sie **Im gesamten Verlauf bearbeiten** oder **In Nur in dieser Sitzung bearbeiten**.

Die Liste wird mit dem neuen Ersatzbegriff aktualisiert und zeigt an: „Alle Support-Sitzungen, Präsentationssitzungen, Team- und Vault-Konto-Aktivitätsereignisse dieses Support-Technikers werden als anonymisiert markiert am: (Datum und Uhrzeit).“ Klicken Sie nach Überprüfung der Ersatzbegriffe und des Zeitstempels auf **Benutzer löschen und anonymisieren**, um den Anonymisierungsprozess für die gesamte Software zu beginnen. Vor Beginn des Anonymisierungsprozesses müssen Sie Ihren Anzeigenamen eingeben, um zu bestätigen, dass Sie diese Aktion ausführen möchten.

WICHTIG!

Alle Sitzungsaufzeichnungen werden im Rahmen der Anonymisierungsanforderung gelöscht.

Kunden-Anonymisierung

Informationen über Kunden, die Support erhalten, sowie die während Support-Sitzungen durchgeführten Aktionen können anonymisiert werden, um Datenschutzrichtlinien und Compliance-Standards zu erfüllen.

Um Daten zu anonymisieren, geben Sie Name, Computername oder IP-Adresse des Kunden in das Feld ein. Aktivieren Sie das Kontrollkästchen **Teiltreffer**, falls Teiltreffer aufgeführt werden sollen. Klicken Sie dann auf **Kundenaktivitäten suchen**. Werden Daten gefunden, gibt das System eine Liste der zum Kunden gefundenen Informationen zusammen mit einem zufällig generierten vorgeschlagenen Ersatzbegriff für die Informationen wieder. Sie können auch auf **Benutzerdefiniert hinzufügen** klicken. Damit können Sie angepasste Informationen wie Kontonummern eingeben und suchen.

Um den Ersatztext zu ändern, klicken Sie auf die Schaltfläche **Bearbeiten**. Legen Sie in der Eingabeaufforderung **Ersatz bearbeiten** den gewünschten **Ersatz** fest. Wählen Sie **Im gesamten Verlauf bearbeiten** oder **In Nur in dieser Sitzung bearbeiten**.

Die Liste wird mit dem neuen Ersatzbegriff aktualisiert, und die Meldung „Die ausgewählten Support-Sitzungen Tech. und Präsentationssitzungen werden zu folgendem Zeitpunkt als anonymisiert gekennzeichnet: (Datum und Uhrzeit)“ erscheint. Klicken Sie nach dem Überprüfen der Ersatzbegriffe und des Zeitstempels auf **Ausgewählte Sitzungen anonymisieren**, um den Anonymisierungsprozess für die gesamte Software zu beginnen. Vor Beginn des Anonymisierungsprozesses müssen Sie Ihren Anzeigenamen eingeben, um zu bestätigen, dass Sie diese Aktion ausführen möchten.

WICHTIG!

Alle Sitzungsaufzeichnungen werden im Rahmen der Anonymisierungsanforderung gelöscht.

Status

Überprüfen Sie Informationen zu Anonymisierungsaufgaben, darunter gefundene Begriffe, Ersatzbegriffe, Art der zu anonymisierenden Daten und Status der Aufgabe.

Der Auftragsstatus wird alle 15 Sekunden automatisch aktualisiert. Der Status für abgeschlossene Anfragen bleibt 24 Stunden lang verfügbar.

***Hinweis:** Diese Statusinformationen sind außerdem in den Berichten **Support-Sitzungs-Details** und **Präsentationsdetails** verfügbar.*

***Hinweis:** Bei Umgebungen, in denen ein Failover für Atlas konfiguriert ist, wird die Datenanonymisierung erst abgeschlossen, wenn die Synchronisierung über alle Knoten oder Sicherungs-B Series Appliancee erfolgt ist.*

Jump-Item: Bericht über Jump-Item-Aktivität

Berichte | JUMP-ITEM

Administratoren und berechtigte Benutzer können breitgefächerte, umfassende Berichte generieren und auch bestimmte Filterfunktionen aktivieren, um Informationen in diesen Berichten enthalten sind, auf Grundlage von ganz klaren Bedürfnissen anzupassen. Alle Jump-Item-Ereignisse werden protokolliert. Standardmäßig werden die Protokolle 90 Tage lang gespeichert. Dieses Limit kann jedoch unter **Tage zur Aufbewahrung von Jump-Item-Protokollierungsinformationen** in **Verwaltung > Sicherheit > Verschiedenes** geändert werden.

Hinweis: *Stellen Sie sicher, dass die Berechtigung **Berichte anzeigen** in **Jump > Jump-Item-Rollen > Berechtigungen** aktiviert ist. Diese Option ist standardmäßig für alle integrierten Administratoren aktiviert (das erste Administratorkonto, das bei der Installation einer neuen Website erstellt wird).*

Hinweis: *Eine neue **Jump-Item-Rolle** mit dem Namen **Auditor** wird automatisch bei neuen Standortinstallationen erstellt. Bei bestehenden Installationen muss sie erstellt werden. Bei dieser Rolle ist nur eine einzige Berechtigung **Berichte anzeigen** aktiviert, sodass Administratoren einem Benutzer nur die Berechtigung zum Ausführen von Jump-Item-Berichten erteilen können, ohne eine andere Berechtigung erteilen zu müssen.*

Benutzer können die folgenden Ereignisse im Zusammenhang mit Jump-Items in Jump-Gruppen (persönlich oder gemeinsam genutzt) anzeigen:

- Jump Item erstellt
- Jump Item gelöscht
- Jump Item kopiert von
- Jump Item kopiert nach
- Jump Item verschoben von
- Jump Item verschoben nach
- Jump Item-Sitzung wurde gestartet

Die folgenden Informationen sind Bestandteil der Ereignisses:

- Die Uhrzeit, zu der das Ereignis eingetreten ist.
- Wenn das Ereignis von einem Benutzer ausgelöst wurde, werden die Identifikationsdaten des Benutzers mit diesem Ereignis verknüpft. Dies kann ein Benutzer, ein API-Konto oder eine Systeminformation sein. Die Daten in dieser Spalte werden als Hyperlink für **Benutzer** und **API-Konto** generierte Ereignisse angezeigt. Wenn Sie darauf klicken, wird eine Verknüpfung zu dieser **Benutzer**- oder **API-Konto**-Bearbeitungsseite hergestellt, vorausgesetzt, der Benutzer oder das API-Konto hat die entsprechende Berechtigung zum Anzeigen des Berichts.
- Der Ereignistyp.
- Jump-Item-Typ, d. h. einer der unterstützten Jump-Item-Typen, z. B. Jump-Client, Remote-Jump, Remote-RDP, usw.
- Name des Jump-Items. Die Daten in dieser Spalte werden als Hyperlink angezeigt. Wenn Sie darauf klicken, werden in der Berichtsansicht nur die Ereignisse angezeigt, die zu diesem speziellen Jump-Item gehören. Der Titel der Seite ändert sich außerdem in **Alle Jump-Item-Ereignisse zu: <Name des Jump-Items>**.

- Name der Jump-Gruppe. Dies ist die Quell-Jump-Gruppe für die Ereignisse **Jump-Item kopiert von** und **Jump-Item verschoben von**, und die Ziel-Jump-Gruppe für die Ereignisse **Jump-Item kopiert nach** und **Jump-Item verschoben nach**.
- Alle zusätzlichen Daten, die für das protokollierte Ereignis spezifisch sind. In diesem Feld kann die Ziel-Jump-Gruppe für die Ereignisse im Zusammenhang mit den Jump-Items **Kopieren** und **Verschieben** gespeichert werden.

Die Berichtsdaten sind in den Sicherungskopien enthalten.

Weitere Informationen finden Sie unter „Tage für die Aufbewahrung von Jump-Item-Protokollierungsinformationen“ auf Seite 242.

Filter

Sie können Jump-Item-Ereignisse finden, die den folgenden Filtern entsprechen. Sie können mehrere Filter verwenden, aber es werden nur Jump-Item-Ereignisse abgerufen, die allen von Ihnen aktivierten Filtern entsprechen.

Datumsbereich

Wählen Sie das Startdatum, für das Berichtsdaten abgerufen werden sollen. Wählen Sie dann entweder die Anzahl von Tagen, für die Ihr Bericht abgerufen werden soll, oder ein Enddatum.

Jump-Gruppe

Filtern Sie Sitzungen nach Jump-Elementen, die zu einer bestimmten Jump-Gruppe gehören. Wenn ausgewählt sind die folgenden Dropdown-Optionen verfügbar:

- Sucht alle Sitzungen, die über Jump-Elemente gestartet wurden, welche der gewählten Jump-Gruppe zugehören.
- Sucht alle Sitzungen, die über persönliche Jump-Elemente eines bestimmten Nutzers gestartet wurden.
- Sucht alle Sitzungen in Ihrer persönlichen Jump-Gruppe.

Jump-Item

Klicken Sie auf das Suchfeld, um alle Ereignisse zu finden, die ein bestimmtes Jump-Item betreffen.

Durchgeführt von

Klicken Sie auf das Suchfeld, um alle Ereignisse zu finden, die einen bestimmten Benutzer, ein API-Konto oder das System betreffen.

Klicken Sie auf **Bericht anzeigen**, wenn Sie fertig sind.

Syslog: Bericht mit allen Syslog-Dateien auf dem Gerät herunterladen

Syslog-Bericht

Syslog-Dateien herunterladen

Klicken Sie auf die Schaltfläche **Syslog-Dateien herunterladen**, um eine Zip-Datei mit allen auf dem Gerät verfügbaren Syslog-Dateien herunterzuladen.

Öffentliche Portale

Öffentliche Websites: Support-Portal anpassen

Öffentliche Websites

Konfigurieren Sie eine oder mehrere öffentliche Websites für Ihr BeyondTrust Appliance B Series. Eine öffentliche Website ist eine Website, auf der Kunden eine Sitzung beginnen können und über die der gesamte Sitzungsverkehr geleitet wird.

Neue Website hinzufügen, bearbeiten oder löschen

Erstellen Sie eine neue Website, bearbeiten Sie eine bestehende Website oder entfernen Sie eine bestehende Website.

Öffentliche Website hinzufügen oder bearbeiten

Name

Erstellen Sie einen eindeutigen Namen, um diese Website leichter zu identifizieren. Dieser Name hilft Ihnen, das öffentliche Portal zu bestimmen, über das ein Kunde den Zugang initiiert hat. Der standardmäßige Seitenname kann nicht geändert werden.

Website-Adresse

Jede Website muss mindestens eine DNS oder IP-Adresse aufweisen, die zu Ihrem BeyondTrust Appliance B Series hin aufgelöst wird. Mehrere Hostnamen können auf eine Website verweisen, ein Hostname kann aber nicht für mehrere Websites verwendet werden.

Standard-Support-Button-Profil

Wählen Sie, welches Support-Button-Profil auf der öffentlichen Website verwendet werden soll – entweder das Standardprofil oder ein personalisiertes Profil. Die Schaltflächen-Profile werden über die Seite **Konfiguration > Support-Buttonn** konfiguriert.

Öffentliche Vorlage

Konfigurieren Sie das Seitendesign und -layout, indem Sie eine öffentliche Webvorlage auswählen, die über die Seite **Öffentliches Portal > HTML-Vorlagen** konfiguriert wird.

> *Weitere Informationen finden Sie in Anpassen der Vorlage für die öffentliche Website unter https://www.beyondtrust.com/docs/remote-support/how-to/customize-portals/html-templates.htm.*

SAML-Authentifizierung erfordern

Ist auf der Seite **Benutzer und Sicherheit > Sicherheitsanbieter SAML für öffentliche Portale** konfiguriert, ist diese Option verfügbar. Wenn diese Option aktiviert ist, müssen Kunden eine Authentifizierung mit einem Identitätsanbieter durchführen, ehe eine Sitzung über das öffentliche Support-Portal gestartet wird.

Kundenhinweise anzeigen

Optional können Sie Kundenhinweise auf der öffentlichen Website anzeigen. Wenn diese Option aktiviert ist, werden die Hinweise auf dem öffentlichen Portal angezeigt; sie warnen die Kunden vor möglichen Problemen, auf die sie stoßen können und für die möglicherweise derzeit kein Support erforderlich ist. Somit werden die Kunden gar nicht erst in die Support-Warteschlange eingereiht und die Support-Techniker sind in der Lage, ihre Aufmerksamkeit jenen Kunden zuzuwenden, die Hilfe benötigen. Kundenhinweise werden auf der Seite **Öffentliche Portale > Kundenhinweise** konfiguriert.

Hinweis: *Derselbe Kundenhinweis kann auf mehreren Websites oder auf einem benutzerspezifischen Portal verwendet werden. Die XML für das öffentliche Portal enthält einen Abschnitt, in dem alle aktuellen Benachrichtigungen angezeigt werden. Hiermit wird sichergestellt, dass Nachrichten immer auf mehreren Websites synchronisiert sind.*

Weitere Informationen finden Sie in Verbindungsoptionen wählen unter https://www.beyondtrust.com/docs/remote-support/how-to/customize-portals/connection-options.htm.

Es wurde versucht, Sitzungen von installierten Jump-Clients zu starten

Wenn diese Option ausgewählt ist und bereits ein Jump-Client auf dem System des Benutzers installiert ist, wird eine heraufgesetzte Sitzung vom bestehenden Jump-Client gestartet. Dies trifft sowohl auf die Portal- als auch auf die Sitzungserstellungs-API zu.

Hinweis: *Damit die heraufgesetzte Sitzung startet, muss eine ähnliche Berechtigung für den Jump-Client gewährt werden.* *Siehe „Starten von Ad-hoc-Sitzungen auf bestehenden Jump-Clients erlauben“ auf Seite 53*

Support-Technikerliste

Support-Technikerliste verwenden

Die Support-Techniker-Liste enthält die Namen aller angemeldeten Support-Techniker, nach der Anzeigenummer sortiert. Wenn ein Kunde auf einen Namen klickt und den Kunden-Client ausführt, wird sofort eine Sitzung in der persönlichen Warteschlange des jeweiligen Support-Technikers angezeigt.

Wählen Sie dann, ob diese Sitzungseinleitungsoption für dieses Support-Portal zur Verfügung stehen soll. Legen Sie fest, ob diese Option für die öffentliche Website und die API aktiviert sein soll, für die API aktiviert, aber auf der öffentlichen Website ausgeblendet, oder ganz deaktiviert sein soll.

> ***Hinweis:*** *Ein Mitarbeiter, der eine Präsentation hält, wird standardmäßig von der Support-Techniker-Liste entfernt, allerdings kann dieser Ausschluss aus der Support-Technikerliste durch Aktivieren von* ***In Support-Techniker-Liste anzeigen*** *in der Konsole d. Support-Technikers überschrieben werden.*

Hilfetext anzeigen

Wählen Sie, ob für diese Option Hilfetext auf der öffentlichen Website angezeigt werden soll. Sie können den angezeigten Text auch anpassen. Um auf den Standardtext zurückzusetzen, löschen Sie den Text aus dem Feld und speichern Sie dann das leere Feld.

Sitzung mit Click-to-Chat starten

Auswahl aufheben, um Sitzungen mit dem vollständigen Kunden-Client und nicht mit webbasierten Chats zu starten. Es wird empfohlen, Sitzungen mit webbasierten Chats zu beginnen.

Präsentationsliste

Präsentationsliste verwenden

Die Präsentationsliste zeigt aktive Präsentationen an. Damit hier eine Präsentation aufgeführt wird, muss der Support-Techniker die Präsentation gestartet und ausgewählt haben, dass die Präsentation auf der öffentlichen Website angezeigt wird. Wenn ein Kunde auf den Namen einer Präsentation klickt und den Client ausführt, nimmt er sofort an der jeweiligen Präsentation teil.

Hilfetext anzeigen

Wählen Sie, ob für diese Option Hilfetext auf der öffentlichen Website angezeigt werden soll. Sie können den angezeigten Text auch anpassen. Um auf den Standardtext zurückzusetzen, löschen Sie den Text aus dem Feld und speichern Sie dann das leere Feld.

Sitzungsschlüssel

Sitzungsschlüssel verwenden

Sie können einen Sitzungsschlüssel für eine Support-Sitzung Tech. oder Präsentation erstellen und Ihrem Kunden im Voraus geben, damit er ihn auf Ihrer öffentlichen Website einreicht. Wenn der Kunden-Client über einen Sitzungsschlüssel ausgeführt wird, wird der Kunde in die Warteschlange des Support-Technikers eingereiht, der den Schlüssel generiert hat.

Wählen Sie dann, ob diese Sitzungseinleitungsoption für dieses Support-Portal zur Verfügung stehen soll. Legen Sie fest, ob diese Option für die öffentliche Website und die API aktiviert sein soll, für die API aktiviert, aber auf der öffentlichen Website ausgeblendet, oder ganz deaktiviert sein soll.

Hilfetext anzeigen

Wählen Sie, ob für diese Option Hilfetext auf der öffentlichen Website angezeigt werden soll. Sie können den angezeigten Text auch anpassen. Um auf den Standardtext zurückzusetzen, löschen Sie den Text aus dem Feld und speichern Sie dann das leere Feld.

Sitzung mit Click-to-Chat starten

Auswahl aufheben, um Sitzungen mit dem vollständigen Kunden-Client und nicht mit webbasierten Chats zu starten. Es wird empfohlen, Sitzungen mit webbasierten Chats zu beginnen.

Aufforderung vor Download des Remote Support-Kunden-Client

Wenn die Option zur Aufforderung des Kunden aktiviert wird, muss der Remote-Benutzer bestätigen, dass er eine Support-Sitzung Tech. starten bzw. an einer Präsentation teilnehmen möchte, bevor der BeyondTrust-Client heruntergeladen wird. Ist diese Option deaktiviert, beginnt der Client-Download sobald der Kunde den Sitzungsschlüssel abschickt bzw. dem Link zum Sitzungsschlüssel folgt.

Umfrage zum Einreichen von Problemen

Umfrage zum Einreichen von Problemen verwenden

Ihr Kunde kann ein Umfrageformular zum Einreichen von Problemen ausfüllen, um Support anzufordern.

Wählen Sie dann, ob diese Sitzungseinleitungsoption für dieses Support-Portal zur Verfügung stehen soll. Legen Sie fest, ob diese Option für die öffentliche Website und die API aktiviert sein soll, für die API aktiviert, aber auf der öffentlichen Website ausgeblendet, oder ganz deaktiviert sein soll.

Auswahl von Sitzungswarteschlangen

Wenn Sie die Umfrage so einrichten, dass häufige Probleme angezeigt werden, kann Ihr Kunde aus den jeweiligen Problemtypen auswählen. Er kommt dann in die Warteschlange für das Team, das Eigentümer des ausgewählten Problems ist.

Wenn Sie die Umfrage so einrichten, dass die verfügbaren Support-Techniker aufgeführt werden, wird Ihr Kunde in die persönliche Warteschlange des ausgewählten Support-Technikers eingereiht. Bitte beachten Sie, dass unabhängig von der Teammitgliedschaft alle Support-Techniker angezeigt werden.

Probleme für alle Teams anzeigen

Wählen Sie Probleme für alle Teams anzeigen, um alle konfigurierten Probleme aufzuführen, oder wählen Sie die Teams, deren Probleme Sie auf dieser Website anzeigen möchten.

Verfügbare/Angezeigte Felder

Wählen Sie aus den verfügbaren Feldern, welche Informationsfelder auf dieser Seite angezeigt werden sollen. Gehen Sie zu **Konfiguration > Benutzerdefinierte Felder**, um diese Felder zu erstellen und zu verwalten.

Hilfetext anzeigen

Wählen Sie, ob für diese Option Hilfetext auf der öffentlichen Website angezeigt werden soll. Sie können den angezeigten Text auch anpassen. Um auf den Standardtext zurückzusetzen, löschen Sie den Text aus dem Feld und speichern Sie dann das leere Feld.

Sitzung mit Click-to-Chat starten

Auswahl aufheben, um Sitzungen mit dem vollständigen Kunden-Client und nicht mit webbasierten Chats zu starten. Es wird empfohlen, Sitzungen mit webbasierten Chats zu beginnen.

> *Weitere Informationen finden Sie im API-Programmierhandbuch unter www.beyondtrust.com/docs/remote-support/how-to/integrations/api.*

Keine Zielseite für Sitzungsende

Zielseite für Sitzungsende aktivieren

Wählen Sie für jede Website, ob eine Kundenaustrittsumfrage auf der BeyondTrust-Zielseite angezeigt, Ihr Kunde an eine externe URL weitergeleitet oder Ihr Kunde gar nicht weitergeleitet werden soll.

> *Weitere Informationen finden Sie in Anpassen der Deinstallationsmitteilung und der Austrittsumfragen unter https://www.beyondtrust.com/docs/remote-support/how-to/customize-portals/post-session-behavior.htm.*

Verfügbare/Angezeigte Fragen

Wenn Sie die BeyondTrust-Zielseite aktivieren, wählen Sie aus, welche Fragen in der Umfrage dieser Website angezeigt werden sollen. Fragen werden auf der Seite **Öffentliche Portale > Austrittsumfragen** konfiguriert.

Kunden berechtigen, Chat-Mitschriften und/oder Sitzungsaufzeichnungen herunterzuladen

Wenn Sie die BeyondTrust-Zielseite aktivieren, können Sie dem Kunden außerdem einen Link zum Herunterladen der Chat-Mitschrift und/oder der Videoaufzeichnung der Sitzung bereitstellen.

Externe Ziel-URL

Wenn Sie eine benutzerdefinierte Zielseite aktivieren, legen Sie die URL der externen Zielseite fest, auf die Kunden nach einer Support-Sitzung Tech. geleitet werden sollen.

Support-Techniker-Umfrage

Support-Techniker-Umfrage aktivieren

Sie können eine Support-Techniker-Umfrage anzeigen lassen. Die Umfrage wird nach dem Abschluss einer Sitzung angezeigt. Außerdem ist es möglich, dem Support-Techniker während einer Sitzung Zugriff auf die Umfrage zu gewähren. Mit dieser Option können Administratoren die Umfrage verwenden, um detaillierte Arbeitsabläufe mit externen Weblinks und Ressourcen zu erstellen und sicherzustellen, dass Support-Techniker bestimmte Informationen aufzeichnen oder einer festgelegten Anzahl an Support-Schritten folgen. Die Option zur Anzeige der Umfrage während einer Sitzung wird auf der Seite **Öffentliche Portale > Austrittsumfragen** konfiguriert.

Weitere Informationen finden Sie in Support-Techniker-Umfrage unter https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/representative-exit-survey.htm.

Verfügbare/Angezeigte Fragen

Wenn Sie eine Support-Techniker-Umfrage aktivieren, wählen Sie aus, welche Fragen angezeigt werden sollen. Fragen werden auf der Seite **Öffentliche Portale > Austrittsumfragen** konfiguriert.

Planen: Öffnungszeiten für öffentliches Portal festlegen

Öffentliche Portale | PLANEN

Reguläre Portalpläne

Konfigurieren Sie einen oder mehrere Öffnungszeitenpläne für Ihre öffentlichen Portale. Außerhalb dieser geplanten Zeiten werden andere Sitzungsstartmethoden als Sitzungsschlüssel von Ihrer öffentlichen Website entfernt und eine Nachricht „Portal geschlossen“ auf Ihrer öffentlichen Website angezeigt.

