BOMGAR™

Privileged Access Management Benutzerhandbuch für Administratoren 15.3

TC:5/6/2016

Inhaltsverzeichnis

Verwaltungshandbuch für Bomgar Privileged Access Management

Dieses Handbuch behandelt die **/login**-Schnittstelle und soll Ihnen bei der Administration Ihrer Bomgar-Software und von Bomgar-Benutzern helfen. Das Bomgar-Gerät dient als zentrale Administrations- und Verwaltungsstelle für Ihre Bomgar-Software und ermöglicht Ihnen, sich von einem beliebigen Punkt mit Internetzugang aus anmelden zu können, um die Zugriffskonsole herunterladen zu können.

Verwenden Sie dieses Handbuch erst, wenn die anfängliche Einrichtung und Konfiguration des Bomgar-Geräts durch einen Administrator abgeschlossen wurde, entsprechend der Beschreibung im Bomgar Installationshandbuch für Gerätehardware. Ist Bomgar korrekt installiert, können Sie sofort mit dem Zugriff auf Ihre Endpunkte beginnen. Sollten Sie Hilfe benötigen, wenden Sie sich an den technischen Bomgar-Support unter help.bomgar.com.

In der Verwaltungsschnittstelle anmelden

Anmelden

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

Obgleich es sich bei der URL Ihres Geräts um jedes registrierte DNS handeln kann, ist er wahrscheinlich eine Unterdomäne der Primärdomäne Ihres Unternehmens (z. B. zugriff.beispiel.com/login).

Standardbenutzername: **admin**

Standardkennwort: **password**

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

Hinweis: *Wenn für Ihr Konto Mehr-Faktor-Authentifizierung aktiviert wurde, geben Sie den erhaltenen E-Mail-Code ein. Wenn Sie den E-Mail-Code drei Mal hintereinander falsch eingeben, müssen Sie Ihre Anmeldedaten erneut eingeben und einen neuen E-Mail-Code anfordern.*

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.

Kennwort vergessen?

Wenn auf der Seite **/login > Verwaltung > Sicherheit** die Kennwortzurücksetzung aktiviert wurde, wird dieser Link sichtbar sein. Um Ihr Kennwort zurückzusetzen, klicken Sie auf den Link, geben Sie Ihren Benutzernamen ein und beantworten Sie dann die Sicherheitsfrage korrekt. Administratoren können ihre Kennwörter nicht über die Sicherheitsfrage zurücksetzen.

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.

Status

Informationen: Details der Bomgar Privileged Access Management-Software anzeigen

Website-Status

Die Hauptseite der Bomgar Privileged Access Management /login-Schnittstelle bietet einen Überblick über die Statistik Ihres Bomgar-Geräts. Wenn Sie den technischen Bomgar-Support für Softwareaktualisierungen oder zur Problembehebung kontaktieren, werden Sie möglicherweise darum gebeten, einen Screenshot dieser Seite zur Verfügung zu stellen.

Zeitzone

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

Gesamtanzahl gestatteter Jump Clients

Sehen Sie sich die Gesamtanzahl der aktiven und passiven Jump Clients an, die auf Ihrem System gestattet sind. Die Anzahl wird durch die Hardware-Kapazität Ihres Bomgar-Gerätes bestimmt.

Maximale Anzahl an gleichzeitigen Benutzern

Sehen Sie sich die maximale Anzahl von Benutzern an, die sich gleichzeitig in der Zugriffskonsole anmelden können. Die Anzahl wird durch die Hardware-Kapazität Ihres Bomgar-Gerätes bestimmt.

Endpunktlizenzen

Sehen Sie sich die Anzahl der Endpunktlizenzen an, die auf Ihrem Bomgar-Gerät verfügbar sind. Endpunkte umfassen Jump Clients, symbolische Remote-Jump-Links, symbolische lokale Jump-Links, symbolische RDP-Links und symbolische Shell Jump-Links. Wenn Sie mehr Endpunktlizenzen benötigen, kontaktieren Sie die Bomgar-Vertriebsabteilung.

Konfigurierte Endpunkte

Sehen Sie sich die Anzahl der Endpunktlizenzen an, die auf Ihrem Bomgar-Gerät verfügbar sind. Endpunkte umfassen Jump Clients, symbolische Remote-Jump-Links, symbolische lokale Jump-Links, symbolische RDP-Links und symbolische Shell Jump-Links.

Lizenznutzungsbericht herunterladen

Laden Sie eine ZIP-Datei mit detaillierten Informationen zu Ihrer Bomgar-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 Bomgar-Gerätes mit seinem Endpunktlizenzverbrauch.

Neu starten

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

Client-Software verwendet standardmäßig zuerst

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

Verbundene Clients

Zeigen Sie die Anzahl und den Typ der Bomgar Software-Clients an, die mit Ihrem Bomgar-Gerät verbunden sind.

Benutzer: Anzeige angemeldeter Benutzer und Senden von Nachrichten

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 zur 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.

Eigenes Konto: Ändern Sie Kennwort und Benutzername, laden Sie die Zugriffskonsole und andere Software herunter

Bomgar-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.

Bomgar-Zugriffskonsole herunterladen

Webbasierte Zugriffskonsole Privileged Web starten.

Laden Sie das Installationsprogramm der Bomgar-Zugriffskonsole 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 **“”** oder **1** (Standard). Wenn Sie **1** eingeben, wird die Konsole für alle Benutzer auf dem Computer installiert. Ansonsten wird sie nur für den aktuellen Benutzer installiert.
- Wenn Sie nur für den aktuellen Benutzer installieren, können Sie die Konsole automatisch jedes Mal aktualisieren, wenn die Website aktualisiert wird. Geben Sie dazu **SHOULDAUTOUPDATE=1** ein. Der Wert **0** (Standard) bedeutet, dass keine automatische Aktualisierung stattfindet und die Konsole manuell neuinstalliert werden muss, wenn die Website aktualisiert wird. Falls Sie die Konsole für alle Benutzer installieren, wird sie nicht automatisch aktualisiert.

Bomgar Virtual Smart-Card

Für eine Authentifizierung mithilfe einer virtuellen Smart-Card benötigt der Bomgar-Benutzer den Treiber für die virtuelle Smart-Card. Der Computer, auf den zugegriffen wird, muss im heraufgesetzten Modus betrieben werden. Ebenfalls muss entweder der Bomgar Virtual Smart-Card-Treiber für Endpunkte installiert sein oder es muss über die Jump zu-Funktion der Zugriffskonsole auf das System zugegriffen werden. Weitere Einzelheiten und Anforderungen finden Sie im Dokument Smart-Cards für die Remote-Authentifizierung.

Windows-Architektur auswählen

Wählen Sie, ob Sie das Installationsprogramm der Virtual Smart-Card für das System des Bomgar-Benutzers oder für das Endpunkt-System herunterladen möchten.

Installationsprogramm für Virtual Smart-Card herunterladen

Laden Sie das Installationsprogramm für die Virtual Smart-Card entsprechend Ihrer obigen Auswahl herunter. 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.

Bomgar-Dienst für die automatische Heraufsetzung

Windows-Architektur auswählen

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

Installationsprogramm für den Bomgar-Dienst für die automatische Heraufsetzung

In besonderen Fällen benötigen Sie eine Sitzung, bei welcher der Endpunkt-Client bereits im heraufgesetzten Modus startet, oder Sie müssen den Endpunkt-Client ohne die Angabe von Anmeldedaten heraufsetzen. Um eine sichere Heraufsetzung des Endpunkt-Client ohne Aufforderung zu ermöglichen, laden Sie den **Bomgar-Dienst für die automatische Heraufsetzung** herunter und installieren Sie ihn auf den Remote-Windows-Systemen, bevor Sie den heraufgesetzten Zugriff ohne Anmeldedaten benötigen. Sie müssen den Heraufsetzungsdienst mit einem Konto mit Administratorrechten auf dem lokalen System installieren.

Wenn der Heraufsetzungsdienst ausgeführt wird, fügt er in der Registrierung einen Hash-Wert hinzu, der Ihre Bomgar-Site eindeutig kennzeichnet. Wenn das Remote-System dann eine Sitzung von dieser Site aus startet, vergleicht der Heraufsetzungsdienst den Hash-Wert in der Registrierung mit dem Hash-Wert des Client. Im Falle einer Übereinstimmung versucht der Client eine automatische Heraufsetzung.

Registrierungsdatei für den Dienst für die automatische Heraufsetzung herunterladen

Nach einer Bomgar-Softwareaktualisierung ändert sich der Hash-Wert Ihrer Site. Laden Sie die Registrierungsdatei des Heraufsetzungsdienstes herunter und führen Sie sie aus, um den Hash-Wert in der Registrierung bei Systemen mit bereits installiertem Heraufsetzungsdienst zu aktualisieren. Sie müssen die Registrierungsdatei des Heraufsetzungsdienstes mit einem Konto mit Administratorrechten auf dem lokalen System ausführen.

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.

Ändern Sie Ihre E-Mail-Einstellungen

E-Mail-Adresse

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

Bevorzugte E-Mail-Sprache

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

Ändern Sie Ihr Kennwort

Bomgar empfiehlt, dass Sie Ihr Kennwort regelmäßig ändern.

Benutzername, aktuelles Kennwort, neues Kennwort

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

Ändern Sie Ihre Sicherheitsfrage/Antwort

Sicherheitsfrage und -antwort

Mit der Sicherheitsfrage und -antwort kann ein Benutzer ein vergessenes Kennwort zurücksetzen, wenn er die richtige Antwort auf die Frage eingibt. Kennwörter können nur zurückgesetzt werden, wenn **Kennwortrücksetzung aktivieren** auf der Seite **Verwaltung > Sicherheit** aktiviert wurde. Administratoren können ihre Kennwörter nicht über die Sicherheitsfrage zurücksetzen.

Konfiguration

Optionen: Verwalten von Verbindungsoptionen, Aufzeichnen von Sitzungen

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

Neuverbindungs-Zeitüberschreitung

Legen Sie fest, wie lange ein getrennter Endpunkt-Client den erneuten Verbindungsaufbau versuchen soll.

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.

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.

Protokolloptionen für Zugriffssitzung

Bildschirmfreigabe- / Befehlsshell-Aufzeichnung aktivieren

Wählen Sie, ob Bildschirmfreigabe-Sitzungen und/oder 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 Aufzeichnung von Bildschirmfreigabe- / Befehlsshell-Sitzungen

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

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

Automatische Protokollierung von Systeminformationen aktivieren

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.*

Teams: Gruppieren von Benutzern in Teams

Teams :: Verwalten

Das Gruppieren von Benutzer in Teams fördert die Effizienz, indem Hierarchien innerhalb von Benutzergruppen geschaffen werden. In der Konsole des Support-Technikers erscheint jedes Team als separate Warteschlange für wartende Sitzungen.

Neues Team hinzufügen, bearbeiten, löschen

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

Teams :: Hinzufügen oder Bearbeiten

Allgemeine Einstellungen

Teamname

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

Codename

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

Kommentare

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

Gruppenrichtlinien

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

Teammitglieder

Wählen Sie aus der Liste der verfügbaren Benutzer einen oder mehrere Benutzer aus und klicken Sie auf den Pfeil, um sie ins Team zu verschieben.

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.

Teammitglieder, die sich über eine oder mehrere Gruppenrichtlinien eine Mitgliedschaft teilen, werden für Sie aufgelistet, zusammen mit einem Link zur Konfigurationsseite für **Gruppenrichtlinien**.

Jump Client-Zugriff

Zugriff von diesem Team gewährt

Wählen Sie, welche Teams Zugriff auf die Jump Clients haben sollen, die in der Jump-Gruppe dieses Teams fixiert wurden. Standardmäßig hat nur dieses Team Zugriff auf seine eigenen Jump Clients. Sie können jedoch mehrere andere Teams auswählen, welche die Jump Clients dieses Teams anzeigen und einen Jump dorthin vollziehen können sollen.

Zugriff gewährt für dieses Team

Zeigen Sie eine Liste anderer Teams an, die sich den Jump Client-Zugriff mit Mitgliedern dieses Teams teilen.

