Privileged Remote Access 23.2
Administratorhandbuch

TC:12/12/2023

Inhaltsverzeichnis

BeyondTrust Privileged Remote Access Admin-Schnittstelle **5**

Anmeldung in der PRA Verwaltungsschnittstelle 6

Suche /login Verwaltungsschnittstelle 8

Benutzer-Menü 9

Status 10

Informationen: Privileged Remote Access Website-Status and Softwaredetails anzeigen 10

Benutzer: Anzeige angemeldeter Benutzer und Senden von Nachrichten 12

Neues: Siehe Privileged Remote Access-Softwareversionsdetails 12

Konsolen & Downloads: Starten Sie die Web-Zugriffskonsole und laden Sie die Desktop-Zugriffskonsole herunter 14

Konsolen & Downloads: Treiber herunterladen 15

Eigenes Konto: E-Mail-Einstellungen und erweiterter Verfügbarkeitsmodus 16

Eigenes Konto: Passworteinstellungen ändern und passwortlose Authentifizierung hinzufügen 17

Konfiguration 20

Optionen: Verwalten von Verbindungsoptionen, Aufzeichnen von Sitzungen, Beschleunigen von Sitzungen 20

Teams: Gruppieren von Benutzern in Teams 23

Benutzerdefinierte Felder: Benutzerdefinierte API-Felder erstellen, bearbeiten und löschen 25

Jump 27

Jump-Clients: Verwalten von Einstellungen und Installieren von Jump Clients für den Endpunktzugriff 27

Jump-Gruppen: Konfiguration, welche Benutzer auf welche Jump-Elemente zugreifen können 34

Jump-Richtlinien: Zeitpläne, Benachrichtigungen und Genehmigungen für Jump-Elemente festlegen 36

Jump-Element-Rollen: Erstellen von Berechtigungssätzen für Jump-Elemente 40

Jumpoint: Einrichten des unüberwachten Zugriffs auf ein Netzwerk 43

Jump-Elemente: Massenimport von symbolischen Jump-Links und Verwalten der Jump-Element-Einstellungen 46

Vault für Privileged Remote Access 56

Konten: Vault-Konten verwalten 56

Kontogruppen: Kontogruppen hinzufügen und verwalten 67

Kontenrichtlinien: Kontogruppen hinzufügen und verwalten 70
Endpunkte: Erfasste Systeme anzeigen und verwalten 72
Dienste: Erkannte Dienste anzeigen und verwalten 73
Domänen: Hinzufügen und Verwalten von Domänen 73
Discovery: Konten, Endpunkte und Dienste in einer Domain erfassen 75
Optionen: Konfigurieren der globalen Standard-Kontorichtlinieneinstellungen und der Passwortlänge für die Kontorotation 79
Zugriffskonsole 81
Einstellungen für Zugriffskonsole: Standardmäßige Einstellungen für die Konsole verwalten 81
Benutzerdefinierte Links: Hinzufügen von URL-Verknüpfungen zur Zugriffskonsole 84
Vordefinierte Skripts: Skripte für Bildschirmfreigabe- oder Befehlsshell-Sitzungen erstellen 85
Spezielle Aktionen: Erstellen von benutzerdefinierten speziellen Aktionen 87
Benutzer und Sicherheit 89
Benutzer: Kontoberechtigungen für einen Benutzer oder Administrator hinzufügen 89
Benutzerkonten für Passwortrücksetzung: Benutzern das Festlegen von Passwörtern erlauben 100
Zugriffseinladung: Erstellen Sie Profile, um externe Benutzer zu Sitzungen einzuladen 102
Sicherheitsanbieter: Aktivieren von LDAP-, RADIUS-, Kerberos-, SCIM- und SAML2-Anmeldungen 103
Anbietergruppen 119
Sitzungsrichtlinien: Sitzungsberechtigungen und Aufforderungsregeln festlegen 123
Gruppenrichtlinien: Benutzerberechtigungen auf Benutzergruppen anwenden 130
Kerberos-Keytab: Kerberos-Keytab verwalten 143
Berichte 144
Zugriff: Berichte zu Sitzungsaktivitäten 144
Vault: Bericht zum Vault-Konto und zur Benutzeraktivität 146
Anbieter: Bericht zu Anbieter-Konten und zur Benutzeraktivität 148
Jump-Item: Bericht über Jump-Item-Aktivität 148
Syslog: Bericht mit allen Syslog-Dateien auf dem Gerät herunterladen 150
Compliance: Privileged Remote Access Daten anonymisieren zur Erfüllung von Compliance-Standards 150
Sprachen: Verwalten der installierten Sprachen 153
Sprachen: Verwalten der installierten Sprachen 154

Verwaltung 156
Software: Laden Sie ein Backup herunter, nehmen Sie ein Software-Upgrade vor 156
Sicherheit: Verwalten der Sicherheitseinstellungen 159
Website-Konfiguration: HTTP-Ports festlegen, Erforderliche Anmeldungsvereinbarung aktivieren 166
E-Mail-Konfiguration: Konfigurieren der Software für das Versenden von E-Mails 167
Ausgehende Ereignisse: Ereignisse für die Auslösung von Nachrichten festlegen 174
Cluster: Atlas-Cluster-Technologie für Lastenausgleich konfigurieren 177
Failover: Einrichten eines Sicherungs-B Series Appliances für Failover 179
API-Konfiguration: Aktivieren Sie die XML API und konfigurieren Sie benutzerdefinierte Felder 183
Support: Kontakt mit BeyondTrust Technical Support 185
Ports und Firewalls 187
Haftungsausschlüsse, Lizenzierungsbeschränkungen und Technischer Support 188

BeyondTrust Privileged Remote Access Admin-Schnittstelle

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 zugriffskonsole herunterzuladen.

Verwenden Sie dieses Handbuch erst, wenn die anfängliche Einrichtung und Konfiguration des B Series Appliance durch einen Administrator abgeschlossen wurde, entsprechend der Beschreibung im BeyondTrust Appliance B Series-Installationshandbuch für Gerätehardwareunter www.beyondtrust.com/docs/privileged-remote-access/getting-started/deployment/hardware-sra/. Ist BeyondTrust korrekt installiert, können Sie sofort mit dem Zugriff auf Ihre Endpunkte beginnen. Sollten Sie Hilfe benötigen, wenden Sie sich bitte an BeyondTrust Technical Support unter www.beyondtrust.com/support.

Anmeldung in der PRA 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 Primärdomäne Ihres Unternehmens, z. B. **access.example.com/login**.

Standardbenutzername: **admin**

Standardpasswort: **password**

> ***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 finden Sie unter Anmelden in der PRA-Zugriffskonsole unter https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/login-to-the-access-console.htm.*

Passwortlose Anmeldung

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

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

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

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.

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 Privileged Remote Access /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.*

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

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

Starten Zugriffskonsole für Privileged Web Access: Damit haben Sie bequemen Zugriff auf die Web-Konsole von überall in /login.

Herunterladen Zugriffskonsole: Hier finden Sie einen schnellen Link zum Herunterladen der zugriffskonsole.

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

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 Zugriffskonsole für Privileged Web Access 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:

- *„E-Mail-Einstellungen ändern“ auf Seite 16*
- *„Das Passwort ändern“ auf Seite 17*

Status

Informationen: Privileged Remote Access Website-Status and Softwaredetails anzeigen

Status | INFORMATIONEN

Website-Status

Die Hauptseite der BeyondTrust Privileged Remote Access-/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.

Neustart der Privileged Remote Access-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.

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 der gestatteten Jump-Clients

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

Maximale Anzahl an gleichzeitigen Benutzern

Sehen Sie sich die maximale Anzahl der gleichzeitigen Benutzer an, die auf Ihrem System gestattet sind. Wenn Sie mehr Benutzer benötigen, kontaktieren Sie den technischen Support von BeyondTrust.

Endpunktlizenzen

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

Konfigurierte Endpunkte

Sehen Sie sich die Anzahl der Endpunkte an, die aktuell auf Ihrem System konfiguriert sind.

Lizenznutzungsbericht herunterladen

Laden Sie eine ZIP-Datei mit detaillierten Informationen (nur Englisch) zu Ihrer BeyondTrust-Lizenznutzung herunter. Diese Datei enthält eine Liste aller Jump-Elemente (ausschließlich deinstallierter Jump-Clients), tägliche Statistiken für Jump-Element-Vorgänge und die Lizenznutzung und eine Zusammenfassung des B Series Appliance mit seinem Endpunktlizenzverbrauch.

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 vorbereiten kann.

Verbundene Clients

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

Weitere Informationen zum BeyondTrust Appliance B Series finden Sie unter B Series Appliance Übersicht unter https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/deployment/index.htm.

ECM-Clients

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

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

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

Weitere Informationen finden Sie unter Anmelden an Endpunkten mit Anmeldedaten-Einfügung unter https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/web-access/credential-injection.htm.

Benutzer: Anzeige angemeldeter Benutzer und Senden von Nachrichten

Status	BENUTZER

Angemeldete Benutzer

Zeigen Sie eine Liste der in der zugriffskonsole angemeldeten Benutzer an, sowie deren Anmeldezeit und ob sie Support- oder Präsentationssitzungen abhalten.

Beenden

Sie können die Verbindung eines Benutzers auf die zugriffskonsole beenden.

Nachricht an Benutzer senden

Senden Sie über ein Pop-up-Fenster in der zugriffskonsole eine Nachricht an alle angemeldeten Benutzer.

Nutzer der erweiterten Verfügbarkeit

Sie können Benutzer anzeigen, für die der erweiterte Verfügbarkeitsmodus aktiviert wurde.

Deaktivieren

Sie können die erweiterte Verfügbarkeit eines Benutzers deaktivieren.

Neues: Siehe Privileged Remote Access-Softwareversionsdetails

Status	NEUES

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 einer BeyondTrust-Software-Aktualisierung 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 zugriffskonsole auch Benutzern zur Verfügung.

Weitere Informationen finden Sie unter Dokumentation zur Aktualisierung von BeyondTrust Privileged Remote Access unter https://www.beyondtrust.com/docs/privileged-remote-access/updates/index.htm..

Konsolen & Downloads: Starten Sie die Web-Zugriffskonsole und laden Sie die Desktop-Zugriffskonsole herunter

Konsolen & Downloads | ZUGRIFFSKONSOLE

BeyondTrust-Zugriffskonsole für Privileged Web Access

Starten Sie die Zugriffskonsole für Privileged Web Access, eine webbasierte zugriffskonsole. Greifen Sie über Ihren Browser auf Remote-Systeme zu, ohne die volle zugriffskonsole herunterladen und installieren zu müssen.

BeyondTrust Zugriffskonsole

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 Zugriffskonsole für Privileged Web Access-Handbuch unter https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/web-access/index.htm.*

BeyondTrust Zugriffskonsole herunterladen

Laden Sie das BeyondTrust zugriffskonsole-Installationsprogramm herunter.

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**. Wenn Sie **1** eingeben, wird die Konsole für alle Benutzer auf dem Computer installiert. Ansonsten wird sie nur für den aktuellen Benutzer installiert.
- **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.

Konsolen & Downloads: Treiber herunterladen

Konsolen & Downloads | TREIBER

Remote Desktop Agent

Installationsprogramm für den Remote Desktop Agent herunterladen

Zum Herunterladen anklicken. Installieren Sie den Remote Desktop Agent auf 64-Bit-Windows-Servern mit Remote-Desktop-Diensten, um vom Administrator definierte Anwendungen zu starten und Anmeldedaten einzugeben.

Virtual Smart Card

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.

Für eine Authentifizierung mithilfe einer virtuellen Smart-Card benötigt der BeyondTrust-Benutzer den BeyondTrust-Treiber für die virtuelle Smart-Card. Der Computer, auf den zugegriffen wird, muss im heraufgesetzten Modus betrieben werden. Es muss außerdem entweder der BeyondTrust Virtual Smart-Card-Treiber für Endpunkte installiert sein, oder es muss über die Jump-zu-Funktion der zugriffskonsole auf das System zugegriffen werden.

> *Weitere Details und Anforderungen finden Sie im Dokument Smart-Cards für die Remote-Authentifizierung unter https://www.beyondtrust.com/docs/privileged-remote-access/how-to/smart-card/index.htm.*

Windows-Architektur auswählen

Wählen Sie das entsprechende Installationsprogramm der Virtual Smart-Card für das System des BeyondTrust-Benutzers oder für das Endpunkt-System.

Installationsprogramm für Virtual Smart-Card herunterladen

Klicken Sie zum Herunterladen des Installationsprogramms für die Virtual Smart-Card entsprechend Ihrer obigen Auswahl.

Eigenes Konto: E-Mail-Einstellungen und erweiterter Verfügbarkeitsmodus

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

Zeigt die aktuelle Sprache an. Wenn mehr als eine Sprache für Ihre Website aktiviert ist, wählen Sie die gewünschte Sprache aus dem Dropdown-Menü.

Passwort

Geben Sie das Passwort für Ihr /login-Konto, nicht Ihr E-Mail-Passwort, ein. Das Passwort ist erforderlich, um Ihre Identität zu bestätigen, bevor Sie Ihre E-Mail-Einstellungen ändern können.

> ***Hinweis:*** *Um Ihr Passwort zu ändern, lesen Sie bitte „Das Passwort ändern“ auf Seite 17.*

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.

Eigenes Konto: Passworteinstellungen ändern und passwortlose Authentifizierung hinzufügen

Eigenes Konto | SICHERHEIT

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 Authentifizierer können für die sichere Anmeldung ohne Eingabe Ihres Passworts auf der Desktop-zugriffskonsole (nur Windows), Zugriffskonsole für Privileged Web Access 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-zugriffskonsole (nur Windows), Zugriffskonsole für Privileged Web Access 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 auf dem Desktop-zugriffskonsole (nur Windows), Zugriffskonsole für Privileged Web Access 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 Privileged Remote Access **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 zugriffskonsole 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.*

Konfiguration

Optionen: Verwalten von Verbindungsoptionen, Aufzeichnen von Sitzungen, Beschleunigen von Sitzungen

Konfiguration | OPTIONEN

Sitzungsoptionen

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.

Verbindungsoptionen

Zeitüberschreitung bei der Neuverbindung

Legen Sie fest, wie lange ein getrennter Endpunkt-Client versuchen soll, die Verbindung wiederherzustellen.

Schränkt den physischen Zugriff auf den Endpunkt ein, wenn die Verbindung des Endpunkts unterbrochen wird, oder wenn die Verbindung aller an der Sitzung teilnehmenden Benutzer 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.

Protokolloptionen für Zugriffssitzung

Aktivieren der Bildschirmfreigabe-Aufzeichnung

Wählen Sie, ob Bildschirmfreigabe-Sitzungen automatisch als Videos aufgezeichnet werden sollen.

Auflösung für Bildschirmfreigabe-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.*

Benutzeraufzeichnung für Protokoll-Tunnel-Jump aktivieren

Wählen Sie, ob Protokoll-Tunnel-Jump-Sitzungen automatisch als Videos aufgezeichnet werden sollen. Da Protokoll-Tunnel-Jumps die Verwendung einer Drittanbieteranwendung erfordern, wird der gesamte Benutzer-Desktop einschließlich aller Anzeigen aufgezeichnet.

Auflösung für Benutzeraufzeichnung

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.*

Vor Aufzeichnungsbeginn Benutzereinwilligung einholen

Wählen Sie, ob Benutzer beim Start einer Protokoll-Tunnel-Jump-Sitzung eine Aufforderung sehen sollen, die sie darüber informiert, dass der Desktop aufgezeichnet wird. Bitte beachten Sie, dass die Protokoll-Tunnel-Jump-Sitzung nicht fortgesetzt wird, wenn der Benutzer nicht einwilligt.

Aktivieren der Befehlsshell-Aufzeichnung

Wählen Sie, ob Befehlsshell-Sitzungen automatisch als Videos aufgezeichnet werden sollen. Mit dem Aktivieren von Befehlsshell-Aufzeichnungen aktivieren Sie auch die Verfügbarkeit von Befehlsshell-Aufzeichnungen als Text-Abschriften.

Auflösung der 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.*

WICHTIG!

Die auf dieser Seite aktivierten Aufzeichnungseinstellungen können über eine Jump-Richtlinie übersteuert werden, bei der ***Sitzungsaufzeichnungen deaktivieren*** *gewählt wurde. Diese Einstellung wirkt sich auf Bildschirmfreigabe-, Protokoll-Tunnel-Jump- und Befehlsshell-Aufzeichnungen aus.*

Automatische Protokollierung von Systeminformationen aktivieren

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

Sitzungsforensik aktivieren

Wählen Sie, ob Sie die zusätzliche Möglichkeit wünschen, in allen Sitzungen basierend auf Sitzungsereignissen suchen zu können. Dazu gehören Chatnachrichten, Dateitransfers, Registrierungseditor-Ereignisse und Wechsel des im Vordergrund befindlichen Fensters in Sitzungen. Diese Funktion ist standardmäßig aktiviert.

Hinweis: *Wurde Befehlsshell aktiviert, ermöglicht Ihnen die Sitzungsforensik eine tiefgreifende Suche in Befehlsshell-Aufzeichnungen. Wenn Sie nach einem Schlüsselbegriff suchen und in einer gespeicherten Befehlsshell-Aufzeichnung ein Treffer gefunden wird, wird die Wiedergabeposition automatisch an den jeweiligen Zeitpunkt in der Aufzeichnung gesetzt. Befehlsausgaben und Kennwörter werden nicht aufgezeichnet.*

Peer-to-Peer-Optionen

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

Deaktiviert

Dies ist die Standardeinstellung. 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 Befehlsshell erkannt, wird versucht, eine Peer-to-Peer-Verbindung aufzubauen. Falls erfolgreich, baut dies eine direkte Verbindung zwischen dem Benutzer 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.

Verwenden des gehosteten BeyondTrust Peer-to-Peer-Servers

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.

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. Weitere Firewall-Einstellungen sind erforderlich.

Weitere Informationen finden Sie in BeyondTrust Appliance B Series Verwaltung: Einschränken von Konten, Netzwerken und Ports, Aktivieren eines STUN-Servers, Einrichten von Syslog, Aktivieren der Anmeldungsvereinbarung, Zurücksetzen des Administratorkontos unter https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/deployment/web/security-appliance-administration.htm.

Zugriffsportal-Logo

Administratoren können ein benutzerdefiniertes Logo hochladen, das auf öffentlichen Websites angezeigt wird. Damit können externe Benutzer sicherstellen, dass sie sich auf der Website Ihres Unternehmens befinden. Darüber hinaus ergänzen sie das Zugriffsportal mit dem Branding Ihres Unternehmens.

Das Logobild wird auf folgenden öffentlichen Webseiten angezeigt:

- Download-Seite der Zugriffseinladung (die Seite, die nach dem Klick auf den Link in einer Zugriffseinladungs-E-Mail angezeigt wird)
- Öffentliche Aufzeichnungs-URLs (Anzeige und Download)
- Antworten zur erweiterten Verfügbarkeit (die Seite, die nach dem Klick auf den Link in einer Einladungs-E-Mail zur erweiterten Verfügbarkeit angezeigt wird)
- Jump-Genehmigungsautorisierungen (die Seite, die nach dem Klick auf einen Link in einer Jump-Genehmigungs-E-Mail angezeigt wird)

Hinweis: *Hochgeladene Logo-Bilddateien können in jedem üblichen Bildformat gespeichert werden. Die logische maximale Bildgröße ist 250 Pixel breit und 64 Pixel hoch. BeyondTrust unterstützt jedoch HD-Displays, die eine maximale physische Größe von 500 Pixeln breit und 128 Pixeln hoch ermöglichen.*

Teams: Gruppieren von Benutzern in Teams

Konfiguration | TEAMS

Teams verwalten

Das Gruppieren von Benutzern in Teams fördert die Effizienz, indem Hierarchien innerhalb von Benutzergruppen geschaffen werden. In der zugriffskonsole erscheint jedes Team als separate Warteschlange für Sitzungen.

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 eines 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, erstellt PRA automatisch einen.

Kommentare

Fügen Sie Kommentare hinzu, die den Zweck dieses Objekts deutlich machen.

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.

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 zugriffskonsole eine wichtige Rolle.

Zeigen Sie in der folgenden Tabelle bestehende Teammitglieder an. Sie können die Ansicht filtern, indem Sie den Namen eines Benutzers in das Filterfeld eingeben. Sie können auch Mitgliederrollen 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:*** *Womöglich können Sie manche Teammitglieder nicht bearbeiten oder löschen. 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 Gruppenrichtlinie angewandt.*
>
> *Sie können auch eine Person zu einem Team hinzufügen und andernorts definierte Einstellungen übersteuern.*

Dashboard-Einstellungen

In einem Team kann ein Benutzer nur andere Benutzer mit Rollen überwachen, die seiner untergeordnet sind. 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 die Einstellung zum Überwachen **Deaktivieren** oder auf **Nur Zugriffskonsole** beschränken, um einem Teamleiter oder -Manager die Berechtigung zu erteilen, die zugriffskonsole eines Teammitglieds zu überwachen. Die Überwachung betrifft Teamführer und Manager aller Teams.

Sitzungsbeitritt und -übernahme in Dashboard aktivieren

Ist diese Option aktiviert, kann ein Teamleiter die Sitzungen eines Teammitglieds übernehmen oder diesen beitreten. 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.

Team-Chat-Verlauf

Wiederholung des Team-Chatverlaufs aktivieren

Wenn diese Option aktiviert ist, bleiben Chat-Nachrichten an alle im Bereich **Team-Chat** der Zugangskonsole zwischen den Anmeldungen an der Zugangskonsole 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.*

Benutzerdefinierte Felder: Benutzerdefinierte API-Felder erstellen, bearbeiten und löschen

Konfiguration	BENUTZERDEFINIERTE FELDER

Erstellen Sie benutzerdefinierte API-Felder, um Informationen über Ihren Kunden zu sammeln. So können Sie BeyondTrust tiefer mit ihren bestehenden Programmen integrieren. Benutzerdefinierte Felder müssen zusammen mit der BeyondTrust API verwendet werden. Erstellen Sie ein neues Feld, modifizieren Sie ein bestehendes Feld oder entfernen Sie ein bestehendes Feld.

Benutzerdefinierte API-Felder hinzufügen oder bearbeiten

Anzeigename

Erstellen Sie einen eindeutigen Namen, um dieses benutzerdefinierte Feld leichter zu identifizieren. Dieser Name wird in der zugriffskonsole als Teil der Sitzungsdetails angezeigt.

Codename

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

In Zugriffskonsole anzeigen

Wenn Sie **In Zugriffskonsole anzeigen** aktivieren, werden dieses Feld und seine Werte sichtbar, wo immer benutzerdefinierte Sitzungsdetails in der zugriffskonsole angezeigt werden.

Jump

Jump-Clients: Verwalten von Einstellungen und Installieren von Jump Clients für den Endpunktzugriff

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 Privileged Remote Access-Handbuch für Jump-Clients: Unüberwachter Zugriff auf Systeme in einem beliebigen Netzwerk unter https://www.beyondtrust.com/docs/privileged-remote-access/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 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.

Name

Geben Sie einen Namen für den Jump Client ein.