Neuen Plan hinzufügen, bearbeiten, löschen

Erstellen Sie einen neuen Plan, bearbeiten Sie einen bestehenden Plan oder löschen Sie einen bestehenden Plan.

Plan hinzufügen/bearbeiten

Planname

Erstellen Sie einen eindeutigen Namen, um diesen Plan leichter zu identifizieren.

Mitteilung „Portal geschlossen“

Erstellen Sie den Text, der außerhalb der regulären Öffnungszeiten angezeigt werden soll. Nachrichten können Makros enthalten, die die nächsten Öffnungszeiten anzeigen. Sie können Macros und BBCode verwenden, um geringfügige Formatierungsaufgaben wie Hinzufügen von Fettschrift, Farben oder Hyperlinks durchzuführen. Klicken Sie auf **Macros** oder **BBCode**, um eine Liste der Codes und der sich daraus ergebenden Effekte anzuzeigen.

Planen

Legen Sie einen Zeitplan fest, der definiert, wann Kunden Support-Sitzungen initiieren können. Legen Sie die Zeitzone fest, die für diesen Zeitplan verwendet werden soll, und fügen Sie dann einen oder mehrere Zeitplaneinträge hinzu. Geben Sie für jeden Eintrag das Startdatum und die Startuhrzeit an sowie das Enddatum und die Enduhrzeit.

Wenn die Zeit beispielsweise für 8 Uhr (Start) und 17 Uhr (Ende) festgelegt wird, kann ein Support-Techniker jederzeit innerhalb dieses Zeitfensters eine Sitzung starten. Bereits laufende Sitzungen können über den Endzeitpunkt des Plans hinaus laufen. Wenn Sitzungsschlüssel aktiviert sind, kann ein Support-Techniker einem Kunden einen Sitzungsschlüssel senden, um eine Sitzung zu starten, auch außerhalb des Zeitplans der öffentlichen Website.

Auf folgende öffentliche Websites anwenden

Wenn Sie mehr als eine öffentliche Website haben, wählen Sie aus, welche diesen Zeitplan befolgen soll.

Nutzt diese Feiertage

Wählen Sie erstellte Feiertage, die für diesen Zeitplan gelten sollen. Hier erfolgte Verknüfungen gelten auch für die Feiertags-Zeitplaneinstellungen.

Portal-Feiertagskalender

Wenn ein Feiertagszeitplan auf einen regulären Zeitplan angewandt wird, setzen Sie Stunden des Feiertagszeitplan die regulären Geschäftszeiten außer Kraft. Feiertagszeitpläne können festgelegt werden, um Urlaubstage, Tage mit verkürzten Öffnungszeiten oder mit verlängerten Öffnungszeiten einzustellen.

Neuen Feiertag hinzufügen, bearbeiten, löschen

Erstellen Sie einen neuen Feiertag, bearbeiten Sie einen bestehenden Feiertag oder entfernen Sie einen bestehenden Feiertag.

Feiertag hinzufügen/bearbeiten

Feiertagsname

Erstellen Sie einen eindeutigen Namen, um diesen Feiertagszeitplan leichter zu identifizieren.

Datum

Legen Sie das Datum fest, für das dieser Feiertagszeitplan gelten soll.

Mitteilung „Portal geschlossen“

Erstellen Sie den Text, der an diesem Datum außerhalb der planmäßigen Öffnungszeiten angezeigt werden soll. Sie können Macros und BBCode verwenden, um geringfügige Formatierungsaufgaben wie Hinzufügen von Fettschrift, Farben oder Hyperlinks durchzuführen. Klicken Sie auf **Macros** oder **BBCode**, um eine Liste der Codes und der sich daraus ergebenden Effekte anzuzeigen.

Planen

Wählen Sie entweder **Ganztägig geschlossen** oder legen Sie Start- und Endzeitpunkt fest.

Für folgende Portalpläne übernehmen

Wählen Sie jegliche erstellten regulären Zeitpläne, für die dieser Feiertagszeitplan gelten soll. Hier vorgenommene Verknüpfungen gelten auch für die regulären Portal-Zeitplaneinstellungen.

> *Weitere Informationen finden Sie in Mitteilungen und Öffnungszeiten im öffentlichen Portal unter https://www.beyondtrust.com/docs/remote-support/how-to/customize-portals/portal-messages.htm.*

HTML-Vorlagen: Webschnittstelle anpassen

Webvorlage für öffentliche Website

Passen Sie das HTML Ihrer öffentlichen Website so an, dass sie dem Rest Ihrer Website entspricht.

Vorlage hinzufügen oder bearbeiten

Wählen Sie eine bestehende Vorlage aus, die bearbeitet werden soll, oder wählen Sie **Hinzufügen**, um eine neue Vorlage zu erstellen.

Name

Wenn zusätzliche Vorlagen erstellt werden, geben Sie jeder einen eindeutigen Namen, um sie für die weitere Bearbeitung zu identifizieren oder auf eine öffentliche Website anzuwenden.

HTML-Vorlage

Makros ersetzen Echtzeitdaten wie die Sitzungseinleitungsoptionen und das Sprachauswahl-Dropdown-Menü. Dadurch können Sie diese Elemente an beliebigen Stellen auf der Seite positionieren.

BeyondTrust empfiehlt, die öffentliche Website unverändert zu lassen, außer Sie kennen sich mit dem HTML-Format aus.

Auf Standard-HTML zurücksetzen

Nachdem Sie die Website angepasst haben, können Sie die öffentliche Website in ihren ursprünglichen Zustand zurücksetzen, indem Sie unten im Programmierfenster auf **Auf Standard-HTML zurücksetzen** klicken.

Hilfesymbol

Hilfesymbol ändern

Sie können ein neues Bild hochladen, das auf dem öffentlichen Portal als Hilfesymbol fungieren soll.

Auf standardmäßiges Hilfesymbol zurücksetzen

Um das Original-Hilfesymbol von BeyondTrust für eine Vorlage wiederherzustellen, klicken Sie auf die Schaltfläche **Hilfesymbol für Auf Werkseinstellungen zurücksetzen**.

Weitere Informationen finden Sie in Anpassen der Vorlage für die öffentliche Website unter https://www.beyondtrust.com/docs/remote-support/how-to/customize-portals/html-templates.htm.

Kundenhinweise: Erstellen Sie Nachrichten für das Kundenbenachrichtigungssystem

Kundenhinweise

Benachrichtigen Sie die Kunden, wenn sie Support anfordern, über breitenwirksame IT-Ausfälle, um zu vermeiden, dass Ihr BeyondTrust-Support-Techniker mit Anfragen überhäuft wird. Diese Nachrichten können so festgelegt werden, dass sie zu einer vorab bestimmten Zeit ablaufen und auf ein oder mehrere öffentliche Portale angewendet werden.

Nachdem Kundenhinweise erstellt wurden, werden sie im öffentlichen Portal und in den Support-Button-Startfenstern angezeigt, damit die Kunden die erforderlichen Informationen erhalten, bevor sie auch nur versuchen, eine Sitzung einzuleiten. Mitteilungen werden zu Beginn einer Sitzung und/oder nach dem Verschicken von der /login-Schnittstelle aus auch im Kunden-Client-Chat-Fenster angezeigt.

Administratoren und autorisierte Support-Techniker können bis zu 10 pro Portal erstellen, und jede Nachricht kann bis zu 1020 Zeichen enthalten.

Zwar sind Nachrichten nicht pro Sprache konfigurierbar, doch Sie können dennoch unterschiedliche Nachrichten für die auf einem Portal unterstützten Sprachen erstellen.

Administratoren können Kundenhinweise erstellen und bearbeiten und dieses Recht Support-Technikern ohne administrative Berechtigungen gewähren.

Neuen Kundenhinweis hinzufügen, bearbeiten, löschen

Erstellen Sie einen neuen Hinweis, bearbeiten Sie einen bestehenden Hinweis oder entfernen Sie einen bestehenden Hinweis.

Senden

Pushen Sie einen Kundenhinweis an alle gehaltenen Sitzungen.

Kundenhinweis hinzufügen oder bearbeiten

Name

Erstellen Sie einen eindeutigen Namen, um diesen Hinweis leichter zu identifizieren. Dieser Name wird dem Kunden nicht angezeigt.

Hinweistext

Geben Sie den Text ein, der im Kunden-Client, im öffentlichen Portal und auf den Support-Button angezeigt wird. Sie können Macros und BBCode verwenden, um geringfügige Formatierungsaufgaben wie Hinzufügen von Fettschrift, Farben oder Hyperlinks durchzuführen. Klicken Sie auf **Macros** oder **BBCode**, um eine Liste der Codes und der sich daraus ergebenden Effekte anzuzeigen.

Hinweis: *Die Nachrichten sollten relativ kurz sein, damit sie ohne viel Bildlauf in den Fenstern des Kunden-Clients angezeigt werden können. Dies gilt für den nativen Client und die Click-to-Chat-Modi.*

Ablaufdatum

Geben Sie ein Ablaufdatum für den Hinweis an. Wenn Sie **Ohne Ablaufdatum** auswählen, bleibt der Hinweis solange auf Ihrer Website, bis er manuell gelöscht wird. Abgelaufene Hinweise werden 24 Stunden nach ihrem Ablaufdatum automatisch gelöscht.

Öffentliche Websites

Wenn Sie mehr als eine öffentliche Website haben, wählen Sie aus, welche den Hinweis anzeigen soll. Sie können mehrere Portale auswählen.

Weitere Informationen finden Sie in Mitteilungen und Öffnungszeiten im öffentlichen Portal unter https://www.beyondtrust.com/docs/remote-support/how-to/customize-portals/portal-messages.htm.

Dateispeicher: Ressourcendateien hochladen

Öffentliche Portale | DATEISPEICHER

Info

Speichern Sie Dateien, auf die Sie von Ihrer HTML-Vorlage aus verweisen müssen, wie z. B. Bilddateien und Stylesheets, im Online-Dateispeicher. Sie können den Dateispeicher auch als zentralen Zugriffspunkt für Dateien verwenden, die bei Support-Sitzungen Tech. häufig benötigt werden.

Zugriff

Dateilisten für Dateispeicher unter „/files“ anzeigen

Ist diese Option aktiviert, ist Zugriff auf jegliche hier hochgeladenen Dateien möglich, indem Sie zum Hostnamen Ihrer Support-Website, gefolgt von „/files“, navigieren (z. B. support.beispiel.com/files).

Dateispeicher anzeigen

Wenn die obige Option aktiviert ist, klicken Sie auf diese Schaltfläche, um Ihren Online-Dateispeicher anzuzeigen.

Dateispeicherstatistiken

Sie können sich die Anzahl der hochgeladenen Dateien, die maximal verfügbare Kapazität und die maximale Dateigröße ansehen.

Inhalte

Hochladen

Navigieren Sie zu Dateien und laden Sie diese auf Ihren Dateispeicher hoch.

Dateien in Dateispeicher

Sehen Sie sich eine Liste der auf Ihren Dateispeicher hochgeladenen Dateien an.

Ausgewählte Dateien löschen

Wählen Sie eine oder mehrere Dateien aus der obigen Liste aus und klicken Sie auf diese Schaltfläche, um diese Dateien aus Ihrem Dateispeicher zu entfernen.

Weitere Informationen finden Sie in Anpassen des BeyondTrust-Support-Portals auf https://www.beyondtrust.com/docs/remote-support/how-to/customize-portals/file-store.htm.

iOS-Konfigurationsprofile: Apple-Konfigurationsprofile hinzufügen

Öffentliche Portale | IOS-KONFIGURATION

iOS-Konfigurationsprofile

BeyondTrust unterstützt die Verteilung von Apple iOS-Konfigurationsprofilen, damit Support-Techniker iOS-Benutzern den Download von öffentlichen und privaten, vom Administrator konfigurierten Profilen auf ihr iPhone®, iPad™ und iPod touch® bieten können.

Weitere Informationen finden Sie in iOS-Konfigurationsprofile unter https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/apple-ios/iosconfigurationprofiles.htm.

WICHTIG!

*Um sicherzustellen, dass Konfigurationsprofile über eine verschlüsselte HTTPS-Verbindung auf die iOS-Geräte heruntergeladen werden, müssen Sie das Kontrollkästchen **Erzwingen, dass die öffentliche Website HTTPS verwendet** auf der Seite **Verwaltung > Sicherheit** der Verwaltungsschnittstelle /login markieren. Ansonsten werden Profile über nichtverschlüsselte HTTP-Verbindungen heruntergeladen.*

Um Apple iOS-Einstellungen zu verwalten, müssen Sie ein Administratorkonto verwenden. Um Apple iOS-Konfigurationsprofile zu erstellen oder zu modifizieren, benötigen Sie die Benutzerkontoberechtigung **Berechtigt, iOS-Profile zu bearbeiten**. Damit ein Support-Techniker Kunden Zugriff auf private Konfigurationsprofile gewähren kann, benötigt er die Berechtigung **Berechtigt, Zugriffsschlüssel zum Senden von iOS-Profilen zu erstellen**. Wählen Sie in der /login-Verwaltungsschnittstelle **Benutzer und Sicherheit > Benutzer** und/oder **Gruppenrichtlinien**, um Kontoberechtigungen zu ändern.

Verwenden Sie, nachdem Sie ein Konfigurationsprofil aus der kostenfreien Konfigurationsanwendung von Apple für iPhone eingerichtet und exportiert haben, die Verwaltungsschnittstelle /login in BeyondTrust, um das Profil zugänglich zu machen. Die Konfigurationsanwendung für iPhone finden Sie auf der Support-Website für das Apple iPhone.

Neues Profil hinzufügen, bearbeiten, löschen

Erstellen Sie ein neues Profil, bearbeiten Sie ein bestehendes Profil oder entfernen Sie ein bestehendes Profil.

iOS-Konfigurationsprofil hinzufügen oder bearbeiten

Name

Erstellen Sie einen eindeutigen Namen, um dieses Profil leichter zu identifizieren. Der Name dieses iOS-Konfigurationsprofils sollte dem Benutzer bei der Auswahl des richtigen Profils helfen, wenn er Ihr Support-Portal navigiert.

Datei

Laden Sie das Apple iOS-Profil hoch, das Sie mit der iPhone Konfigurationsanwendung erstellt haben. Beachten Sie, dass das zugrunde liegende Apple iOS-Profil angepasst werden muss, um den Inhalt der iOS-Geräteprofile, die Sie an Benutzer mit iOS-Geräten verteilen möchten, zu ändern.

Beschreibung

Fügen Sie eine kurze Beschreibung hinzu, um den Zweck dieser Richtlinie zusammenzufassen.

Öffentlich

Versehen Sie das Kästchen **Öffentlich** mit einem Häkchen, damit das Profil für jeden iOS-Benutzer beim Browsen in Ihrem Supportportal sichtbar ist. Beachten Sie, dass iOS-Benutzer beim Aufrufen des öffentlichen Portals weder eine Support-Techniker-Liste noch ein Kontaktformular für den Problemfall sehen.

Wenn Sie das Kontrollkästchen **Öffentlich** nicht aktivieren, können Sie den Zugriff auf das von Ihnen erstellte iOS-Profil beschränken. Zum Herunterladen der privaten Profilinhalte müssen Benutzer den von Ihnen in der Konsole d. Support-Technikers bereitgestellten Zugangscode eingeben.

Einstellungen

Wählen Sie eine öffentliche Website zum Bearbeiten aus

Wählen Sie im Dropdown-Menü oben auf der Seite die öffentliche Website aus, für die Sie die Einstellungen konfigurieren möchten.

Link zu iOS-Konfigurationsprofilen aktiviert

Wenn diese Option aktiviert ist, sehen Kunden auf iOS-Geräten einen Link zum Portal des iOS-Konfigurationsprofils, wenn sie auf die öffentliche Website zugreifen. Auf dieser Seite werden alle verfügbaren öffentlichen Profile angezeigt. Ferner steht ein Texteingabefeld zur Verfügung, in das Kunden einen Zugriffsschlüssel eingeben können, den sie von ihrem Support-Techniker erhalten haben, wodurch die Kunden zu einem persönlichen Konfigurationsprofil gelangen.

Portal

Titel

Passen Sie den Titel der iOS-Portalseite an. Sie können diesen Text für jegliche aktivierten Sprachen lokalisieren.

Nachricht

Passen Sie den Text an, der auf der iOS-Portalseite angezeigt wird. Sie können diesen Text für jegliche aktivierten Sprachen lokalisieren.

E-Mail-Einladung

Wenn ein Support-Techniker einen Apple iOS-Profilzugriffsschlüssel über die Konsole d. Support-Technikers generiert, kann der Zugriffsschlüssel in einer E-Mail an den iOS-Benutzer gesandt werden.

Betreff

Passen Sie den Betreff dieser E-Mail an. Sie können diesen Text für jegliche aktivierten Sprachen lokalisieren.

Nachricht

Passen Sie den Text dieser E-Mail an. Verwenden Sie eines der unten auf der /login-Seite aufgeführten Makros, um den Text für Ihre Zwecke anzupassen.Sie können diesen Text für jegliche aktivierten Sprachen lokalisieren.

Weitere Informationen finden Sie in Verwalten der Seite für Apple iOS-Konfigurationsprofile unter https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/apple-ios/manageprofilespage.htm.

Umfragen: Kundenaustrittsumfrage und Support-Techniker-Umfrage aktivieren

Kundenaustrittsumfrage oder Support-Techniker-Umfrage

Konfigurieren Sie Fragen, die in Kunden- und Support-Techniker-Umfragen implementiert werden und die bei der Überwachung der Zufriedenheits- und Problemlösungsraten nützlich sind. Die Fragen werden den Umfragen einer Support-Website auf der Seite **Öffentliche Portale > Öffentliche Websites** zugewiesen.

Support-Technikern gestatten, während der Support-Sitzung Tech. die Umfrage zu bearbeiten

Dem Support-Techniker gestatten, während einer Sitzung Zugriff auf die Umfrage zu erhalten. Administratoren können die Umfrage verwenden, um detaillierte Arbeitsabläufe mit externen Weblinks und Ressourcen zu erstellen und sicherzustellen, dass Support-Techniker bestimmte Informationen aufzeichnen oder einer festgelegten Anzahl an Support-Schritten folgen.

Neue Frage hinzufügen, bearbeiten, löschen

Erstellen Sie eine neue Frage, bearbeiten Sie eine bestehende Frage oder entfernen Sie eine bestehende Frage.

Vorschau für Umfrage anzeigen

Vorschau aller Umfrage-Fragen auf der Kundenseite. Mit dem Vorschau der Support-Techniker-Umfrage wird das Grundformat gezeigt, auch wenn die Stile in der Konsole d. Support-Technikers anders angezeigt werden.

Kundenaustrittsumfrage oder Support-Techniker-Umfrage: Neue Frage hinzufügen

Fragentyp

Wählen Sie aus mehreren Fragetypen, z. B. Optionsschaltfläche, Kontrollkästchen, Dropdown-Menüs, Textfelder und Textbereiche.

Fragentext

Geben Sie den Fragetext ein, der in der Umfrage erscheinen soll.

Fragenname

Weisen Sie der Frage zu internen Formatierungszwecken einen Namen zu.

Berichtskopfzeile

Weisen Sie der Frage eine Kopfzeile zu, um sie in Ihren Umfrageberichten zu identifizieren.

Antwort erforderlich

Für Support-Techniker-Umfragen legen Sie fest, ob der Support-Techniker die Frage beantworten muss, bevor die Sitzung geschlossen werden kann.

CSS-Stil

Sie können einen CSS-Stil für eine Frage der Kundenaustrittsumfrage definieren. Diese Optionen stehen für die Webentwicklung zur Verfügung. Benutzer, die mit HTML und CSS nicht vertraut sind, lassen diese Felder leer.

CSS-Klassen

Sie können CSS-Klassen für eine Frage der Kundenaustrittsumfrage definieren. Diese Optionen stehen für die Webentwicklung zur Verfügung. Benutzer, die mit HTML und CSS nicht vertraut sind, lassen diese Felder leer.

HTML-ID

Sie können eine HTML-ID für eine Frage der Kundenaustrittsumfrage definieren. Diese Optionen stehen für die Webentwicklung zur Verfügung. Benutzer, die mit HTML und CSS nicht vertraut sind, lassen diese Felder leer.

Mehrfachauswahl zulassen

Für ein Dropdown-Menü können Sie mehrere Auswahloptionen zulassen.

Größe des Textfelds

Für ein Textfeld können Sie die Größe des Texteingabefelds festlegen.

Max. Anzahl von Zeichen in Antwort

Für ein Textfeld können Sie die maximale Anzahl an Zeichen festlegen, die eingegeben werden können.

Größe des Textbereichs

Für einen Texteingabebereich können Sie die Größe des Texteingabefelds festlegen.

Anzeigereihenfolge

Wählen Sie die Reihenfolge, in der die Fragen in der Umfrage erscheinen sollen. Kleinere Zahlen werden zuerst angezeigt.

Standardwert

Für Textfelder oder Texteingabebereiche können Sie einen Standardtext in das Feld einfügen.

Auf der öffentlichen Standard-Website anzeigen

Wenn Sie diese Option wählen, wird diese Frage automatisch für Ihre Standard-Support-Site zur Umfrage hinzugefügt. Weil jede Umfrage nur zehn Fragen enthalten kann, wird ein Fehler angezeigt, wenn Sie versuchen, eine Frage zu speichern, die diesen Grenzwert für die Standard-Website-Umfrage überschreiten würde. Um eine Frage für eine andere Umfrage zu erstellen, deaktivieren Sie das Kontrollkästchen und speichern dann.

Anzeigewert

Für jede Option in einer Optionsschaltflächen-Gruppe, einer Kontrollkästchen-Gruppe oder in einem Dropdown-Menü können Sie einen Anzeigewert zuordnen, der dem Kunden angezeigt wird.

Protokollierter Wert

Für jede Option in einer Optionsschaltflächen-Gruppe, einer Kontrollkästchen-Gruppe oder in einem Dropdown-Menü können Sie einen protokollierten Wert zuordnen, der in den Austrittsumfrageberichten gespeichert wird.

Standardmäßig ausgewählt

Für eine Optionsschaltflächen-Gruppe, eine Kontrollkästchen-Gruppe oder ein Dropdown-Menü können Sie eine standardmäßig ausgewählte Option festlegen.

Anzeigereihenfolge

Für eine Optionsschaltflächen-Gruppe, eine Kontrollkästchen-Gruppe oder ein Dropdown-Menü können Sie die Reihenfolge festlegen, in der die Optionen unterhalb der Frage angezeigt werden.

Aufsteigend sortieren

Für eine Optionsschaltflächen-Gruppe, eine Kontrollkästchen-Gruppe oder ein Dropdown-Menü können Sie die Optionen in aufsteigender Reihenfolge sortieren.

Absteigend sortieren

Für eine Optionsschaltflächen-Gruppe, eine Kontrollkästchen-Gruppe oder ein Dropdown-Menü können Sie die Optionen in absteigender Reihenfolge sortieren.

Option hinzufügen

Fügen Sie mehrere Optionen zu einer Optionsschaltflächen-Gruppe, einer Kontrollkästchen-Gruppe oder einem Dropdown-Menü hinzu.