Teams :: 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 Teamnmitglieder über das Dashboard überwachen. Sie können wählen, ob Sie diese Einstellung **Deaktivieren**, ausschließlich auf die **Zugriffskonsole** beschränken oder einem Teamführer oder Manager die Erlaubnis erteilen möchten, die Zugriffskonsole eines Teammitglieds zu überwachen. Die Überwachung betrifft Teamführer und Manager aller Teams.

Sitzungstransfer und -übernahme in Dashboard aktivieren

Ist diese Option aktiviert, kann ein Teamführer die Sitzungen eines Teammitglieds übernehmen oder übertragen. Auf ähnliche Weise kann ein Team-Manager sowohl Teammitglieder als auch Teamführer verwalten.

Jump

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

Stapelbereitstellungsassistent für Jump Clients

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

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.

Jump-Gruppe

Wählen Sie aus der Dropdown-Liste, ob Sie den Jump-Client in Ihre persönliche Jump-Gruppe oder in eine Team-Jump-Gruppe fixieren möchten. Durch Fixieren in Ihre persönliche Jump-Gruppe können nur Sie über diesen Jump Client auf diesen Remote-Computer zugreifen. Durch Fixieren in eine Team-Jump-Gruppe wird dieser Jump Client verfügbar für alle Teammitglieder, die auf Jump Clients dieses Teams zugreifen können.

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.

Tag

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

Verbindungstyp

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

Jumpoint-Proxy

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

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.

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. Dieser Zeitraum kann auf einen beliebigen Wert von zehn Minuten bis ein Jahr eingestellt werden. Diese Zeitangabe hat KEINE Auswirkungen darauf, wie lange der Jump Client aktiv ist.

Eine heraufgesetzte Installation versuchen, wenn der Client dies unterstützt

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

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

Bei Bedarf zur Eingabe von Heraufsetzungs-Anmeldedaten auffordern

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

Endpunkt-Client minimiert starten,wenn die Sitzung gestartet wird

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

Hilfe zur Stapelbereitstellung

Die ausführbare Datei für Windows, Mac oder Linux oder die Windows MSI-Datei eignet sich für Systemadministratoren, die das Jump Client-Installationsprogramm auf einer großen Anzahl an Systemen bereitstellen müssen und kann mit dem Systemverwaltungstool Ihrer Wahl verwendet werden. Sie können einen gültigen benutzerdefinierten Installationspfad angeben, in dem der Jump Client installiert werden soll. Sie können ebenfalls bestimmte Installationsparameter entsprechend Ihrer eigenen Anforderungen überschreiben. Diese Parameter können sowohl für die MSI und EXE mit einem Systemadministrationswerkzeug oder der Befehlszeile angegeben werden. Wenn Sie bestimmte Installationsoptionen während der Installation zur Überschreibung markieren, können Sie die folgenden optionalen Parameter zur Modifizierung des Jump Client-Installationsprogramms in individuellen Fällen nutzen. Beachten Sie: Wenn ein Parameter auf der Befehlszeile weitergegeben wird, aber nicht in der /login-Verwaltungsschnittstelle zur Überschreibung markiert wurde, schlägt die Installation fehl. Wenn die Installation fehlschlägt, überprüfen Sie das Ereignisprotokoll des Betriebssystems auf Installationsfehler.

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-jump-group	Benutzer:<benutzername> Team:<team-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-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.

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 (=)*

Beispiel:

```
msiexec /i bomgar-scc-win32.msi KEY_INFO=w0dc3056g7ff8d1j68ee6wi6dhwzfefggyezh7c40jc90 jc_jump_
group=team:general jc_tag=servers
```

Die einzige Ausnahme dieser Regel bildet ***installdir****, das über einen Bindestrich in der EXE-Version verfügt, nicht aber in der MSI-Version.*

Client jetzt herunterladen oder installieren

Plattform

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

Bitte beachten: Im Gegensatz zur Zugriffskonsole führen über MSI installierte Jump Clients automatische Aktualisierungen durch.

Herunterladen/Installieren

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

Für E-Mail-Empfänger bereitstellen

E-Mail

Sie können das Installationsprogramm auch per E-Mail an einen oder mehrere Remote-Benutzer senden. Mehrere Empfänger können den Client über den gleichen Link installieren.

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 zum Betriebssystem, zur Betriebszeit, zum Konsolenbenutzer, zur CPU, zur Festplattennutzung sowie eine Miniaturansicht des Remote-Systems. Bestehende Jump Clients werden in den Jump Client-Statistiken zum nächsten Aktualisierungsintervall berücksichtigt.

Jump Client-Einstellungen

Aktualisierungsintervall für die Statistiken des aktiven Jump Client

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

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 Aktualisierungen der Zugriffskonsole.*

Maximale Bandbreite für gleichzeitige Upgrades für Jump Clients

Sie können die Bandbreitennutzung weiter steuern, indem Sie die Option **Maximale Bandbreite für gleichzeitige Jump Client-Aktualisierungen** festlegen.

> ***Hinweis:*** *Diese Einstellung hat keine Auswirkung auf Aktualisierungen der Zugriffskonsole.*

Gleichzeitigen Benutzerzugriff auf einen einzelnen Jump Client zulassen

Gleichzeitigen Zugriff mehrerer Benutzer auf einen Jump Client zulassen 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. Der erste Benutzer, der auf den Jump Client zugreift, wird Eigentümer der Sitzung. Benutzer in einer freigegebenen Jump-Sitzung sehen die jeweils anderen Benutzer und können mit der Chat-Funktion miteinander kommunizieren.

Hinweis: *Diese Einstellung (nur unter Windows) verhindert, dass ein Kunde einen Jump Client mithilfe des Rechtsklick-Kontextmenüs im Infobereich über seinen lokalen Rechner deaktiviert oder deinstalliert. Um den Jump Client zu entfernen, können Benutzer mit den entsprechenden Berechtigungen auf dem Client-System die Standardfunktion "Software" von Windows verwenden. Wird diese Einstellung geändert, wird sie bei der nächsten Verbindung mit dem Gerät erneut auf einen Jump Client angewendet.*

Benutzern 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 Kennworts für WOL-Umgebungen, welche ein sicheres WOL-Kennwort erfordern.

Standardverbindungstyp für Jump Client

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

Passiver Jump Client-Port

Der **Port für passive Jump Clients** gibt an, welcher Port von einem Jump Client verwendet wird, um einen „Aufweck“-Befehl vom Gerät 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 Gerät auf Port 80 oder 443 (ausgehend).

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

Jump-Richtlinien

Neue Jump-Richtlinie hinzufügen, bearbeiten, löschen

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

Jump-Richtlinien :: Hinzufügen

Anzeigename

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

Codename

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

Beschreibung

Fügen Sie eine kurze Beschreibung hinzu, um den Zweck dieses Objekts zusammenzufassen.

Jump-Zeitplan: Aktiviert

Legen Sie einen Zeitplan fest, der definiert, wann auf Jump Clients 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 einen Jump Client starten und auch nach dem festgelegten Endzeitpunkt weiterarbeiten. Er oder sie kann nach 17 Uhr allerdings nicht erneut auf diesen Jump Client zugreifen.

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 Client gestartet wird, der diese Jump-Richtlinie verwendet. Wenn ein Benutzer versucht, eine Sitzung mit einem

Jump-Client zu starten, der 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 einen Jump Client endet, der diese Jump-Richtlinie verwendet. Wenn ein Benutzer versucht, eine Sitzung mit einem Jump-Client zu starten, der 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 Gerät, 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-Client, der 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 Client versucht wird, der 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-Client anfordern kann, der diese Richtlinie verwendet. Der Benutzer kann eine kürzere Zugriffsdauer anfordern, die aber nicht länger sein darf als hier festgelegt.

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 Gerät, 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-Client, der 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-Richtlinien :: E-Mail-Benachrichtigungsvorlage

Betreff

Passen Sie den Betreff dieser E-Mail an. Verwenden Sie eines der unten auf der /login-Seite aufgeführten Makros, um den Text für Ihre Zwecke anzupassen.

Text

Passen Sie den Text dieser E-Mail an. Verwenden Sie eines der unten auf der /login-Seite aufgeführten Makros, um den Text für Ihre Zwecke anzupassen.

Jump-Richtlinien :: E-Mail-Genehmigungsvorlage

Betreff

Passen Sie den Betreff dieser E-Mail an. Verwenden Sie eines der unten auf der /login-Seite aufgeführten Makros, um den Text für Ihre Zwecke anzupassen.

Text

Passen Sie den Text dieser E-Mail an. Verwenden Sie eines der unten auf der /login-Seite aufgeführten Makros, um den Text für Ihre Zwecke anzupassen.

Jump-Richtlinien :: Ticketsystem

Ticketsystem-URL

Geben Sie unter **Ticketsystem-URL** die URL für Ihr externes Ticketsystem ein. Das Bomgar-Gerät 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.

Aktueller Status

Das Feld **Aktueller Status** wird nur angezeigt, wenn ein gültiger Statuswert vorliegt, um die Verbindung dem Ticketsystem zu melden, das unter **URL für Ticketsystem** konfiguriert wurde. Änderungen an der Ticketsystem-Konfiguration setzen den Wert

zurück.

Zertifikat für HTTPS-Verbindungen hochladen

Klicken Sie auf **Datei wählen**, um das Zertifikat für die HTTPS-Ticketsystemverbindung zum Gerät hochzuladen. Wird Ihr Zertifikat hochgeladen, verwendet das Gerät 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 Bomgar-Gerät beim Senden der Anfrage optional auf den integrierten Zertifikatspeicher zurück.

SSL-Zertifikatfehler ignorieren

Falls aktiviert, fügt das Bomgar-Gerät **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.

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.

Jumpoint: Einrichten des unüberwachten Zugriffs auf ein Netzwerk

Jumpoint-Verwaltung

Bomgars Jump-Technologie ermöglicht es einem Benutzer, auf Computer auf einem Remote-Netzwerk zuzugreifen, ohne Software auf jedem System 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 ein neues Objekt, bearbeiten Sie ein bestehendes Objekt oder entfernen Sie ein bestehendes Objekt.

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.*

Jumpoint :: Hinzufügen oder Bearbeiten

Name

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

Codename

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

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, aktivieren Sie **Shell Jump-Zugriff aktivieren**.

Benutzer hinzufügen

Auf der Jumpoint-Bearbeitungsseite können Sie Benutzer dazu berechtigen, Sitzungen über diesen Jumpoint zu starten. Nach Erstellen des Jumpoints können Sie über **Benutzer und Sicherheit > Gruppenrichtlinien** auch Benutzergruppen den Zugriff erteilen.

Massenimportassistent für symbolische Jump-Links

Bei der Erstellung einer großen Anzahl an symbolischen Jump-Links ist es möglicherweise einfacher, diese über ein Spreadsheet zu importieren, statt sie einzeln in der Zugriffskonsole hinzuzufügen. Wählen Sie aus der Dropdown-Liste im **Massenimportassistent für symbolische Jump-Links** die Art von Jump-Element, das Sie hinzufügen möchten und klicken Sie dann auf **Vorlage herunterladen**. Nutzen Sie den Text in der CSV-Vorlage als Spaltenüberschriften und fügen Sie die Informationen für jeden symbolischen Jump-Link hinzu, den Sie hinzufügen möchten. Optionale Felder können ausgefüllt oder leer gelassen werden.

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. Nur ein Typ von Jump-Element kann in jeder CSV-Datei enthalten sein. Die CSV-Datei sollte das folgende Format aufweisen: Die maximale Dateigröße pro Upload ist 5 MB.