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

Jump-Richtlinie

Wählen Sie eine Jump-Richtlinie, die diesem Jump Client zugewiesen werden soll. Jump-Richtlinien werden auf der Seite **Jump > Jump-Richtlinien** konfiguriert und bestimmen die Zeiten, während denen ein Benutzer Zugriff auf diesen Jump-Client hat. Eine Jump-Richtlinie kann auch eine Benachrichtigung senden, wenn darauf zugegriffen wird, oder kann zum Zugriff eine Genehmigung erfordern. Wird keine

Jump-Richtlinie angewendet, kann ohne Einschränkung auf diesen Jump Client zugegriffen werden.

Verbindungstyp

Stellen Sie den **Verbindungstyp** für die bereitgestellten Jump-Clients auf **Aktiv** oder **Passiv**. Ein aktiver Jump-Client hält eine dauerhafte Verbindung zum B Series Appliance aufrecht, während ein passiver Jump-Client lediglich auf Verbindungsanforderungen wartet.

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 dem B Series Appliance herzustellen. Die Jump-Clients müssen im gleichen Netzwerk installiert sein wie der für den Proxy-Aufruf der Verbindungen ausgewählte Jumpoint.

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.*

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 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.

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.

Sitzungsrichtlinie

Wählen Sie eine Sitzungsrichtlinie, die diesem Jump-Client zugewiesen werden soll. Sitzungsrichtlinien werden auf der Seite **Benutzer und Sicherheit > Sitzungsrichtlinien** konfiguriert. Die diesem Jump Client zugewiesene Sitzungsrichtlinie hat die höchste Priorität bei der Festlegung von Sitzungsberechtigungen.

> *Weitere Informationen finden Sie unter Sitzungsrichtlinien: Sitzungsberechtigungen und Aufforderungsregeln festlegen unter https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/session-policies.htm.*

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.

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.

Tag

Das Hinzufügen eines **Tags** hilft bei der Anordnung von Jump-Clients in Kategorien innerhalb der zugriffskonsole.

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.

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.

> ***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.*

Sie können außerdem bestimmte Installationsparameter entsprechend Ihrer eigenen Anforderungen überschreiben. 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.

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	user:<username>jumpgroup:<jumpgroup-code-name>	Wenn die Überschreibung gestattet ist, überschreibt dieser Befehlszeilenparameter die im Stapelbereitstellungsassistent angegebene Jump-Gruppe.
--jc-session-policy	<session-policy-code-name>	Wenn die Überschreibung gestattet ist, legt dieser Befehlszeilenparameter die Sitzungsrichtlinie des Jump Client fest, der die Berechtigungsrichtlinie während einer Zugriffssitzung steuert.
--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*
- *Hinzufügen eines Leerzeichens zwischen dem Parameter und dem Wert*

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.*

Jump-Client-Statistiken

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

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.

Maximale Anzahl an gleichzeitigen Upgrades für Jump-Clients

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

***Hinweis:** Diese Einstellung hat keine Auswirkung auf zugriffskonsole-Upgrades.*

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 Zugriffskonsole für Privileged Web Access 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 zugriffskonsole 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.*

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 zugriffskonsole 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, sollte dieses Feld auf eine kleinere Zahl gestellt werden als das obige Löschfeld.*

Verhalten des deinstallierten Jump-Client

Verhalten des deinstallierten Jump-Client legt fest, wie ein von einem Endbenutzer gelöschter Jump-Client von der zugriffskonsole 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 zugriffskonsole gelöscht werden. Wenn der Jump-Client das B Series Appliance zum Deinstallationszeitpunkt nicht kontaktieren kann, verbleibt das betroffene Element im Offline-Zustand.

Sonstiges

Standardverbindungstyp für Jump-Client

Legen Sie hier fest, ob der Standard-Verbindungstyp für Jump Clients aktiv oder passiv sein soll.

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-Techniker gestatten, das Aufwecken von Jump-Clients zu versuchen

Benutzern 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.

Hinweis: *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 unter Jump Client-Einstellungen verwalten unter https://www.beyondtrust.com/docs/privileged-remote-access/how-to/jump-clients/settings.htm.

Bildschirmstatus verwenden, um Kundenpräsenz zu erkennen

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. Kundenpräsenz wirkt sich auf die Sitzungsrichtlinie aus, die für von einem Jump-Client gestartete Sitzungen verwendet wird.

Globale Verbindungsrate für Jump-Clients

Die Einstellung zur globalen Verbindungsrate wird von getrennten Jump Clients verwendet, um zu bestimmen, wie aggressiv beim Versuch eines erneuten Verbindungsaufbaus vorgegangen werden muss.

Jump-Gruppen: Konfiguration, welche Benutzer auf welche Jump-Elemente zugreifen können

Jump | JUMP-GRUPPEN

Jump-Gruppen

Eine Jump-Gruppe ist ein Weg, Jump-Elemente zu organisieren und Mitgliedern unterschiedliche Zugriffsstufen für diese Elemente zu gewähren. Benutzer werden entweder 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, erstellt PRA automatisch einen.

ECM-Gruppe

Wählen Sie die mit der Jump-Gruppe zu verbindende ECM-Gruppe aus. Das Dropdown-Menü zeigt an, dass ECM-Gruppen auf der Website erstellt wurden. Wenn keine benutzerdefinierten ECM-Gruppen vorhanden sind, ist nur **Standard** als Option verfügbar. Anmeldedaten-Anfragen, die von Jump-Items in einer persönlichen Jump-Gruppe stammen, werden an die Standard-ECM-Gruppe weitergeleitet.

> ***Hinweis:*** *Diese Funktion ist nur vorhanden, wenn sie bei der Erstellung Ihrer Website aktiviert wurde. Wenn sie nicht vorhanden ist, wenden Sie sich bitte an Ihren Website-Administrator.*

> ***Hinweis:*** *Die ECM-Gruppen müssen zwar vorhanden sein, um mit einer Jump-Gruppen verknüpft zu werden, sie müssen aber dennoch mit einem API-Konto verknüpft sein, damit die Weiterleitung erfolgen kann. Weitere Informationen finden Sie in* *„API-Konfiguration: Aktivieren Sie die XML API und konfigurieren Sie benutzerdefinierte Felder“ auf Seite 183*.

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 **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 > Gruppenrichtlinien** oder **Benutzer und Sicherheit > Benutzer** konfigurierten Rollen verwenden. Eine Jump-Element-Rolle ist ein vordefinierter Berechtigungssatz zur Verwaltung und Nutzung von Jump-Elementen.

Ebenfalls können Sie eine **Jump-Richtlinie** für jeden Benutzer anwenden, um deren Zugriff auf die Jump-Elemente dieser Jump-Gruppe zu verwalten. Wenn Sie stattdessen **Für Jump-Elemente festlegen** wählen, wird die Jump-Richtlinie für das Jump-Element selbst verwendet. Jump-Richtlinien werden auf der Seite **Jump > Jump-Richtlinien** konfiguriert und bestimmen die Zeiten, während denen ein Benutzer Zugriff auf dieses Jump-Element hat. Eine Jump-Richtlinie kann auch eine Benachrichtigung senden, wenn darauf zugegriffen wird, oder kann zum Zugriff eine Genehmigung erfordern. Wird keine Jump-Richtlinie auf den Benutzer oder das Jump-Element angewendet, kann ohne Einschränkung auf dieses Jump-Element zugegriffen werden.

Bestehende Jump-Gruppen-Benutzer werden in einer Tabelle angezeigt. Sie können die Liste der Benutzer filtern, indem Sie einen Benutzernamen in das Feld **Filtern** eingeben. Ebenfalls 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.*

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

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

Jump-Richtlinien: Zeitpläne, Benachrichtigungen und Genehmigungen für Jump-Elemente festlegen

Jump	JUMP-RICHTLINIEN

Jump-Richtlinien

Jump-Richtlinien werden verwendet, um den Zugriff auf Jump-Elemente zu steuern. Dies erfolgt durch Zeitpläne, den Versand von E-Mail-Benachrichtigungen bei einem Jump-Element-Zugriff oder durch die Anforderung einer Genehmigung oder die Benutzereingabe einer Ticket-ID, bevor auf ein Jump-Element zugegriffen werden kann.

Neue Jump-Richtlinie 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-Elemente zu identifizieren.

Codename

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

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 für 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 versucht wird, nach 17 Uhr auf das Jump-Element zuzugreifen, zeigt eine Meldung an, dass der Zeitplan den Start einer Sitzung unterbindet. 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**. 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-Benachrichtigung

Empfänger benachrichtigen, wenn eine Sitzung startet

Ist diese Option aktiviert, wird den angegebenen Empfängern eine Benachrichtigungs-E-Mail gesandt, wann immer eine Sitzung mit einem Jump-Element gestartet wird, der diese Jump-Richtlinie verwendet. Wenn ein Benutzer versucht, eine Sitzung mit einem Jump-Element zu starten, das diese Richtlinie verwendet, erscheint eine Meldung, die angibt, dass eine Benachrichtigungs-E-Mail gesendet wird. Daraufhin wird der Benutzer gefragt, ob die Sitzung dennoch gestartet werden soll.

Empfänger benachrichtigen, wenn eine Sitzung endet

Ist diese Option aktiviert, wird den angegebenen Empfängern eine Benachrichtigungs-E-Mail gesandt, wenn eine Sitzung für ein Jump-Element endet, das diese Jump-Richtlinie verwendet. Wenn ein Benutzer versucht, eine Sitzung mit einem Jump-Element zu starten, das diese Richtlinie verwendet, erscheint eine Meldung, die angibt, dass am Ende der Sitzung eine Benachrichtigungs-E-Mail gesendet wird. Daraufhin wird der Benutzer gefragt, ob die Sitzung dennoch gestartet werden soll.

E-Mail-Adresse(n)

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.

Anzeigename

Geben Sie den Namen des E-Mail-Empfängers ein. Dieser Name erscheint auf der Eingabeaufforderung, die der Benutzer vor einer Sitzung mit einem Jump-Element, das diese Richtlinie verwendet, erhält.

Landeseinstellung

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

Jump-Genehmigung

Ticket-ID erfordern, bevor eine Sitzung gestartet wird

Ist diese Option aktiviert, muss der Benutzer eine gültige Ticket-ID eingeben, bevor eine Zugriffssitzung beginnen kann. Versucht ein Benutzer, auf einen Endpunkt mit dieser Jump-Richtlinie zuzugreifen, muss der Benutzer eine Ticket-ID Ihres bestehenden ITSM oder Ticket-ID-Genehmigungsprozesses eingeben, bevor der Zugriff gewährt wird. Konfigurieren Sie die ITSM- oder Ticketsystemintegration unter **Jump-Richtlinien :: Ticketsystem**.

Genehmigung erfordern, bevor eine Sitzung gestartet wird

Ist diese Option aktiviert, wird den angegebenen Empfängern eine Genehmigungs-E-Mail gesendet, wann immer eine Sitzung mit einem Jump-Element versucht wird, das diese Jump-Richtlinie verwendet. Wenn ein Benutzer versucht, eine Sitzung mit einem Jump-Element zu starten, das diese Richtlinie verwendet, fordert ein Dialog den Benutzer zur Angabe eines Anforderungsgrundes sowie einer Zeit und Dauer für diese Anforderung an.

Maximale Zugriffsdauer

Legen Sie die maximale Dauer fest, für die ein Benutzer den Zugriff zu einem Jump-Element anfordern kann, das diese Richtlinie verwendet. Der Benutzer kann eine kürzere Zugriffsdauer anfordern, die aber nicht länger sein darf als hier festgelegt.

Zugriffsgenehmigung gültig für

Wenn die Genehmigung für ein Jump-Element gewährt wurde, wird das Jump-Element entweder für jeden Benutzer verfügbar, der dieses Jump-Element sehen und den Zugriff anfordern kann, oder nur für den Benutzer, der den Zugriff angefordert hat.

E-Mail-Adresse(n)

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.

Anzeigename

Geben Sie den Namen des E-Mail-Empfängers ein. Dieser Name erscheint auf der Eingabeaufforderung, die der Benutzer vor einer Sitzung mit einem Jump-Element, das diese Richtlinie verwendet, erhält.

Landeseinstellung

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

Aufzeichnungen deaktivieren

Aufzeichnungen deaktivieren

Falls aktiviert, werden mit dieser Jump-Richtlinie gestartete Sitzungen nicht aufgezeichnet, selbst wenn Aufzeichnungen auf der Seite **Konfiguration > Optionen** aktiviert wurden. Dies betrifft die Bildschirmfreigabe, Benutzeraufzeichnungen für Protokoll-Tunnel-Jumps und Befehlsshell-Aufzeichnungen.

E-Mail-Benachrichtigungsvorlage

Betreff

Passen Sie den Betreff dieser E-Mail an. Klicken Sie auf den Link unter dem Feld **Text**, um die Makros anzuzeigen, die Ihnen für die Anpassung Ihrer E-Mails nach Wunsch zur Verfügung stehen.

Text

Passen Sie den Text dieser E-Mail an. Klicken Sie auf den Link unter dem Feld **Text**, um die Makros anzuzeigen, die Ihnen für die Anpassung Ihrer E-Mails nach Wunsch zur Verfügung stehen.

JumE-Mail-Genehmigungsvorlage

Betreff

Passen Sie den Betreff dieser E-Mail an. Klicken Sie auf den Link unter dem Feld **Text**, um die Makros anzuzeigen, die Ihnen für die Anpassung Ihrer E-Mails nach Wunsch zur Verfügung stehen.

Text

Passen Sie den Text dieser E-Mail an. Klicken Sie auf den Link unter dem Feld **Text**, um die Makros anzuzeigen, die Ihnen für die Anpassung Ihrer E-Mails nach Wunsch zur Verfügung stehen.

Ticketsystem

Ticketsystem-URL

Geben Sie unter **Ticketsystem-URL** die URL für Ihr externes Ticketsystem ein. Das B Series Appliance sendet eine ausgehende Anfrage an Ihr externes Ticketsystem. Die URL muss entweder für HTTP oder HTTPS formatiert werden. Wird eine HTTPS-URL eingegeben, muss das Seitenzertifikat für eine gültige Verbindung verifiziert werden. Besteht eine Jump-Richtlinie, die eine Ticket-ID erfordert, muss eine URL des Ticketsystems eingegeben werden oder Sie erhalten eine Warnmeldung.

Zertifikat für HTTPS-Verbindungen hochladen

Klicken Sie auf **Ein Zertifikat wählen**, um das Zertifikat für die HTTPS-Ticketsystemverbindung mit dem B Series Appliance hochzuladen. Wird Ihr Zertifikat hochgeladen, verwendet das B Series Appliance dieses, wenn es das externe System kontaktiert. Wenn Sie kein Zertifikat hochladen und das Kästchen **SSL-Zertifikatfehler ignorieren** unter dieser Einstellung markiert wird, greift das B Series Appliance beim Senden der Anfrage optional auf den integrierten Zertifikatspeicher zurück.

Benutzereingabeaufforderung

Geben Sie unter **Benutzereingabe** den Dialogtext ein, den Besucher der zugriffskonsole sehen sollen, wenn sie aufgefordert werden, die für den Zugriff erforderliche Ticket ID einzugeben.

Ticket-ID als empfindliche Information handhaben

Wird dieses Kästchen aktiviert, wird die Ticket ID als empfindliche Information behandelt und statt Text werden Sternchen angezeigt. Sie müssen eine HTTPS-Ticketsystem-URL verwenden. Wenn eine Adresse mit HTTP eingegeben wird, wird eine Fehlermeldung angezeigt, die Sie daran erinnert, dass HTTPS erforderlich ist.

Wenn diese Funktion aktiviert ist, können Sie Probleme mit SSL-Zertifikaten nicht durch Aktivieren des Kontrollkästchens **SSL-Zertifikatfehler ignorieren** umgehen. Das bedeutet, dass ein gültiges SSL-Zertifikat vorhanden sein muss. Wenn Sie versuchen, das Kontrollkästchen **SSL-Zertifikatfehler** zu aktivieren, erscheint eine Meldung, die angibt, dass Sie SSL-Zertifikatfehler nicht ignorieren können.

Bei als empfindlich behandelter Ticket ID gelten folgende Regeln:

- Sowohl die Desktop- als auch die Web-Zugriffskonsolen zeigen Sternchen anstelle von Text.
- Das Ticket wird weder von der Zugriffskonsole noch von dem B Series Appliance protokolliert.

> *Weitere Informationen finden Sie unter Erstellen von Jump-Richtlinien, um den Zugriff auf Jump-Elemente zu steuern unter https://www.beyondtrust.com/docs/privileged-remote-access/how-to/jumpoint/policies.htm.*

SSL-Zertifikatfehler ignorieren

Falls aktiviert, fügt das B Series Appliance **nicht** die Zertifikatvalidierungsinformationen an, wenn es das externe Ticketsystem kontaktiert. Belassen Sie diese Option deaktiviert, wenn Sie ein Zertifikat für eine sichere HTTPS-Verbindung hochladen.

Jump-Element-Rollen: Erstellen 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-Gruppen** 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-Gruppen** 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.

Hinzufügen oder Bearbeiten einer Jump-Element-Rolle

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 zum Kopieren von Jump-Items finden Sie in Jump-Schnittstelle: Verwenden von Jump-Elementen zum Zugriff auf Remote-Systeme unter https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/jump-interface.htm.

Bestehende Jump-Elemente entfernen

Ermöglicht es dem Benutzer, Jump-Elemente zu löschen.

Berichte anzeigen

Berechtigt den Benutzer, Berichte anzuzeigen. Dies gilt für die Jump-Gruppe, zu welcher der Benutzer mit dieser Rolle hinzugefügt wird.

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.

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.

> *Weitere Informationen finden Sie unter Verwenden von Jump-Element-Rollen, um Berechtigungen für Jump-Elemente zu konfigurieren unter https://www.beyondtrust.com/docs/privileged-remote-access/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.*

Hinzufügen oder Bearbeiten von Jumpoints

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 im gleichen Netzwerk starten müssen.

Codename

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

Externe Jump-Item-Netzwerk-ID

Wenn auf der Seite mit den **Sicherheits**einstellungen **Zugriffskonsole** der **Jumpoint für externe Jump-Item-Sitzungen** auf **Automatisch ausgewählt durch externe Jump-Item-Netzwerk-ID** gesetzt ist, wird dieser Wert mit der Eigenschaft **Netzwerk-ID** der externen Jump-Items abgeglichen, die vom Endpunkt-Anmeldedaten-Manager zurückgegeben werden, um zu bestimmen, welcher Jumpoint eine Sitzung bearbeiten wird.

> ***Hinweis: Netzwerk-ID** entspricht dem Attribut **Workgroup** auf verwalteten Systemen in Password Safe.*

Kommentare

Fügen Sie eine kurze Beschreibung hinzu, um den Zweck dieses Jumpoints zusammenzufassen. Dies ist hilfreich für die Verwaltung von Jumpoints.

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 die Option **Shell Jump-Methode aktivieren**. Die Befehlsfilterung kann so konfiguriert werden, dass eine versehentliche Nutzung von Befehlen, die für Endpunkt-Systeme schädlich sein könnten, vermieden wird.

> *Weitere Informationen zur Befehlsfilterung finden Sie unter Shell Jump zum Zugriff auf ein Remote-Netzwerkgerät verwenden unter www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/shell-jump.htm.*

Protokoll-Tunnel-Jump-Methode aktivieren

Wenn die Option „**Protokoll-Tunnel-Jump-Methode aktivieren**“ aktiviert ist, können Benutzer von ihren Systemen aus TCP-Verbindungen über diesen Jumpoint zu Remote-Endpunkten aufbauen.

RDP-Service-Konto

Wählen Sie das vom Jumpoint für die Ausführung eines vom Benutzer gestarteten Clients auf dem RDP-Server zu verwendende Konto aus. So können Sie zusätzliche Ereignisinformationen von einer mit diesem Jumpoint gestarteten RDP-Sitzung erfassen. Dieses Konto wird nur verwendet, wenn das Remote-RDP-Jump-Element so konfiguriert ist, dass die Funktion zur **Sitzungsforensik** aktiviert ist.

Hinweis: *Die Einstellung für das RDP-Servicekonto darf kein lokales Administratorkonto verwenden, sondern muss ein Domain-Administratorkonto mit minimalen Berechtigungen einschließlich des Zugriffs auf die Erstellung von Remote-Diensten und den Zugriff auf Remote-Dateisysteme verwenden.*

Weitere Informationen zur Einrichtung der Funktion zur ***Sitzungsforensik*** *in der zugriffskonsole finden Sie in Verwenden von RDP zum Zugriff auf einen Remote Windows-Endpunkt unter https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/rdp.htm.*

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 oder Jump-Elemente erstellen, die sich über diesen Jumpoint verbinden, 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 Gruppenrichtlinie angewandt.

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

Weitere Informationen zur Jumpoint-Konfiguration finden Sie unter Konfigurieren und Installieren eines PRA-Jumpoints unter https://www.beyondtrust.com/docs/privileged-remote-access/how-to/jumpoint/installation-windows.htm.

Jump-Elemente: Massenimport von symbolischen Jump-Links und Verwalten der Jump-Element-Einstellungen

Jump | JUMP-ITEMS

Massenimportassistent für symbolische Jump-Links

Über einen Jumpoint können Jump-Verknüpfungen erstellt werden, um:

- Eine Standard-Zugriffssitzung zu starten
- Eine Remote-Desktop-Protokoll-Sitzung mit einem Windows- oder Linux-System zu starten
- Einen Jump zu einer Website auf einem Remote-Browser durchzuführen
- Einen Shell Jump auf ein SSH- oder Telnet-fähiges Netzwerkgerät durchzuführen
- Eine Verbindung mit einem VNC-Server herzustellen
- Eine TCP-Verbindung durch einen Protokoll-Tunnel-Jump aufzubauen

Hinweis: *Linux-Jumpoints können nur für RDP-, SSH/Telnet-, Protokolltunnel-, Web Jump- 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 zugriffskonsole hinzuzufügen.

Weitere Informationen siehe Verwenden eines symbolischen Jump-Links zu einem Remote-System unter https://www.beyondtrust.com/docs/privileged-remote-access/how-to/jumpoint/jump-shortcuts.htm.

Vorlage herunterladen

Wählen Sie aus der Dropdown-Liste im **Massenimportassistent für symbolische Jump-Links** der /login-Schnittstelle 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. Sollten erforderliche Felder fehlen, schlägt der Import fehl. Optionale Felder können ausgefüllt oder leer gelassen werden.

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.Die CSV-Datei sollte das nachfolgende Format aufweisen.

Symbolischer Jump-Link (lokal)

Feld	Beschreibung
Hostname	Der Hostname des Endpunktes, auf den dieses Jump-Element zugreifen soll. Diese Zeichenkette kann maximal 128 Zeichen lang sein.
Name	Der Name des Endpunkts, auf den dieser symbolische Jump-Link zugreifen soll. 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.
Sitzungsrichtlinie (optional)	Der Codename einer Sitzungsrichtlinie. Sie können eine Sitzungsrichtlinie angeben, um die für dieses Jump-Element verfügbaren Berechtigungen zu verwalten.
Endpunkt-Vereinbarungsrichtlinie (optional)	Der Wert **accept** akzeptiert die Endpunkt-Vereinbarung automatisch bei Zeitüberschreitung und ermöglicht das Starten der Sitzung. Der Wert **reject** lehnt die Endpunkt-Vereinbarung automatisch ab und verhindert das Starten der Sitzung. Der Wert **no_prompt** zeigt keine Endpunkt-Vereinbarung, auch wenn die Funktion konfiguriert ist. Dieses Feld hat keine Wirkung, wenn die globale Endpunkt-Vereinbarung nicht aktiviert ist.