Vorschau für Frage anzeigen

Zeigen Sie eine Vorschau an, wie diese Frage für Ihre Kunden angezeigt wird. Mit der Vorschau einer Frage einer Support-Techniker-Umfrage wird das Grundformat angezeigt, auch wenn die Stile in der Konsole d. Support-Technikers unterschiedlich angezeigt werden.

Weitere Informationen finden Sie in Anpassen der Deinstallationsmitteilung und Austrittsumfragen unter https://www.beyondtrust.com/docs/remote-support/how-to/customize-portals/post-session-behavior.htm.

Weitere Informationen finden Sie in Kundenaustrittsumfrage: Feedback abschicken unter https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/customer-exit-survey.htm.

Weitere Informationen finden Sie in Support-Techniker-Umfrage unter https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/representative-exit-survey.htm.

Kunden-Client: Ändern der Optionen für Einladungs-E-Mails, Anzeigeoptionen und Verbindungsoptionen

Öffentliche Portale | KUNDEN-CLIENT

Wählen Sie eine öffentliche Website zum Bearbeiten aus

Wählen Sie im Dropdown-Menü oben auf der Seite die öffentliche Website aus, für die Sie die Einstellungen konfigurieren möchten.

Hinweis: *Standardeinladungs-E-Mails, Kundenvereinbarungen und Nachrichten werden in allen unterstützten Sprachen bereitgestellt. Die Benutzer können diesen Text aktualisieren. Sobald jedoch ein neuer Text in der Datenbank gespeichert ist, wird der Standardtext überschrieben und kann nicht mehr abgerufen werden.*

E-Mail-Einladung

Erstellen Sie eine benutzerdefinierte E-Mail-Nachricht mit eindeutigen Support-Sitzungs-Anweisungen für jede öffentliche Website.

Absender

Optional können Sie das Feld **Von-Adresse** verwenden, um systemgenerierte E-Mail-Einladungen anstelle einer Einladung einzurichten, welche den lokalen E-Mail-Client des Support-Technikers verwendet. Bei einer derartigen Konfiguration werden Sitzungseinladungen über eine zentralisierte, systemweite Adresse versandt (z. B. admin@support.beispiel.com). Dies ist insbesondere dann nützlich, wenn Ihre Support-Techniker aus Sicherheits- oder Datenschutzgründen E-Mail-Beschränkungen auf Unternehmensebene unterliegen. Wird das Feld **Absender** leer gelassen, verwenden die E-Mails die *Absender*, die auf der Seite **E-Mail-Konfiguration** konfiguriert wurde.

Hinweis: *Um systemweite E-Mails zu aktivieren, stellen Sie sicher, dass* ***Serverseitige E-Mails für Support-Einladungen aktivieren*** *auf der Seite* ***/login > Konfiguration > Optionen*** *aktiviert ist.*

Weitere Informationen finden Sie in „E-Mail-Konfiguration: Konfigurieren der Software für das Versenden von E-Mails“ auf Seite 247.

Betreff

Passen Sie den Betreff dieser E-Mail an. Sie können diesen Text für jegliche aktivierten Sprachen lokalisieren.

Text

Passen Sie den Text dieser E-Mail an. Verwenden Sie eines der unten auf der /login-Seite aufgeführten Makros, um den Text für Ihre Zwecke anzupassen.Sie können diesen Text für jegliche aktivierten Sprachen lokalisieren.

Kundenvereinbarungen

Weitere Informationen erhalten Sie unter Kunden-Client: Schnittstelle für Support-Sitzungen Tech. unter https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/customer-support-interface.htm.

Vollständige Client-Sitzungen

Kundenvereinbarung vor Beginn der vollständigen Client-Sitzungen anzeigen

Passen Sie den Text dieser Vereinbarung an.Sie können diesen Text für jegliche aktivierten Sprachen lokalisieren.

Titel

Passen Sie den Titel dieser Vereinbarung an.Der Endbenutzer sieht dies in der Titelleiste der Aufforderung.Sie können diesen Text für jegliche aktivierten Sprachen lokalisieren.

Zeitüberschreitung bei der Annahme

Wenn der Kunde die Vereinbarung nicht innerhalb der festgelegten **Akzeptanz-Zeitüberschreitung** annimmt, wird die Sitzung beendet. Dies gilt nur für unüberwachte Sitzungen.

Text

Geben Sie den Text für die Kundenvereinbarung des vollständigen Clients an. Sie können diesen Text für jegliche aktivierten Sprachen lokalisieren.

Click-To-Chat-Sitzungen

Kundenvereinbarung vor Beginn einer Click-to-Chat-Sitzung anzeigen

Sie können eine Vereinbarung aktivieren, die der Kunde akzeptieren muss, bevor er auf eine Click-to-Chat-Sitzung zugreifen kann.

Nicht besuchte Sitzungen

Kundenvereinbarung vor unüberwachten Sitzungen anzeigen

Aktivieren Sie eine Vereinbarung, die vor dem Beginn einer unüberwachten Sitzung bestätigt werden muss.

Titel

Passen Sie den Titel dieser Vereinbarung an.Der Endbenutzer sieht dies in der Titelleiste der Aufforderung.Sie können diesen Text für jegliche aktivierten Sprachen lokalisieren.

Zeitüberschreitung bei der Annahme

Wenn der Kunde die Vereinbarung nicht innerhalb der festgelegten **Akzeptanz-Zeitüberschreitung** annimmt, wird die Sitzung beendet. Dies gilt sowohl für Sitzungen im vollständigen Client wie auch für Click-to-Chat-Sitzungen.

Automatisches Verhalten

Wählen Sie, ob unüberwachte Endpunkte automatisch über Jump-Clients, Remote-Jumps und Jump-Elemente gestartete Sitzungen annehmen oder ablehnen sollen.

Text

Geben Sie den Text für die Kundenvereinbarung des vollständigen Clients an. Sie können diesen Text für jegliche aktivierten Sprachen lokalisieren.

Anzeigeoptionen

Eingabeaufforderungen anzeigen

Um festzulegen, wie Ihre Aufforderungen Ihren Kunden während einer Support-Sitzung Tech. angezeigt werden, wählen Sie, dass Aufforderungen als Text-Links im Chat-Fenster oder als Pop-Ups über dem Chat-Fenster angezeigt werden sollen. Die Pop-Up-Option gilt nicht für mobile Clients oder Click-to-Chat-Sitzungen.

Kunden-Client für überwachte Sitzungen minimiert starten

Sie können den Kunden-Client unauffällig minimiert starten, ohne dass er in von Kunden initiierten Sitzungen den Fokus erhält.

Hostname der öffentlichen Website im Fenstertitel anzeigen

Wählen Sie eine Option aus, um den Hostnamen Ihrer öffentlichen Website in der Titelleiste des Fensters anzuzeigen.

Sie können beim Fixieren eines Jump-Clients das Standardverhalten so festlegen, dass über diesen Jump-Client gestartete Kunden-Clients minimiert gestartet werden

Sie können den Kunden-Client unauffällig minimiert starten, ohne, dass er in Jump-Client-Sitzungen den Fokus erhält.

Für über lokalen Jump oder Jumpoint gestartete Sitzungen Kunden-Client minimiert starten

Sie können den Kunden-Client unauffällig minimiert starten, ohne dass er in lokalen Jump- oder Jumpoint-Sitzungen den Fokus erhält.

Vor vollständigen Client-Sitzungen Sitzungsaufzeichnungsaufforderung anzeigen

Wird diese Option aktiviert, wird der Kunde zu Beginn einer Sitzung aufgefordert, Sitzungsaufzeichnungen zuzulassen. Wenn der Kunde Aufzeichnungen zulässt, wird die Sitzung gemäß der Konfiguration für dieses öffentliche Portal aufgezeichnet. Wenn der Kunde Aufzeichnungen ablehnt, wird die Sitzung fortgesetzt, aber nicht aufgezeichnet. Dies gilt für Sitzungsfreigabeaufzeichnungen, Befehlsshellaufzeichnungen und Systeminformationsprotokollierungen.

Kundenhinweise im Kunden-Client anzeigen

Wird diese Option aktiviert, zeigt der Kunden-Client bis zur Annahme der Sitzung sowohl bereits zum Zeitpunkt der Sitzungsanforderung aktive Kundenhinweise sowie erstellte und versandte Kundenhinweise an. Nach jedem Hinweis befindet sich ein Link zum Beenden der Sitzung, wenn der Hinweis auf ein bekanntes Problem hinweist, für das der Kunde Support angefordert hat.

Nachrichten

Kundenbegrüßung

Kundenbegrüßung vor Sitzung anzeigen

Die Kundenbegrüßung erscheint im Chat-Fenster, sobald sich die Sitzung in der Warteschlange befindet. Sie können diesen Text für jegliche aktivierten Sprachen lokalisieren.

Informieren Sie die Kunden über ihren Sitzungsstatus, indem Sie ihnen Feedback bezüglich ihrer Position in der Warteschlange und die geschätzte Wartezeit zukommen lassen. Wenn Sie die Kunden diesbezüglich auf dem Laufenden halten, ist es wahrscheinlicher, dass sie in der Warteschlange ausharren und den benötigten Service erhalten.

Wartezeit und -position werden je Warteschlange berechnet. Die Position eines Kunden in der Warteschlange wird anhand des Sitzungsalters auf Basis von „Wer zuerst kommt, mahlt zuerst“ bestimmt. Die Wartezeit wird anhand von aktuellen Sitzungen geschätzt, die in eine Warteschlange eingereiht und von einem Support-Techniker beantwortet wurden. Mindestens fünf Sitzungen sind erforderlich, um genug Daten für eine zuverlässige Berechnung der Wartezeit zu liefern.

Nachrichten werden mithilfe von Makros konfiguriert. Kopieren Sie die Makros **%POSITION_IN_QUEUE%** und **%ESTIMATED_WAIT_TIME%** in das Textfeld.

> ***Hinweis:*** *Die Makros werden zu vollständigen Sätzen erweitert, die die Position des Kunden in der Warteschlange und die geschätzte verbleibende Wartezeit für den Kunden angeben.*

Haltemeldung anzeigen

Warteschleifennachricht anzeigen

Die Warteschleifennachricht wird in gewissen Abständen solange angezeigt, bis ein Support-Techniker die Sitzung annimmt. Sie können diesen Text für jegliche aktivierten Sprachen lokalisieren.

Informieren Sie die Kunden über ihren Sitzungsstatus, indem Sie ihnen Feedback bezüglich ihrer Position in der Warteschlange und die geschätzte Wartezeit zukommen lassen. Wenn Sie die Kunden diesbezüglich auf dem Laufenden halten, ist es wahrscheinlicher, dass sie in der Warteschlange ausharren und den benötigten Service erhalten.

Wartezeit und -position werden je Warteschlange berechnet. Die Position eines Kunden in der Warteschlange wird anhand des Sitzungsalters auf Basis von „Wer zuerst kommt, mahlt zuerst“ bestimmt. Die Wartezeit wird anhand von aktuellen Sitzungen geschätzt, die in eine Warteschlange eingereiht und von einem Support-Techniker beantwortet wurden. Mindestens fünf Sitzungen sind erforderlich, um genug Daten für eine zuverlässige Berechnung der Wartezeit zu liefern.

Nachrichten werden mithilfe von Makros konfiguriert. Kopieren Sie die Makros **%POSITION_IN_QUEUE%** und **%ESTIMATED_WAIT_TIME%** in das Textfeld.

> ***Hinweis:*** *Die Makros werden zu vollständigen Sätzen erweitert, die die Position des Kunden in der Warteschlange und die geschätzte verbleibende Wartezeit für den Kunden angeben.*

Warteschleifennachrichtenintervall

Geben Sie die Anzahl der Minuten an, die zwischen dem Senden jeder Warteschleifennachricht gewartet werden soll.

Text

Geben Sie den Text für die Warteschleifennachricht an.

Geschätzte maximale Wartezeit

Geben Sie für Kunden die längste Zeit an, die sie womöglich warten müssen.

Verwaiste Meldung

Zeigen Sie die folgende Nachricht für eine verwaiste Sitzung an,

Wenn ein Kunde eine Sitzung anfordert, wenn kein Support-Techniker verfügbar ist, kann eine verwaiste Sitzungsnachricht angezeigt werden. Sie können diesen Text für jegliche aktivierten Sprachen lokalisieren.

Und öffnen Sie diese URL

Ist eine Sitzung verwaist, kann automatisch der Web-Browser des Kunden geöffnet und auf eine bestimmte URL verwiesen werden, wie eine Wissensdatenbank oder Kontaktseite.

Text

Geben Sie den Text für die verwaiste Meldung an.

Banner für Chat-Fenster

Chat-Banner ändern

Laden Sie ein Bannerbild für das Kunden-Client-Fenster hoch. Dieses Bild muss im Windows-Bitmap-Format (BMP) mit 256 Farben (8 Bit) vorliegen und 480 Pixel breit sein. Die empfohlene Bildhöhe beträgt 40 Pixel. Sobald Sie ein neues Banner hochladen, verwenden alle neuen Sitzungen dieses Bild. Aktuell laufende Sitzungen sind davon nicht betroffen.

Auf Standard zurücksetzen

Stellen Sie das Standardbanner wieder her. Sobald Sie das Standardbanner wiederherstellen, verwenden alle neuen Sitzungen dieses Bild. Aktuell laufende Sitzungen sind davon nicht betroffen.

Wasserzeichen

Bildschirmanzeige anzeigen, wenn sich ein Support-Techniker in einer Sitzung mit dem Kunden befindet (nur Windows und macOS).

Aktivieren Sie das Kontrollkästchen, um den Bildschirm während einer Sitzung mit einem Wasserzeichen zu versehen.

Wasserzeichen ändern

Laden Sie ein eigenes Wasserzeichenbild zur Anzeige auf dem Client-Desktop hoch. Dieses eigene Bild ersetzt das standardmäßige BeyondTrust-Wasserzeichen. Beim Bild muss es sich um eine .png- oder .bmp-Datei zwischen 32x32 und 256x256 Pixeln handeln. Die empfohlene Bildgröße ist 128x128 Pixel. Sie können das gewählte Bild mit der Schiebeleiste in der Größe verändern oder auf die Schaltfläche **An Kasten anpassen** oder **Gesamten Kasten ausfüllen** klicken. Klicken Sie auf **Wasserzeichen speichern**, um die Änderungen zu speichern, oder auf **Änderungen verwerfen**, wenn Sie das gewählte Bild nicht beibehalten möchten.

Bei der Anzeige des Wasserzeichens auf dem Bildschirm des Kunden wird eine Transparenz von 40 % angewandt. So können Sie ein vollständig undurchsichtiges Bild hochladen, ohne dass dieses die Desktopansicht des Kunden behindert.

Hinweis: *Wenn Sie ein Bild hochladen, das bereits teilweise transparent ist, wird eine weitere Transparenz von 40 % angewandt. Damit kann das Bild transparenter als gewünscht werden.*

Hinweis: *Nachdem Kunden auf BeyondTrust Remote Support 17.1 aktualisiert haben, wird standardmäßig das neue Wasserzeichen als Wasserzeichen für alle öffentlichen Portale verwendet.*

Weitere Informationen finden Sie in Das Kunden-Client-Erscheinungsbild ändern auf https://www.beyondtrust.com/docs/remote-support/how-to/customize-portals/customer-client-appearance.htm.

Auf Standard zurücksetzen

Stellen Sie das Standardbild wieder her. Sobald Sie das Standardwasserzeichen wiederherstellen, verwenden alle neuen Sitzungen dieses Bild. Aktuell laufende Sitzungen sind davon nicht betroffen.

Sitzungsrichtlinie

Sitzungsrichtlinie

Weisen Sie eine Sitzungsrichtlinie für Sitzungen zu, die der oben auf dieser Seite gewählten öffentlichen Website zugewiesen wurden. Diese Sitzungsrichtlinie kann sich auf die Berechtigungen auswirken, die für über diese Site gestartete Sitzungen gestattet wurden.

Weitere Informationen finden Sie in Berechtigungen für das Fixieren/Lösen von Jump-Clients festlegen unter https://www.beyondtrust.com/docs/remote-support/how-to/jump-clients/permissions.htm.

Protokolloptionen

Bildschirmfreigabe-Aufzeichnung aktivieren

Wählen Sie für die oben auf dieser Seite gewählte öffentliche Website aus, ob Sie Bildschirmfreigabesitzungen aufzeichnen möchten. Sie können Aufzeichnungen aktivieren oder deaktivieren oder die auf der Seite **Konfiguration > Optionen** konfigurierte seitenweit geltende Einstellung verwenden. Diese Einstellung kann auf Kundenwunsch entsprechend der obigen Konfiguration über die Einstellung **Vor vollständigen Client-Sitzungen Sitzungsaufzeichnungsaufforderung anzeigen** überschrieben werden.

Befehlsshell-Aufzeichnung aktivieren

Wählen Sie für die oben auf dieser Seite gewählte öffentliche Website aus, ob Sie Befehlsshellsitzungen aufzeichnen möchten. Sie können Aufzeichnungen aktivieren oder deaktivieren oder die auf der Seite **Konfiguration > Optionen** konfigurierte seitenweit geltende Einstellung verwenden. Diese Einstellung kann auf Kundenwunsch entsprechend der obigen Konfiguration über die Einstellung **Vor vollständigen Client-Sitzungen Sitzungsaufzeichnungsaufforderung anzeigen** überschrieben werden.

Automatische Protokollierung von Systeminformationen aktivieren

Wählen Sie für die oben auf dieser Seite gewählte öffentliche Website aus, ob Sie Systeminformationen zu Beginn einer Sitzung automatisch protokollieren möchten. Sie können Aufzeichnungen aktivieren oder deaktivieren oder die auf der Seite **Konfiguration > Optionen** konfigurierte seitenweit geltende Einstellung verwenden. Diese Einstellung kann auf Kundenwunsch entsprechend der obigen Konfiguration über die Einstellung **Vor vollständigen Client-Sitzungen Sitzungsaufzeichnungsaufforderung anzeigen** überschrieben werden.

Verhalten nach Sitzung

Zeigen Sie nach Beendigung der Support-Sitzung die Deinstallationsmeldung an

Nachdem eine Sitzung beendet und kein Jump-Client installiert wurde, kann den Kunden mitgeteilt werden, dass die BeyondTrust-Software deinstalliert wurde.

Benutzerdefinierte Deinstallationsnachricht

Legen Sie den Text für die Deinstallationsmeldung fest. Sie können diesen Text für jegliche aktivierten Sprachen lokalisieren.

> *Weitere Informationen finden Sie in Anpassen der Deinstallationsmitteilung und der Austrittsumfragen unter https://www.beyondtrust.com/docs/remote-support/how-to/customize-portals/post-session-behavior.htm.*

Verbindungsoptionen

Zeitüberschreitung bei der Neuverbindung

Legen Sie fest, wie lange ein getrennter Kunden-Client versuchen soll, die Verbindung wiederherzustellen.

Schränkt den Kundenzugriff auf den Computer ein, wenn die Verbindung des Kunden-Client unterbrochen wird, oder wenn die Verbindung aller an der Sitzung teilnehmenden Support-Techniker unterbrochen wird

Wenn die Sitzungsverbindung verloren geht, kann die Maus- und Tastatureingabe des Remote-Systems vorübergehend deaktiviert und wieder aufgenommen werden, wenn die Verbindung wieder hergestellt oder die Sitzung beendet wird.

Support-Techniker berechtigen, diese Einstellung sitzungsweise zu überschreiben

Sie können einem Benutzer die Übersteuerung der Sitzungsbeendigungseinstellung über die Registerkarte **Zusammenfassung** in der Konsole während einer Sitzung gestatten.

Click-to-Chat

Aufforderung zur Namenseingabe

Passen Sie die Aufforderung zur Namenseingabe so an, dass eine bestimmte Frage oder ein bestimmter Text angezeigt wird, wenn ein Benutzer eine Click-To-Chat-Sitzung startet. Der Standardtext lautet: „Bitte geben Sie Ihren Namen ein.“

Heraufsetzungsaufforderung

Passen Sie den Text an, der dem Benutzer angezeigt werden soll, wenn er die Heraufsetzung einer Click-To-Chat-Sitzung anfordert. Der Standardtext lautet „%REP_NAME% fordert das Heraufsetzen auf vollständigen Remote-Support an, wodurch weitere Funktionen wie die Bildschirmfreigabe und der Dateitransfer verfügbar werden. Sie müssen eine Anwendung ausführen, die Ihnen zugesandt wird. Möchten Sie fortfahren?“

> ***Hinweis:*** *Das Makro* ***%REP_NAME%*** *wird durch den öffentlichen Anzeigenamen des Support-Technikers ersetzt, der die Heraufsetzung anfordert.*

HTML-<head>-Einfügung

Benutzer mit der Berechtigung **Berechtigt, öffentliche Websites zu bearbeiten** können benutzerdefinierten HTML-Code im <head>-Element der Seite einzufügen, die den HTML5 Click-to-Chat-Client darstellt.

Andere Optionen

Automatische Heraufsetzung

Wählen Sie, wie die Heraufsetzung des Kunden-Client auf einem Remote-Windows-System gehandhabt werden soll. Wenn die Option **Heraufsetzung nie versuchen** gewählt ist, versucht der Kunden-Client nie die Ausführung mit Administratorrechten, außer, wenn der Support-Techniker ausdrücklich die Heraufsetzung anfordert. Wenn Sie **Heraufsetzung nur versuchen, wenn der Kunde damit nicht um Berechtigung gebeten wird** gewählt haben, versucht der Kunden-Client automatisch die Ausführung als Administrator; aber nur dann, wenn der Remote-Benutzer hierdurch nicht um Berechtigung gebeten wird. Wenn **Heraufsetzung immer versuchen** gewählt ist, versucht der Kunden-Client immer die Ausführung als Administrator; zu Beginn einer Sitzung erhält der Remote-Kunde möglicherweise eine Aufforderung, die Heraufsetzung zu genehmigen.

Zulassen, dass der Kunde während der Bildschirmfreigabe die freizugebenden Anwendungen beschränkt, wenn dies nicht ausdrücklich erforderlich ist

Wenn Sie dem Kunden die Begrenzung der freigegebenen Anwendungen gestatten, kann Ihr Kunde festlegen, welche Anwendungen Sie während einer Sitzung mit Bildschirmfreigabe sehen können oder nicht. Ist diese Option deaktiviert, erhalten Kunden diese Option nur, wenn der Support-Techniker dies spezifisch anfordert oder nur berechtigt ist, begrenzte Kontrolle anzufordern.

Support-Techniker gestatten, die deaktivierte Strg-Alt-Entf-Einfügerichtlinie zu übergehen (nur Windows Vista® und höher)

Wird Windows Vista oder höher unterstützt, kann der Support-Techniker versuchen, die deaktivierte Sicherheitsaufruf-Einfügerichtlinie zu übergehen, um einen Strg-Alt-Entf-Befehl zu senden

Dem Kunden zulassen, Dateien über die Chat-Oberfläche anzubieten

Wenn Sie Dateiübertragungen vom Kunden an den Support-Techniker unterbinden müssen, können Sie die Möglichkeit des Kunden, während Chat-Sitzungen Dateien anzubieten, deaktivieren.

Wiedergabe von Chat-Sound-Benachrichtigungen im Kunden-Client von unterstützten Plattformen

Sie können festlegen, dass der Kunden-Client einen Mitteilungston ausgibt, wenn eine neue Meldung angezeigt wird.