Symbolischer Jump-Link (lokal)

Feld	Beschreibung
Hostname	Der Hostname des Endpunktes, auf den dieser symbolische Jump-Link zugreifen soll.
Jump-Gruppe	Der Codename des Teams, das diesem Jump-Element zugeordnet werden sollte. ***Hinweis:*** *Mit der Importmethode kann ein Jump-Element nicht einer persönlichen Jump-Gruppe 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 Jump-Link (Remote)

Feld	Beschreibung
Hostname	Der Hostname des Endpunktes, auf den dieser symbolische Jump-Link zugreifen soll.
Jumpoint	Der Codename des Jumpoint, über den auf den Endpunkt zugegriffen wird.
Jump-Gruppe	Der Codename des Teams, das diesem Jump-Element zugeordnet werden sollte. ***Hinweis:*** *Mit der Importmethode kann ein Jump-Element nicht einer persönlichen Jump-Gruppe 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 Remote-Desktop-Protokoll-Link

Feld	Beschreibung
Hostname	Der Hostname des Endpunktes, auf den dieser symbolische Jump-Link zugreifen soll.
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.
Anzeigeauflösung (optional)	Legen Sie die Auflösung fest, in der das Remote-System angezeigt wird. Kann **primär** sein (Standard - die Größe Ihres primären Monitors), **Alle** (die Größe all Ihrer Monitore zusammen), or **XxY** (wobei **X** und **Y** eine Kombination von Höhe und Breite sind, z.B. **640x480**).
Qualität (optional)	Wählen Sie die Qualität aus, in welcher 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 oder **best_qual** (32-Bit für die höchste Bildauflösung). Diese kann nicht während der Remote-Desktop-Protokoll (RDP)-Sitzung geändert werden.
Konsolensitzung (optional)	**1**: Startet eine Konsolensitzung. **0**: Startet eine neue Sitzung (Standard).
Nicht vertrauenswürdiges	**1**: Ignoriert Zertifikatwarnungen. **0**: Zeigt eine Warnung, wenn das Serverzertifikat nicht verifiziert werden kann.

Feld	Beschreibung
Zertifikat ignorieren (optional)	
Jump-Gruppe	Der Codename des Teams, das diesem Jump-Element zugeordnet werden sollte. ***Hinweis:*** *Mit der Importmethode kann ein Jump-Element nicht einer persönlichen Jump-Gruppe 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 dieser symbolische Jump-Link zugreifen soll.
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).
Jump-Gruppe	Der Codename des Teams, das diesem Jump-Element zugeordnet werden sollte. ***Hinweis:*** *Mit der Importmethode kann ein Jump-Element nicht einer persönlichen Jump-Gruppe 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

Feld	Beschreibung
	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-Analyse: Berichte zu offenen Ports an Endpunkten

Konfiguration der Endpunkt-Analyse

Endpunkt-Analyse aktivieren

Falls aktiviert, wird einmal täglich ein Scan von offenen Ports an den Jump-Elementen durchgeführt.

TCP-Ports

Geben Sie die TCP-Ports ein, die gescannt werden sollten. Geben Sie mehrere Ports durch Leerzeichen oder Komma getrennt ein oder geben sie einen Portbereich ein, bei dem Sie den niedrigsten und höchsten Port mit einem Bindestrich trennen.

UDP-Ports

Geben Sie die UDP-Ports ein, die gescannt werden sollten. Geben Sie mehrere Ports durch Leerzeichen oder Komma getrennt ein oder geben sie einen Portbereich ein, bei dem Sie den niedrigsten und höchsten Port mit einem Bindestrich trennen.

Endpunkt-Analysebericht

Jump-Elementtyp

Wählen Sie aus der Dropdown-Liste die Art von Jump-Element, für das Sie einen Bericht erstellen möchten.

Jumpoint

Sie können die Ergebnisse einschränken, indem Sie nur Berichte zu Jump-Elementen erstellen, die sich über einen gewählten Jumpoint verbinden.

Offene Ports mit einschließen, die bereits als „Erwartet“ markiert wurden

Schränken Sie die Ergebnisse weiter ein, indem Sie Ports ausschließen, die bereits als erwartet markiert wurden.

Ergebnisse der Endpunkt-Analyse

Zeigen Sie offene Ports an, die an den auf der vorherigen Seite angegebenen Endpunkten gefunden wurden. Sie können alle Ports als erwartet festlegen, damit sie aus zukünftigen Berichten gefiltert werden. Ebenfalls können alle Ports auf unerwartet gesetzt werden.

Zugriffskonsole

Einstellungen für Zugriffskonsole: Standardmäßige Einstellungen für die Konsole verwalten

Zugriffskonsole verwalten

Sie können die standardmäßigen Einstellungen für die Zugrrifskonsole für Ihre gesamte Nutzerbasis konfigurieren, eine konsistente Benutzererfahrung für die 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 standardmäßige Bomgar-Einstellung als Vorschlag daneben angezeigt.

Die jeweiligen Einstellungen **Aktivieren** und **Deaktivieren** lassen sich über ein Administrator-Kontrollkästchen auch erzwingen. Erzwungene Einstellungen werden ab der nächsten Anmeldung des Benutzers wirksam und lassen sich nicht über die Konsole konfigurieren. Nicht erzwungene Einstellungen können von einem Benutzer mithilfe des Einstellungsfensters in der Zugriffskonsole überschrieben werden. Eine erzwungene Einstellung kann nicht überschrieben werden, es sei denn, ein Administrator deaktiviert das Kontrollkästchen **Erzwungen** in der /login-Verwaltungsschnittstelle.

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

Beachten Sie, dass gespeicherte Einstellungen erst mit der Anmeldung in der Konsole wirksam werden. Selbst wenn Sie die Änderungen speichern und durch Klick auf die Schaltfläche **Jetzt übernehmen** 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 dann alle Konsolenanmeldungen durch Benutzer mit Ihren verwalteten Standardeinstellungen. Für bestehende Benutzer werden bei der nächsten Anmeldung erzwungene Einstellungen übernommen, alle anderen Einstellungen bleiben jedoch unberührt.

Globale Einstellungen

Rechtschreibprüfung aktiviert

Im Abschnitt **Globale Einstellungen** können Sie die 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 :: Chatnachrichten

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

Wählen Sie, 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-Warteschlangen

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

Zugriffssitzungen

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

Alarme :: Warteschlangenalarme

Hörbare Alarme - Einen Sound 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 möchten.

Persönliche Warteschlange - Freigegebene Sitzungen

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

Team-Warteschlangen - 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.

Zugriffssitzungen :: Automatisches Verhalten

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.

Jump-Versuche im lokalen Netzwerk automatisch heraufsetzen

Wählen Sie, ob der Endpunkt-Client automatisch zur Ausführung als Systemdienst heraufgesetzt werden soll, wenn der Benutzer einen lokalen Netzwerk-Jump durchführt.

Zum Heraufsetzen auffordern, wenn sicherer Desktop des Endpunktes aktiviert ist

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

Zugriffssitzungen :: Werkzeuge

Bildschirmfreigabe

Standardqualität

Legen Sie die Standardqualität für Bildschirmfreigabe-Sitzungen fest.

Standardskalierung

Legen Sie die Standardgröße für Bildschirmfreigabe-Sitzungen fest.

Automatisch auf Vollbildschirmmodus umschalten, wenn die Bildschirmfreigabe beginnt

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

Automatisch die Seitenleiste ausblenden, wenn der Vollbildschirmmodus verwendet wird

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

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 für die Website.

Verwaltete Einstellungen der Zugriffskonsole anwenden

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 Nutzerbasis übernommen wurden, erhalten die Benutzer eine Benachrichtigung zur Bestätigung, wenn sie sich nach der Übernahme der Einstellungen zum ersten Mal wieder in der Zugriffskonsole anmelden. In der Benachrichtigung werden sie darüber informiert, dass die Einstellungen geändert wurden und haben die Option, ihr Einstellungsfenster in der Zugriffskonsole zu öffnen, um die Änderungen zu prüfen, oder die Benachrichtigung zu schließen.

Benutzerdefinierte Links: URL-Verknüpfungen zur Zugriffskonsole hinzufügen

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.

Neuen benutzerdefinierten Link erstellen, bearbeiten, löschen

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

Benutzerdefinierte Links :: Hinzufügen oder Bearbeiten

Name

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

URL

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

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

Vordefinierte Skripts

Erstellen Sie benutzerdefinierte Skripts, die in Bildschirmfreigabe- und Befehlsshell-Sitzungen verwendet werden. Das Skript wird während der Ausführung auf der Bildschirmfreigabe- oder Befehlsshell-Schnittstelle angezeigt. Das Ausführen eines Skriptes in der Bildschirmfreigabe-Schnittstelle zeigt das ausgeführte Skript auf dem Remote-Bildschirm an.

Filtern nach

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

Neues vordefiniertes Skript hinzufügen, bearbeiten, löschen

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

Vordefiniertes Skript :: Hinzufügen oder Bearbeiten

Skriptname

Erstellen Sie einen eindeutigen Namen, um dieses Objekt 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 Objekts 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.

Teams

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.

Heraufsetzungsmodus

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

Kategorien

Kategorie hinzufügen, löschen

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

Ressourcen

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.

Löschen

Entfernen Sie eine bestehende Ressourcendatei.

Spezielle Aktionen: Erstellen von benutzerdefinierten speziellen Aktionen

Benutzerdefinierte spezielle Aktionen

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

Eine neue benutzerdefinierte spezielle Aktion hinzufügen, bearbeiten, löschen

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

Spezielle Aktion hinzufügen oder bearbeiten

Aktionsname

Erstellen Sie einen eindeutigen Namen, um dieses Objekt 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 Benutezrs.

Argumente

Wenn der angegebene Befehl Befehlszeilenargumente akzeptiert, können Sie als nächstes diese Argumente eingeben. Argumente können falls notwendig Anführungszeichen verwenden, und Argumente für Windows-Systeme können die bereitgestellten Makros verwenden. Suchen Sie für weitere Informationen zu Windows-Argumenten mit dem Begriff „Befehlszeilenparameter" auf msdn.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 benutzerdefinierte spezielle Aktion durch ihre Wahl aus dem Menü während einer Sitzung sofort ausgeführt.

Heraufgesetzt ausführen

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

Einstellungen für spezielle Aktionen

Integrierte spezielle Aktionen anzeigen

Wenn Sie die von Bomgar 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. Außerdem führt das Deaktivieren der integrierten speziellen Aktionen nicht zur Deaktivierung der standardmäßigen speziellen Aktionen für Mobilgeräte.*

Benutzer und Sicherheit

Benutzer: Kontoberechtigungen für einen Benutzer oder Administrator hinzufügen

Benutzerkonten

Zeigen Sie Informationen über alle Benutzer an, die Zugriff auf Ihr Bomgar-Gerät haben, einschließlich der lokalen Benutzer und aller Benutzer, die über die Integration des Sicherheitsanbieters Zugriff haben.

Neuen Benutzer erstellen, bearbeiten, löschen

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

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.

Suchen

Suchen Sie Benutzerkonten anhand des Benutzernamens und des Anzeigenamens.

Zurücksetzen

Wenn ein Benutzer einen oder mehr fehlgeschlagene Anmeldungsversuche aufweist, klicken Sie auf die Schaltfläche **Zurücksetzen** neben seinem Namen, um den Zähler zurück auf 0 zu setzen.

Benutzer :: Hinzufügen oder Bearbeiten

Benutzereinstellungen

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 Kennwortzurücksetzungen oder Alarme zum erweiterten Verfügbarkeitsmodus.

Bevorzugte E-Mail-Sprache

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

Kennwort

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

Kennwort per E-Mail an Benutzer senden

Schickt eine automatische E-Mail an den Benutzer, die sein neues Kennwort enthält. Wenn diese Option ausgewählt wird, muss der Benutzer sein Kennwort bei der nächsten Anmeldung zurücksetzen. Diese Funktion erfordert eine gültige SMTP-Konfiguration für Ihr Gerät, die auf der Seite **/login > Verwaltung > E-Mail-Konfiguration** eingerichtet wird.

Muss Kennwort bei der nächsten Anmeldung zurücksetzen

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

Ablaufdatum für Kennwort

Führt dazu, dass das Kennwort nach einem bestimmten Datum oder nie abläuft.