Weitere Informationen zur globalen Einstellung finden Sie unter Jump-Elemente: Massenimport von symbolischen Jump-Links und Verwalten von Jump-Element-Einstellungen unter https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/jump-items.htm.

Symbolischer Jump-Link (remote)

Feld	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	Der Name des Endpunkts, auf den dieser symbolische Jump-Link zugreifen soll. Dieser Name kennzeichnet das Element in den Sitzungsregisterkarten. Diese Zeichenkette kann maximal 128 Zeichen

Feld	Beschreibung
	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.
Sitzungsrichtlinie (optional)	Der Codename einer Sitzungsrichtlinie. Sie können eine Sitzungsrichtlinie angeben, um die für dieses Jump-Element verfügbaren Berechtigungen zu verwalten.
Endpunkt-Vereinbarungsrichtlinie (optional)	Der Wert **accept** akzeptiert die Endpunkt-Vereinbarung automatisch bei Zeitüberschreitung und ermöglicht das Starten der Sitzung. Der Wert **reject** lehnt die Endpunkt-Vereinbarung automatisch ab und verhindert das Starten der Sitzung. Der Wert **no_prompt** zeigt keine Endpunkt-Vereinbarung, auch wenn die Funktion konfiguriert ist. Dieses Feld hat keine Wirkung, wenn die globale Endpunkt-Vereinbarung nicht aktiviert ist.

Weitere Informationen zur globalen Einstellung finden Sie unter Jump-Elemente: Massenimport von symbolischen Jump-Links und Verwalten von Jump-Element-Einstellungen unter https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/jump-items.htm.

Symbolischer VNC-Jump-Link

Feld	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	Der Name des Endpunkts, auf den dieser symbolische Jump-Link zugreifen soll. 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*

Feld	Beschreibung
	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.

Symbolischer RDP-Jump-Link (remote)

Feld	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.
Konsolensitzung	**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.
SecureApp-Typ	Die SecureApp-Startmethode. Kann „none“, „remote_app“ (um die eingebaute RemoteApp-Funtionalität des Remote Desktop Agent zu nutzen), „remote_desktop_agent“ (um den Remote Desktop Agent von BeyondTrust zu nutzen) oder „remote_desktop_agent_credentials“ (um den Remote Desktop Agent mit Anmeldedaten-Einfügung von BeyondTrust zu nutzen) sein. Wird „remote_desktop_agent“ oder „remote_desktop_agent_credentials“ ausgewählt, muss der Remote Desktop Agent von BeyondTrust auf dem Remote-System installiert sein.>
Name der Remote-App	Der RemoteApp-Programmname. Diese Zeichenkette kann maximal 520 Zeichen lang sein.

Feld	Beschreibung
Remote-App-Parameter	Eine durch Leerzeichen getrennte Liste von Parametern, die an die RemoteApp weitergegeben werden. Parameter mit Leerzeichen können mit doppelten Anführungszeichen angegeben werden. Diese Zeichenkette kann maximal 16000 Zeichen lang sein.
Parameter der Remote-Anwendung	Eine durch Leerzeichen getrennte Liste von Parametern, die an die mit dem Remote Desktop Agent von BeyondTrust zu startende ausführbare Remote-Datei weitergegeben werden. Parameter mit Leerzeichen können mit doppelten Anführungszeichen angegeben werden. Dieser kann nur verwendet werden, wenn der SecureApp-Typ den Remote Desktop Agent von BeyondTrust verwendet.
Parameter der Remote-Anwendung	Eine durch Leerzeichen getrennte Liste von Parametern, die an die mit dem Remote Desktop Agent von BeyondTrust zu startende ausführbare Remote-Datei weitergegeben werden. Parameter mit Leerzeichen können mit doppelten Anführungszeichen angegeben werden. Dieser kann nur verwendet werden, wenn der SecureApp-Typ den Remote Desktop Agent von BeyondTrust verwendet.
Zielsystem	Der Name des Zielsystems, auf das die Remote-Anwendung zugreift. Mit diesem Wert soll die Liste der eingefügten Anmeldedaten auf diejenigen Anmeldedaten begrenzt werden, die im Zielsystem gültig sind. Dieser Wert kann nur verwendet werden, wenn der SecureApp-Typ den Remote Desktop Agent von BeyondTrust mit Anmeldedaten-Einfügung verwendet.
Art der Anmeldedaten	Die Art der Anmeldedaten, die in die ausführbare Remote-Datei eingefügt werden. Dieser Wert hängt vom Passwort-Vault ab, von dem Anmeldedaten abgerufen werden. Dieser Wert kann nur verwendet werden, wenn der SecureApp-Typ den Remote Desktop Agent von BeyondTrust mit Anmeldedaten-Einfügung verwendet.
Name	Der Name des Endpunkts, auf den dieser symbolische Jump-Link zugreifen soll. 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.
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

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

Feld	Beschreibung
	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	Der Name des Endpunkts, auf den dieser symbolische Jump-Link zugreifen soll. 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.
Sitzungsrichtlinie (optional)	Der Codename einer Sitzungsrichtlinie. Sie können eine Sitzungsrichtlinie angeben, um die für dieses Jump-Element verfügbaren Berechtigungen zu verwalten.

Symbolischer Protokoll-Tunnel-Jump-Link

Feld	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.
TCP-Tunnel	Die Liste einer oder mehrerer Tunnel-Definitionen. Eine Tunnel-Definition ist eine Zuordnung eines TCP-Ports am lokalen Benutzersystem zum TCP-Port am Remote-Endpunkt. Eine Verbindung zum lokalen Port führt zum Aufbau einer Verbindung zum Remote-Port, sodass Daten zwischen dem lokalen und dem Remote-System getunnelt werden. Mehrere Zuordnungen sollten durch ein Semikolon getrennt werden.

Feld	Beschreibung
	Example: auto->22;3306->3306 In diesem Beispiel wird ein zufällig gewählter lokaler Port dem Remote-Port 22 zugeordnet und der lokale Port 3306 wird dem Remote-Port 3306 zugeordnet.
Lokale Adresse (optional)	Die Adresse, von der aus die Verbindung aufgebaut werden soll. Dies kann eine beliebige Adresse im Unterbereich 127.x.x.x sein. Die Standardadresse lautet 127.0.0.1.
Name	Der Name des Endpunkts, auf den dieser symbolische Jump-Link zugreifen soll. 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.
Sitzungsrichtlinie (optional)	Der Codename einer Sitzungsrichtlinie. Sie können eine Sitzungsrichtlinie angeben, um die für dieses Jump-Element verfügbaren Berechtigungen zu verwalten.

Symbolischer Web-Jump-Link

Feld	Beschreibung
Name	Der Name des Endpunkts, auf den dieser symbolische Jump-Link zugreifen soll. Dieser Name kennzeichnet das Element in den Sitzungsregisterkarten. Diese Zeichenkette kann maximal 128 Zeichen lang sein.
Jumpoint	Der Codename des Jumpoint, über den auf den Endpunkt zugegriffen wird.
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.

Feld	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.
Sitzungsrichtlinie (optional)	Der Codename einer Sitzungsrichtlinie. Sie können eine Sitzungsrichtlinie angeben, um die für dieses Jump-Element verfügbaren Berechtigungen zu verwalten.
URL	Die URL der Webseite. Die URL muss entweder mit **http** oder **https** beginnen.
Zertifikat verifizieren (optional)	**1:** Das Seitenzertifikat wird vor Sitzungsbeginn validiert. Wenn Probleme auftreten, wird die Sitzung nicht gestartet. **0:** Das Seitenzertifikat wird nicht validiert.
Benutzernamen-Format	passthru: Der Benutzername wird direkt vom Anmeldedaten-Anbieter durchgereicht. username_only: Wenn der Benutzername im Format UPN (nutzername@domäne) oder DLLN (DOMÄNE\\nutzername) vorliegt, wird die Domäne entfernt. Nur der Benutzername wird eingefügt.
Hinweis Benutzername-Feld	Ein Abfrage-Selektor im CSS-Format, der das Benutzername-Feld identifiziert, um die anfängliche Anmeldedaten-Einfügung zu erleichtern. Wenn dieser Wert vorliegt und kein passendes Element gefunden wird, schlägt die Anmeldedaten-Einfügung fehl.
Hinweis Passwortfeld	Ein Abfrage-Selektor im CSS-Format, der das Passwort-Feld identifiziert, um die anfängliche Anmeldedaten-Einfügung zu erleichtern. Wenn dieser Wert vorliegt und kein passendes Element gefunden wird, schlägt die Anmeldedaten-Einfügung fehl.
Hinweis Schaltfläche "Abschicken"	Ein Abfrage-Selektor im CSS-Format, der die Schaltfläche "Abschicken" identifiziert, um die anfängliche Anmeldedaten-Einfügung zu erleichtern. Wenn dieser Wert vorliegt und kein passendes Element gefunden wird, schlägt die Anmeldedaten-Einfügung fehl.
Zeitüberschreitung bei der Authentifizierung	Die Zeitspanne, die der Web-Jump-Client auf die Authentifizierung warten soll, bevor die Zeit abläuft. Gültige Werte sind 1, 2, 3, 5, 10, 15, 30

Weitere Informationen siehe Verwenden eines symbolischen Jump-Links zu einem Remote-System unter https://www.beyondtrust.com/docs/privileged-remote-access/how-to/jumpoint/jump-shortcuts.htm.

Endpunkt-Benutzerveinbarung

Endpunkt-Benutzereinwilligungskonfiguration für zutreffende Jump-Elemente aktivieren

Aktiviert ein Dropdown-Menü in der Zugriffskonsole, mit dem Endpunkt-Benutzervereinbarungsoptionen für individuelle Jump-Elemente konfiguriert werden können.

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. Um auf den Standardtext zurückzusetzen, löschen Sie den Text aus dem Feld und speichern

Sie dann das leere Feld.

Text

Geben Sie den Text für die Vereinbarung an. Sie können diesen Text für jegliche aktivierten Sprachen lokalisieren. Um auf den Standardtext zurückzusetzen, löschen Sie den Text aus dem Feld und speichern Sie dann das leere Feld.

Zeitüberschreitung bei der Annahme

Akzeptiert der Benutzer die Vereinbarung nicht innerhalb des festgelegten **Annahme-Zeitlimits**, wird die Vereinbarung entweder abgelehnt oder akzeptiert (abhängig von den Eigenschaften des Jump-Elements).

Automatisches Verhalten

Wählen **Automatisch akzeptieren** oder **Automatisch ablehnen**. Die Option **Automatisch akzeptieren** akzeptiert die Endpunkt-Vereinbarung automatisch bei Zeitüberschreitung und ermöglicht das Starten der Sitzung. Die Option **Automatisch ablehnen** lehnt die Endpunkt-Vereinbarung automatisch ab und verhindert das Starten der Sitzung.

Jump-Element-Einstellungen

Gleichzeitige Jumps

Für Jump-Client, Lokaler Jump, Remote-Jump, Remote-VNC und Shell Jump.

Setzen Sie diese Option 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, Remote-VNC und Shell Jump.

Für Remote-RDP

Setzen Sie diese Option 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 Remote-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 Remote-RDP.

Externe Werkzeuge

Benutzern das Öffnen von Remote-RDP-Jump-Verknüpfungen mit einem externen Tool erlauben

Wenn aktiviert, können Sie Ihr eigenes RDP-Werkzeug für Remote-RDP-Jump-Verknüpfungen verwenden.

Benutzern das Öffnen von Shell Jump-Verknüpfungen mit einem externen Tool erlauben

Wenn aktiviert, können Sie Ihr eigenes Tool verwenden, um Shell Jump-Verknüpfungen zu öffnen.

> *Diese Funktionen müssen für jeden Benutzer in der zugriffskonsole aktiviert werden. Weitere Informationen finden Sie unter Einstellungen und Voreinstellungen in Zugriffskonsole ändern unter https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/settings.htm.*

Shell Jump-Filterung

Erkannte Shell-Eingabeaufforderungen

Geben Sie pro Zeile einzelne reguläre Ausdrücke ein, die mit den Befehlsshell-Eingabeaufforderungen in Ihren Endpunkt-Systemen übereinstimmen. Ein regulärer Ausdruck sollte nur mit der letzten Zeile einer mehrzeiligen Eingabeaufforderung übereinstimmen.

Validierung der Übereinstimmung von Shell-Eingabeaufforderungen

Geben Sie eine die Shell-Eingabeaufforderung eines vorhandenen Endpunktes ein, und die Ausgabe gibt an, ob sie mit einem der regulären Ausdrücke auf der Liste übereinstimmt. Mit dieser Funktion können Sie Ihre regulären Ausdrücke testen, ohne eine Sitzung starten zu müssen.

Vault für Privileged Remote Access

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.
- **Kontorichtlinie:** Die mit dem Vault-Konto verbundene Kontorichtlinie.
- **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 das Auschecken von Anmeldedaten, das Einchecken 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 persönlichen Konten, die angezeigt werden, nach **Eigentümer** und **Passwortalter** filtern.*

Konten

Konto hinzufügen

Klicken Sie auf **Hinzufügen**, um manuell geteilte oder persönliche generische Konten zum BeyondTrust-Vault hinzuzufügen.

Rotieren

Wählen Sie ein oder mehrere freigegeben generische Konten, klicken Sie auf **Rotieren** und dann auf **Rotation starten**.

Hinweis:

- *Dienstkonten, die in einer Failover-Cluster-Umgebung laufen, können nicht rotiert werden. Der Fehler „Failover Cluster erkannt. Das run-as-Passwort für den Dienst <service_name> kann nicht geändert werden“ erscheint, wenn ein Rotationsversuch unternommen wird und in der Spalte **Status** wird **Rotation fehlgeschlagen** für den Dienst angezeigt.*
- *Dienste, die ein Microsoft Graph-Konto als „Ausführen als“-Konto verwenden, können nicht rotiert werden.*
- *Dienste, die abhängige Dienste haben, können nicht rotiert werden, da das Risiko besteht, dass Dienste innerhalb der Dienstkette nicht erfolgreich neu gestartet werden.*

Weitere Informationen finden Sie in Privilegierte Anmeldedaten mit BeyondTrust Vault rotieren unter https://www.beyondtrust.com/docs/privileged-remote-access/how-to/vault/rotation.htm..

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 einen Satz geteilter 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 PRA /login-Schnittstelle auschecken unter https://www.beyondtrust.com/docs/privileged-remote-access/how-to/vault/check-out.htm.

Ellipsis-Menü für geteilte Konten

Klicken Sie auf die **Ellipse (...)**, 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**.

Hinweis:

- *Dienstkonten, die in einer Failover-Cluster-Umgebung laufen, können nicht rotiert werden. Der Fehler „Failover Cluster erkannt. Das run-as-Passwort für den Dienst <service_name> kann nicht geändert werden“ erscheint, wenn ein Rotationsversuch unternommen wird und in der Spalte **Status** wird **Rotation fehlgeschlagen** für den Dienst angezeigt.*
- *Dienste, die ein Microsoft Graph-Konto als „Ausführen als“-Konto verwenden, können nicht rotiert werden.*
- *Dienste, die abhängige Dienste haben, können nicht rotiert werden, da das Risiko besteht, dass Dienste innerhalb der Dienstkette nicht erfolgreich neu gestartet werden.*

Weitere Informationen finden Sie in Privilegierte Anmeldedaten mit BeyondTrust Vault rotieren unter https://www.beyondtrust.com/docs/privileged-remote-access/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 persönliche 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: **Passwort**, **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

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, sowie gegebenenfalls die SSH-Schlüssel-Passphrase.

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.

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.

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 Privileged Remote Access-Sitzungen verwenden.
- **Einfügen und auschecken:** Benutzer mit dieser Rolle können dieses Konto in Privileged Remote Access-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 Privileged Remote Access-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 kann. Eine Rolle kann durch die Gruppenrichtlinien des Benutzers zugewiesen werden, während eine andere Rolle durch den expliziten Zugriff des Benutzers auf das Vault-Konto zugewiesen werden kann. 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 zugriffskonsole 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 zugriffskonsole erscheint.
    - **Hostname/IP:** Dieser Filter wird mit dem Wert abgeglichen, der in der Spalte **Hostname/IP** des Jump-Items in der zugriffskonsole erscheint.
    - **Tag:** Dieser Filter wird mit dem Wert abgeglichen, der in der Spalte **Tag** des Jump-Items in der zugriffskonsole erscheint.
    - **Kommentare:** Dieser Filter wird mit dem Wert abgeglichen, der in der Spalte **Kommentare** des Jump-Items in der zugriffskonsole 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

Anhand der Option **Hinzufügen > Persönliches generisches Konto** können Sie Konten 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: **Passwort**, **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

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, sowie gegebenenfalls die SSH-Schlüssel-Passphrase.

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.

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

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.

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.

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 zugriffskonsole 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 zugriffskonsole erscheint.
        - **Hostname/IP:** Dieser Filter wird mit dem Wert abgeglichen, der in der Spalte **Hostname/IP** des Jump-Items in der zugriffskonsole erscheint.
        - **Tag:** Dieser Filter wird mit dem Wert abgeglichen, der in der Spalte **Tag** des Jump-Items in der zugriffskonsole erscheint.
        - **Kommentare:** Dieser Filter wird mit dem Wert abgeglichen, der in der Spalte **Kommentare** des Jump-Items in der zugriffskonsole 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.*

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

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.

Eindeutiger Name

Zeigen Sie den eindeutigen Namen des Kontos 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.

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 zugriffskonsole 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 zugriffskonsole erscheint.
  - **Hostname/IP:** Dieser Filter wird mit dem Wert abgeglichen, der in der Spalte **Hostname/IP** des Jump-Items in der zugriffskonsole erscheint.
  - **Tag:** Dieser Filter wird mit dem Wert abgeglichen, der in der Spalte **Tag** des Jump-Items in der zugriffskonsole erscheint.
  - **Kommentare:** Dieser Filter wird mit dem Wert abgeglichen, der in der Spalte **Kommentare** des Jump-Items in der zugriffskonsole 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 generisches (Passwort) Konto bearbeiten

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.

Passwort und Bestätigung des Passworts

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

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 Privileged Remote Access-Sitzungen verwenden.
- **Einfügen und auschecken:** Benutzer mit dieser Rolle können dieses Konto in Privileged Remote Access-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 zugriffskonsole 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 zugriffskonsole erscheint.
        - **Hostname/IP:** Dieser Filter wird mit dem Wert abgeglichen, der in der Spalte **Hostname/IP** des Jump-Items in der zugriffskonsole erscheint.
        - **Tag:** Dieser Filter wird mit dem Wert abgeglichen, der in der Spalte **Tag** des Jump-Items in der zugriffskonsole erscheint.
        - **Kommentare:** Dieser Filter wird mit dem Wert abgeglichen, der in der Spalte **Kommentare** des Jump-Items in der zugriffskonsole 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 Privileged Remote Access 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: Erfasste Systeme anzeigen und 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 und Jump-Items.

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.

Sie können neue oder vorhandene RDP Jump-Verknüpfungen hinzufügen. Klicken Sie in der Ansicht **Jump-Items** auf **Hinzufügen** und wählen Sie **Remote-RDP-Jump-Verknüpfungen hinzufügen** oder **Vorhandene RDP-Jump-Verknüpfungen zuordnen**.

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 sind **Benutzername**, **Passwort** und **Passwort-Bestätigung** erforderlich. 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.

Discovery: Konten, Endpunkte und Dienste in einer Domain erfassen

Vault	DISCOVERY

BeyondTrust Vault ist ein geräteintegrierter 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 Technisches Whitepaper zu BeyondTrust Vault unter https://www.beyondtrust.com/docs/privileged-remote-access/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 > Zugriffsberechtigungen > 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 BeyondTrust Jumpoint-Handbuch für Privileged Remote Access unter https://www.beyondtrust.com/docs/privileged-remote-access/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. Sie können auch ein vorhandenes Konto verwenden, das in einem vorangehenden Auftrag erfasst oder im Abschnitt **Konten** manuell hinzugefügt worden ist.

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 zugriffskonsole erscheint.
- **Hostname:** Der Hostname des Jump-Clients, wie er in der Spalte **Hostname/IP** der zugriffskonsole erscheint.
- **FQDN:** Der vollqualifizierte Domänenname des Jump-Clients, wie er unter dem **FQDN**-Label des Detailbereichs Jump-Client in der zugriffskonsole 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 zugriffskonsole 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 privilegierten Konten mit BeyondTrust Vault erfassen unter https://www.beyondtrust.com/docs/privileged-remote-access/how-to/vault/discovery.htm.*

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.

Zugriffskonsole

Einstellungen für Zugriffskonsole: Standardmäßige Einstellungen für die Konsole verwalten

Zugriffskonsole | EINSTELLUNGEN FÜR ZUGRIFFSKONSOLE

Verwalten der Zugriffskonsole-Einstellungen

Sie können die Standardeinstellungen der zugriffskonsole für Ihre gesamte Benutzerbasis konfigurieren, ein durchgängiges Benutzererlebnis mit der zugriffskonsole 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. Eine erzwungene Einstellung kann nicht überschrieben werden, es sei denn, ein Administrator deaktiviert das Kontrollkästchen **Erzwungen** in der /login-Verwaltungsschnittstelle.

> *Details dazu, wie ein Benutzer die Einstellungen in der zugriffskonsole nach Bedarf ändern kann, finden Sie in Einstellungen und Voreinstellungen in der Zugriffskonsole ändern unter https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/settings.htm.*

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** unten 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 zugriffskonsole mit Ihren verwalteten Standardeinstellungen. Für bestehende Benutzer werden bei der nächsten Anmeldung erzwungene Einstellungen übernommen, alle anderen Einstellungen bleiben jedoch unberührt.

Globale Einstellungen

Rechtschreibprüfung aktivieren

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

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.

Alarme – Chatalarme

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 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-Chat

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

Zugriffssitzungs

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

Alarme – Warteschlangenalarme

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.

Popup-Benachrichtigungen

Popup-Benachrichtigungen erscheinen unabhängig von der zugriffskonsole 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 - Freigegebene Sitzungen

Wählen Sie, ob ein Benutzer eine Popup-Benachrichtigung für freigegebene Sitzungen in dieser Warteschlange erhalten soll.

Team-Chat - Freigegebene Sitzungen

Wählen Sie, ob ein Benutzer eine Popup-Benachrichtigung für freigegebene Sitzungen in dieser Warteschlange erhalten soll.

Popup-Verhalten – Position und Dauer

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

Zugriffssitzungs

Automatisch Bildschirmfreigabe anfordern

Wählen Sie, ob die Sitzungen Ihrer Benutzer mit der Bildschirmfreigabe beginnen sollen.