Temporäre Deaktivierung der Hardwarebeschleunigung während der Bildschirmfreigabe durch Kunden-Client zulassen

Sie können dem Kunden-Client die Erlaubnis erteilen, zu ermitteln, ob ein Videokartentreiber auf dem Remote-Computer die CPU stark beansprucht. Sollte dies der Fall sein, kann der Kunden-Client bei der Bildschirmfreigabe die Hardware-Beschleunigung zeitweilig unterdrücken, um die Remote-Supportverbindung zu beschleunigen.

Präsentation: Einladungs-E-Mails und Anzeigeoptionen ändern

Öffentliche Portale | PRÄSENTATION

Hinweis: *Die Präsentationsfunktion muss aktiviert sein, wenn Ihre Support-Website erstellt wird. Ist dies nicht der Fall, und Sie müssen Präsentationen durchführen, wenden Sie sich bitte an den Support oder Ihren Website-Administrator.*

WICHTIG!

Diese Präsentationsfunktion ist ab Remote Support 22.1 veraltet und in den Bereitstellungen neuer Websites nicht enthalten. Für Upgrades ist sie AKTIVIERT, Sie können Sie jedoch auch DEAKTIVIEREN. Wenn Sie über eine neue Website-Bereitstellung verfügen und Präsentationen ausführen müssen, wenden Sie sich bitte an den Support oder Ihren Website-Administrator.

Weitere Informationen finden Sie in Eine Präsentation für Remote-Teilnehmer abhalten unter https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/presentation.htm.

Weitere Informationen siehe Präsentationsteilnehmer-Client: Einer Präsentation beitreten unter https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/customer-presentation-interface.htm.

Präsentationsteilnehmer

E-Mail-Einladung für geplante Präsentation

Hinweis: *Derzeit ist nur eine Konfiguration für den Präsentationsteilnehmer-Client verfügbar. Präsentationsteilnehmer-Clients können nicht über öffentliche Websites konfiguriert werden.*

Versand einer E-Mail, die Teilnehmer zu einer für die Zukunft geplanten Präsentation einlädt.

*Fehlt die Schaltfläche **Einladen** im Dialog für die Planung der Präsentation, vergewissern Sie sich, dass kundenseitige E-Mails in Ihrer Instanz konfiguriert und aktiviert worden sind. Weitere Informationen finden Sie in „E-Mail-Konfiguration: Konfigurieren der Software für das Versenden von E-Mails“ auf Seite 247.*

Betreff

Passen Sie den Betreff dieser E-Mail an. Sie können diesen Text für jegliche aktivierten Sprachen lokalisieren.

Text

Passen Sie den Text dieser E-Mail an. Verwenden Sie eines der unten auf der /login-Seite aufgeführten Makros, um den Text für Ihre Zwecke anzupassen.Sie können diesen Text für jegliche aktivierten Sprachen lokalisieren.

E-Mail-Einladung für gestartete Präsentation

Versand einer E-Mail, die Teilnehmer zu einer bereits laufenden Präsentation einlädt.

Betreff

Passen Sie den Betreff dieser E-Mail an. Sie können diesen Text für jegliche aktivierten Sprachen lokalisieren.

Text

Passen Sie den Text dieser E-Mail an. Verwenden Sie eines der unten auf der /login-Seite aufgeführten Makros, um den Text für Ihre Zwecke anzupassen.Sie können diesen Text für jegliche aktivierten Sprachen lokalisieren.

Präsentationsteilnehmer-Client

Anzeigeoptionen

Teilnahmevereinbarung vor Sitzungen anzeigen

Die **Teilnehmervereinbarung** wird angezeigt, bevor der BeyondTrust-Client heruntergeladen wird, um sicherzustellen, dass Ihr Teilnehmer die Bildschirmfreigabefunktionen des Programms kennt.

Kundenbegrüßung vor Sitzung anzeigen

Mit der **Grußmitteilung** wird Ihr Teilnehmer begrüßt, er wird aufgefordert, bis zum Beginn der Präsentation zu warten, und Audiokonferenz-Details werden zur Verfügung gestellt, falls Sie diese in der Seitenleiste für die Support-Techniker-Präsentation konfiguriert haben. Sie können diesen Text für jegliche aktivierten Sprachen lokalisieren.

Text

Passen Sie den Text dieser Vereinbarung an.Sie können diesen Text für jegliche aktivierten Sprachen lokalisieren.

Ablauf-Zeitüberschreitung

Sollte der Moderator nicht online sein, wenn die Präsentation beginnen sollte, bestimmt die **Ablauf-Zeitüberschreitung**, wie lange der Teilnehmer warten kann, bevor die Verbindung unterbrochen wird.

Nachricht für verwaiste Teilnehmer anzeigen

Sollte der Moderator nicht online sein, wenn die Präsentation beginnen sollte, und tritt er nicht vor der Ablauf-Zeitüberschreitung bei, kann Teilnehmern diese Nachricht angezeigt werden. Sie können diesen Text für jegliche aktivierten Sprachen lokalisieren.

Banner für Chat-Fenster

Teilnehmerbanner ändern

Laden Sie ein Bannerbild für das Kunden-Client-Fenster hoch. Dieses Bild muss im Windows-Bitmap-Format (BMP) mit 256 Farben (8 Bit) vorliegen und 480 Pixel breit sein. Die empfohlene Bildhöhe beträgt 40 Pixel. Sobald Sie ein neues Banner hochladen, verwenden alle neuen Sitzungen dieses Bild. Aktuell laufende Sitzungen sind davon nicht betroffen.

Auf Standard zurücksetzen

Stellen Sie das Standardbanner wieder her. Sobald Sie das Standardbanner wiederherstellen, verwenden alle neuen Sitzungen dieses Bild. Aktuell laufende Sitzungen sind davon nicht betroffen.

Verhalten nach Sitzung

Benutzerdefinierte Deinstallationsnachricht

Am Ende der Präsentation wird der Teilnehmer benachrichtigt, dass BeyondTrust deinstalliert wurde. Sie können diesen Text für jegliche aktivierten Sprachen lokalisieren.

Lokalisierung

Echtzeit-Chat: Übersetzen von Chatnachrichten zwischen Support-Techniker und Kunde

Lokalisierung | ECHTZEIT-CHAT

Die optionale Integration von BeyondTrust mit GeoFluent verschafft Ihrem Support-Desk einen globalen Vorteil, da Chats zwischen Support-Technikern und Kunden in Echtzeit übersetzt werden. Ohne Sprachbarriere kann Ihr Support-Team Kunden auf der ganzen Welt erreichen.

Nachrichten zwischen Kunden und Support-Technikern können in Echtzeit übersetzt werden, wenn diese Funktion aktiviert ist. Kunden, die Sitzungen über das öffentliche Portal starten, können oben auf der Seite ihre Sprache aus dem Dropdown-Menü wählen. Support-Techniker können ihre bevorzugte Chatsprache unter **Einstellungen > Globale Einstellungen** in der Konsole d. Support-Technikers festlegen.

API für GeoFluent beziehen

Um diese Integration einzurichten, benötigen Sie ein Lionbridge GeoFluent-Konto, verfügbar unter https://www.lionbridge.com/get-in-touch/.

Sobald Ihr Konto erstellt ist, abonnieren Sie die gewünschten Sprachpaare. Sprachpaare sind richtungsbezogen. Das Sprachpaar Englisch-Französisch übersetzt zum Beispiel englische Wörter ins Französische, aber nicht französische Wörter ins Englische. In diesem Fall ist ein zweites Sprachpaar, Französisch-Englisch, erforderlich, um die Übersetzung Französisch-Englisch zu unterstützen.

> ***Hinweis:*** *Der in Echtzeit übersetzte BeyondTrust-Chat-Support unterstützt in Remote Support Deutsch, Spanisch (Lateinamerika), Spanisch (Europa), Finnisch, Französisch, Italienisch, Japanisch, Niederländisch, Polnisch, Portugiesisch (Brasilien), Portugiesisch (Portugal), Russisch, Schwedisch, Türkisch, Chinesisch und Chinesisch (Kurzzeichen).*

Beziehen Sie von Ihrem GeoFluent-Konto den GeoFluent-API-Schlüssel und das API-Secret. Diese werden verwendet, um die Echtzeit-Chatübersetzung in Remote Support zu konfigurieren.

Echtzeit-Chatübersetzung konfigurieren

Führen Sie die folgenden Schritte aus, um Echtzeit-Chatübersetzungen für Support-Techniker zu aktivieren und Chat-Sprachoptionen auf dem öffentlichen Portal anzubieten:

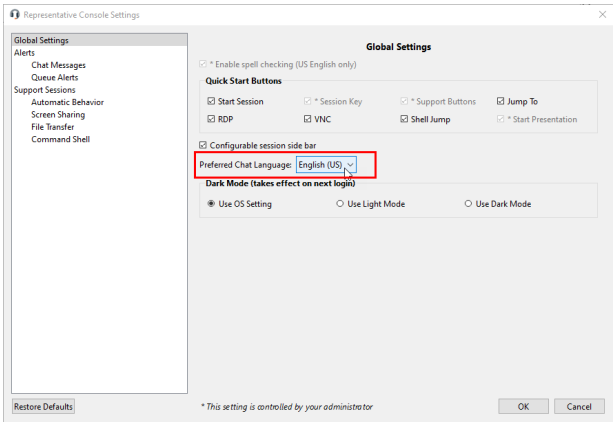
1. Melden Sie sich in der Verwaltungsschnittstelle an.
2. Klicken Sie im linken Menü auf **Lokalisierung** und dann auf die Registerkarte **ECHTZEIT-CHAT**.
3. Es wird eine standardmäßige **GeoFluent API-URL** angezeigt. Die standardmäßige API-URL ist für Benutzer in Nordamerika geeignet. In anderen Regionen kann sich die URL *https://api-eu.geofluent.com* als leistungsfähiger erweisen. Ihr GeoFluent-Vertreter kann Ihnen helfen zu entscheiden, ob Sie diesen Wert ändern müssen.
4. Geben Sie Ihren API-**Schlüssel** ein.
5. Geben Sie Ihr API-**Secret** ein.
6. Klicken Sie auf **Speichern**.

7. Das System testet die Verbindung und zeigt den Status an. Wenn der **Aktuelle Status** nicht **OK** ist, bestätigen Sie die eingegebenen Werte. Wenden Sie sich bei Bedarf an GeoFluent, um Unterstützung zu erhalten.
8. Sobald der Status **OK** lautet, werden die in GeoFluent ausgewählten **Sprachpaare** im unteren Teil des Bildschirms angezeigt.
9. Wählen Sie **Echtzeit-Chatübersetzungen aktivieren** , um diese Funktion für Support-Techniker verfügbar zu machen.

Echtzeit-Chat-Übersetzungen im Konsole d. Support-Technikers aktivieren

Sobald die Chat-Übersetzung in Echtzeit aktiviert ist, können Support-Techniker ihre bevorzugte Chat-Sprache auswählen, indem sie die folgenden Schritte ausführen:

1. Laden Sie die aktualisierte Konsole d. Support-Technikers herunter und installieren Sie sie.
2. Melden Sie sich an und klicken Sie auf **Datei** > **Einstellungen**.
3. Wählen Sie unter **Globale Einstellungen** die **Bevorzugte Chatsprache** aus der Dropdown-Liste.



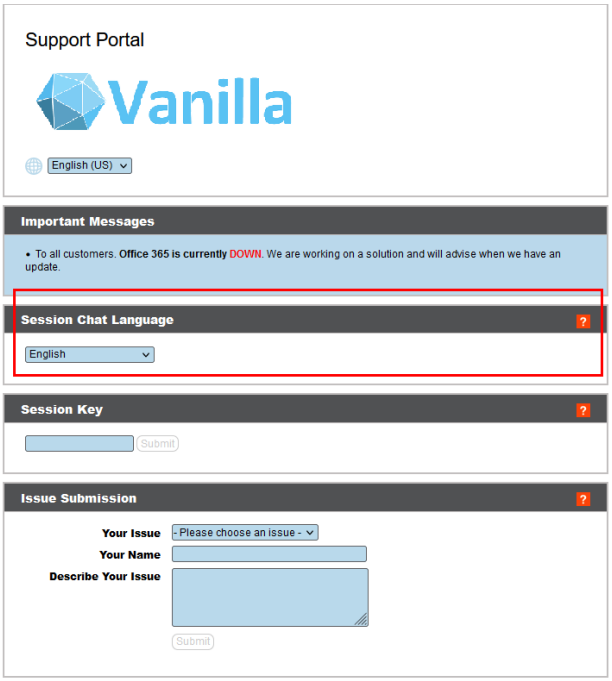
Dropdown-Menü für die Chat-Übersetzung auf öffentlichen Websites aktivieren

Sobald die Echtzeit-Chatübersetzungen aktiviert sind, kann den öffentlichen Portalen eine Option für die Sitzungssprache hinzugefügt werden. Dies ist zusätzlich zur Auswahl der Portalsprache möglich.

Klicken Sie unter **Öffentliches Portal** im unteren Bereich des Bildschirms auf den Link **Öffentliche Website** oder klicken Sie im linken Menü auf **Öffentliche Portale**. Wiederholen Sie die nachstehenden Schritte für jede Website, für die Sie eine Sitzungssprache wählen möchten.

1. Klicken Sie auf das Bleistiftsymbol, um die Seite zu bearbeiten.
2. Aktivieren Sie unter **Öffentliche Website bearbeiten** das Kontrollkästchen **Dropdownmenü für Sitzungs-Chat-Sprache anzeigen**.

Das Portal zeigt jetzt zwei Sprach-Dropdownmenüs an: eins für das Portal am oberen Rand des Bildschirms und eins für die Chat-Sitzung. Der Platz variiert je nach Layout und Optionen des Portals. Die Sprachoptionen für die Chat-Sitzungen sind die in GeoFluent ausgewählten Sprachpaare. Das bedeutet, dass die von einem Benutzer gewünschte Sprache für das Portal möglicherweise nicht für Chat-Sitzungen verfügbar ist und umgekehrt.



Weitere Informationen finden Sie hier:

- *Öffentliche Website: Support anfordern auf https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/public-site.htm.*
- *Während einer Sitzung mit dem Kunden chatten unter https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/chat.htm*

Sprachen: Verwalten der installierten Sprachen

Lokalisierung | SPRACHEN

Sprachen

BeyondTrust unterstützt derzeit Deutsch, Englisch, Lateinamerikanisches Spanisch, Europäisches Spanisch, Finnisch, Europäisches Französisch, Italienisch, Niederländisch, Polnisch, Brasilianisches Portugiesisch, Europäisches Portugiesisch, Schwedisch, Türkisch, Japanisch, Vereinfachtes Chinesisch, Traditionelles Chinesisch und Russisch. BeyondTrust unterstützt internationale Zeichensätze.

Hinweis: *Aufgrund der für die Übersetzung benötigten Zeit kommen Sprachpakete für neue Softwareversionen etwas später als ihr englisches Pendant auf den Markt. Bitte beachten Sie auch, dass die Lokalisierung von einigen Funktionen auf Zeichen der Größe von 1 Byte beschränkt sind. Die Verwendung von Zeichen der Größe von 2 Bytes (bestimmte Sprachpakete) können das Verhalten einiger Funktionen beeinflussen. Die BeyondTrust Jumpoint-Konfigurationsschnittstelle ist derzeit nicht als Übersetzung verfügbar.*

Aktiviert

Wenn mehr als ein Sprachpaket installiert ist, aktivieren Sie das Kontrollkästchen für jede Sprache, die Sie aktivieren möchten. Mit dem Aktivieren der Option wird diese Sprache im Dropdown-Menü in der Verwaltungsschnittstelle, der Konsole d. Support-Technikers und der öffentlichen Website verfügbar.

Standardsprachen

Ist mehr als ein Sprachpaket installiert, wählen Sie eine Sprache, die standardmäßig angezeigt werden soll. Klicken Sie auf **Sprachen aktualisieren**, um die Änderungen zu speichern.

Installation von Sprachpaketen

Sprachpakete müssen vom BeyondTrust-Administrator installiert und aktiviert werden. Der Support von BeyondTrust kann Sprachpakete in Software-Updates kompilieren, wenn er von Kunden dazu aufgefordert wird. Vor der Anforderung von Sprachpaketen sollten Sie sicherstellen, dass diese nicht bereits installiert sind und dass die aktuelle Version diese unterstützt. Um auf Sprachen zu prüfen und die erforderlichen Updates zu erhalten, folgen Sie diesen Schritten:

1. Melden Sie sich als Administrator in der BeyondTrust **/login**-Webschnittstelle an.
2. Navigieren Sie zur Registerkarte **Lokalisierung** und suchen Sie nach den erforderlichen Sprachen.
3. Wenn die Sprachen aufgeführt werden, aktivieren Sie das Kontrollkästchen für die Sprachen, die installiert werden sollen.
4. Wenn die Sprachen nicht aufgeführt werden, kontaktieren Sie den Support, um ein neues Update für sie zu erhalten.
5. Installieren Sie alle nötigen Aktualisierungen und testen Sie das System, um zu sehen, ob die gewünschte(n) Sprache(n) in BeyondTrust erscheinen.

Kunden können die gewünschte Sprache über das Dropdown-Menü **Sprache** online im öffentlichen Portal und über die Austrittsumfragenseite wählen. Support-Techniker können die gewünschte Sprache auf dem Anmeldebildschirm auswählen. Administratoren und Support-Techniker können ihre Sprache über das Dropdown-Menü in **/login** und **/appliance** wählen.

Tipp: *Es ist möglich, in einem Sitzungs-Chat eine Sprache zu verwenden, die von BeyondTrust nicht unterstützt wird, aber von GeoFluent durchaus. Weitere Informationen über diese optionale Integration finden Sie in Echtzeit-Chat: Übersetzen von Chat-Nachrichten zwischen Support-Techniker und Kunde auf https://www.beyondtrust.com/docs/remote-support/getting-started/admin/real-time-chat.htm.*

Suchen: Zeigen Sie benutzerdefinierten Text in aktivierten Sprachen an

Lokalisierung | SPRACHEN

Suchen

Sie können alle anpassbaren Nachrichten auf einer Seite anzeigen. Geben Sie ein Wort oder einen Satz in das Suchfeld ein, um die Suche einzuschränken. Klicken Sie auf die Nachricht, die Sie ändern möchten, um sie in allen aktivierten Sprachen anzuzeigen. Über diese Seite kann jede Nachricht einzeln geändert werden.

Der **Standard-String** kann nicht geändert werden und dient nur als Referenz für Ihre benutzerdefinierten Nachrichten. Sollten Sie eine Nachricht auf ihren Originaltext zurücksetzen müssen, löschen Sie den gesamten Text aus diesem Nachrichtenfeld und speichern Sie die leere Nachricht. Der Standardtext in dieser Sprache wird wieder angezeigt.

Verwaltung

Software: Laden Sie ein Backup herunter, nehmen Sie ein Software-Upgrade vor

Sicherungseinstellungen

Eine bewährte Methode bei der Notfallwiederherstellung besteht darin, regelmäßig eine Sicherungskopie Ihrer Software-Einstellungen zu speichern. BeyondTrust empfiehlt, dass Sie jedes Mal, wenn Sie die B Series Appliance-Einstellungen ändern, eine Sicherungskopie anfertigen. Bei einem Hardware-Ausfall kann eine Sicherungskopie die Wiederherstellung beschleunigen und BeyondTrust ggf. erlauben, Ihnen Zugriff auf temporäre Hostdienste zu gewähren, während die Einstellungen aus Ihrer letzten Sicherung beibehalten werden.

Sicherungspasswort

Um Ihre Softwaresicherungsdatei mit einem Passwort zu schützen, erstellen Sie ein Passwort. Wenn Sie sich entscheiden, ein Passwort festzulegen, können Sie nicht wieder auf die Sicherungskopie zurücksetzen, ohne das Passwort anzugeben.

Protokollierte Sitzungsberichtsdaten anhängen

Wird diese Option aktiviert, wird Ihre Sicherungsdatei Sitzungsprotokolle enthalten. Wird sie nicht aktiviert, werden Sitzungsberichtsdaten nicht in die Sicherungskopie aufgenommen.

Sicherung herunterladen

Speichern Sie eine Sicherungskopie der Softwarekonfiguration. Speichern Sie diese Datei an einem sicheren Ort.

Vault-Verschlüsselungsschlüssel sichern

Der Vault-Verschlüsselungsschlüssel wird zur Ver- und Entschlüsselung aller Vault-Anmeldedaten verwendet, die auf Ihrem BeyondTrust Appliance B Series gespeichert sind. Falls Sie Konfigurationsdaten von einem Sicherungs- auf ein neues B Series Appliance übertragen müssen, müssen Sie auch den Vault-Verschlüsselungsschlüssel von einem Backup wiederherstellen, um die verschlüsselten Vault-Anmeldedaten der Konfigurationssicherungskopie nutzen zu können.

Sicherungspasswort

Um Ihre Softwaresicherungsdatei mit einem Passwort zu schützen, erstellen Sie ein Passwort. Wenn Sie sich entscheiden, ein Passwort festzulegen, können Sie nicht wieder auf die Sicherungskopie zurücksetzen, ohne das Passwort anzugeben.

Vault-Verschlüsselungsschlüssel herunterladen

Klicken Sie auf die Schaltfläche **Vault-Verschlüsselungsschlüssel herunterladen**, um den Vault-Verschlüsselungsschlüssel zur späteren Verwendung herunterzuladen.

> ***Hinweis:*** *Der Vault-Verschlüsselungsschlüssel muss passwortgeschützt sein.*

Einstellungen wiederherstellen

Sicherungsdatei der Konfiguration

Sollten Sie eine Sicherung wiederherstellen müssen, suchen Sie die letzte gespeicherte Sicherungsdatei.

Passwort für die Sicherungsdatei der Konfiguration

Wenn Sie ein Passwort für Ihre Sicherungsdatei erstellt haben, geben Sie es hier ein.

Vault-Verschlüsselungsschlüssel-Sicherungsdatei

Um den Vault-Verschlüsselungsschlüssel für die Konfigurationssicherung anzugeben, wählen Sie die Vault-Verschlüsselungsschlüssel-Sicherungsdatei.

Vault-Verschlüsselungsschlüssel-Sicherungspasswort

Geben Sie das Passwort ein, das Sie zum Herunterladen des BeyondTrust-Vault-Verschlüsselungsschlüssels verwendet haben.

Sicherungsdatei hochladen

Laden Sie die Sicherungsdatei auf Ihr B Series Appliance hoch und stellen Sie die Einstellungen Ihrer Website entsprechend der Einstellungen in der Sicherungsdatei wieder her.