Sicherheitsfrage und Sicherheitsantwort

Mit der Sicherheitsfrage und -antwort kann ein Benutzer ein vergessenes Kennwort zurücksetzen, wenn er die richtige Antwort auf die Frage eingibt. Kennwörter können nur zurückgesetzt werden, wenn **Kennwortrücksetzung aktivieren** auf der Seite **Verwaltung > Sicherheit** aktiviert wurde. Administratoren können ihre Kennwörter nicht über die Sicherheitsfrage zurücksetzen.

Gruppenrichtlinienmitgliedschaften

Liste der Gruppenrichtlinien, denen der Benutzer angehört, die auf die Seite **Gruppenrichtlinie** oder auf die Richtlinien selbst verweisen.

Teammitgliedschaften

Liste der Teams, denen der Benutzer angehört, die auf die Seite **Teams** oder auf die Teams selbst verweisen.

Kontoeinstellungen

Datum der letzten Authentifizierung

Datum und Uhrzeit der letzten Benutzeranmeldung.

Anmeldungscode per E-Mail senden

Aktiviert die Mehr-Faktor-Authentifizierung. Benutzer erhalten bei jeder Anmeldung in der /login-Verwaltungsschnittstelle eine E-Mail mit einem einzigartigen Authentifizierungscode, sowohl beim Desktop- wie auch beim Mobilzugriff. Wird der Code drei Mal hintereinander falsch eingegeben, müssen Benutzer ihre Anmeldedaten erneut eingeben und einen neuen E-Mail-Code eingeben.

Ablaufdatum des Kontos

Führt dazu, dass das Konto nach einem bestimmten Datum oder nie 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.

Berechtigungen

Administrator

Erteilt dem Benutzer volle Administratorrechte.

Berechtigt, Kennwörter festzulegen

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

Berechtigt, Jumpoints zu bearbeiten

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

Berechtigungen für Berichte zu Zugriffssitzung: Berechtigt, Berichte zu Zugriffssitzungen anzuzeigen

Ermöglicht dem Benutzer, Berichte zur Sitzungsaktivität auszuführen, nur Sitzungen anzuzeigen, bei denen er der primäre Sitzungseigentümer war, nur Sitzungen anzuzeigen, bei denen eines seiner Teams das primäre Team oder eines seiner Teammitglieder der primäre Sitzungseigentümer war, oder alle Sitzungen anzuzeigen.

Berechtigt, Aufzeichnungen von Zugriffssitzungen anzuzeigen

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

Berechtigt, Berichts-API zu verwenden

Damit können die Anmeldedaten des Benutzers verwendet werden, um XML-Berichte über die API aufzurufen.

Berechtigt, Befehls-API zu verwenden

Damit können die Anmeldedaten des Benutzers verwendet werden, um Befehle über die API auszugeben.

Berechtigt, Teams zu bearbeiten

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

Berechtigt, vordefinierte Skripts zu bearbeiten

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

Berechtigt, benutzerdefinierte Links zu bearbeiten

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

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.

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 Technology

Gestattete Jump-Methoden: Berechtigt, Sitzungen über Jump Clients zu starten, die eine der folgenden Jump-Methoden verwenden

Ermöglicht es dem Benutzer, mit **Jump Clients**, **Lokaler Jump im lokalen Netzwerk**, **Remote-Jump via Jumpoint**, **RDP via Jumpoint** und/oder **Shell Jump via Jumpoint** Jumps zu Computern auszuführen.

Berechtigungen für Jump-Elemente: Berechtigt, Sitzungen von allen Jump-Elementen im System aus zu starten

Damit kann der Benutzer Jumps auf Remote-Computer in allen Team-Jump-Gruppen durchführen.

Berechtigt, Jump-Elemente in den folgenden Jump-Gruppen bereitzustellen, zu entfernen und zu ändern

Erlaubt dem Benutzer, nur für die persönliche Jump-Gruppe; für die Jump-Gruppen von Teams und Teammitgliedern; oder für alle Jump-Gruppen einschließlich der für Teams bereitgestellten Jump-Gruppen, zu denen der Benutzer nicht gehört sowie für alle persönlichen Jump-Gruppen von Benutzern Sitzungen zu fixieren, Gruppen festzulegen und Kommentare zu Jump-Elementen hinzuzufügen.

Berechtigt, die den Jump-Elementen zugewiesenen Sitzungsrichtlinien zu ändern

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

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

Ermöglicht es dem Benutzer, den Remote-Bildschirm anzuzeigen oder zu steuern. Falls **Nicht definiert** gewählt wurde, wird diese Option durch die Richtlinie der nächstniedrigeren Priorität bestimmt. Diese Einstellung kann von einer Richtlinie mit höherer Priorität überschrieben werden.

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- und Linux-Betriebssysteme und wirkt sich nicht auf Remote Desktop Protocol (RDP)-Sitzungen aus.*

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.

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 Kennwortspeichern oder Vaults zu verwenden.

Die Verwendung des Endpoint Credential Managers erfordert eine separate Dienstleistungsvereinbarung mit Bomgar. Nach Abschluss einer Dienstleistungsvereinbarung können Sie die erforderliche Middleware vom Bomgar Self-Service Center herunterladen.

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 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

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

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

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.

Systeminformationen

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

Zugriff auf Registrierung

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.

Andere Tools

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.

Heraufsetzung

Gibt dem Benutzer die Möglichkeit zu versuchen, den Kunden-Client so heraufzusetzen, dass er mit administrativen Rechten auf dem Remote-System ausgeführt wird.Falls **Nicht definiert** gewählt wurde, wird diese Option durch die Richtlinie der nächstniedrigeren Priorität bestimmt. Diese Einstellung kann von einer Richtlinie mit höherer Priorität überschrieben werden.

Anmeldungszeitplan

Die Benutzeranmeldung auf den folgenden Zeitplan beschränken

Legen Sie einen Zeitplan fest, der definiert, wann sich Benutzer an der Zugriffskonsole anmelden können. Legen Sie die Zeitzone fest, die für diesen Zeitplan verwendet werden soll, und fügen Sie dann einen oder mehrere Zeitplaneinträge hinzu. Geben Sie für jeden Eintrag das Startdatum und die Startuhrzeit an sowie das Enddatum und die Enduhrzeit.

Wenn die Zeit beispielsweise für 8 Uhr (Start) und 17 Uhr (Ende) festgelegt wird, kann sich ein Benutzer jederzeit innerhalb dieses Zeitfensters anmelden und auch nach dem festgelegten Endzeitpunkt weiterarbeiten. Er kann sich nach 17 Uhr allerdings nicht erneut anmelden.

Abmeldung erzwingen, wenn der Zeitplan die Anmeldung nicht gestattet

Wenn eine strengere Zugriffskontrolle erforderlich ist, aktivieren Sie diese Option. Damit wird der Benutzer gezwungen, sich zum geplanten Endzeitpunkt abzumelden. Iin diesem Fall erhält der Benutzer 15 Minuten vor der Trennung der Verbindung wiederholte Benachrichtigungen. Wenn der Benutzer abgemeldet wird, folgen jegliche ihm angehörenden Sitzungen den Regeln zum Sitzungsrückfall.

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 Kennwortrücksetzung: Benutzern gestatten, Kennwörter zu verwalten

Benutzerkonten

Administratoren können durch die Erteilung von Benutzerberechtigungen die Rücksetzung lokaler Benutzerkennwörter und gesperrter Benutzerkonten an berechtigte Benutzer delegieren, ohne diesen dabei den vollständigen Administratorzugang zu gewähren. Lokale Benutzer können ihre eigenen Kennwörter weiterhin zurücksetzen.

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

Wenn ein berechtigter Benutzer ohne Administratorrechte auf die Seite **Benutzer und Sicherheit > Benutzer** in der /login-Verwaltungsschnittstelle zugreift, wird er einen eingeschränkt sichtbaren **Benutzer**-Bildschirm sehen, welcher Links zur **Kennwortänderung** 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.

Suchen

Suchen Sie Benutzerkonten anhand des Benutzernamens und des Anzeigenamens.

Zurücksetzen

Wenn ein Benutzer einen oder mehr fehlgeschlagene Anmeldungsversuche aufweist, klicken Sie auf die Schaltfläche **Zurücksetzen** neben seinem Namen, um den Zähler zurück auf 0 zu setzen.

Kennwort ändern

Ändern Sie das Kennwort für einen nichtadministrativen Benutzer.

Benutzer :: Kennwort ändern

Benutzername

Eindeutige Kennung, die zur Anmeldung verwendet wird. Dieses Feld kann nicht bearbeitet werden.

Anzeigenamen

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 Kennwortrücksetzungen oder Alarme zum erweiterten Verfügbarkeitsmodus, gesendet werden. Dieses Feld kann nicht bearbeitet werden.

Kommentare

Kommentare zum Konto. Dieses Feld kann nicht bearbeitet werden.

Kennwort

Das neue Kennwort, das diesem Benutzerkonto zugewiesen werden soll. Das Kennwort kann nach eigenen Wünschen festgelegt werden, solange die Zeichenfolge die definierte Richtlinie erfüllt, die auf der Seite **/login > Verwaltung > Sicherheit** festgelegt wurde.

Kennwort per E-Mail an Benutzer senden

Schickt eine automatische E-Mail an den Benutzer, die sein neues Kennwort enthält. Wenn diese Option ausgewählt wird, muss der Benutzer sein Kennwort bei der nächsten Anmeldung zurücksetzen. Diese Funktion erfordert eine gültige SMTP-Konfiguration für Ihr Gerät, die auf der Seite **/login > Verwaltung > E-Mail-Konfiguration** eingerichtet wird.

Muss Kennwort bei der nächsten Anmeldung zurücksetzen

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

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

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. Verwenden Sie eines der unten auf der /login-Seite aufgeführten Makros, um den Text für Ihre Zwecke anzupassen.

Text

Passen Sie den Text dieser E-Mail an. Verwenden Sie eines der unten auf der /login-Seite aufgeführten Makros, um den Text für Ihre Zwecke anzupassen.

Sicherheitsanbieter: Anmeldung für LDAP, Active Directory, RADIUS und Kerberos aktivieren

Sicherheitsanbieter

Sie können Ihr Bomgar-Gerät für die Authentifizierung von Benutzern anhand bestehender LDAP-, RADIUS- 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 Multifaktor-Authentifizierungsmechanismen über RADIUS eine zusätzliche Sicherheitsstufe bieten.

Anbieter erstellen

Erstellen Sie eine neue Sicherheitsanbieter-Konfiguration. Wählen Sie aus dem Dropdown-Menü einen LDAP-Anbieter, RADIUS-Anbieter oder Kerberos-Anbieter.

Protokoll anzeigen

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

Synchronisieren

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

Deaktivieren

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

Bearbeiten, löschen

Bearbeiten oder entfernen Sie ein bestehendes Objekt.

Kopie erstellen

Erstellen Sie eine Kopie einer bestehenden Sicherheitsanbieter-Konfiguration. Diese wird als Sicherheitsanbieter auf oberster Ebene und nicht als Teil eines Clusters hinzugefügt.

Knoten duplizieren

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

Auf Cluster upgraden

Stufen Sie einen Sicherheitsanbieter auf einen Sicherheitsanbieter-Cluster auf. Um diesem Cluster mehr Sicherheitsanbieter hinzuzufügen, kopieren Sie einen bestehenden Knoten.

Reihenfolge ändern

Klicken Sie auf diese Schaltfläche, um die Priorität von Sicherheitsanbietern per Drag and Drop festzulegen. Ziehen Sie Server in einem Cluster. Cluster können auch als Ganzes durch Ziehen verschoben werden. Klicken Sie auf **Reihenfolge speichern**. Dadurch treten die Priorisierungsänderungen in Kraft.

Sicherheitsanbieter :: Bearbeiten - LDAP

Allgemeine Einstellungen

Name

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

Aktiviert: Dieser Anbieter ist aktiviert

Falls aktiviert, kann Ihr Bomgar-Gerät diesen Sicherheitsanbieter durchsuchen, wenn sich ein Benutzer anmeldet. Falls nicht aktiviert, wird dieser Sicherheitsanbieter nicht durchsucht.