Automatisch lösen

Sitzungen können entweder als Registerkarten in der zugriffskonsole oder aber automatisch als neue Fenster geöffnet werden.

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.

Endpunkt-Sichtbarkeit bei Beginn der Bildschirmfreigabe automatisch einschränken

Zu Beginn der Bildschirmfreigabe kann das Remote-System automatisch die Anzeige, Maus- und Tastatureingabe einschränken und bewahrt so die Privatsphäre.

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 gespeichert** angezeigt. Alle Benutzer, die sich nach dem Speichern des neuen Profils in der zugriffskonsole anmelden, erhalten die neuen Einstellungen als Standardeinstellungen.

Übernehmen von Zugriffskonsole-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 zugriffskonsole anmelden. Im Dialogfenster werden sie darüber informiert, dass die Einstellungen geändert wurden, und haben die Option, das Dialogfenster zu schließen oder ihr Einstellungsfenster in der zugriffskonsole zu öffnen, um die Änderungen zu prüfen.

Benutzerdefinierte Links: Hinzufügen von URL-Verknüpfungen zur Zugriffskonsole

Zugriffskonsole	BENUTZERDEFINIERTE LINKS

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 Endpunktsystem zu finden, oder ein Customer-Relationship-Management-System (CRM).

Hier erstellte Links werden über die Schaltfläche **Links** auf der zugriffskonsole verfügbar.

Benutzerdefinierten Link hinzufügen, bearbeiten oder löschen

Fügen Sie einen neuen Link hinzu, bearbeiten Sie einen bestehenden Link oder entfernen Sie einen bestehenden Link.

Benutzerdefinierte Links 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. Klicken Sie auf den Link unter dem Feld **Text**, um die Makros anzuzeigen, die Ihnen für die Anpassung Ihrer E-Mails nach Wunsch zur Verfügung stehen.

> *Für weitere Informationen siehe Überblick über Zugriffssitzungen und Tools unter https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/session-overview.htm.*

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

Zugriffskonsole	VORDEFINIERTE SKRIPTS

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.

> *Für weitere Informationen siehe Überblick über Zugriffssitzungen und Tools unter https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/session-overview.htm.*

> *Für weitere Informationen siehe Öffnen der Befehlsshell am Remote-Endpunkt mithilfe der Zugriffskonsole unter https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/command-shell.htm.*

Filter für Teamverfügbarkeit und Kategorien

Filtern Sie Ihre Ansicht, indem Sie eine Kategorie oder ein Team aus der Dropdown-Liste wählen.

Neues vordefiniertes Skript 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. 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 Teams dieses Element nutzen können sollen.

Kategorien

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

Ressourcendatei

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

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. Sie können bis zu 100 MB in Ihr Ressourcendatei-Verzeichnis hochladen.

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

Zugriffskonsole	SPEZIELLE AKTIONEN

Spezielle Aktionen

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

Eine neue spezielle Aktion hinzufügen, bearbeiten, löschen

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

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 spezielle Aktion durch ihre Wahl aus dem Menü während einer Sitzung sofort ausgeführt.

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 spezielle Aktion* ***Windows-Sicherheit (Strg-Alt-Entf)*** *kann nicht deaktiviert werden.*

Benutzer und Sicherheit

Benutzer: Kontoberechtigungen für einen Benutzer oder Administrator hinzufügen

Benutzer und Sicherheit | BENUTZER

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.

Neuen Benutzer 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 bestimmten Benutzerkonten basierend auf Benutzername, Anzeigename oder E-Mail-Adresse.

Sicherheitsanbieter

Wählen Sie einen Sicherheitsanbietertyp aus der Dropdown-Liste, um die Liste der Benutzer nach Sicherheitsanbieter zu filtern.

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.

Fehlgeschlagene Anmeldungsversuche zurücksetzen und Konto entsperren

Wenn ein Benutzer einen oder mehr fehlgeschlagene Anmeldungsversuche aufweist, klicken Sie auf die Schaltfläche **Zurücksetzen** für sein Benutzerkonto, um den Zähler zurück auf Null zu setzen.

Wenn ein Benutzer aufgrund von zu vielen fehlgeschlagenen aufeinanderfolgenden Anmeldeversuchen gesperrt wird, klicken Sie auf die Schaltfläche **Konto entsperren** für sein Benutzerkonto, um die Zahl wieder auf Null zurückzusetzen und sein Konto zu entsperren.

Hinzufügen oder Bearbeiten eines Nutzers

Benutzername

Eindeutige Kennung, die zur Anmeldung verwendet wird.

Anzeigename

Benutzername, wie in Teamchats, Berichten usw. gezeigt.

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.

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.

Passwortrücksetzungslink per E-Mail an Benutzer senden

Ist ein Haken gesetzt, können Administratoren Benutzern einen Passwortrücksetzungslink senden.

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

Aktivieren Sie dieses Kästchen, um das Passwort des Benutzers so einzustellen, dass es nie abläuft.

Passwort-Ablaufdatum

Geben Sie ein Ablaufdatum für das Passwort an.

Mitgliedschaften

> ***Hinweis:*** *Der Bereich* ***Mitgliedschaften*** *wird bei der Erstellung eines Benutzers zunächst nicht angezeigt. Sobald der neue Benutzer gespeichert wurde, wird der Bereich* ***Mitgliedschaften*** *angezeigt und führt jegliche Gruppenrichtlinien oder Teams auf, zu denen der Benutzer hinzugefügt wurde.*

Gruppenrichtlinienmitgliedschaften

Liste der Gruppenrichtlinien, denen der Benutzer angehört.

Teammitgliedschaften

Liste der Teams, denen der Benutzer angehört.

Jumpoint-Mitgliedschaften

Liste der Jumpoints, auf die der Benutzer zugreifen kann.

Jump-Gruppenmitgliedschaften

Liste der Jump-Gruppen, denen der Benutzer angehört.

Kontoeinstellungen

Zwei-Faktor-Authentifizierung

Die Zwei-Faktor-Authentifizierung (2FA) nutzt eine Authentifikator-App, um einen zeitbasierten, einmaligen Code zur Anmeldung in der Verwaltungsschnittstelle und der Zugriffskonsole bereitzustellen. Wenn **Erforderlich** gewählt wird, wird der Benutzer bei der nächsten Anmeldung aufgefordert, sich für 2FA zu registrieren und diese Methode zu nutzen. Wenn **Optional** gewählt wird, hat der Benutzer die Option, 2FA zu nutzen, ist aber nicht dazu verpflichtet. **Klicken Sie auf Aktuelle Authentifikator-App entfernen**, wenn sich ein Benutzer nicht mehr mit einem bestimmten Authentifikator anmelden soll.

Das Konto läuft niemals ab

Ist ein Haken gesetzt, läuft das Konto nie ab. Ist kein Haken gesetzt, muss ein Ablaufdatum für das Konto festgelegt werden.

Konto-Ablaufdatum

Führt dazu, dass das Konto nach 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.

Kommentare

Fügen Sie Kommentare hinzu, die den Zweck dieses Objekts deutlich machen.

Allgemeine Berechtigungen

Verwaltung

Administratorrechte

Erteilt dem Benutzer volle Administratorrechte.

Zur Verwaltung von Vault berechtigt

Ermöglicht dem Benutzer den Zugriff auf Vault.

Passworteinstellung

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

Bearbeiten des Jumpoint

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.

Bearbeiten von Teams

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

Bearbeiten der Jump-Gruppe

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

Bearbeitung vordefinierter Skripts

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

Bearbeiten von benutzerdefinierten Links

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

Berechtigt, Berichte zu Zugriffssitzungen anzuzeigen

Ermöglicht dem Benutzer, Berichte zur Zugriffssitzung-Aktivität auszuführen, nur Sitzungen anzuzeigen, bei denen er der primäre Sitzungseigentümer war, nur Sitzungen für Endpunkte anzuzeigen, die zu einer Jump-Gruppe gehören, deren Mitglied er ist, oder alle Sitzungen.

Berechtigt, Zugriffssitzung-Aufzeichnungen anzuzeigen

Damit kann der Benutzer Videoaufzeichnungen der Bildschirmfreigabe und Befehlsshell-Sitzungen anzeigen.

Berechtigt, Vault-Berichte anzuzeigen

Damit kann der Benutzer seine eigenen Vault-Ereignisse oder alle Vault-Ereignisse anzeigen.

Berechtigt, Syslog-Berichte anzuzeigen

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

Zugriffsberechtigungen

Zugriff

Berechtigt, auf Endpunkte zuzugreifen

Damit kann der Benutzer die zugriffskonsole verwenden, um Sitzungen durchzuführen. Wenn der Endpunkt-Zugriff aktiviert ist, sind auch Optionen für den Endpunkt-Zugriff verfügbar.

Sitzungsverwaltung

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 unter Steuern des Remote-Endpunkts mit der Bildschirmfreigabe unter https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/screen-sharing.htm.*

Berechtigt, externe Benutzer einzuladen

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

> *Für weitere Informationen siehe Einladen eines externen Benutzers zur Teilnahme an einer Zugriffssitzung unter https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/access-invite.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 zugriffskonsole 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 zugriffskonsole zu ändern.

> *Für weitere Informationen siehe Überblick über Zugriffssitzungen und Tools unter https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/session-overview.htm.*

Benutzer-zu-Benutzer-Bildschirmfreigabe

> *Weitere Informationen finden Sie unter Bildschirm für anderen Benutzer freigeben unter https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/user-screensharing.htm.*

Berechtigt, anderen Benutzern 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 Benutzern 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.

Jump-Technologie

Gestattete Methoden für Jump-Items

Ermöglicht es dem Benutzer, mit **Jump Clients**, **Lokalem Jump im lokalen Netzwerk**, **Remote-Jump mittels Jumpoint**, **Remote-VNC mittels Jumpoint**, **Remote-RDP mittels Jumpoint**, **Web Jump mittels Jumpoint**, **Shell Jump mittels Jumpoint** und **Protokoll-Tunnel-Jump mittels Jumpoint** Jumps zu Computern auszuführen.

Jump-Element-Rollen

Eine Jump-Element-Rolle ist ein vordefinierter Berechtigungssatz zur Verwaltung und Nutzung von Jump-Elementen. Klicken Sie für jede Option auf **Anzeigen**, 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 zugriffskonsole kann dieser dann die persönlichen Listen von Jump-Elementen von Benutzern sehen, die keine Teammitglieder sind.

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.*

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

Sitzungsberechtigungen

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.

Beschreibung

Zeigen Sie die Beschreibung einer vordefinierten Berechtigungsrichtlinie an.

Bildschirmfreigabe

Bildschirmfreigabe-Regeln

Wählen Sie den Zugriff des Support-Technikers und des Remote-Benutzers am Remote-System:

- 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.
- **Ablehnen** deaktiviert die Bildschirmfreigabe.
- **Nur Ansicht** ermöglicht es dem Support-Techniker, den Bildschirm zu sehen.

- **Ansicht und Steuerung** ermöglicht es dem Support-Techniker, das System einzusehen und Maßnahmen zu ergreifen. Wenn diese Option ausgewählt ist, können Endpunktbeschränkungen festgelegt werden, um Störungen durch den Remote-Benutzer zu vermeiden:
  - **Keine** legt keine Einschränkungen für das Remote-System fest.
  - **Bildschirm, Maus und Tastatur** deaktiviert diese Eingänge. Wenn diese Option aktiviert ist, steht ein Kontrollkästchen zur Verfügung, um **Automatisch den Bildschirm „Privatsphäre“ bei Sitzungsbeginn anzufordern**. 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 finden Sie unter Steuern des Remote-Endpunkts mit der Bildschirmfreigabe unter https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/screen-sharing.htm.

Synchronisierungsrichtung für Zwischenablage

Wählen Sie, wie der Inhalt der Zwischenablage zwischen Benutzern und Endpunkten ausgetauscht wird. Die Optionen sind:

- **Nicht berechtigt**: Der Benutzer darf die Zwischenablage nicht verwenden, es werden keine Zwischenablage-Symbole im zugriffskonsole angezeigt, und die Befehle zum Ausschneiden und Einfügen funktionieren nicht.
- **Zulässig vom Support-Techniker zum Kunden:** Der Benutzer kann den Inhalt der Zwischenablage an den Endpunkt weiterleiten, kann aber nicht aus der Zwischenablage des Endpunkts einfügen. Nur das Zwischenablage-Symbol **Senden** wird im zugriffskonsole angezeigt.
- **Zulässig in beide Richtungen:** Der Inhalt der Zwischenablage kann in beide Richtungen übertragen werden. Beide Symbole Zwischenablage senden und abrufen werden im zugriffskonsole angezeigt.

Weitere Informationen über den Zwischenablage-Synchronisationsmodus finden Sie unter „Sicherheit: Verwalten der Sicherheitseinstellungen“ auf Seite 159.

Anwendungsfreigabebeschränkungen

Beschränken Sie den Zugriff auf angegebene Anwendungen auf dem Remote-System entweder mit **Nur die aufgeführten ausführbaren Dateien gestatten** oder **Nur die aufgeführten ausführbaren Dateien ablehnen**. Ebenfalls können Sie den Desktop-Zugriff zulassen oder verbieten.

Hinweis: *Diese Funktion gilt nur für Windows-Betriebssysteme.*

Neue ausführbare Dateien hinzufügen

Wenn Anwendungsfreigabebeschränkungen durchgesetzt werden, erscheint eine neue Schaltfläche **Neue ausführbare Dateien hinzufügen**. Mit Klick auf diese Schaltfläche wird ein Dialogfenster geöffnet, in dem Sie ausführbare Dateien angeben können, die gemäß Ihrer Ziele abgelehnt oder gestattet werden sollen.

Nach dem Hinzufügen von ausführbaren Dateien zeigen eine oder zwei Tabellen die Dateinamen oder Hashes an, die zur Einschränkung ausgewählt wurden. Ein bearbeitbares Kommentarfeld ermöglicht Administrationsnotizen.

Geben Sie Dateinamen oder SHA-256-Hashes ein, einen pro Zeile

Geben Sie bei der Einschränkung von ausführbaren Dateien die Dateinamen oder Hashes der ausführbaren Dateien, die sie gestatten oder verbieten möchten, manuell ein. Klicken Sie auf **Ausführbare Datei(en) hinzufügen**, wenn Sie fertig sind, um die gewählten Dateien zu Ihrer Konfiguration hinzuzufügen.

Pro Dialog können bis zu 25 Dateien angegeben werden. Wenn Sie mehr hinzufügen müssen, klicken Sie auf **Ausführbare Datei(en) hinzufügen** und öffnen Sie den Dialog dann erneut.

Navigieren zu einer oder mehreren Dateien

Wählen Sie bei der Beschränkung von ausführbaren Dateien diese Option, um auf Ihrem System zu ausführbaren Dateien zu navigieren und ihre Namen oder Hashes automatisch abzuleiten. Wenn Sie Dateien so auf Ihrer lokalen Plattform bzw. Ihrem lokalen System auswählen, stellen Sie sicher, dass es sich bei den Dateien tatsächlich um ausführbare Dateien handelt. Dies wird auf Browserebene nicht überprüft.

Wählen Sie entweder **Dateiname benutzen** oder **Datei-Hash benutzen**, damit der Browser die Dateinamen oder Hashes der ausführbaren Dateien automatisch ableitet. Klicken Sie auf **Ausführbare Datei(en) hinzufügen**, wenn Sie fertig sind, um die gewählten Dateien zu Ihrer Konfiguration hinzuzufügen.

Pro Dialog können bis zu 25 Dateien angegeben werden. Wenn Sie mehr hinzufügen müssen, klicken Sie auf **Ausführbare Datei(en) hinzufügen** und öffnen Sie den Dialog dann erneut.

Hinweis: *Diese Option ist nur in modernen und nicht in älteren Browsern verfügbar.*

Gestattete Endpunkteinschränkungen

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.

Weitere Informationen finden Sie unter Steuern des Remote-Endpunkts mit der Bildschirmfreigabe unter https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-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 unter Verwenden von Anmerkungen, um auf dem Remote-Bildschirm des Endpunktes zu zeichnen unter https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-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 Endpunkts

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 Benutzers

Gestattet es Benutzern, Dateien direkt zu oder von jeglichen oder nur von bestimmten Verzeichnissen auf seinem lokalen System zu übertragen.

Weitere Informationen finden Sie unter Dateitransfer zum und vom Remote-System-Endpunkt unter https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-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.*

Konfigurieren der Befehlsfilterung, um eine versehentliche Nutzung von Befehlen, die für Endpunkt-Systeme schädlich sein können, zu vermeiden.

Weitere Informationen zur Befehlsfilterung finden Sie unter Shell Jump zum Zugriff auf ein Remote-Netzwerkgerät verwenden unter www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/shell-jump.htm.

Für weitere Informationen siehe Öffnen der Befehlsshell am Remote-Endpunkt mithilfe der Zugriffskonsole unter https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-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 unter Anzeige von Systeminformationen am Remote-Endpunkt unter https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-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 unter Zugriff auf den Registrierungseditor am Remote-Endpunkt unter https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/registry-editor.htm.*

Vordefinierte Skripts

Regeln für vordefinierte Skripts

Damit kann der Benutzer vordefinierte Skripts ausführen, die für seine Teams erstellt wurden. 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.

> *Für weitere Informationen siehe Öffnen der Befehlsshell am Remote-Endpunkt mithilfe der Zugriffskonsole unter https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/command-shell.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

Anmeldungszeitplan

Die Benutzeranmeldung auf den folgenden Zeitplan beschränken

Legen Sie einen Zeitplan fest, der definiert, wann sich Benutzer an der zugriffskonsole. 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. anmelden können.

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.

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.

Benutzerkonten für Passwortrücksetzung: Benutzern das Festlegen von Passwörtern erlauben

Benutzer und Sicherheit | BENUTZER

Benutzerkonten

Administratoren können durch die Erteilung von Benutzerberechtigungen die Zurücksetzung 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.

> ***Hinweis:*** *Administratoren mit der Berechtigung* ***Berechtigt, Kennwörter festzulegen*** *werden keinen Unterschied in der Benutzeroberfläche erkennen.*

Wenn ein berechtigter Benutzer ohne Administratorrechte zur Seite **Benutzer und Sicherheit > Benutzer** in der /login-Verwaltungsschnittstelle navigiert, wird er einen eingeschränkt sichtbaren **Benutzerkonten**-Bildschirm sehen, welcher Schaltflächen 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.

Nach Benutzern suchen

Suchen Sie nach bestimmten Benutzerkonten basierend auf Benutzername, Anzeigename oder E-Mail-Adresse.

Fehlgeschlagene Anmeldungsversuche zurücksetzen und Konto entsperren

Wenn ein Benutzer einen oder mehr fehlgeschlagene Anmeldungsversuche aufweist, klicken Sie auf die Schaltfläche **Zurücksetzen** für sein Benutzerkonto, um den Zähler zurück auf Null zu setzen.

Wenn ein Benutzer aufgrund von zu vielen fehlgeschlagenen aufeinanderfolgenden Anmeldeversuchen gesperrt wird, klicken Sie auf die Schaltfläche **Konto entsperren** für sein Benutzerkonto, um die Zahl wieder auf Null zurückzusetzen und sein Konto zu entsperren.

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

Benutzername, wie in Teamchats, Berichten usw. gezeigt.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 dem Benutzer eine E-Mail, 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.

Zugriffseinladung: Erstellen Sie Profile, um externe Benutzer zu Sitzungen einzuladen

Benutzer und Sicherheit	ZUGRIFFSEINLADUNG

Auf E-Mail-Einladung zugreifen

Mit der Zugriffseinladung kann ein berechtigter Benutzer einen externen Benutzer zur einmaligen Teilnahme an einer Sitzung einladen. Wenn der Benutzer die Einladung erteilt, wählt er ein Sicherheitsprofil aus, um zu bestimmen, welche Berechtigungsstufe dem externen Benutzer gewährt werden soll. Sicherheitsprofile für Zugriffseinladungen werden als Sitzungsrichtlinien auf der Seite **Benutzer und Sicherheit > Sitzungsrichtlinien** konfiguriert und müssen für die Nutzung von Zugriffseinladungen aktiviert werden.

Die Einladungs-E-Mail wird an externe Benutzer gesandt, wenn Sie diese zur Sitzung einladen.

Betreff

Passen Sie den Betreff dieser E-Mail an. Klicken Sie auf den Link unter dem Feld **Text**, um die Makros anzuzeigen, die Ihnen für die Anpassung Ihrer E-Mails nach Wunsch zur Verfügung stehen.

Text

Passen Sie den Text dieser E-Mail an. Klicken Sie auf den Link unter dem Feld **Text**, um die Makros anzuzeigen, die Ihnen für die Anpassung Ihrer E-Mails nach Wunsch zur Verfügung stehen.

> *Für weitere Informationen siehe Einladen eines externen Benutzers zur Teilnahme an einer Zugriffssitzung unter https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/access-invite.htm.*

Sicherheitsanbieter: Aktivieren von LDAP-, RADIUS-, Kerberos-, SCIM- und SAML2-Anmeldungen

Benutzer und Sicherheit | SICHERHEITSANBIETER

Sicherheitsanbieter

Sie können Ihr BeyondTrust Appliance B Series für die Authentifizierung von Benutzern anhand bestehender LDAP-, RADIUS-, SCIM-, SAML2- oder Kerberos-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.

Anbieter hinzufügen

Wählen Sie über das Dropdown-Menü **Hinzufügen** LDAP, RADIUS, Kerberos, SCIM oder SAML2, um eine neue Sicherheitsanbieter-Konfiguration hinzuzufügen.

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.

Deaktivieren

Diese Sicherheitsanbieter-Verbindung deaktivieren. Dies ist für Routinewartungen hilfreich, bei denen ein Server offline genommen, aber nicht gelöscht werden soll.

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.

Protokoll anzeigen

Sehen Sie sich den Statusverlauf für die Verbindung zu einem Sicherheitsanbieter an.

Knoten duplizieren

Erstellen Sie eine Kopie einer bestehenden, in einem Cluster befindlichen Sicherheitsanbieter-Konfiguration. Diese wird als neuer Knoten im gleichen Cluster hinzugefügt.

Auf einen 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.

Bearbeiten, löschen

Bearbeiten oder entfernen Sie ein bestehendes Objekt.

> ***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.*

Bearbeiten des Sicherheitsanbieters – LDAP

Name

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

Aktiviert

Falls aktiviert, kann Ihr B Series Appliance diesen Sicherheitsanbieter durchsuchen, wenn sich ein Benutzer anmeldet. Falls nicht aktiviert, wird dieser Sicherheitsanbieter nicht durchsucht.

Benutzerauthentifizierung

Geben Sie an, ob dieser Anbieter für die Authentifizierung von Benutzern verwendet werden soll. Ist diese Option nicht ausgewählt, sind die für die Benutzerauthentifizierung spezifischen Optionen deaktiviert.

Benutzerbereitstellung

Die Benutzerbereitstellung erfolgt standardmäßig über diesen Anbieter. Wenn Sie einen SCIM-Anbieter eingerichtet haben, können Sie es einrichten, dass Benutzer stattdessen über diesen Anbieter bereitgestellt werden. Wird dieser Anbieter nicht für die Benutzerauthentifizierung verwendet, ist **Benutzer nicht bereitstellen** ausgewählt.