> ***Hinweis:*** *Beachten Sie, dass durch die Wiederherstellung einer Website-Sicherung weder das Hilfesymbol auf das zum Sicherungszeitpunkt festgelegte Bild zurückgestellt wird, noch seit der Sicherung hinzugefügte Dateien entfernt werden. Nicht alle Dateien werden gesichert, nur die ersten 50 Dateien unter 200 KB Größe.*

> *Weitere Informationen finden Sie in Sicherungsverfahren auf https://www.beyondtrust.com/docs/remote-support/how-to/disaster-recovery/index.htm.*

Aktualisierung hochladen

Klicken Sie auf **Datei auswählen**, um neue Softwarepakete von BeyondTrust manuell hochzuladen. Bestätigen Sie, dass Sie das Software-Paket hochladen möchten. Im Abschnitt **Hochgeladene Aktualisierung** werden weitere Informationen angezeigt, um Ihr

hochgeladenes Paket zu verifizieren. Klicken Sie auf **Installieren**, wenn Sie den Installationsvorgang beenden möchten oder **Aktualisierung abbrechen**, wenn Sie die Aktualisierung abbrechen möchten. Wenn Ihr Paket lediglich zusätzliche Lizenzen beinhaltet können Sie die das Update installieren, ohne dass das B Series Appliance neu gestartet werden muss. Nach Ihrer Installationsbestätigung wird auf dieser Seite eine Statusleiste angezeigt, die Sie über den Fortschritt der Aktualisierung informiert. Hier vorgenommene Aktualisierungen aktualisieren automatisch alle Websites und Lizenzen in Ihrem BeyondTrust Appliance B Series.

> ***Hinweis:*** *Ihr B Series Appliance-Administrator kann auch die Funktion* ***Auf Aktualisierungen prüfen*** *der B Series Appliance-Schnittstelle verwenden, um automatisch nach neuen Softwarepaketen zu suchen und diese zu installieren.*

Website-Migration

Mit der Website-Migration können Sie Konfigurationseinstellungen und Daten von einer anderen BeyondTrust Remote Support Website migrieren. Die Migration kann zum Beispiel für den Wechsel von einer lokalen Installation zu einer Cloud-Installation verwendet werden. Bei der Migration wird ein API-Konto zum automatischen Herunterladen und Wiederherstellen einer Sicherung verwendet.

Vorbereitung der Migration

Bevor Sie die Daten migrieren, beachten Sie bitte diese Voraussetzungen und Bedingungen:

- Das API-Konto benötigt Lesezugriff oder höheren Zugriff auf die Befehls-API und Zugriff auf die Backup- und Vault-Kodierungsschlüssel-APIs.
- Der Administrator benötigt Zugriff auf das lokale Administratorkonto, um sich anzumelden, falls die Sicherheitsanbieter nach der Migration nicht ordnungsgemäß wieder verbunden werden.
- Wenn die Quell-Site-Version älter als 21.2 ist, muss der Vault-Kodierungsschlüssel manuell migriert werden.
- Wenn der Zielstandort eine Cloud-Installation ist oder aus anderen Gründen keine passiven Jump-Clients unterstützt, müssen alle bestehenden passiven Jump-Clients vor der Migration in aktive Jump-Clients konvertiert werden. Wenn nicht, werden sie deinstalliert. Wenn der Zielstandort passive Jump-Clients unterstützt, z. B. bei der Migration zu einer lokalen Installation, können passive Jump-Clients migriert werden.
- Aufzeichnungen sind nicht Bestandteil der Migration. Um den Zugriff auf bestehende Aufzeichnungen beizubehalten, lassen Sie die Quelle mit einem anderen Hostnamen online oder verwenden Sie den Integration Client, um die Aufzeichnungen vor der Migration zu sichern.
- Nachdem die Daten migriert wurden, sind weitere Schritte erforderlich, um die neue Instanz voll funktionsfähig zu machen. Diese Schritte sind auf der Seite **Website-Migration** aufgeführt und werden im Folgenden zusammengefasst:
    - Erstellen Sie einen neuen DNS-Eintrag für den Hostnamen, um auf die alte Website zuzugreifen.
    - Fügen Sie den neuen Hostnamen in das öffentliche Portal der alten Site ein.
    - Bestätigen Sie den Zugang zur alten Website.
    - Geben Sie den DNS-Einträgen Zeit, sich in den Netzwerken zu verbreiten.
    - Klicken Sie auf die Schaltfläche **Software neu starten** auf der alten Site, um die Clients auf die neue Site umzustellen.

Daten-Migration

1. Geben Sie die folgenden Informationen über die Quell-Site ein, um eine Migration zu starten:
    - **Hostname**
    - **OAuth Client-ID**
    - **OAuth Client-Secret**

2. Sobald die Informationen eingegeben sind, klicken Sie auf **Verbindung prüfen**.
    - Eine Pop-up-Benachrichtigung bestätigt die Verbindung und dass die Website-Version unterstützt wird.
    - **Zurücksetzen** kann jederzeit vor Beginn der Migration angeklickt werden, wenn Änderungen erforderlich sind.
3. Klicken Sie gegebenenfalls auf **+Zertifikat wählen**, um das **SSL-Zertifikat** für ein selbstsigniertes SSL-Zertifikat auszuwählen.

Hinweis: *Die Zertifikate müssen im PEM-, DER- oder CRT-Format vorliegen.*

Tipp: *Sobald die Verbindung verifiziert ist, steht die Option **Automatischer Beginn der Site-Migration** zur Verfügung. Aktivieren Sie diese Option, um einige der folgenden Schritte und Benachrichtigungen zu umgehen. Wenn diese Option aktiviert ist, klicken Sie auf **Sicherungskopie wiederherstellen** und reagieren Sie auf die Benachrichtigungen, um die Migration abzuschließen.*

4. Überprüfen Sie die angezeigten Informationen und klicken Sie, wenn sie korrekt sind, auf **Sicherungskopie abrufen**. Wenn dies nicht der Fall ist, klicken Sie auf **Zurücksetzen**.
5. Es erscheinen Popup-Bestätigungsmeldungen für die Sicherungsdatei und, falls für Ihre Version zutreffend, für den Vault-Kodierungsschlüssel. Die Dateinamen werden auf dem Bedienfeld angezeigt, ebenso wie eine Schaltfläche **Website migrieren**.
6. Klicken Sie auf **Website migrieren**.
7. Eine Pop-up-Benachrichtigung weist darauf hin, dass ein lokales Konto erforderlich ist, und eine zweite Pop-up-Benachrichtigung weist darauf hin, dass die Migration die Daten auf der aktuellen Website überschreibt. Dann wird eine Meldung **Migration in Bearbeitung** angezeigt.
8. Wenn die Migration abgeschlossen ist, klicken Sie in der Popup-Benachrichtigung auf **Ja**, um die Website zurückzusetzen. Melden Sie sich erneut an, um die migrierten Daten anzuzeigen.
9. Führen Sie die Schritte nach der Migration durch, die im Fenster **Website-Migration** aufgeführt sind.

Sicherheit: Verwalten der Sicherheitseinstellungen

Authentifizierung

Standardmäßige -Authentifizierungsmethode

Die standardmäßige Authentifizierungsmethode ist **Benutzername und Passwort**. Wenn die passwortlose Authentifizierung aktiviert ist, kann passwortloses FIDO2 als Standardauthentifizierungsmethode ausgewählt werden. Wenn die passwortlose Authentifizierung aktiviert ist, kann bei der Anmeldung eine der beiden Authentifizierungsmethoden ausgewählt werden.

Passwortlose FIDO2-Authentifizierung aktivieren

Mit dieser Funktion können sich Benutzer des lokalen Sicherheitsanbieters oder Anbieter-Benutzer registrieren und mit FIDO2-zertifizierten Authentifizierern anstatt sich mit einem Passwort anzumelden. FIDO2-Authentifizierergeräte müssen CTAP2 unterstützen und in der Lage sein, eine Benutzerverifizierung mittels Biometrik oder einer PIN durchzuführen.

Diese Funktion ist standardmäßig aktiviert. Deaktivieren Sie das Häkchen, um die Funktion zu deaktivieren. Wenn deaktiviert:

- Der Abschnitt **Passwortlose Authentifizierer** unter **Mein Konto > Sicherheit** ist ausgeblendet.
- Die **Passwortlose FIDO2**-Option ist in den Anmelde-Dropdowns nicht verfügbar.
- Die Benutzer können sich nicht mit zuvor registrierten Authentifizierern anmelden.

Wenn Sie diese Funktion deaktivieren, werden zuvor registrierte Authentifizierungen nicht entfernt. Wenn es notwendig ist, diese zu entfernen, müssen sie gelöscht werden, bevor die Funktion deaktiviert wird.

Benutzer mit registrierter passwortloser Authentifizierung können sich weiterhin mit ihrem Benutzernamen und Passwort anmelden. Dies kann nützlich sein, wenn sie sich mit einem Gerät anmelden müssen, das die passwortlose Authentifizierung nicht unterstützt.

Diese Funktion kann nicht auf bestimmte Benutzer oder Benutzergruppen beschränkt werden.

Weitere Informationen und die Möglichkeit, Authentifizierer zu registrieren, finden Sie unter „Passwortlose Authentifizierer“ auf Seite 19.

Sperren des Kontos nach

Legen Sie fest, wie oft ein falsches Passwort eingegeben werden darf, bevor das Konto gesperrt wird.

Kontosperrdauer

Legt fest, wie lange ein ausgesperrter Benutzer warten muss, bevor die erneute Anmeldung möglich ist. Alternativ können Sie erfordern, dass ein Administrator das Konto wieder freischalten muss.

Kennwörter

Mindestlänge des Passworts

Legen Sie für lokale Benutzerkonten Regeln bezüglich der Länge von Kennwörtern fest.

Standardgültigkeitsdauer für Kennwörter

Legen Sie für lokale Benutzerkonten Regeln fest, wie oft Kennwörter ablaufen.

Komplexe Kennwörter erforderlich

Legen Sie für lokale Benutzerkonten Regeln bezüglich der Komplexität von Kennwörtern fest.

Passwortrücksetzung aktivieren

Dies ermöglicht es Benutzern mit E-Mail-Adressen, vergessene Kennwörter zurückzusetzen. Der in Passwortrücksetzungs-E-Mails angegebene Link ist gültig, bis eines der folgenden Ereignisse eintritt:

- 24 Stunden sind verstrichen.
- Es wird auf den Link geklickt und das Passwort wird erfolgreich zurückgesetzt.
- Das System sendet einen weiteren Link an die E-Mail-Adresse.

Konsole d. Support-Technikers

Sitzung abbrechen, wenn Konto verwendet wird

Wenn ein Benutzer versucht, sich mit einem bereits verwendeten Konto in der Konsole d. Support-Technikers anzumelden, wird bei aktiviertem Kästchen **Sitzung beenden** die vorhergehende Verbindung unterbrochen, um die neue Anmeldung zu erlauben.

Gespeicherte Anmeldungen aktivieren

Gestatten Sie der Konsole d. Support-Technikers, die Anmeldedaten eines Benutzers zu speichern, oder verweigern Sie es.

Abmelden des inaktiven Support-Technikers nach

Legen Sie fest, wie lange es dauert, bis ein inaktiver Benutzer von der Konsole d. Support-Technikers abgemeldet wird, um die Lizenz für einen anderen Benutzer freizugeben.

Warnung und Abmeldebenachrichtigung bei Zeitüberschreitung wegen Inaktivität aktivieren

Legen Sie fest, ob ein Benutzer eine Eingabeaufforderung erhalten soll, bevor er aufgrund von Inaktivität abgemeldet wird. Die erste Benachrichtigung findet 30 Sekunden vor der Abmeldung statt, die zweite nach der Abmeldung.

Support-Techniker bei Inaktivität aus Sitzung entfernen

Diese Option entfernt den Benutzer nach einer von Ihnen gewünschten Zeit der Inaktivität effektiv aus der Zugriffssitzung. Hierdurch können BeyondTrust-Kunden Konformitätsinitiativen mit Inaktivitätsanforderungen gerecht werden. Der Benutzer wird eine Minute, bevor er entfernt wird, hierüber benachrichtigt und kann die Zeitüberschreitung neu einstellen.

Ein Benutzer wird in einer Sitzung als aktiv angesehen, wenn Dateien entweder über die Registerkarte Datentransfer oder die Chat-Schnittstelle transferiert werden, oder wenn er die Maustaste betätigt oder auf der Registerkarte Sitzung eine Taste drückt. Mausbewegungen an sich gelten nicht als Aktivität. Sobald die Aktivität endet, wird der Inaktivitätszähler gestartet.

Verbindung über mobile Konsole d. Support-Technikers und Web-Konsole des Support-Technikers mit Connect gestatten

Gewährt Benutzern die Option, über die Konsole d. Support-Technikers -App für iOS und Android und die Web-Konsole des Support-Technikers, eine browserbasierte Konsole d. Support-Technikers auf Remote-Systeme zuzugreifen.

Anzeigen der Miniaturansicht in der Konsole d. Support-Technikers

Wird ein Kunde mithilfe mehrerer Bildschirme unterstützt, kann der Benutzer mit dieser Option Miniaturansichten aller verfügbaren Bildschirme anzeigen. Diese Miniaturansichten werden nicht während Sitzungsaufnahmen aufgenommen. Deaktivieren Sie dieses Kästchen, um Rechtecke anstatt Miniaturansichten anzuzeigen.

Zulassen, dass der Support-Techniker einen Remote-Screenshot aufnimmt

Sie können Benutzern erlauben, Bildschirmaufnahmen des Remote-Desktops von der Konsole d. Support-Technikers zu machen.

Steuerung des Kunden-Client-Fensters durch Support-Techniker zulassen

Wird diese Einstellung aktiviert, kann der Support-Techniker im Kunden-Client-Fenster als Benutzer agieren und so zum Beispiel im Chat-Bereich tippen, Dateien versenden und mit Links und Schaltflächen interagieren. Wird diese Einstellung deaktiviert, sind die Möglichkeiten des Support-Technikers im Kunden-Client-Fenster auf Verschieben und Minimieren beschränkt.

Wenn Sie eine Heraufsetzung von der Konsole des Support-Technikers anfordern, erlauben Sie, dass Anmeldedaten eingegeben werden.

Wird eine Sitzung für Administratorrechte heraufgesetzt, erlauben Sie den Benutzern die manuelle Eingabe von Anmeldedaten, die Einfügung aus einem Passwort-Vault oder die Bereitstellung über eine virtuelle Smart-Card. So können Benutzer autorisierte geschützte Anmeldedaten verwenden, um den Kontext der Kunden-Client heraufzusetzen. Nach dem Heraufsetzen wird die Kunden-Client im Kontext des lokalen Systems ausgeführt.

Neustart mit zwischengespeicherten Anmeldedaten zulassen

Bei einer Support-Sitzung mit Administratorrechten auf einem Remote-Windows-Computer kann ein Support-Techniker mit dieser Option den Remote-Rechner ohne Mithilfe des Kunden durch Eingabe der Anmeldedaten vor dem Neustart neu starten. Diese Anmeldedaten können für die Dauer der Support-Sitzung gespeichert werden, wodurch die Anmeldung am Rechner automatisch erfolgt, wenn der Computer mehrmals neu gestartet wird.

Synchronisierungsmodus für Zwischenablage

Synchronisierungsmodus für Zwischenablage legt fest, wie Benutzer die Zwischenablagen innerhalb einer Bildschirmfreigabesitzung synchronisieren dürfen. Verfügbare Einstellungen:

- **Automatisch:** Die Zwischenablagen von Kunde und Support-Techniker werden automatisch synchronisiert, wenn sich in einem von beiden etwas ändert.
- **Manuelle Installation:** Der Support-Techniker muss auf eines der Zwischenablage-Symbole in der Konsole d. Support-Technikers klicken, um entweder Inhalte zu versenden oder aus der Zwischenablage des Endpunktes abzurufen.

Sie MÜSSEN die Software auf der Statusseite neu starten, damit diese Einstellung wirksam wird.

Administratoren können den Zugriff auf die Zwischenablage durch Support-Techniker verhindern und Support-Technikern das Senden von Daten zum Endpunkt erlauben oder den Zugriff in beiden Richtungen erlauben (Senden und Empfangen von Daten). Über diese Einstellungen wird bestimmt, welche Zwischenablagesymbole dem Support-Techniker in der Konsole d. Support-Technikers angezeigt werden, wenn der Modul **Manuell** ausgewält ist, und wie die Synchronisierung im Modus **Automatisch** funktioniert.

Detaillierte Zugriffsoptionen für die Zwischenablage können für Sitzungsrichtlinien und Gruppenrichtlinien eingerichtet sowie bestimmten Support-Technikern gewährt werden. Bitte beachten Sie zu jedem speziellen Fall die nachstehenden Links:

- **„Benutzer: Benutzerberechtigungen für einen Support-Techniker oder Admin hinzufügen“ auf Seite 112****: Benutzer und Sicherheit > Benutzer > Hinzufügen > Berechtigungen für überwachte und unüberwachte Sitzungen > Bildschirmfreigabe**
- **„Sitzungsrichtlinien: Sitzungsberechtigungen und Aufforderungsregeln festlegen“ auf Seite 149****: Benutzer und Sicherheit > Sitzungsrichtlinien > Hinzufügen > Berechtigung > Bildschirmfreigabe**
- **„Gruppenrichtlinien: Benutzerberechtigungen auf Benutzergruppen anwenden“ auf Seite 159****: Benutzer und Sicherheit > Gruppenrichtlinien > Hinzufügen > Berechtigungen für überwachte und unüberwachte Sitzungen**

Suche nach externen Jump-Items zulassen

Dies ermöglicht die Jump-Item-Suche in Remote Support über einen vollständig konfigurierten Endpunkt-Anmeldedaten-Manager (ECM).

> ***Hinweis:*** *Sie müssen die Software neu starten, damit diese Einstellung wirksam wird. Wenn Sie diese Einstellung aktivieren oder deaktivieren, werden Sie auf der* ***Status****-Seite in /login aufgefordert, jetzt neu zu starten oder später neu zu starten.*

Jumpoint für externe Jump-Item-Sitzungen

Dieses Feld ist nur verfügbar, wenn die Option **Suche nach externen Jump-Items zulassen** markiert ist. Alle Sitzungen, die von externen Jump-Items aus gestartet werden, laufen über den hier ausgewählten Jumpoint. Wenn mehrere Jumpoints auf Endpunkten in segmentierten Netzwerken bereitgestellt werden, kann der verwendete Jumpoint durch Abgleich mit der Netzwerk-ID eines externen Jump-Items automatisch ausgewählt werden. Ein Jumpoint muss im Netzwerk positioniert sein, um eine Verbindung zu potenziell jedem der von ECM zurückgegebenen externen Jump-Items herzustellen.

Wählen Sie den Jumpoint, der für externe Jump-Item-Sitzungen verwendet werden soll, aus der Dropdown-Liste der verfügbaren Jumpoints aus, oder belassen Sie die Standardauswahl **Automatisch ausgewählt durch externe Jump Item-Netzwerk-ID**, damit Remote Support bestimmen kann, welcher Jumpoint die Sitzung handhabt.

Die **Externe Jump-Item-Netzwerk-ID** ist ein Attribut, das Sie für den Jumpoint unter **Jump > Jumpoint** in /login festlegen müssen. Es entspricht dem Attribut **Workgroup** auf verwalteten Systemen in Password Safe. Sein Wert wird mit der Eigenschaft **Netzwerk-ID** für externe Jump-Items abgeglichen, die vom ECM zurückgegeben werden, um den Jumpoint für eine Sitzung zu bestimmen.

Externer Jump-Item Gruppenname

Dieses Feld ist nur verfügbar, wenn die Option **Suche nach externen Jump-Items zulassen** markiert ist. Geben Sie optional einen Namen für die externe Jump-Gruppe ein oder belassen Sie die Standardoption **Externe Jump-Items**. Dieser Name wird als Name der Jump-Gruppe angezeigt, wenn Jump-Items in der Konsole d. Support-Technikers oder der Web-Konsole des Support-Technikers angezeigt werden. Klicken Sie auf **Speichern**, wenn Sie den Standardgruppennamen geändert haben.

Spezielle Aktionsbefehle „Ausführen als“ in Sitzungsberichten protokollieren

Deaktivieren Sie diese Option, um die Protokollierung und Meldung aller *Ausführen als*-Befehle zu beenden. Da der gesamte Befehl protokolliert wird, werden Anmeldedaten, die als Befehlsparameter weitergegeben werden, protokolliert.

Sitzungsschlüssel

Sitzungsschlüssellänge

Die **Sitzungsschlüssellänge** kann auf eine beliebige Zahl zwischen 7 und 20 festgelegt werden.

Sitzungsschlüssel zur einmaligen Verwendung

Ist **Sitzungsschlüssel zur einmaligen Verwendung** aktiviert, kann ein Sitzungsschlüssel nicht mehr als einmal zur Erstellung einer Support-Sitzung verwendet werden.

Max. Sitzungsschlüssel-Zeitüberschreitung

Max. Sitzungsschlüssel-Zeitüberschreitung legt die maximale Zeit fest, die ein Sitzungsschlüssel gültig sein kann. Ein Benutzer kann in der Konsole d. Support-Technikers die Lebenszeit jedes generierten Sitzungsschlüssels festlegen, die nicht länger als der auf dieser Seite definierte Zeitraum sein kann. Verwendet der Kunde den Sitzungsschlüssel nicht innerhalb des zulässigen Zeitraums, verfällt der Schlüssel, und der Benutzer muss einen neuen Sitzungsschlüssel ausgeben, um eine Sitzung durchzuführen.

Öffentliches Portal

Öffentliche Website zwingen, HTTPS zu verwenden

Die Option **Öffentliche Website zwingen, SSL zu verwenden (https)** bietet zusätzliche Sicherheit. Durch die Verwendung von HTTPS wird die Internetverbindung mit Ihrem öffentlichen Support-Portal gezwungen, SSL-Verschlüsselung zu verwenden, sodass eine zusätzliche Sicherheitsstufe implementiert wird, um zu vermeiden, dass nicht autorisierte Benutzer auf Konten zugreifen können.

Blockieren von externen Ressourcen, Inline-Skripten undInline-Styles auf der öffentlichen Website

Hindern Sie Ihre öffentliche Website am Laden externer Ressourcen, Ausführen von Inline-Skripten oder der Anzeige von Inline-Styles. Diese Option wird durch Versenden des HTTP-Headers „Content-Security-Policy (CSP)“ mit dem Wert **default-src 'self'** aktiviert.

Der CSP-Header teilt dem Browser mit, Ressourcen wie Bilder, Schriftarten, Stylesheets, Skripte, Frames und andere Unterressourcen, die sich extern zur eigenen Domäne befinden, zu ignorieren. Außerdem werden Inline-Skripte und Styles ignoriert, unabhängig davon, ob sie im Head oder Body der Seite eingebettet sind. Dies wirkt sich auch auf Inline-Skripte und-Styles aus, die zur Laufzeit dynamisch über JavaScript hinzugefügt werden.

Jegliche Ressourcen, die Sie nutzen möchten, müssen unter **Öffentliche Portale > Dateispeicher** auf das B Series Appliance hochgeladen werden. Aktivieren Sie diese Option nicht, wenn Sie die Vorlage Ihrer öffentlichen Website zur Verwendung von Inline-Skripten, Styles oder anderen Ressourcen angepasst haben, die sich außerhalb Ihrer BeyondTrust-Website befinden.

Vereinfachten Sitzungsstart aktivieren

Versuchen, Sitzungen mit ClickOnce oder Java zu starten. Ist diese Option deaktiviert, muss der Kunden-Client manuell heruntergeladen und ausgeführt werden.

Indexierung öffentlicher Websites deaktivieren

Aktivieren Sie **Indizierung öffentlicher Websites deaktivieren**, um Suchmaschinen an der Indizierung von Seiten zu hindern, die von Ihrem B Series Appliance gehostet werden.