Benutzeranzeigenamen: Anzeigenamen mit Remote-System synchronisiert lassen

Diese Felder legen fest, welche Felder als die privaten und öffentlichen Anzeigenamen des Benutzers verwendet werden.

Synchronisierung: LDAP-Objektzwischenspeicher aktivieren

Falls aktiviert, werden dem Gerät sichtbare LDAP-Objekte nächtlich oder falls gewünscht 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.

Autorisierungseinstellungen

Gruppen suchen

Wählen Sie, ob Sie diesen Sicherheitsanbieter nur für die Benutzerauthentifizierung, nur für Gruppensuchen oder für beides verwenden möchten.

Standardmäßige Gruppenrichtlinie *(Nur sichtbar, wenn die Benutzerauthentifizierung gestattet wurde)*

Jeder Benutzer, der sich an einem externen Server authentifiziert, muss Mitglied mindestens einer Gruppenrichtlinie sein, damit er sich an Ihrem Bomgar-Gerät 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 Subject-Namen des öffentlichen SSL-Zertifikats, das Ihr LDAP-Server verwendet, übereinstimmen, oder mit der DNS-Komponente des alternativen Subject-Namens.*

Port

Geben Sie den Port für Ihren LDAP-Server an. Dies ist in der Regel Port **389** für LDAP oder Port **636** für LDAPS. Bomgar unterstützt ebenfalls Global Catalog über den 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* ****.beispiel.com*** *sowohl* ***zugriff.beispiel.com*** *als auch* ***remote.beispiel.com****.*

Anmeldedaten binden

Geben Sie einen Benutzernamen und ein Kennwort an, das Ihr Bomgar-Gerät 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 Kennwort durchführen. Anonyme Bindungen gelten als unsicher und sind standardmäßig an den meisten LDAP-Servern deaktiviert.

Verbindungsmethode

Wenn Sie einen externen Verzeichnisspeicher im gleichen lokalen Netzwerk wie Ihr Bomgar-Gerät verwenden, können die beiden Systeme möglicherweise direkt kommunizieren. In diesem Fall können Sie die Option **Proxy vom Gerät über den Connection Agent** deaktiviert belassen 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 Bomgar-Gerät, 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 **Kennwort 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 Kennwort für den Connection Agent einzugeben, das Sie oben erstellt haben.

Verzeichnistyp

Um die Konfiguration der Netzwerkverbindung zwischen Ihrem Bomgar-Gerät 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 Bomgar auch auf die Kommunikation mit den meisten Sicherheitsanbietern konfigurieren.

Cluster-Einstellungen *(Nur bei Clustern sichtbar)*

Mitgliederauswahlalgorithmus

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.

Benutzerschemaeinstellungen

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 Bomgar-Gerät mit der Benutzersuche beginnen soll. Abhängig von der Größe Ihres Verzeichnisspeichers und der Benutzer, die Bomgar-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 Bomgar-Gerät 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 Bomgar-Gerät das Schema zu kennzeichnen, das der LDAP-Server zur Identifizierung von Benutzern verwendet. Sie können mehrere Objektklassen eingeben, eine pro Zeile.

Attributnamen

Geben Sie an, welche Felder für die eindeutige ID und den Anzeigenamen eines Benutzers verwendet werden sollen.

Eindeutige ID

Dieses Feld benötigt eine eindeutige Kennung für das Objekt. Auch wenn der repräsentative Name als diese ID dienen kann, kann sich der repräsentative Name eines Benutzers im Laufe der Zeit häufig ändern, etwa aufgrund von Namens- oder

Standortänderungen oder durch die Umbenennung des LDAP-Speichers. Daher verwenden die meisten LDAP-Server ein Feld, das pro Objekt einzigartig ist und sich für die gesamte Lebenszeit des Benutzers nicht ändert. Wenn Sie den repräsentativen Namen als einzigartige ID verwenden und sich der repräsentative Name eines Benutzers ändert, wird dieser Benutzer als neuer Benutzer angesehen und jegliche Änderungen, die am Bomgar-Benutzerkonto dieser Person vorgenommen werden, werden nicht für 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.

Verwenden des gleichen Attributs für öffentliche und private Anzeigenamen

Ist diese Option aktiviert, können Sie separate Werte für die privaten und öffentlichen Anzeigenamen des Benutzers angeben.

Anzeigenamen

Diese Werte legen fest, welche Felder als die privaten und öffentlichen Anzeigenamen des Benutzers verwendet werden sollen.

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

Basis-DN suchen

Legen Sie die Ebene in Ihrer Verzeichnishierarchie fest (angegeben durch einen repräsentativen Namen), auf der das Bomgar-Gerät mit der Gruppensuche beginnen soll. Abhängig von der Größe Ihres Verzeichnisspeichers und der Gruppen, welche Zugriff auf das Bomgar-Gerät 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 Bomgar-Gerät 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 Kennwort

Geben Sie einen Benutzernamen und ein Kennwort 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 Kennwort zum Testen eingegeben haben, erhalten Sie eine positive Meldung. Andernfalls sehen Sie eine Fehlermeldung und ein Protokoll, das bei der Fehlerbehebung helfen kann.

Sicherheitsanbieter :: Bearbeiten - RADIUS

Allgemeine Einstellungen

Name

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

Aktiviert: Dieser Anbieter ist aktiviert

Falls aktiviert, kann Ihr Bomgar-Gerät diesen Sicherheitsanbieter durchsuchen, wenn sich ein Benutzer anmeldet. Falls nicht aktiviert, wird dieser Sicherheitsanbieter nicht durchsucht.

Anzeigenamen: Anzeigenamen mit Remote-System synchronisiert lassen

Diese Felder legen fest, welche Felder als die privaten und öffentlichen Anzeigenamen des Benutzers verwendet werden.

Autorisierungseinstellungen

Nur die folgenden Benutzer zulassen

Sie können den Zugriff nur bestimmten Benutzern auf Ihrem RADIUS-Server gewähren. Jeder Benutzername sollte dabei durch einen Zeilenumbruch getrennt werden. Nach der Eingabe stehen diese Benutzer über das Dialogfeld **Richtlinienmitglied hinzufügen** bei der Bearbeitung von Gruppenrichtlinien auf der Seite **/login > Benutzer und Sicherheit > Gruppenrichtlinien** zur Verfügung.

Wenn Sie dieses Feld leer lassen, werden alle Benutzer zugelassen, die sich über Ihren RADIUS-Server authentifizieren. Wenn Sie alle Benutzer zulassen, müssen Sie außerdem eine standardmäßige Gruppenrichtlinie angeben.

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 Bomgar-Gerät 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.

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**.

Verbindungsmethode

Wenn Sie einen externen Verzeichnisspeicher im gleichen lokalen Netzwerk wie Ihr Bomgar-Gerät verwenden, können die beiden Systeme möglicherweise direkt kommunizieren. In diesem Fall können Sie die Option **Proxy vom Gerät über den Connection Agent** deaktiviert belassen 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 Bomgar-Gerät, 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 **Kennwort 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 Kennwort für den Connection Agent einzugeben, das Sie oben erstellt haben.

Gemeinsamer geheimer Schlüssel

Geben Sie einen neuen gemeinsamen geheimen Schlüssel an, damit Ihr Bomgar-Gerät mit Ihrem RADIUS-Server kommunizieren kann.

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.

Cluster-Einstellungen *(Nur bei Clustern sichtbar)*

Mitgliederauswahlalgorithmus

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 Kennwort

Geben Sie einen Benutzernamen und ein Kennwort 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 Kennwort zum Testen eingegeben haben, erhalten Sie eine positive Meldung. Andernfalls sehen Sie eine Fehlermeldung und ein Protokoll, das bei der Fehlerbehebung helfen kann.

Sicherheitsanbieter :: Bearbeiten - Kerberos

Allgemeine Einstellungen

Name

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

Aktiviert: Dieser Anbieter ist aktiviert

Falls aktiviert, kann Ihr Bomgar-Gerät diesen Sicherheitsanbieter durchsuchen, wenn sich ein Benutzer anmeldet. Falls nicht aktiviert, wird dieser Sicherheitsanbieter nicht durchsucht.

Benutzer- und Anzeigenamen: Anzeigenamen mit Remote-System synchronisiert lassen

Diese Felder legen fest, welche Felder als die privaten und öffentlichen Anzeigenamen des Benutzers verwendet werden.

Realm aus Principal-Namen entfernen

Wählen Sie diese Option, um den REALM-Teil aus dem Benutzer-Principal-Namen zu entfernen, wenn Sie den Bomgar-Benutzernamen erstellen.

Autorisierungseinstellungen

Benutzer-Bearbeitungsmodus

Wählen Sie, welche Benutzer sich an Ihrem Bomgar-Gerät 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 Benutzer-Principals, die explizit aufgeführt wurden. **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.

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 Bomgar-Gerät 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.

Sitzungsrichtlinien: Sitzungsberechtigungen und Aufforderungsregeln festlegen

Sitzungsrichtlinien

Mit Sitzungsrichtlinien können Sie die Sicherheitsberechtigungen für Sitzungen Tech. auf bestimmte Szenarien zuschneiden. Sitzungsrichtlinien können auf Benutzer und auf Jump Clients angewandt 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.

Neue Richtlinie erstellen, bearbeiten, löschen

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

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.

Sitzungsrichtlinie :: Hinzufügen oder Bearbeiten

Richtlinieneinstellungen

Anzeigename

Erstellen Sie einen eindeutigen Namen, um dieses Objekt 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, wird automatisch einer erstellt.

Beschreibung

Fügen Sie eine kurze Beschreibung hinzu, um den Zweck dieses Objekts 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.

Verfügbarkeit: Zugriffseinladung

Wählen Sie, ob diese Richtlinie zur Verwendung durch Benutzer zur Verfügung stehen soll, wenn ein externer Benutzer zu einer Sitzung eingeladen wird.

Verfügbarkeit: Jump Clients

Wählen Sie, ob diese Richtlinie zur Zuweisung an Jump Clients zur Verfügung stehen soll.

Verfügbarkeit: Abhängigkeiten

Wenn diese Sitzungsrichtlinie bereits verwendet wird, sehen Sie die Anzahl der Benutzer und Jump Clients, welche die Richtlinie verwenden.

Werkzeuge

Für alle folgenden Berechtigungen können Sie die Berechtigung aktivieren oder deaktivieren, oder sie auf **Nicht definiert** setzen. Sitzungsrichtlinien werden auf hierarchische Art und Weise auf eine Sitzung angewandt, wobei Jump Clients die höchste Priorität haben, gefolgt von Benutzern und schließlich dem globalen Standard. Wenn für eine Sitzung mehrere Richtlinien gelten, erhält die Richtlinie mit der höchsten Priorität Vorrang. Wenn beispielsweise die auf einen Jump Client angewandte Richtlinie eine Berechtigung festlegt, dürfen keine anderen Richtlinien diese Berechtigung für die Sitzung ändern. Um eine Berechtigung durch eine Richtlinie mit niedrigerer Priorität definierbar zu machen, belassen Sie diese Berechtigung auf **Nicht definiert**. Einzelheiten und Beispiele finden Sie unter So verwenden Sie Richtlinien für Sitzungen.

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

Bildschirmfreigabe

Ermöglicht es dem Benutzer, den Remote-Bildschirm anzuzeigen oder zu steuern. Falls **Nicht definiert** gewählt wurde, wird diese Option durch die Richtlinie der nächstniedrigeren Priorität bestimmt. Diese Einstellung kann von einer Richtlinie mit höherer Priorität überschrieben werden.

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- und Linux-Betriebssysteme und wirkt sich nicht auf Remote Desktop Protocol (RDP)-Sitzungen aus.*

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.

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 Kennwortspeichern oder Vaults zu verwenden.

Die Verwendung des Endpoint Credential Managers erfordert eine separate Dienstleistungsvereinbarung mit Bomgar. Nach Abschluss einer Dienstleistungsvereinbarung können Sie die erforderliche Middleware vom Bomgar Self-Service Center herunterladen.

> ***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 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

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

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

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.