> ***Hinweis:*** *Diese Einstellung kann nach dem Speichern dieses Sicherheitsanbieters nicht mehr geändert werden.*

Benutzerinformationen mit LDAP-Server synchronisiert lassen

Ist diese Option aktiviert, ist der Anzeigename eines Benutzers der vom Sicherheitsanbieter festgelegte Name, und der Anzeigename kann in BeyondTrust nicht geändert werden.

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. Ist die Option **Benutzerauthentifizierung** oben nicht aktiviert, ist **Gruppen mit diesem Anbieter suchen** ausgewählt. Die Option zur Suche nach Gruppen mit einem anderen Anbieter ist nur dann verfügbar, wenn bereits ein anderer Anbieter für die Gruppensuche erstellt worden ist.

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 zugriffskonsole anmelden kann. Sie können eine standardmäßige Gruppenrichtlinie wählen, die für alle Benutzer gelten soll, die sich am konfigurierten Server authentifizieren können.

Beachten Sie: 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

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 **access.example.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.

Benutzername

Geben Sie einen Benutzernamen für die Anmeldedatenbindung ein.

Passwort und Bestätigung des Passworts

Geben Sie ein Passwort für die Anmeldedatenbindung ein und bestätigen Sie es.

Verbindungsmethode

Wenn Sie einen externen Verzeichnisspeicher im gleichen lokalen Netzwerk wie Ihr B Series Appliance 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.

> ***Hinweis:*** *BeyondTrust Cloud-Kunden müssen den Verbindungsagenten ausführen, um einen externen Verzeichnisspeicher nutzen zu können.*

Verzeichnistyp

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 nicht 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 Benutzerkennung, den Anzeigenamen und die E-Mail-Adresse 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

Dies legt fest, welches Feld als E-Mail-Adresse des Benutzers verwendet werden soll.

Anzeigename

Dies legt fest, welches Feld als Anzeigename des Benutzers verwendet werden soll.

Gruppenschemaeinstellungen *(Nur bei der Durchführung von Gruppensuchen sichtbar)*

Verzeichnistyp

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.

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 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 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

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. Beachten Sie, dass für den erfolgreichen Test dieser Funktionen diese in Ihrem Sicherheitsanbieter unterstützt und konfiguriert sein müssen.

Test starten

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.

Bearbeiten des Sicherheitsanbieters – RADIUS

Name

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

Aktiviert

Falls aktiviert, kann Ihr B Series Appliance diesen Sicherheitsanbieter durchsuchen, wenn sich ein Benutzer anmeldet. Falls nicht aktiviert, wird dieser Sicherheitsanbieter nicht durchsucht.

Anzeigenamen mit Remote-System synchronisiert lassen

Ist diese Option aktiviert, ist der Anzeigename eines Benutzers der vom Sicherheitsanbieter festgelegte Name, und der Anzeigename kann in BeyondTrust nicht geändert 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.

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.

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 zugriffskonsole anmelden kann. Sie können eine standardmäßige Gruppenrichtlinie wählen, die für alle Benutzer gelten soll, die sich am konfigurierten Server authentifizieren können.

Beachten Sie: 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

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 B Series Appliance 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. Beachten Sie, dass für den erfolgreichen Test dieser Funktionen diese in Ihrem Sicherheitsanbieter unterstützt und konfiguriert sein müssen.

Test starten

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.

Bearbeiten des Sicherheitsanbieters – Kerberos

Name

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

Aktiviert

Falls aktiviert, kann Ihr B Series Appliance diesen Sicherheitsanbieter durchsuchen, wenn sich ein Benutzer anmeldet. Falls nicht aktiviert, wird dieser Sicherheitsanbieter nicht durchsucht.

Anzeigenamen mit Remote-System synchronisiert lassen

Ist diese Option aktiviert, ist der Anzeigename eines Benutzers der vom Sicherheitsanbieter festgelegte Name, und der Anzeigename kann in BeyondTrust nicht geändert 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 B Series Appliance authentifizieren können. **Alle Benutzer zulassen** gestattet es allen, die sich aktuell über Ihr 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.

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.

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.

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 zugriffskonsole anmelden kann. Sie können eine standardmäßige Gruppenrichtlinie wählen, die für alle Benutzer gelten soll, die sich am konfigurierten Server authentifizieren können.

Beachten Sie: 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.*

Bearbeiten des Sicherheitsanbieters – SAML2

Name

Geben Sie einen eindeutigen Namen ein, um Ihren Anbieter leichter zu identifizieren.

Aktiviert

Falls aktiviert, kann Ihr B Series Appliance diesen Sicherheitsanbieter durchsuchen, wenn sich ein Benutzer anmeldet. Falls nicht aktiviert, wird dieser Sicherheitsanbieter nicht durchsucht.

Benutzerbereitstellung

Die Benutzerbereitstellung erfolgt standardmäßig über diesen Anbieter. Wenn Sie einen SCIM-Anbieter eingerichtet haben, können Sie es einrichten, dass Benutzer stattdessen über diesen Anbieter bereitgestellt werden.

> ***Hinweis:*** *Diese Einstellung kann nach dem Speichern dieses Sicherheitsanbieters nicht mehr geändert werden.*

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

Identitätsanbieter-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 **Datei wählen**, um die ausgewählte Datei auszuwählen und hochzuladen.

> ***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.*

Entitäts-ID

Hierbei handelt es sich um die eindeutige Kennung für den Identitätsanbieter, den Sie verwenden.

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

So wird festgelegt, ob ein HTTP-POST erfolgt oder oder der Benutzer an die Anmelde-URL weitergeleitet wird. Dies sollte, sofern vom Identitätsanbieter nicht anderweitig erfordert, als Weiterleitung belassen werden.

Server-Zertifikat

Dieses Zertifikat dient dazu, die vom Identitätsanbieter gesendete Signatur der Assertion zu verifizieren.

Serviceanbieter-Einstellungen

Serviceanbieter-Metadaten

Laden Sie die BeyondTrust-Metadaten herunter. Diese müssen Sie dann bei Ihrem Identitätsanbieter hochladen.

Entitäts-ID

Dies ist Ihre BeyondTrust-URL. Diese bietet eine eindeutige Kennung Ihrer Website gegenüber dem Identitätsanbieter.

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.

Einstellungen der Benutzerattribute *(nur sichtbar, wenn dieser Anbieter für die Benutzerbereitstellung verwendet wird)*

SAML-Benutzerattribute

Diese Attribute werden verwendet, um Benutzer innerhalb von BeyondTrust bereitzustellen. 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.

Authorisierungseinstellungen *(nur sichtbar, wenn dieser Anbieter für die Benutzerbereitstellung verwendet wird)*

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

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 zugriffskonsole anmelden kann. Sie können eine standardmäßige Gruppenrichtlinie wählen, die für alle Benutzer gelten soll, die sich am konfigurierten Server authentifizieren können.

Beachten Sie: 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.*

Weitere Informationen siehe SAML für die Einzelanmeldung unter https://www.beyondtrust.com/docs/privileged-remote-access/how-to/integrations/security-providers/saml/index.htm.

Bearbeiten des Sicherheitsanbieters – SCIM

Hinweis: *Damit SCIM verwendet werden kann, muss die SCIM-API in einem API-Konto aktiviert sein, und die API muss bei Ihrem SCIM-Anbieter konfiguriert sein. API-Konten werden unter* ***/login > Verwaltung > API-Konfiguration*** *verwaltet. Zu diesem Zeitpunkt kann nur ein SCIM-Anbieter erstellt werden. Sobald ein SCIM-Anbieter erstellt worden ist, ist die SCIM-Option in der Dropdown-Liste* ***Anbieter erstellen*** *nicht mehr verfügbar. Die SCIM-Benutzerbereitstellung verwendet SCIM 2.0-Benutzer und -Gruppenobjekte. Weitere Informationen zum SCIM 2.0-Standard finden Sie unter https://scim.cloud/.*

> **Hinweis:** *Privileged Remote Access unterstützt nun SCIM-APIs für Benutzergruppen. Sobald Sie in /login einen SCIM-Anbieter und Benutzer und Benutzergruppen in Ihrer SCIM-Lösung konfiguriert haben, übernimmt PRA die Gruppen aus Ihrer SCIM-Lösung, so dass Sie Gruppenrichtlinien nach SCIM-Gruppe auswählen können.*

Name

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

Aktiviert

Falls aktiviert, kann Ihr B Series Appliance diesen Sicherheitsanbieter durchsuchen, wenn sich ein Benutzer anmeldet. Falls nicht aktiviert, wird dieser Sicherheitsanbieter nicht durchsucht.

SCIM-Benutzerabfrage-ID

Wählen Sie aus der Dropdown-Liste die eindeutige Kennung aus, die SCIM für Benutzerabfragen verwenden sollte.

SCIM-Gruppenabfrage-ID

Wählen Sie aus der Dropdown-Liste die eindeutige Kennung aus, die SCIM für Gruppenabfragen verwenden sollte.

Benutzerbereitstellungseinstellungen

Benutzerattribut

Diese Attribute werden verwendet, um Benutzer innerhalb von BeyondTrust bereitzustellen. Die Standardwerte entsprechen von BeyondTrust zertifizierten Anwendungen mit verschiedenen Identitätsanbietern.

Autorisierungseinstellungen

Eindeutige ID

Geben Sie das SCIM-Attribut ein, das als eindeutige Kennung des Benutzers in BeyondTrust verwendet werden soll.

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 zugriffskonsole anmelden kann. Sie können eine standardmäßige Gruppenrichtlinie wählen, die für alle Benutzer gelten soll, die sich am konfigurierten Server authentifizieren können.

Beachten Sie: 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.*

Attributname

Geben Sie den Namen des SCIM-Attributs ein, das die Benutzer eindeutig identifiziert.

Die mit SCIM bereitgestellten Gruppen werden stets ohne Beachtung von Groß-/Kleinschreibung anhand ihres Namens für Gruppensuchzwecke eindeutig identifiziert.

Anbietergruppen

Benutzer und Sicherheit	ANBIETER

Erstellen Sie Anbietergruppen, um Drittanbieter-Benutzern einen kontrollierten Zugriff auf Systeme zu ermöglichen. Dies kann für Support, Wartung oder andere Aufgaben, die den Zugriff auf das System erfordern, erforderlich sein. Sie können bis zu 100 Anbietergruppen konfigurieren.

Neue Anbietergruppe hinzufügen

Name

Geben Sie einen Namen für diese Anbietergruppe ein.

Autorisierungseinstellungen

Gruppenrichtlinie

In der ausgewählten Gruppenrichtlinie werden die Berechtigungen, Mitgliedschaften und anderen Einstellungen für alle Benutzer definiert, die sich bei diesem Anbieter authentifizieren. Diese Einstellungen können nicht auf Benutzerbasis geändert werden. Wählen Sie eine Richtlinie aus den verfügbaren aus, oder gehen Sie zu **Benutzer und Sicherheit > Gruppenrichtlinien**, um eine neue zu erstellen.

> **Hinweis:** *Gruppenrichtlinien, die administrative Berechtigungen gewähren, sind für Anbieter nicht verfügbar.*

Konto läuft ab nach

Legen Sie die Anzahl der Tage fest, nach denen das Konto deaktiviert werden soll.

PRA Benutzer

Klicken Sie, um einen Administrator oder einen Benutzer von der Liste auszuwählen. Der ausgewählte Benutzer kann die Anbieter-Benutzer in dieser Gruppe und einige Selbstregistrierungseinstellungen verwalten. Dieser Benutzer erhält alle konfigurierten Admin-Benachrichtigungen für diese Anbietergruppe und sollte über eine gültige E-Mail-Adresse verfügen.

Hinweis: *Jeder PRA-Benutzer kann von einem PRA-Administrator beauftragt werden, die Verwaltung dieser Anbietergruppe zu übernehmen, nachdem sie erstellt wurde. Der PRA-Benutzer hat nicht die Berechtigung/Rechte, die für den Anbieter spezifischen Sicherheitseinstellungen zu ändern. Vielmehr ist der PRA-Benutzer der designierte Genehmiger, Empfänger von Benachrichtigungen und hat Sichtbarkeit und Bearbeitungsrechte in Bezug auf die Anbieter-Benutzer selbst.*

Benachrichtigen Sie den PRA-Benutzer, wenn ein Benutzer zu dieser Anbietergruppe hinzugefügt wird

Wenn dieses Kontrollkästchen aktiviert ist, wird jedes Mal eine E-Mail an den PRA-Administrator oder den für die Gruppe zuständigen Benutzer gesendet, wenn ein neuer Benutzer hinzugefügt wird. Sie können für neue Mitglieder eine PRA-Genehmigung verlangen. Wenn eine Genehmigung erforderlich ist, wird neben dem Namen des neuen Mitglieds in der Liste der Gruppenmitglieder eine Meldung angezeigt, die besagt, dass der Benutzer eine **Genehmigung benötigt**.

Benachrichtigen Sie den PRA-Benutzer, wenn ein Benutzer in dieser Anbietergruppe abgelaufen ist

Wenn dieses Kontrollkästchen aktiviert ist, erhält der Administrator oder der für die Gruppenbenutzer zuständige Benutzer eine E-Mail, wenn ein Benutzer abgelaufen ist, sowie einen Link, um den Benutzer erneut zu aktivieren, falls dies gewünscht wird.

Erfordert die Genehmigung des PRA-Benutzers zur Aktivierung von Benutzern in dieser Anbietergruppe

Wenn dieses Kontrollkästchen aktiviert ist, muss ein PRA-Administrator oder der für die Gruppe zuständige Benutzer neue Mitglieder genehmigen.

Erfordert die Genehmigung des PRA-Benutzers, um Benutzer in dieser Anbietergruppe zu erweitern oder zu reaktivieren

Wenn dieses Kontrollkästchen aktiviert ist, muss ein PRA-Administrator oder der für die Gruppe zuständige Benutzer die Erweiterung oder erneute Aktivierung von Benutzern in dieser Anbietergruppe genehmigen.

E-Mail an PRA-Benutzer, wenn Benutzer auf Aktion warten, nach

Wenn dieses Kontrollkästchen aktiviert ist, erhält der PRA-Administrator oder der für die Gruppe zuständige Benutzer eine E-Mail-Benachrichtigung, wenn Benutzer nach einem bestimmten Zeitraum auf eine Aktion warten. Der Standardwert ist ein Tag, aber in der Dropdown-Liste unter dem Kontrollkästchen sind Zeiträume von einer Stunde bis zu einer Woche verfügbar.

Netzwerkbeschränkungen

Netzwerkadressen-Zulassungsliste

Geben Sie die Netzwerkadresspräfixe (einen pro Zeile) in den in den Beispielen gezeigten Formaten 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.

Benutzer, die eine Aktion erfordern

Hier werden die Benutzer aufgeführt, die eine Aktion des Administrators oder des für die Anbietergruppe zuständigen Benutzers erfordern. Unter **Aktion erforderlich** finden Sie das Problem, das Ihre Aufmerksamkeit erfordert. Die aufgelisteten Probleme sind **Deaktiviert**, **Abgelaufen**, **Fehlgeschlagene Anmeldung**, **Gesperrt**, **Benötigt Genehmigung** und **Ausstehend**.

Benutzer

Klicken Sie auf **Hinzufügen**, um Mitglieder zu einer bestehenden Gruppe hinzuzufügen. Sie können das Suchfeld verwenden, um nach aufgelisteten Benutzern via **Zuletzt authentifiziert als**, **Anzeigename** und **E-Mail-Adresse** zu suchen. Über das Einstellungssymbol auf der rechten Seite können Sie auswählen, welche Spaltenkategorien mit Benutzerinformationen angezeigt werden sollen. Die Optionen sind **Zuletzt authentifiziert als**, **Anzeigename**, **E-Mail-Adresse**, **Datum der letzten Authentifizierung**, **Administrator** und **Ablaufdatum**.

Anbieterportal-Einstellungen

Sie können das Portal für die Anbieter-Selbstregistrierung anpassen, das Benutzer bei der Registrierung sehen. Änderungen werden erst nach dem Speichern der Anbietergruppe übernommen.

Anbieterportal aktivieren

Aktivieren Sie das Kontrollkästchen, um das Anbieterportal zu aktivieren. Diese Funktion kann nur nach Auswahl einer Gruppenrichtlinie unter **Berechtigungseinstellungen** aktiviert werden.

Logo hochladen

Klicken Sie, um ein Logo hochzuladen. Dies kann Ihr Logo oder das Logo des Anbieters sein, je nach Ihren Bedürfnissen und Vorlieben. Für das beste Ergebnis sollten Sie ein Bild mit den Abmessungen 128 x 128 Pixel verwenden. Sie können zwei Akzentfarben und eine Hintergrundfarbe festlegen:

- **Akzentfarbe 1:** Steuert die Hintergrundfarbe der Bereichs-Kopfzeile, die Rahmenfarbe und die dunkle Textfarbe.
- **Akzentfarbe 2:** Steuert die Farbe des Links, die Hintergrundfarbe der Schaltfläche und die Farbe des Sprachglobus.

Klicken Sie auf **Auf Standard zurücksetzen**, wenn Sie die vorgenommenen Änderungen nicht beibehalten möchten.

Portal-Anweisungen

Geben Sie den Text ein, der Benutzern angezeigt wird, wenn sie sich im Selbstregistrierungsportal registrieren.

Betreff der E-Mail

Der E-Mail-Betreff, den Benutzer sehen, wenn sie ihre Bestätigungs-E-Mail erhalten, nachdem sie sich über das Selbstregistrierungsportal registriert haben.

Text der E-Mail

Geben Sie den Text für die Bestätigungs-E-Mail ein, die an Benutzer gesendet wird, nachdem sie das Registrierungsformular abgeschickt haben.

Anbieterportal-URL

Geben Sie die URL für die Benutzerregistrierungs-Website ein.

E-Mail-Domänen-Zulassungsliste

Sie können die E-Mail-Adressen auf die hier aufgeführten Domänen beschränken, wenn sich Benutzer über das Portal registrieren. Geben Sie eine E-Mail-Domäne pro Zeile ein. Kommata und Leerzeichen sind nicht zulässig. Wenn nichts angegeben wird, gibt es keine Einschränkungen für zulässige E-Mail-Adressen.

Konfigurierbarer Slug

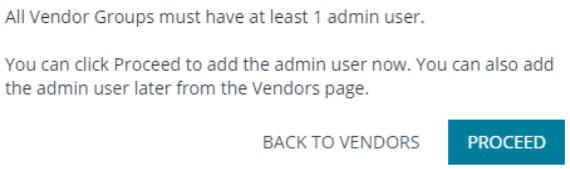
Geben Sie den URL-Slug für Ihre Website ein.

Wenn Sie fertig sind, klicken Sie auf **Vorschau des Anbieterportals**, um zu sehen, wie das Portal aussehen wird.

Anbietergruppen-Administrator zufügen

Anbietergruppen-Administratoren

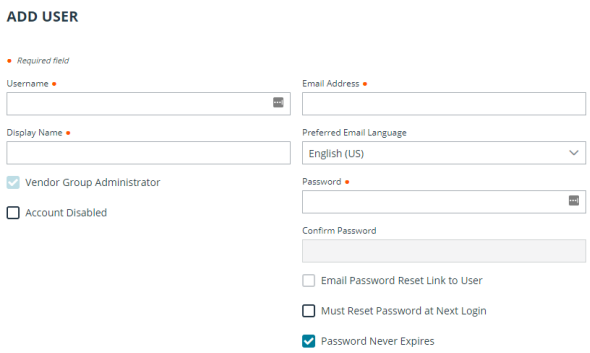
Nachdem Sie auf **Speichern** für die neu erstellte Anbietergruppe geklickt haben, werden Sie darauf hingewiesen, dass allen Anbietergruppen ein Benutzer als Anbieter-Administrator zugewiesen sein muss. Sie können entweder auf **Fortfahren** klicken, um einen Anbieter-Administrator zuzuweisen, oder den Admin-Benutzer später auf der **Anbieter**-Seite hinzufügen.



> ***Hinweis:*** *Anbieter-Admins können keine anderen Anbieter-Admins hinzufügen.*

Benutzer hinzufügen

Wenn Sie einen Anbietergruppen-Admins hinzufügen, stellen Sie sicher, dass das Feld **Anbietergruppen-Administrator** markiert ist.



Sitzungsrichtlinien: Sitzungsberechtigungen und Aufforderungsregeln festlegen

Benutzer und Sicherheit | SITZUNGSRICHTLINIEN

Sitzungsrichtlinien

Mit Sitzungsrichtlinien können Sie die Sicherheitsberechtigungen für Sitzungen Tech. auf bestimmte Szenarien zuschneiden. Sitzungsrichtlinien können auf Benutzer und alle Jump-Items angewendet werden.

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, Zugriffseinladungen und Jump Clients sie verfügbar ist, und für welche Tools sie konfiguriert wurde.

Hinzufügen, Bearbeiten, oder Löschen der Sitzungsrichtlinie

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

Anzeigename

Erstellen Sie einen eindeutigen Namen, um diese Richtlinie leichter zu identifizieren. Dieser Name hilft bei der Zuweisung einer Sitzungsrichtlinie zu Benutzern und Jump Clients.

Codename

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

Beschreibung

Fügen Sie eine kurze Beschreibung hinzu, um den Zweck dieser Richtlinie zusammenzufassen. Die Beschreibung wird angezeigt, wenn eine Richtlinie auf Benutzerkonten, Gruppenrichtlinien und Zugriffseinladungen angewandt wird.

Verfügbarkeit

Benutzer

Wählen Sie, ob diese Richtlinie zur Zuweisung an Benutzer (Benutzerkonten und Gruppenrichtlinien) zur Verfügung stehen soll.

Zugriffseinladung

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, sehen Sie die Anzahl der Benutzer und Jump Clients, welche die 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**.

Legen Sie fest, welche Tools mit dieser Richtlinie aktiviert oder deaktiviert werden sollen.

Heraufgesetzten Zugriff auf Werkzeuge und Sonderaktionen am Endpunkt erlauben

Wenn aktiviert, wird der Zugriff auf die erweiterte Funktionalität in der zugriffskonsole für diese Sitzung ermöglicht, ohne dass die expliziten Rechte eines eingeloggten Benutzers auf dem entfernten Endpunkt benötigt werden.

Wenn diese Einstellung deaktiviert ist, verhindert sie, dass Benutzer vollen Zugriff auf die Dateiübertragungs- und Befehlsshell-Funktionen erhalten, wenn sie einen Jump zu einem heraufgesetzten Jump-Item ausführen, aber keine heraufgesetzten Rechte haben. Dazu werden spezielle Aktionen und Aktionen zur Leistungssteuerung ausgeblendet und sind nicht verfügbar. Sie beschränkt auch die **Dateiübertragung**, die **Befehlsshell** und den **Registrierungszugriff**, wenn kein Benutzer in der Sitzung anwesend ist. Diese Einstellung wird angewendet, wenn sie von der Plattform des Endpunkts zugelassen wird.