Sonstiges

Aufbewahrungszeitraum für Protokollinformationen (in Tagen)

Legen Sie in Aufbewahrungszeitraum für **Protokollinformationen (in Tagen)** fest, wie lange Anmeldeinformationen im B Series Appliance gespeichert bleiben sollen. Diese Information umfasst auch die Berichtdaten und Aufnahmen der Sitzung. Die maximale Dauer, für die Sitzungsberichtsdaten und Aufzeichnungen auf einem B Series Appliance beibehalten werden, beträgt 90 Tage. Dies ist die Standardeinstellung bei einer Neuinstallation. Es ist möglich, dass Sitzungsaufzeichnungen für einige Sitzungen innerhalb des Beibehaltungszeitraums nicht verfügbar sind. Dies kann durch eingeschränkten Speicherplatz oder die Einstellung **Aufbewahrungszeitraum für Protokollinformationen (in Tagen)** bedingt sein.

Das BeyondTrust Appliance B Series führt täglich ein Wartungsskript aus, das einen Speicherplatzverbrauch von nicht mehr als 90 % sicherstellt. Wird dieser Wert überschritten, beginnt das Skript mit der Löschung von Sitzungsaufzeichnungen basierend auf einer Formel, bis der Verbrauch unter 90 % fällt. Wenn die Einstellung **Aufbewahrungszeitraum für Protokollinformationen** kürzlich geändert wurde, kann es bis zu 24 Stunden dauern, bis die neue Einstellung wirksam wird.

> *Wenn Daten oder Aufzeichnungen über das konfigurierte Limit hinaus aufbewahrt werden müssen, empfiehlt BeyondTrust die Nutzung des Integrations-Client (www.beyondtrust.com/docs/remote-support/how-to/integrations/ic) oder der Berichts-API (www.beyondtrust.com/docs/remote-support/how-to/integrations/api/reporting).*

Vorab ausgetauschter Schlüssel zur Kommunikation zwischen Geräten

Geben Sie ein Passwort in das Feld **Geräteübergreifender, vorab geteilter Kommunikationsschlüssel** ein, um eine vertrauenswürdige Verbindung zwischen zwei B Series Applianceen herzustellen. Für zwei oder mehr B Series Appliancee müssen die Schlüssel übereinstimmen, damit sie für Funktionen wie Failover oder Clustering konfiguriert werden können. Der Schlüssel muss mindestens 6 Zeichen lang sein und mindestens einen Großbuchstaben, einen Kleinbuchstaben, eine Zahl und ein Sonderzeichen enthalten.

Tage für die Aufbewahrung von Jump-Item-Protokollierungsinformationen

Wählen Sie, wie lange Jump-Item-Berichtsdaten von dem Gerät aus zugänglich sein sollen. Da Daten nur einmal pro Tag gelöscht werden, kann der Zugriff unter Umständen bis zu 24 Stunden nach dem ausgewählten Wert möglich sein.

Wiederherstellung des Chatverlaufs aktivieren

Aktivieren Sie dieses Kontrollkästchen, damit das Chatfenster die Chatnachrichten wiederherstellt, wenn eine Sitzung unterbrochen und dann wiederaufgenommen wird.

Remote-Support-Client-Verifizierung während Heraufsetzungsversuchen erfordern

Sie müssen während der Heraufsetzung die Verifizierung des Remote-Support-Clients bereitstellen.

SSL-Zertifikatprüfung

Sie können auch eine **SSL-Zertifikatsprüfung** anfordern, um BeyondTrust-Software (einschließlich Konsole d. Support-Technikers, Kunden-Clients, Präsentations-Clients und Jump-Clients) zu zwingen, zu überprüfen, ob die Zertifizierungskette vertrauenswürdig ist, das Zertifikat nicht abgelaufen ist und der Zertifikatname dem Hostnamen des B Series Appliance entspricht. Kann die Zertifizierungskette nicht ordnungsgemäß überprüft werden, wird die Verbindung nicht zugelassen.

Wenn die Zertifikatprüfung deaktiviert wurde und dann wieder aktiviert wird, werden alle Konsolen und Clients automatisch bei der nächsten Verbindung aktualisiert. Bitte beachten Sie, dass die LDAP Connection Agents nicht automatisch aktualisiert werden, sondern erneut installiert werden müssen, damit diese Einstellung in Kraft tritt.

Ist die **SSL-Zertifikatprüfung** aktiviert, werden zusätzlich zur integrierten Sicherheit in BeyondTrust Sicherheitsprüfungen durchgeführt, um die SSL-Zertifizierungskette zu überprüfen, die für die sichere Kommunikation verwendet wird. Es wird dringend empfohlen, die SSL-Prüfung zu aktivieren. Ist die Zertifikatprüfung deaktiviert, wird auf Ihrer Verwaltungsschnittstelle eine Warnmeldung angezeigt. Sie können diese Meldung 30 Tage lang ausblenden.

***Hinweis:** Zur Aktivierung des SSL-Zertifikats müssen Sie das SSL-Zertifikat BeyondTrust zur Verfügung stellen, damit das Zertifikat in die BeyondTrust-Software eingebettet werden kann.*

Weitere Informationen finden Sie in SSL-Zertifikate und BeyondTrust Remote Support auf https://www.beyondtrust.com/docs/remote-support/how-to/sslcertificates/index.htm.

Netzwerkbeschränkungen

Sie können bestimmen, welche IP-Netzwerke auf /login, /api und die Konsole d. Support-Technikers auf Ihr BeyondTrust Appliance B Series zugreifen können. Wenn Sie die Netzwerkeinschränkungen aktivieren, können Sie auch erzwingen, dass die Konsole d. Support-Technikers nur über bestimmte Netzwerke genutzt werden kann.

Definieren Sie Netzwerkregeln für die folgenden Schnittstellen:

Admin-Schnittstelle (/login) und API-Schnittstelle (/api)

- **Netzwerkbeschränkungen immer anwenden**: Anhand dieser Option können Sie entweder eine Berechtigungsliste ausschließlich mit zulässigen Netzwerken oder eine Ablehnungsliste mit Netzwerken erstellen, denen der Zugriff verweigert wird. Anhand dieser Option können Sie festlegen, welche Beschränkungen (wenn überhaupt) für Desktop-, mobile und Webzugriffskonsole gelten sollen.
- **Netzwerkbeschränkungen niemals anwenden**: Wird diese Option aktiviert, finden keine Beschränkungen Anwendung, und es sind keine weiteren Optionen verfügbar, um Beschränkungen für Desktop-, mobile und Webkonsole festzulegen.

Desktop- und mobile Konsole d. Support-Technikers

- **Netzwerkbeschränkungen immer anwenden**: Wird diese Option aktiviert, werden die Netzwerkbeschränkungen der Verwaltungsschnittstelle übernommen.
- **Netzwerkbeschränkungen niemals anwenden**: Bei Auswahl dieser Option werden auf Desktop- und mobilen Konsolen keine Beschränkungen angewendet, Sie haben jedoch die Option, Beschränkungen für die Web-Konsole d. Support-Technikers festzulegen.
- **Netzwerkbeschränkungen nur bei erster Authentifizierung des Benutzers anwenden**: Hiermit werden die oben ausgewählten Beschränkungen angewendet, aber nur beim ersten Anmelden des Benutzers.

Webkonsole (/console)

- **Netzwerkbeschränkungen immer anwenden**: Bei Auswahl dieser Option übernimmt die Web-Konsole d. Support-Technikers die in der Verwaltungsschnittstelle eingegebenen Beschränkungen.
- **Netzwerkbeschränkungen niemals anwenden**: Bei Auswahl dieser Option werden auf die Web-Konsole d. Support-Technikers selbst dann keine Beschränkungen angewendet, wenn bei anderen Zugriffskonsolen-Methoden Beschränkungen gelten.

> *Weitere Informationen finden Sie im Web-Konsole des Support-Technikers-Handbuch auf https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/web/index.htm.*

Definieren Sie Ihre Netzwerkbeschränkungen:

Geben Sie die Netzwerkadresspräfixe (einen pro Zeile) ein. Die Netzmaske ist optional und kann entweder in Dezimalschreibweise mit Punkt oder als Ganzzahlbitmaske angegeben werden. Wird die Netzmaske weggelassen, so wird von einer einzelnen IP-Adresse ausgegangen.

- **Erlauben-Liste**: Nur die spezifizierten Netzwerke erlauben
- **Ablehnen-Liste**: Verweigern Sie die angegebenen Netzwerke.

Port-Einschränkungen für die Verwaltungs-Webschnittstelle

Legen Sie die Ports fest, über die der Zugriff auf Ihre /login-Schnittstelle möglich sein soll.

Proxy-Konfiguration

Konfigurieren Sie einen Proxy-Server so, dass der Datenfluss auf Informationen vom B Series Appliance kontrolliert wird. Dies gilt für ausgehende Ereignisse und API-Anrufe.

Proxy-Protokoll

Konfigurieren Sie HTTP- oder HTTPS-Proxy-Typen für vom B Series Appliance ausgehende Verbindungen.

Proxy-Konfiguration aktivieren

Aktivieren Sie das Kontrollkästchen, um die ausgehende Proxy-Konfiguration zu aktivieren.

Proxy-Host

Gehen Sie die IP-Adresse oder den Hostnamen Ihres Proxy-Servers an.

Proxy-Port

Geben Sie den von Ihrem Proxy-Server verwendeten Port an. Der Standard-Port ist **1080**.

Benutzername und Passwort des Proxys

Wenn für den Proxy-Server eine Authentifizierung erforderlich ist, geben Sie einen Benutzernamen und ein Passwort ein.

Testen

Klicken Sie auf **Testen**, um sicherzugehen, dass die Einstellungen ordnungsgemäß vorgenommen worden sind. Das aktuelle Testergebnis wird im Bereich **Letztes Testergebnis** angezeigt. Fehlermeldungen zeigen an, wo die Einstellungen korrigiert werden müssen.

ICAP-Konfiguration

Sie können Dateiübertragungen so konfigurieren, dass sie über die Secure Remote Access Appliance laufen und von einem ICAP-Server (Internet Content Adaptation Protocol) gescannt werden. Erkennt der ICAP-Server eine schädliche Datei, wird diese nicht weitergeleitet.

WICHTIG!

In den folgenden Szenarien können keine Dateiübertragungen an einen ICAP-Server gesendet werden: Protokolltunnel jump-basierte Dateiübertragungen, Zwischenablage-Dateiübertragungen innerhalb von RDP-Sitzungen und externe Tool-Dateiübertragungen innerhalb von RDP- oder Shell Jump-Sitzungen. Selbst wenn ICAP aktiviert ist, werden diese Übertragungen nicht gescannt.

Hinweis: *Die Aktivierung von ICAP oder die Änderung der ICAP-URL erfordert einen Neustart des Geräts, um sicherzustellen, dass die Clients wieder verbunden und richtig konfiguriert sind. In einer Atlas-Umgebung ist eine Synchronisierung erforderlich.*

Die Verwendung von ICAP verringert die Leistung von Dateiübertragungen aufgrund der zusätzlichen Schritte und Prüfungen. Wenn der ICAP-Server ausgefallen ist, schlägt die Dateiübertragung fehl.

Eine unsachgemäße ICAP-Konfiguration verhindert, dass Jumpoints korrekt funktionieren.

ICAP-Einstellungen

Geben Sie die **ICAP-Server-URL** ein. Diese wird von Ihrem ICAP-Server-Anbieter bereitgestellt. Der Standard-Port ist 1344. Wenn Sie einen anderen Port verwenden, muss er zusammen mit der URL in diesem Format angegeben werden: **icap://example.com:0000** oder **icaps://example.com:0000**.

Wenn das Protokoll **icaps://** lautet, markieren Sie **CA-Zertifikat verwenden**. Klicken Sie dann auf **Ein Zertifikat wählen** und laden Sie das Zertifikat hoch.

Hinweis: *Wenn Sie ein selbstsigniertes ICAPS-Zertifikat verwenden und kein Zertifikat einer Zertifizierungsstelle zu dessen Prüfung hochladen, schlagen alle Übertragungen von Sitzungsdateien fehl.*

Bei abgelaufenen oder ungültigen Zertifikaten schlagen die Übertragungen von Sitzungsdateien ungeachtet dessen fehl, ob ein Zertifikat einer Zertifizierungsstelle hochgeladen wird.

Speichern Sie die ICAP-Einstellungen vor dem Testen.

ICAP-Testverbindung

Nachdem Sie die ICAP-Einstellungen eingegeben und gespeichert haben, klicken Sie auf **TEST MIT EINER DATEI** und wählen eine Datei zum Hochladen aus. Es gibt drei mögliche Ergebnisse:

- Ein Verbindungsfehler. Ein Fehlerhinweis und ICAP-Protokolle werden angezeigt (falls vorhanden).
- Eine bösartige Datei wird entdeckt. Ein Warnhinweise und Antwortdetails werden angezeigt. Es wird nicht angezeigt, um welche Art von bösartigem Inhalt es sich genau handelt.
- Es werden keine Probleme festgestellt. Die Antwortdetails werden angezeigt.

Website-Konfiguration: HTTP-Ports festlegen, Erforderliche Anmeldungsvereinbarung aktivieren

HTTP-Ports

HTTP-Port und HTTPS-Port

Erfahrene Netzwerktechniker, die in nicht standardmäßigen Netzwerkumgebungen arbeiten, können die von BeyondTrust verwendeten Ports ändern. Diese Port-Einstellungen sollten nur angepasst werden, wenn andere Ports als der Standard-Port 80 und 443 für den Internetzugriff verwendet werden.

Erforderliche Anmeldungsvereinbarung für /login

Anmeldungsvereinbarung aktivieren

Sie können eine Anmeldungsvereinbarung aktivieren, die Benutzer annehmen müssen, bevor Sie auf die /login-Verwaltungsschnittstelle oder das Konsole d. Support-Technikers zugreifen können. Die konfigurierbare Vereinbarung gestattet Ihnen die Angabe von Einschränkungen und internen Richtlinien, bevor sich Benutzer anmelden dürfen.

Titel der Vereinbarung

Passen Sie den Titel dieser Vereinbarung an.Sie können diesen Text für jegliche aktivierten Sprachen lokalisieren.

Text der Vereinbarung

Geben Sie den Text für die Anmeldungsvereinbarung an. Sie können diesen Text für jegliche aktivierten Sprachen lokalisieren.

E-Mail-Konfiguration: Konfigurieren der Software für das Versenden von E-Mails

Verwaltung | E-MAIL-KONFIGURATION

E-Mail-Adresse

Hinweis: *Wenn ein B Series Appliance als Sicherungs-B Series Appliance oder Datenverkehrsknoten verwendet wird, wird die E-Mail-Konfiguration dieses B Series Appliances mit der E-Mail-Konfiguration überschrieben, die auf dem primären B Series Appliance definiert wurde.*

Absender

Legen Sie die E-Mail-Adresse fest, von der automatische Nachrichten Ihres B Series Appliance versendet werden sollen.

SMTP-Relay-Server

Konfigurieren Sie Ihr B Series Appliance so, dass es mit Ihrem SMTP-Relay-Server verwendet werden kann, um automatische E-Mail-Benachrichtigungen über bestimmte Ereignisse zu senden.

SMTP-Relay-Server

Geben Sie den Hostnamen oder die IP-Adresse Ihres SMTP-Relay-Servers ein.

SMTP-Port

Wählen Sie den SMTP-Port für den Serverkontakt aus.

SMTP-Verschlüsselung

Wählen Sie je nach den Einstellungen Ihres SMTP-Servers **TLS**, **STARTTLS** oder **Keine**.

SMTP-Authentifizierungstyp

Um eine Form der Authentifizierung mit diesem Server zu verwenden, wählen Sie entweder **Benutzername und Passwort** oder **OAuth2**. Wählen Sie andernfalls **Keine**.

Benutzername und Passwort

Geben Sie einen Benutzernamen und ein Passwort ein, um diese Form der Authentifizierung zu konfigurieren.

OAuth 2

Weitere Informationen finden Sie unter „OAuth2 für Azure Active Directory konfigurieren“ auf Seite 249 oder unter „OAuth2 für Google konfigurieren“ auf Seite 250 am Ende dieses Handbuchs.

Admin-Kontakt

E-Mail-Adressen des Standard-Admin-Kontakts

Geben Sie eine oder mehrere E-Mail-Adressen ein, an die E-Mails gesendet werden sollen. Trennen Sie Adressen mit einem Leerzeichen.

Tägliche Kommunikationsmitteilung schicken

Das B Series Appliance kann eine tägliche Benachrichtigung schicken, um zu gewährleisten, dass die Benachrichtigung korrekt funktioniert.

Senden Sie eine Test-E-Mail, nachdem die Einstellungen gespeichert wurden

Wenn Sie eine sofortige Test-E-Mail-erhalten möchten, um zu bestätigen, dass Ihre SMTP-Einstellungen korrekt konfiguriert sind, aktivieren Sie diese Option, bevor Sie auf **Speichern** klicken.

Neben den Test-E-Mails und täglichen Kommunikationsmeldungen, die oben konfiguriert werden können, werden E-Mails auch für folgende Ereignisse versendet:

- Während Failover-Vorgängen stimmt die Produktversion am primären Knoten nicht mit der Produktversion am Sicherungsknoten überein.
- Während einer Failover-Statusprüfung wird eines der folgenden Probleme erkannt:
    - Das aktuelle B Series Appliance ist der primäre Knoten und eine geteilte IP-Adresse wird in /login konfiguriert, doch die Netzwerkschnittstelle ist nicht aktiviert.
    - Eine geteilte IP-Adresse ist in /login konfiguriert, wird aber in /appliance nicht als IP-Adresse aufgeführt.
    - Der Sicherungsknoten konnte den primären Knoten nicht kontaktieren, und auch nicht eine der Test-IP-Adressen, die auf der Seite **Verwaltung > Failover** konfiguriert wurden.
    - Der Sicherungsknoten konnte keine der Test-IP-Adressen kontaktieren, die auf der Seite **Verwaltung > Failover** konfiguriert wurden.
    - Die Sicherungsvorgänge des Backup-Knoten wurden auf der Seite **Verwaltung > Failover** deaktiviert.
    - Der Sicherungsknoten konnte unerwarteterweise keine Prüfung von sich selbst vornehmen. Dies deutet auf einen Defekt hin.
    - Der Sicherungsknoten konnte den primären Knoten nicht mit dem Hostnamen des primären Knotens erreichen.
    - Der automatische Failover ist deaktiviert, und der Sicherungsknoten konnte keine Prüfung des primären Knotens vornehmen.
    - Der automatische Failover ist aktiviert, und der Sicherungsknoten konnte keine Prüfung des primären Knotens vornehmen. Der Sicherungsknoten wird automatisch zum pimären Knoten, wenn der primäre Knoten weiterhin nicht antwortet.

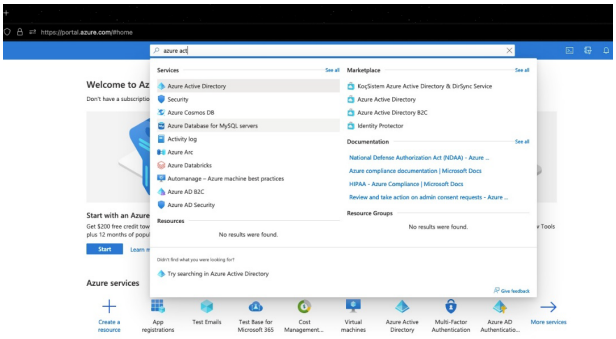
- Der automatische Failover ist aktiviert, und der Sicherungsknoten wird automatisch der primäre Knoten, weil der primäre Knoten zu lange nicht antwortet.
- Der primäre Knoten konnte in den letzten 24 Stunden keine Datensynchronisierung mit dem Sicherungsknoten vornehmen.

OAuth2 für Azure Active Directory konfigurieren

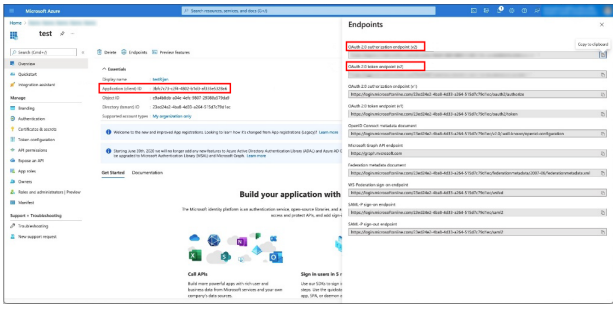
Hinweis: *Bevor Sie mit der Konfiguration auf Azure Active Directory beginnen, muss ein Azure/Office 365-Administrator-authentifiziertes SMTP für jedes Konto auf Exchange online aktivieren. Gehen Sie dazu zu* ***Office 365 Admin Portal (admin.microsoft.com) > Aktive Benutzer > Mail > E-Mail-Anwendungen verwalten*** *und aktivieren Sie* ***Authentifiziertes SMTP****.*

Azure Active Directory konfigurieren

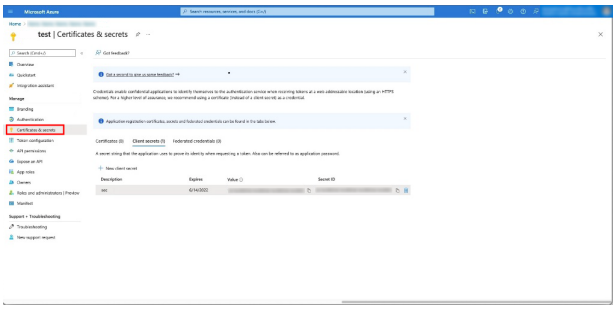
1. Melden Sie sich bei Ihrer Azure-Konsole an (portal.azure.com) und navigieren Sie zu **Azure Active Directory**.
2. Gehen Sie zu **App-Registrierungen** und wählen Sie **Neue Registrierung**.
   - Geben Sie einen Namen ein, z. B. Gerät-OAuth2.
   - Wählen Sie die Kontotypen aus, mit denen Sie sich über OAuth2 bei der Anwendung anmelden können möchten. Wählen Sie **Single Tenant** für nur intern.
   - Geben Sie den **Weiterleitung-URI** in der Form *https:///{URL IHRER APPLIANCE}/login/smtp-verification/* ein.
   - Klicken Sie auf **Registrieren**.



3. Auf der **Übersichtsseite** (ausgewählt aus dem linken Menü) die **Anwendungs-(Client-)ID**. Er wird später benötigt.
4. Klicken Sie auf **Endpunkte** (oberhalb der **Anwendungs-(Client-)ID**).
5. Beachten Sie den **OAuth2.0 Autorisierungsendpunkt (v2)** URI und den **OAuth-Token-Endpunkt (v2)** URI. Diese werden später benötigt.



6. Beachten Sie auf der Seite **Zertifikate & Secrets** (aus dem linken Menü ausgewählt) das **Client-Secret**. Er wird später benötigt. Wenn Sie kein **Client-Secret** haben, klicken Sie auf **New Client-Secret**, um eines zu erstellen.