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

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

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.

Heraufsetzung

Gibt dem Benutzer die Möglichkeit zu versuchen, den Kunden-Client so heraufzusetzen, dass er mit administrativen Rechten auf dem Remote-System ausgeführt wird.Falls **Nicht definiert** gewählt wurde, wird diese Option durch die Richtlinie der nächstniedrigeren Priorität bestimmt. Diese Einstellung kann von einer Richtlinie mit höherer Priorität überschrieben werden.

Richtlinie speichern

Klicken Sie auf **Richtlinie speichern**, um diese Richtlinie verfügbar zu machen.

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 Bomgar-Website importieren, die den Import von Sitzungsrichtlinien unterstützt. Erstellen Sie eine neue Sitzungsrichtlinie und scrollen Sie zum Ende der Seite. Durchsuchen Sie die Richtliniendatei, und klicken Sie auf **Richtlinie importieren**. Nachdem die Richtliniendatei hochgeladen wurde, wird die Seite aktualisiert, sodass Sie Änderungen vornehmen können. Klicken Sie auf **Richtlinie speichern**, um die Richtlinie verfügbar zu machen.

Sitzungsrichtliniensimulator

Da die Schichtung von Richtlinien komplex sein kann, können Sie den **Sitzungsrichtliniensimulator** verwenden, um zu erfahren, welches Ergebnis Sie erhalten. Darüber hinaus können Sie den Simulator auch verwenden, um festzustellen, warum eine Berechtigung entgegen Ihren Erwartungen nicht verfügbar ist.

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. Dies kann ein **Jump Client**, **Remote-Jump** oder **Lokaler Jump** sein.

Jump Client / Jump-Element

Suchen Sie nach einem Jump-Element mithilfe von Name, Kommentare, 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

Gruppenrichtlinien

Mit der Seite **Gruppenrichtlinien** können Sie Benutzergruppen mit gemeinsamen Berechtigungen einrichten.

Neue Richtlinie erstellen, bearbeiten, löschen

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

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.

Reihenfolge ändern

Klicken Sie auf diese Schaltfläche, um die Priorität von Gruppenrichtlinien per Drag and Drop festzulegen. Klicken Sie auf **Reihenfolge speichern**. Dadurch treten die Priorisierungsänderungen in Kraft. Zu Verwaltungszwecken besteht die empfohlene Prioritätsfolge darin, Richtlinien für spezifischere Benutzergruppen als höhere Priorität zu definieren (und das Überschreiben zu verhindern) und sich nach unten vorzuarbeiten, wobei breiteren Gruppen eine niedrigere Prioritätsstufe zugewiesen wird.

Gruppenrichtlinie :: Hinzufügen oder Bearbeiten

Grundeinstellungen

Anmeldungscode per E-Mail senden

Aktiviert die Mehr-Faktor-Authentifizierung. Benutzer erhalten bei jeder Anmeldung in der /login-Verwaltungsschnittstelle eine E-Mail mit einem einzigartigen Authentifizierungscode, sowohl beim Desktop- wie auch beim Mobilzugriff. Wird der Code drei Mal hintereinander falsch eingegeben, müssen Benutzer ihre Anmeldedaten erneut eingeben und einen neuen E-Mail-Code eingeben.

Richtlinienname

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

Richtlinienmitglieder

Um Mitglieder zuzuweisen, klicken Sie auf die Schaltfläche **Hinzufügen**, um ein Auswahlkästchen zu öffnen. Wählen Sie Benutzer Ihres lokalen Systems oder wählen Sie Benutzer oder gesamte Gruppen von konfigurierten Sicherheitsanbietern. 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

In dieser Richtlinie definiert

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.

Ablaufdatum des Kontos

Führt dazu, dass das Konto nach einem bestimmten Datum oder nie 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.

Berechtigungen

Administrator

Erteilt dem Benutzer volle Administratorrechte.

Berechtigt, Kennwörter festzulegen

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

Berechtigt, Jumpoints zu bearbeiten

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

Berechtigungen für Berichte zu Zugriffssitzung: Berechtigt, Berichte zu Zugriffssitzungen anzuzeigen

Ermöglicht dem Benutzer, Berichte zur Sitzungsaktivität auszuführen, nur Sitzungen anzuzeigen, bei denen er der primäre Sitzungseigentümer war, nur Sitzungen anzuzeigen, bei denen eines seiner Teams das primäre Team oder eines seiner Teammitglieder der primäre Sitzungseigentümer war, oder alle Sitzungen anzuzeigen.

Berechtigt, Aufzeichnungen von Zugriffssitzungen anzuzeigen

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

Berechtigt, Berichts-API zu verwenden

Damit können die Anmeldedaten des Benutzers verwendet werden, um XML-Berichte über die API aufzurufen.

Berechtigt, Befehls-API zu verwenden

Damit können die Anmeldedaten des Benutzers verwendet werden, um Befehle über die API auszugeben.

Berechtigt, Teams zu bearbeiten

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

Berechtigt, vordefinierte Skripts zu bearbeiten

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

Berechtigt, benutzerdefinierte Links zu bearbeiten

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

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.

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 Technology

Gestattete Jump-Methoden: Berechtigt, Sitzungen über Jump Clients zu starten, die eine der folgenden Jump-Methoden verwenden

Ermöglicht es dem Benutzer, mit **Jump Clients**, **Lokaler Jump im lokalen Netzwerk**, **Remote-Jump via Jumpoint**, **RDP via Jumpoint** und/oder **Shell Jump via Jumpoint** Jumps zu Computern auszuführen.

Berechtigungen für Jump-Elemente: Berechtigt, Sitzungen von allen Jump-Elementen im System aus zu starten

Damit kann der Benutzer Jumps auf Remote-Computer in allen Team-Jump-Gruppen durchführen.

Berechtigt, Jump-Elemente in den folgenden Jump-Gruppen bereitzustellen, zu entfernen und zu ändern

Erlaubt dem Benutzer, nur für die persönliche Jump-Gruppe; für die Jump-Gruppen von Teams und Teammitgliedern; oder für alle Jump-Gruppen einschließlich der für Teams bereitgestellten Jump-Gruppen, zu denen der Benutzer nicht gehört sowie für alle persönlichen Jump-Gruppen von Benutzern Sitzungen zu fixieren, Gruppen festzulegen und Kommentare zu Jump-Elementen hinzuzufügen.

Berechtigt, die den Jump-Elementen zugewiesenen Sitzungsrichtlinien zu ändern

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

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

Ermöglicht es dem Benutzer, den Remote-Bildschirm anzuzeigen oder zu steuern. Falls **Nicht definiert** gewählt wurde, wird diese Option durch die Richtlinie der nächstniedrigeren Priorität bestimmt. Diese Einstellung kann von einer Richtlinie mit höherer Priorität überschrieben werden.

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- und Linux-Betriebssysteme und wirkt sich nicht auf Remote Desktop Protocol (RDP)-Sitzungen aus.*

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.

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 Kennwortspeichern oder Vaults zu verwenden.

Die Verwendung des Endpoint Credential Managers erfordert eine separate Dienstleistungsvereinbarung mit Bomgar. Nach Abschluss einer Dienstleistungsvereinbarung können Sie die erforderliche Middleware vom Bomgar Self-Service Center herunterladen.

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 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

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

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

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.

Systeminformationen

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

Zugriff auf Registrierung

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.

Andere Tools

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.

Heraufsetzung

Gibt dem Benutzer die Möglichkeit zu versuchen, den Kunden-Client so heraufzusetzen, dass er mit administrativen Rechten auf dem Remote-System ausgeführt wird.Falls **Nicht definiert** gewählt wurde, wird diese Option durch die Richtlinie der

nächstniedrigeren Priorität bestimmt. Diese Einstellung kann von einer Richtlinie mit höherer Priorität überschrieben werden.

Anmeldungszeitplan

Die Benutzeranmeldung auf den folgenden Zeitplan beschränken

Legen Sie einen Zeitplan fest, der definiert, wann sich Benutzer an der Zugriffskonsole anmelden können. Legen Sie die Zeitzone fest, die für diesen Zeitplan verwendet werden soll, und fügen Sie dann einen oder mehrere Zeitplaneinträge hinzu. Geben Sie für jeden Eintrag das Startdatum und die Startuhrzeit an sowie das Enddatum und die Enduhrzeit.

Wenn die Zeit beispielsweise für 8 Uhr (Start) und 17 Uhr (Ende) festgelegt wird, kann sich ein Benutzer jederzeit innerhalb dieses Zeitfensters anmelden und auch nach dem festgelegten Endzeitpunkt weiterarbeiten. Er kann sich nach 17 Uhr allerdings nicht erneut anmelden.

Abmeldung erzwingen, wenn der Zeitplan die Anmeldung nicht gestattet

Wenn eine strengere Zugriffskontrolle erforderlich ist, aktivieren Sie diese Option. Damit wird der Benutzer gezwungen, sich zum geplanten Endzeitpunkt abzumelden. Iin diesem Fall erhält der Benutzer 15 Minuten vor der Trennung der Verbindung wiederholte Benachrichtigungen. Wenn der Benutzer abgemeldet wird, folgen jegliche ihm angehörenden Sitzungen den Regeln zum Sitzungsrückfall.

Mitgliedschaften

Teams

Bezeichnet die Teams, zu denen Benutzer in dieser Gruppe hinzugefügt werden sollten. Ist ein Benutzer in einer anderen Gruppe, die Benutzer zu einem Team hinzufügt, Sie aber nicht möchten, dass Benutzer dieser Gruppe in diesem Team sein sollen, legen Sie diese Richtlinie fest, um Benutzer aus dem jeweiligen Team zu entfernen. Manuell zu einem Team hinzugefügte Benutzer können nicht mithilfe einer Gruppenrichtlinie entfernt werden.

Jumpoints

Bezeichnet Jumpoints, auf die Benutzer in dieser Gruppe zugreifen können.

Nur für Gruppenrichtlinien: Ist ein Benutzer in einer anderen Gruppe, die Zugriff zu einem Jumpoint erteilt, Sie aber nicht möchten, dass Benutzer dieser Gruppe Zugriff auf diesen Jumpoint haben, legen Sie diese Richtlinie fest, um Benutzer von diesem Jumpoint zu entfernen. Manuell zu einem Jumpoint hinzugefügte Benutzer können nicht mithilfe einer Gruppenrichtlinie entfernt werden.

Richtlinie speichern

Klicken Sie auf **Richtlinie 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 Richtlinienname, die Kontoeinstellungen und die Berechtigungen exportiert. Richtlinienmitglieder, Support-Mitgliedschaften und Jumpoint-Mitgliedschaften sind nicht im Export enthalten.*

Richtlinie importieren

Sie können exportierte Gruppenrichtlinieneinstellungen auf jeder anderen Bomgar-Website importieren, die den Import von Gruppenrichtlinien unterstützt. Erstellen Sie eine neue Gruppenrichtlinie, oder bearbeiten Sie eine vorhandene Richtlinie, deren Berechtigungen Sie überschreiben möchten, und rollen Sie zum Ende der Seite. Durchsuchen Sie die Richtliniendatei, und klicken Sie auf **Richtlinie importieren**. Nachdem die Richtliniendatei hochgeladen wurde, wird die Seite aktualisiert, sodass Sie Änderungen vornehmen können; klicken Sie auf **Richtlinie speichern**, damit die Gruppenrichtlinie wirksam wird.

Hinweis: *Durch Importieren einer Richtliniendatei in eine bestehende Gruppenrichtlinie werden alle zuvor festgelegten Berechtigungen überschrieben; ausgenommen sind Richtlinienmitglieder, Teammitgliedschaften und Jumpoint-Mitgliedschaften.*

Kerberos-Keytab: Kerberos-Keytab verwalten

Kerberos-Keytab-Verwaltung

Bomgar unterstützt die Einzelanmeldungs-Funktion mithilfe des Kerberos-Authentifizierungsprotokolls. Hierdurch können sich Benutzer beim Bomgar-Gerät authentifizieren, ohne ihre Anmeldedaten eingeben zu müssen. Kerberos-Authentifizierung gilt sowohl für die Webschnittstelle /login als auch für die Zugriffskonsole.