Bildschirmfreigabe

Bildschirmfreigabe-Regeln

Wählen Sie den Zugriff des Support-Technikers und des Remote-Benutzers am Remote-System:

- 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.
- **Ablehnen** deaktiviert die Bildschirmfreigabe.
- **Nur Ansicht** ermöglicht es dem Support-Techniker, den Bildschirm zu sehen.
- **Ansicht und Steuerung** ermöglicht es dem Support-Techniker, das System einzusehen und Maßnahmen zu ergreifen. Wenn diese Option ausgewählt ist, können Endpunktbeschränkungen festgelegt werden, um Störungen durch den Remote-Benutzer zu vermeiden:
    - **Keine** legt keine Einschränkungen für das Remote-System fest.
    - **Bildschirm, Maus und Tastatur** deaktiviert diese Eingänge. Wenn diese Option aktiviert ist, steht ein Kontrollkästchen zur Verfügung, um **Automatisch den Bildschirm „Privatsphäre“ bei Sitzungsbeginn anzufordern**. 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.

Gestattete Endpunkteinschränkungen

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.

Synchronisierungsrichtung für Zwischenablage

Wählen Sie, wie der Inhalt der Zwischenablage zwischen Benutzern und Endpunkten ausgetauscht wird. Die Optionen sind:

- **Nicht berechtigt**: Der Benutzer darf die Zwischenablage nicht verwenden, es werden keine Zwischenablage-Symbole im zugriffskonsole angezeigt, und die Befehle zum Ausschneiden und Einfügen funktionieren nicht.
- **Zulässig vom Support-Techniker zum Kunden:** Der Benutzer kann den Inhalt der Zwischenablage an den Endpunkt weiterleiten, kann aber nicht aus der Zwischenablage des Endpunkts einfügen. Nur das Zwischenablage-Symbol **Senden** wird im zugriffskonsole angezeigt.
- **Zulässig in beide Richtungen:** Der Inhalt der Zwischenablage kann in beide Richtungen übertragen werden. Beide Symbole Zwischenablage senden und abrufen werden im zugriffskonsole angezeigt.

Weitere Informationen über den Zwischenablage-Synchronisationsmodus finden Sie unter „Sicherheit: Verwalten der Sicherheitseinstellungen“ auf Seite 159.

Anwendungsfreigabebeschränkungen

Beschränken Sie den Zugriff auf angegebene Anwendungen auf dem Remote-System entweder mit **Nur die aufgeführten ausführbaren Dateien gestatten** oder **Nur die aufgeführten ausführbaren Dateien ablehnen**. Ebenfalls können Sie den Desktop-Zugriff zulassen oder verbieten.

Hinweis: *Diese Funktion gilt nur für Windows-Betriebssysteme.*

Neue ausführbare Dateien hinzufügen

Wenn Anwendungsfreigabebeschränkungen durchgesetzt werden, erscheint eine neue Schaltfläche **Neue ausführbare Dateien hinzufügen**. Mit Klick auf diese Schaltfläche wird ein Dialogfenster geöffnet, in dem Sie ausführbare Dateien angeben können, die gemäß Ihrer Ziele abgelehnt oder gestattet werden sollen.

Nach dem Hinzufügen von ausführbaren Dateien zeigen eine oder zwei Tabellen die Dateinamen oder Hashes an, die zur Einschränkung ausgewählt wurden. Ein bearbeitbares Kommentarfeld ermöglicht Administrationsnotizen.

Geben Sie Dateinamen oder SHA-256-Hashes ein, einen pro Zeile

Geben Sie bei der Einschränkung von ausführbaren Dateien die Dateinamen oder Hashes der ausführbaren Dateien, die sie gestatten oder verbieten möchten, manuell ein. Klicken Sie auf **Ausführbare Datei(en) hinzufügen**, wenn Sie fertig sind, um die gewählten Dateien zu Ihrer Konfiguration hinzuzufügen.

Pro Dialog können bis zu 25 Dateien angegeben werden. Wenn Sie mehr hinzufügen müssen, klicken Sie auf **Ausführbare Datei(en) hinzufügen** und öffnen Sie den Dialog dann erneut.

Navigieren zu einer oder mehreren Dateien

Wählen Sie bei der Beschränkung von ausführbaren Dateien diese Option, um auf Ihrem System zu ausführbaren Dateien zu navigieren und ihre Namen oder Hashes automatisch abzuleiten. Wenn Sie Dateien so auf Ihrer lokalen Plattform bzw. Ihrem lokalen System auswählen, stellen Sie sicher, dass es sich bei den Dateien tatsächlich um ausführbare Dateien handelt. Dies wird auf Browserebene nicht überprüft.

Wählen Sie entweder **Dateiname benutzen** oder **Datei-Hash benutzen**, damit der Browser die Dateinamen oder Hashes der ausführbaren Dateien automatisch ableitet. Klicken Sie auf **Ausführbare Datei(en) hinzufügen**, wenn Sie fertig sind, um die gewählten Dateien zu Ihrer Konfiguration hinzuzufügen.

Pro Dialog können bis zu 25 Dateien angegeben werden. Wenn Sie mehr hinzufügen müssen, klicken Sie auf **Ausführbare Datei(en) hinzufügen** und öffnen Sie den Dialog dann erneut.

Hinweis: *Diese Option ist nur in modernen und nicht in älteren Browsern verfügbar.*

Berechtigt, sich mit Anmeldedaten eines Endpunkt-Anmeldedaten-Managers anzumelden

Ermöglichen Sie es einem Benutzer, sich mit Ihrem Endpoint Credential Manager zu verbinden, um Anmeldedaten aus Ihren bestehenden Passwortspeichern oder Vaults zu verwenden.

Die Verwendung des Endpunkt-Anmeldedaten-Managers erfordert eine separate Dienstleistungsvereinbarung mit BeyondTrust. Nach Abschluss einer Dienstleistungsvereinbarung können Sie die erforderliche Middleware vom BeyondTrust Support-Portal herunterladen.

Hinweis: *Vor 15.2 war diese Funktion nur in Sitzungen verfügbar, die auf Windows® über einen heraufgesetzten Jump-Client gestartet wurden. Ab 15.2 können Sie auch den Endpoint Credential Manager in Remote-Jump-Sitzungen, Microsoft® Remote Desktop Protocol-Sitzungen, VNC-Sitzungen und Shell Jump-Sitzungen verwenden. Auf einem Windows®-System können Sie diese Funktion auch mit der speziellen Aktion „Ausführen als“ in einer Bildschirmfreigabesitzung verwenden.*

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.

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 Endpunkts

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 Benutzers

Gestattet es Benutzern, Dateien direkt zu oder von jeglichen oder nur von bestimmten Verzeichnissen auf seinem lokalen System zu übertragen.

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.*

Konfigurieren der Befehlsfilterung, um eine versehentliche Nutzung von Befehlen, die für Endpunkt-Systeme schädlich sein können, zu vermeiden.

> *Weitere Informationen zur Befehlsfilterung finden Sie unter Shell Jump zum Zugriff auf ein Remote-Netzwerkgerät verwenden unter www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/shell-jump.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.

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.

Vordefinierte Skripts

Regeln für vordefinierte Skripts

Damit kann der Benutzer vordefinierte Skripts ausführen, die für seine Teams erstellt wurden. 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.

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.

Speichern

Klicken Sie auf **Speichern**, um diese 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.

Benutzer

Beginnen Sie, indem Sie den Benutzer auswählen, der die Sitzung durchführt. Diese Dropdown-Liste enthält sowohl Benutzerkonten wie auch Zugriffseinladungsrichtlinien.

Sitzungsstartmethode

Wählen Sie die Methode für den Sitzungsstart.

Jump Client / Jump-Kurzbefehl

Suchen Sie nach einem Jump Client oder Jump-Kurzbefehl mithilfe von Name, Kommentaren, Jump-Gruppe oder Tag.

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

Benutzer und Sicherheit | GRUPPENRICHTLINIEN

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

Richtliniename

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?

Wählen Sie für jede Einstellung, ob sie in dieser Richtlinie definiert werden oder für die Konfiguration für einzelne Benutzer verfügbar bleiben soll. Ist sie definiert, können Sie diese Berechtigung nicht mehr für einen einzelnen Benutzer über dessen Benutzerkontoseite ändern.

Falls Sie eine Richtlinie verwenden, die eine Berechtigung definiert, und nicht möchten, dass eine Richtlinie diese Berechtigung ersetzen können soll, müssen Sie auswählen, dass die Berechtigung nicht überschrieben werden kann. Die Richtlinie muss dann höhere Priorität als andere Richtlinien haben durch die diese Einstellung zusätzlich definiert wird.

Zwei-Faktor-Authentifizierung

Die Zwei-Faktor-Authentifizierung (2FA) nutzt eine Authentifikator-App, um einen zeitbasierten, einmaligen Code zur Anmeldung in der Verwaltungsschnittstelle und der Zugriffskonsole bereitzustellen. Wenn **Erforderlich** gewählt wird, wird der Benutzer bei der nächsten Anmeldung aufgefordert, sich für 2FA zu registrieren und diese Methode zu nutzen. Wenn **Optional** gewählt wird, hat der Benutzer die Option, 2FA zu nutzen, ist aber nicht dazu verpflichtet.

Kontoablauf

Ist ein Haken gesetzt, läuft das Konto nie ab. Ist kein Haken gesetzt, muss ein Ablaufdatum für das Konto festgelegt werden.

Konto deaktiviert

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

Kommentare

Fügen Sie Kommentare hinzu, die den Zweck dieses Objekts deutlich machen.

Allgemeine Berechtigungen

Welche allgemeinen Einstellungen soll diese Gruppenrichtlinie regeln?

Wählen Sie für jede Einstellung, ob sie in dieser Richtlinie definiert werden oder für die Konfiguration für einzelne Benutzer verfügbar bleiben soll. Ist sie definiert, können Sie diese Berechtigung nicht mehr für einen einzelnen Benutzer über dessen Benutzerkontoseite ändern.

Falls Sie eine Richtlinie verwenden, die eine Berechtigung definiert, und nicht möchten, dass eine Richtlinie diese Berechtigung ersetzen können soll, müssen Sie auswählen, dass die Berechtigung nicht überschrieben werden kann. Die Richtlinie muss dann höhere Priorität als andere Richtlinien haben durch die diese Einstellung zusätzlich definiert wird.

Verwaltung

Administratorrechte

Erteilt dem Benutzer volle Administratorrechte.

Vault-Administratorrechte

Ermöglicht dem Benutzer den Zugriff auf Vault.

Passworteinstellung

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

Bearbeiten des Jumpoint

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.

Bearbeiten von Teams

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

Bearbeiten der Jump-Gruppe

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

Bearbeitung vordefinierter Skripts

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

Bearbeiten von benutzerdefinierten Links

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

Bericht wird erstellt

Zugriff auf Sitzungs- und Teamberichte

Berechtigt den Benutzer, Berichte zu Zugriffssitzungen anzuzeigen. Je nach gewählter Option können Benutzer ihre Sitzungen, die Sitzungen ihrer Jump-Gruppe oder alle Sitzungen anzeigen.

Berechtigt, Berichte zu Zugriffssitzungen anzuzeigen

Ermöglicht dem Benutzer, Berichte zur Zugriffssitzung-Aktivität auszuführen, nur Sitzungen anzuzeigen, bei denen er der primäre Sitzungseigentümer war, nur Sitzungen für Endpunkte anzuzeigen, die zu einer Jump-Gruppe gehören, deren Mitglied er ist, oder alle Sitzungen.

Berechtigt, Zugriffssitzung-Aufzeichnungen anzuzeigen

Damit kann der Benutzer Videoaufzeichnungen der Bildschirmfreigabe und Befehlsshell-Sitzungen anzeigen.

Zugriff auf Vault-Berichte

Berechtigt den Benutzer, Vault-Berichte anzuzeigen. Je nach gewählter Option können Benutzer ihre Sitzungen oder alle Sitzungen anzeigen.

Berechtigt, Vault-Berichte anzuzeigen

Damit kann der Benutzer seine eigenen Vault-Ereignisse oder alle Vault-Ereignisse anzeigen.

Berechtigt, Syslog-Berichte anzuzeigen

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

Zugriffsberechtigungen

Berechtigt, auf Endpunkte zuzugreifen

Damit kann der Benutzer die zugriffskonsole verwenden, um Sitzungen durchzuführen. Wenn der Endpunkt-Zugriff aktiviert ist, sind auch Optionen für den Endpunkt-Zugriff verfügbar.

Sitzungsverwaltung

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.

Berechtigt, externe Benutzer einzuladen

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

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 zugriffskonsole angemeldet sind.

Berechtigt, externen Schlüssel zu bearbeiten

Ermöglicht es dem Benutzer, den externen Schlüssel aus dem Fenster Sitzungsinformationen einer Sitzung innerhalb der zugriffskonsole zu ändern.

Benutzer-zu-Benutzer-Bildschirmfreigabe

Berechtigt, anderen Benutzern 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 Benutzern 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.

Jump-Technologie

Gestattete Methoden für Jump-Items

Ermöglicht es dem Benutzer, mit **Jump Clients**, **Lokalem Jump im lokalen Netzwerk**, **Remote-Jump mittels Jumpoint**, **Remote-VNC mittels Jumpoint**, **Remote-RDP mittels Jumpoint**, **Web Jump mittels Jumpoint**, **Shell Jump mittels Jumpoint** und **Protokoll-Tunnel-Jump mittels Jumpoint** Jumps zu Computern auszuführen.

Jump-Element-Rollen

Eine Jump-Element-Rolle ist ein vordefinierter Berechtigungssatz zur Verwaltung und Nutzung von Jump-Elementen. Klicken Sie für jede Option auf **Anzeigen**, 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 zugriffskonsole kann dieser dann die persönlichen Listen von Jump-Elementen von Benutzern sehen, die keine Teammitglieder sind.

Sitzungsberechtigungen

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.

Beschreibung

Zeigen Sie die Beschreibung einer vordefinierten Berechtigungsrichtlinie an.

Bildschirmfreigabe

Bildschirmfreigabe-Regeln

Wählen Sie den Zugriff des Support-Technikers und des Remote-Benutzers am Remote-System:

- 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.
- **Ablehnen** deaktiviert die Bildschirmfreigabe.
- **Nur Ansicht** ermöglicht es dem Support-Techniker, den Bildschirm zu sehen.
- **Ansicht und Steuerung** ermöglicht es dem Support-Techniker, das System einzusehen und Maßnahmen zu ergreifen. Wenn diese Option ausgewählt ist, können Endpunktbeschränkungen festgelegt werden, um Störungen durch den Remote-Benutzer zu vermeiden:
    - **Keine** legt keine Einschränkungen für das Remote-System fest.
    - **Bildschirm, Maus und Tastatur** deaktiviert diese Eingänge. Wenn diese Option aktiviert ist, steht ein Kontrollkästchen zur Verfügung, um **Automatisch den Bildschirm „Privatsphäre“ bei Sitzungsbeginn anzufordern**. 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 finden Sie unter Steuern des Remote-Endpunkts mit der Bildschirmfreigabe unter https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/screen-sharing.htm.

Synchronisierungsrichtung für Zwischenablage

Wählen Sie, wie der Inhalt der Zwischenablage zwischen Benutzern und Endpunkten ausgetauscht wird. Die Optionen sind:

- **Nicht berechtigt**: Der Benutzer darf die Zwischenablage nicht verwenden, es werden keine Zwischenablage-Symbole im zugriffskonsole angezeigt, und die Befehle zum Ausschneiden und Einfügen funktionieren nicht.
- **Zulässig vom Support-Techniker zum Kunden:** Der Benutzer kann den Inhalt der Zwischenablage an den Endpunkt weiterleiten, kann aber nicht aus der Zwischenablage des Endpunkts einfügen. Nur das Zwischenablage-Symbol **Senden** wird im zugriffskonsole angezeigt.
- **Zulässig in beide Richtungen:** Der Inhalt der Zwischenablage kann in beide Richtungen übertragen werden. Beide Symbole Zwischenablage senden und abrufen werden im zugriffskonsole angezeigt.

Weitere Informationen über den Zwischenablage-Synchronisationsmodus finden Sie unter „Sicherheit: Verwalten der Sicherheitseinstellungen“ auf Seite 159.

Anwendungsfreigabebeschränkungen

Beschränken Sie den Zugriff auf angegebene Anwendungen auf dem Remote-System entweder mit **Nur die aufgeführten ausführbaren Dateien gestatten** oder **Nur die aufgeführten ausführbaren Dateien ablehnen**. Ebenfalls können Sie den Desktop-Zugriff zulassen oder verbieten.

Hinweis: *Diese Funktion gilt nur für Windows-Betriebssysteme.*

Neue ausführbare Dateien hinzufügen

Wenn Anwendungsfreigabebeschränkungen durchgesetzt werden, erscheint eine neue Schaltfläche **Neue ausführbare Dateien hinzufügen**. Mit Klick auf diese Schaltfläche wird ein Dialogfenster geöffnet, in dem Sie ausführbare Dateien angeben können, die gemäß Ihrer Ziele abgelehnt oder gestattet werden sollen.

Nach dem Hinzufügen von ausführbaren Dateien zeigen eine oder zwei Tabellen die Dateinamen oder Hashes an, die zur Einschränkung ausgewählt wurden. Ein bearbeitbares Kommentarfeld ermöglicht Administrationsnotizen.

Geben Sie Dateinamen oder SHA-256-Hashes ein, einen pro Zeile

Geben Sie bei der Einschränkung von ausführbaren Dateien die Dateinamen oder Hashes der ausführbaren Dateien, die sie gestatten oder verbieten möchten, manuell ein. Klicken Sie auf **Ausführbare Datei(en) hinzufügen**, wenn Sie fertig sind, um die gewählten Dateien zu Ihrer Konfiguration hinzuzufügen.

Pro Dialog können bis zu 25 Dateien angegeben werden. Wenn Sie mehr hinzufügen müssen, klicken Sie auf **Ausführbare Datei(en) hinzufügen** und öffnen Sie den Dialog dann erneut.

Navigieren zu einer oder mehreren Dateien

Wählen Sie bei der Beschränkung von ausführbaren Dateien diese Option, um auf Ihrem System zu ausführbaren Dateien zu navigieren und ihre Namen oder Hashes automatisch abzuleiten. Wenn Sie Dateien so auf Ihrer lokalen Plattform bzw. Ihrem lokalen System auswählen, stellen Sie sicher, dass es sich bei den Dateien tatsächlich um ausführbare Dateien handelt. Dies wird auf Browserebene nicht überprüft.

Wählen Sie entweder **Dateiname benutzen** oder **Datei-Hash benutzen**, damit der Browser die Dateinamen oder Hashes der ausführbaren Dateien automatisch ableitet. Klicken Sie auf **Ausführbare Datei(en) hinzufügen**, wenn Sie fertig sind, um die gewählten Dateien zu Ihrer Konfiguration hinzuzufügen.

Pro Dialog können bis zu 25 Dateien angegeben werden. Wenn Sie mehr hinzufügen müssen, klicken Sie auf **Ausführbare Datei(en) hinzufügen** und öffnen Sie den Dialog dann erneut.

Hinweis: *Diese Option ist nur in modernen und nicht in älteren Browsern verfügbar.*

Gestattete Endpunkteinschränkungen

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.

Weitere Informationen finden Sie unter Steuern des Remote-Endpunkts mit der Bildschirmfreigabe unter https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-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 unter Verwenden von Anmerkungen, um auf dem Remote-Bildschirm des Endpunktes zu zeichnen unter https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-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 Endpunkts

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 Benutzers

Gestattet es Benutzern, Dateien direkt zu oder von jeglichen oder nur von bestimmten Verzeichnissen auf seinem lokalen System zu übertragen.

> *Weitere Informationen finden Sie unter Dateitransfer zum und vom Remote-System-Endpunkt unter https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-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.*

Konfigurieren der Befehlsfilterung, um eine versehentliche Nutzung von Befehlen, die für Endpunkt-Systeme schädlich sein können, zu vermeiden.

> *Weitere Informationen zur Befehlsfilterung finden Sie unter Shell Jump zum Zugriff auf ein Remote-Netzwerkgerät verwenden unter www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/shell-jump.htm.*

> *Für weitere Informationen siehe Öffnen der Befehlsshell am Remote-Endpunkt mithilfe der Zugriffskonsole unter https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-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 unter Anzeige von Systeminformationen am Remote-Endpunkt unter https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-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 unter Zugriff auf den Registrierungseditor am Remote-Endpunkt unter https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/registry-editor.htm.*

Vordefinierte Skripts

Regeln für vordefinierte Skripts

Damit kann der Benutzer vordefinierte Skripts ausführen, die für seine Teams erstellt wurden. 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.

> *Für weitere Informationen siehe Öffnen der Befehlsshell am Remote-Endpunkt mithilfe der Zugriffskonsole unter https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/command-shell.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

Anmeldungszeitplan

Die Benutzeranmeldung auf den folgenden Zeitplan beschränken

Legen Sie einen Zeitplan fest, der definiert, wann sich Benutzer an der zugriffskonsole. 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. anmelden können.

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

Teammitgliedschaft 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 zugriffskonsole 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.

Teammitgliedschaft 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.

Entfernen von Jumpoint-Mitgliedschaft

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 unter Verwenden von Jump-Element-Rollen, um Berechtigungen für Jump-Elemente zu konfigurieren unter https://www.beyondtrust.com/docs/privileged-remote-access/how-to/jumpoint/jump-item-roles.htm.*

Sie können auch eine Jump-Richtlinie anwenden, um den Benutzerzugriff auf die Jump-Elemente dieser Jump-Gruppe zu verwalten. Wenn Sie stattdessen **Für Jump-Elemente festlegen** wählen, wird die Jump-Richtlinie für das Jump-Element selbst verwendet. Jump-Richtlinien werden auf der Seite **Jump > Jump-Richtlinien** konfiguriert und bestimmen die Zeiten, während denen ein Benutzer Zugriff auf dieses Jump-Element hat. Eine Jump-Richtlinie kann auch eine Benachrichtigung senden, wenn darauf zugegriffen wird, oder kann zum Zugriff eine Genehmigung erfordern. Wird keine Jump-Richtlinie auf den Benutzer oder das Jump-Element angewendet, kann ohne Einschränkung auf dieses Jump-Element zugegriffen werden.

> *Weitere Informationen finden Sie unter Erstellen von Jump-Richtlinien, um den Zugriff auf Jump-Elemente zu steuern unter https://www.beyondtrust.com/docs/privileged-remote-access/how-to/jumpoint/policies.htm.*

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 jedes Kontos 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 Privileged Remote Access-Sitzungen verwenden.
- **Einfügen und auschecken:** Benutzer mit dieser Rolle können dieses Konto in Privileged Remote Access-Sitzungen verwenden und das Konto auf **/login** auschecken. Die Berechtigung **Auschecken** hat keinen Einfluss auf generische SSH-Konten.

> ***Hinweis:*** *Aktivieren Sie die Berechtigung **Vault-Kontomitgliedschaften hinzufügen**, um einem Vault-Konto in einer Gruppenrichtlinie eine **Rolle des Vault-Kontos** 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 > Kontogruppen** 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 Privileged Remote Access-Sitzungen verwenden.
- **Einfügen und auschecken:** Benutzer mit dieser Rolle können dieses Konto in Privileged Remote Access-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.*

Speichern

Klicken Sie auf **Speichern**, damit die Richtlinie wirksam wird.