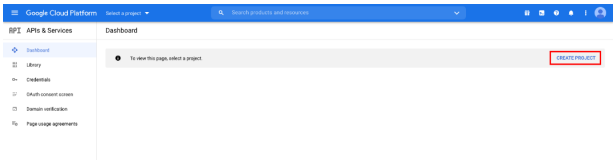
Anmeldedaten bereitstellen für den SMTP-Relay-Server

1. Navigieren Sie in der Privileged Remote Access Verwaltungsschnittstelle zu **Verwaltung > E-Mail-Konfiguration**.
2. Wählen Sie unter **SMTP-Authentifizierungstyp** die Option **OAuth2**, und geben Sie die folgenden Informationen ein:
    - **SMTP-OAuth-Anbieter-ID**: Die zuvor erwähnte Anwendungs-ID.
    - **SMTP-OAuth-Client-Secret**: Das zuvor erwähnte Client-Secret.
    - **SMTP-Oauth-Bereiche**: Geben Sie **https://outlook.office.com/SMTP.Send offline_access** ein.
    - **SMTP-OAuth-Authentifizierungsendpunkt**: Der zuvor erwähnte Autorisierungsendpunkt.
    - **SMTP-OAuth-Token-Endpunkt**: Der zuvor erwähnte Token-Endpunkt.

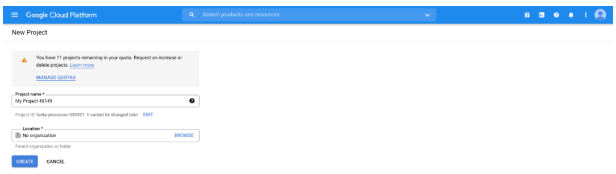
OAuth2 für Google konfigurieren

Google Cloud konfigurieren

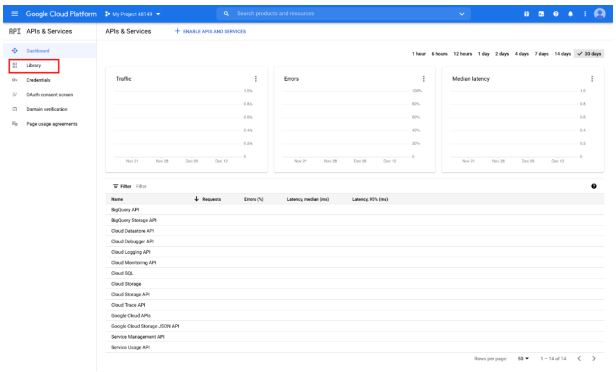
1. Melden Sie sich bei Ihrer Google Cloud Platform-Konsole (Google Dev Console) an (console.cloud.google.com). Verwenden Sie das richtige Gmail-Konto, da nur der Eigentümer des Projekts mit dem Projekt arbeiten kann. Wenn Sie noch kein bezahltes Konto haben, können Sie ein Konto erwerben, indem Sie auf **Aktivieren** im oberen Banner klicken. BeyondTrust kann Ihnen beim Kauf eines Kontos nicht behilflich sein. Klicken Sie auf **Mehr erfahren** im oberen Banner, um Informationen über die Einschränkungen der kostenlosen Konten zu erhalten.



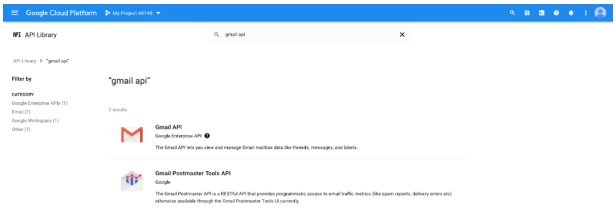
2. Klicken Sie auf **PROJEKT ERSTELLEN**. Sie können auch ein bestehendes Projekt verwenden.
3. Akzeptieren Sie den Standard-**Projektnamen** oder geben Sie einen neuen Namen ein.
4. Akzeptieren Sie die Standardeinstellung **Speicherort** oder wählen Sie einen der für Ihr Unternehmen verfügbaren Ordner.
5. Klicken Sie auf **ERSTELLEN**.



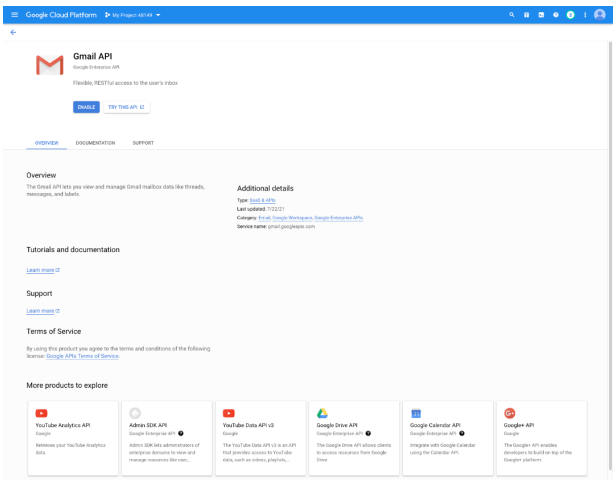
6. Die Seite **APIs und Dienste** wird angezeigt. Klicken Sie im linken Menü auf **Bibliothek**.



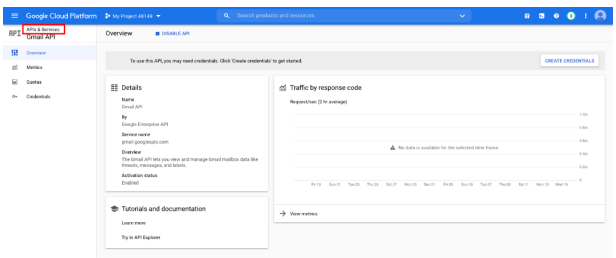
7. Suchen Sie in der Bibliothek nach der **Gmail-API** und klicken Sie darauf.



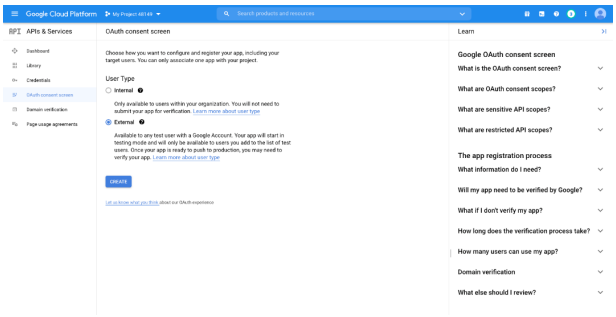
8. Die **Gmail API** erscheint auf einer eigenen Seite. Klicken Sie auf **AKTIVIEREN**.



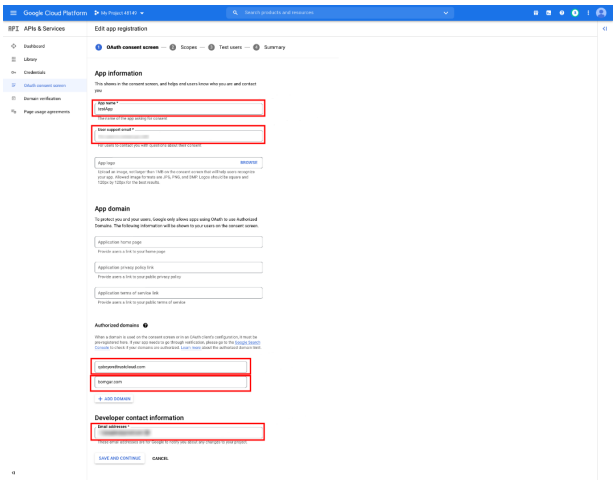
9. Die Seite **Gmail API-Übersicht** wird angezeigt. Klicken Sie oben links auf **APIs & Dienste**.
10. Die Seite **APIs und Dienste** wird wieder angezeigt. Klicken Sie im linken Menü auf **OAuth-Zustimmungsbildschirm**.



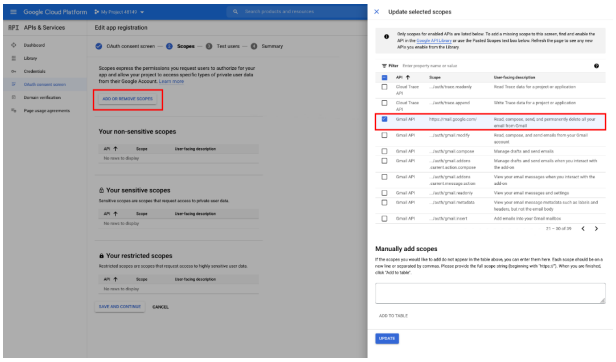
11. Wählen Sie den **Benutzertyp**. Intern erlaubt nur Benutzern innerhalb der Organisation, erfordert aber ein Google Workspace-Konto.
12. Klicken Sie auf **ERSTELLEN**.



13. Geben Sie den **App-Namen** ein.
14. Geben Sie eine **Benutzer-Support-E-Mail**-Adresse ein. Dies kann standardmäßig die Adresse sein, die Sie zum Erstellen des Projekts verwenden.
15. Geben Sie, falls gewünscht, ein Logo für die App ein. Der Abschnitt **Anwendungsbereich** ist ebenfalls optional.
16. Fügen Sie **Zugelassene Domains** hinzu. Für BeyondTrust Testgeräte sind das:
    - qabeyondtrustcloud.com
    - bomgar.com
17. Geben Sie die **Kontaktinformationen des Entwicklers** ein. Dies ist die E-Mail-Adresse, die Sie zur Erstellung des Projekts verwenden.
18. Klicken Sie auf **SPEICHERN UND WEITER**.

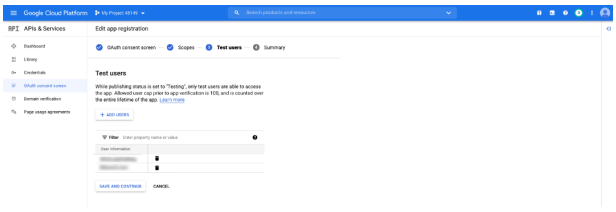


19. Klicken Sie auf der Registerkarte **Bereiche** auf **Bereiche hinzufügen oder entfernen**. Dies öffnet das Fenster **Ausgewählte Bereiche aktualisieren**.
20. Suchen Sie den Bereich **https://mail.google.com/** für die Gmail-API und überprüfen Sie ihn.



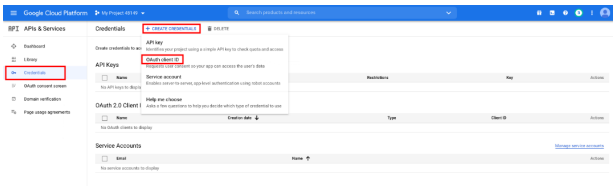
> ***Hinweis:*** *Die API wird nicht angezeigt, wenn sie nicht aktiviert wurde.*

21. Klicken Sie **UPDATE**. Das Fenster **Ausgewählte Bereiche aktualisieren** wird geschlossen.
22. Klicken Sie auf **SPEICHERN UND WEITER**.
23. Klicken Sie auf der Registerkarte **Testbenutzer** auf **BENUTZER HINZUFÜGEN**. Dies öffnet das Fenster **Benutzer hinzufügen**. Fügen Sie die Benutzer hinzu, die Zugriff auf die Anwendung haben, und klicken Sie auf **ZUFÜGEN**. Beachten Sie die Zugriffsbeschränkungen für Testbenutzer und die damit verbundenen Einschränkungen.

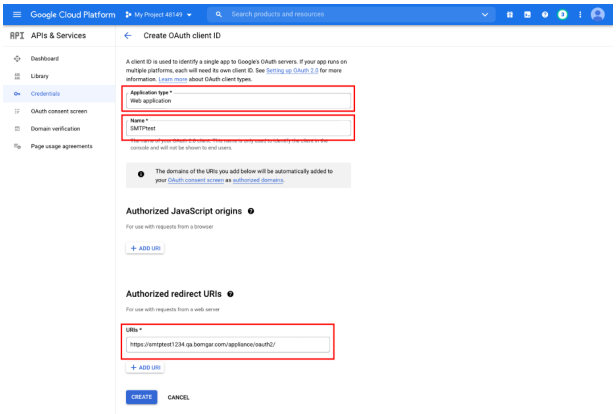


24. Klicken Sie auf **SPEICHERN UND WEITER**.
25. Überprüfen Sie die Zusammenfassung und nehmen Sie gegebenenfalls Änderungen oder Korrekturen vor.
26. Klicken Sie auf **ZURÜCK ZUM DASHBOARD**.

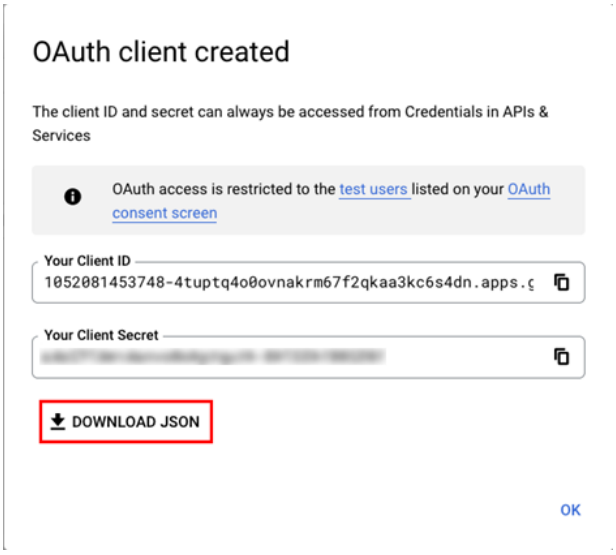
27. Klicken Sie im linken Menü auf **Anmeldedaten**.
28. Klicken Sie auf **ANMELDEDATEN ERSTELLEN** im oberen Banner und wählen Sie **OAuth-Client-ID**.



29. Wählen Sie auf der Seite zum Erstellen von Anmeldedaten **Webanwendung** für den **Anwendungstyp**. Wenn diese Option ausgewählt ist, erscheinen zusätzliche Felder.
30. Geben Sie einen Namen für die Anwendung ein.
31. Scrollen Sie nach unten zu **Zugelassene Umleitungs-URIs** und klicken Sie auf **URI hinzufügen**.
32. Geben Sie den **URI für Autorisierungsweiterleitung** in der Form *https://{URL IHRER APPLIANCE}/login/smtp-verification/* ein.
33. Klicken Sie auf **ERSTELLEN**.



34. Ein Fenster bestätigt die Erstellung des OAuth-Clients und zeigt die **Client ID** und **Client-Secret** an. Klicken Sie hier, um eine JSON-Datei herunterzuladen. Die Datei enthält Informationen, die für die nächsten Schritte benötigt werden.
35. Klicken Sie auf **OK**, um zur Seite "APIs und Dienste" zurückzukehren.



Anmeldedaten bereitstellen für den SMTP-Relay-Server

1. Navigieren Sie in der Privileged Remote Access Verwaltungsschnittstelle zu **Verwaltung > E-Mail-Konfiguration**.
2. Wählen Sie unter **SMTP-Authentifizierungstyp** die Option **OAuth2**, und geben Sie die folgenden Informationen ein:
    - **SMTP-OAuth-Anbieter-ID**: Die **client_id** aus der JSON-Datei, die während der Google-Konfiguration erstellt wurde.
    - **SMTP-OAuth-Client-Secret**: Das **client_secret** aus der JSON-Datei, die während der Google-Konfiguration erstellt wurde.
    - **SMTP-Oauth-Bereiche**: Geben Sie **https://mail.google.com/** ein.
    - **SMTP-OAuth-Authentifizierungsendpunkt**: Das **auth_uri** aus der JSON-Datei, die während der Google-Konfiguration

erstellt wurde.

- **SMTP-OAuth-Token-Endpunkt**: Das **token_uri** aus der JSON-Datei, die während der Google-Konfiguration erstellt wurde.

Ausgehende Ereignisse: Ereignisse für die Auslösung von Nachrichten festlegen

HTTP-Empfänger

Sie können Ihr B Series Appliance darauf konfigurieren, Nachrichten an einen HTTP-Server oder an eine E-Mail-Adresse zu senden, wenn verschiedene Ereignisse ausgelöst werden.

Die vom B Series Appliance gesendeten Variablen kommen als HTTP POST-Methode an und können durch Aufruf der zur Abfrage von POST-Daten in Ihrer Programmiersprache verwendeten Methode eingesehen werden. Wenn der Server nicht mit HTTP 200 den Erfolg bestätigt, reiht das B Series Appliance das aktuelle Ereignis wieder in die Warteschlange ein und versucht es später noch einmal.

Hinzufügen, Bearbeiten, Löschen

Erstellen Sie einen neuen Empfänger, bearbeiten Sie einen bestehenden Empfänger oder entfernen Sie einen bestehenden Empfänger.

HTTP-Empfänger hinzufügen oder bearbeiten

Aktiviert

Sie können das Kontrollkästchen **Aktiviert** deaktivieren, um die Meldungen für den eingerichteten Ereignis-Handler zu stoppen, beispielsweise etwa im Falle eines geplanten Integrationstests.

Name

Erstellen Sie einen eindeutigen Namen, um diesen Empfänger leichter zu identifizieren.

URL

Geben Sie die Ziel-URL für diesen Handler für ausgehende Ereignisse an.

CA-Zertifikat verwenden

Unter einer HTTPS-Verbindung müssen Sie das Root-Zertifikat der Zertifizierungsstelle hochladen, das vom ausgehenden Ereignisserver genannt wird.

Benutzerdefinierte Felder senden

Wählen Sie diese Option, wenn benutzerdefinierte Felder und deren Werte mit dem ausgehenden Ereignis gesendet werden sollen.

Zu sendende Ereignisse

Wählen Sie, welche Ereignisse die zu sendenden Meldungen auslösen.

Wiederholungsintervall

Legen Sie fest, wie häufig die Durchführung eines fehlgeschlagenen Ereignisses erneut versucht werden soll.

Wiederholungsdauer

Wenn ein Ereignis weiterhin fehlschlägt, legen Sie fest, wie lange die Durchführung wiederholt versucht werden soll, bevor das Ereignis ignoriert wird.

E-Mail des Kontakts

Geben Sie eine oder mehrere E-Mail-Adressen ein, an die bei einem Fehler eine Benachrichtigung gesendet werden soll.

E-Mail-Alarm senden nach

Legen Sie fest, wie lange nach einem Fehler die E-Mail versendet werden soll. Ist das Problem vor Ablauf dieser Zeit behoben und ist das Ereignis erfolgreich, wird keine Fehlerbenachrichtigung gesendet.

E-Mail-Alarme erneut senden

Sie können festlegen, wie oft Fehler-E-Mails gesendet werden sollen, wenn der Status weiterhin einen Fehlerstatus meldet.

E-Mail-Empfänger

Hinzufügen, Bearbeiten, Löschen

Erstellen Sie einen neuen Empfänger, bearbeiten Sie einen bestehenden Empfänger oder entfernen Sie einen bestehenden Empfänger.

Wiederholungsdauer

Wenn ein Ereignis weiterhin fehlschlägt, legen Sie fest, wie lange die Durchführung wiederholt versucht werden soll, bevor das Ereignis ignoriert wird.

E-Mail-Empfänger hinzufügen oder bearbeiten

Bevor Sie Ihr B Series Appliance dafür einrichten können, Ereignisnachrichten an eine E-Mail-Adresse zu senden, müssen Sie sicherstellen, dass Ihr B Series Appliance für Ihren SMTP-Relay-Server konfiguriert ist. Gehen Sie zur Seite **Verwaltung > E-Mail-Konfiguration**, um die Einstellungen zu überprüfen.

Aktiviert

Verwenden Sie das Kontrollkästchen **Aktiviert**, um die Meldungen für den eingerichteten Ereignis-Handler zu stoppen, beispielsweise etwa im Falle eines geplanten Integrationstests.

Name

Erstellen Sie einen eindeutigen Namen, um diesen Empfänger leichter zu identifizieren.

E-Mail

Geben Sie die E-Mail-Adresse ein, um über die ausgewählten Ereignisse benachrichtigt zu werden. Sie können bis zu zehn E-Mail-Adressen konfigurieren, durch Komma getrennt.

Externen Schlüssel erfordern

Wird diese Option aktiviert, werden E-Mails nur für Sitzungen versandt, die zum Zeitpunkt des Ereignisses über einen externen Schlüssel verfügen.

Zu sendende Ereignisse

Wählen Sie, welche Ereignisse die zu sendenden Meldungen auslösen.

Betreff

Passen Sie den Betreff dieser E-Mail an. Sie können diesen Text für jegliche aktivierten Sprachen lokalisieren.

Text

Passen Sie den Text dieser E-Mail an. Verwenden Sie eines der unten auf der /login-Seite aufgeführten Makros, um den Text für Ihre Zwecke anzupassen.Sie können diesen Text für jegliche aktivierten Sprachen lokalisieren.

Weitere Informationen finden Sie in Referenzhandbuch für ausgehende Ereignisse -- Variablen und Makros unter https://www.beyondtrust.com/docs/remote-support/how-to/integrations/outbound-events/index.htm.

Cluster: Atlas-Technologie für Lastenausgleich konfigurieren

Status

Geographisch großräumige Bereitstellungen profitieren von der BeyondTrust Atlas Cluster-Technologie, die eine einzige BeyondTrust-Site auf mehreren B Series Applianceen erstellt, die Knoten in einem Cluster genannt werden. Am primären B Series Appliance/primären Knoten finden die meisten Verwaltungsarbeiten statt. Der Datenverkehrsknoten ist ein BeyondTrust Appliance B Series-Gerät, das dazu beiträgt, Ihren Support-Verkehr effektiv zu leiten.

Am primären Knoten konfigurieren Sie sowohl den primären Knoten selbst, wie auch die Datenverkehrsknoten.

> *Weitere Informationen über Atlas finden Sie im BeyondTrust Handbuch für Atlas-Technologie auf https://www.beyondtrust.com/docs/remote-support/how-to/atlas.*

Aktueller Status

Bestätigt die Rolle der Site-Instanz, von der aus Sie auf die Seite zugegriffen haben.

Primäre(r) Knoten

Zeigt eine Liste der verfügbaren Hauptknoten an.

Jetzt synchronisieren

Synchronisiert die im Cluster gruppierten B Series Appliance.

Cluster auflösen

Löst den Cluster auf und entfernt damit jedes B Series Appliance aus seiner Rolle im Cluster.

Statusverlauf

Nachrichtenprotokoll der im Cluster gruppierten B Series Appliance anzeigen oder ausblenden.

Datenverkehrsknoten

Methode zur Auswahl der Datenverkehrsknoten

Mit dieser Auswahl wird definiert, wie ein Verkehrsknoten für eine Verbindung mit dem Support-Techniker- bzw. Kunden-Client ausgewählt wird. Für die Definierung dieser Verbindung stehen die Methoden **Zufällig**, **A-Record-Abfrage**, **SRV-Record-Abfrage**, **IP-Anycast** und **Zeitzonenverschiebung** zur Verfügung. Die Wahl der Verbindungsmethode hängt u.a. stark von Ihrer

Netzwerkinfrastruktur ab.

Hinzufügen, Bearbeiten, Entfernen

Erstellen Sie einen neuen Knoten, bearbeiten Sie einen bestehenden Knoten oder entfernen Sie einen bestehenden Knoten.

Neue Client-Verbindungen annehmen

Stellen Sie sicher, dass diese Einstellung aktiviert ist, da Kunden diesen Verkehrsknoten sonst nicht verwenden können.

Datenverkehrsknoten hinzufügen

Neue Client-Verbindungen annehmen

Ist diese Option aktiviert, dürfen neue Client-Verbindungen diesen Knoten nutzen. Wenn Sie neue Client-Verbindungen für diesen Knoten deaktivieren, sind bestehende Client-Verbindungen davon nicht betroffen.