Um Kerberos mit Ihrem Bomgar-Gerät 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 Bomgar-Gerät 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 Bomgar-Gerät 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 Bomgar-Gerät authentifiziert werden können.

Keytab-Datei importieren

Hochladen

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 Bomgar-Gerät hoch.

Berichte: Berichte zu Sitzungsaktivitäten

Berichte :: Zugriff

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).

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.

Benutzer

Wählen Sie im Dropdown-Menü die Art der Benutzerteilnahme aus, die Sie hinzufügen möchten. Sie können Sitzungen wählen, an denen bestimmte Benutzer oder beliebige Benutzer eines Teams teilgenommen haben, einschließlich Sitzungen, die dem angegebenen Team nie zugeordnet waren.

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.

Bericht für Zugriffssitzung

Sie können alle Sitzungen anzeigen, die den auf der vorherigen Seite angegebenen Kriterien entsprechen.Sitzungsberichte umfassen grundlegende Sitzungsinformationen, zusammen mit Links zu Sitzungsdetails, Chat-Mitschriften und Videoaufzeichnungen von Bildschirmfreigabe- und Befehlsshell-Sitzungen.

Zugriffssitzungsdetails

Sitzungsberichte enthalten eine detaillierte Abschrift des Chats, die Zahl der übertragenen Dateien 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.

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 Eingabeaufforderungsaufzeichnung aktiviert, können Sie auch die Aufzeichnungen und/oder Textabschriften aller während der Sitzung ausgeführten Befehlsshells anzeigen. Alle Aufzeichnungen werden im Bomgar-Gerät im Raw-Format gespeichert und beim Anzeigen oder Herunterladen in ein komprimiertes Format konvertiert.

Zugriffszusammenfassungsbericht

Zusammenfassungsberichte bieten einen Überblick über die Aktivitäten in einem bestimmten Zeitraum und sind nach Benutzer kategorisiert. Statistiken umfassen die Gesamtanzahl ausgeführter Sitzungen, die durchschnittliche Anzahl von Sitzungen nach Wochentag und die durchschnittliche Dauer der Sitzungen.

Berichte :: Teamaktivität

Bereichsbeginn, Dauer, Bereichsende

Wählen Sie das Startdatum, für das Berichtsdaten abgerufen werden sollen. Wählen Sie dann entweder die Anzahl von Tagen, für die Ihr Bericht abgerufen werden soll, oder ein Enddatum.

Beschränkt auf

Wählen Sie das Team, für das Sie Aktivitätsprotokolle anzeigen möchten.

Teamaktivitätsbericht

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 oder abmelden, Chatnachrichten, die zwischen Teammitgliedern ausgetauscht werden, Benutzer-zu-Benutzer-Bildschirmfreigabeaktionen entsprechend der Protokollierung im Chat und alle freigegebenen und heruntergeladenen Dateien.

Verwaltung

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

Software :: Sicherungseinstellungen

Eine bewährte Methode bei der Notfallwiederherstellung besteht darin, regelmäßig eine Sicherungskopie Ihrer Software-Einstellungen zu speichern. Bomgar empfiehlt, dass Sie die Konfiguration Ihres Bomgar-Geräts jedes Mal sichern, wenn Sie dessen Einstellungen ändern. Bei einem Hardware-Ausfall kann eine Sicherungskopie die Wiederherstellung beschleunigen und Bomgar ggf. erlauben, Ihnen Zugriff auf temporäre Hostdienste zu gewähren, während die Einstellungen aus Ihrer letzten Sicherung beibehalten werden.

Sicherungskennwort

Um Ihre Softwaresicherungsdatei mit einem Kennwort zu schützen, erstellen Sie ein Kennwort. Wenn Sie sich entscheiden, ein Kennwort festzulegen, können Sie nicht wieder auf die Sicherungskopie zurücksetzen, ohne das Kennwort anzugeben.

Protokollierten Verlauf aufnehmen

Wird diese Option aktiviert, wird Ihre Sicherungsdatei Sitzungsprotokolle enthalten. Wird sie nicht aktiviert, werden Sitzungsberichtsdaten nicht in die Sicherung aufgenommen.

Sicherung herunterladen

Speichern Sie eine Sicherungskopie der Softwarekonfiguration. Speichern Sie diese Datei an einem sicheren Ort.

Software :: Einstellungen wiederherstellen

Sicherungsdatei

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

Sicherungskennwort

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

Sicherung hochladen

Laden Sie die Sicherungsdatei auf Ihr Bomgar-Gerät hoch und stellen Sie die Einstellungen Ihrer Website wieder her, entsprechend der Einstellungen in der Sicherungsdatei.

Software :: Aktualisierung hochladen

Verwenden Sie **Softwareaktualisierung hochladen**, um neue Softwarepakete von Bomgar manuell hochzuladen. Sie werden gefragt, ob Sie das Softwarepaket hochladen möchten. Im Abschnitt **Hochgeladene Aktualisierung** werden weitere Informationen angezeigt, um Ihr hochgeladenes Paket zu verifizieren. Klicken Sie **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 Gerät 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 Bomgar-Gerät.

Hinweis: *Ihr Bomgar Geräte-Administrator kann auch die Funktion* ***Auf Aktualisierungen prüfen*** *der /appliance-Schnittstelle verwenden, um automatisch nach neuen Softwarepaketen zu suchen und diese zu installieren.*

Sicherheit: Verwalten der Sicherheitseinstellungen

Sicherheit :: Optionen

Mindestlänge des Kennworts

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.

Kennwortrücksetzung aktivieren

Legen Sie für lokale Benutzerkonten Regeln dazu fest, ob ein vergessenes Kennwort nach korrekter Antwort auf eine Sicherheitsfrage zurückgesetzt werden kann.

Gespeicherte Anmeldungen aktivieren

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

Sperren des Kontos nach

Legen Sie fest, wie oft ein falsches Kennwort eingegeben werden darf, bevor das Konto gesperrt wird.

Sitzung abbrechen, wenn Konto verwendet wird

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

Synchronisierungsmodus für Zwischenablage

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

- **Nicht erlaubt** – Der Benutzer darf auf die Zwischenablage des Remote-Computers nicht zugreifen und diese nicht ändern.
- – Der Benutzer kann auf eine Schaltfläche klicken, um den Inhalt der lokalen Zwischenablage an die Zwischenablage des Remote-Computers zu senden.
- **Berechtigt, die Zwischenablage manuell in eine Richtung zu senden** – Der Benutzer kann auf eine Schaltfläche klicken, um den Inhalt der lokalen Zwischenablage zur Zwischenablage des Remote-Computers zu senden, oder den Inhalt der Remote-Zwischenablage an seine lokale Zwischenablage zu senden.

- **Änderungen der Zwischenablage automatisch in beide Richtungen senden** – Der Inhalt der lokalen und Remote-Zwischenablage bleibt automatisch gleich.

Sie MÜSSEN die Software auf der Statusseite neu starten, damit diese Einstellung wirksam wird.

SSL-Zertifikatprüfung

Kann die Zertifizierungskette nicht ordnungsgemäß überprüft werden, wird die Verbindung nicht zugelassen.

Wenn die Zertifikatprüfung deaktiviert wurde und dann wieder aktiviert wird, werden alle Konsolen und Clients automatisch bei der nächsten Verbindung aktualisiert. Bitte beachten Sie, dass die LDAP Connection Agents nicht automatisch aktualisiert werden, sondern erneut installiert werden müssen, damit diese Einstellung in Kraft tritt.

Ist die **SSL-Zertifikatprüfung** aktiviert, werden zusätzlich zur integrierten Sicherheit in Bomgar Sicherheitsprüfungen durchgeführt, um die SSL-Zertifizierungskette zu überprüfen, die für die sichere Kommunikation verwendet wird. Es wird dringend empfohlen, die SSL-Prüfung zu aktivieren. Ist die Zertifikatprüfung deaktiviert, wird auf Ihrer Verwaltungsschnittstelle eine Warnmeldung angezeigt. Sie können diese Meldung 30 Tage lang ausblenden.

> ***Hinweis:*** *Zur Aktivierung des SSL-Zertifikats müssen Sie das SSL-Zertifikat Bomgar zur Verfügung stellen, damit das Zertifikat in die Bomgar-Software eingebettet werden kann.*

Aufbewahrungszeitraum für Protokollinformationen (in Tagen)

Legen Sie in Aufbewahrungszeitraum für **Protokollinformationen (in Tagen)** fest, wie lange Anmeldeinformationen im Bomgar-Gerät gespeichert bleiben sollen. Diese Information umfasst auch die Berichtdaten und Aufnahmen der Sitzung.

Vorab ausgetauschter Schlüssel zur Kommunikation zwischen Geräten

Geben Sie ein Kennwort in das Feld **Geräteübergreifender, vorab geteilter Kommunikationsschlüssel** ein, um eine vertrauenswürdige Verbindung zwischen zwei Geräten herzustellen. Für zwei oder mehr Geräte 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.

Sicherheit :: Netzwerkbeschränkungen

Sie können bestimmen, welche IP-Netzwerke auf /login und /api auf Ihrem Bomgar-Gerät zugreifen können.

Von jedem Netzwerk zulassen

Es werden keine Netzwerkbeschränkungen festgelegt.

Nur die folgenden Netzwerke zulassen

Nur die aufgeführten IP-Adressen können auf Ihr Bomgar-Gerät auf /login oder /api zugreifen.

Nur die folgenden Netzwerke ablehnen

Alle außer den aufgeführten IP-Adressen können auf Ihr Bomgar-Gerät auf /login oder /api zugreifen.

Wenn Sie **Nur bei erster Authentifizierung des Benutzers** auswählen, muss sich der Benutzer bei der ersten Anmeldung in der Zugriffskonsole in einem zugelassenen Netzwerk befinden. Zu diesem Zeitpunkt wird ein Token für das Gerät ausgestellt, sodass weitere Anmeldungen in der Zugriffskonsole über beliebige Netzwerkstandorte erfolgen können.

Wenn Sie **Immer** wählen, muss sich der Benutzer jedes Mal, wenn er sich in der Zugriffsknosole anmeldet, in einem zugelassenen Netzwerk befinden.

Wenn Sie **Nie** wählen, kann ein Benutzer von jedem Netzwerkstandort aus auf die Zugriffskonsole zugreifen.

Sicherheit :: Port-Einschränkungen für die Verwaltungs-Webschnittstelle

Legen Sie die Ports fest, über die der Zugriff auf Ihre /login-Schnittstelle möglich sein soll.

Website-Konfiguration: HTTP-Ports festlegen, Erforderliche Anmeldungsvereinbarung aktivieren

Website :: HTTP

HTTP-Port und HTTPS-Port

Erfahrene Netzwerktechniker, die in nicht standardmäßigen Netzwerkumgebungen arbeiten, können die von Bomgar 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.

Website :: Erforderliche Anmeldungsvereinbarung für /login

Anmeldungsvereinbarung aktivieren

Sie können eine Anmeldungsvereinbarung aktivieren, die Benutzer annehmen müssen, bevor Sie auf die /login-Verwaltungsschnittstelle 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

Konfiguration :: E-Mail-Adresse

Hinweis: *Wenn Ihr Gerät als Backup-Gerät oder Datenverkehrsknoten verwendet wird, wird die E-Mail-Konfiguration dieses Geräts mit der E-Mail-Konfiguration überschrieben, die auf dem primären Master-Gerät definiert wurde.*

Von-Adresse

Legen Sie die E-Mail-Adresse fest, von der automatische Nachrichten Ihres Bomgar-Geräts versendet werden sollen.

Konfiguration :: SMTP-Relay-Server

Konfigurieren Sie Ihr Bomgar-Gerät 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 SSL-Verschlüsselung unterstützt, wählen Sie **SSL** oder **TLS**. Wählen Sie andernfalls **Keine**.

SMTP-Benutzername

Wenn für den SMTP-Server eine Authentifizierung erforderlich ist, geben Sie einen Benutzernamen ein.