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 Richtliniennamen, 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 scrollen Sie dann zum Abschnitt **Richtlinie importieren** am Ende der Seite. Klicken Sie auf **Richtliniendatei auswählen**, durchsuchen Sie die Richtliniendatei und klicken Sie dann auf **Öffnen**. 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

Benutzer und Sicherheit	KERBEROS-KEYTAB

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 zugriffskonsole.

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 zum Hochladen auswählen

Exportieren Sie die Keytab-Datei für den SPN aus Ihrem KDC und laden Sie sie über den auf dieser Seite befindlichen Abschnitt **Keytab-Datei importieren** auf das B Series Appliance hoch.

Berichte

Zugriff: Berichte zu Sitzungsaktivitäten

Berichte | ZUGRIFF

Zugriffsberichte

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

Aktivitätsbericht gemäß drei unterschiedlichen Berichtstypen generieren: **Sitzung**, **Zusammenfassung**, und **Sitzungsforensik** (falls aktiviert).

Sitzungsbericht

Zeigen Sie alle Zugriffssitzungen an, die den von Ihnen in den Berichtsfiltern angegebenen Kriterien entsprechen. Sitzungsberichte umfassen grundlegende Sitzungsinformationen, zusammen mit Links zu Sitzungsdetails, Chat-Mitschriften und Videoaufzeichnungen von Bildschirmfreigabe- und Befehlsshell-Sitzungen sowie Protokoll-Tunnel-Jumps.

Sitzungsberichte enthalten eine detaillierte Abschrift des Chats, die Zahl der übertragenen Dateien (und Details zu fehlgeschlagenen Dateiübertragungen) sowie die bestimmten Aktionen, die während der Sitzung ausgeführt wurden. Windows-Ereignisse, die zu beträchtlichen visuellen Änderungen in der Sitzung geführt haben, werden als Ereignisse in den Sitzungsdetails aufgezeichnet. Dazu gehören Änderungen am Vordergrundfenster mit dem Namen der ausführbaren Datei und dem Fenstertitel.

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 159.

Andere Informationen betreffen unter anderem die Sitzungsdauer, die lokalen und Remote-IP-Adressen und 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. Ist die Aufzeichnung von Protokoll-Tunnel-Jumps aktiviert, können Sie Videoaufzeichnungen des gesamten Benutzerdesktops anzeigen. Ist die Eingabeaufforderungsaufzeichnung aktiviert, können Sie die Aufzeichnungen und/oder Textabschriften 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 Sitzungsaktivitäten in einem bestimmten Zeitraum und sind nach Benutzer kategorisiert. Statistiken umfassen die Gesamtanzahl ausgeführter Sitzungen, die durchschnittliche Anzahl von Sitzungen nach Wochentag und die durchschnittliche Dauer der Sitzungen.

Sitzungsforensik-Bericht

Die Forensikberichte für Zugriffssitzungen ermöglichen Ihnen die Suche nach Sitzungsereignissen in allen Zugriffssitzungen sowie die Suche nach Sitzungen, die den im Filter angegebenen Text oder Satz enthalten. Das durchsucht Chatnachrichten, Befehlsshell-Befehle, Dateiübertragungen, Dateisystemmodifikationen, Registrierungs-Modifikationen und Vordergrund-Fenstertitel.

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.

Endpunkt

Filtern Sie Sitzungen nach Computername, öffentlicher IP oder privater IP.

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.

Benutzer

Wählen Sie einen Benutzer aus dem Feld **Benutzer suchen** aus, um nach Sitzungen zu filtern, an denen ein bestimmter Benutzer teilgenommen hat. Aktivieren Sie **Übereinstimmung nur, wenn der ausgewählte Benutzer der primäre Benutzer der Sitzung ist**, um nur Sitzungen zu finden, in denen der Benutzer der primäre Benutzer war.

Anbietergruppe

Sucht alle Sitzungen, an denen ein Benutzer einer Anbietergruppe teilgenommen hat. Ein Suchfeld ermöglicht es Ihnen, nach einer bestimmten Anbietergruppe zu suchen.

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.

Teamaktivitätsbericht

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, für das Sie Aktivitätsprotokolle anzeigen möchten.

Zeigen Sie alle Team-Aktivitäten an, die den auf der vorherigen Seite angegebenen Kriterien entsprechen. Team-Aktivitäts-Berichte umfassen Informationen zu Benutzern, die sich an der zugriffskonsole an- oder abmelden, Chatnachrichten, die zwischen Teammitgliedern ausgetauscht werden, Benutzer-zu-Benutzer-Bildschirmfreigabeaktionen entsprechend der Protokollierung im Chat und alle freigegebenen und heruntergeladenen Dateien.

> ***Hinweis:*** *Alle in den Privileged Remote Access Berichten aufgeführten Elemente sind in der Reihenfolge vom neuesten bis zum ältesten Element geordnet, mit Ausnahme der forensischen Sitzungsberichte.*

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 Kontonamen ein oder wählen Sie das Konto aus der dynamischen Pop-up-Liste aus.

Durchgeführt von

Um alle Ereignisse anzuzeigen, die einen bestimmten privilegierten Benutzer, ein API-Konto oder das System betreffen, geben Sie den Kontonamen ein oder wählen Sie den Kontonamen aus der dynamischen Pop-up-Liste aus.

Ereignisse der Windows-Dienste einbeziehen

Aktivieren Sie die Option **Ereignisse der Windows-Dienste einbeziehen**, um Ereignisse im Zusammenhang mit der Rotation von Dienstkonten einzubeziehen.

Weitere Informationen finden Sie in Technisches Whitepaper zu BeyondTrust Vault unter https://www.beyondtrust.com/docs/privileged-remote-access/how-to/vault/index.htm.

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/privileged-remote-access/getting-started/admin/reports-compliance.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.

In den **Ergebnissen des Vault-Kontoaktivitätsberichts** zeigt die Spalte **Daten** mit dem Ereignis verbundene Informationen an. Das Ereignis **Anmeldedaten ausgecheckt** enthält einen Link **Details** in der 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.*

Die Spalte **Datendienst** wird in den Berichtergebnissen angezeigt, wenn die Option **Ereignisse der Windows-Dienste einbeziehen** aktiviert ist. In dieser Spalte werden alle Fehler angezeigt, die bei Ereignissen der Rotation von Dienstkonten auftreten.

Anbieter: Bericht zu Anbieter-Konten und zur Benutzeraktivität

Berichte	ANBIETER

Bericht zur Anbieter-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.

Anbietergruppe

Sucht alle Ereignisse mit Beteiligung eines bestimmten Anbieters. Die Berichte enthalten **Zeitstempel**, **Anbietergruppe**, **Ereignistyp**, **Durchgeführt von** und zugehörige **Daten**. **Ereignistypen** umfassen **Anbietergruppe** oder **Anbieter-Benutzer angefordert/erstellt/gelöscht/abgelehnt**.

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 163.

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

Berichte	SYSLOG

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

Compliance: Privileged Remote Access Daten anonymisieren zur Erfüllung von Compliance-Standards

Berichte	COMPLIANCE

WICHTIG!

*Standardmäßig ist die Registerkarte **Compliance** deaktiviert. Wenn Ihr Unternehmen diese Funktion benötigt, kontaktieren Sie bitte den BeyondTrust Support unter www.beyondtrust.com/docs/index.htm#support.*

Benutzer-Anonymisierung

Informationen über Benutzer sowie die in Zugriffssitzungen durchgeführten Aktionen können anonymisiert werden, um Datenschutzvorschriften und Compliance-Standards zu erfüllen.

Um Daten zu anonymisieren, geben Sie den Benutzernamen, den Anzeigenamen oder die E-Mail-Adresse ein und wählen Sie dann den Benutzer aus der Liste aus. Klicken Sie auf **Support-Techniker-Aktivität suchen**. Werden Daten gefunden, gibt das System eine Liste der für den Benutzer gefundenen Informationen sowie einen zufällig generierten, vorgeschlagenen Ersatzbegriff für die Informationen

zurück. Sie können auf den vorgeschlagenen Begriff klicken, wodurch die Aufforderung **Ersatz bearbeiten** erscheint. Innerhalb des Dialogs können Daten anonymisiert werden, indem Sie Ihren bevorzugten Ersatzbegriff für die Daten eingeben. Wenn Sie fertig sind, klicken Sie auf **Ersatzbegriff im gesamten Verlauf ersetzen**, um den Begriff im Abschnitt zu ersetzen.

Die Liste wird mit dem neuen Ersatzbegriff aktualisiert und die Meldung „Alle Zugriffssitzungen und Teamaktivitätsereignisse für diesen Benutzer werden zu folgendem Zeitpunkt als anonymisiert gekennzeichnet: (Datum und Uhrzeit)“ erscheint. Klicken Sie nach dem Überprüfen 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.

WICHTIG!

Alle Sitzungsaufzeichnungen werden im Rahmen der Anonymisierungsanforderung gelöscht.

Endpunkt-Anonymisierung

Informationen über abgerufene Endpunkte sowie die während Zugriffssitzungen durchgeführten Aktionen können anonymisiert werden, um Datenschutzvorschriften und Compliance-Standards zu erfüllen.

Um Daten zu anonymisieren, geben Sie den Namen des Endpunkts, den Hostnamen oder die IP-Adresse 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 für den Endpunkt gefundenen Informationen zusammen mit einem zufällig generierten, vorgeschlagenen Ersatzbegriff für die Informationen zurück. Sie können auf diesen Begriff klicken, wodurch der Dialog **Ersatz bearbeiten** erscheint. Innerhalb des Dialogs können Daten anonymisiert werden, indem Sie Ihren bevorzugten Ersatzbegriff für die Daten eingeben. Wenn Sie fertig sind, klicken Sie auf **Ersatzbegriff im gesamten Verlauf ersetzen**, um den Begriff im Abschnitt zu ersetzen.

Die Liste wird mit dem neuen Ersatzbegriff aktualisiert und die Meldung „Die ausgewählten Zugriffssitzungen 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.

Sie können auch auf **Benutzerdefiniert hinzufügen** klicken. Damit können Sie angepasste Informationen wie Kontonummern eingeben und suchen.

WICHTIG!

Alle Sitzungsaufzeichnungen werden im Rahmen der Anonymisierungsanforderung gelöscht.

Status

Überprüfen Sie Informationen über Anonymisierungsaufträge, darunter die gefundenen und Ersatzbegriffe, die Art der anonymisierten Daten und der Status des Auftrags.

Der Auftragsstatus wird alle 15 Sekunden automatisch aktualisiert. Der Status für abgeschlossene Anfragen bleibt 24 Stunden lang verfügbar.

Hinweis: *Diese Statusinformationen sind auch in Sitzungsberichten 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.*

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 und der zugriffskonsole 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.

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.

> ***Hinweis:*** *Es ist möglich, in einem Sitzungs-Chat eine Sprache zu verwenden, die von BeyondTrust nicht unterstützt wird, aber von GeoFluent durchaus. Weitere Informationen finden Sie im Abschnitt zu optionalen Parametern im API-Handbuch unter https://www.beyondtrust.com/docs/remote-support/how-to/integrations/api/session-gen/index.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 und der zugriffskonsole 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.

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.

Hinweis: *Es ist möglich, in einem Sitzungs-Chat eine Sprache zu verwenden, die von BeyondTrust nicht unterstützt wird, aber von GeoFluent durchaus. Weitere Informationen finden Sie im Abschnitt zu optionalen Parametern im API-Handbuch unter https://www.beyondtrust.com/docs/remote-support/how-to/integrations/api/session-gen/index.htm.*

Verwaltung

Software: Laden Sie ein Backup herunter, nehmen Sie ein Software-Upgrade vor

Verwaltung | SOFTWARE

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 Sitzungsverlaufdaten 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 auf dem B Series Appliance verwendet. Falls Sie jemals Konfigurationsdaten von einem Sicherungs- auf ein neues B Series Appliance übertragen müssen, müssen Sie auch den Vault-Verschlüsselungsschlüssel von einer Sicherung wiederherstellen, um die verschlüsselten Vault-Anmeldedaten der Konfigurationssicherungskopie nutzen zu können.

Einstellungen wiederherstellen

Konfiguration und Vault-Verschlüsselungsschlüssel-Sicherungsdatei

Sollten Sie eine Sicherung wiederherstellen müssen, suchen Sie die letzte gespeicherte Sicherungsdatei.

Konfiguration und Vault-Verschlüsselungsschlüssel-Sicherungspasswort

Wenn Sie ein Passwort für Ihre Sicherungsdatei erstellt haben, geben Sie es hier ein.

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.

> *Weitere Informationen finden Sie in Sicherungsverfahren unter https://www.beyondtrust.com/docs/privileged-remote-access/how-to/disaster-recovery/back-up-procedures.htm.*

Aktualisierung hochladen

Wählen Sie eine Softwareaktualisierungsdatei aus, um neue Softwarepakete von BeyondTrust manuell hochzuladen. Sie müssen bestätigen, 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 B Series Appliance.

> ***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 Privileged Remote Access 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

Verwaltung | SICHERHEIT

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 17.*

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.

Komplexe Kennwörter erforderlich

Legen Sie für lokale Benutzerkonten Regeln bezüglich der Komplexität von Kennwörtern fest.

Standardgültigkeitsdauer für Kennwörter

Legen Sie für lokale Benutzerkonten Regeln fest, wie oft Kennwörter ablaufen.

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.

Zugriffskonsole

Sitzung abbrechen, wenn Konto verwendet wird

Wenn ein Benutzer versucht, sich mit einem bereits verwendeten Konto in der zugriffskonsole anzumelden, wird bei aktiviertem Kästchen **Sitzung beenden** die vorhergehende Verbindung unterbrochen, um die neue Anmeldung zu erlauben.

Gespeicherte Anmeldungen aktivieren

Gestatten Sie der zugriffskonsole, die Anmeldedaten eines Benutzers zu speichern, oder verweigern Sie es.

Abmelden inaktiver Benutzer nach

Legen Sie fest, wie lange es dauert, bis ein inaktiver Benutzer von der zugriffskonsole abgemeldet wird, um die Lizenz für einen anderen Benutzer freizugeben.

Warnung und Abmeldebenachrichtigung bei Zeitüberschreitung wegen Inaktivität aktivieren

Mit dieser Option können Sie einem inaktiven Benutzer 30 Sekunden vor der Abmeldung eine Benachrichtigung anzeigen. Der Benutzer wird nach erfolgter Abmeldung erneut benachrichtigt.

Benutzer 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 Zugriffskonsole und Zugriffskonsole für Privileged Web Access mit Connect gestatten

Gewährt Benutzern die Option, über die BeyondTrust zugriffskonsole-App für iOS und Android und die Zugriffskonsole für Privileged Web Access, eine browserbasierte zugriffskonsole auf Remote-Systeme zuzugreifen.

Synchronisierungsmodus für Zwischenablage

Synchronisierungsmodus für Zwischenablage legt fest, wie Benutzer die Zwischenablagen innerhalb einer Bildschirmfreigabesitzung synchronisieren dürfen. Verfügbare Einstellungen:

- **Automatisch:** Der Endpunkt und die Zwischenablage des Benutzers werden automatisch synchronisiert, wenn sich eines von beiden ändert.
- **Manuelle Installation:** Der Benutzer muss auf eines der Zwischenablage-Symbole in der zugriffskonsole 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 Benutzer verhindern und Benutzern 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 Benutzer in der zugriffskonsole angezeigt werden, wenn der Modus **Manuell** ausgewält ist, und wie die Synchronisierung im Modus **Automatisch** funktioniert.

Detaillierte Zugriffsoptionen für die Zwischenablage können für Sitzungsrichtlinien und Gruppenrichtlinien eingerichtet sowie bestimmten Benutzern gewährt werden. Bitte beachten Sie zu jedem speziellen Fall die nachstehenden Links:

- **Benutzer: Benutzerberechtigungen für einen Benutzer oder Administrator hinzufügen: Benutzer und Sicherheit > Benutzer > Hinzufügen > Sitzungsberechtigungen > Bildschirmfreigabe**
- **Sitzungsrichtlinien: Sitzungsberechtigungen und Aufforderungsregeln festlegen: Benutzer und Sicherheit > Sitzungsrichtlinien > Hinzufügen > Berechtigung > Bildschirmfreigabe**
- **Gruppenrichtlinien: Benutzerberechtigungen auf Benutzergruppen anwenden: Benutzer und Sicherheit > Gruppenrichtlinien > Hinzufügen > Sitzungsberechtigungen [definiert]**

Hinweis: *Sie müssen die Software auf der **Status**-Seite neu starten, damit diese Einstellung wirksam wird.*

Suche nach externen Jump-Items zulassen

Dies ermöglicht die Jump-Item-Suche in Password Safe, wenn Privileged Remote Access über eine Password Safe-Integration und einen vollständig konfigurierten Endpunkt-Anmeldedaten-Manager (ECM) verfügt.

> ***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 PRA 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 zugriffskonsole oder der Web-zugriffskonsole 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.

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 B Series Appliance 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 der Berichts-API (www.beyondtrust.com/docs/privileged-remote-access/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.

Netzwerkbeschränkungen

Sie können bestimmen, welche IP-Netzwerke auf /login, /api und die BeyondTrust zugriffskonsole auf Ihrem B Series Appliance zugreifen können. Wenn Sie die Netzwerkeinschränkungen aktivieren, können Sie auch erzwingen, dass die zugriffskonsole nur über bestimmte Netzwerke genutzt werden kann.

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 Zugriffskonsole

- **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-zugriffskonsole 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-zugriffskonsole die in der Verwaltungsschnittstelle eingegebenen Beschränkungen.

- **Netzwerkbeschränkungen niemals anwenden:** Bei Auswahl dieser Option werden auf die Web-zugriffskonsole selbst dann keine Beschränkungen angewendet, wenn bei anderen Zugriffskonsolen-Methoden Beschränkungen gelten.

> *Weitere Informationen finden Sie im Zugriffskonsole für Privileged Web Access-Handbuch unter https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/web-access/index.htm.*

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

Verwaltung | WEBSITE-KONFIGURATION

HTTP

Website-Adresse

Legen Sie eine oder mehrere DNS-Adressen fest, die zu Ihrem B Series Appliance aufgelöst werden.

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

Anmeldevereinbarung für die Verwaltungsschnittstelle/Zugriffskonsole aktivieren

Sie können eine Anmeldungsvereinbarung aktivieren, die Benutzer annehmen müssen, bevor Sie entweder auf die /login-Verwaltungsschnittstelle, die zugriffskonsole, oder beide 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.

Text der Vereinbarung

Geben Sie den Text für die Anmeldungsvereinbarung an.

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

Wenn Ihr SMTP-Server TLS-Verschlüsselung unterstützt, wählen Sie **TLS** oder **STARTTLS**. Wählen Sie andernfalls **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 hier:

- *„OAuth2 für Azure Active Directory konfigurieren“ auf Seite 169*
- *„OAuth2 für Google konfigurieren“ auf Seite 170*

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.

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.

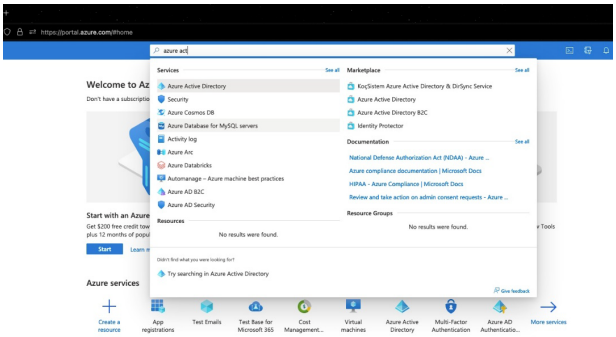
Senden Sie eine Test-E-Mail, nachdem die Einstellungen gespeichert wurden

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.

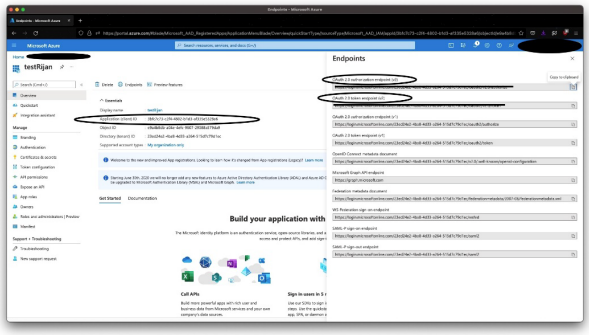
OAuth2 für Azure Active Directory konfigurieren

> ***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

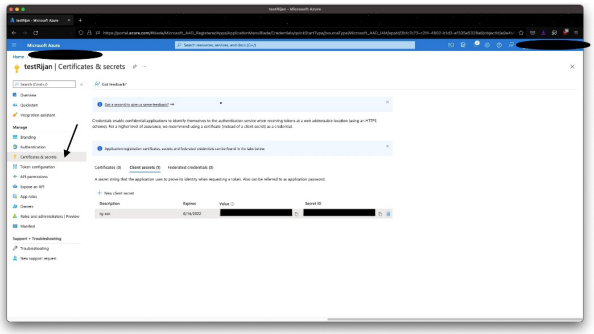


1. Melden Sie sich bei Ihrer Azure-Konsole an (portal.azure.com) und navigieren Sie zu **Azure Active Directory**.
2. Gehen Sie zu **App-Registrierungen** und wählen Sie **Neue Registrierung**.
   - Geben Sie einen Namen ein, z. B. Gerät-OAuth2.
   - Wählen Sie die Kontotypen aus, mit denen Sie sich über OAuth2 bei der Anwendung anmelden können möchten. Wählen Sie **Single Tenant** für nur intern.
   - Geben Sie den **Weiterleitungs-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.



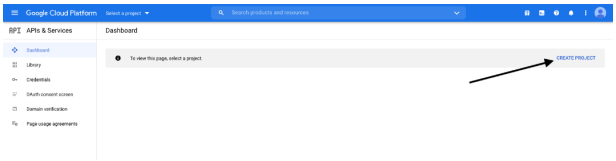
Anmeldedaten bereitstellen für den SMTP-Relay-Server

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.

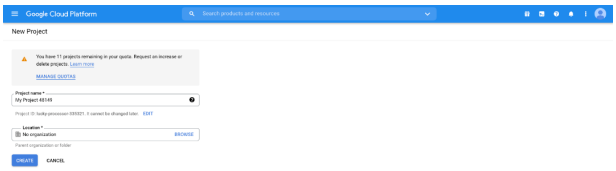
OAuth2 für Google konfigurieren

Google Cloud konfigurieren

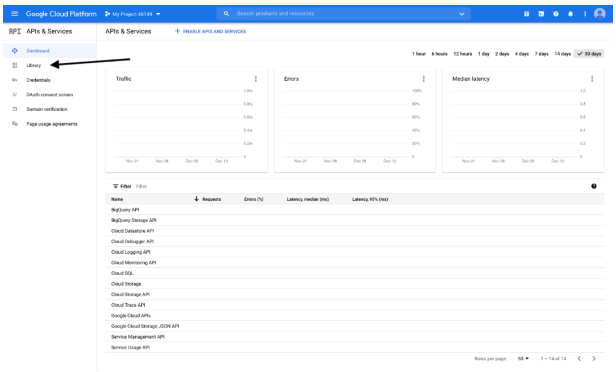
1. Melden Sie sich bei Ihrer Google Cloud Platform-Konsole (Google Dev Console) an (console.cloud.google.com). Verwenden Sie das richtige Gmail-Konto, da nur der Eigentümer des Projekts mit dem Projekt arbeiten kann. Wenn Sie noch kein bezahltes Konto haben, können Sie ein Konto erwerben, indem Sie auf **Aktivieren** im oberen Banner klicken. BeyondTrust kann Ihnen beim Erwerb eines Kontos nicht behilflich sein. Klicken Sie auf **Mehr erfahren** im oberen Banner, um Informationen über die Einschränkungen der kostenlosen Konten zu erhalten.