Hinweis: *Wenn diese Einstellung nicht aktiviert ist, können Clients diesen Verkehrsknoten nicht verwenden.*

Name

Erstellen Sie einen eindeutigen Namen, um diesen Knoten leichter zu identifizieren.

Öffentliche Adresse

Geben Sie den Hostnamen ein, den Sie in DNS für diesen Knoten festgelegt haben und geben Sie den Port ein, über den Clients mit dem Knoten kommunizieren.

Zeitzonenverschiebung

Wird nur genutzt, wenn für die **Methode zur Auswahl von Knotenpunkten** die **Zeitzonenverschiebung** aktiviert ist. Bei diesem Prozess müssen die Zeitzoneneinstellungen der Host-Maschine erfasst und diese Einstellung verwendet werden, damit sie mit dem entsprechenden Verkehrsknoten übereinstimmt, der die am ehesten übereinstimmende Zeitzoneneinstellung aufweist. Die Zeitzonenverschiebung ergibt sich aus der Zeitzoneneinstellung des Kunden relativ zur Koordinierten Weltzeit (UTC).

Interne Adresse

Das kann dieselbe sein wie die öffentliche Adresse. Mit erweiterten Konfigurationen können nach Belieben andere Hostnamen für die Kommunikation zwischen Geräten festgelegt werden.

Netzwerkadresspräfixe

Dieses Feld brauchen Sie nicht auszufüllen.

Geben Sie bei erweiterten Konfigurationen die Netzwerkadresspräfixe ein (einen pro Zeile), in der Form **ip.ad.re.sse[/netzmaske]**. Die Netzmaske ist optional und kann entweder in Dezimalschreibweise mit Punkt oder als Ganzzahlbitmaske angegeben werden. Wird die Netzmaske weggelassen, wird von einer einzelnen IP-Adresse ausgegangen.

Wird dieses Feld ausgefüllt, versucht der primäre Knoten, diesem Datenverkehrsknoten einen Client zuzuweisen, wenn die IP-Adresse des Client einem der Netzwerkadresspräfixe entspricht. Wenn die IP-Adresse des Clients mit mehr als einem Netzwerkadresspräfix eines Datenverkehrsknotens übereinstimmt, wird der Client dem Datenverkehrsknoten mit dem längsten übereinstimmenden Präfix zugewiesen. Sind die übereinstimmenden Präfixe gleich lang, wird einer der übereinstimmenden Datenverkehrsknoten zufällig gewählt. Wenn die IP-Adresse des Clients mit keinem der Netzwerkadresspräfixe der Datenverkehrsknoten übereinstimmt, wird der Client mithilfe der konfigurierten Methode zugewiesen.

Konfiguration des primären Knotens

Primärer Knoten

Name

Erstellen Sie einen eindeutigen Namen, um diesen Knoten leichter zu identifizieren.

Öffentliche Adresse

Geben Sie den Hostnamen ein, den Sie in DNS für diesen Knoten festgelegt haben und geben Sie den Port ein, über den Clients mit dem Knoten kommunizieren.

Interne Adresse

Das kann dieselbe sein wie die öffentliche Adresse. Mit erweiterten Konfigurationen können nach Belieben andere Hostnamen für die Kommunikation zwischen Geräten festgelegt werden.

Sicherungskopie des primären Knotens

Die aktuelle Website-Instanz ist die primäre Website-Instanz in einer Failover-Beziehung. Werden die Failover-Rollen vertauscht, wird die Instanz der Sicherungswebsite zum neuen primären Knoten im Cluster. Sie können die Clusterknotenkonfiguration für die Sicherungs-Website-Instanz unten konfigurieren. Die Sicherungs-Website-Instanz wird automatisch aus dem Cluster entfernt, wenn die Failover-Beziehung unterbrochen wird.

Name

Erstellen Sie einen eindeutigen Namen, um diesen Knoten leichter zu identifizieren.

Öffentliche Adresse

Geben Sie den Hostnamen ein, den Sie in DNS für diesen Knoten festgelegt haben und geben Sie den Port ein, über den Clients mit dem Knoten kommunizieren.

Interne Adresse

Das kann dieselbe sein wie die öffentliche Adresse. Mit erweiterten Konfigurationen können nach Belieben andere Hostnamen für die Kommunikation zwischen Geräten festgelegt werden.

Maximale Client-Rückgriffe auf Primärknoten

Ermöglicht, dass die Anzahl der auf Fallback eingestellten Clients wieder den primären Knoten zur Verkehrssteuerung verwenden.

Wenn ein Client nicht in der Lage ist, einen nutzbaren Standarddatenverkehrsknoten zu wählen (wegen temporärer Fehlkonfigurationen, DNS-Probleme, Software-Unstimmigkeiten usw.), muss auf den primären Knoten als Standarddatenverkehrsknoten zurückgegriffen werden. Um zu vermeiden, dass der primäre Knoten mit zu hohem Datenverkehr überlastet wird, kann mit diesem Wert die Anzahl gleichzeitiger Clients begrenzt werden, die auf den primären Knoten in dieser Funktion zurückgreifen.

Failover: Einrichten eines Sicherungs-B Series Appliances für Failover

Verwaltung | FAILOVER

Weitere Informationen finden Sie in Failover-Konfiguration auf https://www.beyondtrust.com/docs/remote-support/how-to/failover/index.htm.

Konfiguration

Failover-Beziehung einrichten

Neue Verbindungsdetails für den Sicherungsdatei-Ordner

Hostname oder IP-Adresse

Geben Sie den Hostnamen oder die IP-Adresse des B Series Appliance ein, das sie als Backup-Gerät in einer Failover-Beziehung verwenden möchten.

Port

Geben Sie den TLS-Port ein, der diesem primären B Series Appliance gestattet, eine Verbindung zum Sicherungs-B Series Appliance herzustellen.

Verbindungsdetails zu dieser primären Website umleiten

Hostname oder IP-Adresse

Geben Sie den Hostnamen oder die IP-Adresse dieses B Series Appliance ein, das Sie als primäres Gerät in einer Failover-Beziehung verwenden möchten.

Port

Geben Sie den TLS-Port ein, der dem Sicherungs-B Series Appliance gestattet, eine Verbindung zu diesem primären B Series Appliance herzustellen.

Status

Status dieses Hosts

Zeigen Sie den Hostnamen dieser Seite an, zusammen mit dem Status der primären Site-Instanz oder Sicherungswebsite-Instanz.

Status des Peer-Hosts

Zeigen Sie den Hostnamen dieser Seite an, zusammen mit dem Status der primären Site-Instanz oder Sicherungswebsite-Instanz. Außerdem können Sie das Datum und den Zeitpunkt der letzten Statusüberprüfung anzeigen.

Statusverlauf

Sie können die Tabelle der erfolgten Statusereignisse erweitern oder einklappen.

Status der primären oder Sicherungssite-Instanz

Der Text bestätigt, dass Sie sich entweder auf der primären oder der Sicherungssite-Instanz für Ihre Host-Site befinden.

Jetzt synchronisieren

Sie können manuell eine Datensynchronisierung zwischen dem primären B Series Appliance und dem Sicherungs-B Series Appliance erzwingen.

Als Sicherungs-/Primärinstanz festlegen

Sie können die Rollen mit dem Peer-B Series Appliance wechseln und damit ein Failover für eine geplante Wartung oder ein bekanntes Failover-Ereignis erzwingen.

Aktivieren Sie diese Option, um eine Datensynchronisierung von der Site-Instanz bei example.com abzurufen und die Site als Sicherungs-/Primärinstanz festzulegen

Wenn Sie vor dem Tauschen der Rollen Daten vom Peer-B Series Appliance synchronisieren wollen, wählen Sie diese Option. Wenn diese Option ausgewählt wird, wird die Verbindung für alle Benutzer auf dem bestehenden primären B Series Appliance während der Datensynchronisierung unterbrochen, und es stehen keine weiteren Vorgänge zur Verfügung, bis der Swap abgeschlossen ist.

Aktivieren Sie dieses Kästchen, um eine Sicherung festzulegen, auch wenn die Peer-Site-Instanz unter example.com nicht kontaktiert werden konnte

Auf der primären Site-Instanz haben Sie die Option, diese als Sicherung festzulegen, auch wenn das Peer-B Series Appliance nicht kontaktiert werden kann. Wenn diese Option nicht aktiviert wird, wird der Failover abgebrochen, wenn beide B Series Appliancee hinsichtlich ihrer Failover-Rollen (ein Primär- und ein Sicherungsgerät) nicht synchronisiert bleiben können.

Wenn Sie beispielsweise wissen, dass das aktuelle Sicherungs-B Series Appliance online ist, aber vom Primärgerät aufgrund eines Netzwerkproblems nicht kontaktiert werden kann, können Sie diese Option aktivieren, um das Primärgerät als Sicherungsgerät festzulegen, bevor die Netzwerkverbindung wiederhergestellt wird. In diesem Beispiel müssten Sie dann auch auf das aktuelle Sicherheitsgerät zugreifen und dieses als Primärgerät festlegen.

Failover-Beziehungen aufheben

Unterbricht die Failover-Beziehung, wodurch jedes B Series Appliance seine Rolle als Primär- oder Sicherungsgerät verliert.

Konfiguration der Primär- oder Sicherungssite-Instanz

Freigegebene IPs

Steuern Sie die freigegebene IP-Adresse, die die Site-Instanz im Fall eines Failovers verwendet, indem Sie das Kontrollkästchen für die Failover-IP-Adresse auswählen. Wenn Sie die Beziehung zwischen den Sites ändern, werden die markierten IP-Adressen deaktiviert, wenn eine primäre Site zur Sicherungswebsite wird, und werden aktiviert, wenn eine Sicherungssite zur primären Site wird. Sie sollten die Einstellung auf der Peer-Site manuell widerspiegeln, da die Einstellung nicht freigegeben wird.

Sicherungseinstellungen

Die hier konfigurierten Einstellungen werden nur dann aktiviert, wenn die Site-Instanz, die Sie konfigurieren, eine Sicherungsrolle ausübt.

Wenn Sie sich auf der primären Site-Instanz befinden, wählen Sie **Sicherungseinstellungen**, um die Seite mit den Konfigurationsfeldern anzuzeigen oder auszublenden.

Sicherungsvorgänge aktivieren

Website-Sicherungskopien aktivieren oder deaktivieren.

Timeout der primären Site-Instanz

Legen Sie fest, wie lange die primäre Site unerreichbar sein muss, bevor ein Failover stattfindet.

Intervall für automatische Datensynchronisierung

Sie können die Timing-Details des Intervalls für automatische Datensynchronisierung steuern.

Bandbreitengrenzwert für Datensynchronisierung

Legen Sie die Bandbreitenparameter für die Datensynchronisierung fest.

Automatischen Failover aktivieren

Zum schnellen Aktivieren oder Deaktivieren des automatischen Failover.

Netzwerkkonnektivitäts-Test-IPs

Geben Sie die IP-Adressen für die zu prüfende Sicherungswebsite ein, um zu bestimmen, ob die primäre Site von der Sicherungskopie nicht erreicht werden kann, weil die primäre Site offline ist oder weil keine Netzwerkverbindung zur Backup-Site besteht.

API-Konfiguration: Aktivieren Sie die XML API und konfigurieren Sie benutzerdefinierte Felder

Verwaltung | API-KONFIGURATION

API-Konfiguration

XML-API aktivieren

Sie können die BeyondTrust XML-API aktivieren, sodass Sie Berichte ausführen und Befehle ausgeben können, wie z. B. Start oder Übertragung von externen Anwendungen, sowie die automatische Sicherung Ihrer Softwarekonfiguration.

***Hinweis:** Nur die Aufrufe **Befehl**, **Berichte** und **Client-Skripting-API** werden durch diese Einstellung aktiviert/deaktiviert. Andere API-Aufrufe werden unter **Öffentliche Portale** konfiguriert.*

Weitere Informationen finden Sie im API-Programmierhandbuch unter www.beyondtrust.com/docs/remote-support/how-to/integrations/api.

CLI-Client-Download

Das Tool Befehlszeilenschnittstelle (CLI - Command Line Interface) kann heruntergeladen werden, um die Verwendung und Konfiguration von APIs und Automatisierungsskripten zu erleichtern und sie in Ihre BeyondTrust Remote Support Installation zu integrieren. Das CLI-Tool ist für die Plattformen Windows (x64), macOS und Linux (x64) verfügbar. Wählen Sie die entsprechende Plattform und klicken Sie auf **BTAPI CLI Client herunterladen**.

Der Download ist eine komprimierte ausführbare Datei. Extrahieren Sie die Datei, und speichern oder verknüpfen Sie sie in einem ausführbaren Bereich (in Ihrem PATH).

- Für Windowssysteme: Öffnen Sie die Datei in einem Terminal wie Windows Command Prompt oder Windows PowerShell.
- Für macOS-Systeme: Führen Sie die Datei im Terminal aus.

Die Hilfeinformationen, einschließlich Optionen, Befehle und variable Anweisungen, werden beim Öffnen des Programms angezeigt.

Archiv-API aktivieren

Wählen Sie, ob Sie die Status-Archiv-API aktivieren möchten, um Protokolle des Status des B Series Appliance und von Ereignissen bestimmter Tage herunterzuladen.

API-Konten

Ein API-Konto speichert alle Authentifizierungs- und Autorisierungseinstellungen für den API-Klienten. Mindestens ein API-Konto ist erforderlich, um die API zu verwenden, entweder zusammen mit dem Integrations-Client, mit einer Drittanbieter-App oder mit Ihrer intern

entwickelten Software.

Hinzufügen, Bearbeiten, Löschen

Erstellen Sie ein neues Konto, bearbeiten Sie ein bestehendes Konto oder entfernen Sie ein bestehendes Konto.

Ein API-Konto hinzufügen oder bearbeiten

Aktiviert

Falls aktiviert, ist dieses Konto zur API-Authentifizierung berechtigt. Wenn ein Konto deaktiviert ist, werden alle mit dem Konto verknüpften OAuth-Tokens sofort deaktiviert.

Name

Erstellen Sie einen eindeutigen Namen, um dieses Konto leichter zu identifizieren.

OAuth Client-ID

Die OAuth Client-ID und das Client-Secret werden zur Erstellung von OAuth-Tokens verwendet, die für die API-Authentifizierung benötigt werden.

Die OAuth Client-ID ist eine eindeutige ID, die vom B Series Appliance generiert wird. Sie kann nicht geändert werden. Die Client-ID wird als öffentliche Information erachtet und kann daher frei weitergegeben werden, ohne die Integrationssicherheit zu gefährden.

Kommentare

Fügen Sie Kommentare hinzu, die den Zweck dieses Kontos identifizieren.

OAuth Client-Secret

Das OAuth-Client-Secret wird vom B Series Appliance mithilfe eines kryptografisch sicheren, pseudo-zufälligen Zahlengenerators generiert.

> ***Hinweis:*** *Das Client-Secret kann nicht modifiziert werden. Sie können es auf der Seite* ***Bearbeiten*** *jedoch neu erzeugen. Wird ein Client-Secret neu erzeugt und das Konto dann gespeichert, werden sofort sämtliche mit dem Konto verknüpften OAuth-Tokens ungültig. Sämtliche API-Aufrufe unter Verwendung dieser Tokens können nicht mehr auf die API zugreifen.*

Berechtigungen

Wählen Sie die API-Bereiche, die dieses Konto verwenden können soll.

Befehls-API

Wählen Sie für die Befehls-API, ob der Zugriff verweigert, nur schreibgeschützt oder vollständig gewährt werden soll.

Berichts-API

Legen Sie für die Berichts-API fest, ob dieses Konto Zugriff auf Support-Sitzungsberichte und Aufzeichnungen, Präsentationssitzungsberichte und Aufzeichnungen, Lizenznutzungsberichte, Archivberichte und Vaultkonto-Aktivitätsberichte hat.

Sicherungs-API

Legen Sie fest, ob dieses Konto die Sicherungs-API verwenden kann.

API-Konfiguration

Legen Sie fest, ob dieses Konto die Konfigurations-API verwenden kann und ob es in diesem Fall Vaultkonten verwalten kann.

Echtzeit-Status-API

Legen Sie fest, ob dieses Konto die Echtzeit-Status-API verwenden kann.

Endpunkt-Anmeldedaten-Manager-API

Legen Sie fest, ob dieses Konto die Endpunkt-Anmeldedaten-Manager-API verwenden kann.

Netzwerkbeschränkungen

Listet Netzwerkadresspräfixe auf, über die sich dieses Konto authentifizieren kann.

> ***Hinweis:*** *API-Konten sind nicht durch die unter* ***/login > Verwaltung > Sicherheit*** *konfigurierten Präfixe beschränkt. Sie sind nur durch die für das API-Konto konfigurierten Netzwerkpräfixe beschränkt.*

Netzwerkadressen-Zulassungsliste

Geben Sie die Netzwerkadressen ein, die Sie auf die Zulassungsliste setzen möchten.

Support: Kontakt mit BeyondTrust Technical Support

Verwaltung | SUPPORT

BeyondTrust - Support-Kontaktinformationen

Die Support-Seite enthält Kontaktinformationen, falls Sie mit einem BeyondTrust Technical Support-Techniker in Verbindung treten müssen.

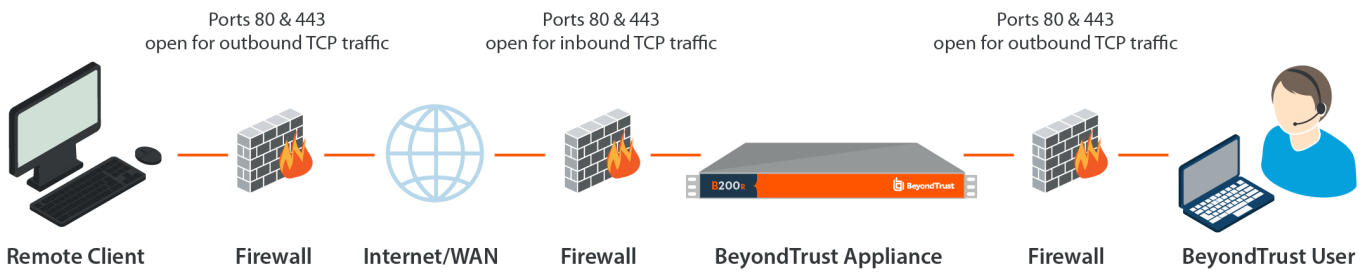
Erweiterter technischer Support von BeyondTrust

Muss ein BeyondTrust Technical Support-Support-Techniker auf Ihr B Series Appliance zugreifen, stellt er Ihnen Support-, Zugriffs- und Übersteuerungscodes bereit, die Sie auf dieser Seite eingeben, um einen geräteseitig initiierten, voll verschlüsselten Support-Tunnel zurück zu BeyondTrust zu erstellen und komplexe Probleme schnell zu beheben.

Ports und Firewalls

BeyondTrust-Lösungen funktionieren transparent durch Firewalls, sodass eine Verbindung mit einem beliebigen Computer mit Internetkonnektivität weltweit hergestellt werden kann. Bei bestimmten, stark gesicherten Netzwerken sind aber unter Umständen einige Konfigurationsschritte erforderlich.

TYPICAL NETWORK SETUP



- Die Ports 80 und 443 müssen für ausgehenden TCP-Verkehr an der Firewall des Remote-Systems und an der des lokalen Benutzers offen sein. Mehr Ports stehen möglicherweise abhängig von Ihrer Konfiguration zur Verfügung. Das Diagramm zeigt eine typische Netzwerkkonfiguration. Weitere Informationen finden Sie im BeyondTrust Appliance B SeriesHardware-Installationsleitfaden.
- Internetsicherheits-Software wie Software-Firewalls darf den Download von ausführbaren BeyondTrust-Dateien nicht blockieren. Einige Beispiele für Software-Firewalls sind McAfee Security, Norton Security und Zone Alarm. Falls Sie eine Software-Firewall verwenden, kann es zu Verbindungsproblemen kommen. Um diese zu vermeiden, konfigurieren Sie Ihre Firewall so, dass die folgenden ausführbaren Dateien zugelassen werden, wobei {uid} ein Platzhalter für eine eindeutige Kennung ist, die aus Buchstaben und Zahlen besteht:
    - bomgar-scc-{uid}.exe
    - bomgar-scc.exe
    - bomgar-pac-{uid}.exe
    - bomgar-pac.exe

  Unterstützung für die Konfiguration der Firewall erhalten Sie beim Hersteller der Firewall-Software.
- Beispielhafte Firewall-Regeln basierend auf dem B Series Applianceestandort finden Sie auf www.beyondtrust.com/docs/remote-support/getting-started/deployment/dmz/firewall-rules.htm.

Wenn weiterhin Probleme beim Herstellen einer Verbindung auftreten, wenden Sie sich an den BeyondTrust Technical Support unter www.beyondtrust.com/support.

Haftungsausschlüsse, Lizenzierungsbeschränkungen und Technischer Support

Haftungsausschlüsse

Dieses Dokument dient ausschließlich Informationszwecken. BeyondTrust Corporation kann den Inhalt ohne Vorankündigung ändern. Es kann weder die Fehlerfreiheit dieses Dokuments garantiert werden, noch unterliegt das Dokument irgendwelchen Garantien oder Gewährleistungen, weder in mündlicher Form noch in konkludenter rechtlicher Form, einschließlich konkludenten Garantien und Gewährleistungen der Marktgängigkeit oder Eignung für einen bestimmten Zweck. Insbesondere lehnt BeyondTrust Corporation jedwede Haftung für den Inhalt des vorliegenden Dokuments ab, und durch dieses Dokument entstehen weder direkt noch indirekt irgendwelche vertraglichen Pflichten. Die hierin beschriebenen Technologien, Funktionen, Dienste und Prozesse können ohne Ankündigung geändert werden.

Alle Rechte vorbehalten. Andere Markenzeichen auf dieser Seite sind Eigentum der jeweiligen Inhaber. BeyondTrust ist keine gecharterte Bank oder Treuhandgesellschaft oder Hinterlegungsstelle. Sie ist nicht befugt, Geldeinlagen oder Treuhandkonten anzunehmen, und wird nicht von einem Staat oder einer Bundesbankbehörde lizensiert oder reguliert.

Lizenzierungsbeschränkungen

Mit einer BeyondTrust Remote Support-Lizenz kann jeweils ein Support-Techniker Probleme auf einer unbegrenzten Anzahl an Remote-Computern beheben. Dabei müssen die Benutzer nicht unbedingt am Computer sein. Obgleich mehrere Konten für die gleiche Lizenz eingerichtet sein können, sind zwei oder mehr Lizenzen (eine pro aktivem Support-Techniker) erforderlich, damit mehrere Support-Techniker gleichzeitig den Fehler beheben können.

Technischer Support

Wir bei BeyondTrust fühlen uns verpflichtet, Service von höchster Qualität zu bieten, indem wir gewährleisten, dass unsere Kunden alles haben, was sie für einen Betrieb bei maximaler Produktivität benötigen. Sollten Sie Hilfe benötigen, wenden Sie sich bitte an www.beyondtrust.com/support.

Technischen Support können Sie mit einem jährlichen Abonnement unseres Wartungsplans in Anspruch nehmen.