SMTP-Kennwort

Wenn für den SMTP-Server eine Authentifizierung erforderlich ist, geben Sie ein Kennwort ein.

Konfiguration :: 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.

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 **Änderungen speichern** klicken.

Tägliche Kommunikationsmitteilung schicken

Das Bomgar-Gerät 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 Backup-Knoten überein.
- Während einer Failover-Statusprüfung wird eines der folgenden Probleme erkannt:
    - Das aktuelle Gerät 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 Backup-Knoten konnte den primären Knoten nicht kontaktieren, und auch nicht eine der Test-IP-Adressen, die auf der Seite **Verwaltung > Failover** konfiguriert wurden.
    - Der Backup-Knoten konnte keine der Test-IP-Adressen kontaktieren, die auf der Seite **Verwaltung > Failover** konfiguriert wurden.
    - Die Backup-Vorgänge des Backup-Knoten wurden auf der Seite **Verwaltung > Failover** deaktiviert.
    - Der Backup-Knoten konnte unerwarteterweise keine Prüfung von sich selbst vornehmen. Dies deutet auf einen Defekt hin.
    - Der Backup-Knoten konnte den primären Knoten nicht mit dem Hostnamen des primären Knotens erreichen.
    - Automatischer Failover ist deaktiviert und der Backup-Knoten konnte keine Prüfung des primären Knotens vornehmen.
    - Automatischer Failover ist aktiviert und der Backup-Knoten konnte keine Prüfung des primären Knotens vornehmen. Der Backup-Knoten wird automatisch zum pimären Knoten, wenn der primäre Knoten weiterhin nicht antwortet.
    - Automatischer Failover ist aktiviert und der Backup-Knoten 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 Backup-Knoten vornehmen.

Ausgehende Ereignisse: Ereignisse für die Auslösung von Nachrichten festlegen

Ausgehende Ereignisse :: HTTP-Empfänger

Sie können Ihr Bomgar-Gerät darauf konfigurieren, Nachrichten an einen HTTP-Server oder an eine E-Mail-Adresse zu senden, wenn verschiedene Ereignisse ausgelöst werden.

Die vom Bomgar-Gerät 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 Bomgar-Gerät das aktuelle Ereignis wieder in die Warteschlange ein und versucht es später noch einmal.

Neuen HTTP-Empfänger hinzufügen, bearbeiten, löschen

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

Ausgehende Ereignisse :: HTTP-Empfänger hinzufügen oder bearbeiten

Name

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

URL

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

Deaktiviert

Wählen Sie das Kontrollkästchen **Deaktiviert**, um die Meldungen für den eingerichteten Ereignis-Handler zu stoppen, beispielsweise etwa im Falle eines geplanten Integrationstests.

CA-Zertifikat

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

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.

Ausgehende Ereignisse :: E-Mail-Empfänger

Neuen E-Mail-Empfänger hinzufügen, bearbeiten, löschen

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

Aktueller Status

Zeigt eine kurze Statusmitteilung vom SMTP-Relay-Server an. Solange das Gerät 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.

Ausgehende Ereignisse :: E-Mail-Empfänger hinzufügen

Bevor Sie Ihr Bomgar-Gerät dafür einrichten können, Ereignisnachrichten an eine E-Mail-Adresse zu senden, müssen Sie sicherstellen, dass Ihr Bomgar-Gerät für Ihren SMTP-Relay-Server konfiguriert ist. Gehen Sie zur Seite **Verwaltung > E-Mail-Konfiguration**, um die Einstellungen zu überprüfen.

Name

Erstellen Sie einen eindeutigen Namen, um dieses Objekt 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.

Deaktiviert

Wählen Sie das Kontrollkästchen **Deaktiviert**, um die Meldungen für den eingerichteten Ereignis-Handler zu stoppen, beispielsweise etwa im Falle eines geplanten Integrationstests.

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. Verwenden Sie eines der unten auf der /login-Seite aufgeführten Makros, um den Text für Ihre Zwecke anzupassen.

Text

Passen Sie den Text dieser E-Mail an. Verwenden Sie eines der unten auf der /login-Seite aufgeführten Makros, um den Text für Ihre Zwecke anzupassen.

Failover: Einrichten eines Backup-Geräts für Failover

Failover :: Konfiguration

Neue Verbindungsdetails für den Backup-Standort: Hostname oder IP-Adresse

Geben Sie den Hostnamen oder die IP-Adresse des Bomgar-Geräts ein, das sie als Backup-Gerät in einer Failover-Beziehung verwenden möchten.

TLS-Port

Geben Sie den TLS-Port ein, der diesem primären Gerät gestattet, eine Verbindung zum Backup-Gerät herzustellen.

Verbindungsdetails zu dieser primären Website umleiten: Hostname oder IP-Adresse

Geben Sie den Hostnamen oder die IP-Adresse des Bomgar-Geräts ein, das Sie als primäres Gerät in einer Failover-Beziehung verwenden möchten.

TLS-Port

Geben Sie den TLS-Port ein, der dem Backup-Gerät gestattet, eine Verbindung zu diesem primären Gerät herzustellen.

Failover :: Status

Status dieses Hosts

Zeigen Sie den Hostnamen dieser Seite an, zusammen mit dem Status der primären Site-Instanz oder Sicherungssite-Instanz.

Status des Peer-Hosts

Zeigen Sie den Hostnamen dieser Seite an, zusammen mit dem Status der primären Site-Instanz oder Sicherungssite-Instanz. Außerdem können Sie das Datum und den Zeitpunkt der letzten Statusüberprüfung anzeigen.

Statusverlauf

Sie können die Tabelle der erfolgten Statusereignisse erweitern oder einklappen.

Failover :: 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 Gerät und dem Backup-Gerät erzwingen.

Als Sicherungs-/Primärinstanz festlegen

Sie können die Rollen mit dem Peer-Gerät 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-Gerät synchronisieren wollen, wählen Sie diese Option. Wenn diese Option ausgewählt wird, wird die Verbindung für alle Benutzer auf dem bestehenden primären Gerät 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-Gerät nicht kontaktiert werden kann. Wenn diese Option nicht aktiviert wird, wird der Failover abgebrochen, wenn beide Geräte hinsichtlich ihrer Failover-Rollen (ein Primär- und ein Sicherungsgerät) nicht synchronisiert bleiben können.

Wenn Sie beispielsweise wissen, dass das aktuelle Sicherungsgerät 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 Gerät seine Rolle als Primär- oder Sicherungsgerät verliert.

Failover :: 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 Sicherungssite 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.

Failover :: 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.

Sicherungs-Vorgänge aktivieren

Site-Backups 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 Sicherungssite ein, um zu bestimmen, ob die primäre Site vom Backup 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

API :: Konfiguration

XML-API aktivieren

Sie können die Bomgar XML API aktivieren, sodass Sie Berichte ausführen und Befehle ausgeben können, wie z. B. Start oder Übertragung von Sitzungen von externen Anwendungen aus, sowie die automatische Sicherung Ihrer Softwarekonfiguration.

Hinweis: *Nur die Aufrufe* ***Befehl****,* ***Berichte*** *und* ***Client-Skripting-API*** *werden durch diese Einstellung aktiviert/deaktiviert. Andere API-Aufrufe werden unter Öffentliche Portale konfiguriert. Detailliertere Informationen finden Sie im API-Programmierhandbuch.*

HTTP-Zugriff auf XML-API zulassen

Standardmäßig ist der Zugriff auf die API SSL-verschlüsselt. Sie können jedoch auch einen unverschlüsselten HTTP-Zugang zulassen. Es wird als bewährte Sicherheitsmethode dringend empfohlen, den HTTP-Zugriff nicht zuzulassen.

API :: Benutzerdefinierte Felder

Erstellen Sie benutzerdefinierte API-Felder, um Informationen über Ihren Kunden zu sammeln. So können Sie Bomgar tiefer mit ihren bestehenden Programmen integrieren. Benutzerdefinierte Felder müssen zusammen mit der Bomgar API verwendet werden. Detailliertere Informationen finden Sie im API-Programmierhandbuch.

Neues Feld erstellen, bearbeiten, löschen

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

API :: Benutzerdefinierte Felder :: Hinzufügen oder Bearbeiten

Anzeigename

Erstellen Sie einen eindeutigen Namen, um dieses Objekt 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, wird automatisch einer erstellt.

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.

Support: Technischen Bomgar-Support kontaktieren

Bomgar-Support - Kontaktinformationen

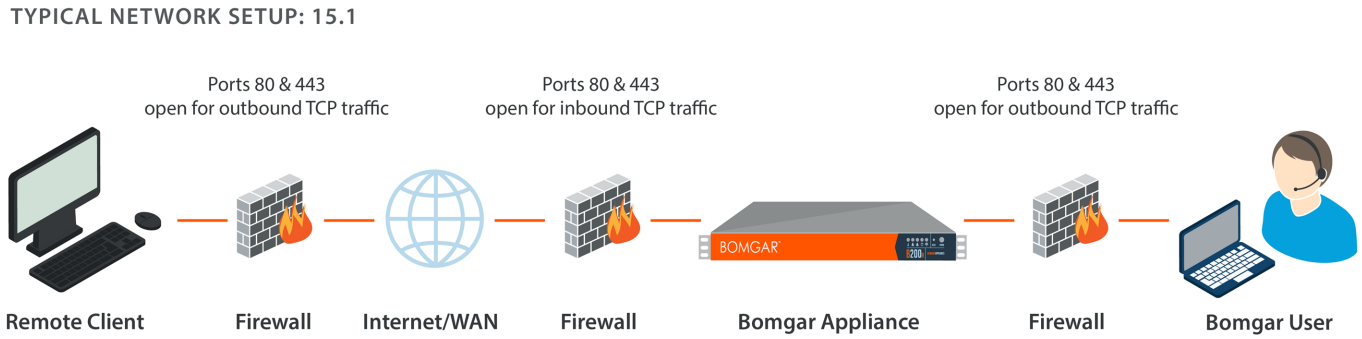
Die Support-Seite enthält Kontaktinformationen, falls Sie mit einem Mitarbeiter des technischen Bomgar-Supports in Verbindung treten müssen.

Erweiterter technischer Support von Bomgar

Muss ein Mitarbeiter des technischen Bomgar-Supports auf Ihr Gerät zugreifen, stellt er Ihnen Support-, Zugriffs- und Übersteuerungscodes bereit, die Sie auf dieser Seite eingeben, um einen geräteseitig initiierten, voll verschlüsselten Support-Tunnel zurück zu Bomgar zu erstellen und komplexe Probleme schnell zu beheben.

Ports und Firewalls

Bomgar-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 Netzwerkeinrichtung. Weitere Informationen finden Sie im Bomgar Installationshandbuch für Gerätehardware.
- Internetsicherheits-Software wie Software-Firewalls darf nicht den Download von ausführbaren Bomgar-Dateien 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-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 Gerätestandort finden Sie unter www.bomgar.com/docs/content/deployment/dmz/firewall-rules.htm.

Sollten weiterhin Probleme beim Herstellen einer Verbindung auftreten, wenden Sie sich an den technischen Bomgar-Support unter help.bomgar.com.

Haftungsausschlüsse, Lizenzierungsbeschränkungen und Technischer Support

Haftungsausschlüsse

Dieses Dokument dient ausschließlich Informationszwecken. Bomgar 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. Bomgar 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.

BOMGAR, BOMGAR BOX, mark B, JUMP und UNIFIED REMOTE SUPPORT sind Warenzeichen von Bomgar Corporation. Andere erwähnte Warenzeichen sind Eigentum ihrer jeweiligen Inhaber.

Lizenzierungsbeschränkungen

Eine Bomgar Privileged Access Management-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 Bomgar fühlen uns verpflichtet, Service von höchster Qualität zu bieten, indem wir gewährleisten, dass unsere Kunden alles haben, was sie für einen Betrieb bei maximaler Produktivität benötigen. Sollten Sie Hilfe benötigen, wenden Sie sich an den technischen Bomgar-Support unter help.bomgar.com.

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