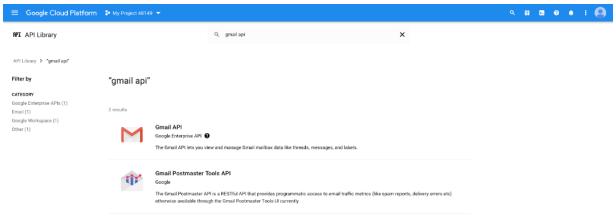
2. Klicken Sie auf **PROJEKT ERSTELLEN**. Sie können auch ein bestehendes Projekt verwenden.
3. Akzeptieren Sie den Standard-**Projektnamen** oder geben Sie einen neuen Namen ein.
4. Akzeptieren Sie die Standardeinstellung **Speicherort** oder wählen Sie einen der für Ihr Unternehmen verfügbaren Ordner.
5. Klicken Sie auf **ERSTELLEN**.



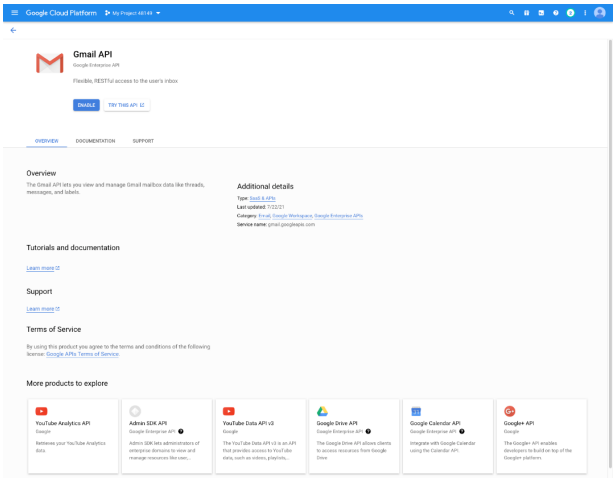
6. Die Seite **APIs und Dienste** wird angezeigt. Klicken Sie im linken Menü auf **Bibliothek**.



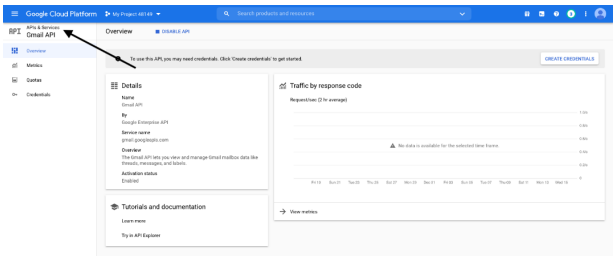
7. Suchen Sie in der Bibliothek nach der **Gmail-API** und klicken Sie darauf.



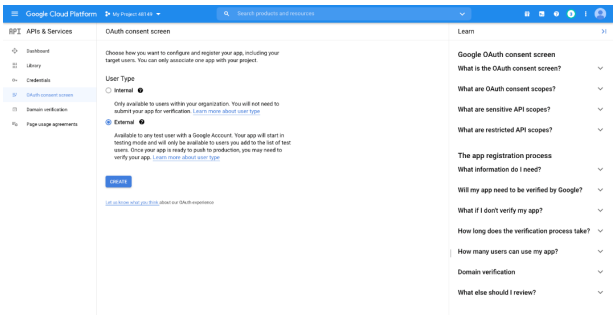
8. Die **Gmail API** erscheint auf einer eigenen Seite. Klicken Sie auf **AKTIVIEREN**.



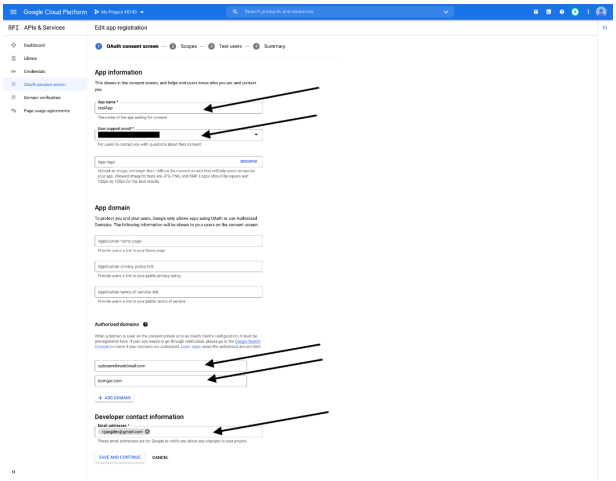
9. Die Seite **Gmail API-Übersicht** wird angezeigt. Klicken Sie oben links auf **APIs & Dienste**.
10. Die Seite **APIs und Dienste** wird wieder angezeigt. Klicken Sie im linken Menü auf **OAuth-Zustimmungsbildschirm**.



11. Wählen Sie den **Benutzertyp**. Intern erlaubt nur Benutzern innerhalb der Organisation, erfordert aber ein Google Workspace-Konto.
12. Klicken Sie auf **ERSTELLEN**.

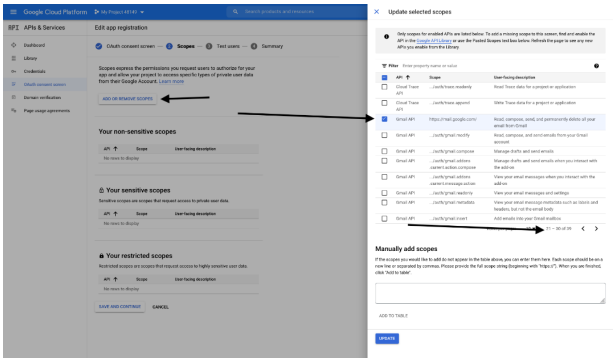


13. Geben Sie den **App-Namen** ein.
14. Geben Sie eine **Benutzer-Support-E-Mail**-Adresse ein. Dies kann standardmäßig die Adresse sein, die Sie zum Erstellen des Projekts verwenden.
15. Geben Sie, falls gewünscht, ein Logo für die App ein. Der Abschnitt **Anwendungsbereich** ist ebenfalls optional.
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**.

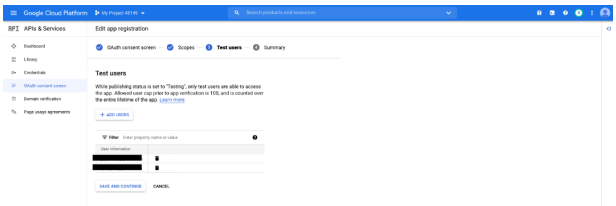


19. Klicken Sie auf der Registerkarte **Bereiche** auf **Bereiche hinzufügen oder entfernen**. Dies öffnet das Fenster **Ausgewählte Bereiche aktualisieren**.
20. Suchen Sie den Bereich **https://mail.google.com/** für die Gmail-API und überprüfen Sie ihn.

> ***Hinweis:*** *Die API wird nicht angezeigt, wenn sie nicht aktiviert wurde.*

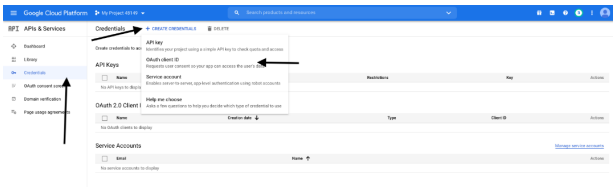


21. Klicken Sie **UPDATE**. Das Fenster **Ausgewählte Bereiche aktualisieren** wird geschlossen.
22. Klicken Sie auf **SPEICHERN UND WEITER**.
23. Klicken Sie auf der Registerkarte **Testbenutzer** auf **BENUTZER HINZUFÜGEN**. Dies öffnet das Fenster **Benutzer hinzufügen**. Fügen Sie die Benutzer hinzu, die Zugriff auf die Anwendung haben, und klicken Sie auf **ZUFÜGEN**. Beachten Sie die Zugriffsbeschränkungen für Testbenutzer und die damit verbundenen Einschränkungen.

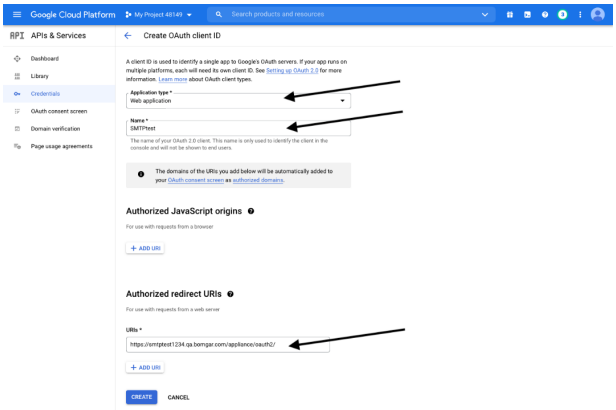


24. Klicken Sie auf **SPEICHERN UND WEITER**.
25. Überprüfen Sie die Zusammenfassung und nehmen Sie gegebenenfalls Änderungen oder Korrekturen vor.
26. Klicken Sie auf **ZURÜCK ZUM DASHBOARD**.

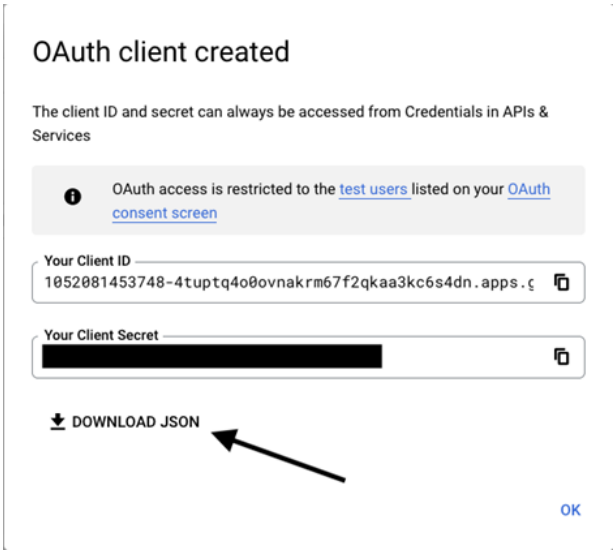
27. Klicken Sie im linken Menü auf **Anmeldedaten**.
28. Klicken Sie auf **ANMELDEDATEN ERSTELLEN** im oberen Banner und wählen Sie **OAuth-Client-ID**.



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

Verwaltung | AUSGEHENDE EREIGNISSE

HTTP-Empfänger

Sie können Ihr BeyondTrust Appliance B Series 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.

Neuen HTTP-Empfänger hinzufügen, bearbeiten, löschen

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

HTTP-Empfänger hinzufügen oder bearbeiten

Name

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

URL

Geben Sie die Ziel-URL für diesen Handler für ausgehende Ereignisse an.

> ***Hinweis:*** *BeyondTrust Cloud-Kunden müssen URLs verwenden, die mit HTTPS beginnen. Nur Port 443 wird unterstützt.*

Aktiviert

Um den Ereignis-Handler zu aktivieren, setzen Sie einen Haken bei **Aktiviert**. Entfernen Sie die Auswahl des Kontrollkästchens **Aktiviert**, um die Meldungen für den eingerichteten Ereignis-Handler zu stoppen, etwa im Falle eines geplanten Integrationstests.

CA-Zertifikat verwenden

Unter einer HTTPS-Verbindung müssen Sie das Root-Zertifikat der Zertifizierungsstelle hochladen, das vom ausgehenden Ereignisserver genannt wird.

Benutzerdefinierte Felder senden

Ist diese Option aktiviert, werden alle auf der Seite **Benutzerdefinierte Felder** konfigurierten benutzerdefinierten Felder im ausgehenden Ereignis berücksichtigt.

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

Neuen E-Mail-Empfänger hinzufügen, bearbeiten, löschen

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

Aktueller Status

Zeigt eine kurze Statusmitteilung vom SMTP-Relay-Server an. Solange das B Series Appliance Nachrichten an den Relay-Server sendet, wird unter dem Status **OK** angezeigt. Ist das nicht der Fall, sollten Sie die Einstellungen Ihres SMTP-Relay-Servers verwenden.

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

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

Um den Ereignis-Handler zu aktivieren, setzen Sie einen Haken bei **Aktiviert**. Entfernen Sie die Auswahl des Kontrollkästchens **Aktiviert**, um die Meldungen für den eingerichteten Ereignis-Handler zu stoppen, etwa im Falle eines geplanten Integrationstests.

Name

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

E-Mail-Adresse

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. Klicken Sie auf den Link unter dem Feld **Text**, um die Makros anzuzeigen, die Ihnen für die Anpassung Ihrer E-Mails nach Wunsch zur Verfügung stehen.

Text

Passen Sie den Text dieser E-Mail an. Klicken Sie auf den Link unter dem Feld **Text**, um die Makros anzuzeigen, die Ihnen für die Anpassung Ihrer E-Mails nach Wunsch zur Verfügung stehen.

Cluster: Atlas-Cluster-Technologie für Lastenausgleich konfigurieren

Verwaltung | CLUSTER

Status

Geographisch großräumige Bereitstellungen profitieren von der BeyondTrust Atlas Cluster-Technologie, die eine einzige BeyondTrust-Site auf mehreren B Series Appliance en erstellt, die Knoten in einem Cluster genannt werden. Am primären B Series Appliance/primären Knoten finden die meisten Verwaltungsarbeiten statt. Der Datenverkehrsknoten ist ein B Series Appliance-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/privileged-remote-access/how-to/atlas/index.htm.*

Aktueller Status

Bestätigt die Rolle der Site-Instanz, von der aus Sie auf die Seite zugegriffen haben.

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 Benutzer- oder Endpunkt-Client-Verbindung 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.

Neuen Datenverkehrsknoten hinzufügen, Knoten bearbeiten, Knoten 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

Stellen Sie sicher, dass diese Einstellung aktiviert ist, da Kunden diesen Verkehrsknoten sonst nicht verwenden können.

Name

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

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).

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.

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.

Maximale Client-Rückgriffe auf Primärknoten

Ermöglicht, dass die Anzahl der auf Fallback eingestellten Clients wieder den Primärknoten zur Verkehrssteuerung verwenden.

Failover: Einrichten eines Sicherungs-B Series Appliances für Failover

Verwaltung | FAILOVER

Hinweis: *Diese Funktion ist nur für Kunden verfügbar, die ein B Series Appliance an ihrem Standort betreiben. BeyondTrust Cloud-Kunden haben keinen Zugriff auf diese Funktion.*

Weitere Informationen finden Sie in Privileged Remote Access Failover-Konfiguration unter https://www.beyondtrust.com/docs/privileged-remote-access/how-to/failover/index.htm.

Konfiguration

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.

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.

Timeout der primären Site-Instanz

Legen Sie fest, wie lange die primäre Site unerreichbar sein muss, bevor ein Failover stattfindet.

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.

CLI-Client-Download

Das Tool Befehlszeilenschnittstelle (Command Line Interface - CLI) kann heruntergeladen werden, um die Verwendung und Konfiguration von APIs und Automatisierungsskripten zu erleichtern und sie in Ihre BeyondTrust Privileged Remote Access 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.

> *Weitere Informationen zur Erstellung von APIs mit CLI finden Sie unter Use Cases Beispiele im BeyondTrust Privileged Remote Access API Guide auf https://www.beyondtrust.com/docs/privileged-remote-access/how-to/integrations/api/use-cases.htm.*

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.

Ein API-Konto 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.

Kommentare

Fügen Sie Kommentare hinzu, die den Zweck dieses Objekts deutlich machen.

OAuth Client-ID

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.

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 auf die API zugreifen.*

Hinweis: *Die OAuth Client-ID und das Client-Secret werden zur Erstellung von OAuth-Tokens verwendet, die für die API-Authentifizierung benötigt werden.*

Weitere Informationen finden Sie im API-Handbuch unter www.beyondtrust.com/docs/privileged-remote-access/how-to/integrations/api/index.htm.

Berechtigungen

Wählen Sie die API-Bereiche, die dieses Konto verwenden können soll. Wählen Sie für die **Befehls-API**, ob der Zugriff verweigert, nur schreibgeschützt oder vollständig gewährt werden soll. Legen Sie ebenfalls fest, ob dieses Konto die **Berichts-API**, die **Sicherungs-API** die **Konfigurations-API** und/oder die **Endpunkt-Anmeldedaten-Manager-API** verwenden kann.

Wenn ECM-Gruppen für die Website aktiviert sind, wählen Sie die zu verwendende ECM-Gruppe aus. ECMs, die nicht mit einer Gruppe verbunden sind, fallen unter **Standard**.

Mit der **Konfigurations-API** können häufige Aufgaben in **/login** verwaltet werden. Diese lassen sich Ihren Organisationsprozessen entsprechend automatisieren und können mit diesen eingesetzt werden.

Über die **SCIM-API-Funktionalität** können Benutzer mit einem anderen Sicherheitsanbieter bereitgestellt werden. Wenn Sie Zugriff auf die SCIM-API-Funktionalität gestatten, wird die Option **Langlebiges Inhaber-Token zulassen** verfügbar. Das Zulassen langlebiger Tokens wird nur dann empfohlen, wenn dies von Ihrem SCIM-Client erfordert wird, da diese Inhaber-Tokens niemals ablaufen. Da alle anderen API-Berechtigungen Tokens erfordern, die nach einer Stunde ablaufen, werden durch das Zulassen langlebiger Tokens für SCIM alle anderen API-Berechtigungen deaktiviert.

Weitere Informationen finden Sie in Vault-Konto-Konfigurations-APIs unter www.beyondtrust.com/docs/privileged-remote-access/how-to/integrations/api/configuration-api.htm.

Netzwerkbeschränkungen

Listet Netzwerkadresspräfixe auf, über die sich dieses Konto authentifizieren kann.

Hinweis: *API-Konten sind nicht durch die auf der Seite **/login > Verwaltung > Sicherheit** konfigurierten Präfixe beschränkt. Sie sind nur durch die für das API-Konto konfigurierten Netzwerkpräfixe beschränkt.*

ECM-Gruppen

Hinweis: *Diese Funktion ist nur vorhanden, wenn sie bei der Erstellung Ihrer Website aktiviert wurde. Wenn sie nicht vorhanden ist, wenden Sie sich bitte an Ihren Website-Administrator.*

Die ECM-Gruppenfunktion unterstützt mehrere getrennte Anmeldedaten-Anbieter. Sie ermöglicht die Integration einer einzelnen PRA-Bereitstellung mit mehreren externen Anmeldedaten-Anbietern wie Password Safe oder Privileged Identity. Diese können sich durch mehrere ECM-Instanzen an verschiedenen Remote-Standorten befinden.

Neuer ECM-Gruppenname

Erstellen Sie einen eindeutigen Namen, um diese ECM-Gruppe leichter zu identifizieren. Sie können bis zu fünfzig ECM-Gruppen konfigurieren.

Support: Kontakt mit BeyondTrust Technical Support

Verwaltung	SUPPORT

BeyondTrust - Support-Kontaktinformationen

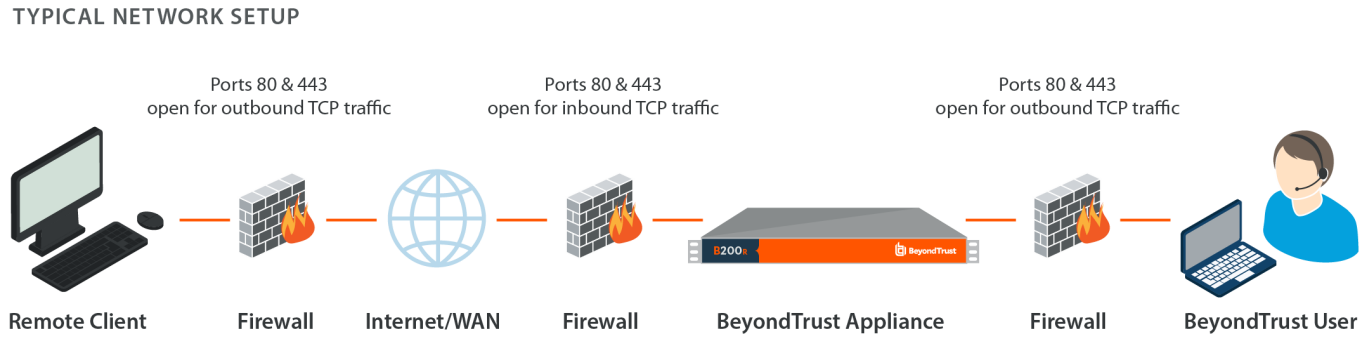
Die Support-Seite enthält Kontaktinformationen, falls Sie mit einem BeyondTrust Technical Support-Techniker in Verbindung treten müssen.

Erweiterter technischer Support von BeyondTrust

Muss ein Mitarbeiter des technischen BeyondTrust Technical Support-Supports auf Ihr B Series Appliance zugreifen, stellt er Ihnen Support-, Zugriffs- und Übersteuerungscodes bereit, die Sie auf dieser Seite eingeben, um einen B Series Appliance-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.



- 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 Installationshandbuch für BeyondTrust Appliance B Series-Hardware unter https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/deployment/hardware-sra/index.htm.
- 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
    - bomgar-pec-{uid}.exe
    - bomgar-pec.exe

    Unterstützung für die Konfiguration der Firewall erhalten Sie beim Hersteller der Firewall-Software.

- Beispiel-Firewall-Regeln basierend auf dem B Series Appliance-Standort finden Sie unter www.beyondtrust.com/docs/privileged-remote-access/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 die hierin enthaltenen Inhalte ohne Ankündigung 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. BeyondTrust Corporation lehnt jegliche Haftbarkeit in Bezug auf dieses Dokument ab, und es entstehen durch dieses Dokument keine direkten oder indirekten vertraglichen Verpflichtungen. 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 Privileged Remote Access-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.

Eine BeyondTrust Privileged Remote Access-Lizenz aktiviert den Zugriff auf ein Endpunkt-System. Obwohl diese Lizenz von einem System auf ein anderes übertragen werden kann, wenn der Zugriff auf das erste System nicht länger erforderlich ist, sind zwei oder mehr Lizenzen (eine pro Endpunkt) erforderlich, um den Zugriff auf mehrere Endpunkte gleichzeitig zu aktivieren.

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, melden Sie sich bitte beim Kundenportal unter https://beyondtrustcorp.service-now.com/csm an, um mit dem Support zu chatten.

Technischen Support können Sie mit einem jährlichen Abonnement unseres Wartungsplans in Anspruch nehmen.